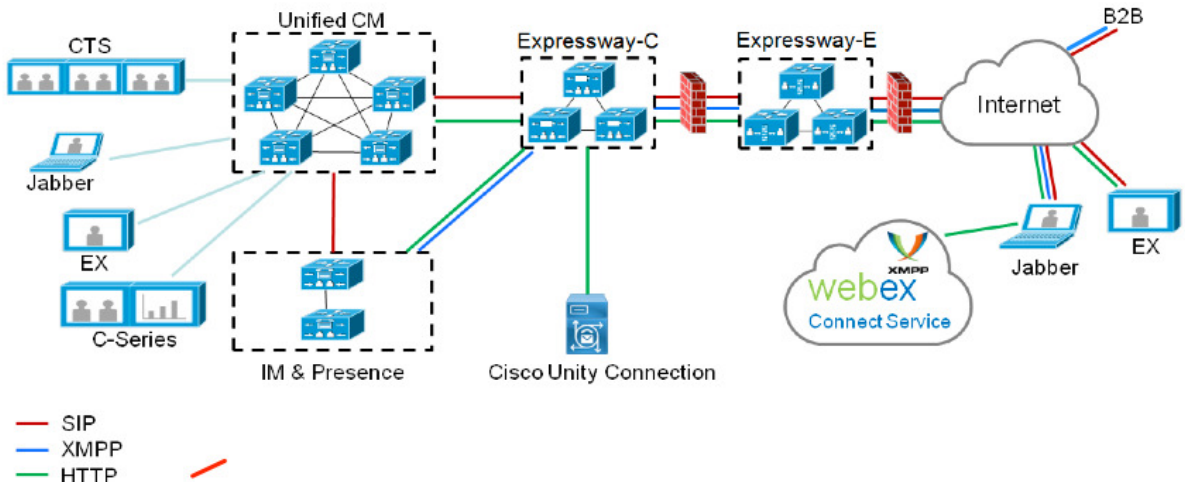
B2B integration with CUCM through Expressway - Audio and Video calls

by OBSERVER psmeunin on 12-02-2014 09:23 AM

- edited on 05-19-2015 02:10 PM by OBSERVER cysimons

Expressway with the Mobile Remote Access feature provides seamless registration of Jabber and TC endpoints located outside the enterprise network as is shown in below picture.
The same architecture does also provide seamless integration/calls between different enterprises, aka Business to Business integration and this for Audio, Video and IM&P. (B2B)
This document covers how to integrate/configure your Expressway and CUCM deployment to be able to make and receive calls from other companies (domains). It does not cover the IM&P part and neither does it cover H.323 integration.

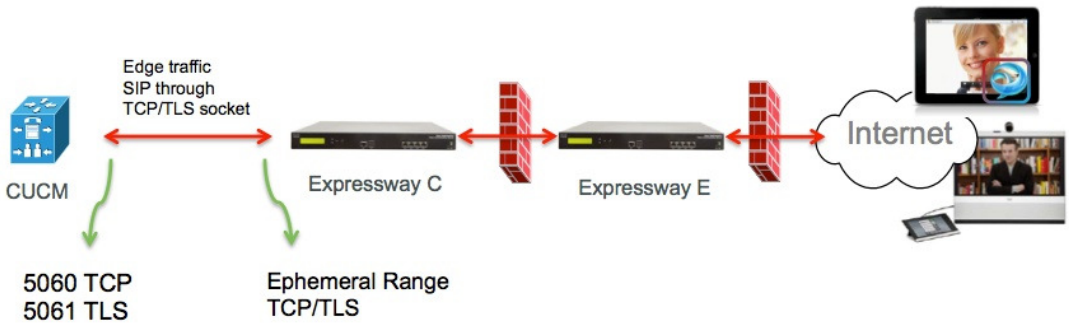


Prior you continue you need to make sure you have the relevant DNS SRV created for your domain, these records are used by other companies to find the location of your Expressway.

Configuration step 1 - SIP trunk between CUCM and Expressway-C

After CUCM discovery is done by Expressway-C, Neighboring zone(s) are automatically configured for each node and transport protocol discovered.
When the CUCM cluster is configured in mixed mode there will be 1 zone for TCP (none-secure traffic) with destination port 5060 and 1 zone for TLS (secure traffic) with destination port 5061. These ports can not be changed.
The 2 zones are used for all edge calls to and from the edge endpoints.

Inbound calls from the edge endpoints will take the route of these auto-added zones and hence will be targetting TCP 5060 or TLS 5061 on CUCM.
Through the established sockets edge endpoints will register and place/receive calls.

