LMS4000

900 MHz Radio Network

User Guide

APCD-LM043-8.0 (DRAFT C)

:

WaveRider Communications Inc.
Software License Agreement

This is a legal agreement between you (either an individual or an entity) and WaveRider Communications Inc. for the use of WaveRider computer software, hereinafter the "LICENSED SOFTWARE".

By using the LICENSED SOFTWARE installed in this product, you acknowledge that you have read this license agreement, understand it, and agree to be bound by its terms. You further agree that it is the full and complete agreement between you and WaveRider Communications Inc., superseding all prior written or verbal agreements of any kind related to the LICENSED SOFTWARE. If you do not understand or do not agree to the terms of this agreement, you will cease using the LICENSED SOFTWARE immediately.

1. GRANT OF LICENSE—This License Agreement permits you to use one copy of the LICENSED SOFTWARE.
2. COPYRIGHT—The LICENSED SOFTWARE is owned by WaveRider Communications Inc. and is protected by copyright laws and international treaty provisions; therefore, you must treat the LICENSED SOFTWARE like any other copyrighted material (e.g., a book or magazine). You may not copy the written materials accompanying the LICENSED SOFTWARE.
3. LIMITS OF FEATURE AVAILABILITY—The LICENSED SOFTWARE is sold with limitations as to certain feature availability and use. These limits are governed by the terms of the purchase agreement. Any actions resulting in the exceeding of these limits is not permitted, and can result in unpredictable performance.
4. OTHER RESTRICTIONS—You may not rent or lease the LICENSED SOFTWARE. You may not reverse engineer, decompile, or disassemble the LICENSED SOFTWARE.
5. LIMITED WARRANTY—The LICENSED SOFTWARE is provided "as is" without any warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the LICENSED SOFTWARE is with you, the licensee. If the LICENSED SOFTWARE is defective, you assume the risk and liability for the entire cost of all necessary repair, service, or correction.

   Some states/jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from state/jurisdiction to state/jurisdiction.

   WaveRider Communications Inc. does not warrant that the functions contained in the LICENSED SOFTWARE will meet your requirements, or that the operation of the LICENSED SOFTWARE will be error-free or uninterrupted.
6. NO OTHER WARRANTIES—To the maximum extent permitted by applicable law, WaveRider Communications Inc. disclaims all other warranties, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, with regard to the LICENSED SOFTWARE and the accompanying written materials.
7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES—To the maximum extent permitted by applicable law, in no event shall WaveRider Communications Inc. or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the LICENSED SOFTWARE, even if WaveRider Communications Inc. has been advised of the possibility of such damages, or for any claim by any other party.

   Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

   In no event will WaveRider's liability exceed the amount paid for the LICENSED SOFTWARE.

:

The following are trademarks or registered trademarks of their respective companies or organizations:

Castlerock SNMPc Server / Castle Rock Computing

Adobe Acrobat

RELEASE 8.0, August 2003

:

Warranty

In the following warranty text, “WaveRider®” shall mean WaveRider Communications Inc.

This WaveRider product is warranted against defects in material and workmanship for a period of **one (1) year** from the date of purchase. During this warranty period WaveRider will, at its option, either repair or replace products that prove to be defective.

For warranty service or repair, the product must be returned to a service facility designated by WaveRider. Authorization to return products must be obtained prior to shipment. The WaveRider RMA number must be on the shipping documentation so that the service facility will accept the product. The buyer shall pay all shipping charges to WaveRider and WaveRider shall pay shipping charges to return the product to the buyer within Canada or the USA. For all other countries, the buyer shall pay shipping charges as well as duties and taxes incurred in shipping products to or from WaveRider.

WaveRider warrants that the firmware designed by it for use with the unit will execute its programming instructions when properly installed on the unit. WaveRider does not warrant that the operation of the unit or firmware will be uninterrupted or error-free.

Limitation of Warranty

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by the buyer, buyer-supplied interfacing, unauthorized modification or misuse, operation outside the environmental specifications for the product, or improper site preparation or maintenance. No other warranty is expressed or implied. WaveRider specifically disclaims the implied warranties of merchantability and fitness for any particular purpose.

No Liability for Consequential Damages

To the maximum extent permitted by applicable law, in no event shall WaveRider or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the product, even if WaveRider has been advised of the possibility of such damages, or for any claim by any other party.

Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

In no event will WaveRider’s liability exceed the amount paid for the product.

Regulatory Notices

This equipment has been tested and found to comply with the limits for a Class B Intentional Radiator, pursuant to Part 15 of the FCC Regulations and RSS-210 of the IC Regulations. These limits are intended to provide protection against harmful interference when the equipment is operated in a residential environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Notice to User

Any changes or modifications to equipment that are not expressly approved by the manufacturer may void the user’s authority to operate the equipment.

Contents

:

:

— This page is intentionally left blank —

Figures

:

Tables

:

:

Preface

About this Manual

WaveRider recommends that you read the following sections before proceeding with the instructions in this guide:

- *Software License Agreement* on page ii
- *Warranty* on page iv
- *Warnings and Advisories* on page xix
- *Conventions* on page xvii

NOTE: The information contained in this manual is subject to change without notice. The reader should consult the WaveRider web site for updates.

Document Scope

This user guide refers to software version 4.0. *What's New in Version 4.0* on page xxi lists the main features of version 4.0.

In this manual, the term "EUM" refers to both EUM3000 and EUM3003 devices, unless specifically stated.

NOTE: EUM3003 devices are limited to Telnet access only and have no serial console port. CCU3000 and EUM3000 devices are accessible through both Telnet and the serial console port.

Conventions

The following conventions are used throughout this document:

WARNING!

Whenever you see this icon and heading, the associated text addresses or discusses a critical safety or regulatory issue.

CAUTION: Whenever you see this icon and heading, the associated text discusses an issue, which, if not followed, could result in damage to, or improper use of, the equipment or software.

:

TIP: Whenever you see this icon and heading, the associated text provides a tip for facilitating the installation, testing, or operation of the equipment or software.

Regulatory Notices

This device has been designed to operate with several different antenna types. The gain of each antenna type shall not exceed the maximum antenna system gain as given in Appendix F on page 229. Antennas having a higher gain are strictly prohibited by Industry Canada and FCC regulations. The required antenna impedance is 50 ohms.

Industry Canada

CCU3000, EUM3000, and EUM3003

The IC Certification Number for the CCU3000 and EUM3000 is 3225104140A. The IC Certification Number for the EUM3003 is 3225B-EUM3003.

Operators must be familiar with IC RSS-210 and RSS-102. The CCU and EUM have been designed and manufactured to comply with IC RSS-210 and RSS-102.

Federal Communications Commission

CCU3000, EUM3000, and EUM3003

The CCU3000, EUM3000, and EUM3003 have been designed and manufactured to comply with FCC Part 15.

Operators must be familiar with the requirements of the FCC Part 15 Regulations prior to operating any link using this equipment. For installations outside the United States, contact local authorities for applicable regulations.

The FCC ID for the CCU3000 and EUM3000 equipment is OOX-LMS3000. The FCC ID for the EUM3003 equipment is OOX-EUM3003.

The transmitter of this device complies with Part 15.247 of the FCC Rules.

The CCU3000, EUM3000, and EUM3003 (with outdoor antenna only) must be professionally installed.

Interference Environment

Operation is subject to the following conditions:

- This device may not cause harmful interference and,
- This device must accept any interference received, including interference that might cause undesired operation.

Operational Requirements

CCU3000, EUM3000, and EUM3003

In accordance with the FCC Part 15 regulations:

1. The maximum peak power output of the intentional radiator shall not exceed one (1) watt for all spread spectrum systems operating in the 902 to 928 MHz band. This power is measured at the antenna port of the CCU or the EUM.
2. Stations operating in the 902 to 928 MHz band may use transmitting antennas of directional gain greater than 6 dBi, provided the peak output power from the intentional radiator is reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.

NOTE: The gains referred to in point 2 are with respect to the total antenna system gain.

3. The operator of a spread spectrum system and the user of the radio device are each responsible for ensuring that the system is operated in the manner outlined in *Interference Environment* on page xviii.

Warnings and Advisories

General Advisory

Operator and maintenance personnel must be familiar with the related safety requirements before they attempt to install or operate the LMS4000 equipment.

It is the responsibility of the operator to ensure that the public is not exposed to excessive Radio Frequency (RF) levels. The applicable regulations can be obtained from local authorities.

Do not operate the CCU or EUM without connecting a 50-ohm termination to the antenna port. This termination can be a 50-ohm antenna or a 50-ohm resistive load capable of absorbing the full RF output power of the transceiver.

WARNING!

The LMS4000 external antennas must be professionally installed and properly grounded. Antennas and associated transmission cable must be installed by qualified personnel. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

:

WARNING!

To comply with FCC RF exposure limits, the antennas for the CCU must be fix-mounted on outdoor permanent structures to provide a separation distance of 2 m or more from all persons to satisfy RF exposure requirements. The distance is measured from the front of the antenna to the human body. It is recommended that the antenna be installed in a location with minimal pathway disruption by nearby personnel.

The antennas for the EUM must be fix-mounted, indoors or outdoors, to provide a separation distance of 20 cm or more from all persons to satisfy RF exposure requirements. The distance is measured from the front of the antenna to the human body. Again, it is recommended that the antenna be installed in a location with minimal pathway disruption by nearby personnel.

Notice to Users

Special Accessories

In order to comply with FCC Part 15 standards, the EUM3003 must be used with an Ethernet Patch Cable with permanently attached ferrite filter. This cable is supplied as part of the EUM3003 kit. Additional cables, both crossover and straight-through, are available from WaveRider Communications Inc. Responsibility to ensure the correct patch cable is used lies with the end-user.

Customer Support

Telephone:	+1 416–502–3161
Fax:	+1 416–502–2968
Email:	**Customer Services Group:** techsupport@waverider.com **Customer Documentation Feedback and Comments:** customerdocs@waverider.com
URL:	www.waverider.com

WaveRider offers a complete training program. Please contact your sales representative for training information.

What's New

What's New in Version 4.3

Version 4.3 introduces the following CCU and EUM features:

Spectrum Analyser

A major new feature available in Version 4.3 is the Spectrum Analyser, a tool useful for site surveys, installation and troubleshooting. Functionally, it provides an indication of signal level and interference, from external sources and from frequency re-use. On the CCU and EUM, the `radio analyze` command will force the radio to step across the 900 MHz ISM frequency band. At each frequency, it will measure and report peak, average and noise floor powers. The radio will also report the presence and level of any packets received from a WaveRider CCU3000 or NCL1900.

The results of the spectral analysis can be displayed in tabular or graphical form. The graphical display is available as an Adobe Portable Document Format (PDF) file, which can be retrieved from the modem through FTP. An example is shown in Figure 1 on page xxii.

:

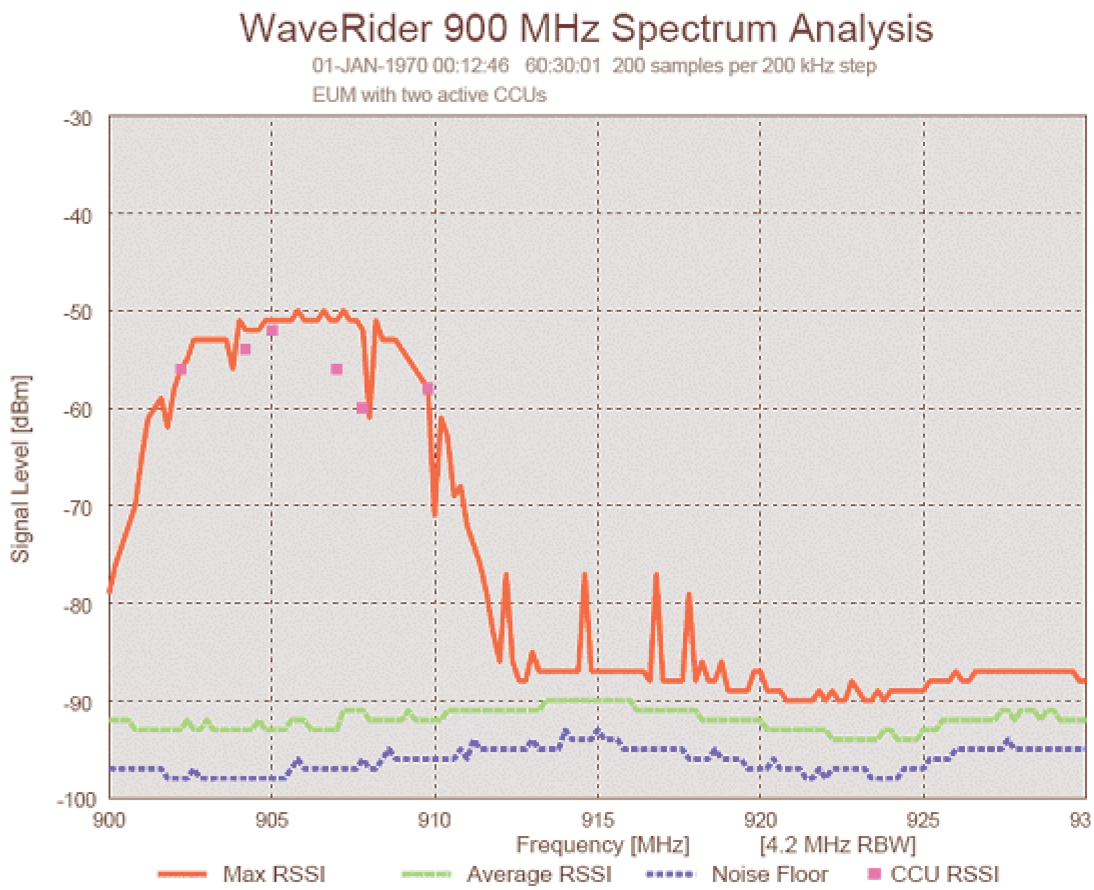


Figure 1 Sample WaveRider 900 MHz Spectral Analysis

Transmit Power Steps

The transmit power level can now be programmed in 1 dB steps from +15 to 26 dBm. The ability to set the transmit power in 1 dB steps is particularly useful in high-density environments, where site-to-site interference may be a problem.

RSSI, SQ and RNA on CCU

The CCU now measures and reports RSSI, SQ and RNA on a per-EUM basis. RSSI is the received power measured when a packet is received from a particular EUM. SQ is the signal quality measured at the same time, and RNA is the difference between the RSSI and the noise floor which, in turn, is measured between packet transmissions and receptions.

These statistics now appear in the Watch Results display, and the RSSI display for the EUM that is under watch. Columns have also been added to the Registration (Air) and ARP Map tables for RSSI, SQ and RNA for each EUM.

Watch Display Summary Calculations

The Watch Results display has been improved and now resembles the Statistics Summary display. Percentages and totals are now displayed for *Transmitted Packets*, *Transmitted Payloads*, *Received* and *Expected Responses* and *Received Payloads.* RSSI, SQ and RNA have also been added to the Watch Results display.

Gratuitous ARP

The EUM now transmits a “gratuitous” ARP (an ARP for its own IP address) two seconds after power up. This gratuitous ARP can be used to determine the IP address of an EUM if it is not already known. The operator can either sniff the ARP packet on the Ethernet interface, or look in the ARP table of a connected host.

Network LED Change

The Network LED now flashes slowly during Ethernet-only traffic, instead of being on solid.

EUMID of Duplicate IP Address Packet

The CCU detects packets that are received over the air with the CCU IP address as the source address. This is considered a “duplicate IP address” and the packet is discarded. The CCU increments the Routing Protocol statistic *Rx Radio Err - Duplicate IP address (Discard)*. It also records the EUMID of the EUM from which the packet was received (*Last Duplicate IP from EUMID XX:XX:XX*).

Problem Fixes

The following problems were resolved in Version 4.3:

- The RADIUS period is now entered in minutes. Conversion of the previous value from seconds will occur automatically if it has been changed.
- The size of the Bridge Table has been increased to *1800*.
- Telnet no longer truncates very large tables.
- The SNMP MIBII sysName has been changed to *LMS3000*.
- RADIUS parameters are now reported, whether the client is enabled or not.
- The radio interface MTU is now correctly reported as *1500*.
- Rx No Match is now displayed correctly in the CCU statistics summary display.

:

What’s New in Version 4.0

Version 4.0 introduced the following CCU and EUM features:

Switched Ethernet Mode and Through Only Mode

The CCU can now act as an Ethernet Switch, with the CCU Ethernet and radio interfaces in the same Ethernet domain, rather than as a router. Packets arriving at the CCU from the radio port are switched either out the Ethernet port, back out the radio port, to the application and/or all three based on the Ethernet header. The switching function on the radio side is identical to Routed mode, but the Ethernet port (in promiscuous receive mode) is added as one more port to switch to. A bridge table is maintained for the Ethernet port, similar to that at the EUM, except that no restriction on “air access” is made.

Through Only mode is identical to Switched Ethernet mode, except that traffic from the radio port (including broadcast) is not switched back out the radio port—it is sent out the Ethernet port instead. This allows the operator to monitor and control traffic between users on the same CCU and is probably most useful with PPPoE operations.

The default mode from the factory is Switched Ethernet mode, but a CCU upgraded from version 3.x remains in Routed mode.

No change is required to the EUMs to support Switched Ethernet or Through Only mode.

> **NOTE:** This allows for multiple IP subnets in the system. That is, PCs could be given public IP addresses and EUMs could be given private IP addresses.

The CCU has only one IP address in these modes (which is the same as the radio IP address in routed mode). It is printed as “IP address” rather than “Ethernet IP address” or “Radio IP address”.

Several new routing protocol statistics have been added to record this activity.

Command changes in Switched Ethernet (and Through Only) Mode

The **`protocol`** command at the CCU selects between “routed”, “switched”, and “through”. The current mode is also reported in the BCF. It does not take effect until a reboot.

The **`ip eth`** and **`ip rad`** commands both set or report the IP address.

The **`bridge`** and **`customer`** commands now display the Ethernet bridge table on the CCU.

PPPoE Support

PPPoE packets are now permitted through the network. Since PPPoE is an Ethernet subnet restricted protocol, the packets only pass from the radio side to the Ethernet side of a CCU in Switched Ethernet or Through Only mode.

RADIUS Authorization and Accounting Support

The CCU now supports RADIUS authorization and accounting. When enabled, the CCU generates a RADIUS access-request message for each registered EUM on a periodic basis. The responses from the RADIUS server are used to maintain the authorization table.

If accounting is enabled, the CCU sends periodic accounting updates to the RADIUS server for each registered EUM. These updates contain the Input and Output Packet and Byte counts for each EUM (Input is received from EUM, Output is transmitted to EUM).

The following new RADIUS commands are available on the CCU:

- **auth radius disable**
- **auth radius enable**
- **auth radius primary**
- **auth radius secondary**
- **auth radius period**
- **auth radius acct disable**
- **auth radius acct enable**
- **stats auth**

All RADIUS commands take effect immediately (without a reboot).

RADIUS settings are stored in basic.cfg, with the shared secret passwords securely encrypted.

The authorization table has a new column indicating whether an entry was entered from the CLI (static) or by a RADIUS response (radius). Non-response to RADIUS requests following the first is indicated in this column as well.

Air Table Accounting Info

The Tx-octet, Tx-packet, Rx-octet and Rx-packet counts maintained for RADIUS accounting are also printed out in the registration table as shown below:

```
Maximum Associations: 75
Deregistration Count: 8
REGISTERED EUMs
  EUM ID GOS Class RSSI[dBm] Time[s] Rx-Octets Rx-Packets  Tx-Octets Tx-Packets
-------------------------------------------------------------------------------
60:30:02    bronze      -63       3    2177379       1471      42042        766

 1 EUMs registered of 300 allowed
```

Low Impact Polling

The polling algorithm has been modified to reduce the number of CCU transmissions under low load—and therefore the amount of time the spectrum is occupied—without reducing capacity or affecting latency. This improvement is achieved primarily by eliminating redundant random access polls.

:

Previously, the CCU chose, at the beginning of each polling cycle, which EUM (or random access) to poll. If no EUM was ready to be polled, a random access poll was sent. Now, the CCU both chooses which EUM (or random access) to poll and when to do so. So, if no EUM (or random access) is ready to be polled immediately, it determines which will be ready soonest and schedules the poll for that time.

In a heavily loaded system, the result is nearly identical (see minIPS change below) to the previous system—there is always an EUM ready to be polled, so the spaces between poll cycles are the minimum possible. No change in capacity or responsiveness occurs.

In a lightly loaded or idle system, the difference in spectral occupancy is profound, without a noticeable change in system responsiveness. In an idle system, random access polls are spaced 55 ms apart (the same spacing as in a heavily loaded system) and are less than 1 ms long, so the channel is occupied less than two percent of the time. When only one or two users are active, the polls occur at exactly the desired rate—every 29 ms for default best effort users—leaving large gaps between cycles.

One parameter has changed meaning slightly. The minIPS parameter previously indicated the minimum allowed spacing between two polls of the same EUM and was primarily used to set an upper limit on the polling rate. The minIPS parameter now indicates the minimum allowed average spacing between two polls of the same EUM. That is, the EUM will be polled no more often, on average, than every minIPS. The average is over a short time span of about 10 polls. This improvement more accurately provides the usually desired control—which is a transfer rate cap—as the effects of transient traffic spikes are averaged out.

To further reduce the impact of a lightly loaded system on other users of the spectrum, gaps between poll cycles are constrained to be at least 10 ms long. Polling cycles that would have been closer together are re-arranged ahead and behind these gaps. Random access polls are treated slightly differently than others to enhance this.

The ideal and max IPS violation counts in the load meter are slightly more sensitive.

NOTE: Low impact polling will be immediately noticeable in the `rad rssi` display: the number of received packets will be as low as 16 per second in an idle system. Users used to seeing 900+ may be concerned.

Long Reply Timeout

The CCU reply timeout has been increased by 200 us, which extends the timeout radius from 10 km to 40 km. Note that it does not improve the RF range.

Duplicate IP Detection and Protection

The CCU discards ARPs from the radio with a duplicate source IP address to its own, while printing out a warning including the EUM ID of the station the packet came from. The routing protocol statistic “Rx Radio Err – Duplicate IP address” counts these duplicates. Previously, setting an EUM or user-PC IP address the same as the CCU would disrupt traffic as these ARP requests and responses would corrupt ARP tables across the network.

Ethernet Link Status Indication

Ethernet Link Status is now reflected in the esmc0 interface operational status MIB variable. It is Up if the link light is on, Down if not. Note that adminStatus is always Up as it is never turned off. These statistics are available from the **`snmp interface`** command or through SNMP.

Radio Link Status Indication

The **`radio`** command now displays the message “Radio disabled” if it is.

Radio Link Status is now reflected in rdr1 interface admin status and operational status MIB variables. These are available from the **`snmp interface`** command or through SNMP.

- CCU: Both are Up if the radio is enabled and Down if not.
- EUM: Admin status is Up if the radio is enabled and Down if not. Operational status is Up if the radio is enabled, it has heard from the CCU lately (RSSI is non-zero) and it believes it is registered (not denied), Down otherwise.

The **`air`** command on the EUM, now reports “Radio disabled”, “Not Registered”, “Registered, but haven't received from CCU in at least 1 second” or “Registered.” It reports registered if it has been registered with the CCU and has not been explicitly deregistered. If it has been denied at the CCU, but the EUM has not originated traffic since, it still reports “Registered”. Also, if no traffic has flowed for 12 hours, or the CCU has been rebooted, the CCU may not have it in the air table, but it still thinks it is registered. A unit denied and then authorized again may take up to 10 minutes to re-register.

Client IP Address Logging

The client IP address is written to the system log on the following events:

- Telnet login
- Telnet debug login
- Telnet password fail 3 times
- FTP login
- FTP password rejected

Command Line History

A ten-line history buffer is kept of previous commands. The up and down arrows scroll through the list of previous commands, which can then be edited. “!!” is no longer supported.

INOP Console Improvements

The commands **`radio`**, **`radio frequency`**, and **`radio rf`** are available in the INOP console. This improvement allows an EUM to be commissioned from the INOP console.

Link Quality Test Shortcuts

The **file get** command syntax has been extended to simplify link quality testing.

The **file get** command, with no parameters, expands to **file get <gatewayIP> buywavc null null**, where **<gatewayIP>** is the gateway IP address for the unit. The operator is prompted for the password. This is the short form for the link quality test at an EUM where its gateway is the CCU.

The **file get <ip>** command, with one parameter, expands to **file get <ip> buywavc null null**, where **<ip>** is the IP address or EUM ID of the unit to get the file from. It prompts you for the password. This is the short form for the link quality test at a CCU or an EUM where the gateway is not the CCU (such as in Switched Ethernet mode).

Address Resolution by EUM ID

If you know the EUM ID of a station, several commands resolve for the IP address, either looking up the corresponding Ethernet MAC address in the ARP table or using a reverse ARP request.

You can enter the EUM ID (in the format XX:XX:XX) rather than the IP address in the following commands:

- **ping <EUM ID>**
- **telnet <EUM ID>**
- **file get <EUM ID>** (with or without the other parameters)
- **arp map <EUM ID>**

NOTE: A 3.x EUM or CCU will NOT respond to the RARP; but if there is an entry in the local ARP table already, the ARP lookup will work.

Watch by IP Address

The **watch** command at the CCU now takes either an EUM ID or an IP address as an argument. Given an IP address, it attempts to determine which EUM the host with that IP address is using. The IP address of the EUM or PC connected to that EUM both resolve to the EUMID.

NOTE: The statistics collected are still for that EUM and not only for packets to and from the IP address.

Table Sorting

The air, authorization, and address tables are now displayed sorted by EUM ID. (Note that the ARP and ARP map tables are already sorted by IP address).

IP and Subnet Print Formatting

The IP address, subnet, and subnet mask are now printed more clearly and in the format they are entered:

- `IP Address: 192.168.10.11 / 24`
- `IP Subnet : 192.168.10.0 ( 255.255.255.0 )`

File Directory CRC

The **`file dir`** command computes and displays a 32 bit CRC over each file in the file system. The FTP “LIST” command produces the same information. The sa1110.exe, sa1110.bak, port.cfg, and bootrom.bin CRCs are published in the software upgrade procedure.

Ping Test Formatting

Ping times are rounded rather than truncated and the precision is reported as +-8 ms on the header line.

Summary Statistics Improvement

The **`stats summary`** command has been enhanced with better explanations, calculations and percentages. The display varies slightly between CCU and EUM. An example of each is shown below. Note that “Fail Q Too Long” and “Fail Timeout” are not included in the totals for the percentages as they are not ever transmitted.

Table 1 CCU and EUM Stats Summary

CCU	EUM
Transmitted Payloads broadcast : 12 0.1% 10k : 5150 82.0% 20k : 842 13.4% 30k : 206 3.2% 40k : 51 0.8% Fail Retry : 19 0.3% Fail Q Too Long : 0 Received and Expected Responses HCRC Error : 0 0.0% Directed : 7006 82.2% Random Access : 12 0.1% No Reply Received : 1495 17.5% Received Payloads FCS Error : 1 0.0% Duplicate : 0 0.0% Too Busy - Discard : 0 0.0% Delivered : 3589 99.9%	Transmitted Payloads 10k : 6209 99.9% 20k : 1 0.0% 30k : 0 0.0% 40k : 0 0.0% Fail Retry : 0 0.0% Fail Timeout : 0 Received Packets HCRC Error : 4 0.0% Directed : 11927 74.2% Broadcast : 4136 25.7% No Match : 0 0.0% Received Payloads FCS Error : 120 1.1% Duplicate : 0 0.0% Too Busy - Discard : 0 0.0% Delivered : 10738 98.8%

Radio Meter Improvement

The **`radio meter`** command can now take an interval in seconds [1-30] as an argument and prints the metered values in rates per second, over that interval. The printouts continue at that interval until a key is pressed or the console times out. If no argument is given, the totals are printed. Only GOS classes that had some activity during the interval are displayed.

Determining the Software Version on a CCU or EUM

If you are uncertain which software version you have installed on a CCU or EUM, use the following commands to determine the version.

To Determine the Software Version on a CCU or EUM

1. Open the CCU or EUM console, as described in *Access Interface* on page 221.
2. At the prompt, type **`sys ver`** and press **Enter**.

   The software version is listed under the SA1110 heading. The Hardware Rev. is “A” if the device is a CCU3000 or EUM3000, and Hardware Rev. is “B” if the device is an EUM3003.

```
60:03:3a> sys ver

                     SA1110
-------------------------------------------------
CPU              : WaveRider LMS3000 - ARMSA1110
Hardware Rev.    : A
OS-BSP Version   : 5.4/1.4
Software Version: v4.0
Software Build   : 9 - Polled MAC
Creation Date    : Mar 24 2003

                     ATMEL
------------------------------------------------
Vendor           : WaveRider
Firmware Version: V2(p)1.2
Hardware Rev.    : V1(CCU)


                     Bootrom
-------------------------------------------------

Copyright 1984-2002 WaveRider Communications, Inc.
VxWorks version 1.4

Bootrom release v4.0
Created          Mar 24 2003, 16:25:10
60:03:3a>
```

1 Introduction

The LMS4000 system provides 900 MHz and 2.4 GHz wireless. high-speed Internet connectivity to business and residential subscribers. This manual, which is specific to the LMS4000 900 MHz Radio Network, provides the following information:

- A detailed description of the operation of the hardware and software
- Guidelines for planning and designing your network
- Instructions for configuring, installing, monitoring, maintaining, and troubleshooting the 900 MHz radio modem
- Support information that you may find useful for operating your network

TIP: The installation of other LMS4000 network equipment is described in *LMS4000 Installation Guide*, which can be obtained from WaveRider.

The LMS4000 900 MHz Radio Network, which operates in the 900 MHz ISM band, offers the following features and benefits:

- **Multiple Communication Modes:** The LMS4000 900 MHz radio network includes three different communication modes:
  - **Routed Mode**—This mode has always been available in the LMS4000 network. With routed mode, the CCU acts as an IP router between the Ethernet and radio subnets and a switch between EUMs.
  - **Switched Ethernet Mode**—In this mode, the CCU acts as an Ethernet switch between the Ethernet port and the EUMs. It supports PPPoE (Point-to-Point Protocol over Ethernet), IP (Internet Protocol), and ARP (Address Resolution Protocol) connections, as well as any number of IP subnets on either or both sides of the CCU. This mode provides simplicity of operation.
  - **Through Only Mode**—Similar to Switched Ethernet mode, this mode constrains all traffic to flow only from a radio link to the Ethernet port or vice versa, not from one radio link to another.
- **Excellent Propagation Characteristics:** LMS4000 900 MHz radio networks provide excellent coverage to non-line of sight installations using WaveRider's proprietary

indoor diversity antenna and extended coverage to installations using external high-gain antennas.The 900 MHz ISM band is more suited to NLOS (non-line of sight) wireless Internet applications than other ISM bands because it has superior propagation performance, demonstrating the following benefits:

- Lower free-space, cable and foliage loss
- Better wall and glass penetration
- More signal recovery from diffraction and reflection

- **High-speed Channel:** The LMS4000 900 MHz Radio Network provides a raw channel bit rate of 2.75 Mbps, which translates to peak FTP rates of 2 Mbps.
- **High-performance Polling MAC:** WaveRider's patented Polling MAC algorithm takes advantage of typical usage patterns found in Internet transactions, such as Web browsing and email, to provide an operating capacity of up to 300 end users per RF channel. Even with large numbers of subscribers, end users generally perceive that they have the entire channel to themselves.
- **Grade of Service Support:** The Polling MAC supports up to four end-user grades of service, which allows the system operator to segment service offerings for those users that demand and are willing to pay for higher grades of service, and those that are only willing to pay for a more basic grade of service.
- **License-free Radio Bands:** The main advantage of using the ISM band is that you need not apply to the FCC or Industry Canada for an operating license. This freedom reduces your time to market and the effort and high cost associated with obtaining a license.
- **Robust Hardware and Software:** LMS4000 hardware and software have been rigorously tested in lab and field environments. The hardware, which is mechanically robust, works over a broad range of temperatures and operating conditions. The software is equally robust and has been designed to recover automatically from unplanned events and abnormal operating conditions.
- **Simple End-user Modem Configuration:** The end-user modem is very easy to configure. Normally, operators pre-configure the EUM prior to field deployment, so they can maintain control over their network.
- **Simple End-user Modem Installation and Operation:** It is very easy to install and operate the EUM. So easy, in fact, that when the installation is based on the WaveRider indoor diversity antenna, the end user should be able to install and operate the modem with no involvement from the network operator. This simplicity saves the network operator the cost and inconvenience of having to visit the end-user's premises. The EUM uses a standard Ethernet interface which means the EUM and the antenna can be located up to 100 meters from the end-user's PC.
- **Flexible Network Topology:** The LMS4000 900 MHz Radio Network has a flexible topology, allowing it to line up with the operator's existing Internet points of presence and site facilities. As well, LMS4000 supports the following connections:
    - Connection between the end-user modem and the Internet through the network operator's gateway router
    - Direct connection between end-user modems through the LMS4000 900 MHz channel units (CCUs), if the CCU is configured to support this routing
    - Connection between end-user modems on different, but co-located, CCUs if these routes are configured in the CCU routing tables, if the CCU is configured to support this routing

- **DHCP Relay:** CCUs support DHCP relay, which, once enabled, allows end-user PCs to automatically obtain their IP and DNS server addresses from the network operator's DHCP servers. DHCP relay simplifies the EUM installation even further and makes it even easier for the modem to be installed by the end user.
- **End-user Registration:** All end user modems automatically transmit a registration request to the LMS4000 system so they can access the wireless network. They can only register if the network operator has authorized them in the CCU. This registration guarantees that only approved subscribers can gain access to LMS4000 wireless services.
- **RADIUS Support:** The LMS4000 system also supports RADIUS Authorization and RADIUS Accounting for EUM registration.
- **Remote System Configuration and Diagnostics:** The network operator can configure and monitor CCUs and EUMs from anywhere. This remote access allows the operator to make configuration changes, download new features, and diagnose problems remotely without having to visit distant network sites or end-user premises.
- **Spectrum Analyser:** The Spectrum Analyser tool is very useful for site surveys, installation and troubleshooting. Functionally, it provides an indication of signal level and interference, from external sources and from frequency re-use. On the CCU and EUM, the `radio analyze` command will force the radio to step across the 900 MHz ISM frequency band. At each frequency, it will measure and report peak, average and noise floor powers. The radio will also report the presence and level of any packets received from a WaveRider CCU3000 or NCL1900.
- **SNMP Support:** Using WaveRider-supplied SNMP MIBs, network operators can integrate the LMS4000 with their existing network management system to allow monitoring of CCUs and EUMs from an existing and/or centralized SNMP manager. Once SNMP is configured, the operator can monitor system events, parameters, and statistics in real time. Statistics can be processed in the SNMP manager to provide alarms, trend data, graphical outputs, and derived performance data.
- **Accurate Time Stamping (SNTP):** The CCUs and EUMs can be programmed to synchronize their internal clocks with one or more NTP servers. Time stamping enables all logged events in the CCUs and EUMs to be correlated with events that have taken place at other locations in the network or with events logged by equipment installed outside the network, if this equipment is equipped with accurate time-stamping. Accurate time-stamping facilitates diagnosis of complex network problems.
- **Field-replaceable Equipment:** In the event of an equipment failure, LMS4000 components are easily replaced with minimal or no disruption to the operation of other components.
- **System Upgradability:** The LMS4000 network architecture supports orderly growth from simple installations, through single-CCU CAP (Communication Access Point) sites and multi-CCU CAP sites, to multi-CAP networks.
- **Port Filtering:** The LMS4000 network operator can configure CCUs and EUMs to filter IP packets on specific TCP and UDP ports to improve network performance, security, and privacy.
- **Low Maintenance:** CCUs and EUMs require no routine maintenance, other than maintenance of their operating environments within the specified temperature and humidity range.

- **Extensive Installation, Maintenance and Diagnostic Support:** The CCU and EUM are equipped with a wide range of features and utilities to facilitate unit installation, operation, maintenance, monitoring, and diagnostics:
  - Visual status indicators on all units
  - Simple-to-use command-line interface, offering full unit configuration capability
  - Windows-based EUM configuration and installation utilities
  - RSSI (receive signal strength indication) output, to simplify antenna pointing and performance indication
  - Ability to remotely FTP files to and from CCUs and EUMs
  - Wide range of operating and performance statistics
  - SNMP support
  - RADIUS authorization and accounting
  - Simple and reliable field-upgrade process
  - Remote download of equipment configuration files to CCUs and EUMs

Your decision to implement an LMS4000 900 MHz Radio Network enables you to deliver high-quality, high-speed wireless Internet service to the business and residential subscribers in your serving area.

2 Quick Startup

This section outlines the procedure for setting up a very simple LMS4000 900 MHz radio network consisting of one CCU and one EUM. This simple network, which can be set up in a lab environment, helps you become familiar with basic LMS4000 configuration and operation. As you become more confident and are ready to progress to customer installations, WaveRider recommends reading the other sections in the manual.

Quick Startup uses static IP addresses for the purpose of simplicity, even though the CCU and EUM support DHCP relay.

2.1 Equipment

As a minimum, the Quick Startup requires the following equipment:

one CCU kit, consisting of

- CCU
- CCU power supply and cable
- CCU setup antenna

one EUM kit, consisting of

- EUM
- EUM power supply and cable
- 3m CAT5 crossover Ethernet cable with ferrite bead

one PC, equipped with terminal emulation software such as HyperTerminal and an Ethernet network interface card

one WaveRider indoor antenna, complete with mounting bracket and RF cable

one Straight-through RS-232 serial cable, DB-9 male to DB-9 female

2.2 Quick Startup Network

Figure 1 shows the IP addressing scheme for the quick startup network described in this chapter.

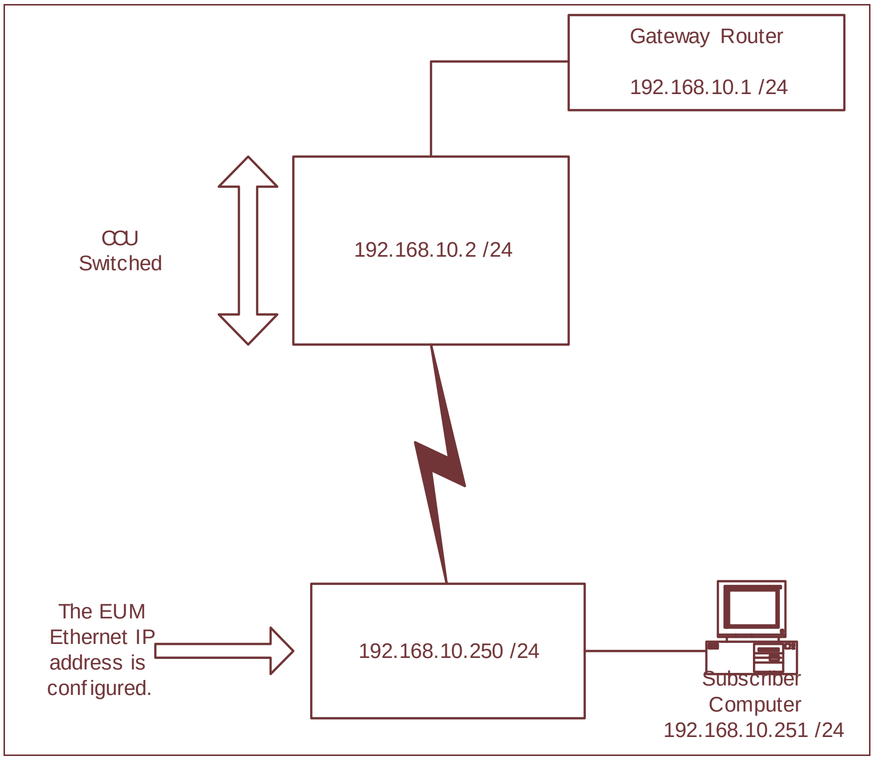


Figure 1 Quick Startup Network

2.3 Equipment Setup

Remove the equipment from the boxes and set up the physical configuration shown in Figure 2. The CCU is configured in Switched Ethernet mode with a gateway router being the gateway for the CCU, EUM, and subscriber PC. Use this setup procedure to configure the CCU, while keeping the following points in mind:

- Maintain the order of installation shown in Figure 2.
- Maintain at least 15 feet (4.5 meters) of physical separation between CCUs and EUMs.

- Ensure the paths between the CCU and EUMs are relatively free from obstruction.

