Establishing a Diameter Peering Session

In This Chapter

This section provides information about establishing a diameter peering session.

Topics in this section include:

Applicability

This example is applicable to all 7750 SR/SR-c and 7450 ESS chassis.

The configuration was tested on release 12.0.R3.

Overview

Diameter is an Authentication, Authorization and Accounting (AAA) protocol that has been defined by the IETF in RFC 3588, *Diameter Base Protocol*, as a replacement for other AAA protocols like TACACS and RADIUS. While wireline access networks are largely based on RADIUS for subscriber authentication, authorization, and accounting, it was decided by 3rd Generation Partnership Project (3GPP) that wireless access networks will be largely based on Diameter. Over time, operators are looking to converge both types of networks, and one of the aspects of this is to replace RADIUS in wireline access networks by Diameter.

Diameter is based on three layers: the transport layer, the Diameter base protocol layer and the Diameter applications as shown in Figure 369.

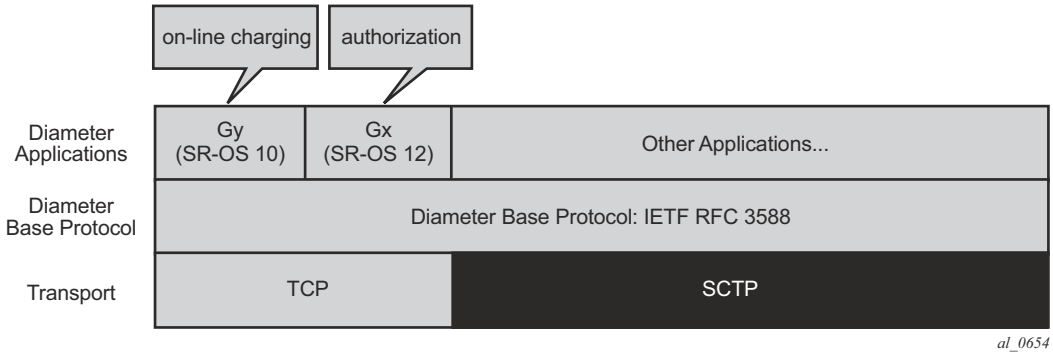

Figure 369: Diameter Protocol Stack

The bottom layer is the transport layer and can be either TCP or SCTP, but only TCP is supported by SR OS. The Diameter base protocol implementation is based on RFC 3588. The top layer contains the Diameter applications. SR OS 10.0 introduced the Gy Diameter application for on-line charging, and SR OS 12.0 introduces the Gx Diameter application for authorization.

Configuration

The Diameter base protocol and the Diameter applications have to be configured separately, where the Diameter base protocol has to be configured first, and the Diameter applications next. The transport layer configuration is part of the Diameter base protocol layer. This example only describes the Diameter base protocol configuration.

The diameter-peer-policy configuration resides in the aaa context and contains the full Diameter base protocol configuration. An example diameter-peer-policy configuration is shown below.

```
configure aaa
     diameter-peer-policy "DSC.26.206" create
          applications gx
          origin-host "wlangw-2.SRrealm"
          origin-realm "SRrealm"
          router 10000
          source-address 10.23.0.130
          peer "DSC.26.206" create
               address 10.40.11.2
               destination-realm "Tc3eRealm"
               no shutdown
          exit
```

The diameter-peer-policy is identified by name (**DSC.26.206** in the example above). This name is used by the Diameter application configuration. The Diameter application making use of this Diameter peer policy must be specified (for instance Gx), and so is the Diameter identity. The Diameter identity consists of 2 parts: the Diameter host name and the Diameter realm, **wlangw-2.SRrealm** and **SRrealm**, respectively, in the example above. Configuration of the Diameter application making use of the Diameter peer is required such that the Diameter connection including the capability exchange, which negotiates the Diameter application with the peer, can already start without configuration of the specific Diameter application.

By default the system originates the Diameter peering session from the Base router but a different routing context (a VPRN or the management routing context used for out-of-band management) can be used (VPRN **10000** in the example). Also a source address (belonging to an IP interface in the configured routing context) can be specified (**10.23.0.130** in the example), but when no source address is specified an address is selected automatically. As such, best practice is to explicitly configure the source address.

