IDAN-ID5915

Cisco® 5915 Embedded Services Router for IDAN

User's Manual

IDM-650020046 Rev. B

RTD Embedded Technologies, Inc.
AS9100 and ISO 9001 Certified

RTD Embedded Technologies, Inc.
103 Innovation Boulevard
State College, PA 16803 USA
Telephone: 814-234-8087
Fax: 814-234-5218

www.rtd.com

sales@rtd.com
techsupport@rtd.com

Revision History

Rev A	Initial Release
Rev B	Corrected Storage Temperature to match Cisco's specifications, minor fixes.

Failure to follow the instructions found in this manual may result in damage to the product described in this manual, or other components of the system. The procedure set forth in this manual shall only be performed by persons qualified to service electronic equipment. Contents and specifications within this manual are given without warranty, and are subject to change without notice. RTD Embedded Technologies, Inc. shall not be liable for errors or omissions in this manual, or for any loss, damage, or injury in connection with the use of this manual.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Product Overview

The IDAN-ID5915 incorporates the Cisco 5915 Embedded Services Router into RTD's standard IDAN packaging technology. It provides all necessary connections to interface with the board-level router product. The router may be operated standalone with a power supply, or stacked with RTD's cpuModules and other peripherals using the PCI/104-Express stackable bus structure. Using RTD StackNET™ technology, the router may be stacked with RTD's line of scalable Gigabit Ethernet Switches to provide additional ports.

1.2 Features

- Integrated Cisco 5915 Embedded Services Router (ESR)
  - Cisco IOS 15.x Operating System
  - Enterprise Base software standard
    - Industry-standard Cisco IOS command set and configuration
    - Support for WAN connection redundancy on Routed ports
      - Primary and Backup Interface
      - IP SLA
    - VLAN Support
      - Up to 32 VLANs
      - 802.1q Trunking
    - Standard routing protocols such as RIP, OSPF, BGP
    - PPP and PPPoE
    - Network Address Translation (NAT)
    - DHCP client, server, and relay
    - Traffic Management (QoS, 802.1p)
    - Management via Serial Console, Telnet, HTTP, SNMP
  - Optional Advanced Enterprise software adds the following features:
    - Cisco IOS Service Advertisement Framework (SAF)
    - MLD Proxy
    - IPv6 Support
    - Firewall and Intrusion Prevention
    - VPN Support
    - Radio-aware routing (DLEP, R2CP, RFC 5578)
    - OSPFv3 Support for Ad Hoc Mobile Networks
    - Mobile IP
    - Security and Cryptography Features (IPsec, AES, IKE, Suite-B, SSL/TLS, PKI)
    - Cisco Unified Communications Manager Express support (up to 48 phones)
    - Secure Shell (SSH) Client and Server
  - Cisco Mobile Ready Net capabilities
  - Highly secure data, voice, and video communication
  - Onboard hardware encryption
  - 512 MB DRAM
  - 256 MB Flash Memory
- 5x Fast Ethernet 10/100 Ports (4x available for external connectivity)
  - RJ-45 connectors with integrated LEDs
  - Supports auto-negotiation of speed and duplex
  - 2x Routed Ports for remote connections (Layer 3)
  - 2x Switched Ports for local connections (Layer 2)
  - 1x Switched Port internal to the stack for use with other RTD StackNET™ products
- 1x Serial Console Port
  - Management and configuration interface
  - RS-232 signaling
  - Modem Flow Control
- LED indicators
  - Power/Status
  - Ethernet Link/Activity
  - Over Temperature
  - Factory Defaults
- Push button erasure of router memory and flash for quick declassification.
- PCI/104-Express stackable bus structure

  - PCIe pass-through (Universal, Type 1 or Type 2)
  - PCI pass-through expansion bus
- Two StackNET^{TM} configurations available
  - Upward stacking, for use at the bottom of an IDAN stack
  - Downward stacking, for use at the top of an IDAN stack
- Modular rugged milled aluminum frames
- Maintains the PC/104 bus self-stacking concept
- Allows quick interchangeability of modules
- Passive structural heat sink
- Aluminum Alloy - 6061, Temper-T6
- Finish - MIL-PRF-85285 polyurethane topcoat, per FED-STD-595, color 36495 (light gray).
- Panel engravings per FED-STD-595, color 37038 (black).
- Additional paint options available upon request

1.3 Ordering Information

The IDAN-ID5915 is available with the following options:

Table 1: Ordering Options

Part Number	Description
IDAN-ID5915D-4E	Cisco 5915 Router in modular IDAN slice, downward-stacking StackNET™ configuration, Enterprise Base software
IDAN-ID5915U-4E	Cisco 5915 Router in modular IDAN slice, upward-stacking StackNET™ configuration, Enterprise Base software
IDAN-ID5915D-4A	Cisco 5915 Router in modular IDAN slice, downward-stacking StackNET™ configuration, Advanced Enterprise software
IDAN-ID5915U-4A	Cisco 5915 Router in modular IDAN slice, upward-stacking StackNET™ configuration, Advanced Enterprise software

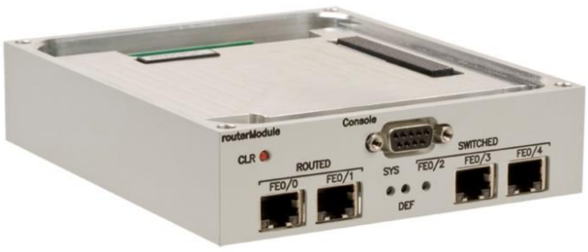


Figure 1: IDAN-ID5915D (Downward Stacking)

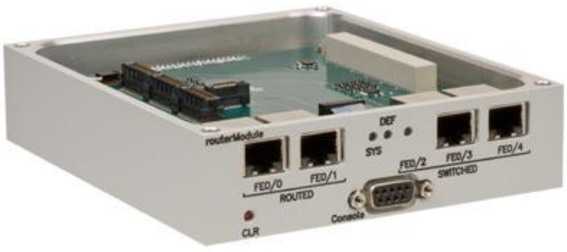


Figure 2: IDAN-ID5915D (Upward Stacking)

The Intelligent Data Acquisition Node (IDAN®) building block can be used in just about any combination with other IDAN building blocks to create a simple but rugged 104™ stack. This module can also be incorporated into a tailored RTD HiDAN® or HiDANplus® High Reliability Intelligent Data Acquisition Node with cylindrical connectors. Ready-made eBuild^{TM} systems are available as well. Contact RTD sales for more information on our high reliability systems.

