Livingston Enterprises, Inc.

ComOS 3.5L Release Note

Introduction

The new Livingston Enterprises ComOS™ 3.5L software release is now available for the PortMaster Office Router. This release is provided at no charge to all Livingston customers.

This release note documents commands and features in ComOS releases 3.5L, 3.4.2L, and 3.4.1L in addition to those described in the *Command Line Administrator's Guide*. All Livingston manuals are available in PostScript and Adobe Acrobat PDF format in **ftp://ftp.livingston.com/pub/le/doc/manuals/**.

Note – You *must* use PMconsole™ 3.5.1 when upgrading to ComOS 3.5L; see "Upgrade Instructions" on page 31 after reading "Memory Requirements" on page 30.

Contents

ComOS 3.5L

New Features

ComOS 3.5L includes the following new features:

- Variable Length Subnet Masks. In previous releases ComOS required the same netmask to be used for all subnets of a network. In release 3.5L, variable length subnet masks (VLSM) are supported. To ease the transition, the command **set user-netmask off** is available; see below for details.
- OSPF. See the OSPF chapter in the *Command Line Administrator's Guide*, which is available in printed form or in PostScript and Adobe Acrobat PDF format in **ftp://ftp.livingston.com/pub/le/doc/manuals/**.
- The add route command supports VLSM.
- The **show routes** command can show specific networks.
- RADIUS™ can now be used to authenticate administrative logins.
- Syslog messages can now be directed to facilities other than **auth**.
- Easier commands for erasing flash memory.
- Support for VLSM in RADIUS Framed-Route.
- RADIUS Accounting entries are retransmitted sooner.
- RADIUS now supports passwords up to 48 characters in length.
- The size of the Assigned Address Pool can be set with the **set pool** command.
- The ARP cache has been increased from 24 to 96 entries.
- Debug statements can now be timestamped.

Variable Length Subnet Masks

ComOS release 3.5L supports Variable Length Subnet Masks. In previous releases ComOS required the same netmask to be used for all subnets of a network. In release 3.5L, variable length subnet masks (VLSM) are supported. To ease the transition, the command **set user-netmask off** treats all netmasks specified in the User Table or RADIUS as though they were 255.255.255.255, the way earlier releases did. The command **set user-netmask on** adds routes based on the specified netmask. The default is off.

In previous ComOS releases, the PortMaster always used 255.255.255.255 for the user's Framed-IP-Netmask, regardless of the value of the attribute. ComOS 3.5L adds support for Variable Length Subnet Masks (VLSM), but by default ignores the Framed-IP-Netmask the same way earlier releases did. To have ComOS 3.5L accept the netmask value, issue the following commands on the PortMaster:

```
set user-netmask on
save all
```

After user-netmask is set on, the PortMaster uses the actual value of the Framed-IP-Netmask to update the routing table when a user logs in. Use caution with this feature, because it affects both routing and Proxy ARP on the PortMaster.

If you want to route to that one host, use the following attribute:

```
Framed-IP-Netmask = 255.255.255.255
```

You should always use netmask 255.255.255.255 when using the PortMaster assigned address pool (or omit the attribute, which defaults to 255.255.255.255).

If you want to route to an entire 24-bit subnet, you use

```
Framed-IP-Netmask = 255.255.255.0
```

"add route" command supports VLSM

Static Routes support VLSM. For example, to add a route to the 192.168.1.32/27 subnet through gateway 192.168.1.1 with metric 2 you would use the command

```
add route 192.168.1.32/27 192.168.1.1 2
```

OSPF

ComOS 3.5L supports the Open Shortest Path First (OSPF) routing protocol.

See the OSPF Chapter in the *Command Line Administrator's Guide,* available in printed form or in PostScript and Adobe Acrobat PDF format in **ftp://ftp.livingston.com/pub/le/doc/manuals/**. Some additional commands were added after that manual went to press and are documented in **ftp://ftp.livingston.com/pub/le/doc/notes/ospf** and in this release note.

Virtual links are not supported, meaning that all PortMasters running OSPF must either be in one area, or have at least one interface in area 0.

When injecting RIP routes into OSPF, ComOS 3.5L includes the RIP gateway as the gateway.

Before configuring OSPF, you must enter the following commands:

```
set ospf enable
save all
reboot
```

reset ospf

The **reset ospf** command resets the OSPF router engine in the PortMaster. You must enter this command after making changes to the PortMaster's OSPF configuration.

OSPF cost, hello-interval, dead-time

OSPF cost, hello-interval, and dead-time can be configured by interface.

Note – The value for cost, hello-interval, and dead-time must be the same for all routers attached to a common network.

- set *Ether0* ospf on cost *Number*

  This command sets the cost of sending a packet on the interface, expressed in the link state metric. *Number* is a number from 1 to 65535. The default value is 1. Example: set ether0 ospf on cost 2

- set *Ether0* ospf on hello-interval *Number*

  This command sets how often the hello packet is transmitted; the interval can be any value from 10 to 120 seconds. The default value of hello-interval is 10 seconds. Example: set ether0 ospf on hello-interval 40

- set *Ether0* ospf on dead-time *Number*

  This command sets the number of seconds the PortMaster will wait after ceasing to receive a neighbor router's hello packets before marking the remote router as down. The range is 40 to 1200 seconds. The default value is 40 seconds. Example: set ether0 ospf on dead-time 60

"show routes" command can show specific networks

The **show routes** command now accepts an optional argument to only display routes that match that argument. For example, **show routes 172.16** only shows routes that contain "172.16".

RADIUS for administrative logins

The PortMaster now supports Service-Type Administrative-User and NAS-Prompt-User.

In previous releases, the !root administrative login granted full control to the PortMaster. While !root remains, ComOS 3.5L adds the ability to authenticate administrative logins with RADIUS to provide two classes of users:

- administrative users with full configuration ability (everything that !root can do)
- read-only administrative users who cannot change the configuration, but can reset ports, reboot, set debug flags, and show status.

Now, rather than requiring everyone in a Network Operations Center (NOC) to know the global administrative passwords to all your PortMasters, you can create individual accounts to track access and limit configuration changes to appropriate personnel, if desired.

In ComOS 3.5L and later, if a RADIUS Access-Accept returns a Service-Type of Administrative-User (6), the PortMaster treats it as a !root login. If a RADIUS Access-Accept returns a Service-Type of NAS-Prompt-User, a restricted administrative login is granted that has permission to use the following commands:

- ifconfig
- ping
- ptrace
- reboot
- reset
- set console
- set debug
- show
- traceroute
- Any other commands that do not affect the configuration

A NAS-Prompt-User does not have access to the following commands: add, delete, erase, save, tftp, or any set commands other than **set debug** and **set console**.

