了解会议服务器上的呼叫路由逻辑

目录

简介

本文档介绍思科Meeting Server (CMS)（以前称为Acano产品）的呼叫路由逻辑，该逻辑分为多个呼叫路由表。本文档介绍呼叫通过这些呼叫路由表可以采取的不同阶段和方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Meeting Server呼叫网桥组件。

使用的组件

本文档中的信息基于2.3.x版的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Meeting Server (CMS)的呼叫路由逻辑是什么？

CMS上的呼叫路由涉及几个不同的呼叫路由表。通过可下载的流程图，您可以遵循到达CMS的每个呼叫的呼叫路由逻辑。这适用于所有类型的呼叫：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，除非另有说明。

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)计划的出站呼叫或CMA客户端呼出)，其中会绕过呼叫转发表功能。

以下是CMS中呼叫路由过程的顺序：

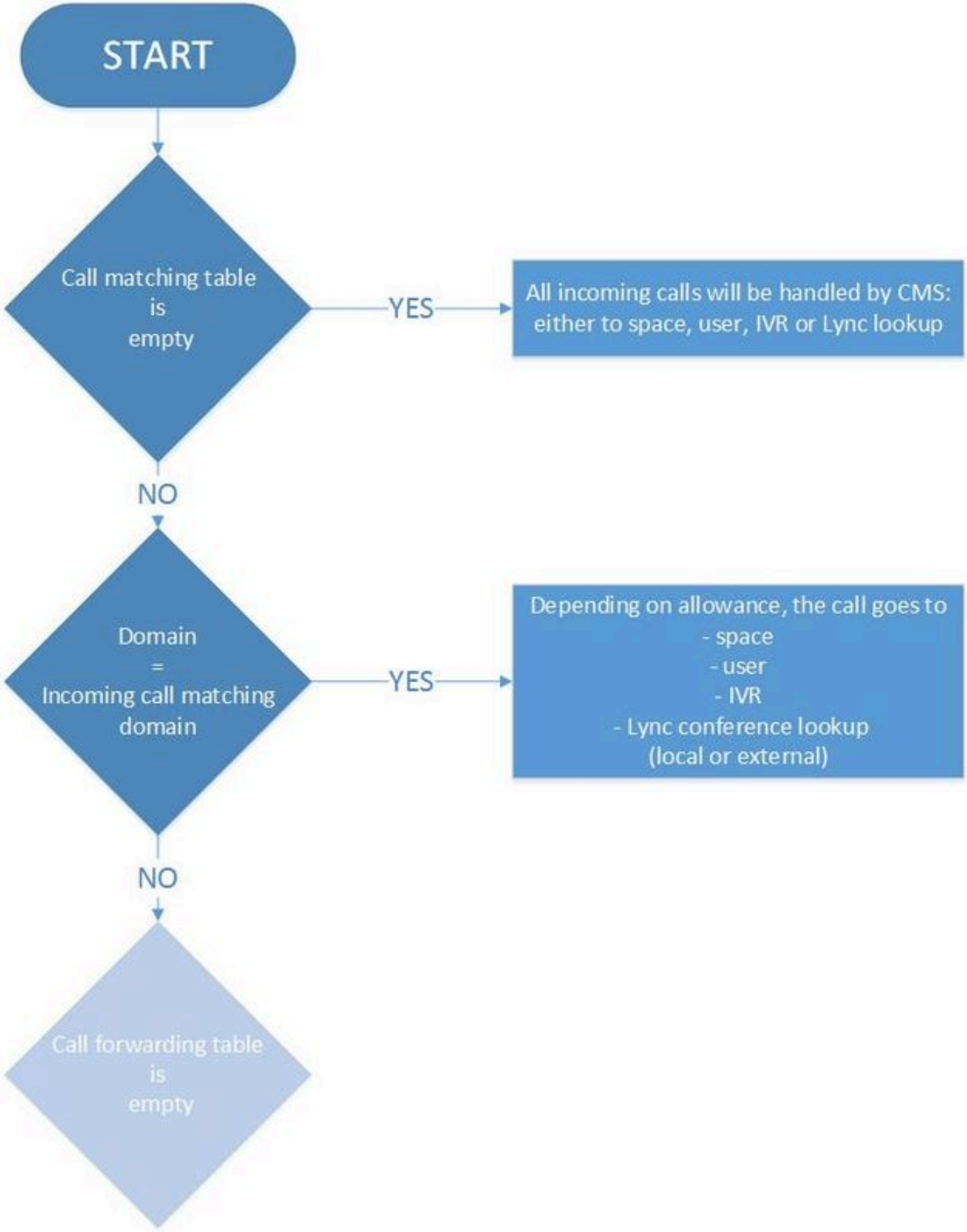
1. 来电匹配表
2. 传入呼叫转发表
3. 出站呼叫表

本文档后面会更详细地介绍每个表，其中包括仅显示相关部分的图像。

注意：CMS仅根据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，就像在具有目录号码路由（路由模式）的Cisco Unified Communications Manager (CUCM)上一样。

