Lab 5: MRA

Lab Written by:
Gabriel Valentino
Collaboration CSE

Technical Overview
Maria del Pilar Muñoz
Video CSE

Reviewed by:
Alejandro Rodriguez
Systems Engineer

Version 1.2

Contents

Objective Statement:

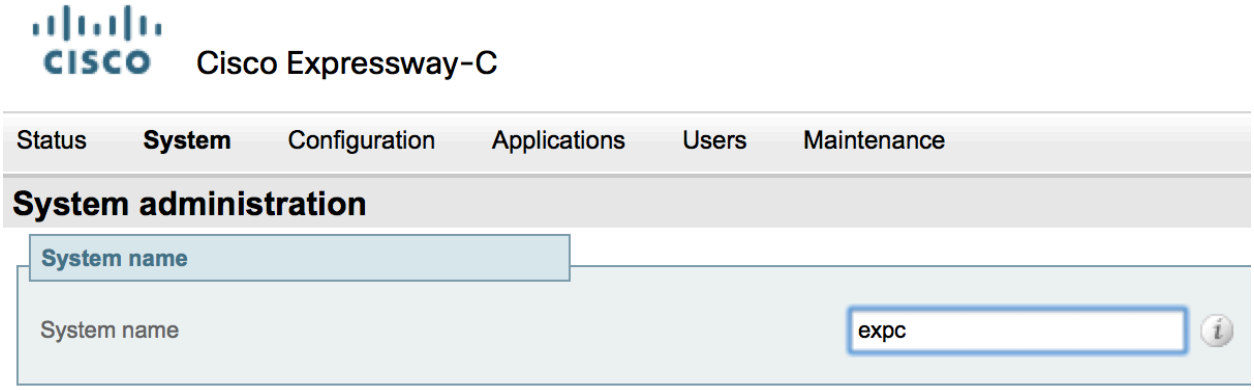
The following chapter will guide through the necessary steps to deploy MRA with expressway. Only certain steps regarding the basic configuration (Release and option keys) of the expressway-C and –E machines have been pre-configured already.

Task -1: Basic Configuration on Expressway-C

In the next steps we will be configuring System Name, NTP and DNS

1) System Name configuration

1. From the Expressway-C web administration page
2. Go to **System --> Administrator**
3. Configure the System Name : expc

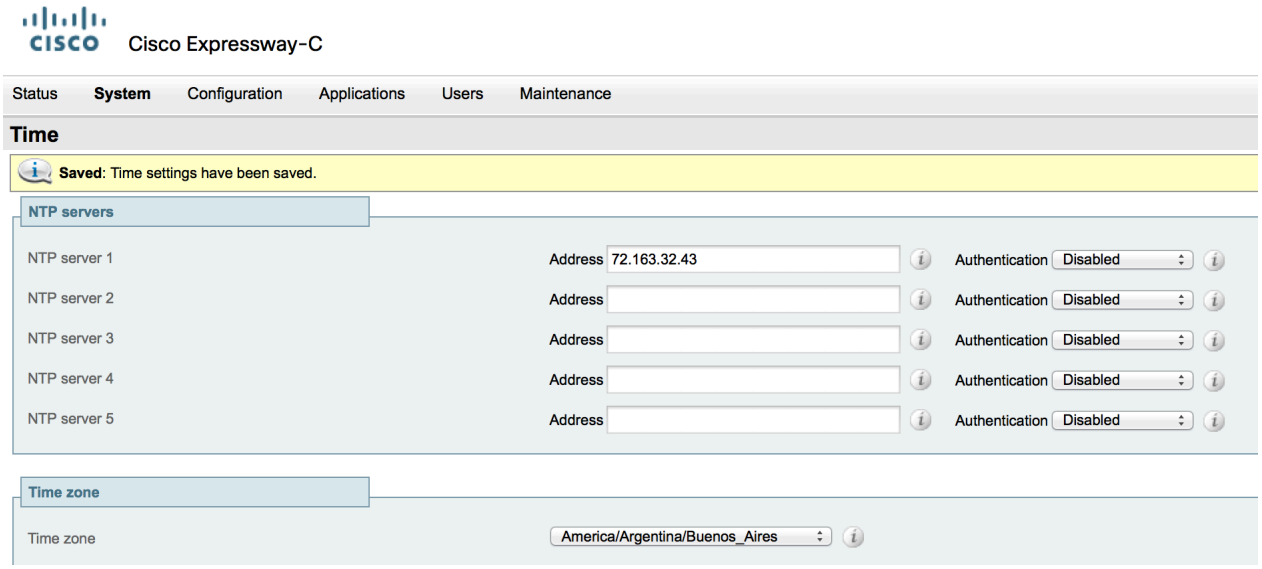


4. Click **Save**

2) NTP Server Configuration

Expressway relies on certificates for several security related features and functionalities. Ensure that all expressway systems are synchronized to a reliable time source. To configure the required NTP parameters navigate to:

1. From the Expressway-C web administration page
2. Go to **System --> Time**
3. If there are any existing entries remove them all
4. Configure the **NTP Server 1** : use the appendix provided by the instructor
5. Configure **Time Zone**: use the appendix provided by the instructor