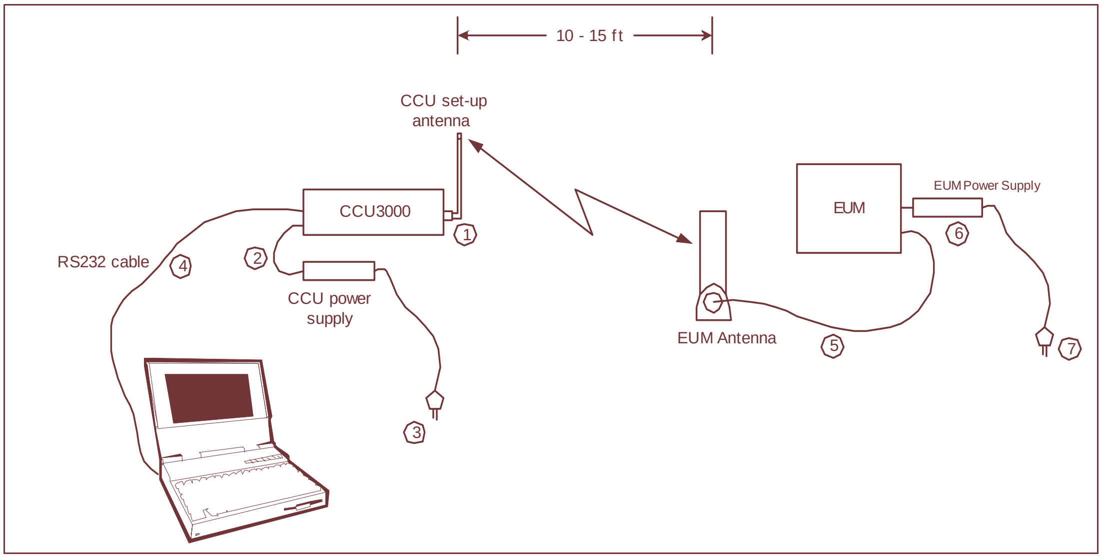


Figure 2 Quick Startup — CCU Configuration

For detailed information on connecting to CCUs and EUMs, please refer to Appendix E on page 221.

This section explains how to configure CCU and EUM parameters using the CLI.

2.4 CCU Configuration

The CCU serves as a switch. Normal end-user traffic is switched between the CCU Ethernet and radio interfaces.

In the following procedure, you will configure the following parameters on the CCU:

- Gateway IP address
- Radio IP address and subnet mask
- Radio frequency

To Configure the CCU

1. Open a connection to the serial console port, as described in *Access Interface* on page 221.

   You will see the following prompt:

   ```
   WaveRider Communications, Inc. LMS3000
   Password:
   ```

2. Type the password and press **Enter**.

   NOTE: The factory default password is a carriage return.

You will see the CCU command prompt:

```
60:03:3a>
```

NOTE: The default prompt on a CCU includes the last five characters of the CCU Serial Number.

3. Type the following commands to configure the CCU (commands are shown in bold):

```
60:03:3a> protocol switched
CCU in Switched Ethernet Mode

60:03:3a> ip radio 192.168.10.2 24
IP Address: 192.168.10.2 / 24
IP Subnet : 192.168.10.0 ( 255.255.255.0 )

60:03:3a> ip gateway 192.168.10.1
Gateway IP Address: 192.168.10.1

60:03:3a> ra freq 9050
Radio Frequency: 9050

60:03:3a> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved

60:03:3a>
```

NOTE: The new configuration will not be stored in non-volatile memory until you enter the **save** command. New IP and radio settings will not take effect until you **reset** the CCU.

4. Reboot the CCU for the changes to take effect.

```
60:03:3a> reset
rebooting CCU ...
```

5. Once the CCU has finished rebooting, log back into the unit and enter the commands shown in bold below to confirm the new IP and radio configurations:

```
WaveRider Communications, Inc. LMS3000
Password: ****

60:03:3a > protocol
CCU in Switched Ethernet Mode

60:03:3a > ip
IP Address: 192.168.10.2 / 24
IP Subnet : 192.168.10.0 ( 255.255.255.0 )
Gateway IP Address: 192.168.10.1

60:03:3a > radio
RF Power: HIGH
Radio Frequency: 9050
60:03:3a >
```

CCU configuration is now complete.

6. Type **`exit`** and press **Enter** to log out of the CCU.

2.5 EUM Configuration

The EUM serves as a bridge, connecting the PC Ethernet port to the airlink.

In the following procedure, you will use the factory configuration of the EUM:

- Ethernet IP address and subnet mask (192.168.10.250 /24)
- Gateway IP address (192.168.10.1 /24)
- Radio frequency (9050)

Figure 3 shows the EUM configuration for the Quick Startup.

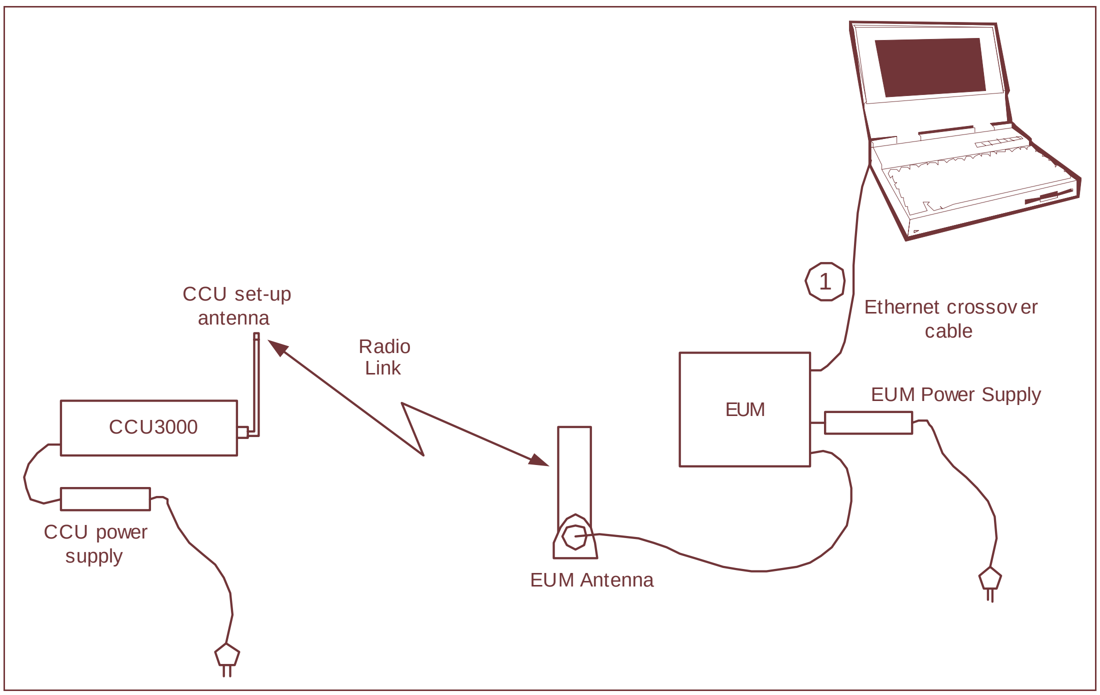


Figure 3 Quick Startup — EUM Configuration

To Configure an EUM

1. Open a connection to the EUM, as described in *Access Interface* on page 221.

   You will see the following prompt:

   ```
   WaveRider Communications, Inc. LMS3000
   Password:
   ```

2. Type the password and press **Enter**.

   NOTE: The factory default password is a carriage return.

You will see the EUM command prompt:

```
60:ff:fe>
```

NOTE: The default prompt on an EUM includes the last five digits of the EUM serial number.

3. Enter the commands shown in bold below to confirm the IP and radio configurations:

```
60:ff:fe> ip
IP Address: 192.168.10.250 / 24
IP Subnet : 192.168.10.0 ( 255.255.255.0 )
Gateway IP Address: 192.168.10.1
60:ff:fe> radio
RF Power: HIGH
Radio Frequency: 9050
60:ff:fe>
```

EUM configuration is now complete.

4. Type **`exit`** and press **Enter** to log out of the EUM.

2.6 Subscriber PC Configuration

While the CCU supports DHCP Relay, this Quick Startup chapter describes a static configuration.

1. On the subscriber PC, open the TCP/IP Properties window. For more information, refer to *To Configure PC Network Settings (Windows XP Operating System)* on page 226.
2. Configure the following TCP/IP properties:
   - IP Address: 192.168.10.251
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.10.1

2.7 Testing CCU–EUM Communications

Once you have completed the configuration of the Quick Startup, you can test communications between the CCU and the EUM by pinging the EUM from the CCU.

To Run a Ping Test Through the EUM Ethernet Port

1. Connect the PC to the EUM Ethernet port, as shown in Figure 4.

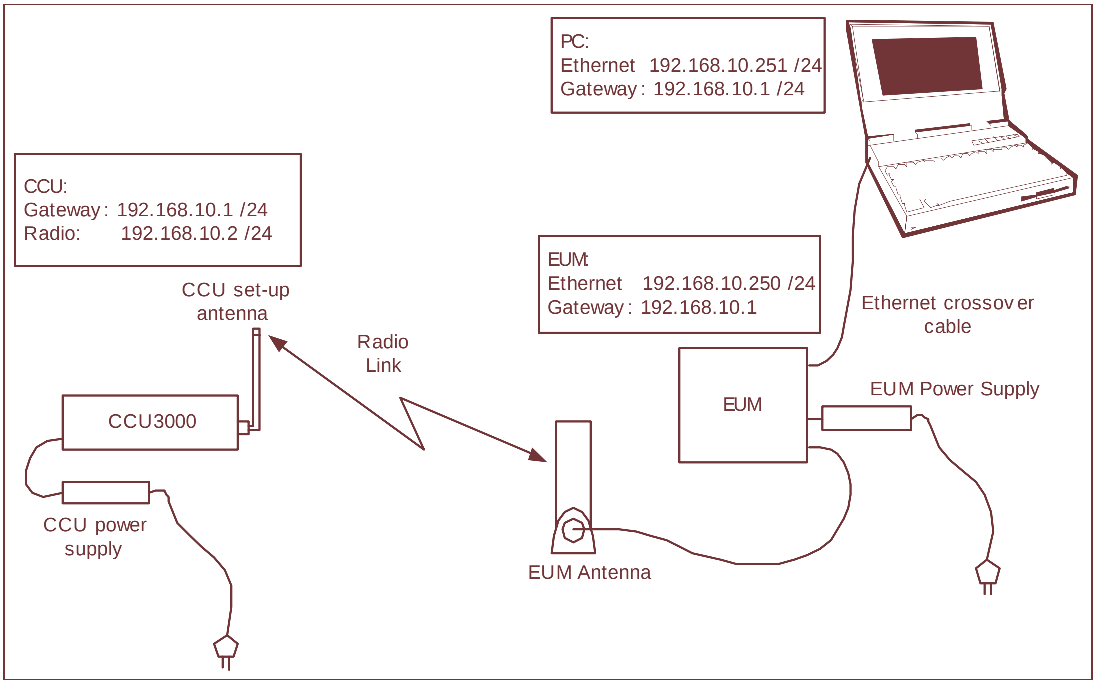


Figure 4 Quick Startup — Ping Test (from EUM Ethernet port)

2. From the PC, progressively ping the PC Ethernet port (192.168.10.251), the EUM (192.168.10.250), the CCU radio (192.168.10.2), and the CCU gateway (192.168.10.2).

```
C:\>ping 192.168.10.251

Pinging 192.168.10.251 with 32 bytes of data:

Reply from 192.168.10.251: bytes=32 time<60ms TTL=128
Reply from 192.168.10.251: bytes=32 time<60ms TTL=128
Reply from 192.168.10.251: bytes=32 time<60ms TTL=128
Reply from 192.168.10.251: bytes=32 time<60ms TTL=128

Ping statistics for 192.168.10.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum =  60ms, Average =  60ms

C:\>ping 192.168.10.250

Pinging 192.168.10.250 with 32 bytes of data:

Reply from 192.168.10.250: bytes=32 time=40ms TTL=63
Reply from 192.168.10.250: bytes=32 time=71ms TTL=63
Reply from 192.168.10.250: bytes=32 time=50ms TTL=63
```

```
Reply from 192.168.10.250: bytes=32 time=60ms TTL=63

Ping statistics for 192.168.10.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum =  71ms, Average =  55ms



C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=2ms TTL=64
Reply from 192.168.10.2: bytes=32 time<10ms TTL=64
Reply from 192.168.10.2: bytes=32 time<10ms TTL=64
Reply from 192.168.10.2: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  2ms, Average =  0ms



C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=81ms TTL=255
Reply from 192.168.10.1: bytes=32 time=73ms TTL=255
Reply from 192.168.10.1: bytes=32 time=105ms TTL=255
Reply from 192.168.10.1: bytes=32 time=83ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 73ms, Maximum =  105ms, Average =  85ms
```

3 Detailed Description

This section describes the technologies and features used in the LMS4000 900 MHz Radio Network.

3.1 LMS4000 Overview

Figure 5 is a high-level schematic of the LMS4000 system, showing the key system components and interfaces.

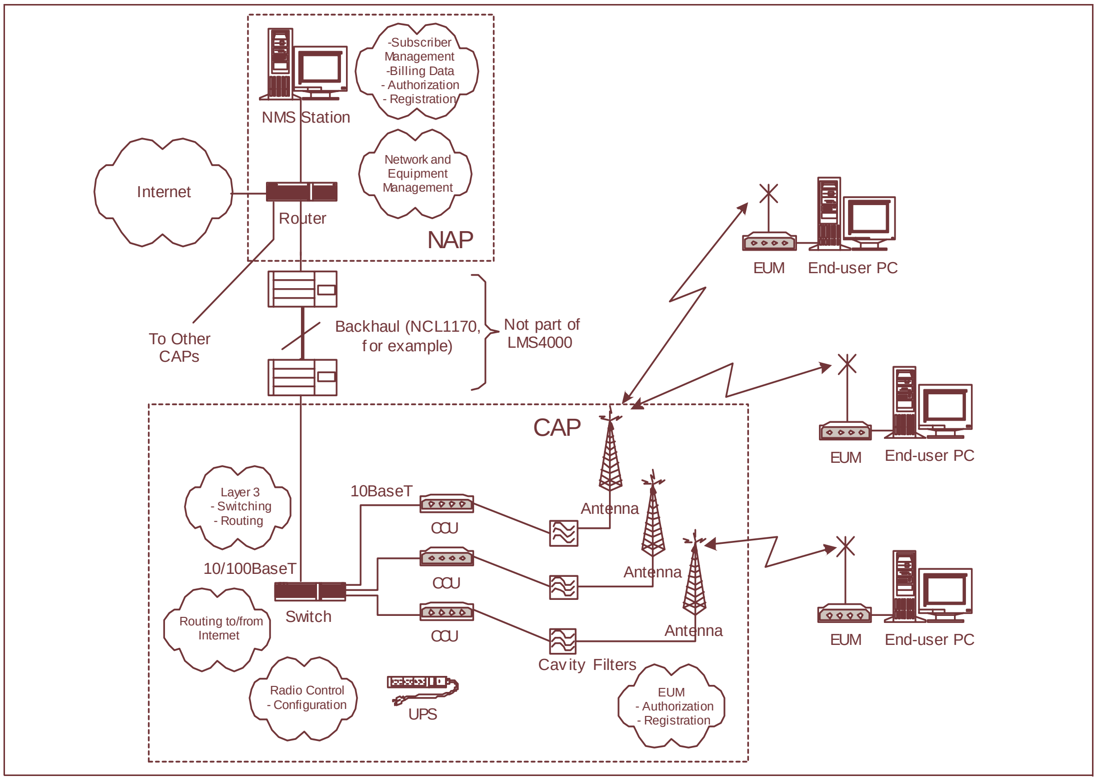


Figure 5 LMS4000 System

As shown, each LMS4000 component is associated with one of three major system entities. Each of these entities is described in the following pages:

- *End-user Modem or Customer-premises Equipment* on page 14
- *Communications Access Point (CAP)* on page 18
- *Network Access Point (NAP)* on page 20

3.1.1 End-user Modem or Customer-premises Equipment

The EUM equipment is installed at the end-user's premises. It provides an interface to the customer's computer or local area network on one side and wireless access to the LMS4000 network on the other.

Key Components

The following components are key to the customer-premises equipment components. Each component is described on the following pages:

- *EUM* on page 15
- *EUM Antenna* on page 15

- *Transmission Line* on page 17
- *Lightning Arrestor* on page 17 (for outdoor antenna installation)

EUM

The EUM, shown in Figure 6, is a wireless modem that connects to the end-user's computer through an Ethernet connection.

The EUM, which acts as a network bridge, receives data from the CCU over the 900 MHz radio link, and then forwards this data to EUM internal processes or to the end-user's computer through the Ethernet port. In the other direction, the EUM forwards data received from the end-user's computer over the radio link to the CCU.

Figure 6 EUM

The EUM functional blocks are the same as those of the CCU and are illustrated in Figure 10.

EUM Antenna

For many EUM installations, you can use an indoor antenna. WaveRider recommends the WaveRider directional antenna with switched-beam diversity. This antenna, shown in Figure 7, performs very well in cases where the radio path to the CCU is obstructed and/or where there is significant multipath. The antenna comes with a mounting bracket and is designed to mount vertically on walls (using drywall screws), or horizontally (on desks, for example, using the suction cups). **The concave surface of the antenna is the front.**

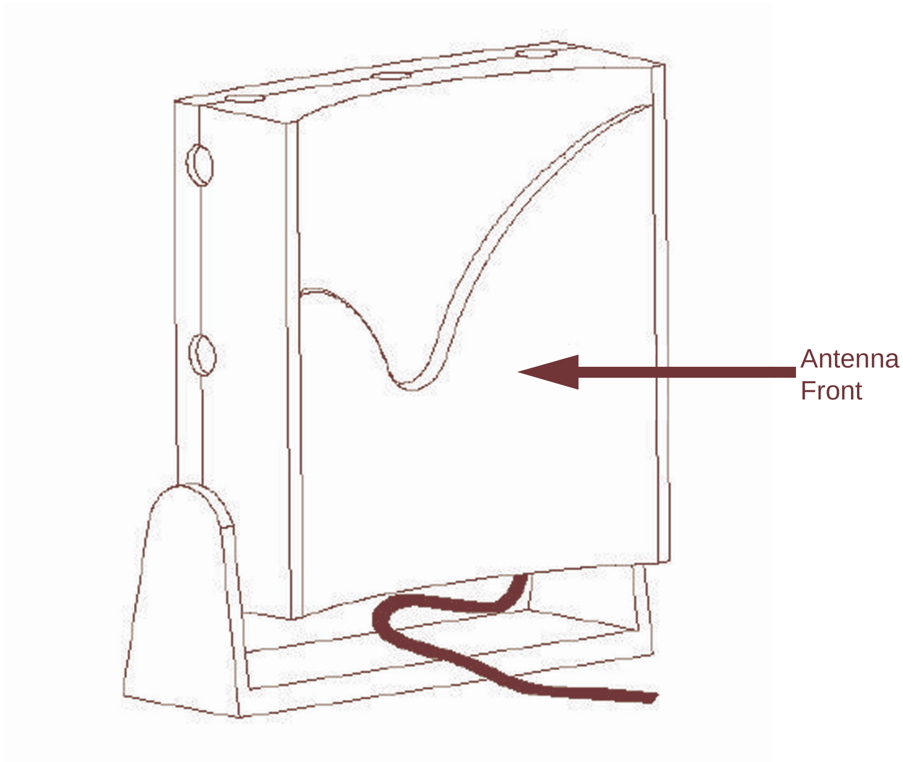


Figure 7 WaveRider Indoor Directional Antenna with Switched-beam Diversity

The WaveRider diversity antenna contains two vertical antenna elements mounted inside and on either side of the antenna housing. The phasing between these elements, which modifies the antenna pattern, is controlled by a DC voltage from the EUM. It produces two patterns, one perpendicular to the face of the antenna, which has a gain of about 6 dBi, and the other, a dual-beam pattern off both sides, offering about 3 dBi gain for each beam. These beam patterns are illustrated in Figure 8.

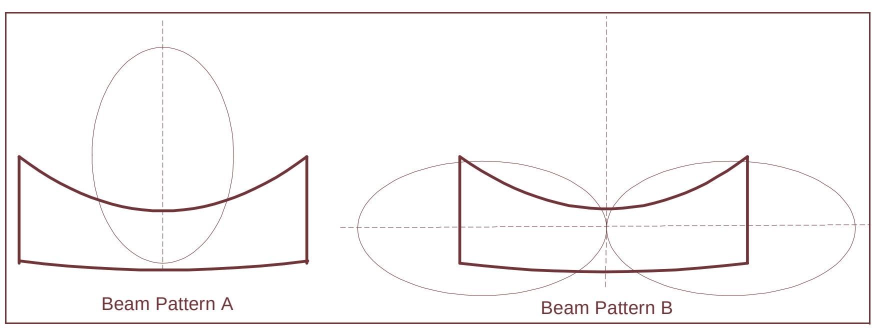


Figure 8 WaveRider Switched-beam Diversity Antenna — Beam Patterns

The EUM samples the signal strength from both antenna patterns during the preamble of every received packet and automatically selects the best signal. When the EUM transmits, it sends on the antenna pattern that was last used to receive a signal. Since most of the traffic comes from the CCU, the EUM samples the signal strength often—typically faster than once every 5 ms.

The end user must position the switched-beam diversity antenna correctly to receive an adequate signal level. The Radio LED on the EUM, described in *Indicators and Connectors* on page 88, can be used to help with the alignment. Since the switched-beam diversity antenna has a good front-to-back ratio, it can be positioned to suppress interference from other wireless devices at the end-user's premises.

Other WaveRider-approved antennas can be used at EUM locations that require outdoor antennas. A professional installer is required to install outdoor EUM antennas to ensure the antenna system is properly installed with lightning protection and consistent with FCC and Industry Canada guidelines, which are outlined in Appendix F on page 229.

Transmission Line

If the WaveRider diversity antenna is used, it comes equipped with RF cables and connectors. The connector is a proprietary WaveRider connector, which is mandated by the FCC requirement that the connectors used in ISM band products that are not professionally installed must be unique, or at least not readily available. If an alternate indoor or outdoor antenna is used, the installer must obtain an RF jumper cable to connect the antenna cable to the EUM. These jumper cables can be obtained from WaveRider.

Lightning Arrestor

A lightning arrestor is required at the EUM only if an outdoor antenna is used.

Ethernet Port

The EUM has one 10BaseT Ethernet port.

Any DC voltage applied to the Ethernet port may damage the EUM, the Ethernet cable, and/or network gear. The EUM is not a Power-over-Ethernet device.

3.1.2 Communications Access Point (CAP)

The CAP is the collection and distribution point for data travelling to and from EUMs. In the EUM-to-network direction, the CAP aggregates data from the radio channels into a single data stream, which is passed either directly or over a backhaul facility to the Network Access Point.

In the Internet-to-EUM direction, the CAP receives data from the Network Access Point and distributes this data to the appropriate radio channels for transmission to the EUMs over the 900 MHz radio link.

Key Components

The following key components of the Communication Access Point are described in detail on the following pages:

- *CCU* on page 18
- *Cavity Filters* on page 20
- *Lightning Arrestors* on page 20
- *Transmission Line* on page 20
- *Antenna* on page 20
- *Ethernet Port* on page 20

CCU

The CCU, shown in Figure 9, is the wireless access point for up to 300 end-user modems. The functional blocks of the CCU are illustrated in Figure 10.

Figure 9 CCU

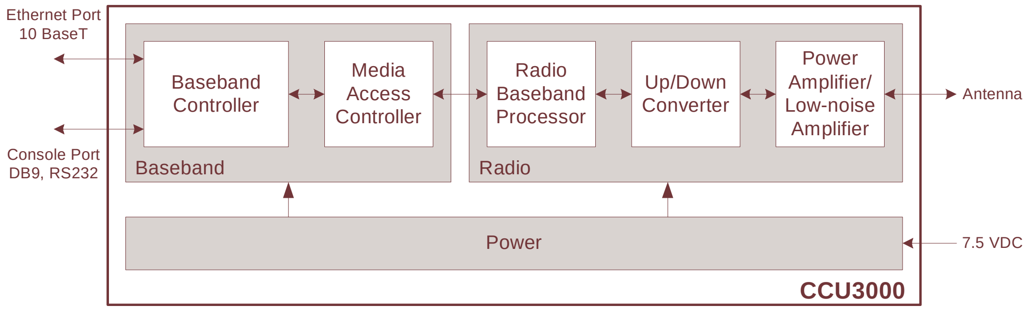


Figure 10 CCU Functional Blocks

The CCU forwards packets received from the CCU radio port

- to internal CCU processes,
- through the CCU Ethernet port to any router on the Ethernet network, such as the Network Access Point, or
- back out the radio port to other EUMs (EUM-to-EUM packets).

The CCU forwards packets that are received from the Network Access Point through the Ethernet port

- to internal CCU processes, or
- through the radio port to the destination EUM.

The CCU can be installed in a standalone configuration, or in a CCU shelf, as shown in Figure 11, with other operating CCUs. The CCU is powered by an AC/DC power supply, which can also stand alone or be installed in the CCU shelf. The CCU operates independently of other CCUs and can be swapped out without interrupting the operation of other CCUs.

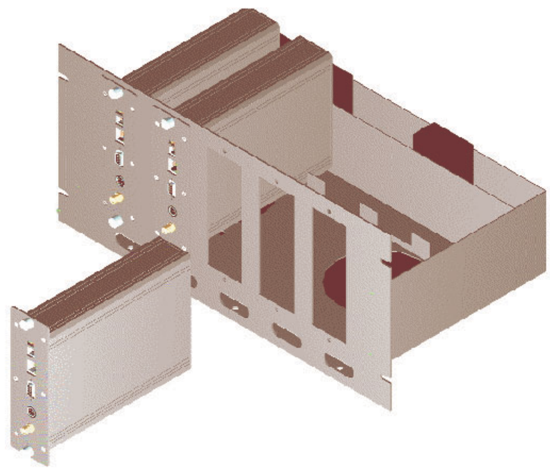


Figure 11 CCU Shelf

Up to four operating CCUs can be installed at the same CAP, each with its own cavity filter, lightning protector, transmission line, and antenna.

The CCU comes with a setup antenna, which can be used during CCU configuration and test, prior to deployment.

Cavity Filters

WaveRider recommends the use of cavity filters with all CCUs and is mandatory if co-located with other CCUs. Cavity filters help to isolate the CCU from inband interferers, such as co-located CCUs or non-WaveRider ISM band equipment, as well as out-of-band interferers, such as cellular base stations and paging transmitters.

Lightning Arrestors

Since the CCU antenna is mounted outdoors, lightning arrestors are required with all CCU installations. Lightning arrestors divert most of the energy from a lightning strike away from the RF transmission line and equipment, to a bonded ground point. The lightning arrestor is installed in series with the RF transmission line, as close as possible to the point where the transmission line enters the building.

Transmission Line

A good quality RF transmission line should always be used to connect the CCU to the antenna. “Good quality RF transmission line” means one that is weather resistant and UV-protected, and that has low attenuation characteristics. All connectors in the transmission line should be wrapped to prevent water penetration. Connecting the CCU to the transmission line requires RF jumper cables, available from WaveRider.

Antenna

Each active CCU requires its own antenna. Antennas can be omnidirectional or have a sectored beam pattern (for example, 180, 120, or 90 degrees). The choice of antenna is based on site and RF engineering considerations, and FCC and Industry Canada guidelines, which are summarized in Appendix F on page 229.

Ethernet Port

The CCU has one 10BaseT Ethernet port.

An Ethernet switch is required at the CAP if it is provisioned with more than one CCU, or to interface with certain types of backhaul equipment.

Any DC voltage applied to the Ethernet port may damage the CCU, the Ethernet cable, and/or network gear. The CCU is not a Power-over-Ethernet device.

3.1.3 Network Access Point (NAP)

The NAP provides the Internet connection point for one or more CAPs. An LMS4000 system can have more than one NAP. The number of NAPs depends on the geographical layout of the LMS4000 system and the location of available Internet access points. A single NAP can provide Internet connection for one CAP, or several CAPs, each either co-located with the NAP or connected to the NAP over backhaul facilities.The following sections discuss the operation of the LMS4000 900 MHz Radio Network, of which the CCU and EUM are the key components.

3.2 LMS4000 Transmission Concept

This section explains the transmission concept for the following CCU protocol modes:

- *Routed Mode* on page 21
- *Switched Ethernet Mode* on page 22
- *Through Only Mode* on page 23

3.2.1 Routed Mode

In Routed mode, the LMS4000 900 MHz Radio Network can be thought of as an Ethernet switch with a built-in router, as shown in Figure 12.

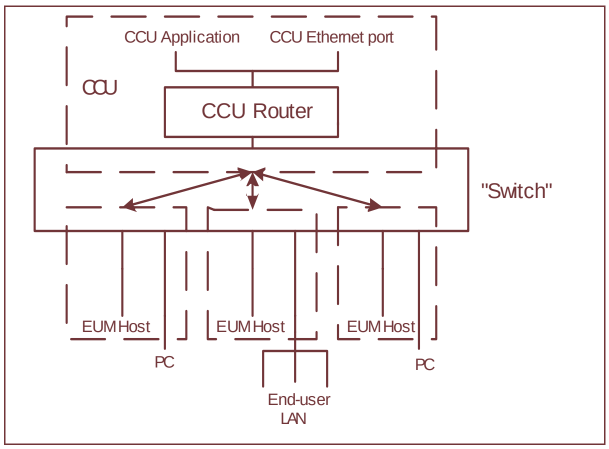


Figure 12 LMS4000 Transmission Concept - Routed Mode

In the above diagram, the “switch” consists of the CCU and EUM physical, MAC, and IP bridging layers, and the 900 MHz link between them. IP packets originating from any host in the radio subnet (EUM or PC, for example), which are destined for a host that is also in the radio subnet, are “switched” by the CCU directly to that host. IP packets originating from any host in the radio subnet, which are destined for a host outside the radio subnet, are “switched” to the CCU router for routing to the destination host.

IP packets coming into the CCU Ethernet port, which are destined to a host in the radio subnet, are routed to the “switch” and “switched” to the host.

In the Routed mode, the Ethernet interface of the CCU is on a different IP subnet than the “radio” subnet. The latter connects the CCU radio interface, and Ethernet interfaces of all EUMs & subscribers PCs.

3.2.2 Switched Ethernet Mode

Figure 13 shows the LMS4000 900 MHz Radio Network transmission concept for Switched Ethernet mode.

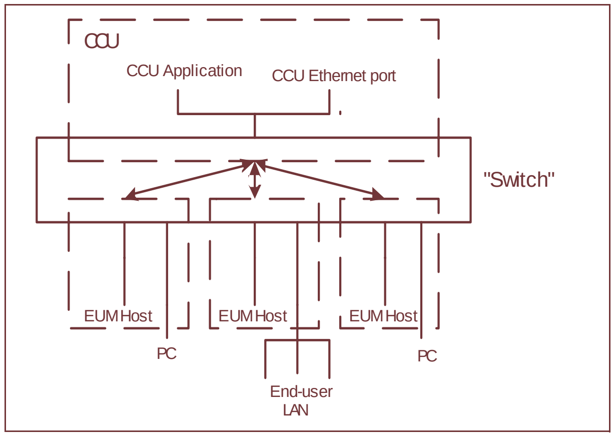


Figure 13 LMS4000 Transmission Concept - Switched Ethernet Mode

In Switched Ethernet mode, the Ethernet and radio interfaces of the CCU belong to the same Ethernet domain, with a switch between, enabling any number of IP subnets to be supported on either or both sides of the CCU. This flexibility allows placing all subscribers on public IP addresses and “hiding” the radio network from the subscribers, without using public IP addresses for the EUMs and CCUs. A different subnet may be set up on the Ethernet side of the CCU to enable ISPs to manage and monitor all devices (CCU and EUMs) on the radio network. Figure 14 illustrates the above configuration.

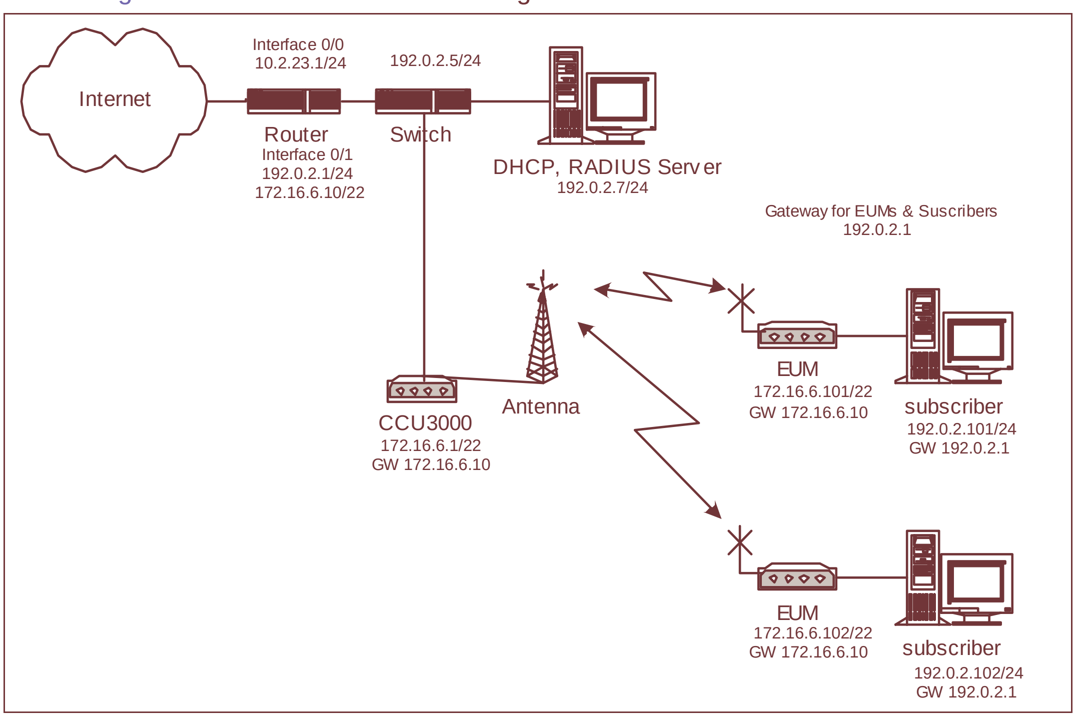


Figure 14 Switched Ethernet Mode with Multiple Subnets

The network configuration in Figure 15 illustrates Switched Ethernet mode where the CCU supports a single IP subnet on the radio interface, all EUMs and subscribers are on the same subnet.

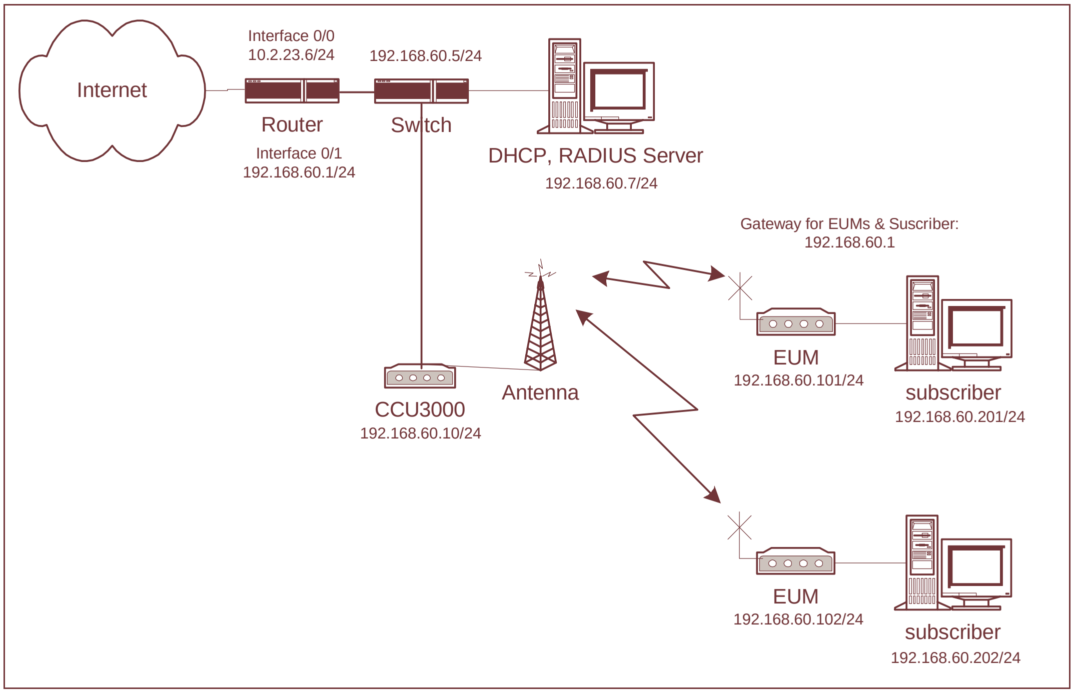


Figure 15 Switched Ethernet Mode with a Single Subnet

Switched Ethernet mode supports IP, ARP and PPPoE packets. The IP forwarding function of the CCU is disabled, preventing routing through the CCU.

> **NOTE:** PPPoE incurs more overhead than IP directly over Ethernet, leading to about 2% slower downloads.

3.2.3 Through Only Mode

Through Only mode on a CCU behaves similarly to Switched Ethernet mode except that all network traffic (except traffic to the CCU) is constrained to flow only from the CCU's radio interface to its Ethernet interface or vice versa. For EUMs on the same CCU to communicate, you must make provisions externally to send the packets back through the Ethernet link, using either the PPPoE server or an associated router. In addition, the IP forwarding function of the CCU is disabled, preventing routing through the CCU.

> **NOTE:** Through Only mode supports the network configurations described above.

> **NOTE:** Through Only mode is a special case intended for PPPoE-only support. Contact WaveRider Technical Support for details.

3.3 Basic Data Transmission

This section describes how an EUM registers, and once it is registered, how data traffic flows from the Internet to the end-user PC and from the end-user PC to the Internet. The process in both directions involves CCU and EUM data tables, which are described in more detail in Appendix G on page 231. The description of basic data transmission is divided into the following sections:

3.3.1 EUM Registration

An EUM must register with the CCU before user traffic can pass between the LMS4000 900 MHz Radio Network and the end-user. The heart of EUM registration is the Authorization Table, discussed in *Authorization Table (CCU only)* on page 239. If your LMS4000 system includes a RADIUS server, it can manage EUM registration by maintaining the Authorization Table. The CCU restricts the maximum number of EUMs that can be registered at any one time to 300.

Before installing an EUM, you must configure a grade of service for that EUM, which can be done one of three ways:

- Add an entry to the Authorization Table (see *Authorization Table (CCU only)* on page 239).
- Add an entry in a RADIUS database and manage the Authorization Table with a RADIUS server.
- Use the default grade of service.

EUM Registration Process

The following steps describe the EUM registration process:

1. On power up, the EUM sends a Registration Request message containing its EUMID to the CCU.
2. The CCU looks for an Authorization Table entry for the EUM to obtain a grade of service. If there is no entry, it obtains the default grade of service.

3. If the grade of service is not DENIED, the CCU adds the EUM to the Registration Table, described in *Registration Table (CCU only)* on page 240 and sends a Registration Response message to the EUM. Data communications are then enabled. However, if the Registration Table on the CCU is already full, the CCU treats it as DENIED.
4. If the grade of service is DENIED, the CCU sends a Deregistration Request to the EUM and data communications are disabled. The EUM continues to send Registration Requests to the CCU approximately every 10 minutes, starting again at step 1.
5. If RADIUS authorization is enabled and there is no entry for the EUM in the Authorization Table, the CCU queries the RADIUS server for the EUM's grade of service. When the RADIUS server responds, an entry is made in the Authorization Table. The Registration Table and the grade of service offered to the EUM are then updated. An Access Accept message contains one of the non-DENIED grades of service, while an Access Reject message is equivalent to a DENIED grade of service.
6. If the previous grade of service was not DENIED and an Access Reject is received, the EUM is de-registered immediately, removed from the Registration Table, and data communication is disabled.
7. If the previous grade of service was DENIED and an Access Accept is received, the EUM is directed to attempt registration again immediately, which will be successful due to the new entry in the Authorization Table.
8. On a periodic basis, for each Authorization Table entry created by a RADIUS response, the CCU queries the RADIUS server for the EUM's grade of service. If the response is different from the previous response, the Authorization Table, Registration Table and grade of service offered to the EUM are updated. If the RADIUS server does not respond over the course of three query periods, the EUM reverts to the default grade of service.
9. If at some later time, the EUM does not respond to messages from the CCU, the CCU sends a Deregistration Request to the EUM and removes the EUM from the Registration Table. The EUM must then repeat the registration process to obtain access.
10. If there has been no traffic to or from the EUM for more than 12 hours, the CCU removes the EUM from the Registration Table without sending a Deregistration Request. The EUM must then repeat the registration process to obtain access.

NOTE: If a RADIUS-authorized EUM power cycles, the EUM re-registers using the existing entry in the Authorization Table, without generating an immediate RADIUS query.

NOTE: An authorization entry made through the CLI is marked as “static” and is not updated through RADIUS.

