

了解会议服务器上的呼叫路由逻辑

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[思科会议服务器\(CMS\)的呼叫路由逻辑是什么？](#)

[步骤1.来电匹配表](#)

[步骤2.来电转接表](#)

[重写域](#)

[主叫方 ID](#)

[步骤3.呼出呼叫表](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍思科会议服务器(CMS) (以前称为Acano产品) 的呼叫路由逻辑，该逻辑被拆分到多个呼叫路由表中。本文档介绍呼叫可通过这些呼叫路由表经历的不同阶段和场景。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科会议服务器呼叫网桥组件。

使用的组件

本文档中的信息基于版本2.3.x的Cisco Meeting Server。

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。

思科会议服务器(CMS)的呼叫路由逻辑是什么？

CMS上的呼叫路由涉及一些不同的呼叫路由表。通过可下载的流程表，您可以按照到达CMS的每个呼叫的呼叫路由逻辑进行操作。这适用于所有类型的呼叫：除非另有说明，否则思科会议应用 (CMA — 胖客户端或WebRTC)、标准会话发起协议(SIP)呼叫或Microsoft SIP呼叫。

注意：唯一的例外是CMS发起的呼叫(CMS直接用于网真管理套件(TMS)计划出站呼叫或CMA客户端呼出)，其中会绕过呼叫转发表。

以下是CMS中呼叫路由过程的顺序：

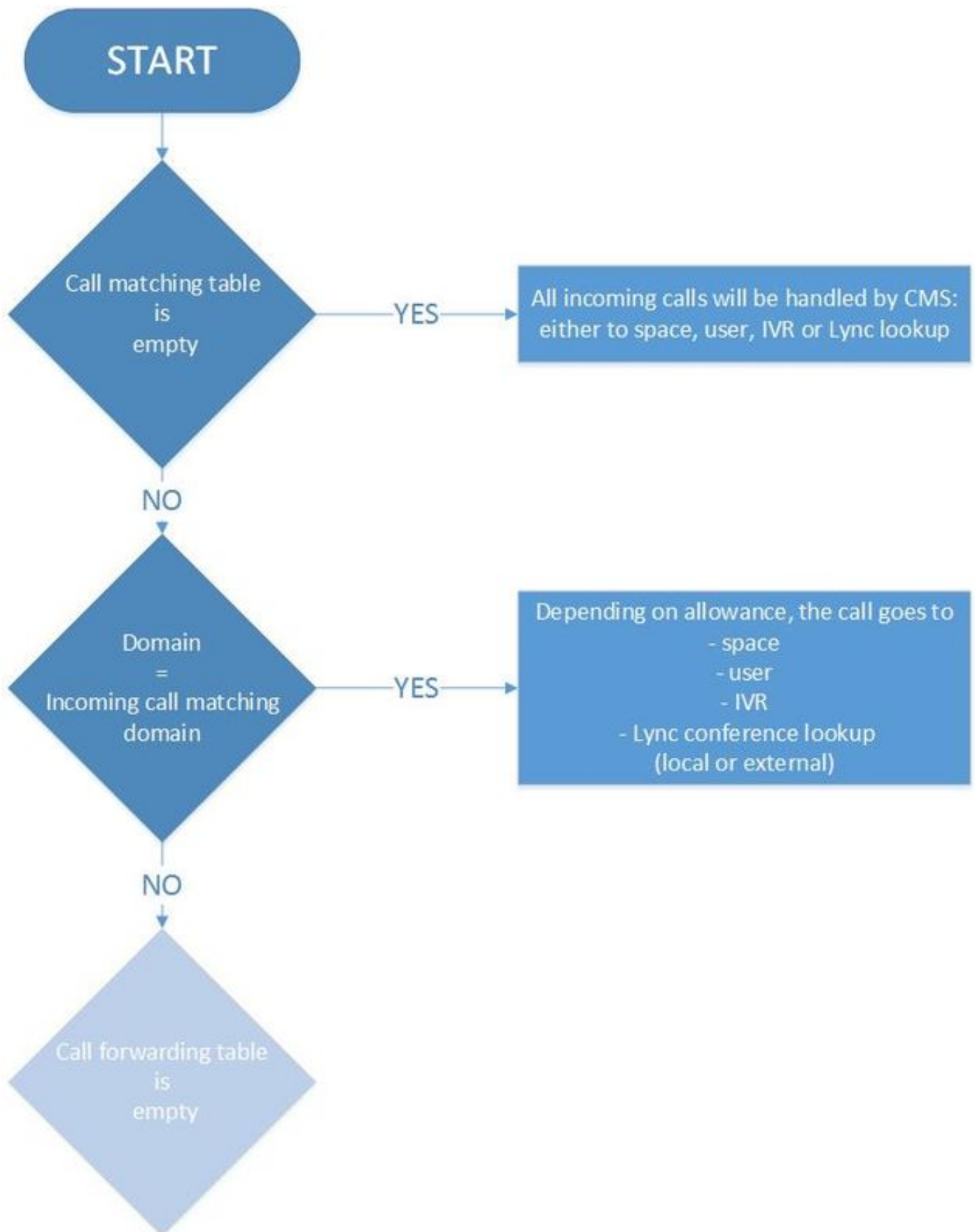