To enable this feature on your RADIUS server:

- If running RADIUS 1.16, modify **/etc/raddb/dictionary** to include the following two lines; then kill and restart radiusd:

```
VALUE User-Service-Type Administrative-User 6
VALUE User-Service-Type NAS-Prompt-User 7
```

- If running RADIUS 2.0, modify **/etc/raddb/dictionary** to add the following line (it already has a definition for Administrative-User); then kill and restart radiusd:

```
VALUE Service-Type NAS-Prompt-User 7
```

Here are two examples (for RADIUS 2.0) of **/etc/raddb/users** file entries to illustrate:

```
!noc        Password = "dontuseth1s"
            Service-Type = NAS-Prompt-User

!pmconfig   Auth-Type = System, Prefix = "!"
            Service-Type = Administrative-User
```

Caution – If you are using your RADIUS server with a combination of Livingston products and other vendors' products, confirm that they either do not use these two Service-Types or that their use is compatible.

Syslog messages can be redirected

In releases prior to ComOS 3.5L, packet filter logging went to the loghost at AUTH facility and NOTICE priority, and all other logging was done to the AUTH facility at INFO priority. In ComOS 3.5L, the facility and priority can be set for each of five types of logged events.

To display the current syslog settings, use the **show syslog** command. The default settings are displayed in this example:

```
Command> show syslog

  Syslog Configuration Settings

      admin-logins: auth.info
      user-logins: auth.info
      packet-filters: auth.notice
      commands: disabled
      termination: disabled
```

To change the syslog settings, use the **set syslog *Logtype Where*** command. *Logtype* is one of the following: admin-logins, user-logins, packet-filters, commands, or termination. *Where* is either the keyword **disabled**, indicating not to send that type of message to syslog, or a facility and priority separated by a period. For example, to log all commands issued on the PortMaster to the LOCAL0 facility at DEBUG priority use the following command:

```
set syslog commands local0.debug
```

The five areas you can set logging for are defined as follows:

Logtype	**Description**
admin-logins	!root and administrative logins
user-logins	Non-administrative logins (You might want to disable this if you already use RADIUS Accounting.)
packet-filters	Packets that match rules with the **log** keyword
commands	Every command entered at the command line interface
termination	More detailed information on how user sessions terminate (See the ComOS 3.3.2 Release Note.)

The facilities and priorities are defined on the following page. Livingston recommends that you use the AUTH facility or LOCAL0 through LOCAL7 facilities for receiving syslog messages from PortMasters, but all the facilities are provided. See your operating system documentation for information on configuring syslog on your host.

Facility	Facility Number	Facility	Facility Number
kern	0	cron	15
user	1	local0	16
mail	2	local1	17
daemon	3	local2	18
auth	4	local3	19
syslog	5	local4	20
lpr	6	local5	21
news	7	local6	22
uucp	8	local7	23

The following priorities are available:

Priority	Priority Number	Typically Used for
emerg	0	system is unusable
alert	1	action must be taken immediately
crit	2	critical messages
err	3	error messages
warning	4	warning messages
notice	5	normal but significant message
info	6	informational message
debug	7	debug-level messages

Flash erasure commands

For more information on these commands see the “General Commands” chapter of the *Command Line Administrator’s Guide*. ComOS 3.5L has a set of commands for erasing all or part of the nonvolatile flash memory of the PortMaster.

Command	Use
erase all-flash	Erases **all** the nonvolatile memory in the PortMaster including the configuration and ComOS.
erase comos	Erases the ComOS that the PortMaster boots from.
erase configuration	Erases the configuration, returning the PortMaster to factory defaults after its next reboot.
erase file *String*	Erase the specified file from configuration nonvolatile memory, see **show files** for a list.
erase partition *Number*	Use this command only if told to do so by Livingston Technical Support.

RADIUS Framed-Route supports VLSM

ComOS release 3.5L supports the subnet length specifier in RADIUS Framed-Route attributes. For example:

```
Framed-Route = “192.168.1.32/28 192.168.1.33 1”
```

RADIUS Accounting retransmits sooner

RADIUS Accounting packets are now retransmitted every 30 seconds. The Authenticator field in a retransmitted Accounting-Request is now calculated using the method specified in the current RADIUS specification.

RADIUS now supports passwords up to 48 characters in length

RADIUS now supports user passwords up to 48 characters in length. The RADIUS 1.16 and RADIUS 2.0 servers support passwords up to 16 characters in length; a future release of the Livingston RADIUS server will support passwords up to 48 characters.

Assigned pool size

The PortMaster allocates a pool of IP addresses starting at the Assigned Address base value (set from the global menu or by the **set assigned** command) and counting up. The total number of addresses is equal to the number of ports configured for Network Dialin. If someone dials in and requests an unused address from the pool, that is assigned; if someone dials in and requests any address, the next address from the pool is assigned, if someone disconnects, their address is placed at the end of the pool for reuse.

In ComOS 3.5L, the size of the pool can also be set explicitly with the **set pool *Number*** command, where *Number* is the number of IP addresses to allocate for the pool. If the pool size is decreased, the PortMaster must be rebooted for the change to take effect.

Increased ARP cache

The Ethernet ARP cache has been increased from 24 entries to 96, to improve performance.

Debug timestamps

The command **set debug clock** on time-stamps console debug messages using the time since last reboot, specified in days, hours, minutes, seconds, and hundredths of a second. To turn the timestamps off use the command **set debug clock off**.

Bug Fixes

The following bugs are fixed in ComOS 3.5L:

- Three small memory leaks are fixed.
- In previous releases, if both B channels on a BRI were active and the BRI was provisioned for **Additional Call Offering** and a voice call came in, a B channel was set to idle. In ComOS 3.5L, the PortMaster properly refuses the call.
- In previous releases, if a synchronous PPP device called in and the PortMaster missed the first PPP packet, after one second the PortMaster sent a V.120 frame to wake up the device. Some devices treated the V.120 frame as an invalid protocol and hung up. In ComOS 3.5L, the PortMaster waits five seconds before sending the V.120 frame, because the PPP specification requires the device to retransmit within three seconds.
- The Omron ME2814BII modem drops CTS for less than 80 microseconds. In a previous release, the PortMaster detected the drop but not the rise 1/12500 second later, causing the PortMaster to flow control the port and hang the session. This behavior has not been detected on any other brand of modem, but ComOS 3.5L now handles it properly.

ComOS 3.4.2L

New Features

ComOS 3.4.2L includes the following new features:

- Support for International ISDN
- Command to show flash file system
- Session Termination Cause logging in RADIUS Accounting
- RADIUS Outbound-User support
- TCP port number for Login User in RADIUS Accounting
- Maximum Receive Unit increased to 1520 bytes
- PAP and CHAP for Dialback PPP users
- Easier configuration of CHAP for dial-out Locations
- ChoiceNet without RADIUS
- Set all command made easier
- Debug off command

Support for International ISDN

Support for International ISDN using the OR-ST has been added. The OR-ST is the PortMaster ISDN Office Router for use in Europe, Japan, and other countries using international ISDN standards. New ISDN switch type settings for **set isdn-switch** are listed in the following table.

set isdn-switch	**Used For**
net3	EuroISDN standard (includes Swiss extensions)
vn2	France - Older switch type
vn3	France - Older switch type
vn4	France - Current National switch type
1tr6	Germany - Older switch type
ntt	Japan
kdd	Japan

A change in switch type does not take effect until the PortMaster is rebooted.