1.4 Contact Information

1.4.1 SALES SUPPORT

For sales inquiries, you can contact RTD Embedded Technologies sales via the following methods:

Phone: 1-814-234-8087 Monday through Friday, 8:00am to 5:00pm (EST)
E-Mail: sales@rtd.com

1.4.2 TECHNICAL SUPPORT

If you are having problems with your system, please try the steps in the Troubleshooting chapter of this manual. For help with this product, or any other product made by RTD, you can contact RTD Embedded Technologies technical support via the following methods:

Phone: 1-814-234-8087 Monday through Friday, 8:00am to 5:00pm (EST)
E-Mail: techsupport@rtd.com

> ***The IDAN-ID5915 includes one year of technical support and software updates from Cisco for the 5915 Embedded Services Router. Questions regarding the 5915 ESR configuration should be directed to Cisco TAC. Visit http://support.cisco.com for contact information.***

2 Specifications

2.1 Operating Conditions

Symbol	Parameter	Test Condition	Min	Max	Unit
V_{cc5}	5V Supply Voltage		4.75	5.25	V
V_{cc3}	3.3V Supply Voltage		n/a	n/a	V
V_{cc12}	12V Supply Voltage		n/a	n/a	V
V_{cc-12}	-12V Supply Voltage		n/a	n/a	V
T_a	Operating Temperature		-40	+85	C
T_s	Storage Temperature	Limited by Cisco 5915 ESR specification	-51	+85	C
RH	Relative Humidity	Non-Condensing	0	90%	%
MTBF	Mean Time Before Failure	Telcordia Issue 2 30°C, Ground benign, controlled		TBD	Hours

Table 2: Operating Conditions

2.2 Electrical Characteristics

Symbol	Parameter	Test Condition	Min	Typical	Max	Unit
P	Total Power Consumption	V_{cc5} = 5.0V		5.6	10.19	W
I_{cc5}	5V Input Supply Current	Active		1120	2038	mA
		Inrush		2121		mA
V_{OUT3}	PCI 3.3V Output Voltage		3.14	3.3	3.47	V
I_{OUT3}	PCI 3.3V Output Current			500		mA

Table 3: Electrical Characteristics

3 IDAN Connections

3.1 Module Handling Precautions

To prevent damage due to Electrostatic Discharge (ESD), keep your module in its antistatic bag until you are ready to install it into your system. When removing it from the bag, hold the module by the aluminum enclosure, and do not touch the components or connectors. Handle the module in an antistatic environment, and use a grounded workbench for testing and handling of your hardware.

3.2 Physical Characteristics

- Weight: Approximately 0.68 Kg (1.5 lbs.)
- Dimensions: 152 mm L x 130 mm W x 35 mm H (5.983 in L x 5.117 in W x 1.388 in H)

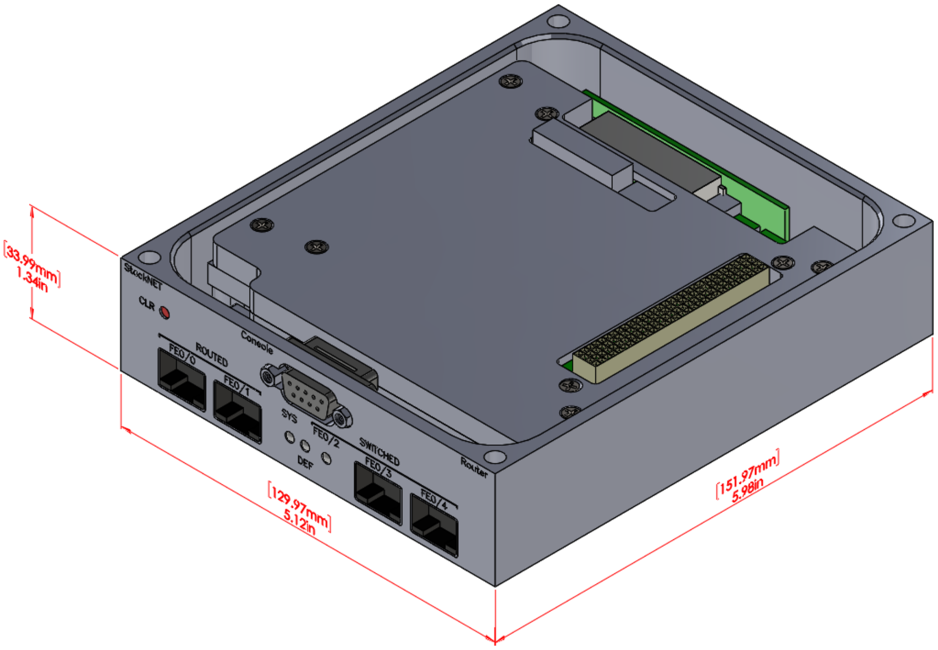


Figure 3: Exterior Dimensions for IDAN-ID5915D (Not to Scale)

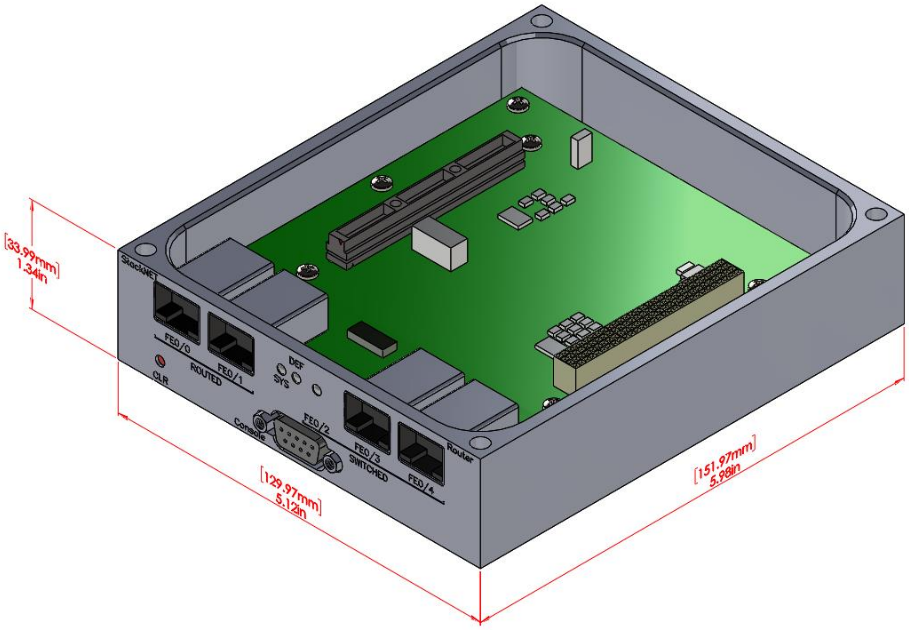


Figure 4: Exterior Dimensions for IDAN-ID5915U (Not to Scale)

