

This chapter describes how to configure input and output filters. IP, IPX and SAP rules are reviewed and filter examples are given.

This chapter includes the following topics:

- An overview of packet filters and how they are organized and created
- A description of IP, IPX, and SAP filter rules
- Filtering FTP packets
- How filters are used to limit network access

Each of the topics in this chapter include examples of filters used to accomplish the goal described.

Overview of Filters

Packet filters are used to increase security on your network. Filters are especially useful for restricting information that is passed across organizational and corporate boundaries. Filters can be used to limit certain kinds of internetwork communications by permitting or denying the passage of packets through network interfaces or ports. By designing appropriate filters, you can control access to specific hosts, networks, and network services.

Packet filtering requires the analysis of the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded. If a packet is not permitted by a filter, an appropriate ICMP unreachable or TCP Reset message is returned to the originator. This process reduces network traffic and provides more immediate feedback to the user attempting the unauthorized access.

Filters can also be used for packet selection, such as when using a packet trace to debug a connection. The packets permitted by the ptrace filter are displayed, while packets not permitted by the filter are not displayed. For more information about ptrace, see “Tracing Packets” on page 19-8.

The packet filtering mechanism is designed with four objectives:

- Reliability
- Predictability
- Flexibility
- Efficiency

The features listed in Table 10-1 help achieve these objectives.

Table 10-1 Features of PortMaster Filtering

Feature	Description
Input and Output Filters	Each user, each location, and each network hardwired port can be assigned both an input packet filter and an output packet filter. Having both input and output filters can decrease the number of rules needed and can provide better tuning of your security policy.
Source and Destination Address Filtering	You can create filters that evaluate both the source and destination addresses of a packet against a rule list. The number of significant bits used in IP address comparisons can be set, allowing filtering by a specific host, subnet, network number, or a group of hosts whose addresses are within a given bit-aligned boundary.
Protocol Filtering	Packets of certain protocols can be permitted or denied by a filter, including IPX, SAP, TCP, UDP, and ICMP packets.
Source and Destination Port Filtering	You can create filters that use the source and destination port numbers to control access to certain network services. This includes evaluation based upon whether the port number is less than, equal to, or greater than a specified value.
Established Session Filtering	You can create filters that use the status of TCP connections as part of the rule set. This can allow network users to open connections to external networks without allowing external users access to the local network.

Table 10-1 Features of PortMaster Filtering (Continued)

Feature	Description
Number of Rules	Each filter can have any number of rules, limited only by the memory available within the PortMaster.
Simple Rule Creation	You can create filters that only include as much information as is necessary to describe the rule. For example, if the rule is not based on specific source and destination addresses, they can be omitted from the rule.
In-line Rule Processing	Rules are processed in the order they are specified in the rule set. This eliminates ambiguity about how a packet is handled. The first rule that matches the packet is applied. If the rule is defined as permit, the packet is allowed to pass. If the rule is defined as deny, the packet is discarded. If there are any rules in the filter and the packet does not match any of the rules, the packet is discarded.

Filter Organization

Filters are maintained in a Filter Table in the PortMaster nonvolatile configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter has a name of up to 16 characters.

Each packet filter can contain three sets of rules: IP, IPX, and SAP. Within each set, the rules are numbered starting at one. Newly created packet filters do not contain any rules.

An empty set of rules is equivalent to the permit rule. If there are one or more rules in the set, any packet not explicitly permitted by a rule is denied at the end of the rule set.

IP and IPX packet filters are attached to users, locations, or network hardwired ports as either input or output filters. SAP filters are only attached as output filters. For asynchronous interfaces, the packet filter is enabled when the port transitions to the established state. The Ethernet interface filter is enabled as soon as the name of the input or output filter is attached to the interface.

All packets passing into an interface with an input filter are evaluated against the rules in the filter. As soon as a packet matches a rule, the action specified by that rule is taken. If no rules match the specific packet, the packet is denied and is discarded. Whenever an IP packet is discarded, the PortMaster generates an ICMP Host Unreachable message back to the originator. For interfaces with output filters attached, all packets going out of the interface are evaluated against the filter rules and only those packets permitted by the filter are allowed to pass out of the interface.

Filter Creation

Filters are created using the Filter Table available with any of the PMconsole interfaces to the PortMaster or from the command line. To create a filter, open the Filter Table by selecting Filters from the Tables menu. Figure 10-1 shows an example of the Filter Window. The window you see depends on the version of PMconsole you are using to configure your PortMaster.

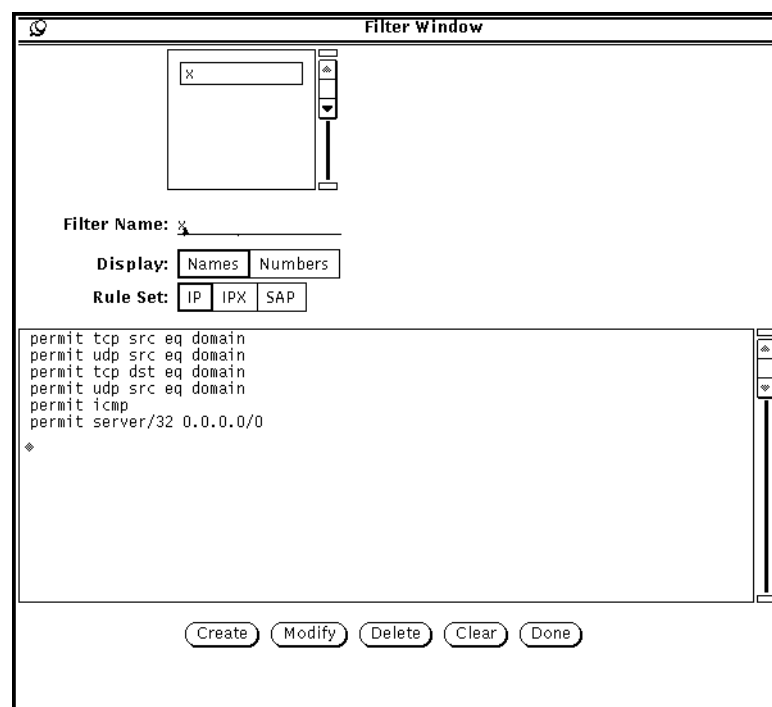


Figure 10-1 Filter Table Window—X Windows GUI

Setting Filters

Filters are constructed by creating the filter and then adding rules that permit or deny certain types of packets. Packets are evaluated in the same order as the rules are listed. Therefore, the packets representing the highest volume of traffic should be specified early in the list of rules, where possible.

Filters can be attached to Ethernet interfaces, hardwired serial ports, users, and locations. Ethernet filters are used to control the types of packets that are allowed to pass through the local Ethernet port. Filters are set on asynchronous ports configured for hardwired operation when security with another network is an issue.

User filters are attached to users configured for dial-in SLIP or PPP access. When a user makes a PPP or SLIP connection the designated filters are attached to the interface used.

Location filters are attached to dial-out locations using SLIP or PPP connections. When the connection is established to a remote site the designated filters are attached to the interface used.

You can attach filters for incoming packets or for outgoing packets or both. It is usually more effective to filter incoming packets for two reasons:

- You know which interface the packet is coming in on
- You can protect the PortMaster itself

Setting IP Filters

IP rules are specified using the following syntax:

```
action [[source_addr/mask dest_addr/mask] protocol [option]] [log]
```

Each of the criteria and its options are shown in Table 10-2.

Table 10-2 Description of IP Rule Syntax

Criteria	Options	Description
action	permit	Permits the packet to pass through the interface.
	deny	Stops the packet from passing through the interface. The packet is dropped and an ICMP Host Unreachable message is sent to the source address.
source_addr/ mask		Specifies the comparison with the source IP address of the packet. The number of high-order bits of the source IP address is determined by the mask. Common mask values are: 0—To match all packets with any source address 16—Looks only at network number of class B IP addresses 24—Looks only at network number of class C IP addresses 32—Looks at the entire IP address
dest_addr/ mask		Specifies the comparison with the destination IP address contained in the packet. The number of high-order bits of the destination IP address is determined by the mask.
protocol	TCP	Specifies that the filter looks for TCP packets. This type of rule supports filtering on source and destination port numbers as well as the established state of the connection.
	UDP	Specifies that the filter looks for UDP packets. This type of rule supports filtering on source and destination port numbers.
	ICMP	Specifies that the filter looks for ICMP packets. This rule supports filtering on the type of ICMP message. The only option for this rule is: [type icmp_message_type] A comparison is made with the ICMP message type contained in the packet. ICMP message types are defined in RFC 1700, "Assigned Numbers."

Table 10-2 Description of IP Rule Syntax (Continued)

Criteria	Options	Description
option		The options depend on the protocol specified. The TCP options are described in Table 10-3. The UDP options are described in Table 10-4. The ICMP option is described in the ICMP option above.
log		If this rule is matched a syslog message is sent to the loghost with <code>auth.notice</code> facility and priority.

The syntax for TCP options is shown below and the options are explained in Table 10-3:

```
[src eq|gt|lt port_number] [dst eq|gt|lt port_number] [estab]
```

Table 10-3 TCP Rule Options

Option	Description
src	Compare the port number in the filter with the TCP source port number
dst	Compare the port number in the filter with the TCP destination port number
eq	The port number in the packet should be tested to see if it is equal to the port number specified in the rule
gt	The port number in the packet should be tested to see if it is greater than the port number specified in the rule
lt	The port number in the packet should be tested to see if it is less than the port number specified in the rule
estab	Determine if the packet is for an established TCP network connection. Packets being sent to start new TCP connections do not match this rule.

The syntax for UDP options is shown below and the options are explained in Table 10-4:

```
[src eq|gt|lt port_number] [dst eq|gt|lt port_number]
```

Table 10-4 UDP Rule Options

Option	Description
src	Compare the port number in the filter with the UDP source port number
dst	Compare the port number in the filter with the UDP destination port number
eq	The port number in the packet should be tested to see if it is equal to the port number specified in the rule
gt	The port number in the packet should be tested to see if it is greater than the port number specified in the rule
lt	The port number in the packet should be tested to see if it is less than the port number specified in the rule

Table 10-5 lists common TCP and UDP services. A more complete list is available in RFC 1700, “Assigned Numbers.” If you are configuring filters with PMconsole, you can use the service name or number for the port, as found in the `/etc/services` file on most hosts. If you are configuring filters from the command line interface, you must use the port number, not the name.

Table 10-5 TCP and UDP Port Services

Service	Port	Type	Description
ftp-data	20	tcp	File Transfer (Default Data)
ftp	21	tcp	File Transfer (Control)
telnet	23	tcp	Telnet
smtp	25	tcp	Simple Mail Transfer (email)
nicname	43	tcp	Who Is
nicname	43	udp	Who Is

Table 10-5 TCP and UDP Port Services (Continued)

Service	Port	Type	Description
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	Gopher
gopher	70	udp	Gopher
finger	79	tcp	Finger
finger	79	udp	Finger
www-http	80	tcp	World Wide Web HTTP
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Authentication Service
auth	113	udp	Authentication Service
nntp	119	tcp	Network News Transfer Protocol
ntp	123	tcp	Network Time Protocol
ntp	123	udp	Network Time Protocol
snmp	161	tcp	SNMP
snmp	161	udp	SNMP
snmptrap	162	tcp	SNMPTRAP
snmptrap	162	udp	SNMPTRAP
imap3	220	tcp	Interactive Mail Access Protocol v3
imap3	220	udp	Interactive Mail Access Protocol v3
exec	512	tcp	remote process execution
login	513	tcp	remote login

Table 10-5 TCP and UDP Port Services (Continued)

Service	Port	Type	Description
who	513	udp	remote who (rwhod)
cmd	514	tcp	remote command (rsh)
syslog	514	udp	System Log Facility
printer	515	tcp	lpd spooler
talk	517	tcp	terminal to terminal chat
talk	517	udp	terminal to terminal chat
ntalk	518	tcp	newer version of terminal to terminal chat
ntalk	518	udp	newer version of terminal to terminal chat
router	520	udp	RIP
uucp	540	tcp	UNIX to UNIX Copy
uucp	540	udp	UNIX to UNIX Copy
uucp-rlogin	541	tcp	a different variant of UUCP/TCP
uucp-rlogin	541	udp	a different variant of UUCP/IP
klogin	543	tcp	Kerberized login
klogin	543	udp	Kerberized login
pmd	1642	tcp	PortMaster daemon in.pmd
pmconsole	1643	tcp	PortMaster Console Protocol
radius	1645	udp	Remote Authentication Dial In User Service
radacct	1646	udp	RADIUS Accounting

Setting IPX Filters

IPX rules are specified using the following syntax:

```

        action [keyword value] [keyword value] ...
    
```

Each of the valid keywords are shown in Table 10-6.

Table 10-6 Description of IPX Rule Syntax

Option/Keyword	Description
action	The two options for action are permit and deny. Permit allows the packet to pass freely through the interface. Deny stops the packet from passing through the interface.
srcnet	Compares the stated value with the source IPX network address of the packet. This value must be in hexadecimal format.
dstnet	Compares the stated value with the destination IPX network address in the packet. This value must be in hexadecimal format.
srchost	Compares the stated value with the source IPX node address in the packet. This value must be in hexadecimal format.
dsthost	Compares the stated value with the destination IPX node address in the packet. This value must be in hexadecimal format.
srcsocket	Compares the stated value with the source IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid values for the second keyword are: eq, lt, or gt. The value follows the second keyword.
dstsocket	Compares the stated value with the destination IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid values for the second keyword are: eq, lt, or gt. The value follows the second keyword.

Setting SAP Filters

SAP can be filtered on output. SAP rules are specified using the following syntax:

```
action [keyword value] [keyword value] ...
```

Each of the valid keywords are shown in Table 10-7.

Table 10-7 Description of SAP Rule Syntax

Option/Keyword	Description
action	The two options for action are permit and deny. Permit allows the SAP entry to be broadcast in SAP packets. Deny stops the SAP entry from being sent in SAP broadcasts.
server	Compares the value with the name of the server which is advertising its service. The server value is case-sensitive.
network	Compares the stated value with IPX network address of the server. This value must be in hexadecimal format.
host	Compares the stated value with the IPX node address of the server. This value must be in hexadecimal format.
socket	Compares the stated value with the IPX socket number of the server. A second keyword indicating the type of comparison must be specified. Valid values for the second keyword are: eq, lt, or gt. The value follows the second keyword.

Filtering FTP Packets

Filters can be used to either permit or deny FTP packets. It is important to understand how this protocol works before you develop FTP filters.

File Transfer Protocol (FTP) uses TCP port 21 as a control channel, but it transfers data on another channel initiated by the FTP server from TCP port 20 (FTP-data). Therefore, if you want to allow your internal hosts to FTP outward, you must allow external hosts to open an incoming connection from TCP port 20 to a destination port above 1023. Allowing this type of access to your network can be very risky if you are running RPC or X Windows on the host from which you are FTPing. As a result, many sites use FTP proxies or passive FTP, neither of which is discussed in this guide.

However, *Firewalls and Internet Security: Repelling the Wily Hacker* by Cheswick and Bellovin (Addison-Wesley 1994, ISBN 0-201-63357-4) and *Building Internet Firewalls* by Chapman and Zwicky (O'Reilly & Associates 1995, ISBN 1-56592-124-0) are good references.

Likewise, if you want to allow external hosts to connect to your FTP server and transfer files, you must allow incoming connections to TCP port 21 on your FTP server and allow outgoing connections from TCP port 20 of your FTP server.

In the following examples, ftp.edu.com is the name of your FTP server and proxy.edu.com is the name of the host from which you allow outgoing FTP.

```
internet.in filter
permit tcp 0.0.0.0/0 proxy.edu.com/32 src eq 20 dst gt 1023
permit tcp 0.0.0.0/0 proxy.edu.com/32 src eq 21 estab
permit tcp 0.0.0.0/0 ftp.edu.com/32 dst eq 21
permit tcp 0.0.0.0/0 ftp.edu.com/32 src gt 1023 dst eq 20 estab
```

```
internet.out filter
permit tcp proxy.edu.com/32 0.0.0.0/0 dst eq 21
permit tcp proxy.edu.com/32 0.0.0.0/0 src gt 1023 dst eq 20 estab
permit tcp ftp.edu.com/32 0.0.0.0/0 src eq 20 dst gt 1023
permit tcp ftp.edu.com/32 0.0.0.0/0 src eq 21 dst gt 1023 estab
```

If you allow any internal host to FTP outwards, replace proxy.edu.com/32 with 0.0.0.0/0 or your *network_number*/24. Take appropriate precautions to reduce the risk this configuration creates.



Note – This configuration is not recommended if you run any of the following protocols on any of the hosts from which you allow ftp access: NFS, X, RPC, or any other service that listens on ports above 1023.

Filter Examples

Filters are very flexible; therefore, it is very important that you evaluate the types of traffic that a specific filter permits or denies through an interface before attaching the filter. If possible, filters should be tested from both sides of the filtering interface to verify that the filter is operating as you intended. The `log` keyword is very useful when testing and refining filters.



Note – Any packet that is not explicitly permitted by a filter is denied, except for the special case of a filter with no rules, which permits everything.

Simple Filter Example

The filter is written as follows:

```
permit udp dst eq domain
permit tcp dst eq smtp
permit icmp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit tcp src eq ftp-data dst gt 1023
```

Table 10-8 shows the description of the filter.

Table 10-8 Description of Simple Filter

Rule	Description
1	Permits Domain Name Service (DNS) UDP packets from any host to any host.
2	Permits SMTP (mail) packets.
3	Permits ICMP packets, including ping packets.
4	Permits FTP from any host but only to the host ftp.edu.com.
5	Permits FTP data to return to the requesting host. This rule is required to provide a reverse channel for the data portion of FTP.

Filter for Internet Connection on a Hardwired Port

The filter in this example is designed as an input filter for a hardwired network interface set up to connect to the Internet. If this filter were used for dial on-demand connections it should be attached to the appropriate user and location. The filter is written as follows:

```
deny 192.168.1.0/24 0.0.0.0/0 log
permit tcp estab
permit 0.0.0.0/0 mail.edu.com/32 tcp dst eq smtp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit tcp 0.0.0.0/0 www.edu.com/32 dst eq www-http
permit tcp src eq ftp-data dst gt 1023
permit udp dst eq domain
permit tcp dst eq domain
permit icmp
```

Table 10-9 describes the filter.

Table 10-9 Description of Internet Filter

Rule	Description
1	Deny any incoming packets from your own network (192.168.1.0). This blocks IP spoofing attacks. Log the header information using syslog.
2	Permits already established TCP connections.
3	Permits SMTP connections to the mail server mail.edu.com.
4	Permits FTP to the host ftp.edu.com.
5	Permits www (http) access to the host www.edu.com.
6	Permits FTP data channel.
7	Permits Domain Name Service.
8	Permits Domain Name Service zone transfers. (You may wish to restrict this rule to allow only connections to your name servers.)
9	Permits ICMP packets.

Domain Name Server is Outside Your Local Net

If the DNS name server for your domain is outside your local net you should add the following rule to your input filter:

```
permit udp src eq domain
```

This permits DNS replies into your local net. You should then add the following output filter described in Table 10-10 to the interface:

```
deny 0.0.0.0/0 192.168.1.0/24 log
permit tcp
permit udp src eq domain
permit udp dst eq domain
permit gw.edu.com/32 rt.isp.net/32 udp dst eq 520
permit icmp
```

Table 10-10 Description of External DNS Output Filter

Rule	Description
1	Denies any outgoing packets to your own network (192.168.1.0) and makes a log.
2	Permit any TCP connection.
3	Permit Domain Name Service replies from your network.
4	Permit Domain Name Service queries from your network.
5	Permits outgoing RIP packets from the PortMaster (gw.edu.com) to the router (rt.isp.net) at the other end of the serial link.
6	Permit ICMP packets.



Note – Since the PortMaster does not apply filter rules to its own UDP and ICMP packets, rule 5 is not necessary. However, if you are broadcasting routing through this interface it is a good idea to include this rule in case PortMaster behavior is changed in the future.

Filter to Listen to RIP Information

To permit incoming RIP packets, add the following rule to your input filter:

```
permit rt.isp.net/32 gw.edu.com/32 udp dst eq 520
```

Filter to Allow Auth Queries

To allow auth queries used by some mailers and FTP servers, add the following rule to your input filter:

```
permit tcp dst eq 113
```

For more information about these types of queries, refer to RFC 1413.

Limiting Access to Specified Hosts

Security on your network can be increased if you limit the authorized activities for certain hosts. For example, you can limit the DNS and SMTP interchange with the Internet to a single well-secured host on your network. All Internet hosts would then access this single server for those services. If you have several name servers or mail servers, you can use additional rules to allow access to these servers.

To allow some other network (172.16.12.0) to have complete access to your network, add the following rule:

```
permit 172.16.12.0/24 192.168.1.0/24
```



Caution – Beware of associative trust. If 192.168.1 trusts 172.16.12 and 172.16.12 trusts 10.5.137, then 192.168.1 trusts 10.5.137 whether 192.168.1 knows it or not.

Restrictive Internet Filter

This filter is an example of an input filter for a network hardwired port. If you use dial on-demand you should add this filter to the appropriate Location Table entry.

This example allows any kind of outgoing connection from the Internet server but blocks all incoming traffic to any host but your designated Internet server. This filter allows incoming SMTP, NNTP, DNS, FTP, and ICMP traffic to the Internet server and blocks all other traffic.



Note – Unless you have the latest versions of `ftpd`, `httpd`, and `sendmail` you may be vulnerable to attacks through these ports. Check the latest CERT advisories, available on ftp.cert.org, for existing vulnerabilities.

In the following example, the name `server` should be replaced by the IP address or host name of your Internet server.

```
deny 192.168.1.0/24 0.0.0.0/0 log
permit 0.0.0.0/0 server/32 tcp estab
permit 0.0.0.0/0 server/32 tcp dst eq ftp
permit 0.0.0.0/0 server/32 tcp src eq ftp-data dst gt 1023
permit 0.0.0.0/0 server/32 tcp dst eq nntp
permit 0.0.0.0/0 server/32 tcp dst eq smtp
permit 0.0.0.0/0 server/32 tcp dst eq www-http
permit 0.0.0.0/0 server/32 udp dst eq domain
permit 0.0.0.0/0 server/32 tcp dst eq domain
permit 0.0.0.0/0 server/32 icmp
```

Table 10-11 describes the filter.

Table 10-11 Description of Restrictive Internet Filter

Rule	Description
1	Denies any incoming packets from your own network (192.168.1.0) and makes a log.
2	Permits packets from any established TCP connection to the Internet server.
3	Permits FTP from any one to the Internet server.

Table 10-11 Description of Restrictive Internet Filter

Rule	Description
4	Permits FTP data back channel.
5	Permits incoming NNTP (news) to the Internet server.
6	Permits incoming SMTP (mail) to the Internet server.
7	Permits www (http) requests to the Internet server.
8	Permits Domain Name Service queries to the Internet server.
9	Permits DNS zone transfers from the Internet server.
10	Permits ICMP to the Internet server. You can further limit ICMP to types 0, 3, 8, and 11 using four rules instead of one. See <i>RFC 1700</i> for the list of ICMP packet types.

To log all blocked packets add the following rule to the end of your filter:

```
deny log
```

Access Filters

Access filters allow you to limit access to a specified host or group of hosts. Interactive users, those using telnet and rlogin, can be allowed to select a host for their sessions. However, you may want to limit their access to specific hosts or networks. An access control filter allows you to designate a limited set of hosts or networks accessible by the user when they are presented with the “Host:” prompt.

Connecting a Branch Office to the Main Office

11

This chapter describes how to use the PortMaster to connect your office to another office using a dial on-demand configuration. This type of connection is designed to take the place of a costly dedicated line between the two locations, where the amount and duration of traffic does not justify a leased line or Frame Relay connection.

The following topics are described:

- Overview of the configuration
- Description of hardware configuration
- Description of software configuration on the PortMaster in the branch office
- Description of the software configuration on the PortMaster in the main office
- Testing the configuration
- How to setup multi-line load-balancing
- Using ISDN for on-demand connections

Overview of Main Office Connection Configuration

The configuration described in this chapter can be implemented with any PortMaster, however, the PortMaster Office Router is used in this example.

