Troubleshoot Most Common Issues for Business to Business Calls Through Expressway

Contents

Introduction

This document describes the most common issues in Business to Business (B2B) deployment. How to troubleshoot B2B calls through Expressways.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Expressway-C (Exp-C)
- Expressway-E
- Cisco Unified Call Manager (CUCM)
- Telepresence Video Communication Server-C (VCS-C)

Components Used

The information in this document is based on these software and hardware versions:

- Expressway C and E X8.1.1 or later

- Unified Communications Manager (CUCM) 10.0 or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Common Issues

1. Error "//SIP/SIPTcp/wait_SdlReadRsp: Ignoring large message. Only allow up to 5000 bytes. Resetting connection."

Calls from TelePresence endpoints registered to VCS, inbound on a Session Initiation Protocol (SIP) trunk to CUCM, fail with "//SIP/SIPTcp/wait_SdlReadRsp: Ignoring large message. Only allow up to 5000 bytes. Resetting connection."

Call routing configuration in the Expressway-C/VCS-C is correct and the call is sent to CUCM. SIP Invite message is sent to CUCM, but in the SDL logs there's no SIP messages. This error can be seen in the SDL logs:

"|AppInfo |SIPTcp - Ignoring large message from xxx.xxx.xxx.xxx:[27469]. Only allow up to 5000 bytes. Resetting connection."

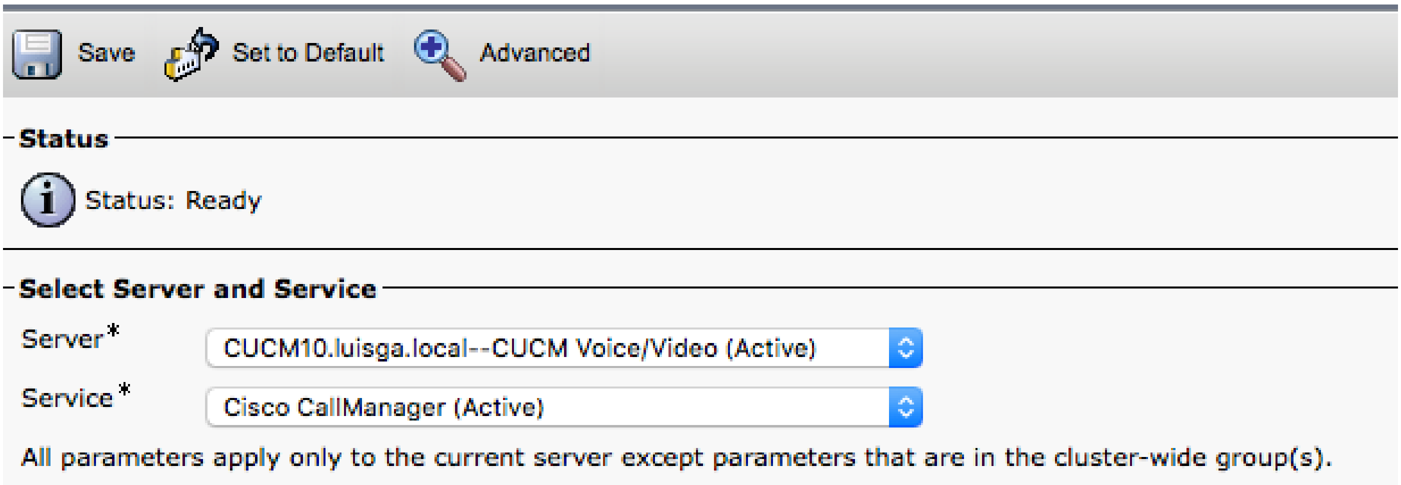
In CUCM 8.6 and below the default value for SIP Max Incoming Message Size was 5000, after CUCM 9.X changed to 11000. However, upgrade from 8 or below to version 9 or 10 will keep the default value in the previous version of software (5000).

