Net-Net 2600

Release 3.6.0M2

Release Notes

780-0004-00
Revision 1.20
June 18, 2010

Notices

Contents

NN2600
Release Notes, Version 3.6.0

NN2600
Release Notes, Version 3.6.0

This notice describes the current release of the Acme Packet NN2600® software. NN2600 systems and third-party hardware running the NN2600 software provide application level security, control, monitoring and interoperability services for real-time communication and collaboration applications and VoIP services based on the Session Initiation Protocol (SIP).

Note: For existing customers who are upgrading from a prior release, the Covergence hardware and software components have been renamed under Acme Packet, Inc., as follows:

- Covergence — now **Acme Packet**
- Session Manager — now **Net-Net 2600 (NN2600)**
- CMS Web — now **NN2600 Management System**
- CXC-354 — now **NN2610**
- CXC-554 — now **NN2620**
- CVA — now **Net-Net 2600 Virtual Machine (or NN2600-VM)**
- CLI prompt — now **NNOS-E** (default)

You should review this notice for details about Release 3.6.0, information about operational considerations and known issues from prior releases, and for instructions on installing and upgrading to this release.

Contacting Acme Packet

Acme Packet, Inc.
71 Third Avenue
Burlington, MA 01803 USA
t: 781-328-4400
f: 781-425-5077

www.acmepacket.com

Evaluation site information

Product evaluation sites are provided with a customer-specific Web site URL that connects to the Acme Packet Support Web page. This page provides current software downloads, documentation, MIBs, and troubleshooting information.

For problem reporting and technical support, e-mail Acme Packet at support@acmepacket.com

Technical documentation

Acme Packet provides the following documentation set in PDF format, viewable using Adobe Reader 5.0 or later. These PDF files are available when you download NN2600 software from Acme Packet, as well from your customer Web portal.

- *Net-Net 2600 – Net-Net 2610/2620 Quick Installation*
- *Net-Net 2600 – Network Interface Card Installation*
- *Net-Net 2600 – USB Creation and Commissioning Instructions*
- *Net-Net 2600 – Slide Rail Kit Installation Instruction*
- *Net-Net 2600 – Virtual Machine Information Guide*
- *Net-Net 2600 – System Installation and Commissioning Guide*
- *Net-Net 2600 – Using the NN2600 Management Tools*
- *Net-Net 2600 – System Administration Guide*
- *Net-Net 2600 – Session Services Configuration Guide*
- *Net-Net 2600 – Objects and Properties Reference*

- *Net-Net 2600 – System Operations and Troubleshooting*

Note: Acme Packet provides updates to the manuals on a regular basis. Go to your Acme Packet Web portal for the latest files in PDF format.

Release note revision history

This section contains a revision history for this document.

Date	Revision Number	Description
December 14, 2009	Revision 1.01	• Initial Release of 3.6.0 software.
March 9, 2010	Revision 1.10	• Updates document to include 3.6.0m1 adaptations.
June 18, 2010	Revision 1.20	• Updates document to include 3.6.0m2 adaptations.

Net-Net 2600: 2610 and 2620 Series models

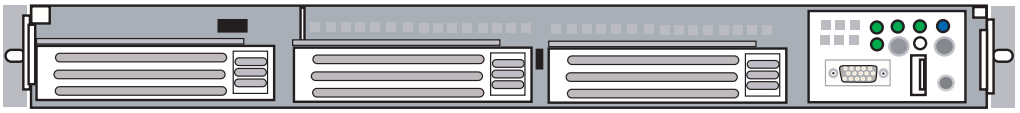
Acme Packet provides the NN2600 NN2610 and NN2620 Series systems in the following configurations:

- **NN2610**— 1U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with one non-redundant AC power supply and cooling fans; six (6) Ethernet ports with optional network interface cards; 750 GB hard disk storage; standard 8GB memory. Commissioned using an Acme Packet NN2600 USB stick.
- **NN2620** — 2U rack-mountable chassis, 120/240V AC powered, dual quad-core processor system with redundant, hot swappable power supplies and cooling fans; six (6 ethernet ports and up to twelve (12) Ethernet ports with optional network interface cards; 750 GB hard disk storage with RAID; and standard 8GB memory. Commissioned using an Acme Packet NN2600 USB stick.

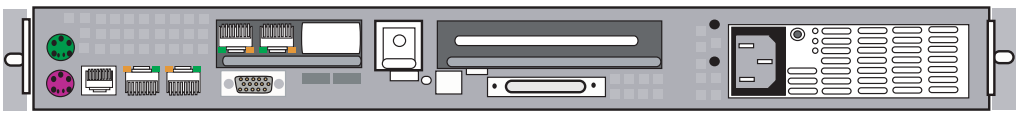
The following image illustrates the NN2600 — NN2610 (1U) chassis views.

NN 2610 with front bezel

NN 2610 with front bezel removed



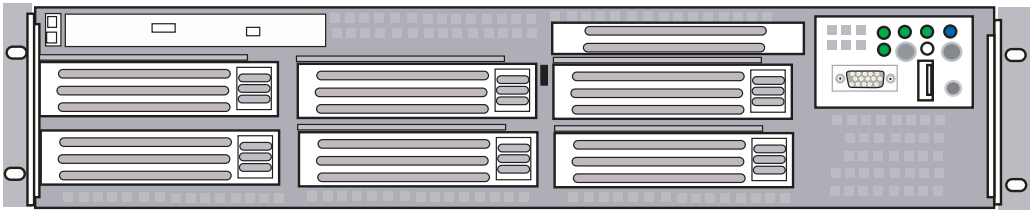
NN 2610 back view



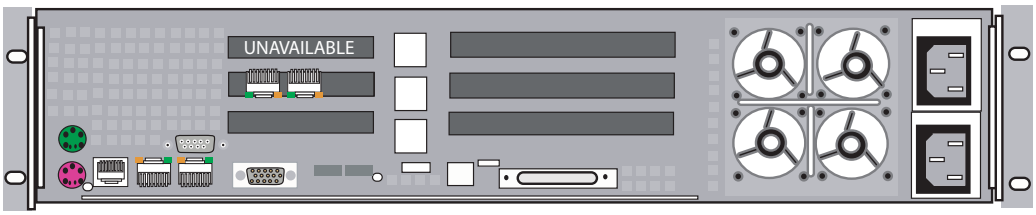
The following image illustrates the NN2600 — NN2620 (2U) chassis views.

NN 2620 with front bezel

NN 2620 with front bezel removed



NN 2620 back view



New system hardware installation

For information on the physical installation of the specific NN2600 model, refer to the following documents:

- *Net-Net 2600 – Net-Net 2610/2620 Quick Installation*
  - — Included in the shipping container.
- *Net-Net 2600 – USB Creation and Commissioning Instructions*
  - — Included with the NN2600 software download; covers installation on hardware and third-party platforms and blades.
- *Net-Net 2600 – System Installation and Commissioning Guide*

— Included with the NN2600 documentation set.

New installations require that you attach a local terminal or PC to the RJ-45 RS-232D Serial port. See the appropriate document (listed above), for information on making these connections.

Third-party platforms and blades

The NN2600 software is supported on third-party platforms and blades as part of integrated solutions that can only be obtained through authorized OEM partners.

For additional details, contact your Acme Packet representative.

NN2600 Virtual Machine

The NN2600, available as a VMware®, XEN, or ESX virtual machine (VM), runs on x86-based PCs and servers, and offers the majority of the operational features and capabilities provided by physical NN2600 devices, such as the NN2610, NN2620.

The VM is intended for SIP customers who are interconnecting branch offices and small businesses to SIP service providers. The VM supports up to 50 concurrent SIP media sessions.

For complete information on downloading and running the VM on compatible x86-based PCs and servers, refer to the *Net-Net 2600 – Virtual Machine Information Guide*.

Software download and commissioning process

The software download mechanism allows new and existing customers to acquire NN2600 software directly from Acme Packet. Using secure URLs that can be accessed over the internet, Acme Packet provides all necessary software downloads for USB creation, product licensing, and commissioning of your selected hardware.

As part of each download, and depending on your actual requirements, Acme Packet provides the following:

- Acme Packet Boot Media Creator with the NN2600 Release 3.6 software.
- Feature licenses.
- Documentation on how to create a NN2600 USB stick for commissioning the software on your selected hardware.
- Standard set of NN2600 technical publications.

If not included in the shipment, you will need to provide a USB stick with between 1-4GB storage to handle NN2600 software downloads. Acme Packet has tested a variety of USB sticks available from current suppliers and manufacturers. Most USB sticks manufactured today will work.

For complete information on accessing the Acme Packet download server, creating an installation USB, and commissioning a NN2600 device, refer to the *Net-Net 2600 – USB Creation and Commissioning Instructions*.

Upgrading to Release 3.6.0

This section explains now to upgrade to Release 3.6.0 from previous releases of the NN2600.

Upgrading to Release 3.6.0m2 from Release 3.6

From Release 3.6, perform the upgrade to Release 3.6.0m2 using the following procedure.

> **Note:** Acme Packet recommends you run the procedure from a local console so you do not lose connectivity during the procedure itself. If you choose to run the upgrade remotely over Telnet, or from the CMS Web **Tools** option, you will not be able to observe when the NN2600 has completed the upgrade process.
>
> **Note:** When upgrading from 3.6m1 to 3.6m2 with H.323 configured, you must contact Acme Packet technical support to obtain the transform utility for the upgrade to work properly.

Perform the following steps:

1. Copy or run TFTP to copy the following file to the /cxc directory on the NN2600.

- nnSE360m2.tar.gz

  If you are currently logged on using the CMS Web, you can use the **Tools/ Upload File** option to browse for the file on your local PC or network location to obtain the file to upload to the NN2600.

2. At the NNOS-E prompt, run the install program, as follows:

```
NNOS-E> install file nnSE360m2.tar.gz
Are you sure (y or n)? y
Installing: nnSE360m2.tar.gz
Success! Rebooting Session Manager
```

If you are using the CMS Web to perform the upgrade remotely, use the CMS **Tools/ Update Software** option with the "Install the Update" selection checked off to run the upgrade.

Upgrading to Release 3.6.0 from Release 3.5.x

The accounting functionality has changed from release 3.5.x to release 3.6.0. When purging is enabled, your NN2600 accounting service deletes all 3.5.x unpersisted CDRs it finds during the upgrade process.

In order to not lose any raw CDRs, you must find accounting targets which have not received all applicable CDR data using the **scan utility** to view an accounting store to see if there are any unpersisted CDRs in the 3.5.x version that need to be persisted before the upgrade to 3.6.0 can be done. The execution of the scan utility action is performed in the shell.

1. Copy or run TFTP to copy the following file to the /cxc directory on NN2600.

   - accounting35store

   If you are currently logged on using the NN2600 Management System, you can use the **Tools/Upload File** option to browse for the file on your local PC or network location to get the file uploaded to NN2600.

2. Stop running traffic. This allows any lagging accounting service time to catch up.

3. At the NNOS-E> prompt, enter the **shell** action as follows:

```
NNOS-E> shell
localhost app_slot_1 #
```

4. Enter the scan utility command using the following syntax:

```
localhost app_slot_1 # accounting35store -s [3.5x store location]
-m [target]
```

where:

- -s—Specifies the accounting store folder. The location of this folder is specified in the configuration under the **accounting-root-directory**.
- -m—Specifies the mode for results which can be **target** (results per target), **file** (results per file), or **incomplete** (list incomplete files only; default behavior)

For example:

```
localhost app_slot_1 # accounting35store -s /acme_common/
accounting35/test1/ -m target
```

The following are more arguments you can use with the **scan utility** to narrow down your accounting target search:

- -f—Specifies an individual file to check
- -csv—Output the results in CSV format
- -w—The results are printed into this file.
- -force—Scan every file
- -d—Specifies the debug mode which can be **error** (only errors are printed; default), **info** (information level messages are printed), or **debug** (debug level messages are printed)
- -h—Displays the help for the scan utility.

5. If any bad accounting targets are found, fix them. The following is an example of the message you receive when a bad target is found:

```
localhost app_slot_1 # accounting35store -s /acme_common/
accounting35/test1/ -m target
-----------------------------------------------------------------
***  Failed Targets ***
-----------------------------------------------------------------
  1. vsp\accounting\database\group mssqlDB
         server-name:
                type: database
              failed: 24
-----------------------------------------------------------------
```

6. Allow accounting service to run until processing is complete. To ensure the process is complete you can execute the **scan utility** again.

After all of this has been completed, you can begin the upgrade process.

If you are currently running Release 3.5.x, perform the upgrade to Release 3.6.0 using the procedure covered in the section using the Release 3.6.0 tar file, available from your Acme Packet Web portal.

Caution: Acme Packet recommends that you run the upgrade procedure from a local console so that connectivity is not lost during the procedure itself. If you choose to run the upgrade remotely over Telnet, or from the NN2600 Management System **Tools** options, you will not see when the NN2600 device has completed the upgrade process.

To upgrade the NN2600, perform the following steps:

1. From the current configuration, save the standard configuration using a unique file name of your choice with the .cfg extension. Preserve this file as a backup copy of your configuration if you need to revert to the earlier release.

   For example:

   ```
   NNOS-E>> config save standard cxcbackup.cfg
   Success
   ```

2. Save the configuration as an XML file.

   For example:

   ```
   NNOS-E>> config save xml /cxc_common/cfg35.xml
   Success
   ```

3. Copy or run TFTP to copy the following files to the /cxc directory on NN2600.

   - nnSE360m2.tar.gz

   If you are currently logged on using the NN2600 Management System, you can use the **Tools/Upload File** option to browse for the file on your local PC or network location to get the file uploaded to NN2600.

4. At the NNOS-E> prompt, run the **install** program, as follows:

   ```
   NNOS-E>> install file nnSE360m2.tar.gz
   Are you sure (y or n)? y
   Installing: nnSE360m2.tar.gz
   Success! Rebooting Net-Net OS-E
   ```

5. Convert the Release 3.5 configuration using the following style sheet:

   - 3.5-to-3.6.xls

```
NNOS-E>> xml transform 3.5-to-3.6.xls /cxc_common/cxc35.xml
cxc36m2.xml
Success!
```

6. Replace the configuration file with the new file named cxc36m1.xml

   ```
   NNOS-E>> config replace cxc36m2.xml
   ```

7. Save the configuration in standard format using the default configuration file name (cxc.cfg).

   ```
   NNOS-E>> config save standard cxc.cfg
   ```

8. Perform a restart warm to boot with the new configuration.

   ```
   NNOS-E>> restart warm
   ```

If you are using the NN2600 Management System to perform the upgrade remotely, use the **Tools/Update Software** option with the "Install the Update" selection checked off to run the upgrade.

Upgrading to Release 3.6.0 from Release 3.4.2 or later

If you are currently running Release 3.4.2, 3.4.3 or 3.4.4, you should perform the upgrade to Release 3.6.0 from a USB stick. Refer to the *Net-Net 2600 – USB Creation and Commissioning Instructions* for information on creating the USB stick and commissioning the NN2600 device. Contact Acme Packet for assistance when performing these upgrades.

Note: When upgrading from release 3.4 to releases 3.5 or 3.6 on third party hardware, a manual procedure must be performed to ensure that the interfaces remain on the current ethernet ports. For more information about this, contact Acme Packet technical support.

Special considerations after running the upgrade

NN2600 creates an alternate, inactive directory that captures the files associated with the release from which you are upgrading. This inactive directory holds customer-created configuration files and phone configurations. You may need to access this directory to copy these custom files to the new active release directory. Otherwise, for example, SIP phones may not work properly.

The release files associated with the older release are moved to a directory of the form:

/cxc_rel/app-<slot 1-3>

where "app" is a literal text string, followed by the version and release numbers that are explicit to the release software.

Acme Packet recommends that you place a copy of any uploaded configuration or phone files into a common directory for easy access when upgrades are completed. For example, copy the files into the /cxc_common/ directory so that the files remain there after any upgrade.

Release 3.6.0m2

New Features

The following sections describe the new features that have been added to Release 3.6.0m2.

Route Server Tandem Routing Enhancement

The NN2600 now supports tandem hop route server functionality when a call must traverse regions. In previous NN2600 releases, only specific gateways configured locally were routed.

When the NN2600 receives a response from the route server, it looks for a specific match configured on the sip-gateways. Both the carrier and endpoint tags must match for the NN2600 to route the server.

The **settings > named-lookup-match** property allows you to configure a secondary lookup system. When an endpoint does not match, this property allows you to either match all endpoints under the carrier, or use DNS to resolve the endpoint as an FQDN. For more information on the **named-lookup-match** property, see Configuration changes in Release 3.6.0m2.

Improved ANI Configurations For H.323-SIP Calls

In releases prior to 3.6.0m2, the NN2600 required specification of the ANI source for use in creating the SIP From: header URI. The NN2600 is now flexible while creating the SIP From: header used for inbound H.323 calls that are interworked to SIP and ensures the From: header always contains a complete URI.

A property, **useanon**, under the **h323-to-sip-fromheader-spec** object, has been created to enable this functionality. For more information on the useanon property, see Configuration changes in Release 3.6.0m2. When this property is enabled, the From: header is assembled in the following manner:

- The configured scheme (default value sip:) is always used.
- The configured user is then appended. This value can be taken from the Q931 Calling Party Number, the sourceAddress alias in the Setup-UUIE (h323-id, url-id, or email-id), or a configured string. If this portion is omitted, the user is automatically set to “anonymous.”
- The configured host is then appended. This value can be taken from the configured h323-server domain, the sourceAddress alias in the Setup-UUIE (h323-id, url-id, or email-id), or a configured string. If this portion is omitted, the host is automatically set to the IP address of the H.323 gateway which transmitted the Setup.
- The configured suffix is then appended. This value defaults to an empty string unless otherwise configured by the NN2600 Administrator.

Linking H.323 Servers to Services Routing Mechanics

The NN2600 now uses standard services routing to dynamically identify the most appropriate local interface and listening port to use and advertise for each remote H.323 gateway and gatekeeper. When the H.323 process starts, services routing is consulted to determine the most appropriate local listening ports to use when contacting the server for each configured H.323 server.

The following lists the types of remote H.323 servers that can be configured on a NN2600 and the way the NN2600 binds listening ports to servers for each type:

- A remote H.323 Gateway (GW). This configuration is often referred to as “GW-GW.” No specific listeners are bound to the configured remote H.323 GW. When the NN2600 makes an outbound H.323 call, services routing is used to select the appropriate local interface for reaching the remote H.323 GW and establishing H.225.0 and H.245 TCP connections.

- A remote H.323 Gatekeeper (GK) where the NN2600 contacts the remote GK as an H.323 GW. This configuration is often referred to as “GW-GK.” An H.225.0 RAS listener and H.225.0 call signal listener are bound to each remote GK (both active and standby). When the NN2600 registers, these listeners are sent to the remote GK. If the GK supplies any alternate GKs, the NN2600 binds RAS and H.225.0 call signal listeners to each alternate GK.
- A remote H.323 GK where the NN2600 contacts the remote GK as a peer GK. This configuration is often referred to as “GK-GK.” An H.225.0 RAS listener and an H.225.0 call signal listener are bound to the remote peer GK. If the NN2600 confirms a location request from that GK, these listeners are transmitted to the peer GK.

Thus, there are 3 types of H.323 listening ports that can be configured on the NN2600. All H.323 listening ports are configured under a particular interface and IP address. The following table displays the port types that can be configured:

Configuration	Port	Transport	Use
h323 > port	H.225.0 Call Signaling	TCP	All
h323 > gatekeeper-port > port-type=peer	H.225.0 RAS	UDP	GK-GK
h323 > gatekeeper-port > port-type=client	H.225.0 RAS	UDP	GW-GK

Peer Gatekeeper Support on the NN2600

The NN2600 allows for the configuration of external peer gatekeepers. A peer gatekeeper (peer-GK) is an H.323 gatekeeper that communicates with the NN2600 via Location Request (LRQ) messages for call routing information.

The following configurations must be applied for the peer-GK to function properly on the NN2600:

- A peer-GK must have a unique IP address.
- A peer-GK’s IP address and UDP RAS port must be configured in the first server-pool entry.
- The server-pool for a configured peer-GK must have only one entry.

- At least one peer GKPort must be configured. The NN2600 creates a UDP listener for each GKPort specified.

Note: Clustered GK support exists only for non-peer GKs.

A peer-GK is configured in the **vsp > enterprise > servers** object. The following example shows a configuration for a peer-GK:

```
   config h323-server GnuGK-Peer-FC4
    set server-type h323-gatekeeper
    config server-pool
     config server GnuGK-Peer-FC4
      set host 172.44.200.35
      set port 1719
      set local-ip 172.44.10.67
      set connection-role responder
     return
    return
    set local-server-type h323-gatekeeper
    set ras-settings 3600 5 3 X +1 h323ID disabled false false 10 false
PollRejected 15 5 5 15
    config h225-settings
     set h323-user-alias dialedDigits
    return
   return
```

It is possible to specify the RAS listening port for peer-GK communication. This is configured in the box > interface > ip > h323 > gkport. The following example shows a configuration for two listening TCP ports accepting inbound H.323 call requests (ports 1720 and 1721) and two listening UDP ports for accepting peer-GK RAS traffic (1719 and 1725):

```
   config interface eth0
      config ip federate-a
       set ip-address static 172.44.10.67/16
       config h323
        set port 1720
        set port 5021
        set port 5022
        set port 5023
        set gatekeeper-port 1717 client
        set gatekeeper-port 1719 peer
        set gatekeeper-port 1748 client
        set gatekeeper-port 7000 peer
```

If destination route lookup for the LRQ succeeds, an LCF message is sent by the NN2600 to the peer-GK. The location confirmation message contains the IP address and port indicated by the destination route lookup engine. The location confirmation rasAddress is set to the NN2600 local IP and port used for RAS messaging to this peer.

The following table lists conditions when LRQ will not be confirmed. In some cases the LRQ will be silently discarded and in others an LRJ will be generated by the NN2600:

Errors encountered during processing LRQ	Action
Remote GK not found in config	Discard LRQ
Remote GK not peer	Discard LRQ
Internal errors (ie., memory allocation)	Discard LRQ
LRQ already being processed	Discard LRQ
LRQ destinationInfo aliases missing	LRJ sent, aliasesInconsistent
LRQ destinationInfo aliases unsupported	LRJ sent, neededFeatureNotSupported
LRQ replyAddress not ipAddress	LRJ sent, neededFeatureNotSupported
LRQ processing timeout	LRJ sent, resourceUnavailable
SIP LCR returns not-found	LRJ sent, notRegistered

Using Peer-GK for H.323 Outbound Call Routing

With the peer-GK support on the NN2600, the NN2600 is now capable of issuing H.225.0 RAS Location Requests to configured peer-GKs when making outbound H.323 calls, regardless of whether the inbound call-leg is SIP or H.323. The LRQ response furnished by the peer-GK is used to decide if the call should be admitted or rejected and determine to where the outbound SETUP message should be delivered.

Zone-Directory Gatekeeper Support

The NN2600 now handles receiving RAS admission and location responses from any configured external gatekeeper. The NN2600 can issue an admission or location RAS request to one gatekeeper and receive the corresponding RAS response from a different gatekeeper.

One example of this is to have a Zone Gatekeeper (ZGK) configured to receive admission and location requests from the NN2600. The ZGK then goes onto forward those requests to a Directory Gatekeeper (DGK).

If the external gatekeeper transmitting the RAS response is not configured on the NN2600 and there is no default gatekeeper configured, the RAS response is discarded. There can be no more than 65535 outstanding admission and location requests with zone-directory gatekeeper support.

Clustered Gatekeeper Support

The NN2600 allows you to configure multiple external gatekeepers with identical **server-pool** > **host** and **port** values. When configured this way, the NN2600 supplies each remote gatekeeper with unique RAS information in order to differentiate.

When a remote gatekeeper sends RAS traffic to the NN2600, the combination of the gatekeeper remote IP address and the local RAS port receiving the RAS traffic is used as a lookup key to identify the remote gatekeeper. Once identified, the NN2600 validates the traffic. If no default gatekeeper exists, any RAS traffic not matching a configured external gatekeeper is discarded.

However, when an external gatekeeper is configured with **server-pool > local-port** set to zero, the user must ensure each remote gatekeeper has a unique IP address.

Paravirtualization Support for Xen

The NN2600 now supports paravirtualization (PV) for Xen support. Because of this, the Xen installation has changed.

Installing software on the Xen server

This section explains how to install a NN2600 disk image on a generic 3.4.2 Xen server running on a Centos 5.4 system.

NOTE: These instructions should be considered a guide and may need to be modified appropriately for a particular environment.