3.3.2 Internet to End-user Computer Data Transmission using Routed Mode

1. Internet traffic comes through the gateway router, and possibly through backhaul and Ethernet switches, to the CCU Ethernet port.
2. The CCU receives a packet through the CCU Ethernet port and checks the TCP or UDP port number. If the port number appears in the CCU Port Filter Table, described in *Port Filter Table (CCU and EUM)* on page 231, the packet is discarded.
3. The CCU reads the destination MAC address. If the destination MAC address is the same as either the CCU Radio or Ethernet MAC address, the packet is sent to the CCU application.
4. The CCU checks the Routing Table, described in *Routing Table (CCU and EUM)* on page 232. If the route to the destination is through the CCU Ethernet port, then the packet is discarded, since it is not destined for a host in the CCU's radio subnet.
5. If the route to the destination is through the CCU Radio Port, then the CCU obtains the destination Ethernet MAC address from the ARP Table, described in *ARP Table (CCU and EUM)* on page 236. If the destination is not listed in the ARP Table, the CCU obtains its MAC address by issuing an ARP query. Once it gets the MAC address, it adds the entry to the ARP Table.
6. Using the destination Ethernet MAC address, the CCU obtains the EUM ID from the Address Translation Table, described in *Address Translation Table (CCU only)* on page 238.
7. Using the EUM ID, the CCU obtains the EUM grade of service from the Registration Table, described in *Registration Table (CCU only)* on page 240.
8. The packet is then transmitted through the Polling MAC and radio interface to the EUM.
9. The EUM receives the packet through the EUM radio port and checks the port number. If the port number appears in the EUM Port Filter Table, the packet is discarded.
10. If the port number does not appear in the EUM Port Filter Table, the EUM checks the destination MAC address. If the MAC address is the EUM MAC address, then the packet is forwarded to the EUM application; otherwise, the packet is sent out through the Ethernet port to the end user's equipment.

3.3.3 End-user Computer to Internet Data Transmission using Routed Mode

1. The EUM receives packets from the end-user's equipment through the Ethernet port.
2. The EUM checks the port number. If the port is listed in the EUM Port Filter Table, the packet is discarded.
3. If it is not already in the list, the EUM adds the source Ethernet address to the Bridge Table, described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242. The EUM determines whether or not the source is entitled to air access, based on the Bridge Table.
4. If the source is not entitled to air access, the packet is discarded.

5. The EUM checks the destination MAC address. If the destination MAC address appears in the Bridge Table, meaning the destination is on the Ethernet side, the packet is discarded.
6. If the destination MAC address is the same as the EUM MAC address, then the packet is forwarded to the EUM application; otherwise, it is forwarded through the polling MAC and radio link to the CCU.
7. The CCU receives the packet through the CCU radio port. The CCU either updates or adds the Ethernet address to the Address Table.
8. The CCU checks the port number. If the port number appears in the CCU Port Filter Table, the packet is discarded.
9. The CCU checks the destination MAC address. If the destination MAC address is not in the Address Table, the packet is sent to the CCU router application.
10. If the MAC address is the same as either the CCU radio or Ethernet MAC address, the packet is forwarded to the CCU application; otherwise, the CCU gets the appropriate gateway IP address from the Routing Table and the gateway MAC address from the ARP Table, and then sends the packet to the gateway (most likely the NAP router) through the Ethernet port.

NOTE: The CCU and EUM pass only IP, ARP, and PPPoE packets. All other packets are discarded so non-Ethernet packets, such as IPX/SPX, are not passed over the radio link.

3.3.4 Internet to End-user Computer Data Transmission using Switched Ethernet Mode or Through Only Mode

In Switched Ethernet and Through Only modes, the CCU has only one IP address for both the Ethernet and the radio interface.

1. Internet traffic comes through the gateway router, and possibly through backhaul and Ethernet switches, to the CCU Ethernet port.
2. The CCU receives a packet through the CCU Ethernet port and checks the TCP or UDP port number. If the port number appears in the CCU Port Filter Table, described in *Port Filter Table (CCU and EUM)* on page 231, the packet is discarded.
3. If it is not already in the list, the CCU adds the source Ethernet address to the Bridge Table, described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242.
4. The CCU checks the Bridge Table. If the destination address is in the Bridge table, then the packet is discarded since it is not destined for a host in the CCU's radio subnet.
5. Using the destination Ethernet MAC address, the CCU obtains the EUM ID from the Address Translation Table, described in *Address Translation Table (CCU only)* on page 238.
6. Using the EUM ID, the CCU obtains the EUM grade of service from the Registration Table, described in *Registration Table (CCU only)* on page 240.

7. The packet is then transmitted through the Polling MAC and radio interface to the EUM.

8. The EUM receives the packet through the EUM radio port and checks the port number. If the port number appears in the EUM Port Filter Table, the packet is discarded.

9. If the path to the destination is through the CCU radio port, then the CCU obtains the destination Ethernet MAC address from the ARP Table, described in *ARP Table (CCU and EUM)* on page 236. If the destination is not listed in the ARP Table, the CCU obtains its MAC address by issuing an ARP query. Once it receives the MAC address, it adds the entry to the ARP Table.

10. If the port number does not appear in the EUM Port Filter Table, the EUM checks the destination MAC address. If the MAC address is the EUM MAC address, then the packet is forwarded to the EUM application; otherwise, the packet is sent out through the Ethernet port to the end user’s equipment.

3.3.5 End-user Computer to Internet Data Transmission using Switched Ethernet Mode

1. The EUM receives packets from the end-user’s equipment through the Ethernet port.

2. The EUM checks the port number. If the port is listed in the EUM Port Filter Table, the packet is discarded.

3. If it is not already in the list, the EUM adds the source Ethernet address to the Bridge Table, described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242. The EUM determines whether or not the source is entitled to air access, based on the Bridge Table.

4. If the source is not entitled to air access, the packet is discarded.

5. The EUM checks the destination MAC address. If the destination MAC address appears in the Bridge Table, meaning the destination is on the Ethernet side, the packet is discarded.

6. If the destination MAC address is the same as the EUM MAC address, then the packet is forwarded to the EUM application; otherwise, it is forwarded through the polling MAC and radio link to the CCU.

7. The CCU receives the packet through the CCU radio port. The CCU either updates or adds the Ethernet address to the Address Table.

8. The CCU checks the port number. If the port number appears in the CCU Port Filter Table, the packet is discarded.

9. The CCU checks the destination MAC address. If the destination MAC address is in the Address Table, the packet is sent to the associated EUM.

10. If the destination MAC address is the same as either the CCU radio or Ethernet MAC address, the packet is forwarded to the CCU application.

11. The CCU checks whether the destination MAC address is in the bridging table. If it is, the packet is transmitted out the Ethernet port; otherwise, the packet is broadcast out the radio and sent out the Ethernet port.

3.3.6 End-user Computer to Internet Data Transmission using Through Only Mode

1. The EUM receives packets from the end-user's equipment through the Ethernet port.
2. The EUM checks the port number. If the port is listed in the EUM Port Filter Table, the packet is discarded.
3. If it is not already in the list, the EUM adds the source Ethernet address to the Bridge Table, described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242. The EUM determines whether or not the source is entitled to air access, based on the Bridge Table.
4. If the source is not entitled to air access, the packet is discarded.
5. The EUM checks the destination MAC address. If the destination MAC address appears in the Bridge Table, meaning the destination is on the Ethernet side, the packet is discarded.
6. If the destination MAC address is the same as the EUM MAC address, then the packet is forwarded to the EUM application; otherwise, it is forwarded through the polling MAC and radio link to the CCU.
7. The CCU receives the packet through the CCU radio port. The CCU either updates or adds the Ethernet address to the Address Table.
8. The CCU checks the port number. If the port number appears in the CCU Port Filter Table, the packet is discarded.
9. If the destination MAC address is the same as either the CCU radio or Ethernet MAC address, the packet is forwarded to the CCU application; otherwise, the packet is sent out the Ethernet port.

NOTE: Unlike Switched Ethernet mode, the Bridge Table is not checked. Also, broadcast packets are not sent to the radio interface.

3.3.7 RADIUS Authorization

The Remote Authentication Dial-In User Service (RADIUS) simplifies administration of large networks.

RADIUS support, through a RADIUS Client in the CCU, enables a remote RADIUS Server to authorize the WaveRider Grade of Service settings for EUMs on the radio network. Once the RADIUS Client is configured and enabled on the CCU, the CCU queries the RADIUS server upon EUM registration and at subsequent operator-defined intervals. Any GOS change entered in the RADIUS database takes effect after the next query. RADIUS is essentially an access control protocol enabling you to create a central list of devices that can access the radio network.

Figure 16 depicts the typical exchange of RADIUS messages between the CCU RADIUS Client and the remote RADIUS Server.

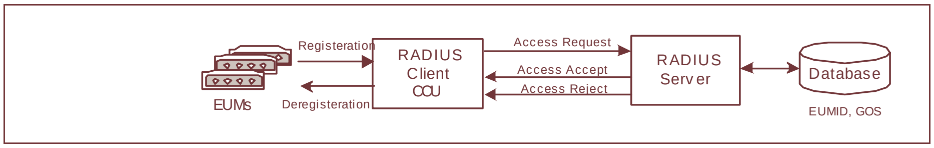


Figure 16 RADIUS Authorization

1. The CCU queries the RADIUS server with an Access Request message, which contains an EUM ID and RADIUS client (CCU) IP address.
2. After receiving the Access Request message, the RADIUS server authenticates the CCU as a recognized RADIUS client and then validates the received EUM ID against the database entries.
3. If the EUM is allowed, the RADIUS server returns an Access Accept message, containing the extracted GOS value from the database, to the CCU. The CCU then updates the GOS entry in the Authorization table for the requested EUM.

   NOTE: If the GOS is not present in the Access Accept message, the current default GOS value will be used. The CCU will not make an entry in the Authorization table, and it will not send out any more Access Request messages for the EUM.

4. If the RADIUS Server responds with an Access Reject message (for example, if there is no entry for that EUM in the database), the CCU marks the EUM as “DENIED” in the Authorization table.

   The RADIUS database contains the EUM IDs and the desired GOS value.

You may make static authorization entries in the CCU through the CLI. Static entries override any RADIUS replies and are marked “STATIC” in the Authorization table.

3.3.8 RADIUS Accounting

The RADIUS client on the CCU provides support for RADIUS accounting. RADIUS accounting packets are sent to the remote RADIUS server on a periodic basis and on special events for each EUM.

Figure 17 illustrates the RADIUS messages that are sent to the RADIUS server.

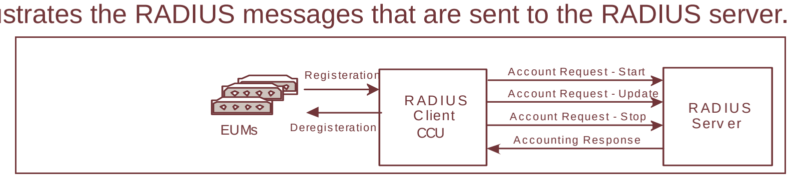


Figure 17 RADIUS Accounting

1. For each EUM authorized through RADIUS, the CCU sends an “Account Request – Start” message upon registration.
2. Subsequently, the RADIUS server sends an “Account Request – Update” message at fixed intervals, with updates of Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets.

3. On EUM deregistration, the RADIUS server sends an “Account Request – Stop” message with the final counts.
4. The RADIUS server sends an Accounting Response message to acknowledge any of the three Accounting Requests.

3.4 LMS4000 Protocol Stacks

The LMS4000 900 MHz Radio Network is an IP (layer 3 for Routed mode; layer 2 for Switched Ethernet and Through Only modes) network that provides connectivity from the end-user’s computer to the Internet.

Figure 18 and Figure 19 show the protocol stacks through which an IP packet traverses as it travels between the end-user’s computer, shown on the left, and the Internet, shown on the right

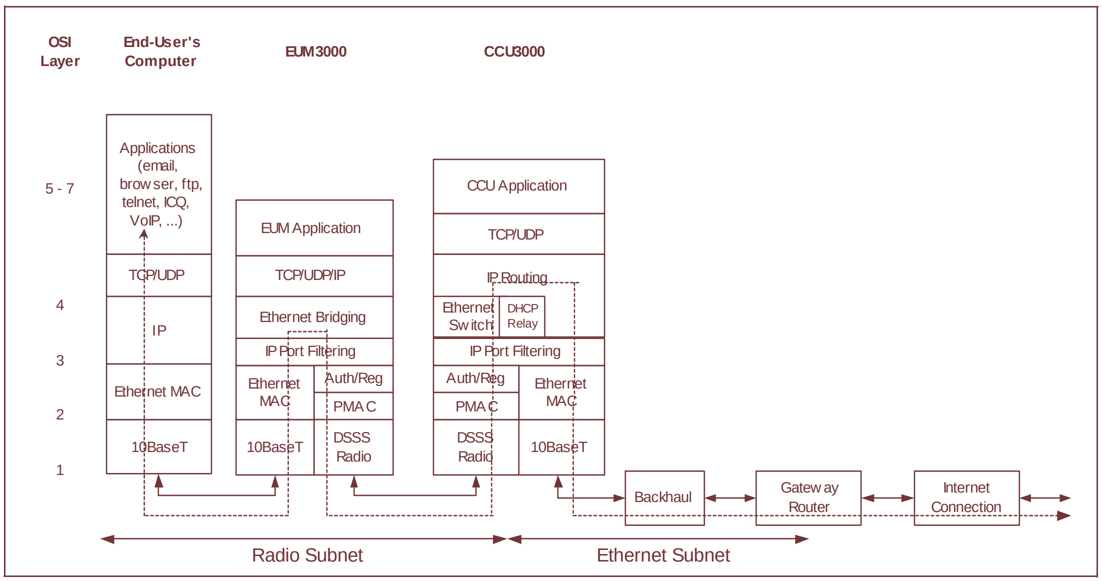


Figure 18 Routed Mode

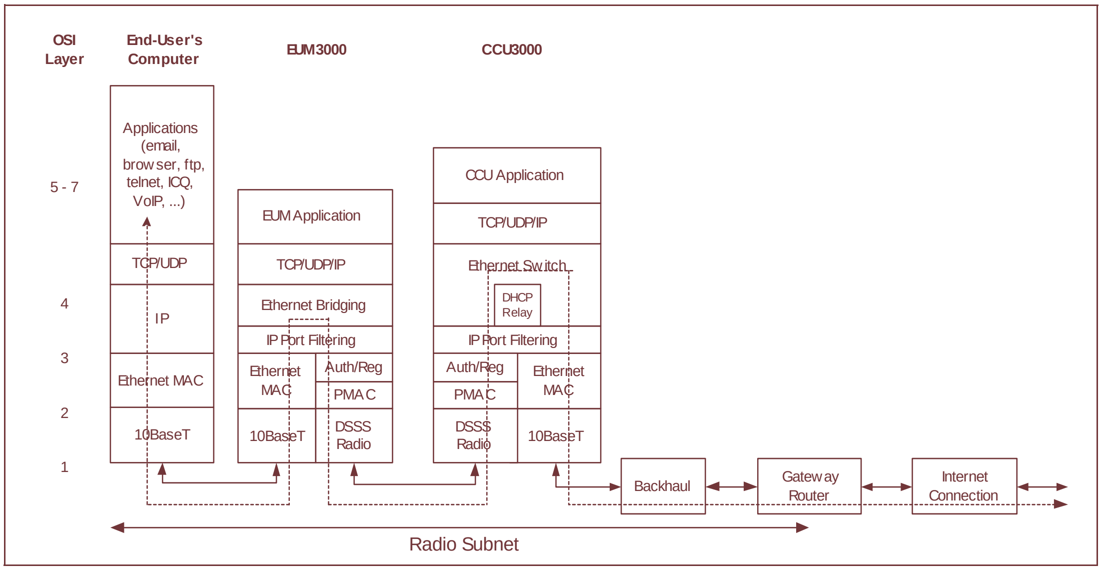


Figure 19 Switched Ethernet Mode and Through Only Mode

In routed mode, normal end user traffic is Routed in the CCU between the Ethernet and radio subnets.

In Switched Ethernet mode, the LMS4000 acts as an Ethernet switch, with the CCU Ethernet port, CCU application, each EUM application, and each EUM Ethernet port acting as a switch port.

In Through Only mode, packets received from an EUM are passed to the CCU application and/or the Ethernet port, but not to another EUM.

3.4.1 Addressing of Packets

Figure 21 shows how the source and destination MAC and IP addresses are sent in packets travelling between the end-user's PC and the Internet network servers.

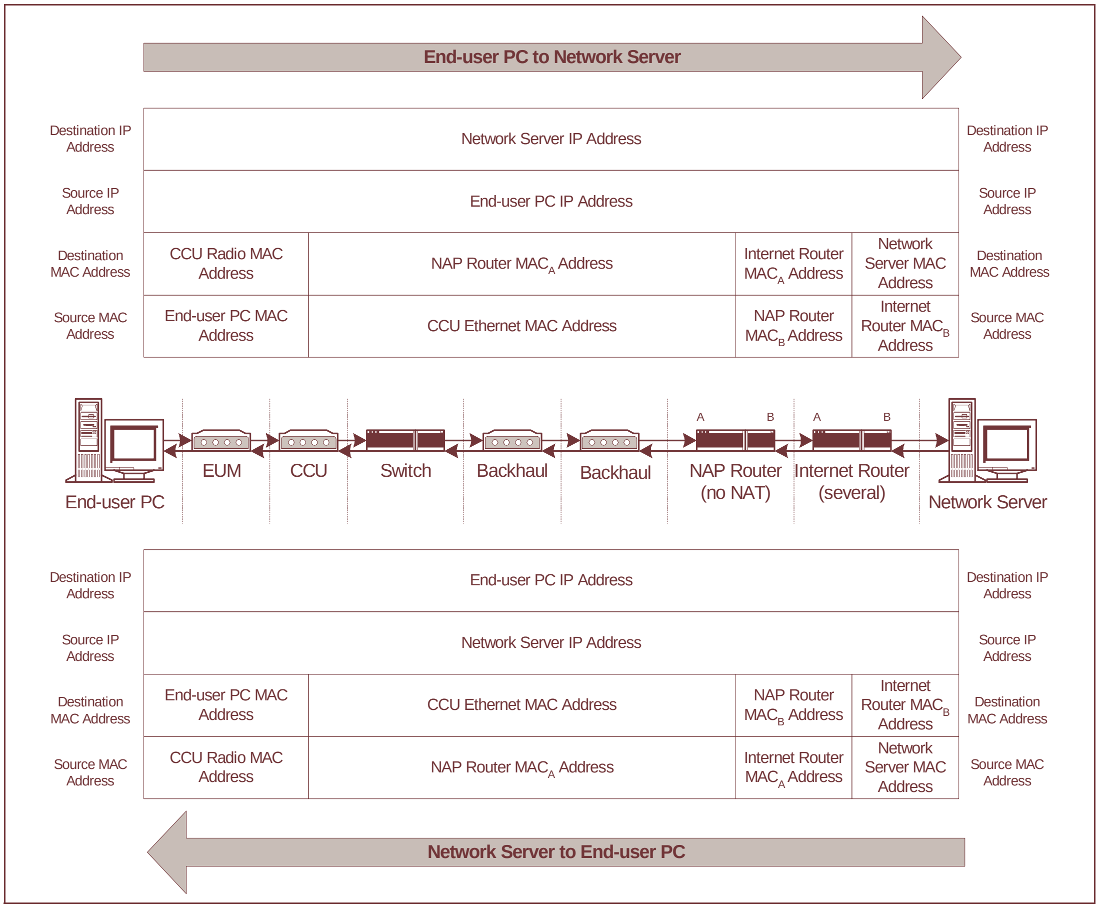


Figure 20 Addressing of Packets—Routed Mode

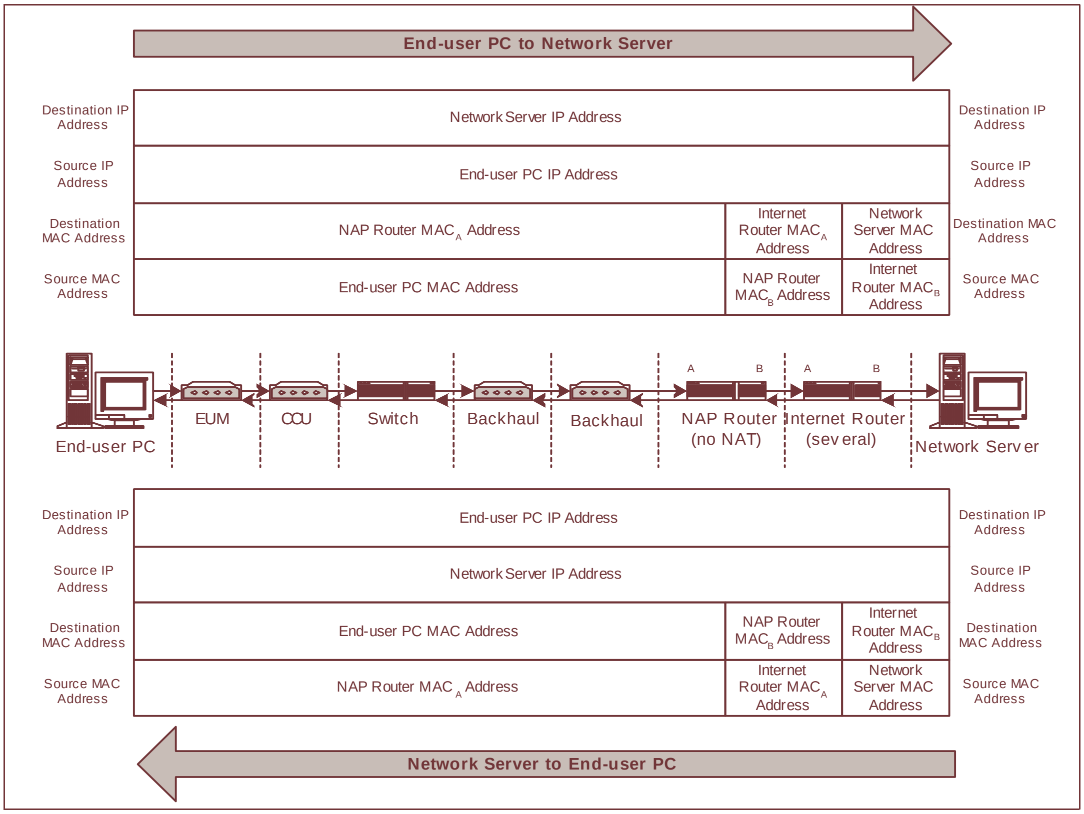


Figure 21 Addressing of Packets—Switched Ethernet Mode

As shown in Figure 21, if NAT is not enabled in the NAP Router, then the source and destination IP addresses are maintained throughout the route between the end-user PC and network servers. The source and destination MAC addresses, however, change whenever the packet is passed through a router. This change of MAC addresses also takes place in the CCU router application.

3.5 CCU–EUM Interface Physical Layer (DSSS Radio)

This section provides a detailed technical description of following aspects of the CCU–EUM Interface Physical Layer (DSSS Radio):

3.5.1 Frequency Band

The LMS4000 900 MHz Radio Network operates in the 902-928 MHz Industry, Scientific, and Medical (ISM) frequency band.

3.5.2 Channel Bandwidth

The channel bandwidth is 6 MHz. This channel bandwidth is used to determine the lowest and highest allowable channel in the band. As illustrated in Figure 22, the center frequency of the lowest and highest channels have to be set such that the signal power that falls in the bands adjacent to the ISM band does not exceed FCC and Industry Canada limits.

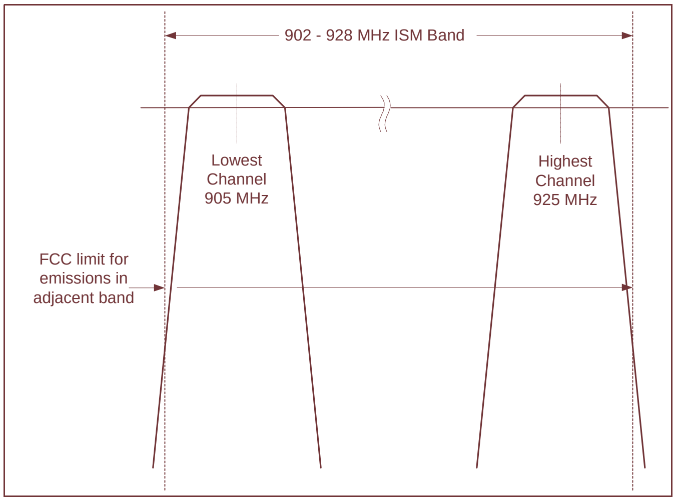


Figure 22 Determination of Lowest and Highest Channel

The channel bandwidth also determines the minimum adjacent channel spacing for co-located CCUs.

3.5.3 Channels

There are 101 channels in the band, set in 0.2 MHz increments:

Table 1 LMS4000 900MHz Radio Network Channelization

Channel	Center Frequency
Lowest channel	905.0 MHz
...	905.2 MHz
...	905.4 MHz
...	...
...	924.8 MHz
Highest channel	925.0 MHz

3.5.4 Modulation

The CCU-EUM radio channel is based on DSSS (Direct-Sequence Spread Spectrum) signals, modulated with CCK and Barker-coded BPSK and QPSK, similar to that defined in IEEE 802.11 for the 2.4 GHz ISM band.

DSSS offers the following advantages:

- **Reduced power spectral density:** Spreading over a wider bandwidth reduces the spectral density (power per Hz of bandwidth) of the transmitted signal, allowing simultaneous operation of many spread-spectrum systems in the same frequency band and geographic area. The reduced spectral density also allows you to meet the regulatory emissions requirements in the ISM frequency bands.
- **Transmission security:** It is technologically more difficult to recover (or interfere with) spread-spectrum signals than it is to recover conventional narrowband signals.
- **Interference suppression:** The same mechanism that de-spreads the desired signal in the receiver, spreads undesired signals, which then appear to the receiver as lower levels of RF noise. This effect is illustrated in Figure 23.

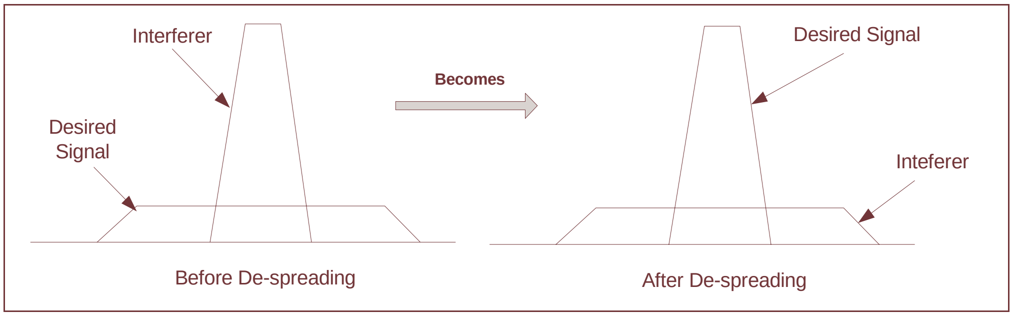


Figure 23 Effect of Despreading

3.5.5 Data Rate

The raw channel bit rate is 2.75 Mbps. The maximum data rate presented to the MAC layer is 2.4 Mbps, which translates to a peak FTP rate of about 2 Mbps.

3.5.6 Co-located Channels

A maximum of four orthogonal (nonoverlapping) channels can be provisioned at a single CAP but WaveRider recommends a maximum of three. To ensure adequate isolation between channels, a minimum co-channel spacing of 6.6 MHz is recommended, as is the use of channel filters and a properly engineered antenna system. A possible frequency set for a three-channel CAP is

- 905.0 MHz
- 915.0 MHz
- 925.0 MHz

A separate CCU, channel filter, transmission line, lightning protector, and antenna are required for each of the orthogonal channels.

3.5.7 Duplexing

The radio channel uses Time Division Duplexing (TDD), which means that the CCU or EUM is in either receive or transmit mode, but does not transmit and receive at the same time.

3.5.8 Transmit Power

The maximum transmit power (HIGH power setting) of the CCU and EUM is +26 dBm, measured at the unit's RF connector. It does not include gains and losses from antennas, transmission lines, and lightning arrestors, all of which affect the ERP (Effective Radiated Power) from the CAP or customer's premise. Refer to Appendix F on page 229 for a discussion of related FCC and Industry Canada guidelines.

The CCU and EUM transmit power can also be set to +15 dBm (LOW power setting), or to any level in the range +15 dBm to +26 dBm, in 1 dB steps, to address special or regional applications of the LMS4000, or for bench testing.

3.5.9 Receive Sensitivity

The receive sensitivity (received signal required to attain a raw data BER of 10^{-5} or better using 1000-byte packets) of the CCU and EUM is $\leq$ -86 dBm, measured at the unit's RF connector.

3.5.10 Antenna Connector

The RF connector used on the CCU and EUM is a WaveRider-proprietary connector. As noted above, the use of a proprietary antenna connector is mandated by FCC requirements for a unique RF connector on ISM products.

3.5.11 Antenna Control (EUM)

A DC voltage (5 VDC or 7.5 VDC) is applied to the EUM RF connector for powering and controlling the WaveRider diversity antenna. One beam pattern is selected if the voltage is 5 VDC. A second beam pattern is selected if the voltage is 7.5 VDC.

CAUTION: The EUM sends DC power and control voltages through the RF connector to the switched-beam diversity antenna. You must use WaveRider-approved indoor or outdoor antennas; otherwise, you could inadvertently short out the DC voltage and damage the EUM. Contact WaveRider Technical Support for a list of approved antennas.

3.5.12 Propagation Path

CCU and EUM radios and antennas provide the basis for excellent radio propagation in both line of sight (LOS) and non line of sight (NLOS) EUM installations. Radio propagation in the 902 – 928 MHz ISM band is superior to propagation in higher ISM bands for several reasons:

- Lower free space loss
- Lower cable loss
- Lower vegetation loss
- Better wall and glass penetration

- More signal recovery from diffraction
- More signal recovery from reflections

Radio line of sight exists when there is a clear optical path between the CCU and EUM antennas, as well as adequate clearance of the path over terrain, foliage, and buildings. This clearance requirement is called the Fresnel clearance. The required clearance varies along the path and reaches a maximum at the path midpoint. If you have a path with Fresnel clearance, the loss between the antennas is generally equivalent to free-space loss and can be readily calculated.

NLOS exists when the path between the CCU and EUM is obstructed, or partially obstructed, by terrain, buildings, or foliage. NLOS is illustrated in Figure 24. Since radio waves reflect, refract, and diffract, a non line of sight path does not necessarily mean the EUM-CCU radio link does not have enough signal margin. It simply means that the path loss is greater than the LOS path loss. Within the engineered NLOS coverage range of the CCU, the NLOS path, using an indoor antenna, is acceptable for most EUM installations.

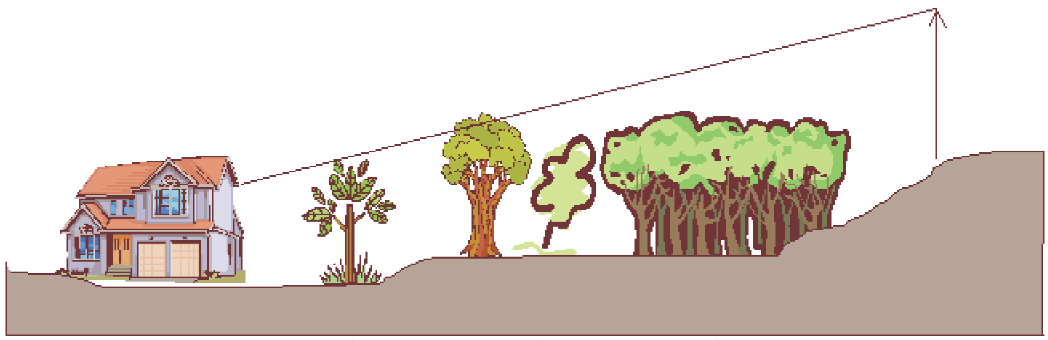


Figure 24 Typical NLOS Path

It is difficult to accurately predict NLOS path loss; however, a lot of field data has been collected and factored into commercially available path-prediction software.

LMS4000 900 MHz radio coverage prediction depends on the following:

- CCU radio output power, transmission-line losses, and antenna height and gain
- Length of the path between the CCU and EUM
- Height of terrain, foliage, and buildings along the path between the CCU and EUM, which determines the percentage of the path that is obstructed.
- EUM antenna height and gain, transmission-line losses, and receiver sensitivity
- If the EUM antenna is installed indoors, location of the EUM antenna within the end-user premises, and the premises building type and wall construction

The EUM has been designed to work with the WaveRider indoor switched-beam diversity antenna. Where greater range is required, outdoor EUM antennas are also available.

Generally, the higher the CCU antenna, the better the range, especially for LOS performance. Ideally, the CCU antenna should be installed well above the average height of trees in the vicinity of the CCU.

Table 2 shows the typical radio coverage (distance from the CCU) that the LMS4000 900 MHz Radio Networks can achieve. Table 2 should be used as a planning guideline only, due to the difficulty of accurately predicting radio coverage.

Table 2 Typical Radio Coverage

EUM Installation	Typical LOS Range	Typical NLOS Range
Indoor Antenna (path to CCU is through a window)	3 mi (5 km)	1 mi (1.6 km)
Outdoor Antenna	5 mi (8 km)	2 mi (3.2 km)

The following assumptions have been made in calculating the above ranges:

- For practical purposes, assume that typically 80% of the subscribers in the predicted coverage area will be able to receive service. Higher coverage is possible but often requires more extensive RF engineering.
- LOS (line of sight) means optical view and radio Fresnel clearance between the EUM premise and the CCU antenna.
- Typical CCU antenna height of 130 ft. (40 m), at least 10 ft. (3 m) above the trees.
- Typical EUM antenna height (for outdoor antennas) of at least 13 ft. (4 m).
- The CCU EIRP has been maximized to +36 dBm in all cases. However, it is a maximum of 34.8 dBm for indoor use. Refer to Appendix F on page 229 for further guidelines.
- The EUM outdoor antenna (Yagi antenna, for example) has a gain of 9 dBi, and the indoor antenna (WaveRider switched-beam diversity antenna) has a gain of 6.2 dBi.
- Coverage with the WaveRider indoor switched-beam diversity antenna depends on the composition of the exterior walls and structure of the end-user’s premises. For best results, the EUM antenna should be installed behind a window.

Actual results vary significantly due to local conditions. Coverage-area prediction that takes into account local terrain and clutter factors provides a better estimate of coverage.

3.6 CCU–EUM Interface MAC Layer (Polling MAC)

This section describes the following the following aspects of the CCU–EUM Interface MAC Layer (Polling MAC):

- *EUM States* on page 41
- *Basic Operation of the Polling MAC* on page 42
- *Network Usage* on page 43
- *Association* on page 43

3.6.1 EUM States

The LMS4000 900 MHz Radio Network data transmission is based on a WaveRider's patented polling algorithm, which takes advantage of patterns found in typical Internet usage. Based on the EUM's subscribed grade of service and current traffic level, the Polling MAC continuously adjusts the rate at which the EUM is polled. This process is illustrated in the EUM State Diagram in Figure 25.

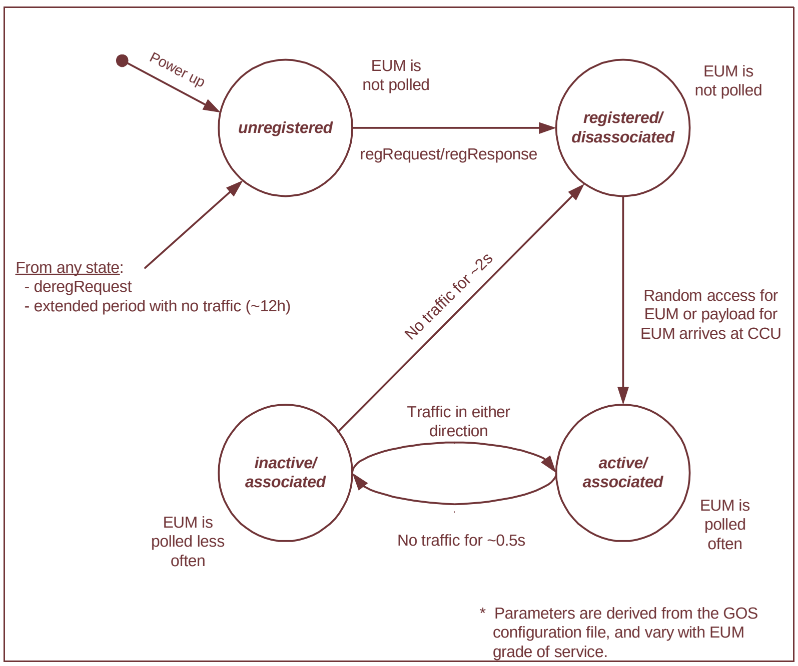


Figure 25 EUM State Diagram

When an EUM first powers up, it is in an *unregistered* state.

In the *unregistered* state, the EUM is not being polled and is therefore not passing traffic. As outlined in *EUM Registration* on page 24, an *unregistered* EUM sends a *registration_request* to the CCU. If the EUM is authorized in the CCU Authorization Table, it becomes *registered/ disassociated*.

In the *registered/disassociated* state, the EUM is still not being polled. But if the EUM has traffic to send, it tries to associate with the CCU through the random access channel. The EUM may also become *associated* if the CCU has a payload to send to the EUM. Once *associated*, the state of the EUM changes to *active/associated*.

In the *active/associated* state, the EUM is polled often, at a rate consistent with its subscribed grade of service. If there is no traffic to or from an *active/associated* EUM for a defined interval (typically set around 0.5 seconds), the state of the EUM changes to *inactive/associated*.

An *inactive/associated* EUM is polled less frequently than an *active/associated* EUM. If traffic is resumed, the state of the EUM changes back to *active/associated*. If there is no traffic for a longer defined interval (typically set around 2 seconds), the state of the EUM changes back to *registered/associated*.

If an EUM is issued a deregistration request, for any reason, or if it has no traffic for an extended period of time, 12 hours or so, its state changes back to *unregistered*.

3.6.2 Basic Operation of the Polling MAC

The Media Access Control (MAC) layer determines which EUM may transmit and when it may transmit. Through the MAC layer, the CCU determines which associated EUM may transmit next and indicates to the EUM that it can transmit by polling it. The frequency with which an EUM is polled is based on its assigned Grade of Service (GOS). The CCU transmits a directed poll to the EUM, which immediately transmits a response to the CCU. After the response is received from the EUM, the CCU transmits the next poll. In this way, the inbound (EUM-to-CCU) and outbound (CCU-to-EUM) channels are maintained collision free.

If the CCU has data to send to an EUM, then that data is sent with the directed poll. If the EUM has data to send to the CCU, then that data is sent with the EUM response to the poll.

EUMs that are not *authorized* are not polled.

To optimize polling efficiency, EUMs that no longer have traffic to send are not polled. EUMs that are not being polled can submit a request to be polled by responding to a special random access poll transmitted regularly by the CCU. Collisions may sometimes occur on this random access channel; however, since only a small number of users are vying for service through the random access channel at any one time, the effect on channel performance is negligible. Recovery from these collisions is made possible by random back-off and retry.

Once again, if the EUM requesting service through the random access channel has data to send to the CCU, it will be included with the request message. If the CCU has outstanding broadcast messages to send, they will be sent to all EUMs with the random access poll.

An automatic repeat request (ARQ) scheme, using acknowledgements and retransmissions to recover from message losses due to collisions or radio link errors, provides reliable transport. Each transmitted data payload is numbered in the packet header. Each packet header also contains an acknowledgement for the last correctly received payload, by number. If a CCU or EUM does not receive an acknowledgement for a payload that it has transmitted, it retransmits that payload with the following poll of, or response from, that EUM. A payload is transmitted a maximum of four times, after which it is discarded. Note that contrary to the 802.11b system, MAC-layer acknowledgements are not transmitted as separate packets, reducing overhead by 33%, on average.

3.6.3 Network Usage

The design of the Polling MAC has been optimized to allow maximized user capacity for typical patterns found in Internet usage, which include browsing the world wide web, accessing email, transferring files, and streaming audio and video. The common characteristic of these uses is that they are bursty—data is transferred in bursts, with time in between the bursts when no data is transferred. As a result, not all users will be transferring data at the same time. In fact, the number of users that are actually transferring data at any one time is generally much smaller than the number sitting in front of their computers which, in turn, is much smaller than the total number of end users. As a result, many users can share the radio link and, for the short time they need it, use a significant portion of the link bandwidth. In other words, many users share the limited bandwidth of the channel, yet each perceives that they have most of the channel bandwidth to themselves. This over-subscription model is the basis of Ethernet, DOCSIS cable networks, 802.11 radio networks, Bluetooth, and on a larger scale, the public switched telephone network.

If a significant portion of the network traffic does not meet this typical bursty model, the Polling MAC adjusts to maximize the user capacity. In this case, the maximum number of users is less than the case where most of the traffic is bursty. As described in *Specialized Applications* on page 177, the Polling MAC can also be optimized to support LMS4000 applications, which have been designed, for example, to cost-effectively extend the coverage range.

