ComOS 3.4.1L Release Note

Introduction

The new Livingston Enterprises ComOS™ 3.4.1L software release is now available for the PortMaster™ Office Router OR-M and OR-U, and adds support for the new PortMaster Synchronous 384K Office Router (OR-LS) and PortMaster Synchronous T1/E1 Office Router (OR-HS). The only feature change from 3.4L is the support for the two new synchronous office routers.

This software release is provided at no charge to all Livingston customers. The following document describes the features of the ComOS 3.4L and 3.4.1L software release and how to upgrade your PortMaster. Upgrade instructions are included at the end of this release note.

WARNING! YOU MUST USE PMINSTALL VERSION 3.3 OR LATER IN ORDER TO PERFORM THIS UPGRADE!

Contents

Introduction 1
Contents 1
New Features in ComOS 3.4.1L 1
New Features in ComOS 3.4L 2
Bug Fixes in ComOS 3.4L 6
ISDN Basic Rate Interface (BRI) support 6
Configuring ISDN 7
New RADIUS Attributes 9
Quick Setup Example for OR-U 10
Quick Setup Example for OR-LS or OR-HS 11
Upgrade Instructions 11
Copyright and Trademarks 12
Notices 12
Contacting Livingston Technical Support 12

New Features in 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.

New Features in ComOS 3.4L

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

Description of New Features in ComOS 3.4L

This section describes the new features in ComOS 3.4L in more detail.

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 6 for specific information about ISDN support on the OR-U.

Multilink PPP on ISDN

Multilink PPP is now supported on ISDN interfaces. This is supported concurrently with the Livingston Multi-line Load Balancing. The PortMaster 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 PC modem to make 128Kbps connections to the PortMaster OR-U. 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 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 attributes have been added to allow more user control when performing outbound dialing. Specifically the new attributes 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. 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`" causes the modules to not load. Any device drivers or subsystems not needed provide additional operational memory for the PortMaster.

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. In this case the only authentication supported is PAP or simple username/password. 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 (MP) 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 using 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 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 login users through the user Table. By using the "`set user` *`Username`* `local-ip-address` *`IPaddress`*" command, the PortMaster advertises the local-ip-address as its IP address as 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 so clients can learn 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 now logs an Accounting Start record (with no User-Name) 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. To authenticate using PAP as user *User* with password *Password*, 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 V25bis 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 in ComOS 3.4L

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.

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 the BRI port 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 Multiline 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. 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 7 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 on the PortMaster ISDN dialer 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 two additional things need to be configured on the PortMaster to permit ISDN service, with an optional third thing. They are: the ISDN Switch type, a Service Profile Identifier (SPID) for each ISDN port, and optionally a directory number 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:

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

To turn off debugging use the 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 the command "`set debug isdn on`" provides debugging information. 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 *Communications Server 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 V25bis 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 TelCo
NO-SERVICE	DCD- CTS+ TELCO+ NT1+	Cable and ISDN circuit OK but SPID not registered

Port Status	Modem Status	Description
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 as described below, 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 Enhancements 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 assigned address pool. She is only allowed to connect once concurrently per PortMaster. After ten minutes of idle time without any traffic she is disconnected. After two hours elapsed time she is disconnected regardless of what she is doing.

```
#
# Example PPP user, address Assigned by PortMaster
#
Pfn         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
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
```

Upgrade Instructions

These upgrade instructions assume you have already installed the PMconsole™ software into `/usr/portmaster` from floppy, CDROM, or FTP from `ftp://ftp.livingston.com/pub/le/`. To upgrade, run `pminstall`:

```
# /usr/portmaster/pminstall
```

To upgrade to ComOS 3.4.1L, run `pminstall` (version 3.3 or later) and choose the Upgrade PortMaster option, choose `or_3.4.1L` from the menu of upgrade choices, enter the hostname or IP address of your PortMaster, and enter the administrative password of your PortMaster. `pminstall` then upgrades your PortMaster to ComOS 3.4.1L.

Copyright and Trademarks

© 1996 Livingston Enterprises, Inc. All rights reserved.

The product names, “ComOS,” “IRX,” “PortMaster,” “PMconsole,” and “TelePath” are trademarks belonging to Livingston Enterprises, Inc.

All brand product names mentioned in this document are trademarks or registered trademarks of their respective manufacturers.

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 free lifetime software technical support and a one year hardware warranty. Livingston Enterprises provides free technical support via voice, FAX, and electronic mail. Technical support is available Monday through Friday 6am-5pm Pacific Time (GMT-8).

To contact Livingston technical support by voice, dial 1-800-458-9966 within the US or 1-510-426-0770 outside the US, by FAX, dial 1-510-426-8951, by electronic mail, send mail to support@livingston.com, and through the World Wide Web at http://www.livingston.com/.