1. Place the disk image on the Centos server with an applicable method such as SCP or FTP.
2. Uncompress the image:

   ```
   gunzip nnSE360m2-xen.img.gz
   ```

3. Ensure there are at least two virtual bridges for connecting to the NN2600. A standard Xen installation should create a bridge based on the primary interface. The example used here is eth0. In the following example, two additional virtual bridges are created and physical interfaces eth1 and eth2 are attached to them:

```
brctl addbr virbr0
brctl addif virbr0 eth1
brctl addbr virbr1
brctl addif virbr1 eth2
```

4. Create a Xen configuration file in /etc/xen. Further steps assume the name **NNOSE**. The following example sets the memory to 1GB with 4 CPUs. Change the mac addresses to be unique in your network, and ensure that the file in the **disk** line properly references your disk image.

```
name=”NNOSE”
memory=1024
vcpus=4
on_poweroff=”destroy”
on_reboot=”restart”
on_crash=”restart”
disk=[‘file:/vms/nnSE360m2.tar.gz,xvda,w’]
vif=[“mac=00:16:4e:00:00:00,bridge=eth0”,”mac=00:16:4e:00:00:01,
bridge=virbr0”,
“mac=00:16:4e:00:00:02,bridge=virbr1”]
kernel=”/usr/lib/xen/boot/pv-grub-x86_32.gz”
extra=”(hd0,1)/grub/menu.lst”
```

5. Launch the VM with the serial console to complete installation. The following is a small sample of the expected output from this step:

```
xm create -c NNOSE
[root@xen-centos vms]# xm create -c NNOSE
Using config file "/etc/xen/NNOSE".
Started domain NNOSE (id=1)

                             Xen Minimal OS!
  start_info: 0xa67000(VA)
    nr_pages: 0x40000
  shared_inf: 0xcfe50000(MA)
     pt_base: 0xa6a000(VA)
nr_pt_frames: 0x9
    mfn_list: 0x967000(VA)
   mod_start: 0x0(VA)
     mod_len: 0
       flags: 0x0
    cmd_line: (hd0,1)/grub/menu.lst
```

```
      stack:      0x946780-0x966780
    MM: Init
          _text: 0x0(VA)
         _etext: 0x61af5(VA)
       _erodata: 0x76000(VA)
         _edata: 0x7b6d4(VA)
    stack start: 0x946780(VA)
           _end: 0x966d34(VA)
      start_pfn: a76
        max_pfn: 3fffd
    Mapping memory range 0xc00000 - 0x3fffd000
    setting 0x0-0x76000 readonly
    skipped 0x1000
    MM: Initialise page allocator for c70000(c70000)-0(3fffd000)
    MM: done
    Demand map pfns at 3fffe000-bfffe000.
    Heap resides at bffff000-fffff000.
    Initialising timer interface
    Initialising console ... done.
    gnttab_table mapped at 0x3fffe000.
    Initialising scheduler
    Thread "Idle": pointer: 0xbffff008, stack: 0xc90000
    Initialising xenbus
    Thread "xenstore": pointer: 0xbffff478, stack: 0xca0000
    Dummy main: start_info=0x966880
    Thread "main": pointer: 0xbffff8e8, stack: 0xcb0000
    "main" "(hd0,1)/grub/menu.lst"
    vbd 51712 is hd0
    ******************* BLKFRONT for device/vbd/51712 **********


    backend at /local/domain/0/backend/vbd/1/51712
    Failed to read /local/domain/0/backend/vbd/1/51712/feature-barrier.
    Failed to read /local/domain/0/backend/vbd/1/51712/
feature-flush-cache.
    83886080 sectors of 0 bytes
    *************************
    Press `ESC' to enter the menu... 0
      Booting 'Covergence Session Manager on 1st partition'

    root (hd0,2)
     Filesystem type is reiserfs, partition type 0x83
    kernel /boot/vmlinuz-covergence root=/dev/xvda3 rootdelay=10
ramdisk_size=4096
    crashkernel=64M@16M clocksource=acpi_pm

    ...
```

```
Net-Net OS-E
Copyright (c) 2004-2010  Acme Packet Inc.

username:
Net-Net OS-E
Copyright (c) 2004-2010  Acme Packet Inc.

username:
```

Locally Generated Ringback During Unattended Call Transfers

The NN2600 provides support to specify an audio file to be played to the user while waiting for an unattended call transfer to be completed. Upon successful connection to the transferee, the audio file is terminated and the transferred party is re-invited with audio information from the transferee.

If the connection attempt fails after all possible configured routes have been attempted, the audio file is terminated and, if possible, audio is restored between the transferred and transferrer. If the transferrer is no longer available, the transferred party is disconnected.

The configuration parameter **transfer-file**, under the **third-party-call-control** object, has been created to allow the user to specify the audio file to be played during transfer. For more information about this parameter see Configuration changes in Release 3.6.0m2.

TCP Kernel Buffer Congestion Control Status Display

The **show tcp-skb-congestion-control** command displays the status of the TCP kernel buffer congestion control feature, including the admin state, current threshold, as well as some kernel buffer usage counters.

```
NNOS-E> show tcp-skb-congestion-control
  admin:  enabled
  threshold:  5000
  skbs-in-use:  2096
  max-skbs-in-use: 2506
  tcp-dropped-pkts: 378
```

Field	Description
admin	**Displays whether or not TCP kernel buffer congestion control is enabled.**
threshold	**Displays the configured threshold of the TCP kernel buffer congestion control.**
skbs-in-use	**Displays the current number of system-wide kernel buffers currently in use.**
max-skbs-in-use	**Displays the maximum number of kernel buffers that the NN2600 has had in use at any given time.**
tcp-dropped-pkts	**Displays the number of TCP packets that have been dropped because the kernel buffer usage has exceeded the configured threshold.**

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.0m2:

Component	Description	Problem ID	Found in Release
Routing	Some trace events, associated with weighted round robin load balancing in services-routing are at error level when they are not really error conditions.	pd11171	3.6m1
SIP	Pointer incoffectly deleted, causing faults.	pd11008	3.6m1
Dial Plans	Joined-matches does not work when one route is a hunt group.	pd11256	3.6m1
H.323	The NN2600 is transmitting a 404 Not Found when there is a default gatekeeper configured.	pd11217	3.6m1
LCR	Move memory allocation so that the allocated resource persists for the life of the call.	pd11288	3.6m1
Cluster	Errors in the SIP process after a vsp-reset is executed in a multibox cluster.	pd11029	3.6m1
SIP	Handle null pre-session configuration settings.	pd11083	3.6m1
SIP	Faults occurring during parallel forking.	pd10571, 10572, 10573	3.5.4

Component	Description	Problem ID	Found in Release
Database	Database problems after load test.	pd10774	3.5.8
Accounting	File-system accounting not working properly.	pd10952	3.6.0
H.323	LRJ takes 5 seconds to respond to GK.	pd11559, 11565	3.6m2
H.323	H.323 to SIP calls need a Local IP option when creating To: address.	pd11610	3.6m2
H.323	H.323 calls that are routed back to GK get an LCF.	pd11623	3.6m2
H.323	LRQ gets LCF even with LCR lookup failure.	pd11603	3.6m2
LCR	LCR diameter traffic being routed improperly.	pd11498	3.6m2
H.323	The capability preference table is being overrun.	pd10951	3.5.2
LCR	Route-server missing alteration settings after a replace-file.	pd11665	3.6m1
Media	Auto anchoring not releasing the media.	pd11056	3.5.5
Media	In cases where endpoints are behind a NAT for which the NN2600 will release media, crypto information is negotiated between both parties and the call comes up fine. However, after the call is put on hold, the crypto information is not included when the NN2600 sends an Invite.	pd9954	3.5.5
Media	Post-Dial Digits for file-play-broadcast are not being recognized by distant end systems.	pd11629	3.6m1
LCR	Cannot call-hunt in conjunction with LCR hookups.	pd11763	3.6m2
SIP	When the UAC performs parallel forking where the only difference in the invites is the Via branch, both calls share the same session.	pd11818	3.6m1
Diameter	Diameter connection does not detect a down server and failover to another member of the diameter group.	pd11936	3.6m2
Interworking	If media ports are unavailable during a SIP-H.323 call, the H.323 side of the call fails but does not clear out the SIP side of the call.	pd11934	3.6m2

Component	Description	Problem ID	Found in Release
DNS	When a DNS endpoint is returned via the route server, the NN2600 only routes the first result.	pd11975	3.6m2
H.323	LRQ and LCF handling uses the GK server profile for the outbound setup rather than the default or explicit server profile.	pd11695	3.6m2
Route Server	When resolving routes via DNS, the route server does not route to addresses not already configured on the NN2600.	pd11930	3.6m2
SSH	Intermittent SSH connectivity problems occurring.	pd11898	3.6m2
Dial Plans	Subscribe messages using dial plan routed incorrectly after a 401 Unauthorized message.	pd10833	3.6.0
Route Server	Route-set configuration does not have the ability to trim duplicates.	pd11935	3.6m2
Diameter	Diameter request not honoring the **diameter-group** > **request-timeout** configuration.	pd12076, 12148	3.6m2
Interworking	Information for policy matching not being sent over to SIP for H.323-SIP calls.	pd12157	3.6m2
Interworking	Session-config policy authorization not merged into H.323-SIP calls	pd12161	3.6m2
Loopback Calls	Loopback call support not functioning properly.	pd11199, 11200	3.6.0
LCR	LCR to DNS must be able to resolve to a sip-gateway.	pd11947	3.6m2
Interworking	H.323 to SIP calls are ignoring sip-directive policy.	pd12187	3.6m2
Status	After issuing **show sip-summary-rates-by-box** sampling services experiences faults.	pd12188	3.6m2
SIP	The NN2600 refuses a NOTIFY after the initial SUBSCRIBE and NOTIFY messages succeed.	pd12183	3.6m1p1
SIP	The 3PCC pre-call announcement is not being played.	pd11885	3.6m2

Component	Description	Problem ID	Found in Release
Kernel	The **tcp-skb-congestion-control** property incorrectly defaults to enabled with a 40,000 kernel buffer threshold if the **box > os** configuration object is not configured.	pd12099	3.6m1
SIP	After receiving a REFER message, the NN2600 disconnects the call.	pd11855	3.6m1
DNS	The NN2600 needs the ability to configure CNAME DNS records locally.	pd12238	3.6m2
Config	The master-service server-load is no longer present after an upgrade from 3.4 to 3.6.	pd12237	3.6m1p1
Base Services	Fix initializing timing issue with memory pools.	pd12329	3.6m2
LCR	Route-server databases become out of sync after upgrade.	pd11950	3.6m2
SIP	The virtual dial plan is selectable in the dial plan peer type compound, however the virtual dial plan pool is hidden.	pd12469	3.6.0m1
DNS	Need the ability to configure CNAME and wildcard CNAME DNS records locally.	pd12238	3.6.0m2

Configuration changes in Release 3.6.0m2

The section provides a summary of the additions, changes, and deletions to the NN2600 configuration when upgrading to Release 3.6.0m2. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New objects in Release 3.6.0m2

Object name	Associated properties	Description
cluster-server-load		Configures sampling for the SIP server load status.
	admin [enabled | disabled]	Specifies whether the status sampling configuration is active and in effect. **Example: set admin disabled** The default setting is **enabled**.
	interval	Defines how often the NN2600 polls the status provider for data. The minimum polling time is 30 seconds. **Example: set interval 1:45:00** The default setting is **1:00:00**.
active-calls		Configures the sampling for currently active calls.
	admin [enabled | disabled]	Specifies whether the status sampling configuration is active and in effect. **Example: set admin disabled** The default setting is **enabled**.
	interval	Defines how often the NN2600 polls the status provider for data. The minimum polling time is 30 seconds. **Example: set interval 1:30:00** The default setting is **1:00:00**.
cname		A CNAME record maps a configured alias to a known name. This value can be exact or wildcarded. **Example: config cname abc.com**

Object name	Associated properties	Description
	match	Select whether the NN2600 matches the CNAME exactly or if it is a wildcarded match. The following are valid options: • exact — The NN2600 only matches if the FQDN is exact (in this example abc.com). • wildcard — The NN2600 matches if the FQDN is a wildcard (in this example www.abc.com, but not if it's exactly abc.com). **Example: set match wildcard** The default setting is **exact**.
	alias	Enter the alias you want associated with the CNAME records. **Example: set alias internal.abc.com**

New properties in Release 3.6.0m2

Object name	Associated properties	Description
settings	named-lookup-match	When the NN2600 receives a response from the route server, it looks for a specific match configured on the sip-gateways. Both the carrier and endpoint tags must match for the NN2600 to route the server. This parameter allows you to configure a secondary lookup. The following are valid values: • specific—The NN2600 does not make a second effort. The carrier and endpoint tags must both match. • grouped—If the endpoint does not match, match all endpoints under the carrier. • dns—If the endpoint does not match, use DNS to resolve the endpoint as an FQDN. **Example: set named-lookup-match dns** The default setting is **grouped**.
h323-to-sip-fromheader-spec	use-anon [true | false]	When enabled, as the H.323 process builds the SIP From: header for a received H.323 SETUP message it will do the following: • use anonymous as the user portion of the URI if after applying h323-to-sip-fromheader-spec config the user portion is empty • use the IP address of the H.323 gateway which transmitted the SETUP as the host portion of the URI if, after applying h323-to-sip-fromheader-spec config, the host portion is empty This guarantees a valid From: header URI will exist when sent to the SIP process. When set to false there is some chance an incomplete URI could be passed to SIP. **Example: set use-anon true** The default setting is **false**.

Object name	Associated properties	Description
route-server	client-request-sender	Describes who sends requests to the route-server. The following are valid values: • only-master—The request goes from the route-server master in the client cluster. • local-host-box—The host must be listed as a host-box for route-server master-service. **Example: set client-request-sender local-host-box** The default setting is **only-master**.
session-config>sip-settings\ session-config-pool>sip-settings	last-resort-request-uri [enabled | disabled]	If both the dial plan and location cache look ups fail, when this parameter is enabled, the NN2600 attempts to route the call using the Request-URI of the incoming INVITE. If you want to limit routing to dial plans and the location cache, set this parameter to disabled. **Example: set last-resort-request-uri disabled** The default setting is **enabled**.
authentication	initial-challenge-stale	Specifies whether the stale parameter is included in authentication challenges, per RFCs 2069 and 3261. The following are valid values: • true—Includes stale=”true” in the challenge. • false—Includes stale=”false” in the challenge. • none—The stale parameter is not included in the challenge. **Example: set initial-challenge-stale none** The default setting is **true**.

Object name	Associated properties	Description
altered-header\header-normalization\altered-body\reg-ex-header\reg-ex-collector	apply-to-dialog	Allows you to configure where to apply these options for a session. The following are valid values: • inbound—Apply to inbound dialog only. • outbound—Apply to outbound dialog only. • both—Apply to both inbound and outbound dialogs. **Example: set apply-to-dialog inbound** The default setting is **both**.
inbound-header-settings\header-settings	apply-to-allow-block-to-dialog	Specifies whether the allow and block properties of this object apply to a specific dialog or not. The following are valid values: • inbound—Apply to the inbound dialog only. • outbound—Apply to the outbound dialog only. • both—Apply to both inbound and outbound dialogs. **Example: set apply-to-allow-block-to-dialog inbound** The default setting is **both**.
third-party-call-control	allow-lcr-for-refer [enabled | disabled]	When running the route server under third-party-call-control, information may need to be obtained off of the NN2600, causing a delay. When this parameter is enabled, the NN2600 can avoid potential problems caused by this delay. **Example: set allow-lcr-for-refer enabled** The default setting is **disabled**.
third-party-call-control	transfer-file	Select the file of the media to be played while a blind transfer is taking place. **Example: set transfer-file data1** There is no default setting.

Object name	Associated properties	Description
settings	track-sip-messages [enabled | disabled]	Specifies whether the NN2600 tracks the response to SIP REGISTER and INVITE messages. When enabled, the show sip-register-responses and show sip-invite-responses status providers include data indicating the type and number of responses sent and received (e.g., the number of 200 OKs, 503s, etc.) **Example: set track-sip-messages enabled** The default setting is **disabled**.
settings	database-connection-memory -limit	Specifies the maximum memory, in kilobytes, allowed per database connection. The connection ends if this memory limit is exceeded. Minimum: 100000 Maximum: 3000000 **Example: set database-connection-memory-limit 200000** The default setting is **automatic**.
settings	unclean-shutdown-recover	Specifies how the local database is handled during startup after an unclean shutdown. An unclean shutdown may cause corruption in the database and is usually caused by a crash. The following are valid values: • always-archive—Always archive data if unclean shutdown is detected. You must also enter the number of times for the NN2600 to archive (from 1 to 20). • attempt-repair—Attempt corruption detection and repair and archive only if repair fails. **Example: set unclean-shutdown-recover attempt-repair** The default setting is **always-archive 3**.

Object name	Associated properties	Description
settings	allow-route-set-duplicates [enabled | disabled]	*This is a secondary property.* By default, the NN2600 allows duplicate destination routes. When this property is disabled, duplicate entries are removed and the NN2600 has only one entry in the route-set. **Example: set allow-route-set-duplicates disabled** The default setting is **enabled**.
os	tcp-skb-congestion-control [enabled | disabled] <threshold>	Sets a threshold of system-wide kernel buffer usage before the NN2600 will proactively prevent the depletion of the remaining system resources by dropping all received TCP packets. When enabled, TCP packets will be dropped until the kernel buffer usage falls below the configured threshold. **Example: set tcp-skb-congestion-control enabled 300000** The default settings are **disabled** and **automatic**.
route-server	simple-updates	This parameter allows users to run controlled updates only without the possibility of running a simple update accidentally. When disabled and a simple update is executed, the user receives the error, “Only controlled updates are permitted by config.” **Example: set simple-updates disabled** The default setting is **enabled**.

Deleted properties in Release 3.6.0m2

Object name
vinterface > preempt-delay

Default and other changes in Release 3.6.0m2

Property name	Change
h323 > gkport	**Default for port-type is now peer.**
virtual-threads > urgent-congestion-threshold	**Default changed from 128 to 32.**
virtual-threads > priority-congestion-threshold	**Default changed from 256 to 64.**
virtual-threads > regular-congestion-threshold	**Default changed from 32 to 128.**

MIB changes in Release 3.6.0m2

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB tables in Release 3.6.0m2

MIB table name	Description
clusterServerLoadTable	Previously marked obsolete.
clusterServerLoadDetailTable	Previously marked obsolete.
gatewayLoadMirrorTable	Previously marked obsolete.
trunkLoadMirrorTable	Previously marked obsolete.
callsTable	Displays a list of active calls for the specified time period.
sessionsTable	Active sessions, indexed by session ID.
sipRequestsTable	Statistics for SIP request messages.
sipRequestsByTagTable	Statistics for SIP request messages associated with tags.
routeServerBackupsTable	Statistics for LCR backup.

New MIB objects in Release 3.6.0m2

MIB object/table name
routeServerActionStatusAction
tcpSkbCongestionControlAdmin
tcpSkbCongestionControlThreshold

MIB object/table name (continued)
tcpSkbCongestionControlSkbsInUse
tcpSkbCongestionControlMaxSkbsInUse
tcpSkbCongestionControlTcpDroppedPkts

New SNMP trap entries in MIB for Release 3.6.0m2

Trap name	Description
h323CallRejected	An H.323 call leg has been terminated.
skbUsageTrap	An increase in the kernel buffer usage indicates a possible depletion of NN2600 resources.
tcpSkbCongestionDroppedPktsTrap	TCP packets dropped due to kernel buffer congestion indicates a possible depletion of NN2600 resources.

Obsolete MIB objects/tables in Release 3.6.0m2

MIB object/table name
There are no obsolete MIB objects or tables in Release 3.6.0m2.

Changed Tables in Release 3.6.0m2

MIB table name	Description
activeSessionTable	ADDED: activeSessionInitialMethod
arenaAllocatorTable	arenaAllocatorTotalMemory changed from an Integer to Counter64
h323ExternalGatekeepersTable	ADDED: h323ExternalGatekeepersConfigType, h323ExternalGatekeepersGatekeeperType, h323ExternalGatekeepersRaslisten, h323ExternalGatekeepersCallsiglisten
activeH323CallsTable	ADDED: activeH323CallsH225Port, activeH323CallsH245Port
sipAuthorizationDetailsTable	ADDED: sipAuthorizationDetailsOtherErrorCount

Known problems, restrictions, and operational considerations in 3.6.0m2

Changing a Configured H.323 IP Address

When an IP address has H.323 configured and enabled, if the user changes the ip-address property, then the user must disable and then reenable H.323 in order for the NN2600 to recognize the IP address change.

Configuring Gatekeeper Ports on a Single Interface

When configuring an H.323 server, you cannot configure a **gatekeeper-port** of type **client** and a second port of type **peer** using the same port number. The NN2600 does not currently enforce this rule. This applies to a single interface only.

Performing Controlled Updates and Activations on Route Servers

Previously, when upgrading, activating, or deleting a backup route server file on the NN2600s within a cluster, there was nothing to ensure route server databases on each NN2600 were properly synced.

An action has been created that allows you to manually verify that route servers on each NN2600 in a cluster are synced up properly during a route-set update, activating a new route-set, deleting a backup, or cancelling a controlled update or activation.

When this action, **route-server-controlled**, is executed, the master NN2600 controls and checks the success of each operation on each of the NN2600 slaves. The following are the operations you can execute with this action.

- **route-server-controlled update <file> [activate-time] [peer-wait-seconds]**—Allows you to replace the route-set used by the cluster while ensuring the route server databases on each NN2600 are properly synced. You can optionally configure the specific time for this action to be executed, as well as how many seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.

- **route-server-controlled activation [activate-time] [peer-wait-seconds]**—Activate a new route-set used by the cluster while ensuring the route server databases on each NN2600 are properly synced. You can optionally configure the specific time for this action to be executed, as well as how many seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.
- **route-server-controlled delete-backup <backup-name>**—Delete a backup route-set that the cluster does not use anymore while ensuring the route server databases on each NN2600 are properly synced.
- **route-server-controlled cancel [peer-wait-seconds]**—Cancel a controlled update or activation that is currently in progress. You can optionally configure the number of seconds the master will wait for a peer to finish each step in the action. The master allows each peer three attempts at a step. The first attempt, the master waits the configured number of seconds. The second try, the master waits twice the configured number of seconds, and the third time three times the number of seconds before the master will halt the entire action.

When this action, **route-server-controlled**, is executed, the master NN2600 controls the update, activation, or deletion, and checks the success of each operation on each of the NN2600 slaves. Any error that occurs during the upgrade and activation processes, either on the master or any slave, results in the master initiating a rollback. The entire operation is retried and all failures that occur are logged and traced.

Before executing the **route-server-controlled** action, both NTP and logging must be configured on all NN2600s. This action must always be executed by the master. Any attempt to execute this action on a slave results in the error, “Execute action on master.”

To execute a controlled update, activation, or deletion:

1. Generate and save (in XML format) a route-set file using the LCR import tool and DID mapping. For more information on using the LCR import tool, see the *Net-Net 2600 Session Services Guide.*
2. Using a method such as FTP, upload the route-set file to the master route-server box.
3. Unzip the .xml.gz file on the NN2600.

4. Run the **route-server-controlled** command.

Both the master and slave NN2600s cycle through a set of states during a controlled update. The following table shows the states a master NN2600 goes through.

State	Description
Ready	The master is ready to receive a new action request.
Loading	The master is loading.
Peers_Fetching	Waiting for all slaves to get the file from the master.
Peers_Loading	Waiting for all slaves to load.
Peers_Activating	Waiting for all slaves to activate before the master activates itself.
Peers_Cancelling	Cancel the current operation.
Initializing	The master NN2600 is initializing its state.
Activate_Scheduled	A controlled activation is scheduled.

The following table shows the states a slave NN2600 goes through.

State	Description
Ready	The slave is ready to receive a new action request.
Fetching file	Received route-set .xml file from master.
Loading	Slave is loading.
Activating	Slave is activating.
Cancelling	Master requested a cancel.

To view the progress of a currently executing update, activation, or deletion, use the **show route-server-controlled-action-status** action.

```
Cluster1> show route-server-controlled-action-status

box        master state                    routes     load-set
---        ------ -----                    ------     --------
2          true   Peer_Fetch_InProgress    80993      rsdid_201004131550.xml
3          false  Fetch_Success            0          rsdid_201004131550.xml
4          false  Active                     3
5          false  Fetch_Success            0          rsdid_201004131550.xml
6          false  Fetch_Success            0          rsdid_201004131550.xml
```

Field	Description
box	The NN2600 ID.
master	Whether the NN2600 is the master.
state	The state of the NN2600. This field captures the information in both the box-state and result.
routes	The number of routes currently loaded.
load-set	The cluster is updating to this route-set.

To view the state of the route-server in the cluster use the **show route-server-box** action:

```
Cluster1> show route-server-box

box        master activated-at             routes     active-set
---        ------ ------------             ------     ----------
2          true   19:13:22 Wed 2010-05-26  3          five.xml
3          false  19:13:31 Wed 2010-05-26  3          five.xml
4          false  19:13:22 Wed 2010-05-26  3          five.xml
5          false  19:13:22 Wed 2010-05-26  3          five.xml
6          false  19:13:21 Wed 2010-05-26  3          five.xml
```

Field	Description
box	The NN2600 ID.
master	Whether the NN2600 is the master
activated-at	The currently active route-set was activated at this time.
routes	The number of routes in the currently active route-set.
active-set	The route-set file that is currently active.

Syncing a New NN2600 With an Existing Cluster

When adding a new NN2600 to an existing cluster, you may find that the new NN2600 does not update to the active route-set. To ensure all NN2600s in a cluster are in sync perform the following steps.

1. Check the following status providers.

   ```
   show route-server-box
   show route-server-controlled-update
   ```

2. If you find the NN2600s are not all in sync, execute the **route-server-controlled-cancel** command. This works as a reset and syncs the NN2600s in a cluster.

3. Or you can also execute the **route-server-controlled update** command with the route-set you want to activate. Even if that route-set is already active on some NN2600s, it will ensure all of the NN2600s in the cluster are running the same route-set.

Using IWF In a Redundant Cluster

When running IWF traffic in a redundant cluster, the backup NN2600 logs irrelevant BYE messages to the call-logs following the termination of a call. These erroneous BYE messages appear only in the call-logs and do not affect functionality.

Release 3.6.0m1

New Features

The following sections describe the new features that have been added to Release 3.6.0m1.

Server Pool Call Admission Control

The NN2600 now supports server pool call admission control (CAC). A **server-pool-call-admission-control** object can be configured on any enterprise server that contains a server pool. A CAC object can be configured for each member of a server pool.

This server-level CAC can be enforced as either admission or emission control and you can configure the following statistics:

- Calls in setup
- Concurrent calls
- Used bandwidth

- Call rate

The server pool CAC configuration settings and call stats can be seen via the new status provider **show sip-gateway-cac**. The server pool call statistics are an aggregate of all server pool members below it. If the server pool CAC limits are exceeded, then all pool members are removed from active routes.

```
NNOS-E> show sip-gateway-cac

gateway current-local current-cluster current-max   bw-local    bw-cluster bw-max
-------    ------------- --------------- -----------   --------    ----------
SIPpServer 0             0               0             0           0          0
SIPpClient 0             0               0             0           0          0
```

Field	Description
gateway	**The gateway whose statistics you are viewing.**
current-local	**Number of calls connected locally to this gateway, but not mirrored around the cluster.**
current-cluster	**Number of calls connected to this gateway, mirrored around the cluster.**
current-max	**Maximum number of concurrent calls configured on the NN2600.**
bw-local	**Amount of bandwidth in use locally by calls that are not mirrored around the cluster.**
bw-cluster	**Amount of bandwidth in use by calls mirrored around the cluster.**
bw-max	**Maximum bandwidth configured on the NN2600.**

Forked Media Flow Direction Control with NICE systems

In NN2600 releases previous to 3.6.0, via the “Forwarding-Based Recording Using SIP” protocol, the NICE equipment identified sessions and which RTP traffic should be replicated, providing the destination for replication for each stream direction (Rx and Tx). The Session Director always used the originator of the call as a reference for deciding which stream is the Rx and which is the Tx.

