Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-C(X)6.2.0
Formerly Net-Net Session Director

September 2013

ORACLE

Notices

Contents

Preface

About this guide

The Net-Net S-C(X)6.2.0 Maintenance Release Guide provides information about the contents of maintenance releases related to Net-Net OS S-C(X)6.2.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release of the Net-Net OS from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting Net-Net OS S-C(X)6.2.0, this document informs you of changes made to the Net-Net OS software in the maintenance releases of S-C(X)6.2.0. Consult this document for content specific to maintenance releases. For information about general Net-Net OS features, configuration, and maintenance, consult the Related Documentation (iv) listed in the section below and then refer to the applicable document.

Organization

The Net-Net S-C(X)6.2.0 3000 and 4000 Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix (iii), showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Acme Packet has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Maintenance Release Availability Matrix

The table below lists the availability for version S-C(X)6.2.0 maintenance releases.

Maintenance release number	Availability Notes
S-CX6.2.0M1	March 23, 2010
S-CX6.2.0M2	May 5, 2010

Maintenance release number	Availability Notes
S-CX6.2.0M3	June 18, 2010
S-CX6.2.0M4	October 27, 2010
S-CX6.2.0M5	January 31, 2011
S-CX6.2.0M6	April 15, 2011
S-CX6.2.0M7	October 21, 2011
S-CX6.2.0M8	November 3, 2011
S-CX6.2.0M9	February 3, 2012
S-CX6.2.0M10	February 28, 2012
S-CX6.2.0M11	March 28, 2012
S-CX6.2.0M12	January 11, 2013

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Net-Net 4500 System Hardware Installation Guide (400-0101-00)	Contains information about the components and installation of the Net-Net 4500 system.
Net-Net 3800 Hardware Installation Guide (400-0118-00)	Contains information about the components and installation of the Net-Net 3800 system.
Net-Net 3000 & 4000 Release Notes (400-0066-00)	Contains information about the current documentation set release, including new features and management changes.
Net-Net 4000 ACLI Configuration Guide (400-0061-00)	Contains information about the administration and software configuration of the Net-Net SBC.
Net-Net 4000 ACLI Reference Guide (400-0062-00)	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Net-Net 4000 Maintenance and Troubleshooting Guide (400-0063-00)	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
Net-Net 4000 MIB Reference Guide (400-0010-00)	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Net-Net 4000 Accounting Guide (400-0015-00)	Contains information about the Net-Net SBC's accounting support, including details about RADIUS accounting.

1

S-C(X)6.2.0M1

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M1.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M1.

Content Type	Description
Defect	So that comma-separated SIP header values can be treated as multiple headers when HMR is performed, two parameters are part of the SIP manipulation configuration. split-headers — Defines a list of SIP headers with comma-separated values for the Net-Net SBC to split into multiple headers with individual values each with its own line. Splitting takes place prior to SIP manipulation execution. join-headers — Defines a list of SIP headers the Net-Net SBC will combine into a single header with its values separated by commas. Joining takes place after all SIP manipulations have been executed. You set both parameters in the sip-manipulation configuration.
Forward Merge	S-C6.1.0M3 Adaptations & Defect Fixes
Forward Merge	S-C6.1.0M4 Adaptations & Defect Fixes

2

S-C(X)6.2.0M2

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M2.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M2.

Content Type	Description
Adaptation	1814 - TLS Endpoint Certificate Data Caching
Adaptation	2246 - NMC before E-CSCF
Adaptation	2251 - Secure and Nonsecure flows in same realm

TLS Endpoint Certificate Data Caching

To provide a higher level of security for unified messaging (UM), the Net-Net SBC allows you configure enforcement profiles to cache data from TLS certificates. During the authentication process, the system caches the data so it can use that data in subsequent SIP message processing. Thus the Net-Net SBC can:

- Add custom SIP header populated with information from TLS certificates—When the Net-Net SBC receives an INVITE from a GW, it can write proprietary headers into the SIP message. It uses the certificate information the GW provided during the TLS authentication process with the Net-Net SBC to do so.
- Compare the host of the Request-URI with information from TLS certificates—When an INVITE is destined for the unified messaging server, the Net-Net SBC checks the domain of the Request-URI it has generated prior to HMR application. It does so to verify that the Request-URI matches the domain information the UM server provided during the TLS authentication process with the Net-Net SBC.

TLS endpoint certificate data caching can only applies to call-creating SIP INVITEs. The Net-Net SBC looks to the following configurations, in order, to apply an enforcement profile: session agent, realm, and SIP interface associated with the INVITE. As a final step, it checks the SIP profile for enforcement profile association.

Inserting Customized SIP Headers in an Outgoing INVITE

Whenever theNet-Net SBC establishes a new TLS connection, it caches these peer certificate attributes:

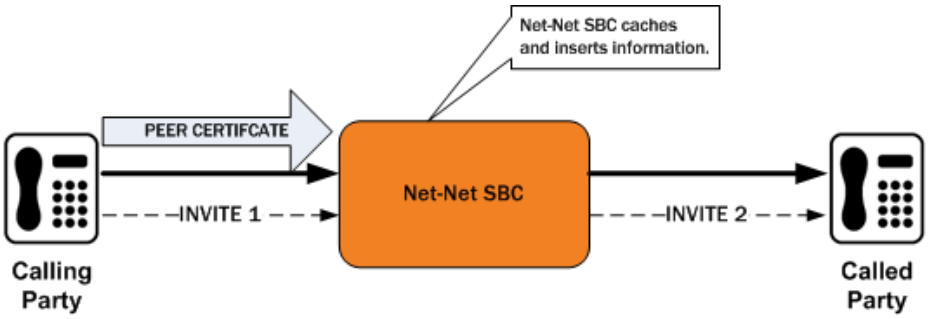
- Certificate Subject Name

- Certificate Subject Alternative Name (only DNS)

TheNet-Net SBC constructs a customized P-Certificate-Subject-Common-Name SIP header and inserts it into the outgoing INVITE with the Certificate Subject Name. It also constructs and inserts in the outgoing INVITE one or more P-Certificate-Subject-Alternative-Name SIP headers.

If you enable this capability and the incoming INVITE already has P-Certificate-Subject-Common-Name and P-Certificate-Subject-Alternative-Name headers, the Net-Net SBC strips them before insert the new customized ones. It does so to avoid the risk of any attempt to spoof the headers and thereby gain unauthorized access to the UM server.

This diagram shows a scenario where the calling party establishes a TLS connection with the Net-Net SBC. Because mutual authentication is enabled, the Net-Net SBC receives the peer certificate and caches required information from it. This information is inserted in the outgoing INVITE.



The peer certificate from the calling party during the TLS handshake with the Net-Net SBC would look like this. Relevant information in the sample appears in bold font.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=MA, L=Woburn, O=Smith Securities, OU=Certificate
Authority Dept, CN=Smith Certificate Authority/emailAddress=Smith@CA.com
        Validity
            Not Before: Dec 10 21:14:56 2009 GMT
            Not After : Jul 11 21:14:56 2019 GMT
        Subject: C=US, ST=MA, L=Burlington, O=Acme Packet, OU=Certificate
Authority Dept, CN=*.acme.com/emailAddress=ph1Client@acme.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
        X509v3 extensions:
            X509v3 Basic Constraints:
            CA:FALSE
            X509v3 Issuer Alternative Name:
            email:Smith@CA.com
            X509v3 Subject Alternative Name:
            DNS:gw1.acme.com, DNS:gw3.ano.com, DNS:gw2.some.com
            X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
    Signature Algorithm: sha1WithRSAEncryption
```

The outgoing SIP INVITE (INVITE 2 in the diagram) would then look like the sample below. You can see where the Net-Net SBC uses information from the certificate; the text is bold.

```
INVITE sip:222222@acme.com:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.27.113:5060;branch=z9hG4bK4jmg29cmm8l0cg7smmrn85o4q7
From: 111111 <sip:111111@acme.com>;tag=_ph1_tag
To: 222222 <sip:222222@acme.com>
Call-ID: _1-2_call_id-10147@acme.com-1-
CSeq: 1 INVITE
Contact: <sip:111111@172.16.27.113:5060;transport=udp>
```

```
P-Certificate-Subject-Common-Name: *.acme.com
P-Certificate-Subject-Alternative-Name: gw1.acme.com
P-Certificate-Subject-Alternative-Name: gw3.ano.com
P-Certificate-Subject-Alternative-Name: gw2.some.com
Max-Forwards: 69
Subject: TBD
Content-Type: application/sdp
Content-Length: 138
Route: <sip:222222@172.16.27.188:5060;lr>
v=0
o=user1 53655765 2353687637 IN IP4 172.16.27.113
s=-
c=IN IP4 172.16.27.113
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Validating the Request-URI Based on Certificate Information

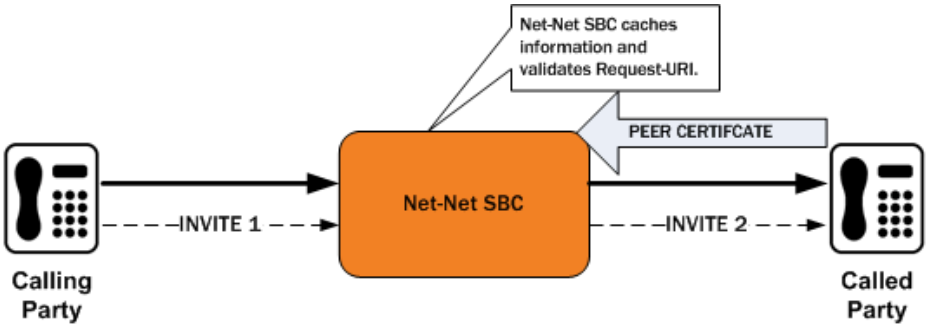
When you configure the Net-Net SBC to cache TLS certificate information to validate Request-URIs, it stores the Certificate Subject Name and Certificate Subject Alternative Name (only DNS) it learns from peer certificate attributes. It then takes these actions:

- Extracts the host from the Request-URI of the outgoing INVITE
- Compares this host (exact or wildcard match) with the Certificate Common Name or Certificate Subject Alternative name of the certificate it has received
- Sends out an INVITE if the Certificate Common Name or Certificate Subject Alternative name match; Sends a 403 Forbidden rejection to the endpoint from it received the INVITE if there is no match

Wildcard matching applies only to the prefix of the Request-URI:

```
*.acme.com
    *.*.acmepacket.com
```

This diagram shows a peering scenario where the Net-Net SBC receives an INVITE from the calling party, which it processes and prepares to send out INVITE 2. After establishing a TLS connection with the called party and caching the required information, the Net-Net SBC validates the Request-URI. Once validation occurs, the Net-Net SBC sends INVITE 2.



The peer certificate from the called party during the TLS handshake with the Net-Net SBC would look like this. Relevant information in the sample appears in bold font.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=MA, L=Woburn, O=Smith Securities, OU=Certificate
Authority Dept, CN=Smith Certificate Authority/emailAddress=amith@CA.com
        Validity
            Not Before: Dec 10 21:14:56 2009 GMT
            Not After : Jul 11 21:14:56 2019 GMT
```

```
        Subject: C=US, ST=MA, L=Woburn, O=Acme Packet, OU=Certificate
Authority Dept, CN=*.acme.com/emailAddress=ph2Server@acme.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
        X509v3 extensions:
            X509v3 Basic Constraints:
            CA:FALSE
            X509v3 Issuer Alternative Name:
            email:Smith@CA.com
            X509v3 Subject Alternative Name:
            DNS:gw1.acme.com, DNS:*.ano.com, DNS:*.some.com
            X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
    Signature Algorithm: sha1WithRSAEncryption
```

The outgoing SIP INVITE (INVITE 2 in the diagram) would then look like the sample below. The INVITE is sent because smith.acme.com matches the common name *.acme.com. Other valid SIP Request-URIs would be:

```
222222@gw1.acme.com
222222@smith.ano.com
222222@amith.some.com
```

You can see where the Net-Net SBC uses information from the certificate; the text is bold.

```
INVITE sip:222222@smith.acme.com:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.27.113:5060;branch=z9hG4bK4jmg29cmm8l0cg7smmrn85o4q7
From: 111111 <sip:111111@acme.com>;tag=_ph1_tag
To: 222222 <sip:222222@acme.com>
Call-ID: _1-2_call_id-10147@acme.com-1-
CSeq: 1 INVITE
Contact: <sip:111111@172.16.27.113:5060;transport=udp>
Max-Forwards: 69
Subject: TBD
Content-Type: application/sdp
Content-Length: 138
Route: <sip:222222@172.16.27.188:5060;lr>
v=0
o=user1 53655765 2353687637 IN IP4 172.16.27.113
s=-
c=IN IP4 172.16.27.113
t=0 0
m=audio 20000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

SIP Endpoint Certificate Data Caching Configuration

To configure SIP endpoint certificate data caching for an enforcement profile:

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

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

2. Type session-router and press Enter.

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

3. Type enforcement-profile and press Enter. If you are adding this feature to a pre-existing enforcement profile configuration, you will need to select and edit your configuration.

   ```
   ACMEPACKET(session-router)# enforcement-profile
   ACMEPACKET(enforcement-profile)#
   ```

4. add-certificate-info—Enter a list of one or more certificate attribute names to enable TLS certificate information caching and insertion of cached certificate information into a customized SIP INVITEs. This parameter is empty by default.

If you want to list more than one value, enclose the value in quotation marks (“ “) and separate the values with Spaces.

```
ACMEPACKET(enforcement-profile)# add-certificate-info "sub-common-name sub-
alt-name-DNS"
```

5. certificate-uri-check—Change this parameter from disabled, its default, to enabled if you want your Net-Net SBC to cache TLS certificate information and use it to validate Request-URIs. Enabling this parameter also means the Net-Net SBCwill use the cached TLS certificate information in a customized SIP INVITE.
6. Type done and continue.

E-CSCF Emergency Setting Precedence for NMC

RTN 2246

When the Net-Net SBC acts as an E-CSCF, it can route emergency or priority calls (i.e., 112, 911, 999 calls) to the corresponding ECS/PSAP based on the calling party’s information. However, for registered users, this ability mixes with the Net-Net SBC NMC function so that the Service Routes takes precedence over the NMC. So rather than routing the emergency call to the ECS/PSAP, the call ends up at the S-CSCF of the Service Route.

For non-registered users where there no Service Route exists, this is not an issue.

Adding the apply-local-policy value to the options parameter in the network management controls configuration allows the NMC takes precedence over cached Service Route when a session matches an NMC rule. Instead, it locates a matching local policy.

Details

Without the NMC configured to take precedence, the Net-Net SBC does not function optimally as an E-CSCF for registered users.

Consider the following scenario in which a UE registers as a P-CSCF to the S-CSCF via the Net-Net SBC. In this case, the registrar returns a Service Route header in a 200 OK response to the REGISTER message to the Net-Net SBC. Or, if an implicit service route is enabled, the Net-Net SBC generates a Service Route that it saves in the register cache before forwarding the 200 OK on to the UA. Then when a new INVITE comes from the UA, the Net-Net SBC checks its register cache and uses the Service Route as the next hop—without taking local policy into consideration.

Using the apply-local-policy value requires local policy’s consideration in deciding the next hop. If you configure this option and the Net-Net SBC receives a new INVITE, it will decide whether the session is priority, registered, or with Service Route. Then it will determine if the call is E-CSCF. If so and the first matching local policy has E-CSCF enabled, the priority local policy is applied over the Service Route. The Net-Net SBC stays with the Service Route if not.