3.6.4 Association

The Polling MAC has been designed to take advantage of the bursty, intermittent nature of Internet usage through the concept of association. When users are transferring bursts of data, their EUMs are *associated* with the CCU, and they are allocated a portion of the polling sequence. In between bursts, the EUM is *disassociated*, freeing that part of the polling sequence for other users. The determination of when to disassociate an EUM is based on the time that has expired since any data was transferred to or from that EUM. As more and more EUMs become *associated*, the bandwidth allocated to each EUM gets smaller and smaller, consistent with the GOS constraints discussed below.

When an EUM is not *associated* but has data to send, it uses the random access mechanism to send the first packet. On receiving this first packet, the CCU considers the EUM associated and begins to poll it. The EUM remains *associated* as long as traffic continues to flow, but after a short period of inactivity it is directed to disassociate.

If the CCU has data to send to a *disassociated* EUM, the status of the EUM changes to *associated*, and the data is sent to the EUM the first time it is polled.

The maximum number of EUMs that can be *associated* at any one instant of time is 75. Any EUMs trying to associate beyond this limit are denied access until the number of *associated* EUMs falls below the limit.

3.6.5 Grade of Service (GOS)

In the Polling MAC, the grade of service (GOS) determines how often, and when, an *associated* EUM is polled. Since the EUM can only send one packet each time it is polled, the data rate is related to the polling rate.

Operational objectives that are factored into the determination of the basic polling rate include the following:

- Maximize overall user capacity and minimize the overhead related to empty polls.
- Accommodate different types of data; for example, short, bursty data, such as email and browsing, and large file transfers.
- Support differentiation of user classes in terms of committed information and maximum burst rate throughput levels.
- Control packet latency to support interactive services such as VoIP and chat.
- Support both symmetrical and asymmetrical data applications.
- Control unauthorized web hosting or gaming applications.
- Support multi-user network applications at a single EUM

To accommodate these often-conflicting operational objectives, WaveRider has designed a patented Polling MAC layer that incorporates an integrated GOS management algorithm. Within this algorithm, a total of 11 GOS parameters (GOS parameter set) are controlled to achieve specific performance objectives.

To maximize the performance of the GOS algorithm, and therefore Polling MAC, control of the following factors is key:

- Delay between packets transmitted to (or from) an EUM
- Relative weighting of different GOS classes
- Determination of when an EUM is *active* or *inactive*.

Manipulating these factors through the GOS parameter set can provide

- differentiated levels of service to end-users, which are defined in terms of average committed and maximum burst throughput rates, and
- other special service classes.

The polling algorithm controls packet rates and timing, which in turn provide varying data throughput in kbps, depending on the packet sizes for a given application.

GOS classes are defined based on particular combinations of the GOS parameter set. The system operator assigns a GOS class to each EUM, and the CCU gets the EUM's polling parameters from that class.

In determining the order in which to poll the EUMs, the CCU tries to

- ensure consecutive polls of an EUM occur within the range defined by the EUM's grade of service,
- maintain the average time between polls defined by the grade of service, and
- divide the total number of polls among EUMs consistent with the grades of service of the EUMs being polled.

Since it is inefficient to poll an EUM if there is no data to send either way, an EUM can be polled less often if it has not recently transmitted or received traffic. The GOS parameter set essentially provides for independent control of the polling characteristics for both *active* EUMs (those that have recently had traffic) and for *inactive* EUMs (those that have recently had no traffic), where “recently” is defined by the GOS parameter set.

In addition to efficiently managing the usage of the radio link and providing differentiated service capabilities, the polling MAC inherently smooths the upstream (EUM-to-CCU) packet arrival times. It also has a smoothing effect on the downstream traffic arrivals, which positively impacts network performance by reducing

- surges in data traffic,
- transients in queue occupancy, and
- packet discards.

3.6.6 GOS Configuration Files

Each GOS is defined by configuration files that are stored in the CCU. The CCU can maintain up to five GOS configuration files, consisting of

- up to four assignable GOS configuration files, and
- one GOS configuration file for broadcast messages.

The operator assigns each EUM to one of the four assignable GOS configuration files, which have the fixed labels of Gold, Silver, Bronze, and Best Effort. Although the labels are fixed, the actual service level is determined by the configuration file that is associated with label.

Although only four assignable GOS configuration files can exist simultaneously in the CCU, each of these files can be readily changed by FTPing a new configuration file to the CCU, to replace the existing one. This change can be done while the CCU is active and takes effect immediately.

As specific requirements are identified, WaveRider creates and makes available sets of predefined configuration files. To illustrate the operation of the GOS configuration files, the performance of the factory default GOS service levels is summarized in Table 3. This default GOS configuration file is tailored for networks consisting of both residential and business-class users.

Table 3 Factory Default GOS Configuration File

Service Class	Polling Rate (polls/second)	FTP Rate (see note)	Operator Assigned
Best Effort	1 - 34	0 - 384 kbps	Yes
Bronze	1 - 90	0 - 1024 kbps	Yes
Silver	12 - 22	128 - 256 kbps	Yes
Gold	22 - 46	256 - 512 kbps	Yes
Broadcast	Varies with channel load, from 16 to 29	Not applicable	No
Denied	0	0	Yes

NOTE: While recognizing that the performance of data transmission through packet radio networks is randomly dependent on many variables, typical FTP rates based on empirical data are included in the table to demonstrate the performance that the operator might expect on single, large FTP transfers using maximum-sized packets.

There are several important observations that can be made about the above service-class descriptions:

- All of the default service classes impose a limit on the maximum polling rate.
- The Silver and Gold service classes have a lower bound on the polling rate (12 and 22 polls per second [pps] respectively). The Polling MAC treats this limit as a minimum committed level, which is subject to overall radio link capacity.
- In determining the order and frequency with which to poll EUMs, the CCU first tries to ensure all *associated* EUMs are polled no more frequently than the maximum service class polling rate, and no less frequently than the minimum service class polling rate.
- As the system usage increases, the end-user throughput in all classes decreases from the maximum. Bronze users see the largest reduction, then Gold users, and then Best Effort users. When all users have been reduced to 256 kbps (the minimum threshold for Gold), the next reduction will be shared by the Best Effort, Bronze, and Silver class users (Gold will not be reduced further), until the minimum threshold for Silver is reached. After this, if further reductions are required, this reduction would be shared equally between the Best Effort and Bronze users.

  In practice, the bursty nature of Internet usage is such that this methodical reduction in throughput is not apparent to the end-user, and these variations in service level tend to be instantaneous and transitory. Overall, end-users tend to see a relatively high average throughput consistent with their assigned GOS class, as is shown later in detailed simulation results based on real user data.

3.6.7 Transmit Queue Limits

CCU transmit buffer space is a limited resource shared between the EUMs. If more traffic is received at the CCU for transmission to an EUM than can actually be transmitted to it, that EUM might eventually use up all available CCU buffer space, effectively starving all other users. Therefore, the number of packets in each EUM's transmit queue is intentionally limited.

Packets arriving beyond this limit are discarded, resulting in retransmission of TCP/IP packets by the host computer and TCP/IP adjusts by slowing down. The EUM transmit queue length limit, which is never less than the lower bound given in the GOS parameter set, is dynamic and based on total queue occupancy.

EUM transmit queue length limit determines the optimal TCP receive window size (the maximum allowed number of outstanding unacknowledged bytes) used by the host application. Some Internet Speed Boost programs intended for DOCSIS or ADSL connections, simply increase the receive window size to very large values. This increase results in very long queues at the CCU, more discarded packets, increased retransmissions, and reduced throughput. To maximize throughput, WaveRider recommends setting the receive window size of these applications to between 18000 bytes (~12 packets) and 24000 bytes (~16 packets).

3.6.8 Polling MAC Statistics

A wide range of Polling MAC statistics are recorded by the CCU and EUM. These statistics are very useful, particularly during installation and as an aid to troubleshooting. A complete list of statistics provided by entering the <stats mac> command through the CLI can be found in *Monitoring the Network* on page 165.

3.6.9 Performance Modelling

The performance of packet radio systems like the LMS4000 900 MHz Radio Network cannot easily be derived from analytic calculations. However, using computer simulations that are designed to accurately reflect the system implementation, and user and network traffic distributions, it is possible to produce statistical representations of LMS4000 system performance.

WaveRider has developed a model that simulates LMS4000 system processes, tasks, protocols, propagation delays, and queue sizes. The model can simulate systems with large numbers of EUMs and wide ranges of user traffic. The inputs to the model include

- number and geographical distribution (distance from CCU) of EUMs,
- user traffic statistics, and
- RF link-quality distributions.

These inputs are based on WaveRider’s experience with actual customer installations. The outputs of the model are statistical representations of system performance.

To illustrate the output of the model, consider the following example. First of all, make the following general assumptions:

- LMS4000 900 raw channel rate is MHz 2.75 Mbps

- There are no channel errors
- Servers are fast and do not present a bottleneck
- There are no external link or backhaul bottlenecks
- Typical CCU to EUM range is 0 to 3 km
- GOS is unlimited
- One end user for each EUM

Furthermore, assume that typical end-user traffic is Web browsing, averaging one 60 kbyte HTTP transfer every two minutes. This traffic pattern is based on analyses of busy-hour data collected from LMS systems consisting primarily of residential users. In normal usage, users randomly and independently download a file or Web page, take time to process the information, and then download another file or Web page. Assuming this type of traffic, the performance shown in Figure 26 results.

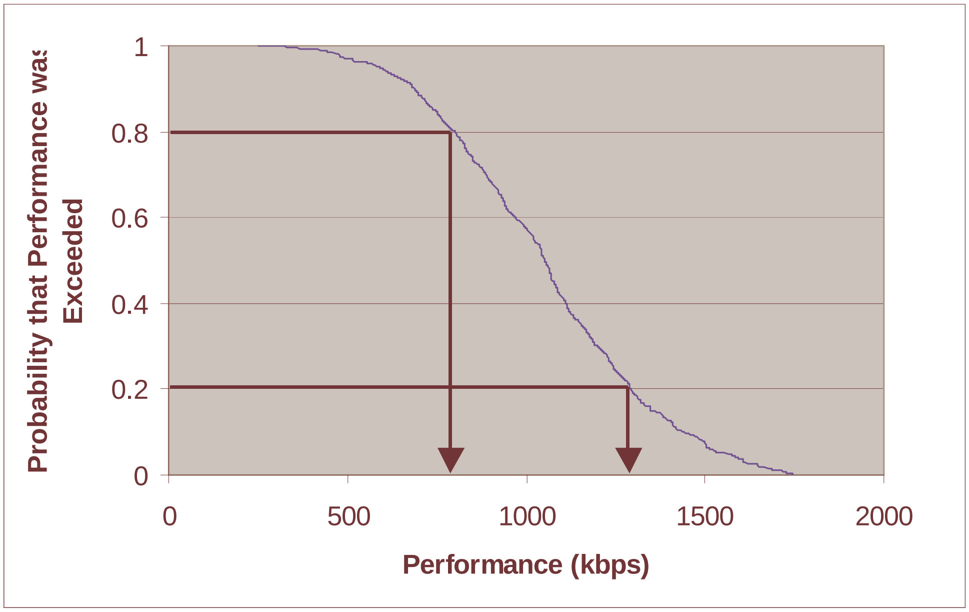


Figure 26 Net Throughput per Transfer (100 End users, 60 kbyte HTTP every 2 minutes)

From Figure 26, each of the 100 end users can expect a net throughput better than 800 Kbps 80% of the time, and better than 1.3 Mbps 20% of the time. You can also assess system performance based on the number of EUMs that are *associated* at any given time, as is illustrated in Figure 27.

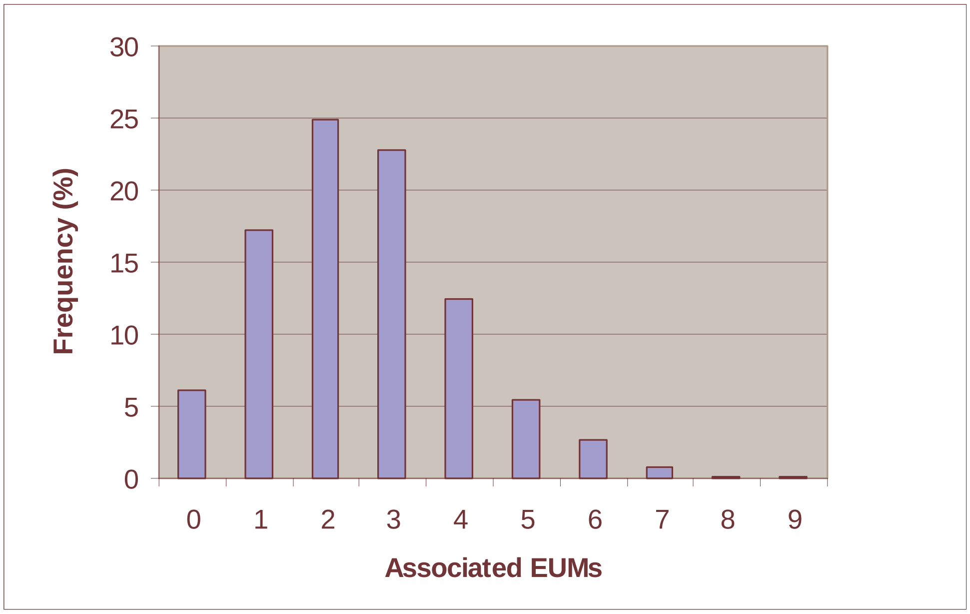


Figure 27 Associated EUMs — 100 EUMs, 60 kbyte HTTP every 2 minutes

Of the 100 EUMs, each is *associated* at random times and for random intervals, so the probability of having more than ‘n’ EUMs *associated* must be determined statistically.

From Figure 27, 25% of the time only 2 of the 100 EUMs are *associated* at the same time. Less than 1% of the time, there are 7 or more associated EUMs. Even with 100 EUMs, where end users are browsing and downloading during the same period, 6% of the time no EUM is *associated.*

By increasing the number of EUMs to 300 and maintaining the same level of traffic per EUM, the modelled performance becomes

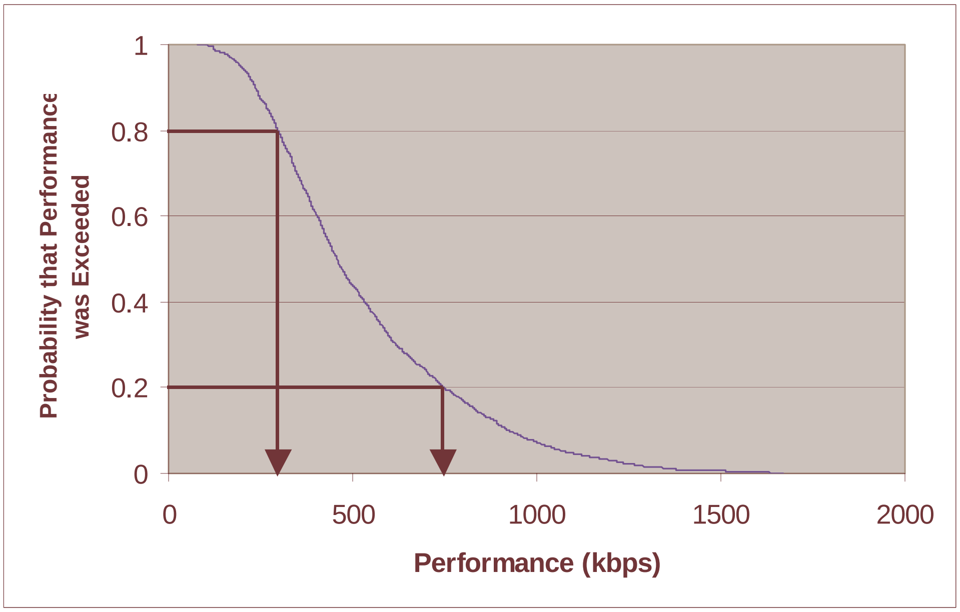


Figure 28 Net Throughput per Transfer (300 End users, 60 kbyte HTTP every 2 minutes)

From Figure 28, each of the 300 end users can expect a net throughput better than 300 kbps 80% of the time, and better than 750 kbps 20% of the time. Once again, you can assess system performance based on the number of EUMs that are *associated* at any given time, as is illustrated in Figure 29.

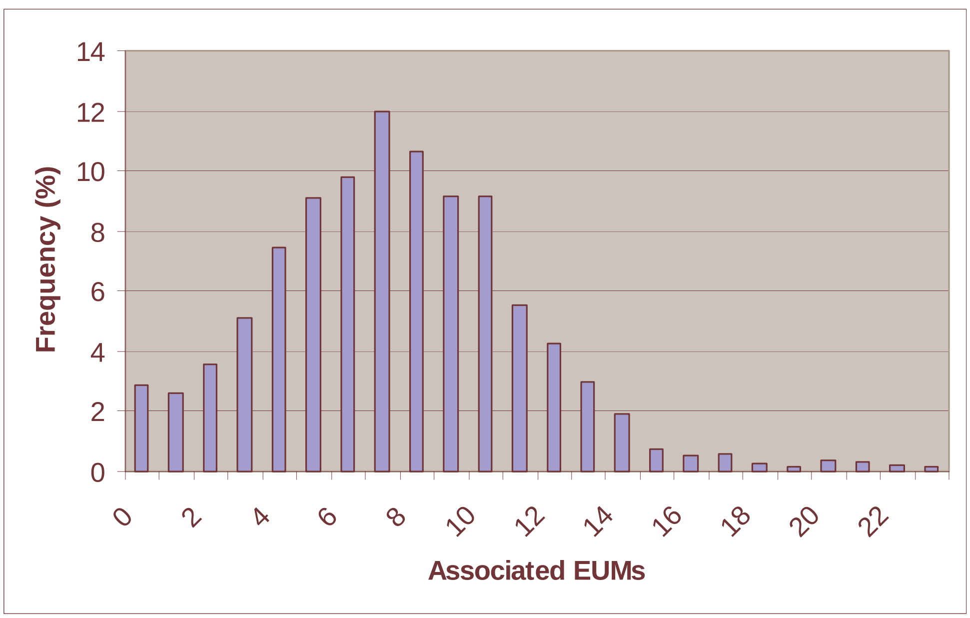


Figure 29 Associated EUMs — 300 EUMs, 60 kbyte HTTP every 2 minutes

From Figure 29, of 300 EUMs, eight were *associated* 12% of the time, and 14 were *associated* less than 3% of the time. The amount of time 25 or more EUMs were *associated* was less than 0.4%.

All of these charts illustrate that **many (LMS4000) users can share the limited bandwidth of the channel, yet most of the time, each perceives that they have most of the channel to themselves.**

3.6.10 Atypical Applications

The Polling MAC has been optimized for normal user applications. One basic assumption that has been made in the design of the Polling MAC is that users are only *associated* for a small fraction of the time they are sitting in front of their computers. This usage is typified, for example, by a file transfer (Web page for example) every two minutes or so—each transfer taking a second or two. The MAC takes advantage of this usage pattern by only associating with *active* EUMs.

A second assumption is that EUMs become *active* independently. If many EUMs simultaneously attempt to use the random access opportunity, they will collide multiple times and may not get through.

If the above assumptions are reasonable, then it is also reasonable to assume that a limited number of EUMs will be *associated* at any given time, as demonstrated in *Performance Modelling* on page 47.

There are several computer applications where usage is not consistent with the above assumptions. These applications, which are discussed below, can compromise the efficient operation of the LMS4000 network and may cause the network to slow down.

3.6.11 Broadcast Applications

Some applications broadcast messages to which all or a large number of hosts are expected to respond. If these applications are running over the system, not only will responses from *disassociated* EUMs collide as the random access opportunities are overwhelmed, but those that do get through will quickly use up all of the available associations. With so many *associated* EUMs, polls are farther apart and throughput degrades, even if the newly *associated* EUMs have no further traffic to send. As well, EUMs that are not *associated* are not able to associate and are therefore be blocked for a few seconds. The following applications can cause this type of problem:

- **Broadcast pings:** WaveRider recommends not using broadcast pings.
- **SNMP broadcast requests:** WaveRider recommends not using SNMP broadcast requests.
- **Windows Network Neighborhood:** WaveRider recommends blocking this type of traffic using port filtering at the CCU or EUM level, as discussed in *Port Filtering* on page 54.

Periodic Packet Sources

Some applications send individual packets at fixed, often large, intervals, expecting only a single packet or small number of packets in response. The direct impact of these applications is that EUMs that are sent periodic packets remain *associated* for a longer period of time than that warranted by their end-user traffic level and continue to be polled unnecessarily. The atypical applications themselves will function very well; however, they will use up a significant amount of the channel bandwidth. This group includes the following applications:

- **Pings** (interval is typically 1 second): WaveRider recommends the operator avoid running applications that generate a lot of pings, such as *What's Up Gold*.
- **Network gaming** (interval is typically 0.25 seconds): WaveRider can provide a GOS class for managing this kind of traffic if specific end users are running this type of application.
- **SNMP poll** (interval is typically 30 seconds): This traffic is usually generated by the operator. WaveRider recommends increasing the SNMP poll interval to a large value, for example, greater than one hour and, if possible, that the SNMP application not poll all EUMs in the same short interval.

TIP: Consult WaveRider for a special GOS Configuration File to limit the impact of these atypical applications for specific EUMs.

3.6.12 Network Monitoring

Some applications send packets to each host on the network, usually to determine whether the host is accessible and/or functioning. These applications, which may be run by the system operator, cause EUMs that otherwise would not be *associated* to become *associated*. Often, the additional load from applications of this type can even exceed the end-user traffic load on the system. Since these applications tend to be periodic, the load is presented to the system regularly over an indefinite period. Also, with large networks, application polling may soon exceed the maximum number of associations. In this case, the application may not be able to receive responses from some EUMs, presenting the operator with misleading status information. This group includes the following applications:

- **SNMP polling:** As noted above, WaveRider recommends increasing the SNMP poll interval to a large value, for example, greater than one hour, and staggering polls to groups of EUMs.
- **SNMP service discovery:** Service discovery is not required for management of the LMS4000 900 MHz Radio Network.
- **Ping scripts**, such as *What's Up Gold*: WaveRider recommends obtaining a tool to stagger the pings.

Since the network operator controls most of the above applications, WaveRider recommends limiting or at least delaying their use until non-busy hours.

3.6.13 Voice Over IP (VoIP)

Voice over IP (as opposed to streaming audio or video) requires small packets to be sent at very short intervals — usually around 20 ms — with very little latency allowed in either direction. While the LMS4000 900 MHz Radio Network may be able to support this level, either as a guaranteed grade of service class parameter or on a best effort basis, VoIP applications result in a high per packet overhead on the radio channel. This overhead and the requirement for low latency mean the VoIP call occupies about 10% of the available bandwidth for the duration of the call. It obviously does not take very many VoIP users to significantly affect system performance. Also, unless this grade of service guarantee is given, the quality of the call may be affected as other users become *associated*, increasing the polling interval beyond 20 ms. Since the grade of service applies to an EUM and not to an individual service, a VoIP user would have to be given a very high grade of service, to the possible detriment of other end users.

3.7 CCU and EUM Feature Description

This section describes the following CCU and EUM features:

- *DHCP Relay* on page 53
- *Port Filtering* on page 54
- *SNTP/UTC Time Clock* on page 55
- *Customer List* on page 56
- *SNMP Support* on page 56

3.7.1 DHCP Relay

NOTE: DHCP Relay is needed only in Routed mode, and is not required in Switched Ethernet or Through Only mode.

IP address information for CCUs and EUMs are manually entered. In the case of end-user PCs, IP addresses can be entered manually or obtained automatically from a DHCP server, if CCU DHCP relay is enabled.

Once DHCP Relay is *enabled* in the CCU, DHCP requests from the end-user's computer pass transparently through the CCU and EUM to the operator's DHCP server. Since the IP address assigned to the end-user's computer must be on the same subnet as the CCU radio port, the operator needs to preassign an appropriate block of IP addresses in the DHCP server.

TIP: It is helpful to assign meaningful names, such as the customer name, to customer computers or home network routers. Then, if a DHCP server is implemented, the address leases pool includes this name with the client IP address, facilitating easier identification.

The gateway router can provide DHCP server functionality, or you can implement a dedicated DHCP server, as shown in Figure 30.

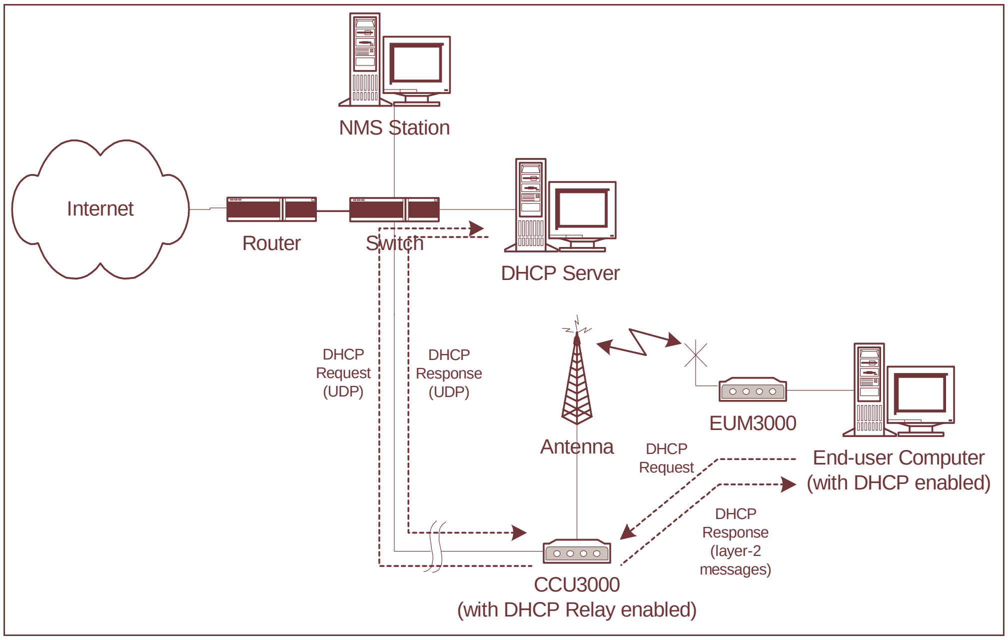


Figure 30 DHCP Relay

3.7.2 Port Filtering

The CCU and EUM both support TCP and UDP port filtering. The IP protocol suite is made up of many subcomponents consisting of ports and protocols. Up-to-date listings of TCP and UDP ports can be obtained off the Web. Some of these ports are required for normal LMS4000 operation, but most are not. The system operator can configure the CCU and EUM to filter packets on specific TCP or UDP ports to improve network performance, security, or privacy.

For example, to prevent end-users from having visibility of, and access to, other end-users through Windows Network Neighborhood, filter the following ports at the CCU for both UDP and TCP packets:

- Port 137 NETBIOS Name Service
- Port 138 NETBIOS Datagram Service
- Port 139 NETBIOS Session Service
- Port 445 Microsoft Windows SMB over TCP Service
- Port 1512 Microsoft Windows Internet Name Service

CAUTION: The EUM is delivered with port filtering enabled.

CAUTION: Do not enable filters to block Telnet (port 23), FTP (ports 20 and 21), or SNMP (ports 161 and 162); otherwise, you will not be able to manage your network.

3.7.3 SNTP/UTC Time Clock

The Simple Network Time Protocol (SNTP)/UTC feature provides LMS4000 devices with an accurate clock for time stamping events in the log file.

SNTP/UTC Time Clock operation is illustrated in Figure 31.

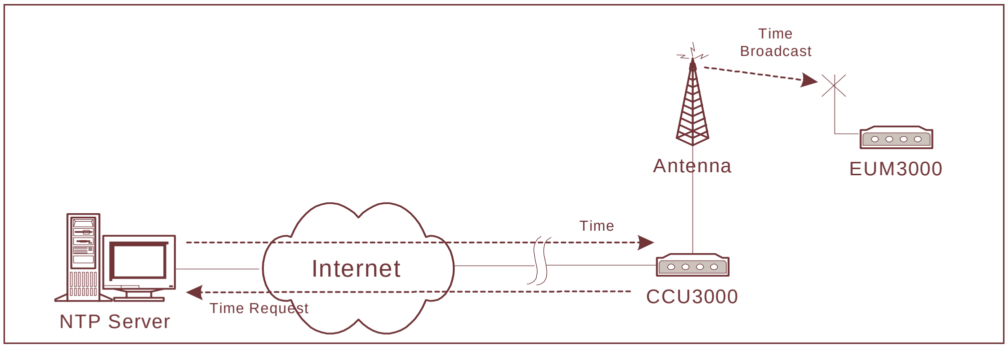


Figure 31 SNTP/GMT Time Clock

The CCU, acting as an SNTP time client, regularly resynchronizes to one of several NTP Servers from which it obtains UTC (Universal Coordinated Time). The CCU resynchronization and retry periods can be set by the operator. The resynchronization period is the time between a successful CCU resynchronization and the next CCU resynchronization attempt, typically set to one hour. The retry period is the time between an unsuccessful resynchronization attempt and the next resynchronization attempt, typically set to 30 seconds.

The operator can configure the CCU to act as an SNTP time server to the EUMs and broadcast time information to all EUMs after it has synchronized with the NTP server. It also broadcasts this information whenever an EUM powers up and registers.

UTC, the international time standard, is based on a 24-hour clock. It is the current term for what was commonly referred to as Greenwich Mean Time (GMT). SNTP, specified in RFC1769 and RFC2030, is a simplified version of NTP, which is specified in RFC1305.

By default, the CCU SNTP client is *disabled*. Once SNTP is *enabled*, the CCU tries to synchronize with an NTP server. The operator can configure the CCU to synchronize with

- a local router or network device, if the router or network device is configured as an NTP time server,
- any open-access NTP server of the operator's choosing, or
- one of the factory-default open-access NTP servers listed below:
  - 132.246.168.148 time.nrc.ca stratum 2, Canada
  - 140.162.8.3 ntp.cmr.gov stratum 2, US
  - 136.159.2.1 ntp.cpsc.ucalgary.ca stratum 2, Canada
  - 192.5.5.250 clock.isc.org stratum 1, US

3.7.4 Customer List

For each EUM, the system operator can control the number of end-user computers that can access the LMS4000 network for the purpose of controlling network performance or service differentiation. The use of this list is described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242.

3.7.5 SNMP Support

Simple Network Management Protocol (SNMP) allows a network management server to monitor, control, and remotely configure LMS4000 network devices. In SNMP, these devices are also referred to as agents.

Community Strings

Community strings act as passwords to facilitate communication between the SNMP server and a network device. There are three types of community strings:

- **Read community strings**, which enable SNMP servers to retrieve information from a network device
- **Write community strings**, which enable SNMP servers to send information, such as configuration commands, to a network device.

  NOTE: At this time, there are no writable SNMP MIB entries. All configuration is done through the CLI.

- **Trap server IP address and community strings**, which enable SNMP servers to receive unsolicited messages from a network device. These unsolicited messages indicate asynchronous events, such as an interface going down or coming up, a unit performing a cold or warm start, or an operational failure.

Each network device monitored by SNMP must have at least one of each type of community string defined. Each CCU and EUM can have up to five read or read/write and five trap servers/community strings defined. Non-WaveRider devices may have only one of each type of community string defined. Community strings are case sensitive.

Table 4 Factory Configured Community Strings

Community String Type	Community String
Read	public
Write	private
Trap	<none>

CAUTION: By convention, most equipment ships with the default community strings defined in Table 4. WaveRider recommends that you change the community strings before you bring the LMS4000 equipment online, so that outsiders cannot see information about the internal network or configure system components.

Management Information Bases (MIBs)

All messages sent between the SNMP server and a network device are based on number codes. Each of these number codes corresponds to a specific type of information (such as the quantity of data packets received) associated with a specific type of network device (such as a CCU). These number codes and their meanings are stored in a management information base (MIB). The SNMP server and network devices use these MIBs as lookup tables for translating messages sent between them.

LMS4000 implements SNMPv2c and includes a number of standard and enterprise MIBs:

- RFC1157 (MIB-II)
- RFC1493 (bridging)
- WaveRider Enterprise MIB (defined in Appendix I on page 251)

You can download WaveRider Enterprise MIBs, which include a comprehensive set of CCU and EUM parameters and statistics, from the technical support page at www.waverider.com.

— This page is intentionally left blank —

4 IP Network Planning

This section is intended to guide you through the process of planning the topology of your LMS4000 900 MHz network, including IP addressing schemes and the placement and configuration of routers, Ethernet switches, and network servers. These decisions will be affected by your subscribers' requirements, the services you intend to offer, your existing network environment, level of technical expertise, network size, and future expansion plans.

The CCU provides three protocol modes that determine how it processes network traffic:

- Routed mode
- Switched Ethernet mode
- Through Only mode

4.1 WaveRider Terminology

Ethernet Device—Any device that has an Ethernet MAC address and can communicate over Ethernet is considered an Ethernet device. Typically, there are two Ethernet Devices per EUM: the EUM itself and the subscriber's computer. However, each Ethernet device attached to an EUM and given air access (see *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242) should be counted.

Directed Ethernet Packets—Ethernet packets destined for a specific Ethernet device.

Broadcast Ethernet Packets—Ethernet packets with the Ethernet broadcast address as the destination. All Ethernet devices receive all broadcast packets.

Multicast Ethernet Packets—Ethernet packets with an Ethernet multicast address as the destination. They are generally destined for one or more Ethernet devices. Multicast Ethernet packets that make it into the radio network are treated as broadcast packets to all EUMs and hosts.

Ethernet Segment—All of the Ethernet devices that receive the same directed Ethernet packets are considered to be on one Ethernet segment. Any device on this segment could put its Ethernet interface into promiscuous mode and see all Ethernet traffic to and from another device on the same segment. For 10/100BaseT Ethernet, Ethernet devices connected directly, through Ethernet hub(s) or through Ethernet repeater(s) are on the same segment. Ethernet switches normally support one Ethernet segment per port since directed Ethernet traffic is switched from a port to only one other port, once the switch has learned which Ethernet devices are on which port. In all modes, the CCU radio interface is a switch, so EUMs are always on separate Ethernet segments. Therefore, an EUM only receives directed Ethernet packets destined for itself or any host on the Ethernet side of the EUM.

Ethernet Broadcast Domain—All of the Ethernet devices that receive an Ethernet broadcast packet are considered to be on the same Ethernet broadcast domain. In general, this includes all Ethernet segments connected by Ethernet switches. An Ethernet broadcast domain is usually bounded by IP routers.

IP Broadcast Packet—An IP packet address to the subnetwork broadcast address. If the IP subnet is 172.16.4.0 / 22, then 172.16.7.255 is the IP broadcast address for that subnetwork. Older addressing schemes use 172.16.4.0 as well for the subnet broadcast address.

Radio Network—The radio network consists of the CCU radio interface, the EUMs, and the subscribers. Note that if an IP router is attached to an EUM, other network(s) may be created behind this router, accessible through the radio network.

CCU Ethernet Network—The Ethernet network refers to the CCU Ethernet interface and all devices attached to it through Ethernet switches and/or Ethernet hubs.

VLAN—Virtual LAN. Some Ethernet switches and routers can be configured to support multiple Ethernet broadcast domains, each limited to a set of segments, or even—for devices supporting it—individual devices. While CCUs do not support VLAN tagging, the technique may be used between the gateway router and an Ethernet switch to limit Ethernet broadcast traffic that would otherwise unnecessarily be carried over the air link and fill the CCUs' bridge tables in Switched Ethernet topologies. Contact WaveRider Technical Support for more information.

4.2 Routed Mode

In this mode, basic IP routing principles apply. The Ethernet network and the radio network are divided into separate broadcast domains, as shown in Figure 32 on page 62.

This mode offers greater flexibility in scalability, if the maximum radio network size is planned in advance. CCU radio networks are assigned to different IP subnets and routed to a gateway router. This mode offers effective control of Ethernet broadcast domains and added security over Switched Ethernet mode by isolating subnets.

In Routed mode, it is important to consider the expected network size (taking into account any future growth) and plan the subnet size accordingly. Changes to the subnet size at a later stage would require reconfiguration of all the network devices in the radio subnet. The subnet should be large enough to cater for both the expected number of subscribers and the EUMs.

For example, if the network will be limited to no more than 200 EUMs and about 200 to 300 subscribers (allowing for more than one subscriber per EUM visible to the radio network), then an IP subnet that allows 512 addresses (510 usable, since host address 0 and all 1s are reserved for IP broadcast) can be used. This is a subnet with a 23-bit netmask, allowing the last 9 bits of the IP address to be used for host addresses. If more than 510 IP addresses are needed at a later stage, then every EUM and subscriber needs to have a new IP subnet mask assigned.

Routed mode does not allow the assignment of subscribers to different IP subnets in the radio network. Also, you cannot assign subscribers to one IP subnet and EUMs to another IP subnet.

Network Address Translation (NAT) can be used to provide private-to-public IP address-mapping for subscribers. Note that not all user applications work through NAT. NAT must be provided by a third-party device, often the gateway router, and is beyond the scope of this document.

NOTE: PPPoE is not supported in Routed mode.

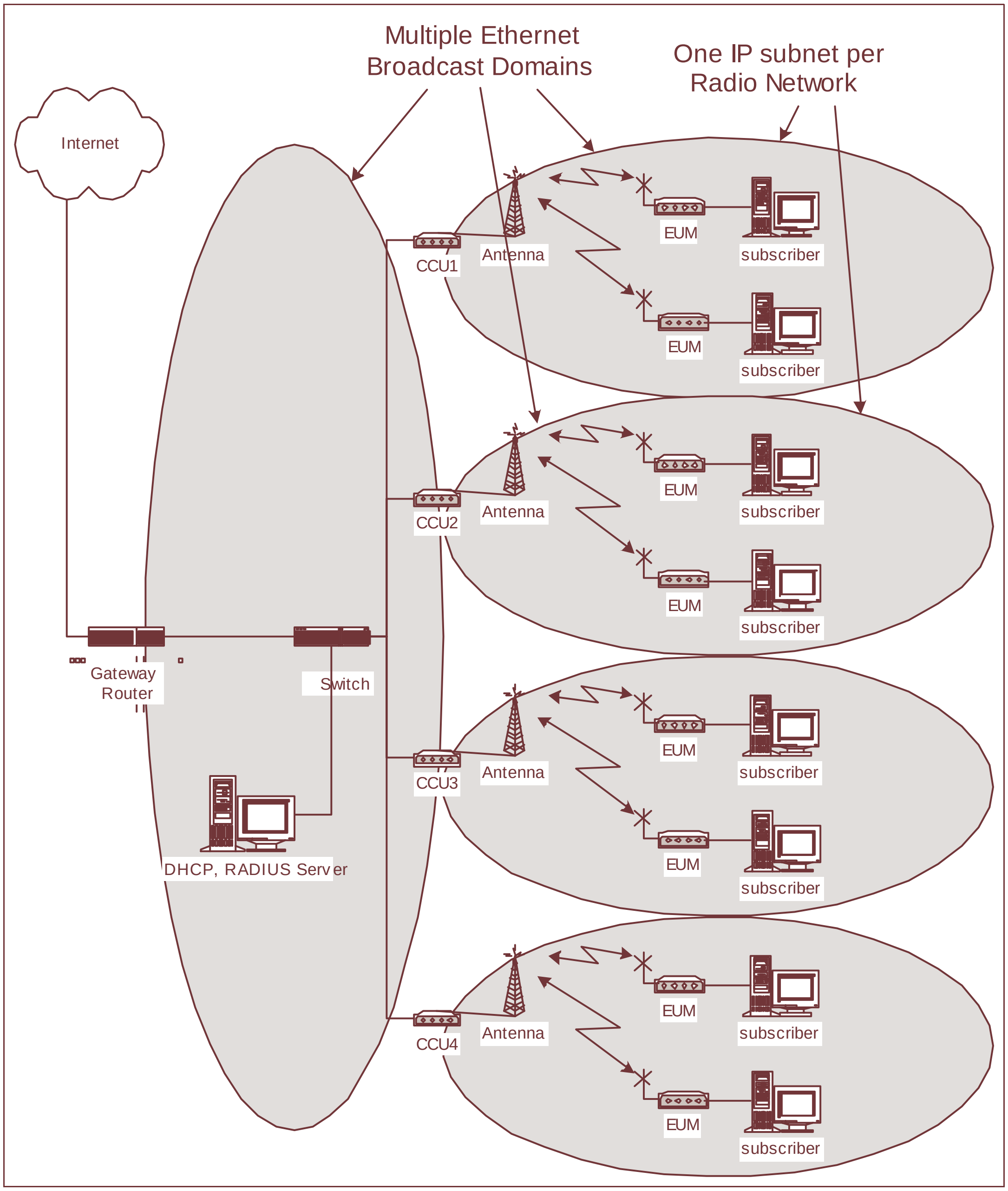


Figure 32 Routed Mode – Ethernet Broadcast Domains

4.3 Switched Ethernet Mode

In Switched Ethernet mode, the CCU acts as an Ethernet switch between the Ethernet interfaces of the CCU and the EUMs in the radio network.

This mode provides simplicity of operation and integration into existing small networks.

