Cisco Jabber DNS Configuration Guide

First Published: February 20, 2014

Last Modified: March 26, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

How the Client Uses Domain Name Servers

Cisco Jabber uses domain name servers to do the following:

- Automatically discover on-premises servers inside the corporate network.
- Locate access points for Expressway Mobile and Remote Access on the public Internet.
- Determine whether the client is inside or outside the corporate network.

How the Client Finds a Name Server

Cisco Jabber looks for DNS records from:

- Internal name servers inside the corporate network.
- External name servers on the public Internet.

When the client’s host computer or device gets a network connection, the host computer or device also gets the address of a DNS name server from the DHCP settings. Depending on the network connection, that name server might be internal or external to the corporate network.

Cisco Jabber queries the name server that the host computer or device gets from the DHCP settings.

How the Client Gets a Services Domain

The services domain is discovered by the Cisco Jabber client in different ways.

New installation:

- User enters an address in the format `username@example.com` in the client user interface.
- User clicks on a configuration URL that includes the service domain. This option is only available in the following versions of the client:

    - Cisco Jabber for Android version 9.6 or later
    - Cisco Jabber for Mac version 9.6 or later
    - Cisco Jabber for iPhone and iPad version 9.6.1 or later

- The client uses installation switches in bootstrap files. This option is only available in the following version of the client:
    - Cisco Jabber for Windows version 9.6 or later

Existing installation:

- The client uses the cached configuration.
- User manually enters an address in the client user interface.

In hybrid deployments the domain required to discover Cisco WebEx domain through CAS lookup may be different to the domain where the DNS records are deployed. In this scenario you set the ServicesDomain to be the domain used to discover Cisco WebEx and set the VoiceServicesDomain to be the domain where DNS records are deployed. The voice services domain is configured as follows:

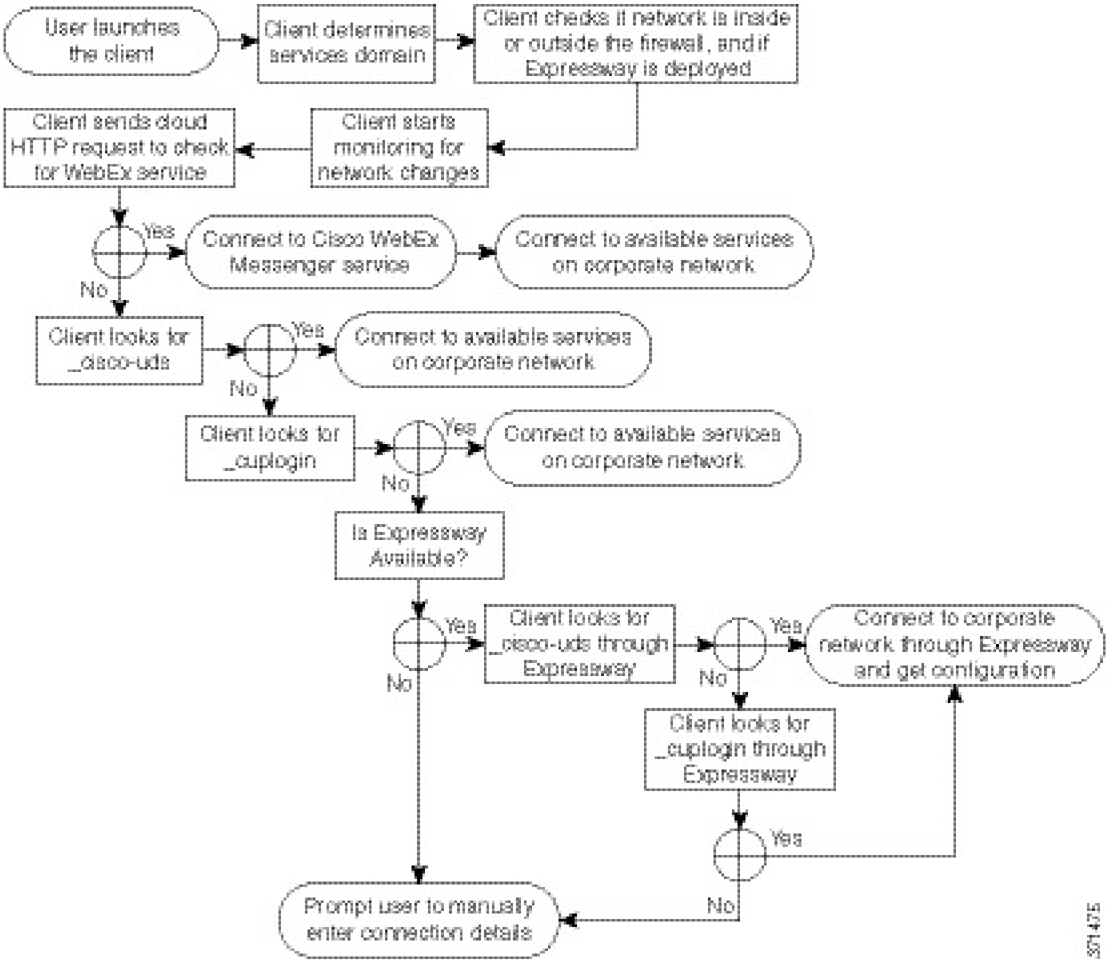
- The client uses the VoiceServicesDomain parameter in the configuration file. This option is available in clients that support the `jabber-config.xml` file.
- User clicks on a configuration URL that includes the VoiceServicesDomain. This option is available in the following clients:
    - Cisco Jabber for Android version 9.6 or later
    - Cisco Jabber for Mac version 9.6 or later
    - Cisco Jabber for iPhone and iPad version 9.6.1 or later
- The client uses the Voice_Services_Domain installation switch in the bootstrap files. This option is only available in the following version of the client:
    - Cisco Jabber for Windows version 9.6 or later

