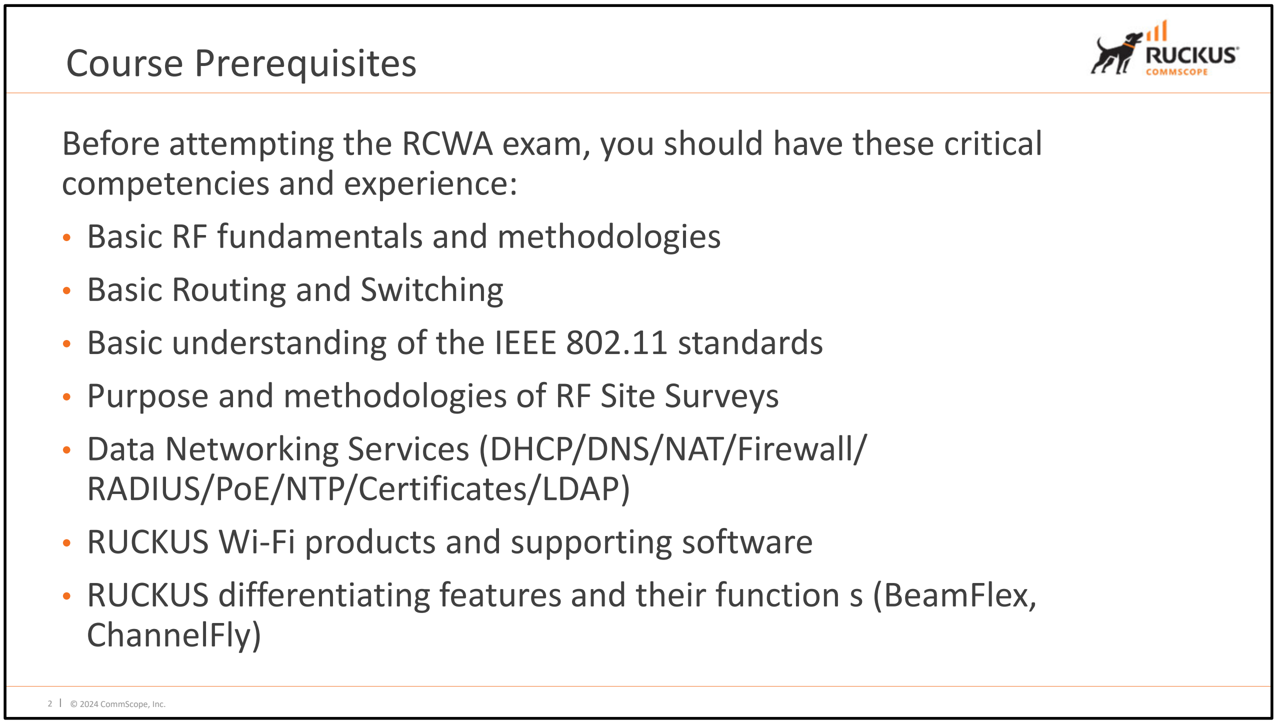
RCWA Nutshell Study Guide

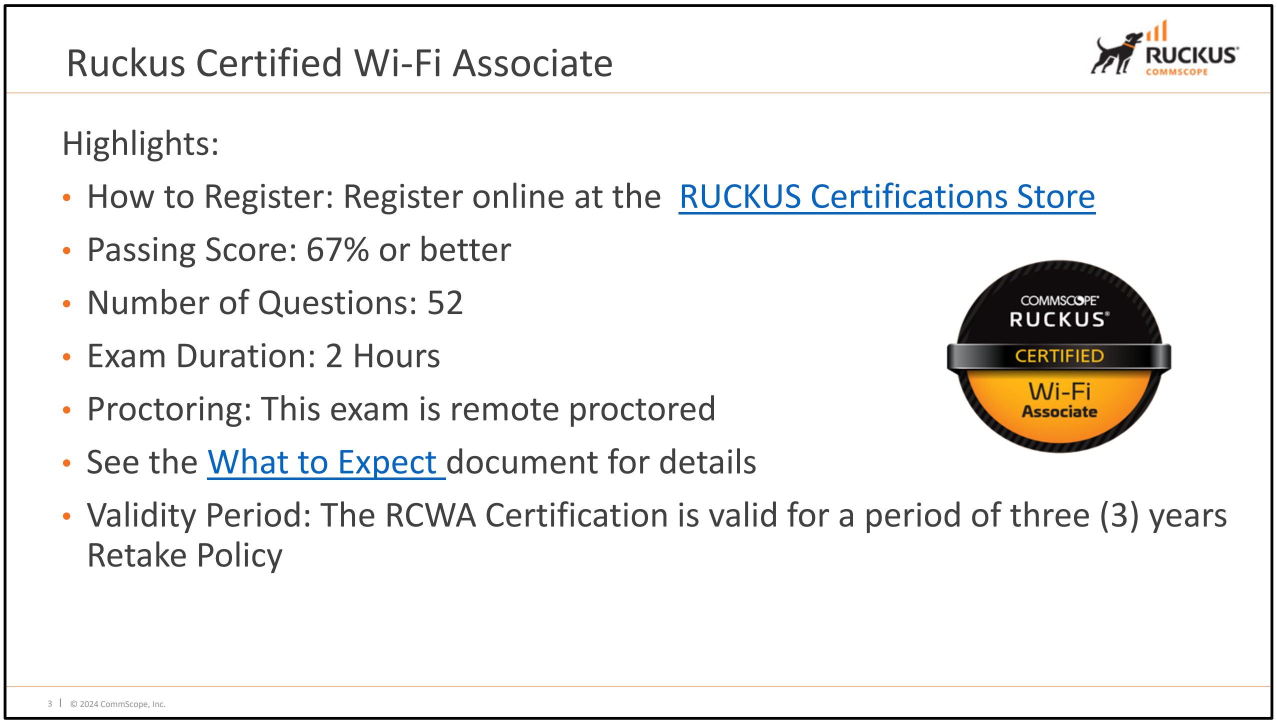


Course Prerequisites

Before attempting the RCWA exam, you should have these critical competencies and experience:

- Basic RF fundamentals and methodologies
- Basic Routing and Switching
- Basic understanding of the IEEE 802.11 standards
- Purpose and methodologies of RF Site Surveys
- Data Networking Services (DHCP/DNS/NAT/Firewall/ RADIUS/PoE/NTP/Certificates/LDAP)
- RUCKUS Wi-Fi products and supporting software
- RUCKUS differentiating features and their function s (BeamFlex, ChannelFly)

2 |



Ruckus Certified Wi-Fi Associate

Highlights:

- How to Register: Register online at the RUCKUS Certifications Store
- Passing Score: 67% or better
- Number of Questions: 52
- Exam Duration: 2 Hours
- Proctoring: This exam is remote proctored
- See the What to Expect document for details
- Validity Period: The RCWA Certification is valid for a period of three (3) years Retake Policy

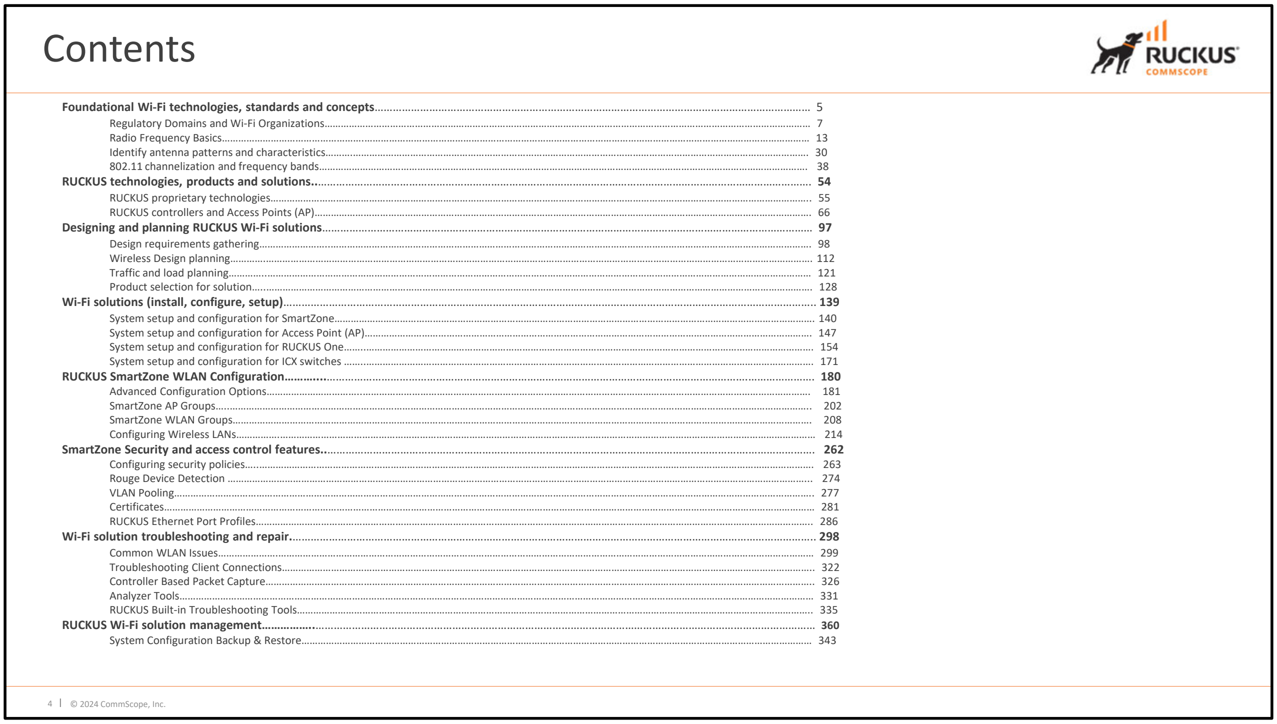
3 | © 2024 CommScope, Inc.

Once you have passed the exam, you may not retake the exam except to recertify.

If failed, you may retake the exam immediately, however, after a second attempt you must wait 14 days.

After a third or fourth attempt, you must wait 30 days.

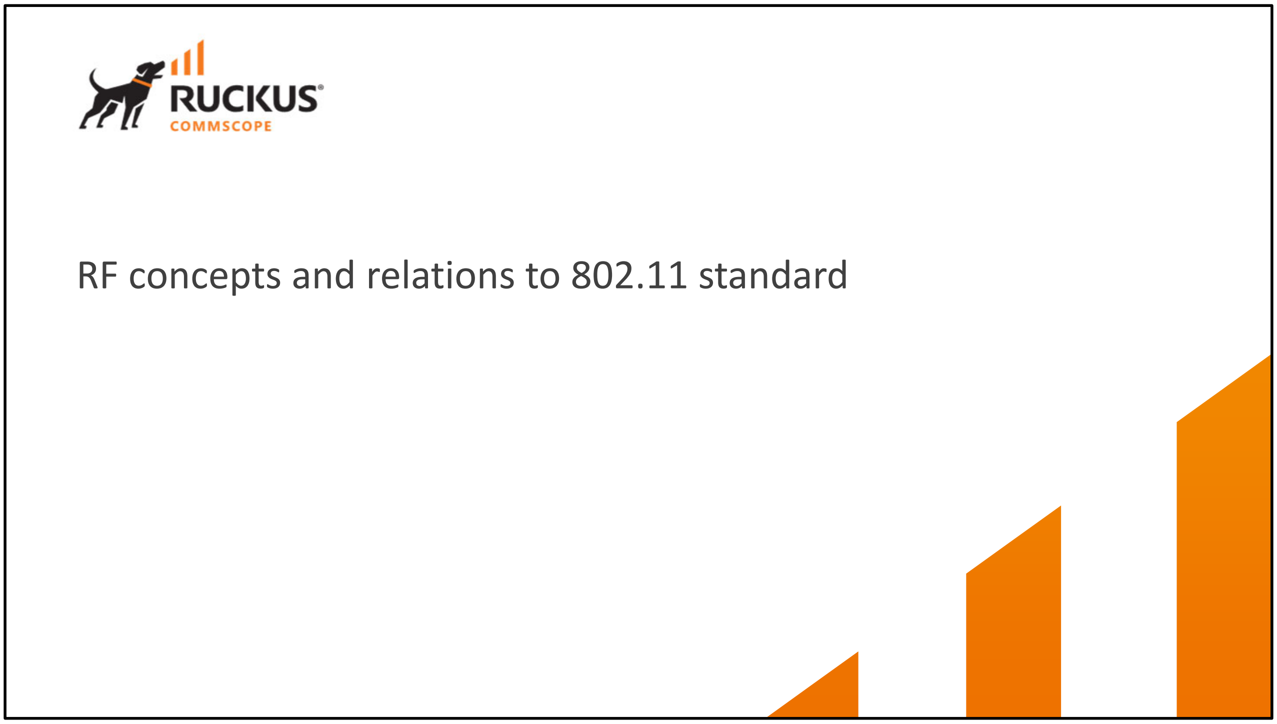
No more than 5 retakes are allowed within one year from your first attempt.



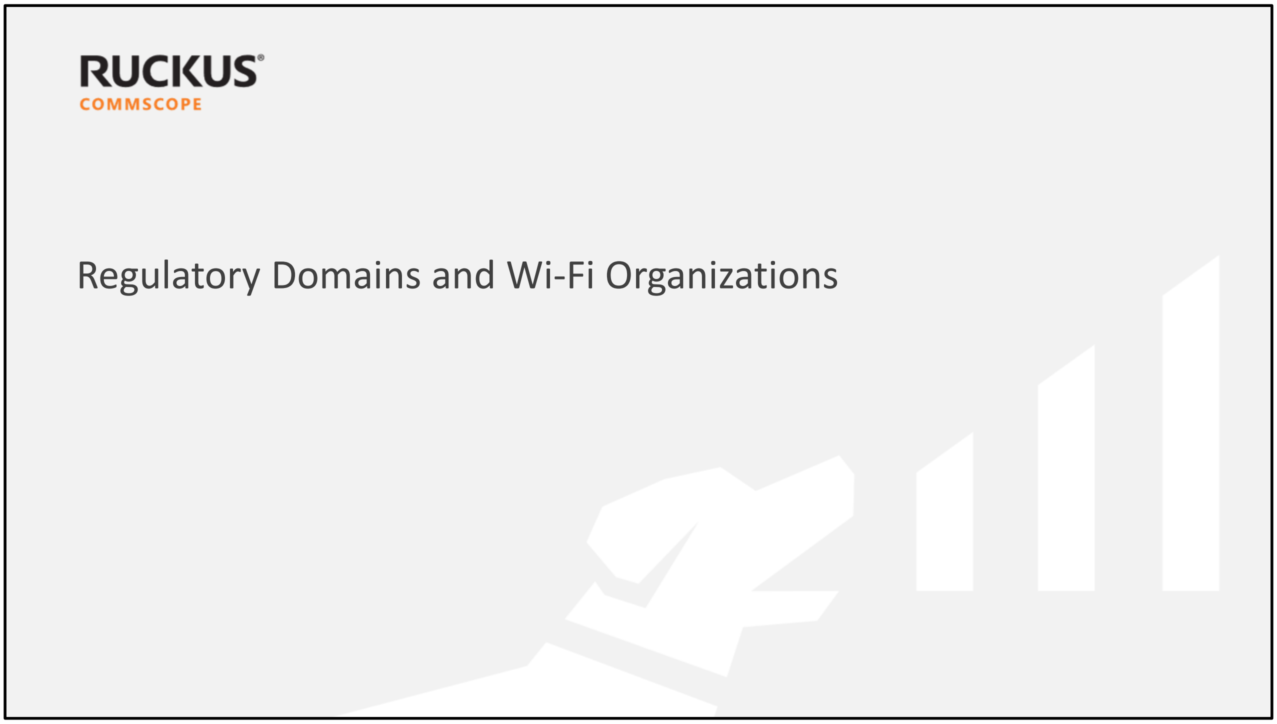
Contents

4 |

Foundational Wi-Fi technologies, standards and concepts

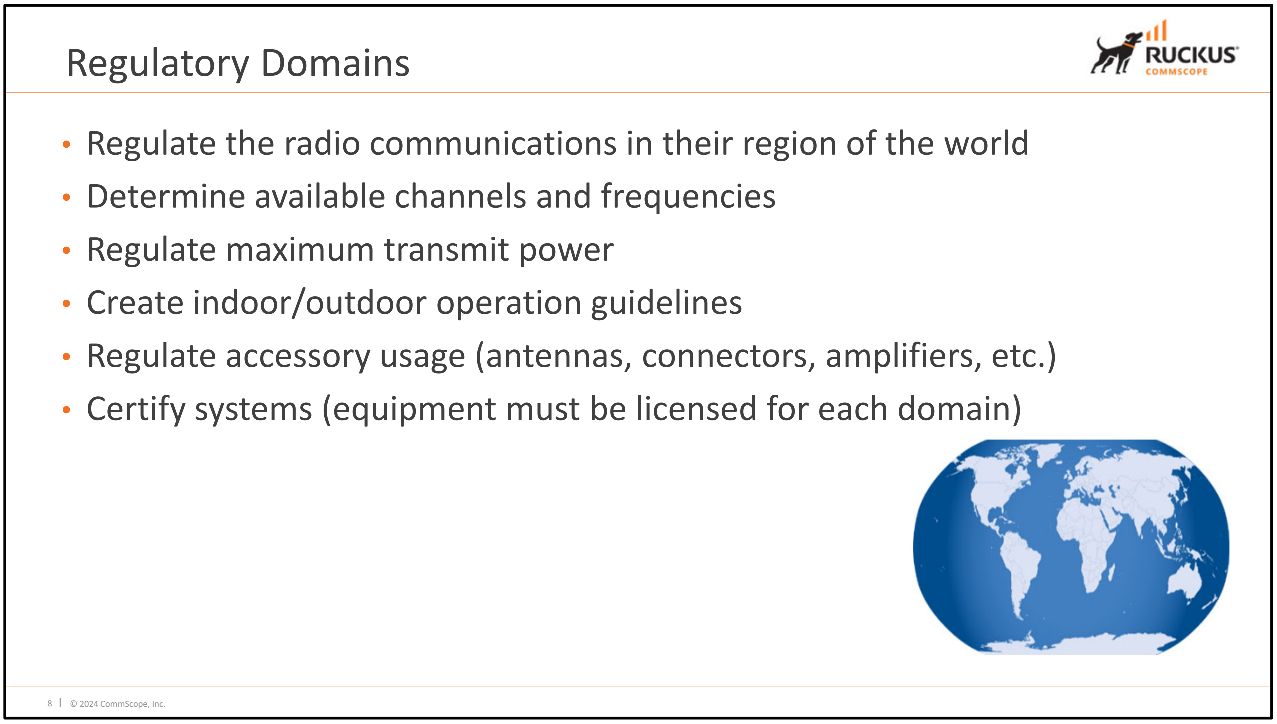


RF concepts and relations to 802.11 standard



RUCKUS
COMMSCOPE

Regulatory Domains and Wi-Fi Organizations



Regulatory Domains

- Regulate the radio communications in their region of the world
- Determine available channels and frequencies
- Regulate maximum transmit power
- Create indoor/outdoor operation guidelines
- Regulate accessory usage (antennas, connectors, amplifiers, etc.)
- Certify systems (equipment must be licensed for each domain)

8 | © 2024 CommScope, Inc.

Regulatory domains dictate the specific allowances, behaviors and technologies that are allowed to operate in a geographic region. Some countries follow only their own regulations when using RF signaling. Others follow a common set of regulations regionally. These regulatory domains regulate the radio communications in their region of the world, Determine available channels and frequencies, regulate maximum legal transmit power, create indoor and outdoor operation guidelines, regulate accessory usage, and certify radio systems.

As a WLAN administrator, you must know the limits imposed by these organizations. You must follow these regulations across your deployments based upon the physical location of your equipment. What is legal and common in one region may be neither in another. Some items that may be important to consider are:

- How much output power am I allowed to use for a device?
- What frequencies are allowed for public use within my regulatory domain?
- What connector types am I allowed to use within my WLAN system?

Industry Regulations and Laws

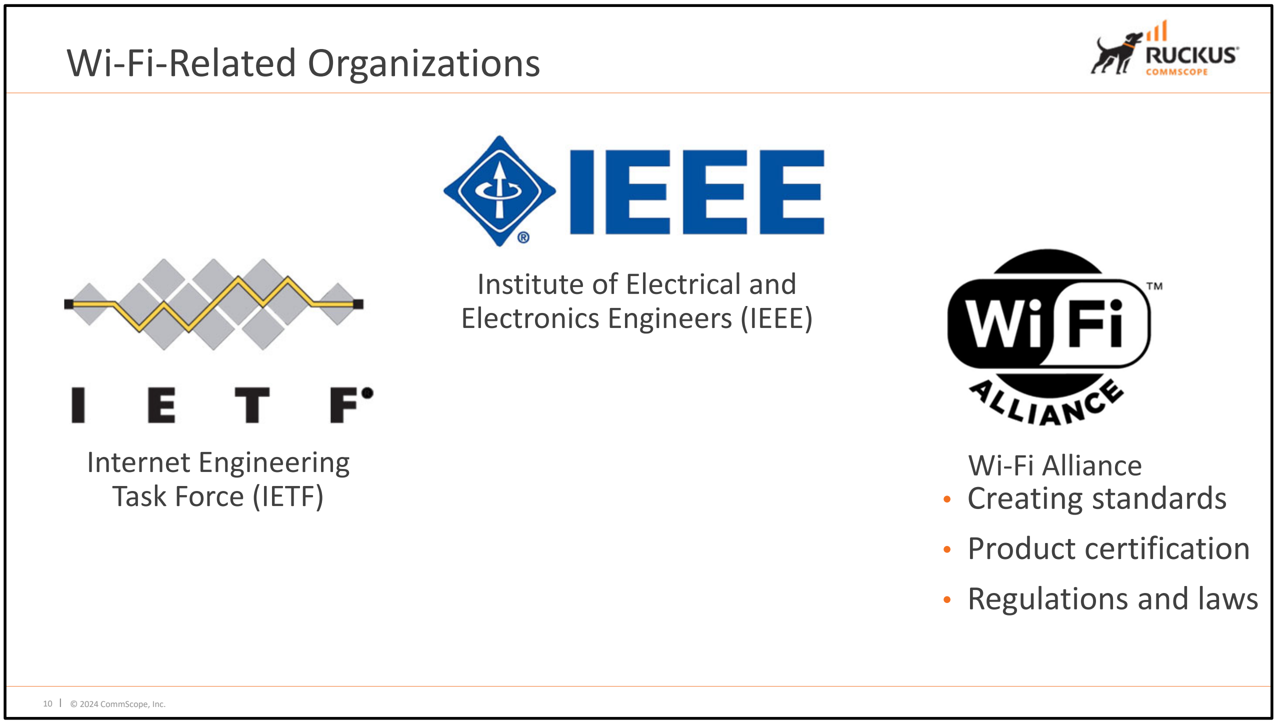
RUCKUS
COMMSCOPE
FEDERAL COMMUNICATIONS COMMISSION · USA ·
FCC
TELEC
ETSI
World Class Standards
Industry Canada
Industrie Canada
総務省
Ministry of Internal Affairs and Communications

9 | © 2024 CommScope, Inc.

Industries within different verticals and governments have a large impact on WLAN use. Within different verticals, you will find different requirements for networking, some specific to WLAN use and some just networking in general. These are usually related to data protection and network security. Governments control by law two very important things to us in WLAN deployment. They control the frequency space we can use and the amount of power we can use within that space.

When designing a WLAN, you must ensure that the design falls within the industry and governmental requirements for each location. Multinational deployments can be quite tricky, given the varied frequency and power use requirements across multiple countries. Non-compliant deployments can result in large fines. You must ensure that your designs meet the industry and government requirements in addition to the requirements of your customer’s needs.

When deploying a RUCKUS WLAN, you can use Zones to assign country codes to the APs, ensuring the APs in each Zone will only use channels and powers that are legal for the configured country code. More information about this configuration can be found in the RASZA 200 course and on the support website.



Wi-Fi-Related Organizations

Internet Engineering Task Force (IETF)

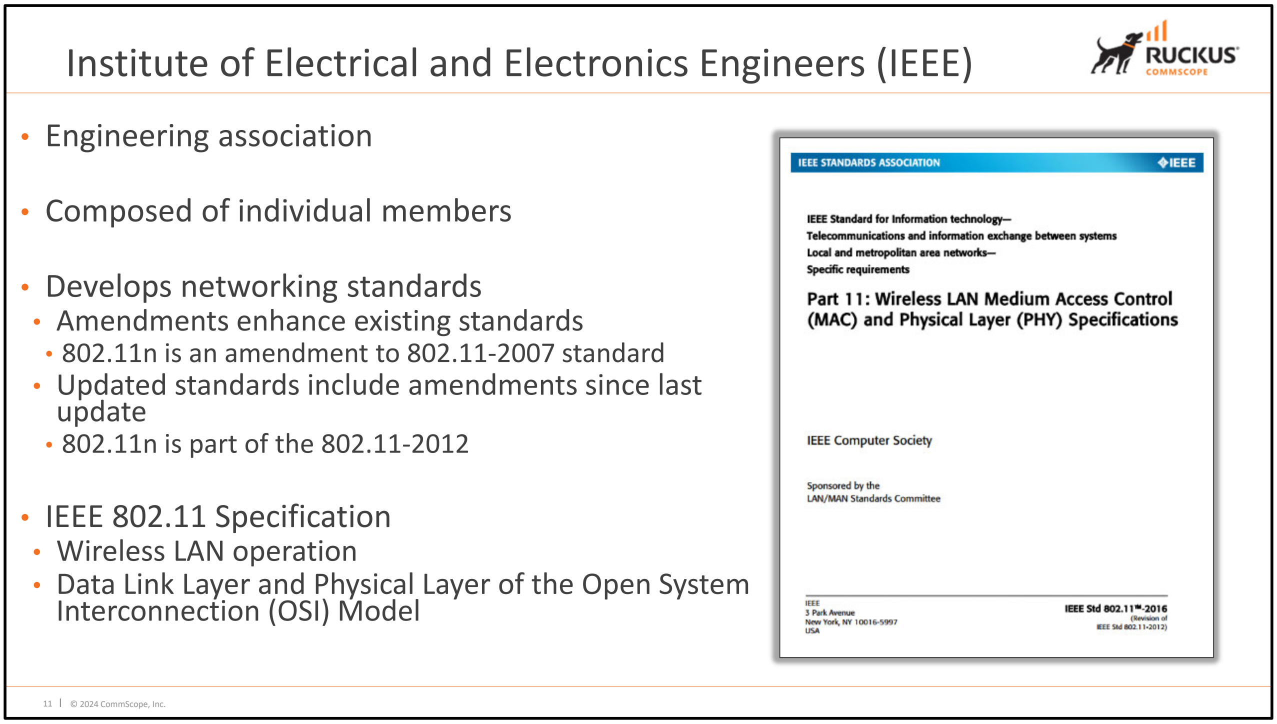
Institute of Electrical and Electronics Engineers (IEEE)

Wi-Fi Alliance

- Creating standards
- Product certification
- Regulations and laws

10 | © 2024 CommScope, Inc.

There are several Wi-Fi related organizations that directly impact how we use RF in wireless networking. The Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers, and the Wi-Fi Alliance. Some define the standards that must be followed. Some certify products to guarantee interoperability. There are even some that set local regulations and laws. These various organizations will be explored.



Institute of Electrical and Electronics Engineers (IEEE)

- Engineering association
- Composed of individual members
- Develops networking standards
  - Amendments enhance existing standards
    - 802.11n is an amendment to 802.11-2007 standard
  - Updated standards include amendments since last update
    - 802.11n is part of the 802.11-2012
- IEEE 802.11 Specification
  - Wireless LAN operation
  - Data Link Layer and Physical Layer of the Open System Interconnection (OSI) Model

IEEE STANDARDS ASSOCIATION ◆IEEE

IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

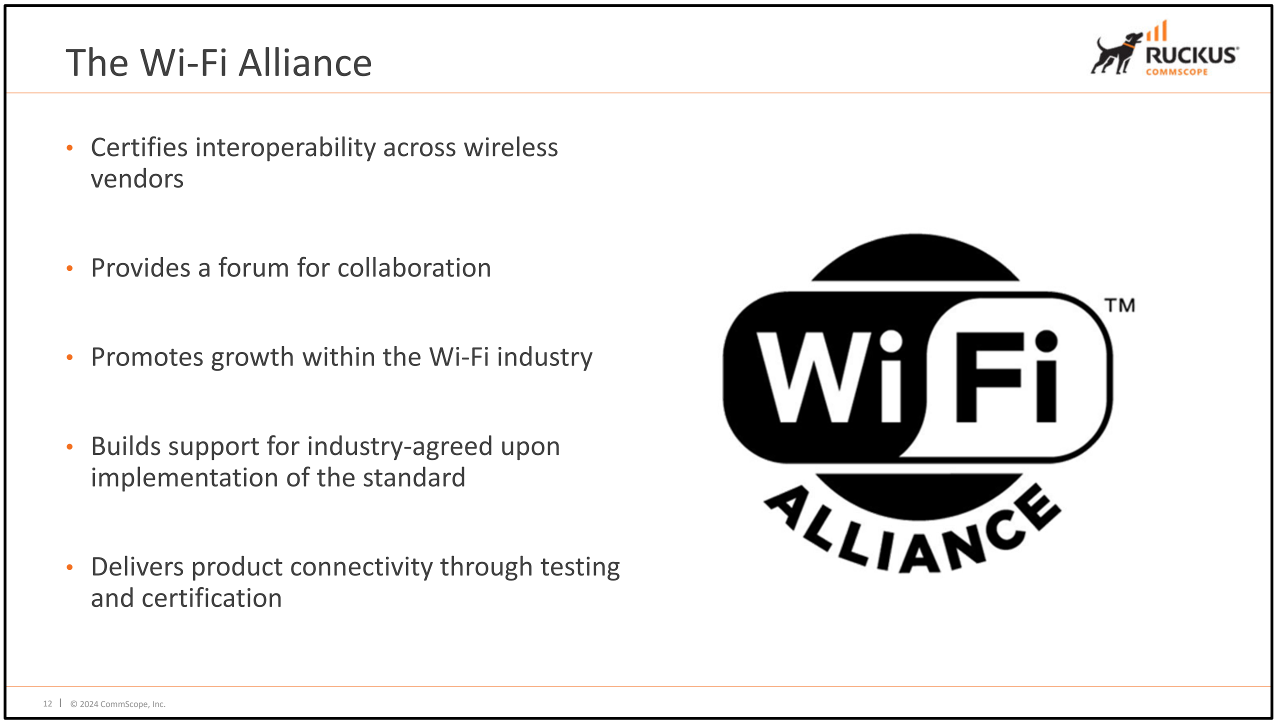
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.11™-2016
(Revision of
IEEE Std 802.11-2012)

11 | © 2024 CommScope, Inc.

The Institute of Electrical and Electronics Engineers (IEEE) is made up of actual engineer members. These individual member engineers work in committees. Through these committees, they define standardized methods of communication. The IEEE creates the standards and subsequent amendments that today's wireless products adhere to. Once an amendment to a standard is ratified, it will become part of the standard the next time it is updated. The specifications the IEEE creates are within the confines of regulatory domains. Which means, even though something is part of an IEEE standard, you must still implement and use that technology within the laws of the regulatory domain in which it is deployed.

The IEEE 802 task group creates standardized data communications protocols for Layers 1 and 2 of the OSI model. The 802 task group responsibilities includes 802.11 (Wi-Fi) and 802.3 (Ethernet). The 802.11 standard is of particular concern to those of us working in Wi-Fi. And, because, at some point the wireless network must connect to the wired network, it makes sense to have an understanding of both the 802.11 and 802.3 standards.

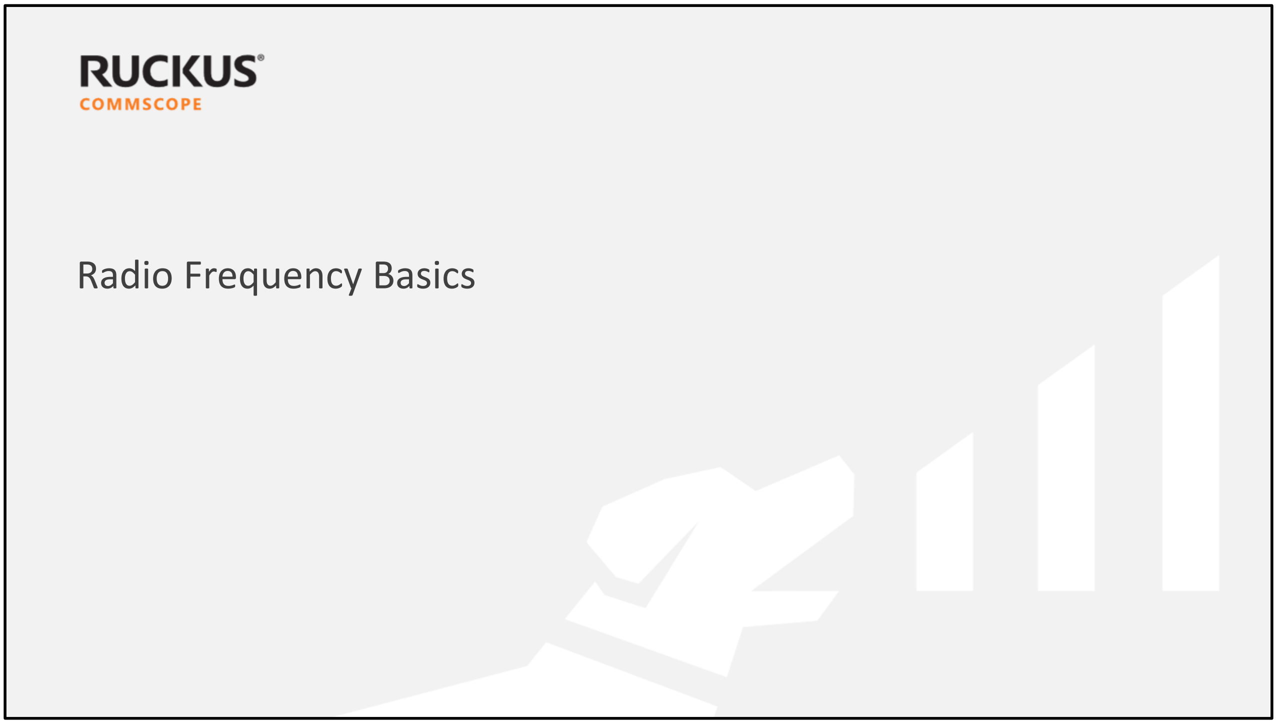


The Wi-Fi Alliance

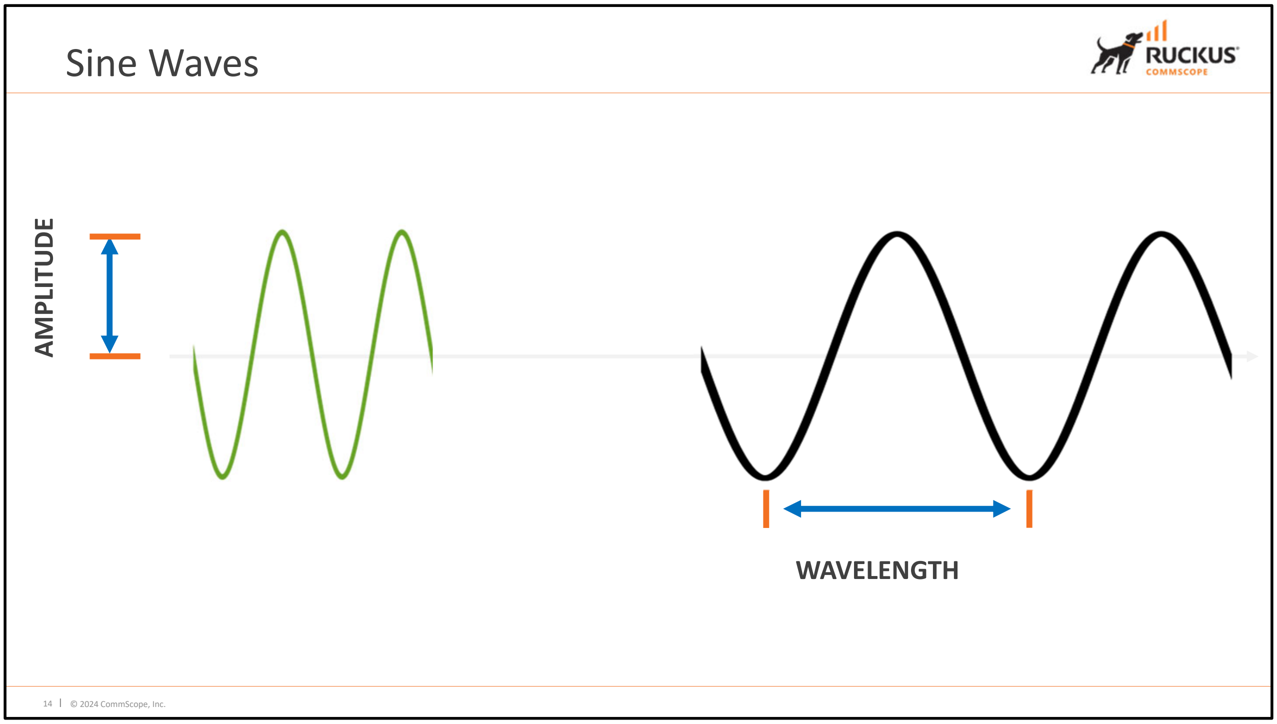
- Certifies interoperability across wireless vendors
- Provides a forum for collaboration
- Promotes growth within the Wi-Fi industry
- Builds support for industry-agreed upon implementation of the standard
- Delivers product connectivity through testing and certification

The Wi-Fi alliance was formed to help foster interoperability and to aid in the growth of wireless device use. In fact, Wi-Fi is a marketing term used to describe 802.11 wireless communications. Unlike Hi-Fi, Wi-Fi is not an abbreviation for anything.

What are some of the things the Wi-Fi Alliance does for the industry? It Certifies interoperability across wireless vendors. Provides an effective forum for collaboration, Helps the industry grow, supports industry agreed upon implementation of the standard and delivers product connectivity through testing and certification. That is what is behind the Wi-Fi certified logo you see on the packaging on many wireless devices.



Radio Frequency Basics



Sine Waves

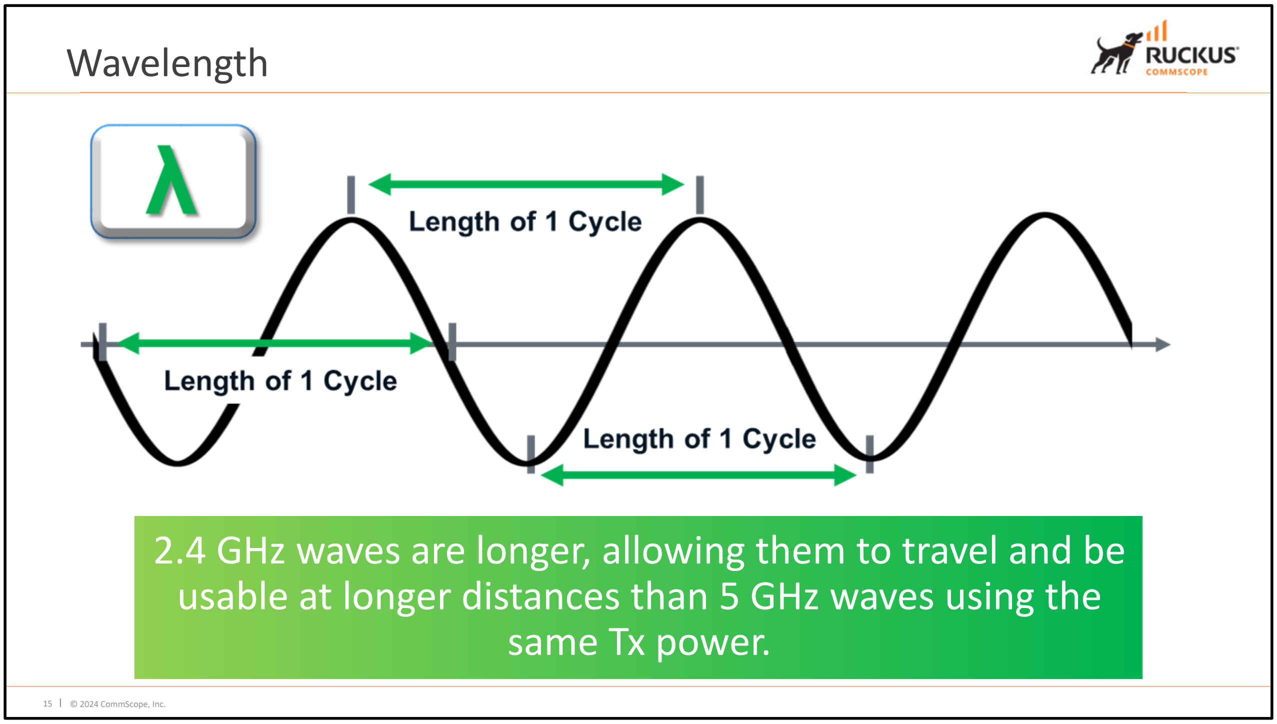
A sine wave is a curve that describes a smooth periodic oscillation which represent energy entirely concentrated at a single frequency such as with wireless signals.
As shown on the slide, sine waves have a few basic properties.

Amplitude is the distance from zero to the maximum positive and negative alternation, which are the same. The Period of the wave is measured by how long it takes to complete one entire cycle.

Wavelength is the distance traveled by the sine wave during the period and is Indicated by the Greek lambda symbol λ. It is the distance between one value to the same value on the next cycle.

The **frequency** is the number of cycles per unit time. With wireless signals, the frequency is usually measured in cycles per second or Hertz (Hz). One million cycles per second is represented in megahertz (MHz). While one billion cycles per second are represented by gigahertz (GHz).

Transmission on a medium can be changed or modulated, allowing it to carry information. Likewise, demodulation can be used to recover that information. As it applies to radio frequency (RF) communications, modulation involves impressing the characteristics of one waveform onto a second waveform by varying the amplitude, frequency, phase, or other characteristic of the second, or carrier, waveform. AM radio uses amplitude modulation, varying the power to transmit information, while FM radio uses frequency modulation, varying the frequency to transmit information.



Wavelength

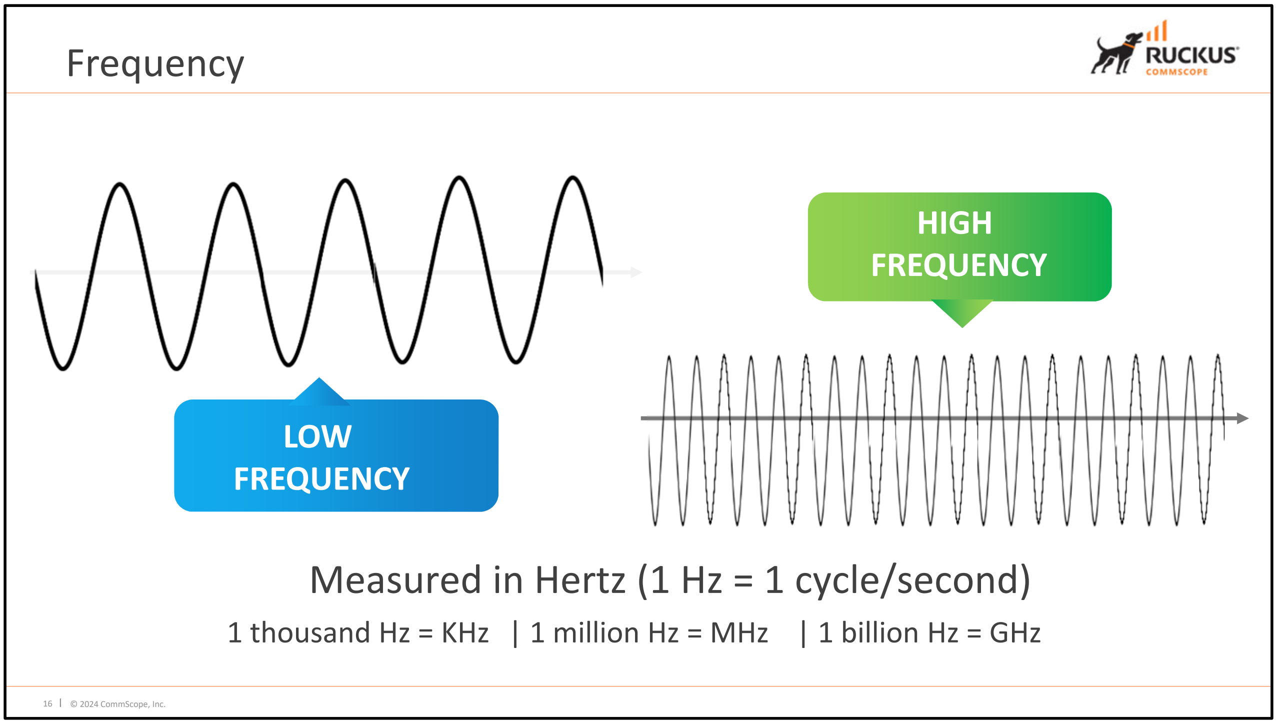
2.4 GHz waves are longer, allowing them to travel and be usable at longer distances than 5 GHz waves using the same Tx power.

15 | © 2024 CommScope, Inc.

As discussed, Wavelength is the distance traversed during one oscillation, or cycle, of the sine wave. This can be measured at any point in the waveform as long it is measured at the same point on each oscillation. The λ (lambda) symbol is used to represent wavelength.

Wavelengths of the RF signals used in wireless networks can be physically measured in centimeters. On average a 2.4 GHz wavelength is 12.5 cm, or 4.9 inches, while a 5 GHz wavelength averages to 6 cm, or 2.3 inches.

2.4 GHz waves are physically longer, travel further and are able to be used at longer distances than 5 GHz when using the same TX power.

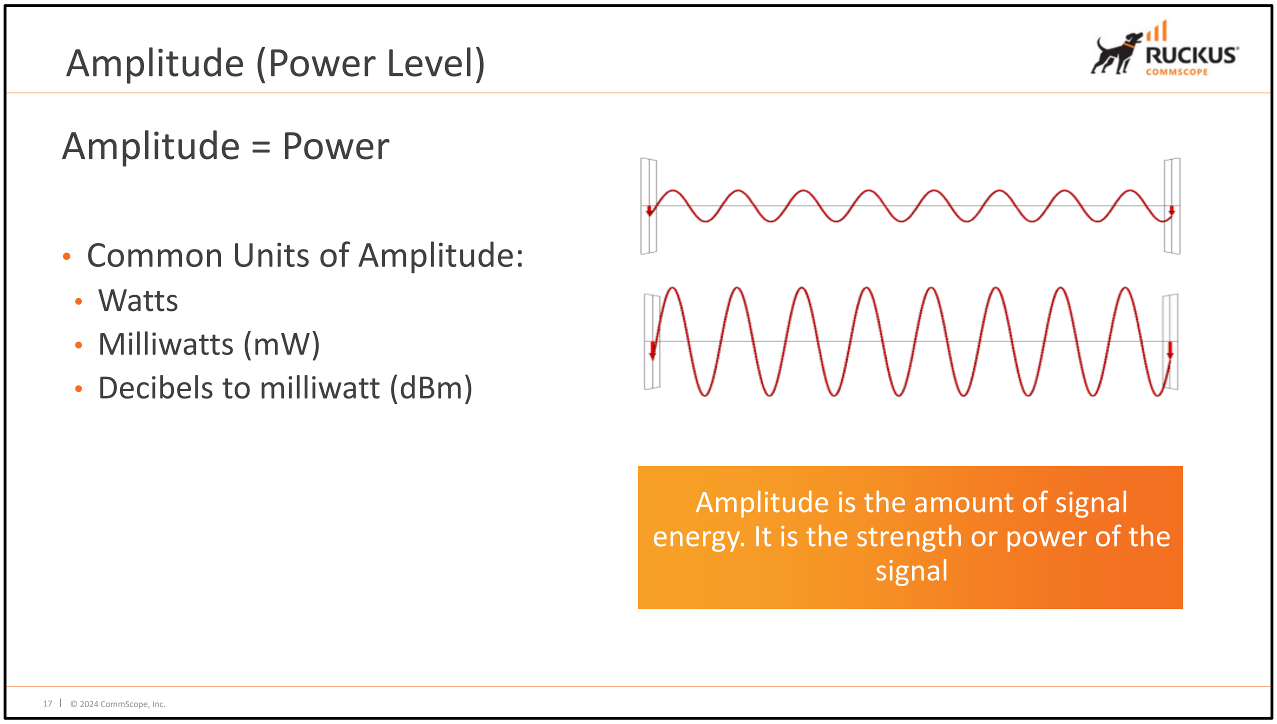


Frequency

Measured in Hertz (1 Hz = 1 cycle/second)

1 thousand Hz = KHz | 1 million Hz = MHz | 1 billion Hz = GHz

Frequency is the number of times that a wave oscillates within a period of time. For wireless communications, frequency is measured in one second intervals. One oscillation in a second is known as a Hertz (Hz). 2.4 GHz signals oscillate around 2.4 to 2.5 billion times per second and 5 GHz signals oscillate around 5 to 6 billion times per second.



Amplitude (Power Level)

Amplitude = Power

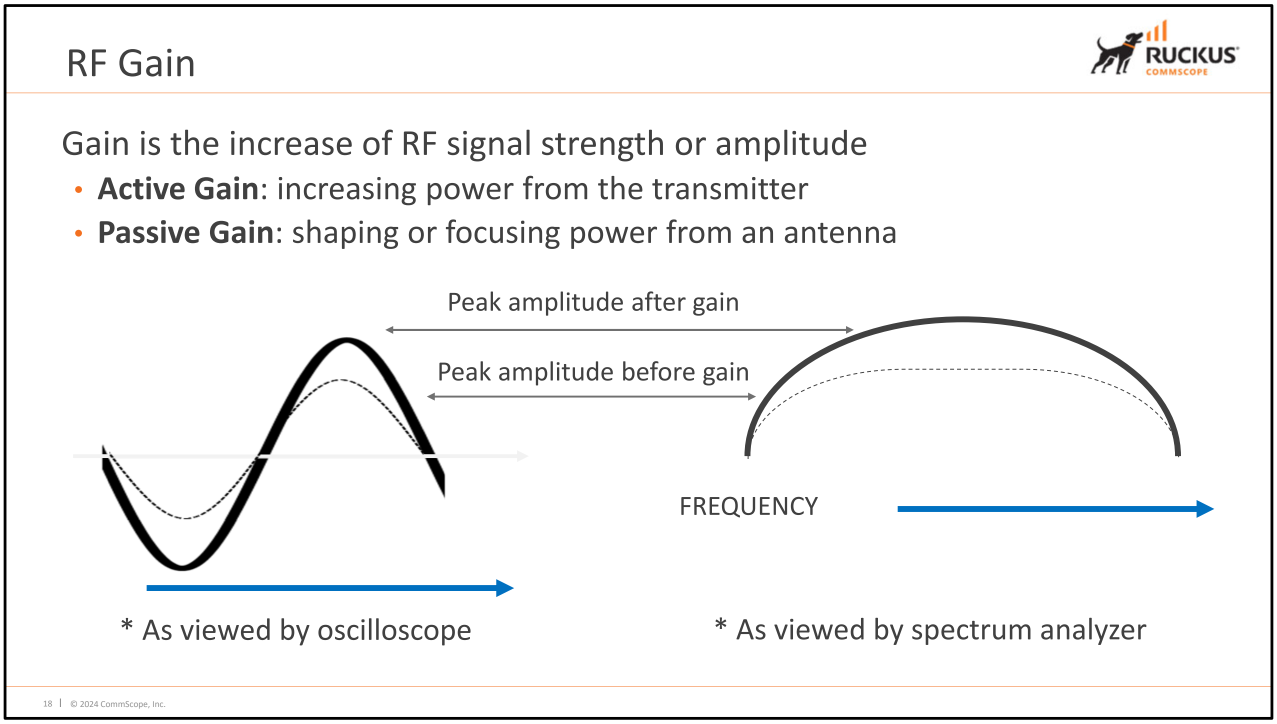
- Common Units of Amplitude:
  - Watts
  - Milliwatts (mW)
  - Decibels to milliwatt (dBm)

Amplitude is the amount of signal energy. It is the strength or power of the signal

17 | © 2024 CommScope, Inc.