Solution

This problem is related to bug [CSCts00642]

Increase CUCM Advanced Service Parameter **SIP Max Incoming Message Size** from the default value of 5000 to a size adequate for these types of calls. 11000 appears to be a good value for the majority of anticipated customer scenarios.

From **CUCM Administration Page,** navigate **to Service Parameters** and **select** your **CUCM server and the CallManager Service**:



Select on the **Advanced** option and search for **SIP Max Incoming Message Size**:

SIP Max Incoming Message Size *	11000	11000
SIP Max Incoming Message Headers *	100	100

2. Media Streams Stop If Another Call Server Transfers the Call.

This can happen in Mobile and Remote Access (MRA) and B2B calls.

It can cause no sound one way or a buzzing noise (same noise when you try to play a capture with encrypted audio) after the call is transferred. This happens because a crypto suite is selected on call setup that isn't supported by the endpoint it is transfered to.

You can compare the SIP negotiation before and after the transfer of the call. In the first negotiation in the VCS or CUCM logs you can see crypto lines in the 200 OK message from VCS:

```
m=audio 54582 RTP/SAVP 9 96 97 0 8 18 101
a=rtpmap:9 G722/8000
a=rtpmap:96 G7221/16000
a=fmtp:96 bitrate=32000
a=rtpmap:97 G7221/16000
a=fmtp:97 bitrate=24000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:ckXijkT3CcVY+xlOf3ozX/TjHPz05OzEdY49rAHA|2^48
a=sendrecv
a=rtcp:54583 IN IP4 10.1.201.7
m=video 54658 RTP/SAVP 96 97
b=TIAS:4000000
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e01e;max-fs=1621;packetization-mode=1;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42e01e;max-fs=1621;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:S8BJvGB/2l6F7XP8izXxId443Xd9f27oUI/4gxSt|2^48
```

Crypto lines are accepted in the first call, but in the second call you see that the ACK message removes the crypto lines:

```
m=audio 24826 RTP/AVP 0
c=IN IP4 10.1.231.30
a=ptime:20
a=rtpmap:0 PCMU/8000
m=video 0 RTP/AVP 126
c=IN IP4 10.1.98.80
b=TIAS:448000
a=label:11
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3601;max-rcmd-nalu-
size=32000;level-asymmetry-allowed=1
a=content:main
```

VCS tries to use the crypto lines negotiated at the beginning, even if the endpoint that the call is transferred to doesn't support encryption.

Solution

This problem is related to bug [CSCuv11790]

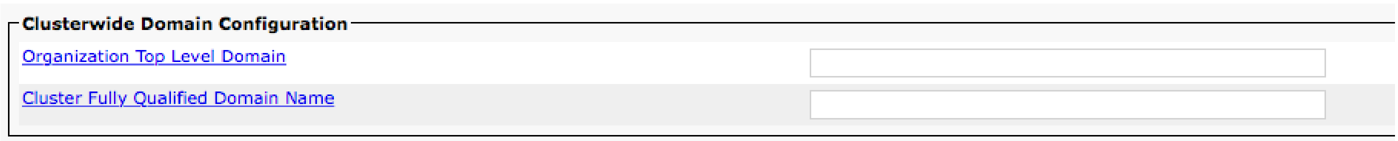
Upgrade VCS/Expressway to x8.6.1 in order to fix this problem.

3. Top Level Domain Not Configured in CUCM.

If the Top Level domain Enterprise Parameter is not set, it causes CUCM to route inbound calls to its own domain and the SIP Route Patterns is used. This could cause a loop because the call is most likely sent back to Exp-C, or it can also fail with a "404 Not Found error".

