



Application Enablement Services
Installation and Upgrade Guide for a
Bundled Server Release 4.0

An Avaya MultiVantage[®] Communications Application

02-300356
Issue 4.0
July 2007

© 2007 Avaya Inc.
All Rights Reserved

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full support information, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03-600758.

To locate this document on our Web site, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: <http://www.avaya.com/support>.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>.

Contents

Chapter 1: Prerequisites	7
Intended audience	7
Hardware requirements	7
Client application machine requirements	7
Communication Manager and media server requirements	7
Required network characteristics	8
Supported network configurations	8
Bundled Server network interface speed and duplex settings	9
IP Migration Readiness and Optimization analysis	9
Prerequisites for the Bundled Server installation	10
AE Services licenses needed	10
Information needed before installation.	10
Environmental prerequisites	10
Application Enablement Server hardware/software prerequisites	11
Bundled Server hardware at customer site	11
Prerequisites for Communication Solutions and Integration (CSI) technician	12
System precautions	12
Chapter 2: Installing and configuring hardware.	15
Installing additional memory	15
Mounting the server in the rack.	15
Attaching the brackets to the x306	16
Attaching the rails to the rack	17
Attaching the x306 to the rails	18
Connecting the modem	19
Chapter 3: Installing the software	21
Before you begin.	21
Installing the server software	21
Preparing for the installation	21
Installing and configuring the server software	24
Testing the SAMP connection	28
Upgrading the SAMP firmware	28
Preparing the system for remote configuration.	28
Testing the SAMP modem.	29
Finishing the installation	29
Partitioning the Bundled Server disk drive	31
Locations of installation/upgrade logs and RPMs.	32

Contents

Chapter 4: Installing licenses	33
Installing the Application Enablement Services license file	33
Restarting mvap	34
Troubleshooting the AE Services license installation	34
If you receive error messages from WebLM	35
If you do not have a license	35
Identifying the MAC address	36
Chapter 5: Initial administration for AE Services	37
Administering Communication Manager for AE Services	37
Administering AE Services	38
Chapter 6: Testing connectivity	41
Running tests from the OAM pages	41
Running the sample application (Device, Media, and Call Control only)	42
Chapter 7: Security considerations and guidelines	43
Chapter 8: Upgrading and updating the AE Services software	45
Upgrade considerations for RFA license	45
Upgrading the software	45
Before you begin	45
Performing the upgrade	47
Performing the upgrade from a DVD	47
Restoring the synchronized LDAP and Postgres database	50
Performing the upgrade from an ISO image	50
Restoring the synchronized LDAP and Postgres database	52
Installing a new license	52
Updating the software	53
Installing updates and patches	53
Uninstalling updates and patches	54
Appendix A: Running the sample application (Device, Media, and Call Control only)	55
Before you begin	55
The sample application files	55
Administer AE Services for the sample application	56
Administer Communication Manager for the sample application	56

Administer a station	57
Administer network region/gateway configuration (if needed).	57
Edit the tutorial properties file	57
Running the sample application	58
Troubleshooting the sample application.	59
Appendix B: Linux commands for the AE Services Bundled Server . . .	61
Server commands	61
ssh	61
scp and sftp	61
swversion	61
netconfig	62
tethereal	62
dateconfig	62
ethtool	63
service DBService start/stop/restart/status	63
service mvap start/stop/restart/status	64
service tomcat5 start/stop/restart	64
boostprio	64
route	64
shutdown -r now	65
df	65
makecert.sh	65
uname	65
RMB commands	65
rmbuseradd	65
rmbuserdel	65
rmbpasswd	65
rmbusermod	65
SAMP commands	66
samp_ppp	66
sampinfo	66
sampupdate	66
sampxmlupdate	67
Appendix C: AE Services WAN requirements	69
Appendix D: Changing NIC configurations	71
Changing NIC configuration from the OAM	71
Editing network scripts to change NIC configurations	71
Editing the network scripts for releases 3.0 and 3.1.0	71

Contents

Editing the mvap script for releases 3.1.1, 3.1.2, and 4.0	72
Appendix E: Multiple upgrade considerations	73
Index	75

Chapter 1: Prerequisites

Intended audience

- IT hardware technicians and system administrators to install and configure the hardware and software for the Bundled Server offer
 - Communication Manager administrators to administer Communication Manager
-

Hardware requirements

Client application machine requirements

You must provide a client application machine for your AE Services system.

Device, Media, and Call Control applications can be developed and executed on any machine that is capable of running the Java 2 Platform, Standard Edition (J2SE) 1.5.

For the other AE Services clients, refer to the *Application Enablement Services 4.0 TSAPI, JTAPI, and CVLAN Client and SDK Installation Guide*.

Communication Manager and media server requirements

You must have the official Communication Manager R3.1.x/4.0 running on an IP-enabled media server.

Note:

Only Communication Manager 3.1.x or later provides link bounce resiliency for AEP transport links.

AE Services supports all media servers and gateways that support Communication Manager 3.1.x/4.0.

Required network characteristics

The AE Services Bundled Server is equipped with a dual port network interface card (NIC) with port 1 defined as eth0 and port 2 defined as eth1. The Bundled Server can be configured to use a single NIC (eth0) or a dual NIC (eth0 and eth1).

With one exception, Avaya Services recommends that you configure AE Services to use dual NICs (eth0 and eth1).

- Single NIC (recommended for S8300, S8400, and S8500c media servers)

The application machine, AE Services server, and Communication Manager server reside on a private LAN, virtual LAN (VLAN), or WAN.

- Dual NIC (recommended for all other Communication Manager media servers)

In a dual NIC configuration, one interface is for the communication channel between the AE Services server and the application, and the second interface is for the communication channel between the AE Server and the Communication Manager C-LAN. or processor C-LAN.

- The application and the AE Services server are on a LAN (production LAN or VLAN) or WAN.
- The AE Services server and the Communication Manager C-LAN interfaces are on a private LAN or VLAN.

Supported network configurations

Regardless of whether a LAN, VLAN or WAN is used, The TCP/IP links between the AE Services server and Avaya Communication Manager can be connected with the following network latency requirements:

- No more than a 200ms average round trip packet delivery time as measured with ping over every one-hour time period
- Periodic spiked delays of no more than two seconds while maintaining the 200ms average round trip delivery time as measured with ping over every one-hour time period

These requirements are to maintain the AE Services communication channel with Communication Manager C-LANs over a LAN/VLAN or WAN.

Note:

The communication channel between the AE Services server and Communication Manager (C-LANs) requires a hub or data switch. A crossover cable is not supported.

Bundled Server network interface speed and duplex settings

AE Services has been tested at 100BaseT full duplex, and these are the required speed and duplex mode settings.

However, the AE Services Bundled Server defaults to network auto-negotiation. This means that a far-end node could auto-negotiate a session that sets the AE Server's network interface with speed and duplex settings that are not recommended for AE Services, such as 1000BaseT, 10BaseT, or 100BaseT half duplex.

To prevent this from happening, the installation technician can make changes to the NIC configuration from the OAM. See [Appendix D: Changing NIC configurations](#). The appendix also provides instructions for manually editing network scripts in case a browser is not available.

IP Migration Readiness and Optimization analysis

We recommend that you use the Avaya IP Migration Readiness and Optimization services to help you safely implement IP-based solutions in a stable, optimized infrastructure.

These services include a two-phased, detailed analysis of the entire network to help assess whether you can deploy a converged IP solution such as AE Services without adversely affecting your existing network applications and services.

The first phase of this analysis is the Customer Infrastructure Readiness Survey (CIRS). Certified Avaya engineers conduct a high-level evaluation of the local and wide area network infrastructure to identify any significant network issues that must be resolved prior to deploying the proposed IP solution.

Phase 2 of this analysis, Network Analysis/Network Optimization (NANO) is required when the CIRS indicates that the network will not support the proposed IP solution at the desired performance levels. Starting with the information and data gathered for the CIRS, Avaya engineers perform problem diagnosis to get at the root causes of network issues. They also provide functional requirements and recommendations for a network design that optimizes all of the resources needed to support the IP solution.

Prerequisites for the Bundled Server installation

AE Services licenses needed

For the clients being used, make sure the customer has obtained the correct licenses.

Information needed before installation

Before you begin the bundled server installation, make sure you have the following information:

- Application Enablement clients that the customer is using:
- IP addresses for:
 - AE Services server (two needed)
 - Communication Manager media server and its interfaces
 - DNS and NTP server (if needed)
 - RAS PPP IP address (obtained from ART)
- Also need these names:
 - Host name for Communication Manager media server
 - Host name for AES server
 - DNS domain name (if needed)

Environmental prerequisites

- A 19-inch 4-post rack OR a 2-post rack with a shelf and 12 inches of space above
- Rack space for the server
- Network taps for:
 - The private LAN for Communication Manager and Application Enablement Services
 - The LAN (public or private) between Application Enablement Services and application machines
- Power supply
- An analog phone line provisioned for a modem

Application Enablement Server hardware/software prerequisites

Bundled Server hardware at customer site

As part of the Bundled Server offer, Avaya provides all of the Bundled Server hardware and should have already shipped the following to the customer site. Check with the customer to ensure that these items are at the customer site before the arranged time of installation:

- An IBM x306 or x306m box

Note:

Throughout this book, the term *x306* will generally be used to refer to both the x306 and the x306m. Where there are differences between the two, the text will clearly specify which box is being referred to.

The x306 comes standard with:

- 3.0 GHz processor
- 800-MHz front-side bus
- 512 MB memory plus three more available slots for additional memory
- 300 watt AC power supply
- 80 GB hard disk drive
- DVD/CD read-only drive
- Server Availability Management Processor (SAMP) card, adapter kit, and cable

Note:

The SAMP card is a remote maintenance board that is pre-installed in the x306. This card provides remote maintenance and serviceability to the x306. The SAMP provides the following functionality:

- Secure dial-in connection to the host machine using SSH, secure shell
- Services laptop access to the SAMP, and subsequently, the host machine
- Support of hardware watchdog functionality that allows the SAMP to reset a hung processor (not available on x306m)
- Floppy disk drive for BIOS updates (not available on x306m)
- 2 10/100/1000BASE-T Ethernet Controllers onboard NICs (x306m has four more NICs)
- 2 64-bit, 66/100 MHz PCI half-length slots
- Rail kit, 4-post
- Standard BIOS with Avaya splash screen and custom defaults
- 2-post rail kit

Prerequisites

- Avaya-branded bezel and packaging
- LAN cable to connect the AE Services server to the customer's LAN

This box should be blank, or you should have permission to wipe the disk clean before the installation begins.

- USB modem (required for CSI to perform remote configuration and install the license)
- Another 512 MB of memory
- The Application Enablement Services installation DVD for bundled server

Prerequisites for Communication Solutions and Integration (CSI) technician

The technical support representative performing initial hardware configuration and software installation brings the following to the customer site:

- A laptop computer with remote access clients like `puttytel` (telnet only), `putty`, (ssh and telnet), and `pscp` (secure file copy).
- A cross-over network cable for the laptop to connect to the services port on the x306 server

The technical support representative performing the remote configuration tasks must have the customer's order number and the appropriate AE Services license file. For information about getting a license file, see [Chapter 4: Installing licenses](#).

System precautions

DO NOT make mechanical or electrical modifications to the computer. Sun Microsystems is not responsible for regulatory compliance of modified computers.



DANGER:

For installations in Japan, the power cord set included in the shipment or associated with the x306 is meant to be used with that server only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

Ensure that the voltage and frequency of the power outlet used matches the electrical rating labels on the equipment.

