



**Secure, Multi-lateral Peering
With
FreeRADIUS 2.1.4**

Revision History

Revision	Date of Issue	Changes
0.1	Feb 2, 2009	Initial draft
0.2	Mar 4, 2009	Updated for OSP Toolkit 3.5.0
0.3	May 4, 2009	1. Added instructions to configure Acme Packet SBC 2. Added disabling security features option
0.4	June 22, 2009	Updated for OSP Toolkit 3.5.1
0.5	July 2, 2009	Updated for OSP Toolkit 3.5.2 and OSP module ACME-0.3.0
0.6	July 7, 2009	Updated osp.conf Added Acme Packet SBC configuration
0.7	July 29, 2009	Updated for OSP module NexTone-0.1.0 RADIUS records from NexTone/GenBand now supported. Added ignoreddestinationslist to ignore CDRs to certain destination IP addresses
0.71	July 30, 2009	Minor edits

Mailing list: <https://lists.sourceforge.net/lists/listinfo/osp-toolkit-client>
Copyright © 2003-2009 by TransNexus. All Rights Reserved.
TransNexus and OSP Secured are trademarks of TransNexus, Inc.

Contents

Revision History	2
Contents	4
1 Build OSP Toolkit.....	5
1.1 Unpacking OSP Toolkit.....	5
1.2 Preparing to Build OSP Toolkit.....	6
1.3 Building OSP Toolkit	6
2 Build FreeRADIUS with OSP Module.....	7
2.1 Download FreeRADIUS Source.....	7
2.2 Download OSP module.....	7
2.3 Modify stable File.....	7
2.4 Build FreeRADIUS.....	7
3 Configure FreeRADIUS with OSP Module	8
3.1 clients.conf.....	8
3.2 sites-available/default	8
3.3 dictionary	8
3.4 modules/osp	9
4 Run FreeRADIUS with OSP Module.....	14
5 Appendix-1 Use Security Features	14
5.1 Building Enroll Utility	15
5.2 Enroll FreeRADIUS with Peering Servers	15
5.2.1 Overview.....	15
5.2.2 Using Enroll Script	15
6 Appendix-2 FreeRADIUS Example Files	16
6.1 stable	16
6.2 clients.conf.....	17
6.3 sites-available/default	22
6.4 dictionary for ACME.....	32
6.5 ACME dictionary.....	32
7 Appendix-3 ACME SBC configurations	40

1 Build OSP Toolkit

OSP Toolkit, when compiled, is a library comprised of OSP client functions that simplify sending and receiving OSP peering messages. It is this library, which will be integrated into the OSP module of FreeRADIUS. OSP Toolkit uses third party software (by default OpenSSL) for cryptographic algorithms and for secure internet transactions (HTTPS). OSP Toolkit also includes the application, **enroll**, which enables the OSP client device to generate its own public-private key pair, get the public key from an OSP peering server, send a certificate request to a peering server and receive the resulting signed certificate from the peering server.

In order to successfully compile and use OSP Toolkit, the following list of software is required:

- **OpenSSL** (required) - Open Source SSL protocol and Cryptographic Algorithms (version 0.9.8i recommended) from <http://www.openssl.org>. Pre-compiled OpenSSL packages are not recommended because of the binary compatibility issue.
- **Perl** (required) - A programming language used by OpenSSL for compilation. Any version of Perl will work. One version of Perl is available from <http://www.activestate.com/activeperl>. If pre-compiled OpenSSL packages are used, Perl package is not required.
- **C compiler** (required) - Any C compiler should work. The GNU Compiler Collection from <http://www.gnu.org> is routinely used for building OSP Toolkit for testing.
- **OSP Server** (required for testing) - Two open source OSP server projects are available. OpenOSP, an OSP server written in C code, is located at <http://www.vovida.org/applications/downloads/openosp>. RAMS, a Java based OSP server, is located at <http://sourceforge.net/projects/rams>. Also, a free version of the TransNexus commercial OSP server can be downloaded from http://www.transnexus.com/OSP%20Toolkit/Peering_Server/VoIP_Peering_Server.htm.

1.1 Unpacking OSP Toolkit

After downloading OSP Toolkit (version 3.5.2 or later release) from <http://sourceforge.net/projects/osp-toolkit>, perform the following steps in order:

- Copy the OSP Toolkit distribution into the directory where it will reside, say */usr/src*.
- Un-package the distribution file by executing the following command

```
gunzip -c OSPToolkit-###.tar.gz | tar xvf -
```

Where ### is the version number separated by dots. For example, if the version is 3.5.2, then the above command would be

```
gunzip -c OSPToolkit-3.5.2.tar.gz | tar xvf -
```

A new OSP Toolkit directory, */usr/src/TK-3_5_2-20090702*, will be created within the same directory as the tarball file.

- Go to the OSP Toolkit directory by running this command

```
cd /usr/src/TK-3_5_2-20090702
```

Within this directory, you will find directories and files similar to what is listed below if the command "ls -F" is executed)

```
ls -F
bin/  crypto/  enroll/  include/  lib/  LICENSE.txt  README.txt
RELNOTES.txt  src/  test/
```

In the remains of this documentation, we use "OSP Toolkit directory" to stand the OSP Toolkit source tree root directory. We use "OSP Toolkit **XXXXX** directory" to stand the **XXXXX** directory under OSP Toolkit source tree root directory.

1.2 Preparing to Build OSP Toolkit

- Compile OpenSSL according to the instructions provided with the OpenSSL distribution (You would need to do this only if you don't have OpenSSL already).
- Copy the OpenSSL header files (the *.h files) into the OSP Toolkit *crypto/openssl* directory. The OpenSSL header files are located under the OpenSSL *include/openssl* directory.
- Copy the OpenSSL library files (libcrypto.a and libssl.a) into the OSP Toolkit *lib* directory. The OpenSSL library files are located under the OpenSSL directory.
Note: If the OpenSSL package has been installed, above steps are not necessary.
- Optionally, change the install directory of OSP Toolkit. Open Makefile in the OSP Toolkit *src* directory, look for the install path variable – **INSTALL_PATH**, and edit it to be anywhere you want (defaults */usr/local*).
Note: Please change the install path variable only if you are familiar with both OSP Toolkit and FreeRADIUS. Otherwise, it may make FreeRADIUS does not support the OSP protocol.

1.3 Building OSP Toolkit

- From the OSP Toolkit directory start the compilation script by executing the following commands

```
cd src
make clean; make build
```

- Use the make script to install OSP Toolkit

```
make install
```

The make script installs the OSP Toolkit header files and the library into **INSTALL_PATH** directory specified in Makefile.

Note:

- Please make sure you have the rights to access **INSTALL_PATH** directory. For example, in order to access */usr/local* directory, root privileges are required.

- By default, OSP Toolkit is compiled in the production mode. The following table identifies which default features are activated with each compile option:

Default Feature	Production	Development
Debug Information Displayed	No	Yes

The "Development" option is recommended for a first time build. The **CFLAGS** definition in Makefile must be modified to build in development mode.

- By default, OSP module of FreeRADIUS does not use the security features that OSP Toolkit provides. If the security features are used, the enroll utility must be built and FreeRADIUS must be enrolled with peering servers. The instructions are listed in section 5.

2 Build FreeRADIUS with OSP Module

2.1 Download FreeRADIUS Source

The latest stable version is 2.1.4 when this documentation is processing. It can be downloaded from FreeRADIUS website <http://freeradius.org>. Uncompress / untar FreeRADIUS source code tarball (i.e. freeradius-server-2.1.4.tar.bz2) to create the FreeRADIUS source code tree root directory, *\$RADIUS_HOME*.

2.2 Download OSP module

The OSP module of FreeRADIUS is hosted on <http://sourceforge.net/projects/radius-to-osp>. The latest stable version is rlm_osp-NexTone-0.1.0.tar.gz. It should be downloaded into *\$RADIUS_HOME/src/modules* directory and uncompressed / untared by following commands.

```
cd $RADIUS_HOME/src/modules
gunzip -c rlm_osp-NexTone-0.1.0.tar.gz | tar xvf -
```

A new directory *\$RADIUS_HOME/src/modules/rlm_osp* will be generated.

2.3 Modify stable File

The OSP module, rlm_osp, must be added into stable file under *\$RADIUS_HOME/src/modules* directory to allow the module to be built with FreeRADIUS.

```
...
rlm_policy
rlm_dynamic_clients
rlm_osp
```

Please reference the example file in section 6.1.

2.4 Build FreeRADIUS

To install FreeRADIUS, root rights may be necessary.

- For Linux platforms, from within *\$RADIUS_HOME* directory execute the following commands at the command prompt

```
./configure
make clean
make
make install
```

For Solaris 10 x86 platform, from within *\$RADIUS_HOME* directory execute the following commands at the command prompt

```
./configure --without-rlm_perl --without-rlm_python
make clean
make
make install
```

Note: rlm_perl and rlm_python may have problems to work on Solaris 10 x86. We do not use them.

