

MRA电话服务因源IP转换通过NAT反射而失败 (启用静态NAT的单NIC配置)

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[网络图](#)

[详细信息](#)

[诊断日志中的证据](#)

[解决方案](#)

[在防火墙上禁用源IP端口转换](#)

[移至双网卡配置](#)

[相关信息](#)

简介

本文档介绍如何使用Expressway-E单NIC和静态NAT配置来排除因源IP转换通过NAT反射导致的MRA电话服务故障。

先决条件

Cisco 建议您了解以下主题：

- NAT (Network Address Translation , 网络地址转换)
- SIP (会话初始协议)
- 思科视频通信服务器(VCS)或Expressway基本配置
- 通过Expressway或VCS的移动和远程访问(MRA)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意:在整个文档中，Expressway设备称为Expressway-E和Expressway-C。但是，相同的配置适用于视频通信服务器(VCS)Expressway和VCS控制设备。

背景信息

本文档介绍使用单个NIC和静态NAT地址（如《Expressway基本配置指南》所述，使用单个Expressway-E LAN接口将移动和远程访问部署在Expressway E上）上的方案。MRA用户能够成功登录，但无法访问电话服务。

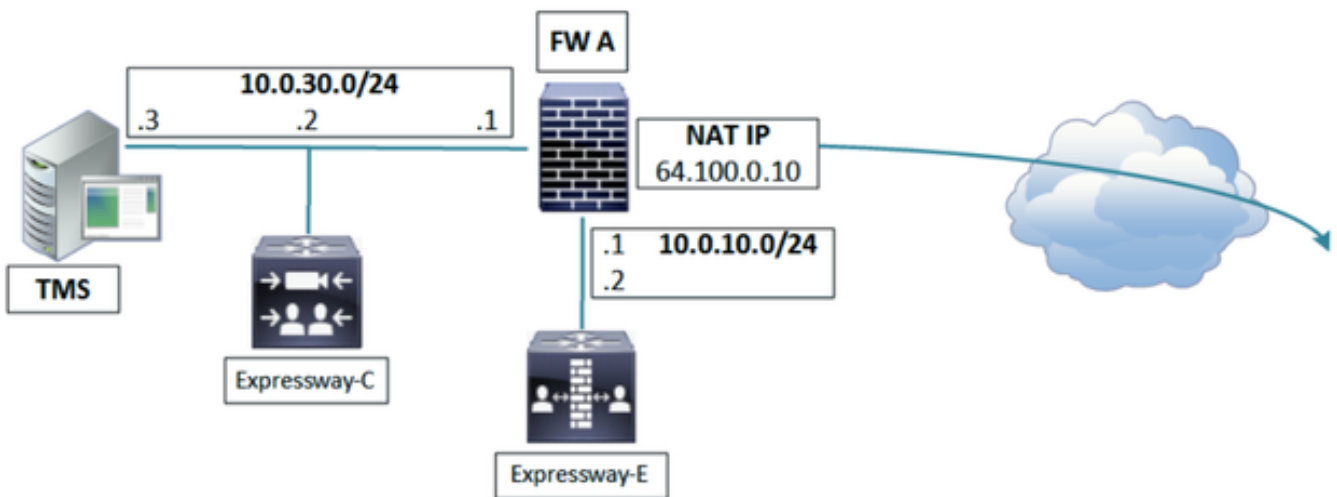
来自外部客户端的SIP REGISTER消息由Expressway-E在端口5061上成功接收。然后，Expressway-E会创建指向Expressway-C的SIP SERVICE消息。此请求将导致408请求超时。

问题

电话服务失败，因为SIP REGISTER消息未通过Cisco Unified Communications Manager (CUCM或Call Manager)。Expressway-E和Expressway-C无法使用SIP服务消息交换正确交换其证书。SIP SERVICE消息仅从Expressway-C获得408请求超时作为响应。由于SIP SERVICE消息不成功，Expressway-E不会将SIP REGISTER消息转发到Expressway-C。这是由于Expressway-C和Expressway-E之间的防火墙对从Expressway-C到Expressway-E的消息进行源IP（和端口）转换。这会导致Expressway-C将这些SIP服务消息错误地路由到该转换后的地址，而不是其自己的本地地址。在成功的场景中，Expressway-C会处理SIP服务消息本身。（Expressway-E和Expressway-C之间的SIP SERVICE消息用于检查证书，因此仅在遍历区域设置开始或首次通过MRA注册时可见。）