Wear antistatic wrist straps when handling any magnetic storage devices and printed circuit boards.

The computer uses nominal input voltages of 100-240 V AC at 50-60 Hz. The computer should be powered by an uninterruptible power supply (UPS) or a non-switched, dedicated, 20-amp circuit. Sun products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electrical shock, do not plug Sun products into another type of power source. Contact your facilities manager or qualified electrician if you are unsure what type of power is supplied to your building.

A UPS provides a temporary electrical supply to a computer for several minutes, depending on the number of components connected to the UPS. For an AE Services Bundled Server, a 2KVA minimum UPS is required for all installations. See your UPS documentation to determine the projected amount of backup battery time for your model. If the system is without power for longer than the backup time, the system may shut down improperly, and the customer could lose data.

Each of the following items requires a separate power cord:

- Computer
- External peripherals
- Monitor

Prerequisites

Chapter 2: Installing and configuring hardware

Installing additional memory

The x306 has 512 MB pre-installed memory. Avaya provides another 512 MB for the Bundled Server offer.

1. Install the 512 MB DIMM that Avaya sent to the customer's site.

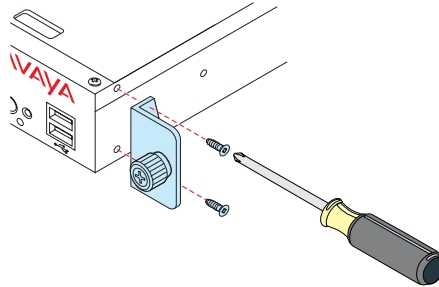
Mounting the server in the rack

The x306 ships with a 4-post rail kit.

1. Mount the x306 box into the Avaya rack using the mounting bracket kit and the included rail kit.

Attaching the brackets to the x306

1. Using the provided screws and mounting brackets, attach the mounting brackets to the front of the x306.



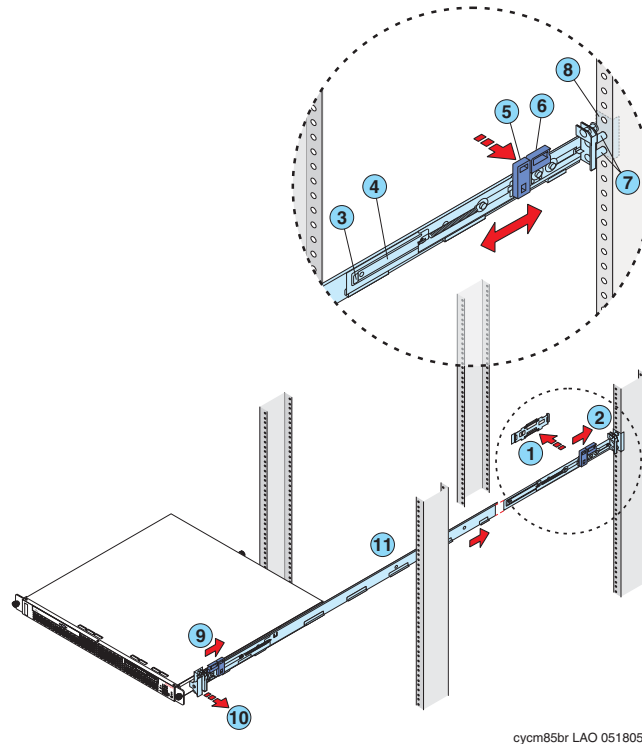
cycm85bm LAO 051805

Attaching the rails to the rack

The rails are included in the x306 shipment to the customer.

! CAUTION:

Be careful when working with the rail-locking carriers on the rails. When released, the rail-locking carriers can pinch fingers severely.



cycm85br LAO 051805

1. Press the release tab on the front shipping bracket (1) and remove the front shipping bracket from the slide rail (11). Repeat this step for the rear shipping bracket.
2. Press on the rail-adjustment bracket (3) on the rear of the slide rail to prevent the bracket from moving.
3. Press on tabs (5 and 6) and slide the rail-locking carrier toward the front of the slide rail until it snaps into place.
4. Press on tabs 5 and 6 on the front rail-locking carrier and slide the rail-locking carrier toward the rear of the slide until it snaps into place.

Note:

If you need to adjust the slide-rail length, lift the release tab (3) and fully extend the rail-adjustment bracket from the rear of the slide rail until it snaps into place.

Installing and configuring hardware

5. Align the pins (7) on the rear rail-locking carrier with the holes on the rear mounting flange.

Note:

For the next step be sure that the pins (7) are fully extended through the mounting flange (8) and slide rail.

Note:

The pins require a square-hole rack. If you have a round-hole rack, you will need to adjust the rails and use the optional screws that are shipped with the equipment to install the rails.

6. Press tab (5) to secure the rear of the slide rail to the rear mounting flange. The rail-locking carrier secures the rail to the desired position.
7. Align the pins (7) on the front rail-locking carrier to the front mounting flange (8). If you adjusted the rail length, push the rail-locking carrier back toward the rear of the slide rail to align the slide rail with the mounting flange (8).

Note:

For the next step, be sure that the pins (7) are fully extended through the mounting flange (8) and slide rail.

8. Press tab (5) to secure the front of the slide rail to the front mounting flange (8).

Attaching the x306 to the rails

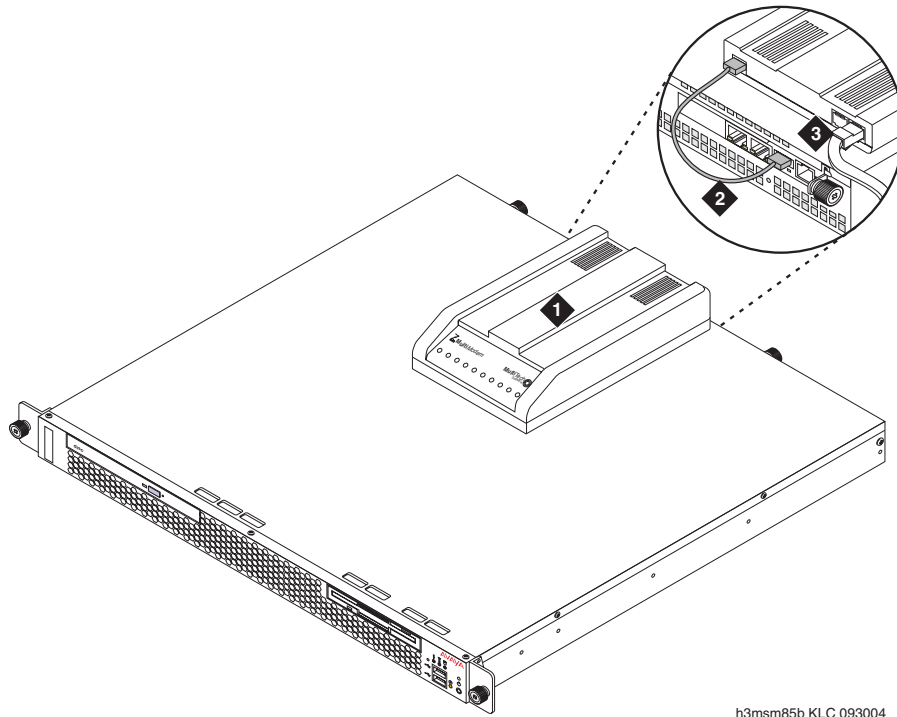
1. Align the x306 on the slide rails and push the x306 fully into the rack cabinet.
2. Secure the x306 to the front mounting flanges with the captive thumbscrews.

Connecting the modem

Note:

The modem requires a touch tone line. A rotary line will not work

The modem connects to the USB port on the Server Availability Management Processor (SAMP). Required options on the SAMP modem are set by Avaya defaults on the SAMP.



h3msm85b KLC 093004

Figure notes:

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. Modem 2. USB cable connecting the USB modem to the SAMP USB port on the x306. | <ol style="list-style-type: none"> 3. Telephone line connecting the modem to the outside line. |
|---|---|

To connect the modem.

1. Connect the modular telephone cord (supplied with the modem) to the **Line** port on the modem.
2. Connect the modem USB cable to the USB port on the SAMP.
3. Hook up the additional power supply for the SAMP.

Chapter 3: Installing the software

Before you begin

Make sure you have the following available before beginning the installation:

- The Bundled Server software DVD provided by Avaya
- A laptop with telnet and an ssh client like `puttytel` or `putty`.
- A cross-over network cable for the laptop to connect to the temporary Services port on the x306 server
- Two network taps
- A USB modem
- IP address of the modem
- PPP IP address for modem (obtained from ART script)

Installing the server software

The Bundled Server Installer installs all of the software that goes on the AES server: operating system, third-party software, AE Services software. The Installer installs all of the software in the correct order and performs all of the configuration steps that are not specific to the customer or the customer's configuration.

Note:

The IBM x306 main processor is sometimes referred to here as the host processor.

Preparing for the installation

1. Power up the x306 box (or reboot if already up).

Note:

If you do not have the Avaya-provided Bundled Server Installation DVD, obtain the latest Bundled Server ISO image from DevConnect and build a DVD from that image before the next step.

Installing the software

2. Insert the Bundled Server Installation DVD into the x306 and wait a couple of minutes.

3. Configure your laptop with the following:

```
ipaddress=192.11.13.5
```

```
netmask=255.255.255.252
```

```
gateway=192.11.13.4
```

4. Plug in a cross-over ethernet (or CAT5) network cable from the laptop to the temporary Services port on the x306 (the port labeled **2** on the back of the x306).

Note:

Port 2 will be used as the Services port until the SAMP is configured during the software installation.

The backs of the x306 and the x306m are different and the SAMP card orientation is different in the two models. Refer to the following two graphics for help in locating ports on these boxes.

Figure 1: Back of x306

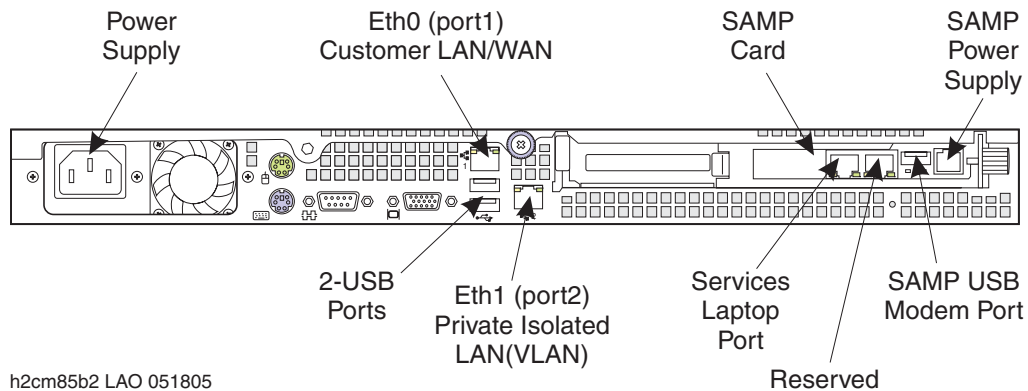
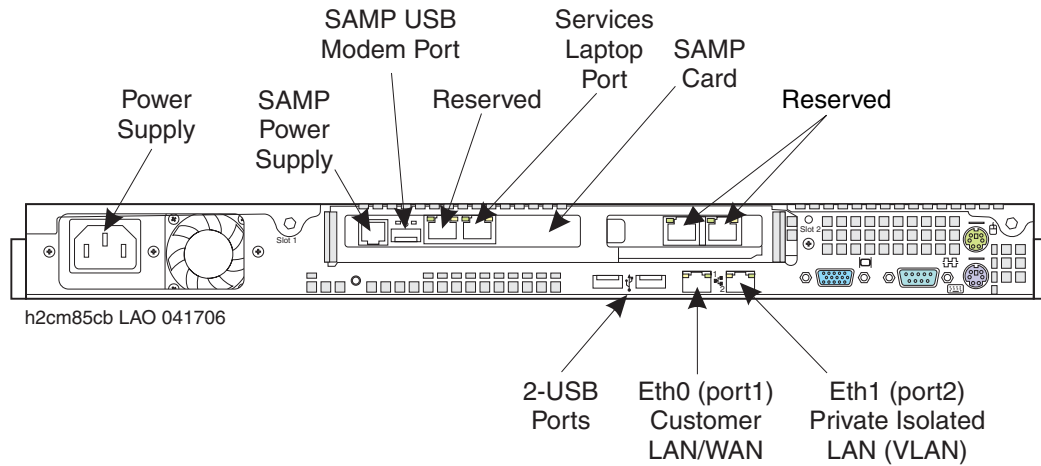