Amplitude means power, in RF discussions. Amplitude is the height, strength, or power of a wave. The higher the output power the higher the amplitude of the wave.

Amplitude can be controlled by turning the signal on and off or by varying the strength of a signals. Some common units of measure for amplitude or RF signal power are Watts, Milliwatts and Decibels referenced to 1 mW. Absolute power values are expressed in Watts, Milliwatts and Decibels measured. When you see dBm it means decibels measured and can be used as a power level. Decibels are a measure of change. In Wi-Fi we reference 0 dBm to 1 mW as our starting point.



RF Gain

Gain is the increase of RF signal strength or amplitude

- **Active Gain**: increasing power from the transmitter
- **Passive Gain**: shaping or focusing power from an antenna

* As viewed by oscilloscope

* As viewed by spectrum analyzer

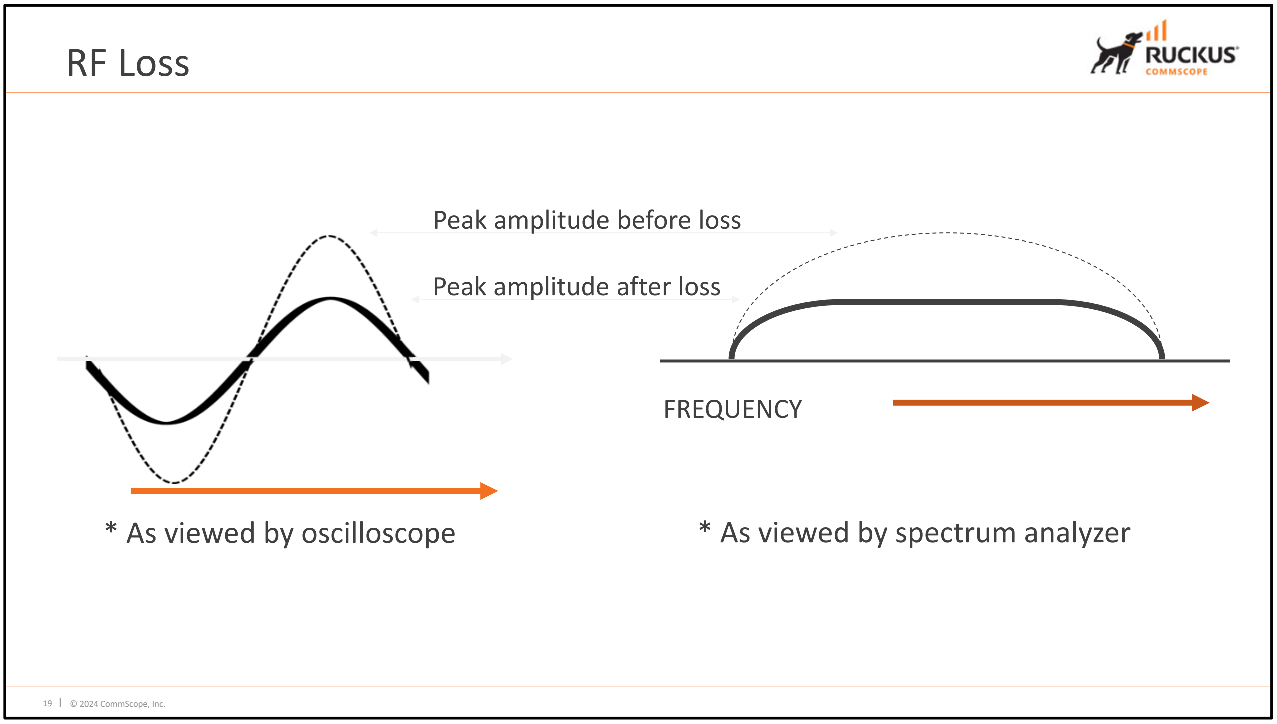
18 |

An RF signal's amplitude can be increased by the use of external devices such as amplifiers and antennas. *Gain*, or *amplification*, is an increase of signal strength and can be achieved with active gain or passive gain.

Active gain is accomplished by placing an amplifier on the cable that connects the radio to the antenna. Amplifiers are typically bidirectional and increase the signal level of the primary signal and the noise heard from the source in each direction. It is important to note that active amplifiers not only increase the signal, but they also increases any noise present in it. Active gain devices require the use of an external power source.

Passive gain is accomplished by focusing the RF signal by using a directional antenna. Antennas are passive amplifiers that do not require an external power source. Instead, an antenna focuses its passive power in one geographical direction, intensifying its signal.

Gain can be viewed with either an oscilloscope or spectrum analyzer. This illustration shows how gain would appear with an oscilloscope or a spectrum analyzer.



RF Loss

* As viewed by oscilloscope

* As viewed by spectrum analyzer

19 | © 2024 CommScope, Inc.

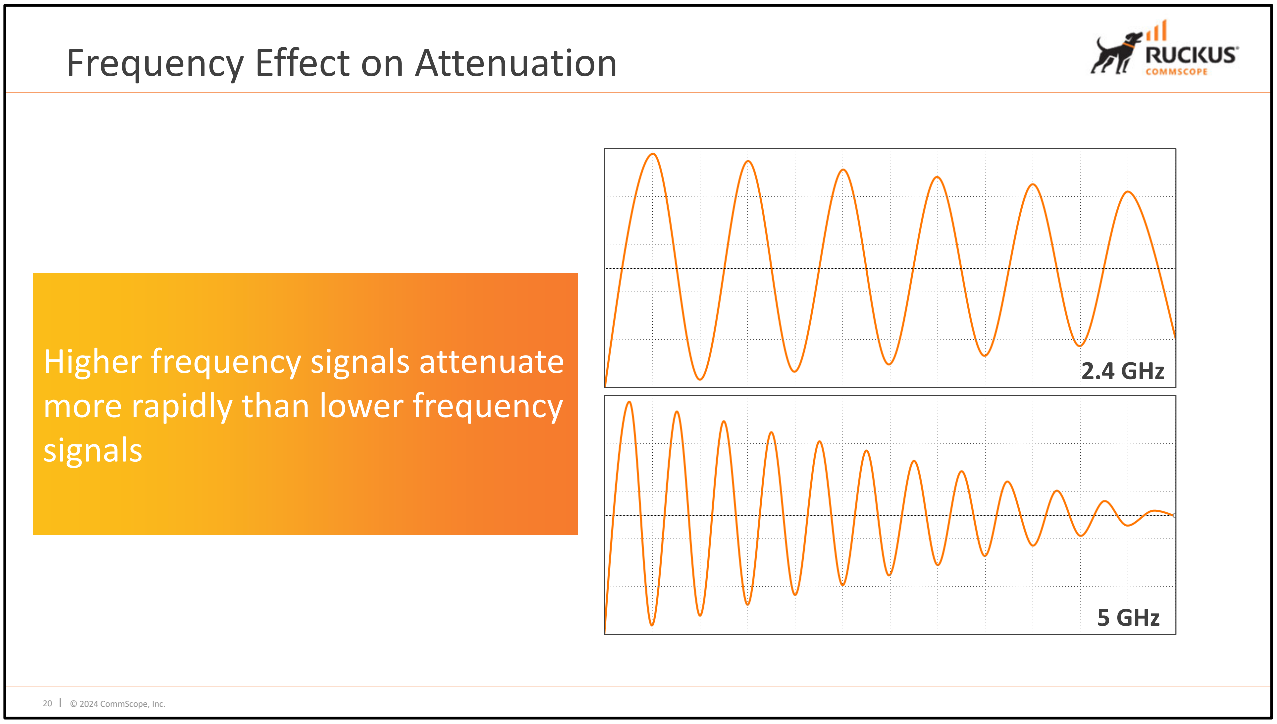
Loss is a decrease in signal strength and can be caused by a number of things such as:

Diffusion – which occurs naturally as the wave travels away from the signal source

Attenuation – which occurs as the RF signal reacts to its physical environment. These can be in the form of Reflection, Refraction, Diffraction, Scattering and Absorption.

Interference – the weakening of the RF signal as it exists in a noisy, unwanted signals in the same radio frequency spectrum as the Wi-Fi network.

Attenuators – component designed to introduce loss in the amplitude of a signal. This is the opposite of the work done by an amplifier. These are typically used to ensure compliance with regulatory domain limits and to restrict the coverage.

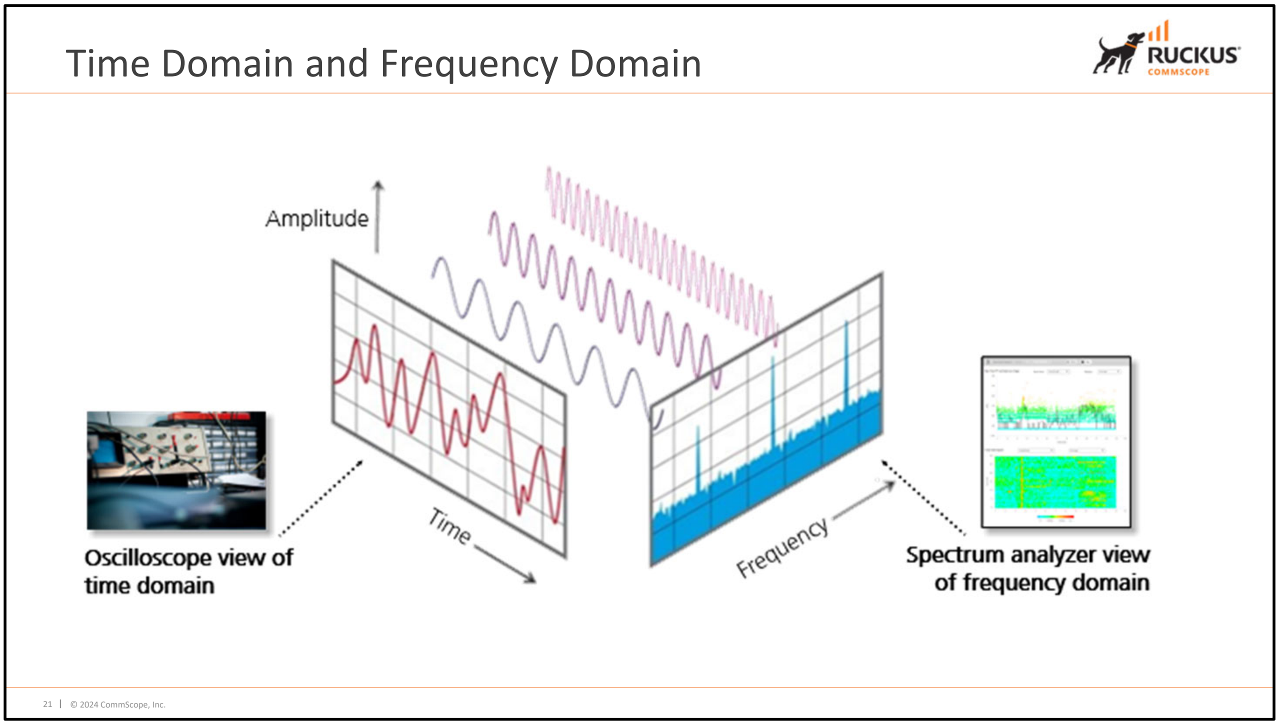


Frequency Effect on Attenuation

Higher frequency signals attenuate more rapidly than lower frequency signals

20 | © 2024 CommScope, Inc.

Lower frequencies have longer wavelengths than higher frequencies. Therefore, a higher frequency signal attenuates faster than a lower frequency signal. Lower frequency signals are also able to penetrate obstacles better than higher frequency signals for the same reason.



Time Domain and Frequency Domain

Amplitude
Time
Frequency
Oscilloscope view of time domain
Spectrum analyzer view of frequency domain

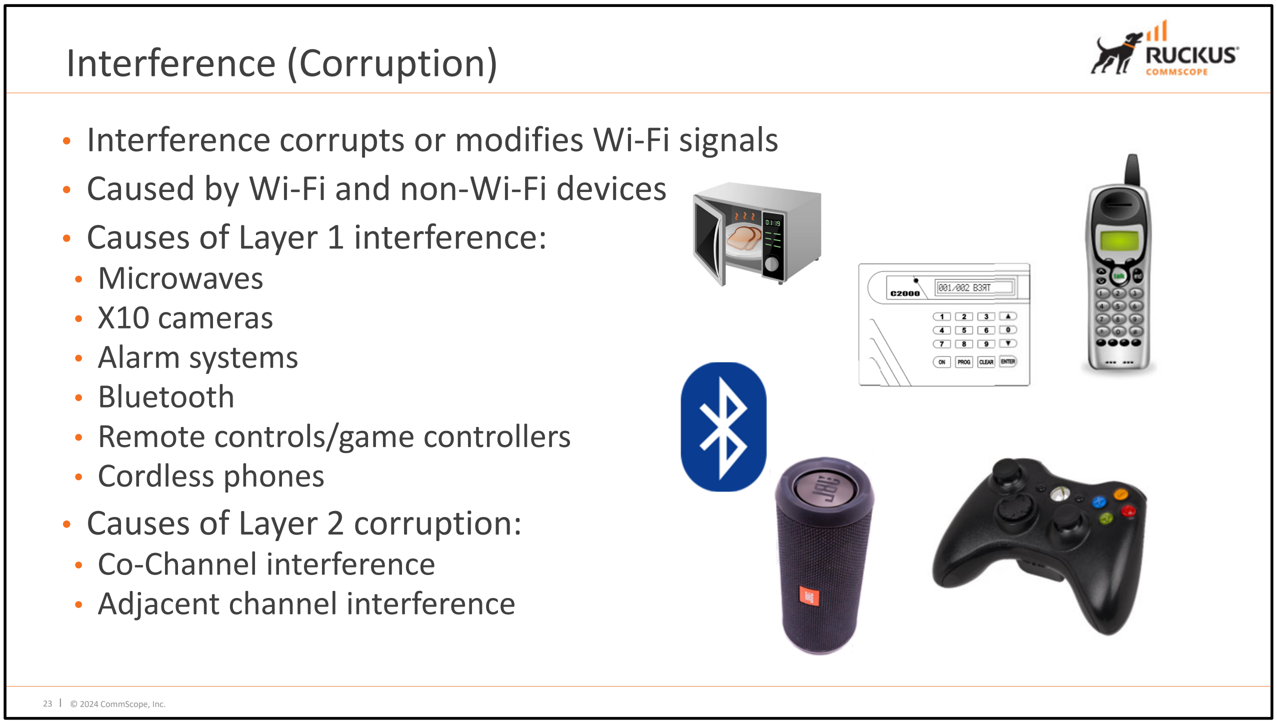
21 | © 2024 CommScope, Inc.

Tools, such as oscilloscopes, are used to measure Time Domain and how a signal amplitude changes over time. They are rarely used by engineers or administrators during wireless LAN surveys or implementations, but they are used by design engineers during hardware development and testing.

Unlike the time domain, engineers and administrators frequently use tools to visualize RF in the frequency domain. The most common tool is a spectrum analyzer. There are many ways a spectrum analyzer can be used to present data, and it is important to know that when using a spectrum analyzer you are measuring the frequency domain

In Spectrum Capture, you can select the radio frequency values (2.4GHz or 5GHz) for the analysis from the Radio option. You can select and view the spectrum analysis trends in these graphs:

- **Spectrum Usage**: This chart uses a color-based view to show collections of data points over time. As more data samples are measured at a specific frequency and amplitude coordinate, the color shown at that coordinate will change.
- **Real-Time Fast Fourier Transform, or FFT** : This chart is a second-by-second (2sec) update of measured data across the band. If you view by Amplitude (signal strength), then the chart displays both average and maximum amplitudes of energy measured across the band for that sample period. If you view by Utilization (duty cycle), then the chart displays the percentage (%) of time at which the frequency is utilized at an amplitude above N.



Interference (Corruption)

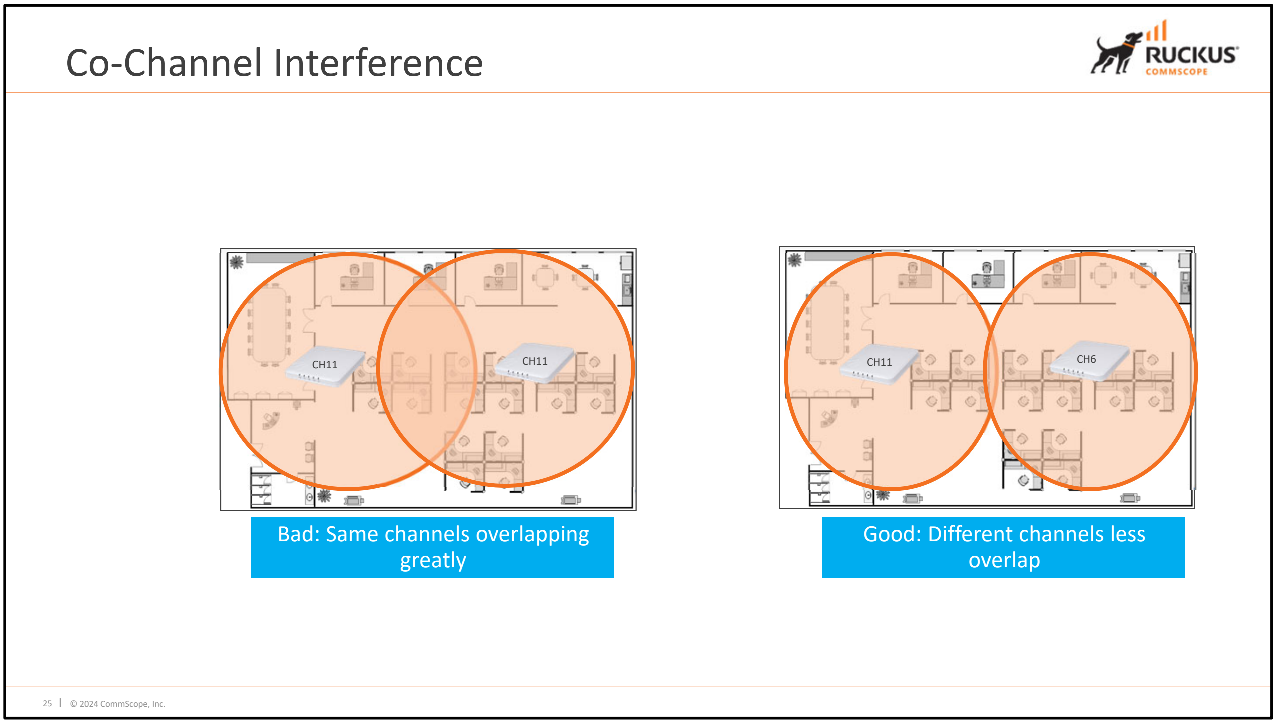
- Interference corrupts or modifies Wi-Fi signals
- Caused by Wi-Fi and non-Wi-Fi devices
- Causes of Layer 1 interference:
  - Microwaves
  - X10 cameras
  - Alarm systems
  - Bluetooth
  - Remote controls/game controllers
  - Cordless phones
- Causes of Layer 2 corruption:
  - Co-Channel interference
  - Adjacent channel interference

23 | © 2024 CommScope, Inc.

Interference in Wi-Fi is anything that corrupts or modifies the original signal. It is usually from sources like non-Wi-Fi transmitters, Multipath fading, co-channel and adjacent-channel Wi-Fi devices.

Interference may occur between waves of identical, similar, or harmonically related frequencies as well as multipath components. Interference occurs at both Layer One and Layer Two.

Layer One interference comes from many common non-802.11 sources such as microwaves, X10 cameras, alarm systems, Bluetooth, remote control devices, cordless phones and even weather radar. This type of interference disrupts the physical carrier sense of Wi-Fi communications, effectively disrupting the medium itself. 802.11 devices will detect this, but not as a transmission from another device with which to contend for the media. Therefore, they will attempt to transmit, and their transmissions will most likely collide with the noise. This causes the intended receiver to never receive the signal, which will not generate an acknowledgement back to the sender. With no acknowledgement from the receiver the original sender then retransmits again and again, up to 32 times. A high retransmission rate is an indication of physical layer interference.



Co-Channel Interference

Bad: Same channels overlapping greatly

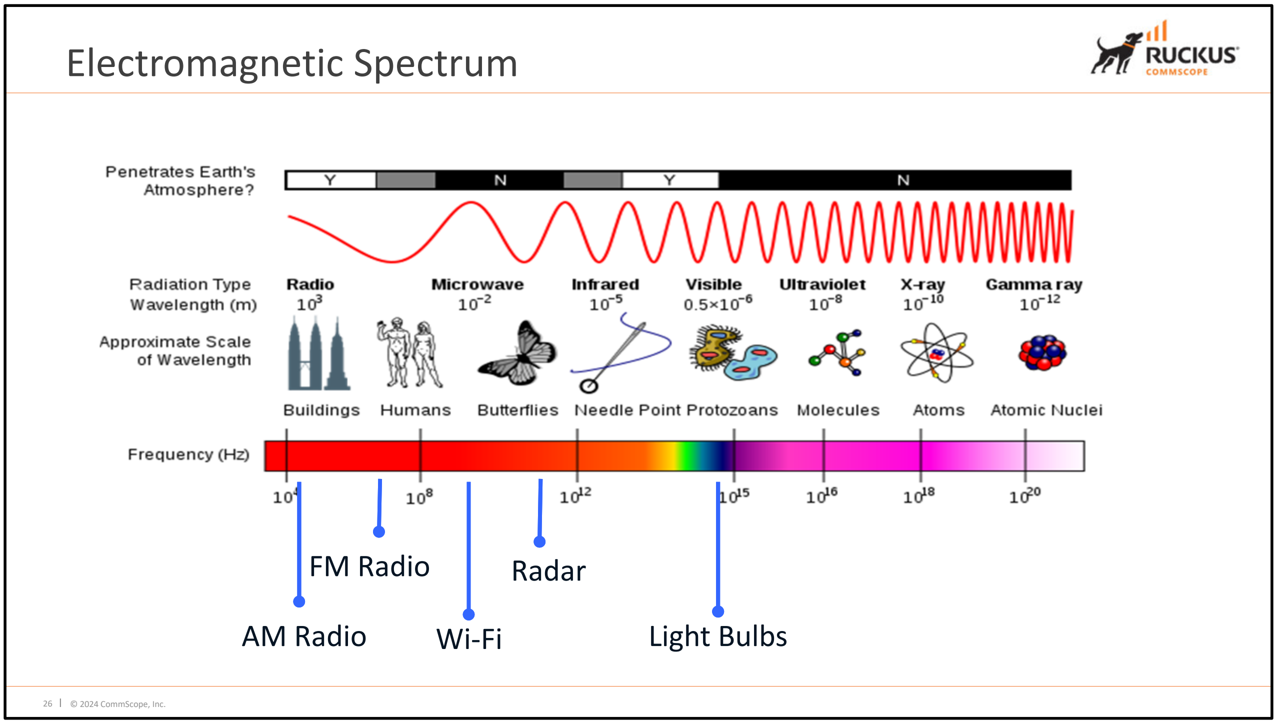
Good: Different channels less overlap

25 | © 2024 CommScope, Inc.

Sometimes RF signals can be too strong and cause issues with co-channel interference. Co-channel interference, or CCI as it's commonly called, is the number one cause of unnecessary airtime consumption. If your airtime is being consumed there is unnecessary contention with the medium and poor performance will result.

Within the 2.4 GHz band some amount of CCI is unavoidable. You can lessen the impact however with a proper channel plan using non-overlapping channels 1, 6, and 11. You can also adjust the transmit power of the AP downward to limit the size of the RF cells, reducing overlap.

In the 5 GHz band CCI can be almost completely avoided with a good channel plan, especially if you are able to use Dynamic Frequency Selection (DFS) channels in your region. You can also adjust 5 GHz radios down in power to help reduce CCI.



Electromagnetic Spectrum

FM Radio

Radar

AM Radio

Wi-Fi

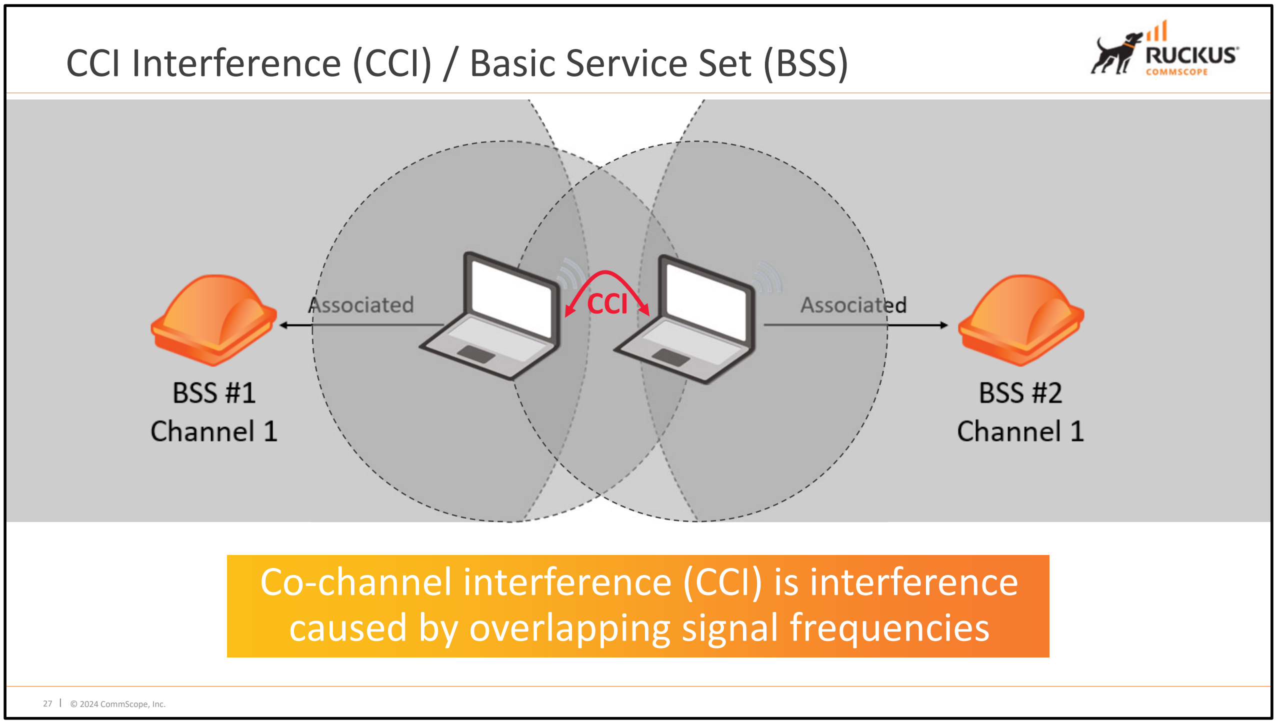
Light Bulbs

26 | © 2024 CommScope, Inc.

You are probably familiar with several technologies which use radio frequencies. These technologies include many common things such as:

AM radio, FM radio, Wi-Fi, Radar and, Light bulbs.

The complete range of all electromagnetic radiation is called the electromagnetic spectrum. In Wi-Fi, it is often simply called spectrum without the reference to electromagnetics.



CCI Interference (CCI) / Basic Service Set (BSS)

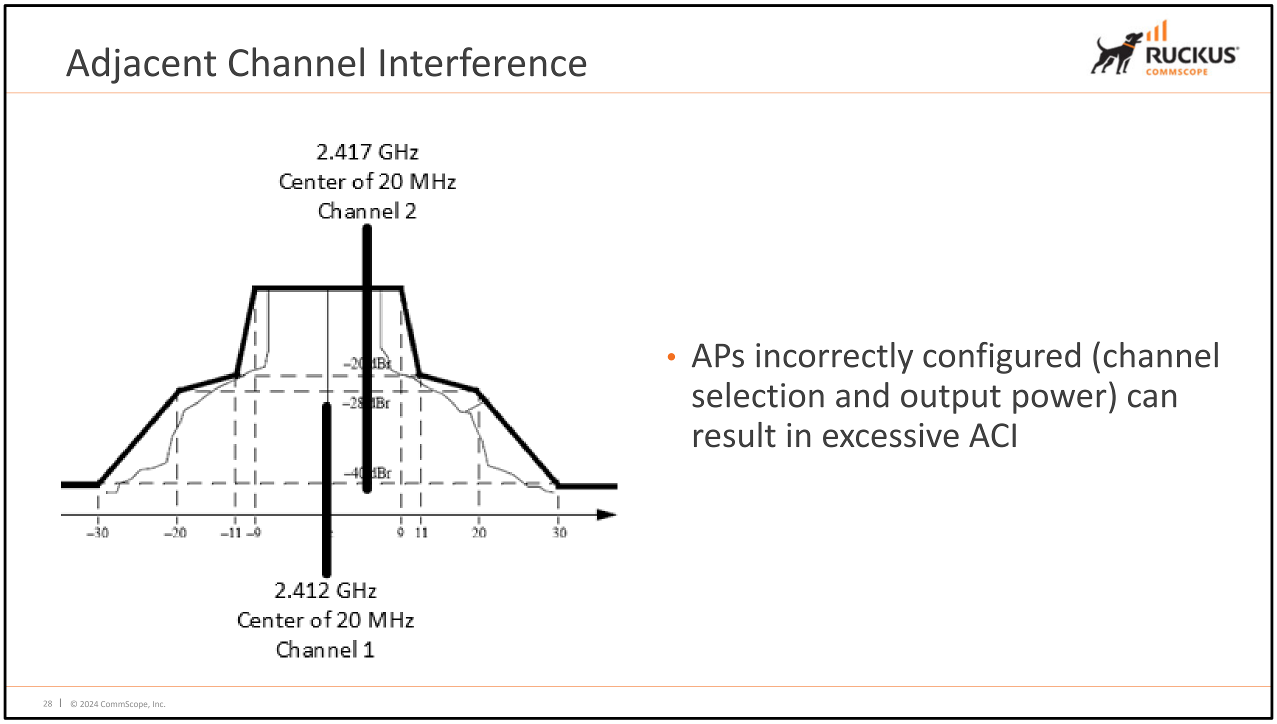
Co-channel interference (CCI) is interference caused by overlapping signal frequencies

27 | © 2024 CommScope, Inc.

Co-channel interference often occurs whenever there are two Basic Service Sets (BSS) in close enough proximity on the same channel or may be caused by any carrier centered on the same frequency. With the scenario of two BSS, this can be APs that have overlapping coverage or clients on the edge of the two overlapping BSS. In the example here the client on the left is associated with the AP in BSS #1. The client on the right is associated with the AP in BSS #2. The clients can cause CCI with each other (if they are in range of each other) and potentially cause CCI on the AP to which they are not associated.

CCI occurs within a channel and not within a BSS because STAs (both APs and clients) must acknowledge frames from other BSSs in the same channel if they are received with a significant signal level. Co-Channel Interference is nothing more than an increase in the number of devices within contention domain. It is not the same as interference from other non 802.11 sources such as a microwave or radar but will impact your communications. The largest source of CCI is client stations on the edge of overlapping cells using the same channel.

To reduce this, you will need to implement a proper channel plan taking into account 3D space, which may impact things above or below you. CCI occurs more often in the 2.4 GHz space than in the 5 GHz space due to the more limited number of non-overlapping channels available for use in 2.4 GHz. You will see a three-channel plan of 1, 6 and 11 used quite often. The key is to reduce the number of times the same channels are used on overlapping cells as much as possible. Some people use will disable 2.4 GHz on some radios throughout the environment to help accomplish this.



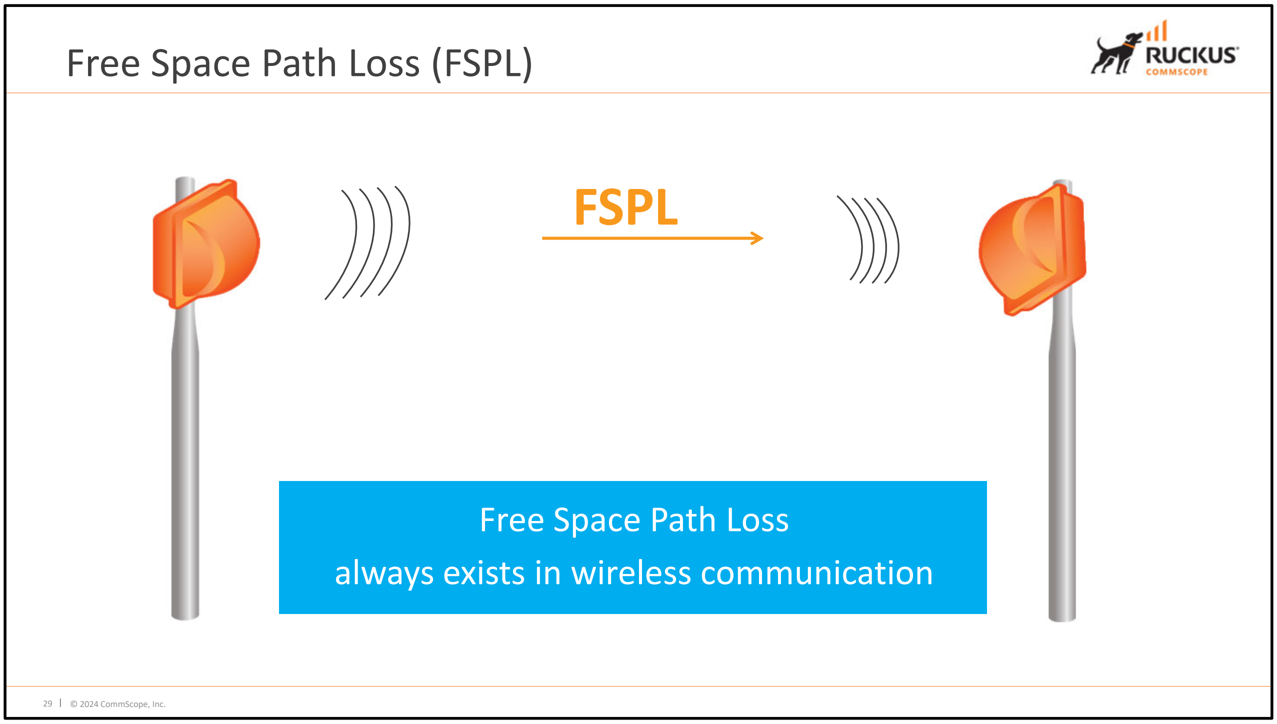
Adjacent Channel Interference

- APs incorrectly configured (channel selection and output power) can result in excessive ACI

Adjacent Channel Interference (ACI) is caused when channels overlap by design, like 2.4 GHz channels, or when non-overlapping channels cause side-lobe interference, like 5 GHz channels.

2.4 GHz channels are 5 MHz apart and 20 or 22 MHz wide, therefore it is a certainty that adjacent channels will overlap and cause interference. In the image shown we have an overlay of the center frequency for channel 1 and channel 2. When adjacent channels overlap they cause ACI, which can manifest as corrupt frames or simply prevent communications due to energy detected in 2.4 GHz.

In 2.4 GHz, ACI can be prevented within your controlled networks by using channels 1, 6 and 11. However, in areas where neighbor WLANs can be seen, if they are using channels 2-5, 7-10 or 11-14, ACI may exist regardless of your network settings. This can be mitigated by carefully planning channel selections nearest to these neighbor WLANs.



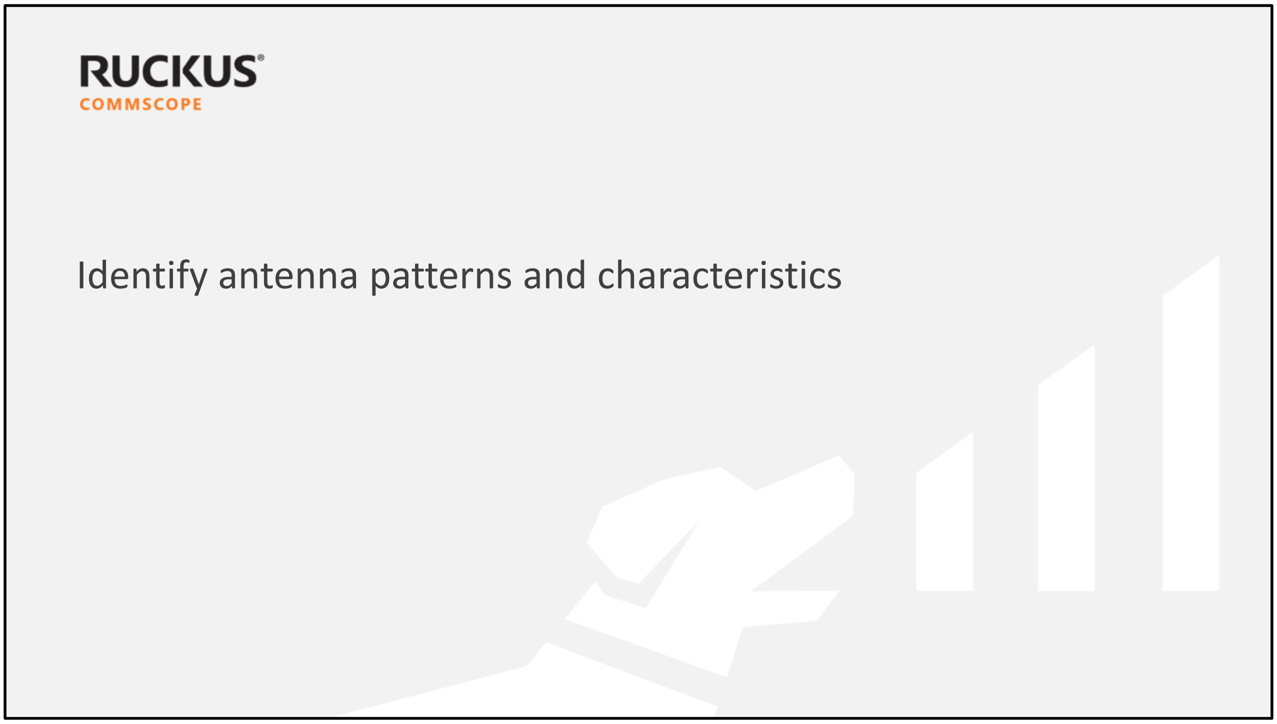
Free Space Path Loss (FSPL)

Free Space Path Loss always exists in wireless communication

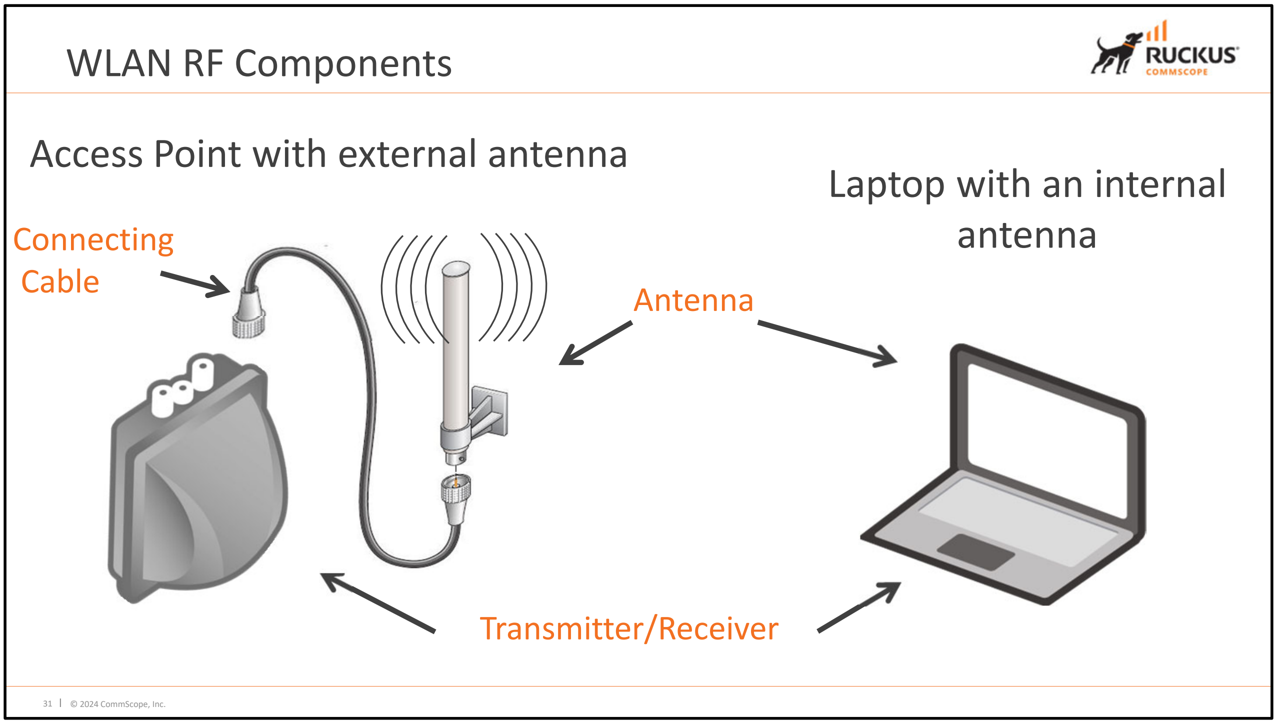
29 | © 2024 CommScope, Inc.

In addition to these forms of interference, you must consider signal loss in free space. Free Space Path Loss is the loss in signal strength of a wave that would result from a line-of-sight path through free space, with no obstacles nearby to cause reflection or diffraction; similar to the loss in bounded networks as the signal travels through the cables. As a signal moves away from the source, it naturally decreases in power due to the broadening of the wave.

Free Space Path Loss always exists in wireless communication. The degree to which it impacts the communications varies with the power, frequency used and distance of the transmission, both indoors and outdoors alike.



Identify antenna patterns and characteristics



WLAN RF Components

Access Point with external antenna

Laptop with an internal antenna

Connecting Cable

Antenna

Transmitter/Receiver

31 | © 2024 CommScope, Inc.

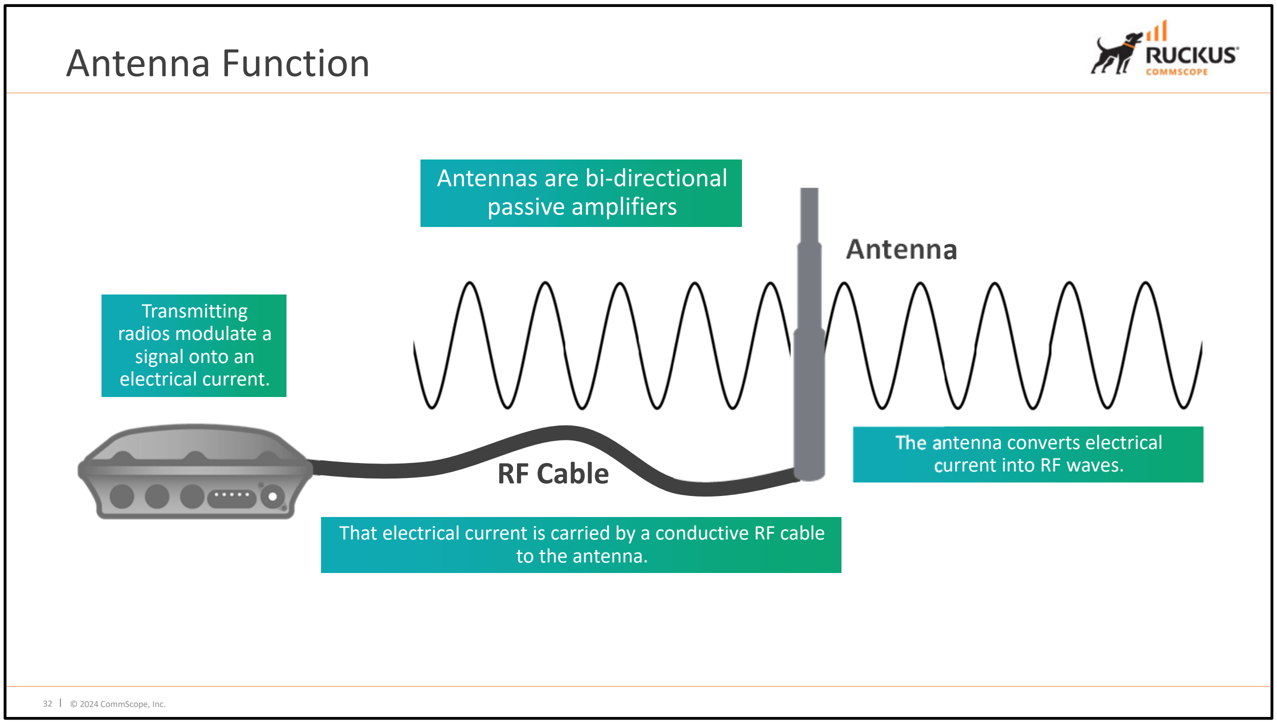
Access Points contain radios that are RF transceivers which generate an RF signal. When using an external antenna the RF signal travels along the connected coaxial cable connecting the antenna to the AP. However, not all wireless devices have antennas that you are able to visibly see. Most APs and laptops have internal wireless antennas.

The radio in the device receiving the signal is known as the RF receiver. Since the radios used in Wi-Fi are both transmitters and receivers they referred to as transceivers. In laptops the antennas are usually integrated into bezel around the screen. The transceiver used in modern laptops is integrated into the system board of the laptop. Older laptops may have wireless network cards that connect via USB.

The transmitter receives data for transmission and converts it to an oscillating signal which is then modulated with the data to be sent wirelessly. When the wireless signal includes the data for transmission it is referred to as the “carrier signal”. The power level of the transmitter’s amplifier determines the amplitude of the wave and once placed into the air via the antenna becomes an RF Signal

The steps involved in wireless transmission are:

1. The transmitter receives the data to be transmitted.
2. It converts the AC signal using a modulation technique to encode the data into the AC signal.
3. Once modulated to include data it is referred to as a carrier signal meaning that it contains the data being transmitted.
4. Carrier signal is sent to the antenna for propagation.
5. The signal is sent out of the antenna at a configured amplitude or power level based upon the properties of the antenna.



Antenna Function

Antennas are bi-directional passive amplifiers

Transmitting radios modulate a signal onto an electrical current.

The antenna converts electrical current into RF waves.

That electrical current is carried by a conductive RF cable to the antenna.

32 | © 2024 CommScope, Inc.

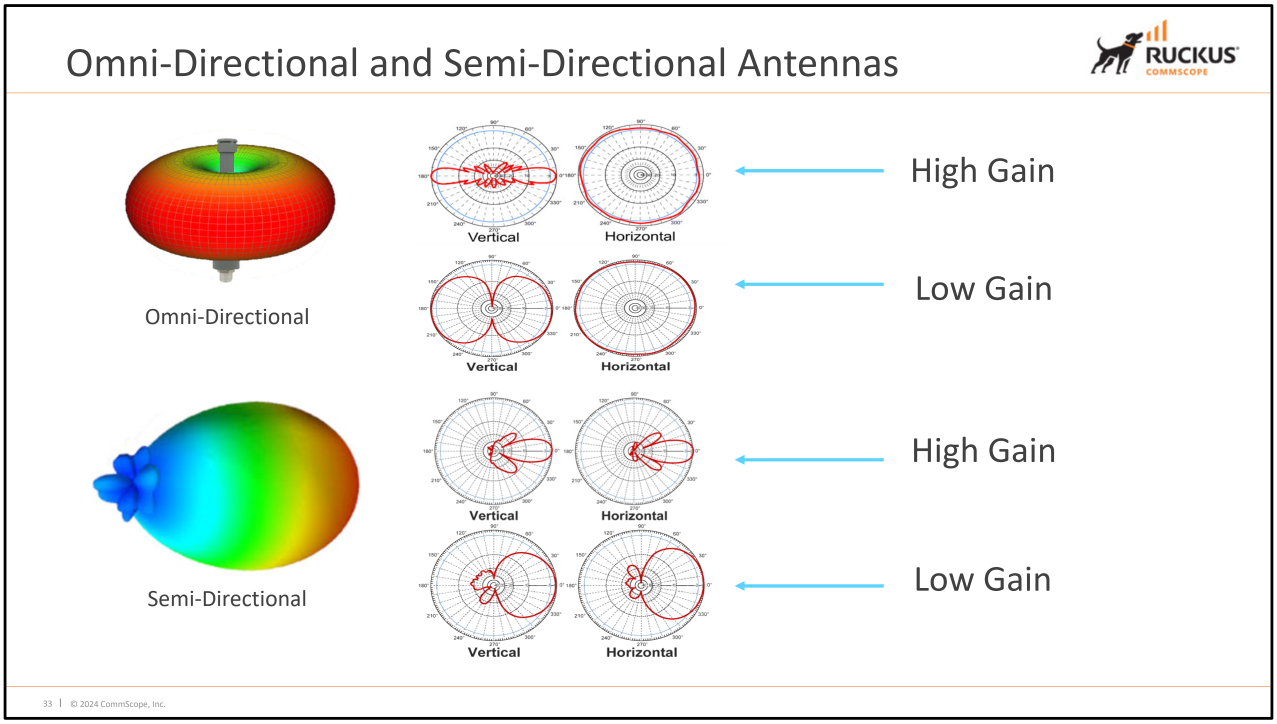
It is important to know that antennas are bi-directional passive amplifiers and are used in both transmission and reception of RF signals.

Antennas are connected to a radio transceiver via an RF cable and convert electrical current into RF waves. The wireless radio then modulates the signal onto an electric current which passes over the RF cable typically made of a copper core. The current then makes it way to the antenna which generates electromagnetic waves known as Radio Frequency waves or RF waves.

As we previously mentioned antennas both send and receive these waves (also referred to as signals when they are carrying data) and their send / receive functionality depends on which way the traffic is flowing. If transmitting the antenna will place the signal in the air and when receiving it will take it from the air and pass it over the RF cable back to the transceiver.

When a device transmits data, the antenna takes an oscillating signal from the transmitter and turns them into RF waves, directing them away from the antenna.