Solution

From **CUCM Administration page, navigate to System > Enterprise Parameters** to change this setting



4. CUCM Certificate Must Have the Client Authentication Attribute Applied.

When a secure connection is set between the Exp-C and CUCM (TLS Verify On), SSL handshake is started by a specific call sever which depends in the direction of the call. This means that both servers must have client and server authentication in their certificates. This error is seen in the VCS/Expressway logs if the attribute is not present:

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,060"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connecting"
Line 239: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,071"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Established"
Line 249: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,081"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Closed" Reason="no certificate returned"
```

Solution

Details about how to configure a template with both web client and server attributes can be found in the VCS certificate guide

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf

5. Interworking Issues.

VCS/Expressway version X8.6.x had some problems with the Interworking process.

Bugs related to the issue:

Defect [CSCuw85626]() can be detected if you check the diagnostic logs from VCS/Expressway for video m lines being rejected:

This error message is shown when the media lines in the TCS portion of the H323 flow is negotiated.

medialine index: 1

rejected: true, direction: SDP_MEDIA_DIR_SENDRECV

type: video / SDP_MF_AU_VID

Defect [CSCuw85715]() is similar but in this case, the VCS/Expressway logs will specify that the cause is dataTypeNotSupported:

```
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="INFO": Action="Sent" Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Detail="Sending H.245 OpenLogicalChannelRejResponse "
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXX tvcs: UTCTime="2015-10-29 05:49:00,197"
Module="network.h323" Level="DEBUG": Dst-ip="XXXXXXXXXXXXXXXX" Dst-port="49162"
Sending H.245 PDU:
value MultimediaSystemControlMessage ::= response : openLogicalChannelReject :
{
forwardLogicalChannelNumber 3,
cause dataTypeNotSupported : NULL
}
```

Solution

Upgrade to X8.7 or later.

6. ACK Message Received from CUCM Is Not Sent to VCS-E/Expressway-E.

This is usually seen when the configured traversal zone does not point to the correct IP address of the VCS Expressway / Expressway-E.

In single NIC deployments (on the Expressway/Edge), the traversal client zone on the Control/Core needs to point to the public IP address of the traversal server.

In dual NIC deployments, the traversal client needs to point to the internal IP address (internal NIC is usually LAN1 but can be LAN2) of the traversal server. Keep in mind this is the internal IP address of the internal LAN.

Solution

Please refer to Appendix 4 of the [Cisco VCS Expressway and VCS Control - Basic Configuration]() for more information and a diagram of the different network deployments.