A configuration property has been created which allows you to indicate which leg is the call center PBX, and thereby control how the Rx and Tx streams of a call are determined so that they match the NICE equipment’s Rx and Tx streams. The property under the **third-party-call-control** object is the **media-forward-direction-reference** and allows you to specify **in-leg** or **out-leg**.

Configuration Backup Enhancement

In releases prior to 3.6.0, the NN2600 retained 4 backup configurations in the backup directory. It now retains up to 100.

File-Play-Broadcast Post-Dial Digits

The file-play and file-play-broadcast actions provide unattended outbound dialing services. This feature enhances the file-play and file-play-broadcast actions to allow for post-dialing digits to be sent as DTMF after the initial call is established. Each called party specified in these actions have the option of including a post-dial digit sequence as part of the user information section of the SIP To URL.

The post-dial digit sequence is an optional string that can be included in the user portion of the SIP To URL. When present, the post-dial digit sequence is played after the initial call is established. The post-dial digit string is case insensitive and is represented by the following string:

;postd=xxxx

where xxxx can be one of the following:

- phone digit— 0-9
- DTMF digit— * | # | A | B | C | D
- Pause character— ‘p’ to pause one second
- Visual separator characters (These are used for visual purposes only and are ignored during the playing of the sequence):
  - Period ‘.’
  - Hyphen ‘-’
  - Open parenthesis ‘(‘
  - Closed parenthesis ‘)’

file-play

Purpose

Places a call to the specified SIP URL, plays the .WAV file, and then disconnects the call. This could be a .WAV file you recorded and moved to NN2600, for instance with the **file fetch** action.

Compare this to the **playback** action. The **playback** action plays recorded sessions only (NN2600 takes care of mixing the media for playing). This action plays any audio file. For example, if you made a file using the **mix-session** action, you can play it using **file-play**.

Enter the following information:

- filename—The location of the .WAV file you want played.
- to—The SIP URL that specifies where to place the call. Enter the optional post-dial value here (**;postd=xxxx**).
- from—A SIP URL that appears as the caller ID.
- transport—The transport protocol to use, either **any**, **UDP**, **TCP**, or **TLS**.
- requestID—The optional string that represents this call's request Identifier. This is returned in all events from this action.
- actionIdentifier—The optional action ID string that is returned in the accounting record associated with this call.

file-play-broadcast

Purpose

Places a call to multiple specified SIP URIs, plays the .WAV file, and then disconnects the call. This could be a .WAV file you recorded and moved to NN2600, for instance with the **file fetch** action.

Compare this to the **playback** action. The **playback** action plays recorded sessions only (NN2600 takes care of mixing the media for playing). This action plays any audio file. For example, if you made a file using the **mix-session** action, you can play it using **file-play-broadcast**.

Enter the following information:

- filename—The location of the .WAV file you want played.
- from—A SIP URI that appears as the caller ID.

- to—The SIP URIs that specify where to place the calls. Enter the optional post-dial value here (**;postd=xxxx**).
- config—(Optional) The **session-config** to use when calling the To SIP URL. For example: "**vsp\session-config-pool\entry <name>"**.

2175 - RADIUS Authorization and Routing

The NN2600 now supports RADIUS authorization and routing. When configured, the NN2600 sends a request to the RADIUS server, including the to-URL and from-URL. The RADIUS server responds with information the NN2600 uses to create session-configs applied to the session.

To configure RADIUS authorization and routing:

1. Enter the **route-server** configuration object.

```
NNOS-E> config master-services route-server
config route-server>
```

2. Enable the **route-server** object and configure the **host-box** and **group**.

```
config route-server> set admin enabled
config route-server> set host-box cluster\box 5
config route-server> set group 0
```

3. Enter the **radius-group** configuration object.

```
NNOS-E> config vsp radius-group rgroup1
config radius-group>
```

4. Enable the **radius-group** object and set the **application** parameter to **routing**.

```
config radius-group> set admin enabled
config radius-group> set application routing
```

5. Enter the **authorization** configuration object.

```
NNOS-E> config vsp default-session-config authorization
config authorization>
```

6. Set the **mode** parameter to **radius <group-name>**.

```
config authorization> set mode radius rgroup1
config authorization>
```

7. Configure the RADIUS server per the server's documentation to accept the request from the NN2600.
8. Save and activate your configuration.

show radius-routing

Purpose

Displays configuration information, status, count, and speed statistics for each RADIUS server configured for routing.

Sample output

```
NNOS-E> show radius-routing

Status for RADIUS group 'Boston' (fail-over):
-------------------------------------------------------------------------------
Server Name      State    Pr | Out  Pending  Requests  Accepts  Rejects Errors
-------------------------------------------------------------------------------
boston           Idle      1 |   0        0         0        0        0       0
127.0.0.1        Idle      1 |   0        0         0        0        0       0
-------------------------------------------------------------------------------
    -
Totals:                      |   0        0         0        0        0       0
```

Properties

Field	Description
Status for RADIUS group...	The name of the group reported on as well as the RADIUS group authentication operational algorithm.
Server Name	The name of IP address that identifies the server that is part of this RADIUS group.

Field	Description
State	The state of the RADIUS server. The following are valid options: • **Idle**—The server is enabled, but has not received traffic. • **Disabled**—The server is disabled in the configuration. • **Healthy**—The server is responding normally to system requests. • **Failing**—The server has not responded to some system requests, but not enough to trigger a fail-over (if configured). • **Failed**—The server has failed to respond to too many requests and the NN2600 has determined that it is down. If the RADIUS group is configured with fail-over mode, and a backup server is configured, the NN2600 stops sending requests to this server and begins forwarding requests to the next. • **Secret**—There is an error with the shared secret configured for this server.
Pr	The priority of the RADIUS group ranging from 1 (highest priority) to 99 (lowest property).
Out	The number of outstanding requests that the NN2600 has sent to the RADIUS server without a response.
Pending	The number of requests that have been generated but have not yet been sent to the server. The server's **window** setting defines the number of allowed requests. Requests generated once that threshold has been reached are considered pending.
Requests	The total number of authentication requests generated.
Accepts	The number of times the RADIUS server has accepted a request, indicating that the user has the correct password.
Rejects	The number of times the RADIUS server has rejected a request, indicating that either the user has an incorrect password or the shared secret isn't right.
Errors	The number of request errors.

radius-authorize

Purpose

Enables, disables, or tests a previously configured server that is part of a RADIUS group configured for authorization. Enter a reference to the configured server (configured with the RADIUS group server object.) Enclose the reference path in quotation marks. The server name is case-sensitive.

When using the test action, you can validate user credentials on the server via the NN2600. When invoked, the NN2600 sends a test message to the server to ensure the RADIUS server is configured properly. This action verifies the server and to-url, and optionally the from-url and display-mode. Enter the following:

- **server**—a reference to the configured server and group. Enter this in quotations marks in the format "groupNamePath\server ipAddress."
- **to-url**—the to-url IP address.
- **from-url**—optional; the from-url IP address
- **display-mode**—optional; select either **standard** or **verbose**.

Syntax

```
radius-authorize deactivate <server>
radius-authorize reactivate <server>
radius-authorize test <server> <to-url> [from-url] [display-mode]
```

Example

```
NNOS-E> radius-authorize deactivate "vsp\radius-group boston\server
boston"
NNOS-E> radius-authorize reactivate "vsp\radius-group boston\server
boston"
NNOS-E> radius-authorize test "vsp\radius-group boston\server
boston" sip: 2125551212@voiop.acmepacket.com standard
```

Management System Access

The NN2600 has three new permissions regarding what a user can view and edit. The View menu under the Configuration tab lists the permitted views. The following are the permitted views:

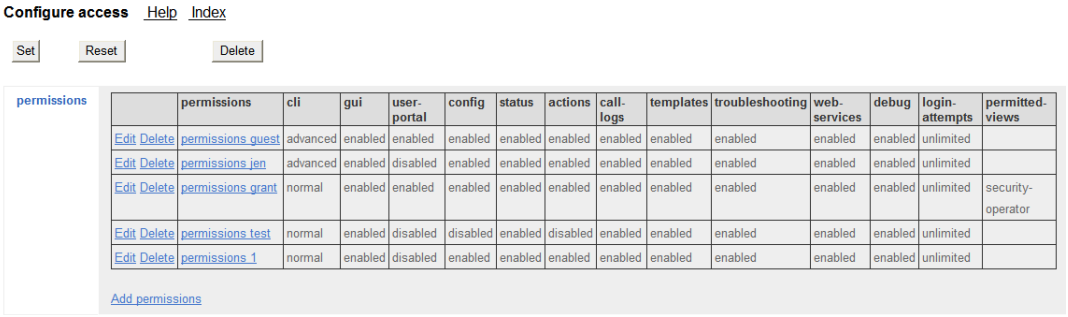
- Security-admin—Users with this permitted view are able to add, modify, and delete the following configuration objects that are security related:

- **interface/op** (all objects)
- **vsp/policies/dos-policy**
- **vsp/tls**
- **filter-intf** can be changed

- Security-operator—Users with this permitted view are able to add, modify, and delete objects under Access/Users. Users are blocked from viewing anything under the Configuration tab.
- Sip-admin—Users with this permitted view are able to add, modify, and delete configuration objects that are not security related. Users with this view are blocked from viewing the Access configuration.

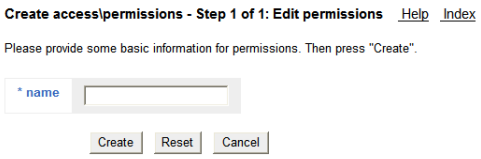
To assign a permission set:

1. Create a new access permission under the Access tab by clicking **Add permissions**.



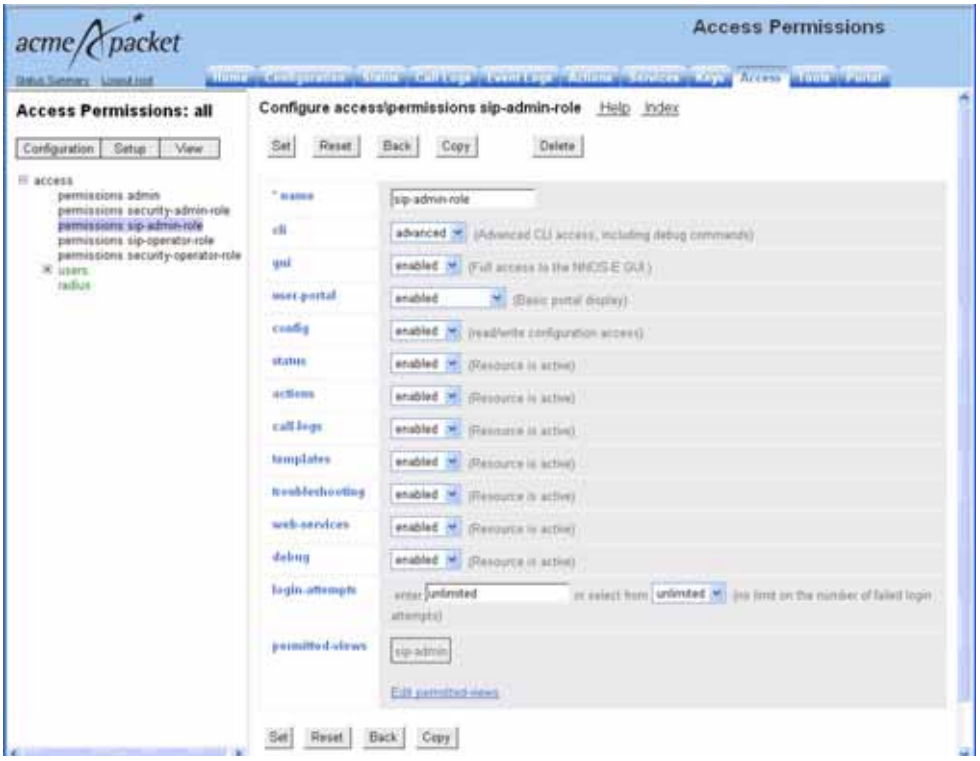
	permissions	cli	gui	user-portal	config	status	actions	call-logs	templates	troubleshooting	web-services	debug	login-attempts	permitted-views
Edit Delete	permissions guest	advanced	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions jen	advanced	enabled	disabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions grant	normal	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	security-operator
Edit Delete	permissions test	normal	enabled	disabled	disabled	enabled	disabled	enabled	enabled	enabled	enabled	enabled	unlimited	
Edit Delete	permissions 1	normal	enabled	disabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	unlimited	

2. Enter the name you want to use for this access permission and select **Create**.

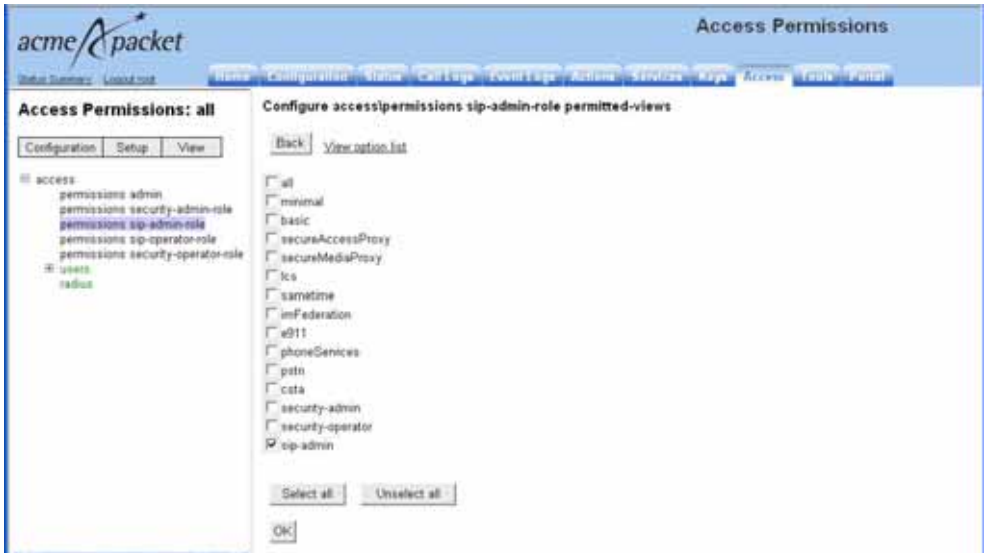


The page listing all permissions appears.

3. The following image shows access permission **sip-admin-role** created with permitted view **sip-admin** assigned.



The following image shows available permitted views.



4. Create a new user and assign the access permissions to the user. The following image shows user **WSmith** created with access permission **sip-admin-role** assigned.

5. Save and activate your configuration.

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.0m1:

Component	Description	Problem ID	Found in Release
Transcoding	Codec renegotiation, using **terminate-reinvite-locally** sending wrong codec.	pd7956	3.5.5
DTMF Translation	**dtmf-notify** header incorrect.	pd8310	3.5.4
Pushlet	Incorporate p_xxx properties from original pushlet into eventpush service.	pd8266	3.6.0
NICE	Only one direction of call replicated to NICE.	pd8297	3.5.2
OS	Adjusting hardware clock could change the time significantly.	pd8091	3.5.5
SIP	SIP Crash on NN2600 after upgrade to 3.6.0.	pd8418	3.6.0
Kernel	Modify kernel TCP buffer handling under congestion	pd8181	3.5.5
Route Server	“Up to outbound peer,” logic is removed from RS routing.	pd8568	3.6.0
Registration	Calling-Group REGISTERs fail.	pd8452	3.5.5
SIP	No ringback when A calls B (g711) and B refers to C (g729) and C answers with a different codec.	pd10000	3.6.0
3PCC	Fault attempting **call-control** park.	pd8573	3.5.x
Media	200 OK to delayed offer INVITE does not offer all codecs.	pd8502	3.6.0
H.323	RIP to sender of LRQ should use replyAddress.	pd10038	3.6.0m1
SIP	Server unregistered-sender-directive does not work.	pd4717	3.3.8
SIP	Action **call-control** call is timing out.	pd10110	3.6.0m1
Location Services	Best-match location-match-preferred using session from peer sip-gw when routing to registered endpoints.	pd8476	3.5.3
DNS	DNS fails processing for tel URLs.	pd10219	3.6.0m1
SIP	No way to remove SDP from OS-E SIP messages.	pd10097	3.5.5

Component	Description	Problem ID	Found in Release
H.323	The NN2600 SIP functionality does not differentiate between g729 and g729A	pd10241	3.6.0m1
SIP	DTMF Notify Content-Length 0; bw-local and bw-cluster counter leaking with server pool CAC.	pd10240/10259	3.6.0m1
H.323	SIP fault while running an H.323/SIP test with logs of DTMF <--> SIP INFO translations	pd10273	3.5.2
Kernel	Kernel fault causing failover.	pd10202	3.5.2
H.323	H.323-H.323 calls using internal tunnel-msg to forward Progress pass incorrect ports to H.323	pd10217	3.6.0m1
GUI	Can't load XML file into web interface configuration	pd10297	3.6.0m1
Accounting	Post-Digit Dialed Numbers provided in file-play-broadcast are missing from CDR.	pd10306	3.6.0m1
SIP	Post-Dial Digit Functionality not working with TEL URL	pd10242	3.6.0m1
SIP	SIP fault when loopback test is run.	pd10469	3.6.0
SIP	Segmentation Fault with Reg-Ex Rule for REFER.	pd10390	3.5.7
ENUM	Third party call control must be enabled for TEL/SIPS translation to work on ENUM.	pd10392	3.6.0
H.323	CUCM SIP to Avaya ACM H.323 one-way voice race condition.	pd10398	3.6.0m1
Dial Plans	Route dial plan matching on From-URI of directory CSV.	pd8349	3.5.3
LCR	Fix for poisoned-buffer access on LCR lookup timeout.	pd10490	3.6.0m1
SIP	600 error when 487 Request Terminated is ACKed.	pd8340	3.6.0
H.323	When H.323 side shuffle is complete, the SDP is copied to the SIP side outbound message.	pd8367	3.6.0
Kernel	Lock references to the kernel rule refcnt causing faults.	pd10596	3.6.0m1

Component	Description	Problem ID	Found in Release
Kernel	Kernel page counts error in the media-drop shared memory.	pd10632	3.6.0m1
SIP	SIP process faults during upgrade.	p-d10474	3.6.0m1
SIP	Unable to modify Request Header before routing.	pd10622	3.6.0m1
Util	Faults after load test during NSN testing.	pd10595	3.5.8
Kernel	Ensure all rule-handles are converted to rules using Krnl_RuleLock().	pd10634	3.6.0m1
Media	Fault during load test.	pd10635	3.6.0m1
H.323	Crash during H.323-H.323 calls	pd10731	3.6.0m1
Cfg Transform	The active-call incorrectly handled during upgrade.	pd10732	3.5.7
DNS	DNS faults during synchronous requests.	pd10039	3.6.0
SIP	Parallel forking faults.	pd10571 pd10572 pd10573	3.5.4
3PCC	The NN2600 isn't sending 100 Trying for re-INVITEs when 3PCC is enabled.	pd10845	3.6.0m1
SIP	The NN2600 sends ACK for 200 OK responses from port 5060 after sending all subsequent messages from source port 5060.	pd10879	3.6.0
SIP	Multiple entries on outgoing Call-Info header	pd10912	3.6.0m1
Accounting	File-system accounting errors.	pd10952	3.6.0

Configuration changes in Release 3.6.0m1

The section provides a summary of the additions, changes, and deletions to the NN2600 configuration when upgrading to Release 3.6.0m1. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New objects in Release 3.6.0m1

Object name	Associated properties	Description
vsp/enterprise/servers/ sip-gateway | h323-server | avaya | lcs | mcs | sametime / server-pool/ server-pool-admission-control		Allows you to configure a server-pool CAC on any enterprise server that contains a pool.
	max-bandwidth	Enter the maximum amount of bandwidth, in kbits per second, the NN2600 allocates to the AOR. When the system reaches the maximum bandwidth limit for a server, it rejects calls until bandwidth use drops below the maximum. **Example**: set max-bandwidth 10000 Min: 0 / Max: unlimited The default setting is **unlimited**.
	max-number-of-concurrent-calls	Specify the maximum number of active calls allowed for this AOR at one time. When this value is reached, the connection does not accept calls until the value drops below the threshold. **Example**: **set max-number-of-concurrent-calls 5000** Min: 0 / Max: 1000000 The default setting is **1000**.
	max-calls-in-setup	Sets the maximum number of simultaneous call legs in setup stage that are allowed for this AOR. A call leg in setup is much more compute-intensive than established call legs, so this value is more restrictive than the concurrent call leg value. A value of 0 causes the system to decline all calls and registrations. **Example**: **set max-calls-in-setup 5000** Min: 0 / Max: 10000 The default setting is **30**.

Object name	Associated properties	Description
	call-rate-limiting	Limits the number of calls sent to an AOR within a certain interval in seconds. Once this interval is reached, the system rejects any calls to or from this AOR until the rate decreases, returning a response code and message. This feature sets the acceptable arrival rate for incoming calls when used with admission-control and the acceptable set-up rate when used with emission-control. When this feature is enabled, set the number of calls and the measurement interval. You can also enter a result code from 400 to 699 and a text string to accompany call rejection if no available server is found. **Example**: **set call-rate-limiting enabled** The default setting is **disabled**
	admission-control {enabled | disabled}	Specifies whether the system considers AOR limitations when forwarding a call from the AOR. The system tracks the number of concurrent (both incoming and outgoing) active calls for this AOR. **Example**: **set admission-control enabled** The default setting is **disabled**.
	emission-control	Specifies whether the system considers AOR limitations when forwarding a call to this AOR. The system tracks the number of concurrent (both incoming and outgoing) active calls for this AOR. **Example**: **set emission-control enabled** The default setting is **disabled**.
	call-admission-control-error-code	Enter the call admission error code. **Example**: **set call-admission-control-error-code 700** Min: 400 / Max: 999 The default setting is **503**.

Object name	Associated properties	Description
	call-admission-control-error-string	Enter the text string the users sees when a call admission control error occurs. **Example**: **set call-admission-control-string cac error**
	call-emission-control-error-code	Enter the call emission error code. **Example**: **set call-emission-control-error-code 800** Min: 400 / Max: 999 The default setting is **503**.
	call-emission-control-error-string	Enter the text string the user sees when a call emission control error occurs. **Example**: **set call-emission-control-error-string cec error**

Object name	Associated properties	Description
default-session-config > dialog-control-settings		Allows you to configure the NN2600 to reject a message sent within a dialog that contains specified release code and text.
	refused-methods	Select the type of message you want the NN2600 to reject. The following are valid values: • INVITE • ACK • BYE • REGISTER • REFER • NOTIFY • OTHER • PRACK • CANCEL • SUBSCRIBE • OPTIONS • MESSAGE • INFO • PUBLISH • UPDATE • SERVICE • PING • NONE Specify the release code you want the NN2600 to reject. The minimum value is 400 and the maximum value is 499. The default value is 405. Specify the text you want the NN2600 to reject. The default setting is Method Not Allowed. **Example**: **set refused-methods invite 450 Method Rejected**

New properties in Release 3.6.0m1

Object name	Associated properties	Description
permissions	permitted-view	Assign a permitted view you want a user to have. If no permitted-view is specified, the default permitted view is set to **all**. The following are valid permitted views: • all • minimal • basic • secureAccessProxy • secureMediaProxy • lcs • sametime • imFederation • e911 • phoneServices • pstn • csta • security-admin • security-operator • sip-admin **Example**: **set permissions security-admin** The default setting is **all**.
server | server-pool {static | dynamic}	server-gatekeeper-id	*Secondary property.* Specifies the way the NN2600 reaches an H.323 Gatekeeper. • dynamic—The NN2600 learns the Gatekeeper ID via RAS messaging. • static—The GKId string must be configured. The NN2600 uses this configured string to contact a remote H.323 Gatekeeper. **Example**: **set server-gatekeeper-id dynamic** The default value is **dynamic**.

Object name	Associated properties	Description
third-party-call-control	media-forward-reference-direction	Identifies which leg of a call is to the call-center PBX, mapping the Rx and Tx streamsx to match the NICE equipment Rx and Tx streams. The following are valid options: • in-leg • out-leg **Example**: **set media-forward-reference-direction in-leg** The default setting is **out-leg**.
	inhibit-100-trying-for-reinvite	When enabled, the NN2600 does not send out a 100 Trying when it receives a re-INVITE. When disabled, the NN2600 does send out a 100 Trying in response to a re-INVITE. Example: **set inhibit-100-trying-for-reinvite disabled** The default setting is **enabled**.
radius-group	application	Enter the RADIUS application ID for the servers in this group. The following are valid options: • authentication—use SIP authentication • routing—use Acme Packet SIP routing Note that Java accounting ignores this setting and considers all RADIUS servers as candidates for RADIUS accounting. **Example: set application routing** The default setting is **authentication**.
contact-uri-settings-3xx-response	add-maddr [enabled | disabled]	When enabled, the NN2600 adds a maddr URI parameter if the original host is a fully qualified domain name (FQDN). **Example: set add maddr enabled** The default setting is **disabled**.

Object name	Associated properties	Description
session-policies	outbound-policy	Apply a session configuration policy to a session as it egresses the NN2600. **Example: set outbound-policy vsp\tls\certificate test**
altered-body	remove-body {true | false}	*Secondary property.* When this property is set to true, the NN2600 removes the SIP message body from the matching of SIP messages. This includes the “Content-Type” and other related headers. **Example: set remove-body true** The default setting is **false**.
q931-cause-sip-response map		Allows the configuration of q931-cause and/or h225 reason code for calls cleared by an external SIP UA. When an IW call is cleared on the SIP side, the SIP response code is used to consult an internal table for q931/h225 information needed when generating the ReleaseComplete, Admission Reject, or Location Reject message. By adding a q931-cause-sip-response-map entry, you can override the internal table defaults.
	q931-cause	Select a q931-cause to use when clearing the H.323 side of the call. If this map entry will not generate a q931-cause, or you want to use the default, select **Any**. **Example: set q931-cause userbusy**

Object name	Associated properties	Description
	h2250-reason	Select a h225-reason to use when clearing the H.323 side of the call. The following are valid values: • none—use the default h225-reason. • lrj—select lrj if you are generating LRJ messages and enter a relevant reason. • arj—select arj if you are generating ARJ messages and enter a relevant reason. • any—specifying only the q931-cause in this entry. **Example: set h225-reason arj** The default setting is **none**.
	sip-response	Select the sip-response match criteria for this entry. If this entry will not generate a q931-cause or you want to use the default, select **Any**. **Example: set sip-response 500** Min: 300 / Max: 699 The default setting is **0**.
sip-response-q931-cause-map		Allows the configuration of sip-response code for calls cleared by an external H.323 GW. When a ReleaseComplete, Admission Reject, or Location Reject message is received by the NN2600, the NN2600 consults an internal table to determine the appropriate SIP response code to generate when clearing the SIP side of the call. By adding a sip-response-q931-cause-map entry, you can override the internal table defaults.
	sip-response	Define the sip-response that will be used when clearing the SIP side of the call. **Example: set sip-response 350** Min: 300 / Max: 699 The default setting is **0**.