注：每个表都是由优先级属性设置的排序列表。优先级越高，表示它会尝试先进行匹配。如果不匹配，则继续列表中的下一条规则。作为一般经验法则，给更一般性的规则（如匹配任何域的*）比更具体的规则具有更低的优先级。这样，特定规则会首先处理，您可能会回退到更通用的规则。

步骤1:来电匹配表

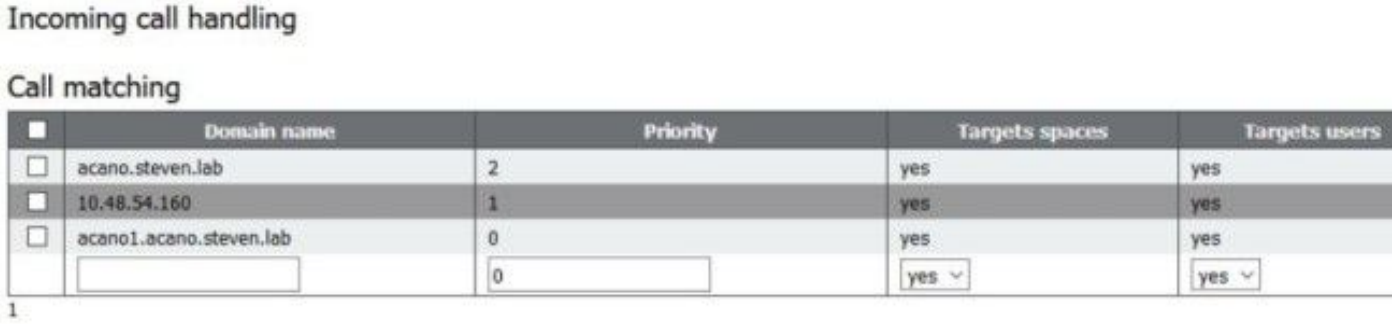


这是CMS确定入站呼叫是否发往思科Meeting Server本身并需要在其上进一步处理的流程中的第一步，或者该呼叫是发往另一个系统的呼叫，其中CMS是交互呼叫的代理并处理媒体和信令（例如，到标准SIP终端的Skype网关呼叫，反之亦然）。

它检查传入URI的域部分是否与传入匹配表匹配。如果匹配，则它可以将呼叫路由到空间、用户、IVR或根据此拨号方案规则的配置执行Lync会议查找（内部或外部）。该表不允许使用通配符域，它要求完全匹配。

