# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>4</td>
</tr>
<tr>
<td>NOT ALL WI-FI NETWORKS CAN MEET THE REQUIREMENTS FOR ENTERPRISE LYNC</td>
<td>4</td>
</tr>
<tr>
<td>SOLUTION COMPONENTS</td>
<td>4</td>
</tr>
<tr>
<td>WHAT'S NEW IN ARUBAOS V6.4</td>
<td>6</td>
</tr>
<tr>
<td>LYNC OVER WI-FI – CONFIGURATION GUIDELINES</td>
<td>6</td>
</tr>
<tr>
<td>RF RECOMMENDATIONS</td>
<td>6</td>
</tr>
<tr>
<td>MOBILITY CONTROLLER SETTINGS</td>
<td>6</td>
</tr>
<tr>
<td>NETWORK PERFORMANCE</td>
<td>6</td>
</tr>
<tr>
<td>SDN API CONFIGURATION</td>
<td>6</td>
</tr>
<tr>
<td>CONFIGURING ARUBA MOBILITY CONTROLLER FOR SDN API INTEROPERABILITY</td>
<td>9</td>
</tr>
</tbody>
</table>
# Table of Contents

- **Common Configuration for ArubaOS v6.3 and v6.4** ........................................... 10
- **Configuration Specific to ArubaOS v6.3** ......................................................... 17
- **Things to Remember in ArubaOS v6.4** ............................................................. 18
- **UCC Dashboard for System and Client Visibility into Lync Calls** ..................... 19
- **Lync Diagnostics and Troubleshooting from CLI** ........................................... 22
- **Diagnostics Commands Common to Both V6.3 and V6.4** ................................. 22
- **Diagnostics Commands Available Only in ArubaOS V6.4** ............................... 23
- **Appendix** ........................................................................................................ 24
- **About Aruba Networks, Inc.** ......................................................................... 25
INTRODUCTION

The adoption of unified communication (UC) applications such as Lync in the enterprise is growing quickly. The combination of mobile UC clients and a UC enabled Wi-Fi solution have enabled companies to improve collaboration, communication and mobility in the enterprise. Mobile devices running UC applications also create an excellent opportunity to rightsize networks and forgo investments in expensive switching infrastructure, backup power refresh and desk phones.

One of the biggest obstacles for mobile UC over Wi-Fi has been the Wi-Fi infrastructure’s limited ability to provide a high quality user experience for UC as well as the lack of visibility into the UC traffic for monitoring and management. With the introduction of Aruba’s integration into Microsoft Lync through the SDN API we can now meet these quality and visibility requirements. This solution is currently available on Aruba Mobility Controllers for Microsoft Lync 2013 and 2010 systems.

This document explains the Lync and Aruba WLAN solution when Lync SDN API is integrated with the Aruba Mobility Controller. The document details the configuration, monitoring and diagnostics features added to the Aruba platform to support the Lync API integration.

This document assumes the existence of a tested Microsoft Lync installation as well as a functioning Aruba wireless LAN system. Prior to configuration of the WLAN solution please confirm the function of all components. This guide references best practice settings, please refer to the ArubaOS user guide as well as the campus design guide for additional detailed configuration steps needed to ensure proper WLAN configuration.

NOT ALL WI-FI NETWORKS CAN MEET THE REQUIREMENTS FOR ENTERPRISE LYNC

Building a WLAN system to handle real time voice and video traffic requires the ability to distinguish real time traffic from other traffic on the system. Once traffic is identified, the system must be able to prioritize and protect that traffic from disruption.

In addition, enterprise systems must have the ability to report and identify problems with real time traffic. As more UC solutions focus on consumer devices the traffic is being encrypted to handle different Wi-Fi situations. This is required as users are just as likely to use UC clients in a coffee shop with an open SSID as well as in an enterprise with an encrypted SSID.

The Lync SDN API provides an interface to the Aruba Mobility Controller to access Lync network diagnostic information about voice, video, desktop-sharing and file-transfer without having to see into the traffic.