The PortMaster Office Router is designed to provide cost-effective connectivity between small remote (branch) offices and larger headquarters (main) offices. These types of connections are typically established on an as-needed basis. For most applications it is not cost-effective to maintain a continuous connection when a connection can be established to transfer network traffic when necessary. These types of connections are usually handled by a dial on-demand link.

A dial on-demand link establishes a connection with the specified location when network traffic is queued. The PortMaster Office Router OR-M is designed to support a dial on-demand connection with another office using the PCMCIA modem port, designated S1. Figure 11-1 shows an example of this configuration. The console port, S0, can be used as a console or an external modem can be connected to provide an additional dial on-demand port for multi-line load-balancing during peak traffic periods.

The PortMaster Office Router-ISDN (OR-U) has an ISDN BRI port designated S1/S2 instead of a PCMCIA modem port. The ISDN port can be used for ISDN dial on-demand connections.

The example in this chapter uses the PCMCIA asynchronous modem port on the OR-M. To use the ISDN port on the OR-U, see “Using ISDN for On-Demand Connections” on page 11-15.

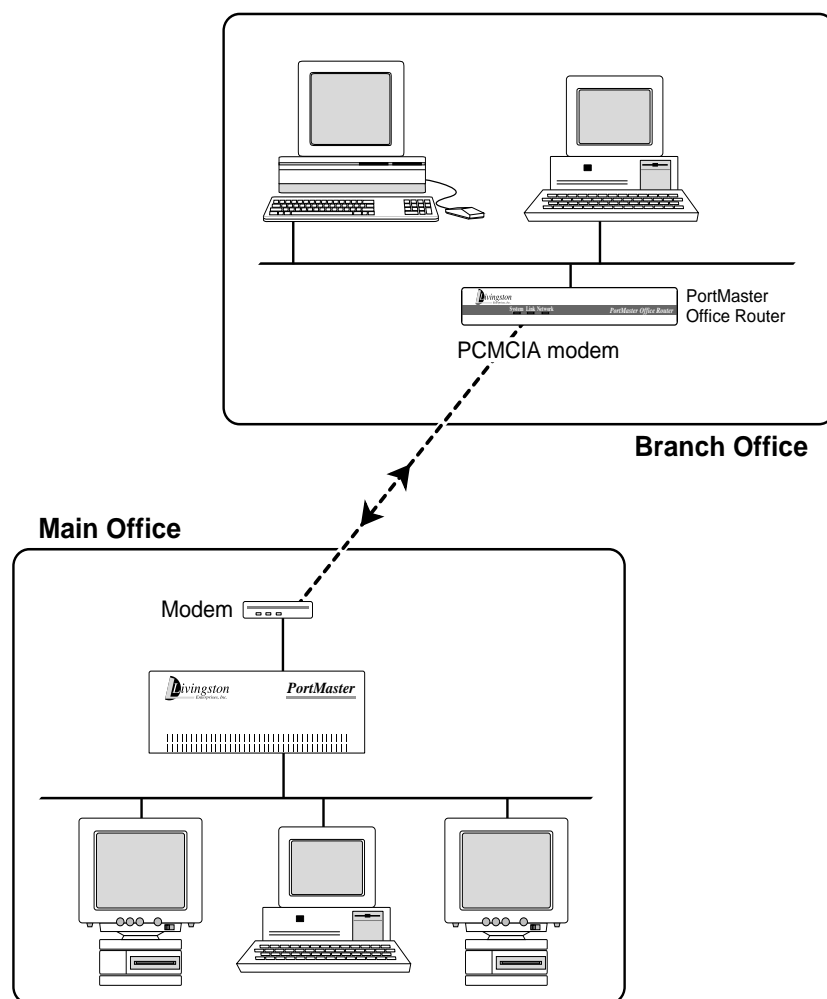


Figure 11-1 Office to Office Dial On-Demand Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster Office Router located in a branch office with a PortMaster of some type in a main office. This connection is initiated on an on-demand basis whenever traffic for the other office is queued at either end. The on-demand connection is configured for dial-in and dial-out operation using the PCMCIA port, S1. The variables shown in Table 11-1 are used in this example. Change variable values to actual values that reflect your network.

Table 11-1 Example Configuration Variables

Variable Description	Value for this Example
Name of router in the branch office	branch
IP address of router in the branch office	192.168.200.1
Network type and number	Class C 192.168.200.0
IPX network of router in the branch office	000000F3
IPX Frame Type	IEEE 802.2 on Ethernet
Name of PortMaster router in the main office	hq
IP address of router hq in the main office	192.168.1.1
Network type and number of router hq in the main office	Class C, 192.168.1.0
IPX network of router in the main office	000000F1
IPX network for the serial link	000000F2
Idle Timeout	5 minutes

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch(es) appropriately.**
3. **Connect the power cable.**

4. **Insert the PCMCIA modem card into the PCMCIA slot marked S1.**
5. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

6. **Turn on the power switch.**

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

7. **Press [Return] on the console.**

The PortMaster login prompt is displayed.

8. **Type !root then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

9. **Press [Return] at the password prompt.**

10. **Set the password on the PortMaster by typing:**

```
Command> set password password
```

This step is optional but highly recommended.

11. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

12. **Set the netmask and broadcast values if necessary.**

13. **Save the address to the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```


14. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:

```
Command> quit
```

Configuring the Software on the Router in the Branch Office

In order to use the PMconsole graphical user interface to configure the Office Router, you must install the software on a UNIX workstation or a Microsoft Windows compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 11-2. These values only apply to this example; use values appropriate for your network.

Table 11-2 Global Parameter Values

Parameter	Value
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Sysname	branch

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 11-3.

Table 11-3 Ethernet Parameter Values

Parameter	Value
Protocol	PPP/IP/IPX
IPX Network	000000F3
IPX Frame Type	802.2
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the PCMCIA Serial Port Parameters

The PCMCIA modem port on the PortMaster Office Router is designated S1. Configure the port parameters with the values shown in Table 11-4. The PCMCIA modem must be installed in order to configure port S1.

Table 11-4 PCMCIA (s1) Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Dial In&Out (or twoway for command line)
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise. Use the highest DTE speed supported by your modem.
Speed 2	Same as speed 1

Table 11-4 PCMCIA (s1) Port Parameter Values (*Continued*)

Parameter	Value
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Idle Timeout	5 minutes
Dial Group	1

All the other parameters should be left at their default values. For more information about asynchronous ports and configuring your modem, refer to Chapter 6, “Configuring an Asynchronous Port.”

Defining a Dial-In User

A user account must be set up on the router in the branch office so the PortMaster in the main office can dial in when traffic is queued at the main office. The new user hq should be configured with the parameter values shown in Table 11-5.

Table 11-5 User Table Parameter Values for User hq

Parameter	Value
User Name	hq
Password	anypasswd (The password must match the password used in the dial script set on the PortMaster in the main office for location branch.) Do not use the same password used for the administrative !root login.
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)

Table 11-5 User Table Parameter Values for User hq (Continued)

Parameter	Value
MTU	1500
Compression	On (Unless using multi-line load-balancing.)

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location

A location entry on the PortMaster Office Router in the branch office must be created for the location identified as hq. This allows the Office Router in the branch office to call the PortMaster in the main office when network traffic is queued. The new location hq should be configured with the parameter values shown in Table 11-6.

Table 11-6 Location Table Parameter Values for Location hq

Parameter	Value
Location Name	hq
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP/IP/IPX
IP Destination	Specified 192.168.1.1 (Allows the PortMaster to know when to dial after the Type is switched to On-Demand later.)
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (Unless using multi-line load-balancing.)
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)

Table 11-6 Location Table Parameter Values for Location hq (Continued)

Parameter	Value
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	1
Send and Expect Pairs	Send: ATDT5551212\r Expect: CONNECT Send: \r Expect: ogin: Send: branch\r Expect: ssword: Send: anypasswd\r Expect: PPP

For more information about configuring Location Table parameters, refer to Chapter 9, “Configuring Dial-Out Locations.”

After the port, user, and location parameters are entered, the port should be reset to make the new configuration active.

Configuring the Software on the PortMaster in the Main Office

In our example, the remote machine is the PortMaster in the main office. To configure this PortMaster to dial the branch office when there is any traffic queued, you must configure the main office exactly the same as the branch office except that the names and addresses are reversed as described in the following subsections.

Setting the Port Parameters

For all ports that you want enabled for dial-in and out to branch, enter the values shown for the parameters in Table 11-7.

Table 11-7 Dial-Out Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Dial In&Out (or twoway for command line)

Table 11-7 Dial-Out Port Parameter Values (Continued)

Parameter	Value
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual advises otherwise
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Idle Timeout	5 minutes (If you are also using the PortMaster in the main office for user dial in, you want to set this parameter higher or off.)
Dial Group	1

Defining a Dial-In User

A user account must be set up on the PortMaster in the main office so the router in the branch office can dial in when traffic is queued. The new user branch should be configured with the parameter values shown in Table 11-8.

Table 11-8 User Table Parameter Values for User branch

Parameter	Value
User Name	branch
Password	anypasswd (The password must match the password used in the dial script set on the PortMaster in the branch office for location hq.) Do not use the same password used for the administrative !root login.
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F2

Table 11-8 User Table Parameter Values for User branch (*Continued*)

Parameter	Value
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (Unless using multi-line load-balancing.)

Defining a Dial-Out Location

A location entry on the PortMaster in the main office must be created for the location identified as branch. This allows the PortMaster in the main office to call the PortMaster in the branch office when network traffic is queued. The new location branch should be configured with the parameter values shown in Table 11-9.

Table 11-9 Location Table Parameter Values for Location branch

Parameter	Value
Location Name	branch
Type	Manual (The location is set for manual dialing until configuration has been tested. After verification, the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (If you are not using multi-line load-balancing.)
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0
Send and Expect Pairs	Send: ATDT5551020\r Expect: CONNECT Send: \r Expect: ogin: Send: hq\r Expect: ssword: Send: anypasswd\r Expect: PPP

Reset the port to make the new settings active.

Testing the Setup

The configuration should be tested before either of the locations are set for On-Demand dialing. To test the configuration, follow these steps:

- 1. Use the Dialer to connect from branch to hq.**

If you are using PMconsole, select Dialer from the View menu. Set the Watch Dialer parameter to Yes. If you are using the command line interface, type the following:

```
Command> set console  
Command> set debug 0x55  
Command> dial hq
```

- 2. Monitor the dial and connect sequence between the two locations.**

- 3. If everything connects as expected, reset the port on the Office Router in the branch office and change the location Type parameter to On Demand.**

To reset the port, click the reset button on the Port window or type `reset s1` at the command prompt.

- 4. If there is a problem, reset the port on the Office Router in the branch office and change the dial script or other parameters. Dial the main office again. Repeat this procedure until the connection is made correctly.**

- 5. Repeat steps 1 through 4, dialing from the main office to the branch office.**

Setting the Console Port for Multi-line Load-balancing

Multi-line load-balancing is used to add additional lines when network traffic is heavy. If more than one line to the same location is established, the PortMaster balances the traffic among the lines. To configure the Office Router for multi-line load-balancing, an external modem must be attached to the console port.



Note – TCP/IP header compression cannot be used with multi-line load-balancing.

In this example the console port is being configured for use as another serial port. Once you set this configuration, the port is no longer used for the system console. Figure 11-2 diagrams the multi-line load-balancing configuration.

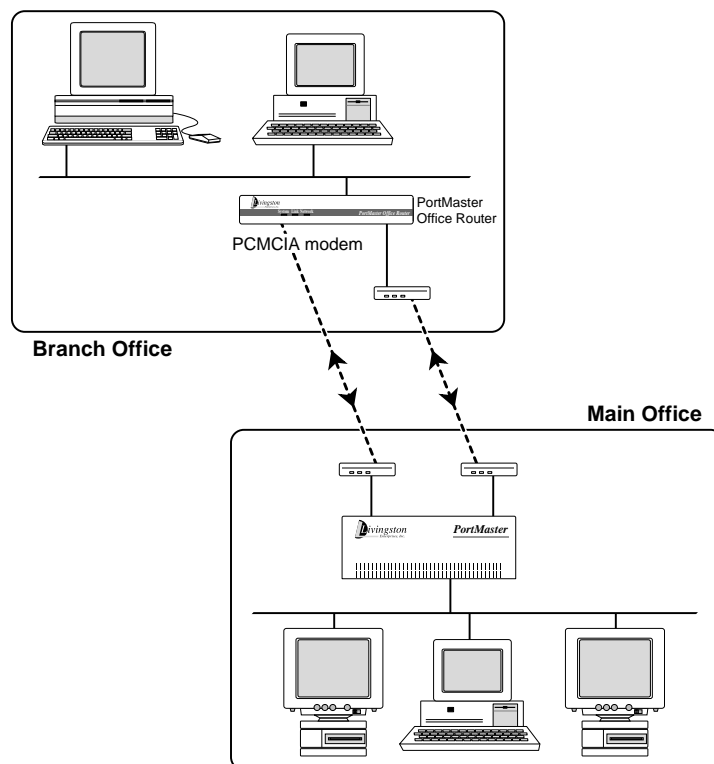


Figure 11-2 Multi-line Load-Balancing

To enable multi-line load-balancing, you must configure the S0 port using the same parameters as shown for the PCMCIA port in Table 11-4. When you configure the location hq on the router in the branch office use the parameter values shown in Table 11-10.

Table 11-10 Location (hq) Parameter Values for Load-Balancing

Parameter	Value
Maximum Ports	2

Table 11-10 Location (hq) Parameter Values for Load-Balancing

Parameter	Value
High Water Mark	100 bytes

The value of the High Water Mark parameter depends on the type of traffic and how many queued bytes of traffic you want before the second line is used.

Using ISDN for On-Demand Connections

Using the ISDN BRI port on the PortMaster Office Router-ISDN (OR-U) is very similar to using the PCMCIA port on the OR-M, except you must do the following:

- Configure the ISDN switch type as a global parameter
- Set the SPID on the port
- Do not set the port speed, flow control, or modem control
- Use a V.25bis dialing script in the Location Table setup

For more information about ISDN connections, see Chapter 18, “ISDN Connections” and for information about V.25bis dialing scripts, see Chapter 9, “Configuring Dial-Out Locations.”

This chapter describes how to configure the PortMaster to establish a continuous connection to an Internet Service Provider (ISP). This creates a gateway from your office to the Internet using a dial-out connection through one of the serial ports on your PortMaster. Internet connections can also be set for on-demand operation. For more information about on-demand connections, refer to Chapter 9, “Configuring Dial-Out Locations” and Chapter 11, “Connecting a Branch Office to the Main Office.”

The following topics are discussed:

- Overview of establishing continuous connections
- Setting a dial out Internet connection using a modem port
- Setting a hardwired connection to the Internet using a modem port
- Setting packet filtering

Overview of the Continuous Internet Configuration

Continuous connections from serial ports are used to establish a constant link with another location over a dial up telephone line. In the configurations described in this chapter, the PortMaster is configured for a continuous dial-up connection with an Internet Service Provider (ISP) using dial-up or dedicated lines. Figure 12-1 shows an example of this configuration.

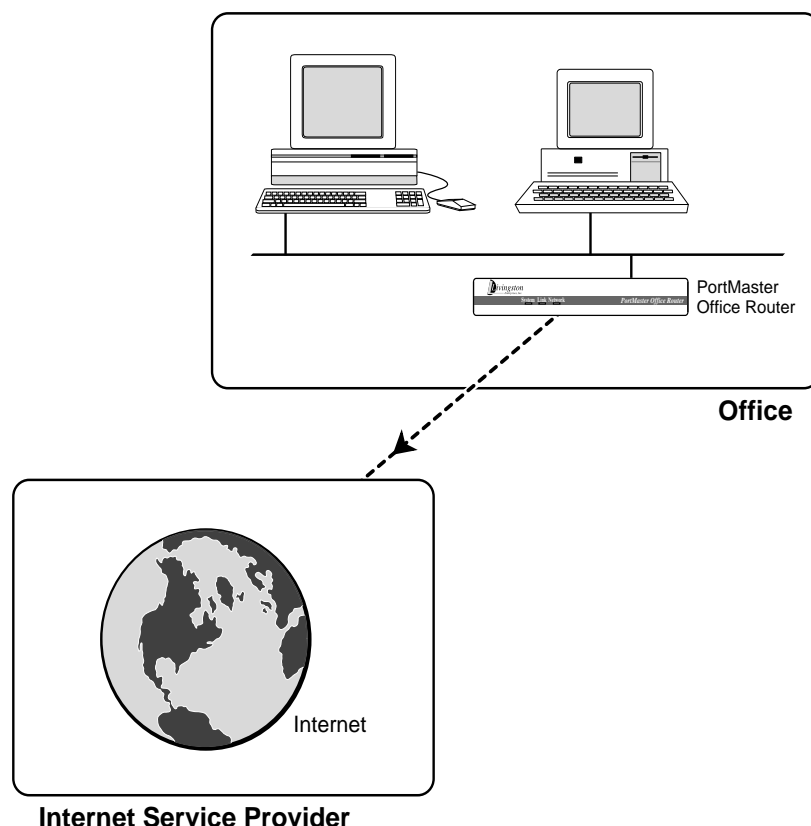


Figure 12-1 Continuous Internet Connection

Description of the Example Configuration

The example described in this chapter connects a PortMaster located in an office with an Internet Service Provider (ISP). If you use a continuous dial-out link from the S1 serial port, one Location Table entry is needed for the ISP. If you use a network hardwired port, no entries are needed in the Location Table.

A continuous dial-out connection starts as soon as the PortMaster boots and is redialed whenever the telephone connection is dropped. The network hardwired configuration is typically used if you are using a leased analog line or an asynchronous to synchronous converter. Both of these configurations are described in this chapter. For this example, IPX packets are not transmitted to or from the Internet Service Provider.

The connection to the ISP can also be configured for dial on-demand operation, as described in Chapter 11, “Connecting a Branch Office to the Main Office.” However, dial on-demand ISP connections do not allow Internet users access to your site when the dial-up connection is not established.



Note – Network connections using synchronous ports are described in Chapters 15 through 18.

The examples shown use the variables listed in Table 12-1. Change these values to reflect your network.

Table 12-1 Example Configuration Variables

Variable Description	Value for this Example
Name of router in office	office
IP address of router in office	192.168.200.1
Network type and number	Class C 192.168.200.0
Timeout for hang up	0 minutes (never hang up)
Network protocol	PPP
IP address of the ISP	192.168.5.6
Name of the ISP	isp

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network DIP switch(es) appropriately.**
3. **Connect the power cable.**
4. **Connect a modem to the serial port you are using for this configuration.**

5. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

6. **Turn on the power switch.**

The PortMaster performs power on self diagnostics. The self diagnostics are displayed on the console if the console DIP switch is UP.

7. **Type `!root` at the login: prompt, then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A message is displayed with the new IP address.

10. **Set the netmask and broadcast values if necessary.**

11. **Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

12. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software on the PortMaster

In order to use PMconsole to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

Setting Global Parameters

Set the name of the system to “office” using the System Name parameter. If you are using PMconsole, this parameter is found in the SNMP Window. Refer to your *Administrator’s Guide* for more information.

Set the Default IP Gateway parameter to the address of your ISP’s router.

For this configuration, none of the other global parameters need to be set. However, you may want to define some of these parameters for your installation.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 12-2.

Table 12-2 Ethernet Port Parameter Values

Parameter	Value
Protocol	IP
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet port parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Serial Port Parameters for Dial-Out

For continuous dial out on a serial port, configure the port parameters with the values shown in Table 12-3.

Table 12-3 Serial Port Parameter Values for Continuous Dial Out

Parameter	Value
Port Type	Network
Network Type	Dial Out

Table 12-3 Serial Port Parameter Values for Continuous Dial Out (Continued)

Parameter	Value
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise.
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Dial Group	1

All the other parameters should be left with their default values. For more information about the asynchronous ports and configuring modems, refer to Chapter 6, “Configuring an Asynchronous Port.”

Setting the Serial Port Parameters for a Hardwired Connection

To establish a hardwired connection on a serial port, configure the port parameters with the values shown in Table 12-4.

Table 12-4 Serial Port Parameter Values for a Hardwired Port

Parameter	Value
Port Type	Network
Network Type	Hardwired
Protocol	PPP
MTU	1500
Speed 1	Use 115200 if the attached device supports this speed. Otherwise, use the speed suggested by the device manual.
Modem Control	On (If using a modem or CSU/DSU.) Off (If using a direct physical connection.)
Flow Control	RTS/CTS

Table 12-4 Serial Port Parameter Values for a Hardwired Port (*Continued*)

Parameter	Value
IP Destination	192.168.5.6
Netmask	255.255.255.0 for a Class C address
Routing	Typically Off; however, your ISP may request that you set this parameter to Broadcast.
Compression	Enabled

All the other parameters should be left with their default values. For more information about asynchronous ports, refer to Chapter 6, “Configuring an Asynchronous Port.”

Defining a Dial-Out Location

If you are using a continuous dial-out link, a location entry on the PortMaster must be created for the location identified as isp. This allows the PortMaster to establish a connection with the Internet Service Provider as soon as it is booted. The new location isp should be configured with the parameter values shown in Table 12-5, or as instructed by your ISP.

Table 12-5 Location Table Parameter Values for Location isp

Parameter	Value
Location Name	isp
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified, change the Type to Continuous.)
Protocol	PPP
IP Destination	Specified 192.168.5.6
Netmask	255.255.255.0
Routing	Typically Off; however, your ISP may request that you set this parameter to Broadcast.
MTU	1500
Compression	On (If you are not using multi-line load-balancing.)

Table 12-5 Location Table Parameter Values for Location isp (Continued)

Parameter	Value
Input Filter	internet.in
Output Filter	internet.out (if needed)
Idle Timeout	0
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	1
Send and Expect Pairs	Send: ATDT5551212\r Expect: CONNECT Send: \r Expect: ogin: Send: office\r Expect: ssword: Send: passwd\r Expect: PPP



Note – The strings you send following the login: and password: prompts must be provided to you by your ISP. Your chat script may differ from this example depending on your ISP.

You can also authenticate using CHAP if it is supported by the ISP. To use CHAP authentication, use only the first Send and Expect string in the chat script shown above. You must also create a user called “isp” with the password “passwd.” For more information about configuring users, refer to Chapter 8, “Configuring Dial-In Users.” For more information about configuring Location Table parameters, refer to Chapter 9, “Configuring Dial-Out Locations.”

After the configuration is entered and saved, the port should be reset to make the new settings active.

Testing the Continuous Dial-Out Setup

The configuration should be tested before the location isp is set for continuous dialing. To test the configuration, follow these steps:

- 1. Use the Dialer to connect to the ISP.**

Select Dialer from the PMconsole View menu. Set the Watch Dialer parameter to Yes. If you are using the command line interface, type: `dial isp -x`

- 2. Monitor the dial and connect sequence between the two locations.**

- 3. If everything connects as expected, reset the port and change the Location Type parameter to Continuous.**

- 4. If there is a problem, reset the port and change the dial script or other parameters. Dial the ISP again. Repeat this procedure until the connection is made correctly.**

Contact your ISP if you are unable to connect as expected. They may be able to provide additional information.



Note – You may need to get specific dial script examples from the ISP before configuring the location.

Testing the Network Hardwired Setup

To test the configuration, follow these steps:

- 1. Reset the newly configured serial port.**

The network hardwired connection should be established within a few seconds.

- 2. Verify that the connection becomes ESTABLISHED.**

Use the `show s1` command (if you are using port s1).

- 3. If there is a problem, check your configuration.**

Contact your ISP if you are unable to connect as expected.

Setting Network Filtering

Your connection to the Internet can be vulnerable to attack from other Internet users. Therefore, it is recommended that you add an input filter to the location isp for the continuous dial-out connection. For a hardwired connection, the input filter can be attached to the hardwired port.



Note – This section describes an example filter that may not protect your network from all forms of attack. For more information about filters, refer to “References” and Chapter 10, “Configuring Filters.”