3.3 Connectors

3.3.1 External I/O Connectors

3.3.1.1 Front Panel Connector Locations

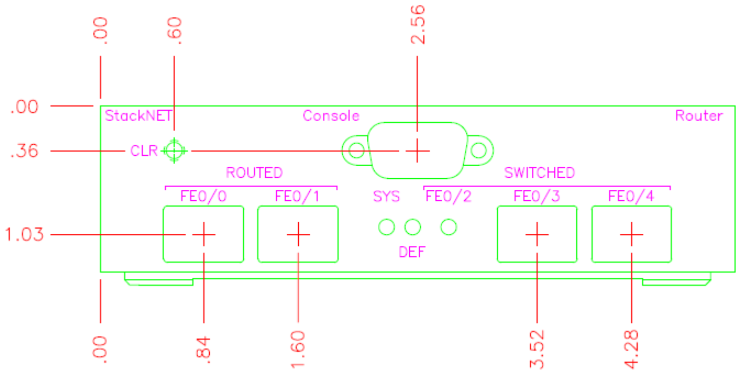


Figure 5: Front Panel Connector Locations for IDAN-ID5915D (Not to Scale)

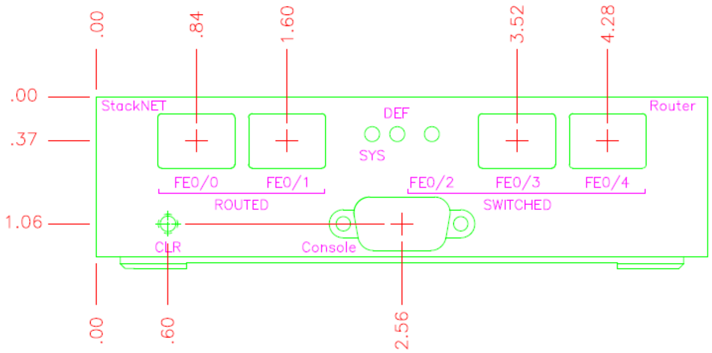


Figure 6: Front Panel Connector Locations for IDAN-ID5915U (Not to Scale)

3.3.1.2 RJ-45 Fast Ethernet Ports (FE0/0, FE0/1, FE0/3, and FE0/4)

FE0/0, FE0/1, FE0/3, and FE0/4 are standard female RJ-45 connectors. The figure below shows the pin numbers when **looking into the connector**.

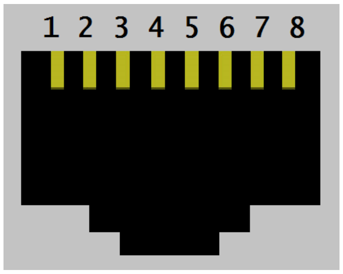


Figure 7: RJ-45 Connector

FE0/0, FE0/1, FE0/3, and FE0/4 use UTP (Unshielded Twisted Pair) wiring normally used for 10/100 Base-T Ethernet. Both routed and switched ports use the same pinout. The following table gives the pinout.

Pin	10/100 Function
1	A0+ (Transmit +)
2	A0- (Transmit -)
3	A1+ (Receive +)
4	A2+ (Not Used)
5	A2- (Not Used)
6	A1- (Receive -)
7	A3+ (Not Used)
8	A3- (Not Used)

Table 4: RJ-45 Signal Assignments

3.3.1.3 Serial Console Port

The Serial Console port is a standard female 9-pin D-SUB connector. The figure below shows the pin numbers when **looking into the connector**.

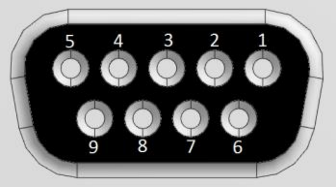


Figure 8: Console Connector

The Serial Console signaling level is RS-232, and it follows the standard RS-232 device pinout. The following table gives the pinout.

Pin	Function
1	No Connect
2	TXD
3	RXD
4	DSR
5	GND
6	DTR
7	CTS
8	RTD
9	No Connect

Table 5: Console Signal Assignments

Since the Serial Console uses the device pinout, connections from a computer should be made using a straight-through serial cable (M-to-F). A Null Modem cable (which is typically M-to-M) will not work. The straight-through cable pinout would be as follows:

Computer Serial Port			Router Console Port	
DB-9 Male			DB-9 Female	
Pin	**Function**		**Pin**	**Function**
1	DCD	X	1	No Connect
2	RXD	←	2	TXD
3	TXD	→	3	RXD
4	DTR	→	4	DSR
5	GND	↔	5	GND
6	DSR	←	6	DTR
7	RTS	→	7	CTS
8	CTS	←	8	RTS
9	RI	X	9	No Connect

Table 6: Serial Console Cable Signal Assignments

3.3.2 Internal Bus Connectors

CN1(Top) & CN2(Bottom): PCIe Connector

The PCIe connector provides power to the IDAN slice. Either CN1 or CN2 will be populated, depending on whether an upward or downward stacking configuration was ordered. The position and pin assignments are compliant with the *PCI/104-Express Specification*. (Refer to the PC/104 Specifications in the Additional Information chapter.)

While the Cisco 5915 Router uses PC/104 form factor, it is not an "active" device on the bus. It does not communicate over the PCIe bus, and it does not consume a PCIe link. The PCIe bus is used for power only.

When powered via the PCIe/104 connector, only +5V is required. The IDAN slice includes a voltage regulator to provide +5V and +3.3V the Cisco 5915 board requires. Note this onboard regulator **does not** provide +3.3V to the PCIe/104 bus. (However, it does provide +3.3V to the PCI-104 bus, see below.)

CN3: PCI Connector

The PCI connector provides power to the Cisco 5915 Router. The PCI connector may be accessible from either the top of the bottom of the IDAN slice, depending on whether the upward or downward stacking configuration was ordered. The position and pin assignments are compliant with the *PCI-104 Specification*. (Refer to the PC/104 Specifications in the Additional Information chapter.)

While the Cisco 5915 Router uses PCI-104 bus structure, it is not an "active" PCI device. It does not communicate over the PCI bus, and it does not consume a PCI slot. The PCI bus is used for power only. The LAN25E5915 board in the IDAN slice includes a voltage regulator to provide +5V and +3.3V the Cisco 5915 board requires. If powering the IDAN-ID5915 from the PCI bus, only +5V should be connected.

NOTE: The IDAN-ID5915 provides +3.3V power to the PCI bus. Care must be taken to ensure there are no other devices providing +3.3V on the bus (such as a power supply board). If multiple +3.3V power supplies are operating simultaneously, the system may be damaged or destroyed.

CN4(Top) & CN7(Bottom): FE0/2 StackNET™ Connector

CN4/CN7 is a board-to-board Fast Ethernet connection which allows the IDAN-ID5915 to be stacked with other RTD StackNET™ products, such as Ethernet switches. Either CN4 or CN7 will be populated, depending on whether an upward or downward stacking configuration was ordered. By stacking the router with an Ethernet switch, the overall Ethernet port count of the IDAN system may be increased.