6. Click **Save**

3) Domain Name System (DNS) Server Configuration

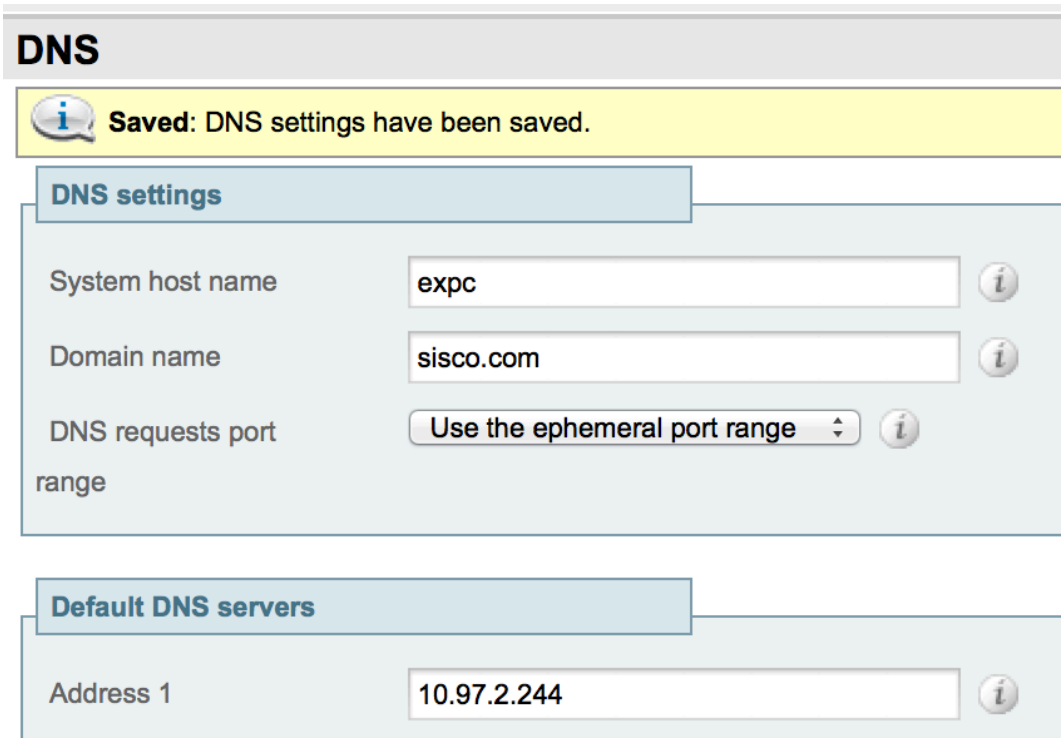
Expressway requires DNS to be configured for resolution of full qualified hostnames (FQDN) to IP addresses. DNS is also required for certain aspects of the SIP-Proxy operations of expressway. For these reasons it is **mandatory** to configure

1. From the Expressway-C web administration page
2. Go to **System--> DNS**
3. In the System **Host Name: expc**

a. In the **Domain Name** : Use Your POD Domain Name provided by the instructor.

   i. E.g: pod1.com or sisco.com

4. In the **Default DNS Server-Address 1** use the appendix provided by the instructor
5. Click **Save**
6. **Note:** Domain name is used when attempting to resolve server addresses



NOTE: The screen shoots on this lab guide should be used as a reference

Task -2: Configuring Expressway-C for Unified Communications

To provide provisioning, SIP registration and IM&P services Expressway needs to be aware of the deployed topology of servers. On the Expressway-C the administrator needs to enter the necessary connection parameters and credentials

1) Expressway-C Configuration

1. Log in to Expressway-C
2. Navigate to **Configuration --> Unified Communications --> Configuration**
3. Set **Unified Communications Mode** to Mobile and Remote Access
4. Click **Save**
5. Click **Configure IM & Presence Service Nodes**
6. Click **New**
7. Enter the following and click Add Address
    i. IM and presence Service: imp.[yourdomain].com
    ii. Username: imp server administator user provided by de instructor
    iii. Password: imp server password user provided by de instructor
    iv. TLS Off
8. Click **Add Address**

9. Navigate to **Configuration --> Unified Communications --> Configuration**
10. Click **Configure Unified CM servers**
11. Click **New**
12. Enter the following and click Add Address
    I. IM and presence Service FQDM: cucm.[yourdomain].com
    II. **Note:** FQDN recommended for certificate validation
    III. Username: cucm server administator user provided by the instructor
    IV. **Note**: Unified CM AXL enabled user, for this lab the general Unified CM admin userid and password is used. It is a good best practice to create a separate AXL enabled user for real deployments
    V. Password: cucm password user provided by the intructor
    VI. TLS Off
13. Click **Add Address**

Task -2.1: Configure domains to route to Unified CM on Expressway-C

You must configure the domains for which registration, call control, provisioning messaging and presence services are to be routed to Unified CM. Navigate to:

1) Expressway-C Configuration

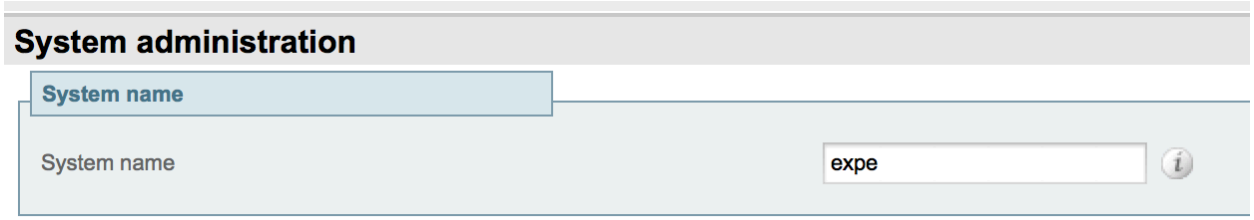
1. On Expressway-C
2. Navigate to **Configuration --> Domains**
3. Click **New**
    i. Domain Name: [yourdomain].com
    ii. SIP Registrarion: ON
    iii. IM and Presence ON
4. Click **Save**

Task -3: Basic Configuration on Expressway-E

In the next steps we will be configuring System Name, NTP and DNS

1) System Name configuration

1. From the Expressway-E web administration page
2. Go to **System --> Administrator**
3. Configure the System Name : expe



4. Click **Save**

2) NTP Server Configuration

Expressway relies on certificates for several security related features and functionalities. Ensure that all expressway systems are synchronized to a reliable time source. To configure the required NTP parameters navigate to:

1. From the Expressway-E web administration page
2. Go to **System --> Time**
3. If there are any existing entries remove them all
    i. Configure the **NTP Server 1** : use the appendix provided by the instructor
    ii. Configure **Time Zone**: use the appendix provided by the instructor
4. Click **Save**

3) Domain Name System (DNS) Server Configuration

Expressway requires DNS to be configured for resolution of full qualified hostnames (FQDN) to IP addresses. DNS is also required for certain aspects of the SIP-Proxy operations of expressway. For these reasons it is **mandatory** to configure

1. From the Expressway-E web administration page
2. Go to **System--> DNS**
    i. In the System **Host Name: expe**
    ii. In the **Domain Name** : use Your POD Domain Name
    iii. In the **Default DNS Server-Address 1** use the appendix provided by the instructor
3. Click **Save**
4. **Note:** Domain name is used when attempting to resolve server addresses

Task -3.1: Network Configuration on Expressway-E

This setup utilizes the dual network option on Expressway-E. Utilizing dual network interfaces on Expressway-E requires extra steps to ensure that IP connectivity towards the public Internet and the internal enterprise network is correctly routed out the respective interfaces and to the correct next hop addresses. Advance Networking option key has been already installed.

1. From the Expressway-E web administration page
2. Go to **System--> Network Interface -->IP**
    i. Use dual network interfaces: YES
    ii. External LAN interface: LAN 2
    iii. IPv4 Gateway: use the LAN 2 default gateway provided by the instructor
3. **Note:** The default gateway needs to point toward the internet to enable Expressway-E to reach any device trying to connect from outside. This default gateway is reachable via the LAN2 interface designed as the external facing LAN interface
4. LAN2 configuration
    i. IPv4 Address: use the ip address for **LAN2** provided by the instructor
    ii. IPv4 Subnet Mask: use the appendix provided by the instructor
5. Note: In this lab we will not use static NAT mode. In a real enviroment this is not proper configuration
6. Click **Save**
7. Click **Restart**, then **Restart** and **OK**

Expressway-E can be deployed behind a **static** NAT. With the emphasis on static as dynamic NAT configuration are not supported. When deploying behind a NAT device (i.e. Firewall) NAT mode must be set to ON and the publicly visible address that is used by expressway-e must be configured

Task -3.2: Configuring Expressway-E for Unified Communications

Similar to Expressway-C, Expressway-E has to be configured for Unified Communications. Navigate to:

1) Expressway-E Configuration

1. Log in to Expressway-E
2. Navigate to **Configuration --> Unified Communications --> Configuration**
3. Set **Unified Communications Mode** to Mobile and Remote Access
4. Click **Save**

Task -4: Setting up Secure Traversal Zone (Expressway-C & -E)

A secure traversal zone connection must be configured between the Expressway-C and Expressway-E, but before doing it we need to create a local user to authenticate the traversal connection

Expressway-E

When Expressway-C (traversal client) establishes the connection to Expressway-E (traversal server) a userID and password is exchanged for authentication. On Expressway-C these info will be entered in the traversal zone configuration. On Expressway-E the credentials must be configured in the local authentication database.

