CHAPTER 11

Troubleshooting Cisco Emergency Responder

These topics address problems you might encounter with Cisco Emergency Responder (Emergency Responder), and provide ways to resolve them; also included are other tasks associated with problem identification and resolution.

Troubleshooting Phone-Related Problems

These topics help you troubleshoot problems related to assigning phones to ERLs and managing the phones:

Undiscovered Phones

If Cisco Emergency Responder (Emergency Responder) is not discovering the phones homing to Cisco Unified Communications Manager (Cisco Unified CM), check that all Cisco Unified CMs are SNMP-reachable and that the SNMP settings are correct. Emergency Responder logs an event if Cisco Unified CM is SNMP-unreachable.

To verify the Cisco Unified CM SNMP settings, follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Administration CLI and use the following command to ping the Cisco Unified CM server:

```
utils network ping <ipaddress of CUCM>
```

Step 2 If you successfully ping the Cisco Unified CM, verify that the SNMP settings are correct on Cisco Unified CM, as follows:

- If you are using a Linux-based version of Cisco Unified CM (version 6.0 or higher), log in to the Cisco Unified CM Serviceability web interface and use the SNMP web pages to check the SNMP community string settings.
- If you are using a Windows-based version of Cisco Unified CM, open the services on Cisco Unified CM and choose:

  Start > Settings > Control Panel > Administrative Tools > Services Properties > SNMP > Properties > Security Tab

Step 3 Check to see if Cisco Unified CM is SNMP reachable by running the following CLI command on the Emergency Responder server:

```
utils snmp get <ccm ip-address/host name> <snmp-read-community-string> 1.3.6.1.2.1.1.2.0
```

If the Cisco Unified CM is SNMP reachable, then the output of the preceding command should be similar to the following:

```
Variable = 1.3.6.1.2.1.1.2.0
value    = OBJECT IDENTIFIER <sys-oid-of-ccm>
```

Too Many Unlocated Phones

Emergency Responder obtains a list of registered phones from Cisco Unified CM and tries to locate all phones. If Emergency Responder cannot locate a phone behind a switch port or in any configured IP subnets, and the phone is not a configured synthetic phone, the phone is placed in the list of unlocated phones.

If there are a lot of unlocated phones, first try running the switch port and phone update process to see if Emergency Responder can resolve some of the problems automatically. See the "Manually Running the Switch-Port and Phone Update Process" section on page 4-50 for more information.

These are some things that can prevent Emergency Responder from locating a phone:

- If more than one switch port reports the phone as a CDP (Cisco Discovery Protocol) neighbor, then the phone is placed in unlocated phones. This condition is corrected in the next phone tracking when only one switch port reports this phone as its CDP neighbor.

- The phone is attached to a switch that is not defined in Emergency Responder. See the "Identifying the LAN Switches" section on page 4-46 for information about defining switches.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch. See the "Network Hardware and Software Requirements" section on page 1-4 for a list of supported switches. See the "Manually Defining a Phone" section on page 4-62 for information about configuring these types of phones if you cannot connect them to a supported device.
- The phone is connected to a hub, which is connected to a supported switch port, but it does not support CDP. Emergency Responder can consistently discover CDP-enabled phones attached to hubs (which are attached to supported switch ports), but cannot always track non-CDP phones attached in this manner. For non-CDP phones, ensure the phones are attached directly to supported switch ports.
- The switch to which the phone is connected is currently unreachable, for example, it does not respond to SNMP queries. This could be for several reasons:
  - The SNMP read community string on the switch does not match the string configured in Emergency Responder. Correct the Emergency Responder configuration. See the "Configuring the SNMP Connection" section on page 4-44.
  - The phone requires CAM table access, but CAM tracking is not enabled for the switch in Emergency Responder. See the "Identifying the LAN Switches" section on page 4-46.
  - There is a network outage preventing communication between the Emergency Responder server and the switch. Locate and resolve the network outage problem.

  Unreachable switches are not retried until Emergency Responder runs the next full switch-port and phone update process, unless you run it against the individual switch.
- The phone has moved to a switch served by a different Emergency Responder group. If this is the case, the Emergency Responder group name is shown for the phone in the unlocated phones list. If the phone is not locatable in the next incremental phone tracking process after it is moved, the phone remains unlocated in any Emergency Responder group until a full switch-port and phone update process is run.
- The phone requires CAM-based tracking, but CAM-based tracking is not enabled on the switch to which the phone is connected. Cisco IP SoftPhone and some other phone models require CAM-based tracking. See the "Identifying the LAN Switches" section on page 4-46 for information about enabling CAM-based tracking, and "Network Hardware and Software Requirements" section on page 1-4 for a list of phones that require CAM-based tracking.

After fixing the problems that are preventing Emergency Responder from locating phones, run the switch-port and phone update process on the affected switches, or on all switches:

- To run the process on a specific switch—Select **Phone Tracking>LAN Switch Details** and select the switch in the left-hand column; then click **Locate Switch Ports**.
- To run the process on all switches—Select **Phone Tracking>Run Switch-Port & Phone Update**.

Related Topics

- Identifying Unlocated Phones, page 4-60
- IP Subnet Phones, page A-52
- Cisco Unified OS CLI Commands, page F-4

Phone Sometimes Disappears in Cisco Emergency Responder

If Emergency Responder is in the middle of a phone tracking process, and a phone is in the middle of homing to a different Cisco Unified CM cluster, no Cisco Unified CM cluster has a record of the phone. Thus, Emergency Responder does not know the phone exists, and you can not look up the phone in the Emergency Responder interface. However, assuming the phone successfully connects to a Cisco Unified CM cluster, Emergency Responder tracks the phone during the next incremental phone tracking process, and the phone should then appear in the Emergency Responder interface.

This problem can also occur if phones are reconnecting to a primary Cisco Unified CM server from a backup server during the Emergency Responder phone tracking process.

Wrong ERL is Used for a Shared Line

When two or more phones with a shared line appearance move from switches that are monitored by one Emergency Responder group to switches that are monitored by a different Emergency Responder group, then Emergency Responder may assign an incorrect ERL to these phones during an emergency call. This can occur when the phones move to a different campus that has a different Cisco Unified CM cluster (although the moved phones are still registered with the original Cisco Unified CM cluster), and it can also occur when the phones move within a single large campus that is served by multiple Cisco Unified CM clusters.

Because the moved phones are still registered to their original Cisco Unified CM cluster, emergency calls from these phones are routed to the original Emergency Responder group. In this case, the Emergency Responder group detects that the calling phone is connected to a switch that is monitored by a different Emergency Responder group, and the call is forwarded to the appropriate Emergency Responder group through an H.323 inter-cluster trunk. Because the inter-cluster trunk does not pass the MAC address of the calling phone, the receiving Emergency Responder group does not know the MAC address of the calling phone and must associate the phone to an ERL based on the calling party number.

In cases with a single phone connected to the switches monitored by the receiving Emergency Responder group, this is not a problem. However, when multiple phones with a shared line appearance connect to switches monitored by the receiving Emergency Responder group, then Emergency Responder must guess which phone has placed the emergency call. If all of the phones with a shared line appearance are in the same ERL, the guess is correct. If the phones span multiple ERLs, then the guess might be incorrect.

Related Topics

- Deploying Cisco Emergency Responder In Two Main Sites, page 1-28
- Creating Route Patterns for Inter-Cisco Emergency Responder Group Communications, page 3-18

802.11b Endpoints Using Wrong ERL

802.11b endpoints (such as Cisco Wireless IP 7920 Phones and Cisco IP SoftPhones running on 802.11b) are using switch port-based ERL instead of the configured subnet-based ERL.