Command to show flash file system

The **show files** command has been added to display how much of the 128 KB flash configuration file system is in use. Output also shows file names. Files are:

File	**Contents**
confdata	Extensions to port configurations, ether1, RADIUS
config	Global configuration and standard port configurations
passwd	User Table
hosttab	Host Table
routes	Static Routes
location	Location Table, except for chat scripts
script	Chat Scripts for the Location Table
snmp	SNMP
filters	IP filters
listnames	ChoiceNet list IDs contained in filters
ipxfilt	IPX filters
sapfilt	SAP filters
netmasks	Static Netmask Table
modem	Modem Table

Session Termination Cause logging in RADIUS Accounting

RADIUS accounting now reports the reason for session termination. In addition, the new **set debug termination on** command displays more detailed port terminations to the system console as well as sending these messages to syslog. See "RADIUS Accounting Terminate Cause" on page 14 for more information on termination causes and how to edit the RADIUS dictionary file to take advantage of them.

RADIUS Outbound-User support

The PortMaster now supports the RADIUS Outbound-User service-type. In addition, the PortMaster logs outbound user activity to RADIUS accounting. See "RADIUS for Outbound Users" on page 13 for information on using this feature.

Note – If you are currently using outbound Telnet security with RADIUS you must change those entries in your RADIUS users file to use Service-Type = Outbound-User when you upgrade to ComOS release 3.4.2L.

TCP port number for Login User in RADIUS Accounting

The Telnet and Netdata TCP port number is now identified in RADIUS accounting. Previously, Login Users sent to a host with Telnet would be identified only as using the Telnet service even if they were directed by RADIUS to a TCP port number other than 23. In ComOS release 3.3.2, if the user is sent to a port other than 23 RADIUS accounting reports the TCP port number. This is useful for determining whether the user was sent to a special service on the identified host. Accounting records for Login Users using the Netdata (TCP-Clear) login service now always include the TCP port number.

Maximum Receive Unit increased to 1520 bytes

LCP now allows the remote end to request (via a NAK) a maximum receive unit of up to 1520 bytes instead of the previous limit of 1500. This accommodates some Multilink PPP implementations which use a MRU larger than 1500 bytes.

PAP and CHAP for Dialback PPP users

PAP and CHAP authentication support has been added for Dialback PPP users.

Easier configuration of CHAP for dial-out Locations

The new command **set location Location_Name chap [on|off]** has been added to make outbound CHAP authentication easier to configure. When **chap on** is set for the location, the PortMaster requires that it be authenticated using CHAP on an outbound dial. The username and password entered in the location table are used as the **system identifier** and **MD5 secret** in the CHAP authentication. Use of this feature eliminates the need to use the sysname and user table configurations for CHAP unless the device being dialed to also sometimes dials into the PortMaster. The default setting is **chap off**.

ChoiceNet without RADIUS

ChoiceNet can now be used without RADIUS using the following commands:

```
set choicenet  Ipaddress
set choicenet-secret String
```

Set All command made easier

The **set all** command no longer affects the W1 port, the P0 parallel port or the new C0 (PM-2I and PM-2E-10I only) console port. Now it affects only ports S0-29.

The command **set all network dialin** is now supported.

Debug off command

The command **set debug off** has been added. This command clears all debug settings which are currently active in the PortMaster.

Bug Fixes

The following bugs have been fixed in ComOS 3.4.2L.

Zero Length Filters are now ignored

Zero length filters applied to Ethernet interfaces are now treated as permit filters. That is, if a filter has no rules at all it now permits everything through. If it has one or more rules then anything not explicitly permitted by a rule is denied at the end of the filter.

Ports using ChoiceNet can be reset safely

Previously, resetting or disconnecting a port which is waiting for ChoiceNet to upload a dynamic packet filter would cause the PortMaster to reboot. This has been fixed; ports can now be reset without causing a problem.

State Attribute cleared properly

Previously the RADIUS State attribute could be inadvertently retained between login sessions, displaying the wrong RADIUS menu when users logged on. This has been fixed. (RADIUS menus are supported in the RADIUS 2.0 server, to be released later.)

Too-long Filter-Id Attributes now truncate

Previously, a RADIUS Filter-Id attribute longer than 12 characters for PPP users would cause the PortMaster to reboot. This has been fixed. A Filter-Id longer than 12 characters is now truncated to 12 characters before appending the **.in** and **.out** to the filter name.

Host Prompt now works over ISDN

Previously an ISDN port set for host prompt would not echo characters back to the user. This has been fixed.

Location username now deletes properly

Previously, adding a username to a location, deleting the location, and adding the location again would bring back the username entry. The username is now properly deleted when the location is deleted.

Extraneous console message removed

If a user dials in and negotiates IPX while the console is set, the console gets a burst of "e_getpacket: no packet available" messages at the end of negotiations. These are harmless, but have been removed.

Commands fixed

The usage statement for ptrace has been fixed.

Previously, only the command **save host** would save the PortMaster Hosts Table. The plural form **save hosts** is now supported as well.

Additional Notes

RADIUS for Outbound Users

RADIUS on the PortMaster now supports Service-Type = Outbound-User, used to authenticate users gaining outbound access to network device ports.

If you do not have any ports set to **device /dev/network** or **twoway /dev/network** you can ignore this entire section, it does not apply to you. If you do have any ports set to **device /dev/network** or **twoway /dev/network** and have been using RADIUS to authenticate outbound users, you should read this section carefully and understand it completely before upgrading to this release, because things will work differently after the upgrade.

In ComOS release 3.4.1L and earlier, to allow users to access the modems for outbound dialing across your network but require a password for such access, you set the port up like this (after first moving your telnet administration port to something other than 23 with a command like **set telnet 24**):

```
set s1 device /dev/network
set s1 service_device telnet 10000
save s1
reset s1
```

And then set up a user like this in the PortMaster User Table:

```
add user fred
set user fred password What4ever
set user fred service telnet 10000
set user fred host <PortMaster ether0 IP address>
save user
```

A user can then telnet to the PortMaster at the usual telnet port of 23, get a login prompt, enter **fred**, get a password prompt, enter **What4ever**, and would be connected to the device connected to port s1, typically a modem. You can pool multiple ports together by setting their service device telnet port to the same number. Any port number between 10000 and 10100 has this special property.

In ComOS 3.4.2L and later, this behavior has changed. In 3.4.2L, you set up the port the same way as before, but now when the user telnets to port 23 and gives his username and password, the PortMaster first checks the local User Table, as it did before. If the user is not found in the local User Table and the PortMaster is configured to use a RADIUS server, the PortMaster sends a RADIUS Access-Request to the RADIUS server with the hint that Service-Type (6) = Outbound-User (5).

If the PortMaster receives back an Access-Accept from the RADIUS server with Service-Type = Outbound-User, it allows the user to connect to the port. Check your /etc/raddb/dictionary file for the exact spelling of attribute 6 and value 5.

