Cisco Support Community Expert Series Webcast:

CUCM and IP Phone Security

Amit Singh, Engineer Technical Services

Raees Shaikh, Engineer Technical Services

Date: 3rd April 2012

Cisco Support Community – Expert Series Webcast

- Today's featured experts are Cisco Support Engineers Amit and Raees
- Ask them questions now about Cisco Unified CallManager and IP Phone Security

Amit Singh

Raees Shaikh

Thank You for Joining Us Today

Today's presentation will include audience polling questions

We encourage you to participate!

Thank You for Joining Us Today

If you would like a copy of the presentation slides, click the PDF link in the chat box on the right or go to the following url:

https://supportforums.cisco.com/docs/DOC-23637

Polling Question 1

What is your level of experience with CUCM/ Phone Security ?

a) I know basic Security, but no idea about CUCM Security

b) I theoretically know CUCM Security, but no practical experience.

c) I'm playing with it in the lab.

d) I'm running it in production.

Submit Your Questions Now!

Use the Q&A panel to submit your questions. Experts will start responding those

Cisco Support Community Expert Series Webcast:

CUCM and IP Phone Security

Raees Shaikh, Amit Singh

Engineer. Technical Services

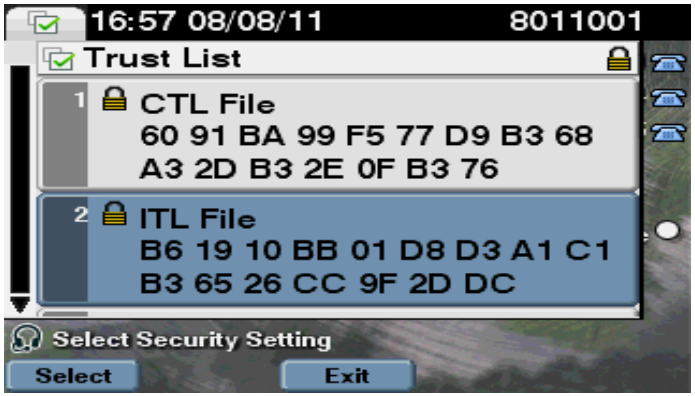
3rd April 2012

Agenda

- Introduction to CUCM Security
  - Terminology
  - Security Fundamentals
  - Security By Default
  - Use case scenario/Best Practices
- Troubleshooting
- Summary

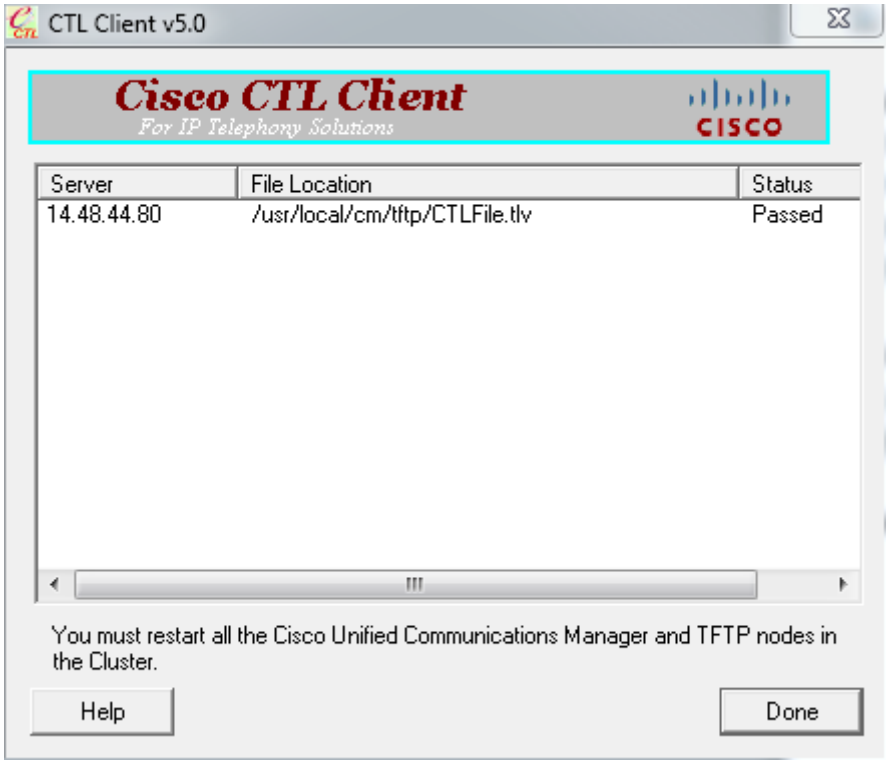
Terminology

- **Public Key Infrastructure (PKI)** : In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA)
- **CTL (Certificate Trust List) File** : It contains a list of identities that are attested to by a systems administrator using a security token.
- **ITL (Identity Trust List) File** : Introduced in CUCM 8.x onwards, contains the minimum list of certificates that are required by the phone for authentication, decryption of Phone Configuration file and contacting the TVS service.
- 7975 Phone >> Setting >> Security Configuration >> Trust List



Terminology

- **CTL Client** : CTL Client is a software installed on Windows workstation or server that has a USB port. This is used to create/update CTL file using eTokens by contacting the CTL server.

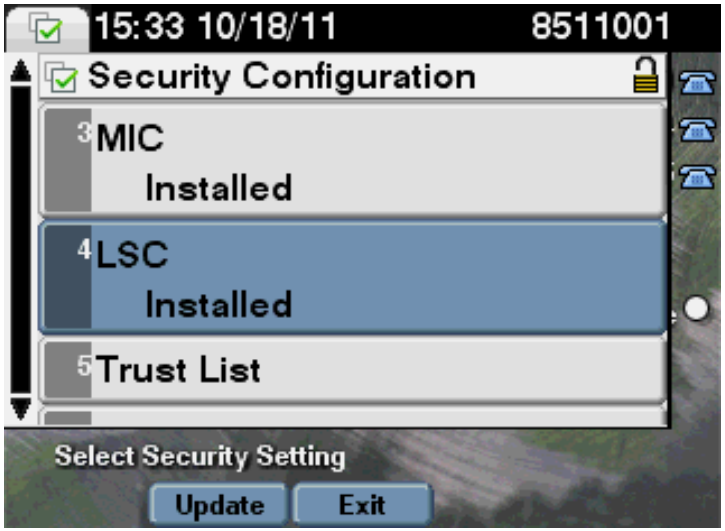


Terminology

- **CAPF (Cisco Certificate Authority Proxy Function):** CAPF Server work as a CA for endpoints and issues LSC (Locally Significant Certificate) certificates to endpoints.
- **eToken** : eTokens have the Public and Private Key issued by Cisco CA which is used for signing the CTL file. At least two USB eTokens are required for turning on Phone Security by running CTL Client and must not be lost.