Object name	Associated properties	Description
	q931-cause	Select a q931-cause that helps to qualify the H.323 call-clear. If this map entry does not depend on the q931-cause value, either because there is no Q.931 present or because any Q.931 cause qualifies, choose **Any**. Example: **set q931-cause noresponse**
	h2250-reason	Select a h2250-reason type. The following are valid values: • LRJ—match an incoming LRJ message. • ARJ—match an incoming ARJ message. • H.225—match all other relevant traffic • none—H.225 reason should not be used as match criteria for this entry. **Example: set h225-reason lrj** The default setting is **none**.
third-party-call-control	transfer-file	Enter the media file you want played while an unattended call transfer is taking place. **Example: set transfer-file ring1** There is no default setting.

Deleted objects in Release 3.6.0m1

Object name	Property name
vsp > enterprise > servers	**call-hunting-type**

Deleted properties in Release 3.6.0m1

Object name
vsp > surveillance

Moved properties in Release 3.6.0m1

Property name	Former location	New location
ras-settings	cluster/box/number/interface/ip/h323	**session-config\ dns-client-settings\ routing-last-resort-dn**s

Changed properties in Release 3.6.0m1

Property	Change
sip-settings > persistent-destination-address	Default is now **true**.

Renamed objects in Release 3.6.0m1

Old name	New name
private-ip-gateway\group	**private-group**
vrrp	**vrrp-advertisements**
cluster-server-load	**server-load-db**
least-cost-routing	**route-server**
3pcc	**jtapi**

Renamed properties in Release 3.6.0m1

Old name	New name
private-ip-gateway\selfConnected	**self-connected**
term-transc-on-bye	**terminate-transaction-on-bye**
cxc-call-policy	**nnos-call-policy**
apply-policy-to-cxc-calls	**apply-policy-to-nnos-calls**
add-cxc-domain	**add-nnos-domain**
use-cxc-domain-in-search	**use-nnos-domain-in-search**
cxc-tunnel-creation	**nnos-tunnel-creation**
lcr-lookup-timeout	**route-server-lookup-timeout**
lcr-lookup-max-pending	**route-server-lookup-max-pending**
cms-preferences	**gui-preferences**
cms	**gui**

MIB changes in Release 3.6.0m1

This section covers changes that have been applied to Management Information Base (MIB) object definitions.

New MIB tables in Release 3.6.0m1

MIB table name	Description
sipGatewayCacTable	SIP Gateway Calling Group Call Admission Control Statistics
callingGroupCacRejectsTable	SIP Calling Group Call Admission Control Reject Statistics”
locationCacheCacRejectsTable	Net-Net OS-E Location Call Admission Control Reject Statistics”
locationCacheCacRejectsInboundTable	Net-Net OS-E Location Call Admission Control Inbound Reject Statistics”
locationCacheCacRejectsOutboundTable	Net-Net OS-E Location Call Admission Control Outbound Reject Statistics”
radiusRoutingTable	RADIUS status for Routing peers”
sipServerCacRejectsTable	SIP Server Call Admission Control Reject Statistics
switchCacRejectsTable	SIP Voice Gateway Call Admission Control Reject Statistics”
trunkCacRejectsTable	SIP TrunkGroup Call Admission Control Reject Statistics”

New MIB objects in Release 3.6.0m1

MIB object/table name
arenaCacheOutstandingCurrentActive
arenaCacheOutstandingMostActive
arenaCacheOutstandingTotalFailures
arenaCacheOutstandingMaxFailures

Obsolete MIB objects/tables in Release 3.6.0m1

MIB object/table name
installInfoTable
InstallInfoProvidesTable
installingInfoRequirementsTable
arenaCacheUsageByAllocatorOtherCount

Changed Tables in Release 3.6.0m1

MIB table name	Description
callAdmissionControlTable	ADDED: callAdmissionControlRejectsInSetup, callAdmissionControlRejectsMaxCalls
servicesRouteDatabaseTable	Index changed
sipServerAvailabilityTable	ADDED: sipServerAvailabilityReason
activeCallsTable	ADDED: activeCallsPostDialDigits
sipGatewayCacTable	ADDED: sipGatewayCacCallRateLimitingState, sipGatewayCacCallRateLimitingRate, sipGatewayCacCallRateLimitingInterval
arenaCacheByAllocatorTable	ADDED: arenaCacheByAllocatorCurrentActive, arenaCacheByAllocatorMostActive, arenaCacheByAllocatorTotalFailures, arenaCacheByAllocatorMaxFailures
arenaCacheUsageOutstandingTable	OBSOLETED: arenaCacheUsageOutstandingOtherCount

Known problems, restrictions, and operational considerations in 3.6.0m1

Configuring forking-settings

When configuring **forking-settings** under **session-configs**, you must enter a value for the **outbound-arbiter-rule** parameter or the **forking-type** parameter is not applied to the session.

Release 3.6

New features and major product changes

This section provides a description of the major features and changes applied with Release 3.6. Refer to the section, "Configuration changes in Release 3.6" for detailed information on new configuration objects and properties.

H.323 Gateway Registration

The NN2600 uses primary, backup, and alternate gatekeepers to route H.323 traffic. When the primary gatekeeper becomes inaccessible, you can configure the NN2600 to automatically switch to either a backup gatekeeper or an alternate gatekeeper. The primary difference is that backup gatekeepers are configured statically, while alternate gatekeepers are configured dynamically.

The NN2600 also provides support for an administrator to configure multiple remote H.323 gateways co-located on the same external IP address. The differentiating characteristic is their TCP port number. Each configured co-located gateway must be provisioned to initiate connections to a unique NN2600 TCP port.

The NN2600 provides the capability for the administrator to map Q.931 cause codes and/or H225 reasons to and from specific SIP response codes.

Configuring Secondary Properties

In order to simplify the presentation of configuration objects to those that are the most commonly used, the following properties listed below are now secondary properties. In order to set these properties via the GUI, you must click on the **Show advanced** button at the top of the screen. To set them in the CLI you need to explicitly set or configure them. They do not show up in the help or command completion.

Object name	Advanced property
servers	• federations • avaya • sip-host • lcs • mcs • sip-connection • sametime • dns-group
enterprise	• user-group-policy • unknown-server-policy
server	• local-ip • local-port • connection-retry-interval
network	• tcp-keepalive-time • tcp-keepalive-probes • tcp-keepalive-interval
carriers	• carrier • qos • currency • country • timeplan • hunt-group

Object name	Advanced property
settings	• accounting-anonymous-match • clear-binding-on-connection-broken • connection-timeout • database-write • filter-mcs-authint-to-auth • filter-mcs-force-IM-decrypt • filter-mcs-independent-header-schemes • filter-mcs-rewrite-ping-contact-hdr • filter-mcs-site-failover-threshold • filter-mcs-suppress-100rel • filter-lcs-input-remove-user-params • filter-lcs-input-remove-record-route-hdrs • ignore-contact-on-ack • location-cache-write-thru • resolve-routing-through-server-domain • max-udp-outbound-log • prune-associations • pruning-interval • read-header-max • read-line-max • read-message-max • cxc-tunnel-creation • socket-receive-buffer-size • sockets-idle-max • sockets-idle-min • sockets-initial-message-timeout • sockets-per-box-max • sockets-per-peer-max • stack-message-queue-max • stack-message-queue-min • stack-message-queue-reg-clip-threshold • supported-extensions • tunnel-policy • udp-tunnel-reclaim • udp-tunnel-reclaim-scan-interval • backup-server • register-retransmit-detection • remote-party-id-accounting • apply-to-methods

Object name	Advanced property
vsp	• local-identity • local-normalization • server-normalization • de-normalization • external-inbound-normalization • displayname-character-set-info • registration-proxy • pstn-gateway • pre-session-config • sip-timers • virtual-threads • virtual-dial-plan-pool • monitor-group • im-filtering • from-interface-group • to-interface-group • phones • presence-database • detect • oci-settings • external-policy-group • external-location-group • external-event-group • surveillance • gateway-routing • dtmf-generation • sip-manipulation-pool

The following properties listed below have been changed from secondary properties to basic.

Object name	Required property
settings	• local-directory-based-user-services

DID Support

In release 3.6, direct inward dial (DID) mapping is supported via the NN2600 Route Server Application, also known as the Least Cost Routing (LCR) client-server application. Under the LCR DID tab, you have the ability to import, generate, restore, backup, view, edit, delete, and purge DID mappings.

For complete information regarding DID support, refer to chapter 12 of the *Session Session Services Configuration Guide*.

Speaker Detection

Speaker detection functionality was introduced in release 3.6. When this feature is enabled and a call connects, the NN2600 monitors the audio to determine whether an answering machine or person are on the other end, or if the answering party is a modem or a fax machine. If the NN2600 detects the constant power training tone of a modem or fax machine, the call is disconnected.

Accounting Enhancements

Several accounting enhancements have been added to release 3.6:

- The **accounting flush** action has been modified. One of two things can happen when this action is executed. A target whose send has previously failed and is waiting for a retry interval to try again, will send again immediately. Also if there is a target writing to an output file, the NN2600 performs a rollover on the file, regardless of whether or not the condition to rollover has been reached yet. The results of this operation are logged and you can view the logs to obtain more information about files that have been flushed.
- You can create an **external-file-system** configuration which allows you to write accounting records to an outside server.
- The **file-system** configuration object, which allows you to write accounting records locally, has been enhanced. You can now format the output to **postgresql**.
- The **file-play** action has been enhanced so that you can configure the accounting CDRs to report more specific information pertinent to call control applications including: whether or not a call was connected successfully, disconnect reasons for specified calls, final response codes for specified calls, and scan times, play times, and file times for specified file-play actions.

IP Discard Packet Logging

You can now configure the NN2600 to account for all discarded packets that do not hit an existing pinhole. You can also generate log messages when such packets are discarded and record more complete information about a selection of these packets. This feature is configured via a new **packet-discard** object.

Re-Invite Handling Modification

As of release 3.6, you have the option to change the way the NN2600 handles re-INVITEs via a new parameter, **terminate-hold-retrieve-locally**, under the **third-party-call-control** object. When this property is enabled and a re-INVITE is received with an SDP that indicates it is either a hold or retrieve request, the NN2600 accepts the re-INVITE locally with the SDP acknowledging the hold or retrieve and the message is not forwarded.

Codec Handling Enhancements

The NN2600 now supports a preferred codec feature. This allows you to define the preferred codec as deduced from SDP offers and answers, adapt to match received codecs, and rewrite rfc-2833 headers when encoding audio. A new configuration object, **transcoding-policy**, has been created to configure this feature.

Media Auto-Anchoring

In releases prior to 3.6, you could enable the NN2600 to auto-anchor media. When the NN2600 has auto-anchoring enabled, it uses certain algorithms to determine anchoring necessity based on a variety of criteria, including whether you have configured smart anchoring via the **autonomous-ip** object and whether the calling devices are behind a firewall.

A new configuration property, **attributeless-auto-anchor**, under the **media** object, has been created. When this property is enabled, the NN2600 attempts to auto-anchor streams without additional NN2600 attributes in the SDP.

Xen Support

The NN2600 can now be downloaded as a Xen virtual machine. For detailed information on how to install the NN2600 software on a Xen server, see chapter one of the *Virtual Machine Information Guide*.

USB Support

As of release 3.6, the NN2600 supports USB sticks with up to 4 GB of storage to handle the NN2600 commissioning.

Acme Packet Naming Conventions

For existing customers who are upgrading from a prior release, the Covergence file names have been renamed under Acme Packet, Inc., as follows:

- Supertar upgrade file: now nnSE360.tar.gz
- USB file: now nnSE360-usb.img.gz
- ISO: now nnSE360.iso
- Archive Viewer: now nnSE360-av.zip
- Troubleshooter: now nnSE360-tshoot.zip
- SDK: now nnSE360-sdk.zip
- .NET SDK: now nnSE360-sdk-dotnet.zip
- JBOSS SDK: now nnSE360-jboss-sdk.zip
- Route Server Import: nnSE360-rsimport.zip
- WSDL tools: nnSE360-wstools.zip

Eventpush-service configuration

The **ip** > **eventpush-service** allows you to configure and redirect logged events to external computer Web browsers. The eventpush-service requires the **external-services** > **event-group** to declare the destination service URL of the external device.

Perform the following steps to enable and configure the eventpush-service:

1. Configure the **ip** > **eventpush-service**.

```
NNOS-E> config box
config box> config interface eth3
config interface eth3> config eventpush-service
config eventpush-service> set admin enabled
config eventpush-service> set protocol http 8081
config eventpush-service> set page-domain acmepacket.com
```

2. Edit the target Web application to include an IFrame. The IFrame is comprised of the name of the NN2600 device running the eventpush-service application, the web services port, and the string /cometapp/acmepacket.html.

For example, if the name of the NN2600 device running the eventpush-service is xyz.com with the service running on port 8081, and if the system is running over HTTP, then the reference is `http://xyz.com:8081/cometapp/acmepacket.html`.

3. Configure the external-service > event-group > event-service service-url property so that events are passed to the destination eventpush service. Enter the destination domain IP, the eventpush-service port, and the string /cometapp/ callouts. For example, `http://127.0.0.1:8081/cometapp/callouts`.

```
NNOS-E> config external-services
config external-services> config event-group a
config event-group a> config event-service cometd
Creating 'event-service cometd'
config event-service cometd> set service-url http://172.0.0.1:8081/
   cometapp/callouts
```

4. Configure vsp to forward events to event-group.

```
NNOS-E> config vsp
config vsp> set external-event-group external-services\event-group a
```

5. Save the configuration.

To change the reporting mechanism from the pushlet-app configuration to the eventpush-service configuration:

1. Configure the eventpush-service object as described in Step 1.
2. Remove the pushlet-app setting from the **box > interface > ip > web-service** application property.
3. Change the service-url property of the external-service > event-group > event-service object, removing the pushlet event service and replacing it with the eventpushservice.

   To do so, enter the eventpush port, and change the context portion of the URL from "pushletapp" to cometapp."

Fixes

The following table summarizes the fixes that have been applied in Release 3.6.

Component	Description	Problem ID	Found in Release
Policy	SIP faults observed during an OCS/ATT transfer test case.	14421	3.4.4
SIP	NN2600 sends 100 trying to the port specified in the VIA header rather than the source port.	14470	3.3.7
Policy	Enhance regex header functionality to be able to specify where the expression is applied.	14511	3.5.1
Management	Problems with sampling active calls.	14219	3.4.4
Media	Calls were improperly terminated after a 180 Ringing message is received.	14567	3.4.4
Location Services	NN260 not sending SIP-directive “refuse” messages.	14340	3.4.4
ENUM	INVITE not generated after ENUM query; ENUM lookup transforming SIP URI incorrectly.	14726, 14684	3.5.1
Manager	Fix fault related to a scheduled action.	14546	3.4.2
OS (upgrade)	After upgrading from 3.3.6 to 3.5.1, eth0 and eth2 interchanged on IBM 3250.	14758	3.5.1
LCR Import	Add to-URL-match and from-URL-match properties to purge a particular LCR route table entry.	14931	3.4.4
Kernel	In-leg and out-leg TOS does not work with TCP.	14072	3.5.0
Servers	Add support for multiple servers with the same IP address but different ports to be configured as h323-server objects.	14767	3.5.1
Pushlet	Web-service leaving connections in a close-wait state.	9346	3.3.0
TCP	NN2600 not opening TCP connection to Tomcat server.	14940	3.4.3
H.323	Control IE element in H.225 setup message.	15014	3.5.1
Transcoding	Preferred codec not always being enforced.	15032	3.5.1

Component	Description	Problem ID	Found in Release
OS	OS drive suddenly went to read-only.	15125	3.5.0
Media Auto Anchor	Auto anchor functionality not working appropriately.	14060	3.5.1
Call Control	Wrong reason code display in session call logs.	13067	3.5.0
Media	Sequence number reset in the same SSRC causes mixer to wait until one leg of the call completed before continuing to play out.	15147	3.4.4
Media	NN2600 anchors call after on-hold.	11989	3.2.8
SIP	Issues with the way the NN2600 is handling NAT on the sametime interface.	14069	3.3.8
Transcoding	Fax failing when transcoding is invoked.	14850	3.5.1
Kernel	Kernel issue processing packets that arrive out of order.	15310	3.5.0
Dial Plans	When first server of the hunt-group is disabled, the NN2600 does not try the entire group.	14887	3.5.1
SIP	Add support for a new parameter from WSDL file-play/file-play-broadcast actions to be added to CDR records.	15352	3.5.1
Servers	Enhance the ability to handle duplicate IPs for servers.	11613, 11922	3.4.4
Kernel	Fix kernel memory leak.	15304	3.5.1
Media	Enhanced support for proprietary secure call indication procedures.	14599	3.5.0
LCR Import	A blank “from” field in an imported CSV file causes an error in the LCRimport application.	15430	3.5.1
Registration	Support forwarding a request to another NN2600 when the binding was registered on another box of the cluster.	15559	3.5.1
GUI	GUI doesn’t properly handle the “monitor” configuration property and causes a fault.	15588	3.6.0
OS	The USB Installer fails on a RAID system without 6 drives.	15607	3.5.1
Location Services	Memory corruption issue in the location services code.	15593	3.5.0

Component	Description	Problem ID	Found in Release
Config Audit	Enhance logging to indicate configuration property changes.	15620	3.5.1
Location Services	Location-summary, total-bindings, and total-aged not being incremented properly.	15348	3.5.0
Kernel	NN2600 not relaying RTP packets in hairpin scenario.	15641	3.5.2
Servers	SIP deadlock causing fault.	15672	3.4.4
Accounting	Enhance the disconnect cause field in the CDR to provide more information on the reason for the disconnect.	15725	3.6.0
SIP	New accounting features added.	15756	
SIP	Add source and destination information labels in the GUI ladder diagrams.	14572	3.5.1
H.323	NN2600 sending an incorrect Call Reference Value in Setup message.	15701	
SNMP	NN2600 not handling getnext properly.	15761	3.4.4
MX	Archiving to FTP server fails after a few calls.	15734	3.5.2
Accounting	Response code should be in CDR.	15812	3.6.0
Location Services	Contact header in the 200 OK to a SUBSCRIBE isn't modified by the NN2600.	15661	3.4.4
Dial Plans	When all servers in the hunt-group are down, the **show call-routing** status displays them as "up."	15558	3.5.1
Location Services	There is no cap on the amount of bindings the NN2600 can register.	15550	
SIP	Added configuration property to control addition of "received=" parameters.	15647	3.5.1
Database	Database failure causing system to be unresponsive.	7455, 15412	3.2.1 / 3.5.1
Registration	When **unregister-aged-bindings**=**client-side**, too many sessions created.	15904	3.5.0
Accounting	The accounting-data entry fields no longer require the tag field to be specified.	15815	3.6.0

Component	Description	Problem ID	Found in Release
SIP	Unable to alter the Allow header with the reg-ex-header settings object.	13844	3.5.0
GUI	Call Logs tab in the GUI faulted if a configuration property was missing.	15941	
Transcoding	Fix transcoding issue where most-preferred codec was not honored.	15032	3.6.0
Media	INVITE wrongly rejected when it is excluding the most-preferred codec.	15970	3.6.0
SIP	NN2600 incorrectly resetting the remote address of the INVITE transaction.	15974	3.6.0
Configuration	**Session-config > sip-settings > persistent-destination-address** needs to default to false.	16042	3.5.2
Accounting	CDR archive push support for one minute intervals.	16083	3.5.4
H.323	If H.323 call has no calling party, SIP-IWF functioning fails.	16126	3.5.2
CAC	Call admission not allowing configured number of calls.	16139	3.5.5
Manager	Unable to mount NFS drive on release 3.5.3.	16188	3.5.3
SIP	NN2600 can't forward received INVITE due to internal parser errors.	16178	
Call Logs	The "Result" value in the call logs is inaccurate.	15793	3.6.0
SIP	In 3PCC, NN2600 unable to apply Inbound or Outbound session configurations.	16183	3.5.5
Media	Incorrect jitter statistics displayed.	16021	3.5.2
Media	NN2600 terminates call due to inactivity timer even after it has released itself from media path.	16112	3.5.2
Kernel	Ensure that auto-anchored calls that are released are not terminated due to the inactivity timer.	15828	3.5.2
Media	After a failover a hold is not detected.	16292, 16234	3.6.0

Component	Description	Problem ID	Found in Release
SNMP	SNMP standard MIB-2 returns nonexisting interface indexes for VRRP IPs.	16202	3.5.5
SIP	Delayed to Early Offer doesn't respond to a 491.	16322, 16374	3.5.1

Configuration changes in Release 3.6

The section provides a summary of the additions, changes, and deletions to the NN2600 configuration when upgrading to Release 3.6. It covers new objects and properties, configuration objects and properties that have been renamed, and those objects that have been deleted and are no longer available.

New objects in Release 3.6.0

Object name	Associated properties	Description
altered-body		This configuration object allows you to alter the body of any SIP message for a matching session. You should only change the SIP message body under specific, required circumstances.
	admin [enabled | disabled]	When enabled, you can alter the body of any SIP message for a matching session. The default setting is enabled.
	altered-body	Alters the body of any SIP message for a matching session.
	apply-to-methods	Specifies the message type to which the system applies message body changes. The system then changes the specified URI according to the settings of the header and destination properties of this object. When you modify this value, the system overwrites the current setting with only the message types you specify. To enter multiple types, enter them separated by a plus sign (+) with no spaces. The default setting is INVITE.

Object name	Associated properties	Description
	apply-to-responses	Specifies whether to apply message body changes to just SIP requests, or to both requests and responses. If you enter a value of yes, you must include the response-code. The default setting is yes.
altered-header		This configuration object allows you to modify or create header values in calls matching this session configuration. You can create multiple header-altering configurations.
	admin [enabled | disabled]	When enabled, you can alter header values in calls matching this session configuration. The default setting is enabled.
	source-header	Specifies the URI from which the NN2600 initially derives the data that is to be written to the destination header.
	source-field	Specifies the portion of the URI that the system writes to the destination. Possible values are: user, host, selection, and value.
	destination	Specifies the header to be created or modified by the properties set in this object. The URI specified in this property is modified with the data from the source-field property. If the header doesn't exist in the message, the NN2600 creates it. The following are valid values: to, from, request. The default setting is from.
	destination-field	Specifies the field in the destination URI to overwrite. The following are valid values: user, host, display, full. There is no default setting.
available-memory		This object allows you to enable a sampling interval for the NN2600 to check the available memory.
	admin [enabled | disabled]	Enable or disable the NN2600 checking the available memory. The default setting is enabled.
	interval	Defines how often the NN2600 pools the status provider for data. The minimum value is 30 and the maximum value is 1036800. The default setting is 1:00:00 (1 hour).

Object name	Associated properties	Description
codec-payload-type-bindings		The codec-payload-type-bindings configures a binding between a codec name and a payload type. Without any codec-payload-type-bindings configured, the NN2600 uses a default DTMF payload type of 101. This configuration element is set when you want to change the default DTMF payload type offered by the NN2600. This property takes precedence over the default of 101. Codec-payload-type-bindings is used when the NN2600 generates its own SDP for outgoing calls. The NN2600 generates its own SDP for features like file-play or when the NN2600 is in a Delayed-Offer/Early-Offer network.
	binding	Bind a codec name to a particular payload type. The syntax for this parameter is: codec-payload-type-bindings <codec> <payload-type>. Payload type can range from 0-127.
external-file-system		Configures the external file system, allowing you to write accounting records to an outside server.
	admin [enabled | disabled]	When enabled, the NN2600 forwards accounting and SIP call detail records to the target file path. The default setting is enabled.
	format	The output format of the file you are creating. The available file formats are: csv, proprietary, tab, and postgresql. The default setting is csv.
	url	Enter the URL of the external target to which you are sending CDRs.

Object name	Associated properties	Description
	cdr-processing	Specify how the CDRs are collected. The following are available processes: batch (Min: 0 / Max: 4294967295; default 20000), roll-over (never, hourly, daily, per-minute; default hourly), and interval (Min: 60 seconds, Max: 1036800 seconds; default 0).
h225-settings		This configuration object allows you to configure H.225 support on the NN2600.
	fast-start [enabled | disabled]	When enabled, the NN2600 accepts inbound H.323 fast start calls and includes fast start in SETUP messages for outbound H.323 calls. The calls fall back to slow if fast start is unsuccessful. The default setting is enabled.
	manual-ringback [enabled | disabled]	If enabled, the NN2600 prohibits remote ringback. When this property is disabled, SIP to H.323 calls attempt to open an audio channel for remote ringback. The default setting is enabled.
	use-inbound-call-settings [enabled | disabled]	When enabled for an H.323 to H.323 call, the NN2600 uses inbound H.323 call settings for H.323 outbound calls. The default setting is disabled.
	fwd-progress-as-alerting [enabled | disabled]	When enabled, the NN2600 sends an Alerting message instead of a Progress message. The default setting is disabled.
	default-terminal-type	Identifies the NN2600 terminal type. This is used for MSD. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 60.
	multiple-calls [enabled | disabled]	When enabled, the NN2600 allows calls to share an H.225 connection. The default setting is disabled.
	maintain-connection [enabled | disabled]	When enabled, the NN2600 keeps an H.225 connection open after calls are cleared. The default setting is disabled.

