



Cisco Support Community Expert Series Webcast



Understanding and Managing Cisco Unified Communications Manager Certificates

Akhil Behl

Solutions Architect

Author of '*Securing Cisco IP Telephony Networks*'

<http://www.ciscopress.com/title/1587142953>

Jan 7th 2014

Cisco Support Community – Expert Series Webcast (Presenter and Speaker)

- Today's featured expert is Cisco's Solutions Architect Akhil Behl
- Ask him questions now about CUCM Certificates and UC Security



Akhil Behl
(Solutions Architect)

Cisco Support Community – Expert Series Webcast (Panel of Expert)



Aashish Jolly
(Sr. Network Consultant)

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:



Document url:

<https://supportforums.cisco.com/docs/DOC-39186>

Polling Question 1

Do you have UC Security deployed in your Cisco Collaboration network?

- a) Yes – I have multiple UC security controls deployed and leverage them in my Cisco Collaboration network**
- b) No – But I want to deploy UC Security and ensure that my Cisco Collaboration network is protected against common and uncommon threats**
- c) I'm not sure if I should have UC Security in place, it's still in the works**
- d) I'm pretty sure that my network is hack/attack proof and I don't need UC Security as I have firewalls, (N/H)IPS, Content Aware security etc.**

Submit Your Questions Now!

Use the Q&A panel to submit your questions. The expert panelist will start responding those





Cisco Support Community Expert Series Webcast



Understanding and Managing Cisco Unified Communications Manager Certificates

Akhil Behl

Solutions Architect

Author of '*Securing Cisco IP Telephony Networks*'

<http://www.ciscopress.com/title/1587142953>

Agenda



An introduction to Cisco Unified Communications PKI

Insight to CUCM Certificates

Understanding CUCM Certificates and their Functions

Managing CUCM Certificates

Q&A



An Introduction to Cisco Unified Communications Public Key Infrastructure

What is Public Key Infrastructure (PKI)?

The Basics

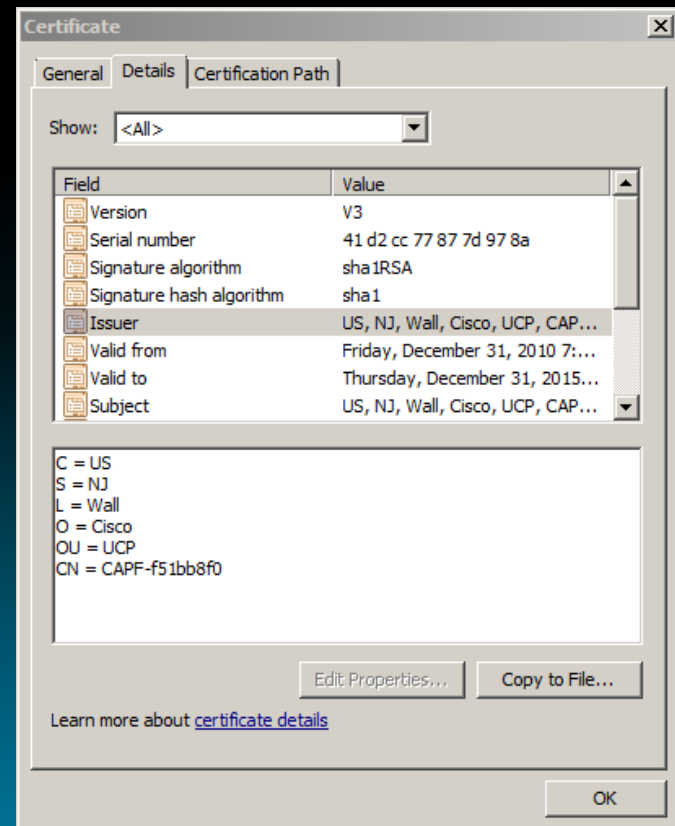
- PKI provides a secure, scalable public key distribution mechanism.
- PKI offers Encryption and Digital Signature Verification Services.
- PKI enrollment must be performed securely and some form of PKI revocation is always required.
- X.509v3 is the standard for PKI data formats and protocols.