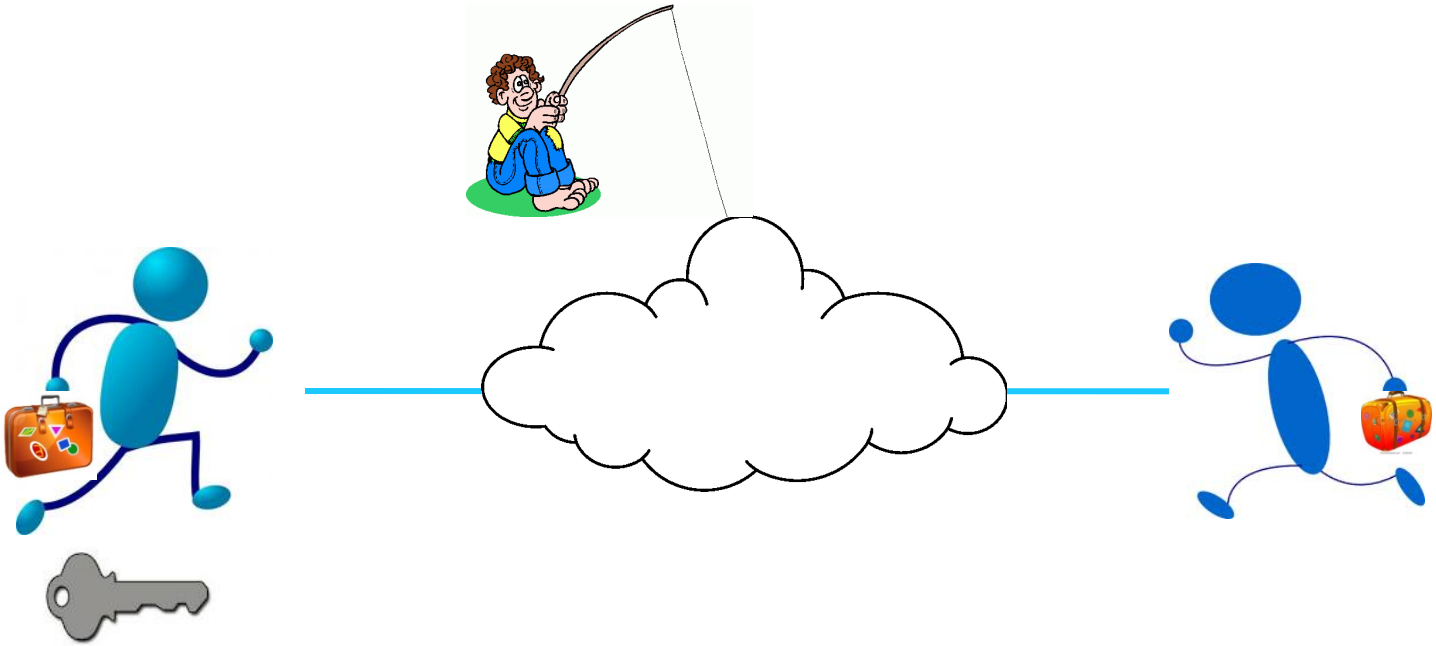
Terminology

- **MIC (Manufacture-installed certificate) :** Cisco Manufacturing automatically installs this certificate in supported phone models. Manufacturer-installed certificates authenticate to Cisco Certificate Authority Proxy Function (CAPF) for LSC installation.
- **LSC (Locally significant certificate)** : The LSC secures the connection between Cisco Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.



