Oracle® Communications Application Session Controller

System Installation and Commissioning Guide

Release 3.7.0

May 2016

ORACLE®

Copyright ©2016, 2005, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface 11
About Net-Net OS-E® Documentation.. 11
Revision History 12
Conventions Used in This Manual 15
Typographical Conventions.. 15
Acronyms 15
Net-Net OS-E® Series Overview 21
About this Chapter 21
Net-Net OS-E Overview.. 21
Running the Net-Net OS-E on Other Devices.. 24
Net-Net OS-E 2610 and 2620 Series models 24
Information on Net-Net OS-E Software and Licensing 26
Obtaining Your License 27
Adding New Features Later 28
License Expirations and Renewals 28
Interoperating With SIP Vendors.. 28
System Management.. 28
For More Information 29
Installing and Upgrading Release 3.7.0M4 29
Downloading the OS-E ISO File 29
Installing the Net-Net OS-E System.. 33
About This Chapter.. 33

Net-Net OS-E Series Models 33
Net-Net OS-E Series specification 36
NN2610 Specifications 36
NN 2620 Specifications 37
System and Network Connections 38
VGA Video, System Keyboard, and Power 38
RS-232 Serial B Port, DB9-to-RJ45 Adapter, and Null Modem Cable 38
Gigabit Ethernet (IEEE 802.3ab, 1000Base-TX) 39
USB 2.0 Port.. 40
System Software and Licensing 41
System Components 41
Intel® SE7520JR2 Server Board.. 41
System Fans and Cooling 42
Power Modules.. 43
Hard Disk Drives.. 44
Removable Bezel 45
System Control Panel... 45
Push buttons and LEDs.. 45
Installing the NN 2610 and 2620 Series 48
Required Tools... 48
Unpacking the System.. 48
Installing and Removing the Front Bezel.. 49
Mounting the System In a Rack 51
Connecting Console Equipment... 51
Using the Serial B Console Port 52
Using the Video and Keyboard Connections.. 54
Connecting the Ethernet Interfaces.. 55
NN 2620 Half- and Full-Height Slots 58
Ethernet Port Assignments... 59
Moving NICs After Installation 59
Connecting AC Power 59
AC Power Requirements 59

Connecting the AC Power Source 60

Inserting the USB Stick 61

Applying Power 62

Checking the LEDs 63

Logging On and Starting the CLI 65

Assigning a Management IP Address 65

Using the Setup Script 66

Enabling Network Access 67

Defining a Default Route and Gateway IP 68

Cluster Installation 68

Quick Commissioning New OS-E Systems 69

About This Chapter 69

Prerequisites to Quick Commissioning 69

Building the Configuration File 70

Basic Network Topology 71

Step 1. Configuring Basic IP Connectivity 72

Using the Setup Script 73

Enabling Network Access 74

Defining a Default Route and Gateway IP 74

Launching the OS-E Management System 74

Changing the Linux Root Password 75

Step 2. Configuring Advanced IP Connectivity 76

Step 3. Creating User Accounts for Basic Access 78

Step 4. Enabling Master Services 80

Step 5. Configuring Basic Services 81

Step 6. Enabling the Virtual System Partition (VSP) 83

Step 7. Configuring the Accounting Environments 84

Step 8. Editing the Default Session Configuration 86

Step 9. Enabling Registration Services 87

Step 10. Reviewing the Configuration 88

Installing Net-Net OS-E Clusters 91
About This Chapter 91
Net-Net OS-E Cluster Overview 91
Cluster Operations and Services 92
Master-Services.. 92
Heartbeat Interface, BOOTP, and Messaging 97
Event Logging.. 97
Network Time Protocol (NTP).. 98
Cluster Redundancy Operations 98
Notes on Cluster Management... 98
Cluster Installation Prerequisites 99
Cluster Installation Procedure 100
Configuring External Messaging 106
Configuring Cluster Load Balancing.. 107
Restarting an OS-E Cluster... 108

Installing Certificates and Commissioning TLS Networks 111
About This Chapter 111
TLS Overview... 111
Steps to Configuring TLS.. 111
Before Configuring TLS 113
Step 1. Creating a Self-Signed Certificate and Key Pair from the OS-E 114
Step 2. Generating a Certification Signing Request (CSR) 118
Step 3. Signing a CSR Using Either a Valid CA or OpenSSL.................... 120
Step 4. Updating the Self-Signed Certificate 131
Subject Alternative Name for HTTPS Certificates Support 132
Configuring the Certificate on the Net-Net OS-E... 135
Displaying the Certificates Installed on the OS-E...................................... 135
Other TLS Certificate Settings.. 135
Using Certificate vs. Default-Outgoing-Settings 135
Verifying Peer Certificates 136
Enabling Peer Certificate Verification 137

Controlling the CA Files and CRLs to Apply to the Certificate 138
Setting the Required Peer Name.. 138
Configuring TLS on Ethernet Interfaces 138

Configuring Secure Media (SRTP) Sessions 141

About This Chapter 141
Anchoring Media Sessions.. 141
Configuring Inbound and Outbound Encryption 142
Inbound Encryption Mode and Type.. 143
Outbound Encryption Mode, Type, and Require-TLS Setting 144
Linksys Encryption 145

Performing Maintenance and System Upgrades to the NN2600........... 149

About This Chapter 149
Warnings 149
System Power On/Off.. 149
Hazardous Conditions, Devices and Cables 149
Electrostatic Discharge (ESD) and ESD Protection 150
ESD and Handling Boards... 150
Installing or Removing Jumpers 150
Safety Cautions.. 150
Attaching an ESD Strap.. 155
Installing the Racking Mounting Brackets.. 155
Installing and Removing the Front Bezel.. 156
Removing and Installing the Chassis Cover.. 158
On the NN2610.. 158
On the NN2620.. 160
Replacing a System Fan 162
On NN 2620 systems only 162
Installing or Replacing a Hot-Swap Power Supply 164
On NN2620 Systems Only 164
Installing and Removing a Hard Disk Drive... 165
On NN2610 and NN2620 Systems.. 165

Creating and Commissioning USB Sticks.. 169

Supported USB Sticks 170

USB Stick Restrictions... 170

Running the Boot Media Creator 170

Ensuring the USB Contents For Existing Systems 176

About the New USB Stick — Please Read!.. 176

Accessing License Files 177

Net-Net OS-E Commissioning Steps.. 180

Using the Setup Script... 183

Creating a New USB Rescue Stick 184

Using the Rescue Utility USB... 184

Using the Expert Mode 187

System and Data Drive Locations 188

Installing and Running the OS-E Virtual Machine 189

Server-Based Requirements 189

Linux Installations... 190

Installing the VM... 190

Installing the OS-E on an Oracle Virtual Machine 190

Installing the OS-E On a VMware ESXi... 211

Installing the OS-E As a XEN Virtual Machine 214

Installing the OS-E On KVM 219

Using WinSCP to Transfer the License 220

Configuring the VM.. 222

Using Config Setup.. 222

Sample VM Configuration.. 223

Enabling the OS-E Management System... 230

Bridging to Additional Ethernet Ports 230

Adding an Additional VMnet 230

Editing the VM Configuration File 231

Net-Net OS-E-VM Troubleshooting 232

Installing the VM on Slow Systems 232

Other VM Limitations and Considerations 235
NEBS/ETSI 237
AC Power Cords 237
Safety and EMC Regulatory Compliance (Class A) 238
Product Regulatory Compliance Markings 238
Electromagnetic Compatibility Notices 240
FCC (USA) 240
Industry Canada (ICES-003) 241
Europe (CE Declaration of Conformity) 242
VCCI (Japan) 242
BSMI (Taiwan) 242
Korean RRL Compliance 243

Preface

About Net-Net OS-E® Documentation

The Net-Net OS-E references in this documentation apply to the Net-Net OS-E operating system software that is used for the following Oracle and third-party SBC products:

- Oracle Communications Application Session Controller (ASC)
- Oracle Communications WebRTC Session Controller (WSC)
- Oracle Communications OS-E Session Director (SD) Session Border Controller (SBC)
- Oracle Communications 2600 Session Director (SD) Session Border Controller (SBC)
- Third-party products that license and use Oracle Communications OS-E software on an OEM basis.

Unless otherwise stated, references to Net-Net OS-E in this document apply to all of the Oracle and third-party vendor products that use Net-Net OS-E software.

The following documentation set supports the current release of the OS-E software.

- *Oracle Communications Application Session Controller System and Installation Commissioning Guide*
- *Oracle Communications Application Session Controller System and Installation Commissioning Guide Release 3.7.0M4*
- *Oracle Communications Application Session Controller Management Tools*
- *Oracle Communications Application Session Controller System Administration Guide*

- *Oracle Communications Application Session Controller Session Services Configuration Guide*
- *Oracle Communications Application Session Controller Objects and Properties Reference*
- *Oracle Communications Application Session Controller System Operations and Troubleshooting*
- *Oracle Communications Application Session Controller Release Notes*
- *Oracle Communications Application Session Controller Single Number Reach Application Guide*
- *Oracle Communications Application Session Controller Web Services SOAP REST API*
- *Oracle Communications WebRTC Session Controller Installation Guide*

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
June 28, 2013	Revision 1.00	• GA Release of OS-E 3.7.0 software.
	Revision 1.10	• Adds Chapter 8 USB Installation and Commissioning. • Adds Chapter 9 Installing and Running the Net-Net OS-E Virtual Machine. • Removes inaccurate statement about the RS-232 Serial B port using Telnet, SSH, or using an SNMP application. • Removes inaccurate statement about transcoding not being supported on VMs.

Date	Revision Number	Description
January 2015	1.20	• Removes note incorrectly stating that x86-based servers with AMD processors do not support transcoding. • Replaces the “Running License Fetch” section with “Obtaining Your License”. • Updates the “Adding New Features Later” and “License Expirations and Renewals” sections. • Removes the “Evaluation Systems” section. • Updates all licensing information in the “Creating and Commissioning USB Sticks” chapter. • Removes the “Downloading a License” and “Running the License Fetch Program” sections from the “Installing and Running the OS-E Virtual Machine” chapter. • Adds “Downloading the OS-E ISO File” section to the “Net-Net OS-E Series Overview” chapter.
March 2015	1.21	• Removes deprecated “Additional Information on Net-Net OS-E Licensing” section from “Installing the Net-Net OS-E System” chapter. • Includes list of certified platforms and VM platforms. • Updates VM software requirements. • Updates the “USB Stick Restrictions” section.

Date	Revision Number	Description
July 2015	1.30	• Updates procedures on installing the OS-E on the OVM 3.3.1, VMware ESXi 5.5, XEN 3.4.3, and KVM 1.5.3. • Updates version of OVM certified from 3.2.8 to 3.3.1. • Removes “Installing Software on a Hyper-V Virtual Machine”. • Removes “Installing the VMPlayer Image”. • Adds KVM 1.5.3 to the list of supported platforms. • Removes references to custom-designed media acceleration card. • Adds “Changing the Linux Password” to the “Quick Commissioning New OS-E Systems” chapter. • Removes information regarding adding additional Ethernet interfaces in the “Server-Based Requirements” section of the “Installing and Running the OS-E Virtual Machine” chapter. • Updates the “Using the Rescue Utility USB” section to include a more comprehensive list of servers.
August 2015	1.31	• Updates the “Adding New Features Later” and “Downloading the OS-E ISO File” sections.
May 2016	1.32	• Adds *Oracle Communications Application Session Controller System Installation and Commissioning Guide Release 3.7.0M4* to the 3.7.0 doc set. • Adds “Installing and Upgrading Release 3.7.0M4” section. • Adds “Interoperating With SIP Vendors” section.

Conventions Used in This Manual

Typographical Conventions

Key Convention	Function	Example
key name	Identifies the name of a key to press.	Type **abc**, then press [ENTER]
CTRL+*x*	Indicates a control key combination.	Press CTRL+C
brackets [ ]	Indicates an optional argument.	[*portNumber*]
braces { }	Indicates a required argument with a choice of values; choose one.	{enabled | disabled}
vertical bar |	Separates parameter values. Same as “or.”	{TCP | TLS}
Monospaced bold	In screen displays, indicates user input.	config> **`config vsp`**
Monospaced italic	In screen displays, indicates a variable—generic text for which you supply a value.	`config servers>` **`config lcs`** *`name`*
bold	In text, indicates literal names of commands, actions, objects, or properties.	...set as the secondary directory service (with the **unifier** property)...
bold italic	In text, indicates a variable.	...set the **domain** property of the ***directory*** object.

Acronyms

The OS-E manuals contain the following industry-standard and product-specific acronyms:

AAA	Authentication, authorization, and accounting
ALI	Automatic location identifier
ANI	Automatic number identification
ANSI	American National Standards Institute
AOR	Address of record
API	Application programming interface
ARP	Address Resolution Protocol
AVERT	Anti-virus emergency response team

B2BUA	Back-to-back user agent
BOOTP	Bootstrap Protocol
CA	Certificate authority
CAP	Client application protocol
CBC	Cipher block chaining
CBN	Call back number
CCS	Converged Communication Server
CDR	Call detail record
CIDR	Classless interdomain routing
CLI	Command line interface
CMOS	Comparison mean opinion score
CNAME	Canonical name record
CNI	Calling number identification
CODEC	Compressor/decompressor or coder/decoder
CPE	Customer-premise equipment
CRL	Certificate revocation list
CSR	Certificate signing request
CSTA	Computer-supported telecommunications applications
CSV	Comma-separated values
DDDS	Dynamic delegation discovery system
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DN	Distinguished name
DNIS	Dialed number identification service
DNS	Domain name service
DOS	Denial of service
EIM	Enterprise instant messaging
ESD	Electrostatic discharge
ESGW	Emergency services gateway
ESQK	Emergency services query key
ESRN	Emergency services routing number
FQDN	Fully qualified domain name

GUI	Graphical user interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I2	National Emergency Number Association defined VoIP solution
ICAP	Internet Calendar Access Protocol
ICMP	Internet Control Message Protocol
IM	Instant messaging
IP	Internet Protocol
JDBC	Java database connectivity
JMX	Java management extensions
JRE	Java runtime environment
LATA	Local access and transport area
LCS	Live Communications Server
LCR	Least-cost routing
LDAP	Lightweight Directory Access Protocol
LIS	Location information service
MAC	Media access control
MCS	Multimedia Communications Server
MIB	Management information base
MOS	Mean opinion score
MSAG	Master street address guide
MTU	Maximum transmission unit
NAPTR	Naming authority pointer
NAT	Network address translation
NENA	National Emergency Number Association
NIC	Network interface card
NS	Name server
NSE	Named signaling events
NTLM	NT Lan Manager
NTP	Network Time Protocol
OC	Office Communicator
OCI	Open Client Interface

ODBC	Open database connectivity
OTP	Over temperature protection
OVP	Over voltage protection
PBX	Private branch eXchange
PEM	Privacy-enhanced mail
PERL	Practical Extraction and Reporting Language
PING	Packet internet groper
PKCS#12	Public Key Cryptography Standard #12
PKI	Public Key Infrastructure
PSAP	Public safety answering point
PSCP	PuTTY secure copy
PSTN	Public switched telephone network
QOP	Quality of protection
QOS	Quality of service
RADIUS	Remote Authentication Dial-in User Service
RTC	Real-time collaboration
RTCP	Real-time Control Protocol
RTP	Real-time Transport Protocol
RTT	Round-trip time
SATA	Serial ATA
SCSI	Small computer system interface
SDK	Software development kit
SDP	Session Description Protocol
SFTP	Secure Shell File Transfer Protocol
SIMPLE	SIP Instant Messaging and Presence Leveraging Extension
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol over TLS
SLB	Server load balancing
SMB	Server message block
SNMP	Simple Network Management Protocol
SOA	Server of authority
SOAP	Simple Object Access Protocol

SQL	Structured Query Language
SRTP	Secure Real-time Transport Protocol
SRV	Server resource
SSH	Secure Shell
SSL	Secure socket layer
SSRC	Synchronization source
STUN	Simple Traversal of UDP over NATs
TCP	Transmission Control Protocol
TDM	Time division multiplexing
TGRP	Trunk group
TLS	Transport Layer Security
TOS	Type of service
TTL	Time to live
UPS	Uninterruptable power supply
US	User agent
UAC	User agent client
UAS	User agent server
UDP	User Datagram Protocol
UID	Unique identifier
URI	Uniform resource identifier
URL	Uniform resource locator
UTC	Universal coordinated time
VoIP	Voice over IP
VLAN	Virtual local area network
VPC	VoIP positioning center
VRRP	Virtual Router Redundancy Protocol
VSP	Virtual system partition
VXID	Virtual router interface ID
WAR	Web application resource
WAV	Waveform audio
WM	Windows Messenger
WSDL	Web Services Description Language

XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Chapter 1. Net-Net OS-E® Series Overview

About this Chapter

This chapter provides an overview of the Oracle OS-E® Series hardware and software. In addition to running on Oracle hardware offerings, OS-E software is supported on compatible third-party platforms and blades.

See Chapter 8, Creating and Commissioning USB Sticks for information on the supported third-party devices.

Net-Net OS-E Overview

The OS-E series of enterprise data and service provider systems provide application level security, control, monitoring and interoperability services for applications based on the Session Initiation Protocol (SIP). The OS-E resides at points in the network where administrators define and enforce fine-grained policies on the SIP-based signaling and media traffic.

In Enterprise Deployments

In an enterprise deployment, OS-E systems reside in a corporate “Demilitarized Zone” (DMZ), between the SIP-based business applications and the enterprise boundary, such as,

- SIP-enabled IP telephony
- Session border control, real-time collaboration, multi-media conferencing, SIP trunking, third-party call control

- Multivendor interoperability among hosted SIP applications, such as IBM Sametime and Microsoft Live Communications Server (LCS) and Office Communication Server (IOCS)

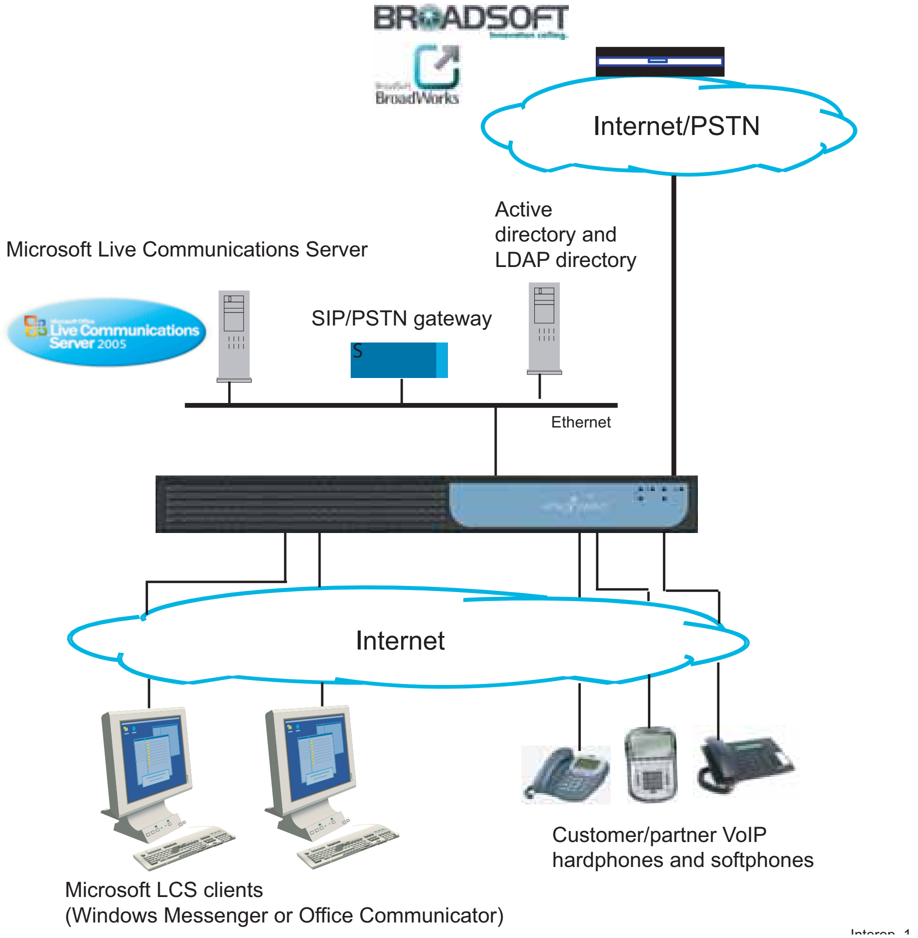
In Service Provider/Carrier Networks

The OS-E provides secure “business class” VoIP and real-time collaboration services for residential, Small and Medium Businesses (SMB), and enterprise subscribers. Service provider deployments include:

- **Subscriber edge**—Where the OS-E terminates secure voice sessions.
- **Customer premises**—Where the OS-E is a managed CPE component for end-to-end VoIP services offered by carriers and service providers.

The OS-E system includes an operating system, application and management software installed on data center and carrier class server systems. The system software includes integrated clustering, synchronization, load balancing, and failover technology that enables enterprises to scale the performance and availability of the system up to carrier class levels simply by adding systems to the cluster.

The following image shows a sample OS-E service provider network


BROADSOFT
BroadWorks
Internet/PSTN
Active directory and LDAP directory
Microsoft Live Communications Server
Live Communications Server 2005
SIP/PSTN gateway
Ethernet
Internet
Customer/partner VoIP hardphones and softphones
Microsoft LCS clients
(Windows Messenger or Office Communicator)
Interop_1

Running the Net-Net OS-E on Other Devices

You can run the OS-E on a number of supported third-party servers.

The following platforms have been certified for use with the OS-E:

- Sun Netra X3-2
- HPDL360 G7
- HPDL585 G7
- HPDL320 G8
- HPDL360 G8
- Cisco C200
- NN2610
- NN2620

The following VM platforms have been certified for use with the OS-E:

- OVM 3.2.8
- VMware ESXi 5.5
- XEN 3.4.3

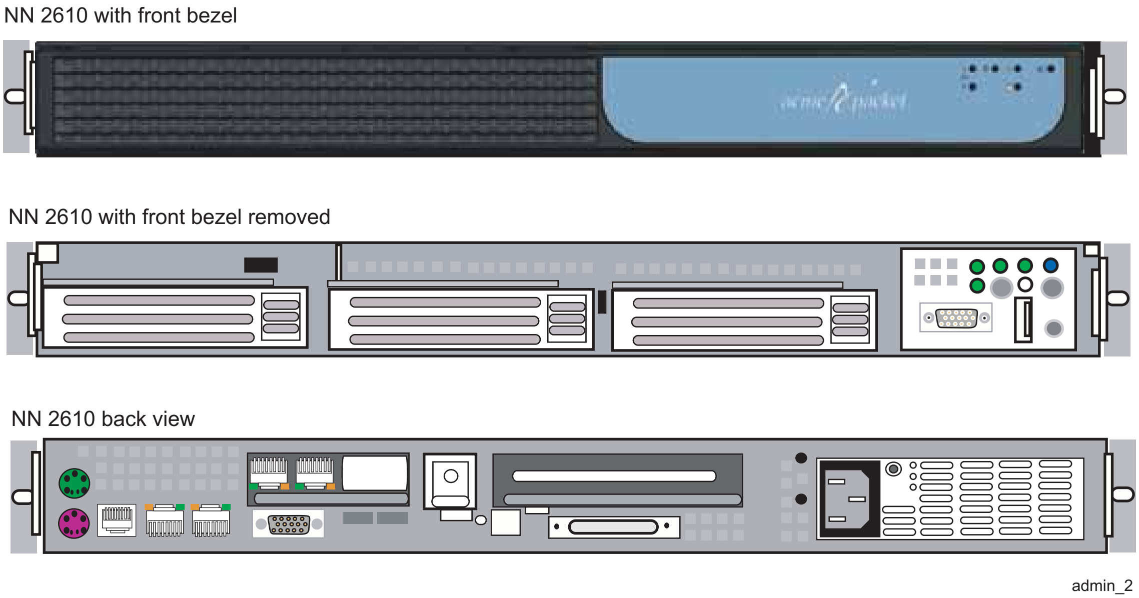
Net-Net OS-E 2610 and 2620 Series models

Oracle supports the Net-Net OS-E NN 2610 and 2620 series systems in the following configurations:

- **NN 2610**— 1U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with non-redundant power supplies and cooling fans; up to six (6) Ethernet ports with optional network interface cards; 750 GB hard disk drive; standard 8GB memory, multiprocessor upgrade option. Commissioned using an Oracle Net-Net OS-E USB stick.

- **NN2620** — 2U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with redundant, hot swappable power supplies and cooling fans; up to eighteen (18) Ethernet ports using a combination of two optional MX-1 media acceleration cards and network interface cards; 750 GB standard hard disk drive, optional 1.5 TB hard disk drive with RAID; standard 8GB memory, multiprocessor upgrade option. Commissioned using an Oracle USB stick

The following image illustrates the NN 2610 series with and without the front bezel installed.

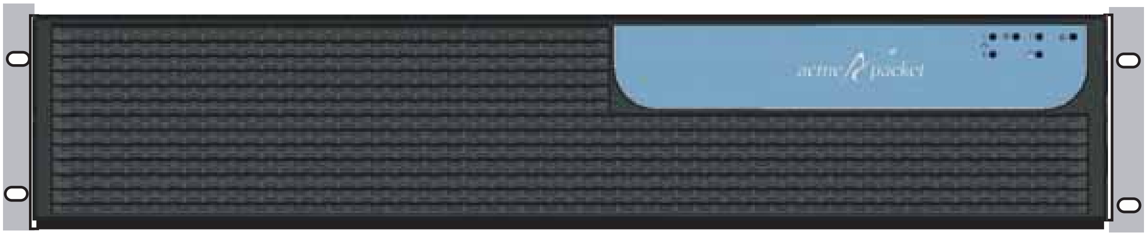

NN 2610 with front bezel

NN 2610 with front bezel removed

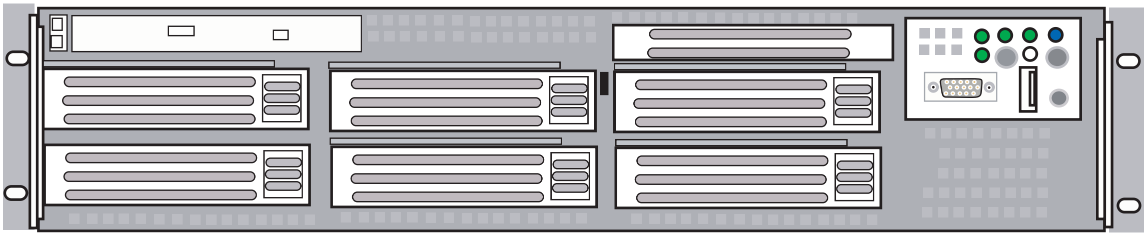
NN 2610 back view

The following image illustrates the NN 2620 (2U) Series chassis.

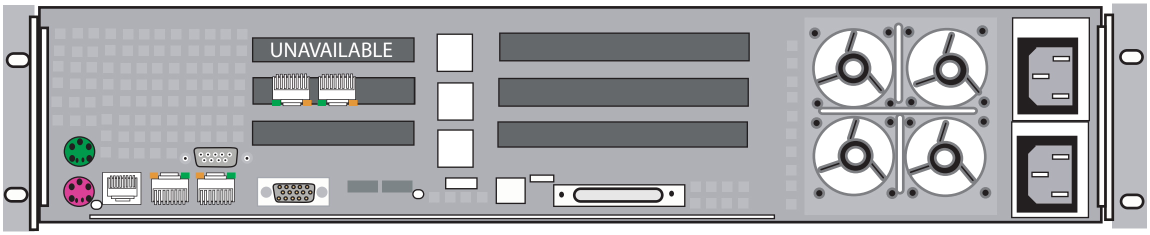
NN 2620 with front bezel



NN 2620 with front bezel removed



NN 2620 back view



Information on Net-Net OS-E Software and Licensing

Using the Internet and secure Web URLs, Oracle provides all necessary software downloads for USB creation, product licensing, and commissioning of your selected hardware.

As part of each download, and depending on your actual requirements, Oracle can provide the following:

- Oracle USB Creation Utility with the OS-E software
- Feature licenses
- Documentation on how to create an Oracle USB stick and commission the OS-E software on your selected hardware
- Standard set of Oracle OS-E technical publications

You must provide a USB stick with 4GB storage to handle Oracle software downloads. Oracle has tested a variety of USB sticks available from current suppliers and manufacturers. Most USB sticks manufactured today will work.

For complete information on accessing the Oracle download server, creating an installation USB stick, and commissioning OS-E systems, refer to Chapter 8, Creating and Commissioning USB Sticks.

Obtaining Your License

If you are running OS-E version 3.7.0M2 or later and are NOT using Royalty-bearing codecs, you should begin using the default shipping license. There is no loss of functionality as a result.

The default license enables the maximum number of sessions for the system. In the past, the software stopped allowing new sessions at your specific licensed maximum depending on the license. The system no longer relies on the license to apply an upper limit. However, depending on the server hardware in use, the system may not be capable of supporting a higher number of sessions. You may want to edit your configuration file and add the parameters for the maximum number of media sessiosn to be sure that you do not exceed the capabilities of your hardware. This applies to most deployments running a small number of sessions on smaller third-party hardware that could potentially have a problem if traffic increases to a number larger than the system can handle.

Note: You may continue using the legacy licensing system or you may transition to self-provisioning entitlements. In both cases, ensure that your system’s functionality abides by your organization’s contractual obligations with Oracle.

Adding New Features Later

If you find that you do not have one or more of the features that you purchased, or if you want to add features that you did not originally purchase, contact your Oracle Sales Representative or Oracle Product Support. Oracle will correct the problem and supply you with a new license key. Upload the license to your OS-E and use the **license apply** action to commit the license.

As Oracle software becomes available with newly-added features, your Oracle Sales Representative will assist you with ordering the software. Oracle will then provide you with a new licensing key.

License Expirations and Renewals

If your customer-specific license comes with an expiration date, the OS-E system will generate an event when the license nears the expiration date. Contact your Oracle Sales Representative to complete the purchase of the features that you are testing. These expiring licenses should apply only to customers testing royalty-bearing codecs in the transcoding feature of the OS-E.

Interoperating With SIP Vendors

OS-E devices are designed to interoperate with SIP servers, hosted SIP applications, and SIP PBX equipment for VoIP applications.

Contact your Oracle sales representative for a complete list of SIP vendors who interoperate with OS-E software.

System Management

Before you install the system, you should decide on the management tool(s) that you want to use to configure and monitor the system. This will help you decide where you need to create connections based on your equipment and network resources.

System management capabilities include the following secure management interfaces:

- The OS-E command line interface (CLI) from a local console, Telnet, or SSH connection

- The OS-E Management System, a graphical user interface (GUI) that supports remote management using the Internet Explorer Web browser
- Simple Network Management Protocol (SNMP) using third party SNMP MIB compiler/browser applications
- Web Services Description Language (WSDL) and Simple Object Access Protocol (SOAP) messaging using the software development kit (SDK)

For information on configuring the management options, refer to Oracle Communications OS-E Management Tools.

For More Information

See Appendix A, “Technical Specifications,” for regulatory information and product data.

Installing and Upgrading Release 3.7.0M4

As of release 3.7.0M4, the OS-E runs on Oracle Linux (version 7.0 and higher) as opposed to its own custom kernel as in prior releases. Because the OS-E runs on Oracle Linux and uses a yum to install and update RPM files, the installation and upgrade process has changed significantly.

Due to this fact, a 3.7.0M4 version of the installation guide has been created. The *Oracle Communications Application Session Controller System Installation and Commissioning Guide Release 3.7.0M4* is now available with the 3.7.0 doc set.

Downloading the OS-E ISO File

Before you can install the OS-E, you must first download the ISO files you need.

Software can be downloaded from either the Oracle Software Delivery Cloud or the My Oracle Support Patches and Updates tab.

To access the Oracle Software Delivery Cloud:

1. Visit the https://edelivery.oracle.com link.
2. Select the **Sign In/Register** tab and enter your **username** and **password**.

Note: If you are a new user, you must create an account.

3. Click the checkbox to agree to the **Oracle Trial License Agreement and Export Restrictions** and click **Continue**.
4. Select the **Oracle Communications** product pack.
5. Select the **Acme Packet OS** platform and click **Go**.
6. Select **Oracle Communications Application Session Controller 3.7** from the list of results and click **Continue**.
7. Download the appropriate software distribution format of OS-E.

   The available formats for that software appear. The following are available OS-E files:

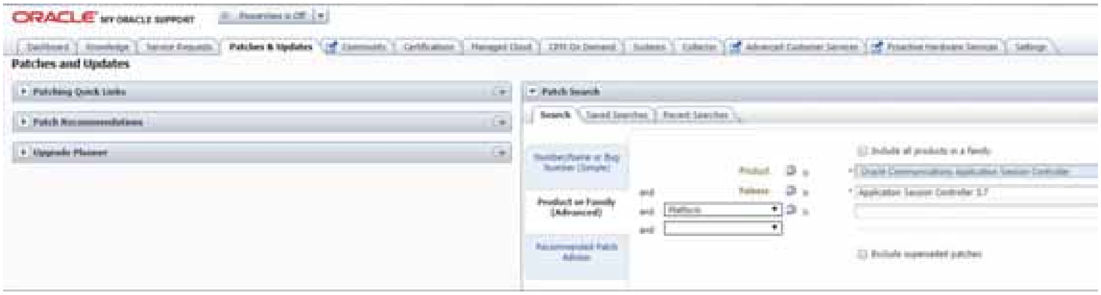
   - Oracle Communications Application Session Controller E3.7.0m*x* Installation Image Supertar
   - Oracle Communications Application Session Controller E3.7.0m*x* Installation USB image
   - Oracle Communications Application Session Controller E3.7.0m*x* Installation ISO image
   - Oracle Communications Application Session Controller E3.7.0m*x* VMWare VMS/VMDK file
   - Oracle Communications Application Session Controller E3.7.0m*x* Xen server image
   - Oracle Communications Application Session Controller E3.7.0m*x* HyperV OVA file
   - Oracle Communications Application Session Controller E3.7.0m*x* LCR Import Tool
   - Oracle Communications Application Session Controller E3.7.0m*x* Embedded LCR Import Tool
   - Oracle Communications Application Session Controller E3.7.0m*x* Samples Kit
   - Oracle Communications Application Session Controller E3.7.0m*x* Archive Viewer Application
   - Oracle Communications Application Session Controller E3.7.0m*x* Weblogic SDK file

- Oracle Communications Application Session Controller E3.7.0m*x* License Document

8. Select the file you need from the list of distribution formats and click **Download**.

To access the Oracle Support Software Patches and Updates:

1. Log into the My Oracle Support Portal.
2. Select the **Patches and Updates** tab.
3. Select the **Search** tab and click **Product or Family (Advanced)**.



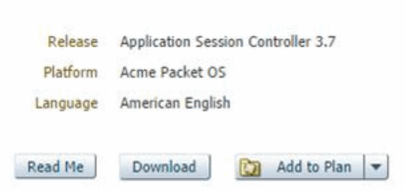
Product: Oracle Communications Application Session Controller

and Release: Application Session Controller 3.7

and Platform

4. **Product:** Enter **Oracle Communications Application Session Controller**.
5. **Release:** Enter **Application Session Controller 3.7**.
6. Click **Search**. The available distribution formats appear and include the following information:
   - Patch Name
   - Description
   - Release
   - Platform (Language)
   - Classification
   - Product
   - Has Prerequisite
   - Size
   - Download Access
7. Select the distribution format that you require.

8. Click either **Download** to download the file or **Read Me** to view the Build Notes for this patch.



Release Application Session Controller 3.7

Platform Acme Packet OS

Language American English

Chapter 2. Installing the Net-Net OS-E System

About This Chapter

This chapter covers OS-E system installation

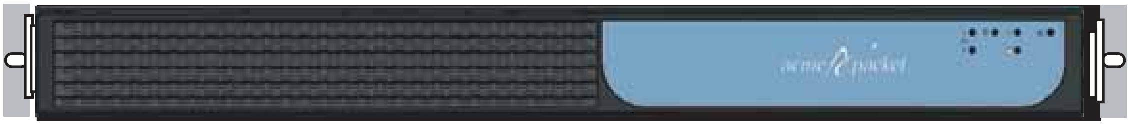
Net-Net OS-E Series Models

Oracle supports the OS-E Series systems in the following configurations:

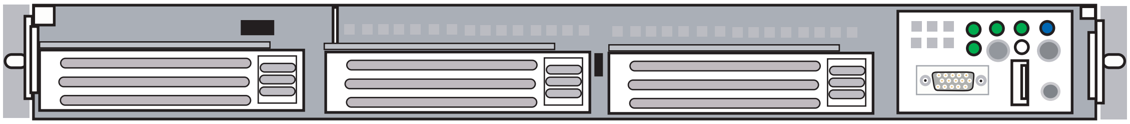
- **NN 2610**— 1U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with non-redundant power supplies and cooling fans; up to six (6) Ethernet ports with optional network interface cards; 750 GB hard disk drive; standard 8GB memory, multiprocessor upgrade option.
- **NN 2620**— 2U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with redundant, hot swappable power supplies and cooling fans; up to eighteen (18) Ethernet ports using a combination of two optional MX-1 media acceleration cards and network interface cards; 750 GB standard hard disk drive, optional 1.5 TB hard disk drive with RAID; standard 8GB memory, multiprocessor upgrade option.

The following image illustrates the NN 2610 series with and without the front bezel installed.

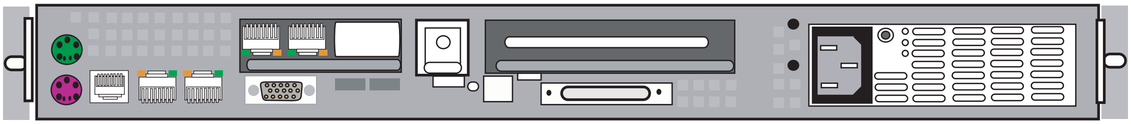
NN 2610 with front bezel



NN 2610 with front bezel removed

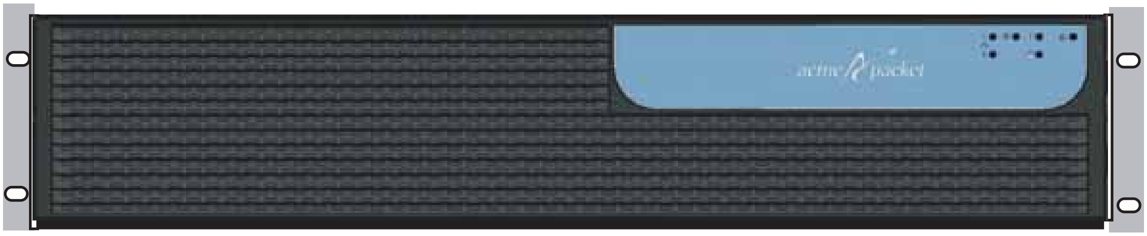


NN 2610 back view

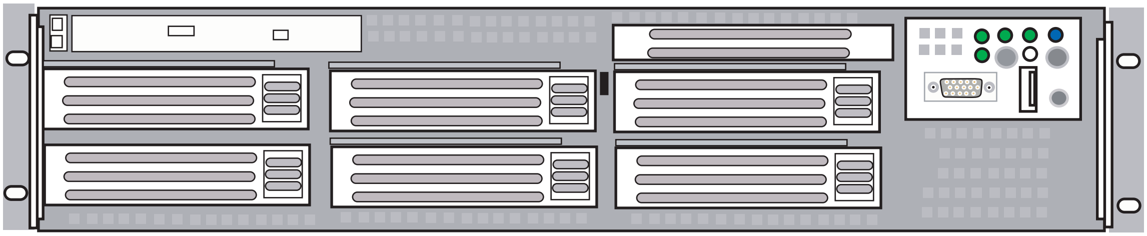


The following image illustrates the NN 2620 (2U) series chassis.

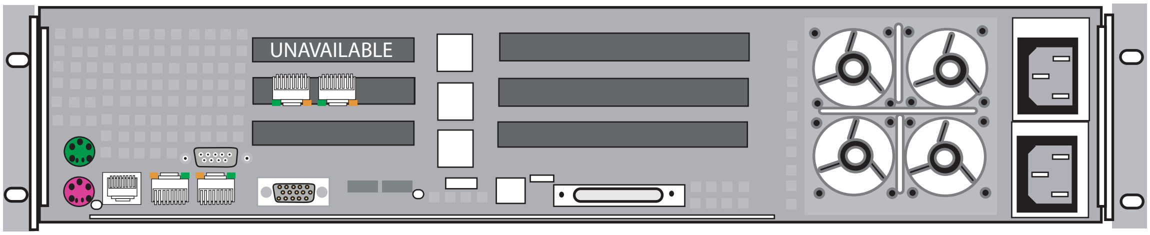
NN 2620 with front bezel



NN 2620 with front bezel removed



NN 2620 back view



Net-Net OS-E Series specification

NN2610 Specifications

Specification	Description
Chassis form factor	1U rack mount server
Dimensions	Height: 1.7” (4.3 cm) Width: 16.93” (43.0 cm) Depth: 26.46” (67.2) cm) Weight: 30 lbs (13.6 kg) approximate
Processors	Quad-Core Intel® Xeon® processor 5355, 8M Cache, 2.66 GHz, 1333 FSB
Memory	8 GB DDR2 667 MHz SDRAM
Storage	750 GB non-redundant hard disk storage
Power supply	Power: Single 600W AC voltage: 100-127/200-240VAC; 6.5 / 3.2A, 43-67 Hz, auto-ranging
Network interfaces	Up to six (6) 10/100/1000BaseTX (RJ-45) Ethernet ports with dual network interface cards installed.
Power and heat dissipation	NN 2610 with dual Ethernet cards (6 ports): 540W input (worst case); 1843 BTUs
Management	Policy based management software (CLI, Web GUI, Java (desktop) GUI, SNMP, XML, WSDL
External I/O ports	One (1) RJ-45 Serial B (DB-9 adapters supplied with product) One (1) PS2 keyboard 2 x 15-pin VGA
Fans and cooling	Four dual-rotor 56mm fans and one single-rotor 28mm fan mounted in tool-less fan module to support cooling for processors, hard drives, and add-in cards. Two 28mm fans for power supply cooling. All fans monitored and instrumented to provide RPM data for fan-failure prediction and detection.
Security	Mechanical locking bezel with key

Specification	Description
Ambient temperature	Operating: 0°C to +40°C (+32°F to 104°F) Non-operating: -20°C to +70°C (-4°F to 158°F)
Relative humidity	Operating and non-operating: 5% to 95% relative humidity, non-condensing

NN 2620 Specifications

Specification	Description
Chassis form factor	2U rack mount server
Dimensions	Height: 3.45” (8.75 cm) Width: 16.93” (43.0 cm) Depth: 26.46” (67.2 cm) Weight: 50 lbs (22.7 kg) approximate
Processors	Quad-Core Intel® Xeon® processor 5355, 8M Cache, 2.66 GHz, 1333 FSB
Memory	8 GB DDR2 667 MHz SDRAM
Storage	750 GB non-redundant hard disk storage, or 1.5 TB (max) redundant (RAID-10) hard disk storage
Power supply	Power: 2X redundant, 750W hot swappable AC voltage: 100-127/200-240VAC; 5.4 / 3.2A, 43-67 Hz, auto-ranging; separate power cords
Network interfaces	Up to eighteen (18) Ethernet 10/100/1000BaseTX (RJ-45) ports using dual network interface cards and dual MX-1 media acceleration cards installed.
Power and heat dissipation	NN 2620 with dual Ethernet cards (6 ports): 660W input (worst case); 2048 BTUs NN 2620 with dual Ethernet cards (6 ports), plus dual MX-1 Media acceleration cards (8 ports): 730W input (worst case); 2491 BTUs
Management	Policy based management software (CLI, Web GUI, Java (desktop) GUI, SNMP, XML, WSDL
External I/O ports	One (1) RJ-45 Serial B (DB-9 adapters supplied with product) One (1) PS2 keyboard 2 x 15-pin VGA

Specification	Description
Fans and cooling	2X redundant sets of four (4) 60mm fans in tool-less fan module; fans provide cooling for the processors, hard drives, and add-in cards; two 40mm fans per power-supply module for cooling the power-supply module All fans monitored and instrumented to provide RPM data for fan-failure prediction and detection.
Security	Mechanical locking bezel with key
Ambient temperature	Operating: 0°C to +40°C (+32°F to 104°F) Non-operating: -20°C to +70°C (-4°F to 158°F)
Relative humidity	Operating and non-operating: 5% to 95% relative humidity, non-condensing

System and Network Connections

This section summarizes the interface ports and connections that are supported with the OS-E 2600 Series. The image above illustrates the ports and connections on the NN2610. The NN2620 uses these same ports and connections as the NN2610 and are similarly located.

VGA Video, System Keyboard, and Power

The system provides direct connections for a VGA video monitor, keyboard, and AC power. Connecting these devices allows direct access to the CLI.

Note: VGA video connections are available on both the front and rear of the chassis. Only one of the VGA video connections can be used at a time.

RS-232 Serial B Port, DB9-to-RJ45 Adapter, and Null Modem Cable

The RS-232 Serial B port on the back of the system allows you to connect a PC or terminal directly to the system.

DB9 to RJ-45 Adapter

The system comes with three identical DB9-to-RJ45 cable adapters. While you only need one per system console connection, Oracle provides two spare adapters that you can use as needed.

Null Modem Serial Cable

For console and laptop PC connections to the RJ45 RS232 Serial B port, you will need a DB9-to-DB9 null modem cable and one DB9-RJ45 adapter.

Note Regarding RS-232 DB-9 Port on NN 2620 Systems

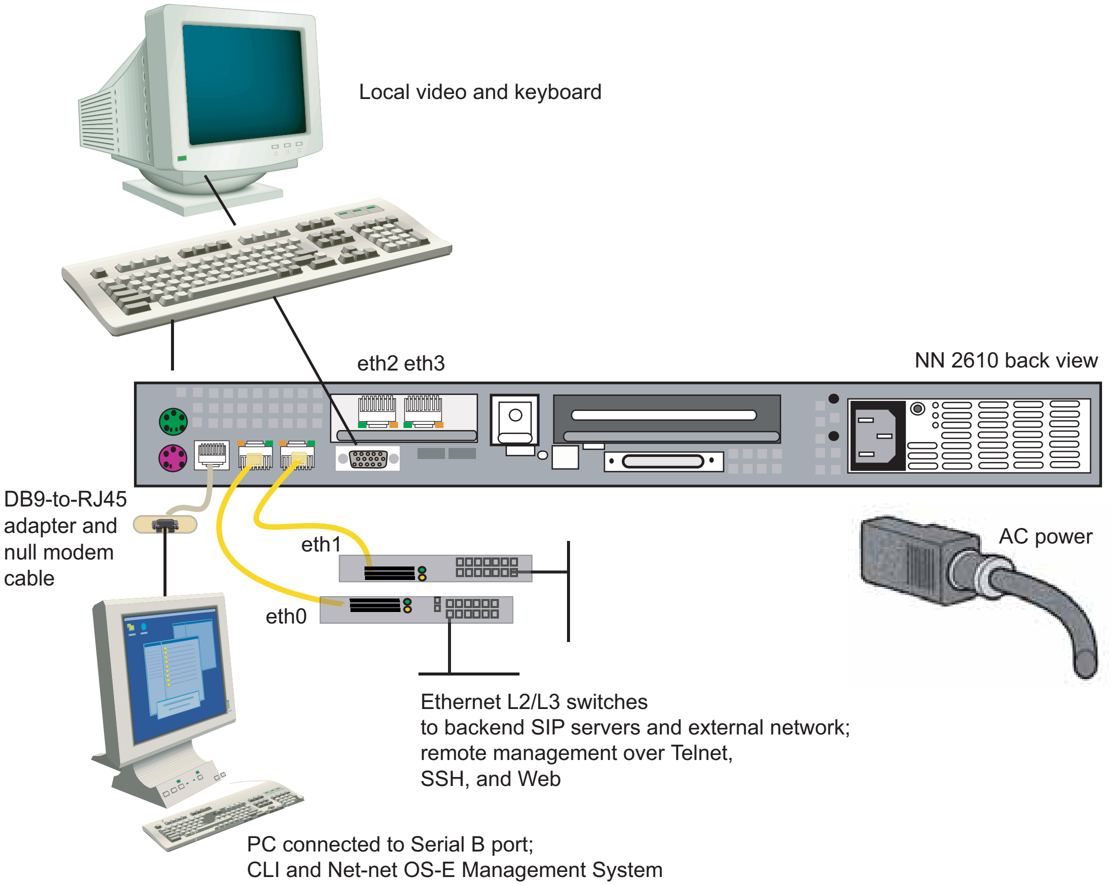
The physical RS-232 DB-9 port, while present on the back of N 2620 systems, is *not* available as an active console port. *Do not* plug the DB-9 end of a null modem console cable into this port.

Gigabit Ethernet (IEEE 802.3ab, 1000Base-TX)

The Ethernet interfaces on the system support auto negotiation 10/100/1000 Mbps copper network interface connections (NIC).

Gigabit Ethernet is the latest version of Ethernet that supports data transfer rates of up to 1 Gigabit (1,000 megabits) per second. The Ethernet ports are IEEE 802.3ab for CAT5 or CAT5e unshielded twisted pair (UTP) cable, with 8-pin NIC connector.

The following image displays OS-E network connections.


Local video and keyboard
eth2 eth3
NN 2610 back view
DB9-to-RJ45 adapter and null modem cable
eth1
eth0
AC power
Ethernet L2/L3 switches
to backend SIP servers and external network;
remote management over Telnet,
SSH, and Web
PC connected to Serial B port;
CLI and Net-net OS-E Management System

USB 2.0 Port

The Universal Serial Bus (USB) 2.0 ports allow you to perform the following functions:

- Commission and license OS-E software at initial startup.
- Create a system restore USB stick containing the latest system configuration should the system have a catastrophic failure requiring system recovery.
- Create a system utilities USB from which you can run Oracle programs to diagnose system problems.

System Software and Licensing

The system software and features license is downloaded to the system hard drive(s) when you insert the Oracle USB stick and power up the system for the first time. Software upgrades are available and released by Oracle on a regular basis.

System Components

This section summarizes the system hardware components provided with the Oracle OS-E 2610 and 2620 systems:

- Intel® SE7520JR2 Server Board
- Cooling fans
- Power modules
- Hard disk drives
- Removable bezel

Intel® SE7520JR2 Server Board

The Intel® SE7520JR2 Server Board controls the following system features:

- Two Ethernet data ports (Ethernet 10/100/1000 Mbps auto negotiation); up to four Ethernet ports on the 2U chassis with the MX-1 media acceleration card.
- RJ-45 Serial B port for terminal or PC hookup
- Light-emitting diode indicators (LEDs) on Ethernet ports
- PS2 ports for a directly-attached keyboard and mouse; video connector for a directly-attached monitor
- System status indicator LEDs on front control panel
- AC power input; dual/redundant AC input in 2U chassis
- 500W power module in 1U chassis; redundant 700W hot-swappable power modules in the 2U chassis
- Over temperature protection (OTP) and over voltage protection (OVP) circuitry

System Fans and Cooling

Oracle OS-E systems require a normal operating environment for computing equipment, using internal fans, air baffles, and air ducts to ensure adequate airflow. When external ambient temperatures remain within specified limits, the system fans provide sufficient airflow through the system, pulling air from the front of the chassis to the back.

