Meeting Serverのコールルーティングロジックについて

内容

はじめに

このドキュメントでは、複数のコールルーティングテーブルに分割されるCisco Meeting Server(CMS)（以前のAcano製品）のコールルーティングロジックについて説明します。このドキュメントでは、コールがこれらのコールルーティングテーブルを通過できるさまざまな段階とシナリオについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Meeting Server Call Bridgeコンポーネント。

使用するコンポーネント

このドキュメントの情報は、バージョン2.3.xのCisco Meeting Serverに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Cisco Meeting Server(CMS)のコールルーティングロジックとは何ですか。

CMSのコールルーティングには、いくつかの異なるコールルーティングテーブルが含まれます。ダウンロード可能なフローチャート（登録ユーザ専用）を使用して、CMSに到達した各コールのコールルーティングロジックに従うことができます。これは、Cisco Meeting App（CMA – シッククライアントまたはWebRTC）、標準Session Initiation Protocol(SIP)コール、または特に指定のない限りMicrosoft SIPコールなど、すべてのタイプのコールに有効です。

注：唯一の例外は、コール転送テーブルがバイパスされるCMSが開始したコール(TelePresence Management Suite(TMS)のスケジュールされた発信コールに対して直接CMSを使用するか、またはCMAクライアントコールを発信する)です。

CMSでのコールルートプロセスの順序を次に示します。

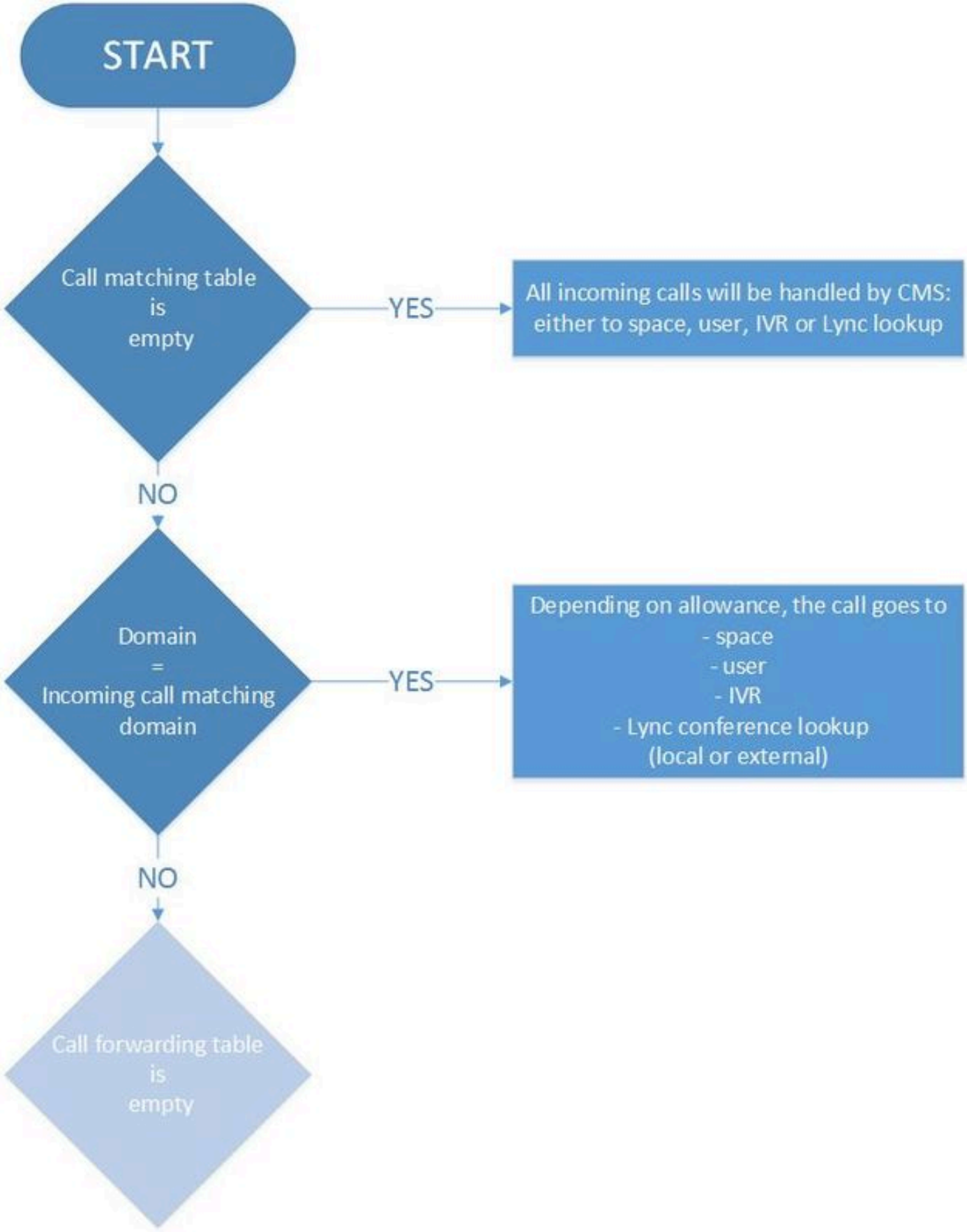
1. 着信コール照合テーブル
2. 着信コール転送テーブル
3. 発信コールテーブル