E-CSCF Emergency Configuration

This section shows you how to configure a network management control rule to take precedence over a Service Route.

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

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

2. Type session-router and press Enter.

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

3. Type net-management-control and press Enter.

```
ACMEPACKET(session-router)# net-management-control
ACMEPACKET(net-management-control)#
```

4. options——Follow your entry with this value: +disable-temp-file

```
ACMEPACKET(net-management-control)# options +apply-local-policy
```

   This value allows a network management control rule to take precedence over a service route for an emergency or priority call.

5. Type done and continue.

Secure and Non-Secure Flows in the Same Realm

To simplify deployments, theNet-Net SBC allows secure and non-secure flows in the same realm. For Release S-C6.2.0M2 and later, this broadened set of capabilities means the Net-Net SBC can support RTP and SRTP flows, and it can support a larger group of UAs that might have varying SRTP abilities. Prior to this release, when a cryptographic session arrived at the Net-Net SBC and failed to match an applicable media security profile, it was rejected.

This broadened support for secure and non-secure flows and for UAs with various SRTP abilities is established throughout the Net-Net SBC, residing in these configurations:

- media-sec-policy
- sdes-profile
- mikey-profile

While configurations reside there, you should also note special considerations for the security-policy configuration and implications for security associations.

Mode Settings in the Media Security Policy

The media security policy configuration's mode parameter offers three settings. It is the any mode that allows you to support secure and non-secure flows in the same realm.

For Incoming Flows

This section describes the way all three settings behavior for incoming flows.

- rtp—If the incoming media security policy associated with a realm has rtp set as its mode, then the Net-Net SBC only accepts offer SDP containing RTP/AVP media lines. Otherwise, the Net-Net SBC rejects the session with a 488 Not Acceptable Here.
- srtp—If the incoming media security policy associated with a realm has srtp set as its mode, the Net-Net SBC only accepts offer SDP containing RTP/SAVP media lines. Otherwise, the Net-Net SBC rejects the session with a 488 Not Acceptable Here.
- any—If the incoming media security policy associated with a realm has any set as its mode, the Net-Net SBC accepts offer SDP that has RTP/AVP media lines, RTP/SAVP media lines, or both.

For Outgoing Flows

This section describes the way all three settings behavior for outgoing flows.

- rtp—If the outgoing media security policy associated with a realm has rtp set as its mode, then the Net-Net SBC converts any RTP/SAVP media lines from incoming offer SDP to RTP/AVP for the offer SDP it sends out.

  Incoming offer SDP might look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 192.168.22.180
s=SIP Call
c=IN IP4 192.168.22.180
t=0 0
m=audio 5010 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
```

```
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:f0oLKTuMYwXqrKa7Ch
+MOBvLe8YnXnD6Kmnj4LQ2
```

The Net-Net SBC will take that and convert it to the following for outgoing traffic.

```
v=0
o=MxSIP 0 1480968866 IN IP4 172.16.22.180
s=SIP Call
c=IN IP4 172.16.22.180
t=0 0
m=audio 6000 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-1
```

This conversion can result in multiple media lines with RTP/AVP for the same media profile and an RTP/SAVP media line for the same media profile. To prevent duplicate lines in the SDP the Net-Net SBCsends, the Net-Net SBC inspects incoming SDP to determine is RTP/AVP and RTP/SAVP media lines exist for the same media profile. If it finds such a media profile, the Net-Net SBC disables the RTP/AVP (by setting the port to 0 in the outgoing offer SDP) corresponding to the RTP/AVP media line for that media profile. Doing so forces the UA answering the SDP offer to choose the media lines corresponding to the RTP/SAVP media lines in the incoming offer SDP. An SRTP-RTP session results.

The incoming offer SDP might look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 192.168.22.180
s=SIP Call
c=IN IP4 192.168.22.180
t=0 0
m=audio 5012 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
m=audio 5010 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:f0oLKTuMYwXqrKa7Ch
+MOBvLe8YnXnD6Kmnj4LQ2
```

And the outgoing offer SDP will look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 172.16.22.180
```

```
s=SIP Call
c=IN IP4 172.16.22.180
t=0 0
m=audio 0 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
m=audio 6002 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
```

- srtp—If the outgoing media security policy associated with a realm has srtp set as its mode, theNet-Net SBC converts any RTP/AVP media lines from an incoming offer SDP to RTP/SAVP for the offer SDP the Net-Net SBC sends.

  The incoming offer SDP might look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 192.168.22.180
s=SIP Call
c=IN IP4 192.168.22.180
t=0 0
m=audio 5012 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
```

  And the outgoing offer SDP will look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 172.16.22.180
s=SIP Call
c=IN IP4 172.16.22.180
t=0 0
m=audio 6000 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-1
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:f0oLKTuMYwXqrKa7Ch
+MOBvLe8YnXnD6Kmnj4LQ2
```

  This conversion might result in multiple media lines with RTP/SAVP for the same media profile if the incoming offer SDP has an RTP/AVP media line and an RTP/SAVP media for the same media profile. To prevent multiple identical media lines in the SDP it sends, the Net-Net SBC inspects the incoming SDP to determine whether both

RTP/AVP and RTP/SAVP media lines exist for the same media profile. If it finds such a media profile, the Net-Net SBC disables the RTP/SAVP (by setting the port to 0 in the outgoing offer SDP) corresponding to the RTP/AVP media line for that media profile. Doing so forces the UA answering the SDP offer to choose the media lines corresponding to the RTP/SAVP media lines in the incoming offer SDP. An SRTP-SRTP session results.

The incoming offer SDP might look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 192.168.22.180
s=SIP Call
c=IN IP4 192.168.22.180
t=0 0
m=audio 5012 RTP/AVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
m=audio 5010 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:f0oLKTuMYwXqrKa7Ch
+MOBvLe8YnXnD6Kmnj4LQ2
```

And the outgoing offer SDP will look like this:

```
v=0
o=MxSIP 0 1480968866 IN IP4 172.16.22.180
s=SIP Call
c=IN IP4 172.16.22.180
t=0 0
m=audio 0 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-15
m=audio 6002 RTP/SAVP 0 8 18 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=silenceSupp:off - - - -
a=fmtp:18 annexb=no
a=fmtp:101 0-1
a=crypto:0 AES_CM_128_HMAC_SHA1_80 inline:f0oLKTuMYwXqrKa7Ch
+MOBvLe8YnXnD6Kmnj4LQ2
```

- any—If the outgoing media security policy associated with a realm has any set as its mode, the Net-Net SBC creates offer SDP based on the value configured in the egress-offer-format, which can be set either in the sdes-profile or the mikey-profile configurations.

- If the value is same-as-ingress, the Net-Net SBC leaves the profile of the media lines unchanged.
- If the value is simultaneous-best-effort, the Net-Net SBC inspects the incoming offer SDP and:
  - Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile
  - Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile

Should the media profile in the incoming offer SDP already have two media lines (one fore RTP/AVP and on for RTP/SAVP), the Net-Net SBCdoes not have to make these additions. It will map the media lines in the answer it receives with the media lines from the incoming offer SDP. It will also ensure that media lines in the answer SDP it sends match the media lines from the incoming offer SDP.

Using Security Associations for RTP and RTCP

With RTP and SRTP supported in the same realm, you want to configure your SRTP security policies to preserve system resources and exercise the full capability number of licensed sessions. You need to do to avoid session agent interaction that can have an adverse impact on the number of sessions.

To do so, check the local-ip-match-address for the STRP security policy has an IP address different from the all steering pool IP addresses for realms requiring both RTP and SRTP. The Net-Net SBC recognizes this difference automatically and sets the connection address of media lines in SDP accordingly:

- The connection address for RTP media lines is the IP address of the applicable steering pool. The Net-Net SBC passes through RTP and RTCP packets sent by and received from the steering pool IP address. This operation requires no reference to session agents because the steering pool address does not match the IP address for the SRTP security policy's local-ip-address-match value.
- The connection address of the SRTP media lines continues to be the local-ip-address-match value from the applicable SRTP security policy.

Since RTP and RTCP packets are sent to and from the steering pool's IP address (an IP address for which there is no SRTP security policy configured), there is no reason to reference session agents.

Note: Acme Packet's Enhanced Traffic Controller (ETC) networking interface unit handles traffic differently such the issue with session agent reference is elided. That is, if you are using the ETC NIU (available with NNet-Net SBC Release S-CX6.3.0F1), you do not need to be concerned about this issue.

Secure and Non-Secure Flows Configuration

This section shows you how to configure your Net-Net SBC to support secure and non-secure flows in the same realm.

To configure a security policy to support secure and non-secure flows in the same realm:

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

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

2. Type security and press Enter.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type media-security and press Enter.

```
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)#
```

4. Type media-sec-policy and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

```
ACMEPACKET(media-security)# media-sec-policy
ACMEPACKET(media-sec-policy)#
```

5. Type inbound to enter the setting for inbound flows.

```
ACMEPACKET(media-sec-policy)# inbound
ACMEPACKET(inbound)#
```

6. mode—Enter the mode that you want to use for inbound flows. You can choose from rtp, srtp, and any.
7. protocol—Change this value from either sdes or mikey to none. Use the done command to save your work, and exit the inbound configuration.
8. Type outbound to enter the setting for inbound flows.

```
ACMEPACKET(media-sec-policy)# outbound
ACMEPACKET(outbound)#
```

9. mode—Enter the mode that you want to use for outbound flows. You can choose from rtp, srtp, and any.
10. protocol—Change this value from either sdes or mikey to none. Use the done command to save your work, and exit the outbound configuration.
11. Type done and continue.

Egress Offer Format for SDES Profile Configuration

To set the egress offer format for an SDES profile configuration:

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

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

2. Type security and press Enter.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type media-security and press Enter.

```
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)#
```

4. Type sdes-profile and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

```
ACMEPACKET(media-security)# sdes-profile
ACMEPACKET(sdes-profile)#
```

5. egress-offer-format—Choose an egress offer format for this profile to use when you set the outbound mode in the media security policy to any. You can select one of two values:
   - If the value is same-as-ingress (default), the Net-Net SBC leaves the profile of the media lines unchanged.
   - If the value is simultaneous-best-effort, the Net-Net SBC inspects the incoming offer SDP and:
     - Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile
     - Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile
6. Type done to save your work and continue.

Egress Offer Format for a Mikey Profile Configuration

To set the egress offer format for a mikey profile configuration:

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

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

2. Type security and press Enter.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type media-security and press Enter.

```
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)#
```

4. Type mikey-profile and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

```
ACMEPACKET(media-security)# mikey-profile
ACMEPACKET(mikey-profile)#
```

5. egress-offer-format—Choose an egress offer format for this profile to use when you set the outbound mode in the media security policy toany. You can select one of two values:
   - If the value is same-as-ingress (default), the Net-Net SBC leaves the profile of the media lines unchanged.
   - If the value is simultaneous-best-effort, the Net-Net SBC inspects the incoming offer SDP and:
     - Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile
     - Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile
6. Type done to save your work and continue.

Supporting UAs with Different SRTP Capabilities

To support UAs with different levels of SRTP capabilities, the use-ingress-session-params parameter appears in both the sdes-profile and mikey-profile configurations. The values for this parameter allow the Net-Net SBC to accept and (where applicable) mirror the UA's proposed cryptographic session parameters:

- srtp-auth—Decides whether or not authentication is performed in SRTP
- srtp-encrypt—Decides whether or not encryption is performed in SRTP
- srtcp-encrypt—Decides whether or not encryption is performed in SRTCP

Using these possible values, the Net-Net SBCaccepts the corresponding incoming session parameters.

Note: For MIKEY, this parameter and its function are reserved for future use.

Receiving Offer SDP

When the Net-Net SBC receives offer SDP with applicable session parameters, it uses the same session parameters in its answer SDP (if it can support the same). This is true even if the value for that session parameter differs from the available media security profile.

Consider this example: An SDES profile is applied for incoming direction for a media security policy configured with the srtcp-encrypt value set to enabled. With the use-ingress-session-params parameter set to srtcp-encrypt for the SDES profile, the Net-Net SBC accepts the offer SDP and also sets UNENCRYPTED_SRTCP for the cryptographic attributes in its answer SDP. When the call connects, the Net-Net SBCdoes not encrypt or decrypt SRTCP packets. Without the SDES profile set this way, the Net-Net SBCwould reject offer SDP if any of its cryptographic attributes showed UNENCRYPTED_SRTCP in its session parameters list.

Receiving Answer SDP

When the Net-Net SBC receives answer SDP with the accepted session parameter, the value for the same session parameters that the Net-Net SBC uses might or might not be the same as the incoming value. Configuration of the outbound media security profile controls the value used because the Net-Net SBC makes offer SDP, which cannot be changed, with the session parameters based on the outgoing media security profile.

Consider this example: An SDES profile is applied for incoming direction for a media security policy configured with the srtcp-encrypt value set to enabled, so the cryptographic attributes in the SDP the Net-Net SBC sends do not have the UNENCRYPTED_SRTCP session parameters. If the UNENCRYPTED_SRTCP appears in the corresponding answer SDP it receives, the Net-Net SBC accepts it if the srtcp-encrypt value appears in the use-ingress-session-params parameter. But the Net-Net SBC still performs SRTCP encryption. When the call connects, the Net-Net SBC encrypts outgoing SRTCP packets but does not decrypt incoming SRTCP packets. So if the UA (receiving theNet-Net SBC offer SDP) does not support SRTCP decryption, it will likely reject the offer SDP.

Ingress Session Parameters for SDES Profile Configuration

To set the ingress session parameters for an SDES profile configuration:

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

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

2. Type security and press Enter.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type media-security and press Enter.

```
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)#
```

4. Type sdes-profile and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

```
ACMEPACKET(media-security)# sdes-profile
ACMEPACKET(sdes-profile)#
```

5. use-ingress-session-params—Enter the list of values for which the Net-Net SBC will accept and (where applicable) mirror the UA's proposed cryptographic session parameters:

   - srtp-auth—Decides whether or not authentication is performed in SRTP
   - srtp-encrypt—Decides whether or not encryption is performed in SRTP
   - srtcp-encrypt—Decides whether or not encryption is performed in SRTCP

```
ACMEPACKET(sdes-profile)# use-ingress-session-params srtp-auth srtp-encrypt
srtcp-encrypt
```

6. Type done to save your work and continue.

Refining Interoperability

To refine any remaining interoperability issues, you can use the options parameter in these configurations: media-sec-policy, sdes-profile, and mikey-profile.

Common values to configure an option are include-local-id and include-remote-id. By default, the Net-Net SBC does not include the IDi or IDr when sending the MIKEY I_MESSAGE. And it does not set the IDr in the MIKEY R_MESSAGE. Using the options provides these results:

- include-local-id—The Net-Net SBC includes the IDi in the I_MESSAGE and the IDr in the R_MESSAGE.

  When used for the outbound direction of a media security policy, the IDi is included in the I_MESSAGE the Net-Net SBC sends. The content of the IDi is the value of the Contact header found in the INVITE message.

  When configured for the mikey-profile associated with the inbound media security policy, the Net-Net SBC includes the IDr in the R_MESSAGES it sends in response to incoming I_MESSAGES. The content of the IDr is the value of the Contact header found in the 200 OK response.
- include-remote-id—The Net-Net SBC includes the IDr in the I_MESSAGE.

