SIEMENS

Edition 05/2022

Configuration Manual

SIMATIC NET

Networking Components

RUGGEDCOM APE (Application Processing Engine)

For APE1402, APE1402W7, APE1404, APE1404 ADM, APE1404W7, APE1404CKP

https://www.siemens.com/ruggedcom

SIEMENS

SIMATIC NET

Networking Components RUGGEDCOM APE (Application Processing Engine)

Configuration Manual

For APE1402, APE1402W7, APE1404, APE1404 ADM, APE1404W7, APE1404CKP

05/2022
C79000-G8976-1121-06

Legal Information

Warning Notice System

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

⚠ NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper Use of Siemens Products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Canada Ltd.. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

C79000-G8976-1121-06
© 05/2022 Subject to change

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 modules
- Obtaining, installing and using the RUGGEDCOM APE software
- Configuring networks with RUGGEDCOM APE
- 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.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cert.

Related Documents

The following are other documents related to this product that may be of interest. Unless indicated otherwise, each document is available on the Siemens Industry Online Support (SIOS) [https://support.industry.siemens.com] website.

Note
Documents listed are those available at the time of publication. Newer versions of these documents or their associated products may be available. For more information, visit SIOS or consult a Siemens Customer Support representative.

Catalogs

Document Title	Link
RUGGEDCOM RX1500 Modules Catalog	https://support.industry.siemens.com/cs/ww/en/view/109747072

Installation Guides

Document Title	Link
RUGGEDCOM RX1500 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82166529
RUGGEDCOM RX1501 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82164308
RUGGEDCOM RX1510 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82164310
RUGGEDCOM RX1511 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82166915
RUGGEDCOM RX1512 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82167597

SIMATIC NET Glossary

The SIMATIC NET Glossary describes special terms that may be used in this document.

The glossary is available online via Siemens Industry Online Support (SIOS) at:

https://support.industry.siemens.com/cs/ww/en/view/50305045

Registered Trademarks

RUGGEDCOM®, ROS®, RCDP®, and RUGGEDCOM Discovery Protocol® are registered trademarks of Siemens Canada Ltd.

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

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

Warranty

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

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

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 https://www.siemens.com 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 https://w3.siemens.com/aspa_app/?lang=en.

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

Contacting Siemens

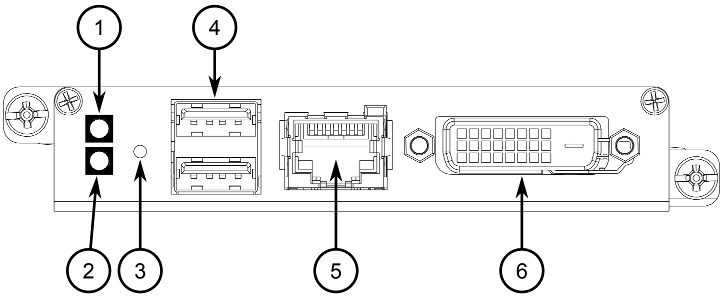
Address	Siemens Canada Ltd. Digital Industries Process Automation 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7
Telephone	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995
E-Mail	info.ruggedcom@siemens.com
Web	https://www.siemens.com

Overview

The RUGGEDCOM APE (Application Processing Engine) is an x64-based computer designed to occupy a single line module slot in a RUGGEDCOM RX15xx device. The RUGGEDCOM APE can host a variety of x64-based operating systems and features Gigabit Ethernet, USB ports and a DVI-D Video port.

The following RUGGEDCOM APE modules are available:

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



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

Figure 1.1 RUGGEDCOM APE Module

1.1 Operating System

Each RUGGEDCOM APE module comes with a pre-installed operating system.

Module	Operating System
APE1402	Debian Linux®
APE1402W7	Windows® Embedded Standard 7

Module	Operating System
APE1404	Debian Linux®
APE1404 ADM	Debian Linux® + CROSSBOW ADM
APE1404W7	Windows® Embedded Standard 7
APE1404CKP	Check Point GAiA™

Upgrading or Changing the Operating System

The operating system can be upgraded or extended as needed. It can also be changed to an alternative software platform, such as Linux Mint or Ubuntu.

IMPORTANT
Siemens assumes no responsibility for upgrades or changes made to the operating system.

Other Software/Applications

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.

Check Point GAiA™ Licensing

To run Check Point GAiA™ on the RUGGEDCOM APE, the Check Point operating system must be activated after the RUGGEDCOM APE module has been installed.