各テーブルについては、このドキュメントの後半で詳しく説明します。各テーブルには、の関連部分だけを示すイメージが含まれています。

注:CMSはドメインルーティングに基づいてのみコールルーティングを実行します。したがって、Uniform Resource Identifier(URI)の右側(RHS)に基づきます。電話番号ルーティング（ルートパターン）を使用するCisco Unified Communications Manager(CUCM)のように、URIの左側(LHS)に基づくコールルーティング機能はありません。

注：各テーブルは、priority属性で設定された順序付きリストです。プライオリティの高いパケットは、最初に一致を試みることを意味します。一致しない場合は、リスト内の次のルールに進みます。一般的な経験則として、より一般的な規則（どのドメインにも一致する*など）には、より具体的な規則よりも低い優先順位を与えます。これにより、特定のルールが最初に処理され、より一般的なルールにフォールバックする可能性があります。

ステップ 1：着信コール照合テーブル



これは、CMSが着信コールがCisco Meeting Server自体を宛先とし、それ以上の処理が必要かどうかを判断するプロセスの最初のステップです。または、着信コールが別のシステムを宛先とし、コールをインターワーキングし、メディアとシグナリングの両方を処理するエージェント（Skypeゲートウェイコールと標準SIPエンドポイントの間）であるかどうかを判断します。

着信URIのドメイン部分が着信マッチングテーブルに一致するかどうかを確認します。一致する場合、このダイヤルプランルールの設定に従って、コールをスペース、ユーザ、IVRにルーティングするか、Lync会議ルックアップ（オンプレミスまたはオフプレーム）を実行できます。このテーブルでは、ワイルドカードドメインは許可されません。完全に一致する必要があります。

注：ドメインに一致する着信コールが設定されていない場合、CMSはコールブリッジに着信するSIPまたはLyncコールからのすべての着信URIを受け入れます。CMAクライアント（WebRTCまたはシッククライアント）の場合、コールは受け入れますが、正しいスペースまたはユーザに自動的にルーティングされません。したがって、この場合は、CMAクライアントを使用してスペースまたはユーザにダイヤルするときに、正しいドメインに入力することが重要です。

たとえば、図にはコールマッチングテーブルが示されています(簡略化のため、Targets spacesとTargets usersオプションのみが表示されています)。