Figure 2: Back of x306m



Note:

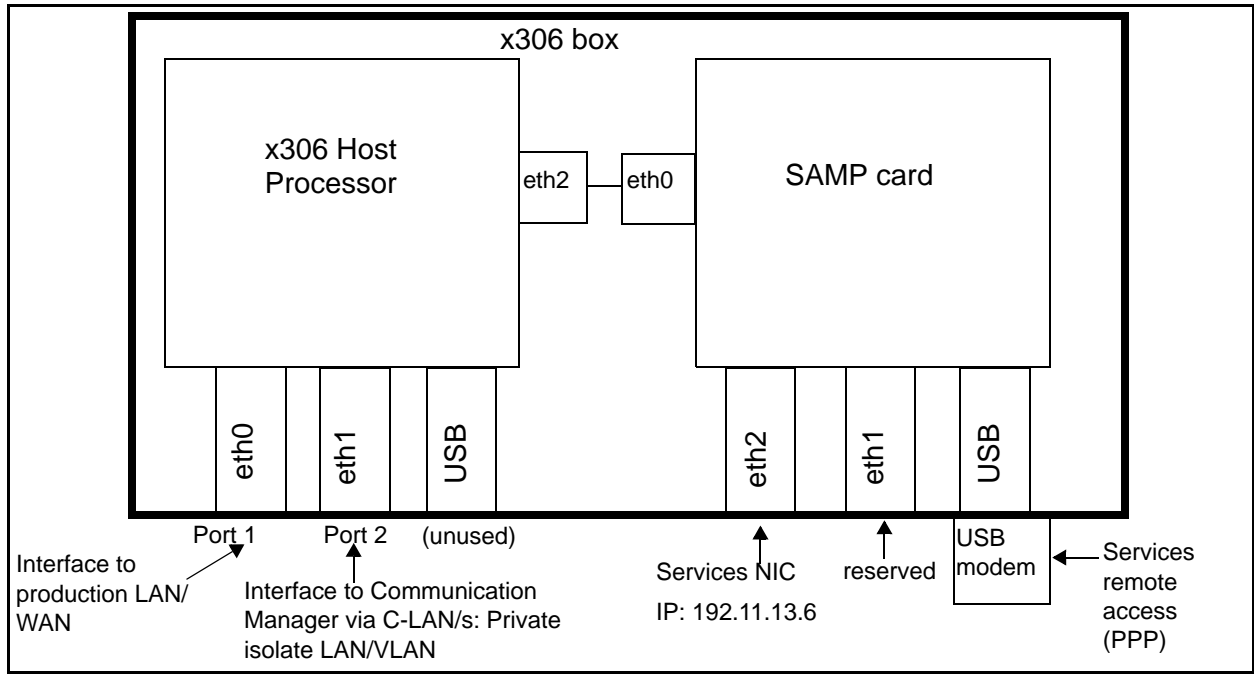
For this step and any following steps that refer to the NICs/NIC ports on the x306:

The NICs and NIC ports on the x306 are labeled on the box as **1** and **2**, but are referred to in the AE Services software as **eth0** and **eth1**.

Reference to NIC/port in AE Services software	Label for port on x306 box
eth0	1
eth1	2

The following graphic shows the network interfaces on the Bundled Server box.

Figure 3: Bundled server network interfaces



5. Verify link connectivity:

- a. From the laptop: `ping 192.11.13.6`
- b. If ping works: `telnet 192.11.13.6`

You can also check the LED on the temporary Services port (labeled **2**) of the x306 and the LED on the network card of the laptop.

These LEDs are green when the link is up and are not lit when the link is down.

Installing and configuring the server software

Note:

Always use *this* procedure, *not* an RPM command to install the AE Services software.

- 1. If you haven't already done so, power up and insert the DVD.

2. Using the MS/DOS Command Prompt from the laptop, telnet to 192.11.13.6.

This page appears.



3. Select **Install**.

4. Select **OK** and press **Enter**. Then wait a couple of minutes while the installation script begins.

 **Tip:**

In the following steps, installer screens will prompt you to make choices. To navigate and select from these screens:

- Use the arrow keys to navigate from screen to screen.
- Use the Tab key to move from option to option.
- Use the Spacebar to select an option.

Installing the software

Note:

AE Services installation requires at least 1 GB of RAM. If the x306 has less than 1 GB of RAM, a WARNING page with that information appears. It asks if you want to continue with the installation.

The Date/Time Initialization screen appears.

Date/Time Initialization
Choose Timezone

Date: Aug 09
Year: 2006
Time: 21 : 30

NTP Server: _____

OK Skip

America/Curacao
America/Danmarkshavn
America/Dawson
America/Dawson_Creek
America/Denver
America/Detroit
America/Dominica
America/Edmonton

5. Select or enter information for **Date**, **Year**, **Time**, **Choose Timezone**.
6. Leave the **NTP Server** field blank unless a known NTP server is installed on site.
7. Select **OK** and press **Enter**.

The Configure Network Information screen appears.

Configure Network Information

Hostname: server1
DNS Domain: _____
DNS Server: _____

Interface	Type	Address	Netmask	Enable
eth0	[]	_____	_____	[]
eth1	[]	192.11.13.6	255.255.255.252	[X]
eth2	[]	_____	_____	[]
eth3	[]	_____	_____	[]
eth4	[]	_____	_____	[]

Default Gateway: _____

OK Skip

8. Provide information for the following fields.

- **Hostname**
- **DNS Domain**
- **DNS Server** - IP address
- **eth0** - IP address of the public network

Type an **X** under **Enable**.

The public network is used for communication to the application as well as for communication for Device and Media Control Services bearer/media.

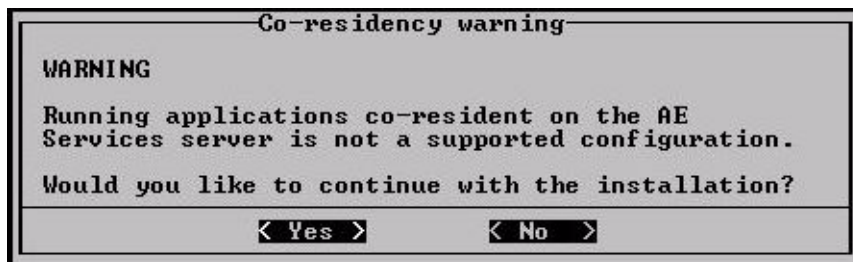
- **eth1** - Initially, this is the IP address of the Services NIC.

Do not change anything for eth1. It is initially used for the Services NIC. This NIC (eth1) with an IP address of 192.11.13.6, is initially used by the Services technician. When the Services technician runs `netconfig` (see step 4 in [Finishing the installation](#) on page 29), the technician specifies the private network IP address.

- **Default Gateway** - IP address

9. Select **OK** and press **enter**.

The co-residency warning screen appears:



10. Select **Yes** to continue the installation.

The Installer completes the installation.

After about five minutes, the installer ejects the DVD and reboots the x306 server.

Note:

After the reboot, it takes about 5 - 7 minutes for all services within AE Services to come up.

Note:

For security reasons, the firewall on the Bundled Server enables only the ports and port ranges that AE Services uses. Traffic on all other ports is disabled by default. For a list of the enabled ports see the *White-paper on Security in Application Enablement Services for Bundled and Software only solutions*.

11. Register the AE Services server with Avaya.

Testing the SAMP connection

Run:

```
sampcmd samp-update status
```

If a response comes back from the SAMP, there is connectivity to the SAMP.

Upgrading the SAMP firmware

1. Download the R2 or later SAMP firmware from support.avaya.com to the /tmp directory.
2. Log into the x306 as **craft**.

Note:

Use the default craft password for the release you are upgrading from, either 3.1.x or an earlier 4.0 release.

3. `cd /tmp`
4. Update the SAMP firmware (**xxx.tbz**) file:

```
sampupdate /tmp/xxx.tbz
```

where **xxx.tbz** is the downloaded SAMP firmware file.

If the password has changed in the firmware, the system prompts you for the SAMP craft password.

5. If prompted for the password, enter the default SAMP craft password.

Preparing the system for remote configuration

To prepare the system for configuration by a CSI technician:

1. Configure the PPP IP address of the modem (local and remote) on the SAMP card:
 - a. Log into the x306 as **craft**.

Note:

Use the default craft password for the release you are upgrading from, either 3.1.x or an earlier 4.0 release.

- b. Enter this command:

```
samp_ppp_config -i xxx.xxx.xxx.xxx
```

where:

- **xxx.xxx.xxx.xxx** = the local PPP IP address of the SAMP

Note:

The remote PPP IP address automatically becomes `xxx.xxx.xxx.xxx +1`.
Both IP addresses are obtained through the Automatic Registration Tool (ART).

Testing the SAMP modem

Before you test the modem, verify that there are two red LEDs (to the extreme right) lit on the Multitech Modem. After you have verified that the LEDs are lit, dial into the x306 Multitech modem using either a regular phone or a modem on a PC/laptop. Verify that the modem answers the call.

Finishing the installation

To finish the installation and check connectivity:

1. Plug in the cross-over cable from your laptop to the Services NIC on the SAMP.
For help in locating the Services port see.
 - [Figure 1: Back of x306](#) on page 22
 - [Figure 2: Back of x306m](#) on page 23
2. Wait for a couple of minutes. Then from your laptop, perform the following steps for the Bundled Server you are using:
 - For the x306:
 - a. Use a program like `putty` to `ssh` into the x306 host processor: `ssh 192.11.13.6`.
The system prompts you for a login and password.
 - b. Log in as `craft` and use the default password.
 - For the x306m:
 - a. Use a program like `putty` to `ssh 192.11.13.6` on port 10022.
The system prompts you for a login and password.
 - b. Log in as `craft` and use the default craft password.
 - c. `ssh craft@my-host` or `ssh craft@192.11.13.1`.
The system prompts you for a password.
 - d. Enter the default craft password.

You are now logged into the host processor of the Bundled Server (as the SAMP reroutes to the host processor).

Installing the software

3. Plug the two network cables into NIC ports labeled **1** and **2** on the back of the x306. **1** will be plugged into the public network and **2** will be plugged into the private network.

Note:

The SAMP NIC now becomes the permanent Services NIC.

4. Run `netconfig` to change the eth1 IP address.

Note:

This eth1 IP address is provided by the customer for the customer's private network.



Important:

Do not change anything for **eth2**. eth2 is for the SAMP.