1. 来电匹配表
2. 来电转发表
3. 呼出呼叫表

每个表在文档的后面部分有更详细的说明，其中包括仅显示相关部分的图像。

注意：CMS仅基于域路由执行呼叫路由，因此基于统一资源标识符(URI)的右侧(RHS)。没有基于URI左侧(LHS)的呼叫路由功能，就像您在Cisco Unified Communications Manager(CUCM)上使用DirectoryNumber路由（路由模式）时一样。

注意：每个表都是由优先级属性设置的有序列表。更高的优先级意味着它会首先尝试匹配。如果不匹配，则继续使用列表中的下一个规则。一般经验法则是，将比较一般的规则（如与任何域匹配的*）的优先级低于较具体的规则。这样，特定规则将首先处理，您有可能回退到更一般的规则。

步骤1.来电匹配表



这是CMS确定入站呼叫是发往思科会议服务器本身，并需要进一步处理的过程中的第一步，或是它是发往不同系统的呼叫，其中CMS是交互工作呼叫并处理媒体和信令(例如，Skype网关呼叫标准SIP终端，反之亦然)。

它检查传入URI的域部分是否与传入匹配表匹配。如果匹配，它可以根据您对此拨号方案规则的配置将呼叫路由到空间、用户、IVR或执行Lync会议查找(内部或外部)。该表不允许使用通配符域

, 它需要完全匹配。

注意：如果您没有配置任何呼入呼叫匹配域，CMS将接受来自SIP或Lync呼叫的所有呼入URI，这些呼入URI将登录到呼叫桥。对于CMA客户端（WebRTC或胖客户端），虽然它接受呼叫，但它不会自动路由到正确的空间或用户。因此，在本例中，使用CMA客户端拨号到空间或用户时，必须输入正确的域。

例如，图中显示了呼叫匹配表(它仅显示“目标”空间和“目标”用户选项以简化):