When the device receives data the antenna takes the RF signal out of the air, turns it back into an oscillating carrier signal and directs it back through the RF cable to the receiver



Omni-Directional and Semi-Directional Antennas

High Gain

Low Gain

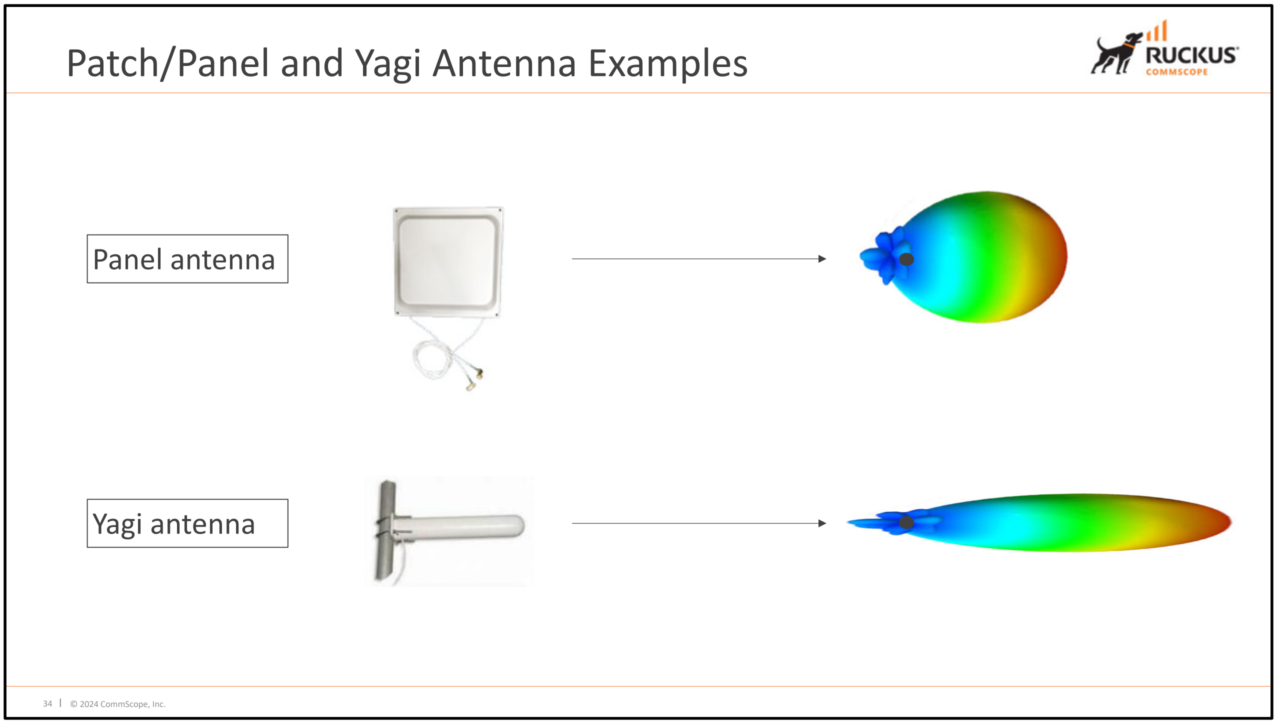
High Gain

Low Gain

33 | © 2024 CommScope, Inc.

Omni-Directional antennas are only Omni-Directional in name. The small, rubber dipole antenna, is an example of this kind of antenna. It is the default antenna of most external antenna access points. A perfect omni-directional antenna would radiate RF energy like the Sun radiating light in all directions. These antennas however, do not radiate RF energy from their tips nor do they from the cable connector. Therefore, you get what is commonly referred to as a doughnut pattern. They do, however, radiate and detect RF energy in a 360 degree pattern around the antenna in their horizontal beamwidth. The vertical portion of their pattern can be larger or small based upon the gain of the antenna. A higher gain Omni has a smaller or more narrow vertical beamwidth while a lower gain Omni has a larger or wider vertical beamwidth.

Semi-Directional antennas have a more focused beam than Omni-Directional antennas. They are used to limit the coverage provided to a more limited space in one direction vs. 360 degree coverage.



Patch/Panel and Yagi Antenna Examples

Panel antenna

Yagi antenna

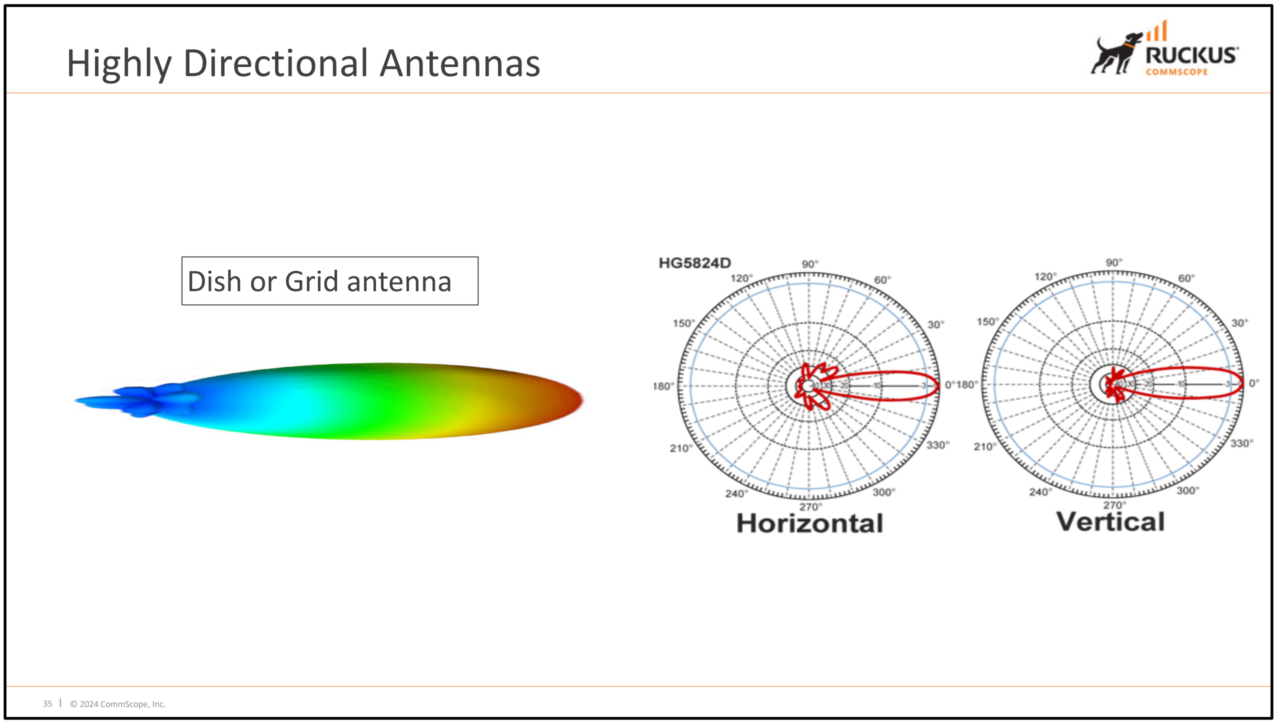
34 | © 2024 CommScope, Inc.

Semi-directional antennas focus RF waves into coverage patterns of various shapes and sizes allowing a wireless engineer to provide coverage where it is needed.

Panel antennas (also commonly referred to as a patch antennas) consist of one or more active elements mounted above a reflecting surface (ground plane). These antennas are typically used indoors to provide coverage to specific areas such as hallways, gymnasiums, etc. Where omni-directional coverage is not needed and have up to 180 degree coverage pattern. Yagi antennas are generally used outdoors and at longer distances and typically have up to a 90 degree coverage pattern.

We talk about typical use, but in the field you may see a Yagi used indoors and a panel antenna used outdoors. As long as legal guidelines are being met, both are acceptable.

In addition to focusing the RF energy only where it is needed, both of these antennas reduce the likelihood of creating or suffering from interference and aid somewhat in security by helping to contain the signals within the desired areas..



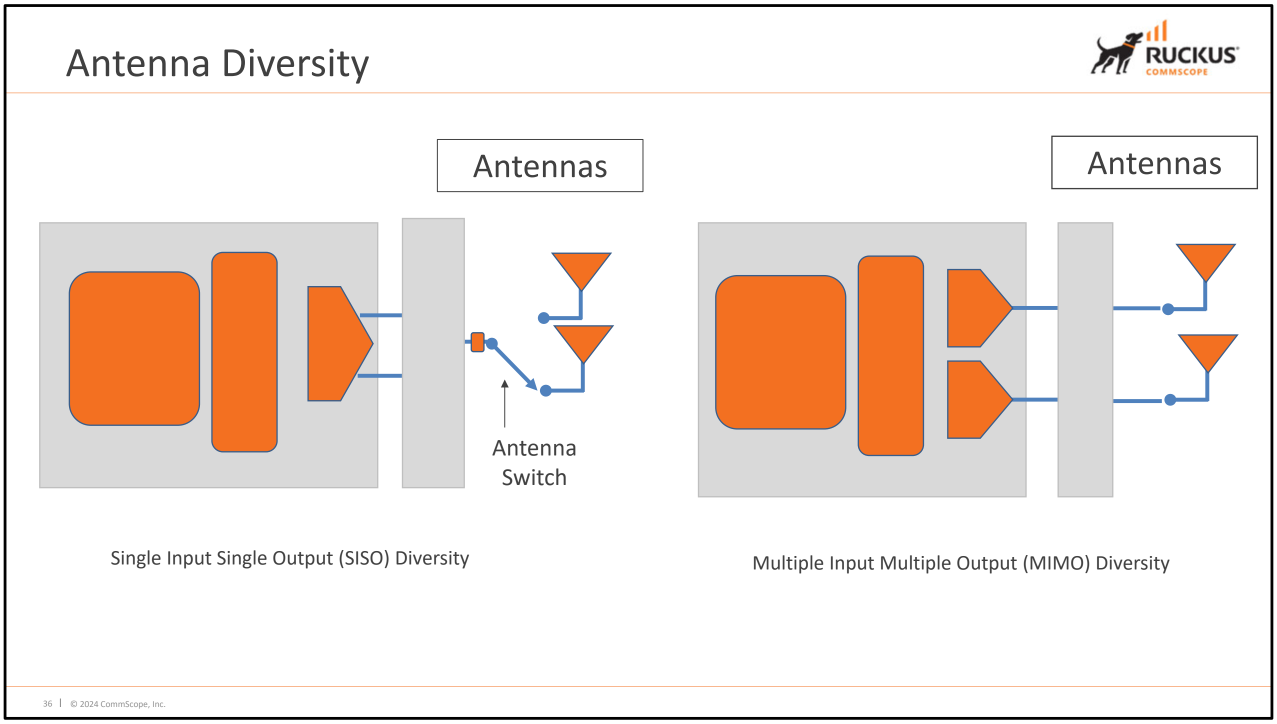
Highly Directional Antennas

RUCKUS COMMSCOPE

Dish or Grid antenna

35 | © 2024 CommScope, Inc.

Highly-Directional antennas have very narrow beamwidths and usually very high passive gain. These antennas are more often used for outdoor point-to-point bridge links than they are for area coverage; however, they may be used to target one or more remote clients in a very specific area as well. They normally have a beamwidth less than 25 degrees.



Antenna Diversity

Antennas

Antenna Switch

Single Input Single Output (SISO) Diversity

Antennas

Multiple Input Multiple Output (MIMO) Diversity

36 | © 2024 CommScope, Inc.

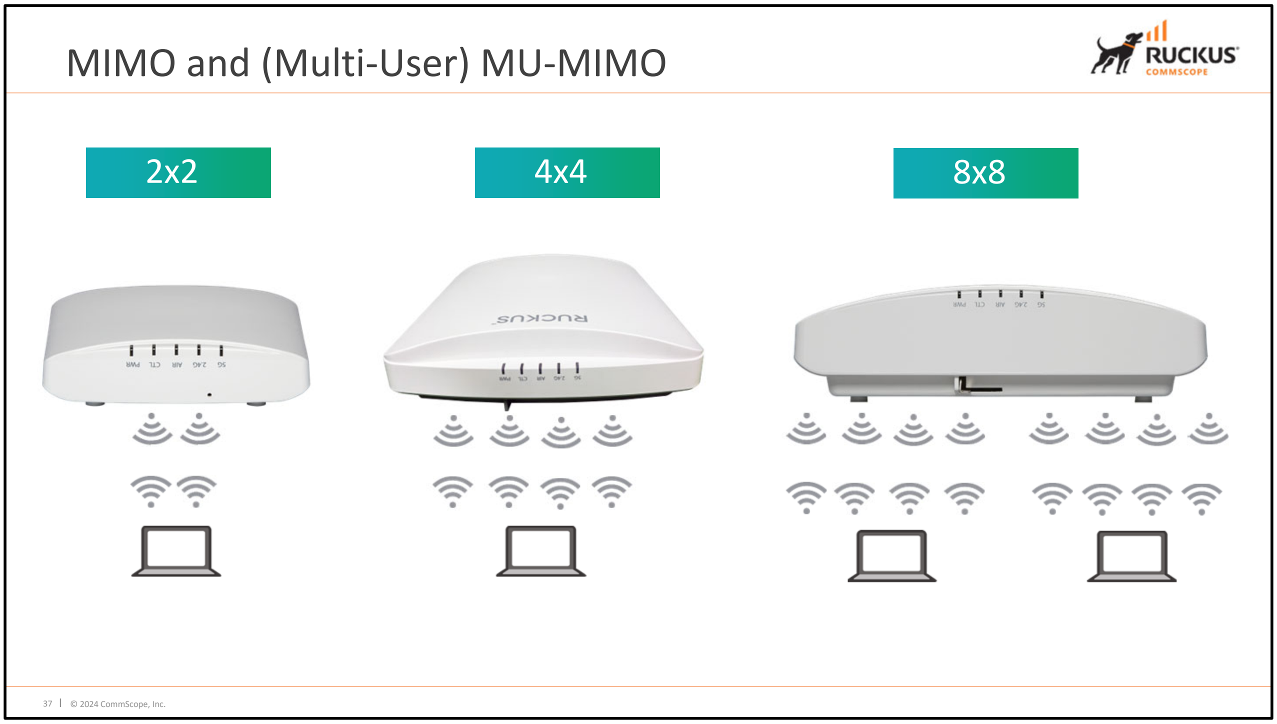
Single Input Single Output (SISO) Diversity is used to mitigate multipath in legacy systems. Simple Diversity systems maximize wireless range and coverage. They use multiple antennas to increase probability of there being a high quality signal path.

Diversity antenna systems use two or more antennas spaced multiple wavelengths apart. They use only one antenna at a time and change antennas only when a received signal is weak or has poor SNR. Simple diversity and multiple signal combining techniques can be effective even if used only on one side of a link. Diversity antenna systems are used to improve transmissions and should never be used to provide coverage in different directions.

SISO diversity was used commonly on systems supporting legacy 802.11 a/b/g transmissions. 802.11n, 802.11ac and 802.11ax require Multiple Input Multiple Output or MIMO antenna systems.

Multiple Input/Multiple Output (MIMO) diversity uses at least two antennas. These antennas are connected to the radio through separate radio chains for each antenna. The radio can send and receive using multiple antennas at the same time instead of just using antenna selection. This enhancement over simply diversity allows for greater throughput.

Whereas SISO was used to combat the downfade introduced by multipath, MIMO systems take advantage of the multipath signals received in such a way as to increase signal quality and provide better throughput. The receiving radio can include information about the reception of signals in acknowledgement frames sent to the transmitter. The transmitter uses that information to alter the next signal sent to that station. This process is part of transmit beam forming.



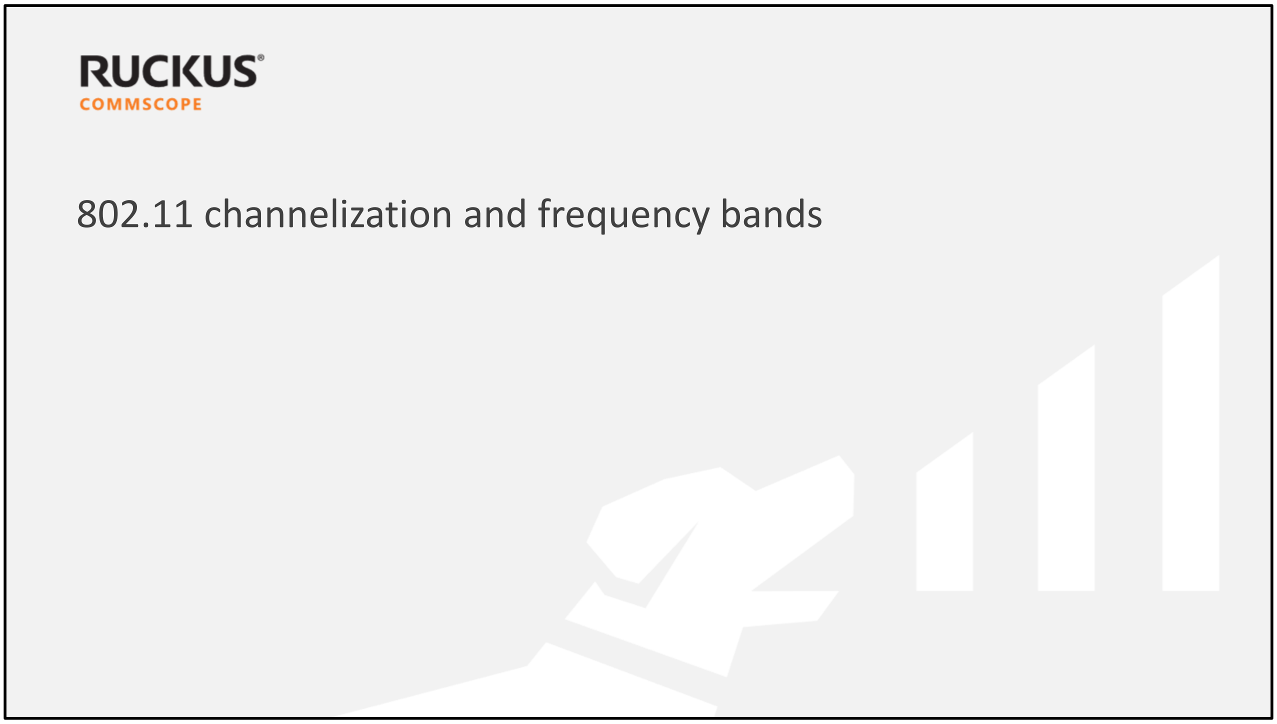
MIMO and (Multi-User) MU-MIMO

37 | © 2024 CommScope, Inc.

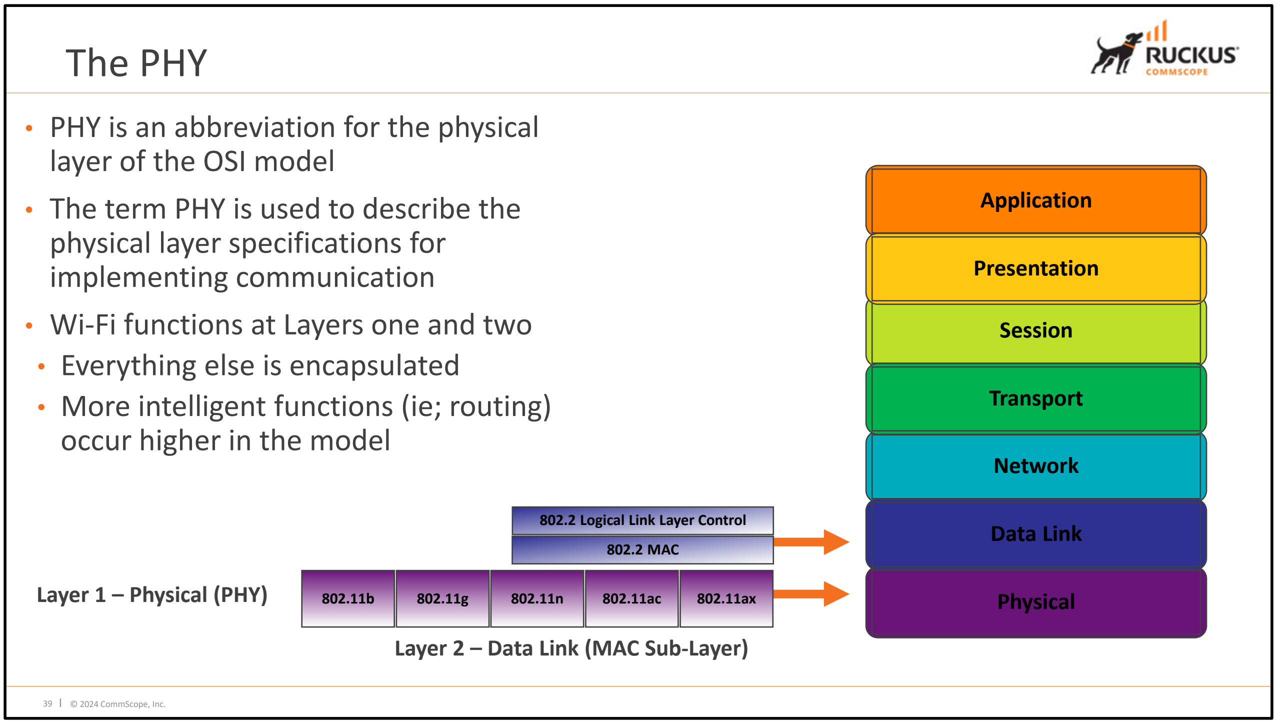
MIMO added support for multiple transmit and receive antennas per access point and was introduced as part of the 802.11n standard. MIMO allows an AP to have multiple streams of data over corresponding antennas to one (or multiple) STAs providing higher data throughput.

Multi-User MIMO or MU-MIMO allows for more than one STA to take advantage of these spatial streams at a time allowing more users to be serviced simultaneously.

When looking at AP capabilities you will commonly see the number of antennas indicated as 2x2, 4x4 or even 8x8. This gives a reference to the AP’s capabilities and outlines data rates depending on which PHYs, modulation, and coding schemes are planned to be used.



802.11 channelization and frequency bands



The PHY

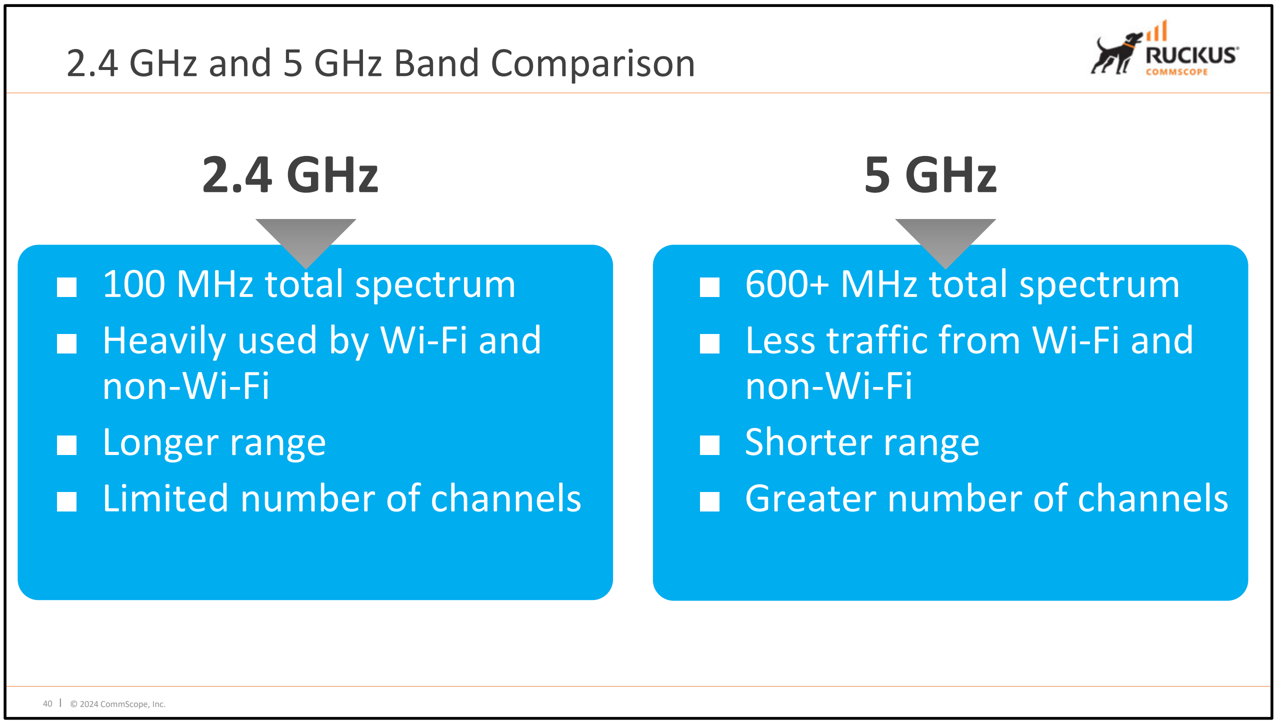
- PHY is an abbreviation for the physical layer of the OSI model
- The term PHY is used to describe the physical layer specifications for implementing communication
- Wi-Fi functions at Layers one and two
  - Everything else is encapsulated
  - More intelligent functions (ie; routing) occur higher in the model

39 | © 2024 CommScope, Inc.

PHY is an abbreviation for the physical layer of the OSI model. In Wi-Fi discussions, the term PHY is used to describe the physical layer specifications for implementing wireless communication.

Many folks refer to the PHY’s 802.11 amendment when describing how a device operates. For example, you may hear someone say that when an n device connects to an ac network it will not be able to use the top ac speeds. So, we still use the IEEE amendment names in the industry.

The various PHYs have different data rate capabilities and modulations used to achieve them. As wireless continues to evolve speeds and capabilities grow. The original specifications in 802.11 for the PHY offered us only 1 and 2 Mbps data rates using Direct Sequence Spread Spectrum (DSSS). Today 802.11ax offers up to 1.1 Gbps in single stream and beyond with devices capable of supporting multiple steams simultaneously.



2.4 GHz and 5 GHz Band Comparison

2.4 GHz

- 100 MHz total spectrum
- Heavily used by Wi-Fi and non-Wi-Fi
- Longer range
- Limited number of channels

5 GHz

- 600+ MHz total spectrum
- Less traffic from Wi-Fi and non-Wi-Fi
- Shorter range
- Greater number of channels

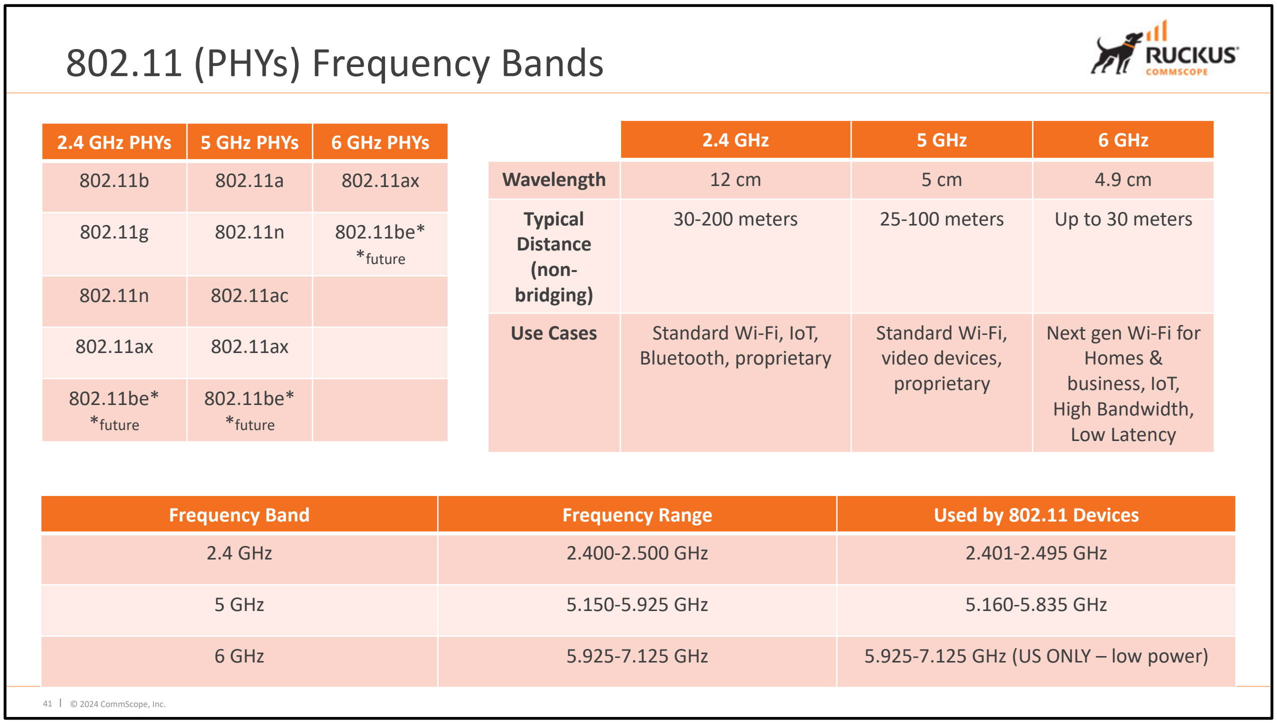
40 | © 2024 CommScope, Inc.

The 2.4 and 5 GHz bands are both unlicensed bands, available for many different applications. However, for several different reasons, 2.4 GHz has been heavily adopted and utilized by both Wi-Fi and non-Wi-Fi wireless devices. One reason for this is that lower frequencies have better range characteristics than high frequencies, so they are more useful at longer distances. Additionally, 2.4 GHz radios are normally less expensive, due to their popularity. Unfortunately, there is only 100 MHz of usable 2.4 GHz spectrum.

Until recent years, 5 GHz has not been widely used by non-Wi-Fi devices. This means there is less contention in this space. The tradeoff with 5 GHz is usually shorter range. However, as more users adopt Wi-Fi and more devices implement it, shorter range becomes an advantage because it can handle higher density with less interference.

In general, 5 GHz operation is very suitable for enterprise use and 2.4 GHz deployments are still implemented to support older clients or those clients that do not support 5 GHz channels.

Additionally, 5 GHz operation is more suitable for high density deployments because of the greater number of available channels, allowing you to create more collision domains with fewer stations per domain to reduce contention.



802.11 (PHYs) Frequency Bands

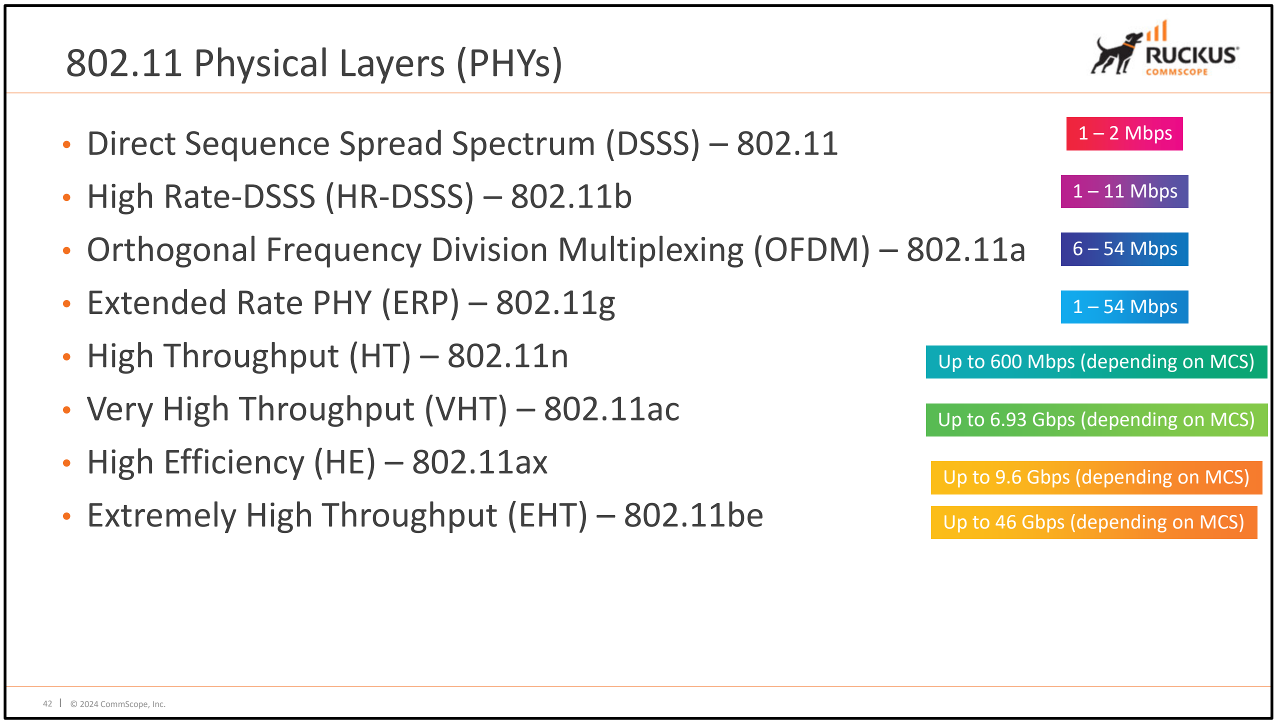
2.4 GHz PHYs	5 GHz PHYs	6 GHz PHYs
802.11b	802.11a	802.11ax
802.11g	802.11n	802.11be* *future
802.11n	802.11ac	
802.11ax	802.11ax	
802.11be* *future	802.11be* *future	

	2.4 GHz	5 GHz	6 GHz
Wavelength	12 cm	5 cm	4.9 cm
Typical Distance (non-bridging)	30-200 meters	25-100 meters	Up to 30 meters
Use Cases	Standard Wi-Fi, IoT, Bluetooth, proprietary	Standard Wi-Fi, video devices, proprietary	Next gen Wi-Fi for Homes & business, IoT, High Bandwidth, Low Latency

Frequency Band	Frequency Range	Used by 802.11 Devices
2.4 GHz	2.400-2.500 GHz	2.401-2.495 GHz
5 GHz	5.150-5.925 GHz	5.160-5.835 GHz
6 GHz	5.925-7.125 GHz	5.925-7.125 GHz (US ONLY – low power)

802.11 wireless networks are permitted to use frequency space ranging from 700 MHz to 66 GHz, currently the two most commonly used frequencies are 2.4 GHz and 5 GHz. As 6 GHz devices emerge you should expect to see 6E Wi-Fi networks become increasingly adopted. Looking at our PHY chart here you can see some PHYs can use 2.4 and 5 GHz such as 802.11n While others can operate in all three bands such as 802.11ax as well as the proposed 802.11be standard.

The range of RF communications shorten as the frequency raises and as you learned earlier, the distance a signal can travel and be useful is directly related to the power or amplitude of the signal output at the transmitter. The table in the top right indicates typical distances or ranges, but these are impacted in all bands by output power and receiver sensitivity/antenna gain. Just know that signals transmitted in lower frequencies use less power to travel the same distance as signals using higher frequencies require.



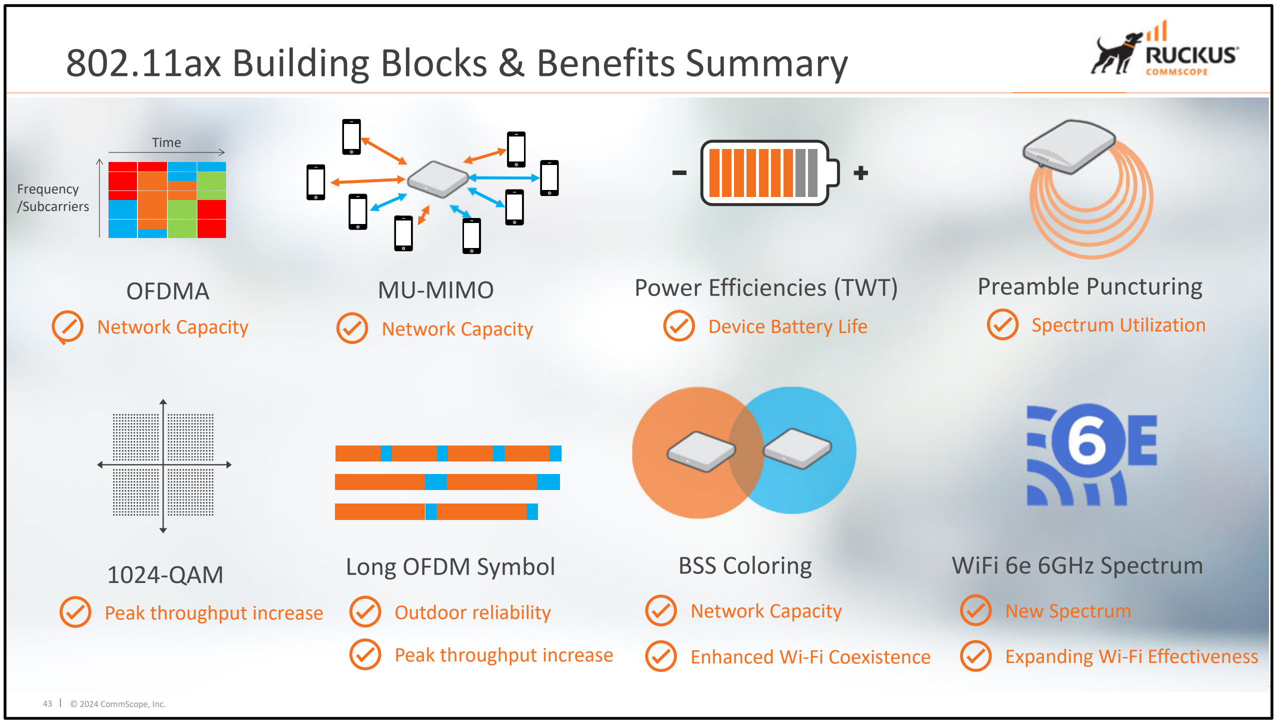
802.11 Physical Layers (PHYs)

Direct Sequence Spread Spectrum (DSSS) – 802.11	1 – 2 Mbps
High Rate-DSSS (HR-DSSS) – 802.11b	1 – 11 Mbps
Orthogonal Frequency Division Multiplexing (OFDM) – 802.11a	6 – 54 Mbps
Extended Rate PHY (ERP) – 802.11g	1 – 54 Mbps
High Throughput (HT) – 802.11n	Up to 600 Mbps (depending on MCS)
Very High Throughput (VHT) – 802.11ac	Up to 6.93 Gbps (depending on MCS)
High Efficiency (HE) – 802.11ax	Up to 9.6 Gbps (depending on MCS)
Extremely High Throughput (EHT) – 802.11be	Up to 46 Gbps (depending on MCS)

42 | © 2024 CommScope, Inc.

As wi-fi evolves new PHYs allow for increased data rates. Although we mostly refer to the protocols used in the 802.11 amendments for example: 802.11b, g, n, ac and ax.

The PHYs have names which relate to their transmission techniques. You may see these names on Modulation Coding Scheme (MCS) charts. And while outside of the scope of this discussion MCS charts can be helpful to see the supported data rates for each PHY in a given configuration.


RUCKUS
COMMSCOPE
Time
Frequency
/Subcarriers
6E

802.11ax Building Blocks & Benefits Summary

OFDMA
✓ Network Capacity

MU-MIMO
✓ Network Capacity

Power Efficiencies (TWT)
✓ Device Battery Life

Preamble Puncturing
✓ Spectrum Utilization

1024-QAM
✓ Peak throughput increase

Long OFDM Symbol
✓ Outdoor reliability
✓ Peak throughput increase

BSS Coloring
✓ Network Capacity
✓ Enhanced Wi-Fi Coexistence

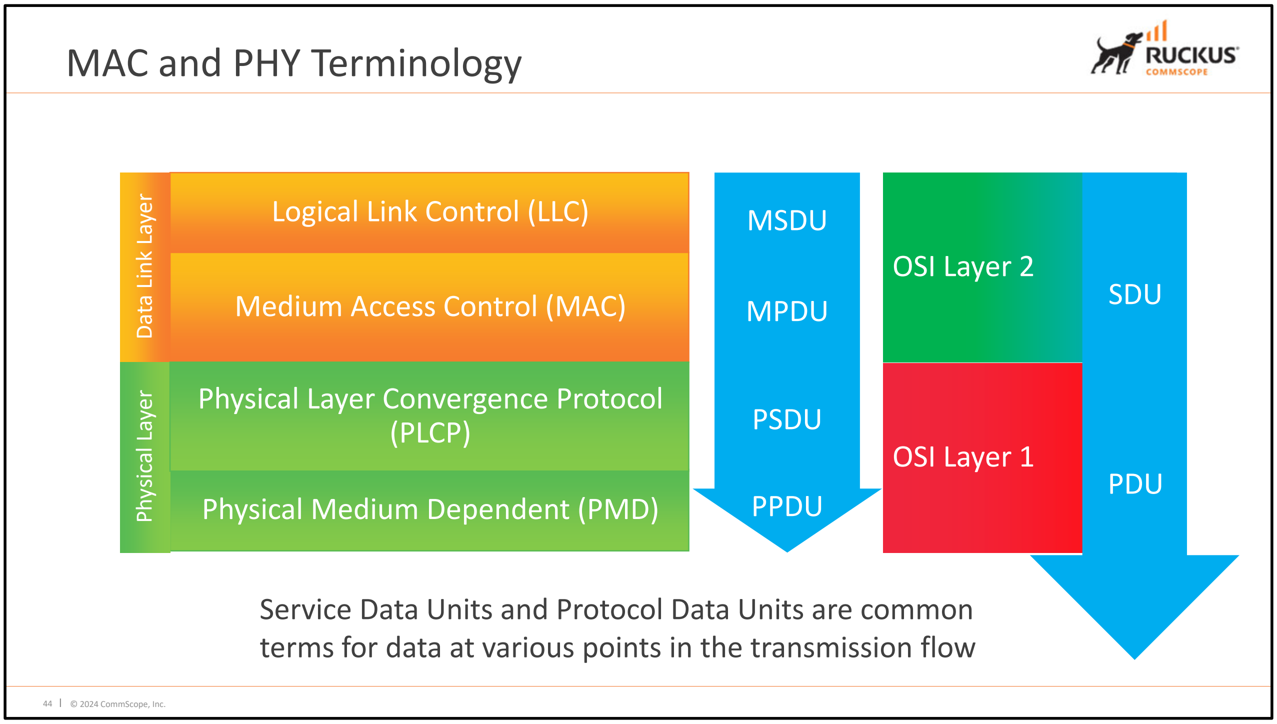
WiFi 6e 6GHz Spectrum
✓ New Spectrum
✓ Expanding Wi-Fi Effectiveness

43 | © 2024 CommScope, Inc.

Wi-Fi6 or 802.11ax is designed for high-density connectivity, and offers up to a four-fold capacity increase over its 11ac - Wi-Fi 5 predecessor.

With Wi-Fi 6, multiple APs deployed in dense device environments can collectively deliver required quality-of-service (QoS) to more clients with more diverse usage profiles. This is made possible by a range of technologies such as OFDMA, MU-MIMO with 8 uplinks and 8 downlinks, Target Wake Time, 1024-QAM, Long OFDM Symbol
BSS coloring and increased frequencies.

These technologies will play a critical role in helping Wi-Fi evolve into a collision-free, deterministic wireless technology as the IEEE looks to integrate future iterations of the mechanism into new wireless standards to support the future of Wi-Fi and beyond.



MAC and PHY Terminology

Data Link Layer

Logical Link Control (LLC)

Medium Access Control (MAC)

Physical Layer

Physical Layer Convergence Protocol (PLCP)

Physical Medium Dependent (PMD)

MSDU

MPDU

PSDU

PPDU

OSI Layer 2

OSI Layer 1

SDU

PDU

Service Data Units and Protocol Data Units are common terms for data at various points in the transmission flow

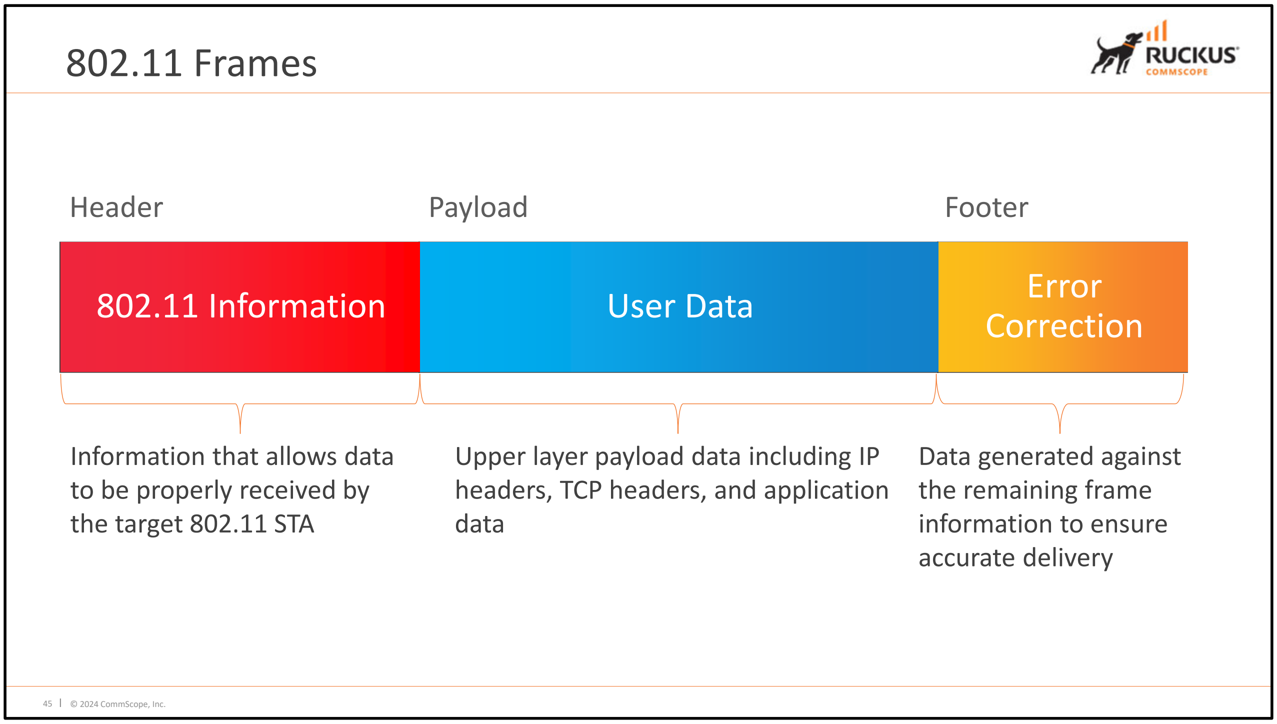
44 |

Wireless operations occur at Layers 1 and 2 of the OSI model. The MAC Service Data Unit or MSDU operates at layer 2 and receives data from layers 7-3, these MSDUs are included in all wireless frames that carry data for upper layers. The only exception to this are 802.11 management frames, they do NOT have MSDUs as they do not contain upper layer data.

The MAC protocol data unit or MPDU is what is delivered to the Physical Layer Convergence Protocol or PLCP which will be converted into a PLCP protocol data unit or PPDU and transmitted. Simply put the MSDU is what is received by upper layers 7-3 and the MPDU is what is passed down to the lower layer. This indicates directionality of the traffic.

The PLCP service data unit or PSDU is what is received from the MAC sub-layer. It is has the exact same data as the MPDU within the MAC sub-layer, but in the physical layer it is referenced as the PSDU. The PLCP adds information to the PSDU and provides the result to the PMD as a PPDU.

The PPDU, *PLCP protocol data unit*, is what is actually transmitted on the RF medium. The PPDU is a result of the data that was received from the PLCP and all of the layers above it.



802.11 Frames

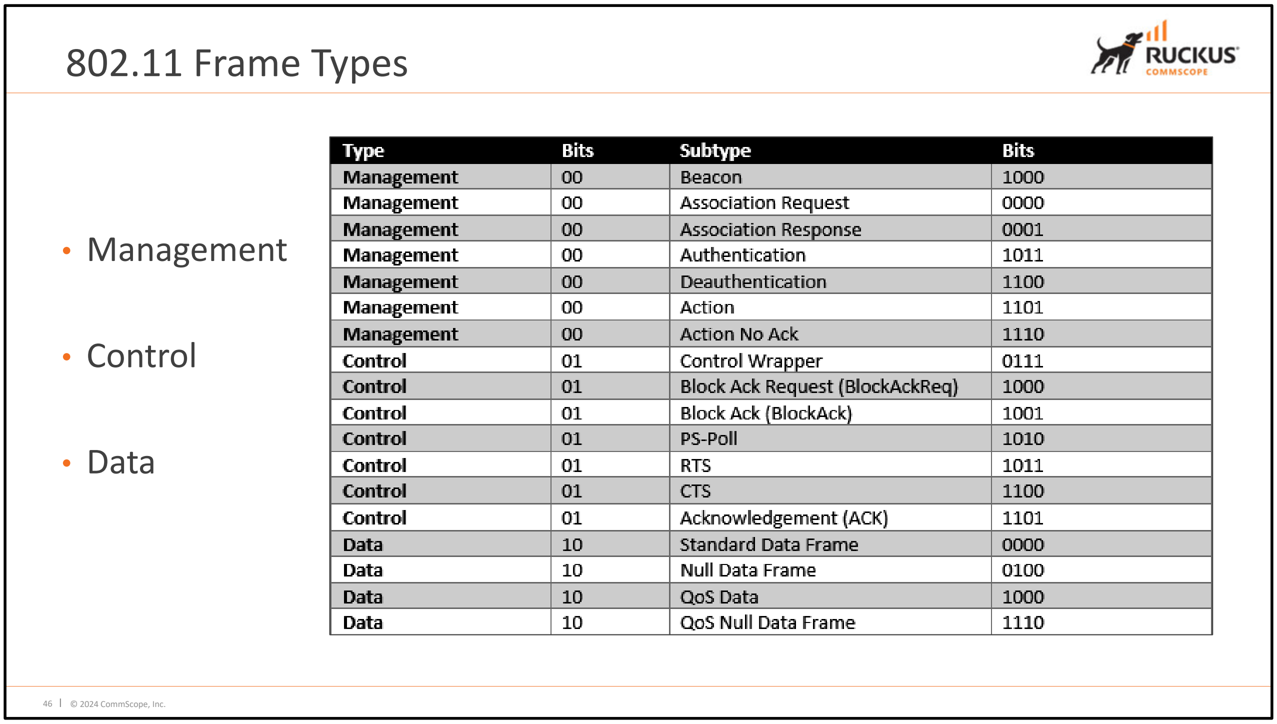
Header	Payload	Footer
802.11 Information	User Data	Error Correction
Information that allows data to be properly received by the target 802.11 STA	Upper layer payload data including IP headers, TCP headers, and application data	Data generated against the remaining frame information to ensure accurate delivery

45 | © 2024 CommScope, Inc.

802.11 network frames consists of a header, an optional payload, and a footer. This header information allows for proper transmission within the wireless medium and can provide management or control information for 802.11 networks. These headers are always transmitted in cleartext, even when encryption is used.