An example entry in the /etc/raddb/users file for an Outbound-User follows:

```
fred    Password = "What4ever", Service-Type = Outbound-User
        Service-Type = Outbound-User,
        Login-Service = Telnet,
        Login-TCP-Port = 10000
```

Note that the user file can only have one entry named **fred**. If fred is already used in the RADIUS users file as a different kind of user, you must use a different username to dial out with. RADIUS 2.0 will make this easier.

RADIUS Accounting Terminate Cause

Release 3.4.2L has added support for the RADIUS Accounting Acct-Terminate-Cause attribute to provide information on the cause of session termination. In addition, if termination debugging is turned on using the **set debug termination on** command, additional termination information is sent to syslog (auth.info) and the system console.

Before upgrading the PortMaster, update your **/etc/raddb/dictionary** file by adding the following lines, kill your **radiusd** and restart it. An updated dictionary file is available at **ftp://ftp.livingston.com/pub/le/radius/dictionary**.

```
ATTRIBUTE     Acct-Terminate-Cause        49                      integer

VALUE         Acct-Terminate-Cause        User-Request            1
VALUE         Acct-Terminate-Cause        Lost-Carrier            2
VALUE         Acct-Terminate-Cause        Lost-Service            3
VALUE         Acct-Terminate-Cause        Idle-Timeout            4
VALUE         Acct-Terminate-Cause        Session-Timeout         5
VALUE         Acct-Terminate-Cause        Admin-Reset             6
VALUE         Acct-Terminate-Cause        Admin-Reboot            7
VALUE         Acct-Terminate-Cause        Port-Error              8
VALUE         Acct-Terminate-Cause        NAS-Error               9
VALUE         Acct-Terminate-Cause        NAS-Request             10
VALUE         Acct-Terminate-Cause        NAS-Reboot              11
VALUE         Acct-Terminate-Cause        Port-Unneeded           12
VALUE         Acct-Terminate-Cause        Port-Preempted          13
VALUE         Acct-Terminate-Cause        Port-Suspended          14
VALUE         Acct-Terminate-Cause        Service-Unavailable     15
VALUE         Acct-Terminate-Cause        Callback                16
VALUE         Acct-Terminate-Cause        User-Error              17
VALUE         Acct-Terminate-Cause        Host-Request            18
```

The following simple script produces a list of termination causes seen. Note that this script does not remove duplicates, so it provides only an approximate count.

```
cat /var/adm/radacct/*/detail | grep Acct-Terminate-Cause | \
sort | uniq -c
```

The syslog messages and their meanings are displayed on the following page. Where a message would also go to RADIUS Accounting, the Acct-Terminate-Cause is included in the syslog message before the dash. In normal operation you would expect to see User-Request, Host-Request, and Lost-Carrier, although Lost-Carrier can be caused by the user hanging up his end of the connection or by line or modem problems.

Syslog Message	Meaning
Admin-Reset	Port was reset by administrator. Also sent to RADIUS Accounting if a session was active on the port.
Callback	Callback User is disconnected so the port can be used to call user back.
Cause Unknown	Contact Livingston Technical Support.
Host Request - PMD	Disconnected or logged out from host using in.pmd service. This can mean either normal termination of a login session, or the remote host has crashed or become unreachable. Also sent to RADIUS Accounting.
Host Request	Disconnected or logged out from host. This can mean either normal termination of a login session, or the remote host has crashed or become unreachable. Also sent to RADIUS Accounting.
Idle Timeout	Idle timer expired for user or port. Also sent to RADIUS Accounting.
Login Timeout	The login:, password:, or host: prompt is set to timeout after five minutes with no input and has done so.
Lost Carrier	Session terminated when modem dropped DCD. This can either mean the user or his modem hung up the phone from their end, in which case there is no problem, or can mean that the line was dropped or took a noise hit too severe for the modems to recover from, or can mean that the local modem dropped DCD for some other reason. Also sent to RADIUS Accounting.
Lost Service - Interface Down	Contact Livingston Technical Support.
Lost Service - Interface Error	Contact Livingston Technical Support.
Lost Service - LMI	A Frame Relay interface missed six consecutive LMI replies.
Lost Service - No netbufs	No netbufs are available for service. Contact Livingston Technical Support.
NAS Error - PPP Unknown State	The PortMaster could not determine state of PPP. Contact Livingston Technical Support.
NAS Request - Modem Config Complete	The Modem table entry has finished initializing the modem attached to the port.
NAS Request - PPP Maximum Retransmissions	PPP negotiations failed after the PortMaster sent 10 configuration requests. This is caused by a configuration error on the client, PortMaster, or RADIUS user entry.

<table>
<tr><th>Syslog Message</th><th>Meaning</th></tr>
<tr><td>No Event Identified</td><td>Contact Livingston Technical Support.</td></tr>
<tr><td>Port Error - PPP Couldn’t Send</td><td>The PortMaster could not send PPP negotiation. Check that the port and modems at both ends are properly configured for hardware flow control (RTS/CTS); if the problem still occurs, contact Livingston Technical Support.</td></tr>
<tr><td>Port Error - PPP Loop Detect</td><td>The PortMaster saw its own Magic Number in an LCP Configuration Request. The two most likely causes are either that our modem is in echo mode or that we dialed into a UNIX system and it is echoing our packets back to us. In the former case, correct the configuration in the modem. In the latter case, change the chat script in the location table entry on the PortMaster to expect “ ~ ” instead of PPP .</td></tr>
<tr><td>Port Error - Spurious Interrupts</td><td>Attached device is causing too many interrupts, so the PortMaster reset the port. Also sent to RADIUS Accounting if a session was active on the port.</td></tr>
<tr><td>Port Error - Unknown State</td><td>Contact Livingston Technical Support.</td></tr>
<tr><td>Port Error - Wrong Type</td><td>Port is configured for login users only and a network user is trying to log in, or vice versa. To configure ports appropriately, use one of the following:

set all login — Login users only
set all network dialin — Network users only
set all network login dialin — Login and network users</td></tr>
<tr><td>Service Unavailable - Access Denied</td><td>The port Access Filter does not permit connection to requested host. If you get this message and you wish to allow a connection to the host:
• If you did not intend to use an access filter, remove the ifilter from the port with set Port ifilter
• If you are using an access filter, check your filter rules.</td></tr>
<tr><td>Service Unavailable - Auth Failed</td><td>Three attempts by the user to authenticate at the login: prompt have failed, so the user is disconnected.</td></tr>
<tr><td>Service Unavailable - Device</td><td>Port is set for host device but in.pmd or the pseudo-tty configured is unavailable. This gets logged once per second until the situation is corrected.</td></tr>
<tr><td>Service Unavailable - Host</td><td>Login session was unable to connect to host. The most common cause is that the host is down or refusing connections or not running in.pmd or rlogind.</td></tr>
<tr><td>Service Unavailable - PPP Auth Failed</td><td>Contact Livingston Technical Support.</td></tr>
</table>