The NN 2610 chassis uses a non-redundant multi-system fan module and dual non-redundant power module fans. The NN 2620 chassis supports up to eight system fans in a modular 4+4 configuration.

In addition to the eight system fans, each power module installed provides an additional two non-redundant fans that pull air from inside the chassis to the back. By default, the NN 2620 chassis is equipped with four system fans with no fan redundancy.

During system installation, allow at least 6 inches (150 mm) of unobstructed space at the front and back. The chassis requires no air space above or below.

If you install the system in an enclosed equipment rack, be sure there is adequate airflow and the following environmental requirements:

- Operating ambient air temperature: 10°C to +35°C (50° to 95°F)
- Non-operating ambient air temperature: -40°C to +70°C (-40° to 158° F)
- Non-operating humidity: 90% non-condensing @ 35°C
- Power and heat dissipation:
  - — NN 2610 with dual Ethernet cards (6 ports): 540W input (worst case); 1843 BTUs
  - — NN 2620 with dual Ethernet cards (6 ports): 660W input (worst case); 2048 BTUs
  - — NN 2620 with dual Ethernet cards (6 ports), 730W input (worst case); 2491 BTUs

Power Modules

For NN 2610 (1U) Chassis

The NN 2610 (1U) chassis uses a single non-redundant 500W power module with the following integrated management features:

- Status LED
- Over temperature protection (OTP)
- Over voltage protection (OVP)

The power supply provides two non-redundant 28mm fans for self cooling and system cooling at an airflow rate of 10 CFM. Air moving through the power supply is pre-heated from the system and exhausts out the back.

To protect the equipment, Oracle recommends using a conditioned power source or uninterruptable power supply (UPS). The power source must provide a reliable earth ground, and provide the following:

- Voltage: 100 to 127 VAC @ 43 to 67 Hz; 6.5A maximum
- Voltage: 200 to 240 VAC @ 43 to 67 Hz; 3.2A maximum

The power module connector uses a standard 3-prong keyed IEC 320 C-14 receptacle rated for 15A/250VAC. The power cord is supplied with an IEC connector on one end, NEMA 5-15 plug (U.S. domestic) on the other end.

For the NN 2620 Chassis

The NN 2620 chassis uses up to two 700W power supplies. The system can be configured to support a single power module in a non-redundant configuration, or dual power modules in a 1+1 redundant power configuration. In a redundant configuration, a single failed power module can be hot-swapped with the system running. Either configuration supports up to a maximum of 700 watts of power with the following integrated management features:

- Status LED
- Over temperature protection (OTP)
- Over voltage protection (OVP)

Oracle recommends using a conditioned power source or uninterruptable power supply (UPS). The power source must provide a reliable earth ground, and provide the following:

- Voltage: 100 to 127 VAC @ 50/60 Hz; 8.9A maximum
- Voltage: 200 to 240 VAC @ 50/60 Hz; 5.4A maximum

The power module connector uses a standard 3-prong keyed IEC 320 C-14 receptacle rated for 15A/250VAC. The power cord is supplied with an IEC connector on one end, NEMA 5-15 plug (U.S. domestic) on the other end.

Hard Disk Drives

OS-E systems use 500GB and 750GB hard disk drives to store the operating system and the OS-E software.

NN 2610 (1U) Chassis

The NN 2610 chassis provides three hot-swappable hard drive bays and one slim-line bay at the front of the chassis. The hard drive bays support Serial ATA (SATA)* hard disk drives.

- For hot swap drive configurations, 3.5”x 1” hard disk drives are mounted to hot swap drive trays for easy insertion and extraction.
- For cabled drive configurations, SATA drives are mounted to non-hot swappable drive trays. Cabled hard drives can only be removed by unlatching the drives from inside the chassis.

⛔ **Caution:** All hard drive bays must be populated to maintain system airflow and cooling. Drive trays must have a drive or a drive blank inserted.

NN 2620 2U Chassis

The NN 2620 chassis provides up to five (default) SATA hard disk drives. One slim-line peripheral bay is available for either optical or floppy drive.

- For hot swap drive configurations, 3.5”x 1” hard disk drives are mounted to hot swap drive trays for easy insertion and extraction.

- For cabled drive configurations, SATA drives are mounted to non-hot swappable drive trays. Cabled hard drives can only be removed by unlatching the drives from inside the chassis.

⛔ **Caution:** All hard drive bays must be populated to maintain system airflow and cooling. Drive trays must have a drive or a drive blank inserted.

Removable Bezel

OS-E Series systems have a removable front bezel. The bezel snaps into the front of the chassis and is secured with a keyed lock. These systems can operate with or without the front bezel. Removing the bezel allows you to access the system control panel and the hard disk drives on the front of the system. Installing the bezel provides a secure way to protect the system from unwanted intrusion and manipulation of the system control panel. For information on removing and installing the bezel, refer to Chapter 7, “Performing Maintenance and System Upgrades.”

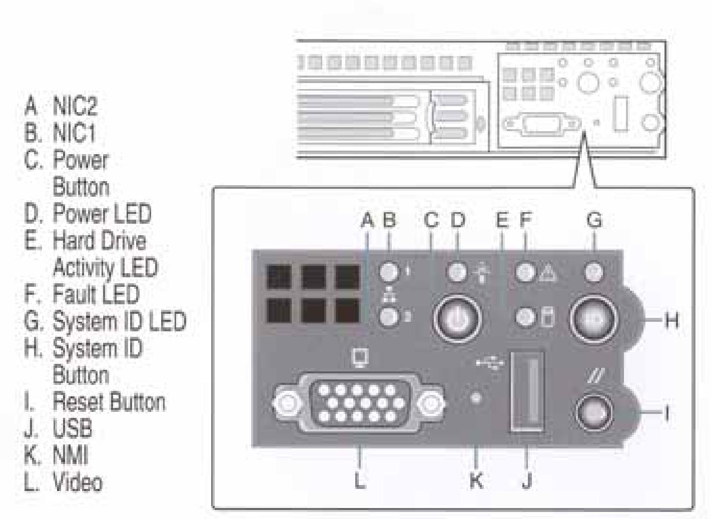
***** SATA is a specification for consumer hard drive connections that boosts the data transfer rate up to150MB/second. It changes IDE/ATA from a parallel interface requiring 40 separate wires to connect components to a serial interface requiring only 6 wires.

System Control Panel

The system control panel supports several push buttons and status LEDs on the front of the system. OS-E Series systems use the same control panel.

Push buttons and LEDs

The following image illustrates the system control panel push buttons and LEDs.



The following table displays system control panel functions.

Reference	Feature	Function
B	NIC1 (eth0) activity	Continuous green light indicates a link between the system and the network to which it is connected
A	NIC2 (eth1) activity	Blinking green light indicates network activity
C	Power/Sleep button	Toggles the system power on/off. This button also functions as a Sleep button if enabled by an ACPI-compliant operating system.
D	Power/Sleep LED	Continuous green light indicates the system has power applied to it. Blinking green indicates the system is in a sleep state. No light indicates the power is off.
E	Hard disk drive activity LED	Random blinking green light indicates hard disk drive activity (SCSI or SATA). No light indicates no hard disk drive activity.

Reference	Feature	Function
F	System Fault LED	Solid green indicates normal operation. Blinking green indicates degraded performance. Solid amber indicates a critical or non-recoverable condition. Blinking amber indicates a non-critical condition. No light indicates power-on-self-test (POST) is running or the system is off.
G	System Identification LED	Solid blue indicates system identification is active. No light indicates system identification is not activated.
H	System Identification button	Toggles the front panel ID LED and the baseboard LED on/off. The baseboard LED is visible through the rear of the chassis and allows you to locate the server you are working on from behind a rack of servers.
I	Reset button	Reboots and initializes the system.
J	USB 2.0 port	Allows you to commission the system using a USB stick. See the *Net-Net OS-E – USB Creation and Commissioning Instructions* for information.
K	NMI button	Puts the system in a halt state for diagnostic purposes.
L	Video port	Allows you to attach a video monitor to the front of the chassis. The front and rear video ports cannot be used at the same time.

Installing the NN 2610 and 2620 Series

This section covers the required information for installing the NN 2610 and NN 2620 Series systems.

Required Tools

If you are installing the system in a rack, you will need a #2 Phillips screwdriver to install the mounting ears to the front of the chassis. There are no other special tools required for installing the system. Refer to the instructions included with the rack mounting hardware for information.

Unpacking the System

The system shipping container includes the following items:

- NN 2610 or NN 2620 chassis
- *Net-Net OS-E – Net-Net 2610/2620 Quick Installation* card
- System accessories (front bezel, rack mounting rails, etc.)

Note: Hardware needed to mount the system to a rack or cabinet, such as custom mounting screws, nuts and miscellaneous hardware items, are not included due to the many variations available.

If you ordered the tool-less rail kit that allows you to mount the system in a compatible rack or cabinet, the necessary hardware and rack installation instructions are included in the kit.

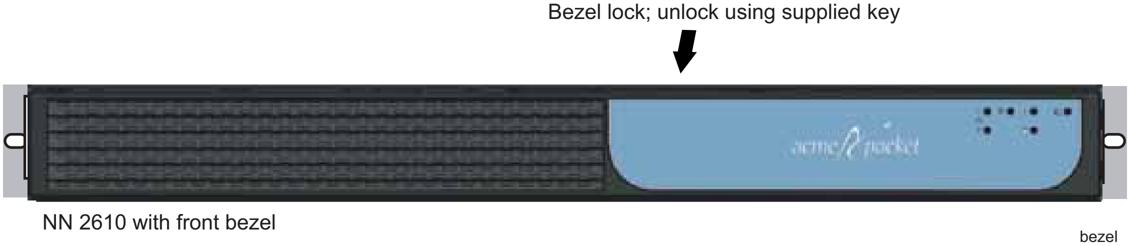
If any of these components are missing, contact Oracle. Locate the unpacking instructions included with the shipment for the proper procedures for safely unpacking the system.

Installing and Removing the Front Bezel

OS-E systems have a removable front bezel. The bezel snaps into the rack mounting brackets at front of the chassis and is secured with a keyed lock, illustrated in the following image. NN 2610 and NN 2620 Series systems can operate with or without the front bezel.

Removing the bezel allows you to access the system control panel and the hard disk drives on the front of the system. Installing the bezel provides a way to protect the system from unwanted intrusion and manipulation of the system.

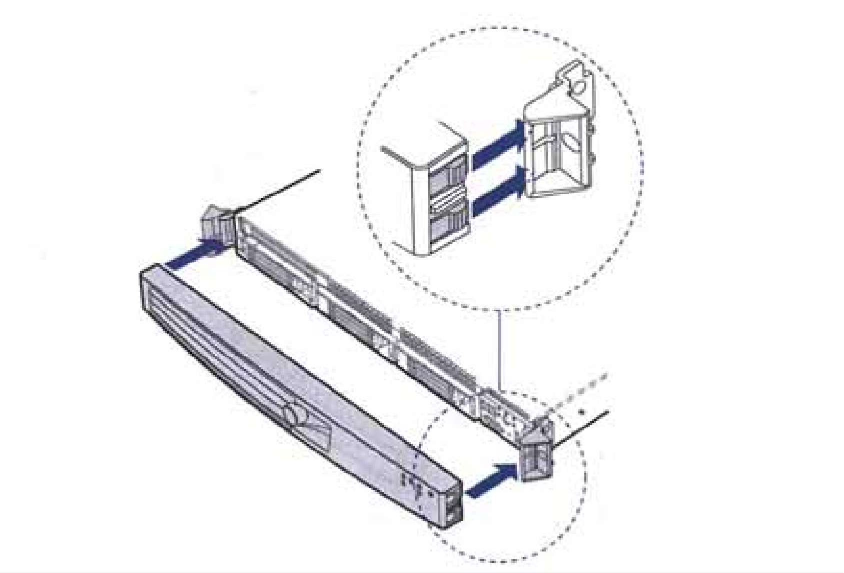
NN 2610 locking bezel



To install the front bezel, perform the following steps:

1. At each end of the bezel, line up the center notch on the bezel with the center guide on the rack handles.
2. Push the bezel onto the front of the chassis until it clicks into place.
3. Connect any necessary cables to the front control panel area at the right side of the chassis.
4. Lock the bezel using the supplied key.

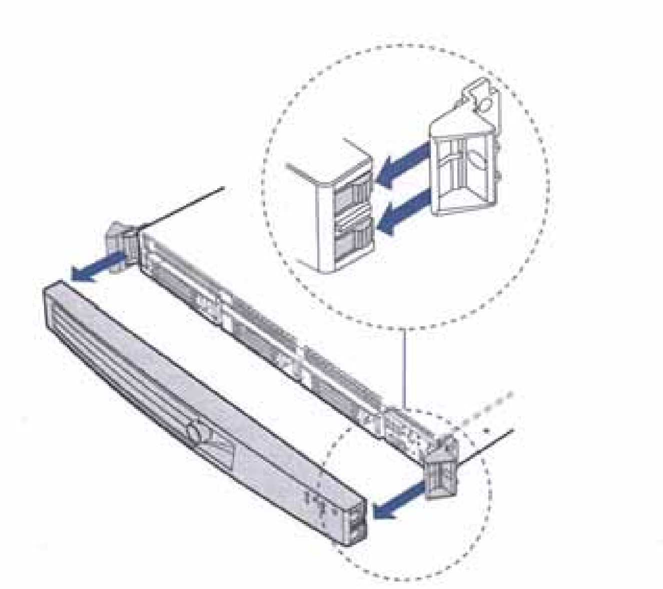
The following image displays the front bezel being installed.



To remove the bezel, perform the following steps:

1. Unlock the bezel using the supplied.key.
2. Remove any cables that are attached to the front of the system.
3. Pull on the left- and right-most edges of the bezel to pop it out.

The following image displays the front bezel being removed.



Mounting the System In a Rack

The OS-E 2600 Series chassis installs in any standard 19-inch by 30-inch deep 2- or 4-post computer rack or 4-post EIA-310D compatible server cabinet.

A sliding rail kit allows you to mount the chassis in a standard (19-inch by and up to 30-inch deep) rack. When installing the system in a rack, Oracle recommends you install systems from the bottom of the rack to the top. This means that you install the first system in the rack into the bottom position of the rack, the second system in the second position from the bottom, and so on.

Instructions for installing the rack are included with the rail kit in the shipping container as well as in PDF format with the OS-E technical documentation.

Connecting Console Equipment

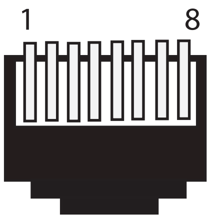
This section shows you how to connect console equipment (PC or terminal) to the system: There are two ways to make a direct local connection:

- Using the Serial B port on the back of the chassis
- Using the video and keyboard connections

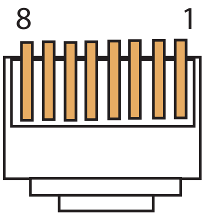
Using the Serial B Console Port

The Serial B console port provides a serial EIA-561 RS232D connection with a DTE interface using a male RJ-45 plug. Attaching a terminal or PC allows you to connect to the system CLI for initial setup at the installation site. To connect a terminal or PC to the RJ-45 Serial B port, you need a DB-9 to DB-9 serial cable and the supplied RJ-45 dongle that connects between the DB-9 cable and the RJ-45 socket.

The following image illustrates the RJ-45 and lists the pin/signal information.



CXC Series RJ45 socket



RJ45 plug end (male; front view)

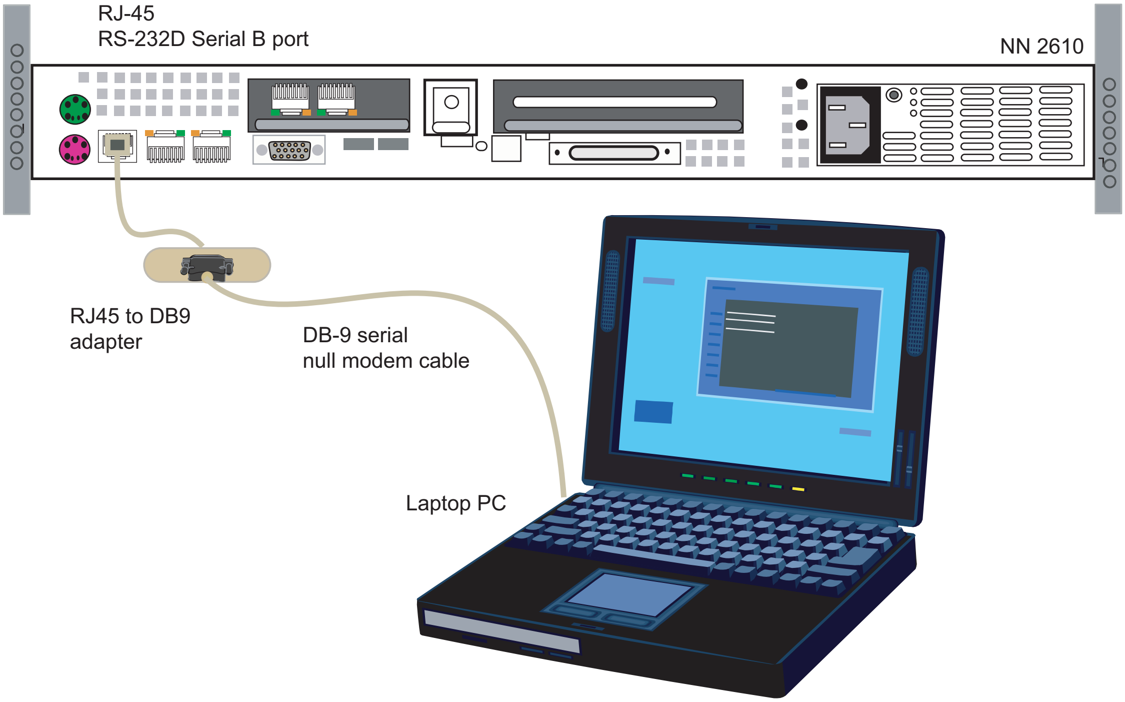
Pin No.	Signal Name/Description	
1	RTS	Request to Send
2	DTR	Data Terminal Ready
3	TXD(	Transmit Data
4	GND	Ground
5	RI	Ring Indication
6	RXD	Receive Data
7	DSR/DCD	Data Set Ready/Data Carrier Detect 1
8	CTS	Clear to Send

Note: The physical RS-232 DB-9 port, while present on the back of NN 2620 systems, is *not* available as an active console port. *Do not* plug the DB-9 end of a null modem console cable into this port.

Perform the follow steps to connect a PC or video terminal to the Serial B port:

1. Check the video terminal or PC for the type of serial connector that it uses (either DB-9 or DB-25) and locate the appropriate cable:
   - DB-9 to DB-9 (customer supplied null modem)
   - DB-9 to DB-25
2. Using a DB9- to RJ45 adapter, connect the RJ45 plug end of the cable into the Serial B port.
3. Connect the DB-9 end of the null modem serial cable to the adapter; connect the other end of the cable (DB-9 or DB-25 to the video terminal or PC.
4. Turn the video terminal or PC on.
5. Configure the video terminal or PC (using a terminal emulation program such as HyperTerminal) with the following settings:
   - Baud rate: 115200
   - Terminal type: VT-100 (if prompted)
   - Connect to: COM1
   - Stop bits: 1
   - Data bits: 8
   - Parity: none
   - Flow control: none

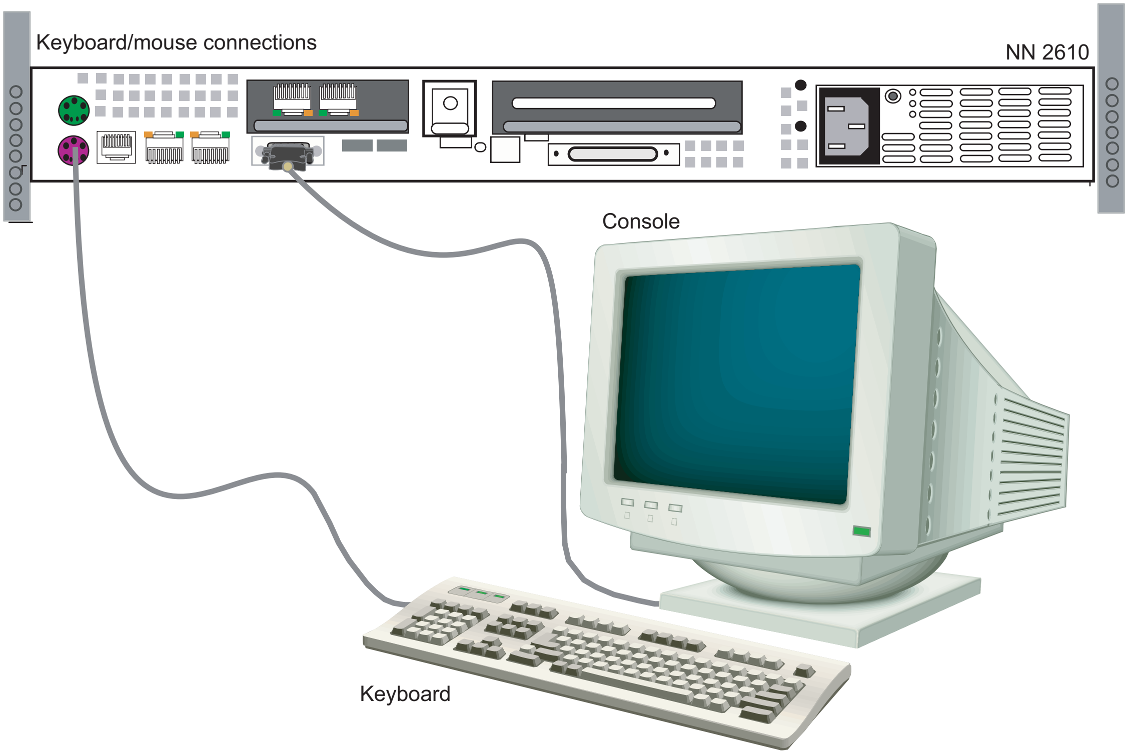
The following image illustrates connecting a PC or terminal.



Using the Video and Keyboard Connections

You can create direct connections to the system by simply connecting a monitor and keyboard. The system has two video console interfaces that accept a standard 15-pin console cable; one connector on the front of the system, and another on the back. You can only connect one video console at a time. This means that both video connectors cannot be used simultaneously.

The following image illustrates the direct video and keyboard connections. A VGA console is recommended.



Connecting the Ethernet Interfaces

The Ethernet interfaces on the system support auto negotiation 10/100/1000 Mbps copper network interface connections (NIC). This means that you can connect to Ethernet equipment that supports 10, 100, or 1000 Mbps connections. Ethernet ports label 1 to 4 translate to Ethernet interfaces eth 0 to eth3 in the product software.

The NN 2610 is equipped with up to six Ethernet interfaces, and the NN 2620 is equipped with up to twenty Ethernet interfaces usingnetwork interface cards.

To connect to the data network, you need the following:

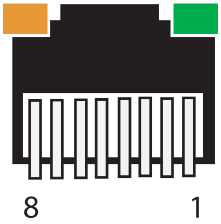
- For connection to an Ethernet hub or switch, an RJ-45 to RJ-45 straight-through cable (100 ohm, Category 5 or 5E, with a maximum length of 328 feet (100 meters))

- For a direct connection to a PC or laptop computer, an Ethernet cross-over cable (for local Telnet connection or access to the OS-E Management System from your Web browser).
- For links to the external network, a connection to an upstream Layer 2 switch behind the firewall, and a switch that connects to the backend communications servers.

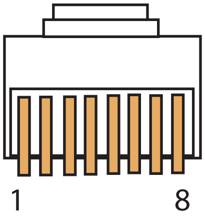
Caution: Do not insert an RJ-11 telephone connector into any Ethernet interface on the system. Damage to the interface may occur.

Note: Any Ethernet interface can be used for management traffic. However, Oracle recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other OS-E systems. Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

The following image illustrates the Ethernet port associated pin information.



RJ-45 socket



RJ-45 plug end (male; front view)

Pin No.	Signal Description	
	Fast Ethernet	Gigabit Ethernet
1	TX+	MD0+
2	TX-	MD0-
3	RX+	MD1+
4	T45	MD2+
5	T45	MD2-
6	RX-	MD1-
7	T78	MD3+
8	T78	MD3-

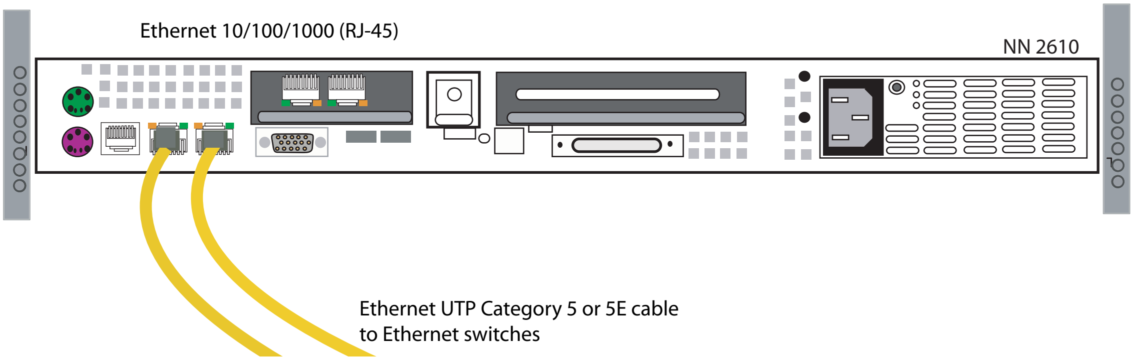
Perform the following steps to connect to the Ethernet interfaces:

1. Connect one end of the RJ-45 Ethernet straight-through cable to the port labeled 1 or 2. (eth0 and eth1, respectively).

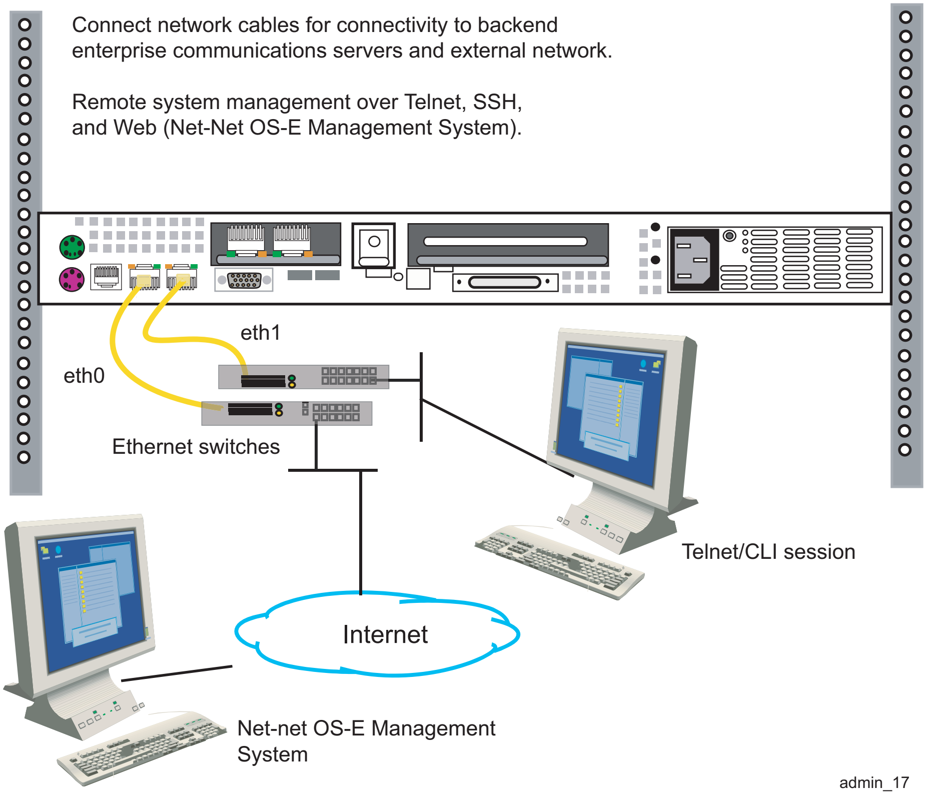
Note: Ethernet ports on the system are labeled with numbers, and are oriented left to right, top to bottom. The port labeled “1” is the same as eth0, the port labeled “2” is the same as eth1, and so on.

2. Connect the other end of the cable to an available port on the Ethernet hub or switch. The LEDs should display green (Link) and yellow (Activity).
3. If connecting a PC or laptop computer directly to eth0 or eth1, use an Ethernet crossover cable or crossover adapter to ensure a proper connection to the port.

The following image illustrates the OS-E 2600 Series Ethernet connections.

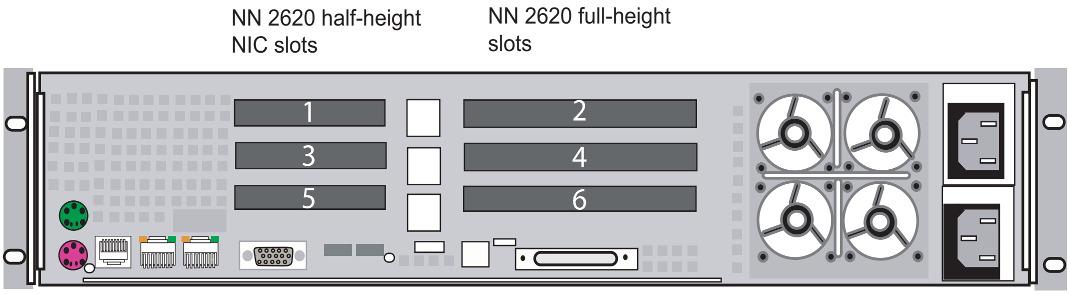

Ethernet 10/100/1000 (RJ-45)
NN 2610
Ethernet UTP Category 5 or 5E cable
to Ethernet switches

The following image illustrates the Net-Net OS-E Series sample network connections.


Connect network cables for connectivity to backend
enterprise communications servers and external network.
Remote system management over Telnet, SSH,
and Web (Net-Net OS-E Management System).
eth1
eth0
Ethernet switches
Telnet/CLI session
Internet
Net-net OS-E Management
System
admin_17

NN 2620 Half- and Full-Height Slots

The following image illustrates the back of the NN 2620 chassis showing the half- and full-height NIC slots, labeled 1 to 6. Both the half- and full-height slots can accommodate the standard Ethernet dual-port NIC.



For Standard Dual-Port NIC Installations

Install multiple NICs in the following sequence:

1. Install the first NIC in full-height slot 5.
2. Install the second NIC in full-height slot 3.

Ethernet Port Assignments

NN 2620 Ethernet port numbering depends on the number of NIC cards that you are using. Looking at the back of the chassis, port numbering runs left to right, and progresses top to bottom.

- Chassis ports: **eth0, eth1**
- Ethernet NIC 1: **eth2, eth3**

Moving NICs After Installation

There are a number of important considerations if you must relocate NIC cards within the same NN 2620 chassis.

1. Installed NIC cards maintain their port numbering and MAC addressing after initial installation. This means that if you relocate a NIC card from half-height slot 1 to half-height slot 3, the first Ethernet port in slot 3 will be eth2.
2. When relocating a NIC from a half-height slot to a full-height slot, the orientation of the card will be reversed in the new full-height slot installation. This means that the port numbering from the original installation will be reversed in the new slot.
3. Adding NIC cards after the initial installation will result in new port numbers that begin using the highest port number plus 1. For example, if the highest port number is eth11, the first port on the newly added card will be eth12.

Connecting AC Power

This section shows you how to connect and apply system power to the NN 2600 Series system..

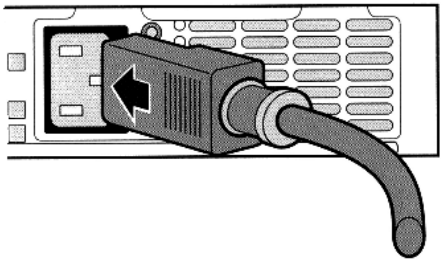
AC Power Requirements

Before installing the power cable, be sure that your site meets the following AC power requirements:

- Voltage: automatic selection/ranging
  100 to 127 VAC; 8.2 A maximum @ 50/60HZ;
  200 to 240 VAC; 4.1 A max @ 50/60 HZ
- AC power cord — North America (CBL-PWR-USA):

  Power module connector: Standard 3-prong keyed IEC receptacle on power module; cord supplied with IEC connector on one end, NEMA 5-15 plug (U.S. domestic) on the other end.
- Other power cords are available for the following countries:
  - Europe (CBL-PWR-EUR)
  - United Kingdom (CBL-PWR-GBR)

The following image illustrates the NN 2610 power connection at the back of the system.

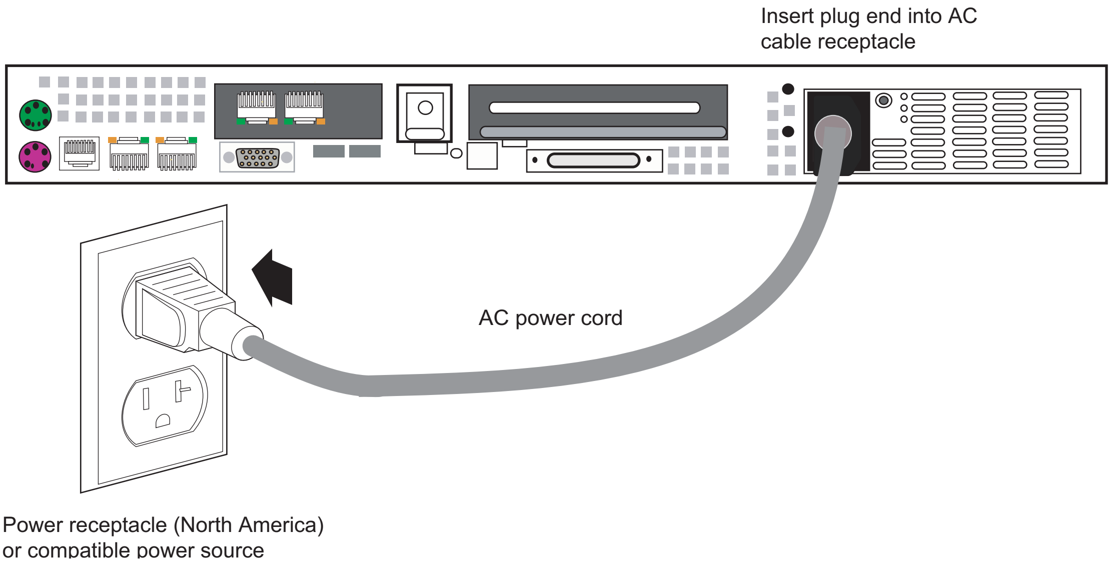


Connecting the AC Power Source

To connect the AC power cables, perform the following steps

1. Locate the system power cord.
2. Insert the plug end into the AC cable receptacle at the back of the system.
3. Plug the other end of the cable into a compatible power source.
4. Repeat Steps 1 to 3 for the redundant power supply, if installing the NN 2620 with redundant power.

The following image displays the NN 2610 AC power installation.


Insert plug end into AC cable receptacle
AC power cord
Power receptacle (North America) or compatible power source

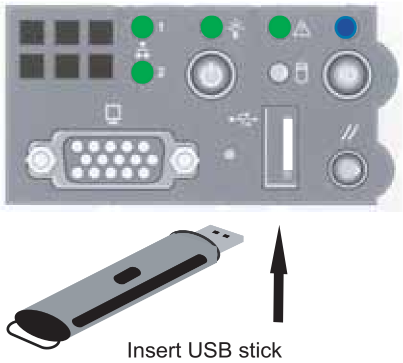
Inserting the USB Stick

Before proceeding with this step, and if you have not already done so, create an installation USB stick from the OS-E software download. Refer to the *Net-Net OS-E – USB Creation and Commissioning Instructions* for complete information on how to use the software download process, create an installation USB, and then commission the system from the USB stick.

When you install the USB into any of the USB ports and then apply power to a new system, the process will install the license and initialize the system. At the end of the boot-up process, the system rewrites the USB stick so that the box identifier and the installed license are matched to this particular system.

You need to remove the USB stick after the system has successfully booted. Later, and if required, you can use this USB stick to run system utilities to restore the system in the event of a failure. Other functions are also available from the utility USB stick.

The following image illustrates inserting the USB stick.



Refer to the *Net-Net OS-E – USB Creation and Commissioning Instructions* for information on USB commissioning, as well as how to create system utility and system restore USBs.

Applying Power

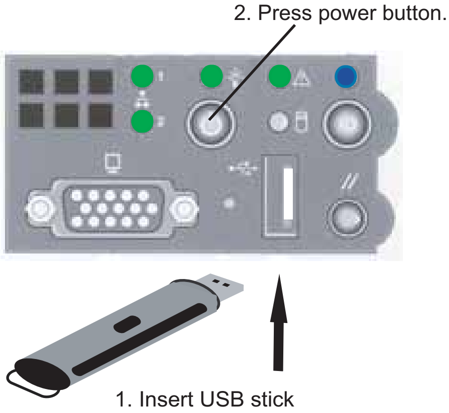
To apply power and to initiate system startup, make sure that the USB stick is installed, then press the system power button on the control panel.

Note: Depending on the actual hardware revision that you are running, the system may power up a few seconds after you attach the power cord. This means that the system will start without having to press the system power button.

The system will take several minutes to go through the startup and diagnostics routines before you will see the username and login prompts.

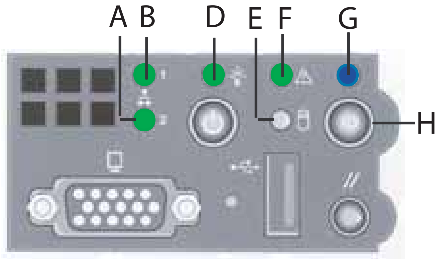
At the NNOS-E prompt, type **umount usb** to properly dismount the USB stick. Physically remove the USB stick from the USB connector.

The following image illustrates the OS-E Series power button.



Checking the LEDs

After powering the system ON, check the system LEDs to ensure proper cabling and connections. The following image illustrates the control panel.



The following table lists LED States that you should verify after powering the system on.

Reference	Feature	Function
B	NIC1 (eth0) activity	Continuous green light indicates a link between the system and the network to which it is connected.
A	NIC2 (eth1) activity	Blinking green light indicates network activity.
D	Power/Sleep LED	Continuous green light indicates the system has power applied to it. Blinking green indicates the system is in a sleep state. No light indicates the power is off.
E	Hard disk drive activity LED	Random blinking green light indicates hard disk drive activity (SCSI or SATA). No light indicates no hard disk drive activity.
F	System Fault LED	Solid green indicates normal operation. Blinking green indicates degraded performance. Solid amber indicates a critical or non-recoverable condition. Blinking amber indicates a non-critical condition. No light indicates power-on-self-test (POST) is running or the system is off.
G	System Identification LED	Solid blue indicates system identification is active. No light indicates system identification is not activated.
H	System Identification button	Toggles the front panel ID LED and the baseboard LED on/off. The baseboard LED is visible through the rear of the chassis and allows you to locate the server you are working on from behind a rack of servers.

Logging On and Starting the CLI

Using a locally attached console with a terminal emulation program, log on to the system for the first time by first pressing the [Enter] key a few times to display the `username` prompt, and then by responding to the `username` and `password` prompts by pressing the [Enter] key. This displays the NNOS-E> prompt on your screen.

```
username: [Enter]
Password> [Enter]
NNOS-E>
```

Assigning a Management IP Address

Before you can manage an OS-E system remotely over the Internet using the OS-E Management System or over a Telnet connection, you need to locally assign an IP address to one of the Ethernet interfaces, **eth0**, **eth1, eth2,** or **eth3.** If you are setting up the device remotely, you will also need to configure an IP route, a route to a destination host or network, and a gateway IP address.

If you are using the OS-E Management System, you will also need to know the assigned IP address on one of the Ethernet ports to manage the OS-E configuration. The OS-E Management System application runs directly on the OS-E system over the Internet using the Internet Explorer Web browser.

The following CLI session creates and enables an IP interface named *mgmt-int***,** sets the static IP address and network mask, configures an IP route (if connecting remotely), and enables Web access on this IP interface. You will need to enable ICMP on the OS-E IP interface before you can use the **ping** command from your console to test the device as a responding node on the network. Use the **show -v** command to display the configuration.

CLI Session

```
NNOS-E> config box
config box> set hostname local2610
config box> config interface eth0
config interface eth0> config ip mgmt-int
Creating ‘mgmt-int’
config mgmt-int> set admin enabled
config mgmt-int> set ip-address static 192.168.124.5/24
config mgmt-int> config routing
config routing> config route internetGateway
Creating ‘route internetGateway’
config route internetGateway> set destination default
config route internetGateway> set gateway 192.168.124.3
config route internetGateway> return
config routing> return
config ip mgmt-int> config web
config web> set admin enabled
config web> set port 80
config web> return
config mgmt-int> config icmp
config icmp> set admin enabled
config icmp> top
config> save
config> show -v
```

Using the Setup Script

An optional configuration setup script called *cxc.setup* is now included with newly shipped systems. After installing a new system, you can run the script directly from the NNOS-E> prompt, as shown in the example session below.

The script presents a set of questions to help you with the initial system configuration. The information in the script include the following:

- Local hostname
- IP interface names and addresses
- SSH and Web access
- Default route and any additional static routes per interface for remote management
- User-defined CLI prompt

Every OS-E Series system has a minimum of two Ethernet interfaces. Any Ethernet interface on the system can be used for management traffic, however, Oracle recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other systems. Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI Session

```
NNOS-E> config setup
set box\hostname: <name>
config box\interface: eth1
set box\interface eth1\ip a\ip-address: <ipAddress/mask>
config box\interface eth1\ip a\ssh (y or n)? n
config box\interface eth1\ip a\web (y or n)? y
config box\interface eth1\ip a\routing\route: <routeName>
set box\interface eth1\ip a\routing\route localGateway\gateway:
<ipAddress>
set box\cli\prompt: <newPrompt>
Do you want to commit this setup script (y or n) y
Do you want to update the startup configuration (y or n)? y
```

Note: The /cxc directory on the system may include vendor-specific scripts that address unique startup configuration requirements. Specify the name of the script on the command line following the **config setup** command. For example:

```
NNOS-E> config setup vendor.setup
```

Check the /cxc directory for any vendor-specific setup files included with your system.

Enabling Network Access

To ensure you can manage the system using services such as Telnet or the OS-E Management System, you must configure the system so that it is available on the network. You need to create a default (or static) IP route, a route to a destination host or network, and a gateway IP address.

After you configure the static route, enable ICMP and then use the **ping** command at the top-level of the CLI to test network accessibility.

Defining a Default Route and Gateway IP

If you are setting the box remotely, you will need to configure an IP route, a route to a destination host or network, and a gateway IP address.

CLI Session

The example CLI session shows the routing context (in **bold** text) and the route named *internetGateway*. This the default route that uses 192.168.124.3 as the default gateway

```
NNOS-E> config box
config box> set hostname local2610
config box> config interface eth0
config interface eth0> config ip mgmt-int
Creating ‘mgmt-int’
config mgmt-int> set admin enabled
config mgmt-int> set ip-address static 192.168.124.5/24
config mgmt-int> config routing
config routing> config route internetGateway
Creating ‘route internetGateway’
config route internetGateway> set destination default
config route internetGateway> set gateway 192.168.124.3
config route internetGateway> return
config routing> return
config ip mgmt-int>
```

Cluster Installation

If you are installing OS-E systems in a network cluster, refer to Chapter 4, “Installing Net-Net OS-E Clusters,” and the Oracle Communications OS-E Release Notes for the latest information.

Chapter 3. Quick Commissioning New OS-E Systems

About This Chapter

The chapter provides the basic information that allows you to configure OS-E software after you have physically installed the system in your network. Commissioning enables an OS-E system or compatible third-party device to process locally registered SIP phone calls.

Prerequisites to Quick Commissioning

Before using the information in this chapter, make sure that you have properly installed and cabled the system, as covered in Chapter 1. The following OS-E documents provide additional information on configuring Session OS-E services, as well as how manage the system using the OS-E CLI and the OS-E Management System.

- *Net-Net OS-E – System Administration Guide*
- *Net-Net OS-E – Objects and Properties Reference*
- *Net-Net OS-E – Management Tools*

Additionally, the *Net-Net OS-E – Release Notes* provides important information about the software that you should review before commissioning a system in your network.

Steps 1 through 5 cover the tasks and services for getting the system up and running on an IP network so that the Ethernet interfaces can process SIP sessions. When enabled on an IP network, you can manage the system and its configuration remotely over the Internet using the OS-E Management System.

Steps 6 through 10 cover the tasks that allow you to control and monitor SIP sessions, as well as store call detail records and recordings.

Building the Configuration File

The OS-E configuration file (*cxc.cfg*) is made up of configuration objects and property settings that control how the system processes and manages SIP traffic. As you open these objects and set properties using the CLI or the Net-Net OS-E Management System, the software builds a configuration hierarchy of objects that are applied to SIP sessions. You can display this configuration hierarchy using the **show** and **show -v** (verbose) commands.

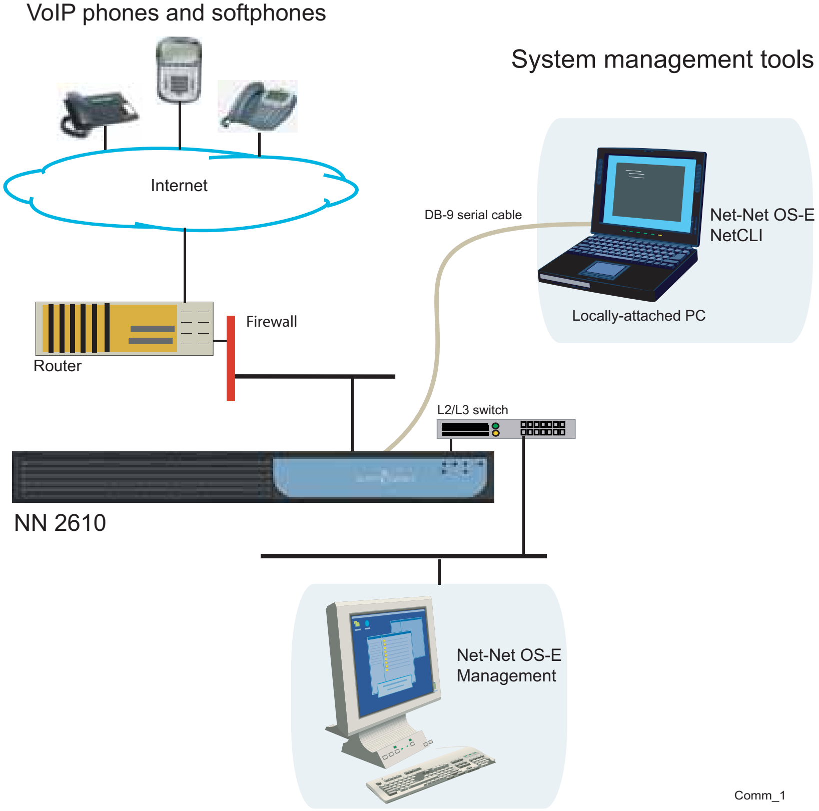
For new users, as well as for users who are adding functionality to their configuration, you will need to open configuration objects using the **config** command to enable the default settings for those objects, even if you choose not to edit any of their associated properties. For example, if you need to enable the **ICMP** protocol and its default settings, you simply open the object and execute **return**, as shown in the session below. Notice that the ICMP object has been added to the configuration hierarchy at the end of the session on the eth4 interface.

```
config> config box interface eth4
config interface eth4> config ip 172.26.2.14
config ip 172.26.2.14> config icmp
config ip 172.26.2.14> return
config interface eth4> return
config box> return
config> show -v
interface eth4
  admin enabled
  mtu 1500
  arp enabled
  speed 1Gb
  duplex full
  autoneg enabled
  ip 172.26.2.14
   admin enabled
   ip-address dhcp
   geolocation 0
   metric 1
   classification-tag
   security-domain
   address-scope
   filter-intf disabled
   icmp
    admin enabled
    limit 10 5
```

To remove an object from the configuration hierarchy, use the CLI or OS-E Management System **delete** command.

Basic Network Topology

The following image illustrates a network topology using the OS-E with a directly-attached PC for initial setup, and the OS-E Management System for remote access using a graphical user interface.



Step 1. Configuring Basic IP Connectivity

Before you can manage an OS-E system remotely over the Internet using the OS-E Management System or over a Telnet or SSH connection, you need to locally assign an IP address to one of the Ethernet interfaces, **eth0**, **eth1, eth2,** or **eth3.** If you are setting up the device remotely, you will also need to configure an IP route, a route to a destination host or network, and a gateway IP address.

If you are using the OS-E Management System, you will also need to know the assigned IP address on one of the Ethernet ports to manage the OS-E configuration. The OS-E Management System application runs directly on the OS-E system over the Internet using the Internet Explorer Web browser.

The following CLI session creates and enables an IP interface named **192.168.124.5,** sets the static IP address and network mask, configures an IP route (if connecting remotely), and enables Web access on this IP interface. You will need to enable ICMP on the OS-E IP interface before you can use the **ping** command from your console to test the device as a responding node on the network. Use the **show -v** command to display the configuration.

CLI Session

```
NNOS-E> config box
config box> set hostname local2610
config box> config interface eth1
config interface eth1> config ip mgmt-int
Creating ‘mgmt-int’
config mgmt-int> set admin enabled
config mgmt-int> set ip-address static 192.168.124.5/24
config mgmt-int> config routing
config routing> config route internetGateway
Creating ‘route internetGateway’
config route internetGateway> set destination default
config route internetGateway> set gateway 192.168.124.3
config route internetGateway> return
config routing> return
config ip mgmt-int> config web
config web> set admin enabled
config web> set port 80
config web> return
config mgmt-int> config icmp
config icmp> set admin enabled
config icmp> top
config> save
config> show -v
```

Using the Setup Script

An optional configuration setup script called *cxc.setup* is now included with newly shipped systems. After installing a new system, you can run the script directly from the NNOS-E> prompt, as shown in the example session below.

The script presents a set of questions to help you with the initial system configuration. The information in the script includes the following:

- Local hostname
- IP interface names and addresses
- SSH and Web access
- Default route and any additional static routes per interface for remote management
- User-defined CLI prompt

Every OS-E system has a minimum of two Ethernet interfaces. Any Ethernet interface on the system can be used for management traffic, however, Oracle recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other OS-E systems. Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI Session

```
NNOS-E> config setup
set box\hostname: <name>
config box\interface: eth1
set box\interface eth1\ip a\ip-address: <ipAddress/mask>
config box\interface eth1\ip a\ssh (y or n)? n
config box\interface eth1\ip a\web (y or n)? y
config box\interface eth1\ip a\routing\route: <routeName>
set box\interface eth1\ip a\routing\route localGateway\gateway:
<ipAddress>
set box\cli\prompt: <newPrompt>
Do you want to commit this setup script (y or n) y
Do you want to update the startup configuration (y or n)? y
```

Note: The /cxc directory on the OS-E system may include vendor-specific scripts that address unique startup configuration requirements. Specify the name of the script on the command line following the **config setup** command. For example:

```
NNOS-E> config setup vendor.setup
```

Check the /cxc directory for any vendor-specific setup files included with your system.