网络图

下图提供了网络图的示例，在本文档中用作参考：



详细信息

从Expressway-C数据包捕获中，您可以看到Expressway-C(10.0.30.2)成功连接到端口7003上的Expressway-E静态NAT公有IP地址(64.100.0.10)。(注意Expressway-C的源端口为27901):

| No. | Time | Source | Destination | Support | DstPort | Protocol | Length | Info |
|-----|-----------------|-----------|-------------|---------|---------|----------|--------|--|
| 80 | 09:09:04.879232 | 10.0.10.2 | 64.100.0.10 | 27901 | 7003 | TCP | 1024 | 27901->7003 [PSH, ACK] Seq=1 Ack=1 wln=1384 Len=904 TSval=1492541627 TSecr=1492190916 |
| 81 | 09:09:04.882328 | | | 7003 | 27901 | TCP | 661 | 7003->27901 [PSH, ACK] Seq=1 Ack=969 wln=1392 Len=595 TSval=1492190902 TSecr=1492541627 |
| 82 | 09:09:04.882370 | | | 27901 | 7003 | TCP | 66 | 27901->7003 [ACK] Seq=969 Ack=596 wln=1384 Len=0 TSval=1492541630 TSecr=1492210902 |
| 83 | 09:09:04.884037 | | | 27901 | 7003 | TCP | 1419 | 27901->7003 [PSH, ACK] Seq=969 Ack=596 wln=1384 Len=1351 TSval=1492541632 TSecr=1492210902 |
| 84 | 09:09:04.894490 | | | 7003 | 27901 | TCP | 1078 | 7003->27901 [PSH, ACK] Seq=596 Ack=2322 wln=1392 Len=1032 TSval=1492210903 TSecr=1492541632 |
| 85 | 09:09:04.913990 | | | 27901 | 7003 | TCP | 66 | 27901->7003 [ACK] Seq=2322 Ack=1608 wln=1384 Len=0 TSval=1492541682 TSecr=1492210915 |
| 831 | 09:09:13.971915 | | | 7003 | 27901 | TCP | 1514 | 7003->27901 [PSH, ACK] Seq=1608 Ack=2322 wln=1392 Len=1448 TSval=1492219992 TSecr=1492541682 |
| 832 | 09:09:13.971976 | | | 27901 | 7003 | TCP | 66 | 27901->7003 [ACK] Seq=2322 Ack=3056 wln=1384 Len=0 TSval=1492550720 TSecr=1492219992 |
| 833 | 09:09:13.972343 | | | 7003 | 27901 | TCP | 1514 | 7003->27901 [PSH, ACK] Seq=3056 Ack=2322 wln=1392 Len=1448 TSval=1492219992 TSecr=1492541682 |
| 834 | 09:09:13.972365 | | | 27901 | 7003 | TCP | 66 | 27901->7003 [ACK] Seq=2322 Ack=4504 wln=1384 Len=0 TSval=1492550720 TSecr=1492219992 |

在Expressway-E的数据包捕获中，您可以看到连接来自目标为10.0.10.2和端口7003的端口4401（它自己的静态NAT公有IP地址）上的64.100.0.10:

| No. | Time | Source | Destination | Support | DstPort | Protocol | Length | Info |
|-----|-----------------|-------------|-------------|---------|---------|----------|--------|---|
| 33 | 09:09:04.830500 | 64.100.0.10 | 10.0.10.2 | 4401 | 7003 | TCP | 1024 | 4401->7003 [PSH, ACK] Seq=1 Ack=1 wln=1384 Len=904 TSval=1492541627 TSecr=1492190916 |
| 34 | 09:09:04.882482 | | | 7003 | 4401 | TCP | 661 | 7003->4401 [PSH, ACK] Seq=1 Ack=969 wln=1392 Len=595 TSval=1492190902 TSecr=1492541627 |
| 35 | 09:09:04.883242 | | | 4401 | 7003 | TCP | 66 | 4401->7003 [ACK] Seq=969 Ack=596 wln=1384 Len=0 TSval=1492541630 TSecr=1492210902 |
| 36 | 09:09:04.883368 | | | 4401 | 7003 | TCP | 1419 | 4401->7003 [PSH, ACK] Seq=969 Ack=596 wln=1384 Len=1351 TSval=1492541632 TSecr=1492210902 |
| 37 | 09:09:04.894747 | | | 7003 | 4401 | TCP | 1078 | 7003->4401 [PSH, ACK] Seq=596 Ack=2322 wln=1392 Len=1032 TSval=1492210903 TSecr=1492541632 |
| 38 | 09:09:04.913508 | | | 4401 | 7003 | TCP | 66 | 4401->7003 [ACK] Seq=2322 Ack=1608 wln=1384 Len=0 TSval=1492541682 TSecr=1492210915 |
| 923 | 09:09:13.971946 | | | 7003 | 4401 | TCP | 2962 | 7003->4401 [PSH, ACK] Seq=1608 Ack=2322 wln=1392 Len=2896 TSval=1492219992 TSecr=1492541682 |
| 924 | 09:09:13.972018 | | | 7003 | 4401 | TCP | 1206 | 7003->4401 [PSH, ACK] Seq=4504 Ack=2322 wln=1392 Len=1140 TSval=1492219992 TSecr=1492541682 |

