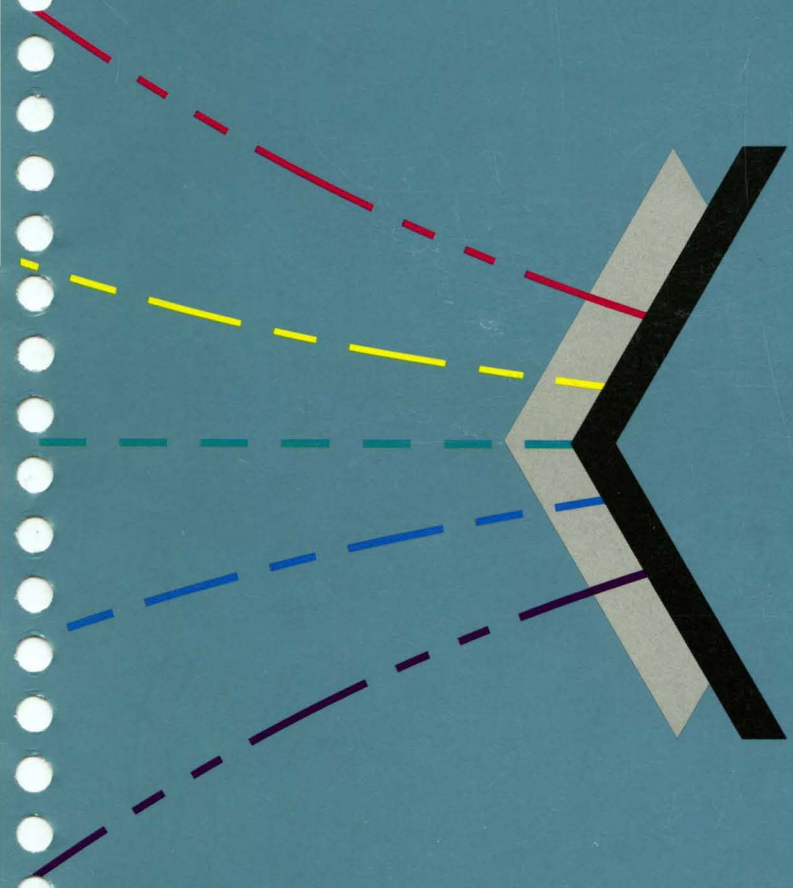
WELLFLEET communications



CONFIGURATION GUIDE

VOLUME II

Wellfleet Configuration Guide

Volume II

Wellfleet Communications, Inc.

Printed in U.S.A.

December 1991

Part # 103609 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

11 Configuring DECnet Phase IV

This chapter tells you how to configure the DECnet Phase IV Router.

As DECnet Phase IV supports large networks (in theory, over 64,000 nodes), a Phase IV network is partitioned into distinct non-overlapping areas. Each area is assigned a network-unique ID (from 1 to 63); each node is assigned an area-unique ID (from 1 to 1023).

Phase IV routing is hierarchical. Routing *within* an area is called Level 1 routing; routing *between* areas is called Level 2 routing. Level 2 routers maintain paths to destination areas. Level 1 routers, in contrast, maintain paths to local nodes, and keep track of the identity of the nearest Level 2 router within the area. When a level 1 router receives a packet destined for a remote area, it forwards the packet to the nearest Level 2 router. The packet then travels via Level 2 routing to the destination area where it is delivered to the packet recipient by a Level 1 router.

The functions of a DECnet router include: determining the location of the other routers and nodes within the local area, determining the location of the nearest Level 2 router, building the network's topology on the basis of this information, and then deciding on the best route for a particular packet to follow.

A DECnet router periodically transmits *hello* and *topology* messages to determine the location of, and the characteristics of the nodes and other routers in the network. The information contained in these messages enables the router to develop the network's topology and to determine the best route to each node in the network. The router uses a connectivity algorithm to maintain path lengths, and a traffic-assignment algorithm to maintain path costs. The information derived from these algorithms is used to update the router's database.

When the router receives a packet, it first checks the destination address contained in the packet's header. If the packet is intended for a local node, the router returns the packet to the local network. If the packet is intended for a remote node, the router selects the least cost path (not necessarily the shortest path) to the destination and forwards the packet.

If the router determines that a packet's destination is not known, or is for some reason unreachable, the router checks the packet's header information to determine whether the packet should be returned to its source address or simply discarded.

11.1 Filtering DECnet Phase IV Packets

Filters enable the router to relay or drop a particular frame based on the contents of specific fields within the DECnet Phase IV packet. Filters examine the following packet fields either singly or in combination: destination area, destination node, source area, and source node. Filters also examine bits 1, 2, and 3 of the Routing Layer control flag which identify the packet type. Table 11-1 list packet types.

Table 11-1: DECnet Phase IV Packet Types

Value	Type
0	Initialization message
1	Verification message
2	Hello and Test messages
3	Level 1 Routing message
4	Level 2 Routing message
5	Ethernet Router Hello message
6	Ethernet Endnode Hello message

Filtering decisions are based on user-defined rules. A DECnet filter rule consists of a DECnet packet 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 packet field and the value; an action (*drop* or *forward*); and a filter precedence.

For example, the DECnet Filter-rule-A shown graphically in Figure 11-1 prevents routing updates emanating from a suspect router (DECnet network address, 100; DECnet node address, 10) from being promulgated throughout the network.

DECnet Filter-rule-B isolates a DECnet host device (network number 50; node ID, 250), probably storing sensitive or confidential access, from all access except from a single host device (network number 62; host number 13)

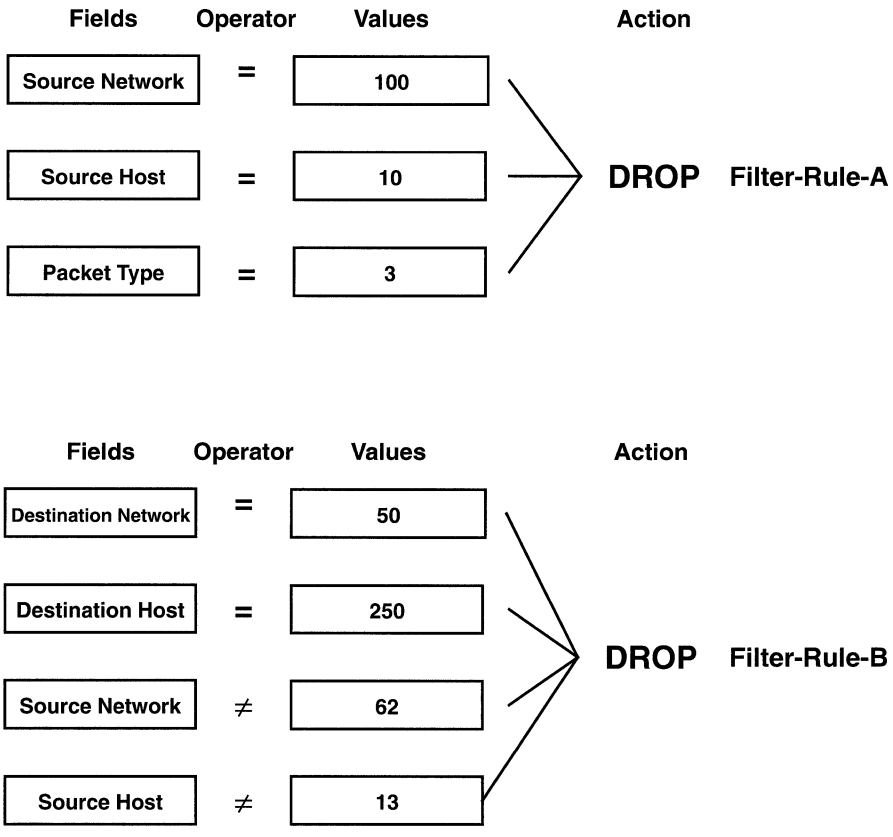


Figure 11-1 DECnet Sample Filters

11.2 Setting DECnet Phase IV Basic Parameters

To begin DECnet Phase IV configuration, you assign values to basic parameters. The basic parameters (listed in Table 11-2) apply to the entire router, rather than to individual circuit groups.

Table 11-2: DECnet Phase IV Basic Parameters

Parameter	Function
Auto Enable	specifies the initialization state
Max. Area	specifies the size of the DECnet network
Max. Nodes	specifies area size
Area	identifies the local DECnet area
Node	assigns a DECnet node_id to the router
Area Max. Hops	specifies an inter-area network diameter
Max. Hops	specifies a node-to-node network diameter
Area Max. Cost	specifies an inter-area transit cost
Max. Cost	specifies a node-to-node transit cost
Max. Visits	specifies the number of times a packet can cross the router
Max. Bcast Endnodes	specifies the number of adjacent nodes
Bcast Routing Timer	specifies the interval between topology packets

You set DECnet Phase IV basic parameters from the Configuration Menu. At **Enter Selection (0 for Previous Menu)** enter the number that appears to the left of **DECNET IV Routing Service.** The screen displays the following:

No DECNET IV Routing Service record(s) found
Do you wish to add DECNET IV Routing Service record(s)?

Press `[RETURN]` to display the DECnet IV Basic Parameters Screen (Figure 11-2).

- **Auto Enable** specifies the initial state of the DECnet IV router.

  This DECnet-specific **Auto Enable** works in conjunction with global auto enable (refer to Section 2.1) to enable or disable DECnet Phase IV when the router boots.

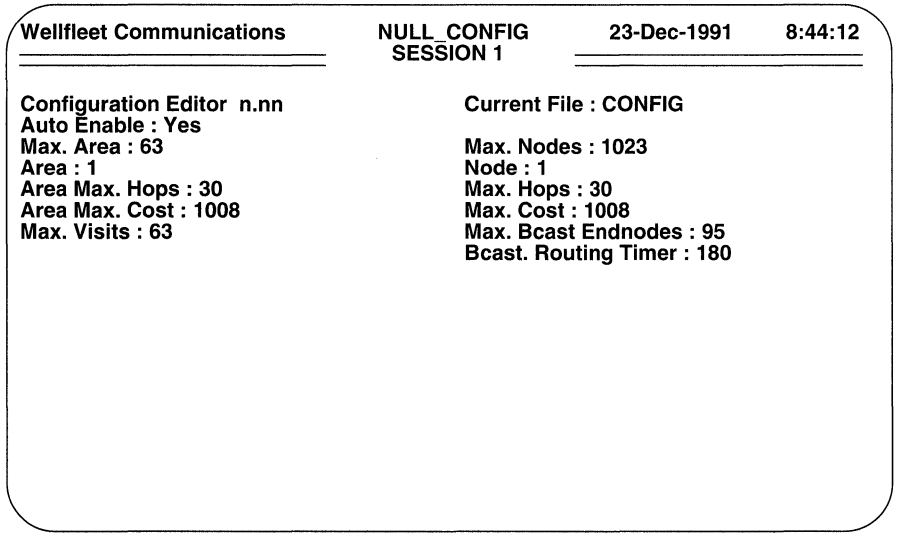


Figure 11-2 DECnet IV Basic Parameters Screen

When global auto enable is **No**, DECnet Phase IV is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable DECnet Phase IV with NCL commands after the router boots.

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

- **Max.Area** (a Level 2 parameter referred to as *NA* by DEC) specifies the maximum area number in the Phase IV network.

  Enter the highest area ID number in your network (within the range 1 to 63), then press `[RETURN]`.

- **Max. Nodes** (referred to a s *NN* by DEC) contains the maximum address (highest node number) within an area.

  Enter the highest node number in the Phase IV network (within the range 1 to 1023), then press `[RETURN]`.

NOTE

All routers within the Phase IV network must be configured with the same **Max. Area** and **Max. Nodes** values.

- **Area** contains the DECnet ID number of the local area.

  Enter the area ID (from 1 to 63).

- **Node** contains the DECnet ID number of the router.

  Enter the node ID.

NOTE

DECnet Phase IV uses the Area and Node parameters to derive a unique MAC-level address for the DECnet Phase IV router. DECnet first derives a 16-bit binary address by prepending **Area** (expressed as an 6-bit binary value) to **Node** (expressed as an 10-bit binary value). DECnet then swaps the bytes and converts the resulting 16-bit binary value to 4-digit hexadecimal. The MAC address is formed by appending the 4-digit hexadecimal value to hexadecimal AA 00 04 (the Digital Equipment Corporation vendor code) 00 (a pad to ensure a 12-digit hexadecimal address). Thus Node 32, in Area 256 equates to the MAC address AA 00 04 00 00 81.

- **Area Max. Hops** (a Level 2 parameter referred to as *AMaxh* by DEC) specifies the maximum path length to any area.

  When computing **Area Max. Hops**, DEC suggests a value equal to twice the worst-case longest path length in hops. Enter this value or another value (up to a maximum of 30).

- **Max. Hops** (referred to a s *Maxh* by DEC) specifies the maximum path length in an area.

  The range of values is 1 to 30. When you set this parameter, ensure that its value is equal to or exceeds the value of **Area Max. Hops**.

- **Area Max. Cost** (a Level 2 parameter referred to as *AMaxc* by DEC) specifies the maximum path cost to any area.

  DECnet determines path costs on the basis of the sum of the individual, sequential *circuit costs*. Circuit costs are decimal values (from 1 to 25) that reflect the relative speed of the transmission media: the faster the media, the lower the cost.

  Table 11-3 lists suggested circuit costs for transmission media of various speeds.

Table 11-3: Suggested DECnet Circuit Cost Values

Speed	Cost	Speed	Cost
100Mb/sec	1	64Kb/sec	14
16Mb/sec	2	56Kb/sec	15
10Mb/sec	3	38.4Kb/sec	16
4Mb/sec	5	32Kb/sec	17
1.54Mb/sec	7	19.2Kb/sec	18
1.25Mb/sec	8	9.6Kb/sec	19
833Kb/sec	9	7.2Kb/sec	20
625Kb/sec	10	4.8Kb/sec	21
420Kb/sec	11	2.4Kb/sec	22
230.4Kb/sec	12	1.2Kb/sec	25
125Kb/sec	13		

For example, the recommended cost for an Ethernet circuit is 3, and the cost of a full T1 circuit is 7. If a path traverses a T1 circuit followed by an Ethernet circuit, the path cost is 10. Referring to Figure 11-3, the cost from A to C by way of B is 14; the cost from A to C directly is 15.

The range of allowable values is from 1 to 1008.

- **Max. Cost** (referred to a s *Maxc* by DEC) specifies the maximum network path cost (the cost of a path to any *node* in the network).

  When you set this parameter, ensure that its value is equal to or exceeds the value of **Area Max. Cost**.

- **Max. Visits** (referred to a s *Maxv* by DEC) enables packet lifetime control by designating the number of times a packet can pass through the router. Such a limitation prevents a corrupted packet, or a packet whose destination has become unreachable, from continuously traveling through the network.

  Ensure that you select a value that is greater than or equal to **Max. Hops**.

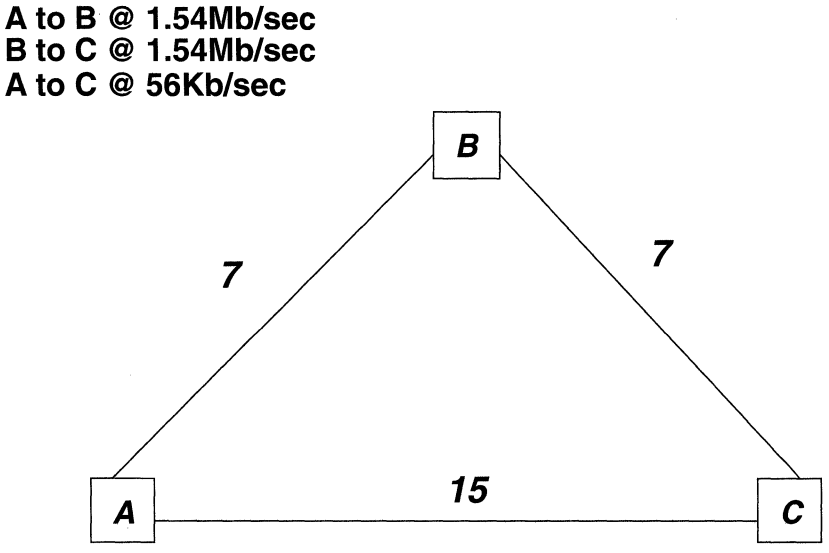


Figure 11-3 Sample DECnet Circuit Costs

- **Max. Bcast Endnodes** (referred to as *NBEA* by DEC) specifies the number of nodes adjacent to the Phase IV router on an Ethernet.

  The range of allowable values is 1 to 1023. Refer to your network topology drawing and find the largest number of adjacent nodes.

NOTE

The higher the number of adjacent nodes, the greater the impact on network performance and memory utilization.

- **Bcast. Routing Timer** specifies the maximum number of seconds between routing topology messages issued by the router.

  The range of values is 15 to 180, in increments of 15 seconds. Press the `[RIGHTARROW]` to select a value, then press `[RETURN]`.

The screen displays the DECnet IV Detailed Parameters Access Screen (Figure 11-4).

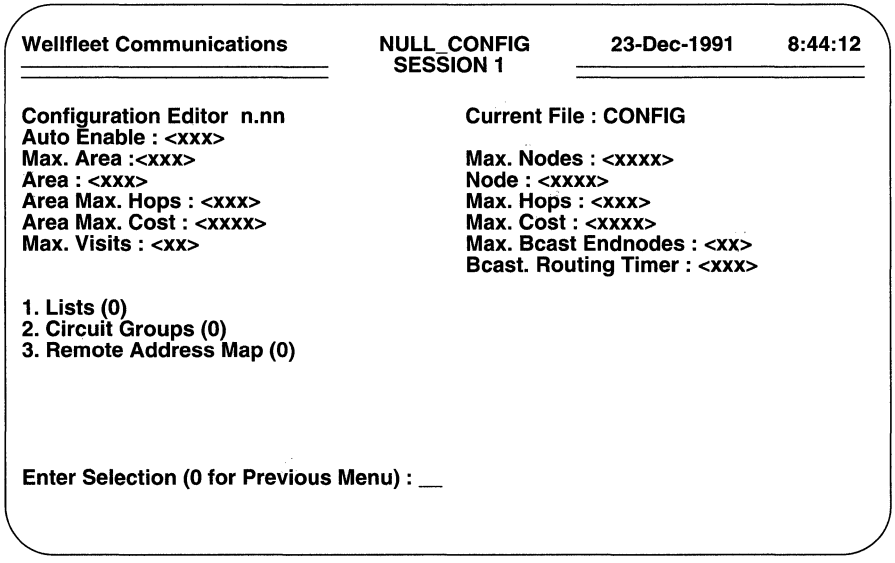


Figure 11-4 DECnet IV Detailed Parameters Access Screen

11.3 Defining DECnet Phase IV Circuit Groups

Circuit group parameters are specific for each individual circuit group, and must be set on a circuit-group-by-circuit-group basis. Circuit group parameters are listed in Table 11-4.

Table 11-4: DECnet Phase IV Circuit Group Parameters

Parameter	Function
Circuit Group Name	specifies the circuit group
Cost	assigns a circuit cost
Hello Timer	specifies the interval between Hello messages
Router Priority	assigns router priority
Number of Routers	specifies the number of routers

You set circuit group parameters from the DECnet Phase IV Detailed Parameters Access Screen. 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 DECnet IV Circuit Group Parameters Screen.

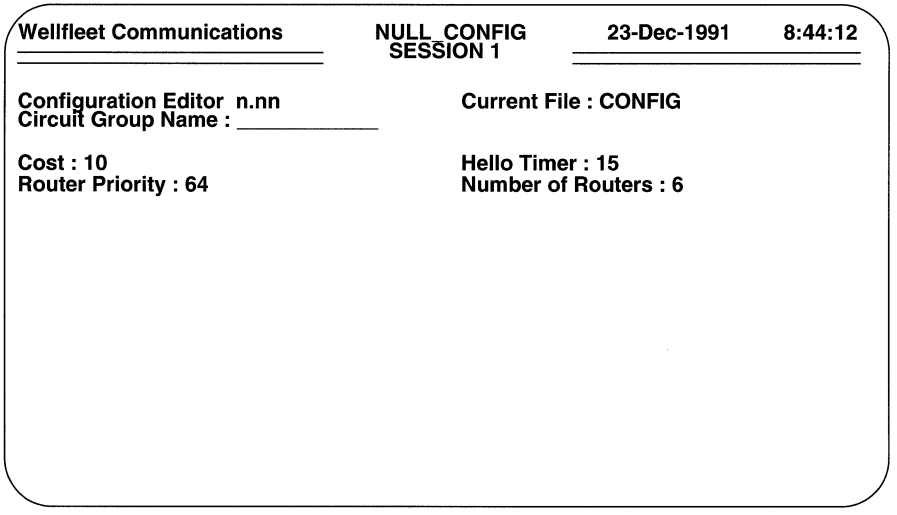


Figure 11-5 DECnet IV Circuit Group Parameters Screen

- **Circuit Group Name** identifies the circuit group.

  Enter the name of a circuit group.

- **Cost** specifies the cost of the circuit.

  Phase IV determines path costs on the basis of the *sum* of the individual *circuit costs*. The cost that you assign to a particular circuit typically reflects the speed of the transmission medium. Low costs reflect high-speed media, while high costs reflect slower media. Refer to Table 11-3 for a list of suggested DECnet circuit costs.

  Phase IV always selects the circuit(s) with the lowest cost when defining a path, so assigning each circuit a cost is, in effect, a way of assigning it a priority. If you don't want a particular circuit to be used on a regular basis, assign it a high cost.

  The range of allowable values is 1 to 25. Press the `[RIGHTARROW]` to select a cost, then press `[RETURN]`.

- **Hello Timer** specifies the interval in seconds between DECnet *hello* messages transmitted across the circuit group.

  Select from eight possible responses (from 15 to 3600 seconds).

- **Router Priority** dictates which router will be the designated router on an Ethernet segment.

  Routers with the highest priority are called *designated routers*. Nodes on an ethernet who do not know where to send a packet, forward such packets to the designated router. Only one router on any given Ethernet can be the designated router for a given area (note that DECnet architecture allows for multiple areas on a single Ethernet).

  Valid responses are in the range of 1 to 127. The router with the highest priority becomes the designated router. If two routers share the same priority, the router with the highest node number becomes the designated router.

- **Number of Routers** (referred to as *NBRA* by DEC) specifies the number of other routers on an Ethernet.

  Refer to your network topology drawing to determine this number, then enter the value (from a minimum of 1 to a maximum of 33).

After you specify the number of routers, the screen prompts for DECnet filter data.

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

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Group Name : _____________

Cost : <xx>                                 Hello Timer : <xx>
Router Priority : <xxx>                     Number of Routers : <xx>


1. Traffic Filters (0)



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

Figure 11-6 DECnet IV Filters Access Screen

If you want to configure circuit group-specific DECnet filters, proceed to Sections 11.5, *Compiling DECnet Phase IV Filter Lists* and 11.6, *Configuring DECNet Phase IV Filters*. If you are not configuring filters, enter `<0>` at **Enter Selection (0 for Previous Menu)** to return to the DECnet IV Detailed Parameters Access Screen. You define additional DECnet router circuit groups from this screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the DECnet IV Circuit Groups Summary Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG
Auto Enable : <xxx>
Max. Area :<xxx>                            Max. Nodes : <xxxx>
Area : <xxx>                                Node : <xxxx>
Area Max. Hops : <xxx>                      Max. Hops : <xxx>
Area Max. Cost : <xxxx>                     Max. Cost : <xxxx>
Max. Visits : <xx>                          Max. Bcast Endnodes : <xx>
                                            Bcast. Routing Timer : <xxx>

                        Circuit Groups
   Circuit Group Name          Cost        Hello Timer
1. <xxxxxxx>                   <xx>        <xxx>


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

Figure 11-7 DECnet IV Circuit Groups Summary Screen

To define additional circuit groups, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the DECnet IV Circuit Group Parameters Screen. Now use the same procedure as before to define another DECnet IV circuit group. Repeat this process until you have defined all Phase IV circuit groups.

11.4 Drawing the DECnet Phase IV Remote Address Map

If you are routing DECnet Phase IV traffic across either X.25, Frame Relay or SMDS circuits, you must draw a remote address map which associates DECnet area and node addresses with WAN protocol addresses.

You draw the remote address map from the DECnet IV Detailed Parameters Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Remote Address Map record(s) found
Do you wish to add Remote Address Map record(s)?

Press **[RETURN]** to display the DECnet IV Remote Address Map Parameters Screen.

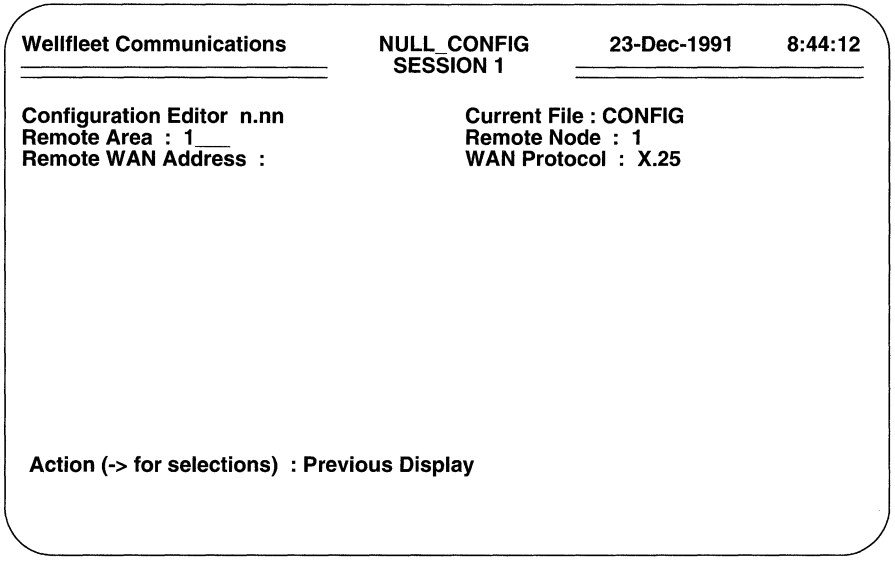


Figure 11-8 DECnet IV Remote Address Map Parameters Screen

- **Remote Area** specifies the area address of the remote target.
  Enter the area address (from 1 to 63).
- **Remote Node** specifies the node address of the remote target.
  Enter the node address (from 1 to 1023).
- **Remote WAN Address** specifies the protocol address of the remote target.
  Enter the remote target's X.25, Frame Relay, or SMDS address.
- **WAN Protocol** specifies the WAN protocol that provides service to the remote target.
  Select **X.25**, **Frame Relay**, or **SMDS**.

After you select the wide area protocol, the screen prompts **Hit Return to Continue**. Press **[RETURN]** to go back to the DECnet IV Detailed Parameters Access Screen. You add address map entries from this screen. Enter **<3>** at **Enter Selection (0 for Previous Menu)** to display the DECnet IV Remote Address Map Summary Screen (Figure 11-9).

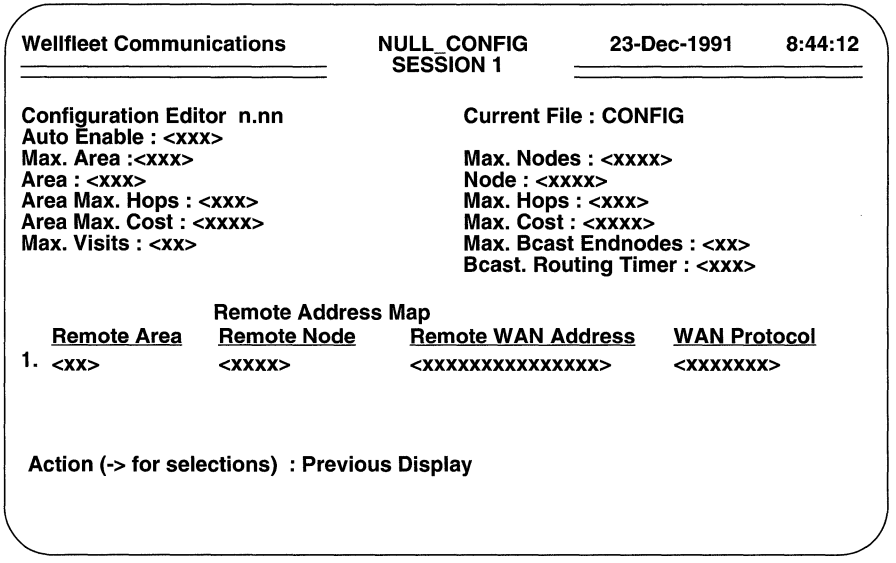


Figure 11-9 DECnet IV Remote Address Map Summary Screen

Press the `[RIGHTARROW]` to select **Add**, and then press `[RETURN]` to display the DECnet IV Remote Address Map Parameters Screen. Now follow the same procedures as before to add another address map entry. Continue until you have entered all map entries.

11.5 Compiling DECnet Phase IV 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 DECnet IV filter specifies a list name, packets are checked against the range of values specified by the list.

You compile lists from the DECnet IV 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 DECnet IV List Access Screen (Figure 11-10).

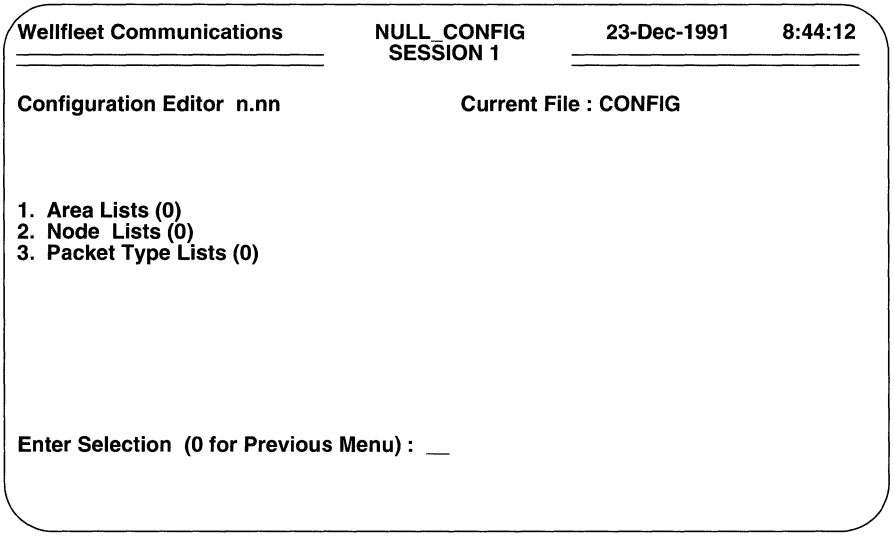


Figure 11-10 DECnet IV List Access Screen

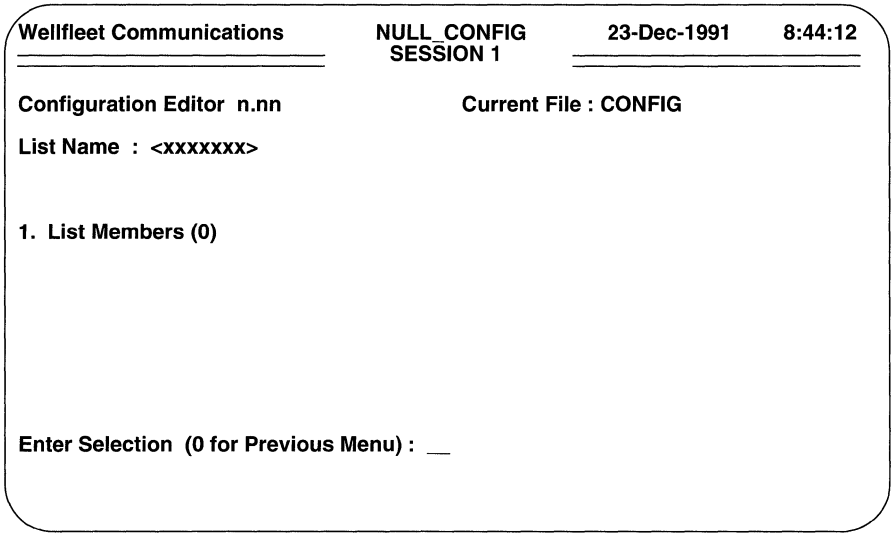


Figure 11-11 DECnet IV List Member Access Screen

11.5.1 Area Lists

Area lists specify ranges of DECnet IV area IDs.

You compile an area list from the DECnet List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the area list.

  Enter a list name.

After you name the area list, the screen prompts for list members (Figure 11-11).

To assign a range of DECnet area IDs 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 DECnet IV Area Range Screen.

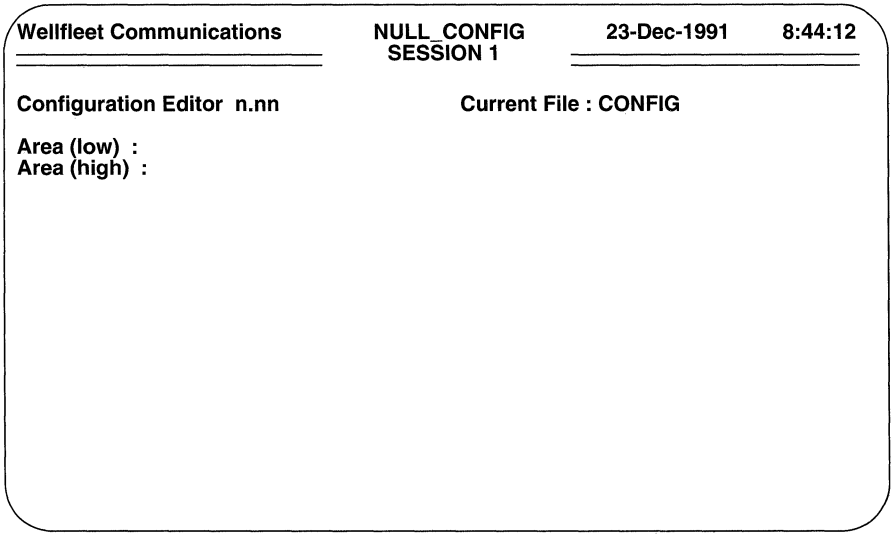


Figure 11-12 DECnet IV Area Range Screen

- **Area (low)** specifies the lower boundary of the filtered DECnet IV area ID range.

  Enter the DECnet IV area ID.

- **Area (high)** specifies the upper boundary of the filtered range.

  Enter the DECnet IV area ID, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Area (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the DECnet IV List Member Access Screen.

If you want, you can add other DECnet IV area ID ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the DECnet IV Area List Members Screen (Figure 11-13). To add another range of area IDs press the `[RIGHTARROW]` to select **Add** and then press `[RETURN]` to display the DECnet IV Area Range Screen. Now follow the same procedure as before to add another area ID range; continue in this fashion until you have added all desired ranges to the list.

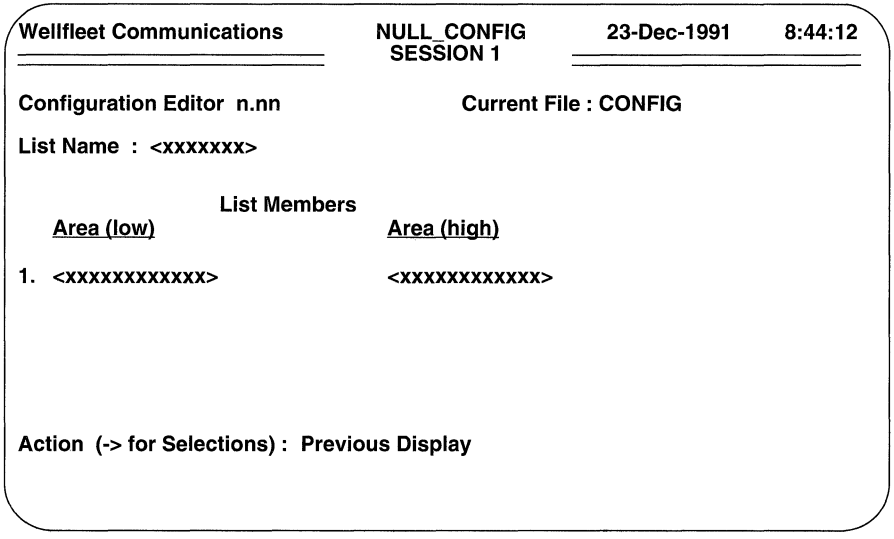


Figure 11-13 DECnet Area List Members Screen

You compile additional DECnet area lists from the DECnet IV List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the DECnet IV Area List Summary Screen (Figure 11-14).

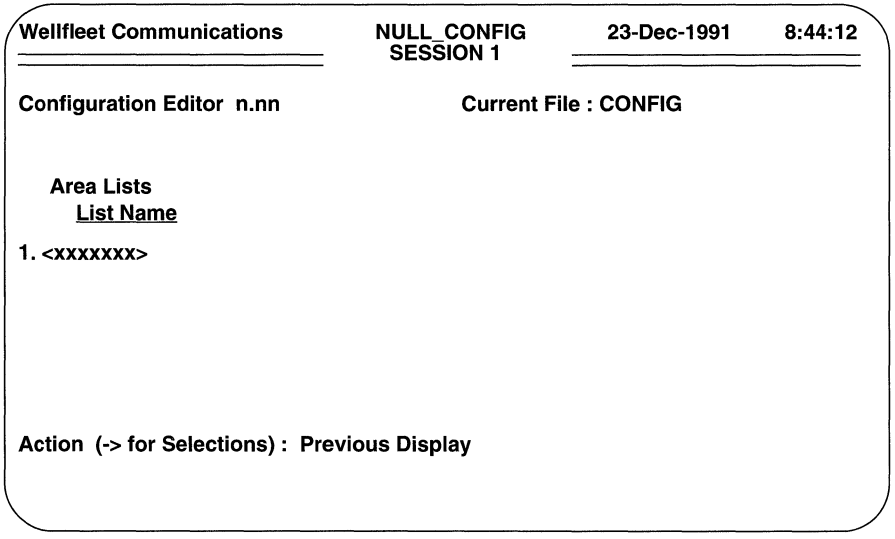


Figure 11-14 DECnet IV Area List Summary Screen

To compile another DECnet area list, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]`. Now follow the previously described procedure to construct an additional area list; repeat this procedure until you have compiled all DECnet IV area lists.

11.5.2 Node Lists

Node lists specify ranges of DECnet IV node IDs.

You compile a node list from the DECnet IV List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the node list.

  Enter a list name.

After you name the node list, the screen prompts for list members.

To assign a range of DECnet node IDs 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 DECnet IV Node Range Screen.

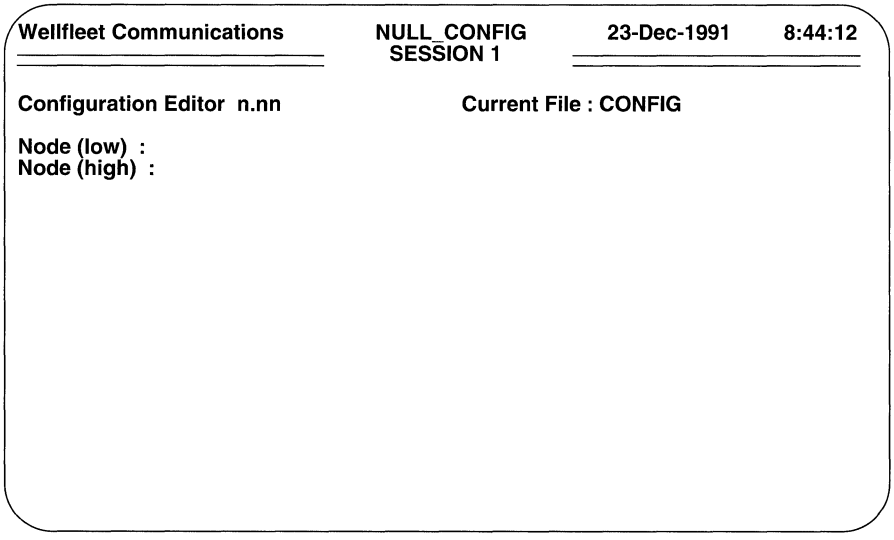


Figure 11-15 DECnet IV Node Range Screen

- **Node (low)** specifies the lower boundary of the filtered DECnet IV node ID range.

  Enter the DECnet IV node ID.

- **Node (high)** specifies the upper boundary of the filtered range.

  Enter the DECnet IV node ID, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Node (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the DECnet IV List Member Access Screen.

If you want, you can add other DECnet node ID ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the DECnet IV Node List Members Screen (Figure 11-16). To add another range of node IDs press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the DECnet IV Node Range Screen. Now follow the same procedure as before to add another node ID range; continue in this fashion until you have added all desired ranges to the list.

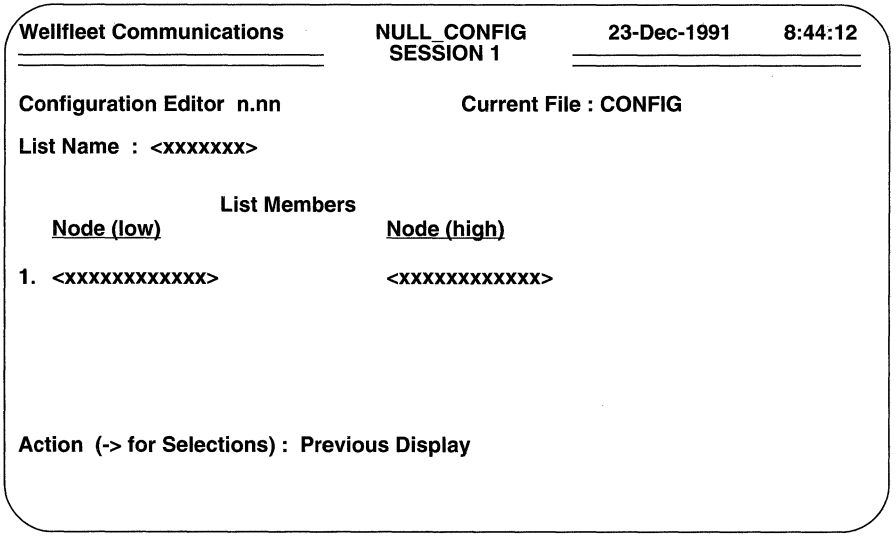


Figure 11-16 DECnet IV Node List Members Screen

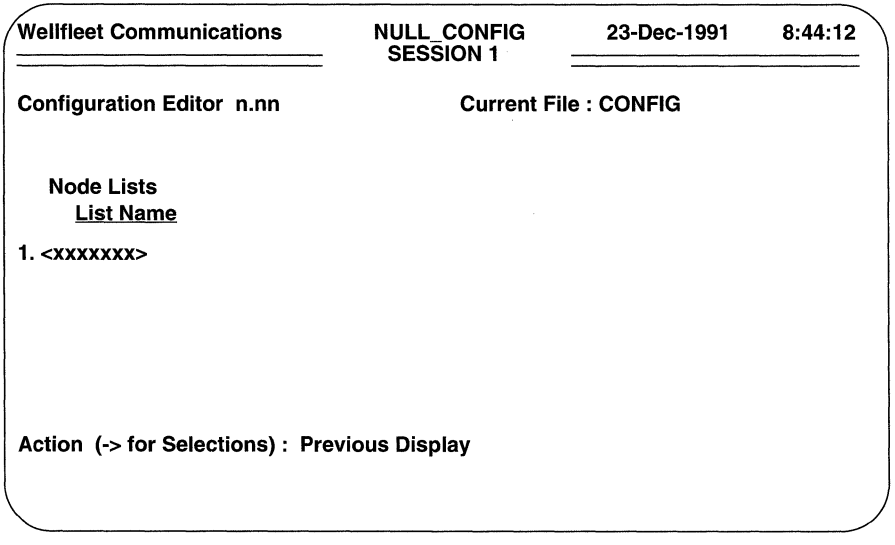


Figure 11-17 DECnet IV Node List Summary Screen

You compile additional DECnet IV node lists from the DECnet IV List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the DECnet IV Node List Summary Screen (Figure 11-17).

To compile another DECnet IV node list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional node list; repeat this procedure until you have compiled all DECnet IV node lists.

11.5.3 Packet Type Lists

Packet type lists specify ranges of DECnet IV packet type numbers.

You compile a packet type list from the DECnet IV List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Packet Type Lists record(s) found
Do you wish to add Packet Type Lists record(s)?

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the packet type list.

  Enter a list name.

After you name the packet type list, the screen prompts for list members.

To assign a range of DECnet IV packet type 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 DECnet IV Packet Type Range Screen (Figure 11-18).

- **Packet Type (low)** specifies the lower boundary of the filtered DECnet IV packet type range.

  Enter the DECnet IV packet type number.

- **Packet Type (high)** specifies the upper boundary of the filtered range.

  Enter the DECnet IV packet type number, and then press `[RETURN]`. If you want the list range to consist of a single value (that entered in response to the **Packet Type (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the DECnet List Member Access Screen.