Enabling Network Access

To ensure you can manage the system using services such as Telnet or the OS-E Management System, you must configure the OS-E system so that it is available on the network. You need to create a default (or static) IP route, a route to a destination host or network, and a gateway IP address.

After you configure the static route, enable ICMP and then use the **ping** command at the top-level of the CLI to test network accessibility.

Defining a Default Route and Gateway IP

If you are setting the box remotely, you will need to configure an IP route, a route to a destination host or network, and a gateway IP address.

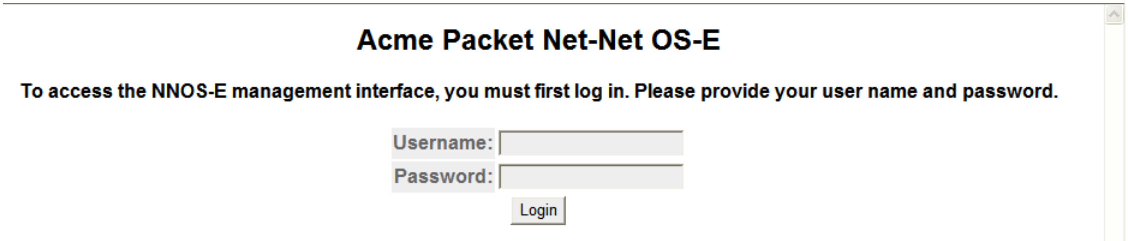
Refer to Step 1. Configuring Basic IP Connectivitythe previous section in this chapter, for the example CLI session that shows the routing context and the route named *internetGateway*. This is the default route that uses 192.168.124.3 as the default gateway.

Launching the OS-E Management System

In addition to the CLI, you can use the OS-E Management System to configure the OS-E. To access the OS-E using the OS-E Management System, open an HTTP or secure HTTP window (HTTPS) to the IP address of the Eth0 port on the OS-E system. For example:

https://192.168.124.5

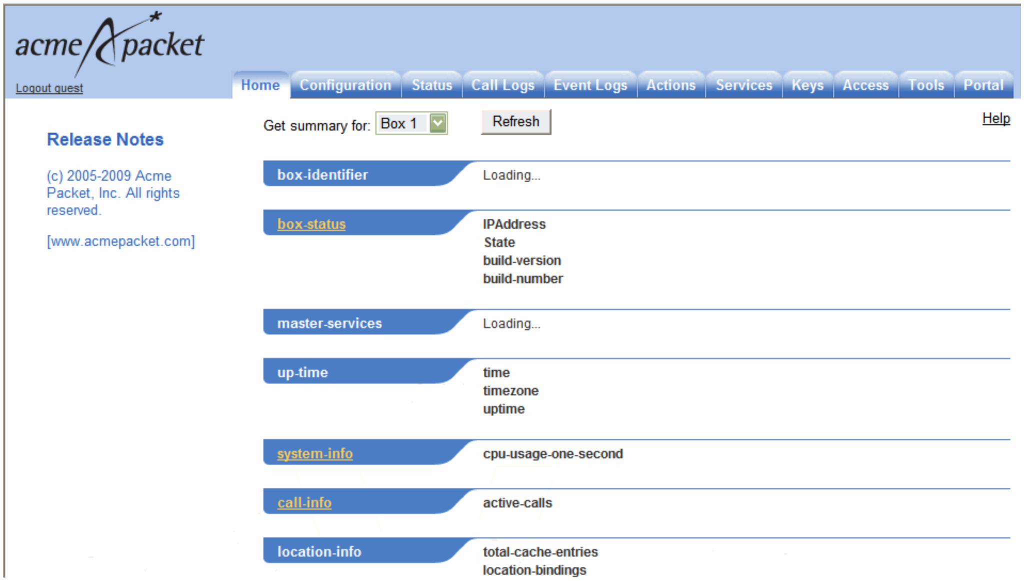
You should see the Oracle OS-E Log In window, illustrated in the following image.



Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

By default, there are no user accounts configured on a new system. This means any value can be entered in for username & password, or leave the fields blank and click **Login**. Once you log in, the OS-E Management System main page appears.



Release Notes

(c) 2005-2009 Acme Packet, Inc. All rights reserved.

[www.acmepacket.com]

box-identifier: Loading...

box-status: IPAddress, State, build-version, build-number

master-services: Loading...

up-time: time, timezone, uptime

system-info: cpu-usage-one-second

call-info: active-calls

location-info: total-cache-entries, location-bindings

The remaining steps in this chapter use the OS-E Management System to commission the OS-E.

Changing the Linux Root Password

To change the Linux root password, use the secret root action. When prompted, specify and confirm the new password. For example:

```
NNOS-E>secret root
password:*******
confirm:*******
```

```
Success!
NNOS-E>
```

Note: The password must be at least four characters long.

For more information on the **secret root** action, see the *Oracle Communications Application Session Controller Objects and Properties Reference Guide*.

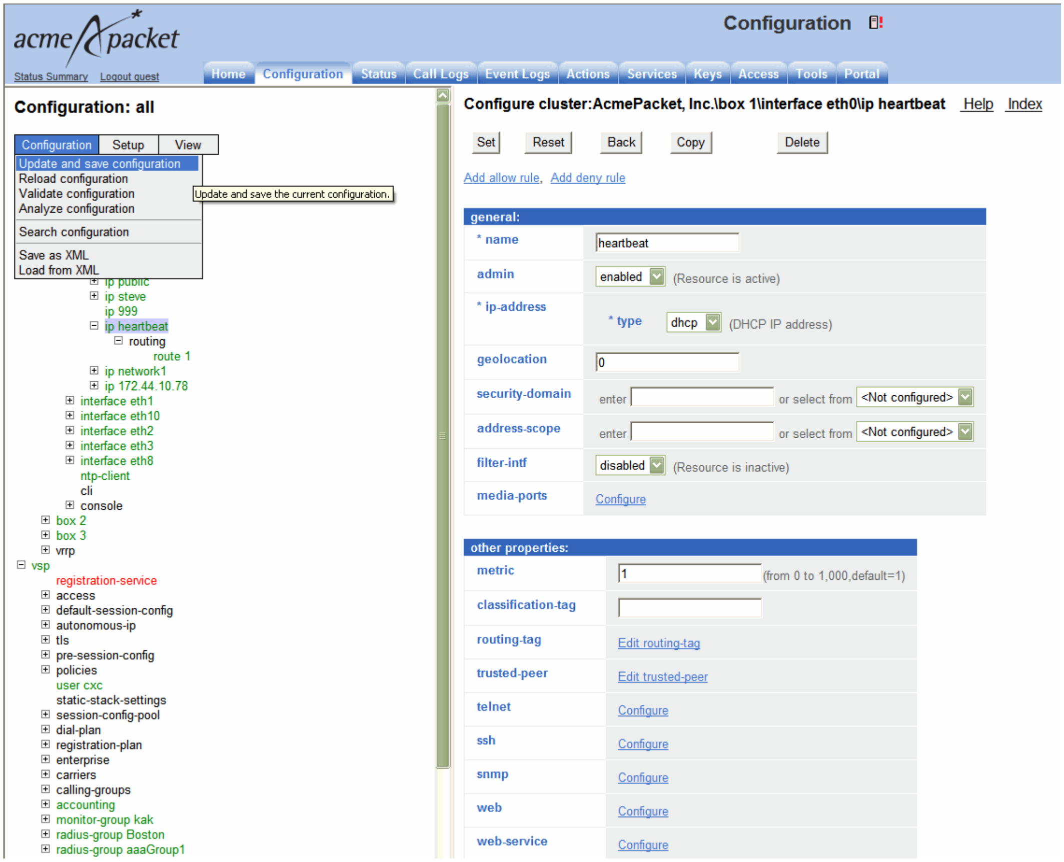
Step 2. Configuring Advanced IP Connectivity

Use the **Configuration** tab or the CLI to configure several additional Ethernet interfaces, as covered in Step 1. As a security device, the NN 2600 Series uses a default setting of **disabled** for these objects in the configuration file. This means that you must enable each interface. These objects include:

- **SSH**—To enable SSH client connectivity on the interface
- **Media ports**—To enable a range of port numbers for on the interface
- **SIP**—To enable SIP traffic on the interface)

When editing Ethernet interface and examining each object using the OS-E Management System, note that many of the objects are already visible, but they are not yet enabled. For these objects to actually be enabled on the OS-E system, you must select the object and save the configuration.

After editing an interface configuration, elect **Set**, then **Update & save configuration**, as illustrated in the following image.



Configure cluster:AcmePacket, Inc.\box 1\interface eth0\ip heartbeat

general:

* name	heartbeat
admin	enabled (Resource is active)
* ip-address	* type dhcp (DHCP IP address)
geolocation	0
security-domain	enter or select from <Not configured>
address-scope	enter or select from <Not configured>
filter-intf	disabled (Resource is inactive)
media-ports	Configure

other properties:

metric	1 (from 0 to 1,000,default=1)
classification-tag	
routing-tag	Edit routing-tag
trusted-peer	Edit trusted-peer
telnet	Configure
ssh	Configure
snmp	Configure
web	Configure
web-service	Configure

When you select **Configuration/Update and save configuration** you will be asked "Do you want to update the live configuration?" followed by "Do you also want to save the live configuration?" Click **OK** for both questions to ensure that the configuration is properly saved to the OS-E configuration file, *cxc.cfg*.

The following steps are necessary to set some specific parameters for the objects listed above:

1. Select the Configuration **Cluster/ Box 1/Interface Eth0/IP local** object on the left menu tree. Under the **General** field, edit the Media Ports properties as desired, then click **Set**.

2. Under the **Other Properties** field, edit the SSH properties. Accept the defaults by clicking **Set**.

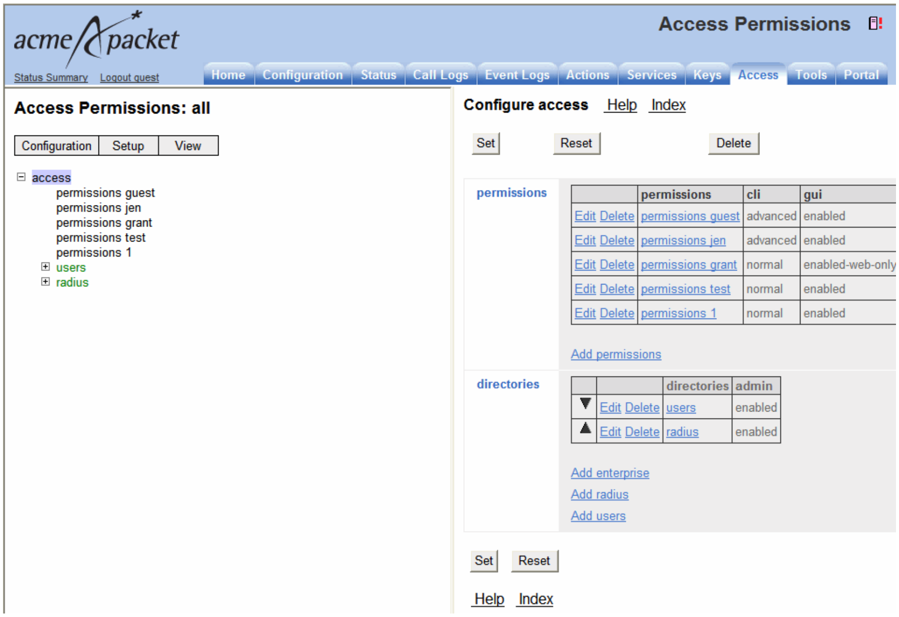
3. Select **SIP** from the menu tree. Enter the following values for each fields:
    - admin: enabled (default)
    - NAT translation: disabled (default)
    - UDP port: Select **Add UDP port**, accept the defaults, then click **Finish->Set**.
    - TCP port: Select **Add UDP port**, accept the defaults, then click **Finish->Set**.
    - TLS port: Select **Add UDP port**, accept the defaults, then click **Finish->Set**.
    - Certificate: blank (default)

When you are finished editing the SIP fields, select **Set->Configuration/Update and save configuration**.

Step 3. Creating User Accounts for Basic Access

By default, the OS-E does not contain any predefined user accounts. This means it is possible to access the management interfaces without entering any login credentials (username and password). You are not required to create user accounts, but it may be desirable for security reasons. If you want to create a user account at this time, follow the steps below. If not, go directly to Step 4.

1. Using the OS-E Management System, select the **Access** tab, then select **Access** from the left menu pane. The Access Permissions/Configure Access page appears.



	permissions	cli	gui
Edit Delete	permissions guest	advanced	enabled
Edit Delete	permissions jen	advanced	enabled
Edit Delete	permissions grant	normal	enabled-web-only
Edit Delete	permissions test	normal	enabled
Edit Delete	permissions 1	normal	enabled

		directories	admin
▼	Edit Delete	users	enabled
▲	Edit Delete	radius	enabled

2. Under **permissions**, select **Add permissions** and create a permissions group called *super-user* and accept all default settings with all permission types enabled.

   Select **Set**, then select **Update and save configuration** from the Configuration pull-down in the left pane**.**

3. From the **Directories** object, select **Add users**. Accept the default setting of enabled.

4. Select **Add user** and enter the required **name** and **password** of your choice, then re-enter the password to **confirm** your original password entry. In the **permissions** field, choose the permissions group that you just created (super-user).

5. Click **Create.** Select **Configuration->Update and save configuration**.

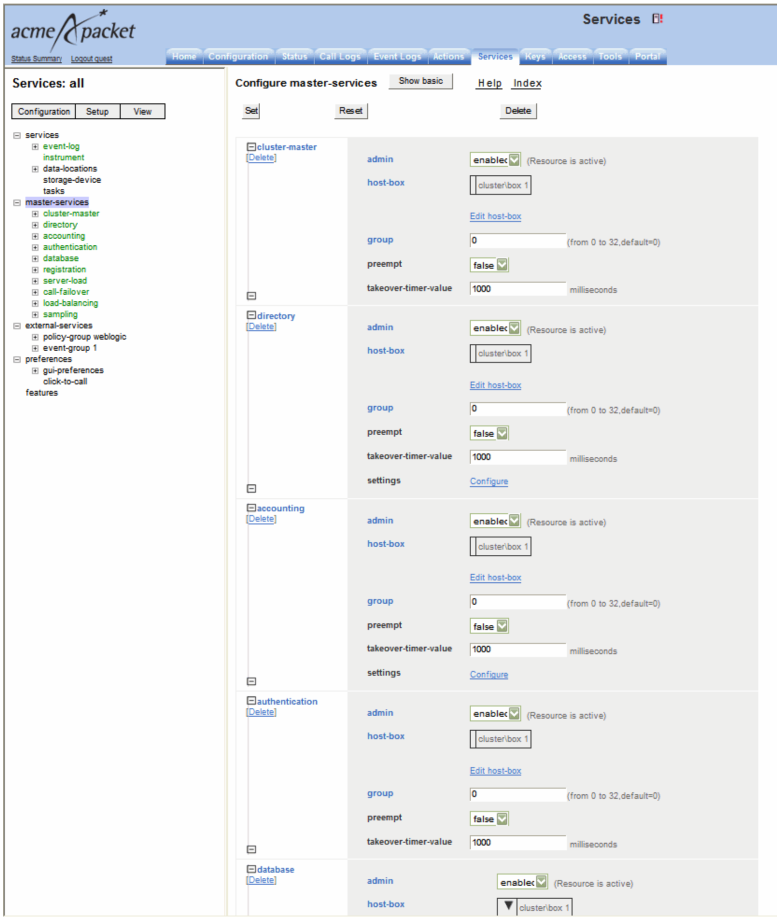
These steps created a username and password for a super-user account. Future attempts to log in to the OS-E (using the CLI or the OS-E Management System) will require that you specify these login credentials. If needed, you can also create user accounts with one or more of the super-user permissions.

Step 4. Enabling Master Services

The **master-services** configuration enables directory, accounting, database and registration services to run on the system. Perform the following steps to configure these master services:

1. Select the **Services** tab, then select **master-services** form the left menu pane.
2. Accept the default settings for **cluster-master**, **directory, accounting**, **database** (with **Show advanced** button selected), and **registration**. Click **Set**.

After you have configured all five services, select Configuration->**Update and save configuration**. The completed Master Services configuration should appear as shown in the following image.



cluster-master [Delete]
admin: enabled (Resource is active)
host-box: cluster\box 1
Edit host-box
group: 0 (from 0 to 32,default=0)
preempt: false
takeover-timer-value: 1000 milliseconds

directory [Delete]
admin: enabled (Resource is active)
host-box: cluster\box 1
Edit host-box
group: 0 (from 0 to 32,default=0)
preempt: false
takeover-timer-value: 1000 milliseconds
settings: Configure

accounting [Delete]
admin: enabled (Resource is active)
host-box: cluster\box 1
Edit host-box
group: 0 (from 0 to 32,default=0)
preempt: false
takeover-timer-value: 1000 milliseconds
settings: Configure

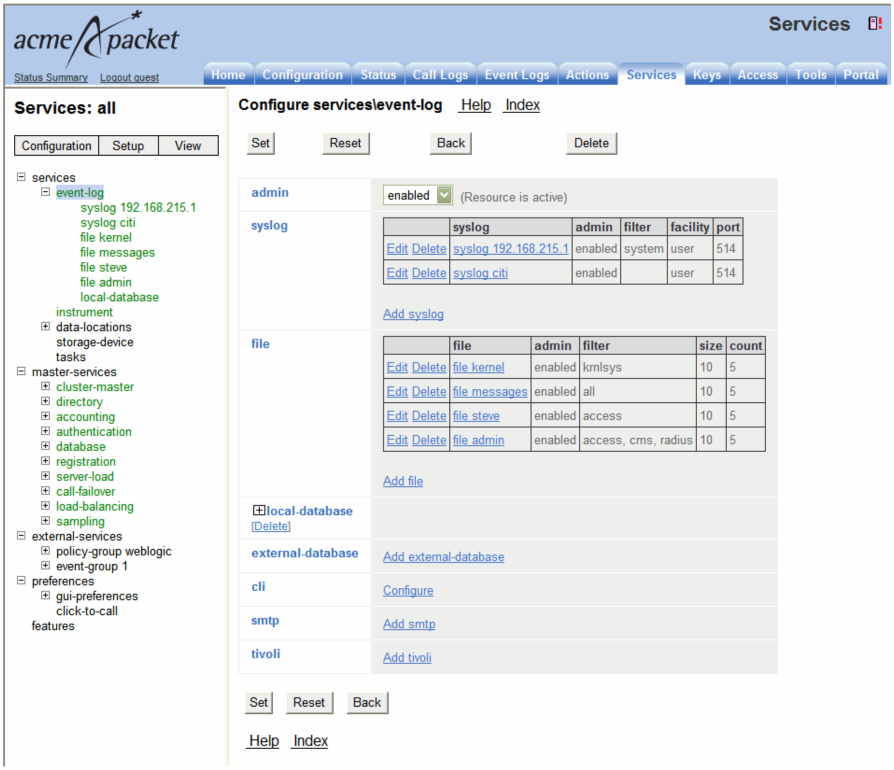
authentication [Delete]
admin: enabled (Resource is active)
host-box: cluster\box 1
Edit host-box
group: 0 (from 0 to 32,default=0)
preempt: false
takeover-timer-value: 1000 milliseconds

database [Delete]
admin: enabled (Resource is active)
host-box: cluster\box 1

Step 5. Configuring Basic Services

The **Services** configuration enables event logging and virus scanning services to run on the OS-E. Perform the following steps to configure event logging on the system.

1. Select the **Services** tab then select Services from the left menu pane.
2. On the Configure services page, select **event-log** from the menu pane, accept the defaults and click **Set**. Under the **event-log** configuration, additional options are available that you can configure, as illustrated in the following image.



Configure services\event-log

admin: enabled (Resource is active)

syslog:

	syslog	admin	filter	facility	port
Edit Delete	syslog 192.168.215.1	enabled	system	user	514
Edit Delete	syslog citi	enabled		user	514

Add syslog

file:

	file	admin	filter	size	count
Edit Delete	file kernel	enabled	krnlsys	10	5
Edit Delete	file messages	enabled	all	10	5
Edit Delete	file steve	enabled	access	10	5
Edit Delete	file admin	enabled	access, cms, radius	10	5

Add file

local-database [Delete]

external-database: Add external-database

cli: Configure

smtp: Add smtp

tivoli: Add tivoli

You can direct the event logs to one or more of the following locations:

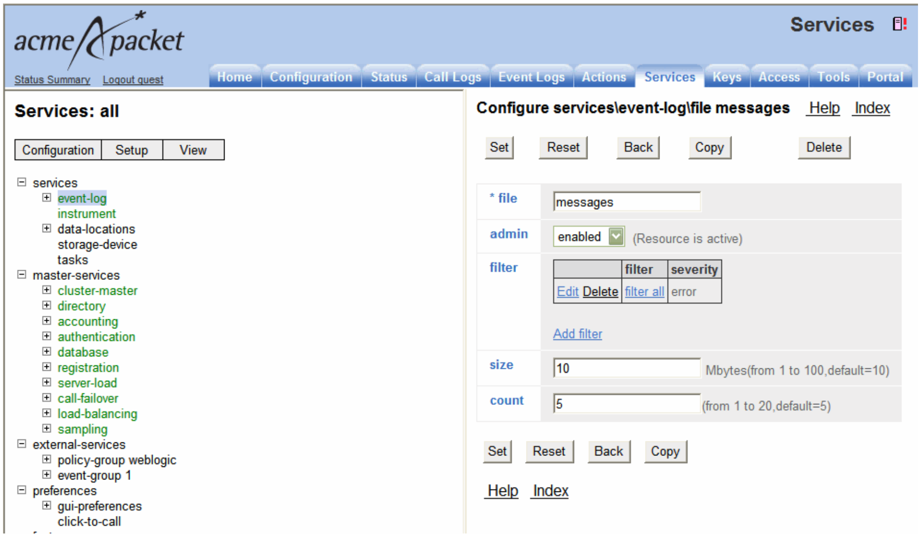
- A syslog server
- An ASCII file in an OS-E directory
- A database on the OS-E system
- An external database

The following image shows a configuration that specifies that logs should be directed to a syslog host (at 192.168.215.1), a local file on the system, and the local database. The syslog system will receive messages of the system severity (or lower). The local file is named *messages* is created in the log directory.

The configuration also shows two filters: the first filter captures events of the *system* class with **debug** severity level, and the second filter captures event messages that match the **error** severity level. Refer to the *Net-Net OS-E – System Administration Guide* for information about event logs, syslog, and event filters.

3. In the **file** object, click **Edit**, then enter the name *event-log* in the text block. Click **Set**.

   This configures event logging so that messages are written to the local file named *event-log*.



Configure services\event-log\file messages

* file	messages
admin	enabled (Resource is active)
filter	
size	10 Mbytes(from 1 to 100,default=10)
count	5 (from 1 to 20,default=5)

	filter	severity
Edit Delete	filter all	error

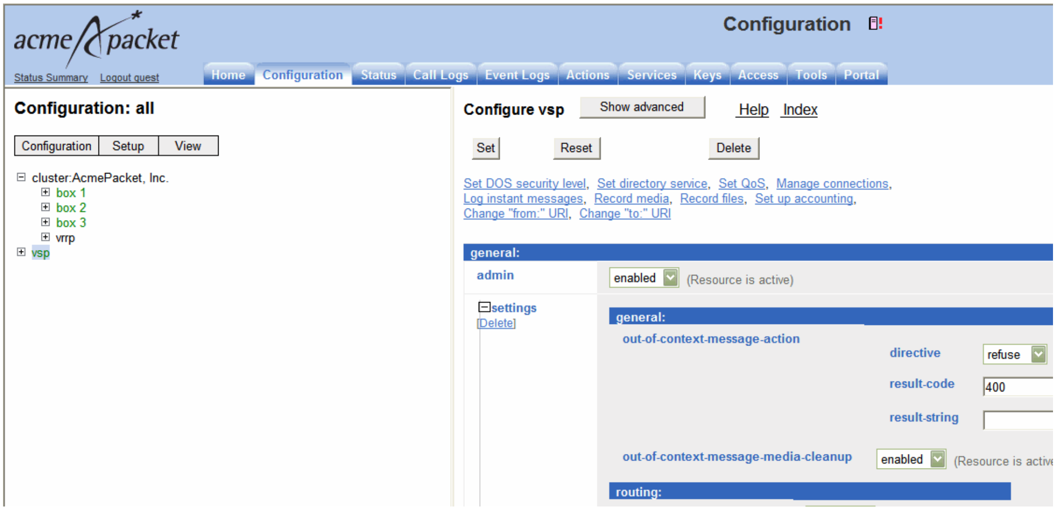
Add filter

Step 6. Enabling the Virtual System Partition (VSP)

The OS-E virtual system partition (VSP) is the part of the system that holds the comprehensive customer-defined configuration that controls how the system processes, stores, directs, and routes SIP traffic. The VSP is where you can create session configurations, registration and dial plans, and policies that handle SIP REGISTER and SIP INVITE traffic (and other SIP methods) that the system will receive and forward to a SIP call destination, authentication and accounting database, VoIP service provider or carrier, enterprise server, and so on.

Using the OS-E Management System, perform the following steps.

1. Select the **Configuration** tab, then select **vsp** from the menu to open the Configure vsp page, as illustrated in the following image.



Configuration: all

- cluster:AcmePacket, Inc.
  - box 1
  - box 2
  - box 3
  - vrrp
- vsp

Configure vsp

general:

admin: enabled (Resource is active)

settings

general:

out-of-context-message-action
- directive: refuse
- result-code: 400
- result-string:

out-of-context-message-media-cleanup: enabled (Resource is active

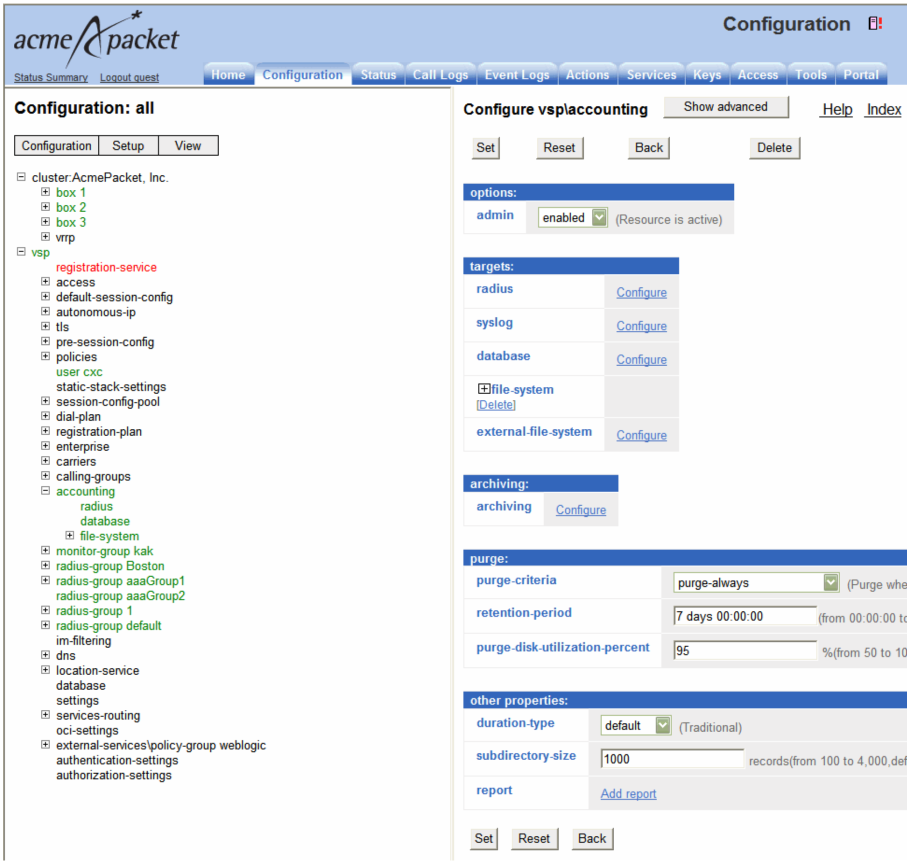
2. Under the general heading:, change the **admin** state to **enabled**.

3. Click **Set,** then select **Configuration->Update and save configuration**.

Step 7. Configuring the Accounting Environments

This step is necessary to configure the system to store call detail records and voice call recordings.

1. Select the OS-E Management System **Configuration** tab, then select **vsp->accounting** from the menu to display the Configure vsp\accounting page, as illustrated in the following image.



admin: enabled (Resource is active)

purge-criteria: purge-always (Purge whe

retention-period: 7 days 00:00:00 (from 00:00:00 tc

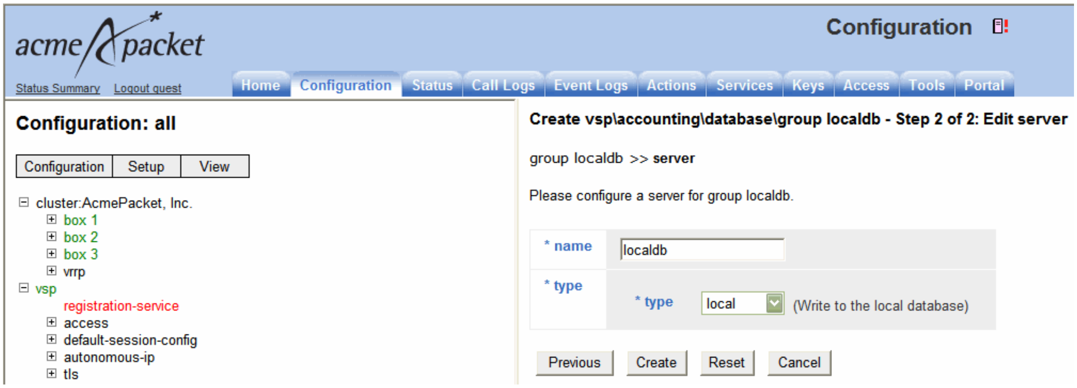
purge-disk-utilization-percent: 95 %(from 50 to 10

duration-type: default (Traditional)

subdirectory-size: 1000 records(from 100 to 4,000,def

2. Under **targets**, go to the **database** and set the **admin** property to enabled.

3. Select the database **Add group** command. The Edit group screen appears, as illustrated in the following image.



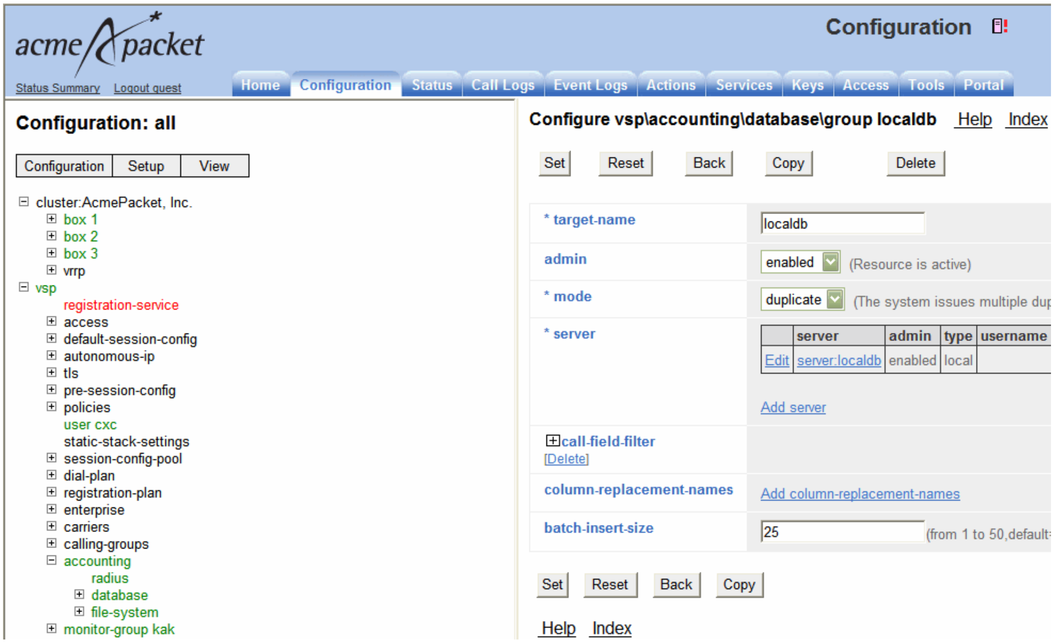
Create vsp\accounting\database\group localdb - Step 2 of 2: Edit server

group localdb >> **server**

Please configure a server for group localdb.

* name	localdb
* type	* type local (Write to the local database)

4. Enter *localdb* in the **target-name** field and select **Create** to display the Configure database group page**,** as illustrated in the following image..



Configure vsp\accounting\database\group localdb

* target-name	localdb
admin	enabled (Resource is active)
* mode	duplicate (The system issues multiple dup
* server	Add server
call-field-filter [Delete]	
column-replacement-names	Add column-replacement-names
batch-insert-size	25 (from 1 to 50,default

	server	admin	type	username
Edit	server:localdb	enabled	local	

5. Click **Edit** and configure the following settings:

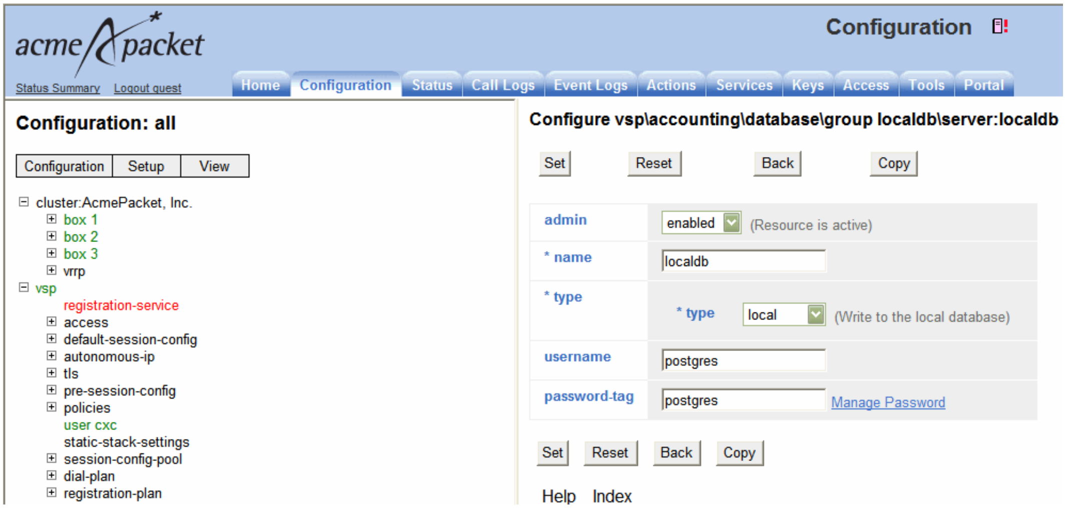
- **admin:** enabled
- **name:** localdb
- **type:** Select **local**

- **username**: postgres
- **password-tag:** postgres

Note: If you set the server **type** to *local*, using the local database as the accounting target, set the **username** and the **password-tag** to *postgres*. If you edit the **username** and **password-tag** properties to anything other than *postgres*, data will not be written to the database.

For information about password tags, refer to the *Net-Net OS-E – Objects and Properties Reference*.

6. Click **Set,** then select **Configuration->Update and save configuration**. The screen appears as illustrated in the following image.



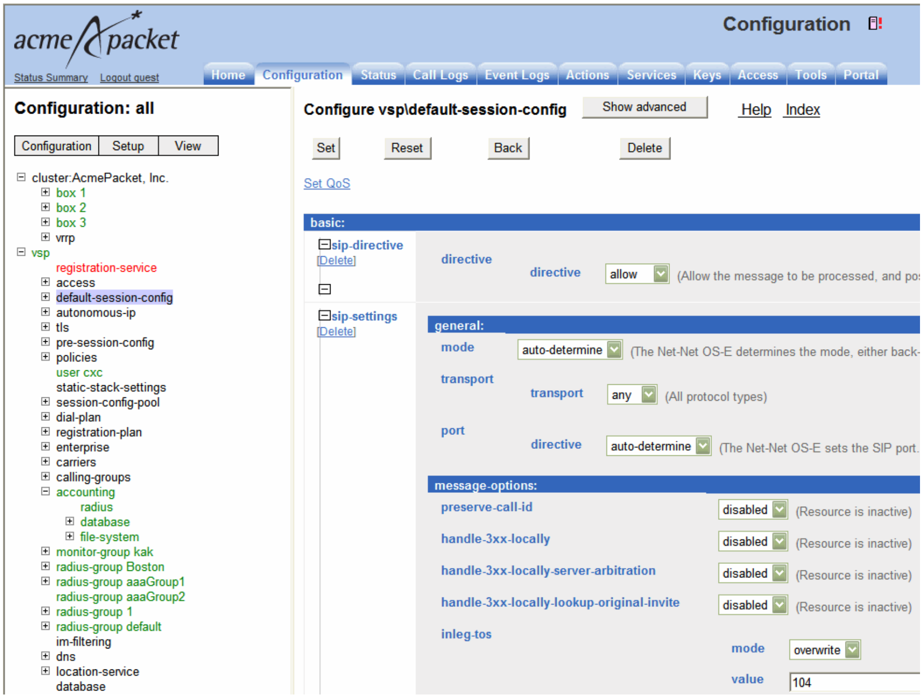
Configure vsp\accounting\database\group localdb\server:localdb

admin	enabled (Resource is active)
* name	localdb
* type	* type local (Write to the local database)
username	postgres
password-tag	postgres

Step 8. Editing the Default Session Configuration

Step 8 configures a default system policy that allows the OS-E to process SIP traffic. By default, and for security purposes, the OS-E does not allow any SIP traffic to pass.

1. Select the Configuration tab, then select **vsp->default-session-config** from the menu to display the vsp/default-session-config page, as illustrated in the following image (top portion).



Configure vsp\default-session-config

cluster:AcmePacket, Inc.
- box 1
- box 2
- box 3
- vrrp
- vsp
  - registration-service
  - access
  - default-session-config
  - autonomous-ip
  - tls
  - pre-session-config
  - policies
  - user cxc
  - static-stack-settings
  - session-config-pool
  - dial-plan
  - registration-plan
  - enterprise
  - carriers
  - calling-groups
  - accounting
    - radius
    - database
    - file-system
  - monitor-group kak
  - radius-group Boston
  - radius-group aaaGroup1
  - radius-group aaaGroup2
  - radius-group 1
  - radius-group default
  - im-filtering
  - dns
  - location-service
  - database

basic:

sip-directive [Delete]
- directive
  - directive: allow (Allow the message to be processed, and po

sip-settings [Delete]

general:
- mode: auto-determine (The Net-Net OS-E determines the mode, either back-
- transport
  - transport: any (All protocol types)
- port
  - directive: auto-determine (The Net-Net OS-E sets the SIP port.

message-options:
- preserve-call-id: disabled (Resource is inactive)
- handle-3xx-locally: disabled (Resource is inactive)
- handle-3xx-locally-server-arbitration: disabled (Resource is inactive)
- handle-3xx-locally-lookup-original-invite: disabled (Resource is inactive)
- inleg-tos
  - mode: overwrite
  - value: 104

2. In the **sip-directive** object, change the directive policy to **allow**, if not already set. This allows SIP traffic to traverse the OS-E system. Click **Set**.

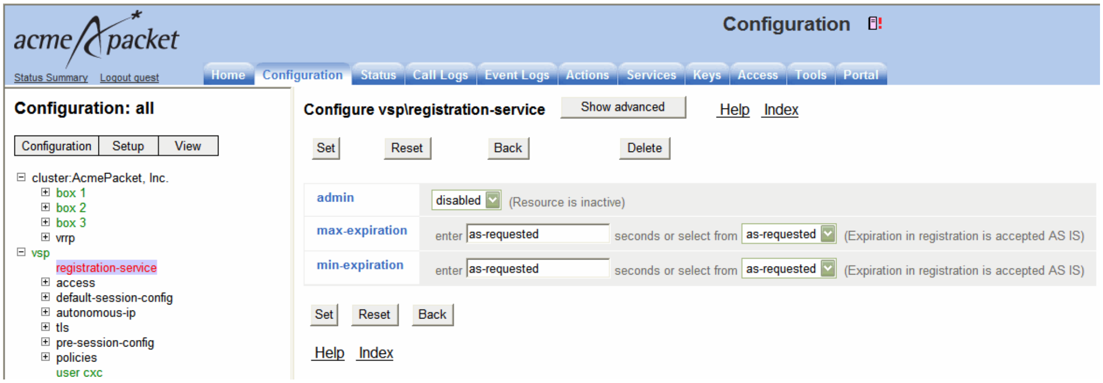
3. Scroll down to the **media** object. Change the **anchor** and the **recording-policy/record** properties to **enabled.** Accept all other default settings.

4. Click **Set**, then select **Configuration->Update and save configuration.**

Step 9. Enabling Registration Services

Step 9 enables the OS-E to handle SIP REGISTER sessions, allowing locally registered SIP clients to pass SIP sessions, as well as forward REGISTER sessions to upstream destination registrars.

1. Select the Configuration tab, then select **vsp/ registration-service** from the menu tree to display the vsp/registration-service page, as illustrated in the following image.



Configure vsp\registration-service

admin	disabled	(Resource is inactive)
max-expiration	enter as-requested seconds or select from as-requested	(Expiration in registration is accepted AS IS)
min-expiration	enter as-requested seconds or select from as-requested	(Expiration in registration is accepted AS IS)

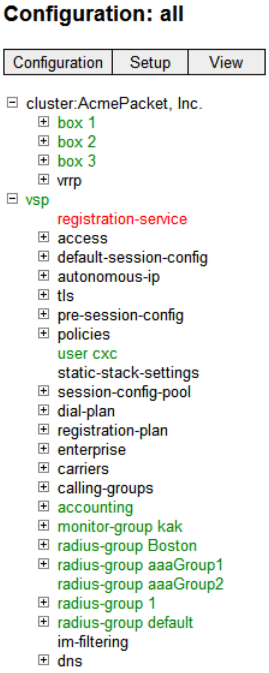
2. Accept the default settings and click **Set**. This enables the registration service on the OS-E system.

The OS-E will now provide support for basic SIP calls between locally registered clients.

Step 10. Reviewing the Configuration

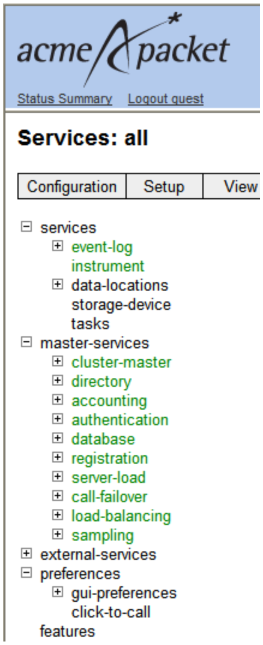
Once you have completed Steps 1 though 9, review the configuration to make sure it is accurate. A quick way to do this is to scan the OS-E Management System navigation tree to make sure there is an entry for each of the objects that you configured.

The following image is a listing of the Configuration and Services objects configured as part of basic OS-E commissioning. If you are using the CLI, run the **`show -v`** command from the NNOS-E prompt to display the configuration that you just created. The following image displays the configuration and services navigation trees.



Configuration: all

```
⊟ cluster:AcmePacket, Inc.
    ⊞ box 1
    ⊞ box 2
    ⊞ box 3
    ⊞ vrrp
⊟ vsp
      registration-service
    ⊞ access
    ⊞ default-session-config
    ⊞ autonomous-ip
    ⊞ tls
    ⊞ pre-session-config
    ⊞ policies
      user cxc
      static-stack-settings
    ⊞ session-config-pool
    ⊞ dial-plan
    ⊞ registration-plan
    ⊞ enterprise
    ⊞ carriers
    ⊞ calling-groups
    ⊞ accounting
    ⊞ monitor-group kak
    ⊞ radius-group Boston
    ⊞ radius-group aaaGroup1
      radius-group aaaGroup2
    ⊞ radius-group 1
    ⊞ radius-group default
      im-filtering
    ⊞ dns
```



Services: all

```
⊟ services
    ⊞ event-log
      instrument
    ⊞ data-locations
      storage-device
      tasks
⊟ master-services
    ⊞ cluster-master
    ⊞ directory
    ⊞ accounting
    ⊞ authentication
    ⊞ database
    ⊞ registration
    ⊞ server-load
    ⊞ call-failover
    ⊞ load-balancing
    ⊞ sampling
⊞ external-services
⊟ preferences
    ⊞ gui-preferences
      click-to-call
  features
```

Chapter 4. Installing Net-Net OS-E Clusters

About This Chapter

This chapter provides information on how to install an OS-E cluster, a group of OS-E systems that operate together to support redundancy and failover, high-availability, load balancing, and configuration.

Net-Net OS-E Cluster Overview

A “high-availability” cluster is a group of OS-E systems that provides a single point of configuration management, and at the same time, expands functionality across multiple devices participating in the cluster. An OS-E *master* manages the configuration for the entire cluster. All members of the cluster share network resources, network load, media ports and streaming, registration, and other processes.

OS-E systems within a cluster may be geographically dispersed in the network. A cluster recovers from the failure of one or more cluster members through health monitoring, shared master services migration, and network redundancy using the Virtual Router Redundancy Protocol (VRRP).

A cluster can be set up to operate as a two-system primary/standby redundant configuration.

Cluster Operations and Services

In the two-system redundant configuration, one OS-E system is the active master, performing signaling & media processing, and the other OS-E system is available as a standby system for the signaling & media processing if the master fails. Master failover allows another OS-E system to assume the master role in the cluster should the originally configured master become unavailable. VRRP is responsible for handling the failover from the master to the backup device.

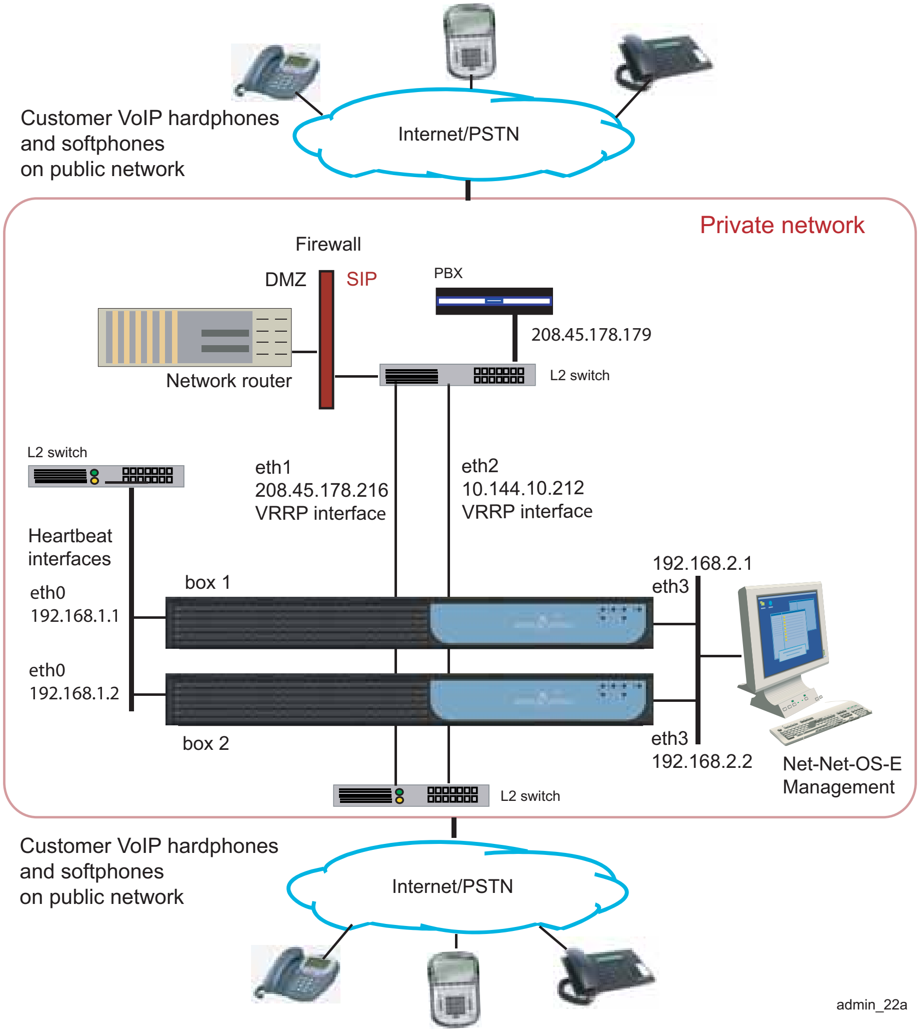
Master-Services

The **master-services** configuration is responsible for mirroring the state of the cluster to allow reliable failover to a standby device. The following sections describe the suggested settings for the **master-services** objects:

Cluster-Master

A **cluster-master** configuration on the OS-E system designated as the master is responsible for passing configuration changes to cluster members. A secondary property called **takeover-timer-value** specifies the number of milliseconds (such as 500) that the master-service stays in “awaiting takeover” mode at boot time.

Use the **show -v** command to display the **current takeover-timer** value. When the OS-E boots, each hosted master-service waits for this period to determine if any existing devices in the cluster are already running that service before assuming mastership.



admin_22a

Directory

When enabled, directory services allows the OS-E master to use enterprise (or corporate) directories that contain the identities of SIP users who are authorized to access the SIP enterprise communications servers.

In environments running CSTA, it is necessary to link the **directory** master service into a VRRP group with an interface to reach a Broadsoft OCI server. If the directory service is running on an OS-E system that cannot reach the OCI server, the CSTA-to-OCI translation will not function. Use a **takeover-timer-value** of 500 milliseconds.

Accounting

When enabled, accounting services supports RADIUS accounting, system logging (syslog), DIAMETER protocol services, the accounting database, and the accounting file-system

Authentication

Authentication services enables or disables all authentication functions on the OS-E, such as RADIUS and local user profiles. If authentication is disabled, you can still configure the authentication services, but the services do not become active until you enable this master service.

It may be necessary to link the authentication service to VRRP interface(s) using a group configuration if the VRRP interface is used to contact the authentication servers. Use a **takeover-timer-value** of 500 milliseconds for authentication.

Database

The master-services **database** object allows you to configure maintenance and other settings for the OS-E system database. The OS-E database is the local repository for call accounting records and media files

The **database** master service should be on a backup OS-E system, with the secondary property **preempt** set to *true*. This will help maintain the data in one location in the event of a brief service outage.

The **preempt** property specifies whether the master-service should resume the mastership if it has gone down and then returned to operation. If set to *true*, the master resumes its position. If set to *false*, the backup service retains master control.

Server-Load

The master-services **server-load** object configures the OS-E to calculate server load. This object must be enabled if your dial plan arbiter rule settings use **least-load** as the routing algorithm option. (The arbiter rule property sets the criteria by which the OS-E selects the server to which it forwards calls.)

Configure the **server-load** master-service for outbound server load balancing or server based admission\emission control. Currently, the **server-load** master-service should be linked to the VRRP SIP signaling interfaces over a configured group.

Call-Failover

The **call-failover** master-service configures failover for the media and signaling streams. As a master-service, the configured host OS-E master distributes copies of the media and kernel rules to all backup devices in a cluster. The OS-E uses the database on the host box, but enabling **call-failover** ensures that there is an active copy of the database on another device in the cluster in the event of a failure.