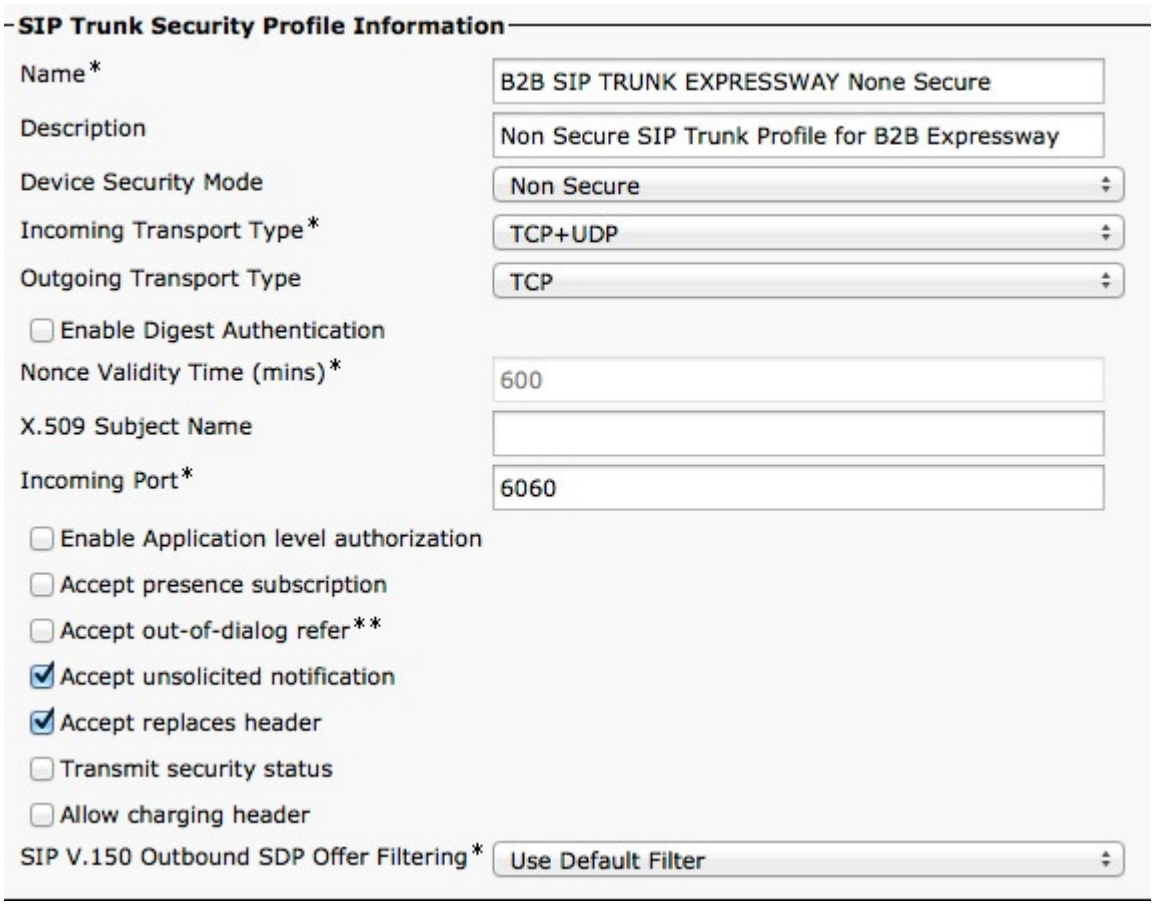


For B2B calls we need to configure a SIP trunk on CUCM pointing to Expressway C where typically CUCM will listen on port 5060 or 5061 for inbound traffic from this gateway.
Since edge traffic is coming from the same source IP with port 5060/5061 we will need to use a different listening port for this trunk on CUCM. Otherwise edge traffic will be routed to the SIP trunk device on CUCM and not to the endpoint device (CSF or EX)
On Expressway-C side we continue to use 5060 and 5061 for SIP TCP/TLS.
Below is an example where CUCM listens on port 6060/6061 for inbound traffic on this trunk.

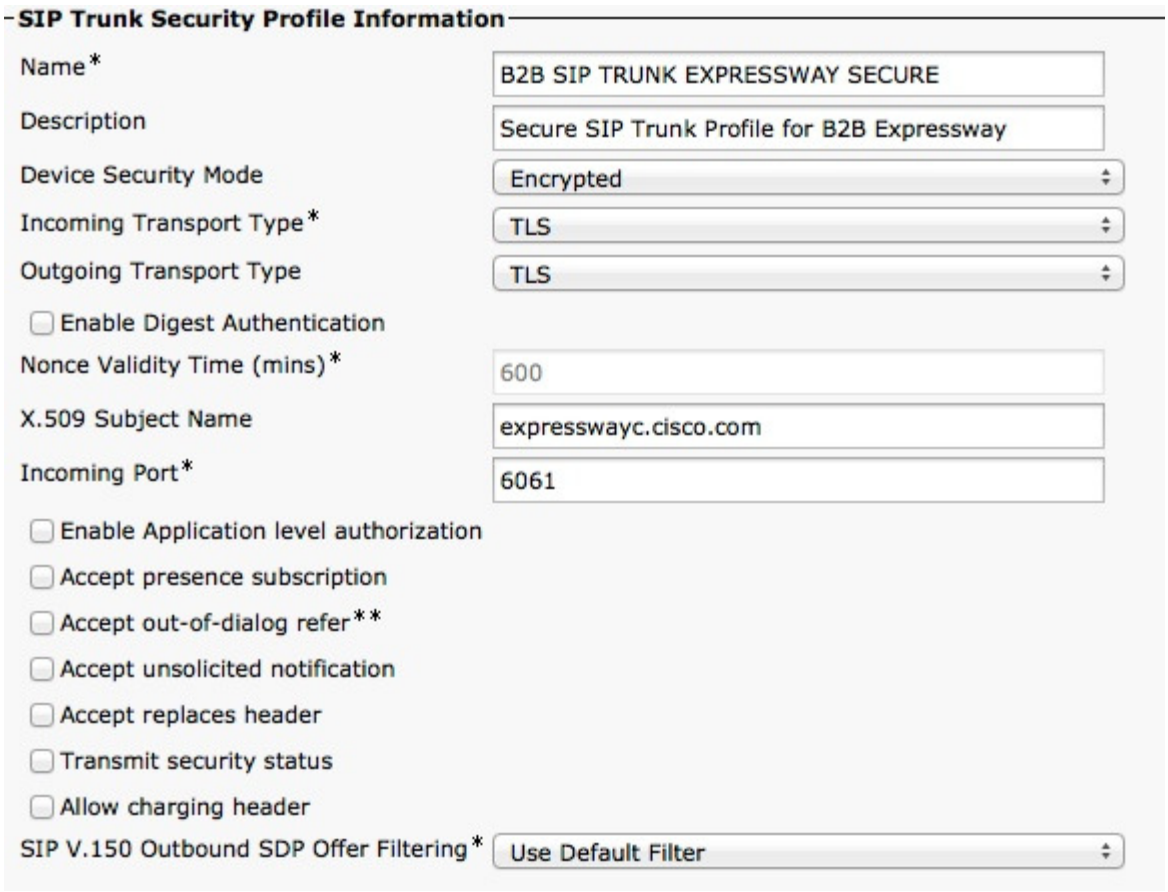
Below are the different configuration steps documented for this deployment.
Both for secure and non-secure deployments.