3 Configure FreeRADIUS with OSP Module

The OSP module of FreeRADIUS can be configured to support both Acme Packet and NexTone/GenBand SBCs. In this document, the term NexTone refers to a NexTone/Genband SBC. All configuration files are under */usr/local/etc/raddb* directory, except osp configuration file and sites-available/default.

3.1 *clients.conf*

Add test clients at the end of the configuration file.

```
# Transnexus RADIUS test configuration
client xxx.xxx.xxx.0/24 {
secret = password
nastype = other
}
```

Please reference the example file in section 6.2.

3.2 *sites-available/default*

Add OSP module into accounting block.

```
# Transnexus RADIUS test configuration
osp
```

Please reference the example file in section 6.3.

3.3 *dictionary*

For Acme Packet, the dictionary file in section 6.5 (for Net-Net 4000 C6.1) should be stored as */usr/local/share/freeradius/dictionary.acme*. It should be included in FreeRADIUS dictionary file.

```
# Transnexus RADIUS test configuration
```

```
$INCLUDE /usr/local/share/freeradius/dictionary.acme
```

Please reference the example file in section 6.4.

For NexTone/GenBand, it is not necessary to include any vendor specific dictionary file.

3.4 modules/osp

- The "default_xxx" sections list all supported options and the default values. Please do not change these sections. They are only used as reference.
- "running used" section is for the running options of the OSP module of FreeRADIUS.
- "provider used" section is for the provider options.
- Acme Packet section is for Acme Packet SBC specific configuration and NexTone section is for NexTone/Genband SBC specific configuration. The prefix "mapping" tells the OSP module which SBC is used.
- The ignoreddestinationlist option is useful for call scenarios when a SIP redirect servers is used and the RADIUS client reports RADIUS records for the SIP redirect call legs. The RADIUS records for the call leg to the redirect server should be ignored. The IP addresses of the redirect servers should be listed in the ignoreddestinationlist.

Note: ignoreddestinationlist syntax in ABNF

```
subnetlist = "NULL" / [subnet [othersubnets]]
```

```
subnet = ip [subnetdelimiter mask]
```

```
ip = dotted-decimal IP address
```

```
subnetdelimiter = "/"
```

```
mask = dotted-decimal IP address
```

```
othersubnet = *3(listdelimiter subnet)
```

```
listdelimiter = "," / ";"
```

Only *spuri1* in "provider used" section must be configured.

```
# -*- text -*-
##
## osp.conf -- Configuration for OSP running parameters
##
## $Id: osp.conf,v 1.7.2.6 2009/07/23 10:37:46 di-shi Exp $
#####
##
#
# OSP configuration
#
osp {
    # OSP module running parameters
    default_running { # This is the default running configuration
section. Please do not touch it!!!
        loglevel = 1 # 0 - short, 1 - long */
    }

    running used { # This is the used running configuration
section.
    }
}
```

```

# OSP provider parameters
default_provider { # This is the default provider configuration
section. Please do not touch it!!!
    accelerate = no
    security = no
    spuril = http://osptestserver.transnexus.com:1080/osp
    # spuril = https://[1.2.3.4]:1443/osp
    spweight1 = 1000
    spweight2 = 1000
    spweight3 = 1000
    spweight4 = 1000
    privatekey = /usr/local/etc/raddb/pkey.pem
    localcert = /usr/local/etc/raddb/localcert.pem
    cacert0 = /usr/local/etc/raddb/cacert_0.pem
    cacert1 = /usr/etc/raddb/cacert_1.pem
    ssllifetime = 300
    persistence = 60000
    maxconnections = 20 # 1 ~ 1000
    retrydelay = 0 # 0 ~ 10
    retrylimit = 2 # 0 ~ 100
    timeout = 10000 # 200 ~ 60000
    deviceip = localhost
    deviceport = 5060
}

provider used { # This is the used provider configuration
section.
    spuril = http://127.0.0.1:1080/osp
    deviceip = 192.168.0.1
}

# RADIUS OSP mapping parameters
default_mapping { # This is the default mapping configuration
section. Please do not touch it!!!
    radiusclienttype = 0 # 0 - undefined, 1 -
ACME, 2 - NexTone */
    ignoreddestinationlist = NULL
    callorigin = NULL # Only for NexTone
    transactionid = NULL
    callid = %{Acct-Session-Id}
    iscallinguri = yes
    callingnumber = %{Calling-Station-Id} # From header
    iscalleduri = yes
    callednumber = %{Called-Station-Id} # To header
    assertedid = NULL
    sourcedevice = NULL
    source = %{NAS-IP-Address}
    proxy = %{NAS-IP-Address} # Only for NexTone
    destination = NULL
    destinationdevice = NULL
    destinationcount = NULL
    sourcenetworkid = NULL
    destinationnetworkid = NULL
    timestringformat = 0 # 0 - time_t, 1 -
ctime, 2 - NTP w/o week day, 3 - NTP */

```

```
starttime = %{Acct-Session-Start-Time}
altertime = NULL
connecttime = NULL
endtime = NULL
duration = %{Acct-Session-Time}
postdialdelayunit = 0 # 0 - seconds, 1 -
milliseconds */
postdialdelay = NULL
releasesource = NULL
releasecause = %{Acct-Terminate-Cause}
destinationprotocol = NULL
inboundsessionid = NULL
outboundsessionid = NULL
forwardcodec = NULL
reversecodec = NULL
conferenceid = NULL
reportstatistics = yes
sendlostpackets = NULL
sendlostfraction = NULL
receivelostpackets = NULL
receivelostfraction = NULL
rtpdownstreamlostpackets = NULL
rtpdownstreamlostfraction = NULL
rtpupstreamlostpackets = NULL
rtpupstreamlostfraction = NULL
rtcpdownstreamlostpackets = NULL
rtcpdownstreamlostfraction = NULL
rtcpupstreamlostpackets = NULL
rtcpupstreamlostfraction = NULL
rtpdownstreamjittersamples = NULL
rtpdownstreamjitterminimum = NULL
rtpdownstreamjittermaximum = NULL
rtpdownstreamjittermean = NULL
rtpdownstreamjittervariance = NULL
rtpupstreamjittersamples = NULL
rtpupstreamjitterminimum = NULL
rtpupstreamjittermaximum = NULL
rtpupstreamjittermean = NULL
rtpupstreamjittervariance = NULL
rtcpdownstreamjittersamples = NULL
rtcpdownstreamjitterminimum = NULL
rtcpdownstreamjittermaximum = NULL
rtcpdownstreamjittermean = NULL
rtcpdownstreamjittervariance = NULL
rtcpupstreamjittersamples = NULL
rtcpupstreamjitterminimum = NULL
rtcpupstreamjittermaximum = NULL
rtcpupstreamjittermean = NULL
rtcpupstreamjittervariance = NULL
rtpdownstreamdelaysamples = NULL
rtpdownstreamdelayminimum = NULL
rtpdownstreamdelaymaximum = NULL
rtpdownstreamdelaymean = NULL
rtpdownstreamdelayvariance = NULL
rtpupstreamdelaysamples = NULL
rtpupstreamdelayminimum = NULL
```

```

rtpupstreamdelaymaximum = NULL
rtpupstreamdelaymean = NULL
rtpupstreamdelayvariance = NULL
rtcpdownstreamdelaysamples = NULL
rtcpdownstreamdelayminimum = NULL
rtcpdownstreamdelaymaximum = NULL
rtcpdownstreamdelaymean = NULL
rtcpdownstreamdelayvariance = NULL
rtcpupstreamdelaysamples = NULL
rtcpupstreamdelayminimum = NULL
rtcpupstreamdelaymaximum = NULL
rtcpupstreamdelaymean = NULL
rtcpupstreamdelayvariance = NULL
rtpdownstreamoctets = NULL
rtpupstreamoctets = NULL
rtcpdownstreamoctets = NULL
rtcpupstreamoctets = NULL
rtpdownstreampackets = NULL
rtpupstreampackets = NULL
rtcpdownstreampackets = NULL
rtcpupstreampackets = NULL
rfactorscaleindex = 4 # 0 - 0.0001, 1 -
0.001, 2 - 0.01, 3 - 0.1, 4 - 1, 5 - 10, 6 - 100, 7 - 1000, 8 - 10000
*/
rtpdownstreamrfactor = NULL
rtpupstreamrfactor = NULL
rtcpdownstreamrfactor = NULL
rtcpupstreamrfactor = NULL
mossscaleindex = 4 # 0 - 0.0001, 1 -
0.001, 2 - 0.01, 3 - 0.1, 4 - 1, 5 - 10, 6 - 100, 7 - 1000, 8 - 10000
*/
rtpdownstreammoscq = NULL
rtpupstreammoscq = NULL
rtcpdownstreammoscq = NULL
rtcpupstreammoscq = NULL
rtpdownstreammoslq = NULL
rtpupstreammoslq = NULL
rtcpdownstreammoslq = NULL
rtcpupstreammoslq = NULL
custominfo1 = NULL
custominfo2 = NULL
custominfo3 = NULL
custominfo4 = NULL
}

ACME { # This is the ACME mapping configuration section.
radiusclienttype = 1
callednumber = %{Acme-Primary-Routing-Number} #
Original called number
# callednumber = %{Acme-Egress-Final-Routing-Number} #
Transaltaed called number
assertedid = %{Acme-P-Asserted-ID}
sourcedevice = %{Acme-Ingress-Remote-Addr}
destination = %{Acme-Egress-Remote-Addr}
timestringformat = 2
starttime = %{h323-setup-time}