Incoming call handling

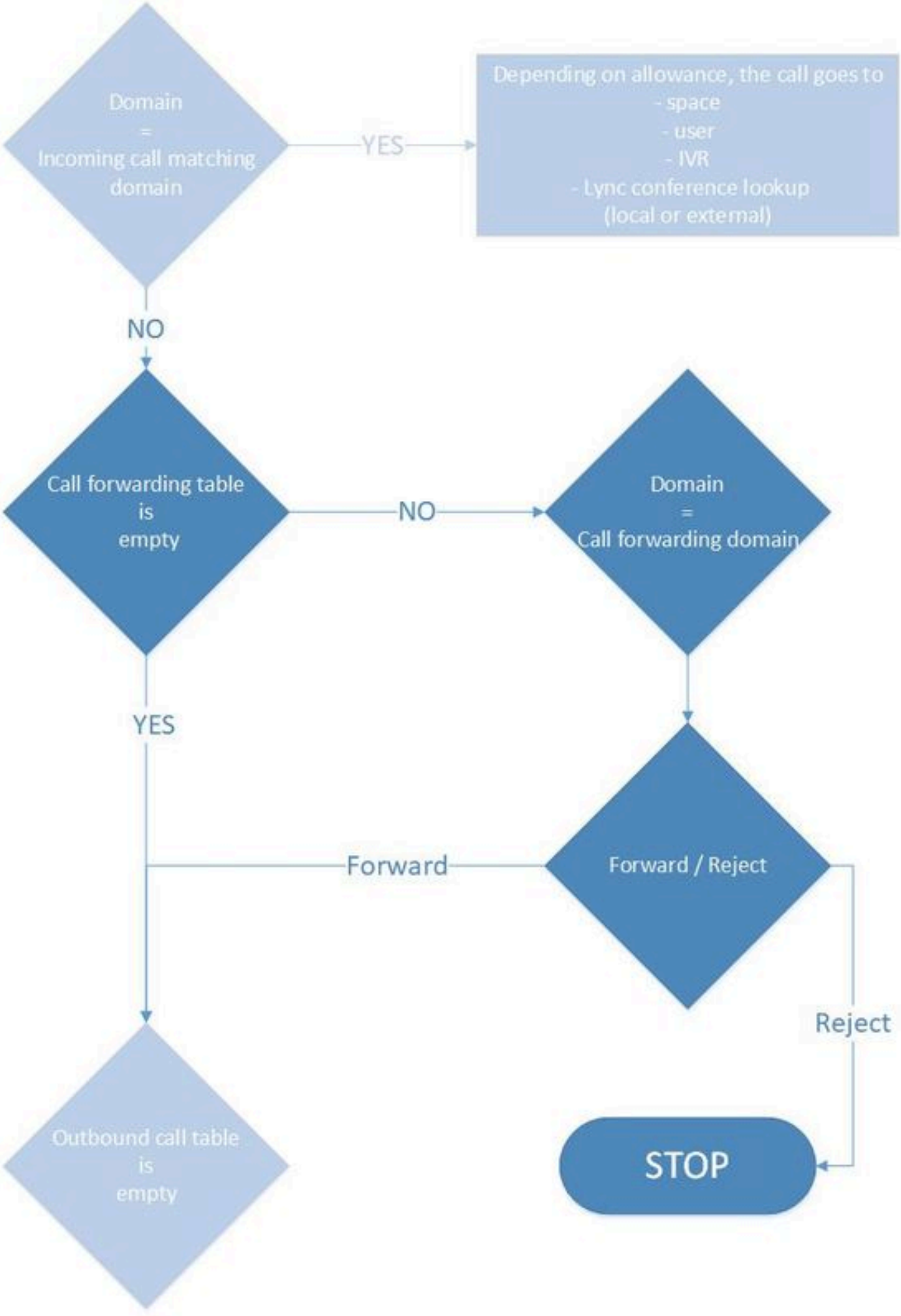
Call matching

	Domain name	Priority	Targets spaces	Targets users
☐	acano.steven.lab	2	yes	yes
☐	10.48.54.160	1	yes	yes
☐	acano1.acano.steven.lab	0	yes	yes
		0	yes	yes

1

ここでは、ドメインはクライアントが通常ダイヤルするacano.steven.labとして設定されています。ただし、テーブル内の最初と2番目のフォールバックルールによって、コールブリッジのIPアドレス（この場合は10.48.54.160）またはコールブリッジの完全修飾ドメイン名(FQDN)（この場合はacano1.acano.steven.lab）のいずれかに一致する特定のコールブリッジ（クラスタの場合）のみを対象とするCUCM（またはExpressway検索ルール）からのアドホックコールまたは特定のSIPルートパターンも可能です。