Registration

Enabling the registration service allows the OS-E to accept SIP REGISTER requests in behalf of other SIP servers (called *registrar peers*) that reside in other domains.

The **registration** master-service configures the registration process for intracluster registration lookups. In a cluster, the registration database runs on the specified master and the selected backups. The **host-box** property establishes the master and selective mirroring. The first OS-E listed is the master, while subsequent devices have mirrored databases. The OS-E systems <u>not configured</u> with the **host-box** property use the local location cache instead of the registration database. The **registration** master-service must be enabled for load-balancing of SIP processing (across backing interfaces configured with the **sip** object) to function correctly.

Load-Balancing

The master-services **load-balancing** object configures OS-E systems to host the load-balancing master service. For detailed information, see Configuring Cluster Load Balancing.

File-Mirror

The master-services **file-mirror** object sets all participating OS-E systems to share particular files (the types of files shared are preset in the OS-E operating system), such as media recordings, log files, etc. The file-mirror master service distributes files to all OS-E systems listed as hosts for the service.

Once the files are mirrored, you can play them back from any OS-E system that functions as a host.

Least-Cost-Routing

The master-services **route-server** object sets the route-server master service, which manages the server process. The master service handles requests from local or remote OS-E systems for least cost route definitions.

For detailed information on the route-server, see the following manuals:

- *Net-Net OS-E – System Administration Guide*
- *Net-Net OS-E – Objects and Properties Reference*
- *Net-Net OS-E – Session Services Configuration Guide*

Sampling

The master-services **sampling** object opens the mechanism for setting the interval at which the OS-E samples operational aspects of the system for either:

- Display in the OS-E Management System, or
- For sending to an IBM Tivoli server

By setting sampling for a status provider, you can view data for that provider over a specified period of time. The OS-E supports two sampling targets—a Postgres SQL database and an IBM tivoli server. (Set the provider data sent to the target using the **status** and **provider** objects. See *Net-Net OS-E – Objects and Properties Reference* for more information on configuring these objects.)

Once you have enabled **sampling**, the master service stores the samples in its local database.

Third-Party-Call-Control (3PCC)

The master-services **3pcc** (third-party-call-control) object configures call control, allowing the OS-E or a CSTA client to control (become the third party) in a call. Specifically, this object controls the WAV files that the OS-E should play and the external status events reported to an external server for calls created by the OS-E.

For detailed information on CSTA, see the following manuals:

- *Net-Net OS-E – System Administration Guide*
- *Net-Net OS-E – Objects and Properties Reference*
- *Net-Net OS-E – Session Services Configuration Guide*

Heartbeat Interface, BOOTP, and Messaging

Use the Ethernet physical interface **eth0** as the heartbeat interface for the OS-E cluster. This interface is used by default for any backup OS-E system that you added to the cluster. The systems will perform a BOOTP request over that interface and you will be able to add these systems by creating an entry for each to the configuration, and then booting them.

Once an OS-E is a member of the cluster, that system will receive a saved configuration file (*cxc.cfg)* from the master. Each time the *cxc.cfg* file is saved on the master, the latest copy of the cxc.cfg file is sent to each device in the cluster. You will need to configure a messaging interface on each cluster member so that the master knows the interface over which members of the cluster will receive the cxc.cfg file.

Event Logging

Event logs are stored on each box individually and represent the events that occurred on that particular OS-E system. You configure event logging in the **services/ event-logs** configuration object. The recommended event log filters on a cluster are as follows:

- Local-database all error
- File *name* system error
- File *name* krnlsys info
- File *name* system info

- File *name* db info

Network Time Protocol (NTP)

Ensure that you have NTP configured on all OS-E systems, ensuring that they point to a timeserver which will keep their time synchronized. DO NOT use a VRRP interface as your route to the timeserver, since one device will always have the VRRP interfaces down and will not be able to contact the NTP server.

If you do not have access to an external NTP server, configure one of the clustered OS-E systems to be an NTP server for the other cluster members. It is important to run NTP, as the time on all clustered system must be kept synchronized. If the times on the OS-E systems drift apart, the Denial of Service (DOS) software will not function properly, as timestamps are required to make this work across the cluster.

You can configure the NTP-server on the messaging interface on one OS-E system, and have all other devices point to this IP address in their NTP-client configuration.

Cluster Redundancy Operations

The OS-E cluster redundancy operates as follows:

- Internal messaging is exchanged so that each OS-E system knows the state of the other boxes, either up or down.
- If the active cluster master goes down, the box listed next in the list of cluster masters becomes the active cluster master. (Note that mastership does not automatically go back to the original system when it returns to service.)
- All the other master services work similarly, with an ordered list of devices that can run the service and the active service running on the next device in the list if the active master fails.

If an OS-E system fails, another device in the cluster will assume its network interfaces using VRRP.

Notes on Cluster Management

The OS-E cluster management operates as follows:

- Within a given cluster, one box functions as the active cluster master.

- Configuration and management of all boxes within a cluster is performed through the cluster master.
- There are no limitations on how many boxes within the cluster can be configured as backup cluster masters or backups for any of the master services.
- The configuration contains a list of boxes that can be cluster masters. The ordering of this list reflects the order in which boxes attempt to become master (i.e. the box listed first becomes the initial master, if that box fails then the next box in the list attempts to become the master, etc.)
- The OS-E Management System connects to the cluster master and provides a single point of management for the following:
  - Configuration
  - Status reports
  - Call logs
  - Accounting data
  - Actions
- The CLI provides single point of management for configuration using the CLI on the cluster master. The CLI is still available on all the other devices in the cluster, so any CLI commands can be executed on individual boxes.
- Note that the management functionality available from a given cluster is dependent on the functionality being performed by that cluster. For example, call logs are available only on clusters where signaling is performed; media recordings are available only on clusters where media streaming is performed.

Cluster Installation Prerequisites

Before beginning the cluster installation, ensure that any L2/L3 switch supporting the cluster has the Port Fast, Fast Link, or similar feature turned on. This allows the switch to run the Spanning Tree 802.1 protocol so that the switch ports being used by the OS-E go directly to the “forwarding” state. If the switch does not support Port Fast or Fast Link, disable the Spanning Tree protocol for the VLANs associated with the switch ports being used by the OS-E.

Cluster Installation Procedure

There are a number of steps that you need to follow to install an OS-E network cluster. You will need to know certain information about all the systems in the cluster for proper operation.

Each step uses a sample CLI session of commands that best illustrate how to best configure important settings.

1. Determine the specific OS-E system to assume the role of cluster master. Configure **master-services** to specify the device the cluster to assume initial mastership.

```
NNOS-E> config master-services
config master-services> config cluster-master
config cluster-master> set admin enabled
config cluster-master> set host-box cluster\box 1
config cluster-master> set host-box cluster\box 2
config cluster-master> set group 1
config cluster-master> return
```

2. Note the MAC address (identifier) on each device in the cluster. The MAC address is on a sticker on the back of the system. Write down each MAC address on a pad or piece of paper.

   On each device, if there is no sticker present, attach a laptop or standard PC to the system console port and perform the following steps:

   — Power up the system

   — At the NNOS-E prompt, execute the **show interface-details eth0** command to display the MAC address.

3. Attach a console to the cluster master and power up the OS-E system.

4. Configure the cluster master by configuring the Ethernet interfaces, IP addresses, and protocols. Ethernet interface eth0 is the “heartbeat” interface for the cluster. Use the eth0 interface on each OS-E system as the connection to the cluster.

```
NNOS-E> config cluster
config cluster> config box 1
config box 1> set identifier 00:04:23:d7:9f:34
config box 1> config interface eth0
config interface eth0> config ip heartbeat
Creating ‘ip heartbeat’
config ip heartbeat> set ip-address static 192.168.1.1/24
config ip heartbeat> config telnet
config telnet> return
config ip heartbeat> config ssh
config ssh> return
config ip heartbeat> config bootp-server
config bootp-server> return
config ip heartbeat> config vrrp
config vrrp> return
```

➡ **Note:** Optionally, you can run the **config setup** script to configure the IP addresses, management port, and other settings presented in the script.

By configuring messaging on the OS-E master, the master looks through the configurations of all other devices to find out which interface is used for messaging. (If multiple interfaces are configured, the master only communicates with one—the first it finds.) The master then communicates with the identified interface to share configuration and data.

```
config ip heartbeat> config messaging
config messaging> set admin enabled
config messaging> set certificate vsp tls
  certificate 208.45.178.216.pfx
config messaging> set port 5312
config messaging> set protocol tls
config messaging> return
config ip heartbeat> return
config interface eth0> return
config box 1>
```

Configure the interface and the protocols over which you will run management sessions to the OS-E. This is an “out-of-band” interface that allows you to separate management traffic from SIP signaling and media streams.

```
config box 1> config interface eth3
Creating ‘interface eth3’
config interface eth3> config ip mgmt
Creating ‘ip mgmt’
config ip mgmt> set ip address static 192.168.2.1/24
config ip mgmt> config ssh
config ssh> return
config ip mgmt> config web
config web> set protocol https 443 0
config web> return
config ip mgmt> config sip
config sip> set udp-port 5060
config sip> return
config ip mgmt> config icmp
config icmp> return
config ip mgmt> config media-ports
config media-ports> return
config ip-mgmt> return
config interface eth3> return
config box 1> config cli
config cli> set prompt nn2610-1
config cli> set banner ““
config cli> set display paged 50
config cli> return
config box 1> return
config cluster>
```

5. Configure the second OS-E system in the cluster. Note that you also configure eth0 as the “heartbeat” interface to the cluster.

```
   config cluster> config box 2
config box 2> set hostname nn2610-2
config box 2> set name ““
config box 2> set contact ““
config box 2> set location ““
config box 2> set identifier 00:04:23:c3:22:f4
config box 2> config interface eth0
config interface eth0> config ip heartbeat
config ip heartbeat> set ip-address static 192.168.1.2/24
config ip heartbeat> config telnet
config telnet> return
config ip heartbeat> config ssh
config ssh> return
config ip heartbeat> config web
config web> set protocol https 443 0
config web> return
config ip heartbeat> config icmp
config icmp> return
config ip heartbeat> config vrrp
config vrrp> return
config ip heartbeat> config messaging
config messaging> set admin enabled
config messaging> set certificate vsp tls
  certificate 208.45.178.216.pfx
config messaging> set port 5312
config messaging> set protocol tls
config messaging> return
config ip heartbeat> return
config interface eth0> return
config box 2>
```

Configure the interface and the protocols over which you will run management sessions. This is an “out-of-band” interface that allows you to separate management traffic from SIP signaling and media streams.

```
config box 2> config interface eth3
Creating ‘interface eth3’
config interface eth3> config ip mgmt
Creating ‘ip mgmt’
config ip mgmt> set ip address static 192.168.2.2/24
config ip mgmt> config ssh
config ssh> return
config ip mgmt> config web
config web> set protocol https 443 0
config web> return
config ip mgmt> config sip
config sip> set udp-port 5060
config sip> set nat-translation enabled
config sip> return
config ip mgmt> config icmp
config icmp> return
config ip mgmt> config media-ports
config media-ports> return
config ip-mgmt> return
config interface eth3> return
config box 1> config cli
config cli> set prompt NNOS-E-2
config cli> set banner ""
config cli> set display paged 50
config cli> return
config box 1> return
config cluster> set share media-ports true
config cluster> set share signaling-entries true
config cluster> set mirror-media-streams true
```

6. Configure VRRP on the OS-E interfaces to handle the public and private sides of the network. Note that the first VRRP interface connects the public side; the second VRRP interface connects the private side.

   A VRRP configuration for IP interfaces includes a list of box/interface pairings. The first pair in this list is the *primary interface*. The second pair in the list is the *backup interface* and will take over if the primary goes down. You can configure additional levels of redundancy by specifying more box/interface pairs of lower priority. Priority is based on the positioning of the **set host-interface** command.

```
config cluster> config vrrp
config vrrp> config vinterface vx0
config vinterface vx0> set group 1
...vinterface vx0> set host-interface cluster box 1 interface eth1
...vinterface vx0> set host-interface cluster box 2 interface eth1
config vinterface vx0> config ip public
Creating 'ip public'
config ip public> set ip-address static 208.45.178.216/28
config ip public> config ssh
config ssh> return
config ip public> config web
config web> set protocol https 443 0
config web> return
config ip public> config sip
config sip> set nat-translation enabled
config sip> set udp-port 5060
config sip> set tcp-port 5060
config sip> set tls-port 5061
config sip> set certificate vsp\tls\certificate 208.45.178.216.pfx
config sip> return
config ip public> config icmp
config icmp> return
config ip public> config media-ports
config media-ports> return
config ip public> config routing
config routing> config route default
Creating 'route default'
config route default> set gateway 208.45.178.209
config route default> return
config routing> return
config ip public> return
config vinterface vx0> return
config vrrp>

config cluster> config vrrp
config vrrp> config vinterface vx1
config vinterface vx1> set group 1
...vinterface vx1> set host-interface cluster box 1 interface eth2
...vinterface vx1> set host-interface cluster box 2 interface eth2
config vinterface vx1> config ip private
Creating 'ip private'
config ip private> set ip-address static 208.45.178.216/28
config ip private> config ssh
config ssh> return
config ip public> config web
config web> set protocol https 443 0
config web> return
config ip private> config sip
config sip> set nat-translation enabled
config sip> set udp-port 5060
config sip> set tcp-port 5060
config sip> set tls-port 5061
config sip> set certificate vsp\tls\certificate 208.45.178.216.pfx
config sip> return
config ip private> config icmp
config icmp> return
config ip private> config media-ports
config media-ports> return
config ip private> config routing
config routing> config route static-to-asx
Creating 'route static-to-asx’
config route static-to-asx> set destination network 208.45.178.0/24
config route static-to-asx> set gateway 10.144.10.254
config route static-to-asx> return
config routing> return
config ip private> return
config vinterface vx1> return
config vrrp> return
config cluster> return
```

7. Configure the master-services that you want to run on the cluster.

```
config> config master-services
config master-services> config accounting
config accounting> set host-box cluster\box 1
config accounting> set host-box cluster\box 2
config accounting> set group 1
config accounting> return
config master-services> config database
config database> set host-box cluster\box 1
config database> set host-box cluster\box 2
config database> set group 1
config database> set media enabled
config database> return
config master-services> return
config>
```

8. For TLS, you will need to upload the TLS certificate file on each OS-E system in the cluster. Copy the certificate that you receive from the CA to the OS-E using a compatible file transfer mechanism, such as PuTTY Secure Copy (PSCP). If you have the file on a local network PC, use PSCP to move the file to a directory path on the OS-E.

   The following example PSCP command copies the certificate file named **208.45.178.216.pfx** from the PC root directory to the OS-E system at IP address **208.178.216.pfx** in the directory **/cxc/certs/208.45.178.216.pfx**.

```
C:\ pscp -l root -pw sips -P 2200 208.45.178.216.pfx 208.45.178.216:/
    cxc/certs/208.45.178.216.pfx
```

   The following CLI session sets the directory and certificate file name path, specifies the passphrase, and whether to allow SSL Version 2 operability.

```
NNOS-E> config vsp
config vsp> config tls
config tls> config certificate 208.45.178.216.pfx
config certificate 208.45.178.216.pfx> set allow-sslv2 true
config certificate 208.45.178.216.pfx> set certificate-file /cxc/
    certs/208.45.178.216.pfx.pfx
config certificate 208.45.178.216.pfx> set passphrase-tag pass
```

   By default, the OS-E only supports SSLv3 or TLSv1. If you require SSLv2 for interoperability, set this property **true**. Specify the passphrase-tag associated with the certificate file. Use this property if the certificate file is encrypted to have its private key information protected. This passphrase tag must match the string with which the certificate was encrypted.

9. Power up the other OS-E systems in the cluster and connect them to the network. This initiates a configuration download from the cluster master so the systems acquire their initial configuration (IP addresses, etc.).

10. Use the CLI or OS-E Management System at the cluster master to configure any additional features. These features include the objects and settings under the VSP object, including:

- default-session-config
- registration-plan
- dial-plan
- enterprise servers, carriers, and gateways

Configuring External Messaging

Messaging is the mechanism the OS-E uses to communicate among boxes in a cluster. Messaging sets up a listening socket on an interface, enabling the interface to receive messaging traffic and participate in clustering and media partnering.

In a cluster, the master looks through the configurations of all OS-E systems to find out which interface is used for messaging. (If multiple interfaces are configured, the master only communicates with one—the first it finds.) The master then communicates with the identified interface to share configuration and data.

In media partnering, you configure a specific IP address (on a different box) as a partner. On the box that owns that IP address, you need to configure and enable messaging for media partnering to operate.

CLI Session

The following CLI session configures messaging on box 1, interface eth0.

```
NNOS-E> config cluster
config cluster> config box 1
config box 1> config interface eth0
config interface eth0> config ip boston1
config ip boston1> config messaging
config messaging> set admin enabled
config messaging> set certificate vsp tls certificate name
config messaging> set port 13002
config messaging> set protocol tls
```

Configuring Cluster Load Balancing

Load balancing of SIP processing across cluster interfaces requires both headend and backing interfaces. The *headend* interface is the central distribution point. It does not do any SIP processing, it only forwards the calls to its configured backing interfaces. When you configure a SIP phone, you would configure it to point to the headend interface.

To configure an IP interface as a headend interface, you simply configure the **sip** object with backing interfaces. Their presence contained within the IP configuration results in the interface being treated by the OS-E as a headend interface.

The *backing-interfaces* are identified as such within this **sip** object. In the **backing-interface** property, you reference previously configured IP interfaces. The backing interface is the location at which the OS-E terminates TCP and TLS connections (and where UDP transport messages arrive) and handles SIP processing. The OS-E uses round-robin load-balancing to distribute message across the configured backing interfaces.

To correctly configure load-balancing for SIP processing, you must do the following:

1. Configure the IP interfaces that will be used for both the headend and backing interfaces.
2. The SIP properties of the backing interfaces must match those of the head interface. For example, they must all use the same port assignments, and if you are using TLS, they must all use the same certificate.
3. You must enable the **master-services registration** object so that the interfaces can share the registration database.

To verify your configuration, first ensure that all SIP properties match. From the CLI at the headend, execute the **show load-balance** command. This lists all associated backing interfaces (and statistics). From each box hosting a backing interface, execute **show backing-interface** to display configuration and statistics information.

The following CLI session assumes that you have configured a three-box cluster, with box 1 containing the headend interface, with boxes 2 and 3 containing the backing interfaces over which traffic is load balanced. This session sets the backing interfaces for load balancing SIP traffic that is distributed from the headend interface at IP address 215.2.3.0/24.

CLI Session

```
config> config cluster
config cluster> config box 1
config box 1> config interface eth1
config interface eth1> config ip public
Creating 'ip public'
config ip public? set ip-address static 215.2.3.0/24
config ip public> config sip
config sip> config load-balancing
config load-balancing> set backing-interface cluster box 2 interface
   eth1 ip public
Creating 'cluster\box 2\interface eth1\ip public'
config load-balancing> set backing-interface cluster box 3 interface
   eth1 ip public

config sip> show
cluster
 box 1
  interface eth1
   ip public
    sip
     admin enabled
     backing-interface cluster\box 2\interface eth1\ip public2
     backing-interface cluster\box 3\interface eth1\ip public3
```

```
NNOS-E> show load-balance

Head-end IP 215.2.3.0:  undersubscribed:
------------------------------------------------------------------------------
Backing IP      State       Added   Removed   Maximum   Current  Percent
-------------------------------------------------------------------------
215.6.7.0       Down            0         0         0         0     0.0%
215.8.9.0       Down            0         0         0         0     0.0%
------------------------------------------------------------------------------
Totals:                         0         0         0         0   100.0%

NNOS-E>
```

Restarting an OS-E Cluster

You can perform a simultaneous warm restart of all systems in a cluster by using the **restart cluster** command. A warm restart simply restarts the OS-E applications on each system without rebooting the operating system.

If you warm restart an individual device in the cluster, the OS-E automatically rejoins the cluster when it comes back up. If that box is hosting a master service or a VRRP interface, the service or interface may fail over to a different OS-E system.

If you need to shut a system down by turning the power off, use the **restart halt** command before pressing the power button or disconnecting the power source. A **restart halt** will properly prepare a system for a shutdown. The OS-E system will rejoin the cluster when it comes back up.

Chapter 5. Installing Certificates and Commissioning TLS Networks

About This Chapter

This chapter provides information on commissioning the OS-E to run the Transport Layer Security protocol (TLS) over Ethernet interfaces.

TLS Overview

TLS is an encapsulation (and cryptographic) protocol that provides privacy and security between communicating applications over the Internet. The OS-E uses TLS to authenticate SIP users and to encrypt/decrypt SIP traffic across participating carrier and enterprise SIP applications.

For a complete description of the TLS protocol, refer to the following RFCs:

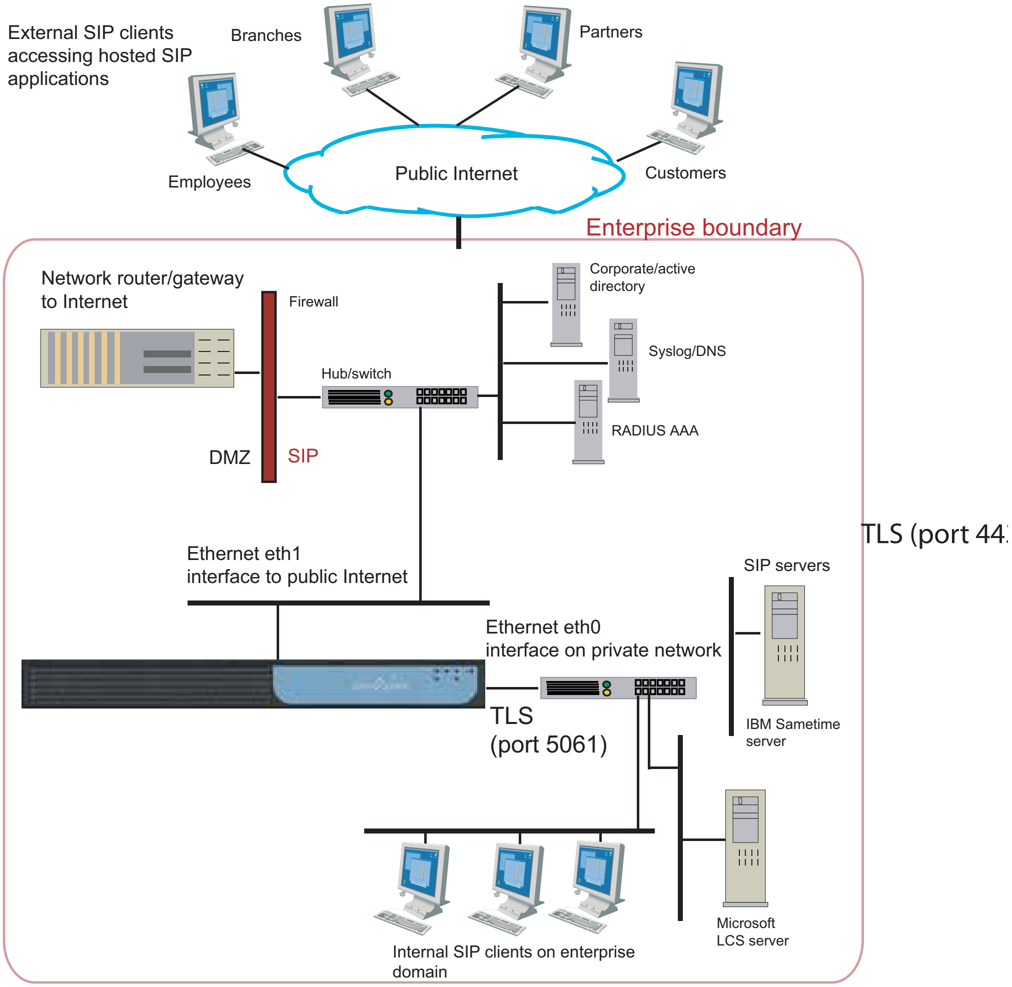
- RFC 2246, The TLS Protocol Version 1.0
- RFC 3261, Session Initiation Protocol (see Section 26.3.1)

The image below illustrates a sample network running TLS on Ethernet interfaces to both the private network and the public Internet.

Steps to Configuring TLS

To configure the private and public network interfaces in the image below, with TLS you need to perform the following steps:

1. If not already done, configure the management interfaces, network routes, protocols, and services using the **cluster/box**, **master-services**, and **services** objects.
2. If not already done, install a signed certificate from a valid Certificate Authority (CA). Go the section, “Before Configuring TLS.”.
3. Configure the certificate using the **tls/vsp** configuration object. Go to the section, “Configuring the Certificate on the OS-E.”
4. Configure the SIP protocol on each interface to use the installed certificate. Go to the section, “Configuring TLS on Ethernet Interfaces.”


External SIP clients accessing hosted SIP applications
Branches
Partners
Employees
Public Internet
Customers
Enterprise boundary
Network router/gateway to Internet
Firewall
Corporate/active directory
Syslog/DNS
Hub/switch
RADIUS AAA
DMZ
SIP
TLS (port 44
SIP servers
Ethernet eth1 interface to public Internet
Ethernet eth0 interface on private network
TLS (port 5061)
IBM Sametime server
Microsoft LCS server
Internal SIP clients on enterprise domain

➡ **Note:** If you are operating with Microsoft Live Communications Server (LCS), refer to the *Net-Net OS-E – System Administration Guide* for information on installing, importing, and exporting certificates.

Before Configuring TLS

You will need to install the required X.509 certificate(s) for the TLS protocol and SIP session establishment. A certificate includes the *.cer* certificate file name and the encrypted keys, mathematically related private and public data keys indexed by a unique name. A private key is kept secure—never displayed and never transmitted over the network. A public key, when bound to a fully qualified domain name (FQDN) by an authorized certification authority (CA), becomes an X.509 certificate.

If you do not have a certificate and encrypted key for your network, use this section to create and install a certificate. See the following table below for a summary of required steps.

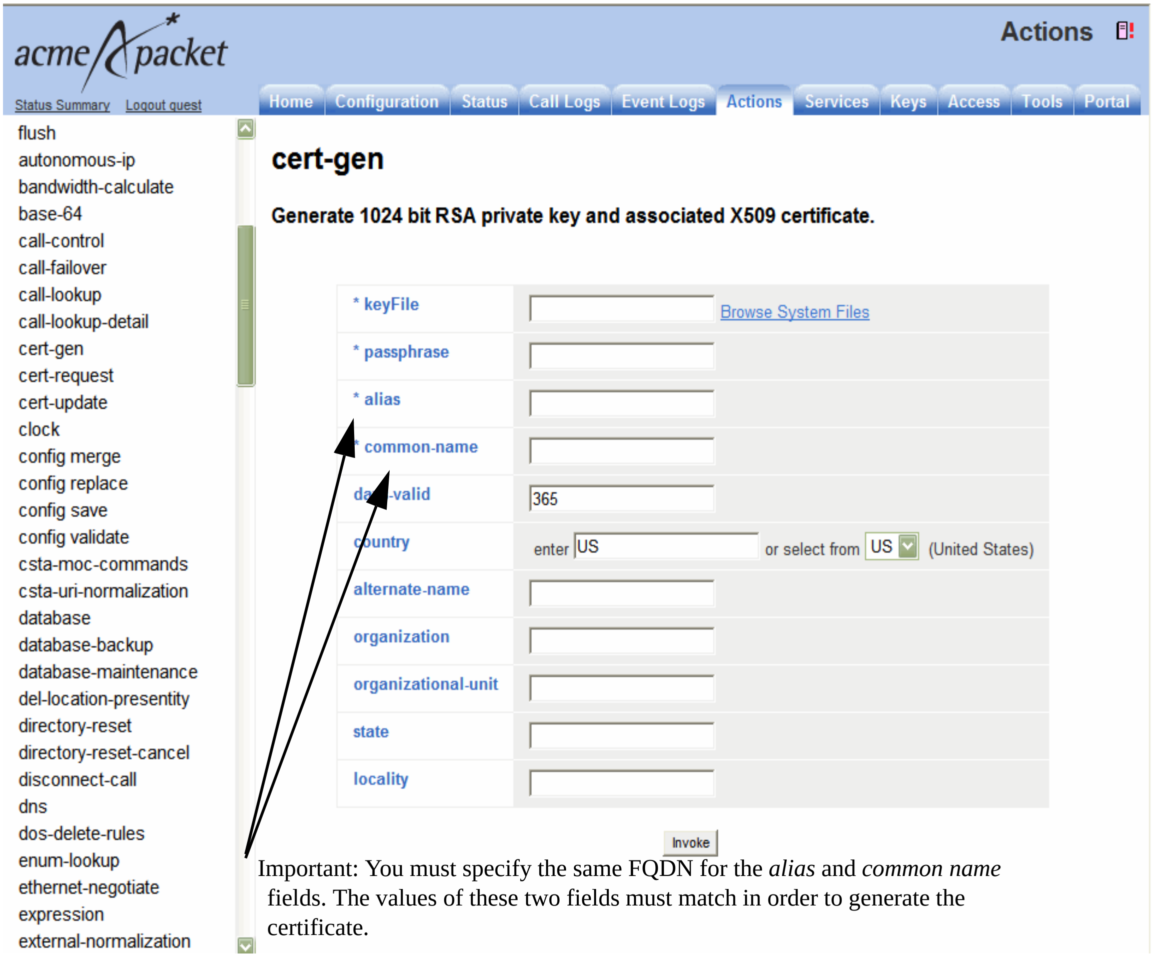
Task	See this section	CLI command
1. Using the OS-E software, create a self-signed X.509 certificate and encrypted key.	*Creating a self-signed certificate and key pair from the OS-E*	**`cert-gen`**
2. Using the self-signed certificate that you created in Step 1, generate a Certification Signing Request (CSR) in PEM format.	*Generating a Certification Signing Request (CSR)*	**`cert-request`**

Task	See this section	CLI command
3. Sign the CSR using one of these two methods: • Use a a valid CA, like VeriSign (required if a “trusted” certificate is necessary) to sign the CSR **or** • Use OpenSSL to sign the CSR	*Signing a CSR using either a valid CA or OpenSSL*	N/A
4. When you receive the signed certificate, use the OS-E software to load the signed certificate onto the system.	*Updating the self-signed certificate*	**`cert-update`**

Step 1. Creating a Self-Signed Certificate and Key Pair from the OS-E

Use the OS-E software to generate a cryptographic key pair and a self-signed X.509 certificate in PKCS#12 format. Once you create a self-signed certificate, you can generate the Certification Signing Request, a portion of which will be required by the CA upon submission of their form.

Under **Actions**, select **cert-gen** from list. The following image illustrates the OS-E Management System **Generate new key and certificate** page.



cert-gen

Generate 1024 bit RSA private key and associated X509 certificate.

* keyFile	Browse System Files
* passphrase	
* alias	
* common-name	
days-valid	365
country	enter US or select from US (United States)
alternate-name	
organization	
organizational-unit	
state	
locality	

Important: You must specify the same FQDN for the *alias* and *common name* fields. The values of these two fields must match in order to generate the certificate.

Complete the fields on the **Generate new key and certificates** page, as follows:

keyFile—Specify the name and directory path of the resulting key name that you want to use, along with the p12 or .pfx file extension. This is a mandatory field.

Example: /cxc/certs/myNetworkKey.p12

passphrase—Specify a password to be associated with the self-signed certificate. The text that you specify will be encrypted in the certificate.

alias—Specify the FQDN of the OS-E system using this certificate, such as *nn2610.acmepacket.com*. Omit HTTP:// and HTTPS://. This allows the certificate to be referenced.

➡ **Note:** The value (FQDN) you enter for the **alias** field must be identical to the value you enter for the **common-name** field.

common-name—Specify the FQDN of the OS-E system using this certificate, such as *nn2610.acmepacket.com*. Omit HTTP:// and HTTPS://. Do not use your personal name in this field. The common name is a component attribute of the certificate’s *distinguished name*.

days-valid—Enter the number of days for which the certificate is valid. If your certificate if effective for one year, then enter the number 365

country—Select the ISO country code: US (United States), AU (Australia), IN (India), IT (Italy), UK (United Kingdom), CA (Canada). The country is a component attribute of the certificate’s *distinguished name*.

alternate-name—Optional; this usually a name that complies with the ASN.1 specification, such as a DNS name, IP address, URI, etc.

organization—Optional. Enter the name under which your business is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request. If you are enrolling as a small business/sole proprietor, enter the certificate requestor's name in the “Organization” field, and the DBA (doing business as) name in the “Organizational Unit” field. The organization is a component attribute of the certificate’s *distinguished name*.

organizational-unit—Optional. Use this field to differentiate between divisions within an organization. For example, “Engineering” or “Human Resources.” If applicable, you may enter the DBA (doing business as) name in this field.The organizational unit is a component attribute of the certificate’s *distinguished name*.

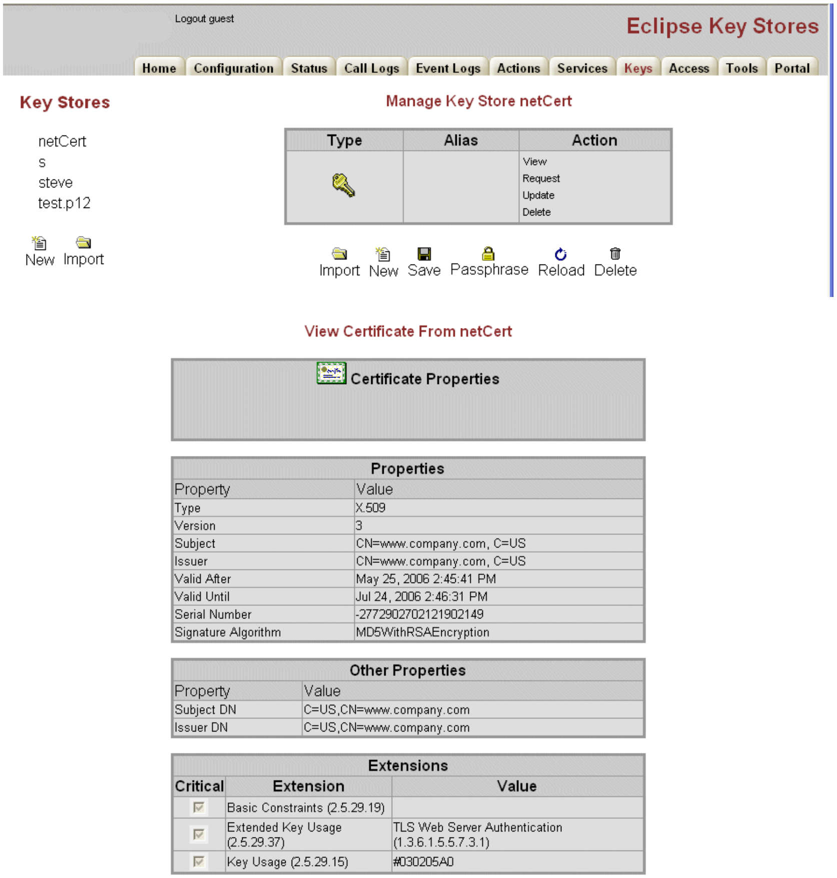
state—Optional; if in the US, enter one of the fifty state names in full where your organization is located, such as Massachusetts; if outside the US, enter the full name of a province or region.

locality—Optional; enter the name of a city.

When you are finished filling out the fields, click **Invoke**. The message line on the **Generate new key and certificate** page should report “Success.”

Viewing the Certificate

To view the self-signed certificate, select the **Keys** tab from the main menu bar, then select the keyFile that you just created from the Key Stores list on the left. Click View to display the Certificate Properties page, as shown in the following image.



Manage Key Store netCert

Type	Alias	Action
		View Request Update Delete

View Certificate From netCert

Certificate Properties

Properties	
Property	Value
Type	X.509
Version	3
Subject	CN=www.company.com, C=US
Issuer	CN=www.company.com, C=US
Valid After	May 25, 2006 2:45:41 PM
Valid Until	Jul 24, 2006 2:46:31 PM
Serial Number	-2772902702121902149
Signature Algorithm	MD5WithRSAEncryption

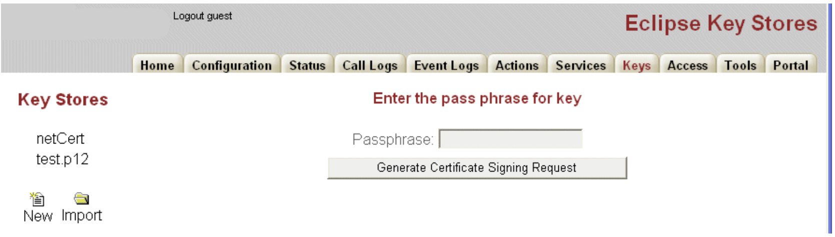
Other Properties	
Property	Value
Subject DN	C=US,CN=www.company.com
Issuer DN	C=US,CN=www.company.com

Extensions		
Critical	Extension	Value
☑	Basic Constraints (2.5.29.19)	
☑	Extended Key Usage (2.5.29.37)	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
☑	Key Usage (2.5.29.15)	#030205A0

Step 2. Generating a Certification Signing Request (CSR)

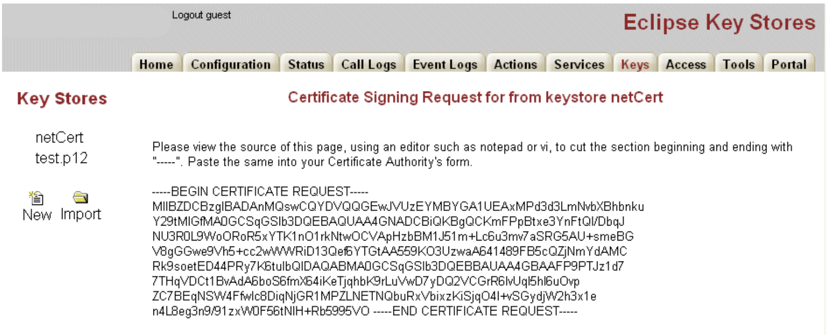
After you create the self-signed certificate from Step 1, you need to generate a certification signing request (CSR) that you can submit to the CA for the X.509 certificate. Select the **request** action.

The following image illustrates the Generate Certificate Signing Request page and the resulting certificate signing request. Enter the password that you created in Step 1 in the passphrase text box and click on **Generate Certificate Signing Request**.



Enter the pass phrase for key

Passphrase:



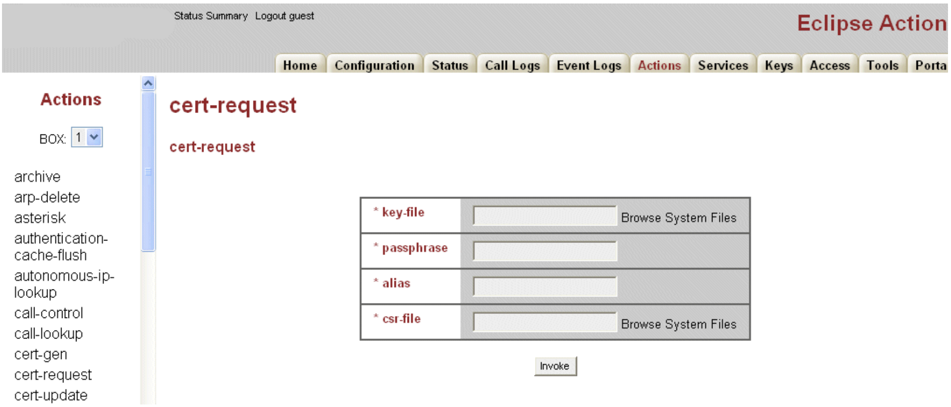
Certificate Signing Request for from keystore netCert

Please view the source of this page, using an editor such as notepad or vi, to cut the section beginning and ending with "-----". Paste the same into your Certificate Authority's form.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZDCBzgIBADAnMQswCQYDVQQGEwJVUzEYMBYGA1UEAxMPd3d3LmNvbXBhbnku
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKmFPpBtxe3YnFtQI/DbqJ
NU3R0L9WoORoR5xYTK1nO1rkNtwOCVApHzbBM1J51m+Lc6u3mv7aSRG5AU+smeBG
V8gGGwe9Vh5+cc2wWWRiD13Qef6YTGtAA559KO3UzwaA641489FB5cQZjNmYdAMC
Rk9soetED44PRy7K6tulbQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAAFP9PTJz1d7
7THqVDCt1BvAdA6boS6fmX64iKeTjqhbK9rLuVwD7yDQ2VCGrR6lvUql5hl6uOvp
ZC7BEqNSW4Ffwlc8DiqNjGR1MPZLNETNQbuRxVbixzKiSjqO4I+vSGydjW2h3x1e
n4L8eg3n9/91zxW0F56tNIH+Rb5995VO -----END CERTIFICATE REQUEST-----
```

Follow the instructions on the Certificate Signing Request page to copy and paste the text into the certificate application form provided by the CA.

If you choose to create a CSR in a PEM-formatted file, select the **cert-request** action. The file will contain the same request as shown in the following image.



Complete the fields on the **Generate Certification Request** page, using the same settings that you invoked from Step 1, as follows:

key-file—Specify the name and OS-E directory path of the resulting key name that you want to use, along with the p12 or .pfx file extension. This is a mandatory field. Example: /cxc/certs/myNetworkKey.p12

passphrase—Specify a password to be associated with the certificate issued by the CA. The text that you specify will be encrypted in the CSR.

alias—Optional. However, the value you enter for the **alias** field must be identical to the value you enter for the **common-name** field.

csr-file—Specify the name and directory path of the resulting CSR file. This is the file from which you will cut and paste the required information for the CA at the time that you submit the certificate request. By default, the CSR file resides in the directory named /cxc/certs.

When you are finished filling out the fields, click **Invoke**. The message line on the Generate Certification Request page should report “Success.”

Viewing the .CSR File

Since the .cer file is in PEM format, you can open the view the file using a text editor.

Step 3. Signing a CSR Using Either a Valid CA or OpenSSL

After you generate the CSR, you need to sign the CSR using *one* of two methods. You can either:

— Sign the CSR using a well-known CA, for example, VeriSign. (*See the instructions below).*

or

— Sign the CSR using OpenSSL.

This section describes how to sign the CSR using either method.

Note: If your network requires a "trusted" certificate, then follow the instructions below to sign the CSR using a valid, well-known CA.

Using a Certification Authority to Sign the CSR (Method 1)

You get the signed X.509 certificate from a valid CA, such as VeriSign. The CA issues a certificate stating and guaranteeing that the key contained in the certificate belongs to the person or organization noted in the certificate. The CA verifies the identify of the applicant's so that users can trust certificates issued by that CA to belong to the people and data identified in it, and not to an imposter

Certificate Formats

The OS-E certificate file can be in the following formats:

- PKCS#12—Public Key Cryptography Standard #12 format from Microsoft IIS Version 5 (binary)
- PEM—Privacy-enhanced mail (PEM) encoded format from any OpenSSL-based Web server (ASCII)

Using OpenSSL to Sign the CSR (Method 2)

This section provides information on how you can generate a self-signed certificate for testing TLS with the OS-E using OpenSSL. This is an alternative method to using a valid CA to sign the CSR.

This section describes how to do the following things:

- Create an OpenSSL Certificate Authority (CA).
- Generate a private key and CSR on the OS-E system and sign in with the OpenSSL CA.
- Generate a Private Key and CSR without the OS-E system (not supported).
- Use OpenSSL to convert an X.509 certificate and/or RSA key to a Public-Key Cryptography Standard #12 (PKCS#12) format.

Note: Before using this method, download the OpenSSL program and install it on a Unix/Linux or Windows system. You also need to add the location of the OpenSSL executables to the PATH. In a Windows environment, this will need to do this manually, requiring a reboot to take effect.

Creating an OpenSSL Certificate Authority (CA)

To create and Open SSL Certificate Authority (CA) on a Unix/Linux system, perform all steps as “root.” On a Windows system, perform all steps as “Administrator.”

1. **Create directories to store certificates.**

   The main CA folder is the directory where the **C**ertificate **A**uthority files will reside. The “private” directory stores the private keys. The “certs” directory stores the certificates (or public keys). The “csrs” directory stores the Certificate Signing Requests.

On Unix:

```
mkdir /CA
mkdir /CA/private
mkdir /CA/csrs
mkdir /CA/certs
```

Windows (cmd):

```
mkdir C:\CA
mkdir C:\CA\private
mkdir C:\CA\csrs
mkdir C:\CA\certs
```

2. **Create files to support the generation process.**

Create the “index.txt” file with no contents. This is the database to which OpenSSL keeps track of generated certificates generated. Create the “serial” file with a number so that each generated certificate is labeled with a number for tracking purposes.

Unix:

```
touch /CA/index.txt
echo 01 > /CA/serial
```

Windows (cmd):

```
copy con C:\CA\index.txt
echo 01 > C:\CA\serial
```

3. Create the OpenSSL configuration file.

Unix:

Using a text editor, create “/CA/openssl.cnf.”

```
[ ca ]
default_ca      = local_ca

[ local_ca ]
dir             = /CA
certificate     = $dir/certs/ca.cer
database        = $dir/index.txt
new_certs_dir   = $dir/certs
private_key     = $dir/private/ca.key
serial          = $dir/serial



default_crl_days        = 365
default_days            = 365
default_md              = md5

policy          = local_ca_policy
x509_extensions = local_ca_extensions

[ local_ca_policy ]
commonName              = supplied
stateOrProvinceName     = optional
countryName             = optional
emailAddress            = optional
organizationName        = optional
organizationalUnitName  = optional
```

```
[ local_ca_extensions ]
basicConstraints        = CA:true
nsCertType              = server

[ root_ca_extensions ]
basicConstraints        = CA:true
nsCertType              = server

[ req ]
default_bits    = 2048
default_keyfile = /CA/private/ca.key
default_md      = md5

prompt                  = yes
distinguished_name      = root_ca_distinguished_name
x509_extensions         = root_ca_extensions

[ root_ca_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = US
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = MA

localityName                    = Locality Name (eg, city)
localityName_default            = Maynard

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Acme Packet, Inc.

organizationalUnitName          = Organizational Unit Name
  (eg,section)
organizationalUnitName_default  = Support

commonName                      = Common Name (eg, YOUR name)
commonName_max                  = 64

emailAddress                    = Email Address
emailAddress_default            = jgentile@acmepacket.com
emailAddress_max                = 64

[ req_attributes ]
challengePassword               = A challenge password
challengePassword_min           = 4
challengePassword_max           = 20

unstructuredName                = An optional company name
```

Windows:

Using a text editor, create “C:\CA\openssl.cnf.”