1) Expressway-E Configuration

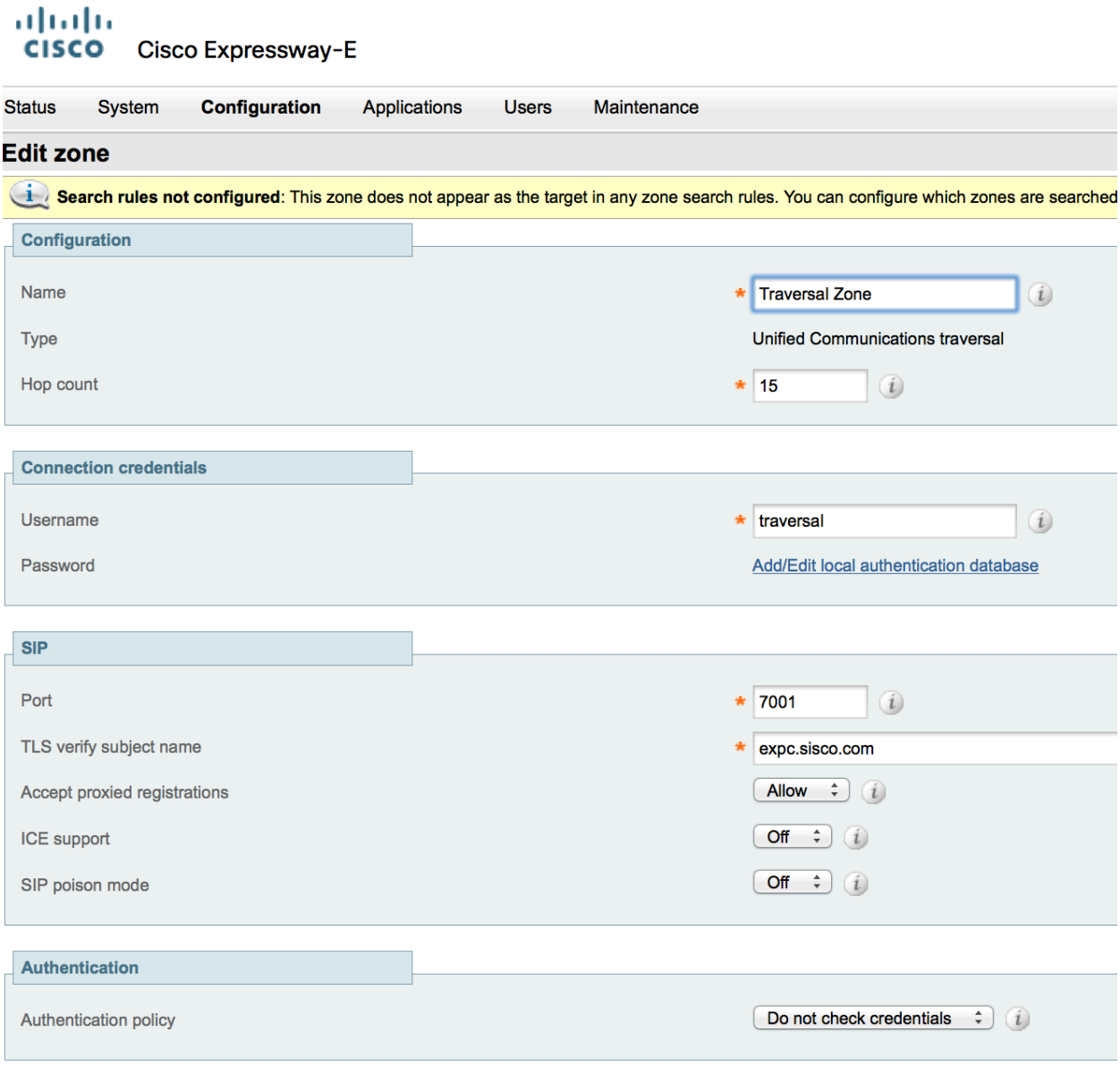
1. Log in to Expressway-E
2. Navigate to **Configuration --> Authentication --> Local Database**
3. Click **New**
    i. Name: traversal
    ii. Password: Cisco,123
4. Click **Create Credential**

2) Expressway-E Treversal Server Configuration

1. Log in to Expressway-E
2. Navigate to **Configuration --> Zones --> Zones**
3. Click **New**
    i. Name: Traversal Zone
    ii. Type: Unified Communications Traversal
4. Under **Connection Credential** use the username you just created: traversal
5. Under SIP

i. Port: 7001
ii. TLS verify subject name: **expc.[yourdomain].com**

6. **Note**: The certificate must hold that FQDN
7. Click **Create zone**
8. **Your configuration should look like this:**



3) Expressway-C Treversal Client Configuration

1. Log in to Expressway-C
2. Navigate to **Configuration --> Zones --> Zones**
3. Click **New**
    i. Name: Traversal Zone
    ii. Type: Unified Communications Traversal
9. Under **Connection Credential**
    i. Use the username you just created: traversal
    ii. Password: Cisco,123
10. Under SIP
    i. Port: 7001
11. Under Location
    i. Peer 1 Addres: expe.[yourdomain].com
12. Click **Create zone**

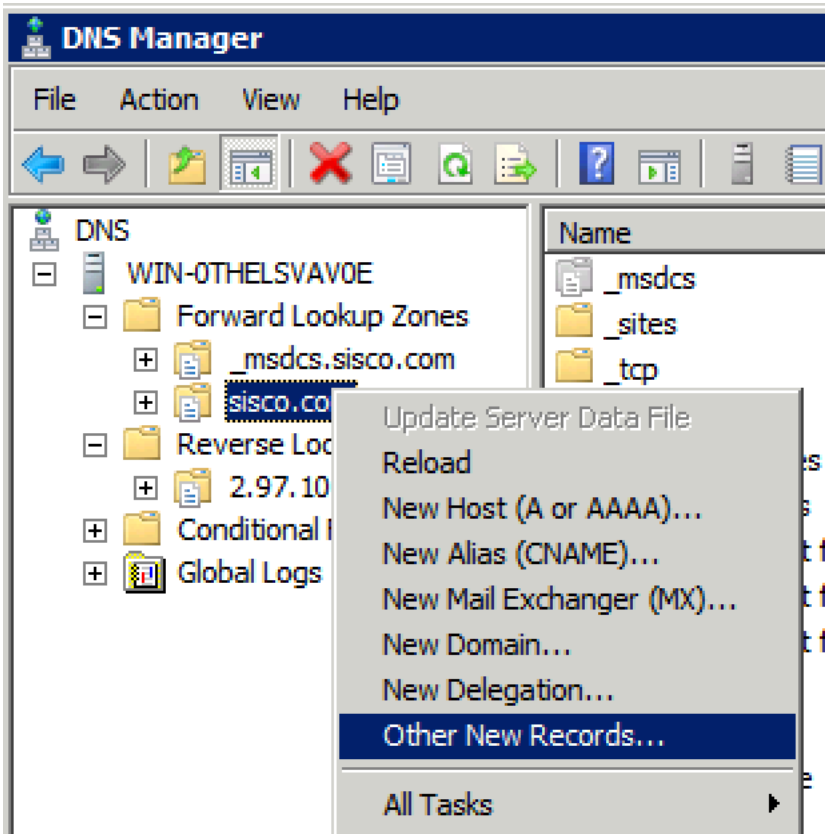
Navigate back to **Configuration--> Zones--> Zones** and verify the status of the Traversal zone is Failed since certificares are not active yet.