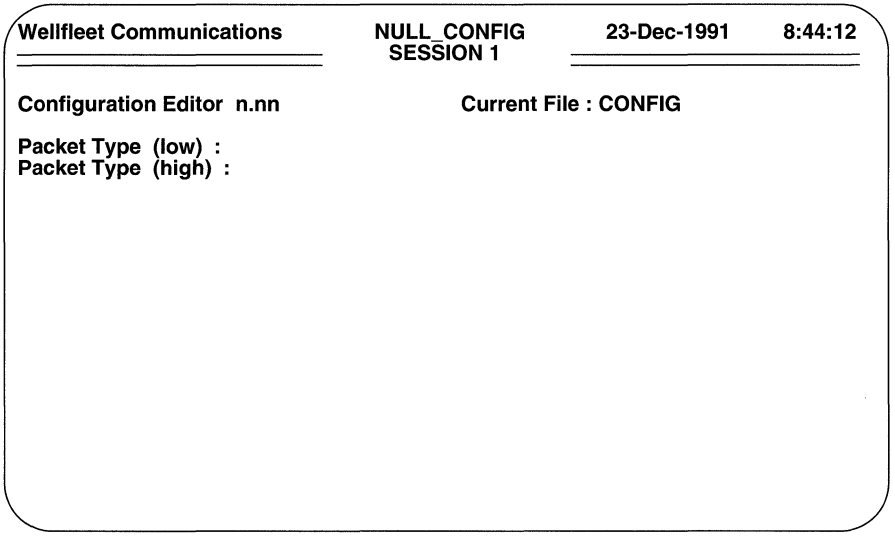


Figure 11-18 DECnet IV Packet Type Range Screen

If you want, you can add other DECnet IV packet type number ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the DECnet Packet Type List Members Screen (Figure 11-19). To add another range of packet type numbers press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the DECnet IV Packet Type Range Screen. Now follow the same procedure as before to add another packet type number range; continue in this fashion until you have added all desired ranges to the list.

You compile additional DECnet IV packet type lists from the DECnet IV List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the DECnet IV Packet Type List Summary Screen (Figure 11-20). To compile another DECnet IV packet type list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional packet type list; repeat this procedure until you have compiled all DECnet IV packet type lists.

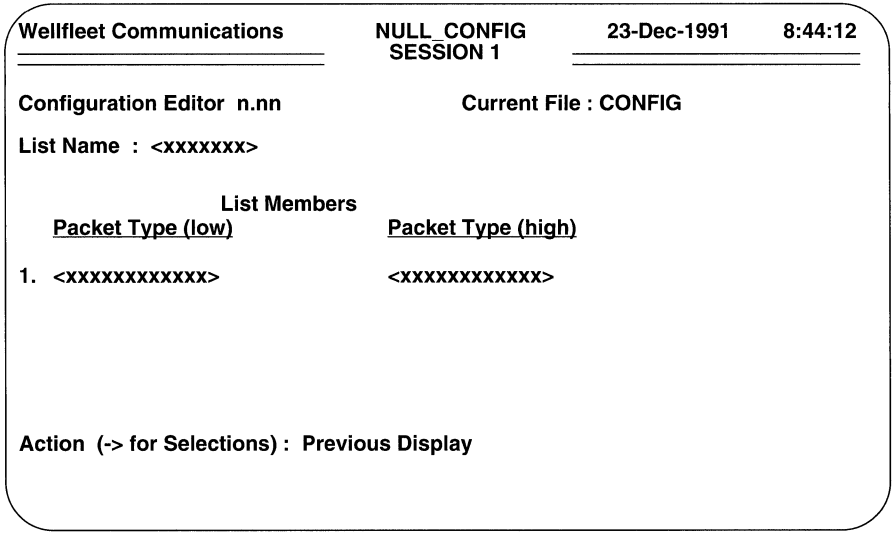


Figure 11-19 DECnet IV Packet Type List Members Screen

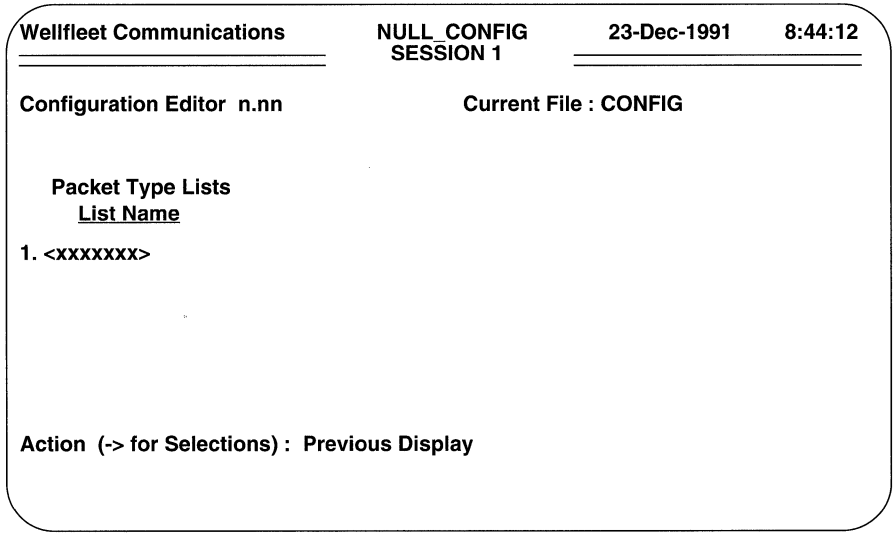


Figure 11-20 DECnet IV Packet Type List Summary Screen

11.6 Configuring DECnet Phase IV Filters

DECnet IV traffic filters apply to all in-coming DECnet traffic across the circuit group. You can, if you wish, construct up to 31 filters for each DECnet circuit group. You configure circuit-group-specific DECnet IV traffic filters from the DECnet IV Filters Configuration Screen. 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 DECnet IV Filters Rule Screen.

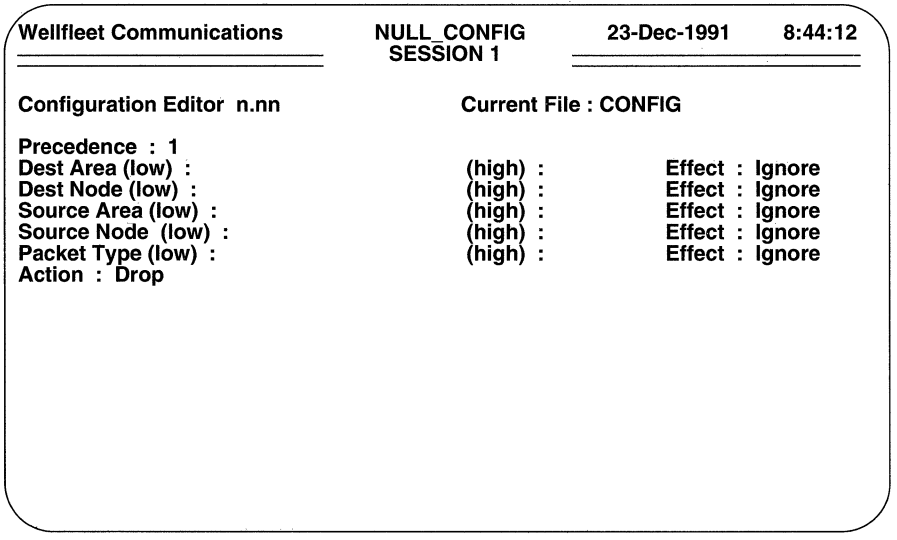


Figure 11-21 DECnet IV Filters Rule Screen

- **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

  You can construct up to 31 filters per DECnet IV circuit group. The **Precedence** value is used when an in-coming DECnet IV packet 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.

NOTE

In the event of two filters with equal precedence, the first configured filter takes precedence.

- **Dest Area (low)** specifies the lower boundary range of filtered DECnet IV destination areas.

  If you do not want to filter DECnet IV destination areas, press `[RETURN]`.

  To filter DECnet IV destination areas, do one of the following:

  - enter the name of an area list
  - enter an area ID at the lower boundary of the DECnet IV destination area range that you want to filter
  - enter a single destination area ID that you want to filter

- **(high)** specifies the upper boundary of the filtered range.

  If you do not want to filter DECnet IV destination areas, press `[RETURN]`.

  To filter DECnet IV destination areas, do one of the following:

  - if you entered the name of an area list at **Dest Area (low)**, or if you want to filter the single area ID entered at **Dest Area (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Dest Area (low)**, enter an area ID at the upper boundary of the area range that you want to filter.

- **Effect** designates one of three operators applied to the destination area pattern specified by **Dest Area (low)** and **(high)**.

  If the filter does not care about destination area values, press `[RETURN]` to accept the default, **Ignore**.

  To filter destination areas, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Area (low)** and **(high)** includes the destination area field of the DECnet IV packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Area (low)** and **(high)** does not include the destination area field of the DECnet IV packet.

- **Dest Node (low)** specifies the lower boundary range of filtered DECnet IV destination nodes.

  If you do not want to filter DECnet IV destination nodes, press **[RETURN]**.

  To filter DECnet IV destination nodes, do one of the following:

  - enter the name of a node list
  - enter a node ID at the lower boundary of the DECnet IV destination node range that you want to filter
  - enter a single destination node ID that you want to filter

- **(high)** specifies the upper boundary of the filtered range.

  If you do not want to filter DECnet IV destination nodes, press **[RETURN]**.

  To filter DECnet IV destination nodes, do one of the following:

  - if you entered the name of a node list at **Dest Node (low)**, or if you want to filter the single destination node entered at **Dest Node (low)**, press **[RETURN]**.
  - if you entered a lower boundary range value at **Dest Node (low)**, enter a node ID at the upper boundary of the node range that you want to filter.

- **Effect** designates one of three operators applied to the destination node pattern specified by **Dest Node (low)** and **(high)**.

  If the filter does not care about destination node values, press **[RETURN]** to accept the default, **Ignore**.

  To filter destination nodes, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Node (low)** and **(high)** includes the destination node field of the DECnet IV packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Node (low)** and **(high)** does not include the destination node field of the DECnet IV header.

- **Source Area (low)** specifies the lower boundary range of filtered DECnet IV source areas.

  If you do not want to filter DECnet IV source areas, press **[RETURN]**.

  To filter DECnet IV source areas, do one of the following:

  - enter the name of an area list
  - enter an area ID at the lower boundary of the DECnet IV source area range that you want to filter
  - enter a single source area ID that you want to filter

- **(high)** specifies the upper boundary of the filtered range.

  If you do not want to filter DECnet IV source areas, press `[RETURN]`.

  To filter DECnet IV source areas, do one of the following:

  - if you entered the name of an area list at **Source Area (low)**, or if you want to filter the single source area entered at **Source Area (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Area (low)**, enter an area ID at the upper boundary of the range that you want to filter.

- **Effect** designates one of three operators applied to the source area pattern specified by **Source Area (low)** and **(high)**.

  If the filter does not care about source area values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source areas, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Area (low)** and **(high)** includes the source area field of the DECnet IV packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Area (low)** and **(high)** does not include the source area field of the DECnet IV header.

- **Source Node (low)** specifies the lower boundary range of filtered DECnet IV source nodes.

  If you do not want to filter DECnet IV source nodes, press `[RETURN]`.

  To filter DECnet IV source nodes, do one of the following:

  - enter the name of a node list
  - enter a node ID at the lower boundary of the DECnet IV node ID range that you want to filter
  - enter a single source node ID that you want to filter

- **(high)** specifies the upper boundary of the filtered range.

  If you do not want to filter DECnet IV source nodes, press `[RETURN]`.

  To filter DECnet IV source nodes, do one of the following:

  - if you entered the name of a node list at **Source Node (low)**, or if you want to filter the single source node entered at **Source Node (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Node (low)**, enter a node ID at the upper boundary of the source node ID range that you want to filter.

- **Effect** designates one of three operators applied to the source node pattern specified by **Source Node (low)** and **(high)**.

  If the filter does not care about source node values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source nodes, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Node (low)** and **(high)** includes the source node field of the DECnet IV packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Node (low)** and **(high)** does not include the source node field of the DECnet IV packet.

- **Packet Type (low)** specifies the lower boundary range of filtered DECnet IV packet types.

  If you do not want to filter DECnet IV packet types, press `[RETURN]`.

  To filter DECnet IV packet types, do one of the following:

  - enter the name of a packet type list
  - enter a packet type number at the lower boundary of the DECnet IV packet type range that you want to filter
  - enter a single packet type number that you want to filter

- **(high)** specifies the upper boundary of the filtered range.

  If you do not want to filter DECnet IV packet types, press `[RETURN]`.

  To filter DECnet IV packet types, do one of the following:

  - if you entered the name of a packet type list at **Packet Type (low)** or if you want to filter the single packet type entered at **Packet Type (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Packet Type (low)**, enter a packet type number at the upper boundary of the range that you want to filter.

- **Effect** designates one of three operators applied to the packet type pattern specified by **Packet Type (low)** and **(high)**.

  If the filter does not care about packet type values, press `[RETURN]` to accept the default, **Ignore**.

  To filter packet types, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** includes the packet type field of the DECnet IV packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** does not include the packet type field of the DECnet packet.

❒ **Action** specifies the disposition of DECnet IV packets 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, press `[RETURN]`.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the DECnet IV Filters Access Screen. You configure additional filters (up to a maximum of 31 per DECnet IV circuit group) from this screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the DECnet IV Filters Summary Screen (Figure 11-22).

At **Action (-> for selections)**, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]` to display the DECnet IV Filters Rule Screen. Now follow the same procedures as before to define an additional DECnet IV filter; repeat these procedures until you have configured all filters.

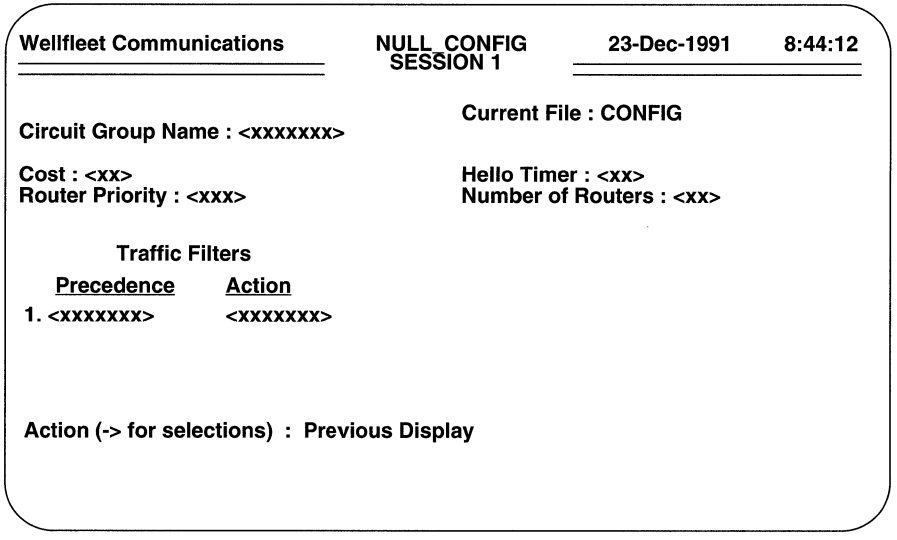


Figure 11-22 DECnet IV Filters Summary Screen

12 Configuring XNS

This chapter tells you how to configure the XNS Router.

The XNS router implementation is compatible with the "Grey Book" standard and fully supports the XNS Level 1 Internet Datagram Protocol, and the XNS Level 2 Echo, Error, and Routing Information Protocols.

As you configure the XNS router, you supply information that it uses to route packets through an XNS internet. The XNS internet packet header consists of 30 bytes of address and delivery data as shown in Figure 12-1.

- Bytes 1 and 2 of the header contain a checksum of the entire packet. FFFF (hexadecimal) indicates that checksumming has been disabled.
- Bytes 3 and 4 contain the internet packet length (from 30 to 576 bytes).
- Byte 5 contains a transport control mechanism. The least significant four bits are unused and always set to 0. The most significant four bits contain a hop count that enumerates the number of routers encountered in a packet's transit from source to destination. Each router that forwards a packet to another intervening router increments the hop count by one. A packet that reaches its 16th router is discarded.
- Byte 6 contains a value that identifies the protocol carried in the packet's data section. Table 12-1 lists common protocol types.

Table 12-1: XNS Packet Types

Type	Protocol
0	Unknown
1	Routing Information Protocol
2	Echo Protocol
3	Error Protocol
4	Sequenced Packet Protocol

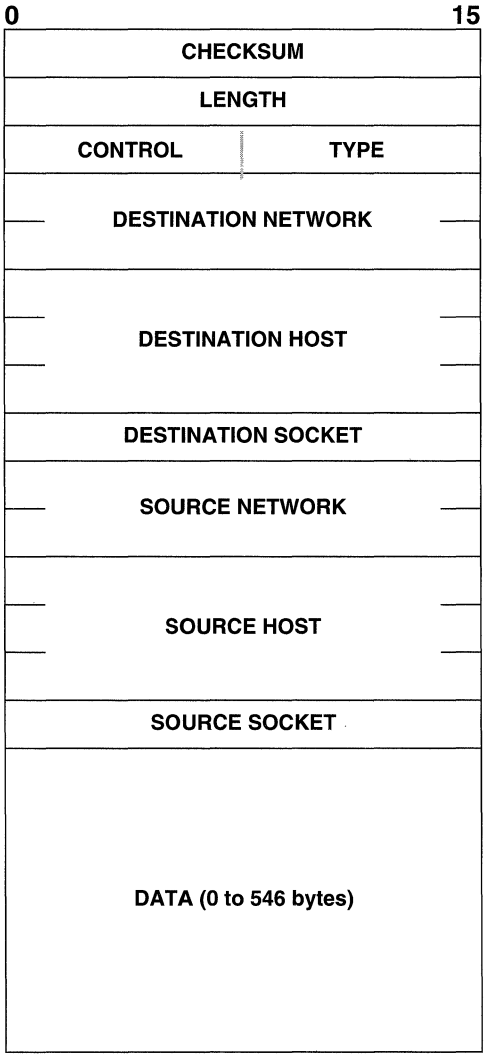


Figure 12-1 XNS Internet Packet Format

- Bytes 7, 8, 9, and 10 contain the destination network number. If the number is less than 32 bits in length, it is written in the least significant portion of the destination network field, and the unused bits are set to 0.
- Bytes 11, 12, 13, 14, 15, and 16 contain the physical address (also called host number) of the destination host. This address can be the universally

administered 48-bit Ethernet address, or it can be a locally assigned address of arbitrary length (but less than 48 bits). If the address is less than 48 bits in length, it is written in the least significant portion of the destination host field and the unused bits are set to 0.

- Bytes 17 and 18 contain the destination socket (a local address identified with a specific software service). XNS reserves well-known sockets for use by certain protocols. Table 12-2 lists well-known socket numbers.

Table 12-2: XNS Well-Known Sockets

Socket Number	Protocol
0	Unknown
1	Routing Information Protocol
2	Echo Protocol
3	Error Protocol

- Bytes 19, 20, 21, and 22 contain the source network number.
- Bytes 23, 24, 25, 26, 27, and 28 contain the physical address of the source host.
- Bytes 29 and 30 contain the source socket.

12.1 Filtering XNS Packets

Filters enable XNS to relay or drop a particular packet based on the contents of specific fields within the internet packet. Filters examine the following packet fields either singly or in combination: destination network, destination host, destination socket, source network, source host, source socket, and packet type.

Filtering decisions are based on user-defined rules. An XNS filter rule consists of an packet 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 packet field and the value; an action (*drop* or *forward*); and a filter precedence.

For example, the XNS filter-rule-A depicted in Figure 12-2 prevents routing updates issued by a suspect router (XNS network address, 000B0011; XNS host address, 0000A1000159) from being promulgated throughout the internet.

XNS Filter-rule-B isolates a device (network number 000B000A; host number, 0000A1001000), probably storing sensitive or confidential access, from all access except from a single host device (network number 000B0009; host number 0000A1000444)

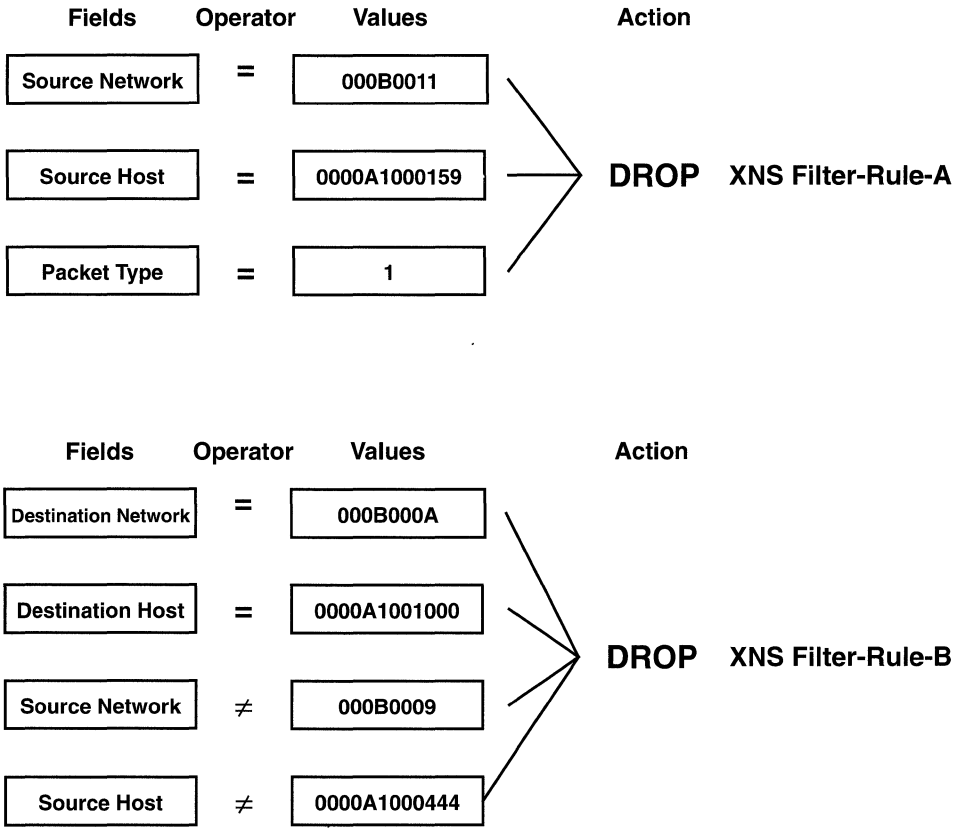


Figure 12-2 XNS Sample Filters

12.2 Setting XNS Basic Parameters

To begin configuring XNS, you assign values to the basic parameters listed in Table 12-3.

You set basic parameters from the Configuration Menu. At **Enter Selection (0 for Previous Menu)** enter the menu item number that appears to the left of **Xerox Routing Service**. The screen displays the following:

Table 12-3: XNS Basic Parameters

Parameter	Function
Host Number	assigns an XNS host address
Auto Enable	specifies the initialization state

No Xerox Routing Service record(s) found
Do you wish to add Xerox Routing Service record(s)?

Press `[RETURN]` to display the XNS Basic Parameters Screen.

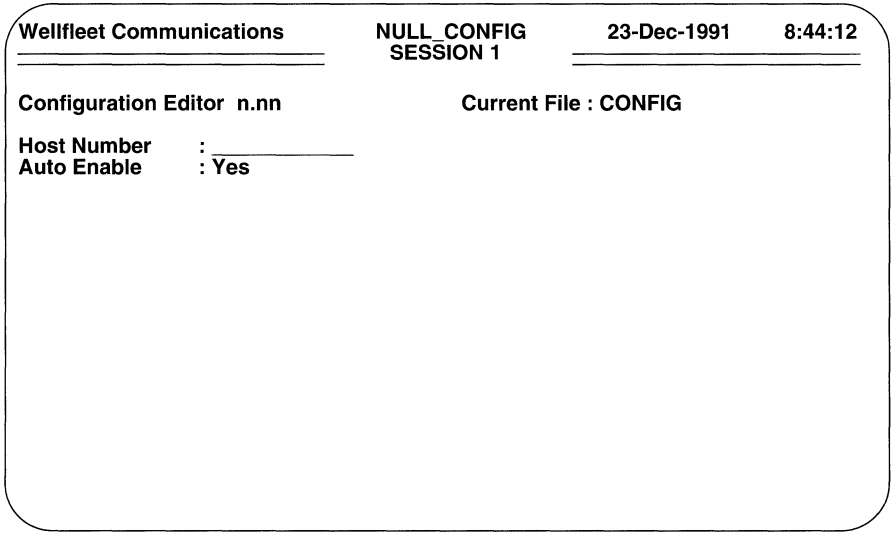


Figure 12-3 XNS Basic Parameters Screen

- **Host Number** assigns an XNS host address to the node.

  Enter the host address in 12-digit hexadecimal format (pad with leading zeros if necessary) and press `[RETURN]`.

  If you wish to use the universally administered 48-bit Ethernet address, simply press `[RETURN]`.

- **Auto Enable** specifies the initial state of the XNS router.

  This XNS-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable XNS.

When global auto enable is **No**, XNS is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will subsequently need to enable XNS manually with NCL commands after the router boots.

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

The screen displays the XNS Detailed Parameters Access Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG

Host Number      : <xxxxxxxx>
Auto Enable      : <xxx>


1. Lists (0)
2. Network Interface Definitions (0)
3. Static Route Definitions (0)




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

Figure 12-4 XNS Detailed Parameters Access Screen

12.3 Defining XNS Network Interfaces

Depending on the complexity of your network topology, the router is connected to at least two -- and in most instances, more than two -- XNS networks. Each connection constitutes a network interface. Each network interface requires specific definition.

You define a network interface from the XNS 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 XNS Network Interface Parameters Screen (Figure 12-5).

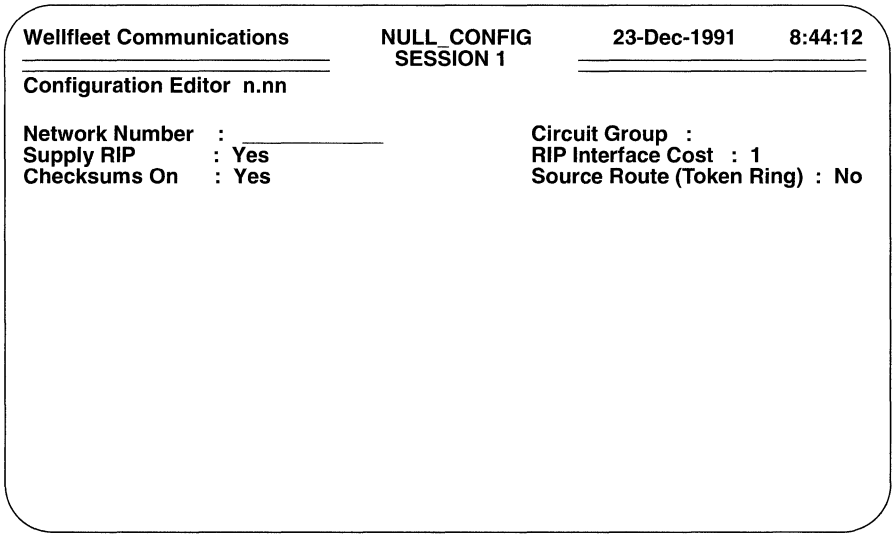


Figure 12-5 XNS Network Interface Parameters Screen

- **Network Number** identifies the connected XNS network.

  Enter the XNS network number as an 8-digit hexadecimal value (pad with leading zeros, if necessary).

- **Circuit Group** identifies the circuit group that connects the router and the network.

  Enter the circuit group name.

- **Supply RIP** enables or disables the RIP supply function.

  Supply RIP specifies whether the router transmits periodic RIP updates across **Circuit Group**. Select **Yes** (to enable RIP supply) or **No** (to disable RIP supply).

- **RIP Interface Cost** sets the cost for each router hop.

  Standard XNS RIP implementations assign a cost of 1 to each hop. You can increase this cost by entering a new value. You should keep in mind, however, that if you increase the cost, you will more rapidly converge upon the value of 16 (at which value XNS declares a destination unreachable).

  Select 1, or enter a new cost (up to a maximum of 15), then press **[RETURN]**.

- **Checksums On** enables or disables checksum processing.

  XNS generally enables checksumming. Select **Yes** (enable checksumming) or **No** (disable checksumming).

- **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 end station. Such a peer relationship enables a transition between source route bridging and XNS routing environments and allows the XNS 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 XNS 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]`.

After you enable or disable end node support, the screen prompts for filter data.

```
Wellfleet Communications        NULL_CONFIG          23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn

Network Number   : <xxxxxxxxx>                Circuit Group  : <xxxxxxx>
Supply RIP       : <xxx>                     RIP Interface Cost  : <xx>
Checksums On     : <xxx>                     Source Route (Token Ring) : <xxx>


1. Traffic Filters (0)




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

Figure 12-6 XNS Filters Configuration Screen

If you want to configure interface-specific XNS filters, proceed to Sections 12.5, *Compiling XNS Filter Lists* and 12.6, *Configuring XNS Filters*. If you are not configuring filters, enter **<0>** at **Enter Selection (0 for Previous Menu)** to return to the XNS Detailed Parameters Access Screen.

You define additional network interfaces from the XNS Detailed Parameters Access Screen. Enter <2> at **Enter Selection (0 for Previous Menu)** to display the XNS Network Interface Summary Screen.

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

Configuration Editor  n.nn                    Current File : CONFIG

Host Number      : <xxxxxxxx>
Auto Enable      : <xxx>


        Network Interface Definitions
    Network Number        Circuit Group
1.  <xxxxxxxx>            <xxxxxxx>


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

Figure 12-7 XNS Network Interface Summary Screen

At **Action (-> for selections)**, press the [RIGHTARROW] to display **Add**, then press [RETURN]. The screen displays the XNS Network Interface Parameters Screen.

Follow the same procedures as before to define an additional XNS network interface; repeat these procedures until you have defined all network interfaces.

12.4 Configuring XNS Static Routes

Static routes are user-specified transmission paths. You configure static routes when you want to restrict the paths that packets can follow to paths you specifically define.

Static routes, like routes learned through RIP, are listed in the XNS routing table. Unlike routes learned through RIP, however, static routes cannot be overwritten.

You configure a static route from the XNS Detailed Parameters Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)**. The screen prompts:

No Static Routes Definitions record(s) found
Do you wish to add Static Route Definitions record(s)?

Press [RETURN] to display the XNS Static Route Parameters Screen (Figure 12-8).

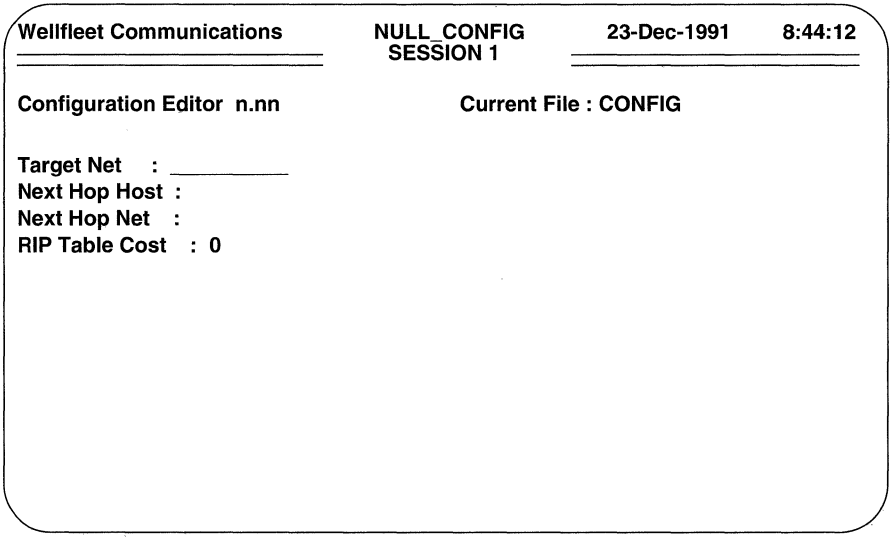


Figure 12-8 XNS Static Route Parameters Screen

- **Target Net** identifies a destination network.

  Enter the network number of the destination network.

- **Next Hop Host** identifies the host address of the next-hop router used to reach **Target Net**.

  Enter the host address of the next-hop router.

- **Next Hop Net** identifies the network address of the next-hop router.

  Enter the network address of the next-hop router.

- **RIP Table Cost** sets the cost for the relay to **Target Net**.

  To use the standard XNS RIP cost value of 1 for each hop, enter the number of hops to **Target Net** and press `[RETURN]`. If you are using non-standard cost values, total the individual RIP costs of each hop to **Target Net** (up to a maximum of 15), and press `[RETURN]`.

  You should keep in mind, however, that if you increase the cost, you will more rapidly converge upon the value of 16 (at which value XNS declares the destination unreachable).

After you specify the **RIP Table Cost**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to display the XNS Detailed Parameters Access Screen. You define additional static routes from this screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the XNS Static Routes Summary Screen.

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

Configuration Editor  n.nn                    Current File : CONFIG

Host Number      : <xxxxxxxx>
Auto Enable      : <xxx>


                    Static Route Definitions
    Target Net          Next Hop Host          Next Hop Net
1.  <xxxxxxxx>          <xxxxxxx>              <xxxxxxx>


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

Figure 12-9 XNS Static Routes Summary Screen

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the XNS Static Route Parameters Screen. Follow the same procedures as before to define an additional static route; repeat these procedures until you have configured all static routes.

12.5 Compiling XNS 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 XNS Detailed Parameters Access Screen. To begin, 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 XNS List Access Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


1. Network Lists (0)
2. Host  Lists (0)
3. Socket Lists (0)
4. Packet Type Lists (0)


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

Figure 12-10 XNS List Access Screen

12.5.1 Network Lists

Network lists specify ranges of XNS network numbers.

You compile a network list from the XNS List Access Screen. Enter **<1>** at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

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

Press **[RETURN]**. The screen prompts for a **List Name**.

- **List Name** identifies the network list.

  Enter a list name, and then press **[RETURN]**.

After you name the network list, the screen prompts for list members (Figure 12-11).

To assign a range of XNS networks to the list, enter **<1>** at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press **[RETURN]**. The screen displays the XNS Network Range Screen (Figure 12-12).

```
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 12-11 XNS List Member Access Screen

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

Configuration Editor  n.nn                  Current File : CONFIG

Network Number (low)  :
Network Number (high)  :
```

Figure 12-12 XNS Network Range Screen

- **Network Number (low)** specifies the lower boundary of the network range.

  Enter an XNS network number.

- **Network Number (high)** specifies the upper boundary of the network range.

  Enter an XNS network number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Network Number (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the XNS List Member Access Screen.

If you want, you can add other network ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the XNS Network 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
   Network Number (low)                 Network Number (high)

1. <xxxxxxxxxxxx>                       <xxxxxxxxxxxx>




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

Figure 12-13 XNS Network List Members Screen

To add another range of network numbers, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen displays the XNS Network Range Screen. Now follow the same procedure as before to add another network number range; continue in this fashion until you have added all desired ranges to the list.

You compile additional network lists from the XNS List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the XNS Network List Summary Screen (Figure 12-14).

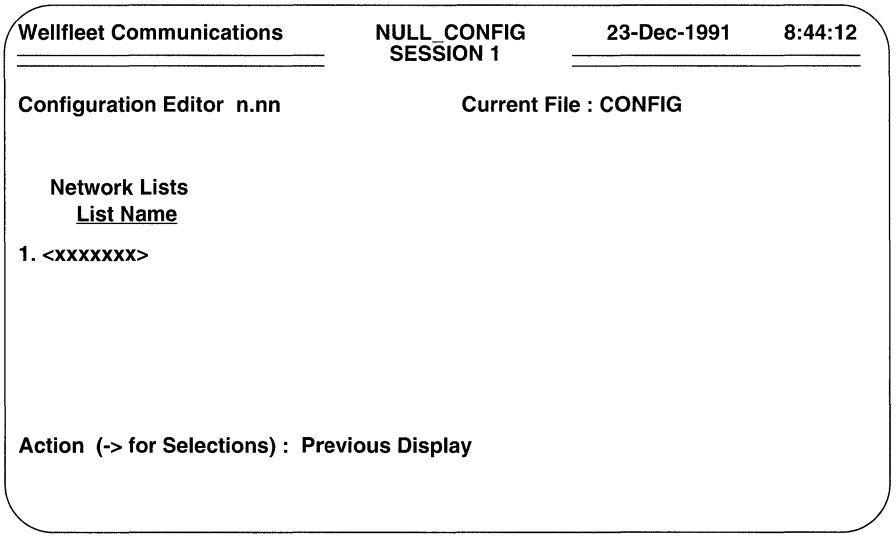


Figure 12-14 XNS Network List Summary Screen

To compile another network 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 XNS network lists.

12.5.2 Host Lists

Host lists specify ranges of XNS host numbers.

You compile a host list from the XNS List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the host list.

  Enter a list name, and then press `[RETURN]`.

After you name the host list, the screen prompts for list members.

To assign a range of XNS hosts to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the XNS Host Range Screen.

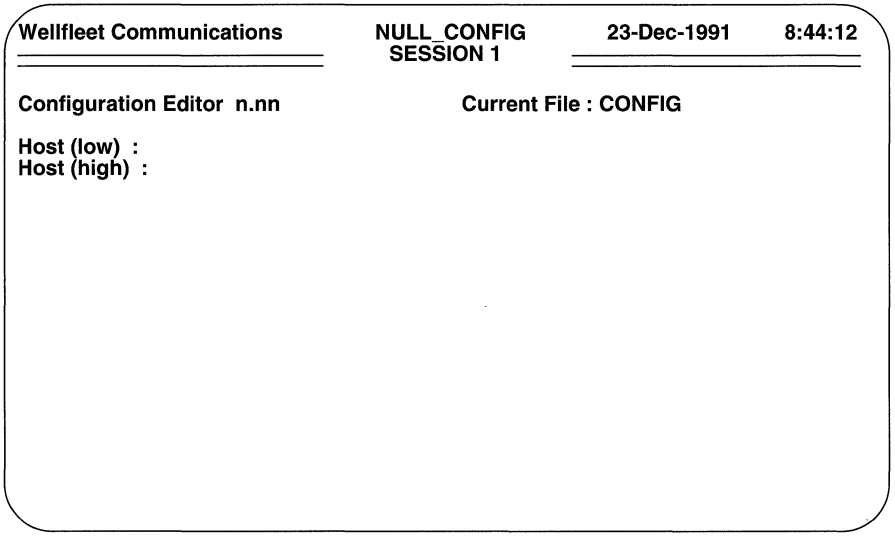


Figure 12-15 XNS Host Range Screen

- **Host (low)** specifies the lower boundary of the host range.

  Enter an XNS host number.

- **Host (high)** specifies the upper boundary of the host range.

  Enter an XNS host number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Host (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the XNS List Member Access Screen.

If you want, you can add other XNS host ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the XNS Host List Members Screen (Figure 12-16). To add another range of hosts, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.

The screen displays the XNS Host Range Screen. Now follow the same procedure as before to add another host 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

List Name  : <xxxxxxx>

                        List Members
   Host Number (low)                  Host Number (high)

1.  <xxxxxxxxxxxx>                    <xxxxxxxxxxxx>




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

Figure 12-16 XNS Host List Members Screen

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

Configuration Editor  n.nn                  Current File : CONFIG


   Host Lists
      List Name

1. <xxxxxxx>




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

Figure 12-17 XNS Host List Summary Screen

You compile additional host lists from the XNS List Access Screen. Enter **<2>** at **Enter Selection (0 for Previous Menu)** to display the XNS Host List Summary Screen (Figure 12-17).

To compile another host list, press the **[RIGHTARROW]** to display **Add**, then press **[RETURN]**. Now follow the previously described procedure to compile an additional host list; repeat this procedure until you have compiled all XNS host lists.

12.5.3 Socket Lists

Socket lists specify ranges of XNS socket numbers.

You compile a socket list from the XNS List Access Screen. Enter **<3>** at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press **[RETURN]**. The screen prompts for a **List Name**.

- **List Name** identifies the socket list.

  Enter a list name, and then press **[RETURN]**.

After you name the socket list, the screen prompts for list members.

To assign a range of XNS sockets to the list, enter **<1>** at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press **[RETURN]** to display the XNS Socket Range Screen (Figure 12-18).

- **Socket (low)** specifies the lower boundary of the socket range.

  Enter an XNS socket number.

- **Socket (high)** specifies the upper boundary of the socket range.

  Enter an XNS socket number, and then press **[RETURN]**. If you want the list range to consist of a single value, that entered in response to the **Socket (low)** parameter, press **[RETURN]**.

After you specify the upper boundary, the console screen prompts **Hit Return to Continue**. Press **[RETURN]** to revert to the XNS List Member Access Screen.

If you want, you can add other socket ranges to the list. To add an additional range, enter **<1>** at the **Enter Selection (0 for Previous Menu)** prompt to display the XNS Socket List Members Screen (Figure 12-19).

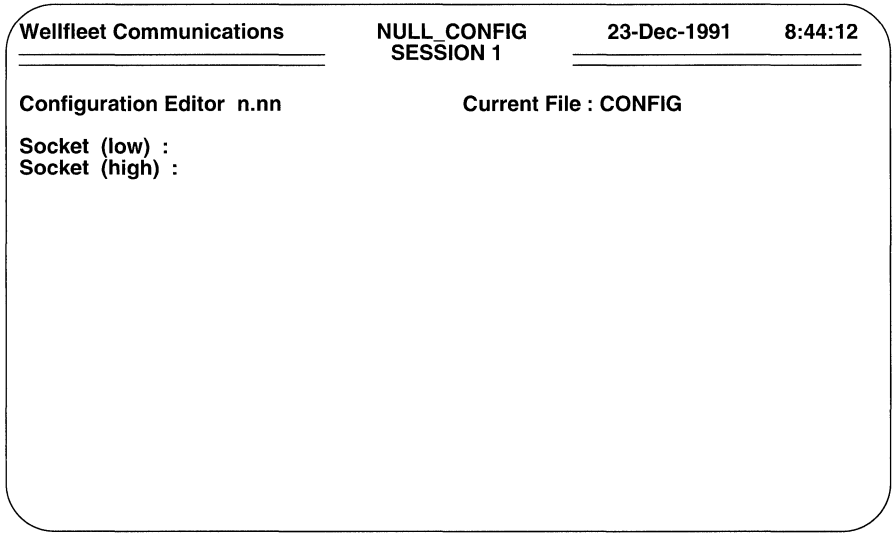


Figure 12-18 XNS Socket Range Screen

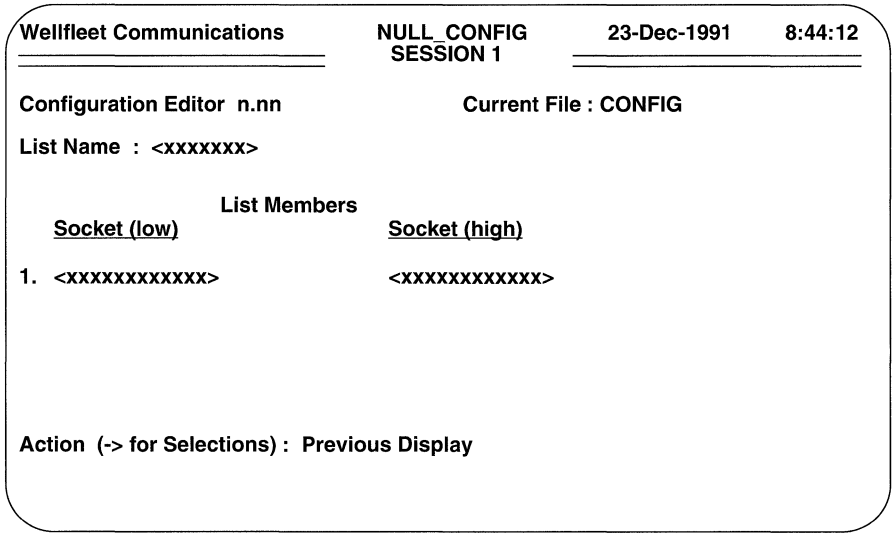


Figure 12-19 XNS Socket List Members Screen

To add another range of socket numbers, press the [RIGHTARROW] to display **Add** and then press [RETURN].The screen displays the XNS Socket Range Screen. Now follow the same procedure as before to add another socket range; continue in this fashion until you have added all desired ranges to the list.

You compile additional socket lists from the XNS List Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)** to display the XNS Socket List Summary Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


   Socket Lists
      List Name
1. <xxxxxxx>




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

Figure 12-20 XNS Socket List Summary Screen

To compile another XNS socket list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the previously described procedure to compile an additional socket list; repeat this procedure until you have compiled all XNS socket lists.

12.5.4 Packet Type Lists

Packet type lists specify ranges of XNS packet type numbers.

You compile a packet type list from the XNS List Access Screen. Enter <4> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Packet Type Lists record(s) found
Do you wish to add Packet Type Lists record(s)?

Press [RETURN]. The screen prompts for a **List Name**.

- **List Name** identifies the packet type list.

  Enter a list name, and then press `[RETURN]`.

After you name the packet type list, the screen prompts for list members.

To assign a range of packet types to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the XNS Packet Type Range Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG

Packet Type  (low) :
Packet Type  (high) :
```

Figure 12-21 XNS Packet Type Range Screen

- **Packet Type (low)** specifies the lower boundary of the packet type range.

  Enter an XNS packet type number.

- **Packet Type (high)** specifies the upper boundary of the packet type range.

  Enter an XNS packet type number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Packet Type (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the XNS List Member Access Screen.

If you want, you can add other packet type ranges to the list. To add an additional range, enter **<1>** at the **Enter Selection (0 for Previous Menu)** prompt to display the XNS Packet 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
   Packet Type (low)                Packet Type (high)

1. <xxxxxxxxxxxx>                   <xxxxxxxxxxxx>




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

Figure 12-22 XNS Packet Type List Members Screen

To add another range of packet types, press the [**RIGHTARROW**] to display **Add** and then press [**RETURN**].The screen displays the XNS Packet Type Range Screen. Now follow the same procedure as before to add another packet type range; continue in this fashion until you have added all desired ranges to the list.

