SIEMENS

RUGGEDCOM APE

User Guide

01/2016
RC1121-EN-02

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd..

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address
Siemens Canada Ltd.
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

Web
www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes how to install and configure the RUGGEDCOM APE in any RUGGEDCOM RX15xx device. Its purpose is to familiarize users with the ways that RUGGEDCOM APE can be used to support processing applications in RX15xx networks. It includes information about:

- The RUGGEDCOM APE module
- Obtaining, installing and using the RUGGEDCOM APE software
- Configuring networks with RUGGEDCOM APE
- Creating and loading recovery images
- Troubleshooting

This guide is intended for use by network technical support personnel who are familiar with the operation of networks and the supplied operating system (i.e. Windows, Linux, Check Point, etc.). Others who might find the book useful are network and system planners, system programmers, and line technicians.

Alerts

The following types of alerts are used when necessary to highlight important information.

DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.

NOTE
NOTE alerts provide additional information, such as facts, tips and details.

CLI Command Syntax

The syntax of commands used in a Command Line Interface (CLI) is described according to the following conventions:

Example	Description
command	Commands are in bold.
command parameter	Parameters are in plain text.
command parameter1 parameter2	Parameters are listed in the order they must be entered.
command parameter1 *parameter2*	Parameters in italics must be replaced with a user-defined value.
command [parameter1 | parameter2]	Alternative parameters are separated by a vertical bar (|). Square brackets indicate a required choice between two or more parameters.
command { parameter3 | parameter4 }	Curly brackets indicate an optional parameter(s).
command parameter1 parameter2 { parameter3 | parameter4 }	All commands and parameters are presented in the order they must be entered.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM RX1500 Installation Guide*
- *RUGGEDCOM RX1501 Installation Guide*
- *RUGGEDCOM RX1510 Installation Guide*
- *RUGGEDCOM RX1511 Installation Guide*
- *RUGGEDCOM RX1512 Installation Guide*

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

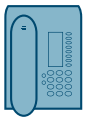
Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

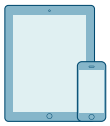
Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

Online
Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.



Telephone
Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.



Mobile App
Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Overview

The RUGGEDCOM APE (Application Processing Engine) is an x86-based computer designed to occupy a single line module slot in a RUGGEDCOM RX15xx device. The APE can host a variety of x86-based operating systems and features Gigabit Ethernet, USB ports and a DVI-D Video port.

The following RUGGEDCOM APE models are available:

- APE1402
- APE1402W7
- APE1404
- APE1404W7
- APE1404CKP (Requires a valid Check Point GAiA™ license for activation)

CAUTION!
Electrical hazard – risk of power failure. Installing more RUGGEDCOM APE modules than allowed on an RUGGEDCOM RX15xx device can lead to power fluctuations and irregular shut downs. On an RX1512 device, do not install more than one RUGGEDCOM APE module. On an RX1500, RX1501, RX1510 or RX1511 device, do not install more than two RUGGEDCOM APE modules.

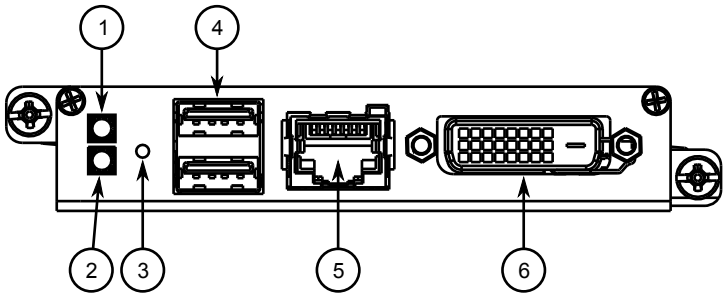


Figure 1: RUGGEDCOM APE Module

1. Drive Activity LED **2.** Power LED **3.** Power Button **4.** USB Ports **5.** Gigabit Ethernet (GbE) Port **6.** DVI-D Video Port

NOTE
For installation instructions and technical specifications, refer to the Installation Guide for your RUGGEDCOM RX15xx device.

The following sections describe the RUGGEDCOM APE in more detail:

Section 1.1

Security Recommendations

To prevent unauthorized access to the module, note the following security recommendations:

Hardware/Software

- Before using the Linux-based version of the RUGGEDCOM APE, make sure all relevant CERT security advisories and applications are applied. Security advisories that include links to applications are available on the Industrial Security website [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Only enable the services that will be used on the module, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the module.

Authentication

- Replace the default passwords (if configured) before the module is deployed. For a list of default user profiles and passwords, refer to Section 2.1, “Logging in to APE”.
- Replace the default boot and BIOS passwords before the module is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc.
- Passwords should not be re-used across different usernames and systems, or after they expire.
- SSL and SSH keys are accessible to users who connect to the module via the gigabit Ethernet port. Make sure to take appropriate precautions when shipping the module beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with *throwaway* keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the module returns, create and program new keys for the module.
- When connecting to the RUGGEDCOM APE via SSH, configure the SSH client to:
  - Use Counter (CTR) operation mode based ciphers. CTR mode is considered more secure than Cipher Block Chaining (CBC) operation mode.
  - Use SHA1 (256 bit) and SHA2 (512 bit) MAC algorithms. These are considered more secure than MD5 and 96 bit MAC algorithms.