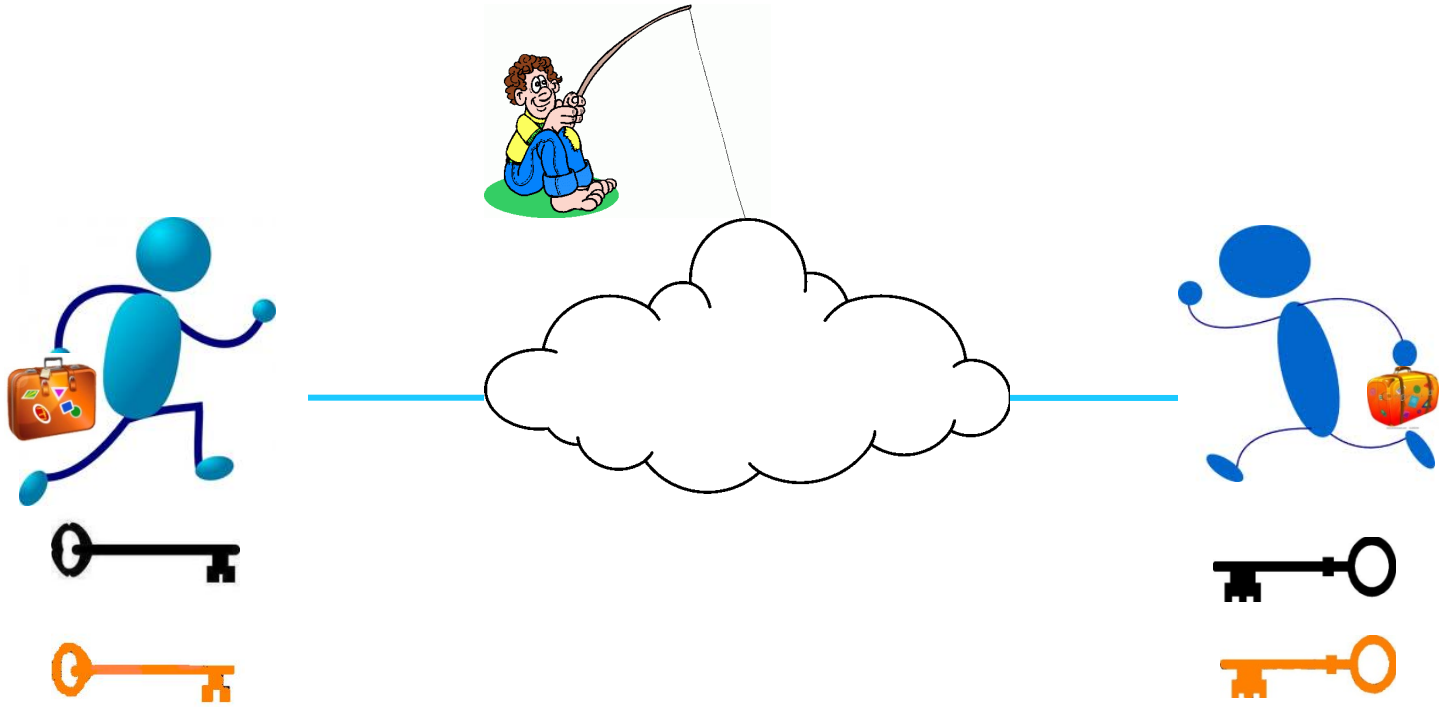
Security Fundamentals

Symmetric Encryption



Limitation: Secret Key can be compromised & the data decrypted

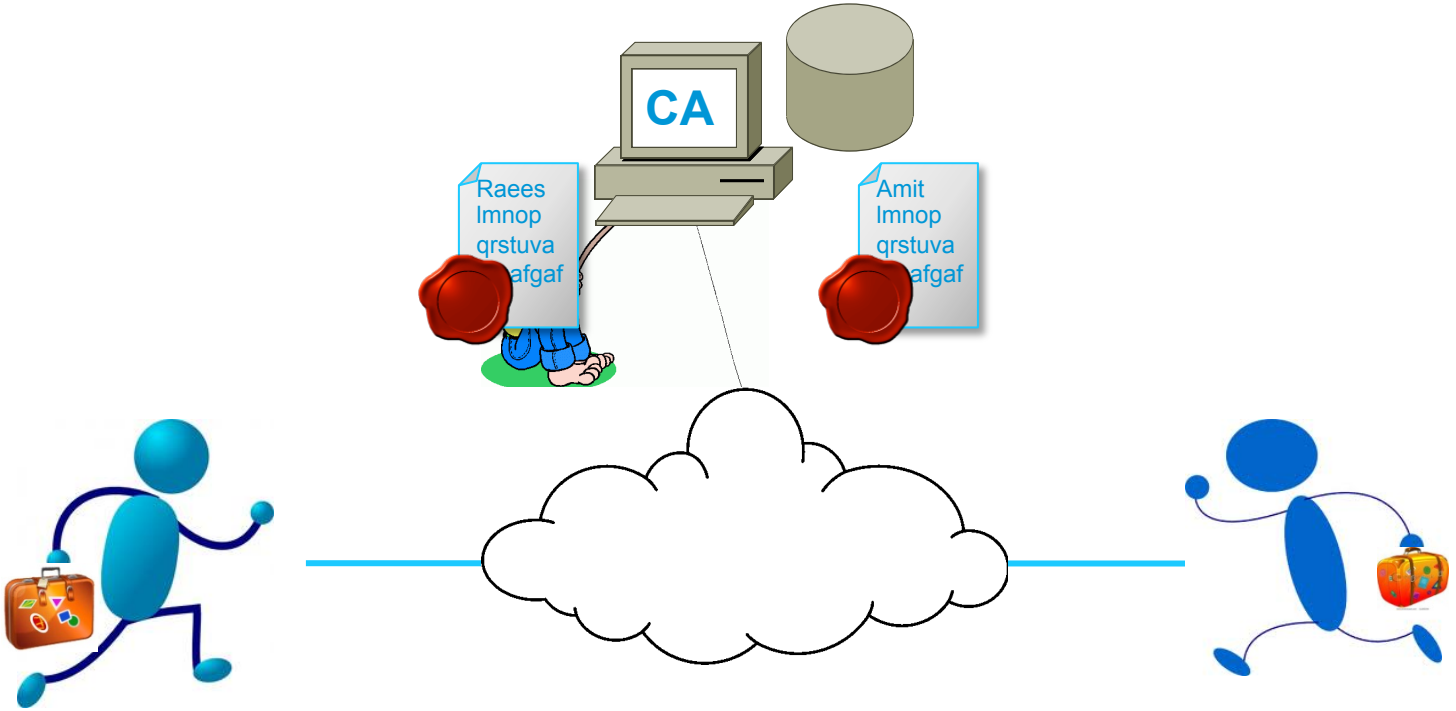
Asymmetric Encryption



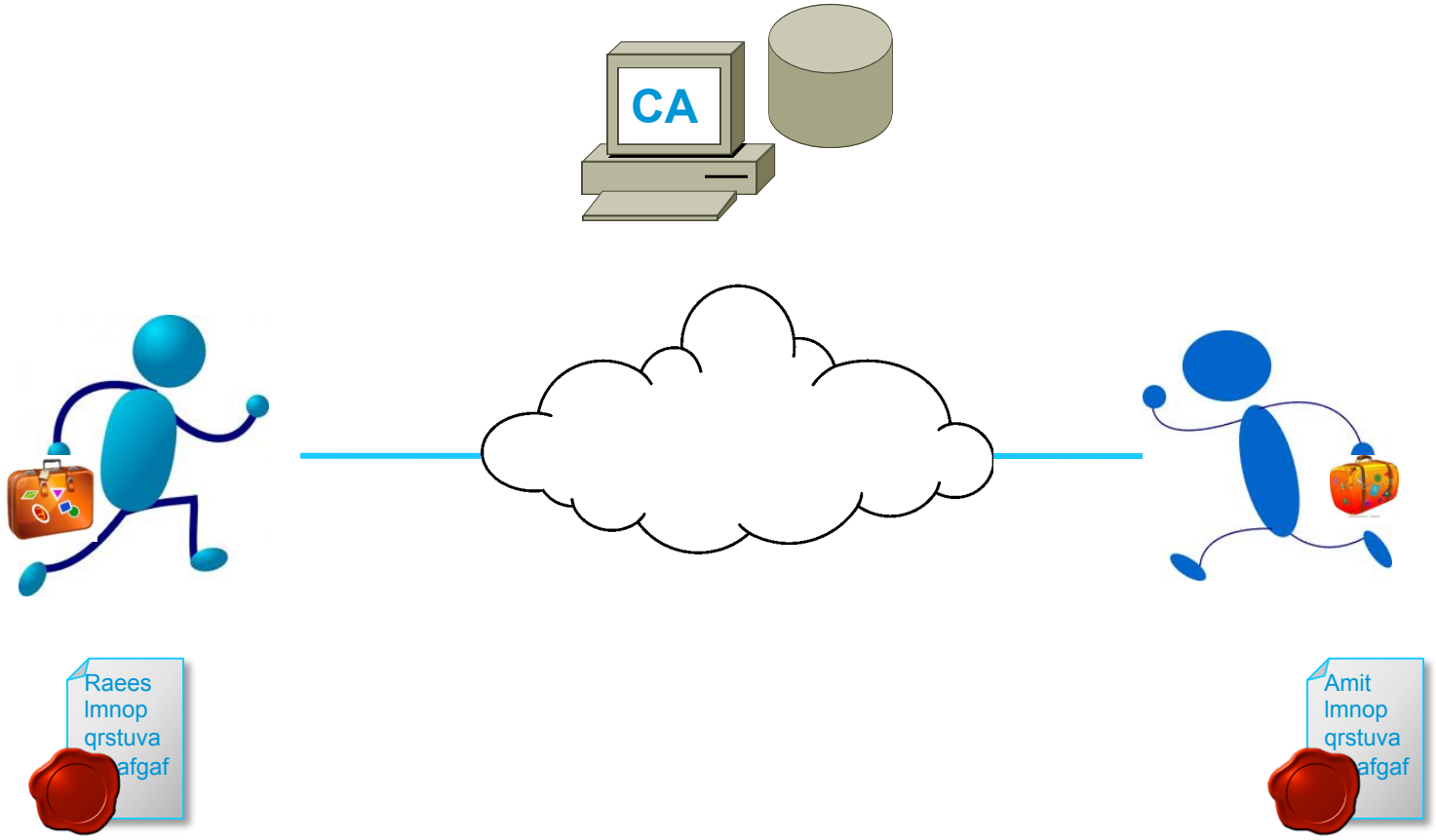
Limitations :

how to be sure that we are using the correct public key for an entity we communicate with ?

Public Key Infrastructure



Public Key Infrastructure



Phones Security in Pre-8.0 CUCM

- Built around the CTL paradigm: all trusted certificates bundled in a digitally signed file (CTL File). CTL File is downloaded by phones.

Issues:

- **Not scalable**: CTL File does not scale well with the growing number of certificates that a phone might need to trust.
- **Not flexible**: Every time a new certificate needs to be trusted, CTL File needs to be rebuilt, signed and downloaded to phones. Similarly, every time a certificate should not be trusted anymore, the CTL File needs to be rebuilt, signed and downloaded to phones.

Security by Default

- Default authentication of TFTP downloaded files (configuration, locale, ringlist, etc) using a signing key.
- Optional encryption of TFTP configuration files using a signing key.
- Certificate verification for phone initiated HTTPS connections using a remote certificate trust store on Communications Manager (Trust Verification Service).

Phones that Support SBD (and TVS)

Supported:

TNP Phones – 7906, 7911, 7931, 7941, 7961, 7970, 7971

Wireless IP Phones – 7921, 7925 (CSCsz46363: load pending)