```

```

connecttime = %{h323-connect-time}
endtime = %{h323-disconnect-time}
postdialdelayunit = 1
postdialdelay = %{Acme-Post-Dial-Delay}
releasesource = %{Acme-Disconnect-Initiator}
releasecause = %{Acme-SIP-Status} # SIP
# releasecause = %{Acme-Disconnect-Cause} # ISDN
destinationprotocol = %{Acme-Session-Protocol-Type}
inboundsessionid = %{Acme-Session-Ingress-CallId}
outboundsessionid = %{Acme-Session-Egress-CallId}
forwardcodec = %{Acme-FlowType_FS1_F}
reversecodec = %{Acme-FlowType_FS1_R}
rtcpdownstreamlostpackets = %{Acme-Calling-RTP-Packets-
Lost_FS1}
rtcpupstreamlostpackets = %{Acme-Called-RTP-Packets-Lost_FS1}
rtcpdownstreamlostpackets = %{Acme-Called-RTCP-Packets-
Lost_FS1}
rtcpupstreamlostpackets = %{Acme-Calling-RTCP-Packets-
Lost_FS1}
rtcpdownstreamjittermaximum = %{Acme-Calling-RTP-
MaxJitter_FS1}
rtcpdownstreamjittermean = %{Acme-Calling-RTP-Avg-Jitter_FS1}
rtcpupstreamjittermaximum = %{Acme-Called-RTP-MaxJitter_FS1}
rtcpupstreamjittermean = %{Acme-Called-RTP-Avg-Jitter_FS1}
rtcpdownstreamjittermaximum = %{Acme-Called-RTCP-
MaxJitter_FS1}
rtcpdownstreamjittermean = %{Acme-Called-RTCP-Avg-Jitter_FS1}
rtcpupstreamjittermaximum = %{Acme-Calling-RTCP-
MaxJitter_FS1}
rtcpupstreamjittermean = %{Acme-Calling-RTCP-Avg-Jitter_FS1}
rtcpdownstreamdelaymaximum = %{Acme-Called-RTCP-
MaxLatency_FS1}
rtcpdownstreamdelaymean = %{Acme-Called-RTCP-Avg-Latency_FS1}
rtcpupstreamdelaymaximum = %{Acme-Calling-RTCP-
MaxLatency_FS1}
rtcpupstreamdelaymean = %{Acme-Calling-RTCP-Avg-Latency_FS1}
rtcpdownstreamoctets = %{Acme-Calling-Octets_FS1}
rtcpupstreamoctets = %{Acme-Called-Octets_FS1}
rtcpdownstreampackets = %{Acme-Calling-Packets_FS1}
rtcpupstreampackets = %{Acme-Called-Packets_FS1}
rfactorscaleindex = 2
rtcpdownstreamrfactor = %{Acme-Called-R-Factor}
rtcpupstreamrfactor = %{Acme-Calling-R-Factor}
mosscaleindex = 2
rtcpdownstreammoscq = %{Acme-Called-MOS}
rtcpupstreammoscq = %{Acme-Calling-MOS}
custominfo1 = %{Acme-Custom-VSA-200}
}

mapping NexTone { # This is the NexTone mapping configuration
section.
radiusclienttype = 2
ignoreddestinationlist = x.x.x.x/y.y.y.y,z.z.z.z
callorigin = %{h323-call-origin}
callid = %{h323-incoming-conf-id}
iscallinguri = no

```

```

        iscalleduri = no
        callednumber = %{gw-rxd-cdn}                # Original called
number
        # callednumber = %{gw-final-xlated-cdn}    # Transaltaed
called number
        sourcedevice = %{h323-remote-address}
        proxy = %{NAS-IP-Address}
        destination = %{h323-remote-address}
        timestringformat = 3
        starttime = %{h323-setup-time}
        connecttime = %{h323-connect-time}
        endtime = %{h323-disconnect-time}
        releasesource = %{release-source}
        releasecause = %{h323-disconnect-cause} # ISDN
        destinationprotocol = %{session-protocol}
        inboundsessionid = %{h323-incoming-conf-id}
        outboundsessionid = %{h323-conf-id}
        reportstatistics = no
    }
}

```

4 Run FreeRADIUS with OSP Module

At the first time, the FreeRADIUS server must be run by root to create the cert files.

```

cd /usr/local/sbin
./radiusd -X

```

Note: For Solaris 10 x86 platform, the following steps may be needed to generate the FreeRADIUS cert files before running "`./radiusd -X`".

```

cd /usr/local/etc/raddb/certs
change Makefile random block "-e" to "-f"
./bootstrap

```

Then it must be run in front mode to allow the multiple thread feature of the OSP module.

```

cd /usr/local/sbin
./radiusd -f &

```

To allow debug log, "-fx" option may replace the "-f" option.

5 Appendix-1 Use Security Features

If the security features that OSP Toolkit provides are not used, it is not necessary to build enroll utility and enroll FreeRADIUS server with peering servers.

5.1 Building Enroll Utility

The enroll program is a utility application for establishing a trusted relationship between a FreeRADIUS server and an OSP peering server or certificate authority. The following steps will build the enroll utility included within OSP Toolkit.

- For Linux platforms, from within the OSP Toolkit directory, */usr/src/TK-3_5_2-20090702*, execute the following commands at the command prompt

```
cd enroll
make clean; make linux
```

- For Solaris 10 x86 platform, from within the OSP Toolkit directory, */usr/src/TK-3_5_2-20090702*, execute the following commands at the command prompt

```
cd enroll
make clean; make
```

Compilation is successful if there is not any error in the compiler output. The enroll program is now located in the OSP Toolkit *bin* directory. For more information on **enroll** utility, please see http://www.transnexus.com/OSP%20Toolkit/OSP%20Toolkit%20Documents/Device_Enrollment.pdf.

5.2 Enroll FreeRADIUS with Peering Servers

5.2.1 Overview

It requires three crypto files to establish a secure relationship between an OSP peering server and the OSP module in FreeRADIUS. These files are:

- **localcert.pem** - The local certificate for FreeRADIUS signed by the OSP server.
 - **pkey.pem** - The private key generated by the enroll utility for FreeRADIUS.
 - **ca-cert_#.pem** - The Certificate Authority (CA) certificate from an OSP server. FreeRADIUS may enroll with multiple certificate authorities or peering servers. The # represents an integer indicating the CA certificate from different peering servers.
- enroll** utility automates the process of enrolling FreeRADIUS with peering servers and creating the crypto files. By default, the OSP Module of FreeRADIUS will load the crypto files from the configuration directory, default */usr/local/etc/raddb*. If the files are not present, the OSP Module of FreeRADIUS will not start.

5.2.2 Using Enroll Script

The script **enroll.sh** requires AT&T korn shell (ksh) or any of its compatible variants. The OSP Toolkit *bin* directory should be in the PATH environment variable. From the command line, type enroll.sh followed by the IP addresses or domain name of the peering servers. Below is an example of the Enroll utility being used to enroll FreeRADIUS with a peering server named *osptestserver.transnexus.com*. The gray boxes indicate optional input which will be included in the certificate of FreeRADIUS. Error Code 0 indicates the operation was successful with no error.

```
enroll.sh osptestserver.transnexus.com
```

```

Generating a 512 bit RSA private key
.....+++++
.+++++
writing new private key to 'pkey.pem'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: ████████
State or Province Name (full name) [Some-State]: ████████
Locality Name (eg, city) []: ████████
Organization Name (eg, company) [Internet Widgits Pty Ltd]: ████████
Organizational Unit Name (eg, section) []: ████████
Common Name (eg, YOUR name) []: ████████
Email Address []: ████████

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: ████████
An optional company name []: ████████

Error Code returned from openssl command : 0

CA certificate received
[SP: ospptestserver.transnexus.com]Error Code returned from getcacert
command : 0

output buffer after operation: operation=request
output buffer after nonce: operation=request&nonce=6096834216798074
X509 CertInfo context is null pointer
Unable to get Local Certificate
depth=0 /CN=ospptestserver.transnexus.com/O=OSPSPServer
verify error:num=18:self signed certificate
verify return:1
depth=0 /CN=ospptestserver.transnexus.com/O=OSPSPServer
verify return:1
The certificate request was successful.
Error Code returned from localcert command : 0

```

Note: `localcert.pem`, `pkey.pem` and `cacert_#.pem` files generated by the Enroll utility must be copied to the FreeRADIUS configuration directory (default `/usr/local/etc/raddb`).

