Oracle® Communications Session Border Controller

User Guide

Release S-CX6.3.9

Formerly Net-Net Session Director

March 2014

ORACLE®

Table of Contents

About this Guide

Overview

This *Oracle® Communications Session Border Controller User Guide,* Release S-C[xz]6.3.9 GA is the general availability release of software version Release S-C[xz]6.3.9. This release differs from previous Oracle releases by providing platform flexibility through the availability of three distinct *editions*, with each edition targeted toward a specific network environment.

The *Server Edition*, targeted for distributed small to medium enterprises, runs on a certified server to support a maximum of 1000 concurrent SIP audio calls.

The *VM Edition*, also targeted for distributed small to medium enterprises, runs on a generic server within a virtualized environment to support a maximum of 250 concurrent SIP audio calls per Virtual Machine (VM). The VM Edition supports both VMware and Hyper-V virtualization software.

The *Oracle Hardware Edition*, targeted for medium to large enterprises, runs on Oracle purpose-built hardware, specifically the Acme Packet 3280 SBC and Acme Packet 4500 SBC, to support a maximum of 16,000 concurrent SIP audio calls.

This guide provides an overview of all three editions. It does not serve as a comprehensive guide to configuring common, cross-platform functionality. Refer to the Oracle Communications SBC C6.3 documentation for that level of detailed information.

Supported Platforms

This guide supports the Acme Packet 3800 and the Acme Packet 4500 C-series platforms, as well as the Enterprise Session Border Controller-Server Edition and Virtual Machine Edition. For more information about these platforms, see the *Oracle® Enterprise Session Border Controller Configuration Guide.*

Related Documentation

The following table lists related S-C[x]6.3.0 documents you can use as reference.

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3800 system.

Document Name	Document Description
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.

Revision History

This section contains the revision history for this document.

Date	Revision Number	Description
January 30, 2012	Revison 1.00	• New user guide to support the release of the new Oracle Enterprise Session Director Server Edition.
June 29, 2012	Revision 2.00	• Updated user guide to support Virtual Machines (VMs)
July 27, 2012	Revision 3.00	• Fixed some issues with missing graphics.
January 17, 2013	Revision 3.01	• Removed references to the collector for SIP Monitoring and Trace. • Updated the “About This Guide” section. • Added “Configuring Certificates” for the Web Server configuration. • Added a note indicating the Oracle Communications SBC supports the use of the MS Hyper-V Manager for importing and setting up the Hyper-v VM files (vhd). It does not support creating new VMs from the MS System Center Virtual Machine Manager (SC-VMM) application, but does allow you to manage the VM using SC-VMM once the VMs have been created using MS Hyper-V Manager. • Oracle Communications SBC does not support IPFIX for SIP Tracing and Monitoring so it was removed.
January 30, 2013	Revision 3.02	• Support for new 3rd party server platforms documented in Chapter 1.
February 8, 2013	Revision 3.03	• Added explanation of howSIP packets are processed for SIP Monitor and Trace in Chapter 5. • Fixed some issues with displayed graphics in Chapter 7.
March 4, 2013	Revision 3.04	• Removed Appendix D, Notices and 3rd party Licenses. This information now displays when initiating the “show features” ACLI command AND in the “About” link in the Web GUI.
July 19, 2013	Revision 3.05	• Corrected description of “session-recording-required” parameter in SIPREC chapter. • Added a graphic in Chapter 4 to describe how Palladion handles incoming and outgoing data. • Incorporated M1 and M2 release information into this document.
June 4, 2014	Revision 3.06	• Changed the value for simultaneous-recording-servers from “1 to 100” to “1 to 3” to conform to system behavior.

1 Platforms

Oracle Hardware Platforms Edition

Release S-C[xz]6.3.9 runs on Oracle purpose-built hardware, specifically the mid-capacity Acme Packet 3820 and high-capacity Acme Packet 4500 Session Border Controllers (SBC), and provides identical functionality (save for the number of concurrently supported SIP audio sessions) on both Oracle platforms.

Build Image

The Release S-C[xz]6.3.9 build image (*nnSCx639.tar*, where *x* specifies an Oracle platform) differs from most previous releases that were delivered in *.gz* format. The *.tar* format is used to package an embedded web server with the build image.

Bootloader Upgrade Procedure

Upgrade of an operational Acme Packet 3820 or Acme Packet 4500 to Release S-C[xz]6.3.9 requires the prior installation of a bootloader released on January 19, 2012.

This bootloader is available at the Oracle customer support portal at:

> *https://support.acmepacket.com/SD_images/NN4500-Bootloader-Upgrade-011912.zip*

This file includes two files *bootrom.sys* and *stage2.gz* that are moved to a standalone SBC, or to the primary and secondary SBCs in an HA pair. Additionally, the file includes an MS Word document that provides specific instructions for the installation of this bootloader, and a small text file illustrating output from the installation procedure.

Documentation Information

Users of the Release S-C[xz]6.3.9 should use the existing C6.3 Oracle documentation set to configure and manage most functions. They should use this guide to configure and manage new functions supported by Release S-C[xz]6.3.9.

- Session Initiation Protocol Recording (SIPREC) — refer to Chapter 3
- Communications Monitoring Probe — refer to Chapter 4
- SIP Monitoring and Tracing — refer to Chapter 5, Chapter 6, and Chapter 7
- Personal Profile Manager (PPM) - refer to Chapter 8
- Installation Wizard — refer to Chapter 9
- Dynamic Payloads (SIP/H.323 internetworking) — refer to Chapter 9
- Dynamic Payloads (TCS) — refer to Chapter 9
- Dynamic Payloads (OLA) — refer to Chapter 9

Server Edition

The Server Edition software (Release S-C[xz]6.3.9) is delivered on a 4GB USB drive (referred to in this document as a *USB stick*) that is pre-installed (embedded) within a certified third party server described in the Supported Servers section. The USB stick provides the unique serial number that serves as a license key. It also contains all programs and tools required for the installation of Oracle application software on the host server; the USB stick is required for installation, operation, and licensing.

The USB stick is used to boot the Server Edition software for the first time. The USB stick loads the bootloader from the hard drive, which then boots the customized kernel and the Server Edition software.

Build Image

The Release S-C[xz]6.3.9 build image (*nnSCz639.bz*, where *z* specifies a 3rd party platform) is compressed by the zlib software library.

System Requirements

The system requirements described in this section are specific to Release Cz6.3.9 Final.

Supported Servers

Oracle provides the following Oracle Communications Session Border Controller hardware servers:

- HP ProLiant DL120 G7 (2)
- HP ProLiant DL320e G8 (3)
- Dell PowerEdge R210 II (4)

Each of these servers and their parts are described below.

HP ProLiant DL120 G7

The certified server, the HP ProLiant DL120 G7, has two on-board management ports *wancom0* and *wancom1*, and a Network Interface Card (NIC) that hosts two signaling and media ports *s0p0* and *s1p0*. Optional NIC controllers provide for additional management and media ports.

The *wancom0* port can be used for HP Integrated Lights Out (iLo). Oracle recommends using iLo for hardware monitoring. Users should also refer to the HP documentation shipped with the server.

Server configuration is described in the following table.

Part Number	Item
647339-B21	HP Proliant DL 120 G7 Server
641912-L21	Quad-Core Intel Xeon Processor E-3-1220 (3.10GHz, 8MB, 80W)
500672-B21	HP 4GB (1x4GB) Dual Rack x8 PC3-10600 (DDR3-1333)
458928-B21	HP Embedded 4 Port SATA Controller HP 500GB 3G SATA 7.2K rpm SFF (2.5-inch) Midline 1yr Warranty Hard Drive
412648-B21	HP NC360T PCI Express Dual Port Gigabit Server Adapter - Low Profile
515739-B21	HP 400W Factory Integrated Power Supply
AF556A	HP 1.83m 10A C13-UL US Power Cord (or a suitable C13 power cord)

Part Number	Item
534616-B21	HP ProLiant Foundation Pack Single Release Factory Integrated Software Protected by HP Services, warranty includes 3 year Next Day Parts replacement, 0-Years Labor, 0-Years Onsite support. Limited Global warranty - Certain restrictions and exclusions apply.
Optional Components	
512485-B21	iLO Advanced License - 1 year
BD505A	iLO Advanced License - 3 year
Note: Because the customized Linux kernel provided by the USB stick supports Oracle Communications Session Border Controller, the certified server does not require an installed operating system.	

HP ProLiant DL320e G8

The certified server, the HP ProLiant DL320e G8, has two on-board management ports *wancom0* and *wancom1*, and a Network Interface Card (NIC) that hosts two signaling and media ports *s0p0* and *s1p0*. Optional NICs provide for additional management and media ports.

The *wancom0* port can be used for HP iLo. Oracle recommends using iLo for hardware monitoring. Users should also refer to the HP documentation shipped with the server.

Server configuration is described in the following table.

Part Number	Item
675596-B21	HP Proliant DL320e G8 NHP 4LFF CTO Server
682785-L21	HP DL320e Gen8 E3-1230v2 FIO Kit (Intel® Xeon® 3.30GHz/4-core/8MB/69W, HT, Turbo2)
669322-B21	HP 4GB 2Rx8 PC3-12800E-11 Memory Kit
659341-B21	HP 500GB 6G SATA 7.2K rpm LFF (3.5-inch) Non-hot plug Midline 1yr Warranty Hard Drive
662961-B21	HP Internal USB Gen8 FIO Kit
615732-B21	HP Ethernet 1Gb 2-port 332T Adapter
663202-B21	HP 1U LFF BB Gen8 Rail Kit
675450-B21	HP 350W 1U Power Supply Kit
534616-B21	HP ProLiant Foundation Pack Single Release Factory Integrated Software Protected by HP Services, warranty includes 3 year Next Day Parts replacement, 0-Years Labor, 0-Years Onsite support. Limited Global warranty - Certain restrictions and exclusions apply
Optional Components	
674845-B21	HP Dedicated iLO Management Port Kit
512485-B21	iLO Advanced License - 1 year
BD505A	iLO Advanced License - 3 year
Note: Because the customized Linux kernel provided by the USB stick supports Oracle Communications Session Border Controller, the certified server does not require an installed operating system.	

Dell PowerEdge R210 II

The certified server, the Dell PowerEdge R210 II, has built-in reliability and energy efficiency. It has low wattage power supplies, and noise level is low (similar to a desktop computer) to meet the needs of sound-sensitive office environments.

The Dell PowerEdge R210 II has two on-board management ports *wancom0* and *wancom1*, and a Network Interface Card (NIC) that hosts two signaling and media ports *s0p0* and *s1p0*. Optional NICs provide for additional management and media ports.

Users should refer to the Dell documentation shipped with the server.

Server configuration is described in the following table.

Part Number	Item
SYS-G-ACTR2100II-00	Oracle PowerEdge R210II XL chassis which includes all components and parts.

Note: Because the customized Linux kernel provided by the USB stick supports Oracle Communications Session Border Controller, the certified server does not require an installed operating system.

Embedded Appliance

The certified servers contain an embedded appliance — the USB stick. The customized kernel on the USB stick provides partial Linux functionality and is not accessible once installed. The kernel contains a multiboot bootloader that performs all the functions required to load the server edition software. The bootloader runs when the system starts then loads and transfers control to the Linux kernel software that reads the boot parameters, decompresses and loads the boot file, and displays console options.

Software verifies the presence of the USB stick on a daily basis. Failure to detect the USB stick is equivalent to license expiration, and results in loss of functionality. Once the USB stick is re-installed, and the server rebooted, functionality is restored.

Licensing

Server edition licenses are based on the serial number of the USB stick, and are read and loaded directly from the USB stick during installation. You can add additional licenses (for example, additional feature groups, or additional session support) by sending a request to Oracle that includes the USB stick serial number.

1. Determine the serial number of your USB stick by using the **`show version boot`** command. This number is displayed under Oracle Serial Number.
2. Send your license request that includes the serial number to Oracle.
3. Add your license using the **`add`** command in *Configuration* mode.
4. Verify your license using the **`show features`** command in *Privileged* mode.

Architectural Differences

This section provides an overview of the architecture of the software-only Oracle Communications Session Border Controller, Server Edition. Because this version does not include the same hardware components found with the other Oracle platforms (Acme Packet 3820 or Acme Packet 4500 for example), the internal system works differently.

Datapath

The Middle Box Control Daemon (MBCD) is a key task within the host subsystem. This application adds, deletes or modifies media forwarding rules to the kernel. Forwarding rules are analogous to entries in the Content Addressable Memory (CAMs) provided by system hardware.

Management traffic, whether coming from a management interface or from a media interface via Host-In-Path (HIP) configuration entry travels to and from the management applications within the host subsystem using the same software datapath.

Packet Processing

Packet processing includes, but is not limited to, ingress and egress signaling packets and media packets. This section describes these three packet types and how they are processed.

All ingress IP packets follow the same datapath for processing. Those users familiar with other Oracle platforms such as Acme Packet 3820 and Acme Packet 4500, will find some similarities with matching in the CAM and processing in the NP. For example:

- VLAN decoding
- Pattern matching
- Target processing

The combination of matching certain packets with the operations to perform on those matched packets form a kernel rule. The creation and management of these rules for media interfaces, for example media and signaling packets, are initiated from MBCD. The rules for management interfaces are separate and are created from different parts of the software.

The target processing section performs the following actions with the different packet types:

Packets	Action
Management	Along with HIP packets get directed to the host IP stack, which is protected against flooding and other traffic attacks.
Signaling	Get directed to the IP+SIP/H.323 stack, which is bandwidth protected according to the DoS settings in the media-manager. Packets are placed in different queues according to trust level and processed accordingly by the applications.
Media	Get processed. For performance and latency reasons, the media packets are processed entirely in the kernel, based on the instructions set in the kernel rule targets. Kernel rule targets include NAT, RFC2833 processing, source-tracking for latching and QoS analysis.

System Highlights

This section provides an overview of the aspects of the system unique to Oracle Communications Session Border Controller, Server Edition. For those users familiar with (or curious about) the other Oracle hardware platforms, you will find references to what makes
Oracle Communications Session Border Controller, Server Edition different from the other platforms.

Hardware

Because Oracle Communications Session Border Controller, Server Edition is a software-only product, it does not have the following hardware-related components:

- Dedicated network processors
- Content Addressable Memory (CAM)
- Non-Volatile Access Memory (NVRAM)
- Identification Programmable Read Memory (IDPROM)
- Fixed management ports

File System

The Oracle Communications Session Border Controller, Server Edition install creates the following file system:

- Three system partitions on the hard drive
- Zero to four variable-sized extended partitions that are user configurable (/mnt/sys and /mnt/app are the factory defaults for user file systems)

The three system partitions include:

- /boot: 2 GB partition containing the key files needed to start the system, including the single boot image and the MAC address table (mactab) file. This is the folder into which you copy your upgrade images.
- /code: 2 GB partition containing all the same files you find on the other Oracle platforms. Your configuration files and boot image reside here.
- /opt: 16 GB partition containing information such as logs, crash files, temporary data and so on. Logs are rotated in /opt/logs.

Boot Process

The boot process starts automatically when you power on the system for the first time or after a reset. The bootloader process, using the file system drivers, reads the boot configuration and loads the compressed build file (for example, *nnscz639.bz*) from the source specified by the boot parameters. By default, the process boots the Server Edition software from the hard disk.

The bootup output is directed to the VGA console by default; but it can be changed to a COM port by editing a boot parameter.

Boot Parameters

You can change some of the boot parameter values such as the default boot filename or the target name, which specifies your system's name. The following table lists the boot parameters along with a description.

Parameter	Description
Boot File	System inserts the filename bzImage as the default boot filename after installation. You can change this name during operational load changes such as upgrades.
IP Address	Specifies the IP address for wancom0.
VLAN	Specifies an optional VLAN tag for wancom0.
Netmask	Specifies the IP mask for wancom0.
Gateway	Specifies the IP address for the wancom0 default gateway.
Host IP	The IP address of an FTP server, a source on image files.
FTP username	The FTP username used for retrieval of image files.
FTP password	The FTP password used for retrieval of image files.
Flags	For use by Oracle for diagnostic procedures.
Target Name	Name you choose to specify your system (maximum of 64 characters)
Console Device	Specifies the interface to which the output of the kernel console is sent. All consoles are always active for accessing Oracle Communications SBC output. But there is only one console to which the kernel information is output. Having only one console for the output means you collect kernel core information from it; which provides a failsafe method of collecting the information regardless of system state. You can specify the following interface values for serial console data: • first serial port COM1 • VGA (You can use a standard USB keyboard to generate input.)
Console Baudrate	Speed of your serial console interface.
Other	For use by Oracle for diagnostic procedures

Accessing Boot Parameters

Boot parameters are accessible during the boot process and in configuration mode. You access the boot parameters when you want to enter and/or edit information such as the name of the boot file.

To access boot parameters during a boot:

1. While the boot process is running, press the spacebar to stop the automatic boot process.
2. Enter p at the prompt to display the list of boot parameters. (You can enter a question mark (?) at the prompt to display a list of boot parameter commands.)
3. Enter c at the prompt to edit the parameters if you want to add or edit existing information.

To access boot parameters in configuration mode:

1. Login with the appropriate username.

2. Enter the enable mode using the required password.
3. Enter the configuration mode by typing `configure terminal` and pressing Enter.
4. Enter `bootparam` to access the boot parameters.
5. Enter new or edit existing information.

Interface Mapping

Oracle Communications Session Director, Server Edition uses the Ethernet interfaces provided by the host. The Ethernet interface names for physical ports are configured dynamically by the kernel and can change between system boots, for example when hardware changes are made to the platform, such as adding new PCI cards. (For users familiar with the other Oracle platforms, such as Acme Packet 3800 or Acme Packet 4500, interfaces are identified as either management or media interfaces.)

Interfaces are assigned to slots and ports through the use of a file located in the /boot directory called mactab. The file contains the mapping of MAC addresses to Ethernet interface names. If upon first boot, the mapping does not exist, it creates a default one.

For example:

- First interface: *wancom0*
- Second interface: *wancom1*
- Third interface: s0p0 (slot 0, port 0)
- Fourth interface: s1p0 (slot 1, port 0)
- Fifth interface: s0p1 (slot 0, port 1)
- Sixth interface: s1p1 (slot 1, port 1)

A placeholder for *wancom2* and all media interfaces up to slot 1 port 3 are created.

The system attempts to place the interfaces in a logical order if it can identify the platform. For the HP ProLiant DL 120 G7 server the default configuration is four interfaces.

- On-board (left to right): wancom0, wancom1
- NIC (left to right): s0p0, s1p0

The maximum number of interfaces supported is eleven; one management, two redundant High Availability links, and eight media.

Oracle Communications Session Director, Server Edition requires a persistent mapping of Ethernet interface names and MAC physical addresses to ensure continual usability by your configuration.

Commands

You can view the mapping of Server Edition Ethernet interface names against the available MAC physical interfaces, as well as change that mapping to suit your specific network layout using the commands described in the following section. For example, you can change the mapping if you require a redundant HA interface (wancom2) or if you have a hardware change such as the removal of an existing NIC from the system.

In addition, the commands let you visually locate a specific media interface by blinking their LEDs. For example, you can locate the ports on PCI cards for which the list order can vary. The exception is for the wancom interfaces that always default to the on-board Ethernet ports of the certified third-party server.

Note: Locate is not supported for *wancom* ports on the HP DL 120 G7.

The following example is of the default mactab file contents displayed when the `interface-mapping show` command is used:

```
# show interface-mapping
Interface Mapping Info
=================================================================
Eth-IF      MAC-Addr                   Label
wancom0     00:16:3E:30:00:2A          # ctrl port, onboard MAC
wancom1     00:16:3E:30:00:2B          # 2nd ctrl port, onboard MAC
s0p0        00:16:3E:30:00:2C          # PCI left side
s1p0        00:16:3E:30:00:2D          # PCI right side
=================================================================
```

.

Note: All interface-mapping commands, with the exception of locate, require a reboot to activate the new mactab.

When you execute the `interface-mapping` command to view interface mapping information, you can append different subcommands to focus on specific information. The reference to <ethernet if name> can be in either <wancomX> or <SxPy> format:

- <wancomX> indicates a control interface with port #X
- <SxPy> indicates a media interface of slot #x and port #y

The following table lists the interface-mapping subcommands along with their descriptions.

Command	Description
interface-mapping show	Display the existing content of /boot/mactab file, with the mapping information of all the available Ethernet Interface Names versus Physical Interface MAC addresses, along with any customer provided label information.
interface-mapping locate <ethernet if name> <seconds>	Lets you visually locate the Ethernet media interface. One way to achieve this is to flashing the LED of the physical interface when its device name is located. The parameter <seconds> indicates the seconds flashing of LED will occur.
interface-mapping label <ethernet if name> “labeling text”	Lets you label the Ethernet interface identified by <eth-if-name> with a text string you define. For example, you can use a label that is meaningful for your network layout. This label is stored and then displayed as “#” string after the MAC address for the Ethernet interface in the /boot/mactab file.

Command	Description
interface-mapping delete <ethernet if name>	Delete an unused Ethernet interface. The unused Ethernet interface could be result of changing network configuration. For example, if you replace an old NIC with a new one, the system writes the new one into mactab file, but does not delete the old one. A confirmation step appears with warning message. When you confirm the action, this entry is deleted from /boot/mactab file.
interface-mapping swap <ethernet if name1> <ethernet if name2>	Swap the mapping of Ethernet interface names against the available MAC physical interfaces. For example, you can first execute the interface-mapping show command to display the current information. interface-mapping show wancom0 00:16:3E:30:00:2A# control port, onboard MAC wancom1 00:16:3E:30:00:2B# 2nd control port, onboard MAC s0p0 00:16:3E:30:00:2C# **PCI left side** s1p0 00:16:3E:30:00:2D# **PCI right side** Then you can execute the interface-mapping swap command. interface-mapping swap s0p0 s1p0 wancom0 00:16:3E:30:00:2A# control port, onboard MAC wancom1 00:16:3E:30:00:2B# 2nd control port, onboard MAC s0p0 00:16:3E:30:00:2D# **PCI right side** s1p0 00:16:3E:30:00:2C# **PCI left side** A warning message appears. Once you confirm the action, the MAC addresses and their corresponding labels are swapped in the /boot/mactab/file.

After completing required interface mapping, you can run the Installation Wizard to set required basic parameters.

Refer to *Interface Wizard* for additional information.

High Availability

This section provides an overview of the Server Edition High Availability (HA) differences from other Oracle platforms. For those users familiar with other Oracle platforms, such as Acme Packet 3800 and Acme Packet 4500, you will find the configuration is similar, with the following exceptions:

- Configuring the virtual MACs differs
- By default only the wancom1 control interface exists for HA, unless you upgrade to an additional PCI card and create a wancom2
- Wancom1 on the active and standby systems should be connected together using an Ethernet cable.

Defining Virtual MAC Addresses

To support HA, you configure virtual Ethernet (MAC) address MAC addresses based on the Burned In Addresses (BIA) of the media interfaces. To determine what the virtual MAC addresses should be, you first identify a BIA and then calculate the virtual MACs based on that.

To define the virtual addresses you need to configure for each interface:

1. Identify the base MAC of eth0/wancom0 physical interface using the `show interfaces` command. For example, in the following display, you can see the base MAC is 00:50:56:C0:00:08:

```
eth      (unit number 0):
         Flags: (0x78843) UP BROADCAST MULTICAST ARP RUNNING INET_UP
         Type: ETHERNET_CSMACD
         inet: 111.22.0.123
         Broadcast address: 111.22.255.255
         Netmask 0xffff0000 Subnetmask 0xffff0000
         Ethernet address is 00:50:56:C0:00:08
```

2. Set the bottom nibble of the first byte to 2 to define the address as locally administered
3. Set the top nibble of the first byte to 0 and increment it for each interface.

   For example, using the base-MAC for eth0, 00:50:56:C0:00:08, you assign the virtual addresses as follows:

   - First media interface virtual MAC = **02**:50:56:C0:00:08
   - Second media interface virtual MAC = **12**:50:56:C0:00:08
   - Third media interface virtual MAC = **22**:50:56:C0:00:08
   - Forth media interface virtual MAC = **32**:50:56:C0:00:08

Virtual Machine (VM) Edition

As its name indicates, the VM Edition software is designed for use within virtualized network environments. It provides support for VMware VSphere ESXi 5 hypervisor, and Microsoft Hyper-V on Windows Server 2008 R2.

> **Note:** The Oracle Communications SBC supports the use of the MS Hyper-V Manager for importing and setting up the Hyper-v VM files (vhd). It does not support creating new VMs from the MS System Center Virtual Machine Manager (SC-VMM) application, but does allow you to manage the VM using SC-VMM once the VMs have been created using MS Hyper-V Manager.

VMware ESXi 5 is the preferred hypervisor; it supports

- Dynamic Host Configuration Protocol (DHCP)
- dynamic booting
- VLANs
- external USB devices

while Hyper-V provides none of these capabilities. Additionally, the ESXi 5 hypervisor supports up to 250 SIP audio sessions per VM; in contrast, Hyper-V supports a maximum of 50 such sessions per VM.

The VM Edition software, like the Server Edition software, is delivered on a 4GB USB stick. Within VMware environments, the USB stick is functionally identical to its Server Edition counterpart. It provides the unique serial number that serves as a license key for the Oracle SBC software. It also contains all programs and tools required both for Oracle application software operations, and for interaction with the VMware virtualization software. Each USB stick supports one VMware VM instance. Consequently the number of VMs supported by a server is constrained by the number of available USB connectors. Software verifies the presence of the USB stick on a daily basis. Failure to detect the USB stick is equivalent to license expiration, and results in loss of functionality. Once the USB stick is re-installed, and the server rebooted, functionality is restored.

Within Windows 2008 environments, the USB stick is used only for installation, and performs no operational role. A self-generated serial number is used for licensing.

The customer end-user installs the VM Edition USB stick in a server of the customer’s choice — to include the HP ProLiant DL120 G7 that is certified for the Server Edition. The stick can be installed in any available USB connector. For security reasons, Oracle recommends that the stick be installed in an internal USB connector.

Build Images

For VMware virtualization environments, the Release S-C[xz]6.3.9 build image (*nnSCz639-img-bin.ova)*, where *z* specifies a 3rd party platform, is delivered as an *.ova* (open virtualization archive) file. An *ova* file is a tar compression of a VMware virtualization image.

For Windows 2008 R2 virtualization environments, the Release S-C[xz]6.3.9 build image (*nnSCz639-img-bin.vhd)*, where *z* specifies a 3rd party platform, is delivered as a *.vhd* (virtual hard disk) file. The *vhd* file format is used by several Microsoft products to include Hyper-V.

Customers can obtain a VM Edition evaluation image from Oracle. This image, which does not require the presence of a USB stick, allows users to evaluate VMware-based or Windows-Server-based virtual machines for a 90-day trial.

Minimum VM Resources

Each VM instance, regardless of the virtualization environment (VMware or Windows) requires the following minimum allocation or network resources.

– CPU cores	2
– Memory	2GB
– Hard drive storage	40GB
– 32-bit application	
– Interfaces	8 recommended (less can be used)

Licensing

VM Editionlicenses are based on either the serial number of the USB stick (for VMware environments), or on a generated serial number (for Windows environments). You can add additional licenses (for example, additional feature groups, or additional session support) by sending a request to Oracle that includes the serial number.

1. Determine the serial number of your USB stick by using the **`show version boot`** command. This number is displayed under Oracle Serial Number.
2. Send your license request that includes the serial number to Oracle.
3. Add your license using the **`add`** command in *Configuration* mode.
4. Verify your license using the **`show features`** command in *Privileged* mode.

Available Documentation

VMware and Microsoft maintain extensive documentation sites. For information on Hyper-V Windows Server 2008/Windows Server 2008 R2 refer to:

http://technet.microsoft.com/en-us/library/cc753637.aspx

For information on ESXi 5 (VMware VSphere 5) refer to:

http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

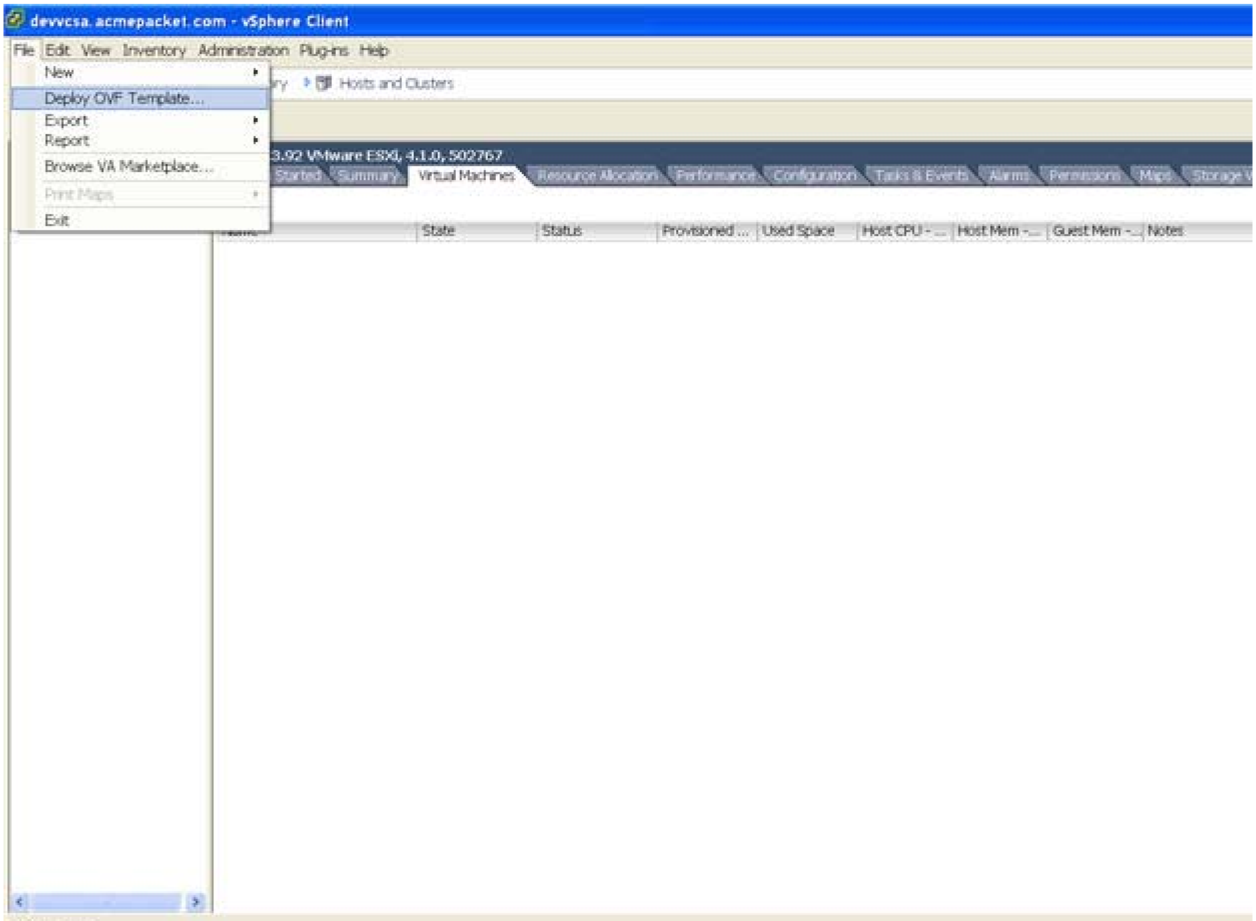
Creating and Deploying VMware Oracle Communications OS VM Edition

This section explains how to deploy the VM Edition using VMware. It assumes the user has already installed the VMware ESXi 5 Hypervisor on an appropriate network server. VMware virtual machine images are deployed as.*ova* files. An.*ova* file is a tar file providing a file directory, an OVF (Open Virtualization Format) template, and a virtual disk image that contains all required Oracle application software. OVF is an open standard for distributing virtual machines.

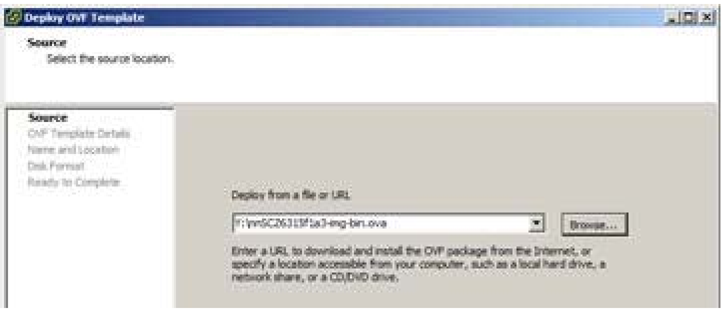
> **Note:** The Oracle Communications SBC supports the use of the MS Hyper-V Manager for importing and setting up the Hyper-v VM files (vhd). It does not support creating new VMs from the MS System Center Virtual Machine Manager (SC-VMM) application, but does allow you to manage the VM using SC-VMM once the VMs have been created using MS Hyper-V Manager.

Use the following procedure to deploy a VM

1. Open the vSphere Client application to the Home page.



2. From the Main Menu, select **File->Deploy OVF Template...**. to display the **Source** window.



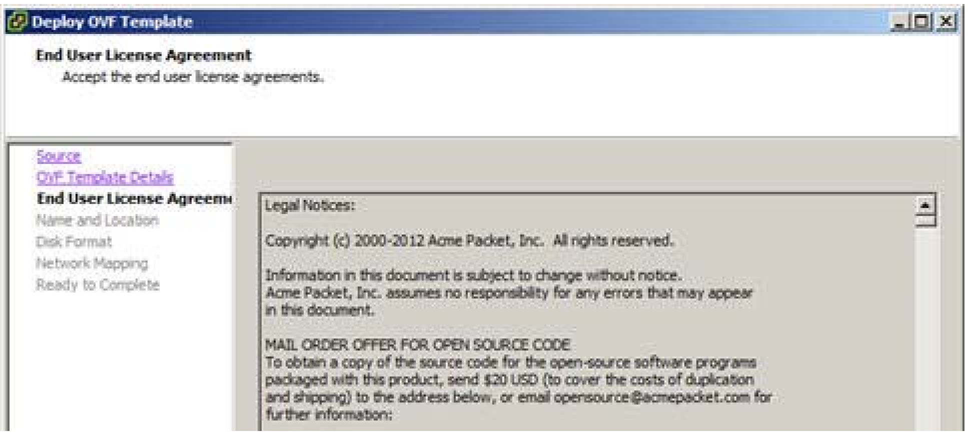
Source
Select the source location.

Deploy from a file or URL

F:\nnSC26313f1a3-eng-bin.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Click **Browse**, navigate to the target*.ova* file (*nnSC639.ova*, in this instance), and click **Next** to display the **End User License Agreement**.



End User License Agreement
Accept the end user license agreements.

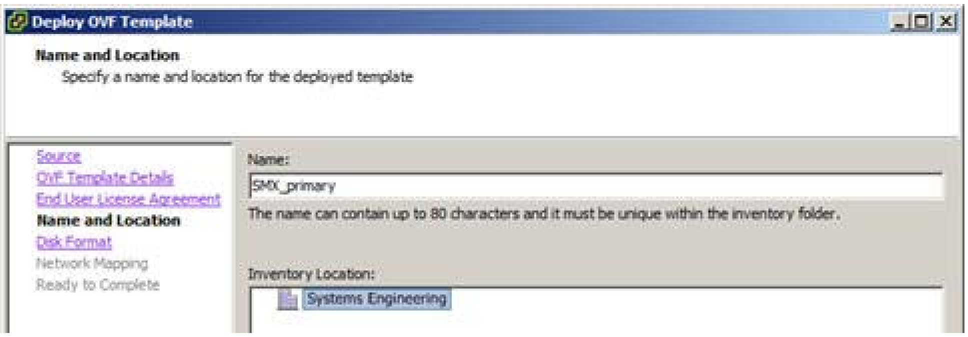
Legal Notices:

Copyright (c) 2000-2012 Acme Packet, Inc. All rights reserved.

Information in this document is subject to change without notice.
Acme Packet, Inc. assumes no responsibility for any errors that may appear in this document.

MAIL ORDER OFFER FOR OPEN SOURCE CODE
To obtain a copy of the source code for the open-source software programs packaged with this product, send $20 USD (to cover the costs of duplication and shipping) to the address below, or email opensource@acmepacket.com for further information:

4. Click **Accept** to accept the license agreement, and to display the **Name and Location** window.

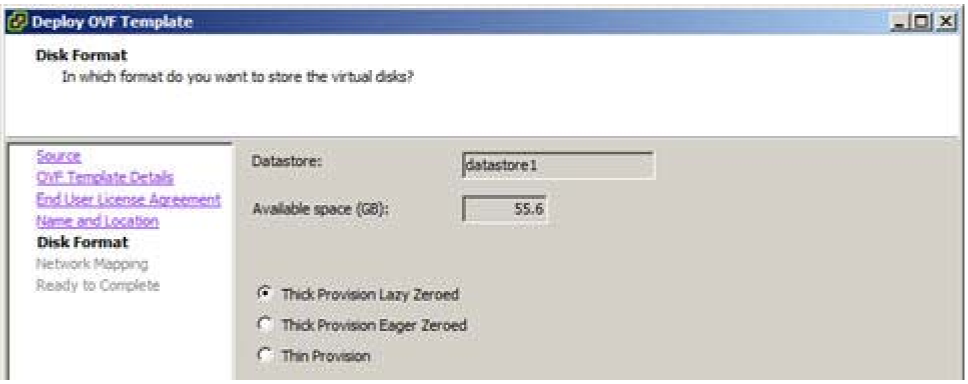


Name and Location
Specify a name and location for the deployed template

Name:
SMX_primary
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:
Systems Engineering

5. Provide a meaningful name for the VM and click **Next** to display the **Disk Format** window.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 55.6

● Thick Provision Lazy Zeroed

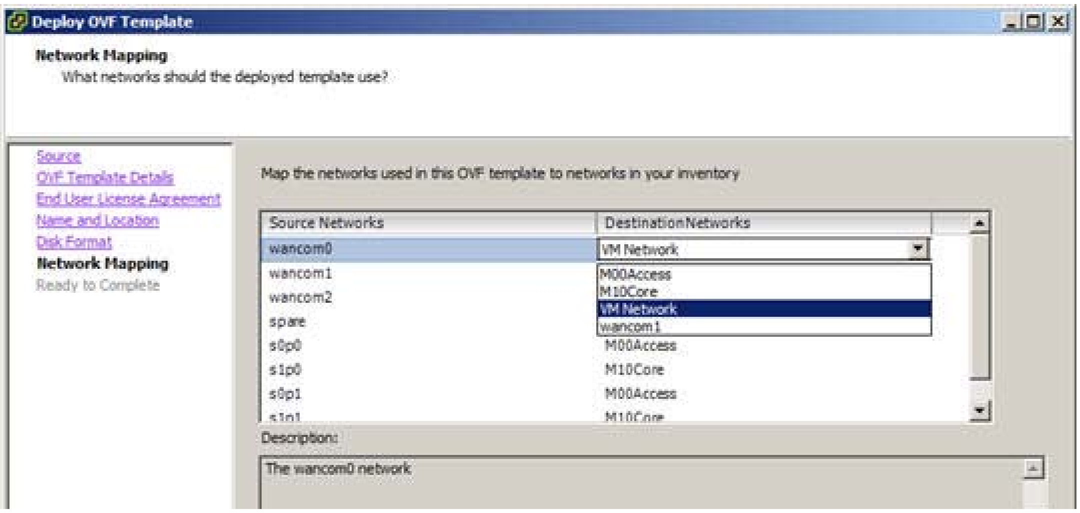
○ Thick Provision Eager Zeroed

○ Thin Provision

6. Choose an available datastore and select the **Thick Provisioned Lazy Zeroed** format.

   Thick Provision format allocates disk space immediately; **Thin provision** format allocates disk space on demand.

   Click **Next** to display the **Network Mapping** window.



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

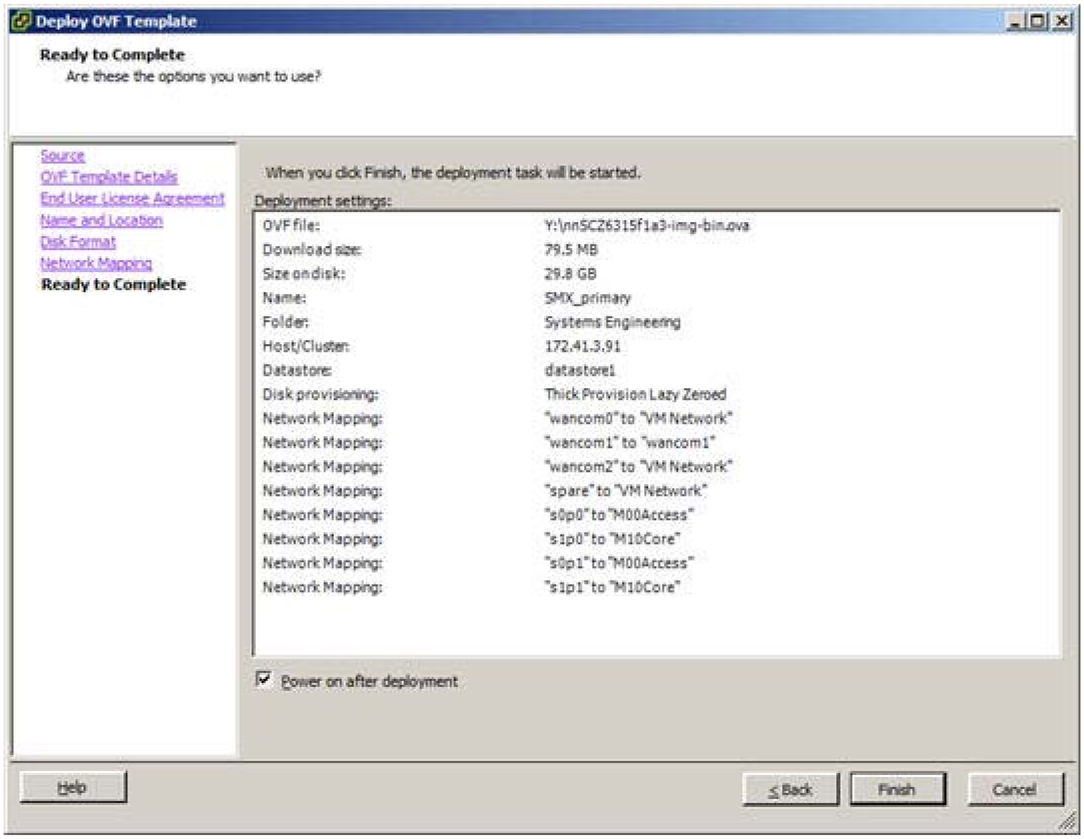
Source Networks	DestinationNetworks
wancom0	VM Network
wancom1	
wancom2	
spare	
s0p0	M00Access
s1p0	M10Core
s0p1	M00Access
s1p1	M10Core

Description:

The wancom0 network

7. Mapping of VM interfaces to existing vSwitch instances ensures external access via the physical Ethernet ports provided by the ESXi host server. Match each of the VM interface to a corresponding vSwitch instance. Choose a default network for any unused ports, generally based on the port type, media/signaling or management/control.

   Click **Next** to display the **Ready to Complete** window.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

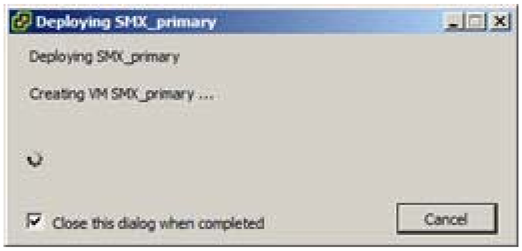
Deployment settings:

OVF file:	Y:\nnSCZ6315f1a3-img-bin.ova
Download size:	79.5 MB
Size on disk:	29.8 GB
Name:	SMX_primary
Folder:	Systems Engineering
Host/Cluster:	172.41.3.91
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"wancom0" to "VM Network"
Network Mapping:	"wancom1" to "wancom1"
Network Mapping:	"wancom2" to "VM Network"
Network Mapping:	"spare" to "VM Network"
Network Mapping:	"s0p0" to "M00Access"
Network Mapping:	"s1p0" to "M10Core"
Network Mapping:	"s0p1" to "M00Access"
Network Mapping:	"s1p1" to "M10Core"

☑ Power on after deployment

8. Review all selections in the **Ready to Complete** window.

   If edits are required, use the Back button to navigate to the appropriate window and enter amended data. When edits are completed, or if no edits are required, click **Finish** to initiate VM creation and deployment.



Deploying SMX_primary

Creating VM SMX_primary ...

☑ Close this dialog when completed

VM creation and deployment is completed when the window closes.

Essential VM Configuration

After creating and deploying a VM, you can use the Oracle ACLI to perform essential VM configuration required for all VM operations.

Essential configuration entails:

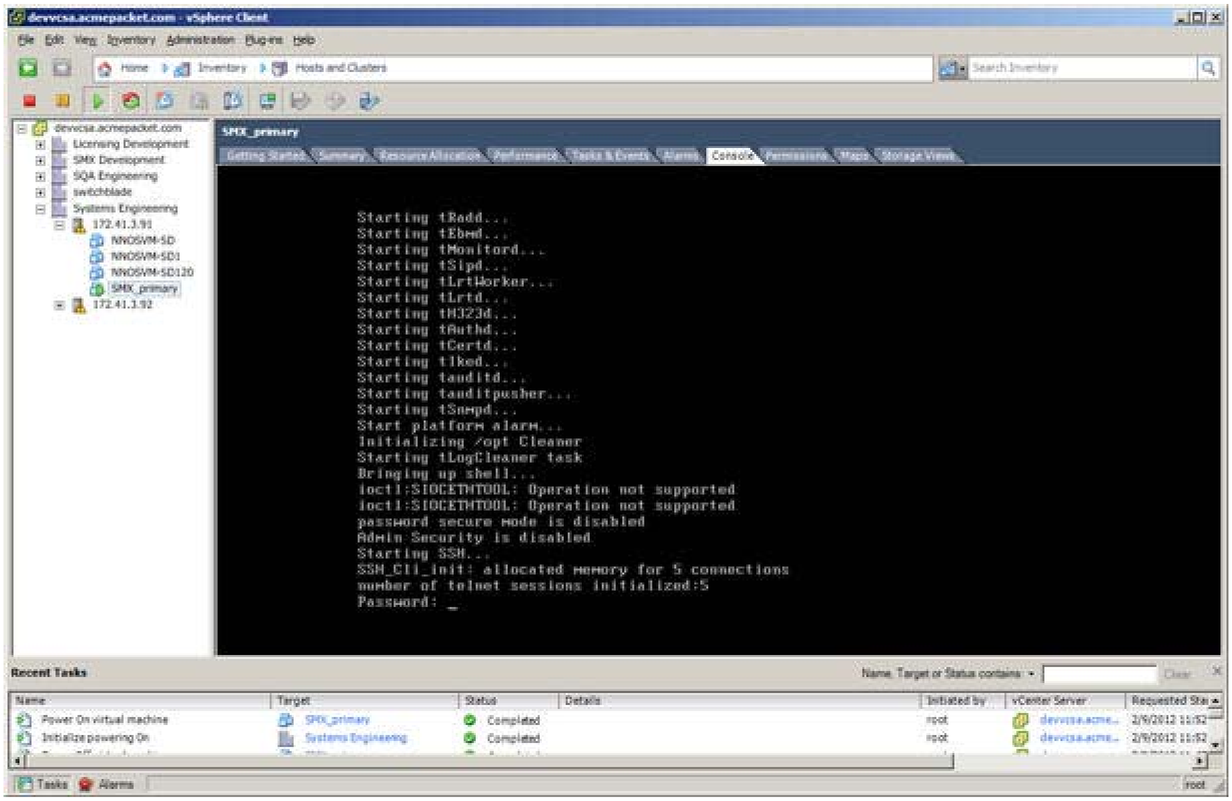
- Setting boot parameters
- Formatting the VM hard disk

These two operations should be performed immediately after VM creation and deployment.

Setting Boot Parameters

You can use Dynamic Host Configuration Protocol (DHCP) or a static identification to specify the source on image files.

1. Open the vSphere Client application to the Home page.
2. Expand the left-hand tabs to display all VMs.
3. Ensure that the target VM in powered ON.
4. Select the **Console** tab, and click anywhere within the window to identify that tab as the source of keyboard input.