Incoming call handling

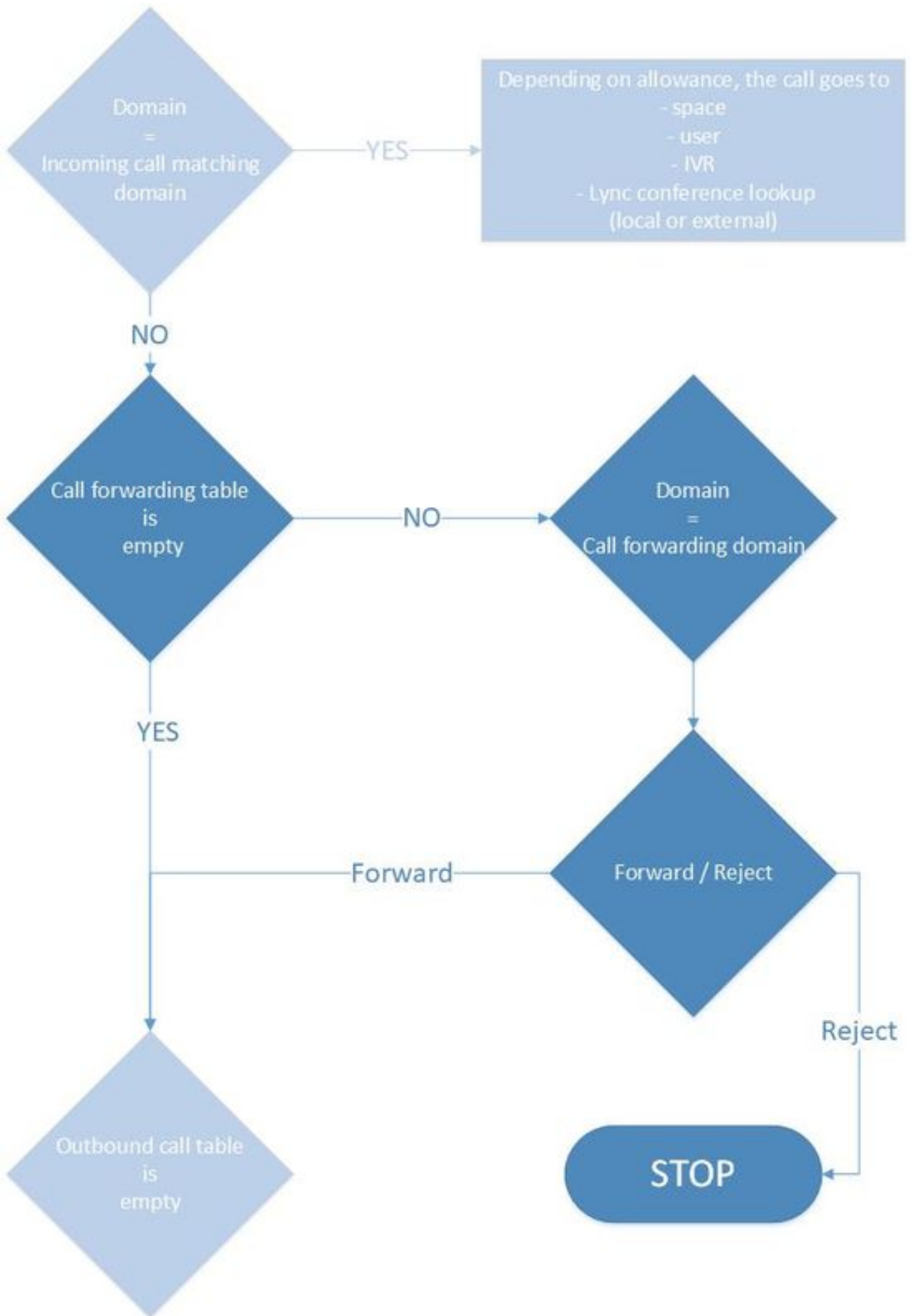
Call matching

<input type="checkbox"/>	Domain name	Priority	Targets spaces	Targets users
<input type="checkbox"/>	acano.steven.lab	2	yes	yes
<input type="checkbox"/>	10.48.54.160	1	yes	yes
<input type="checkbox"/>	acano1.acano.steven.lab	0	yes	yes
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	yes ▾	yes ▾

1

此处，域设置为客户端通常拨打的acano.steven.lab。但是，它还允许来自CUCM的临时呼叫或特定SIP路由模式（或Expressway搜索规则），这些模式仅针对特定呼叫网桥（在集群中）的表中的第一和第二回退规则，该规则与呼叫网桥的IP地址（本例中为10.48.54.160）或完全限定域名(FQ)匹配fqdn)。

步骤2.来电转接表



如果呼叫未达到传入呼叫匹配表上的任何规则，或者呼叫未匹配以继续（例如用户拨打的空间URI不存在或错误），则呼叫将通过名为呼叫转发表的第二个表。这也仅基于域，允许您明确阻止对特定域的呼叫或仅允许对特定域的呼叫。如果要执行此操作，必须具有更高优先级的更具体规则，因此首先检查这些规则。

此示例显示，对dummy.com的呼叫被拒绝，而对tplab.local的呼叫被转发：

Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
<input type="checkbox"/> dummy.com	0	reject	use dial plan	no		[edit]
<input checked="" type="checkbox"/> tplab.local	0	forward	use dial plan	no		[edit]
<input type="text"/>	0	reject	use dial plan	no		[Add New] [Reset]

如果将呼叫转发表留空，则会导致CMS不充当Skype和SIP参与者之间的网关（例如，没有任何呼叫转发规则）的状态。假设来电的域在来电匹配表上不匹配或域匹配，但在空间、用户或IVR（或Skype会议）上不匹配，则呼叫不会根据去电表转发。