The X.509v3 Standard

The Standard

X.500 was the original standard (never implemented) aimed to have a global naming structure (Directory Information Tree) with everything leading to the same root, with countries directly under the root.

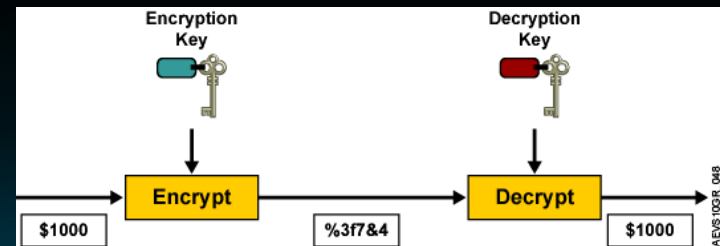
- CN – Common Name
- OU – Organizational Unit
- O – Organization
- L – Locality
- S – State
- C – Country



Encryption

Cryptography

- Encryption is the process via which the Confidentiality or Privacy of a message is maintained. RSA, Blowfish, IPsec, SSL, are various encryption algorithms/processes.
- While encrypting, a message is transformed to gibberish, using either symmetric (same key) or asymmetric (different key) encryption.



- In Cisco Unified Communications Manager (CUCM) and rest of Cisco Collaboration applications, asymmetric encryption is used for encrypting signaling (TLS) and media (SRTP).

PKI Components

The Building Blocks

- **Certificate Authority (CA)**
Trusted third party that signs CSR, binding key to Identity Certificate.
- **Registration Authority (RA)**
Part of the CA – Verifies that you own the name being signed in the certificate.
- **Certificate Signing Request (CSR)**
Requested name, combined with public key data.
- **Identity Certificate**
Certificate resulting from CA signing the CSR. Installed on the server.
- **CA Certificate**
A self signed certificate generated by a trusted third party (CA). Used to sign CSR. Installed on the client before signed certificate can be installed.
- **Server**
Entity serving data.
- **Client**
Entity accessing data.

Certificate Chains

The Dominos Effect

Certificate Chain



PKI Client to Server Certificate Signing Overview

- Client generates a key pair on the requesting server and submits a CSR with desired name to a trusted or local CA
- CA (or intermediary CA) accepts the CSR and signs it with its private key to create a CA signed Identity Certificate that will be installed on the requesting server
- Client downloads a list of trusted CA certificates (root CA and any intermediary CA certificates as mandated by the CA)
- Client installs the root CA certificate (and any intermediary CA certificate)
- Client installs CA signed CSR (now identity certificate)



An Insight to CUCM Certificates

Polling Question 2

Which CUCM Certificate based services do you leverage in your Cisco Collaboration network?