3.4 Steps for Installing

1. Always work at an ESD protected workstation, and wear a grounded wrist-strap.
2. Turn off power to the IDAN system.
3. Remove the module from its anti-static bag.
4. Check that pins of the bus connector are properly positioned.
5. Check the stacking order; make sure all of the busses used by the peripheral cards are connected to the cpuModule.
6. Hold the module by its edges and orient it so the bus connector pins line up with the matching connector on the stack.
7. Gently and evenly press the module onto the IDAN system.
8. If any boards are to be stacked above this module, install them.
9. Finish assembling the IDAN stack by installing screws of an appropriate length.
10. Attach any necessary cables to the IDAN system.
11. Re-connect the power cord and apply power to the stack.
12. Boot the system and verify that all of the hardware is working properly.

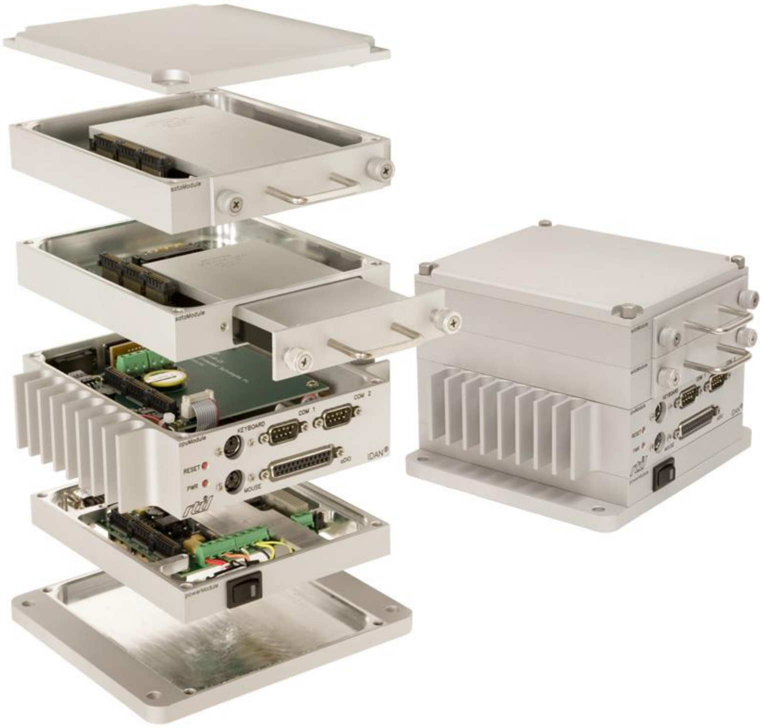


Figure 9: Example IDAN System

4 Functional Description

4.1 Block Diagram

The Figure below shows the functional block diagram of the IDAN-ID5915. The various parts of the block diagram are discussed in the following sections.

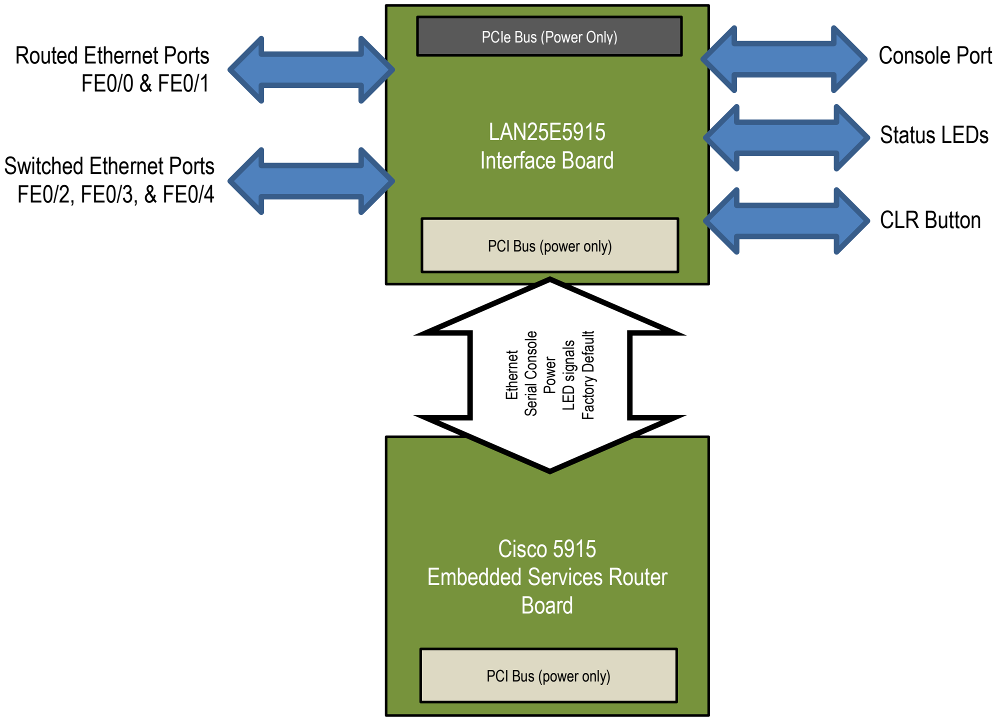


Figure 10: IDAN-ID5915 Block Diagram

4.2 Routed Ethernet Ports (FE0/0 & FE0/1)

The routed ports are traditionally used for the WAN interface of the system. Each port is an independent Layer 3 interface, and may be configured with its own IP address. In the Cisco IOS operating system, these ports are identified as follows:

- FE0/0 is identified as interface FastEthernet0/0
- FE0/1 is identified as interface FastEthernet0/1

In the factory default configuration, the routed interfaces are disabled and have no IP address assigned. Since the interfaces are disabled, the Ethernet ports will not link. To enable the ports and set IP addresses, connect to the router via the serial console and configure the interfaces. Refer to the Software Configuration chapter later in this manual for details.

4.3 Switched Ethernet Ports (FE0/2, FE0/3, & FE0/4)

The switched ports are traditionally used for the LAN interface of the system. FE0/2 is used internally in the IDAN system for the RTD StackNET^{TM} interface. FE0/3 & FE0/4 are available on the IDAN front panel for external connections. The switched ports are Layer 2 interfaces, and do not have an IP address assigned directly. However, the ports may be assigned to VLANs, and IP addresses may be assigned to VLAN interfaces. In the Cisco IOS operating system, these ports are identified as follows:

- FE0/2 is identified as interface FastEthernet0/2

- FE0/3 is identified as interface FastEthernet0/3
- FE0/4 is identified as interface FastEthernet0/4

By default, the switched interfaces are enabled and assigned to VLAN 1, but the VLAN 1 interface has no IP address assigned. To set an IP address, connect to the router via the serial console and configure the VLAN 1 interface. Refer to the Software Configuration chapter later in this manual for details.