The radio networks for every CCU and the CCU Ethernet network, up to the router port, are part of a single Ethernet broadcast domain. All Ethernet devices connected to the same router port through Ethernet switches and radio networks contribute to broadcast traffic on this network, as shown in Figure 33 and Figure 34.

Different IP subnets can be assigned to different devices in the radio network, if required. For example, EUMs may be assigned to one IP subnet for management and subscribers to another, or even to multiple IP subnets. This requires configuring the gateway router with multiple IP addresses and subnets, and routing between the subnets. Note that all traffic between the subnets (from a subscriber to the attached EUM for example) must travel to the router and back, which—especially if this involves backhaul equipment—may introduce unexpected latencies in communication, noticeable in throughput tests.

DHCP can be used to assign IP addresses to all subscribers. A CCU or router can relay DHCP, or the DHCP server can be placed in the broadcast domain. If all subscribers' IP addresses are to be assigned from the same pool, then a simple implementation of DHCP can be used. If separate IP address pools are to be used for each radio network, then alternative approaches to DHCP need to be considered. This is beyond the scope of this document. Please contact WaveRider for further information.

If subscribers' IP addresses and subnets are obtained through DHCP and are on a separate IP subnet from the EUMs, the subscriber IP network can be reconfigured by revoking the DHCP leases and reconfiguring the DHCP pools, the gateway router, and any other equipment on that IP subnet. This makes the network more scalable within limits.

In large networks, Ethernet broadcast traffic could become a major issue. Therefore, it is very important to plan for the expected size of the network when selecting Switched Ethernet mode. Some guidelines on network size are given below.

In summary, while Switched Ethernet mode offers easy integration to smaller networks with network size limited, implementing this mode in medium to large networks requires a higher level of planning and implementation skills.

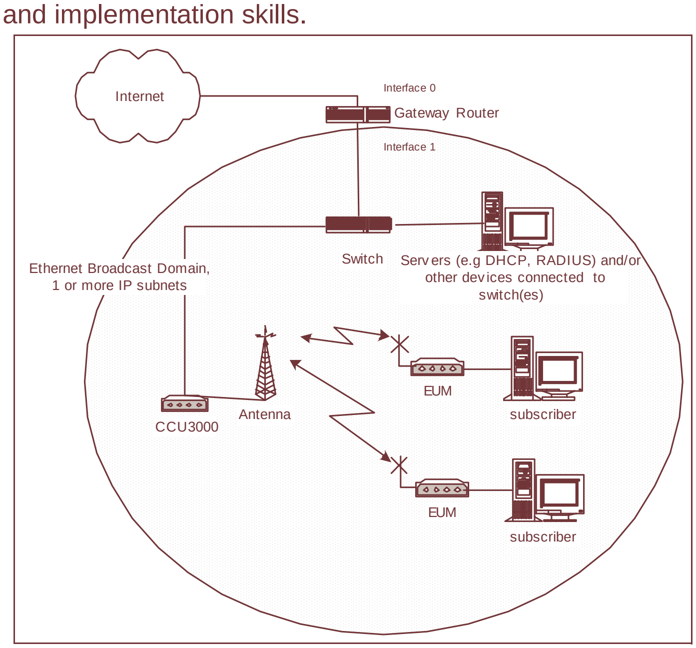


Figure 33 Switched Ethernet Mode – Ethernet Broadcast Domain for a single CCU

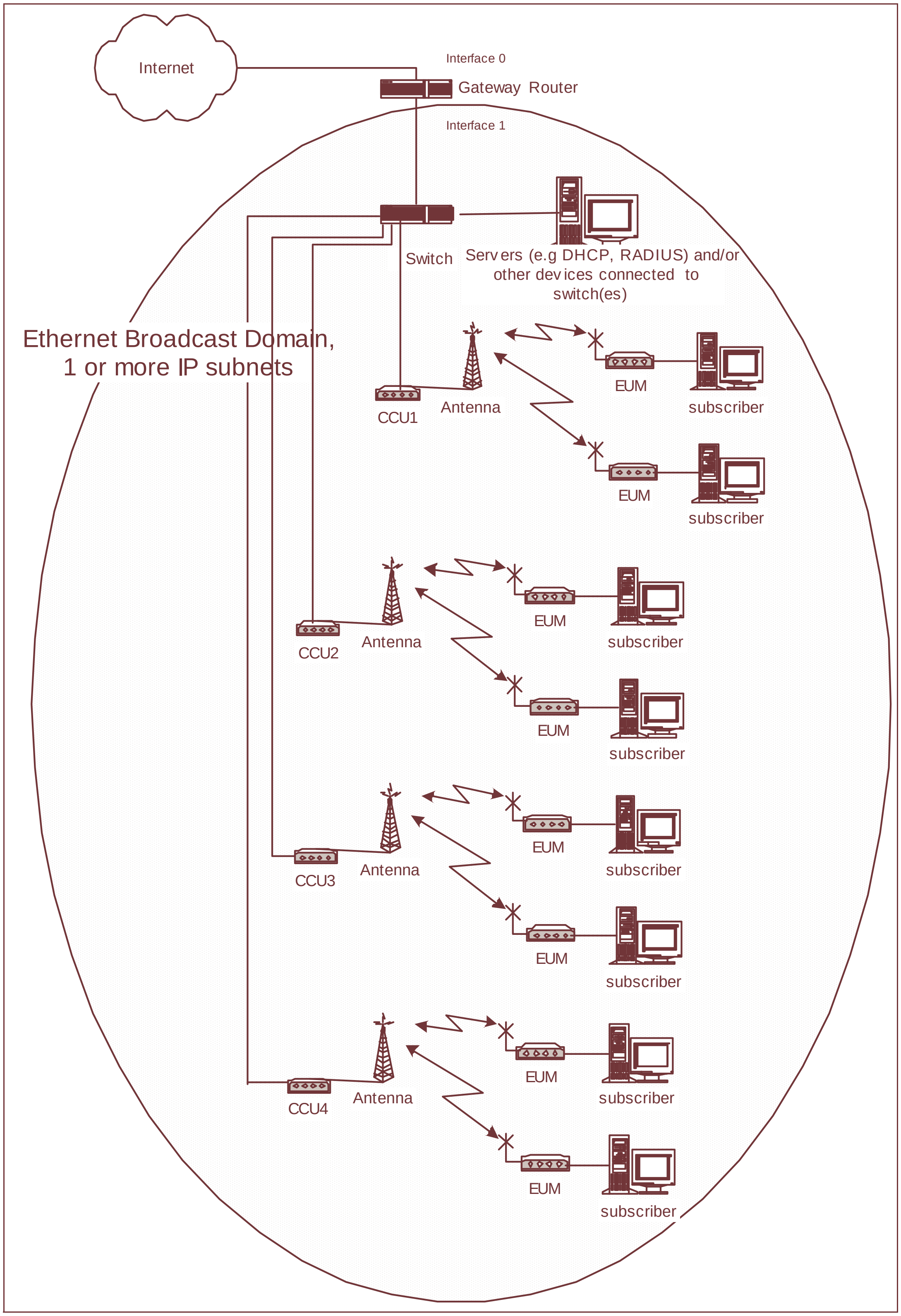


Figure 34 Switched Ethernet Mode – Ethernet Broadcast Domain for multiple CCUs

4.4 Through Only Mode

This mode should only be used for PPPoE networks where ALL subscriber traffic is to be passed to or from a PPPoE server. This is a specialized configuration and not to be used for most networks.

In Through Only mode, the CCU passes all radio network traffic to the CCU Ethernet network, regardless of the Ethernet destination MAC address. This differs from Switched Ethernet mode, where the packet would be passed back to the radio network if the Ethernet destination MAC address is that of an Ethernet device on the radio network. Similarly, a CCU in Switched Ethernet mode passes Ethernet broadcast packets received from an EUM out both the radio and CCU Ethernet networks.

For Ethernet packets from the CCU Ethernet network, Through Only mode is the same as Switched Ethernet mode.

4.5 Network Size Guidelines

In Routed mode, a single CCU can support up to 300[1] subscribers. Assuming one subscriber per EUM, this limits a radio network to 300 EUMs, 300 subscribers, and 1 CCU, each an Ethernet device, for a total of 601 Ethernet devices. This is an Ethernet broadcast domain. This size of broadcast domain provides reasonable performance since broadcast traffic is generally limited to ARP packets. The number of CCUs that can be served by a gateway router port is limited by network capacity rather than by the size of the Ethernet network broadcast domain.

In Switched Ethernet mode with a single CCU, the Ethernet broadcast domain is extended to all devices on the CCU Ethernet network. If this number is limited to about 10 or so devices (e.g., servers, UPS with Ethernet interface, etc.), then there should be little impact on the network performance.

In Switched Ethernet mode with multiple CCUs, the Ethernet broadcast domain is spread over all radio networks and the Ethernet network. Careful planning is required for good network performance.

The guideline is to limit an Ethernet broadcast domain to no more than 650 Ethernet devices, assuming most of the devices use the network lightly. In Switched Ethernet mode with multiple CCUs in a single Ethernet Broadcast domain, this guideline of 650 Ethernet devices still applies.

A general recommendation is that the broadcast and multicast traffic should not be more than 5 percent of the network traffic. Observation of the broadcast traffic may determine whether the guideline limit of 650 devices applies to a specific network or not.

1. This assumes that all subscribers follow a reasonable usage profile. If one or more subscribers use the network more than expected, then the radio network may experience degraded performance with fewer subscribers.

Note that with release V4.0 the CCU Ethernet port bridge table is limited to 256 entries. This imposes a further limit to the size of the Ethernet broadcast domain in Switched Ethernet and Through Only modes. A single CCU Ethernet port should see no more than 256 Ethernet devices. To compute this, take the total number of Ethernet devices in the broadcast domain, and subtract the number of Ethernet devices on the smallest radio network. For example, if there are 3 CCUs with 40, 50 and 60 subscribers, each with an EUM, the total number of Ethernet devices in the broadcast domain is at least 306 (150 EUMs, 150 Subscribers, 3 CCUs, 1 router, 1 switch). This configuration will work. Any CCU Ethernet port will only see the MAC addresses for the EUMs and subscribers for the other CCUs plus devices directly on the CCU Ethernet (e.g., 110 EUMs, 110 subscribers, and 5 other devices in the worst case, for the first CCU). Any broadcast domain with no more than 250 Ethernet devices will also work. This limitation will be removed for V4.1 and later releases.

For networks that are larger than 650 Ethernet devices, multiple Ethernet broadcast domains should be used. Each broadcast domain will contain one or more IP subnets. Multiple Ethernet broadcast domains can be realized by using multiple IP routers, IP routers with multiple ports, or VLANs between a router and a multi-port Ethernet switch.

Using the CCUs in Routed mode is an example of the first method of dividing the broadcast domain, using multiple routers, although the CCU as a router only supports one IP subnet over the radio network.

Figure 35 shows an example of the second method, using a multi-port router.

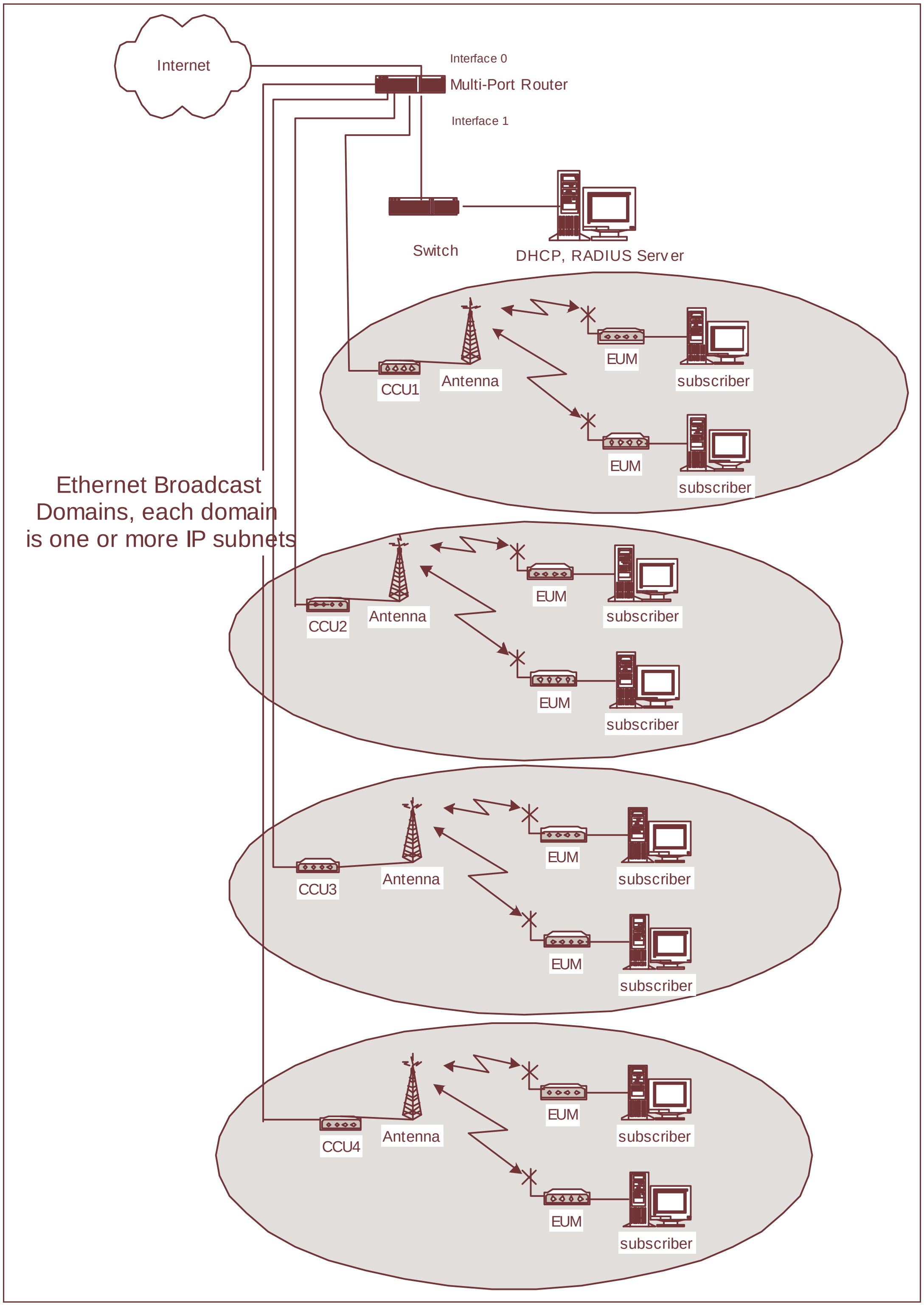


Figure 35 Switched Ethernet Mode – using multi-port router

4.6 Comparison of Modes

	Routed Mode	Switched Ethernet and Through Only Modes
Ethernet Broadcast Domain	Each radio network is a separate domain. The Ethernet network is a separate domain.	The Radio networks and Ethernet networks are in the same domain, so all Ethernet devices up to the nearest router port share the domain.
Number of Ethernet Devices.	Recommend less than 650 per radio network and less than 650 on the Ethernet network. (The Ethernet network is likely to be capacity limited).	Recommend less than 650 total devices including the Ethernet network per router port. With multiple CCUs, v4.0 bridge table size imposes further limits. See *Network Size Guidelines* on page 65.
Radio Network Broadcasts	ARPs generated by EUMs and subscribers appear only on the radio network. IP subnet broadcast packets from outside the network are broadcast on the radio network unless they are blocked, either at the CCU or the gateway router. Other Ethernet broadcast packets are broadcast to the radio network	ARPs generated by EUMs and subscribers and all packets to unknown Ethernet MAC addresses are broadcast over all radio networks and the Ethernet network. Each CCU learns about MAC addresses over time, so packets with unknown Ethernet MAC addresses will be rare. IP subnet broadcast packets from outside the network are broadcast over all radio networks and the Ethernet network unless they are blocked at the gateway router. Other Ethernet broadcast packets are broadcast over all radio networks and the Ethernet network.
Multicast Traffic	Ethernet multicast packets are not passed between the CCU Ethernet network and radio network. CCU does not support or route IP multicast packets. Ethernet multicast packets sourced on the radio network will be treated as an Ethernet broadcast packet.	Ethernet multicast packets will be passed between CCU Ethernet network and radio network, appearing as broadcast traffic on the radio network.
CCU Ethernet Port Mode	Directed. Only broadcast packets and Ethernet packets directed to the CCU are received at the Ethernet interface.	Promiscuous. Every packet seen on the Ethernet port is read and checked. If the Ethernet network has excessive traffic, this can degrade the CCU's performance.

	Routed Mode	Switched Ethernet and Through Only Modes
IP Subnetting	All radio network devices, including the CCU radio interface, EUMs, and subscribers are on one IP subnet.	An arbitrary number of IP subnets can be supported as configured in the gateway router.
Number of routes in gateway router	One per radio network	One per IP subnet defined.
Radio Network Protocols allowed	IP, ARP/RARP	IP, ARP/RARP, PPPoE
Prevention of Broadcast Attacks (SMURF or other denial of service attack)	Add routes to CCU to prevent IP broadcasts from passing between CCU Ethernet and radio networks. Damage is limited to single radio network. Recommend blocking broadcasts at the gateway router as well.	Must be handled by gateway router. Attacks are limited to Ethernet broadcast domain, which can be several radio networks.

4.7 IP Plan Process

This section provides a set of questions and responses that will assist you with the IP planning process.

4.7.1 Which CCU protocol mode is recommended for use?

Switched Ethernet Mode

- Small network with one CCU and up to 300 subscribers per router.
- Network with multiple CCUs in broadcast domain, where no CCU Ethernet port sees more than 256 Ethernet devices. (v4.0 restriction)
- Network with multiple CCUs in broadcast domain, with a total of no more than 650 Ethernet devices.

For networks larger than those above, the broadcast domain must be restricted using additional routers (not CCU), multi-port router(s), and/or VLANs.

To reserve public IP addresses for subscribers only, the EUMs can be assigned to a private IP subnet for management purposes. This provides some added security against external attacks. The subscribers can be assigned the public IP addresses using DHCP if desired.

To allow different IP subnets for different subscribers. The subscribers can be assigned private or public IP addresses as desired, using DHCP if desired.

Through Only Mode

- For a PPPoE Network only, where all subscribers use a PPPoE server.

Routed Mode

- Networks with adequate public IP addresses for all Radio Network Devices
- Networks using private IP addresses for Radio Network Devices and NAT to map subscribers to public IP addresses.
- Large networks where using added routers, multi-port routers or VLANs are not options.

4.7.2 What are the DHCP considerations for the different protocol modes?

DHCP

DHCP is a simple way to provision subscriber IP addresses and is highly recommended in all modes. In general, it is a good idea to limit lease lengths in case it is necessary to change the IP plan.

If DHCP Relay is enabled at a CCU, the CCU will intercept the DHCP request, which is in an Ethernet broadcast packet and relays the request as a directed packet to the DHCP server. The DHCP server can use the CCU IP address, which appears in the packet as the relay agent to determine which pool to allocate from.

IP address assignment can be arbitrary, based on the subscriber's Ethernet MAC address or based on the subscriber's computer's hostname. The latter two approaches allow the WISP to know which IP address is assigned to which subscriber, but require the hostname or Ethernet MAC address to be known (or learned) by the DHCP server.

Routed mode

To use DHCP in Routed mode, the CCU must have DHCP relay enabled.

Use the CCU console command "arp map" to get a list of IP address-to-EUMID mappings.

Switched Ethernet Mode

If the DHCP server is in the Ethernet broadcast domain of the radio networks, it is to serve and either a common pool of IP addresses must be used, or the Ethernet MAC or hostname must be used to select a pool. DHCP relay is not required.

> **NOTE:** Some DHCP servers do not support allocating addresses from an IP subnet to which the relay agent does not belong.

4.7.3 How many subscribers are supported per EUM?

Number of Subscribers per EUM

Network analysis shows that the maximum number of subscribers per radio network is 300, assuming a given subscriber profile. If there are subscribers that use more resources than this profile, then the network performance will start to degrade with fewer subscribers.

With only one subscriber per EUM, this translates to a maximum of 300 EUMs. However, more than one subscriber can use an EUM.

Up to 50 subscribers can have network access through one EUM if the EUM's maximum number of customers is increased. The added subscribers are part of the Ethernet broadcast domain. Regardless of the CCU protocol mode, the added subscribers see all Ethernet broadcasts. This situation is fairly easy to recognize and manage.

An alternative approach is for the subscriber to set up a home network with a router connected to the EUM. NAT allows any number of unseen subscribers to use the radio network. This will use more network resources than would be expected for a single subscriber but is not easily distinguished from a single subscriber who is a heavy user.

The advantage of using a router is that all Ethernet broadcasts from the added (unseen) subscribers are not passed over the radio network. Only one MAC address is required and only one IP address is assigned.

If the subscriber wishes to use his own public IP addresses with his router, it is possible to add special routes to the CCU in Routed mode or to the gateway router in Switched Ethernet mode to route traffic over the radio network to the subscriber's router.

It is your decision whether to allow more than one customer per EUM and whether to permit subscribers to use routers attached to the EUM. It is, however, difficult to detect the latter.

4.7.4 What subnet masks are recommended in the different protocol modes?

Routed Mode

Since all EUMS, as well as subscribers, must be on the same subnet, the largest possible radio network would require 601 IP addresses: 300 for the EUMs, 300 for the subscribers, and one for the CCU. This requires a 22-bit netmask, allowing 1022 host addresses, plus the subnet number and subnet broadcast addresses. If private IP addresses are used, there is no reason not to use this size of subnet.

Most networks never become that large. More often, larger networks are divided between two or more CCUs to provide higher service levels to subscribers. If the maximum network size can be limited to 510 hosts (e.g., 1 CCU, 254 EUMs, and 255 subscribers), then a 23-bit netmask can be used.

Switched Ethernet Mode

Since multiple IP subnets can be supported over Switched Ethernet mode, the IP subnet mask for each subnet is up to you and is dependent on how many devices per subnet you wish to have.

If private IP addresses are used to manage the EUMs, it is best to allocate a large enough subnet for the maximum number of EUMs supported.

5 Radio Network Planning

An important task in the implementation of LMS4000 900 MHz Radio Networks is RF system planning and design. Whether you are deploying a single CCU or a complex multi-CAP, multi-CCU network, proper system design is necessary to provide and maintain high-quality service to end users in your target serving area.

5.1 Design Methodology

The following sections are not intended to provide detailed system design instructions; instead, they provide system design guidelines. WaveRider used this approach for the following reasons:

- Factors affecting system design and implementation vary widely and differ from system to system.
- System design and implementation cannot be encapsulated in a simple formula or set of formulas.

Each system design is unique and must take into account all of the design factors that can influence system operation and performance:

- Topography: Hills and valleys that create coverage holes or conversely, areas that may be very exposed from an RF standpoint, exposing subscribers in these areas to high levels of interference generated from outside the system or by other CAP sites.
- Clutter: Obstructions such as trees and buildings, which tend to reduce the desired signal level and coverage.
- Network Topology: The configuration of the network, implemented to provide optimum service. Network topology is driven by factors such as the location of the Internet point of presence, the availability of towers and roof-top locations that can be used to establish antenna and equipment sites, and the target coverage area.
- Interference: The presence of interference, either in-band (in the ISM band) or out-of-band in your target serving area constrains the freedom that you have for determining the location of CAP sites and for choosing operating frequencies.

In all cases, these wide-ranging factors drive the system design and as a result, no two systems will be implemented the same way.

The design methodology presented in this chapter uses a building-block approach. If the system you are designing is based on a single CCU, you need only read and learn about the guidelines presented in *Basic System Design* on page 74. If you need multiple CCUs or CAPs to satisfy your network requirements, you must perform a much more detailed engineering design based on the general guidelines provided in *Multi-CAP RF Network Design Considerations* on page 81.

For purposes of illustration, coverage areas are presented using the popular cellular hexagonal coverage pattern. In practice, radio coverage does not conform to hexagonal shapes; however, hexagons are used to represent radio coverage because graphically, they can fully cover a plane surface and because they provide an easy-to-understand representation of coverage cells.

5.2 Basic System Design

Basic system design guidelines apply to all LMS4000 system implementations, from a simple, single-CCU system, to more complex multi-CCU CAPs and multi-CAP networks.

5.2.1 Overview of Basic System Design

The basic design of the LMS4000 900 MHz radio network involves the following procedures:

- Conducting a spectral survey to identify, quantify, and assess the impact of existing in-band and out-of-band interference.
- Determining single- or multi-CAP system requirements based on RF coverage, CAP locations, and system loading.

5.2.2 Spectral Survey of the Target Service Area

Before starting the system design, WaveRider recommends conducting a spectral survey of the target serving area to determine the radio landscape—that is, to determine if there are any in-band or out-of-band interferers and how, and to what degree, these interferers constrain your system design (site location, frequency, equipment).

The spectral survey involves travelling to key locations throughout the target serving area, especially to locations that may be potential CAP sites, or where there are significant numbers of potential end users, and recording the radio spectrum (ISM band +/- 10 MHz) at each of these locations. The survey requires the use of a spectrum analyser and a trained RF engineer who is capable of interpreting the results. There are a number of independent RF engineering firms that can provide this service, including the WaveRider Professional Services Group. If you have access to the required equipment and in-house skill set, you can also conduct this survey yourself.

NOTE: If you do not have access to the required equipment or skill set, you can use the CCU/EUM Spectrum analyser feature to conduct the spectral survey. See *Spectrum Analyser* on page 92 for details.

The spectral survey is a critical first step in the system design. Not only does it provide the starting point for the RF network design, it establishes a baseline for the use and occupancy of the spectrum. Keep in mind that one of the major attractions of the ISM band is the fact that it is license free; as such, it is shared spectrum. To regulate the band, regulatory bodies, such as FCC and Industry Canada, require that new operators in the band take responsibility for resolving interference issues when their newly installed system interferes with systems that are already in operation. The spectral survey identifies systems that are operating in the ISM band and establishes a documented baseline, which may provide you some protection from future ISM-band installations that interfere with the operation of your system.

It cannot be overemphasized that radio communications is, by nature, a non-static environment. As a wireless ISP, the more you know about the RF environment in which you are operating, the better prepared you will be to address future service-affecting changes in this environment. Given that the RF environment is dynamic, WaveRider recommends performing spectral surveys on a regular basis, perhaps every 3-6 months.

5.2.3 In-band Interference

In-band interference occurs when other wireless systems are operating in the same band and in the same geographical area as your system. The impact of in-band interference may be limited—that is, the unwanted signal level may be so low as to have no impact at all, or it may only affect service to a single end user or a small number of end users. In-band interference may, however, be system wide, particularly if it is geographically dispersed around your serving area or it is in close proximity to the CAP. System-wide interference obviously causes the most impact to system operation since it affects all end-users in the serving area.

A primary purpose of the spectral survey is to identify in-band interference so that, if it is present, the RF network design can address the interference sources through careful location of the CAP, equipment configuration, and frequency selection, with the goal of maximizing the ratio of the desired to the interfering signals throughout the serving area. If these measures are not adequate, channel filters can in many cases reduce the interference to levels within the operating tolerance of the LMS4000 radio equipment. Channel filters are discussed in *Using Bandpass Filters at CAP Sites* on page 77.

5.2.4 Out-of-band Interference

The radio spectrum is a finite commodity, which in the growing world of wireless communications, means that all users must compete for this limited resource. The implication is that throughout the service life of your LMS4000 system, you need to be aware of your “RF neighbors” and the impact they may have on your system operation and performance. As described in *CCU–EUM Interface Physical Layer (DSSS Radio)* on page 35, the LMS4000 900 MHz product operates in the 902–928 MHz ISM band. In many areas of the world, including North and South America, the 900 MHz ISM band is sandwiched between the top end of the cellular radio band and the bottom end of the commercial paging band.

Cellular radio and paging systems are common in many regions, so you must take precautions when planning your LMS4000 900 MHz radio network. Specifically, you need to know the location of all cellular and paging transmitters that are in, close by, or planned for, your serving area, so that you can limit the impact of these potential interferers through proper site location, equipment configuration, and frequency selection.

Figure 36 shows an actual spectral sweep, recorded using a spectrum analyser as part of a spectral survey, which shows the location of the cellular and paging transmitters in relation to the ISM band. Note the relative levels of the interfering signals.

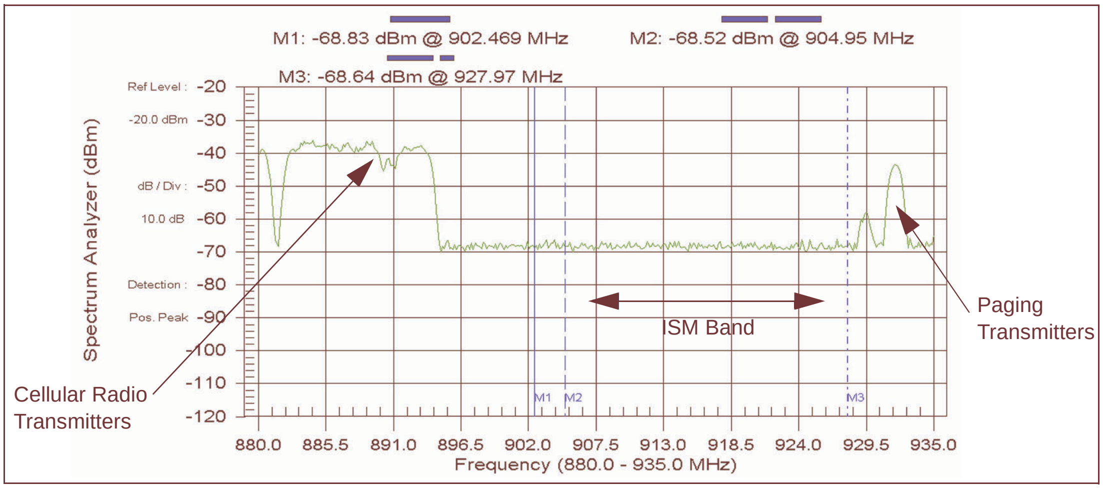


Figure 36 Example of a Spectral Sweep

Cellular and paging systems in the bands adjacent to the ISM band can interfere with your network and need to be addressed as follows:

- Identify and quantify all potential sources of interference by conducting and applying the results of the spectral survey.
- If your CCUs or EUMs are close to cellular or paging sites, their receivers may be desensitized by the high levels of the interfering transmitters, which can operate at very high levels (100 W per cellular radio carrier, 1500W for paging transmitters). To provide service to these EUMs, choose an operating frequency that is as far from these cellular and paging transmitters as possible.

  Try to assign frequencies that are not adjacent to the cellular or paging channels identified in your serving area. Consider the scenario illustrated in Figure 37. As shown, a cellular tower is located in sector A of the LMS4000 radio network. Since cellular frequencies are located just below the ISM band, a reasonable design approach would be to assign a higher frequency to sector A, such as 915 MHz or 925 MHz.

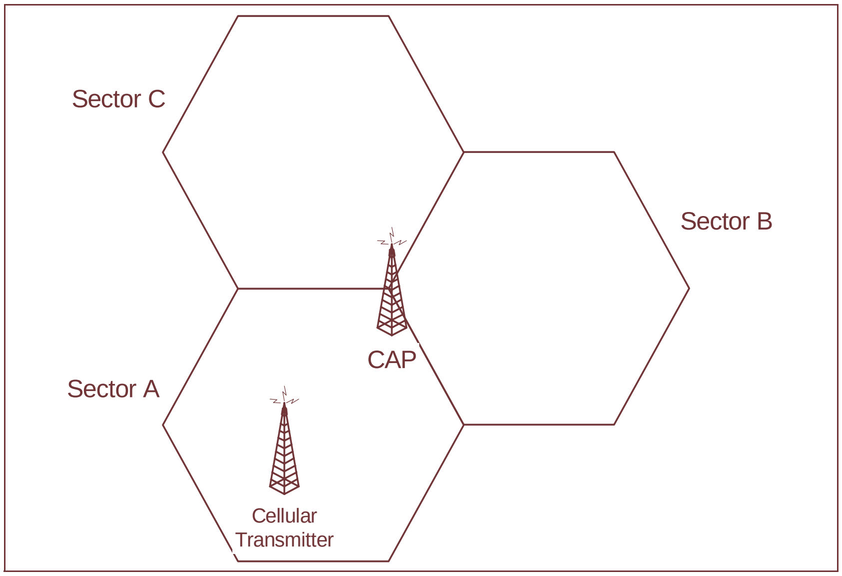


Figure 37 Network Design in the Presence of Out-of-band Interference

5.2.5 Using Bandpass Filters at CAP Sites

WaveRider provides high-quality, specially designed bandpass filters for use with the CCU. These filters reduce the effect of unwanted out-of-band and off-channel in-band interference.

As discussed in *Propagation Path* on page 38, it is highly desirable to locate the CAP site so that the CCU antennas are high enough to provide clear line of sight paths to the maximum number of EUMs in the serving area. The goal is to make sure the CCU can see the maximum number of EUMs and conversely, to make sure the maximum number of EUMs can see the CCU.

Attaining this goal, however, has a consequence since it may mean the CCU will be in an ideal location to see interferers in its sector as well. Bandpass filters at the CCU reduce the effect of interference from out-of-band or off-channel in-band interferers.

On-channel interference may result from

- on-channel interferers in the ISM band, or
- transmitter phase noise or intermodulation products generated by out-of-band interferers.

Bandpass filters cannot resolve on-channel interference; instead, you must change to a more suitable CCU operating frequency.

For CAP sites in which multiple CCUs are installed, use of bandpass filters to ensure non-interfering operation of CCUs is mandatory. It is important to remember that in the 900 MHz ISM band, the radio transmit and receive occur on the same frequency and use Time Division Duplexing (TDD) to switch between the transmit and receive cycles. Multi-CCU installations pose the highest threat of CCU to CCU adjacent channel interference. For the RF network engineer, as specified in Appendix A Specifications, the minimum separation between co-located channels is 6.6 MHz (an orthogonal adjacent channel) and requires a C/I ratio of 50 dB or better for non-interfering CCU operation. Once the antenna system gains and power output of the CCU radio are accounted for, the only way to practically provide adequate isolation for the required adjacent channel isolation is through the use of bandpass filters.

5.2.6 Single- or Multi-CAP Implementation

An important step in basic system design is to determine if a single CAP site adequately covers your target serving area, or if a second CAP site, or multiple CAP sites, will be required. The main factors that drive this decision are the RF coverage and the system loading.

RF Coverage

The RF coverage of the sector is a function of many different factors.

Commercially available radio coverage prediction software calculates radio coverage based on the following factors:

- Propagation characteristics (frequency, distance from the site)
- Radio characteristics (transmit power, receiver sensitivity)
- Antenna system and height
- Topography
- Clutter

Using this coverage prediction software, a qualified RF design engineer is able to produce RF coverage estimates. Again, there are a number of independent RF engineering firms that can provide this service, including the WaveRider Professional Services Group. If you have the required software and in-house skill set, you can perform this coverage analysis yourself.

The location of the CAP site in relation to the serving area determines whether the site will be a corner- or center-illuminated cell. Figure 38 illustrates the difference between these two methods of illumination.

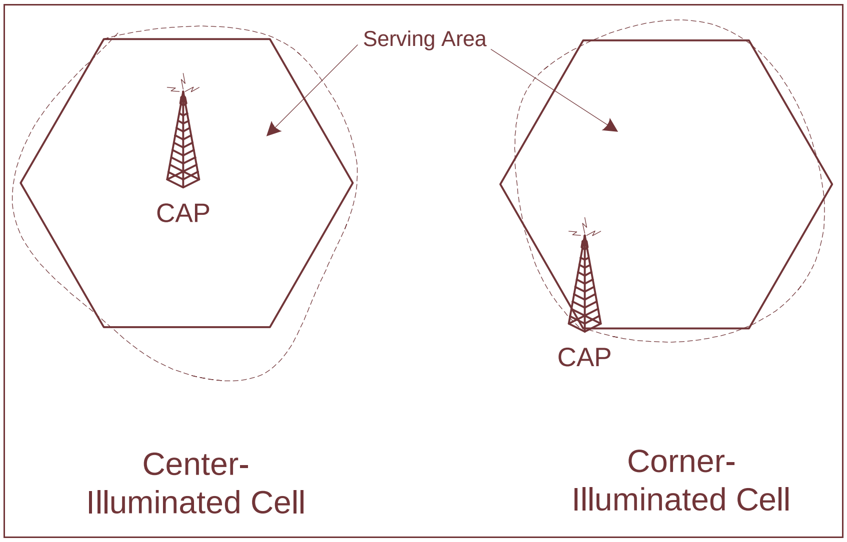


Figure 38 Corner- and Center-illuminated cells

Although the difference between the two approaches may seem academic at first, the choice you make affects the system design, in particular, the selection of sites, site antennas, and the system growth path.

Center Illumination

A center-illuminated cell is generally the simplest to implement. In this case, a site is established at a suitable location near the middle of the target serving area. An omnidirectional antenna is usually installed to deliver 360-degree coverage around the site.

When system traffic increases beyond the capacity of a single CCU because, for example, many subscribers have been added to the system, more CCUs can be added to the CAP site (up to a total of three operating CCUs per CAP site). The omnidirectional antenna would, in this case, be replaced with sectored antennas, for example, three 120-degree sectored antennas. The selection of the sectored antennas would depend on how evenly the subscribers are distributed throughout the serving area. In this example, the resulting configuration would triple the traffic-handling capacity of the site. Figure 39 illustrates the sectoring of a previously center-illuminated omnidirectional cell.

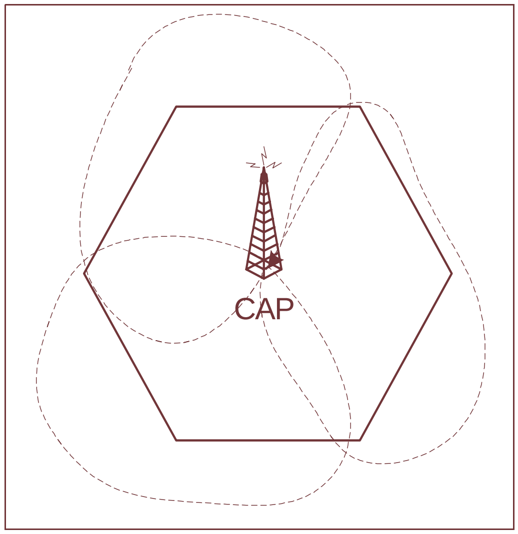


Figure 39 Sectored Cell

Corner Illumination

Corner illumination is generally used when it is not possible to establish a suitable CAP site near the middle of the target serving area. Implementation of a corner-illuminated cell requires more extensive site and system engineering than does the implementation of a center-illuminated cell. This is particularly true when additional traffic-handling capacity is required, since techniques such as overlay/underlay sectors (adding a second CCU to provide coverage to the same geographical area) may have to be applied.

The use of omni-directional antennas at CAP sites, although simple in implementation, is only recommended for simple network installations with low risk of interference and limited exposure to other sites. Omni-directional antennas, by definition, are designed to provide coverage in all directions (360°) horizontally around the antennas. This wide angle-of-view provides for simplicity of an omni-directional antenna installation but also means that the omni-directional antenna is susceptible to any interference in the area. As such, the RF network designer, when faced with interference or system expansion will generally need to replace the omni-directional antenna(s) (and possibly multiple CCUs) in order to serve the same coverage area and to make use of the directional properties of the antennas to address system issues.

System Loading

Sometimes, even with well-engineered RF coverage, the user traffic may be so high that you need to expand the network to a multi-CAP system.

The answer to the question “How many subscribers can each CCU support?” is a qualified “It depends.” Refer to *Performance Modelling* on page 47 for a description of the method used by WaveRider to predict the number of end-users that can be supported by the LMS4000 network. Total system traffic is very dependent on the usage profile of the end users and the tariff structure that has been implemented by the system operator. For instance, an LMS4000 900 MHz system that is providing service to a number of small businesses, each supporting multiple users, likely generates a lot more daytime traffic than a simple residential service used for Web browsing and email.

In summary, the network design engineer must be aware of the intended use of the system — the customer profile, tariff rates, and committed grades of service — since these factors all influence the traffic demand on the system.

5.3 Multi-CAP RF Network Design Considerations

One of the differentiating features of the LMS4000 900 MHz radio system is its ability to support multi-CAP networks. The design of multi-CAP networks is significantly more complex than the design of single-CCU or single-CAP systems. WaveRider highly recommends the use of a qualified RF engineering firm, such as the WaveRider Professional Services Group, to carry out multi-CAP system design. If you are confident that you have the required skill set available in house, you can carry out this design yourself.

5.3.1 Multi-CAP Network Design Process

The process for designing a multi-CAP network can be summarized as follows:

1. Conduct a preliminary site survey and selection.
2. Apply a frequency grid to the sites that you have selected.
3. Determine the site-to-site signal levels by
   - Determining site-to-site distances,
   - Calculating site-to-site propagation loss,
   - Normalizing the signal levels at each site, and
   - Factoring in the antenna isolation.
4. Using the C/I information presented in *Carrier–to–Co-channel Interference Ratio Requirements* on page 82, formulate a frequency plan and channel assignment.
5. Perform and apply antenna down-tilt calculations.
6. Assess the impact of known in-band and out-of-band interferers.
7. Verify and iterate the design as many times as necessary.