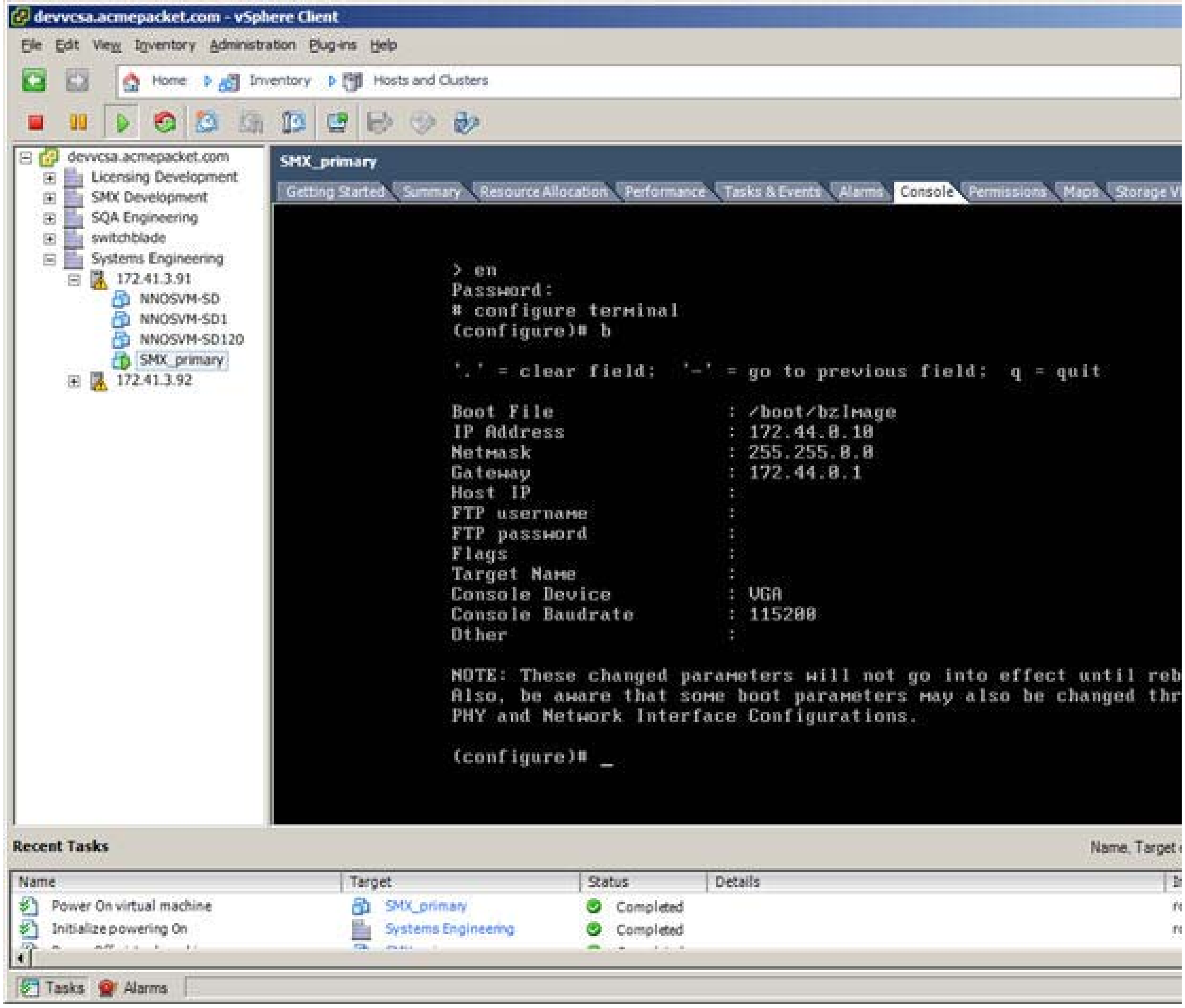

devvcsa.acmepacket.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
Search Inventory
devvcsa.acmepacket.com
Licensing Development
SMX Development
SQA Engineering
switchblade
Systems Engineering
172.41.3.91
NNOSVM-SD
NNOSVM-SD1
NNOSVM-SD120
SMX_primary
172.41.3.92
SMX_primary
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views
Recent Tasks
Name, Target or Status contains: Clear
Tasks Alarms
root

```
Starting tRadd...
Starting tEbmd...
Starting tMonitord...
Starting tSipd...
Starting tLrtWorker...
Starting tLrtd...
Starting tH323d...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Start platform alarm...
Initializing /opt Cleaner
Starting tLogCleaner task
Bringing up shell...
ioctl:SIOCETHTOOL: Operation not supported
ioctl:SIOCETHTOOL: Operation not supported
password secure mode is disabled
Admin Security is disabled
Starting SSH...
SSH_Cli_init: allocated memory for 5 connections
number of telnet sessions initialized:5
Password: _
```

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Sta
Power On virtual machine	SMX_primary	Completed		root	devvcsa.acme...	2/9/2012 11:52
Initialize powering On	Systems Engineering	Completed		root	devvcsa.acme...	2/9/2012 11:52

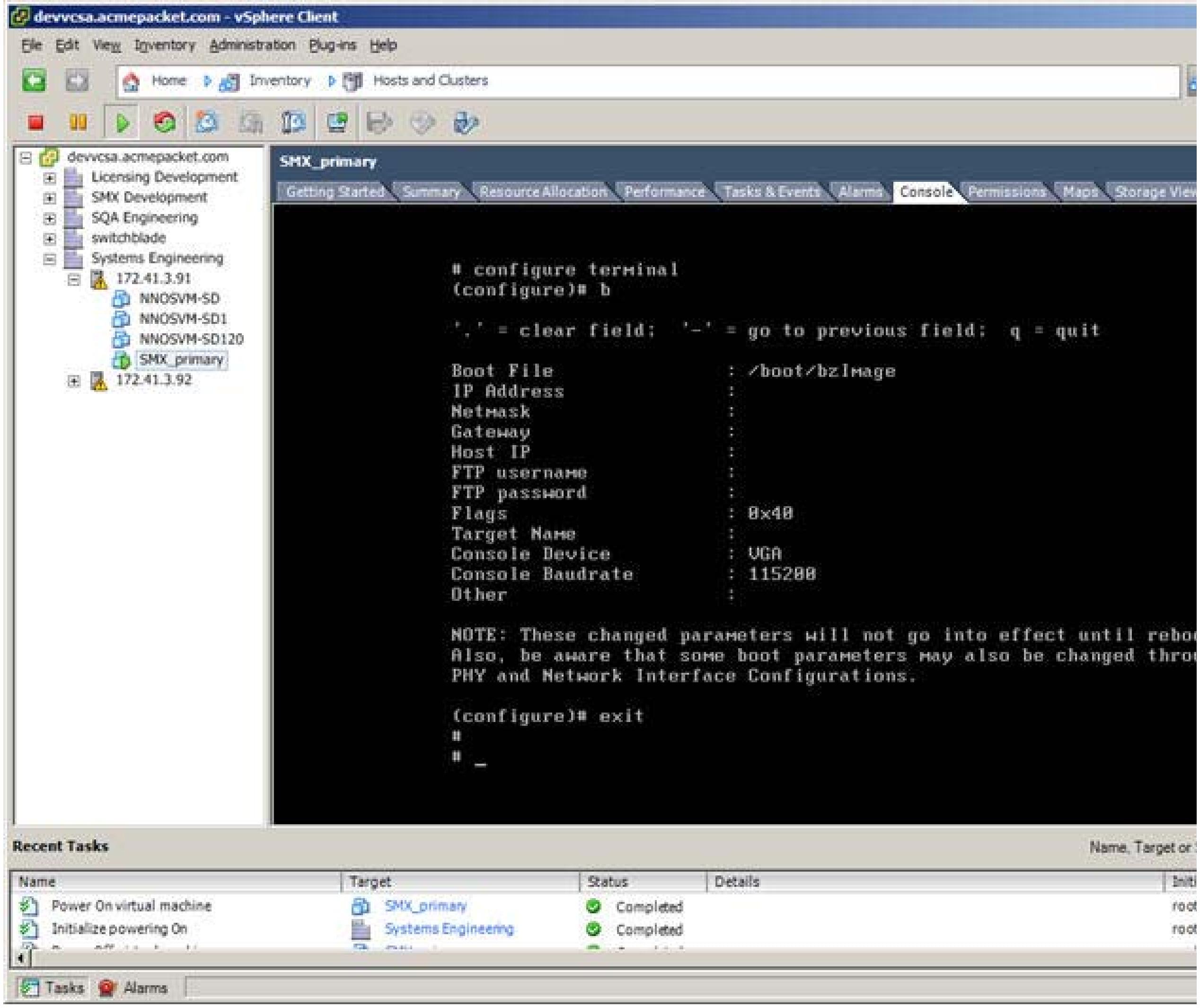
5. Login into *User* mode.
6. Use the **enable** command to enter *Privileged* mode.
7. Use the **configure terminal** command to enter *Configuration* mode.
8. Use the **bootparam** command to set the boot parameters.
9. Use the **done** and **exit** commands to return to Privileged mode.
10. Use the reboot force command to reboot the VM.

    The following two screen shots illustrate the use of static IP (which sets the **IP Address**, **Netmask**, and **Gateway** boot parameters), and DHCP (which requires only the **Flags** boot parameter).



```
> en
Password:
# configure terminal
(configure)# b

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File                  : /boot/bzImage
IP Address                 : 172.44.0.10
Netmask                    : 255.255.0.0
Gateway                    : 172.44.0.1
Host IP                    :
FTP username               :
FTP password               :
Flags                      :
Target Name                :
Console Device             : VGA
Console Baudrate           : 115200
Other                      :

NOTE: These changed parameters will not go into effect until reb
Also, be aware that some boot parameters may also be changed thr
PHY and Network Interface Configurations.

(configure)# _
```

Name	Target	Status	Details
Power On virtual machine	SMX_primary	Completed	
Initialize powering On	Systems Engineering	Completed	


devvcsa.acmepacket.com - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
devvcsa.acmepacket.com
Licensing Development
SMX Development
SQA Engineering
switchblade
Systems Engineering
172.41.3.91
NNOSVM-SD
NNOSVM-SD1
NNOSVM-SD120
SMX_primary
172.41.3.92
SMX_primary
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage View
Recent Tasks
Name, Target or
Tasks Alarms

```
# configure terminal
(configure)# b

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File              : /boot/bzImage
IP Address             :
Netmask                :
Gateway                :
Host IP                :
FTP username           :
FTP password           :
Flags                  : 0x40
Target Name            :
Console Device         : VGA
Console Baudrate       : 115200
Other                  :

NOTE: These changed parameters will not go into effect until rebo
Also, be aware that some boot parameters may also be changed thro
PHY and Network Interface Configurations.

(configure)# exit
#
# _
```

Name	Target	Status	Details	Initi
Power On virtual machine	SMX_primary	Completed		root
Initialize powering On	Systems Engineering	Completed		root

Formatting the VM Hard Drive

Use this procedure to format the VM hard drive.

1. Open the vSphere Client application to the Home page.
2. Expand the left-hand tabs to display all VMs.
3. Ensure that the target VM in powered ON.
4. Select the **Console** tab, and click anywhere within the window to identify that tab as the source of keyboard input.
5. Login into *User* mode.
6. Use the **enable** command to enter *Privileged* mode.
7. Use the **format hard-drive** command to format the VM hard drive.
8. Use the **reboot force** command to reboot the VM and enable the disk changes.

Optional VM Configuration

After creating and deploying a VM, you can use the Oracle ACLI to perform optional VM configuration.

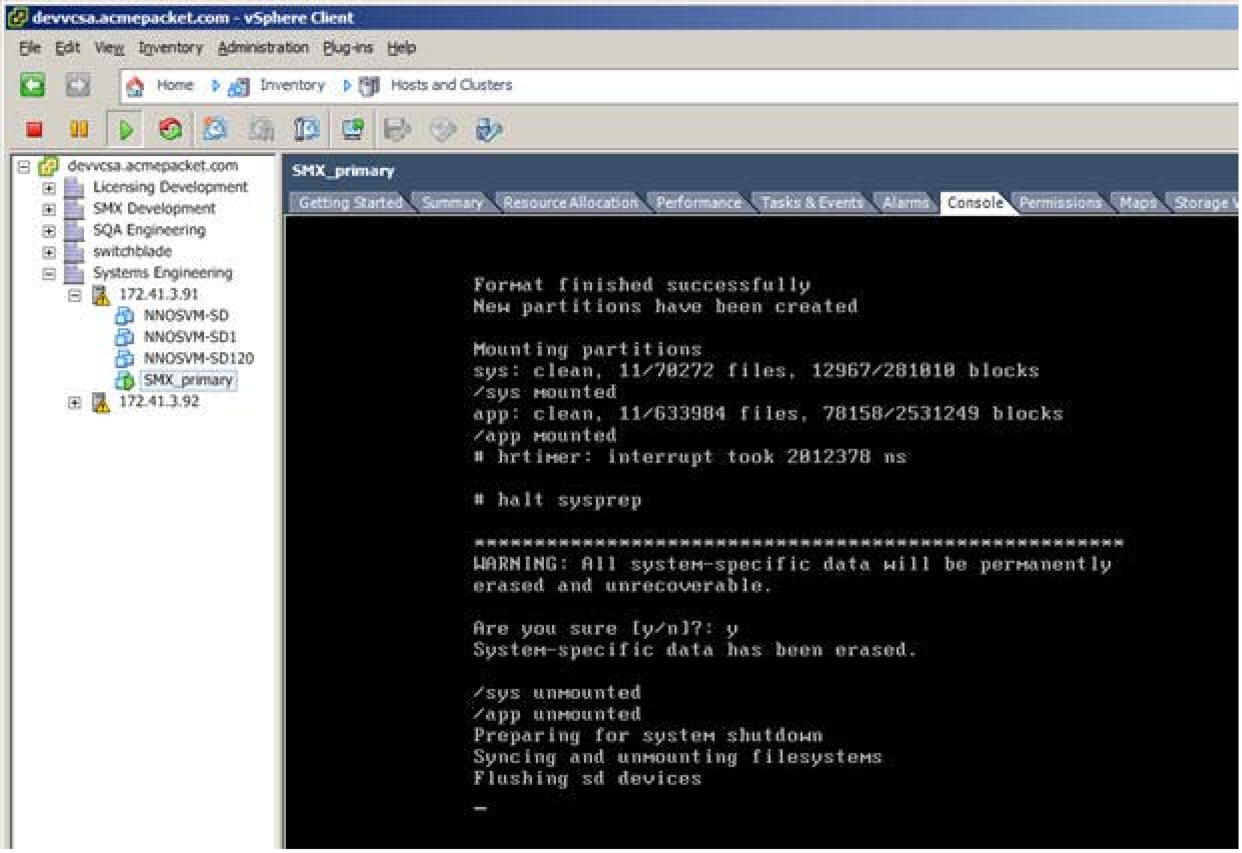
Essential configuration entails:

- Using an existing VM as s template for creating new VMs
- Formatting the VM hard disk

Designating a VM for Use as a Template

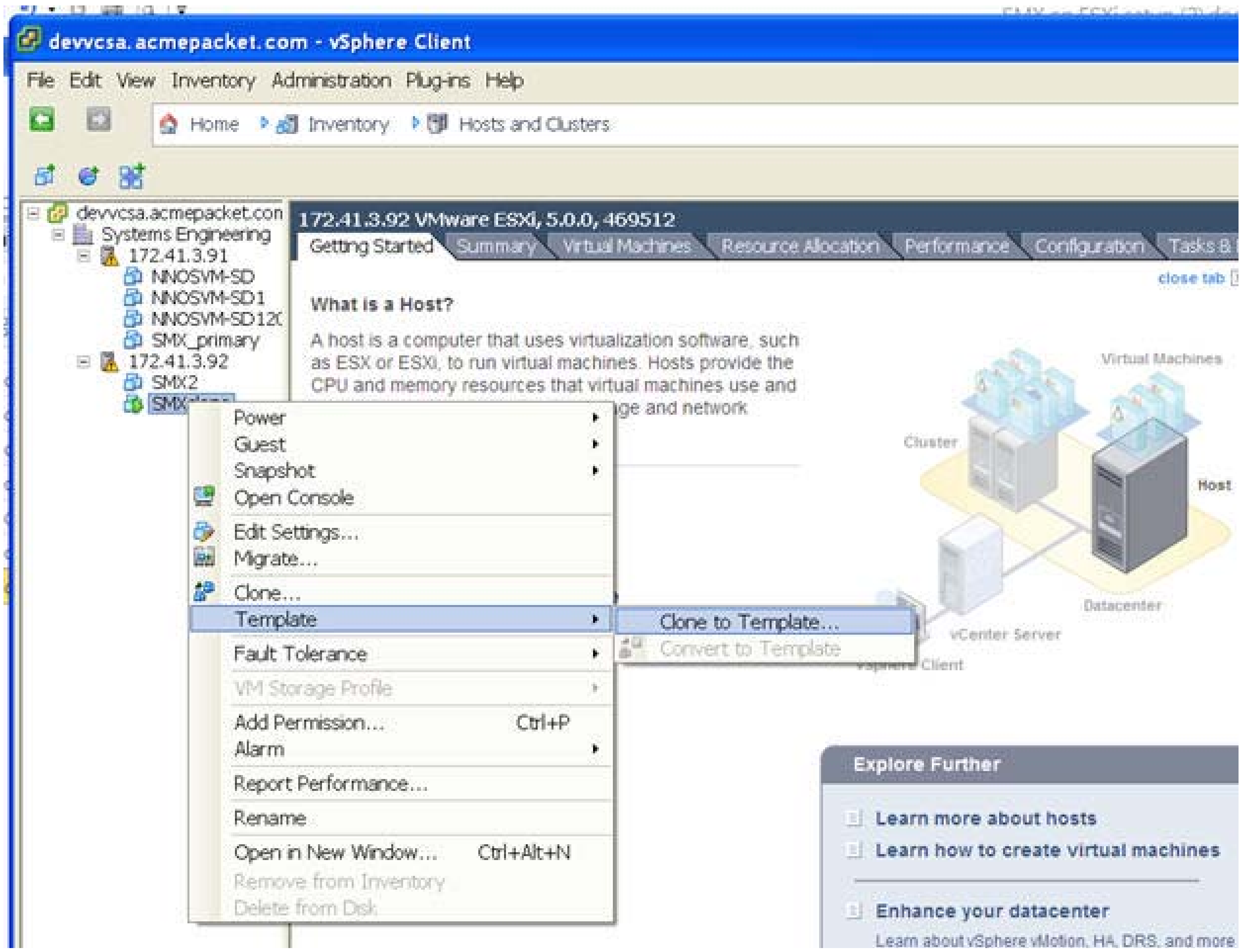
Before cloning a configured VM for use as a template in the creation and deployment of new VMs, all system-specific configuration such as MAC address tables must be deleted from the virtual hard-drive.

1. After formatting the VM hard drive use the **halt sysprep** command to erase all logs from the */opt* file system and remove the persistent MAC address table.



```
Format finished successfully
New partitions have been created

Mounting partitions
sys: clean, 11/78272 files, 12967/281018 blocks
/sys mounted
app: clean, 11/633984 files, 78158/2531249 blocks
/app mounted
# hrtimer: interrupt took 2812378 ns

# halt sysprep

********************************************************
WARNING: All system-specific data will be permanently
erased and unrecoverable.

Are you sure [y/n]?: y
System-specific data has been erased.

/sys unmounted
/app unmounted
Preparing for system shutdown
Syncing and unmounting filesystems
Flushing sd devices
_
```

2. Use the vSphere **Clone to Template** menu to create a new template from the existing VM.

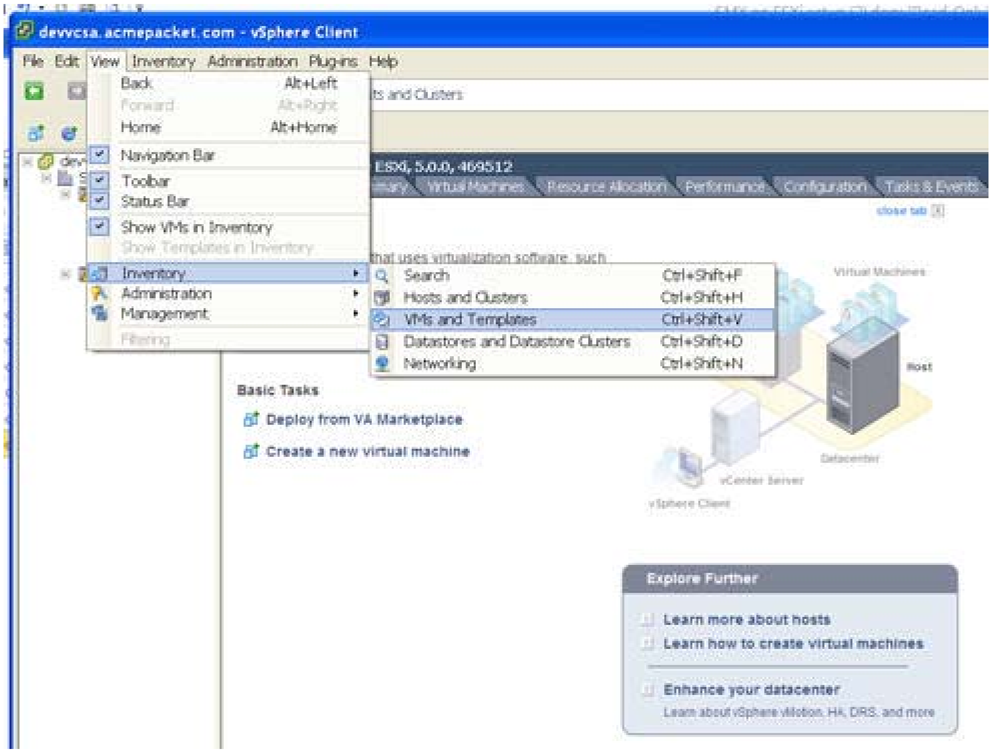


What is a Host?

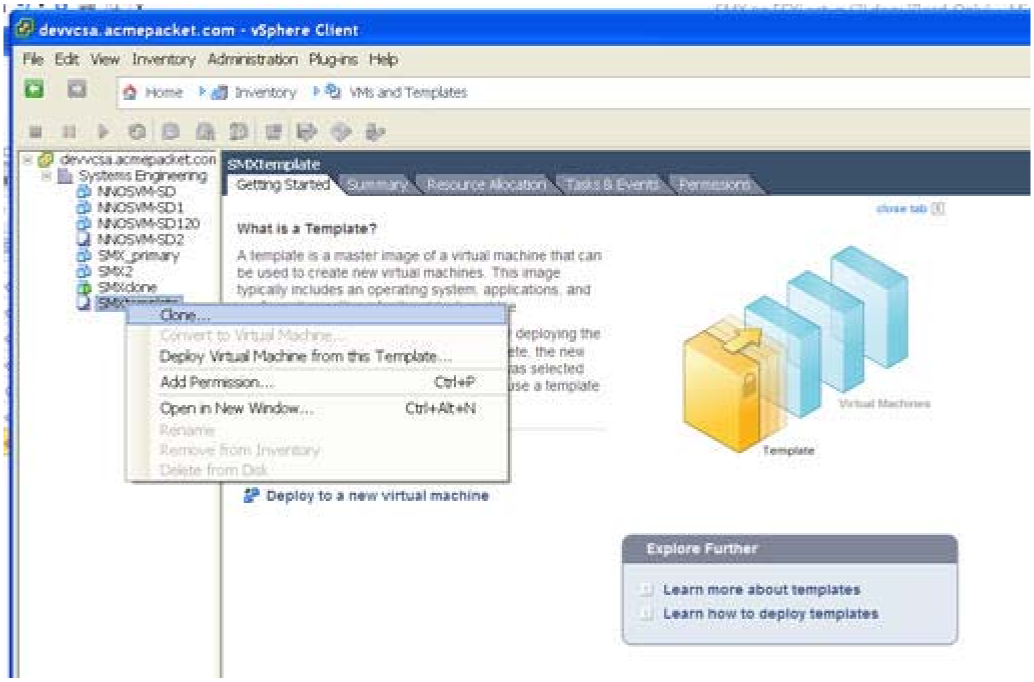
A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and ...ge and network

3. The resulting template can now be deployed as one or multiple VMs. Each new VM is created with unique MAC address, and inherits the boot parameters from the template

4. Use the **View --> Inventory --> VMs and Templates** menu to clone a template to an existing VM.



5. Right-click to clone the template; the Status Bar shows the progress of the operation.



What is a Template?

A template is a master image of a virtual machine that can be used to create new virtual machines. This image typically includes an operating system, applications, and

deploying the ete, the new as selected use a template

2 Software Editions

Overview

This chapter provides an overview of common features and functionality provided by the software-only editions of Release S-C[xz]6.3.9, specifically the Server Edition and the VM Edition.

For more detailed information about the common functionality, refer to the documentation for Net-Net SBC C6.3 release.

Common Functionality

Both the Server Edition and the VM Edition include functionality common across all Oracle platforms:

- ACLI structure, syntax and process (as well as most commands)
- Net-Net Central support
- Net-Net SBC configuration
- Security certificates loaded and stored
- Peering and access models
- SIP trunking
- High availability

Denial of Service Protection

The Server Edition and VM Edition support of Denial of Service (DoS) protection differs from the Oracle Hardware Platforms Edition because of the absence of Oracle network interface hardware. Consequently DoS protection is implemented in software and consumes CPU cycles when responding to attacks.

In addition, the Server Edition and VM Edition handle media packet fragments differently, processing them in the datapath rather than in the host application code. Protection against fragment attacks is still present by ensuring fragments are never kept more than 5 ms.

DoS Calculations

DoS provisioning is accomplished in the *media-manager* configuration mode. Three new parameters (supported on both the Server and VM Editions) define DoS thresholds.

max-trusted-packet-rate	specifies the maximum trusted packet rate in packets/second
max-untrusted-packet-rate	specifies the maximum untrusted packet rate in packets/second
max-arp-packet-rate	specifies the maximum ARP packet rate in packets/second

While the configured rate is expressed as packets/second, the implementation, or actual, rate is measured as packets/millisecond. Configured and actual rates are shown below.

	Configured Rate	Actual Rate
max-trusted-packet-rate	**3200 pkts/sec**	**3 pkts/ms**
max-untrusted-packet-rate	**1700 pkts/sec**	**1 pkt/ms**
max-arp-packet-rate	**1200 pkts/sec**	**1 pkt/ms**

Displays for various **show** commands, such as **show datapath DOS settings**, report the millisecond-based actual rate, leading to the apparent discrepancy between the configured rate and the displayed rate as shown below.

	Configured Rate	Actual Rate	Displayed Rate
max-trusted-packet-rate	**3200 pkts/sec**	**3 pkts/ms**	**3000 pkts/sec**
max-untrusted-packet-rate	**1700 pkts/sec**	**1 pkt/ms**	**1000 pkts/sec**

Ingress Queues

The ingress packets destined for the host are placed in one of four queues:

- untrusted
- trusted
- ARP request
- ARP reply

Events such as latching and RFC2833 translation are placed in a fifth queue. The event queue has the highest priority and is emptied for each iteration, which ensures control traffic is not blocked under DoS attacks.

Net-Net Session Director, Server Edition supports a maximum of 8000 trusted endpoints. Currently, when the trusted queue is full, the next endpoint coming in enters the untrusted queue. This is reported in the output of the `show acl trusted` as `Trusted Entries not allocated due to ACL constraints:`.

DoS Configuration Defaults

The following example shows default DoS values in the media-manager configuration.

```
media-manager
max-signaling-bandwidth 332000
max-untrusted-signaling 100
min-untrusted-signaling 30
app-signaling-bandwidth 0
tolerance-window 30
arp-msg-bandwidth 32000
```

Based on these default values the system calculates the trusted, untrusted, ARP and events packets per second.

Use the `show sw-datapath DOS settings` command to display these values.

```
# show sw-datapath DOS settings
Queue Size PPS
ARP reply 375 250
ARP request 375 250
Trusted 210 142
Untrusted 300 200
Event 8192 9000
```

Packet Trace/PCAP

The Server and VM Edition support of packet tracing differs from the other Oracle platforms such as Net-Net 3800 and Net-Net 4500. When enabled, packets are captured that meet specific criteria. The packets are logged into a file in the /opt/traces directory in a PCAP-formatted format as well as being displayed to the ACLI session from which the capture was executed.

You can enable or disable packet capture in this release. The default filter uses port 5060 on the specified interface to capture both ingress and egress ICMP traffic. This release does not support sending the captured packets off the box in RFC2003 IP in IP format. Therefore the capture-receiver element supported by the other platforms has been removed.

Initiating Packet Capture

You issue the following command to initiate a live packet capture session:

```
packet-trace monitor <interface name>[<capture-filter>]
```

You must specify the name of the physical interface. The optional capture filter argument is a tshark capture filter statement, which must be enclosed in quotes. During a packet trace, a set of .pcap files are created in the /opt/traces directory. The logs created in this directory are rotated by size. The last 25 files are kept and are rotated when they reach 100 MB.

If there are capture files in the /opt/traces directory when this command is run, you are prompted to remove them before running the capture. However, if the maximum of 25 files is created, another run of the `packet-trace monitor` command will not erase the files from the previous execution if the user declines to do so when prompted.

You can exit the session by pressing Ctrl+C.

ACLI Command Support

This section describes common ACLI commands supported only on the Server and VM Editions. Because these are software-only product, you will find that ACLI commands relating to hardware components either are not supported, or differ in syntax and/or output.

Commands Related to Hardware

The following commands relating to hardware components are not supported:

- `show prom-info`
- `fragment-msg-bandwidth`
- `show qos`

Commands Specific to Net-Net Session Director Server Edition

The following commands are specific to the Server and VM Editions:

.

Command	Description
halt	Used by system administrator for an orderly shutdown of the system. Use this when the power needs to be disconnected. You can use the optional parameter force to bypass sanity checks.
interface-mapping	• Allows the wancom and media interfaces to be rearranged • Creates wancom2 or additional media interfaces
packet-trace monitor	Provides packet capture functionality
reboot fast	A new subcommand to the reboot command, fast is used to perform a quick reboot by bypassing a complete hardware reset to restart just the kernel.
show cpu top	Monitor the current CPU load for all processes and threads and provide an interactive display. You press • H to toggle between the display of threads and processes • 1 to toggle the display of the individual CPU loads • q to quit
show datapath	Provides status for different settings/statistics of the datapath. • DOS: displays statistics from the DOS queues controlling the bandwidth. There are four subcommands: •reset: reset DOS queue statistics •settings: display the current DOS values for the five queues •statistics: display the queue statistics for the five queues, including the number of packets and the high-water mark •stats-verbose: display the same information as statistics with additional columns for unexpected error cases For example, show sw-datapath dos settings • instance <instance>: displays the kernel rules for the specified instance. • instances: displays the summary of all kernel, acme.ko, and user-space driver memory
show ip connections	Displays active Linux IP connections
show ip statistics	IP stack stats
show ip tcp	TCP stack stats
show ip udp	UDP stack stats
show route-stats	Route table stats
show routes	Route table

Commands Modified

The following table lists the commands that have been modified for the Server and VM Editions.

Command	Description
timezone-set	Sets the timezone of the Net-Net SBC to one of the current POSIX time zones.
show arp	Additional subcommands for the show arp command displays more ARP database information and statistics. • show arp info: display the ARP database size and memory use • show arp statistics [<slot> <port>}: display global or per-interface ARP statistics
show buffers	Buffer allocation uses a single global pool rather than different pools for different buffer sizes.
show cpu	• List of active CPU cores • Processor speed/model
show memory	Memory statistics
show pci	Lists PCI hardware devices
show support-info	Updated content
show version boot	• SMBIOS system subset • Serial numbers • GRUB boot loader date
show version cpu	SMBIOS CPU subset
show version hardware	• SMBIOS full display • Content depends on manufacturer

Net-Net SBC Functionality Support

This section lists the features and functionality not currently supported by the Server or VM Editions.

- System ACLs
- PHY link redundancy
- SIP port mapping
- Source-based routing
- Jumbo packets
- Full-Mode Session Recording (SRR)
- OCSP
- IPSEC
- sRTP (available on Oracle hardware edition)
- Transcoding
- Fax transcoding
- IPv6
- SCTP
- Bandwidth policing
- Mid-Reserve bandwidth for session agents
- H248
- MGCP
- Lawful Interception
- Border Gateway
- Hide media update

3 SelectiveCall Recording/SIPREC

What is SIPREC?

The SIPREC protocol is the protocol used to interact between a Session Recording Client (SRC) (the role performed by Net-Net SD) and a Session Recording Server (SRS) (a 3rd party call recorder or the Net-Net ISR's Record and Store Server (RSS)). It controls the recording of media transmitted in the context of a communications session (CS) between multiple user agents.

SIPREC provides a selective-based call recording solution that increases media and signaling performance on 3rd party call recording servers, more robust failovers, and the ability to selectively record.

> **Note:**
> 1. SIPREC isolates the 3rd party recorders from the communication session. The 3rd party recorders can determine whether or not recording is desired.
>
> 2. The SRC starts a recording session for every call within a configured realm. All call filtering, if desired, must be accomplished by the SRS. The SRS performs the filtering and selection of which sessions it should record.

License/Hardware Requirements

SIPREC requires the purchase of a Session Recording license. Contact your Oracle Representative for more information.

SIPREC is currently supported on Acme Packet 3820 and Acme Packet Net-Net 4500 running the Oracle Hardware Platforms Edition Release S-C[xz]6.3.9. SIPREC is not currently supported by either the Server Edition or VM Edition.

How it Works

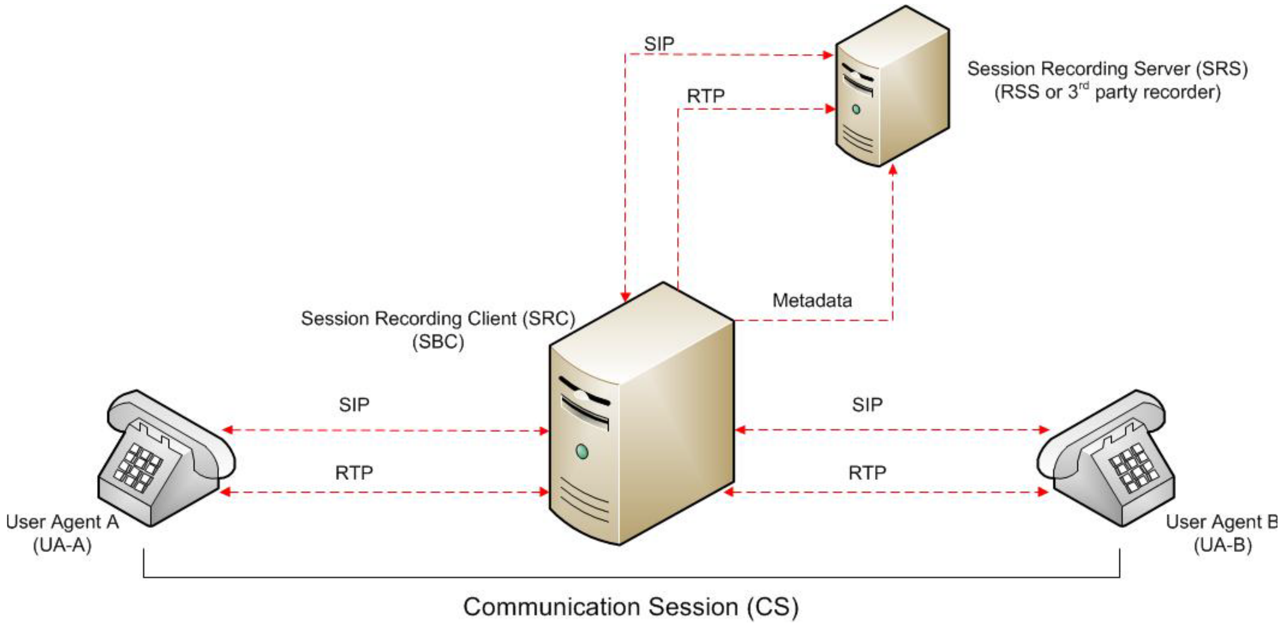
The SIPREC feature supports active recording, where the Net-Net SD acting as the SRC, purposefully streams media to the Net-Net ISR's RSS (or 3rd party call recorder) acting as the SRS. The SRC and SRS act as SIP User Agents (UAs). The SRC provides additional information to the SRS to describe the communication sessions, participants and media streams for the recording session to facilitate archival and retrieval of the recorded information.

The Net-Net SD acting as the SRC, is the source for the recorded media. The Net-Net SD consumes configuration information describing the ecosystem within which it operates. The interface, realm and session agent configuration objects specify the SIPREC configuration. A SIP UA can elect to allow or disallow any network element from recording its media.

During the establishment of a SIP Session, the Net-Net SD determines if SIPREC is configured for recording the call. If so, it then duplicates the media prior to initiating the session with the SRS. (Media replication is set up prior to the recording session). The SRS may choose to record, not record, or cancel the recording session, and then communicates via SIP signaling to the Net-Net SD. If the call is not to be recorded, the SRS signals termination of the recording session.

The Net-Net SD maintains SIPREC metadata information associated with recording sessions. The recording session metadata describes the current state of the recording session and its communication session(s). It is updated when a change of state in the communication session(s) is observed by the Net-Net SD. The SRS is responsible for maintaining call history, etc. The Net-Net SD creates and logs call detail records (CDRs) in the current manner, the 3rd party SRS vendor may collate this information if desired. (For more information about the contents of metadata, see Metadata Contents (45)).

The following illustration shows two endpoints, User Agent A (UA-A) and User Agent B (UA-B). Their session is being recorded by an SRC (the Net-Net SD) and an SRS.


SIP
RTP
Session Recording Server (SRS)
(RSS or 3rd party recorder)
Metadata
Session Recording Client (SRC)
(SBC)
SIP
RTP
SIP
RTP
User Agent A
(UA-A)
User Agent B
(UA-B)
Communication Session (CS)

Configuring SIPREC

This section defines the information required to configure SIPREC on the Net-Net SD. It also provides a sample procedure for configuring SIPREC using the Oracle Command Line Interface (ACLI).

Session Recording Server (SRS)

The Net-Net ISR's RSS acts as the SRS in the network. A **session-recording-server** attribute under the **session-router** object in the Net-Net SD ACLI allows you to enable/disable the SRS. This object is the session recording server that receives replicated media and records signaling. Additional parameters for SRS are configured under the **session-agent**, **realm-config**, and **sip-interface** objects. The rules of precedence for which the Net-Net SD uses these parameters are: **session-agent** takes precedence over the **realm-config**, and **realm-config** takes precedence over **sip-interface**.

Each SRS is associated with a **realm-config**. The realm specifies the source interface from which replicated traffic originates. The destination is an IP Port parameter (IP address or hostname with an optional port) that defines the SIP address (request URI) of the actual SRS.

For an additional level of security, Oracle recommends the SRS be configured in its own realm so as to apply a set of access control lists (ACLs) and security for the replicated communication.

Although the Net-Net SD supports large UDP packets, Oracle recommends the **sip-interface** associated with the SRS realm, be provisioned with a TCP port.

Session Recording Group

The Net-Net SD uses the **session-recording-group** attribute under the **session-router** object in the ACLI to set high availability (HA) for 3rd party call recorders. Using this object, you can define a collection of one or more SRSs. The Net-Net SD utilizes SIP's transport mechanism and keeps track of statistics on each SRS to manage the distribution of traffic and load balancing. (For more information on Net-Net SD load balancing in session recording groups, see Load Balancing (34)). When multiple SRSs are in a session recording group, the Net-Net SD uses heuristics to intelligently route the recording dialog to one or more SRSs utilizing the selection strategy.

The **simultaneous-recording-servers** configuration attribute controls the number of simultaneous SIP dialogs that the Net-Net SD establishes to the SRSs in the session recording group per communication session. For instance, if a session recording group contains 3 SRSs, and **simultaneous-recording-servers** is set to **2**, the recording agent initiates a SIP INVITE to the next two SRSs based on the session recording group strategy. In this way, duplicative recording sessions are instantiated, allowing for recording redundancy in multiple SRSs or within a session recording group.

> **Note:** The Net-Net SD streams media to all SRSs. Each SRS chooses whether or not to ignore the media by returning a "recvonly"(receive only) media line. This permits an SRS to select specific media to record in the recording session, as well as determine whether or not to record the media.

The number of simultaneous recording servers does not dictate the number of recording devices required to be active for a communication session. If two SRSs exist in a session recording group and **simultaneous-recording-servers** is set to **2**, if at least one recording device to any of the servers completes, the recording server is treated as being established.

Load Balancing

The Net-Net SD supports recording server load balancing across members of a session recording group using the following strategies:

[**Round-robin**]: The Net-Net SD remembers the last SRS that was used. Each new recording session selects the next SRS in the session recording group. When simultaneous-recording-servers is greater than 1, the next n recording servers are selected from the session recording group.

[**hunt**]: The Net-Net SD successively attempts to contact SRSs in the session recording group until a successful recording dialog is established with the SRS, starting from the first SRS in the session recording group. The Net-Net SD attempts to contact each SRS in the session reporting group once. When contact is exhausted, the recording device is considered failed. A SIP failure (response greater than 399, timeout or TCP setup failure) causes the Net-Net SD to attempt the next possible SRS. When simultaneous-recording-servers is greater than 1, the Net-Net SD attempts to establish n recording devices in a hunting fashion.

[**least busy**]: For some 3rd party recording devices, the number of concurrent recording servers proves to be the most taxing for system resources. The Net-Net SD tracks the number of recording servers active to a given SRS at any given time. It uses this information to determine which SRS would be the best candidate for the next RS. The SRS with the fewest number of active recording servers receives the next RS. If two or more SRSs in a session recording group currently have the same number of active recording servers, the SRS configured first in the session recording group takes precedence.

[**lowest sustained rate** (fewest-setups-per-minute)]: For some 3rd party recording servers, processing large amounts of sessions in a short amount of time proves to be the most taxing on their system's resources. The Net-Net SD tracks the number of recording server setups over a sliding window of five minutes. The SRS within the session recording group with the fewest setups per the window of time is selected as the next candidate for receiving the recorded session. If two or more SRSs in a session recording group currently have the same value for setups in the given window of time, then the SRS configured first in the session recording group takes precedence.

Session Recording Group within Logical Remote Entities

Each logical remote entity (session-agent, realm-config and sip-interface) has a **session-recording-server** attribute.This attribute is a reference to a specific SRS configuration and can be used to specify a session recording group instead. If a session recording group is specified instead of an SRS, the session recording group name must be prefixed with "**SRG:**" followed by the session recording group name. This distinguishes between an SRS being referenced and a session recording group being referenced.

When the Net-Net SD is configured for legacy SRR features, it is possible to configure a call recording server on both the ingress and egress realms. If configured, the Net-Net SD uses the egress call recording server to record. However, with SIPREC, this process works differently. With SIPREC, if an SRS or session recording group is configured on both the ingress and egress logical remote entities, both the ingress and egress SRS/session recording groups are used. This means that the Net-Net SD records the media between participants twice (or more) - once for the ingress recorders and once for the egress recorders.

If both the ingress and egress SRS/session recording group are the same, the Net-Net SD makes an optimization and only records the media once. Even if the ingress session recording group is the same exact set of SRSs as the egress session recording group (but with a different name), the Net-Net SD replicates media to both destinations. However, if the same set of SRSs has the exact same identifier, the Net-Net SD sends media to one and not both SRSs.

Selective Recording

SIPREC defines a number of use cases for which the Net-Net SD can record communication sessions. These use cases include the use of selective based recording. A **selective recording** is one in which a unique recording server is created per communication session.

> **Note:** The Net-Net SD does not support persistent recording.

For SRSs using selective recording, recording servers are unique per session recording group. For each selective SRS in a session recording group, during the setup of a new communication session, the recording metadata is the same for each recording device. The SRC initiates a new SIP INVITE to the SRS carrying the metadata for that new recording server. The recording agent terminates the SIP dialog at the time that the recording session ends.

> **Note:** The lifetime of a recording session extends beyond the lifetime of the recorded communication. The SRC (Net-Net SD) re-uses the recording session ID in the metadata instead of creating a new ID for each recording.

High Availability (HA) Support

An Net-Net SD using SIPREC supports HA in the network. The Net-Net SD replicates all metadata states between the active and standby Net-Net SDs. Any recording dialogs in progress do not survive the failover, but all calls in progress are preserved. Additionally, the recording dialogs are replicated as well to the failed over Net-Net SD so that in-dialog SIP requests continue to function.

Each recorded communication session replicated to a single SRS counts as two calls instead of one. The Net-Net SD creates two flows between the two participants and two additional flows to the SRS for each of the parent flows.

Single SRS

Assuming that each communication session (CS) is recorded to a single SRS with a single recording session, the total session capacity for recorded sessions is 4000.

SIPREC Configuration Procedure

The following configuration example assumes the Net-Net SD has the session recording license enabled on the Net-Net SD. Changes to the call session recording configuration for SIPREC are dynamic. Active calls in progress remain unaffected by the configuration changes. New calls, however, utilize the changes after a **Save** and **Activate** of the configuration.

The following attributes must be configured:

- **session-recording-server**
- **session-recording-group** (for RSS or 3rd party SRS high availability (HA) only)

  and at least one of the following attributes:
- **realm-config**
- **session-agent**
- **sip-interface**

Session-recording-server Attribute

To configure the "session-recording-server" attribute:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```
2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```
3. Type **session-recording-server** and press <Enter> to access the session recording server-related attributes.

   ```
   ACMEPACKET(session-router)# session-recording-server
   ACMEPACKET(session-recording-server)#
   ```
4. **name** — Enter a unique name for the session recording server. This name can be referenced when configuring realm-config, session-agent, and sip-interface. Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-recording-server)# name SRS1
   ```
5. (optional) **description** — Enter a description for the session recording server. Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-recording-server)# description “<recording server
   name>”
   ```
6. **realm** — Enter the realm for which the session recording server belongs. Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-recording-server)# realm <realm name>
   ```

   Note: Oracle recommends that the session recording server be configured in its own realm.
7. **recording-mode** — Enter the recording mode for the session recording server. Valid values are:
   - **selective** (default) - Unique recording server created per communication session.
   - **persistent** - Not supported. If selected, this option behaves the same as the "selective" option.

   ```
   ACMEPACKET(session-recording-server)# recording-mode selective
   ```

8. **destination** — Enter the destination IP address with IP port (port specification is optional) that defines the SIP address (request URI) of the session recording server. Enter values in the format 0.0.0.0:<port number>. Default is no value specified.

```
ACMEPACKET(session-recording-server)# destination 172.34.2.3:5060
```

9. **protocol** — Enter the protocol that the session recording server uses to accept incoming packets from the session reporting client on the network. Default is **UDP**.

```
ACMEPACKET(session-recording-server)# protocol UDP
```

10. Enter **done** to save the session recording configuration.

```
ACMEPACKET(session-recording-server)# done
```

11. Enter **exit** to exit the session-recording-server configuration.

```
ACMEPACKET(session-recording-server)# exit
```

12. Enter **exit** to exit the session-router configuration.

```
ACMEPACKET(session-router)# exit
```

13. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

14. Enter **save-config** to save the session recording configuration.

```
ACMEPACKET# save-config
```

15. Enter **activate-config** to activate the session recording configuration.

```
ACMEPACKET# activate-config
```

Session-recording-group Attribute (for HA only)

For environments that required high availability (HA) requirements, configure the **session-recording-group** attribute.

To configure the “session-recording-group” attribute and enable HA:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **session-router** and press <Enter> to access the session router-related objects.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type **session-recording-group** and press <Enter> to access the session recording group-related attributes.

```
ACMEPACKET(session-router)# session-recording-group
ACMEPACKET(session-recording-group)#
```

4. **name** — Enter a unique name for the session recording group that is a collection of one or more session recording servers. This name can be referenced when configuring realm-config, session-agent, and sip-interface. Valid values are alpha-numeric characters. Default is no value specified.

```
ACMEPACKET(session-recording-group)# name <SRG Group Name>
```

Note: The name of the session recording group must be prefixed with “SRG”.

5. (optional) **description** — Enter a description for the session recording group. Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-recording-group)# description <Recording Group
   Name>
   ```

6. **session-recording-servers** — Enter the names of the session recording servers that belong to this session recording group. Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-recording-group)# session-recording-servers
   SRS1,SRS2
   ```

   Note: You must enter multiple servers as values for the session-recording-servers attribute.

7. **strategy** — Enter the load balancing strategy that the session reporting client (Net-Net SD) uses when sending recordings to the session reporting server. Valid values are:

   - **Round-robin** (default) - The Net-Net SD remembers the last SRS that was used. Each new recording session selects the next SRS in the session recording group. When simultaneous-recording-servers is greater than 1, the next n recording servers are selected from the session recording group.
   - **hunt** - The Net-Net SD successively attempts to contact SRSs in the session recording group until a successful recording dialog is established with the SRS, starting from the first SRS in the session recording group. The Net-Net SD attempts to contact each SRS in the session reporting group once. When contact is exhausted, the recording device is considered failed. A SIP failure (response greater than 399, timeout or TCP setup failure) causes the Net-Net SD to attempt the next possible SRS. When simultaneous-recording-servers is greater than 1, the Net-Net SD attempts to establish n recording devices in a hunting fashion.
   - **least busy** - For some 3rd party recording devices, the number of concurrent recording servers proves to be the most taxing for system resources. The Net-Net SD tracks the number of recording servers active to a given SRS at any given time. It uses this information to determine which SRS would be the best candidate for the next RS. The SRS with the fewest number of active recording servers receives the next RS. If two or more SRSs in a session recording group currently have the same number of active recording servers, the SRS configured first in the session recording group takes precedence.
   - **lowest sustained rate** (fewest-setups-per-minute) - For some 3rd party recording servers, processing large amounts of sessions in a short amount of time proves to be the most taxing on their system's resources. The Net-Net SD tracks the number of recording server setups over a sliding window of five minutes. The SRS within the session recording group with the fewest setups per the window of time is selected as the next candidate for receiving the recorded session. If two or more SRSs in a session recording group currently have the same value for setups in the given window of time, then the SRS configured first in the session recording group takes precedence.

   ```
   ACMEPACKET(session-recording-group)# strategy round-robin
   ```

8. **simultaneous-recording-servers** — Enter the number of simultaneous SIP dialogs that the session reporting client (Net-Net SD) establishes to the session reporting servers in the session reporting group per communication session. Valid values are **1** to **3**. Default is **0**.

   ```
   ACMEPACKET(session-recording-group)# simultaneous-recording-servers 2
   ```

9. Enter **done** to save the session recording group configuration.

   ```
   ACMEPACKET(session-recording-group)# done
   ```

10. Enter **exit** to exit the session recording group configuration.

    ```
    ACMEPACKET(session-recording-group)# exit
    ```

11. Enter **exit** to exit the session-router configuration.

    ```
    ACMEPACKET(session-router)# exit
    ```

12. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

13. Enter **save-config** to save the session recording group configuration.

```
ACMEPACKET# save-config
```

14. Enter **activate-config** to activate the session recording group configuration.

```
ACMEPACKET# activate-config
```

Realm-config Attribute

To configure the “realm-config” attribute and enable session recording:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **media-manager** and press <Enter> to access the media manager-related objects.

```
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)#
```

3. Type **realm-config** and press <Enter> to access the realm-config-related attributes.

```
ACMEPACKET(media-manager)# realm-config
ACMEPACKET(realm-config)#
```

4. **session-recording-server** — Enter the name of the session-recording server or the session-recording-group in the realm associated with the session reporting client (Net-Net SD). Valid values are alpha-numeric characters. Default is no value specified.

```
ACMEPACKET(realm-config)# session-recording-server <srs-name>

or

ACMEPACKET(realm-config)# session-recording-server SRG:<group-name>
```

Note: The value for this attribute is the name you specified in Step 4 of the Session-recording-server Attribute (36) or Step 4 of the Session-recording-group Attribute (for HA only) (37). If specifying a session-recording-group, you must precede the group name with “**SRG:**”.

5. **session-recording-required** — Enable this parameter to prevent call traffic through the Net-Net ESD, unless there is a successful session established with a recording server. Valid values are:
   - **Enabled** - Prevents call traffic through the Net-Net ESD unless there is a session established with a recording server.
   - **Disabled** (default)- Allows all call traffic through the Net-Net ESD even if the recording server is not available.

```
ACMEPACKET(realm-config)# session-recording-required disabled
```

Note: Oracle recommends that the “session-recording-required” parameter remain disabled.

6. Enter **done** to save the realm configuration.

```
ACMEPACKET(realm-config)# done
```

7. Enter **exit** to exit the realm configuration.

```
ACMEPACKET(realm-config)# exit
```

8. Enter **exit** to exit the media manager configuration.

   ```
   ACMEPACKET(media-manager)# exit
   ```

9. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

10. Enter **save-config** to save the realm configuration.

    ```
    ACMEPACKET# save-config
    ```

11. Enter **activate-config** to activate the realm configuration.

    ```
    ACMEPACKET# activate-config
    ```

Session-agent Attribute

To configure the “session-agent” attribute and enable session recording:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **session-agent** and press <Enter> to access the session agent-related attributes.

   ```
   ACMEPACKET(session-router)# session-agent
   ACMEPACKET(session-agent)#
   ```

4. **session-recording-server** — Enter the name of the session-recording server or the session-recording-group to apply to the session recording client (Net-Net SD). Valid values are alpha-numeric characters. Default is no value specified.

   ```
   ACMEPACKET(session-agent)# session-recording-server <srs-name>

   or

   ACMEPACKET(session-agent)# session-recording-server SRG:<group-name>
   ```

   Note: The value for this attribute is the name you specified in Step 4 of the Session-recording-server Attribute (36) or Step 4 of the Session-recording-group Attribute (for HA only) (37). If specifying a session-recording-group, you must precede the group name with “**SRG:**”.

5. **session-recording-required** — Enable this parameter to prevent call traffic through the Net-Net ESD, unless there is a successful session established with a recording server. Valid values are:

   - **Enabled** - Prevents call traffic through the Net-Net ESD unless there is a session established with a recording server.
   - **Disabled** (default)- Allows all call traffic through the Net-Net ESD even if the recording server is not available.

   ```
   ACMEPACKET(session-agent)# session-recording-required disabled
   ```

   Note: Oracle recommends that the “session-recording-required” parameter remain disabled.

6. Enter **exit** to exit the session agent configuration.

   ```
   ACMEPACKET(session-agent)# exit
   ```

7. Enter **exit** to exit the session router configuration.