Communication

- Log messages should be delivered using TLS-encrypted syslog over TCP to prevent them from being sent as plain text.

Physical/Remote Access

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Control access to the USB and gigabit Ethernet ports to the same degree as any physical access to the module. Access to these ports allows for potential access to BIST mode, which includes tools that may be used to gain complete access to the module.

- If a firewall is required, configure and start the firewall before connecting the module to a public network. Make sure the firewall is configured to accept connections from a specific domain. For more information, refer to Section 2.2, “Using the APE as a Firewall”
- Be aware of any non-secure protocols enabled on the module. While some protocols, such as HTTPS, SSH and 802.1x, are secure, others, such as Telnet and RSTP, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the module/ network.

Policy

- Periodically audit the module to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with for further security recommendations.

Section 1.2
Operating Temperature Range and Behavior

The RUGGEDCOM APE is rated for operation within the temperature range of -40 to 70 °C (-40 to 158 °F).

Section 1.3
Rebooting/Powering Down the APE Module

The RUGGEDCOM APE may be powered down or reset using the **Power** button on the front face of the module. The **Power** button is recessed and can only be reached using either a pin, unfolded paper clip, or a small screwdriver.

IMPORTANT!
*Whenever possible, shut down or reboot the RUGGEDCOM APE from the operating system instead of requesting a shutdown or reboot with the **Power** button. This helps to safeguard against improper shutdowns and protect data integrity.*

Powering Down the RUGGEDCOM APE

To fully power down the module, press the **Power** button with a pin and hold for 4 to 5 seconds.

Rebooting the RUGGEDCOM APE

To reset the module, quickly press and release the **Power** button with a pin.

Section 1.4
BIOS Configuration and Hardware Drivers

The RUGGEDCOM APE module features a BIOS with functionality similar to that of a typical PC.

NOTE
Siemens does not recommend updating/upgrading the BIOS software on the RUGGEDCOM APE module. Contact Siemens Customer Support for assistance with BIOS-related issues.

The following BIOS settings can be configured:

- System Time
- Processor Options
- Boot Options
- Security Options

The most commonly changed options are the boot options, as the USB ports need to be made bootable to install an operating system.

To display the BIOS menus, press **F2** immediately after the RUGGEDCOM APE starts to boot up. To display BIOS help, press **F1** and follow the instructions at the bottom of the screen.

To change the boot device, press **F5** immediately after the RUGGEDCOM APE starts to boot up. The RUGGEDCOM APE will boot from the chosen device. During the next boot cycle, the RUGGEDCOM APE will revert back to the default boot device selected in the BIOS.

Contact Siemens if any BIOS-related issues are experienced.

Section 1.5

Secondary Network Interface

In addition to the gigabit Ethernet interface on the faceplate, the RUGGEDCOM APE features a secondary gigabit Ethernet interface on the back of the module that interfaces with the host RUGGEDCOM RX15xx device. The interface can be used by the operating system running on the RUGGEDCOM APE as a normal network interface. Typical port parameters for the secondary interface, such as speed, duplex, VLANs, and more, can be configured via RUGGEDCOM ROX II.

IMPORTANT!
Interface settings configured via RUGGEDCOM ROX II must be mirrored within the RUGGEDCOM APE module. For instance, if a VLAN is assigned to the module in RUGGEDCOM ROX II, a corresponding VLAN must also be configured via the module's operating system.