1.2 Requirements and Restrictions

Note the following requirements and restrictions for using the RUGGEDCOM APE:

- **Chassis Operating System**

  The RUGGEDCOM RX1500-series chassis must have RUGGEDCOM ROX v2.12.4 or higher installed.

- **Operating Temperature Range**

  Each module is rated for operation within the temperature range of -40 to 75 °C (-40 to 167 °F).

- **Power Consumption**

  ⚠ **NOTICE**

  Electrical hazard - risk of power failure

  Installing more RUGGEDCOM APE modules than allowed on a 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.

1.3 Security Recommendations

To assist in securing the module, note the following recommendations:

Note
When applicable, these recommendations can apply to all software and applications that may be installed on the RUGGEDCOM APE module. This includes Debian Linux, Microsoft Windows, and RUGGEDCOM applications pre-installed on the base image.

Hardware/Software

- Before commissioning and for on-going maintenance of the RUGGEDCOM APE line module, apply the latest security updates from Debian or from Microsoft as per the standard Windows® update procedure in line with the local security policy of the deployed environment. For more information on applying security updates from Debian, refer to the user documentation provided by Debian or Microsoft.
- Before using the RUGGEDCOM APE, make sure all relevant CERT security advisories for the RUGGEDCOM RX1500-series hosting the APE have been applied. For the latest information about security patches for Siemens products, visit the CERT Services website [https://new.siemens.com/global/en/products/services/cert.html]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the ProductCERT Security Advisories website [https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications], or by following @ProductCert on Twitter.
- Only enable the physical ports that are required on the module. Unused physical ports could potentially be used to gain access to the network behind the module.

Authentication

- When using the Linux-based version of the RUGGEDCOM APE, as per the local environment's security policy, add an administrative account, disable the root user on Debian Linux, and replace any default passwords. For a list of default user profiles and passwords, refer to "Logging in to RUGGEDCOM APE (Page 11)".

- When using the Linux-based version of the RUGGEDCOM APE, ensure the GRUB bootloader password is configured. For more information, refer to "Setting the GRUB Bootloader Password (Page 16)".
- 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.
- If an application on the RUGGEDCOM APE uses SSH and/or TLS keys, generate new keys and protect them inline with the environment’s local security policy before provisioning the unit.

Physical/Remote Access

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Exercise extreme caution when changing any settings in the BIOS. For example, USB and PXE boot are disabled by default; enabling these settings is not advisable for securing the module.
- Control access to the USB, SD card slot, and gigabit Ethernet ports to the same degree as any physical access to the module.

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 RUGGEDCOM APE for further security recommendations.

1.4 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).

1.5 Rebooting/Powering Down the RUGGEDCOM 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.

1.6 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.

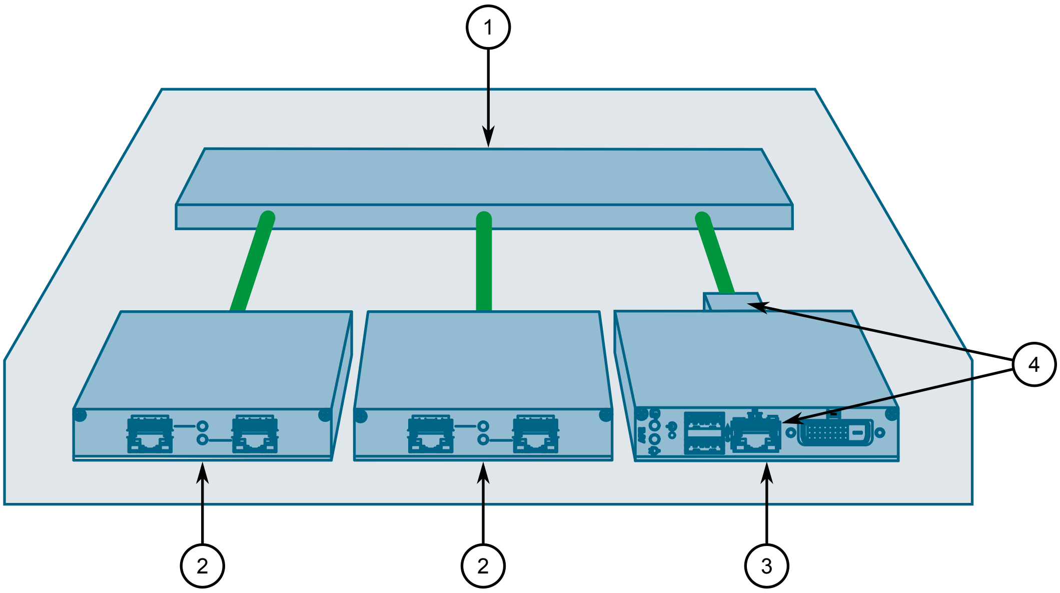
To change the boot device, press **F5** immediately after the RUGGEDCOM APE starts to boot up. The RUGGEDCOM APE will boot from the chosen device. During the next boot cycle, the RUGGEDCOM APE will revert back to the default boot device selected in the BIOS.