Object name	Associated properties	Description
	conn-idle-timeout	Specifies the maximum lifetime in seconds of an idle H.225 connection. A value of 0 indicates an idle connection should never timeout. The minimum configuration value is 300 and the maximum is 65535. The default setting is 3600.
	h323-user-alias	Specifies the source and destination address type in Setup, Alerting, Connect, ARQ, and LRQ messages. The following are valid h323-user-alias values: none, dialedDigits, h323ID, urlID, emailID. The default setting is none.
	call-alerting-timeout	The maximum number in seconds the NN2600 waits for Alerting message after sending a SETUP. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.
	call-establishment-timeout	The maximum number in seconds the NN2600 waits for an H.323 call to be established. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 60.
	end-session-timeout	The maximum number of seconds the NN2600 waits after sending a ReleaseComplete before call resources are reclaimed. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 15.
	h245-establish-timeout	The maximum time, in seconds, the NN2600 waits for an H245 connection to be established. The call clears if this timeout is reached. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 1.
	reinvite-type	*Secondary property.* Indicates if the NN2600 should use Terminal Capability Set or Extended Fast Connect messages to reconfigure media channels. The default setting is emptyTermCapSet.

Object name	Associated properties	Description
	use-progress-inband [enabled | disabled]	When enabled, inband ring information from the inbound H.323 call-leg is propagated to the outbound call-leg. The default setting is enabled.
	fwd-retrieve-no-tx [true | false]	When true, the NN2600 does not pause remotetransmitted if media information is 0.0.0.0. The default setting is true.
	use-server-connection [true | false]	*Secondary property.* specifies whether the NN2600 creates a new, or uses an existing, TCP connection. If true, the NN2600 uses a TCP connection created by the remote gateway instead of creating a new outbound TCP connection. Use this property for a remote H.323 gateway using connection sharing for its H.225 traffic. (It uses a single TCP connection for multiple calls.) The default setting is true.
	enum-lookup-called-party [enabled | disabled]	When enabled, the NN2600 performs an ENUM lookup of the called number before making an outbound H.323 call. The default setting is disabled.
	enum-domain	The domain used for ENUM lookups. The default setting is e164.arpa.
h245-settings		The H.245 settings configuration object allows you to configure H.245 on the NN2600.
	h245-tunnel [enabled | disabled]	When enabled, the NN2600 attempts to use an H.225.0 connection for H.245 traffic. The use of H.245 tunneling depends on indication from both H.323 terminals and gateways. The default setting is enabled.
	early-h245	The NN2600 does not support early H.245. Set this property to indicate how to handle a request for early H.245. The following are valid early-h245 values: • notunnel—The NN2600 ignores the early H.245 and completes the call setup using slowstart. • reject—The NN2600 rejects the call. The default setting is notunnel.

Object name	Associated properties	Description
	wait-for-remote-tcs [true | false]	When true, the NN2600 waits to receive a Terminal Capability Set message before advertising its capabilities. When false, the NN2600 issues a TCS message after a slowstart call is connected. The default setting is true.
	clc-when-pausing-remote [true | false]	*Secondary property.* When true, the NN2600 closes its TX channels when pausing the remote H.323 terminal. The default setting is false.
	send-msd-when-unpausing -remote [true | false]	*Secondary property.* Specifies whether the NN2600 will conduct master-slave determination (MSD) when using TCS to unpause a remote H.323 gateway. The default setting is false.
	use-h450-hold-retrieve [enabled | disabled]	When enabled, the NN2600 uses H.450 supplemental service PDUs for holds and retrieves. The default setting is enabled.
	sip-h323-dtmf-translate	Sets preferences for H.323-SIP DTMF interworking for a particular H.323 trunk. The default setting is inband.
	codec-selection	*Secondary property.* Indicates how the NN2600 chooses converged codecs. The following are valid values: • none—No codec is being used. • local—Use the highest preference common codec seen in SIP SDP. • remote—Use the highest preference common codec in remote TCS. • followMSD—Use the result of master-slave determination to decide. The default setting is remote.
	map-ptime-to-fpp [true | false]	*Secondary property.* When set to **true**, the NN2600 uses SDP ptime parameter to set max-frames-per-packet codec value in Terminal Capability Set. Ptime and FPP are not equivalent, however, this allows compatibility in some interworking scenarios. The default setting is false.

Object name	Associated properties	Description
	map-fpp-to-ptime [true | false]	*Secondary property.* When true, the NN2600 uses max-frames-per-packet codec value in Terminal Capability Set to set SDP ptime parameter. Ptime and FPP are not equivalent, however, this allows compatibility in some interworking scenarios. The default setting is false.
	add-equivalent-codecs [true | false]	*Secondary property.* When true, the NN2600 adds equivalent codecs to Terminal Capability Set. The currently supported case is G729 present in SDP which would add both G729 and G729A in TCS. The default setting is false.
h323-service-routing		Configures the H.323 service routing metrics.
	metric1	Sets the metric1 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is user-metric.
	metric2	Sets the metric2 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
	metric3	Sets the metric3 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
	metric4	Sets the metric4 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.

Object name	Associated properties	Description
	metric5	Sets the metric5 load type. The following are valid values: • none • user-metric • intf-thruput The default setting is none.
header-normalization		This object alters the user portion of the specified header.
	admin [enabled | disabled	Enable or disable header normalization on the NN2600. The default setting is enabled.
	destination	Specifies the header to be created or modified by the properties in this object. That is, the NN2600 modifies this URI with the data from the source.
	value	Specifies the field in the specified destination URI to overwrite. The following are valid values: • none—no normalization applied • prepend—prepend string • prepend-to—prepend string to certain length • strip-off—strip off N characters • strip-off-to—strip off prefix to certain length • replace-prefix—replace prefix with a different prefix • replace-with—replace with a different name • append—append extension number The default setting is none.
	apply-to-methods	Specifies the message type to which the system applies header value changes. The NN2600 then changes the specified URI according to the settings of the header and destination properties of this object. When you modify this value, the NN2600 overwrites the current settings with only the message types you specify. Enter multiple types separated by a plus sign (+) with no spaces. The default setting is INVITE.

Object name	Associated properties	Description
	apply-to-responses	Specifies whether to apply header value changes to SIP requests or requests and responses. If you enter a value of **yes**, you must include the response-code. The following are valid values: • no—do not apply to responses (requests only) • yes—apply to responses of this type The default setting is no.
	session-persistent [enabled | disabled]	Specifies to which messages in a session the NN2600 should apply changes made with this object. When enabled, the NN2600 applies any TO, FROM, or REQUEST URI changes to the first and all subsequent messages in a session. When disabled, the system applies the changes only to the first message in the session. The default setting is disabled.
inbound-header-settings		This configuration object allows you to set fields to remove and/or replace header settings in the SIP headers for inbound traffic.
	pAssert-mode [enabled | disabled]	*Secondary property.* Sets whether or not to strip the number in the P-Asserted-Identity field from the SIP header. When enabled, the NN2600 replaces the value in the From field with the value from the P-Asserted-Identity field for the outbound call leg. (Note that the NN2600 maintains the original From field value in the Contact field.) The default setting is disabled.
	header-to-strip	*Secondary property.* Configures the NN2600 to strip the value of the specified field. Enter a SIP header field name.
	allowed-header	Sets the SIP headers that should be explicitly allowed to remain in the SIP message. You can enter any number of header names by re-executing the command.

Object name	Associated properties	Description
	blocked-header	Sets the SIP headers that should be explicitly removed from the SIP message. You can enter any number of header names by re-executing the command.
	apply-allow-block-to	Sets whether the allow and block properties of this object apply to request messages, response messages, or both. The following are valid apply-allow-block-to values: • requests—apply to requests only • responses—apply to responses only • requests-and-responses—apply to requests and responses The default setting is requests-and-responses.
media-scanner-settings		This object allows you to configure media scanner settings. When media scanner settings are enabled, the media-scanner is started after the outgoing call connects and the pre-scan-time has elapsed. The media-scanner monitors the signal strength and duration of the received audio to divide into intervals.
	admin [enabled | disabled]	Enable or disable the media scanner settings for play-file-broadcast. The default setting is disabled.
	pre-scan-time	The number of milliseconds to delay before invoking the media scanner for speaker detection. The minimum configuration value is 0 and the maximum is 4294967295. The default value is 20 msecs.
	max-scan-time	The maximum number of milliseconds before canceling media scanning due to timeout. The minimum configuration value is 0 and the maximum is 4294967295. The default value is 30000 msecs.
	low-threshold	Enter the quiet signal power threshold in dbM. The minimum configuration value is -63 and the maximum is 3. The default setting is -36.

Object name	Associated properties	Description
	high-threshold	Enter the talk or tone signal power threshold in dbM. The minimum configuration value is -63 and the maximum is 3. The default setting is -36.
	low-long-duration	The number of milliseconds of detected quiet before declaring a long-pause. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 2000.
	high-long-duration	The number of milliseconds of detected talk or tone before declaring a long-talk or stable-tone.The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 900.
	averaging-window	*Secondary property* The window of time used when calculating signal strength. The minimum configuration value is 10 and the maximum is 1000. The default setting is 100.
	nominal-rounding-factor	*Secondary property.* The signal strength is rounded to the nearest multiple of the value you enter for this property. The minimum configuration value is 1 and the maximum is 25. The default setting is 2.
packet-discard		This configuration element allows you to configure the IP discard packet logging feature. If an IP interface has media-ports configured, you must first disable the media-ports > idle-monitor property, before the packet-discard object can be enabled.
	admin [enabled | disabled]	Enable or disable the packet discard feature. The default setting is enabled.
	track-port [enabled | disabled]	When enabled, this will log an additional type of message with the list of ports that were hit within the logging interval. The default setting is disabled.
	scan-interval	The interval in seconds between reading and logging the latest discarded packet information. The minimum configuration value is 10 and the maximum is 86400. The default setting is 60.

Object name	Associated properties	Description
provisional-response		This object allows you to add any additional provisional responses you want sent along after the “100 Trying” response at the start of a normal INVITE dialog.
	additional-response	Enter additional provisional responses you want sent with the INVITE dialog.
q931-cause-sip-response-map		This configuration object allows you to map Q.931 cause codes to SIP response codes.
	translation	Translates Q.931 cause/H.225 reason to SIP response codes.
q931-settings		This configuration object is used to configure Q.931 settings on the NN2600.
	numbering-play	The Q.931 numbering plan set in Calling and Called Party number information elements. The following is a list of valid numbering-plan values: • unknown • ISDN • data • telex • national-standard • private • reserved The default setting is ISDN.
	numbering-type	The Q.931 numbering type set in Calling and Called Party number information elements. The following is a list of valid numbering-type values: • unknown • international • national • network-specific • subscriber • abbreviated • reserved The default setting is allowed.

Object name	Associated properties	Description
	presentation-indicator	Enter the static presentation value to use. The following is a list of valid presentation-indicator values: • allowed • restricted • numberNotAvailable • reserved The default setting is allowed.
	screening-indicator	Enter the static screening value to use. The following is a list of valid screening-indicator values: • notScreened • verifiedPassed • verifiedFailed • networkProvided The default setting is notScreened.
	privacy-dynamic [true | false]	When true, the screening and presentation are dynamic. The default setting is true.
	use-incoming-display-ie [true | false]	When true, the NN2600 attempts to use Display IE from the SETUP message when building SIP From: header display-name. The default setting is true.
	add-outgoing-displaytext-ie [true | false]	When true, the NN2600 attempts to use SIP From: header display-name when building Display IE in the outgoing SETUP message. The default setting is false.
	q931-bearer-capability-ie	Set the Q931. Bearer Capability values used in outgoing H.323 messages.
sip-manipulation		Configure a specific SIP manipulation. This lets you add, modify, and delete SIP headers and parts of the SIP headers called SIP header elements. SIP header elements are the different subparts of the header, such as the header value, header parameter, and URI parameter.
	description	Enter a description of this SIP manipulation object.
	header-rule	Enter a list of header rules for this SIP manipulation.

Object name	Associated properties	Description
sip-manipulation-pool		Secondary object. Allows you to configure the pool of named SIP manipulation objects for the NN2600. These contain lists of SIP header manipulation rules and elements.
	sip-manipulation	Enter the SIP manipulation you want to configure.
sip-response-q931-cause-map		Allows you to translate SIP response codes to q931-cause and h225-reason. This is used when clearing H.323 calls.
	translation	Translate SIP response codes to q931-cause/h225-reason.
transcoding-policy		This transcoding policy object allows you to configure the transcoding policy for the NN2600. This includes defining the preferred codec as deduced from SDP offers and answers, adapting to match received codecs, and rewriting rfc-2833 headers when encoding audio.
	media-types	The types of codecs that may be transcoded. These values are added to the SDP. The following is a list of codecs that may be transcoded: • pcma • pcmu • g7221 • g723 • g728 • g729 • g726-16 • g726-24 • g726-32 • g726-30 • gsm • gsm-amr • iLBC
	most-preferred [true | false]	When true, the NN2600 forces audio to only use the most preferred codec. The default setting is false.

Object name	Associated properties	Description
	symmetric-codec [true | false]	When true, the NN2600 adapts and matches the correct codec when the endpoint has switched the “primary” codec. The default setting is false.
	balance-ptime [true | false]	When true, the NN2600 attempts to balance RTP packet times with the SDP. The default setting is true.
	auto-release [true | false]	When true, the NN2600 attempts to release transcode resources when auto-anchoring is enabled. The default setting is true.
	block-unknown [true | false]	When true the NN2600 blocks unnegotiated packet types. The default setting is false.
	decode-telephone-events [true | false]	When true, the NN2600 decodes telephone-events into audio during transcoding when both sides do not support telephone-events. The default setting is false.

New properties in Release 3.6.0

Existing object name(s)	New property name	Description
accounting-data	**custom-data-grouping-string**	The characters used to associate custom data tags and values. The default setting is =.
	custom-data-delimiter	The characters used to separate group data entries. The default setting is ;.
call-failover	**server-load [enabled | disabled]**	When enabled, the NN2600 calculates the server load and distributes traffic counters around the cluster. Based on these distributed counts, each NN2600 in a cluster knows the fail-over status. The default setting is disabled.
cluster	**share-h323-port [true | false]**	Controls whether the H.323 service routes are pushed around a NN2600 cluster. This property is not currently supported. The default setting is false.
database-group	**batch-insert-size**	The number of CDRs in one database insert request. The minimum configuration value is 1 and the maximum is 50. The default setting is 25.

Existing object name(s)	New property name	Description
eventpush-service	**page-domain**	Specifies the common domain name of the NN2600 and the system running the web application.
file-client	**http-max-redirects**	The number of redirects in an HTTP URL before the NN2600 issues a warning. The minimum configuration value is 1 and the maximum is 100. The default setting is 10.
file-system	**format**	The output format of the file you are creating. The following are available file formats: • csv • proprietary • tab • postgresql The default setting is csv.
	call-field-filter	Filter out what fields are sent with accounting records. If this is left blank, all fields are sent in the accounting records. The following are valid fields: • SessionID • Recorded • CallID • To • From • Method • IncomingRequestURI • PreviousHopIp • PreviousHopVia • OutgoingRequestURI • NextHopIp • NextHopDn • Header • Origin
	file-path	Enter the path and name of the file to write the records.

Existing object name(s)	New property name	Description
	roll-over	Set the schedule for creating new log files. The following values are valid: • never—never renew the file • minute—renew the file once a minute • hourly—renew the file once an hour • daily—renew the file once a day The default setting is daily.
	purge-old-logs [true | false]	Allows you to remove files modified earlier than the retention period, excluding the current file. You can identify the current file using the status provider. The default setting is false.
	retention-period	Set the number of days logs should be retained in the system. The minimum configuration value is 0 and the maximum is 5184000. The default setting is 3 days.
forking-settings	**max-arbitration-options**	*Secondary property.* Specifies the number of potential destinations to consider when applying a rule. The smaller of this and **max-hunt** takes effect when the final destinations are determined. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is unlimited.
h323-server	**session-duration-max**	Sets the maximum duration, in seconds, of an H.323 call. A value of **0** indicates there is no maximum lifetime. The minimum configuration value is 0 and the maximum is 1000000. The default setting is 0.
	admission-control [enabled | disabled]	Enable or disable admission control for SIP as all calls (H.323-SIP and H.323-H.323) pass through the SIP process. The default setting is disabled.
	max-concurrent-h323-calls	The maximum concurrent H.323 calls on this server. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 1500.
h323-settings	**stack-worker-threads-max**	Enter the number of H.323 stack worker threads. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.

Existing object name(s)	New property name	Description
	connection-threads-max	Enter the number of threads processing H.255 TCP traffic. The minimum configuration value is 0 and the maximum is 4294967295. The default setting is 4.
	process-auto-restart [enabled | disabled]	When enabled, causes the H.323 stack to restart when deadlocks are detected. The default setting is enabled.
icmp	**limit**	Limits the number of ICMP packets that can be received per second on this IP interface. The minimum configuration value is 1 and the maximum is 1000. The default setting is 10.
media	**attributeless-auto-anchor [enabled | disabled]**	*Secondary property.* When enabled in conjunction with the **anchor-mode=auto**, the NN2600 attempts to auto-anchor streams without additional NN2600 attributes in the SDP. The default setting is disabled.
	release-provisionally-anchored-media [true | false]	*Secondary property.* Release media resources that have been provisionally anchored. The default setting is false.
	report-last-timestamp [enabled | disabled]	When enabled the NN2600 reports the timestamp of the last received media packet. The default setting is disabled.
	monitor-rfc-2833 [enabled | disabled]	Specifies whether to have the NN2600 change SSRC when it detects RTP sequence number discontinuity on active SSRC. The default setting is disabled.
registration	**ignore-from-tag [enabled | disabled]**	When enabled, the NN2600 uses the call ID only to associate the registration with a session. When disabled, the NN2600 uses both the call ID and the From tag to associate the registration to a session. The default setting is enabled.
sip-settings	**allow-redirect [enabled | disabled]**	When enabled, the NN2600 is able to redirect incoming calls to other servers. The default setting is enabled.
syslog	**port**	Specifies the port number over which the NN2600 should communicate with this syslog server. The minimum configuration value is 1 and the maximum is 65535. The default setting is 514.

Existing object name(s)	New property name	Description
third-party-call-control	**terminate-hold-retrieve-locally [enabled | disabled]**	When this property is enabled, if a re-INVITE is received with an SDP that indicates it is either a hold or retrieve request, The NN2600 accepts the re-INVITE locally with the SDP acknowledging the hold or retrieve and the message is not forwarded. When this property is disabled, re-INVITE messages with an SDP that indicate hold or retrieve receive no special treatment. The default setting is disabled.
	reinvite-originator [enabled | disabled]	When enabled, the NN2600 reinvites the original UAC after the call is initially set up. The default setting is disabled.
	skip-shuffle-complete-if-anchored [enabled | disabled]	When enabled, no reinvite is sent forwarding the SDP contained in the ACK for calls with anchored media. The default setting is disabled.
	forward-302-diversion-header	*Secondary property.* When enabled, if a 302 Redirected response with a Diversion: header is received by the NN2600, the Diversion: header is forwarded in the response. The default setting is enabled.
web-service	**max-message-process-threads**	The maximum number of messaging processing threads. The minimum configuration value is 10 and the maximum is 200. The default setting is 10.
	max-http-connections	The maximum number of outbound http connections. The minimum configuration value is 100 and the maximum is 300. The default setting is 100.
	max-http-client-connections	The maximum number of outbound HTTP connections per host. The minimum configuration value is 5 and the maximum is 100. The default setting is 10.

Renamed objects and properties in Release 3.6.0

Old object or property name (in bold text)	New name
There are no new renamed objects or properties in release 3.6.	

Moved objects and properties in Release 3.6.0

Property name	Former location	New location
settings > local-directory-based-user -services	Secondary property.	Basic property.
hunt-group	vsp > carriers > hunt-group	vsp > hunt-group

Deleted objects and properties in Release 3.6.0

Configuration path	Deleted object or property
vsp > accounting	• accounting-file-check-interval • num-of-threads • queue-directory-allowed-when-busy • directories-to-be-queued
vsp > accounting > archiving	• archive-in-progress-sessions
vsp > default-session-config > file-transfer	• virus-scan
vsp > autonomous-ip location-pattern	• admin • description • match • priority • location • validate-bindings
vsp > default-session-config > media	• rtp-source-lock • hold-translation • hold-remove-telephone-events
preferences > pushlet-app	• page-domain
vsp > default-session-config > sip-settings	• session-match-callid-only
services > virus-scan	
vsp	• de-normalization
box > mx	• network
box > mx > card	• admin • file

Deleted actions in Release 3.6.0

Action or status provider
mx

New and revised actions in Release 3.6.0

Action or status provider	Description
accounting-flush	The **accounting flush** action purges an accounting file you specify. The results of this operation are logged and you can view the logs to obtain more information on files that have been flushed. You can specify a **file-system** or an **external-file-system**.
show accounting-targets	Displays information from all accounting targets configured on the NN2600. The settings are configured using the **file-system** object.
show accounting-targets-file-system	Displays information for each accounting target configured on the NN2600. This shows information for both file-system and external-file-system targets.
show kernel-rule-stats	To display the cumulative packet discard statistics, enter the command with **show kernel-rule-stats instance= packet-discard.**
show media-scanner-summery	Displays media scanner settings. The media-scanner monitors the signal strength and duration of the received audio to divide it into intervals.
show media-scanner-interval	Displays media scanner intervals. The media-scanner monitors the signal strength and duration of the received audio to divide it into intervals.

MIB changes in Release 3.6

This section covers changes that have been applied to Management Information Base (MIB) object definitions since Release 3.5.5.

New MIB objects in Release 3.6.0

MIB Object name
arenaCacheOutstandingInstrumentation
arenaCacheOutstandingMaxCount
arenaCacheOutstandingInitialSize
arenaCacheOutstandingMaxSize

MIB Object name (continued)
arenaCacheOutstandingAllocatedFromCache
arenaCacheOutstandingFreedToCache
arenaCacheOutstandingCreated
arenaCacheOutstandingCreateFailed
arenaCacheOutstandingDestroyed
arenaCacheOutstandingCurrentFree
arenaCacheOutstandingFewestFree
arenaCacheOutstandingCurrentSmall
arenaCacheOutstandingCurrentCorrect
arenaCacheOutstandingcurrentLarge
arenaCacheOutstandingSampleCount
arenaCacheOutstandingTotalAllocs
arenaCacheOutstandingMinAllocs
arenaCacheOutstandingMaxAllocs
arenaCacheOutstandingTotalBytes
arenaCacheOutstandingMinBytes
arenaCacheOutstandingMaxBytes
arenaCacheOutstandingArea1
arenaCacheOutstandingArea2
arenaCacheOutstandingArea3
arenaCacheOutstandingArea4
arenaCacheOutstandingArea5
arenaCacheOutstandingArea6
arenaCacheOutstandingArea7
arenaCacheOutstandingArea8
arenaCacheOutstandingArea9
arenaCacheOutstandingArea10
arenaCacheOutstandingArea11
arenaCacheOutstandingArea12
arenaCacheOutstandingArea13

MIB Object name (continued)
arenaCacheOutstandingArea14
arenaCacheOutstandingArea15
arenaCacheOutstandingArea16
accountingFilesMirrors
accountingFilesTargets
kernelSummaryNumberRulesInGarbage
accountingStoreDirectory
accountingStoreDiskUsage
accountingStoreState
accountingStorePurgeOperations
accountingStoreRecordsPurged
accounting StoreLastPurgeStart
accountingStoreLastPureFinish
interceptSummaryWhatever

Removed MIB Objects for Release 3.6.0

MIB name
httpConnectionTable
kernelSummaryNumCmdPending
kernelSummaryNumberRulesInGarbage

Renamed MIB objects in Release 3.6.0

Old object name	New name
lcrActionStatus group	**routeServerActionStatus group**
lcrCarriersTable	**routeServerCarriersTable**
sipLcrLookupTable	**sipRouteServerLookupTable**

Obsolete Objects for Release 3.6.0

Object name
locationPatternTable
servicesRoutingMetricsTable
gatewayLoadMirrorTable
trunkLoadMirrorTable
accountingFilesSubdirectoryCount
accountingStatusTable
clusterServerLoadTable
clusterServerLoadDetailTable
virusScanTable
cnxInterfacesTable

New MIB tables in Release 3.6.0

MIB table name	Description
accountingTargetsTable	Destination targets for accounting CDRs.
accountingTargetsFileSystemTable	Information on file system accounting targets for CDRs.
httpClientsTable	HTTP connection status.
arenaCacheByAllocatorTable	Arena cache statistics by allocator address.
arenaCacheUsageByAllocatorTable	Arena cache usage distribution by allocator address.
arenaCacheUsageOutstandingTable	Arena cache usage distribution for outstanding arenas.
autonomousTableSummaryTable	Autonomous IP route table summary info by tag.
availableMemoryTable	Basic measure of available memory.
callingGroupQosTable	SIP Calling Group Quality of Service Statistics.
callingGroupRedirectTable	SIP Calling Group 302 Redirect Call Statistics.
functionCallersTable	Function callers.
gatewayAdjacencyTable	Gateway adjacency status.

MIB table name (continued)	Description
gatewayRoutingTable	Gateway routing status.
interceptSentinelsTable	Current intercept sentinel status.
interceptSessionsTable	Information about RTP data on intercepted sessions.
mediaPortsSessionsTable	Addresses used by media stream sessions.
mediaScannerIntervalTable	Media Scanner Interval.
mediaScannerSummaryTable	Media Scanner Summary.
mediaStreamHairpinTable	Addresses in use by hairpinned media stream.
messagingReferencesTable	Messaging session reference status.
serverLoadDbTable	SIP Server Load Status.
servicesRoutingConfigTable	Services routing config status.
servicesRoutingLoadShareTable	Services routing table load share status.
sipServerQosTable	SIP Server Quality of Service Statistics.
sipServerRacTable	SIP Server Registration Admission Control Statistics.
switchQosTable	SIP Voice Gateway Quality of Service Statistics.
switchRacTable	SIP Voice Gateway Registration Admission Control Statistics.
trunkQosTable	SIP Trunk Group Quality of Service Statistics.
trunkRacTable	SIP Trunk Group Registration Admission Control Statistics.
serverLoadExternalStatsTable	SIP server statistics used in calculating server load.
sipServerRedirectTable	SIP Server 302 Redirect Calls Statistics.
switchRedirectTable	SIP Voice Gateway 302 Redirect Calls Statistics.
trunkRedirectTable	SIP Trunk Group 302 Redirect Calls Statistics.