1. Add a new SIP Trunk Security Profile.
   Configure a different Incoming port then 5060/5061, here we use 6060 for TCP and 6061 for TLS

   Non Secure SIP Trunk profile



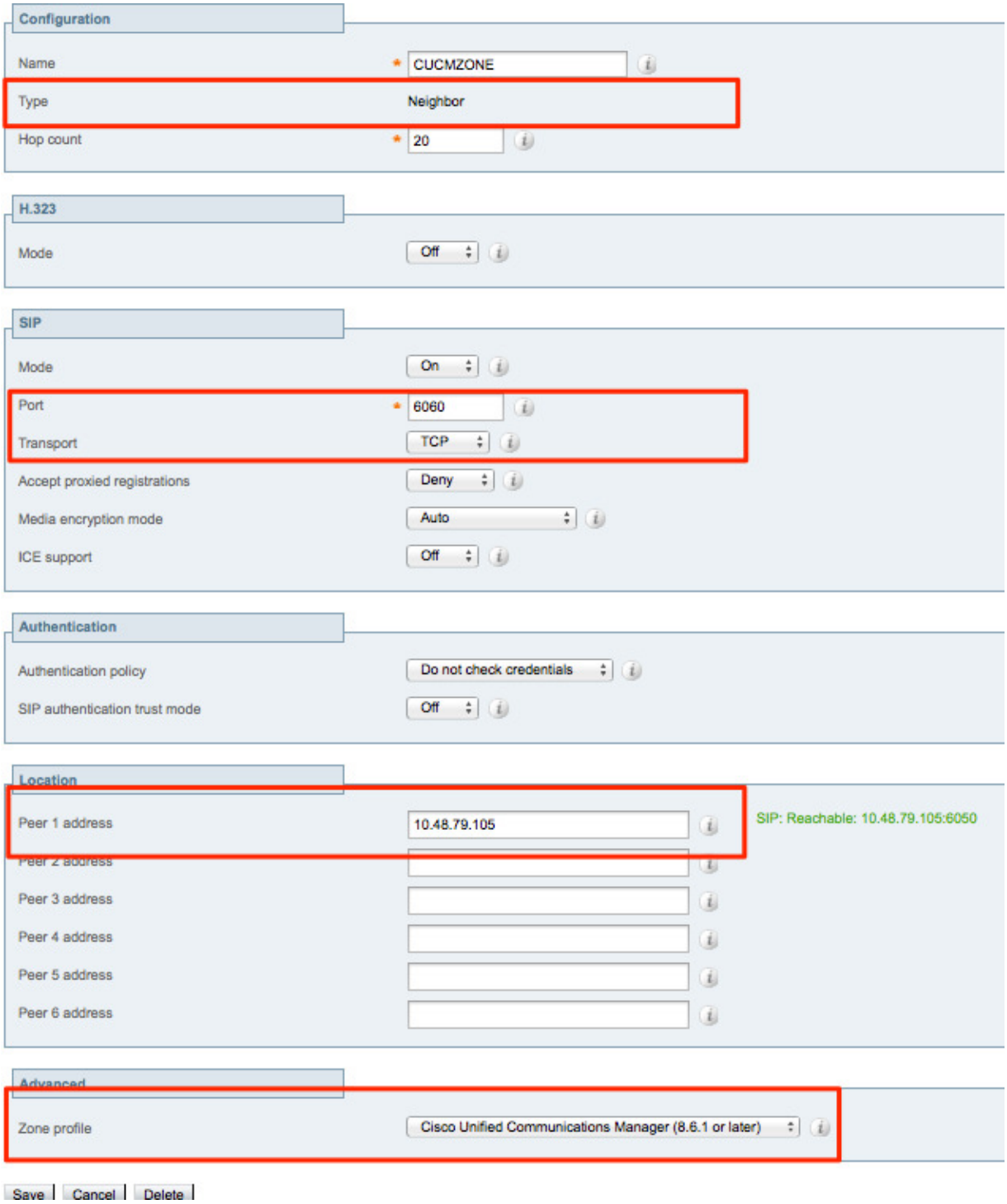
Secure SIP Trunk profile
For TLS you also need to configure the X.509 Subject name matching the CN of the certificate presented by the expressway-c. In addition you also need to upload the Expressway-C or the CA certificate (which issued the expressway-c cert) to the CCM Certificate trust store.