See the appropriate version of the *Installation and Configuration guide*, for more detailed information.

After Cisco Jabber gets the services domain, it queries the name server that is configured to the client computer or device.

How the Client Discovers Available Services

The following diagram illustrates the flow that the client uses to connect to services:


User launches the client
Client determines services domain
Client checks if network is inside or outside the firewall, and if Expressway is deployed
Client starts monitoring for network changes
Client sends cloud HTTP request to check for WebEx service
Yes
Connect to Cisco WebEx Messenger service
Connect to available services on corporate network
No
Client looks for _cisco-uds
Yes
Connect to available services on corporate network
No
Client looks for _cuplogin
Yes
Connect to available services on corporate network
No
Is Expressway Available?
Yes
Client looks for _cisco-uds through Expressway
Yes
Connect to corporate network through Expressway and get configuration
No
No
Client looks for _cuplogin through Expressway
Yes
No
Prompt user to manually enter connection details
371475

To discover available services, the client:

1. Checks if the network is inside or outside the firewall and if Expressway Mobile and Remote Access is deployed. A query is sent to the name server to get DNS Service (SRV) records.
2. Starts monitoring for network changes.

   When Expressway Mobile and Remote Access is deployed, the client monitors the network to ensure that it can reconnect if the network changes from inside or outside the firewall.
3. Issues an HTTP query to a CAS URL for the Cisco WebEx Messenger service.

   This query enables the client to determine if the domain is a valid Cisco WebEx domain.
4. Queries the name server to get DNS Service (SRV) records, unless the records exist in the cache from a previous query.

   This query enables the client to do the following:

   - Determine which services are available.
   - Determine if it can connect to the corporate network through Expressway Mobile and Remote Access.

Note Refer to the latest version of your *Cisco Jabber client Installation and Configuration Guide* for further information on configuring available services.

Client Issues HTTP Query

In addition to querying the name server for SRV records to locate available services, Cisco Jabber sends an HTTP query to the CAS URL for the Cisco WebEx Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Cisco WebEx Messenger service.