You compile additional packet type lists from the XNS List Access Screen. Enter **<4>** at **Enter Selection (0 for Previous Menu)** to display the XNS Packet Type List Summary Screen (Figure 12-23).

To compile another XNS packet type list, press the [**RIGHTARROW**] to display **Add**, then press [**RETURN**]. Now follow the previously described procedure to compile an additional packet type list; repeat this procedure until you have compiled all XNS packet type lists.

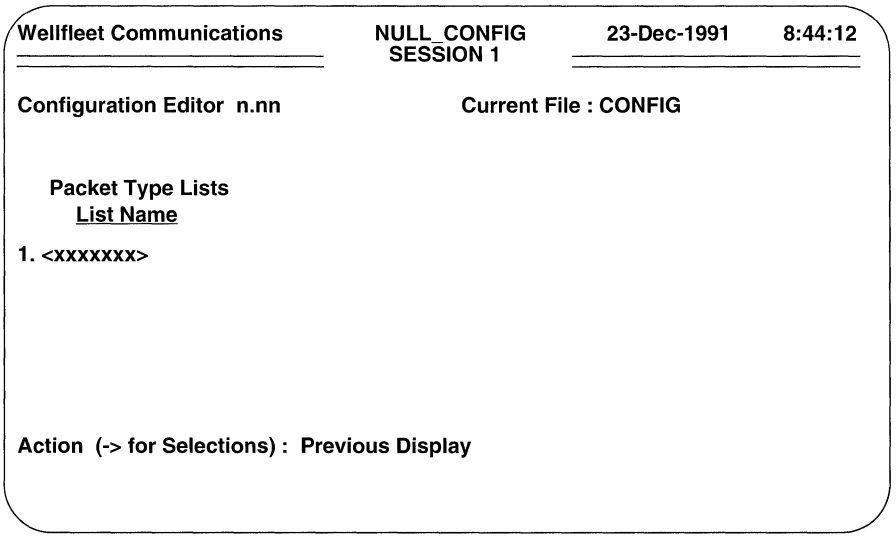


Figure 12-23 XNS Packet Type List Summary Screen

12.6 Configuring XNS Filters

XNS filters apply to all in-coming XNS traffic across the interface. You can, if you wish, construct up to 31 filters for each XNS interface. You configure interface-specific XNS traffic filters from the XNS Filters Configuration Screen (Figure 12-6). Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The console 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 XNS Filters Rule Screen (Figure 12-24).

- **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

  You can construct up to 31 filters per interface. The **Precedence** value is used when an in-coming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

  Press the `[RIGHTARROW]` to select a value from 1 to 31 and then press `[RETURN]`.

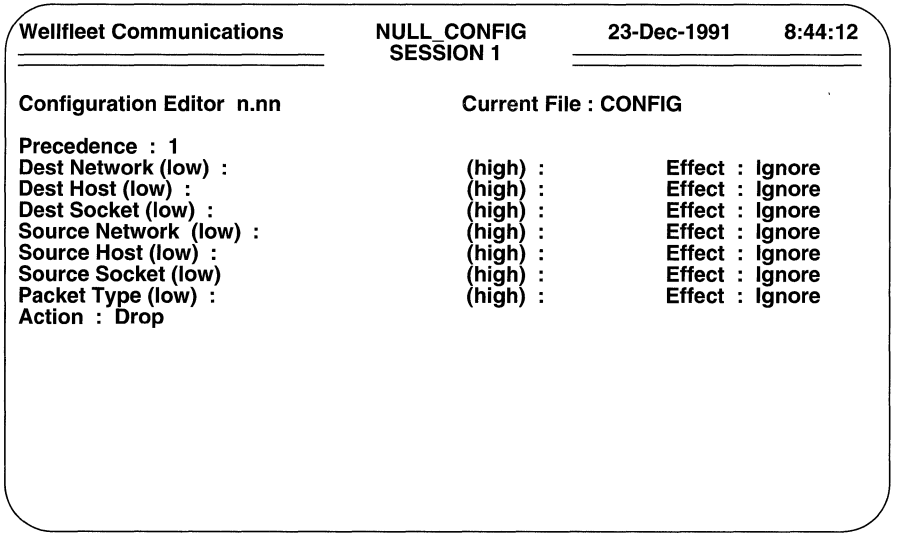


Figure 12-24 XNS Filters Rule Screen

NOTE

In the event of two filters with equal precedence, the first configured filter takes precedence.

- **Dest Network (low)** specifies the lower boundary range of filtered destination networks.

  If you do not want to filter destination networks, press `[RETURN]`.

  To filter destination networks, do one of the following:

  - enter the name of a network list
  - enter a network number at the lower boundary of the destination network range
  - enter a single destination network number

- **(high)** specifies the upper boundary range of filtered destination networks.

  If you do not want to filter destination networks, press `[RETURN]`.

  To filter destination networks, do one of the following:

- if you entered the name of a network list at **Dest Network (low)**, or if you want to filter the single network specified at **Dest Network (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Dest Network (low)**, enter a network number 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 pattern specified by **Dest Network (low)** and **(high)**.

If the filter does not care about destination network values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination networks, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Network (low)** and **(high)** includes the destination network field of the XNS internet packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Network (low)** and **(high)** does not include the destination network field of the XNS internet packet.

❒ **Dest Host (low)** specifies the lower boundary range of filtered destination hosts.

If you do not want to filter destination hosts, press `[RETURN]`.

To filter XNS destination hosts, do one of the following:

- enter the name of a host list
- enter a host number at the lower boundary of the destination host range
- enter a single destination host number

❒ **(high)** specifies the upper boundary range of filtered destination hosts.

If you do not want to filter XNS destination hosts, press `[RETURN]`.

To filter destination hosts, do one of the following:

- if you entered the name of a host list at **Dest Host (low)**, or if you want to filter the single host specified at **Dest Host (low)** press `[RETURN]`.
- if you entered a lower boundary range value at **Dest Host (low)**, enter a host number 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 pattern specified by **Dest Host (low)** and **(high)**.

  If the filter does not care about destination host values, press `[RETURN]` to accept the default, **Ignore**.

  To filter destination hosts, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Host (low)** and **(high)** includes the destination host field of the XNS internet packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Host (low)** and **(high)** does not include the destination host field of the XNS internet packet.

  Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

- **Dest Socket (low)** specifies the lower boundary range of filtered destination sockets.

  If you do not want to filter destination sockets, press `[RETURN]`.

  To filter destination sockets, do one of the following:

  - enter the name of a socket list
  - enter a socket number at the lower boundary of the destination socket range
  - enter a single destination socket number

- **(high)** specifies the upper boundary range of filtered destination sockets.

  If you do not want to filter destination sockets, press `[RETURN]`.

  To filter destination sockets, do one of the following:

  - if you entered the name of a socket list at **Dest Socket (low)**, or if you want to filter the single socket specified at **Dest Socket (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Dest Socket (low)**, enter a socket number 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 pattern specified by **Dest Socket (low)** and **(high)**.

  If the filter does not care about destination socket values, press `[RETURN]` to accept the default, **Ignore**.

  To filter destination sockets, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Socket (low)** and **(high)** includes the destination socket field of the XNS internet packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Socket (low)** and **(high)** does not include the destination socket field of the XNS internet packet.

❒ **Source Network (low)** specifies the lower boundary range of filtered source networks.

If you do not want to filter source networks, press `[RETURN]`.

To filter source networks, do one of the following:

- enter the name of a network list
- enter a network number at the lower boundary of the source network range
- enter a single source network number

❒ **(high)** specifies the upper boundary range of filtered source networks.

If you do not want to filter source networks, press `[RETURN]`.

To filter source networks, do one of the following:

- if you entered the name of a network list at **Source Network (low)**, or if you want to filter the single source network specified at **Source Network (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Source Network (low)**, enter a network number 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 pattern specified by **Source Network (low)** and **(high)**.

If the filter does not care about source network values, press `[RETURN]` to accept the default, **Ignore**.

To filter source networks, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Network (low)** and **(high)** includes the source network field of the XNS internet packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Network (low)** and **(high)** does not include the source network field of the XNS internet packet.

- **Source Host (low)** specifies the lower boundary range of filtered source hosts.

  If you do not want to filter source hosts, simply press `[RETURN]`.

  To filter source hosts, do one of the following:

  - enter the name of a host list
  - enter a host number at the lower boundary of the source host range
  - enter a single source host number

- **(high)** specifies the upper boundary range of filtered source hosts.

  If you do not want to filter source hosts, simply press `[RETURN]`.

  To filter source hosts, do one of the following:

  - if you entered the name of a host list at **Source Host (low)**, or if you want to filter the single host specified at **Source Host (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Host (low)**, enter a host number 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 pattern specified by **Source Host (low)** and **(high)**.

  If the filter does not care about source host values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source hosts, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Host (low)** and **(high)** includes the source host field of the XNS internet packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Host (low)** and **(high)** does not include the source host field of the XNS internet packet.

- **Source Socket (low)** specifies the lower boundary range of filtered source sockets.

  If you do not want to filter source sockets, press `[RETURN]`.

  To filter source sockets, do one of the following:

  - enter the name of a socket list
  - enter a socket number at the lower boundary of the source socket range
  - enter a single source socket number

- **(high)** specifies the upper boundary range of filtered source sockets.

  If you do not want to filter source sockets, press `[RETURN]`.

  To filter source sockets, do one of the following:

  - if you entered the name of a socket list at **Source Socket (low)**, or if you want to filter the single source socket specified at **Source Socket (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Socket (low)**, enter a socket number 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 host address pattern specified by **Source Socket (low)** and **(high)**.

  If the filter does not care about source socket values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source sockets, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Socket (low)** and **(high)** includes the source socket field of the XNS internet packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Socket (low)** and **(high)** does not include the source socket field of the XNS internet packet.

- **Packet Type (low)** specifies the lower boundary range of filtered packet types.

  If you do not want to filter packet types, press `[RETURN]`.

  To filter packet types, do one of the following:

  - enter the name of a packet type list
  - enter a packet type number at the lower boundary of the packet type range
  - enter a single packet type number

  After you enter a packet type or a list name, press `[RETURN]`.

- **(high)** specifies the upper boundary range of filtered packet types.

  If you do not want to filter packet types, simply press `[RETURN]`.

  To filter packet types, do one of the following:

  - if you entered the name of a packet type list at **Packet Type (low)**, or if you want to filter the single socket specified at **Packet Type (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **Packet Type (low)**, enter a packet type number 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 packet type pattern specified by **Packet Type (low)** and **(high)**.

If the filter does not care about packet type values, press `[RETURN]` to accept the default, **Ignore**.

To filter packet types, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** includes the packet type field of the XNS internet packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** does not include the packet type field of the XNS internet packet.

❒ **Action** specifies the disposition of packets 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.

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

You configure additional filters (up to a maximum of 31 per network interface) from the XNS Filters Configuration Screen. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The console screen displays the XNS Filters Summary Screen (Figure 12-25).

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the XNS Filters Rule Screen.

Follow the same procedures as before to define an additional XNS filter; repeat these procedures until you have defined all filters.

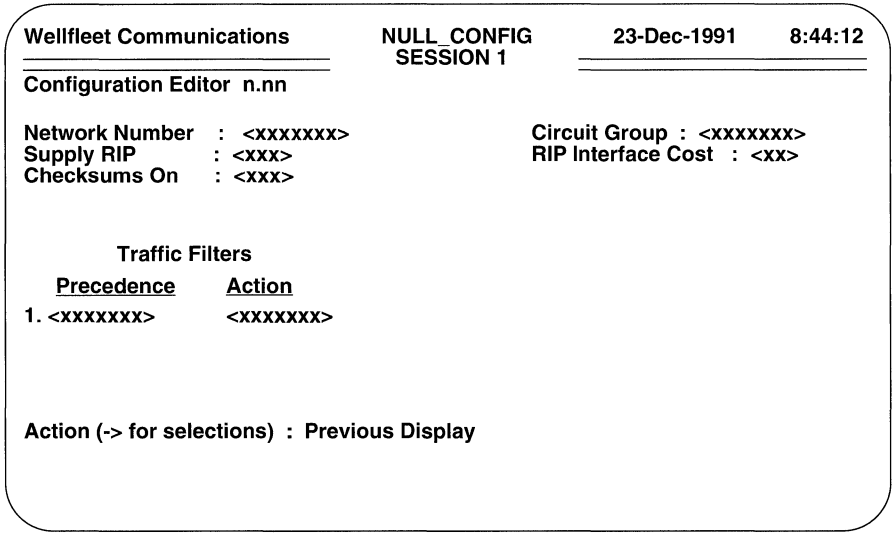


Figure 12-25 XNS Filters Summary Screen

13 Configuring IPX

This chapter tells you how to configure the IPX Router.

The Internet Packet Exchange Protocol (IPX) is the Novell, Inc. implementation of XNS. IPX is generally found in PC and/or workstation environments and supports a wide variety of LAN topologies and media.

IPX uses the XNS internet packet format. Like XNS, IPX makes a "best effort" to deliver internet packets, but does not guarantee delivery. IPX requires that specific applications build upon the basic IPX packet protocol to implement reliable-delivery and other higher-level protocols.

The IPX router supports the Service Advertising Protocol (SAP). SAP enables network-resident value-added servers to inform clients of their presence. By using the identification broadcasting services provided by SAP, a server makes itself known to clients by name, type, and IPX network address.

After initialization, servers broadcast *service advertising packets* at 60 second intervals. Such packets identify the server by name (a network-unique character string up to 48 bytes in length), server type (a 16-bit service type identifier administered by Novell), and network address (consisting of network, host, and socket identifiers). Service advertising packets are received by all routers within the IPX network.

IPX routers maintain a database (called a *bindery*) containing server-specific information: name, type, address, hop count, the interface to the server, and a timer value to age bindery entries. Each time a router receives a service advertising packet, it compares the packet's contents with its bindery. If the bindery contains information on this server, the router simply refreshes the age timer. If, however, the packet contents advertise a previously-unknown service, the router adds a new entry to its bindery and triggers an advertisement of the new service to all connected networks. IPX routers also issue regularly scheduled advertisements of their bindery; these advertisements, issued at 60-second intervals, propagate server tables throughout the IPX network.

Clients can use the IPX broadcast facility to obtain information on network servers. Client information requests can take one or two forms: *general service queries* seek information from all network servers; *nearest service queries* seek information on the closest service of a specified type.

For specific technical information on IPX, refer to the following document:

*Advanced Netware, V2.0 Internet Packet Exchange Protocol (IPX) with Asynchronous Event Scheduler (*Novell, Inc., Specifications as of March 19, 1986*)*

As you configure the IPX router, you supply information that it uses to route packets through an IPX Internet. IPX internet packet header consists of 30 bytes as shown in Figure 13-1.

- Bytes 1 and 2 of the header contain a checksum of the 30-byte IPX header. A value of FFFF (hexadecimal) indicates that checksumming has been disabled.
- Bytes 3 and 4 contain the internet packet length which varies from 30 to 576 bytes.
- Byte 5 contains a transport control mechanism used only by IPX routers. The least significant four bits (bits 0 to 3) are always set to 0. The most significant four bits contain a hop count that enumerates the number of routers encountered in a packet's transit from source to destination. Each router that forwards an internet packet to another intervening router increments the hop count by one. A packet that reaches its 16th router is discarded.
- Byte 6 contains a coded value that identifies the protocol carried in the packet's data section. Table 13-1 lists common IPX protocol types.

Table 13-1: IPX Packet Types

Type	Protocol
0	Unknown
4	Sequenced Packet Protocol

- Bytes 7, 8, 9, and 10 contain the destination network number. All networks are assigned a network number by a local administrator. If the network number is less than 32 bits in length, the network number is written in the least-significant portion of the destination network field, and the unused most-significant bits are set to 0.
- Bytes 11, 12, 13, 14, 15, and 16 contain the physical address (also called host number) of the destination host. All hosts are assigned a unique physical address. This address can be the universally-administered 48-bit Ethernet address, or it can be a locally-assigned address of arbitrary length (but less than 48 bits). If the host address is less than 48 bits in length, it is written in the least-significant portion of the destination host field and the unused most significant bits are set to 0.

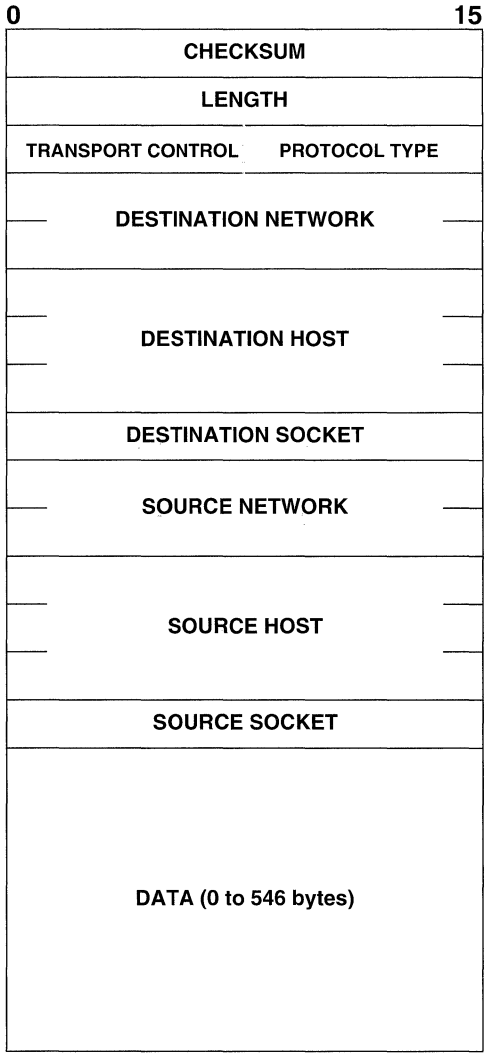


Figure 13-1 IPX Internet Packet Format

Bytes 17 and 18 contain the destination socket (a local address identified with a specific software service). IPX reserves well-known sockets for use by certain protocols. Table 13-2 lists these well-known socket numbers.

Table 13-2: IPX Well Known Sockets

Socket Number	Protocol
0	Unknown
0x451	File Server
0x452	SAP
0x453	RIP
0x455	NetBIOS

- Bytes 19, 20, 21, and 22 contain the source network number.
- Bytes 23, 24, 25, 26, 27, and 28 contain the physical address of the source host.
- Bytes 29 and 30 contain the source socket.

13.1 Filtering IPX Packets

Filters enable the router to relay or drop a particular frame based on the contents of specific fields within the IPX internet packet (shown in Figure 13-1). Filters examine the following packet fields either singly or in combination: destination network, destination host, destination socket, source network, source host, source socket, and packet type.

Filtering decisions are based on user-defined rules. An IPX filter rule consists of an IPX packet 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 packet field and the value; an action (*drop* or *forward*); and a filter precedence.

For example, the IPX filter-rule-A shown graphically in Figure 13-2 prevents routing updates emanating from a suspect router (IPX network address, 000B0011; IPX host address, 0000A1000159) from being promulgated throughout the network.

IPX Filter-rule-B isolates an IPX host device (network number 000B000A; host number, 0000A1001000), probably storing sensitive or confidential access, from all access except from a single host device (network number 000B0009; host number 0000A1000444)

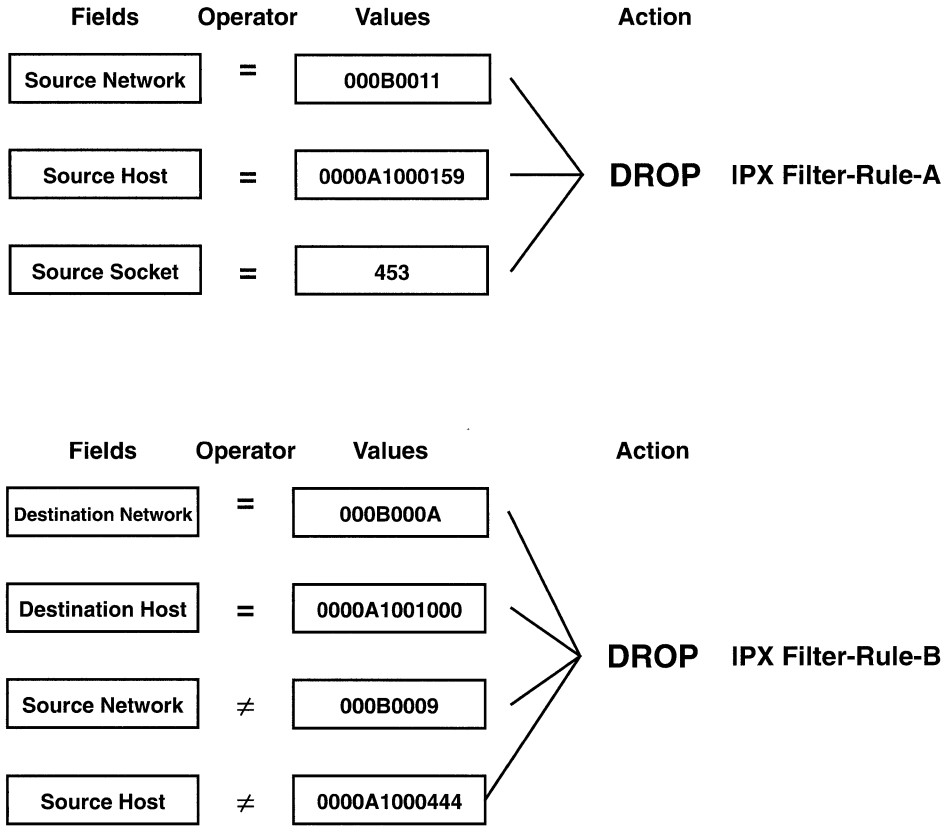


Figure 13-2 IPX Sample Filters

13.2 Enabling IPX

You configure the IPX router from the Configuration Menu. To begin, at **Enter Selection (0 for Previous Menu)** enter the number that appears to the left of **IPX Routing Service**. The screen displays the following prompt:

No IPX Routing Service record(s) found
Do you wish to add IPX Routing Service record(s)?

Press `[RETURN]`. The screen prompts **Auto Enable**.

- **Auto Enable** specifies the initial state of the IPX router.

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

  When global auto enable is **No**, IPX is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable IPX with NCL commands after the router boots.

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

The screen displays the IPX Parameters Access Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG

Auto Enable        : <xxx>




1. Lists (0)
2. Network Interface Definitions (0)
3. Static Route Definitions (0)



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

Figure 13-3 IPX Parameters Access Screen

13.3 Defining IPX Network Interfaces

Depending on the complexity of your network topology, the IPX router is connected to at least two -- and in many instances, more than two -- IPX networks. Each connection constitutes a network interface and requires specific definition.

You define a network interface from the IPX 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 IPX Network Interface Parameters Screen.

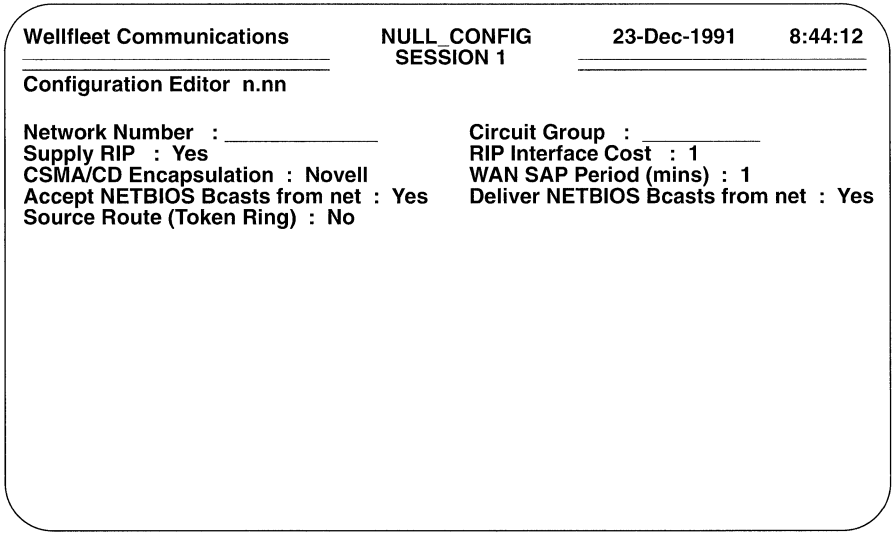


Figure 13-4 IPX Network Interface Parameters Screen

- **Network Number** identifies the IPX network that the interface connects to.

  All IPX networks are identified by locally-assigned network number. Enter this network number as an 8-digit hexadecimal value (pad with leading zeros, if necessary).

- **Circuit Group** identifies the circuit group that provides a connection between the router and the IPX network.

  Enter the circuit group name.

- **Supply RIP** enables or disables the RIP supply function.

  Supply RIP specifies whether the IPX router transmits periodic RIP updates across **Circuit Group**. If you want to enable the transmission of RIP updates, press `[RETURN]`. If you want to disable RIP transmissions, press the `[RIGHTARROW]` to display **No**, then press `[RETURN]`.

- **RIP Interface Cost** sets the cost for each router hop.

  Standard IPX 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 cost, you will more

rapidly converge upon the value of 16 (at which value IPX declares a destination unreachable)

Press the **[RIGHTARROW]** to select 1 (the default), or enter a new cost (up to a maximum of 15), then press **[RETURN]**.

- **CSMA/CD Encapsulation** selects from three available encapsulation methods that can be used on IEEE 802.3 media; this parameter has no effect on other media types.

  NOVELL (Figure 13-5), selects Novell proprietary encapsulation which prefixes an eight-octet preamble, a six-octet destination-address, a six- octet source-address, and a two-octet length field to the unchecksummed IPX packet. It appends a four-octet frame check sequence to the packet.

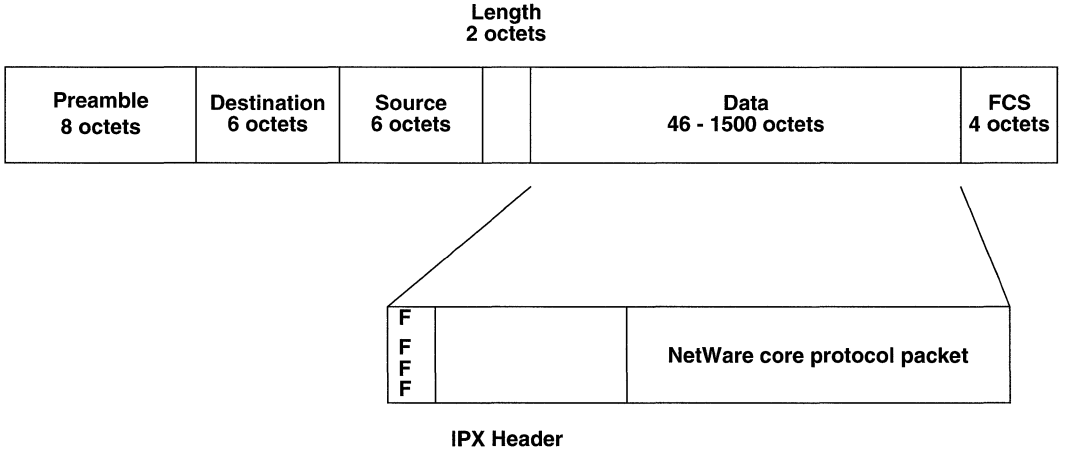


Figure 13-5 Novell Proprietary Encapsulation

Ethernet selects Ethernet 2.0 encapsulation (Figure 13-6) which prefixes an eight-octet preamble, a six-octet destination-address, a six-octet source-address, and a two-octet protocol type (hexadecimal 8137) to the IPX packet. It appends a four-octet frame check sequence to the packet.

802.2 selects IEEE 802.2 logical link control encapsulation (Figure 13-7) which prefixes a one-octet destination service access point (DSAP), a one-octet source service access point (SSAP), and a one-octet control field to the IPX packet. The 802.2 packet, in turn, will be encapsulated within a media-specific packet.

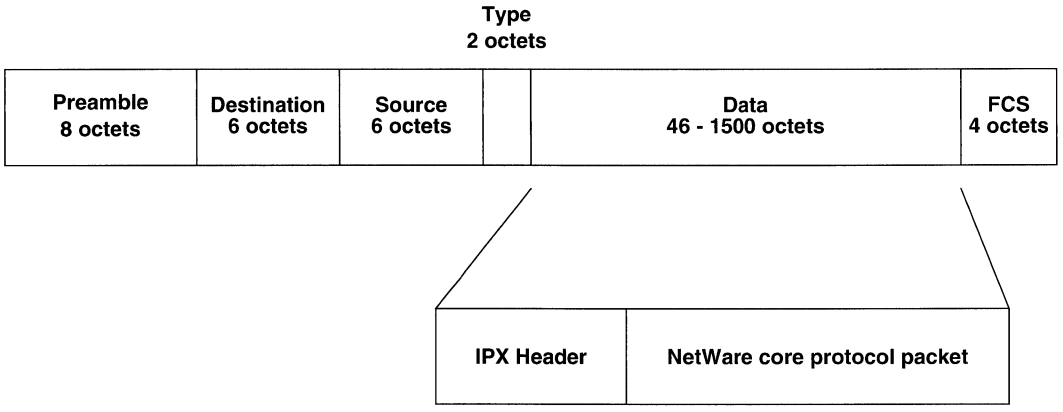


Figure 13-6 Ethernet Encapsulation

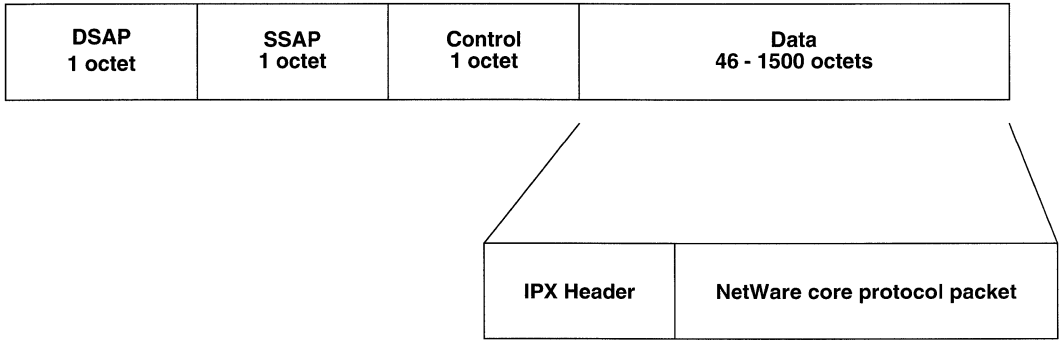


Figure 13-7 802.2 Encapsulation

13.3.1 SAP Advertisements

After you select the CSMA/CD encapsulation method, the cursor moves to **WAN SAP Period (mins)**. This parameter controls the transmission of unsolicited SAP advertisements (referred to as General Server Responses or GSRs) across point-to-point links, thus reducing the amount of bandwidth consumed by the SAP protocol.

NOTE

WAN SAP Period (mins) has no effect on triggered SAP advertisements (those generated in response to bindery changes) or on advertisements generated in response to client requests.

- **WAN SAP Period (mins)** specifies the interval at which the IPX router transmits GSRs across a point-to-point link.

  If **Circuit Group** provides a LAN connection (Ethernet, IEEE 802.3, token ring, or FDDI) simply press `[RETURN]`. The IPX router always transmits GSRs to such media at one minute intervals.

  If **Circuit Group** provides a wide area connection, you can control the frequency of GSR transmission. 1 specifies standard IPX advertisement; GSRs are issued at one minute intervals. To decrease GSR frequency, enter a value (up to a maximum of 99 minutes) and press `[RETURN]`.

  To disable GSR transmission, enter a value of `<0>` and then press `[RETURN]`. You should disable GSR transmission with great care; the loss of a single SAP advertisement can result in unsynchronized binderies at both ends of the link.

NOTE

When the **WAN SAP Period (mins**) parameter is set to anything other than the default value of 1, ensure that the router at the other end of the point-to-point link is configured with the identical **WAN SAP Period (mins)** value.

13.3.2 NetBIOS Broadcasts

After you specify the WAN SAP period, the cursor moves to **Accept NETBIOS Bcasts from net**. You use this parameter in conjunction with the **Deliver NETBIOS Bcasts to net** parameter to tailor, on a per-circuit-group basis, the response of the IPX router to NetBIOS broadcast packets.

NetBIOS (Network Basic Input/Output System) is a session-layer protocol developed by Sytek, Inc. for IBM PC networks. NetBIOS has been widely implemented among other vendors, including Novell. A session is a logical connection between two devices (often workstations) that must be established prior to any communication. NetBIOS establishes that prerequisite logical connection.

Figure 13-8 shows the IPX Router serving four IPX "nets"; in actuality these nets could be a single Novell network or an internet of Novell networks and routers.

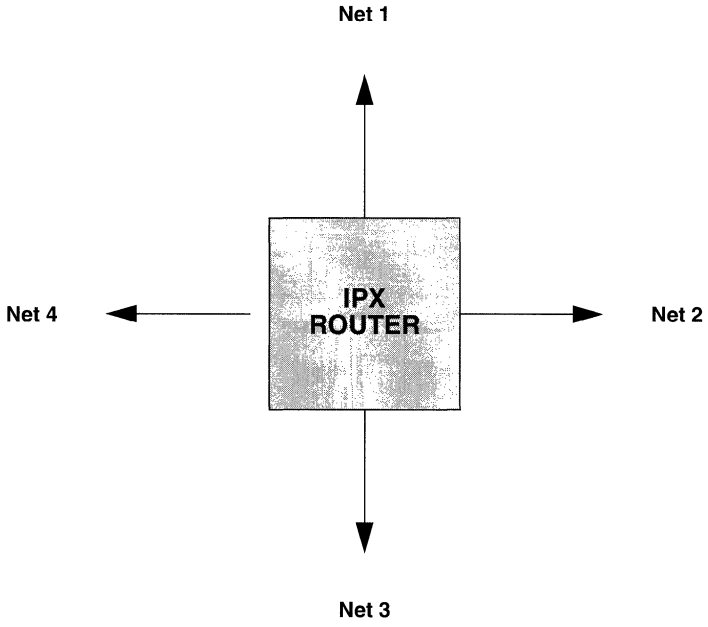


Figure 13-8 Sample IPX Internet

With both NetBIOS parameters (**Accept NETBIOS Bcasts from net** and **Deliver NETBIOS Bcasts to net**) set to **Yes** on all interfaces, a NetBIOS broadcast originated by a client on Net 1 (for example) will be broadcast by the IPX router on all of its other interfaces (Net 2, Net 3, and Net 4).

If, however, the **Accept NETBIOS Bcasts from net** parameter is set to **No** for the Net 1 interface, a NetBIOS broadcast originated by a client on Net 1 will not be broadcast by the IPX router on any interface. As a result, NetBIOS client applications on Net 1 are prevented from initiating and establishing sessions with NetBIOS server applications on any network other than Net 1. Client applications on Nets 2, 3, and 4, however, are not prevented from initiating and establishing sessions with server applications on Net 1.

In a similar fashion, if the **Deliver NETBIOS Bcasts to net** parameter is set to **No** for the Net 1 interface, a NetBIOS broadcast originated by a client on Net 2, 3, or 4 will not be broadcast by the IPX router on the Net 1 interface. As a result, NetBIOS client applications on Nets 2, 3, and 4 are prevented from initiating and establishing sessions with NetBIOS servers on Net 1. Client applications on Net 1, however, are not prevented from initiating and establishing sessions with server applications on Nets 2, 3, or 4.

- **Accept NETBIOS Bcasts from net** enables or disables "local" client access to remote NetBIOS servers.

  Yes, enables NetBIOS client access to the internet; NetBIOS broadcasts generated by clients are broadcast across all IPX router interfaces (save those specifically configured not to accept NetBIOS broadcasts).

  No disables client access to the internet and effectively restricts NetBIOS clients to those services offered by local servers.

- **Deliver NETBIOS Bcasts to net** enables or disables remote access to "local" servers.

  Yes, enables the delivery of received NetBIOS broadcasts across the local interface, thus making local NetBIOS servers available to remote users.

  No disables broadcast and effectively isolates local NetBIOS servers from remote clients.

13.3.3 Token Ring Support

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 end station. Such a peer relationship enables a transition between source route bridging and IPX routing environments and allows the IPX 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 IPX 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]`.

After you set the **Source Route (Token Ring)** parameter the screen displays the IPX Interface Management Screen (Figure 13-9). You use this screen to configure interface-specific-filters and NetBIOS static routes. If you want to configure interface-specific SAP filters, proceed to Section 13.5, *Configuring SAP Filters*; if you want to configure NetBIOS Static Routes, proceed to Section 13.6, *Configuring NetBIOS Static Routes*; if you want to configure traffic filters, proceed to Section 13.7, *Configuring IPX Traffic Filters*. If you do not want to configure these filters or static routes, enter `<0>` at the **Enter Selection (0 for Previous Menu)** prompt to return to the IPX Parameters Access Screen.

```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn

Network Number  :<xxxxxxxx>                 Circuit Group  : <xxxxxxx>
Supply RIP  : <xxx>                        RIP Interface Cost  : <xx>
CSMA/CD Encapsulation  : <xxxxxxxx>        WAN SAP Period (mins)  : <xx>
Accept NETBIOS Bcasts from net  : <xxx>    Deliver NETBIOS Bcasts from net  : <xx>
Source Route (Token Ring)  : <xxx>


1. SAP Network Level Filter Definitions (0)
2. SAP Server Level Filter Definitions (0)
3. NetBIOS Broadcast Static Routes (0)
4. Traffic Filters (0)


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

Figure 13-9 IPX Interface Management Screen

```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn                  Current File : CONFIG

Auto Enable        : <xxx>


        Network Interface Definitions
    Network Number        Circuit Group
1.  <xxxxxxxx>            <xxxxxxx>




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

Figure 13-10 IPX Network Interface Summary Screen

You define additional network interfaces from the IPX Parameters Access Screen. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the IPX Network Interface Summary Screen (Figure 13-10).

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the IPX Network Interface Parameters Screen. Follow the procedures described in Sections 13.3 through 13.3.3 to define an additional IPX interface; repeat these procedures until you have defined all network interfaces.

13.4 Configuring Static Routes

Static routes are user-specified transmission paths that IPX internet packets are to follow on the basis of the packets' destination address. You configure static routes when you want to restrict the paths that packets can follow to paths you specifically define.

Static routes, like routes learned through RIP, are listed in the IPX routing table. Unlike routes learned through RIP, however, static routes cannot be overwritten.

You configure a static route from the IPX Parameters Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen prompts:

No Static Routes Definitions record(s) found
Do you wish to add Static Route Definitions record(s)?

Press `[RETURN]` to display the IPX Static Route Parameters Screen (Figure 13-11).

- **Target Net** identifies a destination network.

  Enter the network number of the destination network.

- **Next Hop Host Number** identifies the host address of the next-hop router used to reach **Target Net**.

  Enter the host address of the next-hop router.

- **Next Hop Network Number** identifies the network address of the next-hop router.

  Enter the network address of the next-hop router.

- **RIP Table Cost** sets the cost for the relay to the next-hop.

  To use the standard IPX RIP cost value of 1 for each hop, enter the number of hops to **Target Net** and press `[RETURN]`. If you are using non-standard cost values, total the individual RIP costs of each hop to **Target Net** (up to a maximum of 15), and press `[RETURN]`.

  You should keep in mind, however, that if you increase the cost, you will more rapidly converge upon the value of 16 (at which value IPX declares the destination unreachable).

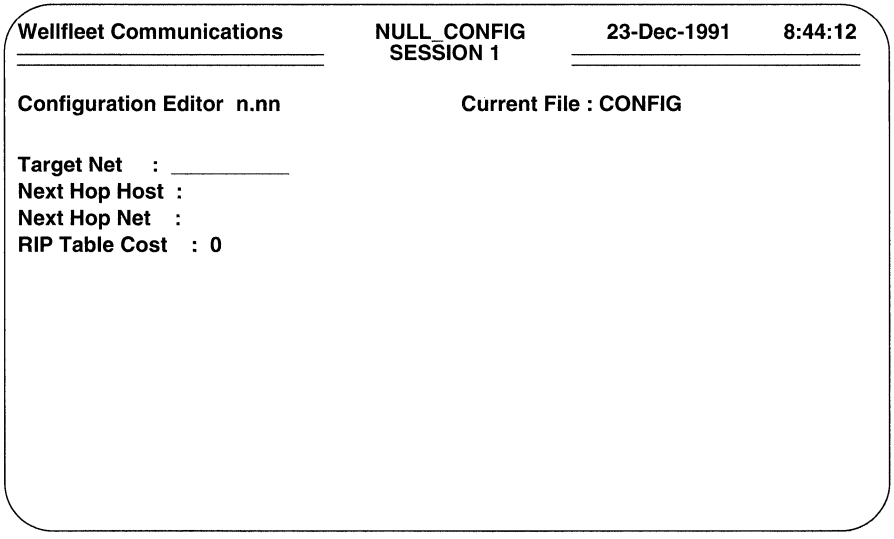


Figure 13-11 IPX Static Route Parameters Screen

After you specify the **RIP Table Cost**, the screen prompts **Hit Return to Continue**. After you press `[RETURN]`, the screen displays the IPX Parameters Access Screen. You define additional static routes from this screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the IPX Static Routes Summary Screen (Figure 13-12).

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the IPX Static Route Parameters Screen. Now follow the same procedures as before to define an additional static route; continue until you have configured all static routes.

13.5 Configuring SAP Filters

SAP transmissions can be filtered on an interface basis. Filtering enables the logical partitioning (for security and/or management purposes) of an IPX internet by controlling the advertisement of servers. If a server is filtered and not advertised on a given IPX network, workstations on that network cannot access the server. SAP filtering, in a sense, erects a user-configurable logical partition(s) between network workstations and network servers.

SAP filtering can be accomplished at both the network and individual server level. Each level supports the specification of up to 50 filters.

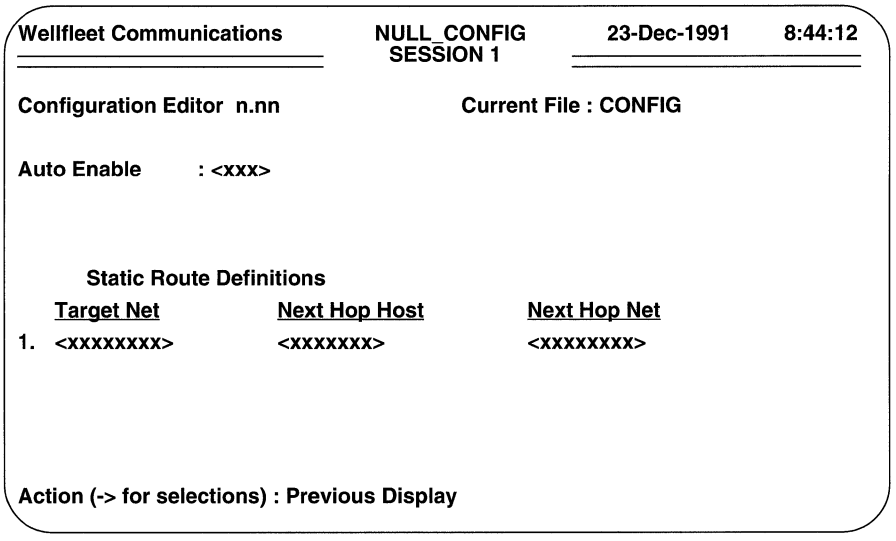


Figure 13-12 IPX Static Routes Summary Screen

At the network level, the filter consists of a pattern (consisting of a network number and a server type) and an action (advertise or ignore). If the action is ignore, any server matching the pattern will not be advertised on the interface. If the action is advertise, any server matching the pattern will be advertised.

At the server level, the filter consists of a pattern (consisting of a server name and a server type) and an action (advertise or ignore). If the action is ignore, any server matching the pattern will not be advertised on the interface. If the action is advertise, any server matching the pattern will be advertised.

Filter precedence within the network or server level is based upon the filter's position in the network- or server-level virtual queue. As filters are configured, they are moved to the virtual queue in the order of their creation. The first-in filter is the one with the lowest precedence; the last-in filter is the one with the highest precedence. Conflicts between server-level and network-level filters are resolved in favor of the server level.

NOTE

In the absence of configured filters, the IPX router advertises all servers listed in its bindery.

13.5.1 SAP Network-Level Filters

You configure SAP network-level filters from the IPX Interface Management Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

No SAP Network Level Filter Definition record(s) found
Do you wish to add SAP Network Level Filter Definitions record(s)?

Press `[RETURN]` to display the IPX SAP Network-Level Filter Parameters Screen.