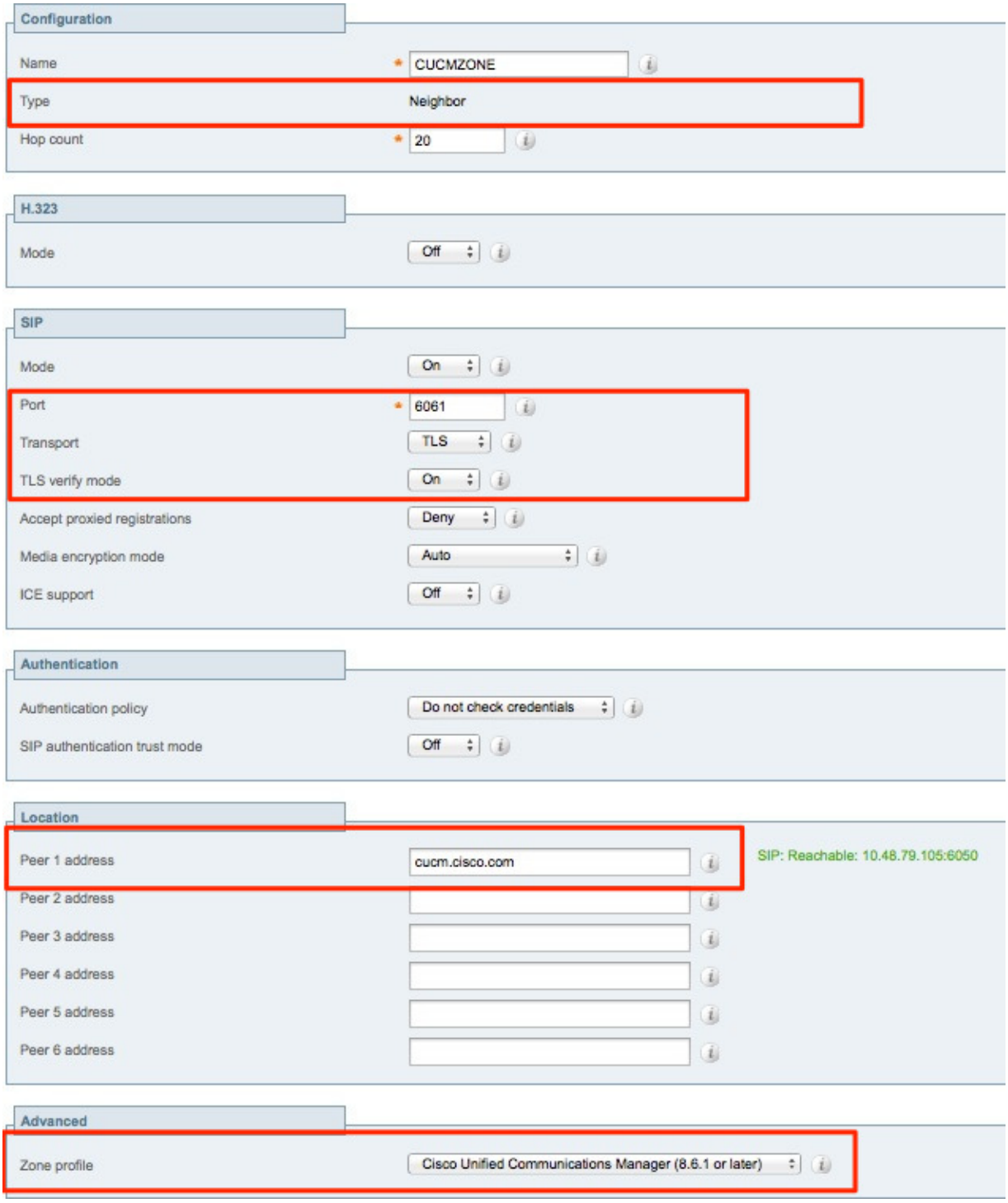
2. Configure the SIP trunk on CUCM.
   Through this trunk all B2B calls will flow, to and from CUCM.
   The SIP trunk configuration parameters are standard for CUCM with VCS deployments.
   Do make sure to associate the security profile created in step 1.

3. Configure a neighbour zone on Expressway-C
   A neighbour zone needs to be configured on Expressway-C targetting CUCM.
   This zone us used to route inbound B2B traffic to CUCM.
   The configuration is standard except that you must make sure to configure the destination port corresponding to the listening port configured on the SIP Trunk Security profile assigned to the SIP trunk on CUCM.