5. Check the `/etc/hosts` file to make sure that:

- 192.11.13.1 is my-host
- 192.11.13.2 is my-samp

Correct these lines if necessary.

6. Check network connectivity.

- a. Go to the OAM Web pages:

`https://x306_IP_address:8443/MVAP`

- b. Log in as **craft**.

- c. Navigate the menu bar on the left:

CTI OAM Admin > Utilities > Ping Host

- d. Enter the host name.

- e. Click **Ping**.

7. At this point, have the customer change the **cust** password. (Default is **custpw**)

8. If the customer needs a root login, add a root login with the required password.

Note:

The hostname of the AE Services server must not be associated with the loop back address 127.0.0.1. The hostname of the AE Services server should be associated with the IP address of eth0.

Partitioning the Bundled Server disk drive

Important:

Read this section *before* creating any directories or files on the server. If you do not follow these recommendations, you could lose files or directories.

The Bundled Server has a SATA Hard Disk with 80 GB of disk space. When AE Services is installed on the Bundled Server, three disk partitions are created.

Partition	Size	Purpose
<code>/</code>	Approximately 19 GB	Active partition
<code>/root2</code>	Approximately 19 GB	Inactive or offline partition
<code>/var</code>	Approximately 37 GB	Common partition

The remaining space is allocated for cache and other uses.

During a fresh installation, the AE Services software is installed on the `/` partition.

When an upgrade of AE Services software is performed:

1. The upgrade script installs the new version of AE Services software on the `/root2` inactive partition
2. Then the upgrade script reboots the Bundled server.
3. When the server reboots, the software versions on the `/` and `/root2` partitions are switched.

The new version of AE Services software is now on the `/` active partition and the old version is on the `/root2` partition.

One exception is that any directory or file created in the `/home` directory under any of the logins like **sroot**, **craft** are always copied over during an upgrade. But copying is an expensive and time-consuming process. For large files like media files or databases, copying these files can delay the upgrade process.

Important:

Thus, if you create directories or files on the Bundled server, you should create them in the `/var` common partition.

We strongly recommend that you store any user level files including media files and databases in the `/var` partition.

Note:

Do not replace any of the directories under `/opt/mvap` with a symbolic link to another directory. This may result in breakage and is not a supported configuration.

Locations of installation/upgrade logs and RPMs

- The Installation/upgrade log files are in
/var/disk/logs/cinstall-xx-xx
where xx-xx = a time stamp
(for example, /var/disk/logs/cinstall-20050307-095150)
- Copies of RPMs for each release that is installed (up to three installs) are kept in:
/var/disk/software

Chapter 4: Installing licenses

AE Services 4.0 users must install a valid 4.0 license file. AE Services will not start with a license file that is missing or from the wrong release.

Installing the Application Enablement Services license file

The AE Services license file is distributed separately in an email from Avaya. If you have not received a license file from Avaya, see [If you do not have a license](#) on page 35.

1. Locate the email containing the AE Services license file.
2. Detach the license file from the email, and store it locally on a PC.

Note:

The PC that the license file is stored on does not have to be same PC that the AE Services server is installed on.

3. Start your browser and type the appropriate URL based on this example:

`https://aeshostname/WebLM/`

where:

- *aeshostname* is your AE Services server host name

For example:

`https://myaessrv.abc.com/WebLM/`

or

`https://192.168.1.1/WebLM/`

4. Accept the SSL certificate that is presented.

The browser then displays the WebLM Administrator Login page.

Note:

If the SSL certificate is not presented, check to make sure that WebLM server is running on an AE Services server.

5. Accept the default User name (**admin**) and type the default password.
6. Click **Continue**.

Your browser displays the Change Administrator Password page.

Installing licenses

Note:

WebLM issues the Change Administrator Password page the first time you log in to WebLM. If you get a new license, you do not have to change your password the next time you log in to WebLM.

7. Complete the Change Administrator Password page and click **Change Password**.

The browser goes back to the login page.

8. Log in as **admin** with the new password you specified.

The browser displays the Install License page.

9. Under **Enter License Path**, click **Browse** and locate the AE Services license file. Once you have located the license file, click **Install**.

WebLM uploads the license file from your PC to the WebLM server and displays the following message: `License File is installed successfully`.

If you do not receive this message, see [Troubleshooting the AE Services license installation](#).

10. Log out of WebLM and restart AE Services to use the capabilities of the new license.

This completes the AE Services license installation.

Restarting mvap

You must restart mvap at this time (not when restarting the other services) because mvap can not restart until after the license file is installed.

```
/sbin/service mvap restart
```

Troubleshooting the AE Services license installation

Use the information in this section to troubleshoot problems you might encounter during installation of the license. It covers the following topics:

- [If you receive error messages from WebLM](#)
- [If you do not have a license](#)

If you receive error messages from WebLM

If your browser displays the following messages, contact your Avaya representative.

Message	Explanation
License file is invalid or not created for this server. License file was NOT installed.	The file is corrupt or the MAC address in the license file does not match the MAC address in the server.
Attempting to install a license file that is currently installed. License file was NOT installed	The license has already been activated.
No valid license file found	This WebLM message may appear after AES provides this successful license installation message: "license file installed successfully" If this happens, make sure that in step 3 in Installing the Application Enablement Services license file on page 33, <i>aeshostname</i> is your AE Services server's host name (not the IP address).

If you do not have a license

If you discover that you have not received the AE Services license file in an email from Avaya, contact your Avaya representative or Avaya Partner representative. To ensure that your request is processed as quickly as possible, be ready to provide the information listed in [Required information for requesting a license file](#).

Note:

You must send a separate request for each license file.

Table 1: Required information for requesting a license file

Required information	Description
Return email address	Avaya emails this license file to you. You must provide a secure email address where you want to receive the license file.
MAC Address of the NIC	For more information, see Identifying the MAC address .

Identifying the MAC address

If you have already installed AE Services, use WebLM to identify the MAC address of the NIC:

1. Start your browser and type the appropriate URL based on this example:

```
https://aeshostname/WebLM/
```

2. When WebLM comes up, the Server Properties page contains a value for **Primary Host ID**. That value is the MAC address.

As an alternate method (if you have not installed AE Services), you can use the Linux `ifconfig` command to identify the MAC address of the NIC on your PC.

1. From the Linux command prompt, type the following command: `ifconfig`

Linux displays the current information about the network interface. For example:

```
eth0  Link encap:Ethernet  HWaddr 00:B0:D0:44:9F:A1
      inet addr:10.10.10.10 Bcast:10.255.255.255  Mask:255.0.0.0
```

In this example, the MAC address (which corresponds to the HWaddr) is 00B0D0449FA1 (when specifying a MAC address do not include colons).

2. Provide the MAC address to your service representative when you request a license.



Important:

If your server is configured with multiple NICs, provide the MAC address of the first NIC. If your server is configured with a dual port NIC, provide the address of the first port.

Chapter 5: Initial administration for AE Services

You must administer both Communication Manager and AE Services to complete the installation of AE Services. This chapter provides tables of these administration procedures, which:

- Establish initial connectivity between AE Services and Communication Manager:
- Allow Communication Manager to interact with Application Enablement Services client applications.

The tables direct you to the appropriate section or sections in the *Application Enablement Services Administration and Maintenance Guide*. The tables also explain the services for which you perform each procedure.

Administering Communication Manager for AE Services

Procedure	Performed if you use these services	Which section in Chapter 1 of AE Services Admin Guide
Check for call control features licensed on Communication Manager	Call Control	"Checking for call control features licensed on Communication Manager"
Set up a transport link	Check the referenced sections in the <i>Administration and Maintenance Guide</i> to decide which links you need to set up.	"Configuring IP Services"
Set up a CTI link		"Call Control Settings"

Initial administration for AE Services

Procedure	Performed if you use these services	Which section in Chapter 1 of AE Services Admin Guide
Check for appropriate VOIP resources	Device, Media, and Call Control	"Checking for appropriate VOIP resources"
Check for IP_API_A licenses		"Checking for IP_API_A licenses"
Add stations for a Device, Media, and Call Control application		"Adding stations for the application"
Configure Communication Manager for signaling and media encryption		<ul style="list-style-type: none"> ● For signaling encryption: "Administering a network region" ● For media encryption: "Checking for media encryption" <p>See also the <i>White paper on Security in Application Enablement Services for Bundled and Software only solutions</i>. This white paper is available on the Avaya support site along with the customer documents.</p>

Administering AE Services

Procedure	Perform procedure If using:	Where to find in AE Services Admin Guide
Create a user account for OAM access	All (without a services contract)	"Adding a Linux user and setting the OAM account password" in Chapter 7, "Administering AE Services from the Operating System Command Prompt"
Administer CT users	TSAPI, JTAPI and Device, Media, and Call Control	"Adding a CT User to the AE Services User Service database" in Chapter 3, "AE Services OAM administration and CTI OAM Administration"

Procedure	Perform procedure If using:	Where to find in AE Services Admin Guide
Specify NICs for AE Services	All	“Administering the local IP for all AE Services” in Chapter 3, “AE Services OAM administration and CTI OAM Administration”
Administer transport link connectivity to Communication Manager C-LAN/P-C-LAN	Check the referenced sections in the <i>Administration and Maintenance Guide</i> to decide when to administer a transport link.	“Administering Switch Connections,” in Chapter 2, “AE Services OAM Administration and CTI OAM Administration”
Administer H.323 Gatekeepers	Device, Media, and Call Control	“Administering Switch Connections,” in Chapter 2, “AE Services OAM Administration and CTI OAM Administration”
Administer links	All call control	“Link Administration - CTI Link Admin on AE Services OAM” in Chapter 2, “AE Services OAM Administration and CTI OAM Administration”
Check application link encryption	Device, Media, and Call Control Services	“Checking application link encryption” in Chapter 2, “AE Services OAM Administration and CTI OAM Administration”
Administer the Security Database settings	TSAPI or Telephony Web Services	Chapter 5, “TSAPI Configuration and the Security Database”

If integrating with a Microsoft Live Communications Server

Procedure	Perform procedure If using:	Where to find:
Administer TR/87	TR/87 to integrate with a Live Communications Server	<i>AE Services TR/87 Implementation Guide</i>

After completing all installation and configuration procedures, you should restart AE Services.

Chapter 6: Testing connectivity

Running tests from the OAM pages

You can use the following OAM Utilities pages to check connectivity:

- ASAI Test - to test ASAI links
- Ping Host - to ping a host name IP address
- TSAPI Test - to place a test phone call
- TR/87 Test - (If connecting to LCS) to make a call

Note:

You can run the TR/87 test only after administering the dialplan.

The following table shows which OAM Utilities page can be used for which services:

	ASAI Test	Ping Host	TSAPI Test	TR/87 Test
Call Control (CVLAN/TSAPI)	X	X		
DLG		X		
Device, Media, and Call Control		X		
Call Control (TSAPI)	X	X	X	
Telephony Web Service			X	
TR/87 (for LCS)				X

These tests are located in the **Utilities menu** in the OAM. For information about running these tests, see the OAM Help pages.

Running the sample application (Device, Media, and Call Control only)

If you are using the Device, Media, and Call Control Services, you can also set up and use the sample application created for these services. Running this application tests that the server files are installed correctly and that you have achieved connectivity with Communication Manager.

See [Appendix A: Running the sample application \(Device, Media, and Call Control only\)](#).

Chapter 7: Security considerations and guidelines

For a complete discussion of the security considerations and guidelines for AE Services, see the *White-paper on Security in Application Enablement Services for Bundled and Software only solutions*. This white paper is available on the Avaya support site along with the customer documents.