注意：虽然CMA客户端（胖客户端和WebRTC）能够发出呼出呼叫（*3.0中的Web应用无法发出呼出呼叫，而是CMS空间发出的呼叫由Callbridge发出），但确实会发生这种情况。同样，在通过API（例如，在TMS计划会议中）进行CMS出站呼叫时，也能正常工作。通常，从CMS本身（直接或通过CMA）发起的呼叫不得遵循呼叫转移逻辑。

在事件日志中，您可以看到突出显示的转发消息，例如当CMS充当SIP和Skype呼叫的网关时。在此之前，您可以看到来电和后来的去电。

```

2018-10-04 06:36:24.612 Info      call 788: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 06:36:24.624 Info      forwarding call to 'sip:stejanss@any.com' to
'stejanss@any.com'
2018-10-04 06:36:24.625 Info      call 789: outgoing SIP call to "stejanss@any.com"

```

如果转发表没有任何规则或拒绝规则，则事件日志不会显示此信息。它只是通知您SIP呼叫不匹配（任何空间、用户、IVR或Lync会议），并且您错过转发规则（或设置为拒绝）以移至出站规则部分。

```

2018-10-04 06:47:12.482 Info      call 790: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 06:47:12.495 Info      call 790: ending; local teardown, destination URI not matched
- not connected after 0:00

```

对于通过TMS安排的会议发起的CMA客户端呼叫或来自CMS的出站呼叫，在事件日志中未看到来电。呼叫会立即进入出站拨号方案表，且不由呼叫转发表处理。

在呼叫转发表中，还有两个其他配置选项：重写域和呼叫方ID。

重写域

此选项允许您将入站呼叫的域重写为不同的域，并更改SIP请求URI的域部分和SIP消息的To报头。

Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
<input type="checkbox"/> any.com	2	forward	use dial plan	yes	newany.com	[edit]
<input type="checkbox"/> dummy.com	0	reject	use dial plan	no		[edit]
<input type="checkbox"/> tplab.local	0	forward	use dial plan	no		[edit]
<input type="text"/>	0	reject	use dial plan	no		[Add New] [Reset]

例如，在此映像上进行配置时，对于域any.com的入站呼叫（在空间、用户、IVR或Skype会议上），在此显示事件日志（启用SIP跟踪），但呼入呼叫匹配表上没有匹配项：

```
2018-10-04 07:02:24.818 Info SIP trace: connection 0: incoming SIP TCP data from
10.48.36.215:56457 to 10.48.80.71:5060, size 1000:
2018-10-04 07:02:24.818 Info SIP trace: INVITE sip:stejanss@any.com SIP/2.0
2018-10-04 07:02:24.818 Info SIP trace: Via: SIP/2.0/TCP
10.48.36.215:5060;branch=z9hG4bK53e4c4ce29394
2018-10-04 07:02:24.818 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=742103~ee545a46-516a-4de6-87d7-7b1f5a5b848a-26001856
2018-10-04 07:02:24.818 Info SIP trace: To: <sip:stejanss@any.com>
..
2018-10-04 07:02:24.822 Info call 797: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-04 07:02:24.834 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@newany.com'
2018-10-04 07:02:24.835 Info call 798: outgoing SIP call to "stejanss@newany.com"
..
2018-10-04 07:02:24.838 Info SIP trace: connection 19: outgoing SIP TCP data to
10.48.36.215:5060 from 10.48.80.71:57854, size 3286:
2018-10-04 07:02:24.838 Info SIP trace: INVITE sip:stejanss@newany.com SIP/2.0
2018-10-04 07:02:24.838 Info SIP trace: Via: SIP/2.0/TCP
10.48.80.71:5060;branch=z9hG4bKefc98b81a2961b37aee24f03c2142d8e
2018-10-04 07:02:24.839 Info SIP trace: Call-ID: 18644f28-e998-4032-a7df-75325e9d11b0
2018-10-04 07:02:24.839 Info SIP trace: CSeq: 659590315 INVITE
2018-10-04 07:02:24.839 Info SIP trace: Max-Forwards: 70
2018-10-04 07:02:24.839 Info SIP trace: Contact: <sip:1060@10.48.80.71;transport=tcp>
2018-10-04 07:02:24.839 Info SIP trace: To: <sip:stejanss@newany.com>
2018-10-04 07:02:24.839 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=2aa2a49bba231a1b
```