  When configured for the mikey-profile associated with the outbound media security policy, the Net-Net SBC includes the IDr in I_MESSAGES it initiates. The content of the IDr is the value of the Request-URI from the INVITE message.

Refining Interoperability Configuration

You can configure these options for media-sec-policy, sdes-profile, and mikey-profile configurations. The following uses the mikey-profile to demonstrate how to enter them.

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

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

2. Type security and press Enter.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type media-security and press Enter.

```
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)#
```

4. Type mikey-profile and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

```
ACMEPACKET(media-security)# mikey-profile
ACMEPACKET(mikey-profile)#
```

5. options——Your entry will look like this when you add both values:

```
ACMEPACKET(mikey-profile)# options include-local-id, include-remote-id
```

You can you the plus sign (+) and the minus sign (-) to add and remove values from the options list.

To remove an value, your entry would look like this:

```
ACMEPACKET(mikey-profile)# options -include-local-id
```

To add an value, your entry would look like this:

```
ACMEPACKET(mikey-profile)# options +include-local-id
```

6. Save and activate your configuration.

3

S-C(X)6.2.0M3

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M3.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M3.

Content Type	Description
Adaptation	2389 - Multi-stage Routing on Realm Navigation
Adaptation	2463 - SIP Header pre-processing HMR

Multi-stage Routing on Realm Navigation

You can configure multi-stage local policy routing to use the next-hop realm (from the current local policy stage) as the source realm for the next stage in a look-up.

Multi-stage Routing on Realm Navigation Configuration

To use the next-hop realm as the source realm for a look-up's next stage:

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

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

2. Type session-router and press Enter.

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

3. Type session-router-config and press Enter.

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

4. multi-stage-src-realm-override—For multi-stage routing scenarios, set this parameter to enabled if you want to use the next-hop realm (from the current local policy stage) as the source realm for the next stage in a look-up. This parameter is disabled by default.
5. Type done and continue.

SIP Header Pre-Processing HMR

RTN 2413

By default, the Net-Net SBC performs in-bound SIP manipulations after it carries out header validation. Adding the inmanip-before-validate option in the global SIP configuration allows the Net-Net SBC to perform HMR on received requests prior to header validation. Because there are occaisional issues with other SIP implementations—causing invalid headers to be used in messages they send to the Net-Net SBC—it can be beneficial to use HMR to remove or repair these faulty headers before the request bearing them are rejected.

When configured to do so, the Net-Net SBC performs pre-validation header manipulation immediately after it executes the top via check. Inbound SIP manipulations are performed in order of increasing precedence: SIP interface, realm, and session agent.

The fact that the top via check happens right before the Net-Net SBC carries out pre-validation header manipulations means that you cannot use this capability to repairs the first via header if it is indeed invalid. If pre-validation header manipulation were to take place at another time during processing, it would not be possible to use it for SIP session agents. The system learns of matching session agents after top via checking completes.

For logistical reasons, this capability does not extend to SIP responses. Inbound manipulation for responses cannot be performed any sooner that it does by default, a time already preceding any header validation.

SIP Header Pre-Processing Configuration

This section shows you how to enable SIP header pre-processing:

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

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

2. Type session-router and press Enter.

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

3. Type sip-config and press Enter.

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

4. options——Follow your entry with this value: +inmanip-before-validate

```
ACMEPACKET(account-config)# options +inmanip-before-validate
```

   This value allows a the Net-Net SBC to perform pre-validation header manipulation in order of increasing precedence: SIP interface, realm, and session agent.

5. Save and activate your configuration.

4

S-C(X)6.2.0M4

This chapter provides descriptions, explanations, and configuration information for the contents ofNet-Net SBCRelease S-C(X)6.2.0M4.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M4.

Content Type	Description
Adaptation	2470 - Diameter e2 Configurable Address-realm AVP
Adaptation	2522 - Disable MIBOCO logging
Adaptation	2554 - CDR Stop Time enhancement for SIP
Adaptation	2463 - Assymetrical handling of DTMF conversion from 2833/INFO
Forward Merge	S-C6.5.0M2 Adaptations & Defect Fixes

DIAMETER e2 Configurable Address-Realm AVP

As of Net-Net SBCRelease S-C(X)6.2.0M4, you can configure a value to be sent in the Address-Realm AVP (communicated in the Globally-Unique-Address AVP) for the DIAMETER e2 interface. This AVP is sent on a per-realm basis in the Location Information Query (UDR) query theNet-Net SBC (as a P-CSCF) sends to the CLF.

The CLF maintains details about IP connectivity access sessions associated with user equipment connected in the network. This CLF supports the standardized DIAMETER e2 interface with an Application Function; from it, the application function (i.e., the Net-Net SBC in the role of P-CSCF) retrieves location information and other data related to the access session. To do so, the AF sends a UDR containing Global-Unique-Address and Requested Information attributes. Then the CLF returns a Location Information Response (UDA) containing either a success result code with location information or an error result code.

In the UDR's Global-Unique-Address, the Net-Net SBC currently supports the mandatory parameters: the Framed-IP-Address AVP and the Address-Realm AVP. The address realm AVP is the realm address in FQDN form, populated based on the realm on which a REGISTRATION arrived or the SIP interface. With nested realms configured, using a realm for this value can quickly become complicated.

To clarify, you can configure the sent in the Address-Realm AVP on a per-realm basis. You set the external policy server's ingress-realm-location parameter to the diam-address-realm value, pointing the Net-Net SBC to the associated realm from which it will learn Address-Realm AVP information. This access realm (or child realm, the realm on which enter registration came in) has its diam-e2-address-realm value set to the value with which to populate the Address-Realm AVP for the outgoing UDR message.

Ingress Realm Location Configuration

This section shows you how to set the ingress-realm-location to diam-address-realm, and how to configure a realm with a diam-e2-address-realm value.

To set the ingress realm location for the external policy server:

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

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

2. Type media-manager and press Enter.

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

3. Type ext-policy-server and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit it.

```
ACMEPACKET(media-manager)# ext-policy-server
ACMEPACKET(ext-policy-server)#
```

4. ingress-realm-location—For the e2 interface, set this parameter from diam-address-realm if you want to use configurable Address-Realm AVPs. This setting points the Net-Net SBC to the associated realm from which it will learn Address-Realm AVP information. The default is realm-in.
5. Type done and continue.

Address-Realm AVP Configuration

To configure the value to use in the Address-Realm AVP:

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

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

2. Type media-manager and press Enter.

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

3. Type realm-config and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit it.

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

4. diam-e2-address-realm—Enter a value for the Net-Net SBC to use when setting the Address-Realm AVP in UDRs destined for the CLF. There is no default for this parameter.
5. Type done and continue.

Disabling Miboco Logging

If your Net-Net SBC configuration is especially large—such that you deem it necessary to preserve as many system resources as possible during activation—you might want to disable Miboco logging. Miboco is a body of control messages allowing certain internalNet-Net SBC process to communicate with one another, and these message constitute part of the call trace logging. By turning Miboco call trace logging office, you provide additional safeguard around system resource and possibly prevent the adverse consequences that might arise from overuse.

Disabling Miboco Logging Configuration

To disable Miboco call trace logging:

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

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

2. Type session-router and press Enter.

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

3. Type sip-config and press Enter.

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

4. options—Follow your entry with this value: +disable-miboco-logging

```
ACMEPACKET(sip-config)# options +disable-miboco-logging
```

   You can enable Miboco logging again by removing the option:

```
ACMEPACKET(sip-config)# options -disable-miboco-logging
```

5. Type done and continue.

SIP CDR Stop Time

You can set up your global SIP configuration so the disconnect time reflected in a RADIUS CDR is the time when the Net-Net SBCreceives a BYE. Enabling this parameter also means the disconnect time is defined when the Net-Net SBC sends a BYE to the UAS and UAC. Otherwise, the the CDR's value is based on when the 200 OK confirms the BYE.

The applicable RADIUS CDR in this case is the standard RADIUS attribute Acct-Session-Time, number 46.

SIP CDR Stop Time Configuration

To enable definition of the disconnect time based on the BYE:

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

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

2. Type session-router and press Enter.

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

3. Type sip-config and press Enter.

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

4. set-disconnect-time-on-bye—Set this parameter to enabled if you want to use the BYE message as the defining factor for the disconnect time. This parameter is disabled by default.
5. Type done and continue.

5

S-C(X)6.2.0M5

This chapter provides descriptions, explanations, and configuration information for the contents ofNet-Net SBC Release S-C(X)6.2.0M5.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M5.

Content Type	Description
Adaptation	2169 - Event Log Notificiation: Demotion from Trusted to Untrusted
Adaptation	2349 - LRT String Lookup
Adaptation	2381 - Removing the T.38 Codec from an H.245 TCS
Adaptation	2440 - Temporary File Naming for an Open CDR File
Adaptation	2461 - Hitless LRT Update
Adaptation	2490 - DIAMETER:CLF e2 Interface - Support of the User-Name AVP
Adaptation	2538 - HMR $LOCAL_PORT for Port Mapping
Adaptation	2580 - DIAMETER Wildcard Transport Protocol
Adaptation	2596 - IPv6 fragment support

Event Log Notification Demotion from Trusted to Untrusted

You can enable your Net-Net SBC to provide event log notification (a syslog message) any time it demotes an endpoint from trusted to untrusted. The log message contains this data: IP address of the demoted endpoint, the endpoint's configured trust level, and the reason for demotion.

To use this feature, the intrusion detection system (IDS) Reporting license must be installed and your media manager configuration must be enabled to send the log messages.

Event Log Notification Configuration

To write event log notifications on endpoint demotion:

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

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

2. Type media-manager and press Enter.

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

3. Type media-manager-config and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit it.

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

4. syslog-on-demote-to-untrusted—Change this parameter from disabled (default), to enabled so the Net-Net SBC will generate event notifications (syslog messages) when an endpoint becomes untrusted. For this capability to work, the IDS license must be installed on your system.
5. Type done and continue.

LRT String Look-up

Removing the T.38 Codec from an H.245 TCS

For SIP-H.323 IWF sessions, H.323 automatically inserts the T.38 FAX codec in the H.246 TCS message. You can stop this insertion using the remove-t38 parameter in the H.323 global configuration.

Removing the T.38 Codec Configuration

To remove the T.38 codec from an H.245 TCS for SIP-H.323 IWF sessions:

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

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

2. Type session-router and press Enter.

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

3. Type h323-config and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit your configuration.

```
ACMEPACKET(session-router)# h323-config
ACMEPACKET(h323-config)#
```

4. remove-t38—For SIP-H.323 IWF sessions, if you want to remove the T.38 FAX codec from the H.245 TCS, set this parameter to enabled. This parameter is disabled by default.
5. Type done and continue.

Temporary File Naming for an Open CDR File

RTN 2440

As of Net-Net SBC Release S-C(X)6.0.0M7, the Net-Net SBC uses a temporary naming convention that makes it easier for you to retrieve CDR files you want.

Before this release was introduced, the Net-Net SBC used the same naming format for all CDR files: cdrYYYYMMDDHHMM[a-j]. If this is the naming convention you still want to use, you can do so simply by adding the disable-temp-file option to your accounting configuration. This mode offers no means of differentiating a file to which the Net-Net SBC is writing information from any other closed file(s).

If you decide to use the new default behavior, then you will now see a the temp-prefix added to the file format. So the file format for the temp file is: temp-cdrYYYYMMDDHHMM[a-j]. The prefix helps you differentiate the file that is currently open from the other CDR files you encounter; this is the file to which the Net-Net SBC is currently writing information and is open. As soon as the file is closed during rotation, the temp- disappears and the file bears only name in the cdrYYYYMMDDHHMM[a-j]. In other words, files in the cdrYYYYMMDDHHMM[a-j] are closed files.

Without this differentiation, it is possible for you to retrieve different versions of the same file and to even do so more than once. In addition, without the temp- differentiation, the Net-Net SBC FTP server is liable to return error messages when move or delete operations occur. These occurrences can trigger false alarms and are not consistent with other vendors' products.

Operational Details

This section offers details of Net-Net SBC operations that effect temporary CDR file naming.

- Reboot—A system reboot can happen unexpectedly, or might be caused by your intentionally rebooting the system using the ACLI reboot command. When a reboot occurs, Net-Net SBC closes the CDR file that was most recently opened (before the reboot) and names it according to the cdrYYYYMMDDHHMM[a-j] convention. It also opens a new file, which bears the temp- differentiation.
- Activating a configuration—If temporary CDR naming is enabled before and after you use the activate-config command, then the last opened file will be closed and have the cdrYYYYMMDDHHMM[a-j] name format. The Net-Net SBC also opens a new file with the temp- prefix to which it will write data.

  In the case where temporary CDR naming is enabled before you activate a configuration and disabled after it, the last open file is named according to the cdrYYYYMMDDHHMM[a-j] name format. The new file to which the Net-Net SBC will write data is also in the cdrYYYYMMDDHHMM[a-j] name format. In other words, the Net-Net SBC does not use the temp- prefix designation at all.

  In the case where temporary CDR naming is disabled before you activate a configuration and enabled after it, the Net-Net SBCcloses the most recently opened file—which must have been in the cdrYYYYMMDDHHMM[a-j] name format. The Net-Net SBC also opens a new file with the temp- prefix to which it will write data.
- Changing the accounting configuration's administrative state—When you disable the accounting configuration, the Net-Net SBC renames the most recently opened file with the temp- prefix to the cdrYYYYMMDDHHMM[a-j] name format.

HA Considerations

The considerations in this section describes the Net-Net SBC behavior when CDR output redundancy is enabled or disabled. You set CDR output redundancy in the accounting configurations cdr-output-redundancy parameter.

- Enabled—When you enable CDR output redundancy, both the Active and Standby systems rotate files. During CDR file rotation, if either the Active or the Standby rotates a file with the temp- prefix, the prefix disappears and the file name appears in the cdrYYYYMMDDHHMM[a-j] name format.

  The Active and the Standby systems always have the same files, including the CDR file with the temp- prefix. So the file exists on both systems.
- Disabled—When you have disables CDR output redundancy and switchover happens for any reason, it is key that there are no residual files with the temp- prefix. For this reason, the Net-Net SBC handles the situation as follows:

  Becoming Active—When it transitions from Standby to Active, a Net-Net SBC checks for any files with the temp- prefix, closes the file if it is open, and renames it according to the cdrYYYYMMDDHHMM[a-j] name format. These actions means that the file is not only renamed, but that it is also rotated. Rotation triggers the creation of a new CDR file with the temp- prefix to use for new CDR data.

Becoming Standby—When it transitions from Active to Standby, a Net-Net SBCcloses the open temp- prefix file and renames it according to the cdrYYYYMMDDHHMM[a-j] name format. Rotation creates a new temp- prefix file on the Standby, which remains empty until it transitions back to the Active state.

Caveats

When the system reboots for any reason or when you issue an activate-config, the Net-Net SBC checks for CDR files with the temp- prefix and renames to the usual cdrYYYYMMDDHHMM[a-j] format.

However, if you change the accounting configuration's file-path value and subsequently the system either reboots or you activate your configuration, the Net-Net SBC will be unable to check for files with the temp- prefix in the old file path. And so it will also be unable to rename them. The Net-Net SBC checks the new path only.