Chapter 8: Upgrading and updating the AE Services software

Upgrade considerations for RFA license

If you are upgrading from AE Services 3.0 or 3.1.x, you must obtain a new RFA license before performing the upgrade.

Upgrading the software

Use this procedure for upgrading from AE Services 3.0 or 3.1.x to AE Services 4.0 or upgrading to a new 4.0 load. There are some differences in these procedures. These differences are noted in the appropriate sections.

Note:

Upgrades can be performed only on a server that already has a version of AE Services installed on it.

Before you begin

Before performing an upgrade:

1. (If upgrading from AE Services 3.0 or 3.1.x) Install the AE Services 4.0 upgrade patch.
 - a. Get the upgrade patch from the Avaya support website and upload it to the AE Services server.
 - b. Ensure that you are logged in as sroot.
 - c. Enable execute permissions on the preupgrade patch:

```
chmod 744 AES4.0-v1.2.preupgrade
```
 - d. Run: `./AES4.0-v1.2.preupgrade`
2. Perform a backup from OAM to back up the database, LDAP, and the AE Services configuration.
 - a. Log in to the AE Services OAM pages.

Upgrading and updating the AE Services software

1. Start your browser and type the appropriate URL based on this example:

```
https://aeshostname:port/MVAP
```

where:

- *aeshostname* is your AE Services server's host name
- *port* is your AE Services server's port number (the default port number is 8443)

2. Log in.

- b. From the AE Services OAM pages:

CTI OAM Admin > Maintenance > Backup Database

Save the database backup file to a safe location that will not be affected by the AE Services 4.0 installation. The backup file is stored at that location under the name `mvapdbddmmyyyy.tar.gz`

For more information, see the section "Backing up the database" in Chapter 2, "AE Services OAM Administration and CTI OAM Admin" in the *Application Enablement Services Administration and Maintenance Guide*.

3. Make sure you also back up any files in directories that are not automatically preserved. This includes the home directories of accounts created by the previous installation (for example, `craft`, `avaya`, `sroot`).
4. From the CTI OAM Main menu, select **Administration > Local IP** and record the Local IP settings listed on the Local IP screen.

Important:

If you create directories or files on the Bundled Server, you should create them in the `/var` common partition so they will not be moved to the `/root2` inactive partition during a software upgrade. For an explanation, see [Partitioning the Bundled Server disk drive](#) on page 31.

*We **strongly recommend** that you store any user level files including media files and databases in the `/var` partition.*

Important:

This following step is an important precaution if you are upgrading from AE Services 3.0 in case the upgrade fails.

5. (Only if upgrading from AE Services 3.0) To maintain a synchronized LDAP and Postgres database.
 - a. Log in to the 3.0 AE Services server as `craft` and `su` to `sroot` (use the command `su - sroot`).
 - b. From the command line, execute the following commands

```
cd /var/lib/ldap
```

```
tar -cvf tar_file_name.tar *.dbb
```

- c. Save the tar file in a safe location that will not be affected by the 4.0 installation.

Performing the upgrade

You can upgrade from a DVD or from an ISO image. Perform the appropriate upgrade procedure.

Note:

The initial install and two upgrades are stored on the server. To store subsequent upgrades, see [Appendix E: Multiple upgrade considerations](#).

Performing the upgrade from a DVD

⚠ WARNING:

Do not boot the Bundled Server from a DVD. Booting the Bundled Server from a DVD will perform a fresh installation of AE Services, not an upgrade.

To upgrade the software from a DVD:

1. Log in to the server as **craft** and **su** to **sroot** (use the command **su - sroot**).
2. Insert the DVD containing the AE Services 4.0 ISO image.
3. From the command line, launch the upgrade script:

```
upgrade -d
```

The upgrade process starts with this prompt:

```

AE Services Upgrade
AE Services Server

Doing an Upgrade will Stop AE Services, Tomcat
and DBService. Do you wish to Continue?

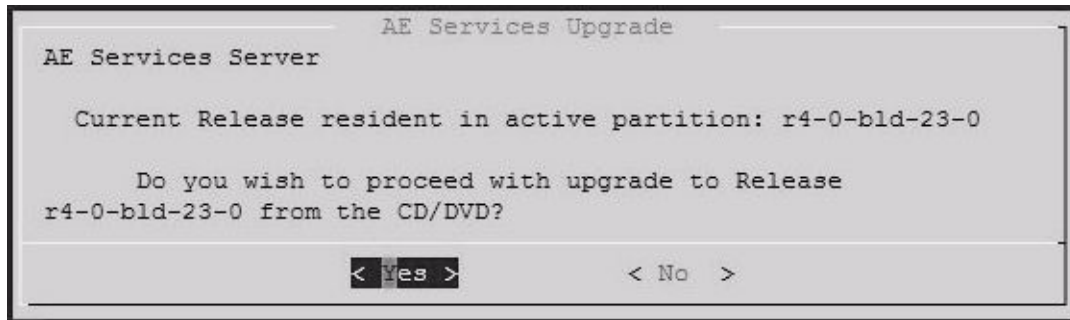
< yes >      < No >

```

4. Select **yes**.

Upgrading and updating the AE Services software

- The system allows you to review the current release and the release you will upgrade to if you continue:



- Select **Yes**.

The upgrade process continues on the inactive partition of the Bundled Server, and the server reboots:

```
Added a1 *
00:57:03 | Setting one-time boot to target a6
00:57:03 | Stamping Version Number
00:57:03 | calling SYSTEM hook final
00:57:03 | system hook final not implemented
00:57:03 | calling CORE hook final
00:57:03 | calling ThirdParty hook final
Third Party Package final hook not implemented
00:57:03 | calling MVAP hook final
00:57:03 | Success
00:57:03 | Update completed at Thu Aug 10 00:57:03 MDT 2006
Ejecting CD/DVD from CD/DVD Drive
```

- Make sure the DVD ejects before the reboot and take out the DVD.


WARNING:

Do not boot the Bundled Server from a DVD. Booting the Bundled Server from a DVD will perform a fresh installation of AE Services, not an upgrade.

- Log in to the server again as **craft** and **su** to sroot (use the command **su - sroot**).
- Manually restore the AES 4.0 database using the Maintenance > Restore Database option in the OAM interface. For detailed description of how to restore the database, refer to Ch. 2 in the *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*.
- Verify that the upgrade was successful:
 - From the command line run **swversion** and verify that the version number and build number are correct.
 - Validate the configuration data:

- a. Log in to the AE Services OAM.
For more information, see step 1 in [Before you begin](#) on page 45.
 - b. Select **CTI OAM Admin > Administration**.
 - c. Check all of the OAM pages listed under **Administration** on the Administration page. Verify that the information is complete and correct.
11. Verify the local IP settings. If they are different from the pre-upgrade settings, change them back to those settings.
12. Perform the appropriate step:
- If the upgrade was *not* successful, do not continue with these steps. Instead, reboot into the original active partition to roll back to the original 3.x software release and configuration.
 - If the upgrade was successful, continue.
13. Upgrade the SAMP firmware
- a. Retrieve the SAMP R2 or later firmware from support.avaya.com.
 - b. Run sampupdate to update the SAMP firmware to R2.

```
sampupdate /tmp/xxx.tbz
```

where **xxx.tbz** is the downloaded SAMP firmware file.
14. Make the upgrade permanent by entering the following command:
- ```
upgrade -p
```
-  **Important:**  
If you do not make the upgrade permanent, on the next reboot, the server will revert to the previous release of AE Services.
15. Do one of the following:
- If you are upgrading from 3.1 or 4.0 to 4.1, the upgrade is complete.
  - If you are upgrading from 3.0 to 4.0 or 4.1, continue with Restoring the synchronized LDAP and Postgres database section below.

### Restoring the synchronized LDAP and Postgres database

If you are upgrading from AE Services 3.0, restore a synchronized LDAP and Postgres database:

1. Log in to the AE Services server as `craft` and `su` to `root` (use the command `su - root`).
2. Copy the saved tar file to `/var/lib/ldap`.
3. From the command line, execute the following commands:

```
cd /var/lib/ldap
tar -xvf tar_file_name.tar
rm tar_file_name.tar
service ldap restart
```

---

### Performing the upgrade from an ISO image

To upgrade the software from an ISO image:

1. Log in to the server as `craft` and `su` to `root` (use the command `su - root`).
2. Download the AE Services 4.0 ISO image.
3. Using the following command, mount the ISO image:

```
mount -o loop bundled-xxx.iso /mnt/cdrom
```

Where `xxx` = the AE Services Bundled Build version.

4. From the command line, launch the upgrade script:

```
upgrade -d
```


The upgrade process starts.

Various prompts appear (for example, to stop services or upgrade).

5. Select **yes** for all prompts.

The upgrade process continues on the offline (inactive) partition of the Bundled Server, and the server reboots.

6. Log in to the server again as `craft` and `su` to `root` (use the command `su - root`)
7. Manually restore the AES 4.0 database using the Maintenance > Restore Database option in the OAM interface. For detailed description of how to restore the database, refer to Ch. 2 in the *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*.

8. Verify that the upgrade was successful:
  - From the command line run `swversion` and verify that the version number and build number are correct.
  - Validate the configuration data:
    - a. Log in to the AE Services OAM.  
For more information, see step 1 in [Before you begin](#) on page 45.
    - b. Select **CTI OAM Admin > Administration**.
    - c. Check all of the OAM pages listed under **Administration** on the Administration page. Verify that the information is complete and correct.
9. Verify the local IP settings. If they are different from the pre-upgrade settings, change them back to those settings.
10. Perform the appropriate step:
  - If the upgrade was *not* successful, do not continue with these steps. Instead, reboot into the original active partition to roll back to the original 3.x software release and configuration.
  - If the upgrade was successful, continue.
11. Upgrade the SAMP firmware
  - a. Retrieve the SAMP R2 or later firmware from support.avaya.com.
  - b. Run `sampupdate` to update the SAMP firmware to R2.
    - `sampupdate /tmp/xxx.tbz`  
where `xxx.tbz` is the downloaded SAMP firmware file.
12. Make the upgrade permanent:  
`upgrade -p`  
 **Important:**  
If you do not make the upgrade permanent, on the next reboot, the server will revert to the previous release of AE Services.
13. Do one of the following:
  - If you are upgrading from 3.1 or 4.0 to 4.1, the upgrade is complete.
  - If you are upgrading from 3.0 to 4.0 or 4.1, continue with Restoring the synchronized LDAP and Postgres database section below.

## Restoring the synchronized LDAP and Postgres database

If you are upgrading from AE Services 3.0, restore a synchronized LDAP and Postgres database:

1. Log in to the AE Services server as `craft` and `su` to `root` (use the command `su - root`).
2. Copy the saved tar file to `/var/lib/ldap`.
3. From the command line, execute the following commands:

```
cd /var/lib/ldap
tar -xvf tar_file_name.tar
rm tar_file_name.tar
service ldap restart
```

---

## Installing a new license

If you upgraded from AE Services 3.x, you should install your new license now. See [Chapter 4: Installing licenses](#) for information about installing licenses.

Whenever you install a new license, you must restart AE Services to get the new capabilities.

1. Log in to the AE Services OAM.
2. **CTI OAM Admin > Maintenance > Service Controller > Restart AE Server**

---

## Updating the software

Avaya provides updates and patches for updating the software.