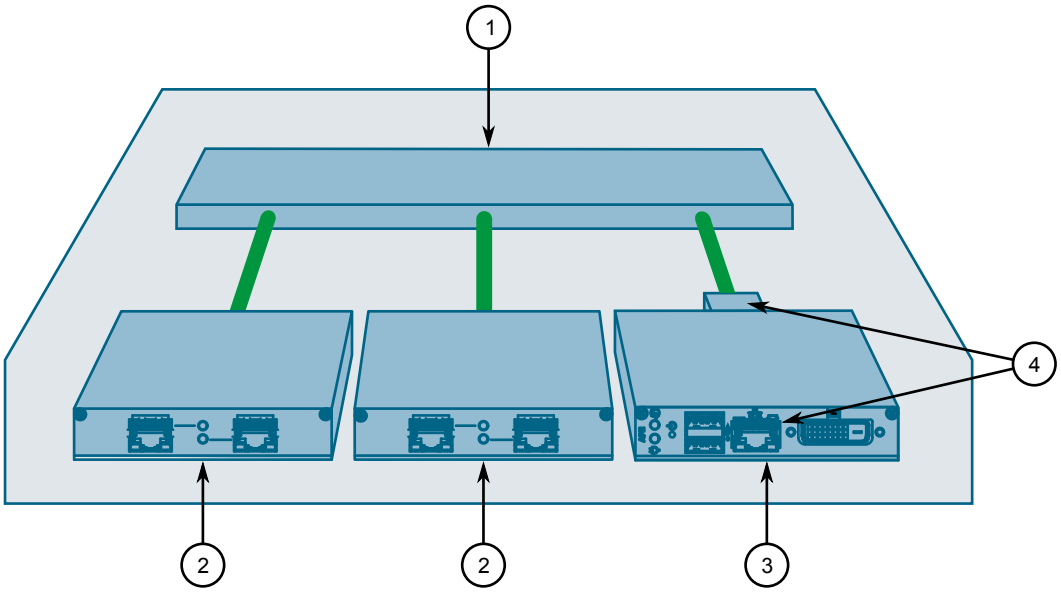


Figure 2: A RUGGEDCOM RX15xx Device With an RUGGEDCOM APE Module Installed

1. Switch Fabric Data Plane **2.** Line Module (10/100/1000Base-TX) **3.** APE Module **4.** Gigabit Ethernet (GbE) Network Interfaces

Section 1.6

Available Software Platforms

Siemens provides the following software platforms on the RUGGEDCOM APE:

- Windows® Embedded Standard 7
- Debian Linux®
- Check Point GAiA™

NOTE
The RUGGEDCOM APE platform is open and may support other software platforms, such as Linux Mint or Ubuntu.

IMPORTANT!
Siemens does not support any software installed on the RUGGEDCOM APE. This includes, but is not limited to, software images provided by Siemens Customer Support.

Section 1.7
Suggested Software

Redo Backup and Recovery

Redo Backup and Recovery is a free and easy-to-use backup and recovery utility available for private and corporate use. To download Redo Backup and Recovery or for more information, refer to (www.redobackup.org).

RUGGEDCOM ELAN SCADA Application Suite

NOTE
The RUGGEDCOM ELAN SCADA Application Suite is only available for Linux platforms.

Siemens's RUGGEDCOM ELAN product family solves a wide range of communications and data integration problems, from the substation to the control center and into the enterprise. The RUGGEDCOM ELAN family of products provide:

- Open, flexible access to all substation and distribution devices, from any authorized user or application
- Preservation of investment in legacy devices and control center applications
- Protocol conversion/normalization
- Support for both SCADA and non-SCADA hosts (e.g. PI historian)
- Automated retrieval of fault file data
- Powerful automation processor
- Reliable extraction/presentation of relay target data
- Wide range of security options

For more information about RUGGEDCOM ELAN, visit www.siemens.com/ruggedcom.

Section 1.8
Default IP Addresses

Based on the software platform installed on the RUGGEDCOM APE, the IP addresses for the front and/or internal ports may be pre-configured or set dynamically by the Domain Host Configuration Protocol (DHCP).

Software Platform	External Port (RJ45)	Internal Port
Windows® Embedded Standard 7	DHCP	DHCP
Debian Linux®	Not Configured	DHCP
Check Point GAiA™ OS	Not Configured	169.254.100.100

Section 1.9

Ethernet and Network Settings

The RUGGEDCOM APE is essentially a two-port industrial computer. When the RUGGEDCOM APE is inserted into a chassis, the first *internal* Ethernet port is activated on the connector that carries power to to the RUGGEDCOM APE. The second RUGGEDCOM APE Ethernet port is available for use on the faceplate of the RUGGEDCOM APE line module.

To the RX15xx device, the RUGGEDCOM APE Ethernet port appears like any other Gigabit capable routed port.

For examples of how the RUGGEDCOM APE can be configured in a RX15xx device, refer to Section 1.9.1, “Example: Networking in Factory Default Conditions” and Section 1.9.2, “Example: RX15xx Services and WAN Networking”.

Section 1.9.1

Example: Networking in Factory Default Conditions

The following figure illustrates how routing and switching would work when the RUGGEDCOM APE is used in a chassis with a four-port Ethernet module in LM2.