Temporary File Naming for an Open CDR Configuration

Since Release S-C(x)6.0.0M7 and later use this capability by default, this section offers instructions for how to turn off temporary CDR file naming if you do not want to use it.

To turn off temporary CDR file naming:

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

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

2. Type session-router and press Enter.

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

3. Type account-config and press Enter.

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

4. options—Follow your entry with this value:

   - +disable-temp-file

     ```
     ACMEPACKET(account-config)# options +disable-temp-file
     ```

     This value turns off the temporary CDR file naming the Net-Net SBC, so it does not use the temp- prefix for open file. Instead, all files follow the cdrYYYYMMDDHHMM[a-j] name format.

     To enable temporary CDR file naming, you must use a minus sign (-) before the disable-temp-file value.

     ```
     ACMEPACKET(account-config)# options -disable-temp-file
     ```

5. Save and activate your configuration.

Hitless LRT Update

In Net-Net SBC releases prior to S-C(X)6.2.0M5, reloading an XML file for the LRT capabilities causes the Net-Net SBC to delete and reload all existing entries. This process relies on internal system processes to keep impact on sessions traversing the Net-Net SBC to a minimum.

In Release S-C(X)6.2.0M5 and later, the Net-Net SBChandles LRT updates in a way that eliminates upgrade impact. New interval communication processes tell LRT function when a table is being added or updated so it can switchover seamlessly to use the new data.

- When adding a new LRT, the Net-Net SBC creates a new table and then tells LRT function about the new table, the number of valid route entries, and the number of invalid route entries. Then the LRT function knows where and how to reach the active table, and updates the LRT statistics.
- When modifying (or refreshing) an existing LRT table, the Net-Net SBCmarks the table being updated as currently being updated while new information is being processed. The Net-Net SBC will also reject any new

requests to modify an LRT. The LRT function continues to use the existing table (not the updated one) until the Net-Net SBC tells it the updating process is complete and the new table is ready for use.

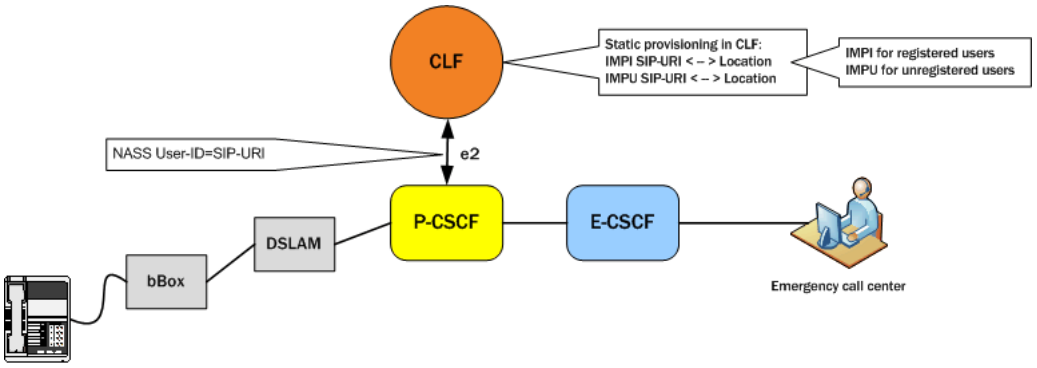
If an error occurs (failure to unzip a file, failure to parse XML, out of memory) when updating an LRT table, the failure is logged an displayed on the ACLI while the LRT function continues to process calls using the current (un-updated) active table.

There is no special configuration require for this feature; it is enabled automatically.

DIAMETER CLF e2 Interface User-Name AVP Support

In compliance with ETSI ES 283 -35 V1.2.1, theNet-Net SBC e2 interface can query the CLF using the SIP endpoint's IP address or its NASS User-ID. The system's e2 interface uses the uses the SIP-URI to query the CLF by including the User-Name AVP in the User Data Request (UDR). The CLF can then furnish the P-CSCF (i.e., theNet-Net SBC) with the INSEE code in the Location-Information AVP in its User Data Answer (UDA).

This diagram shows how this capability works. The Net-Net SBC acts as the P-CSCF.



CLF e2 Interface User-Name AVP Support for Registration

This section describes how the Net-Net SBC handles CLF e2 interface User-Name AVP support for registering and unregistered users.

- Registering users—When it receives a registration request, the Net-Net SBC checks the incoming SIP interface to determine CLF use. If CLF use is unnecessary, the Net-Net SBC forwards the registration message to its destination.

  When CLF is required, theNet-Net SBC selects the AVPs to send the CLF, including the User-Name AVP before sending it a UDR. A none setting for this parameter means theNet-Net SBC does not include the User-Name AVP in any UDRs. The Net-Net SBC adds the User-Name AVP to the UDR if the user-name-mode parameter in the external policy server configuration is set to:

  - endpoint-id—IP address of the registering endpoint is sent as the payload for the User-Name AVP
  - public-id—SIP-URI portion of the TO header from the register message is sent as the payload for the User-Name AVP
  - auth-user—Username attribute of the Authorization header from the register is sent as the payload for the User-Name AVP; if there is no authorization header, the Net-Net SBC will not consult the CLF and will forward the registration message
- Unregistered users—When it receives an INVITE request, the Net-Net SBC checks the incoming SIP interface to determine if it should use an external policy server. If it does not need to use an external policy server, the Net-Net SBC forwards the INVITE message to its destination.

  When the Net-Net SBC does need to use an external policy server, it also checks to determine if the INVITE is in a registration and if location data in the registration cache is avaible for that endpoint. These requirements being met, the Net-Net SBC inserts the P-Access-Network-Info header with the location string into the INVITE it forwards to the destination. If these requirements are not met, the Net-Net SBC consults the CLF before forwarding the INVITE. The following describe the impact of the user-name-mode setting in such instance:

- endpoint-id—IP address of the endpoint that issued the INVITE is sent as the payload for the User-Name AVP
- public-id and auth-user—SIP-URI portion of the INVITE is sent as the payload for the User-Name AVP:

  With a P-Asserted-Id header present in the INVITE, the Net-Net SBC uses the first PAID header (if there are multiple PAID headers)

  Without a P-Asserted-Id header present in the INVITE's P-Preferred-Identity header, the Net-Net SBC uses the first PPI (if there are multiple PPI headers)

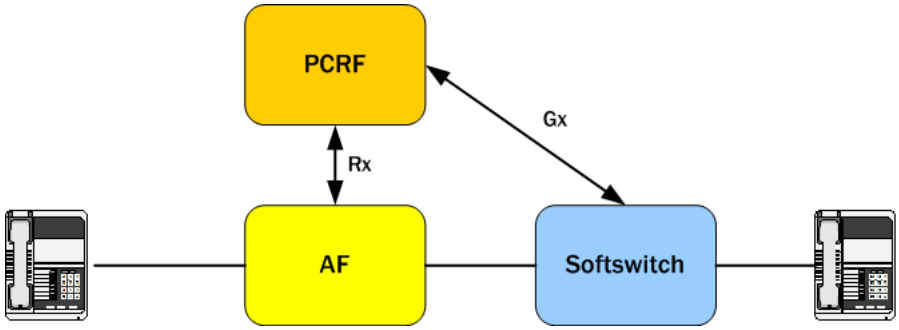
  With neither P-Asserted-Id nor P-Preferred-Identity header present, the Net-Net SBC uses the From header

HMR $LOCAL_PORT for Port Mapping

When you configure SIP HMR and set an element-rule's new-value parameter to $LOCAL_PORT, the Net-Net SBC maps this value to the real port it uses for each signaling exchange. In release prior to S-C(X)6.2.0M5, however, this entry maps to the SIP interface port when port mapping is also enabled on your system.

DIAMETER Wildcard Transport Protocol

The Net-Net SBC external bandwidth management solution provides for an Rx interface that supports the Flow-Description AVP (507). Rather than use a numerical value, this Flow-Description AVP uses an IP filter rule with the keyword "ip." The ip keyword means any transport protocol matches the Flow-Description AVP when issuing AARs to the PCRF. Before it forwards a Gx RAR messages to the softswitch, the PCRF decodes the audio codec into the correct speed and classification. The PCRF passes the Net-Net SBC Flow-Description AVP to the softswitch untouched. But not all softswitches accommodate the ip keyword, resulting in rejected requests.



When you enable the wildcard-transport-protocol parameter, however, you can essentially format the Flow-Description AVP to suit your network.

For sessions that need to allocate media and have applicable external bandwidth management associations, the Net-Net SBC DIAMETER interface checks for the necessary bandwidth. The DIAMETER interface, with an Rx or Rq application mode, constructs an AAR with Flow-Description AVP of ip when the wildcard-transport-protocol parameter is enabled. The flow description would look like this:

```
<Flow-Description-AVP(507) | Avp Flags=128 | AVP Length=72 | Vendor-Id=10415
Data = permit out ip from 168.192.24.20 49500 to 168.192.24.0 8000
<Flow-Description-AVP(507) | Avp Flags=128 | AVP Length=72 | Vendor-Id=10415
Data = permit in ip from 168.192.24.0 8000 to 168.192.24.20 49500
```

With the wildcard-transport-protocol set to disabled, the Net-Net SBC does not use the ip wildcard keyword. Instead, it uses the specific media stream transport protocol in the Flow-Description AVP—and only falls by to the ip keyword when the transport protocol is unknown. The flow description with this parameter disabled would look like this:

```
<Flow-Description-AVP(507) | Avp Flags=128 | AVP Length=72 | Vendor-Id=10415
Data = permit out 17 from 168.192.24.20 49500 to 168.192.24.0 8000
<Flow-Description-AVP(507) | Avp Flags=128 | AVP Length=72 | Vendor-Id=10415
Data = permit in 17 from 168.192.24.0 8000 to 168.192.24.20 49500
```

New Configurations and Upgrading

To comply with 2GPP TS 29.213, wildcard-transport-protocol parameter is disabled by default in new configurations. So if the transport protocol is known, the Net-Net SBC uses it in the Flow-Description AVP.

To maintain default behavior for existing configurations, the Net-Net SBCperforms a check at the time of upgrade to set this parameter to enabled. This setting means the Net-Net SBC does use the ip keyword in the Flow-Description AVP.

DIAMETER Wildcard Transport Protocol Configuration

To wildcard the transport protocol for Rx and Rq interfaces:

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

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

2. Type media-manager and press Enter.

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

3. Type ext-policy-server and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit it.

```
ACMEPACKET(media-manager)# ext-policy-server
ACMEPACKET(ext-policy-server)#
```

4. application-mode—Set this parameter to Rx or Rq.
5. wildcard-trans-protocol—Set this parameter from enabled if you want to use transport protocol wildcarding. Set this parameter to disabled if you want to use the specific media stream transport protocol. For new configurations, this parameter defaults to disabled. For existing upgraded configuration, this parameter defaults to enabled.
6. Type done and continue.

IPv6 Reassembly and Fragmentation Support

As it does for IPv4, the Net-Net SBC supports reassembly and fragmentation for large signaling packets when you enable IPV6 on your system.

The Net-Net SBC takes incoming fragments and stores them until it receives the first fragment containing a Layer 4 header. With that header information, the Net-Net SBCperforms a look-up so it can forward the packets to its application layer. Then the packets are re-assembled at the applications layer. Media fragments, however, are not reassembled and are instead forwarded to the egress interface.

On the egress side, the Net-Net SBCtakes large signaling messages and encodes it into fragment datagrams before it transmits them.

Note that large SIP INVITE messages should be sent over TCP. If you want to modify that behavior, you can use the SIP interface's option parameter max-udp-length=xx for each SIP interface where you expect to receive large INVITE packets.

Other than enabling IPv6 on your Net-Net SBC, there is no configuration for IPv6 reassembly and fragmentation support. It is enabled automatically.

6

S-C(X)6.2.0M6

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M6.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M6.

Content Type	Description
Adaptation	2290 - IPv6 SIP INFO to RFC 2833 Telephone Event Interworking
Adaptation	2485 - SIP-H.323 IWF Support for H.264 and H.263+
Adaptation	2598 - SIP-H.323 IWF in Video Conferencing Applications
Adaptation	2631 - SIP REFER-to-BYE
Adaptation	2661 - Offerless Bandwidth CAC for SIP
Adaptation	2726 - DIAMETER Rx: Opening for RTCP Flows
Adaptation	2762 - New KPIs for SIP Signaling
Adaptation	2630 - IR.92 compliance - Service URN AVP towards PCRF
Adaptation	2547 - LI Documentation available upon request
Forward Merge	S-C6.1.0M8 Adaptations and Defect Fixes

IPv6 SIP INFO to RFC 2833 Telephone Event Interworking

The Net-Net SBC can interwork SIP INFO and RFC Telephone Event messages for IPv4, IPv6—or for any session requiring interworking between IPv4 and IPv6. Other than installing the applicable licences on your Net-Net SBC and enabling IPv6 support in your system configuration (system-config), you do not have to perform any configuration steps for this capability to work.

SIP-H.323 IWF Support for H.264 and H.263+

Signaling protocol interworking between SIP and H.323 supports the H.264 and H.263+ video codecs.

H.264 in H.323 (H.241)

This section describes the H.264 capabilities and media packetization in H.323. Capability exchange signaling looks like this:

```
openLogicalChannel .  SEQUENCE [EMPTY -1] ...
forwardLogicalChannelNumber = 3 .  INTEGER [EMPTY -1] (1..65535)
forwardLogicalChannelParameters .  SEQUENCE [EMPTY -1] ...
 ..   dataType .  CHOICE [EMPTY -1] ...
. . . . . videoData .  CHOICE [EMPTY -1] ...
. . . . . genericVideoCapability .  SEQUENCE [EMPTY -1] ...
. . . . . capabilityIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 7 {itu-t recommendation h 241 0 0 1}.OBJECT
IDENTIFIER [EMPTY-1]
. . . . . maxBitRate = 4480 .  INTEGER [EMPTY -1] (0..-1)
. . . . . collapsing .  SEQUENCE OF [EMPTY -1] SEQUENCE [EMPTY -1] ...
. . . . . * .  SEQUENCE [EMPTY -1] ...
. . . . . parameterIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 41 .  INTEGER [EMPTY -1] (0..127)
. . . . . parameterValue .  CHOICE [EMPTY -1] ...
. . . . . booleanArray = 64 .  INTEGER [EMPTY -1] (0..255)
. . . . . * .  SEQUENCE [EMPTY -1] ...
. . . . . parameterIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 42 .  INTEGER [EMPTY -1] (0..127)
. . . . . parameterValue .  CHOICE [EMPTY -1] ...
. . . . . unsignedMin = 29 .  INTEGER [EMPTY -1] (0..65535)
. . . . . * .  SEQUENCE [EMPTY -1] ...
. . . . . parameterIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 3 .  INTEGER [EMPTY -1] (0..127)
. . . . . parameterValue .  CHOICE [EMPTY -1] ...
. . . . . unsignedMin = 81 .  INTEGER [EMPTY -1] (0..65535)
. . . . . * .  SEQUENCE [EMPTY -1] ...
. . . . . parameterIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 6 .  INTEGER [EMPTY -1] (0..127)
. . . . . parameterValue .  CHOICE [EMPTY -1] ...
. . . . . unsignedMin = 15 .  INTEGER [EMPTY -1] (0..65535)
. . . . . * .  SEQUENCE [EMPTY -1] ...
. . . . . parameterIdentifier .  CHOICE [EMPTY -1] ...
. . . . . standard = 4 .  INTEGER [EMPTY -1] (0..127)
. . . . . parameterValue .  CHOICE [EMPTY -1] ...
. . . . . unsignedMin = 7 .  INTEGER [EMPTY -1] (0..65535)
. . . . multiplexParameters .  CHOICE [EMPTY -1] ...
. . . . . h2250LogicalChannelParameters .  SEQUENCE [EMPTY -1] ...
. . . . . sessionID = 2 .  INTEGER [EMPTY -1] (0..255)
. . . . . mediaControlChannel .  CHOICE [EMPTY -1] ...
. . . . . unicastAddress .  CHOICE [EMPTY -1] ...
. . . . . iPAddress .  SEQUENCE [EMPTY -1] ...
. . . . . network = 4 '.e.' =0xac10650b <172.16.101.11> .OCTET STRING
[EMPTY -1]
. . . . . tsapIdentifier = 50137 .  INTEGER [EMPTY -1] (0..65535)
. . . . . dynamicRTPPayloadType = 109 .  INTEGER [EMPTY -1] (96..127)
. . . . . mediaPacketization .  CHOICE [EMPTY -1] ...
. . . . . rtpPayloadType .  SEQUENCE [EMPTY -1] ...
. . . . . payloadDescriptor .  CHOICE [EMPTY -1] ...
. . . . . oid = 8 {itu-t recommendation h 241 0 0 0 0}.OBJECT
IDENTIFIER [EMPTY -1]
. . . . . payloadType = 109 .  INTEGER [EMPTY -1] (0..127)
```

This table outlines H.241 to H.264 mappings.