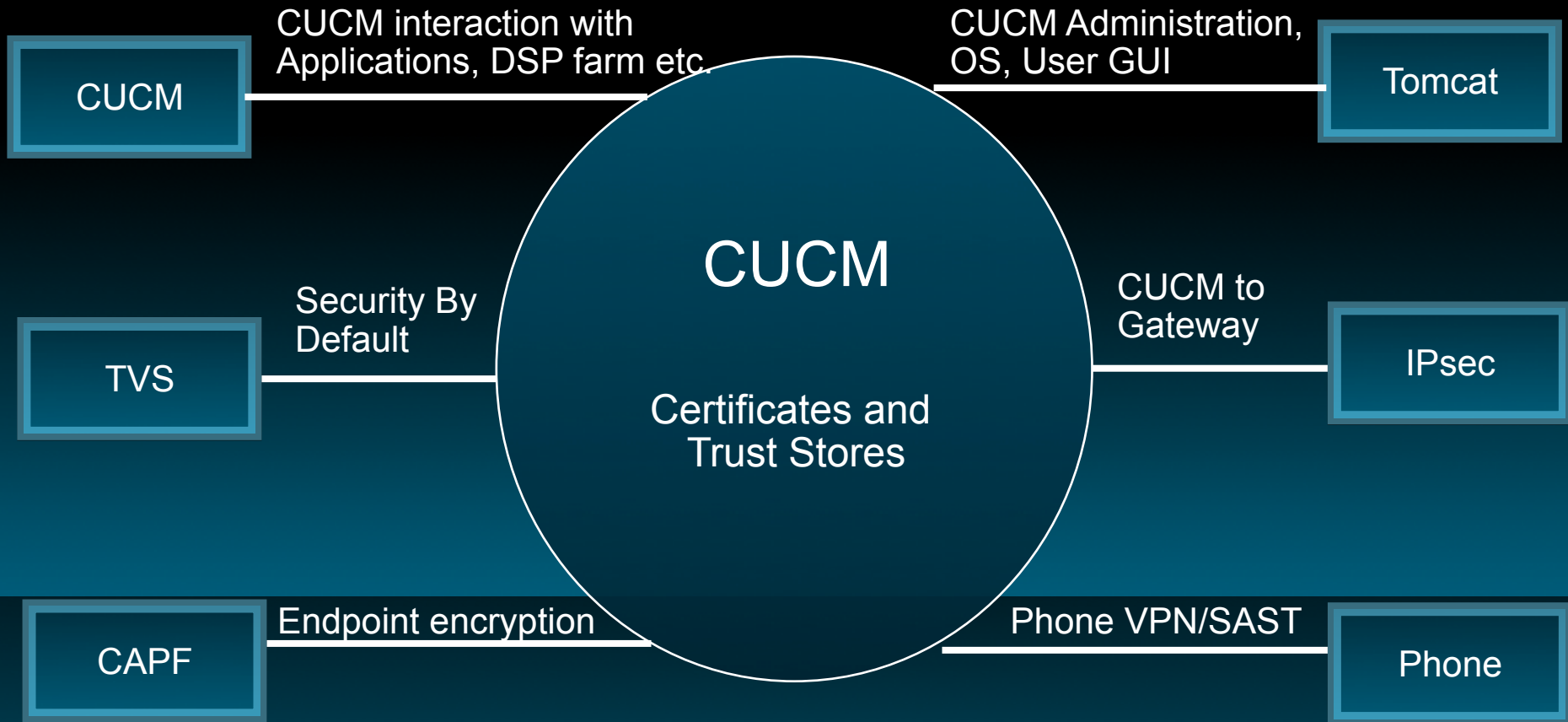
- a) I'm not sure if I'm even using any certificates based service till date
- b) I leverage most commonly used certificates such as Cisco Tomcat, CAPF and TVS
- c) I leverage all available services that use certificates
- d) I have plans to/thinking about using certificates other than Tomcat

Cisco Unified Communications Manager Certificates

CUCM has multiple certificates for multiple purposes however, the major mode of operation pertinent to security remains with Manufacturing Installed Certificates (Cisco Manufacturing) or Externally Signed Certificates (signed by VeriSign, Geotrust, Microsoft CA, CAPF)




- Cisco Manufacturing Certificates (Cisco CA)
- Self-Signed Certificates (Built-in CA generated certificates Tomcat, IPsec, TVS, VPN Phone, CAPF, CallManager)
- Certificates for endpoints (MIC or LSC – MIC is derived from Cisco CA whereas LSC is derived from CAPF)

CUCM Certificates



CUCM Certificates (Cont.)