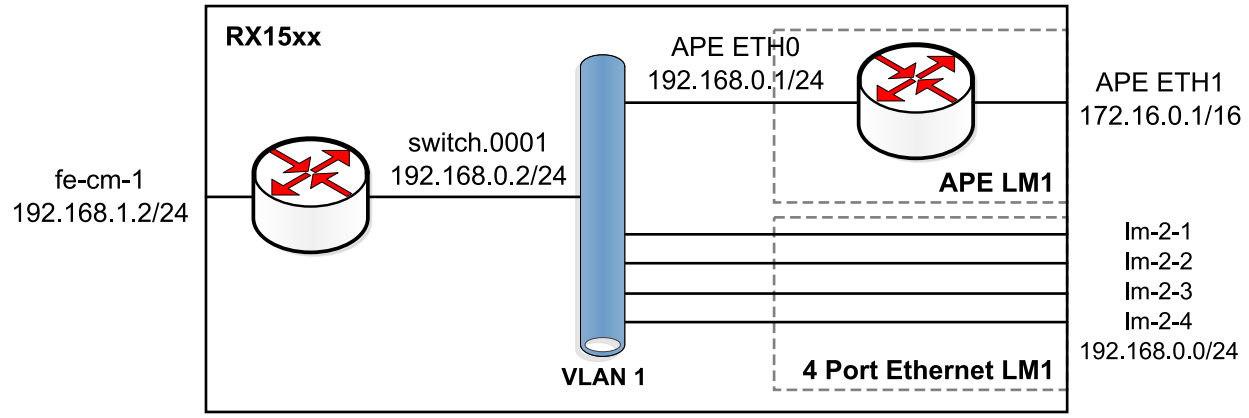


Figure 3: Example Configuration

In the factory default condition, all Ethernet interfaces (including the internal port of the RUGGEDCOM APE) are created as switched ports in the default VLAN. An IPv4 subnet and gateway IP are automatically assigned to this VLAN.

The factory default conditions for this VLAN are to use PVID 1 and to operate untagged. The factory default creates the switch group (switch.0001) for devices on this VLAN and creates a virtual interface 192.168.0.2/24 for devices (such as the RUGGEDCOM APE) in switch.0001 to reach services on the control module and network management.

In this situation, the RUGGEDCOM APE can be assigned an unused IP address in subnet 192.168.0.0/24 and communicate with other devices in VLAN1 at a bridging and routing level. In Figure 3, the RUGGEDCOM APE ETH0 interface has been assigned an address of 192.168.0.1 to allow it to communicate on VLAN1. It has also been assigned a unique subnet to its ETH1 port.

The RUGGEDCOM APE can also access services and network management of the RX1500 control module at its 192.168.0.2 address. These services include SSH, HTTP and HTTPS services for network management, DHCP, NTP and TCP connections to chassis serial ports.

The RUGGEDCOM APE can also communicate with any hosts on interfaces lm-2-1 through lm-2-4.

Should you wish to configure the RUGGEDCOM APE to forward traffic through to the 192.168.1.0/24 network via fe-cm-1, you would need to configure 192.168.0.2 as a default gateway.

For much the same reason, should you wish to forward traffic arriving on fe-cm-1 through to the 172.16.0.0/16 network via the RUGGEDCOM APE, you would need to configure a route for it on the RX15xx device.

NOTE

When operating the RUGGEDCOM APE in either switch or router mode, the RX15xx will issue RSTP BPDUs to the RUGGEDCOM APE.

If you do not wish the RUGGEDCOM APE to receive these BPDUs, they may be disabled in RUGGEDCOM in the interface switch menu for the RUGGEDCOM APE interface.

Section 1.9.2

Example: RX15xx Services and WAN Networking

The following illustration shows how the RUGGEDCOM APE might be used in a more complex situation in which it is routed as opposed to bridged. The use of internal serial ports, firewalls and port forwarding is discussed.

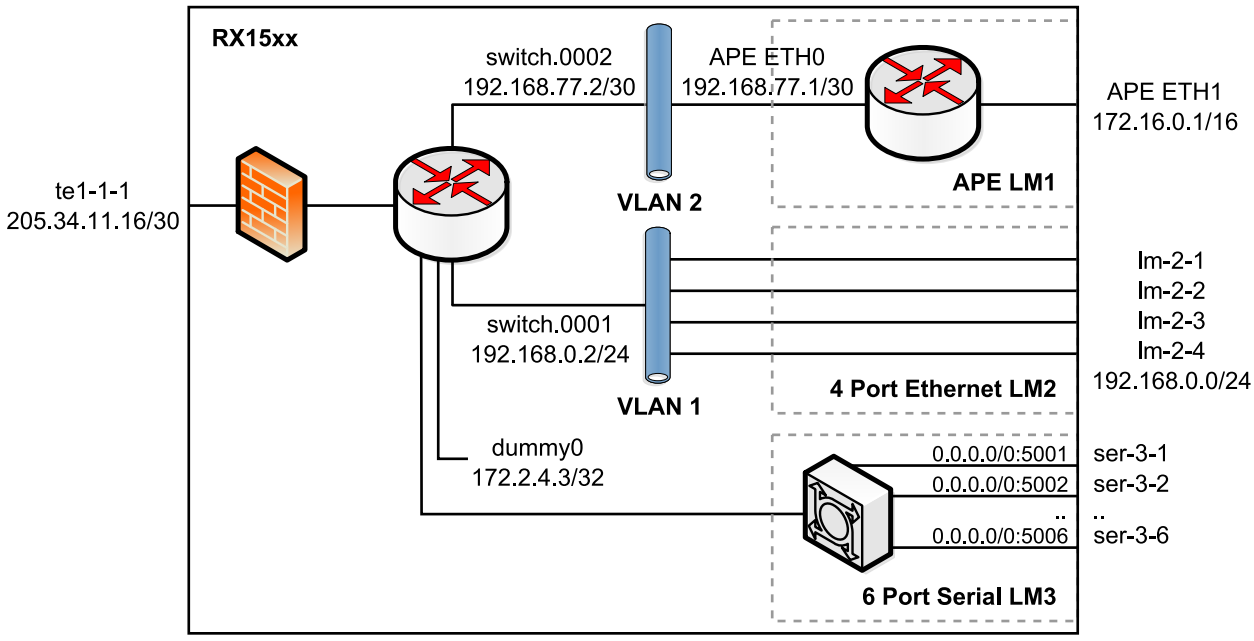


Figure 4: Example Configuration

In this scenario, the RUGGEDCOM APE is reached via a routed interface. This is accomplished by moving the RUGGEDCOM APE port onto its own VLAN, and creating a point-to-point connection between it and the control module.