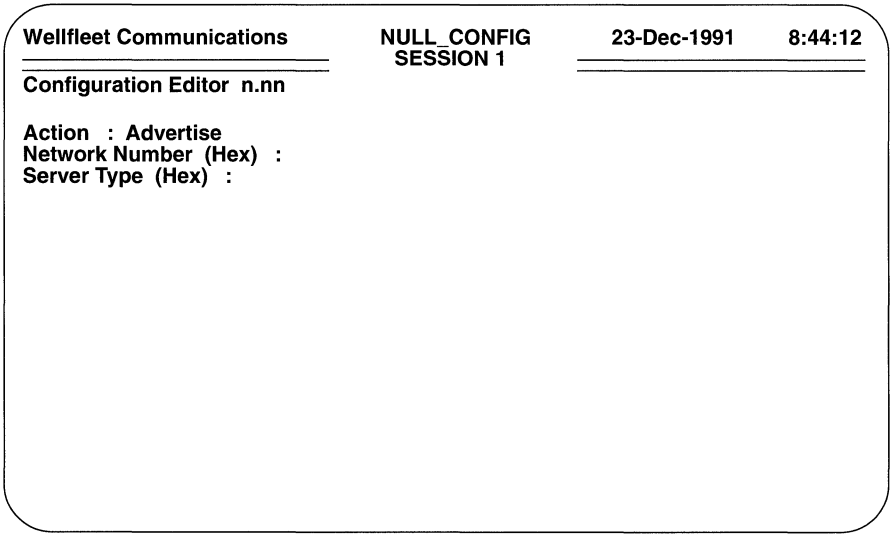


Figure 13-13 IPX SAP Network-Level Filter Parameters Screen

- **Action** tells the IPX router how to process a SAP advertisement which matches the **Network Number/Server Type** pattern.

  Advertise, tells the router to transmit SAP advertisements containing servers which match the pattern. **Ignore** tells the router to drop such servers from the SAP advertisement.

- **Network Number (Hex)** specifies the server network address portion of the filter pattern.

  Enter the IPX network number to be filtered in 8-digit hexadecimal format; be certain in include leading zeros. You can specify FFFFFFFF to indicate "all networks".

- **Server Type (Hex)** specifies the server type portion of the filter pattern.

  Enter the server type number to be filtered in 4-digit hexadecimal format; be certain to include leading zeros. You can specify FFFF to indicate "all types".

After you specify the server type, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the IPX Interface Management Screen. You configure additional SAP network-level filters from this screen. Enter `<1>` at the **Enter Selections (0 for Previous Menu)** prompt. The screen displays the IPX SAP Network-Level Filters Summary Screen.

```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn

Network Number  :<xxxxxxxx>                 Circuit Group  : <xxxxxxx>
Supply RIP  : <xxx>                         RIP Interface Cost  : <xx>
CSMA/CD Encapsulation  : <xxxxxxxx>         WAN SAP Period (mins)  : <xx>
Accept NETBIOS Bcasts from net  : <xxx>     Deliver NETBIOS Bcasts from net  : <xx>

                    SAP Network Level Filter Definitions

      Action      Network Number (Hex)      Server Type (Hex)
1.    <xxxxxxx> <xxxxxxxx>                  <xxxx>




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

Figure 13-14 IPX SAP Network-Level Filters Summary Screen

To add another SAP network-level filter press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen displays the IPX SAP Network Level Filter Parameters Screen. Now follow the same procedure as before to configure an additional filter; continue until you have configured all SAP network-level filters for this interface.

13.5.2 SAP Server-Level Filters

You configure SAP server-level filters from the IPX Interface Management Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No SAP Server Level Filter Definition record(s) found
Do you wish to add SAP Server Level Filter Definitions record(s)?

Press **[RETURN]** to display the IPX SAP Server-Level Filter Parameters Screen.

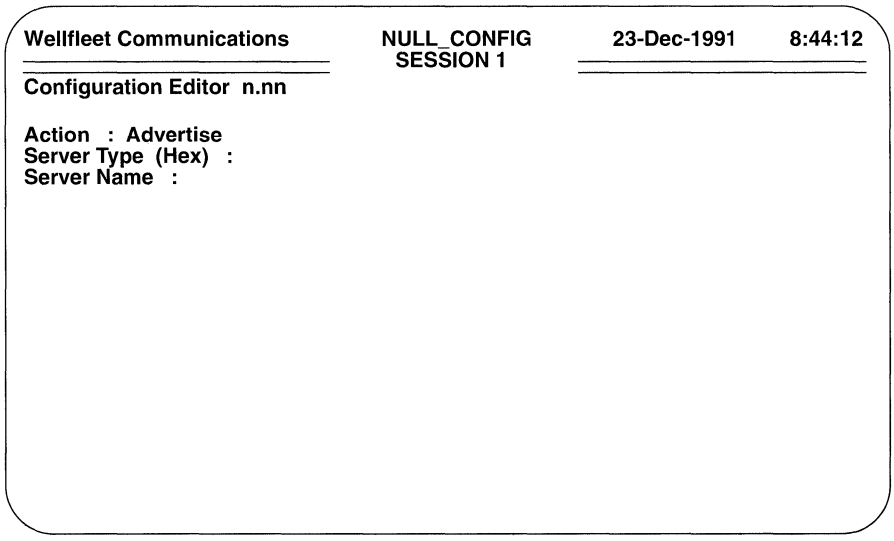


Figure 13-15 IPX SAP Server-Level Filter Parameters Screen

- **Action** tells the IPX router how to handle a SAP advertisement which matches the **Server Type/Server Name** pattern.

  Advertise, tells the router to transmit SAP advertisements containing servers which match the pattern. **Ignore** tells the router to drop such servers from SAP advertisements.

- **Server Type (Hex)** specifies the server type portion of the filter pattern.

  Enter the server type number to be filtered in 4-digit hexadecimal format; be certain to include leading zeros. You can specify FFFF to indicate "all types".

- **Server Name** specifies the server name portion of the filter pattern.

  Server Name can be any valid Novell server name of up to 48 characters; any keyboard character, with the exception of the tilde (~) character can be used.

  If **Server Name** contains 48 characters, the node sets the final character to NULL (hexadecimal 00) when matching against actual server names. If **Server Name** contains less than 48 characters, it is left-justified and the remaining characters are NULL-filled. Name matching is performed up to the first NULL character.

NOTE

Matching is case sensitive; Ken's.IPX.Router is not equivalent to ken's.ipx.router.

After you specify the server name, the screen prompts **Hit Return to Continue**. Press [RETURN] to revert to the IPX Interface Management Screen.

You configure additional SAP server-level filters from the IPX Interface Management Screen. Enter <2> at the **Enter Selections (0 for Previous Menu)** prompt. The screen displays the IPX SAP Server-Level Filters Summary Screen which provides a listing of all previously configured server-level filters.

```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn

Network Number  :<xxxxxxxx>                  Circuit Group  : <xxxxxxx>
Supply RIP  : <xxx>                          RIP Interface Cost  : <xx>
CSMA/CD Encapsulation  : <xxxxxxxx>          WAN SAP Period (mins)  : <xx>
Accept NETBIOS Bcasts from net  : <xxx>      Deliver NETBIOS Bcasts from net  : <xx>
Source Route (Token Ring)  : <xxx>

                    SAP Server Level Filter Definitions

     Action      Server Type (Hex)      Server Name
1.   <xxxxxxx> <xxxxxxxx>               <xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>




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

Figure 13-16 IPX SAP Server-Level Filters Summary Screen

To add another SAP server-level filter press the [RIGHTARROW] to display **Add** and then press [RETURN]. The screen displays the IPX SAP Server Level Filter Parameters Screen. Now follow the same procedure as before to configure an additional filter; continue until you have configured all SAP server-level filters for this interface.

13.6 Configuring NetBIOS Static Routes

The IPX router provides a non-Novell-standard "static routing" mechanism that converts "all nets" IPX NetBIOS broadcast packets to "directed" broadcast (a network-specific broadcast). This feature enables a logical partitioning of an IPX

NetBIOS network, and minimizes the bandwidth used by the IPX "all nets" broadcast facility.

Each IPX router interface supports up to 50 NetBIOS static routes arranged as a table. Each static route specifies a NetBIOS resource name and a destination network (where the resource resides). With NetBIOS static routes configured, the IPX router compares all IPX NetBIOS broadcasts packets received on an interface with interface-specific NetBIOS static routes. If the NetBIOS destination name found in the packet matches a table entry, the NetBIOS packet is routed to the associated destination network; if no match is found, the IPX router treats the packet as specified by the **Accept NETBIOS Bcasts from net** and **Deliver NETBIOS Bcasts to net** parameters.

The static routing mechanism (if configured for an interface) takes precedence over the **Accept NETBIOS Bcasts from net** parameter. Similarly, a statically routed NetBIOS broadcast will be delivered to the destination network regardless of the value of the **Deliver NETBIOS Bcasts to net** parameter at the receiving end.

NetBIOS static routing is typically used to enable a NetBIOS client of one network to establish a session with a remote NetBIOS server. To facilitate session establishment with a minimum of bandwidth usage, the IPX router interface connected to the client network requires a NetBIOS static route that specifies the server's network and the server's name. Judicious configuration of IPX NetBIOS static routes in conjunction with the **Accept NETBIOS Bcasts from net** and **Deliver NETBIOS Bcasts to net** parameters enables session establishment control, thus facilitating internet security and management.

NOTE

As IPX NetBIOS static routing is not a Novell "standard" this feature may not interoperate with non-Wellfleet routers.

You configure NetBIOS static routes from the IPX Interface Management Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No NETBIOS Broadcast Static Route record(s) found
Do you wish to add NETBIOS Broadcast Static Route record(s)?

Press `[RETURN]` to display the IPX NetBIOS Static Route Parameters Screen (Figure 13-17).

- **Dest Network (Hex)** identifies the network where the NetBIOS target resides.

  Enter the network number in 8-digit hexadecimal format (use leading 0's if necessary) and then press `[RETURN]`.

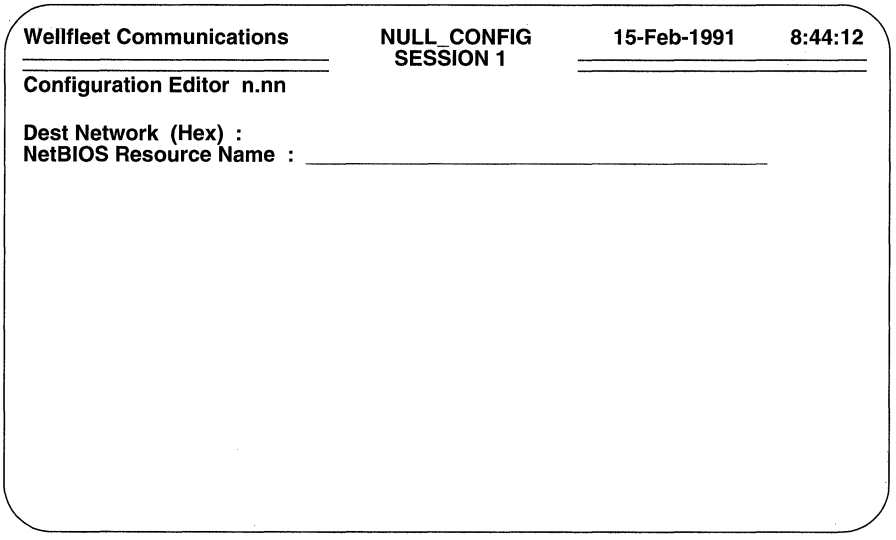


Figure 13-17 IPX NetBIOS Static Route Parameters Screen

- **NetBIOS Resource Name** is the name of the NetBIOS target.

  NetBIOS names consist of up to 16 characters and can include any keyboard character except backslash (\) and tilde (~). If a character cannot be entered from the keyboard it can be entered in two-digit hexadecimal for as "\xx" (where xx is a two-digit hexadecimal value); the backslash character can be entered as "\\". For example, the name

  JOE's Server \\\03\01

  results in the following byte sequence:

4A	4F	45	27	73	20	53	65	72	76	65	72	5C	03	01
J	O	E	'	s		S	e	r	v	e	r	\	03	01

  If **NetBIOS Resource Name** is less than 16-bytes, the byte string is left justified and NULL filled. The name match is performed on all 16 bytes.

NOTE

Matching is case sensitive; JOE's Server is not equivalent to joe's server.

Enter the NetBIOS name (as it appears in IPX NetBIOS *Name Find Packets*) and then press `[RETURN]`.

After you specify the NetBIOS name, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the IPX Interface Management Screen.

You configure additional IPX NetBIOS static routes from the IPX Interface Management Screen. Enter `<3>` at the **Enter Selections (0 for Previous Menu)** prompt. The screen displays the IPX NetBIOS Static Routes Summary Screen (Figure 13-18) which provides a listing of all previously configured static routes.

```
Wellfleet Communications        NULL_CONFIG          23-Dec-1991      8:44:12
                                SESSION 1
Configuration Editor  n.nn

Network Number  :<xxxxxxxx>                  Circuit Group  : <xxxxxxx>
Supply RIP  : <xxx>                          RIP Interface Cost  : <xx>
CSMA/CD Encapsulation  : <xxxxxxxx>          WAN SAP Period (mins)  : <xx>
Accept NETBIOS Bcasts from net  : <xxx>      Deliver NETBIOS Bcasts from net  : <xx>
Source Route (Token RIng)  : <xxx>

                    NETBIOS Broadcast Static Routes

      Dest Network  (Hex)                    NetBIOS Resource Name
1.    <xxxxxxxx>                             <xxxxxxxxxxxxxxxx>

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

Figure 13-18 IPX NetBIOS Static Routes Summary Screen

To add another NetBIOS static route press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen displays the IPX NetBIOS Static Route Parameters Screen. Now follow the same procedure as before to configure an additional static route; repeat this procedure until you have configured all NetBIOS static routes for this interface.

13.7 Compiling IPX Filter Lists

Filter lists (while not required) may facilitate the configuration of filters if you want 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 IPX 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 IPX List Access Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


1. Network Lists (0)
2. Host  Lists (0)
3. Socket Lists (0)
4. Packet Type Lists (0)



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

Figure 13-19 IPX List Access Screen

13.7.1 Network Lists

Network lists specify ranges of IPX network numbers.

You compile a network list from the IPX List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the network list.

  Enter a list name, and then press `[RETURN]`.

After you name the network list, the screen prompts for list members (Figure 13-20).

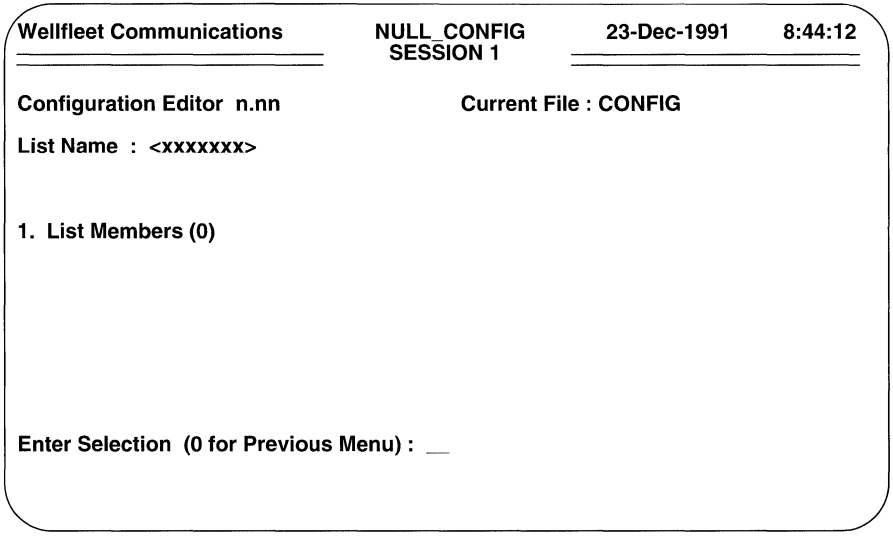


Figure 13-20 IPX List Member Access Screen

To assign a range of IPX networks to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the IPX Network Range Screen (Figure 13-21).

- **Network Number (low)** specifies the lower boundary of the network range.

  Enter an IPX network number.

- **Network Number (high)** specifies the upper boundary of the network range.

  Enter an IPX network number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Network Number (low)** parameter, simply press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the IPX List Member Access Screen.

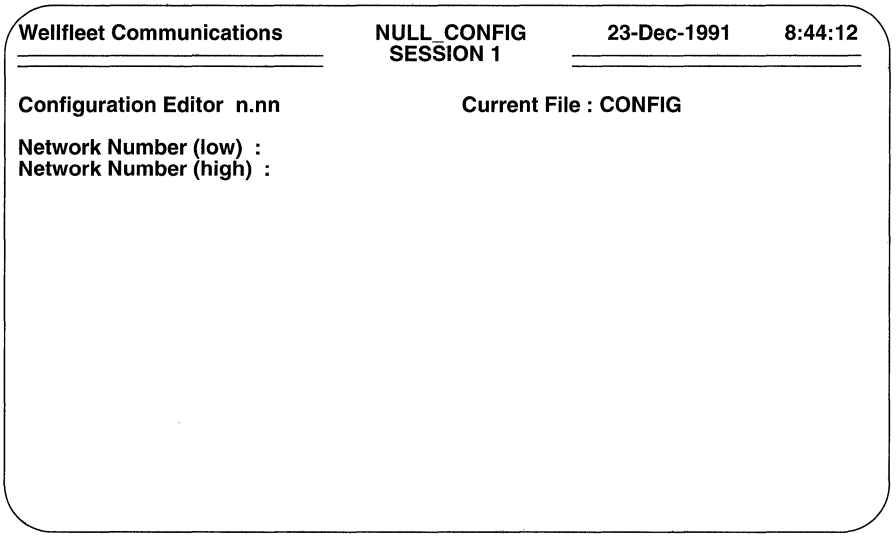


Figure 13-21 IPX Network Range Screen

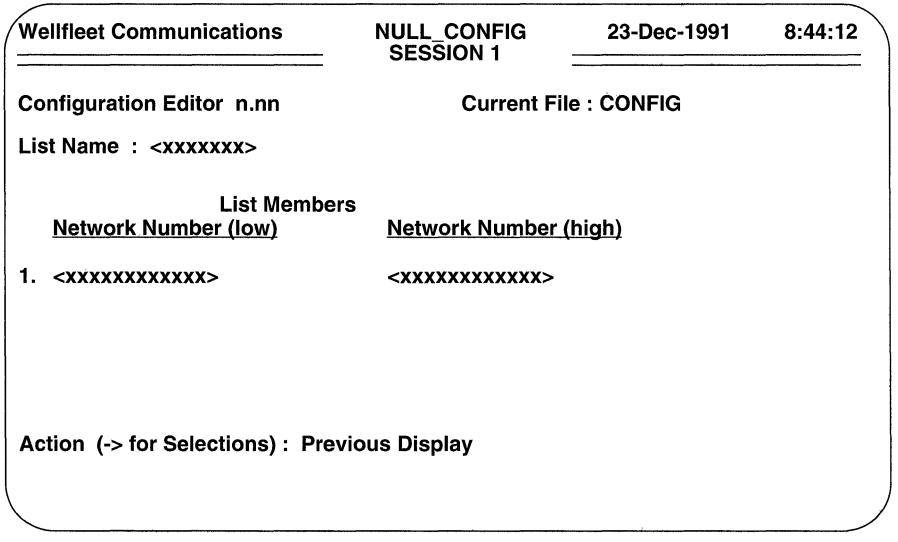


Figure 13-22 IPX Network List Members Screen

If you want, you can add other network ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the IPX Network List Members Screen (Figure 13-22). To add another range of network numbers, with the cursor at the **Action (-> for Selections)** prompt, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.

The screen displays the IPX Network Range Screen. Now follow the same procedure as before to add another network number range; continue until you have added all desired ranges to the list.

You compile additional network lists from the IPX List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the IPX Network List Summary Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


    Network Lists
      List Name

1. <xxxxxxx>




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

Figure 13-23 IPX Network List Summary Screen

To compile another network 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 IPX network lists.

13.7.2 Host Lists

Host lists specify ranges of IPX host numbers.

You compile a host list from the IPX List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the host list.

  Enter a list name, and then press `[RETURN]`.

After you name the host list, the screen prompts for list members.

To assign a range of IPX hosts to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the IPX Host Range Screen (Figure 13-24).

- **Host Number (low)** specifies the lower boundary of the host range.

  Enter an IPX host number.

- **Host Number (high)** specifies the upper boundary of the host range.

  Enter an IPX host number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Host Number (low)** parameter, simply press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the IPX List Member Access Screen.

If you want, you can add other IPX host ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the IPX Host List Members Screen (Figure 13-25). To add another range of hosts, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.

The screen displays the IPX Host Range Screen. Now follow the same procedure as before to add another host range; continue until you have added all desired ranges to the list.

You compile additional host lists from the IPX List Access Screen. To begin, enter `<2>` at **Enter Selection (0 for Previous Menu)** to display the IPX Host List Summary Screen (Figure 13-26).

To compile another host list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional host list; repeat this procedure until you have compiled all IPX host lists.

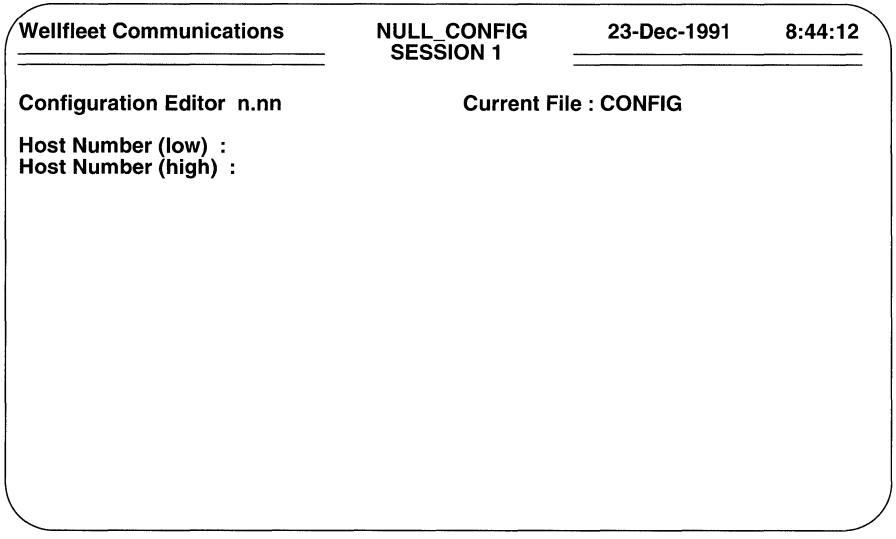


Figure 13-24 IPX Host Range Screen

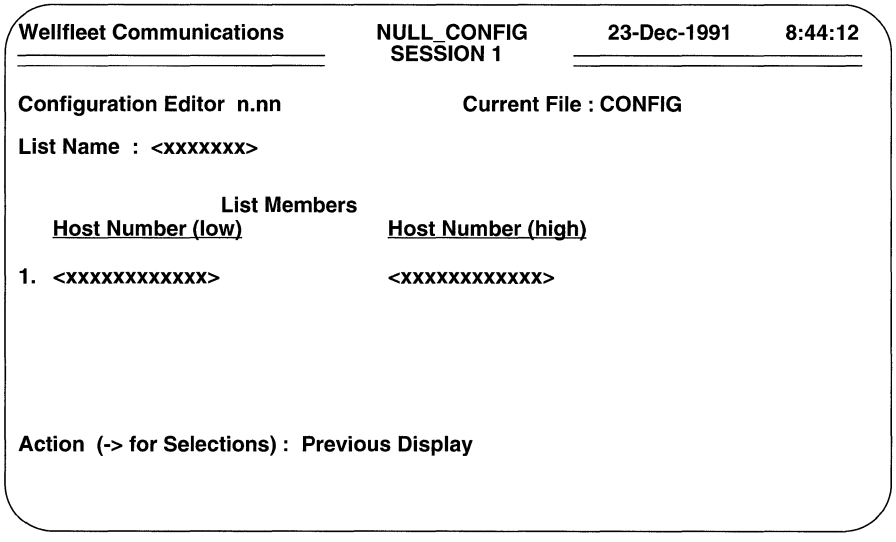


Figure 13-25 IPX Host List Members Screen

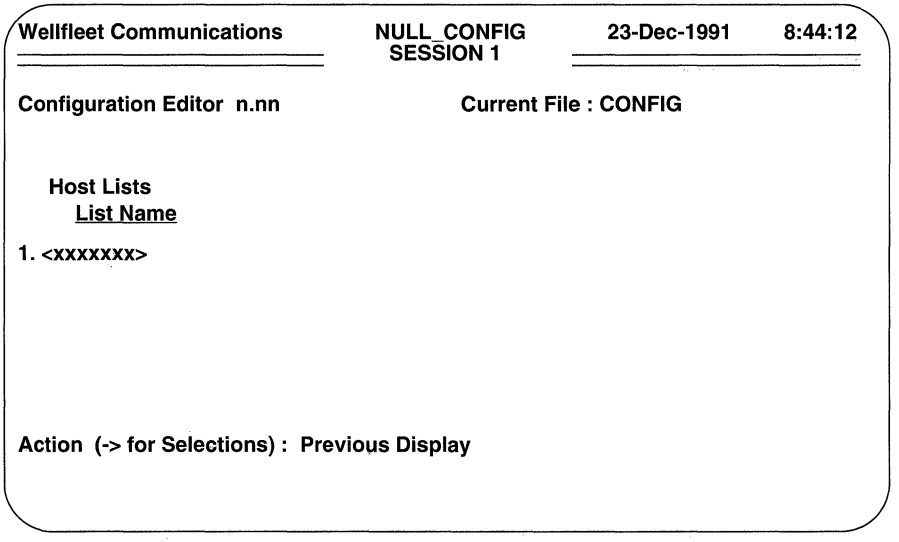


Figure 13-26 IPX Host List Summary Screen

13.7.3 Socket Lists

Socket lists specify ranges of IPX socket numbers.

You compile a socket list from the IPX List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the socket list.

  Enter a list name, and then press `[RETURN]`.

After you name the socket list, the screen prompts for list members.

To assign a range of IPX sockets to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the IPX Socket Range Screen (Figure 13-27).

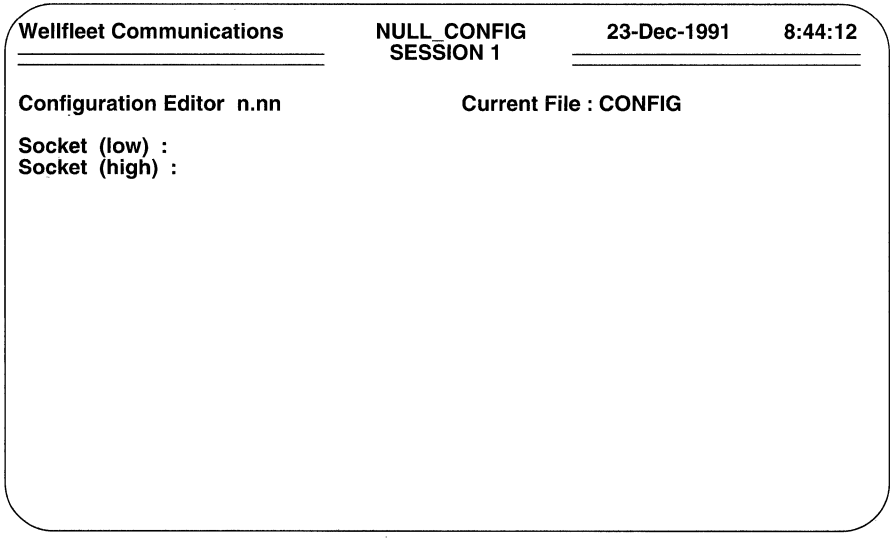


Figure 13-27 IPX Socket Range Screen

- **Socket (low)** specifies the lower boundary of the socket range.

  Enter an IPX socket number.

- **Socket (high)** specifies the upper boundary of the socket range.

  Enter an IPX socket number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Socket (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the IPX List Member Access Screen.

If you want, you can add other socket ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the IPX Socket List Members Screen (Figure 13-28).

To add another range of socket numbers, with the cursor at the **Action (-> for Selections)** prompt, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.The screen displays the IPX Socket Range Screen. Now follow the same procedure as before to add another socket range; continue in this fashion until you have added all desired ranges to the list.

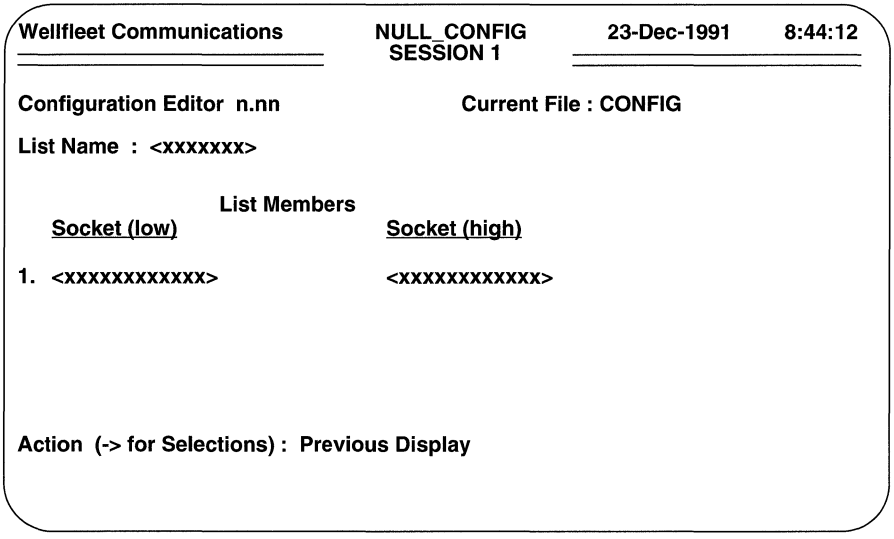


Figure 13-28 IPX Socket List Members Screen

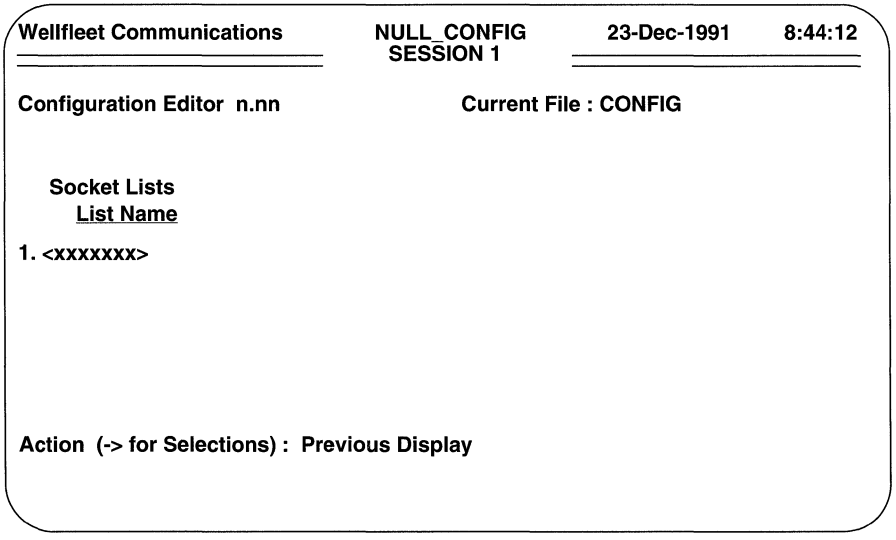


Figure 13-29 IPX Socket List Summary Screen

You compile additional socket lists from the IPX List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)** to display the IPX Socket List Summary Screen (Figure 13-29). To compile another IPX socket list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional socket list; repeat this procedure until you have compiled all IPX socket lists.

13.7.4 Packet Type Lists

Packet type lists specify ranges of IPX packet type numbers.

You compile a packet type list from the IPX List Access Screen. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

No Packet Type Lists record(s) found
Do you wish to add Packet Type Lists record(s)?

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the packet type list.

  Enter a list name, and then press `[RETURN]`.

After you name the packet type list, the screen prompts for list members.

To assign a range of packet types to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the IPX Packet Type Range Screen (Figure 13-30).

- **Packet Type (low)** specifies the lower boundary of the packet type range.

  Enter an IPX packet type number.

- **Packet Type (high)** specifies the upper boundary of the packet type range.

  Enter an IPX packet type number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Packet Type (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the IPX List Member Access Screen.

If you want, you can add other packet type ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the IPX Packet Type List Members Screen (Figure 13-31).

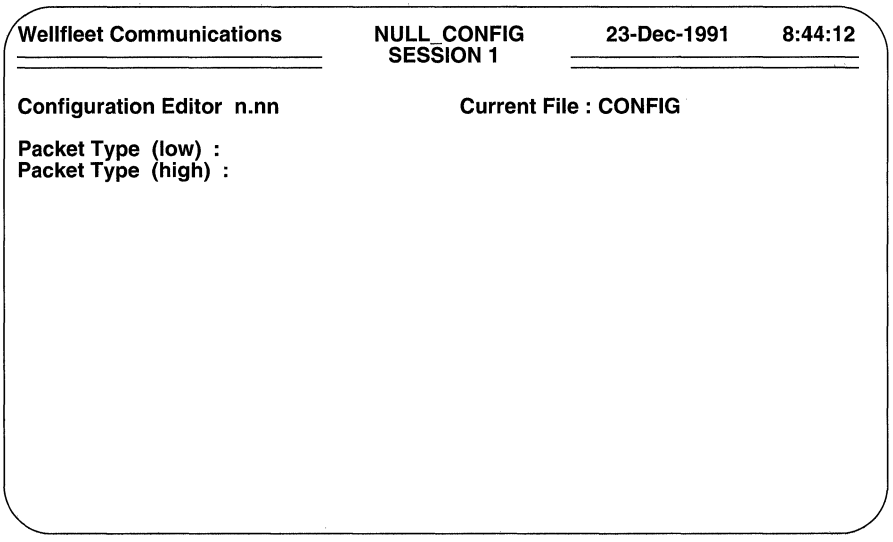


Figure 13-30 IPX Packet Type Range Screen

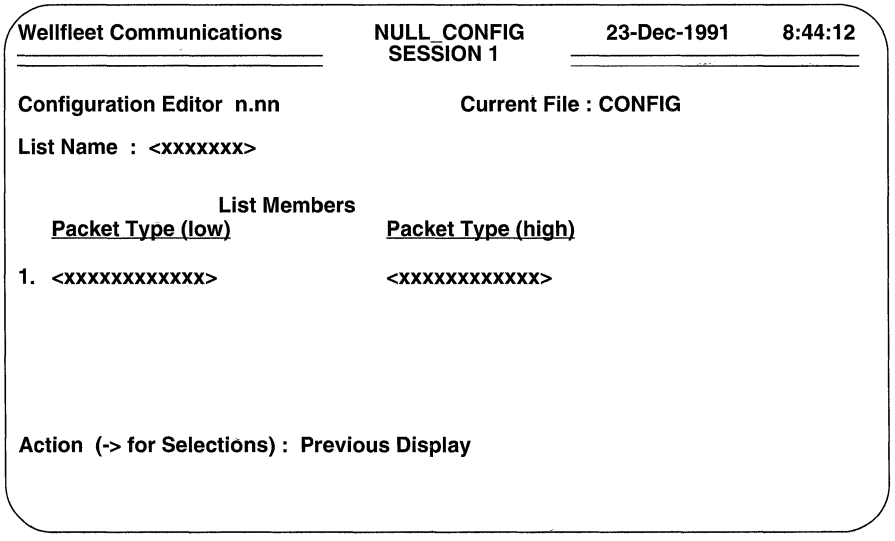


Figure 13-31 IPX Packet Type List Members Screen

To add another range of packet type numbers, with the cursor at the **Action (-> for Selections)** prompt, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.

The screen displays the IPX Packet Type Range Screen. Now follow the same procedure as before to add another packet type range; continue in this fashion until you have added all desired ranges to the list.

You compile additional packet type lists from the IPX List Access Screen. To begin, enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the IPX Packet Type List Summary Screen.

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

Configuration Editor  n.nn                    Current File : CONFIG


    Packet Type Lists
      List Name

1. <xxxxxxx>




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

Figure 13-32 IPX Packet Type List Summary Screen

To compile another packet type list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional packet type list; repeat this procedure until you have compiled all IPX packet type lists.

13.8 Configuring IPX Filters

IPX filters apply to all in-coming IPX traffic across the interface. You can, if you wish, construct up to 31 filters for each IPX interface. You configure interface-specific IPX traffic filters from the IPX Interface Management Screen. Enter `<4>` 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 accept the default response, **Yes**. The screen displays the IPX Filters Rule Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG

Precedence : 1
Dest Network (low) :                (high) :          effect : Ignore
Dest Host (low) :                   (high) :          effect : Ignore
Dest Socket (low) :                 (high) :          effect : Ignore
Source Network (low) :              (high) :          effect : Ignore
Source Host (low) :                 (high) :          effect : Ignore
Source Socket (low)                 (high) :          effect : Ignore
Packet Type (low) :                 (high) :          effect : Ignore
Action : Drop
```

Figure 13-33 IPX 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 interface. The **Precedence** value is used when an in-coming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

  Press the `[RIGHTARROW]` to select a value from 1 to 31 and then press `[RETURN]`.

NOTE

In the event of two filters with equal precedence, the first configured filter takes precedence.

- **Dest Network (low)** specifies the lower boundary range of filtered destination networks.

If you do not want to filter destination networks, press **[RETURN]**.

To filter destination networks, do one of the following:

- enter the name of a network list
- enter a network number at the lower boundary of the destination network range
- enter a single destination network number

After you enter a destination network or a list name, press **[RETURN]**.

- **(high)** specifies the upper boundary range of filtered destination networks.

  If you do not want to filter destination networks, press **[RETURN]**.

  To filter destination networks, do one of the following:

  - if you entered the name of a network list at **Dest Network (low)**, or if you want to filter the single network specified at **Dest Network (low)**, press **[RETURN]**.
  - if you entered a lower boundary range value at **Dest Network (low)**, enter a network number 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 pattern specified by **Dest Network (low)** and **(high)**.

  If the filter does not care about destination network values, press **[RETURN]** to accept the default, **Ignore**.

  To filter destination networks, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Network (low)** and **(high)** includes the destination network field of the IPX packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Network (low)** and **(high)** does not include the destination network field of the IPX packet.

- **Dest Host (low)** specifies the lower boundary range of filtered destination hosts.

  If you do not want to filter destination hosts, simply press **[RETURN]**.

  To filter IPX destination hosts, do one of the following:

  - enter the name of a host list
  - enter a host number at the lower boundary of the destination host range
  - enter a single destination host number

- **(high)** specifies the upper boundary range of filtered destination hosts.

  If you do not want to filter IPX destination hosts, press `[RETURN]`.

  To filter destination hosts, do one of the following:

  - if you entered the name of a host list at **Dest Host (low)**, or if you want to filter the single host specified at **Dest Host (low)** press `[RETURN]`.
  - if you entered a lower boundary range value at **Dest Host (low)**, enter a host number 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 pattern specified by **Dest Host (low)** and **(high)**.

  If the filter does not care about destination host values, press `[RETURN]` to accept the default, **Ignore**.

  To filter destination hosts, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Host (low)** and **(high)** includes the destination host field of the packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Host (low)** and **(high)** does not include the destination host field of the packet.

- **Dest Socket (low)** specifies the lower boundary range of filtered destination sockets.

  If you do not want to filter destination sockets, simply press `[RETURN]`.

  To filter destination sockets, do one of the following:

  - enter the name of a socket list
  - enter a socket number at the lower boundary of the destination socket range
  - enter a single destination socket number

- **(high)** specifies the upper boundary range of filtered destination sockets.

  If you do not want to filter destination sockets, press `[RETURN]`.

  To filter destination sockets, do one of the following:

  - if you entered the name of a socket list at **Dest Socket (low)**, or if you want to filter the single socket specified at **Dest Socket (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **Dest Socket (low)**, enter a socket number 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 pattern specified by **Dest Socket (low)** and **(high)**.

If the filter does not care about destination socket values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination sockets, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Socket (low)** and **(high)** includes the destination socket field of the packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Socket (low)** and **(high)** does not include the destination socket field of the packet.

❒ **Source Network (low)** specifies the lower boundary range of filtered source networks.

If you do not want to filter source networks, press `[RETURN]`.

To filter source networks, do one of the following:

- enter the name of a network list
- enter a network number at the lower boundary of the source network range
- enter a single source network number

After you enter a source network or a list name, press `[RETURN]`.

❒ **(high)** specifies the upper boundary range of filtered source networks.

If you do not want to filter source networks, simply press `[RETURN]`.

To filter source networks, do one of the following:

- if you entered the name of a network list at **Source Network (low)**, or if you want to filter the single source network specified at **Source Network (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Source Network (low)**, enter a network number 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 pattern specified by **Source Network (low)** and **(high)**.

If the filter does not care about source network values, press `[RETURN]` to accept the default, **Ignore**.

To filter source networks, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Network (low)** and **(high)** includes the source network field of the packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Network (low)** and **(high)** does not include the source network field of the packet.

❒ **Source Host (low)** specifies the lower boundary range of filtered source hosts.

If you do not want to filter source hosts, press `[RETURN]`.

To filter source hosts, do one of the following:

- enter the name of a host list
- enter a host number at the lower boundary of the source host range
- enter a single source host number

❒ **(high)** specifies the upper boundary range of filtered source hosts.

If you do not want to filter source hosts, simply press `[RETURN]`.

To filter source hosts, do one of the following:

- if you entered the name of a host list at **Source Host (low)**, or if you want to filter the single host specified at **Source Host (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Source Host (low)**, enter a host number 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 pattern specified by **Source Host (low)** and **(high)**.

If the filter does not care about source host values, press `[RETURN]` to accept the default, **Ignore**.

To filter source hosts, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Host (low)** and **(high)** includes the source host field of the packet.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Host (low)** and **(high)** does not include the source host field of the packet.

- **Source Socket (low)** specifies the lower boundary range of filtered source sockets.

  If you do not want to filter source sockets, simply press `[RETURN]`.

  To filter source sockets, do one of the following:

  - enter the name of a socket list
  - enter a socket number at the lower boundary of the source socket range
  - enter a single source socket number

- **(high)** specifies the upper boundary range of filtered source sockets.

  If you do not want to filter source sockets, press `[RETURN]`.

  To filter source sockets, do one of the following:

  - if you entered the name of a socket list at **Source Socket (low)**, or if you want to filter the single source socket specified at **Source Socket (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Socket (low)**, enter a socket number 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 host address pattern specified by **Source Socket (low)** and **(high)**.

  If the filter does not care about source socket values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source sockets, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Socket (low)** and **(high)** includes the source socket field of the packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Socket (low)** and **(high)** does not include the source socket field of the packet.

- **Packet Type (low)** specifies the lower boundary range of filtered packet types.

  If you do not want to filter packet types, press `[RETURN]`.

  To filter packet types, do one of the following:

  - enter the name of a packet type list
  - enter a packet type number at the lower boundary of the packet type range
  - enter a single packet type number

- **(high)** specifies the upper boundary range of filtered packet types.

  If you do not want to filter packet types, press `[RETURN]`.

  To filter packet types, do one of the following:

  - if you entered the name of a packet type list at **Packet Type (low)**, or if you want to filter the single socket specified at **Packet Type (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Packet Type (low)**, enter a packet type number 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 packet type pattern specified by **Packet Type (low)** and **(high)**.

  If the filter does not care about packet type values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source sockets, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** includes the packet type field of the packet.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Packet Type (low)** and **(high)** does not include the packet type field of the packet.

- **Action** specifies the disposition of packets 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, press `[RETURN]`.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the IPX Interface Management Screen.

You configure additional filters (up to a maximum of 31 per network interface) from the IPX Interface Management Screen. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the IPX Filters Summary Screen.

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the IPX Filters Rule Screen.

Follow the same procedures as before to define an additional IPX filter; repeat these procedures until you have defined all filters.

14 Configuring AppleTalk

This chapter tells you how to configure the AppleTalk router.

AppleTalk is the protocol suite developed by Apple Computer, Inc. to provide connectivity between members of the Macintosh family of personal computers. The AppleTalk router implements the AppleTalk Phase 2 protocol that extends the original AppleTalk suite and offers enhanced routing and naming services.

NOTE

The AppleTalk router does not support AppleTalk Phase 1 routing. You can, however, bridge AppleTalk Phase 1 traffic.

The AppleTalk router is compatible with Apple standards and fully supports the AppleTalk Address Resolution Protocol, the Datagram Delivery Protocol, the Routing Table Maintenance Protocol, the Name Binding Protocol, the Apple Echo Protocol, and the Zone Information Protocol.

- The AppleTalk Address Resolution Protocol (AARP) is a data-link layer protocol that maps AppleTalk node addresses (also called protocol addresses) to their equivalent hardware address. AARP maintains an Address Mapping Table (AMT), a listing of equivalent protocol and hardware addresses accompanied by an indication of the circuit group/port on which the address resolution is in effect. The AMT is maintained and updated through the transmission and receipt of AARP *Response* and *Request* packets. AARP also ensures the integrity of the network-number/node identifier pair by generating AARP *Probe* messages.

  AARP *Probe* is an extension of standard AARP that guards against address duplication. In the absence of an explicitly assigned node identifier, AARP generates a tentative identifier, combines this identifier with a randomly generated network number, and then scans its address mapping tables. If the tentative address is found in the tables (indicating its use by another node), AARP generates another tentative identifier, and repeats its scan of the mapping tables. Upon generating a tentative address not found within the mapping tables, AARP transmits a series of *Probe* packets to the tentative address. In the absence of a positive response to this series of packets (indicating that the address is unused), AARP validates the tentative address.

- The Datagram Delivery Protocol (DDP) is a Network layer protocol that provides a "best-effort" socket-to-socket delivery mechanism.
- The Routing Table Maintenance Protocol (RTMP) is a Transport layer protocol that creates and maintains the routing information required by the AppleTalk router to transmit packets across an internet from a source to a destination socket. Such routing information is contained in the AppleTalk Routing Table. Each table entry includes a destination network range, the AppleTalk protocol address (network number and node identifier) through which the destination is reached, the number of router hops to the destination, and the route status.
- The Name Binding Protocol (NBP) is a Transport layer protocol that translates a character string (the name of a network node) into the equivalent AppleTalk protocol address.
- The Apple Echo Protocol (AEP) is a Transport layer protocol that tests node reachability. AEP enables a node to send a packet to another internet node and to receive an identical (echoed) packet in response.
- The Zone Information Protocol (ZIP) is a Session layer protocol that maintains an internet-wide mapping of zone names and network numbers.

