Table of Contents

CDR Logging Configuration with Syslog Servers and Cisco IOS Gateways

Introduction

Customers may have a requirement to log Call Detail Records (CDRs) from Voice over IP (VoIP) systems for accounting or billing purposes. The recommended way to do this is with an external authentication, authorization, and accounting (AAA) server (RADIUS or TACACS). These AAA systems often provide CDR logging, post call record processing, and a billing report generation facility.

There may be some situations where the complexity or cost of the AAA server prohibits its use, but there is still a requirement for CDR logging. In such a case, it is possible to use the syslog capabilities of the Cisco gateway or router to log VoIP CDRs to an external syslog server. These records are in comma separated variable (CSV) format and therefore can easily be loaded and processed by an external software application such as a spreadsheet, or a database. The syslog server software can run on a basic PC. Basic syslog server applications can be downloaded from the Internet. Cisco makes no recommendations on any particular type or version of syslog server software.

Syslog uses User Datagram Protocol (UDP) as the underlying transport mechanism, so the data packets are unsequenced and unacknowledged. It is possible that on a heavy utilized network, some packets may be dropped and therefore CDR information will be lost. Multiple syslog servers can be specified for redundancy.

For the timestamp on the CDR to be correct, there is a requirement for the Cisco IOS® router or gateway to be configured for time synchronization via a Network Time Protocol (NTP) time source. If the router has no NTP synchronization, the start and stop times of each CDR will be a zero (null) value. If an external NTP source is not available, the router needs to be set as an NTP master. This is explained in the Configuration section below.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Configuration

Following is a sample configuration that enables the router to generate VoIP CDRs and send them to an external syslog server.

```
router#(config)service timestamps log datetime msec localtime

!−−− Ensure that the records are timestamped with an accurate value.

!
router#(config)aaa new−model
!
router#(config)aaa authentication login default none

!−−− Enable AAA, prevent Telnet authentication via AAA.

router#(config)aaa accounting connection h323 start−stop radius

!−−− Generates the H.323 call start/stop CDRs.

router#(config)gw−accounting syslog

!−−− Send the H.323 CDRs to the syslog server.

router#(config)logging 10.64.6.250

!−−− IP address of syslog server. Multiple syslog servers
!−−− can be specified for redundancy.
```

To ensure the H.323 start/stop records have the correct time value, NTP has to be running on the Cisco IOS router or gateway. Two methods of NTP are shown below:

- Use the following Cisco IOS software global configuration command to synchronize the Cisco IOS router or gateway to an external NTP server:

  ```
  router#(config)ntp server ip address
  ```

  ip address − IP address of the time server providing the clock synchronization.
- If there is no external NTP time source, use the internal clock as the time source. This is done with the Cisco IOS software global configuration command shown below:

  ```
  router#(config)ntp master
  ```

  To ensure that the timestamps are correct, the router clock should be set to the correct time (from normal EXEC mode) with the following command:

  ```
  router#clock set 15:15:00 8 May 2001
  ```

  Note: On some Cisco platforms, the router clock is not backed up with a battery source, so the system time will need to be reset after a router reload or power failure.

Sample CDR Output

Shown below is a portion of console output from the router. When the above configuration is enabled, the CDRs will be directed to the router console as well as the syslog server. To remove the logging from the router console, configure **no logging console** in global configuration mode on the router. This prevents the CDRs and other system messages from appearing on the console, but they are still logged to the syslog server.

When a VoIP call is made, it places a call in the forward direction to the destination. The destination makes a return call to get a full duplex VoIP connection to occur. Therefore, there is a CDR for the forward leg , and a second CDR for the return leg. The forward call leg has a *call origin* of 2 while the return call leg has a *call origin* of 1.

Note: Some output lines are broken into multiple lines for printing purposes.

```
router#

!--- The following output is for the forward call leg.

Jun 18 11:15:02.867: %VOIPAAA-5-VOIP_CALL_HISTORY: CallLegType 1, ConnectionId BA55719E
    F8C10015 0 1B1E08, SetupTime 11:14:39.367 UTC Mon
Jun 18 2001, PeerAddress 68575, PeerSubAddress , DisconnectCause 10  , DisconnectText
    normal call clearing., ConnectTime 11:14:49.707 UTC Mon
Jun 18 2001, DisconnectTime 11:15:02.867 UTC Mon Jun 18 2001, CallOrigin 2,
    ChargedUnits 0, InfoType 2, TransmitPackets 1509, TransmitBytes 102600,
    ReceivePackets 1510, ReceiveBytes 138920

router#

!--- The following output is for the reverse call leg.

Jun 18 11:15:02.983: %VOIPAAA-5-VOIP_CALL_HISTORY: CallLegType 1, ConnectionId BA55719E
    F8C10015 0 1B1E08, SetupTime 11:14:41.683 UTC Mon
Jun 18 2001, PeerAddress 2887, PeerSubAddress , DisconnectCause 10  , DisconnectText
    normal call clearing., ConnectTime 11:14:49.703 UTC Mon
Jun 18 2001, DisconnectTime 11:15:02.983 UTC Mon Jun 18 2001, CallOrigin 1,
    ChargedUnits 0, InfoType 2, TransmitPackets 1510, TransmitBytes 102692,
    ReceivePackets 1509, ReceiveBytes 138828
router#
```

This CDR shows the following:

Forward Call Leg	
Time CDR generated	: Jun 18 11:15:02.867
Unique connection ID	: BA55719E F8C10015 0 1B1E08
Setup Time	: 11:14:39.367 UTC Mon Jun 18 2001
PeerAddress (Calling number)	: 68575
Disconnect Cause Code	: 10
Disconnect Cause Text	: normal call clearing
Connect Time	: 11:14:49.707 UTC Mon Jun 18 2001

Call Origin	: 2
Disconnect Time	: 11:15:02.867 UTC Mon Jun 18 2001
Transmit Packets	: 1509
Transmit Bytes	: 102600
Receive Packets	: 1509
Receive Bytes	: 138828

Return Call Leg	
Time CDR generated	: Jun 18 11:15:02.983
Connection ID	: BA55719E F8C10015 0 1B1E08
Setup Time	: 11:14:41.683 UTC Mon Jun 18 2001
PeerAddress (Called number)	: 2887
Disconnect Cause Code	: 10
Disconnect Cause Text	: normal call clearing
Connect Time	: 11:14:49.703 UTC Mon Jun 18 2001
Call Origin	: 1
Disconnect Time	: 11:15:02.983 UTC Mon Jun 18 2001
Transmit Packets	: 1510
Transmit Bytes	: 102692
Receive Packets	: 1509
Receive Bytes	: 138828

The disconnect cause code values default to hexadecimal. The table shown below shows some common hexadecimal values and their explanations:

Hexadecimal Value	Explanation
0x1	Unassigned number
0x3	No route to destination
0x10	Normal call clearing
0x11	User busy
0x12	No user response
0x13	No user answer
0x15	Call rejected

0x1C	Invalid number
0x1F	Normal, unspecified
0x22	No circuit
0x2C	No requested circuit
0x2F	No resource
0x3F	Service or option not available, unspecified

Related Information

- **Troubleshoot and Debug VoIP Calls − the Basics**
- **Voice, Telephony and Messaging Technologies**
- **Voice, Telephony and Messaging Devices**
- **Voice, Telephony and Messaging Software**
- **Voice, Telephony and Messaging TAC eLearning Solutions**
- **Recommended Reading: Troubleshooting Cisco IP Telephony , Cisco Press, ISBN 1587050757**
- **Technical Assistance Center**