NOTE
The default route must be set to 192.168.77.2 on the RUGGEDCOM APE in order for the RUGGEDCOM APE to communicate with the control module.

The figure shows six serial ports available on serial LM 3. In order to become network, accessible these ports are configured as raw socket ports allowing incoming calls on TCP ports 5001 (ser-3-1) through 5006 (ser-3-6). By the nature of the RX1500, these ports are reachable at any address on the RX1500 control module. Good candidate addresses for the RUGGEDCOM APE to use to connect to the serial ports include those of the switch.0001, switch.002 and dummy0 addresses. Specifying a dummy address is also a very useful idea if router redundancy is to be implemented.

As in the previous scenario, devices on the 192.168.0.0/24 subnet are still available to the RUGGEDCOM APE, but through routing.

2 Configuring and Using the APE

The following sections describe how to configure and use the RUGGEDCOM APE:

IMPORTANT!
Before using the RUGGEDCOM APE, create a backup image. This image can be restored at any time should the module be configured improperly. For more information about creating a backup image, refer to Section 2.14, "Creating and Restoring Backup Images".

Warranty does not support modules rendered inoperable/inaccessible due to configuration errors made by the user.

Section 2.1

Logging in to APE

Use the following default username and password to log in to the RUGGEDCOM APE:

WARNING!
To prevent unauthorized access to the device, make sure to change the default password before commissioning the device.

Software Platform	Default Username	Default Password
Windows® Embedded Standard 7	There is no default username or password for Windows® Embedded Standard 7 installations. The username and password is set by the user during the first boot.	

Software Platform	Default Username	Default Password
Linux	root	admin
GAiA	admin	admin

Section 2.2
Using the APE as a Firewall

The RUGGEDCOM APE can be used as a firewall, as an external network interface, or as a one-armed firewall.

As an *external network interface*, the unprotected network is attached to the RUGGEDCOM APE external Ethernet port and a firewall application, such as Shorewall or Check Point GAiA, is used. The RUGGEDCOM APE firewall acts as the primary router and forwards traffic to the RX15xx device. This scenario is ideal when Layer 2 device hardware is used.

NOTE
The GAiA firewall is offered as an alternative to the default firewall that comes on all RX15xx devices. The GAiA firewall is a widely used and accepted firewall used in enterprise and industrial applications and offers easy-to-use management capabilities for deployments where many firewalls must be set up and maintained. The GAiA firewall may be installed by the factory at the time of ordering or installed in the field using software obtained from www.checkpoint.com.

NOTE
Shorewall firewalls are used for Linux distributions. For more information about configuring Shorewall firewalls, refer to http://shorewall.net.

As a *one-armed firewall*, the external network is supplied by an Ethernet or WAN port on the RX15xx device. The traffic on this port is restricted to a VLAN shared with the RUGGEDCOM APE firewall. Traffic inspected and allowed by the RUGGEDCOM APE firewall is returned to the RX15xx device on other VLANs.

Section 2.3
Upgrading Windows® Embedded Standard 7 Drivers

Windows® Embedded Standard 7 drivers for the Atom-e6xx chip set used on the RUGGEDCOM APE module can be obtained from Siemens. For more information, contact Siemens Customer Support.

NOTE
Updated drivers are typically provided with each Linux distribution.

To upgrade the Windows® Embedded Standard 7 drivers, do the following:

1. Obtain a copy of the drivers from Siemens Customer Support.
2. Extract the files and transfer them to a temporary directory on the RUGGEDCOM APE module.
3. Log in to Windows® on RUGGEDCOM APE as an administrator.
4. For each driver, run `setup.exe` and follow the instructions provided.

NOTE
If warned that a driver has not been digitally signed, ignore the warning and continue with the installation. This is expected behavior.

5. Reboot the device.
6. Log in to Windows® on RUGGEDCOM APE as an administrator.
7. Open *Device Manager*. A list of detected hardware devices appears.
8. Verify the new drivers appear in the list of detected hardware devices.

Section 2.4
Adding a User (Linux Only)

To add a new user, type:

```
adduser name
```

Where:

- *name* is the name of the user

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

Follow the instructions provided to complete the user profile. For example:

```
root@wheezyape:~# adduser admin
Adding user `admin' ...
Adding new group `admin' (1000) ...
Adding new user `admin' (1000) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
 Full Name []: Administrator
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] y
root@wheezyape:~#
```

Section 2.5
Setting the Root and User Passwords (Linux Only)

The default user and root Linux passwords must be changed before the module is deployed.