Payloads are either data being sent to or from a client, management data, or control body information. The payload is the only part of the frame that is encrypted when encryption is used.

The footer, also commonly referred to as a trailer is used in error correction, usually as a frame check sequence (FCS)



802.11 Frame Types

- Management
- Control
- Data

Type	Bits	Subtype	Bits
Management	00	Beacon	1000
Management	00	Association Request	0000
Management	00	Association Response	0001
Management	00	Authentication	1011
Management	00	Deauthentication	1100
Management	00	Action	1101
Management	00	Action No Ack	1110
Control	01	Control Wrapper	0111
Control	01	Block Ack Request (BlockAckReq)	1000
Control	01	Block Ack (BlockAck)	1001
Control	01	PS-Poll	1010
Control	01	RTS	1011
Control	01	CTS	1100
Control	01	Acknowledgement (ACK)	1101
Data	10	Standard Data Frame	0000
Data	10	Null Data Frame	0100
Data	10	QoS Data	1000
Data	10	QoS Null Data Frame	1110

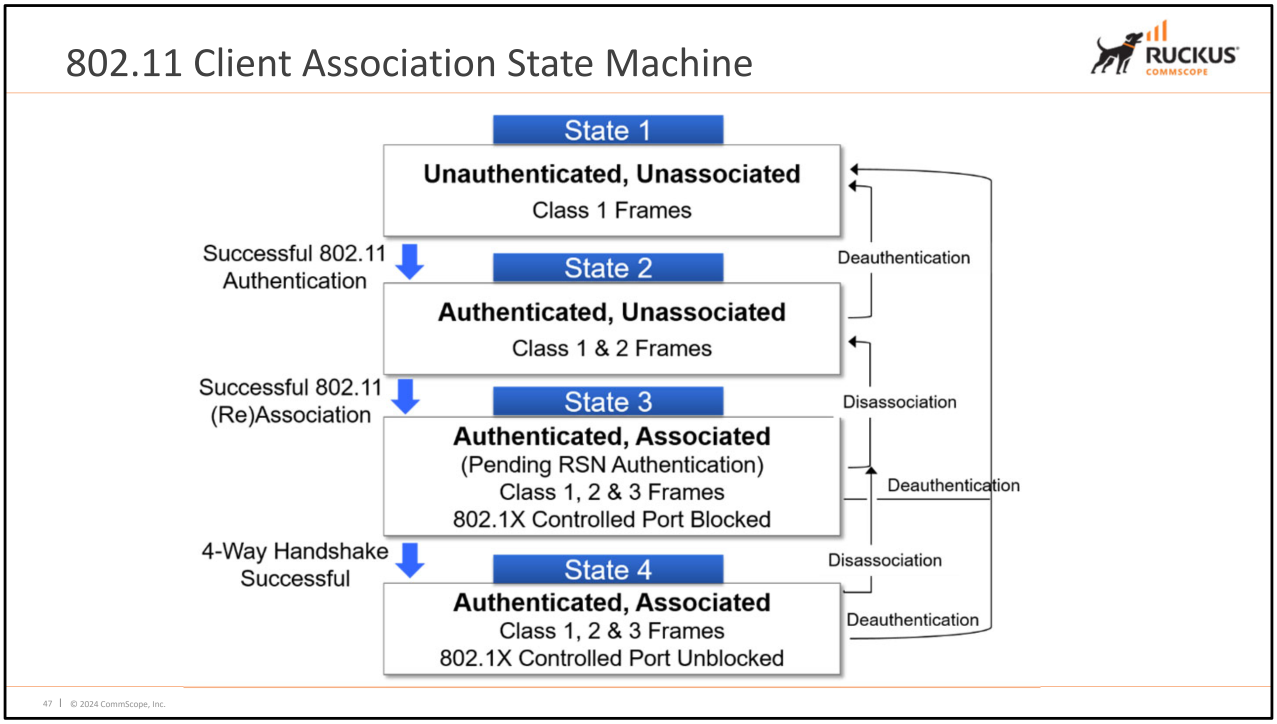
46 | © 2024 CommScope, Inc.

Here we see the three different 802.11 frame types along with each of their sub-types.

Management frames are used when joining and leaving service sets, while control frames provide unicast frame acknowledgement. These control frame acknowledgements are required as 802.11 uses collision avoidance for the delivery of data frames, and are used to gain control of or quiet down a channel

Data frames carry the payload passed down from higher layers in the OSI model.

As a wireless administrator understanding these frame types will help you with understanding packet-captures and troubleshooting.



802.11 Client Association State Machine

RUCKUS COMMSCOPE

State 1
Unauthenticated, Unassociated
Class 1 Frames

Successful 802.11 Authentication

State 2
Authenticated, Unassociated
Class 1 & 2 Frames

Successful 802.11 (Re)Association

State 3
Authenticated, Associated
(Pending RSN Authentication)
Class 1, 2 & 3 Frames
802.1X Controlled Port Blocked

4-Way Handshake Successful

State 4
Authenticated, Associated
Class 1, 2 & 3 Frames
802.1X Controlled Port Unblocked

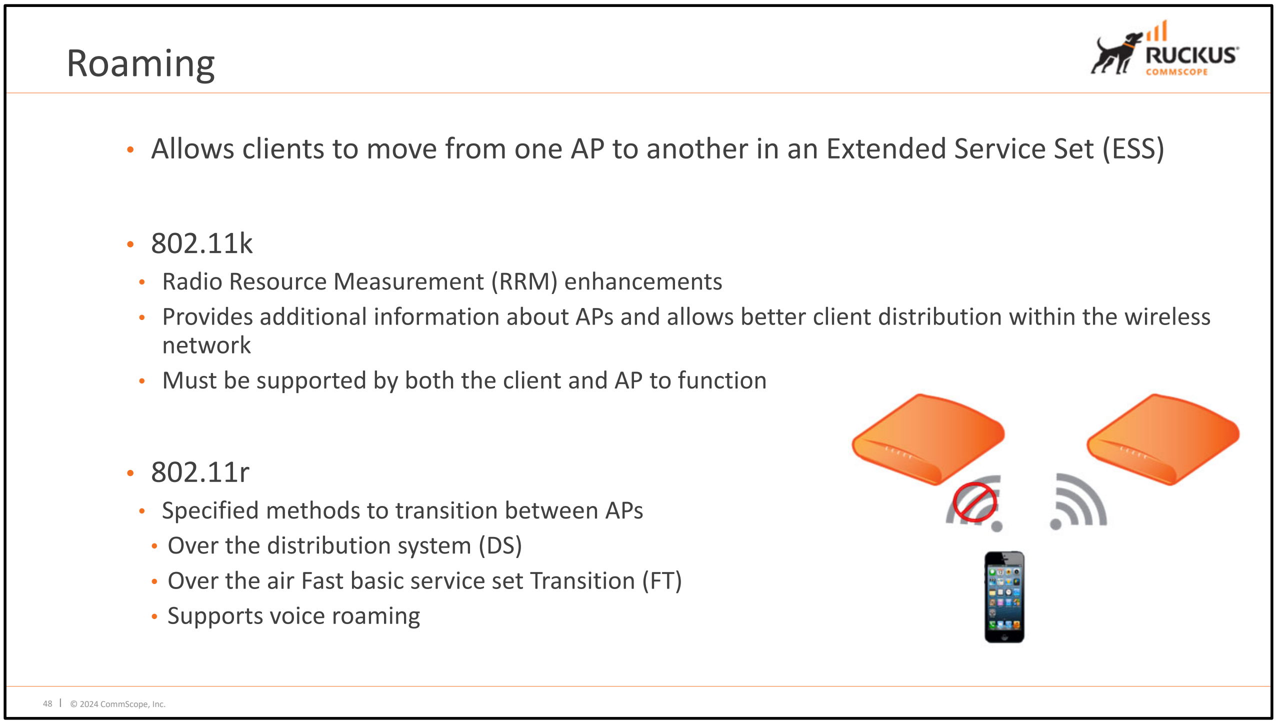
Deauthentication
Disassociation
Deauthentication
Disassociation
Deauthentication

47 | © 2024 CommScope, Inc.

The 802.11 client association state machine defines the four states a client must pass through to complete associating, or connecting to an AP. In the past, there were only three states, however the adoption of the Robust Secure Network (RSN) protocol, part of the 802.11i amendment, has forced the differentiation of the 802.1X controlled port status.

This state machine diagram is meant to provide a summary of the overall client association process. In general, the state machine process proceeds as follows:

- A client begins in an unauthenticated, unassociated state. Here only certain frames, identified as Class 1 frames, can be exchanged.
- Once 802.11 authentication is achieved, the client proceeds to state 2, where Class 2 frames are now allowed. These include additional management frames used to reach an associated state. An STA may reach State 2 with multiple APs.
- When a client is authenticated and associated, it may transition to State 3. State 3 is only necessary when RSN authentication is used, which is commonly 802.1X. Do not confuse RSN with 802.11open system authentication. RSNA is responsible establishing secure communications over a wireless network. State 3 allows Class 1, 2 and 3 frames but the 802.1X controlled port is still blocked, denying general connectivity to the station. It is important to note that if the BSS does not require RSN, client STAs will move from State 2 directly to State 4.
- Once State 4 is achieved, the 802.1X controlled port is unblocked allowing the client full access to the wireless medium.



Roaming

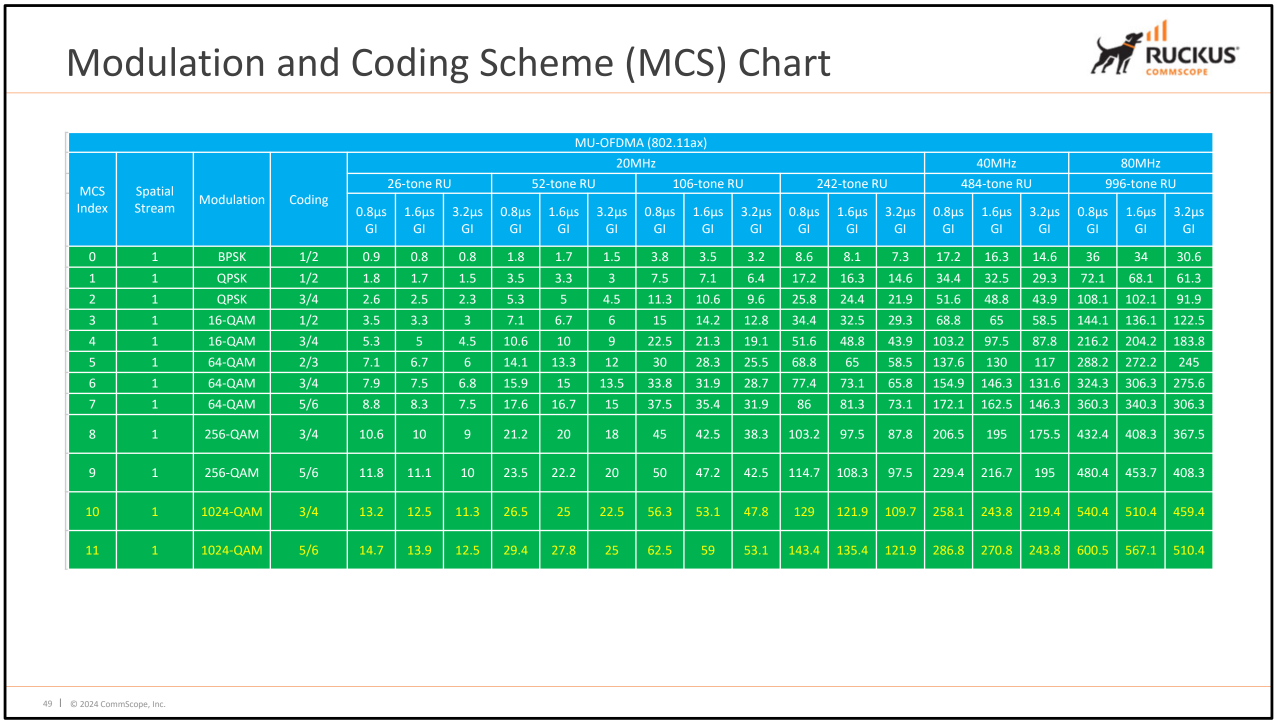
- Allows clients to move from one AP to another in an Extended Service Set (ESS)
- 802.11k
  - Radio Resource Measurement (RRM) enhancements
  - Provides additional information about APs and allows better client distribution within the wireless network
  - Must be supported by both the client and AP to function
- 802.11r
  - Specified methods to transition between APs
    - Over the distribution system (DS)
    - Over the air Fast basic service set Transition (FT)
    - Supports voice roaming

48 | © 2024 CommScope, Inc.

Roaming is when a client station disassociates from one AP and re-associates with another AP that is part of the same extended service set. The goal of roaming is to allow the device to move its association from on AP to another without breaking higher layer connections and or needing to reauthenticate. Client stations determine when and how they roam.

Two amendments to the 802.11 specification were defined to help facilitate roaming:

- 802.11k reduces the time it takes to roam by allowing the client to create optimized lists of available APs to assist in determining when and how to roam.
- 802.11r, referred to as Fast BSS Transition (FT), allows all APs in a ESS to store encryption information for connected clients. This allows clients to associate to another AP in the ESS without repeating the 802.1X/EAP authentication process or the 4-way handshake.

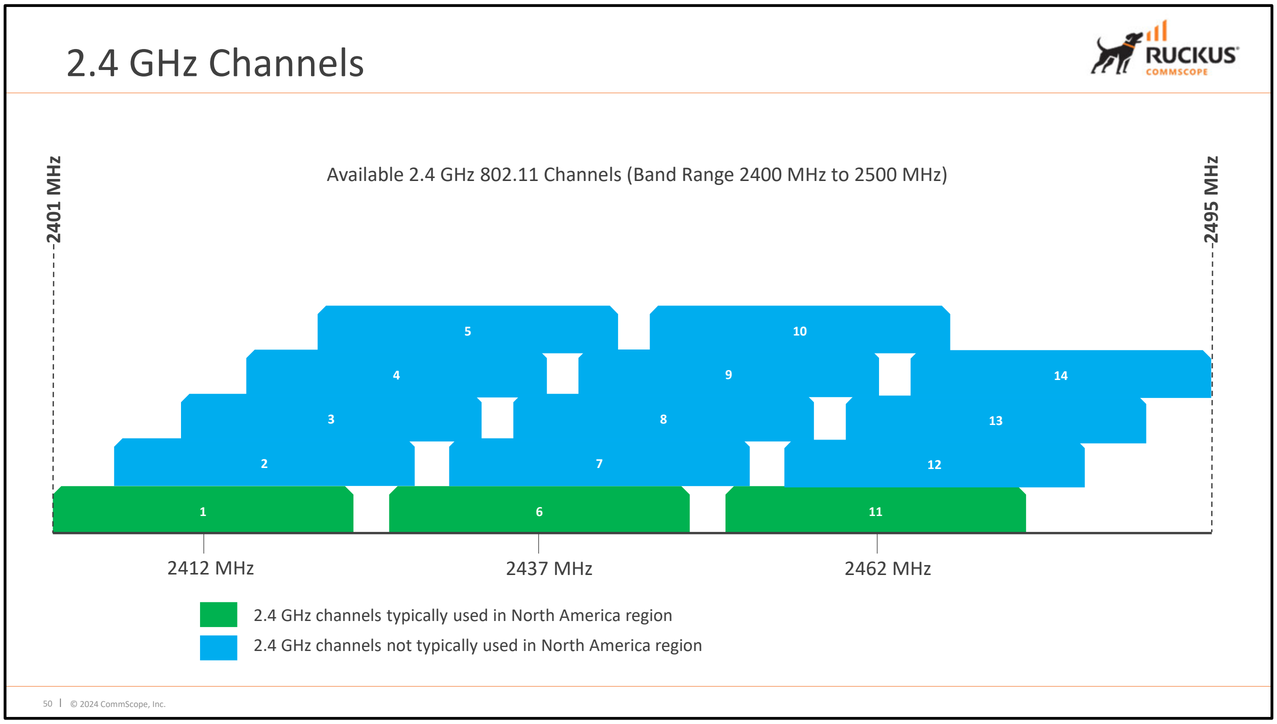


Modulation and Coding Scheme (MCS) Chart

MU-OFDMA (802.11ax)																					
MCS Index	Spatial Stream	Modulation	Coding	20MHz												40MHz			80MHz		
				26-tone RU			52-tone RU			106-tone RU			242-tone RU			484-tone RU			996-tone RU		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSK	1/2	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6
1	1	QPSK	1/2	1.8	1.7	1.5	3.5	3.3	3	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	2.6	2.5	2.3	5.3	5	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	3.5	3.3	3	7.1	6.7	6	15	14.2	12.8	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	5.3	5	4.5	10.6	10	9	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	7.1	6.7	6	14.1	13.3	12	30	28.3	25.5	68.8	65	58.5	137.6	130	117	288.2	272.2	245
6	1	64-QAM	3/4	7.9	7.5	6.8	15.9	15	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	8.8	8.3	7.5	17.6	16.7	15	37.5	35.4	31.9	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	10.6	10	9	21.2	20	18	45	42.5	38.3	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	11.8	11.1	10	23.5	22.2	20	50	47.2	42.5	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3
10	1	1024-QAM	3/4	13.2	12.5	11.3	26.5	25	22.5	56.3	53.1	47.8	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	14.7	13.9	12.5	29.4	27.8	25	62.5	59	53.1	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4

49 |

As mentioned, two new Modulation Schemes (MCS 10 and 11) have been identified with 802.1ax providing increased data rates when 1024-QAM is used. Here you can see with one spatial stream the perceivable rates based on the tone/RU sizes rather than channel width of previous standards since OFDMA can divide channels into sub-carriers or Resource Units.



2.4 GHz Channels

Available 2.4 GHz 802.11 Channels (Band Range 2400 MHz to 2500 MHz)

🟩 2.4 GHz channels typically used in North America region

🟦 2.4 GHz channels not typically used in North America region

50 | © 2024 CommScope, Inc.

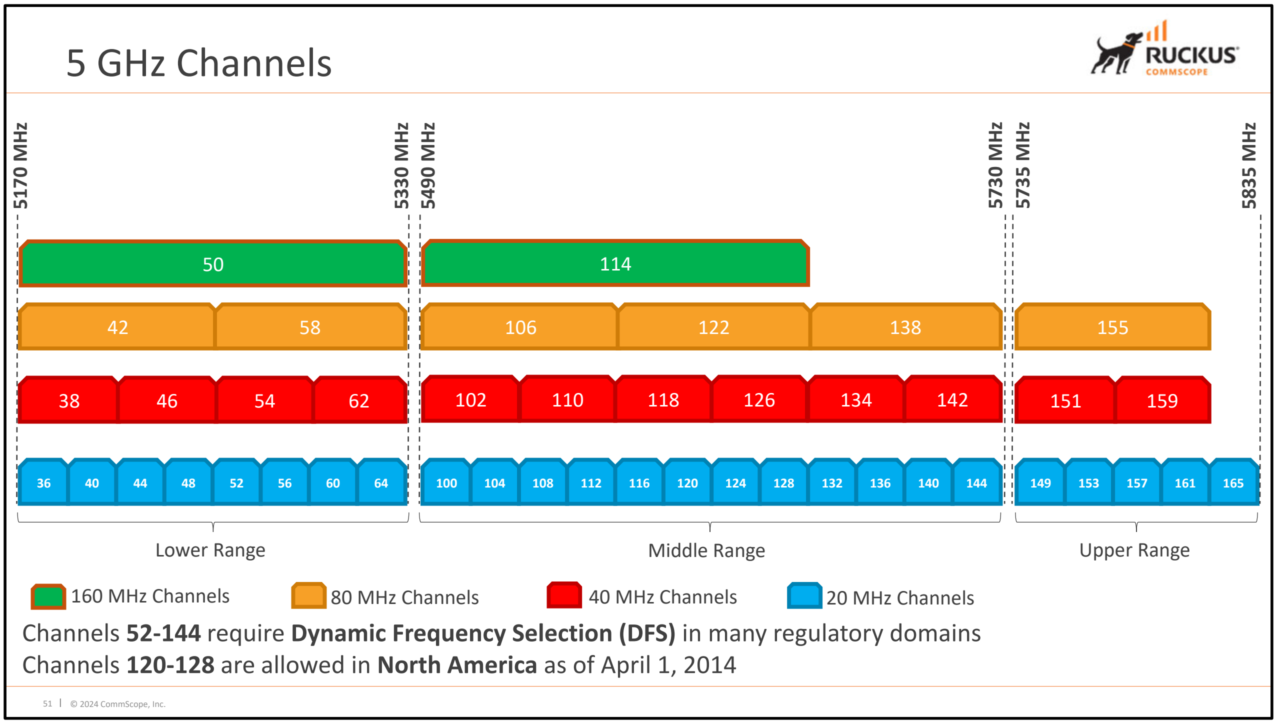
The 2.4 GHz band ranges from 2.400 to 2.500 GHz. 802.11 devices in this space only use the range from 2.401 GHz to 2.495 GHz but, that is only if all 14 channels are supported in the regulatory domain.

For example, North America supports only channels 1 through 11, i.e 2401 MHz – 2473 MHz.

Other parts of the world also support the use of channels 12-13, while Channel 14 is supported in Japan for 802.11b operations.

For this reason, most 2.4 GHz networks in North America are configured to use only channels 1, 6, and 11, since enterprise clients could be traveling between regulatory domains which do not provide support for channels 12 to 14. If these channels were used, most clients from more restrictive domains would not be able to connect. If planning for your least capable device Channels 12-14 are to be avoided.

The channels listed as “not typically used’ in the image are non-recommended channels and are considered overlapping. In some cases, they may be best for use, but such scenarios are rare. Most implementations in 2.4 GHz use a three-channel plan of 1, 6 and 11 to avoid any overlapping channel interference.



5 GHz Channels

🟩 160 MHz Channels 🟧 80 MHz Channels 🟥 40 MHz Channels 🟦 20 MHz Channels

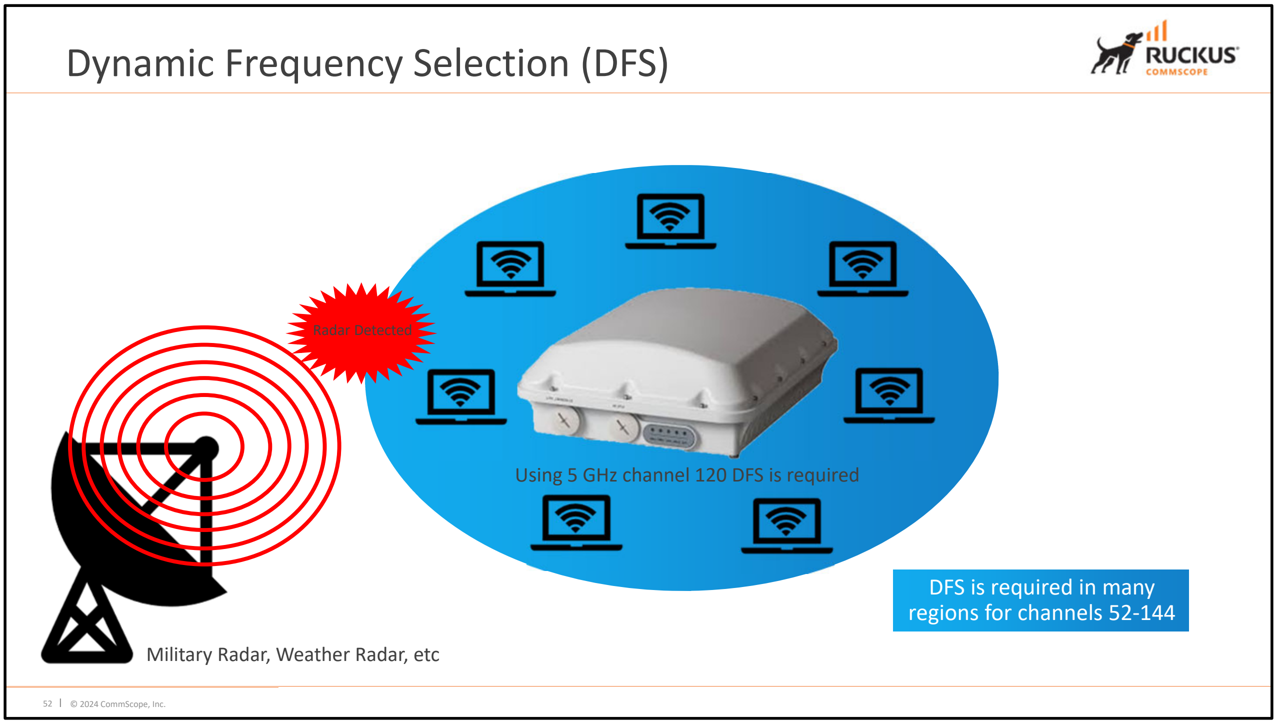
Channels **52-144** require **Dynamic Frequency Selection (DFS)** in many regulatory domains
Channels **120-128** are allowed in **North America** as of April 1, 2014

5 GHz channels are considered non-overlapping, unlike the 2.4 GHz channels. They are all 20 MHz wide and can be bonded together to form channels as wide as 160 MHz. This chart shows the 20, 40, 80 and 160Mhz channels available in North America. As shown there are two 160 MHz channels available, however one of which requires use of Dynamic Frequency Selection (DFS). Additional 160 MHz channels can be constructed using two 80 MHz channels non-contiguously. This provides 13 additional combinations of 160 MHz channels. Hover the 80 MHz channels to see examples.

Since there are more channels available in the 5 GHz there is also more complexity in operations. The complexity is due to channel and power restrictions placed upon us by various regulatory domains. For example, channels 52-144 are considered Dynamic Frequency Selection (DFS) channels in most of the world.

DFS requires radios using the specified DFS channels to scan for other designated use of these channels and move away from these channel if use is detected.

Channel widths of 160 MHz, 80 MHz and 40 MHz are allowed within the 5 GHz band, however they are not always practical. Larger channel widths have the potential for larger bandwidth, but not all clients will support the larger channel widths. Typically, enterprise deployments will use 40 MHz channels with high density areas using a 20 MHz channel



Dynamic Frequency Selection (DFS)

DFS is required in many regions for channels 52-144

Military Radar, Weather Radar, etc

52 | © 2024 CommScope, Inc.

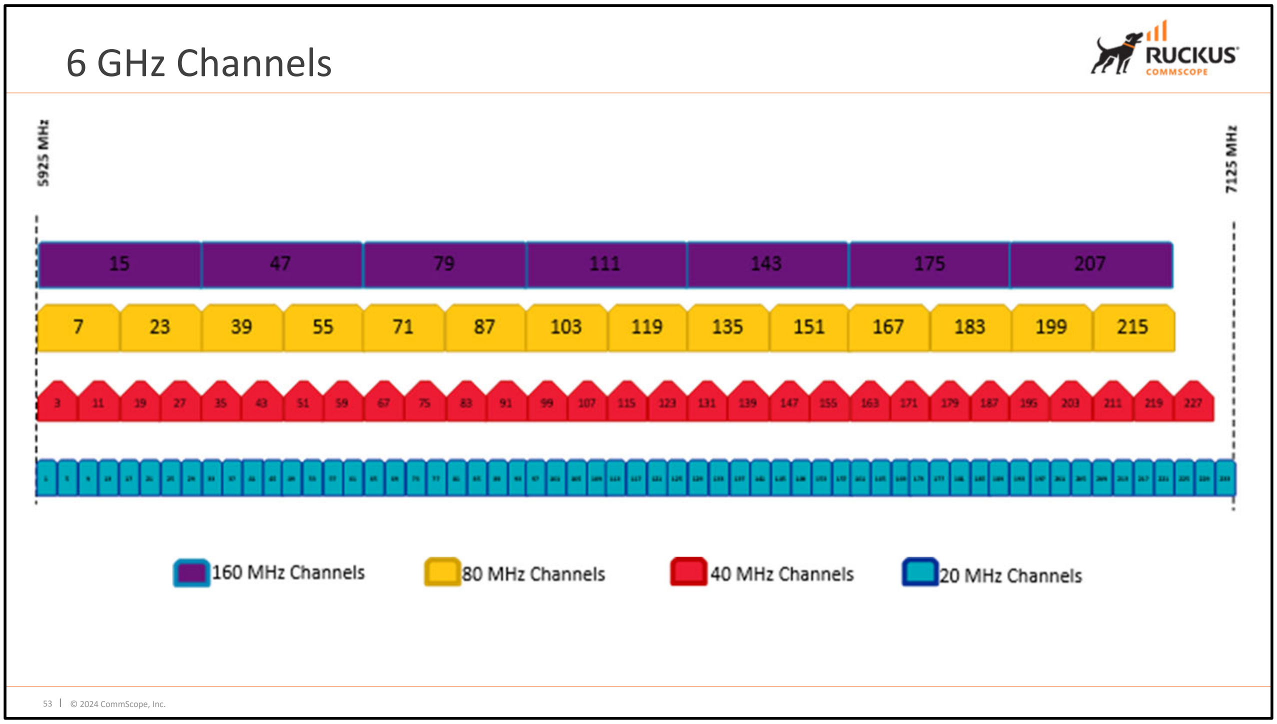
Dynamic Frequency Selection (DFS) is a radar detection and avoidance system for military, weather, and other radars which may be operating on 5 GHz channels. DFS is regulatory domain specific and may be defined regionally on 5 GHz channels while other regions may not allow the use of DFS channels at all.

DFS performs the following functions:

- Quieting the current channel for testing
- Testing for radar before using and while operating in a channel
- Discontinuing operations after detecting radar
- Detecting radar in current and other channels
- Requesting and reporting measurements in the channels using Action frames and elements

If DFS detects radar the AP determines a new channel based on normal vendor proprietary channel selection algorithms, while also factoring in DFS measurement information and channel support information received by clients during association.

Newer clients support the use of DFS channels while some older clients may not, the ability or inability to use these channels will impact your overall channel plan.



6 GHz Channels

53 | © 2024 CommScope, Inc.

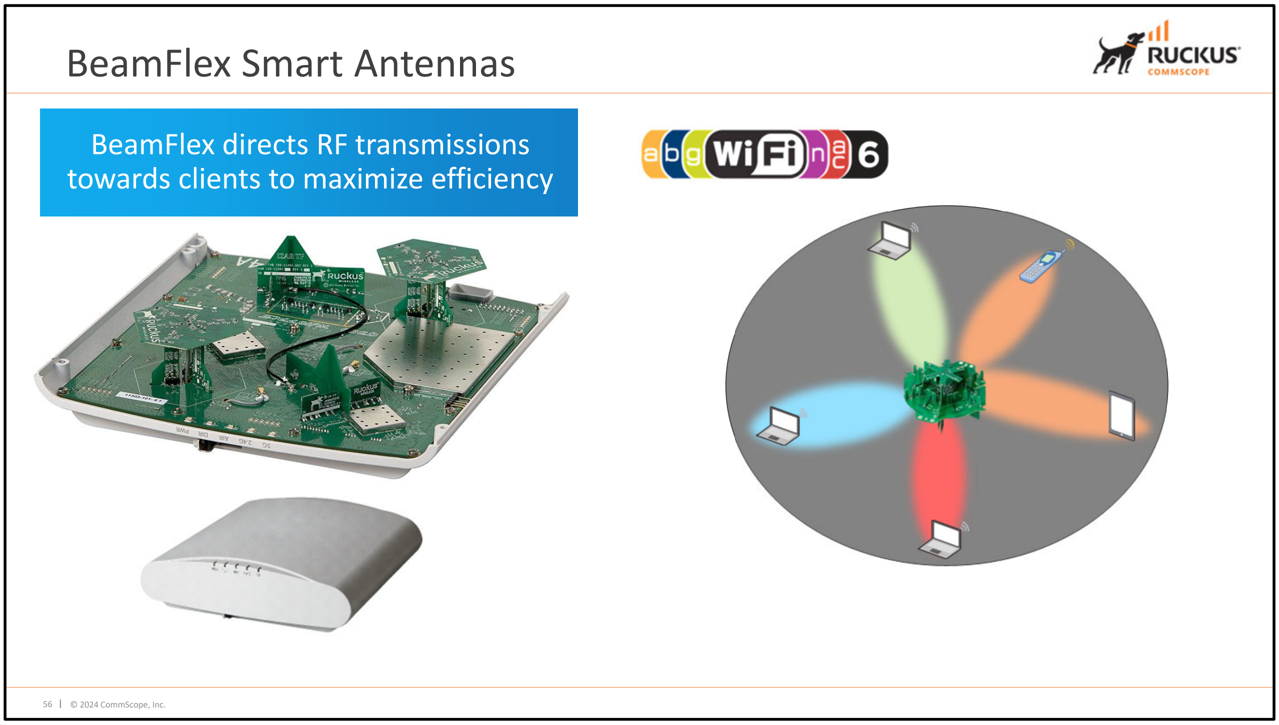
As we outlined earlier the new 6 GHz spectrum dubbed Wi-Fi 6E brings an additional 1200 MHz of spectrum and was approved for use in the US in 2020. You can quickly see one major benefit of the new spectrum by observing the number of non-overlapping channels available. In the US, there are (59) 20 MHz channels, (29) 40 MHz channels, (14) 80 MHz channels and (7) 160 MHz channels available for use.

The chart shown here is specific to the United States as some regions are allocating different amounts of spectrum. For instance, the ETSI in Europe has currently slated 5925 MHz through 6425 MHz which only provides for (24) 20 MHz channels, (12) 40 MHz channels, (6) 80 MHz channels, and (3) 160 MHz channels. The EU has not fully approved 6GHz for wi-fi use and is expected to do so in 2021. Hover the button in the lower right to see the difference in the 6 GHz channel plan between North America and Europe.

RUCKUS technologies, products and solutions

RUCKUS
COMMSCOPE

RUCKUS proprietary technologies



BeamFlex Smart Antennas

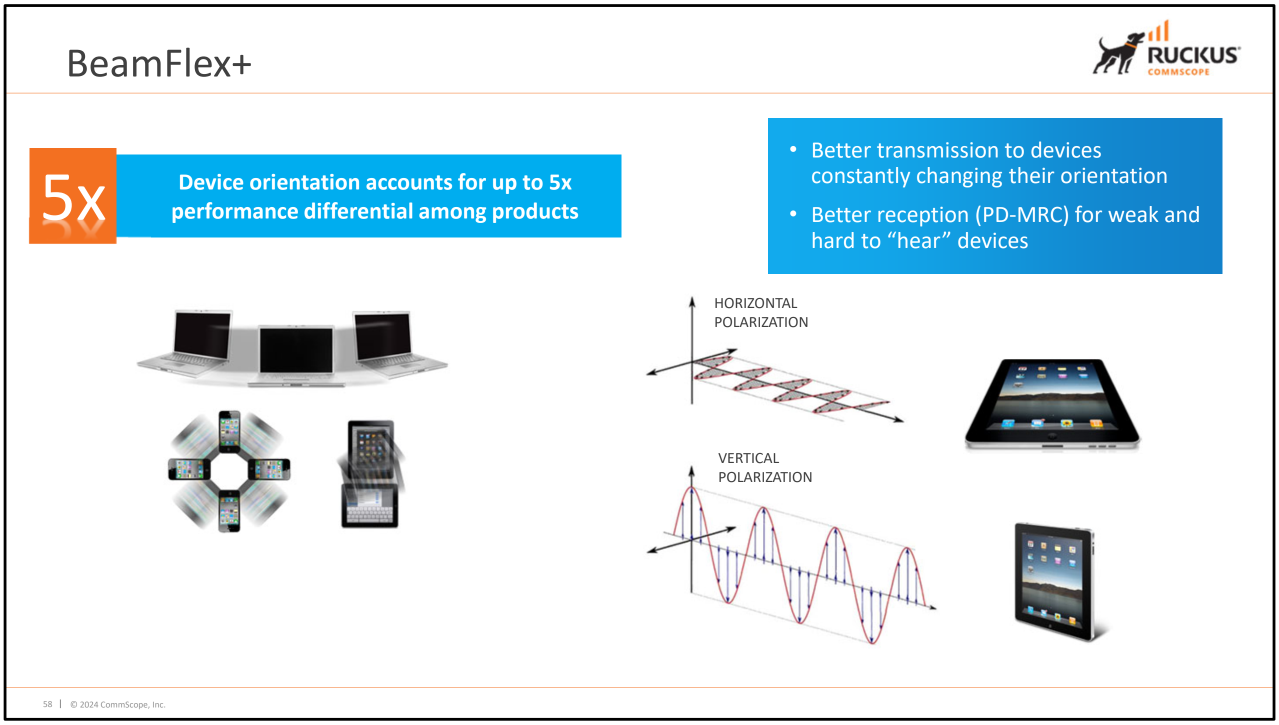
BeamFlex directs RF transmissions towards clients to maximize efficiency

RUCKUS
COMMSCOPE
a b g Wi Fi n ac 6
Ruckus

BeamFlex is a unique RUCKUS technology and one of the main advantages of using a RUCKUS Wireless Access Point. The BeamFlex antenna array directs transmissions towards the client to maximize the efficiency of the transmissions where they are needed which can help steer away from undesired RF interference.

BeamFlex does this by creating dynamic adaptive antennas. Within the RUCKUS access point physical antenna elements which act like lenses or reflectors, depending upon which ones are turned on and off, are part of the antenna array.

This antenna array with multiple elements, in combination with the access points 2.4 or 5 GHz radio chains, uses RUCKUS proprietary algorithms in real time to form thousands of antenna patterns. By customizing the antenna pattern for each user and each packet, BeamFlex can deliver up to a 6 dB of additional gain as seen by the user’s device. 6 dB in RF parlance means a signal that is four times stronger than what you’d get with an omnidirectional antenna. It is important to note that BeamFlex does not change the amount of energy that radiates from the access point, as that is set by regulation, only the amount that the client receives.



BeamFlex+

5x

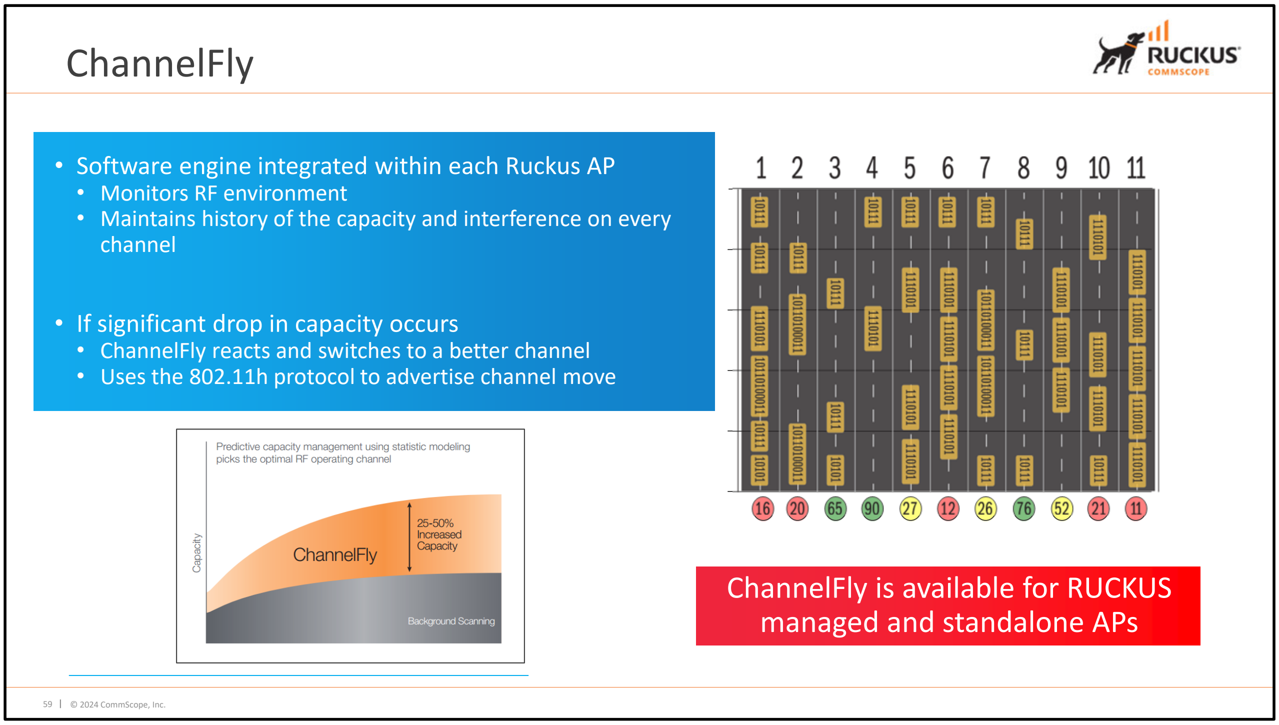
Device orientation accounts for up to 5x performance differential among products

- Better transmission to devices constantly changing their orientation
- Better reception (PD-MRC) for weak and hard to “hear” devices

58 | © 2024 CommScope, Inc.

With the proliferation of phones, tablets, smart watches and other mobile wireless clients, access points are communicating with devices in any number of physical orientations throughout the wireless environment. BeamFlex+ is an enhancement to RUCKUS BeamFlex antenna technology which enables wireless AP antenna selection based on client device orientation.

BeamFlex+ uses Polarization Diversity with Maximum Ratio Combining (PD-MRC) to change an APs antenna polarization based on RF signals received from client devices. It does this by listening to clients on both horizonal and vertical planes, determining which signal is best for the specific client and switching to match the polarization. This provides a higher signal strength, greater wireless data rates and overall a better wireless experience.



ChannelFly

- Software engine integrated within each Ruckus AP
  - Monitors RF environment
  - Maintains history of the capacity and interference on every channel
- If significant drop in capacity occurs
  - ChannelFly reacts and switches to a better channel
  - Uses the 802.11h protocol to advertise channel move

Predictive capacity management using statistic modeling picks the optimal RF operating channel
Capacity
ChannelFly
25-50% Increased Capacity
Background Scanning
1 2 3 4 5 6 7 8 9 10 11
16 20 65 90 27 12 26 76 52 21 11

ChannelFly is available for RUCKUS managed and standalone APs

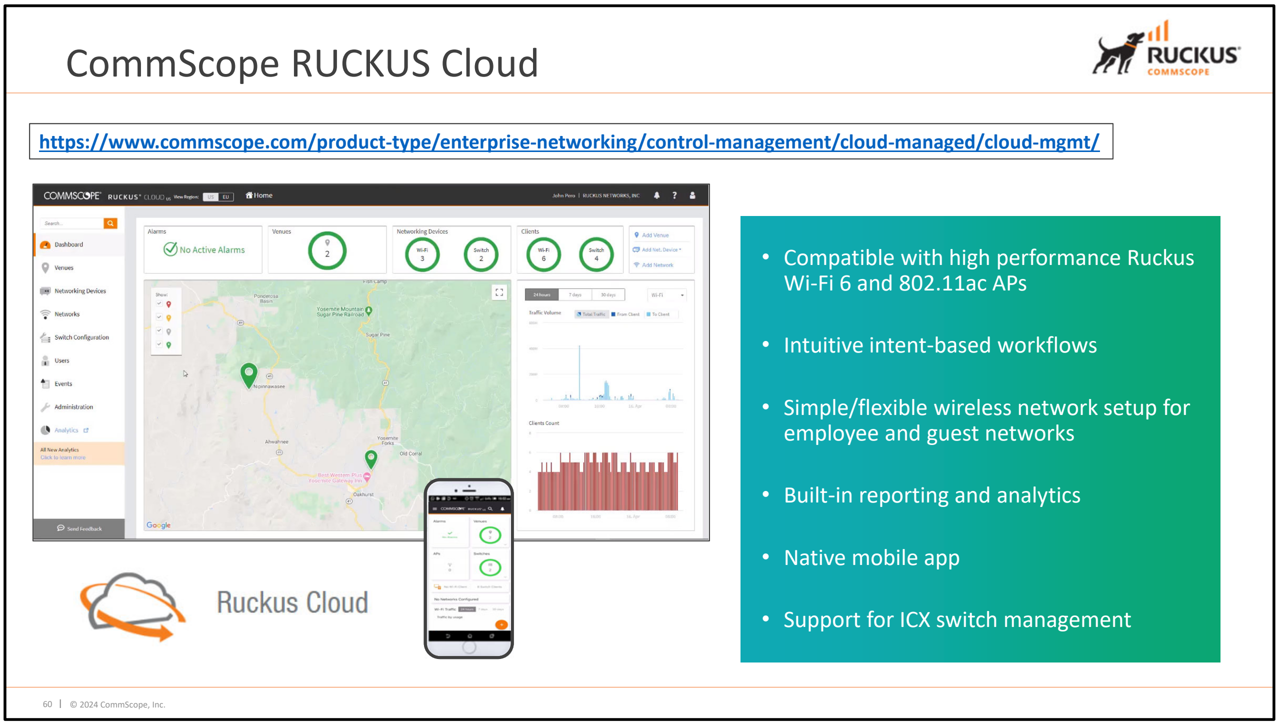
59 | © 2024 CommScope, Inc.

ChannelFly is a RUCKUS proprietary technology that measures the performance of WLANs across all available channels. With ChannelFly, the AP intelligently samples different channels while using them for service. ChannelFly assesses channel capacity every 15 seconds and changes channel when, based on historical data, a different channel is likely to offer higher capacity than the current channel.

Each AP makes channel decisions based on this historical data and maintains an internal log of channel performance individually. When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and Ruckus mesh nodes in the 2.4 GHz and/or 5 GHz bands.

When initially implemented (in the first 30-60 minutes) there will be more frequent channel changes as ChannelFly learns the environment. However, once an AP has learned about the environment and which channels are most likely to offer the best throughput potential, channel changes will occur less frequently unless a large measured drop in throughput occurs.

ChannelFly can react to large measured drops in throughput capacity in as little as 15 seconds, while smaller drops in capacity may take longer to react to.



CommScope RUCKUS Cloud

https://www.commscope.com/product-type/enterprise-networking/control-management/cloud-managed/cloud-mgmt/

- Compatible with high performance Ruckus Wi-Fi 6 and 802.11ac APs
- Intuitive intent-based workflows
- Simple/flexible wireless network setup for employee and guest networks
- Built-in reporting and analytics
- Native mobile app
- Support for ICX switch management

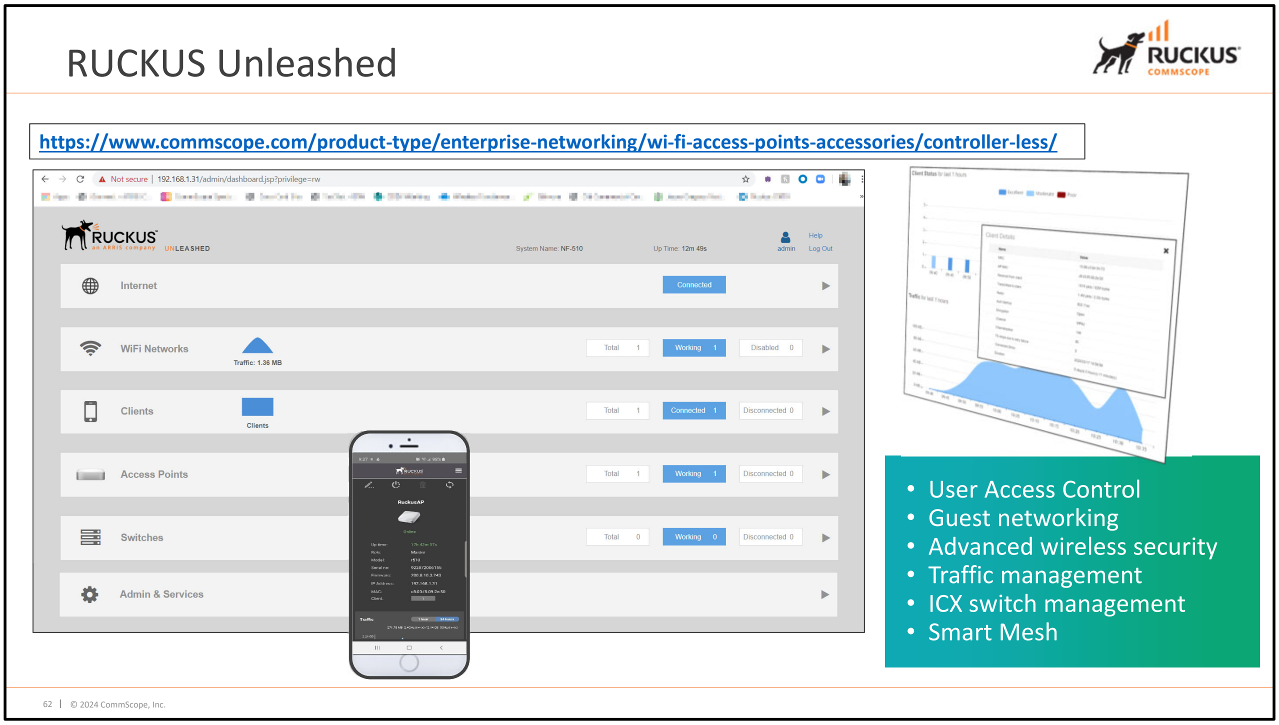
60 | © 2024 CommScope, Inc.

The CommScope RUCKUS Cloud is a cloud-based platform which allows administrators to deploy, monitor, manage and troubleshoot multi-site wireless and wired networks via web-interface or mobile app, giving administrators centralized visibility of their network from anywhere in the world while eliminating the need for an on-prem controller.

CommScope RUCKUS Cloud supports the latest Ruckus Wi-Fi 6 and 802.11ac access points as well as ICX 7150, 7650 and 7850 switching platforms.

The CommScope RUCKUS Cloud interface is intuitive and easy to use, incorporating a single pane of glass to give administrators visibility and control of their WLANs, wired networks, APs, clients and applications.

Network setup is easy and flexible and includes many options to secure employee WLAN access such as Dynamic Pre-Share Key (DPSK), PSK, 802.1X and Cloudpath onboarding. While guest networks can be secured with: Social media login, SMS, e-mail, or passcodes.