ステップ 2：着信コール転送テーブル



コールが着信コール照合テーブルのいずれのルールにも一致しなかった場合、またはコールの

たとえば、次の図の設定では、ドメインany.comの着信コール（スペース、ユーザ、IVR、またはSkype会議のいずれか）に対するイベントログ（SIPトレースが有効）が、着信コール照合テーブルの一致なしで次のように表示されています。

<#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
```

この転送コール回線では、発生した変更が表示されます。SIPトレースを有効にしていない場合でも、newany.comへのany.comの変更が表示されます。

ドメインのこの書き換えの最も一般的な用途は、オンプレミスのLyncとCMSクラスタの統合で、発信ルールの連絡先ヘッダーとFromヘッダーをLync/Skypeにcallbridge固有の完全修飾ドメイン名(FQDN)に設定することを推奨します。これは、次のルーティングルールが原因です。

- Skypeは、ダイアログ内の新しいトランザクション（たとえば、INVITE - 200 OKの後のACKなど）を、CMSから受信した200 OKで指定された連絡先ヘッダーに送信します。SkypeからCMSへのインバウンド接続の場合、Skypeは、最初に、連絡先ヘッダーをINVITEの200 OK応答に入力するする方法ををを指定するするms-feヘッダーをををを含含含含するSIPメッセージをを送信します
- Skypeは、元のINVITEのFromヘッダーに新しいダイアログ（個別のコールであるためコンテンツ共有、不在着信の場合はコールバックなど）を送信します

ドメインが書き換えられると、Lyncコールからのコールバックに関連します。不在着信したINVITEのFromヘッダーは、コールの発信元の特定のコールブリッジを指します。Lyncは、callbridge FQDNと一致するSIP要求URIを使用して新しい要求(INVITE)を送信します。 その後、これらの書き換えルールによってSIPドメインに変換されます。 コールが転送されると、SIPエンドポイントが登録されているCUCMまたはExpressway-Cへの発信ルールが使用されます。

発信者 ID

転送ルールに設定できるオプションは2つあります。パススルーに設定されているのに、発信INVITEのFromヘッダーは変更されないか、またはダイヤルプランを使用するように設定されています。これにより、システムは発信ルールに従ってFromヘッダーを変更できます。この設定は、SIP要求URIと発信INVITEのToヘッダーに関係するドメインの書き換えがあるかどうかには関係

ありません。

たとえば、以前と同じコールが行われましたが、現在はnewany.comへの発信ダイヤルプランルールが（着信コール転送テーブルが書き換えられた後のように）Lyncタイプのコール（追加のSIPヘッダーとしてのMs-Conversation-IDなど）として設定されています。適切な手順として、Lyncコールに対して先に示したように、コールブリッジFQDNを指すようにローカルの発信元ドメイン（およびローカルの連絡先ドメイン）が入力されます。次に、この変更は発信SIP INVITEのFromヘッダーとContactヘッダーの変更に反映されます。 図に示すように、これらは同じ値で入力され、要件に応じて個別に選択できます。

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:
```

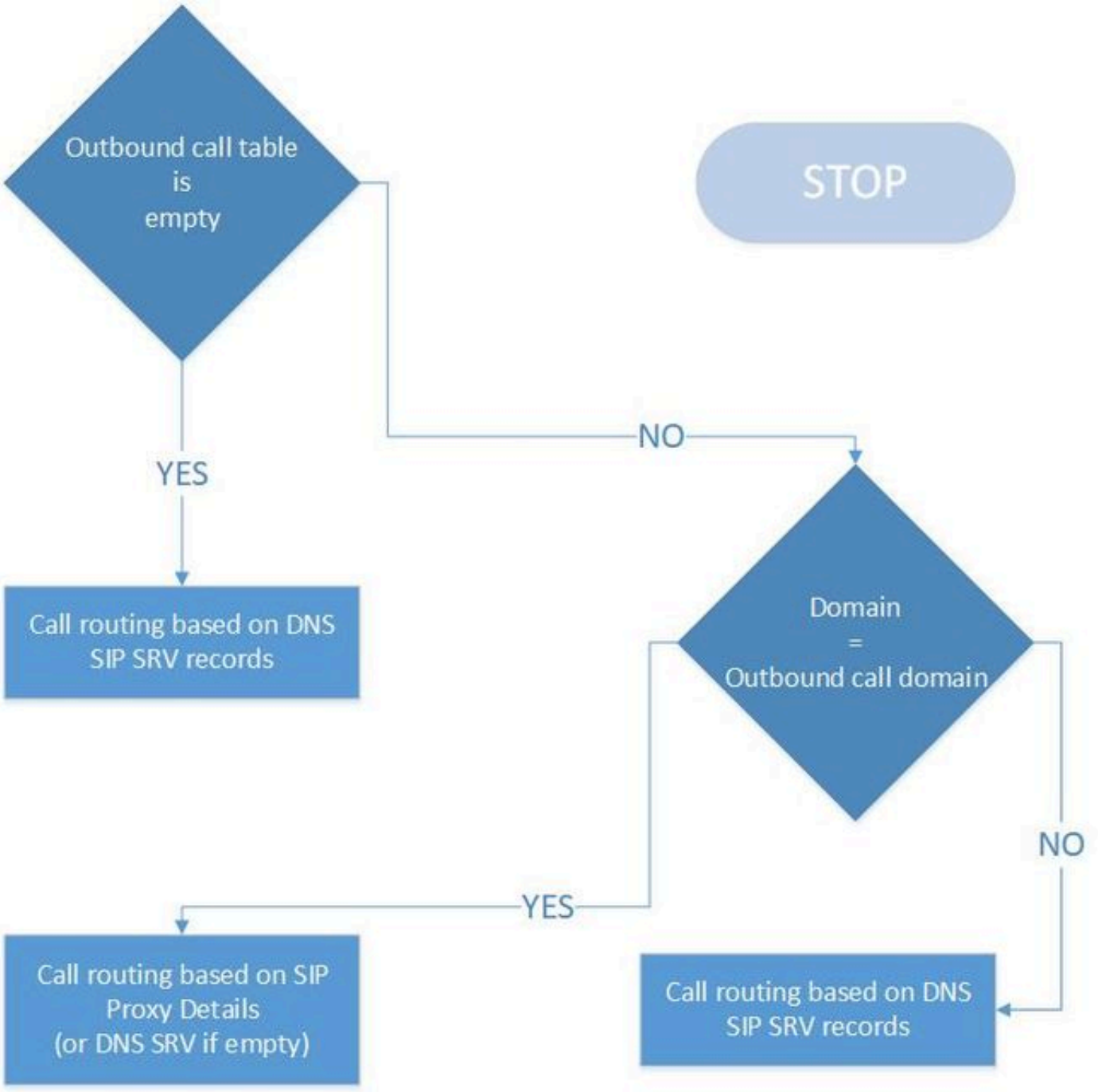
```
Contact

: <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
```

転送ルールが単にパススルー時に設定される場合、前の例と同様にFromヘッダーにも変更はありません（この場合、転送ルールにパススルーが設定されています）。連絡先ヘッダーは、CMSが新しいcallLegを開始し、それ自体に連絡先ヘッダーを追加する必要があるため、常に適合されます。

発信者ID、ローカル連絡先ドメイン、およびローカル発信元ドメインのさまざまな組み合わせを使用できます。発信SIP INVITEのFromヘッダーは、着信コールがusera@from.comのFromヘッダーを使用してCMSに入る表に示すように作成されます。

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>

ステップ 3：発信コールテーブル



これは、コールルーティングロジックの最後のテーブルで、次のように別のサーバにコールを発信します。

- 着信コールはローカルで (着信コール照合ドメインで) 処理されません。
- CMSスペースからの発信コール(CMAまたはTMSスケジュール会議の場合はAPI経由、またはCisco Meeting Manager(CMM)が発信コールを指示)またはCMAクライアントからの発信コールです。

図から、ロジックが比較的簡単であることがわかります。テーブル内にエントリがまったくなくても、発信コールは許可されますが、CMSサーバはSIP要求URIで指定された特定のドメインのSIP SRVレコード(_sips._tcp / _sip._tcp / _sip._udp)で解決できると想定されます。テーブルが空ではなく、ダイヤルされたドメインに一致するものがない場合、同じDNSルックアップロジックが実行されます。ドメインに一致がある場合、その特定のルールのロジックに従います。これに

関して、CMAからの発信コール、またはTMSやCMM経由の発信コールをブロックする場合は、2つの方法があります。DNS SRVレコードがない（またはCMSで解決できない）か、これらのコールをコール制御（CUCMやExpresswayなど）にルーティングし、そこでコールをブロックします。

次の図に、発信コールテーブルの例を示します。

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

最後に一般的な<match all domains>ルールを指定し、最初のルールをSIP Proxy to useを指定しないsteven.labのドメインに適用する方法で情報が入力されます（したがって、そのルールはDNS SRVレコードに依存します）。

これは、プライオリティ値が高い順序付きリストであり、最初に説明するプライオリティ値であることに注意してください。BehaviorをStopに設定したルールと一致した場合、そのルールと一致した後に残りのテーブルを介してコールが転送されることはなく、たとえば、そのSIPプロキシがコールのルーティングに失敗した場合はコールが失敗します。この設定がContinueに設定されている場合は、クラスタ内の別のルートまたは別のノードへのフォールバックを許可できます。たとえば、同じドメインのルールごとに異なるSIPプロキシを指定できます。

ローカル連絡先ドメインとローカル発信元ドメインの設定については、着信コール転送テーブルの前のセクションで説明しています。トランクタイプを使用すると、発信する必要があるコールのタイプを指定できます。このタイプは、受信側システムに応じて、標準SIP、Lync、またはAvayaのいずれかになります。

Encryptionフィールドは、コールのシグナリングを暗号化解除する必要があるか、または暗号化する必要があるかを決定します。ただし、この操作は、Configuration > Call Settingsメニューにあ るSIP media encryption設定で設定されているメディア暗号化を意味するものではないことに注意してください。この設定では、オプションでAutoを選択し、暗号化されたシグナリングを使用して最初にコールを発信し、暗号化されていないシグナリングにフォールバックすることもできます。相手側が暗号化されている、または暗号化されていないことがわかっている場合は、それに応じて定義することを強く推奨します。これにより、フォールバックプロセスによるコールセットアップの遅延を回避できます。

DNSトレースとSIPトレースをdetailedに設定したsteven.labへのコール（着信コール転送テーブルのドメインの書き換え後）のログファイルの出力例は、暗号化が自動に設定されている場合のクエリ済みSRVレコードとフォールバックメカニズムを示しています。

<#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：複数のcallbridgeを使用するクラスタ環境の場合、APIを介してcallbridgeを設定し、APIオブジェクトでcallbridge ID（またはcallbridgeGroup ID）を指定すると、callbridgeごとに発信ダイヤルプランルールを設定できます。たとえば、すべてのコールを特定のドメインの1つの特定のcallbridgeから発信するとします(たとえば、us.example.comにダイヤルする場合、USベースのサーバから発信するとします)。次に、USベースの他の各callbridgeがコールをUSのcallbridgeにルーティングできるように、outboundDialPlanRulesのAPI設定があることを確認します（この例の場合）。

OutboundDialPlanRule(US callbridge用)

- ドメイン= us.example.com
- sipProxy = <DNS SRVを使用している場合は空/手動で設定した場合はIPまたはFQDN>
- スコープ= callbridge
- callbridge = <UScallbridge-ID>

OutboundDialPlanRules（そのコールの発信を許可する必要があるすべての非USコールブリッジ用）（コールブリッジごとに1つ必要）

- ドメイン= us.example.com
- sipProxy = <IPまたはFQDNのUSコールブリッジ>
- スコープ= callbridge
- callbridge = <非USコールブリッジID>

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- Collaboration Solutions Analyzerツール
- CMSドキュメント

注：設定例については、次のガイドを参照してください。

- 単一の統合ガイドによるCMSの設定と統合
- Cisco Meeting ServerおよびCUCMの設定ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。