ARX®–1500 Hardware Installation Guide

MAN-0416-00

Publication Date

This manual was published on August 30, 2012.

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

3DNS, Access Policy Manager, Acopia, Acopia Networks, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, Cloud Extender, CloudFucious, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DSI, DNS Express, DSC, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, IT agility. Your way., L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Module, MSM, Netcelera, OneConnect, OpenBloX, OpenBloX [DESIGN], Packet Velocity, Protocol Security Module, PSM, Real Traffic Policy Builder, Rosetta Diameter Gateway, ScaleN, Signaling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, TrafficShield, Traffix Diameter Load Balancer, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WANJet, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by U.S. Patents 7,877,511; 7,958,347. This list is believed to be current as of August 30, 2012.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

Revision History, MAN-0416-00

September 2012 — Rev. A Hardware release.

Table of Contents

1

Introduction

Audience for this Manual

This manual is intended for field engineers and network administrators responsible for setting up and connecting the switch to a network at an enterprise data center.

Document Conventions

This manual uses the following conventions, when applicable:

- `consolas` text represents system output
- **bold** text represents user input
- *italic* text appears for emphasis, new terms, and book titles

Note

Notes provide additional or helpful information about the subject text.

Important

Important notices show how to avoid possible service outage or data loss.

WARNING

Warnings are instructions for avoiding damage to the equipment.

Danger notices help you to avoid personal injury.

Related Documents

In addition to this guide, the following F5 Data Solutions documentation is available:

- *ARX® -1500 Quick Installation*
- *ARX® Hardware Reference Guide*
- *ARX® CLI Reference*
- *ARX® CLI Network-Management Guide*
- *ARX® CLI Storage-Management Guide*
- *ARX® CLI Maintenance Guide*

Safety and Regulatory Notices

Important

The ambient room temperature range that the unit can operate in is 5 – 35° C.

Important

Do not block power supply vents or otherwise restrict airflow when installing unit in rack.

WARNING

Mechanical loading of rack should be considered so that the rack remains stable and unlikely to tip over.

Class A ITE Label

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This device is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

Note the following radiation emission-related warning if the device is installed in a Class B environment.

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Class A Warning

警告使用者

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Qualified Personnel Warning

WARNING

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Il est vivement recommandé de confier l'installation, le remplacement et la maintenance de ces équipements à des personnels qualifiés et expérimentés.

Battery Warning

小心-可能提供多個電源，維修前請斷開所有電源，以便降低電擊風險

Environmental

High Temperature Warning

WARNING

To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 35° C. To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Pour éviter une surchauffe du commutateur, ne pas le faire fonctionner dans un local dont la température ambiante dépasse le maximum recommandé de 35° C. Pour faciliter la circulation d'air, aménager un dégagement d'au moins 7,6 cm (3 pouces) autour des bouches d'aération.

Restricted Area Warning

WARNING

This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.

Warning for Rack-Mounting and Servicing

WARNING

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

- *When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.*

- *If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.*

WARNING

Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel:

- *Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.*
- *Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.*
- *Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.*

Power

International Power Cord Requirements

International power cords should have the following characteristics:

- Maximum length: 4.5 m/15 feet
- Female End: IEC-320-C13
- Capacity: 10A/250V
- Nominal Conductor size(s): 1.0mm2
- Approvals: Appropriate to the country in which it is to be used.

Power Cord Usage

WARNING

The power supply cords were designed to be connected and used for F5 devices, and the safety for this purpose has been confirmed.

Please do not use them for other devices or usages. There may be danger of causing a fire or an electric shock.

注意 – 添付の電源コードを他の装置や用途に使用しない。
添付の電源コードは本装置に接続し、使用することを目的に設計され、その安全性が確認されているものです。決して他の装置や用途に使用しないで下さい。火災や感電の原因となる恐れがあります。

Electric Shock Warning

An ARX-1500 configured with two power supplies has two power cords. If you must remove AC power from the system, disconnect both power cords before servicing the system.

Cette l'unité ARX-1500 peut être munie de deux cordons d'alimentation. Pour éviter les risques d'électrocution, débrancher les deux cordons d'alimentation avant de réparer l'unité.

Circuit Breaker (15A)

WARNING

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

Power Supply Disconnection Warning

WARNING

Before working on a chassis or working near power supplies, unplug the power cord on AC units.

Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher lecordon d'alimentation des unités en courant.

Contacting Customer Service

You can use the following methods to contact F5 Networks Customer Service:

F5 Networks Online Knowledge Base Online repository of answers to frequently-asked questions.	http://support.f5.com

F5 Networks Services Support Online Online customer support request system	https://websupport.f5.com
Telephone	Follow this link for a list of Support numbers: http://www.f5.com/support/support-services/contact/

2

Unpacking and Installing the Switch

Safety Instructions

To avoid personal injury or damage to equipment when installing or operating the switch, observe the following safety guidelines:

- Never assume that power is disconnected from a circuit; always check.
- Before installation, locate the power toggle switch on the back of the switch and and make sure it is in the OFF position. (LED not lit.)
- To avoid electric shock, disconnect any power or external cables before moving or servicing the switch.

Tools and Equipment

You need the following equipment for unpacking, rack-mounting, and installing the switch:

- Phillips screwdriver
- Tape measure (for rack-mount procedure)
- Laptop or PC to use as a serial console connected to the serial console interface
- Customer-supplied standard 19-inch EIA rack

Unpacking and Verifying Shipment

The ARX-1500 is shipped in a single box with all components installed. It weighs approximately 22.5 lb (10.2 kg)—not including packing materials.

◆ Note

After unpacking, retain all packing materials. Product returns are acceptable only in the original packaging or in packaging obtained from F5 Networks.

To unpack the ARX-1500:

1. Inspect the box for any shipping damage.
2. Open the box (top flaps) and carefully remove the power cords (2), the protective foam, the chassis, and the Accessory Kit.

   If you need to return a component, consult *The F5 Return Materials Authorization (RMA) Process* located on the AskF5 web site:

   http://www.f5.com/pdf/customer-support/rma-process.pdf

3. Verify the contents of the shipping box against the following list:
   - Power cords (2)
   - ARX-1500 (1U)
   - Accessory Kit (packed under the switch)
4. Verify the contents of the Accessory Kit against the following list:
   - Slide-rail kit (pre-packaged, includes instructions) (1)
   - Rack-mounting ear bracket kit (1)
   - Bubble bag containing:
     – Rail-locking brackets (2)
     – #6-32 pan head screws (4)
     – #8-32 pan head screws (2)
     – RJ-45-to-DB9 adapter (1)
     – Power cord retention clips (2)
     – Cross-over cable (8-ft. / 2.4384-M) (1)
     – *ARX-1500 Quick Installation* card
     – *ARX-1500 Hardware Installation Guide*

   In addition to the installation card and the installation guide, consult the *ARX Hardware Reference Guide*, which includes system specifications and requirements and details about the LEDS, cables, external interfaces, power supplies, internal disk drives, and many other hardware details. This guide is available in PDF form from the ARX Manager GUI.
5. Read the instructions for determining which rail kit to use, *Determining Which Rail Kit to Use, on page 2-4*.