Revised MIB tables in Release 3.6.0

MIB table name	Description of change
autonomousIpGatewayTable	ADDED: autonomousIpGatewayRoutingTag, autonomousIpGatewaySubnetAddress, autonomousIpGatewaySubnetMask, autonomousIpGatewayGroupCount REMOVED: autonomousIpGatewayAddressPool, autonomousIpGatewayClassId, autonomousIpGatewayObjectId
autonomousIpGroupTable	ADDED: autonomousIpGroupRoutingTag, autonomousIpGroupSubnetAddress, autonomousIpGroupSubnetMask, autonomousIpGroupHits REMOVED: autonomousIpGroupGateway, autonomousIpGroupClassId, autonomousIpGroupObjectId, autonomousIpGroupGrpIndex
autonomousIpRouteTable	Fields added and removed.
autonomousPrivateGroupTable	Fields added and removed.
autonomousPrivateRouteTable	Fields added and removed.

MIB table name (continued)	Description of change
callingGroupCacTable	Added: callingGroupCacCurrentLocal, callingGroupCacCurrentCluster, callingGroupCacCurrentMax, callingGroupCacCurrentMax, callingGroupCacSetupCluster, callingGroupCacSetupMax OBSOLETE: callingGroupCacMaxBandwidth, callingGroupCacMaxBandwidth, callingGroupCacMaxNumberOfConcurrentCalls, callingGroupCacConnectedCalls, callingGroupCacMaxCallsInSetup, callingGroupCacCallsInSetup, callingGroupCacCallRateLimitingState, callingGroupCacCallRateLimitingRate, callingGroupCacCallRateLimitingInterval, callingGroup CacMaxNumberOfRegistrations, callingGroupCacRegisteredAors, callingGroupMaxRegistrationInProgress, callingGroupCacRegistrationsInProgress, callingGroupCacClusterUsedBandwidth, callingGroupCacClusterConnectedCalls, callingGroupCacClusterCallsInSetup, callingGroupCacClusterWcaNextPercentage, callingGroupCacClusterWcaNextPercentageCalls, callingGroupCacClusterRegisteredAors, callingGroupoCacClusterRegistrationsInProgress, callingGroupCacCLusterRegistrationPercentage, callingGroupCacClusterNextPercentageRegistrations
switchCacTable	Objects added and removed
kernelInstanceTable	ADDED: kernelInstanceAcceleratorRulesDeleteFailed
mediaStreamAddressesTable	Added: mediaStreamAddressesAnchorState OBSOLETE: mediaStreamAddressesAnchored
mediaStreamRtpStatsTable	ADDED: mediaStreamRtpStatsAnchorState OBSOLETE: mediaStreamRtpStatsAvgLatency, mediaStreamRtpStatsMinLatency, mediaStreamRtpStatsMaxLatency, mediaStreamRtpStatsMinTTL, mediaStreamRtpStatsMaxTTL
mediaStreamSrtpTable	ADDED: mediaStreamSRTPAnchorState
mediaStreamStatsTable	ADDED: mediaStreamStatsAnchorState
sipServerCacTable	Objects added and removed
trunkCacTable	Objects added and removed

MIB table name (continued)	Description of change
sipSummaryByBoxTable	ADDED: sipSummaryRatesByBoxCallIDurationMax
sipSummaryRatesByBoxTable	ADDED: sipSummaryRatesByBoxCallDurationMax, sipSummaryRatesByBoxCallDuration replaced by sipSummaryRatesByBoxCallDurationAVG
kernelRuleDetailTable	ADDED: kernelRuleDetailId, kernelRuleDetailSessionID
mediaStreamDtmfTable	ADDED: mediaStreamDtmfAnchorState
rtcpGenerateSessionsTable	rtcpGenerateSessionsReportsSent replaced with rtcpGenerateSessionsGenerated OBSOLETE: rtcpGenerateSessionsType
rtcpGenerateStatsTable	rtcpGenerateStatsReportsSent replaced by rtcpGenerateStatsGenerated OBSOLETE: rtcpGenerateStatsType
callNormalizationTable	ADDED: callNormalizationIsExternal, callNormalizationVirtualDialPlan
callRoutingTable	ADDED: callRoutingIsExternal, callRoutingVirtualDialPlan
mediaPortsHeldTable	ADDED: mediaPortsHeldInterface
mediaPortsProcessUnitsTable	ADDED: mediaPortsProcessUnitsPresent
mediaPortsSummaryTable	ADDED: mediaPortsSummaryInterface
rtcpGenerateReceiverTable	ADDED: rtcpGenerateReceiverTime
rtcpGenerateSenderTable	ADDED: rtcpGenerateSenderTime
serverConnLookupTable	ADDED: serverConnLookupLocalIp, serverConnLookupRoutingTag
serverHostLookupTable	ADDED: serverHostLookupLocalIp, serverHostLookupRoutingTag
serverNameLookupTable	ADDED: serverNameLookupLocalIp, serverNameLookupRoutingTag
servicesBoxDatabaseTable	ADDED: servicesBoxDatabaseMediaMetricMax, servicesBoxDatabaseMediaMetricCurrent
accountingDatabaseTable	ADDED: accountingDatabaseState, accountingDatabaseMissingRecords
activeCallsTable	Added: actyiveCallsConnectyed, activeCallsScanTime, activeCallsFileTime, activeCallsPlayTime, activeCallsDisconnectReason

MIB table name (continued)	Description of change
carrierRoutingTable	RENAMED: carrierRoutingMatch to CarrierRoutingToMatch; carrierRoutingMin to carrierRoutingMinPrefixDigits OBSOLETE: carrierRoutingRoutingTag, carrierRoutingtype, carrierRoutingPrefixPattern, carrierRoutingTime, carrierRoutingTimeRecordId, carrierRoutingAction, carrierRoutingFwd, carrierRoutingSetting
dialPlanTable	ADDED: dialPlanIsExternal, dialPlanVirtualDialPlan
lcrRoutingTable	ADDED: lcrRoutingTableToMatch, lcrRoutingTableMinPrefixDigits OBSOLETE: lcrRoutingTableRoutingTag, lcrRoutingTableType, lcrRoutingTablePrefixPattern, lcrRoutingTableTime, lcrRoutingTableTimeRecordId, lcrRoutingTableAction, lcrRoutingTableFwd, lcrRoutingTableSetting
fileTransferSummaryTable	OBSOLETE: fileTransferSummaryVirusChecked
kernelRuleTable	ADDED: kernelRuleSessionID
kernelRuleAnchorTable	ADDED: kernelRuleAnchorSessionID
kernelRuleRouteTable	ADDED: kernelRuleRouteSessionID
kernelRuleStatsTable	ADDED: kernelRuleStatsSessionID
registrationArbitrationTable	ADDED: registrationArbitrationIsExternal, registrationArbitrationVirtualDialPlan
registrationNormalizationTable	ADDED: registrationNormalizationIsExternal, registrationNormalizationVirtualDialPlan
registrationPlanEntry	ADDED: registrationPlanIsExternal, registrationPlanVirtualDialPlan
registrationProxyTable	ADDED: registrationProxyIsExternal, registrationProxyVirtualDialPlan
registrationProxyRoutingTable	ADDED: registrationProxyRoutingIsExternal, registrationProxyRoutingVirtualDialPlan
registrationRoutingTable	ADDED: registrationRoutingIsExternal, registrationRoutingVirtualDialPlan
routingArbitrationTable	ADDED: routingArbitrationIsExternal, routingArbitrationVirtualDialPlan
servicesInterfaceDatabaseTable	ADDED: servicesInterfaceDatabaseH323
servicesRouteDatabaseTable	ADDED: servicesRouteDatabaseH323
signalingSessionsTable	Objects added and removed

MIB table name (continued)	Description of change
h323ExternalGatekeepersTable	ADDED: h323ExternalGatekeepersObjectID‘
mediaStreamServerSessionsTable	ADDED: mediaStreamServerSessionsAnchorState
productModel	Changed from integer to OCTET STRING
systemInfoModel	Changed from integer to OCTET STRING

New SNMP trap entries in MIB for Release 3.6.0

Trap name	Description
h323CallPortRelease	An H.323 port has been released.
playFailed	Media has failed to be played out onto a leg.
playInitiated	Media has begun to be played out onto a leg.

Revised SNMP trap entries in MIB for Release 3.6.0

Trap name	Description
playComplete	New fields added to trap.
h323CallQ931TunneledMsg	New fields added to trap.

Obsolete SNMP Trap Entries for Release 3.6.0

Trap name
fileTransferAntiVirusFail

Known problems, restrictions, and operational considerations in 3.6

The following section describes the known problems, restrictions, and operational considerations in Release 3.6.

- Issuing the **vsp-reset** command now requires a user confirmation to execute the command successfully.
- In releases previous to 3.5.5, setting the **sticky-via** configuration property modified the VIAs of all messages sent to the next-hop server. Now the NN2600 does not modify response messages going back to the server.

- In releases previous to 3.5.5, the Master Service Up event log message was not given the same severity as the Master Service Down event. Now these are both set to the “alert” severity.
- When using media-shuffle, media anchoring must be enabled to work properly. (ID 14490)

RADIUS attributes, CDRs and RADIUS servers

The following table lists the vendor-specific attributes (VSAs) that Acme Packet writes to RADIUS packets, type Cisco, in Release 3.6..

VSA number (vendor)	Attribute Name	Description
1 (Cisco)	SESSION_PROTOCOL	
1 (Cisco)	CALL_ID	
1 (Cisco)	INCOMING_REQ_URI	
1 (Cisco)	OUTGOING_REQ_URI	
1 (Cisco)	NEXT_HOP_DN	
1 (Cisco)	NEXT_HOP_IP	
1 (Cisco)	PREV_HOP_IP	
1 (Cisco)	DISCONNECT_CAUSE	
1 (Cisco)	PREV_HOP_VIA	
1 (NN2600)	**CXC-Permissions**	The full name of the configuration permissions object for NN2600 users. **Format:** "access permissions admin"
2 (NN2600)	**CXC-SIP-Address**	The SIP address of the user. **Format:** name@companyABC.com
3 (NN2600)	**CXC-Object**	Used when RADIUS is a policy server to return policies and configuration information.
4 (NN2600)	**CXC-Sess-Attr**	Used when RADIUS is a policy server to return policies and configuration information.
5 (NN2600)	**CXC-Version**	The build number associated with the software release.

VSA number (vendor)	Attribute Name	Description
25 (Cisco)	H323_SETUP_TIME	
26 (Cisco)	H323_CALL_ORIGIN	
28 (Cisco)	H323_CONNECT_TIME	
28 (Cisco)	H323_DISCONNECT_TIME	
30 (RADIUS)	CALLING_STATION_ID	
31 (RADIUS)	CALLED_STATION_ID	
200 (NN2600)	**SESSION_ID**	The session identifier assigned by NN2600 on a call session when authenticating a SIP INVITE message.
201 (NN2600)	**RECORDED**	For RADIUS accounting record: TRUE or FALSE.
21798 (Vendor)	**Acme Packet**	The NN2600 globally-assigned RADIUS vendor attribute.

When sending CDRs to an external RADIUS server, ensure that you have configured the **radius-group/call-field-filter** so that the essential records are forwarded to that server. Additionally, the external RADIUS server must have attributes to extract critical records from the CDR, such as the calling party number information for billing purposes. These configured attributes are generally set up in a “dictionary” for that server, but dictionaries are specific to RADIUS vendors.

NN2600 RADIUS VSAs are defined in the directory **/cxc/web/dictionary.covergence**.

Problems, restrictions, and considerations from prior releases

Upgrading to Release 3.6.0

- Currently, cluster and controlled upgrades from any release prior to Release 3.6.0 are not supported. Perform the upgrade procedure on each individual box in the cluster. (ID 15131)

- If you are currently running a release prior to 3.3.8, 3.4.2, or 3.5.1, you will need to perform the upgrade to Release 3.6.0 from a USB stick. Refer to the *Net-Net 2600 – USB Creation and Commissioning Instructions* for information on creating the USB stick and commissioning the NN2600 device.
- If you are currently running Release 3.3.8, 3.4.2, 3.5.1, or later you can perform the upgrade to Release 3.6.0 using the procedure covered in the section, "RADIUS attributes, CDRs and RADIUS servers" using the Release 3.6 tar file, or you can perform the upgrade from a USB stick. This means that you can choose either procedure, however, Acme Packet recommends that you apply the upgrade from the USB stick for better compatibility with future upgrades.
- If the NN2600 device had data drives mounted on the original version of software, these data drives will no longer be mounted after the upgrade to Release 3.6. Run the **add-device** action to restore the data drives to operate with the new software by specifying the *data-1* or *data-2* drive position and the relevant file system.
- When upgrading a NN2620 from a USB stick, the configuration, license, certificates and other components are preserved. However, any data on the RAID-10 data-1 drive is not preserved during this operation as the RAID array is always re-configured, with its data erased. If you require the contents of the RAID-10 data-1 drive, perform the upgrade to 3.6.0 using the procedure, "RADIUS attributes, CDRs and RADIUS servers."

  This does not affect any other platform, including 3rd-party platforms with RAID configured. (ID 14736)

USB stick restrictions

If you are upgrading an existing NN2600 device from a USB stick, check the /cxc directory for .cfg and .xml files that are larger than 2 MB. Files that are larger than 2 MB will not be backed up to the USB stick and restored during the upgrade process.

All *.cfg and *.xml files in the current working directory (/cxc) less than 2 MB in size are backed up to the stick and restored during the upgrade. (ID 13207)

It is important to remember to remove the USB stick once an upgrade is completed in order to maintain the correct modified configuration. (ID 15640)

Virtual interfaces per physical Ethernet

Each physical Ethernet interface supports up to 14 virtual (VX) interfaces.

IP interfaces per physical NN2600 device

Release 3.5 supports a maximum of 4096 named IP interfaces per NN2600 device.

CDR values on external databases

When sending accounting CDRs to external databases, values that are unsigned 32-bit integers are stored as signed 32 bit integers in the database record. If the value of the field is larger than 2147483647 and retrieved as an integer, the value is stored as a negative number.

To decode the negative number, add 2^{32} or 4294967296 to the value.

The following columns are affected:

- Duration
- PacketsReceivedOnSrcLeg
- PacketsLostOnSrcLeg
- PacketsDiscardedOnSrcLeg
- PdvOnSrcLeg
- MaxJitterOnSrcLeg
- LatencyOnSrcLeg
- MaxLatencyOnSrcLeg
- PacketsReceivedOnDestLeg
- PacketsLostOnDestLeg
- PacketsDiscardedOnDestLeg
- PdvOnDestLeg
- MaxJitterOnDestLeg
- LatencyOnDestLeg

- MaxLatencyOnDestLeg
- Rx1000FactorOnDestLeg
- Rx1000FactorOnSrcLeg
- huntingAttempts
- callPDD

(ID 15898)

Modifying the timezone

When the timezone property is modified in the Box configuration several Java processes must be manually restarted on that NN2600 to pickup the modification. The java processes that need to be restarted are:

- Web
- DIR
- WS
- Acct
- Presence
- Eventpush
- DOS

(ID 15640)

Using the configuration import utility

The import and conversion utility that allows you to move the configuration file (*cxc.cfg* by default) to other NN2600 devices. This solves problems associated with managing MAC addresses from one system to another anytime the configuration file is transferred. The import utility uses the XML transform program to run the conversion.

Perform the following steps:

1. Save the current configuration to XML format to a USB stick. The new file is named *template.xml*.

```
NNOS-E>> config save xml /mnt/usb/template.xml
```

2. Insert the USB stick into the USB port on the NN2600 master system to which the template.xml file is imported.
3. Run the XML transform program to import the **template.xml** file.

```
NNOS-E>> xml transform cfg-import.xsl /mnt/usb/template.xml new.xml
“box1=11:11:11:11:11:11 box2=22:22:22:22:22:22
box3=33:33:33:33:33:33 box4=44:44:44:44:44:44”
Success
```

   where *cfg-import.xsl* is the name of the style sheet included with NN2600, *template.xml* is the name of the original *cxc.cfg* file (saved as XML), and *new.xml* is the resulting name of the new configuration file that you just imported to NN2600. Included in quotation marks (“) is the list of MAC addresses to which the new configuration file is imported.

4. At the master NN2600 device receiving the new configuration file, replace the running the configuration file with the *new.xml* file. If the new configuration is operating as expected, execute **config save**. The four devices in cluster will automatically receive the new configuration file.

```
NNOS-E>> config replace new.xml
NNOS-E>> config save
```

Installing the Cisco JTAPI jar file

This is needed only for customers who are using the external presence JTAPI communication feature on a NN2600 device interoperating with the Cisco CallManager.

Perform the following steps to install the Cisco JTAPI software.

1. Log in to the computer where you want to install the Cisco JTAPI client software.
2. Close all Windows programs.
3. Open a Web browser.
4. Go to the Cisco CallManager administration windows at:

   http://*name*/CCMAdmin/main.asp

   where:

   name specifies the name or IP address of the Cisco CallManager.

Note: If the above web address does not access the Cisco CallManager administration window properly, try using the following:

http://<call manager>/plugins/jtapi.jar

5. Choose **Application->Install Plugins**.
6. Choose the **Cisco JTAPI** link.
7. Save the file on your desktop and follow the instructions in the pop-up windows.

Note: Install Cisco JTAPI software on the default drive as directed by the installation software. When Windows NT is installed in C:\WINNT, the default directory, for example, is C:\WINNT\Java\lib.

At the platform or blade running NN2600, perform the following steps:

8. Copy the *jtapi.jar* from the **Windows\Java\lib** directory to **/cxc_common/jtapi** and rename the files to the following:
   - Cisco 4 CallManager **jtapi jar** to **jtapi-cisco-2.1.jar**
   - Cisco 5 Call Manager **jtapi.jar** to **jtapi-cisco-3.0.jar**
   - Cisco 6 Call Manager **jtapi.jar** to **jtapi-cisco-4.0.jar**
9. Restart the presence process by performing a **restart warm**.

Routing to location cache when destination server is “down”

In Release 3.5.3, calls are no longer routed to the location-cache if the destination server is detected as “down” during failover-detection. If there is a matching dial-plan, NN2600 will now return a SIP 503 (Service Unavailable) message rather than route the call through the location-cache and returning a SIP 404 message.

Previously, when all the servers on a route were down, the route was removed from the active routing table, causing failure of the dial-plan match and returning a SIP 404.

Virus scanning

All virus scanning functionality (to include McAfee and icap-server) has been removed and is no longer supported in NN2600.

NN2600 Virtual Machine limitations

- Transcoding is not supported on the VM.
- Feature options that require fine-grained timing such as music-on-hold and announcements may not work properly in the virtual environment. This is due to virtual OS timing issues that are beyond the control of the Acme Packet software. If you plan on using these features as part of your application, please contact your Acme Packet sales representative for further information.

Accounting reset

When directing accounting records to an external database target, you will need to execute the **accounting reset** action if you edit the database secret password after NN2600 has started forwarding records to this database. Otherwise, NN2600 will not be able to contact the external database.

The external database password is configured under the **vsp accounting database group server** object using the **password-tag** property. (ID 15403)

Combination of ringback-file and call introduction

Currently, if a ringback file and a call introduction are configured simultaneously, the call introduction is played immediately, followed by the ringback file. As a result, the call recipient never hears the introduction, and the call originator hears the introduction before the ringback file is played.

When operating correctly, the call introduction is played after the call is connected so that both the caller and the call recipient hear it. (ID 13282)

Web service pushlets over HTTPS

Currently, Web service pushlets and external event service applications with a self-signed certificate will not operate over HTTPS connections. (ID 13421, 14394)

Cisco CallManager interoperability — automatic call forwarding

When Cisco CallManager (CCM) over H.323 is handling an automatic call forward with **inbound faststart** on the CCM disabled, NN2600 sends a CCM non-responding **termCap** when handling remote ringback.

For automatic call forwarding to work properly, ensure that CCM **inbound faststart** is enabled. (ID 13748)

Inleg and outleg TOS values

When editing the session configuration **sip-settings\inleg-tos** and **outleg-tos** overwrite value settings, specify a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 00011010, and 104 for 01101000. The default setting for both of these properties is 0. (ID 14110)

Google Gadgets and NN2600 Management System browser windows

When running the NN2600 Management System and iGoogle (with Gadgets) simultaneously, make sure that you are run the NN2600 Management System and iGoogle in separate browser windows. (ID 14450, 14451)

Accounting

- Currently, when directing CDRs to a RADIUS target, call field filtering (as configured with the vsp\radius-group**call-field-filter** object) does not work. By default, all fields are sent to the RADIUS target. (ID 14893)
- With the vsp\accounting\file-system\path **roll-over** property set to *daily*, the NN2600 software currently creates a new accounting file each time the system is restarted, resulting in multiple accounting targets per day. All files are sent to the target, so the target receives all CDRs meant for it. (ID 14568)
- If you disable an accounting target that is referenced by an accounting policy in any session configuration and then re-enable the target, accounting will not send the records that accumulated while the accounting target was disabled. (ID 15044)
- For CDRs to be properly sent to an external MS SQL database server, the **box\hostname** property must be specified using an IP address or fully qualified domain name (FQDN). If a partial hostname is specified, then the domain name must be qualified using the **vsp\static-stack-settings**. (ID 13292)

- Currently, the **accounting purge** action is operating slowly, causing call records to consume large amounts of disk space. Acme Packet recommends that you set up a second disk for accounting records and set the **accounting-root-directory** (under services\data-locations) to that new drive and directory location. Additionally, set the vsp\accounting **retention-period** to 1 (one day) to ensure frequent purging.

  To enable a second drive, perform the following steps:

  1. Unmount, format, and mount the new target drive, such as *data-1*.

```
NNOS-E>> umount data-1
Success !
NNOS-E>> format data-1 reiser-3
Are you sure (y or n)? y
Success!
NNOS-E>> mount data-1
Device is mounted.

NNOS-E>> show mounts (to display the data-1 drive in the list)
```

  2. Under services\data-locations, set the **accounting-root-directory** property to the new target drive and directory.

```
config data-locations> set accounting-root-directory /cxc_common
  data-1/accounting
```

  3. Set the vsp\accounting **retention-period property** to 1 (one day) to ensure frequent purging of accounting records and free disk space.

  (ID 14905)

Generic JDBC driver

If you are sending CDRs to an external MySQL database server group, (where type is generic), you will need to download and copy the MySQL driver to the NN2600 **/cxc/lib/jdbc** directory to properly connect to the MySQL database.

The MySQL 5.1 download is available from the following link.

http://dev.mysql.com/downloads/mysql/5.1.html

- mysql-connector-java-5.1.7-bin.jar

After copying the driver over to the NN2600 device, restart the accounting process by issuing a **restart warm**.

At the MySQL database server (Windows XP, NT, Linux), you will need to open port 3306 to allow client access, as follows:

1. **Start->Control Panel->Windows Firewall**.
2. Select **Exceptions** and **Add Port**
3. Add the port name *mysql_port* and port number *3306.*

Note: Follow this procedure for any JDBC driver used with accounting generic database target type.

Removing and adding network interface (NIC) cards

Whenever an Ethernet network interface is removed and reinstalled on an NN2620 you need to perform either the **install nic** or the **install nic-reinitialize** action to reassign Ethernet port numbering. Not doing so could result in a system deadlock.

- **install-nic** — Adds a NIC card to a system that was previously running. Interfaces on the new card are assigned “next” available Ethernet interface numbers.
- **nic-reinitialize** — Removes all the existing NIC interface assignments and rebuilds the interfaces in order. For NN2600 hardware, the order (when looking at the back of the unit) is right-to-left, top-to-bottom. For all other hardware, the order is based on how the PCI buses are scanned.

  When upgrading or replacing a NIC card with the same number of ports, either **install-nic** or **nic-reinitialize** action may be used. (ID 14333)

H.323 call details in the call logs

To view H.323 call details from the NN2600 Management System Call Logs, select **Sessions,** then select **View->Other** at the right side of the page. Currently, the **H323 Messages** function does not work. (ID 14852)

H.323 operational issues

Currently, unanchored calls over H.323 networks (most deployments) will result in remote ringback, call hold and release, call transfer, and music-on-hold (MOH) failures. (ID 14490, 14519, 14523, 14927, 14977)

CUCM-SIP and ACM-SIP interoperability — calls on hold

With interoperating SIP environments involving Cisco Unified Communications Manager (CUCM) and Avaya Call Manager (ACM), set the session configuration third-party-call-control **reinvite-delayed-offer-wait-on-ack** setting to *enabled* and the session configuration **in-hold-translation** and **out-hold-translation** offer and answer attributes to *sendrecv*. Otherwise, inconsistent re-INVITE behaviors will result when calls are placed on hold in these environments. (ID 15091)

Multiple VLANs on VRRP networks

If you configure multiple VLANs on a VRRP network, and if you have a VLAN configured on that physical interface, you will need to create corresponding ("phantom") VRRP VLANs on the Ethernet physical interface to enable traffic to reach the VRRP network. However, if the Ethernet interface does not have a VLAN configured, then there is no need to configure the corresponding "phantom" VRRP VLANs. (ID 12378)

NN2600 Management System — Configuration change indication

When exiting the NN2600 Management System, the software does not currently post a configuration change indication if additions and edits were applied with a **Set** or **OK** selection during the active session. Proceed to save or cancel the configuration, as desired. (ID 3920)

Proxy re-registration of SNOM phones

In a proxy registration configuration involving Broadworks and SNOM phones, the first re-register of the phone allows the unregister/register requests to be handled in the correct order. On a second re-register of the phone, the register requests are handled out of order, forcing the phone into the "in-service" state. A third re-register of the phone returns it to the registered state.

DNS and ENUM

The following notes summarize operational issues with the DNS and ENUM functionality.

- The **vsp/enum/resolver** and **vsp/enum/mapping** objects have been removed from the configuration. Both DNS and ENUM servers are now configured using the **vsp/dns/resolver/server** object using the server IP address and the **type** property (dns-only, enum-only, or both).
- The **vsp/dns/resolver/server** entries no longer have the **sip-location** setting. This setting is now a per-session setting that applies to **routing-last-resort-dns** and is configured in **session-config/dns-client-settings**.
- The new **vsp/dns/enum-mapping** requires a domain-name to be specified, replacing the previous **vsp/enum/mapping** object. An upgrade puts e164.arpa as the domain-name.
- An **enum-domain** can not be referenced per server in **vsp/dns/resolver/server**. Use the **vsp/dial-plan/normalization/condition-list/enum-server** configuration. (ID 12881)

Archiving

In Release 3.5, an accounting target of the local database must be configured in order for archiving to work. (ID 12883)

Directory and master services

If the directory Service is configured and enabled in a cluster environment, the directory service and master database must be configured on the same system before upgrade installation.