4.4 Console Port

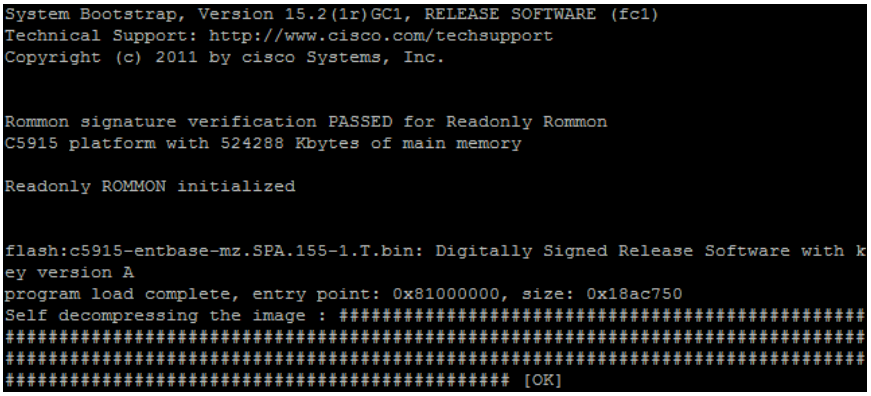
The serial console port is primarily used for initial router configuration and troubleshooting. In Cisco IOS, it is identified as con0.

The Console port may be connected to the RS-232 serial port on an RTD cpuModule, laptop, or a desktop PC. If the computer does not have a serial port available, a USB to RS-232 serial adapter may be used. Connecting to the console will require terminal emulation software such as PuTTY, TeraTerm, HyperTerminal, or similar. After installing the software, configure the serial connection as follows:

- Baud Rate = 9600
- Data Bits = 8
- Parity = None
- Stop Bits = 1
- Flow Control = None

NOTE: The above serial port settings are the factory defaults. It is possible for the user to change them in the Cisco IOS configuration. If these settings are changed on the router, they must be changed in the terminal emulator software as well. If the settings are changed, be sure to write them down. It may be very difficult to access the serial console again if the settings are forgotten!

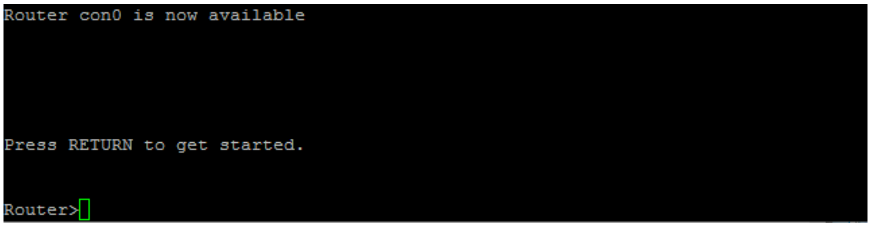
If the console is connected before power is applied to the router, the initial boot messages may be seen. It is also possible to connect the serial console while the router is powered, however the initial boot messages will be missed. If the serial console is connected after the router is booted, it may be necessary to press Enter a few times before any text is displayed.



```
System Bootstrap, Version 15.2(1r)GC1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.


Rommon signature verification PASSED for Readonly Rommon
C5915 platform with 524288 Kbytes of main memory

Readonly ROMMON initialized


flash:c5915-entbase-mz.SPA.155-1.T.bin: Digitally Signed Release Software with k
ey version A
program load complete, entry point: 0x81000000, size: 0x18ac750
Self decompressing the image : #################################################
################################################################################
################################################################################
############################################### [OK]
```

Figure 11: Serial Console Typical Boot Messages

After the router is booted, it may be necessary to press Enter a few times before the command prompt (or login prompt) is displayed. The default command prompt is **Router>**.



```
Router con0 is now available



Press RETURN to get started.


Router>
```

Figure 12: Serial Console Default Command Prompt

NOTE: By default, no password is required for the serial console. Customers are strongly urged to set a password immediately after logging in. Refer to the Software Configuration chapter later in this document for details.

4.5 Status LEDs

The following status LEDs are available on the front panel of the IDAN-IDC5915:

1. RJ-45 Port LEDs - Each port provides a single Green Link/Activity LED, which indicates status of the interfaces:

   a. Off = No Ethernet link detected, or the interface is disabled in the Cisco IOS configuration.

   b. Green Flashing = Ethernet activity detected.

   c. Green Solid = Ethernet link detected.

2. SYS LED – Green/Red LED combines the System and Temperature LED signals from the Cisco 5915 board:

   a. Off = No Power. When power is applied, it takes approximately 10 seconds before SYS will illuminate.

   b. Green Flashing = System is booting (ROMMON boot loader). The router typically takes 1-2 minutes to boot, depending on the configuration. (If the router does not boot in a timely manner, it may be waiting at a ROMMON prompt due to flash corruption or a similar issue. If so, this may be debugged via the serial console.)

   c. Green Solid = System is booted and running normally.

   d. Green/Red Flashing = The board has exceeded the temperature threshold of +85^{O}C. If the system is not immediately cooled down, it will reboot within one minute.

3. DEF LED - Green LED indicates whether or not the Factory Default (declassify) signal has been triggered via the CLR button:

   a. Off = Factory Default not initiated

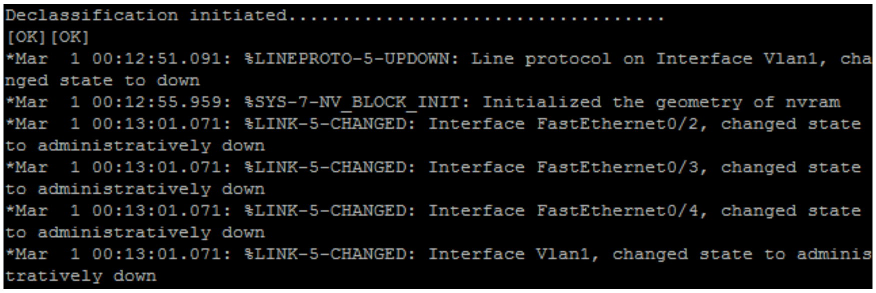
   b. Green Flashing = CLR has been pressed, Factory Default initiated, erasure in process.

   c. Green Solid = Erasure complete, all interfaces disabled. Router is now in a hung state and must be power cycled.

4.6 CLR Button

The CLR button triggers the Factory Default feature, which allows for quick erasure of the router's onboard flash memory. This feature is particularly useful for secure environments where it may be necessary to rapidly remove sensitive information from the router. The CLR button is **not** enabled by default. It must be configured in Cisco IOS via the **service declassify** configuration command.