   In particular, do not use the instructions that come with the slide-rail mounting kit; use the instructions in this guide. These instructions are critical to understanding how to install the rails in the rack and set the component into the rails.

◆ Note

Most equipment racks come with screws for mounting the chassis. You need 4 10-32 screws (5/8” to 7/8” long).

Determining Which Rail Kit to Use

The ARX-1500 platform comes with two types of rack mounting kits: a stationary rack-mounting type and a slide-rail-mounting type. An advantage of installing the slide-rail-mounting type is that you can then slide the component in and out of the rack as needed.

The installation tasks differ for each platform, depending on the type of rack mount you decide on or the type of cabinet you are installing into (single two-post cabinet or four-post cabinet).

General Recommendations for Rack Mounting

Although not required, a 1U space between components makes it easier for you to remove the component from the rack if that component requires service. A 1U space between components also provides additional cable routing options.

We recommend 100 mm spacing from the front panel to the rack front or rack door. This provides enough room to route the cables without excessive bending or insulation damage.

A shelf or similar device is required to support the unit if only one person is installing the unit.

Important

To prevent personal injury or damage to the unit, it is recommended that at least two people perform the installation.

Important

This product is sensitive to electrostatic discharge (ESD). Proper ESD grounding procedures and equipment are recommended when you install or maintain the unit.

Important

***Do not power on** until the management serial console or the management network is connected to the unit.*

About the Rack-Mounting Ear Bracket Kit

If you are installing into a two-post cabinet, you can use the rack-mounting ear bracket kit. You can identify this kit by its black rails. See the following figure.

Figure 2.1 *Rack-Mounting Ear Bracket Kit .*

Installing a Rack-Mounting Ear Bracket Kit

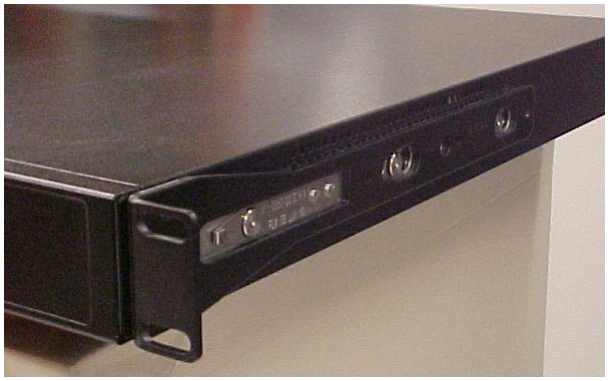
Before installing, review the environmental guidelines to make sure that you are installing and will be using the platform in the appropriate environment. For environmental details, see *Environmental, on page 1-6*.

Note

The rack-mounting ear bracket kit is located in the Accessory Kit.

1. Align the bracket's keyhole slots with the PEM fasteners on the side of the component. The following figure shows the PEM fasteners on the side of the ARX-1500.

2. Attach the bracket to the PEM fasteners, as shown in the following figure.



3. Slide the bracket toward the back of the component to lock the bracket into place.
4. Repeat steps 1 through 3 on the other side of the ARX-1500.
5. Lift the component into the rack.
6. Secure the ARX-1500 to the rack using customer-supplied hardware.

   The component must be securely fastened to the rack to provide adequate stability and to prevent it from falling out of the rack. If the rack does not provide adequate support, a shelf kit may be necessary. If you install a shelf kit, it is recommended that you install one created by the rack manufacturer.

About the Slide-Rail Mounting Kit

The slide-rail mounting kit enables you to slide the switch in or out of the rack for maintenance. You can identify the slide-rail mounting kit by its silver rails. See the following figure.

Figure 2.2 *Slide-Rail Mounting Kit*

Slide-Rail Mounting Hardware

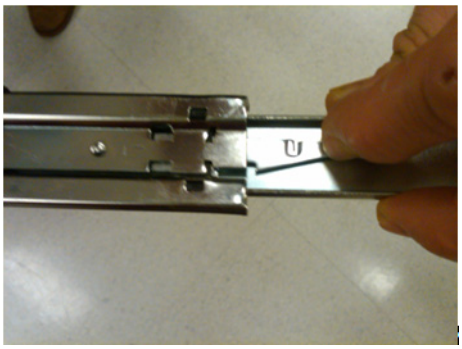
The slide-rail mounting hardware includes the following:

- Slide rails for the left side (1 pair)
- Slide rails for the right side (1 pair)
- Front-mounting bracket (1)
- Rear-mounting bracket (1)
- Thumbscrews (8)
- Wing nuts or kep nuts (8)
- Rail-locking bracket kit (in bubble bag), which includes rail-locking brackets (2), #6-32 pan head screws (4), and #8-32 pan head screws (2)

Installing the Slide-Rail Mounting Hardware

Before installing, review the environmental guidelines to make sure that you are installing and using the platform in the appropriate environment. For environmental details, see *Environmental, on page 1-6*.

1. Separate the side chassis members by lifting the lever and sliding it out.



2. Align the large end of the key holes with the slide-rail mount studs on one side of the chassis.

   The flange on the slide-chassis member should be facing the front of the chassis. Slide the piece toward the back of the chassis until it snaps into place. Repeat this step on the other side.

3. Install the two rail-locking brackets (found in the Accessory Kit bubble bag) using the #6-32 screws provided.

   The #6-32 screws are the 4 smaller screws. Save the 2 larger screws to lock the chassis into the equipment rack in the final step.

   The following figure shows an installed locking bracket.

4. Assemble the front slide-rail mounting brackets (the short ones) to slide-cabinet members, using the wing (or kep) nuts provided.

   Ensure the three-hole side of the bracket is facing out (as shown in the following figure.)