When the client gets a services domain from the user, it appends that domain to the following HTTP query:

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=
```

For example, if the client gets `example.com` as the services domain from the user, it issues the following query:

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

That query returns an XML response that the client uses to determine if the services domain is a valid Cisco WebEx domain.

If the client determines the services domain is a valid Cisco WebEx domain, it prompts users to enter their Cisco WebEx credentials. The client then authenticates to the Cisco WebEx Messenger service and retrieves the configuration and UC services configured in Cisco WebEx Org Admin.

If the client determines the services domain is not a valid Cisco WebEx domain, it uses the results of the query to the name server to locate available services.

Note When the client sends the HTTP request to the CAS URL, it uses any configured system proxies. The following limitations apply when using a proxy for these HTTP requests:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are not supported. Use `example.com` instead of `*.example.com` for example.

Client Queries Name Server

When the client queries a name server, it sends separate, simultaneous requests to the name server for SRV records.

The client requests the following SRV records in the following order:

- `_cisco-uds`
- `_cuplogin`
- `_collab-edge`

If the name server returns:

`_cisco-uds` or `_cuplogin`

The client detects it is inside the corporate network and connects to one of the following:

Cisco Unified Communications Manager

If the name server returns `_cisco-uds`.

Cisco Unified Presence

If the name server returns `_cuplogin`.

`_collab-edge`

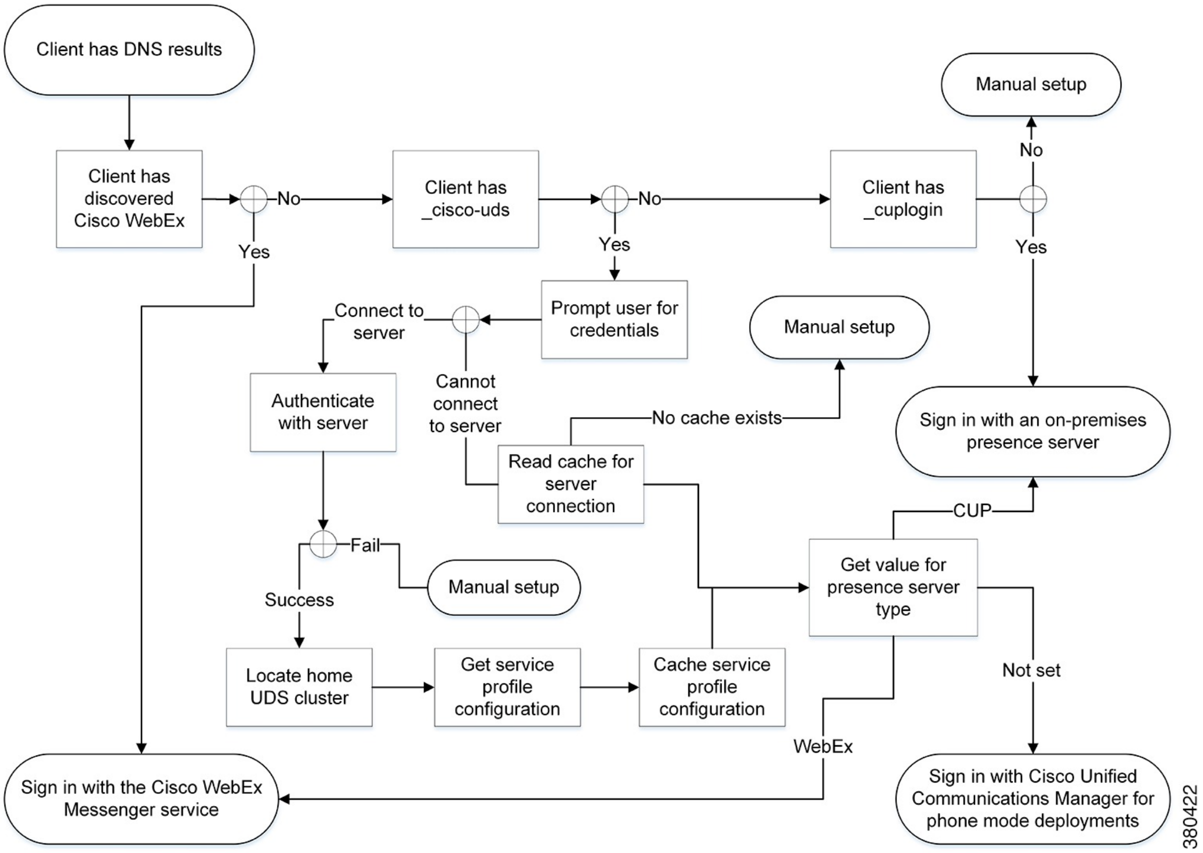
The client attempts to connect to the internal network through Expressway Mobile and Remote Access and discover services.

None of the SRV records

The client prompts users to manually enter setup and sign-in details.

Client Connects to Internal Services

The following diagram illustrates how the client connects to internal services:


Client has DNS results
Client has discovered Cisco WebEx
No
Yes
Client has _cisco-uds
No
Yes
Client has _cuplogin
No
Manual setup
Yes
Prompt user for credentials
Connect to server
Cannot connect to server
Authenticate with server
Fail
Manual setup
Success
Manual setup
No cache exists
Read cache for server connection
Locate home UDS cluster
Get service profile configuration
Cache service profile configuration
Get value for presence server type
CUP
Sign in with an on-premises presence server
Not set
WebEx
Sign in with the Cisco WebEx Messenger service
Sign in with Cisco Unified Communications Manager for phone mode deployments
380422

When connecting to internal services, the goals are to determine the authenticator, sign users in, and connect to available services.

There are three possible authenticators that can get users past the sign in screen, as follows:

Cisco WebEx Messenger Service

Cloud-based or hybrid cloud-based deployments.

Cisco Unified Presence