Syslog Message	Meaning
Service Unavailable - PPP CHAP Auth Failed	The user's PPP CHAP authentication failed.
Service Unavailable - PPP No Protocol	Neither IP nor IPX was negotiated for PPP, so no service can be provided. This is a configuration error for either the dial-in client or the user entry.
Service Unavailable - PPP Outbound PAP Auth Failed	PortMaster dialed out to another site and was being authenticated by PAP but failed, so the PortMaster is hanging up. (Note that if we are authenticated by CHAP and fail, it is the responsibility of the other end to hang up.)
Service Unavailable - PPP PAP Auth Failed	The user's PPP PAP authentication failed.
Session Timeout	Session timer expired for user. Also sent to RADIUS Accounting.
User Error - PPP LCP Protocol Reject	The PortMaster received a LCP Protocol Reject. This should never happen; it indicates there is a bug in the software of the remote system since the remote system is claiming it does not support LCP.
User Error - PPP NCP Active to Reply	PortMaster received a PPP Configuration ACK when a session was already established, so it terminated the session. This is caused by a PPP implementation error in the dial-in client. Also sent to RADIUS Accounting.
User Error - PPP NCP Active to Request	PortMaster received a PPP Configuration Request when a session was already established, so it terminated the session. This is caused by a PPP implementation error in the dial-in client. Also sent to RADIUS Accounting.
User Request - Admin Quit	Quit command issued from the command line interface.
User Request - PPP Term Ack	Dial-in client requested that we terminate immediately without sending an acknowledgment. This message is expected from a proper PPP client termination. Also sent to RADIUS Accounting.
User Request - PPP Term Req	Dial-in client requested that we send a Termination ACK and then terminate. This message is expected from a proper PPP client termination. Also sent to RADIUS Accounting.

ComOS 3.4.1L

ComOS 3.4.1L adds support for the W1 synchronous port on the PortMaster Synchronous 384K Office Router (OR-LS) and PortMaster Synchronous T1/E1 Office Router (OR-HS) and includes all the features of 3.4L.

If the external clock rate on W1 exceeds 384Kbps the OR-LS displays the message "W1: External clock exceeds maximum rate" to the console.

ComOS 3.4L

New Features

ComOS 3.4L includes the following new features:

- ISDN Basic Rate Interface (BRI) support (on OR-U)
- Multilink PPP on ISDN (on OR-U)
- Multilink V.120 on ISDN (on OR-U)
- Data over voice for both inbound and outbound ISDN connections (on OR-U)
- AT strings for more user control for outbound ISDN dialing (on OR-U)
- Dynamic loadable software modules for memory management
- Console now ignores modem type and autolog
- !root login on serial ports can be disabled
- Non-printing characters allowed in passwords
- Require PAP option
- Per user port limit (for Multilink PPP and Multilink V.120)
- Per user idle timeouts
- Per user session time limits
- IP numbered interfaces through User Table
- BOOTP support
- RFC 1877 support so clients can learn DNS server from PortMaster
- Port Type included in RADIUS Authorization and Accounting
- RADIUS Accounting records signed
- Called-Station-Id and Calling-Station-Id RADIUS accounting
- RADIUS accounting sends notification of PortMaster boot
- Input and output octet counters in RADIUS Accounting
- Location Table entries made simpler and easier
- Outbound PAP authentication

ISDN Basic Rate Interface (BRI) support

ISDN basic rate interface support has been added. This release added full support for the ISDN BRI interface on the OR-U. See “ISDN Basic Rate Interface (BRI) support” on page 24 for specific information about ISDN support on the OR-U.

Multilink PPP on ISDN

Multilink PPP (MP) is now supported on ISDN interfaces. This is supported concurrently with the Livingston Multi-line Load Balancing. The PortMaster automatically detects and accepts both Multi-line Load Balancing and Multilink PPP connections. Outbound, the PortMaster can be set to use Multilink PPP via the Location Table by using the **set location Location_Name multilink on** command.

Compatibility with Ascend’s version of Multilink PPP has been added.

Multilink V.120 on ISDN

Implemented Multilink V.120 on ISDN interfaces. This allows the Livingston PowerLink128 ISDN Modem to make 128Kbps connections to the PortMaster. Second connections generate PowerLink128 RADIUS Accounting records.

Data over voice for both inbound and outbound ISDN connections

Data over voice is now supported for both inbound and outbound ISDN connections. The PortMaster automatically accepts voice calls inbound and treats them as data calls. Outbound, setting the voice attribute in the location table with **set Location_Name voice on** forces a voice call. In outbound asynchronous mode, the AT&N55 command forces a voice call.

AT strings for more user control for outbound ISDN dialing

In asynchronous ISDN mode new AT strings have been added to allow more user control when performing outbound dialing. Specifically the new strings are:

&N55	Perform an outbound call using data over Voice (a Voice call is originated).
&N56	Perform an outbound call using a 56000 data connection.
&N64	Perform an outbound call using a 64000 data connection.
&N0	Attempt to autodetect the available data service (64000 or 56000)

Dynamic loadable software modules for memory management

Memory management has been improved and Dynamic Load modules have been implemented. Device drivers now only load if the specific device is present in the PortMaster (i.e. sync port or ISDN). In addition if SNMP or IPX are not needed they can be disabled to save memory. The commands **set ipx off** and **set snmp off** cause the modules to not load. Any device drivers or subsystems not needed provide additional operational memory for the PortMaster. See the memory guidelines below for PortMaster memory requirements.

IMPORTANT - to use IPX, you must now use the **set ipx on** command. If you are upgrading from a previous release and had IPX configured, it defaults to **on** in this release. When turning IPX or SNMP off, you must do a **save all** and reboot the PortMaster before the change takes effect.

Console now ignores modem type and autolog

When the console diagnostic switch is up, the PortMaster no longer attempts to configure the modem specified for the console port. This allows a terminal to be more easily attached to the console for debugging purposes when a modem was previously attached. Any autolog setting on S0 is now ignored if the console diagnostic switch is up.

!root login on serial ports can be disabled

The command **set serial-admin off** disables !root logins on the serial ports. !root can still login on port S0 if the console dip switch is up.

Non-printing characters allowed in passwords

Support has been added to allow the entry of non-printing characters in the login password field.

Require PAP option

The support for Challenge Handshake Authentication Protocol (CHAP) can now be disabled. Administrators who do not wish to support inbound CHAP authentication can now use the command **set chap off** to disable it. If CHAP is disabled, the only authentication supported is PAP or simple username/password login. It is recommended that this form of authentication use more advanced security subsystems like one-time password smart cards.

Per user port limit for Multilink PPP and Multilink V.120

Implemented Port Limits on a per user basis, only for Multilink V.120 and Multilink PPP users. If left unconfigured, port limits are not imposed, and Multilink V.120 and Multilink PPP sessions are allowed. If a port limit is set, the user is limited to that number of ports on the PortMaster for Multilink V.120 and Multilink PPP only. The command to do so is **set user *Username* maxports *Number***. This can be specified as part of the new RADIUS Port-Limit attribute.