```
ACMEPACKET(session-router)# exit
```

8. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

9. Enter **save-config** to save the session agent configuration.

```
ACMEPACKET# save-config
```

10. Enter **activate-config** to activate the session agent configuration.

```
ACMEPACKET# activate-config
```

Sip-interface Attribute

To configure the “sip-interface” attribute and enable session recording:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **session-router** and press <Enter> to access the session router-related objects.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type **sip-interface** and press <Enter> to access the SIP interface-related attributes.

```
ACMEPACKET(session-router)# sip-interface
ACMEPACKET(sip-interface)#
```

4. **session-recording-server** — Enter the name of the session-recording server or the session-recording-group to apply to the SIP interface on the session recording client (Net-Net SD). Valid values are alpha-numeric characters. Default is no value specified.

```
ACMEPACKET(sip-interface)# se ss on-recording-server SRG:<session
recording server name or session-recording group name>
```

Note: The value for this attribute is the name you specified in Step 4 of the Session-recording-server Attribute (36) or Step 4 of the Session-recording-group Attribute (for HA only) (37).

5. **session-recording-required** — Enable this parameter to prevent call traffic through the Net-Net ESD, unless there is a successful session established with a recording server. Valid values are:

- **Enabled** - Prevents call traffic through the Net-Net ESD unless there is a session established with a recording server.
- **Disabled** (default)- Allows all call traffic through the Net-Net ESD even if the recording server is not available.

```
ACMEPACKET(sip-interface)# session-recording-required disabled
```

Note: Oracle recommends that the “session-recording-required” parameter remain disabled.

6. Enter **exit** to exit the SIP interface configuration.

```
ACMEPACKET(sip-interface)# exit
```

7. Enter **exit** to exit the session router configuration.

```
ACMEPACKET(session-router)# exit
```

8. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

9. Enter **save-config** to save the SIP interface configuration.

   ```
   ACMEPACKET# save-config
   ```

10. Enter **activate-config** to activate the SIP interface configuration.

    ```
    ACMEPACKET# activate-config
    ```

SIPREC Ping Support

On the Net-Net SBC, you can check the connectivity between the Net-Net SBC and the session recording server (SRS) using two new, optional ping commands via the ACLI:

- **ping-method** - SIP message or method for which to ping the SRS.
- **ping-interval** - Amount of time, in seconds, that the Net-Net SBC waits before it pings the SRS in subsequent intervals. For example, if this parameter is set for 60 seconds, the Net-Net SBC pings the SRS every 60 seconds.

This SIPREC ping is a signal that the Net-Net SBC transmits to the connected SRS requesting a response pertaining to the message type that you specify for the ping-method. It uses the ping-interval to determine how long it should wait before sending another ping to the SRS. Once configured (save and activated) the Net-Net SBC uses this feature to perform SIP-based pinging to determine if the SRS is reachable or not.

Configuring SIPREC Ping on the Net-Net SBC

To configure SIPREC ping on the Net-Net SBC, you use the **ping-method** and the **ping-interval** objects under call-recording-server. Use the following procedure to configure SIPREC ping on the Net-Net SBC.

To configure SIPREC ping:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **call-recording-server** and press <Enter>.

   ```
   ACMEPACKET(session-router)# call-recording-server
   ACMEPACKET(call-recording-server)#
   ```

4. **ping-method**—Enter the message or method type for which the Net-Net SBC uses in a ping request to the SRS to determine if it is reachable or not. Default is blank. Valid values are:

   - BYE
   - UPDATE
   - CANCEL
   - OPTIONS
   - SUBSCRIBE
   - NOTIFY

5. **ping-interval**—Enter the amount of time, in seconds, that the Net-Net SBC waits before it pings the SRS in subsequent intervals. Valid values are 0 to 99999. Default is 0 (zero). The setting of zero disables the ping interval.

6. Type **done** and press <Enter>.
   ```
   ACMEPACKET(call-recording-server)# done
   ACMEPACKET(call-recording-server)#
   ```
7. Type **exit** and press <Enter>.
   ```
   ACMEPACKET(call-recording-server)# exit
   ACMEPACKET(session-router)#
   ```
8. Type **exit** and press <Enter>.
   ```
   ACMEPACKET(session-router)# exit
   ACMEPACKET(configure)#
   ```
9. Save the configuration.

Example SIPREC Ping Configuration

The following is an example of a SIPREC ping configuration.

```
call-recording-server# show
        name                          SRS1
        description                   session recording server
        realm                         realmA
        mode                          selective
        destination                   132.43.5.6
        port                          5060
        transport-method              DynamicTCP
        ping-method                   OPTIONS
        ping-interval                 60
```

In the above example, the Net-Net SBC sends a ping request to the SRS using the OPTIONS value every 60 seconds to determine if the SRS is reachable or not.

SIPREC Re-INVITE Collision and Back-off Support

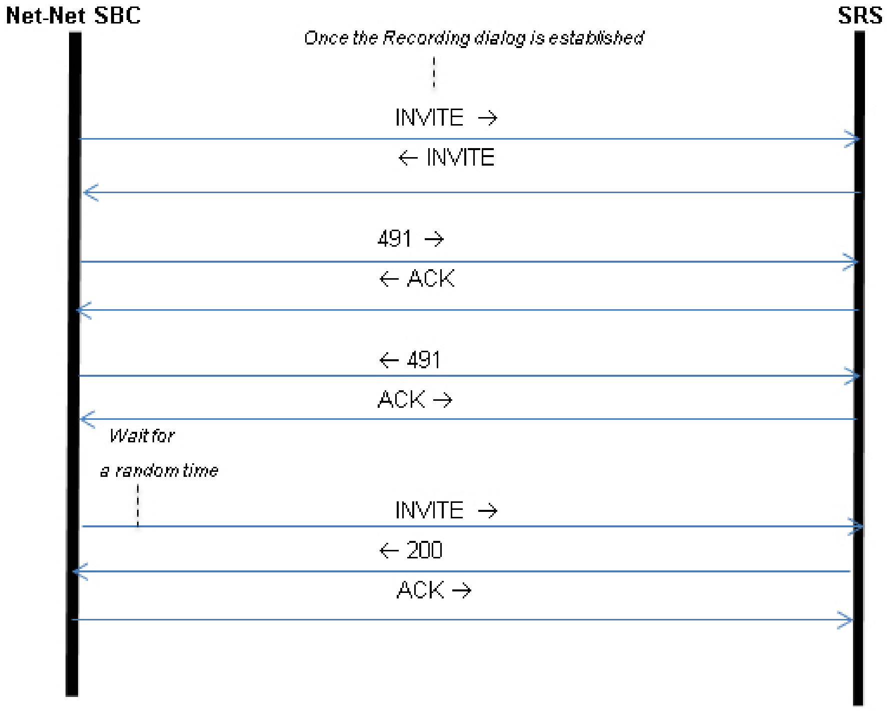
The Net-Net SBC acts a back-to-back User Agent (B2BUA) in all call scenarios. However with SIPREC, the Net-Net SBC acts as a User Agent Client (UAC) when connected with a session recording server (SRS). Therefore, SIP requests can originate from the Net-Net SBC.

During a recording session, when the SRS establishes a recording dialog, the Net-Net SBC and the SRS may send Re-INVITES to each other with updated information. When the Net-Net SBC receives an INVITE while it is still waiting for the response to a previous INVITE it sent out, this produces an INVITE collision.

To avoid an INVITE collision, the Net-Net SBC sends a “491 Request Pending” response back to the SRS and then waits for a random amount of time before re-trying the INVITE. It also acknowledges (ACK) any 491 response received from the other side. RFC 3261 and RFC 6141 describes the way the User Agent (UA) resolves the INVITE collision. The random wait time is chosen based on the following guidelines from RFC 3261:

- If the UAC is the owner of the Call-ID of the dialog ID (i.e., it generated the value), T (the wait time) is a randomly chosen value between 2.1 and 4 seconds in units of 10 milliseconds.
- If the UAC is not the owner of the Call-ID of the dialog ID (i.e., it did not generate the value), T (the wait time) is a randomly chosen value between 0 and 2 seconds in units of 10 milliseconds.

The following call flow diagram shows the Net-Net SBC's feature to avoid INVITE collision.



Metadata Contents

The recording metadata contains a set of related elements which define the recording session. A recording session may contain zero or more communication sessions and/or communication session groups. A communication session represents a call instance; a communication session group represents a related group of communication sessions. A recording session is composed of a sequence of complex element types. Not all element types are required to describe a recording session initiated from the Net-Net SD. The recording session XML schema defines the following element types:

- **dataMode** - partial or complete metadata description (required)
- **group** - a collection of related communication sessions
- **session** - a single communication session of two or more participants (required)
- **participant** - a SIP endpoint representation (required)
- **stream** - a media stream
- **extensiondata** - application specific data outside of the SIPREC scope.

The recording agent generates dataMode, session, participant, and stream elements. Extension data is attached to other elements within the metadata through the use of the parent attribute. The recording metadata is defined as a sequence of element types; therefore all associations between elements are represented as references to element identifiers.

The state of the metadata within a recording session reflects the state of the communication session(s) which is being recorded. SIPREC implements stop-times and reason codes when communication sessions end within a recording session. Once a communication session, participant, or media stream has been marked as 'stopped' and accepted by the SRS, the metadata item is removed from the current metadata state. In addition, media lines within the SDP or the recording session may be re-used/re-labeled for reuse if new communication sessions and media streams are created within the recording session.

The XML schema for the recording metadata is defined in the IETF draft RFC “*draft-ram-siprec-metadata-format-02 [7]*”.

The ACLI command to show recorded metadata is “**show rec** ”. For more information on this command see the section, Show rec (46).

Show Commands for Recording Sessions

The Net-Net SD allows you to utilize the following **show** commands via the ACLI to display statistical information about recording sessions:

- **show rec**
- **show rec redundancy**

Show rec

The **show rec** command displays the count of all metadata objects in sessions managed by the recording agent. These statistics include metadata monitored over an active period of time and over a lifetime period (where “lifetime” totals reflect from the last reboot of the Net-Net SD to the present time). The following example shows the use of this command.

1. Log into the Net-Net SD as a User or Superuser.

   ```
   ACMEPACKET> enable
   ACMEPACKET(enable)#
   ```

2. Type **show rec** and press <Enter> to display the recording metadata statistics. The following output is an example of the “show rec ” command.

   ```
   ACMEPACKET(enable)# show rec
   ```

<u>“Show rec” output</u>

```
13:49:44-81645
Recording Agent Status        -- Period -- -------- Lifetime ----
----
                Active    High   Total      Total  PerMax    High
Rec Sessions         0       1       1          1       1       1
Comm Groups          0       0       0          0       0       0
Comm Sessions        0       1       1          1       1       1
Media Streams        0       2       2          2       2       2
Participants         0       2       2          2       2       2
```

The following table describes the metadata objects in the “show rec ” command output.

Object	Description
Rec Sessions	Number of recording sessions during an active period of time and over a lifetime period.
Comm Groups	Number of active communication session recording groups during an active period of time and over a lifetime period.
Comm Sessions	Number of active communication sessions during an active period of time and over a lifetime period.
Media Streams	Number of active media streams during an active period of time and over a lifetime period.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period.

Show rec redundancy

The **show rec redundancy** command displays information for session recording server statistics when the Net-Net SD is configured for HA. These statistics include metadata monitored over an active period of time and over a lifetime period (where “lifetime” totals reflect from the last reboot of the Net-Net SD to the present time) on both the primary and redundant Net-Net SD. The following example shows the use of this command.

1. Log into the Net-Net SD as a User or Superuser.

   ```
   ACMEPACKET> enable
   ACMEPACKET(enable)#
   ```

2. Type **show rec redundancy** and press <Enter> to display the session recording server statistics for Net-Net SDs in HA mode. The following output is an example of the “show rec redundancy” command.

   ```
   ACMEPACKET(enable)# show rec redundancy
   ```

Show rec redundancy output

Primary System

```
13:49:44-81645

Recording Agent Status        -- Period -- -------- Lifetime ----
----

                Active    High   Total      Total  PerMax    High

Rec Sessions         0       1       1          1       1       1

Comm Groups          0       0       0          0       0       0

Comm Sessions        0       1       1          1       1       1

Media Streams        0       2       2          2       2       2

Participants         0       2       2          2       2       2
```

Redundant System

```
13:49:44-81646

Recording Agent Status        -- Period -- -------- Lifetime ----
----

                Active    High   Total      Total  PerMax    High

Rec Sessions         0       1       1          1       1       1

Comm Groups          0       0       0          0       0       0

Comm Sessions        0       1       1          1       1       1

Media Streams        0       2       2          2       2       2

Participants         0       2       2          2       2       2
```

The following table describes the session recording server statistics in the **show rec redundancy** command output.

Object	Description
Rec Sessions	Number of recording sessions during an active period of time and over a lifetime period.
Comm Groups	Number of active communication session recording groups during an active period of time and over a lifetime period.
Comm Sessions	Number of active communication sessions during an active period of time and over a lifetime period.
Media Streams	Number of active media streams during an active period of time and over a lifetime period.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period.

Codec Negotiation

In a SIPREC environment, it is assumed that the recording ecosystem provides transcoding media servers for which media calls can be redirected to, relieving the issue of codec matching from the recording servers. However, if transcoding media servers are not provided, the responsibility for transcoding falls on the recording server or the recording client in a SIPREC environment. The Net-Net SD/SRC is required to impose some policy decisions on the codec negotiation between the three, or more, end-points. Specifically, the codec negotiation between the two participants and the recording server is subject to additional policy actions.

The SDP answer from the SRS may not agree with the media flows established in the communication session between UA-A and UA-B. If UA-A and UA-B agree to use G729, yet the SRS's answer indicates no support for G729, the SRS is then unable to interpret the media streams. The SDP offer forwarded to the called party (in this case UA-B) limits the codec choices to those supported by the SRS.

> **Note:** The recording agent forwards the original codec offer to the SRS prior to sending the invite to the UA-B. The SRS responds with the SDP answer, indicating the codec list most desirable to the SRS. The codec list in the answer is then forwarded to UA-B. This allows three parties in a conference call to participate in the negotiation of the codecs among the supported formats only.

SIPREC Call Flows

This section provides examples of call flow scenarios that can occur in a SIPREC environment. SIP recording call flow examples include:

For Selective Recording:

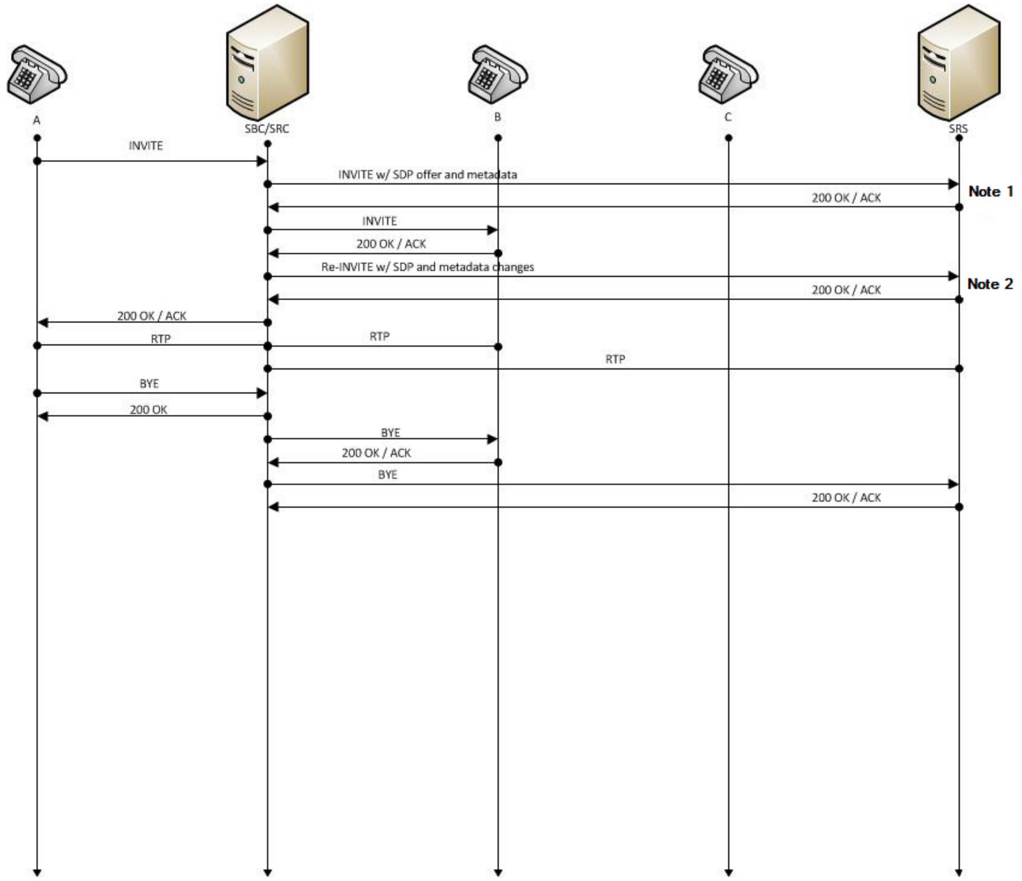
- Normal Call (recording required)
- Normal Call (recording not required)
- Early Media Call (recording not required)
- REFER Pass-Through Call (REFER handled by User Agent)
- REFER Call (REFER handled by Net-Net SD)
- SRS Indicates Busy in Call (recording not required)

Note: REFER is a SIP method indicating that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the request.

Selective Recording

Normal Call (recording required)

The following illustration shows a normal call using selective recording with recording required. For SDP and Metadata information in Notes 1 and 2 , see Sample SDP and Metadata (51).



SIP INVITE, “recording required”, selective recording

I

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE with SDP and metadata to SRS.

e SRS responds with OK to Net-Net SD.

r Net-Net SD sends INVITE to UA-B.

t UA-B responds with OK to Net-Net SD.

y Net-Net SD sends re-INVITE with SDP and metadata changes to SRS.

u SRS responds with OK to Net-Net SD.

i Net-Net SD forwards OK response to UA-A.

o RTP stream initiated between UA-A and Net-Net SD.

a RTP stream initiated between Net-Net SD and UA-B.

s RTP stream initiated between Net-Net SD and SRS.

d UA-A sends BYE to Net-Net SD.

f Net-Net SD responds with OK to UA-A.

g Net-Net SD sends BYE to Net-Net SD.

h Net-Net SD responds with OK to UA-A.

j Net-Net SD sends BYE to UA-B.

k UA-B responds with OK to Net-Net SD.

l Net-Net SD sends BYE to SRS.

; SRS responds with OK to Net-Net SD.

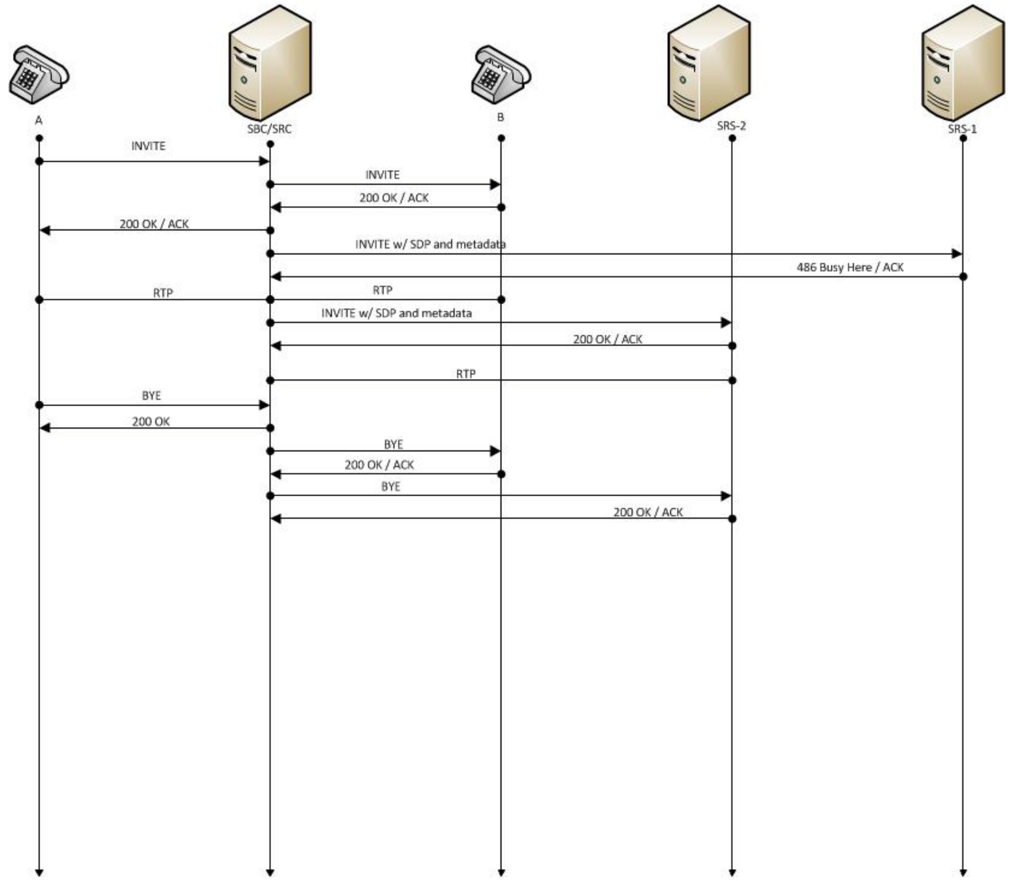
Sample SDP and Metadata

The following sample SDP and Metadata pertain to Notes 1 and 2 in the previous Call Flow diagram.

```
--[Note 1]------------------------------
Content-Type: application/sdp
v=0
o=- 171 213 IN IP4 10.0.0.2
s=-
c=IN IP4 10.0.0.1
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=label:1

Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session
<?xml version='1.0' encoding='UTF-8'?>
<recording xmlns='urn:ietf:params:xml:ns:recording'>
        <dataMode>complete</dataMode>
        <session id="urn:uuid:79b2fcd8-5c7f-455c-783f-db334e5d57d0">
                <start-time>2011-06-27T17:03:57</start-time>
        </session>
        <participant id="urn:uuid:10ac9063-76b7-40bb-4587-08ba290d7327" session="urn:uuid:79b2fcd8-
5c7f-455c-783f-db334e5d57d0">
                <aor>sip:sipp@168.192.24.40</aor>
                <name>sipp </name>
                <send>urn:uuid:07868c77-ef8e-4d6f-6dd5-a02ff53a1329</send>
                <start-time>2011-06-27T17:03:57</start-time>
        </participant>
        <participant id="urn:uuid:797c45f5-e765-4b12-52b0-d9be31138529" session="urn:uuid:79b2fcd8-
5c7f-455c-783f-db334e5d57d0">
                <aor>sip:service@168.192.24.60</aor>
                <name>sut </name>
        </participant>
        <stream id="urn:uuid:4a72a1ed-abb2-4d7c-5f4d-6d4c36e2d4ec" session="urn:uuid:79b2fcd8-5c7f-
455c-783f-db334e5d57d0">
                <mode>separate</mode>
                <start-time>2011-06-27T17:03:57</start-time>
<label>1</label>
        </stream>
</recording>


--[Note 2]------------------------------
Content-Type: application/sdp
v=0
o=- 171 213 IN IP4 10.0.0.2
s=-
c=IN IP4 10.0.0.1
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=label:1
m=audio 6002 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=label:2

Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session
<?xml version='1.0' encoding='UTF-8'?>
<recording xmlns='urn:ietf:params:xml:ns:recording'>
        <dataMode>partial</dataMode>
        <session id="urn:uuid:79b2fcd8-5c7f-455c-783f-db334e5d57d0">
                <start-time>2011-06-27T17:03:57</start-time>
        </session>
        <participant id="urn:uuid:797c45f5-e765-4b12-52b0-d9be31138529" session="urn:uuid:79b2fcd8-
5c7f-455c-783f-db334e5d57d0">
                <aor>sip:service@168.192.24.60</aor>
                <name>sut </name>
                <send>urn:uuid:4a72a1ed-abb2-4d7c-5f4d-6d4c36e2d4ec</send>
                <start-time>2011-06-27T17:03:58</start-time>
        </participant>
        <stream id="urn:uuid:07868c77-ef8e-4d6f-6dd5-a02ff53a1329" session="urn:uuid:79b2fcd8-5c7f-
455c-783f-db334e5d57d0">
                <mode>separate</mode>
                <start-time>2011-06-27T17:03:58</start-time>
<label>2</label>
        </stream>
</recording>
```

Normal Call (recording not required)

The following illustration shows a normal call using selective recording with recording optional.



SIP INVITE, “recording not required”

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE to UA-B.

e UA-B responds with OK to Net-Net SD.

r Net-Net SD forwards OK response to UA-A.

t Net-Net SD sends INVITE with SDP and metadata to SRS.

y SRS responds with OK to Net-Net SD.

u RTP stream initiated between UA-A, Net-Net SD, and UA-B.

i RTP stream initiated between Net-Net SD and SRS.

o UA-A sends BYE to Net-Net SD.

a Net-Net SD responds with OK to UA-A.

s Net-Net SD sends BYE to UA-B.

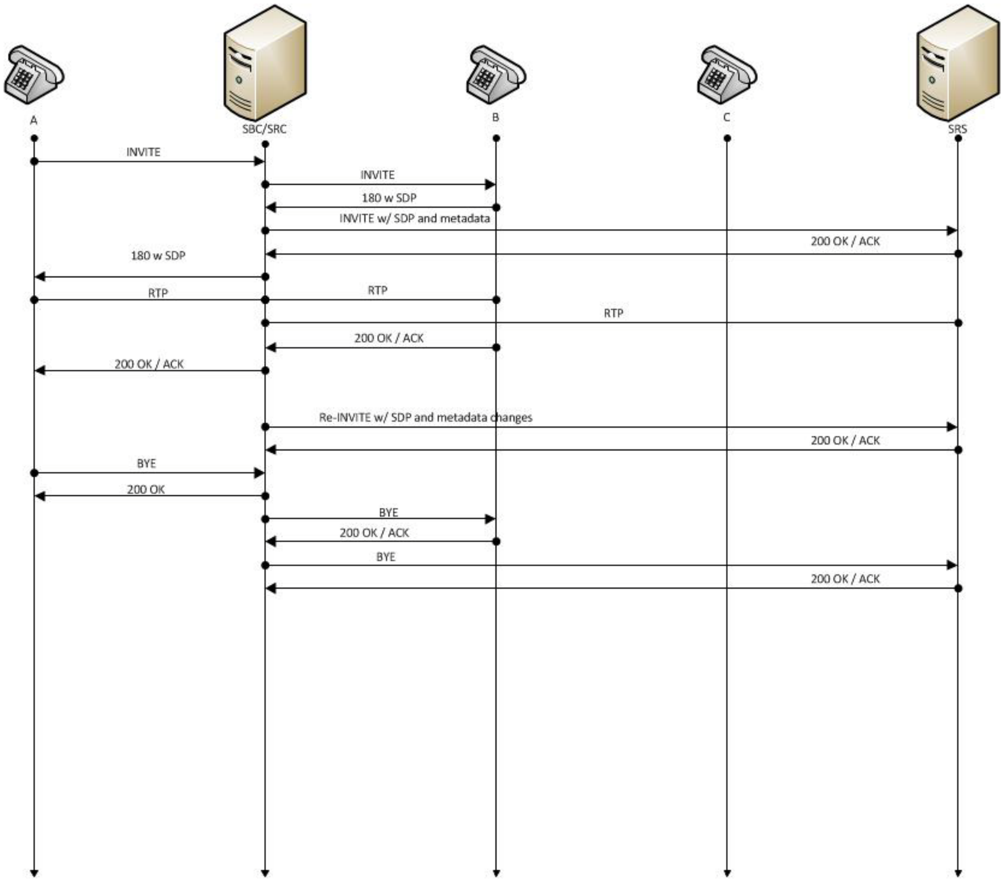
d UA-B responds with OK to Net-Net SD.

f Net-Net SD sends BYE to SRS.

g SRS responds with OK to Net-Net SD.

Early Media Call (recording not required)

The following illustration shows an early media call using selective recording with recording optional.



SIP INVITE, early media , “recording not required”, selective recording

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE to UA-B.

e UA-B sends 180 and SDP to Net-Net SD.

r Net-Net SD sends INVITE with SDP and metadata to SRS.

t SRS responds with OK to Net-Net SD.

y Net-Net SD sends 180 with SDP to UA-A.

u RTP stream initiated between Net-Net SD and UA-A.

i RTP stream initiated between Net-Net SD and UA-B.

o RTP stream initiated between Net-Net SD and SRS.

a UA-B responds with OK to Net-Net SD.

s Net-Net SD forwards OK to UA-A.

d Net-Net SD sends re-INVITE with SDP and metadata changes to SRS.

f SRS responds with OK to Net-Net SD.

g UA-A sends BYE to Net-Net SD.

h Net-Net SD responds with OK to UA-A.

j Net-Net SD sends BYE to UA-B.

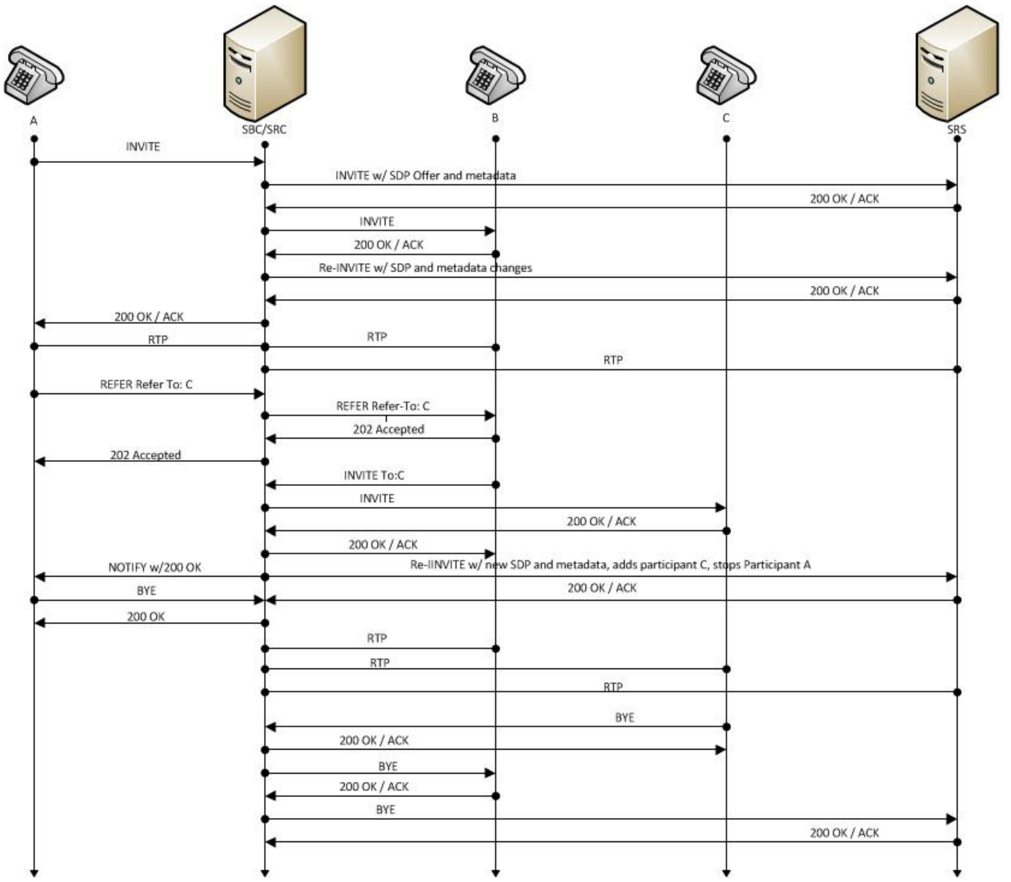
k UA-B responds with OK to Net-Net SD.

l Net-Net SD sends BYE to SRS.

; SRS responds with OK to Net-Net SD.

REFER Pass-Through Call (REFER handled by User Agent)

The following illustration shows a REFER pass-through call using selective recording and the User Agent (UA) handling the REFER on the call. Recording is required in this call flow.



SIP REFER, UA handles REFER, “recording required”, selective recording

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE with SDP Offer and metadata to SRS.

e SRS responds with OK to Net-Net SD.

r Net-Net SD sends INVITE to UA-B.

t UA-B responds with OK to Net-Net SD.

y Net-Net SD sends re-INVITE with SDP and metadata changes to SRS.

u SRS responds with OK to Net-Net SD.

i Net-Net SD forwards OK response to UA-A.

l UA-C responds with OK to Net-Net SD.

; Net-Net SD forwards OK response to UA-B.

⑳ Net-Net SD sends NOTIFY with OK reponse to UA-A.

㉑ Net-Net SD sends re-INVITE to SRS with new SDP and metadata, adds participant C, stops participant A .

㉒ SRS responds with OK to Net-Net SD.

㉓ UA-A sends BYE to Net-Net SD.

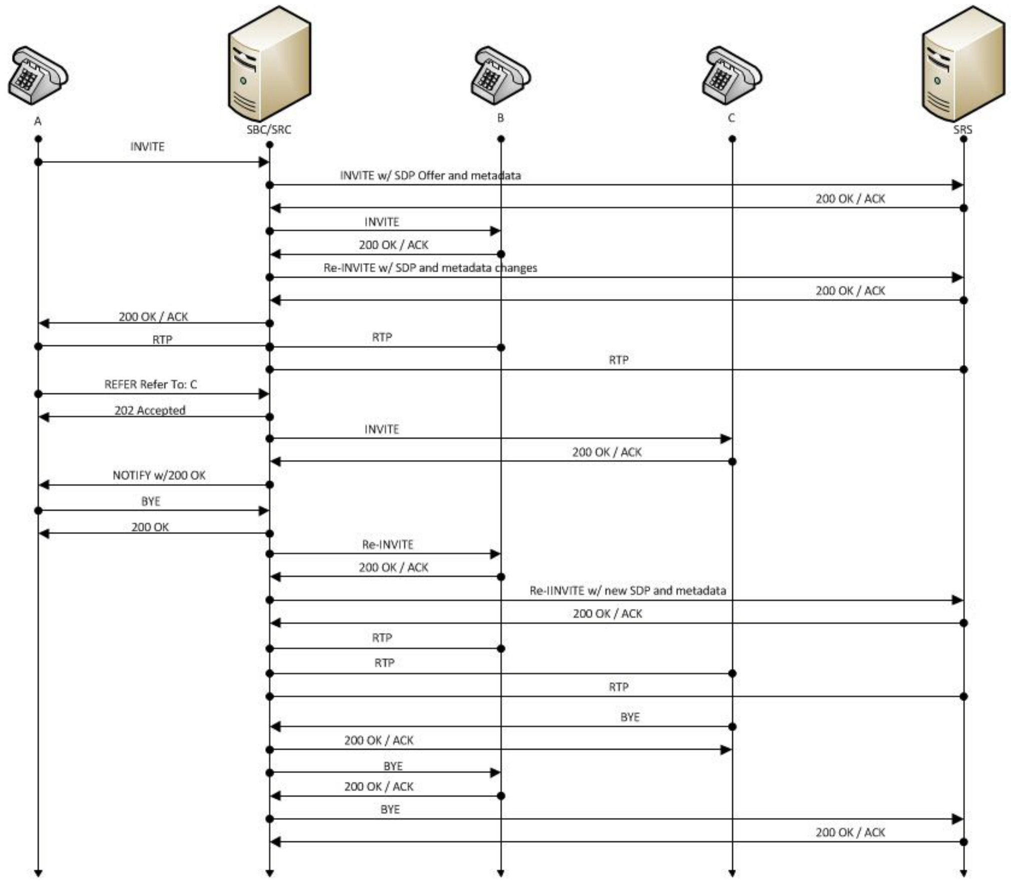
㉔ Net-Net SD responds with OK to UA-A.

㉕ Net-Net SD responds with OK to UA-A.

Call Flow Description	
o RTP stream initiated between UA-A and Net-Net SD.	㉖ RTP stream initiated between Net-Net SD and UA-B.
a RTP stream initiated between Net-Net SD and UA-B.	㉗ RTP stream initiated between Net-Net SD and UA-C.
s RTP stream initiated between Net-Net SD and SRS.	㉘ RTP stream initiated between Net-Net SD and SRS.
d UA-A sends REFER-TO: C to Net-Net SD.	㉙ UA-C sends BYE to Net-Net SD.
f Net-Net SD forwards REFER-TO: C to UA-B.	㉚ Net-Net SD responds with OK to UA-C.
g UA-B responds with 202 ACCEPTED to Net-Net SD.	㉛ Net-Net SD sends BYE to UA-B.
h Net-Net SD forwards 202 ACCEPTED to UA-A.	㉜ UA-B responds with OK to Net-Net SD.
j UA-B sends INVITE TO: C to Net-Net SD.	㉝ Net-Net SD sends BYE to SRS
k Net-Net SD sends INVITE to UA-C.	㉞ SRS responds with OK to Net-Net SD.

REFER Call (REFER handled by Net-Net SD)

The following illustration shows a call using selective recording and the Session Border Controller (Net-Net SD) handling the REFER on the call. Recording is required in this call flow.



SIP REFER, SBC absorbs REFER, “recording required”, selective recording

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE with SDP Offer and metadata to SRS.

e SRS responds with OK to Net-Net SD.

r Net-Net SD sends INVITE to UA-B.

t UA-B responds with OK to Net-Net SD.

y Net-Net SD sends re-INVITE with SDP and metadata changes to SRS.

u SRS responds with OK to Net-Net SD.

i Net-Net SD forwards OK response to UA-A.

j Net-Net SD sends NOTIFY with OK response to UA-A.

k UA-A sends BYE to Net-Net SD.

l Net-Net SD responds with OK to UA-A.

; Net-Net SD sends re-INVITE to UA-B.

⑳ UA-B responds with OK to Net-Net SD.

㉑ Net-Net SD sends re-INVITE to SRS with new SDP and metadata.

㉒ SRS responds with OK to Net-Net SD.

㉓ RTP stream initiated between Net-Net SD and UA-B.

Call Flow Description

o RTP stream initiated between UA-A and Net-Net SD.

a RTP stream initiated between Net-Net SD and UA-B.

s RTP stream initiated between Net-Net SD and SRS.

d UA-A sends REFER-TO: C to Net-Net SD.

f Net-Net SDNet-Net SD responds with 202 ACCEPTED to UA-A.

g Net-Net SD sends INVITE to UA-C.

h UA-C responds with OK to Net-Net SD.

㉔ RTP stream initiated between Net-Net SD and UA-C.

㉕ RTP stream initiated between Net-Net SD and SRS.

㉖ UA-C sends BYE to Net-Net SD.

㉗ Net-Net SD responds with OK to UA-C.

㉘ Net-Net SD sends BYE to UA-B.

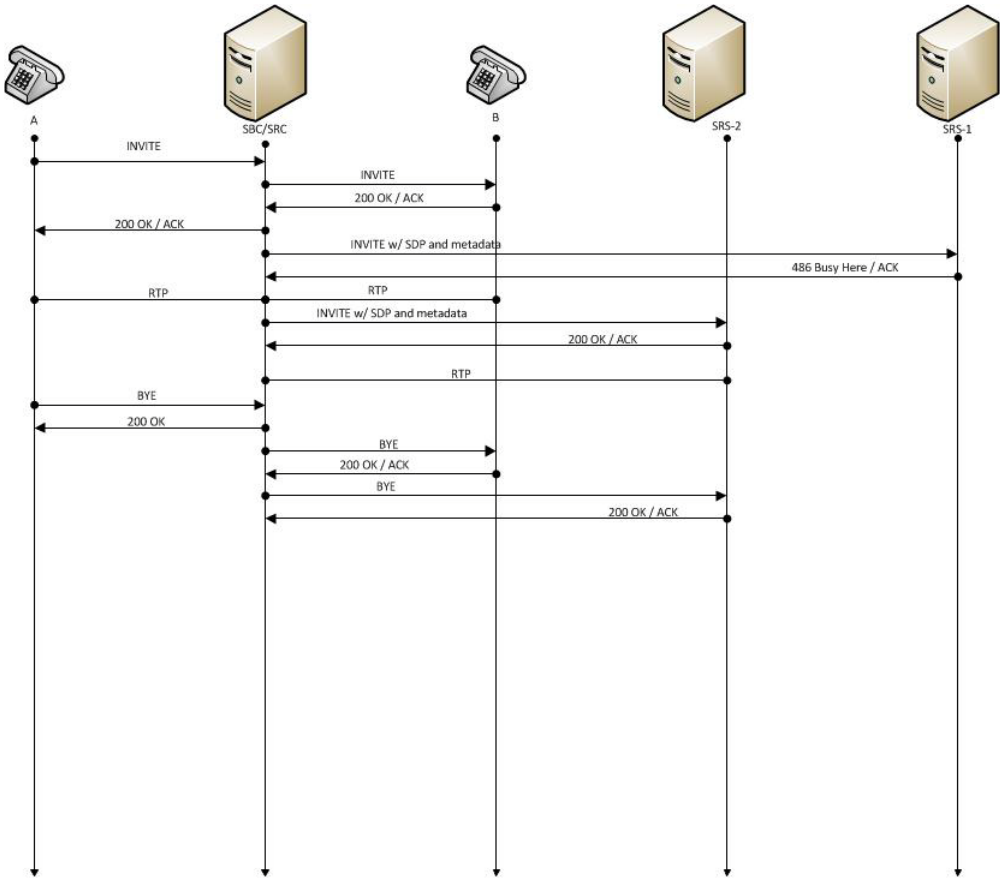
㉙ UA-B responds with OK to Net-Net SD.

㉚ Net-Net SD sends BYE to SRS.

㉛ SRS responds with OK to Net-Net SD.

SRS Indicates Busy in Call (recording not required)

The following illustration shows the Session Recording Server (SRS) is BUSY for a call session. Recording is not required in this call flow.



SIP INVITE, “recording not required”

Call Flow Description

q UA-A sends INVITE to Net-Net SD.

w Net-Net SD forwards INVITE to UA-B.

e UA-B responds with OK to Net-Net SD.

r Net-Net SD forwards OK response to UA-A.

t Net-Net SD sends INVITE to SRS1 with SDP and metadata.

y SRS1 responds to Net-Net SD with 436 BUSY HERE.

u RTP stream initiated between UA-A and Net-Net SD.

i RTP stream initiated between Net-Net SD and UA-B.

o Net-Net SD sends INVITE to SRS2 with SDP and metadata.

a SRS2 responds with OK to Net-Net SD.

s RTP stream initiated between Net-Net SD and SRS2.

d UA-A sends BYE to Net-Net SD.

f Net-Net SD responds with OK to UA-A.

g Net-Net SD sends BYE to UA-B.

h UA-B responds with OK to Net-Net SD.

j Net-Net SD sends BYE to SRS2.

k SRS2 responds with OK to Net-Net SD.

4 Communications Monitoring Probe

Palladion Mediation Engine

Palladion is Oracle’s *Communication Experience Manager*.

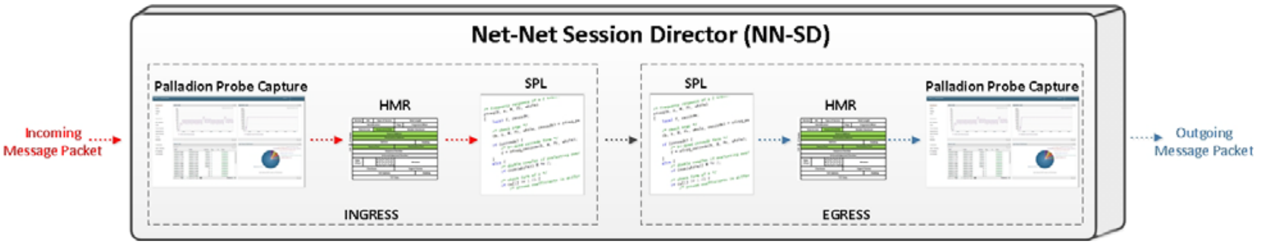
The manager is powered by the Palladion Mediation Engine, a platform that collects SIP, DNS, ENUM, and protocol message traffic received from Palladion Probes. The mediation engine stores the traffic in an internal database, and analyzes aggregated data to provide comprehensive multi-level monitoring, troubleshooting, and interoperability information.

Release S-C[xz]6.3.9 supports an embedded, user-configurable Palladion Communications Monitoring Probe, Version 1. Acting as a Probe, or as an exporter, the Net-Net ESD can:

1. Establish an authenticated, persistent, reliable TCP connection between itself and one or more Palladion Mediation Engines.
2. Optionally ensure message privacy by encrypting the TCP connection using TLS.
3. Use the TCP connection to send a UTC-timestamped, unencrypted copy of a protocol message to the Palladion Engine(s).
4. Accompany the copied message with related data to include: the port/vlan on which the message was sent/received, local and remote IP:port information, and the transport layer protocol.

   Note: The Palladion Communications Monitor Probe communicates over the media interface for signaling and Quality of Service (QoS) statistics using IPFIX. QoS reporting is done via Call Detail Records (CDR) (accounting).

The following illustration shows how the Palladion Communications Monitor Probe handles incoming and outgoing monitored data on the Net-Net ESD.



HMR - Header Manipulation Rules
SPL - Session Plug-in Language
SM&T - SIP Monitor and Trace

Communications Monitor Configuration

Communications Monitor configuration consists of the following steps.

1. Configuration of one or more Net-Net ESD/Palladion exporter/collector pairs.

   Configuration of the *-config* object, which defines common operations across all interfaces, is not required. Default values can be retained to enable standard service.

2. Optional assignment of a TLS profile to an exporter/collector pair.

   Note: The Palladion Communications Monitor Probe communicates over the media interface for signaling and Quality of Service (QoS) statistics using IPFIX. QoS reporting is done via Call Detail Records (CDR) (accounting).

Communication Monitor Probe

Use the following procedure to configure a communication monitoring probe.

1. From superuser mode, use the following ACLI sequence to access *comm-monitor* configuration mode. From *comm-monitor* mode, you establish a connection between the Net-Net OS SD, acting as a exporter of protocol message traffic and related data, and a Palladion Mediation Engine, acting as an information collector.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)# system
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)# comm-monitor
   ACMEPACKET(comm-monitor)#
   ```

2. Use the **state** parameter to enable or disable communication monitoring.

   Communication monitoring is disabled by default.

   ```
   ACMEPACKET(comm-monitor)# state enabled
   ACMEPACKET(comm-monitor)#
   ```

3. Use the **sbc-group-id** parameter to assign an integer value to the Net-Net SD, in its role as an information exporter.

   Retain the default value (0) or assign another integer value.

   ```
   ACMEPACKET(comm-monitor)# sbc-group-id 5
   ACMEPACKET(comm-monitor)#
   ```

4. Use the **network-interface** parameter to identify the network interface whose traffic will be exported to the Palladion Mediation Engine.

   To specify a media interface (the usual case):

   ```
   ACMEPACKET(comm-monitor)# network-interface m01
   ACMEPACKET(comm-monitor)#
   ```

   To specify the *wancom0* management interface (supported, but not generally used):

   ```
   ACMEPACKET(comm-monitor)# network-interface wancom0:0
   ACMEPACKET(comm-monitor)#
   ```

5. If the network interface specified in Step 4 is a media interface, you can optionally use TLS to encrypt the exported traffic and related data.

   To enable TLS encryption, use the **tls-profile** parameter to identify a TLS profile to be assigned to the network interface. The absence of an assigned TLS profile (the default state) results in unencrypted transmission.

   Refer to TLS Profile Configuration for configuration details.

   ```
   ACMEPACKET(comm-monitor)# tls-profile commMonitor
   ACMEPACKET(comm-monitor)#
   ```

6. Use the **qos-enable** parameter to enable or disable to export of RTP, SRTP, and QOS data flow information.

   ```
   ACMEPACKET(comm-monitor)# qos-enable enabled
   ACMEPACKET(comm-monitor)#
   ```

7. Use the **monitor-collector** parameter to move to *monitor-collector* configuration mode.

   While in this mode you identify a Palladion Mediation Engine (a receiver of exported data) by IP address and port number.

   ```
   ACMEPACKET(comm-monitor)# monitor-collector
   ACMEPACKET(monitor-collector)#
   ```

8. Use the **address** and **port** parameters to specify the IP address and port number monitored by a Palladion Mediation Engine for incoming Internet Protocol Flow Information Export (IPFIX) traffic.

   Enter an IPv4 address and a port number with the range **1025** through **65535**, with a default value of **4739**.

   ```
   ACMEPACKET(monitor-collector)# address 172.30.101.239
   ACMEPACKET(monitor-collector)# port 4729
   ACMEPACKET(monitor-collector)#
   ```

9. Use **done** and **exit** to return to *comm-monitor* configuration mode.

10. Use **done**, **exit**, and **verify-config** to complete configuration.

11. Repeat Steps 1 through 10 to configure additional as required.

TLS Profile Configuration

Use the following procedure to configure a *tls-profile* that identifies the cryptographic resources, specifically certificates and protocols, required for the establishment of a secure/encrypted connection between the Net-Net OS SD and the Palladion Mediation Engine.

1. From superuser mode, use the following command sequence to access *tls-profile* configuration mode.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)# security
   ACMEPACKET(security)# tls-profile
   ACMEPACKET(tls-profile)#
   ```

2. Use the **name** parameter to provide a unique identifier for this *tls-profile*.

   ```
   ACMEPACKET(tls-profile)# name commMonitor
   ACMEPACKET(tls-profile)#
   ```

3. Use the required **end-entity-certificate** parameter to specify the name of the *certificate-record* configuration that identifies the credential (specifically, an X509.v3 certificate) offered by the Net-Net SD in support of its asserted identity.

```
ACMEPACKET(tls-profile)# end-entity-certificate commMonitor509
ACMEPACKET(tls-profile)#
```

4. Use the required **trusted-ca-certificates** parameter to compile a list or one or more *certificate-record* configuration elements referencing trusted Certification Authority (CA) certificates used to authenticate the offered certificate. These referenced certificates are conveyed to the Palladion Mediation Engine as part of the TLS exchange.

   Provide a comma separated list of existing CA **certificate-record** configuration elements.