The filter named `internet.in` is written as follows:

```
deny 192.168.200.0/24 0.0.0.0/0 log
permit tcp estab
permit 0.0.0.0/0 mail.edu.com/32 tcp dst eq smtp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit 0.0.0.0/0 www.edu.com/32 tcp dst eq www-http
permit tcp src eq ftp-data dst gt 1023
permit udp dst eq domain
permit tcp dst eq domain
permit icmp
```

Table 12-6 describes the filter.

Table 12-6 Description of Internet Filter

Rule	Description
1	Deny any incoming packets claiming to be from your own network (192.168.200.0). This blocks IP spoofing attacks and logs the attempt.
2	Permits already established TCP connections.
3	Permits SMTP connections to the mail server mail.edu.com.
4	Permits FTP to the host ftp.edu.com.
5	Permits WWW http connections to the web server www.edu.com.
6	Permits FTP data channel.

Table 12-6 Description of Internet Filter (*Continued*)

Rule	Description
7	Permits Domain Name Service.
8	Permits Domain Name Service zone transfers. (You may wish to restrict this rule to allow only connections to your name servers.)
9	Permits ICMP packets.

If your Domain Name Server is outside your local network, refer to “Domain Name Server is Outside Your Local Net” on page 10-16.

Using ISDN for Internet Connections

Using the ISDN BRI port on the PortMaster Office Router-ISDN (OR-U) is very similar to using the PCMCIA port on the OR-M, except you must do the following:

- Configure the ISDN switch type as a global parameter
- Set the SPID on the port
- Do not set the port speed, flow control, or modem control
- Use a V.25bis dialing script in the Location Table setup

For more information about ISDN connections, see Chapter 18, “ISDN Connections” and for information about V.25bis dialing scripts, see Chapter 9, “Configuring Dial-Out Locations.”

This chapter describes how to use the PortMaster to allow users access to centralized hosts and networks. This application is used by Internet Service Providers, academic environments, and corporate telecommuters. In this configuration multiple asynchronous ports are configured with modems for answering incoming calls from users who will then access a networked host connected via Ethernet to the PortMaster.

The following topics are described:

- Overview of the login user configuration
- Description of hardware configuration
- Description of an example software configuration on the PortMaster

Overview of Dial-In User Configuration

The PortMaster configuration described in this example allows up to seven 30 port PortMasters to be connected together to provide up to 210 dial-in asynchronous ports. The PortMaster communications server allows dial-in users to access a host for shell accounts and/or PPP, SLIP, or CSLIP connections. Internet Service Providers can use this example to configure their PortMasters to allow host and network access by dial-in users. The number of ports used is a function of the number of expected subscribers; one port per ten subscribers is the typical ratio, but peak usage and average usage per port should be monitored closely to determine the need for additional ports. RADIUS Accounting can help you to evaluate port usage. See the *RADIUS Administrator's Guide* for more information.

The same application can be used by companies to allow remote users access to their own accounts on the corporate network. Once users are authenticated they can access network resources as if they were connected to the corporate network directly.

Although this example uses seven PortMasters, many more can be used. With more than seven PortMasters, the configuration is the same except that the assigned pools would be arranged differently.

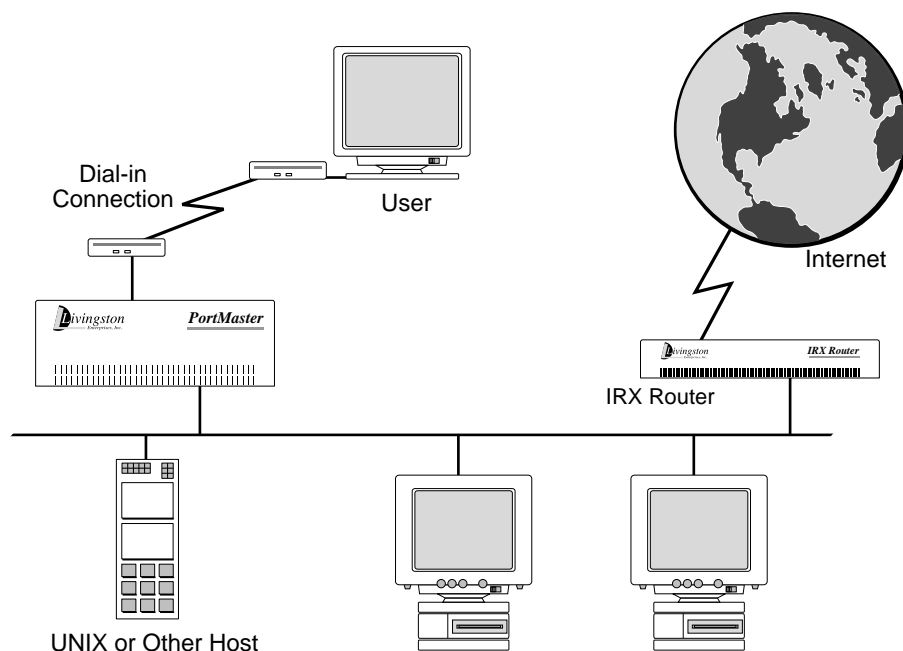


Figure 13-1 Login User Configuration

Description of Sample Configuration

The Internet Service Provider example described in this chapter uses the values shown in Table 13-1. Change variable values to actual values that reflect your network.

Table 13-1 Example Configuration Variables

Variable Description	Value for this Example
Address type	Class C assigned by your provider
Class C IP network	192.168.1.0
IP address and name of router connecting to the Internet	192.168.1.1 (gw.edu.com)
IP address and name of host running RADIUS	192.168.1.2 (rk2.edu.com)

Table 13-1 Example Configuration Variables (Continued)

Variable Description	Value for this Example
IP address and name of host running DNS	192.168.1.2 (rk2.edu.com)
IP address of RADIUS accounting server	192.168.1.2 (rk2.edu.com)
IP address of RADIUS backup accounting server	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host running backup RADIUS	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host that shell users log into	192.168.1.4 (rk4.edu.com) (Optional)
IP addresses reserved for future hosts	192.168.1.5-15, 23-32
IP address and name of first PortMaster	192.168.1.16 (pm1.edu.com)
IP addresses and names for additional PortMasters	192.168.1.17-22 (pm2.edu.com through pm7.edu.com)
Reserved pool of assigned addresses for PortMaster 1	192.168.1.33-62
Reserved pool of assigned addresses for PortMaster 2	192.168.1.65-94
Reserved pool of assigned addresses for PortMaster 3. Continue until PortMaster 7.	192.168.1.97-126
Reserved pool of assigned addresses for PortMaster 7	192.168.1.225-254

You can set the assigned pools a little closer together as long as they do not overlap, however, having the pools fall within bit boundaries makes packet filters easier to write.



Note – This example assumes you are using a PM-2E-30 PortMaster. If you are using a PM-25, the assigned pools can be moved closer together.

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switches appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Turn on the power switch.**

The PortMaster performs power on self diagnostics as it boots. The self diagnostics are displayed to the console if the console DIP switch is UP. Booting takes less than one minute.

6. **Press [Return] on the console.**

The PortMaster login prompt is displayed.

7. **Type !root then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set address 192.168.1.16
```

In this example, 192.168.1.16 is the IP address of the first PortMaster (pm1.edu.com). A confirmation message is displayed showing the new IP address.

10. **Set the netmask if it is not 24 bits and set the gateway if you need to assign a default gateway.**

- 11. Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

- 12. Exit the command mode by typing:**

```
Command> quit
```

- 13. Connect your modems to the serial ports using straight-through modem cables.**

V.34 modems that are capable of 28.8Kbps are best but V.32bis modems that run at 14.4Kbps also work. Modems slower than 14.4Kbps work but are not recommended for network users.

- 14. Make sure that the modem cables are securely fastened and that there is enough room for the modems to stay cool.**

Configuring the Software on the PortMaster

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

The UNIX version of PMconsole includes the `pmcommand` utility that allows you to define a command script and upload the script to the PortMaster. This utility is useful when you are performing the same configuration on multiple PortMasters.



Note – This example describes how to configure the first PortMaster `pm1.edu.com`. Use a similar configuration for the remaining PortMasters.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 13-2.

Table 13-2 Global Parameter Values

Parameter	Value
Default Host	192.168.1.4
Alternate Host	any other shell host, if available
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Name Service	DNS
Name Server	192.168.1.2
Domain	edu.com
Sysname	pm1
Loghost	192.168.1.2
Assigned Address	192.168.1.33

For more information about global parameters, refer to Chapter 4, “Configuring a PortMaster.”

Setting the RADIUS Parameters

RADIUS is usually implemented for user authentication when there are multiple PortMasters and more than a few dozen users. Only a few hundred users can be configured in the User Table and stored in the nonvolatile memory of the PortMaster. This example assumes the use of RADIUS.

The RADIUS parameters are given in Table 13-3, however for information about RADIUS and its parameters, refer to the *RADIUS Administrator's Guide* or FTP from <ftp://ftp.livingston.com/pub/livingston/radius/radius.install>.

Table 13-3 RADIUS Parameter Values

Parameter	Value
Secret	anyvalue (Must be the same secret for pm1.edu.com in the /etc/raddb/clients file on the RADIUS server.)
Authentication Server	192.168.1.2
Alternate Authentication Server	192.168.1.3 (optional) This server must have an identical RADIUS database.
Accounting Server	192.168.1.2
Alternate Accounting Server	192.168.1.3 (optional) This must be another RADIUS server.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 13-4.

Table 13-4 Ethernet Parameter Values

Parameter	Value
IP Address	192.168.1.16
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Asynchronous Port Parameters

The serial modem ports are designated S0 through S29 on the PortMaster. If you are using PMconsole, you can configure one port and clone the configuration to the other serial ports. If you are using the command line interface, use the `set all` command to set the same values for each of the serial ports. The port parameters shown in Table 13-5 can be set on all asynchronous ports. Use the Modem Table described in Chapter 6, “Configuring an Asynchronous Port” to configure the attached modems or set each port as a host device as described in Chapter 14, “Configuring the PortMaster to Access Shared Devices” and configure each modem individually.



Note – V.34 modems should lock the DTE rate at 115200 bps unless the modem manual instructs otherwise. V.32bis modems should lock the DTE rate at 57600 bps. Use the fastest DTE interface speed supported by your modem.

A list of modems and their initialization strings is found in Table 6-6 on page 6-14. The recommended configuration has the modem do the following:

- Raise carrier when a call comes in
- Reset itself when DTR is dropped
- Lock the DTE rate
- Use hardware flow control (RTS/CTS)

If you have already configured your modems on another machine, you should connect to the modem through the PortMaster and set the modem back to the factory default. Then use the recommended modem string to properly configure each modem.

Table 13-5 Serial Port Parameter Values for All Ports

Parameter	Value
Port Type	Login Network
Network Type	Dial In
Security	On
Modem Type	(set to your modem type)

Table 13-5 Serial Port Parameter Values for All Ports (Continued)

Parameter	Value
The following five parameters are set by the Modem Table when you reset the port, provided the port has its default setting.	
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS

Once all of the ports are configured as shown above, save and reset all of the ports.

Defining a Dial-In Login User



Note – The instructions in this section are only used if you are not using RADIUS and you are not using pass-through logins.

A user account must be set up on the PortMaster for each authorized user. Each new user user1 should be configured with the parameter values shown in Table 13-6.

Table 13-6 User Table Parameter Values for user1

Parameter	Value
User Name	user1
Password	passwd
User Type	Login/Normal
Host	Default
Login Service	PortMaster (if the <code>in.pmd</code> daemon is running on the default host, otherwise select “rlogin”)

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-In Network User



Note – The instructions in this section are only used if you are not using RADIUS.

A user account must be set up on the PortMaster for each authorized network user. Each new user user2 should be configured with the parameter values shown in Table 13-6.

Table 13-7 User Table Parameter Values for user2

Parameter	Value
User Name	user2
Password	passwd (any)
User Type	Network/Normal
Protocol	PPP/IP
Address Type	Assigned
Compression	On
Routing	Off

You can also use SLIP or CSLIP instead of PPP, refer to Chapter 8, “Configuring Dial-In Users” for more information about this configuration.

Configuring the PortMaster to Access Shared Devices

14

This chapter describes how to use the PortMaster to connect from networked hosts to shared devices connected to the PortMaster. This type of connection is designed to allow access to modems, printers, and other RS-232 devices.

The following topics are described:

- Overview of shared device configurations
- Description of hardware configuration
- Description of general software configuration
- Description of the specific software configurations for each application
- Testing the configuration

Overview of Shared Device Configurations

There are two methods of accessing shared devices on the PortMaster. The first method requires a UNIX host that supports the PortMaster `in.pmd` daemon. With this daemon, you can configure ports as host devices and access them as pseudo-tty from the host using `tip`, `UUCP`, and other applications.

Alternatively, you can configure the ports as network devices and access them using `telnet`, `rlogin`, or a clear channel TCP connection (`netdata`).

Host Device Configuration

One of the functions of a communications server is to provide network users access to shared devices such as printers and modems. This can be done if the port connected to the printer or modem is configured as a host device port. This configuration is also useful for `tip` and `UUCP` services.

Once a port is defined as a host device, the device service is configured as PortMaster, and a pseudo-tty is chosen for the port. The host device port can now be accessed by establishing a pseudo-tty connection to the port from a UNIX host with the PortMaster daemon software installed. In this case, the port operates as a host-controlled device. Figure 14-1 shows a diagram of the host device configuration using the PortMaster device service and a pseudo-tty connection.

Once the port type is set as host device, the device service must be selected and the host name entered either for the port, or as the global default host. If the device service is set to PortMaster for pseudo-tty operation, a host name and pseudo-tty must be specified. The PortMaster `in.pmd` daemon must be installed on the specified host in order to use the PortMaster device service.

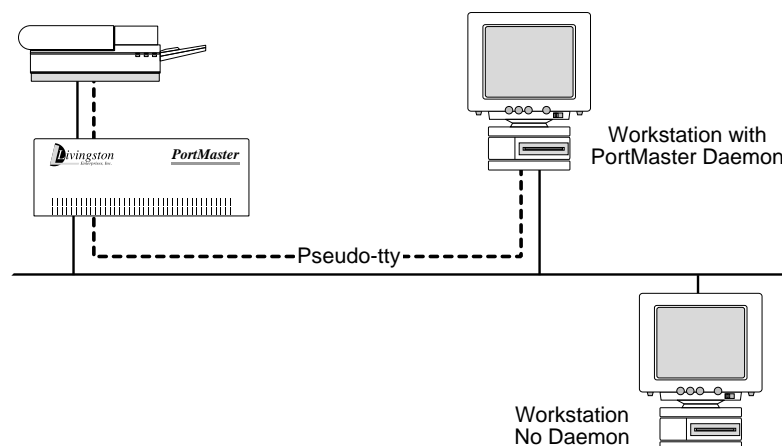


Figure 14-1 Host Device Configuration

In this configuration, a workstation with `in.pmd` installed can access a printer attached to a PortMaster port as though it was attached to the workstation even if the printer is on the other side of the country.

Network Device Configuration

This configuration sets the port for host device access but uses the `rlogin`, `telnet`, or `netdata` device service to access the attached device. In this configuration the host device name is set as `/dev/network`. This configuration is used in cases where users want to `telnet` or `rlogin` to the shared device from multiple hosts or from a host that does not support `in.pmd`. Figure 14-2 shows an example of the network device configuration.

The network user configuration is most commonly used to allow a `telnet` session with the device attached to a specified PortMaster port. The example in this chapter sets ports for network access so the administrator can `telnet` to each modem connected to a

PortMaster port for configuration purposes. In this application, each port is identified by a unique port number assigned during the configuration process. You can also configure a pool of ports at a single TCP port number.

The netdata (TCP clear) device service is most often used when you want to have a custom application open a TCP connection to an RS-232 device, or to connect two serial devices across a network.

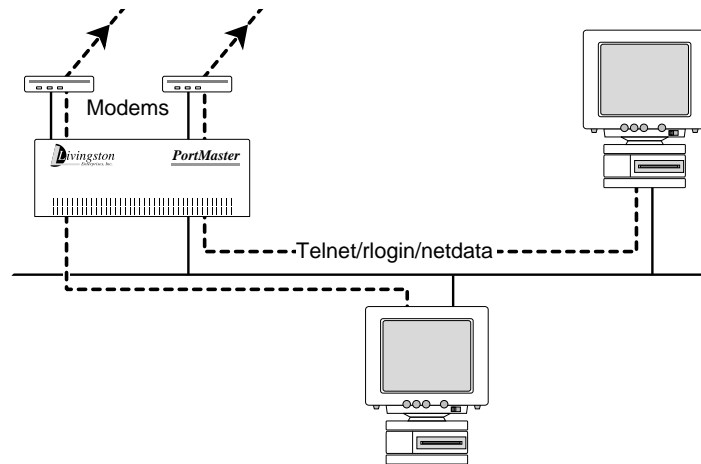


Figure 14-2 Network Device Configuration

Description of Sample Configuration

The example described in this chapter allows a user to dial into port S2 on the PortMaster to login to a workstation, and access a serial printer attached to port S9, as `/dev/ttyre`, using the PortMaster device service. The workstation user would also like to access port S2 as `/dev/ttyrf` when it is not being used for login service.

The modem attached to port S2 is connected with a straight-through cable and uses hardware flow control and carrier detect. The DTE rate between the modem and the PortMaster is locked.

In order to use the PortMaster login or device service, the workstation user must install the PortMaster daemon, `in.pmd` in the `/usr/etc` directory and modify the `/etc/services` and `/etc/inetd.conf` files to tell the workstation where to find `in.pmd`. You must also add `/dev/ttyrf` to the `/etc/remote` file and `/dev/ttyre` to the `/etc/printcap` file.

Change the variable values shown in Table 14-1 to actual values that reflect your network.

Table 14-1 Example Configuration Variables

Variable Description	Value for this Example
Name of PortMaster	pm
IP address of PortMaster	192.168.200.1
Default Host	192.168.200.2 (the workstation)
Speed of modem	28800 bps (DTE rate 115200 bps)
Host device on S2 (modem)	/dev/ttyrf
Host device on S9 (printer)	/dev/ttyre
Speed of printer	9600 baud

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

- 1. Unpack the PortMaster.**
- 2. Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch(es) appropriately.**
- 3. Connect the power cable.**
- 4. Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. Turn on the power switch.

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. Press [Return] on the console.

The PortMaster login prompt is displayed.

7. Type !root then press [Return].

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. Press [Return] at the password prompt.

9. Set the IP address of the new PortMaster by typing:

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. Save the address in the nonvolatile memory of the PortMaster by typing:

```
Command> save all
```

11. Exit the command mode by typing:

```
Command> quit
```

12. Attach the modem to port S2 with a straight-through cable.

13. Attach the printer to port S9 with a null modem cable if the printer is a DTE device.

Pinouts for both cables are given in the *Hardware Installation Guide*.

Configuring the Software for Shared Device Applications

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible PC. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using telnet once the PortMaster address is set.

Setting the Global Parameters

Set the name of the system to pm using the System Name parameter. If you are using PMconsole, the parameter is found in the SNMP window. Refer to your *Administrator's Guide* for more information. Set the Default Host parameter to 192.168.200.2 using the Global Parameter window. You can also set the host for ports S2 and S9 to 192.168.200.2 if you plan to use the other ports for some other host. Set other global parameters that apply to your installation.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 14-2.

Table 14-2 Ethernet Parameter Values

Parameter	Value
Protocol	PPP/IP
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the TwoWay Serial Port (S2) Parameters

In our example, the workstation user wants to dial in to port S2 sometimes and tip out to the modem connected to port S2 at other times. Configure the S2 port parameters with the values shown in Table 14-3.

Table 14-3 Serial Port Parameter Values (S2)

Parameter	Value
Port Type	User Login and Host Device (or twoway for command line)
Host Device	/dev/ttyrf
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise.
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Host	Default (or 192.168.200.2)
Security	Off (if Security is On, you must configure the User Table or RADIUS)
Login Service	PortMaster
Device Service	PortMaster

All the other parameters should be left at their default values. Once all of the ports are configured as shown above, save and reset all of the ports. For more information about asynchronous ports, refer to Chapter 6, “Configuring an Asynchronous Port.”

Setting the Serial Printer Port (S9) Parameters

In our example, a serial printer is connected to port S9. Configure the S9 port parameters with the values shown in Table 14-4. If the printer is a DTE use a null modem cable to connect to the port.

Table 14-4 Serial Port Parameter Values (S9)

Parameter	Value
Port Type	Host Device
Host Device	/dev/ttyre
Speed 1	9600
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	Xon/Xoff
Host	Default (or 192.168.200.2)
Device Service	PortMaster

Once all of the ports are configured as shown above, save and reset all of the ports. The workstation printer subsystem should now be able to send printer jobs to /dev/ttyre and reach the printer.

Setting the Parallel Port (P0) Parameters

The parallel port P0 can be used to access a printer. To configure the P0 port for a printer, use the values shown in Table 14-5.

Table 14-5 Parallel Port Parameter Values (P0)

Parameter	Value
Port Type	Host Device
Host Device	/dev/ttyre

Table 14-5 Parallel Port Parameter Values (P0) (Continued)

Parameter	Value
Host	Default (or 192.168.200.2)
Device Service	PortMaster

Configuring a Network Device for Telnet Access

To access modems or other devices attached to PortMaster ports using telnet, use the general configuration given earlier in this chapter but use the parameters shown in Table 14-6.

Table 14-6 Serial Port Values to Allow a Telnet Connection to Ports S0-S29

Parameter	Value
Port Type	Host Device
Host Device	/dev/network
Modem Control	Off
Device Service	Telnet 6000 through 6029 for ports S0 through S29

To access port S1 using telnet from your host, type:

```
% telnet pm1 6001
```

Where pm1 is the host name of the PortMaster you are accessing and 6001 is the TCP port set for the port you are accessing. You can also set several ports to the same TCP port to create a pool of ports available for telnet access.



Note – If you are using this configuration to configure your modems, see “Configuring Modems and Modem Parameters” on page 6-13 first.

This chapter describes how to use the PortMaster to connect to a synchronous leased line at speeds up to T1 (1.544 Mbps) or E1 (2.048 Mbps). This chapter also describes how to configure a dial backup connection for your synchronous line.

The following topics are described:

- Overview of the leased line configuration
- Description of hardware configuration
- Description of the software configuration for a leased line
- Testing the configuration

Overview of the Leased Line Configuration

PortMasters support leased line connections using synchronous ports and the PPP protocol. In this configuration one PortMaster is usually connected to another PortMaster or other router over a leased line where each router uses its own Ethernet address for the serial link (known as “IP unnumbered”) and the address of the other end is discovered dynamically. In this way a dedicated high-speed connection is established between two routers located in separate sites. The leased line connection requires a CSU/DSU and a carrier that provides external clock. Figure 15-1 shows an example of the leased line connection.

If you are connecting two networks together for the first time you should make sure first that there are no conflicts in the network numbering; that is, make sure that the two networks are not using the same subnet twice in different locations. For more information on network numbers and subnetting see “Network Addressing” on page 2-1.

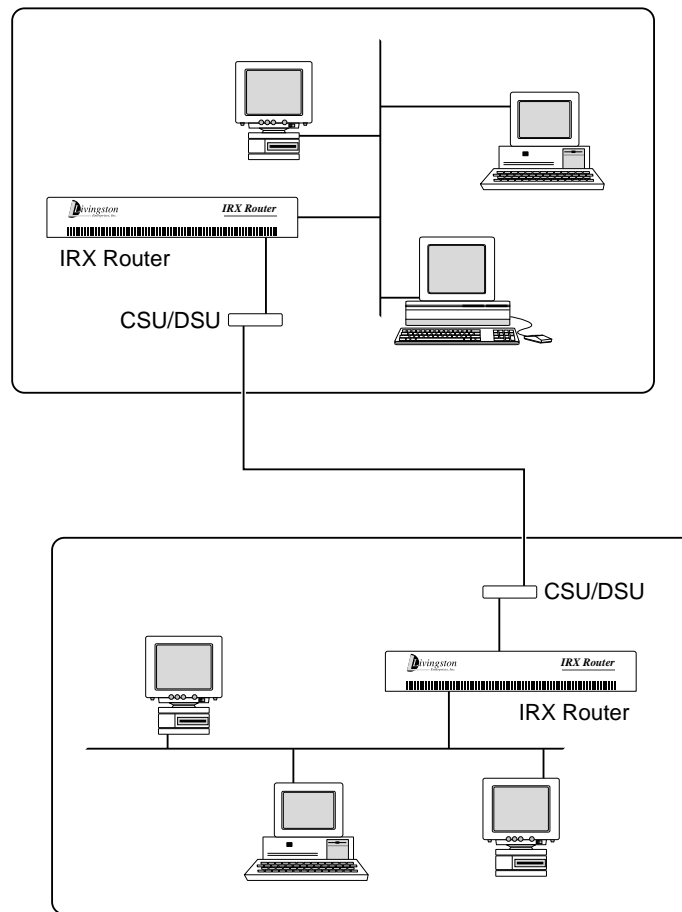


Figure 15-1 Leased Line Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster router located in one office with a PortMaster router located in another office using a dedicated leased line. The variables shown in Table 15-1 are used in this example. Change variable values to reflect the actual values for your network.

Table 15-1 Example Configuration Variables for Leased Line Connections

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**
3. **Connect the power cable.**

4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Turn on the power switch.**

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. **Press [Return] on the console.**

The PortMaster login prompt is displayed.

7. **Type !root then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. **Set the netmask and broadcast values if necessary.**

11. **Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

12. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```


Configuring the Software for a Leased Line Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate PMconsole Administrator's Guide, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

In the leased line configuration described in this section, the Ethernet address of the PortMaster is used as the address for the serial link and the CSU/DSU must provide external clock or pass external clock from the carrier. Since the PortMaster always uses external clock, you do not need to set the speed on the synchronous port, the port speed is whatever the carrier sends. If you choose to set a speed it is for documentation purposes only; the speed is ignored by the PortMaster.



Note – The PortMaster also supports numbered IP interfaces on leased lines, but this is not recommended since it wastes IP address space.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 15-2. These values only apply to this example. Use values appropriate for your network.

Table 15-2 Global Parameter Values

Parameter	Value
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Name Service (optional)	DNS
Name Server (optional)	192.168.200.2
Sysname	office1

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Interface Parameters

Set the following Ethernet parameters to the values shown in Table 15-3.

Table 15-3 Ethernet Parameter Values

Parameter	Value
Protocol	IP/IPX (or IP)
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1 (if you are using IPX)
IPX Frame Type	802.2 (if you are using IPX)
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Synchronous Port Parameters for a Leased Line Connection

Configure the WAN port parameters with the values shown in Table 15-4 for this example only.

Table 15-4 WAN Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Hardwired
Transport Protocol	PPP
Port IP address	Unnumbered (0.0.0.0)
IP Destination	192.168.1.1 (or Negotiated)
Netmask	255.255.255.0

Table 15-4 WAN Port Parameter Values (Continued)

Parameter	Value
IPX Network	000000F3
Line Speed	Speed is a comment only, the actual speed is set by the external clock
Modem Control	On or Off depending on the CSU/DSU configuration
Routing	On (Broadcast and Listen)
MTU	1500

If you are not sure of the IP address on the other end of the connection, you can set the IP Destination parameter to Negotiated (255.255.255.255).

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, “Configuring a Synchronous WAN Port.”

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. However, if you are having problems use the information in this section to debug your configuration.

If you are having trouble with a leased line connection, verify the following:

- Use the following commands to view the PPP negotiation on port S1, if this is the port you are using:

```
Command> set console
Command> set debug 0x51
Command> reset s1
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0x0
Command> reset console
```

- The error counters should be 0 except for abort errors. If your counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cable and it is attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch next to the synchronous port is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing clock to the PortMaster. The CSU/DSU can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- If you have a Cisco router on the other end of your connection, it must be running software release 9.14(5) or later and use PPP encapsulation not hdlc.
- If the framing errors are greater than 0, verify that the router on the other end of the connection is running the PPP protocol.
- If you are still having problems, set the following:

```
Command> set debug 0x51
Command> set console
```

Then set the CSU/DSU for local loopback. You should see the following message:

```
LCP_APPARENT_LOOP
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4.

- If the local loopback works, take the CSU/DSU out of loopback and set line loopback on the remote CSU/DSU. You should see the same result. If you do not, the problem is either in the configuration of one of the CSU/DSU’s or in the line itself.
- When you have finished, turn off debugging by typing:

```
Command> set debug 0
Command> reset console
```

- Contact your carrier to review your configuration and the status of their line.

This chapter describes how to use the PortMaster to connect to a synchronous line using Frame Relay.

The following topics are described:

- Frame Relay terms
- Overview of the Frame Relay configuration
- Description of hardware configuration
- Description of the software configuration for Frame Relay
- Testing the configuration

Frame Relay Terms

Frame Relay uses several special terms that have created a large amount of confusion because of the differences between Frame Relay and other traditional telecommunications methods. In this section, the technology behind Frame Relay is described briefly, and special terms which are defined in the glossary are highlighted in **bold print**.

Frame Relay is a switched digital service, which supports multiple **virtual circuits** being simultaneously connected to a site by a single **physical circuit**. The principle is that a site connects via a physical circuit to a Frame Relay network or cloud. Each site requires only one physical circuit into the cloud, but can have as many virtual circuits as necessary to reach any other sites attached to the cloud. It is possible for Frame Relay to support Switched Virtual Circuits (**SVCs**) or Permanent Virtual Circuits (**PVCs**) but the PortMaster (and most communications providers) only support PVCs. A PVC is used to connect any point A attached to the network to any other point B attached to the network. Each PVC is given a unique number on each physical circuit in the path from point A to point B. This number is called a **DLCI** (Data Link Channel Identifier). The DLCI is automatically changed as it passes through each switch in the path to the number for the PVC on the next physical circuit in the path. Generally, the only two DLCI numbers the customer ever sees are the ones used on the physical circuits at each end. Other numbers are usually kept internal to the

telecommunications provider. A DLCI is different from a network address, in that it identifies a circuit in both directions, not a particular endpoint. That is, a frame contains only one DLCI, not a source and destination.

The physical circuit between point A and the network must be ordered with a certain **line speed**. This is the physical maximum bandwidth for your connection to the Frame Relay network. Expansion beyond this limit is not possible without a hardware change, and a new circuit installation.

The connection into the telecommunications provider's Frame Relay network must be ordered at a particular **port speed**, which is the maximum bandwidth rate that the telecommunications provider accepts from your connection. This number must be less than or equal to the line speed. This speed is the maximum rate at which you can transmit data to any of your PVCs under any circumstances. The port speed differs from line speed only in that it can be upgraded through software without a circuit installation or hardware change.

Each PVC has a property known as Committed Information Rate (**CIR**), which represents the guaranteed minimum bandwidth available to the particular PVC under all conditions. In some implementations, an additional property can be assigned to a PVC, known as "burst speed" or "maximum burst". This speed represents the highest rate at which data is allowed to flow over a given PVC regardless of bandwidth availability.

The PortMaster pushes as much data out of the serial port as it can at port speed for any PVC that has traffic, regardless of CIR. The Frame Relay switch passes as much of the data as possible on to the next link. However, once a particular PVC has transmitted its CIR worth of bits each second, the switch marks any additional frames as "Discard Eligible". If the switch receives more frames than it can pass along, the frames are automatically discarded in the following order:

- Frames that would be marked Discard Eligible even if they are forwarded
- Frames received that were marked as Discard Eligible
- If the switch must discard other frames, the behavior is undefined. In this case, the Frame Relay network is improperly configured because the CIR total exceeds the line speed or port speed.

When ordering Frame Relay service for a private network, it is generally best to order large bandwidth physical circuits (T1), with port speed appropriate to the application, and a CIR that is just barely high enough to provide minimally acceptable performance

for your application. Remember, in most cases you usually get close to your port speed. The CIR is a guaranteed minimum throughput, not a maximum limit. Port speed is the maximum limit.

The following Frame Relay terms relate to network management. The Frame Relay specification supports automatic network status updates, which are exchanged between adjacent devices in the Frame Relay network. These status updates are known as Local Management Interface (**LMI**). There are two forms of LMI available in the Portmaster. Cisco/Stratacom LMI, which is commonly referred to as LMI, and ANSI T1.617 Annex D LMI, which is commonly referred to as **Annex-D**. Generally, your telecommunications provider offers three options for LMI on your physical circuit: LMI, Annex-D, or none. LMI is only between your router and the switch to which your physical circuit connects. Therefore, it does not matter what the remote ends of any of your PVCs are using. However, it is important that your circuit LMI matches the configuration on your PortMaster. Generally, Annex-D is recommended, since it is a more feature-rich and robust version of LMI.

Overview of the Frame Relay Configuration

Frame Relay is a method of encapsulating network information that allows for fast delivery and high line utilization. PortMasters support Frame Relay over synchronous ports. The PortMaster IRX supports speeds up to T1/E1 on ports S1 and S3. The IRX also supports speeds up to 64Kbps on ports S2 and S4. The PortMaster PM-2R series supports up to T1/E1 speeds on the W1 port.

Frame Relay is configured by selecting the Frame Relay protocol, setting the IP address of the port, and specifying the Data Link Connection Identifiers (DLCIs) during the synchronous port configuration. The PortMaster can also discover DLCIs dynamically and learn the IP addresses of the other routers through inverse ARP if you use either LMI or Annex-D keepalives and the other routers on your Frame Relay cloud support inverse ARP as specified in RFC 1490. Both LMI and Annex-D keepalives are supported on PortMasters. In this configuration, the PortMaster sends an LMI status request every 10 seconds (default). Every sixth request is a full status request, the others are keepalives. In this configuration the port state is **CONNECTING** until it receives replies from the switch, then the port state becomes **ESTABLISHED**. After six unanswered requests, the PortMaster resets the port. Figure 16-1 shows an example of a Frame Relay connection.



Note – All synchronous ports require external clock to regulate the port speed.

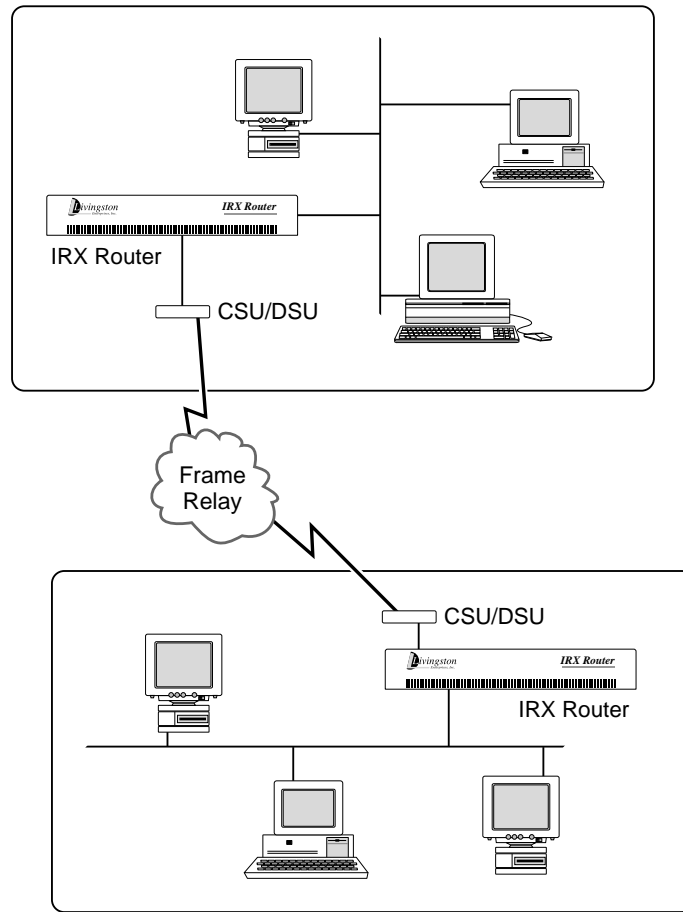


Figure 16-1 Frame Relay Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster router located in one office with a PortMaster router located in another office using Frame Relay on a synchronous interface. The values shown in Table 16-1 are used in this example. Change values to reflect the actual values for your network.

Table 16-1 Example Configuration Variables for Frame Relay Connections

Variable Description	Value for this Example
Name of router in office1	office1
Ether0 IP address of router in office1	192.168.200.1
Ether0 Netmask	255.255.255.0
Gateway	192.168.20.2
Protocol for port S1 in office1	Frame Relay
IP address for port S1 in office1	192.168.20.1
Netmask for port S1 in office1	255.255.255.0
DLCI list for port S1 in office1 ¹	16:192.168.20.2
Annex-D for port S1 in office1	10 seconds (If used, DLCI list is optional); LMI is also available.
Name of router in office2	office2
Ether0 IP address of router in office2	192.168.1.1
Ether0 Netmask	255.255.255.0
Protocol for port S1 in office2	Frame Relay
IP address for port S1 in office2	192.168.20.2
Netmask for port S1 in office2	255.255.255.0
DLCI list for port S1 in office2	16:192.168.20.1
Annex-D for port S1 in office2	10 seconds (If used, DLCI list is optional); LMI is also available.

1. The two ends of a Private Virtual Circuit (PVC) do not have to use the same number for their DLCI's. Use the DLCI's provided by your carrier.

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switches appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Turn on the power switch.**

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. **Press [Return] on the console.**

The PortMaster login prompt is displayed.

7. **Type !root then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. **Set the netmask and broadcast values if necessary.**

11. Save the address in the PortMaster nonvolatile memory by typing:

```
Command> save all
```

12. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:

```
Command> quit
```

Configuring the Software for a Frame Relay Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

Setting Global Parameters

Set the name of the system to office1 using the System Name parameter and the IP Gateway parameter to 192.168.20.2. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

For this example configuration, none of the other global parameters need to be set. However, you may want to define some of these parameters for your installation.

Setting the Ethernet Interface Parameters

Set the following Ethernet parameters on office1 to values appropriate for your network. The values shown in Table 16-2 apply to this example only.

Table 16-2 Ethernet Parameter Values

Parameter	Value
IP Address	192.168.200.1
Netmask	255.255.255.0

Table 16-2 Ethernet Parameter Values (Continued)

Parameter	Value
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Synchronous Port Parameters for a Frame Relay Connection

Configure the WAN port parameters with values appropriate for your network. The values shown in Table 16-3 apply to this example only.

Table 16-3 WAN Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Hardwired
Protocol	Frame Relay
Port IP address	Specified 192.168.20.1
Netmask	255.255.255.0
Speed	(speed is set by external clock)
Modem Control	On or Off depending on the CSU/DSU configuration
Routing	On (Broadcast and Listen)
Compression	Disabled
Annex-D	10 seconds (LMI can be used instead of Annex-D)
DLCI List	16:192.168.20.2 (or empty if remote router supports inverse ARP)

If LMI or Annex-D is set, the PortMaster receives DLCI information in the full status update messages from the Frame Relay switch. The PortMaster then attempts to discover IP addresses of other routers using inverse ARP. You can set DLCI lists statically as well. The `show arp frml` command lists both the static and dynamic DLCI lists for the S1 port.

If Annex-D is available from your carrier for a new connection, it is preferable to LMI.

To connect to Cisco routers using Frame Relay, the Cisco router must be set to use `encapsulation frame-relay ietf` for the serial interface; otherwise, the frame map for your DLCI must have the `ietf` argument appended.

For more information about synchronous ports, refer to Chapter 7, “Configuring a Synchronous WAN Port.”

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you are having problems use the information in this section to debug your configuration.

If you are having trouble with a Frame Relay connection, verify the following:

- The error counters should be 0 except for abort errors. If your counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cables and they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing the clock to the PortMaster. The CSU/DSU can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- Contact your carrier to review your configuration and the status of their line.
- Use the following two commands to view the LMI or Annex-D keepalives:

```
Command> set console
Command> set debug 0x51
```

Once you have verified that the proper keepalives are being received, type:

```
Command> set debug 0
Command> reset console
```

- If you have a Cisco router on the other end of your connection, it must be set for encapsulation `frame-relay ietf` for the serial interface; otherwise, the frame map for your DLCI must have the `ietf` argument appended on the Cisco.

Frame Relay Subinterface

The PortMaster supports a feature called DLCI bundling to allow splitting one synchronous port, with multiple DLCIs, into two Frame Relay subinterfaces. In this configuration the DLCIs are divided between the subinterfaces using the Location Table and the DLCI Table. Only two subinterfaces per port are currently supported, and are referred to as the “primary subinterface” and “secondary subinterface.” Each subinterface must have its own subnet or assigned network. Active discovery of DLCIs via LMI or Annex-D only occurs on the primary subinterface. The secondary subinterface can have an unlimited number of DLCIs.

The Frame Relay subinterfaces can only be set using the command line interface. For example, add a location with the protocol type set to frame:

```
Command> set s1 group 1
Command> add location example
Command> set location example protocol frame
Command> set location example group 1
```

The rest of the Location Table entries are set as described in Chapter 9, “Configuring Dial-Out Locations,” including IP address for the interface, routing, and filtering.

The next step in configuring the subinterfaces is to create an entry in the DLCI Table. Entries can be followed with an optional IP address or hostname. The keyword “`ipdlci`” is a synonym for “`dlci`”. The keyword “`ipxdlci`” is also available for IPX networks. To create a DLCI Table entry, type:

```
Command> add dlci example 16
Command> add dlci example 19 192.168.2.19
Command> add ipdlci example 20 192.168.2.20
Command> add ipxdlci example 21 0e0a001e
```

To remove an entry, use the delete command as follows:

```
Command> delete dlci example
Command> delete ipxdlci example 21
```

There is no `show table dlci` command. Instead, entries which are added or deleted are linked to the Location Table. Therefore, the `show location example` command displays the DLCI entries.

You can only have one Location Table entry per Frame Relay interface (allowing one secondary subinterface), so you can have some DLCIs as part of one location and other DLCIs as part of the port interface. Multiple secondary subinterfaces are not supported yet.

Troubleshooting Subinterfaces

Packets received on a subinterface can only be identified as belonging to that subinterface if the DLCI is properly entered in the DLCI Table for that location. If you are having problems, verify the following:

- Check the list of DLCIs tied to each location using the `show location Location_Name` command
- Verify the DLCI list on a location using the `show arp frmXX` command
- Always reset the port after changing the DLCI list
- Verify that all DLCIs are accounted for by checking the DLCI list for your primary interface. If you enter the wrong DLCI for the subinterface then the real DLCI for the subinterface shows up as belonging to the primary interface, if LMI or Annex-D is in use.

Example of a Frame Relay Subinterface

This example is for an IRX-111 with Frame Relay coming into port S1 with DLCIs 16, 17, and 18. Port S1 has already been configured for Frame Relay, so that portion is not shown here. The following commands split the Frame Relay into a primary subinterface for DLCI 18, and a secondary subinterface for DLCIs 16 and 17.

```
Command> set s1 group 1

Command> add location sub1
Command> set location sub1 protocol frame
Command> set location sub1 group 1
Command> set location sub1 address 192.168.3.1
Command> set location sub1 netmask 255.255.255.0
Command> set location sub1 routing on

Command> add dlci sub1 16
Command> add dlci sub1 17

Command> same all
Command> reset s1
```

You now have the following two subinterfaces:

- DLCI 18 on s1
- DLCI 16 and 17 on s1 (sub1)



Note – You could not define another subinterface on port S1 using other DLCIs, but you could add other DLCIs to either of these two existing subinterfaces. A future release will remove this restriction and allow you to divide each Frame Relay interface into as many virtual subinterfaces as you like.

Synchronous V.25bis Dial-Up Connections

17

This chapter describes how to use the PortMaster to connect two Local Area Networks (LANs) via synchronous V.25bis dialing applications such as, ISDN, terminal adapters, or switched 56K.

The following topics are described:

- Overview of the ISDN and switched 56K configuration
- Description of hardware configuration
- Description of the software configuration for ISDN with a V.25bis terminal adapter or switched 56K
- Testing the configuration

Overview of the ISDN and Switched 56K Configurations

PortMasters support dial on-demand ISDN and switched 56K connections using synchronous ports and the PPP protocol. ISDN speeds of up to 64Kbps are possible with an outside carrier and an external terminal adapter (TA). Speeds of up to 128Kbps are possible if the TA supports B-channel BONDING. Contact your service provider for specific information about the required terminal adapter.

Switched 56K connections require an external CSU/DSU. ISDN and switched 56K connections can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the Location Table for dial-out connections and a dial-in user must be specified in the User Table for dial-in connections.

PAP is available for dial-in authentication, when a router dials into your PortMaster. CHAP is available for dial-in and dial-out authentication.

When connecting an asynchronous ISDN terminal adapter to an asynchronous port using AT commands to dial, configure the PortMaster just as you would for a modem. Refer to Chapter 11, “Connecting a Branch Office to the Main Office” and Chapter 12, “Connecting Your Office to the Internet” for more information. In this configuration, keep in mind that a 115.2Kbps asynchronous DTE rate can only support a single 64Kbps B-channel, because it takes 10 bits to send a byte of asynchronous data (including the start and stop bits). However, it takes only 8 bits to send a byte of

synchronous data. Therefore, a 115.2Kbps DTE rate cannot properly support two 64Kbps B-channels because the TA is unable to buffer the excess data when data is coming in from the ISDN line at 16 kilobytes/second and the DTE can only accept 11.5 kilobytes/second.

Figure 17-1 shows an example of an ISDN or switched 56K connection.

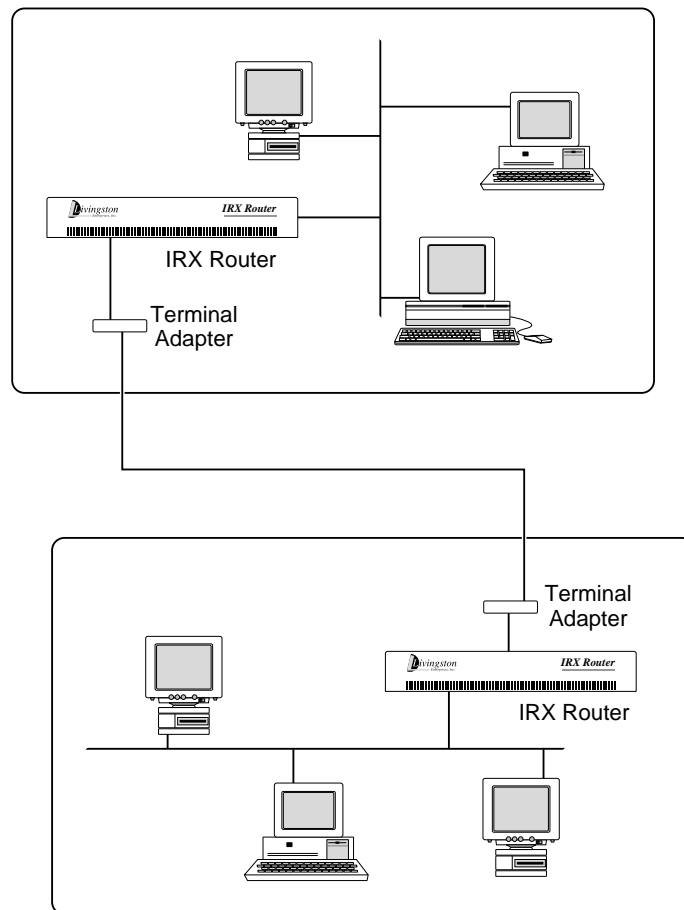


Figure 17-1 Example of an ISDN or Switched 56K Connection

Description of Sample Configuration

This example connects a PortMaster located in one office with a PortMaster located in another office using a synchronous interface that is initiated on-demand using an ISDN or switched 56K connection. The variables shown in Table 17-1 are used in this example. Change variable values to reflect the actual values for your network.

Table 17-1 Example Configuration Variables for V.25bis Connections

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
Phone number of router in office1	17005551111
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of router in office2	000000F2
IPX Frame Type	IEEE 802.2 on Ethernet
Phone number of router in office2	17005552222
IPX network of the serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**

3. Connect the power cable.

4. Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. Turn on the power switch.

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. Press [Return] on the console.

The PortMaster login prompt is displayed.

7. Type !root then press [Return].

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. Press [Return] at the password prompt.

9. Set the IP address of the new PortMaster by typing:

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. Set the netmask and broadcast values if necessary.