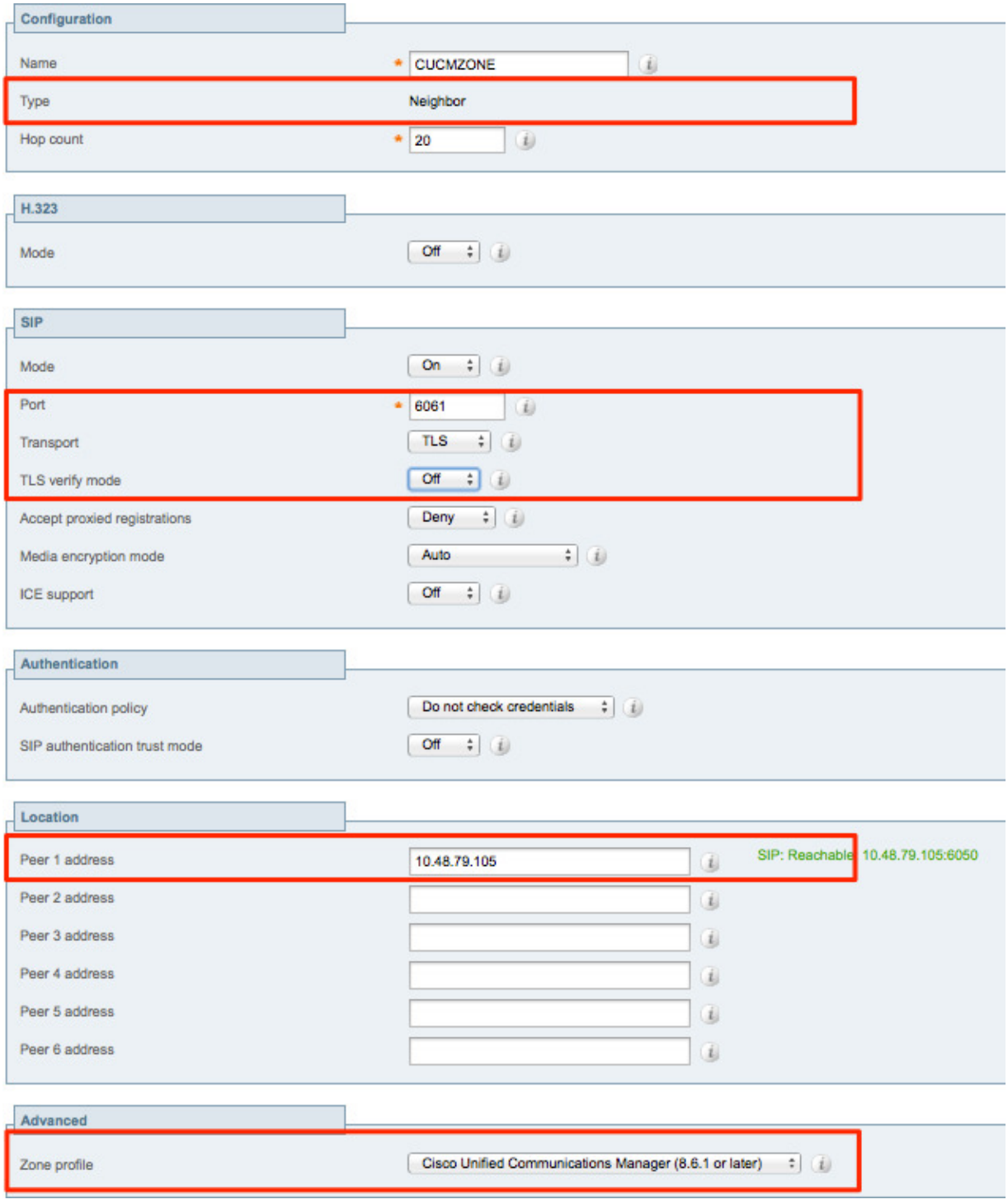
   In this example the destination port will be 6060 for SIP/TCP and 6061 for SIP/TLS. (refer to step 1)
   Neighbour zone for SIP TCP:



Neighbour zone for SIP TLS - with TLS verify mode on
When TLS verify mode is set to on you must make sure the "peer address" matches the CN or SAN from the certificate presented by CUCM. Typically with TLS verify mode on you configure the FQDN of the CUCM node for peer address.



Neighbour zone for SIP TLS - with TLS verify mode off
When TLS verify mode is set to off the peer address can be either the IP address, hostname or FQDN of the CUCM node.

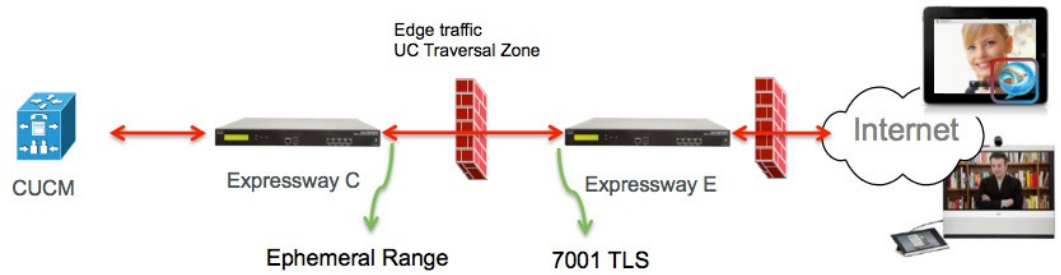


4. For TLS, make sure that
   - Expressway C server certificate or CA root (used to sign certificate) is uploaded to the Callmanager Trust store on all servers in the CUCM cluster.
   - Callmanager certificate or CA root (used to sign certificate) is uploaded to the 'Trusted CA Certificate' list on the Expressway C server

