COMMSCOPE®

RUCKUS®

Configuration Guide

RUCKUS Switch Configuration: Hospitality

October 2020

Table of Contents

5

Intended Audience

This document addresses factors and concerns related to configuring the RUCKUS ICX switches for hospitality environments. Many factors can affect both the initial work and final performance. These are considered here.

This document is written for and intended for use by technical engineers with some background in networking, Wi-Fi design, and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

Overview

This document provides network designers, architects, and WLAN professionals guidance for configuring ICX switches using CommScope's RUCKUS networking equipment and software. This document is one in a series of design and configuration guides. This document is the third in this series created for the Hospitality market. Please reference the full suite of Design and Configuration Guides for Hospitality.

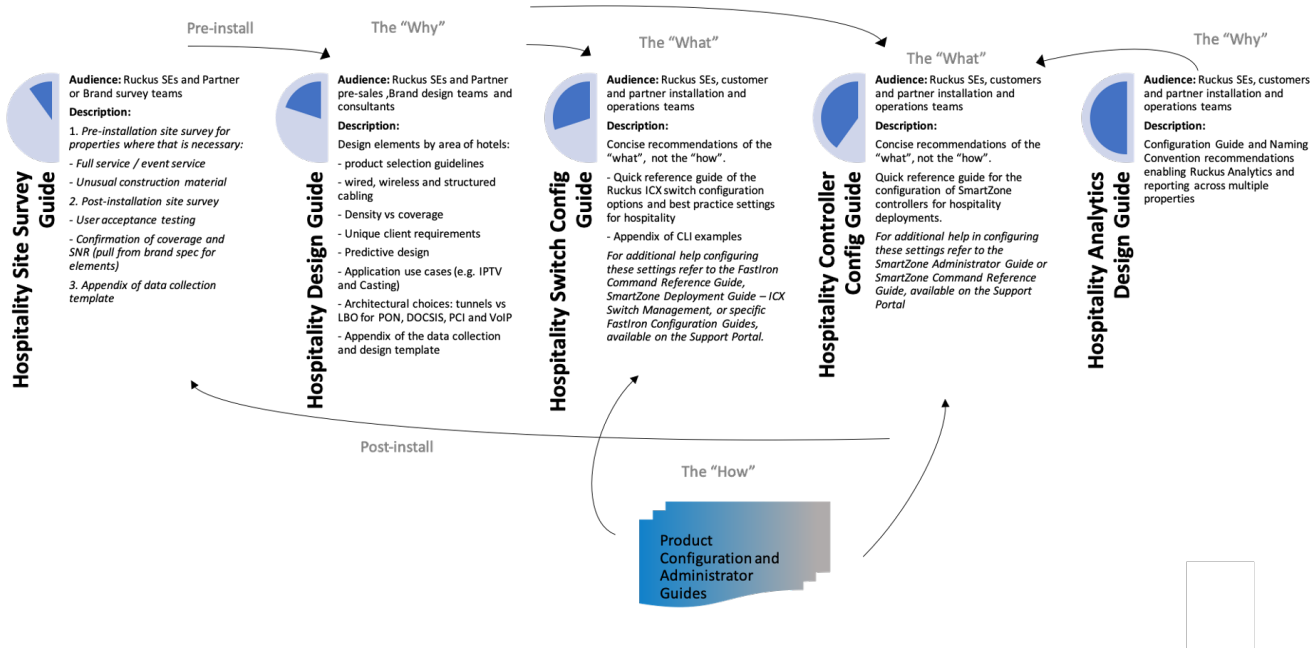

FIGURE 1: SUITE OF DESIGN AND CONFIGURATION GUIDES FOR HOSPITALITY

This document is intended to provide guidance to Hospitality Managed Service Providers to ensure consistency and optimal performance of deployed RUCKUS network infrastructures across properties.

This document is one in a series of Design and Configuration Guides specific to the Hospitality vertical. Please refer to the other documents to provide a more complete picture. The intended audience for this body of work includes Ruckus Systems Engineers and customer and/or partner installation and operations teams. These documents are intended to primarily cover the "What" and some of the "Why", not necessarily the "How", when it comes to configurations. Ruckus provides separate additional resources, both in the form of online and offline configuration guides, internal/partner support portal knowledge base, and How-to videos posted to YouTube. Partners can always engage Ruckus Systems Engineers or Field Engineers with questions or assistance as needed.

ICX Switch Models

The following switch model families are recommended for hospitality properties worldwide.

