CONFIGURING JUNIPER WLAN FOR AN OPTIMAL MICROSOFT LYNC EXPERIENCE

Table of Contents

Introduction

This guide provides supplemental detail for Microsoft Lync unified communications (UC) administrators wishing to implement a Juniper wireless LAN (WLAN) solution.

Scope

The following sections present a brief discussion of topics relevant to UC over WLAN and will provide configuration examples where relevant. A complete CLI-based configuration example for Juniper Networks® WLC Series WLAN Controllers is provided in the Appendix. Specific sections with configuration recommendations implemented in the example will be noted.

Design Considerations

About Lync

Microsoft Lync is a popular Unified Communications & Collaboration (UC&C) platform that provides utilities for integrated instant messaging (IM), Web conferencing and content collaboration through file sharing, as well as voice and video chat. It is in support of the voice and video communications where proper network configuration and provisioning becomes critical to the success of the overall solution.

Why, When and Where QoS Is Important

Quality of service (QoS) is the mechanism by which network traffic is appropriately categorized and prioritized for subsequent handling by the network infrastructure. Voice communications such as a VoIP call or video chat are particularly sensitive to delays or disruptions in network communications. QoS ensures that the traffic associated with the voice application has the best opportunity to traverse the network without impedance. Voice and video traffic are frequently referred to as Real-Time Multimedia (RTM).

Client to AP/Infrastructure

In many cases, the first step of a journey is the most important. This is especially true for wireless clients using RTM applications. Due to the nature of 802.11-based wireless networks, the radio frequency (RF) space in enterprise environments is frequently shared by many devices. Functionally, this means that wireless connections are one of the most likely portions of a network to encounter contention or congestion. Because traffic flows in both directions over this RF medium, it is the shared responsibility of both clients and infrastructure access points (APs) to implement a functional QoS methodology.

To this end, RTM clients *must be configured* to support proper QoS handling of the critical RTM traffic. On today's 802.11 wireless networks, QoS is achieved through a protocol referred to as Wi-Fi Multimedia (WMM), which prioritizes access to the RF medium and includes a specific marking that allows receiving devices to infer appropriate QoS for any further forwarding of the marked traffic that may be required. Most client wireless interface drivers derive WMM categories from IP DiffServ code point (DSCP) values specified by the application. It is therefore critical that RTM clients not only support both DSCP and WMM, but are configured to use both. Without WMM, the client will have trouble accessing the RF medium with priority, potentially losing the QoS battle before it has even begun.

For more information on configuring endpoint QoS, see the Microsoft Techlink article at **http://technet.microsoft.com/en-us/library/gg405409.aspx**.

Infrastructure to AP/Client

Just as it is important for a wireless client to use the proper QoS, it is equally important for the rest of the network infrastructure to implement the same. Wireless APs utilize the same WMM in order to prioritize access to the RF medium. The Juniper WLAN solution has a few options for translating the wired network's QoS markings into the 802.11 WMM values it needs.

- **DSCP**: The most common method for marking QoS is with the DiffServ code point field that exists in all IP packets. The Juniper WLAN system has visibility into this field and will translate it into the appropriate WMM handling at the AP. DSCP markings function at Layer 3 of the OSI model and are persistent throughout the network.
- **802.1p Class of Service (CoS)**: CoS marking is incorporated at Layer 2 within the 802.1q standard VLAN tag structure. Since 802.1p does not persist through IP router connections by default, it is considered to be more specific. If the Juniper WLAN solution receives a datagram from the wired interface with conflicting CoS and DSCP values, the CoS setting will take precedence.
- **Policy**: It is possible through various policy interfaces within the Juniper WLAN solution to affect or alter QoS handling. This is useful in specific circumstances, and the general recommendation is to use the default DSCP/CoS prioritization within the system.

Implementation

Recommendations for the configuration of Juniper WLAN with Lync QoS are as follows:

- **Wi-Fi Multimedia (WMM):** WMM is enabled by default; no specific configuration is required.
- **QoS profile:** The Juniper WLAN solution allows for a flexible mapping of customizable QoS profiles supporting a number of QoS options to wireless user sessions via RADIUS attribute. Most of these options are not applicable to optimal UC&C support; therefore, default configuration values should be retained in most cases.
- **DSCP-to-CoS/CoS-to-DSCP mapping**: The Juniper WLAN solution offers a default mapping of DSCP-to-CoS (and by extension WMM) and CoS-to-DSCP values that are applicable in the vast majority of cases. However, if for some reason either an endpoint or the network provides a QoS marking that does not translate into the desired WMM handling, it is possible to customize these values.
- **WMM powersave:** While not strictly a QoS setting, clients that support WMM-powersave (sometimes called APSD) can enjoy enhanced battery life while maintaining appropriate QoS handling. This feature is disabled by default. Additional improvements in battery life can be realized by customizing the delivery traffic indication message (DTIM) interval value on the WLAN system radio profile. The default value is 1, causing broadcast and multicast packets to be scheduled after each WLAN beacon transmission. Changing the DTIM interval to 2 or 3 creates a compromise where wireless clients do not have to come out of sleep state to listen for relevant broadcast/multicast traffic as frequently, but delivery is still reasonably timely. See the Appendix for an example of this configuration.