This chapter does not provide detailed instructions on how to carry out each of the above tasks as it is beyond the scope of the document. It does, however, provide you with the LMS4000-specific information that you or your RF engineering firm need to be able to carry out the above steps.

5.3.2 Frequency Selection — Standard Frequency Set

LMS4000 900 MHz equipment (CCUs and EUMs) can operate on all channels from 905 to 925 MHz, in increments of 0.2 MHz (refer to Table 1 on page 36 for channelization information). Throughout this manual, however, WaveRider has referred to the standard frequency set shown in Table 5.

Table 5 Standard Frequency Set

905.0 MHz
915.0 MHz
925.0 MHz

The standard frequency set represents a convenient and safe set of frequency assignments. The frequencies are orthogonal in that they do not overlap, and they provide enough separation between the frequencies so that one channel does not interfere with either of the other channels, even if they are installed at the same CAP site with appropriate filters. Using the standard frequency set, you can implement small systems without much concern for self-generated interference.

In the case of a multi-CAP network, however, the standard frequency set may not be inadequate. Instead, you must use other sets of frequencies at neighboring CAP sites. The selection of these other frequency sets is governed largely by the minimum C/I requirement for the CCU and EUM radio; i.e., the amount of interference, from within or from outside the system, that the LMS4000 radio equipment can tolerate.

5.3.3 Carrier–to–Co-channel Interference Ratio Requirements

The CCU and EUM carrier–to–co-channel interference ratio (C/I) requirements are outlined in Table 6.

Table 6 Required C/I Ratio for Multi-CAP Design

C/I Ratio	Frequency Separation	PER
22 dB	0.2 MHz	$\leq$ 1%
19 dB	1.6 MHz	$\leq$ 1%
11 dB	3.4 MHz	$\leq$ 1%

As shown in Table 6, as the frequency separation between the desired LMS4000 signal and an interfering LMS4000 signal increases, the level of an interfering signal that can be tolerated also increases. Consider the case where the frequency separation between the desired channel and an interfering channel from a remote site is 0.2 MHz. To maintain a packet error rate of 1% in the local cell, you would need to ensure that the EUMs in the local cell are receiving the desired CCU signal at a level which is at least 22 dB higher than the interfering CCU signal, 0.2 MHz away.

Using this information, and information about the number and location of the required CAP sites, your RF designer should be able to define a frequency plan for your system.

As an example, consider the frequency plan shown in Table 7.

Table 7 Sample Frequency Plan — Multi-CAP Design

Frequency Set A	905.0	-	911.6	-	918.4	-	925.0
Frequency Set A'	-	908.4	-	915.0	-	921.6	-

In Table 7, *Frequency Set A* uses the minimum frequency spacing that should be considered for a single CAP site, 6.6MHz. *Frequency Set A'* represents a set of channels which are interstitial to those in *Frequency Set A*. The channels in *Frequency Set A'* fall midway between the channels in *Frequency Set A* yet still adhere to the minimum recommended spacing between any two co-located channels, 6.6MHz.

From Table 6, if two sites have a frequency separation of 3.4 MHz (*Frequency Set A* to *Frequency Set A'*, for example), a C/I signal margin of 11dB is required.

CAUTION: The concept of frequency reuse patterns, commonly used in the design of cellular radio systems, cannot be directly applied in the design of LMS4000 900MHz radio networks. Instead, due to the nature of the Polling MAC, you should never reuse frequencies in networks where a CCU or EUM can receive a signal from a unit in another sector or coverage area. The minimum channel separation cannot be less than 0.2MHz. When Polling MAC is applied in a multi-CAP environment, it is possible for an EUM to inadvertently lock onto the signal from a remote CCU if that CCU is operating on the same frequency. This situation does not occur if the remote CCU is offset by 0.2MHz or more from the local CCU, and the required C/I ratio is maintained. In summary, no two CCUs in a single network can be assigned exactly the same frequency .

5.3.4 Dealing with External Interference

Up to this point, the discussion has been concentrating on the effect of self-generated interference—that is, interference between CAPs or EUMs in the same network.

As indicated in *Basic System Design* on page 74, you must also account for the effect of external interferers such as cellular and paging systems. The RF system design engineer needs to make sure external interference sources do not affect system operation. You can use a similar treatment to the one developed above for self-generated interference to assess the effects of external interference sources.

5.3.5 Verifying the Design

No matter how carefully the system has been designed, you must verify the system in the field before turning it up to ensure network operation is consistent with the design standards set out by the system design engineer. With this in mind, your system implementation plan must provide enough time and resources for the engineering team to verify the design in the field through testing and signal-level measurements.

Once you have established your CAP sites on the air, you can verify received signal levels throughout the network using a portable spectrum analyser. You can then compare these with those predicted by the RF system design. In many cases, discrepancies between predicted and actual results can be corrected, if necessary, through adjustment of antenna azimuths and/or down-tilting.

As the system grows and capacity is added, the frequency plan may have to be adjusted and more attention given to fine-tuning the isolation between CAP sites.

Verification Checklist

When reviewing and verifying the design of a multi-CAP network, here is a checklist of items that might be considered:

- General system design considerations:
  - Paging transmitters
  - Cellular transmitters
  - In-band interference
  - Frequency assignments
- CAP-to-CAP frequency assignments and isolation, achieved through
  - Lowering antenna heights,
  - Antenna mounting, and the use of mounting structures to achieve greater isolation (building, towers),
  - Antenna radiation patterns (directionality and side lobes), and
  - Antenna characteristics, back to front isolation.
- CAP-to-EUM propagation must provide coverage to all EUMs from selected sites. Run the RF model with the specified system parameters to verify thorough propagation.

5.3.6 Summary of RF Design Guidelines

A summary of guidelines presented in this chapter can be found in Table 8.

Table 8 Summary of RF Design Guidelines

DO	DO NOT
• DO read and understand this chapter before you start your system design activity. • DO contact WaveRider Professional Services Group if you need assistance with spectral surveys, RF coverage analyses, or system engineering. • As a first step, always DO a spectral survey. • DO understand the RF environment in your serving area, and DO learn as much as you can about potential sources of interference. • DO verify your system design through field testing, prior to turning up the service to end users. • DO try to design your system to take advantage of your existing real estate or radio sites. • DO use bandpass filters to reduce the effect of off-channel in-band and out-of-band interference. • DO use different frequency assignments or take advantage of antenna patterns to address on-channel interference. • Wherever you can, DO use the standard frequency set. • In the design of multi-CAP networks, DO maintain the required C/I ratio shown in Table 6 on page 82. • In a multi-CAP network, DO use a minimum frequency offset of 0.2MHz between CCUs. • DO migrate from an omnidirectional to a sectored cell when your traffic warrant it, or interference is an issue.	• DO NOT assume a static RF environment. • DO NOT install the CAP site in proximity to in-band or out-of-band interferers. • DO NOT install the CAP site in a low area, or area surrounded by clutter and obstructions. • DO NOT use frequencies that are close to the edges of the ISM band if you have identified cellular and paging transmitters above or below the band. • DO NOT ignore the usage patterns of your end users when designing your network. • DO NOT assign the same frequency to two or more CCUs in your network.

6 Installation & Diagnostic Tools

The CCU and EUM are equipped with the following features that facilitate unit installation, operation, maintenance, monitoring, and diagnostics:

CAUTION: When entering IP addresses in the CCU or EUM, note that a leading ‘0’ forces the CCU or EUM operating system to interpret the entry as octal rather than decimal. For example, pinging 10.0.2.010 actually pings 10.0.2.8

6.1 Indicators and Connectors

The CCU and EUM are equipped with LED indicators that provide a visual indication of the status of the unit and its interfaces. The EUM LED indicators are illustrated in Figure 41, the CCU LED indicators in Figure 42, and a detail view of the Ethernet connector in Figure 43.

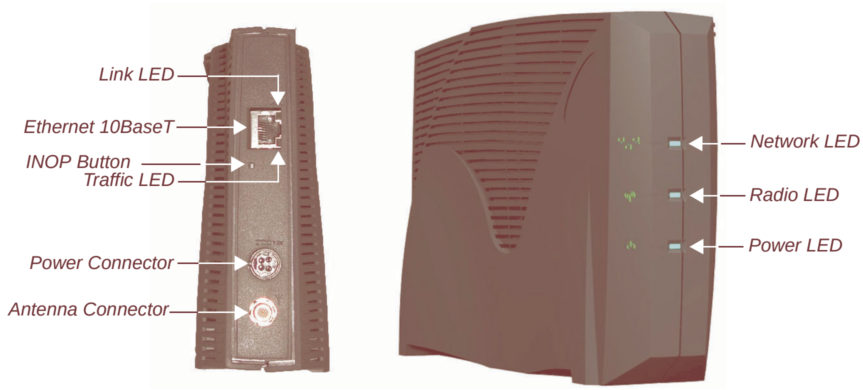


Figure 40 EUM3003 LEDs and Connectors

Figure 41 EUM3000 LEDs and Connectors

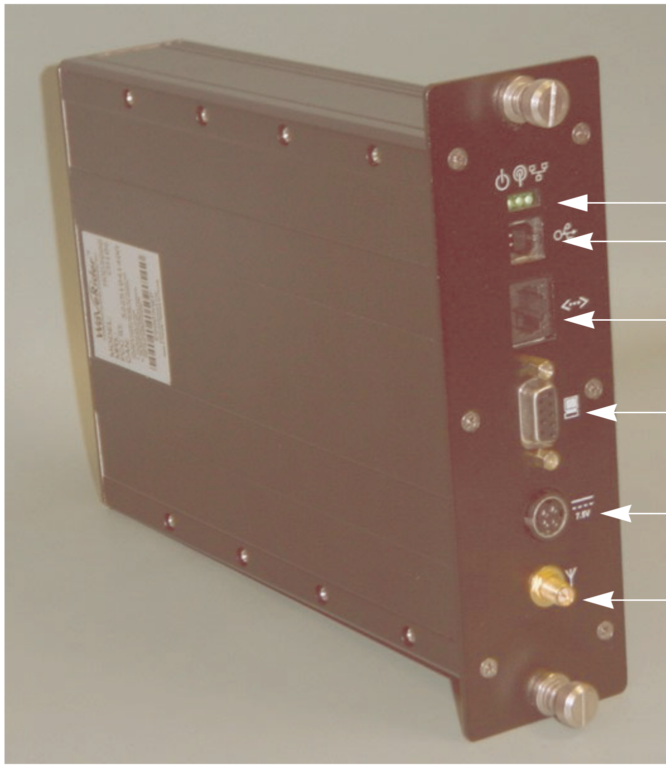


Figure 42 CCU LEDs and Connectors

The LEDs are described below:

6.1.1 Network LED

Table 9 Network LED

LED State	Ethernet Traffic Status
OFF	No Ethernet traffic present
Slow Flash	Ethernet traffic present but no radio traffic
Fast Flash	Ethernet and radio traffic present

NOTE: A Network LED *fast flash* flashes at 2.5 Hz, 50% duty cycle, about two or three times per second.

6.1.2 Radio LED

In the following table, RSS is the Radio Signal Strength, in dBm.

Table 10 Radio LED

LED State	RSS Value
OFF	No radio signal present
Slow Flash	Receive Threshold < RSS < -80 dBm
Fast Flash	-80 dBm $\leq$ RSS < -70 dBm
ON Solid	RSS $\geq$ -70 dBm

NOTE: A Radio LED *slow flash* flashes at 0.83 Hz, 33% duty cycle, about once per second. A Radio LED *fast flash* flashes at 2.5 Hz, 50% duty cycle, about two or three times per second.

6.1.3 Power LED

Table 11 Power LED

LED State	Power Status
OFF	No power
ON	Power

6.1.4 Ethernet LEDs

The Ethernet connector used in the CCU and EUM, shown in Figure 43, has two LEDs. These LEDs are described in Table 12.

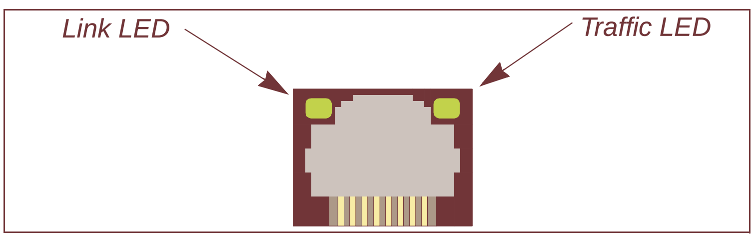


Figure 43 Ethernet LEDs

Table 12 Ethernet LEDs

LED State	Ethernet Status
Link LED	If the Link LED is ON, the Ethernet physical connection is configured and working properly. If the Link LED is OFF, then the Ethernet physical connection is not working properly, which could be because the wrong type of cable was used (a straight-through cable at the EUM instead of a crossover cable) or there is a problem with the host or device Ethernet interface.
Traffic LED	The Traffic LED flashes whenever the link is transferring data.

The CCU is equipped with the same LEDs as the EUM but in a slightly different physical configuration. As shown in Figure 42, the CCU indicator LEDs are closely grouped and are, in order left to right: Power LED, Radio LED (not used on CCU), and Network LED.

6.2 Command-line Interface

The CCU and EUM are equipped with a simple command line interface through which you can monitor unit status and configure all unit parameters. The command-line syntax is defined in Appendix C on page 189.

The command-line interface can be accessed

- locally or remotely, using a Telnet session, or
- directly, through the DB-9 console port on the CCU, using a PC equipped with terminal emulation software, using the console settings specified in Table 13.

Table 13 Console Settings

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow Control	None

6.3 EUM Configuration Utility

The EUM can also be configured and monitored using the EUM Configuration Utility, a Windows-based graphical user interface (GUI) running on a PC. The PC connects to the EUM through the unit Ethernet port or from anywhere in the LMS4000 900 MHz Radio Network. The EUM Configuration Utility and *EUM Configuration Utility User Guide* can be downloaded from the WaveRider Web site at www.waverider.com.

6.4 Spectrum Analyser

On the CCU or EUM, the `radio analyse` command forces the radio to step across the frequency band. At each frequency, it will measure and report the peak, average and noise floor powers. It will also report the presence and level of any packets received from a WaveRider CCU3000 or NCL1900. The radio analysis is configured using the parameters described in Table 14:

Table 14 Radio analyser Configuration Parameters

Parameter	Description
Samples	The number of RSSI and noise floor samples taken at each frequency. *Samples* affects the accuracy and duration of the measurement. The default value is *200*. The maximum RSSI reported is the largest of the RSSI samples, the average RSSI reported is the mean of the RSSI samples, and the noise floor reported is the maximum of the noise floor samples. **NOTE:** Samples are not synchronized to any packet transmissions or receptions. Since many transmission sources, including WaveRider systems, transmit intermittently, there is the possibility that sources may not be transmitting when the samples are taken, and that they will subsequently be missed.
Interval	The step size between sample points. The default is *2* (200 kHz), which is also the minimum step size allowed. The maximum interval is *200* (20 MHz). **NOTE:** Although the step size can be set in 100's of kHz, odd frequencies (9053 and 9057 MHz, for example) will always be rounded down (to 9052 and 9056 MHz, in the preceding example).
Start	The lowest frequency sampled, in 100's of kHz. The default is *9000* (900.0 MHz), which is also the minimum allowed. This minimum value is outside the allowed transmit range of the EUM and CCU, which is permitted since the radio does not transmit during spectrum analysis. This provides the operator with information about interference near the band edge, which can aid in the identification of any interferers.

Parameter	Description
Stop	The upper boundary on frequencies sampled, also in 100's of kHz. The default is *9300* (930.0MHz), which is also the maximum. Again, this is outside the allowed CCU and EUM transmission range.

To configure the above parameters, enter the following in the command line:

```
radio analyse <samples> <interval> < start> <stop>
```

For example:

```
radio analyze 100 10 9000 9300
```

will program the Spectrum Analyser to take 100 samples at every frequency, in 100 kHz steps, starting at 900 MHz and ending at 930 MHz. If you leave any parameters off the list, they will be set to the default. In the above example, entering

```
radio analyze 100 1
```

would have had the same effect, since *9000* is the default value for Start, and *9300* is the default value for Stop.

The CCU RSSI that is reported by the Spectrum Analyser is the level of any packets received from a WaveRider CCU3000 or NCL1900. Unlike other measurements, it is synchronized with packet reception. Only the value of the last packet received is shown.

NOTE: For each CCU detected, three points will be shown - the center frequency, and the upper and lower band edges (± 2.8 MHz).

A comment can be added to the analysis using the `radio comment` command. This comment will also be displayed on the graph. For example, entering the following in the command line:

```
radio comment Site 1 Spectral Analysis
```

will display "Site 1 Spectral Analysis" in the line below the date and time.

The command `radio analyse last` will redisplay the results of the last analysis that was performed.

A graphical display of the results is available as a PDF (Adobe Portable Document Format) document called `specan.pdf`, which can be retrieved from the modem through FTP:

```
-> ftp 192.168.10.250
Connected to 192.168.10.250.
220 FTP server ready
331 Password required
User: s
331 Password required
Password:******
230 User logged in
ftp> bi
200 Type set to I, binary mode
```

```
ftp> get specan.pdf
local: specan.pdf remote: specan.pdf
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
6394 bytes received in 0.04 secs (171.3 kB/s)
ftp> bye
```

NOTE: Click here to obtain a copy of Acrobat Reader from the Adobe Web site.

Examples of Spectrum Analyser graphical displays are shown in Figure 44, Figure 45, and Figure 46.

Figure 44 (Spectral Analysis - Example A) illustrates the spectral analysis from one of three co-located CCUs, each equipped with a bandpass filter, in a quiet RF environment.

Figure 45 (Spectral Analysis - Example B) illustrates the spectral analysis from an EUM that is near a site with four co-located CCUs, each equipped with a bandpass filter, in a quiet RF environment.

Figure 46 (Spectral Analysis - Example C) illustrates a spectral analysis from a CCU, without a bandpass filter, at an extremely congested RF site. It shows two very large interferers, at the upper and lower ends of the band. This (actual) installation is running well with more than 20 EUMs at 915 MHz, with a bandpass filter installed.

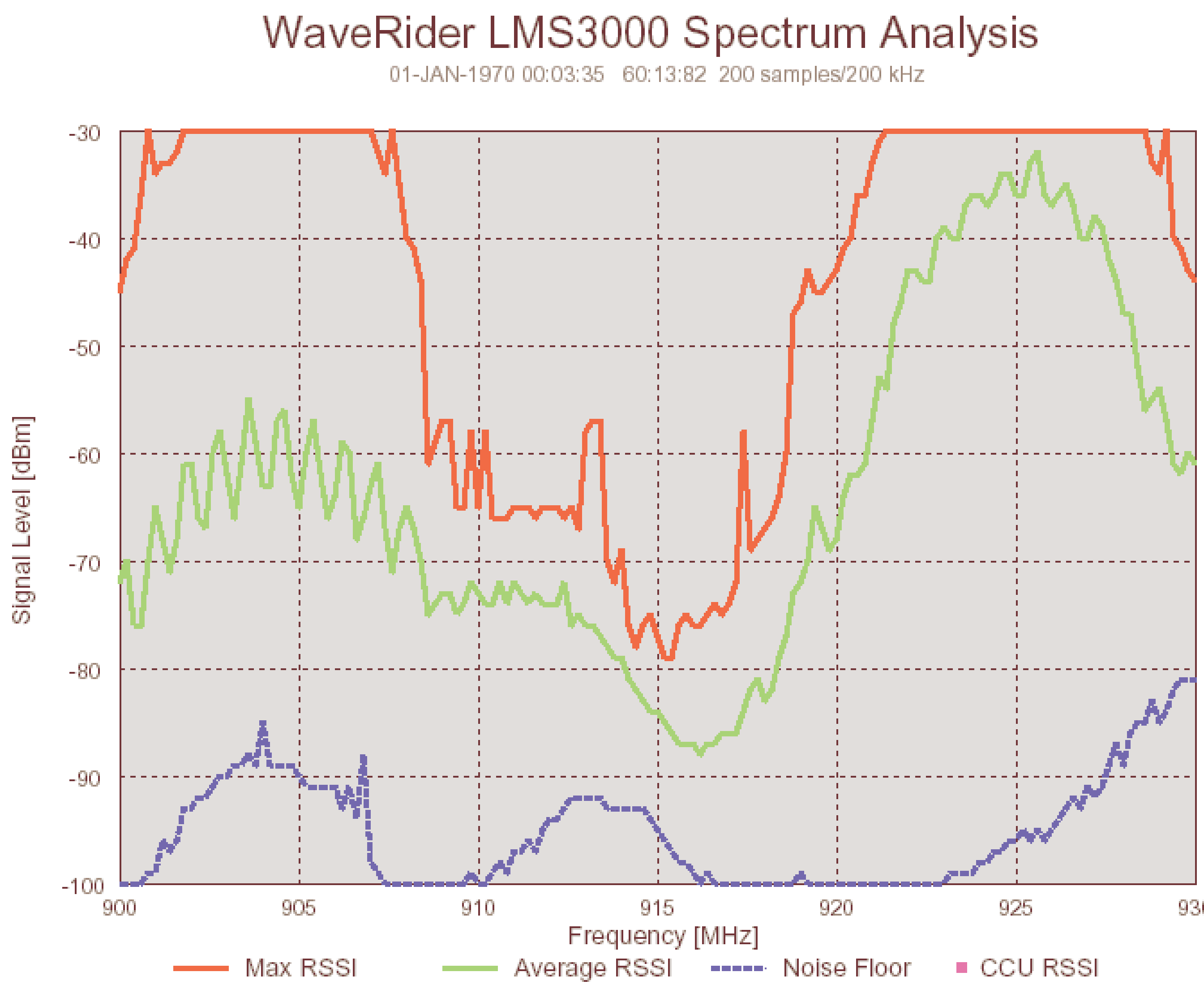


Figure 44 Spectral Analysis - Example A

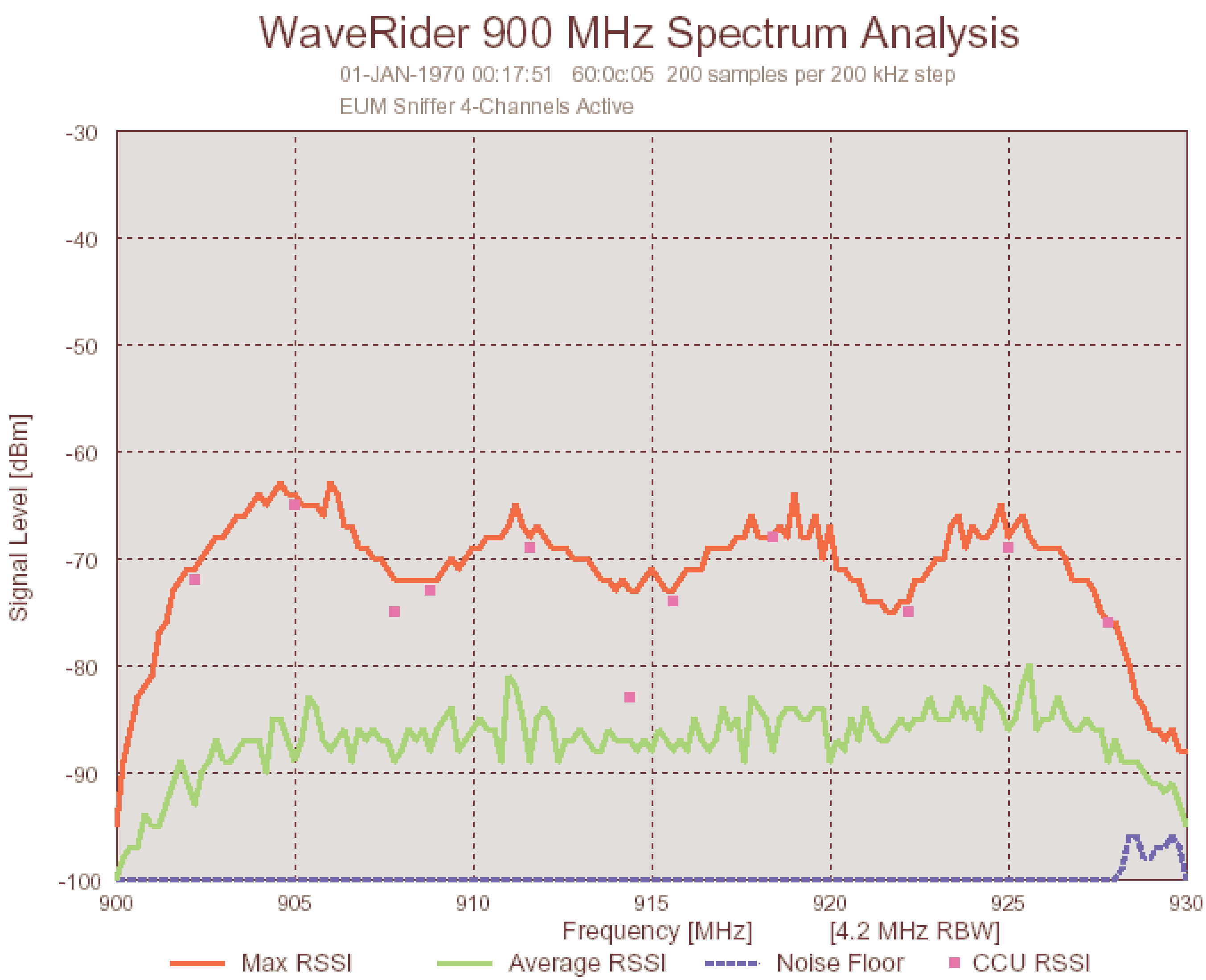


Figure 45 Spectral Analysis - Example B

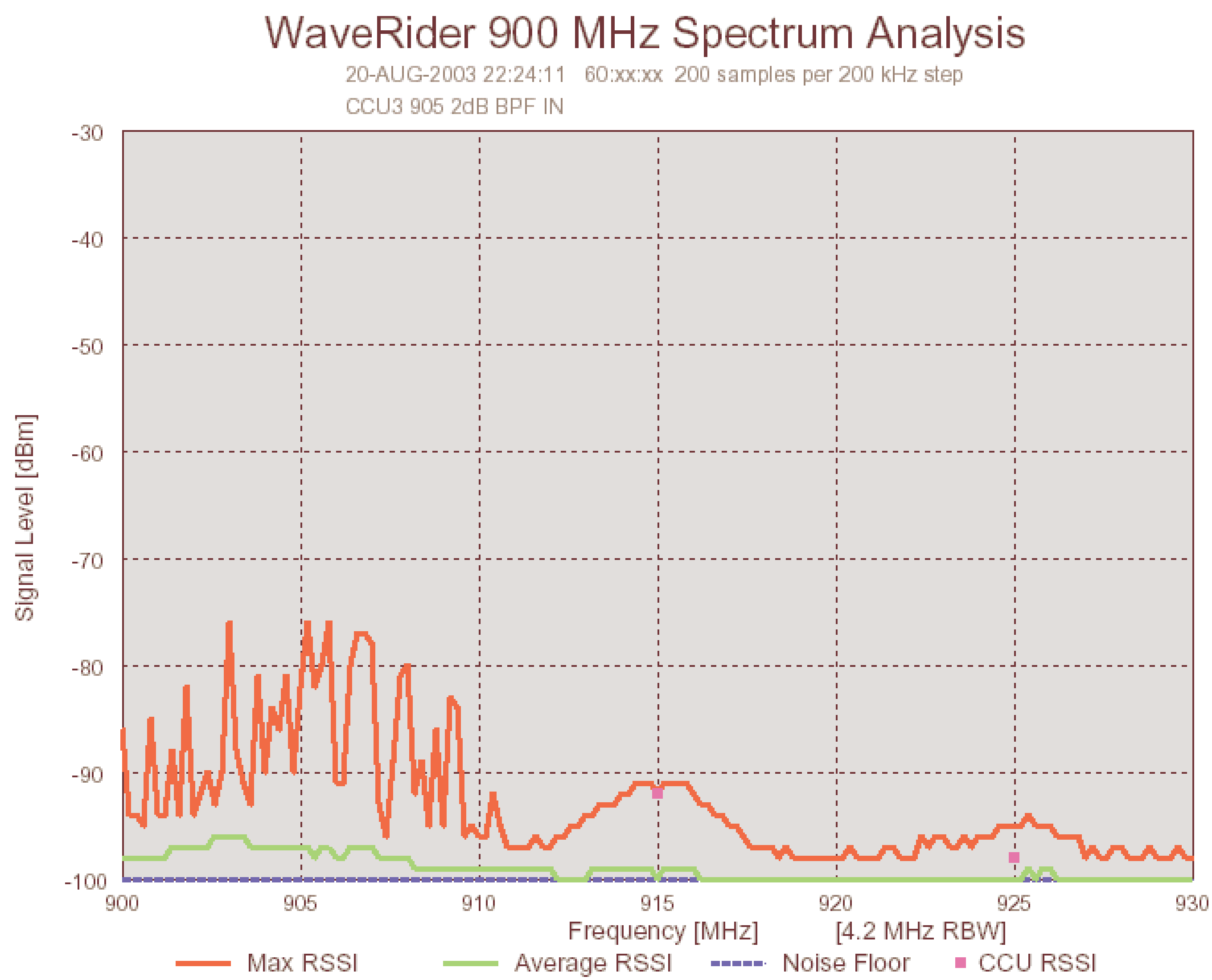


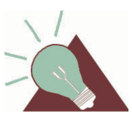
Figure 46 Spectral Analysis - Example C

To analyze and interpret the spectral graph, use the following guidelines:

1. If the Average RSSI (green dashed line) is greater than -40 dBm, use an external filter at the output of the EUM or CCU. The EUM/CCU operating frequency should be at least 10 MHz away from any signal that has an Average RSSI greater than -40 dBm.
2. If the Max RSSI (red solid line) is more than 15 dB above the Average RSSI (green dashed line), then the usable EUM signal, for normal airlink operation, will be 10 dB above the Average RSSI.
3. If the Max RSSI (red solid line) is less than 15 dB above the Average RSSI (green dashed line), then the usable EUM signal, for normal airlink operation, will be greater than the Max RSSI (red solid line).

When interpreting the display, it is important to remember that the spectral measurements are made with the same filters used in normal data reception. Therefore, the signal level measured at each point includes all interference that will be experienced by the modem when set to that frequency. It is not correct to “fold-in” energy from adjacent frequencies as this has already been done. The resulting resolution bandwidth result is approximately 4.2 MHz.

NOTE: Spikes that appear in the spectral output are most likely sampling artifacts, caused by intermittent transmitters that became inactive by the time the Spectrum Analyser moved on to neighboring frequencies.



TIP: During the analysis, the radio link is disabled. If you run a spectral analysis from a CCU, no data will flow to, or from, any EUM in that sector during the analysis. Traffic will resume immediately after the analysis is complete. Similarly, if you run an analysis from an EUM, no traffic will flow to, or from, that EUM during the analysis. Other EUMs are not affected. As a result, if you start an analysis from a telnet session that uses the data link, no results will be reported and the session will not respond until the analysis is complete. Once it is complete, all of the results will show up at once.

If the radio link is disabled before the analysis is done (with `radio disable`), it will remain disabled afterwards.

6.5 RSSI, Signal Quality, and Antenna Pointing

The EUM Radio LED and the continuous Receive Signal Strength Indication (RSSI) reading provide an indication of the level of the signal received from the CCU and an excellent tool for locating and aligning the EUM antenna. Since the system is based on a polling MAC, there will always be a signal to receive and monitor from the CCU.

Table 15 Radio RSSI Data

Data	Description
dBm	Received radio power measured in dBm.
RX	The number of polls received from the CCU. A number between 16 and 700 is normal.
TX	The number of payloads transmitted and acknowledged on the first try from this EUM. This number will always be 0 unless there is some traffic from the EUM to the network.
R1	The number of payloads transmitted and acknowledged on the second try from this EUM, implying that the first transmission was not acknowledged (i.e., failed).
R2	The number of payloads transmitted and acknowledged on the third try from this EUM, implying that the first two transmissions were not acknowledged (i.e., both failed).
R3	The number of payloads transmitted and acknowledged on the fourth try from this EUM, implying that the first three transmissions were not acknowledged (i.e., all failed).
F	The number of payloads not acknowledged after the fourth try from this EUM. The payload was discarded.
Retry %	Total percentage of packet retries over the total number of sent packets.
SQ	SQ is a measure of signal quality. The lower the value, the better. For EUM and CCU installations, an average value of *8* or less is good. The “rad rh” command displays a histogram of SQ values, which indicates the long term quality of the link. It is acceptable to have occasional values of SQ that are greater than 8, however, if SQ is consistently above 8, this suggests the radio has trouble tracking the carrier signal, possibly due to severe multipath or interference, or low signal-to-noise ratio.
RNA	RSSI Noise A (RNA) is an estimate of the signal to noise ratio at the A antenna in dB. Values above 20 indicate a good signal to noise ratio, while links with values below 15 are likely to experience significant packet error rates.
RNB	RSSI Noise B (RNB) is the same as RNA above, except it applies to antenna B.

The procedure for aligning the EUM antenna is discussed in more detail in *Positioning the Antenna* on page 149.

Table 16 Signal Quality Checks

Retry Rate	Average SQ	RNA RNB	RSSI	Indication
High	≤ 8	< 20	Low (<-80 dBm)	Poor signal.
High	≤ 8	< 20	Good (>-80 dBm)	Possible multipath or interference. If RNA and RNB are different, they may give an indication of the direction of the interferer.
High	> 8	< 20	Good	Possible severe multipath or interference problem.

6.6 Testing Connectivity Using the Ping Utility

The CCU and EUM include a ping utility to test for network connectivity, latency, and packet loss. The ping command sends an ICMP echo request to a specific destination and reports the round-trip time, number of bytes sent, and success or failure.

Installation testing requires you to use both short and long packet pings to confirm satisfactory packet error rates over the radio link. You can run this test from the command prompt at the customer PC connected to an EUM, assuming the PC is available and properly connected to the EUM.

The ping test accepts up to three arguments:

- address
- length (default is 64 bytes)
- interval (in milliseconds) (default is 490 milliseconds)

Enter the command arguments in the following order: ping <destination> <length> <interval>. If you omit either <length> or <interval>, the command will use the default settings.

Measuring Active Latency of a Connection

The standard DOS ping test transmits subsequent pings at one second intervals. Given the design of the Polling MAC, which moves an EUM from active to inactive status after 500 milliseconds of inactivity, this standard ping test does not accurately measure the connection latency for an active EUM. The ping utility on the CCU and EUM allows you to configure the time interval between repeated pings. The default time interval between pings on CCUs and EUMs is 490 milliseconds, less than the 500 millisecond interval after which the EUM status becomes inactive. This time interval allows the ping test to accurately measure the active latency of the connection.

Measuring Radio Link Connectivity

Different sized pings can help you gauge the quality of the wireless link. A good quality wireless link can pass large sized packets without any loss. If a link is of poor quality, small sized pings may be successful, while large sized pings may experience lost packets or packets that cannot transmit at all. CCUs and EUMs support pings with packets between 64 and 1460 bytes in length. A common practice is to ping a link with 64-byte packets and then with 1460-byte packets. You can then compare the success rate of the different ping sizes. The ping utility reports the packet loss rate after as many as four retries. In addition to monitoring the packet loss rate, you should evaluate the ping times. Transmit retry rates provide a better indication of the radio link quality.

To Measure Radio Link Connectivity by Pinging with 64-byte Packets

1. At the CCU, use the **`auth`** command to check that the EUM is authorized, either statically, through the default, or through RADIUS.
2. At the CCU, use the **`air`** command to check that the EUM is registered. (For more information, refer to *Registration Table (CCU only)* on page 240.)
3. At the CCU, type **`ping <aaa.bbb.ccc.ddd>`**, where **`<aaa.bbb.ccc.ddd>`** is the IP address of the EUM, and press **Enter**.

   Or, at the EUM, type **`ping <aaa.bbb.ccc.ddd>`**, where **`<aaa.bbb.ccc.ddd>`** is the IP address of the CCU, and press **Enter**.

```
60:03:3a> ping 192.168.22.2
Press any key to stop (time resolution: 16 ms)
PING 192.168.22.2: 56 data bytes
64 bytes from 192.168.22.2: icmp_seq=0. time=80. ms
64 bytes from 192.168.22.2: icmp_seq=1. time=48. ms
64 bytes from 192.168.22.2: icmp_seq=2. time=32. ms
64 bytes from 192.168.22.2: icmp_seq=3. time=32. ms
64 bytes from 192.168.22.2: icmp_seq=4. time=32. ms
64 bytes from 192.168.22.2: icmp_seq=5. time=48. ms
64 bytes from 192.168.22.2: icmp_seq=6. time=48. ms
64 bytes from 192.168.22.2: icmp_seq=7. time=48. ms
64 bytes from 192.168.22.2: icmp_seq=8. time=32. ms
64 bytes from 192.168.22.2: icmp_seq=9. time=32. ms
----192.168.22.2 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 32/43/80

60:03:3a>
```

To Measure Radio Link Connectivity by Pinging with the Maximum Packet Size

1. At the CCU, use the **`auth`** command to check that the EUM is authorized, either statically, through the default, or through RADIUS.
2. At the CCU, use the **`air`** command to check that the EUM is registered. (For more information, refer to *Registration Table (CCU only)* on page 240.)
3. At the CCU, type **`ping <aaa.bbb.ccc.ddd> 1460`**, where **`<aaa.bbb.ccc.ddd>`** is the IP address of the EUM, and press **Enter**.

   Or, at the EUM, type **`ping <aaa.bbb.ccc.ddd> 1460`**, where **`<aaa.bbb.ccc.ddd>`** is the IP address of the CCU, and press **Enter**.

```
60:03:3a> ping 192.168.22.2 1460
Press any key to stop (time resolution: 16 ms)
PING 192.168.22.2: 1452 data bytes
1460 bytes from 192.168.22.2: icmp_seq=0. time=80. ms
1460 bytes from 192.168.22.2: icmp_seq=1. time=32. ms
1460 bytes from 192.168.22.2: icmp_seq=2. time=64. ms
1460 bytes from 192.168.22.2: icmp_seq=3. time=64. ms
1460 bytes from 192.168.22.2: icmp_seq=4. time=48. ms
1460 bytes from 192.168.22.2: icmp_seq=5. time=48. ms
1460 bytes from 192.168.22.2: icmp_seq=6. time=48. ms
1460 bytes from 192.168.22.2: icmp_seq=7. time=32. ms
1460 bytes from 192.168.22.2: icmp_seq=8. time=32. ms
1460 bytes from 192.168.22.2: icmp_seq=9. time=64. ms
----192.168.22.2 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 32/51/80

60:03:3a>
```

6.7 Testing the Radio Link Quality Using the File Get Command

You can run a simple File Get test to verify the performance and integrity of the communications between the CCU and EUM. The file get command prints and updates a transfer rate in kbps for every 20 packets for image, config, and null files received to RAM before being written to flash memory. Retrieving the file “null” using FTP results in a 2 MB file of uninitialized characters.

The File Get test tests only the radio link, eliminating any problems due to the Ethernet side or customer computer. The following procedure explains how to run the File Get test from the EUM; however, you can also run the same test from the CCU, and the results will be equally valid.

The FTP session will timeout after 60 seconds without a response, or the operator can terminate the session.

To Test Radio Link Quality Using File Get Throughput Test

1. At the EUM, use the **`stats clear`** command to reset all statistics.

   ```
   60:03:3a> statistics clear
   ```

2. At the CCU, use the **watch <eum_id>** command to begin gathering watch statistics for the EUM. (For more information about the **`watch`** command, refer to *CCU Watch Statistics* on page 298.)

   ```
   60:03:3a> watch 60:ff:fe
   Watching 60:ff:fe
   ```

3. At the EUM, type **file get <ccu_ip_address>**, and press **Enter**.

   ```
   60:ff:fe>
   60:ff:fe> file get 172.16.4.1
   Enter password:
   Getting remote file 'null' from 172.16.4.1 as local file 'null'
     (press 'qqq' to abort)...
   bytes processed:    2097152 at  1969 kbps
   ```

```
file transfer complete
Transfered "/tffs0/null" Okay.
60:ff:fe>
```

NOTE: For more information about the “file get” command, refer to Appendix C on page 189.