Guinness Phones – 7942, 7945, 7962, 7965, 7975

Conference station (Polycom) – 7937 (CSCsz46415: load pending)

RoundTable Phones

Not Supported:

7905, 7912, 7920, 7936, 7940, 7960, 7985 (Tandberg)

The ITL File (Identity Trust List)

- Basically, the ITL File is a smaller, leaner CTL File.
- ITL File has the same format as the CTL File
- Unlike the CTL File, the ITL File is built automatically when the cluster is installed.
- The ITL File does not require eTokens. It uses a soft eToken (the TFTP private key).
- The ITL File is downloaded by phones at boot up time or during reset, right after downloading the CTL File (if present).
- The ITL File consists of TFTP/CM Certificate, TVS Certificate and the CAPF Certificate.

Signed Configuration file

- Once the CUCM upgrade from 7.x to 8.x version is complete, the phone will upgrade its firmware too

4536	720.312989	14.160.112.101	14.160.112.118	TFTP	61 Error Code, Code: File not found, Message: File not found
4742	754.298980	14.160.112.118	14.160.112.101	TFTP	70 Read Request, File: SCCP75.9-2-3S.loads, Transfer type: octet
4743	754.319531	14.160.112.101	14.160.112.118	TFTP	558 Data Packet, Block: 1
4744	754.320124	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 1
4745	754.320484	14.160.112.101	14.160.112.118	TFTP	184 Data Packet, Block: 2 (last)
4746	754.321013	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 2
4753	755.321433	14.160.112.118	14.160.112.101	TFTP	75 Read Request, File: jar75sccp.9-2-3TH1-9.sbn, Transfer type: octet