```
ACMEPACKET(tls-profile)# trusted-ca-certificates
verisignClass3-a,verisignClass3-b,baltimore,thawtePremium,acme-CA
ACMEPACKET(tls-profile)#
```

5. Retain the default value, **all**, for the **cipher-list** parameter.

6. Use the **verify-depth** parameter to specify the maximum number of chained certificates that will be processed while authenticating end-entity certificate received from the Palladion Mediation Engine.

   Provide an integer within the range 1 through 10 (the default).

   The Net-Net SD supports the processing of certificate chains (consisting of an end-entity certificate and some number of CA certificates) when X.509v3 certificate-based authentication is used. The following process validates a received TLS certificate chain.

   a. Check the validity dates (*Not Before* and *Not After* fields) of the end certificate. If either date is invalid, authentication fails; otherwise, continue chain validation

   b. Check the maximum length of the certificate chain (specified by **verify-depth**). If the current chain exceeds this value, authentication fails; otherwise, continue chain validation.

   c. Verify that the *Issuer* field of the current certificate is identical to the *Subject* field of the next certificate in the chain. If values are not identical, authentication fails; otherwise, continue chain validation.

   d. Check the validity dates (*Not Before* and *Not After* fields*)* of the next certificate. If either date is invalid, authentication fails; otherwise, continue chain validation.

   e. Check the *X509v3 Extensions* field to verify that the current certificate identifies a CA. If not so, authentication fails; otherwise, continue chain validation.

   f. Extract the *Public Key* from the current CA certificate. Use it to decode the *Signature* field of the prior certificate in the chain. The decoded *Signature* field yields an MD5 hash value for the contents of that certificate (minus the *Signature* field).

   g. Compute the same MD5 hash. If the results are not identical, authentication fails; otherwise, continue chain validation.

h. If the hashes are identical, determine if the CA identified by the current certificate is a trust anchor by referring to the *trusted-ca-certificates* attribute of the associated TLS-profile configuration object. If the CA is trusted, authentication succeeds. If not, return to Step 2.

```
ACMEPACKET(tls-profile)# verify-depth 8
ACMEPACKET(tls-profile)#
```

7. Use the **mutual-authenticate** parameter to **enable** or **disable** (the default) mutual authentication.

   Protocol requirements mandate that the server present its certificate to the client application. Optionally, the server can implement mutual authentication by requesting a certificate from the client application, and authenticating the certificate offered by the client.

   Upon receiving a server certificate request, the client application must respond with a certificate; failure to do so results in authentication failure.

```
ACMEPACKET(tls-profile)# mutual-authenticate disabled
ACMEPACKET(tls-profile)#
```

8. Retain the default value, **compatibility**, for the **tls-version** parameter.
9. Retain default values for all other parameters.
10. Use **done**, **exit**, and **verify-config** to complete *tls-profile* configuration.
11. Repeat Steps 1 through 10 to configure additional *tls-profiles* as required.

Palladion Probe Enhancement

Performance enhancements were made to the Palladion Probe functionality in Release S-C(xz)6.3.9M1. This enhancement simplifies the operation of software-based Palladion probes by enabling the transmission of IPFIX data to one or more Palladion Mediation Engines, possibly on different sub-nets. This enhancement requires a slight change in the ACLI hierarchy -- specifically, the removal of the network-interface parameter from the comm-monitor configuration object, and its transfer to the monitor-collector configuration object.

Consequently, users who are migrating from a previous S-C[xz]6.3.9 release to S-C[xz]6.3.9M1 must be aware of the following anomaly. After the upgrade, probes based/anchored on media interfaces revert to the default network-interface value of wancom0:0.

The following illustrates a pre-S-C(xz)6.3.9M1 configuration.

```
comm-monitor
      state                    enabled
      qos-enable               disabled
      sbc-grp-id               0
      tls-profile
      network-interface        M10:0

      monitor-collector
             address           172.16.29.102
             port              4739
```

The following illustrates the upgraded S-C[xz]6.3.9M1 configuration.

```
comm-monitor
      state                    enabled
      qos-enable               disabled
      sbc-grp-id               0
      tls-profile

      monitor-collector
             address           172.16.29.102
             port              4739
             network-interface  wancom0:0
```

Note: Restoration of prior service requires a simple workaround, namely, the update of the network-interface parameter to its original value of M10:0.

5 Configuring Monitoring Filters

Introduction

The SIP monitoring and tracing feature provides the ability to set filters on the Net-Net SBC for filtering SIP session data, and displaying the results in a Web-based graphical user interface (GUI). You can use the data for the purpose of troubleshooting your Net-Net SBC(s).

This section provides information about how SIP monitoring and tracing works, configuring filters for filtering SIP session data, and how you can view/analyze monitored SIP session information via the Web-based GUI.

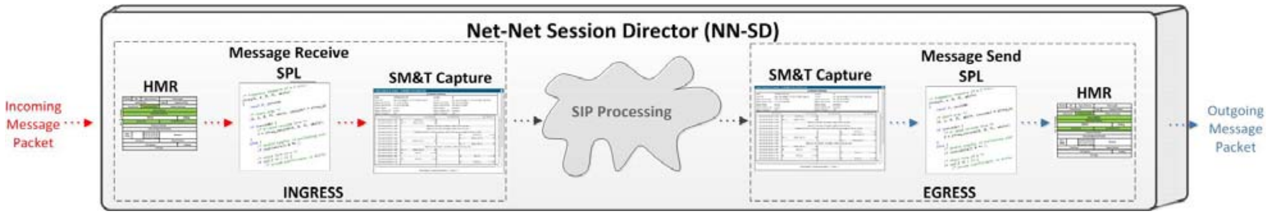
Topics include:

- How it Works (65)
- Filters to Configure (67)
- Creating Custom Filters (68)
- Dynamic Filters (81)

How it Works

The SIP Monitor and Trace feature allows SIP sessions on the NN-SD(s) in your network to be monitored. When the Net-Net SD receives an incoming message packet, it applies the configured Header Manipulation Rules (HMR), applies the message-receive Session Plug-in Language (SPL), and then captures the data from the message and displays it in the SIP Monitor and Trace application. The Net-Net SD then processes the SIP information it received, and sends it out from the SIP Monitor and Trace application, applies the message-send SPL, and then applies HMR before sending the message out from the Net-Net SD.

Refer to the illustration below for the message in/message out process for SIP Monitor and Trace.



You configure the monitoring process to use filters to filter the active session data from original ingress or final egress SIP session messages. These filters are based on Oracle's Command Line Interface (ACLI)-configured filters matching criteria or dynamic events that occur, and are used for the purpose of troubleshooting SIP sessions on the network.

As a system monitors active sessions, it captures data using the following filters:

- **Static filters** - Configured filters that filter the data on ingress and egress requests and responses in the SIP session dialogs.

  You configure these filters via the ACLI as part of the Net-Net SBC configuration. The configured filters save to the current configuration (after saving and activating the configuration).

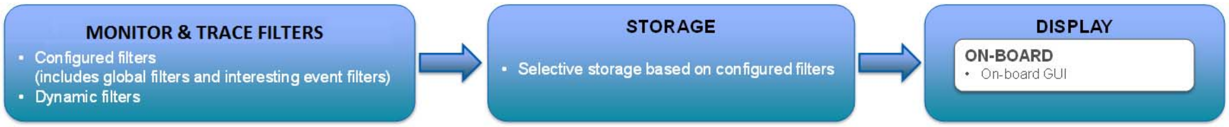
- **Dynamic filters -** Filters you specify that match information in the ingress/egress SIP messages according to the filters you dynamically specified.

  You use the ACLI to specify these filters, but there is no change to the current configuration. The filters take effect immediately, and do not require the use of the “Save” and “Activate” commands. Using dynamic filters is recommended if you want to set specific filters but make no changes to the current configuration.

  For more information about configuring static filters and dynamic filters, see Filters to Configure (67) and Dynamic Filters (81)

When a filter configuration is enabled, the system matches the values in the configured filters to the headers of messages before it applies any changes. If no match is found in the headers during monitoring, the system uses the filter defaults in the system configuration to perform the filtering. The system logs the filter results along with any additional call details and displays the results in the Web-based GUI.

The following illustration shows the SIP monitoring and tracing flow process.


MONITOR & TRACE FILTERS
• Configured filters
(includes global filters and interesting event filters)
• Dynamic filters
STORAGE
• Selective storage based on configured filters
DISPLAY
ON-BOARD
• On-board GUI

The SIP Monitor and Trace function can store up to 100 messages per session and it can store up to 2000 cumulative sessions across all report types. Once the 2000 sessions maximum is reached, the system removes the oldest call and adds the newest call. The call database is not persistent across reboots.

Filters to Configure

This section provides information about enabling the use of SIP monitoring and tracing filters you can configure on the Net-Net SBC. It includes a description and examples of the filter objects and attributes you can set to monitor specific SIP session data on the Net-Net SBC.

Filter Objects

The Net-Net SBC provides filter objects you can configure on the Net-Net SBC for enabling/disabling filtering, and for creating customized filters for SIP Monitoring and Tracing. When filtering is enabled, the system can monitor and filter specific SIP session data and display it to the Web-based GUI. The filter objects you can configure include:

Filters	Description
Filters	**Description**
filter-config	Object that allows you to create custom filters to use for SIP monitoring and tracing. You can then configure session agents (SA) and/or realms to use these filters, or set sip-monitoring to use the filters on a global basis. For more information, see .
sip-monitoring	Object that allows you to configure SIP monitoring and tracing features. **Note**: You must configure the sip-monitoring object to enable filtering. A session agent and/or realm must also be configured, or you must set filtering on a global basis, for monitoring and tracing to occur.
state	Attribute that enables/disables SIP monitoring and tracing. For more information, see .
monitoring-filters	Attribute that allows you to specify the name of the custom filter(s) to use on a global basis. This value is based on the filter(s) created in “filter-config”. You can also specify an “*” (asterisk) as a value for this attribute, which monitors all session data on the Net-Net SBC. For more information, see Using Filters to Monitor on a Global-Basis (72).
interesting-events	Object that allows you to configure the following attributes: • **type** - Sets the interesting events to monitor (short-session, local-rejection) • **trigger-threshold** - Sets the number of interesting events that must occur within the time set by the “trigger-window” value. If the number of events reaches the trigger-threshold during the trigger-window time, monitoring is started. • **trigger-timeout** - Sets the amount of time, in seconds, that the trigger is active once monitoring has started. If no interesting events occur in the time frame set for this value, monitoring never starts. For example, if trigger-timeout is set to 40, and no interesting events occur in 40 seconds, then monitoring never starts. **Note**: Interesting Events are always enabled on a global-basis on the Net-Net SBC. For more information, see Configuring Interesting Events (76).

The following paragraphs provide information and procedures for configuring these features.

Creating Custom Filters

You can create single or multiple custom, session filters on the Net-Net SBC for monitoring and tracing purposes. These filters allow incoming and outgoing session data to be filtered with specific information and then displayed to the Web-based GUI. You can use the custom filter(s) during monitoring on a global basis, or when monitoring session agent (SAs) and/or realms.

You create custom filters using the "**filter-config**" object at the path *Configure terminal->session-router->filter-config* in the ACLI.

The following table identifies the attributes you can configure for each filter.

Filters	Description
filter-config	Object that allows you to create a custom filter(s) to be used for monitoring and tracing on the Net-Net SBC.
name	Name of the custom filter. **Note**: You specify this filter name when configuring global monitoring, SA monitoring, and/or realm monitoring.
address	IP address to be filtered. Depending on the value you specify for this attribute, filtering matches the IP address or IP address and netmask, in the message header. For example: 1.1.1.1 is <IP address> 1.1.1.1/24 is <IP address>/<Netmask>
user	Phone number or user-part to be filtered. Depending on the value you specify for this attribute, filtering matches the phone number string or the user-part with the following header information if it exists in the message: From URI, To URI, Request URI, P-Preferred URI, P-Asserted Identity, P-Associated URI, P-Called Party URI.

You can define a single or multiple filters with specific names and then specify the filter name(s) to use for global monitoring, session agent monitoring, and/or realm monitoring.

Creating a Custom Filter

Use the following procedure to create a custom filter on the Net-Net SBC.

To configure a filter(s):

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **filter-config** and press <Enter> to access the filter configuration-related attributes.

   ```
   ACMEPACKET(session-router)# filter-config
   ACMEPACKET(filter-config)#
   ```

   name—Enter a name to assign to this filter. Valid values are alpha-numeric characters. Default is blank.

   ```
   ACMEPACKET(filter-config)# name FILTER1
   ```

   Note: You can use this filter name when configuring monitoring on a global-basis, or when monitoring session-agents and/or realms.

   address—Enter the IP address to apply to this filter. You can specify netmask if required. IP Address must be entered in dotted decimal format (0.0.0.0). Default is 0.0.0.0.

   ```
   ACMEPACKET(filter-config)# address 1.1.1.1    (filters on IP address)
   ACMEPACKET(filter-config)# address 1.1.1.1/24 (filters on IP address and netmask)
   ```

   user—Enter a phone number or user-part to apply to this filter. Valid values are numeric characters. Default is blank.

   ```
   ACMEPACKET(filter-config)# user 5551212
   ```

   Note: You must specify either the phone number OR user part for the "user" attribute. If you want both the phone number AND user part to be filtered, you must create separate filters to set each value.

4. Enter **done** to save the filter.

   ```
   ACMEPACKET(filter-config)# done
   ```

5. Enter **exit** to exit the filter configuration.

   ```
   ACMEPACKET(filter-config)# exit
   ```

6. Enter **exit** to exit the session-router configuration.

   ```
   ACMEPACKET(session-router)# exit
   ```

7. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

8. Enter **save-config** to save the filter configuration.

   ```
   ACMEPACKET# save-config
   ```

9. Enter **activate-config** to activate the filter configuration.

   ```
   ACMEPACKET# activate-config
   ```

Multiple Custom Filter Examples

The following examples show three custom filters (FILTER1, FILTER2, and FILTER3) created for SIP monitoring and tracing on the Net-Net SBC.

Filter 1

```
ACMEPACKET(filter-config)# name FILTER1
ACMEPACKET(filter-config)# address 1.1.1.1
ACMEPACKET(filter-config)# user 5551212
```

Filter 2

```
ACMEPACKET(filter-config)# name FILTER2
ACMEPACKET(filter-config)# address 3.3.3.3/24
ACMEPACKET(filter-config)# user 1781
```

Filter 3

```
ACMEPACKET(filter-config)# name FILTER3
ACMEPACKET(filter-config)# user sip
```

You can specify the Net-Net SBC monitoring process to use FILTER1, FILTER2, and/or FILTER3 for global monitoring, or for monitoring SAs and/or realms. However, before you apply the custom filters, you can enable/disable SIP monitoring on the Net-Net SBC.

To enable/disable SIP monitoring, see .
To use a custom filter(s) on a global basis, see Using Filters to Monitor on a Global-Basis (72).
To use a custom filter(s) when monitoring SAs, see Using Filters when Monitoring Session Agents (73).
To use a custom filter(s) when monitoring realms, see Using Filters when Monitoring Realms (74).

Enabling/Disabling SIP Monitoring & Tracing

You can enable or disable the Net-Net SBC to perform SIP monitoring using the "**state**" parameter at the path *Configure terminal->session-router->sip-monitoring* in the ACLI.

Use the following procedure to enable/disable SIP monitoring on the Net-Net SBC.

> **Note:** You must enable the sip-monitoring object for monitoring and filtering to occur on the Net-Net SD. With sip-monitoring enabled, you can configure a filter(s) on a global basis, as well as for a session agent and/or a realm. You can also initiate dynamic filter commands.

To enable/disable sip-monitoring:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **sip-monitoring** and press <Enter> to access the SIP monitoring-related attributes.

   ```
   ACMEPACKET(session-router)# sip-monitoring
   ACMEPACKET(sip-monitoring)#
   ```

   state—Enter whether or not to enable the sip monitoring on the Net-Net SBC. Default is "enabled". Valid values are:

   - enabled (default)
   - disabled

4. Enter **done** to save the setting.

   ```
   ACMEPACKET(sip-monitoring)# done
   ```

5. Enter **exit** to exit the sip-monitoring configuration.

   ```
   ACMEPACKET(sip-monitoring)# exit
   ```

6. Enter **exit** to exit the session-router configuration.

   ```
   ACMEPACKET(session-router)# exit
   ```

7. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

8. Enter **save-config** to save the filters.

   ```
   ACMEPACKET# save-config
   ```

9. Enter **activate-config** to activate the filters in the current configuration.

   ```
   ACMEPACKET# activate-config
   ```

10. Configure global filters, or assign filters to a session agent and/or realm. For more information, see the following:

    - Using Filters to Monitor on a Global-Basis (72)
    - Using Filters when Monitoring Session Agents (73)
    - Using Filters when Monitoring Realms (74)

    With sip-monitoring enabled, you can also initiate dynamic filter commands if required. For more information about dynamic filter commands, see Dynamic Filters (81).

    .

Using Filters to Monitor on a Global-Basis

The Net-Net SBC allows you to filter SIP session data on a global-basis using the "**monitoring-filters**" object at the path *Configure terminal->session-router->sip-monitoring->monitoring-filters* in the ACLI. You can apply a single or multiple custom filter for global monitoring. For more information about creating a custom filter, see Creating a Custom Filter (69).

To configure filtering on a global basis:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **sip-monitoring** and press <Enter> to access the SIP monitoring-related attributes.

   ```
   ACMEPACKET(session-router)# sip-monitoring
   ACMEPACKET(sip-monitoring)#
   ```

4. Type **select** and press <Enter> to select the sip-monitoring objects.

   ```
   ACMEPACKET(sip-monitoring)# select
   ACMEPACKET(sip-monitoring)#
   ```

   monitoring-filters—Enter the custom filter name(s) you want to use when monitoring on a global-basis. You can enter multiple filter names in a comma-separated list (with no spaces) if required. To add to an existing filter list, use the "+" before the filter name you are adding. Use a "-" to remove filter names. Enter an "*" (asterisk) to filter all session data.

   ```
   ACMEPACKET(sip-monitoring)# monitoring-filters FILTER1,FILTER2
   ACMEPACKET(sip-monitoring)# monitoring-filters FILTER1,FILTER2 +FILTER3
   ACMEPACKET(sip-monitoring)# monitoring-filters FILTER1,FILTER2 -FILTER3
   ACMEPACKET(sip-monitoring)# monitoring-filters *
   ```

   Note: If you enter the "*" with a filter name, the filter name is ignored and the Net-Net SD uses the "*" to filter all session data.

5. Enter **done** to save the configuration.

   ```
   ACMEPACKET(sip-monitoring)# done
   ```

6. Enter **exit** to exit the sip-monitoring configuration.

   ```
   ACMEPACKET(sip-monitoring)# exit
   ```

7. Enter **done** to save the sip-monitoring configuration.

   ```
   ACMEPACKET(session-router)# done
   ```

8. Enter **exit** to exit the session-router configuration.

   ```
   ACMEPACKET(session-router)# exit
   ```

9. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

10. Enter **save-config** to save the configuration.

    ```
    ACMEPACKET# save-config
    ```

11. Enter **activate-config** to activate the configuration.

    ```
    ACMEPACKET# activate-config
    ```

Using Filters when Monitoring Session Agents

You can configure the Net-Net SBC to perform filtering of SIP session data for session agent (SA) configurations. You must specify the hostname of the SA and the filter to use to perform the filtering, at the path *Configure terminal->session-router->session-agent* in the ACLI. For more information about creating a custom filter, see Creating a Custom Filter (69).

To configure filtering for a Session Agent:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **session-agent** and press <Enter> to access the session agent-related attributes.

   ```
   ACMEPACKET(session-router)# session-agent
   ACMEPACKET(session-agent)#
   ```

4. Type **select** and press <Enter>.

   ```
   ACMEPACKET(session-agent)# select
   ACMEPACKET(session-agent)#
   ```

   hostname—Specify the hostname of the session agent to which you want to apply the custom filter(s).

   ```
   ACMEPACKET(session-agent)# hostname SA1
   ```

   monitoring-filters—Enter the custom filter name(s) you want to use when monitoring on a global-basis. You can enter multiple filter names in a comma-separated list (with no spaces) if required. To add to an existing filter list, use the "+" before the filter name you are adding. Use a "-" to remove filter names. Enter an "*" (asterisk) to filter all SIP session data.

   ```
   ACMEPACKET(session-agent)# monitoring-filters FILTER1,FILTER2
   ACMEPACKET(session-agent)# monitoring-filters FILTER1,FILTER2 +FILTER3
   ACMEPACKET(session-agent)# monitoring-filters FILTER1,FILTER2 -FILTER3
   ACMEPACKET(session-agent)# monitoring-filters *
   ```

   Note: If you enter the "*" with a filter name, the filter name is ignored and the Net-Net SD uses the "*" to filter all session data.

5. Enter **done** to save the configuration.

   ```
   ACMEPACKET(session-agent)# done
   ```

6. Enter **exit** to exit the session-agent configuration.

   ```
   ACMEPACKET(session-agent)# exit
   ```

7. Enter **done** to save the configuration.

   ```
   ACMEPACKET(session-router)# done
   ```

8. Enter **exit** to exit the session-router configuration.

   ```
   ACMEPACKET(session-router)# exit
   ```

9. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

10. Enter **save-config** to save the configuration.

    ```
    ACMEPACKET# save-config
    ```

11. Enter **activate-config** to activate the configuration.

    ```
    ACMEPACKET# activate-config
    ```

Using Filters when Monitoring Realms

You can configure the Net-Net SBC to perform filtering of SIP session data for realm configurations. You must specify the realm identifier and the filter to use to perform the filtering, at the path *Configure terminal->media-manager->realm-config* in the ACLI. For more information about creating a custom filter, see Creating a Custom Filter (69).

To configure filtering for a realm:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **media-manager** and press <Enter> to access the media manager-related objects.

   ```
   ACMEPACKET(configure)# media-manager
   ACMEPACKET(media-manager)#
   ```

3. Type **realm-config** and press <Enter> to access the realm configuration-related attributes.

   ```
   ACMEPACKET(media-manager)# realm-config
   ACMEPACKET(realm-config)#
   ```

4. Type **select** and press <Enter>.

   ```
   ACMEPACKET(realm-config)# select
   ACMEPACKET(realm-config)#
   ```

   identifier—Specify the identifier of the realm to which you want to apply the custom filter(s).

   ```
   ACMEPACKET(realm-config)# identifier REALM1
   ```

   monitoring-filters—Enter the custom filter name(s) you want to use when monitoring on a global-basis. You can enter multiple filter names in a comma-separated list (with no spaces) if required. To add to an existing filter list, use the "+" before the filter name you are adding. Use a "-" to remove filter names. Enter an "*" (asterisk) to filter all SIP session data.

   ```
   ACMEPACKET(realm-config)# monitoring-filters FILTER1,FILTER2
   ACMEPACKET(realm-configg)# monitoring-filters FILTER1,FILTER2 +FILTER3
   ACMEPACKET(realm-config)# monitoring-filters FILTER1,FILTER2 -FILTER3
   ACMEPACKET(realm-config)# monitoring-filters *
   ```

   Note: If you enter the "*" with a filter name, the filter name is ignored and the Net-Net SD uses the "*" to filter all session data.

5. Enter **done** to save the configuration.

   ```
   ACMEPACKET(realm-config)# done
   ```

6. Enter **exit** to exit the realm-config configuration.

   ```
   ACMEPACKET(realm-config)# exit
   ```

7. Enter **done** to save the configuration.

   ```
   ACMEPACKET(media-manager)# done
   ```

8. Enter **exit** to exit the media-manager configuration.

   ```
   ACMEPACKET(media-manager)# exit
   ```

9. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

10. Enter **save-config** to save the configuration.

    ```
    ACMEPACKET# save-config
    ```

11. Enter **activate-config** to activate the configuration.

    ```
    ACMEPACKET# activate-config
    ```

Global, SA, and Realm Filter Examples

The following are examples of global, session agent, and realm filters configured on the Net-Net SBC. These examples assume that FILTER1, FILTER2, and FILTER3 have been pre-configured as custom filters.

Global Filter

```
ACMEPACKET(sip-monitoring)# monitoring-filters FILTER1,FILTER3
```

This filter captures the SIP session data based on the filter settings in FILTER1 and FILTER3 only, for all sessions on the Net-Net SBC.

Session Agent Filters

```
ACMEPACKET(session-agent)# hostname SA1
ACMEPACKET(session-agent)# monitoring-filters FILTER2

ACMEPACKET(session-agent)# hostname SA2
ACMEPACKET(session-agent)# monitoring-filters FILTER2,FILTER3
```

These filters capture the SIP session data for SA1 only, based on the filter settings in FILTER2, and the SIP session data for SA2 only, based on the filter settings in FILTER2 and FILTER3.

Realm Filters

```
ACMEPACKET(realm-config)# identifier REALM1
ACMEPACKET(realm-config)# monitoring-filters *

ACMEPACKET(realm-config)# identifier REALM2
ACMEPACKET(realm-config)# monitoring-filters FILTER1
```

These filters capture all SIP session data for REALM1, and the SIP session data for REALM2 only, based on the filter settings in FILTER1.

> **Note:** If you leave a “monitoring-filter” field blank, no monitoring takes place for that object.

Configuring Interesting Events

Interesting events on the Net-Net SBC are those events that are considered "interesting" for the purpose of troubleshooting SIP sessions in your network. You can specify the type of interesting event you want to filter using the object, "**interesting-events**" at the path, *Configure terminal->session-router->sip-monitoring ->interesting-events* in the ACLI.

Currently, there are two types of interesting events that the Net-Net SBC can monitor:

- **short-session** (short session events on the Net-Net SBC)
- **local-rejection** (local rejection events on the Net-Net SBC)

You can use the following trigger attributes to specify time provisioning for the interesting events:

- **trigger-threshold**
- **trigger-timeout**

> **Note:** You can also set a trigger-window object to support these trigger attributes. For more information, see Configuring a Trigger Window (79).

The following table identifies the attributes you can set for the "interesting-events" object.

Filter	Description
interesting-events	**Allows you to configure trigger attributes that apply to the filters you set on the Net-Net SBC. You can configure the following interesting-event attributes:** **Note: Interesting Events are always enabled on a global-basis on the Net-Net SBC.**
type	**Sets the interesting events to monitor (short-session, local-rejection)**
trigger-threshold	**Sets the number of interesting events that must occur within the time set by the "trigger-window" value. If the number of events reaches the trigger-threshold during the trigger-window time, monitoring is started.**
trigger-timeout	**Sets the amount of time, in seconds, that the trigger is active once monitoring has started. If no interesting events occur in the time frame set for this value, monitoring never starts. For example, if trigger-timeout is set to 40, and no interesting events occur in 40 seconds, then monitoring never starts.**

The Net-Net SBC considers "short session" and "local rejection" interesting events. A session is viewed as a "short session" if the length of time, in seconds, is equal to or below the "short-session-duration" value configured at the path *Configure terminal->session-router->session-router-config->short-session-duration*. A "local rejection" can occur when sessions are locally rejected at the Net-Net SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.)

If a short session or local rejection event occurs, the Net-Net SBC uses the values configured for the trigger attributes to determine when to start filtering the SIP session data.

Note: If a short session event occurs when the Net-Net SBC is NOT monitoring, the event information is taken from the last "BYE" that occurred in the session; therefore, only some parts of the call flow may display in the Web-based GUI. If a local rejection event occurs when the Net-Net SBC is NOT monitoring, it displays only the information in the last rejected transaction.

Use the following procedure to configure interesting events for SIP monitoring and tracing on the Net-Net SBC.

To configure interesting events:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **session-router** again and press <Enter> to access the session router configuration-related attributes.

   ```
   ACMEPACKET(session-router)# session-router
   ACMEPACKET(session-router-config)#
   ```

   short-session-duration—Enter the maximum session duration, in seconds, to be considered a short session. Default is 0 (disabled). Valid values are 0 to 999999999.

   ```
   ACMEPACKET(session-router-config)# short-session-duration 30
   ```

4. Enter **done** to save the filters.

   ```
   ACMEPACKET(session-router-config)# done
   ACMEPACKET(session-router-config)#
   ```

5. Enter **exit** to exit the interesting-events configuration.

   ```
   ACMEPACKET(session-router-config)# exit
   ACMEPACKET(session-router)#
   ```

6. Type **sip-monitoring** and press <Enter> to access the SIP monitoring-related attributes.

   ```
   ACMEPACKET(session-router)# sip-monitoring
   ACMEPACKET(sip-monitoring)#
   ```

7. Type **select** and press <Enter>.

   ```
   ACMEPACKET(sip-monitoring)# select
   ACMEPACKET(sip-monitoring)#
   ```

8. Type **interesting-events** and press <Enter> to access the interesting events-related attributes.

   ```
   ACMEPACKET(sip-monitoring)# interesting-events
   ACMEPACKET(interesting-events)#
   ```

   type—Enter the type of interesting event you for which you want to filter. Default is blank and disables this filter. Valid values are:

   - short-session
   - local-rejection

   ```
   ACMEPACKET(interesting-events)# type short-session
   ```

trigger-threshold — (optional) Enter the number of interesting events that must occur within the time set by the "trigger window ()" value. If the number of events reaches the trigger-threshold during the trigger-window time, monitoring is started.Default is 0 (disabled). Valid values are 0 to 999999999.

```
ACMEPACKET(interesting-events)# trigger-threshold 50
```

trigger-timeout —Sets the amount of time, in seconds, that the trigger is active once monitoring has started. If no interesting events occur in the time frame set for this value, monitoring never starts. Default is 0 (trigger always on). Valid values are 0 to 999999999.

```
ACMEPACKET(interesting-events)# trigger-timeout 30
```

9. Enter **done** to save the filters.

```
ACMEPACKET(interesting-events)# done
```

10. Enter **exit** to exit the interesting-events configuration.

```
ACMEPACKET(interesting-events)# exit
```

11. Enter **exit** to exit the sip-monitoring configuration.

```
ACMEPACKET(sip-monitoring)# exit
```

12. Enter **done** to save the configuration.

```
ACMEPACKET(session-router)# done
```

13. Enter **exit** to exit the session-router configuration.

```
ACMEPACKET(session-router)# exit
```

14. Enter **save-config** to save the filters.

```
ACMEPACKET# save-config
```

15. Enter **activate-config** to activate the filters in the current configuration.

```
ACMEPACKET# activate-config
```

Note: For SIP Monitor and Trace to trigger interesting-events, the "monitoring-filters" object must be configured via the ACLI.

The following example shows the monitoring-filter configured to include all session data (*).

```
sip-monitoring
     state                         enabled
     monitoring-filters            *
     interesting-events
         type                      local-rejection
         trigger-threshold         0
         trigger-timeout           0
     trigger-window                30
```

The following example shows the monitoring-filter configured to include only the session data configured for Filter1.

```
sip-monitoring
     state                         enabled
     monitoring-filters            filter1
     interesting-events
         type                      local-rejection
         trigger-threshold         0
         trigger-timeout           0
     trigger-window                30
```

Configuring a Trigger Window

The “**trigger-window**” attribute specifies the amount of time, in seconds, for the window of time that the “trigger-threshold (78)” value must reach before monitoring begins. For example, if “interesting-event” type is set to short-session, “trigger-threshold” is set to 2, and “trigger-window” is set to 60, monitoring begins when the Net-Net SBC has discovered 2 short-session events in a 60 second window.

Use the following procedure to configure a trigger window.

To configure a trigger window:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter> to access the session router-related objects.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **sip-monitoring** and press <Enter> to access the SIP monitoring-related attributes.

   ```
   ACMEPACKET(session-router)# sip-monitoring
   ACMEPACKET(sip-monitoring)#
   ```

4. Type **select** and press <Enter>.

   ```
   ACMEPACKET(sip-monitoring)# select
   ACMEPACKET(sip-monitoring)#
   ```

   trigger-window—Enter the amount of time, in seconds, for the window of time that the “trigger-threshold” value must reach before monitoring begins. Default is 30. Valid values are 0 to 999999999. Zero (0) disables this the trigger-window parameter.

   ```
   ACMEPACKET(sip-monitoring)# trigger-window 50
   ```

5. Enter **done** to save the filters.

   ```
   ACMEPACKET(sip-monitoring)# done
   ```

6. Enter **exit** to exit the sip-monitoring configuration.

   ```
   ACMEPACKET(sip-monitoring)# exit
   ```

7. Enter **done** to save the configuration.

   ```
   ACMEPACKET(session-router)# done
   ```

8. Enter **exit** to exit the session-router configuration.

   ```
   ACMEPACKET(session-router)# exit
   ```

9. Enter **exit** to exit the configure mode.

   ```
   ACMEPACKET(configure)# exit
   ```

10. Enter **save-config** to save the filters.

    ```
    ACMEPACKET# save-config
    ```

11. Enter **activate-config** to activate the filters in the current configuration.

    ```
    ACMEPACKET# activate-config
    ```

Example

The following is an example filter configuration, filtering interesting events with a trigger window on the Net-Net SBC. These parameters perform filtering on a global basis.

Monitoring Enabled on a Global Basis

```
ACMEPACKET(sip-monitoring)# state enabled
```

Short-Session Configured

```
ACMEPACKET(interesting-events)# type short-session
ACMEPACKET(interesting-events)# trigger-threshold 2
ACMEPACKET(interesting-events)# trigger-timeout 60
```

Local-Rejection Configured

```
ACMEPACKET(interesting-events)# type local-rejection
ACMEPACKET(interesting-events)# trigger-threshold 1
ACMEPACKET(interesting-events)# trigger-timeout 0
```

Trigger-Window Configured

```
ACMEPACKET(sip-monitoring)# trigger-window 120
```

The configuration above has global SIP monitoring "**enabled**" and is set to capture interesting events that are "**short-session**" and "**local-rejection**" events.

Per the triggers for the short-session configuration, if **2** (trigger-threshold) short-session events occur in a window of **120** seconds (trigger-window), then monitoring is started. If no short-session events occur after **60** seconds (trigger-timeout), no monitoring is started.

Per the triggers for the "local-rejection" configuration, if more that **1** (trigger-threshold) local-rejection event occurs in a window of **120** seconds (trigger-window), then monitoring is started. The value of **0** (trigger-timeout) indicates that monitoring is always enabled for this event.

Dynamic Filters

The SIP monitoring and tracing feature provides a time-saving feature of adding filters dynamically, and turning the filters ON and OFF as required. The filtering process performs on a dynamic basis dependant on the filters you specify.

Dynamic Filter Commands

You can use the ACLI to initiate the following dynamic filtering commands:

- **capture start** - starts the filters you specify in the filter syntax
- **capture stop** - stops the filters you specify in the filter syntax

> **Note:** Initiating these commands does NOT change the values set in the ACLI-configured filters on the Net-Net SBC. The Net-Net SBC uses the dynamic filters until you initiate a stop command.

The syntax for the dynamic filter commands are:

```
capture start <main filter> <subfilter(s)>
capture stop <main filter> <subfilter(s)>
```

> **Note:** You MUST enter a “<main filter>” AND a“<subfilter(s)>” when initiating the “capture start” and “capture stop” commands.

The following table identifies the values you can use for each attribute in the command syntax.

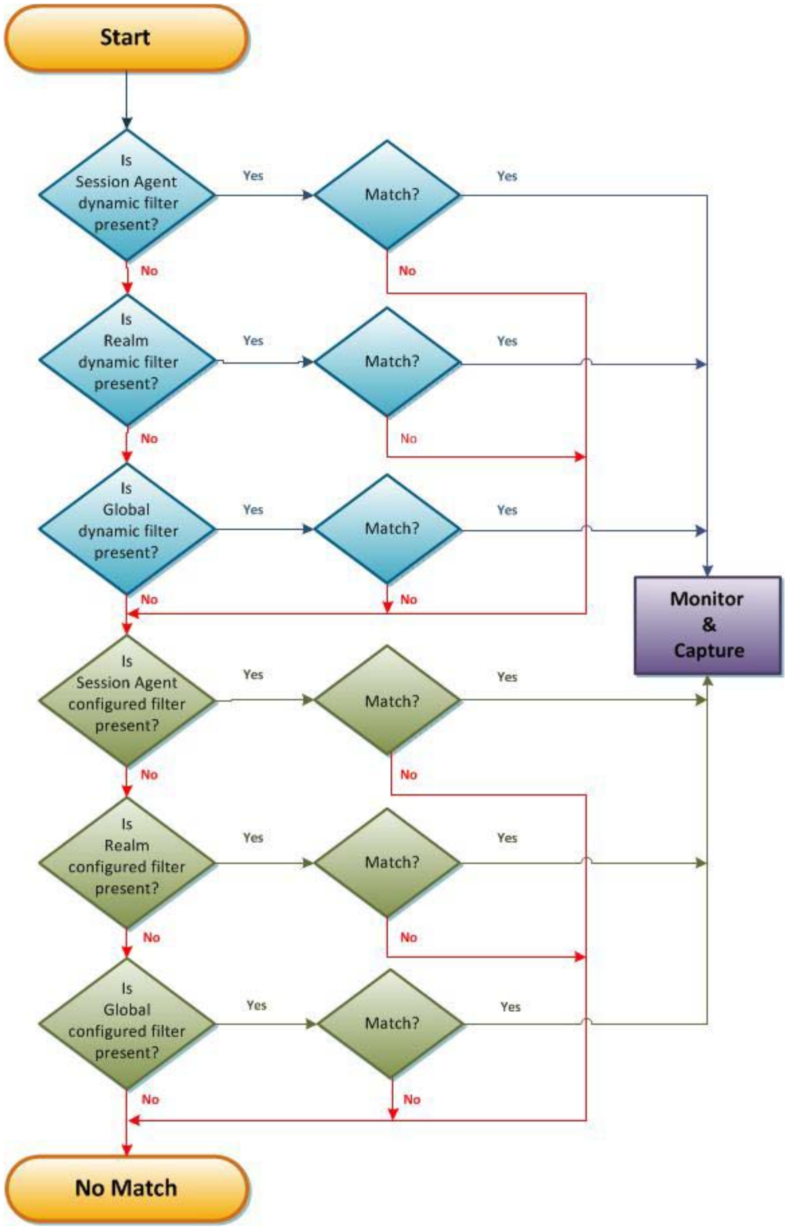
Syntax Attribute	Values
<main filter>	• **global -** monitors and captures all • **realm** <realm name> - monitors and captures everything matching realm • **session-agent** <session-agent name> - monitors and captures everything matching session agent. • **int-ev** <short-session | local-rejection> - monitors and captures everything matching a short-session and/or local-rejection.
[<subfilter(s)>]	• * - monitors and captures all sessions. • **user** <Phone Number or User Part URI> - monitors and captures everything that matches this phone number or user part. • **addr-prefix** <IP address or IP address and netmask> - monitors and captures everything that matches this address or address prefix.

Examples

The following table provides examples for using the dynamic filter commands.

Example	Description
capture start global *	Captures all session data.
capture start global user USER1	Captures all session data for USER1.
capture start global addr-prefix 1.1.1.1	Captures all session data for IP address 1.1.1.1.
capture start global addr-prefix 1.1.1.1/24	Captures all session data for IP address 1.1.1.1 using netmask of 24.
capture start session-agent 172.1.1.1 addr-prefix 10.10.10.10	Captures session data for SA 172.1.1.1 at IP address 10.10.10.10.
capture start int-ev local-rejection	Captures session data for interesting events that occur that are of type “local-rejection”.
capture start int-ev short session	Captures session data for interesting events that occur that are of type “short-session.”

The following flow chart shows the dynamic filter process.


Start
Is Session Agent dynamic filter present?
Yes
Match?
Yes
No
No
Is Realm dynamic filter present?
Yes
Match?
Yes
No
No
Is Global dynamic filter present?
Yes
Match?
Yes
No
No
Monitor & Capture
Is Session Agent configured filter present?
Yes
Match?
Yes
No
No
Is Realm configured filter present?
Yes
Match?
Yes
No
No
Is Global configured filter present?
Yes
Match?
Yes
No
No
No Match

> **Note:** Dynamic filters are removed after a save/activate command, and after a reboot/switchover of the Net-Net SD.

Issuing another dynamic command may or may not affect previous dynamic commands that were already initiated. If you issue a dynamic command with a <main filter> object, and then issue another command with the same <main filter> object, the new command tasks precedence. If you issue a dynamic command with a different <main filter> object, then the Net-Net SD uses both <main filter> commands to monitor traffic.

For example, if you enter the following dynamic command:

```
ACMPACKET# capture start realm1 user 123
```

and then enter:

```
ACMPACKET# capture start realm2
```

The Net-Net SD monitors realm1 AND realm2 with user 123.

The command "**show monitoring dynamic-monitoring-filters summary**" indicates the dynamic filters currently being used. For example:

```
ACMPACKET# show monitoring dynamic-monitoring-filters summary

Active Filters for realm [realm1]
Monitoring Filters: userPart=123

Active Filters for realm [realm2]
Monitoring Filters: userPart=123
```

> **Note:** For more information about the “show monitoring dynamic-monitoring-filters summary”command, see .

To stop dynamic filter commands, you can initiate the “**capture stop <main filter>**” command. For example:

```
ACMPACKET# capture stop realm1 user 123
```

> **Note:** To stop configured filters, you must manually remove them from the ACLI configuration.

Clearing all Dynamic Filters

You can clear all dynamic filters using the following command:

- **reset monitoring dynamic-commands** - clears all dynamic filters previously initiated

The Net-Net SBC maintains a record of all dynamically initiated active filters. When you initiate this reset command, the Net-Net SBC searches through all of the filters and resets all the dynamic filters for each main filter (realm, session-agent, session-group, interesting event).

Example

The following command is an example of using the reset command to clear all dynamic capture filters.

```
ACMEPACKET# reset monitoring dynamic-commands
```

The following message displays:

Reset all dynamically created monitoring capture commands....

Clearing Event Monitoring Records

You can clear all records stored in the event monitoring in-memory database using the following command:

- **reset monitoring records** - clears all event monitoring records from the in-memory database.

Use the following procedure to clear all event monitoring records.

To clear event monitoring records:

1. At the prompt, type **reset monitoring records**, and press <Enter>.

   ```
   ACMEPACKET# reset monitoring records
   ```

   The following prompt displays:

   ```
   All in-memory event monitoring records will be deleted [y/n]?:
   ```

2. Type "**y**" and press <Enter>.

   ```
   All in-memory event monitoring records will be deleted [y/n]?: y
   ```

   The following message displays.

   "*Deleting the in-memory event records*".

   If you enter "**n**" for Step 2, the following message displays.

   "*Cancelling the reset*".

   No event monitoring records are deleted.

6 Web Server Configuration

Introduction

The Net-Net SBC includes an embedded Web-based GUI that can display the SIP session data results from a filtered session. This GUI displays SIP sessions data on one or multiple Net-Net SBCs, and provides traces in a common log format for local viewing or for exporting to your PC.

This chapter provides the information required to prepare the Web Server for running the Web-based GUI.

Topics include:

- Configuring the Web Server (87)
- Configuring TLS for the Web Server (89)
- Management Commands for the Web Server (95)

Configuring the Web Server

To use the Web-based GUI via your browser, you must first enable the GUI using the ACLI.

> **Note:** You install the Web-based GUI via an ACLI installation wizard. For more information about the installation wizard, refer to Chapter 9, Additional Features (141).

Use the following procedure to configure the Web server:

To configure the Web server:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter> to access the system-related objects.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **web-server-config** and press <Enter> to access the event monitoring-related attributes.

   ```
   ACMEPACKET(system)# web-server-config
   ACMEPACKET(web-server-config)#
   ```

   state—Enter whether or not to enable the Web-based GUI. Default is "**enabled**". Valid values are:

   - enabled (default)
   - disabled

   ```
   ACMEPACKET(web-server-config)# state enabled
   ```

inactivity-timeout—Enter the amount of time, in minutes, that the Web-based GUI must have remained inactive before it ends Web session. For example, if this timeout value is set as "5", after 5 minutes of no activity, the Web session disconnects. Default is **5**. Valid values are **0** to **20**.

```
ACMEPACKET(web-server-config)# inactivity-timeout 5
```

Note: The following **http-state**, **http-port**, **https-state**, and **https-port** parameters may have already been set via the Web-based GUI installation wizard on your Net-Net SBC. You can edit these parameters if required using the ACLI.

http-state—Enter whether or not to enable HTTP for accessing the Web server. Default is "**enabled**". Valid values are:

- enabled (default)
- disabled

```
ACMEPACKET(web-server-config)# http-state enabled
```

http-port—Enter the HTTP port to use to connect to the Web server. Default is "**80**". Valid values are **1** to **65535**.

```
ACMEPACKET(web-server-config)# http-port 80
```

https-state—Enter whether or not to enable HTTPS (secure connection) for accessing the Web server. Default is "**disabled**". Valid values are:

- enabled
- disabled (default)

```
ACMEPACKET(web-server-config)# https-state enabled
```

https-port—Enter the HTTPS port to use to connect to the Web server. Default is "**443**". Valid values are **1** to **65535**.

```
ACMEPACKET(web-server-config)# https-port 443
```

tls-profile—Enter the Transport Layer Security (TLS) Protocol profile name to use with HTTPS. Default is blank. Valid values are alpha-numeric characters.

```
ACMEPACKET(web-server-config)# tls-profile tlsSM&T
```

Note: If you specify a "tls-profile", and HTTP is enabled, the Net-Net SBC checks against the TLS profile table for a match. If there is no match, the applicable errors display during the verification of the configuration.

To create a TLS profile, see Configuring a TLS Profile (93).

4. Enter **exit** to exit the Web server configuration.

```
ACMEPACKET(web-server-config)# exit
```

5. Enter **exit** to exit the system configuration.

```
ACMEPACKET(system)# exit
```

6. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

7. Enter **save-config** to save the configuration.

```
ACMEPACKET# save-config
```

8. Enter **activate-config** to activate as the current configuration.

```
ACMEPACKET# activate-config
```

Configuring TLS for the Web Server

The SIP monitoring and tracing feature supports the use of HTTP over Transport Layer Security (TLS) using the TLS Protocol. TLS is a cryptographic protocol that provides communication security over the Internet. It encrypts the segments of network connections at the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

> **Note:** For more information about setting up security on your Net-Net SBC, refer to the "**Security**" section of the *Net-Net ACLI Configuration Guide* for your model Net-Net SBC.

To use TLS with SIP monitoring and tracing, you must configure a TLS certificate and a TLS profile using the ACLI at the path *Configure Terminal->Security*. This configuration stores the information required to run SIP over TLS.

> **Note:** If you enable TLS on the active Net-Net SBC, the Web-based GUI interface on the standby system is disabled.

Process Overview

In summary, you need to take the following steps to enable your Net-Net SBC for TLS.

1. Make sure that your Net-Net SBC has the appropriate hardware installed and that you have obtained an enabled the licenses related to TLS support. (Note that the Net-Net 4250 does not require an additional license for TLS support.)
2. Configure certificates.
3. Configure the specific parameters related to TLS.

Configuring Certificates

Configuring certificates is a three-step process:

1. Create a certificate record configuration on the Net-Net SBC
2. Generate a certificate request by the Net-Net SBC and save the configuration
3. Import the certificate record into the Net-Net SBC and save the configuration

Configuring the Certificate Record

The certificate record configuration represents either the end-entity or the Certificate Authority (CA) certificate on the Net-Net SBC. If it is used to present an end-entity certificate, a private key should be associated with this certificate record configuration using the ACLI security certificate request command.

No private key should be associated with the certificate record configuration if it was issued to hold a CA certificate. A certificate can be imported to a certificate record configuration using the ACLI security certificate import command.

> **Note:** There is no need to create a certificate record when importing a CA certificate or certificate in pkcs12 format.

To configure a certificate:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **security** and press <Enter> to access the security-related objects.

```
ACMEPACKET(configure)# security
```

3. Type **certificate-record** and press <Enter> to access the certificate record parameters.

```
ACMEPACKET(security)# certificate-record
ACMEPACKET(certificate-record)#
```

name—Enter the name of the certificate record. This is a key field, and you must enter a value for it. For example, acmepacket.

country—Enter the name of the country. The default is US.

state—Enter the name of the state of for the country. The default is MA.

locality—Enter the name of the locality for the state. The default is Burlington.

organization—Enter the name of the organization holding the certificate. The default is Engineering.

unit—Enter the name of the unit for the holding the certificate within the organization.

common-name—Enter the common name for the certificate record.

key-size—Enter the size of the key for the certificate. Use the default of 1024, or change it to one of the other supported values: 512, 2048, or 4096.

alternate-name—Enter the alternate name of the certificate holder.

key-usage-list—Enter the usage extensions you want to use with this certificate record. This parameter can be configured with multiple values, and it defaults to the combination of digitalSignature and keyEncipherment. For a list of possible values and their descriptions, see the section “Key Usage Control” in the *Net-Net ACLI Configuration Guide* for your Net-Net SBC model.

extended-key-usage-list—Enter the extended key usage extensions you want to use with this certificate record. The default is serverAuth. For a list of possible values and their descriptions, see the section “Key Usage Control” in the *Net-Net ACLI Configuration Guide* for your Net-Net SBC model.

4. Enter **done** to save the certificate-record configuration.

```
ACMEPACKET(certificate-record)# done
```

5. Enter **exit** to exit the certificate-record configuration.

```
ACMEPACKET(certificate-record)# exit
```

6. Enter “**y**” at the prompt to save the configuration.

```
Save Changes [y|n]?: y
```

7. Enter **exit** to exit the security configuration.

```
ACMEPACKET(security)# exit
```

8. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

9. Enter **save-config** to save the configuration.

```
ACMEPACKET# save-config
```

10. Enter **activate-config** to activate as the current configuration.

    ```
    ACMEPACKET# activate-config
    ```

    Note: For verifying a certificate record, see the "**Security**" section of the *Net-Net ACLI Configuration Guide* for your Net-Net SBC model.

Generating a Certificate Request

Using the ACLI **security certificate request** command allows you to generate a private key and a certificate request in PKCS10 PEM format.

> **Note:** You can only perform this step once you have configured a certificate record.

The Net-Net SBC stores the private key that is generated in the certificate record configuration in 3DES encrypted form with an internally generated password. The PKCS10 request is displayed on the screen in PEM (Base64) form.

You use this command for certificate record configurations that hold end-entity certificates. If you have configured the certificate record to hold a CA certificate, then you do not need to generate a certificate request because the CA publishes its certificate in the public domain. You import a CA certificate by using the ACLI **security certificate request import** command.

This command sends information to the CA to generate the certificate, but you cannot have Internet connectivity from the Net-Net SBC to the Internet. You can access the internet through a browser such as Internet Explorer if it is available, or you can save the certificate request to a disk and then submit it to the CA.

To run the applicable command, you must use the value you entered in the name parameter of the certificate record configuration. You run the command from the main Superuser mode command line, and then save and activate the configuration.