14.1 Filtering AppleTalk DDP Packets

Filters enable the router to relay or drop a particular datagram based on the contents of specific fields within the DDP extended-header datagram (Figure 14-1). The extended form DDP header is used to exchange packets between different AppleTalk networks across an internet.

- Byte 1 of the DDP header contains a four-bit hop count field that enumerates the number of routers encountered in a datagram's transit from source to destination. Each router that forwards a packet to another intervening router increments the hop count by one. A datagram that reaches its 16th router is discarded.

  The upper two bits of Byte 1 are set to 0, while the remaining bits contain the most significant bits of the datagram length.
- Byte 2 contains the lower eight bits of the datagram length.
- Bytes 3 and 4 contain a 16-bit checksum.
- Bytes 5 and 6 contain the 16-bit destination network.
- Bytes 7 and 8 contain the 16-bit source network.
- Byte 9 contains the eight-bit destination node.
- Byte 10 contains the eight bit source node.

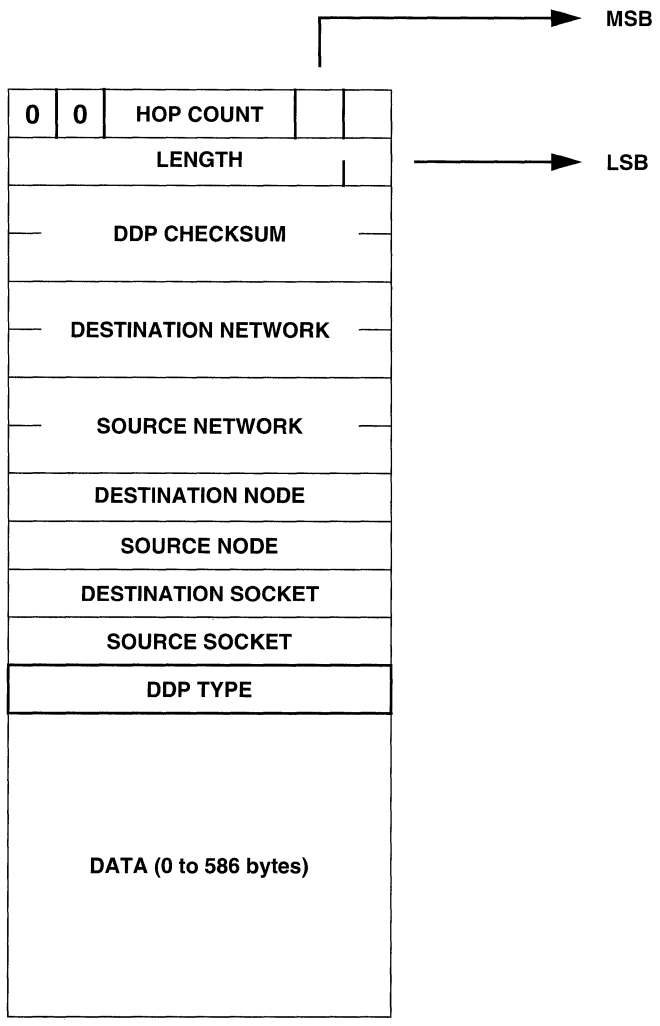


Figure 14-1 AppleTalk DDP Datagram Format

- Byte 11 contains an eight-bit destination socket (a local address associated with a specific software process). AppleTalk reserves well-known sockets for use by certain protocols. Table 14-1 lists certain well-known socket numbers found in the DDP header.

Table 14-1: AppleTalk Well-Known Sockets

Socket Number	Protocol
01	Routing Table Maintenance Protocol
02	Name Binding Protocol
04	AppleTalk Echo Protocol
06	Zone Information Protocol

- Byte 12 contains the eight bit source socket.
- Byte 13 contains the protocol type carried in the Data portion of the DDP packet. Table 14-2 lists common protocol types.

Table 14-2: AppleTalk Packet Types

Type	Protocol
01	Routing Table Maintenance Protocol
02	Name Binding Protocol
03	AppleTalk Transaction Protocol
04	AppleTalk Echo Protocol
05	Routing Table Maintenance Protocol
06	Zone Information Protocol
07	AppleTalk Data Stream Protocol

AppleTalk filters examine the following DDP packet fields either singly or in combination: destination network, destination node, destination socket, source network, source node, source socket, and DDP type.

Filtering decisions are based on user-defined rules. An AppleTalk filter rule consists of an DDP datagram 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 datagram field and the value; an action (*drop* or *forward*); and a filter precedence.

For example, the AppleTalk filter-rule-A depicted in Figure 14-2 prevents routing updates issued by a suspect router (AppleTalk network address, 100; node address, 24) from being promulgated throughout the internet.

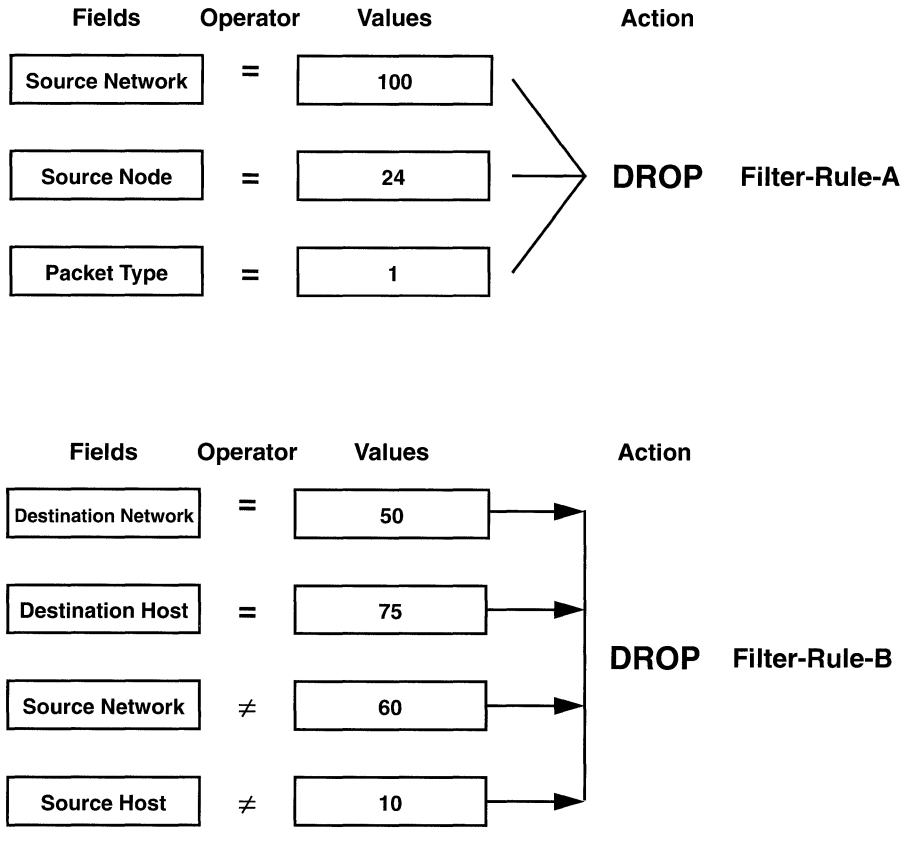


Figure 14-2 AppleTalk Sample Filters

Filter-rule-B isolates an AppleTalk node (network address 50; node address, 75), probably storing sensitive or confidential access, from all access except from a single node (network address 60; host address 10).

14.2 Setting AppleTalk Basic Parameters

The AppleTalk basic parameters are listed in Table 14-3.

Table 14-3: AppleTalk Basic Parameters

Function	Parameter
Auto Enable	specifies the initialization state
AARP Mapping Table	allocates memory for the address resolution table
Routing Table Size	allocates memory for the routing table

You set AppleTalk basic parameters from the Configuration Menu. Enter the number that appears to the left of **AppleTalk Router** at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]` to display the AppleTalk Basic Parameters Screen.

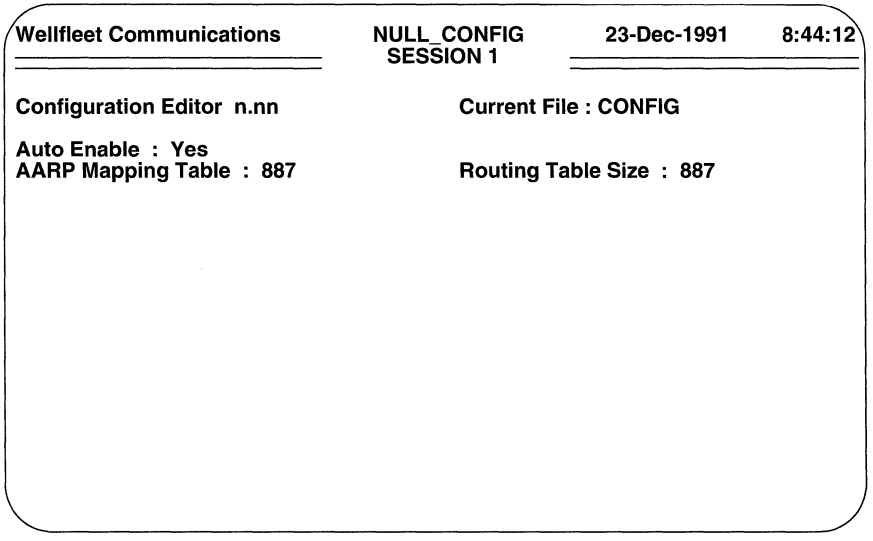


Figure 14-3 AppleTalk Basic Parameters Screen

- **Auto Enable** specifies the initial state of the AppleTalk router.

  The AppleTalk-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable AppleTalk.

  When global auto enable is **No**, AppleTalk is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable AppleTalk with NCL commands after the router boots.

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

- **AARP Mapping Table** allocates memory for the AppleTalk address resolution mapping table.

  Estimate the number of directly connected end-nodes potentially reachable by AppleTalk. Select the next highest number from the available responses.

- **Routing Table Size** allocates memory for the AppleTalk routing table. The routing table lists network numbers, the distance (in hops) to the network, the port to the next hop router (or to a directly connected network), the address of the next hop router, and a route entry state (good, bad, or suspect).

  Estimate the number of networks potentially reachable through AppleTalk. Select the next highest number from the available responses.

After you specify the size of the routing table, the screen displays the AppleTalk Detailed Parameters Access Screen (Figure 14-4).

14.3 Defining an AppleTalk Circuit Group

When you define AppleTalk circuit groups, you describe the connections between the AppleTalk router and its neighboring networks, routers, or backbone networks. Such connections are referred to as *ports* in Apple terminology. These connections are described by a parameter sequence (a *port descriptor*) that specifies, among other attributes, the port number, the router's port-specific node identifier, and the network number to which the port is connected. Some of these parameters are dynamically supplied by the AppleTalk router; others must be explicitly configured.

You define AppleTalk circuit groups/ports from the AppleTalk Detailed Parameters Access Screen. 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 AppleTalk Circuit Group Parameters Screen (Figure 14-5).

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

Configuration Editor  n.nn                  Current File : CONFIG

Auto Enable : <xxx>
AARP Mapping Table : <xxxx>                 Routing Table Size : <xxxx>


1. Lists (0)
2. Circuit Groups (0)


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

Figure 14-4 AppleTalk Detailed Parameters Access Screen

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

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Group Name : _____________

Probe : Yes                                 Checksum : No
Node ID : 0                                 Source Route (Token Ring) : No
Seed Router : No
```

Figure 14-5 AppleTalk Circuit Group Parameters Screen

- **Circuit Group Name** identifies the circuit group that connects the router to the neighboring network, router, or backbone network.

  Enter the name of the circuit group.

- **Probe** works in conjunction with the **Node ID** and, in the case of seed routers, **Network** parameters to enable or disable the generation of AARP *Probe* packets and their subsequent transmission across **Circuit Group Name**.

NOTE

You should enable *Probe*, even if you plan to assign an explicit node identifier. Enabling *Probe* guards against duplicate AppleTalk addresses.

If **Circuit Group Name** supports a non-seed AppleTalk router, you can disable *Probe* only if you explicitly assign a node identifier. If you choose not to assign a node identifier (thus leaving it to the AppleTalk router to generate a random identifier), *Probe* is forced regardless of the value you assign to the **Probe** parameter.

Node ID	Probe	*Probe* Implemented?
assigned	disabled	No
unassigned	disabled	Yes
--------	enabled	Yes

If **Circuit Group Name** supports a seed AppleTalk router, you can disable *Probe* only if you explicitly assign a node identifier and a network number. If you choose not to assign a node identifier and a network number, *Probe* is forced regardless of the value you assign to the **Probe** parameter.

Node ID	Network	Probe	*Probe* Implemented?
assigned	assigned	disabled	No
assigned	unassigned	disabled	Yes
unassigned	assigned	disabled	Yes
unassigned	unassigned	disabled	Yes
--------	--------	enabled	Yes

Select **Yes** to enable the generation of *Probe* packets or **No** to conditionally disable the generation of *Probe* packets.

- **Checksum** enables or disables the calculation of the DDP checksum for datagrams originated by the AppleTalk router.

  AppleTalk provides the option to include a 16-bit checksum in the header of DDP packets. With checksumming enabled, the AppleTalk router calculates and writes a checksum to the header of any DDP datagram originated by the AppleTalk router. With checksumming disabled, the AppleTalk router does not calculate a checksum, and writes a value of 0 to the DDP packet header.

  Checksum has no effect upon incoming packets. If the AppleTalk router receives a packet containing a checksum, it verifies the checksum value.

  Select **Yes** (to enable checksumming) or **No** (to disable checksumming).

- **Node ID** specifies the circuit group/port-specific node identifier portion of the AppleTalk address.

  The AppleTalk routers uses multiple AppleTalk addresses (one address for each network to which the router is directly connected). The AppleTalk address (the network number, node identifier pair) must be unique for each node.

  You can explicitly assign a node identification (within the range 1 to 253), or you can allow the AppleTalk router to generate its own node identifier. Regardless of the method used, it is strongly recommended that you enable AARP *Probe* to ensure a unique node identifier.

  To assign an explicit node identifier, enter a decimal value from 1 to 253. To enable router generation of the node identifier, press `[RETURN]`.

- **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 end station. Such a peer relationship enables a transition between source route bridging and AppleTalk routing environments and allows the AppleTalk 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 AppleTalk 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]`.

- **Seed Router** specifies whether the AppleTalk router is a seed or non-seed router for the network to which it is attached.

  A *seed router* is a router whose port descriptor includes a network range and default zone name (and possibly an optional zone name list). All AppleTalk routers need not be configured as seed routers.

In the case of a network serviced by multiple AppleTalk routers, only a single router need be configured as the seed. The other AppleTalk routers servicing the network can be configured as nonseed routers. Nonseed routers will acquire the correct network information (network range and zone names) by receiving RTMP *Data* and ZIP packets transmitted by the seed router.

In the case of a network serviced by a single AppleTalk router, the router must be configured as a seed router.

Select **Yes** (to designate the router as a seed router) or **No** (to designate the router as a non-seed router).

If you do not designate the router as a seed router, 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
Circuit Group Name  : _____________

Probe  : <xxx>                              Checksum  : <xxx>
Node ID  : <xxx>                            Source Route (Token Ring)  : <xxx>
Seed Router  : No


1.  Traffic Filters (0)



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

Figure 14-6 AppleTalk Filters Access Screen

To configure circuit-group-specific filters, proceed to Section 14.5, *Compiling AppleTalk Filter Lists*, and Section 14.6, *Configuring AppleTalk Filters*. If you do not want to configure filters enter **<0>** at **Enter Selection (0 for Previous Display)** to return to the AppleTalk Detailed Parameters Access Screen. Now proceed to Section 14.4, *Defining Additional AppleTalk Circuit Groups*.

If you designate the AppleTalk router as a seed router, the screen displays the AppleTalk Seed Router Configuration Screen (Figure 14-7) to prompt for additional parameter values.

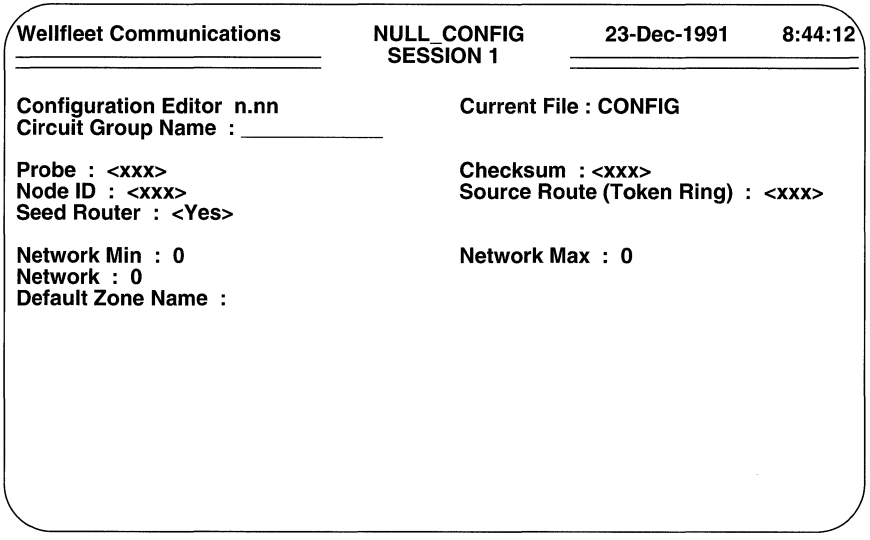


Figure 14-7 AppleTalk Seed Router Configuration Screen

- **Network Min** (in conjunction with **Network Max**) specifies the range of network numbers available to nodes on the directly-connected network.

  In order to increase the number of nodes that can reside on a local network medium, AppleTalk Phase 2 mandates that the seed router provide a range of network numbers which are then made available to nodes. Nodes can then randomly generate a network number (from within the provided range) just as they randomly generate a node identifier.

  Enter the lower boundary of the network range (from 1 to 65279).

- **Network Max** (in conjunction with **Network Min**) specifies the range of network numbers available to nodes on the directly-connected network.

  Enter the upper boundary of the network range (from 1 to 65279).

- **Network** specifies the circuit group/port-specific network number.

  Network assigns the network number to the seed port. To explicitly assign the network number, enter a value equal to or greater than **Network Min** and equal to or less than **Network Max**. To have the AppleTalk router assign a random network number (within the range bounded by **Network Min** and **Network Max**), press `[RETURN]`.

- **Default Zone Name** assigns the AppleTalk router to a zone.

  A zone is a logical grouping of network devices. Such a logical grouping can be confined to a single network or span multiple networks.

  Each zone is identified by a zone name. A zone name consists of a maximum of 32 characters and can include any keyboard-generated character (except for the tilde, ~) or characters from the AppleTalk character set. These special characters are represented as follows:

  \xx

  Where \ is the backslash character and **xx** is the 2-digit hexadecimal value that identifies the special AppleTalk character. For example, to use the zone name "ΔΣπ", enter the following string:

  \c6\b7\b9

  Where c6, b7 and b9 are the hexadecimal values of the AppleTalk characters Δ, Σ, and π, respectively.

  The backslash character (\) can be used in the zone name if you precede it with another backslash. For example, to use the zone name "Bldg1\1st-floor", enter the following string:

  Bldg1\\1st-floor

NOTE

The 32-character limit applies to the zone name as it is entered. When you compute the zone name length, count each AppleTalk character as three characters and each escaped backspace character as 2 characters.

After you assign the default zone name, the screen displays the AppleTalk Seed Router Detailed Parameters Access Screen (Figure 14-8) to prompt for a list of zone names.

In contrast with the mandatory default zone name, the zone name list is optional. If you do not want to construct a zone name list, nor do you want to configure circuit-group-specific filters, enter **<0>** at **Enter Selection (0 for Previous Menu)** and then press **[RETURN]** to return to the AppleTalk Detailed Parameters Access Screen. If you do not want to construct a zone name list, but do want to configure circuit-group-specific filters, proceed to Section 14.5, *Compiling AppleTalk Filter Lists*, and Section 14.6, *Configuring Filters*.

If you do wish to construct a zone name list, enter **<1>** at **Enter Selection (0 for Previous Menu)**, and then press **[RETURN]**. The screen displays the following:

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

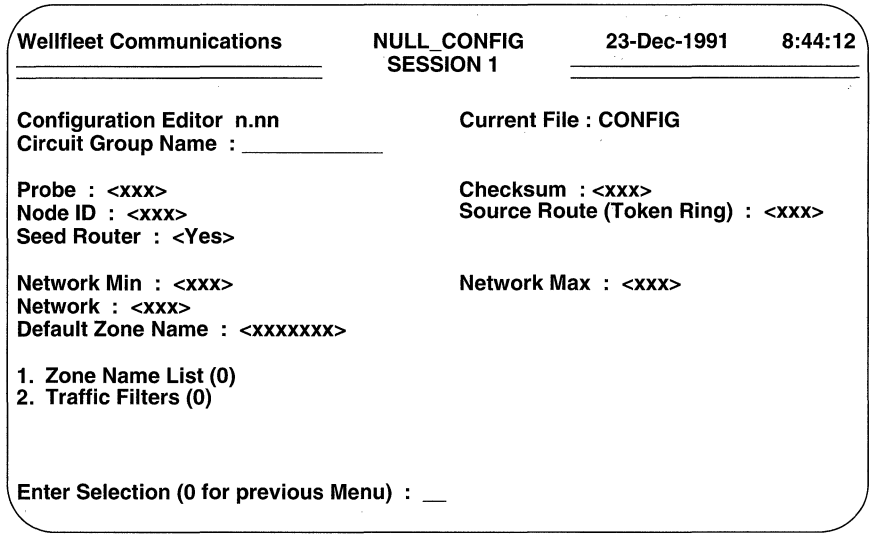


Figure 14-8 AppleTalk Seed Router Detailed Parameters Access Screen

Press `[RETURN]` to display the AppleTalk Zone Name List Screen (Figure 14-9).

At **Zone Name**, enter the name of a zone on the directly-connected network. The screen prompts **Hit Return to Continue**. After you do so, the screen displays the AppleTalk Seed Router Detailed Parameters Access Screen.

You can add additional zone names (up to a maximum of 10) from the AppleTalk Zone Name List Access Screen. To add a zone, enter `<1>` at **Enter Selection (0 for Previous Menu)**, and then press `[RETURN]`. The screen displays the AppleTalk Zone Summary Screen (Figure 14-10).

To add another zone name, at **Action (-> for Selections)** press the `[RIGHTARROW]` to display **Add**, and then press `[RETURN]`. The screen displays the AppleTalk Seed Router Detailed Parameters Access Screen from which you can add an additional zone. Continue in this manner until you have listed up to 10 zones (not counting the mandatory default zone) on the directly-connected AppleTalk medium.

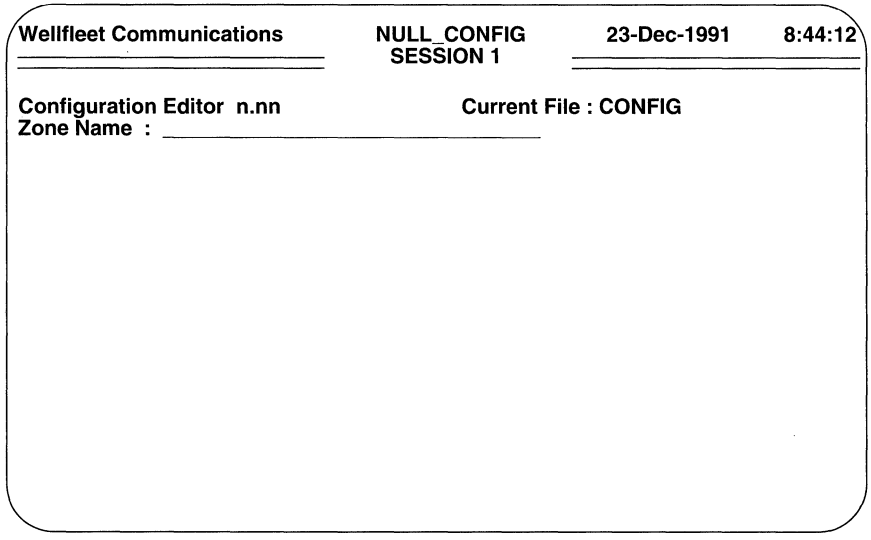


Figure 14-9 AppleTalk Zone Name List Screen

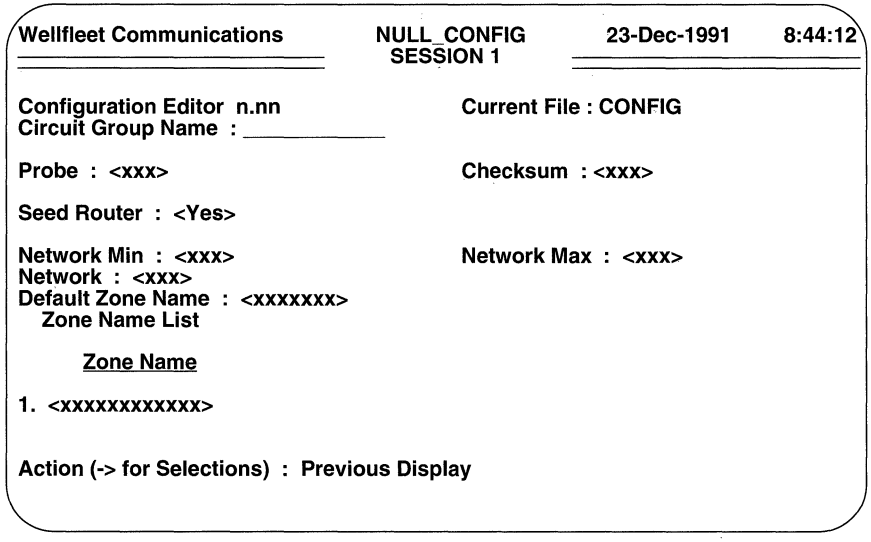


Figure 14-10 AppleTalk Zone Summary Screen

14.4 Defining Additional AppleTalk Circuit Groups

You define additional AppleTalk circuit groups from the AppleTalk Detailed Parameters Access Screen. Enter **<2>** at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Circuit Group Summary Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG

Auto Enable  : <xxx>
AARP Mapping Table  : <xxx>                 Routing Table Size  : <xxx>

      Circuit Groups
   Circuit Group Name

1. <xxxxxxx>

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

Figure 14-11 AppleTalk Circuit Groups Summary Screen

To define an additional AppleTalk circuit group press the **[RIGHTARROW]** to display **Add**, and then press **[RETURN]**. The screen displays the AppleTalk Circuit Group Parameters Screen. Now follow the same procedure as before to define an additional circuit group. Continue until you have defined all AppleTalk circuit groups.

14.5 Compiling AppleTalk 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 AppleTalk Detailed Parameters Access Screen. Enter **<1>** at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

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

Press [RETURN] to display the AppleTalk List Access Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


1. Network Lists (0)
2. Node  Lists (0)
3. Socket Lists (0)
4. DDP Type Lists (0)


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

Figure 14-12 AppleTalk List Access Screen

14.5.1 Network Lists

Network lists specify ranges of AppleTalk network numbers.

You construct a network list from the AppleTalk List Access Screen. Enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press [RETURN] to accept the default response. The screen prompts for a **List Name**.

- **List Name** identifies the network list.

  Enter a list name.

After you name the network list, the screen prompts for list members (Figure 14-13).

To assign a range of AppleTalk network numbers to the list, enter <1> at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press [RETURN] to display the AppleTalk Network Range Screen (Figure 14-14).

```
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 14-13 AppleTalk List Member Access Screen

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

Configuration Editor  n.nn                  Current File : CONFIG

Network  (low)  :
Network  (high) :
```

Figure 14-14 AppleTalk Network Range Screen

- **Network (low)** specifies the lower boundary of the network range.

  Enter an AppleTalk network number.

- **Network (high)** specifies the upper boundary of the network range.

  Enter an AppleTalk network number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Network (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the AppleTalk List Member Access Screen.

If you want, you can add other network ranges to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the AppleTalk Network 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
   Network Number (low)                 Network Number (high)

1. <xxxxxxxxxxxx>                       <xxxxxxxxxxxx>

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

Figure 14-15 AppleTalk Network List Members Screen

To add another range of network numbers press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the AppleTalk Network Range Screen. Now follow the same procedure as before to add another network number range; continue in this fashion until you have added all desired ranges to the list.

You compile additional network lists from the AppleTalk List Access Screen. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Network List Summary Screen (Figure 4-16).

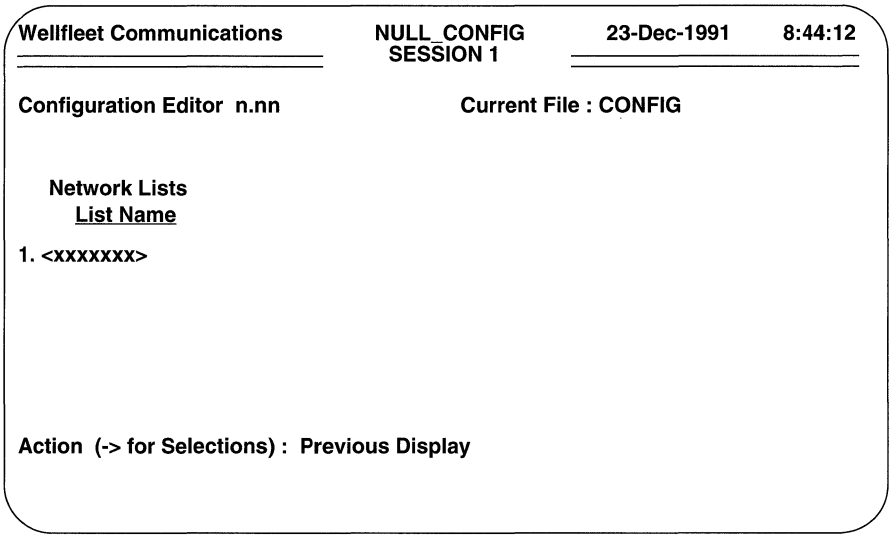


Figure 14-16 AppleTalk Network List Summary Screen

To compile another network 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 network lists.

14.5.2 Node Lists

Node lists specify ranges of AppleTalk node identifiers.

You construct a node list from the AppleTalk List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press `[RETURN]` to accept the default. The screen prompts for a **List Name**.

- **List Name** identifies the node list.

  Enter a list name.

After you name the node list, the screen prompts for list members.

To assign a range of AppleTalk nodes to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press [RETURN] to display the AppleTalk Node Range Screen.

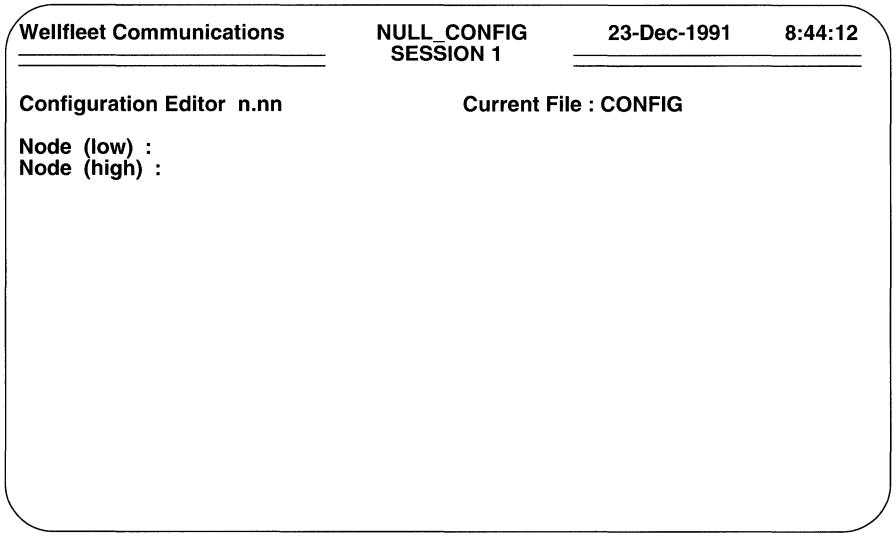


Figure 14-17 AppleTalk Node Range Screen

- **Node (low)** specifies the lower boundary of the node identification range.

  Enter an AppleTalk node identifier.

- **Node (high)** specifies the upper boundary of the node identification range.

  Enter an AppleTalk node identifier, and then press [RETURN]. If you want the list range to consist of a single value, that entered in response to the **Node (low)** parameter, press [RETURN].

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press [RETURN] to go back to the AppleTalk List Member Access Screen.

If you want, you can add other AppleTalk node ranges to the list. To add an additional range, enter <1> at the **Enter Selection (0 for Previous Menu)** prompt to display the AppleTalk Node List Members Screen (Figure 14-18). To add another range of nodes press the [RIGHTARROW] to display **Add** and then press [RETURN].

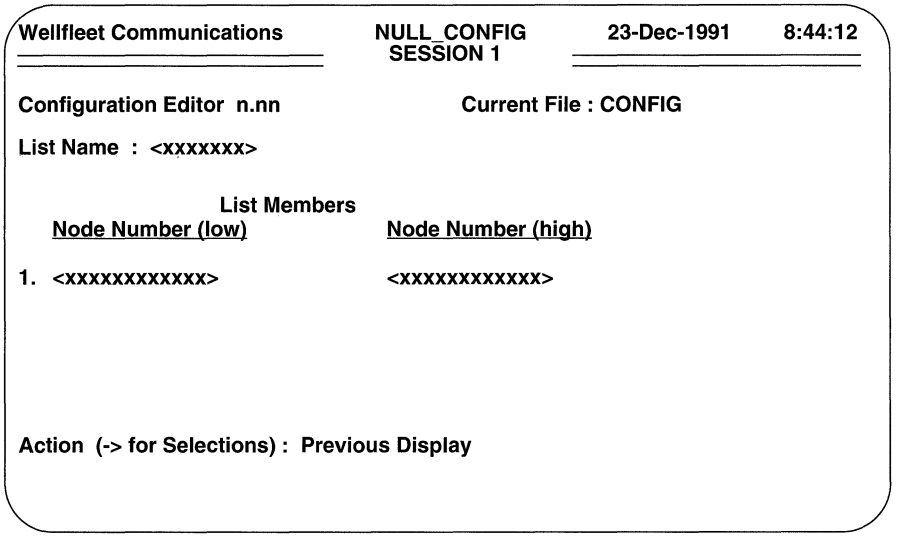


Figure 14-18 AppleTalk Node List Members Screen

The screen displays the AppleTalk Node Range Screen. Now follow the same procedure as before to add another node range; continue in this fashion until you have added all desired ranges to the list.

You construct additional node lists from the AppleTalk List Access Screen. To begin, enter <2> at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Node List Summary Screen (Figure 14-19.

To compile another node list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the previously described procedure to compile an additional node list; repeat this procedure until you have compiled all node lists.

14.5.3 Socket Lists

Socket lists specify ranges of AppleTalk socket numbers.

You construct a socket list from the AppleTalk List Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

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

Press [RETURN] to accept the default. The screen prompts for a **List Name**.

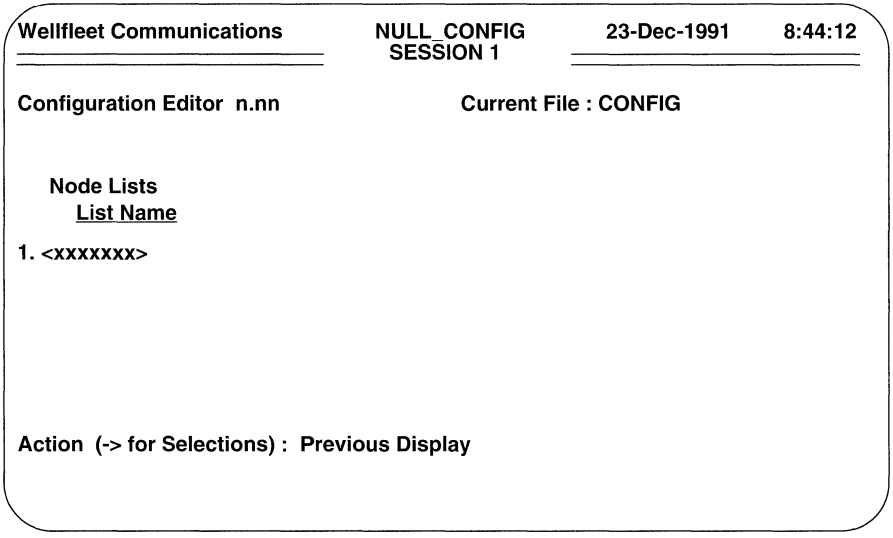


Figure 14-19 AppleTalk Node List Summary Screen

- **List Name** identifies the socket list.

  Enter a list name.

After you name the socket list, the screen prompts for list members.

To assign a range of AppleTalk sockets to the list, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

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

Press `[RETURN]` to display the AppleTalk Socket Range Screen (Figure 14-19).

- **Socket (low)** specifies the lower boundary of the socket range.

  Enter an AppleTalk socket number.

- **Socket (high)** specifies the upper boundary of the socket range.

  Enter an AppleTalk socket number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **Socket (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the AppleTalk List Member Access Screen.

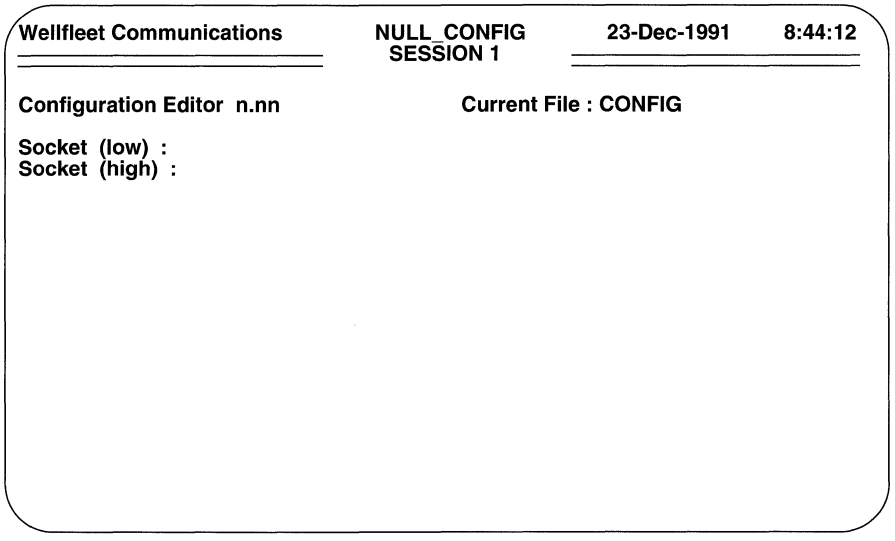


Figure 14-20 AppleTalk Socket Range Screen

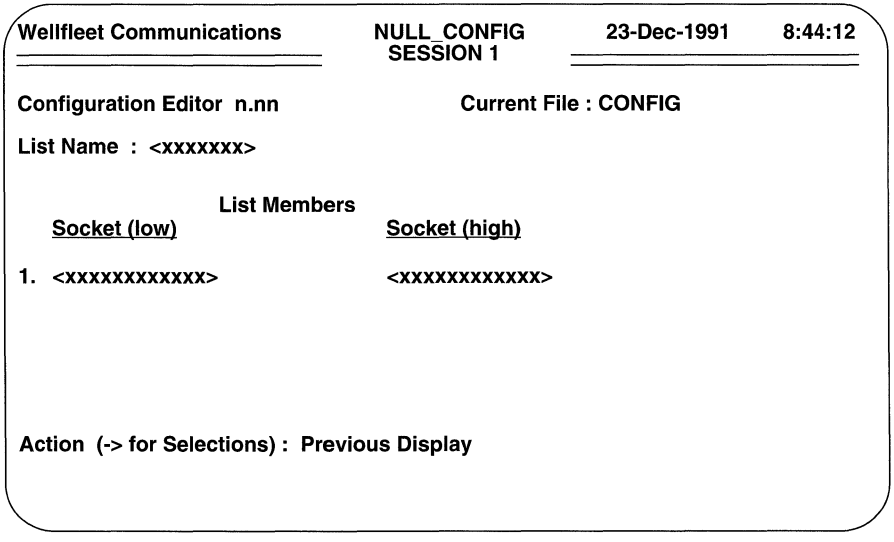


Figure 14-21 AppleTalk Socket List Members Screen

If you want, you can add other socket ranges to the list. To add an additional range, enter <1> at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Socket List Members Screen (Figure 14-21).

To add another range of socket numbers press the [RIGHTARROW] to display **Add** and then press [RETURN] to display the AppleTalk Socket Range Screen. Now follow the same procedure as before to add another socket range; continue in this fashion until you have added all desired ranges to the list.

You compile additional socket lists from the AppleTalk List Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Socket List Summary Screen.

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

Configuration Editor  n.nn                  Current File : CONFIG


   Socket Lists
      List Name

1. <xxxxxxx>




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

Figure 14-22 AppleTalk Socket List Summary Screen

To compile another AppleTalk socket list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the previously described procedure to compile an additional socket list; repeat this procedure until you have compiled all socket lists.

14.5.4 DDP Type Lists

DDP Type lists specify ranges of DDP packet types.

You construct a DDP Type list from the AppleTalk List Access Screen. Enter <4> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No DDP Type Lists record(s) found
Do you wish to add DDP Type Lists record(s)?

Press `[RETURN]`. The screen prompts for a **List Name**.

- **List Name** identifies the DDP Type list.

  Enter a list name.

After you name the DDP Type list, the screen prompts for list members.

To assign a range of DDP protocol types to the list, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays:

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

Press `[RETURN]` to display the AppleTalk DDP Type Range Screen.

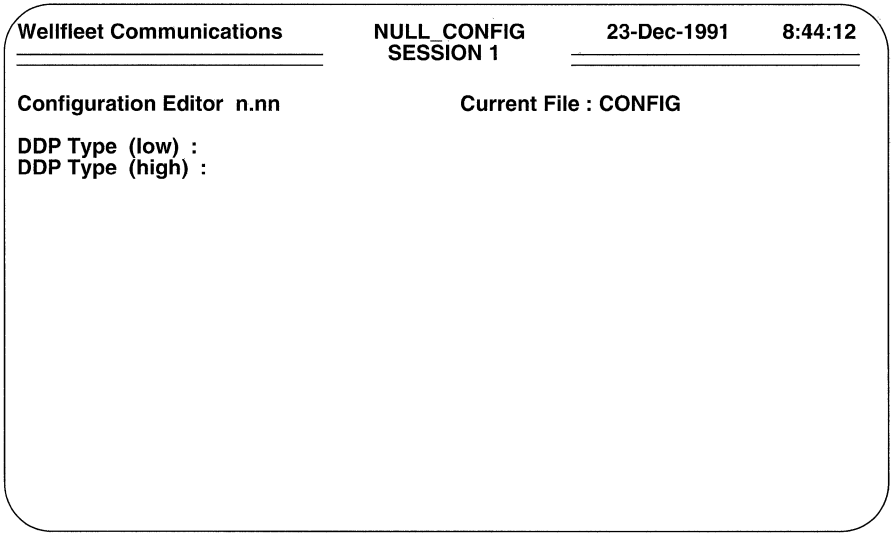


Figure 14-23 AppleTalk DDP Type Range Screen

- **DDP Type (low)** specifies the lower boundary of the DDP protocol type range.

  Enter an AppleTalk packet type number.

- **DDP Type (high)** specifies the upper boundary of the DDP protocol type range.

Enter an AppleTalk DDP type number, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **DDP Type (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the AppleTalk List Member Access Screen.

If you want, you can add other DDP type ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the AppleTalk DDP Type List Members Screen. To add another range of DDP type numbers press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`.

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

Configuration Editor  n.nn                    Current File : CONFIG

List Name  : <xxxxxxx>

                        List Members
   DDP Type (low)                    DDP Type (high)

1. <xxxxxxxxxxxx>                    <xxxxxxxxxxxx>




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

Figure 14-24 AppleTalk DDP Type List Members Screen

The screen displays the AppleTalk DDP Type Range Screen. Now follow the same procedure as before to add another DDP type range; continue in this fashion until you have added all desired ranges to the list.

You compile additional DDP type lists from the AppleTalk List Access Screen. To begin, enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the AppleTalk DDP Type List Summary Screen (Figure 14-25).

To compile another DDP type list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional DDP type list; repeat this procedure until you have compiled all DDP type lists.

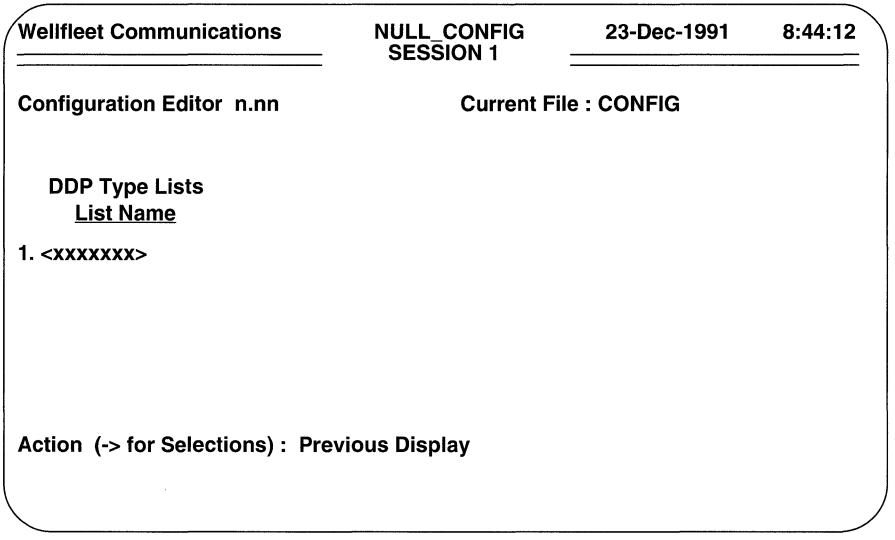


Figure 14-25 AppleTalk DDP Type List Summary Screen

14.6 Configuring AppleTalk Filters

AppleTalk filters apply to all in-coming AppleTalk traffic across the circuit group. You can, if you wish, construct up to 31 filters for each AppleTalk circuit group. You configure circuit-group-specific AppleTalk traffic filters from the AppleTalk Filters Access Screen (Figure 14-6) or from the AppleTalk Seed Router Detailed Parameters Access Screen (Figure 14-8). To begin, enter the number that appears to the left of **Traffic Filters** at **Enter Selection (0 for Previous Display)**. 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 AppleTalk Filters Rule Screen (Figure 14-26).

- **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

  You can construct up to 31 filters per circuit group. The **Precedence** value is used when an in-coming packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

  Press the `[RIGHTARROW]` to select a value from 1 to 31 and then press `[RETURN]`.

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

Configuration Editor  n.nn                  Current File : CONFIG

Precedence : 1
Dest Net (low) :                (high) :          Effect : Ignore
Dest Node (low) :               (high) :          Effect : Ignore
Dest Sock (low) :               (high) :          Effect : Ignore
Source Net  (low) :             (high) :          Effect : Ignore
Source Node (low) :             (high) :          Effect : Ignore
Source Sock (low)               (high) :          Effect : Ignore
DDP Type (low) :                (high) :          Effect : Ignore
Action : Drop
```

Figure 14-26 AppleTalk Filters Rule Screen

NOTE

In the event of two filters with equal precedence, the first configured filter takes precedence.