Directory service and master system database must be configured and co-exist in the same box. In 3.5, the directory service communicates with the master system database and instructs master system database to load users data from the local file system where the directory service is running. If the Directory service and the master system database do not co-exist on the same device, the master system database will no be able to load files generated by the directory service.

Additionally, directory services database tables are not populated to the backup device. In a cluster, NN2600 does not support directory services failing over to the backup box. This is because user ID numbers get regenerated and may not match IDs stored in the database for past traffic. (ID 13203)

Monitor-groups

Currently, the **vsp/monitor-group** and the **media/monitor** *monitor-group* reference are not currently operational. In the NN2600 Management System, this affects the **Call-out** function found under Call Logs/Sessions, User Sessions, and Accounting, and when selecting the **Set up playback** template from Call Logs/User Sessions. (ID 13425)

Siemens Fujitsu RX100 and RX300 servers

When running NN2600 on Siemens Fujitsu RX100 and RX300 servers, the onboard Ethernet ports (two) on these servers not currently supported in Release 3.6. (ID 13294)

Media verification issue

When using media-verification, if call endpoints do not agree upon a packet interval (ptime), the media-verification may end up dropping RTP packets as outside the range for that CODEC/packet interval. (ID 12381)

Inleg and outleg TOS values

When editing the session configuration **sip-settings\inleg-tos** and **outleg-tos** overwrite value settings, specify a number that represents the 8-bit Differentiated Services (DS) field of the IP packet in decimal format, such as 26 for 011010, and 104 for 01101000. The default setting for both of these properties is 0. (ID 14110)

Call monitoring and transcoding — no audio

Currently, there is no audio heard between call endpoints if both transcoding and attendant call monitoring are configured in combination. This problem will be addressed in a later release. (ID 12387)

Policy Manager running over WebSphere

When running Policy Manager over WebSphere, note the following:

- An HTTP 500-Internal Server error will occur when retrieving any status using Call Manager and the Status application. This problem only occurs if there are no users and permissions configured under the **access** object. Be sure to configure NN2600 user names and passwords for the required Web services authentication as described in the manual, *Net-Net 2600 – Using the NN2600 Management Tools*. (ID 11114)
- Ensure that the proper web-service credentials are provided when making web service requests to the NN2600 domain. Otherwise, NN2600 will return an HTTP 401 (Unauthorized) response, causing the WebSphere Policy Manager application to hang. (ID 11619)

Third party call control (3PCC) call transfers

During third party call control (3PCC) sessions involving a Cisco Call Manager server, a call transfer involving multiple recipients will result in a new call control window at first call transfer recipient. Normally, the original call control window should remain active without a refresh. (ID 11298)

SIP server pools

Currently, the **show sip-server-pool** command does not display the number of out packets; a 0 count is reported. (ID 11504)

Virtual Machine uptime reporting

Currently, if you shut down and then restart the NN2600 Virtual Machine on the same device, executing the **show system-info** command will report the new VM with an incorrect uptime. The command shows the uptime starting with the statistic associated with previous VM instead of beginning at zero uptime. (ID 11396)

Attendant call monitoring

- With anchoring, recording, and call monitoring enabled, NN2600 records the call for the call participants (caller A to caller B), but does not record the call session with the third-party attendant (C). Although the call log shows a separate entry for the INVITE from A to C, the Play field is greyed out, indicating no recording. (ID 9542)

- Currently, an intermittent SIP trace error has been observed with locally-registered phones when the call attendant endpoint picks up while the dialed phone is still ringing. (ID 10989)

QoS call duration statistics

Currently, QoS average call duration and post dial delay statistics for endpoints are not being reported (displaying 0 with the **show switch-pool -v** command). (ID 11549)

H.323 — SIP directive

The session configuration **sip-directive/directive refuse** setting is not currently applied in H.323 to SIP sessions. (ID 11925)

Unmatched sessions returned when searching by Date/To/From

When searching the NN2600 Management System **Call Logs->Sessions** using the Date/To/From criteria, a partial fromURI field is shown in the display, causing the matched sessions to appear “unmatched” in the search results. (ID 11868)

Call field filtering on jitter and media CDR fields

To properly display jitter and media CDR fields that are added with the **vsp\accounting\database\group\call-field-filter** object, select PDV on the call-field-filter to display the jitter fields, and select RFACTOR under media fields to display the rfactor fields. (ID 11866)

No audio available to call monitors

Currently, audio is not being sent to SIP phone third-party endpoints configured in the VSP **monitor-group**. (ID 11951)

Microsoft LCS to IBM Sametime

NN2600 users federating IBM Sametime and Microsoft LCS may experience issues with federated presence when moving to 3.4.1 and using their previous configuration. Specifically, **sip-settings** can no longer be used to configure the transport for federated traffic. The **request-uri-specification** should be used instead. (ID 11950)

Admission control behavior changes

To address call admission control behaviors, the following admission control settings are now *disabled* by default:

- **registration-admission-control** — If enabled, the controls set with the pending registration high- and low-watermarks are applicable. This admission control suppresses new registrations to allow resolving registrations in progress, preventing “rate of registration” attacks.
- **call-admission-control** — If enabled, allows call admission control (CAC) on NN2600. The following settings are only applicable if **call-admission-control** is enabled:
  - **cac-max-calls**
  - **cac-max-calls-in-setup**
  - **cac-min-calls-in-setup**
  - **cac-max-number-of-tls**
  - **cac-max-tls-in-setup**
  - **calls-cpu-limit**
  - **call-response-code-at-threshold**
  - **call-response-string-at-threshold**

  When disabled, only the **static-stack-settings max-number-of-sessions** property controls setup and connection limits.

The following threshold settings have also been modified:

- **registrations-high-cpu-threshold** — Default is 90%. Sets an upper threshold, as a percentage, for registration processing average CPU usage. The registration dynamic threshold is calculated based on the admission-control/ **pending-registrations-high-watermark** property. When the average CPU usage exceeds this high threshold, NN2600 decrements the dynamic threshold by 10% until it reaches the value set with the **pending-registrations-low-watermark** property.
- **registrations-low-cpu-threshold** — Default is 70%. Sets the low-end threshold, as a percentage, for registration processing average CPU usage based on the registration dynamic threshold. When the SIP process CPU falls to the low threshold, NN2600 increments the threshold by 16% if the average CPU is less than the low threshold and by 4% if less than the high watermark.

Audio viewer — Audio loss during playback

The Archive Viewer may loose audio or video during playback if the RTP stream switches to a CODEC not supported by the Archive Viewer. (ID 9256)

location-cache changes not taking effect

If you edit the **location-call-admission-control** settings in the session configuration, the changes do not take effect after updating and saving the configuration. Any **location-call-admission-control** changes in the session configuration will require a **location-database flush** action for the new settings to take effect. (ID 10801)

apply-to-methods settings

For REGISTER-based sessions and existing registered endpoints, if you edit the **apply-to-method** setting in the session configuration, the change does not take effect after updating and saving the configuration. Any **apply-to-method** change in the session configuration will require a **location-database flush** action for the new setting to take effect. (ID 11149)

H.323 protocol

High availability support (call failover) is not supported. (ID 10966)

Identical SSH host keys

In order to secure access through SSH, Acme Packet recommends that you periodically run the new **ssh-regenerate** action to create unique SSH host keys on each platform running NN2600 software. The action will initiate a cold restart of the system.

New software installations from USB sticks will automatically generate new and unique SSH host keys at installation time.

After running the **ssh-regenerate** action, some SSH clients may experience a problem when making a secure connection to the system.

Over Putty:

The SSH client will display a pop-up window with the message "WARNING - POTENTIAL SECURITY BREACH!" and explain that the server's host key does not match. Since the host key was changed, the correct action is to click **Yes** to begin the Putty session.

Over Linux-based SSH:

The SSH client will display the following banner followed by a series of messages:

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

To correct this problem, review the series of messages and edit the file specified in the "Offending key in" line at the line number indicated. You can delete this line and then save the file. When the SSH client is run again, the new host key will be added to the known hosts file. (ID 10909)

Large configurations with 4K VLANs or more

When running large configurations containing 4000 VLANs or more, NN2600 may take several minutes to load at a system **restart,** or from other operations involving the configuration file, such as a **config replace.** Use the **cpu-monitor** action to observe CPU usage during configuration loading or any time while NN2600 is running. When the CPU usages falls below 10%, the configuration has successfully loaded. (ID 10050)

Call recording and file mirroring limits

When performing call recording and file mirroring, the system now caps the number of files at 50,000 to prevent an excessive number of stored records and overconsumption of system and memory resources. You should configure periodic maintenance (**services/tasks**) to remove old records at regular and scheduled intervals. Optionally, Acme Packet provides a software license that will allow you to increase the call recording and file mirroring capacity to 200,000 files. (ID 10036)

TFTP servers

Configuring a TFTP server on a NN2600 interface over UDP/TFTP port 69 may result in TFTP not working. For information on properly configuring a TFTP server, Acme Packet recommends that you run the WinAgents download from the following Web location.

http://www.winagents.com/en/solutions/tftp-over-firewall.php

(ID 10293)

Calling group address limitation

In vsp/calling-groups/group, the **max-number-of-addresses** property sets the maximum number of AORs that can be associated with a calling group. However, currently only one AOR can be associated with a calling-group.

Licensed features display

When displaying features from the NN2600 Managment System **Services->Features** page, fields that appear in the greyed-out state showing the default values currently being enforced cannot be edited from this page. This includes the “no royalty” CODECs and other licensed features.

The fields that appear greyed-out require the Acme Packet license update that includes the field(s) to be configurable. (ID 10496)

SIP tracing during system load

The NN2600 tracing functions are designed to be used in short duration, isolated troubleshooting conditions. These tools should not be used when the system is under heavy SIP traffic load, and doing so may cause system deadlocks and crashes. This is a tool intended for use only with the assistance of Acme Packet. (ID 9875)

Outbound local port setting

The session configuration **sip-settings/outboundLocalPort** property is not supported with the new tag routing feature in Release 3.3. (ID 8746)

Multiple unique media streams

With some SIP phones, NN2600 (with media anchoring enabled) may return two unique media streams, one disabled, and one accepted. This happens in cases where the SIP phones offer multiple media descriptions for alternate SRTP/clear RTP. (ID 8899)

Alter-contact setting overriding sip-settings/outboundLocalPort

The **registration-plan/route alter-contact** property setting is currently overriding the session configuration **sip-settings/outbound-local-port** setting used for communicating with the peer. The **alter-contact** setting should only select a port if it is set to trunk-port-per-aor or trunk-port-per-binding. (ID 8749)

Local enterprise directory user files

Local user files for XML and CSV directories, as well as introduction and periodic announcement files, should be stored in a folder under the NN2600-recognized directory named **/cxc_common**. If you place local user files in an unknown or unique directory, NN2600 will not be able to locate users after you upgrade the device to the current release. (ID 5578)

SIP sessions

- The SIP transport is currently missing a time-out setting for TLS and TCP connections. A connection is dropped only if the connection is terminated by the remote SIP client or SIP server.
- During the SIP call session, **disconnect-call** and **terminate-call** actions only operate in back-to-back mode and not in proxy mode.
- The condition-list associated with a policy rule is applied to the first SIP call session only.
- Session termination due to a media verification failure will not work when NN2600 is operating in proxy mode. This includes voice and video calls created using Windows Messenger. Calls using Sametime or regular SIP phones are not affected. The **terminate-session** setting in the media verification object (vsp/media-verify-config <name>) contains the configuration setting.

EyeBeam softphone with Rport option turned on

The EyeBeam softphone puts a contact address in the INVITE with a port that is different from where the INVITE is sent. Any requests within the dialog originating from the far end are sent to this contact address. This behavior is correct but the EyeBeam phone is ignoring the request in this case. (ID 8286)

Preventing call routing loops

Forwarding loops can occur when a user agent (UA) registered over NN2600, in delegate or local mode, sends an INVITE to a delegate server, and then that delegate server sends the INVITE back to NN2600 for further routing. In some cases, the INVITE from the delegate server might be destined for a UA that is also registered over NN2600. Administrators should ensure that if an INVITE is destined for the UA, that the INVITE matches an existing dial-plan, with the dial-plan **location-match-preferred** property set appropriately. Depending on your network routing, this tells NN2600 about the order in which it should attempt a match with the **location-cache** rather than with the **dial-plan**.

A routing loop can also occur if NN2600 forwards an INVITE to a delegate server, and that delegate server returns the INVITE to NN2600. In some cases, the inbound INVITE may match the same dial-plan, causing a routing loop where both NN2600 and the delegate server continue to send INVITE sessions to each other for the same destination until the **max-forwards** property setting has expired to 0. This causes NN2600 to allocate several hundred media ports (where NN2600 is anchoring the call), quickly exhausting resources if several UAs are participating in the loop.

NN2600 administrators can reduce the possibility of routing loops by performing the following tasks:

- Enable the **vsp/location-service/admission-control** to prevent an address-of-record (AOR) from placing more than **vsp/location-service/ max-concurrent-calls-per-AOR** setting for simultaneous calls.
- Enable the **vsp/location-service/emission-control** to prevent an AOR from receiving more than **vsp/location-service/max-concurrent-calls-per-AOR** setting for simultaneous calls.

These settings are only active when the **unregistered-sender-directive** is not set to *allow* for the AOR in question. The **unregistered-sender-directive** property must be set to *refuse* in the **vsp/enterprise/servers/sip-gateway** configuration. Setting the **unregistered-sender-directive** in the **pre-session-config** has no effect.

NN2600 returns a “503 Server Unavailable “message to an INVITE if the AOR attempts to place more than the supported number of concurrent calls when these settings are enabled.

Additionally, if NN2600 acts as a back-to-back user agent (B2BUA) between several user agents, routing loops may occur. In this configuration, NN2600 forwards an INVITE to a server, and then that server sends it back to the NN2600 device where NN2600 again forwards the INVITE on to another server. In some cases, this may not be a routing loop but a valid routing configuration. NN2600 administrators can prevent invalid routing loops by editing the **vsp/enterprise/servers/sip-gateway *name*/loop-detection** property.

RADIUS authentication and server priorities

If you set the **vsp/radius-group/authentication-mode** to *prioritized*, be sure to change the **vsp/radius-group/server** *priority* setting on any configured RADIUS group servers. All previously configured servers inherit the default value of 1. Without setting different priority values, NN2600 randomly selects from these servers and ignores the prioritized mode. The system will generate an event indicating that multiple servers have the same priority.

Media transcoding

- When performing transcoding, NN2600 drops RTCP (regardless of the setting of the media **rtcp** property). NN2600 records RTCP according to the session-config/media/**rtcp log** setting, but does not forward it since the transcoding may change the synchronization source (SSRC) of RTP along the way. If RTCP were forwarded, it may cause problems for endpoints because the stream described with RTCP may not match the RTP packets sent and received.
- When NN2600 is transcoding, it changes the SSRC from the original RTP stream. Some phones do not respond well to an SSRC change in the middle of a call. This may occur when a phone changes from a CODEC that is passed through to a CODEC that is transcoded. (ID 7802)

Eyebeam phones

Eyebeam softphones (Version 1.5.10.2 build 33793) do not play music-on hold generated by NN2600. (ID 7799)

Registration plans and registered states

In an LCS environment, a **registration-plan** must be configured to enable the location-cache to report an AOR in a registered state. Without a registration-plan, the AOR state will be declared as unregistered. The registration-plan must have a configured **route** with the **peer**, **action**, and **registration-throttling** settings configured. (For example, peer=LCS-server, action=tunnel, registration-throttling=no). (ID 8162)

CODEC licensing

- If transcoding is configured with CODECs that require licenses and if a call is placed on hold without the available licenses, the call will be terminated. (ID 8206)
- In the NN2600 Management System, some CODECs display a message saying they are "Available with upgrade." In fact, these CODECs are available, but the number of license seats, set at 200,000, is not configurable. This applies to the following CODECs: g728, g726-16, g726

SSH session limit clarification

The SSH object **max-sessions** property sets the maximum number of concurrent SSH sessions allowed, enforced at the box level. The enforced value is an aggregate of the SSH session limits set on each IP interface that has SSH enabled. For example, to enforce a limit of five total SSH sessions per box, you could set IP "A" to an SSH session limit of two and IP "B" to an SSH session limit of three, for a total of five.

Call failover

If you configure the fault-group so that a SIP process crash results in a VRRP failover, if the call-failover group is not set, and if the failed NN2600 device is the call-failover master, the failover master-service is not transferred and the resulting call is lost. All active calls are deleted across all NN2600 devices. (ID 7110)

Encryption of fragmented RTP packet

Currently, NN2600 does not perform reassembly of fragmented RTP packets that require encryption. Because encryption requires the entire non-fragmented RTP packet, fragmented RTP packets are dropped. (ID 6462)

Eyebeam 1.5 phone disconnect

Performing Broadsoft session auditing on both legs of a SIP call will cause Eyebeam 1.5 phones running TLS/SRTP to disconnect. (ID 4700)

Rapid UDP registrations and maximum sessions

When the **vsp\settings\max-number-of-sessions** property setting is reached, and with **vsp\call-admission-control** set to *disabled*, repeated error messages will occur if there are rapid UDP registrations consuming NN2600 memory resources.

Use the **vsp\sip-timers\max-udp-session-linger** property to set the number of milliseconds that NN2600 maintains a SIP session after its useful life is over. Enter a value from 0 to 60,000 milliseconds; the default setting is 30,000 ms (30 seconds). A value of 5 sets NN2600 to remove the session 5 milliseconds after receipt/ transmission of the first final response. (ID 5483)

NOTIFY message from BroadSoft server

If the **vsp\enterprise\servers\dns-group** is set with the **domain-port** property configured, or if the **local-port** is configured for an enterprise server, configure that port on all interfaces so that a SIP NOTIFY uses that port on the inbound call leg to the call destinations. Otherwise, the SIP NOTIFY will attempt to use a nonexisting local port and generate a “400 Bad Request” message back to the server on the trunk side of the network. (ID 5893)

NN2600 Management System

- There will be a conflict the first time two users simultaneously open a NN2600 configuration in the NN2600 Management System (using the Configuration, Services or Access tab), and if one of the users does not make any changes or configuration updates before the other user. This problem will resolve itself after the first update without any actual configurations changes applied. However, there will be ongoing conflicts if the configuration contains a phantom directory. (ID 6182)
- The NN2600 Management System is not supported over the Firefox Web browser. (ID 3506)
- In order for online help to display properly using Internet Explorer, you must be logged in to the NN2600 Management System with an active session. The NN2600 Management System is only supported over Internet Explorer, even though the default browser on your system may be different.
- After making any changes to the NN2600 Web server configuration, such as changes made to the idle timeout and the connection protocol, and enabling and disabling the trap target, there may be a delay of three minutes while the Web server resets and allows the NN2600 Management System to reconnect. Since there is a significant delay while the new settings are applied, the NN2600 Management System user interface may be unresponsive if you attempt to perform other operations immediately after making changes to the Web server configuration. (ID 4052)

NN2600 actions available at the NNOS-E> prompt

The **set-call-forwarding** and **set-do-not-disturb** actions each show an optional cookie argument in the command line. The optional cookie argument is not supported for customer use. (ID 4180)

DHCP

DHCP is not currently implemented, even though you can configure DHCP using the NN2600 Management System. (ID 4367)

Call recording and playback

- Recording of a video call will only record the audio portion of the call.

- After changing from an audio-only to audio & video call (and vice-versa), only the audio will be recorded.
- The call monitor-group "snoop" method does not function in this release. (ID 1100)
- Recorded calls cannot be played back using Windows Media Player V10.0 when the Web port is Port 443 (HTTPS). Windows Media Player only plays back recorded calls over Web port 80 (HTTP). As a workaround, use QuickTime instead of Windows Media Player, as QuickTime supports HTTPS. (ID 1732)

IM management policies

Message-to-sender and **message-to-recipient** text configured as part of an IM policy is not delivered as a separate IM message. The **message-to-recipient** text is prepended to the current message. The **message-to-sender** text is pre-pended to the next message going back to the sender. (ID 696)

Presence database

In the **vsp/presence-database** object, the **repair-st-tags** and **force-un-subscribe** properties are available for debugging purposes only and are not intended for customer use. (ID 4618)

SMTP archiving with authentication

The password-tag and authentication functionality associated with SMTP archiving (**vsp\accounting\archiving\smtp-server**) is not currently supported. (ID 4521)

Policies

If you are using the header or content **sip-message-condition** properties, you must use the '(?s).' option at the beginning of the regular expression. For example, if you want to search for a user-agent RTC, use **`header match "(?s).*\bRTC/*\b".`** If you want to search for the media type in SDP, use **`content match "(?s).*\bm=video\b"`**

User and group filters

If you create a user or group filter under vsp/enterprise/directories, the filter will only take effect after a **directory-reset** action. (ID 2458)

LDAP and LDAP authentication

- When you login to NN2600 using SSH, it first asks you for a username and a password. This is the username/password combination of *root/sips* and not the LDAP username/password that you may have configured.
- Due to problems in the Java library, if an LDAP retrieval (import) of users fails, subsequent imports from other directories are not completed. This is a Java problem that will be fixed in a later JDK release. (ID 3300)

SNOM phone interoperability

- Certain random SRTP key values cause SNOM to play static or cause audio silence to the user. (ID 1587)
- SRTP with SNOM versions before v5.2 always produce static.

SRTP

Most RTCP implementations are still under development. If doing SRTP with an Eyebeam v1.5.6.1 or earlier, all RTCP packets requiring encryption (Sender and Receiver Reports) will be dropped. Since SNOM phones do not include authentication in RTCP packets, all SNOM RTCP Sender and Receiver Report packets are dropped. (ID 5206).

Linksys SRTP

In the **vsp/default-session-config/media** object, if you set the **rtcp** property to *pass*, NN2600 will not send RTCP packets to endpoints in a Linksys SRTP configuration. (ID 6878)

Registration-plan

The **location-service settings** object and the **registration-plan route** object both allow you to set the **max-bindings-per-AOR** property. Currently this value is set to 1 in settings and 0 (as-is) in route, and should not be changed.

Archiving

- If NN2600 is configured for registration delegation (instead of handling registrations directly), and if archiving is enabled, SIP calls will be archived twice, with both archives containing the same information. (ID 2658)
- When configuring archiving based on the new **record-count** property in Release 3.1, calls made through a server (such as Asterisk) originate two records per call so that the number of records is twice the real number of calls. For example, if you configure the archive **record-count** to 100, archiving occurs at the 50th call because of the two records per call. (ID 5335)
- If using the **record-count** property to set the threshold that determines the number of accounting records to be written before the whole group is then archived, setting a value to 0 (the default), disables this feature. When set to any number greater than 0, the accounting software checks every 30 seconds to calculate whether the requisite number of records are waiting.

  Archiving only occurs when you invoke it specifically, as an action or as a scheduled text. Note that setting this property to any value other than 0 causes both the archive action and/or task to fail. Use this property with care, as the archiving function consumes system resources. (ID 5387, 5404)

Assigning a management IP address

Before you can configure the NN2600 device remotely over the Internet using the NN2600 Management System, or over a Telnet connection, you need to locally assign an IP address to one of the Ethernet interfaces, **eth0**, **eth1, eth2,** or **eth3.** If you are setting up the device remotely, you will also need to configure an IP route, a route to a destination host or network, and a gateway IP address.

If you are using the NN2600 Management System, you will also need to know the assigned IP address on one of the Ethernet ports to manage the configuration. You access the NN2600 Management System application running on the NN2600 device over the Internet using the Internet Explorer Web browser.

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

CLI session

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

Using the setup script

An optional configuration setup script called *cxc.setup* is included with NN2600 software. After installing a new system, you can run the script directly from the NNOS-E> prompt, as shown in the example session below.

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

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

Every NN2600 Series system has a minimum of two Ethernet interfaces. Any Ethernet interface can be used for management traffic, however, Acme Packet recommends the use of eth1, as eth0 is reserved for fault-tolerant clustering with other NN2600 devices . Management traffic is also supported on any interface that is carrying private or public network traffic. This means that it would be possible to use eth1 to carry SIP traffic and management traffic.

CLI session

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

Note: The /cxc directory on the NN2600 device may include vendor-specific scripts that address unique startup configuration requirements. Specify the name of the script on the command line following the **config setup** command. For example:

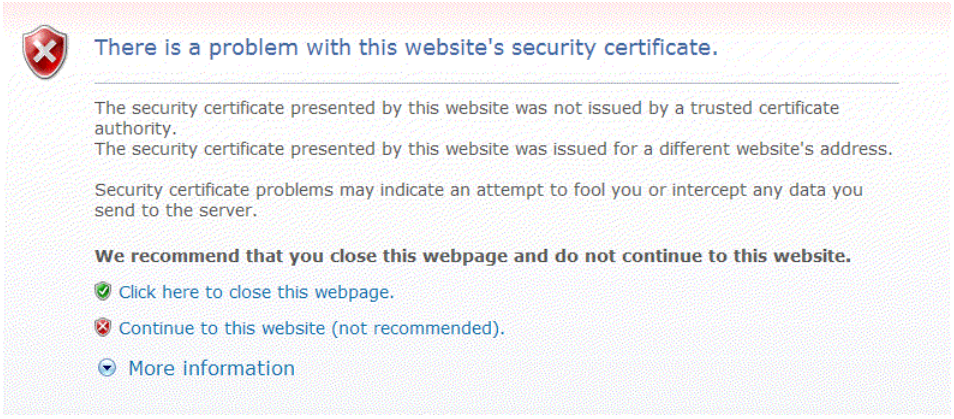
```
NNOS-E> config setup vendor.setup
```

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

Logging on using the NN2600 Management System

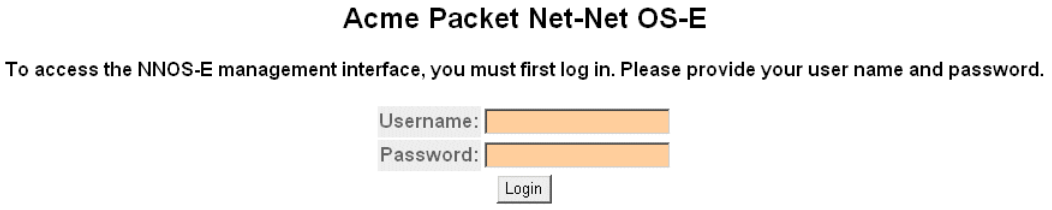
If you are using HTTPS (Port 443) to connect to the NN2600 device (HTTPS://<ipaddress> from your Web browser), you will need to configure the Web service so that a valid SSL certificate is referenced at login time. Otherwise, your Web browser will display a screen similar to the following image, warning you of the security issues with the absence of an SSL certificate.