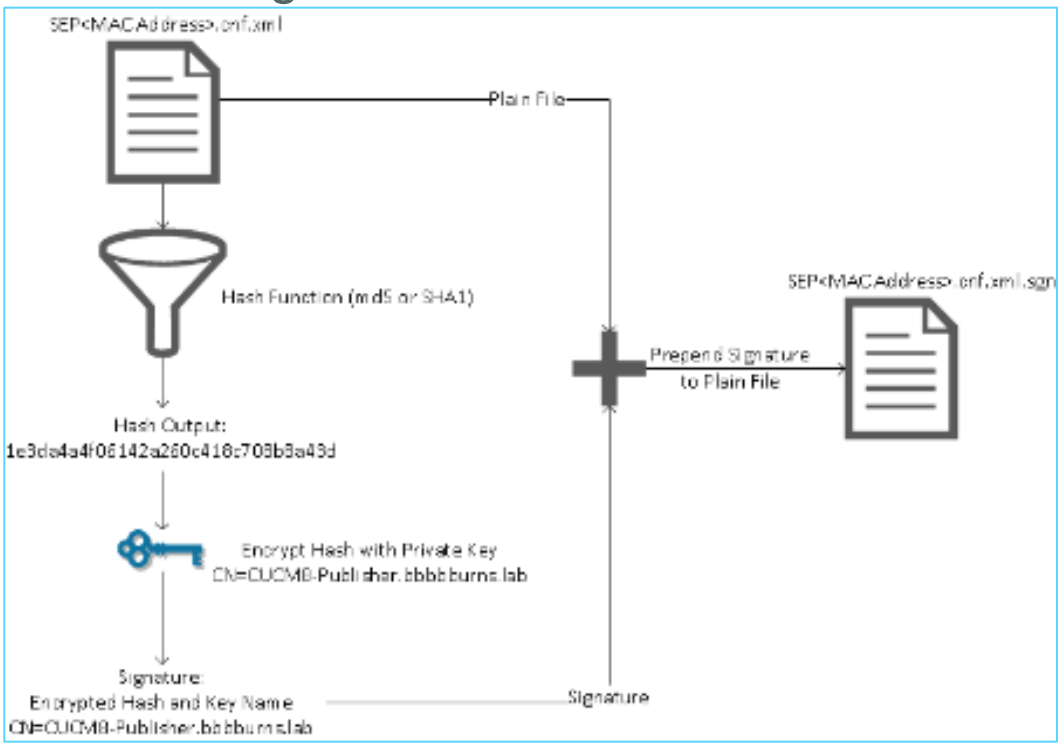
- Next, the phone will request for CTL and ITL Files

42991	798.621560	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 4324
44036	1001.16861	14.160.112.118	14.160.112.101	TFTP	73 Read Request, File: CTLSEP0026CBBDA45D.tlv, Transfer type: octet
44037	1001.16970	14.160.112.101	14.160.112.118	TFTP	61 Error Code, Code: File not found, Message: File not found
44039	1001.26922	14.160.112.118	14.160.112.101	TFTP	73 Read Request, File: ITLSEP0026CBBDA45D.tlv, Transfer type: octet
44040	1001.27033	14.160.112.101	14.160.112.118	TFTP	558 Data Packet, Block: 1
44041	1001.27137	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 1

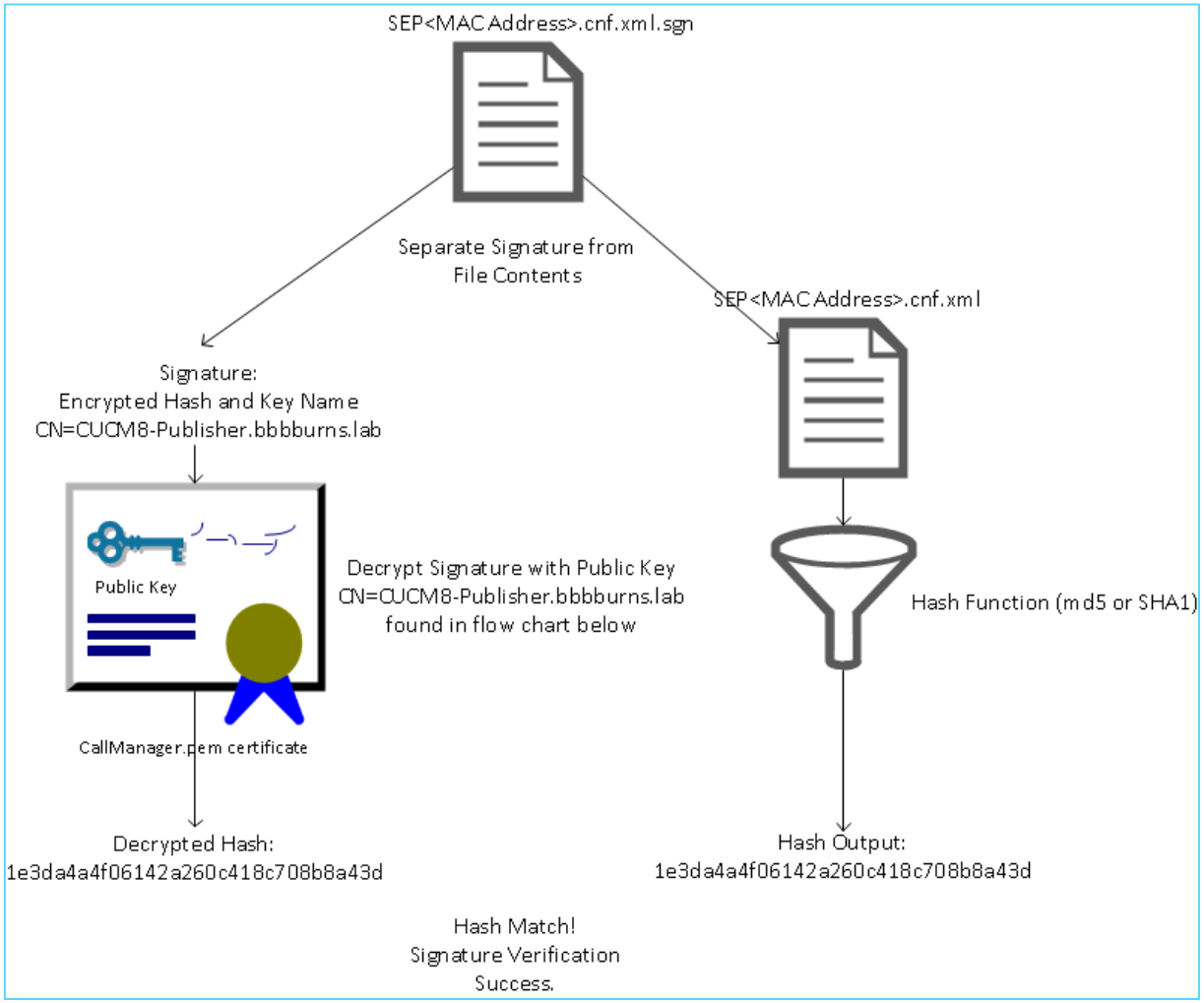
- Once the phone receives the ITL File, it will request for signed configuration file from the tftp server