Notice next to the Peer 1 Addres the SIP: Failed to connect to expressway-E ip Addres :7001 : TLS negotiation failure

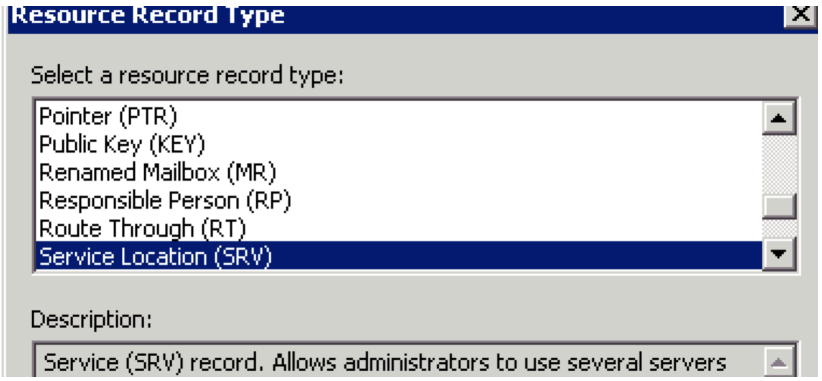
Task -5: Internal DNS Configuration

1) Internal DNS ¨SRV¨ Records

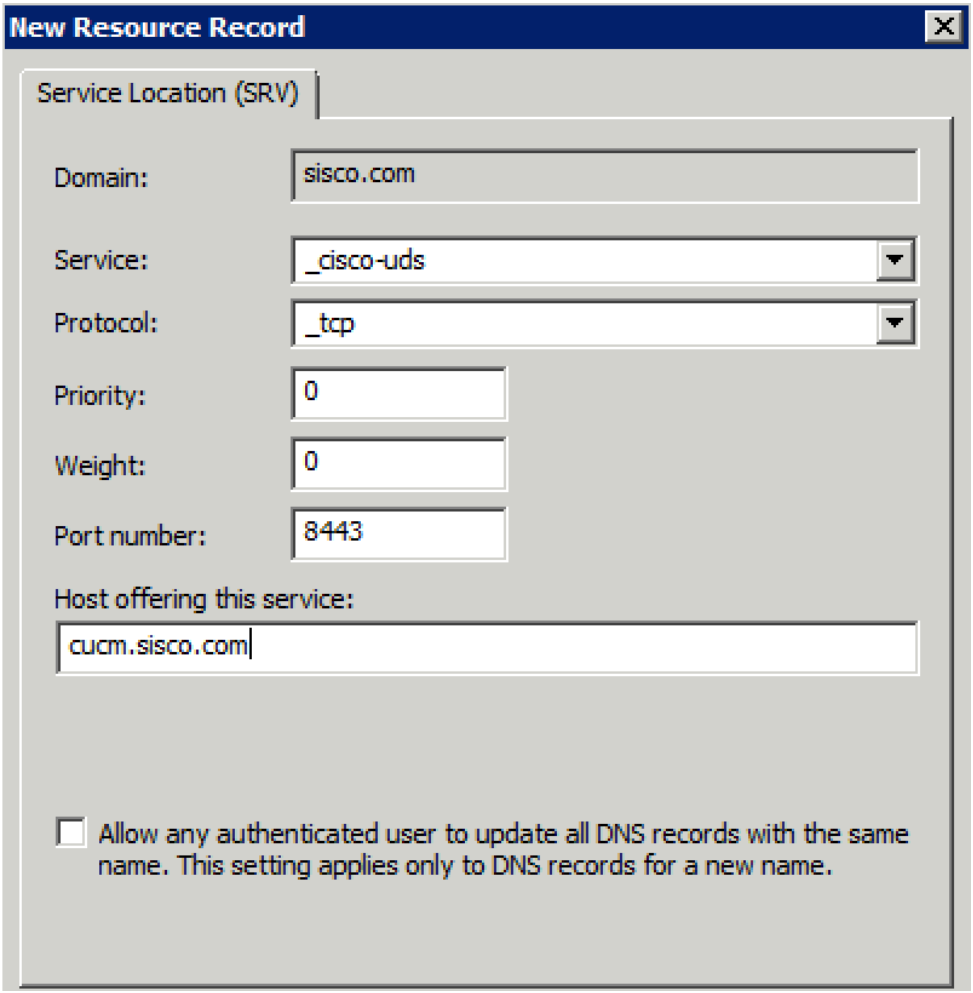
1. From your PC, Remote Desktop to Internal DNS
    i. User name: Administrator
    ii. Pass: C1sco,123
2. Navigate to Start, DNS
3. Expand Forward Lookup Zones
4. Expand your domain
5. Right click on [yourdomian].com and click on Other New Records



