

CSTA Server (Phase III)

OPERATIONAL DIRECTIONS



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2018, Mitel Networks Corporation

All rights reserved

1

GENERAL

The Computer Supported Telecommunications Applications (CSTA) is an application protocol that allows the interfacing of a computer domain with a telephony domain. It supports applications or services normally provided by one domain to be available to the other domain that normally does not support such application without major enhancement or redesign.

The purpose of this functionality is to support a Computer Telephony Integration (CTI) protocol, for example, ECMA-CSTA, between a telephony domain (MX-ONE Service Node and the protocol converter) and a computing domain (host computer with CTI application) or a Web Server serving the Web Service Clients. The CSTA application in the MX-ONE Service Node functions as a server to support the CSTA clients.

The CSTA Application Session Authentication services (according to the ECMA-354 Standard, with some proprietary additions) are also supported, but is optional.

The CSTA Application supports the Web Service clients through a Web Server on a port different from the one used for CTI clients.

The rest of the document will refer to the CSTA Application in MX-ONE as CSTA Server.

The main type of application for the CSTA implementation is call centers, where agents handling incoming calls can get synchronized screen updates with the telephone calls. When a call arrives at an agent position, a message is sent from the exchange to the computer, informing the computer of the event. The message will contain information about the call, like:

- Which agent received the call
- Who is calling (A-number)
- What number was dialed (could be an internal group hunting group number)

The computer will typically take this information and do a data base search to update the computer screen of the agent with the caller's profile.

Normally, the agent would handle the telephony traffic from the computer terminal, causing CSTA requests to be sent from the computer to the exchange. It is possible for the agents to wear head-sets, and use the computer terminal as a telephone.

Other types of applications could be outbound call centers, like tele-marketing or debt collection.

The CSTA Server in the MX-ONE supports the CTI application or the Web Service clients via the following functions:

- Generating CSTA events for monitored objects, that is, the status of the object or the queue status of the object.
- Performing telephony functions that are requested from the CTI application, for example, to make calls.

A monitored object can be:

- IP/SIP extension (both ODN and EDN for SIP)
- remote extension
- cordless DECT extension
- virtual extension (generic extension without logged on terminal)
- digital extension (both ODN and ADN)

- analog extension
- CAS extension
- CTI/ACD group
- Hunt group (including cascade ring group)

The general CSTA configuration is shown in Figure 1.