Contact Siemens if any BIOS-related issues are experienced.

1.7 Internal Network Interface

In addition to the gigabit Ethernet interface on the faceplate, the RUGGEDCOM APE features an internal 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 internal 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.



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

Figure 1.2 A RUGGEDCOM RX15xx Device With an RUGGEDCOM APE Module Installed

1.8 Suggested Software

RUGGEDCOM ELAN SCADA Application Suite

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

Siemens' RUGGEDCOM ELAN product family solves a wide range of issues related to communications and data integration, 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 http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/ruggedcom-portfolio/software/Pages/elan.aspx.

1.9 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 Dynamic Host Configuration Protocol (DHCP).

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

1.10 RUGGEDCOM APE 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 internal Ethernet port appears like any other Gigabit-capable switched or routed port.

For examples of how the RUGGEDCOM APE can be configured in a RX15xx device, refer to "Example: Networking in Factory Default Conditions (Page 8)" and "Example: RX15xx Services and WAN Networking (Page 9)".

1.10.1 Example: Networking in Factory Default Conditions

The following figure illustrates how routing and switching would work when the RUGGEDCOM APE is used in a RUGGEDCOM RX15xx chassis with a four-port Ethernet module in LM2.

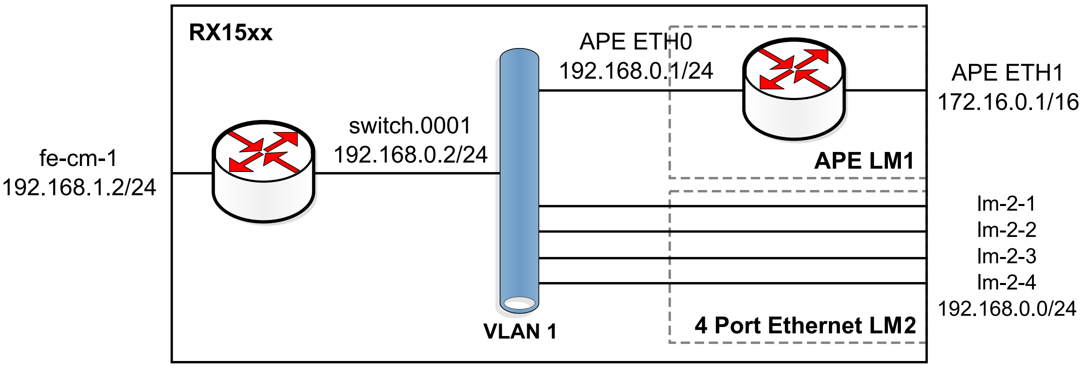


Figure 1.3 Example Configuration

In the factory default condition, all Ethernet interfaces on the RUGGEDCOM RX15xx router (including the internal port of the RUGGEDCOM APE) are created as switched ports in the default VLAN. When DHCP is configured in RUGGEDCOM ROX II, an IPv4 subnet and a gateway IP are automatically assigned to this VLAN.

In RUGGEDCOM ROX II, the 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 1.3, “Example Configuration”, the RUGGEDCOM APE ETH0 interface has been assigned an address of 192.168.0.1, either manually by the user or automatically by a pre-configured DHCP server, 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 RUGGEDCOM 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 RUGGEDCOM RX15xx device and enable IP forwarding from the Windows or Linux operating system.

Note

When operating the RUGGEDCOM APE in either switch or router mode, the RUGGEDCOM 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 RUGGEDCOMRUGGEDCOM APE in the interface switch menu for the RUGGEDCOM APE interface.

1.10.2 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.