On-premises deployments in the default product mode. The default product mode can be either full UC or IM only.

Cisco Unified Communications Manager

On-premises deployments in phone mode.

The client connects to any services it discovers, which varies depending on the deployment.

1 If the client discovers that the CAS URL lookup indicates a Cisco WebEx user, the client:

   a Determines that the Cisco WebEx Messenger service is the primary source of authentication.

   b Automatically connects to the Cisco WebEx Messenger service.

   c Prompts the user for credentials.

   d Retrieves client and service configuration.

2 If the client discovers a `_cisco-uds` record, then the client:

   1 Prompts the user for credentials to authenticate with Cisco Unified Communications Manager.

   2 Locates the user's home cluster.

   Locating the home cluster enables the client to automatically get the user's device list and register with Cisco Unified Communications Manager.

Important In an environment with multiple Cisco Unified Communications Manager clusters, you must configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster.

See the appropriate version of the *Cisco Unified Communications Manager Features and Services Guide* to learn how to configure ILS.

   3 Retrieves the service profile.

   The service profile provides the client with the authenticator as well as client and UC service configuration.

   The client determines the authenticator from the value of the **Product type** field in the IM and presence profile, as follows:

   Unified CM (IM and Presence)

   Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence is the authenticator.

WebEx (IM and Presence)

The Cisco WebEx Messenger service is the authenticator.

Note As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service.

As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments. Setting the value of the **Product type** field to **WebEx** may have no practical effect if the client already discovered the WebEx service using a CAS lookup.

Not set

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

4. Sign in to the authenticator.

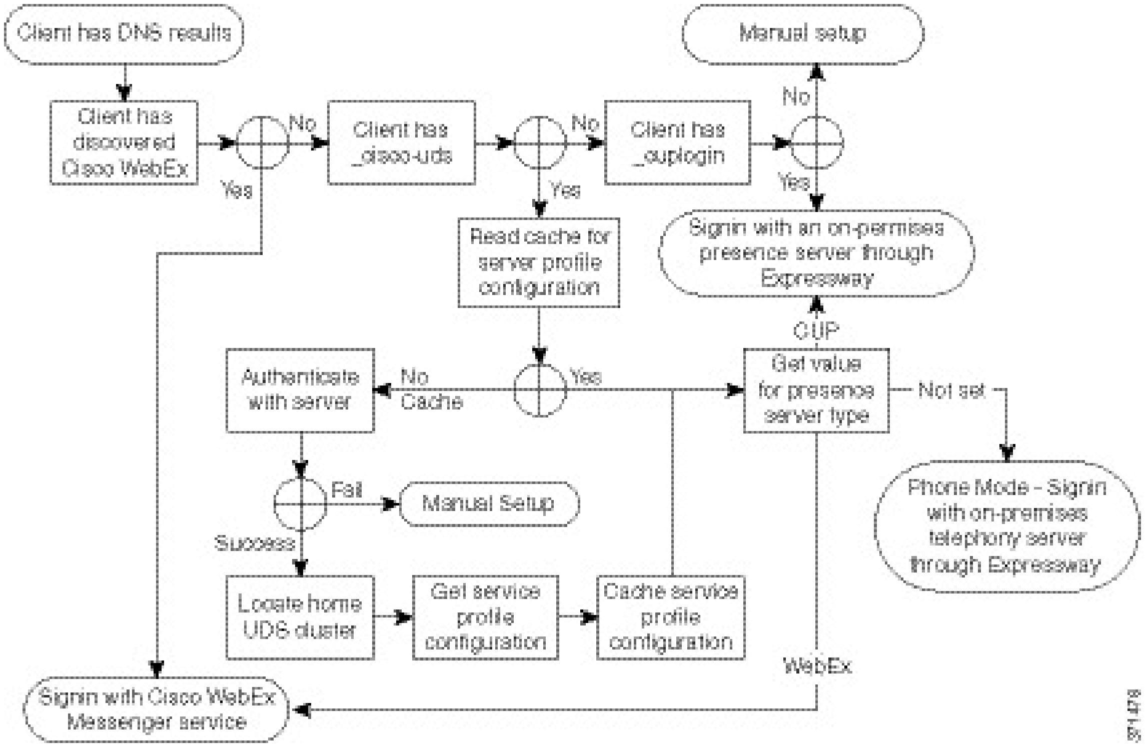
   After the client signs in, it can determine the product mode.

3. If the client discovers a `_cuplogin` record, the client:
   1. Determines that Cisco Unified Presence is the primary source of authentication.
   2. Automatically connects to the server.
   3. Prompts the user for credentials.
   4. Retrieves client and service configuration.

Client Connects through Expressway Mobile and Remote Access

If the name server returns the `_collab-edge` SRV record, then the client attempts to connect to internal servers through Expressway Mobile and Remote Access.

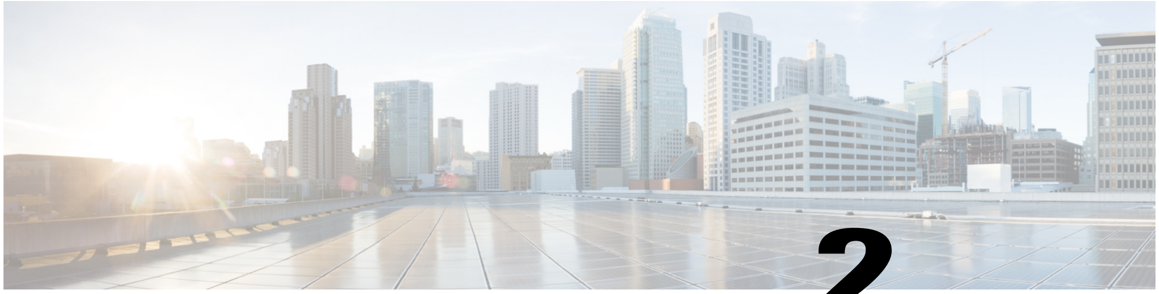
The following diagram illustrates how the client connects to internal services when the client is connected to the network through Expressway Mobile and Remote Access:


Client has DNS results
Client has discovered Cisco WebEx
No
Yes
Client has _cisco-uds
No
Yes
Client has _cuplogin
No
Yes
Manual setup
Signin with an on-permises presence server through Expressway
Read cache for server profile configuration