Using this API, Microsoft provides Aruba with all the information needed to identify the traffic and allow network managers differentiated control over prioritizing real-time and non-real time Lync traffic. It also gives the administrator a view into the call quality correlated with wireless device and AP health.

SOLUTION COMPONENTS

Lync 2010/2013 front-end server

Clients connect directly to a Lync front-end server in order to make calls and communicate with other users. The front-end server is also the component that talks to the Aruba infrastructure via Lync SDN API and SDN Manager.

Lync QoE server

This system component includes a Microsoft SQL Server database. Clients send call quality reports to the QoE server, and the QoE server stores the information and creates reports for the administrator. The QoE server shares call metrics data with Aruba Mobility Controller via SDN API on Lync Server.

If there is no QoE server on the network, call quality metrics data such as MoS (mean opinion score) etc. will not be reported to Aruba Mobility Controller.

Lync 2010/2013 clients

Lync clients provide a single interface for the user to communicate via instant messaging, voice messaging, calling to outside phones, video conferencing, web conferencing and file sharing. Clients are available for nearly all operating systems, including Windows, Mac OS, Android, iOS, Windows Mobile and BlackBerry.

Lync SDN API 2.0

The Lync SDN API is a software component developed by Microsoft. It can be installed on a Lync 2010 or Lync 2013 server. Lync SDN API provides an interface to the Aruba Mobility Controller to access Lync network diagnostic information about Lync voice and video calls, desktop-sharing and file-transfer.

The Aruba Mobility Controller uses this diagnostics data to prioritize the Lync traffic and to provide visibility into usage of Lync applications on the network. Interface between Lync server and web server is via HTTPS/HTTP (XML) message.
Microsoft had released SDN API 1.2 in later part of 2013. SDN API v1.2 needed to be installed on all Lync Front end servers. Aruba Mobility Controller IP address needed to be configured on all Front End Servers where SDN API v1.2 was installed. In a large network with many Mobility Controllers, replicating the same configuration across all Lync Front End Servers was redundant and cumbersome. SDN API 2.0 addresses this problem.

SDN API 2.0 has two components –
- Lync Dialog Listener (LDL) which is installed on Lync FE server
- Lync SDN Manager (LSM), which is installed on any 2008/2012 Windows Server. Refer to SDN Manager installation guide for additional server specific configuration requirements. LSM can be installed on multiple servers to have redundancy (Primary/Secondary).

Lync Dialog Listener (LDL) captures signaling and diagnostic observations about media traffic between or among Lync endpoints.

Lync SDN Manager (LSM) collects the data from one or more LDLs and sends it to Aruba Mobility Controllers.

The following is SDN API 2.0 architecture and data flow diagram (Source: Microsoft)


SDN API 2.0 is compatible with ArubaOS v6.3 and above. See the configuration section for more details.

**Aruba Mobility Controllers**
Aruba Mobility Controllers provide centralized Wi-Fi and network services to Aruba APs. Mobility Controllers come in different capacities and form factors designed to fit into any size customer network. In order to take advantage of the Lync SDN API integration, your Mobility Controller must be running ArubaOS 6.3.1 or later. Lync SDN API is supported on all Aruba Mobility Controllers.

**Aruba APs**
Aruba Wi-Fi access points come in a variety of different configurations, providing options for various speeds of 802.11ac, 802.11n, and 802.11a/b/g. Any access point that is compatible with your Mobility Controller can be used with the Lync integration.
WHAT’S NEW IN ARUBAOS V6.4
The following are the enhancements in v6.4 –
1. UCC dashboard
2. UI client dashboard page has been enhanced to include real-time call quality analysis

Refer to UCC dashboard section to get more details on this.

LYNC OVER WI-FI – CONFIGURATION GUIDELINES
The following best practices are required for a successful wireless Lync solution. Please refer to the ArubaOS user guide and campus design guide for details on making these settings.

NOTE: Please review Aruba default wmm dscp mapping values in “show wlan ssid-profile <ssid name>” output to verify it matches qos settings on the server and wired infrastructure as appropriate.