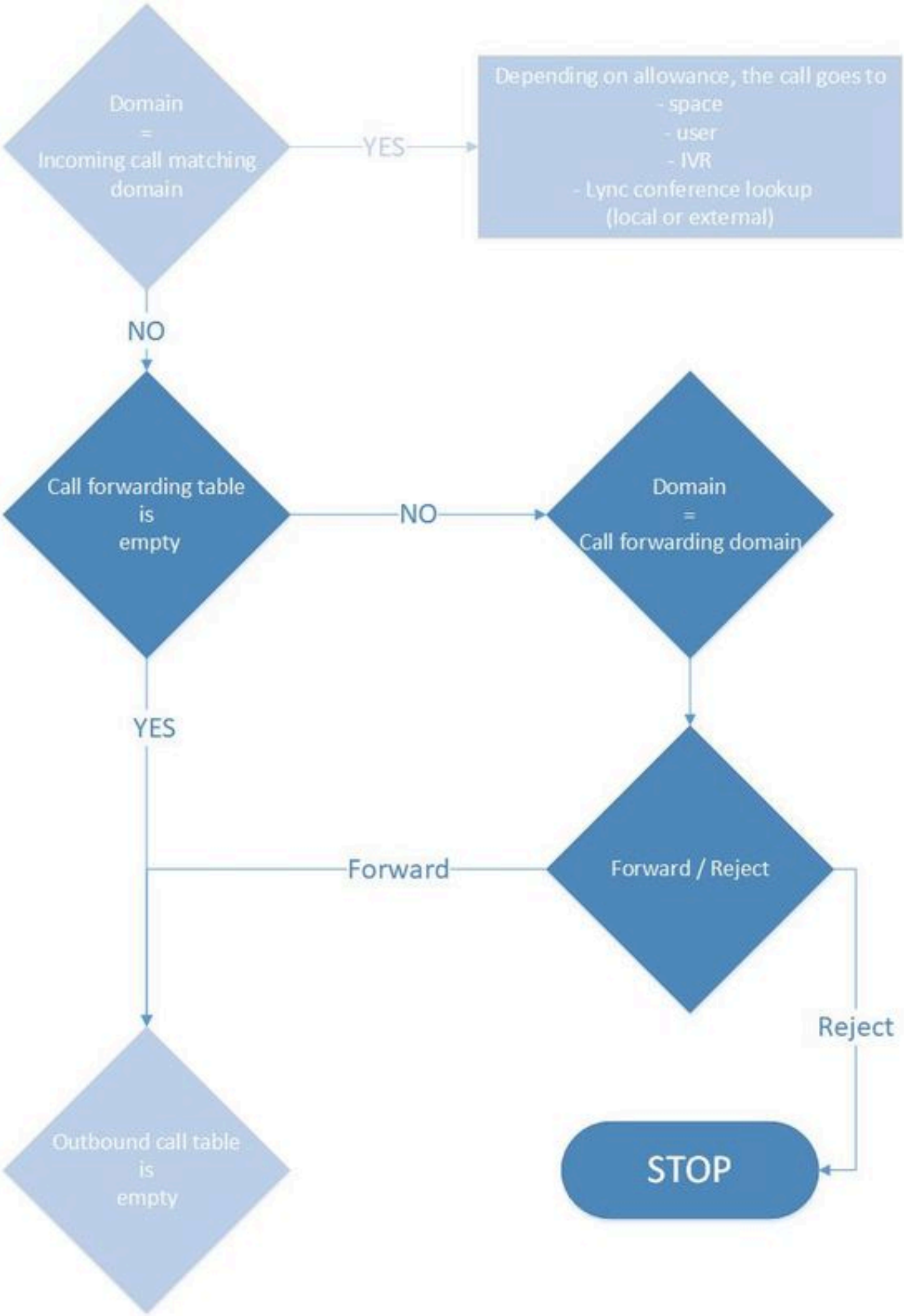
注意：如果未配置任何传入呼叫匹配域，则CMS会接受来自SIP或Lync且位于Callbridge上的所有传入URI。对于CMA客户端（WebRTC或胖客户端），虽然它接受呼叫，但不会自动路由到正确的空间或用户。因此，在这种情况下使用CMA客户端拨号到空格或用户时，在正确的域中输入是很重要的。

例如，图中显示了一个呼叫匹配表(该表只显示了Targets spaces和Targets users选项，以便简要说明)：



此处，域设置为acano.steven.lab，客户端通常拨打此域。但是，它还允许临时呼叫或来自CUCM的特定SIP路由模式（或Expressway搜索规则），这些模式仅通过表中的第一个和第二个回退规则来定位特定Callbridge（如果是集群），这些规则与Callbridge的IP地址（本例中为10.48.54.160）或Callbridge的完全限定域名(FQDN)（本例中为acano1.acano.steven.lab）匹配。

第二步：传入呼叫转发表



如果呼叫未命中传入呼叫匹配表中的任何规则，或者没有匹配来让呼叫继续（例如，用户拨打了不

参与者之间的网关的状态，例如没有任何呼叫转发规则。假设传入呼叫的域在传入呼叫匹配表上不匹配，或者域匹配，但在空间、用户或IVR（或Skype会议）上不匹配，则呼叫不会相对于出站呼叫表转发。

注意：这对CMA客户端（胖客户端和WebRTC）确实会发生，因为它们能够进行出站呼叫（3.0中的*Web应用无法进行出站呼叫，而是由Callbridge发出的CMS空间发出的呼叫）。同样，通过API（例如，在TMS预先安排的会议中）进行CMS上的出站呼叫也可以正常工作。一般来说，从CMS本身（直接或通过CMA的CMS）发起的呼叫不能遵循呼叫转移逻辑。

在事件日志中，您可以看到突出显示的forwarding消息，例如，当CMS用作SIP和Skype呼叫的网关时。在此之前，您可以看到来电呼叫和之后的去电呼叫。

<#root>

```
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，则事件日志不会明确显示此规则。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。

<#root>