Cisco Emergency Responder (Emergency Responder) give a higher priority to switch port association for call routing. If Emergency Responder finds a switch port mapping for any endpoint (including 802.11b endpoints), it uses the switch port mapping to route emergency calls. If the switch port mapping is not found or if the ERL is not configured for the corresponding switch port, Emergency Responder 1.2 routes emergency calls using subnet-ERL configuration.

Be aware that Emergency Responder 8.6 locates 802.11b endpoints behind a switch port under the following conditions:

- CDP (Cisco Discovery Protocol) is disabled on the access point or the switch port on which it is connected; and
- CAM tracking is enabled in Emergency Responder for that particular switch.

See the switch port screen or the ERL debug tool (see Using The ERL Debug Tool to Verify Cisco Emergency Responder Configuration, page 11-18) to check if the 802.11b endpoint is associated with a switch port.

It is recommended that you track 802.11b endpoints using subnet-based ERLs. Therefore, enable CDP on the switch port and the access points to route emergency calls from 802.11b endpoints using subnet-based ERLS.

Related Topics

- Configuring IP Subnet-based ERLs, page 4-37

Troubleshooting Emergency Call Problems

These topics help you troubleshoot problems related to the routing of emergency calls and the information supplied with the calls:

Emergency Calls are Not Being Intercepted by Cisco Emergency Responder

If Emergency Responder is not intercepting emergency calls, there is probably a mistake in your Cisco Unified CM configuration or its representation in the Emergency Responder configuration.

- The emergency call number (911) is in the Phones partition and uses the E911CSS calling search space. Ensure this number was identified during Emergency Responder installation (see the "Installing Cisco Emergency Responder 8.6 on a New System" section on page 2-14). This ensures that users can dial the emergency number. See Creating the Emergency Call Route Points, page 3-6 for information about setting up the Cisco Unified CM configuration for this number.
- The standby Emergency Responder server route point (912) is in the E911 partition and uses the E911CSS calling search space. See Creating the Emergency Call Route Points, page 3-6 for information about setting up the Cisco Unified CM configuration for this number. Ensure this

number is defined as the standby server route point in the Emergency Responder configuration (see the "Configuring Group Telephony Settings For the Cisco Emergency Responder Server" section on page 4-22).

- The PSAP callback route point pattern (913XXXXXXXXXX) is in the E911 partition and uses the E911CSS calling search space. See Creating the Emergency Call Route Points, page 3-6 for information about setting up the Cisco Unified CM configuration for this number. Ensure this number is defined as the PSAP callback route point pattern in the Emergency Responder configuration, and that the strip prefix (913) is also identified (see the "Configuring Group Telephony Settings For the Cisco Emergency Responder Server" section on page 4-22).
- All ELIN route patterns are in the E911 partition. See the "Creating the Route Patterns for ERLs" section on page 3-11 for information about setting up the Cisco Unified CM configuration for these numbers.
- All phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces in the same manner as these partitions in the examples described in the "Setting Up Cisco Emergency Responder to Handle Emergency Calls" section on page 4-4.
- All gateways to the service provider's network use the E911CSS calling search space. See Configuring the Calling Search Space for the Gateways Used to Connect to the PSAP, page 3-18 for more information.
- The Cisco Unified CM Version (JTAPI jar) being configured is proper. To check the Cisco Unified CM version, follow these steps:
  1. Login to the Emergency Responder Admin Utility website.
  2. Select **Update>CCM Version**
  3. In the **Status** section, check the **Current Version of CCM**.

ELIN not Transmitted to the PSAP

If the ELIN is not transmitted to the PSAP, and you are using a PRI connection to route emergency calls to the PSAP, check the configuration of the gateway. The PRI must be configured to send the real calling party number (the ELIN) rather than a static number, such as the main site number. See the "Obtain CAMA or PRI Trunks to the PSTN" section on page 1-18.

ELIN For Default ERL Used For Calls From Other ERLs

If an emergency call is assigned an ELIN defined for the Default ERL rather than an ELIN assigned to the ERL whence the call was made:

- Check the Cisco Unified CM configuration for the route pattern for the ELIN you expected to be used. See the Creating the Route Patterns for ERLs, page 3-11.
- Check the ERL definition in Emergency Responder to ensure that the ELIN is correctly configured for the ERL. See the "Setting Up an Individual ERL and Its Automatic Location Information (ALI)" section on page 4-34.

If the route pattern for an ERL fails, Emergency Responder uses the route pattern defined for the Default ERL.

Emergency Calls Not Routed to the Correct PSAP

If an emergency call is not routed to any PSAP, check whether the route patterns used for the ERL from which the call was made and for the default ERL are configured and use the correct partitions and calling search spaces (see the "Creating the Route Patterns for ERLs" section on page 3-11). Ensure that the partitions and calling search spaces for the gateways are correct (see Configuring the Calling Search Space for the Gateways Used to Connect to the PSAP, page 3-18).

If an emergency call successfully leaves your network but does not get routed to the correct PSAP, look at these possible points of failure:

- Is Emergency Responder configured to assign the correct ELIN to the ERL assigned to the phone? Emergency calls are routed based on the ELIN, so if you assign the wrong ELIN, the call is not routed correctly. See the "Creating ERLs" section on page 4-32.
- If the ELIN is correct, is the ELIN route pattern configured to use the correct gateway? If you select the wrong gateway, the call might be routed to a part of the service provider's network that cannot connect to the desired PSAP. Consult with your service provider to determine gateway requirements.

  See these topics:

  - •Creating ERLs, page 4-32, page 3-9
  - Deploying Cisco Emergency Responder in One Main Site with Two or More PSAPs, page 1-23
- Does the service provider's ALI database contain the correct information for the ELIN? Emergency call routing outside your network is based on the information in the service provider's database, not on the information in your local network. See the "Exporting ERL Information" section on page 4-40.
- Does the emergency caller's phone register with a Cisco Unified CM cluster supported by a different Emergency Responder group than the Emergency Responder group that supports the originating switch port? Then you might have a miss-configured Emergency Responder cluster. See these topics:

  - Installing Cisco Emergency Responder 8.6 on a New System, page 2-14
  - Creating Route Patterns for Inter-Cisco Emergency Responder Group Communications, page 3-18
  - Configuring Group Telephony Settings For the Cisco Emergency Responder Server, page 4-22

Note If the call reaches the PSAP, but the PSAP cannot talk to the caller, ensure that the Cisco Unified CM for the remote Emergency Responder group has the Cisco Unified CM for the local Emergency Responder group defined as a gateway.

Emergency Callers Sometimes Get Busy Signal and Emergency Calls Are Sometimes Not Routed

If callers hear a busy signal when calling the emergency call number, or if emergency calls sometimes do not get routed, there is probably a problem with the configuration of your standby Emergency Responder server:

- If you have only configured a primary Emergency Responder server, install and configure a standby Emergency Responder server. If CPU utilization on the primary server reaches 100%, Emergency Responder cannot handle emergency calls. In this case, the standby server handles the calls.

- Check the route point configuration for the standby server. Ensure the emergency call route point's call forward settings are configured to forward calls to this number. See Creating the Emergency Call Route Points, page 3-6 for information about the Cisco Unified CM configuration, and the "Configuring Group Telephony Settings For the Cisco Emergency Responder Server" section on page 4-22 for the Emergency Responder configuration.

PSAP Call Back Errors

You might encounter these problems if a PSAP operator tries to call back an emergency caller using the ELIN provided by caller ID:

Symptom PSAP could not reach the original emergency call extension.

Recommended Action Emergency Responder caches a mapping between the caller's true extension and the ELIN you define for an ERL. If more calls get made than the number of ELINs you define for an ERL, Emergency Responder must reuse these numbers and thus overwrites the original caller's extension. You can view the call history to determine the extension of the original caller. See the "What Happens When an Emergency Call Is Made" section on page 1-9.

If this is not the problem, check the configuration of the PSAP callback route point in Cisco Unified CM and Emergency Responder (see Creating the Emergency Call Route Points, page 3-6 and the "Configuring Group Telephony Settings For the Cisco Emergency Responder Server" section on page 4-22), and the ELIN translation patterns in Cisco Unified CM (see the "Creating the Translation Patterns for ELINs" section on page 3-13).

Symptom Onsite alert (security) personnel get callbacks from the PSAP.

Recommended Action Emergency Responder routes PSAP callbacks to the onsite alert personnel for the default ERL if ELIN-to-extension mapping for the emergency call has expired from the cache. By default, this is three hours, although you can configure expiration to be a longer or shorter time. See the "Cisco Emergency Responder Group Settings" section on page A-3.

Onsite Alert Personnel Are Not Getting Telephone Alerts

If the onsite alert personnel are not getting telephone alerts when an emergency call is made in an ERL they are covering, ensure that all phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces in the same manner as these partitions in the examples described in the "Setting Up Cisco Emergency Responder to Handle Emergency Calls" section on page 4-4.

Also, ensure that the Emergency Responder configuration for the Cisco Unified CM clusters is correct. The Emergency Responder configuration should show the correct begin address for the telephony ports you defined as CTI ports in Cisco Unified CM, and the number of telephony ports should be the correct number and it must be greater than 0 for any calls to occur. Emergency Responder uses this CTI ports to place the telephone calls to onsite alert personnel.

If the Event Viewer in the Emergency Responder Serviceability web interface displays the error message "No port to place call," then there were not enough CTI ports defined to initiate all the calls to onsite alert personnel. Therefore, you must define additional ports. To access the Event Viewer, log in to the Emergency Responder Serviceability web interface and select **Tools>Event Viewer**.

Onsite Alert Phone Does Not Ring When Emergency Call is Placed

You might encounter this problem if the onsite alert phone does not ring when an emergency call is placed:

Symptom The onsite alert phone does not ring when an emergency call is placed.

Possible Cause The onsite alert phone does not ring if the Do Not Disturb (DND) feature is enabled on the phone and if Emergency Responder is configured with Cisco Unified CM 6.x.

Recommended Action Do not enable DND on an onsite alert phone.

Prompts for Phone Alerts Not Getting Played

You might encounter this problem if prompts for phone alerts are not getting played:

Symptom Prompts do not get played at the onsite alert phone when the call is initiated from the CTI ports.

Explanation This problem can occur when a single CTI port is configured with multiple lines. Prompts may not get played from one or more of these lines when the onsite alert notifications call is initiated through them.

Recommended Action To avoid this problem, configure only one line per CTI port in the Cisco Unified CM that is configured for Emergency Responder.

Onsite Alert Personnel Not Getting Email (or Paging) Notifications

If the onsite alert personnel are not getting email, or email-based pages, even though you configure email addresses for them (see the "Onsite Alert Settings" section on page A-13), check the Emergency Responder configurations SMTP settings. Ensure that the SMTP server address and source mail ID are correct (see the "Cisco Emergency Responder Group Settings" section on page A-3), and that there is an account for the mail ID in the SMTP server.

Incorrect Location Information Sent To Onsite Alert Personnel

If your onsite alert (security) personnel are receiving incorrect location information for an emergency call, consider these potential problems:

- Is the ALI data for the ERL correct? See the "Creating ERLs" section on page 4-32.
- Is the phone location data for the switch port correct? See the "Configuring Switch Ports" section on page 4-52.

- Is the correct ERL assigned to the switch port to which the phone is connected? If not, there could be two problems:
  - Someone switched wires on the switch, so your formerly correct configuration is no longer correct. Wires cannot be moved from port to port without potentially invalidating the ERL assignment. See the "Data Integrity and Reliability Considerations" section on page 1-16.
  - The wiring closet is secure, the ERL assignment is simply incorrect. See the "Configuring Switch Ports" section on page 4-52.
- Did the call come from the Default ERL (assuming you do not use the Default ERL for any permanent ERL)? This could indicate these problems:
  - The phone is connected to an unsupported port and is not defined as a manual phone. See the "Manually Defining a Phone" section on page 4-62.
  - The phone is not supported and it is not defined as a manual phone. See the "Manually Defining a Phone" section on page 4-62.
  - The phone is supported but Emergency Responder could not locate it. You might have to manually assign the phone to an ERL if you cannot resolve the problem. See the "Too Many Unlocated Phones" section on page 11-2.
- Did the call come from a manually-defined phone extension? If so, it is likely the incorrect ERL is assigned, perhaps because the phone moved. See the "Manually Defining a Phone" section on page 4-62.

Emergency Call History Problems

These are some issues you might encounter when viewing the emergency call history information (see the "Viewing the Emergency Call History" section on page 4-65):

Symptom Emergency call information does not show up in call history right away.

Recommended Action Emergency Responder writes call history information to the database every 15 seconds. You should be able to view history information after 15 seconds.

Symptom The call history does not show the ELIN and route pattern used for a call.

Recommended Action If the call could not be routed to the PSAP, you will not see an ELIN or route pattern. Check to determine why the call could not be routed. See the "Emergency Calls Not Routed to the Correct PSAP" section on page 11-7.

Troubleshooting Email Alerts

These topics help you troubleshoot problems related to the email alerts that Emergency Responder generates:

Emergency Call Alert

Whenever a user makes a 911(Emergency) call, Emergency Responder generates an email alert. Emergency Responder sends the email alert to all of the onsite alert (security) personnel whose email ids are configured for the ERL from which the call was made. (See the "Configuring a Cisco Emergency Responder Server Group" section on page 4-21.)

Security personnel are expected to respond to that user. For detailed call information, see the following URL:

http://<<*CERServer HostName*>>/ceruserreports

When a 911 call is made and the backup Emergency Responder server handles the call, an alert similar to the following is sent:

```
Subject: Emergency Call Alert -- Extn # 332101 (Generated by Backup Cisco ER)
Message: EMERGENCY CALL DETAILS (Generated by Emergency Responder)
Caller Extension:332101
Zone/ERL         :Z1
Location         :ddd
Call Time        :June 2, 2003 3:47:30 PM IST
```

Transition Alert

When the standby Emergency Responder server takes control and becomes the active server, a Transition Alert is sent to the Emergency Responder administrator. This situation occurs under any of the following circumstances:

- If the primary Emergency Responder server is stopped.
- If the Emergency Responder service is stopped on that server.
- If the connectivity between primary and standby Emergency Responder servers is broken.

The administrator should diagnose the cause and fix the problem as soon as possible.

When the Emergency Responder backup server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Backup is active
Message:
Backup Cisco ER <<CER HostName>> has taken control as Active Cisco ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

When the master Emergency Responder server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Master is active
Message:
Master Cisco ER <<Emergency Responder Server HostName>> has taken control as Active Cisco
ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

Tracking Failure

At the end of a switch-port and phone tracking process, if there are any devices that could not be tracked, Emergency Responder sends a Tracking Failure email to the Emergency Responder administrator.

The administrator should look at the event log on the Emergency Responder server to find the list of devices that were not tracked. Then the administrator should check the following and make any required corrections:

1. Make sure that the correct SNMP Community String is configured in Emergency Responder.
2. Check that the device is connected.
3. Check that the host name for the Emergency Responder server is resolvable, that is, it can be found.
4. Check that the SNMP service is enabled on that particular device (Switch / Cisco Unified CM).

Here is an example of a tracking failure alert.

```
Subject: CER Phone Tracking failed to track some devices
Message:
CER Phone Tracking could not get information [using SNMP] from 2 Cisco Cisco Unified CM(s)
and 1 Switch(es)
Check Event Viewer on CER Server for details.
```

Failed To Get Provider

Emergency Responder sends a Failed to Get Provider Alert to the Emergency Responder administrator if Emergency Responder is not able register to one of the configured Cisco Unified CM clusters. Emergency Responder continues trying the registration until it succeeds. Emergency Responder sends the Failed to Get Provider email after a few retries.

The message provides information about how to clear the problem, as shown in the following example.

```
Subject: Failed to get JTAPI Provider for Cisco Unified CM <<CCM IP/Host Name>> (Generated
by Backup Cisco ER)
Message:
Please check the following:
1) Check if the Cisco Unified CM is connected to the CER server.
2) Check if the configured Call Manager is running a version supported by the CER server.
3) Check if the given login credentials are correct:
    CTI Manager Host Name:<<CCM IP/HostName>>
```

Failed to Establish Communication with Cisco Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server fails to establish communication with the Phone Tracking Engine for some time. This can occur if the Emergency Responder Phone Tracking Engine service is down. The administrator should perform the following steps:

1. If the Emergency Responder Phone Tracking Engine service is down, start the service.
2. Make sure that the Host Name of the Emergency Responder server does not contain any underscore (_) characters.

Here is an example of a tracking failure alert.

```
Subject: CER Server failed to establish communication with CER Phone Tracking Engine.
Message:
```

```
CER Server could not communicate with CER Phone Tracking Engine.
```

Lost Communication with Cisco Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server loses communication with the Emergency Responder Phone Tracking Engine. This is most liked to occur if the Emergency Responder Phone Tracking Engine service goes down when the Emergency Responder server is running.

The administrator should restart the Emergency Responder Phone Tracking Engine service.

The following shows an example of a tracking failure alert.

```
Subject: CER Server lost communication with CER Phone Tracking Engine
Message:
CER Server could not communicate with CER Phone Tracking Engine.
```

Failed to Send Unlocated Phone Details to Remote Cisco Emergency Responder Server Group

If Emergency Responder fails to send unlocated entries to a server group because it is already in the process of sending entries to that server group, this alert is sent.

This alert occurs very rarely. It can occur when a Emergency Responder server is found in more than one Emergency Responder server group. To resolve this problem, check to see which server group is an old configuration and remove that server group.

```
Subject: CER Server failed to send Unlocated Phones details to Remote CER Server Group.
Message:
CER Server failed to send Unlocated Phones to Remote CER Server Group. Please ensure that
the CER servers are not found under more than one CER Server Group.
CER Servers in Remote Server Group:<< CERServer HostNames >>
```

Emergency Call Could Not be Routed

If the emergency call routing to some route patterns configured in the ERL fails, Emergency Responder sends an email to the system administrator.

Subject: Emergency call could not be routed using some route patterns (CERServer:<*server hostname*>)

Message Body: Emergency call from: <Caller Extn> could not be routed using some Route Patterns. Check Event Log.

The Event Log displays the following message:

```
Emergency call from <extn> could not be routed using the following route patterns

<RoutePattern1>
<RoutePattern2>
*****************
Call Routed to <RoutePattern-X>

Please check the availability of the above routes. Also, check for the following error
conditions:

1. If FAC and/or CMC are configured on the route patterns used for Cisco ER, please
disable them.
```

```
2. If the "Calling Party Number Modification" flag on the CER user page in the Cisco
Unified CM is not enabled, please enable it.
```

Solution

1. If you are running Cisco Unified CM 4.2 or 4.3, check to make sure that the Calling Party Number checkbox on the Emergency Responder User page is checked.
2. If you are running Cisco Unified CM 5.x or Cisco Unified CM 6.x, check to make sure that the routes are available.
3. Add the Emergency Responder Application User to the "Standard CTI Allow Calling Number Modification" user group.

Calling Party Modification Failed

If the calling party modification was not successful, Emergency Responder sends the following email to the system administrator:

Subject: Emergency Calling Party Modification Failed (Emergency ResponderServer: <*server*>)

Message Body: Emergency call from: <Caller Extn> cannot be routed with calling party modification. Check Event Log.

The Event Log displays the following message:

```
Emergency Call from <Caller Extn> has been routed to default ERL because the calling party
modification failed.
Please make sure that the checkbox "Enable Calling Party Number Modification: is checked
on the Cisco Unified CM user page for the CER user. PSAP callbacks MAY NOT work correctly.
The CER service will need to be restarted once the flag is checked on the Cisco Unified CM
User page.
```

Solution Check the box for the "Enable Calling Party Number Modification" in the Emergency Responder user page in Cisco Unified CM 4.2 or 4.3 Administration. After you enable this flag, restart the Emergency Responder service for the changes to take effect.

Troubleshooting Web Alerts

You might encounter this problem when receiving web alerts:

Symptom Web alert continues to refresh every 30 seconds. You can see this problem by checking the status in the browser. The status displays the seconds remaining before refresh if it is in this mode.

Recommended Action Check if there are other web alert screens open on the same client machine. Only one browser from a client machine can operate in the real-time mode. Remove any extra browsers.

Troubleshooting Cisco Emergency Responder System and Administration Problems

These topics help you troubleshoot problems related to the Emergency Responder system and its administration, such as server and web server problems:

Cannot Validate Publisher

If the installation cannot validate the Publisher (Step 5 of the "Installing the Cisco Emergency Responder Subscriber" section on page 2-18), check the following:

1. Verify that the Publisher hostname is correct and that the Publisher is reachable by hostname.
2. Verify that the Publisher and Subscriber servers are running the same version of Emergency Responder.
3. Verify that the database password that you entered is correct. This password was specified on the Database Access Security Configuration page during installation.
4. Make sure that the Subscriber has been configured correctly on the Publisher.

Troubleshooting Login Problems

These are some issues you might encounter while logging into Emergency Responder:

Symptom You cannot log in to the Emergency Responder Administration website.

Recommended Action Log in to CLI and run the **utils service list** command. Check if the status "Cisco IDS" is STARTED. If not, start the service using the **utils service start** *service name* command.

Symptom You cannot open multiple Emergency Responder sessions using Netscape Navigator.

Recommended Action Netscape/Mozilla Navigator uses the same session ID across multiple windows. This creates problems if you try to log into Emergency Responder using different IDs. Normally, you can open multiple windows when logged in as system administrator. With Internet Explorer, if you open separate IE session by starting a new IE instance (rather than by opening a new window from an existing session), IE uses different session IDs, and you should be able to log in using separate IDs (for example, as a user and an administrator, or as LAN switch and ERL administrators).

Related Topics

- Using The ERL Debug Tool to Verify Cisco Emergency Responder Configuration, page 11-18

Using Cisco Unified Operations Manager

Use Cisco Unified Operations Manager 2.01 to continuously monitor the health of the Emergency Responder system.

For information about setting up Emergency Responder to use Cisco Unified Operations Manager, see the "Configuring Test ERLs" section on page 4-39.

For information about installing and using Cisco Unified Operations Manager, see the documentation at:

http://www.cisco.com/en/US/products/sw/cscowork/index.html

Troubleshooting Cisco Emergency Responder Switch and Port Configuration Problems

You might encounter the following issues while configuring switches or switch ports in Emergency Responder:

Symptom Emergency Responder is configured with Cisco Unified CM information, but no phones get discovered.

Recommended Action Ensure that the Cisco Unified CM servers are reachable on the network. Then, ensure that the SNMP read community strings are configured correctly for the switches and Cisco Unified CM servers (see the "Configuring the SNMP Connection" section on page 4-44.) Then, manually run the switch port and phone update process (see the "Manually Running the Switch-Port and Phone Update Process" section on page 4-50.) Use the CLI-based **utils snmp command** to determine if the Cisco Unified CM is SNMP reachable.

Symptom Emergency Responder does not show the ports on a switch configured in Emergency Responder.

Recommended Action If you add a supported switch to Emergency Responder and run phone tracking on the switch after adding it, you should be able to view the list of Ethernet ports on the switch. If Emergency Responder does not list the ports, check the SNMP settings in Emergency Responder for the switch (see the "Configuring the SNMP Connection" section on page 4-44.) Also, verify that the

switch is reachable over the network. Retry the selective phone tracking process on the switch (click **Locate Switch Ports** when viewing the switch details; see the "LAN Switch Details" section on page A-43.)

If the problem persists, ensure that the switch is supported (see the "Network Hardware and Software Requirements" section on page 1-4.) Also, check the Event Viewer for error messages.

Symptom Some phones do not appear in the switch port list.

Recommended Action Check if the phone is found under configured IP subnets or in synthetic phones. If it is not found in either of those places, then they are placed as unlocated phones. See the "Too Many Unlocated Phones" section on page 11-2 for a list of reasons that a phone could not be located.

Symptom Cannot delete a switch from the Emergency Responder configuration.

Recommended Action You cannot delete a switch when a phone tracking process is in progress. Retry the deletion after the process has ended. If this is not the problem, the Emergency Responder server might not be running. Check the control center and restart the server (see the "Starting and Stopping a Cisco Emergency Responder Server" section on page 11-24.)

Symptom Import or export of the switch port details fails.

Recommended Action If a switch port import or export attempt fails, it might be due to these reasons: the first switch-port and phone update process has not yet ended (wait for it to finish); the Emergency Responder server is not running (use the control center to restart it, see the "Starting and Stopping a Cisco Emergency Responder Server" section on page 11-24); the Emergency Responder server is not completely initialized (wait for it to initialize).

Symptom The import of some switch port configurations fail.

Recommended Action To import switch port configurations, Emergency Responder must already be configured with the switch and Emergency Responder must first discover the ports on the switch using the switch-port and phone update process. If you try to import a configuration for ports not yet discovered in Emergency Responder, the importation of those settings fails. See the "Manually Running the Switch-Port and Phone Update Process" section on page 4-50 for information about the process. Run it on the switches whose port configurations you could not import, then retry the import.

Symptom Phones moved from other Emergency Responder groups to this Emergency Responder group, and then moved back, are still showing up in the switch port details for the Emergency Responder group.

Recommended Action This types of phones are not removed from the switch port details until the next full switch-port and phone update process is run. If this is an issue for you, you can run the process on the switch (or on all switches) manually. See the "Manually Running the Switch-Port and Phone Update Process" section on page 4-50.

Using The ERL Debug Tool to Verify Cisco Emergency Responder Configuration

The ERL Debug Tool takes a phone extension as the search criteria and displays the ERLs currently being used for routing emergency calls for the phones.

Use this diagnostic tool to verify the Emergency Responder configuration during the ERL creation and the ERL assignment phase, and to troubleshoot calls directed to incorrect ERLs.

For example, you configured the phone in ERL_1 as a manually configured phone, however a misconfigured IP subnet matches this phone's IP address, and associates it with ERL_2. Now that you have found the configuration problem using the Debug Tool, you can correct it.

To use the ERL Debug Tool, follow these steps.

Procedure

Step 1 Select **Tools > ERL Debug Tool**.

Emergency Responder displays the ERL Debug Tool page.

Step 2 At the Find Phones field, to list specific phones, select the search criteria and click **Find.**

Emergency Responder displays the ERL currently being used for routing emergency calls for the phone.

Step 3 If the configurations are not correct, make the required changes.

Note Emergency Responder displays a maximum of 1,000 records.

Replacing the Publisher Server and Subscriber Servers

If you must replace a faulty Publisher server or a faulty Subscriber server, perform the appropriate procedure:

- Replacing a Faulty Subscriber, page 11-18
- Replacing a Faulty Publisher, page 11-19

Replacing a Faulty Subscriber

To replace a faulty Subscriber, go to Emergency Responder administration and delete the faulty Subscriber. Install a new Emergency Responder Subscriber for the Publisher (see the "Installing Cisco Emergency Responder 8.6 on a New System" section on page 2-14).

Note If the same host name is not going to be used by the replacement Subscriber server, you must delete the faulty Subscriber using the Emergency Responder administration screen on the Publisher server.

Replacing a Faulty Publisher

You can restore the Publisher only if you have backed up the Publisher using the Disaster Recovery System available as part of the Emergency Responder. See the "Backing Up and Recovering Data" section on page 11-32.

To replace a faulty Publisher, follow these steps:

Procedure

Step 1 Install the same version of the Emergency Responder Publisher on a server with the same host name as the one you used previously.

Step 2 Choose the same configuration options (such as the Cisco Unified CM version, and so on) during the installation.

Step 3 Restore the old configuration data using the Disaster Recovery System.

Using the Cisco Emergency Responder Admin Utility

You can use the Emergency Responder Admin Utility tool to perform the following tasks:

- To update Emergency Responder cluster database host details
- To upgrade the CCM version

This section describes the following topic:

- How to Use the Cisco Emergency Responder Admin Utility Tool, page 11-19

How to Use the Cisco Emergency Responder Admin Utility Tool

To use the Emergency Responder Admin Utility tool, follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface.

Step 2 Using the menu bar, choose a task to perform:

a. To change the Publisher that the Subscriber server points to, select **Update > Publisher**.

b. To update the Cisco Unified CM version, select **Update > CCM Version**.

c. To update the cluster settings on both the Publisher and Subscriber servers, select **Cluster > DBHost**.

Note This action updates the Emergency Responder cluster DB details for this server group only. Other servers in this Emergency Responder cluster will NOT be updated automatically.

Step 3 To save the changes that you have made, restart both the Publisher and the Subscriber servers.

Troubleshooting the Subscriber Database Setup

To configure the Publisher-Subscriber setup again if you have an issue with the Subscriber (apart from DB replication), follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface on the Subscriber server.

Step 2 Select **Update > Publisher**.

Step 3 Specify the same Publisher Host Name, IP address (already being pointed to) and database access security password.

Step 4 Click **Go**.

This step might a take a while setup.

Troubleshooting the Database and Enterprise Replication

Use the following CLI commands for troubleshooting the Informix Dynamic Server (IDS) database:

- **utils service list—U**sed to check whether the IDS service is running or not
- **show tech dbstateinfo**—Gives the DB state information which is helpful in debugging database issues
- **show tech dbinuse**—Displays the currently used database
- **show tech dbintegrity**—Shows database integrity information
- **show tech database**—Creates a .csv file with contents of all the tables in the database

Use the following CLI commands for troubleshooting Enterprise Replication:

- **utils dbreplication status**—Used to show the status of the database replication
- **utils dbreplication reset**—Resets and restarts the database replication between the Publisher and Subscriber
- **utils dbreplication repair**—Compares the data on replication servers (Publisher and Subscriber) and create a report listing data inconsistencies and repairs the data inconsistencies. This command also tries to repair replication by rebuilding the corrupted .rhosts file if it is corrupted for some reason.

For troubleshooting database problems using logs, download logs from the Emergency Responder Serviceability website or through CLI.

The following logs provide information for debugging database related issues

- Install/Upgrade logs—/var/log/install/
- Install DB logs—/var/log/active/er/trace/dbl/sdi/
- CERDbMon logs—/var/log/active/er/trace/dbl/sdi/cerdbmon/
- CLI logs—/var/log/active/platform/log/

Symptom Replication fails to start after the Subscriber is installed with DNS and the CLI command **utils dbreplication status** shows replication not working.

Possible Cause The .rhosts have the Host Name for the Subscriber instead of FQDN (Fully Qualified Domain Name) of the Subscriber.

Recommended Action Use the CLI command **utils dbreplication repair** to repair the replication issue. This command tries to repair replication by rebuilding the corrupted .rhosts file.

Troubleshooting Cisco Emergency Responder System Problems

These are some issues you might encounter with general operation of the Emergency Responder system and the configuration screens that involve the Emergency Responder server, group, and cluster:

Symptom Emergency Responder intra-cluster call routing fails or Emergency Responder does not discover phones correctly.

Recommended Action Ensure that all the Emergency Responder servers in an Emergency Responder cluster can be found by their host name, and ensure that all are reachable on the network by all the other Emergency Responder servers.

Recommended Action Ensure that all the Emergency Responder servers can reach the Emergency Responder cluster DB host and that the cluster DB password is the same across all servers in the cluster.

Symptom Emergency Responder exits after starting.

Possible Cause You have configured Emergency Responder to use a TCP port that is already in use.

Recommended Action Check the Windows Event Viewer for the message "CER could not open socket at port *peer-tcp-port*, Exiting." If you see this message, change the Emergency Responder group configuration to use a different TCP port. See the "Configuring a Cisco Emergency Responder Server Group" section on page 4-21 for instructions.

Symptom The Emergency Responder Groups in Cluster screen does not load, and exhibits the error "Cannot connect to cluster DB host."

Recommended Action Ensure that the cluster DB host can be found by host name.

Ensure that the specified cluster db host password is the same across all Emergency Responder server groups in the cluster.

For more information, see the "8.6 Cisco Emergency Responder Cluster and Cluster DB Host" section on page 4-28.

Related Topics

- Identifying the Cisco Emergency Responder Groups and Servers in a Cisco Emergency Responder Cluster, page 11-23
- Starting and Stopping a Cisco Emergency Responder Server, page 11-24

- Viewing Event Messages, page 11-29
- Managing Performance, page 11-30
- Backing Up and Recovering Data, page 11-32

Troubleshooting Cisco Unified Communications Manager Configuration Problems

These are some issues that you might encounter when the Emergency Responder communicates with Cisco Unified CM. Additional problems with symptoms that involve emergency call failures are discussed in the "Troubleshooting Emergency Call Problems" section on page 11-5.

Symptom Emergency Responder does not register with the route points and CTI ports configured for its use.

Recommended Action Ensure that the route points and CTI ports are associated with the Cisco Unified CM Cisco Emergency Responder user (see the "Creating a Cisco Emergency Responder Cisco Unified CallManager User" section on page 3-20.) Ensure that the CTI Manager on the Cisco Unified CM server (or the DC Directory on a Windows-based Cisco Unified CM server) is running properly.

Symptom When trying to delete a Cisco Unified CM from the Cisco Emergency Responder configuration, Emergency Responder prevents me and displays the message "Phone tracking in progress."

Recommended Action You cannot delete a Cisco Unified CM server from the Emergency Responder configuration while a phone tracking process is in progress. Retry the deletion after the process has ended.

Updating Cisco Emergency Responder After You Add Devices

You must create a Cisco Unified CM user for Emergency Responder use and CTI ports and route points that must be assigned to the user before Emergency Responder tries to create a provider with the Emergency Responder cluster. Emergency Responder only registers the CTI ports and route points that are associated with the user when the provider is created. Thus, any devices you add to the user after starting Emergency Responder is not registered by Emergency Responder.

If you add devices to the Emergency Responder user in Cisco Unified CM, you can force Emergency Responder to recreate the provider using any of these techniques:

- Restart the Emergency Responder server.
- Delete the Cisco Unified CM server from the Emergency Responder configuration and re-enter it.
- Change the backup CTI Manager setting for the Cisco Unified CM server in the Emergency Responder configuration and click **Update**. This forces Emergency Responder to log off the provider and recreate it.
- Change the name of the user in Cisco Unified CM, or create a new user, and associate all devices with it. Then update the Emergency Responder configuration to use the new user.

Identifying the Cisco Emergency Responder Groups and Servers in a Cisco Emergency Responder Cluster

If you are connected to the administrator interface on a Emergency Responder server, you can view the details of the server and the Emergency Responder group's standby server by selecting **System > Cisco ER Group Settings**.

You can also identify the Emergency Responder groups and their Emergency Responder servers that are in the same Emergency Responder cluster. To view the other Emergency Responder groups in the cluster, select **System > Cisco ER Groups in Cluster**. From the Emergency Responder Groups in Cluster page, select the group you want to view; and Emergency Responder displays the Emergency Responder servers that are in the group. To view the details for these servers, you must log in t to the Emergency Responder Administration interface running on one of the servers, select **System > Cisco ER Groups in Cluster**, then select the group you want to view from the list of groups.

If you must uninstall a Emergency Responder group, first delete the group from the Emergency Responder cluster using this page. You must log in as a system administrator to delete the group. Deleting the group from the cluster simply removes the entries for the group from the Emergency Responder Cluster DB; it does not remove Emergency Responder from the group's servers.

Related Topics

- Cisco Emergency Responder Server Groups in Cluster, page A-2

Phones Moving Between Clusters

The following scenario illustrates how Emergency Responder clusters work and how Emergency Responder treats phones moving between clusters:

- Server Group A (SGA) has a phone (Phone_1) that is moving out of SGA.
  - Emergency Responder discovers Phone_1 in Server Group B (SGB).
  - The Unlocated Phones page in SGA display the phone in SGB.
- If both the Emergency Responder servers (Publisher and Subscriber) in SGB go down, SGA still displays Phone_1 in SGB.
  - Calls made from Phone_1 during this time are redirected to SGB and Emergency Responder takes the same steps to route this emergency call when Emergency Responder servers are not there in SGB.
  - Phone_1 is also treated like any other phone in SGB when both the SGB Emergency Responder servers are down.
- If Phone_1 moves to Server Group C (SGC):
  - It is discovered after the next incremental phone tracking on SGA and then in SGC.
  - The Unlocated Phones page changes the association of Phone_1 to SGC.
- If Phone_1 moves back to SGA, it is discovered in the next incremental phone tracking and displayed under the corresponding switch port.

Starting and Stopping a Cisco Emergency Responder Server

When you install Emergency Responder, the Emergency Responder server is set up to automatically start whenever the computer is powered up or rebooted. However, you can stop and then restart an Emergency Responder server through the Emergency Responder Serviceability web interface without powering down or rebooting the computer. You might find this helpful if you are trying to debug a problem.

To start or stop an Emergency Responder server, follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Serviceability web interface and select **Tools > Control Center**.

The Control Center Services page displays, showing all Emergency Responder services and the current status of each one.

Step 2 Click the radio button to the left of the service name, then click **Start**, **Stop**, or **Restart** to perform the desired action on the service. Click **Refresh** to refresh the screen with updated information.

Note The buttons only appear if the action is possible; for example, **Start** only appears if the service is currently stopped.

Note The Cisco Tomcat and Cisco IDS services cannot be started or stopped from the Control Center. These services can only be started or stopped using the **utils service** command. For additional information, see the "utils service" section on page F-79.

Table 11-1 explains the meaning of the icons you see on the Control Center Services page.

Table 11-1 Cisco Emergency Responder Control Center Icons

Icon	Meaning
	The Emergency Responder server or the Emergency Responder Phone Tracking Engine is started and functioning normally.
	The Emergency Responder server Emergency Responder Phone Tracking Engine was stopped by the administrator.

Related Topics

- Control Center, page B-1

Troubleshooting ALI Data Uploads

Periodically, you must export your ALI data and submit it to your service provider. The ALI data is used to route emergency calls from your network to the correct PSAP, and provide the PSAP with information about the location of the emergency call.

Emergency Responder lets you export the ALI data in a variety of NENA formats. Ask your service provider which format you should use.

During the upload process, you might find that some ALI data records did not upload correctly. Your service provider should be able to provide you with a list of errors, or you might see these when using your service provider's data upload software. You must fix any mistaken records and resubmit the ALI data export file. To fix the records, you might need to manually edit the records in error.

These sections describe the general procedure for fixing ALI data records, and explain how to edit the various types of NENA formatted files:

- Fixing ALI Data Records, page 11-25
- Editing NENA 2.0 and 2.1 File Formats, page 11-25
- Editing NENA 3.0 File Formats, page 11-26

Fixing ALI Data Records

To correct data errors you might receive when uploading ALI records to your service provider, follow these steps:

Before You Begin

Obtain NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, from NENA or your service provider. This document explains the various NENA formats in detail.

Procedure

Step 1 Look through the error reports to determine the problems you encountered.

Step 2 Emergency Responder web interface, change the fields that were in error for the ERL/ALI records that failed. For example, if the Street Suffix was an unacceptable abbreviation, change it to an acceptable one. Save all of your changes.

Step 3 Export the ALI data again (see the online help).

Step 4 If any of the records in error were new, you must change the database function for the records. Because Emergency Responder has already exported these records, Emergency Responder labels them as updates rather than new insertions. However, because these records failed on upload, the service provider's database views them as new.

Open the ALI export file in a text editor and change the function code for the records that you are fixing. Use an editor that will not add formatting or other extra characters. See these sections for details about editing the files:

- Editing NENA 2.0 and 2.1 File Formats, page 11-25
- Editing NENA 3.0 File Formats, page 11-26

Step 5 Submit the edited file to your service provider.

Editing NENA 2.0 and 2.1 File Formats

The NENA 2.0 and 2.1 file formats have these characteristics:

- Fixed-length records

- Fields are in a specific order
- Unused fields are filled with blanks
- End of record is indicated by an asterisk (*)

Use NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, to determine the byte location and length of each field. When you edit the file, ensure that you are not lengthening the records. Delete any extra spaces that get added. If the length of an item is less than the length of a field, pad the field with blanks. Depending on the field, padding might be on the right or the left.

The file contains one header and one trailer record. The ALI data records are contained between these records.

Table 11-2 describes the fields you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 11-2 NENA 2.0 and 2.1 Common Fields

Field	Description
Function Code	**Location:** Byte 1. **Length:** 1 character. **Description:** The database function for the record. One of: • **I**—Insert new ALI record • **C**—Change existing record. You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record. Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in Emergency Responder, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Location:** Byte 62 to 67. **Length:** 6 characters. **Description:** The sequence number of the file you are submitting to the service provider (for example, 1, 2, etc.) The number is right-aligned with leading spaces. Your service provider might ignore this field.
Record count	**Location:** Byte 62 to 70 in the trailer record. **Length:** 9 characters. **Description:** The total number of records in the file you are submitting to the service provider (for example, 1, 2, etc.) The number is right-aligned with leading spaces.

Editing NENA 3.0 File Formats

The NENA 3.0 file format has these characteristics:

- Variable-length records.
- Fields are a tag and data combination, and can be in any order.

- Unused fields are not included. The presence or absence of a tag has this effect:
  - If the tag is not included, the previous value of the element, if any, is left unchanged.
  - If the tag is included with a blank value, any previous value for the element is removed.
  - If the tag is include with a non-blank value, the value of the element is changed to the new value.
- Tags are separated by a vertical bar (|).
- End of record is indicated by a pre-defined character.

Use NENA Doc 02-010, *Recommended Formats and Protocols for Data Exchange*, to determine tag name and values for each field. Ensure that your values do not exceed the maximum length for the field. You do not need to pad fields with extra blanks.

The file contains one header and one trailer record. The ALI data records are contained between these records.

Table 11-3 describes the fields you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 11-3 NENA 3.0 Common Fields

Field	Description
Function Code	**Tag:** FOC. **Description:** The database function for the record. One of: • **I**—Insert new ALI record (FOCI) • **C**—Change existing record (FOCC). You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record (FOCD). Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in Emergency Responder, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Tag:** CYC. **Description:** The sequence number of the file you are submitting to the service provider (for example, CYC1, CYC2, etc.) Your service provider might ignore this field.
Record count	**Tag:** REC in the header and trailer records. **Description:** The total number of records in the file you are submitting to the service provider (for example, REC1, REC2, etc.)

Collecting Call History Logs

Emergency Responder maintains extensive call history logs, which include entries for each emergency call handled. You can view call history information from the administration and user interfaces.

Emergency Responder maintains in its database a history of the emergency calls that have been placed. When the primary Emergency Responder server (Publisher) is not active, emergency calls are handled by the backup Emergency Responder server (Subscriber). Through replication, the call history records on both these servers are synchronized when they are active. For this reason, the call history can be viewed on either of the Emergency Responder servers.

To download these records, click on the **Download** button at the top of the table displaying the call history. These records are downloadable in Excel (.xls) format.

Collecting Trace and Debug Information

When you contact Cisco Technical Support for help with a problem that you are having with Emergency Responder, Cisco might request that you collect trace and debug information.

Because collecting trace and debug information affects Emergency Responder performance, you should only turn on tracing and debugging at Cisco's request. The generated information is for Cisco's use in resolving product problems.

Use the following sections to learn about:

- Collecting Trace and Debug Information, page 11-28
- Enabling Syslog, page 11-29

Enabling Detailed Trace and Debug Information for Cisco Emergency Responder

To enable detailed trace and debug information for Emergency Responder, follow these steps:

Procedure

Step 1 From the Emergency Responder web interface, select **Cisco ER Group>Server Settings**.

Emergency Responder opens the Server Settings page.

Step 2 From the left column, select the server from which you must collect debug or trace information.

Emergency Responder displays the settings for the server.

Step 3 Scroll down to the debug package and trace package sections and select the packages that Cisco Technical Support has requested.

The lists in each section are identical; make sure that you select the package in the list that Cisco requested. Packages selected in the Debug list generate trace information plus extra debug data. If Cisco requests that you select all packages, click **Select All** for the appropriate list.

The available packages include:

- CER_DATABASE—The database subsystem, covers the log information generated by the database access code.
- CER_REMOTEUPDATE—The remote update subsystem, which manages updates between servers.
- CER_PHONETRACKINGENGINE—The phone tracking subsystem, which runs the phone tracking and switch-port and phone update processes.
- CER_ONSITEALERT—The onsite alert subsystem for notifying onsite alert personnel.

- CER_CALLENGINE—The call engine subsystem, which routes and processes calls.
- CER_SYSADMIN—The system administration web interface subsystem.
- CER_TELEPHONY—The telephony subsystem, used for interactions with Cisco Unified CM.
- CER_AGGREGATOR—The aggregator module covers all Emergency Responder server communication and data handling with the phone tracking engine. The module includes the search and lookup of tracked data for the subsystems like cluster, Administration, Cisco IP SoftPhone and call routing.
- CER_GROUP—The Emergency Responder server group subsystem, used for communicating between servers within a group.
- CER_CLUSTER—The server cluster subsystem, used for communicating between Emergency Responder groups in a cluster.

Step 4 Click **Update** to save and activate your changes.

Emergency Responder begins generating the requested trace and debug information.

Note The traces for Emergency Responder can be collected from either Emergency Responder Serviceability web interface or by using the CLI.

Step 5 When you have finished generating debug and trace information, click **Clear All** for each section in which you have made a selection to turn off debug and trace. Then, click **Update** to complete the change.

Related Topics

- Server Settings for Emergency ResponderServerGroup, page A-7
- Appendix B, "Serviceability Web Interface For Cisco Emergency Responder"
- Appendix F, "Command Line Interface"

Enabling Syslog

To collect trace and debug information, you must enable syslog for Emergency Responder).

To enable syslog for Emergency Responder, see the "Collecting Information from Syslog" section on page 11-31.

Viewing Event Messages

You can view Emergency Responder event messages to help diagnose problems with the software by using the Emergency Responder Serviceability web interface.

For information about viewing Emergency Responder events, see the "Using the Event Viewer" section on page 6-2.

For details about the Find and List Events page, see the "Event Viewer" section on page B-2.

Managing Performance

See the *Release Notes for Cisco Emergency Responder 8.6* for supported Cisco MCS Unified CM Appliance platforms and their Emergency Responder scalability.

Emergency Responder performance can be affected if Emergency Responder is managing switches across a WAN link. Emergency Responder must send SNMP requests to the managed switches, and WAN delays can lead to SNMP timeouts and increase the time needed to track phone and switch changes. You might need to tune the SNMP parameters. See the "Configuring the SNMP Connection" section on page 4-44 for more information.

Integrating with Network Management Systems

You can manage the status of the Emergency Responder server remotely using CiscoWorks2000 or another SNMP-based network management system. CiscoWorks2000 is the standard Cisco network management system, but it is not bundled with Emergency Responder. For more information about CiscoWorks2000, Campus Manager, and Topology Services, see the documentation, available at the following URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/tsd_products_support_category_home.html

These topics provide information to assist you in integrating Emergency Responder with network management systems:

Understanding CDP Support

Cisco Emergency Responder uses the Cisco Discovery Protocol (CDP) to periodically send out CDP messages, on the active interface, to a designated multicast address. These messages contain information such as device identification, interface name, system capabilities, SNMP agent address, and time-to-live. Any Cisco device with CDP support can locate a Cisco Emergency Responder server by listening to these periodic messages.

Using information provided through CDP, the CiscoWorks2000 Server can detect the Cisco Emergency Responder server, and the Campus Manager application, Topology Services, can build topology maps displaying the Cisco Emergency Responder server.

In addition to sending out CDP messages, the Cisco Emergency Responder server uses CDP to locate phones that support CDP. You must ensure CDP is enabled on your switches so that Cisco Emergency Responder can obtain this information through SNMP queries to the switches.

Table 11-4 shows the SNMP OIDs for the Cisco Emergency Responder hardware platforms.

Table 11-4 Cisco Emergency Responder Hardware Platform OIDs

Hardware Platform	SNMP OID
Cisco MCS-7815-I	1.3.6.1.4.1.9.1.582
Cisco MCS-7825-H	1.3.6.1.4.1.9.1.583

Table 11-4 Cisco Emergency Responder Hardware Platform OIDs

Hardware Platform	SNMP OID
Cisco MCS-7825-I	1.3.6.1.4.1.9.1.746
Cisco MCS-7835-H	1.3.6.1.4.1.9.1.584
Cisco MCS-7835-I	1.3.6.1.4.1.9.1.585
Cisco MCS-7845-H	1.3.6.1.4.1.9.1.586
Cisco MCS-7845-I	1.3.6.1.4.1.9.1.587

Monitoring Cisco Emergency Responder Subsystem Status

Cisco Emergency Responder supports the SYSAPPL-MIB that allows you to use CiscoWorks2000 or a third-party SNMP browser to remotely access information about the following Emergency Responder components:

- Cisco Emergency Responder Server
  - CERServer.exe
- Cisco PhoneTrackingEngine
  - CERPhoneTracking.exe
- MSQL Server-related Services

The SYSAPPL-MIB uses SNMP. Emergency Responder supports the following SYSAPPL-MIB tables:

- SysApplInstallPkgTable—provides installed application information such as Manufacturer, Product Name, Version installed, Date installed, and Location, which is a partial URL for accessing the associated Application Administration web page (when applicable).
- SysApplRunTable—describes the application starting time and run-time status.
- SysApplInstallElmtTable—describes the individual application elements, or associated executables, which comprise the applications defined in the SysApplInstallPkgTable.
- SysApplElmtRunTable—describes the processes, or executables, that are currently running on the host system.

Collecting Information from Syslog

You can configure Emergency Responder to use the Cisco Syslog Collector. Cisco Syslog Collector and Cisco Syslog Analyzer are offered with CiscoWorks2000 as part of the Resource Management Essentials package. You can also adapt Syslog output from Emergency Responder for use with other network management systems.

The Cisco Syslog Collector keeps common system logs of messages reported to Emergency Responder.

The Cisco Syslog Analyzer controls and displays all events efficiently so they can easily be read, interpreted, and used for system maintenance and problem solving.

To install and configure the Cisco Syslog Collector, see the CiscoWorks2000 documentation.

To enable syslog, follow these steps:

Procedure

Step 1 Select **System > Cisco ER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Select enable in **Enable Syslog**.

Step 3 Enter the fully-qualified DNS name of the server in the **Syslog Server** field, for example, server.domain.com.

Step 4 Click **Update Settings** to save your changes.

Emergency Responder immediately begins writing messages to syslog.

Related Topics

- Cisco Emergency Responder Group Settings, page A-3

Backing Up and Recovering Data

Emergency Responder 8.6 uses the Disaster Recovery System to backup and restore system data.

For information about using the Disaster Recovery System, see Chapter 8, "Configuring the Cisco Emergency Responder 8.6 Disaster Recovery System."

Related Topics

- Collecting Call History Logs, page 11-27

Troubleshooting the Data Migration Assistant

The Data Migration Assistant (DMA) operates in two phases. In the first phase, Database, the following folders are backed up to a tar file:

- export
- import
- etc
- nena_msag_records

In the second phase, the contents of the backed-up Emergency Responder database are verified against the Emergency Responder 8.6 database schema.

Symptom DMA backup and validation failed.

Recommended Action Go through the following check list:

– Check if MSDE is running. If the database is not running, the backup fails.

- Verify that the node being backed up is a Publisher node, not a Subscriber node. DMA backup cannot be performed on a Subscriber node.
- Verify that CSA is not running. If CSA is running, stop it before starting the backup.

Symptom DMA backup is successful but the validation failed.

Recommended Action Go through the following check list:

- Verify that CSA is not running. If CSA is running, stop it before starting the backup. CSA interferes with DMA operation.
- Collect the data validation logs for further analysis. In this case, some changes may need to be made to the data in the database before a migration to Emergency Responder 8.6 can succeed.

The DMA Logs are in the following locations:

- exportdb.log and migratecCERCSV.log are in C:\CiscoWebs\DMA\Bin
- installdbw1.log, installdbw1.log.err, installdbccm.log, installdbccm.log.err, and dbl_INSTALLDBxxxxxx.txt are located under C:\Program Files\Cisco\Trace\DBL
- Log Files are located under C:\Program Files\Cisco\Trace\DMA

The validation log files are as follows:

- exportdb.log
- installdbw1.log
- installdbw1.log.err
- dbl_INSTALLEDBxxxxxx.txt

Troubleshooting Linux Upgrades

You might encounter certain problems when upgrading to future versions of Emergency Responder from Emergency Responder 8.6. This section explains what could cause these problems and the provides recommended actions.

Symptom On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch, the error message “No valid upgrade options found” appears.

Recommended Action Verify that you are not trying to upgrade the Subscriber before upgrading the Publisher. When upgrading an Emergency Responder servergroup, you must always upgrade the Publisher first.

Recommended Action Verify that the local/remote path that you have specified actually contains a valid, signed ISO image, having the extension .sgn.iso.

Symptom On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch at a remote location, the error message “Incorrect user name/password” appears.

Recommended Action Verify that the username and password entered for the remote SFTP/FTP location are correct.

Symptom After downloading the ISO image onto the Emergency Responder server, the checksum values do not match.

Recommended Action Download a fresh ISO image from Cisco.com and try the upgrade again.

Symptom The upgrade was cancelled, but a warning message appears prompting you to reboot the system.

Recommended Action During the upgrade, certain services on the Emergency Responder server could have been stopped, depending on when the upgrade was cancelled. In this case, it is highly recommended that you reboot the server.