Certificate List

 Generate New  Upload Certificate/Certificate chain  Generate CSR

Certificate List (1 - 19 of 19)

Find Certificate List where

Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	VeriSign Class 3 Secure Server CA - G3.pem
tomcat-trust	trust-certs	cucmpub.pem
ipsec-trust	trust-certs	cucmpub.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco Manufacturing CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem
CallManager-trust	trust-certs	CAPF-af6b1cd2.pem
CAPF-trust	trust-certs	Cisco Manufacturing CA.pem
CAPF-trust	trust-certs	CAP-RTP-001.pem
CAPF-trust	trust-certs	Cisco Root CA 2048.pem
CAPF-trust	trust-certs	CAP-RTP-002.pem
CAPF-trust	trust-certs	CAPF-af6b1cd2.pem
Phone-VPN-trust	trust-certs	CAPF-f51bb8f0.pem

CUCM Certificate Essentials

- There are two major certificate stores in CUCM – **certificate-type-trust** and **certificate**. Each service has its own service certificate and trust certificates.
- Trust acts as local root for the certificate i.e. self-signed or trusted CA signed root CA (and intermediary CA) certificates go to trust whereas identity (or signed) certificates go to regular certificate store.
- When accessing any service e.g. Tomcat, it is the identity certificate that is presented to requesting client and the trust certificate (root) acts as an authenticator in the background.
- As each node is identified by its unique name (hostname), each node must generate a CSR that is signed by external CA (remember that certificates work on CN=hostnames)

CUCM Certificate Essentials (Cont.)

- CUCM offers ability to generate CSR, upload or download certificates and delete (certain instances) certificates.
- It is possible to enable certificate expiry monitor such that before actual expiry of certificate, a notification is sent to pre-defined email address.
- Bulk certificate management (export/import) is offered by CUCM for functions like Extension Mobility Cross Cluster.



CUCM Certificate Formats

- CUCM can support various certificate formats such as DER (Distinguished Encoding Rules) and PEM (Privacy Enhanced Mail).
- DER is a binary encoded file that has special characters when opened in a text editor.
- PEM is a Base-64 encoded block file, that can be easily opened in text editor and has clear BEGIN CERTIFICATE and END CERTIFICATE markings.
- CER, CRT, CSR are various extensions to a certificate file and can be either in DER or PEM format.

CUCM Certificate Format – CA Certificate

- Following is an output from a CA root certificate

Version: V3

Serial Number: 13191820897365828600584855809293073756

SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)

Issuer Name: CN=APJCPDI-PDI-CA, DC=APJCPDI, DC=LAB

Validity From: Mon Jan 06 02:28:22 IST 2014

To: Sun Jan 06 02:38:20 IST 2019

Subject Name: CN=APJCPDI-PDI-CA, DC=APJCPDI, DC=LAB

Key: RSA (1.2.840.113549.1.1.1)

CUCM Certificate Format – CSR

- Following is an output from a Certificate Signing Request (CSR)

-----BEGIN CERTIFICATE REQUEST-----

```
MIIDQDCCAigCAQAwgbMxCzAJBgNVBAYTAKIOMQ4wDAYDVQQIEwVrdGFrYTE  
OMAwGA1UEBxMFYmxvcmUxDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEw  
NwZGkxGzAZBgNVBAMTEkNVQ005MC5hcGpjcGRpLmxhYjFJMEcGA1UEBRNA  
NTgwMmU4ZjQ2MwIwNwViMmFkNjJINDA1NjZmNDQ3YmUyOTJmMTYxZmExM  
zlxMjQ2Y2FIN2UwMjMyYjUwMzM3MDCCASlwDQYJKoZIhvcNAQEBBQADggE
```

<removed for brevity>

```
DMdVpv7StkqbL+yH8PEX3my8ctvsKWODvzP+/8cj6dEZ3NWOHRsxnUZL9R  
+yFIfPGmC8Awlh3G1rLR3TNEsfyOHwBFZxqBrdE7fNVELDcj7xmlrKusSJQhBmav  
PDv7KmfdrZct+A/Wrqby1PTh5yiYetL3UxxFXdIA0Fbx4i/  
YNGDyEHziliSgYhGrcHs61NqW9OY7nFHbkPiXUvIFMJ6+AaUYNizNSucoDRaJg  
3hGWjkSn0+4cYsd/EDX2E/RjhE3JX9LL2buFUDHiSpxqN1Kbs=  
-----END CERTIFICATE REQUEST-----
```