- **Dest Net (low)** specifies the lower boundary range of filtered destination networks.

  If you do not want to filter destination networks, press `[RETURN]`.

  To filter destination networks, do one of the following:

  - enter the name of a network list
  - enter a network number at the lower boundary of the destination network range
  - enter a single destination network number

- **(high)** specifies the upper boundary range of filtered destination networks.

  If you do not want to filter destination networks, press `[RETURN]`.

  To filter destination networks, do one of the following:

  - if you entered the name of a network list at **Dest Net (low)**, or if you want to filter the single network specified at **Dest Net (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **Dest Net (low)**, enter a network number 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 pattern specified by **Dest Net (low)** and **(high)**.

If the filter does not care about destination network values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination networks, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Net (low)** and **(high)** includes the destination network field of the AppleTalk DDP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Net (low)** and **(high)** does not include the destination network field of the AppleTalk DDP datagram.

❒ **Dest Node (low)** specifies the lower boundary range of filtered destination nodes.

If you do not want to filter destination nodes, press `[RETURN]`.

To filter AppleTalk destination nodes, do one of the following:

- enter the name of a node list
- enter a node number at the lower boundary of the destination node range
- enter a single destination node number

❒ **(high)** specifies the upper boundary range of filtered destination nodes.

If you do not want to filter AppleTalk destination nodes, press `[RETURN]`.

To filter destination nodes, do one of the following:

- if you entered the name of a node list at **Dest Node (low)**, or if you want to filter the single node specified at **Dest Node (low)** press `[RETURN]`.
- if you entered a lower boundary range value at **Dest Node (low)**, enter a node number 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 pattern specified by **Dest Node (low)** and **(high)**.

If the filter does not care about destination node values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination nodes, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Node (low)** and **(high)** includes the destination node field of the AppleTalk DDP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Node (low)** and **(high)** does not include the destination node field of the AppleTalk DDP datagram.

❒ **Dest Sock (low)** specifies the lower boundary range of filtered destination sockets.

If you do not want to filter destination sockets, press **[RETURN]**.

To filter destination sockets, do one of the following:

- enter the name of a socket list
- enter a socket number at the lower boundary of the destination socket range
- enter a single destination socket number

❒ **(high)** specifies the upper boundary range of filtered destination sockets.

If you do not want to filter destination sockets, press **[RETURN]**.

To filter destination sockets, do one of the following:

- if you entered the name of a socket list at **Dest Sock (low)**, or if you want to filter the single socket specified at **Dest Sock (low)**, press **[RETURN]**.
- if you entered a lower boundary range value at **Dest Sock (low)**, enter a socket number 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 pattern specified by **Dest Sock (low)** and **(high)**.

If the filter does not care about destination socket values, press **[RETURN]** to accept the default, **Ignore**.

To filter destination sockets, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Sock (low)** and **(high)** includes the destination socket field of the AppleTalk DDP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Dest Sock (low)** and **(high)** does not include the destination socket field of the AppleTalk DDP datagram.

- **Source Net (low)** specifies the lower boundary range of filtered source networks.

  If you do not want to filter source networks, press `[RETURN]`.

  To filter source networks, do one of the following:

  - enter the name of a network list
  - enter a network number at the lower boundary of the source network range
  - enter a single source network number

- **(high)** specifies the upper boundary range of filtered source networks.

  If you do not want to filter source networks, press `[RETURN]`.

  To filter source networks, do one of the following:

  - if you entered the name of a network list at **Source Net (low)**, or if you want to filter the single source network specified at **Source Net (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Net (low)**, enter a network number 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 pattern specified by **Source Net (low)** and **(high)**.

  If the filter does not care about source network values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source networks, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Net (low)** and **(high)** includes the source network field of the AppleTalk DDP datagram.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Net (low)** and **(high)** does not include the source network field of the AppleTalk DDP datagram.

- **Source Node (low)** specifies the lower boundary range of filtered source nodes.

  If you do not want to filter source nodes, press `[RETURN]`.

  To filter source nodes, do one of the following:

  - enter the name of a node list
  - enter a node number at the lower boundary of the source node range
  - enter a single source node number

- **(high)** specifies the upper boundary range of filtered source nodes.

  If you do not want to filter source nodes, press `[RETURN]`.

  To filter source nodes, do one of the following:

  - if you entered the name of a node list at **Source Node (low)**, or if you want to filter the single node specified at **Source Node (low)**, press `[RETURN]`.
  - if you entered a lower boundary range value at **Source Node (low)**, enter a node number 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 pattern specified by **Source Node (low)** and **(high)**.

  If the filter does not care about source node values, press `[RETURN]` to accept the default, **Ignore**.

  To filter source nodes, you choose between the **Match** and **Don't Match** operators.

  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Node (low)** and **(high)** includes the source node field of the AppleTalk DDP datagram.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Node (low)** and **(high)** does not include the source node field of the AppleTalk DDP datagram.

- **Source Sock (low)** specifies the lower boundary range of filtered source sockets.

  If you do not want to filter source sockets, press `[RETURN]`.

  To filter source sockets, do one of the following:

  - enter the name of a socket list
  - enter a socket number at the lower boundary of the source socket range
  - enter a single source socket number

- **(high)** specifies the upper boundary range of filtered source sockets.

  If you do not want to filter source sockets, press `[RETURN]`.

  To filter source sockets, do one of the following:

  - if you entered the name of a socket list at **Source Sock (low)**, or if you want to filter the single source socket specified at **Source Sock (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **Source Sock (low)**, enter a socket number 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 host address pattern specified by **Source Sock (low)** and **(high)**.

If the filter does not care about source socket values, press `[RETURN]` to accept the default, **Ignore**.

To filter source sockets, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Sock (low)** and **(high)** includes the source socket field of the AppleTalk DDP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Source Sock (low)** and **(high)** does not include the source socket field of the AppleTalk DDP datagram.

❒ **DDP Type (low)** specifies the lower boundary range of filtered DDP types.

If you do not want to filter DDP types, press `[RETURN]`.

To filter DDP types, do one of the following:

- enter the name of a DDP type list
- enter a DDP type number at the lower boundary of the DDP type range
- enter a single DDP type number

❒ **(high)** specifies the upper boundary range of filtered DDP types.

If you do not want to filter DDP types, press `[RETURN]`.

To filter DDP types, do one of the following:

- if you entered the name of a DDP type list at **DDP Type (low)**, or if you want to filter the single DDP type specified at **DDP Type (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **DDP Type (low)**, enter a DDP type number 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 DDP type pattern specified by **DDP Type (low)** and **(high)**.

If the filter does not care about DDP type values, press `[RETURN]` to accept the default, **Ignore**.

To filter DDP types, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **DDP Type (low)** and **(high)** includes the DDP type field of the AppleTalk DDP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **DDP Type (low)** and **(high)** does not include the packet type field of the AppleTalk DDP datagram.

❒ **Action** specifies the disposition of AppleTalk DDP datagrams that meet the filter rule.

Drop discards a datagram that meets the filter rule; **Drop and Log** discards the datagram and records an event message in the event log; **Accept** relays a datagram that meets the filter rule; **Accept and Log Drop** relays the datagram 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 datagrams. Consequently, the log actions should generally be used only to record anomalous events.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the AppleTalk Filters Access Screen or to the AppleTalk Seed Router Detailed Parameters Access Screen.

You configure additional filters (up to a maximum of 31 per circuit group) from these screens. To begin, enter the number that appears to the left of **Traffic Filters** at **Enter Selection (0 for Previous Menu)** to display the AppleTalk Filters Summary Screen. At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the AppleTalk Filters Rule Screen.

Follow the same procedures as before to define an additional AppleTalk filter; repeat these procedures until you have defined all filters.

15 Implementing *config*

After configuring the application software modules and the SNMP agent software, you are ready to complete the configuration process.

Completing the process consists of the following tasks:

- Saving *config*
- Powering down the multiprotocol router
- Cabling network devices
- Powering up the multiprotocol router

15.1 Saving *config*

You save *config* from the Configuration Menu. At **Enter Selection (0 for Previous Menu)** press **<0>**.

The console displays **Back To Menu?** at the lower left corner of the screen. Press the **[RIGHTARROW]** to display **Save and Exit?,** then press **[RETURN]**. The screen displays:

Save As : CONFIG

To save *config*, press **[RETURN]**.

After saving *config*, you must dismount the system diskette, log off, and power down the router.

You dismount the system diskette and log off from the Main Menu. To access the Main Menu, press the **[RIGHTARROW]** at **Enter Selection (0 for Previous Menu)** to select **Exit without Saving?**, then press **[RETURN]**.

15.2 Powering Down the Multiprotocol Router

At the Main Menu, press **<2>** to access NCL. At the NCL prompt, type **REMOVE**, followed by **[RETURN]** to dismount the system diskette.

After dismounting the diskette, type **EXIT**, followed by **[RETURN]** to go back to the Main Menu. At the Main Menu, enter **<5>** to log off.

After you log off, remove the system diskette from the disk drive. You then power down the router by turning the power switch to OFF, and by unplugging the power cord from the power source.

15.3 Cabling Network Devices

With the power removed, you install cabling for all network devices (LANs, modems, channel banks, T1 switches, and so forth) connected to the router. Ensure that all connections are secure, and are made to the appropriate connector.

15.4 Powering Up the Multiprotocol Router

To restart the router, first verify that the power is switched to OFF. Then plug the power cord into the power source, and turn the power switch to ON. After you apply power, the router runs diagnostic tests as described in the *Installation Guide*. When the router completes power-up diagnostics (indicated by illuminated **POWER**, **RUN**, and **BOOT** LEDs), insert the system diskette in the disk drive.

The red LED on the disk drive and the **BOOT** LED are lit while the router boots with the `config` file. After the router boots, it displays the Main Menu.

A File Management

This appendix tells you how to save, quit, retrieve, examine, and alter *config*. You should also refer to the *Operator's Guide* for descriptions of certain Network Control Language Interpreter commands (COPY, DELETE, DIRECTORY, and TYPE) that assist in file management.

A.1 Saving *config*

When you save *config*, the multiprotocol router writes its contents to the diskette installed in the disk drive. After the router saves the file, it returns you to the Main Menu.

You save *config* from the Configuration Menu. Enter **<0>** at **Enter Selection (0 for Previous Menu)**.

The console displays **Back To Menu?** at the lower left corner of the screen. Press the **[RIGHTARROW]** to display **Save and Exit?**, then press **[RETURN]**. The screen prompts:

Save As : <CONFIG>

To save the file, press **[RETURN]**.

If you wish to change the file name, enter the new name from the keyboard, then press **[RETURN]**.

If you attempt to save a file under an invalid name (more than 8 characters in a file name, or more than 3 characters in a file extension), the screen displays the following:

<filename> - Invalid file name structure
Hit Return to Continue

After you press **[RETURN]**, the screen displays:

Save As : <filename>

It then waits for you to enter a valid file name, followed by **[RETURN]**.

If you attempt to save a file under the name of an existing file, the screen displays the following:

<filename> already exists
Do you wish to overwrite the file?

To overwrite the earlier version, press the [RIGHTARROW] to display **Yes**, then press [RETURN]. If you wish to retain the earlier version, and to save the new file under a different name, press the [RIGHTARROW] to display **No**, then press [RETURN]. The screen displays:

Save As

allowing you to enter a new file name.

A.2 Quitting *config*

When you quit *config*, the router does not write the file's contents to the diskette; it discards all work that you have done on the file during the present editing session. If, however, you are modifying or editing a previously existing file, the router retains the original copy of that file.

You quit *config* from the Configuration Menu. Enter <0> at **Enter Selection (0 for Previous Menu)**.

The console displays **Back To Menu?** at the lower left corner of the screen. To quit *config*, press the [RIGHTARROW] to display **Exit without Saving?**, then press [RETURN]. The screen returns to the Main Menu.

NOTE

The router does not issue a prompt to verify the quit. Because a file cannot be retrieved after quitting, be sure that you do not wish to retain a copy of the file before quitting.

If you wish to quit a file and access another file, press the [RIGHTARROW] to select **Edit another File?**, then press [RETURN]. The screen then quits the active file (without saving it) and displays the Configuration Editor Access Screen, from which you can access another file by typing its name at **Enter File Name**.

A.3 Retrieving *config*

After saving *config*, you subsequently access it from the Configuration Editor Access Screen.

At **Enter File Name**, enter CONFIG. The router reads *config* from the diskette and displays the Configuration Menu, from which you can access *config* by using the procedures described in Sections A.4 or A.5.

A.4 Examining *config*

The Configuration Editor BROWSE command furnishes a series of screens that list configuration parameters and their assigned values.

You access the BROWSE command from the Configuration Menu. At **Enter Selection (0 for Previous Menu)**, enter the number of the menu item you wish to

examine: for example **<1>**, to examine system records. The console displays **Action (-> for Selections)** at the bottom of the screen.

Press the **[RIGHTARROW]** to select **Browse**, then press **[RETURN]**. Because you requested to browse through system records, the screen displays the Sessions Access Screen. If you had specified other records, the screen would have displayed a similar screen for each record type.

The Sessions Access Screen lists the name of the current file (*config*), the system name, and the values you assigned to **Auto Enable**, **Automatic Reboot**, and **Enable Logging**. The display also indicates the number of session records, and enables you to examine values assigned to session parameters.

To examine session parameters, enter **<1>** at **Enter Selection (0 for Previous Menu)**. The screen displays the Sessions Summary Screen. This screen adds session-specific information: namely, **Event Filter Level** and **Session Mode**.

To view a complete display of all session mode parameters, along with their assigned values, press the **[RIGHTARROW]** to select **Browse**, then press **[RETURN]**. At **Enter Selection (0 for Previous Menu)**, enter the number of the session that you wish to examine, then press **[RETURN]**. The screen displays a listing of session-specific parameters and prompts you to **Hit Return To Continue**. When you press **[RETURN]**, the screen redisplays the Sessions Access Screen.

A.5 Altering *config*

Two Configuration Editor commands, MODIFY and DELETE, enable you to alter *config*. Each of these commands is described in the following sections.

A.5.1 MODIFY

You use the Configuration Editor MODIFY command to change *config* file contents. The MODIFY command operates similarly to the BROWSE command. As you did with BROWSE, you access the MODIFY command from the Configuration Menu. At **Enter Selection (0 for Previous Menu)**, enter the number of the menu item you wish to modify: for example **<1>**, to modify system records. The screen displays **Action (-> for Selections)**. Press the **[RIGHTARROW]** to select **Modify**, then press **[RETURN]**. Because you requested to modify system records, the screen displays the Sessions Access Screen. If you had specified other records, the screen would have provided a similar display for each record type.

The cursor is positioned at **System Name,** the first editable field on the screen. If you wish to change the system name, enter a new name from the keyboard, then press **[RETURN]**.

Note that all changes must be completed by pressing **[RETURN]**.

If you wish to retain the current system name, use either the [DOWNARROW] or [RETURN] to move the cursor to the next editable field, **Auto Enable**.

At **Auto Enable**, or at any other field that contains pre-set parameter values from which you select, you use the [RIGHTARROW] to display available options. Proceed through each editable field, using ARROW keys and [RETURN] as summarized below:

[LEFTARROW]	Display optional values
[RIGHTARROW]	Display optional values
[DOWNARROW]	Retain original value, move to next field
[RETURN]	Retain currently displayed value; move to next field

After you proceed through **Enable Logging**, the screen redisplays the Sessions Access Screen.

To begin modifying session parameters, press <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the Sessions Summary Screen. At **Action (-> for selections)**, press the [RIGHTARROW] to display **Modify**, then press [RETURN].

At **Enter Selection (0 for Previous Menu)**, enter the number of the session that you wish to modify, then press [RETURN]. The screen displays a listing of session-specific parameters. Proceed through each parameter, using the ARROW keys and [RETURN] to modify or accept displayed values. After completing the last field, the screen prompts **Hit Return to Continue**. When you press [RETURN], you revert to the Sessions Access Screen.

Now press <0> to return to the Configuration Menu, and follow the procedure described in Section A.1 to save the modified *config* file.

A.5.2 DELETE

You use the Configuration Editor DELETE command to delete *config* file records. As you did with other Configuration Editor commands, you access DELETE from the Configuration Menu.

At **Enter Selection (0 for Previous Menu)**, enter the number of the menu item you wish to delete: for example <2>, to delete software records. The screen displays the Application Software Summary Screen, with the cursor positioned at **Action (-> for Selections)**.

Use the [RIGHTARROW] to select **Delete**, then press [RETURN]. The screen displays **Enter Selection (0 for Previous Menu)**. To delete one of the listed

software records, enter the number of the record, then press **[RETURN]**. The screen displays the following prompt to confirm the delete operation:

You are sure you want to delete?

If you want to continue with the deletion, press the **[RIGHTARROW]** to display **Yes**, then press **[RETURN]**. The router deletes the record, and then returns you to the Configuration Menu. Now follow the procedure described in Section A.1 to save the modified *config* file.

If you want to abort a deletion, press **[RETURN]** to accept the default response, **No**. The router maintains the record and returns you to the Configuration Menu.

B Session Modes

This appendix tells you how to configure printer, disk-logging, and telnet sessions.

B.1 Configuring a Printer Session

During a printer session, output is directed to a hardcopy device. You configure a printer session from the Configuration Menu. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

Action (-> for selections)

Press the `[RIGHTARROW]` to display **Browse**, then press `[RETURN]`. Because you have already configured a user session, the screen displays the Sessions Access Screen.

At **Enter Selection (0 for Previous Menu)**, enter `<1>` to display the Sessions Summary Screen. At **Action (-> for selection)**, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]`. The screen displays the Session Selection Screen.

- **Event Filter Level** specifies which router-generated event messages are sent to the printer.

  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 sent to the printer.

  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 sent to the printer, then press `[RETURN]`.

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

  Select **Printer**.

The screen displays the Printer Session Screen I.

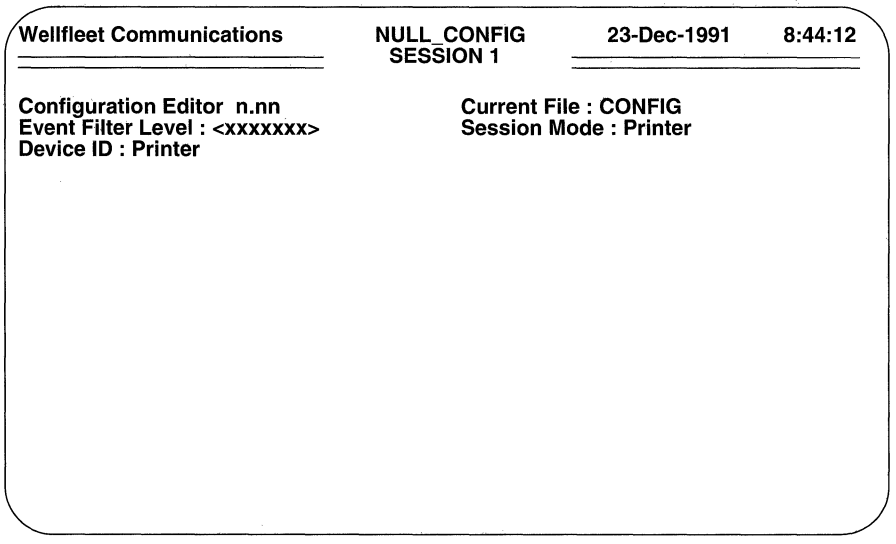


Figure B-1 Printer Session Screen I

- **Device ID** identifies the physical port on the System I/O board to which the printer 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.

NOTE

You can configure up to four user and/or printer sessions (one for each port on the System I/O board). No two sessions, however, can share a common port.

The screen displays the Printer Session Screen II.

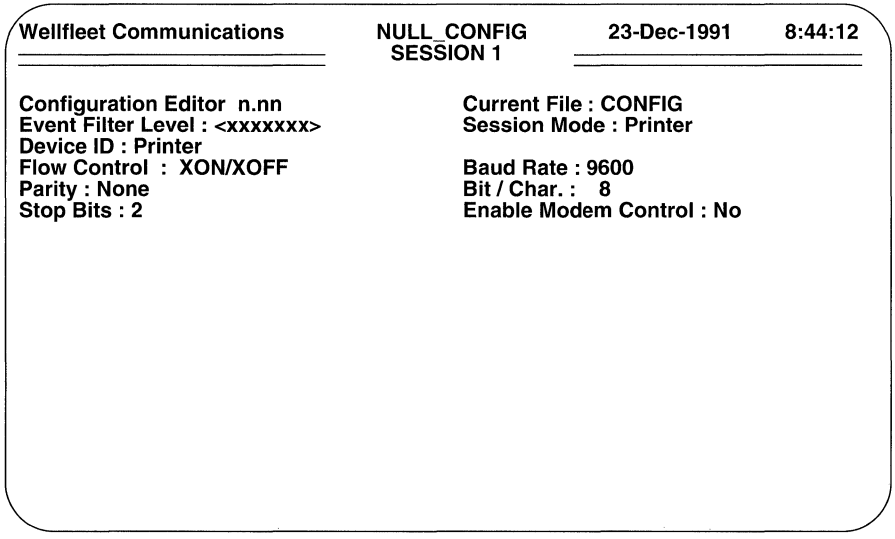


Figure B-2 Printer Session Screen II

- **Flow Control** enables/disables the XON/XOFF protocol, which controls the rate of data transfer between the printer and the node.

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

- **Baud Rate** sets the rate of data transfer between the printer and the node.

  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.

  Set **Parity** to match printer requirements, then press `[RETURN]`.

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

  Set **Bit / Char** to match printer requirements, then press `[RETURN]`.

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

  Set **Stop Bits** to match printer requirements, then press `[RETURN]`.

- **Enable Modem Control** specifies the type of connection between the printer and the router.

  If your printer is connected to the node by a modem, select **Yes**, otherwise, select **No**.

After the screen displays **Hit Return to Continue**, press `[RETURN]` to display the Sessions Access Screen. This screen echoes the values you have previously assigned to the **System Name**, **Auto Enable**, **Automatic Reboot**, and **Enable Logging** parameters.

System Session (n) verifies the creation of multiple session records containing the parameter values you assigned to the printer session and to any other previously configured sessions.

B.2 Configuring a Disk Logging Session

During a disk logging session, output is directed to a disk file. The router supports a single disk logging session. Once created, the session can be disabled with the NCL DISABLE command, and re-enabled with the NCL ENABLE command.

NOTE

The NCL REMOVE command automatically disables disk logging. The NCL INSERT command restores disk logging. Disk logging is also disabled during the operation of the NCL COPY command.

You configure a disk-logging session from the Configuration Menu. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

Action (-> for selections)

Press the `[RIGHTARROW]` to display **Browse**, then press `[RETURN]`. Because you have already configured a user session, the screen displays the Sessions Access Screen.

At **Enter Selection (0 for Previous Menu)**, enter `<1>` to display the Sessions Summary Screen. At **Action (-> for selection)**, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]`. The screen displays the Session Selection Screen.

- **Event Filter Level** specifies which router-generated event messages are logged in the disk file.

  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 sent to the printer.

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 logged, then press `[RETURN]`.

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

  Select **Disk Logging**.

NOTE

If you configure a disk logging session when the **Enable Logging** parameter (refer to Section 2.1) is set to **No**, the router creates the disk logging session, but stores no events in the disk file until the session is enabled with the NCL ENABLE command.

The screen displays the Disk Logging Session Screen (Figure B-3).

- **Log File Name** names the log file.

  Enter the name of the disk file you wish to create, then press `[RETURN]`; or, press `[RETURN]` to accept the default file name, **LOG**.

  If you wish, you can implement a log-file numbering feature that creates up to 10 log files (identified by a sequential numeric suffix, 0 through 9). With this feature enabled, the router creates a new log file each time it is rebooted either with the RESET button or with the NCL BOOT command. Prior to creating the new file, it closes the previous log file, appends a numeric suffix to the file name, and saves the file on the system diskette.

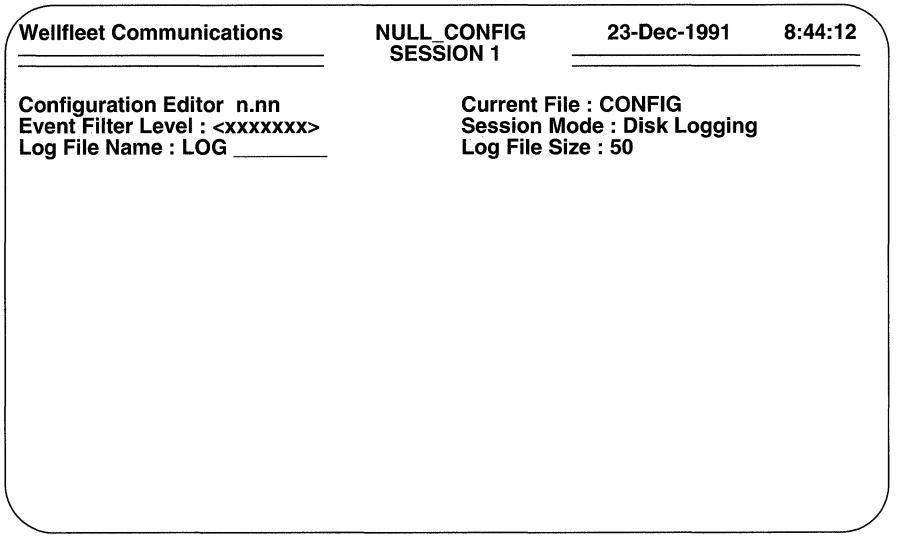


Figure B-3 Disk Logging Session Screen

NOTE

The numeric suffix appended to the file name corresponds to the crash file number. Consequently, the nth log file is logically accompanied by the nth crash file that describes the reason for the reboot.

To implement sequential log files, at **Log File Name** enter a file name in the following format:

```
filename.*   for example, log.*
```

- **Log File Size** specifies the number of event messages contained in the log file. Once this number is exceeded, the oldest file item is overwritten as new items are added.

  Enter the size of the log file (to a maximum of 999), then press `[RETURN]`.

After the screen displays **Hit Return to Continue**, press `[RETURN]` to display the Sessions Summary Screen. This screen echoes the values you previously assigned to the **System Name**, **Auto Enable**, **Automatic Reboot**, and **Enable Logging** parameters.

System Session (n) verifies the creation of multiple session records containing the parameter values you assigned to the disk-logging session and to any other previously configured sessions.

B.3 Configuring aTelnet Session

During a telnet session, you use the TCP/IP TELNET protocol to establish a virtual-terminal connection between the router and a remote device. The TELNET protocol is specified in Internet RFC 854. If you are not familiar with TELNET, you should refer to this RFC. The router supports up to two telnet sessions.

You configure a telnet session from the Configuration Menu. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

Action (-> for selections)

Press the `[RIGHTARROW]` to display **Browse**, then press `[RETURN]`. Because you have already configured a user session, the screen displays the Sessions Access Screen.

At **Enter Selection (0 for Previous Menu)**, enter `<1>` to display the Sessions Summary Screen. At **Action (-> for selection)**, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]`. The screen displays the Session Selection Screen.

- **Event Filter Level** specifies which router-generated event messages are sent to the remote device.

  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 sent to the printer.

  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 sent to the remote device, then press `[RETURN]`.

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

  Select **Telnet**.

The screen displays the Telnet Session Screen.

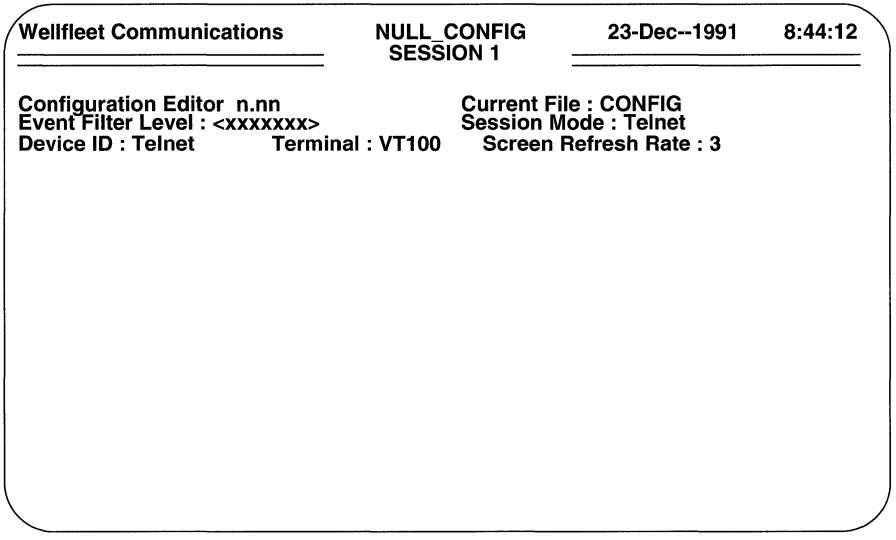


Figure B-4 Telnet Session Screen

- **Device ID** identifies the connection type.

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

- **Terminal** identifies the type of the remote input device.

  If the remote device is a VT100, or a compatible device, press `[RETURN]` to accept the default response, **VT100**. If the remote device is ANSI-compatible, use the `[RIGHTARROW]` to select **ANSI**, then press `[RETURN]`.

- **Screen Refresh Rate** specifies the rate (in seconds per cycle) at which the router 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.

  Before selecting a cycle, you should bear in mind that the frequent update of reporting metrics may cause network congestion and represent an inefficient use of available bandwidth.

  Press the `[RIGHTARROW]` to select a cycle, then press `[RETURN]`.

After the screen displays **Hit Return to Continue**, press `[RETURN]` to display the Sessions Summary Screen. This screen echoes the values you previously assigned to the **System Name**, **Auto Enable**, **Automatic Reboot**, and **Enable Logging** parameters.

System Session (n) verifies the creation of multiple session records containing the parameter values you assigned to the telnet session and to any other previously configured sessions.

Table C-1: Ethernet Line Summary Chart

Physical Access Method	Slot	Connector	Circuit Name
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	

Table C-1: Ethernet Line Summary Chart

Physical Access Method	Slot	Connector	Circuit Name
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	
CSMA/CD		XCVR_	

Table C-2: Synchronous Line Summary Chart

Physical Access Method	Slot	Connector	Signal Mode	Clock Source	Clock Speed	RTS/CTS Control	PPP Support	Frame Relay Interface	SMDS Interface	X.25 Interface	Circuit Name
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									

Table C-2: Synchronous Line Summary Chart

Physical Access Method	Slot	Connector	Signal Mode	Clock Source	Clock Speed	RTS/CTS Control	PPP Support	Frame Relay Interface	SMDS Interface	X.25 Interface	Circuit Name
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									
SYNC		COM_									

Table C-3: T1 Line Summary Chart

Physical Access Method	Slot	Connector	Frame Type	Line Buildout	B8ZS	PPP Support	Frame Relay Interface	X.25 Interface	Circuit 1 Name	Circuit 2 Name
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								
DS1		DS1-_								

Table C-4: E1 Line Summary Chart

Physical Access Method	Slot	Connector	Clock Mode	HDB3 Supported	PPP Supported	Frame Relay interface	X.25 Interface	Circuit 1 Name	Circuit 2 Name
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							
E1		E1-_							

Table C-5: Token Ring Line Summary Chart

Physical Access Method	Slot	Interface Type	Circuit Name
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			
TOKEN RING			

Table C-6: FDDI VME Line Summary Chart

Physical Access Method	Slot	Board Number	Circuit Name
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			

Table C-7: FDDI MODULE Line Summary Chart

Physical Access Method	Slot	Bridge Type	Circuit Name
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			
FDDI			

Table C-8: Ethernet Circuit Summary Chart

Circuit Name	Auto Enable	Quality of Service	Circuit Type	LAN Address	XCVR Polling
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active

Table C-8: Ethernet Circuit Summary Chart

Circuit Name	Auto Enable	Quality of Service	Circuit Type	LAN Address	XCVR Polling
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active
		LLC1	LAN		Active

Table C-9: Point-to-Point Circuit (LLC1) Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	Address	Frame Spacing	Remote Signal & Sense	Protocol
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					
	Point-to-Point	LLC1					

Table C-9: Point-to-Point Circuit (LLC1) Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	Address	Frame Spacing	Remote Signal & Sense	Protocol
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						
	Point-to-Point						

Table C-10: Point-to-Point Circuit (LLC2) Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	N2 Timer	T1 Timer	Connect Retries	T3 Timer	Modulus	Window	Address	Frame Spacing	Remote Signal & Sense	Protocol
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											
	Point-to-Point	LLC2											

Table C-10: Point-to-Point Circuit (LLC2) Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	N2 Timer	T1 Timer	Connect Retries	T3 Timer	Modulus	Window	Address	Frame Spacing	Remote Signal & Sense	Protocol
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												
	Point-to-Point												

Table C-11: Ring Circuit Summary Chart

Circuit Name	Auto Enable	Quality of Service	Circuit Type	LAN Address	XCVR Polling
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active

Table C-11: Ring Circuit Summary Chart

Circuit Name	Auto Enable	Quality of Service	Circuit Type	LAN Address	XCVR Polling
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active
		LLC1	RING		Active

Table C-12: PPP Circuit Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	LQM Time	Link Quality	Frame Spacing	Extended (32-bit) CRC	Max Pkt Size	IP Address	LCP Active Open	LCP Auto Restart	Use UDAP
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										
	PPP	LLC1										

Table C-13: SMDS Circuit Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	Min Frame Spacing	Individual Address	Group Address	ARP Group Address	CRC 16/32-bit	Max Pkt Size	Use SNAP
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								
	SMDS	LLC1								

Table C-14: Frame Relay Circuit Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	DLCI Encoding Type	DLCI Encoding Length	Max Packet Size	Provide InARP	Management Type
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						
	Frame Relay	LLC1						

Table C-15: LAPB Circuit Summary Chart

Circuit Name	Type	Quality of Service	Auto Enable	PDN	T1	N2	Min Frame Spacing	Flow Control	Pkt Window	Pkt Size	SVCs	Service Levels
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										
	LABP	X.25										

Table C-16: X.25 Point-to-Point Virtual Circuit Summary Chart

Circuit Name	Remote DTE Address	Connection ID	Flow Control

Table C-16: X.25 Point-to-Point Virtual Circuit Summary Chart

Circuit Name	Remote DTE Address	Connection ID	Flow Control

D auto config

auto config enables the creation of a "default" system configuration in the absence of an existing configuration file.

D.1 System Requirements

auto config requires a Revision 15 or more recent System Controller installed in Slot 1 of the multiprotocol; earlier revisions of the System Controller do not support auto config.

Operation of auto config is maximized when all ACE boards are at Revision 14 or more recent. Faster diagnostics on these ACE boards allow auto config to learn the complete hardware configuration.

NOTE

Routers which mix Revision 14 ACE boards with pre-Revision 14 ACE boards may not auto-configure properly. If different revisions of ACE boards are installed in a router, put the oldest revision in Slot 2, the master slot.

D.2 auto config Overview

When a router is booted manually (by pressing the **RESET** button) and its system diskette does not contain a file named `config`, the auto config feature creates a "default" `config` that contains physical layer, data-link layer, and circuit group records based on the router's hardware complement. This "default" `config` file also sets global and session-mode parameters, loads the Bridge software to all occupied slots, and configures and disables a minimal transparent bridging functionality.

In a similar fashion, when a router is booted with the NCL BOOT command, and the BOOT command is not accompanied by an argument identifying a specific configuration file, and the router diskette does not contain a file named `config`, the auto config feature creates a "default" `config`.

You can bypass the automatic configuring feature by booting the system from a named configuration file using the BOOT command (refer to the *Operator's Guide* for a description of BOOT command syntax) or by writing a file named `config` to the diskette.

To force auto config, delete or rename *config* and reboot the router.

NOTE

If an error has caused the boot to fail, a zero-length configuration file (named `config`) will be left on the diskette. Delete this file, correct the error condition, and reboot.

D.3 Global and Session Parameters

auto config sets global parameters as listed in Table D-1.

Table D-1: auto config Global Parameter Values

Parameter	auto config Value
System Name	default_config
Automatic Reboot	No
Auto Enable	Yes
Enable Logging	Yes

auto config establishes three sessions: two user mode sessions, and a disk logging mode session. The first user mode session (referred to as the console session) enables direct connection of a console device through the **Console** port on the System I/O board; the second user mode session (referred to as the modem session) enables remote node access through the **Modem1** port on the System I/O board. Session parameters are listed in Tables D-2, D-3, and D-4.

D.4 Loading Software

auto config loads a copy of the Bridge software to each occupied slot.

D.5 Physical Layer Parameters

A physical-access-method-specific line is configured for each connector which exists in the system. Line parameters are listed in Tables D-5 through D-9. Within each table **x** designates a decimal numeral (from 2 to 14, depending on router model) that identifies the backplane slot housing the connector; **y** designates a decimal numeral (from 1 to 4, depending on board type) that identifies the specific physical connector.

NOTE

auto config does not support the configuration of FDDI lines or circuits.

Table D-2: auto config Console Session Parameter Values

Parameter	auto config Value
Event Filter Level	Show All Events
Session Mode	User
Device ID	Console
Terminal	ANSI
Flow Control	XON/XOFF
Baud Rate	9600
Parity	None
Bit / Char	8
Stop Bits	2
Enable Modem Control	No
Screen Refresh Rate	3

Table D-3: auto config Modem Session Parameter Values

Parameter	auto config Value
Event Filter Level	Show All Events
Session Mode	User
Device ID	Modem1
Terminal	ANSI
Flow Control	XON/XOFF
Baud Rate	2400
Parity	None
Bit / Char	8
Stop Bits	2
Enable Modem Control	Yes
Screen Refresh Rate	3

Table D-4: auto config Disk Logging Session Parameter Values

Parameter	auto config Value
Event Filter Level	Show All Events
Session Mode	Disk Logging
Log File Name	LOG
Log File Size	50

Table D-5: auto config Ethernet Line Parameter Values

Parameter	auto config Value
Connector	XCVRy
Circuit Name	Exy

Table D-6: auto config Synchronous Line Parameter Values

Parameter	auto config Value
Connector	COMy
Clock Source	External
Signal Mode	Balanced
Clock Speed	56k
RTS/CTS Control	No
Circuit Name	Sxy

Table D-7: auto config T1 Line Parameter Values

Parameter	auto config Value
Connector	DS1-y
Frame Type	D4
Line Buildout	5
B8ZS Supported	No
Circuit 1 Name	Txy
MiniDACS 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

Table D-8: auto config E1 Line Parameter Values

Parameter	auto config Value
Connector	E1-y
HDB3 Supported	No
Circuit 1 Name	Cxy
MiniDACS Configuration	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

Table D-9: auto config Token Ring Line Parameter Values

Parameter	auto config Value
Ring Interface	4MBs
Circuit Name	Oxy

Circuits are named according to the following convention:

<id><slot><connector>

where:

<id>

Is a unique character that identifies the physical access method: e for Ethernet, s for synchronous, t for T1, c for E1 (CEPT), and o for Token Ring.

<slot>

Is an integer identifying the slot that houses the physical connector.

<connector>

Is an integer that identifies the physical connector.

D.6 Data-Link Layer Parameters

A single circuit is configured for each line. Circuit parameters are listed in Tables D-10 through D-14.

NOTE

auto config supports only a single circuit for T1 and E1 lines.

Table D-10: auto config Ethernet Circuit Parameter Values

Parameter	auto config Value
Auto Enable	Yes
Quality of Service	LLC1
Circuit Type	LAN
XCVR Signal Polling	Active

Table D-11: auto config Synchronous Circuit Parameter Values

Parameter	auto config Value
Auto Enable	Yes
Quality of Service	LLC1
Circuit Type	Point-to-Point
Point-to-Point Address	Explicit
Minimum Frame Spacing	2
Remote Signal and Sense	Active
Data Link Layer Protocol	Standard
Local Address	7
Remote Address	7

Table D-12: auto config T1 Circuit Parameter Values

Parameter	auto config Value
Auto Enable	Yes
Quality of Service	LLC1
Circuit Type	Point-to-Point
Point-to-Point Address	Explicit
Minimum Frame Spacing	2

Table D-12: auto config T1 Circuit Parameter Values

Parameter	auto config Value
Remote Signal and Sense	Active
Data Link Layer Protocol	Standard
Local Address	7
Remote Address	7

Table D-13: auto config E1 Circuit Parameter Values

Parameter	auto config Value
Auto Enable	Yes
Quality of Service	LLC1
Circuit Type	Point-to-Point
Point-to-Point Address	Explicit
Minimum Frame Spacing	2
Remote Signal and Sense	Active
Data Link Layer Protocol	Standard
Local Address	7
Remote Address	7

Table D-14: auto config Token Ring Circuit Parameter Values

Parameter	auto config Value
Auto Enable	Yes
Quality of Service	LLC1
Circuit Type	LAN
Remote Signal and Sense	Active

D.7 Circuit Group Configuration

Circuit groups are configured with a one-to-one mapping to circuits. For example, four circuits translate to four circuit groups with each circuit group consisting of a single member.

Circuit group names consist of the name of the circuit prepended with G_. For example, G_*e21* is the name of the circuit group containing the circuit *e21*.

D.8 Learning Bridge Configuration

The auto config feature configures a minimal transparent bridge functionality; neither spanning tree algorithm nor source routing is enabled. Table D-15 lists bridge global parameters while Table D-16 list circuit-group-specific parameters.

Table D-15: auto config Bridge Parameter Values

Parameter	auto config Value
Auto Enable	No
Spanning Tree Enable	No
Flood Interval	0
Forward Table Size	887
Priority	32768
Max Age	20
Hello Time	2
Forward Delay	4

Table D-16: auto config Bridge Circuit Group Parameter Values

Parameter	auto config Value
Cost	100
Priority	128

E Hardware Configuration

This chapter identifies the physical configuration of jumpers and switches on the printed circuit boards (PCBs) that are currently sold for use in the FN, LN, and CN.

Table E-1 lists the PCBs. The sections that follow this table show illustrations of each board and list the settings of its jumpers and switches. These sections are in order of the part numbers listed in Table E-1. Each section title includes the name of the board, its 4-digit model number, and its 6-digit part number. Before configuring a board, be sure its part number matches the one in the section title. Part numbers are printed on the boards.

Each illustration shows the cable connectors (if applicable) and the component side of the board. The panel of cable connectors in each illustration is upside down in relation to the board so that you can read the connector labels.

The illustration of each board shows the factory-default positions of the jumpers and switches. A table after each illustration shows the option (function) of each jumper/switch, a description of the factory-default setting (if configurable), and the associated jumper/switch position.

The term "not configurable" in the Setting column means that changing the setting could jeopardize the functioning of the board. If an option is user-configurable, alternative settings and associated jumper/switch positions follow the factory-default setting.

The S1 jumper designates the revision of the board (unless otherwise noted). The S1 jumper is *not* user-configurable and is *not* listed in the table of settings for each board. For consistency, the illustrations show the S1 pins jumpered, but the S1 pins on your board may show a different jumper configuration.

Some pins are jumpered on the solder (back) side of the board. These pins are *not* configurable. Also, some pins identified as "not configurable" may not appear on the board, depending on the release of the board.

DANGER

Due to high-energy hazards, only personnel with written authorization from Wellfleet Communications are permitted to service a Wellfleet router. This router contains no user-serviceable parts. Do not attempt to disassemble this product. Do not remove the aluminum Radio-Frequency Interference (RFI) shield or power-supply screens behind the front cover. Do not remove the modules in the rear of the unit.