Identifier	Description
Capability name	ITU-T Rec H.241 H.264 Video Capabilities
Capability identifier type	Standard
Capability identifier value	{itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) generic-capabilities(1)}
maxBitRate	This field shall be included, in units of 100 bit/s. This field represents the maximum bitrate of the H.264 Type II bitstream as defined in Annex C/H. 264.
collapsing	This field shall contain the H.264 Capability Parameters.

Capabilities

The H.264 capability set is structured as a list of one or more H.264 capabilities, each of which has:

- Profile (mandatory)
- Level (mandatory)
- Zero or more additional parameters

These capabilities communicate the ability to decode using one or more H.264 profiles contained in a GenericCapability structure. For each H.264 capability, optional parameters can appear. These parameters permits a terminal to communicate that it has capabilities in addition to meeting the support requirements for the signaled profile and level.

Optional parameters include: CustomMaxMBPS, CustomMaxDPB, CustomMaxBRandCPB, MaxStaticMBPS, max-rcmd-unit-size, max-nal-unit-size, SampleAspectRatiosSupported, AdditionalModesSupported, amd AdditionalDisplayCapabilities.

H.264 Media Packetization

For H.323, systems signal their H.264 mediaPacketization by including: MediaPacketizationCapability.rtpPayload.Type.payloadDescriptor.oid, with the OID having the value {itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) iPpacketization(0) h241AnnexA(0)}.

In compliance with RFC 3984's non-interleaved mode, the following is supported: MediaPacketizationCapability.rtpPayloadType.payloadDescriptor.oid, with the OID having the value {itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) iPpacketization(0) RFC3984NonInterleaved(1)}.

In compliance with RFC 3984's interleaved mode, the following is supported: MediaPacketizationCapability.rtpPayloadType.payloadDescriptor.oid, with the OID having the value {itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0)iPpacketization(0) RFC3984Interleaved(2)}.

H.264 in SIP

H.264 in SIP can contain these optional parameters, which be included in the "a=fmtp" line of SDP if they appear: profile-level-id, max-mbps, max-fs, max-cpb, max-dpb, maxbr, redundant-pic-cap, sprop-parameter-sets, parameter-add, packetization-mode, spropinterleaving-depth, deint-buf-cap, sprop-deint-buf-req, sprop-init-buf-time, sprop-max-dondiff, and max-rcmd-nalu- size.

The profile-level-id parameter is a base 16[6] hexidecimal representation of the following three bytes in sequence:

1. profile_idc
2. profile_oip—Composed of the values from constraint_set0_flag, constraint_set1_flag, constraint_set2_flag, and reserved_zero_5bits—in order of bit significance, starting from the most significant bit.

3. level_idc—Note that reserved_zero_5bits is required to be equal to 0 in [1], but other values for it may be specified in the future by ITU-T or ISO/IEC.

H.264 Packetization Mode

In SIP, the packetization-mode parameter signals the properties of the RTP payload type or the capabilities of a receiver's implementation. Only a single configuration point can be indicated. So when capabilities support more than one packetization-mode are declared, multiple configuration points (RTP payload types) must be used.

- When the value of packetization-mode equals 0 or packetization-mode is not present, the single NAL mode is used.
- When the value of packetization-mode equals 1, the non- interleaved mode is used.
- When the value of packetization-mode equals 2, the interleaved mode is used.

This example shows a SIP offer-answer exchange. Here is the offer SDP:

```
m=video 49170 RTP/AVP 100 99 98
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=42A01E; packetization-mode=0;
a=rtpmap:99 H264/90000
a=fmtp:99 profile-level-id=42A01E; packetization-mode=1;
a=rtpmap:100 H264/90000
a=fmtp:100 profile-level-id=42A01E; packetization-mode=2;
```

And here is the answer SDP for the example:

```
m=video 49170 RTP/AVP 100 99 97
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42A01E; packetization-mode=0;
a=rtpmap:99 H264/90000
a=fmtp:99 profile-level-id=42A01E; packetization-mode=1;
a=rtpmap:100 H264/90000
a=fmtp:100 profile-level-id=42A01E; packetization-mode=2;
```

H.264 IWF Conversions

This section contains two table that show profile, level, and media packetization conversions for H.264 undergoing interworking.

Profile	H.264 in SIP	H.264 (H.241 in H.323)
H264_PROFILE_STR_BASELINE	66	64
H264_PROFILE_STR_MAIN	77	32
H264_PROFILE_STR_EXTENDED	88	32

H.264 Level	H.2264 in SIP	H.264 (H.241 in H.323)	Constraints
1	10	15	0x00
1b	11	19	0x10
1.1	11	22	0x00
1.2	12	29	0x00
1.3	13	36	0x00
2	20	43	0x00
2.1	21	50	0x00
2.2	22	57	0x00

H.264 Level	H.2264 in SIP	H.264 (H.241 in H.323)	Constraints
3	30	64	0x00
3.1	31	71	0x00
3.2	32	78	0x00
4	40	85	0x00
4.1	41	92	0x00
4.2	42	99	0x00
5	50	106	0x00
5.1	51	113	0x00

H.264 SIP Packetization	H.264 (H.241 in H.323) OID in mediaPacketization
packetization-mode=0	{itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) iPpacketization(0) h241AnnexA(0)}
packetization-mode=1	{itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) iPpacketization(0) RFC3984NonInterleaved(1)}
packetization-mode=2	{itu-t(0) recommendation(0) h(8) 241 specificVideoCodecCapabilities(0) h264(0) iPpacketization(0) RFC3984Interleaved(2)}

IWF Unsupported Parameters

The following H.241 parameters are not supported for interworking: CustomMaxMBPS, CustomMaxFS CustomMaxDPB, CustomMaxBRandCPB, MaxStaticMBPS, max-rcmd-nal-unit-size, max-nal-unit-size, SampleAspectRatiosSupported, AdditionalModesSupported, and AdditionalDisplayCapabilities.

The following SDP parameters are not supported for interworking: max-mbps, max-fs, max-cpb, max-dpb, maxbr, redundant-pic-cap, sprop-parameter-sets, parameter-add, spropinterleaving-depth, deint-buf-cap, sprop-deint-buf-req, sprop-init-buf-time, sprop-max-dondiff, and max-rcmd-nalu-size.

H.263+ in H.323

This section describes the H.264 capabilities and media packetization in H.323. Capability exchange signaling looks like this:

```
. . . . . capability .  CHOICE [EMPTY -1] ...
. . . . . . receiveVideoCapability .  CHOICE [EMPTY -1] ...
. . . . . . . h263VideoCapability .  SEQUENCE [EMPTY -1] ...
. . . . . . . . sqcifMPI = 1 .  INTEGER [EMPTY -1] (1..32)
. . . . . . . . qcifMPI = 1 .  INTEGER [EMPTY -1] (1..32)
. . . . . . . . cifMPI = 1 .  INTEGER [EMPTY -1] (1..32)
. . . . . . . . maxBitRate = 1000 .  INTEGER [EMPTY -1] (1..192400)
. . . . . . . . unrestrictedVector = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . arithmeticCoding = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . advancedPrediction = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . pbFrames = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . temporalSpatialTradeOffCapability = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . errorCompensation = 0 .  BOOLEAN [EMPTY -1]
. . . . . . . . h263Options .  SEQUENCE [EMPTY -1] ...
```

```
. . . . . advancedIntraCodingMode = 1 .  BOOLEAN [EMPTY -1]
. . . . . deblockingFilterMode = 1 .  BOOLEAN [EMPTY -1]
. . . . . improvedPBFramesMode = 0 .  BOOLEAN [EMPTY -1]
. . . . . unlimitedMotionVectors = 0 .  BOOLEAN [EMPTY -1]
. . . . . fullPictureFreeze = 1 .  BOOLEAN [EMPTY -1]
. . . . . partialPictureFreezeAndRelease = 0 .  BOOLEAN [EMPTY -1]
. . . . . resizingPartPicFreezeAndRelease = 0 .  BOOLEAN [EMPTY -1]
. . . . . fullPictureSnapshot = 0 .  BOOLEAN [EMPTY -1]
. . . . . partialPictureSnapshot = 0 .  BOOLEAN [EMPTY -1]
. . . . . videoSegmentTagging = 0 .  BOOLEAN [EMPTY -1]
. . . . . progressiveRefinement = 0 .  BOOLEAN [EMPTY -1]
. . . . . dynamicPictureResizingByFour = 0 .  BOOLEAN [EMPTY -1]
. . . . . dynamicPictureResizingSixteenthPel = 1 .  BOOLEAN [EMPTY -1]
. . . . . dynamicWarpingHalfPel = 0 .  BOOLEAN [EMPTY -1]
. . . . . dynamicWarpingSixteenthPel = 0 .  BOOLEAN [EMPTY -1]
. . . . . independentSegmentDecoding = 0 .  BOOLEAN [EMPTY -1]
. . . . . slicesInOrder-NonRect = 0 .  BOOLEAN [EMPTY -1]
. . . . . slicesInOrder-Rect = 0 .  BOOLEAN [EMPTY -1]
. . . . . slicesNoOrder-NonRect = 0 .  BOOLEAN [EMPTY -1]
. . . . . slicesNoOrder-Rect = 0 .  BOOLEAN [EMPTY -1]
. . . . . alternateInterVLCMode = 1 .  BOOLEAN [EMPTY -1]
. . . . . modifiedQuantizationMode = 1 .  BOOLEAN [EMPTY -1]
. . . . . reducedResolutionUpdate = 0 .  BOOLEAN [EMPTY -1]
. . . . . separateVideoBackChannel = 0 .  BOOLEAN [EMPTY -1]
. . . . . videoBadMBsCap = 0 .  BOOLEAN [EMPTY -1]
. . . . . h263Version3Options .  SEQUENCE [EMPTY -1] ...
. . . . . . dataPartitionedSlices = 0 .  BOOLEAN [EMPTY -1]
. . . . . . fixedPointIDCT0 = 0 .  BOOLEAN [EMPTY -1]
. . . . . . interlacedFields = 0 .  BOOLEAN [EMPTY -1]
. . . . . . currentPictureHeaderRepetition = 0 .  BOOLEAN [EMPTY -1]
. . . . . . previousPictureHeaderRepetition = 0 .  BOOLEAN [EMPTY -1]
. . . . . . nextPictureHeaderRepetition = 0 .  BOOLEAN [EMPTY -1]
. . . . . . pictureNumber = 0 .  BOOLEAN [EMPTY -1]
. . . . . . spareReferencePictures = 0 .  BOOLEAN [EMPTY -1]
```

H.263+ in SIP

H.263+ in SIP appears looks like this:

```
a=rtpmap:100 H263-1998/90000
a=fmtp:100 CIF=1; QCIF=1; SQCIF=1; D=1; F=1; I=1; J=1; L=1; S=1; T=1
a=rtpmap:34 H263/90000
a=fmtp:34 CIF=1; QCIF=1; SQCIF=1
```

H.263+ IWF Conversions

This section contains a table showing H.263+ conversions for SIP-h.323 interworking.

H.263+ in H.323 **Parameters (Annex) in ftmp line**	**H.263+ in SIP**
sqcifMPI	SQCIF
qcifMPI	QCIF
cifMPI	CIF
	CIF4
	CIF16
maxBitRate	
unrestrictedVector	D

H.263+ in H.323 Parameters (Annex) in ftmp line	H.263+ in SIP
arithmeticCoding	E
advancedPrediction	F
pbFrames	G
temporalSpatialTradeOffCapability	
errorCompensation	H
h263Options	
advancedIntraCodingMode	I
deblockingFilterMode	J
improvedPBFramesMode	
unlimitedMotionVectors	
fullPictureFreeze	L
partialPictureFreezeAndRelease	
resizingPartPicFreezeAndRelease	
fullPictureSnapshot	
partialPictureSnapshot	
videoSegmentTagging	
progressiveRefinement	
dynamicPictureResizingByFour	P = 1
dynamicPictureResizingSixteenthPel	P = 2
dynamicWarpingHalfPel	P = 3
DynamicWarpingSixteenthPel	P = 4
independentSegmentDecoding	R
slicesInOrder-NonRect	K = 1
slicesInOrder-Rect	K = 2
slicesNoOrder-NonRect	K = 3
slicesNoOrder-Rect	K = 4
alternateInterVLCMode	S
modifiedQuantizationMode	T
reducedResolutionUpdate	Q
separateVideoBackChannel	
videoBadMBsCap	
	PAR
	CPCF

H.263+ in H.323 Parameters (Annex) in ftmp line	H.263+ in SIP
	CUSTOM
h263Version3Options	

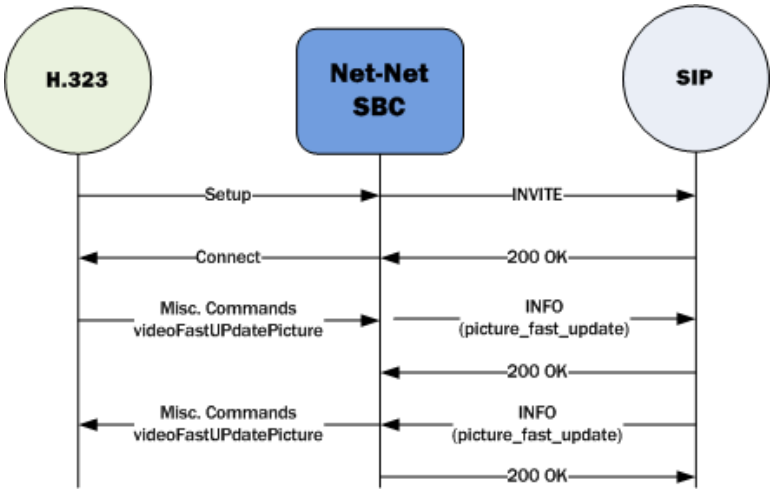
There no configuration for this capability; it is enabled automatically.