7. CUCM drops TCP session on inbound calls

When calls are forward from VCS control / Expressway Core, CUCM might reject this by drop of the TCP session.

This might happen when the port between the neighbor zone and the sip trunk security profile does not match or is configured to be 5060/5061.

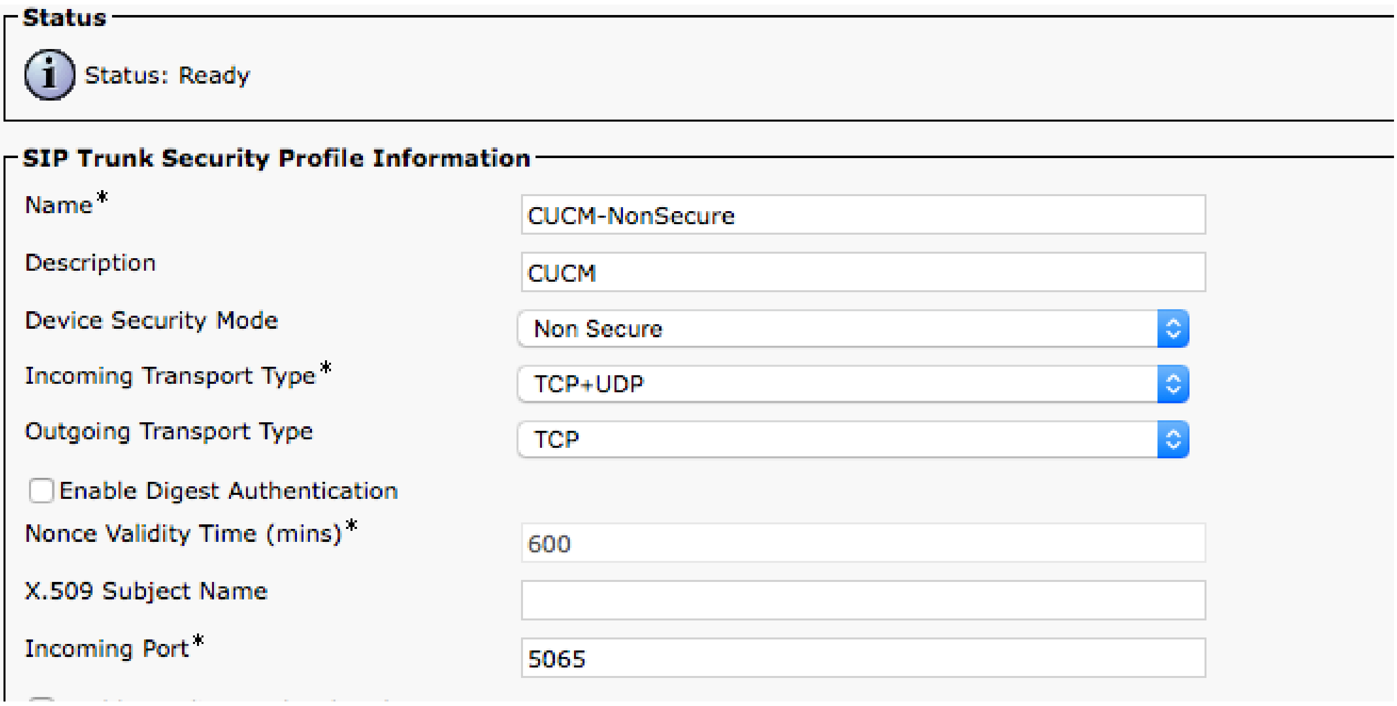
MRA uses an in-line communication while B2B calls use a trunk communication, CUCM has a limitation that does not allow in-line and trunk communications to pass through the same port. Since MRA is mostly configured automatically, B2B deployments need to use a different port.

Solution

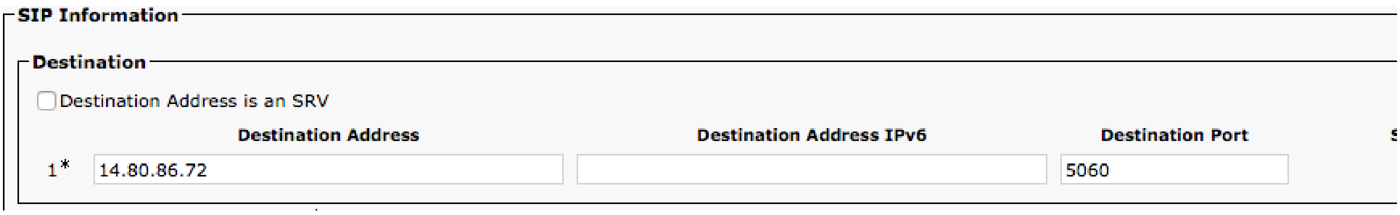
In order to do this, the destination port configured on the neighbor zone to CUCM (on VCS-C/Expressway-C) needs to be different than 5060/5061, normally 5065 is used but other can be used, the port configured needs to match with the port configured on the sip trunk security profile assigned to the sip trunk to this server on CUCM.

From **CUCM Administration page,** navigate **to Device > Trunk.**

SIP Trunk Security Profile with port 5065.

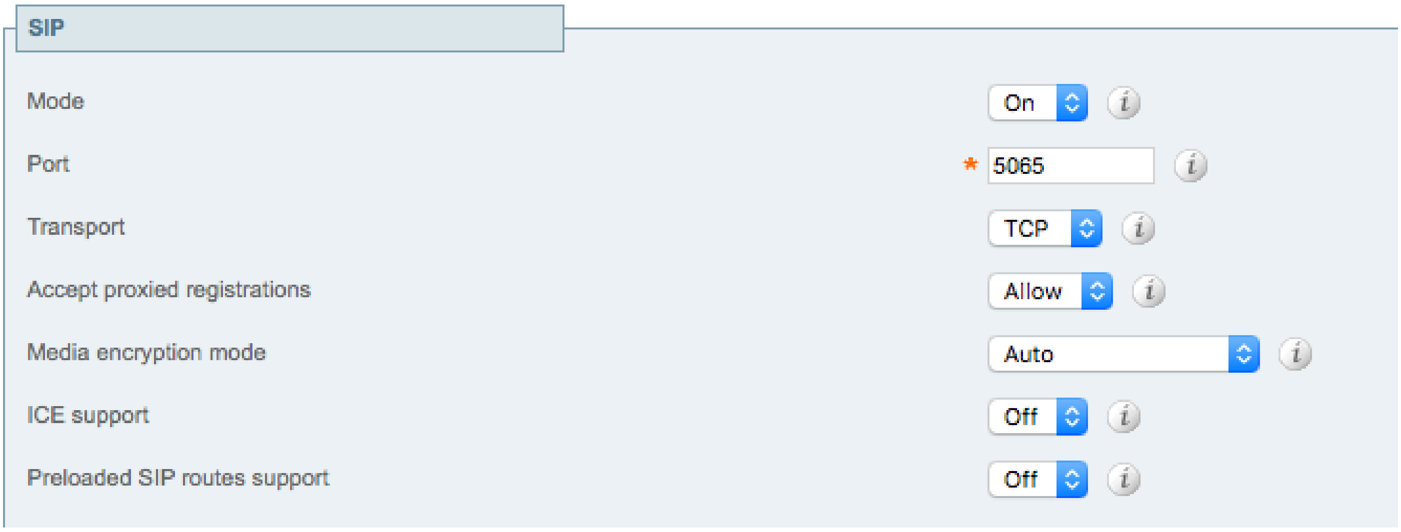


SIP Trunk destination port can be 5060/5061, as shown in the image.



SIP port in the VCS/Expressway neighbor zone needs to match the port configured in the SIP Trunk Security Profile, as shown in the image.

From **Expressway Administration page,** navigate to **Configuration > Protocols > SIP**