11. Save the address in the PortMaster nonvolatile memory by typing:

```
Command> save all
```

12. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:

```
Command> quit
```

Configuring the Software for an ISDN or Switched 56K Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a PC running Microsoft Windows. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

The configuration using V.25bis dialing for both ends of the connection is given in this section.

Configuring ISDN or Switched 56K on office1

The PortMaster in Office 1 (office1) is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Office 2 (office2).

Setting the Global Parameters on office1

Set the following global parameters to the values shown in Table 17-2. These values only apply to this example. Use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 17-2 Global Parameter Values on office1

Parameter	Value
IP Gateway	192.168.1.1
Default Route	Broadcast
Sysname	office1

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Interface Parameters on office1

Set the following Ethernet parameters to the values shown in Table 17-3.

Table 17-3 Ethernet Parameter Values on office1

Parameter	Value
Protocol	IP/IPX
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Synchronous Port Parameters on office1

Configure the synchronous WAN port parameters with the values shown in Table 17-4 for the example in this chapter. Your configuration should reflect your network.

Table 17-4 WAN Port Parameter Values on office1

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Line Speed	The speed is a comment only, the actual speed is set by the external clock
Modem Control	On
Dial Group	0 (same as for Location Table entry)

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, “Configuring a Synchronous WAN Port.”

Defining the Dial-In User on office1

A user account must be set up on the router office1 so the PortMaster office2 can dial in when traffic is queued. The new user office2 should be configured on office1 with the parameter values shown in Table 17-5.

Table 17-5 User Table Parameter Values for User office2

Parameter	Value
User Name	office2 (must be the SNMP system name of the remote PortMaster)
Password	anypasswd (The password must match the password for user office1 on PortMaster office2)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500

No compression is used on synchronous lines. For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location on office1

A location entry on the PortMaster office1 must be created for the location identified as office 2. This allows the router office1 to call the PortMaster office2 when network traffic is queued. The new location office2 should be configured on office1 with the parameter values shown in Table 17-6.

Table 17-6 Location Table Parameter Values for Location office2

Parameter	Value
Location Name	office2
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0 (same as for WAN port)
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005552222 (V.25bis dialing does not require the carriage return) Expect: =DCD=

For more information about configuring Location Table parameters, refer to Chapter 9, “Configuring Dial-Out Locations.”

After the port, user, and location parameters are entered, the port should be reset to make the new configuration active.

Configuring a V.25bis Dial-Up Connection on office2

The PortMaster in Office 2 (office2) is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Office 1 (office1).

Setting the Global Parameters on office2

Set the following global parameters to the values shown in Table 17-7. These values only apply to this example; use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 17-7 Global Parameter Values on office2

Parameter	Value
IP Gateway	Set to the address of the next upstream router
Default Route	Off
Sysname	office2

Setting the Ethernet Interface Parameters on office2

Set the following Ethernet parameters to the values shown in Table 17-8.

Table 17-8 Ethernet Parameter Values on office2

Parameter	Value
Protocol	IP/IPX
IP Address	192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

Setting the Synchronous Port Parameters on office2

Configure the synchronous port parameters with the values shown in Table 17-9 for the example in this chapter. Your configuration should reflect your network.

Table 17-9 WAN Port Parameter Values for office2

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Transport Protocol	PPP
Port IP address	Un-numbered
Netmask	255.255.255.0
Line Speed	The speed is a comment only, the actual speed is set by the external clock
Modem Control	On
Group	0

Defining the Dial-In User on office2

A user account must be set up on the router office2 so the PortMaster office1 can dial in when traffic is queued. The new user office1 should be configured on office2 with the parameter values shown in Table 17-10.

Table 17-10 User Table Parameter Values for User office1

Parameter	Value
User Name	office1 (must be the SNMP system name of the remote system)
Password	anypasswd (The password must match the password for user office2 on PortMaster office1)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1

Table 17-10 User Table Parameter Values for User office1 (Continued)

Parameter	Value
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	Off

No compression is used on synchronous lines. For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location on office2

A location entry on the PortMaster, office2, must be created for the location identified as office1. This allows the router, office2, to call the PortMaster, office1, when network traffic is queued. The new location office1 should be configured on office2 with the parameter values shown in Table 17-11.

Table 17-11 Location Table Parameter Values for Location office1

Parameter	Value
Location Name	office1
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Idle Timeout	5 minutes

Table 17-11 Location Table Parameter Values for Location office1 (Continued)

Parameter	Value
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005551111 Expect: =DCD=

Use the dialer to connect between the two offices. Once everything is working properly, reset the ports and change the Location Type parameter from Manual to On-Demand on both routers.

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you have problems use the information in this section to debug your configuration.

Troubleshooting V.25bis Dial-Up Connections

If you are having trouble with a V.25bis dial-up connection, verify the following:

- The error counters should be 0 except for a small number of abort errors resulting from plugging cables in or out. If your error counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cables and they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU or synchronous terminal adapter is providing the clock to the PortMaster. The CSU/DSU or TA can generate the clock or receive it from the carrier, it does not matter to the PortMaster.
- Verify that the CSU/DSU or synchronous terminal adapter is configured properly.
- Contact your carrier to review your configuration and the status of their line.

- Use the following commands to view the PPP negotiation:

```
officel> set console  
officel> set debug 0x55  
officel> dial office2
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0  
Command> reset console
```


This chapter describes how to use the PortMaster to connect two Local Area Networks (LANs) via ISDN using V.25bis dialing on a BRI interface with integrated NT1.

The following topics are described:

- Overview of the ISDN configuration
- ISDN BRI configuration commands
- Description of hardware configuration
- Description of the software configuration for ISDN with integrated NT1
- Testing the configuration

Overview of the ISDN Configuration

PortMasters support dial on-demand ISDN connections using BRI ports and the PPP protocol. Each BRI supports two 64 Kbps B channels for data and one 16 Kbps D channel for signalling. Multiple lines can be used to increase bandwidth, either using multi-link PPP as defined in RFC 1717 or using Livingston's multi-line load balancing. ISDN BRI ports are easier to configure than asynchronous or synchronous ports because the NT1 is integrated in the port, so no modem, CSU/DSU, or external terminal adapter is required.

ISDN ports can also be used to do anything that an asynchronous port can be used for except network hardwired. Async or sync usage is autodetected. 56K or 64K speed is also autodetected.

ISDN connections can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the Location Table for dial-out connections and a dial-in user must be specified in the User Table or RADIUS for dial-in connections. Figure 18-1 shows an example of an ISDN connection.

CHAP is available for dial-in or dial-out authentication. PAP is available for dial-in authentication, and is available for dial-out authentication if the =PAP= Send string is used in the V.25bis dialing script.

Contact your service provider for specific information about your ISDN switch type and Service Profile Identifier (SPID).

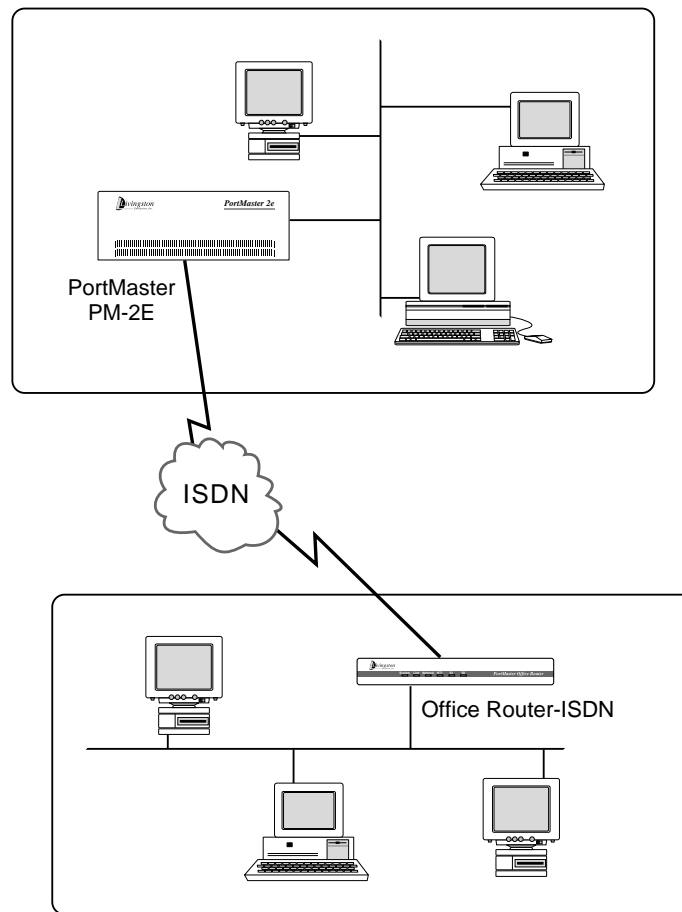


Figure 18-1 Example of an ISDN Connection

ISDN BRI Port Configuration Commands

Two special parameters need to be configured on the PortMaster to permit ISDN service: the ISDN Switch type and a Service Profile Identifier (SPID) for each port. Optionally a directory number for each port can be specified.

To display ISDN debug information on the console, use the following commands:

```
Command> set console
Command> set debug isdn on
```

To turn off debugging, use the following commands:

```
Command> set debug isdn off
Command> reset console
```

ISDN Switch Type

The ISDN Switch Type is a global configuration parameter that can be set to one of three values: DMS-100, NI-1 (National ISDN-1), or 5ESS, also known as ATT-5ESS. Obtain the switch type from your telephone company. Use one of the following commands to set the switch type. The default is NI-1.

```
Command> set isdn-switch ni-1
Command> set isdn-switch dms-100
Command> set isdn-switch 5ess
```

SPID

The Service Profile Identifier (SPID) is a number up to 20 digits long set for each port, which identifies the port to the telephone company. The telephone company provides you with the SPIDs for each line. To set the SPID, use the following command:

```
Command> set s10 spid 1510555121200
```

The `set debug isdn on` command shows any invalid SPIDs.

Terminal Identifier (TID)

The Terminal Identifier (TID) is a numeric value used by some telephone companies for additional identification. Some telephone companies require the SPID, while others require a TID as well. When configuring the PortMaster, append the TID to the SPID if required by your carrier.

Directory Number

The optional Directory Number is a 10-digit phone number provided by the telephone company. If it is set, an incoming call must match this number to determine which port the call should be taken on. The Directory Number must be set in order to allow V.120 multilink calls from the PowerLink128 ISDN Card.

Use either of the following commands to set the Directory Number.

```
Command> set s10 dn 510555111
Command> set s10 directory 510555111
```

ISDN Port Configuration Tips

ISDN ports are simpler to configure than asynchronous ports. Note the following:

- Modem control (carrier detect), flow control, and speed are not set on an ISDN port. The PortMaster senses the speed and sets the port to 64000 bps or 56000 bps accordingly. Flow control is not set on a synchronous line since clock is provided by the telephone company and carrier detect is always used.

Refer to your *Hardware Installation Guide* for information on ISDN LED activity.

- The ISDN ports support synchronous PPP and asynchronous V.120 PPP or SLIP. The `show port` command displays 64000/async if the port is in use for an asynchronous V.120 connection.
- ISDN ports can be configured for all of the same functions as an asynchronous port, except that network hardwired is not supported.
- When using the ISDN port for network dial-out, the dial-out location should use a V.25bis script and authenticate using CHAP, or using PAP with the =PAP= V.25bis Send string.

Description of Sample Configuration

This example connects a PortMaster located in one office with a PortMaster located in another office using an on-demand ISDN connection. The variables shown in Table 18-1 are used in this example. Change variable values to actual values that reflect your network.

Table 18-1 Example Configuration Variables for an ISDN Connection

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
ISDN Switch Type for office1	NI-1
ISDN Phone numbers of 2 B channels in office1	17005551111, 17005551112
SPID for 2 B channels in office1	700555111100, 700555111201
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of router in office2	000000F2
IPX Frame Type	IEEE 802.2 on Ethernet
ISDN Switch Type for office2	NI-1
ISDN Phone numbers of 2 B channels in office2	17005552222, 17005552223
SPID for 2 B channels in office2	700555222200, 700555222301
IPX network of the serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Connect the BRI port to the ISDN telephone line.**



Caution – Do not plug an analog telephone line into the PortMaster BRI RJ-45 connector. The analog line does not work and the PortMaster could be damaged.

6. **Turn on the power switch.**

The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

7. **Press [Return] on the console.**

The PortMaster login prompt is displayed.

8. **Type !root then press [Return].**

You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

9. **Press [Return] at the password prompt.**

10. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

- 11. Set the netmask and broadcast values if necessary.**
- 12. If your version of PMconsole does not support setting the ISDN switch type, SPID, and directory number, then set these parameters from the command line as follows:**

```
Command> set isdn-switch ni-1
Command> set s1 spid 700555111100
Command> set s2 spid 700555111201
Command> set s1 dn 7005551111
Command> set s2 dn 7005551112
```

- 13. Save the configuration in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

- 14. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software for an ISDN Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible PC. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

Configuring ISDN on office1

The PortMaster in office1 is being configured for an ISDN dial-up connection to the PortMaster in office2.

Setting the Global Parameters on office1

Set the following global parameters to the values shown in Table 18-2. These values only apply to this example. Use values appropriate for your network.

Table 18-2 Global Parameter Values on office1

Parameter	Value
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast
Sysname	office1
ISDN Switch	NI-1 (or as identified by the carrier)

For more information about global parameters, refer to Chapter 4, “Configuring a PortMaster.”

Setting the Ethernet Port Parameters on office1

Set the following Ethernet parameters to the values shown in Table 18-3.

Table 18-3 Ethernet Parameter Values on office1

Parameter	Value
Protocol	IP/IPX
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the ISDN Port Parameters on office1

Configure the ISDN port parameters with the values shown in Table 18-4 for the example in this chapter. Your configuration should reflect your network. This example assumes the BRI used is port S1-S2 on a PortMaster Office Router-ISDN (OR-U). If your application uses ports S10 through S29 on a PM-2E, adjust these values accordingly.

Table 18-4 ISDN Port Parameter Values on office1

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Dial Group	2
SPID	S1:700555111100 S2:700555111201

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, “Configuring a Synchronous WAN Port.”

Defining the Dial-In User on office1

A user account must be set up on the router office1 so that PortMaster office2 can dial in when traffic is queued. The new user office2 should be configured with the parameter values shown in Table 18-5.

Table 18-5 User Table Parameter Values for User office2

Parameter	Value
User Name	office2 (must be the system name of the remote system)
Password	anypasswd (The password must match the password for user office1 set on the remote PortMaster.)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1

Table 18-5 User Table Parameter Values for User office2 (Continued)

Parameter	Value
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location on office1

A location entry on the PortMaster office1 must be created for the location identified as office2. This allows the router office1 to call the PortMaster office2 when network traffic is queued. The new location office2 should be configured with the parameter values shown in Table 18-6.

Table 18-6 Location Table Parameter Values for Location office2

Parameter	Value
Location Name	office2
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On

Table 18-6 Location Table Parameter Values for Location office2 (*Continued*)

Parameter	Value
Idle Timeout	2 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	2
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005552222 ¹ Expect: =DCD=

1. V.25bis dialing does not require a carriage return at the end of the string.

For more information about configuring Location Table parameters, refer to Chapter 9, “Configuring Dial-Out Locations.” After the port, user, and location parameters are entered and saved, the port should be reset to make the new configuration active.

Configuring an ISDN Dial-Up Connection on office2

The PortMaster office2 is being configured for an ISDN dial-up connection to the PortMaster office1.

Setting the Global Parameters on office2

Set the following global parameters to the values shown in Table 18-7. These values only apply to this example, use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 18-7 Global Parameter Values on office2

Parameter	Value
IP Gateway	Set to the address of the next upstream router
Default Route	Off
Sysname	office2
ISDN Switch Type	NI-1

Setting the Ethernet Port Parameters on office2

Set the following Ethernet parameters to the values shown in Table 18-8.

Table 18-8 Ethernet Parameter Values on office2

Parameter	Value
Protocol	IP/IPX
IP Address	192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
IPX Frame Type	802.2
Broadcast Address	high (192.168.1.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

Setting the ISDN Port Parameters on office2

Configure the ISDN port parameters with the values shown in Table 18-9 for the example in this chapter. Your configuration should reflect your network.

Table 18-9 WAN Port Parameter Values on office2

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Dial Group	2
SPID	S1:700555222200 S2:700555222301

Defining the Dial-In User on office2

A user account must be set up on the router office2 so the PortMaster office 1 can dial in when traffic is queued. The new user office1 should be configured with the parameter values shown in Table 18-10.

Table 18-10 User Table Parameter Values for User office1

Parameter	Value
User Name	office1 (must be the system name of the remote system)
Password	anypasswd (The password must match the password used for user office2 set on the PortMaster office1.)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location on office2

A location entry on the PortMaster office2 must be created for the location identified as office1. This allows the router office2 to call the PortMaster office1 when network traffic is queued. The new location office1 should be configured with the parameter values shown in Table 18-11.

Table 18-11 Location Table Parameter Values for Location office1

Parameter	Value
Location Name	office1
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On
Idle Timeout	2 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	2
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005551111 ¹ Expect: =DCD=

1. V.25bis dialing does not require a carriage return at the end of the string.

Use the dialer to connect between the two offices. Once everything is working properly, change the Location Type parameter from Manual to On-Demand on both routers and reset the ports.

Troubleshooting the Configuration

Most ISDN configurations come up with little trouble if you have configured the PortMaster using information from your carrier. However, if you are having problems use the information in this section to try to debug your configuration.

If you are having trouble with an ISDN connection, verify the following:

- The error counters should be 0 except for a few abort errors. If your counters are non-zero, there is a problem external to the PortMaster or the values received from your carrier may be incorrect.
- Verify that you are using the correct cables and they are attached securely to the correct port.
- Verify that the ISDN status light is on solid; otherwise, refer to the *Hardware Configuration Guide* for more information. This indicates connectivity to the ISDN switch.
- Verify your configuration as described in this chapter.
- Contact your carrier to review the ISDN switch type, SPIDs, and the status of their line.
- Use the following commands to view the PPP negotiation:

```
Command> set console  
Command> set debug 0x51
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0  
Command> reset console
```

ISDN Port Status

Table 18-12 describes how to interpret the output of the ISDN BRI ports.

Table 18-12 ISDN BRI Port Status

Port Status	Modem Status				Description
NO-SERVICE	DCD-	CTS-	TELCO-	NT1-	No SPID set
NO-SERVICE	DCD-	CTS-	TELCO-	NT1+	No cable or no circuit to TelCo
NO-SERVICE	DCD-	CTS+	TELCO+	NT1+	Cable and ISDN circuit OK but SPID not registered
IDLE	DCD-	CTS+	TELCO+	NT1+	SPID registered and ready to use
ESTABLISHED	DCD-	CTS+	TELCO+	NT1+	Connecting or providing device service but no carrier sensed
ESTABLISHED	DCD+	CTS+	TELCO+	NT1+	Connected
ESTABLISHED	DCD+	CTS-	TELCO+	NT1+	Connected with V.120 async but flow controlled by other end

ISDN Status LEDs

On each ISDN board there is a green LED next to each of the five RJ-45 connectors. When you first turn power on, each LED blinks 8 times per second for about one second while performing an internal self-test of the NT1. If the self-test does not occur, contact Livingston Technical Support.

The LED goes off if no SPID is set on the port and there is no circuit to the telephone company. If no SPID is set on the port but there is a circuit to the telephone company, the LED blinks once per second. If there is a valid SPID and a circuit, the LED blinks once per second while synchronizing with the telephone company, then becomes solid.



Note – On the PortMaster Office Router ISDN (OR-U) this LED is on the front panel, labeled NT1.

Troubleshooting the PortMaster Configuration

19

This chapter describes how to analyze and evaluate issues with your PortMaster configuration. The following topics are discussed:

- How to recognize a network problem
- How to debug a network problem
- PPP negotiation quick reference information
- Booting from the network

Recognizing Network Problems

If you suspect you have a network problem there are several things you can do to try to determine the exact cause of the problem. A problem may be indicated if packets are not sent and received by the PortMaster the way you intended. Use the information in this section to troubleshoot your network.

Most of the commands described in this section can only be accessed using the command line interface, which is useful for debugging for the following reasons:

- The command line can be accessed from a console terminal regardless of network condition.
- The command line provides the most detailed feedback about events in the system and on the network.

Verifying Your Network Connections

You can use the Ping command to verify connectivity between your PortMaster and devices on your network. The Ping command sends an ICMP echo request to the host specified and listens for the corresponding echo reply from the specified host. If a reply is received, there is connectivity. If no reply is received there is a lack of connectivity somewhere on your network between the machine issuing the Ping request and the specified device.

If you do not receive a Ping response, check the following:

- Verify that the host you pinged is running and connected to the Ethernet.
- Verify that all of the cables are connected to the PortMaster properly.

- If the machine you pinged is on another subnet, verify that you are using the correct netmask.

Verifying Your Configuration

If you have verified that everything is connected properly, you should check the configuration of your PortMaster interfaces using the `ifconfig` command. The `ifconfig` command allows you to view the active configuration of each network interface by showing the name of the interface, various flags, and other configuration information. The `ifconfig` flags are described in Table 19-1.

Table 19-1 `ifconfig` Flags

Flag	Description
IP_UP	Indicates that the interface is up and running the IP protocol.
IP_DOWN	Indicates that the IP protocol is not in use.
IPX_UP	Indicates that the interface is up and running the IPX protocol.
IPX_DOWN	Indicates that the IPX protocol is not in use.
BROADCAST	Indicates that this is an Ethernet interface.
POINT_TO_POINT	Indicates that the network connection on this interface is a point-to-point connection.
LISTEN	Indicates that the interface is set to listen for RIP packets but not broadcast them.
RIPSEND	Indicates that RIP packets are being sent out from the interface but are not listened for.
PRIVATE	Indicates that no routing information is being sent or listened to on this interface.
SUSPENDED	Indicates that this interface is set for on-demand dial-out operation and is available, but does not have an active telephone connection to the remote site.
COMPRESS	Van Jacobsen TCP/IP header compression is being done on this interface.

The second and third lines of the `ifconfig` response contain the information described in Table 19-2.

Table 19-2 Additional `ifconfig` Information

Information	Description
<code>inet</code>	Indicates the IP address of the interface.
<code>dest</code>	Indicates the destination IP address of a point-to-point connection.
<code>netmask</code>	Indicates the netmask for the IP address shown in <code>inet</code> or <code>dest</code> .
<code>broadcast</code>	Indicates the broadcast address of the interface (only on Ethernet interfaces.)
<code>mtu</code>	Indicates the maximum transmission unit for the interface.
<code>ipxnet</code>	Indicates the IPX network number of the interface.
<code>ipxframe</code>	Indicates the IPX frame type for the interface (only on Ethernet interfaces.)

Debugging Network Problems

The following subsections describe some of the things that you can do to correct network problems related to your PortMaster once they are discovered. Most of the commands described in this section can only be accessed using the command line interface.

Determining the Software Version

When PMconsole is started the software version is displayed. To determine the version of the ComOS, either look at the bottom of the PMconsole screen after you have logged into a PortMaster or telnet to the PortMaster, login as `!root` and type `version`.



Note – Always include the version number of your ComOS when reporting problems to Livingston Technical Support.

Resetting Ports

PortMaster ports should be reset after any change to their configuration to make the new settings active. Resetting a port causes DTR to be held low for 500 milliseconds. Ports are reset when a connection drops. You can reset the whole system or specific ports using the `reset` command or by clicking the Reset button in PMconsole.

Disabling a Synchronous Port

A synchronous network hardwired port can be disabled by setting its IP address to 0.0.0.0 and the destination IP address to 0.0.0.0.

Tracing Routes with IP

You can use the `traceroute` command to identify the routers used to reach a remote host. The `traceroute` command sends UDP packets to the specified host and listens for ICMP messages returning. A host name or IP address of the destination host is entered with the `traceroute` command, and a list of router addresses in the order seen is printed.

To stop the `traceroute` command, enter the `traceroute` command with no address.

Interpreting LCP and IPCP Debug Output

The PPP negotiation process can be debugged and interpreted using the commands and information given in this section.