IWF Unsupported Parameters

The following optional SDP parameters are not supported for H.263+ interworking: SQCIF, QCIF, CIF, CIF4, CIF16, CUSTOM, PAR, CPCF.

SIP-H.323 IWF in Video Conferencing Applications

For video conferencing and other video applications, the Net-Net SBC supports interworking between the H.323 Miscellaneous Commands videoFastUpdatePicture and the SIP INFO containing XML schema for Full Update. The noted H.323 message commands the video encoder to enter fast-update mode.



There is no configuration required for the interworking between these two messages to work.

SIP REFER-to-BYE

The Net-Net SBC SIP REFER-to-BYE capability addresses situations when other network elements do not support the REFER method but do offer blind transfer in a SIP BYE request. The target number is encoded in a Reason header of the BYE request. In such cases, the Net-Net SBC terminates the REFER and passes the Refer-To number in a Reason header of the BYE.

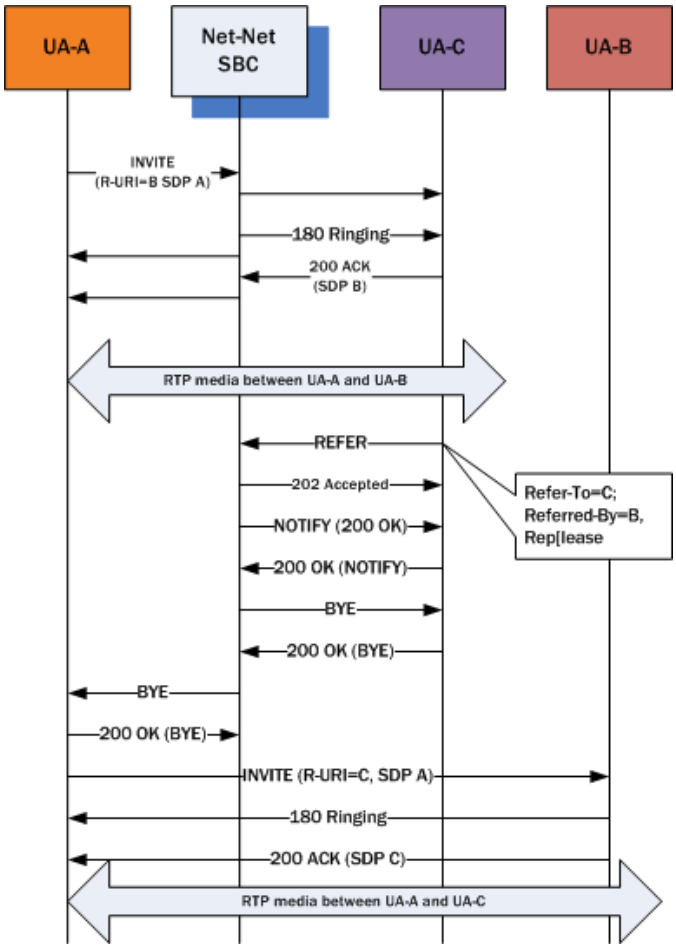
You configure both SIP interfaces and SIP session agents with the refer-to-bye option to use this function:

- SIP interface—You add this ability to SIP interfaces facing the SIP elements that need to receive a BYE instead of a REFER. This setting only applies when the next hop is not a session agent.
- SIP session agent—The SIP session agent takes precedence over the SIP interface. You add this ability to SIP session agents that need to receive a BYE instead of a REFER. If the next hop SIP element—the remote target in the dialog—is a session agent, in other words, you need to configure the option for it. Note that when you use this option for SIP session agents, the SIP interface or realm on which the REFER is received takes precedence over the REFER-to-BYE capability.

When a REFER request arrives and the REFER-to-BYE capability applies, the Net-Net SBC responds to it with a 202 Accepted and sends a NOTIFY to terminate the implicit refer subscription. This NOTIFY contains a message/sipfrag body with SIP/2.0 200 OK. Upon receiving the response to this NOTIFY, the Net-Net SBC sends a BYE with an added Reason header (encoded with the Refer-To number) to the other end.

The network element that does not accept REFERs takes the BYE with the Reason header and issues a new initial INVITE that initiates transfer, which the Net-Net SBC sees as starting a new and independent session.

The diagram below shows how the REFER-to-BYE capability works.



SIP REFER-TO-BYE Configuration

You can configure this capability either for a SIP interface or SIP session agent. Since the configuration steps are the same once you create or edit a configuration, this section uses the SIP session agent as an example.

To enable REFER-to-BYE for a SIP session agent:

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

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

2. Type session-router and press Enter.

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

3. Type session-agent and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

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

4. options——Your entry will look like this:

```
ACMEPACKET(session-agent)# options refer-to-bye
```

You can you the plus sign (+) and the minus sign (-) to add and remove values from the options list.

To remove a value, your entry would look like this:

```
ACMEPACKET(session-agent)# options -refer-to-bye
```

To add a value, your entry would look like this:

```
ACMEPACKET(session-agent)# options +refer-to-bye
```

5. Type done and continue.

Offerless Bandwidth CAC for SIP

For SIP sessions offerless INVITEs (i.e., INVITEs that have no SDP offer), the Net-Net SBC can reserved bandwidth and support the session if you set up applicable media profile associations in the global SIP configuration. Otherwise, the Net-Net SBC terminates these sessions.

You configure support for offerless bandwidth CAC by setting up your global SIP configuration with the options parameters set to offerless-media-bw-profiles. The option takes multiple media profile names as values to apply when treating offerless INVITEs. When such an INVITE arrives and your configuration supports this option, the Net-Net SBC checks and reserves bandwidth for the session. If there is insufficient bandwidth to reserve, the Net-Net SBC terminates the session. Otherwise, the actual SDP negotiation takes place unaffected while the Net-Net SBC forwards the offerless INVITE. Once the negotiation completes, theNet-Net SBC updates bandwidth reservation.

If the called party's actual bandwidth needs exceed available bandwidth, theNet-Net SBC must terminate the session, even if the session is ringing or answered. To minimize this occurrence as much as possible, you should consider all case scenarios when you select media profiles to use with the offerless-media-bw-profiles option.

Offerless Bandwidth CAC for SIP Configuration

To configure offerless bandwidth CAC for SIP:

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

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

2. Type session-router and press Enter.

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

3. Type sip-config and press Enter. If you are editing a pre-existing configuration, you needs to select it before you can make changes.

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

4. options——Your entry will look like this:

```
ACMEPACKET(sip-config)# options offerless-bw-media-profiles=PCMU,G729
```

You can you the plus sign (+) and the minus sign (-) to add and remove values from the options list.

5. Type done and continue.

Diameter Rx: Opening for RTCP Flows

When the Net-Net SBC functions as the AF (i.e., A-SBC or P-CSCF), you can configure it to explicitly open RTCP ports, just as it does for RTP. Without explicitly opening these ports, theNet-Net SBC relies on possibly unreliable PDN-GWs and BRAs to open RTCP ports and it sends only RTP information in AARs.

In external bandwidth managements configurations where the application mode is Rx and the include-rtcp-in-request parameters is enabled, the Net-Net SBC ensures RTCP ports are opened. It sends AAR requests to the policy server (PCRF) that contain both RTP and RTCP, opening the gates (ports) for both RTP and RTCP flows. RTCP information in the AAR is the number of the RTP port plus one (RTP port + 1 = RTCP ports) for all sessions. Flow information for RTCP is part of a different Media-Sub-component AVP as the RTP, but under the same Media-Component-Description AVP. RTCP flow information will also include the Flow-Usage AVP with RTCP (1). The RTCP port is set to 0 when the RTP ports is also unknown and therefore set to 0.

Diameter Rx Opening for RTCP Flows Configuration

When you enable theNet-Net SBC to open RTCP ports, remember that you must set the application-mode parameter to Rx.

To include RTCP information in AAR requests:

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

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

2. Type media-manager and press Enter.

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

3. Type ext-policy-server and press Enter. If you are adding this feature to a pre-existing configuration, you will need to select and edit it.

```
ACMEPACKET(media-manager)# ext-policy-server
ACMEPACKET(ext-policy-server)#
```

4. application-mode—Set this parameter to Rx.
5. include-rtcp-in-request—Change this parameter from disabled (default), to enabled so the Net-Net SBC will include RTCP information in AARs. RTCP information is the number of the RTP port plus one (RTP port + 1 = RTCP ports) for all sessions.
6. Type done and continue.

New KPIs for SIP Signaling

In Net-Net SBC Releases S-C(X)6.2.0M6 and later, you can collect and view realm-based statistics for your Net-Net SBC. Prior to this release, statistical information for registration and sessions are primarily gathered on a global basis. Gathering statistics by realm can enable you to manage your network more effectively, especially when—for instance—individual signaling cores and services are assigned to different realms. You can access this information via and HDR CSV file or the ACLI.

About Registration Statistics

This section describes the registration statistics you can access on a per-realm basis. The Net-Net SBC supports three categories of registration statistics:

- Initial registrations
- Refresh registrations
- De-registrations

Each category has three counters: the total received, the number of successful REGISTER messages, and the number of unsuccessful REGISTER messages. All counters are based on the messages ingress realm. For example, when a de-registration message arrives on a realm different from the realm of the initial registration, the de-registration counter for the realm where the de-registration arrives increments.

HDR Registration Statistics

HDR now supports a group called registration-realm, which gathers the registration statistics. This table shows you the data HDR collects.

Header Name	Description
Realm Name	Name of the realm
Total Initial Registrations	Total number of initial registrations. This counter does not increment when registrations are challenged by 401, 407, or 423 responses. The counter only increments once for each initial REGISTER, even when the REGISTER is challenged.
Successful Initial Registrations	Number of successful registration. This counter increments the response to an initial registration is 200 OK.
Unsuccessful Initial Registrations	Number of unsuccessful registrations. This counter increments when the response to the initial REGISTER has a non-success status code other than 401, 407, or 423. When a 401, 407, or 423 is received, no counters are incremented.
Total Refresh Registrations	Total number of refresh registrations.
Successful Refresh Registrations	Number of successful refresh registrations.
Unsuccessful Refresh Registrations	Number of unsuccessful refresh registrations.
Total Deregistrations	Total number of deregistrations.
Successful Deregistrations	Number of successful deregistrations.
Unsuccessful Deregistrations	Number of unsuccessful deregistrations.

About Session Statistics

Session statistics counters are incremented for ingress and egress realms. The ingress realm is the realm on which the INVITE is received. The egress realm is the realm from which the outgoing INVITE was sent.

HDR Session Statistics

HDR's session-realm group now collects information about early and successful session. This table shows you the data HDR collects.

Header Name	Description
Early Sessions	Number of 18X responses processed. When there is no 180X for a call flow, the counter increments is established with a 200 OK. The counter represents the number of sessions that have reached the early dialog state or later.
Successful Sessions	Number of 200 OK responses received for an initial INVITE. This counter is not incremented for reINVITES.

This is an example of the session-realm group HDR, with the new headers in bold font:

```
TimeStamp,Realm Name,Inbound Active Sessions,Inbound Session Rate,Outbound
Active Sessions, Outbound Session Rate, Inbound Sessions Admitted,Inbound
Sessions Not Admitted,Inbound Concurrent Sessions High,Inbound Average
Session Rate,Outbound Sessions Admitted,Outbound Sessions Not
Admitted,Outbound Concurrent Sessions High,Outbound Average Sessions Rate,Max
Burst Rate,Total Seizures,Total Answered Sessions,Answer/Seizure
```

```
Ratio,Average One-Way Signaling Latency,Maximum One-Way Signaling
Latency,Average QoS RFactor,Maximum QoS RFactor,Current QoS Major
Exceeded,Total QoS Major Exceeded,Current QoS Critical Exceeded,Total QoS
Critical Exceeded, Early Sessions, Successful Sessions
```

ACLI Show Command Extension

When entered with the name of a specific realm, the ACLI show sip realms command displays information about registrations and sessions for that realm. The following example shows the augmented command output:

New command data

```
ACMEPACKET# show sipd realms public
12:03:49-54
Realm public() [In Service]
                                        -- Period -- -------- Lifetime --------
                                Active    High   Total      Total  PerMax    High
Inbound Sessions                0         0      0          0      0         0
  Rate Exceeded                 -         -      0          0      0         -
  Num Exceeded                  -         -      0          0      0         -
  Burst Rate                    0         0      0          0      0         0
  Reg Rate Exceeded             -         -      0          0      0         -
  Reg Burst Rate                0         0      0          0      0         0
Outbound Sessions               0         0      0          0      0         0
  Rate Exceeded                 -         -      0          0      0         -
  Num Exceeded                  -         -      0          0      0         -
  Burst Rate                    0         0      0          0      0         0
  Reg Rate Exceeded             -         -      0          0      0         -
Out of Service                  -         -      0          0      0         -
Trans Timeout                   0         0      0          0      0         0
Requests Sent                   -         -      0          43     30        -
Requests Complete               -         -      0          42     20        -
Seizure                         -         -      0          0      0         -
Answer                          -         -      0          0      0         -

ASR Exceeded                    -         -      0          0      0         -
Requests Received               -         -      0          0      0         -
QoS Major Exceeded              -         -      0          0      0         -
QoS Critical Exceeded           -         -      0          0      0         -
Latency=0.000; max=0.000
QoS R-Factor Avg=0.00; max=0.00
Early Sessions                  -         -      0          24     10        -
Successful Sessions             -         -      0          42     20        -
Initial Registrations
 Total                          0         0      0          0      0         0
 Successful                     0         0      0          0      0         0
 Unsuccessful                   0         0      0          0      0         0
Refresh Registrations
 Total                          0         0      0          0      0         0
 Successful                     0         0      0          0      0         0
 Unsuccessful                   0         0      0          0      0         0
De-Registrations
 Total                          0         0      0          0      0         0
 Successful                     0         0      0          0      0         0
 Unsuccessful                   0         0      0          0      0         0
```

HDR Registration Configuration

If your HDR configuration is already configured with the “session-realm” group, you do not need to add it to receive per-realm statistics for sessions. If you want HDR data for registrations per realm, then you need to add the registration-realm group to your configuration.

To add the registration-realm group to your HDR configuration:

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

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

2. Type system and press Enter.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type system-config and press Enter.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type group-settings and press Enter.

```
ACMEPACKET(system-config)# group-settings
ACMEPACKET(group-settings)#
```

5. group-name—Set this parameter to registration-realm.
6. sample-interval—Enter the time in minutes for how often you want theNet-Net SBC to sample data records for the specified group. The minimum is 0; the maximum is 120.
7. start-time—Enter the exact date and time (for your local timezone) when you want the Net-Net SBC start collecting records for this group. This time is either now or a time in the future. Your entry must be in the format yyyy-mm-dd-hh:mm:ss, where yyyy is the year, mm is the month, dd is the day, hh is the hours, mm is the minutes, and ss is the second. There is no default for this parameter.
8. end-time—Enter the exact date and time (for your local timezone) when you want the Net-Net SBC stop collecting records for this group. This time is either never or a time in the future. Your entry must be in the format yyyy-mm-dd-hh:mm:ss, where yyyy is the year, mm is the month, dd is the day, hh is the hours, mm is the minutes, and ss is the second. There is no default for this parameter.
9. Type done and continue.