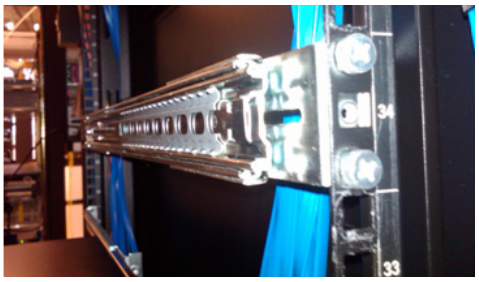
   The ends of the rail-mount brackets must be 1 1/2 inches from the ends of the slide-cabinet members before tightening the wing nuts. This ensures the chassis front is flush with the front of the equipment rack rails.

5. To determine the location of the rear-rail mount brackets, measure the inside surface of the front rail to the inside surface of the back rail of the equipment rack where the chassis will be installed.

6. Install the rear-rail mount brackets (the long ones) to the slide-cabinet members, as shown below, using the wing nuts provided. Before tightening the wing nuts, ensure the end-to-end measurement of the slide rails of the mounting brackets matches the rail-to-rail measurement of the equipment rack.

   Ensure the three-hole side of the bracket is facing out (as shown in both of the following figures.)

7. Install the slide rails on the inside rail of the equipment rack. Insert the thumb screws provided in the top and bottom holes by screwing them through the cabinet rails and into the slide-bracket threaded inserts. (Leave the middle hole open.)



8. Repeat the previous step to secure the slide rail to the rear equipment rack rail.

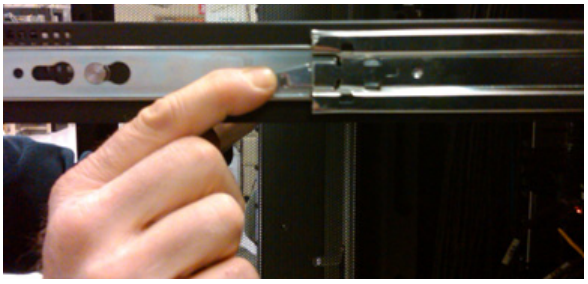
9. Extend the slide-cabinet members to their fully-locked position.

10. **This step requires two people.**

    Carefully lift the chassis and align slide-chassis members with the slide-cabinet member black plastic alignment pins.

11. Push the chassis in until it stops.

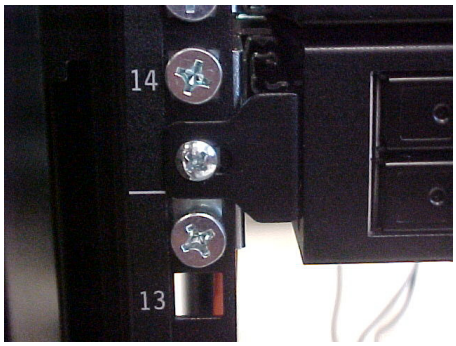
12. Unlock the slide rail by pulling up the left slide lever and pressing the right-slide lever down.



13. Slide the chassis into the rack.

14. On each side of the chassis, secure the rail-locking brackets to the rack using the 2 larger screws from the rail-locking bracket kit.

    The following figure shows the result of this step.



Attaching Cables and Powering On

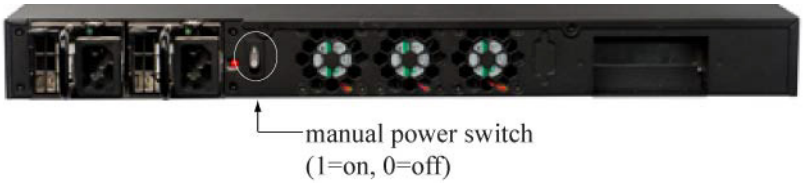
This section contains the procedure for attaching cables and powering on.

Important

***Before powering on**, make sure all AC outlets to the switch are properly grounded. Never assume that power is disconnected from a circuit; always check.*

1. On the back of the switch to the right of the power supplies, locate the manual power (toggle) switch and ensure it is in the **Off** position.

   To locate the power switch, see the following figure.



2. Attach power cords to the power supplies. Attach one power supply to one AC line feed and the second power supply to a separate line feed.

   To locate the power plug locations, see the following figure.

3. Connect the power supplies to a power source.

4. Attach the power cord retention clips by gently squeezing the sides of the clip and inserting the ends into the holes on both sides of the power supply inlet. (Retention clips are shipped in the Accessory Kit.)

5. From the front of the switch, attach a serial console cable to the serial console port (identified in the following figure).

6. From the back of the switch, locate the power switch and toggle it to the **On** position.

Cabling the Client/Server Ports

You can attach cables to the client/server ports before or after the switch is connected to the network.

F5 Networks does not supply Ethernet cables. For cable specifications and requirements, consult the *ARX Hardware Reference Guide*.

3

Connecting the Switch to the Network

Identifying the Management Ports

The ARX-1500 provides the following management ports:

- Console. Serial console port for connecting a console terminal. Labeled CONSOLE on the front of the switch.
- Management. 10/100/1000 Ethernet port for connecting an out-of-band management station. Labeled 1/1 MGMT on the front of the switch. You can use this port as either a management or a client/server port.

Both ports are identified in the following figure.

Figure 3.1 *ARX-1500 Management Ports*

During the initial-boot process (described in this chapter), you can access only the serial (CONSOLE) port. After you boot the switch, you can connect the management port to a management station or network. See *Connecting the Out-of-Band Management Port, on page 3-18*.

Connecting the Console Port

Set the following terminal parameters to match those on the console interface:

- 9600 baud rate (default)
- XON-XOFF flow control
- 8 data bits
- 1 stop bit parity

Connect the console terminal to the serial console port on the front panel. An RJ-45 to DB9 adapter is included in the installation kit if you want to connect to your management station's serial DB9 port.

Booting the Switch

The initial-boot script runs automatically at switch startup. It prompts for basic configuration and security information required to access the switch and manage it remotely.

At the console terminal, boot the switch as follows:

1. Power-on the switch (as shown in *Attaching Cables and Powering On, on page 2-12*). After some boot-up messages that may take several minutes, the following prompt appears:

   ```
   Press <Enter> to start the Switch Configuration Wizard.
   ```

2. Press the **Enter** key as prompted.

The initial-boot script is comprised of questions that prompt you for basic network information (such as management-IP address, subnet mask, and gateway). The script will also prompt you to enter the base registration key and a DNS name server IP address (needed to access the license activation server).

◆ Note

The alarm LEDs on the ARX-1500 and the ARX-2500 will remain red until the Switch Configuration process is complete. This is normal. For more information on the alarms and statuses for the ARX-1500 and ARX-2500, see the hardware installation guides for each platform (sections ARX-1500 Alarm and Status LEDs and ARX-2500 Alarm and Status LEDs).