Per user idle timeouts

Implemented idle timeouts on a per user basis. Idle timeouts can be set in the User Table or can be provided as part of the new RADIUS Idle-Timeout attribute. To set them in the User Table use the **set user *Username* idle *Minutes*** command.

Per user session time limits

Implemented session limits from the User Table or RADIUS. If RADIUS returns a session time limit using the new Session-Timeout attribute, the user is automatically disconnected when the time limit is exceeded. To set a session limit in the User Table use the **set user *Username* session-limit *Minutes*** command.

IP numbered interfaces through the User Table

Implemented IP numbered interfaces for network users through the User Table. By using the **set user *Username* local-ip-address *IPaddress*** command, the PortMaster uses the local-ip-address as its IP address to the serial interface. This function is not available in RADIUS.

BOOTP support

BOOTP Support has been added. Clients dialing into the PortMaster can now make BOOTP requests to determine IP address, Subnet Mask, Default Gateway, DNS server, and Domain Name. The PortMaster only responds to BOOTP requests on its serial or ISDN lines.

RFC 1877 support added so clients can learn their DNS server from PortMaster

Support for RFC 1877 has been added. This allows hosts which support RFC 1877 to learn their DNS (and other servers) through the PPP protocol negotiation. Use the **set nameserver Ipaddress** command on the PortMaster to set the nameserver that the PortMaster tells the host about. You can set an alternate name server with **set nameserver 2 Ipaddress**.

Port Type included in RADIUS Authorization and Accounting

RADIUS accounting and authorization has been extended. The new NAS-Port-Type is now included in Access Requests and Accounting Requests. This allows administrators to know definitively whether a user is attempting a session on an asynchronous port, an ISDN port, or a synchronous port.

RADIUS Accounting records signed

RADIUS accounting has been extended to deliver signed accounting records for verification of authenticity as per the current RADIUS Internet-Draft.

Called-Station-Id and Calling-Station-Id for RADIUS accounting

RADIUS Accounting has been extended to provide Called-Station-Id and Calling-Station-Id on ISDN dial-up connections (where provided by the ISDN carrier). These attributes can be used to differentiate ISDN calls from analog calls and to track origination of ISDN calls.

RADIUS accounting sends notification of PortMaster boot

The PortMaster logs a Start record with no Username to the RADIUS accounting server at boot time.

Input and output octet counters in RADIUS Accounting

RADIUS accounting has been extended to include input and output bytes counts in the RADIUS Stop records.

Outbound PAP authentication

Outbound PAP authentication is now supported. The PortMaster previously required the remote end to authenticate with CHAP. Now, by specifying a PAP username and Password in the Location Table dial script, the PortMaster can be authenticated by the remote end using PAP. This is done by setting the Send String in the last line of the dial script to contain the PAP information. The command is:

```
set location Location_Name script Number "=PAP=User/Password"
```

Location Table entries made simpler and easier

New location table entries now default to PPP and its associated configuration parameters to simplify data entry for the most common types of dial locations.

Automatic location table scripting has been implemented. Instead of requiring the administrator to enter a V.25bis or AT style send/expect dial script, they can simply enter the telephone number, user name, and password to use when dialing to a remote location.

The following commands have been added to support this:

```
set location Location_Name telephone 8005551212
set location Location_Name username PPP_PAP_username
set location Location_Name password PPP_PAP_password
```

Bug Fixes

The following bugs have been fixed in ComOS 3.4L.

- The PortMaster no longer loses track of IP addresses it provided as assigned address from the pool. This bug caused the PortMaster to start giving out address 0.0.0.0 to dial-in hosts because it is out of addresses.
- Users which have initiated a PPP connection using PPP autodetect and get authenticated and authorized as a SLIP user are now properly handled. Service is denied and the PortMaster cleans up the session. Previously a variety of symptoms would be experienced causing an incorrect active configuration.
- The correct active user is retained for ports configured for host prompt.
- Serial port spurious interrupt handling has been extended to include detecting streams of framing errors. Some modems get confused about their configuration and begin sending continuous data to the PortMaster at a baud rate different than set on the PortMaster. This would cause all operation on the PortMaster to appear stopped for several minutes to several hours. The PortMaster now attempts to reset the modem and continues to operate properly even if the modem does not recover.

Additional Notes

ISDN Basic Rate Interface (BRI) support

ComOS 3.4L adds support for Livingston's new PortMaster ISDN Office Router (OR-U).

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 signaling. Multiple lines can be used to increase bandwidth, either using Multilink PPP, as defined by 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. 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. Asynchronous or synchronous usage is autodetected. 56K or 64K speeds are also autodetected. Hayes AT commands have been added to allow a user to telnet to a 64K B-channel and use the ISDN port as a dial-out modem. The ISDN ports support synchronous PPP and asynchronous V.120 PPP or SLIP.

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.

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.

The following commands have been added to configure ISDN:

```
set isdn-switch ni-1|dms-100|5ess|5ess-ptp
set Port spid Number
set Port directory Number
```

See "Configuring ISDN" on page 25 for more information on the ISDN commands.

Hayes AT commands can be used for ISDN dial-out modems.

Any 64K ISDN B-channel port can be used as a dial-out ISDN modem. A user can telnet to a ISDN port and then execute a Hayes AT dialing command to connect to a remote ISDN PortMaster, PortMaster ISDN Office Router, or external ISDN modem.

The PortMaster responds to any **AT** command which is not specifically a dial command with an **OK**. That way, attempts to set S registers, flow control, or other things needed by analog modems are accepted by the PortMaster but ignored. This allows existing configured dialer software to be used with the PortMaster ISDN port without any changes.

The **AT&N56** command sets the port for 56K operation for this dialout, and the **AT&N64** command sets the port for 64K. The **AT&N0** command attempts to autodetect the available data service, either 56000 or 64000. The **AT&N55** command performs an outbound call using data over voice.

A dial command can be ATDT, ATD or ATDP followed by the phone number. Phone numbers can have dashes " **-** ", commas " **,** " or digits in them, ending with a carriage return. Since ISDN does not require pauses in dialing, commas in the phone number are accepted but ignored.