6 Appendix-2 FreeRADIUS Example Files

6.1 stable

```

rlm_acctlog
rlm_acct_unique
rlm_always

```

```
rlm_attr_filter
rlm_attr_rewrite
rlm_chap
rlm_checkval
rlm_copy_packet
rlm_counter
rlm_dbm
rlm_detail
rlm_digest
rlm_eap
rlm_exec
rlm_expiration
rlm_expr
rlm_fastusers
rlm_files
rlm_ippool
rlm_krb5
rlm_ldap
rlm_linelog
rlm_logintime
rlm_mschap
rlm_ns_mta_md5
rlm_otp
rlm_pam
rlm_pap
rlm_passwd
rlm_perl
rlm_preprocess
rlm_python
rlm_radutmp
rlm_realm
rlm_sql
rlm_sqlcounter
rlm_sqlippool
rlm_sql_log
rlm_unix
rlm_policy
rlm_dynamic_clients
rlm_osp
```

6.2 *clients.conf*

```
# -*- text -*-
##
## clients.conf -- client configuration directives
##
##      $Id$

#####
##
#
# Define RADIUS clients (usually a NAS, Access Point, etc.).
```

```
#
# Defines a RADIUS client.
#
# '127.0.0.1' is another name for 'localhost'. It is enabled by
default,
# to allow testing of the server after an initial installation. If
you
# are not going to be permitting RADIUS queries from localhost, we
suggest
# that you delete, or comment out, this entry.
#
#
#
# Each client has a "short name" that is used to distinguish it from
# other clients.
#
# In version 1.x, the string after the word "client" was the IP
# address of the client. In 2.0, the IP address is configured via
# the "ipaddr" or "ipv6addr" fields. For compatibility, the 1.x
# format is still accepted.
#
client localhost {
    # Allowed values are:
    #     dotted quad (1.2.3.4)
    #     hostname   (radius.example.com)
    ipaddr = 127.0.0.1

    # OR, you can use an IPv6 address, but not both
    # at the same time.
#   ipv6addr = ::   # any.  ::1 == localhost

#
# A note on DNS: We STRONGLY recommend using IP addresses
# rather than host names. Using host names means that the
# server will do DNS lookups when it starts, making it
# dependent on DNS. i.e. If anything goes wrong with DNS,
# the server won't start!
#
# The server also looks up the IP address from DNS once, and
# only once, when it starts. If the DNS record is later
# updated, the server WILL NOT see that update.
#

# One client definition can be applied to an entire network.
# e.g. 127/8 should be defined with "ipaddr = 127.0.0.0" and
# "netmask = 8"
#
# If not specified, the default netmask is 32 (i.e. /32)
#
# We do NOT recommend using anything other than 32. There
# are usually other, better ways to achieve the same goal.
# Using netmasks of other than 32 can cause security issues.
#
# You can specify overlapping networks (127/8 and 127.0/16)
# In that case, the smallest possible network will be used
```

```

# as the "best match" for the client.
#
# Clients can also be defined dynamically at run time, based
# on any criteria. e.g. SQL lookups, keying off of NAS-
Identifier,
# etc.
# See raddb/sites-available/dynamic-clients for details.
#

# netmask = 32

#
# The shared secret use to "encrypt" and "sign" packets
between
# the NAS and FreeRADIUS. You MUST change this secret from
the
# default, otherwise it's not a secret any more!
#
# The secret can be any string, up to 8k characters in
length.
#
# Control codes can be entered vi octal encoding,
# e.g. "\101\102" == "AB"
# Quotation marks can be entered by escaping them,
# e.g. "foo\"bar"
#
# A note on security: The security of the RADIUS protocol
# depends COMPLETELY on this secret! We recommend using a
# shared secret that is composed of:
#
# upper case letters
# lower case letters
# numbers
#
# And is at LEAST 8 characters long, preferably 16
characters in
# length. The secret MUST be random, and should not be
words,
# phrase, or anything else that is recognizable.
#
# The default secret below is only for testing, and should
# not be used in any real environment.
#
secret = testing123

#
# Old-style clients do not send a Message-Authenticator
# in an Access-Request. RFC 5080 suggests that all clients
# SHOULD include it in an Access-Request. The configuration
# item below allows the server to require it. If a client
# is required to include a Message-Authenticator and it does
# not, then the packet will be silently discarded.
#
# allowed values: yes, no
require_message_authenticator = no

```

```

#
# The short name is used as an alias for the fully qualified
# domain name, or the IP address.
#
# It is accepted for compatibility with 1.x, but it is no
# longer necessary in 2.0
#
# shortname      = localhost

#
# the following three fields are optional, but may be used by
# checkrad.pl for simultaneous use checks
#

#
# The nastype tells 'checkrad.pl' which NAS-specific method
to
# use to query the NAS for simultaneous use.
#
# Permitted NAS types are:
#
#     cisco
#     computone
#     livingston
#     max40xx
#     multitech
#     netserver
#     pathras
#     patton
#     portslave
#     tc
#     usrhiper
#     other          # for all other types

#
nastype      = other      # localhost isn't usually a NAS...

#
# The following two configurations are for future use.
# The 'nasspasswd' file is currently used to store the NAS
# login name and password, which is used by checkrad.pl
# when querying the NAS for simultaneous use.
#
# login          = !root
# password       = someadminpas

#
# As of 2.0, clients can also be tied to a virtual server.
# This is done by setting the "virtual_server" configuration
# item, as in the example below.
#
# virtual_server = homel
}

# IPv6 Client
#client ::1 {

```

```

#       secret          = testing123
#       shortname       = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
#}

#client some.host.org {
#       secret          = testing123
#       shortname       = localhost
#}

#
# You can now specify one secret for a network of clients.
# When a client request comes in, the BEST match is chosen.
# i.e. The entry from the smallest possible network.
#
#client 192.168.0.0/24 {
#       secret          = testing123-1
#       shortname       = private-network-1
#}
#
#client 192.168.0.0/16 {
#       secret          = testing123-2
#       shortname       = private-network-2
#}

#client 10.10.10.10 {
#       # secret and password are mapped through the "secrets" file.
#       secret          = testing123
#       shortname       = liv1
#       # the following three fields are optional, but may be used by
#       # checkrad.pl for simultaneous usage checks
#       nastype         = livingston
#       login           = !root
#       password        = someadminpas
#}

#####
##
#
# Per-socket client lists. The configuration entries are exactly
# the same as above, but they are nested inside of a section.
#
# You can have as many per-socket client lists as you have "listen"
# sections, or you can re-use a list among multiple "listen"
sections.
#
# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combination
# will then accept ONLY the clients listed in this section.
#

```

```

#clients per_socket_clients {
#   client 192.168.3.4 {
#       secret = testing123
#   }
#}

# Transnexus RADIUS test configuration
client 172.16.4.0/24 {
    secret = testradius
    nastype = other
}

```

6.3 sites-available/default

```

#####
#
#
#   As of 2.0.0, FreeRADIUS supports virtual hosts using the
#   "server" section, and configuration directives.
#
#   Virtual hosts should be put into the "sites-available"
#   directory.  Soft links should be created in the "sites-
enabled"
#   directory to these files.  This is done in a normal
installation.
#
#   $Id$
#
#####
#
#
#   Read "man radiusd" before editing this file.  See the section
#   titled DEBUGGING.  It outlines a method where you can quickly
#   obtain the configuration you want, without running into
#   trouble.  See also "man unlang", which documents the format
#   of this file.
#
#   This configuration is designed to work in the widest possible
#   set of circumstances, with the widest possible number of
#   authentication methods.  This means that in general, you
should
#   need to make very few changes to this file.
#
#   The best way to configure the server for your local system
#   is to CAREFULLY edit this file.  Most attempts to make large
#   edits to this file will BREAK THE SERVER.  Any edits should
#   be small, and tested by running the server with "radiusd -X".
#   Once the edits have been verified to work, save a copy of
these
#   configuration files somewhere.  (e.g. as a "tar" file).
Then,
#   make more edits, and test, as above.
#
#   There are many "commented out" references to modules such

```

```

#       as ldap, sql, etc.  These references serve as place-holders.
#       If you need the functionality of that module, then configure
#       it in radiusd.conf, and un-comment the references to it in
#       this file.  In most cases, those small changes will result
#       in the server being able to connect to the DB, and to
#       authenticate users.
#
#####
#
#
#       In 1.x, the "authorize", etc. sections were global in
#       radiusd.conf.  As of 2.0, they SHOULD be in a server section.
#
#       The server section with no virtual server name is the
"default"
#       section.  It is used when no server name is specified.
#
#       We don't indent the rest of this file, because doing so
#       would make it harder to read.
#
# Authorization.  First preprocess (hints and huntgroups files),
# then realms, and finally look in the "users" file.
#
# The order of the realm modules will determine the order that
# we try to find a matching realm.
#
# Make *sure* that 'preprocess' comes before any realm if you
# need to setup hints for the remote radius server
authorize {
    #
    # The preprocess module takes care of sanitizing some
bizarre
attributes
    # attributes in the request, and turning them into
attributes
    # which are more standard.
    #
    # It takes care of processing the 'raddb/hints' and the
    # 'raddb/huntgroups' files.
    #
    # It also adds the %{Client-IP-Address} attribute to the
request.
    preprocess

    #
    # If you want to have a log of authentication requests,
    # un-comment the following line, and the 'detail auth_log'
    # section, above.
#       auth_log

    #
    # The chap module will set 'Auth-Type := CHAP' if we are
    # handling a CHAP request and Auth-Type has not already been
set
    chap