Table E-1 Wellfleet PCB Boards

Board Type	Board Name	Model Number	Part Number
System Controller	SYSCON	5000	100007
FDDI Controller	FDDI	5912	102232
System I/O	SYS I/O	5010	100013
	SYS I/O	5010	102937
Link Module	CSU	5210	100005
	DSDE 4	5430	102279
	DSE 4	5420	102293
	DST-4/16	5740	101531
	Dual Token Ring	5710	103366
	E1-75	5250	101337
	ENET 2	5405	100809
	ESA 2x0	5505	102495
	ESA 2x2	5530	102494
	Multimode FDDI (with daughter board)	5930 (with 4995)	102675 (with 103269)
	QENET (QENET with High Speed Filter)	5450 (5550)	102690 (102671)
	QSYNC 4	5280	102285
	SSE 4	5410	102296
	T1 2	5200	100831
	T1 2 56K	5201	101667
	T1SGLPORT	5220	101338
	TS416 1x0	5705	102484
	TS416 1x1	5720	102483
	TS416 1x2	5740	102482

Table E-1 Wellfleet PCB Boards

Board Type	Board Name	Model Number	Part Number
Daughter	FDDI Daughter Board for FDDI model 5930	4995	103269 (See 102675 for illustration.)
	QENET High Speed Filter	None. See "Quad ENET (with High Speed Filter)" in this table	102671 (See 102690 for illustration.)
	V.35 DTR	4290	102310

E.1 CSU Board (5210;100005)

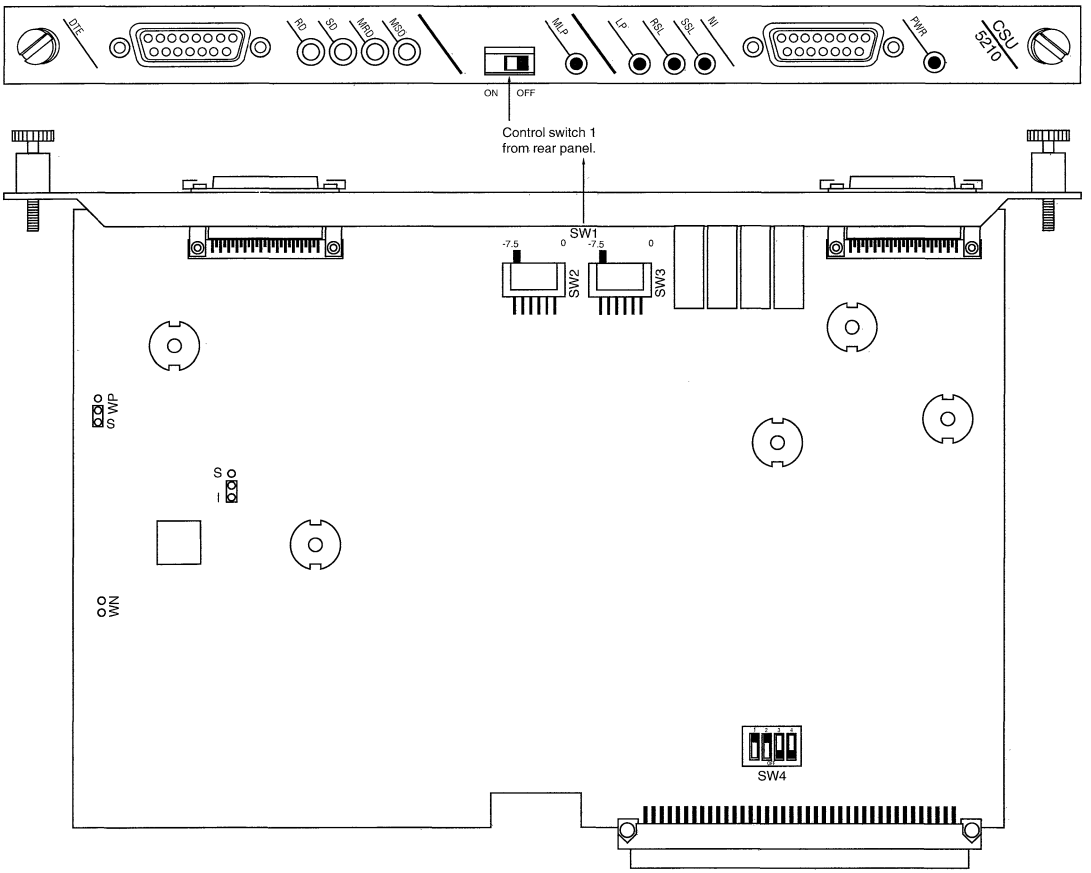


Figure E-1 CSU Board (5210; 100005)

Table E-2 CSU Settings (5210; 100005)

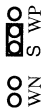
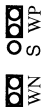
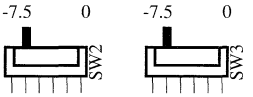
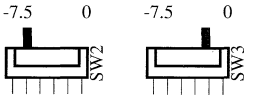
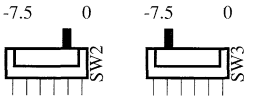
Option	Setting	Jumper or Switch
Power	Local (Internal)	
	Line (Simplex)	
Wet Loop Mode **Note:** The jumpers are at separate locations on the left side of board.)	Off	
	On	
Line Build Out	-15 dB	
	-7.5 dB (Either configuration)	
		

Table E-2 CSU Settings (5210; 100005)

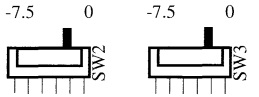
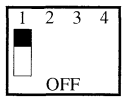
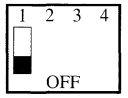
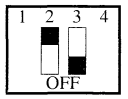
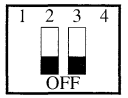
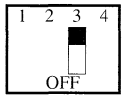
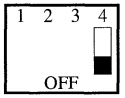
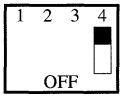
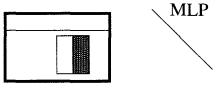
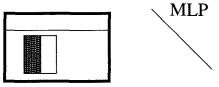
Option	Setting	Jumper or Switch
Line Build Out (continued)	0 dB	
Keep Alive Signal **Note:** The black square indicates the end of the switch that is pressed down.	All 1s	
	Loopback	
Zero Suppression	Enabled, 15-bit suppression	
	Enabled, 8-bit suppression	
	Clear Channel	

Table E-2 CSU Settings (5210; 100005)

Option	Setting	Jumper or Switch
Fault Cap	1 - uf	
	Short	
Manual Loop (Front Panel Switch)	Off	
	On	

E.2 System Controller Board (5000; 100007)

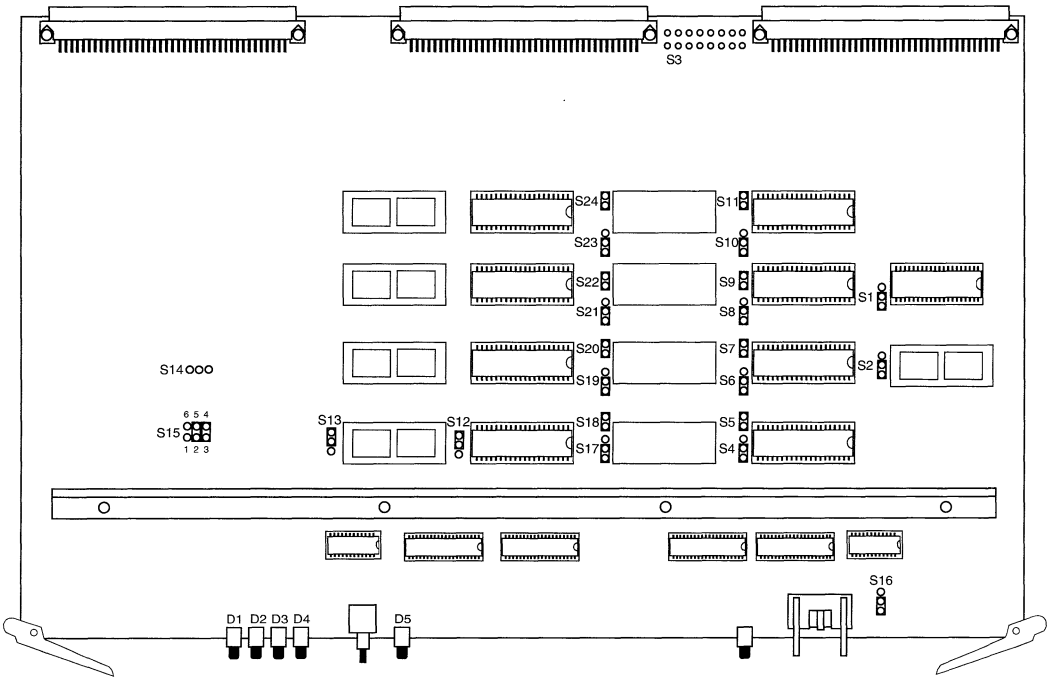


Figure E-2 System Controller Board (5000; 100007)

Table E-3 System Controller Settings (5000; 100007)

Option	Setting	Jumper
Address line for 32-pin NVRAM at U41	Not configurable	S1 3 2 1
Address line for 32-pin NVRAM at U33	Not configurable	S2 3 2 1
Interrupt rector value	Not configurable	S3 16 9 1 8
Address line for 32-pin EPROM at U22	Not configurable	S4
Power for 28-pin EPROM at U22	Not configurable	S5
Address line for 32-pin EPROM at U34	Not configurable	S6
Power for 28-pin EPROM at U34	Not configurable	S7

Table E-3 System Controller Settings (5000; 100007)

Option	Setting	Jumper
Address line for 32-pin EPROM at U42	Not configurable	S8 3 2 1
Power for 28-pin EPROM at U42	Not configurable	S9
Address line for 32-pin EPROM at U53	Not configurable	S10
Power for 28-pin EPROM at U50	Not configurable	S11
Address line for larger SRAM at U24, U36, U44, U55	Not configurable	S12 3 2 1
Address line for larger SRAM at U25, U37, U45, U56	Not configurable	S13 3 2 1
Reserved	Not configurable	S14

Table E-3 System Controller Settings (5000; 100007)

Option	Setting	Jumper
VME deadman time-out	Not configurable	S15 6 5 4 / 1 2 3
Resets when VCC falls below 4.75 V	Not configurable	S16 3 2 1
Address line for 32-pin EPROM at U23	Not configurable	S17 3 2 1
Power for 28-pin EPROM at U23	Not configurable	S18
Address line for 32-pin EPROM at U35	Not configurable	S19 3 2 1
Power for 28-pin EPROM at U35	Not configurable	S20
Address line for 32-pin EPROM at U43	Not configurable	S21 3 2 1

Table E-3 System Controller Settings (5000; 100007)

Option	Setting	Jumper
Power for 28-pin EPROM at U43	Not configurable	S22
Address line for 32-pin EPROM at U54	Not configurable	S23 3 2 1
Power for 28-pin EPROM at U54	Not configurable	S24

E.3 System I/O Board (5010; 100013)

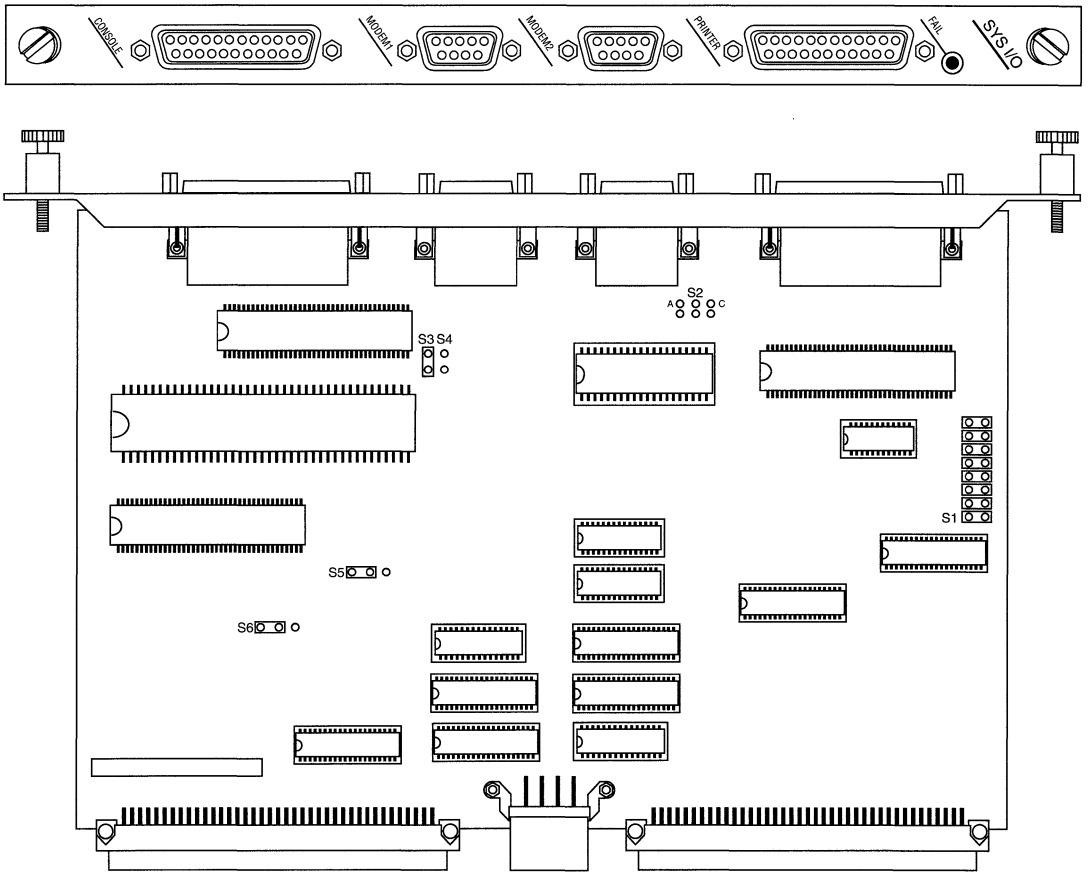
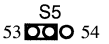


Figure E-3 System I/O Board (5010; 100013)

Table E-4 System I/O Settings (5010; 100013)

Option	Setting	Jumper
Board Option	Not configurable	
8 MHz operation of UART **Note:** S3 jumper is hard-wired behind the board.	Not configurable	
Type of floppy drive **Note:** S5 and S6 appear in separate locations on the board.	Not configurable	 

E.4 ENET 2 Board (5405; 100809)

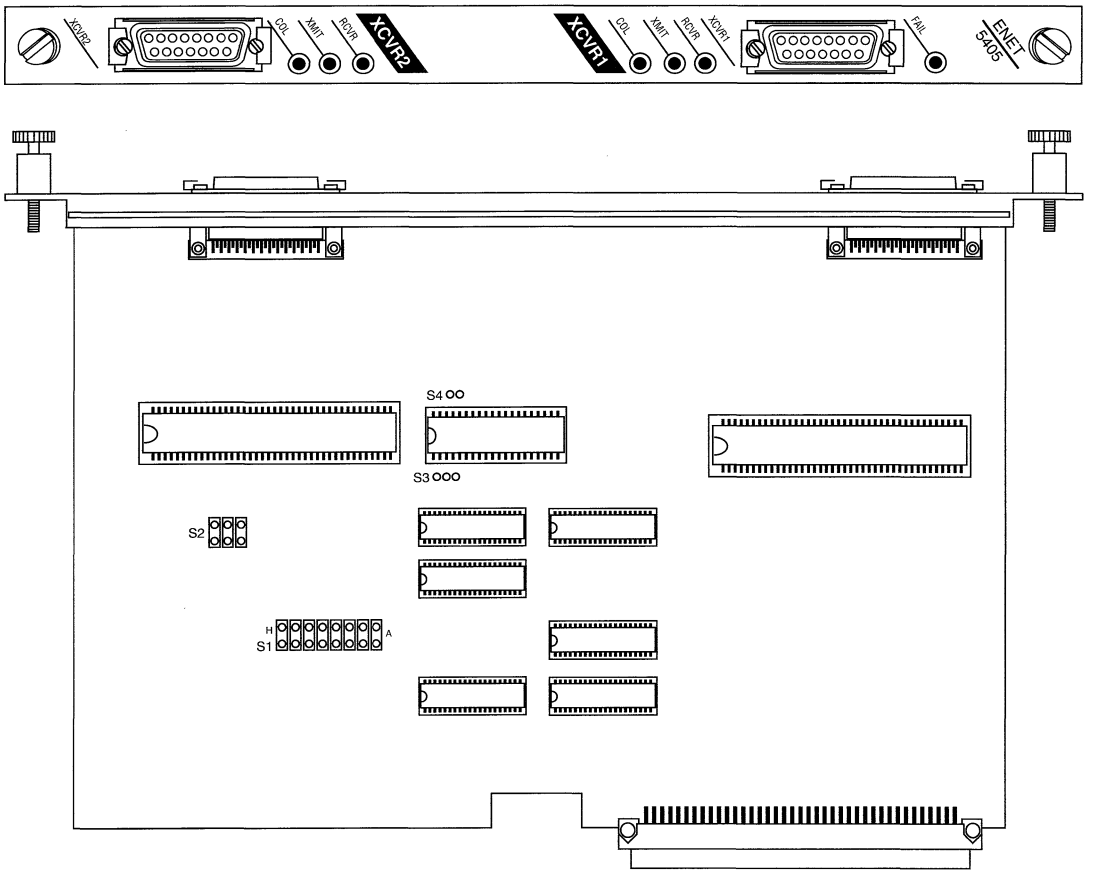


Figure E-4 ENET 2 Board (5405; 100809)

Table E-5 ENET 2 Settings (5405; 100809)

Option	Setting	Jumper
Model ID and Board Option **Note:** This jumper may be hard-wired.	Not configurable	S2 
32-bit EPROM option	Not configurable	S3 ○○○
Power for 28-pin EPROM This jumper may be hard-wired.	Not configurable	S4 ○○

E.5 T1 2 Dual Board (5200; 100831)

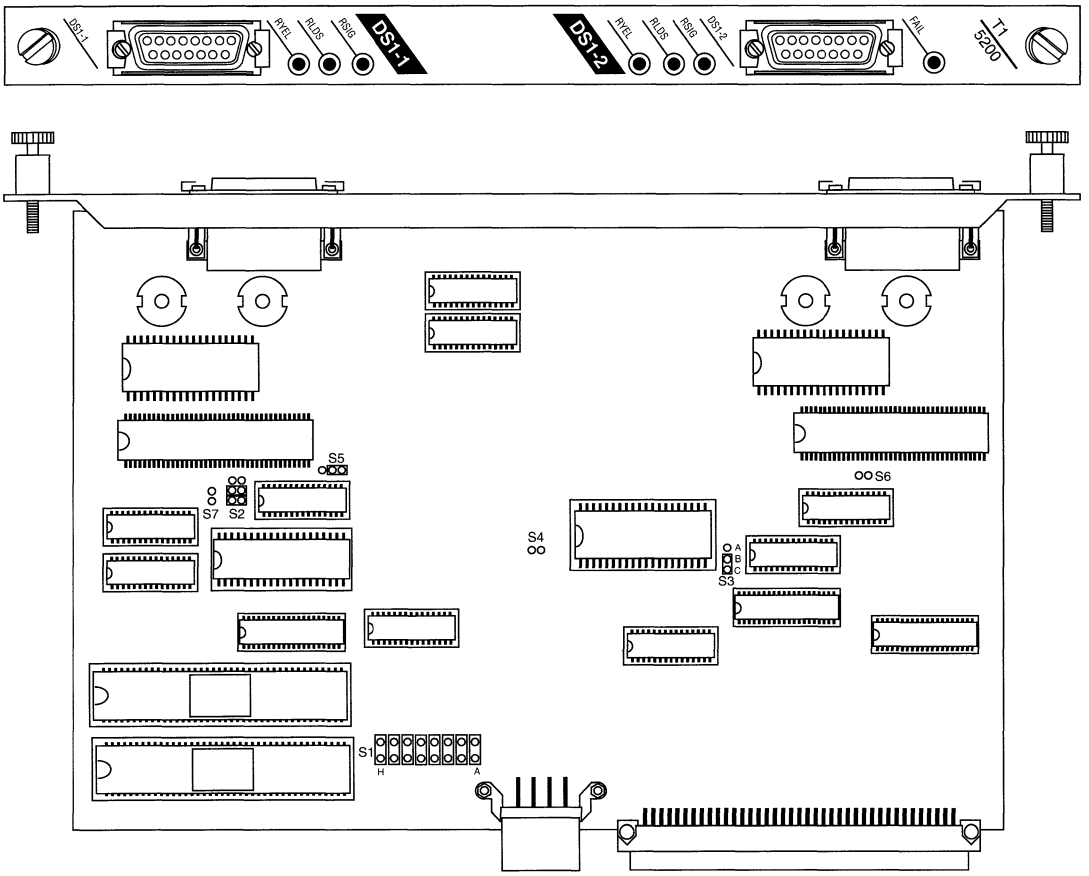


Figure E-5 T1 2 Dual Board (5200; 100831)

Table E-6 T1 2 Dual Settings (5200; 100831)

Option	Setting	Jumper
Board option	Not configurable	S2
32-pin EPROM option	Not configurable	S3 A B C
Power for 28-pin EPROM	Not configurable	S4
Internal clock	Enabled (master)	S5
	Disabled (slave)	S5
Unused (Installed on E1)	Not configurable	S6 S7

E.6 E1-75 Board (5250; 101337)

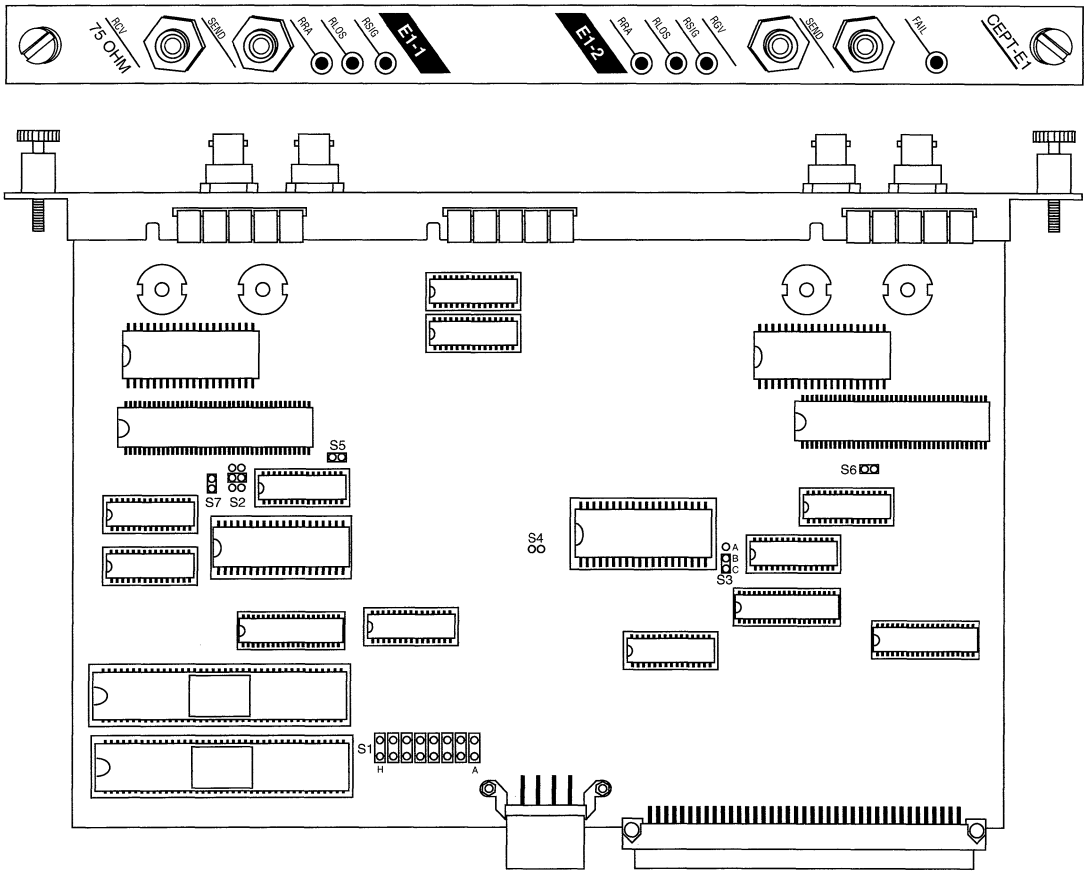
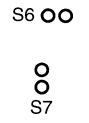


Figure E-6 E1-75 Board (5250; 101337)

Table E-7 E1-75 Settings (5250; 101337)

Option	Setting	Jumper
Option Setting	Not configurable	
Address line for 32-pin EPROM option)	Not configurable	
Power for 28-pin EPROMs	Not configurable	
Internal clock	Enabled (master)	
	Disabled (slave)	
Unused (Installed on E1)	Not configurable	

E.7 T1 Single Port Board (5220; 101338)

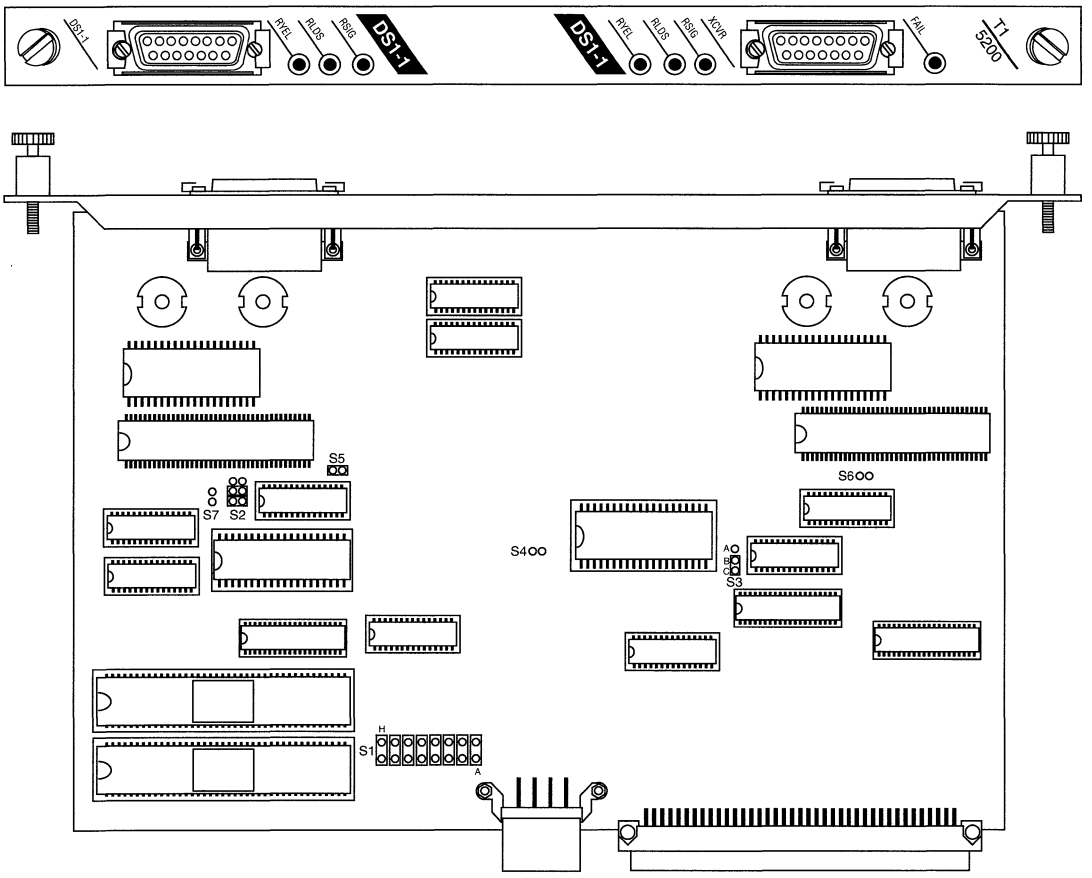


Figure E-7 T1 Single Port Board (5220; 101338)

Table E-8 T1 Single Port Settings (5220; 101338)

Option	Setting	Jumper
Option	Not configurable	S2 
32-pin EPROM option	Not configurable	S3  A B C
Power for 28-pin EPROM	Not configurable	S4
Internal clock	Enabled (master)	S5 
	Disabled (slave)	S5
Unused (Installed on E1)	Not configurable	S6  S7

E.8 DST-4/16 Board (5740; 101531)

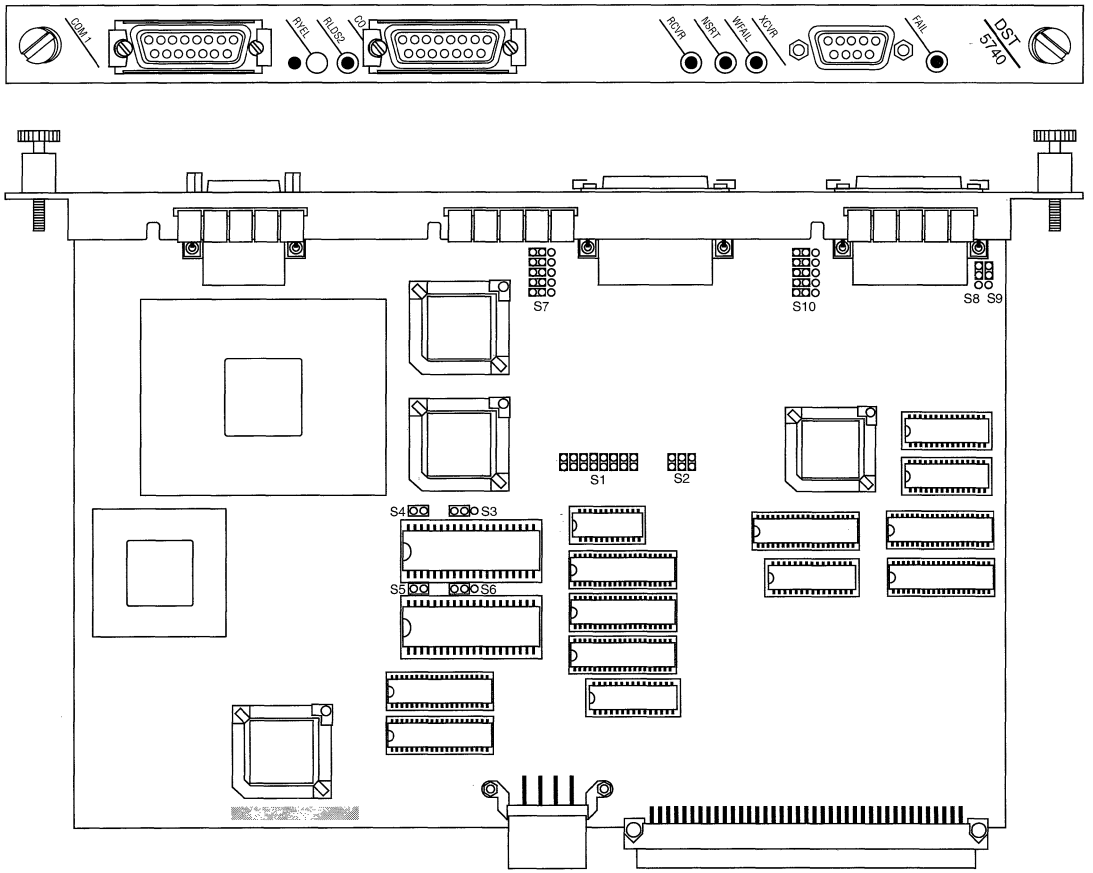


Figure E-8 DST-4/16 Board (5740; 101531)

Table E-9 DST-4/16 Settings (5740; 101531)

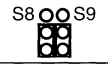
Option	Setting	Jumper
Model ID and Board Option	Not configurable	
32-bit EPROM option at V36	Not configurable	
Power for 28-pin EPROM	Not configurable	
Power for 28-pin EPROM at U48	Not configurable	
32-bit EPROM option at U48	Not configurable	
Standard or X.21 for Comm port 2	Standard	
	X.21	
RS-232 or RS-423	RS-232	
	RS-423	

Table E-9 DST-4/16 Settings (5740; 101531)

Option	Setting	Jumper
Standard or X.21 for Comm port 1	Standard	
	X.21	

E.9 T1 2 56K Board (5201; 101667)

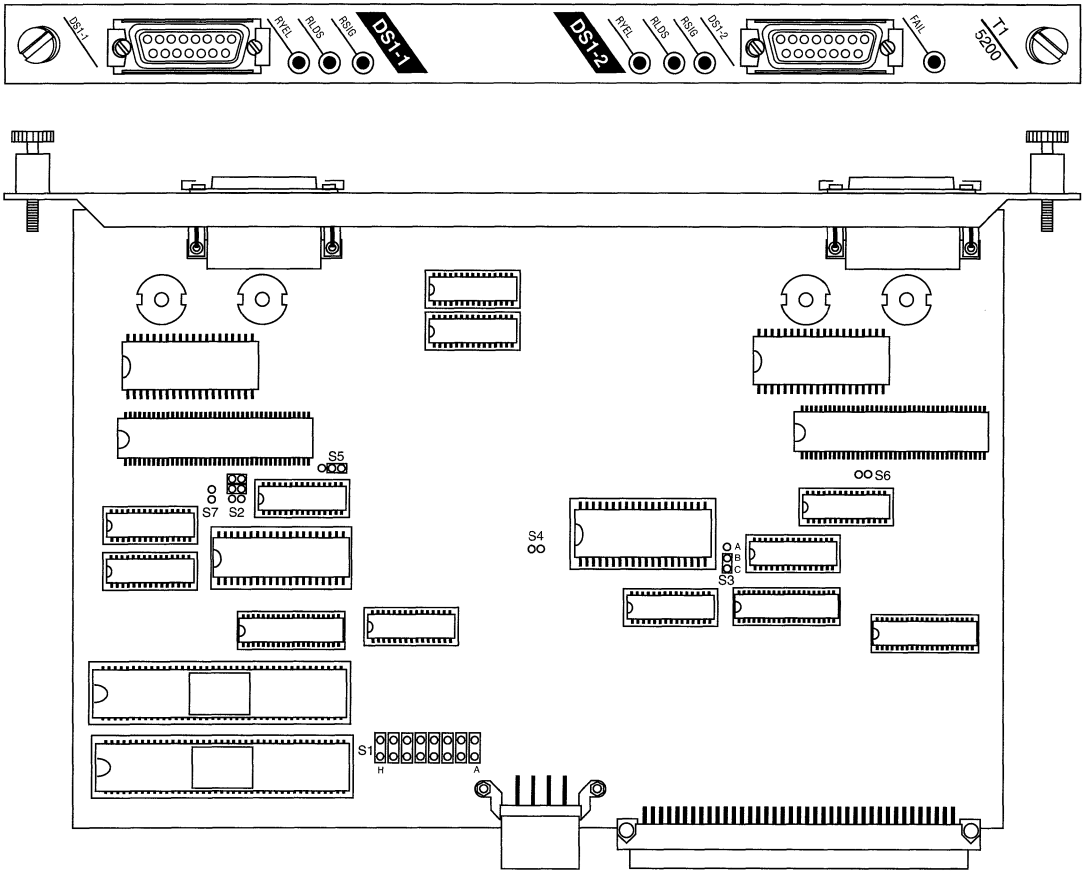
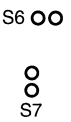


Figure E-9 T1 2 56K Board (5201; 101667)

Table E-10 T1 2 56K Settings (5201; 101667)

Option	Setting	Jumper
Option	Not configurable	
32-pin EPROM option	Not configurable	
Power for 28-pin EPROM	Not configurable	
Internal clock	Enabled (master)	
	Disabled (slave)	
Unused (Installed on E1)	Not configurable	

E.10 FDDI Controller Board (5912; 102232)

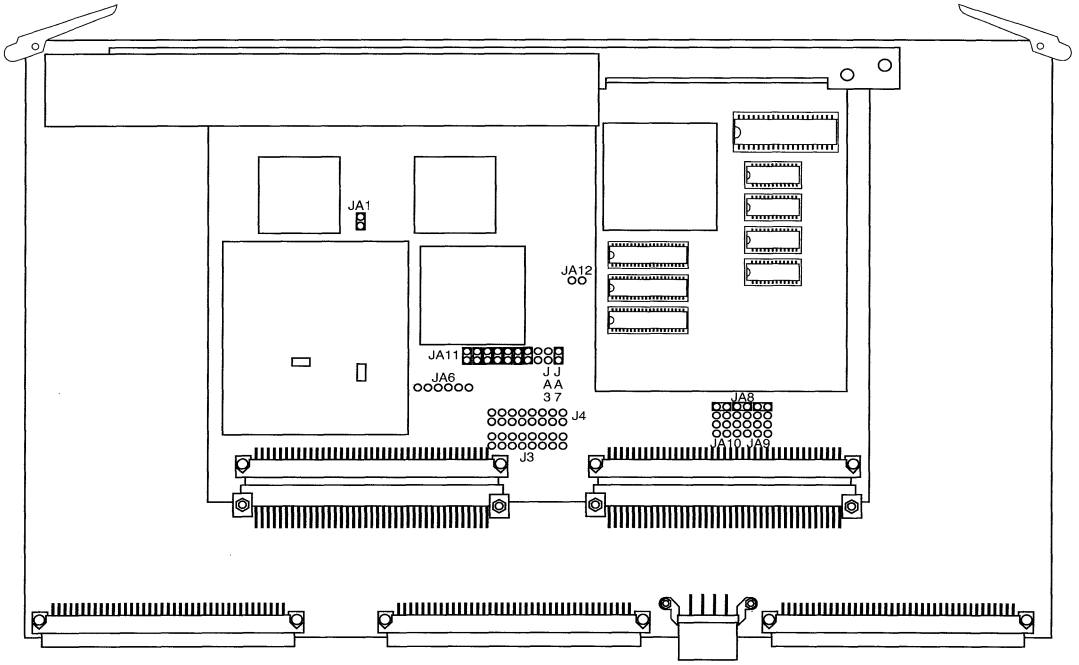


Figure E-10 FDDI Controller Board (5912; 102232)

Table E-11 FDDI Controller Settings (5912; 102232)

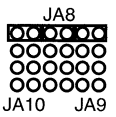
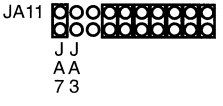
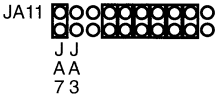
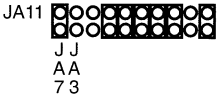
Option	Setting	Jumper
Reserved	Not configurable	
Reserved	Not configurable	
Dual PHY	Not configurable	
Optical Bypass Control	Not configurable	
VMEbus Request Level	Not configurable	
Short Address	0000 (for first FDDI in node)	
	0200 (for second FDDI in node)	
	0400 (for third FDDI in node)	

Table E-11 FDDI Controller Settings (5912; 102232)

Option	Setting	Jumper
Factory test	Not configurable	

E.11 DSDE 4 Board (5430; 102279)

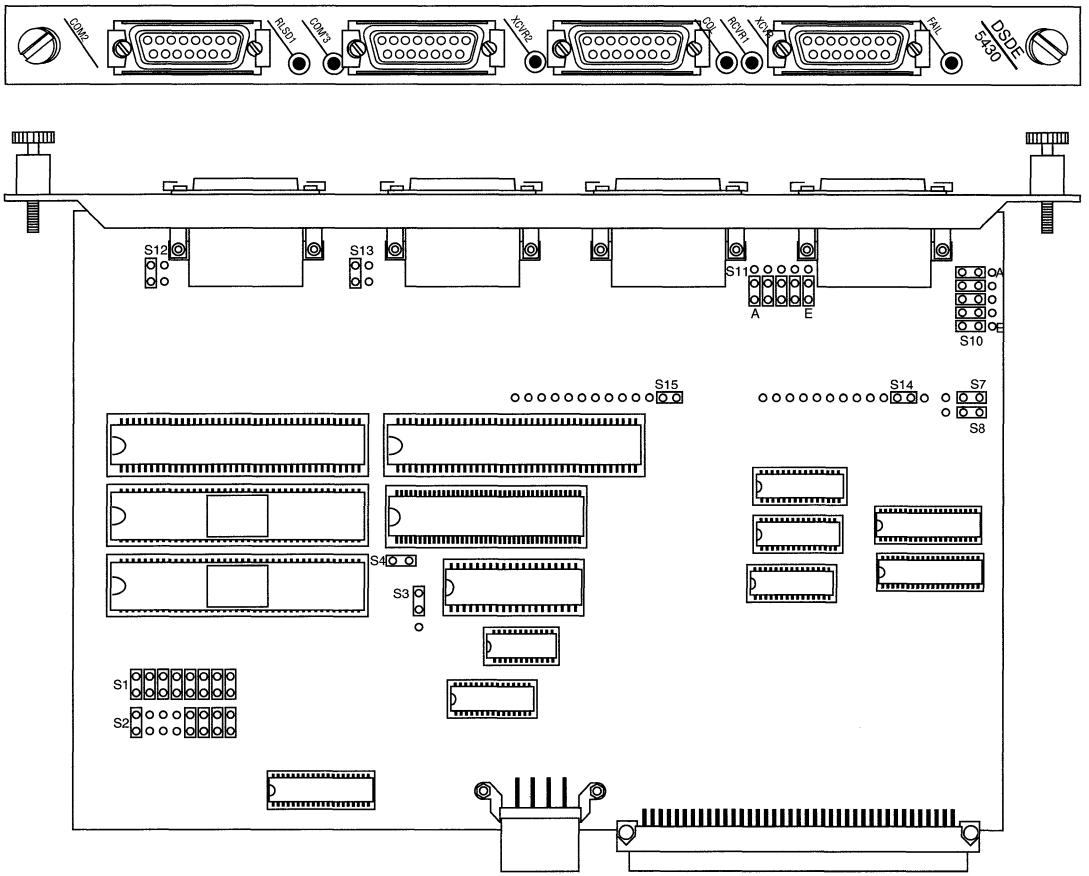


Figure E-11 DSDE 4 Board (5430; 102279)

Table E-12 DSDE 4 Settings (5430; 102279)

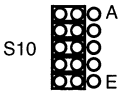
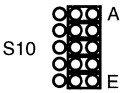
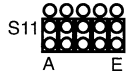
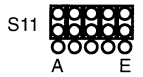
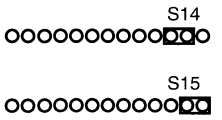
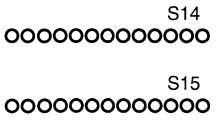
Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 35-pin EPROM	Not configurable	
Power for 28-pin EPROM	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
Comm port 2	Standard	
	X.21	

Table E-12 DSDE 4 Settings (5430; 102279)

Option	Setting	Jumper
Comm port 1	Standard	
	X.21	
Chassis ground connection for unused pins on J1	Not configurable	
Chassis ground connection for unused pins on J2	Not configurable	
Installation of V.35 daughter board	V.35 daughter board *not* installed	
	V.35 daughter board installed	

E.12 QSYNC 4 Board (5280; 102285)

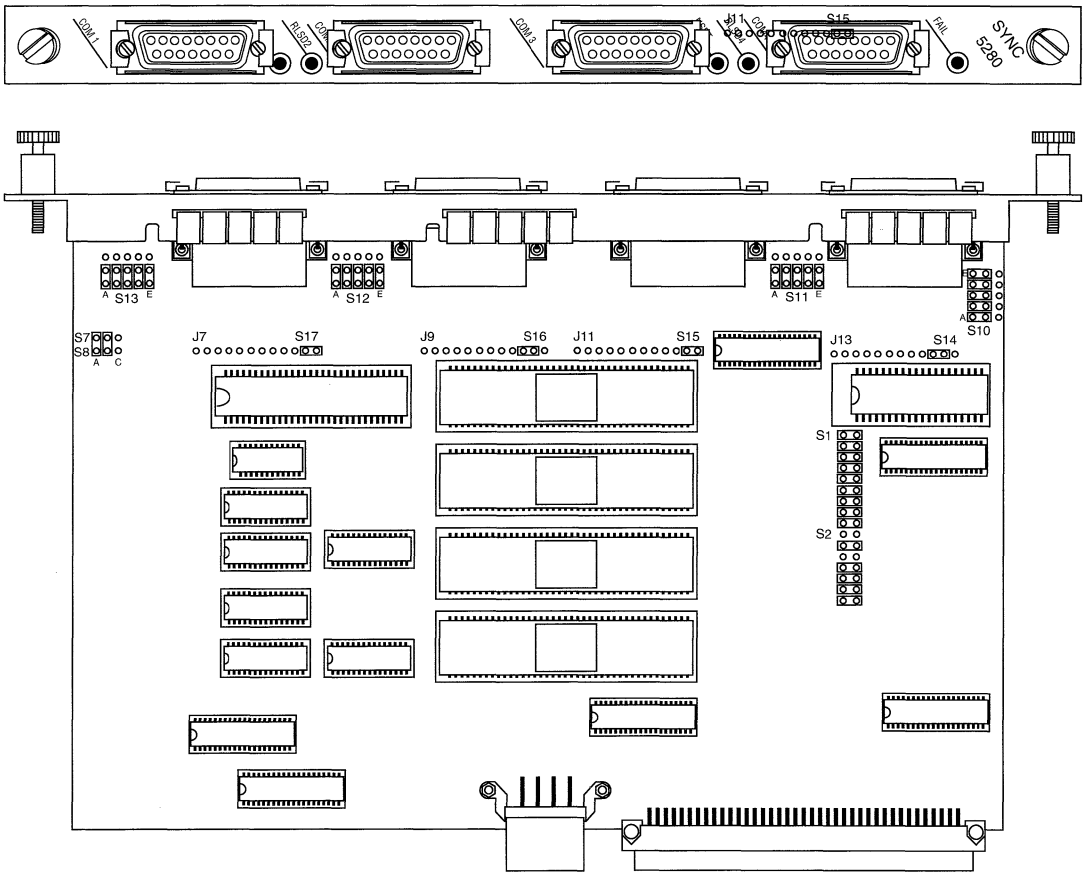


Figure E-12 QSYNC 4 Board (5280; 102285)