Yes
No Cache
Authenticate with server
Fail
Manual Setup
Success
Locate home UDS cluster
Get service profile configuration
Cache service profile configuration
CUP
Get value for presence server type
Not set
Phone Mode - Signin with on-premises telephony server through Expressway
WebEx
Signin with Cisco WebEx Messenger service
371478

When the name server returns the `_collab-edge` SRV record, the client gets the location of the Cisco VCS Expressway or Cisco Expressway-E server. The Cisco VCS Expressway or Cisco Expressway-E server then provides the client with the results of the query to the internal name server.

Note The Cisco VCS Control or Cisco Expressway-C server looks up the internal SRV records and provides the records to the Cisco VCS Expressway or Cisco Expressway-E server.

After the client gets the internal SRV records, which must include `_cisco-uds`, it retrieves service profiles from Cisco Unified Communications Manager. The service profiles then provide the client with the user's home cluster, the primary source of authentication, and configuration.



CHAPTER 2

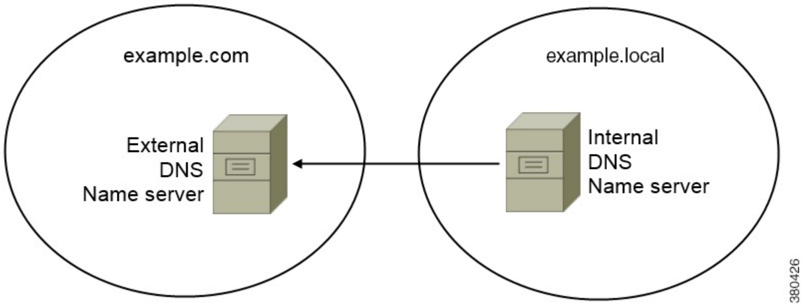
Domain Name System Designs

Where you deploy DNS service (SRV) records depends on the design of your DNS namespace. Typically there are two DNS designs:

- Separate domain names outside and inside the corporate network.
- Same domain name outside and inside the corporate network.

Separate Domain Design

The following figure illustrates a separate domain design:



An example of a separate domain design is one where your organization registers the following external domain with an Internet name authority: `example.com`.

Your company also uses an internal domain that is one of the following:

- A subdomain of the external domain, for example, `example.local`.
- A different domain to the external domain, for example, `example.com`.

With a separate domain design:

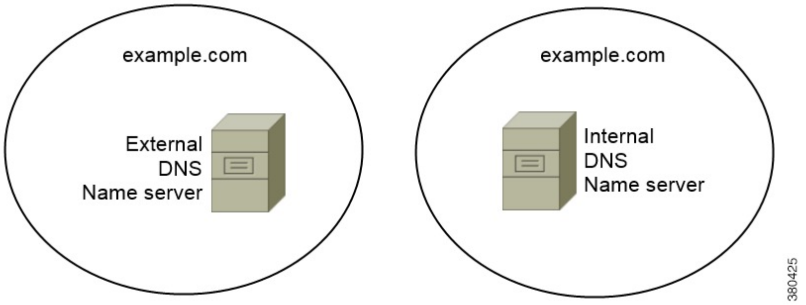
- The internal name server has zones that contain resource records for internal domains. The internal name server is authoritative for the internal domains.
- The internal name server forwards requests to the external name server when a DNS client queries for external domains.
- The external name server has a zone that contains resource records for your organization's external domain. The external name server is authoritative for that domain.
- The external name server can forward requests to other external name servers. However, the external name server cannot forward requests to the internal name server.

Same Domain Design

An example of a same domain design is one where your organization registers `example.com` as an external domain with an Internet name authority. Your organization also uses `example.com` as the name of the internal domain.

Same Domain, Split-Brain

The following figure illustrates a same domain, split-brain domain design:



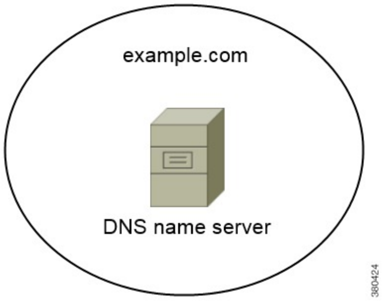
Two DNS zones represent the single domain; one DNS zone in the internal name server and one DNS zone in the external name server.

Both the internal name server and the external name server are authoritative for the single domain, but serve different communities of hosts.