RUCKUS Unleashed

https://www.commscope.com/product-type/enterprise-networking/wi-fi-access-points-accessories/controller-less/

- User Access Control
- Guest networking
- Advanced wireless security
- Traffic management
- ICX switch management
- Smart Mesh

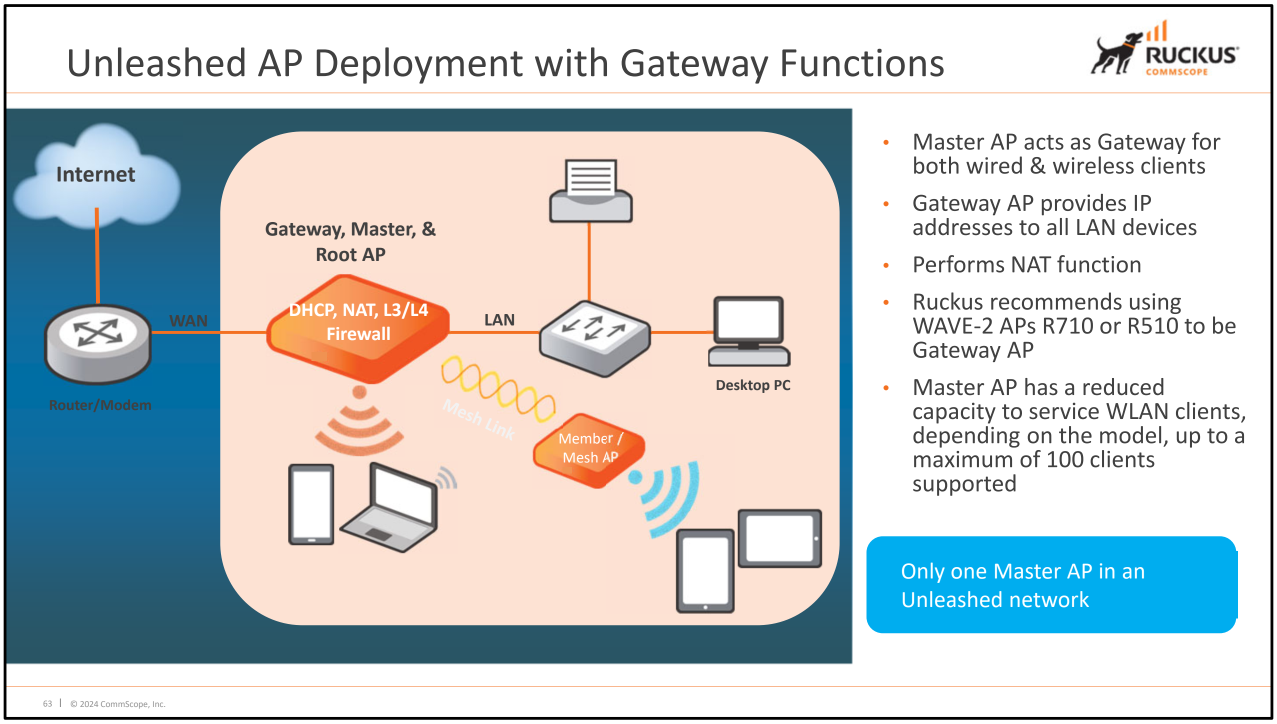
62 | © 2024 CommScope, Inc.

RUCKUS Unleashed allows small to mid-sized businesses to deploy and manage Ruckus access points without the need for a standalone controller. Ruckus Unleashed is custom designed software that runs directly on the AP and is supported on many Ruckus access point models. The intuitive browser based web interface enables simplistic configuration of the many features and capabilities of unleashed which include (but are not limited to):

- User Access Control
- Guest Networking
- Advanced Wi-Fi Security
- Traffic Management
- ICX switch Management
- Smart Mesh (some models)

The RUCKUS Unleashed mobile app enables configuration and troubleshooting of your unleashed network from your handheld device. At the time this course was created Ruckus Unleashed version 200.8 supports up to 128 APs and 2048 clients and as customers needs scale beyond these limitations the migration to controller based Wi-Fi is easy, all while using the same access points.

If you wish to transition managing AP's running unleashed firmware to management with SmartZone controllers, additional CLI configuration is required.



Unleashed AP Deployment with Gateway Functions

- Master AP acts as Gateway for both wired & wireless clients
- Gateway AP provides IP addresses to all LAN devices
- Performs NAT function
- Ruckus recommends using WAVE-2 APs R710 or R510 to be Gateway AP
- Master AP has a reduced capacity to service WLAN clients, depending on the model, up to a maximum of 100 clients supported

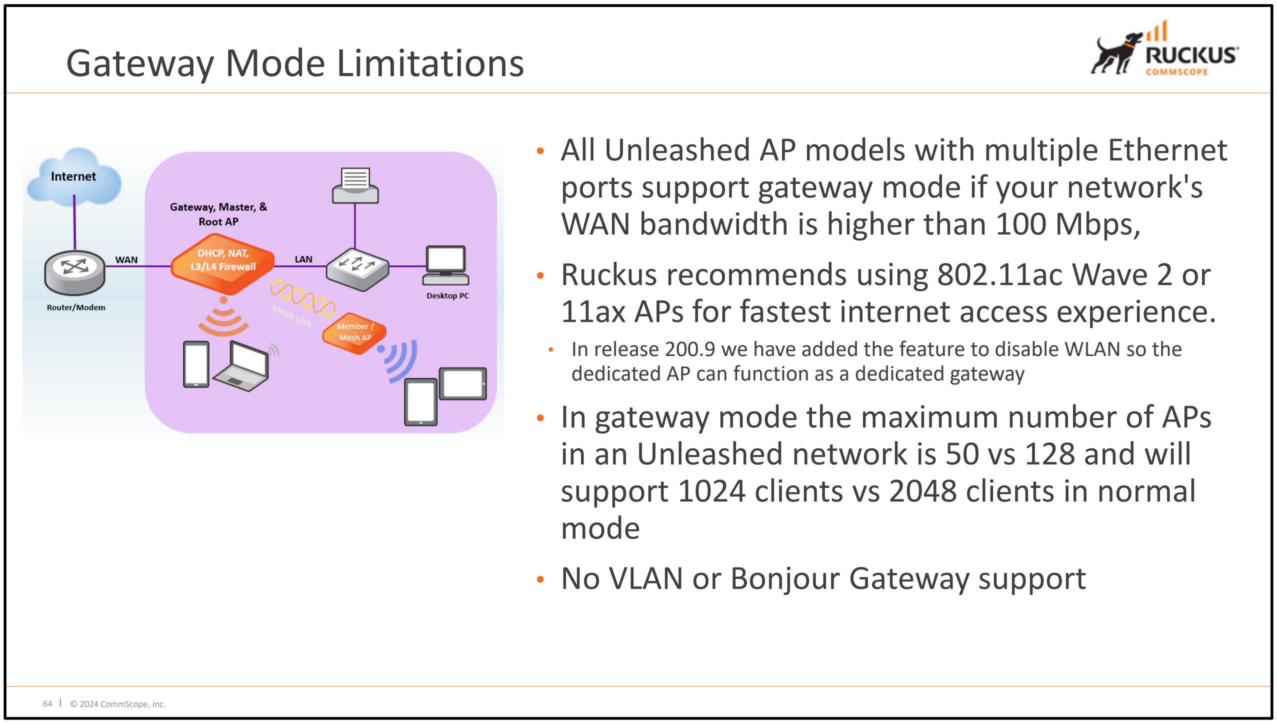
Only one Master AP in an Unleashed network

63 | © 2024 CommScope, Inc.

When configuring the Master Unleashed AP as a Gateway, the AP is going to be sitting in between your LAN and WAN connection.

It will act as a gateway for both wired and wireless clients.

All the traffic will go through this AP and the AP will do the DHCP server function as well as NAT and other master functions.



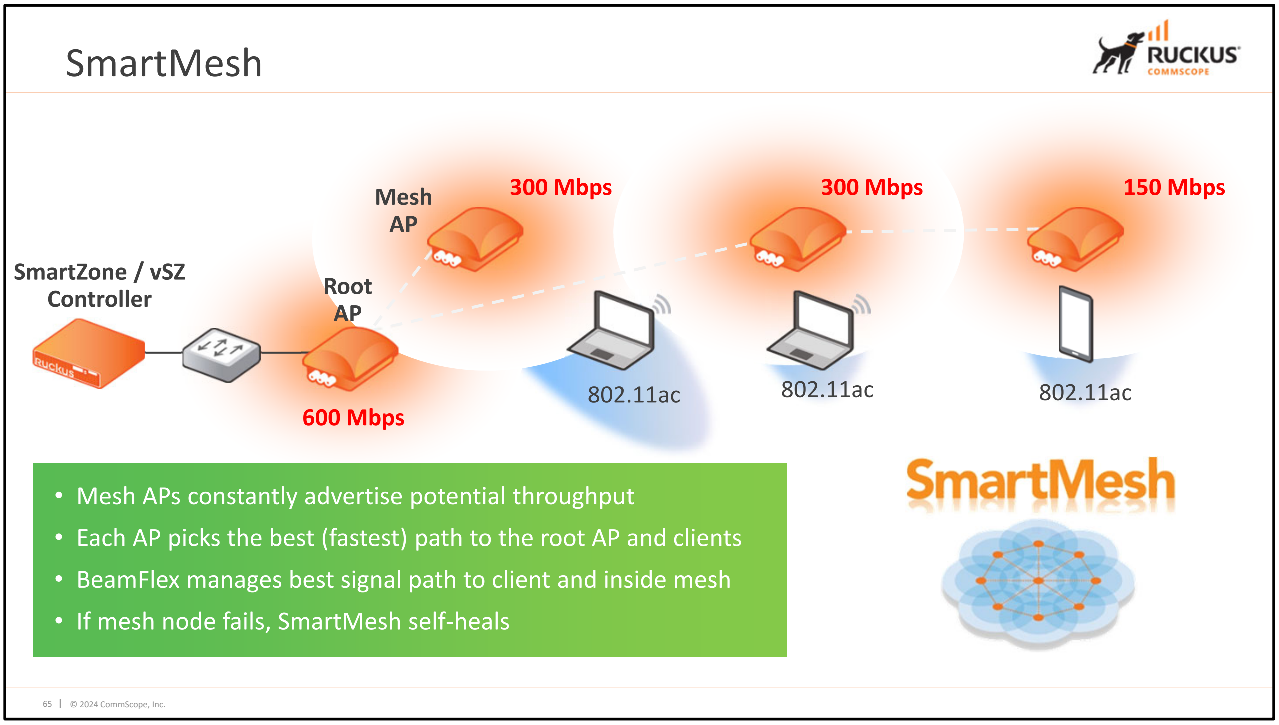
Gateway Mode Limitations

- All Unleashed AP models with multiple Ethernet ports support gateway mode if your network's WAN bandwidth is higher than 100 Mbps,
- Ruckus recommends using 802.11ac Wave 2 or 11ax APs for fastest internet access experience.
  - In release 200.9 we have added the feature to disable WLAN so the dedicated AP can function as a dedicated gateway
- In gateway mode the maximum number of APs in an Unleashed network is 50 vs 128 and will support 1024 clients vs 2048 clients in normal mode
- No VLAN or Bonjour Gateway support

64 | © 2024 CommScope, Inc.

All Unleashed AP models with multiple Ethernet ports support gateway mode. If your network's WAN bandwidth is higher than 100 Mbps, Ruckus recommends using 802.11ac Wave 2 or later APs (such as R510, R610, R710, R720) to enjoy the fastest internet access experience.

- The Master AP acts as the gateway for both wired and wireless clients.
- The gateway AP provides IP addresses and performs NAT (routing) functions in addition to serving as the Unleashed Master AP, and servicing wireless clients. For this reason, it is preferable to use an AP with higher CPU/memory resources, especially 802.11ac Wave 2 or later APs (e.g., R510, R610, R710, R720) as the Gateway AP, if possible.
- If gateway mode is enabled, the maximum number of APs in an Unleashed network is 25, even if the Master AP could otherwise support more.
- No VLAN support in gateway mode.
- Bonjour Gateway is not supported in gateway mode (no VLANs).
- When Mesh is enabled in gateway mode, and when the WAN IP address is obtained via PPPoE, the Master AP cannot be part of a Meshtree. However, Mesh can still be enabled and any member AP can be a Root AP or Mesh AP.
- The WAN and LAN IP addresses must be in different IP subnets, and the address ranges may not overlap.
- If gateway mode is enabled, redundancy is disabled. This means that if the Master (gateway) AP goes offline for any reason, a member AP will not be able to take over and become the new Master.



SmartMesh

SmartZone / vSZ Controller

Root AP

600 Mbps

Mesh AP

300 Mbps

300 Mbps

150 Mbps

802.11ac

802.11ac

802.11ac

- Mesh APs constantly advertise potential throughput
- Each AP picks the best (fastest) path to the root AP and clients
- BeamFlex manages best signal path to client and inside mesh
- If mesh node fails, SmartMesh self-heals

SmartMesh

SmartMesh enables Access Points to create a dynamic mesh without the need for cable connectivity.

Here, we see a root AP connected with an Ethernet cable to a Layer 2 network. The layer 2 network includes additional access points managed via a SmartZone controller.

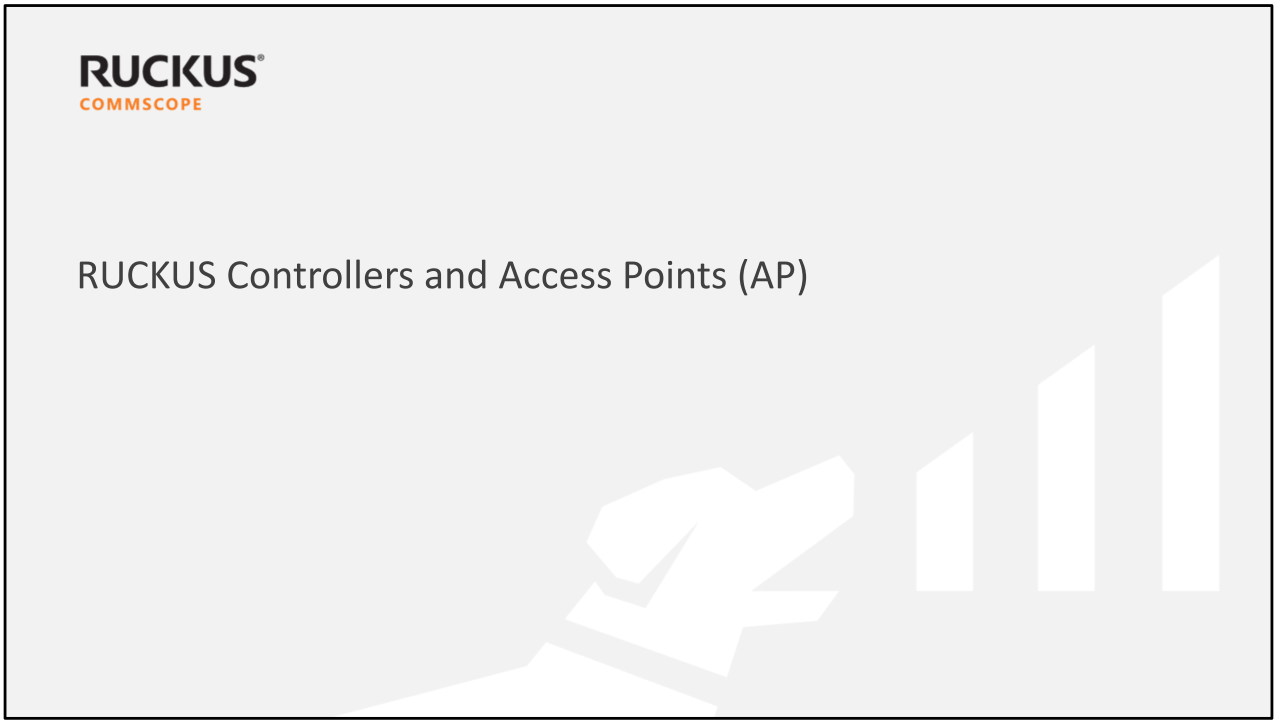
Members APs of a SmartMesh constantly advertise the potential throughput.
Here, the first meshing AP advertises a capacity of 300 megabits second.

The second meshing AP has direct view of the root AP and may also advertise a capacity of a 300 megabits per second.

The third meshing AP does not have a direct view of the root AP. As a result of taking an extra hop (2 in this case), its capacity advertisement is 150 megabits per second.

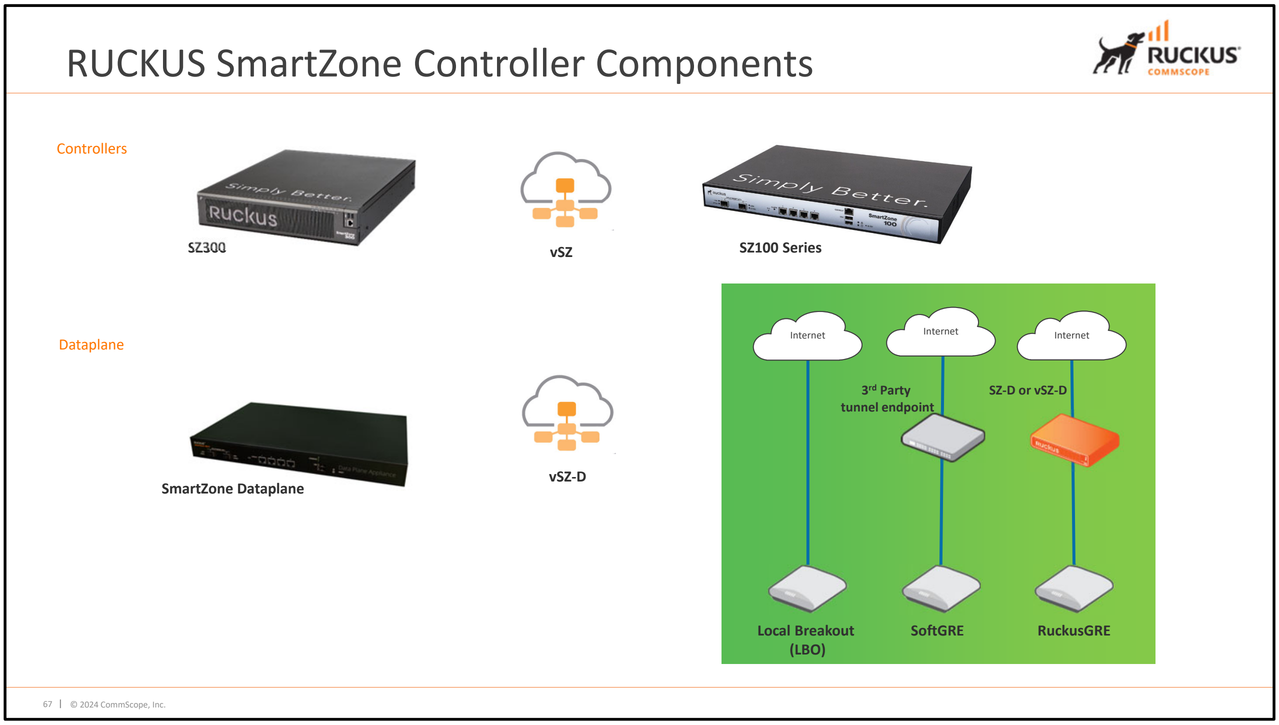
BeamFlex is used to manage the best signal path to the clients inside the mesh as well as the best signal paths within the mesh topology. Mesh nodes constantly monitor mesh links. If any mesh links experience problems or are down, the remaining nodes automatically reconfigure without intervention.

RUCKUS Mesh links utilizing the 5GHz radio also support client connections on 5GHz as well. It is best practice to limit the number of hops from the root AP within your mesh to minimize the decrease in bandwidth for mesh nodes.



RUCKUS
COMMSCOPE

RUCKUS Controllers and Access Points (AP)



RUCKUS SmartZone Controller Components

Controllers

SZ300

vSZ

SZ100 Series

Dataplane

SmartZone Dataplane

vSZ-D

Internet

Internet

Internet

3rd Party tunnel endpoint

SZ-D or vSZ-D

Local Breakout (LBO)

SoftGRE

RuckusGRE

67 | © 2024 CommScope, Inc.

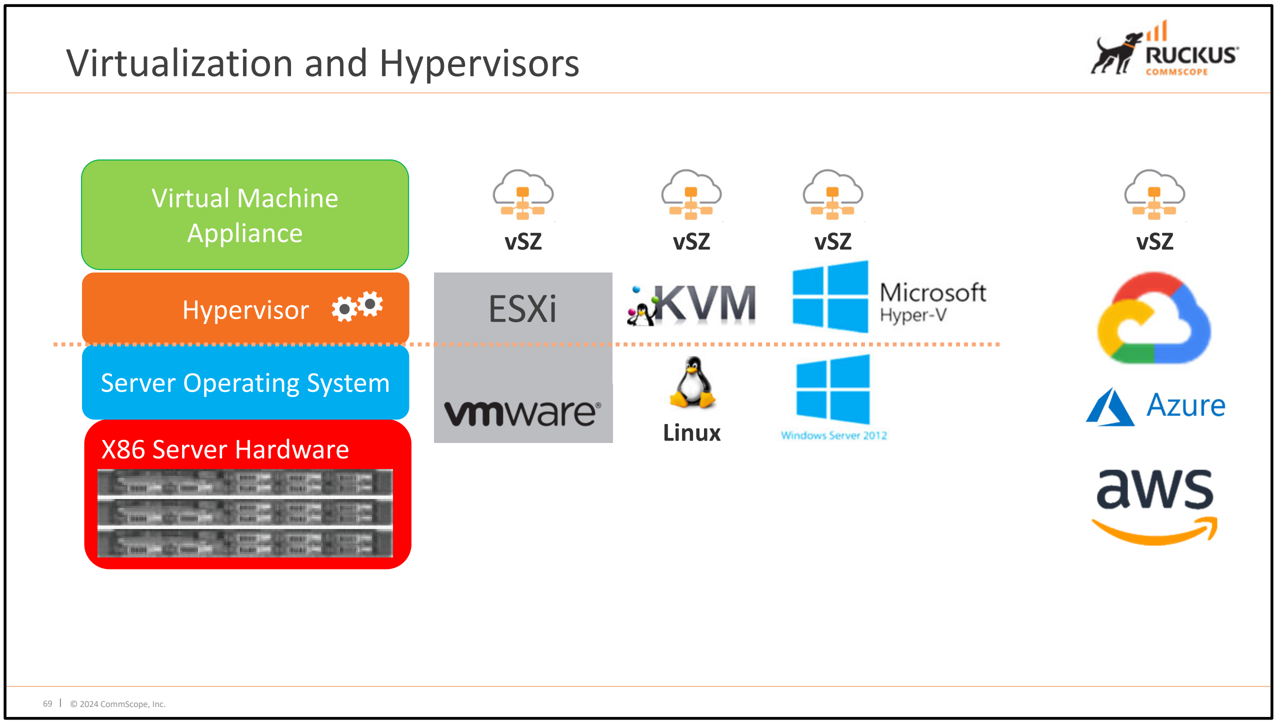
The RUCKUS SmartZone products are Wireless LAN Controllers that provide management and control for RUCKUS indoor and outdoor Access Points.

The RUCKUS controllers are:

- **SmartZone 300** – can support up to 10,000 Access Points per node, and 30,000 in a cluster, running SmartZone in High Scale mode.
- **Virtual SmartZone** – Virtualized versions of the SmartZone controllers, both High Scale and Essentials.
- **SmartZone 100** – managing networks up to 1,024 Access Points, or 3,000 in a cluster, running SmartZone in Essentials mode.

One of the functions of a SmartZone Controller is to manage and monitor data tunnels for Access Points managed by the controller. Tunnel options for Access Points include:
- Local Breakout, which means APs forward traffic based on their L2 networks
- SoftGRE, which allows APs to establish a GRE tunnel with a 3rd party partner gateway
- RuckusGRE, which allows APs to establish a RuckusGRE tunnel with SmartZone dataplane products.

SmartZone Dataplane – Integrates with SmartZone controllers providing flexible options for tunnelling of AP traffic. SmartZone Dataplane comes in both physical and virtual form factors. Certain models of the SmartZone physical appliances also have dataplane capabilities (SZ144-D)



Virtualization and Hypervisors

69 | © 2024 CommScope, Inc.

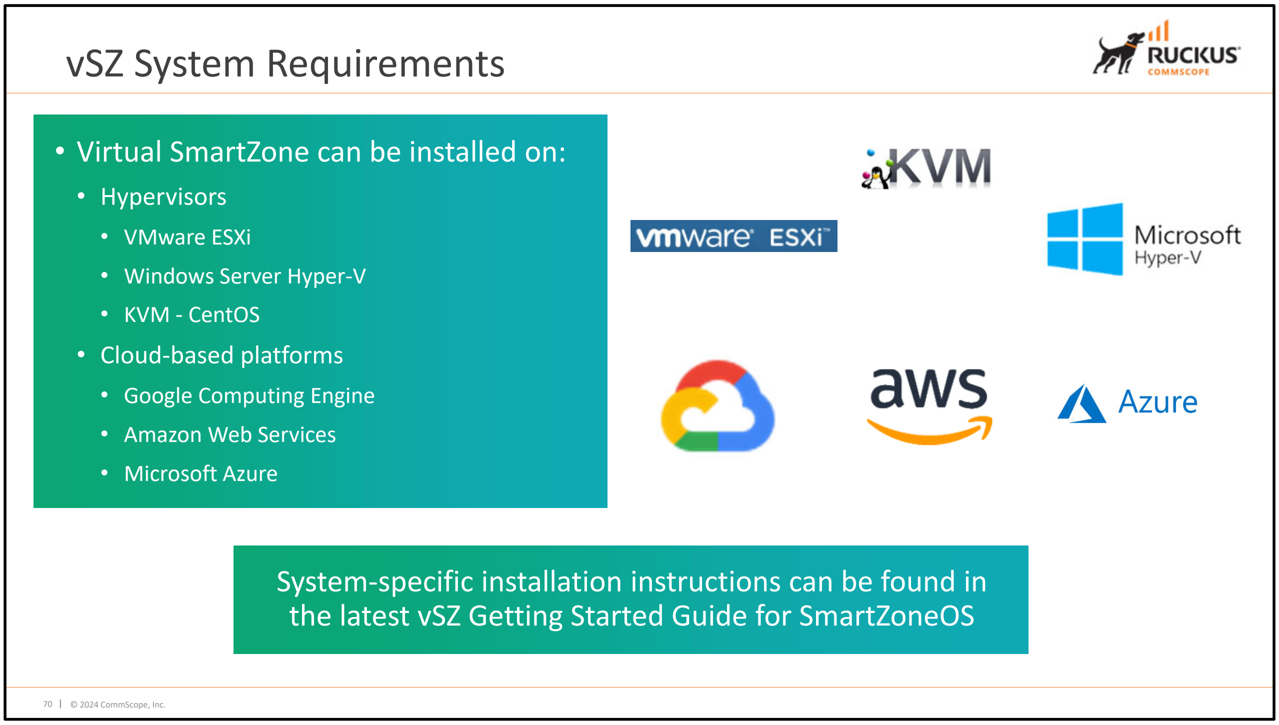
Virtual SmartZone consists of a virtual machine appliance hosted on an x86 server instead of utilizing independent dedicated physical server hardware.

A virtual infrastructure consists of server hardware capable of running virtualization software.
At the time this course was created, the supported platforms include:

- VMWare
- Linux Cent OS
- Microsoft Windows Server

Hypervisors which manage the virtual machines may need to be additionally installed. The corresponding hypervisors for the supported platforms are:
-In VMWare environments vSphere ESXi.
-In Linux environments KVM
-In Microsoft Windows environments Hyper-V
Once the virtual environment is ready the SmartZone controller virtual machine appliance is then installed. It is also possible to install Virtual SmartZone within commercial Cloud services such as: Google Compute Engine, Microsoft Azure and Amazon Web Services.

You can consult the Virtual SmartZone Getting Started Guide for additional information including version requirements and installation steps.



vSZ System Requirements

- Virtual SmartZone can be installed on:
  - Hypervisors
    - VMware ESXi
    - Windows Server Hyper-V
    - KVM - CentOS
  - Cloud-based platforms
    - Google Computing Engine
    - Amazon Web Services
    - Microsoft Azure

System-specific installation instructions can be found in the latest vSZ Getting Started Guide for SmartZoneOS

RUCKUS
COMMSCOPE
KVM
vmware ESXi
Microsoft
Hyper-V
aws
Azure

70 | © 2024 CommScope, Inc.

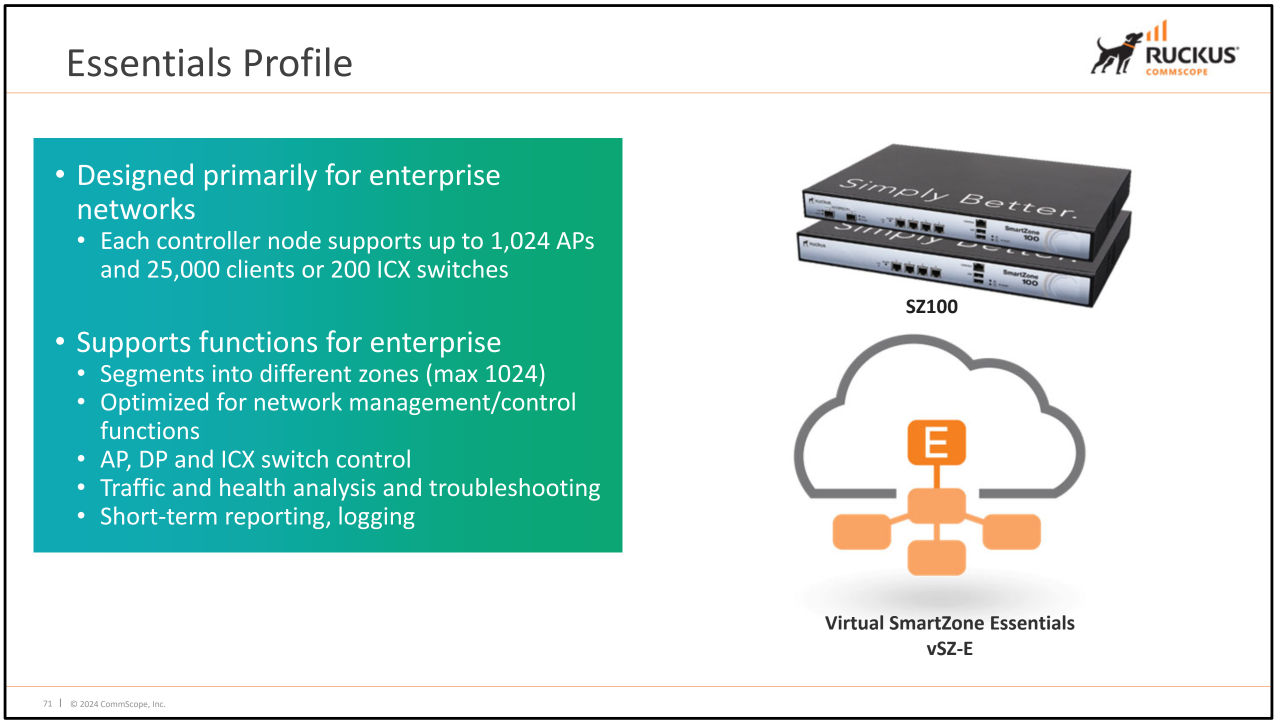
SmartZone is available on several hypervisor platforms, including:

- VMWare ESXi
- Windows Hyper-V
- KVM on CentOS

It is also available for cloud platforms, which include:

- Google Compute Engine
- Amazon Web Services
- Microsoft Azure

Each of the platforms has specific requirements that must be met for proper operation, so be sure to review the Virtual SmartZone Getting Started Guide for this release before installing. As there are several variables to factor in including, but not limited to, the number of virtual CPUs, memory and hard disk space required, keep in mind these factors are based on the number of deployed devices that will be managed by the SmartZone network controller.



Essentials Profile

- Designed primarily for enterprise networks
  - Each controller node supports up to 1,024 APs and 25,000 clients or 200 ICX switches
- Supports functions for enterprise
  - Segments into different zones (max 1024)
  - Optimized for network management/control functions
  - AP, DP and ICX switch control
  - Traffic and health analysis and troubleshooting
  - Short-term reporting, logging

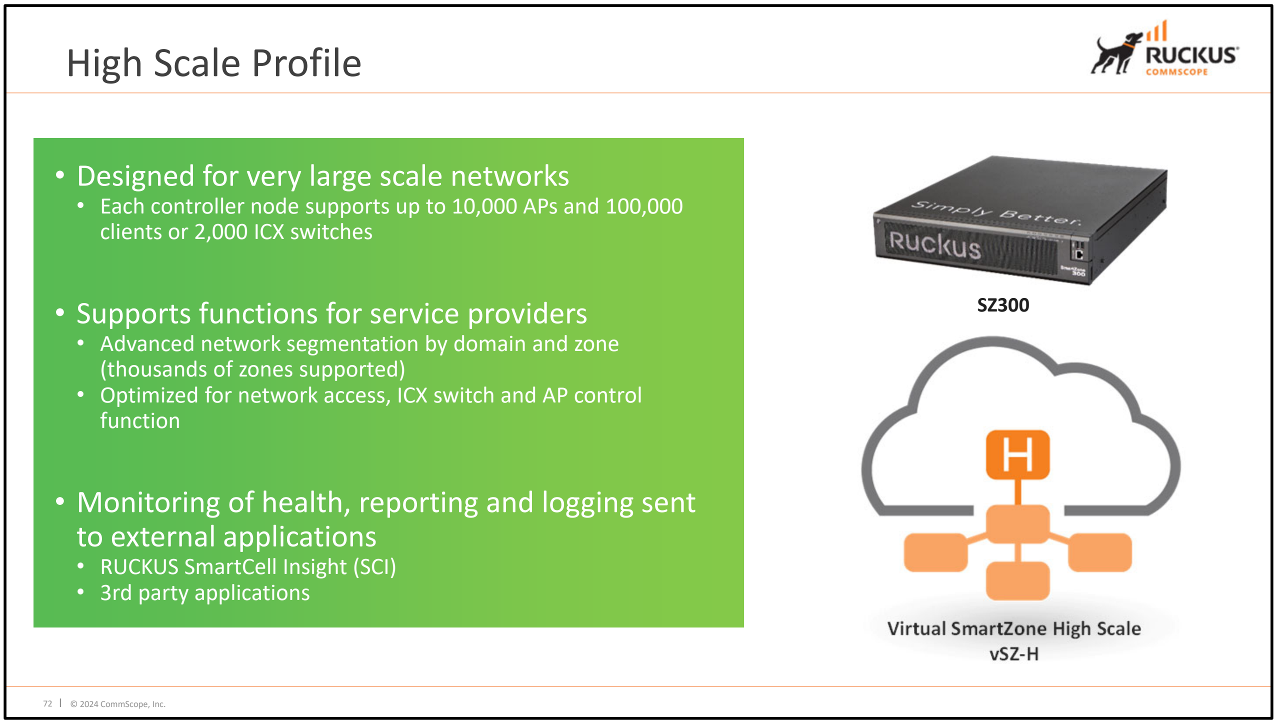
SZ100

Virtual SmartZone Essentials
vSZ-E

71 | © 2024 CommScope, Inc.

Essentials deployments commonly support enterprise, hospitality, education, retail, healthcare, and businesses in many other market types including some small-scale Managed Service Providers (MSPs). Single nodes can support up to 1k APs with 25k clients or 200 ICX switches. Network management and control functions are available along with health analysis and troubleshooting. Short term reporting is also stored with the option to report to external services such as RUCKUS Analytics and other 3rd party applications.

Virtual Essentials and High Scale platforms use the same software package, and the version is simply chosen at the time of deployment to fit your requirements.



High Scale Profile

- Designed for very large scale networks
  - Each controller node supports up to 10,000 APs and 100,000 clients or 2,000 ICX switches
- Supports functions for service providers
  - Advanced network segmentation by domain and zone (thousands of zones supported)
  - Optimized for network access, ICX switch and AP control function
- Monitoring of health, reporting and logging sent to external applications
  - RUCKUS SmartCell Insight (SCI)
  - 3rd party applications

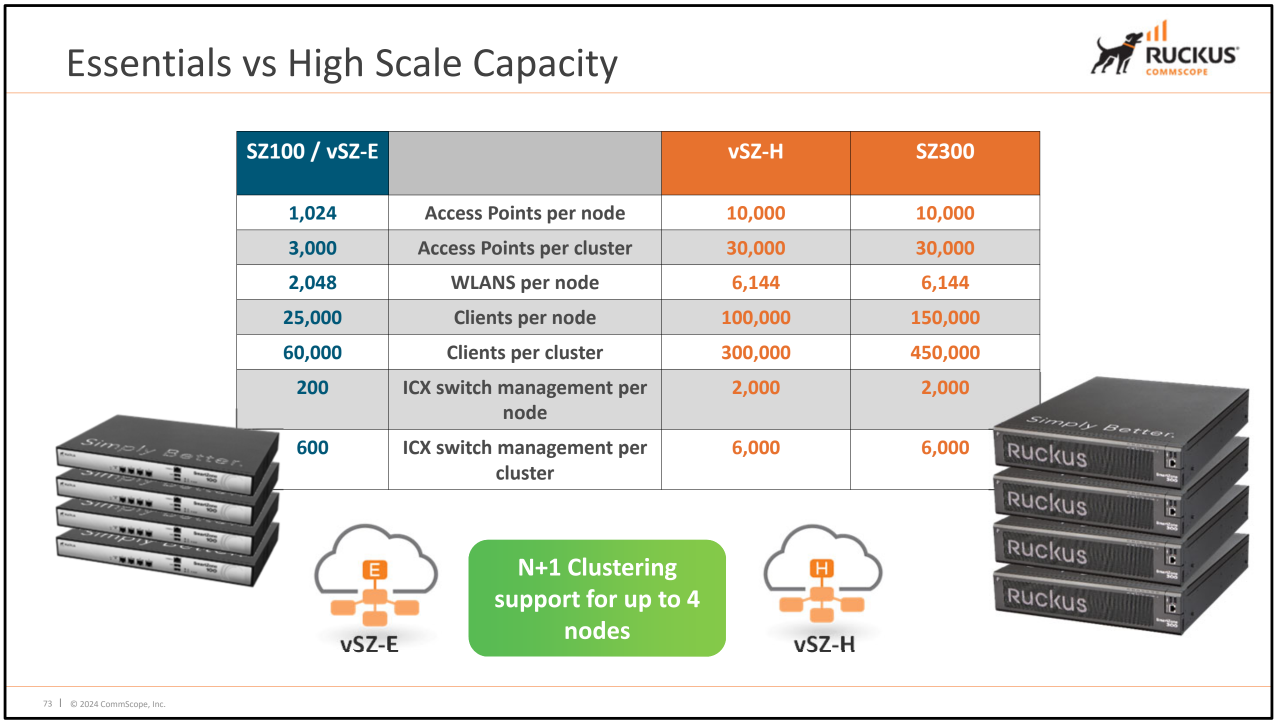
SZ300

Virtual SmartZone High Scale
vSZ-H

72 | © 2024 CommScope, Inc.

High Scale deployments typically are used in large scale environments such as Managed service provider (MSP) or Mobile Virtual Network Operators (MVNO) where a single instance or cluster can provide support for thousands of AP devices along with thousands of clients with additional scalability when clustering is used.

High scale provides additional segmentation by domain (think of them as administrative domains) in addition to zones providing an ability to provide segmented management and control of many clients while maintaining unique settings for each. High scale is also designed to efficiently provide health reporting, traffic analysis and logging to external management applications like RUCKUS Analytics.



Essentials vs High Scale Capacity

SZ100 / vSZ-E		vSZ-H	SZ300
1,024	Access Points per node	10,000	10,000
3,000	Access Points per cluster	30,000	30,000
2,048	WLANS per node	6,144	6,144
25,000	Clients per node	100,000	150,000
60,000	Clients per cluster	300,000	450,000
200	ICX switch management per node	2,000	2,000
600	ICX switch management per cluster	6,000	6,000

vSZ-E

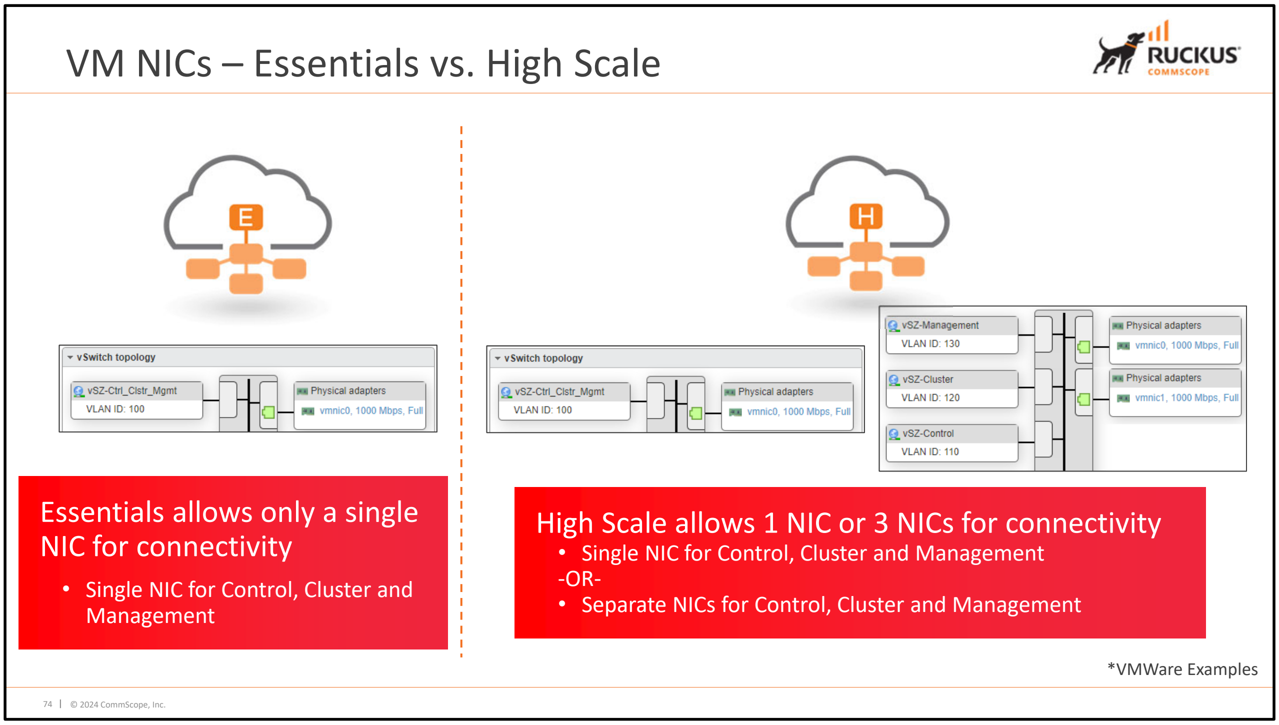
N+1 Clustering support for up to 4 nodes

vSZ-H

73 | © 2024 CommScope, Inc.

This table shows the differences in capacity between the Essentials and High Scale platform. The platforms remain functionally much the same with some operational differences.

Clustering of appliance or virtual deployments regardless of the chosen profile increases the capacity of SZ while providing additional redundancy.



VM NICs – Essentials vs. High Scale

Essentials allows only a single NIC for connectivity

- Single NIC for Control, Cluster and Management

High Scale allows 1 NIC or 3 NICs for connectivity

- Single NIC for Control, Cluster and Management

-OR-

- Separate NICs for Control, Cluster and Management

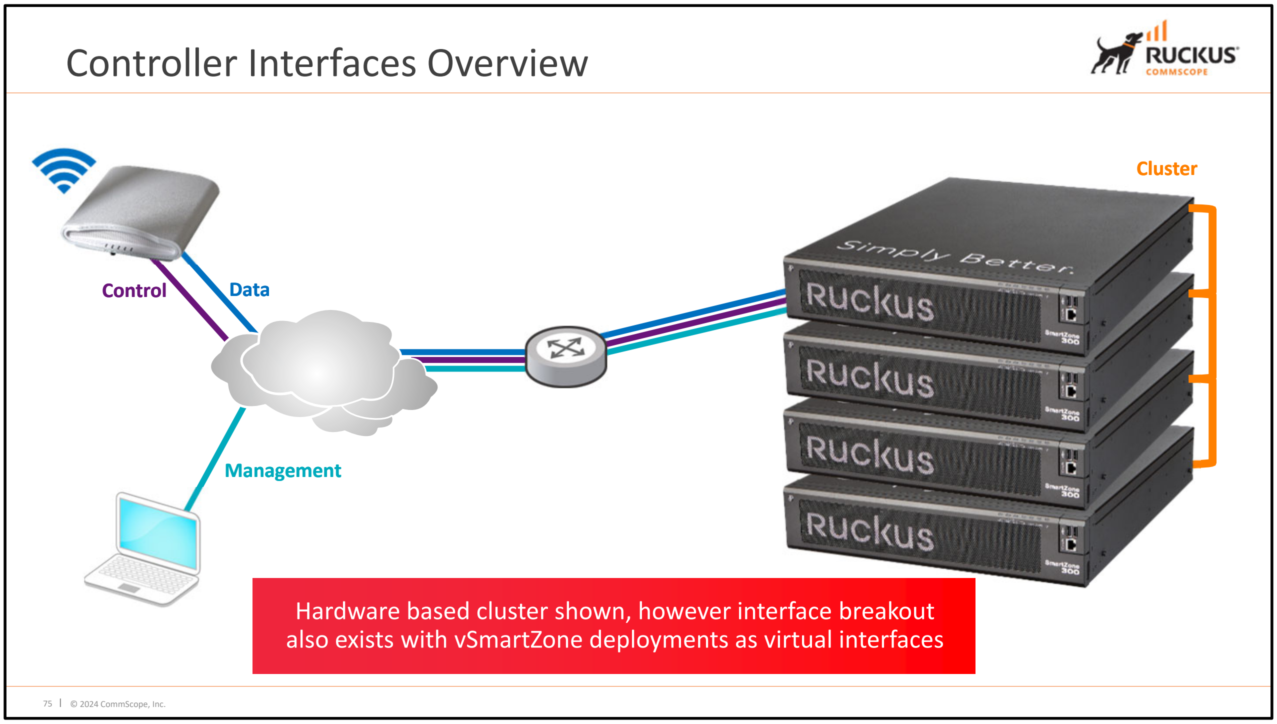
*VMWare Examples

74 |

The Virtual SmartZone Essentials edition of the network controller only allows the use of a single virtual NIC on a hypervisor. This single NIC will provide connectivity for the Control, Cluster and Management planes.

The High Scale edition allows some flexibility in this way. You can configure it with a single NIC for providing connectivity to Control, Cluster and Management planes or it can be configured with three virtual NICs with each providing connectivity for only one the operational planes.

In this VMWare deployment example, the Essentials and single-NIC High Scale, a single port group to provide connectivity. For the High Scale 3-NIC example, there are three separate port groups, one for each NIC/function. The decision of how to deploy the High Scale edition is made during initial setup and cannot be altered after the setup operation is complete.



Controller Interfaces Overview

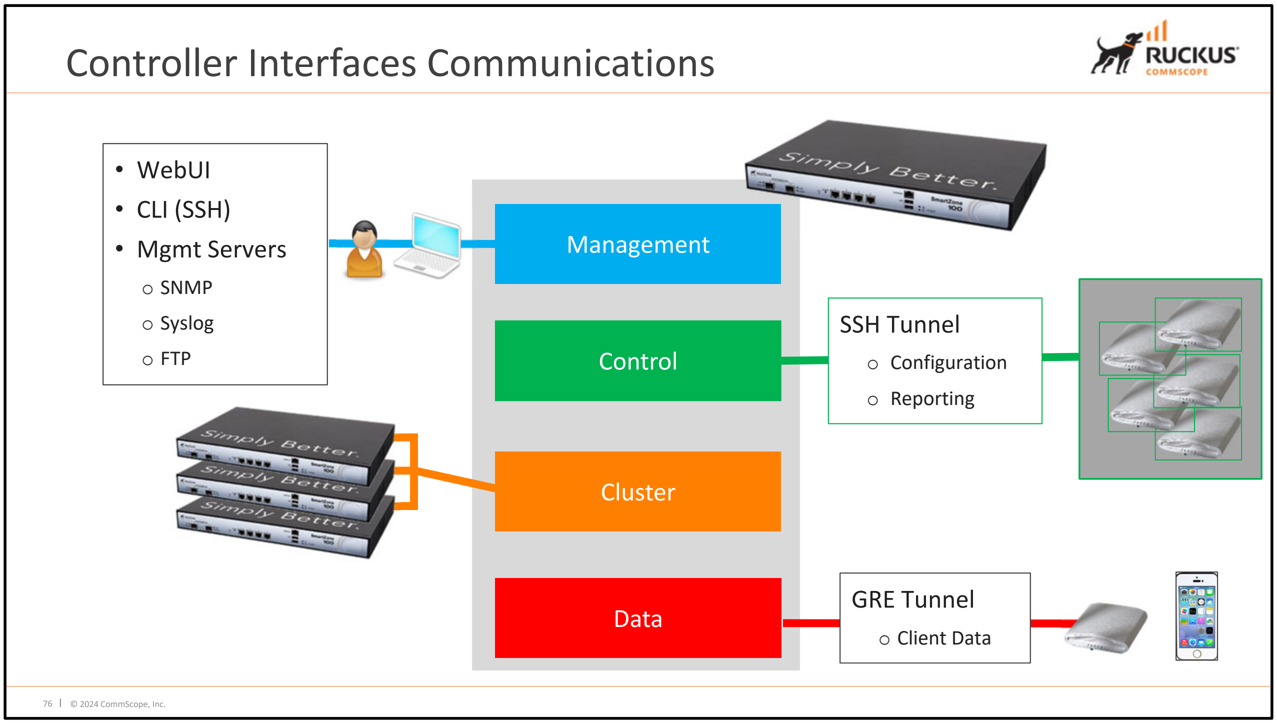
Hardware based cluster shown, however interface breakout also exists with vSmartZone deployments as virtual interfaces

75 |

SmartZone controllers communicate over network interfaces that can be dedicated to specific communication types. They are found in the web interface under the Cluster settings, and so are collectively known as the Cluster Planes. The four interfaces are:

- Management
- Control
- Cluster
- Data

Note: SmartZone essentials uses a single NIC for Control, Cluster and Management Traffic. It is also possible to use a single NIC configuration within high scale.



Controller Interfaces Communications

- WebUI
- CLI (SSH)
- Mgmt Servers
  - SNMP
  - Syslog
  - FTP

Management

Control

Cluster

Data

SSH Tunnel
- Configuration
- Reporting

GRE Tunnel
- Client Data

The SmartZone Controller interfaces perform the following functions:

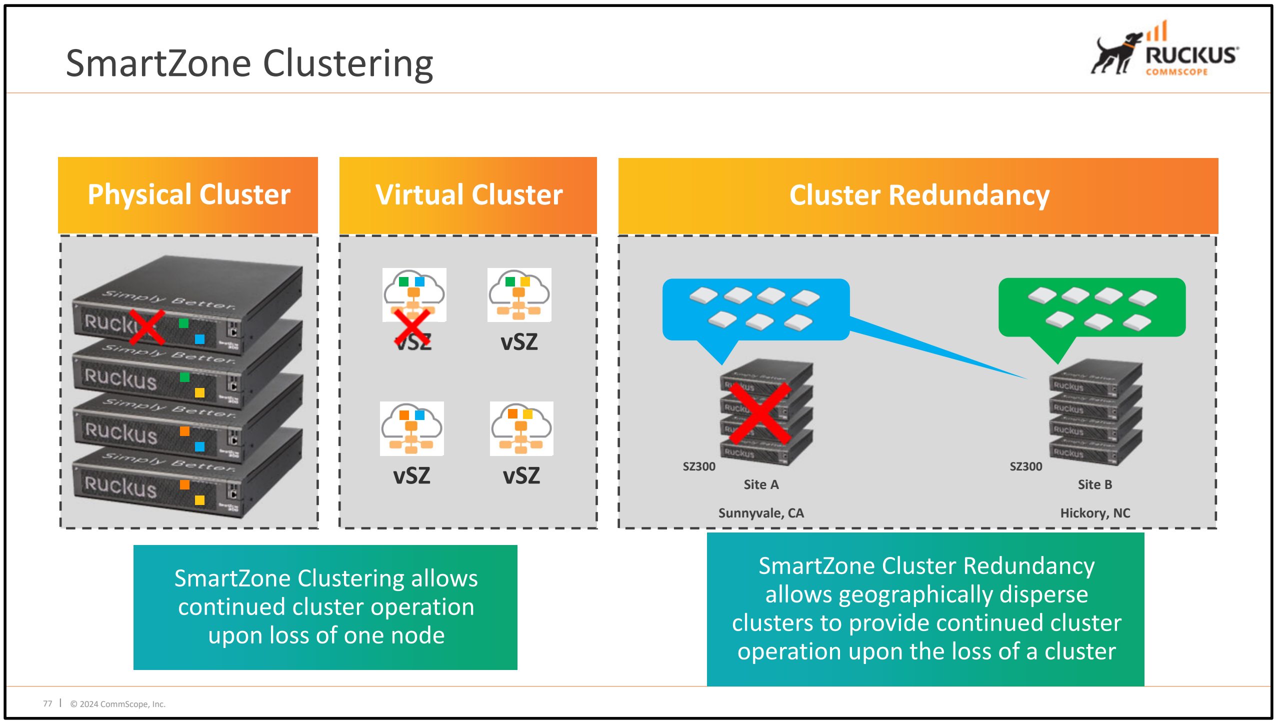
- **Management**: The Web interface that you log in to is accessed via the Management interface, as is the CLI. Services, such as SNMP, Syslog and FTP also communicate via the Management interface.