RF RECOMMENDATIONS
• 100% coverage in all areas of Lync use
• Capacity-based RF design:
  • Distance between two APs should not exceed more than 50 feet
  • Min and max AP power difference no greater than two steps
  • AP power setting to low to moderate power
• Disable lower data rates
• Set supported beacon rate to higher rate
• Minimum RF signal (RSSI) levels of -65 dBm
• Minimum signal-to-noise ratio (SNR) of 25 dB
• Local probe request threshold to 18
• Cell size reduction to 15 dB for dense deployment with AP-225s, and 10 dB for dense deployments with AP-135s

MOBILITY CONTROLLER SETTINGS
• Broadcast filter ARP – enabled on the virtual AP profile
• Enable fair-access station shaping policy in the traffic management profile
• On the SSID profile
  • Set max-retries to eight
  • Configure QoS Settings (DSCP-WMM mapping) to be the same as the wired network and as per the tagging in the client devices if configured
• In the ARM profile
  • Enable voice/video aware scan
  • ClientMatch – enabled

• In case of 802.1X authentication in the dot1X profile
• Enable Opportunistic Key Caching (OKC)
• Enable validate-pmkid
• Enable EAPOL rate optimization

NETWORK PERFORMANCE
• End-to-end QoS: Make sure the same QoS configured and matched across all the wired switches/routers and in wireless infrastructure end-to-end. Ensure that APs are included in QoS trust to enable upstream markings.
• Round trip delay of less than 100 ms between clients
• Jitter of less than 10 ms
• Packet loss <5%
• QoS trust on all voice ports

SDN API CONFIGURATION
Lync Dialog Listener must be installed and configured on the Lync front-end server. Lync SDN Manager must be installed on a separate Windows 2008/2012 server (not on the Lync front-end server). If there are multiple front-end servers, Lync Dialog Listener should be installed on each and configured to point at the Lync SDN Manager. On Lync SDN Manager, Aruba Mobility Controller information needs to be configured.


NOTE: Read and follow the installation instruction PDF that comes with the SDN API 2.0 to install Lync Dialog Listener and Lync SDN Manager.
Lync Dialog Listener (LDL) configuration

During LDL installation process, the user is prompted to enter “Primary/Secondary SDN Manager URI” and the path used to place log files. Replace “sdnmanager” with SDN Manager IP address in Primary/Secondary SDN Manager URI field as below.

Note: These SDN Manager IP addresses from SDN Manager URI fields are automatically populated into LyncDialogListener.exe.config file.

The LyncDialogListener.exe.config file is located in the Lync SDN API’s installation directory. By default, the path to this directory is C:\Program Files\Microsoft Lync Server\Microsoft Lync SDN API.
Edit the 'LyncDialogListener.exe.config' file to ensure the appsettings keys match those below.

```xml
<appSettings>
    <add key="submituri" value="http://10.68.64.22:9333/LDL/CallInfo"/>
    <add key="alternativeuri" value=""/>
    <add key="hidetripi" value="false"/>
    <add key="sendallcallqoe" value="true"/>
    <add key="sendrawsdp" value="false"/>
    <add key="sendcallinvites" value="false"/>
    <add key="sendmeetingroominfo" value="false"/>
</appSettings>
```

**Lync SDN Manager (LSM) configuration**

During the LSM installation process, the user is prompted to enter “Target Uri” and the path used to place log files. The Mobility Controller IP or FQDN should be entered in the “Submit URI” field. When multiple Mobility Controllers are used, their addresses need to be separated as a space-, comma- (,) or semi-colon-separated string, for example, “http://server1/site1;http://server2/site2”. Note: These Mobility Controller IPs and FQDNs from “Submit Uri” are automatically populated into SDNManager.exe.config file.

Once the API is installed you may edit the configuration file (SDNManager.exe.config) to add any additional new Mobility Controller IP addresses. The SDNManager.exe.config file is located in the Lync SDN API’s installation directory. The wireless Mobility Controller IP address/host name and transport mode (http/https) are configured in this file. By default, the path to this directory is `C:\Program Files\Microsoft Lync Server\Microsoft Lync SDN API`. 