在此转接呼叫线路中，它显示已发生的修改。如果未启用SIP跟踪，它仍会显示any.com对newany.com的修改。

此域重写最常用的方法是与[CMS集群内部Lync集成](#)，建议将出站规则中的“联系人”报头和“发件人”报头设置为Lync/Skype至Callbridge特定的完全限定域名(FQDN)。这是因为以下路由规则：

- Skype在对话框内（例如，在INVITE - 200 OK后发出ACK）将新事务发送到从CMS收到的200 OK中指定的Contact标题。对于从Skype到CMS的入站连接，Skype首先发送NEGOTIATE SIP消息，该消息包含To报头中的ms-fe报头，该报头指定在INVITE上的200 OK回复中必须填入联系人报头的方式（因为它使用相同的TCP信道）
- Skype将新的对话框（如内容共享，因为它是单独的呼叫，或在未接呼叫时回叫）发送到原始INVITE的“发件人”报头

在重写域时，它与Lync呼叫的回叫相关。未接INVITE的From报头指向呼叫来源的特定呼叫桥。然后，Lync发送带有SIP请求URI的新请求(INVITE)，该URI与呼叫桥FQDN匹配。然后通过这些重写规则将其转换为SIP域。转发呼叫后，它将使用出站规则到注册SIP终端的CUCM或Expressway-C。

主叫方 ID

此处有两个选项可设置在转发规则上。设置为通过，然后不对出站INVITE的From报头进行任何修改，或者设置为使用拨号方案，允许系统根据出站规则修改From报头。此设置与域是否重写无关，因为重写仅涉及SIP请求URI和出站INVITE的To报头。

例如，与之前进行的呼叫相同，但现在有一个到newany.com的出站拨号方案规则（如在传入呼叫转发表上重写后），该规则设置为Lync类型呼叫（例如，Ms-Conversation-ID作为额外SIP报头）。相应地，本地发件人域（和本地联系域）填充为指向Lync呼叫前面所示的callbridge FQDN。然后，这将反映出站SIP邀请的发件人和联系人标题上的更改。如图所示，这些信息填充了相同的值，可根据您的要求单独选择。