License Activation

If you have any questions about license activation, consult the ASKF5 Knowledge Base solution on that subject. Launch a browser and enter:

http://support.f5.com/kb/en-us/solutions

On the AskF5 Knowledge Base page, enter the keyword **sol12800** and click **Search**.

Booting a Non-Replacement Switch

The following example shows the simplest initial-boot scenario: booting a new (non-replacement) switch that is either standalone or the *first* member of a redundant pair.

The answers in the example are *not* appropriate to the following scenarios:

- Replacing a defunct switch
- Joining a running switch as its redundant peer
- Re-installing a switch after F5 personnel performed a *Manufacturing Installation* on a previously-running switch (which returns a switch to its factory defaults)

Later sections discuss these contingencies and how to handle each of them. The answers below apply to the simplest case only — booting a new (non-replacement) switch that is either standalone or the *first* member of a redundant pair.

Answers are highlighted in bold text.

```
F5 ARX Startup

This F5 ARX switch does not currently have critical system
information programmed.  The following wizard prompts you
for this information.  You can connect to the switch through
the out-of-band management interface when you finish.

To restart the configuration program, enter 'r' at any prompt.


The switch's management port requires an IP address and mask.
1. Enter the management port IP address
   in the format nnn.nnn.nnn.nnn or 'none'. # 10.1.33.105
2. Enter the management port subnet mask
   in the format nnn.nnn.nnn.nnn.(default=255.0.0.0) # 255.255.255.0

The switch's management port requires a gateway IP address.
3. Enter the gateway IP address for the management interface
   in the format nnn.nnn.nnn.nnn or 'none'.(default=10.1.33.1) # 10.1.33.1

A name server address must be assigned so that the software license
   can be activated.
4. Enter the DNS name server IP address to access the license server
   in the format nnn.nnn.nnn.nnn. # 192.168.90.19

A switch replacement requires additional configuration questions.
5. Are you doing a switch replacement?
   in the format 'yes' or 'no'.(default=no) # no

The base registration key is used to activate the software license for this system.
6. Enter the switch's base registration key
   in the format xxxxxxx-xxxxxx-xxxxx-xxxx-xxxxxxx. (default=A362247-945361-27183-5068-9388182) #
<Enter>

The crypto-officer is the most privileged user in the system.
7. Enter the crypto-officer username
   in the format text (1-28 characters). # admin

8. Enter the crypto-officer password
   in the format text (6-28 characters). # ******
         Confirm the crypto-officer password # ******

A system password is required for access to the master key.
9. Enter a system password
   in the format text (12-28 characters). # *************
         Confirm the system password # *************

The master key is used to encrypt critical security parameters.
10. Enter the master key
    in the format base64-encoded key or keyword 'generate'.(default=generate) # <Enter>
```

The system displays a configuration summary. See the following example.

```
Configuration Summary

    Management IP Address    10.1.33.105
    Management IP Mask       255.255.255.0
    Management Gateway       10.1.33.1
    DNS IP Address           192.168.90.19
    Chassis GUID             64a6417e-cc3d-11df-80ca-a73fbeb72ef8
    Chassis Base Reg Key     A362247-945361-27183-5068-9388182
    Switch Password          #######
    Switch Master Key        generate

    Crypto-officer Username  admin
    Crypto-officer Password  #######

Enter 'yes' to load the configuration or 'r' to redo the interview
#yes

 You have completed the switch startup configuration.
The switch will now initialize the local database.
When the login prompt appears, log into the switch using
the crypto-officer's username and password.

Closing configuration file.
Processing configuration file. (boot-config)
...
```

The boot-up process continues to the **Username** prompt. Confirm that an administrator can log in by using the crypto-officer username and password that you entered in the initial-boot script, as in the following example.

```
...
User Access Authentication

Username: admin
Password: mypassword
SWITCH>
```

The switch is now ready for configuration through the CLI or GUI. For configuration instructions, see the *ARX GUI Quick Start: Network Setup* or the *ARX CLI Network-Management Guide*. Both are available from the ARX Manager (GUI).

Preparing for Switch Replacement

The process of replacing a defunct switch is more complicated than the initial-boot process for a new (non-replacement) switch.

You can replace a single switch or a switch that is a member of a redundant pair. The interview that runs during installation is identical regardless of the type of replacement.

When Replacing a Standalone ARX

If you replace a standalone ARX, the replacement ARX must re-import all of the managed volumes hosted by the failed ARX. This re-import occurs automatically at the end of the switch replacement process. With a standalone installation, the configuration is not saved on a backup switch. Thus, you have to save key pieces of configuration data *prior* to the switch failure.

Every ARX keeps its local network parameters in *running-config*. To replace a standalone switch, you need to copy from running-config:

- Master key (extracted and wrapped)
- Master key wrapping key password

When Replacing a Member of a Redundant Pair

Every redundant pair of ARX devices shares a single *global-config*, containing namespace and service parameters.

An ARX *startup-config* contains both *running-config* and *global-config* in a single file. Therefore, a redundant pair requires two or more saved configuration files:

• two startup-configs (one per ARX), or

• two running-configs (one per ARX) and a single global-config

These items and the procedures for saving them are described fully in the *ARX Site Planning Guide*, *Best Practice: Regularly Saving the Configuration*. For details, consult that guide (available from the ARX Manager).

Choosing Switch Replacement

When the initial-boot script asks if this is a switch replacement, answer **yes** to invoke the questions required to replace the failed switch as in the following example.

```
A switch replacement requires additional configuration questions.
6. Are you doing a switch replacement?
   in the format 'yes' or 'no'.(default=no) # yes
```

Matching the Private Subnet

The next several questions ask for the switch *private subnet*, the *private VLAN* for that subnet, and the VLAN for a *private metalog subnet*.

If the failed switch was in a redundant pair and/or Resilient-Overlay Network (RON), the private subnets of the replacement switch should match those of the failed switch. Each ARX uses its private subnet for communication with other ARX devices in the same RON and/or the switch's redundant peer. All private subnets in the RON and/or pair are carried by the same VLAN. This private VLAN, and the separate metalog VLAN, must be reserved for ARX traffic only.