4. At the CCU, use the **watch** command to view the EUM watch statistics.

```
60:03:3a> watch
      The EUMID under watch is: 60:ff:fe
              Grade of service:  be
                    RSSI [dBm]:  -24
       Time since last payload:  0
                  Input Octets:  2378095
                 Input Packets:  3370
                 Output Octets:  2731787
                Output Packets:  3344
               rxPktsDirected:  44743
              rxPktsBroadcast:  19
              rxPktsDuplicate:  0
                 rxPktsFCSFail:  2
          rxPayloadsDelivered:  2584
                  rxPktsEmpty:  42176
                       txPkts:  44767
                  txPktsEmpty:  42154
                   txPayloads:  2613
               txPayloads1Ok:  2585
               txPayloads2Ok:  14
               txPayloads3Ok:  0
               txPayloads4Ok:  0
         txPayloadsFailRetry:  0
       txPayloadsFailTimeout:  0
  txPayloadsFailQueueTooLong:  0
          replyOrRssiTimeouts:  25
```

5. At the EUM, use the **stats summary** command to view the EUM statistics

```
60:ff:fe> stats summary
----------------- MAC Summary ---------------------------------

Transmitted Payloads
                1Ok :       921  89.8%
                2Ok :        99   9.6%
                3Ok :         5   0.4%
                4Ok :         0   0.0%
         Fail Retry :         0   0.0%
       Fail Timeout :         0

Received Packets
         HCRC Error :         2   0.0%
           Directed :      3955  56.0%
          Broadcast :      3097  43.9%
           No Match :         0   0.0%

Received Payloads
          FCS Error :       102   6.3%
          Duplicate :        36   2.2%
  Too Busy - Discard :         0   0.0%
          Delivered :      1467  91.4%
60:ff:fe>
```

NOTE: Output Packets and Octets (from the CCU's perspective have increased by 2 MB after the file get command from the EUM.

6.8 Testing End-to-End Throughput

The procedures outlined below will *get* a file from the CCU, and then *put* a file onto the CCU. In both cases, you can record the file transfer performance. WaveRider recommends doing this procedure with a screen capture, so you have a permanent record to baseline the performance of the link.

Before you carry out the FTP test, you may want to baseline the performance of the computer you are using at the EUM, by first connecting it directly to an FTP server and running an FTP test back-to-back with the server. This back-to-back FTP test should be at least 3 Mbps, or you may have a problem with your server or computer setup.

NOTE: The EUM can be used as an FTP server, provided the PC is on the same subnet as the EUM or appropriate routes have been added to the gateway router.

Entering `null` as the destination filename in the *put* command ensures the file will not be permanently stored to CCU memory. If you inadvertently forget to enter **`null`** at the end of the **`put`** command, and consequently save the file to memory, the measured throughput will be lower than expected. You can remove the file using the CCU file services, available through the command line interface. As long as you enter `null` after the *put* command, any size file can be used.

The FTP throughput should correspond to a value near the maximum allowed by the GOS, assuming no other traffic is being carried by the CCU.

To Test End-to-End Throughput Using FTP

1. At the EUM, use the **`stats clear`** command to reset all statistics.

```
60:03:3a> statistics clear
```

2. At the CCU, use the **`watch <eum_id>`** command to begin gathering watch statistics for the EUM. (For more information about the **`watch`** command, refer to *CCU Watch Statistics* on page 298.)

```
60:03:3a> watch 60:ff:fe
Watching 60:ff:fe
```

3. At a PC connected to the EUM, open a console window and type **`ftp <aaa.bbb.ccc.ddd>`**, where <aaa.bbb.ccc.ddd> is the CCU Ethernet IP address.

4. In the FTP window, enter the following commands to *get* a null file from the CCU:

```
Connected to <aaa.bbb.ccc.ddd>.
220 FTP server ready
User (<aaa.bbb.ccc.ddd>:(none)):           (Press Enter.)
331 Password required
Password: ********
230 User logged in
```

```
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> binary
200 Type set to I, binary mode
ftp> get null
200 Port set okay
150 Opening BINARY mode data connection
############################################################################
############################################################################
##################################################################
226 Transfer complete
ftp: 463713 bytes received in 10.80Seconds 42.96Kbytes/sec.
ftp>bye
221 Bye...See you later.
```

5. Enter the following commands to *put* the null file to the CCU.

```
Connected to <aaa.bbb.ccc.ddd>.
220 FTP server ready
User (<aaa.bbb.ccc.ddd>:(none)):
331 Password required
Password:
230 User logged in
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> binary
200 Type set to I, binary mode
ftp> put null
200 Port set okay
150 Opening BINARY mode data connection
############################################################################
############################################################################
##################################################################
226 Transfer complete
ftp: 463713 bytes sent in 8.30Seconds 55.86Kbytes/sec.
ftp>bye
221 Bye...See you later.
```

6. At the CCU, use the **`watch`** command to view the EUM watch statistics.

```
60:03:3a> watch
      The EUMID under watch is: 60:ff:fe
              Grade of service:  be
                    RSSI [dBm]:  -24
       Time since last payload:  0
                  Input Octets:  2378095
                 Input Packets:  3370
                 Output Octets:  2731787
                Output Packets:  3344
                rxPktsDirected:  44743
               rxPktsBroadcast:  19
               rxPktsDuplicate:  0
                 rxPktsFCSFail:  2
           rxPayloadsDelivered:  2584
                 rxPktsEmpty:  42176
                      txPkts:  44767
                 txPktsEmpty:  42154
                  txPayloads:  2613
               txPayloads1Ok:  2585
               txPayloads2Ok:  14
               txPayloads3Ok:  0
               txPayloads4Ok:  0
         txPayloadsFailRetry:  0
       txPayloadsFailTimeout:  0
  txPayloadsFailQueueTooLong:  0
```

```
replyOrRssiTimeouts:  25
```

7. At the EUM, use the **`stats summary`** command to view the EUM statistics.

```
60:ff:fe> stats summary
----------------- MAC Summary ---------------------------------

Transmitted Payloads
                 1Ok :        921  89.8%
                 2Ok :         99   9.6%
                 3Ok :          5   0.4%
                 4Ok :          0   0.0%
          Fail Retry :          0   0.0%
        Fail Timeout :          0

Received Packets
          HCRC Error :          2   0.0%
            Directed :       3955  56.0%
           Broadcast :       3097  43.9%
            No Match :          0   0.0%

Received Payloads
           FCS Error :        102   6.3%
           Duplicate :         36   2.2%
  Too Busy - Discard :          0   0.0%
           Delivered :       1467  91.4%
60:ff:fe>
```

6.9 Operating Statistics

The CCU and EUM collect a wide range of IP, radio, MAC, and network layer statistics, which can be used for measuring system performance and troubleshooting. These statistics can be accessed through the command line interface, outlined in Appendix C on page 189 or by using an SNMP manager. A list of available statistics and their meanings can be found in Appendix J on page 277.

The CCU also includes a “watch” command, which enables you to monitor link statistics for a single specified EUM. For instructions about using the watch command, refer to *CCU Watch Statistics* on page 298.

NOTE: A subset of all statistics are logged at regular intervals, allowing checks on historical operation.

6.10 SNMP

The CCU and EUM are SNMP-ready. To make use of the CCU and EUM SNMP capabilities, you must obtain the associated WaveRider MIBs from the technical support page at www.waverider.com and install them on your SNMP manager (SNMPc, or HP OpenView, for example).

Once you have obtained and installed these MIBs, you will, from the SNMP manager, be able to carry out the following functions for both CCUs and EUMs:

- Read hardware and software configuration parameters, such as unit serial number, MAC address, regulatory domain, and hardware and firmware version.
- Read operator-configurable parameters, such as IP addresses, radio frequency, transmit power level, and the contents of the CCU Authorization and Registration Tables.
- Read system operating statistics from the MAC layer, and the radio and Ethernet drivers.
- Receive trap messages such as CCU or EUM power cycles.

In addition, you can program your SNMP manager to perform the following operations:

- Generate a warning or alarm whenever an operating statistic falls outside an acceptable range.
- Perform mathematical calculations on a collection of statistics and generate a warning or an alarm if the result of the calculation falls outside an acceptable range. This calculation is done when a statistic, in isolation, cannot be interpreted; i.e., it can only be interpreted properly when compared with the current value of other statistics.
- Perform a trend analysis on a statistic or group of statistics and generate a warning or alarm when the statistic or group of statistics is starting to move towards an unacceptable limit.

For more detailed information on how to use SNMP to monitor the performance of your LMS4000 900 MHz Radio Network, refer to *Monitoring the Network* on page 165 and Appendix I on page 251.

6.11 Field Upgrade Process

CCU and EUM operating software can be upgraded using FTP. The upgrade mechanism is designed to be robust and reliable.

Hash codes are generated with each new software image. The new image is FTPed with the hash code to the unit that is being upgraded, and the new software is received and written to memory. A hash code for the new image is generated locally and compared with the hash code that was FTPed with the new image.

If the hash code comparison is unsuccessful, the downloaded image will not be written to the file system, and a report will be returned.

If the hash code comparison is successful, then the existing executable software is copied as a backup (.bak file), and the newly downloaded image becomes the unit executable.

If the new executable is found to be corrupt for any reason, then the unit reverts to the backed-up, older image.

NOTE: CRCs are available in the upgrade procedure.

6.12 FTPing CCU and EUM Configuration Files

FTP enables you to transfer configuration files to CCUs and EUMs from anywhere that has network access to the LMS4000 900 MHz Radio Network. FTP is a useful tool for the following operations:

- Restoring a unit to an earlier working state.
- Restoring configuration files that have been corrupted.
- Configuring replacement CCUs and EUMs when units have failed.
- Changing default configurations, such as GOS.

Some of the configuration files may be the same throughout the network (port filter configuration file, for example), and others are different for all units. Some configuration files are loaded instantly (as soon as the file is FTPed), and some require a unit reboot to take effect. Table 17 provides a summary of the configuration files used in the CCUs and EUMs, whether they are typically the same throughout the system, and whether they require a unit reboot to take effect.

Table 17 FTPing Configuration Files

Configuration File	File Name	CCU	EUM	Reboot Required?	System-wide? (note 1)
GOS Configuration File	gosbe.cfg gosbronz.cfg gossilve.cfg gosgold.cfg	Yes		No	Yes
Authorization Configuration File	authdb.cfg	Yes		No	No
DHCP Configuration File	dhcp.cfg	Yes		Yes	Yes
Port Configuration File	port.cfg	Yes	Yes	Yes	Yes
Route Configuration File	route.cfg	Yes		Yes	No
SNTP Configuration File	sntp.cfg	Yes	Yes	Yes	Yes
Basic Configuration File	basic.cfg	Yes	Yes	Yes	No

NOTE: System-wide means that the configuration file in question (for example, the port configuration file) will normally be the same throughout your network. Configuration files, such as the route configuration file, vary from CCU to CCU.

CAUTION: Use FTP to transfer configuration files between like units only; for example, from a CCU to another CCU. (Ensure the file is transferred using image or binary mode.) Although port filters are used in both the CCU and EUM, there may be differences between the port configuration file for the CCU and the port configuration file for the EUM.

One way of using this feature is to build configuration files using a spare CCU and a spare EUM. Both units should have their RF outputs terminated in 50-ohm loads (or they could be connected to each other through an attenuator) to ensure the units are not transmitting signals that could interfere with operating CCUs and EUMs.

Once the CCU or EUM configuration files are built and saved in the spare units, they can be downloaded to target CCUs and EUMs, as necessary. GOS configuration files are provided by WaveRider. You can also use the WaveRider Grade of Service Creation Utility to create your own custom GOS files.

Alternately, the configuration files could be built and saved in operating units, then downloaded from these units to other CCUs and EUMs in the system.

Remember to save any changes made at the CLI before downloading the configuration files from the device.

7 Configuring the CCU

This section explains the following procedures and topics:

Before you configure the CCU

- Familiarize yourself with the CLI commands, syntax and shortcuts, outlined in Appendix C on page 189. This appendix provides a complete list of the available CCU commands, some of which are not discussed in this section.
- Connect a PC to the CCU directly to the console port, or through a Telnet session. See *Command-line Interface* on page 91 for console settings.

CAUTION: Remember to regularly enter **save** or **commit** and press **Enter**, to save your configuration changes to the file system. As well, some parameters and configuration files (refer to Table 17 on page 108 for details) do not take effect until you reboot the unit, specifically the RF frequency, transmit power, and IP addressing.

CAUTION: After you have finished making your configuration changes, remember to disconnect your terminal from the CCU.

7.1 CCU and EUM Serial Number, MAC Address, and Station ID

The EUM/CCU product ID, serial number, station ID, and Ethernet and radio MAC addresses, are related:

- **Product ID:** The product ID is the 14-character string just below the bar code on the product label, which is affixed to the case of the unit, for example:
  - EUM3000AB02A129E00A32
- **Serial Number:** The serial number is the last six characters of the product ID. In the above example, the serial number is:
  - E00A32
- **Station (CCU or EUM) ID:** The station ID is derived by prefacing the last five characters of the serial number with ‘6’ appended. In the above example, the station ID, in hexadecimal notation, is:
  - 60:0A:32
- **Ethernet MAC Address:** The Ethernet MAC address is derived by prefacing the serial number with the characters ‘00:90:c8’. In the above example, the Ethernet MAC address is:
  - 00:90:c8:E0:0A:32
- **Radio MAC Address:** The radio MAC address is derived by prefacing the station ID with the characters ‘00:90:c8’. In the above example, the radio MAC address is:
  - 00:90:c8:60:0A:32

7.2 Setting the CCU Password

To Change the CCU Password

1. Type `password` and press **Enter**.
2. At the **Enter Current Password** prompt, type the old password.
3. At the **Enter New Password** prompt, type the new password.

TIP: Passwords are alphanumeric and case-sensitive. For example, “abc” is not the same as “aBc”.

4. At the **Verify password** prompt, type the new password again.

The system displays a message that your password has been successfully changed.

Example:

```
60:03:3a> password
Enter Current Password: ********
Enter New Password: ********
Verify password: ********
Saving new password
Password Changed
60:03:3a>
```

CAUTION: Remember to record the password. Unlocking the CCU can only be performed by contacting WaveRider Technical Support.

7.3 Configuring the CCU RF Parameters

To Set the CCU Operating Frequency

1. Type **radio frequency <frequency>** and press **Enter**.
    - <frequency> is the CCU operating frequency in tenths of a MHz. For example, 917.0 MHz is entered as 9170.
2. Type **save** or **commit** and press **Enter**.
3. Before the new radio frequency will take effect, you must reboot the CCU by typing **reset** and pressing **Enter**.

To Set the CCU Power Level

1. Type **radio rf <power level>** and press **Enter**. <power level> is the CCU transmit power level, either:
    - the desired power level, in dBm, any integer value in the range 15 - 26 inclusive,
    - high (+26 dBm), or
    - low (+15 dBm).

    For example, radio rf 22 will set the RF output power to +22 dBm.

    NOTE: Use the HIGH power level unless your site has unique requirements for which a numerically set power level, or the LOW power level, is more appropriate. For example, the capability to numerically set the power level may be useful in high-density environments, where site-to-site interference is a problem.

2. Type **save** or **commit** and press **Enter**.
3. Before the new power level will take effect, you must reboot the CCU by typing **reset** and pressing **Enter**.

The following example

- Sets the CCU operating frequency to 917 MHz,
- Sets the transmit power level to `high`,

  NOTE: Changes to the transmit power level take effect immediately, they do not require a CCU reboot.

- Saves the new settings,
- Reboots the CCU so that the new parameters take effect, and
- Displays the CCU RF parameters.

```
60:03:3a> radio frequency 9170
Radio Frequency: 9170
60:03:3a> radio rf high
RF Power: HIGH
60:03:3a> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved

60:03:3a> reset

rebooting CCU ...

(... Power On Self Test ...)

WaveRider Communications, Inc. LMS3000
Password:
60:03:3a> radio
RF Power: HIGH
Radio Frequency: 9170
60:03:3a>
```

7.4 Configuring CCU Protocol Modes and IP Addresses

This section explains how to configure the CCU to use Routed, Switched Ethernet, or Through Only mode.

In previous software versions, all systems used Routed mode. In Routed mode, all EUMs and end-user computers have the CCU radio IP address as their gateway. If you wish to convert a system from Routed mode to Switched Ethernet or Through Only mode, it may be simpler to assign that IP address to the new gateway router port, rather than changing the gateway IP address on all the EUMs as associated end-user computers. The reverse applies to changing from Switched Ethernet or Through Only mode to Routed mode.

In *IP Network Planning* on page 59, you determined the following:

- CCU Protocol Mode
- CCU gateway IP address

- CCU radio IP address and subnet mask
- CCU Ethernet IP address and subnet mast (Routed Mode only)

7.4.1 Configuring Routed Mode

NOTE: The CCU gateway IP address must be on either the Ethernet or the radio IP subnet, as explained in *IP Network Planning* on page 59.

To Configure the CCU to Operate in Routed Mode

1. Type **protocol routed** and press **Enter** to set the CCU to routed mode.

```
60:06:4e> protocol routed
CCU in Routed Mode
```

2. Type **ip ethernet <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU Ethernet address.
   - <aaa.bbb.ccc.ddd> is the CCU Ethernet IP address.
   - <net mask> is the number of bits set in the net mask (1 to 32).

CAUTION: The CCU only accepts subnet masks using the shorthand notation; for example, it accepts '16', but not 'ffff0000' or '255.255.0.0'.

```
60:06:4e> ip ethernet 192.168.60.13 24
Ethernet IP Address: 192.168.60.13 / 24
Ethernet IP Subnet : 192.168.60.0 < 255.255.255.0 >
```

3. Type **ip radio <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU radio address.
   - <aaa.bbb.ccc.ddd> is the CCU radio IP address.
   - <net mask> is the net mask.

```
60:06:4e> ip radio 172.16.6.1 22
      Radio IP Address: 172.16.6.1 / 22
      Radio IP Subnet : 172.16.4.0 < 255.255.252.0 >
```

4. Type **ip gateway <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU gateway IP address.

```
60:06:4e> ip gateway 192.168.60.1 24
      Gateway IP Address: 192.168.60.1
```

5. Type **save** and press **Enter** to save the new settings.

```
60:06:4e> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
```

6. Type **reset** and press **Enter** to reboot the CCU.

```
60:06:4e> reset
rebooting CCU ...
```

7. On reset, type **protocol** and press **Enter** to display the protocol mode.

```
60:06:4e> protocol
CCU in Routed Mode
```

8. Type **ip** and press **Enter** to display the ip addresses.

```
60:06:4e> ip
Radio IP Address: 172.16.6.1 / 22
Radio IP Subnet : 172.16.4.0 < 255.255.252.0 >
Ethernet IP Address: 192.168.60.13 / 24
Ethernet IP Subnet : 192.168.60.0 < 255.255.255.0 >
Gateway IP Address: 192.168.60.1
```

You must also configure all EUMs and subscriber PCs connected to the CCU to have IP addresses on the CCU's IP subnet and have the CCU radio IP address as their gateway.

7.4.2 Configuring Switched Ethernet Mode

This section explains how to configure Switched Ethernet mode for both a single subnet and a multiple subnet configuration.

With a multiple subnet configuration, you can use public IP addresses for some or all of the customer PCs without expending public IPs on EUMs.

To Configure Switched Ethernet Mode

1. Type **protocol switched** and press **Enter** to set the CCU to Switched Ethernet mode.

```
60:06:4e> protocol switched
CCU in Switched Ethernet Mode
```

2. Type **ip radio <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU IP address.
   - **<aaa.bbb.ccc.ddd>** is the CCU IP address
   - **<net mask>** is the CCU IP subnet mask

```
60:06:4e> ip radio 192.168.60.99 24
IP Address: 192.168.60.99 / 24
IP Subnet : 192.168.60.0 < 255.255.255.0 >
```

3. Type **ip gateway <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU gateway to be the gateway router.
   - **<aaa.bbb.ccc.ddd>** is the CCU gateway IP address
   - **<net mask>** is the CCU gateway IP address subnet mask

```
60:06:4e> ip gateway 192.168.60.1. 24
Gateway IP Address: 192.168.60.1
```

4. Type **save** and press **Enter** to save the new settings.

```
60:06:4e> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
```

5. Type **`reset`** and press **Enter** to reboot the CCU.

```
60:06:4e> reset
rebooting CCU ...
```

6. On reset, type **`protocol`** and press **Enter** to display the protocol mode.

```
60:06:4e> protocol
CCU in Switched Ethernet Mode
```

7. Type **`ip`** and press **Enter** to display the ip addresses.

```
60:06:4e> ip
IP Address: 192.168.60.99 / 24
IP Subnet : 192.168.60.0 < 255.255.255.0 >
Gateway IP Address: 192.168.60.1
```

For a system with a single IP subnet, all subscribers PCs and EUMs are given IP addresses on one IP subnet. The gateway router is given an address in the same subnet and is the gateway address for all PCs and EUMs.

A multiple subnet configuration has the advantage that you can use public IP addresses for some or all of the customer PCs without expending public IPs on EUMs. In this case, the Ethernet interface of the gateway router connected to the CCU is given two IP addresses on two separate subnets (192.0.2.1 / 24 and 172.16.6.1 / 24 in the example). Subscribers are given IP addresses on the public subnet, with the public IP address of the gateway router (192.0.2.1 in the example) as their gateway address. EUMs and the CCU are given addresses on the private subnet, with the private IP address of the gateway router (172.16.6.1 in the example) as their gateway address.

7.4.3 Configuring Through Only Mode

The following procedure demonstrates how to configure Through Only mode.

To Configure Through Only Mode

1. Type **`protocol through`** and press **Enter** to set the CCU to Through Only mode.

```
60:06:4e> protocol through
CCU in Through Only Mode
```

2. Type **`ip radio <aaa.bbb.ccc.ddd> <net mask>`** and press **Enter** to set the CCU IP address.
   - **`<aaa.bbb.ccc.ddd>`** is the CCU radio IP address
   - **`<net mask>`** is the CCU radio IP address subnet mask

```
60:06:4e> ip radio 192.168.60.99 24
IP Address: 192.168.60.99 / 24
IP Subnet : 192.168.60.0 ( 255.255.255.0 )
```

3. Type **ip gateway <aaa.bbb.ccc.ddd> <net mask>** and press **Enter** to set the CCU IP address.
   - **<aaa.bbb.ccc.ddd>** is the CCU gateway IP address, which is also the IP address of the gateway router
   - **<net mask>** is the CCU radio IP address subnet mask

```
60:06:4e> ip gateway 192.168.60.1. 24
Gateway IP Address: 172.16.6.10
```

4. Type **save** and press **Enter** to save the new settings.

```
60:06:4e> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
```

5. Type **reset** and press **Enter** to reboot the CCU.

```
60:06:4e> reset
rebooting CCU ...
```

6. On reset, type **protocol** and press **Enter** to display the protocol mode.

```
60:06:4e> protocol
CCU in Through Only Mode
```

7. Type **ip** and press **Enter** to display the ip addresses.

```
60:06:4e> ip
IP Address: 192.168.60.99 / 24
IP Subnet : 192.168.60.0 < 255.255.255.0 >
Gateway IP Address: 192.168.60.1
```

7.5 Configuring DHCP Relay

To configure DHCP relay

- Determine the DHCP server IP address.
- Enable DHCP Relay.
- Add the DHCP server to the CCU.

To Enable DHCP Relay

1. Type **dhcp enable** and press **Enter**.
2. Type **save** or **commit** and press **Enter**.

To Add a DHCP Server

1. Type **dhcp relay add <aaa.bbb.ccc.ddd> <net mask>** and press **Enter**.
   - <aaa.bbb.ccc.ddd> is the IP address of the DHCP server you want to add.
   - <net mask> is the net mask of the DHCP server.

2. Repeat step 1 for any alternate DHCP servers in your network. WaveRider recommends that your network have at least one alternate DHCP server.
3. Type **`save`** or **`commit`** and press **Enter**.

The following example

- Enables DHCP relay,
- Adds a DHCP server with IP address 192.168.50.1 /24,
- Adds an alternate DHCP server with IP address 192.168.50.15 /24,
- Saves the new settings, and
- Displays the DHCP status.

```
60:03:3a> dhcp enable
60:03:3a>
60:03:3a> dhcp relay add 192.168.50.1 24
60:03:3a> dhcp relay add 192.168.50.15 24
60:03:3a>
60:03:3a> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
60:03:3a>
60:03:3a> dhcp relay
DHCP Relay Enabled:

DHCP Server Table:

DHCP Server Table:

  IP Address: 192.168.50.1
  Mask      : ffffff00

  IP Address: 192.168.50.15
  Mask      : ffffff00

60:03:3a>
```

7.6 Configuring Port Filtering

To add a port filter

- Determine the port number you want to filter.
- Determine whether you want to filter UDP, TCP, or both types of packets.
- Add the port filter to the CCU.

To Add a Port Filter

1. Type **`port add <number> <type>`** and press **Enter**.
   - <number> is the number of the port you want to filter.
   - <type> is the type of IP packet you want to filter, either `udp, tcp,` or `both.`
2. Repeat step 1 for any other ports that you want to filter out.
3. Type **`save`** or **`commit`** and press **Enter**.

The following example

- Configures the CCU to filter both UDP and TCP packets on ports 137, 138, 139, 445 and 1512,
- Saves the new settings, and
- Displays the TCP/UDP port filters.

```
60:03:3a> port add 137 both
60:03:3a> port add 138 both
60:03:3a> port add 139 both
60:03:3a> port add 445 both
60:03:3a> port add 1512 both
60:03:3a>
60:03:3a> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
60:03:3a>
60:03:3a> port
PORT FILTERS
    Port                  Filter
---------------------------------
      445                  both
      137                  both
      138                  both
      139                  both
     1512                  both
----------------------------------
60:03:3a>
```

The EUM factory default settings have ports 137, 138, 139, 445, and 1512 filtered out for both TCP and UDP, to prevent Network Neighborhood from seeing other end users' computers.

NOTE: These factory defaults are stored in the supplied port.cfg file.

7.7 Configuring the SNTP/UTC Time Clock

Configuring the SNTP/UTC Time Clock involves the following procedures, each of which is explained in detail on the following pages:

- Add an NTP server, if the one to which you want the CCU to synchronize has not already been added. You may want to delete the default NTP servers, to force the CCU to synchronize to the server you are adding.
- Set the SNTP client resynchronization period. The factory default setting is 3600 seconds, and WaveRider recommends not changing this default setting.

  NOTE: These factory defaults are stored in the supplied sntp.cfg file.

- Enable the SNTP client, to force the CCU to synchronize to an NTP server.
- Enable the SNTP relay, if you want the EUMs to be synchronized to the CCU.

To Add an NTP Server

1. Type **`time server add <aaa.bbb.ccc.ddd>`** and press **Enter**.
   - <aaa.bbb.ccc.ddd> is the IP address of the NTP server you are adding.
2. Type **`save`** or **`commit`** and press **Enter**.

```
60:00:43> time server add 10.0.0.1

NTP SERVERS
-----------------------------------
    132.246.168.148
    140.162.8.3
    136.159.2.1
    192.5.5.250
    10.0.0.1
-----------------------------------
60:00:43> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved

60:00:43>
```

NOTE: It is a good idea to ping the time servers from the CCU before adding them, to ensure you have connectivity.

To Enable the SNTP Client

NOTE: Enabling the time client on the CCU causes the CCU to get the time from the server on a regular basis.

1. Type **`time client enable`** and press **Enter**.
2. Type **`save`** or **`commit`** and press **Enter**.

```
60:00:43> time client enable
Time Client enabled
60:00:43>
```

To Enable SNTP Relay

NOTE: Enabling time relay on a CCU causes the CCU to forward the time to the EUMs.

1. Type **`time relay enable`** and press **Enter**.
2. Type **`save`** or **`commit`** and press **Enter**.

```
60:00:43> time relay enable
Relay enabled.
60:00:43>
```

To Display the SNTP Configuration and NTP Server List

- Type **`time print`** and press **Enter**.

```
60:00:43> time print
SNTP Client and Relay Configuration
-----------------------------------

Relay
    Enabled :                 Yes
    Destination :             Default Net Broadcast. (radio IF)
    Send time on...
        Boot :                Yes
        EUM Registration :    Yes

Server (send/listen)
    Port :                    123
    Unsynchronized Stratum :  15
    Synchronized Stratum :    Received NTP Stratum +5

Client (fetch only)
    Enabled :                 Yes
    Port :                    123
    Resync period :           30 seconds.
    Retry period :            30 seconds.

NTP SERVERS
-----------------------------------
    132.246.168.148
    140.162.8.3
    136.159.2.1
    192.5.5.250
    10.0.0.1
-----------------------------------
60:00:43>
```

To Display System Time

- Type **`time`** and press **Enter**.

```
60:00:43> time
22-JUL-2002 16:19:01
60:00:43>
```

To Force a Time Update

- Type **`time relay period 0`** and press **Enter**.

```
60:00:43> time relay period 0
14-AUG-2002 20:21:19
60:00:43>
```

NOTE: This command does not change the time client period.

7.8 Configuring SNMP

To fully configure SNMP

- Set the SNMP contact (name of the WISP, for example).
- Set the SNMP system location (physical location of the CCU, for example).
- Add an SNMP read community.
- Add an SNMP write community.
- Add an SNMP trap community.

To Set the SNMP Contact

1. Type **`snmp contact <contact>`** and press **Enter**.
   - <contact> is text field, often used for a contact name and phone number, a URL, or an email address, from 1-80 characters in length.
2. Type **`save`** or **`commit`** and press **Enter**.

To Set the SNMP System Location

1. Type **`snmp location <location>`** and press **Enter**.
   - <location> is the location of the CCU, from 1-80 characters in length.
2. Type **`save`** or **`commit`** and press **Enter**.

To Add an SNMP Read Community

1. Type **`snmp community add <community> read`** and press **Enter**.
   - <community> is the name of the read community string. The default read community string is "public". The read community string can be from 1-31 characters in length, but spaces are not allowed.
2. Type **`save`** or **`commit`** and press **Enter**.

To Add an SNMP Write Community

1. Type **`snmp community add <community> write`** and press **Enter**.
   - <community> is the name of the write community string. The default write community string is "private". The write community string can be from 1-31 characters in length, but spaces are not allowed.
2. Type **`save`** or **`commit`** and press **Enter**.

To Add an SNMP Trap Server

1. Type **`snmp trap add <aaa.bbb.ccc.ddd> <community>`** and press **Enter**.
   - <aaa.bbb.ccc.ddd> is the IP address of the trap server
   - <community> is the name of the community on the trap server, from 1-63 characters in length.
2. Type **`save`** or **`commit`** and press **Enter**.

The following example

- Sets the SNMP contact as WaveRider,
- Sets the SNMP location as Calgary_South,
- Adds SNMP read community `WaveRider_Calgary`,
- Adds SNMP write community `WaveRider_Calgary`,
- Adds SNMP trap server `WaveRider_Calgary`, IP address `10.0.1.68`,
- Saves the new settings, and
- Displays the SNMP settings.

Example:

```
60:03:3a>
60:03:3a> snmp contact WaveRider
60:03:3a> snmp location Calgary_South
60:03:3a> snmp community add WaveRider_Calgary read
60:03:3a> snmp community add WaveRider_Calgary write
60:03:3a> snmp trap add 10.0.1.68 WaveRider_Calgary
60:03:3a>
60:03:3a> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
60:03:3a>
60:03:3a> snmp
Contact: WaveRider
Location: Calgary_South
Name: LMS3000
SNMP Read Communities:
        WaveRider_Calgary

SNMP Write Communities:
        WaveRider_Calgary
SNMP Traps:
       10.0.1.68 WaveRider_Calgary
60:03:3a>
```

7.9 Adding EUMs to the Authorization Table

EUMs can be authorized either statically in the authorization table or through a RADIUS server.

To Add an EUM to the CCU Authorization Table

1. Type **`auth add <eum id> <gos>`** and press **Enter**.

   NOTE: <gos> is the grade of service that you want to assign to the EUM, one of: be (best effort), bronze, silver, gold, or denied.

2. Type **`save`** or **`commit`** and press **Enter**.

   The “auth” command takes effect immediately.

The following example

- Adds EUM ID `60:0a:32` to the Authorization Table, and assigns it the `gold` grade of service,
- Saves the new settings, and
- Displays the Authorization Table.

```
60:00:43> auth add 60:00:83 gold
Added 60:00:83 as gold
60:00:43> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved

60:00:43> auth

EUM ID       GOS CLASS      TYPE
-----------------------------------
60:00:83 gold     static
Default      be
Total of 1 entries

60:00:43>
```

7.10 Configuring RADIUS

This section explains how to configure the RADIUS server and client.

Refer to *WaveRider Attribute Definition* on page 325 for the vendor-specific attribute definition.

> **NOTE:** The WaveRider RADIUS client implementation conforms to RFC's 2865 and 2866.

7.10.1 Configuring the RADIUS Server

> **NOTE:** There is some confusion about which ports to use for the RADIUS protocol. From RFC2865, "The early deployment of RADIUS used UDP port number 1645, which conflicts with the "datametrics" service. The officially assigned port number for RADIUS is 1812." As well, from RFC2866, "The early deployment of RADIUS Accounting was done using UDP port number 1646, which conflicts with the "sa-msg-port" service. The officially assigned port number for RADIUS Accounting is 1813."

As stated earlier, when RADIUS authorization is enabled, the CCU will periodically generate RADIUS access-request messages for each registered EUM. The responses from the RADIUS server are then used to maintain the CCU Authorization Table, described in *Authorization Table (CCU only)* on page 239. This requires that the RADIUS server has been configured to work with the LMS4000, and a list of authorized EUMs, with their grades of service, have been entered in the RADIUS server's user table.

If RADIUS accounting is enabled, the CCU will periodically send accounting updates to the RADIUS server for each registered EUM. These updates will contain the Input and Output Packet and Byte counts for each EUM, where Input Packets is the number of packets received from the EUM, and Output Packets is the number of packets transmitted to the EUM.

To illustrate the configuration of the RADIUS server, consider the wired and wireless RADIUS configurations shown in Figure 47 and Figure 48 respectively.

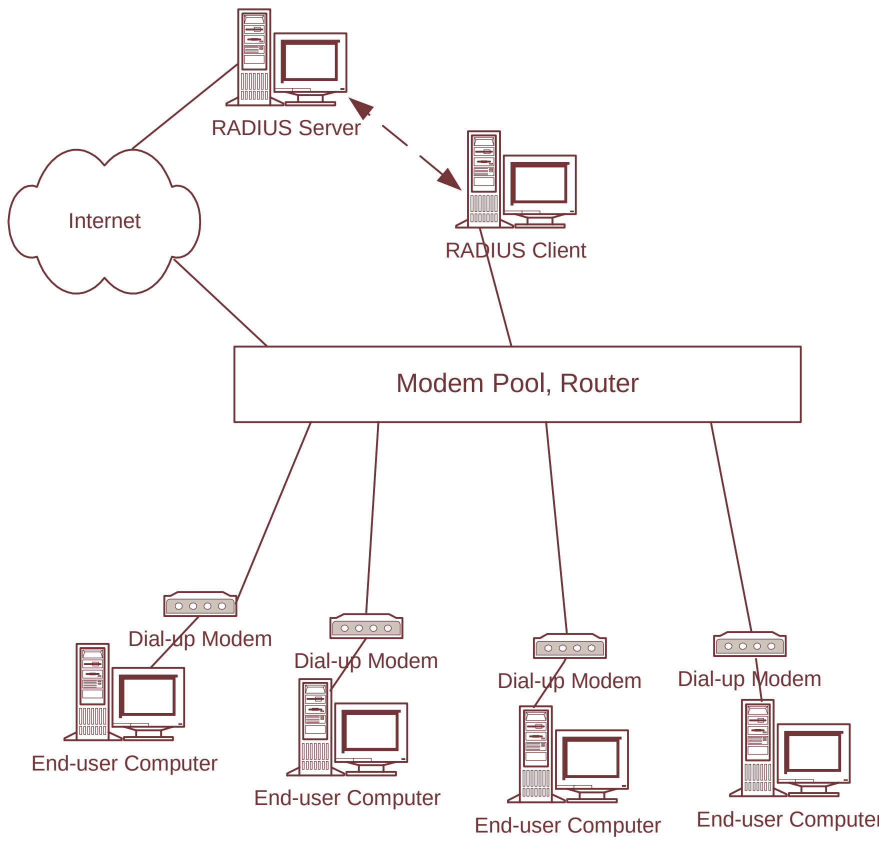


Figure 47 RADIUS Configuration - Wired Application

In wired applications, the RADIUS client is usually a PPP server; that is, a modem-bank controller. The links that are being controlled are the dial-up connections between the user's modem, and the modem pool. To set up the PPP link, the user supplies a username and password. The RADIUS client communicates with the RADIUS server, which is usually situated in at a central location. The RADIUS server has access to a list (database) of authorized usernames, and the associated user passwords (or it will have a means of checking the user password) and options. The link between the RADIUS client and server is protected by a "shared secret password". RADIUS servers may serve many different clients, each with its own modem pool, and different shared secret passwords.

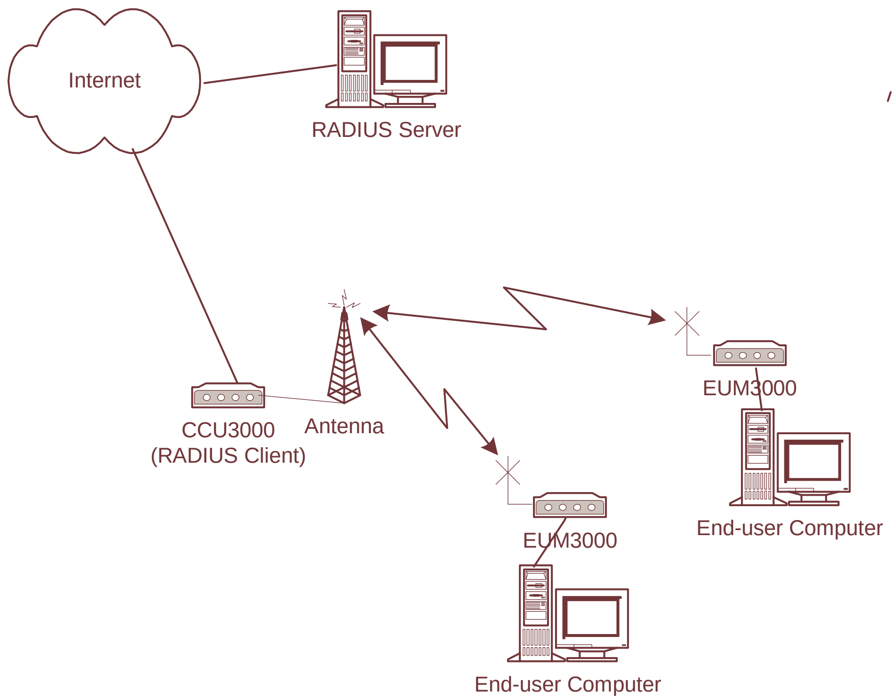


Figure 48 RADIUS Configuration - LMS4000 Wireless Application

In the LMS4000 wireless application, the RADIUS client is the CCU which, in many ways, can also be considered a “modem bank”. The links that are being controlled are the “always on” connections between the EUMs and the CCU. These links correspond to, and are managed on the basis of EUMIDs, rather than by user passwords, which do not need to be provided by the end users. Since the RADIUS messages require a user password, the CCU uses a fixed string, “buywavc”. The username is the EUMID, a string in the form of XX:XX:XX (for example, 61:23:45). Entries in the list of LMS4000 users on the RADIUS server will have the EUMID as the username, “buywavc” as the user password, and the vendor-specific option, “WaveRider-Grade-of-Service”, depending on the grade of service subscribed to by the user. The link between the CCU and the RADIUS server is protected by a shared secret password that is entered on the CCU using the `auth radius primary` or `auth radius secondary` command.

Although there are many makes and models of RADIUS servers, each with their own user interface and terminology, each will require the entry of the following:

- Dictionary entries for vendor specific attributes (i.e. WaveRider LMS4000 Grade-Of-Service Attributes).
- RADIUS Client (i.e. CCU) IP Address
- Shared Secret Password

You will also need to enter EUMIDs in the RADIUS database. Each entry will have the following attributes:

Table 18 RADIUS Database - LMS4000 User Attributes

username	`XX:XX:XX` (EUMID)
password	`buywavc`
WaveRider-Grade-of-Service	`be, bronze, silver or gold`

To illustrate the configuration of the RADIUS server, consider the following entries, which are required to configure FreeRADIUS, a commonly used open-source, free RADIUS software application. The following FreeRADIUS files need to be modified to support LMS4000:

Table 19 Free RADIUS Files

dictionary	This FreeRADIUS file needs to be modified to include the WaveRider LMS4000 dictionary.
dictionary.waverider	This file needs to be added to the FreeRADIUS server. It provides vendor- (WaveRider) specific details such as the vendor ID and WaveRider-Grade-of-Service attribute enumeration details.
clients	This FreeRADIUS file needs to be modified to include the CCU (RADIUS client) IP address and shared secret password.
users	Authorized EUMs are added to this FreeRADIUS file. Each user entry includes the authorization type (`local`), user password (`buywavc`), and Grade of Service (`be, bronze, silver` or `gold`)

Examples of the above files are shown in Table 20.