Outbound calls

Filter	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority
<input type="checkbox"/>	steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	5
<input type="checkbox"/>	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4

```

2018-10-12 09:09:24.488 Info SIP trace: connection 28: incoming SIP TCP data from
10.48.36.215:44460 to 10.48.80.71:5060, size 1000:
2018-10-12 09:09:24.489 Info SIP trace: INVITE sip:stejanss@any.com SIP/2.0
2018-10-12 09:09:24.489 Info SIP trace: Via: SIP/2.0/TCP
10.48.36.215:5060;branch=z9hG4bKf4a230ec178e
2018-10-12 09:09:24.489 Info SIP trace: From: "EX60 Steven"
<sip:1060@steven.lab>;tag=118288~ee545a46-516a-4de6-87d7-7b1f5a5b848a-32900729
2018-10-12 09:09:24.489 Info SIP trace: To: <sip:stejanss@any.com>
2018-10-12 09:09:24.489 Info SIP trace: Call-ID: 81e67f80-bc0164c4-f2c6-
d724300a@10.48.36.215

2018-10-12 09:09:24.494 Info call 803: incoming SIP call from "sip:1060@10.48.36.215" to
local URI "sip:stejanss@any.com"
2018-10-12 09:09:24.506 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@newany.com'
2018-10-12 09:09:24.507 Info call 804: outgoing SIP call to "stejanss@newany.com" (Lync)

2018-10-12 09:09:24.507 Info SIP trace: connection 33: allocated for outgoing connection
to 10.48.36.46:5060
2018-10-12 09:09:24.508 Info SIP trace: connection 33: outgoing connection successful,
10.48.80.71:39782 to 10.48.36.46:5060
2018-10-12 09:09:24.510 Info SIP trace: connection 33: outgoing SIP TCP data to
10.48.36.46:5060 from 10.48.80.71:39782, size 2971:
2018-10-12 09:09:24.510 Info SIP trace: INVITE sip:stejanss@newany.com SIP/2.0
2018-10-12 09:09:24.510 Info SIP trace: Via: SIP/2.0/TCP
10.48.80.71:5060;branch=z9hG4bK15bdde97ab641b586f162187cfdd98b5
2018-10-12 09:09:24.510 Info SIP trace: Call-ID: c366ddaf-e602-4fa5-b1d6-2e16ec08534a
2018-10-12 09:09:24.510 Info SIP trace: CSeq: 1498747095 INVITE
2018-10-12 09:09:24.510 Info SIP trace: Max-Forwards: 70
2018-10-12 09:09:24.510 Info SIP trace: Contact:
<sip:1060@callbridgefqdn.any.com;transport=tcp>
2018-10-12 09:09:24.510 Info SIP trace: Ms-Conversation-ID: 3P5Hu8grR1GGDF1BSMZAmw==
2018-10-12 09:09:24.510 Info SIP trace: To: <sip:stejanss@newany.com>
2018-10-12 09:09:24.510 Info SIP trace: From: "EX60 Steven"
<sip:1060@callbridgefqdn.any.com>;tag=fb4ae780677e9d9b

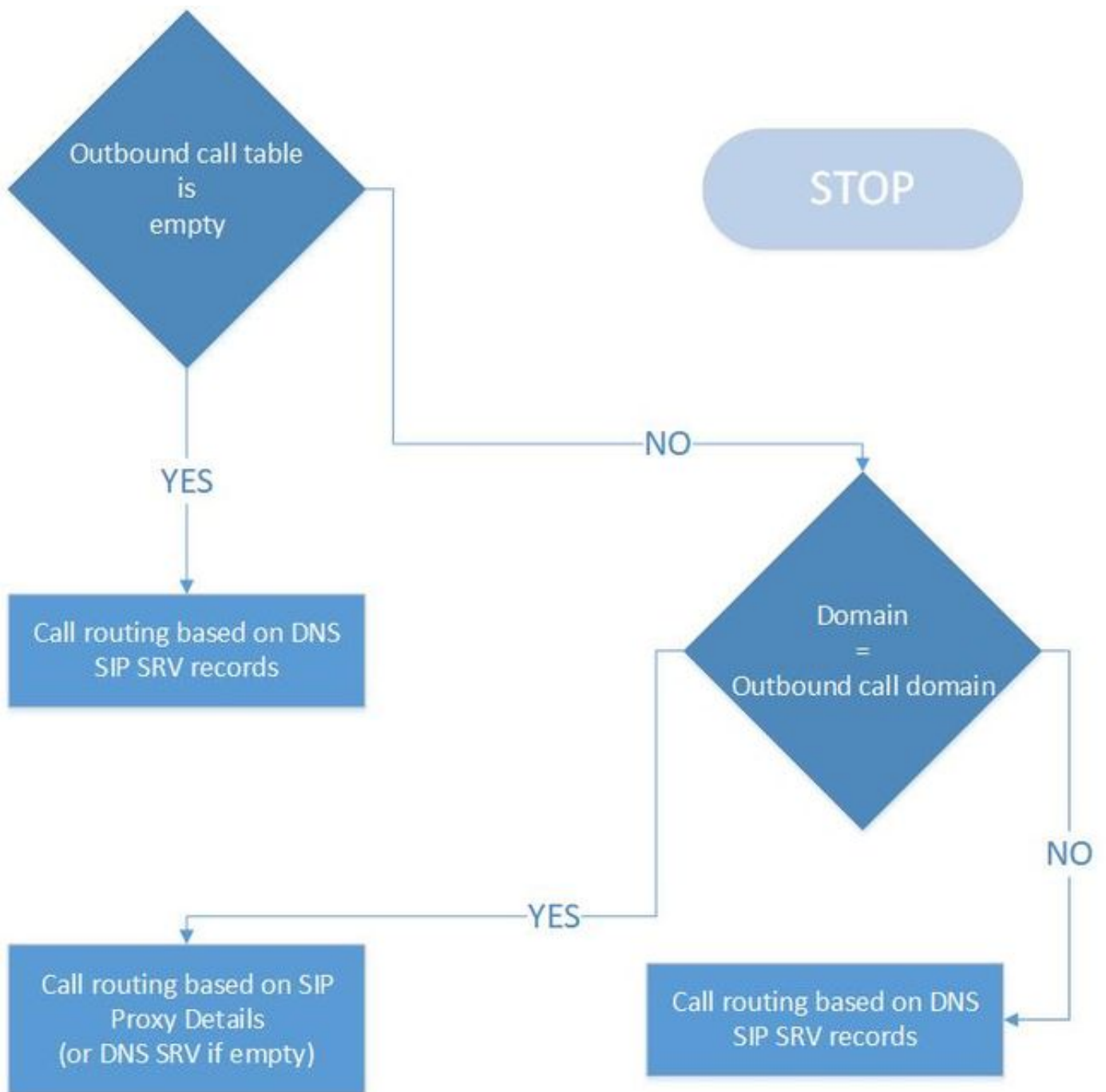
```