```

```

#
# If the users are logging in with an MS-CHAP-Challenge
# attribute for authentication, the mschap module will find
# the MS-CHAP-Challenge attribute, and add 'Auth-Type := MS-
CHAP'
# to the request, which will cause the server to then use
# the mschap module for authentication.
mschap

#
# If you have a Cisco SIP server authenticating against
# FreeRADIUS, uncomment the following line, and the 'digest'
# line in the 'authenticate' section.
# digest

#
# Look for IPASS style 'realm/', and if not found, look for
# '@realm', and decide whether or not to proxy, based on
# that.
# IPASS

#
# If you are using multiple kinds of realms, you probably
# want to set "ignore_null = yes" for all of them.
# Otherwise, when the first style of realm doesn't match,
# the other styles won't be checked.
#
suffix
# ntdomain

#
# This module takes care of EAP-MD5, EAP-TLS, and EAP-LEAP
# authentication.
#
# It also sets the EAP-Type attribute in the request
# attribute list to the EAP type from the packet.
#
# As of 2.0, the EAP module returns "ok" in the authorize
stage
# for TTLS and PEAP. In 1.x, it never returned "ok" here,
so
# this change is compatible with older configurations.
#
# The example below uses module failover to avoid querying
all
# of the following modules if the EAP module returns "ok".
# Therefore, your LDAP and/or SQL servers will not be
queried
# for the many packets that go back and forth to set up TTLS
# or PEAP. The load on those servers will therefore be
reduced.
#
eap {
    ok = return
}

```

```
#
# Pull crypt'd passwords from /etc/passwd or /etc/shadow,
# using the system API's to get the password.  If you want
# to read /etc/passwd or /etc/shadow directly, see the
# passwd module in radiusd.conf.
#
unix

#
# Read the 'users' file
files

#
# Look in an SQL database.  The schema of the database
# is meant to mirror the "users" file.
#
# See "Authorization Queries" in sql.conf
# sql

#
# If you are using /etc/smbpasswd, and are also doing
# mschap authentication, the un-comment this line, and
# configure the 'etc_smbpasswd' module, above.
# etc_smbpasswd

#
# The ldap module will set Auth-Type to LDAP if it has not
# already been set
# ldap

#
# Enforce daily limits on time spent logged in.
# daily

#
# Use the checkval module
# checkval

expiration
logintime

#
# If no other module has claimed responsibility for
# authentication, then try to use PAP.  This allows the
# other modules listed above to add a "known good" password
# to the request, and to do nothing else.  The PAP module
# will then see that password, and use it to do PAP
# authentication.
#
# This module should be listed last, so that the other
modules
# get a chance to set Auth-Type for themselves.
#
pap
```

```

#
# If "status_server = yes", then Status-Server messages are
passed
# through the following section, and ONLY the following
section.
# This permits you to do DB queries, for example. If the
modules
# listed here return "fail", then NO response is sent.
#
# Autz-Type Status-Server {
#
# }
#
# Authentication.
#
#
# This section lists which modules are available for authentication.
# Note that it does NOT mean 'try each module in order'. It means
# that a module from the 'authorize' section adds a configuration
# attribute 'Auth-Type := FOO'. That authentication type is then
# used to pick the appropriate module from the list below.
#
# In general, you SHOULD NOT set the Auth-Type attribute. The
server
# will figure it out on its own, and will do the right thing. The
# most common side effect of erroneously setting the Auth-Type
# attribute is that one authentication method will work, but the
# others will not.
#
# The common reasons to set the Auth-Type attribute by hand
# is to either forcibly reject the user (Auth-Type := Reject),
# or to or forcibly accept the user (Auth-Type := Accept).
#
# Note that Auth-Type := Accept will NOT work with EAP.
#
# Please do not put "unlang" configurations into the "authenticate"
# section. Put them in the "post-auth" section instead. That's
what
# the post-auth section is for.
#
authenticate {
#
# PAP authentication, when a back-end database listed
# in the 'authorize' section supplies a password. The
# password can be clear-text, or encrypted.
Auth-Type PAP {
    pap
}
#
# Most people want CHAP authentication
# A back-end database listed in the 'authorize' section
# MUST supply a CLEAR TEXT password. Encrypted passwords

```

```

# won't work.
Auth-Type CHAP {
    chap
}

#
# MSCHAP authentication.
Auth-Type MS-CHAP {
    mschap
}

#
# If you have a Cisco SIP server authenticating against
# FreeRADIUS, uncomment the following line, and the 'digest'
# line in the 'authorize' section.
#
# digest

#
# Pluggable Authentication Modules.
#
# pam

#
# See 'man getpwent' for information on how the 'unix'
# module checks the users password. Note that packets
# containing CHAP-Password attributes CANNOT be
authenticated
# against /etc/passwd! See the FAQ for details.
#
# unix

# Uncomment it if you want to use ldap for authentication
#
# Note that this means "check plain-text password against
# the ldap database", which means that EAP won't work,
# as it does not supply a plain-text password.
#
# Auth-Type LDAP {
#     ldap
# }

#
# Allow EAP authentication.
#
# eap
}

#
# Pre-accounting. Decide which accounting type to use.
#
# preacct {
#     preprocess

#
# Ensure that we have a semi-unique identifier for every
# request, and many NAS boxes are broken.
#
# acct_unique

```

```

#
# Look for IPASS-style 'realm/', and if not found, look for
# '@realm', and decide whether or not to proxy, based on
# that.
#
# Accounting requests are generally proxied to the same
# home server as authentication requests.
#
# IPASS
# suffix
# ntdomain

#
# Read the 'acct_users' file
# files
}

#
# Accounting. Log the accounting data.
#
accounting {
#
# Create a 'detail'ed log of the packets.
# Note that accounting requests which are proxied
# are also logged in the detail file.
# detail
# daily

# Update the wtmp file
#
# If you don't use "radlast", you can delete this line.
# unix

#
# For Simultaneous-Use tracking.
#
# Due to packet losses in the network, the data here
# may be incorrect. There is little we can do about it.
# radutmp
# sradutmp

# Return an address to the IP Pool when we see a stop
# record.
# main_pool

#
# Log traffic to an SQL database.
#
# See "Accounting queries" in sql.conf
# sql

#
# Instead of sending the query to the SQL server,
# write it into a log file.
#
# sql_log

```

```

# Cisco VoIP specific bulk accounting
pgsql-voip

# Filter attributes from the accounting response.
attr_filter.accounting_response

#
# See "Autz-Type Status-Server" for how this works.
#
# Acct-Type Status-Server {
#
# }

# Transnexus RADIUS test configuration
osp
}

# Session database, used for checking Simultaneous-Use. Either the
radutmp
# or rlm_sql module can handle this.
# The rlm_sql module is *much* faster
session {
    radutmp

    #
    # See "Simultaneous Use Checking Queries" in sql.conf
# sql
}

# Post-Authentication
# Once we KNOW that the user has been authenticated, there are
# additional steps we can take.
post-auth {
    # Get an address from the IP Pool.
# main_pool

    #
    # If you want to have a log of authentication replies,
    # un-comment the following line, and the 'detail reply_log'
    # section, above.
# reply_log

    #
    # After authenticating the user, do another SQL query.
    #
    # See "Authentication Logging Queries" in sql.conf
# sql

    #
    # Instead of sending the query to the SQL server,
    # write it into a log file.
    #
# sql_log

```

```

#
# Un-comment the following if you have set
# 'edir_account_policy_check = yes' in the ldap module sub-
section of
# the 'modules' section.
#
# ldap

exec

#
# Access-Reject packets are sent through the REJECT sub-
section of the
# post-auth section.
#
# Add the ldap module name (or instance) if you have set
# 'edir_account_policy_check = yes' in the ldap module
configuration
#
Post-Auth-Type REJECT {
    attr_filter.access_reject
}
}

#
# When the server decides to proxy a request to a home server,
# the proxied request is first passed through the pre-proxy
# stage. This stage can re-write the request, or decide to
# cancel the proxy.
#
# Only a few modules currently have this method.
#
pre-proxy {
#    attr_rewrite

#    Uncomment the following line if you want to change
attributes
#    as defined in the preproxy_users file.
#    files

#    Uncomment the following line if you want to filter
requests
#    sent to remote servers based on the rules defined in the
#    'attrs.pre-proxy' file.
#    attr_filter.pre-proxy

#    If you want to have a log of packets proxied to a home
#    server, un-comment the following line, and the
#    'detail_pre_proxy_log' section, above.
#    pre_proxy_log
}

#
# When the server receives a reply to a request it proxied
# to a home server, the request may be massaged here, in the
# post-proxy stage.