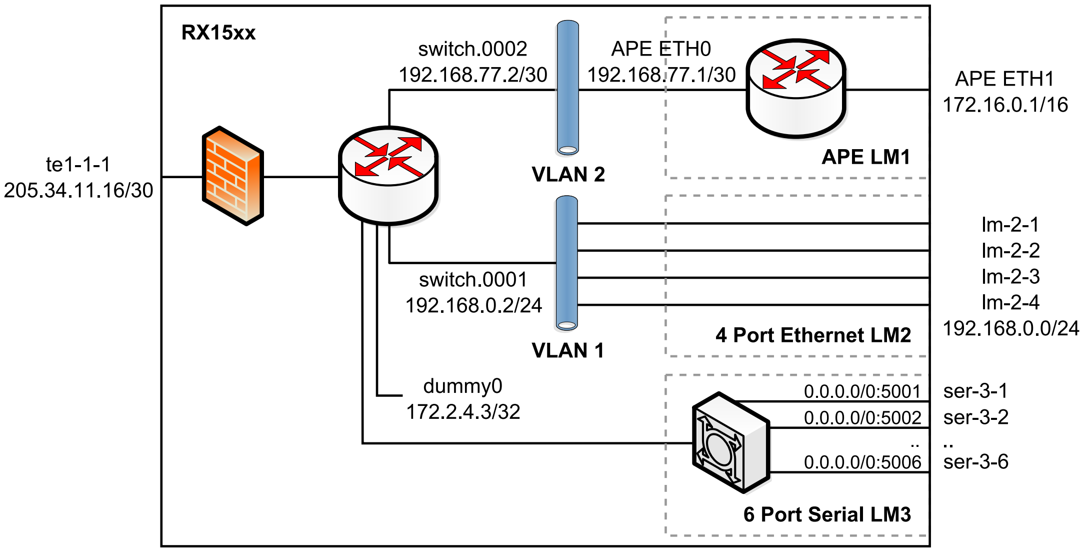


Figure 1.4 Example Configuration

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.

The figure shows six serial ports available on serial LM 3. In order to become network-accessible, these ports must be configured as socket ports that allow incoming calls on TCP ports 5001 (ser-3-1) through 5006 (ser-3-6). While any address on the RX1500 control module may be used to connect the RUGGEDCOM APE to these ports, switch.0001, switch.0002, and dummy0 addresses are recommended. In particular, dummy0 addresses are useful when router redundancy is implemented.

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

1.11 Decommissioning the Module

Before taking a RUGGEDCOM APE module out of service make sure the module has been fully decommissioned. This includes removing any sensitive, proprietary information.

Note

For additional assistance in decommissioning the module, contact Siemens Customer Support.

To decommission a RUGGEDCOM APE module, do the following:

1. Create a bootable USB running an operating system that can support data erasure tools.
2. Load the operating system by selecting the USB device from the BIOS boot settings.
3. From the operating system, use standard erasure tools to erase data on the module that represents the RUGGEDCOM APE's flash memory. For example, use standard Linux tools, such as dd, wipe, or shred, to wipe data from the module.

⚠ **NOTICE**

Security hazard – risk of data exploitation

Regardless of the erasure tool or method employed, even following multiple rounds of flashing, erasure, or overwriting, residual data may still be present on Flash-based storage media. To guarantee the destruction of all sensitive data persisting on the unit, physical destruction of the storage media/platform may be required.

Configuring and Using the RUGGEDCOM APE

2

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

IMPORTANT
Before using the RUGGEDCOM APE, create a backup image that can be restored should the module be configured improperly. Warranty does not support modules rendered inoperable/inaccessible due to configuration errors made by the user.

2.1 Logging in to RUGGEDCOM APE

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

⚠ NOTICE
Security hazard – risk of unauthorized access 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.	
Linux	root	admin
Linux + CROSSBOW ADM	admin	admin
Check Point GAiA™	admin	admin

2.2 Using the RUGGEDCOM 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 https://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.

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.