- **Control**: The Access Points you deploy will communicate with the controller over the Control interface, primarily via an SSH tunnel. Access Point configuration changes are delivered to the Access Points via the tunnel, and reporting and statistics are delivered to the controller.

- **Cluster**: Multiple controllers configured as a cluster will communicate using the Cluster interface. This interface is used exclusively for cluster communications and requires good bandwidth and latency. It's not recommended that cluster nodes are geographically separated.

- **Data**: The Data interface is used in limited cases where you want to tunnel all the client data. This interface is natively built into the SmartZone hardware appliance and its features can be enhanced by use of a dedicated Virtual or Physical SmartZone DataPlane.

Virtual SmartZone does give you the option to deploy using a single virtual interface for Control, Clustering, and Management.



SmartZone Clustering

Physical Cluster

Virtual Cluster

Cluster Redundancy

SmartZone Clustering allows continued cluster operation upon loss of one node

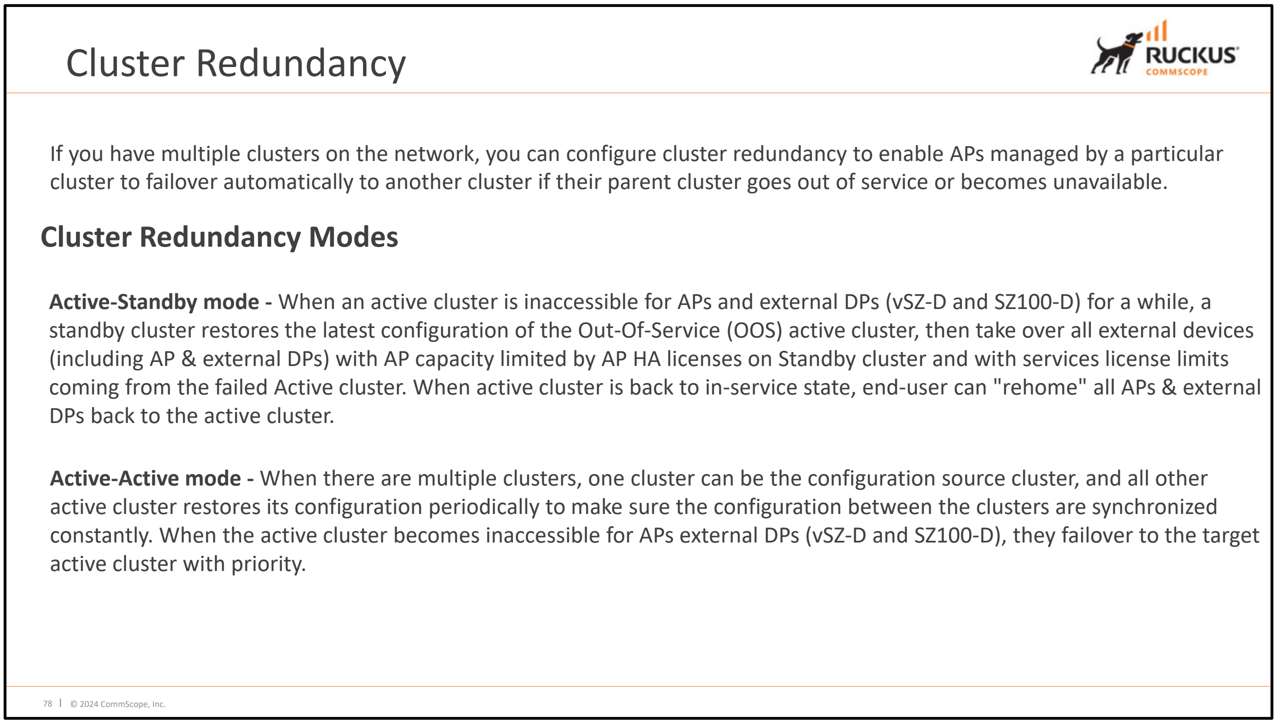
SmartZone Cluster Redundancy allows geographically disperse clusters to provide continued cluster operation upon the loss of a cluster

77 | © 2024 CommScope, Inc.

SmartZone Clustering

SmartZone controllers support clustering of up to 4 nodes for N+1 redundancy. Physical and virtual appliances running either essentials or high scale can be clustered, but all cluster members should of the same type running the same software. The cluster is active/active meaning that all nodes in the cluster provide management services to their associated APs. The cluster shares a database between all members and in the event of node failure , management functions and operations previously performed by the failed node, continue to be provided by the remaining cluster members.

SmartZone Cluster Redundancy introduces an additional level of high availability which allows multiple SmartZone clusters, geographically independent of one another, to perform as active/active or active/standby in one-to-one or many-to-one environments. Cluster redundancy members will synchronize configurations with each other and in the event of a cluster failure the remaining cluster will takeover control of APs and even SmartZone Dataplane tunnels. Cluster redundancy is supported only on SmartZone 300 and vSZ-H appliances. The Standby controllers will need an AP-High Availability license.



Cluster Redundancy

If you have multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to failover automatically to another cluster if their parent cluster goes out of service or becomes unavailable.

Cluster Redundancy Modes

Active-Standby mode - When an active cluster is inaccessible for APs and external DPs (vSZ-D and SZ100-D) for a while, a standby cluster restores the latest configuration of the Out-Of-Service (OOS) active cluster, then take over all external devices (including AP & external DPs) with AP capacity limited by AP HA licenses on Standby cluster and with services license limits coming from the failed Active cluster. When active cluster is back to in-service state, end-user can "rehome" all APs & external DPs back to the active cluster.

Active-Active mode - When there are multiple clusters, one cluster can be the configuration source cluster, and all other active cluster restores its configuration periodically to make sure the configuration between the clusters are synchronized constantly. When the active cluster becomes inaccessible for APs external DPs (vSZ-D and SZ100-D), they failover to the target active cluster with priority.

78 | © 2024 CommScope, Inc.

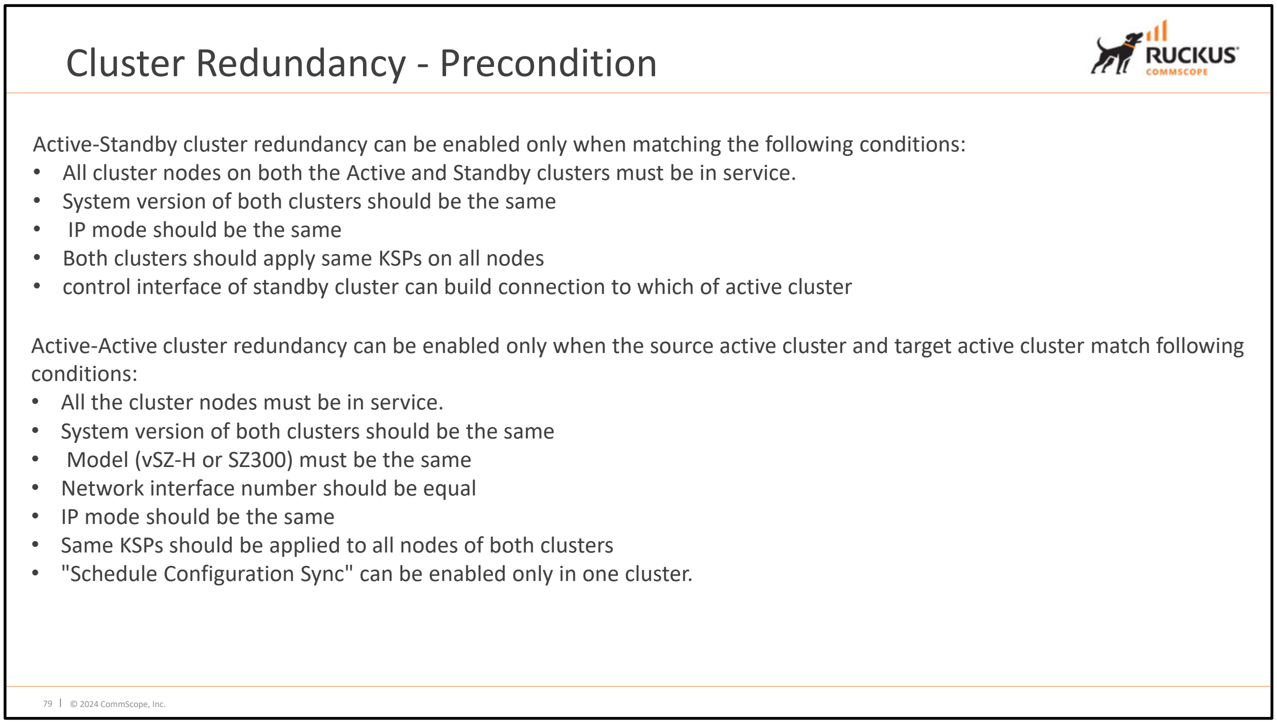
If you have multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to failover automatically to another cluster if their parent cluster goes out of service or becomes unavailable.

Active-Standby mode - When an active cluster is inaccessible for APs and external DPs (vSZ-D and SZ144-D) for a while, a standby cluster restores the latest configuration of the Out-Of-Service (OOS) active cluster, then take over all external devices (including AP & external DPs) with AP capacity limited by AP HA licenses on Standby cluster and with services license limits coming from the failed Active cluster. When active cluster is back to in-service state, end-user can "rehome" all APs & external DPs back to the active cluster.

Active-Active mode - When there are multiple clusters, one cluster can be the configuration source cluster, and all other active cluster restores its configuration periodically to make sure the configuration between the clusters are synchronized constantly. When the active cluster becomes inaccessible for APs external DPs (vSZ-D and SZ144-D), they failover to the target active cluster with priority.

NOTE: Cluster redundancy is supported only on SZ300 and vSZ-H and failover works only for external DPs (vSZ-D and SZ144-D).

A single standby cluster serves as a failover option for one or many distributed active clusters. Different AAA servers can be configured on active and standby clusters.



Cluster Redundancy - Precondition

Active-Standby cluster redundancy can be enabled only when matching the following conditions:

- All cluster nodes on both the Active and Standby clusters must be in service.
- System version of both clusters should be the same
- IP mode should be the same
- Both clusters should apply same KSPs on all nodes
- control interface of standby cluster can build connection to which of active cluster

Active-Active cluster redundancy can be enabled only when the source active cluster and target active cluster match following conditions:

- All the cluster nodes must be in service.
- System version of both clusters should be the same
- Model (vSZ-H or SZ300) must be the same
- Network interface number should be equal
- IP mode should be the same
- Same KSPs should be applied to all nodes of both clusters
- "Schedule Configuration Sync" can be enabled only in one cluster.

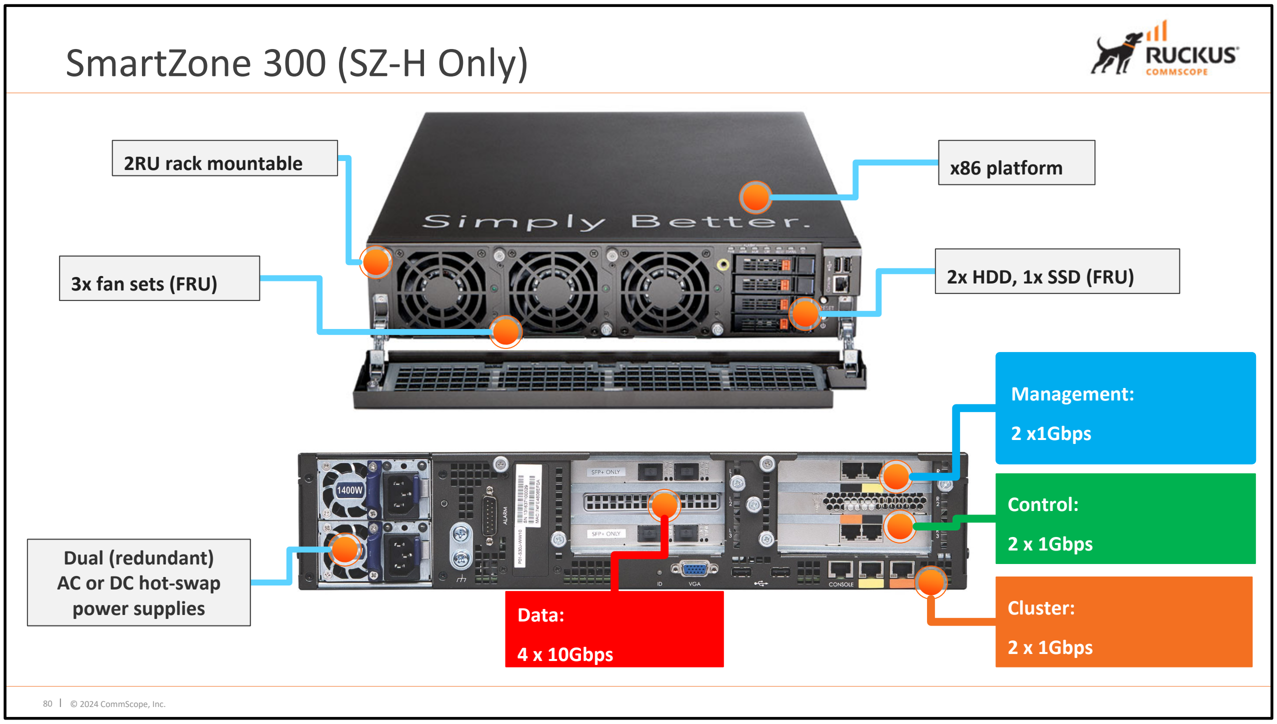
79 | © 2024 CommScope, Inc.

Active-Standby cluster redundancy can be enabled only when matching the following conditions:

- All cluster nodes on both the Active and Standby clusters must be in service.
- System version of both clusters should be the same
- IP mode should be the same
- Both clusters should apply same KSPs on all nodes
- Control interface of standby cluster must be configured to connect to an active cluster

Active-Active cluster redundancy can be enabled only when the source active cluster and target active cluster match following conditions:

- All the cluster nodes must be in service.
- System version of both clusters should be the same
- Model (vSZ-H or SZ300) must be the same
- Network interface number should be equal
- IP mode should be the same
- Same KSPs should be applied to all nodes of both clusters
- "Schedule Configuration Sync" can be enabled only in one cluster.



SmartZone 300 (SZ-H Only)

2RU rack mountable

x86 platform

3x fan sets (FRU)

2x HDD, 1x SSD (FRU)

Management:

2 x1Gbps

Control:

2 x 1Gbps

Cluster:

2 x 1Gbps

Dual (redundant) AC or DC hot-swap power supplies

Data:

4 x 10Gbps

80 | © 2024 CommScope, Inc.

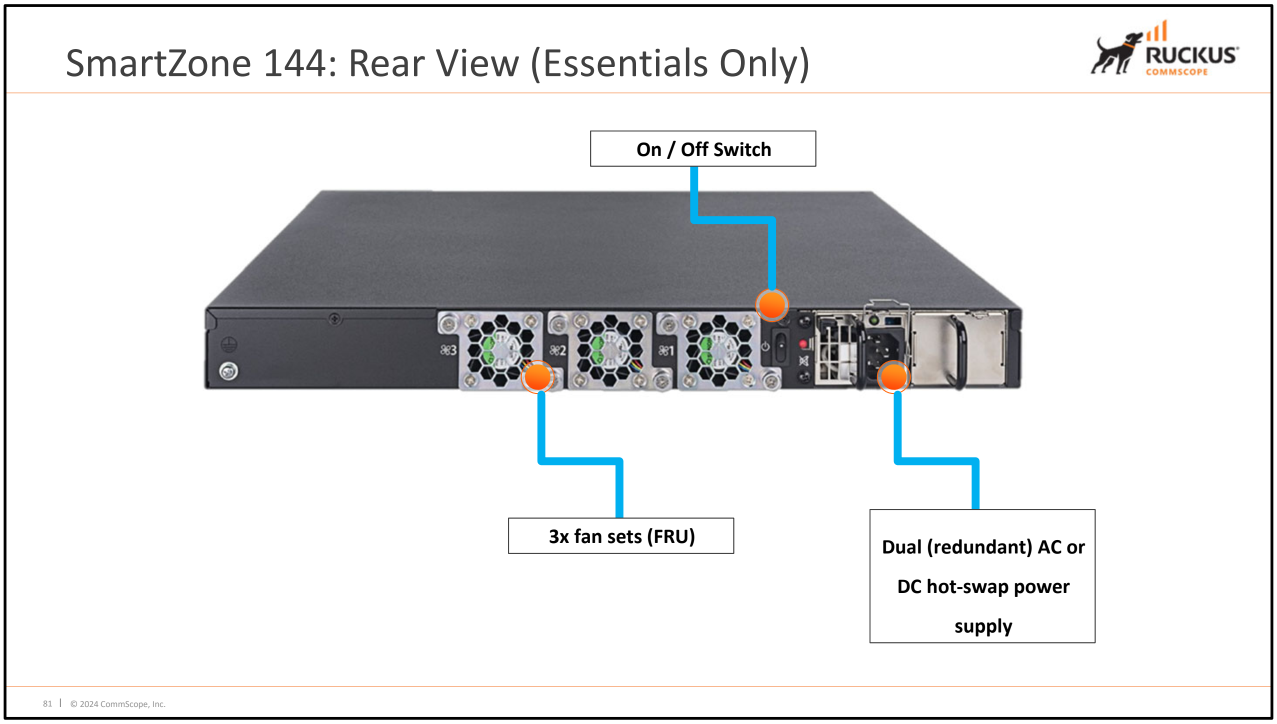
The RUCKUS SmartZone 300 is a high performance, high availability hardware platform designed for large scale critical carrier networks.

The 2u rack mountable chassis opens from the front to allow access to:

- Field-replaceable fans
- Redundant disk drives

The rear of the chassis contains:

- Dual redundant hot-swappable power supplies
- Management, Control, Cluster and Data Plane ports



SmartZone 144: Rear View (Essentials Only)

On / Off Switch

3x fan sets (FRU)

Dual (redundant) AC or DC hot-swap power supply

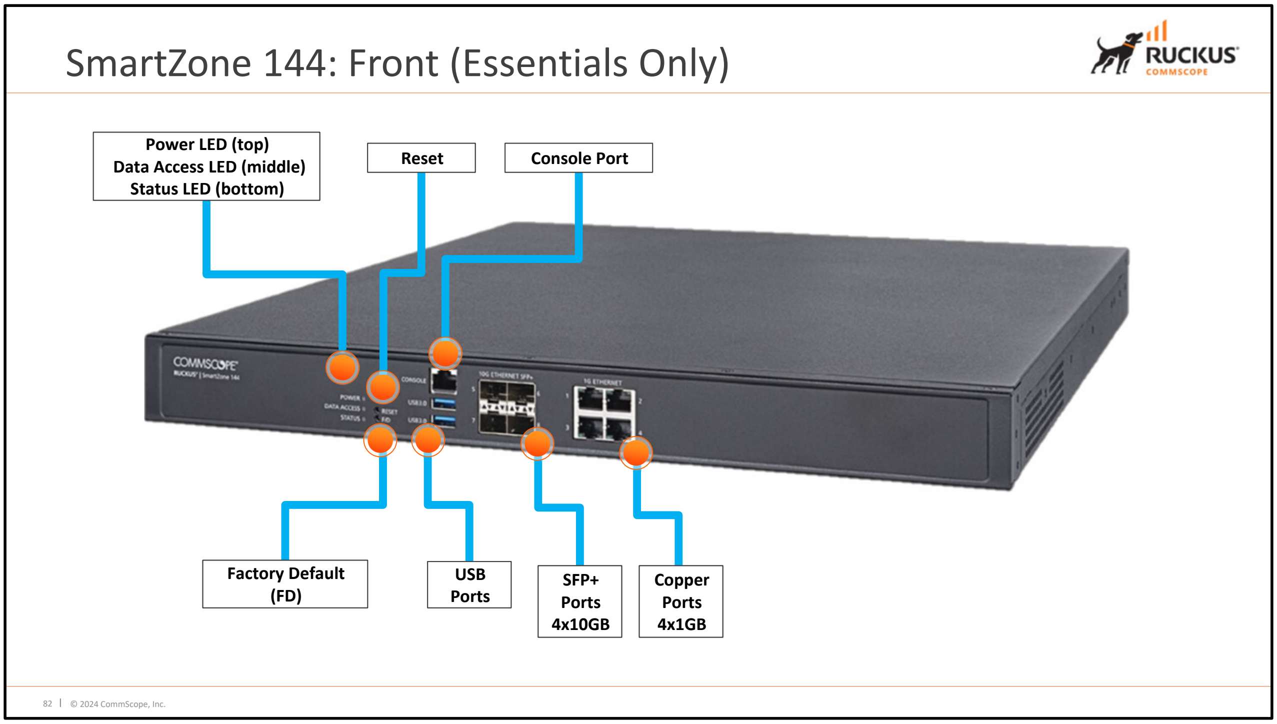
81 | © 2024 CommScope, Inc.

Now let’s look at the SmartZone 144.

SmartZone™ 144 (SZ-144) is the next-generation high-performing Wireless LAN controller within the CommScope Ruckus family of products.

The rear of the SmartZone 144 chassis contains:

- Single power supply (and includes the ability to add an additional power supply for redundancy)
- Incorporated on/off switch
- Redundant fans



SmartZone 144: Front (Essentials Only)

Power LED (top)
Data Access LED (middle)
Status LED (bottom)

Reset

Console Port

Factory Default (FD)

USB Ports

SFP+ Ports 4x10GB

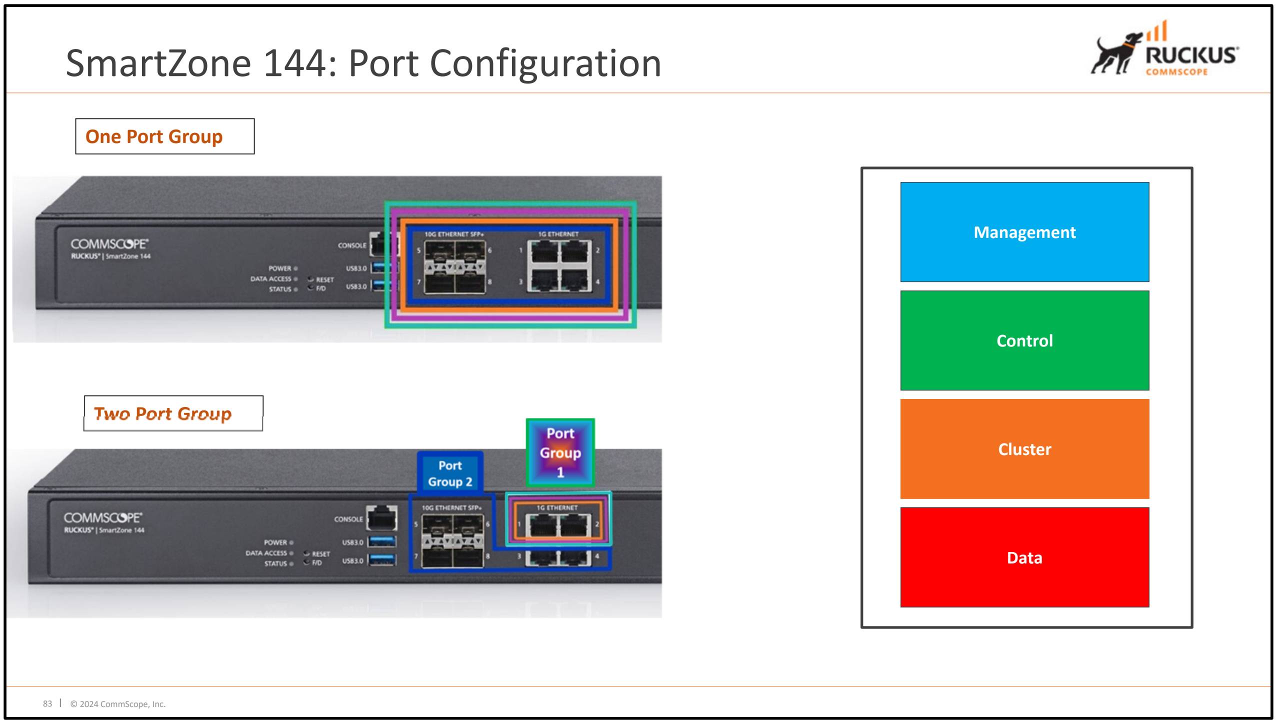
Copper Ports 4x1GB

Let’s tour the front of the SmartZone 144 chassis.

The front of the SmartZone 144 contains:

- Power, Data access, and Status LEDs
- A Reset button (used for restarting the device)
- An F/D button (used for resetting the device back to factory default)
- A Console port
- Two USB 3.0 ports
- Four 10-Gigabit Ethernet SFP+ ports
- Four 1-Gigabit Ethernet RJ-45 copper ports

In fact, the fours in the name SmartZone 144 denote its four SFP Ethernet ports and four Copper Ethernet ports.



SmartZone 144: Port Configuration

One Port Group

Two Port Group

Management

Control

Cluster

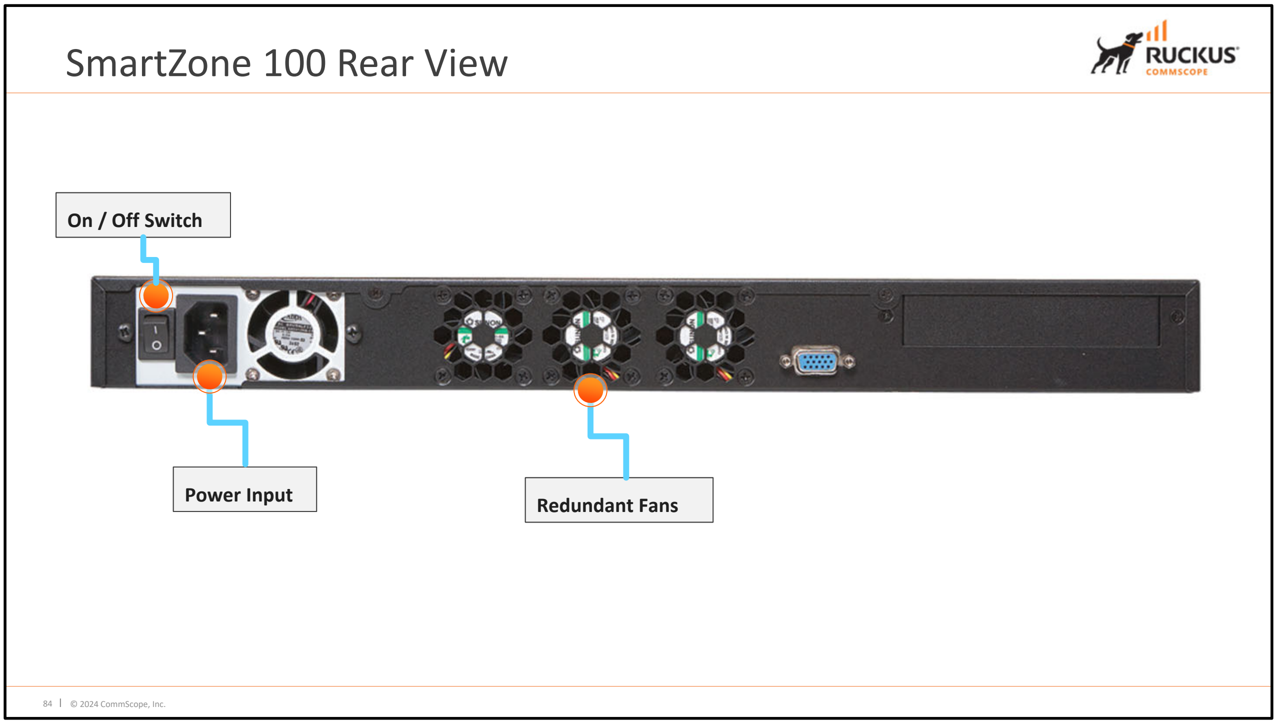
Data

83 | © 2024 CommScope, Inc.

The eight Gigabit Ethernet Ports on the SmartZone 144 can be configured as either One Port Group or Two Port Groups.

In a One Port Group, Management and AP tunnel traffic are combined. All of the interfaces are bridged and all management, control, cluster, and data traffic will flow through a single active port on the bridged interface. The interfaces are not a LAG and do not aggregate the traffic – only one port will be active, though others can be used for redundancy.

In a Two Port Group, Port Group 1 (PG1) is used for Management and AP control while Port Group 2 (PG2) is used for AP tunnel data.

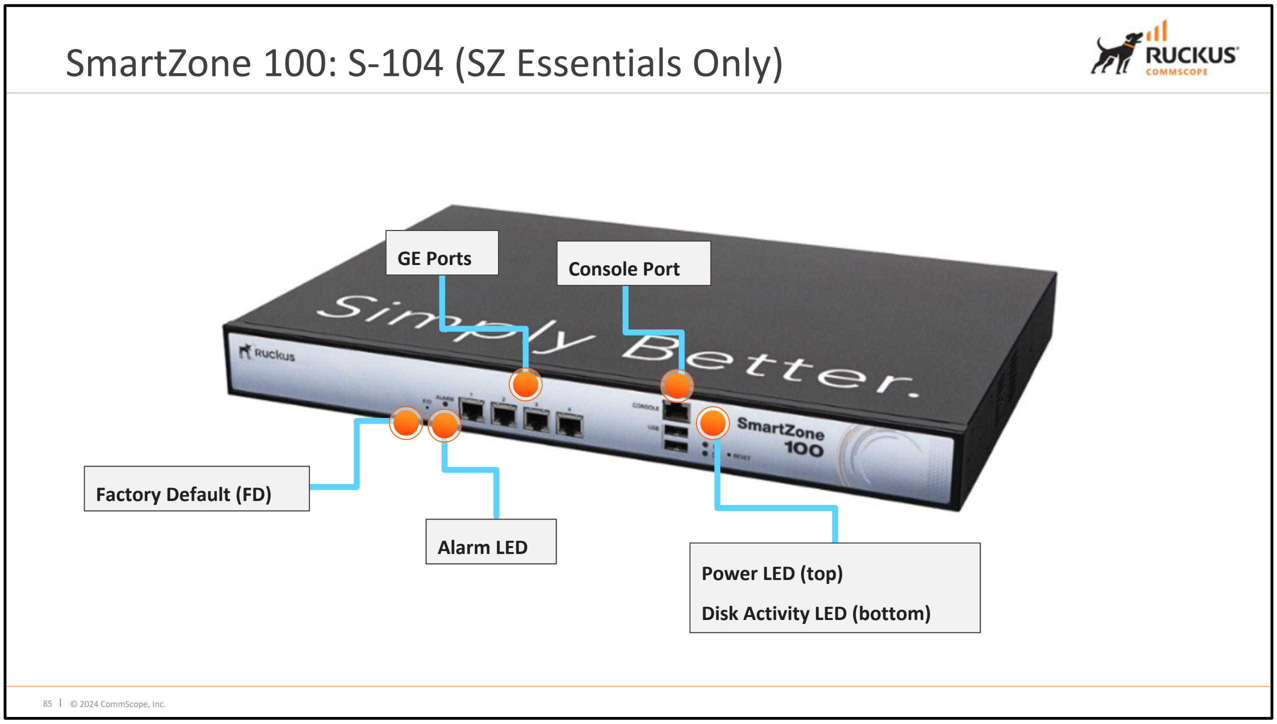


SmartZone 100 Rear View

84 | © 2024 CommScope, Inc.

The SmartZone 100 is supplied in two versions. For both, the rear is the same. It contains:

- Single power supply
- Incorporated on/off switch
- Redundant fans



SmartZone 100: S-104 (SZ Essentials Only)

GE Ports

Console Port

Factory Default (FD)

Alarm LED

Power LED (top)

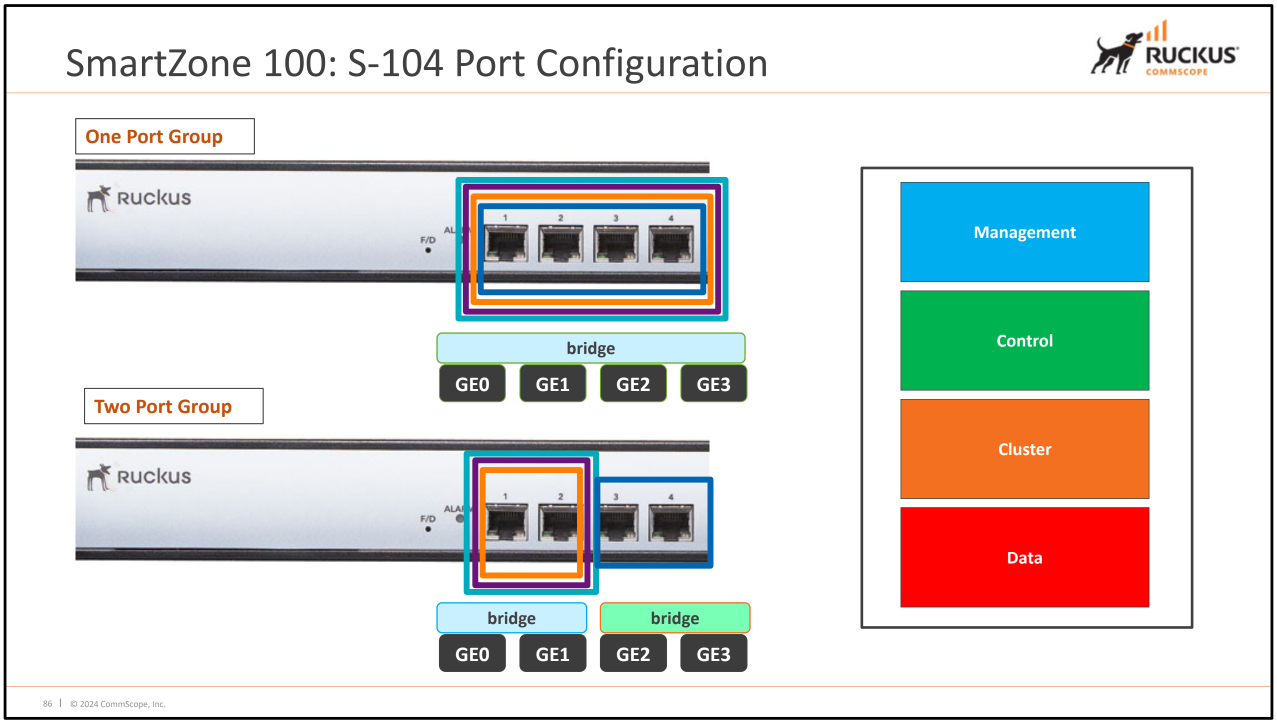
Disk Activity LED (bottom)

85 | © 2024 CommScope, Inc.

The first variant of the SmartZone 100 is the S-104. The 4 in 104 denotes the addition of 4x1Gb ethernet ports

The front chassis of the SZ-104 contains:

- Factory default pinhole
- Alarm led
- 4 x Gigabit Ethernet ports
- Console port
- Power and led activity lights



SmartZone 100: S-104 Port Configuration

One Port Group

bridge

GE0 GE1 GE2 GE3

Two Port Group

bridge | bridge

GE0 GE1 GE2 GE3

Management

Control

Cluster

Data

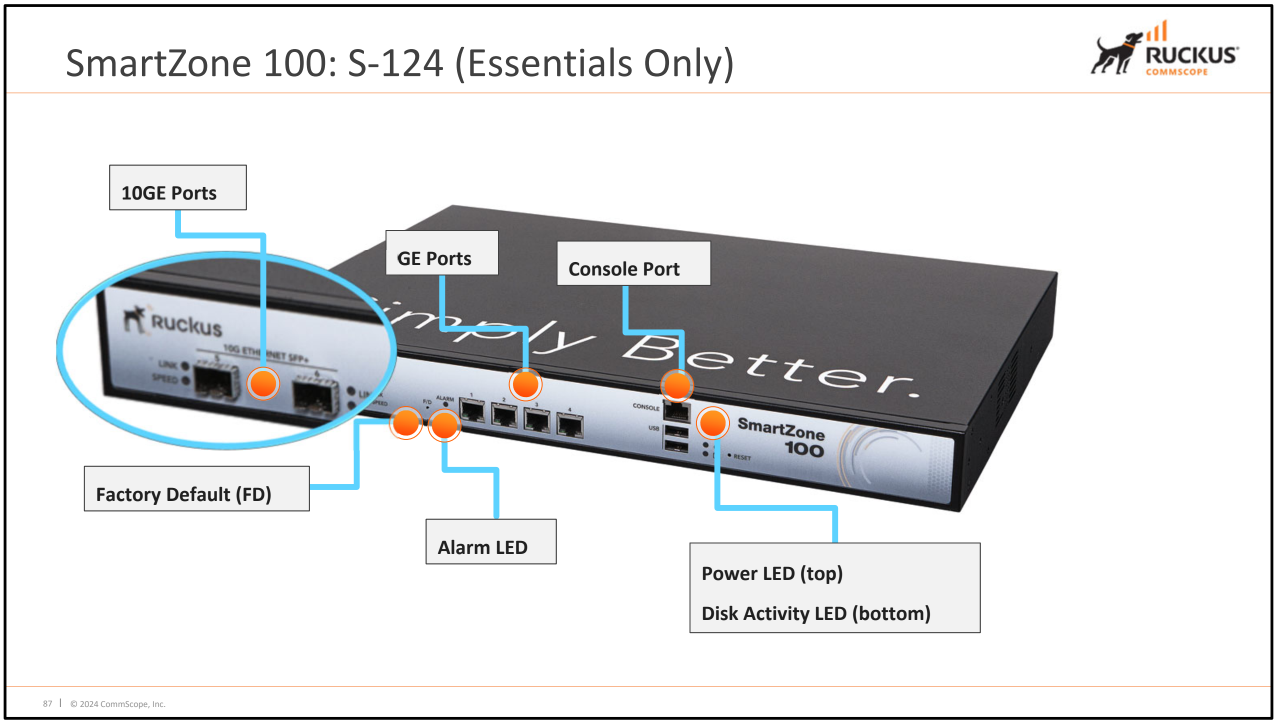
86 | © 2024 CommScope, Inc.

The 4 x Gigabit Ethernet Ports on the SmartZone 100: S-104 can be configured as either:

- One Port Group
- Two Port Group

In a One Port Group, all of the interfaces are bridged and all management, control, cluster and data traffic will flow through a single active port on the bridged interface. The interfaces are not a LAG and do not aggregate the traffic – only one port will be active, though others can be used for redundancy.

In a Two Port Group, the first and second ports are bridged and used for management, control and cluster traffic, while the third and fourth ports used for data traffic.



SmartZone 100: S-124 (Essentials Only)

10GE Ports

GE Ports

Console Port

Factory Default (FD)

Alarm LED

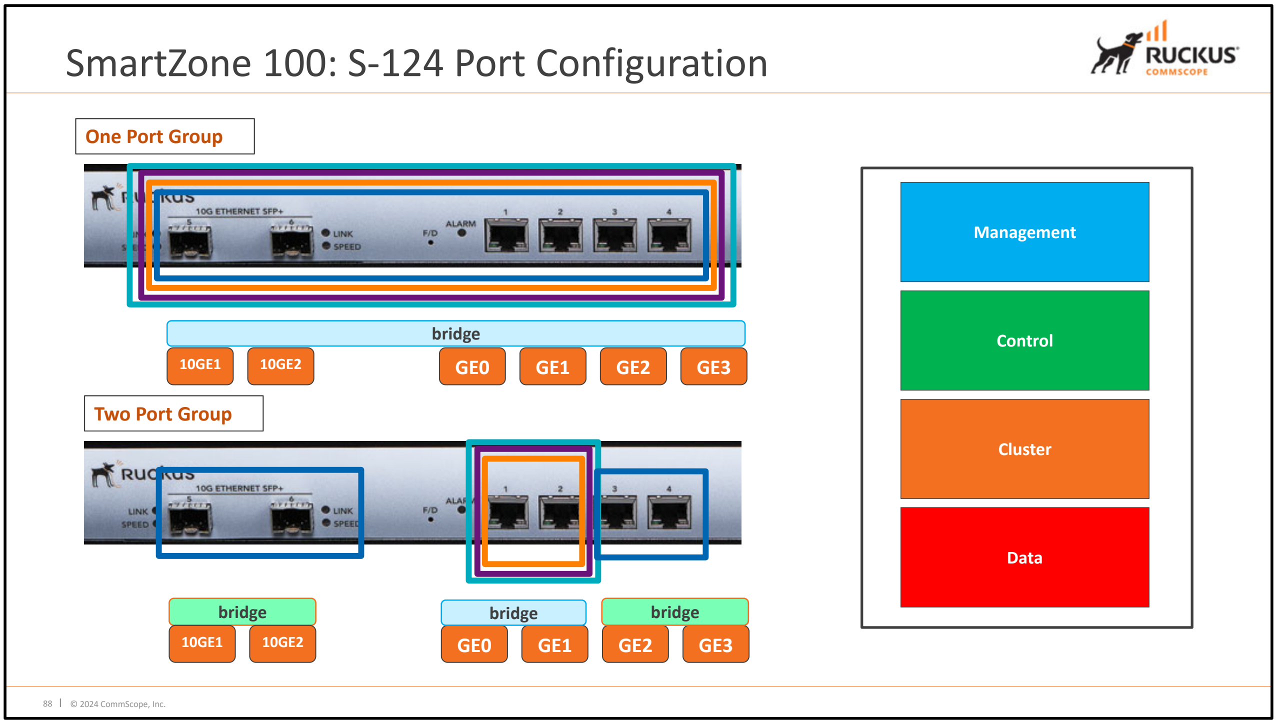
Power LED (top)

Disk Activity LED (bottom)

87 | © 2024 CommScope, Inc.

The second variant of the SmartZone 100 is the S-124. The 2 in 124 denotes the additional of 2x10Gb ports, where as we stated the 4 is for the 4x1Gb ports.
As with the S-104, the S-124 contains the same rear and front features.

S-124 additionally includes 2 x 10 Gigabit SFP+ ports

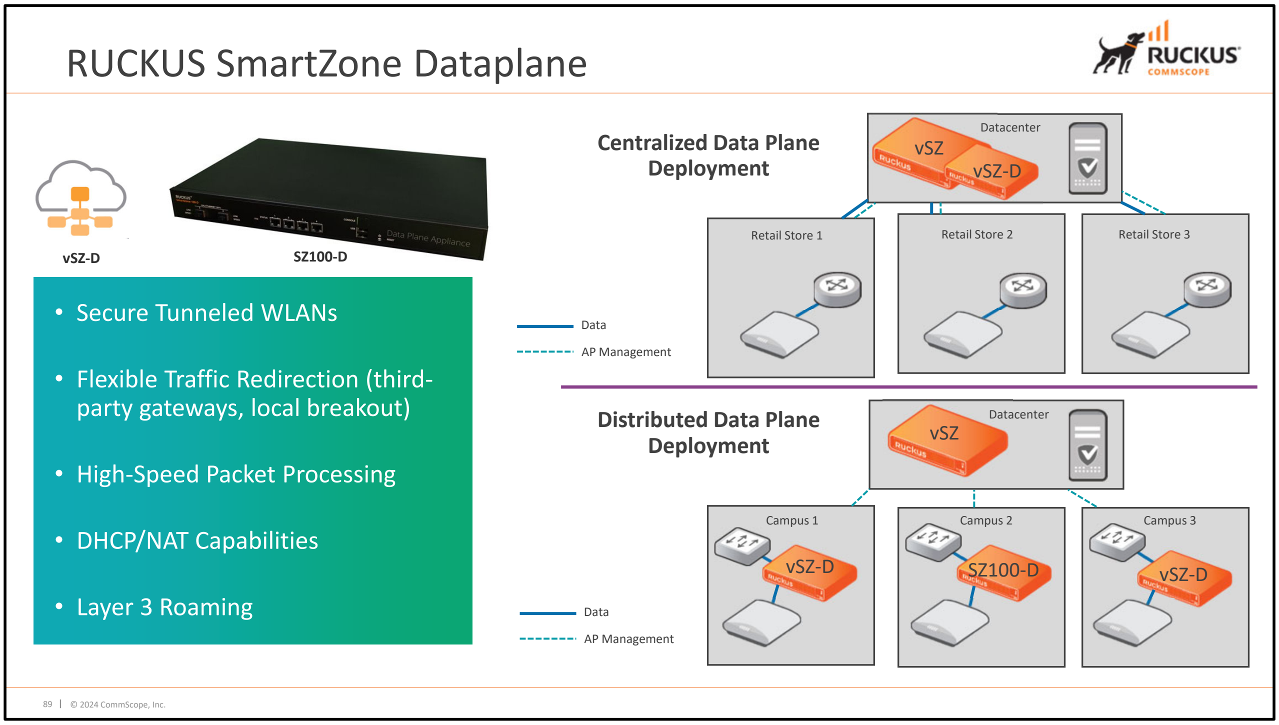


Similarly, to the S-104 the The 4 x Gigabit Ethernet and 2 x 10GB Ports on the S-124 can be configured as:

- One Port Group
- Two Port Group

In a One Port Group configuration, all of the interfaces including the 2 x 10GB ports are bridged and all management, control, cluster and data traffic will flow through a single active port on the bridged interface. The interfaces are not a LAG and do not aggregate the traffic – only one port will be active, though others can be used for redundancy.

In a Two Port Group, as with the S-100, the first and second ports are bridged and used for management, control and cluster traffic, and the third and fourth ports used for data traffic, with the addition of the two 10GB ports.



RUCKUS SmartZone Dataplane

- Secure Tunneled WLANs
- Flexible Traffic Redirection (third-party gateways, local breakout)
- High-Speed Packet Processing
- DHCP/NAT Capabilities
- Layer 3 Roaming

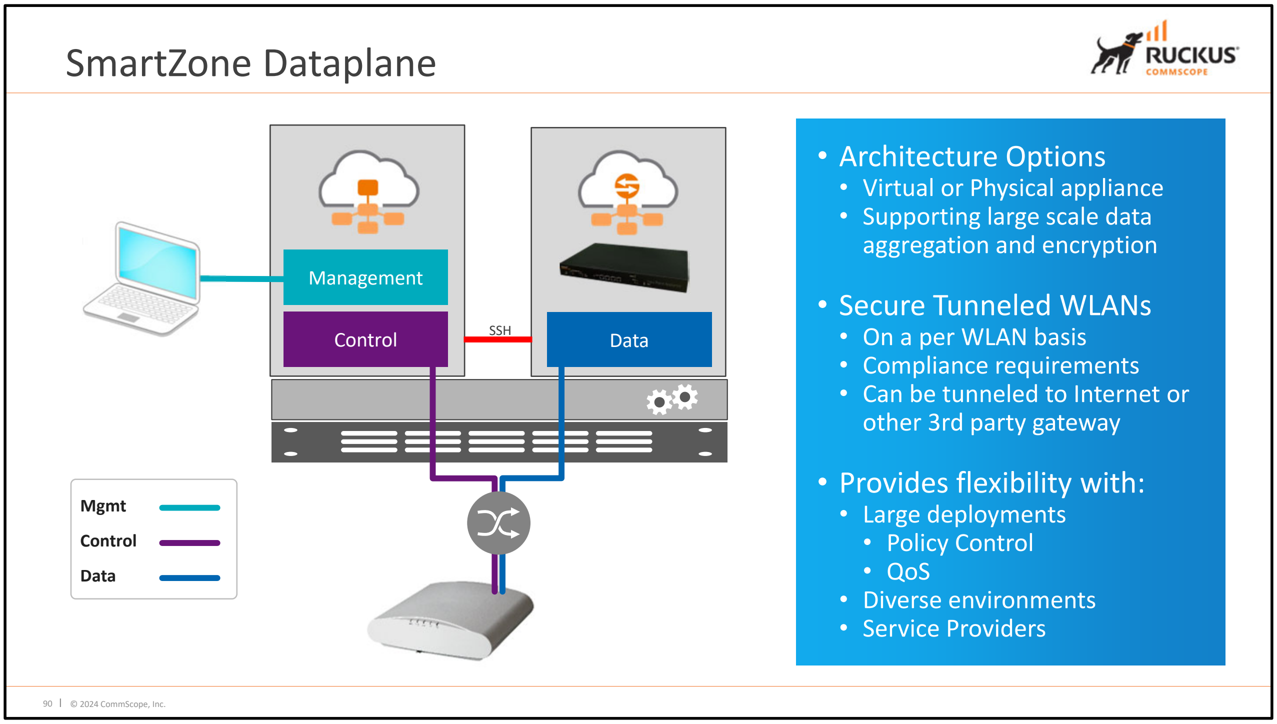
89 | © 2024 CommScope, Inc.

Ruckus SmartZone Dataplane is a scalable wireless LAN data plane appliance that comes in virtual and physical form factors. SmartZone Dataplane enables:
-Per WLAN forwarding of user traffic through secure tunnels, third-party gateways
-Scalable High Speed Packet Processing
-DHCP, NAT, and Layer 3 roaming functions

SmartZone Dataplane appliances integrate with SmartZone for seamless management, and can be deployed alongside SmartZone in a datacenter, or in remote tenant locations allowing for flexibility with either centralized or distributed deployments.

Dataplane can be used to tunnel traffic for lawful intercept, to ensure protection of personal information or to apply policies to WLAN traffic.

SmartZone Dataplane can scale up to 10,000 tunnels on a single instance and supports 10 SmartZone Dataplane instances per SmartZone controller. Clustered SmartZone controller environments can support up to 40 Dataplane instances.
Throughput for SmartZone Dataplane is scalable starting with a base throughput of 1Gbps with options to increase to 10Gbps or higher.



SmartZone Dataplane

- Architecture Options
  - Virtual or Physical appliance
  - Supporting large scale data aggregation and encryption
- Secure Tunneled WLANs
  - On a per WLAN basis
  - Compliance requirements
  - Can be tunneled to Internet or other 3rd party gateway
- Provides flexibility with:
  - Large deployments
    - Policy Control
    - QoS
  - Diverse environments
  - Service Providers

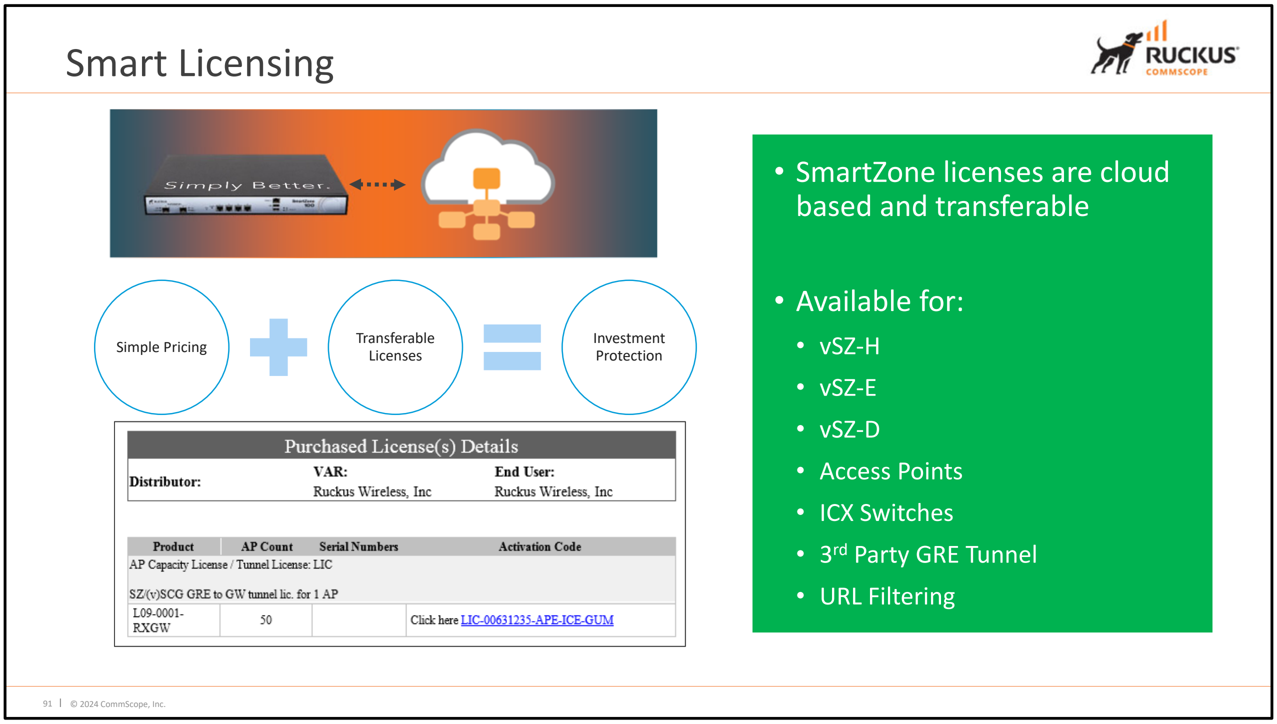
90 |

The vSZ-Dataplane is a separate virtual machine or physical appliance that provides enhanced Data Plane functionality within virtual SmartZone, for both vSZ-E and vSZ-H. SmartZone Dataplane is managed via SmartZone Controller and once deployed, offers secured tunneling, on a per WLAN basis, of user data traffic with encryption from RUCKUS APs to the SmartZone dataplane appliance. This allows administrators flexibility to create a tunnel for WLAN guest traffic for additional security filtering, while wireless POS data traffic can be tunneled separately for PCI compliance.

With SmartZone Dataplane administrators can maintain flat WLAN topologies by enabling L2/L3 roaming, while preserving client IP addresses without the need for additional mobility controllers. vSZ-D can perform DHCP/NAT functions and includes per site policy control and QoS capabilities helpful for large deployments, or diverse multi-tenant environments.

SmartZone dataplane can be deployed alongside SmartZone controllers in the datacenter for a centralized deployment or distributed in remote/regional locations allowing flexibility in data forwarding. For instance a school district a may prefer to deploy physical or virtual SmartZone Dataplane instances at each of their school campuses allowing them to tunnel AP traffic back to their datacenter for centralized inspection.

Deployments of SZ in public cloud services such as AWS benefit from vSZ Data Plane as well by forwarding the traffic in a local environment if proxy or VOIP services are being used.


Simply Better.
Simple Pricing
Transferable Licenses
Investment Protection

Smart Licensing

Purchased License(s) Details		
Distributor:	**VAR:** Ruckus Wireless, Inc	**End User:** Ruckus Wireless, Inc

Product	AP Count	Serial Numbers	Activation Code
AP Capacity License / Tunnel License: LIC SZ/(v)SCG GRE to GW tunnel lic. for 1 AP			
L09-0001-RXGW	50		Click here LIC-00631235-APE-ICE-GUM

- SmartZone licenses are cloud based and transferable
- Available for:
  - vSZ-H
  - vSZ-E
  - vSZ-D
  - Access Points
  - ICX Switches
  - 3rd Party GRE Tunnel
  - URL Filtering

91 | © 2024 CommScope, Inc.

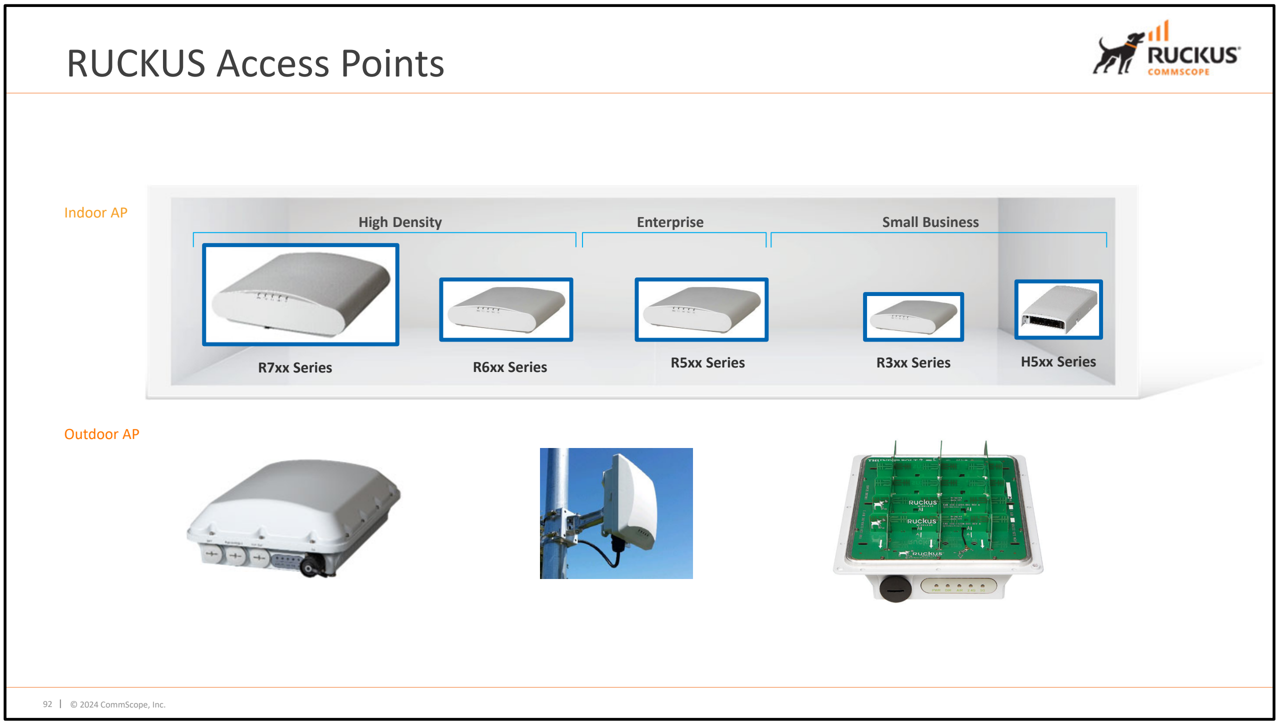
Once a deployment platform has been decided, you will need to consider licensing.

Licenses are required for, but not limited to:

- Virtual SmartZone controllers
- Virtual SmartZone Data Plane
- Access Points
- ICX Switches
- Non-RUCKUS GRE Tunnels
- URL Filtering

Flexible license options give organizations the freedom to manage licensing according to their business needs. Licenses are available per Access Point, are cloud managed using the LiMAN (license management) portal and are transferable, within the same product family. The SmartZone controller syncs with LiMAN automatically once every 24 hours or can be manually sync'd and applies the licenses associated to your device.

Note: The RUCKUS LiMAN portal can be accessed through the RUCKUS Support portal. If you would like to know more, you should view the Smart Licencing course on the RUCKUS Training portal. Additionally check out the RUCKUS Education channel on Youtube for quick hits on licensing subjects.



RUCKUS Access Points

92 | © 2024 CommScope, Inc.

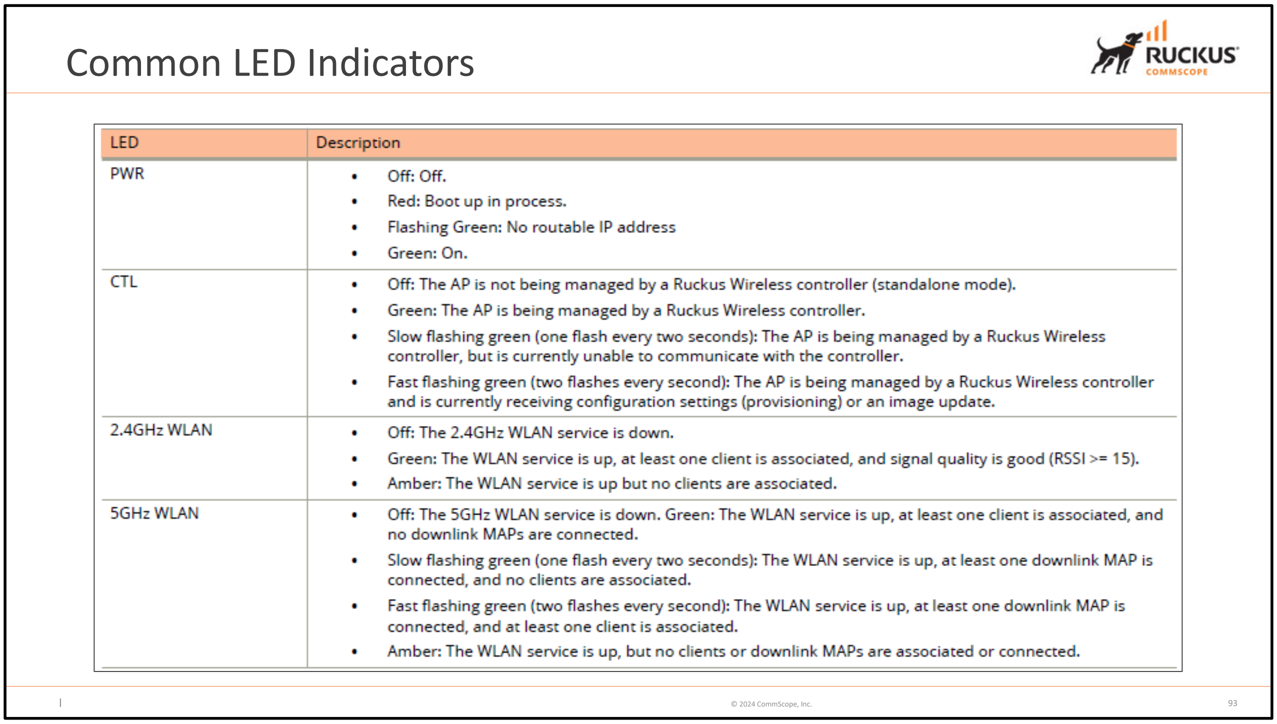
RUCKUS SmartZone controllers manage Ruckus Access Points. This provides a solution for every deployment scenario from Small Business WLANs to mission-critical, high-density carrier grade installations.

The H series APs are omni-directional and are typically deployed in hospitality environments where one AP is used per room. These APs have multiple additional ethernet ports to support connections for devices like IPTV or Voice over IP phones and can provide PoE power, reducing the amount of cabling required in the infrastructure.

The enterprise and high-density APs are also omni-directional and each model has differences in number of transmitters, receivers and spatial streams. As well as the amount of throughput and client types supported as well as other features such as multi-gig ports for additional uplink capacity.

The T- series APs also know as RUCKUS Outdoor Access Points are used in a range of environments mounting and antenna options to suit your needs. These APs provide Point-to-Bridges connectivity between remote sites. The APs are semi-directional. They have varying beamwidths based on the application needed and are more suitable for an environment with extreme environmental conditions.

For a full overview of Ruckus indoor and outdoor Access Points, please refer to the CommScope website for more details.

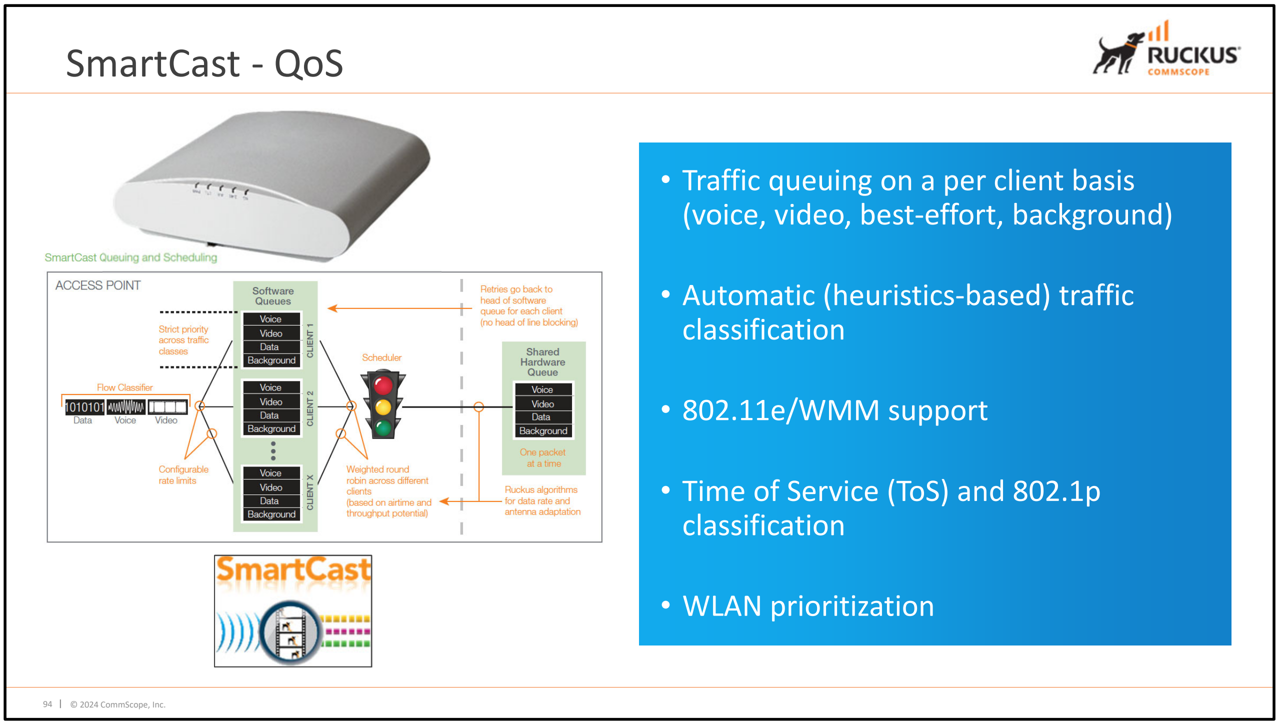


Common LED Indicators

LED	Description
PWR	- Off: Off. - Red: Boot up in process. - Flashing Green: No routable IP address - Green: On.
CTL	- Off: The AP is not being managed by a Ruckus Wireless controller (standalone mode). - Green: The AP is being managed by a Ruckus Wireless controller. - Slow flashing green (one flash every two seconds): The AP is being managed by a Ruckus Wireless controller, but is currently unable to communicate with the controller. - Fast flashing green (two flashes every second): The AP is being managed by a Ruckus Wireless controller and is currently receiving configuration settings (provisioning) or an image update.
2.4GHz WLAN	- Off: The 2.4GHz WLAN service is down. - Green: The WLAN service is up, at least one client is associated, and signal quality is good (RSSI >= 15). - Amber: The WLAN service is up but no clients are associated.
5GHz WLAN	- Off: The 5GHz WLAN service is down. Green: The WLAN service is up, at least one client is associated, and no downlink MAPs are connected. - Slow flashing green (one flash every two seconds): The WLAN service is up, at least one downlink MAP is connected, and no clients are associated. - Fast flashing green (two flashes every second): The WLAN service is up, at least one downlink MAP is connected, and at least one client is associated. - Amber: The WLAN service is up, but no clients or downlink MAPs are associated or connected.

The table in the above slide display the common LED indicators present on the RUCKUS indoor APs. LEDs indicates connection status of:

1. APs power supply
2. Controller connection
3. Clients Connection
4. WLAN services
5. Routable IPs



SmartCast - QoS

RUCKUS
COMMSCOPE
SmartCast Queuing and Scheduling
ACCESS POINT
Software Queues
Voice
Video
Data
Background
CLIENT 1
CLIENT 2
CLIENT X
Strict priority across traffic classes
Flow Classifier
1010101
Data
Voice
Video
Configurable rate limits
Scheduler
Weighted round robin across different clients (based on airtime and throughput potential)
Retries go back to head of software queue for each client (no head of line blocking)
Shared Hardware Queue
One packet at a time
Ruckus algorithms for data rate and antenna adaptation
SmartCast

- Traffic queuing on a per client basis (voice, video, best-effort, background)
- Automatic (heuristics-based) traffic classification
- 802.11e/WMM support
- Time of Service (ToS) and 802.1p classification
- WLAN prioritization

94 |

SmartCast is a superset of the IEEE 802.11e/ (Wi-Fi MultiMedia) WMM hardware-based queuing standard, ensuring uncompromised performance while remaining standards-compliant.

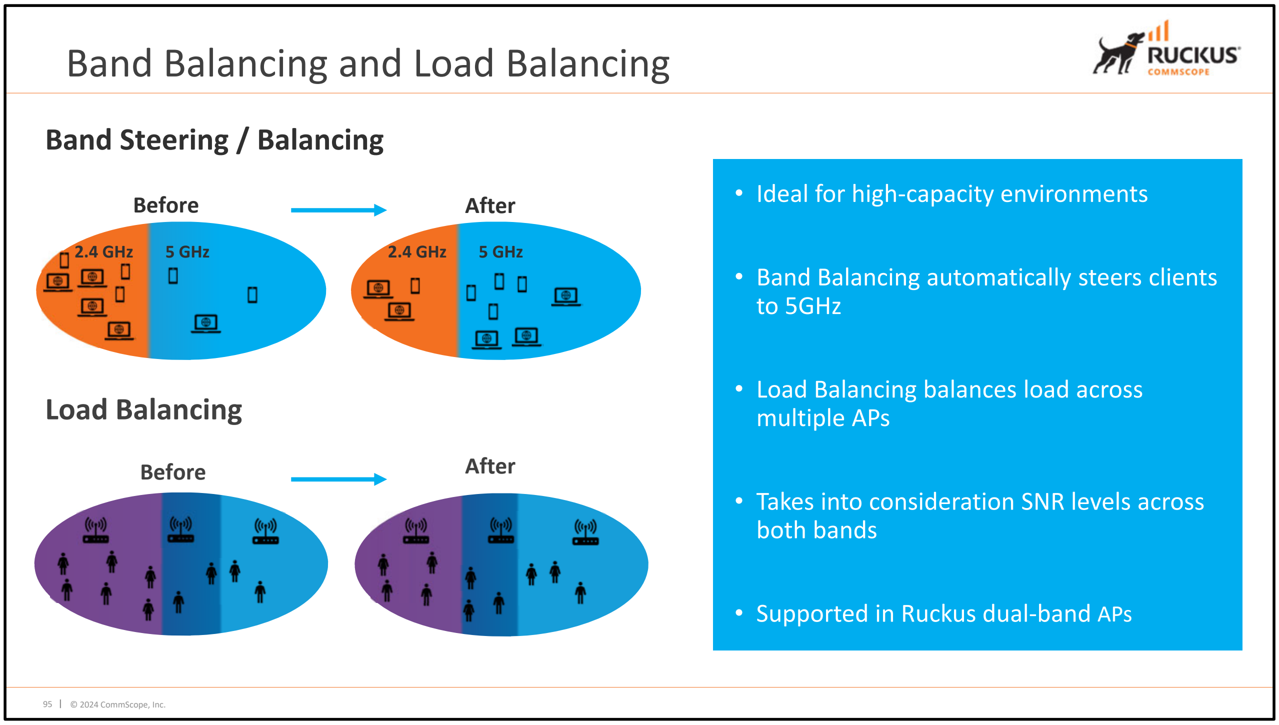
With per-client queuing, SmartCast is ideal for video and voice over Wi-Fi. It ensures disruptive clients don't negatively effect the performance of others clients on the network.

SmartCast automatically utilizes Quality of Service (QoS) mechanisms to ensure that WLAN traffic is processed and transmitted in the most efficient manner possible.

It is a powerful, sophisticated, application-aware classification engine, that provides per-client scheduling and prioritization for WLANs

SmartCast eliminates jitter and delay for video and voice, providing quality of service and outstanding user experience.

SmartCast is the only proven QoS system for IPTV, as it can convert multicast traffic to unicast at the AP, delivering video traffic to individual subscribers at the highest data rate that the client is capable of supporting.



Band Balancing and Load Balancing

Band Steering / Balancing

Load Balancing

- Ideal for high-capacity environments
- Band Balancing automatically steers clients to 5GHz
- Load Balancing balances load across multiple APs
- Takes into consideration SNR levels across both bands
- Supported in Ruckus dual-band APs

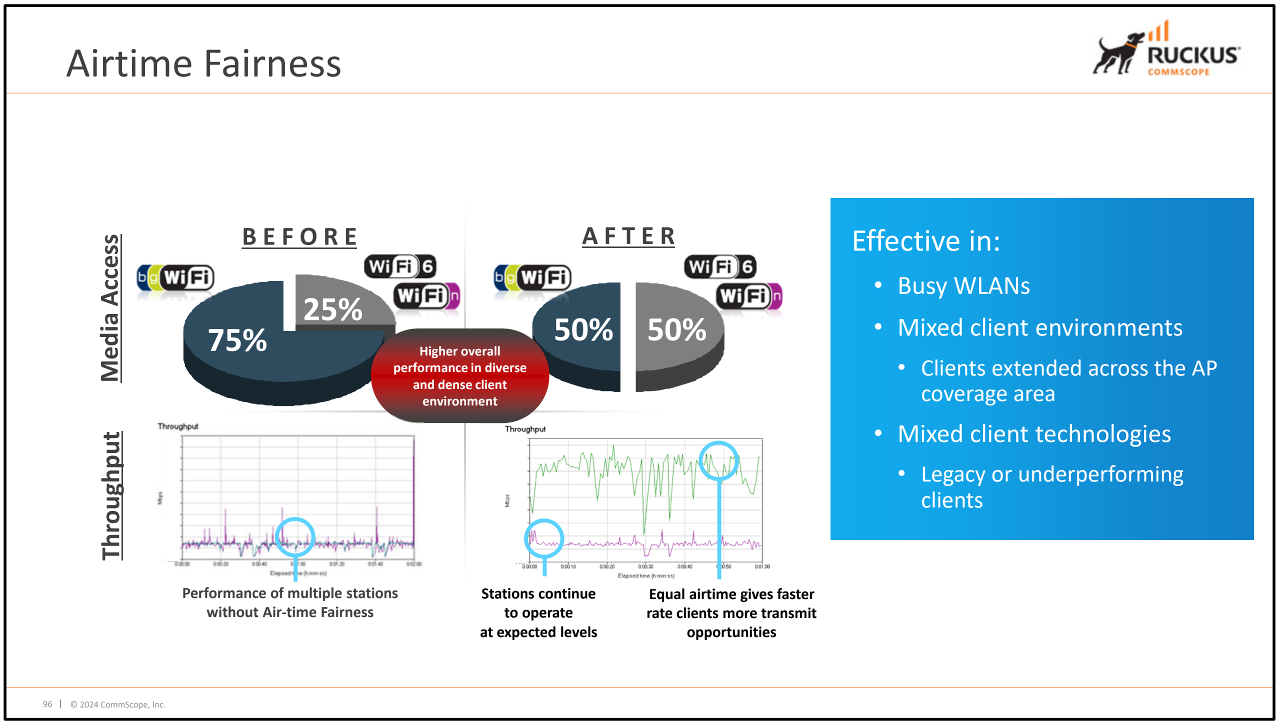
95 |

RUCKUS APs can also utilize Band Balancing and Load Balancing to maximize WLAN performance by enabling clients to efficiently use the AP and RF spectrum resources by either moving clients to higher speed radios, moving clients to less utilized access points, or both.

Band Balancing spreads the client devices across the available 2.4Ghz and 5 Ghz radio bands. Load Balancing spreads the client load across available Access Points

We don’t deauthenticate clients to move existing connections, instead we silence probe responses to clients for new connections. Allowing a more suitable AP to take over.

These load balancing and band balancing techniques are ideal for high-density client environments such as auditoriums, conference halls and public venues where many users try to concurrently connect to the WLAN.



Airtime Fairness

Higher overall performance in diverse and dense client environment

Performance of multiple stations without Air-time Fairness

Stations continue to operate at expected levels

Equal airtime gives faster rate clients more transmit opportunities

Effective in:

- Busy WLANs
- Mixed client environments
  - Clients extended across the AP coverage area
- Mixed client technologies
  - Legacy or underperforming clients

96 | © 2024 CommScope, Inc.

In a busy WLAN, some client stations are able to modulate at higher rates, while others, usually towards the edge of the coverage, will use lower data rates. The result is that the clients using higher data rates will be using much less of the available transmission time. Airtime fairness is an advanced scheduling technique that ensures legacy Wi-Fi clients as well as under performing 802.11n clients don't slow down the performance of faster 802.11n clients by taking too long to transmit.

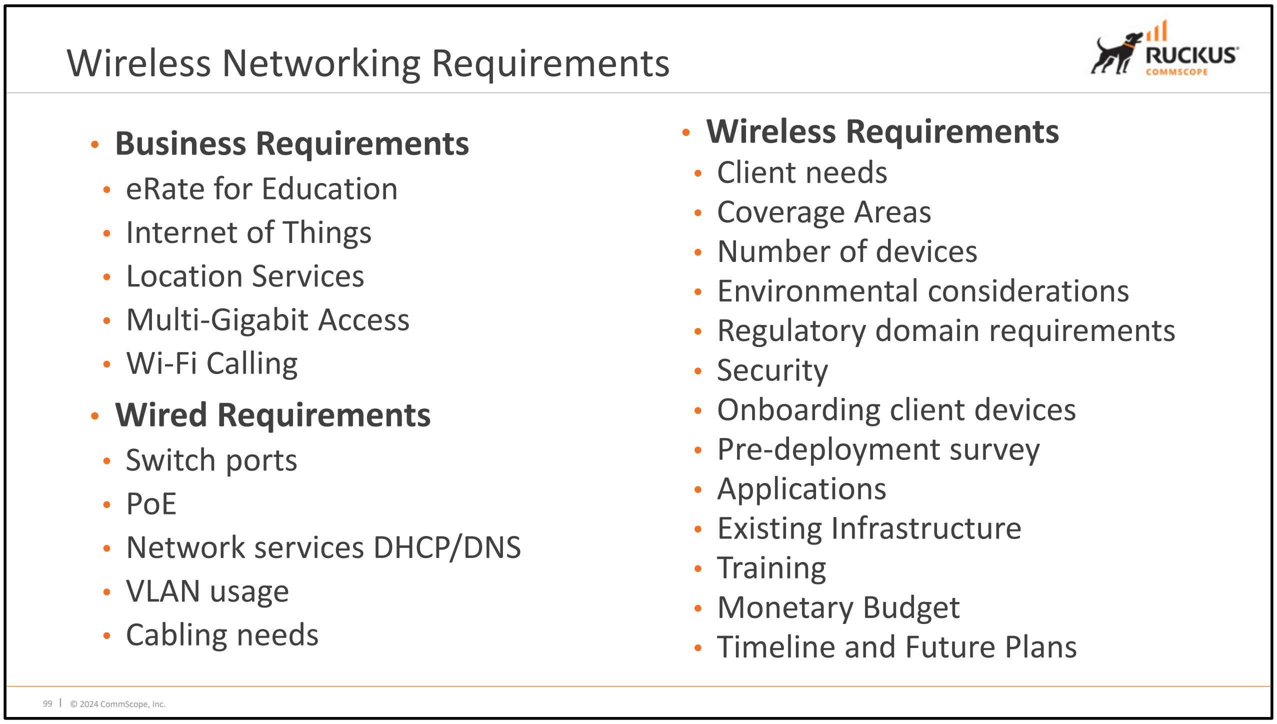
Airtime Fairness ensures that the available airtime is fairly allocated amongst devices. Airtime fairness is applied automatically, transmit queues are scheduled based on the airtime constraints per station using a weighted round robin algorithm. With airtime fairness, users have an equal time on the air and can continue to send packets so long as their airtime use allows. This enables clients with faster potential throughput to recapture the advantages of their higher rate potential and increases overall network capacity.

As an example, Imagine a bridge. On one side we have a line of racecars waiting to cross, on the other we have a line of tractors waiting. When we open the bridge to the racecars for 30 seconds, they will cross very quickly and let's say 50 make it across. When we open the bridge for 30 seconds to the tractors, they are much slower and only 10 make it across. However, the use of the bridge was fair for both sides and the tractors didn't congest the bridge for an extended period of time.

RUCKUS
COMMSCOPE

Designing and planning RUCKUS Wi-Fi solutions

Design requirements gathering



Wireless Networking Requirements

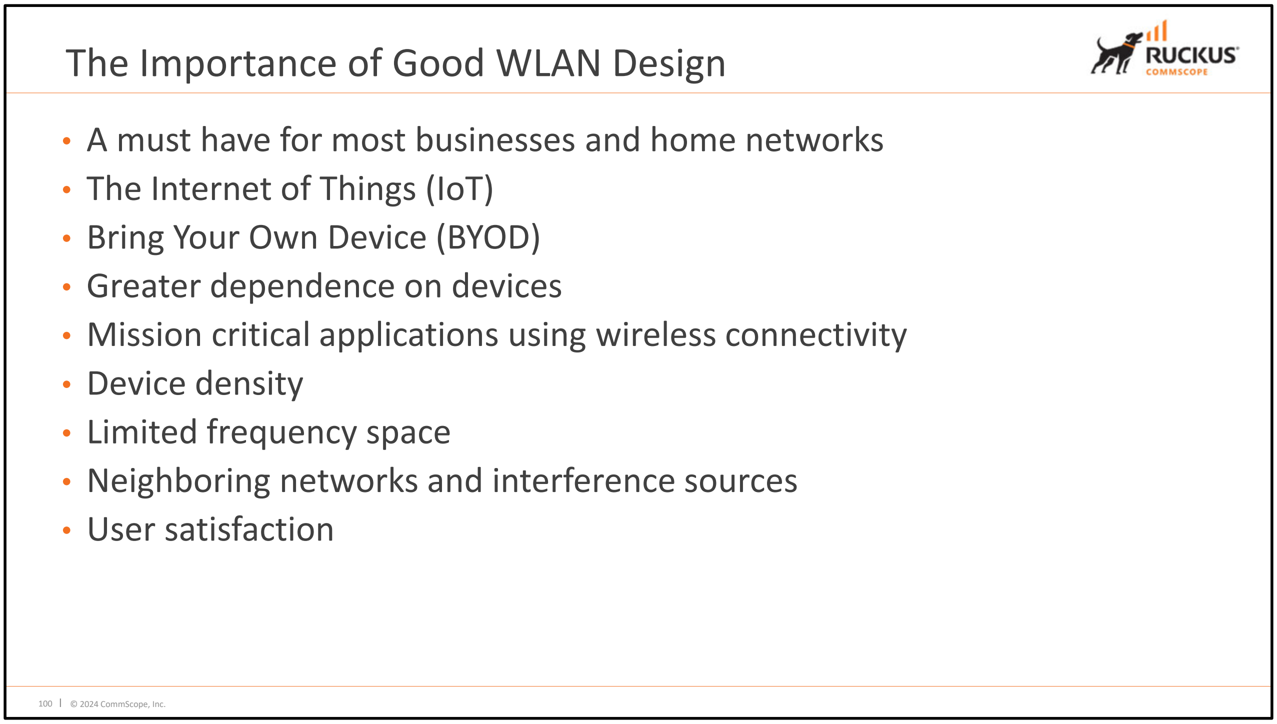
- **Business Requirements**
  - eRate for Education
  - Internet of Things
  - Location Services
  - Multi-Gigabit Access
  - Wi-Fi Calling
- **Wired Requirements**
  - Switch ports
  - PoE
  - Network services DHCP/DNS
  - VLAN usage
  - Cabling needs
- **Wireless Requirements**
  - Client needs
  - Coverage Areas
  - Number of devices
  - Environmental considerations
  - Regulatory domain requirements
  - Security
  - Onboarding client devices
  - Pre-deployment survey
  - Applications
  - Existing Infrastructure
  - Training
  - Monetary Budget
  - Timeline and Future Plans

99 |

It is important to restate that the number one cause of Wi-Fi problems is poor design. To be able to better recognize poor design related problems, you must have at least a basic understanding of the design process. Failure to gather the actual business requirements is a leading cause of poor design. When gathering user requirements, you should interview all stake holders from the executive staff to the entry level employees. This often time consuming process will provide you a better idea of the true needs of the wireless LAN. Customers may only indicate that they need wireless coverage for a specific area, however it is up to the engineer to understand the complete requirements and have a dialogue with the customer to make sure the design meets the needs of the business.

Designing Wi-Fi is more often than not a iterative process. Customers know what they think they need or want but may not have any idea of what they really need. WLAN designers often get a statement such as “We need Wi-Fi everywhere”, when asking about requirements. This statement does not address airtime utilization nor does it address throughput, capacity, density, application needs or future plans. This can prove to be the most challenging portion of the information gathering process, because the designer needs to be an educator as well. You will most often need to educate the customers about how Wi-Fi truly works, so that they understand the why of the design process.

The design is the foundation of the WLAN. If it is incomplete or in any way inadequate, there will be problems on the network. When talking about business requirements be sure to note which functionalities are needed from the network for the business's devices, users, and applications to function as desired. You should take into account current and future networking needs as the use of technology will change over the lifecycle of the design.



The Importance of Good WLAN Design

- A must have for most businesses and home networks
- The Internet of Things (IoT)
- Bring Your Own Device (BYOD)
- Greater dependence on devices
- Mission critical applications using wireless connectivity
- Device density
- Limited frequency space
- Neighboring networks and interference sources
- User satisfaction

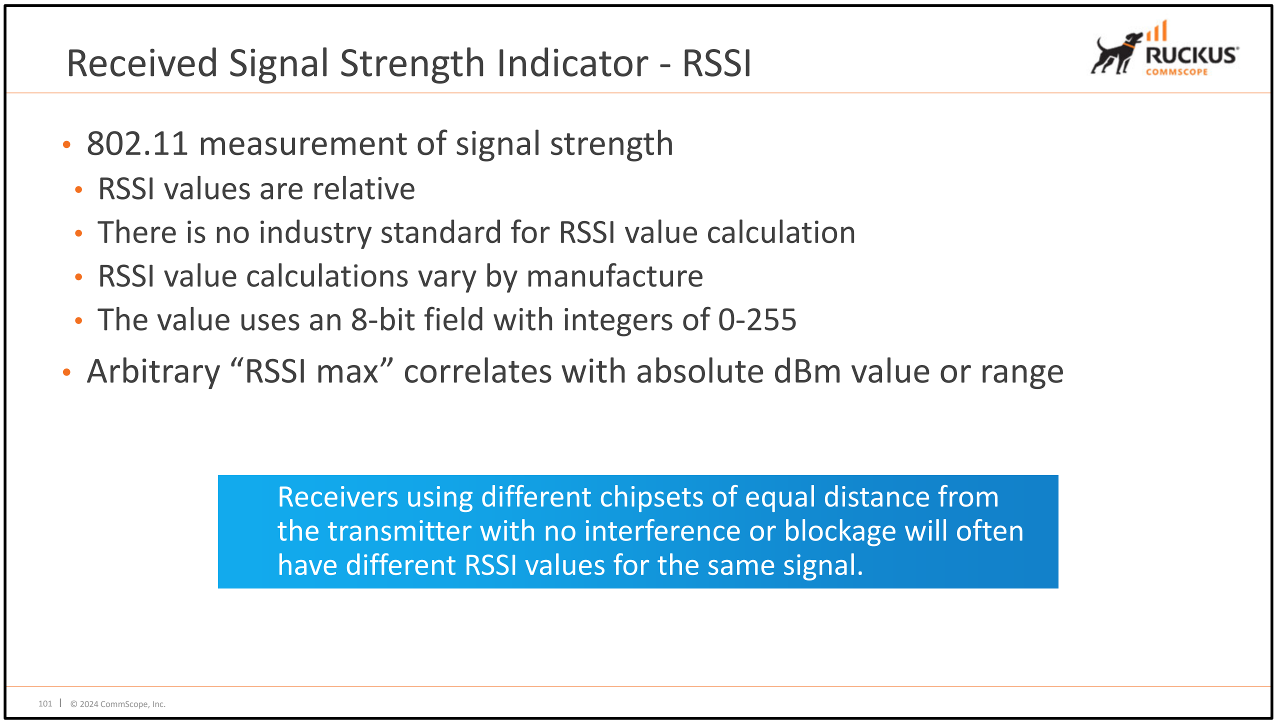
100 | © 2024 CommScope, Inc.

Why is well designed Wi-Fi so important? Wi-Fi has transitioned from a nice to have to a must have status over the last two decades. People just expect a wireless network, even in odd places. The older model for WLAN deployment was wired by default and wireless as demanded. Now it is Wi-Fi by default and wired as necessary to support the Wi-Fi. No one wants to be tethered any longer at work, at home or on the go. Many client devices are wireless only, with no wired port whatsoever. Their users simply expect there to be a wireless network for their use. The growth of the Internet of Things and Bring Your Own Device policy acceptance have made the existence of a WLAN truly expected everywhere.

Users have come to depend upon their devices a great deal more than in the past. Additionally, there are many verticals in which mission critical applications must run over wireless connections. There has also been a dramatic increase in the number of devices used within networks, going from one per user to several per user. These devices have varying requirements and capabilities.

Our WLANs operate in the unlicensed spectrum where there is a limited amount of space for them to support users. The fact that it is an unlicensed space means we must share it with neighboring networks and any other source of RF within it. That takes careful planning and implementation.

Finally, the users must be able to use the network well to complete their jobs. If the users are not able to work efficiently, business suffers. Business travelers often list a good wireless network as one of the top requirements in choosing a hotel. The demand for good Wi-Fi is so great that even in places where it was once forbidden, such as in financial institutions and even on airplanes, are now making Wi-Fi a requirement.



Received Signal Strength Indicator - RSSI

- 802.11 measurement of signal strength
  - RSSI values are relative
  - There is no industry standard for RSSI value calculation
  - RSSI value calculations vary by manufacture
  - The value uses an 8-bit field with integers of 0-255
- Arbitrary “RSSI max” correlates with absolute dBm value or range

Receivers using different chipsets of equal distance from the transmitter with no interference or blockage will often have different RSSI values for the same signal.

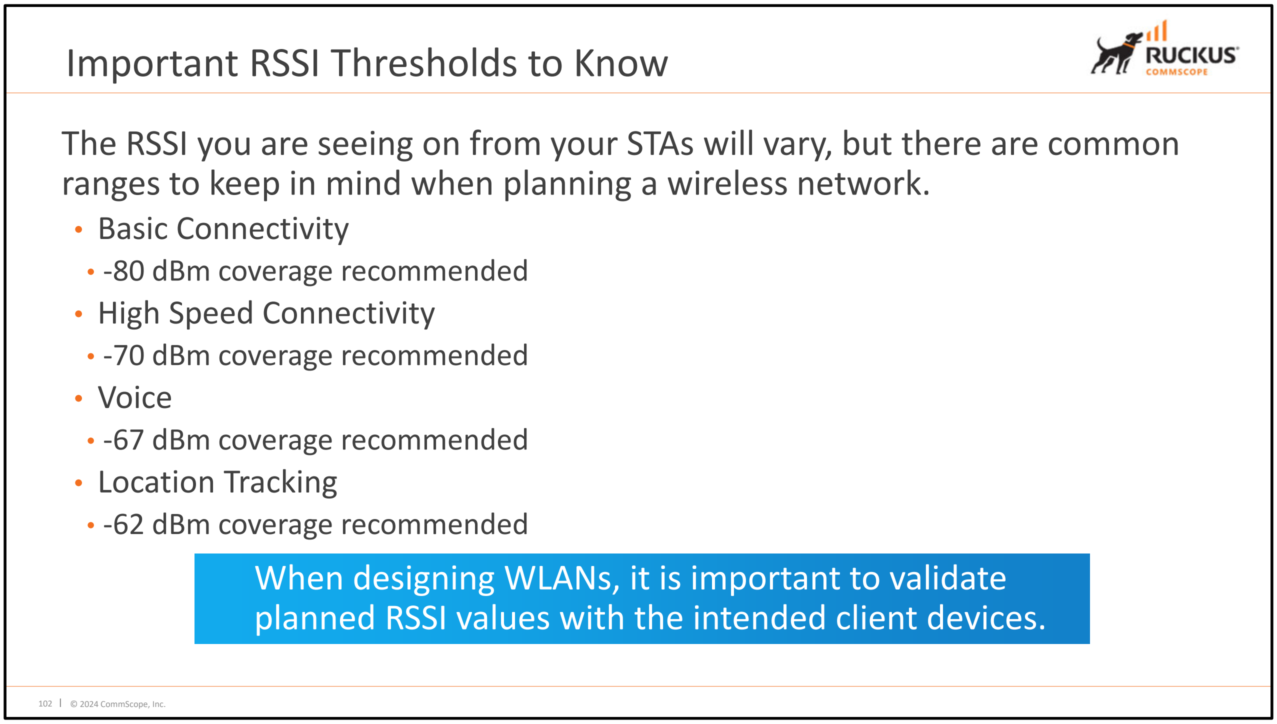
101 | © 2024 CommScope, Inc.

The received signal strength indicator value RSSI is a *relative* value of the strength and quality of an RF signal being received by the antenna. There is no industry standard for calculating the RSSI value. Each chipset calculates is configured by the manufacture.

Two radios at the same distance from the transmitter and in the same RF environment may display different RSSI values for the same signal. The 802.11 standard states that RSSI is intended to be used in a relative manner and that absolute accuracy of the RSSI reading is not specified.

It is usually measured during the reception of the 802.11 frame preamble. The RSSI will be seen as negative dBm values. As you learned earlier, an RF signal weakens as it propagates. The largest portion of loss comes about 5 meters away from the antenna of the transmitter. This loss is exponential. The farther away the receiver is from the transmitter, the weaker the RSSI value. In our previous example of RF math calculation the EIRP was 20 dBm (100 mW).

An intended receiver a short distance away may have an RSSI value for that same signal of a mere -40 dBm. Relatively speaking, this is a weak signal compared to the EIRP. However it is a great signal strength in Wi-Fi.



Important RSSI Thresholds to Know

The RSSI you are seeing on from your STAs will vary, but there are common ranges to keep in mind when planning a wireless network.

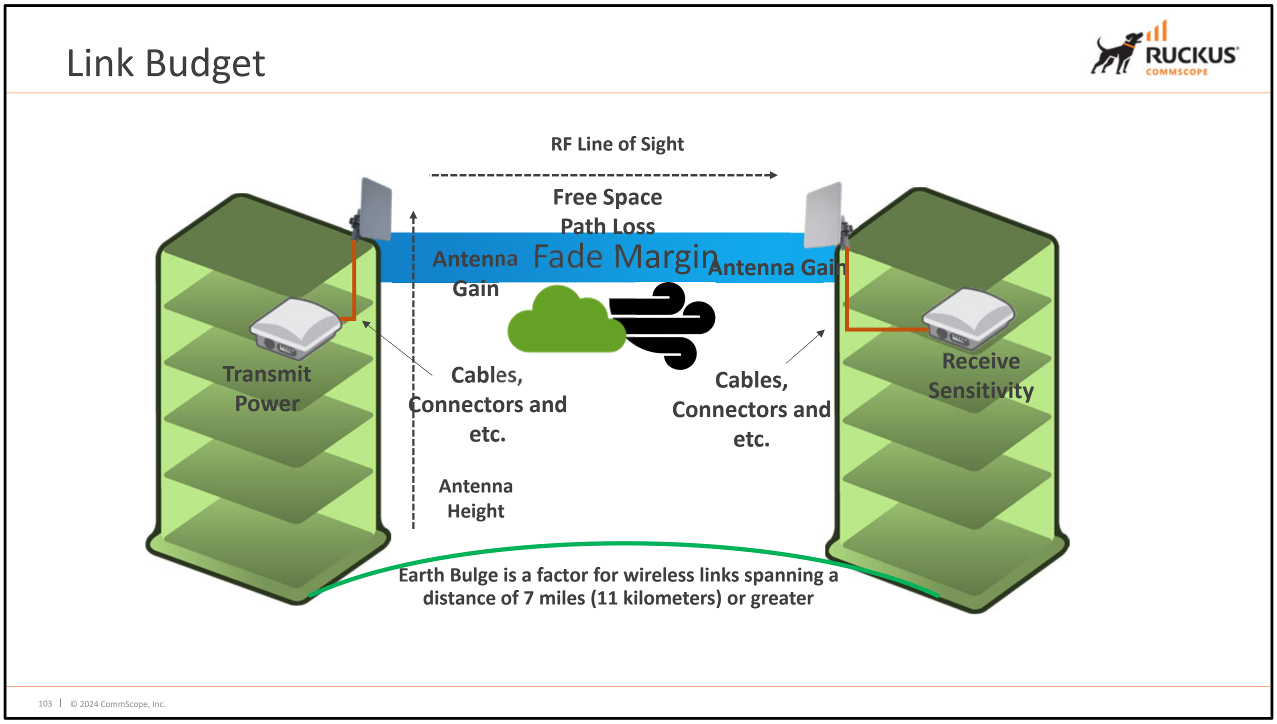
- Basic Connectivity
  - -80 dBm coverage recommended
- High Speed Connectivity
  - -70 dBm coverage recommended
- Voice
  - -67 dBm coverage recommended
- Location Tracking
  - -62 dBm coverage recommended

When designing WLANs, it is important to validate planned RSSI values with the intended client devices.

102 | © 2024 CommScope, Inc.

Remember that there is no industry standard for the calculation of the RSSI values by the receiver as it is determined by the chip set manufacturer. It is of great importance when designing wireless networks to know the requirements of the intended client devices and applications. A deployment that works well for a laptop may not work at all for phones or tracking devices. If you have a high noise floor, you may need to increase your transmit power levels, remaining within the legal limits of your regulatory domain, or add more APs than initially thought needed to cover the space.

Design is about the needs of the clients and your environment not just coverage. If the noise floor is not -95 dBm but is higher you will need to account for this when setting transmit powers. Some of the most common RSSI values used in deployments are -80 dBm for basic connectivity, -70 dBm for high speed connectivity, -67 dBm for voice with some phones requiring -65 dBm and -62 dBm for location tracking. Always verify the requirements with the device manufacture and plan for your least capable device in each area of coverage. You may see in the field and on the exam situations in which everything was fine during design and deployment but now there is additional noise for which you need to account in your environment. If you are not able to remove the noise, you may need to change channels or revisit your transmit power settings and AP locations.



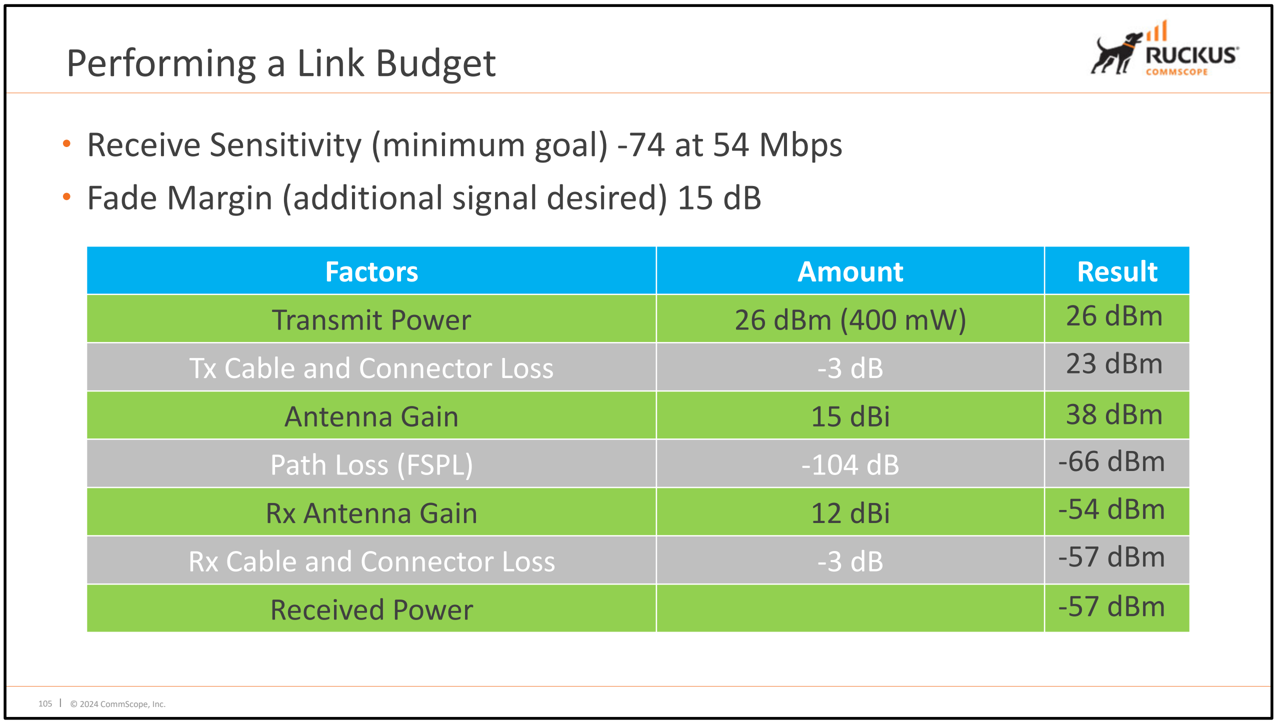
Link Budget

RF Line of Sight
Free Space Path Loss
Antenna Gain
Fade Margin
Antenna Gain
Transmit Power
Cables, Connectors and etc.
Cables, Connectors and etc.
Receive Sensitivity
Antenna Height
Earth Bulge is a factor for wireless links spanning a distance of 7 miles (11 kilometers) or greater

103 | © 2024 CommScope, Inc.