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

Changing the Root Password

To change the default root password for Linux, do the following:

1. Login or gain root access.
2. Type **`passwd`** and follow the on screen instructions.

Changing User Passwords

To change the password for a user profile, type:

```
passwd user
```

Where:

- *`user`* is the user name (e.g. root, admin, operator, guest, etc.)

Section 2.6

Setting the BIOS Password

A password for the RUGGEDCOM APE BIOS is not set by default.

To set the BIOS password, do the following:

IMPORTANT!
If the BIOS password is lost, the module must be returned to Siemens for service. For more information, contact Siemens Customer Support.

This service is not supported by warranty.

1. Make sure a recent backup image is available before setting the BIOS password. For more information about creating a backup image, refer to Section 2.14, “Creating and Restoring Backup Images”.
2. Power on the RUGGEDCOM APE.
3. Press **F2** to access the BIOS.
4. Select **Security**.

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

NOTE
Users logging in to the BIOS using a user password can only change settings for their own account.

NOTE
Supervisor-level users are granted full control of all RUGGEDCOM APE settings.

5. Set the supervisor and user passwords.
6. Press **F10** to save and reboot.

Section 2.7
Setting the BIOS Bootloader Password

The BIOS bootloader can be configured to authenticate users before the BIOS is loaded.

IMPORTANT!
If the BIOS bootloader password is lost, the module must be returned to Siemens for service. For more information, contact Siemens Customer Support.

This service is not supported by warranty.

To set the BIOS bootloader password, do the following:

NOTE
Only supervisor-level users are permitted to change the BIOS bootloader password.

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

1. Power on the RUGGEDCOM APE.
2. Press **F2** to access the BIOS.
3. Enter the supervisor password to access the BIOS.
4. Select **Security**.
5. Set **Authenticate to Boot** to **Enabled**.
6. Press **F10** to save and reboot.

Section 2.8
Setting the GRUB Bootloader Password

To set the GRUB bootloader password, do the following:

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

1. Login or gain root access.
2. Create the GRUB bootloader password by typing:

```
grub-mkpasswd-pbkdf2
```

Type the new password when requested. GRUB displays a message similar to the following:

```
Your PBKDF2 is grub.pbkdfs.sha512.10000.{salt}.{hashed_password}
```

Record the password for future use in the upcoming steps.

3. Using vim or nano, open the file /etc/defaults/grub.password.
4. In the file /etc/defaults/grub.password, locate the the following line:

   ```
   GRUB_USER=
   ```

   Add a username (e.g. root) to this line. For example:

   ```
   GRUB_USER=root
   ```

5. Locate the the following line:

   ```
   GRUB_ENCRYPTED_PASSWORD=
   ```

   Add the GRUB password created in Step 2 to this line. For example:

   ```
   GRUB_ENCRYPTED_PASSWORD=grub.pbkdf2.sha512.10000.82BA3D30037BBBB0A5EEED9395A036E973299517EAC3530A46
   45406C692279EBDF12603E11E0E2F02BF32888A2F61DD8467FA8C0F3641CF8FDA452F40571E988.BF312D710D4E451A63264
   C47C8CCBF40D429E1D6FF21D6AE95CA36F2D9AEE44C37AE1DF59C5303A9736840C7B2BBC1AA8045984FB6017F08559B11D0C
   19E5E0F
   ```

6. Save and close the file.
7. Apply the GRUB bootloader password by typing:

   ```
   update-grub
   ```

8. Using vim or nano, open the file `/boot/grub/grub.cfg` and verify the username and password defined within are correct.

Section 2.9

Setting the Hard Drive Password

To set a password for the hard drive, do the following:

CAUTION!
Configuration hazard – risk of data loss. Losing the hard drive password will render the device inaccessible and all data will be lost. In this situation, contact Siemens Customer Support for assistance.

This service is not supported by warranty.

IMPORTANT!
If the hard drive password is lost, the module must be returned to Siemens for service. For more information, contact Siemens Customer Support.

IMPORTANT!
Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc.

1. Power on the RUGGEDCOM APE.
2. Press **F2** to access the BIOS.
3. Enter the supervisor or user password to access the BIOS.
4. Select **Security**.
5. Set the HDD000 password.
6. Set **Flash Controller Lock** to **Enabled**.
7. Set **HDD password state** to **User+Master** or **User**.
8. Press **F10** to save and reboot.

Section 2.10
Disabling Alternative Boot Options

To prevent users with physical access to the module from logging in to the device and bypassing the bootloader password, it is recommended that alternative, unauthorized boot options be disabled before the module is deployed.

To disable alternative boot options, do the following:

1. Power on the RUGGEDCOM APE.
2. Press **F2** to access the BIOS.
3. Enter the supervisor or user password to access the BIOS.
4. Select **Boot**.