以下是Expressway-C与E之间连接的观点：

Expressway-C:10.0.30.2:27901 <-> 64.100.0.10:7003
 Expressway-E:64.100.0.10:4401 <-> 10.0.10.2:7003

这表示Expressway-C和Expressway-E之间的防火墙正在对这些消息执行源IP和端口转换。如果您查看Expressway-E上的SIP通信流，您可以看到它从MRA客户端设备获取SIP REGISTER，然后Expressway-E生成SIP SERVICE消息以与Expressway-C交换其证书，但这会导致408请求超时。

诊断日志中的证据

请注意，此SIP服务消息的路由报头（从Expressway-E发送到Expressway-C）包含NAT地址（64.100.0.10:4401）的IP和端口。当此消息到达Expressway-C时，Expressway-C会尝试根据该路由报头将消息路由到64.100.0.10:4401。由于此地址在Expressway E服务器端，因此无法连接到此地址，因此此操作失败。即使Expressway-C能够连接到此地址，也不正确，因为SIP SERVICE消息旨在供Expressway-C接收和处理。

SIP服务消息到达Expressway-C:

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCtime="2016-04-19 07:09:13,973" Module="network.sip"
Level="DEBUG": Action="Received" Local-ip="10.0.30.2" Local-port="27901" Src-ip="64.100.0.10" Src-port="7003" Msg-Hash="123456789123456789"
SIPMSG:
|SERVICE sip:serviceserver@cucm02.example.local SIP/2.0
Via: SIP/2.0/TLS 64.100.0.10:7003;egress-zone=UCTraversal;branch=[branchID];proxy-call-id=[callid];rport
Via: SIP/2.0/TCP 127.0.0.1:5060;branch=[branchID];received=127.0.0.1;rport=25063;ingress-zone=DefaultZone
Call-ID: abcd12345678@127.0.0.1
CSeq: 4616 SERVICE
Contact: <sip:serviceproxy@cucm02.example.local>
From: <sip:serviceproxy@cucm02.example.local>;tag=0987654321aaaa
To: <sip:serviceserver@cucm02.example.local>
```

Max-Forwards: 15
Route: <sip:64.100.0.10:4401;transport=tls;apparent;ds;lr>
Route: <sip:127.0.0.1:22210;transport=tcp;vcs-cate;lr>
User-Agent: TANDBERG/4132 (X8.7.2)
Date: Tue, 19 Apr 2016 07:09:13 GMT
Event: service
P-Asserted-Identity: <sip:serviceproxy@cucm02.example.local>
X-TAATag: e90b4983919b1f7a46d38f835
Identity:
"7ioJ9gpsS5ob2TUAttNxBGYRWDbnRuf5skrxxP+B14ngRvjkiWIu7BQP5W7vW1BTvyVaGuubV5u7rPdc5anDx9u46i/8TxxYuxkr83DEh/cYPWlw07JvTP5nub6/EtEt6RXvwizy6Gm/MXV4eMqQJ06kA86EFxP1SsRxop0YjUs61B10JnBrTQjOicskoAuMGzNjIBKvcCAbrASgtWP015vRp9Khcs3e8vmkpZH5Qtef6+gNaRWPES3MS=="
Content-Type: multipart/mixed;boundary=boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Length: 2555

--boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Type: application/text