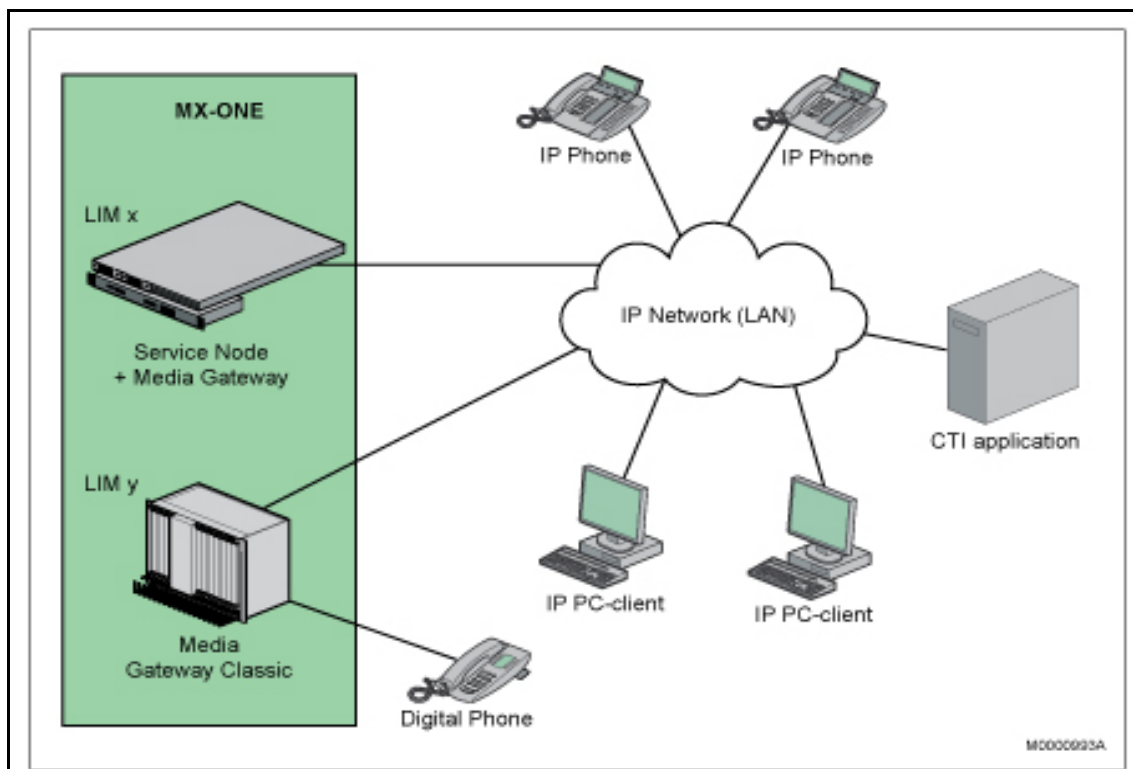


Figure 1: General configuration. The CSTA Server are installed on the LIMs.

The CTI clients are shown in Figure 2.

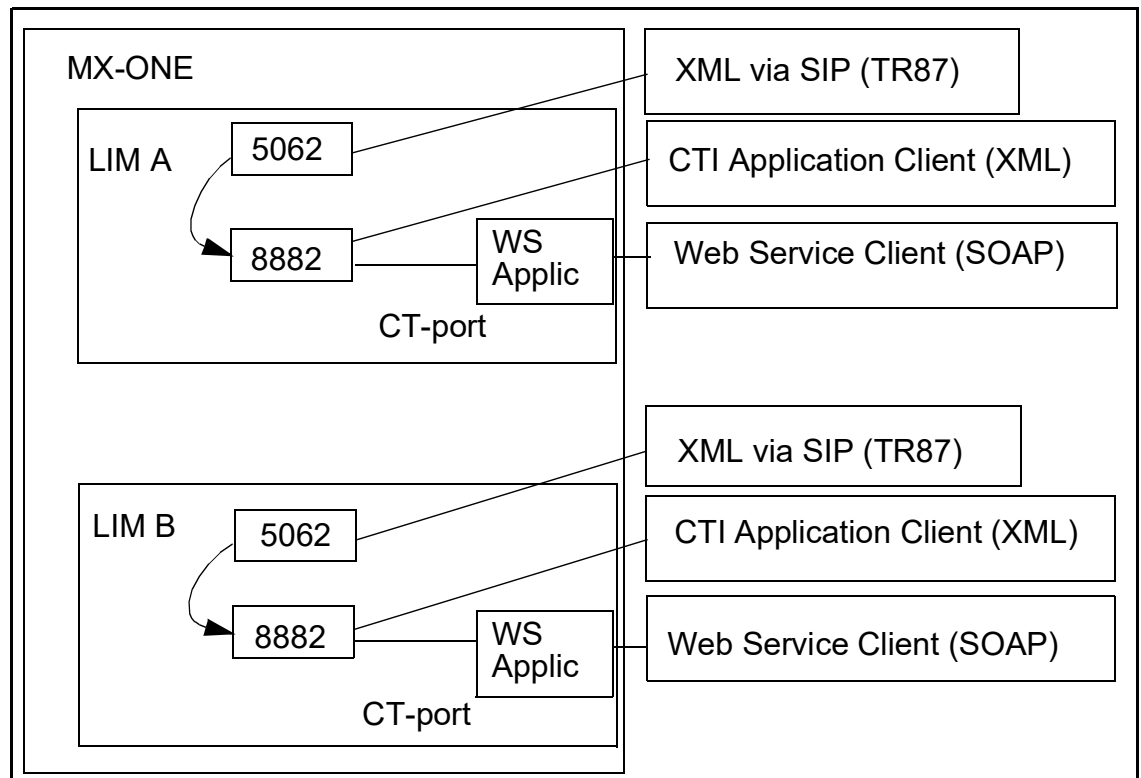


Figure 2: An example CSTA Server configuration. Note that the port numbers are default values, but any free port number could be used.

As can be observed, the CTI client and Web Services client are supported on different ports (5062 vs 8882). XML and also XML via SIP use the same port (8882) as the web services application.

CTI Application client (XML) can also use TLS (Transport Layer Security) to secure the communication between the server and the client. TLS default port with TLS is 8883 for XML.

2 PREREQUISITES

CTI Application Client (XML) that wants to use TLS must have a server with a valid certificate to initiate the port (to enable or to initiate the CSTA server port, this must have the Service Node server with a valid certificate). This is handled with the command *mxone certificate*.

CTI Application Client (XML) running TLS must have a server with a valid certificate to initiate the port. This is handled with the command `mxone certificate`.

Web Service Client (SOAP) must have a Linux user account(s) to be used for the client application authentication at login must have been created before the CSTA Server Application can be initiated.