One or more peers can be configured, with a maximum of five peers. In case more than one peer is configured, these peers can provide redundancy when supported by the Diameter application making use of the Diameter peer policy. Each peer is identified by name (which could be the same as the Diameter peer policy as in the example above) and has an IP address and a destination Diameter realm (**10.40.11.2** and **Tc3eRealm**, respectively, in the example). The IP address is that of the device terminating the TCP session, which either is the final destination or a Diameter Routing Agent (DRA) (intermediate destination). The destination realm is typically the realm of the final destination. Optionally the destination host can be configured. If the destination host is

not configured, then it will be dynamically learned from the received Diameter application messages (learned from the received origin-host). This means that if it is not configured, the first Diameter application message does not contain a destination-host, only a destination-realm, but all subsequent messages will include the learned destination-host. If destination-host is configured, it will be included in the first Diameter application message. The destination host is configured per peer using following command:

```
*A:BNG-1# configure aaa diameter-peer-policy "DSC.26.206" peer "DSC.26.206" destination-
host
  - destination-host <destination-host-string>
  - no destination-host

 <destination-host-*> : [80 chars max]
```

Configuration of the origin-host, origin-realm, destination-realm and at least 1 peer is mandatory. These attributes do not have default values and are needed before a peer can be put in a **no shutdown** state. Doing a **no shutdown** of a peer fails in case any of these attributes are not configured, for instance:

```
*A:BNG-1>config>aaa>diameter-peer-plcy>peer$ no shutdown
MINOR: DIAM #1205 Origin-host is not configured yet

*A:BNG-1>config>aaa>diam-peer-plcy# peer "test" no shutdown
MINOR: DIAM #1206 Origin-realm is not configured yet

*A:BNG-1>config>aaa>diam-peer-plcy# peer "test" no shutdown
MINOR: DIAM #1208 Destination-realm is not configured yet
```

When doing a **no shutdown** of the peer, the system tries to establish the TCP session. Once the TCP session is up, the system starts the Diameter capability negotiation using the configured attributes: the Diameter identity is advertised together with the configured Diameter applications. An example of a capability negotiation is examined in detail in the troubleshooting section. All Diameter messages are sent with a DSCP set to AF41. The DSCP value cannot be changed.

The status of the Diameter peers can be verified as follows:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.26.206"
===============================================================================
Diameter Peer Policy : DSC.26.206
===============================================================================
Last Mgmt Change      : 03/18/2014 17:50:50
-------------------------------------------------------------------------------
Diameter Base Values (config)
-------------------------------------------------------------------------------
Origin Host           : wlangw-2.SRrealm
Origin Realm          : SRrealm
Connection Timer      : 30 (default)       Source Address     : 10.23.0.130
Transaction Timer     : 30 (default)       Router             : 10000
Watchdog Timer        : 30 (default)
Vendor Support        : 3GPP (default)
-------------------------------------------------------------------------------
Peer Name            Oper  PSM State     Susp  Cooldown  Pref  Order  Pri/Sec
```