```
2018-10-04  06:47:12.482  Info     call 790:
```

incoming

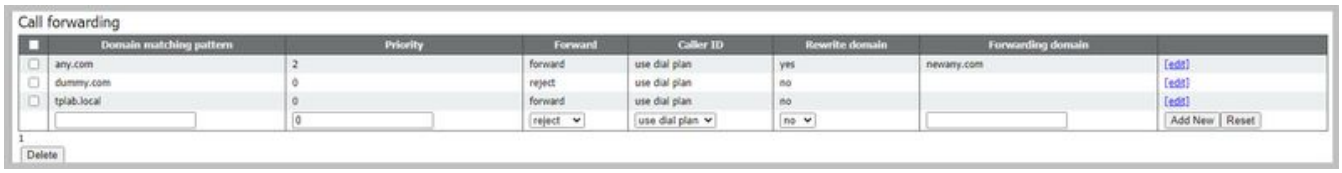
```
SIP call from "sip:1060@10.48.36.215" to local URI "sip:stejanss@any.com"
2018-10-04  06:47:12.495  Info     call 790: ending; local teardown, destination URI not matched - not
```

对于通过TMS计划会议发起的CMA客户端呼叫或来自CMS的出站呼叫，事件日志中没有传入呼叫。呼叫会立即进入出站拨号方案表，呼叫转发表不会处理该呼叫。

在呼叫转发表中，还有另外两个配置选项：重写域和呼叫方ID。

重写域

通过此选项，您可以将入站呼叫的域重写为其他域，并更改SIP消息SIP请求URI的域部分以及To报头。



例如，利用此映像上的配置，对于域为any.com但在传入呼叫匹配表中没有匹配项（在空间、用户、IVR或Skype会议上）的入站呼叫，此处显示事件日志（启用SIP跟踪）：

<#root>

```
2018-10-04  07:02:24.818  Info      SIP trace: connection 0: incoming SIP TCP data from 10.48.36.215:564
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=z9hG4bK53e4c4ce
2018-10-04  07:02:24.818  Info      SIP trace: From: "EX60 Steven" <sip:1060@steven.lab>;tag=742103~ee54
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
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=z9hG4bKefc98b81a
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=2aa2a49bba2
```

在此转接呼叫线路中，它显示已发生的修改。如果您没有启用SIP跟踪，仍然会显示对any.com到newany.com的修改。

此域重写的最常见用法是本地使用Lync与CMS集群的集成，建议您将出站规则中的联系人报头和发件人报头设置为Lync/Skype，以连接到Callbridge特定的完全限定域名(FQDN)。这是因为以下路由规则：

- Skype将对话（例如，邀请- 200 OK后的ACK）发送到其从CMS收到的200 OK中指定的联系人标头。对于从Skype到CMS的入站连接，Skype首先发送NEGOTIATE SIP消息，在To标头中包含一个ms-fe标头，该标头指定如何在INVITE上的200 OK应答中填充联系人标头（因为它使用同一TCP信道）
- Skype将新对话（如内容共享，因为这是一个单独的呼叫，或者未接呼叫时的回叫）发送到原始邀请的From报头

在重写域时，它与来自Lync呼叫的回叫相关。未接的INVITE的From标头指向呼叫来自的特定Callbridge。然后，Lync会发送一个新请求(INVITE)，其中包含与Callbridge FQDN匹配的SIP请求URI。 然后，会通过这些重写规则将其转换为SIP域。 呼叫被转发后，会使用出站规则前往注册SIP终端的CUCM或Expressway-C。

主叫方 ID

此处有两个可在转发规则上设置的选项。此设置设置为pass through，然后不对出站INVITE的“发件人”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“发件人”报头。此设置与域是否重写无关，因为仅涉及SIP请求URI以及出站INVITE的To标头。

例如，与之前进行的呼叫相同，但现在newany.com有一个出站拨号方案规则（与对传入呼叫转发表进行重写后）设置为一个Lync类型呼叫（例如，Ms-Conversation-ID作为额外SIP报头）。相应地，系统会填写本地发件人域（和本地联系人域），以指向先前所示的Lync呼叫的Callbridge FQDN。然后，这将反映出站SIP INVITE的发件人和联系人报头的更改。 如图所示，它们填充有相同的值，可以根据需要单独选择。

Outbound calls

Filter Submit Query

■	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority
□	steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	5
□	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4

<#root>