```
<?xml version="1.0" encoding="utf-8"?>
<methodCall><params><username>john.smith</username><realm>expe.example.com</realm><nonce>2i78worv9unccs6vbcflfi4xai78worv9unccs6vbcflfi4xa4i15j</nonce><qop>auth</qop><cnonce>54f80570</cnonce><nc>00000001</nc><response>2i78worv9unccs6vbcflfi4xa4i15j</response><uri>sip:cucm02.example.local</uri><method>REGISTER</method><id>12345678</id>< caching-enabled>true</caching-enabled><reqtype>collab-edge</reqtype></params><methodName>DigestAuth</methodName><version>1.0</version><msgid>12345678979</msgid><sipdomain>cucm02.example.local</sipdomain></methodCall>
```

--boundary-6j7zrmj35ifsu3efg5ga603hzn1nbf
Content-Type: application/x-x509-ca-cert

```
-----BEGIN CERTIFICATE-----
hknS5nQ8NJEspXPY0N4BvA8iL7ZasOqngqgHRLj95N8bn
OfigoKhe90kV6Y7PRbRpwFv6jGiFR8hyepr3t2BPec0aZ
ZAK3ZC92RQbDjCxy2U99L8WLLTpJQwIuTjLHicbiNcNZu
Be9xEMgewwGFVfSzw08DzlecJNXpsKqQ0ivbplbwreXJG
SCbcse3067yvgHMDsotcK4gur11FZW0ZJFa3EMlgoT3Mj
ApGvMfL9caTjY1EaLWD15rWGGe8FpRLCizrZ0wwUGg7Px
Moy6kAuJtolwN9BUI0sgJ98MnBuuREJZNW7g7nJL5zywT
FXhMgy9PBUMuwjgu5KruY4caWDYtNu1kZzCtnm044lOk7
xhIOoOWWj9sNFndQGDrgBIFBjggEihSbZr6h4Pq2ZMZ4r
i5yGpz0j7a6lg2NOKm6FXpfqV1B7zvyQsM6x0XJEImpjV
al0nHYkTLkBEk5jVosgyOrSWpZPimc364sRxRW4ABZZX
M6XstZNGhvQNDVklJlfcN5yRtEgEkkizeWOHJcts922wL
2rVTfufWGXMkca8YHKj2ixkthNnHVbLG0YoUNOUDHq1xu
49F7Kcw7neuQQZ4MmEif59lnyhY7qEIQVEpGn0jggZAX8
omNVxTewa9nTXvjxo5xvTLghYfESCqniBbtWwMhhRuR7N
eh090vFwsuUyHJmDBYpoNZWTXEB4Fw5XwfjzZAoHzOFV6
xcE4LGYrpI4EbaZ58r8uVrfXkrNrgepFw2zMgamhfw9n5
AzEU2gh9vTUNZEAn8De5XQKAipeeh08Dpef2JTBLV5avf
nh7rfxh8BZY4xteSRox8iBnT4Na6qsDMb2gvp6gTYFFJH
RGMHIE5siI1HhARqDjen4EwrKfMOYNJWTqmx4mjDrqyme
-----END CERTIFICATE-----
```

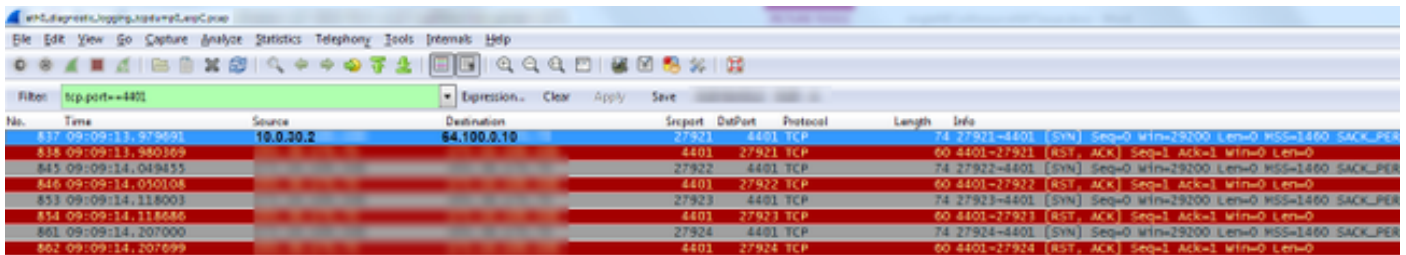
2016-04-19T17:09:13+10:00 expc tvcs: UTCtime="2016-04-19 07:09:13,977"
Module="developer.sip.leg" Level="INFO"
CodeLocation="ppcmains/sip/siproxy/SipProxyLeg.cpp(10047) "
Method="SipProxyLeg::routeViaNettleIfNeeded" Thread="0x3150905deea6": this="0xc76759f343ca"
Type="Outbound" routingViaNettle="false" twoInARow="false" oneIsATraversalServerZone="false"
isCall="false" isRefer="false" fromClusterPeer="false" fromNettle="false" toNettle="false"
inboundZone=UC_Traversal (encryption-mode=on ice-mode=off) outboundZone=DefaultZone (encryption-mode=auto ice-mode=off) encryptionSettingsRequireNettle="true" iceSettingsRequireNettle="false"
needlesslyNettling="false" routeViaNettle="false"

Expressway-C尝试发送此SIP服务消息以告知其在路由报头中显示的内容，但连接失败：

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,979" Module="network.tcp"
Level="DEBUG": Src-ip="10.0.30.2" Src-port="27921" Dst-ip="64.100.0.10" Dst-port="4401"
Detail="TCP Connecting"
```

