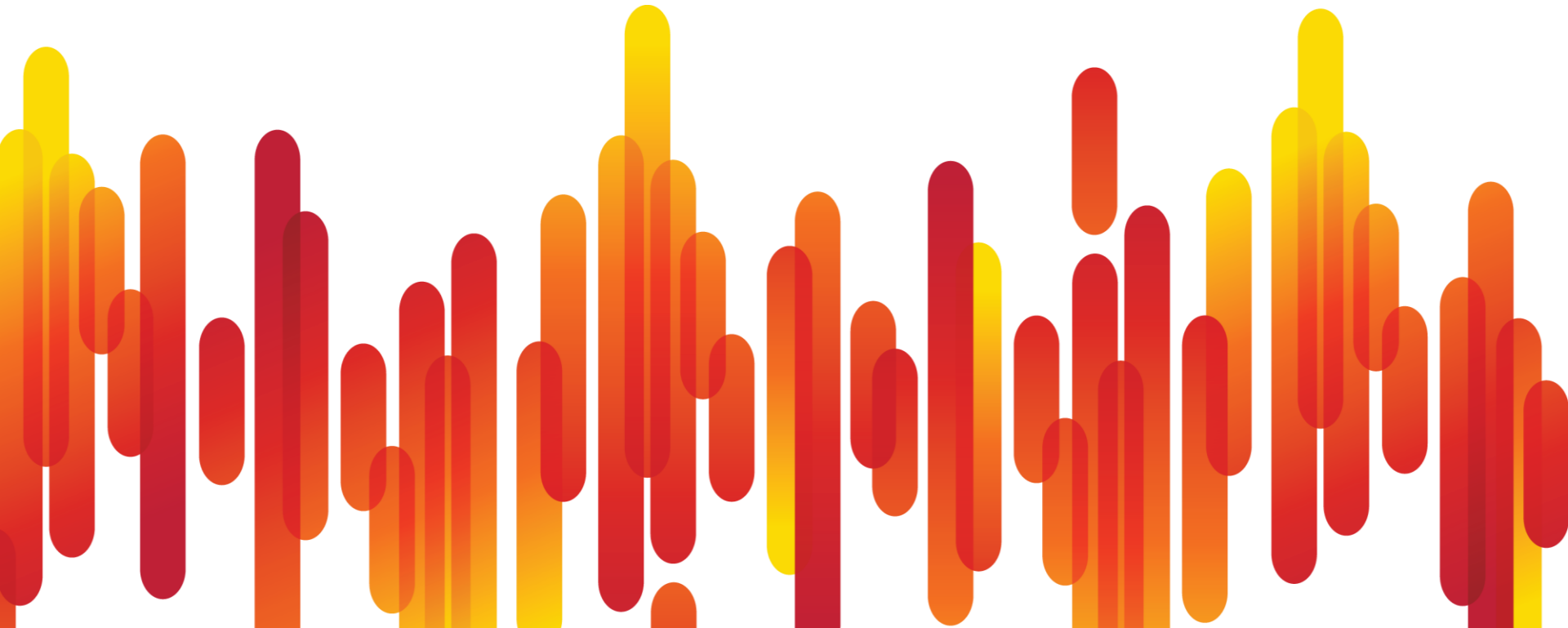




Cisco TelePresence Video Communication Server Update

Arne B. Østensen, Team Lead



Cisco Support Community – Expert Series Webcast

- Today's featured expert is Team Lead Arne B. Østensen
- Ask him questions now about Cisco Video Communications Server (VCS)



Arne B. Østensen

Cisco TelePresence Solution Group

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

<https://supportforums.cisco.com/community/netpro/service-providers>

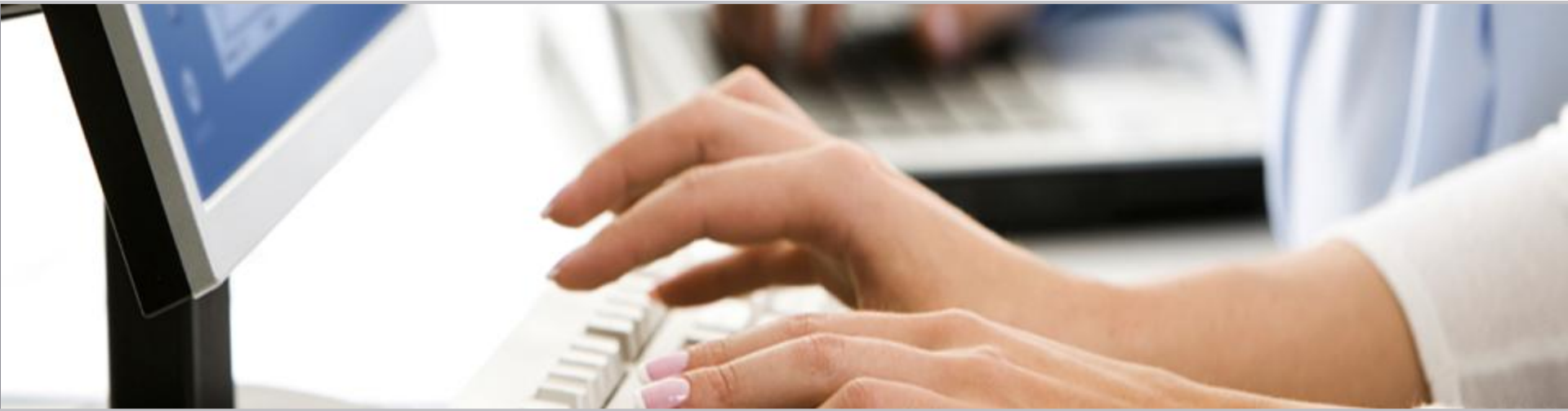
Or, <https://supportforums.cisco.com/docs/DOC-19067>



Polling Question 1

Do you know the Video Communication Server (VCS)?

- a) No, what's this thing?**
- b) Some**
- c) Yes, I have barely tried it**
- d) Yes, I know it**
- e) Yes, I am a guru**



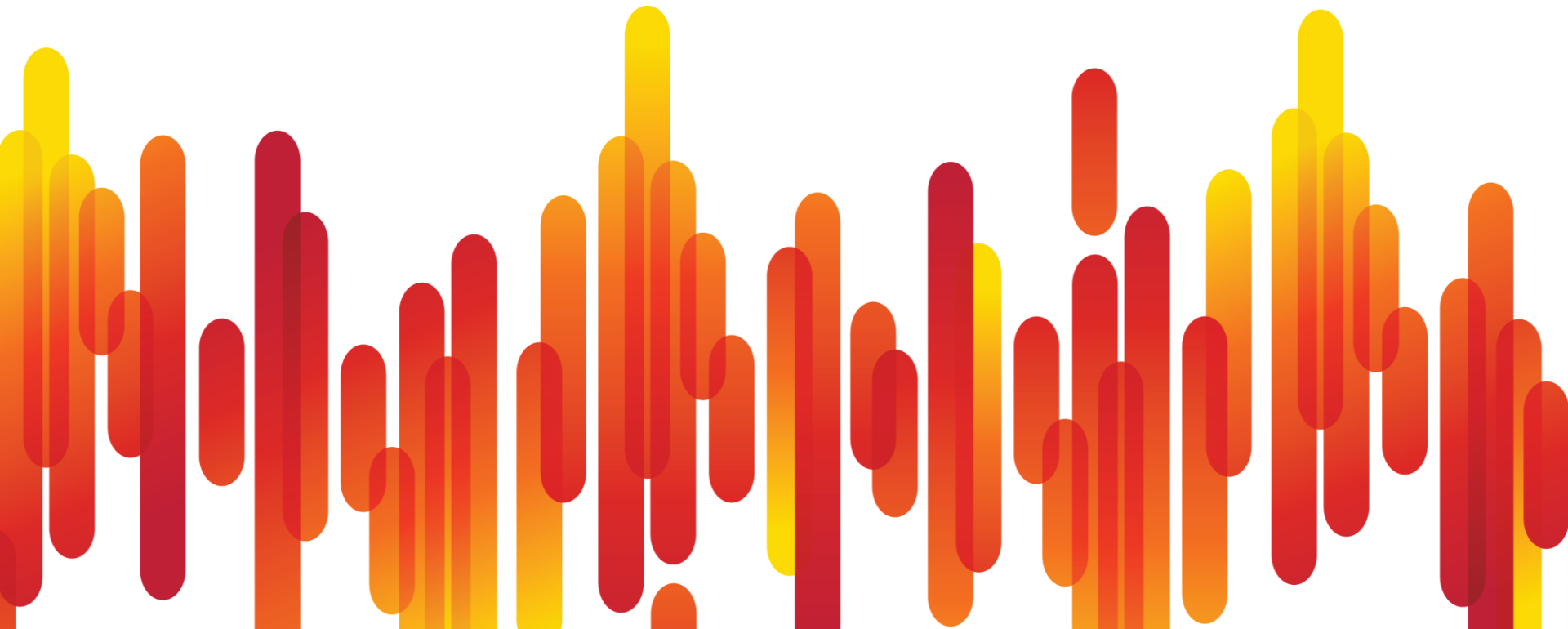
Submit Your Questions Now

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



Cisco TelePresence Video Communication Server Update

Arne B. Østensen, Team Lead



Cisco Video Communication Server

- Standards-based Gatekeeper/Proxy
- Industry leading interoperability including seamless interworking with Microsoft OCS 2007 and other VoIP products
- Flexible with scalability to suit the expanding demands of customers
- B2B communications with standards based Firewall traversal
- Sophisticated Web based configuration and management



X7.0: Enhanced Solution for New and Existing Customers

VCS X7.0 New Features at a Glance



- Greater Flexibility, Efficiency and Resilience
 - Shared call licenses within a Cisco VCS Cluster
- Enhanced Interworking for Home Workers and B2B Users
 - Support for OCS/Lync clients connecting through Microsoft Edge Server
- Simpler Scalability of Deployments
 - Active Directory (AD) integration for Cisco TelePresence Movi
- Sophisticated Call Application Management
 - Ability to access External Policy Servers, applying rules for Call Management, such as Calling party white list, Least cost routing etc.
- Improved Operations Support
 - Advanced Diagnostic tools available on the web

New Features for X7.0



- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

Cluster Call Licensing Management - Shared Cluster Licensing

- Resilience

If Connectivity to a VCS fails, its Licenses can be used by the other VCS peers within a Cluster

- Flexible and Efficient use of Licenses

VCS Licenses are shared within a Cluster - calls can be handled when unbalanced across the cluster peers

Limitation:

- Physical hardware maximum = Max call licenses on one VCS:
 - 500 non-traversal
 - 100 traversal calls
- Licenses of a disconnected peer are available to other peers for up to 2 weeks

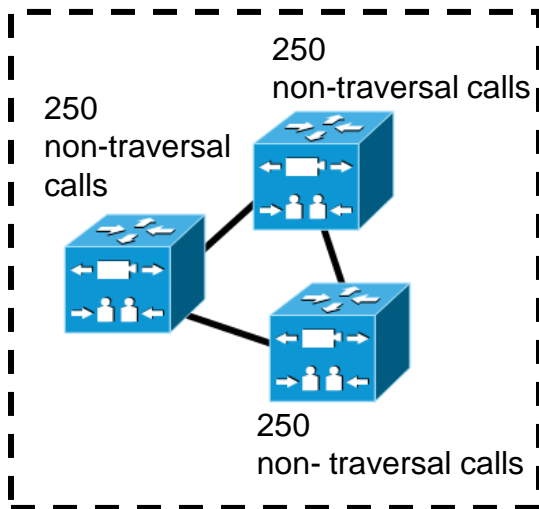
Cluster Call Licensing Management - Shared Cluster Licensing

- VCS is aware of cluster peers and can share call licenses within cluster.

- If VCS connectivity fails, its call licenses are available to peer VCS for 2 weeks

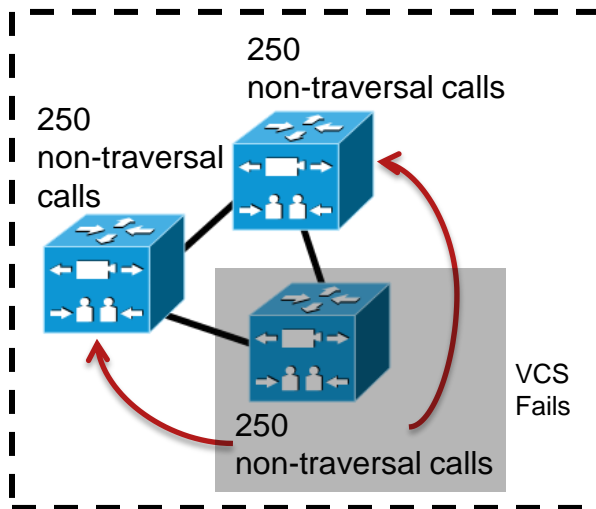
- Limit to maximum total number of call licenses on a VCS is
 - ✓ 500 non-traversal
 - ✓ 100 traversal calls

VCS Cluster



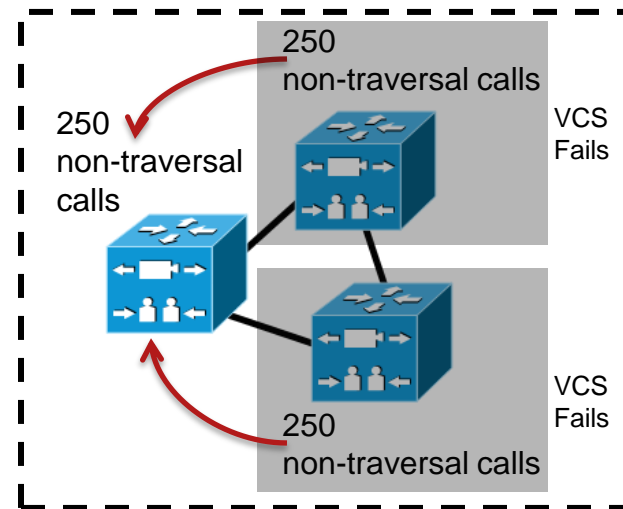
Combined 750 non-traversal calls

VCS Cluster



Combined 750 non-traversal calls

VCS Cluster



Combined 500 non-traversal call license, due to 500 limit per VCS

New Features for X7.0



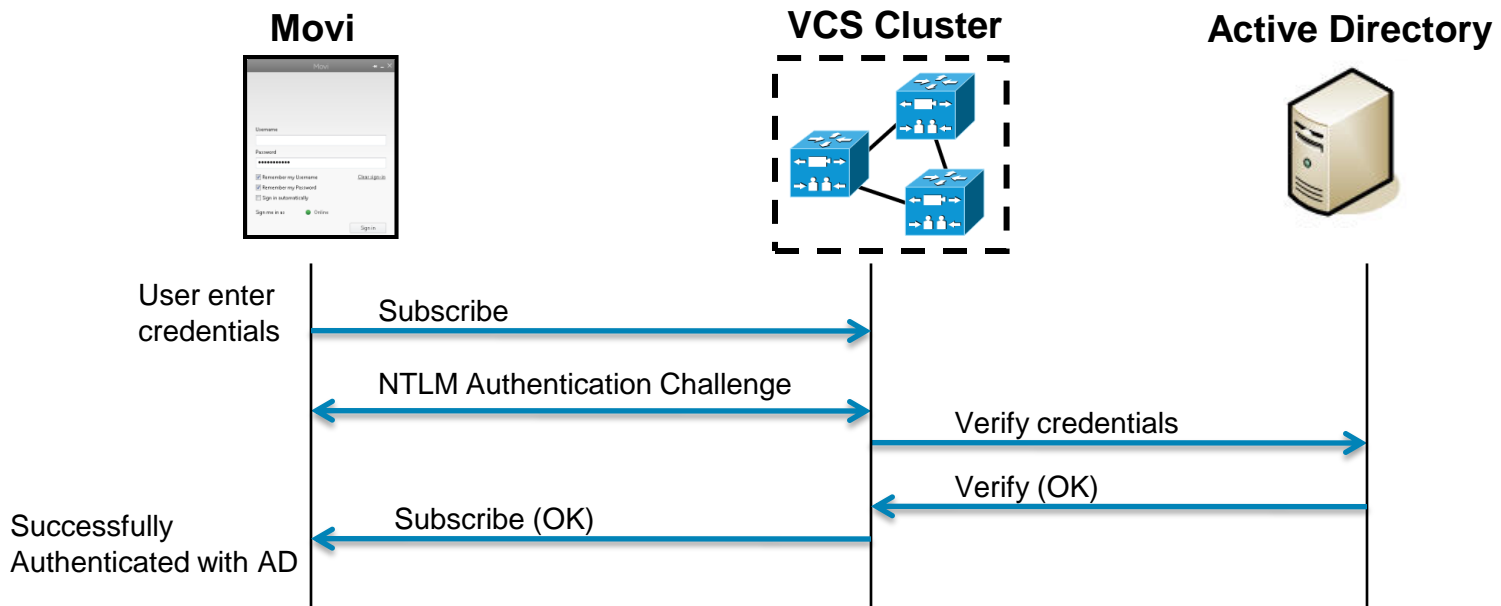
- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

AD/LDAP Device Authentication

- Authentication via Active Directory Service

- VCS Authentication via Active Directory Service
 - ✓ Secure Authentication
 - ✓ Increased User Provisioning Efficiency
 - ✓ No H.350 schema needed on AD server

User Authentication through standard Active Directory lookup



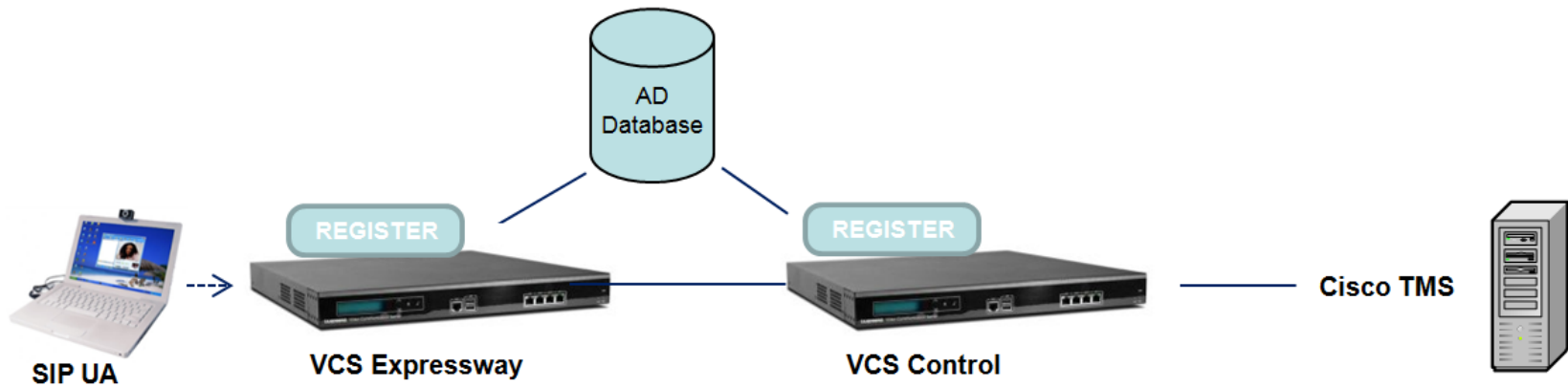
AD/LDAP Device Authentication

- Authentication via Active Directory Service

- Setup
 - Configure AD details on VCS
 - VCS joins the AD domain
 - ✓ Configure with Command Line Interface (CLI) (available in 6.1)
 - ✓ Configure on Web interface (**new in X7.0**)
- SIP signaling
 - VCS challenges Movi (4.2 or later) with NTLM challenge
- VCS using NTLM challenge requires direct connection to AD server
- Other endpoints may be authenticated utilizing H.350 or local database
- *See Authenticating devices deployment guide.*

Device Authentication - Authentication and Provisioning

- VCS Expressway and VCS Control

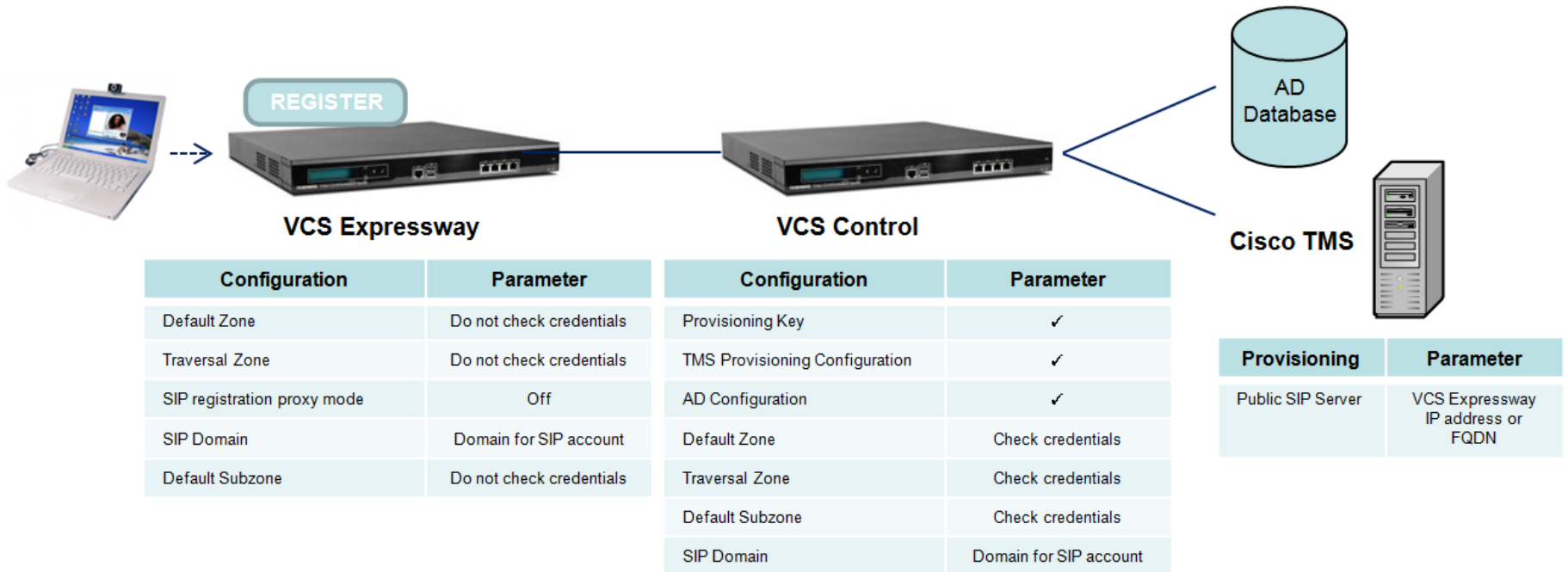


Configuration	Parameter	Configuration	Parameter
AD Configuration	✓	Provisioning Key	✓
Default Zone	Check credentials	TMS Provisioning Configuration	✓
Traversal Zone	Check credentials	AD Configuration	✓
Default Subzone	Check credentials	Default Zone	Check credentials
SIP Domain	Domain for SIP account	Traversal Zone	Check credentials
SIP registration proxy mode	Off	Default Subzone	Check credentials
		SIP Domain	Domain for SIP account

Provisioning	Parameter
Public SIP Server	VCS Expressway IP address or FQDN

Device Authentication - Authentication and Provisioning

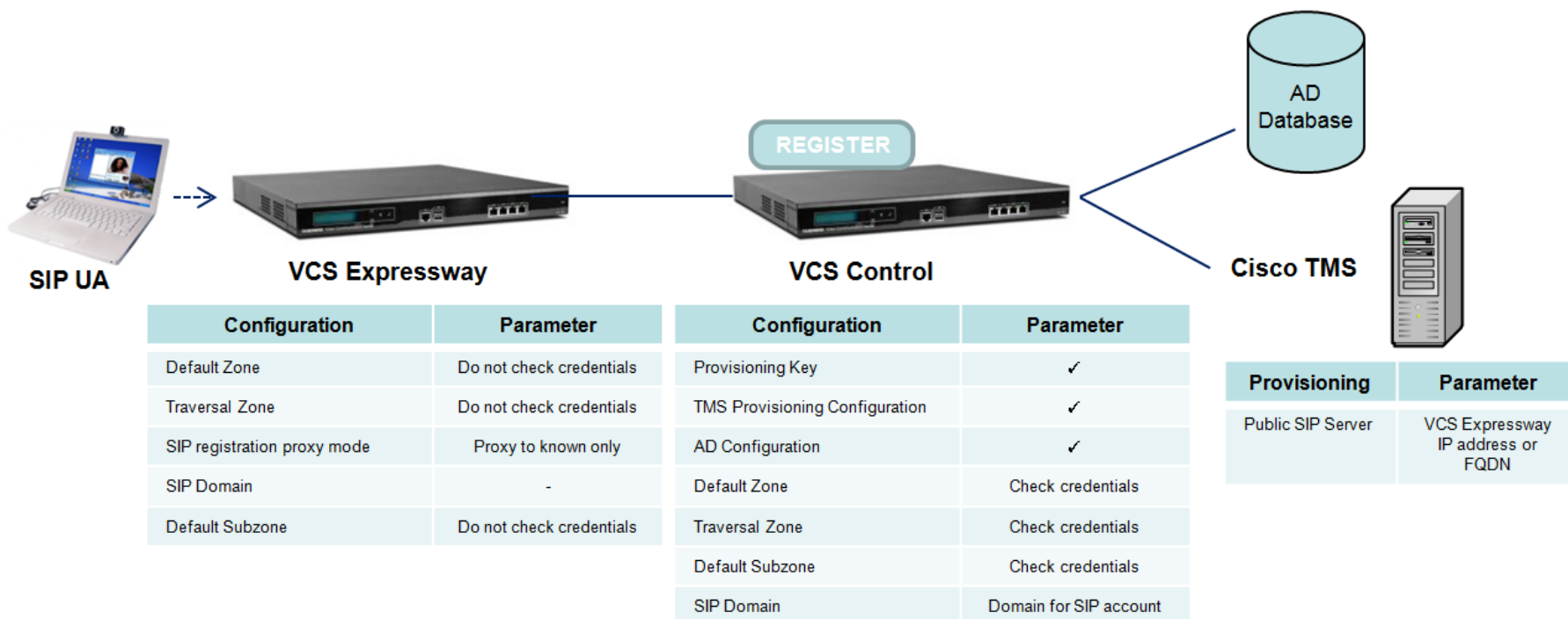
- VCS Expressway and VCS Control – Only Control accesses AD
 - External registrations unauthenticated on Expressway



Device Authentication

- Authentication and Provisioning

- VCS Expressway and VCS Control – Only Control accesses AD
- Proxied registrations



New Features for X7.0



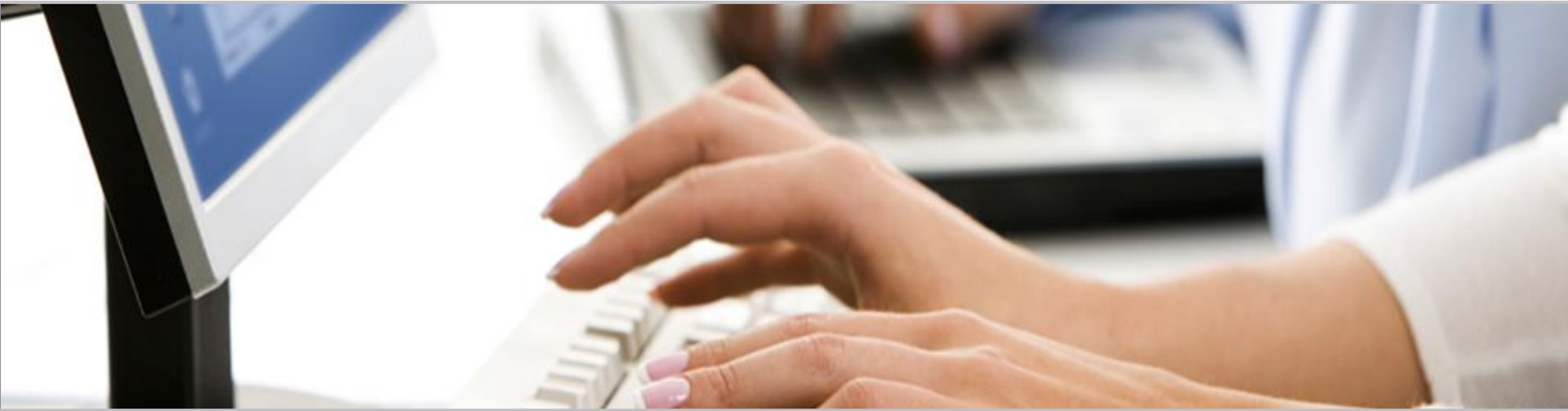
- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

Polling Question 2

What do you prefer to use: Cisco Movi or MS Lync?

- a) Lync is much easier to deploy and manage, and I don't like Movi!**
- b) Lync**
- c) I think both are great**
- d) Movi**
- e) Movi is the easiest to deploy and manage, I will always go with Movi!**





Submit Your Questions Now

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

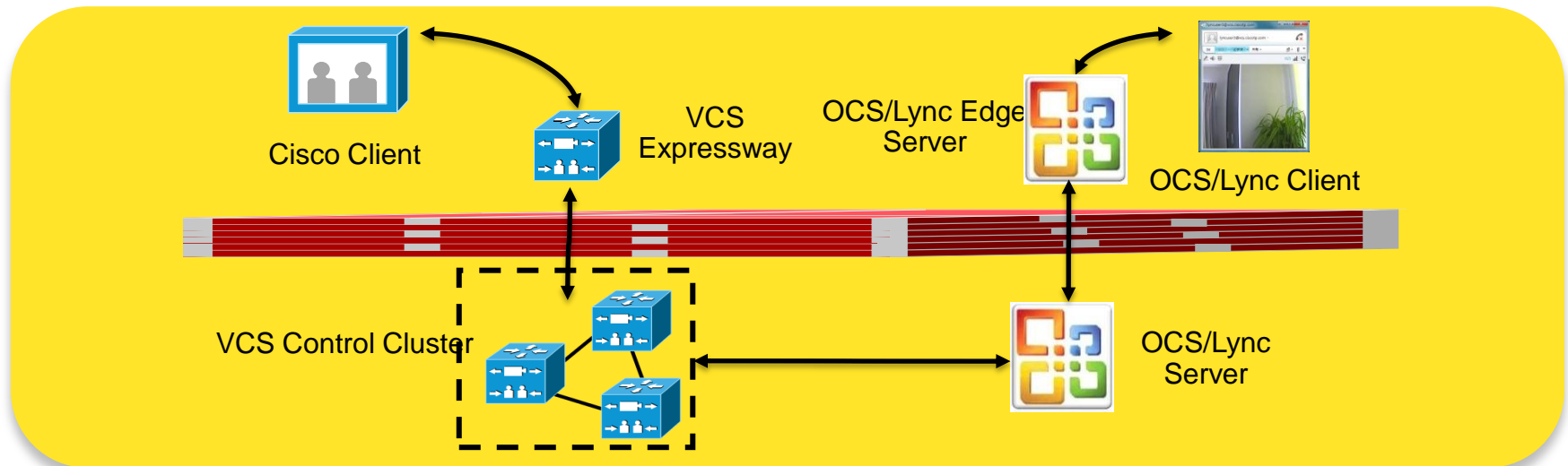
Microsoft OCS/Lync Interworking - B2BUA Service

- Back to Back user agent
 - Recommended configuration
 - Old configuration continues to be supported in X7.x
 - Gives VCS more control
 - Keep standards based and OCS / Lync signalling separate e.g. To support Microsoft Edge Server
 - Media is always taken by B2BUA
 - Presence is supported from VCS to OCS/Lync
 - Registering FindMe users (OCS relay functionality) is supported and strongly recommended

Microsoft OCS/Lync Interworking

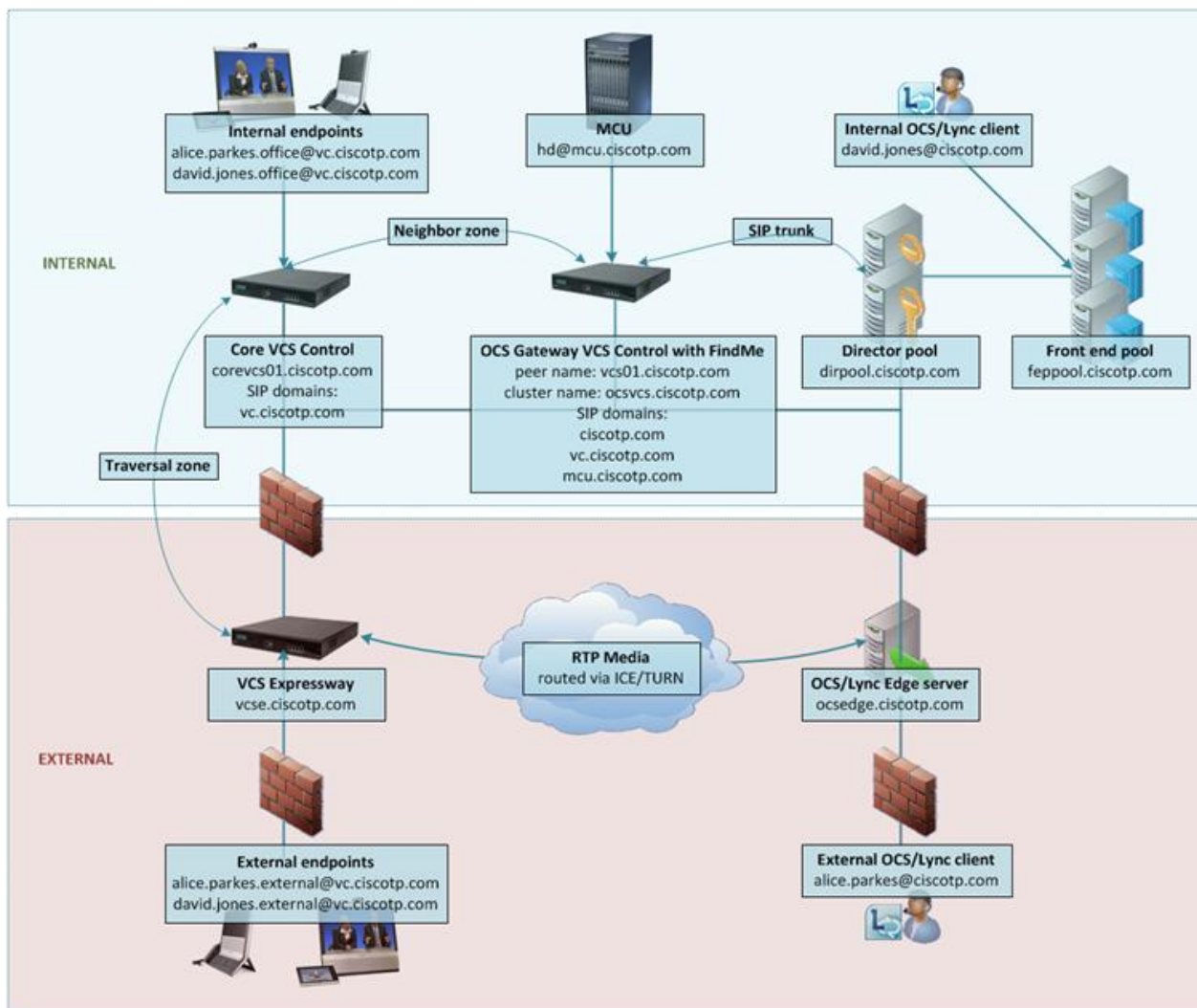
- B2BUA Service

- Additional Capabilities supported with Microsoft OCS/Lync Clients
 - ✓ Support for Call Transfer, Call Hold and Multiway calling with AM GW
 - ✓ Encrypted and unencrypted combinations are supported. One leg of the call could be encrypted while the other leg could be unencrypted
- Expressway enables B2B calling for Cisco endpoints and OCS/Lync clients connected to Microsoft Edge Server
- Supports interoperability with
 - ✓ OCS 2007 R2
 - ✓ Lync 2010



Microsoft OCS/Lync solution

- Example of the total solution scenario with VCS and OCS/Lync integration



Microsoft OCS/Lync Interworking

- B2BUA Service

- Call Licensing Overview

Deployment Scenario		Call licenses used	
Non Encrypted	B2B UA Service (new)	SIP-SIP call without AMGW	2 x non-traversal call license
		H323-SIP interworking call without AMGW	1 x traversal call license 1 x non-traversal license
		SIP-SIP call with AMGW	2 x non traversal call license
		H323-SIP interworking call with AMGW	1 x traversal call license 1 x non-traversal license
	OCS Relay (old)	SIP-SIP call without AMGW	2 x non traversal call license
		H323-SIP interworking call without AMGW	1 x non-traversal license 1 x traversal call license
		SIP-SIP call with AMGW	3 x non-traversal call license
		H323-SIP interworking call with AMGW	1 x traversal call license & 2 x non-traversal call license

Microsoft OCS/Lync Interworking - B2BUA Service

			Call Licenses used
Encrypted	B2B UA Service (new)	SIP-SIP call without AMGW	2 x non-traversal call license
		H323-SIP interworking call without AMGW	1 x traversal call license 1 x non-traversal call license
		SIP-SIP call with AMGW	Needs AM GW 1.1 2 x non-traversal call licenses
		H323-SIP interworking call with AMGW	Needs AM GW 1.1 1 x traversal call license 1 x non-traversal call license
	OCS Relay (old)	SIP-SIP call without AMGW	1 x non-traversal call license 1 x traversal call license
		H323-SIP interworking call without AMGW	1 x non-traversal call license 1 x traversal call license
		SIP-SIP call with AMGW	Needs AM GW 1.1 2 x non-traversal call license 1 x traversal call license
		H323-SIP interworking call with AMGW	Needs AM GW 1.1 1 x non-traversal call license 2 x traversal call license

New Features for X7.0

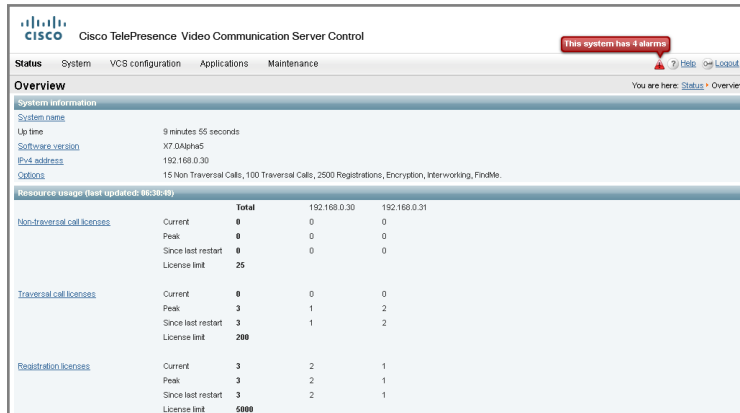


- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

Enhanced Diagnostics

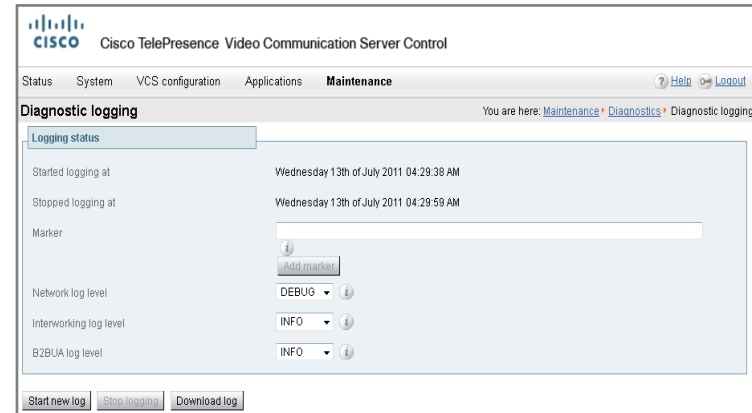
- Improved Diagnostic Capabilities

- Reduced Operational Resources required to support Fault Finding and Management
- Reduction in Equipment Down-time and associated Costs
 - ✓ Diagnostic Logging: Generate and download log of system activity
 - ✓ Network utilities: Ping/Traceroute/DNS lookup
 - ✓ Alarms: Cluster view of all alarms, new alarm icons



The screenshot shows the 'Overview' page of the Cisco TelePresence Video Communication Server Control interface. At the top right, a red banner indicates 'This system has 4 alarms'. The page is divided into several sections: 'System information' (Up time: 9 minutes 55 seconds, Software version: X7.0A(ah)2, IP address: 192.168.0.30, Options: 15 Non Traversal Calls, 100 Traversal Calls, 2500 Registrations, Encryption, Interworking, FinMe), 'Resource usage (last updated: 06:30:09)', 'Non-traversal call licenses', 'Traversal call licenses', and 'Registration licenses'. A table summarizes the resource usage for each category.

Resource usage (last updated: 06:30:09)	Total	192.168.0.30	192.168.0.31
Non-traversal call licenses			
Current	0	0	0
Peak	0	0	0
Since last restart	0	0	0
License limit	25		
Traversal call licenses			
Current	0	0	0
Peak	3	1	2
Since last restart	3	1	2
License limit	200		
Registration licenses			
Current	3	2	1
Peak	3	2	1
Since last restart	3	2	1
License limit	5000		



The screenshot shows the 'Diagnostic logging' page of the Cisco TelePresence Video Communication Server Control interface. The page is titled 'Diagnostic logging' and shows the logging status. It includes a 'Logging status' section with the following information: Started logging at Wednesday 13th of July 2011 04:28:38 AM, Stopped logging at Wednesday 13th of July 2011 04:29:59 AM, and a 'Marker' field with an 'Add marker' button. Below this, there are dropdown menus for 'Network log level' (set to DEBUG), 'Interworking log level' (set to INFO), and 'B2BUA log level' (set to INFO). At the bottom, there are buttons for 'Start new log', 'Stop logging', and 'Download log'.

Enhanced Diagnostics

- Alarm feature improvement

- Warnings are now referred to as Alarms.
- The Alarms page indicates
 - when an alarm was last raised
 - and the number of times it has occurred since the last restart.

Cisco Cisco TelePresence Video Communication Server Control

Status System VCS configuration Applications Maintenance This system has 4 alarms ? Help Logout

Alarms You are here: Status **Alarms**

Alarm	Description	State	Severity	Peer	Action	Time raised	Count	ID
<input type="checkbox"/> Application failed	An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash	Raised	Error	This system	View the incident reporting page	2011-07-06 09:44:05	1	15010
Application failed	An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash	Raised	Error	192.168.0.31	Connect to the remote peer to investigate this alarm.	2011-07-06 09:41:04	3	15010
Application failed	An unexpected software error was detected in app[1110]: SIGSEGV (address not mapped to object) @0x0000000c01f55488	Raised	Error	192.168.0.31	Connect to the remote peer to investigate this alarm.	2011-07-06 15:43:53	50	15011
<input type="checkbox"/> Application failed	An unexpected software error was detected in app[3490]: SIGSEGV (address not mapped to object) @0x0000000c00000001	Raised	Error	This system	View the incident reporting page	2011-07-06 16:03:35	60	15011

Acknowledge Select all Unselect all

Enhanced Diagnostics - Alarm feature improvement

- Automatically filter and display event log by Alarms ID from Alarms page and easily trace how often and when the alarms have occurred.

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. The top navigation bar includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. A red notification bubble indicates 'This system has 4 alarms'. The 'Alarms' section displays a table with columns: Alarm, Description, State, Severity, Peer, Action, Time raised, Count, and ID. The table lists four 'Application failed' alarms, all with ID '15010'. A blue arrow points from the ID '15010' in the table to the filter field in the 'Event Log' section below. The 'Event Log' section has a 'Filter' field containing 'Id="15010"'. Below the filter are 'Filter' and 'Reset' buttons. The 'Results' section shows a list of event log entries, with the entry for ID '15010' highlighted in red.

Alarm	Description	State	Severity	Peer	Action	Time raised	Count	ID
Application failed	An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash	Raised	Error	This system	View the incident reporting page	2011-07-06 09:44:05	1	15010
Application failed	An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash	Raised	Error	192.168.0.31	Connect to the remote peer to investigate this alarm.	2011-07-06 09:41:04	3	15010
Application failed	An unexpected software error was detected in app[28850]: SIGBUS (Sent by the kernel) @0x0000000000000000	Raised	Error	192.168.0.31	Connect to the remote peer to	2011-07-06	47	15011
Application failed	An unexpected software error was detected in app[28850]: SIGBUS (Sent by the kernel) @0x0000000000000000	Raised	Error	192.168.0.31	Connect to the remote peer to	2011-07-06	47	15011

Event Log Filter: Id="15010"

Results:

- Jul 6 09:44:05 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"
- Jul 6 08:35:49 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"
- Jul 5 17:14:25 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"
- Jul 5 12:33:54 **crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in app[28850]: SIGBUS (Sent by the kernel) @0x0000000000000000"**
- Jul 5 12:02:13 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"
- Jul 5 12:02:13 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"
- Jul 5 09:57:55 crashreporter: Level="INFO" Event="Alarm Raised" Id="15010" UUID="9cd08a04-af8c-11df-8045-6361fdf14697" Severity="error" Detail="Application failed: An unexpected software error was detected in clusterconfigurationsynchroniser.py: An unexpected exception occurred during Cluster Configuration Synchronisation causing the configuration synchroniser process to crash"

Enhanced Diagnostics

- System snapshot

- Multiple levels of System snapshot

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. At the top, there is a navigation menu with 'Maintenance' selected. Below the menu, the 'System snapshot' section is displayed. It includes a breadcrumb trail: 'You are here: Maintenance > Diagnostics > System snapshot'. The 'System information' section shows 'Software version: X7.0' and 'Hardware serial number: 0DABF861'. A 'System snapshot' section contains a warning: 'WARNING: The system snapshot process may take several minutes to complete. You may experience a drop in system performance during this time.' At the bottom, there are three buttons: 'Create status snapshot', 'Create logs snapshot', and 'Create full snapshot'.

System Snapshot	Signaling Route
Status snapshot	contains the system's current configuration and status settings.
Logs snapshot	contains log file information (including the Event Log, Configuration Log and Network Log).
Full snapshot	contains a complete download of all system information. The preparation of this snapshot file may take several minutes to complete and may lead to a drop in system performance while the snapshot is in progress.

Enhanced Diagnostics

- Diagnostic Logging Feature

- The “netlog” command on CLI replaced by Diagnostic Logging mechanism on Web GUI

Maintenance > Diagnostics > Diagnostic logging

The screenshot displays the Cisco TelePresence Video Communication Server Control interface. At the top left is the Cisco logo. The main title is "Cisco TelePresence Video Communication Server Control". Below this is a navigation bar with tabs for "Status", "System", "VCS configuration", "Applications", and "Maintenance" (which is selected). On the right of the navigation bar are links for "Help" and "Logout".

The main content area is titled "Diagnostic logging" and includes a breadcrumb trail: "You are here: Maintenance > Diagnostics > Diagnostic logging". A sub-tab "Logging status" is active. The configuration area includes:

- "Started logging at": Wednesday 13th of July 2011 04:29:38 AM
- "Stopped logging at": Wednesday 13th of July 2011 04:29:59 AM
- "Marker": An empty text input field with an "Add marker" button below it.
- "Network log level": A dropdown menu set to "DEBUG" with an information icon.
- "Interworking log level": A dropdown menu set to "INFO" with an information icon.
- "B2BUA log level": A dropdown menu set to "INFO" with an information icon.

At the bottom of the configuration area are three buttons: "Start new log", "Stop logging", and "Download log".

Enhanced Diagnostics

- Diagnostic Logging Feature

- How to retrieve the system log?

Configure log level

Log Level	Description
INFO	
ERROR	
WARN	
INFO	Equivalent to “netlog 1”
DEBUG	Equivalent to “netlog 2”
TRACE	Equivalent to “netlog 3”

Click  to start logging

Add “Event=“Diagnostic Logging” Detail=“Logging started; DEBUG_MARKER:” as indication in log with timestamp in log file

Click  to add marking on log as needed

Add “Event=“Diagnostic Logging” Detail=“Added marker; DEBUG_MARKER” as indication in log with timestamp in log file in default, otherwise marker keyword will add (as added in “Marker” field).

Click  to stop logging

Click  to retrieve log file (in text format) from VCS to local PC

Enhanced Diagnostics

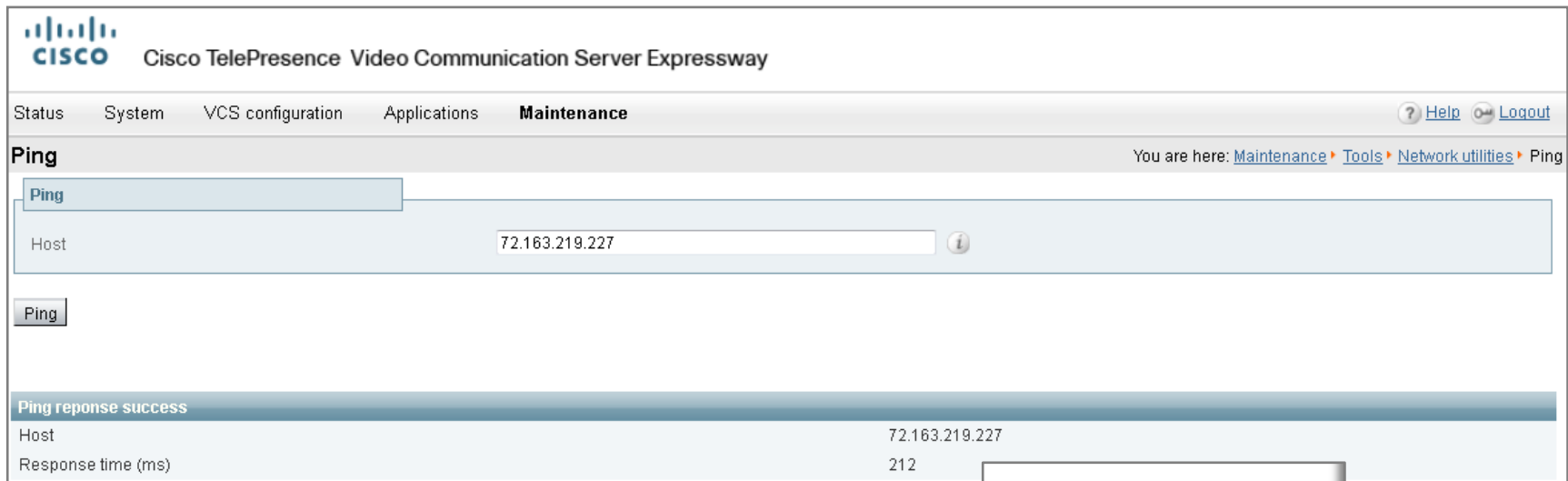
- Diagnostic Logging Feature

- Which logs to retrieve?

Scenario	Logging Level
H323 or SIP call	Network log level = Debug
H323/SIP Interworking call	Network log level = Debug Interworking log level = Debug
Lync integration using B2BUA	Network log level = Debug B2BUA log level = Debug

Enhanced Diagnostics - Network Tool - Ping

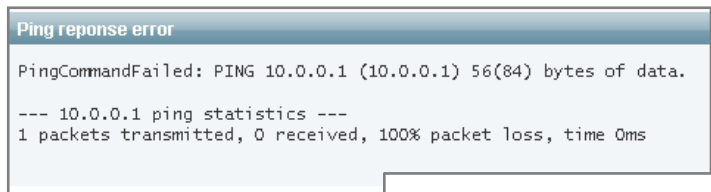
- Ping network test feature now supported from Web GUI
Maintenance > Tools > Network utilities > Ping



The screenshot shows the Cisco TelePresence Web GUI interface. At the top, there is a navigation menu with 'Maintenance' selected. Below the menu, the 'Ping' tool is active, showing a host IP address of 72.163.219.227. The results section, titled 'Ping reponse success', displays the following data:

Host	Response time (ms)
72.163.219.227	212

Success Result



The screenshot shows the 'Ping reponse error' section of the Web GUI. It displays the following error message:

```
PingCommandFailed: PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.  
--- 10.0.0.1 ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Failed Result

Enhanced Diagnostics - Network Tool - Traceroute

- Traceroute network test feature now supported from Web GUI
Maintenance > Tools > Network utilities > Traceroute

The screenshot displays the Cisco TelePresence Web GUI. At the top, the Cisco logo and the text "Cisco TelePresence Video Communication Server Expressway" are visible. Below this, a navigation bar includes "Status", "System", "VCS configuration", "Applications", and "Maintenance" (which is highlighted). On the right side of the navigation bar, there are links for "Help" and "Logout".

The main content area is titled "Traceroute" and includes a breadcrumb trail: "You are here: Maintenance > Tools > Network utilities > Traceroute". Below the title, there is a "Traceroute" tab and a form with a "Host" label and a text input field containing the IP address "64.233.183.105".

Below the form, there is another "Traceroute" tab and a section titled "Traceroute response success". This section contains a table with the following data:

TTL	Response
1	122.208.146.193 (122.208.146.193) 1.034 ms 1.028 ms 1.028 ms
2	221.112.3.145 (221.112.3.145) 1.992 ms 2.006 ms 2.007 ms
3	221.112.21.53 (221.112.21.53) 2.007 ms 2.009 ms 2.984 ms
4	221.112.16.97 (221.112.16.97) 2.994 ms 3.976 ms 3.987 ms
5	61.122.113.205 (61.122.113.205) 6.968 ms 6.980 ms 6.981 ms
6	61.122.114.53 (61.122.114.53) 4.960 ms 3.897 ms 4.854 ms
7	61.122.123.97 (61.122.123.97) 4.845 ms 10.298 ms 10.286 ms
8	58.159.238.42 (58.159.238.42) 10.280 ms 10.279 ms 11.231 ms
9	209.85.241.90 (209.85.241.90) 11.909 ms 11.914 ms 16.057 ms
10	209.85.255.58 (209.85.255.58) 19.030 ms 209.85.255.36 (209.85.255.36) 19.844 ms 19.805 ms
11	209.85.255.39 (209.85.255.39) 50.780 ms 50.801 ms *
12	* * 209.85.243.21 (209.85.243.21) 46.487 ms
13	72.14.238.218 (72.14.238.218) 50.264 ms 72.14.238.42 (72.14.238.42) 57.225 ms 57.225 ms
14	64.233.183.105 (64.233.183.105) 46.211 ms 45.620 ms 45.603 ms

Enhanced Diagnostics

- Network Tool - DNS lookup

- DNS lookup test feature now supported from Web GUI
Maintenance > Tools > Network utilities > DNS lookup
- Supports A, AAAA, SRV and NAPTR record lookup
– also reverse IP to name lookup
 - Looks up hosts table and does DNS lookup – may get hostname or FQDN returned

The screenshot shows the Cisco TelePresence Web GUI interface. The breadcrumb navigation is: Maintenance > Tools > Network utilities > DNS lookup. The 'DNS lookup' form has 'Host' set to 'tandberg.com' and 'Query type' set to 'All'. A 'Lookup' button is visible. Below the form is a table with the following data:

Query type	Name	TTL	Class	Type	Response
A	tandberg.com.	242	IN	A	69.20.64.85

The screenshot shows the Cisco TelePresence Web GUI interface. The breadcrumb navigation is: Maintenance > Tools > Network utilities > DNS lookup. The 'DNS lookup' form has 'Host' set to '_h323ls._udp.ciscotp.com' and 'Query type' set to 'SRV (SIP and H323 servers)'. A 'Lookup' button is visible. Below the form is a table with the following data:

Query type	Name	TTL	Class	Type	Response
SRV	_h323ls._udp.ciscotp.com.	14375	IN	SRV	0 0 1719 pstbc1.ciscotp.com.
SRV	_h323ls._udp.ciscotp.com.	14375	IN	SRV	10 0 1719 pstbc2.ciscotp.com.

New Features for X7.0



- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

System Feature Enhancement

- Call Routing Mode Configuration

- Neighbor Zones can now be customized to augment the VCS-wide Call Routing mode such that, if desired, the Cisco VCS can remain call-routed when routing toward a neighbor.
 - TLS certificates
 - Authentication limits

The screenshot shows the 'Advanced' configuration page for a VCS. The 'Call signaling routed mode' is highlighted with a red box and is set to 'Auto'. Other settings include 'Zone profile' set to 'Custom', 'Monitor peer status' set to 'Yes', and 'SIP SDP attribute line limit length' set to 130.

Mode	Signaling Route
Auto	Signaling will be taken as determined by the Call Routed Mode configuration.
Always	Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration.

Default Configuration: Auto

Example Scenario:

CUCM connected using TLS to VCS ... if it steps out of the path, CUCM has to accept certificates from all other VCSs in the deployment, pinch point for authentication trust.

System Feature Enhancement

- TMS Agent Database Credentials

- TMS Agent database credentials included within local authentication database lookups
- In addition to any manually created entries, the Cisco VCS now checks credentials stored within the TMS Agent database when the device authentication database type is set to Local database.
 - This makes it easier to enable authentication on the Cisco VCS when provisioning process was using passwords originating from TMS.

New Features for X7.0



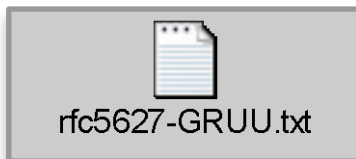
- Cluster Call License Management
- AD/LDAP Device Authentication
- Microsoft OCS/Lync Interworking (B2BUA Service)
- Policy Server
- Enhanced Diagnostics
- System Feature Enhancement
- New Feature Implementation

New Feature Implementation

- Globally Routable User-Agent URIs

- Now supporting the Public GRUU element of RFC 5627:
Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)
- The GRUU is a SIP URI that can be used anywhere on the internet to route a request to a specific AOR instance.
- Used by SIP devices for their 'contact:' header
 - Instead of typical `name@local_IP_address_of_device:port`

Note: The registration local domain must be globally routable as VCS uses this as the GRUU domain.



New Feature Implementation

- PLPMTUD Support

- Now supporting the PLPMTUD - Packetization Layer Path MTU Discovery - element of RFC 4821:
To dynamically discover the MTU of a path by probing with progressively larger packets.
- This feature is supported with CLI command only
xConfiguration IP RFC4821 Mode: <Auto/Enabled/Disabled>

Mode	Signaling Route
Enabled	Packetisation layer MTU probing always performed..
Auto	Disabled by default, enabled when an ICMP black hole detected.
Disabled	Packetisation layer MTU probing is not performed.



rfc4821-Packetization Layer Path MTU Discovery.txt

Summary VCS X7.0



Enhanced solution for new and existing customers

- Greater Flexibility, Efficiency and Resilience
 - Shared call licenses within a Cisco VCS Cluster
- Enhanced Interworking for Home Workers and B2B Users
 - Support for OCS/Lync clients connecting through Microsoft Edge Server
- Simpler Scalability of Deployments
 - Active Directory (AD) integration for Cisco TelePresence Movi
- Sophisticated Call Application Management
 - Ability to access external Policy Servers, applying rules for Call Management, such as Subscriber white list, Least cost routing
- Improved Operations Support
 - Advanced Diagnostic tools available on the web

Polling Question 3

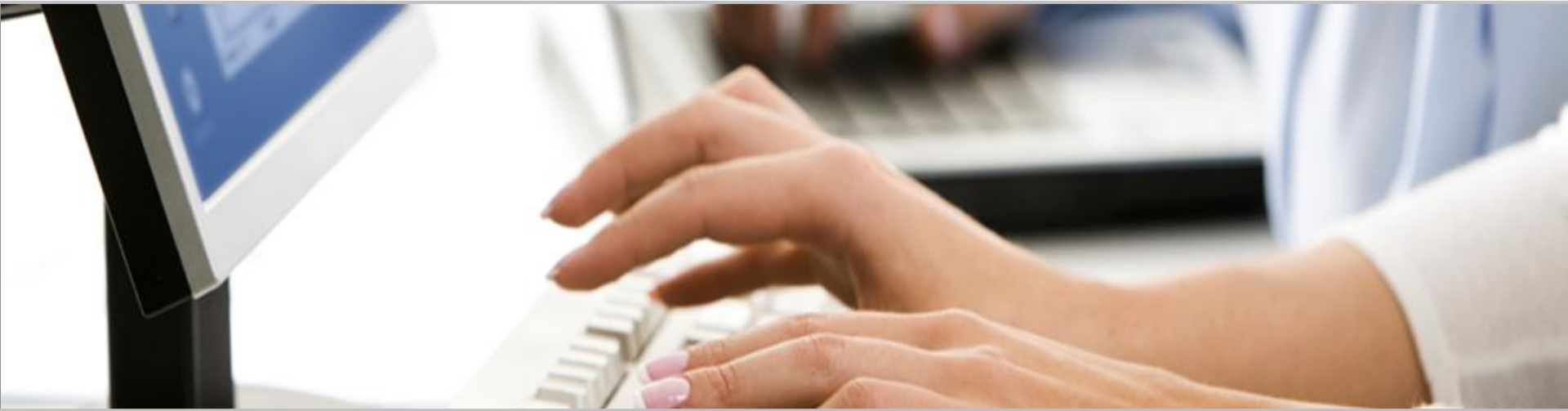
Do you still think the Video Communication Server is the best Video Gatekeeper there is?

- a) No, it's too expensive, I still prefer Open Source**
- b) No, I'll stick with my old Gatekeeper**
- c) I might consider one**
- d) Yes**
- e) Of course! I wouldn't trade it for the World!**

References



- X7.0.1 Software Release Notes:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/release_note/Cisco_VCS_Release_Note_X7-0-1.pdf
- Authenticating devices Deployment Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Authenticating_Devices_Deployment_Guide_X7-0.pdf
- Lync Integration Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/solutions/Cisco_TelePresence_Integration_with_Microsoft_Lync_Server_Solution_Guide.pdf
- Troubleshooting Guide:
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/troubleshooting/Cisco_VCS_Troubleshooting_Procedures.pdf
- More Guides:
http://www.cisco.com/en/US/partner/products/ps11337/tsd_products_support_series_home.html



Submit Your Questions Now

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



Q&A

We Appreciate Your Feedback!

The first 5 listeners
who fill out the Evaluation Survey
will receive a free:

\$20 USD Gift Certificate

To complete the evaluation, please click on link
provided in the chat.

Ask The Experts Event (with Expert)

If you have additional questions, you can ask them to Expert He will be answering from 10/18/2011 to 10/28/2011.

<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 CSC Expert Series Webcast

Topic: Wide Area Application Server (WAAS)

Tuesday, November 15th, at
2:00 p.m. Pacific Time
5:00 p.m. East Time

Join Technical Support Engineer
Bhavin Yadav from **San Jose**.

He will talk about WAAS products and provide tips for configuring and troubleshooting them.

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

Register for this live Webcast at

www.CiscoLive.com/ATE

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>

We have communities in other languages?

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

- **Spanish** → <https://supportforums.cisco.com/community/spanish>
- **Polish** → <https://supportforums.cisco.com/community/etc/netpro-polska>
- **Japanese** → <https://supportforums.cisco.com/community/csc-japan>

We're also running a pilot for **Russian and Portuguese**. You can register at the following links

- **Russian:**

<https://www.ciscofeedback.vovici.com/se.ashx?s=6A5348A712220E19>

- **Portuguese:**

<https://www.ciscofeedback.vovici.com/se.ashx?s=6A5348A77EE5C0B7>

Thank You for
Your Time

Please Take a Moment to Complete the Evaluation





CISCO