```
2018-10-12  09:09:24.488  Info     SIP trace: connection 28: incoming SIP TCP data from 10.48.36.215:44
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=z9hG4bKf4a230ec
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
2018-10-12  09:09:24.508  Info     SIP trace: connection 33: outgoing connection successful, 10.48.80.7
2018-10-12  09:09:24.510  Info     SIP trace: connection 33: outgoing SIP TCP data to 10.48.36.46:5060
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=z9hG4bK15bdde97a
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

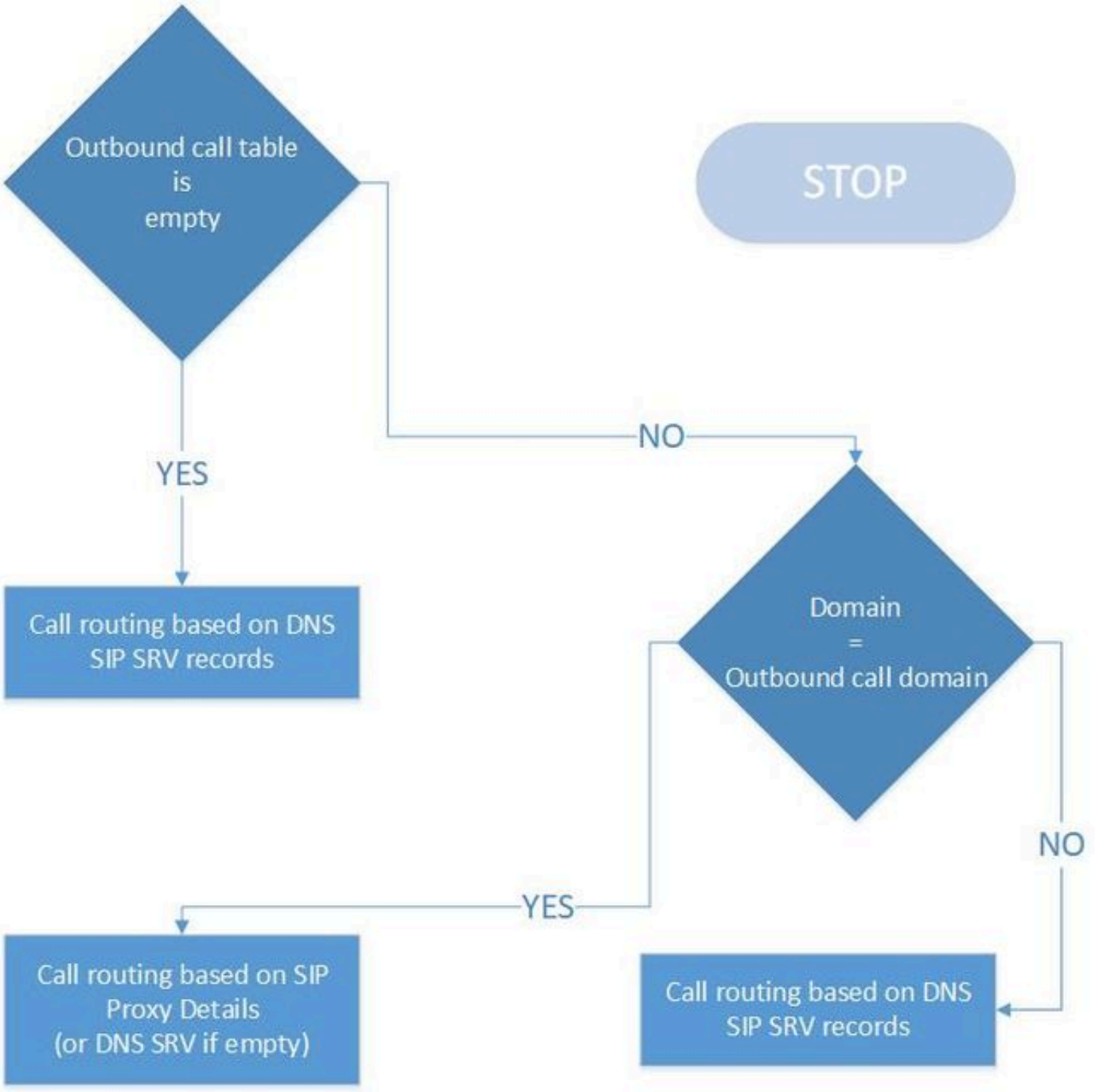
```
;transport=tcp>
2018-10-12  09:09:24.510  Info     SIP trace:

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
```