Security certificate warning



To proceed immediately to the NN2600 Management System login page, select **Continue to this website**, as illustrated in the following image. Then, click **Login** to bypass the Username and Password prompts. Once you are logged in, you can configure usernames and passwords for access to this NN2600 device using the **access\users\user** configuration path.

NN2600 Log In screen.



Acquiring and configuring the certificate

NN2600 requires a signed SSL certificate from a valid Certificate Authority (CA), or you can use NN2600 to create a self-signed certificate. The supported format for the certificate is PKCS#12, (Public Key Cryptography, standard #12 format).

For complete information on managing certificates, refer to the *Net-Net 2600 – System Installation and Commissioning Guide*.

Configuring the Web service for HTTPS

Once you have installed a valid certificate, you will need to edit the NN2600 **web-service** object to reference the certificate at NN2600 Management System login time. This will remove the security certificate warning shown above. The following CLI session references the certificate over Port 443 using the **protocol** property under the **web-service** object.

CLI session

```
NNOS-E> config box
config box> config interface eth1
config interface eth1> config ip 172.26.2.14
Creating 'ip 172.26.2.14'
config ip 172.26.2.14> config web-service
config web-service> set protocol https 443 “vsp tls certificate
   company.pfx”
```

Building the configuration file

The NN2600 configuration file (*cxc.cfg*) is made up of configuration objects and property settings that control how the system processes and manages SIP traffic. As you open these objects and set properties using the CLI or the NN2600 Management System, NN2600 builds a configuration hierarchy of objects that are applied to SIP sessions. You can display this configuration hierarchy using the **show** and **show -v** commands.

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

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

To remove an object from the configuration hierarchy, use the CLI or NN2600 Management System **delete** command.

Creating cluster networks

If you are installing multiple NN2600 devices in a high-availability cluster, refer to the *Net-Net 2600 – System Installation and Commissioning Guide* for information.

Installing NN2600 software updates

Periodic NN2600 software updates and patches are available to Acme Packet customers whenever software improvements and functionality changes enhance NN2600 operation. System software updates are available from the Acme Packet Support Web site.

Getting software from the Product Support Web site

Using your Web browser, open your Acme Packet customer URL to access the Product Support Web site. Follow the instructions on your screen to download the software update to your PC or to a network location, then follow one of the procedures below to install the new NN2600 software.

- Installation procedure using the CLI.
- Installation procedure using the NN2600 Management System.

Installation procedure using the CLI

Once you have downloaded the NN2600 release software, you can use the CLI to install the file on each NN2600 device in the network. Use the **file fetch** command to get the file from its current location to the NN2600 device.

The **file fetch** command accepts a large number of URL schemes that you can you use to fetch the release file. Use the **file fetch ?** command to display the file fetch command options. The CLI session below shows only those URL schemes that would be the most useful for file transfers.

CLI session

```
NNOS-E> file fetch ?

manage Net-Net OS-E files

 syntax: file erase file
         file fetch source-url [destination-file]
         file send source-file destination-url

ftp://              File Transfer Protocol (RFC 1738)
http://             Hypertext Transfer Protocol (RFC 2616)
https://            Hypertext Transfer Protocol Secure (RFC 2818)
gopher://           The Gopher Protocol (RFC 1738)
file://             Host-specific file names (RFC 1738)
ftps://             File Transfer Protocol Secure
                      (RFC-draft-murray-auth-ftp-ssl-16.txt)
tftp://             Trivial File Transfer Protocol (RFC 3617)
```

Refer to the RFC that applies to the URL scheme you are using for the exact formatting of the command line.

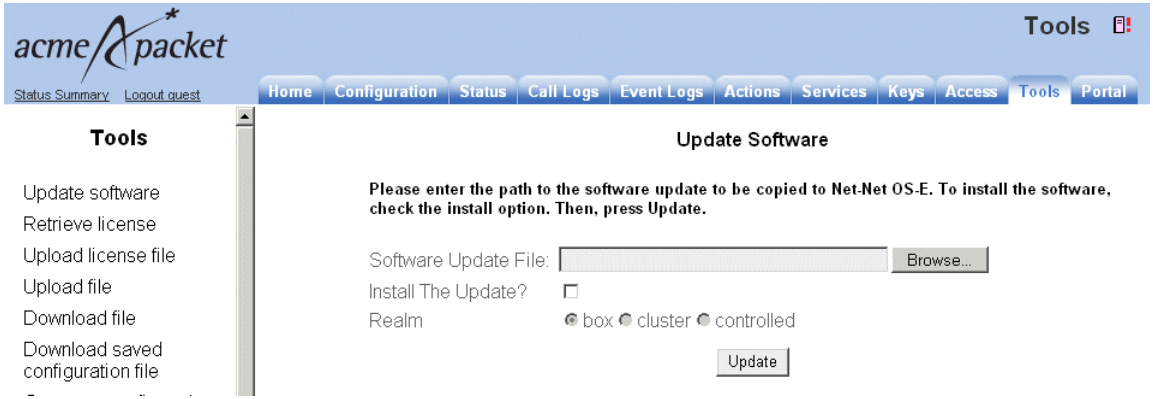
Installation procedure using the NN2600 Management System

Once you have downloaded the NN2600 software update from the Product Support Web site, use the NN2600 Management System to install the software on the NN2600 device. Perform the following steps:

1. Launch the NN2600 Management System.
2. Click on the **Tools** tab, as shown in Figure 5.
3. Click **Update Software**.
4. At the “Software Update File” field, click **Browse** to locate the software release file on your PC, or enter the path and file name in the box.
5. At the “Install the Update?” field, check the box to install the software.
6. At the “Realm” field, check one of the option: **box**, **cluster**, or **controlled**. This instructs the upgrade software to operate on the local NN2600 device (box), across the NN2600 cluster, or in a controlled manner.

Selecting **controlled** in a two system (active/standby) cluster configuration performs the cluster upgrade so that the currently active NN2600 device continues to handle SIP traffic. Once the backup device has completed the software upgrade, it informs the active device that it is available to process calls. New SIP traffic then migrates to the backup device. When the active NN2600 device is no longer processing calls, it becomes the backup device where the software update is applied.

7. Click **Update** to install the software and to restart the NN2600 device.
8. Refresh your Internet Explorer Web browser by selecting **View->Refresh.**Update Software page



Information on NN2600 licensing

You are no longer required to run the **license fetch** command with newly-installed CXC systems and third-party hardware platforms to activate the features that you purchased. Your licensed features are included with your initial NN2600 download. Refer to the *Net-Net 2600 – USB Creation and Commissioning Instructions* for complete information.

However, you will need to run **license fetch** under certain conditions, such as renewing an expired license, and when installing licensed features that you did not originally purchase with the system.

Adding licensed features

If you find that you do not have one or more of the features that you purchased, or if you want to add features that you did not originally purchase, contact your Acme Packet Sales Representative or Acme Packet Product Support. Acme Packet will correct the problem and supply you with a new key that operates with the **license fetch** command.

As NN2600 software becomes available with newly-added features, your Acme Packet Sales Representative will assist you with ordering the software. Acme Packet will then provide you with a new licensing key.

License expirations and renewals

If your customer-specific license comes with an expiration date, NN2600 will generate an event when the license nears that expiration date. You can renew your license by re-executing the **license fetch** command. The Acme Packet license server verifies that there is a valid license renewal associated with your system ID, and then resets the license expiration to a new date.

Evaluation systems

For evaluation systems in lab environments without Internet connectivity, Acme Packet will provide you with an alternate method for acquiring the appropriate license to operate and configure NN2600. Contact your Acme Packet Sales Representative or Acme Packet Support for details.

License fetch procedure

Before you execute the **license fetch** command, ensure that

1. You have a connection to the public Internet, and
2. Port 616 is available and not blocked by any firewalls. This allows connectivity to the Acme Packet license server.

Note: If you do not run the **license fetch** command to successfully unlock your customer-specific features, you will not be able to configure NN2600 with any of the licensed options provided by Acme Packet.

Fetching the signed license from the CLI

From the CLI prompt, run the following command:

```
NNOS-E> license fetch <license-key-text>
Success!
```

Where **<license-key-text>** is the private key provided to you by Acme Packet. This command will contact the Acme Packet licensing server, authenticate your unique key, and then install a license on your system. Make sure that NN2600 reports "Success!"

Note: If you are unable to fetch an encrypted license using the Acme Packet key, cannot access the licensing server, or if you receive a message other than "Success!,"contact Acme Packet Product Support immediately for assistance.

Fetching the signed license from the NN2600 OS-E Management System

If you are using the NN2600 Management System, go the **Actions** tab and select **license->fetch** and paste the Acme Packet key into the key field, as illustrated in the following image. Click **Invoke** to install the signed license.

License fetch page

You can also manage licenses from the **Tools** tab using the **Retrieve License** and the **Upload License** functions. **Retrieve License** operates the same as the **license fetch** command, contacting the Acme Packet license server over the Internet.

If for some reason you are unable to access the Acme Packet license server, and if Acme Packet e-mails the license file to you, place the license on your local PC, use the NN2600 Management System **Tools->Upload License file** to browse for the file, select **Apply License**, then click **Upload.**

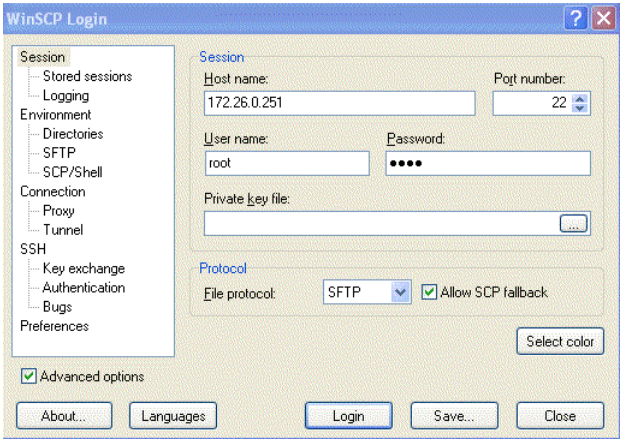
Using WinSCP to transfer the license

If you do not have access to the NN2600 Management System, Acme Packet recommends that you use WinSCP to transfer the license file to the NN2600 device. WinSCP is an open source free SFTP client and FTP client for Windows and is available as a free download from the following URL:

http://winscp.net/eng/index.php

The following image illustrates the WinSCP login window.

WinSCP Login

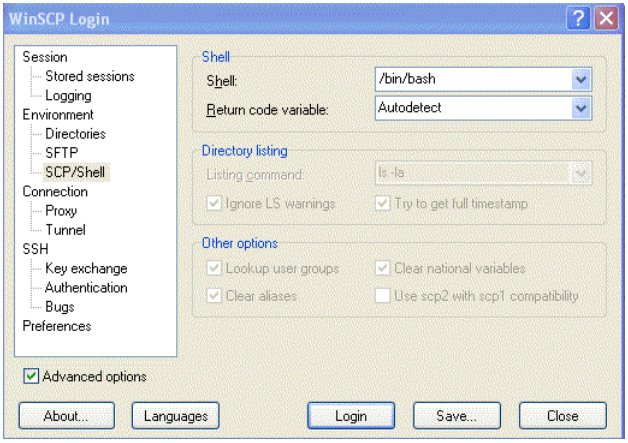


Perform the following steps:

1. At the **Hostname** field, enter the IP address that you assigned to the management interface at NN2600 device. Port **22** is the default port number for SSH sessions.
2. At the **Username** and **Password** fields, type *root* for the username and *sips* for the password.

3. At the Environment menu, select **SCP/Shell** and select **/bin/bash** from the pull-down menu, as illustrated in the following image. Leave all other fields at their default settings.

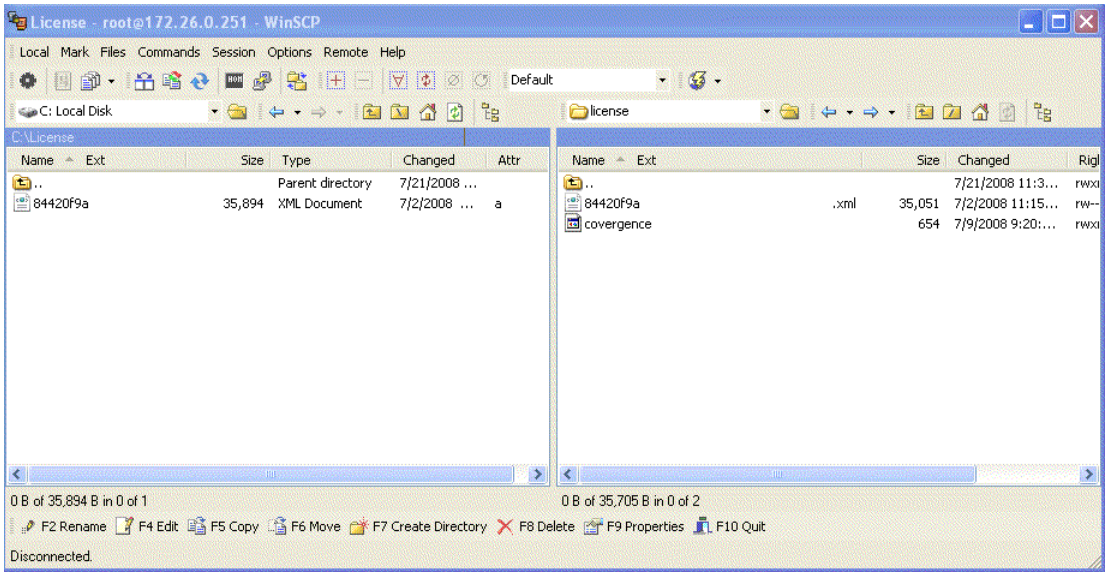
WinSCP Login SCP/Shell window



4. Click **Login**. A series of progress message will appear as the connection is established.

5. From the left pane, browse and locate the license file, then drag the license to the *cxc/license* directory, as illustrated in the following image. In this example, the file is copied from the **c:\license** directory to the **cxc\license** directory on NN2600.

Using WinSCP to copy the license to NN2600



6. Once the license file is present in the /cxc/license folder, you will need to do one of the follow tasks for the NN2600 license to take effect:

   - Perform a physical restart of the NN2600 device, or
   - From a CLI session to the NN2600 device, execute the **license apply** action, as follows:

```
NNOS-E> license apply /cxc/license/
84420g9a-da13-3007-8853-z00a7a4d771d.xml
Success!

NNOS-E> show licenses

name: License for customer.com
description: License for customer.com
        key: 84420g9a-da13-3007-8853-z00a7a4d771d
    expires:
       file: 84420g9a-da13-3007-8853-z00a7a4d771d.xml
```

Interoperating with SIP vendors

NN2600 devices are designed to interoperate with SIP servers, hosted SIP applications, and SIP PBX equipment for VoIP applications.

Contact your Acme Packet sales representative for a complete list of SIP vendors who interoperate with NN2600 software.

Downloading optional management files

If you are using an SNMP management application, use the NN2600 Management System to download the following management files from the NN2600 software release:

- CXC.MIB (Acme Packet NN2600 Enterprise MIB)
- XML Schema (mgmt_data.xsd), describing the structure of the XML data.

Perform the following steps:

1. Launch the NN2600 Management System.
2. Click on the **Tools** tab.
3. At the Management Information section, click **XML Schema** or click **MIB** to download the file to your Web browser.
4. Use the **Save** command from your browser to save a copy of the file. Import the CXC-MIB file into the SNMP management application.

CDR field descriptions and data types

The following table lists and describes the fields and data types that make up a call detail record in this release.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
session-id	type="uint64" format="hex" key="index"	type=”int8”	**NUMBER**	The unique session identifier in hexadecimal format, unassigned 64-bit integer.
recorded	type="Boolean"	type=”int4”	**NUMBER**	The true or false indication as to whether the SIP call was recorded.
call-id	type="String"	type-”name”	**VARCHAR2 (256) (256)**	The unique call identifier of the inbound call leg.
to	type="String"	type=”name”	**VARCHAR2 (256) (256)**	The string in the To URI: field of the SIP header.
from	type="String"	type=”name”	**VARCHAR2 (256)**	The string in the From URI:field of SIP header.
method	type="String”	type=”name”	**VARCHAR2 (256)**	The SIP method, such as INVITE or REGISTER, that initiated the call session.
incoming-request-uri	type="String”	type=”name”	**VARCHAR2 (256)**	The Request URI on the inbound call leg.
previous-hop-ip	type="IPHost"	type=”int4”	**NUMBER**	The IP address of the previous hop; the last network node handling the call before received at the NN2600 device.
previous-hop-via	type="String"	type=”name”	**VARCHAR2 (256)**	The VIA header from the previous hop.
outgoing-request-uri	type="String"	type=”name”	**VARCHAR2 (256)**	The Request URI on the outbound leg.
next-hop-ip	type="IPHost”	type=”int4”	**NUMBER**	The IP address of the next hop; the next network node handling the call forwarded by the NN2600 device.
next-hop-dn	type="String"	type=”name”	**VARCHAR2 (256)**	The fully qualified domain name (FQDN) or IP address of the next network node handling the call forwarded by the CXC.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
header	type="String"	type=”name”	**VARCHAR2 (256)**	An arbitrary header associated with the SIP call.
origin	type="String"	type=”name”	**VARCHAR2 (256)**	The ORIGIN header associated with the SIP call.
setup-time	type="Time" key="index"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was set up at the CXC in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*
connect-time	type="Time"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was connected to the SIP call destination in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*
disconnect-time	type="Time"	type= ”timestamp”	**TIMESTAMP**	The time at which the SIP was disconnected from the SIP call destination in the format *hour:minutes:seconds.milliseconds: weekday year-month-day.*
disconnect-cause	type=“DisconnectType"	type=”int4”	**NUMBER**	The reason for the call disconnection, such as BYE.
duration	type=”uint32”	type=”int4”	**NUMBER**	Duration of the call in seconds.
scp-name	type="String"	type=”name”	**VARCHAR2 (256)**	The CXC virtual system partition (VSP) that handled the call.
call-id-2	type="String"	type=”name”	**VARCHAR2 (256)**	The secondary call identifier for the outgoing leg.
origGW	type=”String”	type=”name”	**VARCHAR2 (256)**	The name of the originating gateway associated with the call.
termGW	type-”String”	type=”name”	**VARCHAR2 (256)**	The name of the gateway where the call was terminated.
packets-received-on src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets received on the inbound call leg.
packets-lost-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets lost on the inbound call leg.
packets-discarded-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets discarded on the inbound call leg.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
pvd-on-src -leg	type="uint32"	type=”int4”	**NUMBER**	The packet delay variation (jitter) associated with the call on the inbound call leg.
max-jitter-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum jitter on the source leg.
codec-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The CODEC associated with the inbound call leg.
mimetype-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The MIME type associated with the inbound call leg, such as audio/pcmu.
latency-on-src-leg	type="uint32"	type=”int4”	**NUMBER**	The total processing time of the inbound call leg.
max-latency-on -src-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum latency on the inbound call leg.
rfactor-on-src-leg	type="uint16” or type=”uint32”	type=”int4”	**NUMBER**	The R-factor integer used in the MOS score compilation on the inbound call leg.
packets-received-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets received on the outbound call leg.
packets-lost-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets lost on the outbound call leg.
packets-discarded-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total number of packets discarded on the outbound call leg.
pvd-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The packet delay variation (jitter) associated with the call on the outbound call leg.
max-jitter-on-dst-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum jitter on the destination leg.
codec-on-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The CODEC associated with the outbound call leg.
mimetype-on-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The MIME type associated with the outbound call leg, such as audio/pcmu.
latency-on-dest-leg	type="uint32"	type=”int4”	**NUMBER**	The total processing time of the outbound call leg.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
max-latency-on-dst-leg	type="uint32"	type=”int4”	**NUMBER**	The maximum latency on the destination leg.
rfactor-on-dest-leg	type="uint16”	type=”int4”	**NUMBER**	The R-factor integer used in the MOS score compilation on the destination call leg.
rfactor-on-dest-leg-times-1000	type-”uint32”	type=”int4”	**NUMBER**	The R-factor integer * 1000 this is used in the MOS score compilation on the destination call leg.
rfactor-on-src-leg-times-1000	type-”uint32”	type=”int4”	**NUMBER**	The R-factor integer * 1000 this is used in the MOS score compilation on the inbound call leg.
mos-fmt-dest-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The formatted MOS calculation on the oubound call leg. See the *Net-Net 2600 – Session Services Configuration Guide* for more information.
mos-fmt-on-src-leg	type="String"	type=”name”	**VARCHAR2 (256)**	The formatted MOS calculation on the inbound call leg. See the *Net-Net 2600 – Session Services Configuration Guide* for more information.
mos-on-dest-leg	type="uint32"	type=”int4	**NUMBER**	The MOS calculation * 1000 on the oubound call leg. See the *Net-Net 2600 – Session Services Configuration Guide* for more information.
mos-on-src-leg	type="uint32"	type=”int4	**NUMBER**	The MOS calculation * 1000 on the inbound call leg. See the *Net-Net 2600 – Session Services Configuration Guide* for more information.
call-type	type="String"	type=”name”	**VARCHAR2 (256)**	The type of call, such as IV for Inbound Voice.
disconnect-error-type	type="String"	type=”name”	**VARCHAR2 (256)**	The type of error that caused the disconnection.
ani	type="String"	type=”name”	**VARCHAR2 (256)**	The caller ID for the ANI after any manipulation is done by the CXC.

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
call-source-regid	type="String"	type=”name”	**VARCHAR2 (256)**	The server name if available, or user portion of the From: URI.
call-dest-regid	type="String"	type=”name”	**VARCHAR2 (256)**	The server name if available, or user portion of the To: URI.
new-ani	type="String"	type=”name”	**VARCHAR2 (256)**	The caller ID for the ANI after any manipulation is done by the CXC.
cdr-type	type="String"	type=”name”	**VARCHAR2 (256)**	The call record type, either START or STOP.
hunting-attempts	type="uint32"	type=”int4”	**NUMBER**	The number of times the CXC used the arbiter to select a dial-plan and a failure occurred (including subsequent attempts).
call-pdd	type="uint32"	type=”int4”	**NUMBER**	The post dial delay between the initial INVITE and the 180/183 RINGING.; calculated in msec.
call-source-realm-name	type="String"	type=”name”	**VARCHAR2 (256)**	The source domain name from which the call was received.
call-dest-realm-name	type="String"	type=”name”	**VARCHAR2 (256)**	The destination domain name to which the call was forwarded.
call-dest-cr-name	type="String"	type=”name”	**VARCHAR2 (256)**	The name of the dial plan that forwarded the call.
in_peer_dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the destination phone to which the CXC forwarded the inbound call leg. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
in_anchor_src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the CXC where the inbound call leg was forwarded to the destination peer. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
in_anchor_ dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the CXC where the inbound call leg was received from the source peer. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
in_peer_src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the source phone that contacted the CXC over an inbound call leg. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
out_peer_dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the destination phone to which the CXC forwarded the outbound (return) call leg. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
out_anchor_ src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the CXC where the outbound call leg was forwarded back to the source peer. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
out_anchor_ dst	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port at the CXC where the outbound (responding) call leg was received from the destination peer. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)
out_peer_src	type="IPPort"	type=”name”	**VARCHAR2 (256)**	The IP address and port of the responding destination phone from which an outbound call leg was returned to the CXC. (See the *Net-Net 2600 – Session Services Configuration Guide*, Appendix B, for more information.)

CDR field	MS-SQL data types	PostgreSQL data types	Oracle data types	Description
called-party-after-src-calling-plan	type="String"	type=”name”	**VARCHAR2 (256)**	The called party number after any manipulation on leg 1, but before any manipulation on leg 2.
last-status-message	type="uint16”	type=”int4”	**NUMBER**	An integer indicating SIP message type last status message (omitting “200 OK”) and therefore call progress.
last-pkt-timestamp-on-dest-leg	type=”Time”	type= ”timestamp”	**TIMESTAMP**	The time of the last media packet on the destination leg.
last-pkt-timestamp-on-src-leg	type= “Time”	type= ”timestamp”	**TIMESTAMP**	The time of the last media packet on the source leg.
setup-time-integer	type=”uint64”	type=”int8”	**NUMBER**	The call setup time indicated as an integer.
incoming-uri-stripped	type=”String”	type=”name”	**VARCHAR2 (256)**	The stripped down version of the incoming request URI.
dnis	type=”String”	type=”name”	**VARCHAR2 (256)**	Dialed Number Identification Service
newDnis	type=”String”	type=”name”	**VARCHAR2 (256)**	New Dialed Number Identification Service
custom-data	type=”String”	type=”name”	**VARCHAR2 (256)**	Custom data field as defined by the **accounting-data** object.
creation-timestamp	type= “Time”	type= ”timestamp”	**TIMESTAMP**	The time the accounting record was written to the accounting target.

New event log messages

This section lists the new events under each category for Release 3.5 versions. For a complete listing of event messages, refer to *Net-Net 2600 – Using the NN2600 Management Tools*.

PktLog events

Event Name	Severity	Displayed Text

```
stats                   error     %s@%s: Discarded %llu %s pkts within
                                  previous %u seconds
blacklist               error     %s@%s: Blacklist %s:%u Discarded
   %llu %s pkts within previous %u seconds
packet                  notice    %s@%s: Discarded pkt: %s:%u ->
   %s:%u, Proto: %s
track_port              notice    %s@%s: %u %s ports hit within
   previous %u seconds. %s
```

Result codes

For information on the possible result codes that can appear within event messages, refer to the *Net-Net 2600 – Using the NN2600 Management Tools*.

Acme Packet, Inc.
71 Third Avenue
Burlington, MA 01803 USA
t 781-328-4400
f 781-425-5077
http://www.acmepacket.com

Net-Net 2600
Release Notes

780-0004-00
Rev. 1.20
June 9, 2010
Printed in United States of America