```
[ ca ]
default_ca      = local_ca

[ local_ca ]
dir             = C:\CA
certificate     = $dir\certs\ca.cer
database        = $dir\index.txt
new_certs_dir   = $dir\certs
private_key     = $dir\private\ca.key
serial          = $dir\serial

default_crl_days        = 365
default_days            = 365
default_md              = md5

policy          = local_ca_policy
x509_extensions = local_ca_extensions

[ local_ca_policy ]
commonName              = supplied
stateOrProvinceName     = optional
countryName             = optional
emailAddress            = optional
organizationName        = optional
organizationalUnitName  = optional

[ local_ca_extensions ]
basicConstraints        = CA:false
nsCertType              = server

[ root_ca_extensions ]
basicConstraints        = CA:true
nsCertType              = server

[ req ]
default_bits    = 2048
default_keyfile = C:\CA\private\ca.key
default_md      = md5

prompt                  = yes
distinguished_name      = root_ca_distinguished_name
x509_extensions         = root_ca_extensions

[ root_ca_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = US
```

```
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = MA

localityName                    = Locality Name (eg, city)
localityName_default            = Maynard

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Acme Packet, Inc.

organizationalUnitName          = Organizational Unit Name (eg,
                              section)
organizationalUnitName_default  = Support

commonName                      = Common Name (eg, YOUR name)
commonName_max                  = 64

emailAddress                    = Email Address
emailAddress_default            = jgentile@acmepacket.com
emailAddress_max                = 64

[ req_attributes ]
challengePassword               = A challenge password
challengePassword_min           = 4
challengePassword_max           = 20

unstructuredName                = An optional company name
```

4. **Generate the CA's private key and Master Certificate (public key).**

   This step will generate two files:

   - **CA/private/ca.key** (**C:\CA\private\ca.key** on Windows) – This is the CA's private key used to sign certificates. Keep this secure. If this key is compromised, it can be used to create certificates for malicious purposes.
   - **CA/private/ca.cer** (**C:\CA\private\ca.cer** on Windows) – This is the CA's certificate (public key). This is the file that would be distributed to client's "Trusted Root" stores to trust any certificates signed by this CA's private key.

Unix:

```
openssl req -x509 -new -config /CA/openssl.cnf –days 3000 -out /CA/
certs/ca.cer
```

Windows (cmd):

```
openssl req -x509 -new -config C:\CA\openssl.cnf –days 3000 -out
   C:\CA\certs\ca.cer
```

The **ca.key** is created automatically based on the configuration file.

Enter a strong passphrase for the CA key. Remember it, as this helps protect the security of your CA.

Fill in the following fields:

```
Country Name (2 letter code) [US]: <your country>
State or Province Name (full name) [MA]: <your state/province>
Locality Name (eg, city) [Maynard]: <your locale>
Organization Name (eg, company) [Acme Packet]: <your company>
Organizational Unit Name (eg, section) [Support]: <your department>
Common Name (eg, YOUR name) []: <Use the FQDN of the CA system
  running OpenSSL>
Email Address []: <your email address>
```

Note: The "Common Name" field is the most important. This is the name that will be provided to the CA, so use the Fully Qualified Domain Name (FQDN) of the system on which you are running OpenSSL.

5. **Change permissions on the CA's key to only allow "root" access**:

Unix:

```
chmod 700 /CA/private/ca.key
```

Windows (cmd):

```
echo y|cacls C:\CA\private\ca.key /G %COMPUTERNAME%\Administrator:F
```

Note: You should only need to complete the process for setting up the CA) once, while the processes for signing Certificates must be repeated every time a certificate needs to be generated.

Generating a Private Key and Certificate Signing Request (CSR) with the OS-E

To generate a private key and CSR on the OS-E and sign in with the OpenSSL CA, perform the following steps:

1. **Create a CSR on the OS-E.**

   Refer to the section in the chapter, “Before Configuring TLS.”:

   - Use the **cert-gen** utility to generate a Self-Signed Certificate (known as a private key) in PKCS#12 format. In this example, the file name is *cxc.pfx***.**
   - Use the **cert-request** utility to generate a Certificate Signing Request (CSR) in PEM format on the appropriate OS-E system. In this example, the file name is *cxc.csr.*

Note: The “common-name” field on the “cert-gen” page is the most important. This is the name that will be used to validate the certificate. Use the Fully Qualified Domain Name (FQDN) of the appropriate OS-E system, such as nnose.acmepacket.com.

Currently, some phones, such as Eyebeam do not support wildcard certificates where the common-name uses an asterisk character (*) in the domain name, such as *.acmepacket.com.

These files are created in the **/cxc/certs/** directory on the OS-E.

2. **Copy the CSR to the OS-E.**

   Download the .csr file generated on the OS-E, and then copy it to the CA system into the **/CA/csrs/** directory. For a Windows system, copy it to the **C:\CA\csrs\** directory.

3. **Sign the CSR with your OpenSSL CA.**

Unix

```
openssl ca -config /CA/openssl.cnf -in /CA/csrs/cxc.csr –out /CA/
certs/cxc.pem
```

Windows

```
openssl ca -config C:\CA\openssl.cnf -in C:\CA\csrs\cxc.csr –out
C:\CA\certs\cxc.pem
```

Enter the pass phrase for the CA key

Respond “y” to the questions to generate and commit.

4. **Update the private key (cxc.pfx) with the signed public key (cxc.pem) on the system.**

   Upload the newly generated *cxc.pem* file back to the OS-E , as covered earlier in this chapter. Refer to the section in the chapter, “Before Configuring TLS.”

   - Use the **cert-update** utility to update the “/cxc/certs/cxc.pfx” file on the OS-E with the “/cxc/certs/cxc.pem” file.
   - Configure a TLS certificate, as covered earlier in this chapter. Be sure to associate it with the SIP protocol on the appropriate network interface.

Note: You can use the /CA/certs/ca.cer (C:\CA\certs\ca.cer on Windows) file to import into a “Trusted Root Store.” For example, you can install this in Windows (Internet Explorer) for use with Soft Phones, such as Eyebeam. If you deploy the ca.cer file to multiple systems into the “Trusted Root Store”, then those systems will “trust” any certificates signed by this CA.

Generating a Private Key and Certificate Signing Request (CSR) without the OS-E

Instead of generating the private key and CSR on the OS-E, you can generate it using OpenSSL exclusively. This is not the supported method.

1. **Create a CSR and Private Key for the OS-E System**

Unix:

```
openssl req -new -config /CA/openssl.cnf -out /CA/csrs/cxc_csr.pem
-keyout /CA/certs/cxc_pk.pem
```

Windows (cmd:)

```
openssl req -new -config C:\CA\openssl.cnf -out
C:\CA\csrs\cxc_csr.pem -keyout C:\CA\certs\cxc_pk.pem
```

Use the OpenSSL “req” utility to generate a Self-Signed Certificate (private key) and the Certificate Signing Request (CSR) in PEM format. In this example, the file names are *cxc_pk.pem* for the private key, and *cxc_csr.pem* for the CSR.

Enter a pass phrase for the CA key, and complete he following fields::

```
Country Name (2 letter code) [US]: <your country>
State or Province Name (full name) [MA]: <your state/province>
Locality Name (eg, city) [Maynard]: <your locale>
Organization Name (eg, company) [Acme Packet]: <your company>
Organizational Unit Name (eg, section) [Support]: <your department>
Common Name (eg, YOUR name) []: <Use the FQDN of the CXC>
Email Address []: <your email address>
```

➡ **Note:** The “common-name” field is the most important entry. This is the name that will be used to validate the certificate. Use the Fully Qualified Domain Name (FQDN) of the appropriate OS-E system, such as nnose.acmepacket.com.

Currently, some phones, such as Eyebeam do not support wildcard certificates where the common-name uses an asterisk character (*) in the domain name, such as *.acmepacket.com

2. **Sign the CSR with your OpenSSL CA.**

Unix

```
openssl ca -config /CA/openssl.cnf -in /CA/csrs/cxc_csr.pem –out /
CA/certs/cxc.pem
```

Windows

```
openssl ca -config C:\CA\openssl.cnf -in C:\CA\csrs\cxc_csr.pem
–out C:\CA\certs\cxc.pem
```

Enter the pass phrase for the CA key, then respond “y” to the questions to generate and commit.

3. **Merge the Private Key and Signed Public Key into one file**.

Unix

```
cat /CA/certs/cxc.pem /CA/certs/cxc_pk.pem > /CA/certs/cxc.list.pem
```

Windows (cmd)

```
copy /CA/certs/cxc.pem + /CA/certs/cxc_pk.pem /CA/certs/
```

```
cxc.list.pem
```

4. Upload the newly generated *cxc.list.pem* file back to the OS-E, then configure a TLS certificate, as covered earlier in this chapter. Be sure to associate it with the SIP protocol on the appropriate network interface.

➡ **Note:** You can use the /CA/certs/ca.cer (C:\CA\certs\ca.cer on Windows) file to import into a “Trusted Root Store.” For example, you can install this in Windows (Internet Explorer) for use with Soft Phones, such as Eyebeam. If you deploy the ca.cer file to multiple systems into the “Trusted Root Store”, then those systems will “trust” any certificates signed by this CA.

Using OpenSSL to Convert X.509 and RSA Keys

This section describes how to use OpenSSL to convert an X.509 certificate and/or RSA key to a Public-Key Cryptography Standard #12 (PKCS#12) format.

Requirements

You must have a working installation of the OpenSSL software and be able to execute OpenSSL from the command line.

Refer to “CTX106627 - How to Install the OpenSSL Toolkit,” for more information on obtaining and installing OpenSSL.

The PKCS#12 specifies a portable format for storing and transporting certificates, private keys, and miscellaneous secrets. It is the preferred format for many certificate handling operations and is supported by most browsers and recent releases of the Windows family of operating systems. It has the advantage of being able to store the certificate and corresponding key, root certificate, and any other certificates in the chain in a single file.

Procedure

1. Ensure that the certificate(s) and key are in PEM format.

   - **To convert a certificate from DER to PEM:**

```
x509 –in input.crt –inform DER –out output.crt –outform PEM
```

   - **To convert a key from DER to PEM:**

```
rsa –in input.key –inform DER –out output.key –outform PEM
```

   - **To convert a key from NET to PEM:**

```
rsa –in input.key –inform NET –out output.key –outform PEM
```

Note: The obsolete NET (Netscape server) format is encrypted using an unsalted RC4 symmetric cipher so a passphrase will be requested. If you do not have access to this passphrase it is unlikely you will be able to recover the key

2. Use the **openssl** command to read the PEM encoded certificate(s) and key and export to a single PKCS#12 file as follows:

```
openssl pkcs12 -export -in input.crt -inkey input.key -out
   bundle.p12
```

Note: By default, the key will be encrypted with Triple DES so you will be prompted for an export password (which may be blank).

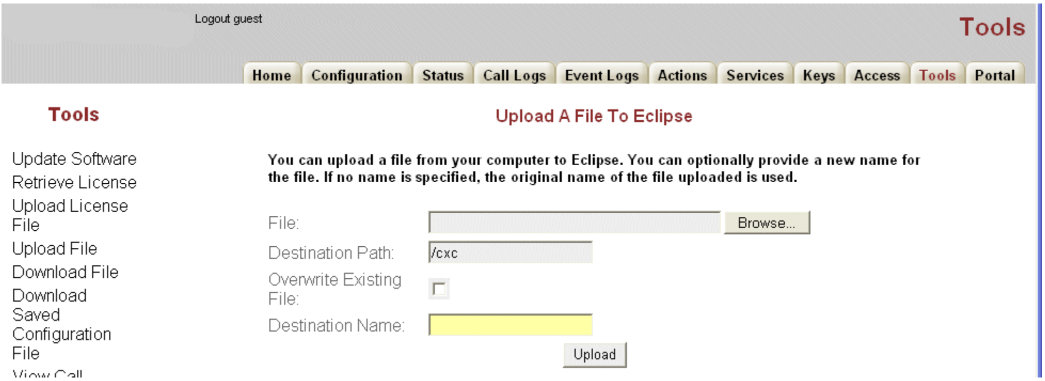
The PEM formatted root certificate and any other certificates in the chain can be merged into a single file such as root.crt, and included in the PKCS#12 file as follows:

```
openssl pkcs12 -export -in input.crt -inkey input.key -certfile
root.crt -out bundle.p12
```

Step 4. Updating the Self-Signed Certificate

The **cert-update** action allows you to load the signed certificate that you receive from the CA. Once you have received the file, perform the following steps:

1. Upload the file to the OS-E using the **Tools**/**Upload file** function to browse for CA’s certificate. Specify the destination path on the OS-E system, such as /cxc/certs, and specify the destination name of the certificate, as illustrated in the following image.



Upload A File To Eclipse

You can upload a file from your computer to Eclipse. You can optionally provide a new name for the file. If no name is specified, the original name of the file uploaded is used.

File:

Destination Path: /cxc

Overwrite Existing File: □

Destination Name:

2. Select the **Keys** tab and select the appropriate key from the Key Stores list to display the Manage Key Store page.
3. Click **Update** to browse for the file that you uploaded in Step 1.
4. Click **Update** to load the signed certificate to the CXC.

If you choose to update the certificate using the **cert-update** action rather than from the **Keys** tab, complete the fields as follows:

keyFile—Specify the name and directory path of the key that you want to update.

Example: /cxc/certs/myNetworkKey.p12

alias—Optional. Specify the alias for the keyFile name, if previously created.

password—Specify the password associated with the keyFile, as specified previously.

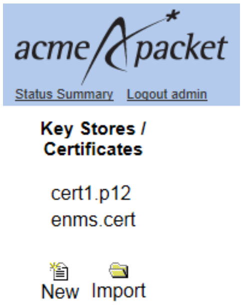
certFile—Specify the name and directory path of the signed certificate that you received from the CA and uploaded to the OS-E using the OS-E Management System **Tools/Upload File** function or other file transfer mechanism.

Subject Alternative Name for HTTPS Certificates Support

The OS-E supports Subject Alternative Name (SAN) for use with HTTPS certificates. SAN is a X509 version 3 certificate extension that allows one to specify a list of host names protected by a single SSL certificate.

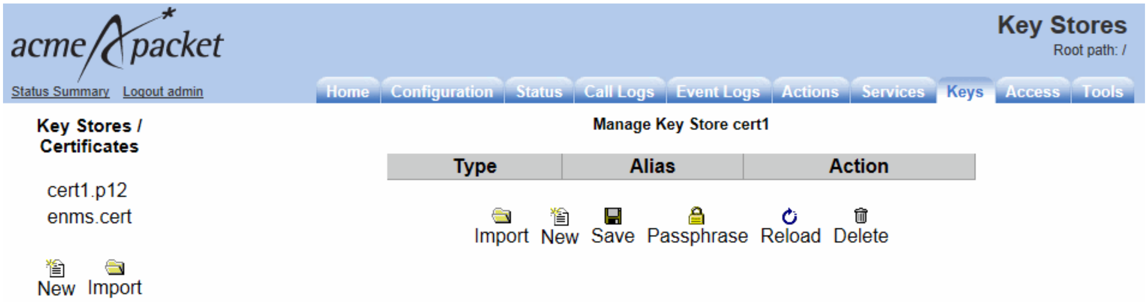
To add multiple SANs to a certificate:

1. Select the **Keys** tab and either click **New** to create a new key store or select the existing store on which you want to add a certificate.



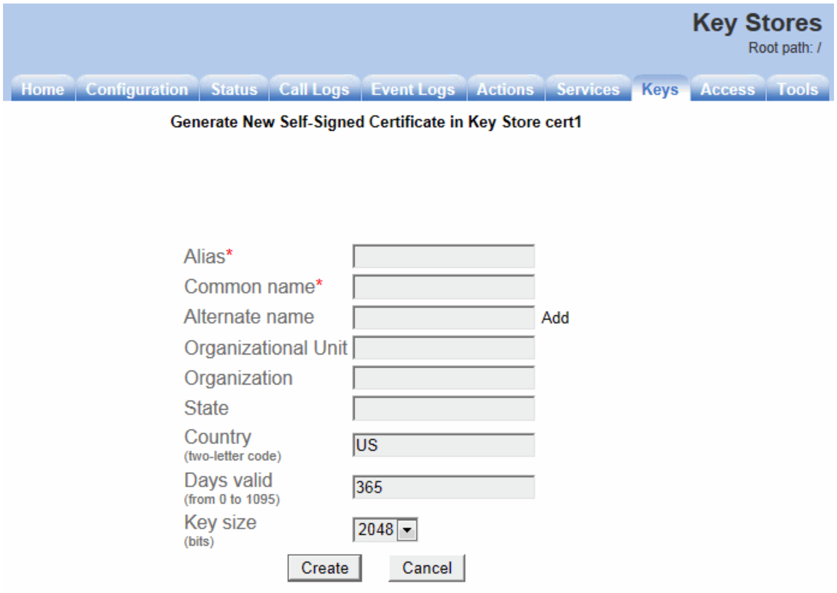
2. Enter a name and passphrase if creating a new keystore and click **Create**.

   The key store appears.



3. Click **New**. The Generate New Self-Signed Certificate in Key Store *X* page appears.

4. Click **Add** beside the **Alternate name** field to add alternate host names be added to the certificate's subjectAltName field.



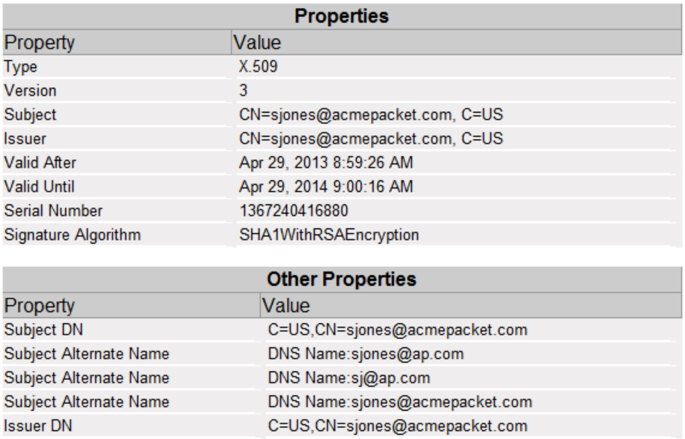
Generate New Self-Signed Certificate in Key Store cert1

Alias*		
Common name*		
Alternate name		Add
Organizational Unit		
Organization		
State		
Country (two-letter code)	US	
Days valid (from 0 to 1095)	365	
Key size (bits)	2048	

5. Click **Create**. The certificate appears in the key store.

   Note: When configuring the OS-E via the CLI, separate multiple SAN entries using the '|' character.

To view the SANs within a certificate click **View** next to the certificate name. The following image shows three SANs.



Properties

Property	Value
Type	X.509
Version	3
Subject	CN=sjones@acmepacket.com, C=US
Issuer	CN=sjones@acmepacket.com, C=US
Valid After	Apr 29, 2013 8:59:26 AM
Valid Until	Apr 29, 2014 9:00:16 AM
Serial Number	1367240416880
Signature Algorithm	SHA1WithRSAEncryption

Other Properties

Property	Value
Subject DN	C=US,CN=sjones@acmepacket.com
Subject Alternate Name	DNS Name:sjones@ap.com
Subject Alternate Name	DNS Name:sj@ap.com
Subject Alternate Name	DNS Name:sjones@acmepacket.com
Issuer DN	C=US,CN=sjones@acmepacket.com

Configuring the Certificate on the Net-Net OS-E

Once you have imported the certificate to a directory on the OS-E system, configure the settings that control how the OS-E uses the certificate.

CLI session

The following CLI session sets the directory and certificate destination file name path, specifies the passphrase, and whether to allow SSL Version 2 operability.

```
NNOS-E> config vsp
config vsp> config tls
config tls> config certificate myNetworkCert.pfx
Creating ‘certificate myNetworkCert.pfx’
config certificate myNetworkCert.pfx> set allow-sslv2 true
config certificate myNetworkCert.pfx> set allow-null-cipher enabled
config certificate myNetworkCert.pfx> set certificate-file /cxc/certs/
   nyNetworkCert.pfx
config certificate myNetworkCert.pfx> set passphrase-tag pass
```

By default, the OS-E only supports SSLv3 or TLSv1. If you require SSLv2 for interoperability, set this property **true**. Specify the **passphrase-tag** associated with the certificate file. Use this property if the certificate file is encrypted to have its private key information protected. This **passphrase-tag** must match the string with which the certificate was encrypted.

Displaying the Certificates Installed on the OS-E

Use the **show certificates** to command to display the list of installed certificates on the system.

Other TLS Certificate Settings

Using Certificate vs. Default-Outgoing-Settings

The OS-E uses a certificate configuration to identify the certificate file and the characteristics of the certificate. There are two types of certificate configuration—a named certificate entry that can be applied to specific TLS connects and a default certificate settings for use when a specific entry was not identified.

The entry created by the **certificate** object is used when the OS-E functions as a server in a TLS connection. Or, it can be used in an OS-E-as-client setup, if you have configured the connection to use a specific certificate. For example, when you set the connection type to the LDAP server to TLS in the **directory** object, you are required to enter a named certificate.

The entry created by the **default-outgoing-settings** object is used when the OS-E is a client with an unspecified certificate. For example, if you set the protocol that the DNS resolver server uses to TLS, you are not prompted for a certificate name. In this case, the OS-E uses either:

- The certificate identified in the **sip-settings** object, if the session matched a configured policy.
- The **default-outgoing-settings** if the session did not match a configured policy or the policy did not have a certificate specified.

Refer to the *Net-Net OS-E – Objects and Properties Reference* for detailed information on the default-outgoing-settings object under TLS.

Verifying Peer Certificates

The OS-E allows you to verify peer certificates. By default, the OS-E accepts all peer certificates. However, you can configure the OS-E to reject a connection if a peer’s certificate does not meet the requirements of the network. Basic verification checks that the certificate's chain is valid, that it was signed by a trusted CA, and that the certificate has not expired.

To verify a peer’s certificate, the appropriate CA file must be installed on the OS-E. For example, to connect to an LCS server, there are four requirements,

1. A client certificate that Session Presents presents to LCS at connection time,
2. A CA file (in PEM or PKCS#12) to verify the server's certificate when it is presented to the OS-E,
3. A Certificate Revocation List (CRL) in PEM format, a list of certificates that a CA has revoked, and thus can no longer be trusted. If any of the certificates in the chain presented to the OS-E appear in the CRL, the OS-E rejects the connection. This is an optional step. And,

4. A valid, verifiable host name that is presenting the certificate. If the host name doesn't match what the OS-E expects, the OS-E rejects the connection, even if the chain is valid.

CLI Session

The following CLI session defines multiple default CA files, and multiple default CRL files:

```
NNOS-E> config vsp tls
config tls> config default-ca
config default-ca> set ca-file /cxc/certs/ca1.pem tag1
config default-ca> set ca-file /cxc/certs/ca2.pem tag2
config default-ca> return
config tls> config default-crl
config default-crl> set crl-file /cxc/certs/crl1.pem tag3
config default-crl> set crl-file /cxc/certs/crl2.pem tag4
config default-crl>
```

Enabling Peer Certificate Verification

The **peer-certificate-verification** property allows you to control whether the OS-E validates a peer’s certificate.

```
NNOS-E> config vsp tls
config tls> config certificate myNetworkCert.pfx
config myNetworkCert.pfx> set peer-certificate verification {none |
   if-presented | required}
```

None—The OS-E will not request a certificate from the peer, and will verify a certificate if presented with one. This is the default setting.

IfPresented—If a peer presents a certificate, the OS-E verifies it, or rejects the connection if the certificate fails verification. If no certificate is presented, the OS-E allows the connection.

Required—If a peer presents a certificate, the OS-E verifies it, or rejects the connection if the certificate fails verification. If no certificate is presented, the OS-E rejects the connection.

Note: TLS treats clients (initiators) and servers (answerers) differently. In a typical TLS connection, only the server presents a certificate; the client is only allowed to present a certificate if it is requested to do so by the server. Therefore, the **IfPresented** option applies only for a client connection.

Controlling the CA Files and CRLs to Apply to the Certificate

Configure each certificate entry to use or ignore the default CA and CRL settings.

```
config> config vsp tls certificate myNetworkCert.pfx
config certificate myNetworkCert.pfx> set use-default-ca true
config certificate myNetworkCert.pfx> set use-default-crl false
```

Optionally, you can configure each certificate entry to use an extra CA and an extra CRL, independent of the default settings, using the file path and passphrase tag.

```
config certificate myNetworkCert> set specific-ca-file /cxc/certs/
   ca9.pem tag9
config certificate myNetworkCert> set specific-crl-file /cxc/certs/
   crl9.pem tag10
```

Setting the Required Peer Name

The **required-peer-name** property specifies the name that appears in the presented certificate.

- If you do not configure a peer name, then the OS-E does not check the presented name.
- If you do configure a peer name, then that name must appear in the DNS field of the **alternateName** field, or in the **commonName** field for the certificate.

The **required-peer-name** can include wildcards, such as "*.acmepacket.com". If the presented name does not match the required name, the OS-E rejects the connection.

Configuring TLS on Ethernet Interfaces

Referring to the network illustrated in the “Steps to Configuring TLS,” section, note that one Ethernet interface is connected to public Internet on port 443, and other Ethernet interface connects to the enterprise or service provider’s private network on the known TLS port 5061. Using port 443 on the public side of the network allows HTTPS requests to pass through the network firewall to the OS-E system.

CLI Session

The following CLI session configures IP on the public and private OS-E interfaces, and the SIP protocol, ports, and TLS certificate destination name references.

```
NNOS-E> config cluster
config cluster> config box 1
config box 1> config interface eth0
config interface eth0> config ip private
Creating ‘ip private’
config ip private> set ip-address static 10.1.1.1/24
config ip private> config sip
config sip> set udp-port 5060
config sip> set tcp-port 5060
config sip> set tls-port 5061
config sip> set certificate vsp tls certificate myNetworkCert.pfx
Creating ‘vsp\tls\certificate myNetworkCert.pfx’
config sip> return
config ip public> return
config interface eth0> return
config box 1>

config box 1> config interface eth1
config interface eth0> config ip public
Creating ‘ip public’
config ip private> set ip-address static 216.1.1.1/24
config ip private> config sip
config sip> set udp-port 5060
config sip> set tcp-port 5060
config sip> set tls-port 443
config sip> set certificate vsp tls certificate myNetworkCert.pfx
Creating ‘vsp\tls\certificate myNetworkCert.pfx’
config sip> return
config ip public> return
config interface eth0> return
config box 1>
```

Chapter 6. Configuring Secure Media (SRTP) Sessions

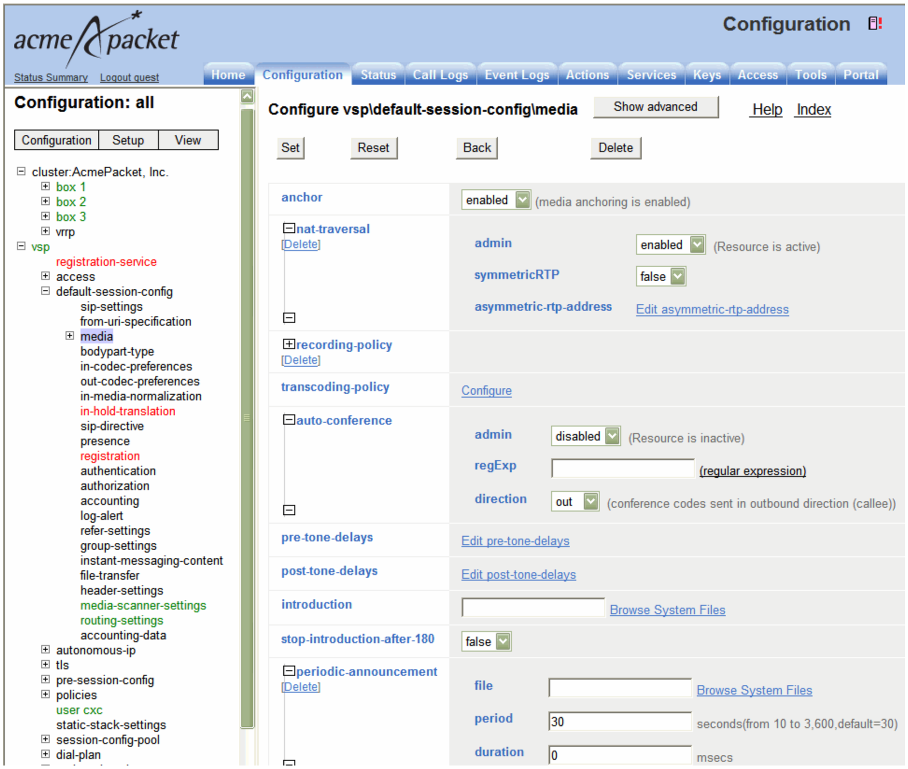
About This Chapter

This chapter provides information on configuring inbound and outbound encryption on SIP media sessions anchored by the OS-E.

Anchoring Media Sessions

Media anchoring forces the SIP media session to traverse the OS-E system. The **auto** setting enables conditional anchoring where the OS-E uses its auto-anchoring algorithms to determine anchoring necessity based on a variety of criteria, including whether you have configured smart anchoring via the **autonomous-ip** object and whether the calling devices are behind a firewall.

The following image shows an OS-E Management System session where you enable media anchoring in the default-session-config.



Configure vsp\default-session-config\media

anchor: enabled (media anchoring is enabled)

nat-traversal
- admin: enabled (Resource is active)
- symmetricRTP: false
- asymmetric-rtp-address: Edit asymmetric-rtp-address

recording-policy

transcoding-policy: Configure

auto-conference
- admin: disabled (Resource is inactive)
- regExp: (regular expression)
- direction: out (conference codes sent in outbound direction (callee))

pre-tone-delays: Edit pre-tone-delays

post-tone-delays: Edit post-tone-delays

introduction: Browse System Files

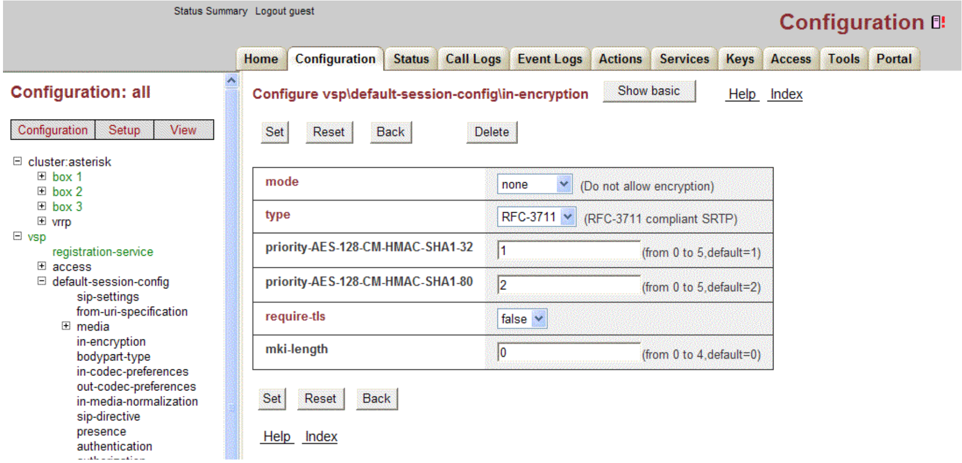
stop-introduction-after-180: false

periodic-announcement
- file: Browse System Files
- period: 30 seconds(from 10 to 3,600,default=30)
- duration: 0 msecs

Configuring Inbound and Outbound Encryption

For secure inbound and outbound media sessions, you need to configure OS-E **in-encryption** and **out-encryption** settings. Inbound encryption handles the portion of the call from the initiator to the OS-E using a specified encryption method. Similarly, outbound encryption handles the portion of the call from the OS-E to the call recipient using a specified encryption method.

The following image shows the inbound encryption configuration page.



Configure vsp\default-session-config\in-encryption

mode	none	(Do not allow encryption)
type	RFC-3711	(RFC-3711 compliant SRTP)
priority-AES-128-CM-HMAC-SHA1-32	1	(from 0 to 5,default=1)
priority-AES-128-CM-HMAC-SHA1-80	2	(from 0 to 5,default=2)
require-tls	false	
mki-length	0	(from 0 to 4,default=0)

Inbound Encryption Mode and Type

Set the inbound encryption mode to one of the following settings:

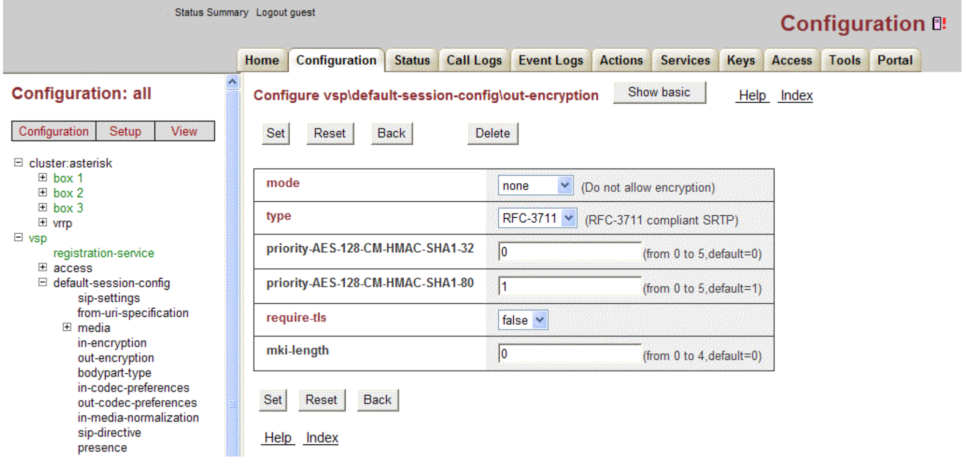
- **none**—The OS-E disables the encryption put forth by the incoming endpoint. (That is, it responds “no” to the encryption portion of the authentication handshake.) If the outbound endpoint requires encryption, then the call is dropped.
- **allow**—The OS-E passes the call through, leaving the encryption setting unchanged.
- **require**—The call must come in with encryption specified or the OS-E drops it.

Set the inbound encryption type to one of the following settings:

- **RFC-1889**—Use encryption as defined in RFC 1889, RTP: A Transport Protocol for Real-Time Applications. This mode is used for compatibility with Windows Messenger and Microsoft Office Communicator, neither of which currently support RFC-3711 encryption. Instead, it uses a DES-CBC encryption of the entire UDP payload (including RTP headers) with no authentication.
- **RFC-3711**—Use encryption as defined in RFC 3711, The Secure Real-time Transport Protocol (SRTP). This is the same encryption as used in the OS-E setting.

- **Linksys**—Use Linksys/Sipura encryption over Linksys phones. Refer to Lynksys Encryption for more information

The following image shows the inbound encryption configuration page.



Configure vsp\default-session-config\out-encryption

mode	none	(Do not allow encryption)
type	RFC-3711	(RFC-3711 compliant SRTP)
priority-AES-128-CM-HMAC-SHA1-32	0	(from 0 to 5,default=0)
priority-AES-128-CM-HMAC-SHA1-80	1	(from 0 to 5,default=1)
require-tls	false	
mki-length	0	(from 0 to 4,default=0)

Outbound Encryption Mode, Type, and Require-TLS Setting

Set the out-encryption mode to one of the following settings:

- **none**—The OS-E disables the encryption put forth by the outbound endpoint. (That is, it responds “no” to the encryption portion of the authentication handshake.) If the inbound endpoint requires encryption, then the call is dropped.
- **offer**—The OS-E changes or establishes the encryption type to the value specified in the **type** property, below.
- **follow**—If the inbound endpoint offered encryption, the OS-E offers that type to the outbound endpoint.
- **require**—The call must come in with encryption specified or the OS-E drops it.

Set the out-encryption type to one of the following settings:

- **RFC-1889**—Use encryption as defined in RFC 1889, RTP: A Transport Protocol for Real-Time Applications. This mode is used for compatibility with Windows Messenger and Microsoft Office Communicator, neither of which currently support RFC-3711 encryption. Instead, it uses a DES-CBC encryption of the entire UDP payload (including RTP headers) with no authentication.

- **RFC-3711**—Use encryption as defined in RFC 3711, The Secure Real-time Transport Protocol (SRTP). This is the same encryption as used in the OS-E setting.
- **Linksys**—Use Linksys/Sipura encryption over Linksys phones. Refer to Linksys Encryption for more information.

Note: Because the OS-E does not always know on the outbound leg the encryption method expected by the recipient (because that recipient isn't in the registry), you must manually set the type of encryption to offer.

Require TLS

The **require-tls** property specifies the requirements of the signaling protocol for a call's outbound leg. That is, it defines whether the OS-E offers SRTP over a non-secure (TCP or UDP) signaling connection. The action of this property depends on the setting of the mode property. When this property is set to:

- **true**—The OS-E only offers encryption when talking to a TLS client. If TLS and SRTP are required (**mode** is set to **require**), the OS-E fails calls going to TCP/ UDP clients. If the mode property is set to **offer** or **follow**, the OS-E forwards the call without SRTP.
- **false**—The OS-E offers SDP messages according to the mode setting without regard for the signaling transport. This allows keys to be exchanged in an insecure message.

Most phones follow RFC 4568, SDP Security Descriptions for media Streams, and thus require that this property be set to *true*.

Linksys Encryption

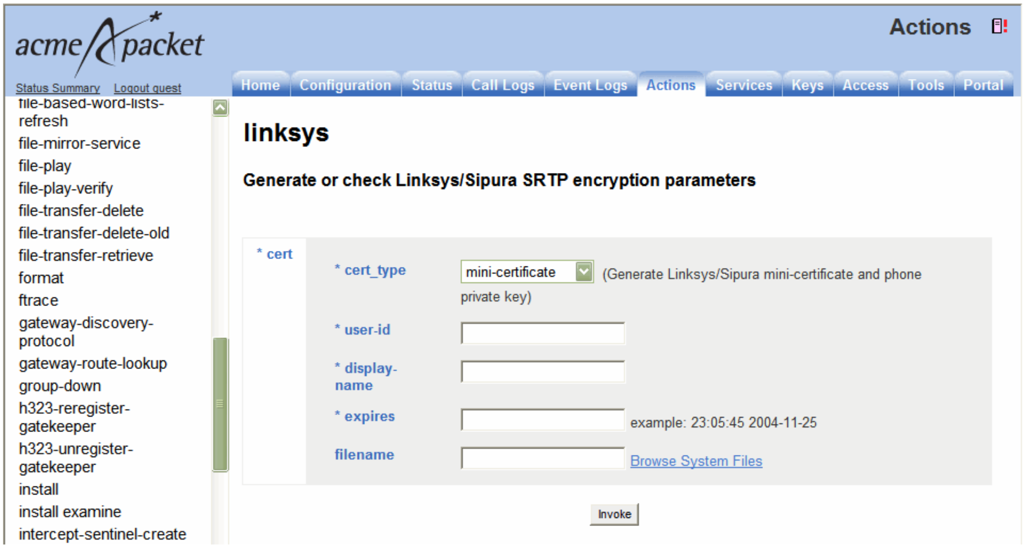
The **linksys** action allows you to generate a Linksys/Sipura mini-certificate and private key which, after loaded into the phone, will be used to exchange the symmetric key. You must execute this action and load the result into both phone parties.

Linksys equipment supports a proprietary version of SRTP. It uses SIP INFO messages to exchange credentials (in mini-certificates) and securely distribute the key used to encrypt/decrypt the RTP packets. The RTP encryption is a variation of RFC-3711; the encryption algorithm is the same (AES-CM-128), but uses HMAC-MD5 instead of HMAC-SHA1 for authentication.

The CLI syntax for the **linksys mini-certificate** action is:

```
linksys mini-certificate user-id display-name expires [filename]
```

The following image shows the linksys mini-certificate page.



linksys

Generate or check Linksys/Sipura SRTP encryption parameters

* cert

* cert_type: mini-certificate (Generate Linksys/Sipura mini-certificate and phone private key)

* user-id

* display-name

* expires: example: 23:05:45 2004-11-25

filename

The **linksys** action provides three tools:

- **mini-certificate**—Creates a mini-certificate, which will later be used by a Linksys phone to exchange an encrypted symmetric key. When both phones in a call support cryptographic exchange, use this action to create a mini-certificate that is sent in an INFO message to the other phone. (You must execute this action for both phones.) After exchanging mini-certificate, the phones can then exchange an encrypted symmetric key.

  Enter the following fields to generate a mini-certificate:

  - **userID**—A name that identifies this phone (subscriber) to the other party. The user ID can be up to 32 characters.
  - **displayName**—A name used by the caller to verify that the callee is the intended call recipient. Enter the user ID field in the Request URI of the INVITE message sent to the proxy server by the caller UAC when making a call to this subscriber (UAS). The display name can be up to 16 characters.
  - **expiration**—The date and time at which this mini-certificate expires. Enter the date in the format *hh*:*mm*:*ss yyyy-mm-dd*.

- **filename**—A name for an output file that will contain the mini-certificate and private key. If you do not specify a file name, the output is not written to a file.

  Once you execute this option, the OS-E returns the content of the mini-certificate and the SRTP private key. You can copy and paste each of these fields into your phones Web GUI (or other software interface), as well as test the certificate using the **check-mini-cert** option.

- **generate-ca-key**—Generates a Linksys/Sipura CA key. This is the public/private key pair that acts as the Sipura certificate authority. It is needed to generate the mini-certificates for each phone and during the key exchange.

  The key is stored in **/cxc/certs/linksys_ca.pem**. When executing this action, you can specify whether to overwrite any previous CA key. The default setting, **false**, does not overwrite the key. Set the field to **true** to force an overwrite.

- **check-mini-cert**—Verifies the contents of a certificate created with the mini-certificate option. When executed, the OS-E checks the expiration date and signature of the certificate. Enter the content of the mini-certificate to invoke this option.

Note: You must have a root certificate loaded on the OS-E system for this action to be successful. The default location for the root certificate is **/cxc/certs/linksys_ca.pem**.

The following CLI session generates the mini-certificate and private key for the Linksys phones.

CLI Session

```
NNOS-E> linksys mini-certificate ?

Generate or load Linksys/Sipura SRTP encryption parameters

 syntax: linksys mini-certificate user-id display-name expires
   [filename]
         linksys generate-ca-key [force]
         linksys check-mini-cert minicert

NNOS-E> linksys mini-certificate 9577 9577-display "23:05:45
 2004-11-25"

Mini Certificate:
```

```
OTU3Ny1kdWVyb2QAAAAAAAAAAAAAAAAAAAAAAAAAAAA5NTc3AAAAAAAAAAAAAAAAMDMwNT
  Q1MjYxMTA0ybYgcwG8IeaYz225Grs7sDJflnfyJxARPehQ+CO6WisAZ77U2zBi8TCapI
  wqcDhNXwgYKZxljAET3dFnzAxs2ze1/
  kEHCqvUmDIEjaYL+1WTySaI1TGKy15FbyZb6dQXtbPF+fXiRP//
  caFfKUBTuuwtjExxaAz0H3u8Tc2YT/wH7a0+snpUTFeK/
  Sv9vd7aAUbufSxewlL2GeTdOu0v2i4R25/
  RH6iOHyChGpVt2EJ3BHAlLgXTfJibiwwkrMSe1grSibsCy0D825ezAt66AVKTa/
  hOmSBvdZvdamJIsbP89vnAJPiOfWNet8T40/wOYyylAE5JDJ/2+G/
  MDyc5ImzFTvifKvIQ55T7Jr5E0RUbacDZIlHy5oW+x4sfawCiQZunnb11qlAgYhvOeuo
  4f3JGUKJAld0GRjHfvjRhb3c=

SRTP Private Key:
Oxq38oJqjhe++yBTtTotoMndnZXulkgnnxFQPd0v96oc81IZ5dug9Szob9ZYQXsPkWAxSb
Oxq38oJqjhe++BVpyxz2P2qtZEg==
NNOS-E> linksys check-mini-cert
  OTU3NwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA5NTc3AAAAAAAAAAAAA
  AAAMTU1ODQ4MTEyNTA0z1TBkpXzjmR6PFX5K4S7G5SxdpozH460T14KpwOxZ8
  ly4KWpFlcC2rTTWEU6WnOufcj5Bfif7cdsAF/
  89kZu83NFceK2ZBRGrJ4cbxREtuPwy1FqkXpBQcztTFXjeyFaq8K7OESebQay
  FetBEceIupuzxfedlJPRsMRhsHN1uKpomc/
  tdJFHJhxSzn+fX+GTACrXQEHzI+ooDL+iQvzhJ1zk/
  gXTGuk76lkJG2XLvSvdjTp8RjQX/F5h0GnBa02d3bQ51n7IBvJnTeaGKp/U/
  e5pQvW5u6vD/uHkqkTGkZDZzOyIISIdgWVxdjA9cpaSa2D5nPhr8G/
  WhOadLZ08fmB0kPwEFjJ0h0dojjknjNJp/
  qVjR5NEEzuj5kH7Qlvxk25l0MThhydCYpbxShy2GSno7apnyCA02YBQCRlGBO
  s=
Certificate has expired