Roaming and Coverage

Local Switching vs. Overlay

The Juniper WLAN solution supports a flexible traffic forwarding model that can be optimized for virtually any network scenario. All forwarding options described below are appropriate for UC&C applications, with each option offering its own advantages.

- **Local switching**: Frequently referred to as a distributed forwarding methodology, local switching allows APs to forward incoming and outgoing wireless client traffic directly to the wired network interface at the AP or to another wireless client. Of particular interest to RTM applications, the local switching method provides superior network latency compared to centralized forwarding implementations. For this reason, local switching is recommended as the preferred forwarding model wherever possible.
- **Overlay**: Often referred to as a centralized forwarding model, overlay forwarding tunnels all incoming and outgoing wireless client traffic to a WLAN controller (in Juniper's case, WLC Series Wireless LAN Controllers) to be distributed to the appropriate network interfaces. This methodology is beneficial in certain security applications (guest access, for example), and it is simply easier to implement. See the Appendix for an example of local switching configuration.

Band Steering/Load Balancing

Most of the time, wireless clients make appropriate choices regarding the best APs to associate themselves with when given multiple options (as is frequently the case in enterprise environments). However, the Juniper WLAN solution can promote the best choice to maximize the chances for an optimal outcome.

- **Band steering**: When enabled, this option encourages clients that are capable of dual-band (2.4 and 5 Ghz) operation to connect to APs offering service on the preferred band. It is recommended that this optional feature be enabled and that 5 Ghz be selected as the preferred band. This is because, in general, 5 Ghz offers a cleaner RF environment and more overall bandwidth, promoting better quality of communications between clients and APs. See the Appendix for an example of a band-steering configuration.
- **Load balancing:** Similar to band steering, the client load-balancing feature can effectively guide wireless clients to choose underutilized APs. This distributes clients more effectively between APs and maximizes RF resources. The default setting is generally recommended for UC&C enterprise applications. More strict steering configurations are possible and may be appropriate in specific scenarios.

802.1X Fast Roaming

Wireless clients connecting via strong 802.1X authentication should be configured to utilize Wi-Fi Protected Access 2 (WPA2) fast roaming via PMK-ID/OKC (Opportunistic Key Caching). The Juniper WLAN solution allows for WPA2 enterprise (802.1X) clients to successfully roam between APs within a defined mobility domain, typically a campus, without the need to renegotiate a complete authentication exchange via RADIUS every time.

Fast roaming/OKC is enabled by default for WPA2 enterprise configured services and can provide dramatically better RTM experience while roaming. WLC Series devices configured as members of the same mobility domain automatically share fast roaming/OKC data, seamlessly enabling PMK-ID-based fast roaming for relevant client sessions. Fast roaming is enabled for all WPA2 enterprise authenticated client sessions.

See the Appendix for an example of a fast roaming configuration.

Other Options

- **Static QoS profile for non UC services**: In some cases, it may be useful to apply a QoS profile with a static low priority CoS value to wireless services or users that are known to not be legitimate UC&C clients (for instance, all sessions on a wireless Guest SSID get CoS value 1/background). See the Appendix for an example of this configuration.
- **Device fingerprinting and policy**: Another optimization method that may prove beneficial is the ability (available with the Juniper WLAN solution) to apply policies based on device type. For example, Lync administrators may choose to limit support for RTM applications to a specific subset of devices that connect to a given wireless service (SSID)—Apple IOS devices and Windows7 laptops, for instance.

It is also possible to configure low priority CoS value QoS profile assignments that are mapped to other common wireless client types (such as Android devices), ensuring that higher priority WMM category access is reserved for devices and applications with legitimate uses without denying access or overburdening administration. This methodology also preserves the ability to prioritize traffic between applications on the allowed device platforms based on existing QoS markings. See the Appendix for an example of this configuration.

Summary

By following the instructions provided in this implementation guide and using the configuration examples in the Appendix, Microsoft Lync UC administrators can now implement a complete Juniper WLAN solution in their enterprise.