The VCS does not have this limitation or does not apply for this scenario, this means that the SIP trunk itself can be configured with 5060/5061.

8. VCS is unable to properly resolve FQDNs or fails to query SRV records.

For B2B calls originated from CUCM, an issue can be introduced due to the nature of how CUCM handles and routes calls.

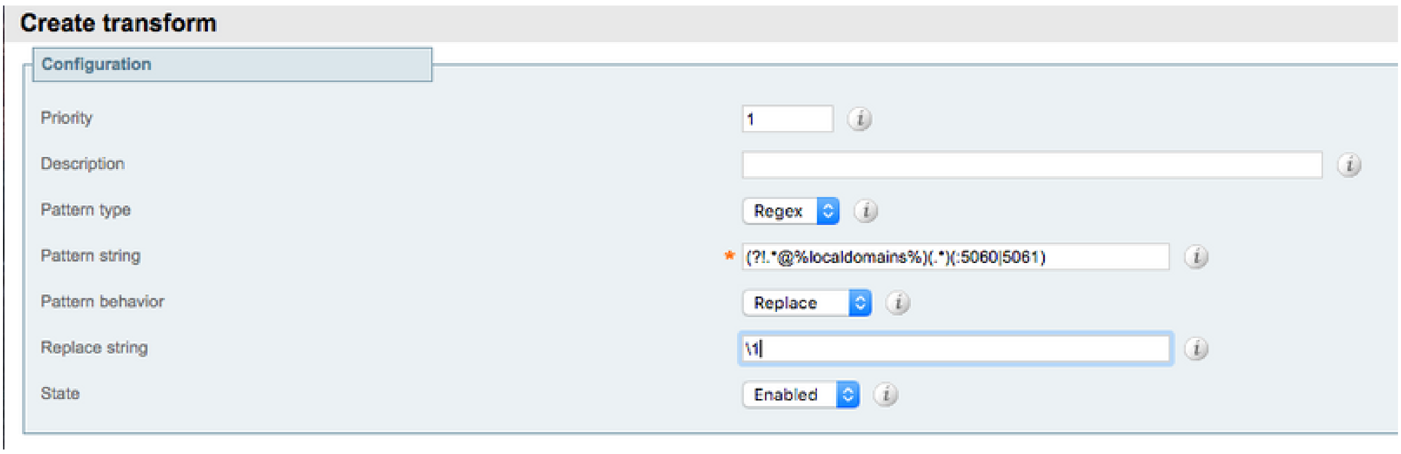
When CUCM forwardi calls to the VCS servers, CUCM tends to add :5060 or :5061 (depend on the configuration) at the end of the URI dialed, (i.e. test@lab.local >> test@lab.local:5060) when it reaches the expressway and hits a search rule towards the DNS zone, the VCS does not querie SRV record, rather it only querie for A or AAAA records. You can confirm this in the diagnostic logs from VCS/Expressway.

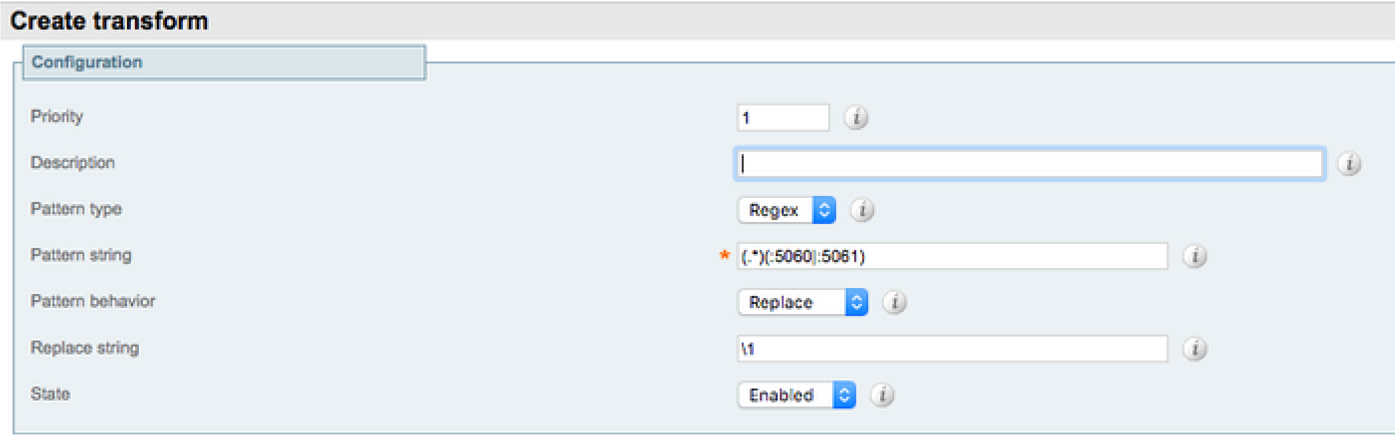
Solution

In order to solve this issue, simply create a transform that removes the port at the end (on either server, it doesn't really matter) before it reaches the DNS zone.

From **Expressway Administration page,** navigate **to Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform**

Transforms examples:





If for some reason a transform cannot be created, it can also be done through search rules but it is recommended to do so through transforms.

From **Expressway Administration page,** navigate **to Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Search Rules**

Related Information

- [Cisco VCS Expressway and VCS Control - Basic Configuration]()