“Lync Dialog Listener” service must be restarted after making any configuration change to this file.
Edit the ‘SDNManager.exe.config’ file to add/edit Mobility Controller IP addresses or URLs as defined below and ensure the appsettings keys match those below.

“Lync SDN Manager” service must be restarted after making any configuration change to this file.  

**NOTE:** Make sure “backwardcompatibility” flag is set to “True” to work with ArubaOS v6.3 and v6.4.

```xml
<appSettings>
  <add key="submituri" value="http://10.68.80.9:15790"/>
  <add key="backwardcompatibility" value="true"/>
  <add key="clientcertificateid" value=""/>
  <add key="submitqueuelen" value="100"/>
  <add key="calltimeout" value="6:00:00"/> <!-- 6 hours -->
  <add key="invitetimeout" value="0:02:00"/> <!-- 2 min -->
  <add key="qoetimeout" value="0:00:05"/> <!-- 5 secs -->
  <add key="endedtimeout" value="0:01:00"/> <!-- 1 min -->
</appSettings>
```

**CONFIGURING ARUBA MOBILITY CONTROLLER FOR SDN API INTEROPERABILITY**

Please note that the following instructions only highlight the SDN API specific Lync ALG configurations. This solution guide does not cover Aruba's heuristics approach for Lync classification. Heuristics based Lync classification does not require any integration with Microsoft. It can provide QoS to Lync Voice/Video traffic, but does not give visibility into Microsoft Lync call quality. Please visit http://support.arubanetworks.com and review the 6.1 or later ArubaOS user guide for information on the heuristics technique, called “Media Classification.”
COMMON CONFIGURATION FOR ARUBAOS V6.3 AND V6.4

A. Configure Aruba Mobility Controller to listen for HTTP (XML) messages from Lync Server SDN API:

I. WebUI Configuration

a. Configure Lync Listening Port: In configuration page, go to Management->General and configure Lync Listening Port:

II. CLI configuration

The following CLI is used to configure the port number on which SDN API will be sending HTTP (XML) messages to Aruba Mobility Controller.

```
#configure terminal
(config) #web-server
(Web Server Configuration) #web-lync-listen-port http 15790
```

In the above example, Aruba Mobility Controller is listening on Port 15790 for HTTP (XML) messages.

b. Configure Aruba Mobility Controller to listen for HTTPS (XML) messages from Lync Server SDN API:

Before configuring the Aruba Mobility Controller to receive Lync SDN API messages using HTTPS, a server certificate must be generated and installed on the Aruba Mobility Controller.

I. Install server certificate

Server certificate must contain the FQDN of the Mobility Controller. The certificate must be signed by a Certificate Authority (CA) and the root certificate must be installed on both the Mobility Controller and the Lync SDN Manager.
Here are the steps below to generate a server certificate for the Mobility Controller and configure the Mobility Controller web server to use HTTPS.

1. In the Mobility Controller web UI, navigate to “Configuration > Management > Certificates” and click on the CSR tab at the top.

2. Fill in the signing request information and click “Generate New” button at the bottom. Make sure that the Common Name (CN) for the CSR corresponds to the FQDN of the Mobility Controller, and Lync SDN Manager is able to resolve the IP of this FQDN.

3. Once the CSR is generated, click on the “View Current” button to view the signing request.
4. Copy the certificate request and generate a server certificate from the certificate authority.
5. Navigate to your certification server.
6. Click the Request a certificate link.
7. Click the Advanced certificate request link.
8. Click the Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file link.
9. In the Saved Request box, paste the certificate request obtained from the Mobility Controller.
10. In the Certificate Template dropdown, choose the web server option.
11. Click the Submit button.

12. Download the server certificate and save it.
13. Also download the root certificate for the CA.
14. Now on the Mobility Controller web UI, navigate to “Configuration > Management > Certificates” and click on the Upload tab at the top.
15. Now enter the certificate name and select the downloaded certificate file and click Upload button.
16. Follow the same steps to upload the root certificate to the Mobility Controller. But choose the certificate type as Trusted CA in upload options.

17. On the Mobility Controller web UI, navigate to “Configuration > Management > General”.

18. Under “Web UI Management Authentication Method” select the server certificate that was uploaded in previous step.

19. Install the root certificate for the CA on the LSM.

II. Web UI configuration

Configure Lync Listening Port: In configuration page, go to Management > General and configure Lync Listening Port:

In the above example, Aruba Mobility Controller is listening on Port 15790 for HTTPS (XML) messages. On the Lync SDN Manager configuration, configure the web service URI as the FQDN of the Mobility Controller. In this example, it is “nebbiolo2.lyncqa.com”. Make sure a record is added for the Mobility Controller host name in the DNS server.

III. CLI Configuration

The following CLI is used to configure the port number on which SDN API will be sending HTTPS (XML) messages to Aruba Mobility Controller.

```
#configure terminal
(config) #web-server
(Web Server Configuration) #web-lync-listen-port https 15790
```
c. Configure Aruba Mobility Controller to enable real-time configuration

This configuration is used to enable UCC monitoring. By default in ArubaOS v6.4 Voice real-time configuration is disabled. Follow the steps below to enable it.

I. Web UI configuration of traffic control profile
   a. Configure traffic control prioritization profile: In configuration page, go to All Profiles->Other profiles->Configure Real-time Analysis

II. CLI configuration

```
# configure terminal
(config) #voice real-time-config
(Configure Real-Time Analysis) #config-enable
```
d. Configure Lync traffic prioritization profile and apply it to a user role

I. Web UI configuration of traffic control profile
   a. Configure traffic control prioritization profile: In configuration page, go to All Profiles->Other profiles->Traffic Control Prioritization

Traffic for prioritized call types will flow with the following DSCP values as configured in the SSID profile.

<table>
<thead>
<tr>
<th>Prioritization</th>
<th>WMM/DSCP Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>DSCP mapping for WMM voice AC</td>
</tr>
<tr>
<td>Video</td>
<td>DSCP mapping for WMM video AC</td>
</tr>
<tr>
<td>Desktop-Sharing</td>
<td>DSCP mapping for WMM video AC</td>
</tr>
<tr>
<td>File-Transfer</td>
<td>DSCP mapping for WMM best-effort AC</td>
</tr>
</tbody>
</table>

If prioritization is disabled, the traffic flows with default best-effort priority.

II. CLI configuration of traffic control profile
   The following is a CLI example of configuring the traffic control profile

   app lync traffic-control prioritize-all-lync
   prioritize-voice
   prioritize-video
   prioritize-desktop-sharing
   prioritize-file-transfer

III. UI configuration to assign traffic control profile to a user role
   a. Assign traffic control profile to a user role: In configuration page, Access Control->Edit button on user role->Traffic Control Profile dropdown box – Select the profile you created
IV. CLI assignment of traffic control profile to a user role

   e. Configure Aruba Mobility Controller to read SIP signaling message sent by Lync clients on port 5061

By default in ArubaOS v6.3.1 and Stateful SIPS processing is enabled. If it is disabled in your configuration, refer to the following how to enable it.

```
user-role authenticated
traffic-control-profile prioritize-all-lync
```

I. Web UI configuration

   a. Enable stateful-sips-processing: Go to Configuration->Advanced Services->Stateful Firewall->Global Settings and enable stateful sips processing and then hit “Apply”.

II. CLI configuration

   f. Lync ACL on Aruba Mobility Controller

Ensure Lync signaling traffic is permitted (TCP Port 5061) in Lync ACL. Make sure this ACL is mapped to the user role to allow Lync Signaling Traffic. Lync ACL can be viewed in the Web UI, from the configuration page: Security→Firewall Policies.

```
#configure terminal
(config) #no firewall disable-stateful-sips-processing
```
II. CLI configuration

In this configuration, Lync ACL is assigned to “test” user role.

**CONFIGURATION SPECIFIC TO ARUBAOS V6.3**

g. Remove media-classification CLI from Aruba Mobility Controller:

Heuristics based detection of Lync traffic is incompatible with the API detection method and must be turned off. The classify media option must not be enabled in the svc-sips ACL applied to the user role.

```plaintext
net service svc-sips tcp 5061 alg sips
!
ip access-list session lync-acl
  any any svc-sips permit queue high
!
user-role test
access-list session lync-acl
```

Use below screen captures from web UI and CLI to determine if ‘classify-media’ is configured in an ‘ip access-list session’ that has been associated to user-role.

I. WebUI screen shot
II. CLI command output

Use below CLI to determine if 'classify-media' is configured in an 'ip access-list session' that has been associated to user-role 'test.'

Use below CLI to remove 'classify-media' if it is configured in 'ip access-list session'

**THINGS TO REMEMBER IN ARUBAOS V6.4**

a. Simultaneous enablement of SDN API and Lync heuristics

In 6.4, both Lync SDN API and heuristics-based classification/prioritization can be enabled simultaneously. In the case, where both methods are enabled SDN API-based Lync classification will take priority.

```
#show rights test
Derived Role = 'test'
 Up BW:No Limit  Down BW:No Limit
 L2TP Pool = default-l2tp-pool
 PPTP Pool = default-pptp-pool
 Periodic reauthentication: Disabled
 ACL Number = 62/0
 Max Sessions = 65535
 access-list List

----------------
Position Name      Type     Location
-------- ----    ----   --------
1     test session

test

----------------
Priority Source Destination Service    Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan ClassifyMedia IPv4/6
-------- ------ ----------- -------    ------ --------- --- ------- ----- --- ----- -------
-- ------ ------- ------------- ------
1     any   any     svc-sips   permit              Low                      Yes      4
(→ Yes indicates that 'classify-media' is configured)
```

Expired Policies (due to time constraints) = 0

```

ip access-list session lync-acl
    any any udp 1025-65535 permit
```

b. Dynamic opening of ports for Lync voice/video traffic

Prior to 6.4, UDP ports are needed be explicitly configured to allow Lync voice/video traffic as below:

In 6.4, firewall sessions will be dynamically opened up in datapath for Lync voice and video calls. For this, UDP Port 3478 needs to be permitted in Lync ACL to allow STUN messages. Lync clients initiate STUN connectivity check prior to media transmission. Once STUN connectivity check is succeeded, media transmission happens.

Dynamic opening of ports is not done for Lync desktop-sharing and file-transfer calls. Administrator needs to open up TCP ports used by these applications.
UCC DASHBOARD FOR SYSTEM AND CLIENT VISIBILITY INTO LYNC CALLS

In ArubaOS version 6.4 Aruba released a new dashboard tab that displays system wide and client specific UCC details. To access the panel go to Dashboard->UCC.

From the main UCC dashboard you can view the system wide UCC counters and statistics for call volume, Call quality, call/client health correlation, per device call counters, call roaming statistics, and QoS correction statistics.

Many of these sections have additional information about UCC calls. From the call volume section we can view call distribution by AP, call quality can show trending call quality.
Additional call quality tabs show quality by devices to spot trends in calls by device types and poor calls by AP to show any problem APs.

One of the main benefits of our integration with Lync is our ability to correlate call quality data with client health information. The correlation scatter plot shows all calls and their XY correlation of calls on the Mobility Controller.

In addition to the high level detail about UCC activity on the Mobility Controller we can also view detailed information about each call, including details on the QoS correction made by the Mobility Controller:
One of the most common uses for the UCC dashboard is to assist in the process of responding to a trouble ticket about a bad call. In the UCC dashboard we can search for a user or device and get a bigger picture of all calls to and from that user across all device types.

We can then drill down into each call and get client and call health graph during each call:
With the visibility information on Aruba’s UCC dashboard and the QoS correction Lync and Network administrators can now have the confidence to run Lync over their WLAN.

LYNC DIAGNOSTICS AND TROUBLESHOOTING FROM CLI

The Aruba Mobility Controller provides a Lync debugging framework that enables a network administrator to monitor the health of the Lync infrastructure for wireless clients. In cases where poor quality Lync experience is reported, the infrastructure provides a rich set of tools to isolate the issue.