For security reasons the account(s) should have a low authority level, and a password that is not the default one.

Decide if Application Session Authentication shall and can be used (for security reasons, and if the application can support it), i.e. a registration and verification of the CTI Application, and possibly a limitation of the session duration.

3 AIDS

I/O terminal.

4 REFERENCES

CSTA Phase 3 Standards.

5 PROCEDURE

The following procedure is recommended for TR87 and CTI Application Client (XML):

- (Skip this step if TLS is not used). Verify that a valid certificate exists, or install/create a certificate with the command *mxone_certificate*. Preferably on all servers.
- Initiate the CSTA Server with the command *csta*. Select preferred server type (TR87 or XML).
- If Application Session Authentication shall be used, initiate the CSTA Session Authentication settings (criteria for authentication) with the command *csta_authentication*. (Only valid for TR87 and XML).

The following procedure is recommended for Web Server Application (SOAP):

- Initiate the Linux user account and password to be used for authentication at login.
- Initiate the CSTA Server with the command *csta*. Select preferred server type (XML). Note that WS/SOAP also transports the XML protocol, so do not select TR87, but XML.

6 EXECUTION

6.1 INITIATE USER ACCOUNT (ONLY FOR WEB SERVICE)

General

The CSTA Web Service application needs a Linux user account and password to be authenticated at login. See the concerned Linux command descriptions for details.

Prerequisites

-

Execution (example)

1. Initiate the user account with low authority level by entering the command:
`useradd -d /tmp -G nobody -s /bin/true csta_user`
2. Initiate a password for the user account by entering the command:
`passwd csta_user`, and enter the new password when prompted.
3. Verify the result by keying appropriate commands.

6.2 INITIATE CSTA SERVER FOR A TELEPHONY DOMAIN

General

-

Prerequisites

-

Execution

1. Initiate the CSTA Server by keying the command `csta -i`.
2. Verify the result by keying the command `csta -p`.

6.3 REMOVE CSTA SERVER FROM A TELEPHONY DOMAIN

1. Remove the CSTA Server by keying the command `csta -e`.
2. Verify the result by keying the command `csta -p`.

6.4 PRINT CSTA SERVER RELATED INFORMATION

Print data about the CSTA Server status or CSTA Server monitored device information by keying the command `csta -p`.

6.5

INITIATE CSTA SERVER FOR AN MS LYNC APPLICATION

General

The CSTA interface is intended to be used for connecting to MS Lync Server 2013.

Note: A dedicated SIP route, which was required in earlier releases, is no longer required.

Prerequisites

The customer wants to use the MS Lync Server 2013 remote call control function for control of SIP extensions in MX-ONE, using Lync clients.

Execution

1. Initiate the CSTA Server by keying the command *csta -i* in the ordinary way. The only specific settings are that port 5062* shall be used, and protocol TR87_uaCSTA (xml transported via SIP) shall be selected.
2. Verify the result by keying the command *csta -p*.

Note: *) Port 5062 is the default, but it can be changed.

6.6

INITIATE CSTA APPLICATION SESSION AUTHENTICATION SETTINGS

General

The CSTA Application Session Authentication services register and verify the application when the session is established. This functionality provides better security, but is optional, i.e. it can be turned off or on. For older application versions, which do not support the Authentication services, the functions would have to be off.

Prerequisites

CSTA Server must have been initiated with command *csta -i*.

Optional function, only valid for the XML/TR87 protocols.

The used CTI applications must support the authentication services. If older versions of the applications are used, they may not support the authentication services.

Execution

1. Initiate the CSTA Authentication settings by keying the command *csta_authentication -i*.

Note: The session authentication services can be set to be mandatory in the *csta -i* command.

2. Verify the result by keying the command *csta_authentication -p*.

6.7

CHANGE CSTA APPLICATION SESSION AUTHENTICATION SETTINGS

1. Change the CSTA Authentication settings by keying the command *csta_authentication -c*.
2. Verify the result by keying the command *csta_authentication -p*.

6.8 REMOVE CSTAAPPLICATION SESSION AUTHENTICATION SETTINGS

1. Remove the CSTA Authentication services by keying the command *csta_authentication -e*.
2. Verify the result by keying the command *csta_authentication -p*.

6.9 PRINT CSTAAPPLICATION SESSION AUTHENTICATION SETTINGS

Print data about the CSTA Server status or CSTA Server monitored device information by keying the command *csta -p*.

7 TERMINATION

If exchange data have been altered a dump to backup media must be performed.