```
ACMEPACKET# security certificate request acmepacket
Generating Certificate Signing Request. This can take several
minutes....
-----BEGIN CERTIFICATE REQUEST-----
MIIB2jCCAUMCAQAwYTELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEMMAoGA1UECxMDYWJj
MQwwCgYDVQQDEwNhYmMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALOMLHo8
/qIOddIDVuqot0Y72l/BfH8lolRKmhZQ4e7sS+zZHzbG8phzmzhfOSECnZiA2bEo
f+Nti7e7Uof4lLwiYl9fvhURfzhENOKThAPKPiJCzBBglTITHTYal00Cq2fj5A8B
ZcuAHj7Vp5wP2zpz6EUTFpqTDMLVdwJGJrElAgMBAAGgOTAMBgNVHRExBRMDZGVm
MCkGA1UdDzEiEyBkaWdpdGFsU2lnbmF0dXJlLGtleUVuY2lwaGVybWVudDANBgkq
hkiG9w0BAQUFAAOBgQAtel4ZSLI8gqgMzodbYwgUHUGqTGeDzQDhJV5fKUXWeMFz
JsTmWn5Gy/kR4+Nq274G14fnk00fTAfMtgQ5aL3gM43TqaPOTZjJ6qgwuRKhoBPI
7hkovkgAxHge7wClghiAp/ELdl7tQ515k04BMd5f/fxG7nNiu8iEg7PO0OIBgg==
-----END CERTIFICATE REQUEST-----
WARNING: Configuration changed, run "save-config" command.
ACMEPACKET# save config
copying file /code/config/dataDoc.gz -> /code/config/dataDoc_3.gz
copying file /code/config/tmp/editing/dataDoc.gz ->
/code/config/dataDoc.gz
Save complete
ACMEPACKET# activate config
activate complete
```

Importing a Certificate Using the ACLI

For an end-entity certificate, once a certificate is generated using the ACLI security certificate request command, that request should be submitted to a CA for generation of a certificate in PKCS7 or X509v3 format. When the certificate has been generated, you can import it into the Net-Net SBC using the security certificate import command.

The syntax is:

```
ACMEPACKET # security certificate import [try-all | pkcs7 | pkcs12 |
x509] [certificate-record file-name]
```

To import a certificate:

1. When you use the security certificate import command, you can specify whether you want to use PKCS7, PKCS12, X509v3 format, or try all. In the command line, you enter the command, the format specification, and the name of the certificate record. Next, the Net-Net SBC will prompt you to enter the certificate in PEM format. Paste the certificate in the ACLI at this point. For example:

   ```
   ACMEPACKET# security certificate import try-all acmepacket
   ```

   The following displays:

   ```
   Please enter the certificate in the PEM format.
   Terminate the certificate with ";" to exit.......
   -----BEGIN CERTIFICATE-----
   VMIIDHzCCAoigAwIBAgIIAhMCUACEAHEwDQYJKoZIhvcNAQEFBQAwcDELMAkGA1UE
   BhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ4w
   DAYDVQQKEwVzaXBpdDEpMCcGA1UECxMgU2lwaXQgVGVzdCBDZXJ0aWZpY2F0ZSBB
   dXRob3JpdHkwHhcNMDUwNDEzMjEzNzQzWhcNMDgwNDEyMjEzNzQzWjBUMQswCQYD
   VQQGEwJVUzELMAkGA1UECBMCTUExEzARBgNVBAcTCkJ1cmxpbmd0b24xFDASBgNV
   BAoTC0VuZ2luZWVyaW5nMQ0wCwYDVQQDEwRhY21lMIGfMA0GCSqGSIb3DQEBAQUA
   A4GNADCBiQKBgQCXjIeOyFKAUB3rKkKK/+59LT+rlGuW7Lgc1V6+hfTSr0co+ZsQ
   bHFUWAA15qXUUBTLJG13QN5VfG96f7gGAbWayfOS9Uymold3JPCUDoGgb2E7m8iu
   vtq7gwjSeKNXAw/y7yWy/c04FmUD2U0pZX0CNIR3Mns5OAxQmq0bNYDhawIDAQAB
   o4HdMIHaMBEGA1UdEQQKMAiCBnBrdW1hcjAJBgNVHRMEAjAAMB0GA1UdDgQWBBTG
   tpodxa6Kmmn04L3Kg62t8BZJHTCBmgYDVR0jBIGSMIGPgBRrRhcU6pR2JYBUbhNU
   2qHjVBShtqF0pHIwcDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
   ETAPBgNVBAcTCFNhbiBKb3NlMQ4wDAYDVQQKEwVzaXBpdDEpMCcGA1UECxMgU2lw
   aXQgVGVzdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCAQAwDQYJKoZIhvcNAQEFBQAD
   gYEAbEs8nUCi+cA2hC/lM49Sitvh8QmpL81KONApsoC4Em24L+DZwz3uInoWjbjJ
   QhefcUfteNYkbuMH7LAK0hnDPvW+St4rQGVK6LJhZj7/yeLXmYWIPUY3Ux4OGVrd
   2UgV/B2SOqH9Nf+FQ+mNZOlL7EuF4IxSz9/69LuYlXqKsG4=
   -----END CERTIFICATE-----;
   Certificate imported successfully....
   WARNING: Configuration changed, run "save-config" command.
   ```

2. Enter **save-config** to save the configuration.

   ```
   ACMEPACKET# save-config
   copying file /code/config/dataDoc.gz -> /code/config/dataDoc_3.gz
   copying file /code/config/tmp/editing/dataDoc.gz ->
   /code/config/dataDoc.gz
   Save complete
   ```

3. Enter **activate-config** to activate as the current configuration.

   ```
   ACMEPACKET# activate-config
   activate complete
   ```

   Note: For importing a certificate using FTP, see the "Security" section of the *Net-Net ACLI Configuration Guide* for your Net-Net SBC model.

   ```
   ACMEPACKET#
   ```

Importing a Certificate Using FTP

You can also put the certificate file in the directory /ramdrv and then execute the **import-certificate** command, or you can paste the certificate in PEM/Base64 format into the ACLI. If you paste the certificate, you may have to copy and paste it a portion at a time, rather than pasting the whole certificate at once.

To import the certificate using FTP:

1. FTP the certificate file on to the Net-Net SBC (directory /ramdrv), let us say the name of the certificate file is `cert.pem`.

2. Once the certificate is successfully transferred to the Net-Net SBC, run the **import-certificate** command.

The syntax is:

```
ACMEPACKET# import-certificate [try-all|pkcs7|x509] [certificate-
record file-name]
```

Using the command will look like this when you have used FTP.

```
ACMEPACKET# import-certificate try-all acme cert.pem
Certificate imported successfully....
WARNING: Configuration changed, run "save-config" command.
```

4. Save your configuration.

```
ACMEPACKET# save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
```

5. Synchronize and activate your configurations.

```
ACMEPACKET# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Add LI Flows
LiSysClientMgr::handleNotifyReq
H323 Active Stack Cnt:  0
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
ACMEPACKET#
```

Configuring a TLS Profile

To configure a TLS profile:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **security** and press <Enter> to access the security-related objects.

```
ACMEPACKET(configure)# security
```

3. Type **tls-profile** and press <Enter> to access the TLS profile-related parameters.

```
ACMEPACKET(security)# tls-profile
ACMEPACKET(tls-profile)#
```

name—Enter the name of the TLS profile. This parameter is required; you cannot leave it empty.

```
ACMEPACKET(tls-profile)# name tls-prof1
```

end-entity-certificate—Enter the name of the entity certification record.

```
ACMEPACKET(tls-profile)# end-entity-certificate cert1
```

trusted-ca-certificates—Enter the names of the trusted CA certificate records.

```
ACMEPACKET(tls-profile)# trusted-ca-certificates cert1
```

Note: To create and import certificate records to be used on the Web Server, see Configuring Certificates (89).

cipher-list—Not supported for SIP monitoring and tracing. The Session Director ignores any value you enter for this parameter.

- AES256-SHA (**TLS_RSA_WITH_AES_256_CBC_SHA**) - Firefox (version 12) and Chrome (version 19.0.1084.46m) only
- AES128-SHA (**TLS_RSA_WITH_AES_128_CBC_SHA**) - Firefox (version 12) and Chrome (version 19.0.1084.46m) only
- DES-CBC-SHA (**SSL_RSA_WITH_DES_CBC_SHA** or **TLS_RSA_WITH_DES_CBC_SHA**) - Internet Explorer (Version 9) only

verify-depth—Not supported for SIP monitoring and tracing

mutual-authenticate—Not supported for SIP monitoring and tracing

tls-version—Enter the TLS version you want to use with this TLS profile. Default is compatibility. Valid values are:

- TLSv1
- SSLv3
- compatibility (default)

```
ACMEPACKET(tls-profile)# tls-version TLSv1
```

cert-status-check—Not supported for SIP monitoring and tracing

cert-status-profile-list—Not supported for SIP monitoring and tracing

ignore-dead-responder—Not supported for SIP monitoring and tracing

4. Enter **done** to save the tls-profile configuration.

```
ACMEPACKET(tls-profile)# done
```

5. Enter **exit** to exit the TLS profile configuration.

```
ACMEPACKET(tls-profile)# exit
```

6. Enter **exit** to exit the security configuration.

```
ACMEPACKET(security)# exit
ACMEPACKET(configure)#
```

7. Enter **exit** to exit the configure mode.

```
ACMEPACKET(configure)# exit
```

8. Enter **save-config** to save the configuration.

```
ACMEPACKET# save-config
```

9. Enter **activate-config** to activate as the current configuration.

```
ACMEPACKET# activate-config
```

Management Commands for the Web Server

The following commands allow you to display information for managing the Web server used for accessing the Web-based GUI.

Command	Description
show ip connections	Displays information about the server connections.
show users	Displays information about users logged into a session on the server.
kill <index>	Terminates a session on the server.

“Show ip connections” Command

The “**show ip connections**” command allows you to display information about active server Transport Control Protocol (TCP) and/or User Datagram Protocol (UDP) connections. For example, this command can show the sockets tied to an HTTPS connection. The following is an example of the “show ip connections” command output.

```
ACMEPACKET# show ip connections
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q  Local Address        Foreign Address      (state)
-------- ----- ------ ------  -------------------- -------------------- -------
75059a0  TCP        0      0  172.30.80.231.1538    172.30.0.39.58497     TIME_WAIT
7506420  TCP        0      0  172.30.80.231.443     10.1.20.14.51006      TIME_WAIT
75044a0  TCP        0      0  172.30.80.231.443     10.1.20.14.51000      TIME_WAIT
7504f20  TCP        0      0  172.30.80.231.443     10.1.20.14.50997      TIME_WAIT
7503f60  TCP        0      0  127.0.0.1.3000        127.0.0.1.1064        ESTABLISHED
7503a20  TCP        0      0  127.0.0.1.3000        127.0.0.1.1063        ESTABLISHED
75034e0  TCP        0      0  127.0.0.1.3000        127.0.0.1.1062        ESTABLISHED
7502fa0  TCP        0      0  127.0.0.1.3000        127.0.0.1.1061        ESTABLISHED
7502a60  TCP        0      0  127.0.0.1.3000        127.0.0.1.1060        ESTABLISHED
7502520  TCP        0      0  127.0.0.1.1063        127.0.0.1.3000        ESTABLISHED
7501fe0  TCP        0      0  127.0.0.1.1062        127.0.0.1.3000        ESTABLISHED
7501aa0  TCP        0      0  127.0.0.1.1061        127.0.0.1.3000        ESTABLISHED
```

The following table describes each column in the above output.

Column Heading	Description
PCB	Printed circuit board in the server that is active on the connection.
Proto	Protocol used on this connection. Valid values are: • TCP - Transport Control Protocol • UDP - User Datagram Protocol
Recv-Q	Receiving queue - pertains to the queue on the server that receives packets from the Internet. This column should always display a zero (0). Packets should not be piling up in this queue.

Column Heading	Description
Send-Q	Sending queue - pertains to the queue on the server that sends out packets to the Internet. This column should always display a zero (0). Packets should not be piling up in this queue.
Local Address	Local server's IP address and port number, or IP address and the name of a service.
Foreign Address	Hostname and service, or IP address and port number to which you are connected. The asterisk is a placeholder for IP addresses, which of course cannot be known until a remote host connects.
(state)	Current state of the TCP or UDP connection. TCP states can be: • LISTEN waiting to receive a connection • ESTABLISHED a connection is active • TIME_WAIT a recently terminated connection; this should last only a minute or two, then change back to LISTEN. The socket pair cannot be re-used as long the TIME_WAIT state persists. UDP is stateless, so the "State" column is always blank.

"Show users" Command

The "**show users**" command displays information about users currently logged into a session on the server. Each user is indicated by an index number. The following is an example of the "show users" command output.

Note: The index number for Web sessions always begins at "31".

```
        ACMEPACKET# show users
Index task-id    remote-address        IdNum duration type    state     User
----- ---------- -------------------- ----- -------- ------- ------ ----------
    0 0x33a4c394                          0 00:01:20 console  user * console
    1 0x33a68858     172.30.0.39:39385     1 00:00:08  telnet  user  user
   31     NA         10.1.20.14:51218    31 00:00:55    http  user  user
   32     NA           10.1.20.14:443    32 00:00:29   https  user  user
```

The following table describes each column in the above output.

Column Heading	Description
Index	Number that the server assigns to the user as an identification of that user. **Note:** The index for Web sessions always begins at index 31.
Task-id	Alpha-numeric number that the server assigns to the task currently being performed. This is the session ID assigned to the task at log-in time. This field is not applicable to the Web server.
Remote-address	IP address and port number for which the server is connected.
IdNum	Identification number of the user currently logged into the server. This number is the same as the "Index" number.
Duration	Amount of time, in hours, minutes, and seconds, that the user has currently been logged into a session on the server. Format is HH:MM:SS.

Column Heading	Description
Type	Type of service that the user is currently using for connection to the server. Valid values can be: Console User is connected to the server via a local console. Telnet User is connected to the server via a Telnet session. FTP User is connected to the server using FTP. HTTP User is connected to the server using a Web HTTP service. HTTPS User is connected to the server using a secure Web HTTPS service.
State	Current state of the connection on the server. Valid values are: • admin • user **Note**: An "*' indicates a current connection.
User	Current user type logged into the server. Valid values are: • console • user • admin

"Kill <index>" Command

The "**kill <index>**" command terminates a session on the server. The following example uses the "show users" command to display the index number to use with the "kill <index>" command.

```
ACMEPACKET# show users
Index task-id    remote-address        IdNum duration type    state     User
----- ---------- -------------------- ----- -------- ------- ------ ----------
    0 0x33a4c394                           0 00:01:20 console  user * console
    1 0x33a68858     172.30.0.39:39385     1 00:00:08  telnet  user  user
   31     NA          10.1.20.14:51218    31 00:00:55    http  user  user
   32     NA            10.1.20.14:443    32 00:00:29   https  user  user

ACMEPACKET# kill 31
```

The above "kill 31" command terminates the Web server session number 31.

After setting the Web server configuration, you can view the stored monitored data from your Net-Net SBC(s) using the Web-based GUI via your Internet browser. For more information about the Web-based GUI, see Web-based GUI.

7 Web-based GUI

Introduction

This chapter provides information and procedures for using the embedded Web-based GUI on your Net-Net SBC. This GUI displays results of filtered SIP session data from one or multiple Net-Net SBCs, and provides traces in a common log format for local viewing or for exporting to your PC. The Web-based GUI client provides local viewing support of SIP sessions only.

Topics include:

Web Browser Support

You can use any of the following Web browsers to access Oracle's Web-based GUI for viewing SIP session data:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Overview

The Web-based GUI allows you to view information about monitored SIP sessions on the Net-Net SBC(s). It supports four types of summary reports:

- **Sessions**
- **Registrations**
- **Subscriptions**
- **Notable events** (interesting events)

Each report summarizes the applicable information, displays it on easy-to-read pages, and allows you to sort and customize columns within each report. You can also perform searches to find specific information in a report.

Each type of report provides sorting, searching, and paging functionality and provides action buttons to use to display additional information or perform a task.

Logging in

You can login to the Web-based GUI using your Web browser (see Web Browser Support (99) for browsers that support this GUI). The Web interface supports authentication functionality similar to a user logging in via TELNET, Secure Shell (SSH), File Transfer Protocol (FTP), and SSH File Transfer Protocol (SFTP). SIP Monitoring an Tracing also supports RADIUS authentication.

> **Note:** Regardless of the privilege level set via authentication (user or admin), logging into the Web-based GUI gives user-level access privileges.

Up to 5 users can log into the same Web-based GUI interface. If more than 5 users attempt to log in, the following error message displays:

> *"User limit reached. Please try again later."*

To login to the Web-based GUI:

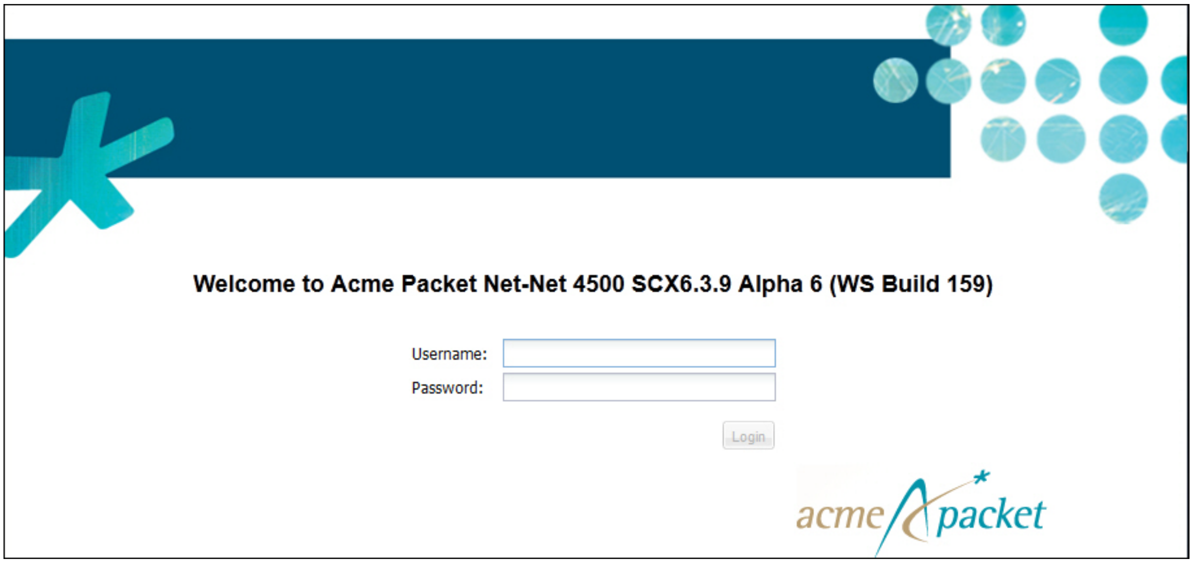
1. On your PC, open an Internet Browser.
2. Start the Web-based GUI by using either the HTTP or HTTPS login:

   http://<*Server IP address*>

   https://<Server IP address>

   Note: Logging in using HTTP and/or HTTPS is dependant on the setting that was made during the Web-based GUI installation wizard. You can change these settings using the ACLI. For more information, see Configuring the Web Server (87).

3. Enter your Web-based GUI username and password. Default username is "**user**" or "**admin**". Default password is "**packet**".
4. Click <**Login**>.

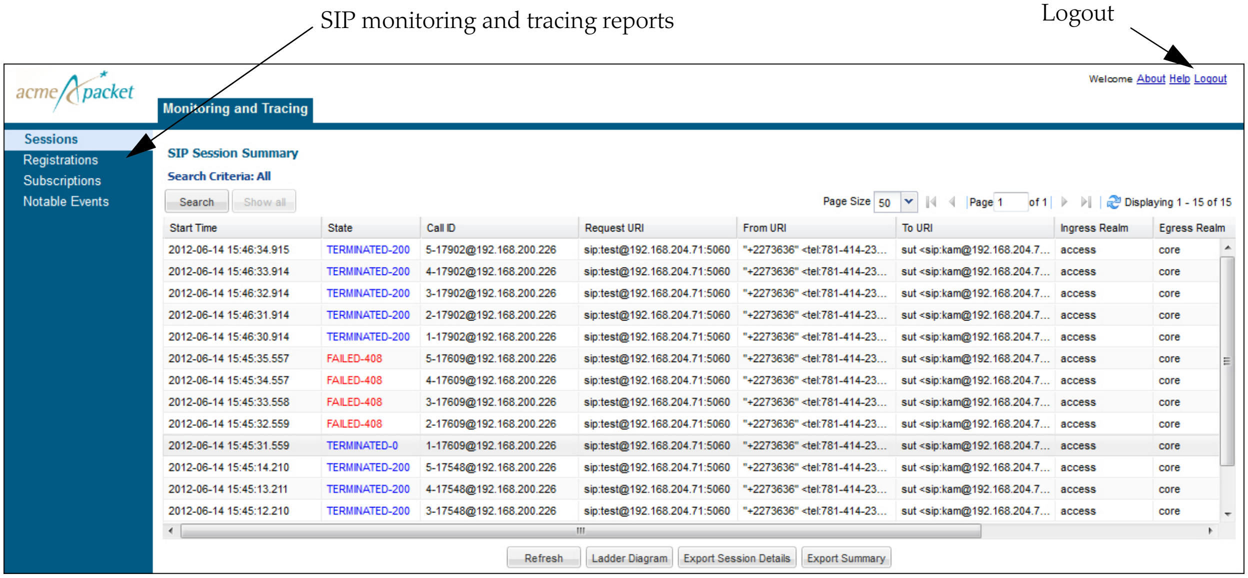


Welcome to Acme Packet Net-Net 4500 SCX6.3.9 Alpha 6 (WS Build 159)

Username:

Password:

5. The Web-based GUI opens.



SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm
2012-06-14 15:46:34.915	TERMINATED-200	5-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:33.914	TERMINATED-200	4-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:32.914	TERMINATED-200	3-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:31.914	TERMINATED-200	2-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:30.914	TERMINATED-200	1-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:31.559	TERMINATED-0	1-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core

6. Click on the report you want to view in the slider on the left side of the page.

   On all Sessions, Registrations, Subscriptions, and Notable Events report pages, you can perform the following:

   - Customize the page display
   - Perform a search for specific data
   - Display a ladder diagram
   - Export session details
   - Export session summary

   The following paragraphs describe each of these tasks.

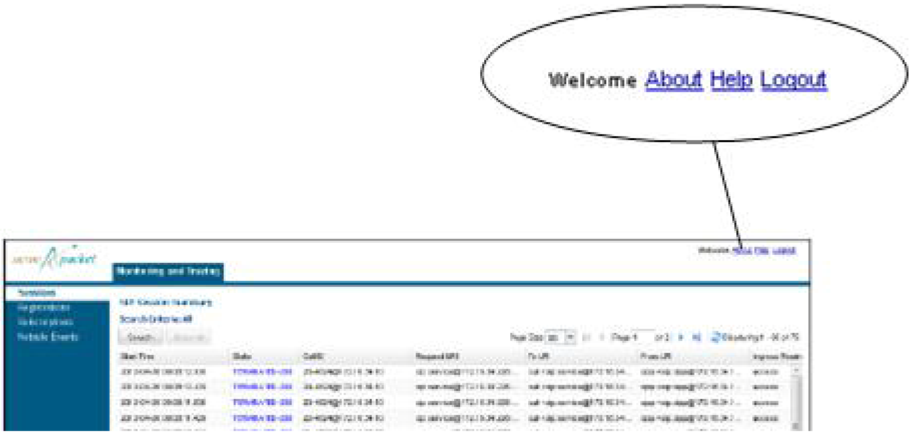
7. To logout of the Web-based GUI, click **Logout** in the upper right corner of the page.

About Information

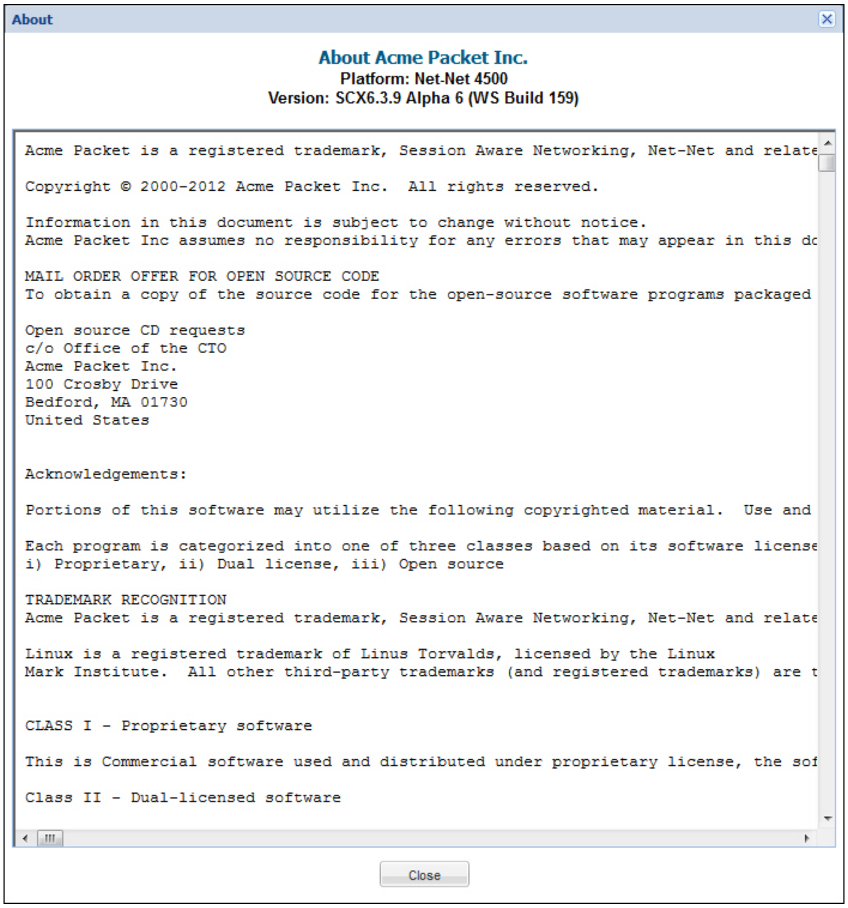
You can display information about the Net-Net SBC you are currently logged into via the Web-based GUI. You can access “About” from any main report summary page.

To display the “About” information:

1. From any main report summary page, click the “**About**” link in the upper right corner on the page.



The following information displays.



About

About Acme Packet Inc.
Platform: Net-Net 4500
Version: SCX6.3.9 Alpha 6 (WS Build 159)

```
Acme Packet is a registered trademark, Session Aware Networking, Net-Net and relate

Copyright © 2000-2012 Acme Packet Inc.  All rights reserved.

Information in this document is subject to change without notice.
Acme Packet Inc assumes no responsibility for any errors that may appear in this dc

MAIL ORDER OFFER FOR OPEN SOURCE CODE
To obtain a copy of the source code for the open-source software programs packaged

Open source CD requests
c/o Office of the CTO
Acme Packet Inc.
100 Crosby Drive
Bedford, MA 01730
United States


Acknowledgements:

Portions of this software may utilize the following copyrighted material.  Use and

Each program is categorized into one of three classes based on its software license
i) Proprietary, ii) Dual license, iii) Open source

TRADEMARK RECOGNITION
Acme Packet is a registered trademark, Session Aware Networking, Net-Net and relate

Linux is a registered trademark of Linus Torvalds, licensed by the Linux
Mark Institute.  All other third-party trademarks (and registered trademarks) are t


CLASS I - Proprietary software

This is Commercial software used and distributed under proprietary license, the sof

Class II - Dual-licensed software
```

This box displays the following about the Net-Net SBC you are currently logged into:

- Net-Net Platform type (3800, 4500, Server Edition, or Virtual Machine Edition)
- Version Number of software (including Build Number)
- Trademark Recognition
- Copyright
- Open Source Mailing Address
- Acknowledgements
- Relevant Proprietary and Open Source Licenses

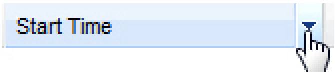
2. Click <**Close**> to close the box.

Customizing the Page Display

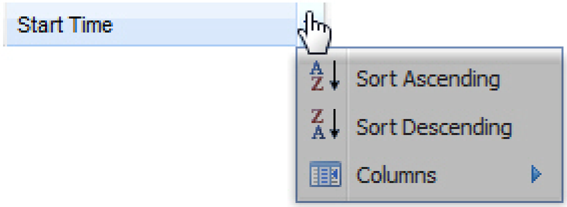
You can customize the data presented in the SM& T pages by changing whether or not specific columns display and how they display. You can also sort the order of item entries.

To customize the page display within any report:

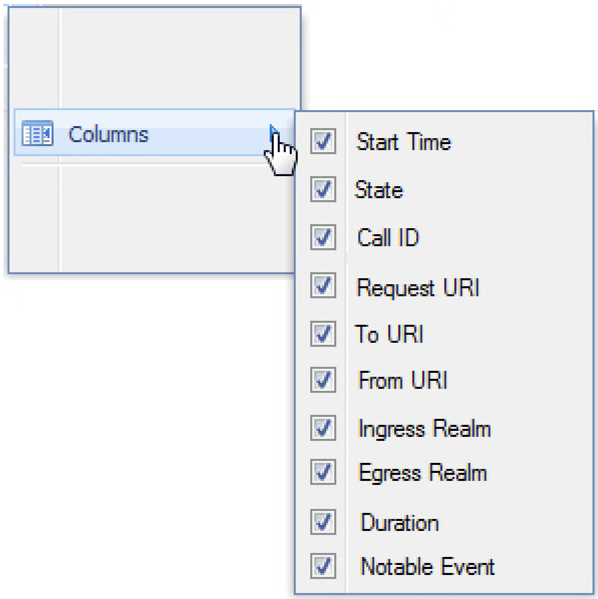
1. Position the cursor over a column heading. A pointer displays on the right hand side of the box. For example:



2. Click the down arrow to display the menu. For example:



3. Click “**Sort Ascending**” to sort the data in the table in ascending order.
4. Click “**Sort Descending**” to sort the data in the table in descending order.
5. Click “**Columns**” to access and customize a list of column names. For example:



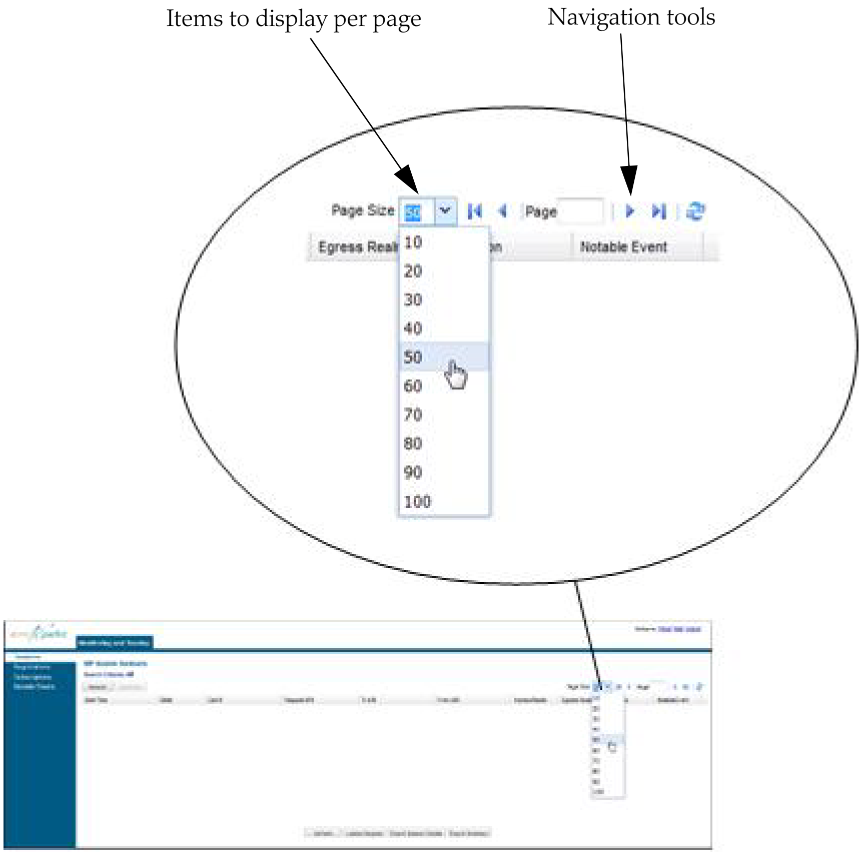
6. Place a checkmark in the box to display that heading/column in the window. Remove the checkmark to hide the heading/column in the window.
7. Click “**Group By This Field**” to group all items in the list according to the column head you currently have selected. For example, if you select the “Site” column heading, and then select “Group By This Field”, all items in the list are grouped by Site.
8. For the “**Show in Groups**” option, place a checkmark in the box to show the current heading in the group when you select “Group By This Field”. Remove the checkmark to hide the current heading when “Group By This Field” is selected.
9. To close the heading menus, click anywhere in the window.

Changing Number of Data Items on the Page

By default, 50 data items are shown per page. You can change the number of items viewed for all tables in Trunk Manager.

To change the number of data items displayed:

1. At the top right corner of the window, click the down arrow next to **Size**. The drop down list of values appears.

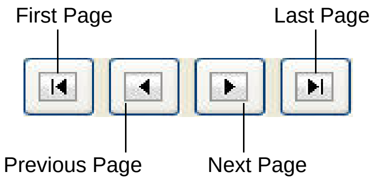


2. Click the number of data items you want to display per page. Default is **50**. Valid values are **10** to **100** in increments of 10.

Navigating Pages

To navigate through multiple pages:

1. Use the navigation arrows located at the top right corner of the window to navigate through multiple pages.
2. Click the navigation icons to display the desired page, such as the first page, previous page, next page, and the last page of Events list view.



Refresh

To refresh the page:

1. Click the <**Refresh**> button at the bottom of the page.

   or

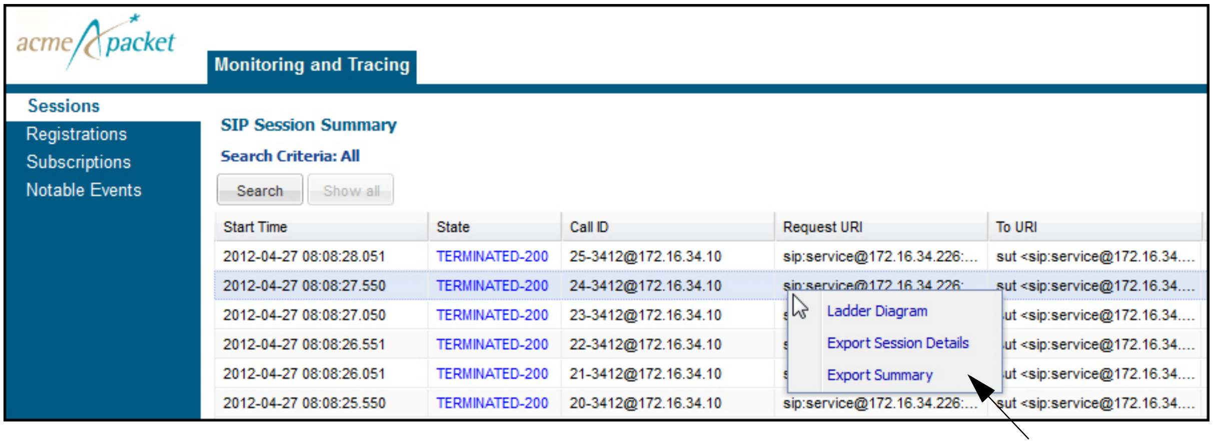
   Click the 🔄 in the upper right corner of the page.

Pop-up Context Menu

All reports (Sessions, Registrations, Subscriptions, and Notable Events) support a pop-up context menu that you can use to select a Ladder diagram, Export Session Details, and Export Session Summary. You display the pop-up context menu by selecting a record and right clicking to show a menu.

To display the pop-up context menu in any report:

1. Click on a record in the report page.



SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	To URI
2012-04-27 08:08:28.051	TERMINATED-200	25-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:27.550	TERMINATED-200	24-3412@172.16.34.10	sip:service@172.16.34.226:	sut <sip:service@172.16.34....
2012-04-27 08:08:27.050	TERMINATED-200	23-3412@172.16.34.10	s	ut <sip:service@172.16.34....
2012-04-27 08:08:26.551	TERMINATED-200	22-3412@172.16.34.10	s	ut <sip:service@172.16.34....
2012-04-27 08:08:26.051	TERMINATED-200	21-3412@172.16.34.10	s	ut <sip:service@172.16.34....
2012-04-27 08:08:25.550	TERMINATED-200	20-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....

Pop-up Context Menu

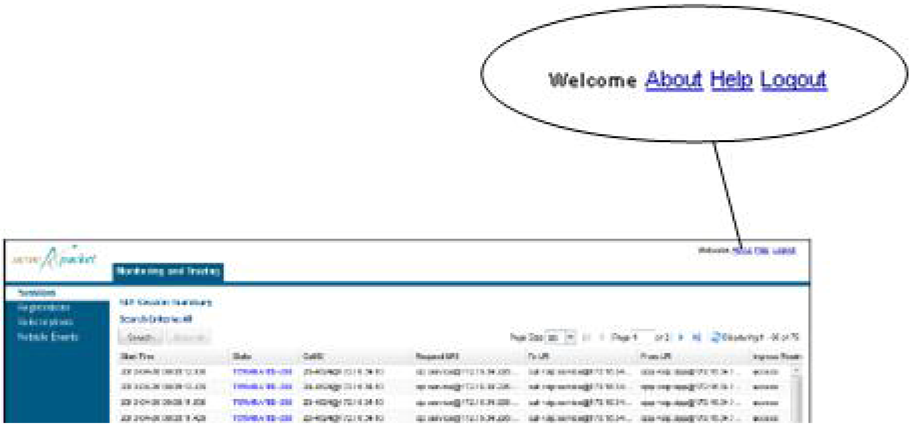
2. Right-click the mouse to display the pop-up context menu.
3. Drag the mouse to an option on the menu and left-click the mouse to select it. The applicable page displays or the export begins, depending on the option you selected (Ladder Diagram, Export Session Details, or Export Summary).

Help Menu

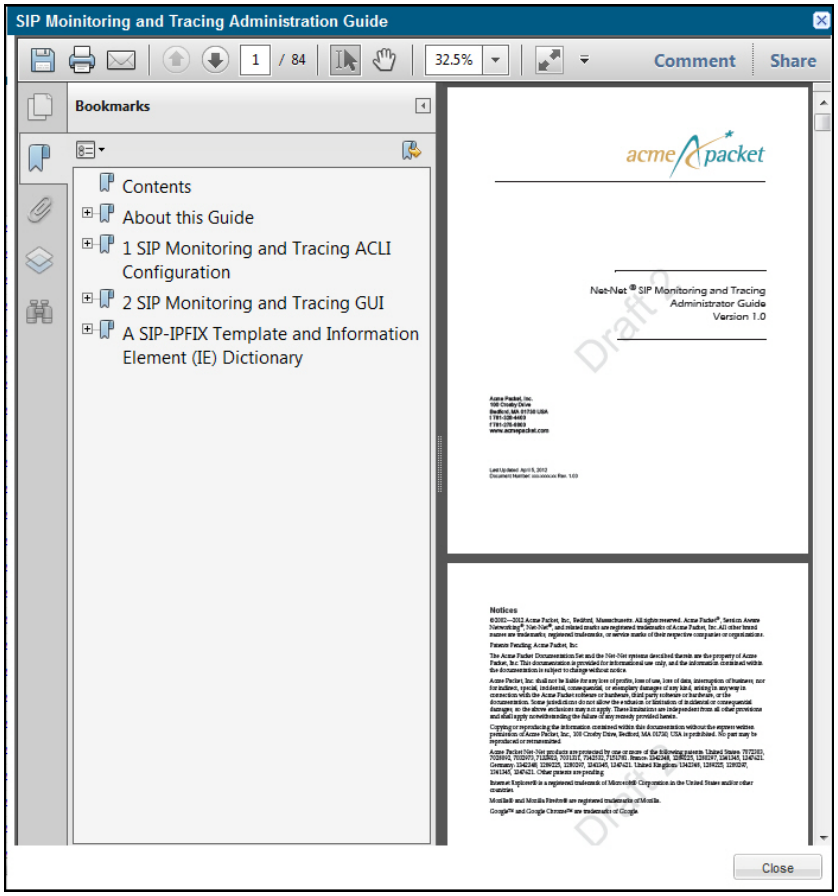
The Web-based GUI provides online help for all of the pages within the GUI. You can access help from any page by clicking the “**Help”** link in the upper right corner of the page.

To display Help:

1. From any main report summary page, click the “**Help**” link in the upper right corner on the page.



The applicable help for the current page displays in a pop-up window.


SIP Moinitoring and Tracing Administration Guide
1 / 84
32.5%
Comment
Share
Bookmarks
Contents
About this Guide
1 SIP Monitoring and Tracing ACLI Configuration
2 SIP Monitoring and Tracing GUI
A SIP-IPFIX Template and Information Element (IE) Dictionary
acme packet
Net-Net® SIP Monitoring and Tracing Administrator Guide Version 1.0
Draft
Notices
Close

2. Click <**Close**> to close the box.

   or

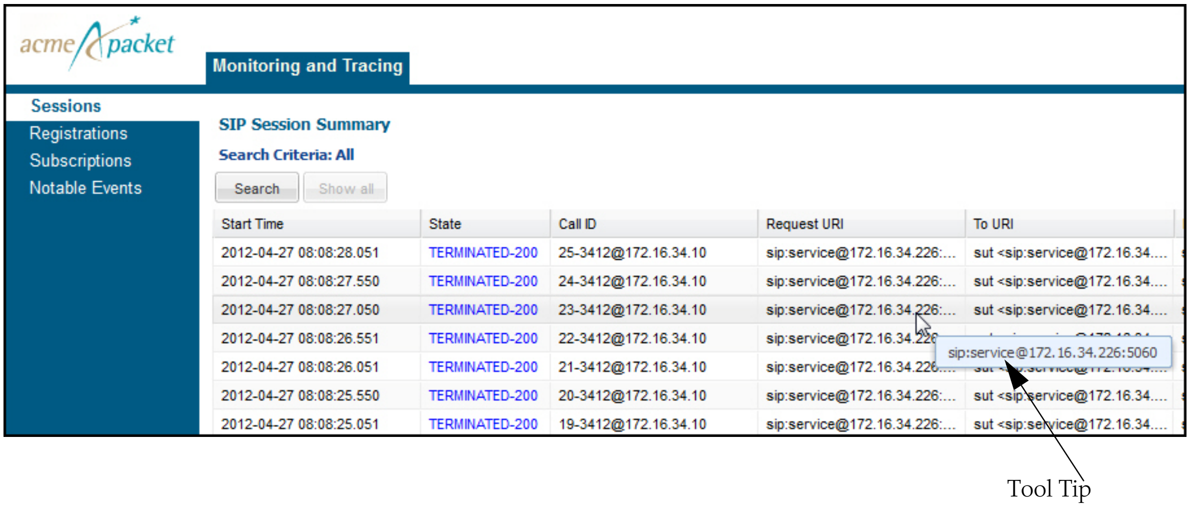
   Click the “**X**” in the upper right corner of the pop-up window.

Tool-Tip Help

Throughout the Web-based GUI, you can scroll over a record within a summary report and display quick information about that record in a temporary pop-up box. This allows you to view a summarized version of help for that record.

To view a tool-tip help:

1. From any main report summary page, use the mouse to scroll over a record in a summary report.



SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	To URI
2012-04-27 08:08:28.051	TERMINATED-200	25-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:27.550	TERMINATED-200	24-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:27.050	TERMINATED-200	23-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:26.551	TERMINATED-200	22-3412@172.16.34.10	sip:service@172.16.34.226	[illegible]
2012-04-27 08:08:26.051	TERMINATED-200	21-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:25.550	TERMINATED-200	20-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....
2012-04-27 08:08:25.051	TERMINATED-200	19-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16.34....

A blue-shaded box displays allowing you to view quick help about the record.

2. To close the tool-tip, scroll off of the record.

   or

   Click at another location within the summary report.

   Note: Ladder diagrams for a specific record also display tool tip summary information. For more information, see Ladder Diagram (120).

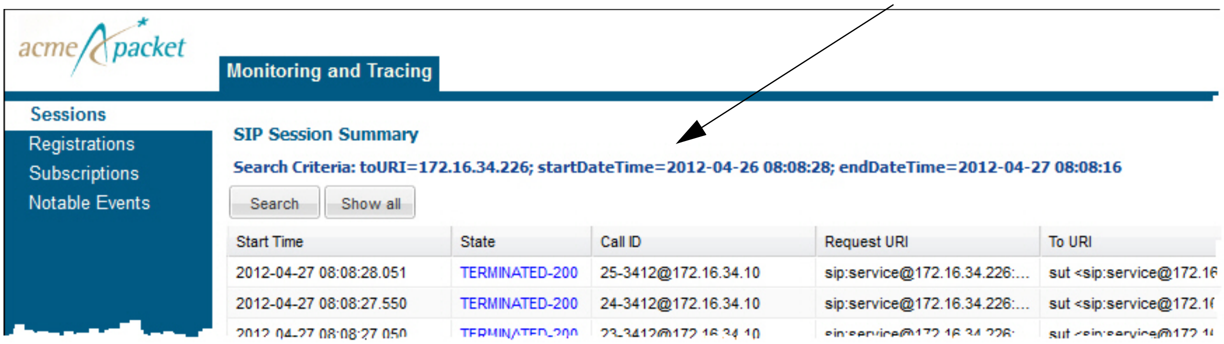
Search for a Record

The <**Search**> button at the top of the report page allows you to perform a search to find a specific record(s) within a report (Sessions, Registrations, Subscriptions, Notable Events). It also allows you to specify criteria on which to perform the search.

After defining a search criteria in the "**Search Filter**" dialog box, clicking <**Search**>, automatically populates the report page with the records that match the criteria you specified. The search performs the filtering process of criteria dependent on the report page from which you are running the search.

For example, performing a search from the Sessions report page displays only the reports pertaining to call sessions. If you performed a search on the Registration report page, only the reports pertaining to call registrations displays on the report page. The search string containing the criteria on which you performed the search, displays in the top left corner of the page.

Search String



SIP Session Summary

Search Criteria: toURI=172.16.34.226; startDateTime=2012-04-26 08:08:28; endDateTime=2012-04-27 08:08:16

Start Time	State	Call ID	Request URI	To URI
2012-04-27 08:08:28.051	TERMINATED-200	25-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.16
2012-04-27 08:08:27.550	TERMINATED-200	24-3412@172.16.34.10	sip:service@172.16.34.226:...	sut <sip:service@172.1(
2012-04-27 08:08:27.050	TERMINATED-200	23-3412@172.16.34.10	sip:service@172.16.34.226:	sut <sip:service@172.1(

The search criteria is saved until you click <**Reset**> in the dialog box, or until you log out of the HTTP session.

To perform a search:

Note:
1. You can specify a value for any or all of the fields in the Search box. The search process searches for records with all of the values you specify and displays only the records with these values. If you perform a "Global Search", AND specify values in other fields, the search process searches the other specified fields first and then filters on the "Global Search" field.

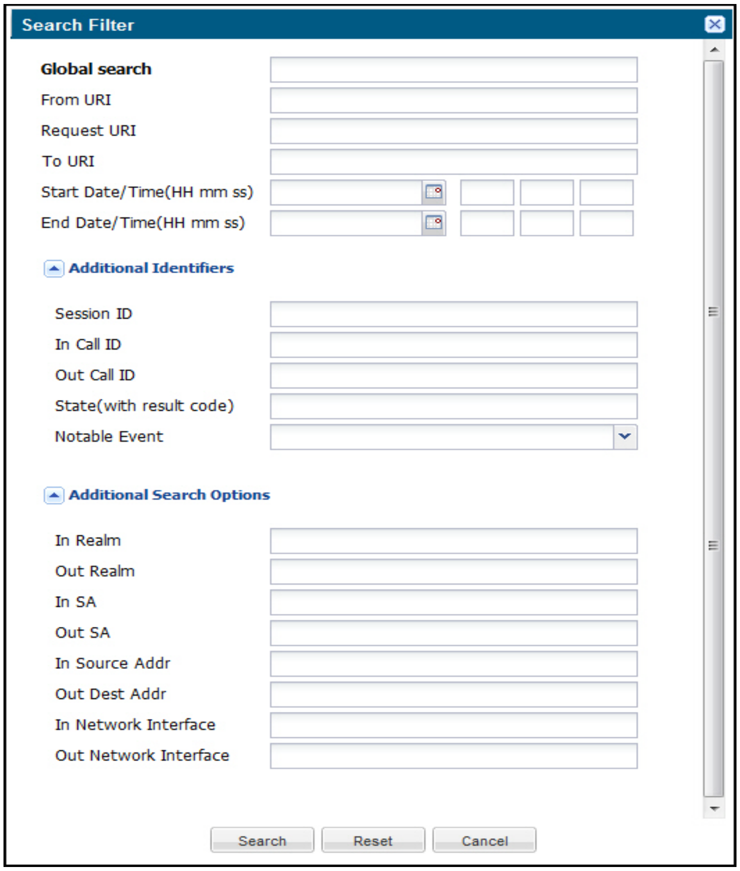
2. If you specify a "*" in a search string, the search is performed on that exact string. For example, if you search for "123*45", the search shows results for all strings containing "123*45".

3. You can use quotes (" ") to specify a search. For example, you can enter "Smith" and the search finds all of the records that match "Smith", such as:

```
John Smithfield<sip:sipp@192.168.1.70:5070>;tag=12260SIPpTag001
```

If you enter a space before or after a quotation mark, (for example, "Smith "), the search returns no data.

1. In any reports page, click <**Search**>.
2. The following dialog box displays.



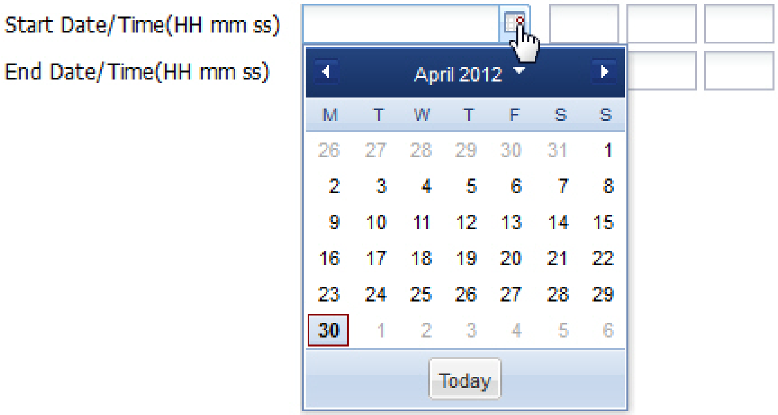
3. In the “**Global Search**” field, specify a string to search all parameters in all records. Valid values are alpha-numeric characters.

   Note: The “Global Search” option searches all parameters in all the session records stored in memory. All values you specify in other fields are searched **before** the value specified in the “Global Search” field is used.

4. In the “**From URI**” field, enter the URI formatted string of the call source information you are searching. Valid values are alpha-numeric characters. For example, sipp<sip:sipp@172.16.34.10:5060;tag=24.
5. In the “**Requested URI**” field, enter the URI formatted string that contains a protocol, name, location, or any other applicable characteristic, that is sent by the Net-Net SBC in the REQUEST header. Valid values are alpha-numeric characters. For example, sip:service@172.16.34.226:5060.
6. In the “**To URI**” field, enter URI formatted string of the call destination information you are searching. Valid values are alpha-numeric characters. For example, sut<sip:service@172.16.34.226:5060;tag=99.
7. In the “**Start Date/Time (HH mm ss)**” field, enter a starting date to search on in the first text box in the format YYYY-MM-DD (where Y =year, M=month, and D=day).

   or

   Click on the calendar icon in this field to display a calendar from which you can select a date. Navigate the calendar to find the date you want and click on it to enter it into this field, or click <**Today**> to enter today’s date. For example, 2012-04-15 would search for all records starting on April 15, 2012. Valid values are numeric characters only.



Start Date/Time(HH mm ss)

End Date/Time(HH mm ss)

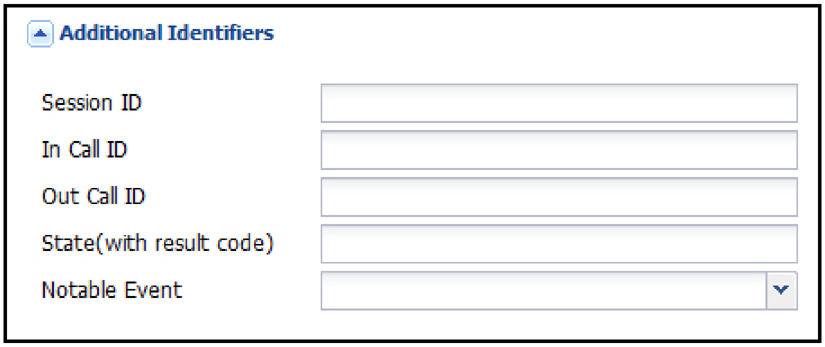
April 2012

M	T	W	T	F	S	S
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

   Enter a start time to search on in the last three text boxes in the format HH mm ss (where H=hour, m=minutes, and s=seconds). For example, 01 30 45 would search for all records starting at 1:30 and 45 seconds. Valid value are numeric characters only.

8. In the “**End Date/Time (HH mm ss)**” field, repeat the process of entering a date and time as provided in Step 7.
9. To search on additional parameters, click on the “**Additional Identifiers**” down arrow to expand the dialog box.

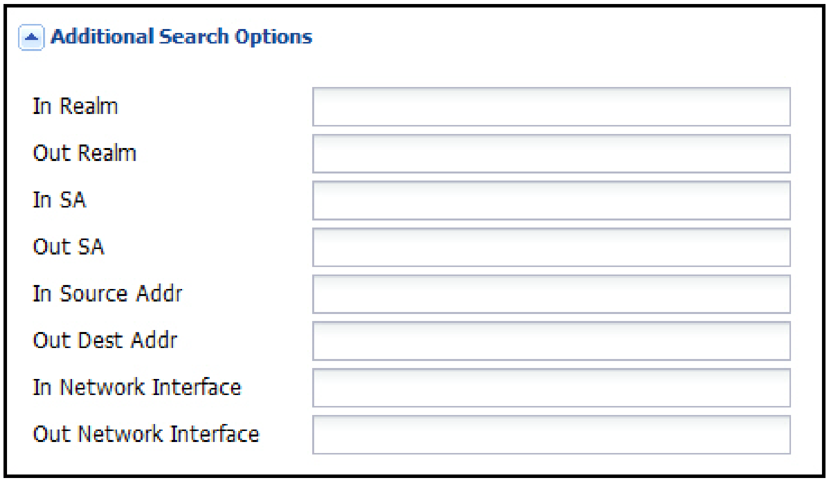
Additional Identifiers



10. In the “**Session Id**” field, enter the ID of the call session you want to search. Valid values are alpha-numeric characters. For example, 22-3412@172.16.34.1.
11. In the “**In Call ID**” field, enter the ID of the incoming call (phone number and source IP address). Valid values are alpha-numeric characters. For example, 25-3412@172.16.34.10.
12. In the “**Out Call ID**” field, enter the ID of the outgoing call (phone number and IP address). Valid values are alpha-numeric characters. For example, 14-3412@172.14.54.6.
13. In the “**State (with result code)**” field, enter the status of the call session with the result code for which you want to search. Valid values are (case-sensitive):
    - INITIAL-<result code>
    - EARLY-<result code>
    - ESTABLISHED-<result code>
    - TERMINATED-<result code>
    - FAILED-<result code>

    Result codes can range from 1xx to 5xx. For example, terminated-200, or failed-400. For a description of each state, see the table on page 117.
14. In the “**Notable Event**” field, select the notable event for which you want to search. Valid values are:
    - any-event - search displays any notable event that was stored in memory.
    - short-session - search displays only records that indicate a short-session duration has occurred.
    - local-rejection - search displays only records that indicate a local-rejection has occurred.
15. To search on additional parameters, click on the “**Additional Search Options**” down arrow to expand the dialog box.

Additional Search Options



Additional Search Options

In Realm

Out Realm

In SA

Out SA

In Source Addr

Out Dest Addr

In Network Interface

Out Network Interface

16. In the “**In Realm**” field, enter the name of the realm for which the incoming call belongs. Valid values are alpha-numeric characters. For example, “access”.
17. In the “**Out Realm**” field, enter the name of the realm for which the outgoing call belongs. Valid values are alpha-numeric characters. For example, “backbone”.
18. In the “**In SA**” field, enter the name of the session agent (SA) on the incoming call session. Valid values are alpha-numeric characters. For example, “SA1”.
19. In the “**Out SA**” field, enter the name of the session agent (SA) on the outgoing call session. Valid values are alpha-numeric characters. For example, “SA2”.
20. In the “**In Source Addr**” field, enter the source IP address of the SA that accepted the incoming call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, “172.45.6.7”.
21. In the “**Out Dest Addr**” field, enter the destination IP address of the SA that accepted the outgoing call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, “172.64.56.7”.
22. In the “**In Network Interface**” field, enter the incoming core network interface that connects the Net-Net SBC to your network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.7.
23. In the “**Out Network Interface**” field, enter the outgoing network interface that connects your Net-Net SBC to the outside network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.8.
24. Click <**Search**> to perform the search with the values you specified. A list of the records that the search process filtered, display in the window.

    The Web-based GUI saves the search specifications until you click <**Reset**> in the search dialog box, OR until you log out of the Web-based GUI.

Exporting Information to a Text File

The Web-based GUI allows you to export information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The data exports to a file that you can open and view as required.

You can export any of the following:

- All information from each report
- Information from a specific record only
- Information from a search result
- Information from a Ladder Diagram

The following table identifies the buttons to use to export specific information from the Web-based GUI. All the export buttons in the GUI export to text files.

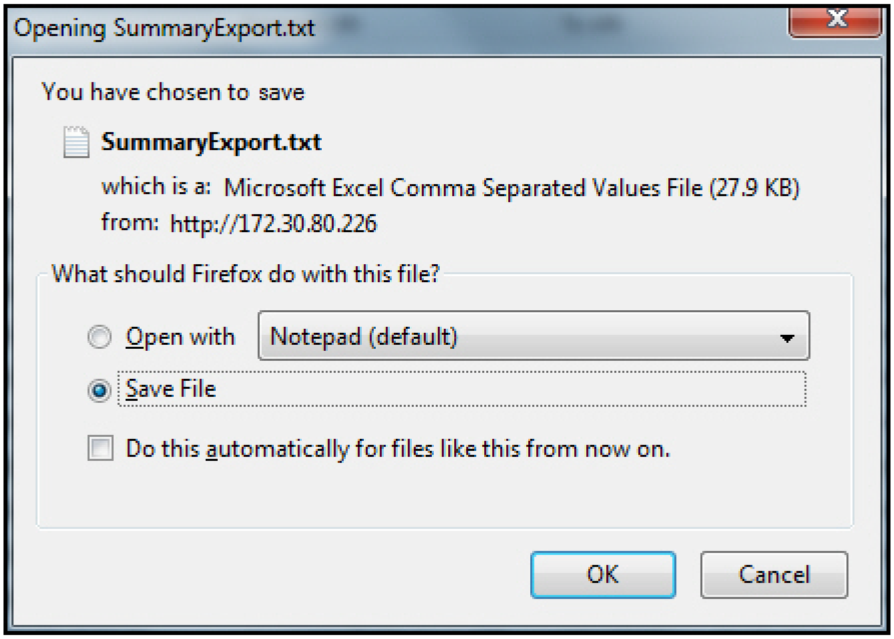
Button	Description
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:	
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine. **Note:** This button exports ALL call session summary records or the records that matched a search criteria to the file.
From the Ladder Diagram:	
Export Diagram	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to an HTML file format on the local machine.
Export Session Details	Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a file in text format on the local machine.

The following procedure is an example of using the export buttons in the Web-based GUI:

To export information to a text file:

1. In the applicable Report window or Ladder Diagram window, click the appropriate “Export” button. The following example illustrates that the <**Export Summary**> button was clicked on a report page.

The following prompt displays.\



Opening SummaryExport.txt

You have chosen to save

SummaryExport.txt

which is a: Microsoft Excel Comma Separated Values File (27.9 KB)
from: http://172.30.80.226

What should Firefox do with this file?

○ Open with Notepad (default)

● Save File

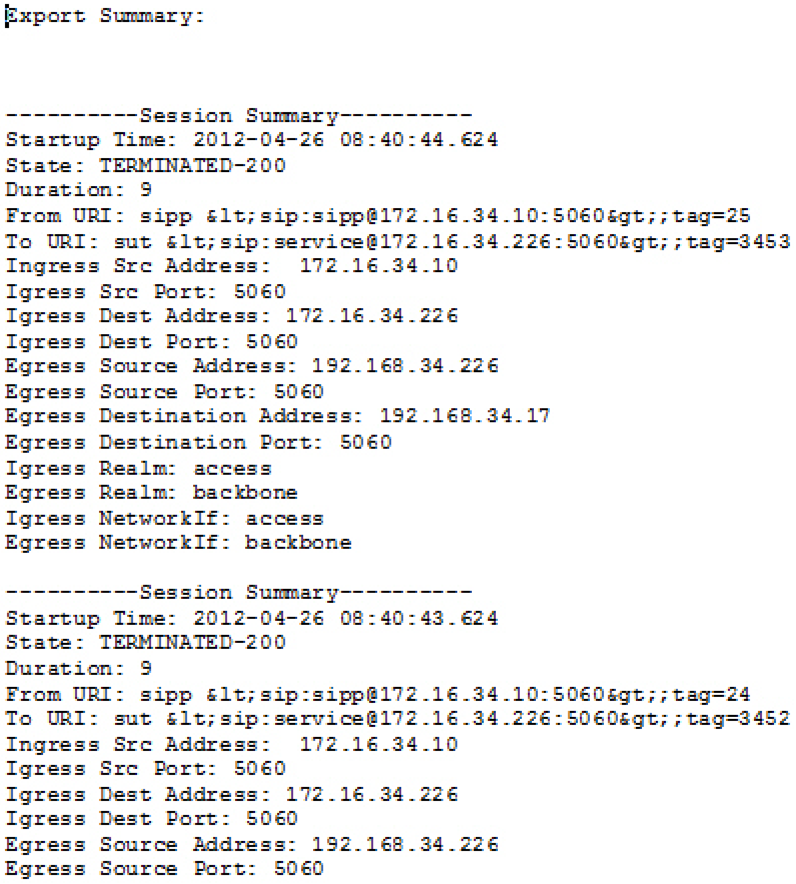
☐ Do this automatically for files like this from now on.

The Web-based GUI assigns the file name for the text file (shown as "*SummaryExport.txt*" in the illustration above.)

Note: The Web-based GUI exports Ladder Diagrams as HTML files.

2. Click "**Open with**" and select the application for which to open the resulting text file.
   or
   Click "**Save File**" to save the text file to your local PC.
3. Click <**OK**> to export the session or media information to the text file.

   The following illustration shows a partial summary of the Sessions Report exported to a text file and opened using Microsoft Word™. For additional examples of exported files, see Format of Exported Text Files (169).



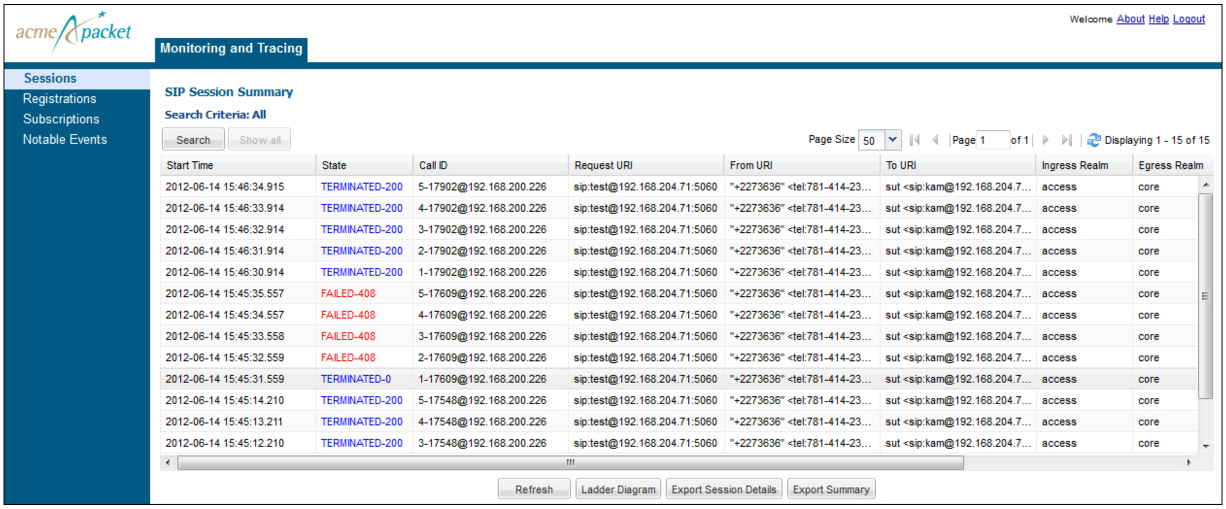
```
Export Summary:



----------Session Summary----------
Startup Time: 2012-04-26 08:40:44.624
State: TERMINATED-200
Duration: 9
From URI: sipp &lt;sip:sipp@172.16.34.10:5060&gt;;tag=25
To URI: sut &lt;sip:service@172.16.34.226:5060&gt;;tag=3453
Ingress Src Address:  172.16.34.10
Igress Src Port: 5060
Igress Dest Address: 172.16.34.226
Igress Dest Port: 5060
Egress Source Address: 192.168.34.226
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone

----------Session Summary----------
Startup Time: 2012-04-26 08:40:43.624
State: TERMINATED-200
Duration: 9
From URI: sipp &lt;sip:sipp@172.16.34.10:5060&gt;;tag=24
To URI: sut &lt;sip:service@172.16.34.226:5060&gt;;tag=3452
Ingress Src Address:  172.16.34.10
Igress Src Port: 5060
Igress Dest Address: 172.16.34.226
Igress Dest Port: 5060
Egress Source Address: 192.168.34.226
Egress Source Port: 5060
```

Session Reports

The Session Report is a SIP session summary of all logged call sessions on the Net-Net SBC. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net SBC.

> **Note:** For setting filters to capture applicable data, see Filters to Configure (67).

The columns that display on the Session Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (104).



SIP Session Summary

Search Criteria: All

Page Size 50 | Page 1 of 1 | Displaying 1 - 15 of 15

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm
2012-06-14 15:46:34.915	TERMINATED-200	5-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:33.914	TERMINATED-200	4-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:32.914	TERMINATED-200	3-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:31.914	TERMINATED-200	2-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:30.914	TERMINATED-200	1-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:31.559	TERMINATED-0	1-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media session. Valid values are: • INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. • EARLY Session received the first provisional response (1xx other than 100). • ESTABLISHED Session for which a success (2xx) response was received. • TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session remains in the terminated state until all the resources for the session are freed up. • FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net SBC in REQUEST headers.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.

Heading	Description
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Duration	Amount of time, in seconds, that the call or media event was active.
Notable Event	Indicates if a “notable event” has occurred on the call session. Valid values are: • **short session** - Sessions that don’t meet a minimum configurable duration threshold; Session dialogue, captured media information and termination signalling; Any event flagged as a short session interesting event • **local rejection** - Sessions locally rejected at the Net-Net SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Calling Pkts	Number of packets that occurred during outbound calling media traffic.
Called Pkts	Number of packets that occurred during inbound called media traffic.
Calling R Factor	Average Quality of Service (QoS) factor observed during the incoming call session. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This column defines the call or transmission quality expressed as an R factor.
Called RFactor	QoS factor observed during the outgoing call session. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This column defines the call or transmission quality expressed as an R factor.
Calling MOS	A measure of voice quality for an incoming media stream.
Called MOS	A measure of voice quality for an outgoing media stream.

The following table describes the buttons on this page.

Button	Description
Refresh	Performs a refresh of the page and updates it with the latest data.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.
Refresh	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.

Note: For information about the Export buttons on this page, see Exporting Information to a Text File (114).

To display a Session Report:

1. After logging into the Web-based GUI, click "**Sessions**" in the left column. The session summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

   For information about Refresh, see Refresh (106).
   For information about the Ladder Diagram, see Ladder Diagram (120).
   For information about exporting information, see Exporting Information to a Text File (114).

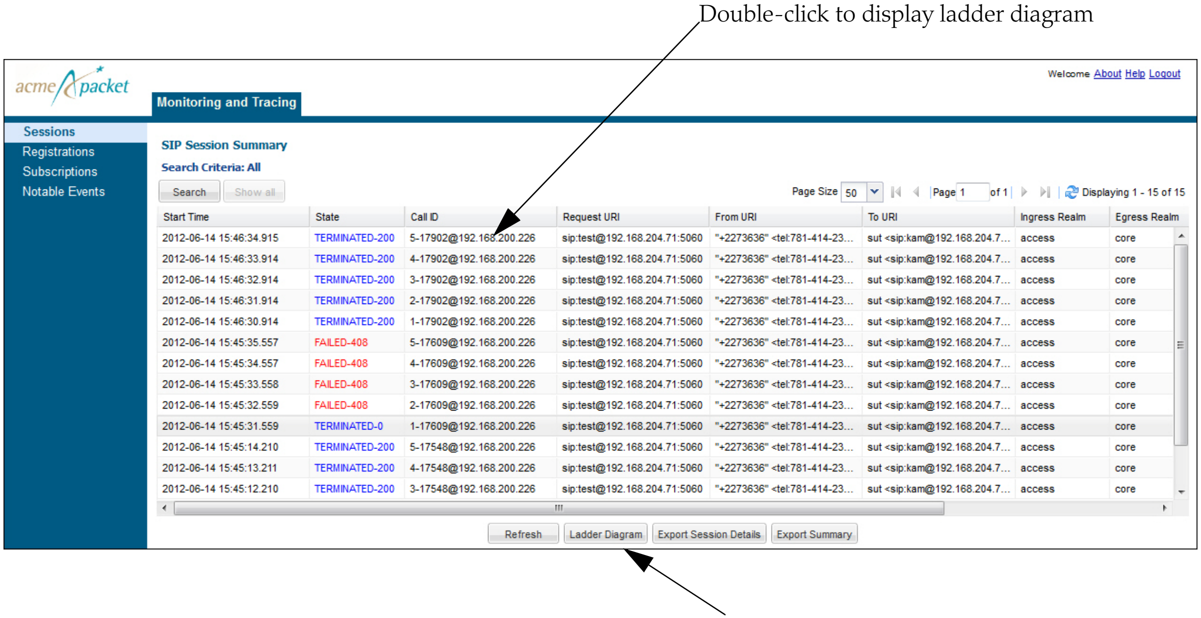
Ladder Diagram

Ladder diagrams in the Web-based GUI are logical schematics that show the call and media flow of packets on ingress and egress routes via the Net-Net SBC.

Ladder diagrams for the Session Report display the following session summary information:

- Quality of Service (QoS) statistics for call sessions
- SIP messages and media events in time sequence

To display a ladder diagram for a specific record in the Session Report, you can double-click a record in the summary table OR click <**Ladder Diagram**> on the Session Report page.



Double-click to display ladder diagram

SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm
2012-06-14 15:46:34.915	TERMINATED-200	5-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:33.914	TERMINATED-200	4-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:32.914	TERMINATED-200	3-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:31.914	TERMINATED-200	2-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:46:30.914	TERMINATED-200	1-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:31.559	TERMINATED-0	1-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core

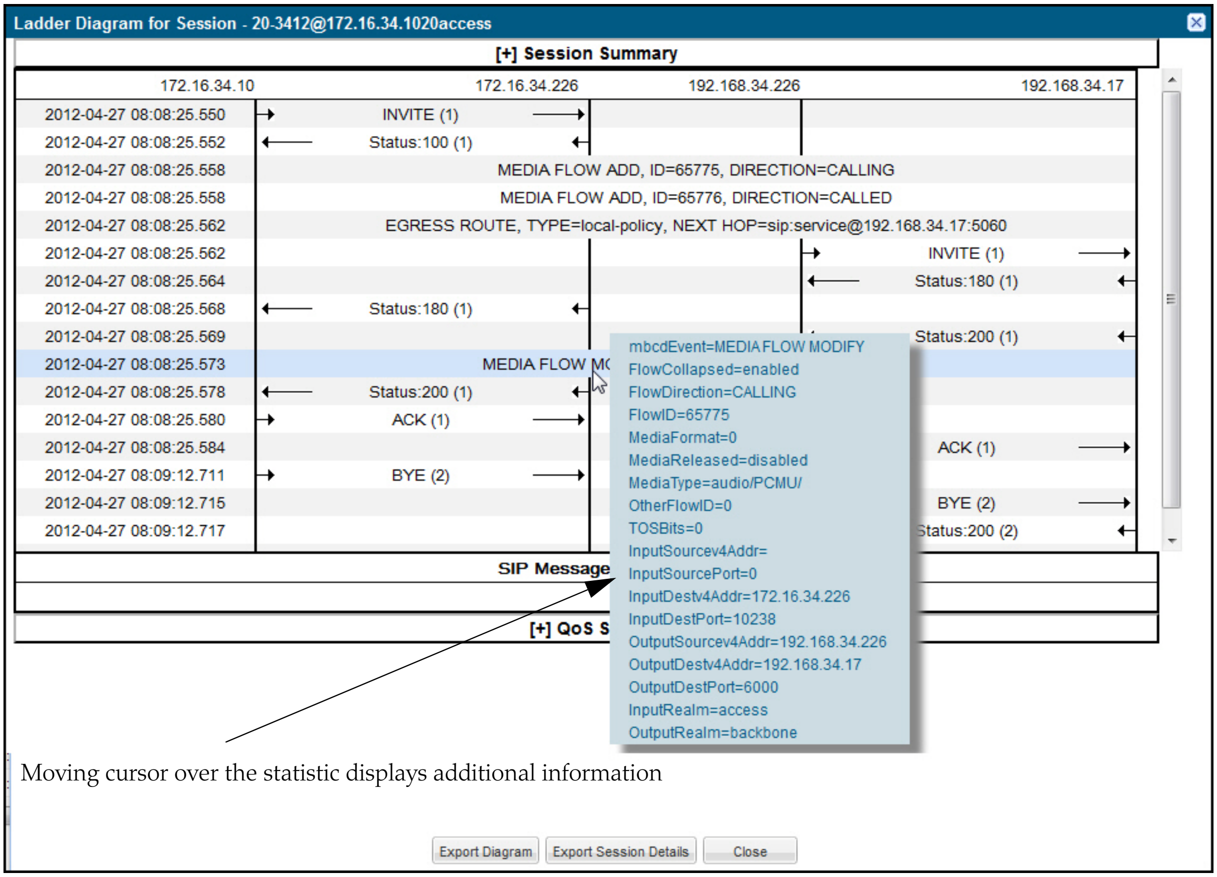
Or click <**Ladder Diagram**>

To display a ladder diagram:

1. On the Sessions Report page, click <**Ladder Diagram**>.

   or

   Select a record in the table and double-click on that record. The following is an example of the ladder diagram that displays.



Ladder Diagram for Session - 20-3412@172.16.34.1020access

[+] Session Summary

```
                      172.16.34.10         172.16.34.226        192.168.34.226            192.168.34.17
2012-04-27 08:08:25.550   →        INVITE (1)        →
2012-04-27 08:08:25.552   ←        Status:100 (1)    ←
2012-04-27 08:08:25.558          MEDIA FLOW ADD, ID=65775, DIRECTION=CALLING
2012-04-27 08:08:25.558          MEDIA FLOW ADD, ID=65776, DIRECTION=CALLED
2012-04-27 08:08:25.562     EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:service@192.168.34.17:5060
2012-04-27 08:08:25.562                                                →     INVITE (1)       →
2012-04-27 08:08:25.564                                                ←     Status:180 (1)   ←
2012-04-27 08:08:25.568   ←        Status:180 (1)    ←
2012-04-27 08:08:25.569                                                      Status:200 (1)   ←
2012-04-27 08:08:25.573            MEDIA FLOW MC
2012-04-27 08:08:25.578   ←        Status:200 (1)    ←
2012-04-27 08:08:25.580   →        ACK (1)           →
2012-04-27 08:08:25.584                                                      ACK (1)          →
2012-04-27 08:09:12.711   →        BYE (2)           →
2012-04-27 08:09:12.715                                                      BYE (2)          →
2012-04-27 08:09:12.717                                                      Status:200 (2)   ←
```

SIP Message

[+] QoS S

```
mbcdEvent=MEDIA FLOW MODIFY
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65775
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.226
InputDestPort=10238
OutputSourcev4Addr=192.168.34.226
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
OutputRealm=backbone
```

Moving cursor over the statistic displays additional information

The Session Record Ladder Diagram consists of the following information:

- **Session Summary** - summary information about the call or media session in focus. For more information, see Session Summary (122).
- **SIP Message Details** - SIP message and call flow information about the call or media session in focus. For more information, see SIP Message Details (123).
- **QoS Statistics** - Quality of Service (QoS) statistic information about the call or media session in focus. For more information, see QoS Statistics (124).

You can move your mouse over any statistic in the Ladder Diagram to view additional parameters and associated values for the statistic in a pop-up window.

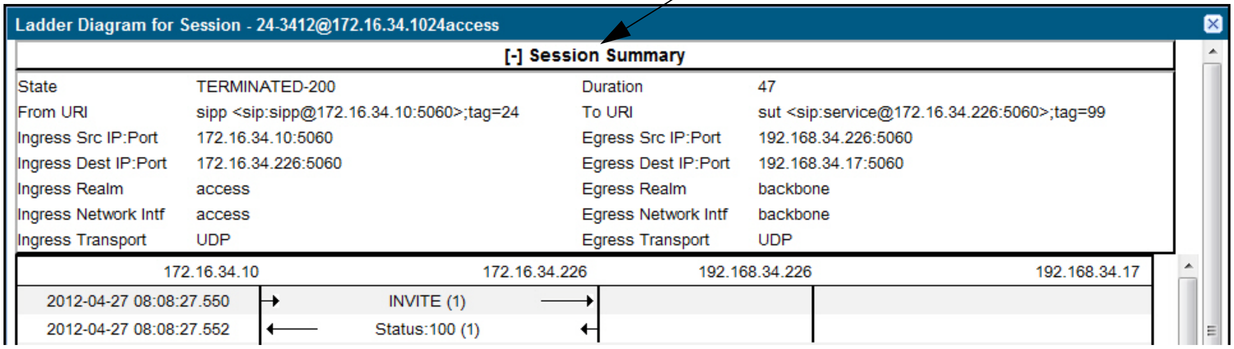
The following table describes the buttons in this Ladder Diagram window.

Button	Description
Export Diagram	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to a file in text format on the local machine.
Export Session Details	Exports detailed information about the SIP messages and media events associated with the session in focus, to a file in text format on the local machine.
Close	Closes the Ladder Diagram window.

Note: For information about the Export buttons on this page, see Exporting Information to a Text File (114).

Session Summary

The Session Summary window in the Ladder Diagram displays an overall summary of the call or media session in focus.



Session Summary

Ladder Diagram for Session - 24-3412@172.16.34.1024access

[-] Session Summary

State	TERMINATED-200	Duration	47
From URI	sipp <sip:sipp@172.16.34.10:5060>;tag=24	To URI	sut <sip:service@172.16.34.226:5060>;tag=99
Ingress Src IP:Port	172.16.34.10:5060	Egress Src IP:Port	192.168.34.226:5060
Ingress Dest IP:Port	172.16.34.226:5060	Egress Dest IP:Port	192.168.34.17:5060
Ingress Realm	access	Egress Realm	backbone
Ingress Network Intf	access	Egress Network Intf	backbone
Ingress Transport	UDP	Egress Transport	UDP

	172.16.34.10	172.16.34.226	192.168.34.226	192.168.34.17
2012-04-27 08:08:27.550	INVITE (1)			
2012-04-27 08:08:27.552	Status:100 (1)			

To display the Session Summary:

1. In the Ladder Diagram, click the **[+]** next to "**Session Summary**" at the top of the Ladder Diagram window. The Session Summary window expands. This window displays a summary of information about the call or media session in focus.

   The following table describes each field in the Session Summary window.

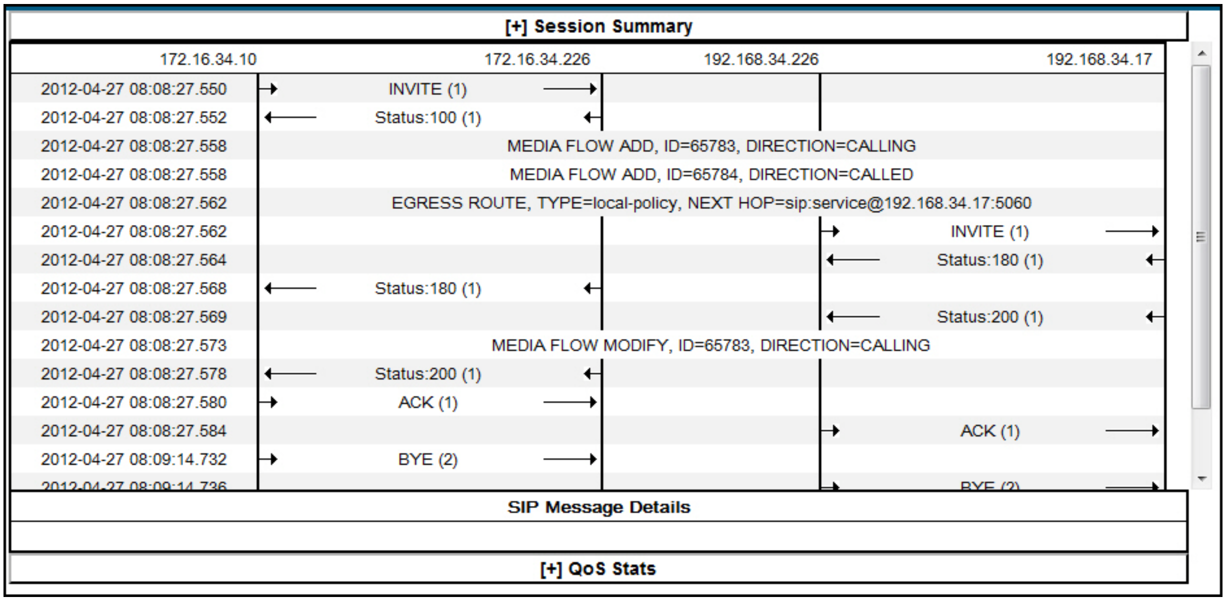
Heading	Description
State	Status of the call or media session. Valid values are: • INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. • EARLY Session received the first provisional response (1xx other than 100). • ESTABLISHED Session for which a success (2xx) response was received. • TERMINATED Session that has ended by receiving or sending a BYE for an "Established" session or forwarding an error response for an "Initial" or "Early" session. The session remains in the terminated state until all the resources for the session are freed up. • FAILED Session that has failed due to a 4xx or 5xx error code.
Duration	Amount of time, in seconds, that the call or media session was active.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Ingress Src IP:Port	Source IP address and port number of the incoming call or media session.
Egress Src IP: Port	Source IP address and port number of the outgoing call or media session.
Ingress Dest IP:Port	Destination IP address and port number of the incoming call or media session.
Egress Dest IP: Port	Destination IP address and port number of the outgoing call or media session.

Heading	Description
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Ingress Network Intf	Name of the incoming network interface on the Net-Net SBC.
Egress Network Intf	Name of the outgoing network interface on the Net-Net SBC.
Ingress Transport	Protocol type used on the incoming call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).
Egress Transport	Protocol type used on the outgoing call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).

2. Click **[-]** to close the “Session Summary” window.

SIP Message Details

The SIP Message Detail window displays detailed information and data flow (ingress and egress) about the call or media event.



	172.16.34.10 → 172.16.34.226	192.168.34.226 → 192.168.34.17
2012-04-27 08:08:27.550	INVITE (1) →	
2012-04-27 08:08:27.552	← Status:100 (1)	
2012-04-27 08:08:27.558	MEDIA FLOW ADD, ID=65783, DIRECTION=CALLING	
2012-04-27 08:08:27.558	MEDIA FLOW ADD, ID=65784, DIRECTION=CALLED	
2012-04-27 08:08:27.562	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:service@192.168.34.17:5060	
2012-04-27 08:08:27.562		INVITE (1) →
2012-04-27 08:08:27.564		← Status:180 (1)
2012-04-27 08:08:27.568	← Status:180 (1)	
2012-04-27 08:08:27.569		← Status:200 (1)
2012-04-27 08:08:27.573	MEDIA FLOW MODIFY, ID=65783, DIRECTION=CALLING	
2012-04-27 08:08:27.578	← Status:200 (1)	
2012-04-27 08:08:27.580	ACK (1) →	
2012-04-27 08:08:27.584		ACK (1) →
2012-04-27 08:09:14.732	BYE (2) →	
2012-04-27 08:09:14.736		BYE (2) →

To display SIP Message Details:

On the Sessions Report page, click <**Ladder Diagram**>.

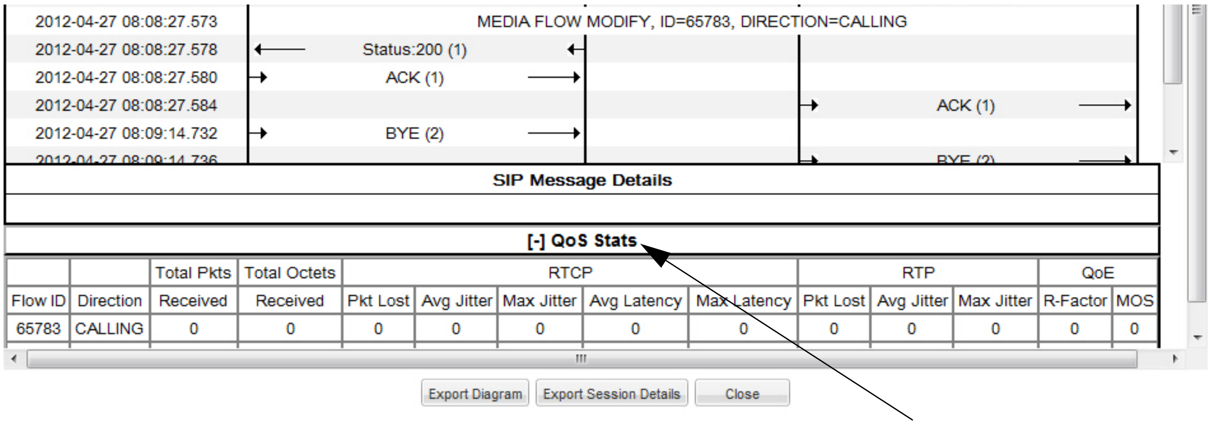
or

Select a record in the table and double-click on that record. The SIP Message Details window displays.

This window displays the messages and status codes that occurred during the active call session or media event. You can use the information to troubleshoot calls/media events that failed or timed out when trying to connect.

QoS Statistics

The Quality of Service (QoS) window displays information about the quality of the service used on the call session or media event when the call or event was active.



```
2012-04-27 08:08:27.573        MEDIA FLOW MODIFY, ID=65783, DIRECTION=CALLING
2012-04-27 08:08:27.578   ←    Status:200 (1)
2012-04-27 08:08:27.580   →    ACK (1)
2012-04-27 08:08:27.584                                        →   ACK (1)
2012-04-27 08:09:14.732   →    BYE (2)
2012-04-27 08:09:14.736                                        →   BYE (2)
```

SIP Message Details

[-] QoS Stats

		Total Pkts	Total Octets	RTCP					RTP			QoE	
Flow ID	Direction	Received	Received	Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
65783	CALLING	0	0	0	0	0	0	0	0	0	0	0	0

QoS Stats

To display QoS Statistics:

1. In the Ladder Diagram, click the **[+]** next to "**QoS Stats**" at the bottom of the Ladder Diagram window. The QoS window expands. This window displays the QoS statistics for the call session or media event in focus.

   The following table describes each field in the QoS Statistics window.

Heading	Description
Flow ID	ID number assigned to the call session or media event flow of data.
Direction	The direction of the call or media event flow. Valid values are: CALLING (egress direction) CALLED (ingress direction)
Total Pkts Received	Total number of data packets received on the interface during the active call session or media event.
Total Octets Received	Total number of octets received on the interface during the active call session or media event. An octet is a unit of digital information that consists of eight bits.
RTCP	Real-time Transport Control Protocol - used to send control packets to participants in a call.
Pkts Lost	Number of RTCP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.
Max Jitter	Maximum measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter).

Heading	Description
Avg Latency	Average observed one-way signaling latency during the active window period. This is the average amount of time the signaling travels in one direction.
Max Latency	Maximum observed one-way signaling latency during the sliding window period. This is the maximum amount of time the signaling travels in one direction. **Note**: For more information about a “sliding window period”, see the *Net-Net C-Series Historical Data Recording Resource Guide*.
RTP	Real-Time Transport Protocol - a standard packet format for delivering audio and video over the internet.
Pkts Lost	Number of RTP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.
Max Jitter	Maximum measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter).
QoE	Quality of Experience - measurement used to determine how well the network is satisfying the end user's requirements.
R-Factor	Average Quality of Service (QoS) factor observed during the active window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
MOS	Mean Opinion Score (MOS) score. MOS is a measure of voice quality. MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using Codecs.

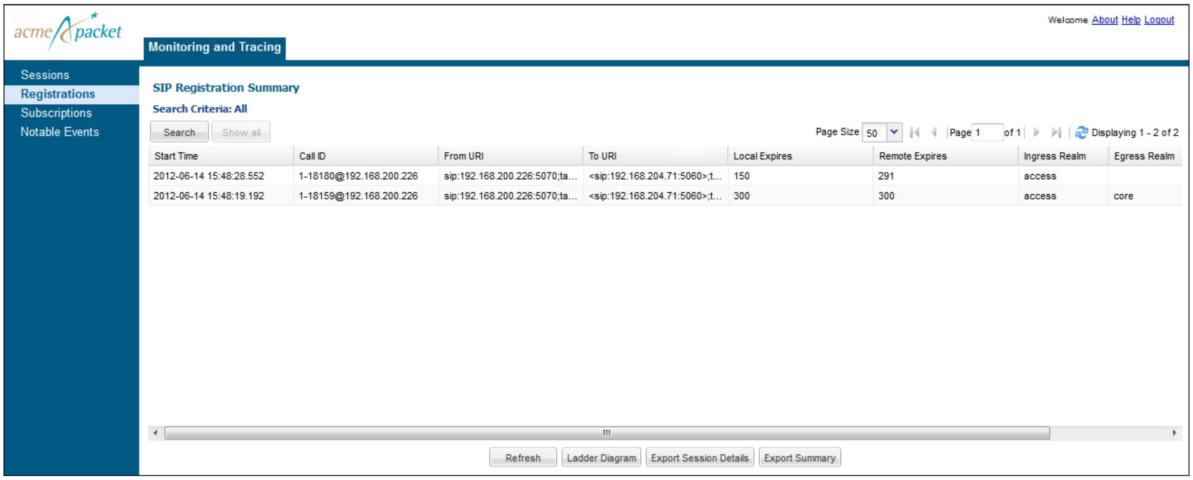
2. Click **[-]** to close the “QoS Stats” window.

Registration Reports

The Registration Report is a summary of all logged SIP registrations sessions on the Net-Net SBC. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net SBC.

> **Note:** For setting filters to capture applicable data, see Filters to Configure (67).

The columns that display on the Registration Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (104).



SIP Registration Summary

Search Criteria: All

Start Time	Call ID	From URI	To URI	Local Expires	Remote Expires	Ingress Realm	Egress Realm
2012-06-14 15:48:28.552	1-18180@192.168.200.226	sip:192.168.200.226:5070;ta...	<sip:192.168.204.71:5060>;t...	150	291	access	
2012-06-14 15:48:19.192	1-18159@192.168.200.226	sip:192.168.200.226:5070;ta...	<sip:192.168.204.71:5060>;t...	300	300	access	core

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.

Heading	Description
Notable Event	Indicates if a "notable event" has occurred on the call session. Valid value is: • **local rejection** - Sessions locally rejected at the Net-Net SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call registration.
Export Session Details	Exports the call registration information associated with the selected record, to a file in text format on the local machine.
Export Summary	Exports all logged call registration records to a file in text format on the local machine.
Refresh	Performs a refresh of the page and updates it with the latest data.
Search	Allows you to specify parameters for performing a search for specific call registration records within the current report.
Show all	Displays all of the call registration records in the Registrations Report.

To display a Registrations Report:

1. After logging into the Web-based GUI, click "**Registrations**" in the left column. The registrations summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

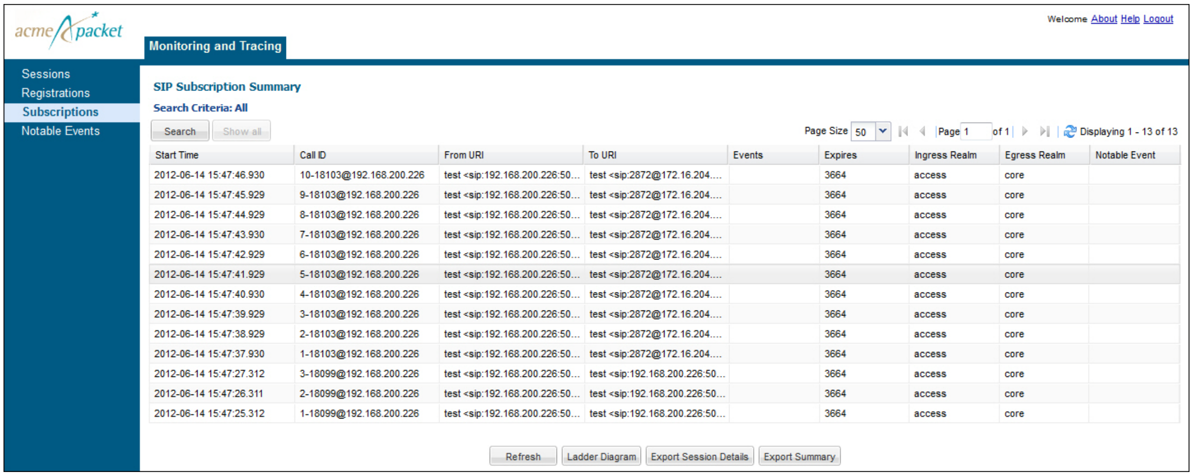
   For information about Refresh, see Refresh (106).
   For information about the Ladder Diagram, see Ladder Diagram (120).
   For information about exporting information, see Exporting Information to a Text File (114).

Subscription Reports

The Subscription Report is a summary of all logged SIP subscription sessions on the Net-Net SBC. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net SBC.

> **Note:** For setting filters to capture applicable data, see Filters to Configure (67).

The columns that display on the Subscription Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (104).



SIP Subscription Summary

Search Criteria: All

Start Time	Call ID	From URI	To URI	Events	Expires	Ingress Realm	Egress Realm	Notable Event
2012-06-14 15:47:46.930	10-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:45.929	9-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:44.929	8-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:43.930	7-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:42.929	6-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:41.929	5-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:40.930	4-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:39.929	3-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:38.929	2-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:37.930	1-18103@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:2872@172.16.204....		3664	access	core	
2012-06-14 15:47:27.312	3-18099@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:192.168.200.226:50...		3664	access	core	
2012-06-14 15:47:26.311	2-18099@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:192.168.200.226:50...		3664	access	core	
2012-06-14 15:47:25.312	1-18099@192.168.200.226	test <sip:192.168.200.226:50...	test <sip:192.168.200.226:50...		3664	access	core	

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.

Heading	Description
Events	Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be: • **conference** - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI). • **consent-pending additions** - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list. • **dialog** - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved. • **kpml** - Event package that enables monitoring of dual-tone multi-frequency (DTMF) signals, and uses XML documents called Key Press Markup Language (KPML). • **message-summary** - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA). • **presence** - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. • **reg** - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR). • **refer** - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request. • **.winfo** - Event package for watcher information. It tracks the state of subscriptions to a resource in another package. • **vq-rtcpx** - Event package that collects and reports the metrics that measure quality for RTP sessions.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a “notable event” has occurred on the call session. Valid value is: • **local rejection** - Sessions locally rejected at the Net-Net SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call subscription.
Export Session Details	Exports the subscription information associated with the selected record, to a file in text format on the local machine.
Export Summary	Exports all logged subscription records to a file in text format on the local machine.
Refresh	Performs a refresh of the page and updates it with the latest data.
Search	Allows you to specify parameters for performing a search for specific subscription records within the current report.
Show all	Displays all of the subscription records in the Subscriptions Report.

To display a Subscriptions Report:

1. After logging into the Web-based GUI, click "**Subscriptions**" in the left column. The subscriptions summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

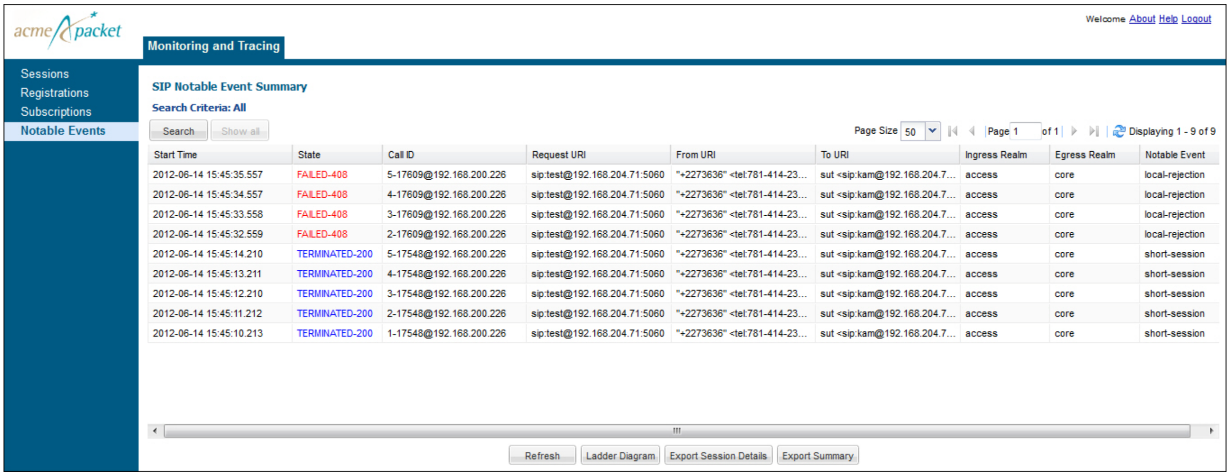
   For information about Refresh, see Refresh (106).
   For information about the Ladder Diagram, see Ladder Diagram (120).
   For information about exporting information, see Exporting Information to a Text File (114).

Notable Event Reports

The Notable Events Report contains all logged sessions that have a notable event associated with the session on the Net-Net SBC. The data that displays in this table is dependent on the filters set via the ACLI on the Net-Net SBC.

> **Note:** For setting filters to capture applicable data, see Filters to Configure (67).

The columns that display on the Notable Events Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (104).



SIP Notable Event Summary

Search Criteria: All

Page Size 50 | Page 1 of 1 | Displaying 1 - 9 of 9

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm	Notable Event
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	local-rejection
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	local-rejection
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	local-rejection
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	local-rejection
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	short-session
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	short-session
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	short-session
2012-06-14 15:45:11.212	TERMINATED-200	2-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	short-session
2012-06-14 15:45:10.213	TERMINATED-200	1-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	short-session

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media event session. Valid values are: • INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. • EARLY Session received the first provisional response (1xx other than 100). • ESTABLISHED Session for which a success (2xx) response was received. • TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session remains in the terminated state until all the resources for the session are freed up. • FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the Net-Net SBC in REQUEST headers.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.

Heading	Description
Events	Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be: • **conference** - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI). • **consent-pending additions** - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list. • **dialog** - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved. • **kpml** - Event package that enables monitoring of dual-tone multi-frequency (DTMF) signals, and uses XML documents called Key Press Markup Language (KPML). • **message-summary** - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA). • **presence** - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. • **reg** - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR). • **refer** - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request. • **.winfo** - Event package for watcher information. It tracks the state of subscriptions to a resource in another package. • **vq-rtcpx** - Event package that collects and reports the metrics that measure quality for RTP sessions.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if an “interesting event” has occurred on the call session. Valid values are: • **short session** - A session is viewed as a "short session" if the length of time, in seconds, is equal to or below the “short-session-duration” value configured at the path *Terminal->session-router->session-router-config->short-session-duration* in the ACLI. • **local rejection** - Sessions that are locally rejected at the Net-Net SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.).
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.

The following table describes the buttons on this page.

Button	Description
	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a notable event.
	Exports the notable event information associated with the selected record, to a file in text format on the local machine.
	Exports all logged notable event records to a file in text format on the local machine.
	Performs a refresh of the page and updates it with the latest data.
	Allows you to specify parameters for performing a search for specific notable event records within the current report.
	Displays all of the notable event records in the Notable Events Report.

To display a Notable Events Report:

1. After logging into the Web-based GUI, click "**Notable Events**" in the left column. The notable events summary report displays.
2. Use the buttons on the bottom of the page to view information about the records in this report.

   For information about Refresh, see Refresh (106).
   For information about the Ladder Diagram, see Ladder Diagram (120).
   For information about exporting information, see Exporting Information to a Text File (114).

8 Personal Profile Manager (PPM) Proxy

Introduction

The Net-Net ESD includes a Personal Profile Manager (PPM) proxy feature. PPM is a web service that runs as part of Avaya Aura Session Manager and Aura System Manager. Local and remote SIP clients may download configuration data from the PPM proxy using SOAP messages over HTTP or HTTPS, enabling soft keys to be customized and contact lists to be loaded. Unfortunately, in enterprise networks certain messages may refer to private IP addresses, which are not routable from remote clients. Oracle now incorporates an application proxy in the Net-Net ESD for such messages, replacing the internal IP addresses with the Net-Net ESD's external SIP interface IP address.

The PPM proxy supports incoming messages over HTTP and HTTPS on a configurable IP address / port. If using HTTPS, the PPM proxy uses a selectable server certificate for Transport Layer Security (TLS).

Remote clients accessing the PPM proxy are authenticated by HTTP digest authentication, using their SIP credentials. The PPM proxy forwards such challenges and responses transparently to the PPM web service for which it is configured.

Since the PPM proxy could potentially be a target of a denial-of-service (DoS) attack, the Net-Net ESD allows you to set DoS rules to protect the proxy port as part of standard configurations. For configuring DoS on the Net-Net ESD, see the “Security” chapter in the Net-Net 4000 Configuration Guide.

How it Works

The Net-Net ESD functions as an HTTP Application Layer Gateway (ALG) for HTTP/HTTPS traffic that originates on Avaya endpoints and terminates on the Avaya Session Manager (ASM) as follows:

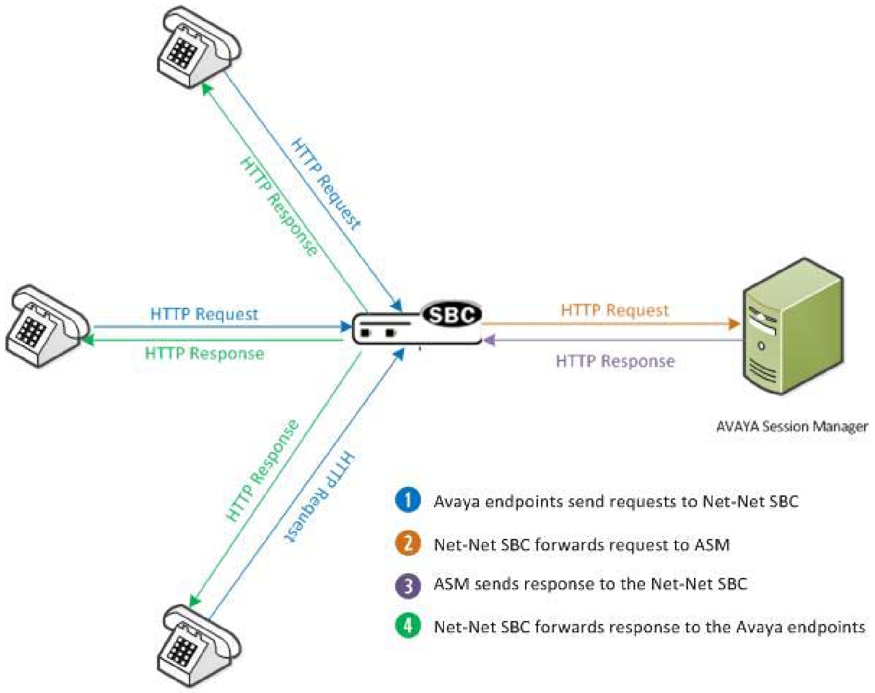
1 The Net-Net ESD receives HTTP requests from Avaya endpoints on a user configurable IP address and port.

2 The Net-Net ESD then forwards the requests to a user configurable destination which is the IP address and port of the ASM.

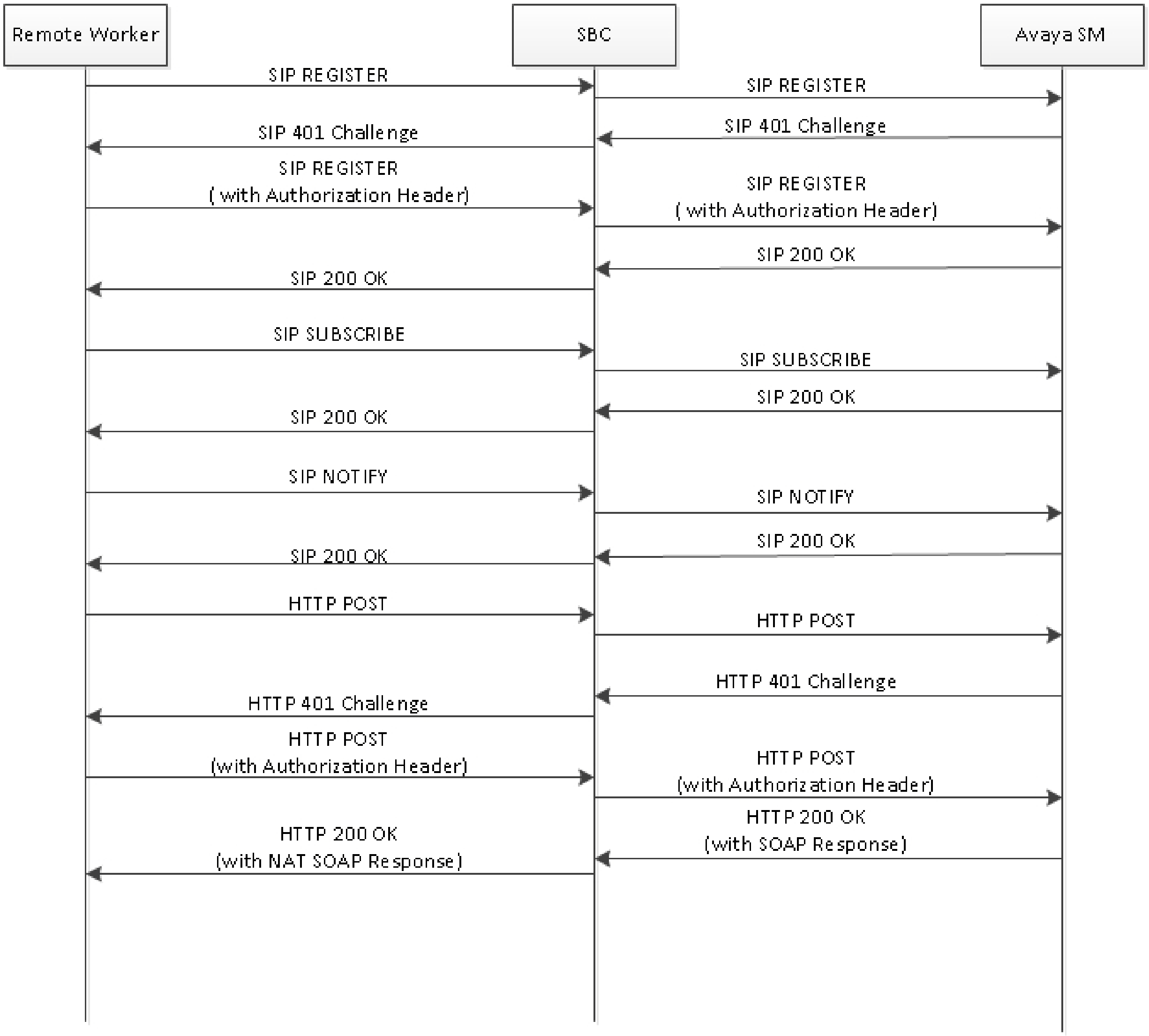
3 The response to the HTTP request is sent from the ASM to the Net-Net ESD.

The Net-Net ESD parses the HTTP response and searches for getHomeServerResponse and getHomeCapabilitiesResponse messages. If the getHomeServerResponse message is found, the Net-Net ESD replaces any text between the <PpmServer> or <SipServer> tags with the IP address of the public interface on which the HTTP-ALG is configured. If the getHomeCapabilitesResponse is found, the Net-Net ESD replaces any text contained between the <ServiceURI> tags with the IP address of the public interface on which the HTTP-ALG is configured.

4 After the Net-Net ESD is done processing the response, it forwards the response to the originating Avaya endpoint. The following illustration shows how the Net-Net ESD sends/receives HTTP requests/responses to the Avaya Session Manager.


HTTP Request
HTTP Response
HTTP Request
HTTP Response
SBC
HTTP Request
HTTP Response
AVAYA Session Manager
HTTP Response
HTTP Request
1 Avaya endpoints send requests to Net-Net SBC
2 Net-Net SBC forwards request to ASM
3 ASM sends response to the Net-Net SBC
4 Net-Net SBC forwards response to the Avaya endpoints

The following is the call flow that occurs as the HTTP/HTTPS requests and responses are passed between the Avaya endpoints, the Net-Net ESD, and the ASM.



Configuring the PPM Proxy on the Net-Net ESD

To configure the PPM proxy on the Net-Net ESD, you use the **http-alg** object under session-router, and the **http-alg-private** or **http-alg-public** settings. Use the following procedure to configure the PPM proxy on the Net-Net ESD.

To configure the PPM proxy:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **http-alg** and press <Enter>.

   ```
   ACMEPACKET(session-router)# http-alg
   ACMEPACKET(http-alg)#
   ```

4. **name**—Enter the name (unique identifier) of the HTTP proxy. Valid values are alpha-numeric characters. Default is blank.
5. **state**—Enter the operational status of the HTTP proxy. Valid values are:
   - **enabled** - (default) Enables the HTTP proxy.
   - **disabled** - Disables the HTTP proxy.
6. **description**—Enter a description of the HTTP proxy. Valid values are alpha-numeric characters. Default is blank.

To set a private setting on the Net-Net ESD:

1. Type **http-alg-private** and press <Enter>.

   ```
   ACMEPACKET(http-alg)# http-alg-private
   ACMEPACKET(http-alg-private)#
   ```

   The private /core side is used to communicate with the Avaya Session Manager (ASM) and forward the incoming HTTP SOAP Requests received from the public side (from outside the network). You define the IP address, port, and TLS certificate used in establishing communication with the ASM by setting this **http-alg-private** attribute.

2. **realm-id**—Name of the realm that the Net-Net ESD uses to proxy the HTTP request. Valid values are alpha-numeric characters. Default is blank.
3. **address**—IPv4 or IPv6 IP address from which the Net-Net ESD forwards the incoming HTTP request. Valid values must be in the format of 0.0.0.0. Default is blank.
4. **destination-address**—IPv4 or IPv6 IP address of the destination server to which the HTTP request is forwarded. Valid values must be in the format of 0.0.0.0. Default is blank.
5. **destination-port**—Port on which the destination server is listening for HTTP traffic. Valid values are 1 to 65535. Default is 80.
6. **tls-profile**—The TLS profile used to establish a secure connection with the destination server. Setting this attribute enables HTTP proxy to listen for HTTPS traffic. Valid values are alpha-numeric characters. Default is blank.
7. Type **done** and press <Enter>.

   ```
   ACMEPACKET(http-alg-private)# done
   ACMEPACKET(http-alg-private)#
   ```

8. Type **exit** and press <Enter>.

   ```
   ACMEPACKET(http-alg-private)# exit
   ACMEPACKET(http-alg)#
   ```

9. Type **exit** and press <Enter>.

   ```
   ACMEPACKET(http-alg)# exit
   ACMEPACKET(session-router)#
   ```

10. Save the configuration.

To set a public setting on the Net-Net ESD:

1. Type **http-alg-public** and press <Enter>.

   ```
   ACMEPACKET(http-alg)# http-alg-public
   ACMEPACKET(http-alg-public)#
   ```

   The public side (outside the network) is used to receive incoming HTTP SOAP Requests from the remote worker. You define the IP address, port, and TLS certificate used to establish a connection with the remote worker by setting this **http-alg-public** attribute.

2. **realm-id**—Name of the realm that the Net-Net ESD uses to listen for the HTTP request. Valid values are alpha-numeric characters. Default is blank.

3. **address**—IPv4 or IPv6 IP address on which the Net-Net ESD is listening for HTTP traffic. Valid values must be in the format of 0.0.0.0. Default is blank.

4. **port—**Port on which the Net-Net ESD is listening for HTTP traffic. Valid values are 1 to 65535. Default is 80.

5. **tls-profile—**The TLS profile used to establish a secure connection with the remote worker. Setting this attribute enables HTTP proxy to listen for HTTPS traffic. Valid values are alpha-numeric characters. Default is blank.

6. Type **done** and press <Enter>.

   ```
   ACMEPACKET(http-alg-public)# done
   ACMEPACKET(http-alg-public)#
   ```

7. Type **exit** and press <Enter>.

   ```
   ACMEPACKET(http-alg-public)# exit
   ACMEPACKET(http-alg)#
   ```

8. Type **exit** and press <Enter>.

   ```
   ACMEPACKET(http-alg)# exit
   ACMEPACKET(session-router)#
   ```

9. Save the configuration.

PPM XML Mapping to ACLI Parameters

Each of the PPM parameters in the ACLI map to specific XML tags. The following table provides the XML/ACLI parameter mapping.

Parameter Name	XML Tag
http-alg	httpAlg
name	name
state	state
description	description
http-alg-private	httpAlgPrivate
realm-id	RealmID
address	address
destination-address	destination-address
destination-port	destination-port
tls-profile	tlsProfile
http-alg-public	httpAlgPublic
realm-id	RealmID
address	address
port	port
tls-profile	tlsProfile

Example PPM Proxy Configuration

The following is an example of a the PPM proxy configuration with private enabled.