The private subnet and VLAN information appear at the top of the output of the **show running-config** command. The private subnet information is bolded in the following example.

```
; ARX-1500
; Version 6.02.000.14353 (Apr 6 2012 15:13:50) [nbuilds]
; Database version: 602000.33
; Generated running-config Wed Apr 11 03:50:43 2012
; System UUID  64a6417e-cc3d-11df-80ca-a73fbeb72ef8
; ip private subnet 169.254.148.0 255.255.255.0
```

Entering the Private Subnet

Enter the private subnet as shown in the following example.

```
The switch's internal subnet requires an IP address and mask.

6. Enter the switch's private IP address
   in the format nnn.nnn.nnn.nnn.(default=169.254.62.0) # 169.254.56.0

7. Enter the switch's private subnet mask
   in the format nnn.nnn.nnn.nnn.(default=255.255.255.0) # <Enter>
```

Finding the UUID of the Failed Switch

When a switch imports storage from back-end file servers, it marks each share with its UUID (Universally-Unique ID). A replacement switch must use the same UUID or it will reject all shares imported by its predecessor. Also, you must set the UUID if the switch is brought back to its factory defaults. A *Manufacturing Installation* by F5 personnel resets the switch and its UUID.

The UUID appears at the top of the output of a **show running-config** command. In the following example from a switch named *canbyA*, the UUID is highlighted in bold.

```
canbyA# show running-config
; ARX-1500
; Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]
; Database version: 602000.33
; Generated running-config Wed Apr 11 03:50:43 2012
; System UUID  64a6417e-cc3d-11df-80ca-a73fbeb72ef8
; ip private subnet 169.254.56.0 255.255.255.0
```

If the failed switch was a member of a RON, you can enter the **show ron** command from any other RON member. The output from this command shows the UUID even if the chassis is no longer online.

In the following example, the **show ron** command (run on another switch in the RON) shows the UUID for a failed (offline) chassis, *canbyA*.

```
bstnA# show ron

Switch Name            HA Peer Switch                              Uptime
```

```
Status                  UUID                                  Management Addr
-------------------------------------------------------------------------------
bstnA                   (None)                                0 days, 02:25:23
ONLINE                  d9bdece8-9866-11d8-91e3-f48e42637d58         10.1.1.7

canbyA                  (None)                                0 days, 04:32:41
OFFLINE                 64a6417e-cc3d-11df-80ca-a73fbeb72ef8       10.1.33.105

gffstnA                 (None)                                0 days, 04:02:32
ONLINE                  e5d870ae-571e-1352-916b-ef324fbc05a2        10.1.49.60

minturnA                (None)                                0 days, 04:23:58
ONLINE                  3d17e8ce-571f-11dc-9852-ef323fbb290f        10.1.27.69

newptA                  (None)                                0 days, 04:27:31
ONLINE                  cf251849-826d-01a8-9110-8dtu78fca5b2       10.1.117.74

provA                   (None)                                0 days, 04:30:03
ONLINE                  db922942-876f-11d8-9110-8dtu78fc8329        10.1.38.19

prtlndA                 (None)                                0 days, 04:31:52
ONLINE                  876616f6-79ac-11d8-946f-958fcb4e6e35        10.1.23.11

stkbrgA                 (None)                                0 days, 04:32:46
ONLINE                  8fa98111-55ec-d1c8-9380-8dtu78fab47d     192.168.66.62

stoweA                  (None)                                0 days, 04:31:45
ONLINE                  05d5a0fa-f2fb-11df-8daf-af50d57e388e        10.1.14.76

bstnA# ...
```

Applying the UUID

Enter the UUID of the replaced switch when prompted by the initial-boot script. See the following example.

```
If this is a replacement switch, the UUID MUST be entered and
    it MUST match the UUID of the failed ARX.  The UUID can be found
    using CLI command "show ron" on the peer switch.

8. Enter the switch's UUID
   in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. #
64a6417e-cc3d-11df-80ca-a73fbeb72ef8
```

Important

No two running chassis should ever share the same UUID. Enter the UUID ***only*** *in a switch-replacement scenario.*

Installing a Redundant Peer or Cluster

If you are installing the second switch in a redundant pair (also called an ARX cluster) or if you are configuring a second ARX cluster in a Disaster Recovery (DR) configuration, you need to provide additional information to the initial-boot script because all members of the cluster share a common master key.

Note

A master key is an encryption key for all critical-security parameters (CSPs), such as administrative passwords.

Redundant switches must use the same master key because they share the same users, groups, and passwords. In the case of a DR configuration, all four ARXs must be configured with a common master key.

At the peer that is currently installed, enter the **show master-key** command to create an encrypted copy of the master key.

The CLI prompts you for the following passwords:

- System password. The system password is entered at initial-boot time and validates that you have permission to access the master key. See step 9 in the example shown in section *Booting a Non-Replacement Switch, on page 3-4.*

  The system password is 12-32 characters long.
- Wrapping password. The wrapping password is set with the **show master-key** command. The security software uses the wrapping password to encrypt (and later decrypt) the master key string.

  Enter 12-32 characters. At least one character in this password must be a number (0-9) or a symbol (!, @, #, $, and so on).

Important

Save this password because you will need it later to decrypt the master key on the replacement switch.

The **show master-key** command outputs a base64-encoded string that is the encrypted master key. Save this string and the wrapping password that you set in the command.

The following example shows the master key on a switch named *canbyB*.

```
canbyB# show master-key
Master Key System Password: %uper$ecretpw
Wrapping Password: an0ther$ecretpw
Validate Wrapping Password: an0ther$ecretpw

Encrypted master key:

2oftVCwAAAAgAAAApwazSRFd2ww/H1pi7R7JMDZ9SoIg4WGA/XsZP+HcXjsIAAAADDRbM
CxE/bc=
canbyB# ...
```

Applying the Master Key

As discussed previously, the initial-boot script prompts for the master key. Answer this prompt with the encrypted master key. Then, the script prompts for the wrapping password (as shown in the following example).

```
The master key is used to encrypt critical security parameters.
13. Enter the master key
   in the format base64-encoded key or keyword
'generate'.(default=generate) #
2oftVCwAAAAgAAAApwazSRFd2ww/H1pi7R7JMDZ9SoIg4WGA/XsZP+HcXjsIAAAADDRbM
CxE/bc=

The wrapping password is used to encrypt and decrypt the master key.
14. Enter the wrapping password
   in the format text (6-28 characters). # an0ther$ecretpw
         Confirm the wrapping password # an0ther$ecretpw
```

Replacing a Redundant Peer

As shown in the example, use the following when replacing a failed peer:

- Private subnet
- UUID
- Master key

◆ Note

If the replacement switch is running an outdated release of software, this example may not exactly match the text on your screen.

```
F5 ARX Startup

This F5 ARX switch does not currently have critical system
information programmed.  The following wizard prompts you
for this information.  You can connect to the switch through
the out-of-band management interface when you finish.

To restart the configuration program, enter 'r' at any prompt.


The switch's management port requires an IP address and mask.
1. Enter the management port IP address
   in the format nnn.nnn.nnn.nnn or 'none'. # 10.1.33.105
2. Enter the management port subnet mask
   in the format nnn.nnn.nnn.nnn.(default=255.0.0.0) # 255.255.255.0

The switch's management port requires a gateway IP address.
3. Enter the gateway IP address for the management interface
   in the format nnn.nnn.nnn.nnn or 'none'.(default=10.1.33.1) # <Enter>

A name server address must be assigned so that the software license
                        can be activated.
4. Enter the DNS name server IP address to access the license server
                        in the format nnn.nnn.nnn.nnn. # 192.168.90.19
```

Note the questions regarding switch replacement in the following:

```
A switch replacement requires additional configuration questions.
5. Are you doing a switch replacement?
   in the format 'yes' or 'no'.(default=no) # yes

The switch's internal subnet requires an IP address and mask.
6. Enter the switch's private IP address
   in the format nnn.nnn.nnn.nnn.(default=169.254.52.0) # 169.254.56.0
7. Enter the switch's private subnet mask
   in the format nnn.nnn.nnn.nnn.(default=255.255.255.0) # <Enter>

The UUID should only be entered if this switch is replacing a failed switch
   and the entered UUID should match the UUID of the failed switch.
8. Enter the switch's UUID
   in the format
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.(default=6df0854c-6af4-11d8-954a-f844c83bc5f3) #
64a6417e-cc3d-11df-80ca-a73fbeb72ef8


The base registration key is used to activate the software license for this system.
9. Enter the switch's base registration key
   in the format xxxxxxx-xxxxxx-xxxxx-xxxx-xxxxxxx.(default=A362247-945361-27183-5068-9388182) #
<Enter>

The crypto-officer is the most privileged user in the system.
10. Enter the crypto-officer username
   in the format text (1-28 characters). # admin
11. Enter the crypto-officer password
   in the format text (6-28 characters). # mypassword
         Confirm the crypto-officer password # mypassword

A system password is required for access to the master key.
12. Enter a system password
   in the format text (12-28 characters). # d0uble$ecRET
         Confirm the system password # d0uble$ecRET
```

Note the use of the encrypted master key and the wrapping password from the redundant peer to answer the master-key question in the following:

```
The master key is used to encrypt critical security parameters.
13. Enter the master key
   in the format base64-encoded key or keyword 'generate'.(default=generate) #
2oftVCwAAAAgAAAApwazSRFd2ww/H1pi7R7JMDZ9SoIg4WGA/XsZP+HcXjsIAAAADDRbMCxE/bc=

The wrapping password is used to encrypt and decrypt the master key.
14. Enter the wrapping password
   in the format text (6-28 characters). # an0ther$ecretpw
         Confirm the wrapping password # an0ther$ecretpw


Configuration Summary
    Management IP Address    10.1.33.105
    Management IP Mask       255.255.255.0
    Management Gateway       10.1.33.1
    DNS IP Address           192.168.90.19
```

```
    Chassis GUID             64a6417e-cc3d-11df-80ca-a73fbeb72ef8
    Switch Password          #######
    Switch MasterKey 2oftVCwAAAAgAAAApwazSRFd2ww/H1pi7R7JMDZ9SoIg4WGA/XsZP+HcXjsIAAAADDRbMCxE/bc=
    Wrapping Password        #######
    Crypto-officer Username  admin
    Crypto-officer Password  #######

Enter 'yes' to load configuration or 'r' to redo the interview #yes

 You have completed the switch startup configuration.
 The switch will now initialize the local database.
 When the login prompt appears, log into the switch using
 the crypto-officer's username and password.

Closing configuration file.
Processing configuration file. (boot-config)
...
User Access Authentication

Username: admin
Password: mypassword
SWITCH>
```

Checking Software and Firmware Before Joining the Pair

At this point, the switch is ready for configuration through the GUI or CLI.

Before proceding, confirm that the replacement switch is running software and firmware compatible with its peer. This ensures a proper rendezvous with the redundant peer. If the replacement ARX is running a lower release or outdated firmware, upgrade it before you proceed.

Go to the redundant peer of the switch you are replacing and check the software version there. You can log into the CLI and use the **show version** command to find this information, or log into the GUI and access the Status screen.

For example, this CLI session shows the running software on an ARX named *canbyA*. The version number is highlighted in bold:

```
canbyA# show version
  Copyright (c) 2002-2012 by F5 Networks, Inc. All rights reserved.
Running Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Armed Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Backup Release
test1.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

System Configuration:  Version 602000.33

  canbyB uptime is 4 weeks, 2 days, 2 hours, 47 minutes.

  Slot  Admin     ModuleType     ModuleState        FW Upgrade
  ----  -------   ------------   ----------------   ----------
    1   Enabled   ACM            Online             Disabled
```

```
 Resource         State                            Forwarding
 --------         -------------------------------  ----------
  Switch           Up                              Disabled
```

Check the version at the replacement ARX. In this example, the software version (6.02.000) is not outdated.

```
SWITCH> show version
  Copyright (c) 2002-2009 by F5 Networks, Inc. All rights reserved.
Running Release
test1.rel :  Version 6.02.000.11927 (Nov 23 2009 21:57:26) [nbuilds]

Armed Release
test1.rel :  Version 6.02.000.11927 (Nov 23 2009 21:57:26) [nbuilds]

Backup Release
test3.rel :  Version 6.02.000.11927 (Nov 23 2009 21:57:26) [nbuilds]

System Configuration:  Version 501000.36
```

Connecting to the Client/Server Network

The replacement switch must be connected to a machine on the network with:

- a new software-release file and
- the running-config file from the failed ARX.

If the replacement switch is running a release earlier than 6.00.000, the interview script only connects the switch to your out-of-band management network. If you are running 6.0.0 or later, or if your ARX release files and running-config files are accessible through the out-of-band network, you can skip this section. These steps are required for systems that need to access the client/server network.