Configuring ISDN

Only three additional things need to be configured on the PortMaster to permit ISDN service. They are: the ISDN Switch type, a Service Profile Identifier (SPID) for each ISDN port, and a directory number(DN) for each ISDN port. All three can be configured from the command line interface. To display ISDN debug information on the console, use the following commands:

```
show isdn
set console
set debug isdn on
```

To turn off debugging use the following commands:

```
set debug isdn off
reset console
```

ISDN Switch Type

The ISDN Switch Type can be set to one of four values. Your telephone company can tell you which type its switch is: National ISDN-1 (NI-1), Northern Telecom DMS-100 Custom, AT&T 5ESS Custom Multi-Point, or AT&T 5ESS Custom Point-to-Point. If they have a DMS-100 or 5ESS switch that uses National ISDN-1, treat that as NI-1.
Use one of the following commands to set the switch type. The default is NI-1. If you change the switch type after setting a SPID on a port, you must reboot the PortMaster for the change to take effect.

```
set isdn-switch ni-1
set isdn-switch dms-100
set isdn-switch 5ess
set isdn-switch 5ess-ptp
```

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 can provide you with the SPIDs for each line. If the spid is invalid, **set debug isdn on** can reveal that. An example command is:

```
set s10 spid 1510555121200
```

Directory Number

If you set the Directory Number, then an incoming call must match this number to determine which port the call is taken on. It is a 10-digit phone number provided by the telephone company. Either of the following commands are accepted:

```
set s10 dn 5105551111
set s10 directory 5105551111
```

Other port configuration

ISDN ports are simpler to configure than asynchronous ports. You never set modem control (carrier detect), flow control or speed on an ISDN port. The PortMaster senses the speed and sets the port to 64000 or 56000 accordingly, flow control isn't needed on a synchronous line since clock is provided by the telephone company, and carrier detect is always used. Refer to the *Office Router Hardware Installation Guide* for information on ISDN LED activity.

The ports support both sync and async PPP (V.120). The **show *port*** command displays 64000/async if async PPP is in use. The port can be configured for anything an async port can be configured for, 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, but PAP is also available.

Here is a table for what **show *port*** displays according to 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 Telephone Company
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

New RADIUS Attributes

To use the new RADIUS attributes with RADIUS 1.16, upgrade your PortMaster to ComOS 3.4L or later, add the following lines to your **/etc/raddb/dictionary** file, kill your **radiusd** daemon and restart it.

```
ATTRIBUTE       Session-Timeout         27              integer
ATTRIBUTE       Idle-Timeout            28              integer
ATTRIBUTE       Called-Station-Id       30              string
ATTRIBUTE       Calling-Station-Id      31              string
ATTRIBUTE       Acct-Input-Octets       42              integer
ATTRIBUTE       Acct-Output-Octets      43              integer
ATTRIBUTE       NAS-Port-Type           61              integer
ATTRIBUTE       Port-Limit              62              integer
VALUE           NAS-Port-Type           Async           0
VALUE           NAS-Port-Type           Sync            1
VALUE           NAS-Port-Type           ISDN            2
VALUE           NAS-Port-Type           ISDN-V120       3
VALUE           NAS-Port-Type           ISDN-V110       4
```

Idle-Timeout is expressed in seconds but is rounded to a minute boundary, and can be any value from 120 (2 minutes) to 14400 (4 hours). Session-Timeout is expressed in seconds but is rounded to a minute, and can be up to a year long. Note that Port-Limit only works with certain types of users; see the New Features section above for restrictions.

Here is an example /etc/raddb/users entry for a network user that is authenticated using a login script or PAP using her password from the UNIX /etc/passwd file, and uses PPP with an address assigned from the PortMaster's dynamic address assignment pool. She is only allowed to connect once concurrently per PortMaster. After 10 minutes (600 seconds) of idle time without any traffic she is disconnected. After 2 hours (7200 seconds) elapsed time she is disconnected regardless of what she's doing.

```
#
# Example PPP user, address Assigned by PortMaster
#
pam         Password = "UNIX"
            User-Service-Type = Framed-User,
            Framed-Protocol = PPP,
            Framed-Address = 255.255.255.254,
            Framed-MTU = 1500,
            Idle-Timeout = 600,
            Session-Timeout = 7200,
            Port-Limit = 1
```

Quick Setup Example for OR-U

This is a quick reference on how to configure your OR-U to dial out on demand to another site using ISDN. You can abbreviate the commands to uniqueness. Fill in the blanks with your information. The filter shown is just an example, see the "Configuring Filters" chapter of the *Configuration Guide for PortMaster Products* or Chapman & Zwicky's *Building Internet Firewalls* for more detailed information on using packet filters.

```
set gateway _____ (IP address of router at other end)
set isdn-switch ni-1 (or dms-100 or 5ess or 5ess-ptp)
set ether0 address _____ (your IP address)
set ether0 netmask 255.255.255.0 (or whatever you are using)

set s1 spid _____
set s1 directory _____
set s1 group 2
set s2 spid _____
set s2 directory _____
set s2 group 2

add filter isp.in
set filter isp.in 1 deny _____/24 0.0.0.0/0 (your network number)
set fil isp.in 2 permit tcp estab
set fil isp.in 3 permit 0.0.0.0/0 _____/32 tcp dst eq 80 (WWW host)
set fil isp.in 4 permit 0.0.0.0/0 _____/32 tcp dst eq 119 (News server)
set fil isp.in 5 permit 0.0.0.0/0 _____/32 tcp dst eq 25 (mail server)
set fil isp.in 6 permit 0.0.0.0/0 _____/32 tcp dst eq 21 (FTP server)
set fil isp.in 7 permit 0.0.0.0/0 _____/32 udp dst eq 53 (DNS server)
set fil isp.in 8 permit 0.0.0.0/0 _____/32 tcp dst eq 53 (DNS server)
set fil isp.in 9 permit tcp src eq 20 dst gt 1023
set fil isp.in 10 permit icmp

add filter isp.out
set filter isp.out 1 deny 0.0.0.0/0 _____/24 (your network number)
set fil isp.out 2 permit tcp estab
set fil isp.out 3 permit tcp dst eq 80
set fil isp.out 4 permit tcp dst eq 119
set fil isp.out 5 permit tcp dst eq 25
set fil isp.out 6 permit tcp dst eq 21
set fil isp.out 7 permit tcp src eq 20 dst gt 1023
set fil isp.out 8 permit udp src eq 53
set fil isp.out 9 permit udp dst eq 53
set fil isp.out 10 permit udp dst eq 520
set fil isp.out 11 permit icmp

add location isp
set location isp on_demand
set location isp destination _____ (same address as gateway)
set location isp netmask 255.255.255.0
```

(Continued on next page)

```
set location isp idletime 2 (2 to 240 minutes, do NOT use 1)
set location isp group 2
set location isp username _____ (your username on isp)
set location isp password _____ (your password on isp)
set location isp telephone _____ (ISDN phone# of isp)
set location isp ifilter isp.in
set location isp ofilter isp.out
set location isp maxports 2

save all
reset s1
reset s2
```

On isp you must add a netuser to the User Table or RADIUS using the above username and password, protocol PPP, TCP header compression on, address either negotiated or set the same as the ether0 address above.