如果转发规则只是在传递时设置，则From报头上也不会像上一个示例一样进行任何修改（在这种情况下，转发规则上设置了传递）。当CMS启动新的callLeg时，联系人信头始终适用，因此必须在联系人信头中添加联系人信头。

可以使用主叫方ID、本地联系域和本地自域的不同组合。出站SIP INVITE上的From报头构建如表所示，其中入站呼叫使用From报头usera@from.com进入CMS。

Forwarding rule Caller ID	Outbound call rule Local contact domain	Local	Outbound call rule Local from domain	Resulting from header
Pass through	NA		NA	usera@from.com
Use dial plan	NA		<u>newfrom.com</u>	usera@newfrom.com
Use dial plan	cms1.test.cms.com		<blank>	usera@cms1.test.cms.com
Use dial plan	<blank>		<blank>	<u>usera@<ip_cms></u>

步骤3.呼出呼叫表



这是呼叫路由逻辑中最后一个表，它将呼出到不同的服务器，如：

- 传入呼叫不在本地处理（在传入呼叫匹配域上）。

- 它是来自CMS空间(例如，在TMS计划会议或Cisco Meeting Manager(CMM)指示出站呼叫的情况下通过CMS空间或API进行的出站呼叫)或来自CMA客户端的出站呼叫。

从图像中可以看出，逻辑相对简单。如果表中没有任何条目，它仍允许出站呼叫，但假定CMS服务器能够解析SIP请求URI中所述的特定域的SIP SRV记录(_sips._tcp / _sip._tcp / _sip._udp)。如果表不为空，但拨号域没有匹配，则执行相同的DNS查找逻辑。如果域上有匹配项，则遵循该特定规则的逻辑。在这方面，如果要阻止来自CMA的出站呼叫或通过TMS或CMM发出的出站呼叫，可以通过两种方式执行此操作。没有任何DNS SRV记录 (或CMS无法解析)，或者将这些呼叫路由到您的呼叫控制 (例如CUCM或Expressway) 并阻止那里的呼叫。

图中显示了一个出站呼叫表示例：

Outbound calls

Filter	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	steven.lab	<none; call directly>	contact.test.com	test.com	Standard SIP	Stop	5	Unencrypted
<input type="checkbox"/>	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4	Unencrypted
<input type="checkbox"/>	any.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	3	Unencrypted
<input type="checkbox"/>	test.cms.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	2	Unencrypted
<input type="checkbox"/>	vcs.steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	1	Unencrypted
<input type="checkbox"/>	<match all domains>	10.48.36.215		<use local contact domain>	Standard SIP	Stop	0	Unencrypted
					Standard SIP	Stop	0	Auto

如果<match all domains>规则位于末尾，且第一个规则位于steven.lab的域，而SIP代理未填充 (因此它依赖于DNS SRV记录)。

请注意，这是优先级值较高的有序列表，其中优先覆盖。如果将规则与Behavior设置为Stop，则在匹配后，呼叫不会通过表的其余部分，如果SIP代理无法路由呼叫，则呼叫失败。当该设置设置为Continue时，您可以允许回退到集群中的其他路由或不同节点。例如，可以为同一域的每条规则指定不同的SIP代理。

“本地联系域”和“本地自域”的设置传入呼叫转发表的上一部分中介绍。中继类型允许您指定需要进行的呼叫类型，该呼叫类型可以是标准SIP、Lync或Avaya，具体取决于接收系统。