```
session-router# show
    http-alg
        name                          Avaya
        state                         enabled
        description                   Avaya Proxy
        http-alg-private
            realm-id                  realmA
            address                   172.45.6.7
            destination-address       123.456.78.1
            destination-port          80
            tls-profile               tls1
        http-alg-public
            realm-id
            address
            port
            tls-profile
```

9 Additional Features

This chapter describes additional new functionality provided by Release S-C[xz]6.3.9.

Unless otherwise noted listed features are available on all software editions (Server Edition, VM Edition, and Oracle Hardware Platforms Edition).

Installation Wizard

The newly available Installation Wizard streamlines the initial configuration process. Initiated at the ACLI, the Installation Wizard asks the user a series of questions that elicit basic configuration data. Virtually all questions provide an intelligent default value that can be accepted by the user to enable reliable and consistent system connectivity. After completing basic configuration with the Installation Wizard, you can perform detailed, network-specific configuration using either the Oracle ACLI or HTTP.

The Installation Wizard is enabled from *privileged* mode, as follows.

```
ACMEPACKET# run setup
```

> **Note:** The Installation Wizard can also be invoked by the **run setup quiet** command which enables a less verbose presentation.

```
-----------------------------------------------------------
Thank you for purchasing the Oracle SBC. The following
short wizard will guide you through the initial set-up.
-----------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


CONFIGURATION

WARNING: Proceeding with wizard will result in existing configuration being
erased.
  Erase config and proceed (yes/no) [no]               :
```

You can use the '**-**' key to back up to the previous field.

You can use the '**?**' key to obtain query-specific help.

You can use the '**q**' key to exit the wizard. **q** provides an escape mechanism allowing you to exit the wizard without making any change to the system configuration.

1. The wizard issues a Warning stating that using the wizard can overwrite the existing running configuration. While this is true, keep in mind that you can always use the '**q**' key to escape the wizard during the initial set-up process. Using this escape mechanism returns you to the ACLI prompt, and makes no changes to the current running configuration. Note also that the Installation Wizard saves a backup copy of the current running configuration prior to making any configuration changes.

   Type **yes** to continue with the wizard. Type **no** to exit the wizard and return to the ACLI prompt.

2. If you typed **yes**, and assuming that an HA license is present, the wizard prompts for the operational mode, *standalone* or *HA*.

   In the absence of an HA license, the wizard queries for the SBC name as described below.

```
SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                      : 1
```

   Type **1** or **2** to specify the operational mode.

3. If you specified **high availability** mode, jump to Step 7. If you specified **standalone** mode, the wizard proceeds as follows:

4. If you specified **high availability** mode, the wizard prompts for the role of this SD within the HA pair, either **primary** or **secondary**.

```
If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
    SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                     : 1
```

   Regardless of the specified mode (**stand** or **high availability**) or role (**primary** or **secondary**), you may be asked respond to the following queries.

```
Unique target name of this SBC [ACMESYSTEM]          : Ragnarok
```

   Provide a new system name, or accept the factory default value of *ACMESYSTEM*.

```
IP address on management interface [172.30.46.11]    :
```

   Provide the management interface address, or accept the default value as obtained from the boot parameters (if configured).

```
Subnet mask [255.255.0.0] :
```

   Provide the management interface subnet mask, or accept the default value as obtained from the boot parameters (if configured).

```
Gateway IP address [172.30.0.1]                      :
```

Provide the default gateway interface address, or accept the default value as obtained from the boot parameters (if configured).

```
Start GUI (yes/no) [yes]                             : yes
```

Enable (**yes**) or disable (**no**) HTTP access to the SD.

```
NNC access (yes/no) [yes]                            : yes
```

Enable (**yes**) or disable (**no**) Net-Net Central access to the SD.

```
NNC IP address                                       : 192.168.54.60
```

If Net-Net Central access is enabled, provide the required address of the Net-Net Central server.

If the specified mode is **high availability**, and the role is **primary**, you will be asked respond to the following query.

```
Peer target name [sbc02]                             :
```

Provide the name of the secondary (backup) SD, or accept the default value.

If the specified mode is **high availability**, and the role is **secondary**, you will be asked respond to the following query.

```
Acquire config from the Primary (yes/no) [yes] :
```

Specify if you want the secondary SD to obtain its configuration file from the primary SD. **yes**, the default (and strongly recommended value), identifies the primary as the source of the configuration file; **no** identifies the secondary as the source of the configuration file.

If you identified the secondary as the source of the configuration file (strongly discouraged by Oracle), you will be asked respond to the following query.

```
Peer target name [sbc02]                             :
```

Provide the name of the primary SD, or accept the default value — only appears if the secondary is the source of the configuration file.

5. After you respond to all queries, the Installation Wizard displays a configuration summary similar to one of the following, depending on the SBC mode and the HA role.

SBC Mode = standalone

```
-- Summary view ---------------------------------------------------------

HIGH AVAILABILITY
  1: SBC mode                                          : standalone
  2: SBC role                                          : N/A
  3: Redundancy interface address                      : N/A
  4: Redundancy subnet mask                            : N/A

SBC SETTINGS
  5: Unique target name of this SBC                    : Ragnarok
  6: IP address on management interface                : 172.30.46.11
  7: Subnet mask                                       : 255.255.0.0
  8: Gateway IP address                                : 172.30.0.1

AUTOMATIC CONFIGURATION
  9: Acquire config from the Primary (yes/no)          : N/A

PEER CONFIGURATION
 10: Peer IP address                                   : N/A
 11: Peer target name                                  : N/A

GUI ACCESS
 12: Start GUI (yes/no)                                : yes

NNC ACCESS SETTINGS
 13: NNC access (yes/no)                               : yes
 14: SNMP community string                             : public
 15: NNC IP address                                    : 192.168.54.60

Enter 1-15 to modify, 'd' to display summary, 's' to save, 'q' to exit. [s]:
```

SBC Mode = HA, Role = Primary

```
-- Summary view ---------------------------------------------------------

HIGH AVAILABILITY
  1: SBC mode                                         : high availability
  2: SBC role                                          : primary
  3: Redundancy interface address                      : 169.254.1.1
  4: Redundancy subnet mask                            : 255.255.255.252

SBC SETTINGS
  5: Unique target name of this SBC                    : Ragnarok
  6: IP address on management interface                : 172.30.46.11
  7: Subnet mask                                       : 255.255.0.0
  8: Gateway IP address                                : 172.30.0.1

AUTOMATIC CONFIGURATION
  9: Acquire config from the Primary (yes/no)          : N/A

PEER CONFIGURATION
 10: Peer IP address                                   : 169.254.1.2
 11: Peer target name                                  : sbc02

GUI ACCESS
 12: Start GUI (yes/no)                                : yes

NNC ACCESS SETTINGS
 13: NNC access (yes/no)                               : yes
 14: SNMP community string                             : public
 15: NNC IP address                                    : 192.168.54.60

Enter 1-15 to modify, 'd' to display summary, 's' to save, 'q' to exit. [s]:
```

SBC Mode = HA, Role = Secondary (acquire config from Primary)

```
-- Summary view ---------------------------------------------------------

HIGH AVAILABILITY
  1: SBC mode                                         : high availability
  2: SBC role                                          : secondary
  3: Redundancy interface address                      : 169.254.1.2
  4: Redundancy subnet mask                            : 255.255.255.252

SBC SETTINGS
  5: Unique target name of this SBC                    : Ragnarok
  6: IP address on management interface                : 172.30.46.11
  7: Subnet mask                                       : 255.255.0.0
  8: Gateway IP address                                : 172.30.0.1

AUTOMATIC CONFIGURATION
  9: Acquire config from the Primary (yes/no)          : yes

PEER CONFIGURATION
 10: Peer IP address                                   : 169.254.1.1
 11: Peer target name                                  : N/A

GUI ACCESS
 12: Start GUI (yes/no)                                : N/A

NNC ACCESS SETTINGS
 13: NNC access (yes/no)                               : N/A
 14: SNMP community string                             : N/A
 15: NNC IP address                                    : N/A

Enter 1-15 to modify, 'd' to display summary, 's' to save, 'q' to exit. [s]:
```

Note: Note that values marked N/A will be obtained from the primary.

SBC Mode = HA, Role = Secondary (do not acquire config from Primary)

```
-- Summary view ------------------------------------------------------------

HIGH AVAILABILITY
  1: SBC mode                                           : high availability
  2: SBC role                                            : secondary
  3: Redundancy interface address                        : 169.254.1.2
  4: Redundancy subnet mask                              : 255.255.255.252

SBC SETTINGS
  5: Unique target name of this SBC                      : Ragnarok
  6: IP address on management interface                  : 172.30.46.11
  7: Subnet mask                                         : 255.255.0.0
  8: Gateway IP address                                  : 172.30.0.1

AUTOMATIC CONFIGURATION
  9: Acquire config from the Primary (yes/no)            : no

PEER CONFIGURATION
 10: Peer IP address                                     : 169.254.1.1
 11: Peer target name                                    : sbc01

GUI ACCESS
 12: Start GUI (yes/no)                                  : yes

NNC ACCESS SETTINGS
 13: NNC access (yes/no)                                 : yes
 14: SNMP community string                               : public
 15: NNC IP address                                      : 192.168.54.60


Enter 1-15 to modify, 'd' to display summary, 's' to save, 'q' to exit. [s]:
```

6. Note that if Net-Net Central access has been enabled, the Installation Wizard, in all instances, provides a default SNMP community string/password (*public*).
7. Note that the Installation Wizard provides default IP addresses for the HA primary and secondary SDs (*Redundancy interface address* and *Peer IP address*). These default addresses are link-local address as specified in RFC 3927, *Dynamic Configuration of IPv4 Link-local addresses*.
8. Note that the Installation Wizard provides default IP addresses for the HA primary and secondary SDs (*Redundancy interface address* and *Peer IP address*). These default addresses are link-local address as specified in RFC 3927, *Dynamic Configuration of IPv4 Link-local addresses*.

Review parameter values; if changes are required for any value (to include the *SNMP community string*, *Redundancy interface address*, and *Peer IP address*), select the target parameter by number, press ENTER, and provide a new value. When satisfied, type ‘**s**’ to initiate a system reboot using these parameter values. If the primary SD has been identified as the source of the configuration file, the secondary SD obtains that file prior to initiating the boot.

Hostname Field Lengths

This feature applies to the Linux OS for the Net-Net Session Director Server Edition (NN-SD SE) and the Net-Net Session Director Virtual Machine Edition (NN-SD VME) platforms only.

The NN-SD bootloader and application target/host name fields accept up to 63 ASCII characters (NULL not included). It modifies the ACLI command, “**configure terminal bootparam**” and allows you to enter a hostname of up to 63 characters. Previously, these fields on the Net-Net 3280 and 4500 accepted only 24 ASCII characters and the name was truncated if you specified more than 24 characters for the hostname.

For example, if the target name was:

`alpha-bravo-charlie-1234567890` (30 characters)

the ACLI on previous systems displayed:

```
alpha-bravo-charlie-1234(configure)#
```

It now displays the “first 12 characters + 3 periods + last 12 characters” (NULL not included) as follows:

```
alpha-bravo-...e-1234567890(configure)#
```

You must upgrade the NN-SD bootloader for this feature to take affect. Refer to Bootloader Upgrade Procedure in Chapter 1.

Video-Conferencing Support

The Net-Net Session Director (NN-SD) supports H323 video-conferencing environments using the H239 Procotol for video-conferencing. It provides critical control functions to enable high quality interactive communication—voice, video and multimedia sessions—across IP network borders.

For additional information about the H323 Protocol, see the *Net-Net 4000 ACLI Configuration Guide, Version 6.3*.

The NN-SD architecture supports both voice and video applications. It uses Codec Media Profiles to determine the proper amount of bandwidth allocated for a given session, distinguishing between G.711 or G729 voice and H.263/264 video requirements. By supporting video transmission as well as voice over the IP Multi-protocol label switching (MPLS) core, the NN-SD allows Service Providers to roll out new services to their enterprise customer such as video/audio conferencing.

> **Note:** IP MPLS is a packet-switched network that uses the Internet Protocol (TCP/IP) enhanced with the Multi-protocol label switching (MPLS) standard.

The NN-SD allows for aggregate bandwidth policies to be configured for each realm. As the NN-SD processes call requests (to and from) a particular realm, the bandwidth consumed for the call is decremented from the bandwidth pool for that realm. The SD determines the required bandwidth from the SDP/H.245 information. Any request that would cause the bandwidth constraint to be exceeded is rejected with a SIP “503 Service Unavailable” or an “H.323 Release Complete”.

To alleviate the bandwidth demands of high-definition video streams, the NN-SD offers a 2 or 4 Gigabit PHY card option.

Flow Control Mapping for Interworking Function (IWF) Video

H.245 is a protocol for the transmission of call management and control signals in networks using H.323 equipment. The H.245 specification is used in audio, video, and data transmissions, as well as in voice over IP (VoIP). H.245 messages are sent over special channels called H.245 control channels.

H.245 signaling is used to manage and control call setup and connection. Functions of H.245 include determining which endpoint is to be the master and which is to be the slave during the call, opening and closing of multiplexed data-transfer paths between the endpoints, establishing an upper limit to the data transfer speed on each logical channel, information exchanges between endpoints concerning the types of data each endpoint can send and receive, requests by the receiving endpoint for changes in the mode of the data sent by the transmitting endpoint, and requests by either endpoint to end the call.

In the H.245 standard, the FlowControlCommand message is used to specify the upper limit of bit rate of either a single logical channel or the whole multiplex. The following is an excerpt from the H.245 standard.

Command Message: Flow Control (from H.245 standard)

```
=======================================================================
FlowControlCommand ::= SEQUENCE
{
    scope CHOICE
    {
        logicalChannelNumber LogicalChannelNumber,
        resourceID INTEGER (0..65535),
        wholeMultiplex NULL
    },
    restriction CHOICE
    {
        maximumBitRate INTEGER (0..16777215), -- units 100 bit/s
        noRestriction NULL
    },
    ...
}
=======================================================================
```

A terminal may send this command to restrict the bit rate that the far-end terminal sends. A receiving terminal must comply with this command.

In an H.323 environment, the Net-Net SD previously used the FlowControlCommand to map to SIP using either the Real-Time Control Protocol (RTCP) feedback function, or the SIP signaling path (for example, the INFO method).

The Net-Net SD now supports the SIP counter part of the H.245 FlowControlCommand using the SIP signaling path with the INFO method. The Net-Net SD sends the SIP INFO message with "change_bitrate" rate parameter that has the value 100* maxBitRate from the corresponding H.245 FlowControlCommnad message. For example, in the following messages, the incoming H.323 message with the H.245 FlowControlCommand, is converted into the outgoing SIP INFO message with the message body.

Incoming H.323 Message with H.245 FlowControlCommand

```
H.245
PDU Type: command (2)
        command: flowControlCommand (4)
            flowControlCommand
                scope: logicalChannelNumber (0)
                    logicalChannelNumber: 102
                restriction: maximumBitRate (0)
                    maximumBitRate: 4480
```

Outgoing SIP INFO Message