Appendix

Use the following configuration examples when configuring Juniper WLAN solutions with Lync Experience.

Juniper MSS Example CLI Configuration

```
LyncDemo2800# sh config
# Configuration nvgen'd at 2013-8-13 14:21:33
# Image 8.0.3.6.0
# Model MX-2800
# Last change occurred at 2013-8-13 14:21:28
set ip route default 10.105.4.250 1
set system name LyncDemo2800
set system ip-address 10.105.4.2
set system countrycode US
set timezone PST -8 0
set qos-profile static_low_priority cos 1
set device-profile nonLyncMobile attr qos-profile static_low_priority
set service-profile Campus_dot1x ssid-name Campus_Secure
set service-profile Campus_dot1x proxy-arp enable
set service-profile Campus_dot1x rsn-ie cipher-ccmp enable
set service-profile Campus_dot1x rsn-ie enable
set service-profile Campus_dot1x attr vlan-name Enterprise
set service-profile Guest ssid-name Guest
set service-profile Guest ssid-type clear
set service-profile Guest proxy-arp enable
set service-profile Guest no-broadcast enable
set service-profile Guest auth-fallthru web-portal
set service-profile Guest web-portal-acl portalacl
set service-profile Guest attr vlan-name Guest
set service-profile Guest attr qos-profile static_low_priority
set vlan-profile secureVLP vlan Enterprise
set radius deadtime 0
set radius server IC address 10.105.4.5 deadtime 0 encrypted-key
044f0e151b284249584b56
set radius server SP address 10.105.4.16 encrypted-key 03105e1812062f4b1f5b4a
set radius server NPS address 10.105.4.200 encrypted-key 105d0c1a171206
set server group IC-group members IC
set server group SP-group members SP
set server group NPS-group members NPS
```

```
set enablepass password 81254119e3b01232456e0b6f652be87b9891
set authentication web ssid Guest * local
set authentication dot1x ssid Campus_Secure ** pass-through NPS-group
set user admin password encrypted 09584b1a0d0c19155a5e57
set user admin attr service-type 6
set user guest password encrypted 130202171818
set device-fingerprint android-generic device-group android
set device-fingerprint android-generic device-profile nonLyncMobile
set device-fingerprint android-generic rule 1 type dhcp option-list EQ
53,57,60,12,55
set device-fingerprint android-generic rule 10 type dhcp option 55 EQ
1,121,33,3,6,28,51,58,59
set device-fingerprint android-generic rule 11 type dhcp option 55 EQ
1,33,3,6,15,28,51,58,59
set device-fingerprint android-generic rule 2 type dhcp option-list EQ
53,50,57,60,12,55
set device-fingerprint android-generic rule 3 type dhcp option-list EQ
53,50,54,57,60,12,55
set device-fingerprint android-generic rule 4 type dhcp option-list CONTAINS
53,61,50,57,60
set device-fingerprint android-generic rule 5 type dhcp option-list CONTAINS
53,61,57,60
set device-fingerprint android-generic rule 6 type dhcp option-list CONTAINS
53,61,50,54,57,60
set device-fingerprint android-generic rule 7 type dhcp option 55 EQ
1,121,33,3,6,15,28,51,58,59,119
set device-fingerprint android-generic rule 8 type dhcp option 55 EQ
1,33,3,6,15,28,44,51,58,59
set device-fingerprint android-generic rule 9 type dhcp option 55 EQ
1,33,3,6,28,51,58,59
set device-fingerprint android-generic rule-expression “((1 or 2 or 3 or 4 or 5 or
6) and (1 or 2 or 4 or 5 or 6 or 7 or 8 or 9 or 10 or 11) and (1 or 2 or 3 or 4
or 5 or 7) and (1 or 2 or 4 or 5 or 7 or 8 or 9 or 10 or 11))”
set device-fingerprint blackberry device-group blackberry
set device-fingerprint blackberry device-profile nonLyncMobile
set device-fingerprint blackberry rule 1 type dhcp option-list EQ 53,12,60,61,55
set device-fingerprint blackberry rule 2 type dhcp option-list EQ
53,54,50,12,60,61,55
set device-fingerprint blackberry rule-expression “(1 or 2)”
set radio-profile default dtim-interval 3
set radio-profile default wmm-powersave enable
set radio-profile default service-profile Campus_dot1x
set radio-profile default service-profile Guest
set ap 1 serial-id jb0211512003 model WLA532-US
set ap 1 radio 1 tx-power 21 mode enable
set ap 1 radio 2 mode enable