CUCM Certificate Format – Identity Certificate

- Following is an output from a CA signed (identity) certificate

Version: V3

Serial Number: 458323223657516437078018

SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)

Issuer Name: CN=APJCPDI-PDI-CA, DC=APJCPDI, DC=LAB

Validity From: Mon Jan 06 02:36:27 IST 2014

To: Wed Jan 06 02:36:27 IST 2016

Subject Name: CN=CUCM90.apjcpdi.lab, OU=pdi, O=cisco, L=blore,
ST=ktaka, C=IN

Key: RSA (1.2.840.113549.1.1.1)



Understanding CUCM Certificates and their Functions

CUCM Tomcat Certificate

- CUCM Tomcat certificate is leveraged for CUCM Administration, OS, CCMUser, DRS GUI interfaces.
- Moreover, recent versions of CUCM starting CUCM version 8.5 and later, Tomcat certificate is also used for Secure LDAP (LDAPS) integration with Microsoft, Netscape, and other X.500 compatible AD services.
- Tomcat server redirects unencrypted (HTTP) sessions to HTTPS sessions (TCP port 80 to 8443) using default self-signed certificate.
- Tomcat certificate can be signed by external (trusted) CA such that the HTTPS / LDAPS connections are initiated based on trusted root CA (chain). This requires the client / LDAP server(s) to also have root CA certificate (and any intermediary CA certificates)

CUCM IPsec Certificate

- CUCM IPsec certificates are used for securing communication between CUCM and voice gateway.
- Also, as IPsec tunnels are also created between CUCM cluster members (implicit during install) for secure traversal of intra-cluster signaling, IPsec certificates are used for the same as well.
- IPsec certificates are vital for services like DRF (Cisco DRS) and backup restore can fail if IPsec certificates are not in sync between nodes.

CUCM CAPF Certificate

- CUCM CAPF certificate is leveraged for secure endpoint communication with CUCM / ASA (for signaling) and amongst themselves (for media).
- CAPF service enables creation of Certificate Trust List (CTL) file that is downloaded to all phones (irrespective of fact whether the endpoint is secure or not) and LSC certificate (on secure phones).
- CTL client enables security of a CUCM cluster as it signs server certificates with hardware eTokens.

CUCM CallManager Certificate

- CallManager certificate is used for secure integration with multiple applications and devices such as for secure DSP farm – secure mtp and secure conference bridge.
- CallManager certificate is also used for exchange with Cisco ASA (phone proxy, TLS proxy), with CUPS, Unity/Unity Connection and so on.

CUCM TVS Certificate

- TVS certificate is used for Security By Default (SBD) feature that is activated by default on CUCM version 8.0 and later.
- TVS certificate works behind the scenes for device to CUCM trust service and ITL.
- SBD does not need any physical eToken as the ITL file is built while CUCM cluster is installed and signed by built in TVS CA.

CUCM Phone VPN Certificate

- A Phone VPN certificate is used by Cisco Phone VPN service and is a result of Cisco ASA self-signed certificate uploaded to CUCM.
- Phone VPN certificate is intended to authenticate CUCM to ASA and vice-versa for proxy of signaling and media.
- Phone VPN itself can be setup for either username password (VPN Group) or certificate based authentication (using LSC as authentication certificate to ASA).