NNOS-E> linksys generate-ca-key
Unable to overwrite Linksys CA key
```

Chapter 7. Performing Maintenance and System Upgrades to the NN2600

About This Chapter

This chapter describes the Net-Net OS-E 2610 and 2620 hardware maintenance and upgrade tasks that you can perform at your installation site. You do not need onsite assistance from Oracle personnel to perform these tasks.

Before performing any type of maintenance or upgrade activity, make sure that you first read the Warnings and Safety Cautions sections at the beginning of this chapter.

Warnings

System Power On/Off

The power button DOES NOT turn off the system AC power. To remove power from system, you must unplug the AC power cord from the wall outlet. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

Hazardous Conditions, Devices and Cables

Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it. Otherwise, personal injury or equipment damage can result.

Electrostatic Discharge (ESD) and ESD Protection

ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground — any unpainted metal surface—on your server when handling parts.

Refer to Attaching an ESD Strap for more information.

ESD and Handling Boards

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

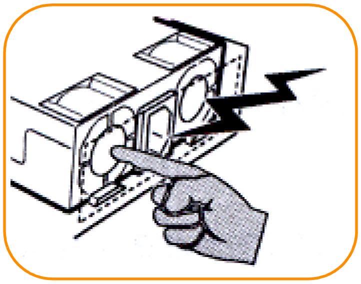
Installing or Removing Jumpers

A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle nosed pliers. If your jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool you use to remove a jumper, or you may bend or break the stake pins on the board.

Safety Cautions

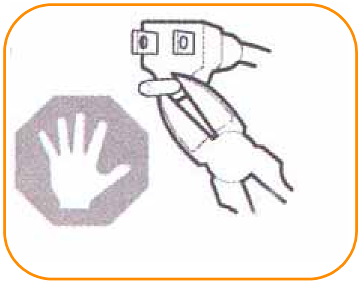
Read all caution and safety statements in this document before performing any of the instructions.

.



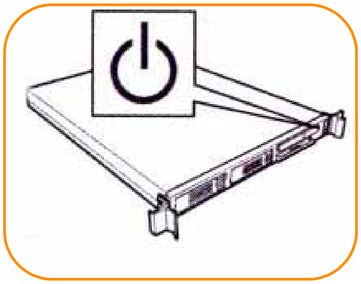
The power supply in this product contains no user-serviceable parts. Refer servicing only to qualified Oracle support personnel.

.



Do not attempt to modify or use the supplied AC power cord if it is not the exact type required. A product with more than one power supply will have a separate AC power cord for each supply.

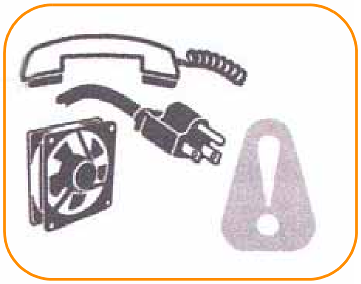
.



The power button on the system does not turn off system AC power. To remove AC power from the system, you must unplug each AC power cord from the wall outlet or power supply.

The power cord(s) is considered the disconnect device to the main (AC) power. The socket outlet that the system plugs into shall be installed near the equipment and shall be easily accessible

.



SAFETY STEPS: Whenever you remove the chassis covers to access the inside of the system, follow these steps:

1. Turn off all peripheral devices connected to the system.

2. Turn off the system by pressing the power button.

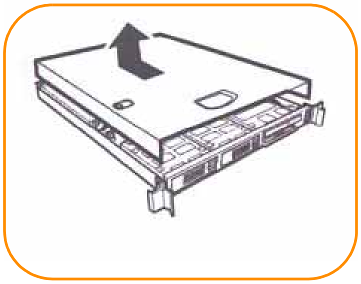
3. Unplug all AC power cords from the system or from wall outlets.

4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.

5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.

6. Do not operate the system with the chassis covers removed.

.

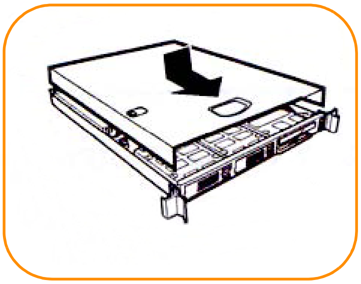


After you have completed the six SAFETY steps above, you can remove the system covers.
To do this:

1. Unlock and remove the padlock from the back of the system if a padlock has been installed.

2. Remove and save all screws from the covers.

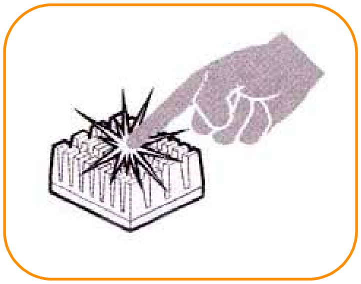
3. Remove the covers.



For proper cooling and airflow, always reinstall the chassis covers before turning on the system. Operating the system without the covers in place can damage system parts.

To install the covers:

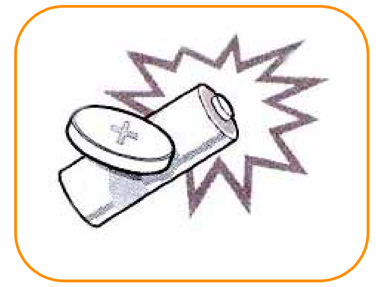
1. Check first to make sure you have not left loose tools or parts inside the system.
2. Check that cables, add-in boards, and other components are properly installed.
3. Attach the covers to the chassis with the screws removed earlier, and tighten them firmly.
4. Insert and lock the padlock to the system to prevent unauthorized access inside the system.
5. Connect all external cables and the AC power cord(s) to the system.



A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts

Contact should be made with care. Consider wearing protective gloves.

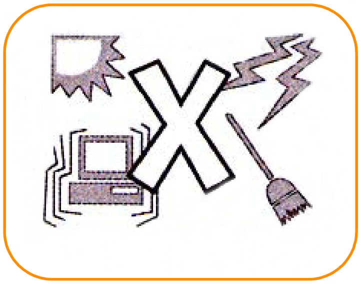
.



Danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer.

Dispose of used batteries according to manufacturer’s instructions.

.



The system is designed to operate in a typical office, service provider, or Telco environment.

Choose a site that is:

— Clean and free of airborne particles (other than normal room dust.

— Well ventilated and away from sources of heat including direct sunlight.

— Away from sources of vibration and shock.

— Isolated from strong electromagnetic fields produced by electrical forces.

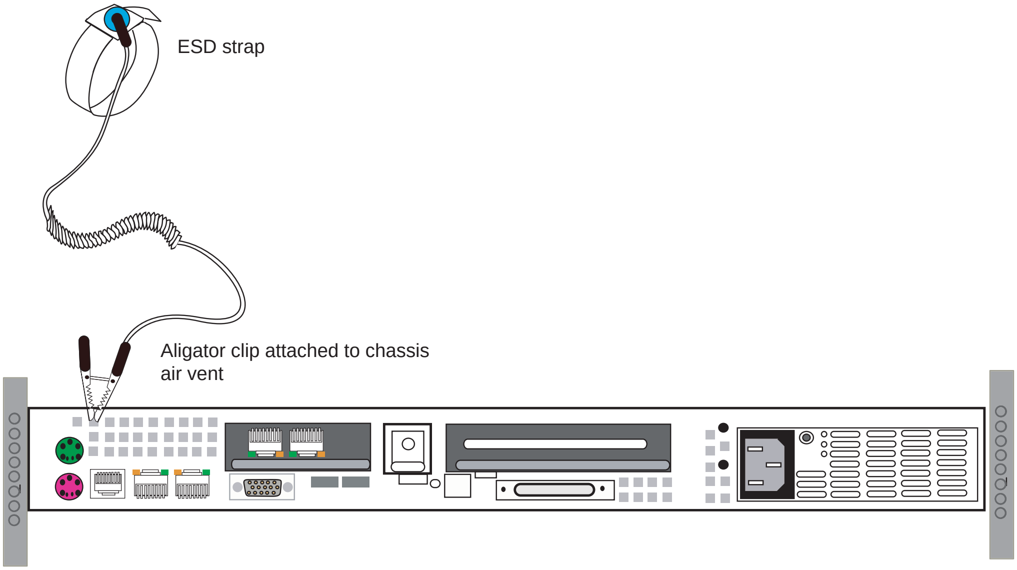
— In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines during an electrical storm.

— Provided with a properly grounded wall outlet.

— Provided with sufficient space at access the power supply cord(s), because they serve as the product’s main power disconnect.

Attaching an ESD Strap

Make sure that you attach an electrostatic discharge (ESD) strap to the system anytime you perform any maintenance that involves removing the top cover. ESD straps usually have an alligator-style clip that allows you to easily attach the strap to the system sheet metal. Air vents holes in the sheet metal allow for easy attachment of an ESD strap, as illustrated in the following image.



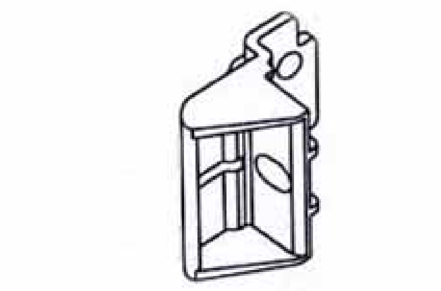
Installing the Racking Mounting Brackets

On NN2610 and NN2620 Systems

NN 2610 and NN 2620 systems include rack mounting brackets that secure the front bezel and to allow installation in a rack. You will need a #2 Phillips screwdriver to install the brackets.

If you have not already installed the brackets (as described in Chapter 2, “Installing the NN2610 and NN2620 Series Systems”), locate the two brackets and the four screws in the accessory box included in the shipping container. Install the brackets at the front sides of the chassis, using two screws required for each bracket.

The following image illustrates the bracket. Note that both brackets are identical, so you can start with either bracket on the either side.

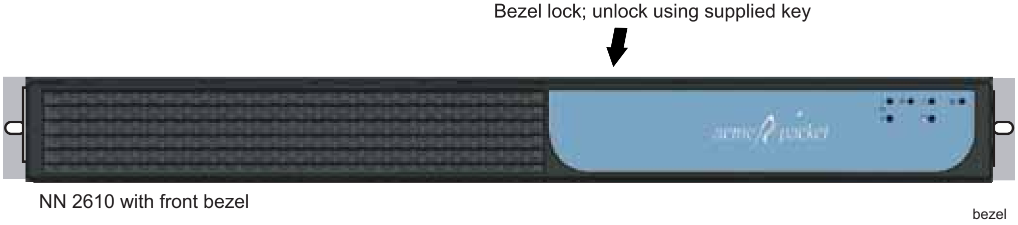


Installing and Removing the Front Bezel

On NN2610 and NN2620 Systems

OS-E Series systems have a removable front bezel. The bezel snaps into the rack mounting brackets at front of the chassis and is secured with a keyed lock, illustrated in the following image. OS-E Series systems can operate with or without the front bezel.

Removing the bezel allows you to access the system control panel and the hard disk drives on the front of the system. Installing the bezel provides a way to protect the system from unwanted intrusion and manipulation of the system.

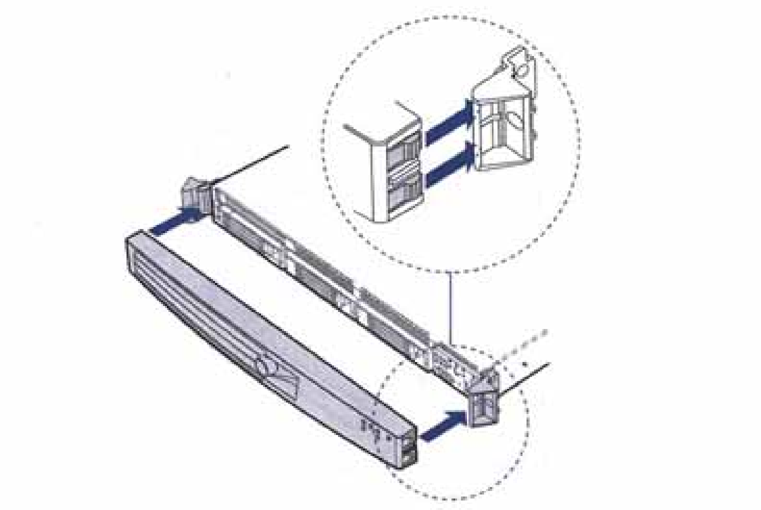


To install the front bezel, perform the following steps:

1. At each end of the bezel, line up the center notch on the bezel with the center guide on the rack handles.
2. Push the bezel onto the front of the chassis until it clicks into place.

3. Connect any necessary cables to the front control panel area at the right side of the chassis.

4. Lock the bezel using the supplied key.

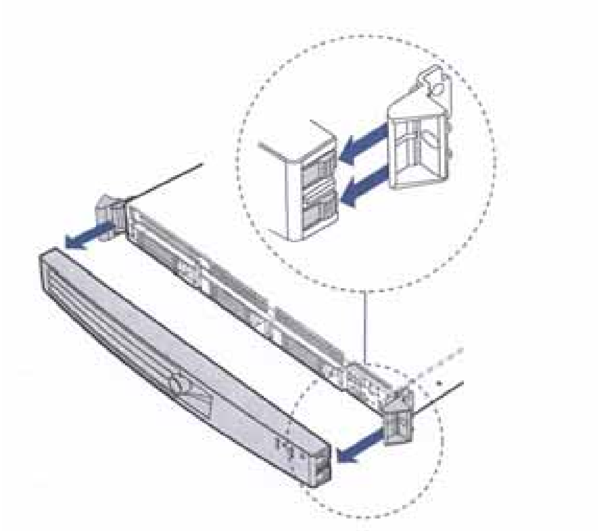


To remove the bezel, perform the following steps:

1. Unlock the bezel using the supplied.key.

2. Remove any cables that are attached to the front of the system.

3. Pull on the left- and right-most edges of the bezel to pop it out.



Removing and Installing the Chassis Cover

On the NN2610

Removing the Chassis Cover

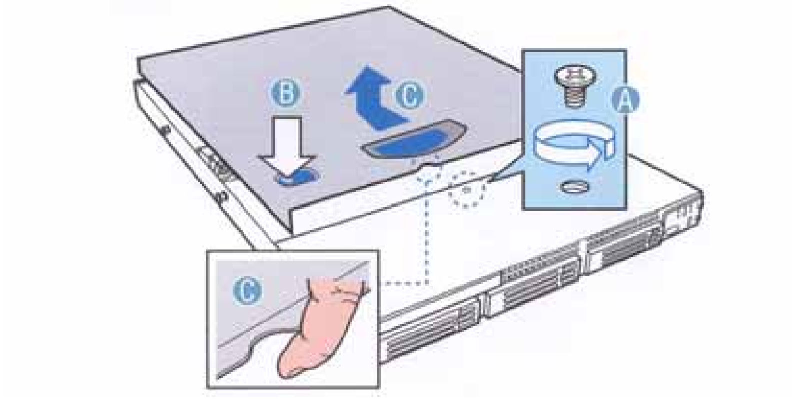
The NN 2610 must have the top cover in place to ensure proper cooling. You will need to remove the top cover to add or replace components inside of the platform. Before removing the top cover, power down the server and unplug all peripheral devices and the AC power cable. None of the components inside the chassis are hot-swappable.

➡ **Note:** A nonskid surface or a stop behind the chassis may be needed to prevent the chassis from sliding on your work surface.

Perform the following steps:

1. Observe the warnings and cautions covered at the beginning of this chapter.
2. Turn off all peripheral devices connected to the NN 2610, then turn off the NN 2610.

3. Disconnect the AC power cord.
4. Remove the shipping screw (if installed). See letter “A” in the figure below.
5. While holding in the blue button at the top of the chassis in (see letter “B”), slide the top cover back until it stops (See letter “C”).
6. Lift the cover upward to remove it.

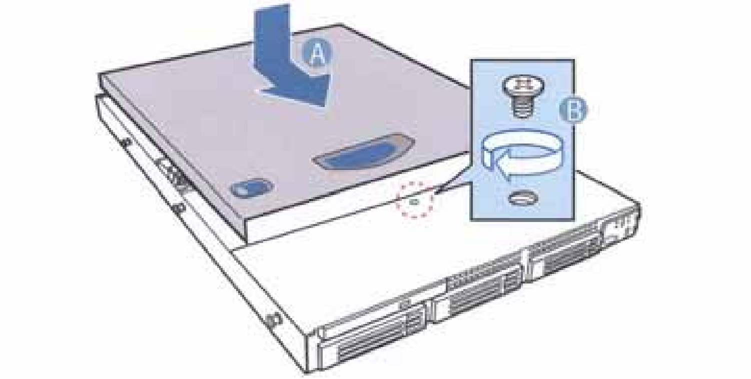


Installing the Chassis Cover on the NN2610

Perform the following steps:

1. Place the cover over the chassis so that the side edges of the cover sit just inside the chassis sidewalls.
2. Slide the cover forward until it clicks into place. See letter “A” in the figure below.
3. (Optional) Insert the shipping screw at the center of the top cover. See letter “B” in the figure.

4. Reconnect all peripheral devices and the AC power cord.



On the NN2620

Removing the Chassis Cover

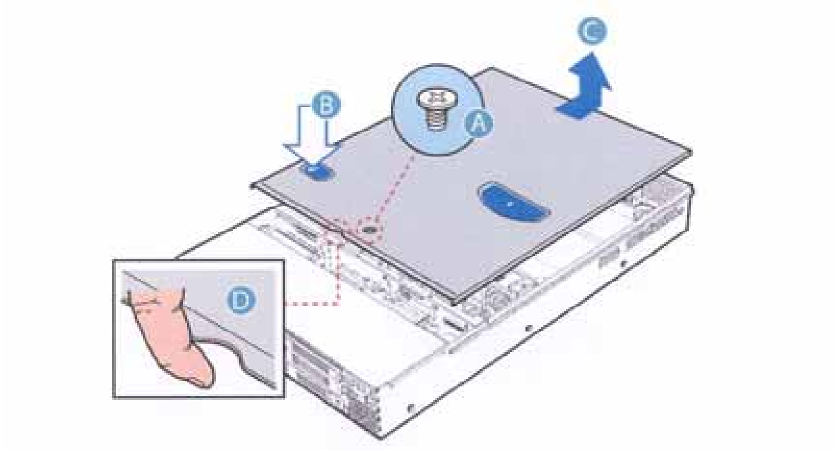
The NN 2620 must have the top cover in place to ensure proper cooling. You will need to remove the top cover to add or replace components inside of the chassis. Before removing the top cover, power down the server and unplug all peripheral devices and the AC power cable. Except for the redundant power supply, none of the components inside the chassis are hot-swappable.

➡ **Note:** A nonskid surface or a stop behind the chassis may be needed to prevent the chassis from sliding on your work surface.

Perform the following steps:

1. Observe the safety and ESD precautions at the beginning of this book. See “Safety Information.”
2. Turn off all peripheral devices connected to the NN 2620, then turn off the NN 2620.
3. Disconnect the AC power cord.
4. Remove the shipping screw (if installed). See letter “A” in the figure below.
5. While holding in the blue button at the top of the chassis in (see letter “B”), slide the top cover back until it stops (see letter “C”).

6. Lift the cover upward and remove it. A notch in the cover is provided to help lift it upward to remove it (see letter “D”).

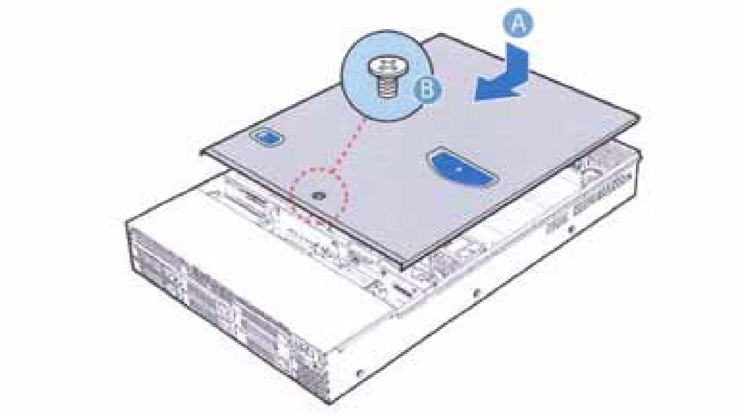


Installing the Chassis Cover on the NN2620

Perform the following steps:

1. Place the cover over the chassis so that the side edges of the cover sit just inside the chassis sidewalls.
2. Slide the cover forward until it clicks into place. See letter “A” in the figure below.
3. (Optional): Insert the shipping screw at the center of the top cover. See letter “B” in the figure.

4. Reconnect all peripheral devices and the AC power cord.



Replacing a System Fan

On NN 2620 systems only

➡ **Note:** For NN 2610 fan replacement, refer servicing to qualified Oracle support personnel.

The system fans at the front of the NN 2620 can be individually replaced if one of them fails. You must have four fans installed in the back four positions of the fan module.

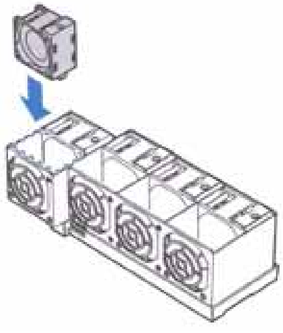
The chassis also allows you to install four redundant fans. The redundant fans must be installed as a set of four and are installed in the four front fan sockets of the fan module. The instructions for installing a redundant fan are the same as the instructions for installing a replacement fan, except that when you are first installing the redundant set of fans, you do not need to remove any fans.

The fans that are integrated into the power supply cannot be replaced separately. If one of these fans fails, the power supply module must be replaced.

To replace a system fan, perform the following instructions. To install the redundant fans, perform the following instructions, but disregard step 4.

Caution: Fans are NOT hot swappable. Before removing or replacing a fan, you must first take the server out of service, turn off all peripheral devices connected to the system, turn off the system by pressing the power button, and unplug the AC power cord from the system or wall outlet.

1. Observe the warnings and cautions covered at the beginning of this chapter.
2. Power down the server system and unplug all peripheral devices and the AC power cable.
3. Remove the chassis cover. For instructions, see Removing and Installing the Chassis Cover.
4. There are no screws to loosen. Lift the failed fan from the module. An LED should indicate the failed fan(s).
5. Position the fan so the connector on the fan is at the right and pointing down.
6. With the fan oriented correctly, insert the fan into the fan module, engaging the connector on the fan into the matching connector on the fan module.
7. Install the chassis cover. For instructions, see Removing and Installing the Chassis Cover.



Installing or Replacing a Hot-Swap Power Supply

On NN2620 Systems Only

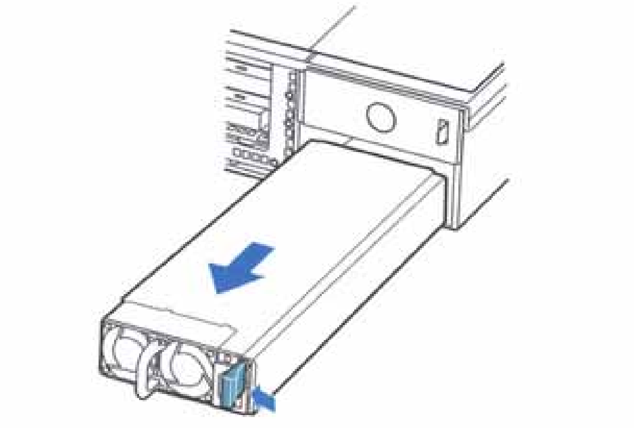
The power supply can be replaced if it, or one of the fans integrated into it, fails. If your server uses a redundant power supply, you do not need to power down your system to replace the failed power supply, as long as the remaining power supply is plugged into an AC power source and is functioning. If you do not have a redundant power supply installed, you must power down your server system before replacing the power supply.

Note: For NN 2610 power supply replacement, refer servicing to qualified Oracle support personnel.

Removing a Hot-Swap Power Supply

To replace the power supply, perform the following steps.

1. (Non-redundant power supply only) Power down the server.
2. Remove the AC power cable from the failed power supply.
3. Press the green latch at the rear of power supply and pull the power supply from the chassis.



Installing a Hot-Swap Power Supply

To install a replacement power supply or to add a redundant power supply, use the following instructions.

1. (Replacing power supply only) Remove the failed power supply. For instructions, see Removing a Hot-Swap Power Supply.
2. (Installing redundant power supply only): Remove the filler panel from the upper power supply bay by pulling it out.
3. Slide the new power supply into the opening until it clicks into place. The latch on the rear of the power supply must be at the right.
4. Plug in the AC power cable for the new power supply.

Installing and Removing a Hard Disk Drive

On NN2610 and NN2620 Systems

The NN 2610 supports up to three SATA hot-swap hard drives, and the NN 2620 supports up to six SATA hard drives.

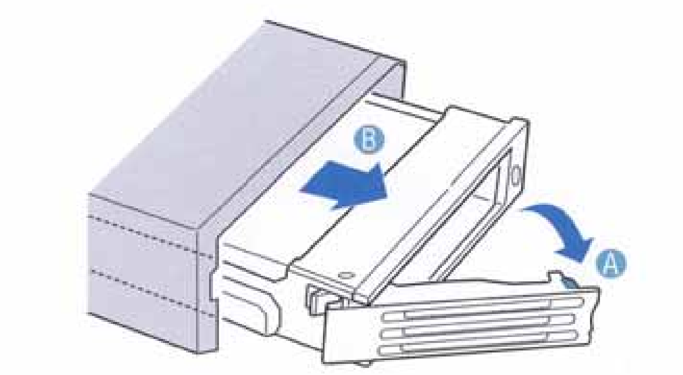
⛔ **Caution:** If you need to replace one or more disk drives, contact your Oracle sales representative for ordering information. Disk drives provided by Oracle are the only compatible models. Do not install disk drives that are not supplied by Oracle.

Removing a SATA Hot-Swap Hard Disk Drive

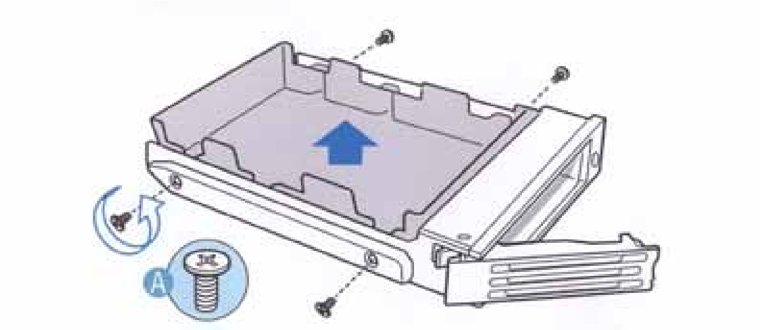
Perform the following steps:

1. Remove the front bezel if it is installed. For instructions, see Installing and Removing the Front Bezel.
2. Press in on the green latch at the front of the hard drive carrier. See letter “A” in the image below

3. Pull out on the black lever and slide the carrier from the chassis. See letter “B” in the figure below.



4. Remove the four screws that attach the plastic retention device or the previously installed hard drive to the drive carrier. Two screws are at each side of the retention device or the hard drive. If required, store the plastic retention device for future use.

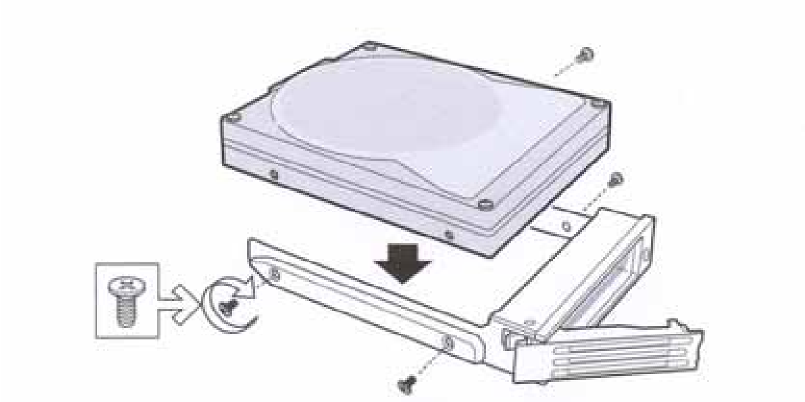


Installing a SATA Hot-Swap Hard Disk Drive

Perform the following steps:

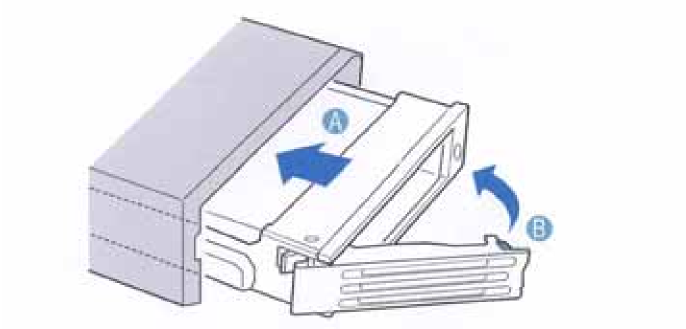
1. Remove the hard drive from its wrapper and place it on an antistatic surface.
2. Set any jumpers and/or switches on the drive according to the drive manufacturer’s instructions.
3. With the drive circuit-side down, position the connector end of the drive so that it is facing the rear of the drive carrier. See the image below.

4. Align the holes in the drive to the holes in the drive carrier and attach it to the carrier with the screws that were attached to the plastic retention device.



5. With the black lever in the fully open position, slide the drive assembly into the chassis. The green latch at the front of the drive carrier must be to the right. Do not push on the black drive carrier lever until the lever begins to close by itself.

6. When the black drive carrier lever begins to close by itself, push on it to lock the drive assembly into place.



7. (Optional) Install the front bezel. For instructions, see Installing and Removing the Front Bezel.

Chapter 8. Creating and Commissioning USB Sticks

This chapter provides information on creating and commissioning OS-E USB software installation sticks for commissioning third-party servers. Using the Internet and secure Web URLs, Oracle provides all necessary software downloads for USB creation, product licensing, and commissioning of the OS-E on your selected hardware.

As part of each download, and depending on your actual requirements, Oracle can provide the following:

- USB Boot Media Creator (BMC) with the OS-E software.
- Feature licenses
- Documentation on how to create a USB stick and commission the OS-E software on your selected hardware
- Standard set of Oracle OS-E technical publications

See the section, “Download Processes and Expiration Timers,” for specific information on feature licensing and what you will need to do if you are running third-party hardware or the OS-E Virtual Machine (OS-E-VM).

In addition to the Oracle NN2610 and NN2620 hardware, Chapter 2 covers USB commissioning information for installing OS-E software on supported third-party hardware platforms and servers.

Supported USB Sticks

You will need to provide a USB stick with at least 1GB storage, and up to 4 GB storage, to handle OS-E software downloads. Oracle has tested a variety of USB sticks available from current suppliers and manufacturers. Most 1GB USB sticks manufactured today will work.

USB Stick Restrictions

If you are upgrading an existing OS-E system from a USB stick, check the /cxc directory for *.cfg* and *.xml* files that are larger than 2 MB. Files that are larger than 2 MB will not be backed up to the USB stick and restored during the upgrade process.

All *.cfg and *.xml files in the current working directory (/cxc) that are less than 2 MB in size are backed up to the stick and restored during the upgrade.

In the event that Internet access is unavailable, use the **show system-info** command to display the box identifier. Access https://licensecodes.oracle.com and click Acme Packet. The Acme Packet License Key Request page appears. Enter the required fields, including the **show system-info** value for **Original Chassis Serial #(s)**, and click **Submit**. After your customer information has been verified, Oracle will send the license(s) to you via email. You can then use the OS-E Management System **Upload License** function or **WinSCP** to place the license files on the system.

- **Downloads for the OS-E Virtual Machine**—Includes the VM for running the OS-E/ASC software on x86-based hardware running OVM 3.2.8, VMware ESXi 5.5, or XEN 3.4.3. The OS-E and ASC technical documentation download is also included.

  For complete information on the VM, see “Installing and Running the OS-E Virtual Machine”.

Running the Boot Media Creator

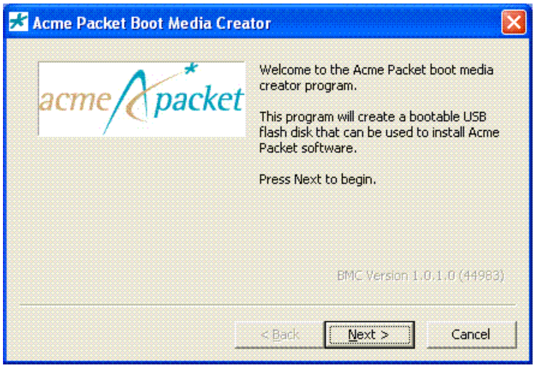
The Boot Media Creator (BMC) is the program that creates the OS-E software installation USB stick. Before using the **bmc.exe** program you must first download both the USB image file you are using to commission your system and the ZIP file containing the BMC tool. Then extract the **bmc.exe** program from the ZIP file.

Note: The BMC supports the following OS types:

- Windows XP
- Windows Vista
- Windows 7

To extract the BMC:

1. Click on the file named **nnSE#####-bmc.exe**.
2. Click **Run.**
3. Click **Next** to start the BMC.



Acme Packet Boot Media Creator

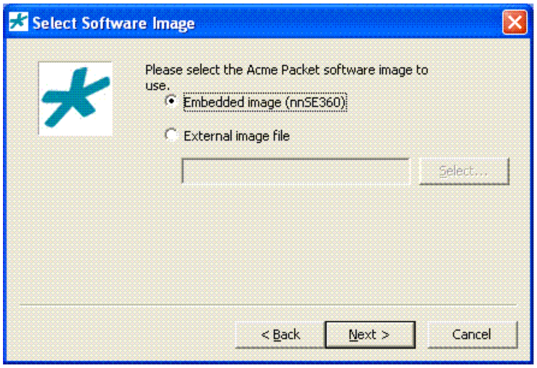
Welcome to the Acme Packet boot media creator program.

This program will create a bootable USB flash disk that can be used to install Acme Packet software.

Press Next to begin.

BMC Version 1.0.1.0 (44983)

4. Click **Next** to display the Select Software Image page.



Select Software Image

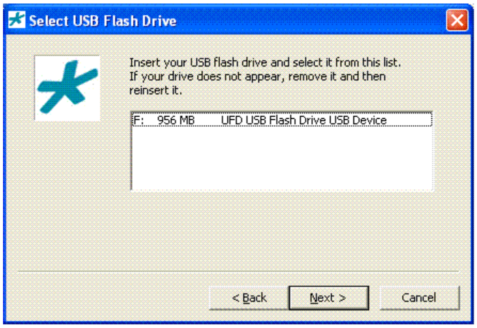
Please select the Acme Packet software image to use.

● Embedded image (nnSE360)

○ External image file

5. Select the **External image file** radio button.
6. Click the **Select...** button to browse to the USB image you downloaded and saved. The USB image name is in the format nnSE####-usb.img.gz.
7. Click **Next** to validate the software image.

8. Insert a USB stick into a USB drive on your PC or workstation.

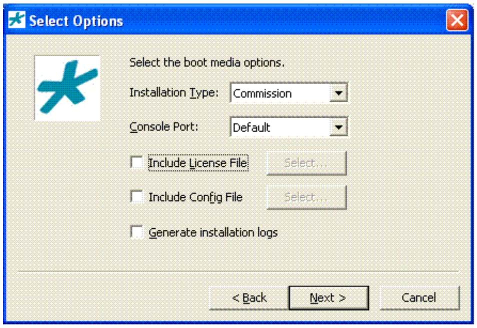


Select USB Flash Drive

Insert your USB flash drive and select it from this list. If your drive does not appear, remove it and then reinsert it.

F: 956 MB UFD USB Flash Drive USB Device

9. Select the USB stick from the list and click **Next** to display the Select Options page.



Select Options

Select the boot media options.

Installation Type: Commission

Console Port: Default

□ Include License File

□ Include Config File

□ Generate installation logs

10. For new installations, set the following:

- **Installation Type:** Commission
- **Console Port**: COM2 (serial1)

Installation Type options:

- **Rescue**—Creates a USB rescue stick. This will boot the system to the Rescue menu. See Chapter 3 for information.
- **Commission**—Copies the system license and configuration file from the OS-E system to the stick, commissions the system, and then reinstalls the license and configuration file. After commissioning the system, the USB stick becomes a rescue stick.
- **Decommission**—Do not use; Oracle use only.
- **Manufacturing**—Do not use; Oracle use only.

Console Port options to sets the destination for local management of the system.

- **Default**—VGA port
- **COM1 (serial 0)**—Serial port 0
- **COM2 (serial 1)**—Serial port 1

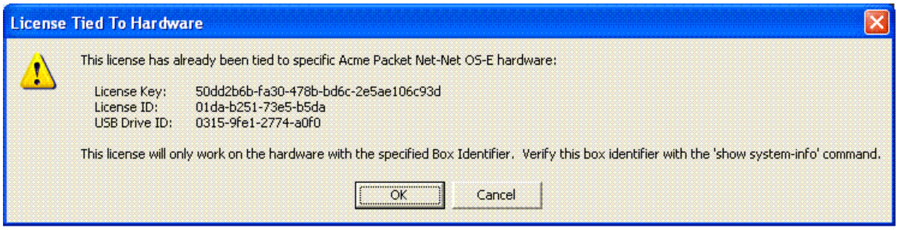
Note: If you are commissioning the Net-Net 2610 or 2620 (as well as the older CXC-350 and CXC-550 series systems) and you want to use the RJ-45 serial port on the rear of the chassis for your console output, choose the COM2 (serial 1) option”

If you are unsure about this setting, see Chapter 2 for detailed information on each platform or third-party server.

During commissioning (covered in Chapter 3), when the GNU GRUB window appears, you will have the opportunity to change the port where your console device is connected, if necessary. If you made the correct selection during this step, simply wait 10 seconds for the installation to begin. If you need to make a new console port selection, follow the instructions on the menu to direct management output to the desired console port.

11. Check off the **Generate installation logs** box if you want to generate detailed installation-related messages for troubleshooting purposes. These messages are stored on the USB device in the /logs directory.

12. Click **Next** to display the License Tied to Hardware page.



License Tied To Hardware

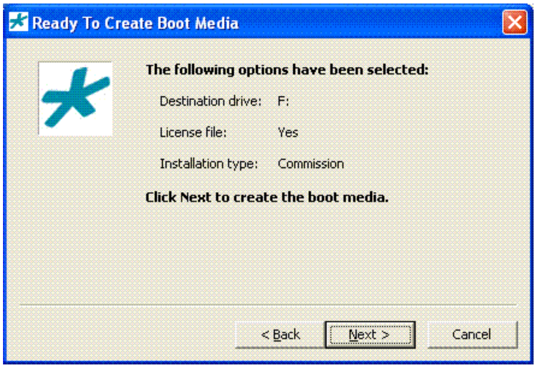
This license has already been tied to specific Acme Packet Net-Net OS-E hardware:

```
License Key:    50dd2b6b-fa30-478b-bd6c-2e5ae106c93d
License ID:     01da-b251-73e5-b5da
USB Drive ID:   0315-9fe1-2774-a0f0
```

This license will only work on the hardware with the specified Box Identifier. Verify this box identifier with the 'show system-info' command.

Note: If you have purchased royalty-bearing codecs for transcoding, you must specify that license file at this point in the installation process. Check the box next to **Include License File** and click **Select**. Browse to the appropriate license file and click **OK**.

13. Click **OK** to display the Ready to Create Boot Media page.



Ready To Create Boot Media

The following options have been selected:

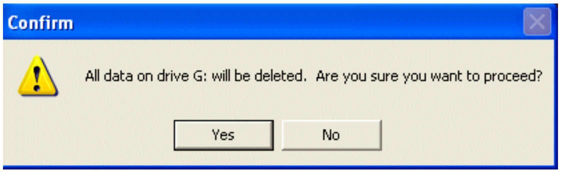
Destination drive: F:

License file: Yes

Installation type: Commission

Click Next to create the boot media.

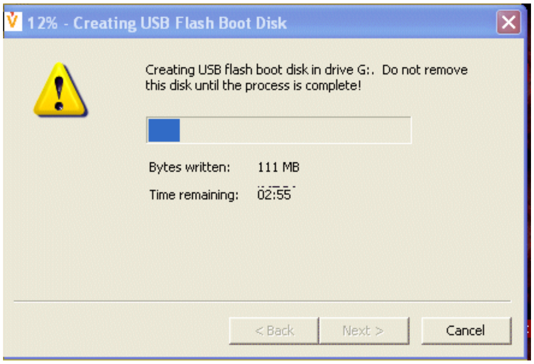
14. Click **Next** to display the confirmation page.



Confirm

All data on drive G: will be deleted. Are you sure you want to proceed?

15. Click **Yes** to display the Creating USB Flash Boot Disk page.



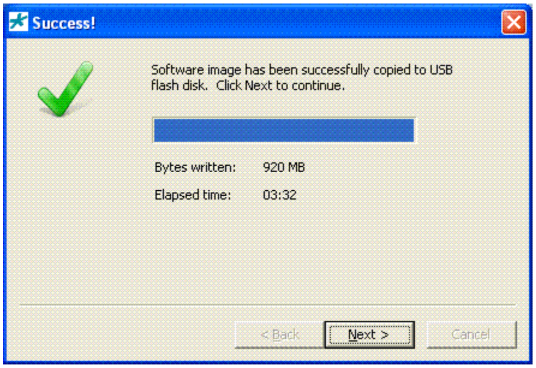
12% - Creating USB Flash Boot Disk

Creating USB flash boot disk in drive G:. Do not remove this disk until the process is complete!

Bytes written: 111 MB

Time remaining: 02:55

16. Click **Next** from the Success! page.



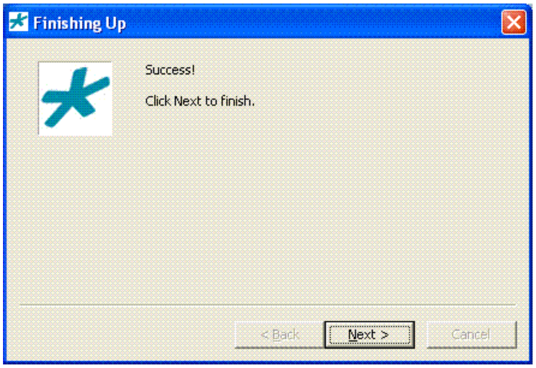
Success!

Software image has been successfully copied to USB flash disk. Click Next to continue.

Bytes written: 920 MB

Elapsed time: 03:32

17. Click **Next** from the Finishing Up page.

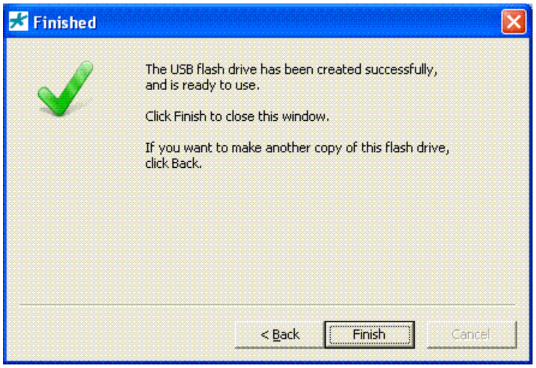


Finishing Up

Success!

Click Next to finish.

18. Click **Next** to display the Finished page.



Finished

The USB flash drive has been created successfully, and is ready to use.

Click Finish to close this window.

If you want to make another copy of this flash drive, click Back.

19. Click **Finish**.

20. Remove the USB drive from your PC.

21. Reinsert the USB drive into the PC and browse the USB drive to verify that the software and license files are present.

Ensuring the USB Contents For Existing Systems

If you are running the BMC to create a USB stick to commission an existing system, (a system with an existing configuration file and license), you will need to follow the steps in this section to ensure that the system will be commissioned with the current configuration file and license, if needed, covered in Chapter 3.

1. Insert the USB stick into the PC and open an Explorer window to view the contents of the USB.
2. Open the **\setup\cxc** directory. You should see the **License** folder in this directory.
3. Copy the *cxc.cfg* file into the **\setup\cxc** directory so that the directory contains the **License** folder and the *cxc.cfg* file.
4. Open the **License** folder to ensure that a license file is present.

   Note: If the license folder is not present, create the directory named **License** and copy the OS-E license file to this location.
5. Remove the USB stick from the PC.

About the New USB Stick — Please Read!

The OS-E USB stick provides three important functions:

- **Commissioning**—Boots and licenses a new third-party server using the OS-E software.
- **Rescue utilities**—After you have successfully commissioned the system (booted and licensed), the system automatically rewrites the USB stick so that you can use it to run system utilities in the event of a catastrophic failure. You will not be able to use this USB again to license another system. The USB can only be used at the specific system from which it was originally written.

  Additionally, licensing information is rewritten to the USB, directly associating the license with the system. Use the **show system-info** action to display the box identifier (box-id) to which this USB is associated. The USB also contains log and debug files that you can use to help diagnose problems associated with the USB licensing process.

- **Rescue stick creation**—With the original USB commissioning stick, use the **restore-stick-create full-backup** action to capture the current software, certificates, and operating system image to the USB stick. Oracle recommends that you use **restore-stick-create full-backup** to preserve the image prior to performing a system software upgrade, or whenever you have made significant and reliable changes to the system configuration.

See Chapter 3 of this guide for information on these functions.

Accessing License Files

To manage OS-E licenses, select the **Tools** tab and click **Upload License**.

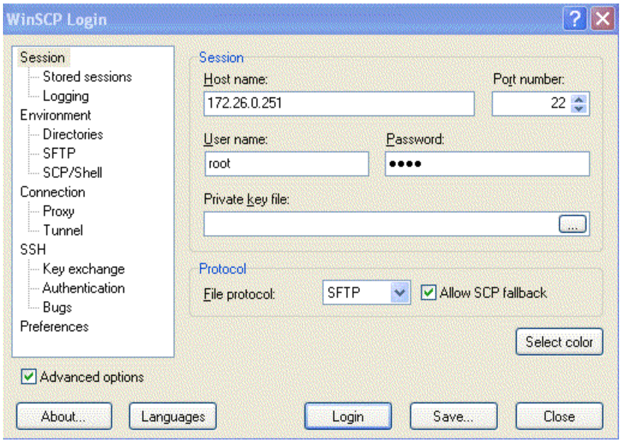
If you receive a license file by email, save the license to your local PC, then select the **Tools** tab and click **Upload License file**. Browse to the file and click **Apply License**, then click **Upload**.

Using WinSCP to Transfer the License

If you do not have access to the OS-E Management System, Oracle recommends that you use WinSCP to transfer the license file to the OS-E system. WinSCP is an open source free SFTP client and FTP client for Windows and is available as a free download from the following URL:

http://winscp.net/eng/index.php

The image below illustrates the WinSCP login window.



WinSCP Login

Session

Host name: 172.26.0.251

Port number: 22

User name: root

Password: ●●●●

Private key file:

Protocol

File protocol: SFTP

☑ Allow SCP fallback

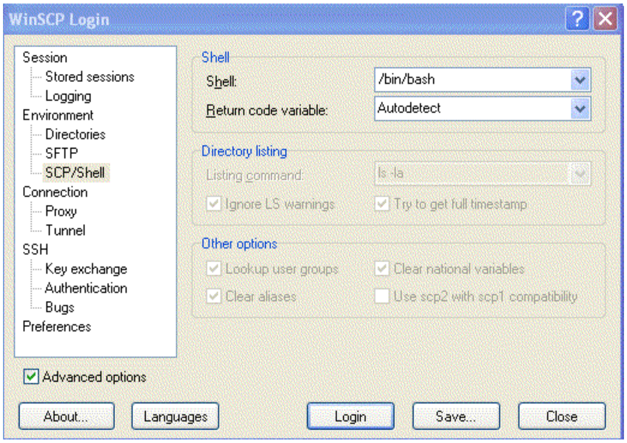
☑ Advanced options

Perform the following steps:

1. At the **Hostname** field, enter the IP address that you assigned to the management interface at the OS-Esystem. Port **22** is the default port number for SSH sessions.

2. At the **Username** and **Password** fields, type *root* for the username and *sips* for the password.

3. At the Environment menu, select **SCP/Shell** and select **/bin/bash** from the pull-down menu, as illustrated in the image below. Leave all other fields at their default settings.



WinSCP Login

Shell

Shell: /bin/bash

Return code variable: Autodetect

Directory listing

Listing command: ls -la

☑ Ignore LS warnings ☑ Try to get full timestamp

Other options

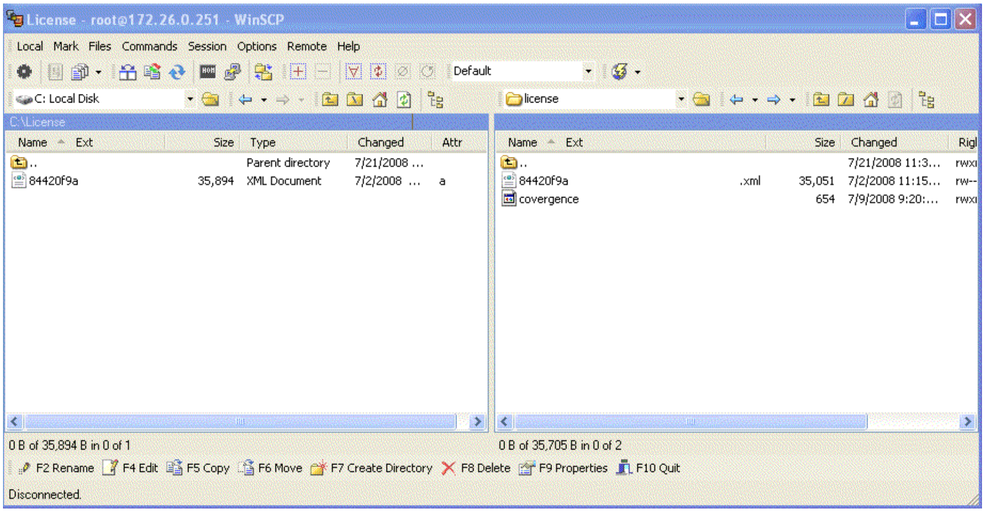
☑ Lookup user groups ☑ Clear national variables

☑ Clear aliases □ Use scp2 with scp1 compatibility

☑ Advanced options

4. Click **Login**. A series of progress message will appear as the connection is established.

5. From the left pane, browse and locate the license file, then drag the license to the *cxc/license* directory, as illustrated in the image below . In this example, the file is copied from the **c:\license** directory to the **cxc/license** directory OS-E.



C:\License

Name	Ext	Size	Type	Changed	Attr
..			Parent directory	7/21/2008 ...	
84420f9a		35,894	XML Document	7/2/2008 ...	a

Name	Ext	Size	Changed	Rigl
..			7/21/2008 11:3...	rwxı
84420f9a	.xml	35,051	7/2/2008 11:15...	rw--
covergence		654	7/9/2008 9:20:...	rwxı

0 B of 35,894 B in 0 of 1

0 B of 35,705 B in 0 of 2

Disconnected.

6. Once the license file is present in the *cxc/license* folder, you will need to do one of the follow tasks for the OS-E license to take effect:

   - Perform a physical restart of the OS-E system, or
   - From a CLI session to the device, execute the **license apply** action, as follows:

```
NNOS-E> license apply /cxc/license/
   84420g9a-da13-3007-8853-z00a7a4d771d.xml
Success!

NNOS-E> show licenses

name: LICENSE for Company.com
description: LICENSE for Company.com
        key: 84420g9a-da13-3007-8853-z00a7a4d771d
    expires:
       file: 84420g9a-da13-3007-8853-z00a7a4d771d.xml
```

Net-Net OS-E Commissioning Steps

You will need to perform the steps in this section to properly boot and license new NN2600 series systems and third-party servers.

Caution: Before starting, make sure that you have an operating terminal/ console attached to the system. Refer to Chapter 2 for the appropriate console serial port for the platform or third-party server you are commissioning. Perform any pre-installation tasks that may involve insertion and removal of the USB stick prior to beginning this sequence of steps.

If you are installing IBM X3550 or X3650 servers, see Chapter 2 for information on initializing RAID drives in the event that you have new factory servers delivered with uninitialized RAID configurations.

Note: For third-party platforms and servers, ensure that you have followed the vendor-supplied instructions for initial setup, followed by any changes to BIOS and other importang settings prior to OS-E commissioning.

1. Insert the USB drive into one of the USB ports on the device you are commissioning.
2. Restart or reboot the platform or third-party server.

   Refer to the documentation supplied with the platform for specific information on restarting and rebooting the device.
3. The USB and disk lamps will blink during the boot-up process followed by a series of system messages. **Press any key to continue,** or perform the appropriate action below for specific hardware.
   - **IBM X3550 and HS21** — Press **F12**.
   - **Dell 1950 and 2950** — Press **F11**.
   - **Dell R220** — Press **F11**.

4. When the GNU GRUB window appears, you will have the opportunity to select the port where your console device is connected. If you made the correct selection when you originally created the USB stick with the BMC (covered in Chapter 1), simply wait 10 seconds for the installation to begin. If you need to make a selection that is now different, follow the instructions on the menu to direct management output to the desired console port.

```
GNU GRUB  version 0.97  (639K lower / 1045376K upper memory)

+--------------------------------------------------------------+
Acme Packet USB Setup (Default)
Acme Packet USB Setup (force VGA console)
Acme Packet USB Setup (force 1st serial Port @115200,n,8,1)
Acme Packet USB Setup (force 2nd serial port @115200,n,8,1)
+---------------------------------------------------------------+
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the
      commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 10 seconds.
```

5. If a stick needs to be removed because the system will not reboot after the initial installation, reinsert the stick into the system at any point during the following sequence.

```
Loading Stage 1.5…
Grub Loading Please Wait...
Press any key to continue
Press any key to continue
```

6. Wait for the series of messages to complete over several minutes.

Note: If using a VGA console, you will presented with **login** prompt. Type *root* and press **Enter**.

7. At the username: and password: prompts, press **Enter** at each prompt to bypass the login and to display the NNOS-E prompt. Later, you will be able to configure users with appropriate user names and passwords.

```
Acme Packet, Inc.
Copyright (c) 2004-2009 Acme Packet, Inc.

username: <Enter>
password: <Enter>

Access granted since there are no configured users
Type 'config setup' to configure your system.
```

8. Execute the **show licenses** command to display licensing information. The information includes the name, description, key, file name, and the expiration date of the license.

```
NNOS-E> show licenses

       name: CUSTOMER ONE LICENSE
description: LICENSE FOR CUSTOMER ONE
        key: 84420f9a-da13-4107-8833-d00b7d4d751d
    expires:
       file: 84420f9a-da13-4107-8833-d00b7d4d751d.xml
```

   If **show licenses** does not display any information, make sure that the USB stick is inserted and perform a **restart warm**.

9. At the NNOS-E prompt, type **umount usb** to properly dismount the USB stick. Physically remove the USB stick from the USB port. This is now your utility USB device. Refer to Using the Rescue Utility USB for information.

10. If the platform contains additional drives to be used for data (physical or a logical due to RAID) then they need to be added to the system before they can be used. To format and attach the first data drive to the system formatted with the XFS file system format, enter the following command:

    >**format data-1 xfs**

    Use **data-2** if there is a second data driver to be formatted and added, and so on.

    If an existing data drive is being added to the system, for example when commissioning an existing system, use the OS-E **add-device** to attach drives.

    Note that this only applies to data drives formatted from an existing OS-E system and not an arbitrarily formatted drive. Ensure you specify the correct file-system type as what the drive was originally formatted.

    To attach the first data drive to the system formatted with the XFS file system format, enter the following command:

    >**add-device data-1 xfs**

11. Configure the OS-E software for your network. Run the setup script to configure basic IP connectivity and services. See Using the Setup Script.

Using the Setup Script

An optional configuration setup script called *cxc.setup* is included with the OS-E software. After installing a new system, you can run the script directly from the NNOS-E> prompt, as shown in the example session below.

The script presents a set of questions to help you with the initial system configuration. The information in the script includes the following:

- Local hostname
- IP interface names and addresses
- SSH and Web access
- Default route and any additional static routes per interface for remote management
- User-defined OS-E

Oracle OS-E systems have a minimum of two Ethernet interfaces. Any Ethernet interface on the system can be used for management traffic, however, Oracle recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other OS-E systems. Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI Session

```
NNOS-E> config setup
set box\hostname: <name>
config box\interface: eth1
set box\interface eth1\ip a\ip-address: <ipAddress/mask>
config box\interface eth1\ip a\ssh (y or n)? y
config box\interface eth1\ip a\web (y or n)? y
config box\interface eth1\ip a\routing\route: <routeName>
set box\interface eth1\ip a\routing\route localGateway\gateway:
<ipAddress>
set box\cli\prompt: <newPrompt>
Do you want to commit this setup script (y or n) y
Do you want to update the startup configuration (y or n)? y
```

Creating a New USB Rescue Stick

The **restore-stick-create full-backup** action allows captures the current OS-E software and the operating system image and creates a new USB rescue stick. Oracle recommends that you use **restore-stick-create full-backup** to preserve the image prior to performing a system software upgrade, or whenever you have made significant and reliable changes to the system configuration.

Perform the following steps:

1. At the NNOS-E prompt, type **umount usb**.

   Ignore the warning about the USB stick not being mounted.

2. Remove the USB stick and wait at least five seconds before reinserting the stick.

3. Invoke the **restore-stick-create full-backup** action. The resulting USB is a boot device from which you can restart and restore the OS-E.

Note: The log event indicating that the operation has completed successfully appears while data is being written to the stick. DO NOT immediately remove the USB stick when you see this log event. Instead, issue the **umount usb** command again, and wait for it to complete.

4. Remove the restore USB when the **restore-stick-create** action has completed.

Note: PostgreSQL database, media recordings, system tar files(.gz) are not written to the restore stick with the **restore-stick-create** action.

Note: Use the **restore-stick-create config-backup** action to create a restore stick containing the current configuration file only.

Using the Rescue Utility USB

To use the rescue utility USB, perform the following steps:

1. Insert the rescue utility USB into one of the USB slots.

2. At the NNOS-E prompt, if available, enter **restart cold** to do a full restart.

3. The USB and disk lamps will blink during the boot-up process followed by a series of system messages. Press any key to continue, or perform the appropriate action below. On the

   - **Sun Netra X3-2**—Press **F8.**
   - **HPDL360 G7**—Press **F11**.
   - **HPDL585 G7**—Press **F11**.
   - **HPDL320 G8**—Press **F11**.
   - **HPDL360 G8**—Press **F11**.
   - **CXC-350** — Press the **ESC** key.
   - **Sun x4150** — Press **F8**.
   - **IBM X3650, X3550, X-3350** — Press **F12**.
   - **Dell 1950 and 2950** — Press **F11**.
   - **Dell R220** — Press **F11**.
   - **IBM HS20 and HS21** — Press **F12**.
   - **Fugitsu Siemens RX200 S5** — Press **F12**.
   - **Fugitsu Siemens RX300 S4** — Press **F12**.
   - **ATCA MCLB0040** — Press **F8**.

4. The system enters utility mode and the following menu appears:

```
MAIN MENU
=========
Please select from the following menu below:

1) Save config, install to system drive, restore config
2) Expert mode
3) Debug mode
4) Reboot

Choice:
```

The choices (by number) are as follows:

1). **Save config, install to system drive, restore config**

This function saves the current configuration file (*cxc.cfg*), license, and related files to the USB stick, reinstalls the OS-E software, and then restores the saved configuration files to the OS-E system.

2). **Expert mode** — Displays the following menu:

```
EXPERT MENU
===========

Please select from the following menu below:

1) Do not format and install to partition 4
2) Commission only the system drive
3) Save configs, license, certs and secrets
4) Restore configs, license, certs and secrets
5) Decommission box (VERY dangerous)

q) Return to main menu

Choice:
```

See Using the Expert Mode.

3). **Debug mode** — Displays the debug menu.

Caution: The selections in the debug menu are diagnostic functions and should only be used with assistance from Oracle Technical Support.