如果转发规则仅设置为pass through，则在From报头上不会出现任何修改，正如从上一个示例中看到的那样（在这种情况下，转发规则设置为pass through）。当CMS启动新的callLeg时，始终会修改联系人报头，因此必须添加联系人报头到自身。

可以使用不同主叫方ID和本地联系人域以及本地发件人域组合。出站SIP INVITE上的From报头按表中所示构建，入站呼叫使用usera@from.com的From报头进入CMS。

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

第三步：出站呼叫表



这是呼叫路由逻辑中将呼叫发出到不同服务器的最后一个表，如下所示：

- 传入呼叫不在本地处理（在传入呼叫匹配域上）。
- 它是来自CMS空间的出站呼叫(通过CMA或通过API，以用于TMS安排的会议，或思科会议管理器(CMM)指示的出站呼叫)或来自CMA客户端的出站呼叫。

从图中您可以看到逻辑相对简单。如果表中没有任何条目，它仍然允许出站呼叫，但假设CMS服务器能够解析SIP请求URI中提到的该特定域的SIP SRV记录(_sips._tcp / _sip._tcp / _sip._udp)。如果表不为空，但拨号域不匹配，则会执行相同的DNS查找逻辑。如果域中存在匹配项，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进行的出站呼叫，可以通过两种方式执行此操作。没有任何DNS SRV记录（或者无法通过CMS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。

下图显示了一个出站呼叫表示例：

Outbound calls

Filter Submit Query

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

1

在末尾使用常规<match all domains>规则，在没有填写SIP代理的情况下使用第一个到steven.lab域的规则（因此它依赖于DNS SRV记录）。

请注意，这是一个首先覆盖的具有更高优先级值的有序列表。如果您匹配一条规则并将行为设置为“停止”，则在匹配规则后呼叫将不通过表中的其余部分，并且（例如）在该SIP代理无法路由呼叫时呼叫失败。当该设置被设置为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，可以为同一域中的每个规则指定不同的SIP代理。

本地联系人域和本地发件人域的设置将在传入呼叫转发表的上一节中介绍。中继类型允许您指定需要进行的呼叫类型，可以是标准SIP、Lync或Avaya，具体取决于接收系统。

加密字段确定呼叫的信令必须解密还是加密。但请注意，这并不表示任何在Configuration > Call Settings菜单中的SIP media encryption配置设置的媒体加密。在此配置中，您还可以选择自动(Auto)，该选项会首先尝试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，则强烈建议对其进行相应定义，以避免由于回退进程导致的任何呼叫建立延迟。

在DNS跟踪和SIP跟踪设置为detailed的情况下，执行steven.lab呼叫的日志文件输出示例（在重写传入呼叫转发表上的域之后），显示了查询的SRV记录，以及将Encryption设置为Auto时的回退机制。

<#root>

```
2018-10-12  11:25:16.168  Info     call 821: incoming SIP call from "sip:1060@steven.lab" to local URI
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 82
2018-10-12  11:25:16.181  Info     DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for call 82

succeeded

; results: 1
2018-10-12  11:25:16.181  Info     DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for call 82

10.48.36.215:5061

2018-10-12  11:25:16.181  Info     SIP trace: connection 45: allocated for outgoing encrypted connectio
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
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

10.48.36.215:5060

2018-10-12  11:25:16.202  Info     SIP trace: connection 46: allocated for outgoing connection to 10.48
2018-10-12  11:25:16.203  Info     SIP trace: connection 46: outgoing connection successful, 10.48.80.7
2018-10-12  11:25:16.205  Info     SIP trace: connection 46: outgoing SIP TCP data to 10.48.36.215:5060
2018-10-12  11:25:16.205  Info     SIP trace: INVITE sip:stejanss@steven.lab SIP/2.0
```

注意：对于具有多个呼叫网桥的集群环境，您可以通过API配置每个呼叫网桥的出站拨号方案规则，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都从特定域的一个特定Callbridge发出(例如，当您拨号到us.example.com时，您希望它从您基于美国的服务器发出)。然后确保您拥有outboundDialPlanRules的API配置，以便基于美国的呼叫网桥以外的其他Callbridge能够将该呼叫路由到US Callbridge（在本例中）。

OutboundDialPlanRule(适用于美国Callbridge)

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

OutboundDialPlanRules（适用于必须允许进行该呼叫的所有非美国Callbridge）（每个

Callbridge需要一个规则）

- 域= us.example.com
- sipProxy = <IP-or-FQDN-of-US-Callbridge>
- 范围= 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

注意：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Meeting Server和CUCM指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。