```

```

#
post-proxy {

    # If you want to have a log of replies from a home server,
    # un-comment the following line, and the 'detail
post_proxy_log'
    # section, above.
#     post_proxy_log

#     attr_rewrite

    # Uncomment the following line if you want to filter replies
from
    # remote proxies based on the rules defined in the 'attrs'
file.
#     attr_filter.post-proxy

#
# If you are proxying LEAP, you MUST configure the EAP
# module, and you MUST list it here, in the post-proxy
# stage.
#
# You MUST also use the 'nostrip' option in the 'realm'
# configuration. Otherwise, the User-Name attribute
# in the proxied request will not match the user name
# hidden inside of the EAP packet, and the end server will
# reject the EAP request.
#
#     eap

#
# If the server tries to proxy a request and fails, then the
# request is processed through the modules in this section.
#
# The main use of this section is to permit robust proxying
# of accounting packets. The server can be configured to
# proxy accounting packets as part of normal processing.
# Then, if the home server goes down, accounting packets can
# be logged to a local "detail" file, for processing with
# radrelay. When the home server comes back up, radrelay
# will read the detail file, and send the packets to the
# home server.
#
# With this configuration, the server always responds to
# Accounting-Requests from the NAS, but only writes
# accounting packets to disk if the home server is down.
#
#     Post-Proxy-Type Fail {
#         detail
#     }
}

```

6.4 dictionary for Acme Packet

```
#
# This is the master dictionary file, which references the
# pre-defined dictionary files included with the server.
#
# Any new/changed attributes MUST be placed in this file, as
# the pre-defined dictionaries SHOULD NOT be edited.
#
# $Id$
#
#
# The filename given here should be an absolute path.
#
$INCLUDE /usr/local/share/freeradius/dictionary

# Transnexus RADIUS test configuration
$INCLUDE /usr/local/share/freeradius/dictionary.acme

#
# Place additional attributes or $INCLUDEs here. They will
# over-ride the definitions in the pre-defined dictionaries.
#
# See the 'man' page for 'dictionary' for information on
# the format of the dictionary files.
#
#
# If you want to add entries to the dictionary file,
# which are NOT going to be placed in a RADIUS packet,
# add them here. The numbers you pick should be between
# 3000 and 4000.
#
#
#ATTRIBUTE My-Local-String 3000 string
#ATTRIBUTE My-Local-IPAddr 3001 ipaddr
#ATTRIBUTE My-Local-Integer 3002 integer
```

6.5 ACME dictionary

```
#
# dictionary.acme
#
# Accounting VSAs originally by
# Rick W. Porter <rporter@acmepacket.com>
#
# Version: dictionary.acme,v 1.0 2001/11/19
# Updated 2007/05/29 Sharon Paisner
#
# For documentation on Acme Packet RADIUS attributes, see:
#
# Acme Packet RADIUS Design specification
#
```

```

VENDOR          Acme          9148

#
# Voice over IP attributes.
#
BEGIN-VENDOR    Acme

ATTRIBUTE       Acme-FlowID_FS1_F          1
string

ATTRIBUTE       Acme-FlowType_FS1_F          2
string

ATTRIBUTE       Acme-Session-Ingress-CallId  3
string

ATTRIBUTE       Acme-Session-Egress-CallId  4
string

ATTRIBUTE       Acme-Flow-In-Realm_FS1_F     10
string

ATTRIBUTE       Acme-Flow-In-Src-Addr_FS1_F  11
ipaddr

ATTRIBUTE       Acme-Flow-In-Src-Port_FS1_F  12
integer

ATTRIBUTE       Acme-Flow-In-Dst-Addr_FS1_F  13
ipaddr

ATTRIBUTE       Acme-Flow-In-Dst-Port_FS1_F  14
integer

ATTRIBUTE       Acme-Flow-Out-Realm_FS1_F     20
string

ATTRIBUTE       Acme-Flow-Out-Src-Addr_FS1_F  21
ipaddr

ATTRIBUTE       Acme-Flow-Out-Src-Port_FS1_F  22
integer

ATTRIBUTE       Acme-Flow-Out-Dst-Addr_FS1_F  23
ipaddr

ATTRIBUTE       Acme-Flow-Out-Dst-Port_FS1_F  24
integer

ATTRIBUTE       Acme-Calling-Octets_FS1       28
integer

ATTRIBUTE       Acme-Calling-Packets_FS1      29
integer

ATTRIBUTE       Acme-Calling-RTCP-Packets-Lost_FS1  32
integer

ATTRIBUTE       Acme-Calling-RTCP-Avg-Jitter_FS1  33
integer

ATTRIBUTE       Acme-Calling-RTCP-Avg-Latency_FS1  34
integer

ATTRIBUTE       Acme-Calling-RTCP-MaxJitter_FS1  35
integer

ATTRIBUTE       Acme-Calling-RTCP-MaxLatency_FS1  36
integer

ATTRIBUTE       Acme-Calling-RTP-Packets-Lost_FS1  37
integer

```

ATTRIBUTE integer	Acme-Calling-RTP-Avg-Jitter_FS1	38
ATTRIBUTE integer	Acme-Calling-RTP-MaxJitter_FS1	39
ATTRIBUTE string	Acme-Session-Generic-Id	40
ATTRIBUTE string	Acme-Session-Ingress-Realm	41
ATTRIBUTE string	Acme-Session-Egress-Realm	42
ATTRIBUTE string	Acme-Session-Protocol-Type	43
ATTRIBUTE integer	Acme-Called-Octets_FS1	44
ATTRIBUTE integer	Acme-Called-Packets_FS1	45
ATTRIBUTE integer	Acme-Called-RTCP-Packets-Lost_FS1	46
ATTRIBUTE integer	Acme-Called-RTCP-Avg-Jitter_FS1	47
ATTRIBUTE integer	Acme-Called-RTCP-Avg-Latency_FS1	48
ATTRIBUTE integer	Acme-Called-RTCP-MaxJitter_FS1	49
ATTRIBUTE integer	Acme-Called-RTCP-MaxLatency_FS1	50
ATTRIBUTE integer	Acme-Called-RTP-Packets-Lost_FS1	51
ATTRIBUTE integer	Acme-Called-RTP-Avg-Jitter_FS1	52
ATTRIBUTE integer	Acme-Called-RTP-MaxJitter_FS1	53
ATTRIBUTE string	Acme-Session-Charging-Vector	54
ATTRIBUTE string	Acme-Session-Charging-Function_Address	55
ATTRIBUTE string	Acme-Firmware-Version	56
ATTRIBUTE string	Acme-Local-Time-Zone	57
ATTRIBUTE integer	Acme-Post-Dial-Delay	58
ATTRIBUTE integer	Acme-CDR-Sequence-Number	59
ATTRIBUTE integer	Acme-Session-Disposition	60
ATTRIBUTE integer	Acme-Disconnect-Initiator	61
ATTRIBUTE integer	Acme-Disconnect-Cause	62

ATTRIBUTE string	Acme-Intermediate_Time	63
ATTRIBUTE string	Acme-Primary-Routing-Number	64
ATTRIBUTE string	Acme-Originating-Trunk-Group	65
ATTRIBUTE string	Acme-Terminating-Trunk-Group	66
ATTRIBUTE string	Acme-Originating-Trunk-Context	67
ATTRIBUTE string	Acme-Terminating-Trunk-Context	68
ATTRIBUTE string	Acme-P-Asserted-ID	69
ATTRIBUTE string	Acme-SIP-Diversion	70
ATTRIBUTE integer	Acme-SIP-Status	71
# 72 unused		
# 73 unused		
ATTRIBUTE string	Acme-Ingress-Local-Addr	74
ATTRIBUTE string	Acme-Ingress-Remote-Addr	75
ATTRIBUTE string	Acme-Egress-Local-Addr	76
ATTRIBUTE string	Acme-Egress-Remote-Addr	77
ATTRIBUTE string	Acme-FlowID_FS1_R	78
ATTRIBUTE string	Acme-FlowType_FS1_R	79
ATTRIBUTE string	Acme-Flow-In-Realm_FS1_R	80
ATTRIBUTE ipaddr	Acme-Flow-In-Src-Addr_FS1_R	81
ATTRIBUTE integer	Acme-Flow-In-Src-Port_FS1_R	82
ATTRIBUTE ipaddr	Acme-Flow-In-Dst-Addr_FS1_R	83
ATTRIBUTE integer	Acme-Flow-In-Dst-Port_FS1_R	84
ATTRIBUTE string	Acme-Flow-Out-Realm_FS1_R	85
ATTRIBUTE ipaddr	Acme-Flow-Out-Src-Addr_FS1_R	86
ATTRIBUTE integer	Acme-Flow-Out-Src-Port_FS1_R	87
ATTRIBUTE ipaddr	Acme-Flow-Out-Dst-Addr_FS1_R	88
ATTRIBUTE integer	Acme-Flow-Out-Dst-Port_FS1_R	89
ATTRIBUTE string	Acme-FlowID_FS2_F	90
ATTRIBUTE string	Acme-FlowType_FS2_F	91