```
-------------------------------------------------------------------------------
DSC.26.206           Yes   I-Open        No    -         50    1      Primary
===============================================================================
```

An important information is the **PSM State** of each peer. The state **I-Open** indicates that the peer is up and running. The full Peer State Machine (PSM) is described in RFC 3588.

More advanced configuration can be done as well. Timers can be configured: connection timer, transaction timer and watchdog timer:

- The connection timer is called the Tc timer in RFC 3588. This timer controls the frequency at which a new connection is attempted to be established. The default value is 30 seconds as recommended by RFC 3588.
- The transaction timer is started each time a request is sent to the peer and indicates the time the system waits for an answer before resending the request to one of the other configured peers. In case the Diameter request is retransmitted to another peer, the T-flag (Potentially re-transmitted message flag) is set. Failure of a peer is typically detected by the watchdog messages, but in some cases it is possible that a peer is not responding although watchdog messages are received. This could happen, for instance, when there is a Diameter relay agent or Diameter proxy agent between the system originating the Diameter messages and the final destination.
- The watchdog timer controls the frequency at which device-watchdog-request messages are transmitted to the peer, and is called the Tw timer in RFC 3539, *Authentication, Authorization and Accounting (AAA) Transport Profile*. A small timer results in a faster detection of a peer failure at the expense of generating more messages. The default is 30 seconds.

These timers can be configured at two levels: at Diameter peer policy level and at peer level. If configured at the peer level, then this value is taken for the specific peer, otherwise the configuration is taken from the Diameter peer policy level. If it is also not configured at the policy level, then the default values are used, which is 30 seconds for these three timers.

In case multiple peers are configured in the profile, a preference can be assigned to each of the peers. A lower preference value indicates a more preferred peer. Up to five peers can be configured, and all can be in the **I-Open** state, but the Diameter application will only select a single primary peer on a per application session basis. By default the preference is 50, and the selection on which peer is active and which one standby is shown in following CLI command:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.Geo.Red"
===============================================================================
Diameter Peer Policy : DSC.Geo.Red
===============================================================================
Last Mgmt Change      : 04/23/2014 15:18:24
-------------------------------------------------------------------------------
Diameter Base Values (config)
-------------------------------------------------------------------------------
Origin Host           : wlangw-2.DSC.Geo.Red.SRrealm
Origin Realm          : SRrealm
```

```
Connection Timer      : 30 (default)       Source Address     : 10.23.0.130
Transaction Timer     : 30 (default)       Router             : 10000
Watchdog Timer        : 30 (default)
Vendor Support        : 3GPP (default)
-------------------------------------------------------------------------------
Peer Name            Oper  PSM State     Susp  Cooldown  Pref  Order  Pri/Sec
-------------------------------------------------------------------------------
DSC.Simul            Yes   I-Open        No    -         10    1      Primary
DSC.26.206           Yes   I-Open        No    -         20    2      Secondary
===============================================================================
```

The configuration corresponding to the above show command is as follows.

```
*A:BNG-1# configure aaa diameter-peer-policy "DSC.Geo.Red"
*A:BNG-1>config>aaa>diam-peer-plcy# info
----------------------------------------------
            applications gx
            origin-host "wlangw-2.DSC.Geo.Red.SRrealm"
            origin-realm "SRrealm"
            router 10000
            source-address 10.23.0.130
            peer "DSC.Simul" create
                address 10.55.2.2
                destination-realm "simul.org"
                preference 10
                no shutdown
            exit
            peer "DSC.26.206" create
                address 10.40.11.2
                destination-realm "Tc3eRealm"
                preference 20
                no shutdown
            exit
----------------------------------------------
```

Which redundancy features are supported as well as redundancy behavior is Diameter application specific.

The transport configuration is part of the Diameter peer policy and is configured per peer. SR OS uses TCP as transport and the TCP destination port number is configurable. By default the standard port 3868 is used.

```
*A:BNG-1# configure aaa diameter-peer-policy "DSC.26.206" peer "DSC.26.206" transport
  - transport tcp port <port>
  - no transport

 <tcp>               : keyword
 <port>              : [1..65535]
```

The source port is randomly chosen from the ephemeral port-range.

Troubleshooting

Statistics of each peer can be displayed as follows:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.26.206" peer "DSC.26.206" statistics
===============================================================================
Diameter Peer Policy : DSC.26.206 (statistics)
===============================================================================
Diameter Peer             : DSC.26.206
time statistics cleared   : 04/18/2014 07:52:28
-------------------------------------------------------------------------------
Client initiated tx/rx                  Server initiated tx/rx
-------------------------------------------------------------------------------
TCP Send Failed           : 0           TCP Send Failed           : 0
Diam Rx Drop Count (Resps): 0           Diam Rx Drop Count (Reqs) : 0
Diam Tx Requests          : 3           Diam Rx Requests          : 94
Diam Rx Responses         : 3           Diam Tx Responses         : 94
Pending Messages          : 0
Request Timeouts          : 0
-------------------------------------------------------------------------------
Diameter message breakdown
-------------------------------------------------------------------------------
CCR initial Tx            : 1           CCA initial Rx            : 1
CCR update Tx             : 1           CCA update Rx             : 1
CCR terminate Tx          : 1           CCA terminate Rx          : 1
CER Tx                    : 0           CEA Rx                    : 0
DWR Tx                    : 0           DWA Rx                    : 0
DWR Rx                    : 94          DWA Tx                    : 94
ASR Rx                    : 0           ASA Tx                    : 0
RAR Rx                    : 0           RAA Tx                    : 0
DPR Tx                    : 0           DPA Rx                    : 0
DPR Rx                    : 0           DPA Tx                    : 0
===============================================================================
```

The above command shows several statistics including the number of transmitted and received messages per message type. There is a command to clear the above counters, for instance:

```
clear aaa diameter-peer-policy "DSC.26.206" peer "DSC.26.206" statistics
```

Furthermore, debug at peer level of all Diameter message types are available:

```
debug
    diameter
        detail-level high
        no dest-realm
        diameter-peer DSC.26.206 psm-events
        no diameter-policy
        message-type ccr cca cer cea dwr dwa dpr dpa rar raa asr asa
        no origin-realm
    exit
exit
```

The above debug example will display the detailed output of all Diameter messages sent to and received from peer **DSC.26.206**. A shorter command to obtain the same output is the **debug diameter message-type all** command. Some of the Diameter message types are application specific with certain overlap between the applications. In other words, not all Diameter message types are used by all applications. The message types are:

- ccr credit-control-request
- cca credit-control-answer
- cer capability-exchange-request
- cea capability-exchange-answer
- dwr watchdog-request
- dwa watchdog-answer
- dpr disconnect-peer-request
- dpa disconnect-peer-answer
- rar re-auth-request
- raa re-auth-answer
- asr abort-session-request
- asa abort-session-answer

Note that debug of a request message and the corresponding answer message requires enabling debug for 2 message–types. Common practice is to enable debug for all message types, or for all message types except for the watchdog messages because typically these messages do not contain much interesting information. Including the periodic DWR and DWA messages would make the debug output harder to read.

Every Diameter application supports at least the CER/CEA messages. An example output of CER/CEA messages is shown below. In the CER sent by SR OS, the attributes origin-host, origin-realm, host-ip-addr, and auth-appl-id are coming from the diameter policy configuration. Note that a CER has no destination-host. Other information in the CER is the product-name (set to **SR-OS**) and firmware-revision (set to **1203** in the example below indicating that this debug trace is taken from 12.0R3). The CEA is received from the PCRF, and contains similar information.

```
5 2014/06/26 14:27:32.79 CET MINOR: DEBUG #2001 vprn10000 DIAMETER
"DIAMETER: Message Transmission
CER from [DSC.26.206, DSC.26.206] to 10.40.11.2:3868
  Header
    ver 1  len 196  flags R-------  code 257
    app-id 0  hbh-id 8652  e2e-id 659536111
  AVPs
    origin-host (264) -M------ [24]
      data [16] (DiameterIdentity) : wlangw-2.SRrealm
    origin-realm (296) -M------ [15]
      data [7] (DiameterIdentity) : SRrealm
    host-ip-addr (257) -M------ [14]
      data [6] (Address) : ipv4 10.23.0.130
```

```
    vendor-id (266) -M------ [12]
      data [4] (Unsigned32) : 6527
    product-name (269) -------- [13]
      data [5] (UTF8String) : SR-OS
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777238 : Gx
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 6527
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 10415
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 13019
    vend-specific-appl-id (260) -M------ [32]
      data [24] (Grouped)
        vendor-id (266) -M------ [12]
          data [4] (Unsigned32) : 10415
        auth-appl-id (258) -M------ [12]
          data [4] (Unsigned32) : 16777238 : Gx
    firmware-revision (267) -------- [12]
      data [4] (Unsigned32) : 1203