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:~#
```

2.5 Setting the Root and User Passwords (Linux Only)

For security reasons, the default root Linux password should 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.)

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.
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. Enable **Power On Password**.
6. Set the supervisor and user passwords.
7. Press **F10** to save and reboot.

2.7 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.

2.8 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.

2.9 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}
   ```

3. Copy the password (e.g. select on-screen and then press **Ctrl**-**C**).
4. Using vim or nano, open the file /etc/defaults/grub.password.
5. In the file /etc/defaults/grub.password, locate the following line:

   ```
   GRUB_USER=
   ```

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

   ```
   GRUB_USER=root
   ```

6. Locate the following line:

   ```
   GRUB_ENCRYPTED_PASSWORD=
   ```

   Add the GRUB password created in Step 2 to this line (e.g. press **P** or **p** in vim, or **Ctrl**-**U** in nano). For example:

   ```
   GRUB_ENCRYPTED_PASSWORD=grub.pbkdf2.sha512.10000.82BA3D30037BBB
   B0A5EEED9395A036E973299517EAC3530A46
   45406C692279EBDF12603E11E0E2F02BF32888A2F61DD8467FA8C0F3641CF8F
   DA452F40571E988.BF312D710D4E451A63264
   C47C8CCBF40D429E1D6FF21D6AE95CA36F2D9AEE44C37AE1DF59C5303A9736840C7B2B
   BC1AA8045984FB6017F08559B11D0C
   19E5E0F
   ```

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

   ```
   update-grub
   ```

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

2.10 Setting the Hard Drive Password

On Windows Embedded Standard 7, BitLocker can be used to password-encrypt the hard drive. There are no pre-installed applications to password-encrypt the hard drive on other software platforms.

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
```

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 "Adding a User (Linux Only) (Page 13)".

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
   ```

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
   ```

2.14 Updating Linux Software

Outlined below are the steps required when updating the Linux software on the RUGGEDCOM APE.

IMPORTANT
Take care to follow the steps below in the correct order. If any steps are omitted or executed out of order, the RUGGEDCOM APE may become unusable.

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

IMPORTANT
This procedure is only applicable to Linux variants of the APE1402 and APE1404.

IMPORTANT
Updates must be performed sequentially. Debian v9 (Stretch) cannot be installed on a device running Debian v7 (Wheezy). The Linux software on the RUGGEDCOM APE must be upgraded to Debian 8 (Jessie) before it can be upgraded to Debian v9 (Stretch).

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

Preliminary Steps

Prior to updating the software, do the following:

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. Backup any application or configuration files.
4. Disable the **gma500_gfx driver**. Using vi, open the file `/etc/modprobe.d/fbdev-blacklist.conf` and add the following line:

   ```
   blacklist gma500_gfx
   ```

   When done, save and close the file.
5. Set up the apt sources list. Using vi, open the file `/etc/apt/sources-list` and add the following lines:

   ```
   deb http://deb.debian.org/debian {release} main
   ```

```
deb-src http://deb.debian.org/debian {release} main

deb http://deb.debian.org/debian {release}-updates main
deb-src http://deb.debian.org/debian {release}-updates main

deb http://deb.debian.org/debian-security/ {release}/updates main
deb-src http://deb.debian.org/debian-security/ {release}/updates main
```

Where:

- **`{release}`** is the development codename for the Debian release the RUGGEDCOM APE is currently running (e.g. `wheezy`, `jessie`, etc.).

When done, save and close the file.

6. Update the RUGGEDCOM APE's knowledge of the new software available on the upgrade server by executing the following command:

   ```
   apt-get update
   ```

   Ignore any errors about public keys.

7. Upgrade previously installed packages by executing the following command:

   ```
   apt-get-V upgrade
   ```

   If prompted, select `/dev/sda` as the device path.

8. Reboot the system by executing the following command:

   ```
   reboot
   ```

9. Upgrade the Linux kernel by executing the following command:

   ```
   apt-get install linux-image-686-pae
   ```

10. Reboot the system again by executing the following command:

    ```
    reboot
    ```

Upgrading from Debian v7 (Wheezy) to Debian v8 (Jessie)

To upgrade from Debian v7 (Wheezy) to Debian v8 (Jessie), do the following:

1. In the apt sources list, point all repositories to Debian v8 (Jessie). Using vi, open the file `/etc/apt/sources.list` and replace all instances of "`wheezy`" with "`jessie`." For example:

   ```
   deb http://deb.debian.org/debian jessie main
   deb-src http://deb.debian.org/debian jessie main

   deb http://deb.debian.org/debian jessie-updates main
   deb-src http://deb.debian.org/debian jessie-updates main