   NOTE
   An exclamation mark (!) appears next to boot options that are disabled.
5. For each boot option to disable, highlight the option and press **SHIFT+1**.
6. Press **F10** to save and reboot.

Section 2.11
Disabling SSH (Linux Only)

Uninstalling the SSH server is the most effective way of disabling SSH. From the Linux shell, type:

```
apt-get remove openssh-server
```

Section 2.12
Disabling Root Login via SSH (Linux Only)

To prevent users from logging via SSH as a root user, do the following:

NOTE
Windows® does not come with an SSH server by default.

IMPORTANT!
Make sure to have an user configured before disabling SSH for the root profile. For more information, refer to Section 2.4, "Adding a User (Linux Only)".

1. Login or gain root access.
2. Using vim or nano, open the file /etc/ssh/sshd_config
3. In the file, locate the following line:

```
#PermitRootLogin no
```

4. Change the line to the following:

```
PermitRootLogin no
```

5. Save and close the file.
6. Restart the SSHD service by typing:

```
/etc/init.d/sshd restart
```

Section 2.13
Disabling the Gigabit Ethernet Port (Linux Only)

To disable the RJ45 gigabit Ethernet port on the front face of the RUGGEDCOM APE module, do the following:

1. Login or gain root access.
2. Using vim or nano, open the file /etc/network/interfaces.
3. In the file, locate the following line:

```
auto allow hotplug eth1
iface eth1 inet dhcp
```

4. Change the line to the following:

```
#auto allow hotplug eth1
#iface eth1 inet dhcp
```

5. Save and close the file.
6. Restart the module or restart the networking service by typing:

```
/etc/init.d/networking restart
```

Section 2.14
Creating and Restoring Backup Images

Siemens recommends using Redo Backup and Recovery to backup and restore the RUGGEDCOM software.

NOTE
It is highly recommended that a backup image of the RUGGEDCOM software be created upon commissioning the device to capture the default factory settings. This image can be loaded should the software image ever need to be restored. The only alternative method for restoring the software image is to return the device to Siemens.

Before creating or restoring a backup image of the RUGGEDCOM, make sure you have the following:

- A USB keyboard
- A USB mouse
- A DVI-D Monitor
- A USB DVD-ROM
- A Powered USB hub
- A DVD with Redo Backup and Recovery installed
- A blank USB key with a maximum memory capacity greater than or equal to the amount of hard drive space currently in use by the RUGGEDCOM APE

To create or restore a backup image, do the following:

1. Connect the powered USB hub to the RUGGEDCOM module.
2. Connect the USB keyboard, USB mouse, USB key and the USB DVD-ROM to the hub.
3. Connect the DVI-D monitor to the RUGGEDCOM module.
4. Power on the RUGGEDCOM module. This can be done by either enabling the RUGGEDCOM APE module through the RX15xx device or by pressing the power button on the RUGGEDCOM APE module.
5. When the RUGGEDCOM module begins to start up, immediately press **F5** repeatedly until the startup boot menu appears.
6. Temporarily set the boot target to the USB DVD-ROM.

   NOTE
   The RUGGEDCOM module will boot from the default boot target during the next system boot.

7. Press **Enter** to start booting from the USB DVD-ROM.
8. Follow the on-screen instructions provided by Redo Backup and Recovery to create or restore a backup image. For more information, refer to www.RedoBackup.org.

Section 2.15

Updating Linux Software (APE1402 and APE1404 Only)

To update the software, do the following:

IMPORTANT!
To upgrade the complete Linux distribution currently running on the device, contact Siemens Customer Support.

NOTE
Unless otherwise indicated, Siemens does not provide specific software support for third-party applications.

1. Log in to the RUGGEDCOM APE.
2. Make sure the RUGGEDCOM APE is connected to the upgrade server by pinging the server's name or IP address.
3. Using vi, open the file `/etc/apt/sources.list` and add the following line:

   ```
   deb http://{server}/ {repository} {distribution} main
   ```

   Where:

   - `{server}` is the IP address or host name of the host server
   - `{repository}` is the path to the RUGGEDCOM APE repository on the server
   - `{distribution}` is the name of the RUGGEDCOM APE distribution
4. Save and close the file.
5. Update the RUGGEDCOM APE's knowledge of the new software available on the upgrade server by typing:

   ```
   apt-get update
   ```
6. Start the package upgrade by typing:

   NOTE
   Refer to the Linux Debian user documentation to determine the differences between `upgrade` *and* `dist-upgrade`*.*

   ```
   apt-get [ upgrade | dist-upgrade ]
   ```

   NOTE
   During the update, some services may become temporarily unavailable while the software is being upgraded. The RUGGEDCOM APE may need to be rebooted after the update is completed.
7. [Optional] Install or update an existing Graphical User Interface (GUI) by typing:

   ```
   apt-get install gui
   ```

   Where:

   - *gui* is the name of the GUI to install, such as `xfce4`, `gnome` and `kde`.