```
DEBUG MENU
==========
Please select from the following debug menu below:

1) Shell
2) Disable debug mode
3) Disk repair (fsck)
4) Filesystem repair (fsck --rebuild-tree)
5) Check for disk errors (bad blocks)
6) Mount drives (1st system drive - partition 3)
7) Mount drives (2nd system drive - partition 4)
8) Unmount all drives
9) Fix MBR on system drive (ie GRUB)
a) Set default GRUB boot title item
b) Make USB stick bootable
c) Make USB stick un-bootable
q) Return to main menu

Choice:
```

4). **Reboot** — Performs a **restart cold** action.

Using the Expert Mode

The Expert mode provides utilities that allow you to recover from system failures where there is apparent damage to the software and configuration file, and where recovery is necessary to return the OS-E to normal operation. The Expert mode functions are provided below:

1. **Do not format and install to partition 3/4**

   With Release 3.5.0 and later, this function reinstalls the OS-E to partition 3 (System 1) or partition 4 (System 2) on the system disk drive. Using partitions, you can install more than one release and use the **set-chassis-config-boot** action to select the system (and release) to run at system startup. No formatting of the system drive will occur under this function.

2. **Commission only the system drive**

   If used in conjunction with the “Do not format and install to partition 3/4” option above, this function installs the OS-E software and leaves the current configuration file and licenses intact. See Net-Net OS-E Commissioning Steps.

Warning: If you did not choose the “Do not format and install to partition 3/4” option first, the system drive WILL BE formatted and all configuration and related data will be lost.

3. **Save configs, license, certs and secrets**

   This function saves the current configuration file(s), license, certificates, and secrets from the current partition to the USB rescue stick. Oracle recommends that you use this function on a frequent basis to create an up-to-date rescue stick.

4. **Restore configs, licenses, certs, and secrets**

   This function copies the configuration file(s), license, certificates, and secrets from the USB rescue stick to the current OS-E partition. Use this function, for example, to replace the current configuration file with a previous version, or if there was damage to any of the files (licenses, certs, secrets) during a system failure.

5. **Decommission box (VERY dangerous)**

   This function removes the OS-E software, configuration files, license, certificates, and secrets. The resulting system will not be bootable after using this function. You will then be required to commission the device from scratch.

System and Data Drive Locations

The following system and data drive locations are for Oracle Net-Net OS-E hardware. For all other supported platforms and third-party servers, refer to the documentation that accompanies the hardware.

- **NN 2610**— System drive is disk 1 (left slot); remaining drives (2) are data drives.
- **NN 2620**— System RAID-1 drives are disk 1 (lower left slot) and disk 2 (upper left slot); remaining RAID-10 drives (4) are data drives
- **CXC-50** — Single disk only for both system and data.
- **CXC-350 and CXC-354** — System drive is disk 1 (left slot); remaining drives (2) are data drives.
- **CXC-550** — System drive is disk 1 (top left slot); data drive is disk 2 (lower left slot).
- **CXC-554** — System RAID-1 drives are disk 1 (lower left slot) and disk 2 (upper left slot); remaining RAID-10 drives (4) are data drives.
- **CXC-1250** — System drive is disk 1 (left slot); disk 2 is a data drive.

Installing and Running the OS-E Virtual Machine

This chapter provides information on downloading, installing, and running the OS-E Virtual Machine (VM) software in virtual OS environments. This software is the same software as used for non-virtual OS but has been packaged specifically as a VM for use in virtual OS environments.

The OS-E VM is designed to be used as an evaluation platform so that potential customers can test the OS-E software in an environment that does not require them to install the software on a dedicated piece of hardware. In some cases, the VM can also be used in production environments provided that the customer understands the limitations associated with using the VM software in a virtual OS environment.

Server-Based Requirements

Before downloading the VM to an x86-based server, make sure that you have met the following hardware and software requirements:

Hardware

- x86-based Windows or Linux server with Intel 32- or 64-bit dual-core processors
- 2GB minimum (4 GB recommended) physical memory for each VM instance
- Minimum of 40GB hard disk space per VM instance
- One or two Ethernet interfaces

Software

The following VM platforms have been certified for use with the OS-E:

- OVM 3.3.1
- VMware ESXi 5.5
- XEN 3.4.3
- KVM 1.5.3

Linux Installations

If you are installing the OS-E VM on a Linux workstation running VMware, Oracle recommends the following technical resources:

For Server 1.0

http://www.vmware.com/support/pubs/server_pubs.html

Player 1.0 and 2.0

http://www.vmware.com/support/pubs/player_pubs.html

Installing the VM

This section describes the process for installing the OS-E VM on each of the certified VM platforms.

Installing the OS-E on an Oracle Virtual Machine

The OS-E is certified to run on the Oracle Virtual Machine (OVM) 3.3.1.

Prerequisites

You must meet the following prerequisites before installing the OS-E on an OVM:

- A Network File System (NFS) has been mounted for VM storage with an additional storage file server for repository
- A server pool has been created
- Server(s) have been discovered and added to this pool

- The ISO file has been imported
- Networks and Virtual MAC range have been created
- VM Console access (VNC) has been made available

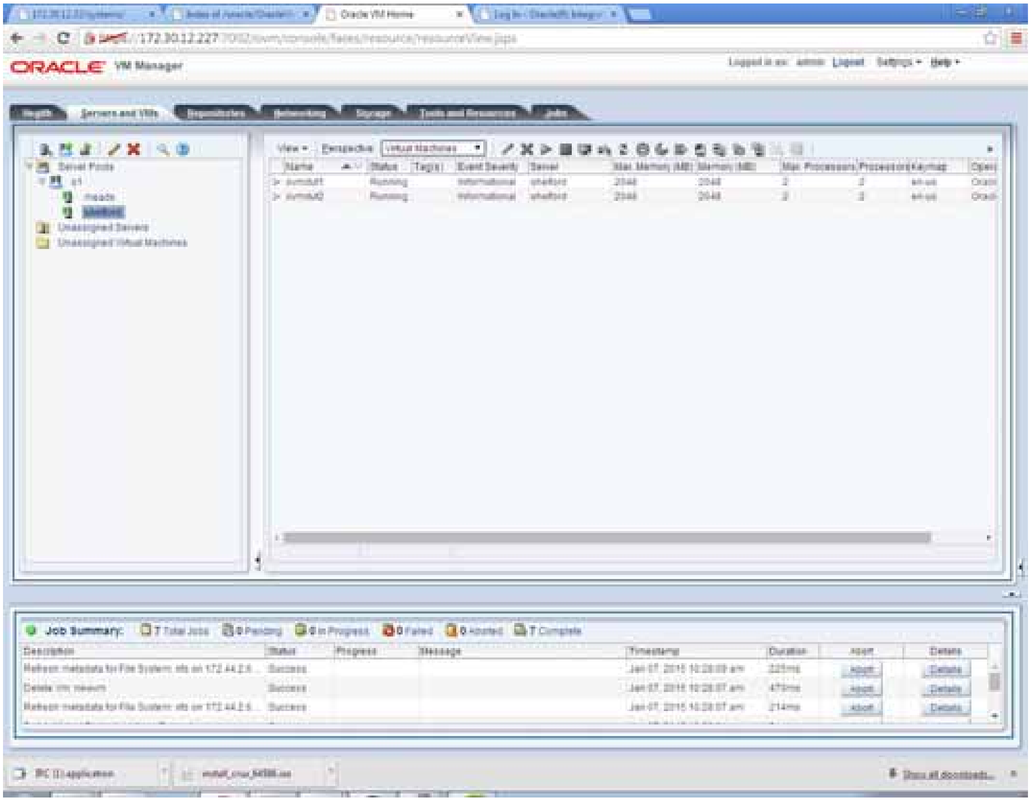
You create the OS-E VM via the OVM Manager GUI. The OVM Manager binds to the weblogic server on the Oracle Linux host’s 7002 SSL port.

Access the OVM Manager using the following link:

`https://`*`x.x.x.x`*`:7002/ovm/console`

Where *x.x.x.x* is the OVM Manager’s IP address.

1. Log into the OVM Manager using the user name and password configured when you set up the OVM.
2. Create external routable interfaces by selecting the **Networking** tab, selecting the **Networks** button, and clicking the plus (+) icon.



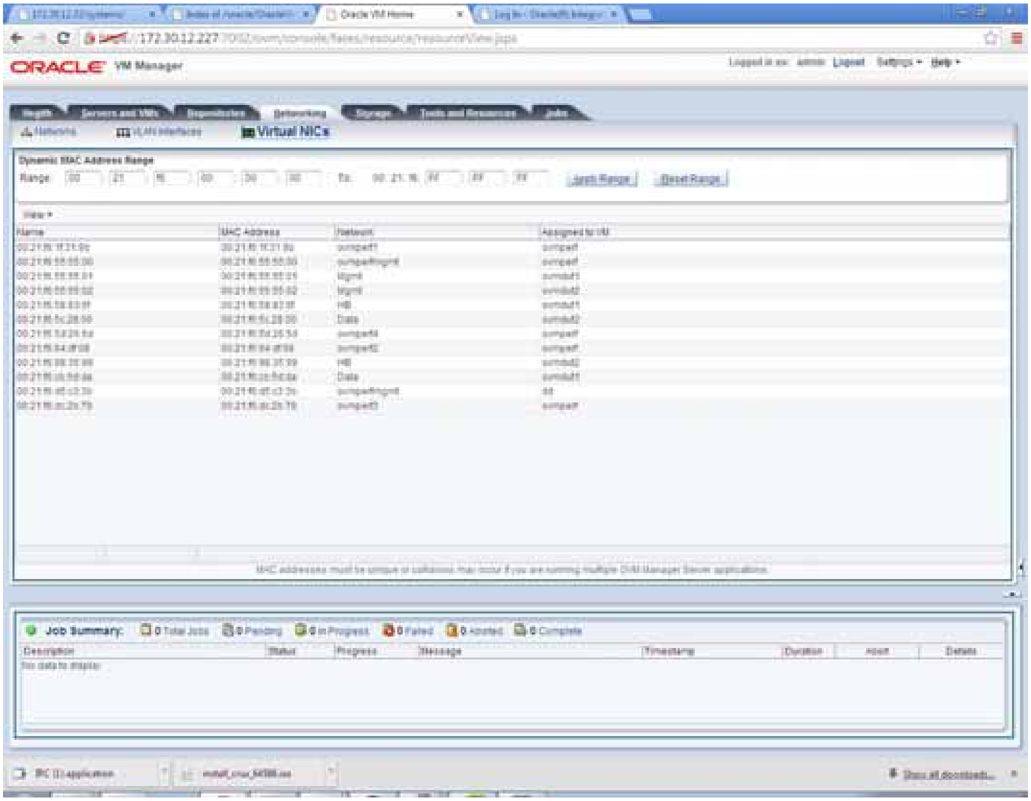
3. Create a new bridge **bonds/ports only** and select **Virtual Machine** in the **Network Uses** field.

4. Bind the new bridge to a free port on the VM host.

5. *Optional*. Create a heartbeat interface (if you choose to configure clustered VMs) by selecting the **Networking** tab, selecting the **Networks** button, and clicking the plus (+) icon.

6. Create a new bridge local network only and select **Virtual Machine** in the **Network Uses** field.

7. Create MAC addresses for each Virtual NIC by selecting the **Networking** tab, selecting the **Virtual NICs** button, and creating a **Dynamic MAC Address Range**.



Dynamic MAC Address Range

Range: 00 : 21 : f6 : 00 : 00 : 00 To: 00 : 21 : f6 : ff : ff : ff

Name	MAC Address	Network	Assigned to VM
00:21:f6:1f:21:0c	00:21:f6:1f:21:0c	csmpaif1	csmpaif
00:21:f6:55:55:00	00:21:f6:55:55:00	csmpaifmgmt	csmpaif
00:21:f6:55:55:01	00:21:f6:55:55:01	Mgmt	csmdut1
00:21:f6:55:55:02	00:21:f6:55:55:02	Mgmt	csmdut2
00:21:f6:58:83:ff	00:21:f6:58:83:ff	HB	csmdut1
00:21:f6:5c:28:50	00:21:f6:5c:28:50	Data	csmdut2
00:21:f6:5d:25:5d	00:21:f6:5d:25:5d	csmpaif4	csmpaif
00:21:f6:84:df:08	00:21:f6:84:df:08	csmpaif2	csmpaif
00:21:f6:98:35:99	00:21:f6:98:35:99	HB	csmdut2
00:21:f6:cb:5d:da	00:21:f6:cb:5d:da	Data	csmdut1
00:21:f6:d5:c3:3c	00:21:f6:d5:c3:3c	csmpaifmgmt	dd
00:21:f6:dc:2b:79	00:21:f6:dc:2b:79	csmpaif3	csmpaif

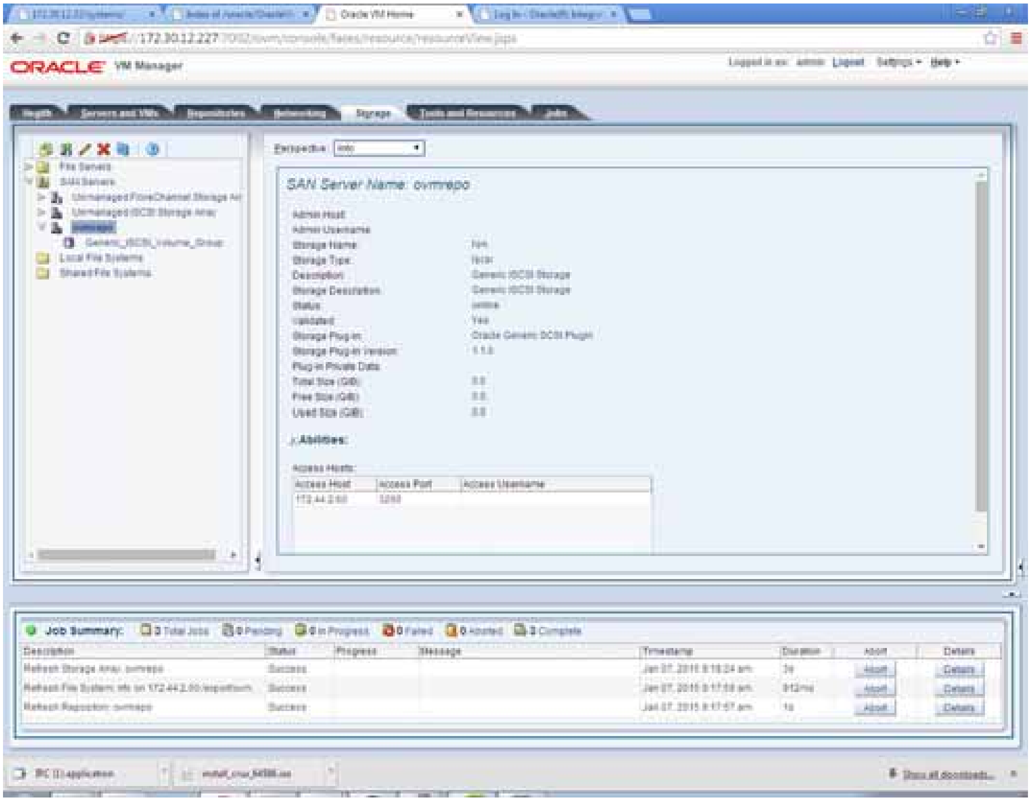
MAC addresses must be unique or collisions may occur if you are running multiple OVM Manager Server applications.

Job Summary: 0 Total Jobs 0 Pending 0 In Progress 0 Failed 0 Aborted 0 Complete

Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
No data to display.							

Note: You must create a unique MAC address for each Virtual NIC.

As mentioned previously in Prerequisites, you must mount an NFS to host the OS-E. The following image shows a properly configured NFS mount point for the VM.



Perspective: Info

SAN Server Name: ovmrepo

Admin Host	
Admin Username	
Storage Name	Nas
Storage Type	iscsi
Description	Generic iSCSI Storage
Storage Description	Generic iSCSI Storage
Status	online
Validated	Yes
Storage Plug-in	Oracle Generic iSCSI Plugin
Storage Plug-in Version	1.1.0
Plug-in Private Data	
Total Size (GiB)	0.0
Free Size (GiB)	0.0
Used Size (GiB)	0.0

Abilities:

Access Hosts:

Access Host	Access Port	Access Username
172.44.2.60	3260	

Job Summary: 3 Total Jobs 0 Pending 0 In Progress 0 Failed 0 Aborted 3 Complete

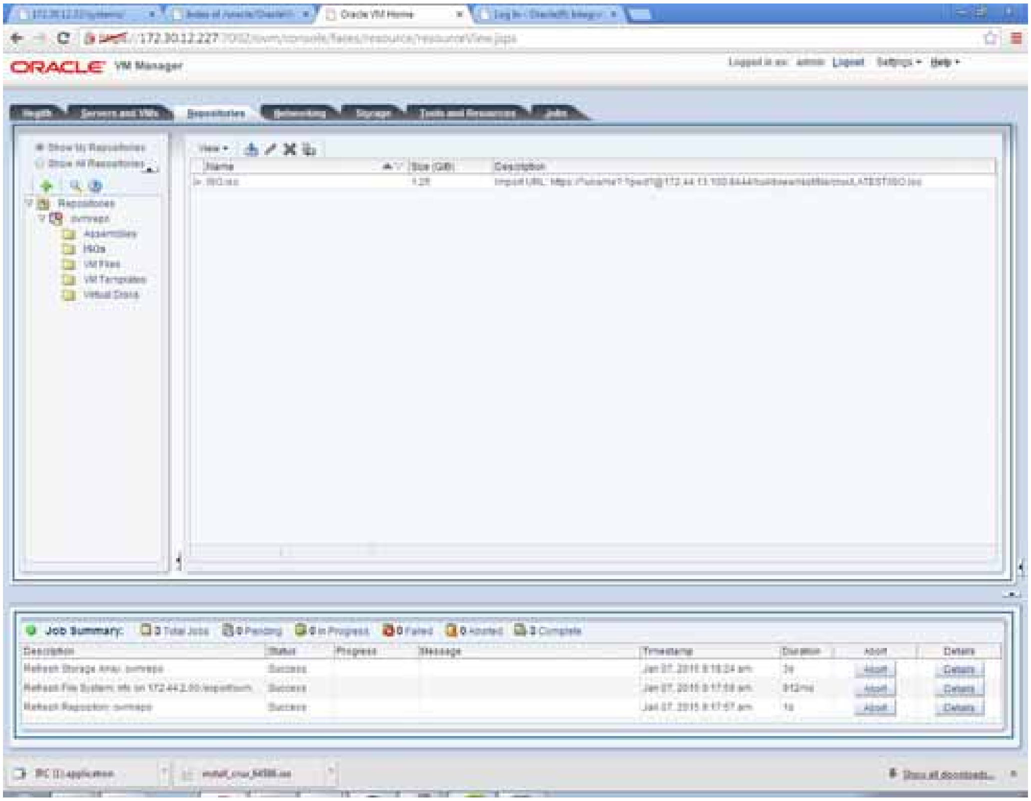
Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
Refresh Storage Array: ovmrepo	Success			Jan 07, 2015 8:18:24 am	3s	Abort	Details
Refresh File System: info on 172.44.2.60:/exportovm	Success			Jan 07, 2015 8:17:58 am	912ms	Abort	Details
Refresh Repository: ovmrepo	Success			Jan 07, 2015 8:17:57 am	1s	Abort	Details

When creating a VM, your storage repository contains an ISO file and the new VM immediately boots from the Virtual DVD.

To boot the VM from the Virtual DVD.

1. Select the **Repositories** tab and select the repository you created from the **File Server**.
2. Select **ISOs**.

3. Via HTTP, import the OS-E’s .iso code.



Name	Size (GiB)	Description
ISO.iso	1.25	Import URL: https://[illegible]@172.44.13.100:8444/[illegible]/LATEST/ISO.iso

Job Summary: 3 Total Jobs 0 Pending 0 In Progress 0 Failed 0 Aborted 3 Complete

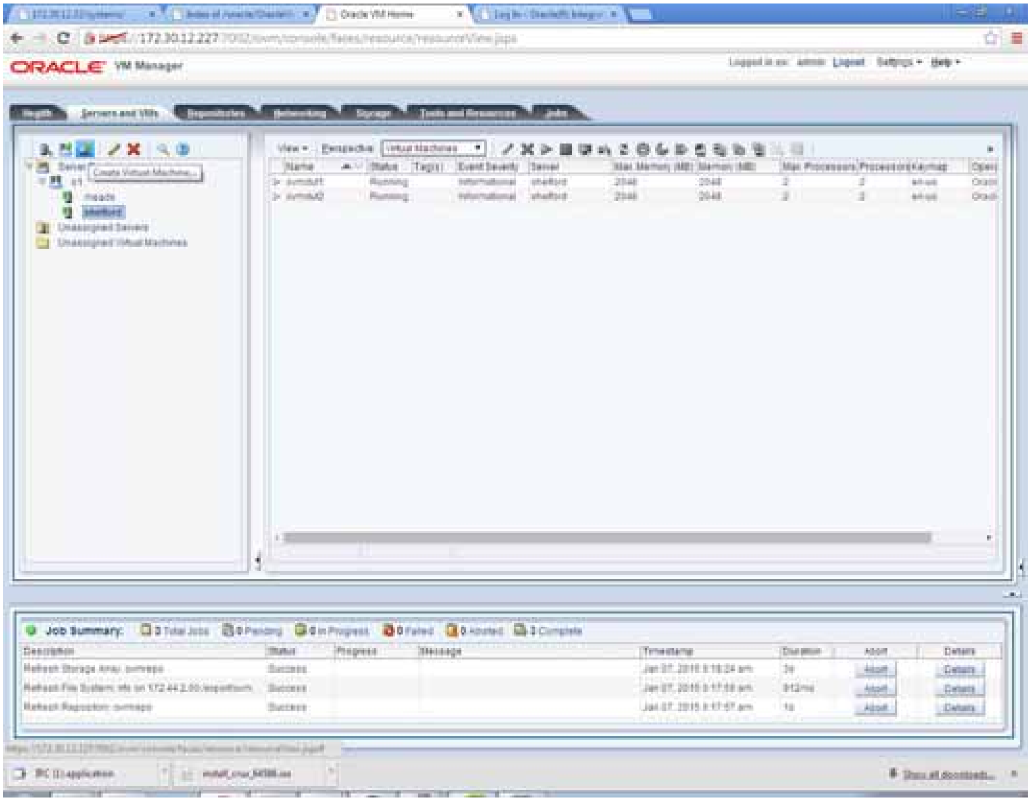
Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
Refresh Storage Array: ovmrepo	Success			Jan 27, 2015 9:18:24 am	3s	Abort	Details
Refresh File System info on 172.44.2.00:/export/ovm	Success			Jan 27, 2015 9:17:58 am	912ms	Abort	Details
Refresh Repository: ovmrepo	Success			Jan 27, 2015 9:17:57 am	1s	Abort	Details

You are now ready to create a VM.

To create a VM:

1. Select the **Servers and VMs** tab and choose the server on which you are hosting the VM.

2. Select **Create Virtual Machine**.



https://172.30.12.227:7002/ovm/console/faces/resource/resourceView.jspx

ORACLE VM Manager

Logged in as: admin Logout Settings ▾ Help ▾

Health | Servers and VMs | Repositories | Networking | Storage | Tools and Resources | Jobs

Create Virtual Machine...

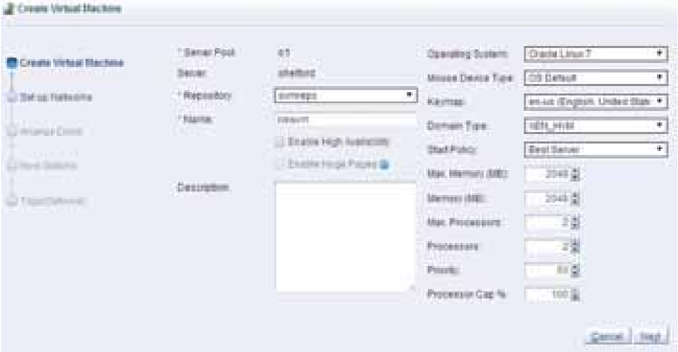
View ▾ Perspective: Virtual Machines ▾

Name	Status	Tag(s)	Event Severity	Server	Max. Memory (MB)	Memory (MB)	Max. Processors	Processors	Keymap	Oper
ovmdut1	Running		Informational	shelford	2048	2048	2	2	en-us	Oracl
ovmdut2	Running		Informational	shelford	2048	2048	2	2	en-us	Oracl

Job Summary: 3 Total Jobs 0 Pending 0 In Progress 0 Failed 0 Aborted 3 Complete

Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
Refresh Storage Array: ovmrepo	Success			Jan 07, 2015 9:18:24 am	3s	Abort	Details
Refresh File System: nfs on 172.44.2.00:/export/ovm	Success			Jan 07, 2015 9:17:58 am	812ms	Abort	Details
Refresh Repository: ovmrepo	Success			Jan 07, 2015 9:17:57 am	1s	Abort	Details

3. Click **Next**.

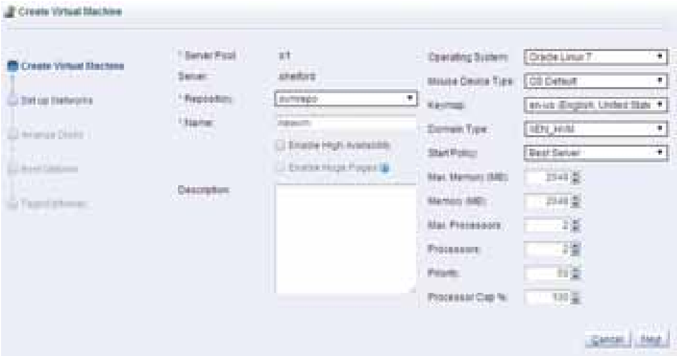


Create Virtual Machine

* Server Pool	41	Operating System	Oracle Linux 7
Server	shelford	Mouse Device Type	OS Default
* Repository	ovmrepo	Keymap	en-us (English, United State
* Name	newvm	Domain Type	Xen_HVM
	□ Enable High Availability	Start Policy	Best Server
	□ Enable Huge Pages	Max. Memory (MB)	2048
Description		Memory (MB)	2048
		Max. Processors	2
		Processors	2
		Priority	50
		Processor Cap %	100

4. Specify a **Name** and set the **Memory** and **Processors** for this VM.

Note: The default **Memory** is **1024** and the default number of **Processors** is **1**.

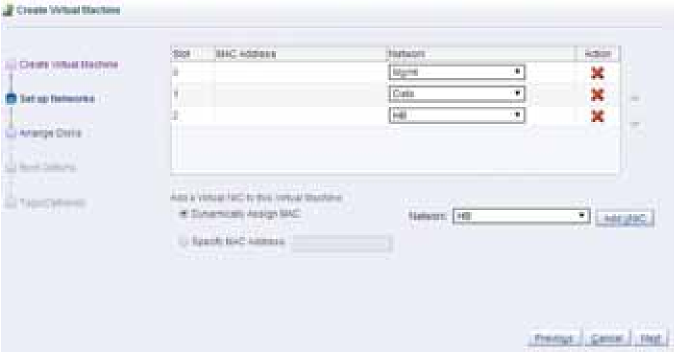


Create Virtual Machine

* Server Pool:	x1
Server:	[illegible]
* Repository:	[illegible]
* Name:	[illegible]
☐ Enable High Availability	
☐ Enable Huge Pages	
Description:	
Operating System:	Oracle Linux 7
Mouse Device Type:	OS Default
Keymap:	en-us (English, United State
Domain Type:	XEN_HVM
Start Policy:	Best Server
Max. Memory (MB):	2048
Memory (MB):	2048
Max. Processors:	2
Processors:	2
Priority:	50
Processor Cap %:	100

5. Click **Next**.
6. Select your networks.

   Note: The order you select the networks affects how the OS-E ethernets align.



Create Virtual Machine

Slot	MAC Address	Network	Action
0		Mgmt	✖
1		Data	✖
2		HB	✖

Add a Virtual NIC to this Virtual Machine

● Dynamically Assign MAC

○ Specify MAC Address

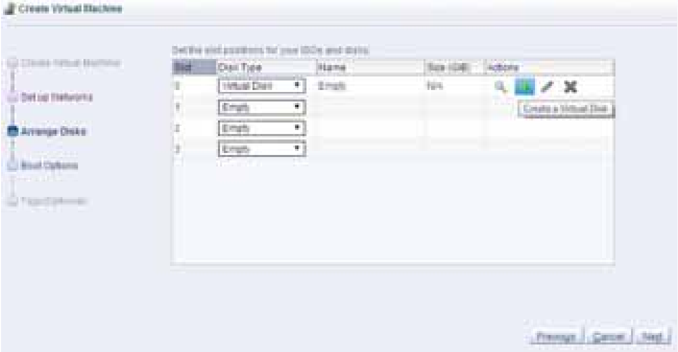
Network: HB

7. Click **Next**.

   These MAC addresses (whether assigned dynamically or statically) now appear as assigned MAC addresses under the Virtual NICs tab in OVM Manager.

To create the VM virtual disk:

1. Select the Virtual Disk’s **Disk Type** and select the **Create a Virtual Disk** icon.

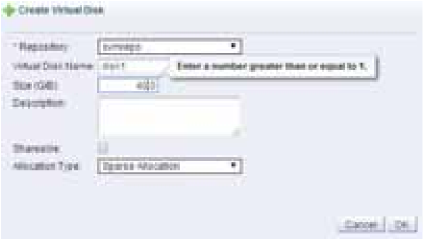


Set the slot positions for your ISOs and disks.

Slot	Disk Type	Name	Size (GB)	Actions
0	Virtual Disk	Empty	N/A	
1	Empty			
2	Empty			
3	Empty			

2. Click **Next**.

3. Select the previously-created **Repository** and enter a **Virtual Disk Name** and a **Size** (Oracle recommends 40 GB).

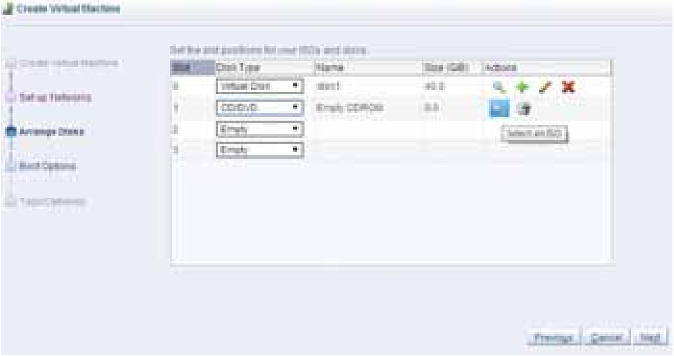


* Repository: [illegible]
Virtual Disk Name: disk1
Size (GB): 40.0
Description:
Shareable: □
Allocation Type: Sparse Allocation

4. Click **OK**.

To point the OS-E ISO code to commission the VM:

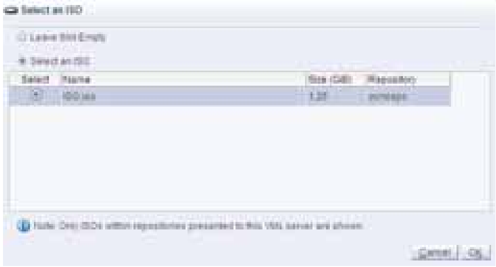
1. Select **CD/DVD** from the Slot 2 **Disk Type** drop-down menu and select **Select an ISO**.



Set the slot positions for your ISOs and disks.

Slot	Disk Type	Name	Size (GB)	Actions
0	Virtual Disk	disk1	40.0	
1	CD/DVD	Empty CDROM	0.0	
2	Empty			
3	Empty			

2. Click **Next**.
3. Select the previously-imported ISO..



Select	Name	Size (GiB)	Repository
○	ISO.iso	1.25	[illegible]

Note: Only ISOs within repositories presented to this VM server are shown.

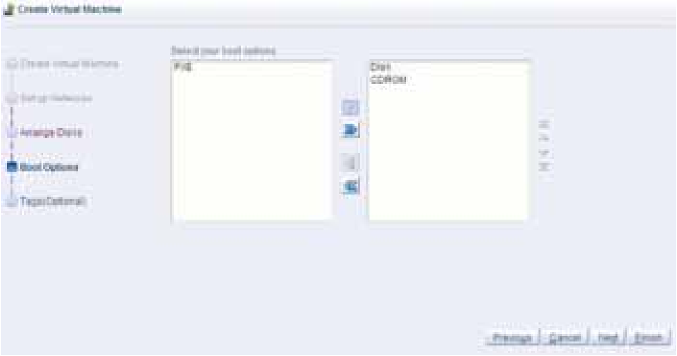
4. Click **OK**

Once the OS-E ISO code is pointed to commission the VM, set the Boot Options. The first time you boot you utilize the CDRom as nothing resides on the Disk yet. All subsequent boots utilize the Disk and ignore the CDRom.

> Note: If you choose CDRom as the first boot option, the initial boot, as well as all subsequent boots, continue to utilize the CDRom.

To set the Boot Options:

1. Select **Disk**.
2. Select **CDRom**.



Select your boot options:

PXE

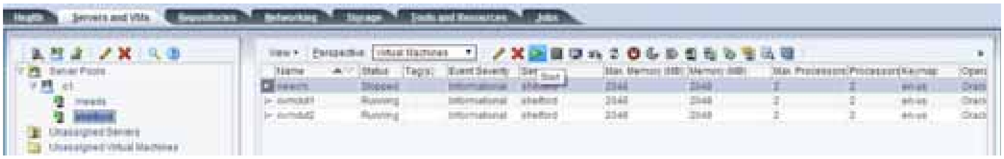
Disk
CDROM

3. Click **Finish**.

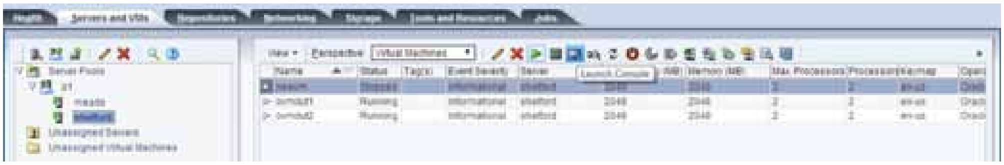
To see the newly-created VM, select the **Servers and VMs** tab and click **Virtual Machines** from the **Perspective** drop-down menu. At this point in the installation process, the **Status** of the VM is **Stopped**.

To start the VM:

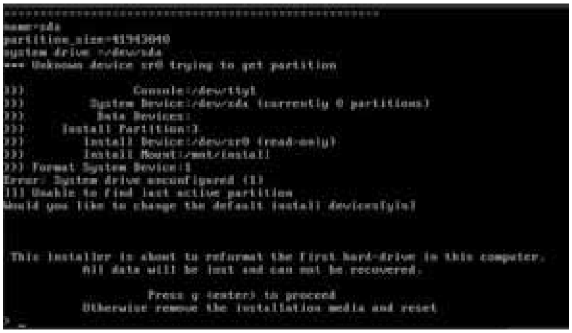
1. Select **Start** to start the VM.



2. Select **Launch Console**.



The OVM Console now displays the installation process. Eventually the following screen appears.



```
===============================================================
name=sda
partition_size=41943040
system drive =/dev/sda
*** Unknown device sr0 trying to get partition

)))                  Console:/dev/tty1
)))            System Device:/dev/sda (currently 0 partitions)
)))             Data Devices:
)))         Install Partition:3
)))           Install Device:/dev/sr0 (read-only)
)))           Install Mount:/mnt/install
))) Format System Device:1
Error: System drive unconfigured (1)
!!! Unable to find last active partition
Would you like to change the default install device[y|n]


 This installer is about to reformat the first hard-drive in this computer.
          All data will be lost and can not be recovered.

                   Press y <enter> to proceed
          Otherwise remove the installation media and reset
> _
```

3. Type **y** and press ***<Enter>*** to complete the installation process.

   The VM reboots and once the installation is complete you see the OS-E login prompt. The OS-E is now ready to be set up and configured.

Configuring OVM Passthrough

On the OVM, there are two ways to directly connect a VM to a physical port: Single Root I/O Virtualization (SR-IOV) and Peripheral Component Interconnect (PCI) Passthrough. You configure hardware passthrough at the OVM Server's CLI.

> **Note:** Prior to configuring hardware passthrough, you must have a fully built VM, however, any NICs designated for hardware passthrough may not have an associated Network. For more information on specifying an NIC Network, see page 196.

SR-IOV is a specification that treats a single physical device as multiple separate Virtual Functions (VF)s.

> **Note:** In development, SR-IOV was found to be available on 10GB ixgbe devices only.

To configure SR-IOV:

1. Access and log into the OVM Server's CLI.

2. Install the necessary packages on the OVM Server.

```
libibumad-1.3.8-2.mlnx1.5.5r2.el5.x86_64.rpm
libibmad-1.3.9-7.mlnx1.5.5r2.el5.x86_64.rpm
opensm-libs-3.3.15-6.mlnx1.5.5r2.el5.x86_64.rpm
kernel-ib-1.5.5.092-2.6.39_300.29.1.el5uek.x86_64.rpm
infiniband-diags-1.5.13.MLNX_20120708-4.mlnx1.5.5r2.el5.x86_64.rpm
ovsvf-config-1.0-6.noarch.rpm
```

3. Create a python script called **vnfs.py** to view and marry PCI addresses to interfaces.

```
#!/usr/bin/python
# Copyright (C) 2012 Steve Jordahl
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU Lesser General Public License as
   published
# by the Free Software Foundation; version 2.1 only.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU Lesser General Public License for more details.
#
# vfns: list SR-IOV virtual functions

import os

info = {}

def catFile(filename):
        readfile = open(filename)
        return readfile.read().strip()
```

```
for dev in os.listdir('/sys/class/net'):
        if dev.startswith('eth'):
                info[dev] = {}
               info[dev]['address'] = catFile('/sys/class/net/' + dev
   + '/address')

for dev in info.keys():
        devLink = os.readlink('/sys/class/net/' + dev + '/device')
        info[dev]['pci address'] = devLink[-7:]
        os.chdir('/sys/class/net/' + dev)
        for devInfo in os.listdir(devLink):
                if devInfo.startswith('virtfn'):
                        info[dev][devInfo] =
   os.readlink(os.path.join(devLink,
devInfo))[-7:]

for dev in sorted(info.keys()):
        print dev
        for detail in sorted(info[dev].keys()):
                print "     " + detail + ":  " + info[dev][detail]
```

4. Create **/etc/pciback/pciback.sh**.

```
#!/bin/sh
if [ $# -eq 0 ] ; then
echo "Require a PCI device as parameter"
exit 1
fi
for pcidev in $@ ; do
if [ -h /sys/bus/pci/devices/"$pcidev"/driver ] ; then
echo "Unbinding $pcidev from" $(basename $(readlink /sys/bus/pci/
   devices/"$pcidev"/driver))
echo -n "$pcidev" > /sys/bus/pci/devices/"$pcidev"/driver/unbind
fi
echo "Binding $pcidev to pciback"
echo -n "$pcidev" > /sys/bus/pci/drivers/pciback/new_slot
echo -n "$pcidev" > /sys/bus/pci/drivers/pciback/bind
done
```

5. Use an Input/Output Memory Management Unit (IOMMU) to allow both the VM and physical devices access to memory. The IOMMU allows the OVM to limit what memory a device is allowed and gives the device the same virtualized memory layout that the guest sees.

```
Edit /boot/grub/grub.conf to enable iommu and comment out the existing
   kernel entry ( see example )

# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
   file
```

```
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sdb2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sdb
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Oracle VM Server-ovs (xen-4.3.0 3.8.13-26.4.2.el6uek.x86_64)
root (hd0,0)
        #kernel /xen.gz console=com1,vga com1=57600,8n1
   dom0_mem=max:1776M allowsuperpage dom0_vcpus_pin dom0_max_vcpus=20
        kernel /xen.gz console=com1,vga com1=57600,8n1
   dom0_mem=max:1776M allowsuperpage
   iommu=passthrough,no-qinval,no-intremap
        module /vmlinuz-3.8.13-26.4.2.el6uek.x86_64 ro
   root=UUID=e2b44279-55a5-48b9-b910-82446b7b8c65 rd_NO_LUKS
   rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16
   KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
        module /initramfs-3.8.13-26.4.2.el6uek.x86_64.img
```

6. Add SR-IOV support to ovs.conf.

   Note: The following example configures support for 10 VFs on the server’s 4 ixgbe interfaces (matching up to ethernets 9-12).

```
[root@meads ~]# vi /etc/modprobe.d/ovs.conf
options bnx2x disable_tpa=1
options ipv6 disable=1
# SRIOV support
options ixgbe max_vfs="10,10,10,10,0,0,0,0,0,0,0,0,0"
install ixgbe /sbin/modprobe pciback ; /sbin/modprobe --first-time
   --ignore-install ixgbe
```

7. Blacklist the Intel VF driver (ixgbevf) in dom0 so that the dom0 kernel does not try to use the VFs.

```
[root@Meads ~]# vi /etc/modprobe.d/blacklist.conf
#
# Listing a module here prevents the hotplug scripts from loading it.
# Usually that'd be so that some other driver will bind it instead,
# no matter which driver happens to get probed first.  Sometimes user
# mode tools can also control driver binding.
#
# Syntax:  driver name alone (without any spaces) on a line. Other
# lines are ignored.
#

# watchdog drivers
blacklist i8xx_tco
```

```
# framebuffer drivers
blacklist aty128fb
blacklist atyfb
blacklist radeonfb
blacklist i810fb
blacklist cirrusfb
blacklist intelfb
blacklist kyrofb
blacklist i2c-matroxfb
blacklist hgafb
blacklist nvidiafb
blacklist rivafb
blacklist savagefb
blacklist sstfb
blacklist neofb
blacklist tridentfb
blacklist tdfxfb
blacklist virgefb
blacklist vga16fb
# ISDN - see bugs 154799, 159068
blacklist hisax
blacklist hisax_fcpcipnp

# intel ixgbe sr-iov vf (virtual function) driver
blacklist ixgbevf
```

8. Reboot the OVM server.

9. Run the vnfs script to view addresses and VFs statistics.

```
[root@Meads ~]# ./vnfs.py
eth0
     address:  a0:36:9f:2c:39:74
     pci address:  30:00.0
eth1
     address:  a0:36:9f:2c:39:75
     pci address:  30:00.1
eth10
     address:  00:21:28:a1:e2:41
     pci address:  88:00.1
     virtfn0:  88:10.1
     virtfn1:  88:10.3
     virtfn2:  88:10.5
     virtfn3:  88:10.7
     virtfn4:  88:11.1
     virtfn5:  88:11.3
     virtfn6:  88:11.5
     virtfn7:  88:11.7
     virtfn8:  88:12.1
     virtfn9:  88:12.3
eth11
```

```
          address:  00:21:28:a1:e2:42
          pci address:  98:00.0
          virtfn0:  98:10.0
          virtfn1:  98:10.2
          virtfn2:  98:10.4
          virtfn3:  98:10.6
          virtfn4:  98:11.0
          virtfn5:  98:11.2
          virtfn6:  98:11.4
          virtfn7:  98:11.6
          virtfn8:  98:12.0
          virtfn9:  98:12.2
     eth12
     address:  00:21:28:a1:e2:43
          pci address:  98:00.1
          virtfn0:  98:10.1
          virtfn1:  98:10.3
          virtfn2:  98:10.5
          virtfn3:  98:10.7
          virtfn4:  98:11.1
          virtfn5:  98:11.3
          virtfn6:  98:11.5
          virtfn7:  98:11.7
          virtfn8:  98:12.1
          virtfn9:  98:12.3
     eth2
          address:  a0:36:9f:2c:39:76
          pci address:  30:00.2
     eth3
          address:  a0:36:9f:2c:39:77
          pci address:  30:00.3
     eth4
          address:  a0:36:9f:2d:0b:a8
          pci address:  a0:00.0
     eth5
          address:  a0:36:9f:2d:0b:a9
          pci address:  a0:00.1
     eth6
          address:  a0:36:9f:2d:0b:aa
          pci address:  a0:00.2
     eth7
          address:  a0:36:9f:2d:0b:ab
          pci address:  a0:00.3
     eth8
          address:  00:21:28:a1:e2:46
          pci address:  5f:00.0
     eth9
          address:  00:21:28:a1:e2:40
          pci address:  88:00.0
          virtfn0:  88:10.0
          virtfn1:  88:10.2
          virtfn2:  88:10.4
          virtfn3:  88:10.6
          virtfn4:  88:11.0
          virtfn5:  88:11.2
          virtfn6:  88:11.4
          virtfn7:  88:11.6
          virtfn8:  88:12.0
          virtfn9:  88:12.2
```

10. Run the module.

```
[root@meads ~]# modprobe xen-pciback
```

11. Assign devices to pciback in the format:

```
Domain 0:Bus:#:Device#:Function #).
```

Note: In the following example the 4 interfaces are VFs on ethernets 9-12.

```
[root@meads ~]# /etc/pciback/pciback.sh 0000:88:10.0
Unbinding 0000:88:00.0 from ixgbe
Binding 0000:88:00.0 to pciback

[root@meads ~]# /etc/pciback/pciback.sh 0000:88:10.1
Unbinding 0000:88:00.1 from ixgbe
Binding 0000:88:00.1 to pciback

[root@meads ~]# /etc/pciback/pciback.sh 0000:98:10.0
Unbinding 0000:98:00.0 from ixgbe
Binding 0000:98:00.0 to pciback

[root@meads ~]# /etc/pciback/pciback.sh 0000:98:10.1
Unbinding 0000:98:00.1 from ixgbe
Binding 0000:98:00.1 to pciback
```

12. View the list of VMs.

```
[root@meads ~]# xm list
Name                                      ID   Mem VCPUs      State
   Time(s)
0004fb0000060000f9b493a2c24f9549            7  8067    16     -b----
   80716.4
Domain-0                                    0  1775    20     r-----
   30379.2
```

13. View the list of assignable devices.

```
[root@meads ~]# xm pci-list-assignable-devices
0000:88:10.0
0000:88:10.1
0000:98:10.0
0000:98:10.1
```

14. Assign these devices to the VM.

Note: In the following example the VM ID is 7.

```
[root@meads ~]# xm pci-attach 7 0000:88:10.0
[root@meads ~]# xm pci-attach 7 0000:88:10.1
[root@meads ~]# xm pci-attach 7 0000:98:10.0
[root@meads ~]# xm pci-attach 7 0000:98:10.1
```

15. View the list of devices for this VM.

```
[root@Meads ~]# xm pci-list 7
Vdev Device
04.0 0000:88:10.0
05.0 0000:88:10.1
06.0 0000:98:10.0
07.0 0000:98:10.1
```

Now VFs on ethernets 9-12 are assigned to VM ID 7, but there are still VFs available to the host. These interfaces appear when you run the **ifconfig** command.

16. Access and log into the OS-E CLI and execute the following.

```
NNOS-E>echo “1” > /sys/bus//pci/rescan
NNOS-E>run ./install_build_mactab.sh
NNOS-E>restart warm
```

After the restart has completed, these interfaces are available on the OS-E.

PCI Passthrough is a specification that allows you to directly connect one VM to one physical device, making the device unavailable to other VMs.

To configure PCI Passthrough:

1. Access and log into the OVM Server’s CLI.

2. Install the necessary packages on the OVM Server.

```
libibumad-1.3.8-2.mlnx1.5.5r2.el5.x86_64.rpm
libibmad-1.3.9-7.mlnx1.5.5r2.el5.x86_64.rpm
opensm-libs-3.3.15-6.mlnx1.5.5r2.el5.x86_64.rpm
kernel-ib-1.5.5.092-2.6.39_300.29.1.el5uek.x86_64.rpm
infiniband-diags-1.5.13.MLNX_20120708-4.mlnx1.5.5r2.el5.x86_64.rpm
ovsvf-config-1.0-6.noarch.rpm
```

3. Create a python script called **vnfs.py** to view and marry PCI addresses to interfaces.

```
#!/usr/bin/python
# Copyright (C) 2012 Steve Jordahl
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU Lesser General Public License as
   published
# by the Free Software Foundation; version 2.1 only.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU Lesser General Public License for more details.
#
# vfns: list SR-IOV virtual functions

import os

info = {}

def catFile(filename):
        readfile = open(filename)
        return readfile.read().strip()

for dev in os.listdir('/sys/class/net'):
        if dev.startswith('eth'):
                info[dev] = {}
               info[dev]['address'] = catFile('/sys/class/net/' + dev
   + '/address')

for dev in info.keys():
        devLink = os.readlink('/sys/class/net/' + dev + '/device')
        info[dev]['pci address'] = devLink[-7:]
        os.chdir('/sys/class/net/' + dev)
        for devInfo in os.listdir(devLink):
if devInfo.startswith('virtfn'):
                        info[dev][devInfo] =
   os.readlink(os.path.join(devLink, devInfo))[-7:]

for dev in sorted(info.keys()):
        print dev
        for detail in sorted(info[dev].keys()):
                print "     " + detail + ":  " + info[dev][detail]
```

4. Create **/etc/pciback/pciback.sh**.

```
#!/bin/sh
if [ $# -eq 0 ] ; then
echo "Require a PCI device as parameter"
exit 1
fi
for pcidev in $@ ; do
if [ -h /sys/bus/pci/devices/"$pcidev"/driver ] ; then
echo "Unbinding $pcidev from" $(basename $(readlink /sys/bus/pci/
   devices/"$pcidev"/driver))
echo -n "$pcidev" > /sys/bus/pci/devices/"$pcidev"/driver/unbind
fi
```

```
echo "Binding $pcidev to pciback"
echo -n "$pcidev" > /sys/bus/pci/drivers/pciback/new_slot
echo -n "$pcidev" > /sys/bus/pci/drivers/pciback/bind
done
```

5. Use an IOMMU to allow both the VM and physical devices access to memory. The IOMMU allows the OVM to limit what memory a device is allowed and gives the device the same virtualized memory layout that the guest sees.

```
Edit /boot/grub/grub.conf to enable iommu and comment out the existing
   kernel entry ( see example )

# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
   file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sdb2
#          initrd /initrd-[generic-]version.img
#boot=/dev/sdb
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Oracle VM Server-ovs (xen-4.3.0 3.8.13-26.4.2.el6uek.x86_64)
root (hd0,0)
        #kernel /xen.gz console=com1,vga com1=57600,8n1
   dom0_mem=max:1776M allowsuperpage dom0_vcpus_pin dom0_max_vcpus=20
        kernel /xen.gz console=com1,vga com1=57600,8n1
   dom0_mem=max:1776M allowsuperpage
   iommu=passthrough,no-qinval,no-intremap
        module /vmlinuz-3.8.13-26.4.2.el6uek.x86_64 ro
   root=UUID=e2b44279-55a5-48b9-b910-82446b7b8c65 rd_NO_LUKS
   rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16
   KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
        module /initramfs-3.8.13-26.4.2.el6uek.x86_64.img
```

6. Reboot the OVM Server.

7. Run the vnfs script to view addresses and VFs statistics.

```
[root@meads ~]# ./vnfs.py
eth0
     address:  a0:36:9f:2c:39:74
     pci address:  30:00.0
eth1
     address:  a0:36:9f:2c:39:75
     pci address:  30:00.1
eth10
     address:  00:21:28:a1:e2:41
     pci address:  88:00.1
eth11
     address:  00:21:28:a1:e2:42
     pci address:  98:00.0
eth12
     address:  00:21:28:a1:e2:43
     pci address:  98:00.1
eth2
     address:  a0:36:9f:2c:39:76
     pci address:  30:00.2
eth3
     address:  a0:36:9f:2c:39:77
     pci address:  30:00.3
eth4
     address:  a0:36:9f:2d:0b:a8
     pci address:  a0:00.0
eth5
     address:  a0:36:9f:2d:0b:a9
     pci address:  a0:00.1
eth6
     address:  a0:36:9f:2d:0b:aa
pci address:  a0:00.2
eth7
     address:  a0:36:9f:2d:0b:ab
     pci address:  a0:00.3
eth8
     address:  00:21:28:a1:e2:46
     pci address:  5f:00.0
eth9
     address:  00:21:28:a1:e2:40
     pci address:  88:00.0
```

8. Run the module.

```
[root@meads ~]# modprobe xen-pciback
```

9. Assign devices to pciback in the format:

```
Domain 0:Bus:#:Device#:Function #).
```

Note: In the following example the 4 interfaces are VFs on ethernets 9-12.

```
[root@meads ~]# /etc/pciback/pciback.sh 0000:88:00.0
Unbinding 0000:88:00.0 from ixgbe
Binding 0000:88:00.0 to pciback

[root@meads ~]# /etc/pciback/pciback.sh 0000:88:00.1
Unbinding 0000:88:00.1 from ixgbe
Binding 0000:88:00.1 to pciback

[root@meads ~]# /etc/pciback/pciback.sh 0000:98:00.0
Unbinding 0000:98:00.0 from ixgbe
Binding 0000:98:00.0 to pciback
```

```
[root@meads ~]# /etc/pciback/pciback.sh 0000:98:00.1
Unbinding 0000:98:00.1 from ixgbe
Binding 0000:98:00.1 to pciback
```

10. View the list of VMs.

```
[root@meads ~]# xm list
Name                                      ID   Mem VCPUs      State
   Time(s)
0004fb0000060000f9b493a2c24f9549             7  8067    16     -b----
   80716.4
Domain-0                                    0  1775    20     r-----
   30379.2
```

11. View the list of assignable devices.

```
[root@meads ~]# xm pci-list-assignable-devices
0000:88:00.0
0000:88:00.1
0000:98:00.0
0000:98:00.1
```

12. Assign these devices to the VM.

Note: In the following example the VM ID is 7.