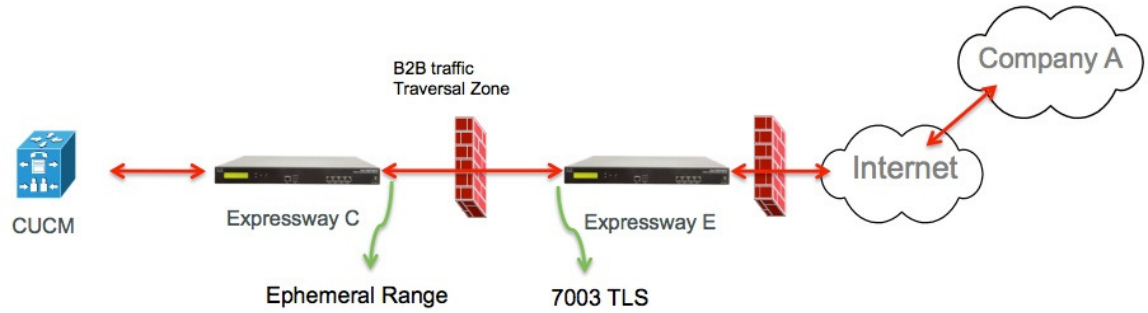
Configuration step 2 : Configure traversal zone between Expressway-C and Expressway-E

A separate traversal zone has to be configured to route the B2B traffic between Expressway-C and Expressway-E. This is a standard traversal zone configuration, but similar as with the SIP trunk on CUCM a different port then the port used by the UC Traversal zone for Edge traffic must be configured.
The standard port for the UC Traversal zone is 7001. For the B2B Traversal zone you can e.g configure 7003.