To initiate Factory Defaults (if configured): While the router is booted (SYS LED is solid green), press and release the CLR button. If a serial console it attached, one can watch the progress messages as the memory is erased. Once the erasure is complete, the DEF LED will be solid green, all Ethernet interfaces will be disabled, and the router will hang. To use the router again, it must be power cycled, and the configuration and/or Cisco IOS image must be reloaded.



```
Declassification initiated...................................
[OK][OK]
*Mar  1 00:12:51.091: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to down
*Mar  1 00:12:55.959: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
*Mar  1 00:13:01.071: %LINK-5-CHANGED: Interface FastEthernet0/2, changed state
to administratively down
*Mar  1 00:13:01.071: %LINK-5-CHANGED: Interface FastEthernet0/3, changed state
to administratively down
*Mar  1 00:13:01.071: %LINK-5-CHANGED: Interface FastEthernet0/4, changed state
to administratively down
*Mar  1 00:13:01.071: %LINK-5-CHANGED: Interface Vlan1, changed state to adminis
tratively down
```

Figure 13: Serial Console After Pressing CLR

5 Software Overview

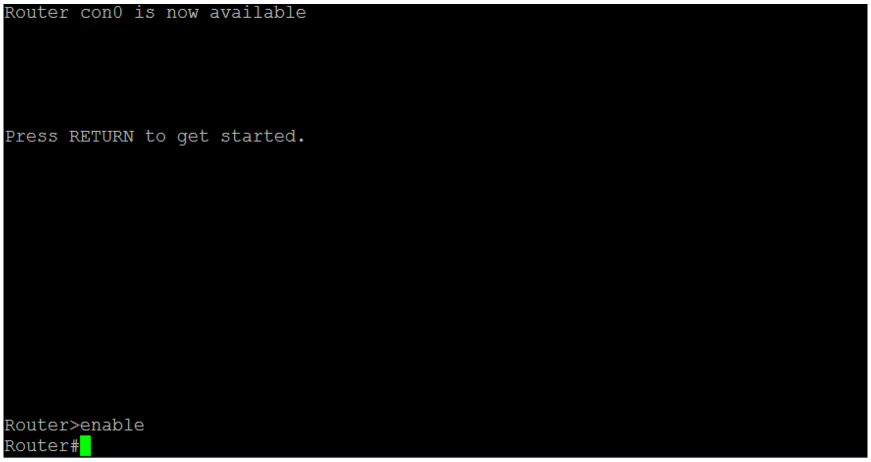
5.1 General Expectations

The Cisco 5915 Embedded Services Router and Cisco IOS Operating System are complex products that support a variety of networking protocols. The router must be configured properly before it may be used on the network. It is not a "plug and play" device, nor does it have a "simple" GUI configuration wizard. To use the IDAN-ID5915, it is assumed that one is already somewhat familiar with the Cisco IOS CLI and network engineering concepts.

The remaining sections in this chapter provide some basic information on how to configure Cisco IOS. An in-depth explanation of Cisco router configuration and network architecture is beyond the scope of this manual. Cisco provides Handbooks and Configuration Guides for IOS-based routers. Refer to the Additional Information chapter for resources. To ensure the router is configured correctly and securely, enlisting the services of a Cisco-certified network engineer is strongly recommended.

5.2 Command Line Basics

By default, when first logging into the router, the console is in user EXEC mode, which is indicated by the command prompt **Router>**. In user EXEC mode, only a limited subset of commands is available. A common task after logging in is to switch to privileged EXEC mode, which is done via the **enable** command. After doing so, the command prompt will change to **Router#**.

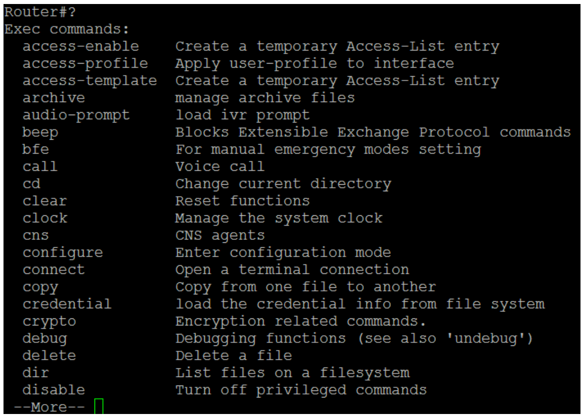


```
Router con0 is now available





Press RETURN to get started.












Router>enable
Router#
```

Figure 14: Switching to privileged EXEC mode

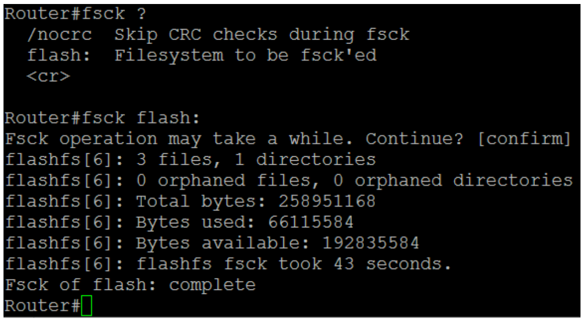
The default hostname is Router, which is reflected in the command prompt. If the hostname is changed, the command prompt will change accordingly.

The Cisco IOS CLI provides a rich help system. For a list of available commands, type **?**. The question mark can also be used to display a list of options for a command. Using this technique, it is possible to discover most of the functionality in the CLI.



```
Router#?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  audio-prompt     load ivr prompt
  beep             Blocks Extensible Exchange Protocol commands
  bfe              For manual emergency modes setting
  call             Voice call
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS agents
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  credential       load the credential info from file system
  crypto           Encryption related commands.
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
 --More--
```

Figure 15: Listing Commands



```
Router#fsck ?
  /nocrc  Skip CRC checks during fsck
  flash:  Filesystem to be fsck'ed
  <cr>

Router#fsck flash:
Fsck operation may take a while. Continue? [confirm]
flashfs[6]: 3 files, 1 directories
flashfs[6]: 0 orphaned files, 0 orphaned directories
flashfs[6]: Total bytes: 258951168
flashfs[6]: Bytes used: 66115584
flashfs[6]: Bytes available: 192835584
flashfs[6]: flashfs fsck took 43 seconds.
Fsck of flash: complete
Router#
```

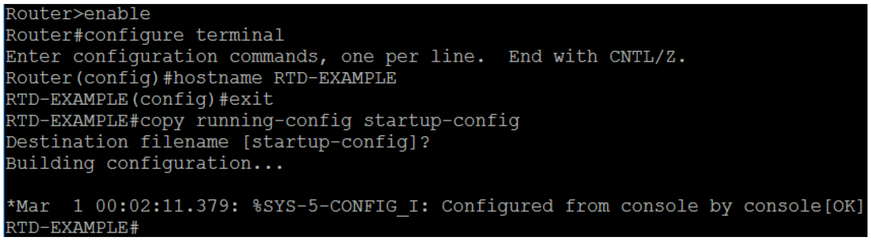
Figure 16: Listing Options for a Command

5.3 Configuration Basics

To view the current configuration of the router, use the **show running-config** command. To change the configuration, one must switch from privileged EXEC mode to configuration mode. This is done with the **configure terminal** command. The command prompt will change from **Router#** to **Router(config)#**. To leave configuration mode, use the **exit** command.