```
[root@meads ~]# xm pci-attach 7 0000:88:00.0
[root@meads ~]# xm pci-attach 7 0000:88:00.1
[root@meads ~]# xm pci-attach 7 0000:98:00.0
[root@meads ~]# xm pci-attach 7 0000:98:00.1
```

13. View the list of devices for this VM.

```
[root@Meads ~]# xm pci-list 7
Vdev Device
04.0 0000:88:00.0
05.0 0000:88:00.1
06.0 0000:98:00.0
07.0 0000:98:00.1
```

Now ethernets 9-12 are assigned to VM ID 7 and are not available to host any other VMs. They also do not show up when you run the **ifconfig** command.

14. Access and log into the OS-E CLI and execute the following.

```
NNOS-E>echo “1” > /sys/bus//pci/rescan
NNOS-E>run ./install_build_mactab.sh
NNOS-E>restart warm
```

After the restart has completed these interfaces are available on the OS-E.

Installing the OS-E On a VMware ESXi

The OS-E is certified to run on the VMware ESXi 5.5.

Oracle recommends the following configuration.

- vCPUs: 16 (16 sockets, 1 core per socket)
- RAM: 8GB
- Disk: 50G

To install the OS-E on a VMware ESXi:

1. Copy the OS-E's ISO file to the Datastore.
2. Click **Inventory**.
3. Create a new VM by clicking the ESXi server on the left.
4. Select **File > New > Virtual Machine** from the menu.
    - **Configuration**: Select **typical** to accept the default number of CPUs and amount of memory (1 CPU and 1GB). Select **custom** to change the default values. Click **Next**.
    - **Name and Location**: Enter a name for the VM. Click **Next**.
    - **Storage**: Select the Datastore. Click **Next**.
    - **Virtual Machine Version**: *For custom configuration only.* Select **Virtual Machine Version: 8**. Click **Next**.
    - **Guest Operating System**: Select **Linux** for **OS** and **Linux Oracle Linux 4/ 5/6 (64-bit)** for **Version**. Click **Next**.
    - **CPUs**: *For custom configuration only.* Select the number of sockets and number of cores/sockets. Click **Next**.
    - **Memory**: *For custom configuration only.* Select the memory size. Note the minimum, maximum, and recommended sizes for the guest OS you are using. Click **Next**.
    - **Network**: Select **3. Data Network**. Click **Next**.
    - **SCSI Controller**: *For custom configuration only.* Select **LSI Logic Parallel** (default). Click **Next**.

- **Select a Disk**: *For custom configuration only.* Select **Create a new virtual disk**. Click **Next**.
- **Create a Disk**: Specify the GB for disk capacity and choose **Thick Provision Lazy Zeroed** and **Store with the virtual machine**. Click **Next**.
- **Advanced Options**: *For custom configuration only*. Check the checkbox for **SCSI (0:0)**. Ensure the **Independent** checkbox remains unchecked. Click **Next**.
- **Ready to Complete**: Click **Finish**.

5. Right-click on the VM and select **Edit Settings...**.
   - Select **CD/DVD Drive 1**.
   - **Device Status**: Select **Connect at power on**.
   - **Device Type**: Select **Datastore ISO File** and choose **install_<*release_version*>_<*build_number*>.iso on Datastore1**.
   - Click **OK**.
6. Power on the VM by clicking the green play button.
7. Right-click the VM and select **Open Console**.

The OS-E is now ready to be set up and configured.

Configuring ESXi Passthrough

On the ESXi, you can directly connect a VM to a physical port via the SR-IOV specification. SR-IOV treats a single physical device as multiple separate Virtual Functions (VF)s. To deploy SR-IOV, you must enable VFs at the host level.

To configure SR-IOV on the ESXi you must have a NIC with an intel 82599 chipset or newer and a BIOS, both supporting SR-IOV.

The configuration for SR-IOV on the ESXi consists of two parts: first you must configure the OS-E’s VM server, then you must assign individual VFs to specific VMs.

To configure the OS-E’s VM server for SR-IOV:

1. Enable SR-IOV in the BIOS.

2. Ensure you have the latest drivers for your intel NIC (ixgbe) and ESXi version. See https://my.vmware.com/web/vmware/info/slug/datacenter_cloud_infrastructure/vmware_vsphere_with_operations_management/5_5#drivers_tools for more information on ESXi 5.5 drivers.

3. Install the appropriate drivers and reboot the host.

4. Log into the ESXi CLI shell and enter the following command to view a list of all NICs on the server and identify which NICs to use for SR-IOV.

```
# lspci | grep -i ‘ethernet\|network’
```

5. Specify the number of VFs you are assigning to each port by executing the following command:

```
# esxcfg-module ixgbe -s max_vfs=<P1=n><P2=n><P3=n><P4=n>
```

where <*Px=n*> stands for the configured ports and their assigned VF values, less than or equal to 63. Assigning a value of 0 makes that port unavailable for SR-IOV.

> **Note:** The SR-IOV specification allows for you to partition the Physical Function (PF) into a particular number of VFs you can then attach to VMs. The maximum number of VFs you can create on a PF depends on the hardware you are using. Typically, for 10GbE chipsets equal to or newer than 82599, that number is 63.

6. Verify that you entered the correct values by entering the following command:

```
# esxcfg-module ixgbe -g ixgbe
```

7. Reboot the server.

8. View the list of configured VFs by either reentering the following command:

```
#lspci | grep -i ‘ethernet\|network’
```

or accessing, via the vSphere GUI, **Host** > **Configuration** > **Advanced Settings**.

To configure a specific OS-E VM for SR-IOV:

> **Note:** To attach a VF to a VM, the VM version must be greater than or equal to 10.

1. Power off the VM.
2. Select **Settings** > **Hardware** > **Add**.
3. Select **PCI device** and select the VF you are adding to the VM.
4. Repeat this procedure for each VF you are adding to the VM.

Note: If you are prompted to “reserve” resources, you may have to click that button for the VM to power on.

Once a VF is attached to a particular VM, you cannot attach it to any other VM.

Installing the OS-E As a XEN Virtual Machine

The OS-E is certified to run on XEN 3.4.3.

Oracle recommends the following configuration.

- vCPUs: 16 (16 sockets, 1 core per socket)
- RAM: 8GB
- Disk: 50G

Note: Oracle recommends using LVM partitions as disks.

1. Create a partition and download the XEN image from buildview into that partition. The following example creates a 50G partition.

```
# lvcreate --size=50G --name=asc ol
# gunzip -c SEN.img.gz | dd of=/dev/mapper/ol-asc bs=512
# fdisk -l /dev/mapper/ol-asc

Disk /dev/mapper/ol-asc: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

                      Device Boot      Start         End      Blocks
   Id  System
/dev/mapper/ol-ascp1            1          63      506015+  82  Linux
   swap / Solaris
/dev/mapper/ol-ascp2         1768        3263    12016620   83  Linux
/dev/mapper/ol-ascp3           64         915     6843690   83  Linux
/dev/mapper/ol-ascp4          916        1767     6843690   83  Linux
```

2. Create a config file for the VM at /etc/xen/asc.cfg. The following is an example config file.

   Note: The following is an example. Ensure you customize your config file, including changing the MAC addresses, to fit your environment.

```
#  -*- mode: python; -*-
#=====================================================================
# Python configuration setup for 'xm create'.
This script sets the parameters used when a domain is created using xm
   create. Use a separate script for each domain you create or set the
   parameters for the domain on the XM command line.
# you can set the parameters for the domain on the xm command line.
#=====================================================================

#---------------------------------------------------------------------
# PV GRUB image file.
kernel = "/usr/lib/xen/boot/hvmloader"
builder = 'hvm'
device_model = '/usr/lib64/xen/bin/qemu-dm'

# Sets path to menu.lst
extra = "(hd0,1)/grub/menu.lst"
# can be a TFTP-served path (DHCP will automatically be run)
# extra = "(nd)/netboot/menu.lst"
# can be configured automatically by GRUB's DHCP option 150 (see grub
   manual)
# extra = ""

# Initial memory allocation (in megabytes) for the new domain.
#
# WARNING: Creating a domain with insufficient memory may cause out of
#         memory errors. The domain needs enough memory to boot kernel
#          and modules. Allocating less than 32MBs is not recommended.
memory = 8192

# A name for your domain. All domains must have different names.
name = "asc"

# 128-bit UUID for the domain.  The default behavior is to generate a
   new UUID
# on each call to 'xm create'.
#uuid = "06ed00fe-1162-4fc4-b5d8-11993ee4a8b9"

# List of which CPUS this domain is allowed to use, default Xen picks
#cpus = ""         # leave to Xen to pick
#cpus = "0"        # all vcpus run on CPU0
#cpus = "0-3,5,^1" # all vcpus run on cpus 0,2,3,5
#cpus = ["2", "3"] # VCPU0 runs on CPU2, VCPU1 runs on CPU3

# Number of Virtual CPUS to use, default is 1
vcpus = 4
cpus = "4-31" # all vcpus run on cpus >3

#---------------------------------------------------------------------
# Define network interfaces.

# By default, no network interfaces are configured.  You may have one
   created
```

```
# with sensible defaults using an empty vif clause:
#
# vif = [ '' ]
#
# or optionally override backend, bridge, ip, mac, script, type, or
   vifname:
#
# vif = [ 'mac=00:16:3e:00:00:11, bridge=xenbr0' ]
#
# or more than one interface may be configured:
#
# vif = [ '', 'bridge=xenbr1' ]

vif = [ 'mac=00:16:3E:62:F7:05, bridge=virbr0',
   'mac=00:16:3E:72:C9:95, bridge=messaging', 'mac=00:16:3E:06:57:B6,
   bridge=data' ]

#---------------------------------------------------------------------
# Define the disk devices you want the domain to have access to, and
# what you want them accessible as.
# Each disk entry is of the form phy:UNAME,DEV,MODE
# where UNAME is the device, DEV is the device name the domain will
   see,
# and MODE is r for read-only, w for read-write.

disk = [ 'phy:/dev/mapper/ol-asc,hda,w' ]

#---------------------------------------------------------------------
# Define frame buffer device.
#
# By default, no frame buffer device is configured.
#
# To create one using the SDL backend and sensible defaults:
#
# vfb = [ 'sdl=1' ]
#
# This uses environment variables XAUTHORITY and DISPLAY.  You
# can override that:
#
# vfb = [ 'sdl=1,xauthority=/home/bozo/.Xauthority,display=:1' ]
#
# To create one using the VNC backend and sensible defaults:
#
# vfb = [ 'vnc=1' ]
#
# The backend listens on 127.0.0.1 port 5900+N by default, where N is
# the domain ID.  You can override both address and N:
#
# vfb = [ 'vnc=1,vnclisten=127.0.0.1,vncdisplay=1' ]
#
# Or you can bind the first unused port above 5900:
```

```
#
# vfb = [ 'vnc=1,vnclisten=0.0.0.0,vncunused=1' ]
#
# You can override the password:
#
# vfb = [ 'vnc=1,vncpasswd=MYPASSWD' ]
#
# Empty password disables authentication.  Defaults to the vncpasswd
# configured in xend-config.sxp.

#----------------------------------------------------------------------
# Define to which TPM instance the user domain should communicate.
# The vtpm entry is of the form 'instance=INSTANCE,backend=DOM'
# where INSTANCE indicates the instance number of the TPM the VM
# should be talking to and DOM provides the domain where the backend
# is located.
# Note that no two virtual machines should try to connect to the same
# TPM instance. The handling of all TPM instances does require
# some management effort in so far that VM configration files (and thus
# a VM) should be associated with a TPM instance throughout the
   lifetime
# of the VM / VM configuration file. The instance number must be
# greater or equal to 1.
#vtpm = [ 'instance=1,backend=0' ]

#----------------------------------------------------------------------
# Configure the behaviour when a domain exits.  There are three
   'reasons'
# for a domain to stop: poweroff, reboot, and crash.  For each of these
   you
# may specify:
#
#   "destroy",        meaning that the domain is cleaned up as normal;
#   "restart",        meaning that a new domain is started in place of
   the old
#                     one;
#   "preserve",       meaning that no clean-up is done until the domain
   is
#                     manually destroyed (using xm destroy, for
   example); or
#   "rename-restart", meaning that the old domain is not cleaned up,
   but is
#                     renamed and a new domain started in its place.
#
# In the event a domain stops due to a crash, you have the additional
   options:
#
#   "coredump-destroy", meaning dump the crashed domain's core and then
   destroy;
#   "coredump-restart', meaning dump the crashed domain's core and the
   restart.
```

```
#
# The default is
#
#   on_poweroff = 'destroy'
#   on_reboot   = 'restart'
#   on_crash    = 'restart'
#
# For backwards compatibility we also support the deprecated option
   restart
#
# restart = 'onreboot' means on_poweroff = 'destroy'
#                            on_reboot   = 'restart'
#                            on_crash    = 'destroy'
#
# restart = 'always'   means on_poweroff = 'restart'
#                            on_reboot   = 'restart'
#                            on_crash    = 'restart'
#
# restart = 'never'    means on_poweroff = 'destroy'
#                            on_reboot   = 'destroy'
#                            on_crash    = 'destroy'

#on_poweroff = 'destroy'
#on_reboot   = 'restart'
#on_crash    = 'restart'

#---------------------------------------------------------------------
#   Configure PVSCSI devices:
#
#vscsi=[ 'PDEV, VDEV' ]
#
#   PDEV   gives physical SCSI device to be attached to specified guest
#          domain by one of the following identifier format.
#          - XX:XX:XX:XX (4-tuples with decimal notation which shows
#                          "host:channel:target:lun")
#          - /dev/sdxx or sdx
#          - /dev/stxx or stx
#          - /dev/sgxx or sgx
#          - result of 'scsi_id -gu -s'.
#            ex. # scsi_id -gu -s /block/sdb
#                  36000b5d0006a0000006a0257004c0000
#
#   VDEV   gives virtual SCSI device by 4-tuples (XX:XX:XX:XX) as
#          which the specified guest domain recognize.
#

#vscsi = [ '/dev/sdx, 0:0:0:0' ]

#=====================================================================

# Guest VGA console configuration, either SDL or VNC
```

```
#sdl = 1
vnc = 1
vncpasswd=""
vncdisplay=10
vnclisten="0.0.0.0"
```

3. Start the VM.

```
# cd /etc/xen
# xl create asc.cfg
```

The OS-E is now ready to be set up and configured.

Installing the OS-E On KVM

The OS-E is certified to run on KVM on OL7.

Oracle recommends the following configuration.

- vCPUs: 8
- RAM: 8GB
- Disk: 50G

  Note: Oracle recommends using LVM partitions as disks.

1. Install the KVM packages.

```
# yum install kvm libyirt
# yum install python-virtinst virt-top virt-manager virt-v2v
   virt-viewer
```

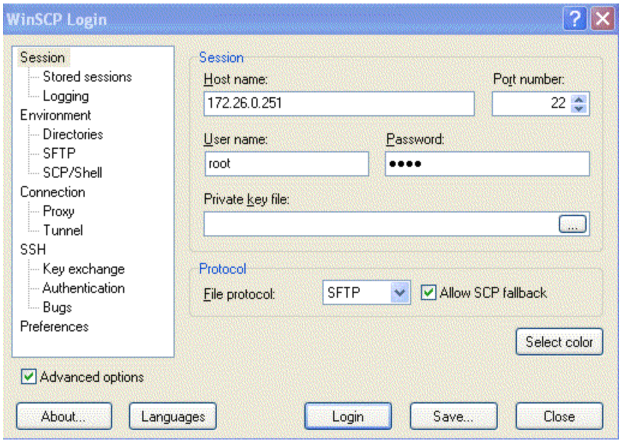
2. Use the virt-manager command to create your networks.
3. Install the OS-E guest by either using the following command in the CLI or via the virt-manager (right-click localhost (QEMU) and click New).

```
virt-install -n asc -r 8192 --os-type=linux --disk /dev/mapper/
   ol-asc,device=disk,bus=virtio,size=50,sparse=false,format=raw -w
   network=management,model=virtio -w network=messaging,model=virtio
   -w network=data,model=virtio -c /mnt/install/<build_version>.iso
   --vcpus=8
```

Using WinSCP to Transfer the License

If you do not have access to the OS-E Management System, Oracle recommends that you use WinSCP to transfer the license file to the OS-E device. WinSCP is an open source free SFTP client and FTP client for Windows and is available as a free download from the following URL:

http://winscp.net/eng/index.php



WinSCP Login

Session

Host name: 172.26.0.251

Port number: 22

User name: root

Password: ••••

Private key file:

Protocol

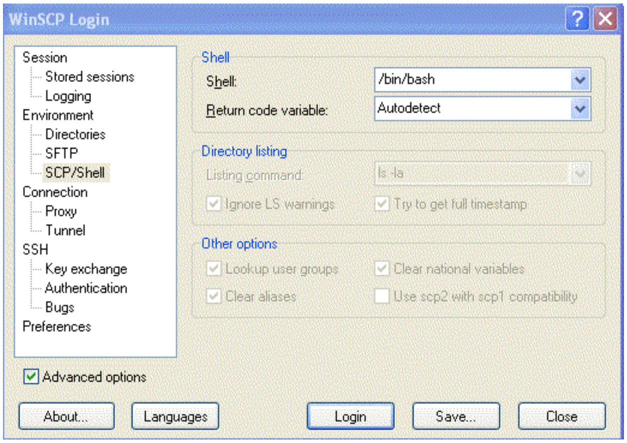
File protocol: SFTP

☑ Allow SCP fallback

☑ Advanced options

Perform the following steps:

1. At the **Hostname** field, enter the IP address that you assigned to the management interface at the OS-E system. Port **22** is the default port number for SSH sessions.
2. At the **Username** and **Password** fields, type *root* for the username and *sips* for the password.
3. At the Environment menu, select **SCP/Shell** and select **/bin/bash** from the pull-down menu. Leave all other fields at their default settings.



Shell: /bin/bash

Return code variable: Autodetect

Listing command: ls -la

☑ Ignore LS warnings ☑ Try to get full timestamp

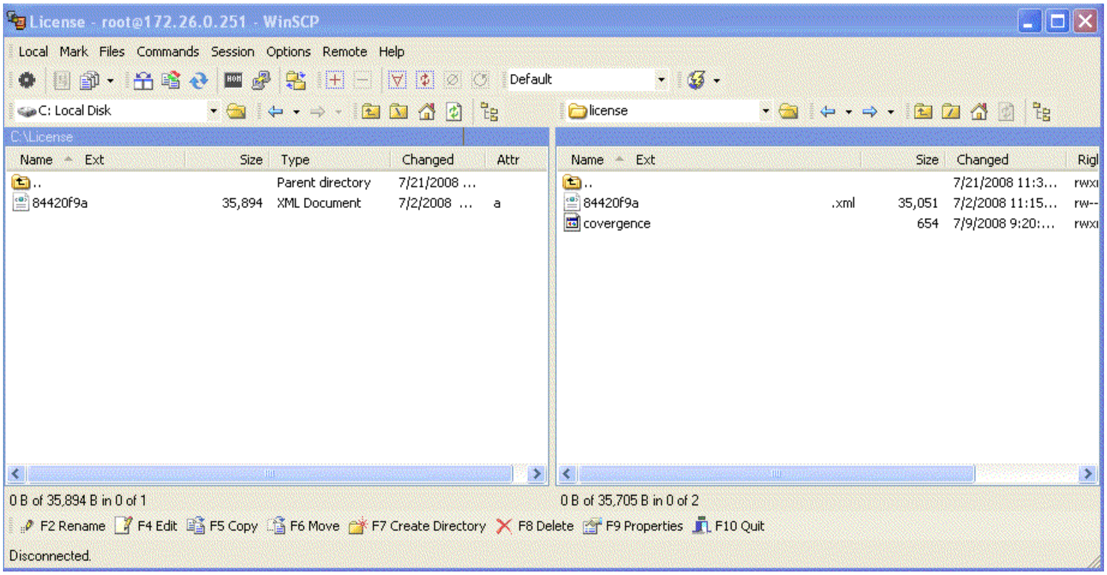
☑ Lookup user groups ☑ Clear national variables

☑ Clear aliases □ Use scp2 with scp1 compatibility

☑ Advanced options

4. Click **Login**. A series of progress message will appear as the connection is established.

5. From the left pane, browse and locate the license file, then drag the license to the *cxc/license* directory. In this example, the file is copied from the **c:\license** directory to the **cxc/license** directory OS-E.



C:\License

Name	Ext	Size	Type	Changed	Attr
..			Parent directory	7/21/2008 ...	
84420f9a		35,894	XML Document	7/2/2008 ...	a

Name	Ext	Size	Changed	Rig
..			7/21/2008 11:3...	rwx
84420f9a	.xml	35,051	7/2/2008 11:15...	rw-
covergence		654	7/9/2008 9:20:...	rwx

0 B of 35,894 B in 0 of 1

0 B of 35,705 B in 0 of 2

Disconnected.

6. Once the license file is present in the *cxc/license* folder, you will need to do one of the follow tasks for the OS-E license to take effect:

- Perform a physical restart of the OS-E system, or
- From a CLI session to the device, execute the **license apply** action, as follows:

```
NNOS-E> license apply /cxc/license/
   84420g9a-da13-3007-8853-z00a7a4d771d.xml
Success!

NNOS-E> show licenses

name: LICENSE for Company.com
description: LICENSE for Company.com
        key: 84420g9a-da13-3007-8853-z00a7a4d771d
    expires:
       file: 84420g9a-da13-3007-8853-z00a7a4d771d.xml
```

Configuring the VM

Once the VM is installed and running, you now must configure it to match the SIP application you are supporting. Since the VM does not have a pre-installed base configuration, Oracle provides the **config setup** configuration setup script that you can use to create a base configuration.

Using Config Setup

For Oracle users who are familiar with OS-E, the *config setup* script enables the configuration on the VM to make it reachable via ICMP (ping), SSH, and HTTPS for further configuration. The script presents a set of questions to help you with the initial system configuration. The information in the script includes the following:

- Local hostname
- IP interface names and addresses
- SSH and Web access
- Default route and any additional static routes per interface for remote management
- User-defined OS-E

Every Oracle OS-E system has a minimum of two Ethernet interfaces. Any Ethernet interface on the system can be used for management traffic, however, Oracle recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other OS-E systems. Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI Session

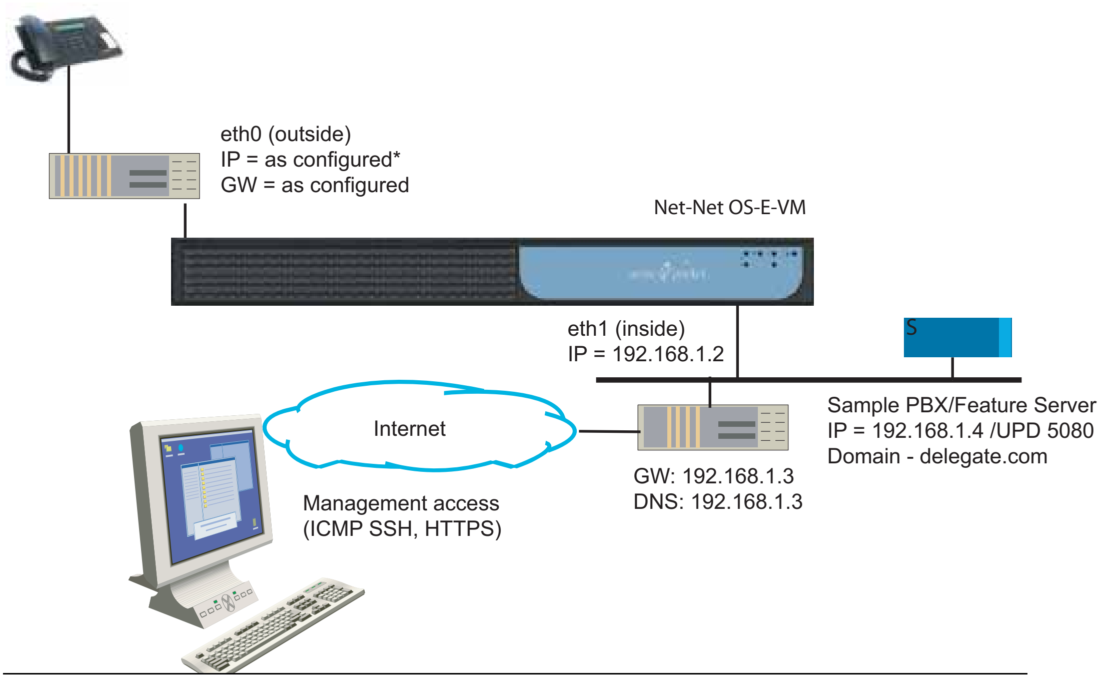
```
NNOS-E-VM> config setup
set box\hostname: <name>
config box\interface: eth1
set box\interface eth1\ip a\ip-address: <ipAddress/mask>
config box\interface eth1\ip a\ssh (y or n)? n
config box\interface eth1\ip a\web (y or n)? y
config box\interface eth1\ip a\routing\route: <routeName>
set box\interface eth1\ip a\routing\route localGateway\gateway:
<ipAddress>
set box\cli\prompt: <newPrompt>
Do you want to commit this setup script (y or n) y
Do you want to update the startup configuration (y or n)? y
```

Sample VM Configuration

The following image illustrates a sample VM network and a base configuration designed to support a standard SBC application where the VM functions with SIP endpoints and a PBX or feature server. The high-level details of this configuration are provided below and additional details are embedded in the configuration file itself at the end of this section.

- Two interfaces: one "outside" and one "inside."
- Management ports for ICMP, SSH, and HTTPS open on both interfaces.
- The IP address associated with a DNS resolver.
- SIP UDP, TCP, and TLS ports open on both interfaces.
- NAT traversal & media anchoring enabled.
- A sample gateway configuration for an attached PBX or feature server.
- A sample registration- and dial-plan for delegation of SIP traffic to the attached PBX or feature server.

- A local registration plan to support registrations and calls locally through the VM (for cases where there is no attached PBX or feature server).



Note: Oracle recognizes that the items in the base configuration will not be 100% applicable to all OS-E-VM deployments. However, by including these items in this sample configuration, new VM users can observe the configuration structure and hierarchy. Any necessary changes to this base configuration can be made using the procedures described in the Oracle manual set. See, “Using Oracle Documentation,” for more information.

Below is a copy of the base configuration. Note that any changes to the configuration should be made using the OS-E Management System (see, “Enabling the OS-E Management System”).

Note: Oracle does not recommend editing the configuration file below directly, and then importing it into the VM. While the VM does support this function, it is possible to introduce syntax errors into the configuration file using this method. Modifying the configuration with the CLI or Net-Net Management System prevents this possibility.

```
#  Copyright (c) 2004-2009 Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 15:00:28 Mon 2009-05-05
```

This section is unique to every VM; you do not need to edit this.

```
config cluster
 set name acmepacket-nnos-e-vm-demo
 config box 1
  set hostname acmepacket-nnos-e-vm-demo
  set name acmepacket-nnos-e-vm-demo
  set identifier 00:0c:29:c9:7a:e2
```

The IP address is configured as part of the configuration script execution.

```
config interface eth0
   config ip outside
    set ip-address static 172.30.3.128/22
    config ssh
    return
    config web
    return
    config sip
     set nat-translation enabled
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" any 0
     set certificate vsp\tls\certificate sample
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route default
      set gateway 172.30.0.1
    return
    return
   return
  return
```

The following section of the configuration provides a DNS resolver entry and is configured as part of the configuration script execution. This is not required for operation but can be helpful if you want to use FQDNs in the config instead of IPs)

```
config dns
  config resolver
   set server 192.168.1.3 UDP 53 100 ALL
  return
```

```
 return
return
```

The following IP is disabled; you can enable it once you change the IP to match your local network conditions.

```
config interface eth1
   config ip inside
    set admin disabled
    set ip-address static 192.168.1.2/24
    config ssh
    return
    config web
    return
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" any 0
     set certificate vsp\tls\certificate sample
    return
    config icmp
    return
    config media-ports
    return
```

This routing config is provided as an example; edit it as needed. Change to match your preferred NTP server.

```
config routing
     config route inside-ntwk
      set destination network 192.168.0.0/16
      set gateway 192.168.1.1
   return
    return
   return
  return
  config ntp-client
   set server pool.ntp.org
return
  config cli
   set prompt nnos-e-vm>
  return
 return
return
```

The following section of the configuration contains all of the event log filters and targets.

```
config services
 config event-log
  config file eventlog
```

```
   set filter all error
  return
  config file access-log
   set filter access info
  return
  config file kernelsys
   set filter krnlsys debug
  return
  config file db
   set filter db debug
  return
  config file system
   set filter general info
   set filter system info
  return
  config file access
   set filter access info
  return
  config file dos
   set filter dosSip alert
  return
  config local-database
   set filter all error
  return
 return
return
```

The following section of the config provides some commonly used default system parameters; further information on these parameters is provided in the tech manuals.

```
config master-services
 config database
  set media enabled
 return
return

config vsp
 set admin enabled
 config default-session-config
  config media
   set anchor enabled
   config nat-traversal
    set symmetricRTP true
   return
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config log-alert
  return
 return
 config tls
  config certificate sample
  return
 return
```

The following section of the configuration provides a sample policy rule to reject calls from a user with a URI that starts with 1000. This sample is provided as a means of introducing a new user to the concept of policy rules)

```
config policies
  config session-policies
   set default-policy vsp\policies\session-policies\policy default
   config policy default
    config rule sample-rule
     set description "sample rule to reject calls"
     config condition-list
      set from-uri-condition user match 1000
     return
     config session-config
      config sip-directive
       set directive refuse 400 "Please Pay Your Bill"
      return
     return
    return
   return
  return
 return
```

The folllowing configuration provides a sample dial-plan that takes a call with a Req URI domain of delegate.com and forwards it to the sample SIP gateway.

```
 config dial-plan
  config route sample-delegate
   set description "delegate to defined server"
   set peer server "vsp\enterprise\servers\sip-gateway sample-gateway"
   set request-uri-match domain-exact delegate.com
  return
 return
```

The following configuration provides a sample registration plan that takes a registration attempt with a domain of *xyz.com* and registers the endpoint locally. This is useful for cases where you want to register an endpoint locally for call testing purposes.

```
config registration-plan
  config route sample-accept-local
   set description "accept registers locally for this domain"
   set action accept
   set peer server "vsp\enterprise\servers\sip-gateway sample-gateway"
   set to-uri-match domain-exact xyz.com
  return
```

The following configuration provides a sample registration plan that takes a registration attempt with a domain of delegate.com and proxies the registration to the attached PBX or feature server.

```
config route sample-delegate
   set description "delegate to the defined server"
   set peer server "vsp\enterprise\servers\sip-gateway sample-gateway"
   set to-uri-match domain-exact delegate.com
  return
 return
```

The following configuration provides a sample SIP gateway that could be used for an attached PBX or feature server. You will need to edit the IP address to reflect the actual server IP or FQDN.

```
 config enterprise
  config servers
   config sip-gateway sample-gateway
    config server-pool
     config server sample-server
      set host 192.168.1.4
     return
    return
   return
  return
 return

config external-services
return
config preferences
 config cms-preferences
 return
return
```

The following configuration provides two different sample permission sets. These permission sets modified and/or can be used with user accounts that you create.

```
config access
 config permissions super-user
  set cli advanced
 return
 config permissions view-only
  set cli disabled
  set ftp disabled
  set config view
  set actions disabled
  set templates disabled
  set web-services disabled
  set debug disabled
 return
return

config features
return
```

Acme Packet recommends that the storage-device fail-threshold be set to 200 MB.

```
services
storage-device
  fail-threshold 200 MB
```

Enabling the OS-E Management System

Once you have configured an Ethernet interface, such as eth1, you can use your Internet Explorer Web browser to point to the configured IP address of this interface to launch the OS-E Management System. The OS-E Management System provides a windows and menu user interface to configuring the OS-E. See the *Net-Net OS-E – Using the NNOS-E Management Tools* for information on using the CMS.

Bridging to Additional Ethernet Ports

Follow the steps in this section if you need to configure VMware Player on a Window platform to use two bridged networks. By default, VMWare Player allows the following functionality:

- One bridged interface (to the first host network interface)
- One NAT interface
- One host-only interface

To create two bridged interfaces, you will need to

1. add an additional VMnet associated with a second interface, and
2. edit the VM configuration file to use the new VMnet.

Adding an Additional VMnet

To add an additional VMnet, perform the following steps:

1. Halt all VMs currently running on this x86-based PC or server.
2. Launch the **vmnetcfg.exe** application from the VMware Player installation directory (c:\Program Files\VMware\VMware Player\vmnetcfg.exe).
3. Select the **Host Virtual Network Mapping** tab.
4. Select a VMnet to use for the second network interface card (NIC), such as VMnet3.
5. From the drop-down men, select the NIC you wish to connect to this VMnet.

If you want to have more control over which VMnet0 which connects to the first NIC perform the following steps:

1. Select the **Automatic Bridging** tab.
2. In the **Automatic Bridging** box, de-select the **Automatically choose and available physical network adapter to bridge to VMnet0**.
3. Select the **Host Virtual Network Mapping** tab.
4. Select a VMnet to use for the first NIC, such as VMnet2.
5. From the drop-down menu, select the NIC you wish to connect to this VMnet.

Note: You can use VMnet0 to assign to a specific NIC. However, avoiding VMnet0 will indicate to a later user of the VMs configuration file that specific NICs were assigned to the VMs virtual interfaces, thus removing any questions about the automatic nature implied with VMnet0 on any particular system.

Editing the VM Configuration File

You will need to edit the VMware configuration file to include the second NIC with the VMware Player. Perform the following steps:

1. Halt all VMs currently running on this x86-based PC or server.
2. Using Windows Explorer, open the Oracle OS-E folder.

- Using a text editor such as Notepad, open the file **nnos-e-vm.vmx**.
- At the bottom of the file add the following lines, substituting the desired VMnets for the Ethernet interfaces:
  - — **ethernet0.connectionType = "custom"**

- — **ethernet0.vnet = "vmnet0"**
- — **ethernet1.connectionType = "custom"**
- — **ethernet1.vnet = "vmnet3"**

- Ensure that there are no other lines in the file specifying **ethernetX.connectionType = "XXXXX"**.

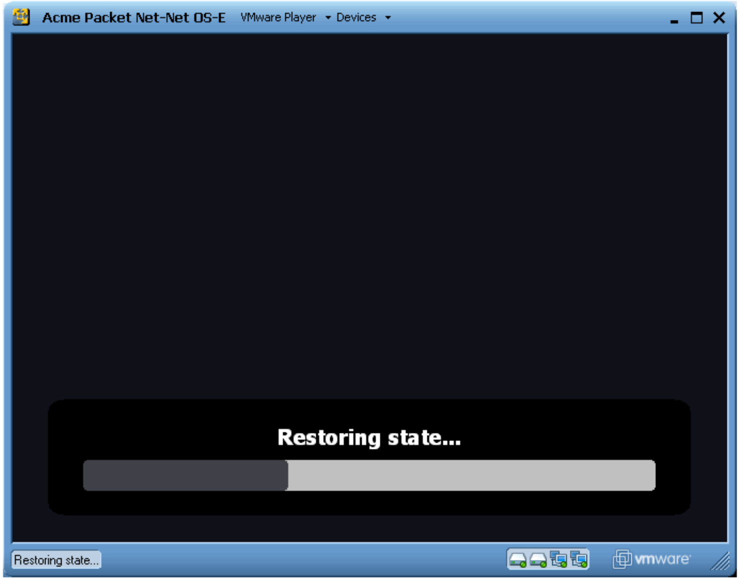
Net-Net OS-E-VM Troubleshooting

Oracle makes every effort to test the VM in a variety of customer environments. This section covers recently reported issues directly from OS-E-VM customers. If you discover an issue with the VM that we need to know about, contact Oracle Customer Support for assistance.

Installing the VM on Slow Systems

There may be cases where you are allowed to log in to the VM before the Oracle OS-E application starts up. This is usually caused by a slow system where you installed the VM, and all necessary software processes are requiring more time to complete their startup routines.

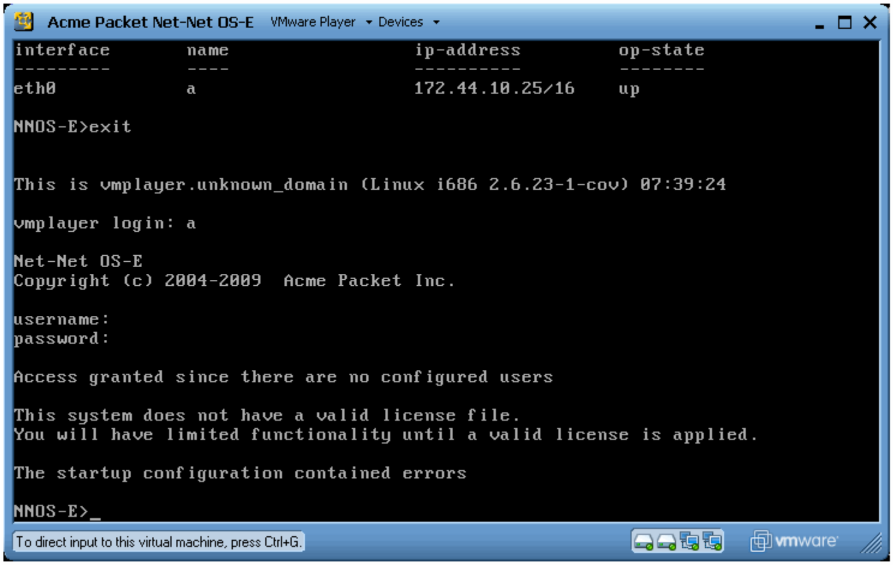
If you shut down the VM, and then start it again later, the VM will return you to the same screen and prompt that was displayed at the time of the shutdown. The VM startup would appear as shown in the following image.



Restoring state...

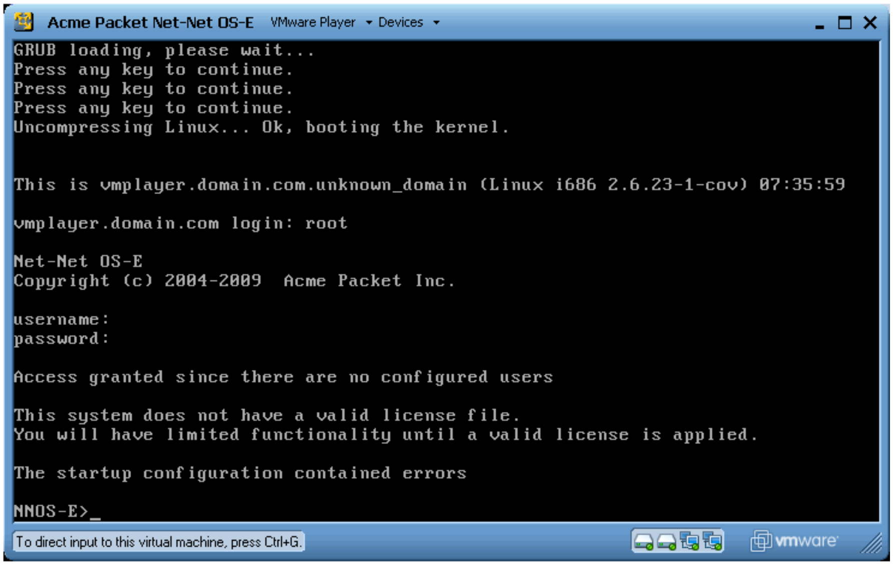
Restoring state...

When the VMWare system returns to the state where you previously logged out, and if you restart VMWare, you will see the login: prompt, such as the hostname *mikeo-cva* in the following image. If you did not previously configure a unique *username* and *password*, just press **ENTER** at the username and password prompts.



```
interface        name                    ip-address          op-state
---------        ----                    ----------          --------
eth0             a                       172.44.10.25/16     up

NNOS-E>exit


This is vmplayer.unknown_domain (Linux i686 2.6.23-1-cov) 07:39:24

vmplayer login: a

Net-Net OS-E
Copyright (c) 2004-2009  Acme Packet Inc.

username:
password:

Access granted since there are no configured users

This system does not have a valid license file.
You will have limited functionality until a valid license is applied.

The startup configuration contained errors

NNOS-E>_
```

If the Oracle OS-E-VM application has not yet started, your screen appears as shown in the following image. Exit and wait a few minutes for the application to complete all the essential startup processes. You can then log in by pressing ENTER/ ENTER at the username and password prompts, or you can enter the previously-configured username and password.



```
GRUB loading, please wait...
Press any key to continue.
Press any key to continue.
Press any key to continue.
Uncompressing Linux... Ok, booting the kernel.


This is vmplayer.domain.com.unknown_domain (Linux i686 2.6.23-1-cov) 07:35:59

vmplayer.domain.com login: root

Net-Net OS-E
Copyright (c) 2004-2009  Acme Packet Inc.

username:
password:

Access granted since there are no configured users

This system does not have a valid license file.
You will have limited functionality until a valid license is applied.

The startup configuration contained errors

NNOS-E>_
```

Other VM Limitations and Considerations

The following limitations and considerations apply:

- Configuring feature options that rely on critical timing are more problematic to VMs. This includes music-on-hold (MoH), announcements, periodic announcements, and transcoding.
- VMs running on AMD systems exhibit more timing issues than on Intel-based systems.
- The type of hardware over which you are running the VM can make a significant difference in VM performance. Improved performance is normal when running the VM over larger and faster running platforms.

Appendix A. Technical Specifications

NEBS/ETSI

- Bellcore GR-63, Physical Protection Requirements
- Bellcore GR-1089, Electromagnetic Compatibility and Electrical Safety Req.

ActionETSI 300 386, Telecommunication Network, Electromagnetic Compatibility

- ETSI 300 019, Environmental Conditions and Environmental Tests
- ETSI 753, Acoustic Noise

AC Power Cords

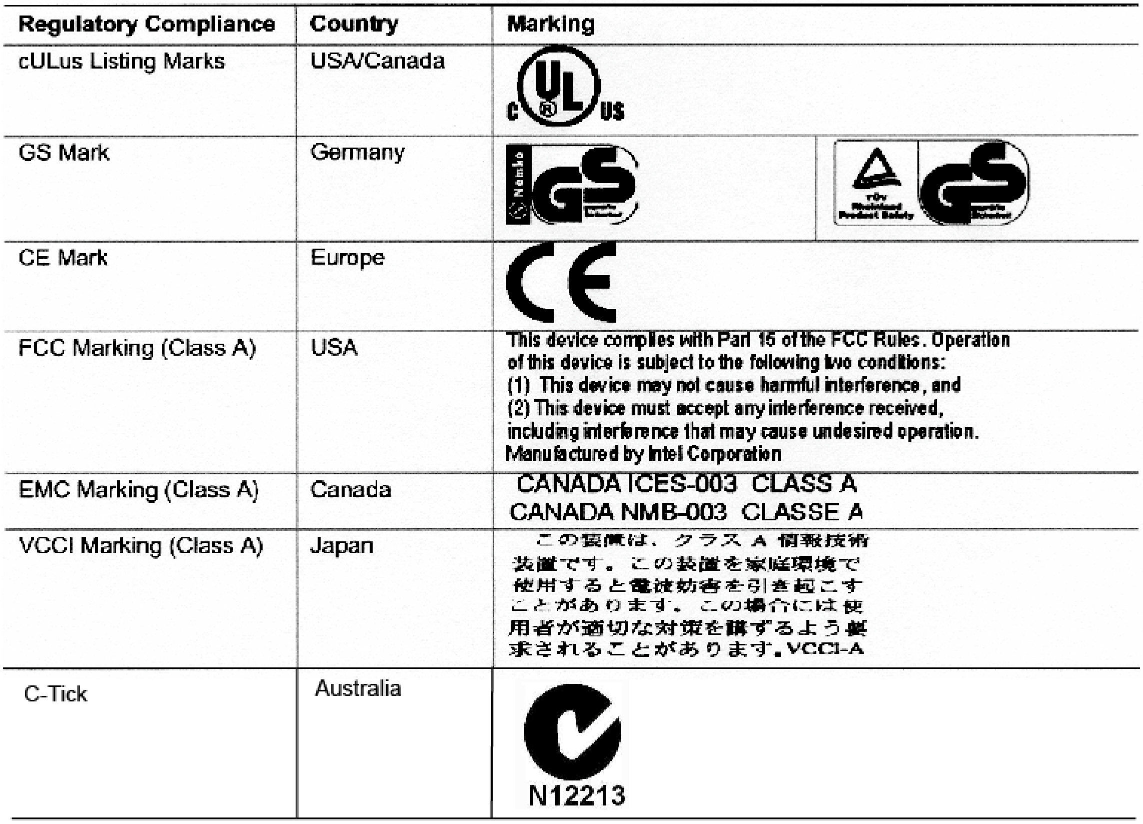
North America, Europe, United Kingdom, Japan, China, Korea, Australia

Safety and EMC Regulatory Compliance (Class A)

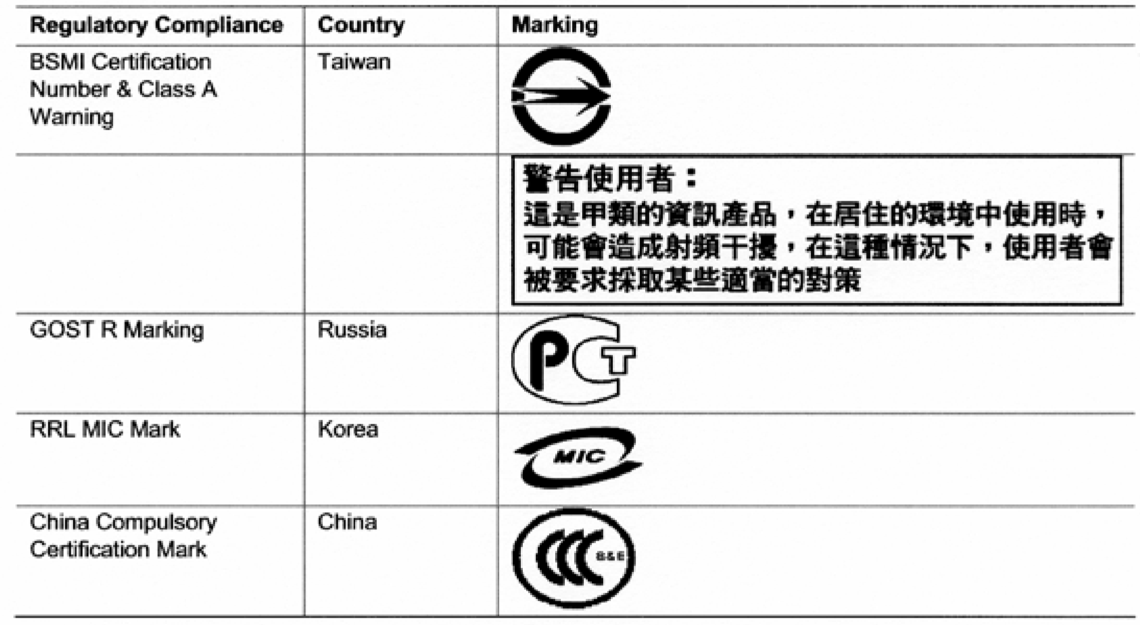
Country	Certification (Safety and/or EMC)	Regulatory Mark (Safety and/or EMC)
Argentina	IRAM	Not applicable
Australia/New Zealand	ACA, MED	C-Tick
Belarus	Bellis	Not applicable
Canada	UL / Industry Canada	cURus / ICES
China	CNCA	CCC
Europe	European Directives	CE
Germany	GS	GS
International	CB Repor / CISPR 22	Not applicable
Japan	VCCI	VCCI
Korea	RRL	MIC
Russia	GOST	GOST
Taiwan	BSMI RPC	BSMI
United States	UL / FCC	CULus / FCC

Product Regulatory Compliance Markings

This product is marked with the following Product Certification Markings:



Regulatory Compliance	Country	Marking
cULus Listing Marks	USA/Canada	C UL ® US
GS Mark	Germany	Nemko GS TÜV Rheinland Product Safety GS
CE Mark	Europe	CE
FCC Marking (Class A)	USA	This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. Manufactured by Intel Corporation
EMC Marking (Class A)	Canada	CANADA ICES-003 CLASS A CANADA NMB-003 CLASSE A
VCCI Marking (Class A)	Japan	この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。VCCI-A
C-Tick	Australia	N12213



Regulatory Compliance	Country	Marking
BSMI Certification Number & Class A Warning	Taiwan	
		警告使用者： 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策
GOST R Marking	Russia	
RRL MIC Mark	Korea	
China Compulsory Certification Mark	China	

Electromagnetic Compatibility Notices

FCC (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions related to the EMC performance of this product, contact:

Intel Corporation

5200 N.E. Elam Young Parkway

Hillsboro, OR 97124

1-800-628-8686

- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit other than the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the grantee of this device could void the user’s authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

Only peripherals (computer input/output devices, terminals, printers, etc.) that comply with FCC Class A or B limits may be attached to this computer product. Operation with noncompliantperipherals is likely to result in interference to radio and TV reception. All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals, that are not shielded and grounded may result in interference to radio and TV reception.

Industry Canada (ICES-003)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le Ministre Canadian des Communications.

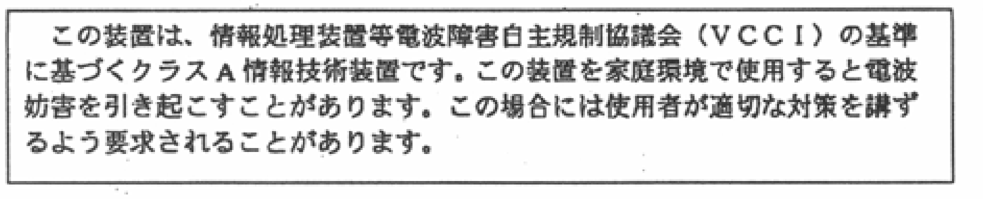
English translation of the notice above:

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.

Europe (CE Declaration of Conformity)

This product has been tested in accordance too, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

VCCI (Japan)

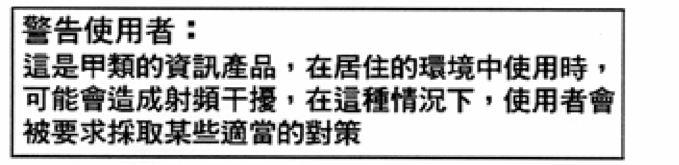


この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

English translation of the notice above:

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) from Information Technology Equipment. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

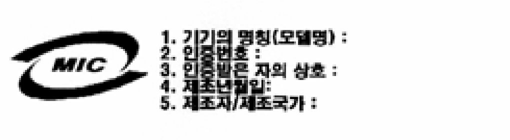
BSMI (Taiwan)



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

The BSMI Certification Marking and EMC warning is located on the outside rear area of the product.

Korean RRL Compliance



1. 기기의 명칭(모델명) :
2. 인증번호 :
3. 인증받은 자의 상호 :
4. 제조년월일:
5. 제조자/제조국가 :

English translation of the notice above:

1. Type of Equipment (Model Name): On License and Product

2. Certification No.: On RRL certificate. Obtain certificate from local Intel representative

3. Name of Certification Recipient: Intel Corporation

4. Date of Manufacturer: Refer to date code on product

5. Manufacturer/Nation: Intel Corporation/Refer to country of origin marked on product