   deb http://security.debian.org/debian-security/ jessie/updates main
   deb-src http://security.debian.org/debian-security/ jessie/updates main
   ```

   When done, save and close the file.

2. Update the apt sources list by executing the following command:

   ```
   apt-get upgrade
   ```

3. Upgrade previously installed packages by executing the following command:

   ```
   apt-get-V upgrade
   ```

   When prompted, allow the system to restart services without asking during package upgrades.

4. Upgrade any packages that may have been held back in the previous step by executing the following command:

   ```
   apt-get dist-upgrade
   ```

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

   When prompted, either allow or disallow the system to disable SSH password authentication for the root account.

   When prompted, do not allow the system to upgrade the blacklist.

5. [Optional] Install or update an existing Graphical User Interface (GUI) by executing the following command:

   ```
   apt-get install  {gui}
   ```

   Where:

   - **`{gui}`** is the name of the GUI to install (e.g. `xfce4`, `gnome` and `kde`, etc.).

6. Configure the GRUB bootloader. Using vi, open the file `/etc/default/grub` and add or un-comment the following line:

   ```
   GRUB_TERMINAL=console
   ```

   When done, save and close the file.

7. Reinstall the GRUB bootloader by executing the following sequence of commands:

   ```
   grub-install /dev/sda
   update-grub
   grub-mkdevicemap
   grub-mkconfig > /boot/grub/grub.cfg
   ```

8. Reboot the system and clean up any unnecessary packages by executing the following sequence of commands:

   ```
   reboot
   dpkg --configure-a
   apt-get -f install
   apt-get autoremove
   reboot
   ```

Once these steps are complete, the RUGGEDCOM APE will be running the latest version of Debian v8 (Jessie).

Upgrading from Debian v8 (Jessie) to Debian v9 (Stretch)

To upgrade from Debian v8 (Jessie) to Debian v9 (Stretch), do the following:

1. In the apt sources list, point all repositories to Debian v9 (Stretch). Using vi, open the file `/etc/apt/sources.list` and replace all instances of "`jessie`" with "`stretch`." For example:

   ```
   deb http://deb.debian.org/debian stretch main
   deb-src http://deb.debian.org/debian stretch main

   deb http://deb.debian.org/debian stretch-updates main
   deb-src http://deb.debian.org/debian stretch-updates main

   deb http://security.debian.org/debian-security/ stretch/updates main
   deb-src http://security.debian.org/debian-security/ stretch/updates main
   ```

   When done, save and close the file.

2. Update the apt sources list by executing the following command:

   ```
   apt-get upgrade
   ```

3. Upgrade previously installed packages by executing the following command:

   ```
   apt-get -V upgrade
   ```

4. Upgrade any packages that may have been held back in the previous step by executing the following command:

   ```
   apt-get dist-upgrade
   ```

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

   When prompted, select the default value as the Snort IP range.

   When prompted, allow the system to correct the Snort configuration error.

5. [Optional] Install or update an existing Graphical User Interface (GUI) by executing the following command:

   ```
   apt-get install { gui }
   ```

   Where:

   - `{ gui }` is the name of the GUI to install (e.g. `xfce4`, `gnome`, and `kde`, etc.).

6. Configure the GRUB bootloader. Using vi, open the file `/etc/default/grub` and add the following line:

   ```
   GRUB_TERMINAL=console
   ```

   When done, save and close the file.

7. Reinstall the GRUB bootloader by executing the following sequence of commands:

   ```
   grub-install /dev/sda
   update-grub
   grub-mkdevicemap
   grub-mkconfig > /boot/grub/grub.cfg
   ```

8. Reboot the system and clean up any unnecessary packages by executing the following sequence of commands:

   ```
   reboot
   dpkg --configure-a
   apt-get -f install
   apt-get autoremove
   reboot
   ```

Once these steps are complete, the RUGGEDCOM APE will be running the latest version of Debian v9 (Stretch).

2.15 Troubleshooting the RUGGEDCOM 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 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 "Installation Manual" for your RUGGEDCOM RX15xx device.

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 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 "Installation Manual" for your RUGGEDCOM RX15xx device.

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 image 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 https://www.checkpoint.com/.

Linux

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

A: Siemens strongly recommends creating a backup image of the RUGGEDCOM APE before it is configured. If this image is available, it can be easily restored.

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.

For more information

Siemens RUGGEDCOM
https://www.siemens.com/ruggedcom

Industry Online Support (service and support)
https://support.industry.siemens.com

Industry Mall
https://mall.industry.siemens.com

Siemens Canada Ltd.
Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada