Nortel Mobile Communication 3100

# Nortel Mobile Communication 3100 Troubleshooting

Release: 3.0
Document Revision: 01.03

www.nortel.com

NN42030-700

Nortel Mobile Communication 3100
Release: 3.0
Publication: NN42030-700
Document status: Standard
Document release date: 9 June 2009

Printed in Canada

LEGAL NOTICE

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel’s express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

# Contents

# New in this release

The following sections details what's new in *Nortel Mobile Communication 3100 Troubleshooting* (NN42030-700) for Mobile Communication 3100 (MC 3100) Release 3.0.

- "Features" (page 5)
- "Other changes" (page 5)

## Features

For information on all the MC 3100 Release 3.0 features, see *Nortel Mobile Communication 3100 Fundamentals* (NN42030-109) .

## Other changes

This document is new for MC 3100 Release 3.0.

### Revision history

| | |
|---|---|
| June 2009 | Standard 01.03. This document is issued to support Nortel Mobile Communication 3100 Release 3.0 SU3. Changes were made to technical content. |
| January 2009 | Standard 01.02. This document is issued to support Nortel Mobile Communication 3100 Release 3.0. Changes were made to "Downloading all log files" (page 19), "Downloading an individual log file" (page 19), "Sorting the log files" (page 20), and "Performing a packet capture" (page 23). |
| September 2008 | Standard 01.01. This document is issued to support Nortel Mobile Communication 3100 Release 3.0. |

# Overview

This document provides information about the troubleshooting of the Nortel Mobile Communication 3100 (MC 3100).

## Navigation

## References

For more information, see the following documents:

- *Nortel Mobile Communication 3100 Fundamentals* (NN42030-109)
- *Nortel Mobile Communication Client 3100 for BlackBerry User Guide* (NN42030-101)
- *Nortel Mobile Communication Client 3100 for Nokia User Guide* (NN42030-102)
- *Nortel Mobile Communication Client 3100 for Windows Mobile User Guide* (NN42030-107)
- *Nortel Mobile Communication 3100 Planning and Engineering* (NN42030-200)
- *Nortel Mobile Communication 3100 Installation and Commissioning* (NN42030-300)
- *Nortel Mobile Communication 3100 Administration and Security* (NN42030-600)

# Accessing the system

This module provides information about the ways to access the system from the Web Console and from the command line.

## Navigation

- "Logging on to the MC 3100 Web Console as an administrator" (page 9)
- "Changing the MC 3100 Web Console password" (page 12)
- "Accessing the server command line as nortel" (page 13)
- "Accessing the server command line as superuser" (page 14)

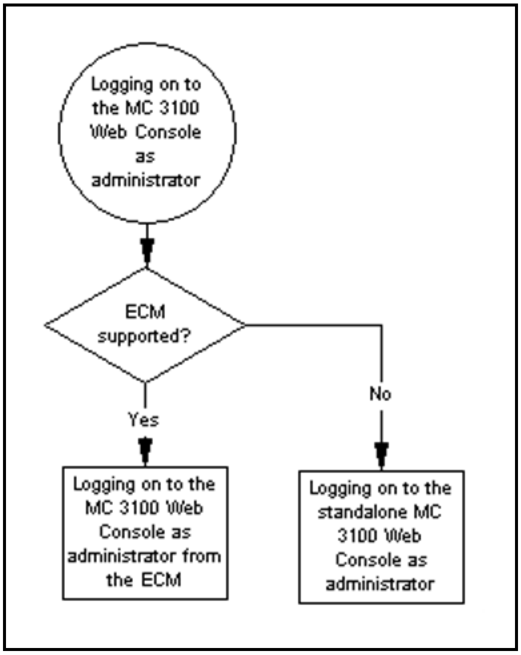
## Logging on to the MC 3100 Web Console as an administrator

This module describes the procedures you use to log on to MC 3100 Web Console to perform administration tasks.

### Logging on to the Web Console as an administrator task flow

The following flowchart depicts the procedures you perform to log on to the Web Console as an administrator. To link to any procedure, go to "Navigation to Logging on to the Web Console as an administrator " (page 10)

**Figure 1**
**Logging on to the Web Console as an administrator task flow**


Logging on to the MC 3100 Web Console as administrator
ECM supported?
Yes
No
Logging on to the MC 3100 Web Console as administrator from the ECM
Logging on to the standalone MC 3100 Web Console as administrator

## Navigation to Logging on to the Web Console as an administrator

- "Logging on to the standalone MC 3100 Web Console as an administrator" (page 10)

## Logging on to the standalone MC 3100 Web Console as an administrator

Log on to the MC 3100 Web Console as an administrator to manage the system, monitor the users, monitor Instant Conferencing, and manage the client server repository.

---

**Attention:** Wait two minutes after starting the MCG 3100 before accessing the MC 3100 Web Console.

---

### Prerequisites

- You need the administrator user id and password to perform this procedure.
- Access the MC 3100 Web Console using a web browser.

---

**Attention:** User names and passwords are case-sensitive.

---

### Procedure Steps

| Step | Action |
|---|---|
| 1 | In the **Address** field of your Web browser, enter<br>`http://<IP address | hostname>:8282/adminserver`<br>**OR**<br>`https://<IP address | hostname>:8553/adminserver` |
| 2 | In the **Username** field, type the user name. |
| 3 | In the **Password** field, type the admin password. |

**Attention:** Nortel recommends that you change the default administrator password. For more information, see "Changing the MC 3100 Web Console password" (page 12).

| Step | Action |
|---|---|
| 4 | Click **Sign In**. |
| 5 | Click a tab at the top of the MC 3100 Web Console to view the corresponding page. |

**--End--**

### Variable definitions

| Variable | Definition |
|---|---|
| <IP address \| hostname> | The name of the MCG server in fully qualified domain name (FQDN) format, or the IP address of the server. |
| user name | Default: admin |
| admin password | Default: password |

## Accessing the MC 3100 Web Console from the ECM

Access the MC 3100 Web Console from the ECM.

### Prerequisites

- The ECM must be configured to contain the MCG 3100 servers as elements.
- You must have a valid user ID and password to access the ECM.

### Procedure Steps

| Step | Action |
|---|---|
| 1 | Open a Web browser. |
| 2 | Navigate to the main ECM Web page.<br>For information on the Web address, userid and password, see your ECM administrator. |
| 3 | In the **User ID** field, enter the ECM userid. |
| 4 | In the **Password** field, enter the ECM password. |
| 5 | Click **Login**.<br>The Elements page displays. |
| 6 | Click on the MCG 3100 element you require.<br>The Web Console for the selected MCG 3100 server displays. |

**--End--**

### Variable definitions

| Variable | Definition |
|---|---|
| User ID | Your ECM user name, as given by your ECM administrator. |
| Password | The password associated with your ECM user name, as given by your ECM administrator |

## Changing the MC 3100 Web Console password

Change the MC 3100 Web Console password from the default password.

### Prerequisites

- You must be logged into the MC 3100 Web Console as administrator. For more information, see "Logging on to the standalone MC 3100 Web Console as an administrator" (page 10).

### Procedure Steps

| Step | Action |
|---|---|
| 1 | On the MC 3100 Web Console main page, click the **Tools** tab. |
| 2 | In the **Admin Server Password** section, in the **Current Password** box, type the current password. |

**Attention:** Passwords are case-sensitive.

3 In the **New Password** box, type a new password.

4 In the **Confirm New Password** box, retype the new password.

5 In the **Admin Server Password** section, click **Save**.

**--End--**

### Variable definitions

| Variable | Definition |
|---|---|
| Current Password | Existing password.<br>The default password for new servers is *password.* |
| New password | New password for the Admin server.<br>Secure passwords use a mix of letters, numbers and alphabetic characters and can be up to 19 characters in length. |
| Confirm New Password | New password for confirmation. |

## Accessing the server command line as nortel

Use this procedure to access the server command line as nortel.

### Prerequisites

- You require the password to the nortel userid on the server.

### Procedure Steps

**Step** **Action**

1 Use SSH to connect to the server.

2 At the userid prompt, enter `nortel`

3 At the password prompt, enter <password>

**--End--**

### Variable definitions

| Variable | Definition |
|---|---|
| <password> | The password associated with the nortel userid. For information on the default nortel password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) . |

## Accessing the server command line as superuser

Use this procedure to access the server command line as root.

### Prerequisites

- You require the password to the nortel userid on the server.
- You require the password to the superuser (root) userid on the server.

### Procedure Steps

| Step | Action |
|---|---|
| **1** | Use SSH to connect to the server. |
| **2** | At the userid prompt, enter `nortel` |
| **3** | At the password prompt, enter <password> |
| **4** | To become the root user, enter `su root` |
| **5** | At the prompt, enter <root_password> |

**--End--**

### Variable definitions

| Variable | Definition |
|---|---|
| <password> | The password associated with the nortel userid. For information on the default nortel password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) . |
| <root_password> | The password associated with the superuser. For information on the default superuser password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) . |

# System recovery

This chapter describes the actions you take if your system becomes unresponsive.

1. Work through the troubleshooting procedures in the next sections of this book.
2. If your system is still unresponsive, execute "Downloading all log files" (page 19).
3. Save the log files on another computer in preparation for assistance from Nortel.
4. Access the command line, using "Accessing the server command line as nortel" (page 13).
5. Enter the following command:
   **`ps`**
6. Record the information displayed on the screen.
7. Contact your Nortel support organization immediately.

---

**Attention:** Do not reboot or restart your system. The Nortel technical support team may require additional information.

---

8. The Nortel support organization will instruct you on to the next steps to take.

# Troubleshooting and maintenance of MC 3100

The following modules describe the Mobile Communication 3100 (MC 3100) troubleshooting and maintenance.

## Troubleshooting license file problems

If you encounter a problem with the license file installation, an error message appears in the License Info field on the System Configuration window. The following table lists the most common error messages and possible solutions.

**Table 1**
**License file error messages**

| Error message | Description | Solution |
|---|---|---|
| License Info: License file not found | The Mobile Communication Gateway 3100 (MCG 3100) is not activated and requires the license file. | Upload the license file on the System Configuration screen. |
| License Info: License is invalid | The MCG 3100 is using another activated machine's license file. | Upload a valid license file on the System Configuration screen. |
| License Info: License expired | The license file is no longer valid. | Upload a valid license file on the System Configuration screen. |
| License Info: ERROR 23: protocol violation | The MCG 3100 is not activated although the license file is valid. The local system clock is out of sync with the licensing server clock. | Reset the clock and restart the system. |

**Table 1**
**License file error messages (cont’d.)**

| Error message | Description | Solution |
|---|---|---|
| License Info: ERROR 103: Client’s system clock is suspect and / or the client configur ation has been tampered with. | The system clock changed after the MCG 3100 was activated. | Reset the clock and restart the system. |
| License Info: ERROR 17: key limit exceeded | The license file has been activated before with other machines and there are no licenses available for you to activate. | Contact the licensing server administrator. |

If the recommended solution fails to correct the problem, or if the problem is not listed, contact the administrator of the licensing server for assistance.

Before contacting the administrator:

- Ensure that the date, time, and time zone for the system is synchronized with the licensing server.
- Check the network connection between your system and the licensing server (route, DNS).
- Check the most recent error message on the Gateway Configuration screen.
- Restart the server.

## Using log files

The MCG 3100 automatically generates the following log files:

- Boot log
- MCG 3100 Alarms log
- Nortel Gateway log
- Server log
- Error log

The log files are generated on a daily basis, with the current day’s output overwriting the output from preceding day.

Use the following procedures to handle the log files:

- "Downloading all log files" (page 19)
- "Downloading an individual log file" (page 19)
- "Sorting the log files" (page 20)
- "Opening a log file" (page 21)

## Downloading all log files

You can download all the log files from the MCG 3100 to a folder on your PC for analysis.

### Prerequisites

- You must be logged into the MC 3100 Web Console as administrator. For more information, see "Logging on to the MC 3100 Web Console as an administrator" (page 9).

### Procedure Steps

| Step | Action |
|---|---|
| **1** | Click the **Tools** tab. |
| | The Tools page displays. |
| **2** | Scroll to the Server Logs section. |
| **3** | In the redundant configuration, select a gateway. |
| **4** | Click **Download all Logs**. |
| **5** | Click **Save**. |
| **6** | Navigate to the folder where you want to save the log files. |
| **7** | Click **Save**. |
| | The log files are saved. |

**--End--**

## Downloading an individual log file

You can download a single log file from the MCG 3100 to a folder on your PC for analysis.

### Prerequisites

- You must be logged into the MC 3100 Web Console as administrator. For more information, see "Logging on to the MC 3100 Web Console as an administrator" (page 9).

### Procedure Steps

| Step | Action |
|---|---|
| 1 | Click the **Tools** tab.<br>The Tools page displays. |
| 2 | Scroll to the Server Logs section. |
| 3 | In the redundant configuration, select a gateway. |
| 4 | Click the **Download** link for the log file you wish to download:<br>• boot.log<br>• MobilityGateway-Alarms.log<br>• MobilityGateway.log<br>• server.log<br>• sipconferror.log |
| 5 | Click **File, Save As**. |
| 6 | Navigate to the folder where you want to save the log file. |
| 7 | Click **Save**.<br>The log file is saved. |

**--End--**

## Sorting the log files

You can sort the logs by name, file size, or date modified.

### Prerequisites

- You must be logged into the MC 3100 Web Console as administrator. For more information, see "Logging on to the MC 3100 Web Console as an administrator" (page 9).

### Procedure Steps

| Step | Action |
|---|---|
| 1 | Click the **Tools** tab.<br>The Tools page displays. |
| 2 | Scroll to the Server Logs section. |
| 3 | In the redundant configuration, select a gateway. |

4 Click the column heading to sort the logs:

- **Filename**—Sort in alphabetical order.
- **Size (MB)**—Sort by file size.
- **Last Modified**—Sort by date modified.

5 To reverse the sorting order, click the column heading again.

**--End--**

## Opening a log file

You can open the log files in a number of applications, including Hilios Text Pad, and Microsoft WordPad. Do not use the Microsoft default viewer (Notepad) because the log file does not display in an easily readable format.

### Procedure Steps

**Step Action**

1 Browse to the folder where you have downloaded the log file.

2 Right-click the file, select **Open With, Choose Program**.

3 Select a file viewer application from the list. For example, WordPad.

4 Click **OK**.

Open the log file in the file viewer application you selected.

**--End--**

# Troubleshooting communication and network problems

The following modules describe the Mobile Communication 3100 (MC 3100) communication and network problem troubleshooting.

## Navigation

- "Performing a packet capture" (page 23)
- "Disabling Wireshark packet checksum verification" (page 24)

## Performing a packet capture

You can use the packet dump utility to capture all of the data transmitted and received on an interface of the MCG 3100 for a period of time (a capture session). After the capture session completes, you can save the packet dump as a *.cap* file.

---

**Attention:** Before performing a packet capture, confirm that the server contains *tcpdump*. If necessary, install *tcpdump* in */usr/sbin*, and change the permissions by logging on as root and using the command **`chmod u+s /usr/sbin/tcpdump`**

---

To open the *.cap* files for troubleshooting and analysis, you require the protocol analyzer called Wireshark (formerly Ethereal).

### Prerequisites

- You must be logged into the MC 3100 Web Console as administrator. For more information, see "Logging on to the MC 3100 Web Console as an administrator" (page 9).

### Procedure Steps

| Step | Action |
|---|---|
| 1 | Click the **Tools** tab. |
| 2 | Scroll to the Packet Capture section. |
| 3 | In the redundant configuration, select a gateway. |
| 4 | Select a network interface:<br>• eth0 (default)<br>• eth1<br>• any (Pseudo-device that captures on all interfaces)<br>• lo |
| 5 | Click **Capture**. |
| 6 | Wait for the packet capture to be performed, then click **Stop**. |
| 7 | Click **Save**. |
| 8 | Navigate to the folder where you want to save the ***dump.cap*** log file. |
| 9 | Click **Save**.<br>The ***dump.cap*** log file is saved. |

**--End--**

## Disabling Wireshark packet checksum verification

You need to disable Wireshark packet checksum verification before you can work with the captured packets.

**Attention:** When you view the packet captures from the MCG 3100 packet capture utility, the trace contains incorrect checksums. The incorrect checksums occur because the network interface on the MCG 3100 performs checksum off-loading, meaning that the network interface adds the checksum to the packets instead of the operating system TCP/IP stack. During the capture process, the host operating system sends the packets (being captured) directly to the capture interface without the addition of a checksum.

Wireshark performs checksum verification. Packet checksum errors can prevent TCP reassembly so you need to disable Wireshark checksum verification.

The following procedure provides the steps for Wireshark Version 0.99.6a (SVN Rev 22276). For more information, see the Wireshark documentation for your version of Wireshark or visit www.wireshark.org

### Procedure Steps

| Step | Action |
|---|---|
| **1** | From the Wireshark **Edit** menu, select **Preferences**. |
| **2** | In the left pane of the **Preferences** dialog box, expand **Protocols**. |
| **3** | In the left pane of the **Preferences** dialog box, select **TCP** and clear the **Validate the TCP checksum if possible** check box. |
| **4** | In the left pane of the **Preferences** dialog box, select **UDP** and clear the **Validate the UDP checksum if possible** check box. |
| **5** | Click **Apply**. |
| **6** | Click **OK**. |

**--End--**

# Troubleshooting data connections between MCC 3100 for Windows Mobile and Gateway

Use this procedure to identify where problems originate when experiencing data connection problems between Mobile Communication Gateway 3100 (MCG 3100) and Mobile Communication Client 3100 (MCC 3100) for Windows Mobile.

## Procedure Steps

| Step | Action |
|---|---|
| **1** | Ping the MCG 3100 from a PC to verify data connectivity of the PC to the MCG 3100. |
| **2** | If you cannot ping the MCG 3100, check the status of the MCG 3100. |
| **3** | Connect the mobile device to the computer with a USB cable. |
| **4** | Start Microsoft ActiveSync on the computer. |
| **5** | On the mobile device, select **Start, Internet Explorer**. |
| **6** | Browse to the Over the air download webpage to verify that the device can contact the MCG 3100 Web Server.<br>Depending on the type of security implemented on your system, enter one of the following:<br>**http://<IP Address or FQDN of MCG 3100>:8080/m**<br>**OR**<br>**https://<IP Address or FQDN of MCG 3100>:8443/m** |
| **7** | If the Over the air download page can be accessed, then you have a data connection. |
| **8** | If the Over the air download page cannot be accessed, try accessing www.nortel.com. |

**9** If you can access the Nortel web site, but cannot access the Over the air download site, check the status of the network supporting the connection between the MCG 3100 to MCC 3100.

**10** If you cannot access any web site, see your Windows Mobile support documentation to restore basic web browsing capability.

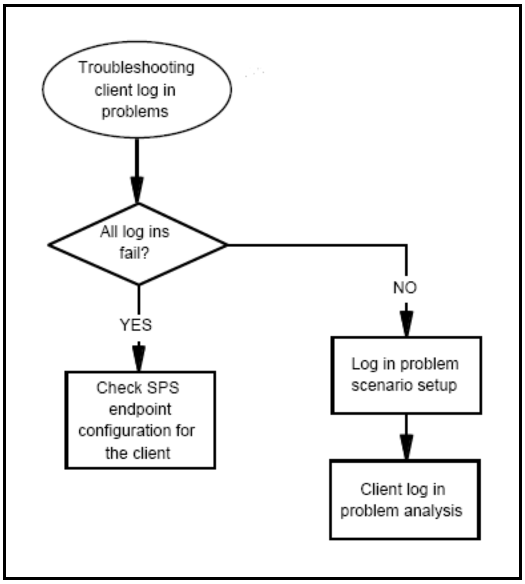
**--End--**

# Troubleshooting client log in problems

Use this section to troubleshoot problems with client log ins.

Figure 2 "Troubleshooting tree for client log in problems " (page 29) shows the troubleshooting tree for this problem.

**Figure 2**
**Troubleshooting tree for client log in problems**


Troubleshooting client log in problems
All log ins fail?
NO
YES
Check SPS endpoint configuration for the client
Log in problem scenario setup
Client log in problem analysis

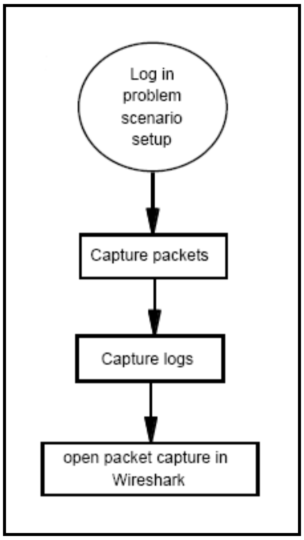
Using the above tree, you start the analysis using the following steps:

1. Do all clients have this problem? If so, check the SPS endpoint configuration.
2. If only a few clients have this problem, set up the scenario with one client as described in "Log in problem scenario setup" (page 30) to capture the information.
3. Analyze the information captured, as described in "Client log in problem analysis" (page 31).

## Log in problem scenario setup

This procedure captures the information required for analysis of the problem.

**Figure 3**
**Log in problem scenario setup tree**


Log in problem scenario setup
Capture packets
Capture logs
open packet capture in Wireshark

### Procedure Steps

| Step | Action |
|---|---|
| 1 | Configure a client to use HTTP instead of HTTPS.<br>Using HTTP means the packets are not encrypted, and removes the use of certificates. |
| 2 | Reproduce the problem. |
| 3 | If the problem does not reproduce, you need to check the certificates. |
| 4 | If the problem reproduces, start the packet capture. |
| 5 | Reproduce the problem. |
| 6 | Stop the packet capture.<br>**Attention:** Keep the packet traces as small as possible, especially in a busy system. |
| 7 | Capture the logs.<br>You capture the logs now so that you have complete information, in case you need to involve Nortel. |

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

**Attention:** In the filter, || means logical or. The | character on most PC keyboards is Shift+\

**--End--**

## Client log in problem analysis

Use this process to analyze the data captured.

**Figure 4**
**Client log in problem analysis (part 1)**

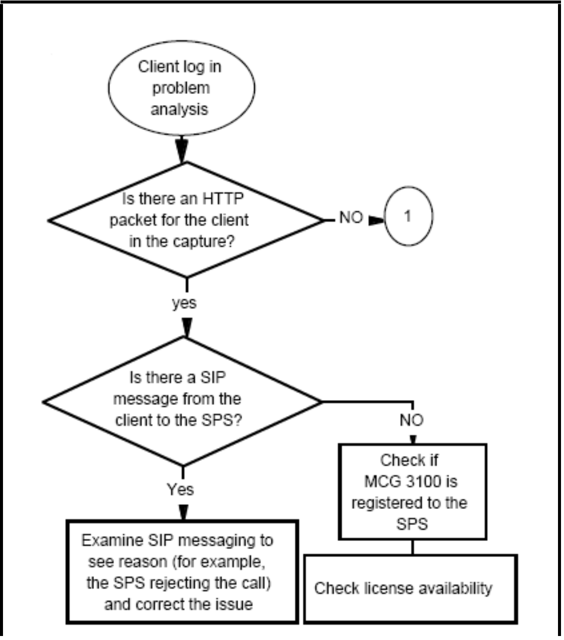
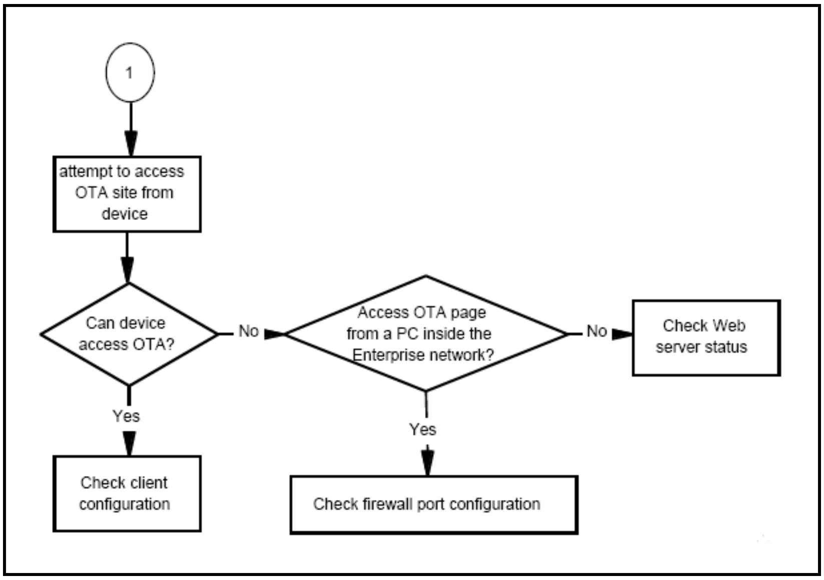

Client log in problem analysis
Is there an HTTP packet for the client in the capture?
NO
1
yes
Is there a SIP message from the client to the SPS?
NO
Check if MCG 3100 is registered to the SPS
Yes
Examine SIP messaging to see reason (for example, the SPS rejecting the call) and correct the issue
Check license availability

**Figure 5**
**Client log in problem analysis (part 2)**


1
attempt to access OTA site from device
Can device access OTA?
No
Access OTA page from a PC inside the Enterprise network?
No
Check Web server status
Yes
Check client configuration
Yes
Check firewall port configuration

## Prerequisites

- "Log in problem scenario setup" (page 30)

## Procedure Steps

**Step** **Action**

1 In the packet capture, look for the HTTP POST request.

You can see the user name and other details in the XML body of the message.

2 If the HTTP packet for the client does not exist, go to step 6.

3 In the packet capture, using the URL fields of the HTTP POST, look for the `SIP` response for the log in attempt to the SPS.

4 If the log in succeeded, the `SIP` message contains the reason that the log in is rejected. Correct the associated issue.

5 If the log in failed,

- Check that the MCG 3100 is registered to the SPS.
- Check the availability of licences on the MCG 3100.

6 Attempt to access the Over the Air (OTA) download site from the device browser.

7 If the OTA page is accessible, then it is likely that the client is not configured correctly. Check the client configuration parameters.

**8** If the OTA page is not accessible, attempt to access the OTA page from a PC inside the Enterprise network.

**9** If the OTA page is accessible, check the firewall port configuration.

**10** If the OTA page is not accessible, check the MCG 3100 web server status and restart the processes if necessary.

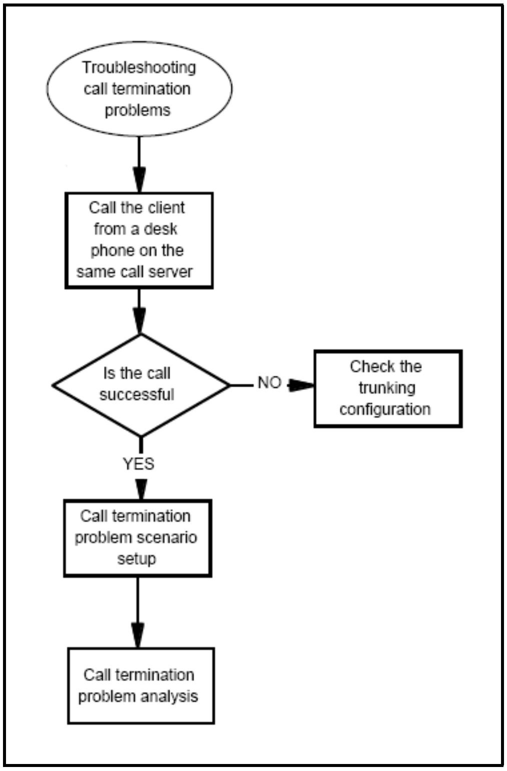
**--End--**

# Troubleshooting call termination problems

Use this section to troubleshoot problems with call termination.

Figure 6 " Troubleshooting tree for call termination problem" (page 35) shows the troubleshooting tree for this problem.

**Figure 6**
**Troubleshooting tree for call termination problem**


Troubleshooting call termination problems
Call the client from a desk phone on the same call server
Is the call successful
NO
Check the trunking configuration
YES
Call termination problem scenario setup
Call termination problem analysis

Using the above tree, you start the analysis using the following steps:

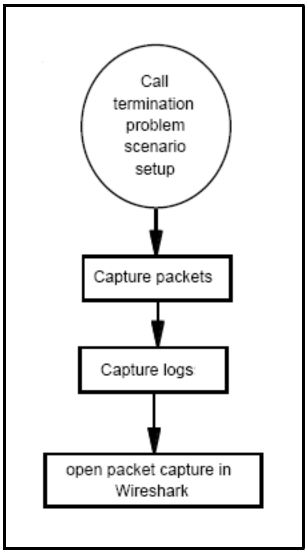
1. Using a desk telephone that is configured on the same call server as the UEXT of the client, make a call to the client.
2. If the call can be made, check the trunking configuration.

3. If the call cannot be made, set up the scenario with one client as described in "Call termination problem scenario setup" (page 36) to capture the information.
4. Analyze the information captured, as described in "Call termination problem analysis" (page 37).

## Call termination problem scenario setup

This procedure captures the information required for analysis of the problem.

**Figure 7**
**Call termination scenario setup tree**


Call termination problem scenario setup
Capture packets
Capture logs
open packet capture in Wireshark

### Procedure Steps

| Step | Action |
|---|---|
| **1** | Configure a client to use HTTP instead of HTTPS.<br>Using HTTP means the packets are not encrypted, and removes the use of certificates. |
| **2** | Reproduce the problem. |
| **3** | If the problem does not reproduce, you need to check the certificates. |
| **4** | If the problem reproduces, start the packet capture. |
| **5** | Reproduce the problem. |
| **6** | Stop the packet capture. |

**Attention:** Keep the packet traces as small as possible, especially in a busy system.

---

7 Capture the logs.

You capture the logs now so that you have complete information, in case you need to involve Nortel.

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

---

**Attention:** In the filter, || means logical or. The | character on most PC keyboards is Shift+\

---

**--End--**

---

## Call termination problem analysis

Use this process to analyze the data captured.

**Figure 8**
**Call termination problem analysis (part 1)**

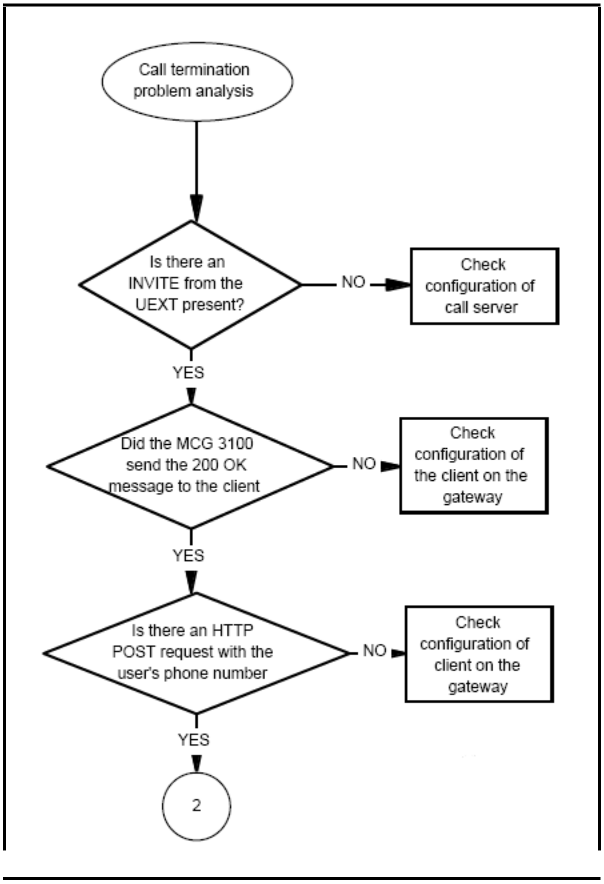
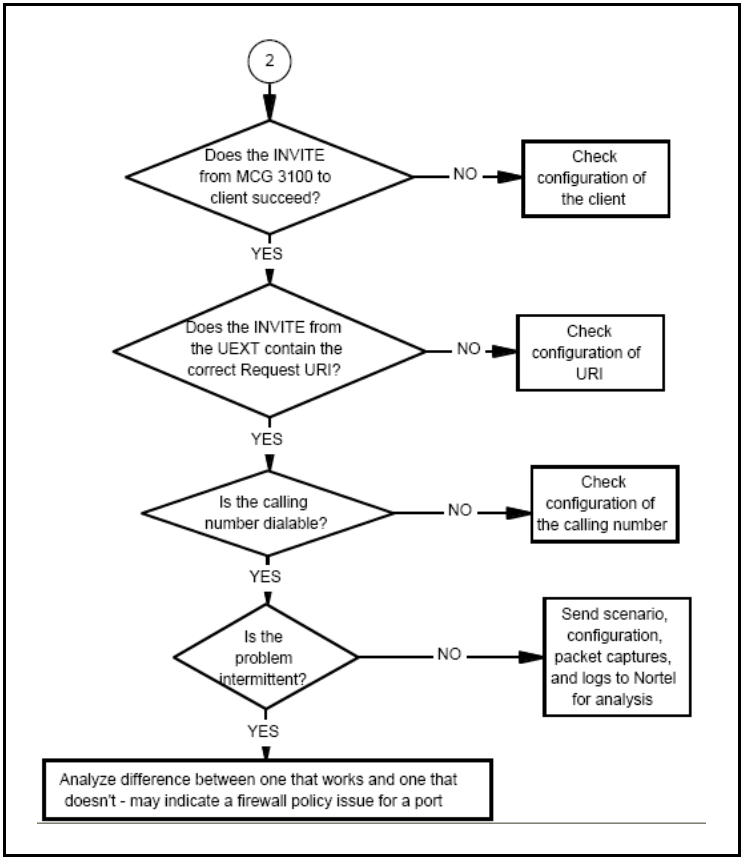

Call termination problem analysis
Is there an INVITE from the UEXT present?
NO
Check configuration of call server
YES
Did the MCG 3100 send the 200 OK message to the client
NO
Check configuration of the client on the gateway
YES
Is there an HTTP POST request with the user's phone number
NO
Check configuration of client on the gateway
YES
2

**Figure 9**
**Call termination problem analysis (part 2)**


2
Does the INVITE from MCG 3100 to client succeed?
NO
Check configuration of the client
YES
Does the INVITE from the UEXT contain the correct Request URI?
NO
Check configuration of URI
YES
Is the calling number dialable?
NO
Check configuration of the calling number
YES
Is the problem intermittent?
NO
Send scenario, configuration, packet captures, and logs to Nortel for analysis
YES
Analyze difference between one that works and one that doesn't - may indicate a firewall policy issue for a port

## Prerequisites

- "Call termination problem scenario setup" (page 36)

## Procedure Steps

| Step | Action |
|---|---|
| 1 | In the packet capture, look for the `INVITE` message from the UEXT. |
| 2 | If the `INVITE` message is not present, check the configuration of the device on the call server. |
| 3 | Look for the `180 ringing` message from the call server to the gateway and determine if the gateway sends the `200 OK` message to the client. |
| 4 | If the `200 OK` message does not appear, check the configuration of the client on the gateway. |

**5** Look for an HTTP POST request with the user’s phone number that the MCC 3100 user requested to answer the call.

**6** If an HTTP POST request is not available with the user’s phone number, check the configuration of the client on the gateway.

**7** In the packet capture, look for the `INVITE` message from the MCG 3100 to the answer destination.

**8** If the `INVITE` message is not present, check the configuration of the client.

**9** In the packet capture, look for the `INVITE` message from the UEXT contains the correct Request URI.

**10** If the `INVITE` message from the UEXT does not contain the correct Request URI, check the configuration of the URI.

**11** Look for a valid dialable number that the user is trying to answer.

**12** If the calling number is not valid, check the configuration of the calling number.

**13** If the problem is intermittent, look for the difference between a trace that works and one that does not. It may indicate a Firewall policy issue for a port.

**14** If the problem is not intermittent, send the scenario, configuration, packet captures, and logs to Nortel for analysis.

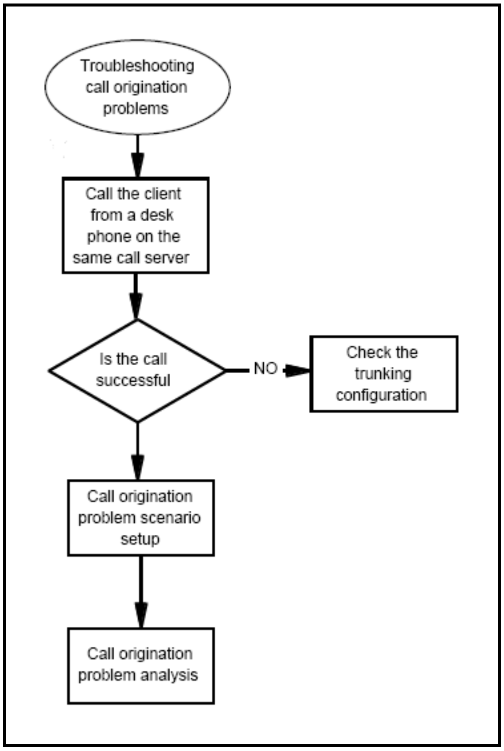
**--End--**

# Troubleshooting call origination problems

Use this section to troubleshoot problems with call origination.

Figure 10 " Troubleshooting tree for call origination problems" (page 41) shows the troubleshooting tree for this problem.

**Figure 10**
**Troubleshooting tree for call origination problems**


Troubleshooting call origination problems
Call the client from a desk phone on the same call server
Is the call successful
NO
Check the trunking configuration
Call origination problem scenario setup
Call origination problem analysis

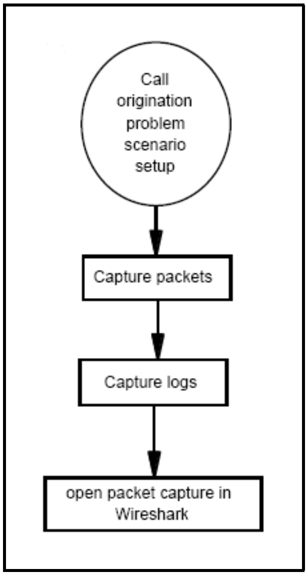
Using the above tree, you start the analysis using the following steps:

1. Do all clients share the call origination problem? If so, check the trunking configuration.
2. If only a few clients have problems with call origination, set up the scenario with one client as described in "Call origination problem scenario setup" (page 42) to capture the information.
3. Analyze the information captured, as described in "Call origination problem analysis" (page 43).

## Call origination problem scenario setup

This procedure captures the information required for analysis of the problem.

**Figure 11**
**Call origination scenario setup tree**


Call origination problem scenario setup
Capture packets
Capture logs
open packet capture in Wireshark

### Procedure Steps

| Step | Action |
|---|---|
| **1** | Configure a client to use HTTP instead of HTTPS.<br>Using HTTP means the packets are not encrypted, and removes the use of certificates. |
| **2** | Reproduce the problem. |
| **3** | If the problem does not reproduce, you need to check the certificates. |
| **4** | If the problem reproduces, start the packet capture. |
| **5** | Reproduce the problem. |
| **6** | Stop the packet capture. |

**Attention:** Keep the packet traces as small as possible, especially in a busy system.

**7** Capture the logs.

You capture the logs now so that you have complete information, in case you need to involve Nortel.

**8** Open the packet capture in Wireshark.

**9** In the filter field, enter **HTTP || SIP**

**Attention:** In the filter, || means logical or. The | character on most PC keyboards is Shift+\

**--End--**

## Call origination problem analysis

Use this process to analyze the data captured.

**Figure 12**
**Call origination problem analysis (part 1)**

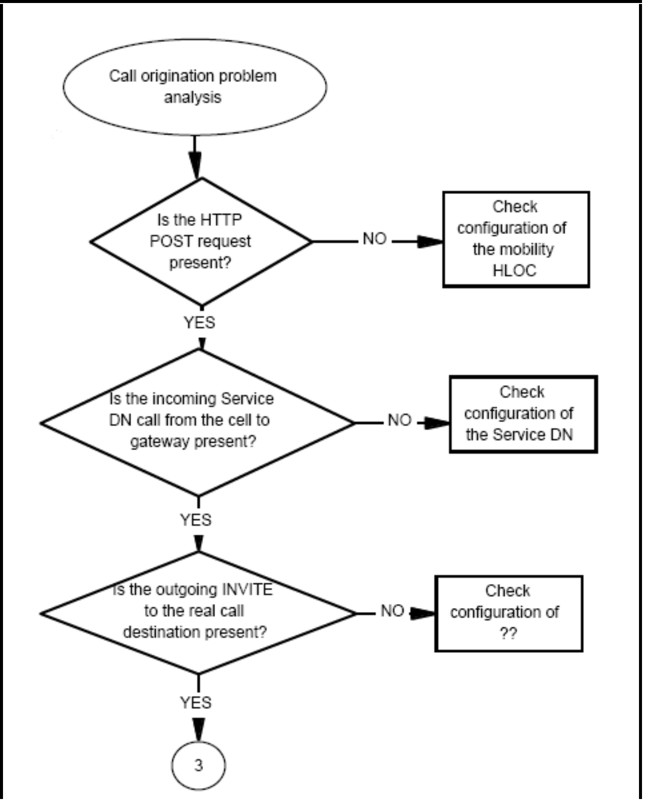

Call origination problem analysis
Is the HTTP POST request present?
NO
Check configuration of the mobility HLOC
YES
Is the incoming Service DN call from the cell to gateway present?
NO
Check configuration of the Service DN
YES
Is the outgoing INVITE to the real call destination present?
NO
Check configuration of ??
YES
3

**Figure 13**
**Call origination problem analysis (part 2)**

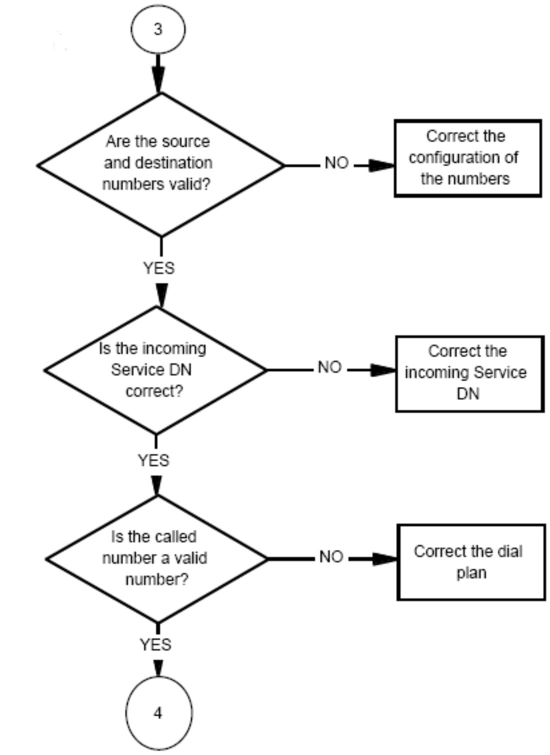
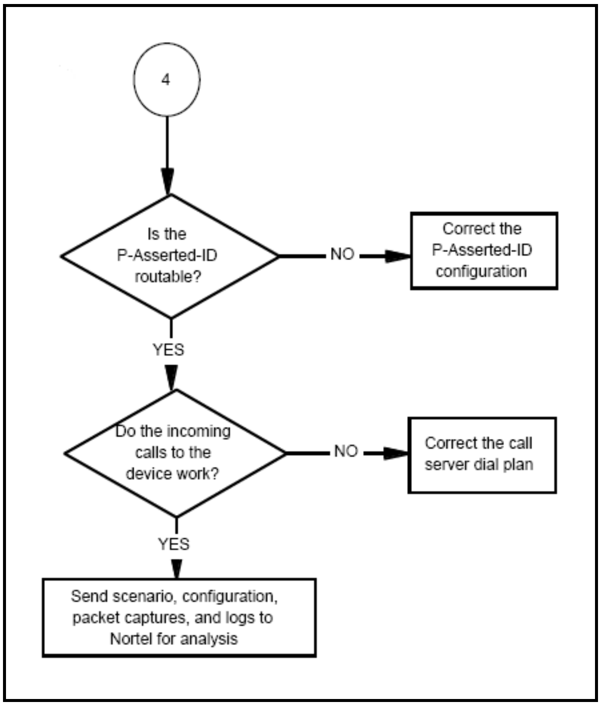

3
Are the source and destination numbers valid?
NO
Correct the configuration of the numbers
YES
Is the incoming Service DN correct?
NO
Correct the incoming Service DN
YES
Is the called number a valid number?
NO
Correct the dial plan
YES
4

**Figure 14**
**Call origination problem analysis (part 3)**


4
Is the P-Asserted-ID routable?
NO
Correct the P-Asserted-ID configuration
YES
Do the incoming calls to the device work?
NO
Correct the call server dial plan
YES
Send scenario, configuration, packet captures, and logs to Nortel for analysis

## Prerequisites

- "Call origination problem scenario setup" (page 42)

## Procedure Steps

| Step | Action |
|---|---|
| 1 | In the packet capture, look for the HTTP POST request from the client that contains the call attempt request. |
| 2 | If the HTTP POST request is not present, check the configuration of the mobility HLOC. |
| 3 | Look for the incoming service DN call from the cell phone to the MCG 3100. |
| 4 | If the incoming service DN call is not present, check configuration of the service DN. |
| 5 | In the packet capture, look for the outgoing `INVITE` message to the real call destination. |
| 6 | If the outgoing `INVITE` message is not present, check the configuration of <something>. |

**Attention:** AUTHOR: don’t know what configuration to check

7 In the packet capture, look for valid source and destination numbers.

8 If the source and destination numbers are not valid, correct the configuration of the numbers.

9 In the packet capture, look for a valid incoming service DN call.

10 If the incoming Service DN call is not valid, correct the incoming Service DN.

11 Look for valid called number in the current dial plan.

12 If the called number is not a valid number, correct the dial plan.

13 In the packet capture, look for the P-Asserted-ID message for the call attempt from the MCG 3100.

14 If the P-Asserted-ID is not routable, correct the P-Asserted-ID configuration.

15 Try making a call to the device directly.

16 If you can call the device directly, send the scenario, configuration, packet captures, and logs to Nortel for analysis.

17 If the incoming calls to the device does not work, correct the call server dial plan.

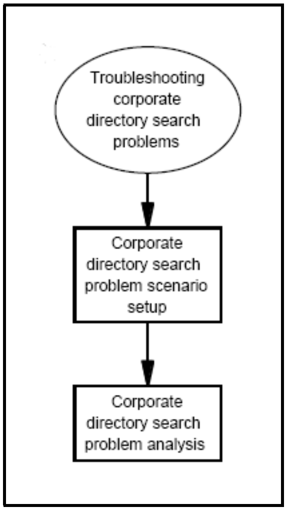
**--End--**

# Troubleshooting corporate directory search problems

Use this section to troubleshoot problems with corporate directory search.

Figure 15 " Troubleshooting tree for corporate directory search problems" (page 49) shows the troubleshooting tree for this problem.

**Figure 15**
**Troubleshooting tree for corporate directory search problems**


Troubleshooting corporate directory search problems
Corporate directory search problem scenario setup
Corporate directory search problem analysis

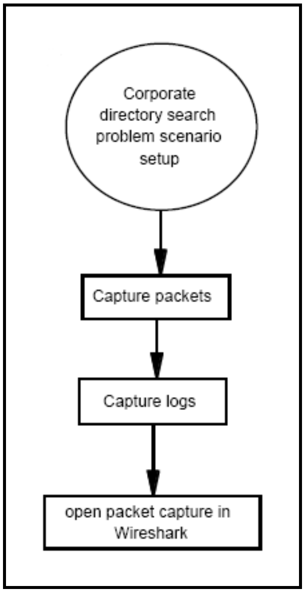
Using the above tree, you start the analysis using the following steps:

1. Do all clients have problem with the corporate directory search? If so, set up the scenario with one client as described in "Corporate directory search problem scenario setup" (page 49) to capture the information.
2. Analyze the information captured, as described in "Corporate directory search problem analysis" (page 51).

## Corporate directory search problem scenario setup

This procedure captures the information required for analysis of the problem.

**Figure 16**
**Corporate Directory search scenario setup tree**


Corporate directory search problem scenario setup
Capture packets
Capture logs
open packet capture in Wireshark

## Procedure Steps

| Step | Action |
|---|---|
| 1 | Configure a client to use HTTP instead of HTTPS.<br>Using HTTP means the packets are not encrypted, and removes the use of certificates. |
| 2 | Reproduce the problem. |
| 3 | If the problem does not reproduce, you need to check the certificates. |
| 4 | If the problem reproduces, start the packet capture. |
| 5 | Reproduce the problem. |
| 6 | Stop the packet capture. |

**Attention:** Keep the packet traces as small as possible, especially in a busy system.

| Step | Action |
|---|---|
| 7 | Capture the logs.<br>You capture the logs now so that you have complete information, in case you need to involve Nortel. |
| 8 | Open the packet capture in Wireshark. |
| 9 | In the filter field, enter **HTTP \|\| SIP** |

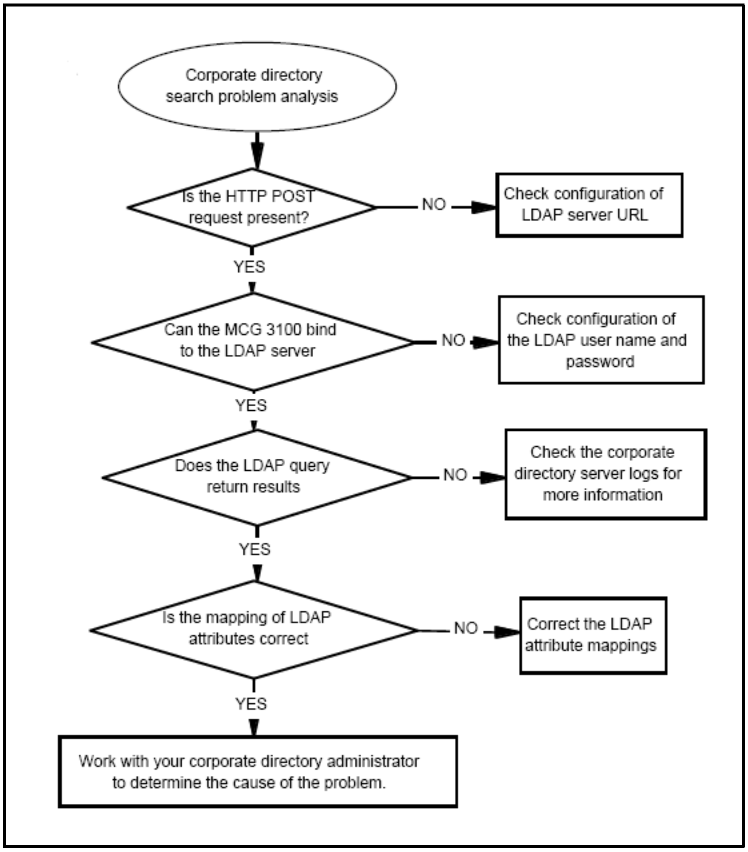
**Attention:** In the filter, || means logical or. The | character on most PC keyboards is Shift+\

**--End--**

## Corporate directory search problem analysis

Use this process to analyze the data captured.

**Figure 17**
**Corporate directory search problem analysis**


Corporate directory search problem analysis
Is the HTTP POST request present?
NO
Check configuration of LDAP server URL
YES
Can the MCG 3100 bind to the LDAP server
NO
Check configuration of the LDAP user name and password
YES
Does the LDAP query return results
NO
Check the corporate directory server logs for more information
YES
Is the mapping of LDAP attributes correct
NO
Correct the LDAP attribute mappings
YES
Work with your corporate directory administrator to determine the cause of the problem.

### Procedure Steps

| Step | Action |
|---|---|
| 1 | In the packet capture, look for the HTTP POST request from the client that contains the directory search request. |
| 2 | If the HTTP POST request is not present, check the configuration of LDAP server URL. |

3 Check for the MCG 3100 bind with the LDAP server.

4 If the MCG 3100 does not bind with the LDAP server, check the configuration of LDAP username and password.

5 In the packet capture, look for the LDAP query request results.

6 If the LDAP query request does not return results, check the corporate directory server logs for more information.

7 Look for the mapping of the phone numbers to LDAP attributes on the MCG 3100.

8 If the mapping of the phone numbers to LDAP attributes is correct, work with your corporate directory administrator to determine the cause of the problem.

9 If the mapping of the phone numbers to LDAP attributes is not correct on the MCG 3100, check the LDAP attribute mappings.

**--End--**

Nortel Mobile Communication 3100

# Nortel Mobile Communication 3100 Troubleshooting

Printed in Canada
Release: 3.0
Publication: NN42030-700
Document status: Standard
Document revision: 01.03
Document release date: 9 June 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

LEGAL NOTICE

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel's express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.