set ap 1 local-switching mode enable vlan-profile secureVLP
set ap 10 serial-id 1193000613 model MP-632
set ap 10 radio 1 tx-power 16 mode enable
set ap 10 radio 2 tx-power 13 mode enable
set ap 10 local-switching mode enable vlan-profile secureVLP
set ap 11 serial-id 1193000416 model MP-632
set ap 11 radio 1 tx-power 16 mode enable
set ap 11 radio 2 tx-power 13 mode enable
set ap 11 local-switching mode enable vlan-profile secureVLP
set ap 12 serial-id jb0211524272 model WLA532-US
set ap 12 radio 1 tx-power 21 mode enable
set ap 12 radio 2 mode enable
```

```
set ap 12 local-switching mode enable vlan-profile secureVLP
set ap 13 serial-id jb0211484122 model WLA532-US
set ap 13 radio 1 tx-power 21 mode enable
set ap 13 radio 2 mode enable
set ap 13 local-switching mode enable vlan-profile secureVLP
set ap 51 serial-id jb0211524999 model WLA532-US
set ap 51 radio 1 tx-power 21 mode enable
set ap 51 radio 2 mode enable
set ap 51 local-switching mode enable vlan-profile secureVLP
set ap 52 serial-id jb0211524538 model WLA532-US
set ap 52 radio 1 tx-power 21 mode enable
set ap 52 radio 2 mode enable
set ap 52 local-switching mode enable vlan-profile secureVLP
set ap 54 serial-id jb0211524950 model WLA532-US
set ap 54 radio 1 tx-power 21 mode enable
set ap 54 radio 2 mode enable
set ap 54 local-switching mode enable vlan-profile secureVLP
set ap 55 serial-id jb0211524847 model WLA532-US
set ap 55 radio 1 tx-power 21 mode enable
set ap 55 radio 2 mode enable
set ap 55 local-switching mode enable vlan-profile secureVLP
set ap 101 serial-id a78102900019 model MP-522E
set ap 101 radio 1 tx-power 20 mode enable
set ap 101 radio 2 mode enable
set ap 101 local-switching mode enable vlan-profile secureVLP
set ap 102 serial-id a78111300509 model MP-522E
set ap 102 radio 1 tx-power 20 mode enable
set ap 102 radio 2 mode enable
set ap 102 local-switching mode enable vlan-profile secureVLP
set ap 103 serial-id 0874101350 model MP-422A
set ap 103 radio 1 tx-power 22 mode enable
set ap 103 radio 2 mode enable
set ap 103 local-switching mode enable vlan-profile secureVLP
set ap 104 serial-id 0874101378 model MP-422A
set ap 104 radio 1 tx-power 22 mode enable
set ap 104 radio 2 mode enable
set ap 104 local-switching mode enable vlan-profile secureVLP
set ap 105 serial-id 0773501616 model MP-422
set ap 105 radio 1 tx-power 22 mode enable
set ap 105 radio 2 mode enable
set ap 105 local-switching mode enable vlan-profile secureVLP
set ap 106 serial-id 0775101858 model MP-422A
set ap 106 radio 1 tx-power 22 mode enable
set ap 106 radio 2 mode enable
set ap 106 local-switching mode enable vlan-profile secureVLP
set ip snmp server enable
set ip telnet server enable
set band-preference 5ghz
set snmp protocol v2c enable
set vlan 1 port 1 tag 1
set vlan 2 name Enterprise
set vlan 2 port 1 tag 2
set vlan 3 name Guest
set vlan 3 port 1 tag 3
set vlan 4 name Remediation
set vlan 4 port 1 tag 4
set vlan 5 name VoIP
set vlan 5 port 1 tag 5
```

```
set vlan 10 name Sslvpn
set vlan 10 port 1 tag 10
set interface 1 ip 10.105.4.2 255.255.255.0
set interface 3 ip 10.0.3.2 255.255.255.0
set snmp community name public access notify-read-write
set mobility-domain mode seed domain-name PDM
set mobility-domain member 10.105.4.3
set mobility-domain ap-affinity-group address 10.105.4.0 netmask 255.255.255.0
set security acl name portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0
255.255.255.255 eq 67
set security acl name portalacl permit udp :: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff eq 546 :: ff
f:ffff:ffff:ffff:ffff:ffff:ffff:ffff eq 547
set security acl name portalacl permit icmpv6 :: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: ffff:ff
:ffff:ffff:ffff:ffff:ffff type 136
set security acl name portalacl deny 0.0.0.0 255.255.255.255 capture
commit security acl portalacl
set cluster mode enable
```

Recommended Software Versions

- MSS version 8.0.3.6.0
- Lync Server Version 2013

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

8010094-001-EN Sept 2013 Printed on recycled paper