Polling Question 3

- **How do you manage you UC PKI?**
 - a) I have a central trusted CA / external CA via which I get all certificates signed and keep an eye on the certificate expiry**
 - b) I leverage the CUCM certificate expiry notification process and follow other Cisco recommended leading practices**
 - c) There is currently no specific set of processes for managing certificates in my Cisco Collaboration network, I'm looking for more insights to how I can setup a process**
 - d) I'm happy with self signed certificates and do not want to get into intricacies of UC PKI**



Managing CUCM Certificates

CUCM Certificate Management – Certificate Expiry

- CUCM certificates whether self-signed or signed by external CA have a definite expiry date.
- Upon expiry of a certificate (or root/trust CA certificate), the associated certificate functions no longer work.
- To avoid any certificate expiry related issues, it is recommended to enable Certificate Expiry Monitor and associated email notifications.
- The leading practice recommendations are to either regenerate a certificate or replace it with a valid certificate well in advance. This may require a maintenance window so plan well.

CUCM Certificate Management – Upgrade to newer version

- While upgrading to a newer version, if a backup is taken from existing CUCM and restored to new CUCM, all certificates and respective keys (ideally) get transferred to new platform (provided the IP addresses / hostnames remain the same).
- It is however, in certain cases (due to certain bugs) that DRS restore may not have required keys/certificates. In such case, it is essential to either regenerate certificate(s), get new signed certificate(s) or re-run CTL client (specifically for CAPF).
- While upgrading from an earlier to a newer release (minor or major release) it is worthwhile to upgrade (where possible) in isolation as a standalone cluster and register a few endpoints to see if they come up as expected.
- Set the enterprise parameter for roll-back when upgrading from pre 8.x to 8.x or later releases.

CUCM Certificate Management – Lost eTokens

- Many a times eTokens can be lost and a cluster can no longer be changed from its current state (secure to unsecure) or a member be added or removed from a cluster. It is therefore recommended to have more than 2 eTokens (default minimum quantity required) to sign the cluster and store in pairs under lock and key at different sites.
- If an eToken pair or all eTokens are lost, the only way out is to rebuild a new cluster and import configuration using BAT and secure it using a new pair of eTokens.

Certificate Management Tools – Windows Certificate Viewer

- Certificate Management Tools help in looking at certificate information and resolve issues pertinent to PKI.
- Most commonly used tool is – Windows Certificate Viewer
- It is easy to use (built into Windows machines), helps find out the certificate path, supports both .pem and .der formats as well as better known .cer format.
- Limitation includes non usability with CSR file and certificate path being represented by local certificate cache.

Certificate Management Tools – OpenSSL

- OpenSSL can be regarded as the ‘Swiss Army Knife’ for certificates (<http://www.openssl.org/>)
- It’s a CLI tool (the only real limitation) that can work with certificates and keys (e.g. RSA keys).
- Helps viewing CSR, verifying keys, certificate match and viewing SSL handshake in real time.
- Syntax is - openssl <command> <options> where commands can be rsa (for working with RSA keys), x509 (for working with x.509v3 certificates), req (for working with CSRs)



Securing Cisco IP Telephony Networks

Securing Cisco IP Telephony Networks



IP COMMUNICATIONS



Securing Cisco IP Telephony Networks

The real-world guide to securing Cisco-based IP telephony applications, devices, and networks

ciscopress.com

Akhil Behl, CCIE® No. 19564

- Addresses the prominent void where UC and Security technologies converge
- Security primer for new professional and refresher for experienced professionals
- Covers threats, risk assessment, security strategy development, security framework
- Covers network infrastructure security, UC application security, UC endpoint security, network management security, advance firewalling and Intrusion Prevention
- A plethora of step-wise instructions, case-studies, and examples to comprehend and master UC security

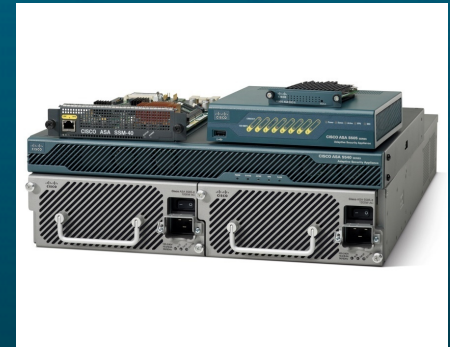
<http://www.ciscopress.com/title/9781587142956>

Further Reading and References

- Securing Cisco IP Telephony Networks

<http://www.ciscopress.com/title/9781587142956>

<http://www.amazon.com/dp/1587142953>



- CUCM Security Guide

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/9_1_1/secugd/CUCM_BK_C0395F44_00_cucm-security-guide-91.html

- CSC Articles <https://supportforums.cisco.com/docs/DOC-29832>

<https://supportforums.cisco.com/docs/DOC-38492>

Submit Your Questions Now!