Table E-13 QSYNC 4 Settings (5280; 102285)

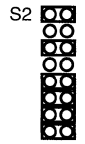
Option	Setting	Jumper
Model ID and Board Option	Not configurable	
32-bit EPROM option	Not configurable	
Power for 28-pin EPROM	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	

Table E-13 QSYNC 4 Settings (5280; 102285)

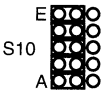
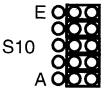
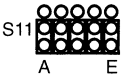
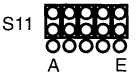
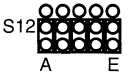
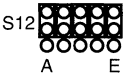
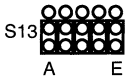
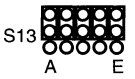
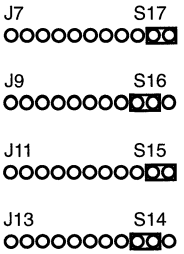
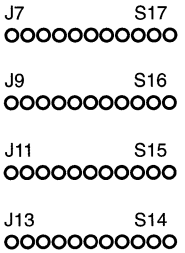
Option	Setting	Jumper
Standard or X.21 for Comm port 1	Standard	
	X.21	
Standard or X.21 for Comm port 2	Standard	
	X.21	
Standard or X.21 for Comm port 3	Standard	
	X.21	

Table E-13 QSYNC 4 Settings (5280; 102285)

Option	Setting	Jumper
Standard or X.21 for Comm port 4	Standard	
	X.21	
Daughter board **Note:** Each J-to-S row is in a separate location on the board	Daughter board *not* mounted	
	Daughter board mounted	

E.13 DSE 4 Board (5420; 102293)

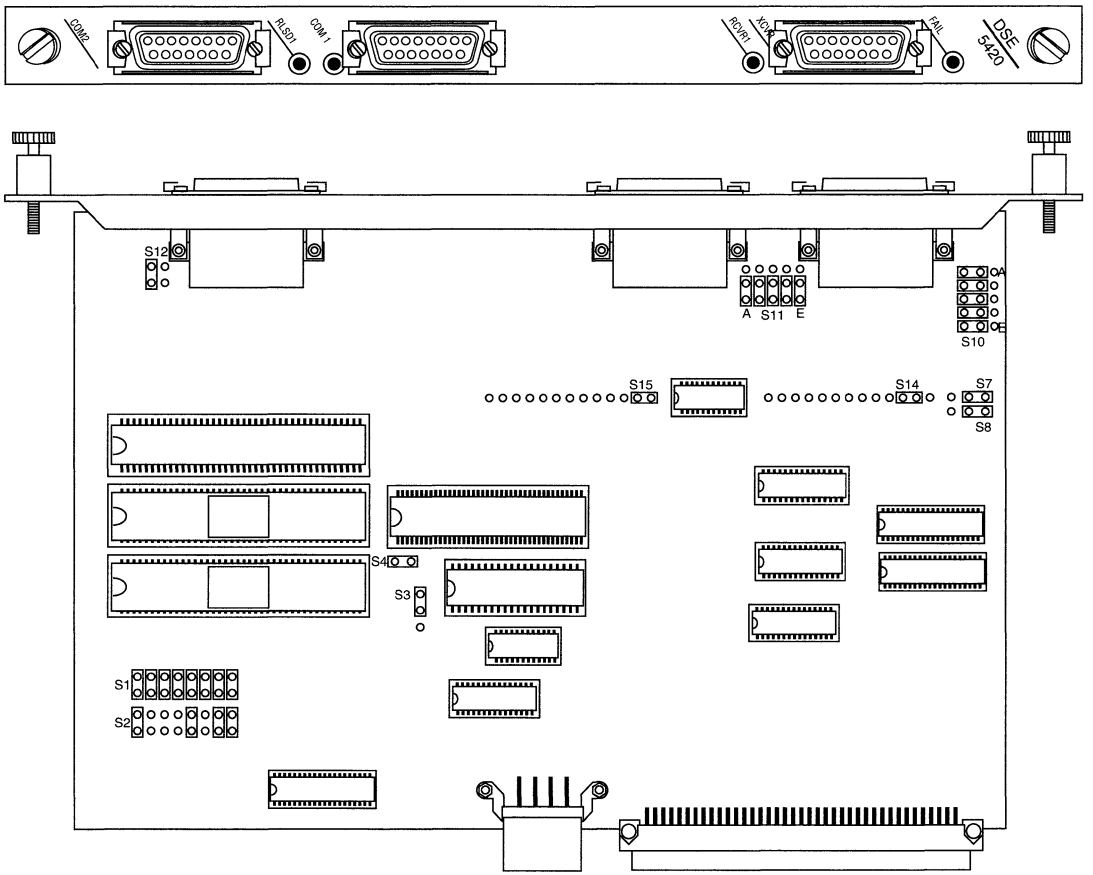


Figure E-13 DSE 4 Board (5420; 102293)

Table E-14 DSE 4 Settings (5420; 102293)

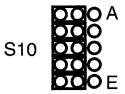
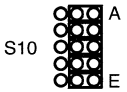
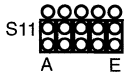
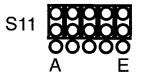
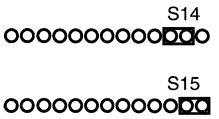
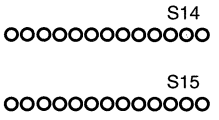
Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 35-pin EPROM	Not configurable	
Power for 28-pin EPROM	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
Comm port 2	Standard	
	X.21	

Table E-14 DSE 4 Settings (5420; 102293)

Option	Setting	Jumper
Comm port 1	Standard	
	X.21	
Chassis ground connection for unused pins on J1	Not configurable	
Installation of V.35 daughter board	V.35 daughter board *not* installed	
	V.35 daughter board installed	

E.14 SSE 4 Board (5410; 102296)

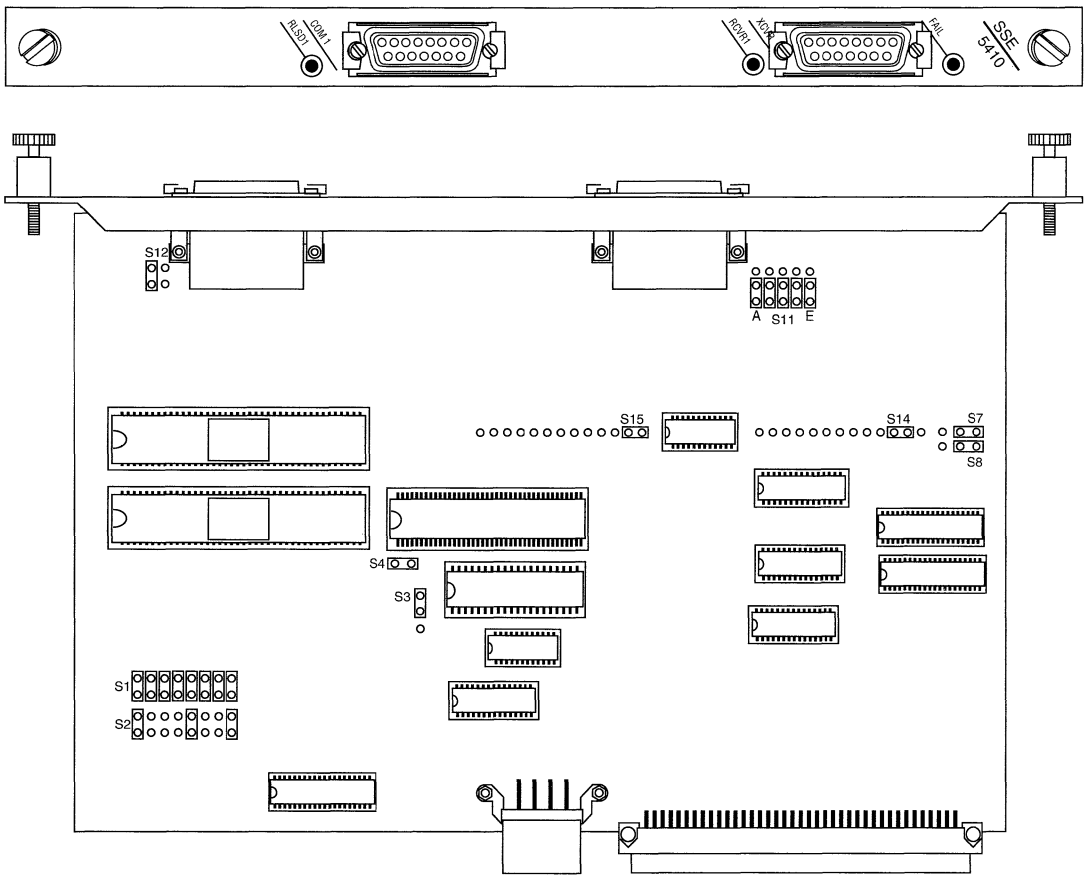


Figure E-14 SSE 4 Board (5410; 102296)

Table E-15 SSE 4 Settings (5410; 102296)

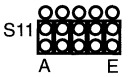
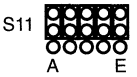
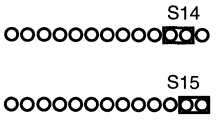
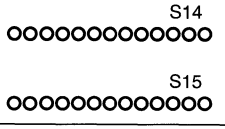
Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 35-pin EPROM	Not configurable	
Power for 28-pin EPROM	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
Comm port 1	Standard	
	X.21	
Chassis ground connection for unused pins on J1	Not configurable	

Table E-15 SSE 4 Settings (5410; 102296)

Option	Setting	Jumper
Chassis ground connection for unused pins on J2	Not configurable	
Installation of V.35 daughter board	V.35 daughter board *not* installed	
	V.35 daughter board installed	

E.15 V.35 Daughter Board (4290; 102310)

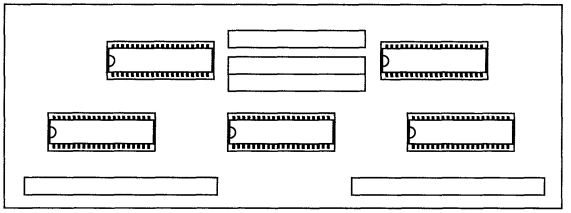


Figure E-15 V.35 Daughter Board (4290; 102310)

This board does *not* contain user-configurable jumpers or switches.

E.16 TS416 1x2 Board (5740; 102482)

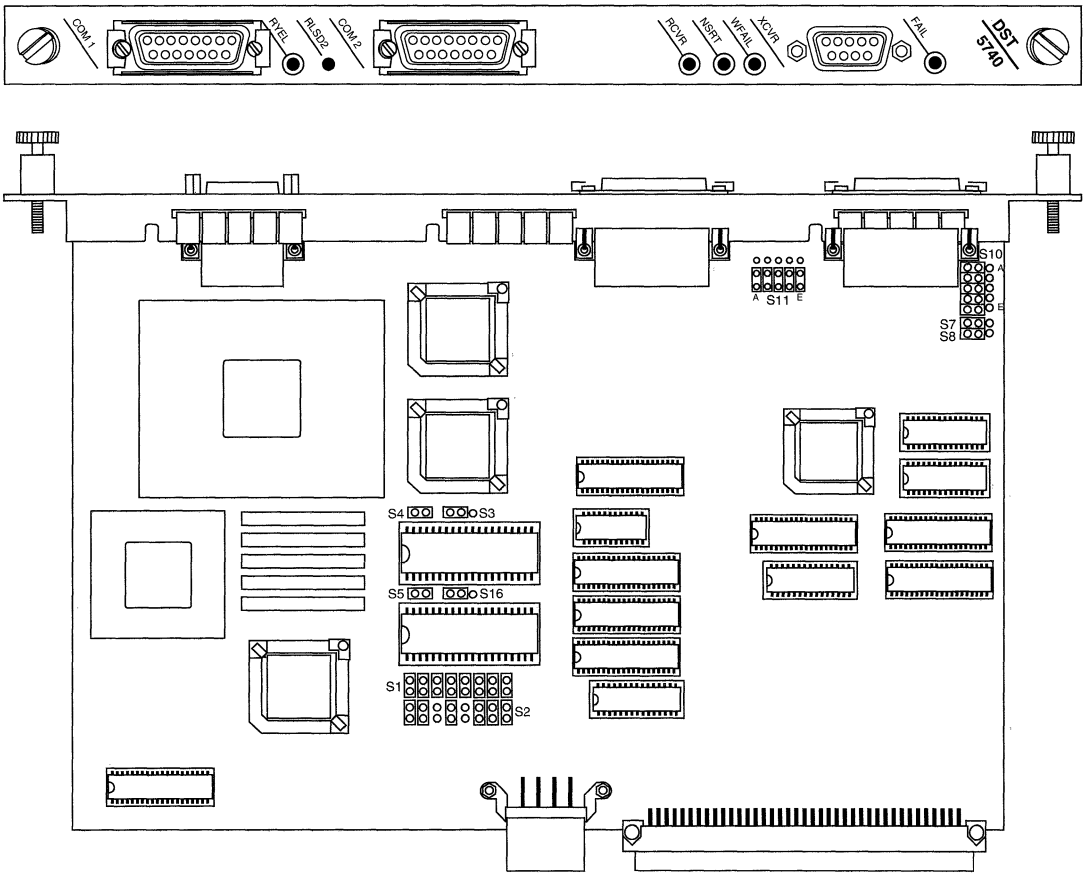


Figure E-16 TS416 1x2 Board (5740; 102482)

Table E-16 TS416 1x2 Settings (5740; 102482)

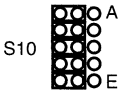
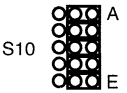
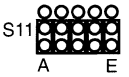
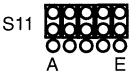
Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 32-pin EPROM at U39	Not configurable	
Power for 28-pin EPROM at U39	Not configurable	
Power for 28-pin EPROM at 50	Not configurable	
Address line for 32-pin EPROM at U50	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
Comm port 1	Standard	
	X.21	

Table E-16 TS416 1x2 Settings (5740; 102482)

Option	Setting	Jumper
Comm port 2	Standard	
	X.21	

E.17 TS416 1x1 Board (5720; 102483)

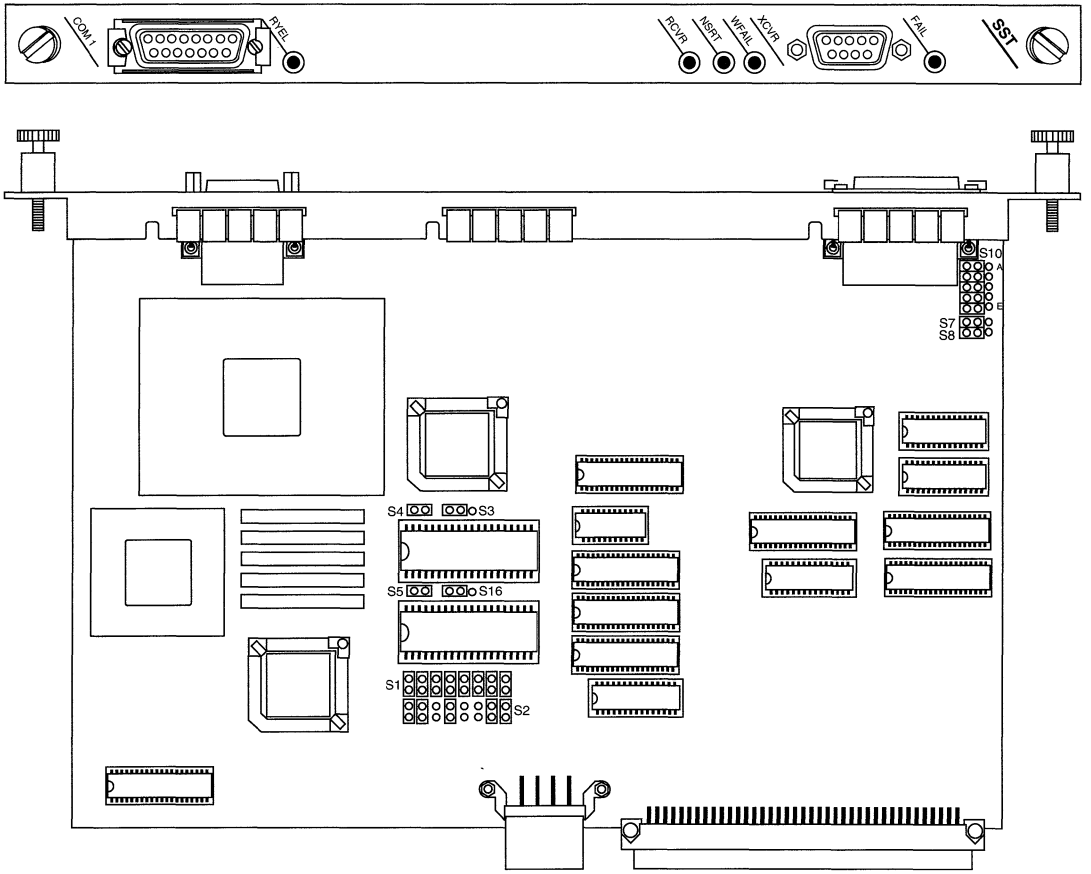
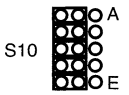
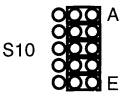


Figure E-17 TS416 1x1 Board (5720; 102483)

Table E-17 TS416 1x1 Settings (5720; 102483)

Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 32-pin EPROM at U39	Not configurable	
Power for 28-pin EPROM at U39	Not configurable	
Power for 28-pin EPROM at 50	Not configurable	
Address line for 32-pin EPROM at U50	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
Comm port 1	Standard	
	X.21	

E.18 TS416 1x0 Board (5705; 102484)

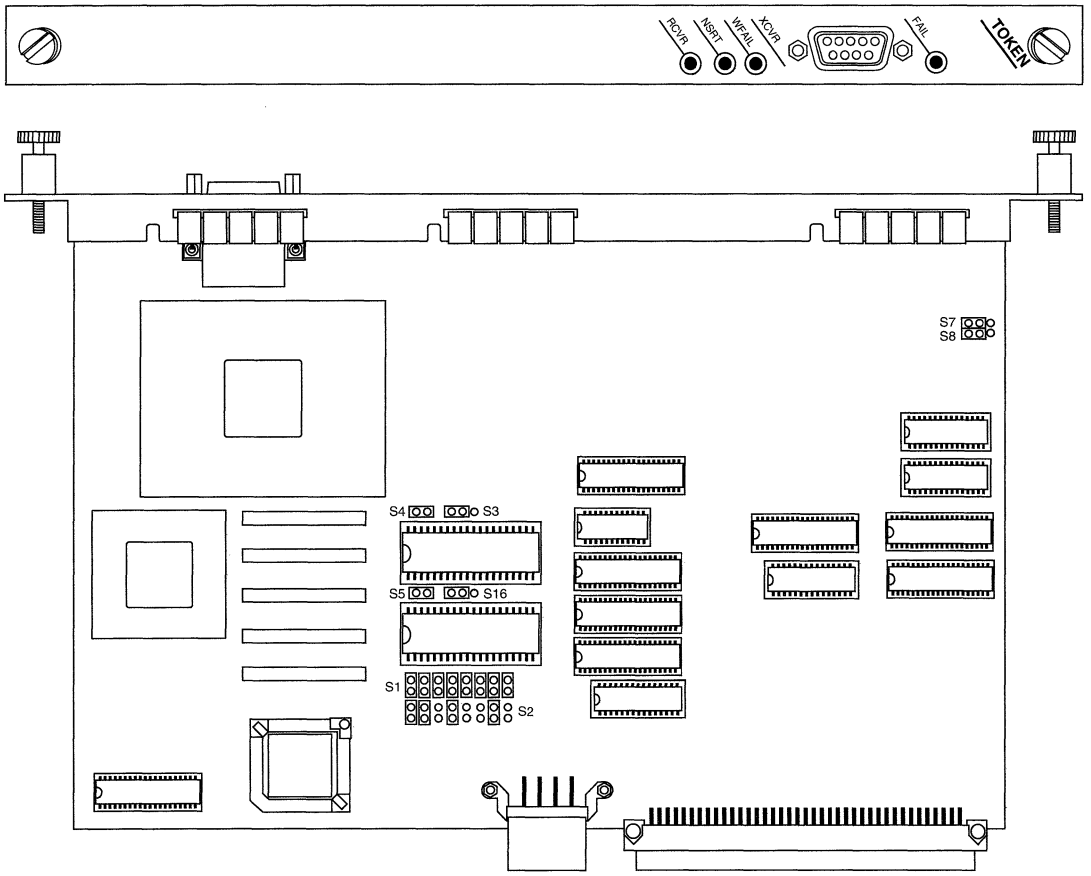
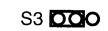
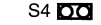
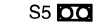
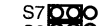
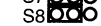


Figure E-18 TS416 1x0 Board (5705; 102484)

Table E-18 TS416 1x0 Settings (5705; 102484)

Option	Setting	Jumper
Model ID and board option	Not configurable	S2 
Address line for 32-pin EPROM at U39	Not configurable	S3 
Power for 28-pin EPROM at U39	Not configurable	S4 
Power for 28-pin EPROM at 50	Not configurable	S5 
Reserved for future use	Not configurable	S7  S8 
Address line for 32-pin EPROM at U50	Not configurable	S16

E.19 ESA 2x2 Board (5530; 102494)

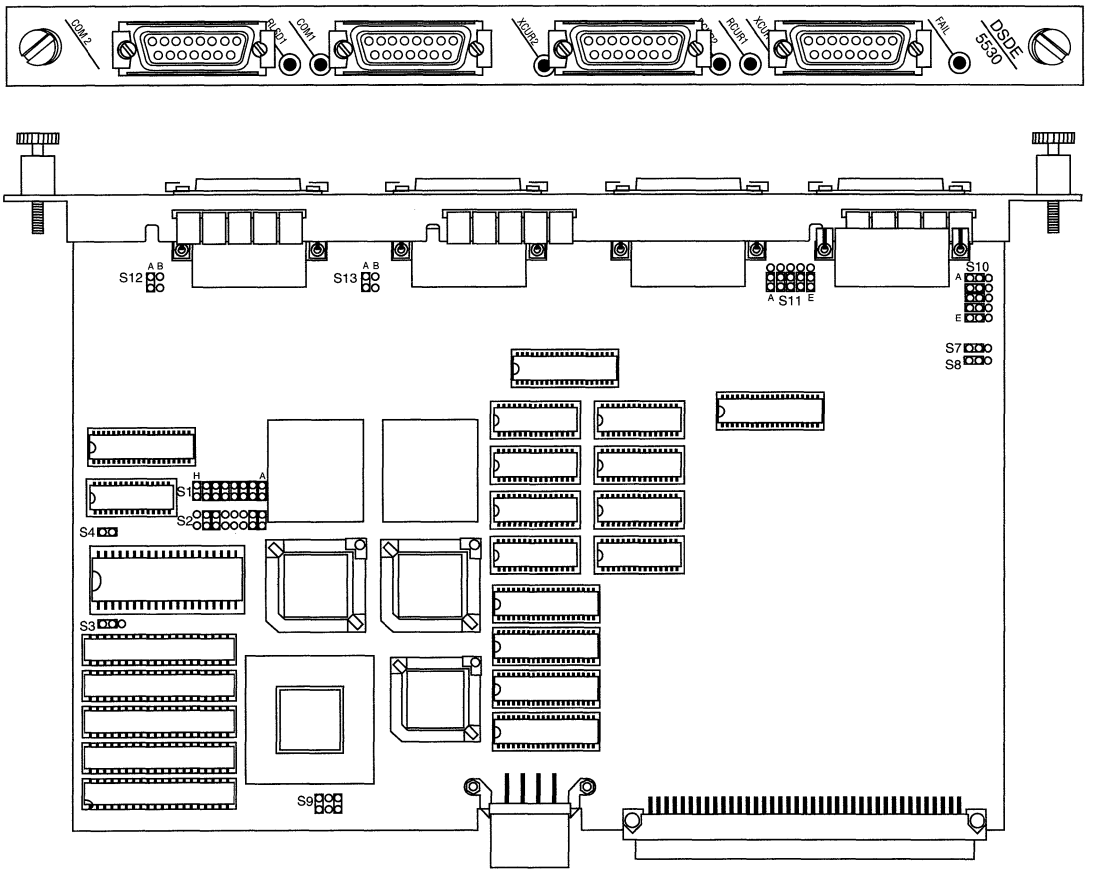


Figure E-19 ESA 2x2 Board (5530; 102494)

Table E-19 ESA 2x2 Settings (5530; 102494)

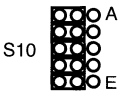
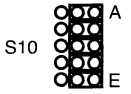
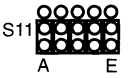
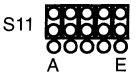
Option	Setting	Jumper
Model ID and board option	Not configurable	
Address line for 32-pin EPROM	Not configurable	
Power for 28-pin EPROM	Not configurable	
RS-232 or RS-423	RS-232	
	RS-423	
2 cams installed	Not configurable	
Comm port 2	Standard	
	X.21	

Table E-19 ESA 2x2 Settings (5530; 102494)

Option	Setting	Jumper
Comm port 1	Standard	
	X.21	
Chassis ground connection for unused pins on J1	Not configurable	
Chassis ground connection for unused pins on J2	Not configurable	

E.20 ESA 2x0 Board (5505; 102495)

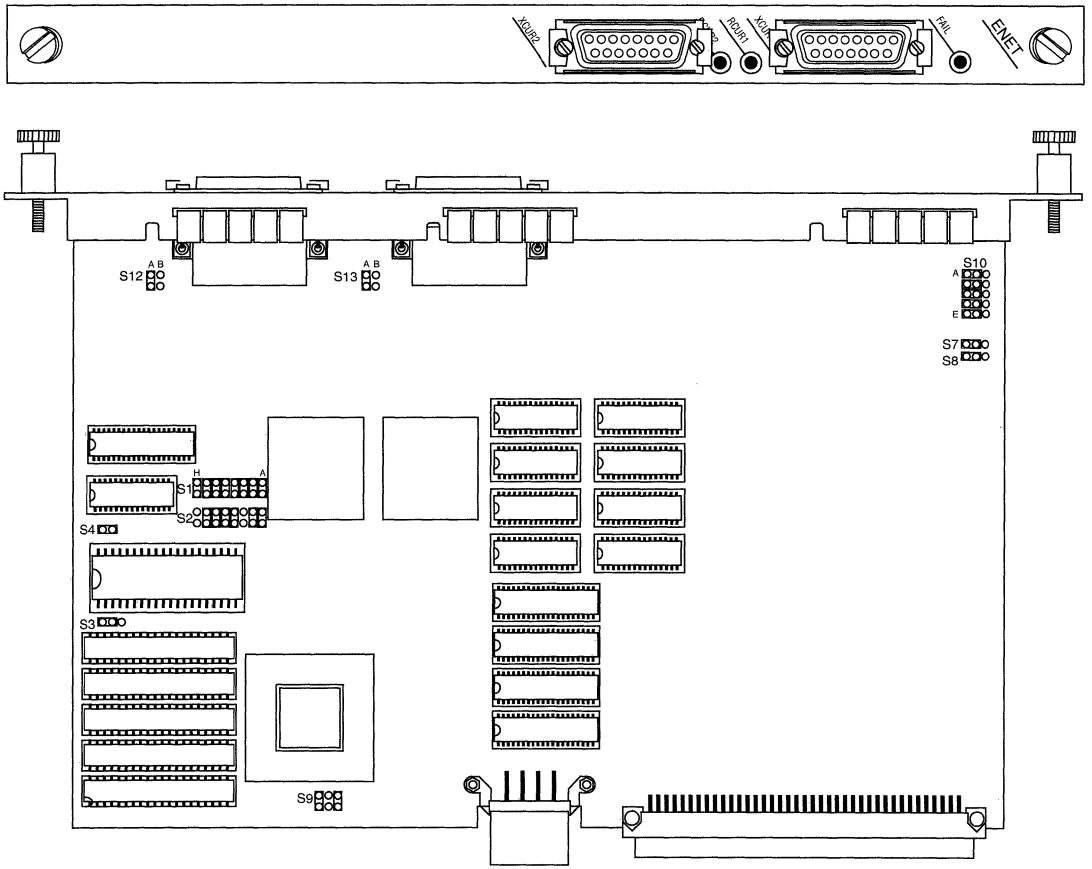
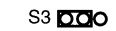


Figure E-20 ESA 2x0 Board (5505; 102495)

Table E-20 ESA 2x0 Settings (5505; 102495)

Option	Setting	Jumper
Model ID and board option	Not configurable	S2 
Address line for 32-pin EPROM	Not configurable	S3 
Power for 28-pin EPROM	Not configurable	S4 
2 cams installed	Not configurable	S9 
Chassis ground connection for unused pins on J1	Not configurable	S12 
Chassis ground connection for unused pins on J2	Not configurable	S13 

E.21 Multimode FDDI Board (5930; 102675) and Daughter Board (4995; 103269)

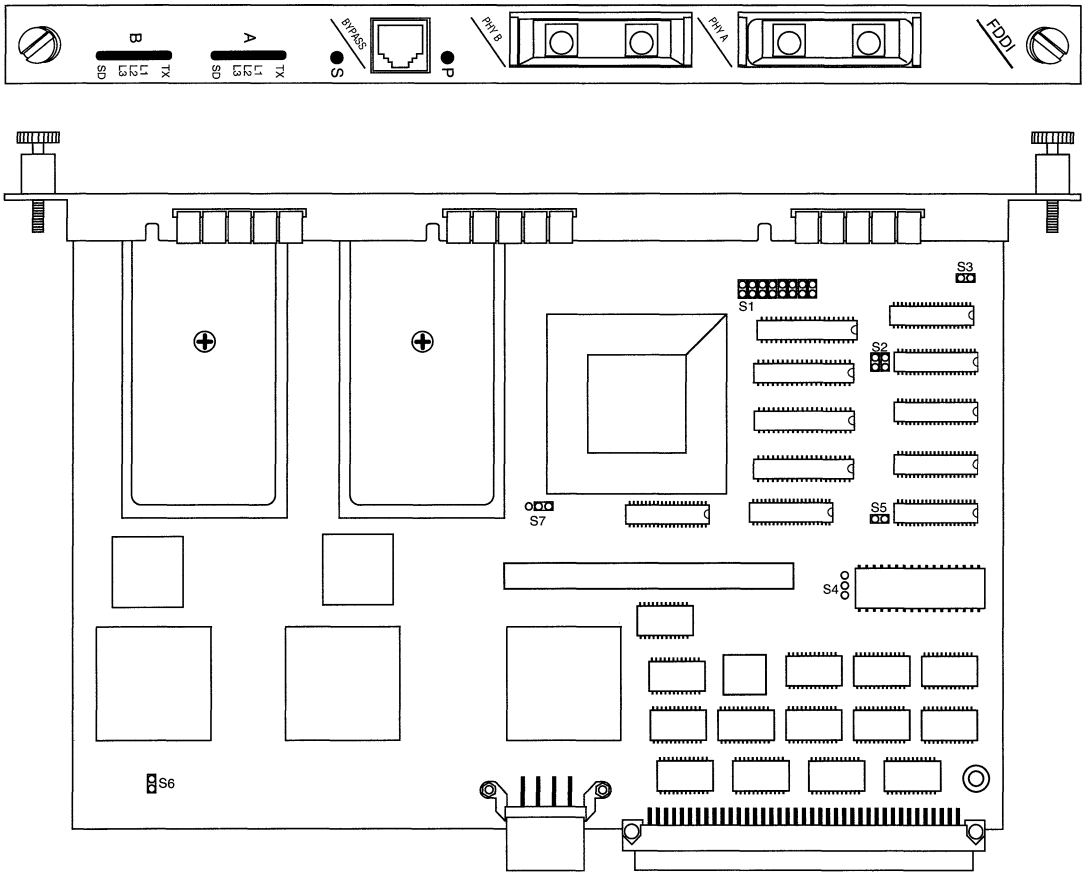


Figure E-21 Multimode FDDI Board (5930; 102675)

The FDDI board requires an ACE 32 at a revision level of 25 or greater and a System Controller at a revision level of 20 or greater. This board does *not* require the installation of IAC backplane jumpers. IAC jumpers do not affect the operation of this board.

Table E-21 Multimode FDDI Settings (5930; 102675)

Option	Setting	Jumper
Options	Not configurable	S2
PROM Configuration	Not configurable	S3
PROM Configuration	Not configurable	S4
PROM Configuration	Not configurable	S5
Clock select	Not configurable	S6
Future compatibility	Not configurable	S7

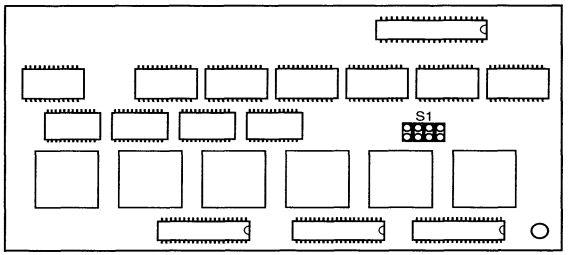


Figure E-22 Multimode FDDI Daughter Board (4995; 103269)

The FDDI Daughter Board does *not* have user-configurable jumpers or switches.

E.22 QENET Board (5450; 102690) and Optional High Speed Filter (102671)

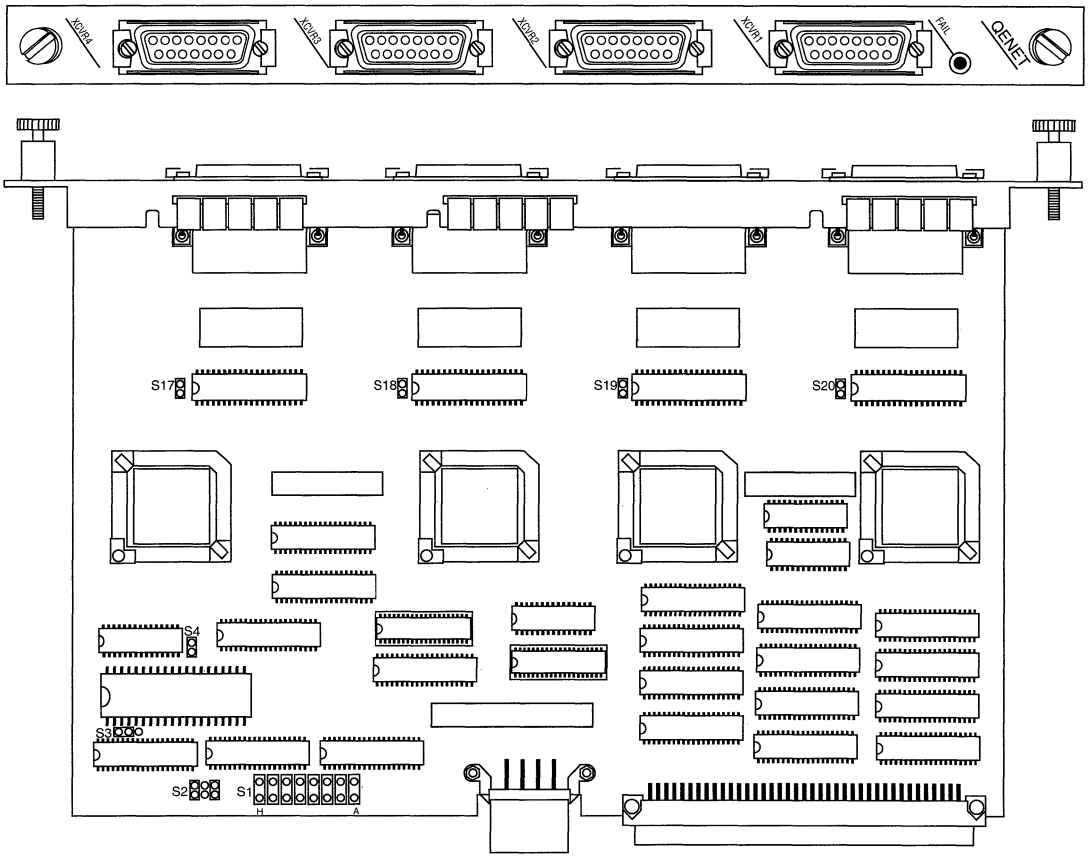
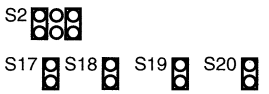
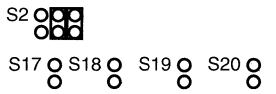


Figure E-23 QENET Board (5450; 102690)

Table E-22 QENET Settings (5450; 102690)

Option	Setting	Jumper
Daughter board **Note:** The jumpers are in separate locations on the board.	Daughter board *not* mounted (*not* customer-configurable)	
	Daughter board mounted (*not* customer-configurable)	
512 K EPROM	(not configurable)	

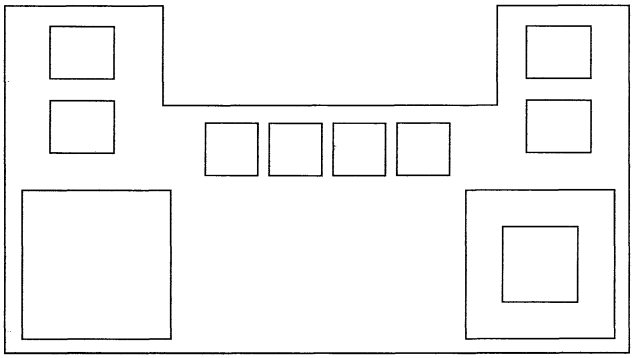


Figure E-24 Optional High Speed Filter (102671)

The High Speed Filter Daughter Board does not have jumpers or switches.

E.23 System I/O Board (5010; 102937)

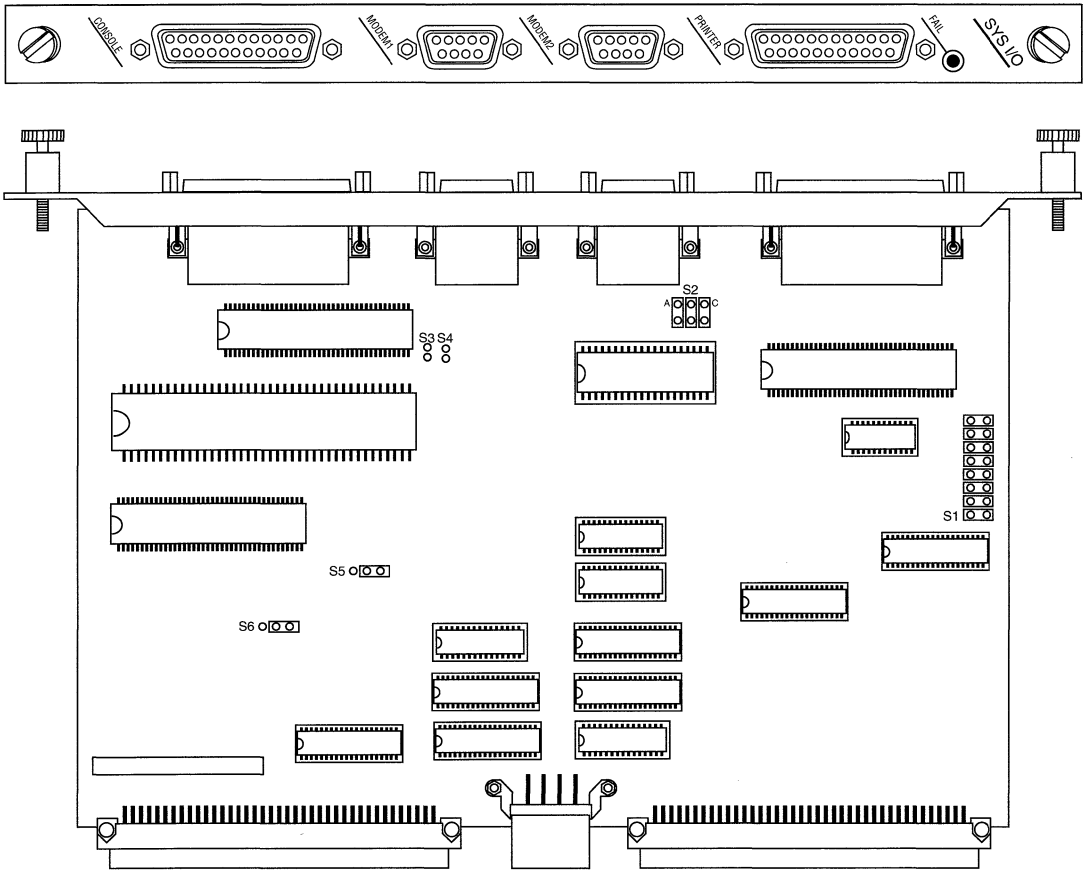


Figure E-25 System I/O Board (5010; 102937)

Table E-23 System I/O Settings (5010; 102937)

Option	Setting	Jumper
Board	Not configurable	 S2
Type of floppy drive used	Not configurable	1 3 S5  1 3 S6 
8 MHz operation of UART	Not configurable	 S7

E.24 Dual Token Ring Board (4710; 103366)

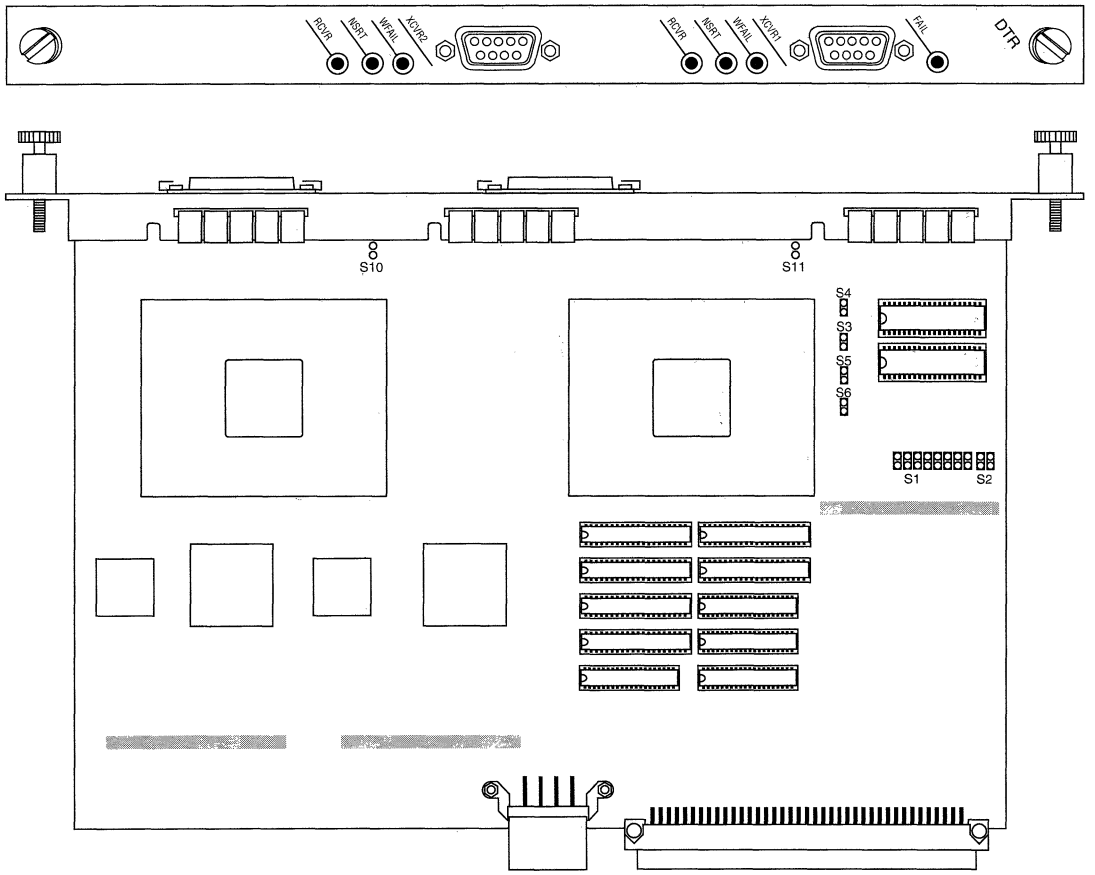


Figure E-26 Dual Token Ring Board (4710; 103366)

Table E-24 Dual Token Ring Settings (4710; 103366)

Option	Setting	Jumper
Board Option	Not configurable	 S2
EPROM address bit 17 for diagnostic PROM	Not configurable	S3 
+5 V to diagnostic PROM	Not configurable	S4 
EPROM address bit 17 for BUD-MAC (bring up diagnostics) in TS-380 Token Ring controller	Not configurable	S5 
+5 V for BUD-MAC in TS-380 Token Ring controller chip	Not configurable	S6 
Reserved for future use	Not configurable	S10 
Reserved for future use	Not configurable	S11 

Index

A

B

C

D

E

F

H

I

T

U

X

15 Crosby Drive, Bedford, MA 01730-2204 Tel: (617) 275-2400 Fax: (617) 275-8421