ATTRIBUTE string	Acme-Flow-In-Realm_FS2_F	92
ATTRIBUTE ipaddr	Acme-Flow-In-Src-Addr_FS2_F	93
ATTRIBUTE integer	Acme-Flow-In-Src-Port_FS2_F	94
ATTRIBUTE ipaddr	Acme-Flow-In-Dst-Addr_FS2_F	95
ATTRIBUTE integer	Acme-Flow-In-Dst-Port_FS2_F	96
ATTRIBUTE string	Acme-Flow-Out-Realm_FS2_F	97
ATTRIBUTE ipaddr	Acme-Flow-Out-Src-Addr_FS2_F	98
ATTRIBUTE integer	Acme-Flow-Out-Src-Port_FS2_F	99
ATTRIBUTE ipaddr	Acme-Flow-Out-Dst-Addr_FS2_F	100
ATTRIBUTE integer	Acme-Flow-Out-Dst-Port_FS2_F	101
ATTRIBUTE integer	Acme-Calling-Octets_FS2	102
ATTRIBUTE integer	Acme-Calling-Packets_FS2	103
ATTRIBUTE integer	Acme-Calling-RTCP-Packets-Lost_FS2	104
ATTRIBUTE integer	Acme-Calling-RTCP-Avg-Jitter_FS2	105
ATTRIBUTE integer	Acme-Calling-RTCP-Avg-Latency_FS2	106
ATTRIBUTE integer	Acme-Calling-RTCP-MaxJitter_FS2	107
ATTRIBUTE integer	Acme-Calling-RTCP-MaxLatency_FS2	108
ATTRIBUTE integer	Acme-Calling-RTP-Packets-Lost_FS2	109
ATTRIBUTE integer	Acme-Calling-RTP-Avg-Jitter_FS2	110
ATTRIBUTE integer	Acme-Calling-RTP-MaxJitter_FS2	111
ATTRIBUTE string	Acme-FlowID_FS2_R	112
ATTRIBUTE string	Acme-FlowType_FS2_R	113
ATTRIBUTE string	Acme-Flow-In-Realm_FS2_R	114
ATTRIBUTE ipaddr	Acme-Flow-In-Src-Addr_FS2_R	115
ATTRIBUTE integer	Acme-Flow-In-Src-Port_FS2_R	116
ATTRIBUTE ipaddr	Acme-Flow-In-Dst-Addr_FS2_R	117
ATTRIBUTE integer	Acme-Flow-In-Dst-Port_FS2_R	118

ATTRIBUTE	Acme-Flow-Out-Realm_FS2_R	119
string		
ATTRIBUTE	Acme-Flow-Out-Src-Addr_FS2_R	120
ipaddr		
ATTRIBUTE	Acme-Flow-Out-Src-Port_FS2_R	121
integer		
ATTRIBUTE	Acme-Flow-Out-Dst-Addr_FS2_R	122
ipaddr		
ATTRIBUTE	Acme-Flow-Out-Dst-Port_FS2_R	123
integer		
ATTRIBUTE	Acme-Called-Octets_FS2	124
integer		
ATTRIBUTE	Acme-Called-Packets_FS2	125
integer		
ATTRIBUTE	Acme-Called-RTCP-Packets-Lost_FS2	126
integer		
ATTRIBUTE	Acme-Called-RTCP-Avg-Jitter_FS2	127
integer		
ATTRIBUTE	Acme-Called-RTCP-Avg-Latency_FS2	128
integer		
ATTRIBUTE	Acme-Called-RTCP-MaxJitter_FS2	129
integer		
ATTRIBUTE	Acme-Called-RTCP-MaxLatency_FS2	130
integer		
ATTRIBUTE	Acme-Called-RTP-Packets-Lost_FS2	131
integer		
ATTRIBUTE	Acme-Called-RTP-Avg-Jitter_FS2	132
integer		
ATTRIBUTE	Acme-Called-RTP-MaxJitter_FS2	133
integer		
ATTRIBUTE	Acme-Egress-Final-Routing-Number	134
string		
ATTRIBUTE	Acme-Session-Ingress-RPH	135
string		
ATTRIBUTE	Acme-Session-Egress-RPH	136
string		
ATTRIBUTE	Acme-Ingress-Network-Interface-Id	137
string		
ATTRIBUTE	Acme-Ingress-Vlan-Tag-Value	138
integer		
ATTRIBUTE	Acme-Egress-Network-Interface-Id	139
string		
ATTRIBUTE	Acme-Egress-Vlan-Tag-Value	140
integer		
ATTRIBUTE	Acme-Refer-Call-Transfer-Id	141
string		
# Attributes 142-150 are taken from CYPHER, they are reserved.		
#ATTRIBUTE	Acme-FlowMediaType_FS1_F	142
string		
#ATTRIBUTE	Acme-FlowMediaType_FS1_R	143
string		
#ATTRIBUTE	Acme-FlowMediaType_FS2_F	144
string		
#ATTRIBUTE	Acme-FlowMediaType_FS2_R	145
string		

#ATTRIBUTE integer	Acme-Flow-PTime_FS1_F	146
#ATTRIBUTE integer	Acme-Flow-PTime_FS1_R	147
#ATTRIBUTE integer	Acme-Flow-PTime_FS2_F	148
#ATTRIBUTE integer	Acme-Flow-PTime_FS2_R	149
#ATTRIBUTE string	Acme-Session-Media-Process	150
ATTRIBUTE integer	Acme-Calling-R-Factor	151
ATTRIBUTE integer	Acme-Calling-MOS	152
ATTRIBUTE integer	Acme-Called-R-Factor	153
ATTRIBUTE integer	Acme-Called-MOS	154
## Reserved for	IPV6 attributes	
#ATTRIBUTE ipv6addr	Acme-Flow-In-Src-IPv6_Addr_FS1_F	155
#ATTRIBUTE ipv6addr	Acme-Flow-In-Dst-IPv6_Addr_FS1_F	156
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Src-IPv6_Addr_FS1_F	157
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Dst-IPv6_Addr_FS1_F	158
#ATTRIBUTE ipv6addr	Acme-Flow-In-Src-IPv6_Addr_FS1_R	159
#ATTRIBUTE ipv6addr	Acme-Flow-In-Dst-IPv6_Addr_FS1_R	160
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Src-IPv6_Addr_FS1_R	161
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Dst-IPv6_Addr_FS1_R	162
#ATTRIBUTE ipv6addr	Acme-Flow-In-Src-IPv6_Addr_FS2_F	163
#ATTRIBUTE ipv6addr	Acme-Flow-In-Dst-IPv6_Addr_FS2_F	164
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Src-IPv6_Addr_FS2_F	165
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Dst-IPv6_Addr_FS2_F	166
#ATTRIBUTE ipv6addr	Acme-Flow-In-Src-IPv6_Addr_FS2_R	167
#ATTRIBUTE ipv6addr	Acme-Flow-In-Dst-IPv6_Addr_FS2_R	168
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Src-IPv6_Addr_FS2_R	169
#ATTRIBUTE ipv6addr	Acme-Flow-Out-Dst-IPv6_Addr_FS2_R	170
#ATTRIBUTE string	Acme-Session-Forked-Call-Id	171
ATTRIBUTE string	Acme-Custom-VSA-200	200

ATTRIBUTE string	Acme-Custom-VSA-201	201
ATTRIBUTE string	Acme-Custom-VSA-202	202
ATTRIBUTE string	Acme-Custom-VSA-203	203
ATTRIBUTE string	Acme-Custom-VSA-204	204
ATTRIBUTE string	Acme-Custom-VSA-205	205
ATTRIBUTE string	Acme-Custom-VSA-206	206
ATTRIBUTE string	Acme-Custom-VSA-207	207
ATTRIBUTE string	Acme-Custom-VSA-208	208
ATTRIBUTE string	Acme-Custom-VSA-209	209
ATTRIBUTE string	Acme-Custom-VSA-210	210
ATTRIBUTE string	Acme-Custom-VSA-211	211
ATTRIBUTE string	Acme-Custom-VSA-212	212
ATTRIBUTE string	Acme-Custom-VSA-213	213
ATTRIBUTE string	Acme-Custom-VSA-214	214
ATTRIBUTE string	Acme-Custom-VSA-215	215
ATTRIBUTE string	Acme-Custom-VSA-216	216
ATTRIBUTE string	Acme-Custom-VSA-217	217
ATTRIBUTE string	Acme-Custom-VSA-218	218
ATTRIBUTE string	Acme-Custom-VSA-219	219
ATTRIBUTE string	Acme-Custom-VSA-220	220
ATTRIBUTE string	Acme-Custom-VSA-221	221
ATTRIBUTE string	Acme-Custom-VSA-222	222
ATTRIBUTE string	Acme-Custom-VSA-223	223
ATTRIBUTE string	Acme-Custom-VSA-224	224
ATTRIBUTE string	Acme-Custom-VSA-225	225
ATTRIBUTE string	Acme-Custom-VSA-226	226
ATTRIBUTE string	Acme-Custom-VSA-227	227
ATTRIBUTE string	Acme-Custom-VSA-228	228