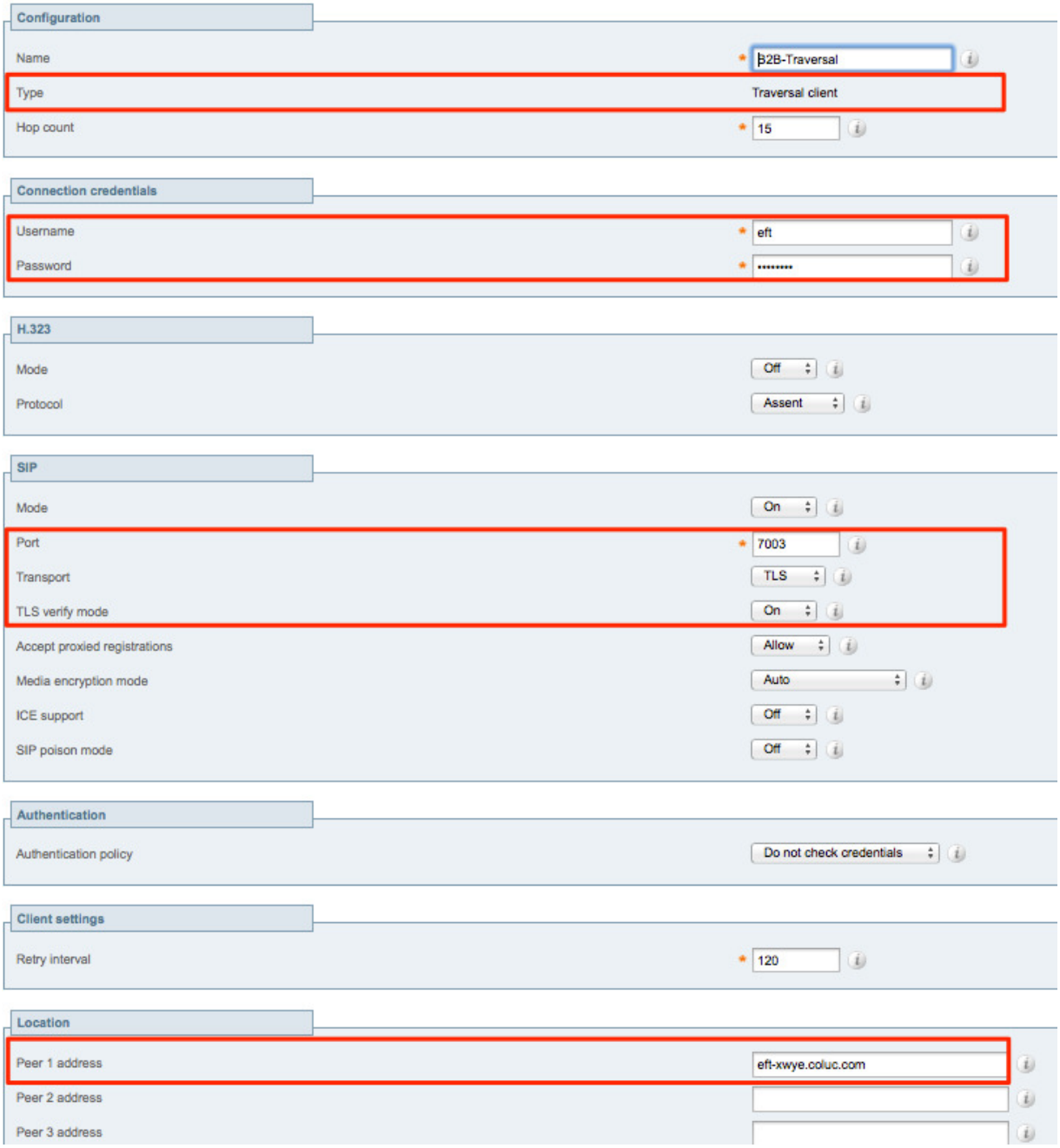
UC Traversal Zone for edge traffic



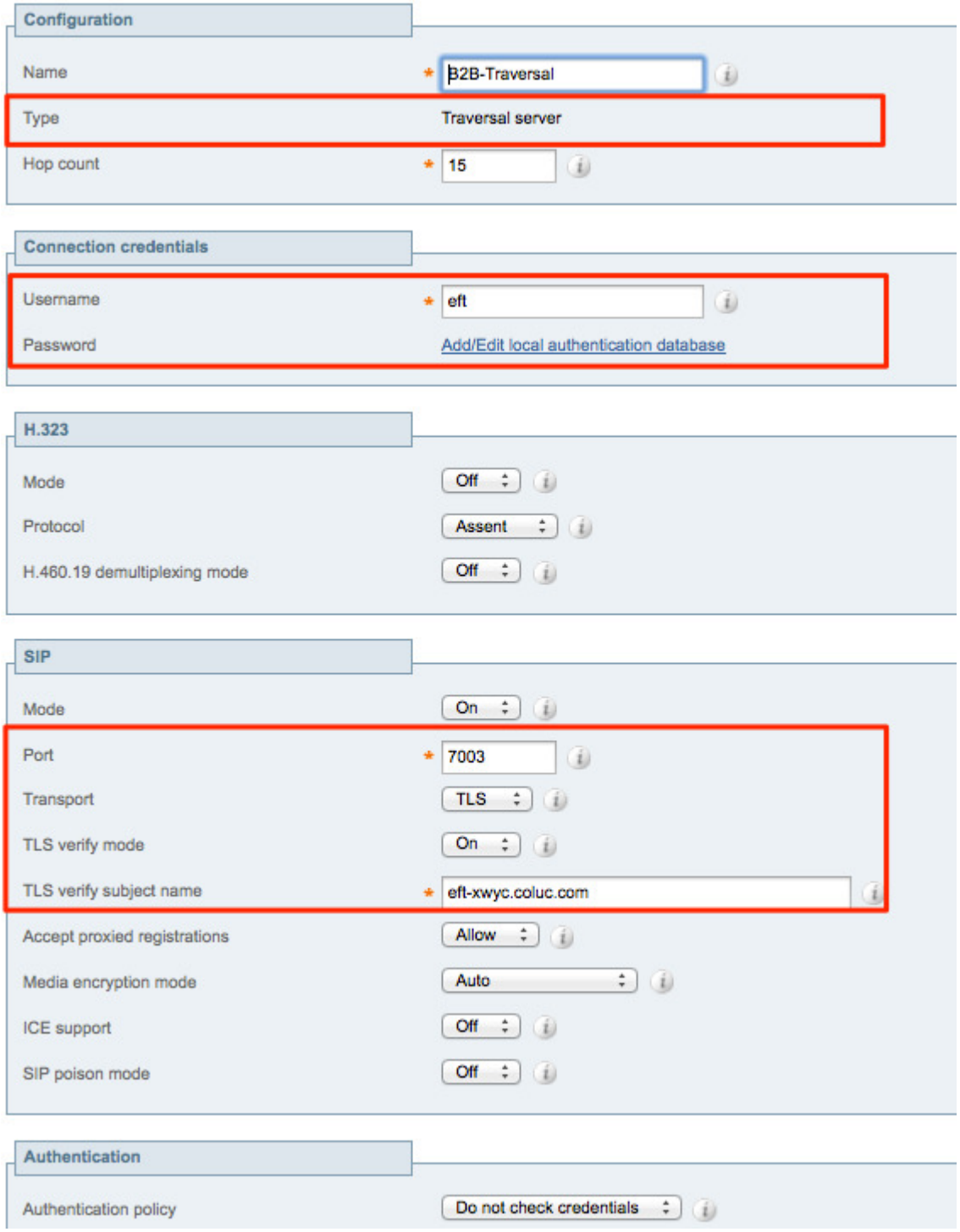
Traversal Zone for B2B traffic



1. Traversal zone configuration for B2B traffic on Expressway-C
   Expressway-C is the traversal zone client, in this example the destination port is 7003
   With TLS verify mode set to On make sure the 'Peer Address' configured matches the CN or SAN of the presented certificate by Expressway-E