Table 20 Free RADIUS Files - Examples

<table>
<tr><td>dictionary</td><td><code>$INCLUDE dictionary.waverider</code></td></tr>
<tr><td>dictionary.waverider</td><td><pre>...
WaveRider Communications Ltd.
http://www.waverider.com/
#
Copyright 2002 WaveRider Communications Ltd.
Freely Distributable
#
VENDOR WaveRider 2979

BEGIN-VENDOR WaveRider

ATTRIBUTE Grade-of-Service 1 integer

VALUE Grade-of-Service be 1
VALUE Grade-of-Service bronze 2
VALUE Grade-of-Service silver 3
VALUE Grade-of-Service gold 4

END-VENDOR WaveRider
...</pre></td></tr>
<tr><td>clients</td><td><pre>...
192.168.10.11 <sharedSecret>
...</pre>(where <code>192.168.10.11</code> is the CCU Ethernet address and <code><sharedSecret></code> is the password entered with the <code>auth radius primary/secondary</code> command)</td></tr>
<tr><td>users</td><td><pre>...
XX:XX:XX Auth-Type := Local, User-Password ==
"buywavc", Grade-of-Service = silver
...</pre>(where <code>XX:XX:XX</code> is the EUMID)</td></tr>
</table>

NOTE: RADIUS settings take place immediately.

7.10.2 Configuring the CCU RADIUS Client

To configure the CCU RADIUS client:

1. Enable RADIUS Authorization.

```
60:06:4e> auth radius enable
Radius Authentication Enabled, Period: 5
Radius Accounting is Disabled
Radius Primary Server   :
Radius Secondary Server:
```

2. Set the primary RADIUS server IP address and Shared Secret Password.

```
60:06:4e> auth radius primary 192.168.60.96
Enter password (up to 16 chars): *********
Radius Authentication Enabled, Period: 5
Radius Accounting is Disabled
Radius Primary Server  : 192.168.60.96
Radius Secondary Server:
```

NOTE: This password must match the Shared Secret Password entered at the RADIUS server.

3. If your network includes a second RADIUS server, set the RADIUS server IP address and Shared Secret Password. Otherwise, set the secondary RADIUS server IP address to “none”.

```
60:06:4e> auth radius secondary 172.16.6.96
Enter password (up to 16 chars): *********
Radius Authentication Enabled, Period: 5
Radius Accounting is Disabled
Radius Primary Server  : 192.168.60.96
Radius Secondary Server: 172.16.6.96
```

4. (Optional) Enable RADIUS accounting.

```
60:06:4e> auth radius accounting enable
Radius Authentication Enabled, Period: 60
Radius Accounting is Enabled
Radius Primary Server  : 192.168.60.96
Radius Secondary Server: 172.16.6.96
```

5. Save settings.

```
60:06:4e> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
Route Config saved
Authorization Database saved
DHCP Server Config saved
```

6. Display the RADIUS settings.

```
60:06:4e> auth radius
Radius Authentication Enabled, Period: 60
Radius Accounting is Enabled
Radius Primary Server  : 192.168.60.96
Radius Secondary Server: 172.16.6.96
```

NOTE: Use the **`stats auth`** command to view RADIUS statistics, which are useful for troubleshooting purposes. Also, use **`sys log`** to detect if there are any malformed RADIUS packets.

7.10.3 RADIUS Packet Transmission

Once the CCU RADIUS client and the RADIUS server have been configured and enabled, access and accounting messages will be transmitted between them. The following is an example of the messages that are transmitted between the two. This information can be used for troubleshooting purposes.

Access Request (CCU to RADIUS Server)

The following is an example of an Access Request, transmitted from a CCU to the RADIUS server.

```
04:12:14.355196 192.168.10.11.1024 > 192.168.10.10.1812: udp 60
             4500 0058 0c20 0000 4011 d90f c0a8 0a0b
             c0a8 0a0a 0400 0714 0044 f906 0108 003c
             b9b2 ea5e c906 e977 5cbe c884 efae b46d
             010a 3630 3a33 303a 3031 0406 c0a8 0a0b
             0506 0000 0001 0212 436e 759e 9db7 b546
             7b4f e35c 0330 2f1e
```

Starting at byte 28, the following information is transmitted in the above Access Request:

Table 21 Example - RADIUS Access Request

Code	01
ID	08
Length	003c
Authenticator (encrypted)	b9b2 ea5e c906 e977 5cbe c884 efae b46d
Username Attribute	010a 3630 3a33 303a 3031
NAS IP Address Attribute	0406 c0a8 0a0b
NAS Port Attribute	0506 0000 0001
Password Attribute (encrypted)	0212 436e 759e 9db7 b546 7b4f e35c 0330 2f1e

Access Response (RADIUS Server to CCU)

The following is an example of an Access Response, transmitted from the RADIUS Server to the CCU.

```
04:12:14.361636 192.168.10.10.1812 > 192.168.10.11.1024: udp 32
             4500 003c 7e8c 0000 4011 66bf c0a8 0a0a
             c0a8 0a0b 0714 0400 0028 66e6 0208 0020
             0df8 7527 66c6 4ee5 252e 3b56 46dd ef30
             1a0c 0000 0ba3 0106 0000 0003
```

Starting at byte 28, the following information is transmitted in the above Access Response:

Table 22 Example - RADIUS Access Response

Code	`02`
ID	`08`
Length	`0020`
Authenticator (encrypted)	`0df8 7527 66c6 4ee5 252e 3b56 46dd ef30`
WaveRider-Grade-of-Service Attribute:	`1a0c 0000 0ba3 0106 0000 0003` (where: `0ba3` is WaveRider's vendor number, `01` is the Grade-of-Service attribute number, `06` is the length and `0000 0003` is the integer *3*, which corresponds to “silver”)

8 Configuring the EUM

This chapter covers the following procedures:

Before you configure the EUM

- Familiarize yourself with the CLI commands, syntax and shortcuts, outlined in Appendix C on page 189. *Command-line Syntax* provides a complete list of the available EUM commands, some of which are not discussed in this section.
- Connect a PC to the EUM with a cross-over Ethernet cable and open a Telnet session.

CAUTION: Remember to regularly enter **save** or **commit and press Enter,** to save your configuration changes to memory. As well, some parameters will not take effect until you reboot the unit, specifically the RF frequency, transmit power and IP addressing.

8.1 Setting the EUM Password

To Change the EUM Password

1. Type `password` and press **Enter**.
2. At the **Enter Current Password** prompt, type the old password.

3. At the **Enter New Password** prompt, type the new password.

TIP: Passwords are alphanumeric and case-sensitive. For example, “abc” is not the same as “aBc”.

4. At the **Verify password** prompt, type the new password again.

   The system displays a message that your password has been successfully changed.

```
60:ff:fe> password
Enter Current Password: ********
Enter New Password: ********
Verify password: ********
Saving new password
Password Changed
60:ff:fe>
```

CAUTION: Remember to record the password. Unlocking the EUM can only be performed by contacting WaveRider Technical Support.

8.2 Configuring the EUM RF Parameters

To Set the EUM Operating Frequency

1. Type **`radio frequency <frequency>`** and press **Enter**.
   - <frequency> is the EUM operating frequency in tenths of a MHz. For example, 917.0 MHz is entered as `9170`.
2. Type **`save`** or **`commit`** and press **Enter**.
3. Before the new radio frequency will take effect, you must reboot the EUM by typing **`reset`** and pressing **Enter**.

To Set the EUM Power Level

1. Type **`radio rf <power level>`** and press **Enter**. `<power level>` is the EUM transmit power level, either:
   - the desired power level, in dBm, any integer value in the range 15 - 26 inclusive,
   - `high` (+26 dBm), or
   - `low` (+15 dBm).

   For example, `radio rf 22` will set the RF output power to +22 dBm.

   NOTE: Use the HIGH power level unless your site has unique requirements for which a numerically set power level, or the LOW power level, is more appropriate. For example, the capability to numerically set the power level may be useful in high-density environments, where site-to-site interference is a problem.

2. Type **`save`** or **`commit`** and press **Enter**.
3. Before the new power level will take effect, you must reboot the EUM by typing **reset** and pressing **Enter**.

The following example

- Sets the EUM operating frequency to 917 MHz,
- Sets the transmit power level to `high`,

  NOTE: Changes to the transmit power level take effect immediately, they do not require an EUM reboot.

- Saves the new settings,
- Reboots the EUM so that they new parameters take effect, and
- Displays the EUM RF parameters.

```
60:ff:fe>
60:ff:fe> radio frequency 9170
60:ff:fe> radio rf high
60:ff:fe>
60:ff:fe> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
60:ff:fe>
60:ff:fe> reset
rebooting EUM ...

WaveRider Communications, Inc. LMS3000
Password:
60:ff:fe>
60:ff:fe> radio
RF Power: HIGH
Radio Frequency: 9170
60:ff:fe>
```

8.3 Configuring EUM IP Parameters

In *IP Network Planning* on page 59, you determined the following:

- EUM gateway IP address
- EUM IP address and subnet mask
- End-user PC Ethernet IP address and subnet mask (not required if using DHCP)

To Set the EUM Ethernet IP Address

1. Type **ip ethernet <aaa.bbb.ccc.ddd> <net mask>** and press **Enter**.
   - <aaa.bbb.ccc.ddd> is the EUM Ethernet IP address.
   - <net mask> is the number of bits set in the net mask (1 to 32).

CAUTION: The EUM only accepts subnet masks using the shorthand notation; for example, it accepts ‘16’, but not ‘ffff0000’ or ‘255.255.0.0’.

2. Type **save** or **commit** and press **Enter**.
3. Before the new EUM Ethernet IP address will take effect, you must reboot the EUM by typing **reset** and pressing **Enter**.

To Set the EUM gateway IP Address

1. Type **ip gateway <aaa.bbb.ccc.ddd>** and press **Enter**.
   - <aaa.bbb.ccc.ddd> is the EUM gateway IP address.
2. Type **save** or **commit** and press **Enter**.
3. Before the new EUM gateway IP address will take effect, you must reboot the EUM by typing **reset** and pressing **Enter**.

The following example

- Sets the EUM Ethernet IP address to 172.16.4.2 /22,
- Sets the EUM gateway IP address to 172.16.4.1,
- Saves the new settings,
- Reboots the EUM so that the new parameters take effect, and
- Displays the EUM IP parameters.

```
60:ff:fe>
60:ff:fe> ip ethernet 172.16.4.2 22
60:ff:fe> ip gateway 172.16.4.1
60:ff:fe>
60:ff:fe> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
60:ff:fe>
60:ff:fe> reset
rebooting EUM ...

WaveRider Communications, Inc. LMS3000
Password:

60:ff:fe> ip
IP Address: 172.16.4.2 / 22
IP Subnet : 172.16.4.0 ( 255.255.252.0 )
Gateway IP Address: 172.16.4.1
60:ff:fe>
```

8.4 Configuring Port Filtering

The procedure for configuring port filtering on an EUM is identical to the procedure for a CCU. To add a port filter:

- Determine the port number you want to filter.
- Determine whether you want to filter UDP, TCP, or both types of packets.
- Add the port filter to the EUM.

To Add a Port Filter

1. Type **port add <number> <type>** and press **Enter**.
   - <number> is the number of the port you want to filter.
   - <type> is the type of IP packet you want to filter, either udp, tcp, or both.
2. Type **save** or **commit** and press **Enter**.

The following example

- Configures the EUM to filter both UDP and TCP packets on ports 137, 138, 139, 445, and 1512,
- Saves the new settings, and
- Displays the TCP/UDP port filters.

```
60:ff:fe> port add 137 both
60:ff:fe> port add 138 both
60:ff:fe> port add 139 both
60:ff:fe> port add 445 both
60:ff:fe> port add 1512 both
60:ff:fe>
60:ff:fe> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
60:ff:fe>
60:ff:fe> port
PORT FILTERS
    Port                      Filter
---------------------------------
      445                      both
      137                      both
      138                      both
      139                      both
     1512                      both
----------------------------------
60:ff:fe>
```

8.5 Configuring SNMP

The procedure for configuring SNMP on an EUM is identical to the procedure for a CCU. To fully configure SNMP

- Set the SNMP contact (name of the WISP, for example).
- Set the SNMP system location (physical location of the EUM, for example).
- Add an SNMP read community.
- Add an SNMP write community.
- Add an SNMP trap server.

To Set the SNMP Contact

1. Type **snmp contact <contact>** and press **Enter**.
    - <contact> is a name and phone number, a URL, or an email address, from 1-80 characters in length.
2. Type **save** or **commit** and press **Enter**.

To Set the SNMP System Location

1. Type **snmp location <location>** and press **Enter**.
    - <location> is the location of the EUM, from 1-80 characters in length.
2. Type **save** or **commit** and press **Enter**.

To Add an SNMP Read Community

1. Type **snmp community add <community> read** and press **Enter**.
    - <community> is the name of the read community string. The default read community string is “public”. The read community string can be from 1-31 characters in length, but spaces are not allowed.
2. Type **save** or **commit** and press **Enter**.

To Add an SNMP Write Community

1. Type **snmp community add <community> write** and press **Enter**.
    - <community> is the name of the write community string. The default write community string is “private”. The write community string can be from 1-31 characters in length, but spaces are not allowed.
2. Type **save** or **commit** and press **Enter**.

To Add an SNMP Trap Server

1. Type **snmp trap add <aaa.bbb.ccc.ddd> <community>** and press **Enter**.
    - <aaa.bbb.ccc.ddd> is the IP address of the trap server
    - <community> is the name of the community on the trap server, from 1-63 characters in length.
2. Type **save** or **commit** and press **Enter**.

The following example

- Sets the SNMP contact as `WaveRider`,
- Sets the SNMP location as `Calgary_South`,
- Adds the SNMP read community `WaveRider_Calgary`,
- Adds the SNMP write community `WaveRider_Calgary`,
- Adds the SNMP trap server `WaveRider_Calgary`, IP address `10.0.1.68`,
- Saves the new settings, and
- Displays the SNMP settings.

Example:

```
60:ff:fe>
60:ff:fe> snmp contact WaveRider
60:ff:fe> snmp location Calgary_South
60:ff:fe> snmp community add WaveRider_Calgary read
60:ff:fe> snmp community add WaveRider_Calgary write
60:ff:fe> snmp trap add 10.0.1.68 WaveRider_Calgary
60:ff:fe>
60:ff:fe> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
60:ff:fe>
60:ff:fe> snmp
Contact: WaveRider
Location: Calgary_South
Name: LMS3000
SNMP Read Communities:
        WaveRider_Calgary

SNMP Write Communities:
        WaveRider_Calgary
SNMP Traps:
       10.0.1.68 WaveRider_Calgary
60:ff:fe>
```

8.6 Configuring the Customer List

You can set the maximum number of customers or PCs (*customer_max*) that can concurrently access the radio link through the EUM, as described in *Bridge Table (EUM or CCU in Switched Ethernet or Through Only Mode)* on page 242.

NOTE: The simulation data presented in *Performance Modelling* on page 47 is based on one end user (one PC) per EUM.

TIP: When you are locally troubleshooting the EUM installation, if *customer_max* is set to ‘1’ and you want to substitute and use a known-working PC in place of the end-user’s PC, you will have to reset the EUM or wait for the Bridge Table to time out. You will not be able to access the EUM for 10 minutes.

To Set *customer_max*

1. Type **`cust max <value>`** and press **Enter**.
   - <value> is the maximum number of customers (PCs), from 1-50.
2. Type **`save`** or **`commit`** and press **Enter**.

The following example

- Sets *customer_max* to 3,
- Saves the new setting, and
- Displays the value of *customer_max*.

```
60:ff:fe>
60:ff:fe> cust max 3
Maximum customers: 3
60:ff:fe>
60:ff:fe> save
Basic Config saved
Port Filter Config saved
sntp cfg file saved
60:ff:fe>
60:ff:fe> cust max
Maximum customers: 3
60:ff:fe>
```

9 Installing the EUM

9.1 Before you Start the EUM Installation

NOTE: The following procedure assumes the end-user PC is using DHCP.

Before you start the EUM installation, ensure the following points have been addressed:

- The EUM has been configured with at least the following settings:
  - IP address
  - Subnet mask
  - Gateway IP address
  - Radio frequency
- The CCU network is installed and verified.
- DHCP is configured, including DHCP relay at the CCU if necessary
- The end-user PC is equipped with an Ethernet interface card, and is configured to obtain its IP address remotely, using DHCP.
- The installer knows the direction from the EUM to the CCU (CAP site).
- The installer has read this chapter.
- The installer knows the EUM IP address.
- The EUM is authorized at the CCU, or through RADIUS, possibly by setting a GOS other than "denied" as the default GOS (or no communications will be possible).

Procedures are provided below for addressing situations where some of the above items could not be taken care of prior to the EUM installation.

9.2 Other EUM Programming Considerations

Although the IP settings identified above are required for basic EUM operation, you should also consider pre-configuring the following EUM parameters:

SNMP

SNMP communities can be configured in the EUM to enable remote monitoring of the EUM using an SNMP manager. Refer to *Configuring SNMP* on page 140.

Customer List

The factory default configuration allows only one PC to be logically connected to the EUM at any given time. If you want to use a separate PC as an aid to installing and confirming the EUM link prior to connecting the end-user PC, then you will have to reset the EUM when changing between the end-user PC and the installation test PC. Refer to *Configuring the Customer List* on page 142.

Port Filtering

Port filtering is set in the EUM to filter out Network Neighborhood. You can edit Port filtering in the EUM, if desired. Refer to *Configuring Port Filtering* on page 139.

Output Power

In most cases, the EUM output power should be set to HIGH, unless the site has unique requirements for which a numerically set, or LOW power level, is more appropriate. For example, you may want to numerically set the power level to a lower value in high-density environments, where site-to-site interference is a problem.

9.3 Installation Overview

Installing the EUM involves the following procedures:

1. *Opening the Box* on page 145
2. *Turning off the End-user's Cordless Phones* on page 146
3. *Choosing a Location for the EUM and Antenna* on page 146
4. *Connecting the EUM Components* on page 146
5. *Conducting a Preliminary Check of the EUM* on page 149
6. *Positioning the Antenna* on page 149
7. *Mounting the Antenna* on page 151

8. *Connecting the End-user's PC* on page 154
9. *Obtaining Valid IP Addresses for the End-user's PC* on page 156
10. *Testing the Data Link* on page 156
11. *Configuring the Browser Application* on page 160
12. *Completing the Installation* on page 160
13. *Baselining the Installation* on page 160

9.4 Installation Procedures

9.4.1 Opening the Box

Before you install the EUM components, verify that the EUM kit is complete.

EUM Kit Components

- EUM modem
- AC/DC power supply with 2-meter DC power cable
- 2-meter AC power cable
- Crossover Ethernet cable with ferrite bead

Antenna Kit Components

- Indoor antenna with attached 3-meter cable
- Flush-mountable antenna bracket
- Two antenna-mount suction cups, two drywall plugs, and two screws

Refer to Figure 49 for an illustration of each EUM component.

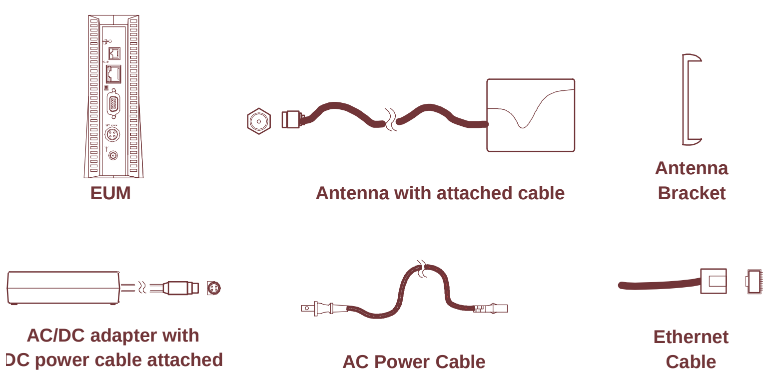


Figure 49 EUM Components

NOTE: The antenna-mount suction cups, drywall plugs, and screws are not shown in Figure 49.

9.4.2 Turning off the End-user's Cordless Phones

Turn off all cordless phones in the customer's premises, and any other equipment that uses the 900 MHz ISM band. Once the installation is complete, turn this equipment back on.

9.4.3 Choosing a Location for the EUM and Antenna

The location of the antenna has a significant effect on the performance of the EUM installation. Before you connect the EUM components, follow the guidelines provided below for choosing the best location for the antenna and the EUM.

Choosing the Best Location for the EUM

The best location for the EUM is

- indoors,
- upright,
- on a stable, flat surface, and
- in a position where its air vents are unobstructed.

NOTE: Avoid placing the EUM in direct sunlight or near other sources of heat (such as an electric heater).

Choosing the Best Location for the Antenna

The best location for the antenna is

- indoors,
- near an outside entrance or window, preferably in the location with the best possible path to the CCU, and
- a minimum of 20 cm (8 in.) from personnel.

9.4.4 Connecting the EUM Components

Now that you have chosen a suitable location, use the instructions in this section for connecting the following components to the EUM, in the order shown in Figure 50:

- Antenna
- EUM AC/DC adaptor (DC cable first, then AC cable)

When you have completed the above tasks, connect the EUM AC/DC adaptor to an AC power bar or outlet.

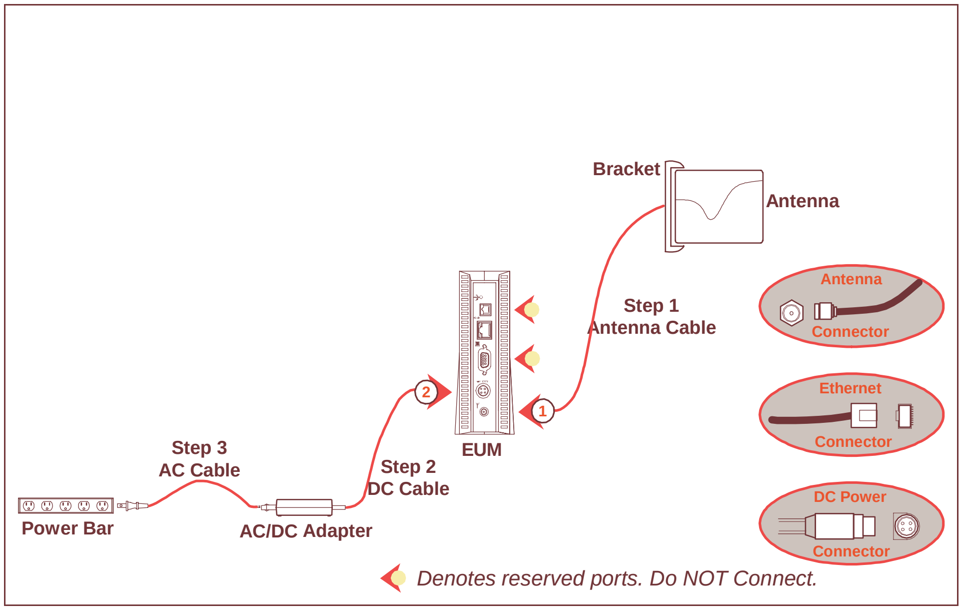


Figure 50 Connecting the EUM Components

To Connect the EUM Components

1. Finger-tighten the antenna cable onto the corresponding connector at the back of the EUM (refer to Step 1 in Figure 50). Do not use wrenches or pliers. Do not cross-thread or over tighten.
2. Connect the AC/DC adaptor to the EUM. To do this, line up the guides in the DC power cord connector with the notches in the power plug on the EUM and press the connector firmly into place (refer to Figure 51).

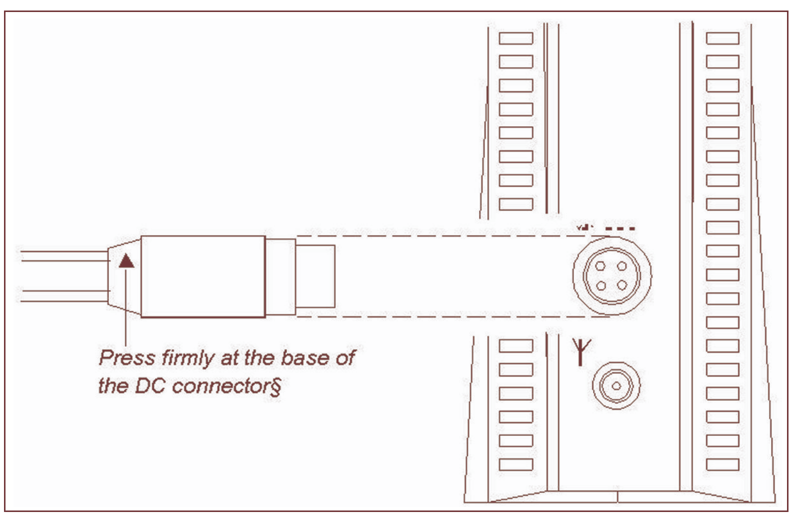


Figure 51 Connect the DC Power Cord to the EUM

NOTE: The DC power cable features a secure locking connector. To disconnect the cable, pull the collar back on the connector, then continue pulling to detach the DC power cable from the EUM.

The EUM uses a custom antenna cable and connector. If you need to extend this cable, contact WaveRider Communications Inc.

3. Connect the AC power cord between the AC/DC adaptor and either an AC power bar (preferred) or AC outlet (Figure 52). The EUM immediately powers up since it does not have an ON/OFF switch.

   NOTE: To avoid potential damage to the EUM components in the event of a power surge, WaveRider recommends using a power bar with surge protection (instead of connecting the AC power cord directly to an AC outlet).

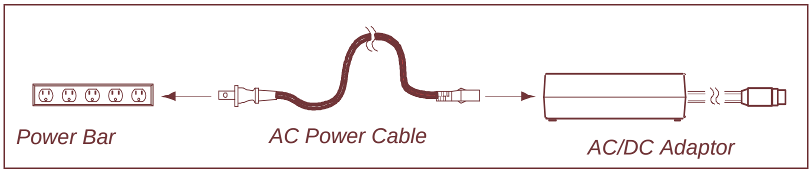


Figure 52 Connect the AC Power Cord

9.4.5 Conducting a Preliminary Check of the EUM

Check the LED indicators on the front of the modem to ensure that the EUM is functioning properly.

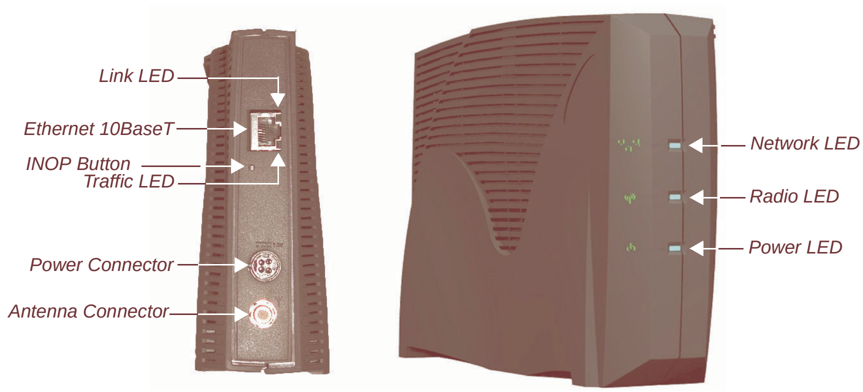


Figure 53 EUM3003 LEDs

Figure 54 EUM3000 LEDs

To Verify Proper EUM Function

- Check that the Power LED is ON. It takes about 7 or 8 seconds to come on after you have plugged in the unit.

9.4.6 Positioning the Antenna

This section explains how to align the EUM antenna. There are four tools available to help with antenna alignment:

- LEDs
- RSSI
- EUM Configuration Utility
- WaveRider Antenna Alignment Tool

The WaveRider Antenna Alignment Tool is an easy to use, Windows-based tool for distribution with EUMs for subscribers who install their own EUMs. Before providing this tool to your subscribers, you should perform a drive test to ensure the subscriber area has coverage. The tool works with EUMs running software version 3.4 or higher, and it requires a unique softkey to access the EUM. You can download the EUM Antenna Alignment Tool from the WaveRider website at http://www.waverider.com.

To Align the EUM Antenna

1. Connect the indoor antenna to the EUM and power up the EUM.
2. Point the antenna in the general direction of the CCU, as shown in Figure 55.

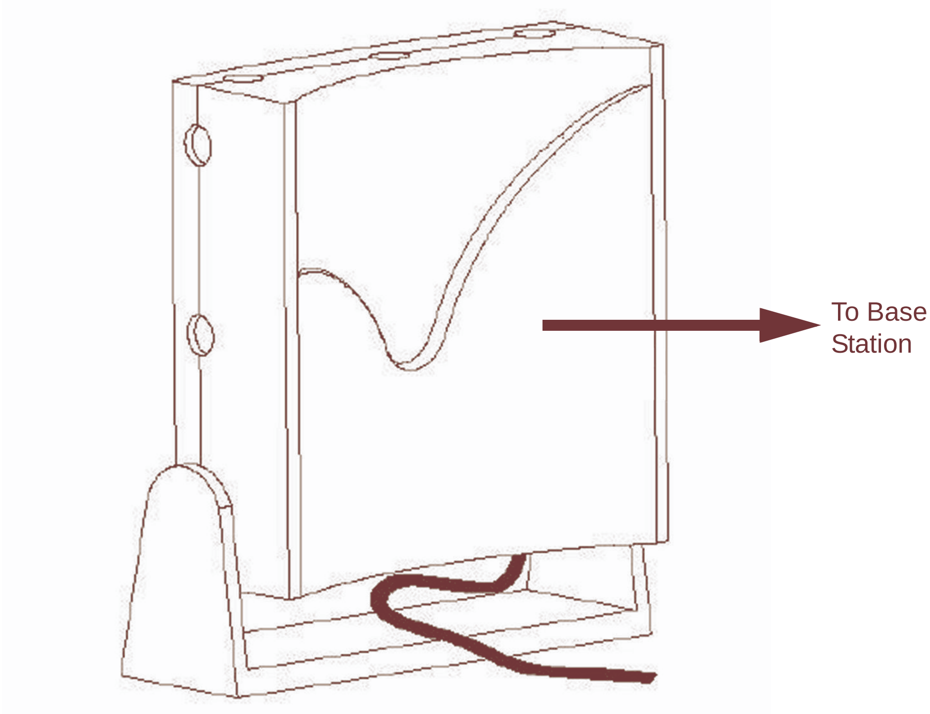


Figure 55 Preliminary Orientation of the Antenna (Top View)

As illustrated, for maximum signal reception, point the concave surface of the antenna toward the CCU, and ensure your body (including fingers) are not between the antenna and the CCU.

NOTE: Moving the antenna only 10 cm can significantly change the link quality.

3. Once the EUM is fully booted, monitor the Radio LED, shown in Figure 53 on page 149 and refer to Table 23. Move the antenna until the Radio LED is flashing quickly, or is ON solidly, indicating that you have a good to very-good radio signal. After each repositioning or reorientation of the antenna, you may have to step back from the antenna so that you are not interfering with the received signal. Use Table 23 on page 150 as a guide.

Table 23 Radio LED Status Displays

Radio LED Display	Status
Off	No radio signal present.

Radio LED Display	Status
Slow Flash	ON/OFF 0.83 times per second. The signal strength is poor to marginal.
Fast Flash	ON/OFF 2.5 times per second. The signal strength is good.
Solid On	The signal strength is very good.

4. If the best location produces a *Fast Flash* or *ON Solid* Radio LED, then the received signal level is good to excellent, and this is a good location to install the antenna.
5. If the Radio LED is off or flashes slowly, then the antenna should be moved to a better location. Keep in mind that the antenna and EUM do not have to be located in the same room as the end-user's PC since up to 100 m (300 ft.) of CAT5 data cable with a ferrite bead can connect the EUM to the PC. To attain the best possible signal below the Fast Flash LED level, turn on the Continuous RSSI through the command-line interface, as follows:

```
60:ff:fe> rad rssi
Press any key to stop

RSSI[dBm]   RX;  TX;  R1;  R2;  R3;   F;Retry%;  SQ; RNA; RNB
RSSI: -36    0;   0;   0;   0;   0;   0;      0;   7;  71;  71
RSSI: -36   18;   2;   0;   0;   0;   0;      0;   5;  72;  71
RSSI: -36   18;   2;   0;   0;   0;   0;      0;   8;  73;  72
RSSI: -36   18;   3;   0;   0;   0;   0;      0;   6;  73;  72
RSSI: -37   18;   2;   0;   0;   0;   0;      0;   5;  72;  72
RSSI: -37   18;   2;   0;   0;   0;   0;      0;   6;  71;  71
RSSI: -36   18;   2;   0;   0;   0;   0;      0;   5;  72;  72

60:ff:fe>
```

6. Adjust the antenna location and pointing for maximum RSSI. You may need to adjust the antenna and then step back each time to read the RSSI, so you do not obstruct the signal from the CCU.
7. Once you have found a good location, you are ready to mount the antenna, as described in *section 9.4.7*, Mounting the Antenna.

9.4.7 Mounting the Antenna

The antenna bracket is designed to accommodate the RF cable and act as a strain relief.

To Mount the Antenna

1. Thread the attached antenna cable through the guides in the back of the antenna bracket, as necessary.

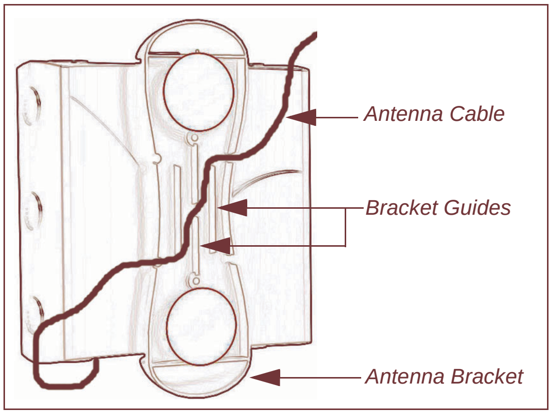


Figure 56 Rear View of Antenna Bracket

NOTE: Bending the antenna cable too sharply can degrade EUM performance. Never allow less than a 1.25 cm (0.5 in.) bend radius. If a quarter (25-cent piece) fits into the curve, the bend is acceptable.

The EUM kit includes suction cups, drywall plugs, and screws to allow a variety of mounting options:

Table 24 Antenna Mount Guidelines

Mounting Method	Guidelines
Suction Cups	Use on flat, smooth surfaces, such as glass, plastic, laminates or metal. Remove all grease, oil, and grit before securing the antenna bracket with suction cups.
Drywall Plugs	Use on all commercial drywall and other plaster surfaces.
Screws	Use on hardwood surfaces.

2. Insert the suction cups or screws into the base of the antenna bracket, then mount the bracket onto the desired surface.

NOTE: If you mount your antenna bracket on a vertical surface, orient the bracket so that the spring clip is closest to the ceiling.

Figure 57 shows the location of the spring clip, suction cup holes, and screw holes on the antenna bracket.

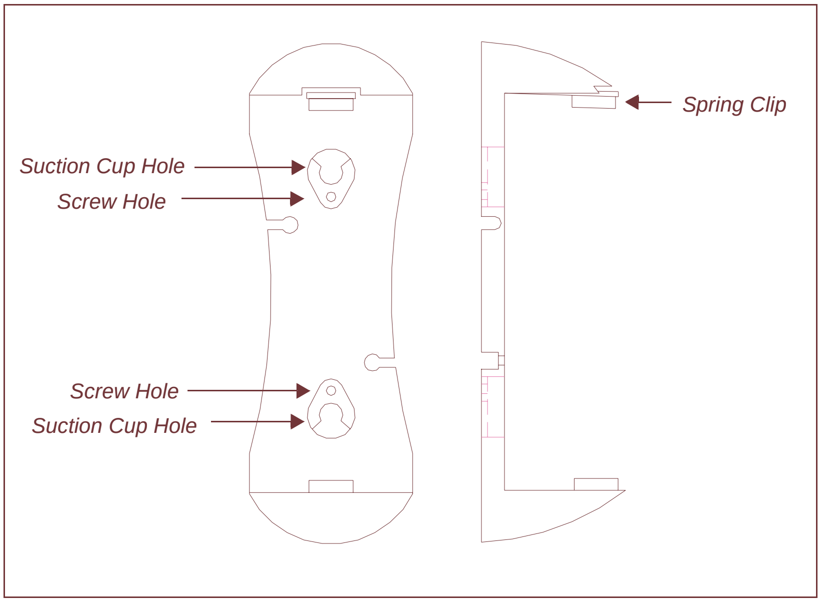
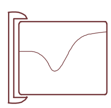
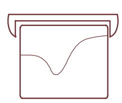
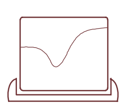
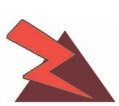


Figure 57 Antenna Bracket Components

Table 25 Surface Mounting Options for the Antenna

Side Mount 	Mount the antenna on a wall, window, window frame, or solid furniture with spring clip side closest to the ceiling.
Top Mount 	Hang the antenna from a ceiling or the shelf of a bookcase.
Bottom Mount 	Mount the antenna on solid furniture (a desk or shelf) or on a window sill.

WARNING!



The antennas for the EUM must be fix-mounted, indoors or outdoors, to provide a separation distance of 20cm or more from all persons, to satisfy RF exposure requirements. The distance is measured from the front of the antenna to the

human body. WaveRider recommends installing the antenna in a location where personnel are not able to bump into it, obstruct the signal from the base station, or trip over antenna cables.

3. Position the antenna in the bracket according to one of the configurations illustrated in Figure 58. Click and lock the antenna in place. For maximum signal reception, ensure the concave surface of the antenna points toward the WISP antenna and the trough of the inset wave points towards the floor.

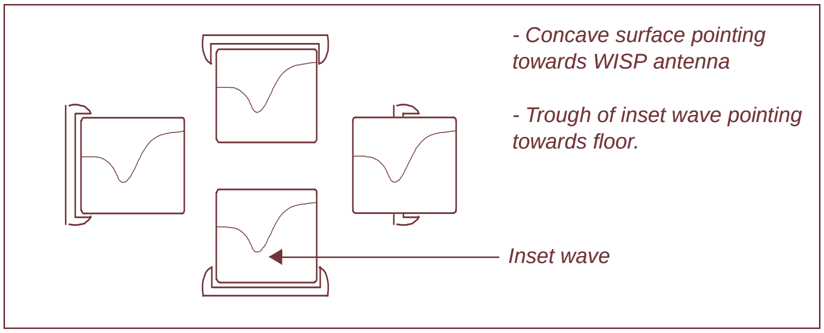


Figure 58 Mounting the Antenna in the Bracket

NOTE: The location, position, and orientation of the antenna affects the robustness of the Internet connection. Pointing the antenna at buildings or other obstacles often impedes communications, but some surfaces may provide desirable signal bounce. For optimal reception, try various positions before fix-mounting your antenna.

4. Once the antenna is permanently mounted, re-align it for best signal.

9.4.8 Connecting the End-user's PC

CAUTION: Any DC voltage applied to the Ethernet port may damage the EUM, the Ethernet cable, and/or the network gear. The EUM is not a Power-over-Ethernet device.

1. Connect the end-user's PC, shown in Figure 59, by attaching the crossover Ethernet cable with ferrite bead that is included with the kit between the Ethernet port on the end-user's computer and the Ethernet port on the EUM.

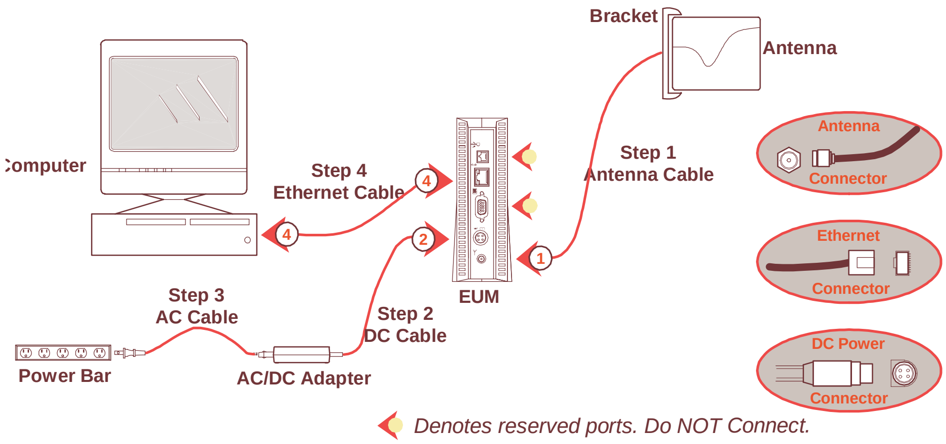


Figure 59 Connecting the End-user's PC

2. Check the Ethernet LEDs on the back panel of the EUM to ensure the Ethernet connection between the EUM and the end-user's PC is active. Refer to Table 26 for an explanation of the Ethernet LED status displays.

Table 26 Ethernet LED Status Displays

Ethernet LED	Status
Ethernet Link LED	This LED is lit when there is a correct connection to the computer, and both ends are powered ON.
Ethernet Traffic LED	Flashes when data passes through the Ethernet connection in either direction.

3. When attempting to send data to, or receive data from, the Internet, check the Ethernet Traffic LED to ensure data transmission is taking place. This LED flashes as data traffic passes between the end-user's PC and the EUM. The network LED on the front of the EUM also flashes and is more accessible than the Traffic LED on the rear of the EUM.