6. Select **Service Location** (SRV)



7. Click **Create Record**
8. Enter the following and then click OK
    i. Service: **_cisco-uds**
    ii. Protocol: **_tcp**
    iii. Port Number: **8443**
    iv. Host Offering this service: **cucm. [yourdomain].com**

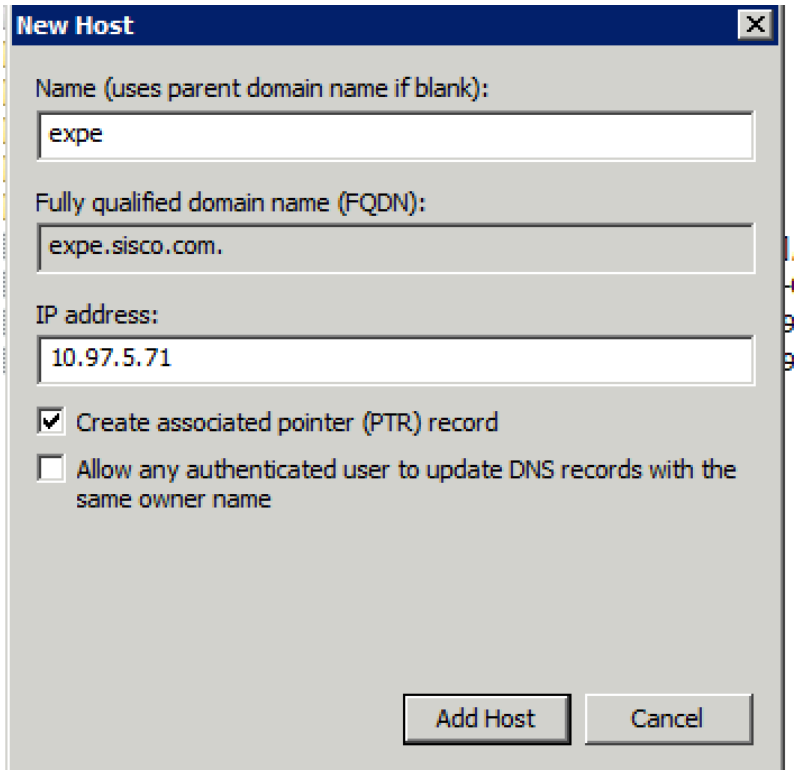


9. Click **OK**
10. Click **Done**
11. Repeat the process for the following information:
12. Enter the following and then click OK
    i. Service: **_cuplogin**
    ii. Protocol: **_tcp**
    iii. Port Number: **8443**
    iv. Host Offering this service: **imp. [yourdomain].com**
13. Click **OK**
14. Click **Done**

Task -6: Public DNS Configuration

1) External DNS ¨A¨ Records

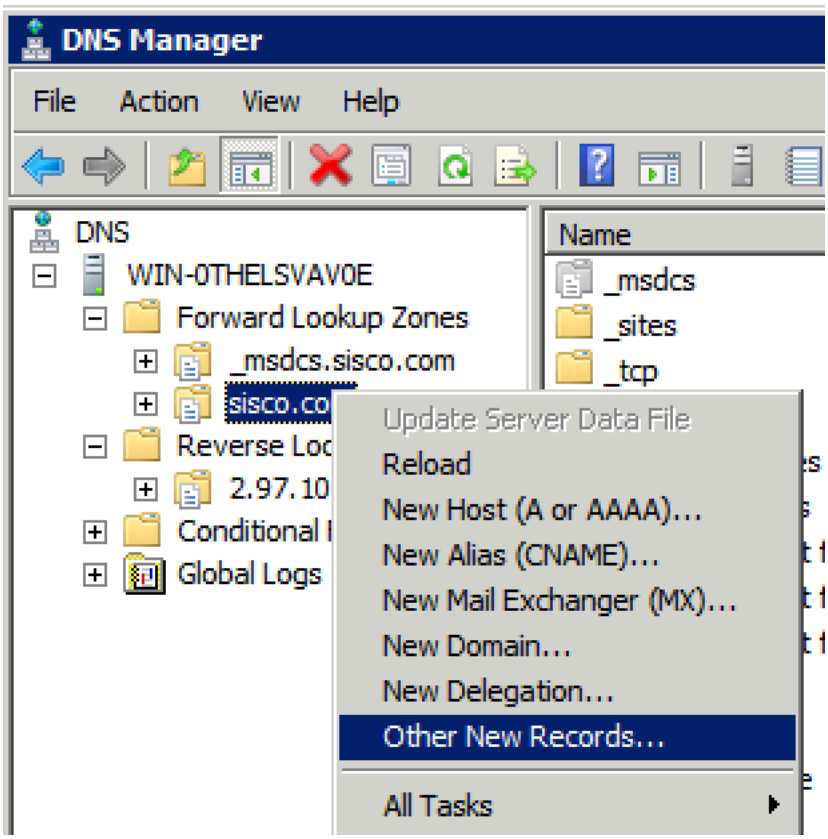
1. From your PC, Remote Desktop to External DNS
    i. User name: Administrator
    ii. Pass: C1sco,123
2. Navigate to Start, DNS
3. Expand Forward Lookup Zones
4. Expand your domain
5. Right click on [yourdomian].com and click New Host (A or AAAA)
    i. Name: expe
    ii. IP Address: Expressway-E LAN 2 IP address