In Cisco IOS, most configuration commands take effect immediately. However, the new configuration will not persist across a reboot unless it is saved to NVRAM by running the command **copy running-config startup-config** in privileged EXEC mode. To revert changes to the running configuration, use the command **copy startup-config running-config**.

The following screenshot demonstrates using configuration mode to change the hostname, and then saves it to NVRAM:



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RTD-EXAMPLE
RTD-EXAMPLE(config)#exit
RTD-EXAMPLE#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

*Mar  1 00:02:11.379: %SYS-5-CONFIG_I: Configured from console by console[OK]
RTD-EXAMPLE#
```

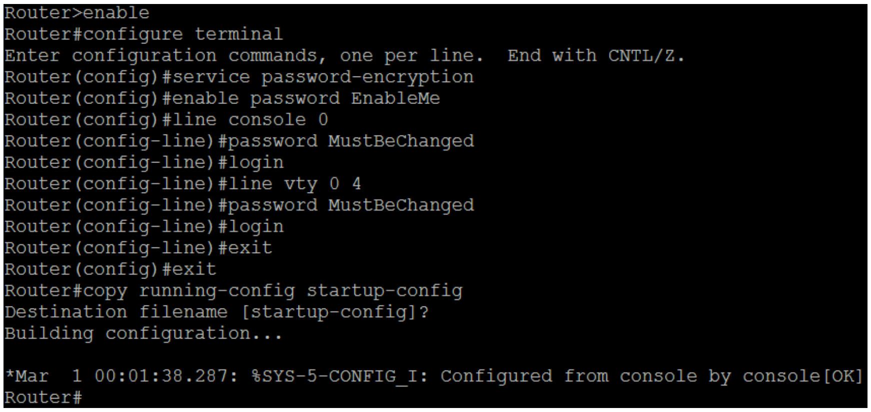
Figure 17: Changing the Configuration

5.4 Setting a Password

By default, the router has no passwords configured, which is a significant security issue. Configuration commands are used to set passwords. The serial console may have a different password than network terminal(s). A separate password may be set on the **enable** command as an additional layer of security.

By default, passwords are stored in plain text in the configuration. This weakens the security of the router as passwords can be printed to the screen via **show running-config**, and are also visible in any configuration backups. Best practice is to use the command **service password-encryption** to store the passwords in an encrypted format.

The following screenshot demonstrates a basic method to set passwords. In the example below, both local serial console and network terminals have a password of MustBeChanged set, while the **enable** command is protected with the password EnableMe.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable password EnableMe
Router(config)#line console 0
Router(config-line)#password MustBeChanged
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password MustBeChanged
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

*Mar  1 00:01:38.287: %SYS-5-CONFIG_I: Configured from console by console[OK]
Router#
```

Figure 18: Setting Passwords

More sophisticated access control is possible by enabling the Authentication, Authorization, and Accounting (AAA) framework. Consult Cisco's documentation for examples.

5.5 Enabling the CLR Button

By default, the CLR button has no effect. To enable it, the **service declassify** command must be added to the configuration. There are three possible options:

1. **service declassify erase-nvram** = The NVRAM filesystem (which contains the router settings) will be erased. The main flash filesystem will be left intact. Upon resetting, the router will be at the factory defaults.

2. **service declassify erase-flash** = The main flash filesystem (which contains the Cisco IOS image, VLAN data, and possibly logging data) will be erased. The NVRAM filesystem will be left intact. Upon resetting, the router will only be able to boot to ROMMON for system recovery.

3. **service declassify erase-all** = Both the flash and NVRAM filesystems will be erased. All data will be erased from the router, except the ROMMON boot loader. Upon resetting, the router will only be able to boot to ROMMON for system recovery.

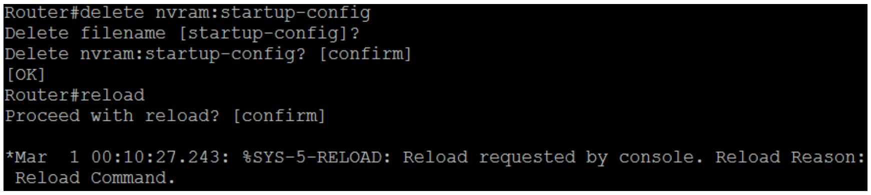
⚠

NOTE #1: Once service declassify has been set in the Cisco IOS configuration, care must be taken to ensure that CLR is not pressed accidently. If the erase-flash or erase-all options are set, the router will no longer be bootable after pressing CLR.

NOTE #2: It is strongly recommended to make a backup of the current configuration and Cisco IOS binary image so that it may be restored after a declassification. Consult Cisco's documentation for more information on backing up and restoring data from the router.

5.6 Restoring Default Settings via CLI

To erase the startup configuration via the command-line interface, run the privileged EXEC command **delete nvram:startup-config**, followed by the **reload** command. When prompted for confirmation, press Enter. The router will reboot. Once the router is booted, it will be using the factory defaults.



```
Router#delete nvram:startup-config
Delete filename [startup-config]?
Delete nvram:startup-config? [confirm]
[OK]
Router#reload
Proceed with reload? [confirm]

*Mar  1 00:10:27.243: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
 Reload Command.
```

Figure 19: Loading Defaults

5.7 Cisco Software Updates

The IDAN-ID5915 includes one year of technical support and software updates from Cisco for the 5915 Embedded Services Router. Software updates for the 5915 ESR may be downloaded from Cisco, as long as a valid support agreement is in place. Visit http://support.cisco.com for more information.

After the first year, customers are responsible for renewing their support agreement with Cisco (SMARTnet or Smart Net Total Care). RTD recommends that customers do not allow their Cisco support to lapse, so they will have access to the latest version of IOS, including security updates and bug fixes.

Once a new version of the IOS binary has been downloaded from Cisco web site, it is typically transferred onto the router via TFTP. Consult Cisco's documentation for more information.

5.8 Network Security Considerations

Since the Cisco 5915 ESR is an "active" device on the network, care must be taken to ensure that is properly secured against network threats. An improperly-configured router can leave an entire network vulnerable. Some basic security precautions include:

1. Set passwords on **all** management interfaces (serial console and network). Use passwords that are long, complex, and unique. Do not re-use passwords between systems.