To debug PPP negotiations, type the following commands:

```
Command> set console
Command> set debug 0x51
```

To stop the debug output, type the following:

```
Command> set debug 0
Command> reset console
```

PPP Quick Reference

The information that follows describes the PPP protocol.

Frame format

Flag	Addr	Ctrl	Protocol	Data	FCS	Flag
7E	FF	03				7E

All the values shown are in hexadecimal. Adjacent frames may be separated by a single flag. Address and control bytes are omitted in nonLCP frames if Address-and-Control-Field-Compression is negotiated. If the first byte of the Protocol field is zero, it is omitted in nonLCP frames if Protocol-Field-Compression is negotiated. On asynchronous links, special characters (flags, escapes, and control characters selected in the negotiated remote Async-Control-Character-Map) between the flags are replaced by an escape (7D) and the original byte with bit 6 inverted (XOR'ed with 0x20).

Table 19-3 shows protocol values. The Network Protocol (NCP) is used to establish a connection for the associated data transfer protocol.

Table 19-3 Protocol Values

Protocol	Value	NCP Value
Internet Protocol (IP)	0021	8021
OSI Network Layer	0023	8023
DECnet Phase IV	0027	8027
Appletalk	0029	8029
Novell IPX	002B	802B
VJ Compressed TCP/IP	002D	
VJ Uncompressed TCP/IP	002F	
Banyan Vines	0035	8035
Link Control Protocol (LCP)		C021
Password Authentication Protocol (PAP)		C023
Link Quality Report (LQM)		C025
Challenge Handshake Authentication Protocol (CHAP)		C223

LCP Packet Formats

Configure-Request

01	ID	Length	Configuration Options
----	----	--------	-----------------------

Configure-Nak

03	ID	Length	Configuration Options
----	----	--------	-----------------------

Terminate-Request

05	ID	Length	Data
----	----	--------	------

Code-Reject

07	ID	Length	Rejected-Packet
----	----	--------	-----------------

Echo-Request

09	ID	Length	Magic-Number	Data
----	----	--------	--------------	------

Discard-Request

0B	ID	Length	Magic-Number	Data
----	----	--------	--------------	------

Configure-Ack

02	ID	Length	Configuration Options
----	----	--------	-----------------------

Configure-Reject

04	ID	Length	Configuration Options
----	----	--------	-----------------------

Terminate-Ack

06	ID	Length	Data
----	----	--------	------

Protocol-Reject

08	ID	Length	Rej'd-Protocol	Rej'd-Info
----	----	--------	----------------	------------

Echo-Reply

0A	ID	Length	Magic-Number	Data
----	----	--------	--------------	------

LCP Configuration Options

Maximum-Receive-Unit

01	04	MRU	Default 1500 decimal
----	----	-----	----------------------

Authentication-Protocol

03	Length	Auth-Prot	Data	Default is no authentication
	04	C0	23	(PAP)
	05	C2	23	05 (CHAP using MD5)

Magic-Number

05	06	Magic-Number	Default is no magic number
----	----	--------------	----------------------------

Address-and-Control-Field-Compression

08	02	Default is no compression
----	----	---------------------------

Async-Control-Character-Map

02	06	Async-Map	Default is FFFFFFFF
----	----	-----------	---------------------

Quality-Protocol

04	Length	Qual-Prot	Data	Default is no LQM
	08	C0	25	Reporting-Period

Protocol-Field-Compression

07	02	Default is no compression
----	----	---------------------------

IPCP Configuration Options

The IP Control Protocol is similar to LCP, except only codes 1 through 7 are used.

IP-Addresses

01	0A	Source-IP-Address	Deprecated
		Destination-IP-Address	

IP-Address

03	06	IP-Address	No Default
----	----	------------	------------

IP-Compression-Protocol

02	Length	Compress-Prot	Data	Default is no compression
	06	00	2D	Max-Slot-ID Comp-Slot-ID (Van Jacobson Compressed TCP/IP)

PAP Packet Formats

Authenticate-Request

01	ID	Length	IDLen	Peer-ID
PwLen	Password			

Authenticate-Nak

03	ID	Length	MsgLen	Message
----	----	--------	--------	---------

Authenticate-Ack

02	ID	Length	MsgLen	Message
----	----	--------	--------	---------

CHAP Packet Formats

Challenge

01	ID	Length	ValSize	Value
Name				

Success

03	ID	Length	Message
----	----	--------	---------

Response

02	ID	Length	ValSize	Value
Name				

Failure

04	ID	Length	Message
----	----	--------	---------

Tracing Packets

The `ptrace` command allows you to see packet information as it passes through the PortMaster. Filters are used to define which packets you want to view. The `ptrace` command uses the name of a filter as its argument. All packets passing through the PortMaster are evaluated against the selected filter, except UDP and ICMP packets generated by the PortMaster itself. Packets that are permitted by the filter are displayed on the console with the following packet information:

- Source address of the packet
- Destination address of the packet
- Protocol
- Other protocol specific information, including source and destination port

Filters are used to narrow the `ptrace` output to only those packets of interest.

If no filter is specified with the `ptrace` command, packet tracing is disabled.



Note – If you are using `ptrace` through an administrative telnet session, your filter should deny your telnet packets. Otherwise, the `ptrace` command displays information for all of your own packets, creating an infinite loop of packets to tell you about the packets being generated.

The following example uses a filter that denies all telnet packets while allowing all other IP traffic for evaluation

```
Command> add filter all
Command> set filter all 1 deny tcp src eq 23
Command> set filter all 2 deny tcp dst eq 23
Command> set filter all 3 permit
Command> ptrace all
```

To stop viewing packet trace information, type:

```
Command> ptrace
```

Backing Up the PortMaster Configuration

The PortMaster configuration can and should be backed up. The backup file is not in human-readable form but can be reloaded using the `pminstall` program or the `install` function of `PMconsole`, which calls `pminstall`. The program used to backup the PortMaster configuration is `/usr/portmaster/pmreadconf`, use the syntax that follows.

Once the output file is created, change its permissions to 600 and move the file to the `/usr/portmaster/pm_data` directory, where it can be read by `pminstall`.

```
# /usr/portmaster/pmreadconf pm_name pm_passwd output_file
# chmod 600 output_file
# mv output_file /usr/portmaster/data
```

If you are using `PMconsole` for Windows, backing up the PortMaster is even simpler; just click the Backup Configuration button. See the *PMconsole for Windows Administrator's Guide* for more information.

Port State Verification

When PortMaster asynchronous ports are configured before cables and modems are attached, you may see two different port states when the `show port` command is invoked. Ports on the main system board may show `IDLE`, while ports on older expansion boards may show `USERNAME`. This is normal behavior because the value of carrier detect (CD) floats high on older expansion boards but not on the main system board. On more recent expansion boards, carrier is pulled low the same way it is on the main system board. On both old and new boards, as soon as modems are attached with `&C1` set and modem control turned on for the port, the ports should show a state of `IDLE`. For more information about port states, refer to Table 3-2 on page 3-6.

Administrative Telnet Sessions

The PortMaster supports up to four administrative telnet connections at a given time. To establish an administrative telnet session, telnet to your PortMaster and login as `!root` with your administrative password. If you are having trouble establishing an administrative telnet session, verify the TCP port for telnet access by typing `"show global"`. Check for stale telnet sessions by typing `show netcon` and looking for administrative connections to that port. Reset any connections that are stale by typing `"reset n#"` where `#` is the handle from the first column of the `"show netcon"` output.

You can make an administrative telnet session the console with the `"set console"` command. To release the console, use the `"reset console"` command.

In addition to four telnet sessions, you can have only one `pmcommand` or `pmconsole` or `pminstall` or `pmreadconf` program running at one time with a given PortMaster.

Diagnostic Mode

To force the PortMaster S0 port into diagnostic mode, follow these steps:

- 1. Attach a terminal to the console port S0 using a null modem cable.**

Configure the terminal for 9600 8N1. For more information, refer to the *Hardware Installation Guide* that came with your PortMaster.

- 2. Raise the Console DIP switch #1 left-most, on the back of the PortMaster to put the console into Diagnostic Mode.**

Refer to your *Hardware Installation Guide* for detailed information about the PortMaster DIP switches.

- 3. Turn the power on and observe the diagnostic output.**

If the PortMaster completes its diagnostics and produces a login: prompt, then the PortMaster booted correctly. If not, network booting may be required. Refer to the "Troubleshooting" chapter of your *Hardware Installation Guide* for more information on diagnostic boot messages.

Forgotten Passwords

This section describes what to do if you have forgotten the administrative password. If you are running a ComOS version prior to 2.4, IRX ComOS prior to 1.8R, or your ROM revision is F or earlier, follow the instructions in “Booting from the Network” instead.

If you are running ComOS version 2.4 or later or IRX ComOS version 1.8R or later, follow these steps if you have forgotten your password.

- 1. Place the PortMaster in diagnostic mode as described in “Diagnostic Mode” on page 19-10.**
- 2. Login to the PortMaster at the PortMaster Console login: prompt using `!root` and a password of `override`.**

A 16-character encrypted challenge is displayed.

- 3. Contact Livingston Technical Support for the appropriate 16-character one-time encrypted response.**

For information about contacting Technical Support, see page xxxii in the Preface of this guide.

- 4. Login to the PortMaster as `!root` and enter the 16-character encrypted response given by technical support as the password.**
- 5. Change the administrative password using the `set password` command.**
- 6. Type the `save all` command to save the new password to nonvolatile memory.**

Booting from the Network

Network booting is necessary if the FLASH RAM on your PortMaster becomes corrupted. You can determine that the FLASH is corrupt if any of the following occur:

- Your PortMaster never reaches the login: prompt during self diagnostics—when DIP switch #1 is UP.
- A checksum error on the ComOS is reported during the diagnostic boot process.
- Three unsuccessful upgrade attempts on PortMasters with a ComOS of version 3.0.4 or prior or IRX ComOS version 3.0.1R or prior. In this case the ComOS has run out of file descriptors.
- Netbooting is also required if you have forgotten the administrative password on a PortMaster with a ComOS prior to 2.4 or IRX ComOS versions prior to 1.8R.



Note – Network booting only works if you have a host on the Ethernet that supports TFTP. Otherwise, you must boot from the PROM monitor using the `download` command.

Network Booting

If you have determined that it is necessary to boot your PortMaster from the network, follow these steps:

1. **FTP the appropriate net-bootable ComOS, by typing:**

```
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd pub/livingston
ftp> get README.NETBOOT
ftp> quit
```

2. **Read the README.NETBOOT file to determine which net-bootable ComOS to download using FTP.**

The ComOS is referred to as GENERIC.OS in the rest of this example.

3. **Repeat step 1 to download the appropriate *GENERIC.OS*.**

4. If your boot host supports RARP and is on the same Ethernet segment as the PortMaster, add the Ethernet address of the PortMaster to your `/etc/ethers` file or your NIS map.
5. Start the `rarpd` service, if it is not already running, by typing:

```
% rarpd -a
```



Note – The exact command may vary depending on your operating system; refer to your system manual for more information about running `rarpd`.

If your boot host does not have RARP, use the procedures in “PROM Booting” on page 19-16.

6. Set up TFTP on your boot host by typing:

```
% umask 22
% mkdir /tftpboot
% mv GENERIC.OS /tftpboot/GENERIC.OS
% cd /tftpboot
% ln -s . tftpboot
```

This procedure should be done even if your host does not support RARP.

If you are booting a PM-2, PM-2E, PM-2R, or PM-2ER from the network, the file `GENERIC.OS` should be moved to `/tftpboot/GENERIC.PM2`. If you are booting an IRX from the network, the `GENERIC.OS` file should be moved to `/tftpboot/GENERIC.IRX`.

7. Using a text editor, uncomment the `tftp` entry in the `/etc/inetd.conf` file. To have the `inetd` daemon reread the `/etc/inetd.conf` file, send a `SIGHUP` signal to the `inetd` process.

This procedure applies to most UNIX systems. However, the procedure for enabling TFTP on your system may vary. Consult your system documentation.

8. Set the network boot (#2) DIP switch on the PortMaster to UP and turn the power switch ON.
9. Boot the PortMaster and login as `!root` with no password.

- 10. If you want to save your PortMaster configuration before reformatting the FLASH RAM and your host is supported, type the following on your UNIX host:**

```
% /usr/portmaster/pmreadconf pm_name pm_password output_file
```

There have been occasions when something in the configuration corrupted the FLASH RAM. If this is the case, reconfigure your PortMaster completely after you have installed the new ComOS in FLASH RAM.

- 11. To erase the configuration information stored in FLASH RAM, do one of the following on the PortMaster console:**

- If you are running ComOS 3.0, 3.0R, or later, type:

```
Command> set register 0xffff 0x0102
```

After about thirty seconds, the following message is displayed:

```
Successfully formatted FLASH 2
```

- If you are running ComOS 2.4 or older, type:

```
Command> set register 0xffff 0x0f02
```

After a few moments, the following message is displayed:

```
Successfully formatted FLASH 2
```

Then type:

```
Command> set register 0xffff 0x0f03
```

After a few moments, the following message is displayed:

```
Successfully formatted FLASH 3
```

- If you are performing this procedure because the ComOS in the FLASH RAM is corrupted, type:

```
Command> set register 0xffff 0x0f63
```

After about 30 seconds, the following message is displayed:

```
Successfully formatted FLASH 99
```



Caution – This command formats all four FLASH chips, thereby removing the entire ComOS. Do not reboot the PortMaster until you reinstall the ComOS.

These procedures have reformatted the FLASH RAM on the PortMaster.

- 12. If you have chosen one of the noconfig files, you need to set the IP address so that you can connect to the PortMaster using the PMconsole program installed on one of your workstations, by typing:**

```
Command> ifconfig ether0 address 192.168.200.1
```

In this case, 192.168.200.1 is the IP address of the PortMaster. If you are using a netmask other than 255.255.255.0 on your network, you must enter the netmask now by typing (for example):

```
Command> ifconfig ether0 netmask 255.255.255.192
```

- 13. To install the new ComOS into the FLASH RAM, run PMconsole on your workstation and select the Upgrade option from the Install menu.**
- 14. Turn off the power on the PortMaster. Remove the terminal from the console port and return the DIP switches to their normal operating positions. Turn on the PortMaster power to reboot the PortMaster.**

Everything should be working at this point. You must now reenter your configuration parameters.

PROM Booting

Beginning with PROM level F, a feature has been added that allows you to boot using the PROM instead of RARP. You can either boot from the `tftpd` daemon, or you can send a ComOS from your workstation to the console port on the PortMaster over a serial cable and boot from that.

If you have determined from the previous section that it is necessary to boot your PortMaster from PROM, follow these steps:



Note – This procedure only works with PROMs of level F or higher. The PROM version is displayed at boot time if the console port is in diagnostic mode.

1. **Place the PortMaster in diagnostic mode as described in “Diagnostic Mode” on page 19-10.**
2. **Attach a terminal to the console port of the PortMaster.**
3. **Turn the power switch to ON.**
4. **As the PortMaster starts to boot, press [ESC] or type ^[to display a > prompt.**

The commands shown in Table 19-4 are now available.

Table 19-4 PROM Commands

Command	Description
address	Allows you to set the address of the Ethernet interface.
netmask	Allows you to set the netmask of the Ethernet interface. Default is 255.255.255.0.
gateway	Allows you to set the default gateway in order to boot from a server on another network.
tftp	Causes the PortMaster to issue the TFTP request to the boot server.
download	Allows you to download the ComOS using the serial port.
continue	Causes the PortMaster to continue attempting to boot using RARP.

5. Enter the address of the PortMaster Ethernet port by typing:

```
> address 192.168.200.1
```

6. Set the gateway and netmask, if needed.
7. FTP the appropriate net-bootable ComOS to the workstation you want to use as the boot server, by typing:

```
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd pub/livingston
ftp> get README.NETBOOT
ftp> quit
```

8. Read the README.NETBOOT file to determine which net-bootable ComOS to download using FTP.
9. Repeat step 7 to download the appropriate *GENERIC.OS*.

If you are booting a PM-2, PM-2E, PM-2R, or PM-2ER from the network, the *GENERIC.OS* file should be moved to */tftpboot/GENERIC.PM2*. If you are booting an IRX from the network, the *GENERIC.OS* file should be moved to */tftpboot/GENERIC.IRX*.

10. Set up TFTP on your boot host by typing:

```
% umask 22
% mkdir /tftpboot
% mv GENERIC.OS /tftpboot/GENERIC.OS
% cd /tftpboot
% ln -s . tftpboot
```

This procedure should be done even if your host does not support RARP.

11. Using a text editor, uncomment the *tftp* entry in the */etc/inetd.conf* file. To have the *inetd* daemon reread the */etc/inetd.conf* file, send a *SIGHUP* signal to the *inetd* process.

This procedure applies to most UNIX systems. However, the procedure for enabling TFTP on your system may vary. Consult your system documentation.

12. Use one of the following to boot the PortMaster.

- To boot the ComOS from the boot server using TFTP, on the console type:

```
> tftp 192.168.200.2
```

Where *192.168.200.2* is the IP address of the TFTP host that has the *GENERIC.OS* software. The PortMaster then boots using the ComOS from the boot server. The new ComOS has not yet been loaded into the FLASH RAM of your PortMaster.

- To download the ComOS directly through the serial line, type:

```
> download size
```

Where *size* is the number of bytes of ComOS that follows. The PortMaster then boots using the ComOS downloaded from the serial connection. The new ComOS has not yet been loaded into the FLASH RAM of your PortMaster.

13. To install the new ComOS into the FLASH RAM, run PMconsole on your workstation and select the Upgrade option from the Install menu or run `pminstall`.

14. After the upgrade has completed, turn off the power on the PortMaster. Remove the terminal from the console port and return the DIP switches to their normal operating positions. Turn on the PortMaster power.

This reboots the PortMaster. Everything should be working at this point.

Command Line Summary 20

This chapter provides a summary of the syntax for all of the commands available from the command line interface for ComOS 3.1.4, 3.2.1R, and 3.2L, except for obsolete or experimental commands. The ISDN-related commands are available in ComOS 3.3 and ComOS 3.3L.

The Values table in the next section describes the different kinds of values that are used with the various commands. These values are shown in uppercase italics (like this: *Device*) to distinguish them from the actual keywords of the commands, which are in a lowercase plain font (like this: `version`).

The rest of the tables in this chapter describe the syntax for commands related to various functions. The choices are separated by vertical bars, like this: `on|off`, where one keyword from the list should be used. Optional portions of a command are surrounded by square brackets, like this: `[optional]`. Default values are underlined like this: `on|off`.

Values

Table 20-1 does not contain commands, it describes the different kinds of values that are used in commands.

Table 20-1 Values

Variable	Usage
<i>Device</i>	/dev/network or a pseudo-tty on a UNIX host
<i>Ether0</i>	ether0 or ether1 (on IRX-211), defaults to ether0 if omitted
<i>Filtername</i>	string up to 12 characters long naming a filter
<i>Group</i>	an integer from 0 to 99, 0 is default
<i>Handle</i>	n followed by a number, with no space between them
<i>Hex</i>	hexadecimal number with leading 0x
<i>Interface</i>	interface specification, e.g. ether0, frm1, ptp1, frmW1, ptpW1

Table 20-1 Values (Continued)

Variable	Usage
<i>Ipaddress</i>	IP dotted quad or hostname
<i>Ipmask</i>	dotted quad with 1's in high order bits, 0's in low order bits
<i>Ipxaddress</i>	IPX address in hex format Ipxnetwork:node
<i>Ipxnetwork</i>	32-bit hexadecimal number
<i>Isock</i>	IPX socket
<i>Itype</i>	ICMP packet type, 0 or higher
<i>Locname</i>	string up to 12 characters long naming a location
<i>MTU</i>	integer from 100 to 1500
<i>Metric</i>	integer from 1 to 15, defaults to 1
<i>Minutes</i>	integer from 0 to 240; note that 1 has special meaning
<i>ModemName</i>	Modem table entry
<i>NM</i>	integer 0 to 32, expressing the number of high-order bits set to 1 in a netmask
<i>Number</i>	number 0 or higher
<i>Password</i>	string up to 16 characters long
<i>Rule Number</i>	integer 1 or higher
<i>S0</i>	any async port s0-s29, or all
<i>S1</i>	any async or sync port s0-s29, w1, or all
<i>S10</i>	ISDN port s1-s2 or s10-s29, depending on model
<i>Seconds</i>	number 0 or higher
<i>String</i>	string of ASCII characters
<i>Tport</i>	TCP/IP port, integer from 0 to 65535
<i>Uport</i>	UDP/IP port, integer from 0 to 65535
<i>Username</i>	string up to 8 characters long naming a user
<i>W1</i>	any sync port s1-s4, w1, or all

General Commands

Table 20-2 lists commands for troubleshooting, general administration, and displaying the configuration of the PortMaster.

Table 20-2 General Commands

Command Syntax
version
reboot
quit
done
exit
help
ifconfig interface [address <i>Ipaddress</i>] [netmask <i>Ipmask</i>] [destination <i>Ipaddress</i>] [ipxnet <i>Ipxnetwork</i>] [ipxframe ethernet_802.2 ethernet_802_ii ethernet_802.3 ethernet_ii] [up] [down] [private] [-private]
dial <i>Locname</i> [-x]
ping [<i>Ipaddress</i>]
tracert [<i>Ipaddress</i>]
ptrace [<i>Filtername</i>]
pmlogin <i>Ipaddress</i>
rlogin <i>Ipaddress</i>
telnet <i>Ipaddress</i>
set debug <i>Hex</i>
set debug isdn [on off]
set register <i>Hex Hex</i>
set console [<i>S0</i> p0]
save <i>Ether0</i> <i>S0</i> <i>W1</i> all console filter host location netmask p0 routes snmp user

Table 20-2 General Commands (Continued)

Command Syntax
reset <i>Handle</i> <i>S0</i> <i>W1</i> all console dialer nic p0
show all
show arp <i>Interface</i>
show global
show ipxroutes
show memory
show netconns
show netstat
show routes
show sap
show sessions
show table filter host location netmask snmp user

Global Configuration

Table 20-3 contains all the global configuration commands that affect the entire PortMaster. For more information about global commands, refer to Chapter 4, “Configuring a PortMaster.”

Table 20-3 Global Configuration Commands

Command Syntax
show global
set password <i>Password</i>
set telnet <i>Tport</i>
set host [1 2 3 4] <i>Ipaddress</i>
set loghost <i>Ipaddress</i>
set namesvc domain nis
set nameserver <i>Ipaddress</i>

Table 20-3 Global Configuration Commands (Continued)

Command Syntax
set domain <i>String</i>
set gateway <i>Ipaddress Metric</i>
set default on <u>off</u> broadcast listen
set assigned_address <i>Ipaddress</i>
set reported_ip <i>Ipaddress</i>
set netbios on <u>off</u>
set pap <u>on</u> off
set maximum pmconsole <i>Number</i>
set isdn-switch att-5ess 5ess dms-100 <u>ni-1</u>

RADIUS Client Configuration

The commands shown in Table 20-4 allow you to configure the PortMaster to use a RADIUS server. RADIUS is consulted if a port is set for security on and a user is not found in the PortMaster User Table. For more information about RADIUS commands, refer to the *RADIUS Administrators Guide*.

Table 20-4 RADIUS Client Commands

Command Syntax
set authentication_server <i>Ipaddress</i>
set alternate_auth_server <i>Ipaddress</i>
set accounting [2] <i>Ipaddress</i>
set secret <i>Password</i>

Ethernet Configuration

The commands shown in Table 20-5 allow you to configure the Ethernet interface(s) ether0 and (on the IRX-211) ether1. For more information about Ethernet interface commands, refer to Chapter 5, “Configuring the Ethernet Interface.”

Table 20-5 Ethernet Interface Commands

Command Syntax
<code>set Ether0 address Ipaddress</code>
<code>set Ether0 netmask Ipmask</code>
<code>set Ether0 broadcast high <u>low</u></code>
<code>set Ether0 routing <u>on</u> broadcast listen off</code>
<code>set Ether0 ipxnet Ipxnetwork</code>
<code>set Ether0 ipxframe ethernet_802.2 ethernet_802.3 ethernet_ii</code>
<code>set ether0 ip up down enabled disabled ¹</code>
<code>set ether0 ipx up down enabled disabled ¹</code>

1. This command is nly available on ether0 port, even on the IRX-211

Asynchronous Port Configuration

The commands shown in Table 20-6 allow you to configure asynchronous serial ports. Commands marked with a leading bullet (•) can only be used if the port is configured for network hardwired operation. For more information about asynchronous port commands, refer to Chapter 6, “Configuring an Asynchronous Port.”