- Hosts inside the corporate network access only the internal name server.
- Hosts on the public Internet access only the external name server.
- Hosts that move between the corporate network and the public Internet access different name servers at different times.

Same Domain, Not Split-Brain

The following figure illustrates a same domain, not split-brain domain design:



In the same domain, not split-brain design, internal and external hosts are served by one set of name servers and can access the same DNS information.

Important This design is not common because it exposes more information about the internal network to potential attackers.

CHAPTER 3

Service (SRV) Records

You deploy multiple DNS SRV records in different locations on your enterprise DNS structure. Understand which records you should provision on which name servers. Review examples of SRV records to ensure a successful deployment.

Deploy SRV Records

The client queries name servers for records in the services domain. The services domain is determined as described in How the Client Discovers Available Services, on page 2.

You must deploy SRV records in each DNS zone for those service domains if your organization has multiple subsets of users who use different service domains.

Deploy SRV Records in a Separate Domain Structure

In a separate name design there are two domains, an internal domain and an external domain. The client queries for SRV records in the services domain. The internal name server must serve records for the services domain. However in a separate name design, a zone for the services domain might not exist on the internal name server.

If the services domain is not currently served by the internal name server, you can:

- Deploy records within an internal zone for the services domain.
- Deploy records within a pinpoint subdomain zone on the internal name server.

Use an Internal Zone for a Services Domain

If you do not already have a zone for the services domain on the internal name server, you can create one. This method makes the internal name server authoritative for the services domain. Because it is authoritative, the internal name server does not forward queries to any other name server.

This method changes the forwarding relationship for the entire domain and has the potential to disrupt your internal DNS structure. If you cannot create an internal zone for the services domain, you can create a pinpoint subdomain zone on the internal name server.

Use a Pinpoint Subdomain Zone

DNS record lookup on the Cisco internal fixed pinpoint subdomain is a legacy feature for service discovery that is only available with the following versions of Cisco Jabber:

- Cisco Jabber for Windows 9.6.x
- Cisco Jabber for iPhone and iPad 9.6.0

Support of the fixed pinpoint subdomain has been replaced in later versions of Cisco Jabber by the support of the new **VoiceServicesDomain** configuration key.

Example configuration using Service Discovery to replace pinpoint subdomains:

- Internal DNS authoritative for : example.local
- External DNS authoritative for : example.com