- An update provides new features or enhancements to the AE Services platform. An update may also include bug fixes. Updates are released only on an as-needed basis for critical fixes. Avaya tests updates before releasing them.
- A patch addresses a specific issue to a specific component or a set of components in the AE Services platform. We do not test patches before releasing them.
- The install script installs the new version of the RPMs in `/var/disk/software`.

**Note:**

`/var/disk/software` also contains all of the previous versions of the RPMs.

- The update script backs up the current version before installing the new version of the RPM.

The next two sections explain how to install or uninstall updates or patches on an AE Services server.

---

## Installing updates and patches

Updates and/or patches are organized as ZIP files of RPMs. Multiple updates or patches can be applied to the system.

 **Important:**

Always use *this* procedure, *not* an RPM command, to install AE Services updates or patches.

You should check the Avaya DevConnect site ([www.devconnectprogram.com](http://www.devconnectprogram.com)) or the Avaya support site ([support.avaya.com](http://support.avaya.com)) periodically to see if there is a new patch. If there is, install the new updates and/or patches:

**Note:**

You should always perform a backup of the database before installing an update.

## Upgrading and updating the AE Services software

To install an update or a patch:

1. Log in to the AE Services server as **craft** and **su** to root (use the command **su - sroot**)
2. Download any new patches (*xxxx.zip*) to the current directory.
3. From the command line, enter **update -u *xxxx.zip***

The update/patch ID and the RPMs contained in the package are displayed and the system prompts you to confirm the installation of the RPMs.

- If you enter **y**, the installation of the updates/patches proceeds:
  - AE Services, Tomcat service, and DBService are stopped.
  - RPMs contained in the package are installed.
  - AE Services, Tomcat service, and DBService are restarted.
- If you enter **n**, the installation of the updates/patches aborts.

Use **swversion -a** if you want to look at all the updates/patches installed in the system.

---

## Uninstalling updates and patches

### Note:

The directory `/opt/mvap/resources/patch-update` contains the `patchnumber.txt` files. RPMs installed in each update/patch are listed in this `patchnumber.txt` file. Use **swversion** if you want to look at all the updates/patches installed in the system.

To uninstall updates or patches:

1. Log in as **craft** to the server machine where AE Services and patches are already installed.
2. **su** to root (use the command **su - sroot**).
3. Use **swversion -a** to find out the number of the update/patch you want to remove.
4. From the command line, enter: **update -e *patchnumber***.

The screen displays a list of all the RPMs to be uninstalled, and the system prompts you for confirmation before uninstalling these RPMs.

- If you enter **y**, the system uninstalls the updates/patches by performing these tasks:
  - AE Services, Tomcat service, and DBService are stopped.
  - RPMs specified in `patchnumber.txt` are rolled back to the previous version.
  - AE Services, Tomcat service, and DBService are restarted.
- If you enter **n**, the upgrade script exits.

# Appendix A: Running the sample application (Device, Media, and Call Control only)

If you are using the Device, Media, and Call Control capabilities of AE Services, the files for running several sample applications were installed. This section explains how to administer and run one of these sample applications (the Tutorial application) in order to:

- Test connectivity between AE Services and Communication Manager
- Perform the various steps involved in running an application
- Learn which files are involved in running an application
- See some of the capabilities of an AE Services Device, Media, and Call Control application

**Note:**

The Tutorial application is the only application that should be run directly on the AE Services Server. All other applications should be run on another machine.

---

## Before you begin

Before you can run the sample application, you must:

- [Administer AE Services for the sample application](#)
- [Administer Communication Manager for the sample application](#)
- [Edit the tutorial properties file](#)

You will need to know the dial plan and which Communication Manager extensions are available.

---

## The sample application files

The following sample application and sample application-related files are included on the AE Services server:

- The application properties file for the sample application (the tutorial properties file)  
`/opt/mvap/cmapi/cmapijava-sdk/examples/resources/tutorial.properties`

## Running the sample application (Device, Media, and Call Control only)

- The sample application media files  
/opt/mvap/cmapi/cmapijava-sdk/examples/media/0001.wav  
/opt/mvap/cmapi/cmapijava-sdk/examples/media/0002.wav  
/opt/mvap/cmapi/cmapijava-sdk/examples/media/0003.wav  
/opt/mvap/cmapi/cmapijava-sdk/examples/media/0004.wav
- A README file containing a description of how to set up and run the sample application.  
/opt/mvap/cmapi/cmapijava-sdk/examples/bin/README.txt

These files are referred to throughout the following procedures.

---

## Administer AE Services for the sample application

1. Ensure that you have specified the same directory for these fields on the OA&M Media Properties screen:
  - **Player Directory**
  - **Recorder Directory**

**Note:**

The default value for both fields is /tmp.

2. Copy the application media files (listed in [The sample application files](#) on page 55) into the directory you have specified for **Player Directory** and **Recorder Directory**.

---

## Administer Communication Manager for the sample application

To run the sample application, you must administer the following on Communication Manager:

- Administer a station to use with the application
- (If needed) Administer out-of-band digit detection
- (If not already configured) Configure network region and gateway configuration



---

## Administer a station

Use the Communication Manager **add station** command to add a station.

For instructions on adding a station (including an example screen for AE Services), see “Adding stations for the API application” in Chapter 1, “Administering Communication Manager for AE Services” in *Application Enablement Services 3.0 Administration and Maintenance Guide*.

For a screen reference, see “Station” in the “Screen Reference” chapter of the *Administrator Guide for Avaya Communication Manager*, 03-300509 (For Communication Manager 3.0).

---

## Administer network region/gateway configuration (if needed)

See the section “Setting up a network region for Device, Media, and Call Control” and “Adding a media gateway to the network,” in Chapter 1, “Administering Communication Manager for AE Services” in *Application Enablement Services 3.0 Administration and Maintenance Guide*.

---

## Edit the tutorial properties file

Before you can run the sample application, you must edit the tutorial properties file (tutorial.properties) to provide information specific to your configuration.

To edit the tutorial properties file:

1. Open tutorial.properties:

```
/opt/mvap/cmapi/cmapijava-sdk/examples/resources/tutorial.properties
```

This is the text of tutorial.properties:

```
IP address of Communication Manager (CLAN)
callserver=nnn.nnn.nnn.nnn
extension=nnnn
password=nnnn
codec choices: g711U, g711A, g729, g729A
codec=g711U
encryption choices: aes, none
encryption=none
IP address of AE Server
cmapi1.server_ip=nnn.nnn.nnn.nnn
cmapi1.username=<user_id>
cmapi1.password=<user_password>
Port for client to connect to AE Server
cmapi1.server_port=4722
Port 4722 is encrypted
cmapi1.secure=true
#cmapi.trust_store_location=sdk/build/mv sdk/cmapijava-sdk/examples/resources/avaya.jks
```

## Running the sample application (Device, Media, and Call Control only)

2. Replace the n's with the following values, using the text editor of your choice:
  - a. For `callserver`, enter the IP address of the media server for Communication Manager, either.
    - (with an S8300 media server) The IP address of the media server
    - or
    - (with any other media server) The IP address of the C-LAN
  - b. For `extension`, enter the extension number of the station that you administered for this application. See [Administer a station](#) on page 57.
  - c. For `password`, enter the security code you administered for that station. See [Administer a station](#) on page 57
3. Save and close `tutorial.properties`.

---

## Running the sample application

### Note:

The AE Services server must be running before you can run an application.

To run the sample application:

1. `ssh` into the AE Services server.
2. On the AE Services server change to the directory where the demonstration application run script resides:

```
cd /opt/mvap/cmapi/cmapijava-sdk/examples/bin
```

3. Run **Ant** on the tutorial application:

```
/opt/mvap/cmapi/cmapijava-sdk/examples/bin/ant.sh runTutorial
(./ant.sh runTutorial)
```

The application starts running. This application acts as a softphone and waits for calls. When the extension is called from any other phone, it answers with a recorded greeting that prompts you to record a message.

4. You can experiment with this application:
  - a. Call the extension and listen to the recorded greeting.
  - b. Follow the prompts to record a message and have it played back to you.

**Note:**

The sample application can only play the last recorded message on a given call. If you make a new call, you will not hear a recording from a previous call. All the recorded files are saved in the directory you have specified in the OAM as the location of the recorded files.

**Note:**

There are also other sample applications installed with the server. After you have checked the AES server/Communication Manager connectivity by running this application, you may want to run those applications from an application machine.

## Troubleshooting the sample application

If the application does not run or does not run as expected:

- Check the log files on the server in /opt/mvap/logs:
  - mvap-trace.log.x
  - mvap-error.log.x
  - mvap-api.log.x
  - mvap-wrapper.log

The best log file to check for Exceptions when troubleshooting is the mvap-error.log.0 file (The.0 file is the latest log file).

- Check for application error messages:

| Application error message:                                             | Troubleshooting procedure                                                                                                                  |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Registration failed because Gatekeeper Reject reason: terminalExcluded | Ensure that the extension number in tutorial.properties corresponds to a correctly administered extension number in Communication Manager. |
| Registration failed because Gatekeeper Reject reason: securityDenial   | Verify that the password in tutorial.properties matches the password administered in Communication Manager for the station.                |

## Running the sample application (Device, Media, and Call Control only)

| Application error message:                                                     | Troubleshooting procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registration failed because Protocol Timeout: reason: GRQ timer, tried 3 times | Verify that the IP address in tutorial.properties for the call server (media server) is correct. Ensure that you can <b>ping</b> the media server from the AE Services server.                                                                                                                                                                                                                                                                                                                                                    |
| Connection refused                                                             | <ul style="list-style-type: none"><li>● Check the tutorial.properties file to make sure that the IP address of the AE Services server is correct.</li><li>● Check for network problems between the application machine and the AE Services server. One way to check this is to ping the AE Services server from the application server.</li><li>● Check the /etc/hosts files to verify that you have included a line that explicitly lists the IP address of the AE Services server, in addition to the localhost line.</li></ul> |

For information about creating and deploying Device, Media, and Call Control applications for AE Services, see the following books:

- *Application Enablement Services Device, Media, and Call Control Java Programmer Guide* (02-300359)
- *Application Enablement Services Device, Media, and Call Control Java Programmer Reference (Javadoc)*
- *Application Enablement Services Device, Media, and Call Control XML Programmer Guide* (02-300358)
- *Application Enablement Services Device, Media, and Call Control XML Programmer Reference (XMLdoc)*

# Appendix B: Linux commands for the AE Services Bundled Server

This section lists the Linux commands for use when installing or upgrading the AE Services server.

---

## Server commands

### **ssh**

Telnet has been disabled on the bundled server for both incoming and outgoing connections. Use **ssh** instead. If you are using a Windows machine to connect to the server, use an **ssh** client like **putty** to connect.

### **scp and sftp**

Use these commands to copy files to and from the bundled server.

### **swversion**

Located at: `/opt/mvap/bin`

There are two versions of this command.

**swversion** lists the following:

- Offer type
- Server type
- Software version number
- Operating system (kernel) version

**swversion -a** lists the following:

- Offer type
- Server type
- Software version number
- Operating system (kernel) version
- List of AE Services RPMs
- List of third-party RPMs

### netconfig

Located at: /opt/mvap/bin

Allows you to set the following:

- Host name
- Domain name
- Domain name server
- IP address and network mask for eth0
- IP address and network mask for eth1
- Default Gateway IP address

### tethereal

Located at: /usr/sbin/

This tool is a sniffer that allows you to sniff packets on the network. **tethereal** is very useful for debugging network traffic.