  01 00 00 c4  80 00 01 01  00 00 00 00  00 00 21 cc
  27 4f b8 ef  00 00 01 08  40 00 00 18  77 6c 61 6e
  67 77 2d 32  2e 53 52 72  65 61 6c 6d  00 00 01 28
  40 00 00 0f  53 52 72 65  61 6c 6d 00  00 00 01 01
  40 00 00 0e  00 01 0a 17  00 82 00 00  00 00 01 0a
  40 00 00 0c  00 00 19 7f  00 00 01 0d  00 00 00 0d
  53 52 2d 4f  53 00 00 00  00 00 01 02  40 00 00 0c
  01 00 00 16  00 00 01 09  40 00 00 0c  00 00 19 7f
  00 00 01 09  40 00 00 0c  00 00 28 af  00 00 01 09
  40 00 00 0c  00 00 32 db  00 00 01 04  40 00 00 20
  00 00 01 0a  40 00 00 0c  00 00 28 af  00 00 01 02
  40 00 00 0c  01 00 00 16  00 00 01 0b  00 00 00 0c
  00 00 04 b3
"

6 2014/06/26 14:27:32.79 CET MINOR: DEBUG #2001 vprn10000 DIAMETER
"DIAMETER: Message Reception
CEA from 10.40.11.2:3868 to [DSC.26.206, DSC.26.206]
  Header
    ver 1  len 776  flags --------  code 257
    app-id 0  hbh-id 8652  e2e-id 659536111
  AVPs
    origin-host (264) -M------ [25]
      data [17] (DiameterIdentity) : stefaan.Tc3eRealm
    origin-realm (296) -M------ [17]
      data [9] (DiameterIdentity) : Tc3eRealm
    result-code (268) -M------ [12]
      data [4] (Unsigned32) : 2001 : DIAM_RESCODE_SUCCESS
    host-ip-addr (257) -M------ [14]
      data [6] (Address) : ipv4 10.40.11.2
    vendor-id (266) -M------ [12]
      data [4] (Unsigned32) : 637
    product-name (269) -------- [36]
      data [28] (UTF8String) : Alcatel-Lucent 5780 DSC (PS)
    origin-state-id (278) -M------ [12]
      data [4] (Unsigned32) : 1364308599
    firmware-revision (267) -------- [12]
      data [4] (Unsigned32) : 600450000
```

```
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777217 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777266 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 1 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777267 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777302 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777303 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777236 :
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 16777238 : Gx
    auth-appl-id (258) -M------ [12]
      data [4] (Unsigned32) : 111 :
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 28458
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 10415
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 12951
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 9
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 7898
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 5535
    supported-vendor-id (265) -M------ [12]
      data [4] (Unsigned32) : 637
    vend-specific-appl-id (260) -M------ [32]
      data [24] (Grouped)
        vendor-id (266) -M------ [12]
          data [4] (Unsigned32) : 10415
        auth-appl-id (258) -M------ [12]
          data [4] (Unsigned32) : 16777236 :
    vend-specific-appl-id (260) -M------ [32]
      data [24] (Grouped)
        vendor-id (266) -M------ [12]
          data [4] (Unsigned32) : 10415
        auth-appl-id (258) -M------ [12]
          data [4] (Unsigned32) : 16777267 :
    vend-specific-appl-id (260) -M------ [32]
      data [24] (Grouped)
        vendor-id (266) -M------ [12]
          data [4] (Unsigned32) : 10415
        auth-appl-id (258) -M------ [12]
          data [4] (Unsigned32) : 16777238 : Gx
    vend-specific-appl-id (260) -M------ [32]
      data [24] (Grouped)
        vendor-id (266) -M------ [12]
          data [4] (Unsigned32) : 9
        auth-appl-id (258) -M------ [12]
          data [4] (Unsigned32) : 16777238 : Gx
    vend-specific-appl-id (260) -M------ [32]
"
```

It is also possible to debug all messages from a specific Diameter policy, origin realm, or destination realm.

Note that these debug commands only show Diameter messages but no TCP messages like TCP-SYN. TCP layer issues must be debugged differently. For instance when there is a routing issue between client and server, then typically the state of the Diameter peer is **Wait-Conn-Ack**:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.26.206"
===============================================================================
Diameter Peer Policy : DSC.26.206
===============================================================================
Last Mgmt Change      : 06/16/2014 13:21:26
-------------------------------------------------------------------------------
Diameter Base Values (config)
-------------------------------------------------------------------------------
Origin Host           : wlangw-2.SRrealm
Origin Realm          : SRrealm
Connection Timer      : 30 (default)       Source Address     : 10.23.0.130
Transaction Timer     : 30 (default)       Router             : 10000
Watchdog Timer        : 10
Vendor Support        : 3GPP (default)
-------------------------------------------------------------------------------
Peer Name            Oper  PSM State     Susp  Cooldown  Pref  Order  Pri/Sec
-------------------------------------------------------------------------------
DSC.26.206           Yes   Wait-Conn-Ack No    Pending   50    -      -
===============================================================================
```