Switch Model	Edge	Core (Select Service)	Core (Full Service)
ICX 7150-C08, C10ZP	✓		
ICX 7150-24, 24F, 24P, 48, 48P, 48PF, 48ZP	✓	✓	
ICX 7250-24, 24P, 48, 48P	✓	✓	
ICX 7450-24, 24P, 48, 48P	✓	✓	✓
ICX 7550-24, 24P, 24ZP, 24F, 48, 48P, 48ZP, 48F	✓	✓	✓
ICX 7650-48F, 48P, 48ZP	✓	✓	✓
ICX 7750-26Q, 48C, 48F	✓	✓	✓
ICX 7850-32Q, 48F, 48FS	✓	✓	✓

TABLE 1 – ICX SWITCH MODELS

ICX Switch Software

Multiple versions of switch software are recommended. New features are being added often so locking in on a specific version is difficult and depends on many factors including feature preference, existing software versions, and LSP preference. These recommendations are the minimums.

If there is a new build, or an LSP is newly looking at ICX, start with the 8.0.95(x) software and test in the lab thoroughly. This version has all the latest features and supports all hardware on the market today.

For existing deployments, 8.0.90(x) is recommended as it has been vigorously tested and deployed. LSPs should be testing and preparing for an 8.0.95 rollout, which will be an extended release for all hardware that is out there today.

Switch Model	Current Version (2020)	Features
Fastiron OS 8.0.90x	8.0.90h	Extended release for all models except for ICX 7150-C08P, C08PT, C10ZP and 24F
Fastiron OS 8.0.92x	8.0.92d*	Release to enable above switch models
Fastiron OS 8.0.95x	8.0.95b**	Upcoming (October 2020) release for all ICX 7000 models

TABLE 2 – ICX SWITCH SOFTWARE

* The ICX 7750 does not support version 8.0.91.

** 8.0.95 is the last version with ICX 7750 new feature support.

ICX Switch Device Features and Interoperability

Ruckus ICX switches use industry standard methods and protocols in order to interoperate in a mixed vendor environment. All of these features have been tested and implemented thoroughly in hospitality environments. Switch features used in Hospitality include but are not limited to the following:

Feature	Description
AAA	Authentication, Authorization and Accounting can be configured to restrict access to the console and management of the switch, and log any such activity locally or to an off-box device
ACLs	Access-control lists are fully configurable to allow or restrict lists of devices either to the management of the switch or to data paths through the switch.
Address Families	Both IPv4 and IPv6 are supported
Authentication	A full 802.1x and Mac-Authentication implementation is supported on all models. Local, RADIUS or TACACS are all supported authentication methods
Banner	Login banners are fully supported
Boot	The switch can be booted from the primary or secondary flash allowing a primary and backup software version to be loaded so that if a failure occurs to the primary, the switch will at least boot to a secondary software version so the device can be analyzed and repaired.
Breakout	Certain 40Gig and 100Gig ports can be configured in breakout mode to allow multiple links from a single port on the switch. This extends the capacity to allow for more connections.
Captive Portal	Captive portal redirection is supported
CDP	Cisco Discovery Protocol is support when Cisco end devices such as phones are present.
Copy	Files can be copied to or from a device to quickly update the configuration or to copy new software to the device for upgrades. HTTP, SCP, TFTP, and USB are all supported
DHCP	By default, all devices are DHCP clients, which aides in auto and zero-touch provisioning. Switches running router images can also be DHCP Severs to service the network's IP addressing needs.
DHCP Snooping	DHCP Snooping can be enabled on VLANs to block unauthorized DHCP servers from returning IP addresses. Combined with the trust-dhcp command, the exact path of authorized DHCP servers can be configured
Hitless Failover	Hitless Failover is configured by default when stacking is enabled. The backup master switch will take over sub-second when it senses the master switch is no longer reachable. This feature will allow management of the device to continue .
Inline Power	PoE enabled switches can be configured by port or group of ports for PoE to support compatible devices. Power by class or power limits can be configured to appropriately allocate power as required.
IP Address	IP Addresses can be configured for management as well as for default-gateway functionality for client devices. 256 different IP addresses may be configured per switch.
IP Helper Address	IP Helper Addresses may be configured when the DHCP server is on a different VLAN from the client device. This allows for centralization and categorization of clients depending on where they originate.