Example **tethereal** command lines:

```
tethereal -i eth0 -V -x > /tmp/sniff.out
```

Sniffs packets on eth0 NIC in verbose mode and also dumps all the raw bytes into /tmp/sniff.out

```
tethereal -i eth1 -V -x "-R ip.addr==136.1.1.1" > /tmp/sniff.out
```

Sniffs packets to/from IP address **136.1.1.1** on eth1 NIC in verbose mode and dumps all the raw bytes into /tmp/sniff.out

```
tethereal -i lo -V -x "-R (ip.addr==136.1.1.1) && (udp.port==6661 || tcp.port==7772) > /tmp/sniff.out":
```

Sniffs packets to/from IP address **136.1.1.1** and udp port 6661 OR tcp port 7772 on NIC lo (loopback) in verbose mode and dumps all the raw bytes into /tmp/sniff.out

### dateconfig

Located at: /opt/mvap/bin

Allows you to set the following:

- Date
- Time
- Time zone
- NTP server IP address

## ethtool

Allows you to query or change the settings of an Ethernet device (a network interface device, sometimes referred to as the NIC, or Network Interface Card). Use `ethtool` to view or change the settings of the network interfaces on the AE Server. When you use `ethtool` to change the network interface settings, the changed settings will not persist after rebooting the AE Server. To make network interface settings permanent, you will need to edit an AE Services script file.

For information about which script file to edit, see [Changing NIC configurations](#) on page 71.

The following list provides a few usage examples for AE Services.

- `ethtool eth0 (`  
Displays the settings of the eth0 network interface
- `ethtool -s eth0 autoneg off`  
.Turns off auto-negotiation of the eth0 network interface. When you want to change the settings of a network interface, such as the network speed or the duplex mode, you must turn off auto-negotiation first.
- `ethtool -s eth1 speed 100`  
Sets the network speed of the eth1 network interface to 100 Mbs. This is the required speed for AE Services.
- `ethtool -s eth1 duplex full`  
Sets the duplex mode to full on the eth1 network interface. This is the required duplex mode for AE Services.
- `ethtool -s eth1 speed 100 duplex full`  
Sets the network speed and duplex mode on eth1 with a single command entry.

**Note:**

For more information about `ethtool` command syntax, see the Linux manual page for `ethtool`.

## service DBService start/stop/restart/status

Avaya technicians can start/stop/restart DBService by logging in as `craft` or `inads` and then:

- `sudo service DBService start`
- `sudo service DBService stop`
- `sudo service DBService restart`
- `sudo service DBService status`

### **service mvap start/stop/restart/status**

Avaya technicians can start/stop/restart the AE Services server by logging in as **craft** or **inads** and then:

- `sudo service mvap start`
- `sudo service mvap stop`
- `sudo service mvap restart`
- `sudo service mvap status`

### **service tomcat5 start/stop/restart**

Avaya technicians can start/stop/restart Tomcat5 by logging in as **craft** or **inads** and then:

- `sudo service mvap start`
- `sudo service mvap stop`
- `sudo service mvap restart`
- `sudo service mvap status`

### **boostprio**

Located at: `/opt/mvap/bin`

Boosts the priority of a shell so that technicians can run a high-priority program.

This tool is used mostly for debugging purposes, especially to see Linux `top` output, for example, CPU usage or memory usage.

#### **Note:**

Use this tool with great care, as any program that runs on this shell has higher priority than AE Services.

To run this tool:

1. run `boostprio $$ 99`

A new shell opens.

2. From this shell, enter your command (for example, `top d 1 b | tee /tmp/top.out`)
3. When you are done debugging, exit the shell by typing: `exit`

### **route**

Allows the user to administer static routes

To use this command, log in as `sroot`, (`sroot/init`) and use the Linux `route` command to view/configure IP routes. For the different options of the `route` command, see a Linux



## **shutdown -r now**

Reboots the bundled server

## **df**

Checks the disk capacities and partitions

## **makecert.sh**

Located at /usr/share/tomcat5/bin

Allows the user to create a unique SSL keystore for this installation's Apache Tomcat server

### **Note:**

This is an interactive tool.

Located at /usr/share/tomcat5/bin

## **uname**

**uname -n** returns the identity or hostname of the AE Services server. This is the hostname that should be entered on the IP-Services Form AE Services Administration Page.

---

## **RMB commands**

### **rmbuseradd**

Adds an RMB user.

### **rmbuserdel**

Deletes an RMB user.

### **rmbpasswd**

Administers an RMB password.

### **rmbusermod**

Modifies an RMB user.

## SAMP commands

### **samp\_ppp**

Configures the PPP IP address of the modem (local and remote) on the SAMP card.

1. Log into the x306 as **craft**.
2. Enter this command:

```
samp_ppp xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
```

where:

- **xxx.xxx.xxx.xxx** = the local PPP IP address of the SAMP
- **yyy.yyy.yyy.yyy** = the remote PPP IP address of the client connecting to the SAMP through the modem

Both IP addresses are obtained through the Automatic Registration Tool (ART).

### **sampinfo**

This tool provides version information apart from other information about the SAMP card.

1. Log into the x306 as **craft**.
2. Enter: **sampinfo**.

The Product Version fields indicate the versions of the SAMP kernel and INP firmware.

**Note:**

sampinfo is not available on the x306m.

### **sampupdate**

Updates the SAMP firmware. To run this tool:

1. Log into the x306 as **craft**.
2. **cd /tmp**
3. Using **sftp**, download the SAMP firmware (**xxx.tbz**) file:

```
sampupdate /tmp/xxx.tbz
```

where **xxx.tbz** is the downloaded SAMP firmware file.

If the password has changed in the firmware, the system prompts you for the SAMP **craft** password.

4. If prompted for the password, enter the SAMP craft password, **craft01**.

If the update is successful, the system will prompt:

```
Commit this software <Y/N>?
```

5. Answer Y.

## **sampxmlupdate**

This tool provides the latest configuration XML file resident on the SAMP and allows you to write a given configuration XML file onto the SAMP.

1. Log into the x306 as **craft**.

2. Use the **sampxmlupdate** command line appropriate to your task:

- To push a new SAMP configuration XML file onto the SAMP, download the latest configuration file and enter:

```
sampxmlupdate -l avaya.xml
```

where **avaya.xml** is the SAMP configuration XML file that needs to be applied to the SAMP card.

- To get the latest SAMP configuration XML file resident on the SAMP, enter:

```
sampxmlupdate -d samp.xml
```

where **samp.xml** is the configuration XML file being used by the SAMP card.

### **Note:**

If the system prompts you for the SAMP craft password, enter **craft01**. This password is different from the craft password of the host processor (x306).



# Appendix C: AE Services WAN requirements

The WAN requirements changed in AE Services 3.1.

This section details the requirements for the customer's network to support CTI links over a WAN/VLAN/LAN. These are links, connected via a WAN/VLAN/LAN, between the AE Services server machine and the C-LAN(s) in a Communication Manager (CM).

- No more than a 200ms average round trip packet delivery time as measured with `ping` over every one-hour time period
- Periodic spiked delays of no more than two seconds while maintaining the 200ms average round trip delivery time as measured with `ping` over every one-hour time period

These requirements are to maintain the CTI link over a WAN/VLAN/LAN. If the implementation is going to issue route requests, then the associated "wait" step must always have a value greater than the largest "periodic spiked delay". With a maximum of 2 seconds allowed (as stated above) your wait step should be greater than 2 seconds. If you can guarantee "periodic spiked delays" less than 2 seconds, then you can reduce the wait step time-out accordingly. If no response to a route select is received by the switch, the call will follow the remaining vector steps in this specific vector. In other words, you will program the vector to deal with this condition.

If you cannot guarantee "periodic spiked delays" of less than two seconds, then it is important to note the following condition:

If you are using AE Services 3.1/4.0 and encounter "periodic spiked delays" greater than two seconds, then messages will either be:

- Stored and retransmitted after recovering from a short network outage
- or
- Dropped during a long network outage



## Appendix D: Changing NIC configurations

The AE Services Bundled server defaults to network auto-negotiation. This means that a far end node could auto-negotiate a session that sets the AE Server's network interface with speed and duplex settings that are not recommended for AE Services, such as 1000BaseT, 10BaseT, or 100BaseT half duplex.

To prevent this from happening, the installation technician can change the NIC configuration. The recommended procedure is to use the OAM.

---

### Changing NIC configuration from the OAM

**CTI OAM > Administration > Network Configuration > NIC Configuration**

For more information about configuring the NICs, see the section "NIC Configuration," in Chapter 2, "AE Services OAM Administration and CTI OAM Administration" in *Application Enablement Services 3.0 Administration and Maintenance Guide*.

---

### Editing network scripts to change NIC configurations

If a browser is not available, the installation technician can make changes to AE Services script files. See the following sections, based on the release you are using.

- [Editing the network scripts for releases 3.0 and 3.1.0](#) on page 71
- [Editing the mvap script for releases 3.1.1, 3.1.2, and 4.0](#) on page 72

---

### Editing the network scripts for releases 3.0 and 3.1.0

Change the network script files, ifcfg-eth0 and ifcfg-eth1, which are located in /etc/sysconfig/network-scripts.

1. Edit the ifcfg-eth0 file by adding the two lines shown in boldface. Save your changes.

```

USERCTL=yes
DEVICE=eth0
BOOTPROTO=static
.
.
.

```

## Changing NIC configurations

```
ONBOOT=yes
TYPE=ethernet
ETHTOOL_OPTS="speed 100 duplex full autoneg off"
```

2. Edit the ifcfg-eth1 file by adding the two lines shown in boldface. Save your changes.

```
USERCTL=yes
DEVICE=eth1
BOOTPROTO=static
.
.
.
ONBOOT=yes
TYPE=ethernet
ETHTOOL_OPTS="speed 100 duplex full autoneg off"
```

3. Edit the /etc/rc.local file by adding the following lines. Save your changes.

```
ethtool -s eth0 "speed 100 duplex full autoneg off"
ethtool -s eth1 "speed 100 duplex full autoneg off"
```

4. Reboot the AE Server.

These changes are permanent. They will persist through subsequent reboots of the AE Server.

---

## Editing the mvap script for releases 3.1.1, 3.1.2, and 4.0

Edit the mvap script file (/etc/init.d directory/mvap) to set both eth0 and eth1 to 100BaseT full duplex:

1. Search for the following text in the mvap script file.

```
To hardcode the eth0 eth1 to 100Mb/s speed and
duplex, please remove the # character at front
of below lines.
```

```
set_eth_full100
```

2. Remove the # character from the line that specifies the Ethernet setting. That is, change this:

```
set_eth_full100
```

to this:

```
set_eth_full100
```

3. Save your changes.
4. Reboot the AE Server.

These changes are permanent. They will persist through subsequent reboots of the AE Server.



# Appendix E: Multiple upgrade considerations

For the AES 4.0 release a new feature was added to the upgrade process. A repository containing the last 3 Install/Upgrades are stored on the server. The initial install is stored in slot 1 and the next 2 upgrades are stored in slots 2 and 3. If an additional upgrade is attempted the upgrade process will fail with the following error.

```
14:24:07 | STEP 1 :
14:24:07 | Building Repository....
14:24:07 | Error: repository already contains maximum of three releases
14:24:07 | clean up repository before continuing
14:24:07 |
14:24:07 | UPDATE-ERROR update exited abnormally at Tue Nov 14 14:24:07 MST 2006
There was an error during upgrade
Exiting.....
Unmounting ISO from /mnt/cdrom
```

Two commands are available to solve this problem.