Wait-Conn-Ack means that the client has sent a TCP-SYN but no SYN-ACK is coming back. If the state is **Closed**, the client is no longer listening for a SYN-ACK and a new attempt to bring up the transport connection is made when the connection timer expires:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.26.206"
===============================================================================
Diameter Peer Policy : DSC.26.206
===============================================================================
Last Mgmt Change      : 06/16/2014 13:21:26
-------------------------------------------------------------------------------
Diameter Base Values (config)
-------------------------------------------------------------------------------
Origin Host           : wlangw-2.SRrealm
Origin Realm          : SRrealm
Connection Timer      : 30 (default)       Source Address     : 10.23.0.130
Transaction Timer     : 30 (default)       Router             : 10000
Watchdog Timer        : 10
Vendor Support        : 3GPP (default)
-------------------------------------------------------------------------------
Peer Name            Oper  PSM State     Susp  Cooldown  Pref  Order  Pri/Sec
-------------------------------------------------------------------------------
DSC.26.206           Yes   Closed        No    Pending   50    -      -
===============================================================================
```

The countdown of the connection timer can be seen with this command:

```
*A:BNG-1# show aaa diameter-peer-policy "DSC.26.206" peer "DSC.26.206"
===============================================================================
Diameter Peer Policy : DSC.26.206
===============================================================================
Diameter Peer          : DSC.26.206
Peer IP address        : 10.40.11.2
Last Mgmt Change       : 06/26/2014 14:27:31
-------------------------------------------------------------------------------
Peer Runtime Values (main)
-------------------------------------------------------------------------------
Peer Table Entry       : DSC.26.206::DSC.26.206
Peer Operational       : Yes              Watchdog Algorithm Active   : No
Peer State Machine     : Closed           Watchdog Answer Pending     : No
Connection Timer  (Tc) : 16               Connection Suspended        : No
Transaction Timer (Tt) : -                Cooldown Sequence Pending   : Yes
Watchdog Timer    (Tw) : -                Cooldown Sequence Active    : No
Primary/Secondary Peer : -                Cooldown Sequence Progress  : -
                                          Peer Removal Pending        : No
===============================================================================
```

In the above example, a new attempt to bring up the TCP session will be made in 16 seconds.

Events

Three events are defined for Diameter:

```
*A:BNG-1# show log event-control "diameter"
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 tmnxDiamPolicyPeerStateChange    MI  gen        8095           0
   2002 tmnxDiamAppMessageDropped        MI  gen           6           0
   2003 tmnxDiamAppSessionFailure        MI  gen           0           0
===============================================================================
```

Trap **tmnxDiamPolicyPeerStateChange** is generated for all changes in the state of the Diameter peer. The second trap, **tmnxDiamAppMessageDropped** is generated when the system drops a Diameter message because it is malformed. Failures in the Diameter application sessions are reported in the trap **tmnxDiamAppSessionFailure**. Note that each Diameter application can have its own specific behavior for each of these traps. These traps are generated when a log is created from security:

```
configure log log-id 88
       from security
       to …
```

Conclusion

Diameter is an alternative to RADIUS. Although it is mainly used by mobile operators, it is finding its way in fixed access networks. Diameter peering provides reliable and secure transport with peer redundancy. Its functionality is defined in a base Diameter protocol specified in RFC3588. Various applications can be layered on top of base Diameter and they can utilize the robust transport capabilities that Diameter provides.