Service-URN AVP for Emergency Calls

When it receives an emergency/priority call on an active Rx interface, the Net-Net SBC will add the Service-URN AVP as the main AVP to its DIAMETER AAR messages. The Service-URN AVP has 525 as its code and is a string type; it indicates that an AF session is used for emergency traffic.

The Net-Net SBC Service-URN will contain a SIP INVITE's service URN when present. In these cases, the Net-Net SBC does not use the urn:service string in the AVP. Instead, for example, it includes sos.fire for a SIP INVITE's service URN of urn: service: sos.fire. Without a service URN in the SIP INVITE, he Net-Net SBC populates the AVP with sos.

Your Net-Net SBC must be configured to identify emergency calls (in applicable net-management-control and realm configurations) and the external policy control configuration's application mode must be set to Rx for this capability to work properly.

7

S-C(X)6.2.0M7

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M7.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M7.

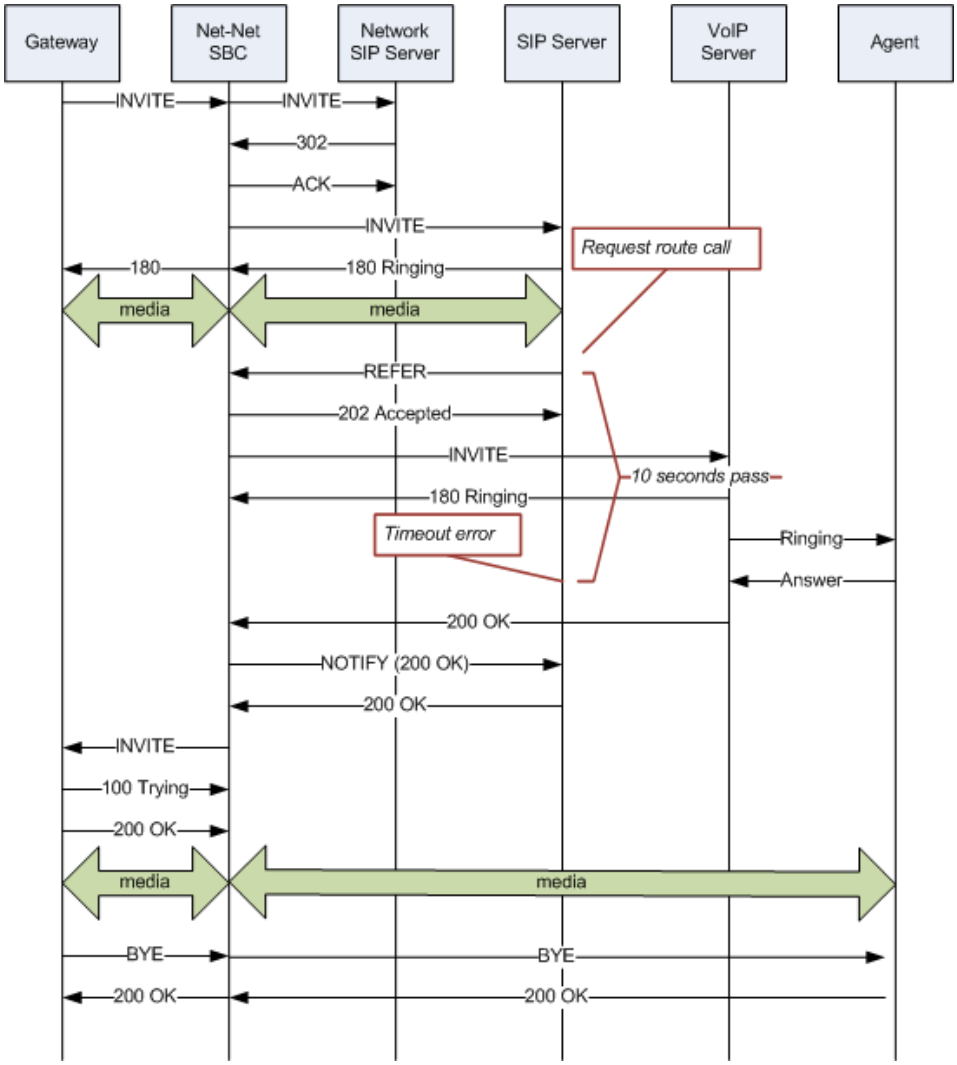
Content Type	Description
Adaptation	2944 - Immediate/180 NOTIFY in Refer Call Transfer
Adaptation	2942 - Diameter: Rx Bearer plane event notifications
Adaptation	2526 - SIP Redirect: Embedded Routes Support
Adaptation	2820 - Configurable MTU size per individual physical interfaces
Forward Merge	S-C6.1.0M9
Forward Merge	S-C6.1.0M10

180 & 100 NOTIFY in REFER Call Transfers

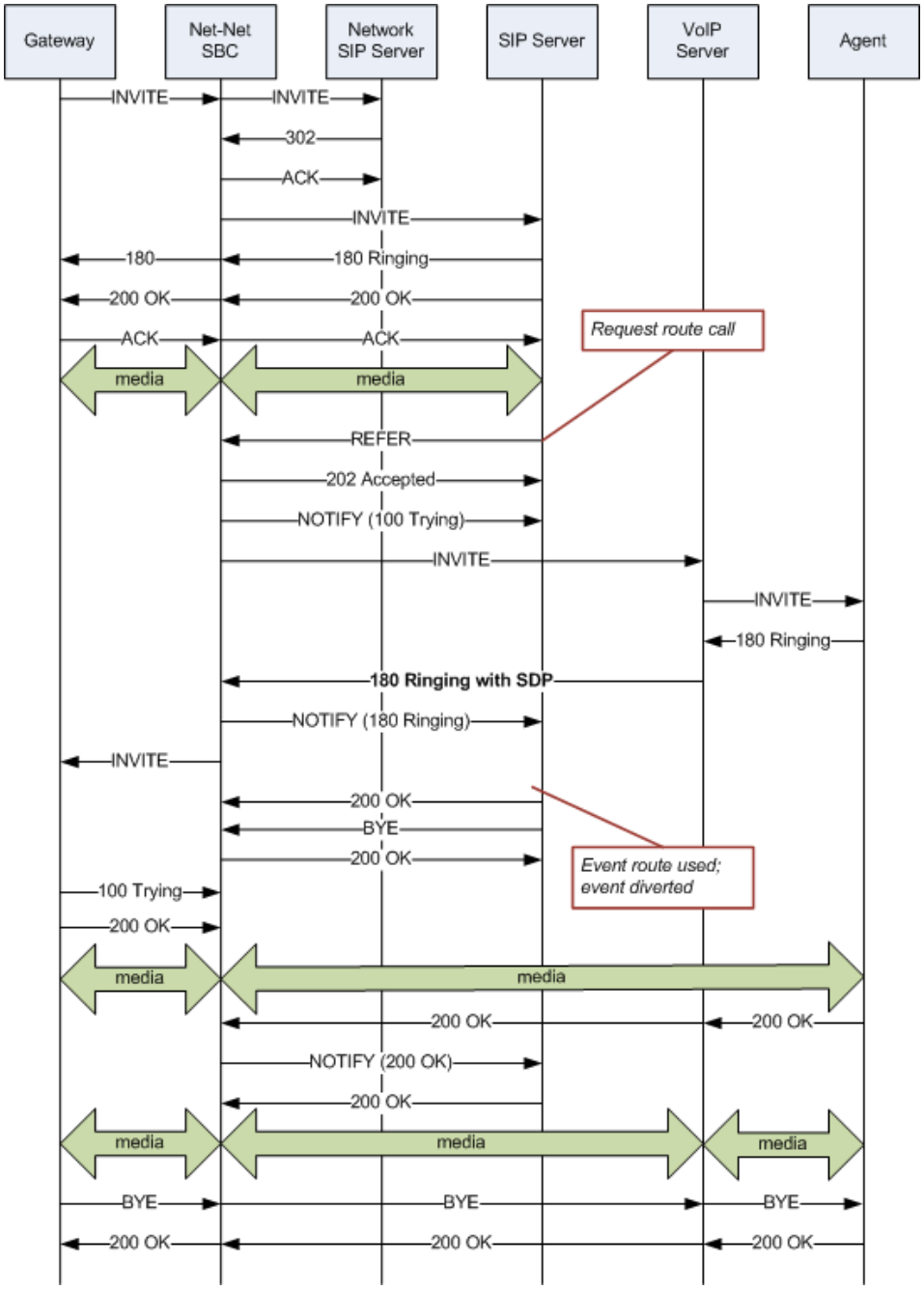
When you configure your Net-Net SBC to support REFER call transfers, you can enable it to send a NOTIFY message after it has received either a 202 Accepted or 180 Ringing message. If your network contains elements that comply with RFC 5589, and so expect the NOTIFY message in response to the 202 Accepted or 180 Ringing, you want to set the refer-notify-provisional to either initial or all, according to your needs.

Without this parameter changed from its default (none), the Net-Net SBC does not return send the NOTIFY until it receives the 200 OK response from the agent being called. If the time between the REFER and the NOTIFY exceeds time limits, this sequencing can cause the Net-Net SBC NOTIFY to go undetected by devices compliant with RFC 5589. Failures during the routing process can result.

You can see how a sample call flow works without setting the refer-notify-provisional parameter.



When you compare the call flow above to the one depicting the scenario when theNet-Net SBC has the refer-notify-provisional changed from its default, you can see that the Net-Net SBC now response with a NOTIFY in response to the 202 Accepted and it sends another after the 180 Ringing.This causes the event to be diverted successfully.



Sample Messages

In compliance with RFC 5589, the NOTIFY message with 100 Trying as the message body looks like the sample below. Note that the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
```

```
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...

SIP/2.0 100 Trying
```

Also in compliance with RFC 25589, the NOTIFY message with 180 Ringing as the message body looks like the sample below. Again, the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...

SIP/2.0 180 Ringing
```

Also in compliance with RFC 25589, the NOTIFY message with 200 OK as the message body looks like the sample below.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 74 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: terminated;reason=noresource
Content-Type: message/sipfrag
Content-Length: ...

SIP/2.0 200 OK
```

100 & 180 NOTIFY Message in REFER Call Transfers Configuration

You can apply the refer-notify-provisional setting to realms or to session agents. This section shows you how to apply the setting for a realm; the same steps and definitions apply to session agents.

If you do not want to insert NOTIFY messages into the exchanges that support REFER call transfers, you can leave the refer-notify-provisional set to none. This means that the Net-Net SBC will send only the final result NOTIFY message. Otherwise, you want to choose one of the two settings described in the instructions below.

To enable 100 and 180 NOTIFY messages in REFER call transfers:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type media-manager and press Enter to access the media-related configurations.

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

3. Type realm-config and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

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

4. refer-notify-provisional—Choose from one of the following settings, where the Net-Net SBC:

   - initial—Sends an immediate 100 Trying NOTIFY, and the final result NOTIFY
   - all—Sends an immediate 100 Trying NOTIFY, plus a notify for each non-100 provisional messages the Net-Net SBC receives; and the final result NOTIFY

```
ACMEPACKET(realm-config)# refer-notify-provisional all
```

5. Save your work.

8

S-C(X)6.2.0M9

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBCRelease S-C(X)6.2.0M9.

Content Map

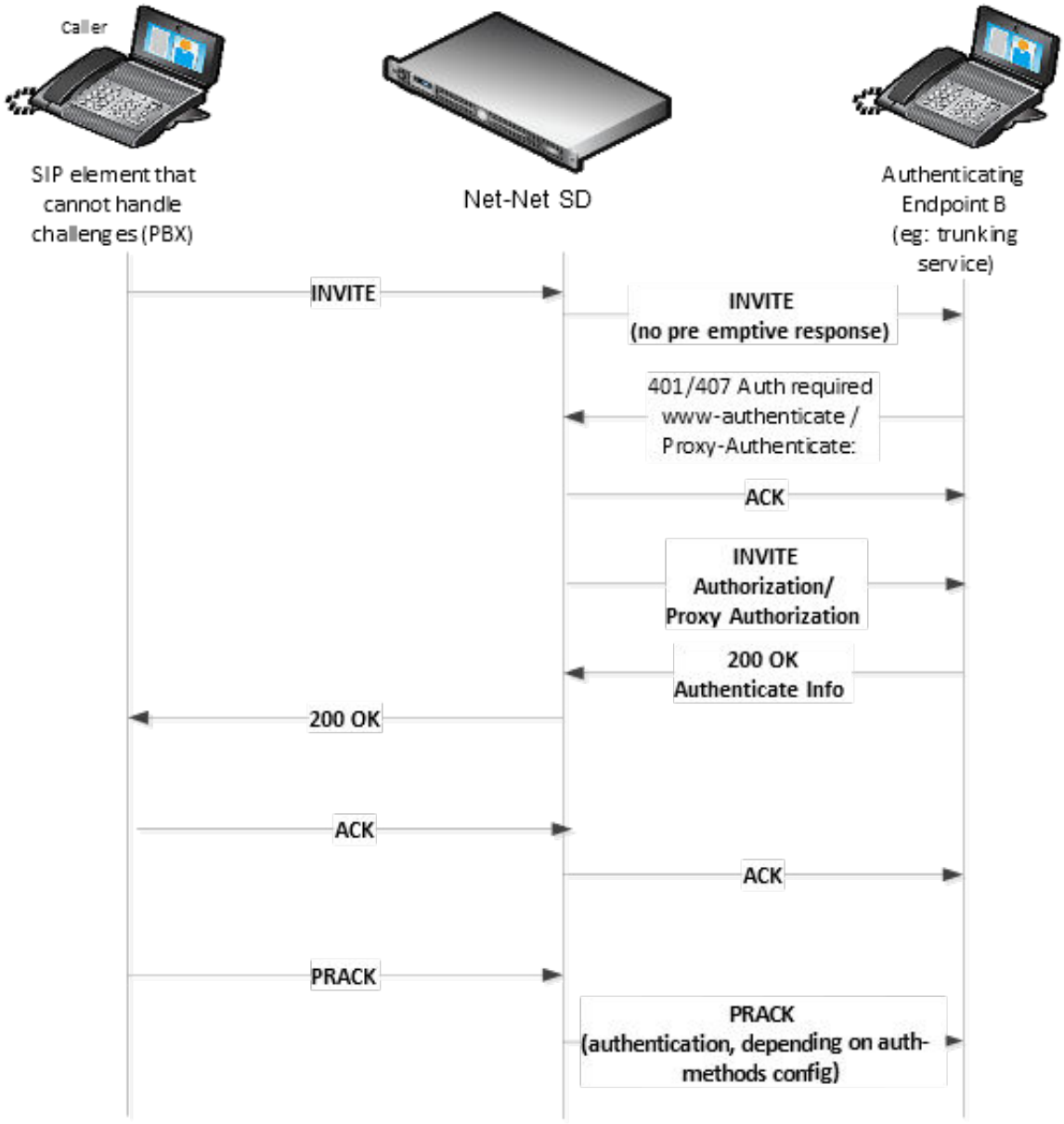
This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M9.

Content Type	Description
Adaptation	3093 - Underscore Configuration in Hostname Support
Adaptation	3047 - SIP INFO DTMF Quick Conversion to RFC2833 Events
Adaptation	2930 - Surrogate Agent Enhancements for Geo Redundancy
Adaptation	2635 - HMR mapping of 100Trying to alternate response value
Adaptation	2666 - Digest Authentication

Digest Authentication with SIP

Digest authentication for Session Initiation Protocol (SIP) is a type of security feature on the Net-Net SBC that provides a minimum level of security for basic Transport Control Protocol (TCP) and User Datagram Protocol (UDP) connections. Digest authentication verifies that both parties on a connection (host and endpoint client) know a shared secret (a password). This verification can be done without sending the password in the clear.

Digest authentication is disabled by default on the Net-Net SBC. When digest authentication is enabled, the Net-Net SBC (host) responds to authentication challenges from SIP trunking Service Providers (endpoint client). The Net-Net SBC performs authentication for each IP-PBX initiating the call. However, the authentication challenge process takes place between the host and the client only since the IP-PBX cannot handle authentication challenges. The following illustration shows the digest authentication process.



The digest authentication scheme is based on a simple challenge-response paradigm. A valid response contains a checksum (by default, the MD5 checksum) of the “username” and password. In this way, the password is never sent in the clear.

By default, the Net-Net SBC uses cached credentials for all requests within the same dialog, once the authentication session is established with a 200OK from the authenticating SIP element. If the in-dialog-methods attribute contains a value, it specifies the requests that have challenge-responses inserted within a dialog.

In digest authentication with SIP, the following can happen:

- More than one authenticating SIP element (IP-PBX) may be the destination of requests.
- More than one authentication challenge can occur in a SIP message. This can occur when there are additional authenticating SIP elements behind the first authenticating SIP element.
- The Net-Net SBC distinguishes whether the IP-PBX is capable of handling the challenge. If Digest Authentication is disabled (no auth-attributes configured) on the Session Agent, the challenge is passed back to the IP-PBX.

Note: If there are multiple challenges in the request, and if the Net-Net SBC has only some of the cached credentials configured, the Net-Net SBC adds challenge-responses for the requests it can handle, and does not pass the challenge back to the IP-PBX.

Challenge-Responses in Requests not in the Dialog

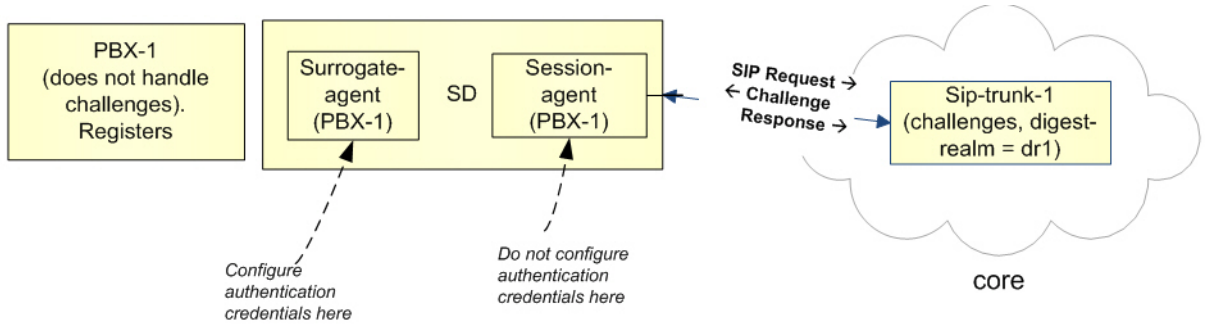
A digest authentication session starts from the client response to a www-authenticate/proxy-authenticate challenge and lasts until the client receives another challenge in the protection space defined by the auth-realm. Credentials are not cached across dialogs; however, if a User Agent (UA) is configured with the auth-realm of its outbound proxy, when one exists, the UA may cache credentials for that auth-realm across dialogs.

Note: Existing Net-Net SBC behavior with surrogate-agents is that they cache credentials from REGISTER for INVITE sessions only if the Net-Net SBC is considered a UA sending to its outbound proxy.

Surrogate Agents and the Net-Net SBC

In the case where a surrogate-agent is configured for the IP-PBX, you do not have to configure digest authentication attributes in the session-agent object for the same IP-PBX. The surrogate-agent authentication configuration takes precedence over the session-agent authentication configuration and so it is ignored.

The following illustration shows an example of a surrogate-agent with a session-agent in the network.



Configuring Digest Authentication

In the Net-Net SBC ACLI, you can access the Digest Authentication object at the path session-router->session-agent->auth-attribute. If enabled, the Digest Authentication process uses the attributes and values listed in this table.

Note: If enabling Digest Authentication, all attributes listed below are required except for the in-dialog-methods attribute which is optional.

The following table lists the digest authentication object