Table 20-6 Asynchronous Port Commands

Command Syntax
<code>show all</code>
<code>show S0</code>
<code>save S0</code>
<code>set S0 extended on <u>off</u></code>

Table 20-6 Asynchronous Port Commands (Continued)

Command Syntax
<pre> set S0 login [device Device] [network dialin dialout twoway] set S0 device Device [network dialin dialout twoway] set S0 twoway Device [network dialin dialout twoway] set S0 network dialin dialout twoway • set S0 network hardwired set S0 speed [1 2 3] 300 600 1200 2400 4800 <u>9600</u> 19200 38400 57600 76800 115200 set S0 parity even <u>none</u> odd strip set S0 databits 5 6 7 <u>8</u> set S0 stopbits <u>1</u> 2 set S0 xon/xoff <u>on</u> off set S0 rts/cts on <u>off</u> set S0 override xon rts speed parity databits on <u>off</u> set S0 modem cd on <u>off</u> set S0 modem ModemName set S0 group Group set S0 idletime Minutes set S0 security on <u>off</u> set S0 message String set S0 prompt String set S0 username autolog String set S0 hangup on <u>off</u> set S0 dialback_delay Seconds set S0 dtr_idle on off </pre>

Table 20-6 Asynchronous Port Commands (*Continued*)

Command Syntax
<pre>set S0 service_login netdata <u>portmaster</u> rlogin telnet [Tport]</pre>
<pre>set S0 service_device netdata <u>portmaster</u> rlogin telnet [Tport]</pre>
<pre>set S0 host <u>default</u> prompt Ipaddress</pre>
<pre>set S0 access on <u>off</u></pre>
<pre>set S0 termtype String</pre>
<pre>set S0 ifilter Filtername</pre>
<ul style="list-style-type: none"> • <pre>set S0 ofilter Filtername</pre>
<ul style="list-style-type: none"> • <pre>set S0 protocol slip ppp</pre>
<ul style="list-style-type: none"> • <pre>set S0 address Ipaddress</pre>
<ul style="list-style-type: none"> • <pre>set S0 netmask Ipmask</pre>
<ul style="list-style-type: none"> • <pre>set S0 destination Ipaddress [Ipmask]</pre>
<ul style="list-style-type: none"> • <pre>set S0 mtu MTU</pre>
<ul style="list-style-type: none"> • <pre>set S0 routing <u>on</u> off broadcast listen</pre>
<ul style="list-style-type: none"> • <pre>set S0 ipxnet Ipxnetwork</pre>
<ul style="list-style-type: none"> • <pre>set S0 compression on <u>off</u></pre>

Synchronous Port Configuration

The commands shown in Table 20-7 are used to configure synchronous serial ports. Commands marked with a leading bullet (•) can only be used if the port is configured for network hardwired operation. For more information about synchronous port commands, refer to Chapter 7, “Configuring a Synchronous WAN Port.”

Table 20-7 Synchronous Port Commands

Command Syntax
<pre>show all</pre>
<pre>show W1</pre>

Table 20-7 Synchronous Port Commands (Continued)

Command Syntax
<pre> save Wl set Wl extended on <u>off</u> set Wl network dialin dialout twoway hardwired set Wl protocol ppp • set Wl protocol frame • set Wl address Ipaddress • set Wl netmask Ipmask • set Wl destination Ipaddress [Ipmask] • set Wl ipxnet Ipxnetwork • set Wl routing on off broadcast listen • set Wl ifilter Filtername • set Wl ofilter Filtername • set Wl mtu MTU • set Wl lmi annex-d Seconds • set Wl dlci Dlci_list set Wl group Group set Wl hangup on off set Wl idletime Minutes set Wl modem cd on <u>off</u> set Wl speed 9600 14400 19200 38400 57600 76800 115200 56000 64000 1344k 1536k 2048k t1 tle e1 set Wl encode nrz nrzi </pre>

ISDN Port Configuration

ISDN BRI ports can be configured similarly to synchronous and asynchronous (V.120) ports. In addition, there are commands that allow you to configure the SPID and (optionally) the directory number (DN). The ISDN port configuration commands are shown in Table 20-8. For more information about ISDN port commands, refer to Chapter 18, “ISDN Connections.”

Table 20-8 ISDN Port Commands

Command Syntax
<code>show all</code>
<code>show S10</code>
<code>save S10</code>
<code>set S10 extended on <u>off</u></code>
<code>set S10 login [device <i>Device</i>]</code> <code> [network dialin dialout twoway]</code>
<code>set S10 device <i>Device</i> [network dialin dialout twoway]</code>
<code>set S10 twoway <i>Device</i> [network dialin dialout twoway]</code>
<code>set S10 network dialin dialout twoway</code>
<code>set S10 spid <i>String</i></code>
<code>set S10 directory dn <i>String</i></code>
<code>set S10 group <i>Group</i></code>
<code>set S10 idletime <i>Minutes</i></code>
<code>set S10 security on <u>off</u></code>
<code>set S10 message <i>String</i></code>
<code>set S10 prompt <i>String</i></code>
<code>set S10 username autolog <i>String</i></code>
<code>set S10 hangup on <u>off</u></code>
<code>set S10 dialback_delay <i>Seconds</i></code>
<code>set S10 service_login netdata <u>portmaster</u> rlogin telnet</code> <code> [<i>Tport</i>]</code>

Table 20-8 ISDN Port Commands

Command Syntax
set S10 service_device netdata <u>portmaster</u> rlogin telnet [Tport]
set S10 host <u>default</u> prompt Ipaddress
set S10 termtype String
set S10 ifilter Filtername

Parallel Port Configuration

The commands shown in Table 20-9 allow you to configure the parallel port P0.

Table 20-9 Parallel Port Commands

Command Syntax
show p0
save p0
set p0 extended on off
set p0 device Device
set p0 disabled
set p0 service_device netdata portmaster rlogin telnet [Tport]
set p0 host default Ipaddress
set p0 disconnect Seconds infinity

DLCI Table Configuration

The commands shown in Table 20-10 allow you to configure the DLCI table, which is used to split a Frame Relay interface into two subinterfaces. For more information about Frame Relay commands, refer to Chapter 16, “Synchronous Frame Relay Connections.”

Table 20-10 DLCI Table Commands

Command Syntax
<pre>show location Locname add dlci Locname Dlci [Ipaddress] add ipdlci Locname Dlci [Ipaddress] add ipxdlci Locname Dlci [Ipxnetwork] delete dlci Locname Dlci delete ipdlci Locname Dlci</pre>

Host Table Configuration

The commands shown in Table 20-11 allow you to configure the host table inside the PortMaster in cases where DNS or NIS is not available.

Table 20-11 Host Table Commands

Command Syntax
<pre>show table host save host add host Ipaddress String delete host Ipaddress String</pre>

Filter Table Configuration

The commands shown in Table 20-12 allow you to configure the filter table. Filters can be applied to users, locations, or network hardwired ports, and can be used for debugging with the `ptrace` command. For more information on setting filters, refer to Chapter 10, “Configuring Filters.”

Table 20-12 Filter Table Commands

Command Syntax
<pre> show table filter show filter <i>Filtername</i> save filter add filter <i>Filtername</i> delete filter <i>Filtername</i> set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress/NM</i>] [log] set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress/NM</i>] tcp [src eq lt gt <i>Tport</i>] [dst eq lt gt <i>Tport</i>] [established] [log] set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress/NM</i>] udp [src eq lt gt <i>Tport</i>] [dst eq lt gt <i>Tport</i>] [log] set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress/NM</i>] icmp [type <i>Itype</i>] [log] set ipxfilter <i>Filtername</i> <i>RuleNumber</i> permit deny [srcnet <i>Ipxnetwork</i>] [srchost <i>Ipxaddress</i>] [srcsocket eq gt lt <i>Isock</i>] [dstnet <i>Ipxnetwork</i>] [dsthost <i>Ipxaddress</i>] [dstsocket eq gt lt <i>Isock</i>] set sapfilter <i>Filtername</i> <i>RuleNumber</i> permit deny [server <i>String</i>] [network <i>Ipxnetwork</i>] [host <i>Ipxaddress</i>] [socket eq gt lt <i>Isock</i>] </pre>

Location Table Configuration

The commands shown in Table 20-13 are used to configure the Location Table, used to specify network dial-out locations. For more information about Location Table commands, refer to Chapter 9, “Configuring Dial-Out Locations.”

Table 20-13 Location Table Commands

Command Syntax
<code>show table location</code>
<code>show location <i>Locname</i></code>
<code>save location</code>
<code>add location <i>Locname</i></code>
<code>delete location <i>Locname</i></code>
<code>set location <i>Locname</i> continuous manual on_demand</code>
<code>set location <i>Locname</i> protocol slip ppp frame</code>
<code>set location <i>Locname</i> destination <i>Ipaddress</i></code>
<code>set location <i>Locname</i> netmask <i>Ipmask</i></code>
<code>set location <i>Locname</i> ipxnet <i>Ipxnetwork</i></code>
<code>set location <i>Locname</i> routing on off broadcast listen</code>
<code>set location <i>Locname</i> group <i>Group</i></code>
<code>set location <i>Locname</i> map <i>Hex</i></code>
<code>set location <i>Locname</i> compression on off</code>
<code>set location <i>Locname</i> mtu <i>MTU</i></code>
<code>set location <i>Locname</i> script v25bis <i>RuleNumber String String</i></code>
<code>set location <i>Locname</i> maxports <i>Number</i></code>
<code>set location <i>Locname</i> high_water <i>Number</i></code>
<code>set location <i>Locname</i> idletime <i>Minutes</i></code>
<code>set location <i>Locname</i> ifilter <i>Filtername</i></code>
<code>set location <i>Locname</i> ofilter <i>Filtername</i></code>

Table 20-13 Location Table Commands (Continued)

Command Syntax
<code>set location Locname multilink on off</code>

Modem Table Configuration

The commands shown in Table 20-14 allow you to configure the modem table, which describes how to initialize a modem attached to an asynchronous port. See the `set modem` command in Table 20-6 on page 20-6 for additional information. For more information about configuring modems, refer to Chapter 6, “Configuring an Asynchronous Port.”

Table 20-14 Modem Table Commands

Command Syntax
<code>show table modem</code>
<code>show modem ModemName</code>
<code>add modem ModemName String Speed String</code>
<code>delete modem ModemName</code>

Netmask Table Configuration

The commands shown in Table 20-15 allow you to configure the netmask table used for routing noncontiguous subnets. Use caution if configuring static netmasks.

Table 20-15 Netmask Table Commands

Command Syntax
<code>show table netmask</code>
<code>save netmask</code>
<code>add netmask Ipaddress Ipmask</code>
<code>delete netmask Ipaddress</code>

Route Table Configuration

The commands shown in Table 20-16 allow you to add and remove static routes to the routing table. The `show route` command marks static routes with the HS (for host) and NS (for network) flags.

Table 20-16 Route Table Commands

Command Syntax
<code>show route</code>
<code>save route</code>
<code>add route <i>Ipaddress Ipaddress Metric</i></code>
<code>delete route <i>Ipaddress</i></code>
<code>add ipxroutes <i>Ipxnet Ipxaddress Metric Ticks</i></code>

SNMP Configuration

The commands shown in Table 20-17 allow you to configure the PortMaster as an SNMP agent. Use caution if you are allowing SNMP writes.

Table 20-17 SNMP Commands

Command Syntax
<code>show table snmp</code>
<code>save snmp</code>
<code>set sysname <i>String</i></code>
<code>set snmp on off</code>
<code>set snmp readcommunity writecommunity <i>String</i></code>
<code>add snmp host reader writer any none <i>Ipaddress</i></code>

User Table Configuration

The commands shown in Table 20-18 allow you to configure the User Table that is used to authenticate dial-in users. RADIUS can also be used to authenticate dial-in users; however, the User Table is consulted first. For more information about User Table commands, refer to Chapter 8, “Configuring Dial-In Users.”

Table 20-18 User Table Commands

Command Syntax
<pre>show table user show user Username save user add netuser Username [password Password] add user Username [password Password] delete user Username set user Username password Password set user Username dialback Locname String set user Username host default prompt Ipaddress set user Username service netdata portmaster rlogin telnet [Tport] set user Username protocol slip ppp set user Username destination Assigned Negotiated Ipaddress set user Username netmask Ipmask set user Username ipxnet Ipxnetwork set user Username routing on off broadcast listen set user Username compression on off set user Username ifilter Filtername set user Username ofilter Filtername set user Username mtu MTU set user Username map Hex</pre>

Glossary

A

agent	A software program installed in a managed network device. An agent stores management information and responds to the manager's request for this information.
alias	A name assigned by the user to a hub or node.
Annex-D	Refers to the ANSI T1.617 Frame Relay Annex D version of the LMI (Local Management Interface) protocol. The Annex-D protocol has a more robust feature set than the proprietary Cisco/Stratacom LMI, but was developed later. Recent versions of the PortMaster software support either type of LMI. Earlier versions supported only the Cisco/Stratacom version. See also LMI.
ARP	Address Resolution Protocol. This protocol discovers physical hardware network addresses that correspond to the high-level IP address for a given node.
ASCII	American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.
AUTOEXEC.BAT	A file that is automatically read and executed by DOS during the startup process.

B

baud	The number of discrete signal events per second occurring on a communications channel. Although not technically accurate, baud is commonly used to mean bit rate.
B-channel	A 64Kbps synchronous channel that is part of an ISDN BRI.
BONDING	Bandwidth ON Demand INTERoperability Group. A method for combining two B-channels into a single 128Kbps channel.

booting	The process in which a device obtains information and begins to process it to attain a state of normal operation.
bps or b/s	Bits per second, a unit for measuring the data rate.
BRI	Basic Rate Interface. ISDN interface that consists of two 64Kbps B-channels for voice or data and one 16Kbps D-channel for signalling.
broadcast packets	Packets that are sent to all network nodes.

C

click	To position the mouse pointer on an object, then press and release the left mouse button.
client-server environment	An environment where a computer system or process requests a service from another computer system. For example, a workstation may request services from a file server across a network.
committed information rate	The minimum bandwidth guaranteed to be available if required on a Virtual Circuit. (Guaranteed Bandwidth) often called CIR.
community strings	Community strings can be assigned to SNMP agents and are used to restrict access to those devices. SNMP community strings include read community and write community.
console port	A serial port on a PortMaster, used to set its IP address using a terminal and for configuration.
CRC errors	Cyclic Redundancy Check errors. These errors can indicate problems with source station hardware, receivers, retiming modules/repeaters, bridges, cabling, or transceivers.
CSU	Channel Service Unit. An ancillary device needed to adapt the V.35 interface to a port on a telephone carrier switch. The CSU is placed between the DTE and the switch.

D

DCE	Data Communications Equipment, such as a modem.
DDE	Dynamic Data Exchange. A form of interprocess communication that uses shared memory to exchange data between applications. Applications can use a one-time data transfer or ongoing exchanges.

DLCI	Data Link Connection Identifier. A unique number that represents a particular PVC on a particular physical segment of the Frame Relay network. As the frame is passed through each switch, the DLCI is remapped as necessary, automatically by the switch. A DLCI identifies a circuit in both directions, not a destination or source.
DLL	Dynamic Link Library. Windows automatically loads the applications into memory when required and unloads them when space is needed for other applications.
DMA	Direct Memory Access. Direct access to computer memory not mediated by a microprocessor.
DOS	The primary Disk Operating System used by IBM and compatible personal computers.
DRAM	Dynamic Random Access Memory. A type of memory computer integrated circuit.
DSU	Digital Service Unit. An ancillary device needed to adapt the V.35 interface on a port to a leased line or Frame Relay switch.
driver	A software module that controls an input/output port or external device such as a keyboard or a monitor. TCP/IP uses a driver to control the network interface cards.
DTE	Data Terminal Equipment, such as a terminal. PortMaster serial ports are DTE.

E

echo test	A diagnostic test used to check network reachability in which an ICMP or SNMP test packet is sent to elicit a standard response.
Ethernet	A network communications system developed and standardized by Digital Equipment Corporation, Intel, and Xerox using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration of Ethernet into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber optic cable, broadband, and unshielded twisted pair.

F

FRAD

Frame Relay Asynchronous Device. A special kind of CSU/DSU that takes an asynchronous SLIP (sometimes PPP) connection and turns it into a single PVC for Frame Relay.

frame

A packaging structure for network data and control information. A frame consists of the destination address, source address, length field, data, pad, and frame check sequence. The 802.3 standard for Ethernet specifies that the minimum size data frame is 64 bytes and the maximum size data frame is 1518 bytes.

FTP

File Transfer Protocol. FTP is a TCP/IP protocol used to log onto a network host, list directories, and transfer files.

G

graphical user interface

See GUI.

GUI

Graphical User Interface. A software interface that is based on a graphical representation of various elements. PMconsole has several different GUIs.

H

hop

A router-to-router transmission required when a data packet must be routed to a remote network.

I

icon

A graphic symbol on a user interface display.

ICMP

Internet Control Message Protocol. This part of the Internet Protocol (IP) allows for generation of error messages, test packets, and informational messages related to IP. This protocol is used by the ping function to send an ICMP Echo Request to a network host, which replies with an ICMP Echo Reply.

in-band signaling

Signaling over a network.

interface	Connection and interaction between hardware, software, and the user. An interface is activated by programming language commands and hardware signals. The interface between components in a network is called a protocol.
internet	A network of networks.
Internet	THE network of networks, stretching worldwide to millions of computers and users.
IP	The Internet Protocol defined in RFC 791.
IPCP	IP Control Protocol. A protocol used by PPP for establishing and configuring an IP link over PPP.
IPX	The Internet Packet Exchange protocol defined by Novell, Inc.
IPXWAN	IPX Wide Area Network protocol, used to establish and configure an IPX link over PPP, as described in RFC 1634.
ISDN	Integrated Services Digital Network. A digital communications standard designed to allow the transmission of voice, data, images, and video over existing copper phone lines.
ISO	International Organization for Standards. The international organization that sets standards for network communication protocols.
K	
KB	Kilobyte(s). 1024 bytes.
Kb	Kilobits, 1024 bits.
Kbps	Kilobits per second.
L	
LAN	Local Area Network. A local collection, usually within a single building or several buildings, of personal computers and other devices connected by cabling to a common transmission medium, allowing users to share resources and exchange files.
LCP	Link Control Protocol. Used by PPP for establishing, configuring, and testing the data-link connection.

LED	Light Emitting Diode.
line speed	The speed of the physical wire attached to the interface or interface hardware. The line speed is 10Mbps for Ethernet and 1.544Mbps for T1. Fractional T1 is often implemented with a wire speed of T1 (1.544Mbps) and a lower port speed. See also port speed. Upgrading line speed is generally a hardware change.
LMI	Local Management Interface. A protocol used to communicate link status and PVC status in Frame Relay. There are two types of LMI available on Frame Relay; the original proprietary Cisco/Stratacom LMI, and the ANSI T1.617 Annex-D LMI. In the PortMaster, LMI refers to the Cisco/Stratacom implementation. See also Annex-D.
local area network	See LAN.
M	
MAC address	Media Access Control address. A unique 48-bit binary number (usually represented as a 12-digit hexadecimal number) encoded in the circuitry of a device to identify it on a local area network.
management information base	See MIB.
management station	A workstation or PC capable of retrieving and analyzing statistical information from networked SNMP agents.
MB	Megabyte(s). 1,048,576 bytes.
Mb/s	Megabits per second, a unit for measuring data rates.
menu bar	An area at the top of a Microsoft Windows display, below the title bar, that displays the names of pull-down menus the user can select with the mouse.
MIB	Management Information Base. A set of parameters that an SNMP-based management station can query from the SNMP agent of a network device.
Microsoft Windows	The graphical user interface for the IBM and compatible personal computers.
modem	A modulator-demodulator; a device that converts between the digital signals used by computers and analog signals that can be transmitted over telephone lines.

mouse	A pointing device, usually containing more than one functional button.
MS-DOS	Microsoft Disk Operating System. A version of DOS used by IBM-compatible personal computers.

N

network	A collection of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances.
network management	In the OSI model, the five functional application areas of accounting management, configuration management, fault management, performance management, and security management.
NIC	Network Information Center. An organization that provides information and services related to networking technologies. NIC also is an acronym for network interface card.
NOC	Network Operations Center.
node	A device, such as a personal computer, server, switching point, bridge, or gateway, connected to a network at a single location; also called station. <i>See</i> station.
NT1	An ISDN term that identifies the customer-end termination of the local phone company wires (local loop).

O

ODI	Open Datalink Interface. Novell's extension to its Open Datalink Interface specification. ODI isolates the protocol stack from the network adapter drivers allowing hardware independence for network connectivity.
out-of-band	A remote connection, or a connection outside of the connected networks, established over a modem. This connection is useful when network communications are not available.

P

packet	A unit of data sent across a network.
partition	Electronic isolation of an Ethernet device from network communications.
physical circuit	A physical connection between two devices.
ping	Packet INternet Groper. A program that is useful for testing and debugging networks. Ping sends an ICMP echo packet to the specified host and waits for a reply. Ping reports success or failure and statistics about its operation.
port	The physical channel or connection through which data flows.
port speed	The rate at which data is accepted by the port at the end of the wire. Specifically, in Frame Relay, or other fractional T1 applications, it is common to have a T1 line between the site and the telecommunications provider, but the telecommunications provider only accepts the number of bits per second ordered by the customer into the port on its equipment. Upgrading port speed is generally a software change.
program manager	The main display in Microsoft Windows, from which the user selects functions and manages applications.
PVC	Permanent Virtual Circuit. A circuit that defines a permanent connection in a switched digital service, such as Frame Relay. Frame Relay is the only switched digital service that uses PVCs supported by PortMasters.

R

RARP	Reverse Address Resolution Protocol. A protocol used in network routers.
RFC	Request For Comments. A document that describes Internet standards such as the Internet Protocol (IP).
router	A device that connects two or more networks and can direct traffic based on network resource availability.
RS-232 interface	A standard for data communication using serial data and control signals.
runt packet	A packet with a frame size between 8 and 63 bytes with FCS or alignment errors. The runt packet is presumed to be a fragment resulting from a collision.

S

serial port	A bidirectional channel through which data flows one bit at a time. Asynchronous serial ports most often use 10 bits for a character of data including 1 start bit, 8 data bits, and 1 stop bit.
server	A computer or a specialized device that provides and manages access to shared network resources, such as hard disks and printers.
SNMP	Simple Network Management Protocol. This protocol is defined in RFC 1157. This protocol relates to management of devices on IP networks.
SPID	Service Profile Identifier.
station	A device, such as a personal computer, server, switching point, bridge, or gateway, connected to a network at a single location; also called a node. <i>See node.</i>
subnet mask	A subnet mask identifies the subnet field of a network address. The subnet mask is a 32-bit Internet address written in dotted-decimal notation with ones in the network and subnet portions of the address.
SVC	Switched Virtual Circuit. A connection established between two physical circuits, such as an ordinary telephone call. The call creates a virtual circuit between the originator and the party called.

T

Telnet	Internet standard protocol for remote terminal connection service. Telnet is described in RFC 854.
terminal	A device with a keyboard, an RS-232 serial interface, and a display for communicating with a computer.
terminal adapter (TA)	A device that provides ISDN compatibility to non-ISDN devices. An asynchronous TA turns an asynchronous bit stream into ISDN and looks like a modem to the PortMaster. A synchronous TA takes a synchronous bit stream and turns it into ISDN, typically supports V.25bis dialing and connects to a PortMaster synchronous port. Some TAs can be configured for synchronous or asynchronous operation.
terminal emulator	A program that makes a PC screen and keyboard act like a video display terminal of another computer.