ATTRIBUTE string	Acme-Custom-VSA-229	229
ATTRIBUTE string	Acme-Custom-VSA-230	230
ATTRIBUTE string	Acme-User-Class	254
END-VENDOR	Acme	

7 Appendix-3 Acme Packet SBC configurations

```

acmesystem# show running-config
account-config
    hostname                localhost
    port                    1813
    strategy                Hunt
    state                   enabled
    max-msg-delay           60
    max-wait-failover       100
    trans-at-close          disabled
    file-output             disabled
    max-file-size           1000000
    max-files               5
    file-path
    file-rotate-time        0
    ftp-push                disabled
    ftp-address
    ftp-port                21
    ftp-user
    ftp-password
    ftp-remote-path
    cdr-output-redundancy   enabled
    generate-start          OK
    generate-interim
                                Unsuccessful-Attempt
    intermediate-period     0
    prevent-duplicate-attrs disabled
    vsa-id-range
    cdr-output-inclusive    disabled
    account-server
        hostname            172.16.4.47
        port                 1813
        state                enabled
        min-round-trip       250
        max-inactivity        60
        restart-delay         30
        bundle-vsa           enabled
        secret                testradius
        NAS-ID
        priority              0
    last-modified-by        admin@172.16.4.7
    last-modified-date      2009-07-02 21:43:36

```

```

local-policy
  from-address
                                     *
  to-address
                                     *
  source-realm
                                     acmerealms
  description
  activate-time
                                     N/A
  deactivate-time
                                     N/A
  state
                                     enabled
  policy-priority
                                     none
  last-modified-by
  last-modified-date
                                     2009-05-05 02:42:11
  policy-attribute
    next-hop
                                     sipproxys
    realm
                                     acmerealms
    action
                                     none
    terminate-recursion
                                     disabled
    carrier
  start-time
                                     0000
  end-time
                                     2400
  days-of-week
                                     U-S
  cost
                                     0
  app-protocol
  state
                                     enabled
  methods
  media-profiles
media-manager
  state
                                     enabled
  latching
                                     enabled
  flow-time-limit
                                     86400
  initial-guard-timer
                                     300
  subsq-guard-timer
                                     300
  tcp-flow-time-limit
                                     86400
  tcp-initial-guard-timer
                                     300
  tcp-subsq-guard-timer
                                     300
  tcp-number-of-ports-per-flow
                                     2
  hnt-rtcp
                                     disabled
  algd-log-level
                                     NOTICE
  mbc-d-log-level
                                     NOTICE
  red-flow-port
                                     1985
  red-mgcp-port
                                     1986
  red-max-trans
                                     10000
  red-sync-start-time
                                     5000
  red-sync-comp-time
                                     1000
  media-policing
                                     enabled
  max-signaling-bandwidth
                                     10000000
  max-untrusted-signaling
                                     100
  min-untrusted-signaling
                                     30
  app-signaling-bandwidth
                                     0
  tolerance-window
                                     30
  rtcp-rate-limit
                                     0
  min-media-allocation
                                     32000
  min-trusted-allocation
                                     1000
  deny-allocation
                                     1000

```

```

anonymous-sdp                disabled
arp-msg-bandwidth             32000
fragment-msg-bandwidth        0
rfc2833-timestamp             disabled
default-2833-duration         100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event   disabled
dnssalg-server-failover       disabled
last-modified-by
last-modified-date            2009-05-05 02:44:41
network-interface
name                           eth0
sub-port-id                     0
description
hostname
ip-address                     172.16.4.146
pri-utility-addr
sec-utility-addr
netmask                       255.255.0.0
gateway                       172.16.4.1
sec-gateway
gw-heartbeat
state                          disabled
heartbeat                      0
retry-count                    0
retry-timeout                  1
health-score                   0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                    11
hip-ip-list
ftp-address
icmp-address
snmp-address
telnet-address
last-modified-by
last-modified-date            2009-05-05 02:47:27
ntp-config
server                        208.113.193.10
last-modified-by
last-modified-date            2009-05-05 02:48:24
phy-interface
name                           eth0
operation-type                 Media
port                           0
slot                           0
virtual-mac
admin-state                    enabled
auto-negotiation               enabled
duplex-mode                    FULL
speed                          100
last-modified-by
last-modified-date            2009-05-05 02:49:13
realm-config

```

identifier	acmerealms
description	
addr-prefix	172.16.4.0/24
network-interfaces	eth0:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
qos-enable	enabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled

codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
last-modified-by	
last-modified-date	2009-05-05 02:52:00
session-agent	
hostname	sipproxy
ip-address	172.16.4.47
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	

```

out-translationid
trust-me disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
last-modified-by admin@172.16.4.7
last-modified-date 2009-07-02 21:16:19
sip-config
state enabled
operation-mode dialog
dialog-transparency disabled
home-realm-id acmerealms
egress-realm-id
nat-mode None
registrar-domain
registrar-host
registrar-port 0
register-service-route always
init-timer 500
max-timer 4000
trans-expire 5
invite-expire 180
inactive-dynamic-conn 32
enforcement-profile
pac-method
pac-interval 10
pac-strategy PropDist
pac-load-weight 1
pac-session-weight 1
pac-route-weight 1
pac-callid-lifetime 600
pac-user-lifetime 3600
red-sip-port 1988
red-max-trans 10000
red-sync-start-time 5000

```

```

red-sync-comp-time          1000
add-reason-header           disabled
sip-message-len             4096
enum-sag-match              disabled
extra-method-stats         disabled
registration-cache-limit    0
register-use-to-for-lp      disabled
add-ucid-header            disabled
last-modified-by
last-modified-date         2009-05-05 02:55:03
sip-interface
state                       enabled
realm-id                   acmerealms
description
sip-port
    address                  172.16.4.146
    port                     5060
    transport-protocol       UDP
    tls-profile
    allow-anonymous          all
    ims-aka-profile
carriers
trans-expire                0
invite-expire                0
max-redirect-contacts       0
proxy-mode
redirect-action             Recurse
contact-mode                 none
nat-traversal                none
nat-interval                 30
tcp-nat-interval            90
registration-caching         disabled
min-reg-expire               300
registration-interval        3600
route-to-registrar          disabled
secured-network              disabled
teluri-scheme                disabled
uri-fqdn-domain
trust-mode                   all
max-nat-interval             3600
nat-int-increment            10
nat-test-increment           30
sip-dynamic-hnt              disabled
stop-recurse                 401,407
port-map-start                0
port-map-end                  0
in-manipulationid            customVSA
out-manipulationid
manipulation-string
sip-ims-feature              disabled
operator-identifier
anonymous-priority           none
max-incoming-conns           0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout         0
untrusted-conn-timeout       0

```

```

network-id
ext-policy-server
default-location-string
charging-vector-mode          pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                none
implicit-service-route        disabled
rfc2833-payload               101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
refer-call-transfer            disabled
route-unauthorized-calls
tcp-keepalive                 none
add-sdp-invite                 disabled
add-sdp-profiles
last-modified-by
last-modified-date            2009-05-05 02:58:01
sip-manipulation
  name                          customVSA
  description
  header-rule
    name                         storeFrom
    header-name                   From
    action                         store
    comparison-type               pattern-rule
    match-value                    .*
    msg-type                       request
    new-value
    methods                         INVITE
  header-rule
    name                         createVSA200
    header-name                   P-Acme-VSA
    action                         add
    comparison-type               case-sensitive
    match-value
    msg-type                       any
    new-value                       200:+$storeFrom.$0
    methods                         INVITE
  last-modified-by
  last-modified-date            2009-05-05 03:09:36
steering-pool
  ip-address                     172.16.4.146
  start-port                      6000
  end-port                        6999
  realm-id                       acmerealm
  network-interface
  last-modified-by
  last-modified-date            2009-05-05 03:02:54
system-config
  hostname                       acme

```

```

description                    Transnexus-ACME
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled                   enabled
enable-snmp-auth-traps        disabled
enable-snmp-syslog-notify     disabled
enable-snmp-monitor-traps     disabled
enable-env-monitor-traps      disabled
snmp-syslog-his-table-length  1
snmp-syslog-level             WARNING
system-log-level              WARNING
process-log-level             NOTICE
process-log-ip-address        0.0.0.0
process-log-port              0
collect
    sample-interval            5
    push-interval              15
    boot-state                 disabled
    start-time                 now
    end-time                   never
    red-collect-state          disabled
    red-max-trans              1000
    red-sync-start-time       5000
    red-sync-comp-time        1000
    push-success-trap-state    disabled
call-trace                     disabled
internal-trace                 disabled
log-filter                    all
default-gateway               172.16.4.1
restart                       enabled
exceptions
telnet-timeout                0
console-timeout               0
remote-control                enabled
cli-audit-trail               enabled
link-redundancy-state         disabled
source-routing                disabled
cli-more                      disabled
terminal-height               24
debug-timeout                 0
trap-event-lifetime           0
last-modified-by              admin@172.16.5.2
last-modified-date            2009-05-07 01:57:06

```

task done