IGMP	IGMP versions 2 and 3 are supported. In conjunction with Multicast devices elsewhere in the network, the IGMP enabled switches can streamline the multicast streams for optimal performance to the client devices.
ISSU	In-Service Software Upgrades allow individual switches in a switch stack to be rebooted separately when upgrading to a new minor release to maximize uptime of clients connected to the stack.
Jumbo	Jumbo frames up to 8192 MTU are supported.
LACP	Link Aggregation Control Protocol is an industry-standard protocol which supported to connect devices together with multiple links in a LAG or link bundle.
LAG	Link Aggregation Groups are supported in either Dynamic or Static mode. Dynamic LAGs use LACP and Static LAGs are hard-coded. Up to 8 or 10 links can be supported across a single device, or a stack depending on the device.
LLDP	Link Layer Discovery Protocol is an industry standard protocol used for neighbor detection and information gathering.
Logging	Logging is available and configurable with various verbose preferences. Logs can be held locally and/or forwarded off-box to a syslog server.
Loop Detection	Loop detection can be enabled to check for loops on physical ports or on VLANs.
MAC Filters	MAC Filters can be configured to permit or deny traffic based on source of destination MAC addresses.
MCT	Multi-Chassis Trunking is a virtual chassis technology that allows two ICX switches to share LACP information from a client and spoof a single chassis. This allows the downstream client(s) to split their traffic to two devices for maximum redundancy and load balancing. MCT required ICX 7650 or higher. The client devices can be any device that supports the LACP protocol.
Management VLAN / Management VRF	Management VLANs and Management VRFs can be configured to isolate and secure management traffic from other traffic traversing the switch
Mirroring	Port Mirroring is available in order to analyze traffic either locally or traffic can be sent remotely for analysis
Multicast	Multicast version 2 and 3 are supported. Switches can be configured as multicast active port passive and rendezvous points
NTP	NTP servers can be configured to sync the system time
Optical Monitoring	With supported optics, Optical Monitoring allows viewing the fiber optic light and power levels for tracking and troubleshooting
OSPF	The Open Shortest Path First protocol is available for connections to protocol compliant devices
PIM	Protocol Indepent Multicast is supported in either Dense or Sparse mode and allows multi-VLAN multicast routing.
Port Security	Port Security allows the configuring of which or how many MAC addresses can access a port for granular security functions
Protected Port	The Protected Port command limits communication between ports to isolate traffic to only ports which are authorized
QOS	A full Quality of Service implementation is available for granular traffic manipulation and prioritization
RADIUS	RADIUS servers can be configured to authenticate management users or devices requesting access to ports
Rate Limiting	Rate Limiting is available to limit traffic inbound or outbound per port

SCP / SSH	Secure Copy and Secure Shell are supported
SNMP	A full SNMP implementation is available for monitoring and configuring of devices. SNMP Traps are also supported
Spanning Tree	Multiple versions of Spanning Tree are available including Regular, Rapid, Multiple (MSTP), Per-VLAN (PVST) and Cisco's PVST+
Stacking	Device stacking allows two or more devices to be connected and be managed as a single virtual device. This extends the capacity of a device to include more and diverse port types. Up to 12 PoE, non-PoE, and fiber devices can all be stacked together and be managed as a single virtual chassis.
System Max	System Max commands can be used to override the default memory allocations for certain variables. For instance, the default value for VLANs is 1024, but a system-max command can re-carver the memory to allow up to 4096.
TACACS	TACACS is support as part of the AAA implementation to authenticate users, authorize commands that can be issues by user or group and log such commands and outputs
Telnet	Telnet is enabled by default in older versions of code but turned off starting in 8.0.80 code. It can be re-enabled if desired.
Terminal Monitor	Terminal Monitor or "Term Mon" can be enabled to log the current session to the console
VE Interface	Virtual-Ethernet interfaces associated to VLANs and contain Layer 3 information for the VLAN it is associated with.
VLANs	Virtual LANs can be configured to isolate Layer 2 traffic. Ports are either tagged or untagged depending on the type of traffic expected. Up to 4096 VLANs can be configured
Write Memory	Write Memory or "Write Mem" saves the current running config to be the startup config
Zero Touch	Zero-Touch provisioning is a feature where the stacking of switches can be streamlined by entering one command on the master switch.