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



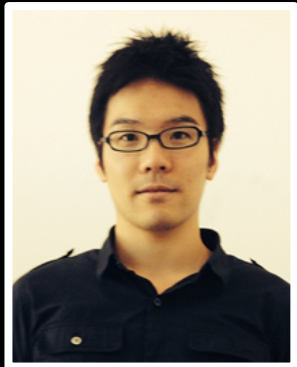
Trivia Question

How is Cisco's UCM fighting crime?

- A.** The Kuala Lumpur, Malaysia police department adopted the Cisco unified videoconferencing and unified messaging solution to enhance communications within the city to allow officers to spend more time on the streets and less time managing communications in the office.
- B.** Interpol adopted a Cisco unified videoconferencing and unified messaging solution which provided communications and database assistance in order to fight international crime.
- C.** North Wales Police adopted a unified videoconference and unified messaging solution on smartphones so that officers can spend less time traveling and more time in the community.

January Expert Series Webcast - Japanese

Topic: Virtual Port Channel (vPC)



Tuesday, January 14, 2014

10:00AM JST Tokyo

5:00PM PDT San Francisco (Monday, January 13, 2014)

Join Cisco Expert:

Takuya Kishida

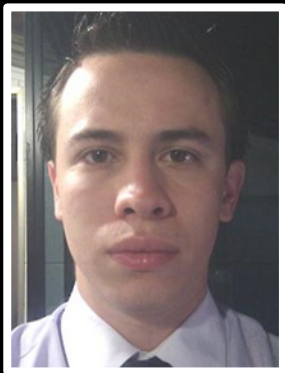
During this live event, the expert Takuya Kishida will focus on the behavior of virtual Port Channel (vPC) which is a typical but major function of Cisco Nexus switches.

Register for this live Webcast at:

[http://tools.cisco.com/gems/cust/customerSite.do?
METHOD=E&LANGUAGE_ID=J&SEMINAR_CODE=S19449&PRIORITY_CODE=](http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=J&SEMINAR_CODE=S19449&PRIORITY_CODE=)

January Expert Series Webcast - Portuguese

Topic: Broadband Network Gateway: Concepts and Configuration



Wednesday, January 15, 2014

11:00AM Brasilia City

1:00PM West Lisbon

5:00AM San Francisco

8:00AM New York

Join Cisco Expert:

Bruno Novais

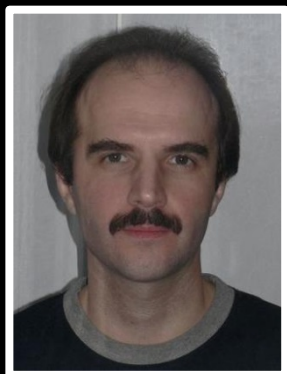
During the live event, Cisco expert Bruno Novais will cover broadband network gateway solution for ASR9K also known as Broadband Remote Access Server (BRAS) or Network Access Server (NAS), which is the solution for aggregator broadband services.