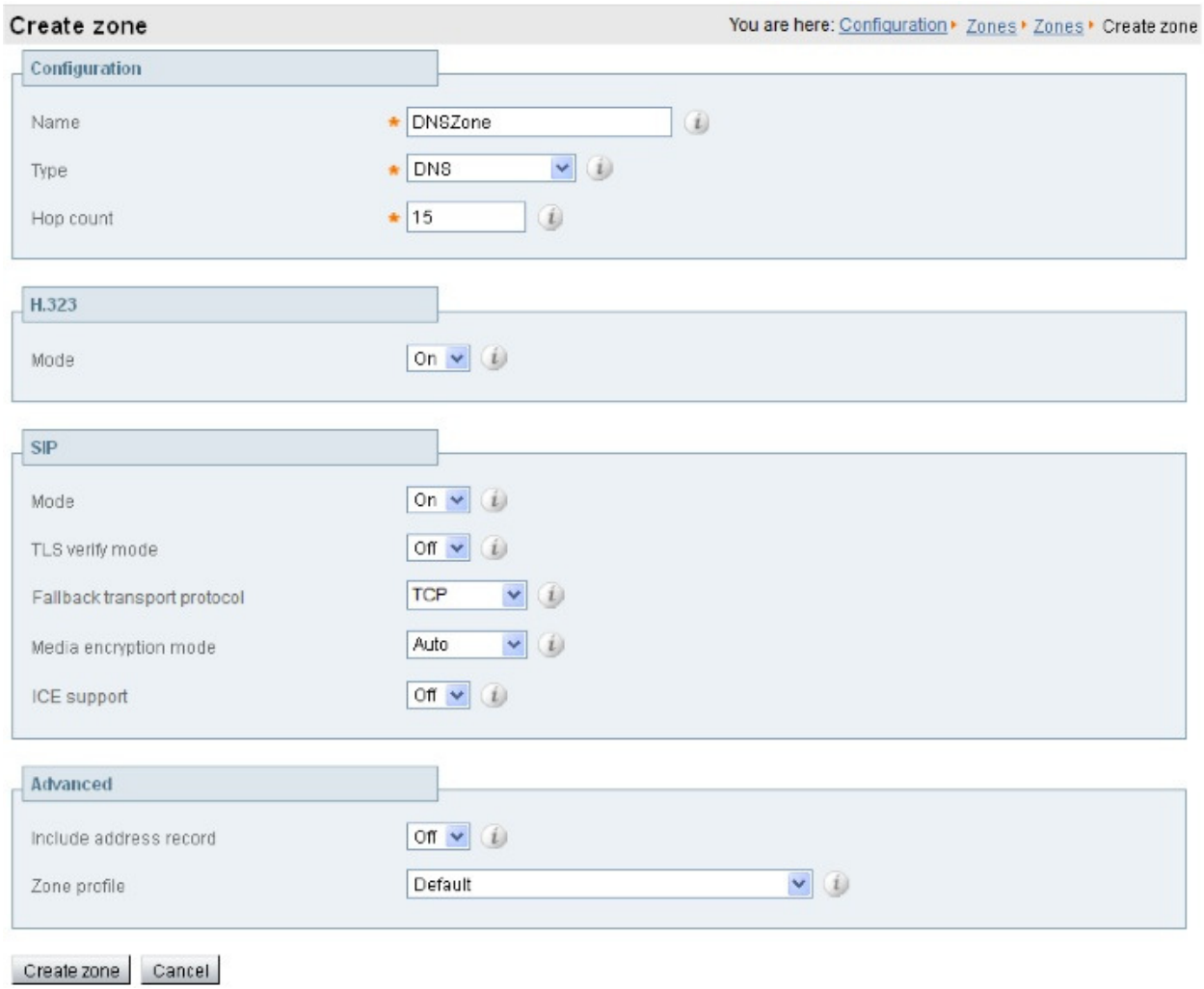
2. Traversal zone configuration for B2B traffic on Expressway-E
   Expressway-E is the traversal zone server, in this example the listening port is 7003.
   With TLS verify mode set to On make sure the 'TLS verify subject name' configured matches the CN or SAN of the presented certificate by Expressway-C



Configuration step 3 : Configure DNS zone on Expressway-E

To route the B2B traffic you have to configure a DNS zone on Expressway-E.
Expressway-E, for traffic destined to this zone, will perform a DNS SRV lookup for ether _sip or _sips and this for the domain derived from the domain portition of the SIP URI.
The SRV target returned by the DNS server will be used to route the SIP call to.

The configuration is a standard DNS zone configuration.



Configuration step 4 : Configure dialplan

1. Transforms and/or Search Rules on Expressway-C and E
   For more information please consult the VCS Deployment guides (Control with Expressway),
   chapter on 'Routing Configuration'
   http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

2. SIP Route pattern(s) on CUCM
   For more information please consult the CUCM System and administration guide (Dialplan Deployment guide)
   http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

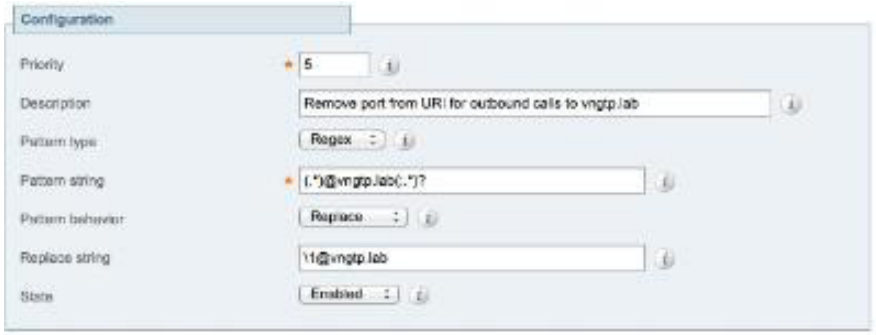
3. For SIP call routing SRV records must be created on the public DNS servers.
   Below diagram lists the required SRV records, including as well for H323 B2B calls which has not been discussed in this document. Also to note that SIP UDP by default is disabled on Expressway

DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	expe.example.com.
example.com.	h323ls	udp	10	10	1719	expe.example.com.
example.com.	sip	tcp	10	10	5060	expe.example.com.
example.com.	sip	udp *	10	10	5060	expe.example.com.
example.com.	sips	tcp	10	10	5061	expe.example.com.

4. Configuring the Cluster Fully Qualified Domain Name on CUCM.
   You can enter multiple entries seperated by comma.

5. Create a transform on Expressway C which removes the port from the URI received in the Invite from CUCM.
   (For more info, look for this document :
   http://www.cisco.com/c/en/us/support/docs/unified-communications/telepresence-video-communication-server-vcs/116729-trouble-cucm-dns-vcs-01.html)



The SRND also contains an extensive chapter on dialplan
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html

Configuration step 5 : Upload rich media licenses to Expressway

Rich media licenses (aka Traversal Zone licenses) must be uploaded to each Expressway Server.
In case these are missing or due to improper configuration calls may be released with following warning

"Call license limit reached: You have reached your license limit of concurrent traversal call licenses"