TABLE 3 – ICX FEATURES

ICX Switch Recommended Configuration

These setting recommendations are based on both theoretical and empirical information regarding the expected or possible client performance and behavior with specific settings values as noted below:

Feature	Recommendation	Description
Software Version	FastIron OS 8.0.90h* Or FastIron OS 8.0.95	• With so many new features being added to the software and with new switches being introduced, the recommendation is to get the latest code possible to maximize the switch's capabilities. • If SmartZone controller management is required, 8.0.80 code is the minimum for read-only access and 8.0.90 code is the minimum read/write access • Always use the latest patch release from support.ruckuswireless.com. • ICX 7750s cannot use 8.0.91. Either go back to 8.0.90(x) or 8.0.92. • As of October 2020, 8.0.95 is released and can be tested and deployed when comfortable
Stacking	Recommended when multiple switches are co-located	• Switches that are co-located benefit from being stacked. Stacked switches allow maximum flexibility to build the right type and right amount of ports without stranding empty slots like a chassis would. • Stacked switches can be mixed so that non-PoE, PoE and even fiber switches can used to fit the different requirements • Up to 12 switches from the same family can be stacked using 10Gig fiber optics or Direct-Attached Cables (DAC). • With the use of fiber optics, switches can be stacked over the distance of the fiber available. In certain instances, this can allow the collapsing of a 3-tiered architecture into a 2-tiered architecture be making the core a virtual chassis across multiple locations. • Stacking can lower the number of uplinks required if each switch in a closet is currently uplinked individually • Stacking is also much more graceful than daisy-chaining or single-uplinking to one switch causing a single point of failure. • Lastly, Stacking allows for uplinks to be spread across multiple devices in the stack which allows for active/active connections without having to use spanning-tree to break the loop.
LAGs	Recommended when multiple links exist between IDFs and MDFs	• Link Aggregation Groups should be used when there is more than one uplink between the IDF and the upstream device. • Redundancy and Load Balancing are the main benefits • Spanning Tree is also not required to break loops because all links in the bundle are active • LAGs can be 1Gig, 10Gig, or 40Gig, but all links in the bundle must be the same speed. • 8 Links on 7150s, and 12 links on all other ICX switches are supported

MCT	Recommended when dual core switches and multiple uplinks from IDFs exist	• Multi-Chassis Trunking is recommended when a Full Service property has the ability to install dual core switches and has two pairs of fiber coming back to the MDF. • Using MCT allows each chassis to act independently, not stacked, such that each switch can be rebooted or taken down independently without affecting the other. • This allows even greater uptime, as even during upgrades, there will always be one core switch up and running
VLANs	Use as needed	• Up to 4096 VLANs can be configured. • 1024 VLANs are allowed by default. Use system-max VLAN <xxxx> command to allow more. • Ports are either tagged (trunked) or untagged (access) • IP Addresses can be added to VLANs by adding the router-interface command to the VLAN which then builds a VE interface

Multicast / Snooping	Typical layer 2 installations would need active multicast on core switch VLANs, and passive multicast on all edge switch VLANs.
	PIM is only needed when routing between VLANs.
		• Up to 3092 multicast groups are allowed on 7150s, and up to 8192 groups are allowed on all other switches.
		• If the source is in the same VLAN as the client, set multicast active on the VLAN on the core switch, and multicast passive on the VLAN on the edge switches
		• The core switch must have an IP address on the VLAN's VE interface which is in the same subnet as the source.
		• If the source is in a different VLAN than the client, then PIM must run on the core switch and the core switch must be configured as a rendezvous point (RP). The IP address of the multicast VLAN or a Loopback can be used as the RP.
		• Multicast fast-convergence allows the switch to listen to other Layer 2 messages like spanning tree to detect a new device and allow it to join multicast faster. This is recommended on the VLAN on the core switch and the edge switch
		• Multicast fast-leave immediately turns off multicast on a port when a leave message is received.
		  ○ DO NOT put this on the core switch or each leave message will kill the stream to that switch.
		  ○ DO NOT put this on an edge switch port that support multiple clients like a suite or a downstream mini-switch

Chromecast / Streaming Media	Add ACL to switch to guard against mDNS flooding	• Chromecasts and other streaming media devices are being installed in greater quantities in Hotels. • These devices have been seen sending mDNS and other broadcasts onto the network to communicate with other devices like themselves as if they were on a home LAN. • In Hospitality these devices should not communicate directly with each other for privacy reasons because each device is tied to one room and one user. • To mitigate this communication, an Access Control List (ACL) can be applied at the switch interface to block this traffic to mitigate

		network performance issues when a large number of streaming devices are added to the network. • See Ruckus Tech Bulletin to see how to apply the ACL to both wired and wireless ports. • https://support.ruckuswireless.com/articles/000009674 (Ruckus Support Login Required)