Encryption字段确定呼叫的信令必须未加密还是加密。但是，请注意，这并不意味着在SIP媒体加密配置中设置任何媒体加密，如Configuration > Call Settings菜单中所示。在此配置中，您还可以选择Auto (自动)，该选项会尝试先使用加密信令进行呼叫，并可能回退到未加密信令。如果您事先知道另一端已加密或未加密，强烈建议相应地定义它，以避免因回退过程而造成任何呼叫设置延迟。

对steven.lab的呼叫 (在传入呼叫转发表上重写域后) 的日志文件输出示例，其中DNS跟踪和SIP跟踪设置为detailed，显示了要查询的SRV记录以及Encryption设置为Auto时的回退机制。

```

2018-10-12 11:25:16.168 Info call 821: incoming SIP call from "sip:1060@steven.lab" to
local URI "sip:stejanss@any.com"
2018-10-12 11:25:16.179 Info forwarding call to 'sip:stejanss@any.com' to
'stejanss@steven.lab'
2018-10-12 11:25:16.180 Info call 822: outgoing SIP call to "stejanss@steven.lab"

2018-10-12 11:25:16.180 Info DNS trace: resolving "steven.lab" (SRV "_sips._tcp",
dnsType:1) for call 822
2018-10-12 11:25:16.181 Info DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for
call 822 returned result, addresses: 1
2018-10-12 11:25:16.181 Info DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for

```

```

call 822 succeeded; results: 1
2018-10-12 11:25:16.181 Info      DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for
call 822 using 10.48.36.215:5061
2018-10-12 11:25:16.181 Info      SIP trace: connection 45: allocated for outgoing encrypted
connection to 10.48.36.215:5061
2018-10-12 11:25:16.201 Info      handshake error 336151576 on outgoing connection 45 to
10.48.36.215:5061 from 10.48.80.71:54864
2018-10-12 11:25:16.201 Info      SIP trace: connection 45: shutting down...

2018-10-12 11:25:16.201 Info      call 822: falling back to unencrypted control connection...

2018-10-12 11:25:16.201 Info      DNS trace: resolving "steven.lab" (SRV "_sip._tcp",
dnsType:1) for call 822
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 returned result, addresses: 1
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 succeeded; results: 1
2018-10-12 11:25:16.202 Info      DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for
call 822 using 10.48.36.215:5060
2018-10-12 11:25:16.202 Info      SIP trace: connection 46: allocated for outgoing connection
to 10.48.36.215:5060
2018-10-12 11:25:16.203 Info      SIP trace: connection 46: outgoing connection successful,
10.48.80.71:59776 to 10.48.36.215:5060
2018-10-12 11:25:16.205 Info      SIP trace: connection 46: outgoing SIP TCP data to
10.48.36.215:5060 from 10.48.80.71:59776, size 3290:
2018-10-12 11:25:16.205 Info      SIP trace: INVITE sip:stejanss@steven.lab SIP/2.0

```

注意：如果集群环境具有多个呼叫网桥，则可以在通过API配置每个呼叫网桥时设置出站拨号方案规则，并在API对象上指定呼叫网桥ID（或callbridgeGroup ID）。例如，假设您希望所有呼叫从特定域的一个特定呼叫桥传出（例如，当您拨到us.example.com时，您希望它从基于美国的服务器传出）。然后，确保您拥有出站DialPlanRules的API配置，以便除基于美国的呼叫桥之外的其他呼叫桥能够将呼叫路由到美国呼叫桥（在本例中）。

OutboundDialPlanRule(适用于US Callbridge)

- domain = us.example.com
- sipProxy = <使用DNS SRV/IP或FQDN（如果手动设置）时为空>
- scope = callbridge
- callbridge = <UScallbridge-ID>

OutboundDialPlanRules（适用于所有必须允许进行该呼叫的非美国呼叫网桥）（每个呼叫网桥需要一个）

- domain = us.example.com
- sipProxy = <IP — 或FQDN-of-US-Callbridge>
- scope = callbridge
- callbridge = <non-US-callbridge-ID>

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有可用于此配置的特定故障排除信息。

相关信息

- [技术支持和文档 - Cisco Systems](#)
 - [协作解决方案分析工具](#)
 - [CMS文档](#)
-

NOTE:有关配置示例，请参阅以下指南：

- [配置和集成CMS单一组合指南](#)
- [配置思科会议服务器和CUCM指南](#)