Register for this live Webcast at:

[http://tools.cisco.com/gems/cust/customerSite.do?
METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S19610&PRIORITY_CODE=](http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=P&SEMINAR_CODE=S19610&PRIORITY_CODE=)

January Expert Series Webcast - **Russian**

Topic: Using Packet-Tracer, Capture, and Other Cisco ASA Tools for Network Troubleshooting



Tuesday, January 21, 2014

12:00PM Moscow time

9:00AM Brussels time

Join Cisco Expert:

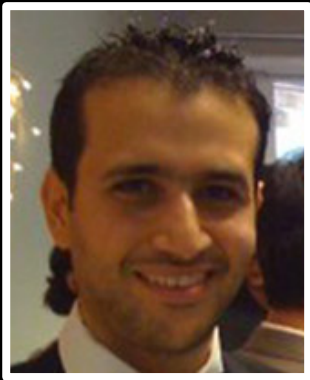
Oleg Tipisov

During the live event, Cisco expert Oleg Tipisov will provide an overview of different Cisco ASA diagnostic tools that would be helpful in troubleshooting of common network, performance, and resource depletion issues.

Register for this live Webcast at:

[http://tools.cisco.com/gems/cust/customerSite.do?
METHOD=E&LANGUAGE_ID=R&SEMINAR_CODE=S19609&PRIORITY_CO
DE=](http://tools.cisco.com/gems/cust/customerSite.do?METHOD=E&LANGUAGE_ID=R&SEMINAR_CODE=S19609&PRIORITY_CODE=)

Ask the Expert Events – Current **English**



Topic: Cisco Catalyst 6800 Series Switches

Join Cisco Expert: **Amer Atout**

Learn and ask questions about Catalyst 6800 Series Switches.

Ends January 17



Topic: Unified Computing System Director

Join Cisco Expert: **Andrew Nam**

Learn and ask questions about Unified Computing System Director

Ends January 17

Join the discussion for these Ask The Expert Events at:

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

Ask the Expert Events – Upcoming English



Topic: Cloud Web Security on ASA

Join Cisco Expert: **Maite Cadenas Sanchez**

Learn and ask questions about Cloud Web Security on ASA.

Starts January 20

Join the discussion for these Ask The Expert Events at:

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

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

<https://supportforums.cisco.com>



<http://www.facebook.com/CiscoSupportCommunity>



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



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



<http://tinyurl.com/cscgoogleplus>



<http://tinyurl.com/cscitunesapp>



<http://tinyurl.com/cscandroidapp>



<http://tinyurl.com/csclinked>



Newsletter Subscription: <http://tinyurl.com/csc-newsletters>

We have communities in other languages

If you speak **Spanish, Portuguese, Japanese 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>
- Russian → <https://supportforums.cisco.com/community/russian>

Join the Cisco Support Community

- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request (*Cisco customers and partners only*)



Documents **Blogs**

Ask the Expert **Video**

Mobile **Discussions**

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

<https://supportforums.cisco.com>

Rate Support Community's Content

Now your ratings on documents videos and blogs count give points to the authors!!!

So, when you contribute and get ratings you now get the points in your profile.

Help us recognize the good quality content in the community and make your searches easier. Rate content in the community.



<https://supportforums.cisco.com/community/netpro/idea-center/cafe/blog/2013/06/07/ratings-extended-to-documents-blogs-and-videos>

Cisco Technical Support Mobile App



Global community members can collaborate with colleagues and other support professionals with easy, on-the-go access to the community's breadth of technical resources in their local language.



With the latest version of the mobile app, you can now access the Spanish, Portuguese, Japanese and Russians communities.

<https://supportforums.cisco.com/community/netpro/online-tools/mobile-technical-support>

Trivia Question

How is Cisco's UCM fighting crime?

A. The Kuala Lumpur, Malaysia police department adopted the Cisco unified videoconferencing and unified messaging solution to enhance communications within the city to allow officers to spend more time on the streets and less time managing communications in the office.

B. Interpol adopted a Cisco unified videoconferencing and unified messaging solution which provided communications and database assistance in order to fight international crime.

C. North Wales Police adopted a unified videoconference and unified messaging solution on smartphones so that officers can spend less time traveling and more time in the community.

Thank You for
Your Time



Please Take a Moment to Complete the Evaluation