Spanning Tree	MSTP	• All variants of Spanning Tree are configurable on ICX switches
		• By default, Switch code runs 802.1D which is regular spanning tree. Router code does not run spanning tree by default.
		• The easiest implementation of spanning tree on ICX is MSTP.
		  ○ It is interoperable with other vendors who run MSTP.
		  ○ It auto-adds and deletes new VLANs into MSTP when they are added to the config
		• STP BPDU Guard can be added to interfaces which will shut down ports that receive BPDUs.
		• Spanning Tree Root Protect can be added to interfaces which will ensure that root-bridge BPDUs are dropped so that the root will not move to the device on the other side of that port.

DHCP Snooping	If protected-port is turned on, dhcp snooping is not required	• DHCP Snooping is recommended to ensure that a rogue DHCP server will not distribute IP addresses if it is not authorized
		• DHCP Snooping is turned on manually per VLAN.
		• All ports that participate in that VLAN will receive the config.
		• Ports that legitimately receive a DHCP return packet, need the dhcp trust command. This is generally the edge switch's uplink port.
		• Add dhcp trust to the core switch that has the connection to the DHCP server
		• If the DHCP server fails to give IP addresses, it may not understand packets received from modern switches.
		  ○ ICX switches for instance, insert their own information into the DHCP request packet from the client.
		  ○ The feature is also commonly called "Option 82"
		  ○ If the server believes the packet is not corrupted, then the switch needed to stop sending that information.
		  ○ The command "no dhcp snooping relay information" needs to be added to all client ports.
		  ○ A global command is now allowed per switch to turn off this feature.

Port Authentication	Required for Backoffice port authentication	• GPNS Standards require the ability to authenticate ports via 802.1x or Mac-Authorization • ICX switches allow the configuration of the restricted-VLAN, dot1x guest VLAN, and critical VLAN to be the same in newer software. • ICX switches also allow the override of the global authentication configuration per port for use with conference rooms that need special configuration.

		• The "multiple-hosts" configuration allows for one device, for instance a switch, to authenticate itself, and then all devices behind it pass through without authentication challenges. This is for parties that need wired internet connection but don't need to authenticate each device. • Protected port and auth version? 8.0.70
Protected Port	Enable on all downstream ports, not on uplinks or servers, gateways	• The protected-port command is used to isolate ports from each other in the Hospitality environment. • It is a port level command affecting all VLANs. • It is recommended to set the command on all ports facing clients such as APs, TVs, Phones, etc. • Do not set the command on the uplink port from the edge switch or no traffic will leave the switch. • Don't forget to set the command on all downlinks on the core switch or each switch will be able to talk to a switch on the other side of the core. • Do not set the command on the gateway, wireless controller, DHCP server, etc. • If port-to-port communication is required in the same VLAN, for instance the AP management VLAN, or the RTP VLAN for VoIP, set the command ip-local-proxy-arp in the VLAN on the core switch, and traffic will go to the core to get bridged back to the other ports in the VLAN.
PoE Power	Set all in-room ports to class 3, set all conference space to class 4	• PoE power is on by default starting with software version 8.0.70. • The default is to allocate the amount of power asked for and deduct it from the overall power budget. • Since most switches in the portfolio have a power budget of 15w per port, but can service 30w per port, there may be an oversubscription f too many devices are attached at 30w. • PoE power can be hard-coded to lower the power draw per port to support more devices • It is recommended for most Ruckus H510 installations, to set the power-by-class on each port to class 3 to allow all APs on the switch to power up and run properly. • If higher-powered devices are attached, their power budget must be deducted from the power budget, and ports should be left open allowed accordingly. • Discuss H510 and power draw • Consumption Mode -- No
LLDP	Turn on to get the most information about neighbors	• LLDP should be enabled in order to see the device's neighbors including Ruckus Access Points. • Industry standard protocol to detect can get information for directly connected physical neighbors

SmartZone Management	Turn on feature to manage switches in SmartZone controllers	• ICX switches can be detected and managed by a SmartZone controller beginning in FastIron 8.0.80. • With 8.0.90 and newer software, the switches can be configured to change port configurations such as VLANs. • The controller can also report the current version and upgrade the software to the desired level. • Interface statistics can be viewed for all interfaces to see traffic patterns and client device MAC addresses

TABLE 4 – ICX RECOMMENDED CONFIGURATION

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.