2. Use the configuration command **service password-encryption** to prevent passwords from being visible as plain text.

3. Only use encrypted protocols for network management (SSH, HTTPS). Do not allow management via unencrypted protocols (Telnet, HTTP, SNMPv1, etc). **Note that most encrypted protocols are not available unless using the Advanced Enterprise version of IOS, refer to the Cisco's 5915 ESR datasheet for details.**

4. Disable network services that are not required (e.g. SNMP) to reduce the attack surface.

5. Block all network management on "untrusted" network interfaces, such as the routed WAN ports. Also disable any protocols on "untrusted" interfaces that can disclose information about the "trusted" portion of the network (CDP, Spanning Tree, etc).

6. Enable rate limiting on logons and temporary account lockout to prevent password brute force attacks.

7. Enable session timeouts to prevent an attacker from taking over a session if the previous user forgot to log out.

8. Configure logging to the flash filesystem or to an external logging server, so the log messages will still be visible after a router crash or reboot.

9. Configure the router to use synchronize its date and time with an available Network Time Protocol (NTP) server. This ensures the timestamps in the log are accurate, and also assists with validating PKI certificates.

10. Make sure the Cisco IOS version installed on the router is up-to-date to protect against security vulnerabilities and other bugs. The customer is responsible for tracking Cisco security bulletins, and installing IOS updates accordingly. Customers are strongly urged to maintain an active support agreement with Cisco (SMARTnet or Smart Net Total Care) or to ensure access to the latest IOS updates.

The above steps are basic best practices, not an exhaustive list. Customers are responsible for determining the proper security settings for their network. For additional resources, refer to Cisco's guidelines for hardening IOS devices.

6 Troubleshooting

If you are having problems with your system, please try the following initial steps:

- **Check LEDs** – Verify the color of the LEDs against the information in Chapter 4. Look for LED output that may indicate a problem.
- **Validate Serial Console** – Connect to the serial console using a terminal emulator and the settings listed in Chapter 4. Check for any serial data output. If necessary, power cycle the router and check the initial boot messages.
- **Check the Log** – If the serial console is functional, login to the router and run the **show log** command. Check for any log messages that may assist in troubleshooting the problem.
- **Restore to Defaults** – If the serial console is functional, login to the router and load defaults per the commands described in Chapter 5. This can rule out problems cause by an improper or corrupt configuration.
- **Upgrade Cisco IOS** – Download the latest version of the IOS Software from Cisco and install it onto the router. See if a new version of the software resolves the problem. (Valid support agreement with Cisco required.)
- **Simplify the System** – Remove modules one at a time from your system to see if there is a specific module that is causing a problem. Perform you troubleshooting with the least number of modules in the system possible.
- **Swap Components** – Try replacing parts in the system one at a time with similar parts to determine if a part is faulty or if a type of part is configured incorrectly.

If problems persist, or you have questions about using the product, the following support options are available:

- For questions regarding the router enclosure, the interface boards, and basic troubleshooting, contact RTD's Technical support via the following methods:

Phone:	+1-814-234-8087
E-Mail:	techsupport@rtd.com

- For questions regarding the Cisco 5915 router itself, particularly network configuration settings, contact Cisco TAC. Visit http://support.cisco.com for more information.

Also, be sure to check the RTD web site (http://www.rtd.com) for updated versions of this manual.

7 Additional Information

7.1 PC/104 Specifications

A copy of the latest PC/104-Express and PCI-104 specifications can be found on the webpage for the PC/104 Embedded Consortium:

www.pc104.org

7.2 Cisco 5915 Embedded Services Router Overview

An executive summary of the 5915 router and its capabilities:

http://www.cisco.com/c/en/us/products/routers/5915-embedded-service-router/index.html

7.3 Cisco 5915 Embedded Services Router Data Sheet

Router technical specifications and Cisco IOS features list:

http://www.cisco.com/c/en/us/products/collateral/routers/5900-series-embedded-services-routers/data_sheet_c78-680067.pdf

7.4 Cisco 5915 Embedded Services Router Hardware Technical Guide

Mechanical and electrical details of the 5915 router board itself:

http://www.cisco.com/c/en/us/td/docs/solutions/GGSG-Engineering/Cisco_5915/Hardware_Install_Guide/5915hw.pdf

7.5 Software Configuration Guide for Cisco IOS

Introduction to Cisco IOS and information on how to configure the 5915 router for common usage scenarios:

http://www.cisco.com/c/dam/en/us/td/docs/solutions/GGSG-Engineering/15_2_2/Config/15_2_2GC_Config_Guide.pdf

7.6 Cisco Guide to Harden Cisco IOS Devices

Recommendations on how to secure a Cisco IOS device:

http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

7.7 Cisco Router Configuration Handbook

A book that provides an introduction to configuring a Cisco IOS router, plus network routing protocols and concepts.

ISBN-13: 061-9472141168

ISBN-10: 1587141167

8 Limited Warranty

RTD Embedded Technologies, Inc. warrants the hardware and software products it manufactures and produces to be free from defects in materials and workmanship for one year following the date of shipment from RTD Embedded Technologies, Inc. This warranty is limited to the original purchaser of product and is not transferable.

During the one year warranty period, RTD Embedded Technologies will repair or replace, at its option, any defective products or parts at no additional charge, provided that the product is returned, shipping prepaid, to RTD Embedded Technologies. All replaced parts and products become the property of RTD Embedded Technologies. Before returning any product for repair, customers are required to contact the factory for a Return Material Authorization (RMA) number.

This limited warranty does not extend to any products which have been damaged as a result of accident, misuse, abuse (such as: use of incorrect input voltages, improper or insufficient ventilation, failure to follow the operating instructions that are provided by RTD Embedded Technologies, "acts of God" or other contingencies beyond the control of RTD Embedded Technologies), or as a result of service or modification by anyone other than RTD Embedded Technologies. Except as expressly set forth above, no other warranties are expressed or implied, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose, and RTD Embedded Technologies expressly disclaims all warranties not stated herein. All implied warranties, including implied warranties for merchantability and fitness for a particular purpose, are limited to the duration of this warranty. In the event the product is not free from defects as warranted above, the purchaser's sole remedy shall be repair or replacement as provided above. Under no circumstances will RTD Embedded Technologies be liable to the purchaser or any user for any damages, including any incidental or consequential damages, expenses, lost profits, lost savings, or other damages arising out of the use or inability to use the product.

Some states do not allow the exclusion or limitation of incidental or consequential damages for consumer products, and some states do not allow limitations on how long an implied warranty lasts, so the above limitations or exclusions may not apply to you.

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

RTD Embedded Technologies, Inc.
103 Innovation Boulevard
State College, PA 16803 USA
Telephone: 814-234-8087
Fax: 814-234-5218

www.rtd.com

sales@rtd.com
techsupport@rtd.com

EMBEDDED-PC PC/104 MODULES®

DESIGNED AND MADE IN THE UNITED STATES™

AS9100

ISO 9001