Section 2.16
Troubleshooting the APE

The following describes potential solutions for common problems.

Lost IP Address

The simplest resolution to this problem occurs when the RUGGEDCOM APE is easily reached and a monitor is attached. The RUGGEDCOM APE can be queried for the IP address and the configuration of the RUGGEDCOM APE or command module may be changed to allow networking.

If the RX15xx device is remotely situated, it may be possible to use the TCPDUMP command to trace IP traffic from the RUGGEDCOM APE. If the RUGGEDCOM APE is networked successfully then one of the captured packets will almost certainly reveal the source IP address. A badly networked RUGGEDCOM APE, attached to an incorrect subnet, may still reveal an IP address.

RUGGEDCOM APE Does Not Boot

If the RUGGEDCOM APE LEDs remain dark after an RX15xx device reboot, the most likely cause of failure is a module-type mismatch. This occurs when a slot's configured module-type does not exactly match that of the RUGGEDCOM APE in that slot. To correct this problem, log in to the RX15xx device and change the module-type for the slot to `none`. After rebooting the device, the module-type will be determined automatically from the RUGGEDCOM APE module.

NOTE
Line modules have the capability of being disabled. When disabled, a line module does not consume power. If your RUGGEDCOM APE does not boot, ensure that it is not disabled. If you are installing an RUGGEDCOM APE to act as a spare, you may wish to disable the RUGGEDCOM APE to reduce power.

If the module-type is correct, the next most likely cause of failure is that the module has been disabled. Enabling the module in the chassis should allow it to boot.

If the module is correctly enabled, the next most likely cause of failure is a power problem. The possibility of a power problem may be eliminated by making sure the power supplied to the RUGGEDCOM APE is sufficient. For information about power requirements, refer to the *RX15xx Installation Guide*.

If power is sufficient the syslog file should be examined for irregularities during the boot. The last boot may have occurred some time in the past and may no longer be recorded in the syslog. If this is the case, the module can be rebooted by disabling it and re-enabling it. The syslog will then contain enties reflecting the RUGGEDCOM APE boot.

If the syslog contains no messages reflecting an improper boot of the RUGGEDCOM APE, return the RUGGEDCOM APE to Siemens.

The RUGGEDCOM APE should be returned to Siemens if its power LEDs remain dark and all above debugging steps have been performed.

If the power LED lights up but the RUGGEDCOM APE does not boot, a monitor must be attached to further diagnose the problems.

Problems with USB Ports

If problems occur when accessing devices (e.g. keyboard, storage media, etc.) via USB, the most likely cause is that the power consumed by all the devices on the USB exceeds the maximum power capability of the RUGGEDCOM APE. This may be tested by employing a powered USB hub. For information about the maximum power available through the USB ports on the RUGGEDCOM APE module, refer to the *RX15xx Installation Guide*.

3 Frequently Asked Questions

General

Q: How do I power a USB DVD-ROM drive or USB hard disk using the RUGGEDCOM APE USB port?

A: The RUGGEDCOM APE USB port is limited in the amount of power it can provide. Use a powered hub to employ devices such as these.

Q: How can I re-install the software platform on the RUGGEDCOM APE?

A: There are two possible options:

- Return the RUGGEDCOM APE module to Siemens and request a re-install. This service is not covered by warranty.
- Restore the backup that was made before commissioning the RUGGEDCOM APE module.

NOTE
Siemens does not provide recovery images for Check Point GAiA. Recovery images must be obtained from www.Check Point.com.

Windows® Embedded Standard 7

Q: How do I use serial ports on a RUGGEDCOM RX15xx device?

A: The serial port baud rate, parity and other settings are managed by the host RUGGEDCOM RX15xx device. If your Windows® application supports serial over IP, you may program it to raise a connection to the serial interfaces at its IP address and port, as configured on your RUGGEDCOM RX15xx device.

Linux

Q: How do I upgrade Linux on the RUGGEDCOM APE?

A: The RUGGEDCOM APE upgrades itself via HTTP using the Debian Advanced Package Tool (APT) system. You must set up a Web server to serve new versions of code to upgrade to.

For more information about upgrading the software platform using a Web server, refer to Section 2.15, “Updating Linux Software (APE1402 and APE1404 Only)”.

Q: How do I recover an image of the original factory settings?

A: RUGGEDCOM APE strongly recommends creating a backup image of the RUGGEDCOM APE before it is configured. If this image is available, it can be easily restored. For more information, refer to Section 2.14, “Creating and Restoring Backup Images”.

If an original backup image is not available, contact Siemens Customer Support for assistance. In most cases, the RUGGEDCOM APE module must be returned to the factory to be re-imaged. This service is not covered by warranty.

Q: Does the RUGGEDCOM APE support a Real Time Operating System (RTOS)?

A: The software distributed by Siemens does not include an RTOS component. However, this software could be installed.

Q: Does the RUGGEDCOM APE have a serial port?

A: The RUGGEDCOM APE does not have serial ports.