DIAGNOSTICS COMMANDS COMMON TO BOTH V6.3 AND V6.4

The command line interface has been enhanced with new CLI that are designed specifically for Lync diagnostics.

Show app lync-tracebuf

This command is used to record activities of Lync clients. Max of 256 entries will be recorded in a circular buffer to save memory. Events such as establishing voice, video, desktop-sharing and file transfer will be recorded. Each entry of CLI will display IP, MAC, client name, timestamp, WMM, DSCP, called-party, media-type and AP name. The intent of this CLI to keep track of individual sessions w.r.t. their handling on the Aruba WLAN.

Show app lync client-status

This command provides details about clients that are actively using Lync. An entry is created for clients that have actively participated in voice, video, desktop-sharing or file-sharing sessions. When a particular client is filtered out with options like active-only, bssid, essid, extn, ip and sta, this CLI will produce the result similar to ‘show voice client status [active-only | bssid | essid | extn | ip | sta]’. In addition, wireless events like AP handoff details will be displayed.

Show app lync call-quality

This command gives details about Lync sessions that have been prioritized after receiving session information from Lync server SDN API. This includes detailed description about call quality statistics for Lync calls.
Show app lync call-cdrs
This command provides the call detail records for Lync voice, video, desktop-sharing and file transfer call. It also displays call quality metrics such as MOS that is received from Lync Server.

DIAGNOSTICS COMMANDS AVAILABLE ONLY IN ARUBAOS V6.4
ArubaOS v6.4 introduces Unified Communication and Collaboration Feature. It provides real-time call quality analysis and additional set of UCC sub features. ArubaOS v6.4 introduces the following CLI commands –

- show ucc call-info cdrs
- show ucc client-info
- show ucc configuration
- show ucc statistics
- show ucc trace-buffer

Details about the above commands and CLI output is described as part of ArubaOS v6.4 CLI reference guide.

Enabling Lync ALG debug logging
Lync ALG debug logs provide granular visibility into the messages exchanged between Lync Server and the Mobility Controller. Debug logging can be enabled as follows. Sample debug logs are shown as part of the following screen capture.

#configure terminal
(config) #logging level debugging user process stm subcat voice

Sample Debug logs:

May 7 14:13:58 :503188: <DBUG> |stm| |voice| VM: vm_lync_handle_xml_msg:1139 LYNC INFO: Received XML message from Lync Server of length = 3772
May 7 14:13:58 :503188: <DBUG> |stm| |voice| VM: vm_lync_check_xml_msg_syntax:2181 LYNC INFO: Stats are start left & right, end left & right = 0 0 1 1
May 7 14:13:58 :503188: <DBUG> |stm| |voice| VM: vm_lync_get_xml_msg_type:3377 LYNC INFO: XML method found startDialog
May 7 14:13:58 :503188: <DBUG> |stm| |voice| VM: vm_lync_parse_xml_msg_n_store:2256 LYNC INFO: lync method is start dialog
May 7 14:13:58 :503188: <DBUG> |stm| |voice| VM: vm_lync_parse_xml_msg_n_store:2314 LYNC INFO: Recv ice-ufrag:BA8k direction attrib in m line
APPENDIX

Lync SDN API specific configuration in running-config is specified below. The Mobility Controller is configured to communicate with Lync Server SDN API over “http”.

By default, Lync voice, video, desktop-sharing and file transfer traffic prioritization is enabled. This can be customized to a traffic profile and can be applied to a user role as discussed below in v6.4.

ArubaOS v6.4 specific configurations are highlighted.

```plaintext
netservice svc-sips tcp 5061 alg sips
!

web-server
web-lync-listen-port “http” 15790
!

ip access-list session lync-acl
  any any svc-sips permit queue high
!
// ArubaOS v6.4 specific Config Begin
app lync traffic-control prioritize-all-lync
prioritize-voice
prioritize-video
prioritize-desktop-sharing
prioritize-file-transfer
!
voice real-time-config
  config-enable
!
// ArubaOS v6.4 specific Config End
user-role test
access-list session lync-acl
traffic-control-profile prioritize-all-lync // ArubaOS v6.4 specific Config
!```
ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.