```
Message Body
        eXtensible Markup Language
            <?xml
                version="1.0"
                encoding="utf-8"
                ?>
            <media_control>
                <vc_primitive>
                    <to_encoder>
                        <change_bitrate>
                            4480000
                            </change_bitrate>
                        </to_encoder>
                    </vc_primitive>
                </media_control>
```

SIP-H.323 interworking with Dynamic Payload Types

The SIP and H.323 Protocols use Internet multimedia signaling over IP, and both use the Real-Time Transport Protocol (RTP) for transferring realtime audio/video data. The interworking function (IWF) provides a means of converting translation and signaling protocols and session descriptions between SIP and H.323. However, SIP and H.323 provide different mechanisms when exchanging payload types for media during IWF calls. Therefore, the International Telecomunications Union (ITU) modified the ITU H.245 recommendations in H.245 v16 to include a new “Dynamic Payload Type Replacement” capability that resolves this payload type conflict. This new capability provides a way for an H.323 endpoint to specify the payload type of a media stream for which the endpoint is willing to receive through the OLC-acknowledgment (OLC-ACK) message in an audio/video call flow.

The Net-Net SD supports this new “Dynamic Payload Type Replacement” capability by ensuring interworking of SIP and H.323 when audio/video call flows use dynamic payload types. The Net-Net SD checks for the presence of this capability in the incoming TCS request. If it finds this capability in the TCS request, it sends an Open Logic Channel Acknowledgement (OLC-ACK) response with the payload type it is willing to receive.

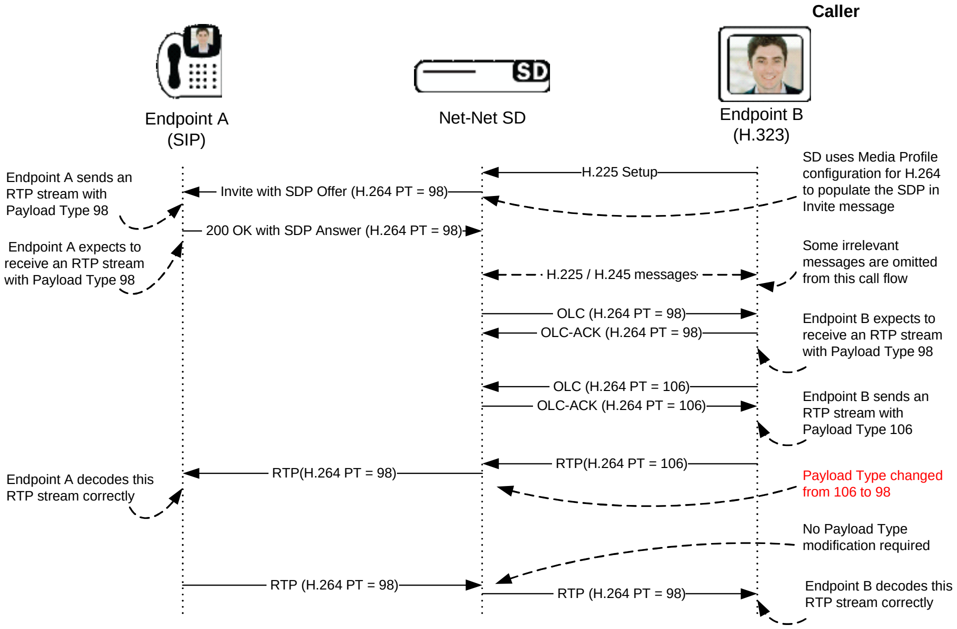
> **Note:** The Net-Net SD always returns an OLC-ACK with a dynamic payload type value that it received in the incoming Session Description Protocol (SDP) from the SIP endpoint

For devices that don't support the H.245 v16 recommendations, the Terminal Capability Set (TCS) request from the H.323 endpoint does not have the "Dynamic Payload Type Replacement" capability present. Therefore, the Net-Net SD rewrites the payload type within the RTP packets when these packets traverse the Net-Net SD. When devices in a session negotiate different payload types between SIP and H.323 packets, the RTP streams that they receive, always have the expected payload type in the RTP header.

> **Note:** The Net-Net SD always maps the payload type on the RTP stream received from the H.323 endpoint, and sends it to the SIP endpoint for both audio and video. The Net-Net SD does not support mapping of payload types in audio streams with 2833 DTMF packets.

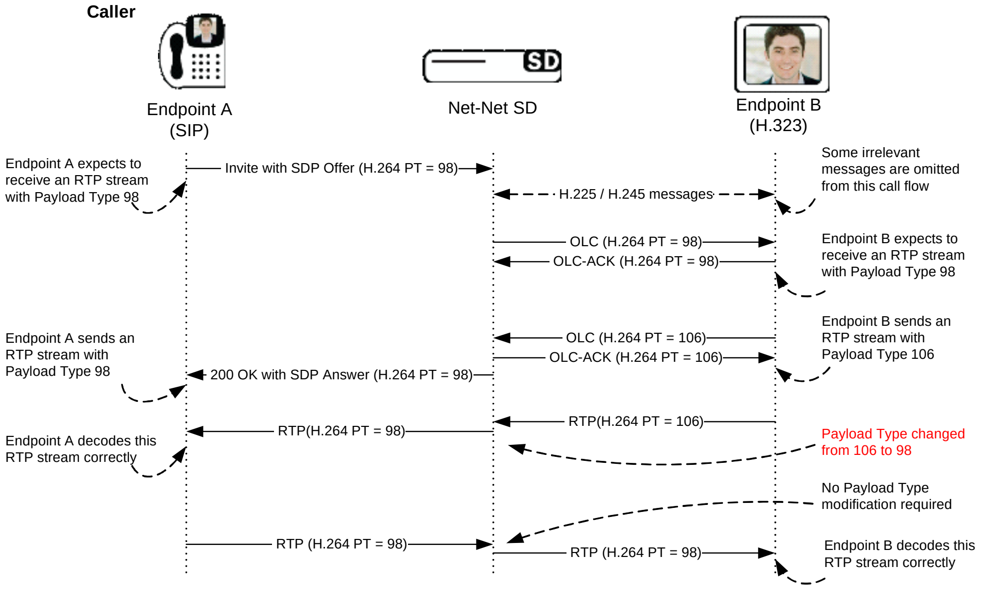
Figure 1a and 1b below shows the call flow from an H.323 Endpoint B to a SIP Endpoint A, and from a SIP Endpoint A to an H.323 Endpoint B, respectively. These illustrations show the negotiation of different dynamic payload types for the video streams but the Codec negotiated is the same. The Net-Net SD dynamically replaces the payload type in the RTP header of the video stream received from the H.323 endpoint.

Figure 1a Endpoint B calling Endpoint A (H.323 endpoint does not have “Dynamic Payload Type Replacement” Capability)


Caller
Endpoint A
(SIP)
Net-Net SD
Endpoint B
(H.323)
SD
H.225 Setup
SD uses Media Profile configuration for H.264 to populate the SDP in Invite message
Endpoint A sends an RTP stream with Payload Type 98
Invite with SDP Offer (H.264 PT = 98)
200 OK with SDP Answer (H.264 PT = 98)
Endpoint A expects to receive an RTP stream with Payload Type 98
Some irrelevant messages are omitted from this call flow
H.225 / H.245 messages
OLC (H.264 PT = 98)
OLC-ACK (H.264 PT = 98)
Endpoint B expects to receive an RTP stream with Payload Type 98
OLC (H.264 PT = 106)
OLC-ACK (H.264 PT = 106)
Endpoint B sends an RTP stream with Payload Type 106
RTP(H.264 PT = 106)
RTP(H.264 PT = 98)
Endpoint A decodes this RTP stream correctly
Payload Type changed from 106 to 98
No Payload Type modification required
RTP (H.264 PT = 98)
RTP (H.264 PT = 98)
Endpoint B decodes this RTP stream correctly

The H.323 Endpoint B is not H.245 v16 compliant, and hence payload type replacement needs to be done in the RTP packets.

Figure 1b Endpoint A calling Endpoint B (H.323 endpoint does not have Dynamic Payload Type Replacement Capability)

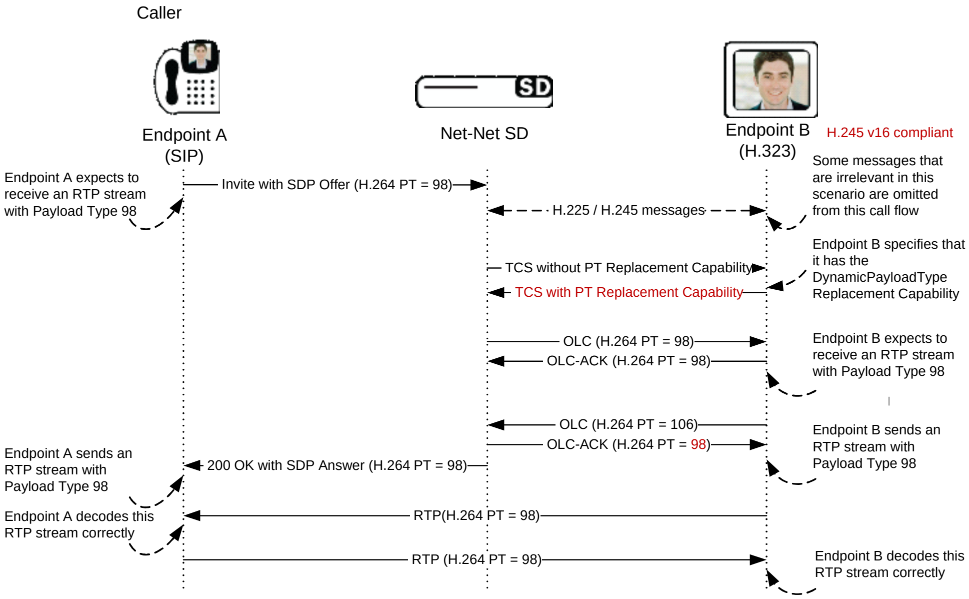

Caller
Endpoint A (SIP)
Net-Net SD
Endpoint B (H.323)
Endpoint A expects to receive an RTP stream with Payload Type 98
Invite with SDP Offer (H.264 PT = 98)
H.225 / H.245 messages
Some irrelevant messages are omitted from this call flow
OLC (H.264 PT = 98)
OLC-ACK (H.264 PT = 98)
Endpoint B expects to receive an RTP stream with Payload Type 98
OLC (H.264 PT = 106)
OLC-ACK (H.264 PT = 106)
Endpoint B sends an RTP stream with Payload Type 106
Endpoint A sends an RTP stream with Payload Type 98
200 OK with SDP Answer (H.264 PT = 98)
RTP(H.264 PT = 106)
RTP(H.264 PT = 98)
Payload Type changed from 106 to 98
Endpoint A decodes this RTP stream correctly
No Payload Type modification required
RTP (H.264 PT = 98)
RTP (H.264 PT = 98)
Endpoint B decodes this RTP stream correctly

The H.323 Endpoint B is not H.245 v16 compliant, and therefore payload type replacement needs to be done in the RTP packets.

There is no concept of H.245 compliance for the SIP Endpoint A.

Figure 2a shows the call flow of SIP Endpoint A calling an H.323 Endpoint B using slow start. The Net-Net SD modifies the dynamic payload type in the OLC-ACK based on payload type received in the incoming SDP OFFER in the "INVITE" message.

Figure 2a Endpoint A calling Endpoint B (H.323 endpoint has TCS with Dynamic Payload Type Replacement Capability)

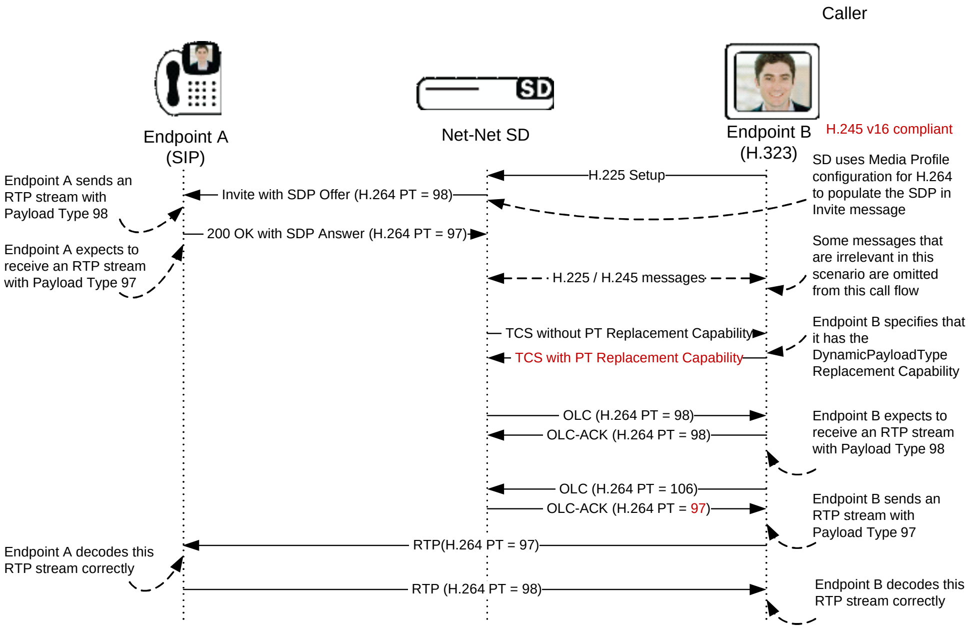

Caller
Endpoint A (SIP)
Net-Net SD
Endpoint B (H.323)
H.245 v16 compliant
Endpoint A expects to receive an RTP stream with Payload Type 98
Invite with SDP Offer (H.264 PT = 98)
H.225 / H.245 messages
Some messages that are irrelevant in this scenario are omitted from this call flow
TCS without PT Replacement Capability
TCS with PT Replacement Capability
Endpoint B specifies that it has the DynamicPayloadType Replacement Capability
OLC (H.264 PT = 98)
OLC-ACK (H.264 PT = 98)
Endpoint B expects to receive an RTP stream with Payload Type 98
OLC (H.264 PT = 106)
OLC-ACK (H.264 PT = 98)
Endpoint B sends an RTP stream with Payload Type 98
Endpoint A sends an RTP stream with Payload Type 98
200 OK with SDP Answer (H.264 PT = 98)
Endpoint A decodes this RTP stream correctly
RTP(H.264 PT = 98)
RTP (H.264 PT = 98)
Endpoint B decodes this RTP stream correctly

The H.323 Endpoint B is H.245 v16 compliant.

There is no concept of H.245 compliance for the SIP Endpoint A.

Figure 2b shows the call flow an H.323 Endpoint B using slow start, calling a SIP Endpoint A. The Net-Net SD modifies the dynamic payload type in the OLC-ACK based on payload type received in the incoming SDP ANSWER in the "200 OK" message.

Figure 2b Endpoint B calling Endpoint A (H.323 endpoint here has TCS without “Dynamic Payload Type Replacement” Capability)


Caller
Endpoint A (SIP)
Net-Net SD
Endpoint B (H.323)
H.245 v16 compliant
H.225 Setup
SD uses Media Profile configuration for H.264 to populate the SDP in Invite message
Invite with SDP Offer (H.264 PT = 98)
Endpoint A sends an RTP stream with Payload Type 98
200 OK with SDP Answer (H.264 PT = 97)
Endpoint A expects to receive an RTP stream with Payload Type 97
H.225 / H.245 messages
Some messages that are irrelevant in this scenario are omitted from this call flow
TCS without PT Replacement Capability
TCS with PT Replacement Capability
Endpoint B specifies that it has the DynamicPayloadType Replacement Capability
OLC (H.264 PT = 98)
OLC-ACK (H.264 PT = 98)
Endpoint B expects to receive an RTP stream with Payload Type 98
OLC (H.264 PT = 106)
OLC-ACK (H.264 PT = 97)
Endpoint B sends an RTP stream with Payload Type 97
RTP(H.264 PT = 97)
Endpoint A decodes this RTP stream correctly
RTP (H.264 PT = 98)
Endpoint B decodes this RTP stream correctly

Appendix A SNMP Support

Overview

This chapter provides information about Net-Net Session Director's SNMP support. The SNMP agent is part of the Net-Net Session Director image and runs as a thread (process) in the application.

The SNMP supports the same services found in Net-Net SBC S-CX6.3.0 releases, which includes SNMP Get/Set and Trap operations in either v1v2 mode or secure trap mode. When the Net-Net Session Director is configured to operate in:

- v1v2 mode, it supports SNMPv1 and v2c queries. SNMP traps are transmitted in v2c format only.
- secure trap mode, it supports only SNMP traps transmitted in v3 format with mandatory authentication and privacy.

MIB Changes

The following changes were made to existing Oracle MIBs for this Net-Net Session Director release.

- ap-products.mib: a product series added called apNetNetOSSeries. For the Phase 1 release, a platform was defined called apNetNetOS.
- ap-license.mib: is not supported in current release.
- ap-entity-vendortype.mib: is not supported in Net-Net Session Director because it is a software-only product.
- ap-env-monitor.mib: is not supported in Net-Net Session Director because it is a software-only product.

SNMPv3 Support

The Net-Net SBC supports SNMPv3, which provides the SNMP agent and SNMP Network Management System (NMS) with authentication, privacy, and access control during the delivery of secured traps. Currently, SNMPv3 traps are supported on the Net-Net SBC; SNMPv3 Get/Get-Bulk/Set actions are not supported at this time.

By default, the Net-Net SBC supports SNMPv1v2. If you want to retain existing SNMPv1v2 behavior, you do not need to update configuration. You can enable SNMPv3 at any time, at which point SNMPv1v2 configurations are ignored, and only SNMPv3 encrypted traps are sent to associated external SNMP managers. **Snmp-agent-mode**, an attribute under **system-config**, allows you to select the desired mode.

Oracle USBC MIB (ap-usbcsys.mib)

The following table describes the SNMP GET query names for the Oracle USBC MIB (ap-usbscsys.mib).

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apUsbcSysMIBObjects (1.3.6.1.4.1.9148.3.17.1)		
Object Identifier Name: apUsbcSysObjects (1.3.6.1.4.1.9148.3.17.1.1)		
apUsbcSysCpuUtilAll	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.1.0	Percentage of CPU utilization.
apUsbcSysCpuCount	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.2.0	Number of CPUs for this system.
apUsbcSysCpuSpeedMHz	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.3.0	Speed in MHz of the CPUs for this system.
apUsbcSysMemSzMB	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.4.0	Number of megabytes of all CPUs for this system.
apUsbcSysMemSzGB	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.5.0	Number of gigabytes of all CPUs for this system.
apUsbcSysAppMemUtil	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.6.0	Percentage of total memory utilization by applications.
apUsbcSysKernelMemUtil	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.7.0	Percentage of total memory utilization by the kernel.
apUsbcSysMyBogoMips	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.8.0	Processor speed in mips(millions of instructions per seond). Speed is calculated by the kernel at boot time.
apUsbcSysAllBogoMips	apUsbcSysObjects: 1.3.6.1.4.1.9148.3.17.1.1.9.0	Sum of all bogo mips (millions of instrctuctions per second) of all CPUs for this system.
Object Identifier Name: apUsbcSysCpuTable (.1.3.6.1.4.1.9148.3.17.1.1.10.1)		
Object Identifier Name: apUsbcSysCpuEntry (.1.3.6.1.4.1.9148.3.17.1.1.10.1.1)		
apUsbcSysCpuNum	apUsbcSysCpuEntry: 1.3.6.1.4.1.9148.3.17.1.1.10.1.1.1	CPU number + 1 of this entry.
apUsbcSysCpuUtil	apUsbcSysCpuEntry: 1.3.6.1.4.1.9148.3.17.1.1.10.1.1.2	Percent of CPU utilization for this CPU.

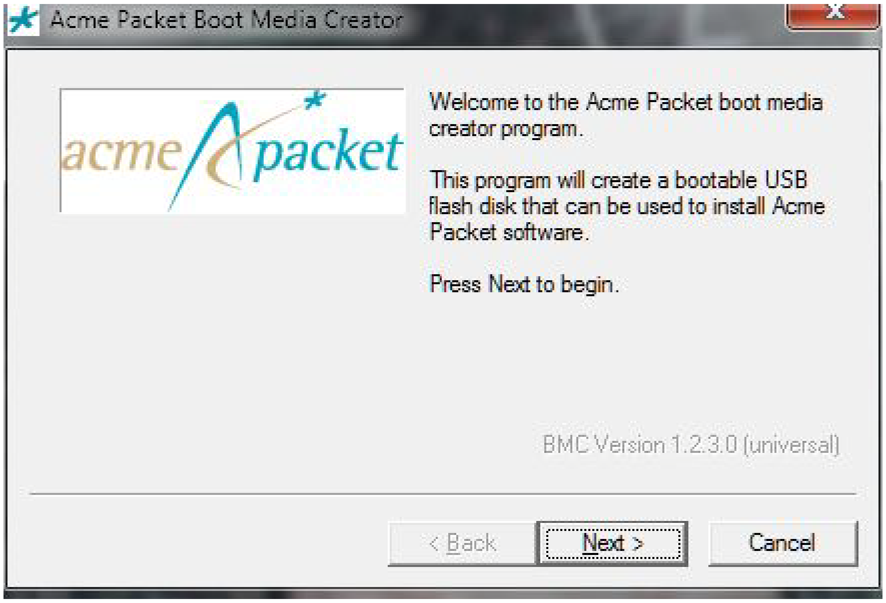
Appendix B Boot Media Creator

Channel partners will use the Boot Media Creator (BMC), a Windows executable file (*nnSCz639-img-usb.exe* for this release cycle) to write a build image to a USB stick. The USB stick will be subsequently be used to load the software to a server.

Writing a Build Image

Use the following procedure to create a USB stick containing only a build image.

1. Open *nnSCz639-img-usb.exe*; click **Next**.



Acme Packet Boot Media Creator

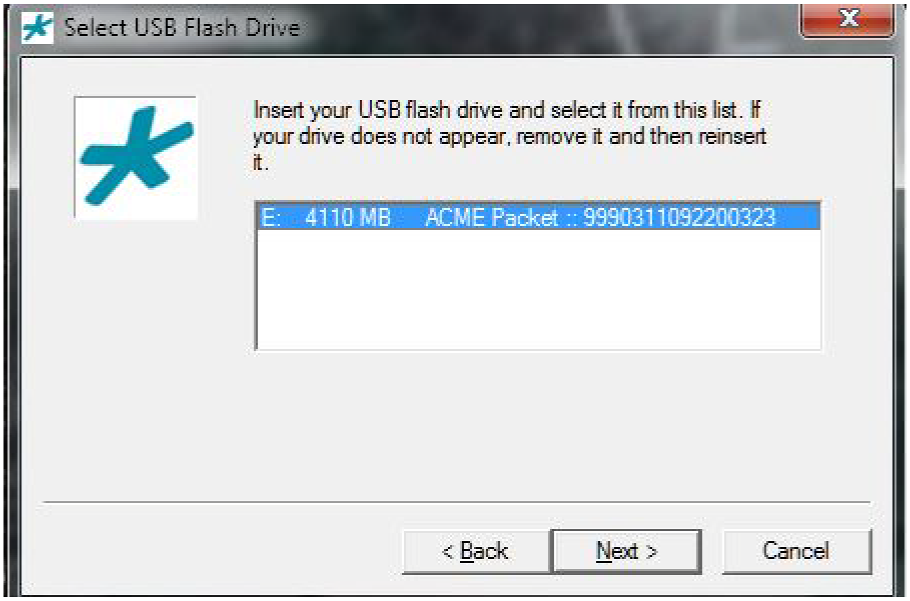
Welcome to the Acme Packet boot media creator program.

This program will create a bootable USB flash disk that can be used to install Acme Packet software.

Press Next to begin.

BMC Version 1.2.3.0 (universal)

2. Insert the USB stick and/or select it from the displayed list; click **Next**.

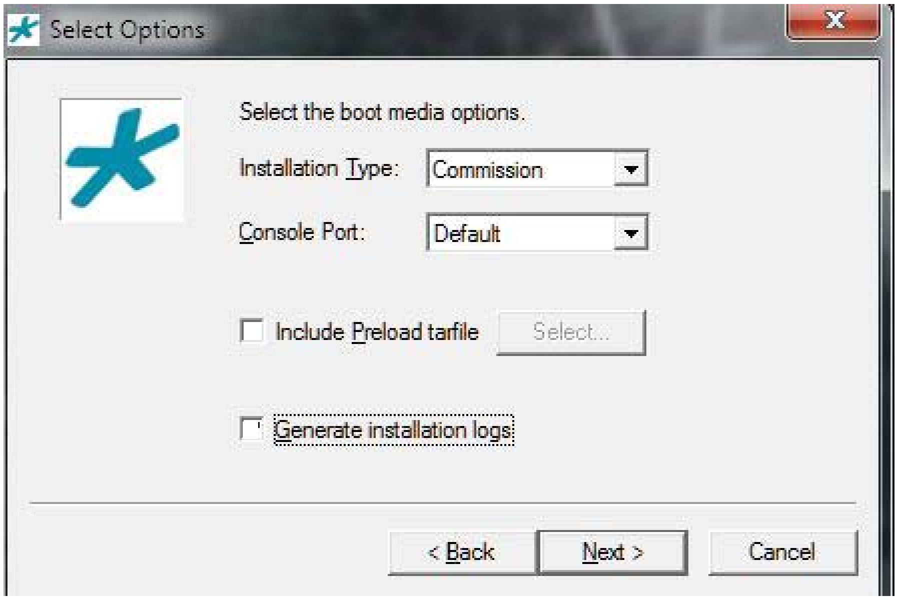


Select USB Flash Drive

Insert your USB flash drive and select it from this list. If your drive does not appear, remove it and then reinsert it.

E: 4110 MB   ACME Packet :: 9990311092200323

3. To write a build image to the USB stick, select **Commission** as the *Installation Type*, as shown below; click **Next**.



Select Options

Select the boot media options.

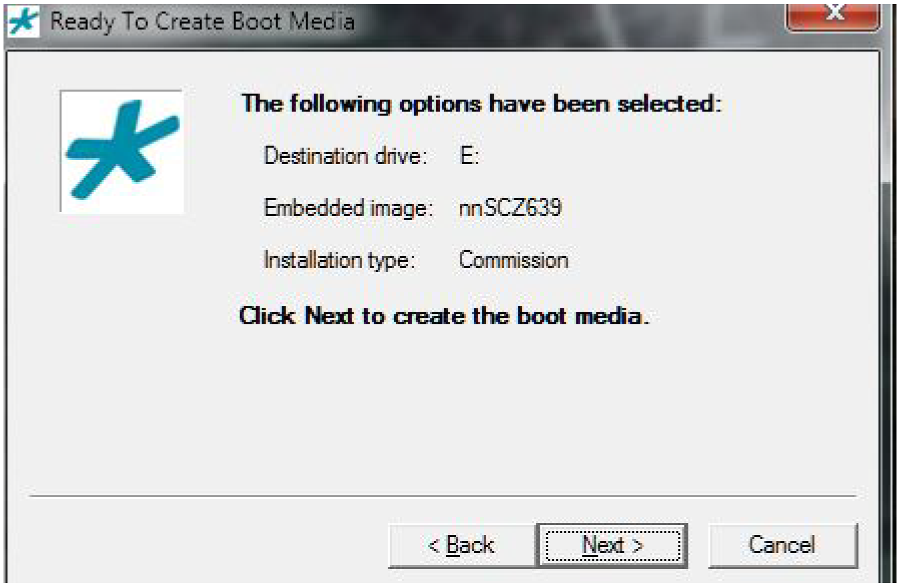
Installation Type: Commission

Console Port: Default

□ Include Preload tarfile

□ Generate installation logs

4. Confirm selected options; click **Next**.



Ready To Create Boot Media

The following options have been selected:

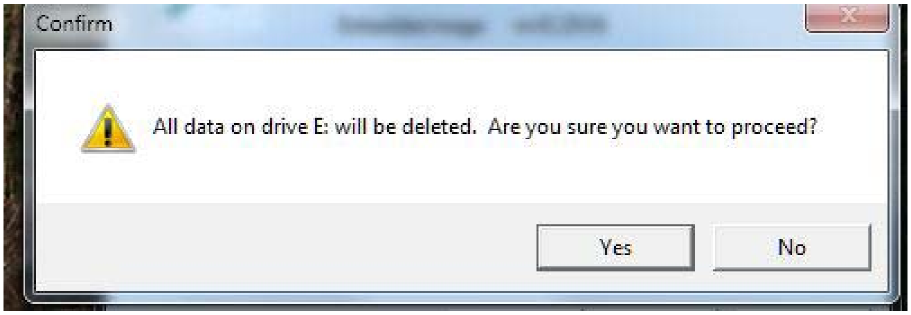
Destination drive: E:

Embedded image: nnSCZ639

Installation type: Commission

Click Next to create the boot media.

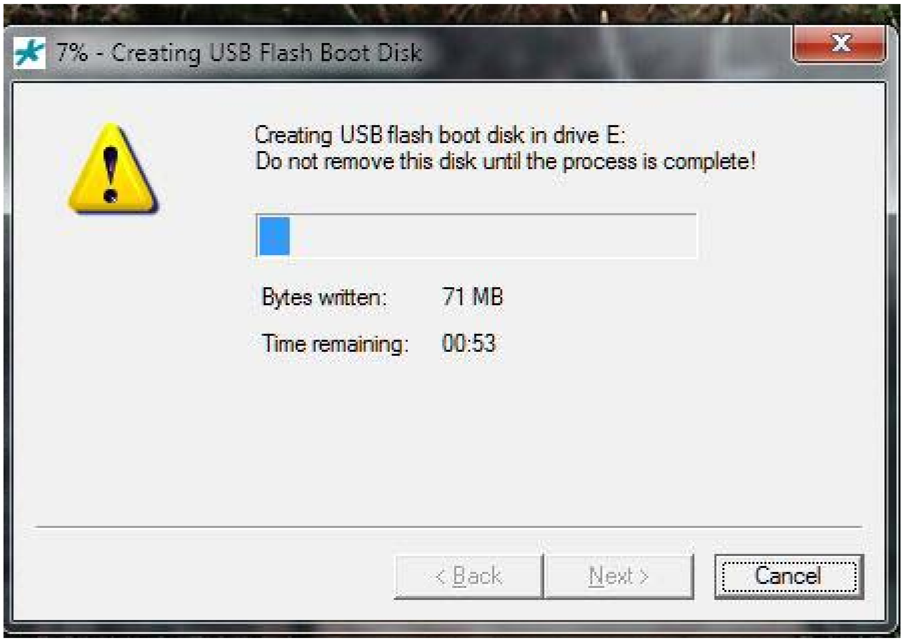
5. Heed the warning; click **Yes**.



Confirm

All data on drive E: will be deleted. Are you sure you want to proceed?

6. Wait while the BMC writes to the USB stick.



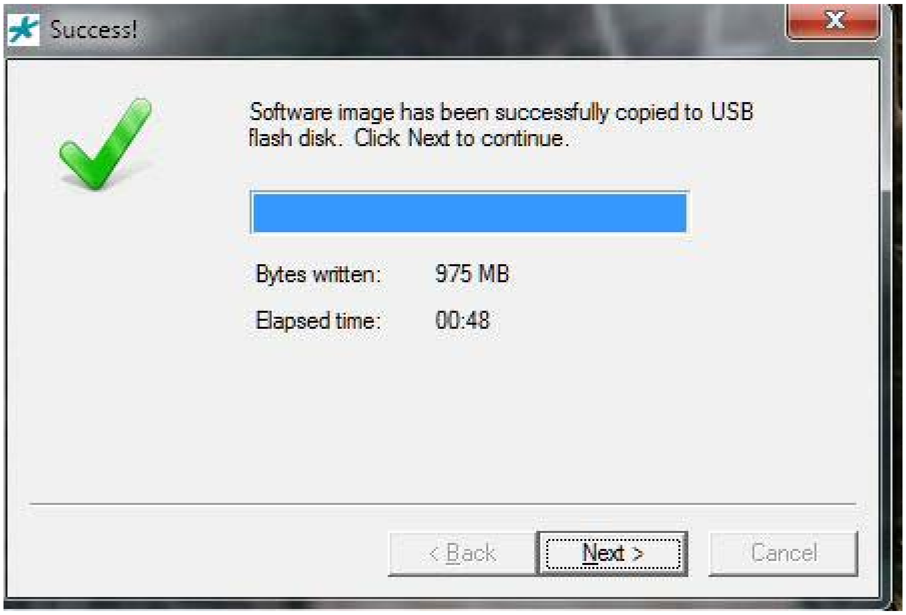
7% - Creating USB Flash Boot Disk

Creating USB flash boot disk in drive E:
Do not remove this disk until the process is complete!

Bytes written: 71 MB

Time remaining: 00:53

7. Click **Next** when the write operation completes.



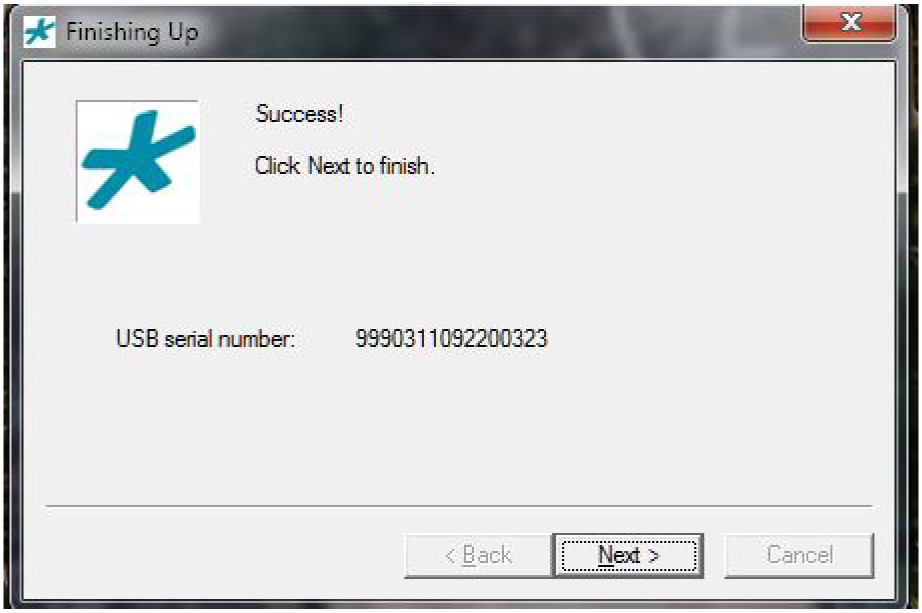
Success!

Software image has been successfully copied to USB flash disk. Click Next to continue.

Bytes written: 975 MB

Elapsed time: 00:48

8. Click **Next** to finish this write operation.



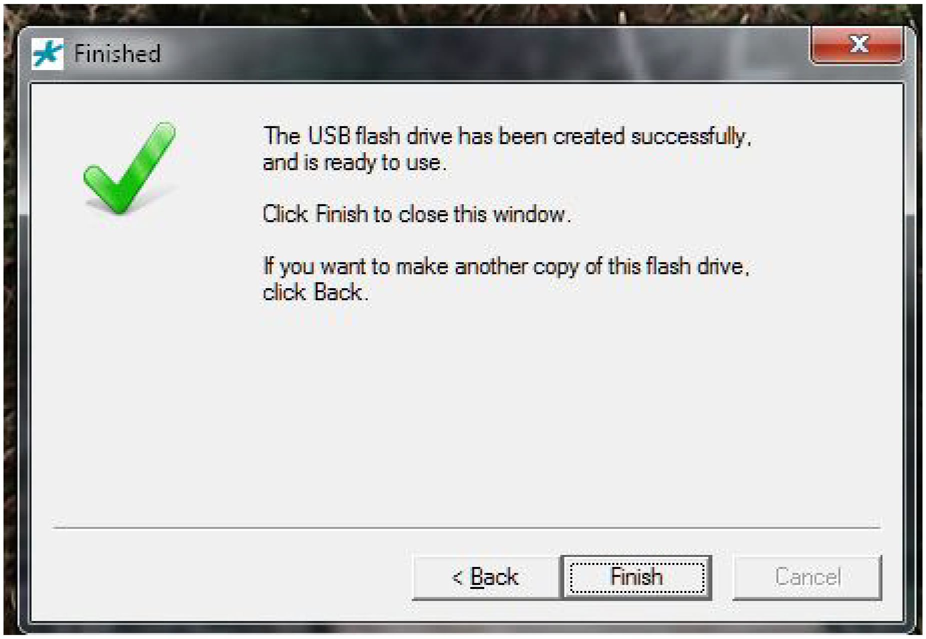
Success!

Click Next to finish.

USB serial number: 9990311092200323

Note: The displayed serial number, which identifies the USB stick, will be used by the end user to obtain product licenses.

9. Click **Back** to make another copy, or **Finish** to exit the BMC.



The USB flash drive has been created successfully, and is ready to use.

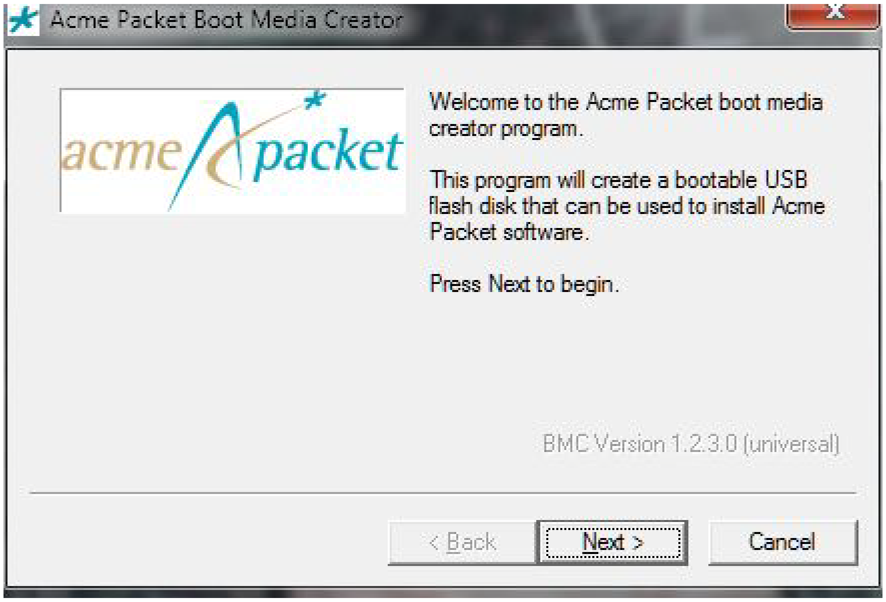
Click Finish to close this window.

If you want to make another copy of this flash drive, click Back.

Writing a Build Image and .tar Archive

Use the following procedure to create a USB Stick containing both a build image and a pre-installed *.tar* archive.

1. Open *nnSCz639-img-usb.exe*; click **Next**.



Acme Packet Boot Media Creator

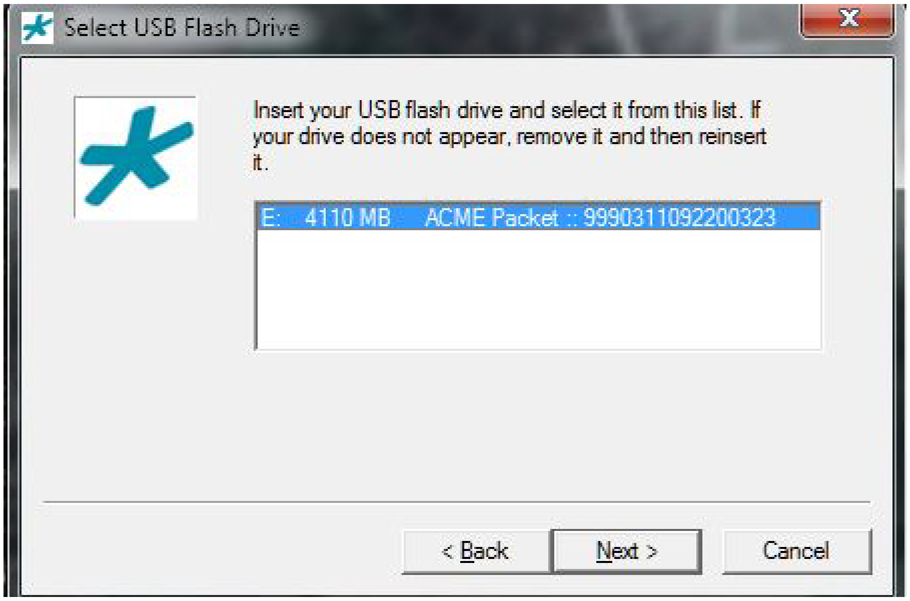
Welcome to the Acme Packet boot media creator program.

This program will create a bootable USB flash disk that can be used to install Acme Packet software.

Press Next to begin.

BMC Version 1.2.3.0 (universal)

2. Insert the USB stick and/or select it from the displayed list; click **Next**.

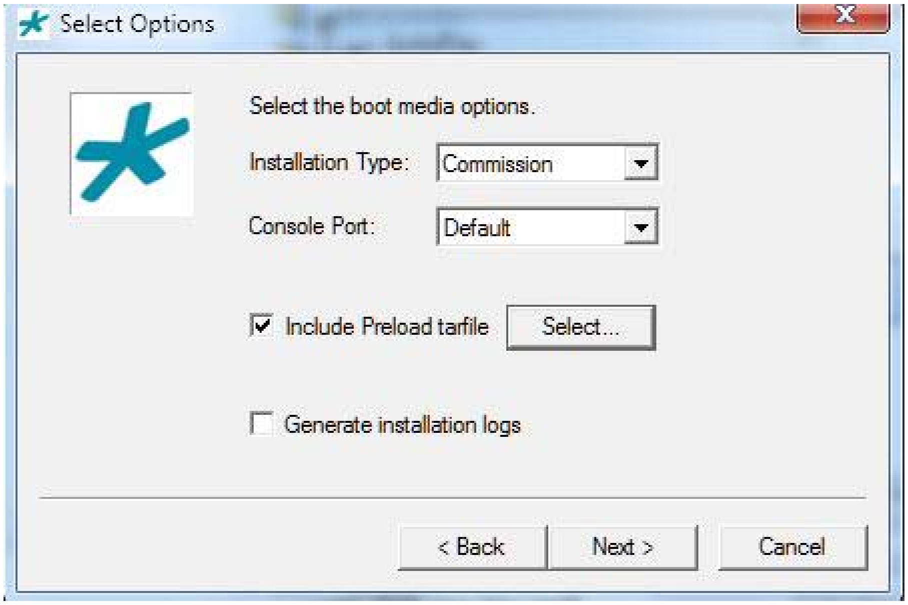


Select USB Flash Drive

Insert your USB flash drive and select it from this list. If your drive does not appear, remove it and then reinsert it.

E: 4110 MB ACME Packet :: 9990311092200323

3. To write both a build image and a *.tar* archive to the USB stick, select **Commission** as the *Installation Type*, and click *Include Preload tarfile* as shown below.



Select Options

Select the boot media options.

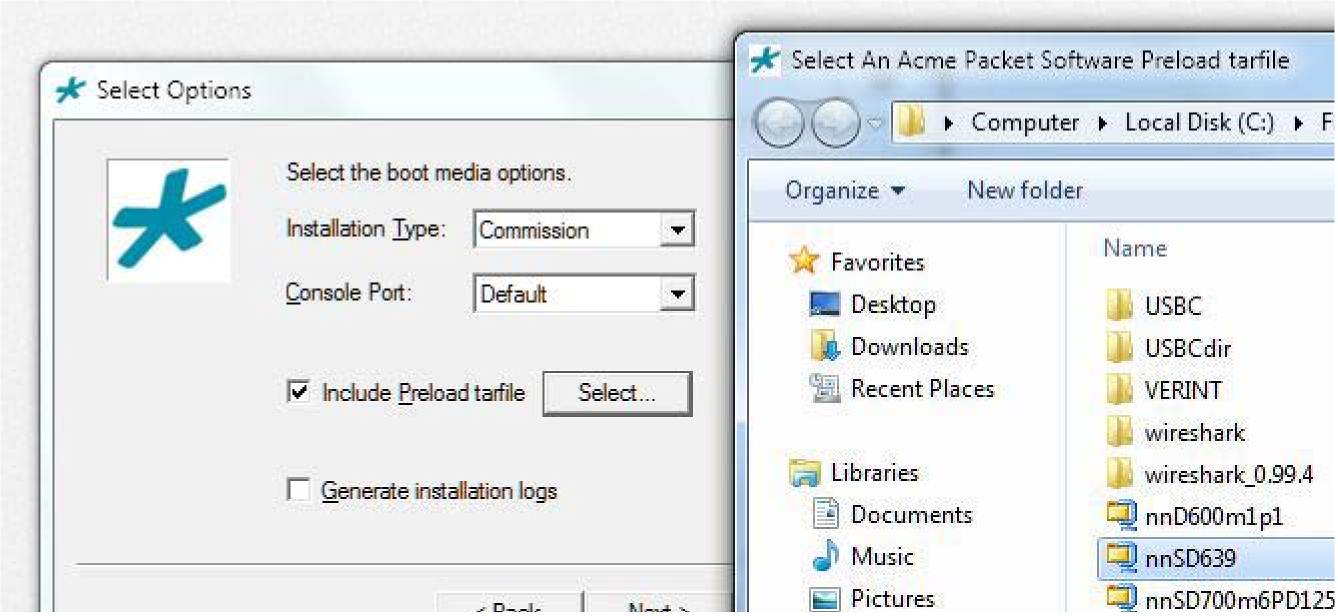
Installation Type: Commission

Console Port: Default

☑ Include Preload tarfile

□ Generate installation logs

4. Use the Select button to navigate to the compressed archive to be written to the USB stick, select the archive, and click **Next**.



Select Options

Select the boot media options.

Installation Type: Commission

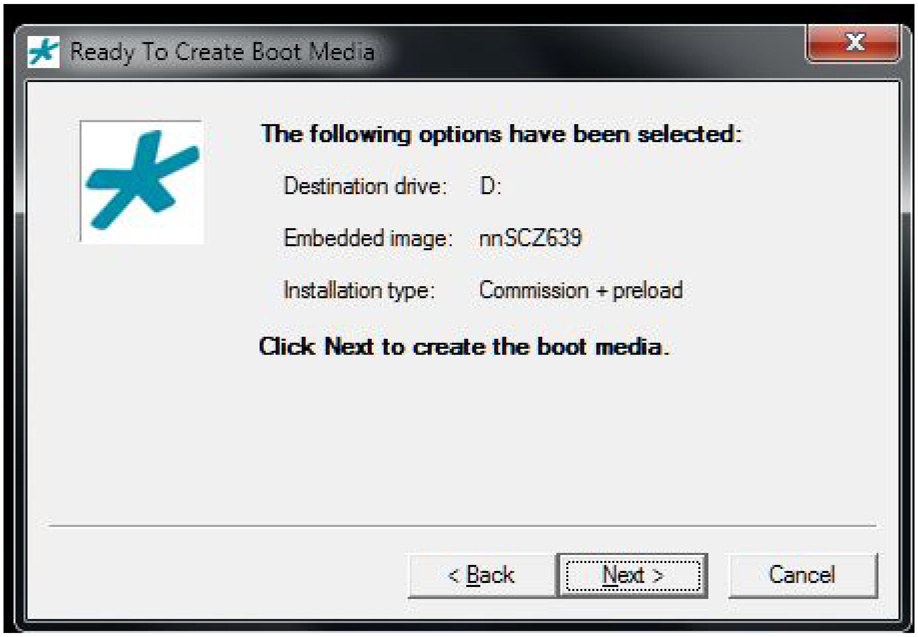
Console Port: Default

☑ Include Preload tarfile

□ Generate installation logs

Select An Acme Packet Software Preload tarfile

5. Confirm selected options; click **Next**.



Ready To Create Boot Media

The following options have been selected:

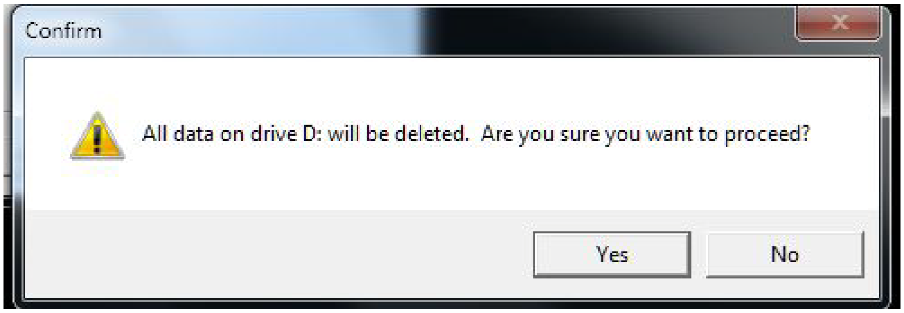
Destination drive: D:

Embedded image: nnSCZ639

Installation type: Commission + preload

Click Next to create the boot media.

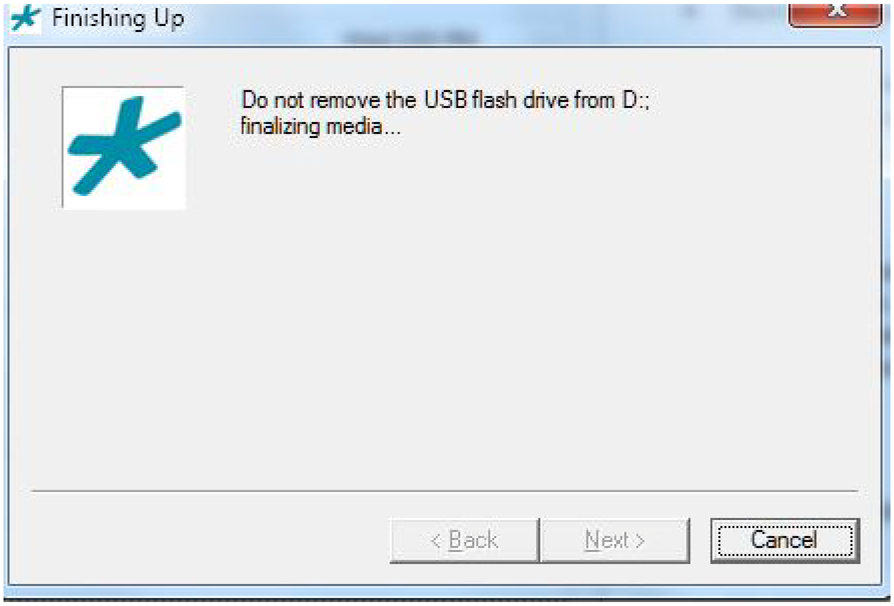
6. Heed the warning; click **Yes**.



Confirm

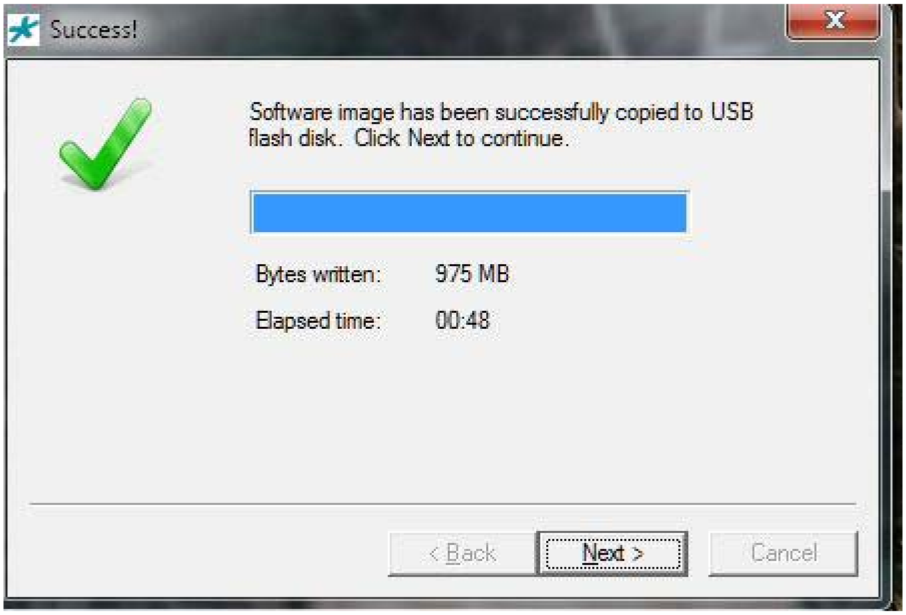
All data on drive D: will be deleted. Are you sure you want to proceed?

7. Wait while the BMC writes to the USB stick.



Do not remove the USB flash drive from D:; finalizing media...

8. Click **Next** to complete this write operation.

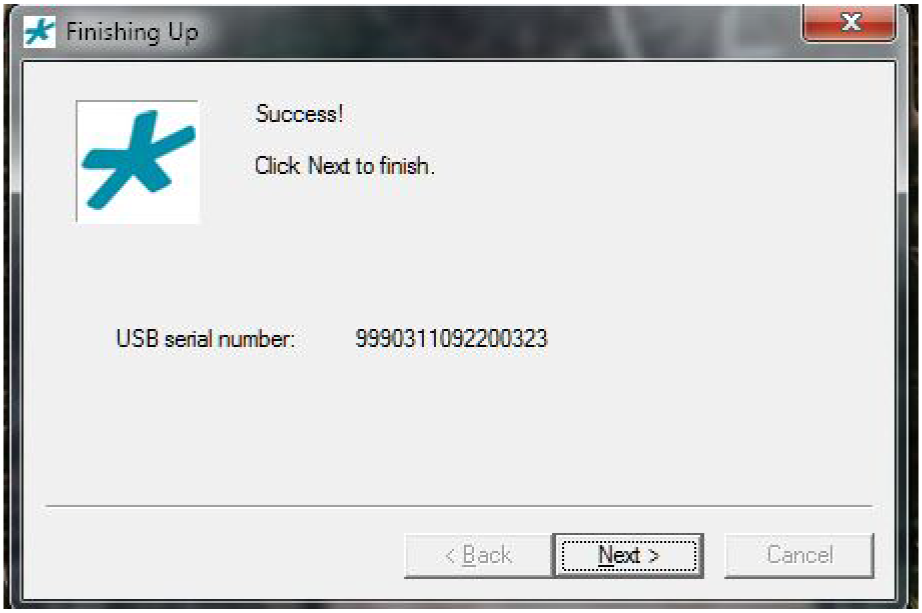


Software image has been successfully copied to USB flash disk. Click Next to continue.

Bytes written: 975 MB

Elapsed time: 00:48

9. Click **Next** to finish this write operation.



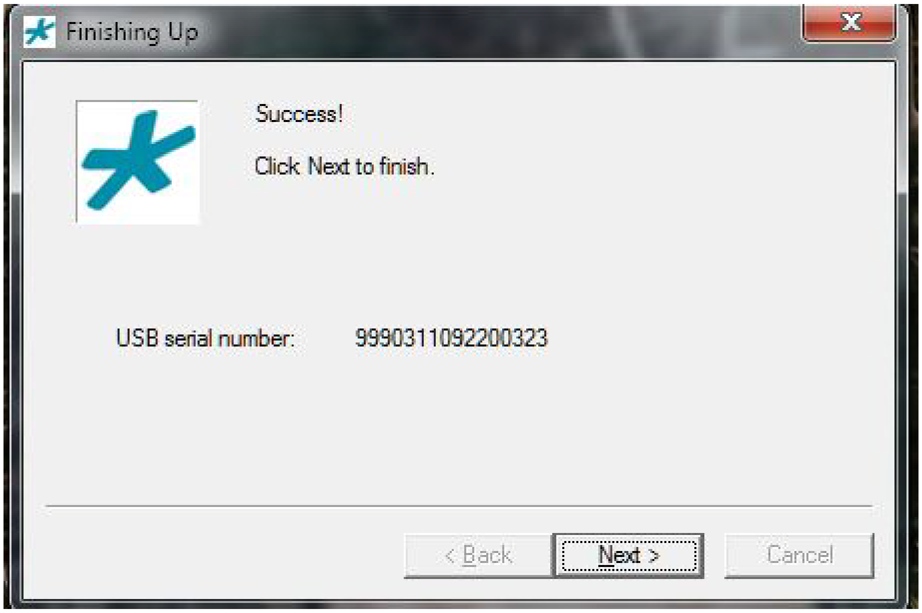
Success!

Click Next to finish.

USB serial number: 9990311092200323

Note: The displayed serial number, which identifies the USB stick, will be used by the end user to obtain product licenses.

10. Click **Back** to make another copy, or **Finish** to exit the BMC.



Success!

Click Next to finish.

USB serial number: 9990311092200323

Appendix C Format of Exported Text Files

Introduction

This Appendix provides a sample and format of each type of exported file from the Web-based GUI. Sample information in these files are provided as a reference for your convenience.

Exported file examples include:

- Session Summary exported file (text format)
- Session Details exported file (text format)
- Ladder Diagram exported file (HTML format)

For more information and a procedure for exporting files from the Web-based GUI, see Exporting Information to a Text File (114) in Chapter 7.

> **Note:** Oracle recommends you open an exported text file using an application that provides advanced text formating, such as Microsoft Word™. Opening the exported file using Notepad, or any other simple text editor can be difficult to read.

Exporting Files

The Web-based GUI allows you to export information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The data exports to a file that you can open and view as required.

You can export any of the following to a file:

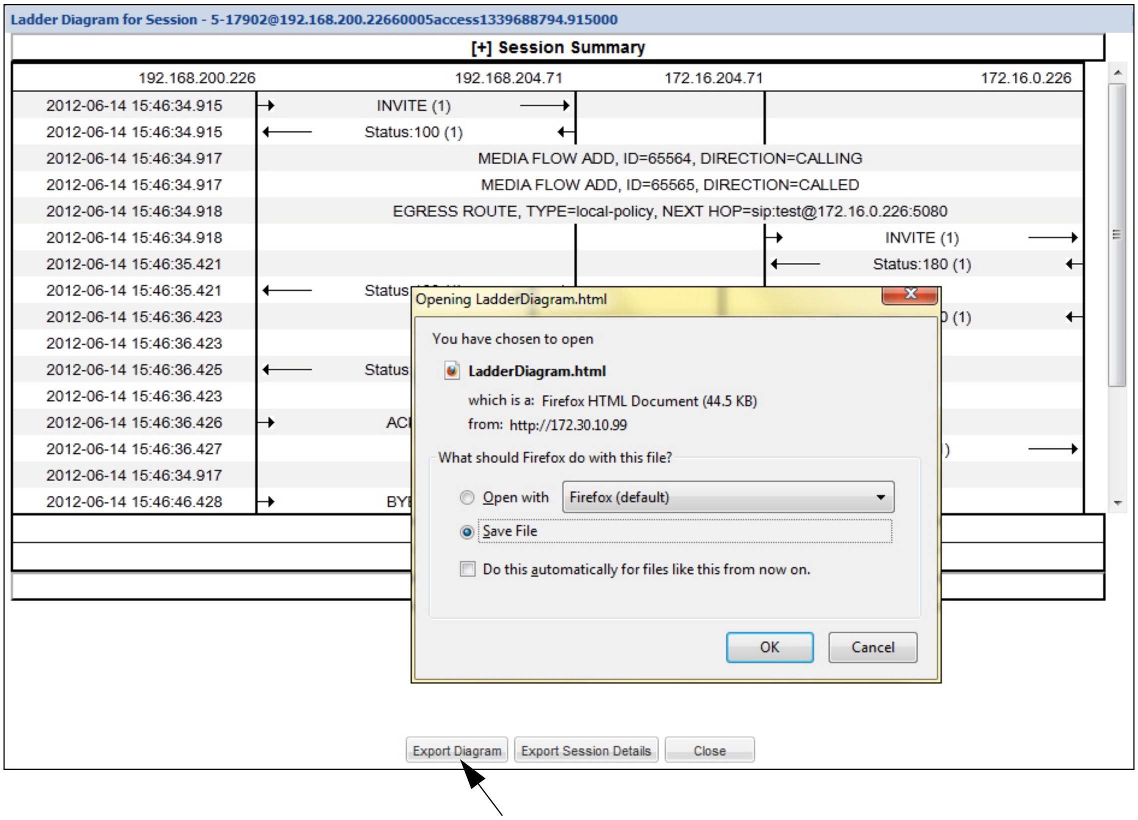
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:

- **Export session details** - Exports the SIP messages and media events associated with the selected session, to a text file.
- **Export summary** - Exports all logged session summary records, to a text file. (Exports ALL call session summary records or the records that matched a search criteria).

From the Ladder Diagram:

- **Export diagram** - Exports all of the information in the Ladder Diagram to an HTML file (Session Summary, SIP Message Details, and QoS statistics).
- **Export session details** - Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a text file.

The following is an example that shows the export of a Ladder Diagram to a file called “LadderDiagram.html”.



Ladder Diagram for Session - 5-17902@192.168.200.22660005access1339688794.915000

[+] Session Summary

```
                          192.168.200.226    192.168.204.71    172.16.204.71    172.16.0.226
2012-06-14 15:46:34.915   INVITE (1)
2012-06-14 15:46:34.915   Status:100 (1)
2012-06-14 15:46:34.917   MEDIA FLOW ADD, ID=65564, DIRECTION=CALLING
2012-06-14 15:46:34.917   MEDIA FLOW ADD, ID=65565, DIRECTION=CALLED
2012-06-14 15:46:34.918   EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:test@172.16.0.226:5080
2012-06-14 15:46:34.918   INVITE (1)
2012-06-14 15:46:35.421   Status:180 (1)
2012-06-14 15:46:35.421   Status
2012-06-14 15:46:36.423   0 (1)
2012-06-14 15:46:36.423
2012-06-14 15:46:36.425   Status
2012-06-14 15:46:36.423
2012-06-14 15:46:36.426   ACI
2012-06-14 15:46:36.427   )
2012-06-14 15:46:34.917
2012-06-14 15:46:46.428   BYI
```

Opening LadderDiagram.html

You have chosen to open

LadderDiagram.html

which is a: Firefox HTML Document (44.5 KB)

from: http://172.30.10.99

What should Firefox do with this file?

○ Open with Firefox (default)

● Save File

□ Do this automatically for files like this from now on.

Click <**Export Diagram**> to display the export dialog box.

The following paragraphs show examples of a:

- Session Summary Exported File (171) (text format)
- Session Details Exported File (172)(text format)
- Ladder Diagram Exported File (180) (HTML format)

Session Summary Exported File

The following is an example of a Session Summary exported text file from the Web-based GUI.

Example

```
----------Session Summary----------
Startup Time: 2011-09-20 12:58:44.375
State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=13451
Ingress Src Address:  172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone

----------Session Summary----------
Startup Time: 2011-09-20 12:58:05.340
State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=13450
Ingress Src Address:  172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone
```

Session Details Exported File

The following is an example of the a Session Details exported text file from the Web-based GUI.

Example

```
Session Details:

----------------------------------------
Nov  3 08:50:56.852 On [2:0]172.16.34.225:5060 received from
172.16.34.16:5060

INVITE sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length:  135

v=0
o=user1 53655765 2353687637 IN IP4 172.16.34.16
s=-
c=IN IP4 172.16.34.16
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----------------------------------------
Nov  3 08:50:56.855 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE


----MBCD Evt
Nov  3 08:50:56.862 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW ADD
```

```
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=
OutputDestPort=0
InputRealm=access
OutputRealm=backbone
----MBCD Evt
Nov  3 08:50:56.862 On 127.0.0.1:2945 received from 127.0.0.1:2944

mbcdEvent=FLOW ADD
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=65542
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=192.168.34.225
InputDestPort=20004
OutputSourcev4Addr=172.16.34.225
OutputDestv4Addr=172.16.34.16
OutputDestPort=6000
InputRealm=backbone
OutputRealm=access
----------------------------------------
Nov  3 08:50:56.865 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

INVITE sip:service@192.168.34.17:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
```

```
CSeq: 1 INVITE
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 140

v=0
o=user1 53655765 2353687637 IN IP4 192.168.34.225
s=-
c=IN IP4 192.168.34.225
t=0 0
m=audio 20004 RTP/AVP 0
a=rtpmap:0 PCMU/8000


----------------------------------------
Nov  3 08:50:56.868 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Length: 0


----------------------------------------
Nov  3 08:50:56.872 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Length: 0


----------------------------------------
Nov  3 08:50:56.872 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Type: application/sdp
Content-Length:  137

v=0
o=user1 53655765 2353687637 IN IP4 192.168.34.17
s=-
c=IN IP4 192.168.34.17
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000

----MBCD Evt
Nov  3 08:50:56.878 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW MODIFY
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
OutputRealm=backbone
----------------------------------------
Nov  3 08:50:56.881 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
```

```
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 138

v=0
o=user1 53655765 2353687637 IN IP4 172.16.34.225
s=-
c=IN IP4 172.16.34.225
t=0 0
m=audio 10004 RTP/AVP 0
a=rtpmap:0 PCMU/8000


----------------------------------------
Nov  3 08:50:56.883 On [2:0]172.16.34.225:5060 received from
172.16.34.16:5060

ACK sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-5
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 ACK
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0


----------------------------------------
Nov  3 08:50:56.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

ACK sip:192.168.34.17:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK48k3k1301ot00ssvf1v0.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 ACK
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Length: 0


----------------------------------------
```

```
Nov  3 08:51:01.883 On [2:0]172.16.34.225:5060 received from
172.16.34.16:5060

BYE sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0


----------------------------------------
Nov  3 08:51:01.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

BYE sip:192.168.34.17:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>
Max-Forwards: 69
Subject: Performance Test
Content-Length: 0


----------------------------------------
Nov  3 08:51:01.889 On [1:0]192.168.34.225:5060 received from
192.168.34.17:5060

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Length: 0


----------------------------------------
Nov  3 08:51:01.892 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060
```

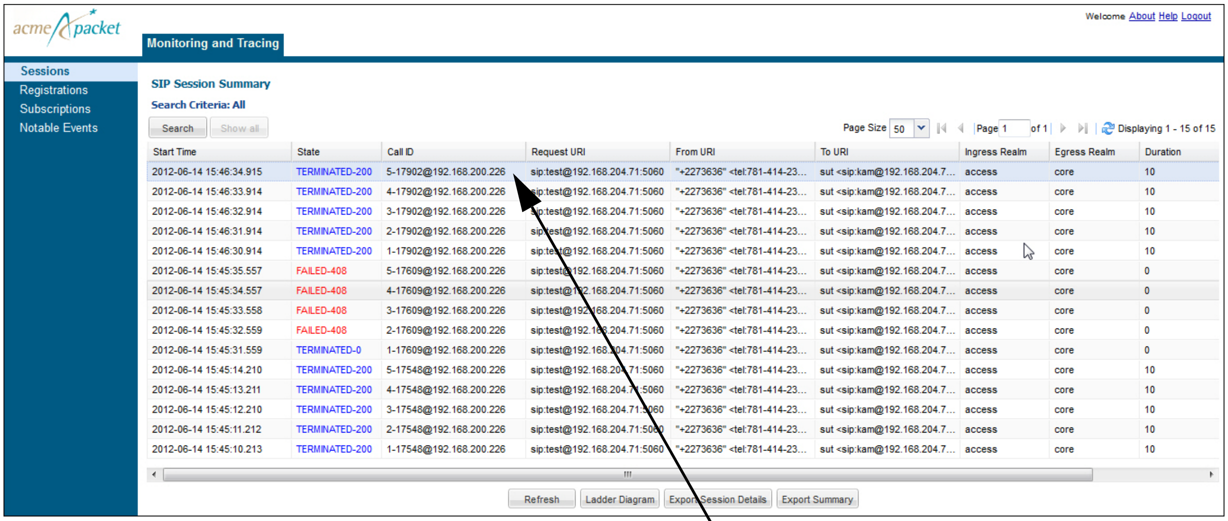
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 2 BYE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Length: 0


----MBCD Evt
Nov  3 08:51:01.891 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW DELETE
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
OutputRealm=backbone
----MBCD Evt
mbcdEvent=FLOW DELETE
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=65542
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=65541
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=192.168.34.225
InputDestPort=20004
OutputSourcev4Addr=172.16.34.225
```

```
OutputDestv4Addr=172.16.34.16
OutputDestPort=6000
InputRealm=backbone
OutputRealm=access

----------Session Summary----------
Startup Time: 2012-01-25 10:28:30.394
State: TERMINATED-200
Duration: 5
From URI: sipp &lt;sip:sipp@172.16.34.16:5060&gt;;tag=1
To URI: sut &lt;sip:service@172.16.34.225:5060&gt;;tag=2578
Ingress Src Address:  172.16.34.16
Igress Src Port: 5060
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone
```

Ladder Diagram Exported File

The following is an example of a Ladder Diagram for a session, exported to an HTML file from the Web-based GUI.

Example

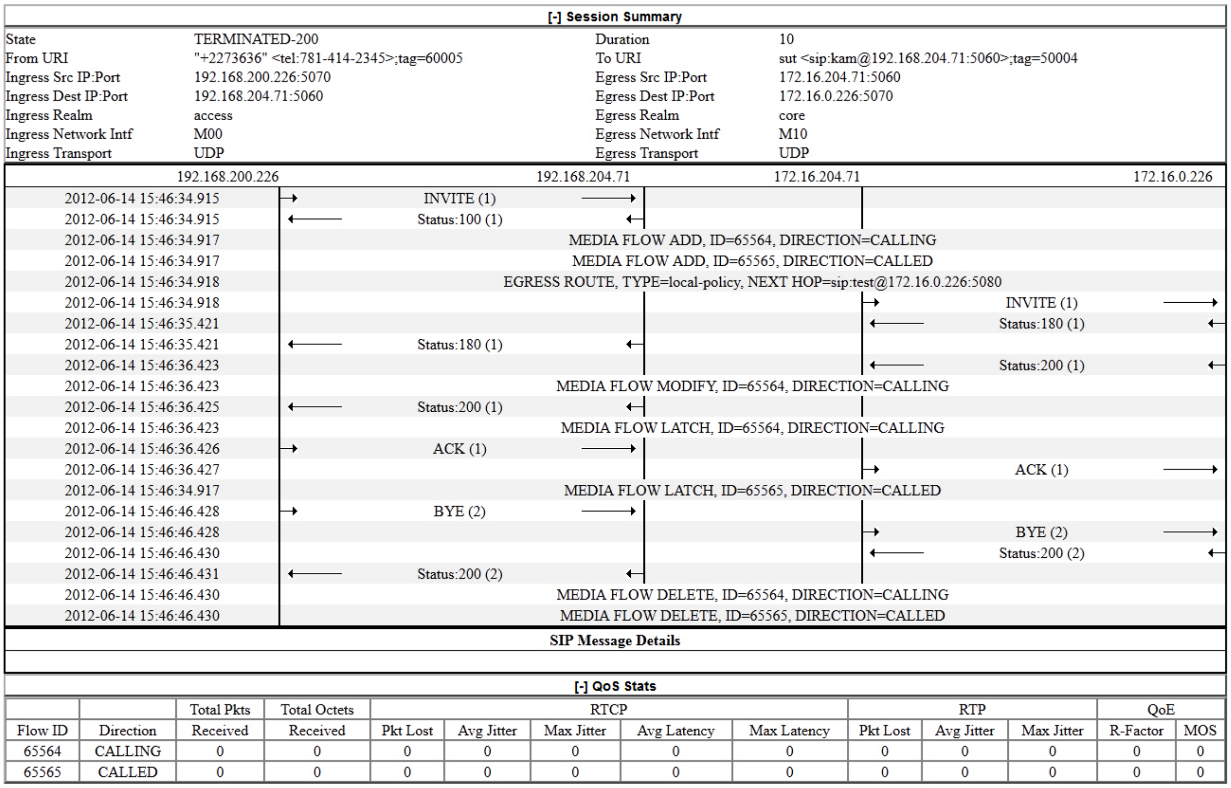


SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm	Duration
2012-06-14 15:46:34.915	TERMINATED-200	5-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:33.914	TERMINATED-200	4-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:32.914	TERMINATED-200	3-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:31.914	TERMINATED-200	2-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:46:30.914	TERMINATED-200	1-17902@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:35.557	FAILED-408	5-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:34.557	FAILED-408	4-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:33.558	FAILED-408	3-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:32.559	FAILED-408	2-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:31.559	TERMINATED-0	1-17609@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	0
2012-06-14 15:45:14.210	TERMINATED-200	5-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:13.211	TERMINATED-200	4-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:12.210	TERMINATED-200	3-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:11.212	TERMINATED-200	2-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10
2012-06-14 15:45:10.213	TERMINATED-200	1-17548@192.168.200.226	sip:test@192.168.204.71:5060	"+2273636" <tel:781-414-23...	sut <sip:kam@192.168.204.7...	access	core	10

Ladder Diagram is from selected session



[-] Session Summary

State	TERMINATED-200	Duration	10
From URI	"+2273636" <tel:781-414-2345>;tag=60005	To URI	sut <sip:kam@192.168.204.71:5060>;tag=50004
Ingress Src IP:Port	192.168.200.226:5070	Egress Src IP:Port	172.16.204.71:5060
Ingress Dest IP:Port	192.168.204.71:5060	Egress Dest IP:Port	172.16.0.226:5070
Ingress Realm	access	Egress Realm	core
Ingress Network Intf	M00	Egress Network Intf	M10
Ingress Transport	UDP	Egress Transport	UDP

	192.168.200.226	192.168.204.71	172.16.204.71	172.16.0.226
2012-06-14 15:46:34.915	INVITE (1) →			
2012-06-14 15:46:34.915		← Status:100 (1)		
2012-06-14 15:46:34.917	MEDIA FLOW ADD, ID=65564, DIRECTION=CALLING			
2012-06-14 15:46:34.917	MEDIA FLOW ADD, ID=65565, DIRECTION=CALLED			
2012-06-14 15:46:34.918	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:test@172.16.0.226:5080			
2012-06-14 15:46:34.918			INVITE (1) →	
2012-06-14 15:46:35.421				← Status:180 (1)
2012-06-14 15:46:35.421		← Status:180 (1)		
2012-06-14 15:46:36.423				← Status:200 (1)
2012-06-14 15:46:36.423	MEDIA FLOW MODIFY, ID=65564, DIRECTION=CALLING			
2012-06-14 15:46:36.425		← Status:200 (1)		
2012-06-14 15:46:36.423	MEDIA FLOW LATCH, ID=65564, DIRECTION=CALLING			
2012-06-14 15:46:36.426	ACK (1) →			
2012-06-14 15:46:36.427			ACK (1) →	
2012-06-14 15:46:34.917	MEDIA FLOW LATCH, ID=65565, DIRECTION=CALLED			
2012-06-14 15:46:46.428	BYE (2) →			
2012-06-14 15:46:46.428			BYE (2) →	
2012-06-14 15:46:46.430				← Status:200 (2)
2012-06-14 15:46:46.431		← Status:200 (2)		
2012-06-14 15:46:46.430	MEDIA FLOW DELETE, ID=65564, DIRECTION=CALLING			
2012-06-14 15:46:46.430	MEDIA FLOW DELETE, ID=65565, DIRECTION=CALLED			

SIP Message Details

[-] QoS Stats

		Total Pkts	Total Octets	RTCP					RTP			QoE	
Flow ID	Direction	Received	Received	Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
65564	CALLING	0	0	0	0	0	0	0	0	0	0	0	0
65565	CALLED	0	0	0	0	0	0	0	0	0	0	0	0