44053	1001.27754	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 7
44055	1001.64878	14.160.112.118	14.160.112.101	TFTP	78 Read Request, File: SEP0026CBBDA45D.cnf.xml.sgn, Transfer type: octet
44056	1001.64978	14.160.112.101	14.160.112.118	TFTP	558 Data Packet, Block: 1
44057	1001.65041	14.160.112.118	14.160.112.101	TFTP	60 Acknowledgement, Block: 1
44058	1001.65077	14.160.112.101	14.160.112.118	TFTP	558 Data Packet, Block: 2

- The TFTP server uses the private key along with an MD5 or SHA1 hash function to create the signed file



- The phone after receiving the configuration file verifies the signature to confirm it has received the configuration file from the correct tftp source



TVS (Trust Verification Service)

- TVS is a new service that provides security with:

- **Scalability**: phones resources are not impacted by the number of certificates to trust.
- **Flexibility**: addition or removal of trust certificates are automatically reflected in the system.
- Non-media and signaling security features are part of the default installation and don't require user intervention.

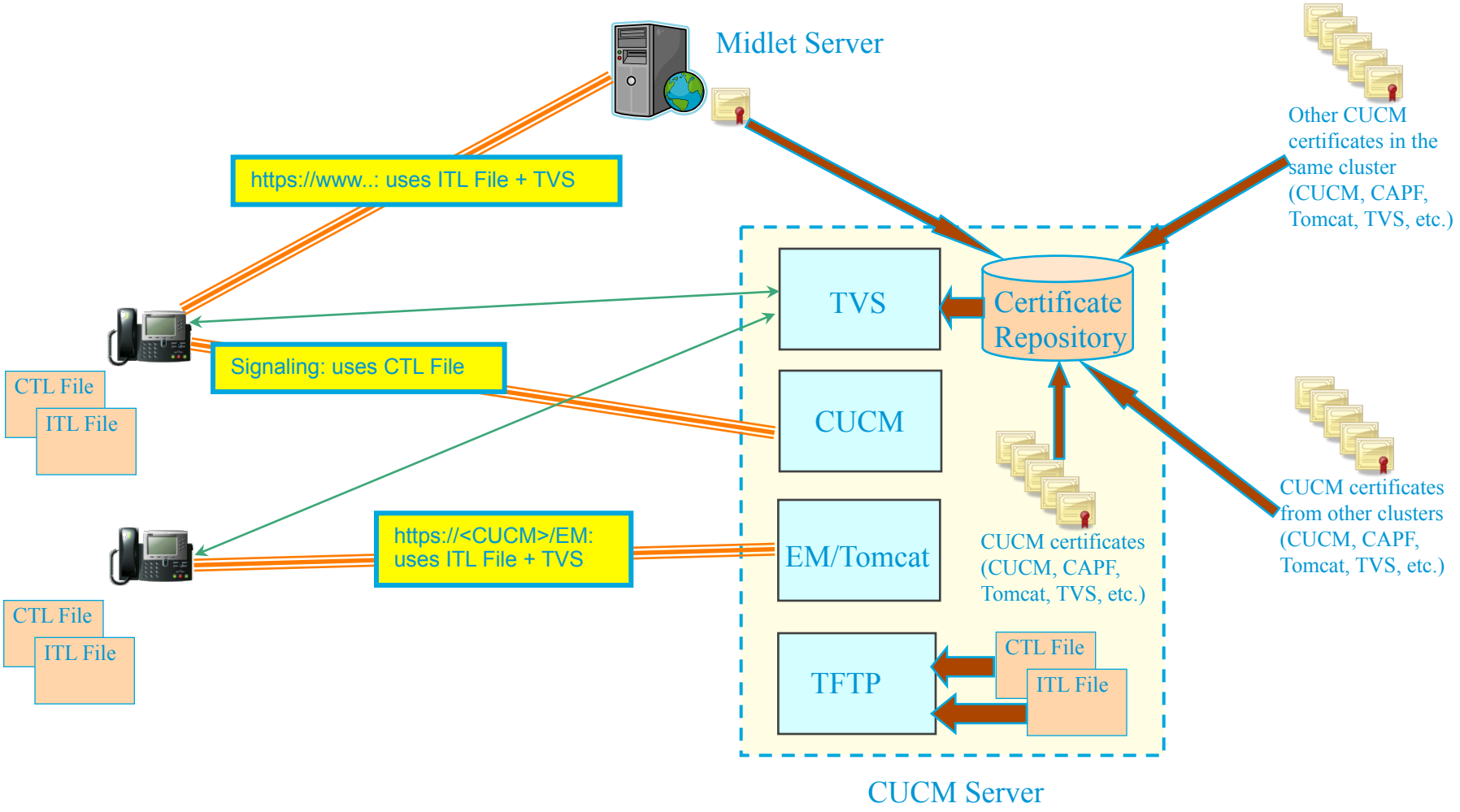
Note: Enabling secure signaling and media still requires the CTL Client.

TVS Basic Concepts

- TVS runs(Port 2445) on the CUCM server and authenticates certificates on behalf of the phone.
- Instead of downloading all the trusted certificates, phones need only to trust TVS i.e. the ITL file downloaded by the phone should consists of the TVS certificate to authenticate against the TVS service.
- The TVS service runs on all servers where Call Manager service is activated.
- In a multi-node CM cluster there can be up to three TVS entries for a phone, one for each CM in the CM Group of the phone.

.