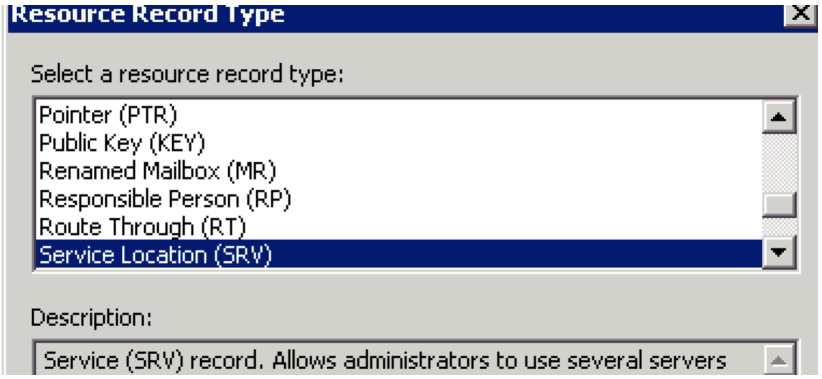
6. Check **Create PTR record**
7. Click **Add Host**
8. Click **Done**

2) External DNS ¨SRV¨ Records

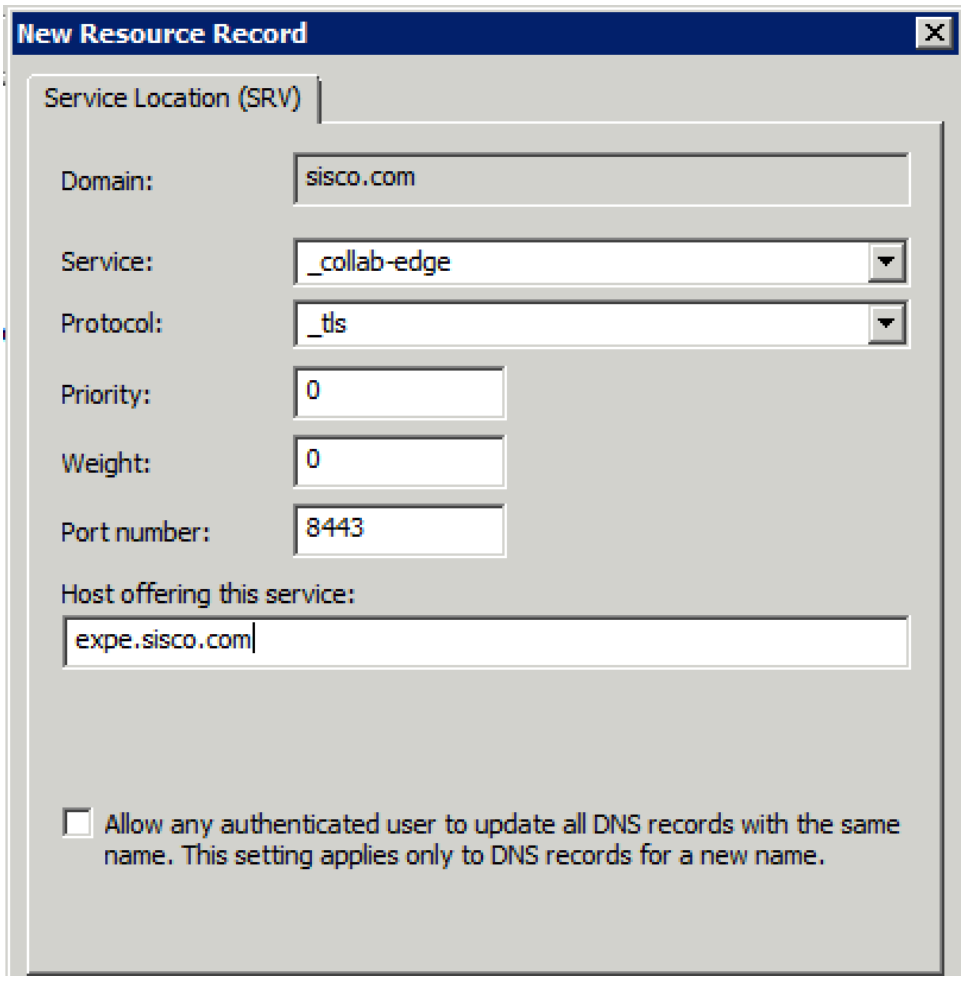
9. From your PC, Remote Desktop to External DNS
    i. User name: Administrator
    ii. Pass: C1sco,123
10. Navigate to Start, DNS
11. Expand Forward Lookup Zones
12. Expand your domain
13. Note: there are **no _TLS records** in the window on the right
14. Right click on [yourdomian].com and click on Other New Records



15. Select **Service Location** (SRV)



16. Click **Create Record**
17. Enter the following and then click **OK**
    i. Service: _collab-edge
    ii. Protocol: _TLS
    iii. Port Number: 8443
    iv. Host Offering this service: expe. [yourdomain].com



18. Click **Done**
19. Close DNS, and log off of RDP session.

Task -7: Expressway Certificates

Retrieve and Upload the Certificate Authority (CA) Certificate

The purpose of this task is to obtain the Root CA certificate.