TFTP	Trivial File Transfer Protocol. A simplified version of FTP that transfers files but does not provide password protection or user directory capability. TFTP can be used by diskless devices that keep software in ROM and use it to boot themselves. The PortMaster can be booted using RARP and/or TFTP.
thick Ethernet	An Ethernet connection using a 15-pin D-shell connector and an AUI cable connected to a transceiver. Also known as 10Base5.
thin Ethernet	An Ethernet connection where the transceivers are built into the device and a BNC connector with cable are used to complete the connection; generally using an RG-58 coaxial cable. Also known as 10Base2.
twisted pair	Abbreviated UTP (unshielded twisted pair), a pair of thin-diameter insulated wires commonly used in telephone wiring. The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Used for 10BaseT Ethernet with RJ-45 connectors.

U

U interface	The ISDN interface defined as the connection between the NT1 and the telephone company local loop. The U interface standard is set by each country. The U interface described in Livingston documentation refers to the U.S. definition.
UDP	User Datagram Protocol. This protocol is defined in RFC 768. This is a connectionless protocol that adds multiplexing to IP.
UNIX	A multiuser, multitasking operating system originally developed by AT&T that runs on a wide variety of computer systems.

V

V.120	A CCITT standard for performing asynchronous rate adaptation into ISDN.
V.25bis	A CCITT standard defining how to dial on synchronous devices such as ISDN or switched 56K.

V.32bis An ITU-T standard that extends the V.32 connection range from 4800 bps to 14.4K bps. V.32 bis modems fall back to the next lower speed when line quality is impaired, and fall back further as necessary. They fall forward to the next higher speed when line quality improves.

V.34 An ITU-T standard that allows data rates as high as 28.8K bps.

virtual circuit A logical connection between two endpoints on a switched digital network. Virtual circuits can be switched or permanent. A switched virtual circuit (SVC) is used when you make an ordinary telephone call, an ISDN connection, or a V.25 switched 56K connection. A permanent virtual circuit (PVC) is used in Frame Relay. See also PVC and SVC.

W

Windows Graphics-based operating environment from Microsoft that integrates with DOS to provide a desktop environment similar to the Macintosh.

References

CCITT

V.25bis

V.120

Requests For Comments (RFC)

These documents can be found online using any World Wide Web browser.

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specification*

RFC 950, *Internet Standard Subnetting Procedure*

RFC 988, *Host Extensions for IP Multicasting*

RFC 1058, *Routing Information Protocol*

RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1166, *Internet Numbers*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1331, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1334, *PPP Authentication Protocols*

RFC 1362, *Novell IPX Over Various WAN Media (IPXWAN)*

RFC 1490, *Multiprotocol Interconnect Over Frame Relay*

RFC 1597, *Address Allocation for Private Internets*

RFC 1627, *Network 10 Considered Harmful (Some Practices Shouldn't be Codified)*

RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*

RFC 1700, *Assigned Numbers*

RFC 1717, *The PPP Multilink Protocol (MP)*

RFC 1814, *Unique Addresses are Good*

Books

Albitz, Paul and Cricket Liu. *DNS and BIND in a Nutshell*. O'Reilly & Associates, Inc. (ISBN 1-56592-010-4)

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc. 1995. (ISBN 1-56592-124-0)

Cheswick, William R. and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley 1994. (ISBN 0-201-63357-4)

Japanese translation (ISBN 4-89052-672-2)

Errata are available from:
ftp://ftp.research.att.com/dist/internet_security/firewall.book

Comer, Douglas. *Internetworking with TCP/IP*. Prentice-Hall. (ISBN 0-13-468505-9)

Hunt, Craig. *TCP/IP Network Administration*. O'Reilly & Associates, Inc. (ISBN 0-937175-82-X)

The Basics Book of ISDN. Addison-Wesley Publishing Company, 1994. (ISBN 0-201-56368-1)

Index

Symbols

=PAP= 9-12

A

access control 10-1

access filter, setting 6-11, 8-8

adding input and output filters 5-3

address

 assigned 8-5

 negotiated 8-5

 specified 8-5

administrative Telnet sessions 19-10

allowing bidirectional communications 6-18

Annex-D

 configuration 16-9

 description of 16-3

 keepalives 7-11

 setting 7-9

ARP 2-9

assigned addresses 8-5

assigned pool 4-10

 configuring 13-3

asynchronous

 applications 1-12

 chat script examples 9-11

 permanent connections 3-16

asynchronous port parameter

 access filter 6-11

autolog 6-12

compression 6-10

console 6-12

destination

 IP address 6-9

 netmask 6-9

dial group 6-8

dial-in and out 6-7

DTR Idle 6-18

enabling routing 6-10

extended information 6-11

flow control 6-18

host 6-4

host device 6-5

host device value 6-5

idle time 6-12

input and output filters 6-10

IPX network number 6-9

line hangup 6-18

login message 6-11

login prompt 6-11

login service 6-3

modem control 6-17

MTU 6-8

network 6-7

override 6-6

parity 6-17

port security 6-12

port type 6-3

- PPP async map 6-10
- protocol 6-8
- TCP header compression 6-10
- terminal type 6-4
- TwoWay 6-6
- user login 6-3
- asynchronous ports
 - configuring 6-1
- attaching
 - filters 10-3
 - modems to ports 6-14
- authentication process 3-5
- autolog parameter 6-12

B

- backup
 - configuration 19-9
- B-channel, definition of 7-6
- bidirectional communications 6-18
- booting a PortMaster 3-2
- booting from a PROM 19-16
- booting from the network 19-12
- boundaries of routes 4-11
- BRI port 7-6
- broadcast 5-3
 - high 5-4
 - low 5-4
- broadcast address, setting 5-4

C

- CHAP
 - authentication 3-15, 6-7, 7-7
 - authentication, ISP 12-8
 - packet formats 19-7

- transactions 3-16
- chat script
 - asynchronous 9-11
 - description of 9-9
 - send and expect strings 9-10
 - V.25bis 9-12
- COMMAND status 3-6
- commands
 - ifconfig 19-2
 - ping 19-1
 - ptrace 19-8
 - reset 19-4
 - traceroute 19-4
- communications servers, description of 1-3, 1-5
- ComOS
 - description of 1-7
 - version number 19-3
- compression
 - bidirectional 8-6
- configuration
 - backing up 19-9
 - overview 1-15
 - steps 4-3
 - testing 9-13
 - tips 4-1
- configuring
 - an ISP 13-1
 - asynchronous ports 6-1
 - modems for login 13-8
 - PortMasters 4-2
- CONNECTING status 3-6
- connection type
 - continuous 9-3
 - manual 9-3
 - on-demand 9-3

connections

- dial on-demand 11-1
- dial-in 1-13
- Frame Relay 16-3
- host device 14-1
- Internet Service Provider 12-1
- ISDN 18-1
- ISDN on-demand 11-14, 12-11
- ISDN, description of 7-6
- leased line 7-3, 15-1
- login to host 1-13
- login user 13-1
- office to office 11-1
- routing over Frame Relay 1-14
- routing over ISDN 1-15
- routing over leased lines 1-14
- routing over switched 56K 1-14
- shared devices 1-14
- switched 56K 7-5
- to the Internet 1-13

console, setting a port 6-12

continuous dial out connections 9-3

controlling access 10-1

conventions xxxi

creating a filter 10-4

CSU/DSU

- switched 56K 17-1

- using 7-9

D

Data Link Channel Identifier 7-4

- description of 16-1

D-channel, definition of 7-6

debugging network problems 19-3

decisions, preconfiguration 1-9

dedicated connections 6-7, 6-8, 7-7

default gateway, setting 4-5

default login host 8-8

default routing, setting 4-5

defining

- dial-in login users 13-9

- dial-in network users 13-10

- dial-in users 11-7, 17-7, 17-10, 18-9

- dial-out locations 11-8, 17-8, 17-11, 18-10

destination

- IP address, setting 6-9, 7-8, 9-5

- netmask, setting 6-9

device services

- description of 3-10

- netdata 3-12, 6-6

- PortMaster 3-11, 6-5

- rlogin 3-11, 6-5

- Telnet 3-12, 6-5

- using 14-4

device value 6-5

diagnostic mode 19-10

dial group

- description of 9-7

- setting 6-8, 7-10, 9-7

dial on-demand routing 9-3

dial script 9-11

dialback

- login user 8-10

- network users, configuring 8-7

- users 8-2

dialer window 9-13

dial-in

- and out operation 3-13, 3-14, 6-7

- connections 1-13

- description of 3-13
- port configuration 14-7
- dial-out
 - connection types 9-3
 - description of 3-14
- dial-out parameters
 - destination IP address 9-5
 - dial group 9-7
 - enabling routing 9-5
 - filters 9-7
 - high water mark 9-9
 - idle timeout 9-7
 - IPX network number 9-5
 - maximum ports 9-8
 - maximum transmission unit 9-6
 - netmask 9-5
 - network protocol 9-4
 - TCP header compression 9-6
- direct data link login applications 3-9
- direct host connections 6-12
- disabling a port 19-4
- DISCONNECTING status 3-6
- displaying extended information 6-11, 7-7
- DLCI 7-4, 16-1
 - learning 7-11
 - list, setting 7-11
- DNS, setting 4-6
- DSR value 6-19
- DTR Idle 6-18
 - transitions 6-19
- dynamically setting the IP address 4-7

E

- enabling

- IP traffic 5-4
 - outbound traffic 6-17, 7-9
 - routing 9-5
- escaping PPP characters 6-10
- ESTABLISHED status 3-6
- establishing a log in session 3-7
- Ethernet
 - 802.2 5-5
 - 802.2_II 5-5
 - 802.3 5-5
 - hardware connections 5-1
 - II 5-5
 - parameter descriptions 5-2
- Ethernet parameters
 - broadcast address 5-4
 - enabling IP traffic 5-4
 - IP address 5-3
 - IPX 5-4
 - IPX frame type 5-5
 - IPX network number 5-5
 - NetBIOS 5-6
 - netmask 5-4
 - routing 5-3
- example applications, all products 1-11
- extended information 6-11, 7-7
- external clock
 - leased line 15-5

F

- Filter Table, description of 10-3
- filters
 - access 10-19
 - adding 5-3
 - adding rules 10-5
 - allow auth queries 10-17

- allowing RIP packets 10-17
- asynchronous port 6-10
- attaching 10-3
- creating 10-4
- description of 10-1
- DNS outside local subnet 10-16
- examples 10-14
- features 10-2
- firewall 10-18
- FTP packets 10-12
- hardwired port 10-15
- input and output 9-7
- internet 10-15
- Internet Service Provider 12-10
- IP rules 10-5
- IPX rules 10-11
- logging results 10-19
- permit and deny 10-14
- rules 10-3
- SAP rules 10-12
- setting input and output 6-10, 7-10, 8-7
- simple 10-14
- synchronous port 7-10
- TCP and UDP port services 10-8
- TCP protocol options 10-7
- tracing packets 19-8
- UDP options 10-8

FireWall IRX router, description of 1-3

FLASH RAM recovery 19-12

flow control

- hardware 6-18
- software 6-18

Frame Relay

- connections 16-3
- description of 16-3
- parameters 7-11

- protocol setting 9-4
- routing 1-14
- subinterface 16-10

FTP packet filtering 10-12

G

gateway, setting 4-8

global parameters

- default gateway 4-5
- default routing 4-5
- example of 4-4
- function 4-3
- gateway 4-8
- Host Table 4-7
- IP address assignment 4-7
- metric 4-9
- name service 4-6
- Netmask Table 4-9
- password 4-5
- route destination 4-8
- setting 4-4
- SNMP monitoring 4-7
- static routes 4-8
- system logging 4-6
- system name 4-4
- Telnet 4-6
- ticks 4-9

H

hanging up a line 6-18

hardware flow control 6-14, 6-18

hardwired connections 3-16

- limitations of 3-17

high water mark

- description of 9-8

- setting 9-9
- high-speed dedicated connections 7-1
- host connections, direct 6-12
- host device 6-5
 - access 6-1
 - configuration 3-10
 - connections 14-1
- host name
 - default 6-4
 - prompt 6-4
 - specifying 6-4
- Host Table
 - configuring 4-7
- HOSTNAME status 3-6
- how to contact Livingston xxxii

I

- IDLE status 3-6
- idle time
 - setting 6-12, 9-7
- ifconfig
 - command 19-2
 - flags 19-2
- in.pmd daemon 14-1
- INITIALIZING status 3-6
- integrated NT1 7-6
- interface, definition of 3-4
- internet (IP) addressing 2-1
 - class A 2-2
 - class B 2-3
 - class C 2-3
 - class D 2-4
 - class E 2-4
 - conventions 2-5
 - examples 2-2
 - notation 2-2
 - reserved addresses 2-4
 - routing 2-8
 - subnet masks 2-6
 - subnetting 2-6
- Internet connections 1-13
- IP
 - enabling traffic 5-4
 - filter rules 10-5
 - protocol 2-1
- IP address
 - assignment 4-7
 - setting 5-3, 8-5, 11-4, 13-4, 14-5, 15-4, 16-6, 17-4, 18-7
- IPCP configuration options 19-7
- IPX
 - addressing conventions 2-5
 - encapsulation 5-5
 - filter rules 10-11
 - frame type 5-5
 - protocol 2-1
- IPX network number, setting 5-5, 6-9, 7-9, 8-5, 9-5
- IRX routers, description of 1-3
- ISDN
 - authentication 18-1
 - B-channel 7-6
 - connection 18-1
 - connections 7-6, 17-1
 - D-channel 7-6
 - on-demand connections 11-14, 12-11
 - routing 1-15
 - SPID 18-5
 - switch type 18-1

- troubleshooting 18-15
 - V.25bis dialing 17-5
 - with BRI ports 18-1
- ISP
- connection to 12-1
 - how to configure 13-1
- K**
- keepalives 7-11
- L**
- LCP
- configuration options 19-6
 - packet formats 19-6
- lease line
- routing 1-14
- leased line
- connection 15-1
 - connections, description of 7-3
 - CSU/DSU 15-1
 - PPP 15-1
- LEDs
- ISDN 18-16
- line hangup 6-18
- line speed, description of 16-2
- listen 5-3
- LMI 7-5
- configuration 16-9
 - description of 16-3
 - setting 7-11
- load-balancing 9-8
- configuring 9-8
- Local Management Interface 7-5
- local management interface, description of 16-3
- location name 9-2
- location parameters
- destination IP address 9-5
 - dial group 9-7
 - enabling routing 9-5
 - filters 9-7
 - high water mark 9-9
 - idle timeout 9-7
 - IPX network number 9-5
 - location name 9-2
 - maximum ports 9-8
 - maximum transmission unit 9-6
 - netmask 9-5
 - network protocol 9-4
 - TCP header compression 9-6
- Location Table
- configuring 9-2
 - description of 9-1
- location types 9-3
- locations
- defining 11-8, 17-8, 17-11, 18-10
- logging into a host 3-7
- login host
- default 8-8
 - prompt 8-8
 - setting 8-8
 - specified 8-8
 - specifying 6-4
- login message, setting 6-11
- login prompt, setting 6-11
- login security 6-11
- login service
- description of 3-8
 - netdata 3-8, 6-4
 - PortMaster 3-8, 6-3

- rlogin 3-8, 6-3
- setting 6-3, 8-9
- Telnet 6-3
- Telnet login 3-8
- using 14-4
- login users 6-1, 8-2
 - configuring 8-7
 - connection 13-1
 - dialback 8-10

M

- manual dial out connections 9-3
- maximum dial-out ports, setting 9-8
- maximum transmission unit (MTU)
 - setting 6-8, 8-6, 9-6
- metric parameter 4-9
- metric, setting 4-9
- modem
 - adding 6-16
 - attaching 6-14
 - cable pinout 6-13
 - configuring 6-13
 - configuring for login 13-8
 - control 6-17, 7-9
 - control signals 6-14
 - output signals 6-13
 - parameters
 - configuring 6-16
 - port speed 6-17
 - strings 6-14
 - table 6-16
- modem pool 9-7
 - setting 6-8, 7-11
- MP 9-9

- MTU, setting 6-8
- multi-line load-balancing 9-8
 - configuration example 11-13
- Multilink PPP 9-9

N

- name service, setting 4-6
- negotiated addresses 8-5
- negotiating IP addresses 6-9, 7-8
- NetBIOS, setting 5-6
- netdata
 - device service 3-12, 6-6
 - login service 3-8, 6-4
- netmask
 - description of 2-6
 - setting 5-4, 7-9, 8-5, 9-5
- Netmask Table 2-7
 - assigned pools 4-10
 - configuring 4-9
- network
 - addressing 2-1
 - booting 19-12
 - connectivity, example of 1-1
 - device configuration 3-10, 14-2
 - dial in 6-7, 7-7
 - dial out 6-7, 7-8
 - dial-in & out 6-7, 7-8
 - hardwired 6-7, 6-8, 7-7
 - problems 19-1
 - problems, debugging 19-3
 - protocol values 19-5
 - protocol, setting 9-4
 - two way 6-7
 - type parameter 7-7

- user, configuring 8-4
 - user, description of 8-2
- new user 8-4
- NIS, setting 4-6
- normal users 8-2
- NO-SERVICE status 3-6
- NT1 integrated 7-6
- null-modem cable 6-13
- O**
- office router
 - description of 1-4
 - hardware description 1-7
- office-to-office connections 11-1
- on-demand
 - connections 11-1
 - dial out connections 9-3
 - routing 9-3
- operation of PortMaster 3-2
- outbound authentication
 - PAP 9-12
- override parameters 6-6
- P**
- PAP
 - authentication 3-15, 6-7, 7-7
 - packet formats 19-7
- parity, setting 6-17
- PASSWORD status 3-6
- passwords
 - recovering 19-11
 - setting 4-5
- permanent asynchronous connections 3-16
- permanent virtual circuit 7-5, 16-1
- physical circuit, description of 16-1
- ping command 19-1
- PMconsole, description of 1-4
- port
 - definition of 3-4
 - description of 1-4
 - IP address, setting 7-8
 - security, setting 6-12
 - speed
 - description of 16-2
 - setting 6-17, 7-9
 - synchronizing 6-17
 - synchronous ports 16-3
 - status 3-6
- port state, verification of 19-9
- port type 7-7
 - host device 6-5
 - setting 6-3
 - TwoWay 6-6
 - user login 6-3
- PortMaster
 - booting 3-2
 - configuration of 4-2
 - daemon 1-7
 - device service 3-11, 6-5
 - login service 3-8, 6-3
 - operation of 3-2
 - security 3-5
 - software 1-7
- PPP
 - address negotiation 9-5
 - async map 6-10
 - encapsulation, description of 3-13
 - negotiation debug 19-5
 - quick reference 19-5

- setting 8-4
- using for dial-in and out 3-15
- preview of guide xxix
- printer port configuration 14-8
- products, description of 1-1
- PROM booting 19-16
- prompt for host name 6-4
- protocol
 - setting 6-8
 - support 1-3
 - user 8-4
- proxy ARP 2-9
- pseudo-tty connection 3-9, 14-1
- ptrace command 19-8
- PVC 7-5

R

RADIUS

- configuring parameters 13-6
- description of 1-4
- logging 4-7

RARP messages 3-2

recognizing network problems 19-1

recovering a password 19-11

related documentation xxxi

remote host connections 1-13

reset command 19-4

resetting the system 19-4

RFC 1717 9-9

rlogin

- device service 3-11, 6-5
- login service 3-8, 6-3

route

- boundaries 4-11
- destination, setting 4-8

Route Table

- setting 4-8

routing

- asynchronous port 6-10
- configuring 5-3
- enabling 8-6
- services 1-1
- synchronous port 7-10

Routing Information Protocol (RIP) 2-9

RS-232 devices 14-1

RTS/CTS 6-18

S

SAP filter rules 10-12

security

- management of 3-5
- port 6-12

Service Profile Identifier 18-5

services

- routing 1-1
- telecommuting 1-1
- terminal 1-1

shared device

- access 6-5
- connections 1-14

sharing

- devices 3-9, 14-1
- modems 14-1
- printers 14-1
- RS-232 devices 14-1

SLIP

- description of 3-13
- using for dial in and out 3-15

- SNMP monitoring, setting 4-7
- socket interface applications 3-9
- software
 - flow control 6-18
 - PortMaster 1-7
 - version 19-3
- specified addresses 8-5
- specifying the host name 6-4
- speed
 - synchronous port 7-1
- SPID 18-5
- starting interfaces 3-3
- static routes
 - description of 4-8
 - setting 4-8
- status
 - COMMAND 3-6
 - CONNECTING 3-6
 - DISCONNECTING 3-6
 - ESTABLISHED 3-6
 - HOSTNAME 3-6
 - IDLE 3-6
 - INITIALIZING 3-6
 - NO-SERVICE 3-6
 - PASSWORD 3-6
 - USERNAME 3-6
- subinterface configuration 16-10
- subnet mask 2-6
- subnets, setting 5-4, 7-9
- subnetting 2-6
 - routing issues 2-6
- SVC 7-5
- switched 56K
 - connections 7-5, 17-1

- CSU/DSU 17-1
 - routing 1-14
- switched virtual circuit 7-5, 16-1
- synchronous
 - applications 1-14
 - connections 7-1
 - port disabling 19-4
 - port speeds 7-1, 16-3
- synchronous port parameters
 - compression 7-10
 - destination IP address 7-8
 - dial group 7-10
 - enabling routing 7-10
 - extended information 7-7
 - Frame Relay 7-11
 - DLCI list 7-11
 - LMI 7-11
 - input and output filters 7-10
 - IPX network number 7-9
 - modem control 7-9
 - netmask 7-9
 - network type 7-7
 - port
 - speed 7-9
 - port IP address 7-8
 - port type 7-7
 - TCP header compression 7-10
 - transport protocol 7-8
- syslog function 4-6
- system logging, setting 4-6
- system name, setting 4-4
- system reset 19-4

T

- TA 7-6

- TCP header compression 6-10, 7-10
 - setting 8-6, 9-6
- TCP port services 10-8
- technical support xxxii
- telecommuting services 1-1
- TelePath, description of 1-4
- Telnet
 - access to shared devices 14-9
 - administrative session 19-10
 - device service 6-5
 - device services 3-12
 - login service 3-8, 6-3
 - setting for administrative tasks 4-6
- terminal adapter 7-6
- terminal services 1-1
- terminal type, setting 6-4
- testing configurations 9-13
- ticks, setting 4-9
- time before reset 6-12
- traceroute command 19-4
- tracing
 - packets 19-8
 - routes 19-4
- transport protocol, setting 7-8
- troubleshooting
 - Frame Relay 16-9
 - ISDN 18-15
 - leased line connection 15-7
 - network problems 19-1
 - subinterfaces 16-11
 - V.25bis 17-12
- TwoWay
 - description of 3-14
 - operation 6-1, 6-6

- type 20 broadcast packets 5-6

U

- UDP port services 10-8
- user login
 - configuration 3-8
 - setting 6-3
- user login service
 - netdata 8-9
 - PortMaster 8-9
 - rlogin 8-9
 - Telnet 8-9
- user parameters
 - access filter 8-8
 - enabling routing 8-6
 - filters 8-7
 - IP address 8-5
 - IPX network number 8-5
 - login host 8-8
 - login service 8-9
 - maximum transmission unit 8-6
 - netmask 8-5
 - new login user 8-7
 - new user 8-4
 - protocol 8-4
 - TCP header compression 8-6
- User Table
 - configuring 8-3
 - description of 8-1
- user types 8-1
- USERNAME status 3-6
- users
 - defining 11-7, 13-9, 13-10, 17-7, 17-10, 18-9
 - dialback 8-2

- login 8-2
- network 8-2
- normal 8-2
- using
 - PPP 3-15
 - SLIP 3-15
- UUCP applications 14-1

V

- V.25bis
 - chat script 9-12
 - connections 17-1
 - dialing 7-10, 17-1
 - ISDN 17-5
- verifying connectivity 19-1
- version of software 19-3
- virtual circuits 7-4
 - description of 16-1

W

- WAN connections 7-1
- WAN port parameters
 - Frame Relay 16-8
 - ISDN 18-9
 - leased line 15-6
 - switched 56K 17-6
 - V.25bis dialing 17-6

X

- Xon/Xoff 6-18