Quick Setup Example for OR-LS or OR-HS

This is a quick reference on how to configure your OR-LS (or OR-HS) to connect to another site using PPP over a synchronous leased line. You can abbreviate the commands to uniqueness. Fill in the blanks with your information. Use the same filters **isp.in** and **isp.out** as described in the previous setup example. If you are connecting using Frame Relay instead of PPP, see "Synchronous Frame Relay Connections" in the *Configuration Guide for PortMaster Products*. The W1 synchronous port always requires external clock from either the telephone company or the CSU/DSU.

```
set gateway _____ (IP address of router at other end)
set ether0 address _____ (your IP address)
set ether0 netmask 255.255.255.0 (or whatever you are using)

set w1 network hardwire
set w1 protocol ppp
set w1 routing broadcast (unless instructed otherwise by ISP)
set w1 destination _____ 255.255.255.0 (same as gateway)
set w1 mtu 1500
set w1 ifilter isp.in
set w1 ofilter isp.out

save all
reset w1
```

Memory Requirements

The following section discusses memory requirements for ComOS 3.5L in general terms; actual memory usage depends on the configuration and use of your PortMaster. For instructions on upgrading memory see the installation guide for the product. All installation guides are available on the PortMaster Software CD, in PDF format on the Livingston web site www.livingston.com, and in PDF and PostScript format on the Livingston FTP site ftp.livingston.com.

All models of the PortMaster Office Router have 1MB of nonupgradeable memory, which is sufficient for ComOS 3.5L.

All models of the PortMaster IRX have 1MB of memory, which is sufficient for ComOS 3.5R unless you are using OSPF with very large networks.

For the PortMaster 2 and PortMaster 25 use the following guidelines to estimate memory usage.

Model	Async	Sync	ISDN	Base Memory
PM-25	25	0	0	780KB
PM-2E-30	30	0	0	800KB
PM-2E-10 + 1 ISDN	10	0	10	860KB
PM-2E-10 + 2 ISDN	10	0	20	910KB
PM-2E-20 + 1 ISDN	20	0	10	935KB
PM-2ER-10 + 1 ISDN	10	1	10	885KB
PM-2ER-10 + 2 ISDN	10	1	20	935KB
PM-2ER-20 + 1 ISDN	20	1	10	960KB

- If SNMP is used, an additional 50KB is required.
- If IPX is used, an additional 20KB is required, plus memory for SAP and RIP.
- If RIP is used, 5KB for every 100 RIP routes should be added.
- If OSPF is used, an additional 50KB is required, plus 5KB for every 40 routes.
- If any other tables are used, such as the User Table or Location Table, those require additional memory.

The PortMaster auto-detects the physical installed memory. Four 30-pin 70ns parity SIMMs are required, either 256KB, 1MB, or 4MB. Mixing of SIMMs is not supported. They can be either 3-chip or 9-chip SIMMs.

Upgrade Instructions

YOU MUST USE PMINSTALL VERSION 3.5.1 OR LATER TO PERFORM THIS UPGRADE! If you are upgrading using PMconsole™ for Windows, you must use PMconsole for Windows version 3.5.1.1 or later.

If you have any port speeds set to 115200 and upgrade to ComOS release 3.5L and then downgrade to any previous release, you must set the port speeds again after downgrading.

The installation software can be retrieved by FTP from **ftp://ftp.livingston.com/pub/le/software/*system*/*tarfile.tar.Z***, replacing *system* and *tarfile.tar.Z* with the actual names of the files.

/pub/le/software/	**Operating System**
bsdi/pm_3.5.1_BSDOS_2.0.tar.Z	BSD/OS 2.0 and 2.1
sgi/pm_3.5.1_IRIX_5.2.tar.Z	SGI Irix 5.2
linux/pm_3.5.1_Linux.tar.Z	Linux 1.2.13 ELF
rs6000/pm_3.5.1_RS6000_4.1.tar.Z	RS6000 AIX 4.1 (no longer 3.2.5)
alpha/pm_3.5.1_alpha_T3.0.tar.Z	Digital Alpha OSF/1 T3.0
hp/pm_3.5.1_hp9000_10.01.tar.Z	HP 9000 HP/UX 10.01
sun4/pm_3.5.1_sun4.tar.Z	SunOS 4.1.4, Solaris 2.5.1 on Sparc
sun86/pm_3.5.1_sun86_5.5.tar.Z	Solaris/X86 2.5.1
pc/pmw3511.exe	Windows 95 and Windows NT 4.0

You can FTP the upgrade image at the same time. This example shows an administrator retrieving the SunOS pminstall and Office Router upgrade image.

```
umask 22
mkdir /usr/portmaster
cd /usr/portmaster
ftp ftp.livingston.com
        (Enter anonymous)
        (Enter your e-mail address; it will not echo.)
 binary
 cd /pub/le/software/sun4
 get pm_3.5.1_sun4.tar.Z pm.tar.Z
 cd /pub/le/upgrades
 get or_3.5L
 quit
tar xvf pm.tar
rm pm.tar
mv or_3.5L data
./pminstall
```

PMconsole 3.5.1.1 for Windows 95 and Windows NT 4.0 is available in **ftp://ftp.livingston.com/pub/le/software/pc/pmw3511.exe** in a self-extracting file. FTP that file, run the file to install PMconsole for Windows, move the upgrade file into the data directory, run PMconsole for Windows, and click on the Upgrade button.

The upgrade images are at **ftp://ftp.livingston.com/pub/le/upgrades/**.

ComOS	Upgrade Image	Product
3.5	pm2_3.5	PortMaster 2, 2E, 2ER, 2R, 2i, 2E-10I
3.5	pm25_3.5	PortMaster 25
3.5R	irx_3.5R	IRX-111, 112, 114, 211
3.5L	or_3.5L	OR-M, U, ST, LS and HS

ComOS 3.5R adds the NAS-Prompt-User attribute to the RADIUS dictionary file. The latest dictionary file is available for RADIUS 1.16 and RADIUS 2.0 at **ftp://ftp.livingston.com/pub/le/radius/dictionary**.

The upgrade does not affect your stored configuration in the PortMaster. If you would like to backup your PortMaster configuration before upgrading, run **pmreadconf**:

```
cd /usr/portmaster
./pmreadconf pmname pmpassword data/pmname.conf
chmod 600 data/pmname.conf
```

Copyright and Trademarks

The names Livingston, PortMaster, ComOS, RADIUS, ChoiceNet, PMconsole, IRX, True Digital, RAMP, and Total Access. Sure and Simple. are trademarks of Livingston Enterprises, Inc. All other marks are the property of their respective owners.

Notices

Livingston Enterprises, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Livingston Enterprises, Inc. reserves the right to revise this publication and to make changes to its content, any time, without obligation to notify any person or entity of such revisions or changes.

Contacting Livingston Technical Support

Every Livingston product comes with a one year hardware warranty. To obtain technical support, contact Livingston Enterprises Monday through Friday between the hours of 6 a.m. and 5 p.m. (GMT -8). Please record your Livingston ComOS version number and report it to the technical support staff.

By voice, dial (800) 458-9966 within the USA (including Hawaii), Canada, and the Caribbean, or +1 (510) 426-0770 from elsewhere. By FAX, dial +1 (510) 426-8951. By electronic mail, send mail to "support@livingston.com." Using the World Wide Web, see "http://www.livingston.com/."

You can schedule one-hour installation appointments in advance by calling the technical support telephone number listed above. New releases and upgrades of Livingston software are available via anonymous FTP from "ftp.livingston.com."