```
Set VoiceServicesDomain=cisco-uc.example.com
```

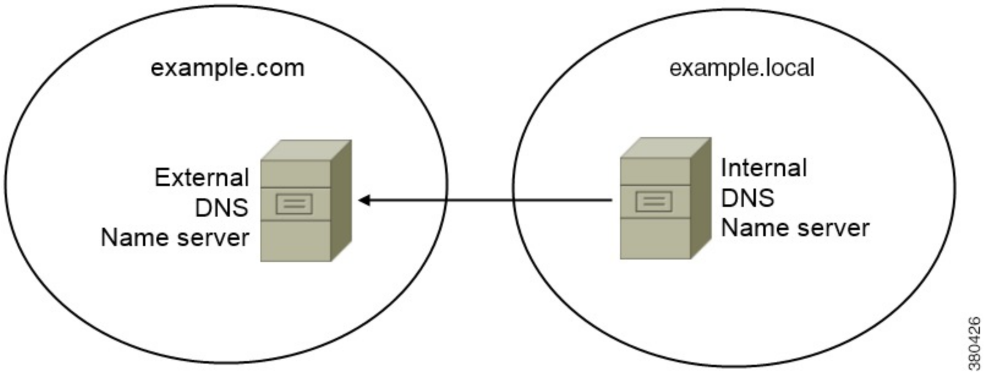
Create a zone on both the internal and external DNS server for `cisco-uc.example.com`.

Create the following SRV records as needed:

- `_cisco-uds._tcp.example.com` (on Internal DNS)
- `_cuplogin._tcp.example.com` (on Internal DNS)

You can create a pinpoint subdomain and zone on the internal name server. The pinpoint zone provides a dedicated location to serve specific records for the pinpoint subdomain. As a result, the internal name server becomes authoritative for that subdomain. The internal name server does not become authoritative for the parent domain, so the behavior of queries for records in the parent domain does not change.

The following diagram illustrates configuration created by the procedure.



In this configuration, the following SRV records are deployed with the internal DNS name server:

- `_cisco-uds._tcp.example.com`
- `_cuplogin._tcp.example.com`

Procedure

Step 1 Create a new zone on the internal name server.

Important You must use the following name for the pinpoint subdomain zone: `cisco-internal.`*`services-domain`*.

The pinpoint subdomain zone responds to queries from hosts on the internal network. However, the domain is a subdomain of the external domain. The first part of the name is a fixed value that the client expects, `cisco-internal`.

Step 2 Deploy the `_cisco-uds` and `_cuplogin` SRV records in the pinpoint subdomain zone.

Before creating a pinpoint subdomain zone

The external name server contains a zone for the parent external domain, `example.com`.

The internal name server contains a zone for the parent internal domain, `example.local`.

The Cisco Jabber Services Domain is `example.com`.

After creating a pinpoint subdomain zone

The external name server contains a zone for the parent external domain, `example.com`.

Internal name server contains the following:

Zone for the parent internal domain, `example.local`.
Zone for the pinpoint subdmain zone, `cisco-internal.example.com`.

The internal name server serves the `_cisco-uds` and `_cuplogin` SRV records from `cisco-internal.example.com`.

When the client queries the name server for SRV records, it issues additional queries if the name server does not return `_cisco-uds` or `_cuplogin`.

The additional queries check for the `cisco-internal.`*`domain-name`* pinpoint subdomain zone.

For example, Adam McKenzie's services domain is `example.com` when he starts the client. The client then issues the following query:

```
_cisco-uds._tcp.example.com
_cuplogin._tcp.example.com
_collab-edge._tls.example.com
```

If the name server does not return `_cisco-uds` or `_cuplogin` SRV records, the client then issues the following query:

```
_cisco-uds._tcp.cisco-internal.example.com
_cuplogin._tcp.cisco-internal.example.com
```

SRV Records

Understand which SRV records you should deploy and review examples of each SRV record.

External Records

The following table lists the SRV record you must provision on external name servers as part of the configuration for Expressway Mobile and Remote Access:

Service Record	Description
`_collab-edge`	Provides the location of the Cisco VCS Expressway or Cisco Expressway-E server. **Note** You must use the fully qualified domain name (FQDN) as the hostname in the SRV record. The client requires the FQDN to use the cookie that the Cisco VCS Expressway or Cisco Expressway-E server provides.

The following is an example of the `_collab-edge` SRV record:

```
_collab-edge._tls.example.com   SRV service location:
          priority       = 3
          weight         = 7
          port           = 8443
          svr hostname   = vcse1.example.com
_collab-edge._tls.example.com   SRV service location:
          priority       = 4
          weight         = 8
          port           = 8443
          svr hostname   = vcse2.example.com
_collab-edge._tls.example.com   SRV service location:
          priority       = 5
          weight         = 0
          port           = 8443
          svr hostname   = vcse3.example.com
```

Internal Records

The following table lists the SRV records you can provision on internal name servers so the client can discover services:

Service Record	Description
`_cisco-uds`	Provides the location of Cisco Unified Communications Manager version 9 and higher. **Remember** In an environment with multiple Cisco Unified Communications Manager clusters, you must configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.
`_cuplogin`	Provides the location of Cisco Unified Presence.

Note You should use the fully qualified domain name (FQDN) as the hostname in the SRV record.

The following is an example of the `_cisco-uds` SRV record:

```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

The following is an example of the `_cuplogin` SRV record:

```
_cuplogin._tcp.example.com      SRV service location:
          priority       = 8
          weight         = 50
          port           = 8443
          svr hostname   = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 5
          weight         = 100
          port           = 8443
          svr hostname   = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
          priority       = 7
          weight         = 4
          port           = 8443
          svr hostname   = cup2.example.com
```