Activity Procedure

Complete these steps:

Step 1 Download the CA Certificate from the Certificate server and upload to both your Expressway-C and your Expressway-E (All Expressways if it is a cluster)

For more detailed steps, click here

Step 1 On your laptop, create a folder on your desktop called Certificates

Step 2 From your laptop, do remote desktop to your CA Authority server, open a browser and *use the following URL https://localhost/certsrv*

Step 4 Click Download a CA Certificate and Click yes

Step 5 Choose Base 64 for the encoding method.

Step 6 Click Download CA Certificate and save the file as CARoot.cert into the Certificates folder on your desktop.

Step 7 Save the file in your folder and rename to identify the file as the route certificate.

Step 8 Log in to your Cisco Expressway-C and go to *Maintenance >Security Certificates > Trusted CA Certificate.*

Step 9 Browse to the file you have just saved, and click Append CA Certificate.

Step 10 Repeat steps 8 and 9 on your second Expressway-E

Generate a CSR File from the Cisco Expressway

The purpose of this task is to generate a CSR files for your Expressway-C and Expressway-E

Activity Procedure

Complete these steps:

Step 1 From *Maintenance > Security Certificates > Server Certificate*

Generate a CSR file for Cisco Expressway-C and Expressway-E

For more detailed steps, click here

Step 1 Log in to your Cisco Expressway-C, using the credentials in your documentation

Step 2 Go to *Maintenance > Security Certificates > Server Certificate*.

Step 3 Click Generate CSR.

Step 4 Enter the following information where requested:

Common Name	FQDN of Exressway-C
Subject Alternative Name	Leave it blank since we do not have a clueter in this lab.
Digest Algorithm	SHA-1
Key Length	2048
Country	US
State or Province	California
Locality	San Jose
Organization	Cisco
Organizational unit	Training

Step 5 Click Generate CSR.

Step 6 Click Download and save the file to a folder on your desktop with an identifiable name

Step 7 Repeat this procedure for the Expressway-E

Using the CSRs and the certificate server, generate a certificate for Expressway

For more detailed steps, click here

Step 1 Enter the IP address of your TP certificate authority server, followed by /certsrv. This takes you to the web interface of the certificate authority. *If this does not work* From your laptop, do remote desktop to your CA Authority server, open a browser and *use the following URL https://localhost/certsrv*

Step 2 Click Request a Certificate.

Step 3 Click Advanced Certificate Request.

Step 4 Open the CSR for Expressway-C in notepad and copy the contents of the CSR to the Certificate Request field in the browser. Include the Begin and End certificate lines, but make sure there is no spare line at the bottom.

Step 5 Click Submit a certificate request by using a base-64.... Paste the CSR content

SELECT **EXPRESSWAY** AS A CERTIFICATE TEMPLATE

You can leave the Attributes box empty and Click Submit

Click OK in the pop-up Windows

Step 6 Select the Base 64 encoded option and click Download certificate

Step 7 Save the file to your folder changing the name to enable you to distinguish which certificate is which

Step 8 Repeat the process for Expressway-E

Upload certificates to the correct Expressway

Step 1 Log into Expressway-C and navigate to *Maintenance > Security certificates > Server certificates*

Step 2 Click Browse in the Upload new certificates section

Step 3 Locate the correct file and click Open then click Upload server certificate data

_____ Note _____

You have not installed the certificate on the PC so you will get

browser warnings at this stage.

_____

Step 4 Repeat for Expressway-E

Task -8: Test

To validate that MRA is configured correctly, we will use Jabber to test.

1. Connect your computer to what we call ¨Internet in this Lab
2. From your PC change the DNS configuration to your external DNS
3. log in as aolmedo
4. Open Jabber
5. When prompted for the password, enter the information based on your lab documentation and click Sign In.
6. Verify that Jabber is logged in and that you can place a call to one of the contacts.
7. MRA Configuration is now validated.

Task -8: DX70/80 MRA Registration

1. Connect the DX to the External network network
2. Log in to CUCM.
3. Navigate to Device, Phones and click Find
4. Find the device labeled Steve Rogers DX and click on it.
5. On the DX, go to Settings, More, Reset network settings (if you do not get a white cisco sign in page do the following) This is a known Alpha issue
    a. Backup and Reset and Factory Reset the endpoint.
6. Upon boot up you will see a Cisco splash screen and Detecting Network followed by a Sign In screen. Fill in the Sign In information with the following and tap Sign In:
    a. Service Name: videolab.com
    b. Username: srogers
    c. Password: C!sc0123

In this lab, you have successfully configured everything needed to facilitate MRA of Jabber clients, DX endpoints and even some of the 8800 series phones that will gain MRA capability this year. Because of the limitations within the environment we are conducting the labs, DX MRA will not successfully work. It requires SSL certificates issued by one of a list of supported public certificate authorities of which we could not acquire for this lab. Take note of this requirement and consult the deployment guide (when published) for a list of said CA's.

7. Move the network cable for the DX back to the inside port and reboot the DX. It should re-register.