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,980" Module="network.tcp"
Level="ERROR": Src-ip="10.0.30.2" Src-port="27921" Dst-ip="64.100.0.10" Dst-port="4401"
Detail="TCP Connection Failed"
```

在Expressway-C的数据包捕获中，TCP SYN尝试获取RST响应：



The image shows a Wireshark packet capture interface. The filter is set to 'tcp.port==4401'. The packet list shows several packets between source IP 10.0.30.2 and destination IP 64.100.0.10. Packet 817 is a SYN packet (Seq=0, Win=29200, Len=0, MSS=1460). Packet 818 is an RST packet (Seq=1, Ack=1, Win=0, Len=0). Packet 815 is another SYN packet. Packet 816 is another RST packet. Packet 813 is a SYN packet. Packet 814 is another RST packet. Packet 861 is a SYN packet. Packet 862 is another RST packet.

结果是Expressway-C向Expressway-E发送408请求超时：

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,982" Module="network.sip"
Level="INFO": Action="Sent" Local-ip="10.0.30.2" Local-port="27901" Dst-ip="64.100.0.10"
Dst-port="7003" Detail="Sending Response Code=408, Method=SERVICE, CSeq=4616,
```

```
To=sip:serviceserver@cucm02.example.local, Call-ID=abcd12345678@127.0.0.1, From-
Tag=0987654321aaaa, To-Tag=0987654321bbbb, Msg-Hash=123456789123456789"
```

```
2016-04-19T17:09:13+10:00 expc tvcs: UTCTime="2016-04-19 07:09:13,982" Module="network.sip"
Level="DEBUG": Action="Sent" Local-ip="10.0.30.2" Local-port="27901" Dst-ip="64.100.0.10"
Dst-port="7003" Msg-Hash="123456789123456789"
```

SIPMSG:

|SIP/2.0 408 Request Timeout

Via: SIP/2.0/TLS 64.100.0.10:7003;egress-zone=UCTraversal;branch=[branchID];proxy-call-
id=[callid];received=64.100.0.10;rport=7003;ingress-zone=UCTraversal;ingress-zone-id=4

Via: SIP/2.0/TCP 127.0.0.1:5060;branch=[branchID];received=127.0.0.1;rport=25063;ingress-
zone=DefaultZone

Call-ID: abcd12345678@127.0.0.1

CSeq: 4616 SERVICE

From: <sip:serviceproxy@cucm02.example.local>;tag=0987654321aaaa

To: <sip:serviceserver@cucm02.example.local>;tag=0987654321bbbb

Server: TANDBERG/4132 (X8.7.2)

Warning: 399 10.0.30.2:5061 "Request Timeout"

Content-Length: 0

解决方案

这种情况有两种可能的解决办法。

在防火墙上禁用源IP端口转换

如果在防火墙上禁用源IP/端口转换，Expressway-E服务器会将Expressway-C流量视为从10.0.30.2:27901（Expressway-C上的实际IP和端口）到达，而不是64.100.0.10:4401（NAT地址）。这样，SIP SERVICE消息上的路由报头包含10.0.30.2:27901值，在收到此消息时，Expressway-C会将其路由到自己并对其执行一些处理，从而使200 OK发回Expressway-E（如果一切正常），然后代理通过SIP REGISTER消息继续注册流程。

移至双网卡配置

在Expressway-E上配置双网卡时，无需执行NAT反射，避免了问题。但是，请确保Expressway-E和Expressway-C（如果存在）之间的内部防火墙不执行从Expressway-C到Expressway-E的流量的源IP/端口转换（这会导致类似问题）。

相关信息

- 《Expressway基本配置指南》的附录4中详细介绍了Expressway[支持的网络部署](#)
- 按照ASA[配置详细信息](#)配置支持的Expressway网络部署