The Big Picture



Polling Question 2

What Advanced CUCM topic are you interested in future webcast…

a) **Follow up session having live demonstration of CUCM Security and troubleshooting.**

b) **Cisco Extension Mobility Cross Cluster**

c) **CUCM Troubleshooting and Trace Reading**

Troubleshooting

- How to get TVS trace on CUCM (detailed mode), phone traces, phone status in phone UI, phone trust list, CLI: show ITL
- What to look for in the CUCM trace
- Service restart following some events (cert. regen)

What to Collect for Troubleshooting

- Enable detailed debug mode for the TVS service.
- Reproduce the issue
- Collect the TVS logs
- In CLI, run “show itl” and show “ctl” and copy paste their outputs to a file(s).
- Collect phone debugs. You can either copy/paste the IP address of the phone into you browser and collect all console logs or use a serial cable.

What to Collect for Troubleshooting (cont.…)

- The xml configuration file of any one of the SBD capable phones. You can obtain it from your laptop by:

```
C:\> tftp -i <your_TFTP_server> get SEP<MAC_Addr_phone>.cnf.xml.sgn
```

- If a specific certificate is thought to be causing a problem, display it in the Certificate Management in the OS Admin UI and copy/paste it to a file.
- Certificate management Logs
- Change Notification Logs

Common Issues and Remedies

I moved my phone to another cluster and it does not register

- **Rollback Enterprise Parameter**

Once "Prepare Cluster for Rollback to pre-8.0" enterprise parameter is set to True, the phones will download ITL file, with empty TVS and TFTP certificate sections.

Phone with an empty ITL file it will accept any unsigned configuration file and any new ITL file .

- **Bulk Certificate Export**

The Bulk Certificate Export method will only work if both clusters are online with network connectivity while the phones are being migrated.

- **Using Hardware Security tokens (KEY-CCM-ADMIN-K9=)**

If we use the same Security Tokens to generate CTL(Certificate Trust List) on old and new Clusters, phones can migrate between clusters.

- **Manually Delete ITL Files**

For any reason if the Certificates or TFTP Private key is not available from the old Cluster, then we need to manually delete the ITL file from phone.

Downgrade/Rollback server to Pre 8.0+

- Set the “Prepare Cluster for Rollback to pre-8.0” Enterprise Parameter to true.
- Restart TVS, TFTP and CUCM on all the node.
- Downgrade server

I have regenerated my CAPF/TVS/CUCM certificate and now my phones don't register

If any of the CAPF, TFTP or TVS certificates is regenerated, the ITL File needs to be updated on the phones. The general procedure is:

- Restart CAPF if the CAPF certificate was regenerated.
- Restart TFTP, so that it refreshes its cache with the new ITL Fille.
- Reset phones or Restart CUCM on all the nodes to force phones to download the new ITL File.

Note* TVS does not need to be restarted and no user intervention is required to rebuild the ITL File.

If you plan to regenerate multiples certificates you must regenerate the TFTP certificate last.

Whenever the TFTP certificate gets regenerated, you must create a new system backup(CUCM 8.0+ DRS backs up TFTP cert and Key)

I upgraded my CUCM 7.x secure cluster to CUCM 8.0+ and phones cannot register

Re-run the CTL Client and update the CTL File if Cluster was in mixed mode.

Auto-registration and SBD

- If the cluster is in non-secure mode, auto-registration will still be supported.
- The default configuration file in 8.0+ will also be signed.
- Phones that don’t support SBD will be served a non-signed default configuration file.

Auto-registration will still not be supported in mixed mode.

Server re-Image

- If a 8.0+ server is re-imaged with another 8.0+ release, a new TFTP private key will be generated
- Phones will be not be able to trust the new ITL File.
- Unless the user deletes the ITL File on every phone, phones will not register.

Set the “Prepare Cluster for Rollback to pre-8.0” Enterprise Parameter to true.

Restart TVS, TFTP and CUCM on all the node.

Re-image server

SUMMARY

- CUCM 8.x + have Security By Default Enabled
- TVS is the new service introduced and will continue in future releases as well
- Ensure TVS Port 2445 is open in your network.
- Auto-registration will still not be supported in mixed mode.
- Once "Rollback Enterprise Parameter" parameter is set to True, the phones will download ITL file, with empty TVS and TFTP certificate sections.
- Any time we regenerate TFTP certificates, take DRS Backup.

Supported Cisco Unified IP Phones

You can obtain a list of the Cisco Unified IP Phones that support security by default by using Cisco Unified Reporting

Future Release Enhancements

- Single Sign On
- PKCS7 Chain upload
- Deleting ITL files from all the phones using UI from CUCM 9.5 onwards

Reference

- Reference 1
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_0_2/secugd/sec-802-cm.html
- Reference 2
  https://supportforums.cisco.com/docs/DOC-17679
- Reference 3
  https://supportforums.cisco.com/docs/DOC-18834
- Reference 4
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html

Submit Your Questions Now!

Use the Q&A panel to submit your questions. Experts will start responding those

Polling Question 3

How useful was this presentation?

a) This was very informative presentation and will help me in understanding Security in CUCM 8.0+.

b) This presentation needed more in depth details.

c) I wanted to see some information on configuration

d) This presentation was somewhat useful

Q & A

Expert responding some of your questions verbally. Use the Q&A panel to continue asking your questions

We Appreciate Your Feedback!

Those who fill out the Evaluation Survey will enter a raffle for a free:

$20 USD Gift Certificate

To complete the evaluation, please click on link provided in the chat or in the pop-up once the event is closed.

Ask The Experts Event (with Expert)

If you have additional questions, you can ask them to Experts. They will be answering from day 3rd April to 13th April

https://supportforums.cisco.com/community/netpro/ask-the-expert

You can watch the video or read the Q&A 5 business days after the event at
https://supportforums.cisco.com/community/netpro/ask-the-expert/webcasts

Next Expert Series Webcast

Topic: Cisco Smart CallConnector and New Mobile Clients

Tuesday, May 8th, at

8:00 a.m. San Francisco (PDT UTC -7)
11:00 a.m. New York (EDT UTC -5),
4:00 p.m. London (BST UTC +1)
5:00 p.m. Brussels (CEST UTC +2)

Join double CCIE, Technical Leader

Jazib Frahim from **RTP**.

He will provide reasons why enterprise network segments get compromised despite their state-of-the-art network security technologies and products that are deployed.

During this interactive session you will be able ask all your questions related to this topic.