**upgrade -l** lists all the stored ISO images in the repository.

For example:

```
upgrade -l
```

Output:

```
r4-0-bld-34-0
r4-0-bld-35-0
r4-0-bld-36-2-0
```

**upgrade -e *isoname*** removes the specified ISO image from the repository.

For example:

```
upgrade -e r4-0-bld-34-0
```

```
upgrade -l
```

Output:

```
r4-0-bld-35-0
r4-0-bld-36-2-0
```

Now you can perform another upgrade.

## Multiple upgrade considerations

# Index

## A

- administering
  - CT users . . . . . [38](#)
  - H.323 Gatekeepers . . . . . [39](#)
  - links . . . . . [39](#)
  - Security Database settings . . . . . [39](#)
  - transport link connectivity . . . . . [39](#)
- administration procedures
  - AE Services . . . . . [38](#), [39](#)
  - Communication Manager . . . . . [37](#)
- application link encryption, checking . . . . . [39](#)
- application machine requirements. . . . . [7](#)
- application properties file for sample application . . . . . [55](#)

## B

- Bundled Server box
  - x306 . . . . . [11](#)
  - x306m . . . . . [11](#)

## C

- checking application link encryption . . . . . [39](#)
- CIRS
  - see Customer Infrastructure Readiness Survey
- commands
  - Linux. . . . . [61](#)
  - RMB . . . . . [65](#)
  - SAMP . . . . . [66](#)
- Communication Manager administration
  - adding stations . . . . . [38](#)
  - checking for appropriate VOIP resources. . . . . [38](#)
  - checking for call control features. . . . . [37](#)
  - checking for IP\_API\_A licenses . . . . . [38](#)
  - configuring for signaling and media encryption . . . . . [38](#)
  - setting up transport link . . . . . [37](#)
  - table of tasks . . . . . [37](#)
- connectivity
  - testing
    - OAM tests . . . . . [41](#)
- creating a user account . . . . . [38](#)
- CT users
  - administering . . . . . [38](#)
- Customer Infrastructure Readiness Survey (CIRS)

## D

- disk partitioning. . . . . [31](#)

## E

- encryption
  - application link . . . . . [39](#)

## F

- figures
  - connecting the modem. . . . . [19](#)
  - network interfaces . . . . . [24](#)

## H

- H.323 Gatekeepers
  - administering . . . . . [39](#)

## I

- installation screens
  - Configure Network Information . . . . . [26](#)
  - Date/Time Initialization. . . . . [26](#)
- installing
  - AE Services license file . . . . . [33](#)
  - license file . . . . . [33](#)
  - memory. . . . . [15](#)
  - modem . . . . . [19](#)
  - server . . . . . [15](#)
  - server software . . . . . [21](#)
  - updates and patches . . . . . [53](#)

## L

- license file
  - error messages . . . . . [35](#)
  - installing . . . . . [33](#)
  - requesting . . . . . [35](#)
  - required information . . . . . [35](#)
  - troubleshooting . . . . . [34](#)
- links
  - administering . . . . . [39](#)
- Linux commands . . . . . [61](#)
  - boostprio . . . . . [64](#)
  - dateconfig . . . . . [62](#)
  - df. . . . . [65](#)

## Index

|                                  |                    |
|----------------------------------|--------------------|
| ethtool . . . . .                | <a href="#">63</a> |
| makecert . . . . .               | <a href="#">65</a> |
| netconfig . . . . .              | <a href="#">62</a> |
| route . . . . .                  | <a href="#">64</a> |
| scp . . . . .                    | <a href="#">61</a> |
| sftp . . . . .                   | <a href="#">61</a> |
| shutdown . . . . .               | <a href="#">65</a> |
| ssh . . . . .                    | <a href="#">61</a> |
| swversion . . . . .              | <a href="#">61</a> |
| tethereal . . . . .              | <a href="#">62</a> |
| uname . . . . .                  | <a href="#">65</a> |
| log files                        |                    |
| for sample application . . . . . | <a href="#">59</a> |
| locations . . . . .              | <a href="#">32</a> |

## M

|                                     |                    |
|-------------------------------------|--------------------|
| MAC address for WebLM . . . . .     | <a href="#">36</a> |
| maintaining security . . . . .      | <a href="#">43</a> |
| media files                         |                    |
| sample application . . . . .        | <a href="#">56</a> |
| media server requirements . . . . . | <a href="#">7</a>  |
| memory, installing . . . . .        | <a href="#">15</a> |
| modem                               |                    |
| connect to media server . . . . .   | <a href="#">19</a> |
| connecting . . . . .                | <a href="#">19</a> |

## N

|                                                |                    |
|------------------------------------------------|--------------------|
| network interfaces . . . . .                   | <a href="#">24</a> |
| network requirements for AE Services . . . . . | <a href="#">8</a>  |
| NICs                                           |                    |
| specifying for AE Services . . . . .           | <a href="#">39</a> |

## P

|                                            |                    |
|--------------------------------------------|--------------------|
| packet delivery time . . . . .             | <a href="#">69</a> |
| partitioning the disk . . . . .            | <a href="#">31</a> |
| periodic spiked delays . . . . .           | <a href="#">69</a> |
| Ping Host . . . . .                        | <a href="#">41</a> |
| power cord precautions . . . . .           | <a href="#">12</a> |
| precautions . . . . .                      | <a href="#">12</a> |
| power cord . . . . .                       | <a href="#">12</a> |
| prerequisites                              |                    |
| environmental . . . . .                    | <a href="#">10</a> |
| for server software installation . . . . . | <a href="#">21</a> |
| for technician . . . . .                   | <a href="#">12</a> |
| hardware . . . . .                         | <a href="#">11</a> |
| remote access clients . . . . .            | <a href="#">12</a> |
| software . . . . .                         | <a href="#">11</a> |

## R

|                       |  |
|-----------------------|--|
| remote access clients |  |
|-----------------------|--|

|                                   |                    |
|-----------------------------------|--------------------|
| putty . . . . .                   | <a href="#">12</a> |
| puttytel . . . . .                | <a href="#">12</a> |
| remote configuration              |                    |
| preparing for . . . . .           | <a href="#">28</a> |
| requirements                      |                    |
| application machine . . . . .     | <a href="#">7</a>  |
| Bundled Server hardware . . . . . | <a href="#">11</a> |
| media server . . . . .            | <a href="#">7</a>  |
| network characteristics . . . . . | <a href="#">8</a>  |
| WAN . . . . .                     | <a href="#">69</a> |
| RMB commands                      |                    |
| rmbpasswd . . . . .               | <a href="#">65</a> |
| rmbuseradd . . . . .              | <a href="#">65</a> |
| rmbuserdel . . . . .              | <a href="#">65</a> |
| rmbusermod . . . . .              | <a href="#">65</a> |
| RPMs                              |                    |
| locations . . . . .               | <a href="#">32</a> |

## S

|                                                          |                    |
|----------------------------------------------------------|--------------------|
| SAMP                                                     |                    |
| see Server Availability Management Processor (SAMP) card |                    |
| SAMP commands . . . . .                                  | <a href="#">66</a> |
| samp_ppp . . . . .                                       | <a href="#">66</a> |
| sampinfo . . . . .                                       | <a href="#">66</a> |
| sampupdate . . . . .                                     | <a href="#">66</a> |
| sampxmlupdate . . . . .                                  | <a href="#">67</a> |
| sample application                                       |                    |
| application error messages . . . . .                     | <a href="#">59</a> |
| application properties file . . . . .                    | <a href="#">55</a> |
| log files . . . . .                                      | <a href="#">59</a> |
| media files . . . . .                                    | <a href="#">56</a> |
| running . . . . .                                        | <a href="#">58</a> |
| troubleshooting . . . . .                                | <a href="#">59</a> |
| tutorial properties file . . . . .                       | <a href="#">57</a> |
| security . . . . .                                       | <a href="#">43</a> |
| Security Database settings                               |                    |
| administering . . . . .                                  | <a href="#">39</a> |
| Server Availability Management Processor (SAMP) card     |                    |
| explanation                                              |                    |
| server commands . . . . .                                | <a href="#">61</a> |
| boostprio . . . . .                                      | <a href="#">64</a> |
| dateconfig . . . . .                                     | <a href="#">62</a> |
| df. . . . .                                              | <a href="#">65</a> |
| ethtool . . . . .                                        | <a href="#">63</a> |
| makecert . . . . .                                       | <a href="#">65</a> |
| netconfig . . . . .                                      | <a href="#">62</a> |
| route . . . . .                                          | <a href="#">64</a> |
| scp . . . . .                                            | <a href="#">61</a> |
| service mvap start/stop/restart . . . . .                | <a href="#">62</a> |
| sftp . . . . .                                           | <a href="#">61</a> |
| shutdown . . . . .                                       | <a href="#">65</a> |
| ssh . . . . .                                            | <a href="#">61</a> |
| swversion . . . . .                                      | <a href="#">61</a> |

|                                           |                    |
|-------------------------------------------|--------------------|
| tethered . . . . .                        | <a href="#">62</a> |
| uname . . . . .                           | <a href="#">65</a> |
| server software                           |                    |
| installing . . . . .                      | <a href="#">21</a> |
| server, mounting in rack . . . . .        | <a href="#">15</a> |
| specifying NICs for AE Services . . . . . | <a href="#">39</a> |
| system precautions . . . . .              | <a href="#">12</a> |

|                 |                    |
|-----------------|--------------------|
| x306m . . . . . | <a href="#">11</a> |
|-----------------|--------------------|

---

## T

|                                    |                    |
|------------------------------------|--------------------|
| testing connectivity               |                    |
| OAM tests . . . . .                | <a href="#">41</a> |
| Ping Host . . . . .                | <a href="#">41</a> |
| test phone call . . . . .          | <a href="#">41</a> |
| transport link connectivity        |                    |
| administering . . . . .            | <a href="#">39</a> |
| tutorial properties file           |                    |
| for sample application. . . . .    | <a href="#">57</a> |
| tutorial.properties file . . . . . | <a href="#">57</a> |
| type approval . . . . .            | <a href="#">12</a> |

---

## U

|                                  |                    |
|----------------------------------|--------------------|
| uninstalled memory . . . . .     | <a href="#">15</a> |
| uninstalling                     |                    |
| updates and patches . . . . .    | <a href="#">54</a> |
| Updating AES software. . . . .   | <a href="#">53</a> |
| upgrading                        |                    |
| from a DVD . . . . .             | <a href="#">47</a> |
| from an ISO image . . . . .      | <a href="#">50</a> |
| user account, creating . . . . . | <a href="#">38</a> |

---

## V

|                           |                    |
|---------------------------|--------------------|
| verification application  |                    |
| running. . . . .          | <a href="#">58</a> |
| troubleshooting . . . . . | <a href="#">59</a> |

---

## W

|                           |                    |
|---------------------------|--------------------|
| WAN requirements. . . . . | <a href="#">69</a> |
| WebLM                     |                    |
| error messages. . . . .   | <a href="#">35</a> |
| troubleshooting . . . . . | <a href="#">35</a> |

---

## X

|                                  |                    |
|----------------------------------|--------------------|
| x306 . . . . .                   | <a href="#">11</a> |
| attaching brackets . . . . .     | <a href="#">16</a> |
| attaching to rails . . . . .     | <a href="#">18</a> |
| description . . . . .            | <a href="#">11</a> |
| ports on back. . . . .           | <a href="#">22</a> |
| power cord precautions . . . . . | <a href="#">12</a> |
| SAMP orientation. . . . .        | <a href="#">22</a> |