```
ACMEPACKET(auth-attribute)# show
        auth-attribute
                auth-realm                      realm01
                username                        user
                password                        ********
                in-dialog-methods               ACK INVITE SUBSCRIBE
```

To configure digest authentication on the Net-Net SBC:

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

   ```
   ACMEPACKET# configure terminal
   ```

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

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

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

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

4. Type auth-attribute and press Enter to access the digest authentication-related attributes.

```
ACMEPACKET(session-agent)# auth-attribute
ACMEPACKET(auth-attribute)#
```

5. auth-realm — Enter the name (realm ID) of the host realm initiating the authentication challenge. This value defines the protected space in which the digest authentication is performed. Valid value is an alpha-numeric character string. Default is blank.

```
ACMEPACKET(auth-attribute)# auth-realm realm01
```

6. username — Enter the username of the client. Valid value is an alpha-numeric character string. Default is blank.

```
ACMEPACKET(auth-attribute)# username user
```

7. password — Enter the password associated with the username of the client. This is required for all LOGIN attempts. Password displays while typing but is saved in clear-text (i.e., *****). Valid value is an alpha-numeric character string. Default is blank.

```
ACMEPACKET(auth-attribute)# password *******
```

8. in-dialog-methods — Enter the in-dialog request method(s) that digest authentication uses from the cached credentials. Specify request methods in a list form separated by a space enclosed in parentheses. Valid values are:

- INVITE | BYE | ACK | CANCEL | OPTIONS | SUBSCRIBE | PRACK | NOTIFY | UPDATE | REFER

```
ACMEPACKET(auth-attribute)# in-dialog-methods (ack invite subscribe)
```

Note: The methods not in this list are still resubmitted if a 401/407 response is received by the Net-Net SBC.

If you do not specify any in-dialog-method value(s), digest authentication does not add challenge-responses to in-dialog requests within a dialog.

This attribute setting applies to in-dialog requests only.

Additional Notes

The following are additional notes that describe the digest authentication process:

- The Net-Net SBC always challenges the first LOGIN request, and initial authentication begins with that request. The recalculated authorization key — the credentials — are then included in every subsequent request.
- If the Net-Net SBC does not receive any communication from the client within the expiration period, the Net-Net SBC logs the client out and tears down the transport connection. Faced with interface loss, the Net-Net SBC default behavior is to flush all warrant information from the target database. This response necessitates that the client first login/re-register with the Net-Net SBC, and then repopulate the empty database using a series of ADD requests. This behavior ensures that client and Net-Net SBC target databases are synchronized.

  Alternatively, when faced with interface loss, the Net-Net SBC can retain all warrant information within the target database. This response necessitates only that the client first login/re-register with the Net-Net SBC. After successful registration the client should, but is not required to, use a series of GET, ADD, and DELETE requests to ensure that the Net-Net SBC and client target databases are synchronized.
- The Net-Net SBC ignores the Authentication-Info header that comes in the 200OK response after digest authentication is complete. The Net-Net SBC receives a 401/407 response from the client. However, some surrogate-agents may process the Authentication-Info header in a single challenge.

Digest Authentication and High Availability

The Net-Net SBC supports digest authentication in high availability (HA) environments. The session-agent configuration, which includes the digest authentication parameters on the primary Net-Net SBC, are replicated on the HA Net-Net SBC. However, cached credentials on the primary device are not replicated on the HA device.

9

S-C(X)6.2.0M10

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBC Release S-C(X)6.2.0M10.

S-C(X)6.2.0M10

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M10.

Content Type	Description
Adaptation	3099 - 120K TCP/TLS Endpoints

120 000 TCP 100 000 TLS Endpoints

The Net-Net SBC supports a maximum of 120,000 TCP and 100,000 TLS connected endpoints.

10

S-C(X)6.2.0M12

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net SBCRelease S-C(X)6.2.0M12.

Content Map

This section provides a table listing documentation content in Net-Net SBC Release S-C(X)6.2.0M12.

Content Type	Description
Adaptation	Palladion Mediation Engine support

Palladion Mediation Engine

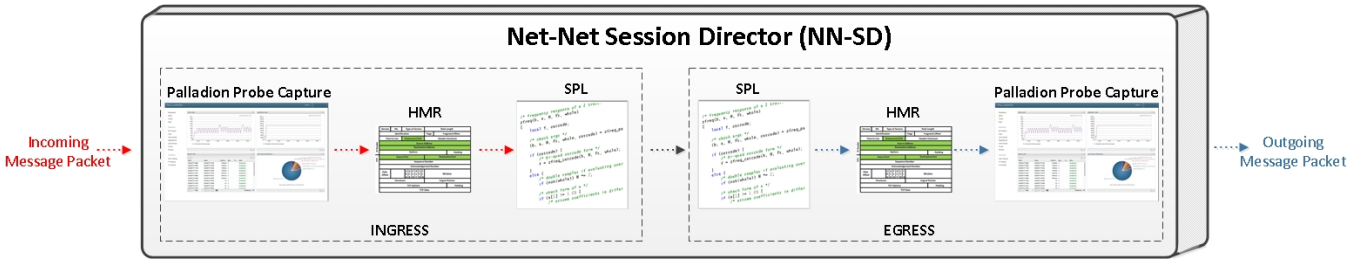
Palladion is Acme Packet's Communication Experience Manager.

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

Version E-C[xz]6.4.0 supports an embedded, user-configurable Palladion Communications Monitoring Probe, Version 1. Acting as a Probe, or as an exporter, the Net-Net SBC can:

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

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



IPFIX

The Net-Net Session Director uses the IPFIX suite of standards to export protocol message traffic and related data to the Palladion Mediation Engine.

- RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*
- RFC 5102, *Information Model for IP Flow Information Export*
- RFC 5470, *Architecture for IP Flow Information Export*
- RFC 5655, *Specification of the IP Flow Information Export (IPFIX) File Format*
- RFC 5815, *Definitions of Managed Objects for IP Flow Information Export*

The IPFIX standards describe the use of templates to format the export of specific types of protocol traffic. The Net-Net Session Director and the Palladion Mediation Engine share ten (10) pre-defined templates that facilitate protocol message exchange, and subsequent processing and analysis by the Palladion Engine.

The pre-defined templates are:

- incoming SIP/DNS over UDP
- incoming SIP over TCP
- incoming SIP over SCTP
- incoming DNS over UDP (entire IP and UDP header not included)
- outgoing SIP/DNS over UDP
- outgoing SIP over TCP
- outgoing SIP over SCTP
- outgoing DNS over UDP (entire IP and UDP header not included)
- media qos and flow record
- IPFIX handshake (used for connection establishment)

Communications Monitor Configuration

Communications Monitor configuration consists of the following steps.

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

   Configuration of the -config object, which defines common operations across all interfaces, is not required. Default values can be retained to enable standard service.
2. Optional assignment of a TLS profile to an exporter/collector pair.

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

Communication Monitor

Use the following procedure to configure communication monitoring:

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

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

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

   Communication monitoring is disabled by default.

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

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

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

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

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

   To specify a media interface (the usual case):

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

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

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

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

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

   Refer to *TLS Profile Configuration* for configuration details.

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

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

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

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

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

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

8. Use the address and port parameters to specify the IP address and port number monitored by a Palladion Mediation Engine for incoming IPFIX traffic.

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

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

9. Use done and exit to return to comm-monitor configuration mode.
10. Use done, exit, and verify-config to complete configuration.

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

TSCF Rekey Profile Configuration

Rekeying is a cryptographic technique that enhances security by enforcing the negotiation of existing keys on an ongoing secure connection. Rekeying can be either time-based, in which case new keys are negotiated at the expiration of a timer, or traffic-based, in which case new keys are negotiated when a threshold byte count is exceeded.

Use the following procedure to configure an optional tscf-rekey-profile. Later, you will assign the profile to a specific TSCF interface. If you do not intend to enforce re-keying, this procedure can be safely ignored.

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

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# tscf
ACMEPACKET(tscf)# tscf-rekey-profile
ACMEPACKET(tscf-rekey-profile)#
```

2. Use the name parameter to provide a unique identifier for this tscf-rekey-profile.

```
ACMEPACKET(tscf-rekey-profile)# name tscfRekey01
ACMEPACKET(tscf-rekey-profile)#
```

3. Use the initiator parameter to identify the rekey initiator.

Supported values are client (default) | server (the Session Director)

```
ACMEPACKET(tscf-rekey-profile)# initiator client
ACMEPACKET(tscf-rekey-profile)#
```

4. Use the max-rekey-time parameter to specify the maximum interval (in minutes) between re-keying operations.

Supported values are 0 (default) | 30 - 1440 (minutes)

The default value, 0, specifies that time-based rekeying is not enforced; other integer values specify that time-based re-keying must be initiated by the tunnel endpoint designated by the initiator parameter.

```
ACMEPACKET(tscf-rekey-profile)# max-rekey-time 30
ACMEPACKET(tscf-rekey-profile)#
```

5. Use the max-rekey-data parameter to specify the maximum traffic exchange (measured in Kb) between rekeying operations.

The default value, 0, specifies that traffic-based rekeying is not enforced; other integer values specify that traffic-based re-keying must be initiated by the tunnel endpoint designated by the initiator parameter.

```
ACMEPACKET(tscf-rekey-profile)# max-rekey-data 0
ACMEPACKET(tscf-rekey-profile)#
```

6. Use done, exit, and verify-config to complete tscf-rekey-profile configuration.

7. Repeat Steps 1 through 6 to configure additional tscf-rekey-profiles as required.

TLS Profile Configuration

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

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

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

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

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

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

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

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

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

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

5. Retain the default value, all, for the cipher-list parameter.
6. Use the verify-depth parameter to specify the maximum number of chained certificates that will be processed while authenticating end-entity certificate received from the Palladion Mediation Engine.

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

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

   a) Check the validity dates (Not Before and Not After fields) of the end certificate. If either date is invalid, authentication fails; otherwise, continue chain validation
   b) Check the maximum length of the certificate chain (specified by verify-depth). If the current chain exceeds this value, authentication fails; otherwise, continue chain validation.
   c) Verify that the Issuer field of the current certificate is identical to the Subject field of the next certificate in the chain. If values are not identical, authentication fails; otherwise, continue chain validation.
   d) Check the validity dates (Not Before and Not After fields) of the next certificate. If either date is invalid, authentication fails; otherwise, continue chain validation.
   e) Check the X509v3 Extensions field to verify that the current certificate identifies a CA. If not so, authentication fails; otherwise, continue chain validation.
   f) Extract the Public Key from the current CA certificate. Use it to decode the Signature field of the prior certificate in the chain. The decoded Signature field yields an MD5 hash value for the contents of that certificate (minus the Signature field).
   g) Compute the same MD5 hash. If the results are not identical, authentication fails; otherwise, continue chain validation.
   h) If the hashes are identical, determine if the CA identified by the current certificate is a trust anchor by referring to the trusted-ca-certificates attribute of the associated TLS-profile configuration object. If the CA is trusted, authentication succeeds. If not, return to Step 2.

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

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

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

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

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

8. Retain the default value, compatibility, for the tls-version parameter.
9. Retain default values for all other parameters.

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

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