To access the client/server network, enable at least one client/server VLAN with at least one member interface and a management IP and establish a default route on that VLAN's IP network. This example reaches a client/server network on VLAN 74:

```
SWITCH> enable
SWITCH# config
SWITCH(cfg)# vlan 74
SWITCH(cfg-vlan[74])# members 1/5
SWITCH(cfg-vlan[74])# exit
SWITCH(cfg)# interface vlan 74
SWITCH(cfg-if-vlan[74])# ip address 192.168.74.66 255.255.255.0
SWITCH(cfg-if-vlan[74])# no shutdown
SWITCH(cfg-if-vlan[74])# exit
SWITCH(cfg)# interface gigabit 1/5
SWITCH(cfg-if-gig[1/5])# no shutdown
SWITCH(cfg-if-gig[1/5])# exit
SWITCH(cfg)# ip route 0.0.0.0 0.0.0.0 192.168.74.1
SWITCH(cfg)# exit
SWITCH#
```

If your network has more complex requirements, consult *Configuring Layer 2* and *Configuring the Network Layer* in the *ARX® CLI Network-Management Guide* for a complete set of options and instructions.

Upgrading the Software and Firmware on the Replacement ARX

If the replacement chassis is running an outdated release, upgrade its software and firmware. Use the instructions in *Upgrading Software* of the *ARX® CLI Maintenance Guide*. If the software is more than two major releases behind the target release (that is, v3.x.y or earlier), upgrade fully to a 4.x or 5.x release and then upgrade to the target release.

The following example shows the command sequence to upgrade both the software and the firmware on the new *canbyB* switch from 5.1.0 to 6.2.0:

```
SWITCH# copy ftp://jusr:jpasswd@mysrv.wwmed.com/12345.rel
releases test5.rel
% INFO: Copying 1013 megabytes from the specified source . . .
...

% INFO: The copy completed successfully.

SWITCH# show releases

  releases
  R A test1.rel              Dec  8 00:14  800 MB
  B   test2.rel              Dec  7 00:06  800 MB
      test5.rel              Sep 10 00:09  1.0 GB
```

Arm the system with the new release and then reload the ARX to activate.

```
SWITCH# boot system test5.rel

% INFO: The boot system command may take up to 5 minutes to complete.

SWITCH# show releases


  releases
  R   test1.rel              Dec  8 00:14  800 MB
      test2.rel              Dec  7 00:06  800 MB
  A B test5.rel              Sep 10 00:09  1.0 GB

SWITCH# reload

Reload the entire chassis? [yes/no/diags] yes

System is resetting.
```

After the reboot, log in and confirm that you are running the new release.

```
User Access Authentication

Username: admin
Password: mypassword
canbyA# show version
```

```
  Copyright (c) 2002-2012 by F5 Networks, Inc. All rights reserved.
Running Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Armed Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Backup Release
test1.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

System Configuration:  Version 602000.33

  canbyA uptime is 4 weeks, 2 days, 3 hours, 40 minutes.

  Slot  Admin     ModuleType     ModuleState        FW Upgrade
  ----  -------   ------------   ----------------   ----------
    1   Enabled   ACM            Online             Disabled
```

Activating the License

To successfully join a redundant pair, activate the ARX license. To prepare for licensing, identify a DNS server that can resolve the name of the F5 license server (activate.f5.com). For example:

```
SWITCH> enable
SWITCH# config
SWITCH(cfg)# ip name-server 192.168.90.18
SWITCH(cfg)# end
SWITCH#
```

Confirm that you can reach the license server, and then activate the software license. To continue the example:

```
SWITCH# ping license-server base-reg-key CRJGVQP-DYWST-ANKR-GBYYDMT

% INFO: Activation server response: 'Thu Apr 19 04:28:00 UTC 2012'

SWITCH# license activate base-reg-key CRJGVQP-DYWST-ANKR-GBYYDMT
% INFO: The license has been successfully activated.

SWITCH#
```

Checking and/or Updating the Firmware

Check for available firmware updates. If any updates are available, install them using the **firmware upgrade all** command. Note that this process results in a system reboot.

```
SWITCH# show firmware upgrade
Show Firmware Update
--------------------

Slot Status Summary
-------------------
```

```
1    Upgrade available
3    Upgrade available
5    Upgrade available
SWITCH# firmware upgrade all

Confirmation of this command commences a firmware upgrade on the
entire chassis. During the upgrade process, the chassis reboots
automatically to complete the upgrade process. If this includes a bios
upgrade, this could take at least 30 minutes.

Proceed? [yes/no] yes

System is resetting.
...

User Access Authentication

Username: admin
Password: mypassword
SWITCH>
```

Running the Running-Config Script and Joining the Redundant Pair

Once the software and firmware are synchronized between the peers, download and run the running-config script (previously saved from the failed chassis). The following example shows the process of downloading this running-config file to the replacement switch and then running it.

```
SWITCH> enable
SWITCH# copy ftp://juser:jpasswd@ftp.wwmed.com/a2kconfig scripts running
SWITCH# show scripts


  scripts
      running                Apr 12 17:45  2.1k


SWITCH# run scripts running

The running-config script set up all local parameters, such as the hostname and the network
settings:

SWITCH#; ARX-2000
SWITCH#; Version 6.02.000.14293 (Dec  2 2011 20:04:01) [nbuilds]
SWITCH#; Database version: 602000.21
SWITCH#; Generated running-config Thu Dec  8 03:10:49 2011
SWITCH#; System UUID 876616f6-79ac-11d8-946f-958fcb4e6e35
SWITCH#; ip private vlan internal 1008 metalog 1009 subnet 169.254.100.0 255.255.255.0
SWITCH#;
SWITCH#terminal character-set unicode-utf-8
SWITCH#;================================ vlan ================================
SWITCH#config
SWITCH#  vlan 74
SWITCH#    description "personnel dept."
SWITCH#    members 1/5 to 1/6
SWITCH#...
SWITCH#;================================ system ================================
SWITCH#config
SWITCH(cfg)#  clock timezone America New_York
SWITCH(cfg)#  hostname canbyA
```

```
canbyA(cfg)# ip domain-list wwmed.com
canbyA(cfg)# ...
canbyA(cfg)# exit
canbyA#
```

If you copied the private subnet and mask from the defunct switch, this completes the switch replacement. Otherwise, the new switch learns its private subnet from its peer, re-configures itself, and reboots.

Note

A reboot is necessary to change the private subnet of an ARX.

For detailed configuration instructions, consult the *ARX® CLI Network-Management Guide*.

Connecting the Out-of-Band Management Port

After you boot the switch, you can connect the Ethernet out-of-band management port to a management station or network. To locate the management port, see *Figure 3.1*. You can use this port to access the GUI (ARX Manager) or the CLI.

To access ARX Manager, direct a web browser to the interface over HTTPS. For example:

```
https://10.1.23.11/
```

To log in, enter the crypto-officer username and password, as entered in the initial-boot script.