Registration will be opened on April 10 at

https://supportforums.cisco.com

First Expert Series Webcast in Russian

Topic: Troubleshooting Common Problems of Layer 3 VPN Multiprotocol Label Switching Networks

Tuesday, April, 17 at

12:00 p.m Moscow Time (MSK UTC +4)

10:00 a.m Brucels Time (CEST UTC +2)

Join double CCIE in R&S and SP

Igor Tumkin from **TAC Center in Moscow**

He will focus on the most common problems of Layer 3 VPN (L3VPN) Multiprotocol Label Switching (MPLS) networks and little-known technical features of MPLS infrastructure

During this interactive session you will be able ask all your questions related to this topic.

Register for this live Webcast at

http://tinyurl.com/c5stz86 or

http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=R&PRIORITY_CODE=4&SEMINAR_CODE=S16357

Next Ask the Expert event in English

Topic: Cisco Prime Network Registrar

This event will be opened from April 9 to April 20th.

Featured Experts

Pete Newcomb and Jim Brown

During this event you will have an opportunity to learn about the newest release of Cisco Prime Network Registrar, Cisco's industry leading solution for integrated DNS, DHCP and IP address management (IPAM) services for both IPv4 and IPv6.

Pete is a Technical Marketing Engineer with over 30 years of experience.

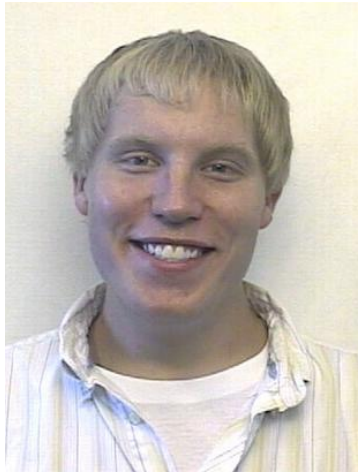
Jim is a Customer Support Engineer with over 14 years working with the Network Registrar Development Team

Join the discussion @

https://supportforums.cisco.com/community/netpro/expert-corner

Next Ask the Expert event in English

Topic: Cisco Hosted Collaboration Solution



This event will be opened from April 9 to April 20th.

Featured Expert

Matt Blanshard

During this event you will have an opportunity to learn and ask questions related about Cisco's new Hosted Collaboration Solution architecture and deployment with Cisco expert Chris Ward.

Chris is a technical marketing engineer working on the Cisco Hosted Collaboration Solution. .

Join the discussion @

https://supportforums.cisco.com/community/netpro/expert-corner

We invite you to actively collaborate in the Cisco Support Community and social media

https://supportforms.cisco.com

http://www.facebook.com/CiscoSupportCommunity

http://twitter.com/#!/cisco_support

http://www.youtube.com/user/ciscosupportchannel

http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

Newsletter Subscription: https://tools.cisco.com/gdrp/coiga/showsurvey.do?surveyCode=589&keyCode=146298_2&PHYSICAL%20FULFILLMENT%20Y/N=NO&SUBSCRIPTION%20CENTER=YES

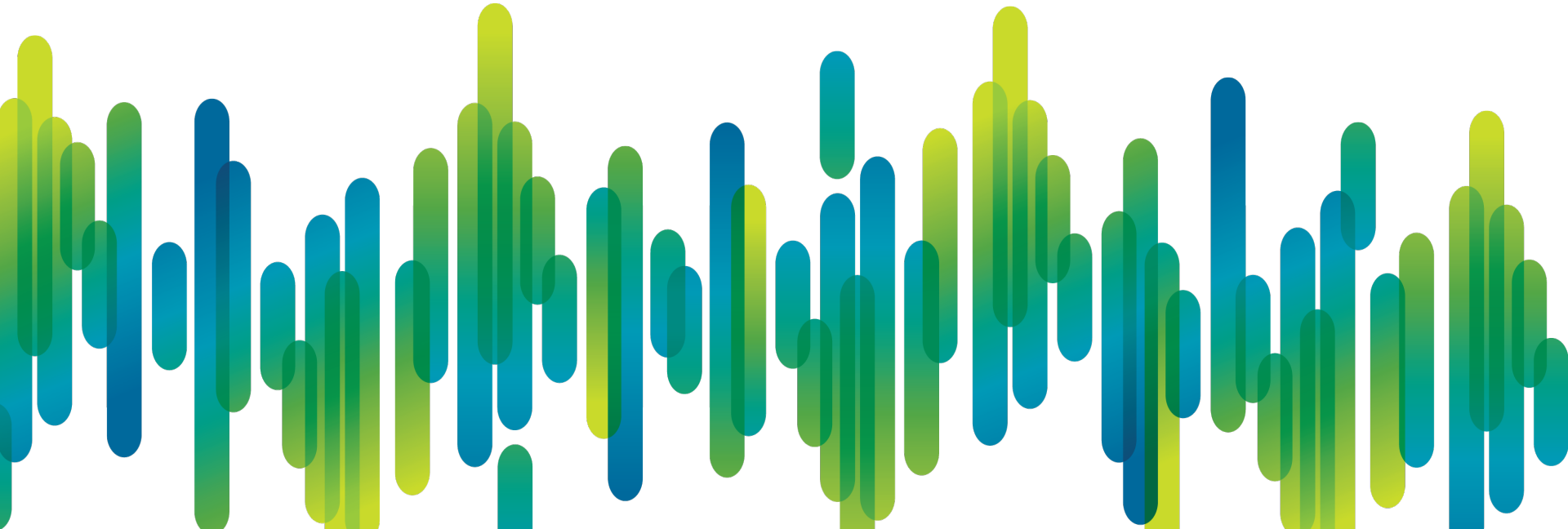
We have communities in other languages

If you speak Spanish, Portuguese, Japanese, Polish or Russian, we invite you to ask your questions and collaborate in your language.

- Spanish → https://supportforums.cisco.com/community/spanish
- Portuguese: → https://supportforums.cisco.com/community/portuguese
- Japanese → https://supportforums.cisco.com/community/csc-japan
- Polish → https://supportforums.cisco.com/community/etc/netpro-polska
- Russian https://supportforums.cisco.com/community/russian

Thank You for Your Time

Please Take a Moment to Complete the Evaluation



Thank you.