To access the CLI, use SSH with the interface and the crypto-officer username, for example:

```
ssh admin@10.1.23.11
```

For instructions on getting starting with ARX Manager, see the *ARX GUI Quick Start: Network Setup*. For instructions and best practices for using the CLI, see the *ARX® CLI Network-Management Guide*.

4

Maintenance

POST Diagnostics

When the switch reboots and the system powers up, POST (power-on self-test) diagnostics run automatically to verify basic hardware integrity. You can view any hardware failures at the system console through the **show version** or **show chassis** commands.

See the following example output for the **show version** command.

```
canbyA# show version
  Copyright (c) 2002-2012 by F5 Networks, Inc. All rights reserved.
Running Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Armed Release
test2.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

Backup Release
test1.rel :  Version 6.02.000.14353 (Apr  6 2012 20:12:43) [nbuilds]

System Configuration:  Version 602000.33
```

See the following example output for the **show chassis** command.

```
canbyA> show chassis

 Identification:
 Hostname                           UUID
 ---------------------------------- --------------------------------------
 canbyA                             64a6417e-cc3d-11df-80ca-a73fbeb72ef8

 Chassis:
 Chassis Type  Model Number                        Serial Number
 ------------  ----------------------------------  -------------
 ARX-1500      ARX1500LE-F5                        XX-ABCD-0508

 Private Subnet:
 Subnet             Subnet Mask
 ----------------   ----------------
 169.254.56.0       255.255.255.0

 Chassis Environment:
 Base MAC Address    Power           Fan(setting)   System Temp.   CPU Temp.
 -----------------   -------------   ------------   ------------   ------------
 00:0a:49:75:5e:00   Online          Online (high)  Normal 32 C    71 C

 Power Details:
 Supply   State
 ------   -----
   A      Online
   B      Online
```

```
Logical Disk Details:
Disk    Status                Verification Mode  Verification Rate
------  --------------------  -----------------  -----------------
1       Degraded              Automatic          10 %

Disk Details:
Disk       Size          State               Transfer Rate   Model
--------   -----------   -----------------   -------------   -----------------
 Bay 1     136.91G       Online              3.0Gb/sec       HUC103014CSS600
 Bay 2     136.91G       Rebuild      100 %  3.0Gb/sec       HUC103014CSS600

RAID Controller Details:
Rebuild Rate  Max Transfer Rate  Firmware       RAID Alarm
------------  -----------------  -------------  ------------
90 %          3.0Gb/sec          5.2-0[17945]   Enabled

Module:
Slot Ports Procs Card      Xeon               ECC State
---- ----- ----- --------  -----------------  -----------------
 1   8     1     ACM       2.6 GHz 8192 MB    Good

Slot MAC Address                   BIOS Version
---- ----------------------------  ----------------------------------
 1   000A49755E00 to 000A49755EFF  080015.20110308.1.3.00004

Disk Usage:
Name                              Total MB    Used MB     Free MB     Used%
--------------------------------  ----------  ----------  ----------  -----
System                            3173        1724        1288        58%
Releases                          6345        3402        2621        57%
Logs                              52838       51          50102       1%
Cores; DiagInfo; Lists            21133       69          19990       1%
Scripts                           3172        49          2962        2%
Reports                           8458        34          7994        1%

Metalog Usage:

Status: STANDALONE

Statistics:

I/O Count           Retransmit Count    Hourly Latency (usecs)
----------------    ----------------    ----------------------
78042               0                   36
```

A

Replacing Chassis

Before You Begin

The following section describes how to replace the ARX-1500 chassis.

Note

When returning a chassis to F5 Networks, you must include the chassis serial number. In some cases, you also need to include the base MAC address.

From the CLI, enter the **show chassis** command to obtain the serial number. If you cannot reach the CLI, read the serial number on the front, righthand side of the chassis (under the cooling vents).

See the following example output for the **show chassis** command and note the serial number and base MAC address.

```
canbyA> show chassis

Identification:
Hostname                UUID
----------------------- ------------------------------------
canbyA                  d64a6417e-cc3d-22df-80ca-a73fbeb72ef8

Chassis:
Chassis Type  Model Number            Serial Number
------------  ----------------------- -------------
ARX-1500      ARX1500LE-F5             F5-ABCD-0508

Private Subnet:
 Subnet             Subnet Mask
 ----------------   ----------------
 169.254.148.0      255.255.255.0

 Chassis Environment:
 Base MAC Address    Power           Fan(setting)   System Temp.   CPU Temp.  CPU
 -----------------   --------------  -------------  -------------  ---------  ----------------
 00:0a:49:75:5e:00   Online          Online (high)  Normal 32 C    51 C       2.6 GHz (Normal)
```

As a general rule, perform all replacements on the backup switch.

WARNING

Static electricity can damage switch components. Wear antistatic straps before handling hardware modules and disk drives.

Replacing a Chassis

Some failures require you to swap out the entire chassis. To complete this process, step through the following procedure that includes failing over and powering down the failed device.

1. Copy the current running configuration to another system (**copy running-config**).

   If the ARX-1500 is a standalone installation, copy the global configuration to another system (**copy global-config**).

2. For the failed device, write down:

   - system password
   - IP address
   - subnet mask (for the out-of-band management port)
   - UUID
   - IP address for the private internal subnet
   - system master-key

   These parameters were set during the initial interview.

   You can enter the **show master-key** command to get an encrypted copy of the master key.

3. Power down by pressing the power button to the 0 position. (The power button is located to the right of the power supplies.)
4. Turn off and unplug all connected peripheral devices.
5. Label each network cable with the name of the port to which it was connected.
6. **Remove all cables, including all power cables.**
7. Remove any screws that hold the device in the rack.
8. Pull the device out of the rack.
9. Remove the ear assemblies.
10. Install the replacement in the rack.
11. Reattach the ear assemblies if necessary.
12. Slide the device back into the rack.
13. Attach all cables, including the power cables.
14. Connect to the console port.
15. Power on by pressing the power button to the 1 position. (The power button is located to the right of the power supplies.)
16. Complete the replacement option of the Switch Configuration wizard. When prompted, enter the UUID and private subnet information collected in step 1. To review an example, see *Preparing for Switch Replacement, on page 3-6*.

If you fail to perform the replacement option, you will be required to rebuild the cluster.

17. Reboot the device.
18. Replace the running configuration.
19. Unless the device is running standalone, ensure that it pairs with the active peer. To confirm, issue the **show redundancy** command and review the output.

Index