Determining the link budget is an important step in wireless bridge design. You need to make sure that you stay within legal transmit power and that your link performs as expected, even when conditions change. To do this you account for all RF gains and Losses throughout the entire link with a minimum RSSI goal defined. This goal of signal strength is the absolute minimum objective for the link to function as required.

To calculate the link budget, you must, account for transmit power, cable and connector loss on both the transmit and receive side of the communication, antenna gain for both transmit and receive, path loss and any other gains or losses in the system.



Performing a Link Budget

- Receive Sensitivity (minimum goal) -74 at 54 Mbps
- Fade Margin (additional signal desired) 15 dB

Factors	Amount	Result
Transmit Power	26 dBm (400 mW)	26 dBm
Tx Cable and Connector Loss	-3 dB	23 dBm
Antenna Gain	15 dBi	38 dBm
Path Loss (FSPL)	-104 dB	-66 dBm
Rx Antenna Gain	12 dBi	-54 dBm
Rx Cable and Connector Loss	-3 dB	-57 dBm
Received Power		-57 dBm

105 | © 2024 CommScope, Inc.

Here you can see a sample of the information needed in calculating a link budget.

We have defined our minimal goal for this bridge link and have factored in a -15 dB Fade Margin.

As we begin with a transmit power of 26 dBm

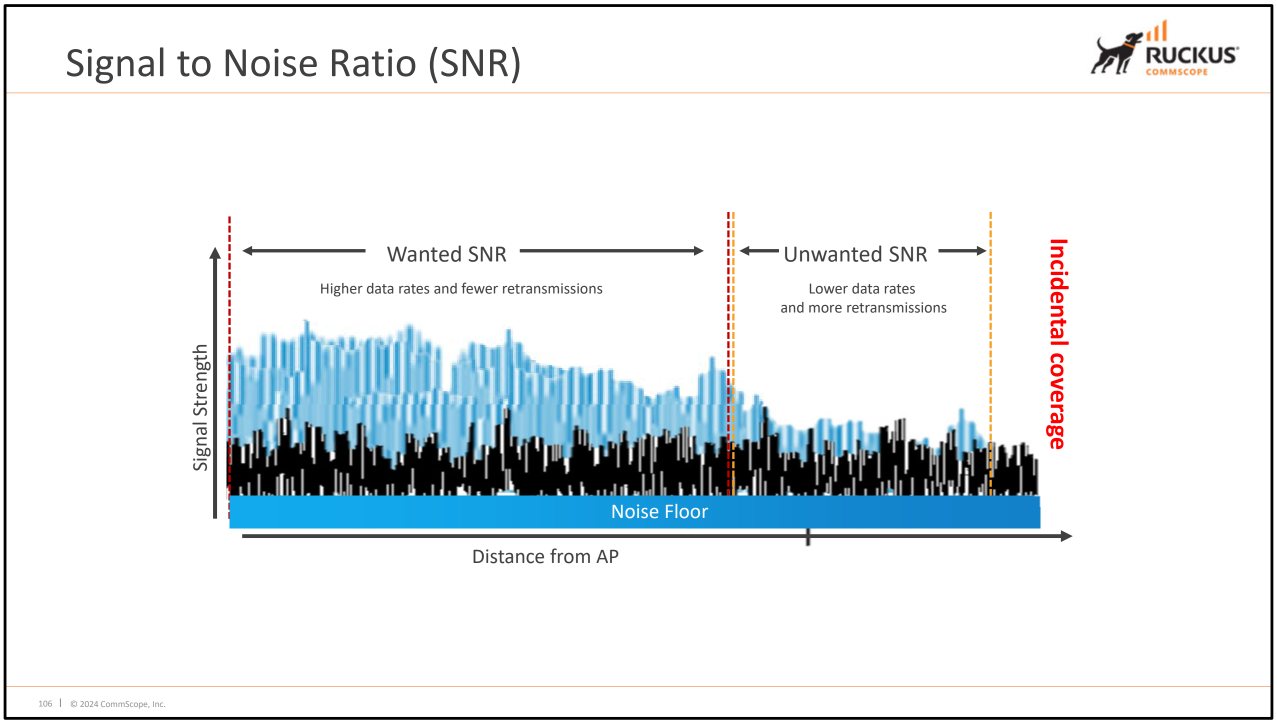
Once we introduce the transmit cable and connector loss we are now at 23 dBm

The transmit antenna adds 15 dBi of gain taking us to 38 dBm

Free Space Path Loss being our largest loss at -104 dB takes us to -66 dBm

The receive antenna adds 12 dBi of gain bringing us to -54 dBm

And once our received signal traverses the receive side cables and connectors we lose another 3 dB for a total of received power of -57 dBm



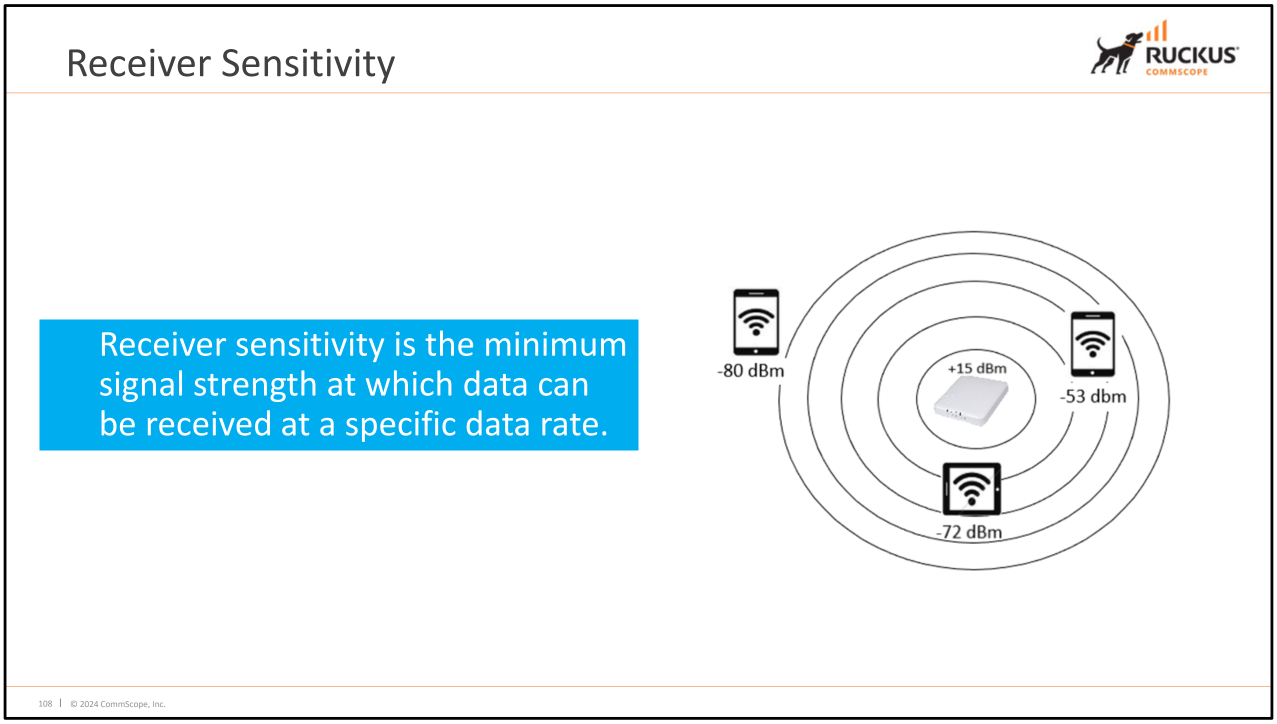
Signal to Noise Ratio (SNR)

106 |

A signal to Noise Ration or SNR is defined as the difference between the noise floor and the signal in dB. This diagram shows the signal strength over distance as a curve that has the best signal strength closer to the transmitter. The diagram also shows the noise within the space. This noise tends to be the garbled up background RF that comes from everything around the receiver, including such things as the sun and stars to man-made interfering devices like Bluetooth headsets or drones.

It is impossible to block out all noise in an enterprise setting and it should not be attempted, since doing so is very cost prohibitive. Low level background noise is called the “noise floor”. The noise floor will vary from location to location based upon local interference sources, even within the same building on the same floor. The ratio of the signal-to-noise (SNR) level defines the quality of the link.

This is directly related to the performance of the network. Based on the SNR, the client and AP negotiate a data rate with which to communicate. The higher the SNR the better, because higher data rates can be used increasing throughput. For good performance, the SNR should be greater than 20 dB and for optimal performance it should be at least 25 dB.



Receiver Sensitivity

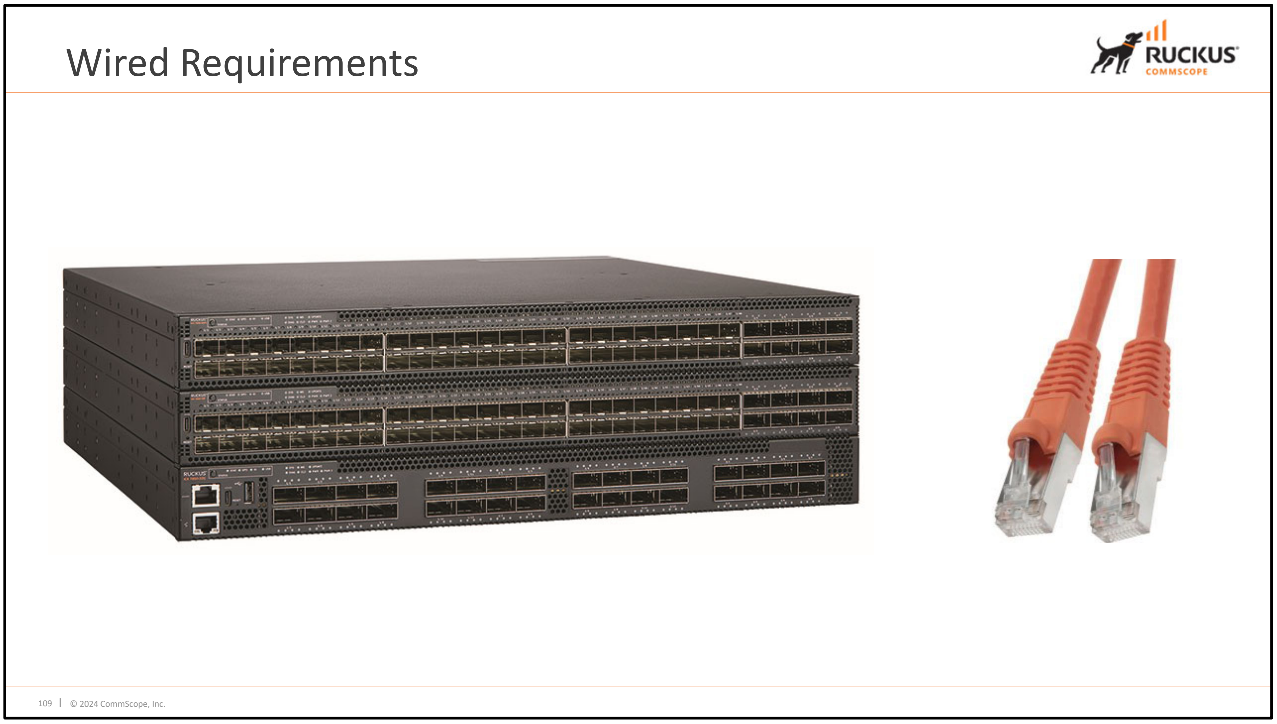
Receiver sensitivity is the minimum signal strength at which data can be received at a specific data rate.

108 | © 2024 CommScope, Inc.

Receiver sensitivity defines the minimum signal strength at which a data rate can be correctly received by a station. As stated earlier, receiver sensitivity varies by device and manufacturer. Vendors publish Receiver Sensitivity Thresholds, and they are usually referenced to dBm.

Remember that dBm is an *absolute* measurement of signal power. RF sensitivity thresholds indicate lower limit of received power required to support operations. The stronger the RSSI value the faster the communications can be. Different applications have different minimum requirements to operate and to be most efficient. Since the Receive Signal Strength is a measurement of the power present in a received radio signal, some receivers need to be closer to the transmitter than others to work well. Receiving devices at different distances from the transmitter will receive the signal at different power levels, due to propagation and obstructions. Due to the allowed industry variance in RSSI value calculations, it is important to plan WLAN deployments around the needs of the client devices.

For example, some Wi-Fi phones need a Receive Signal Strength Indicator (RSSI) value of -67dBm or better to work properly while others require an RSSI value of -65dBm or better. You need to research the devices used within your deployments and build the environment to support them as needed.



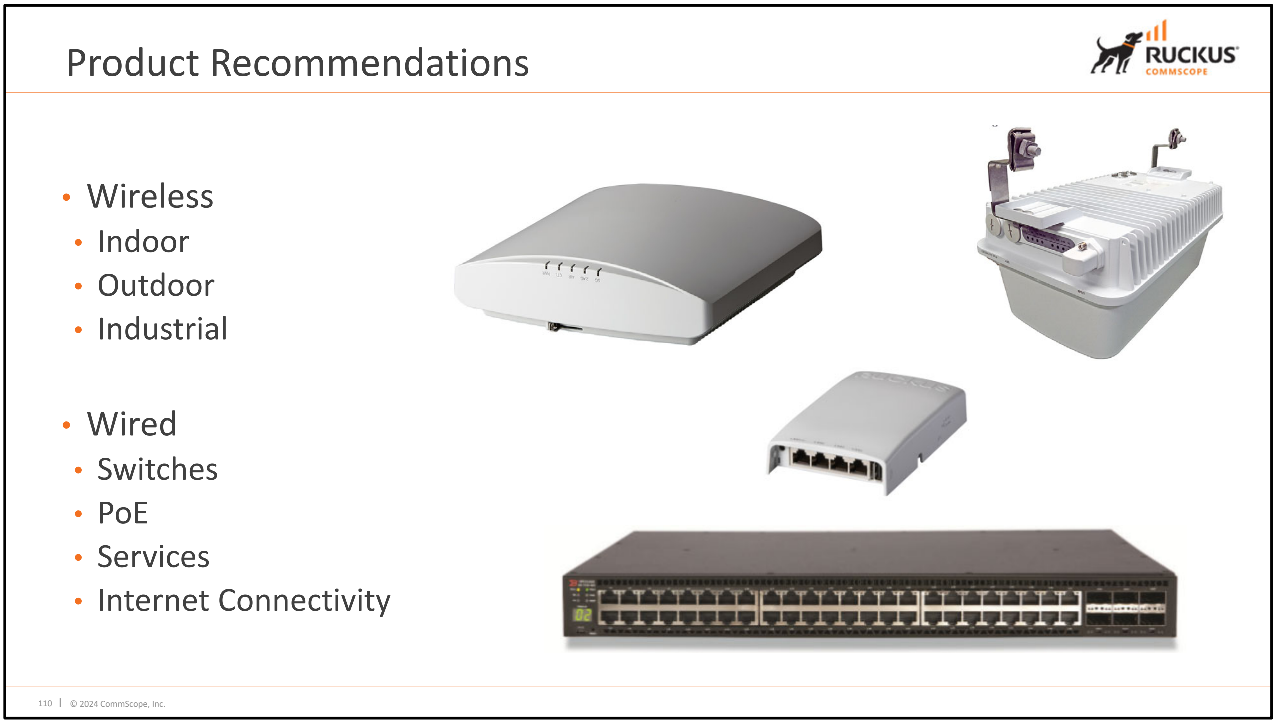
Wired Requirements

As Wi-Fi was being adopted, networks were wired by default with wireless as needed in niche areas. There was no wireless survey and no wireless design, which worked well for early wireless deployments that consisted of one AP in the lobby and one AP in each conference room.

However, as we have transitioned from predominantly wired networking for users, to predominantly wireless networking for users this has changed. Now we see wireless by default and wired as necessary to support the wireless network deployments.

Within traditional wired networks growth was related to expansion of physical components, adding users was a clear process, more ports, cable runs and switch ports were added as required. With additional users being added we had to worry about the Internet connection being able to handle the increase in traffic. We either added additional bandwidth or additional connections. You can see these things. With Wi-Fi, you are not able to see the medium. Adding more users, each with multiple devices is not as easy as it was on the wired network, because in addition to the things we had to think of before, we must now design and build for airtime utilization too.

Redesigning the wireless and wired networks to meet changing network use is often an overlooked part of growing a network. This leads to problems on existing, previously well designed networks. Wired requirements, just like wireless requirements, must be taken into account when building and growing your WLANs.

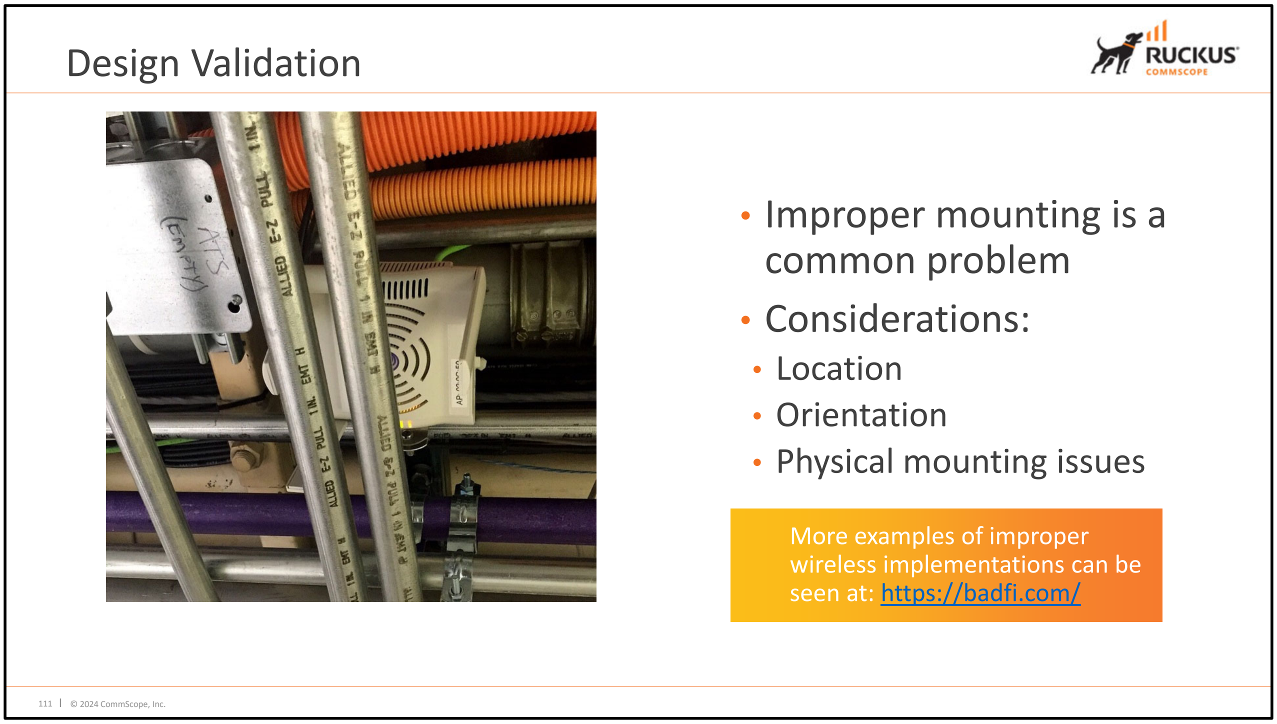


Product Recommendations

- Wireless
  - Indoor
  - Outdoor
  - Industrial
- Wired
  - Switches
  - PoE
  - Services
  - Internet Connectivity

There are a wide range of products designed for use in wireless and wired LANs alike. The key is to recommend the right products for the networks needs. Often, people are more concerned with getting the network installed on time and at or under the budget more than they are about getting the project done the right way. This leads to the wrong devices being deployed to service clients.

Recommending and installing the right products for the network based upon the gathered requirements is an important part of reducing WLAN issues. If the devices are not powerful enough or are too powerful, the design will suffer. Indoor devices should be used indoors or in NEMA enclosures designed to protect the devices within the given environment and heated or cooled as needed. Outdoor devices should be used outdoors or within coolers where they are needed and not for the average indoor WLAN deployments.


RUCKUS
COMMSCOPE
ATS (EMPTY)
ALLIED E-Z PULL 1 IN. EMT

Design Validation

- Improper mounting is a common problem
- Considerations:
  - Location
  - Orientation
  - Physical mounting issues

More examples of improper wireless implementations can be seen at: https://badfi.com/

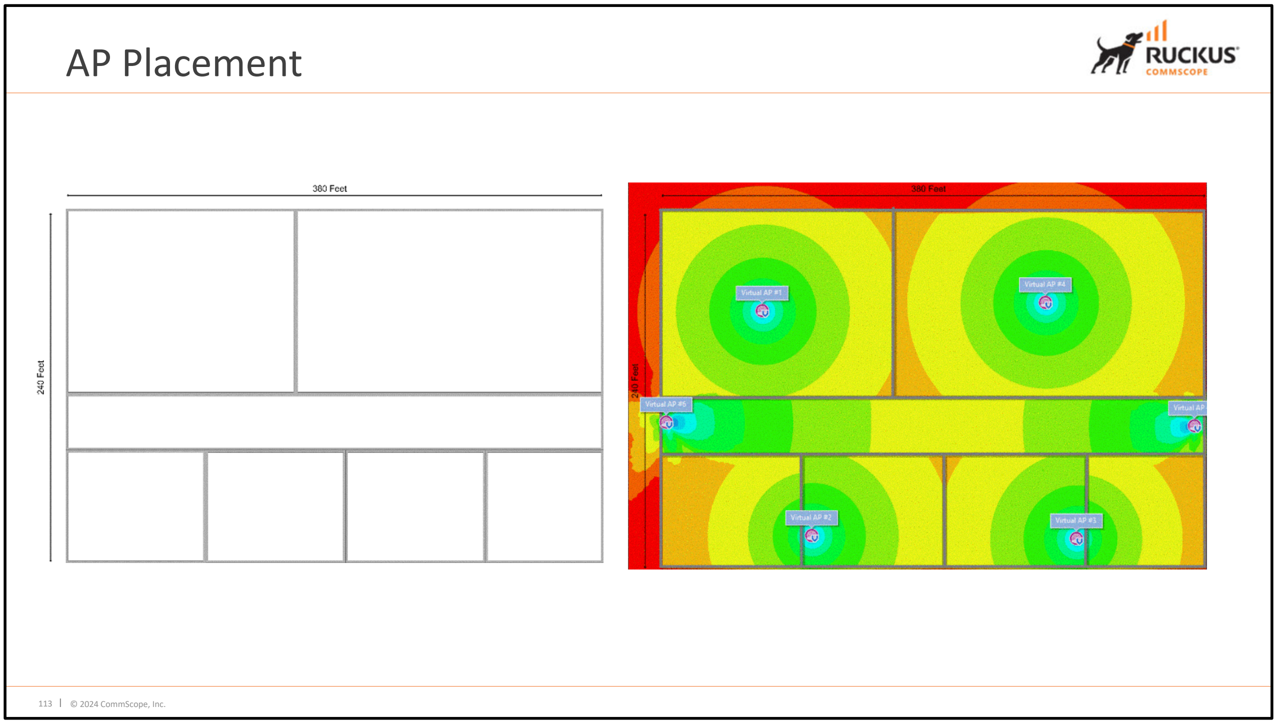
111 |

Many deployments are designed by one team and implemented by another. Regardless of which method is used, the installation must be validated. Installers may not place APs where they needed to be by the design. APs could be deployed using the wrong orientation, pointing the coverage in the wrong direction.

Installers may also place the wrong AP in the right location, leading to troubleshooting and networking issue. If the AP is in the wrong physical location but in the correct location on a network map, diagnosing user issues is impossible. You should conduct a post deployment validation to ensure proper AP placement and ensure the desired coverage exists. This validation should be conducted using the least capable but most important client devices and applications.

RUCKUS
COMMSCOPE

Wireless Design planning



AP Placement

113 | © 2024 CommScope, Inc.

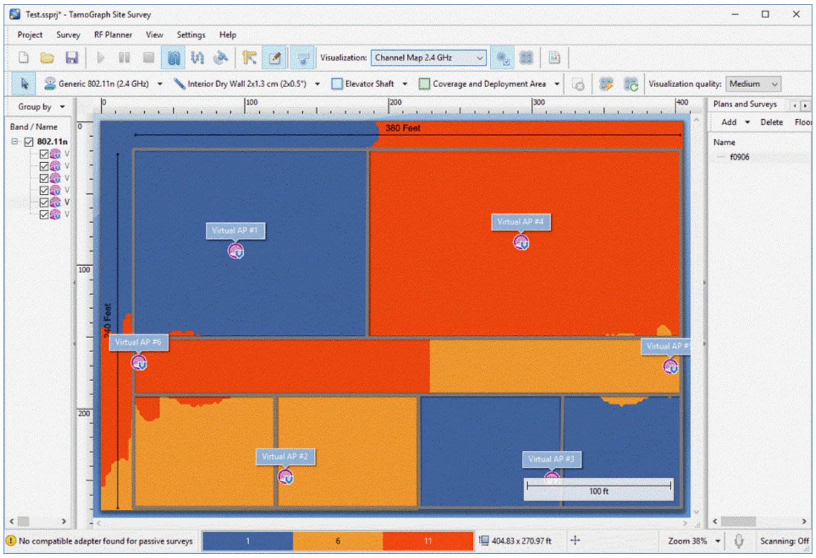
When designing a wireless network, channel layouts and coverage are represented as circles over a floorplan to give a general idea of the placement. In reality however, an APs RF signal does not propagate in a perfect circle and as we've learned previously, the RF waves react to the environment around it. When planning for AP placement there is no need to guess with placement as tools exist such as iBwave Wi-Fi, Ekahau Site Survey, AirMagnet Survey Pro, and TamoGraph Site Survey.

With these tools you can import floor plans, draw walls and set a floorplan scale which will allow you to create passive RF coverage maps that are close to what you would see post implementation. These tools can also be used to conduct an active survey post-implementation by walking through your floor plan while scanning the RF signal.

The slide shows a blank floorplan on the left and on the right our predictive tool once we have detected walls and set the scale. In this example four APs were deployed at 25 mW of output power with omni-directional antennas. Two APs were deployed (at each end of the hallway) with Yagi antennas aimed inward and 25 mW of output power. The result is that the weakest coverage areas indoors are at -71 dBm.

The location of the APs is important as well, moving an AP, even a few feet moves the RF coverage. You should attempt to maximize coverage by placing APs strategically As you can see one AP per office was used for the offices at the top of the design, while the lower offices were able to be covered with two APs placed close to the common walls.

Channel Selection



Visualization: Channel Map 2.4 GHz

Generic 802.11n (2.4 GHz)

Interior Dry Wall 2x1.3 cm (2x0.5")

Elevator Shaft

Coverage and Deployment Area

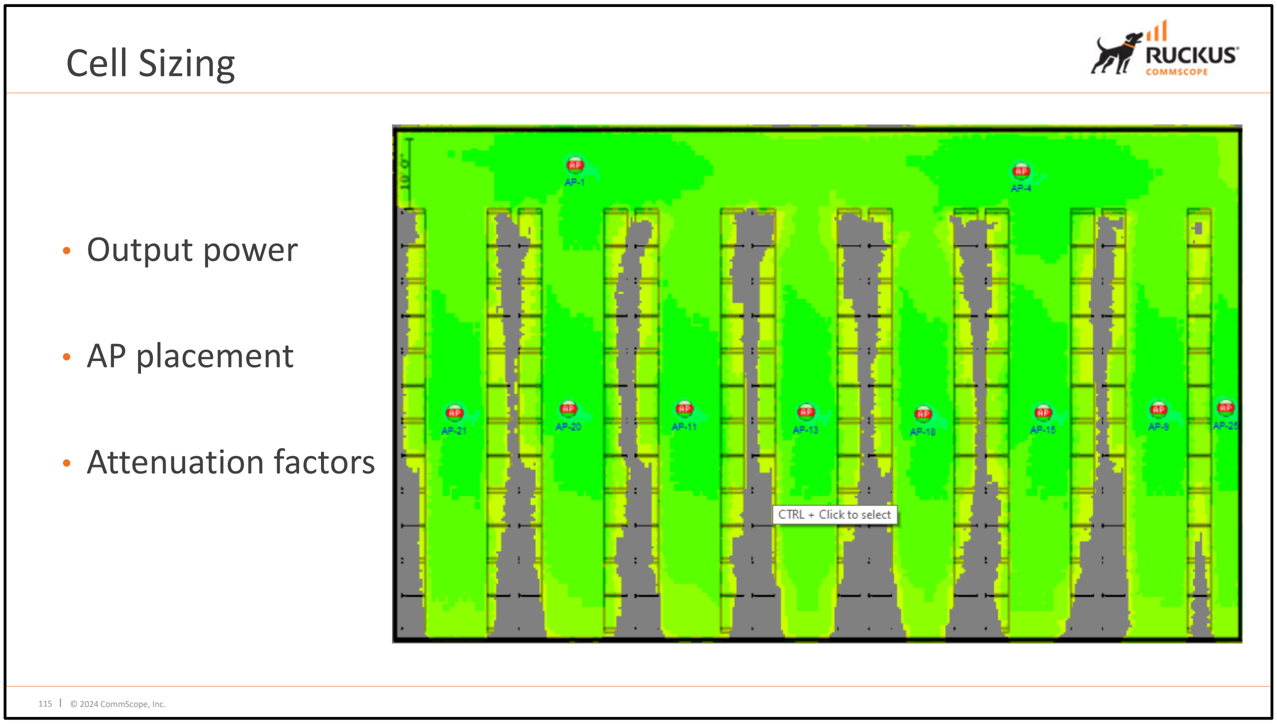
Visualization quality: Medium

No compatible adapter found for passive surveys

114 | © 2024 CommScope, Inc.

Here we can see the same plan with the channel map details. In this environment with the use of 2.4 GHz some co-channel interference is likely to occur, most notably on channel 11. This is to be expected with the use of 2.4 GHz but we have minimized this as much as possible by staggering channels so they are not directly next to each other.

These same concepts apply to larger buildings like schools or hotels with larger floors. Just remember with multiple floors you have to take into account what channels are above and below you. This is easier to accomplish with the use of 5 GHz due to the number of channels available, but 2.4 GHz can still work well for many implementation. It is also not uncommon when using both 2.4 and 5 GHz to disable 2.4 GHz on some radios to help reduce CCI

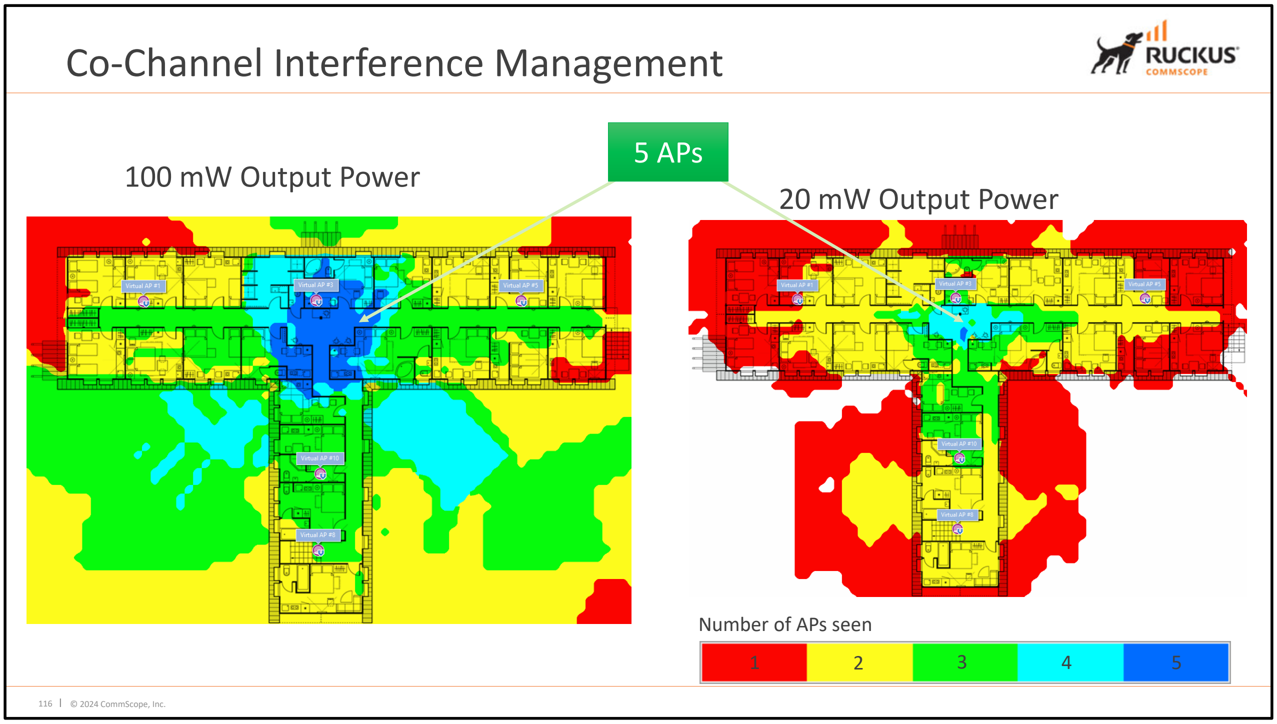


Cell Sizing

- Output power
- AP placement
- Attenuation factors

Within MCA solutions and in addition to channel selection you should also be aware of cell sizing. Cell sizing is the RF coverage area from a particular AP. You need to adjust power levels at each AP so that each cell doesn't overlap too greatly and overpower other APs in the environment. Some overlap should occur, but should be kept around 20% . Where overlap does occur different channels should be used. Going back to the last slide when we talked about dual-band, when there is great overlap on the same channel in the 2.4 GHz space this is you might see the 2.4 GHz radio disabled.

Normal power ranges should be under 100 mW and many APs support dynamically sizing the cell based on what the AP can detect from other neighboring APs. However if you are manually configuring power levels do know that they could need to be adjusted as the environment changes.



Co-Channel Interference Management

5 APs

100 mW Output Power

20 mW Output Power

Number of APs seen

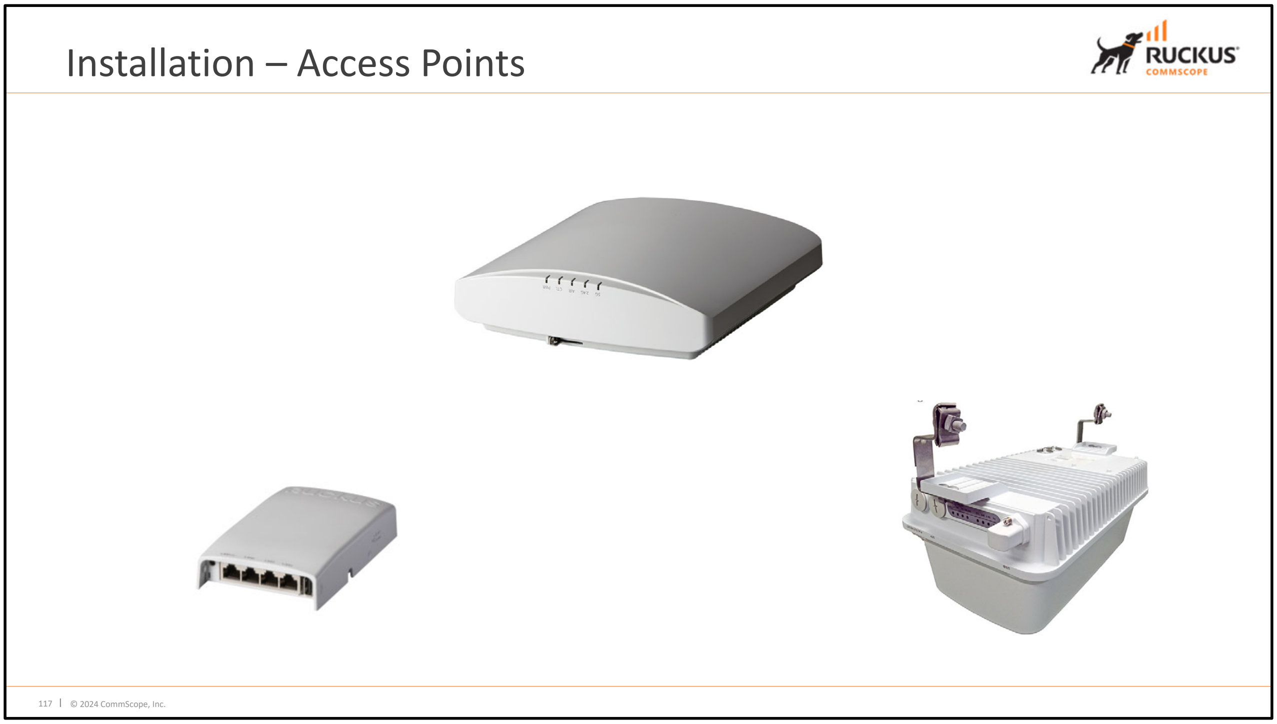
🟥 1 🟨 2 🟩 3 4 5

116 | © 2024 CommScope, Inc.

AP placement, channel planning, and cell sizing are essential to manage the effects of co-channel interference. It is especially challenging in 2.4 GHz as seen in these images. With 5 APs in a very large area and using only channels 1, 6 and 11 at least 2 APs will have overlapping channels. It is not uncommon to see APs on the same channel in an environment with the use of SCA, but these deployments can cause a significant reduction in throughput.

In the graphic shown you see the number of AP's detected from any point on the floorplan. On the left, as you can see the central hub of the building is getting RF from all 5 APs. Once the AP power levels are adjusted to 20 mW you can see the number of APs detected is greatly lessened. Thus, our chance for CCI is reduced.

With 5 GHz, seven or more APs may be used in this pictured space with no co-channel interference because of the number of channels available in the 5 GHz band.



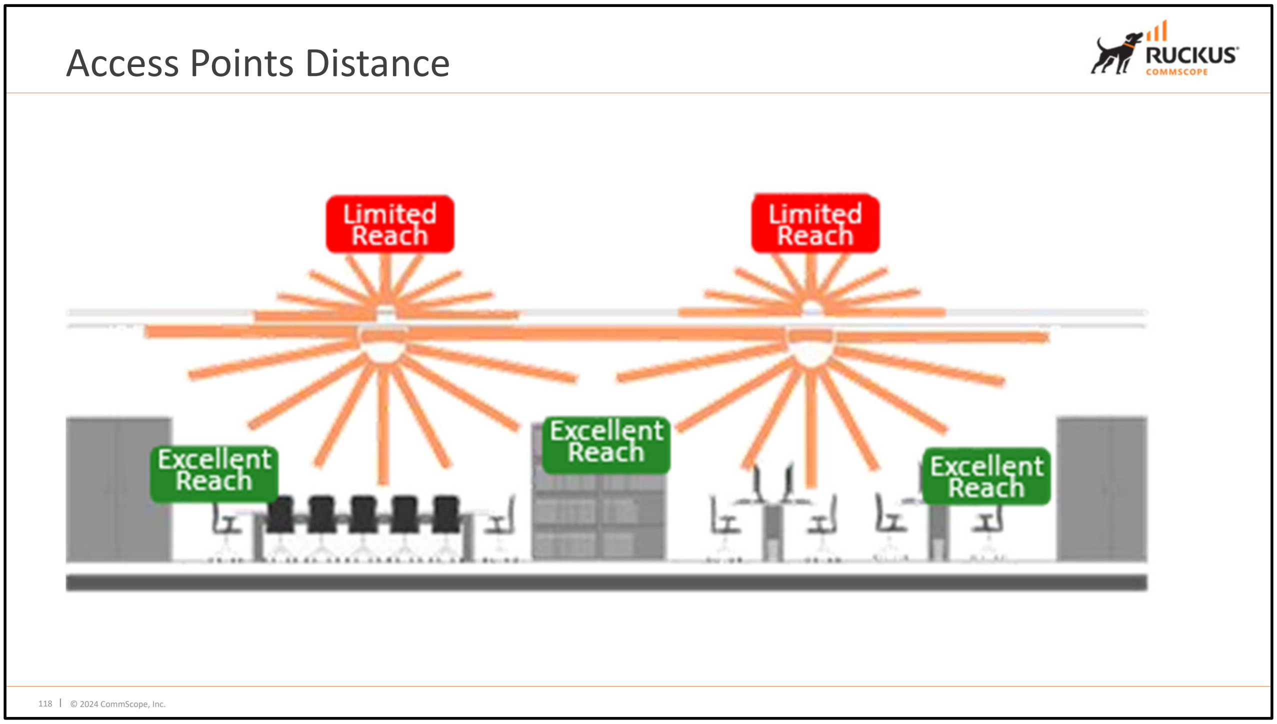
Installation – Access Points

117 | © 2024 CommScope, Inc.

The Installation of the access points is something that should be examined during and after the initial implementation. You should ensure they are mounted in the designed locations, oriented properly, and that they are as secure as required for their given location. Improper mounting will result in undesired coverage, possible physical damage or theft and poor networking conditions.

You will also need to ensure that they are cabled properly. If an AP is mounted but not powered, the ethernet cable could be in a non-PoE port or the AC cable may not be connected properly.

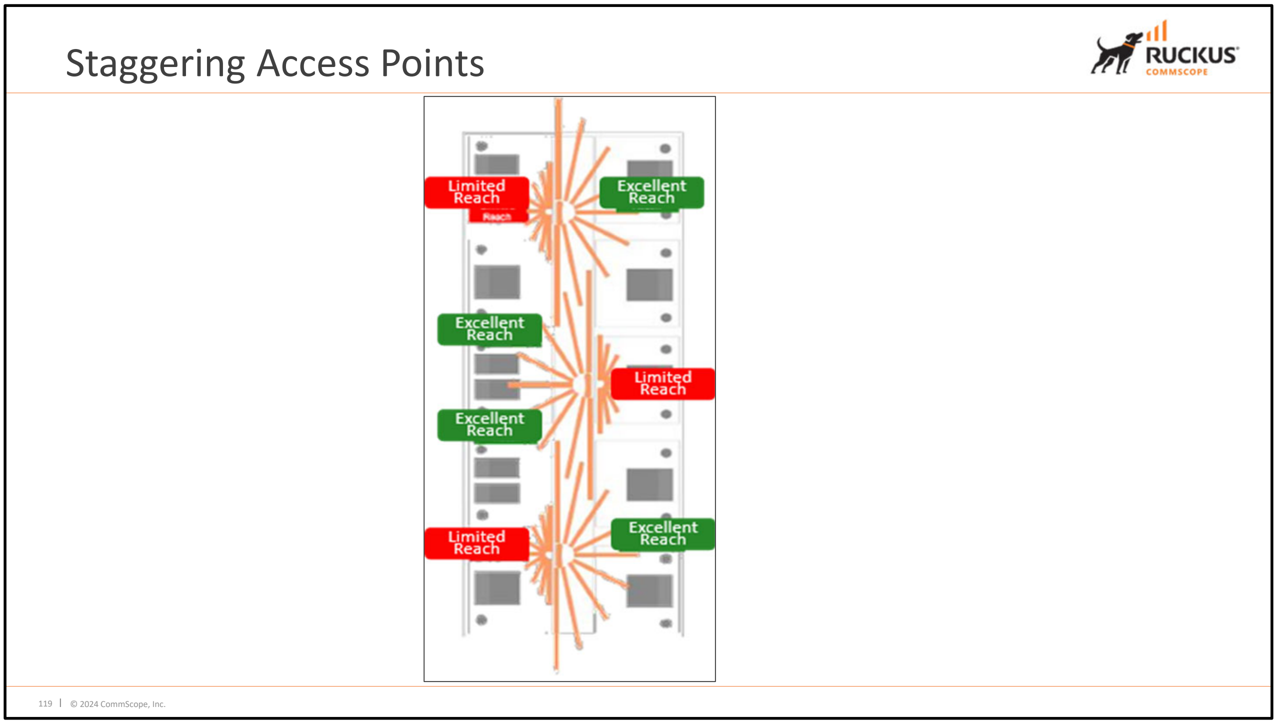
When troubleshooting, it is a good Idea to begin with the physical things first. As part of an on-going WLAN support plan, you should periodically inspect the physical condition of the devices and their connections, even if no trouble is reported. This holds true for a well-maintained security policy as well.



Access Points Distance

118 | © 2024 CommScope, Inc.

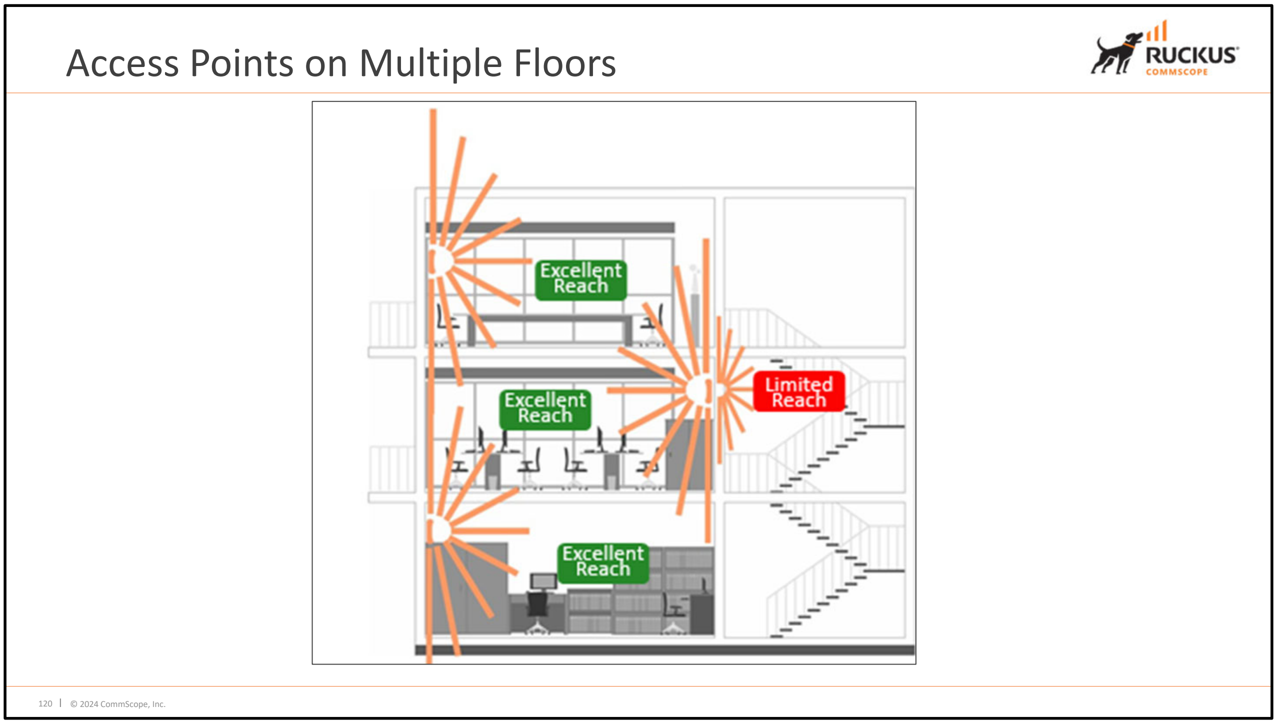
APs mounted are correctly spaced, it provides great coverage and limited interference. Mounting APs too close together limits channel separation and creates conflicts.



Staggering Access Points

119 | © 2024 CommScope, Inc.

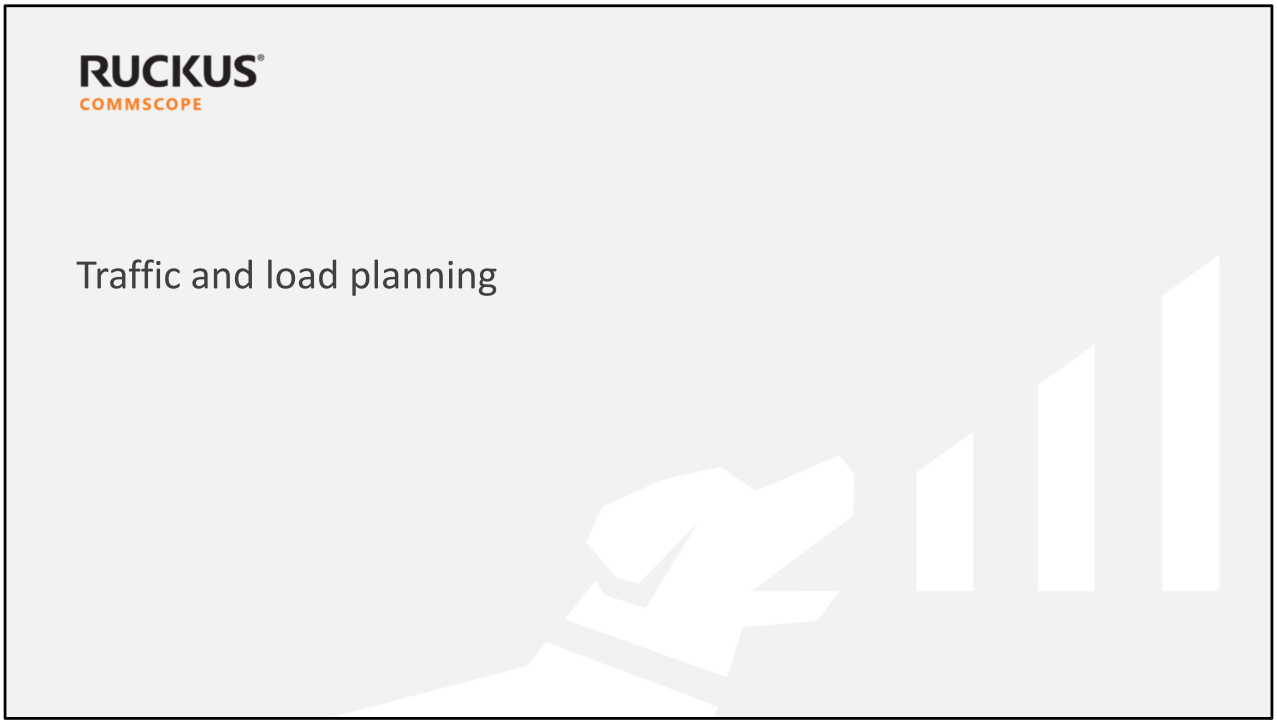
Staggering APs on opposite walls provide a balanced access based on their distance and direction. This method is useful while mounting APs in a long hallway. Keeping APs on same side of hallway can create dead zones and overlapping of coverage.



Access Points on Multiple Floors

120 | © 2024 CommScope, Inc.

Staggering APs on opposite walls of each floor provides even coverage and good AP separation. Keeping APs on same side wall on each floor creates on even coverage and possibly channel overlapping.



RUCKUS COMMSCOPE

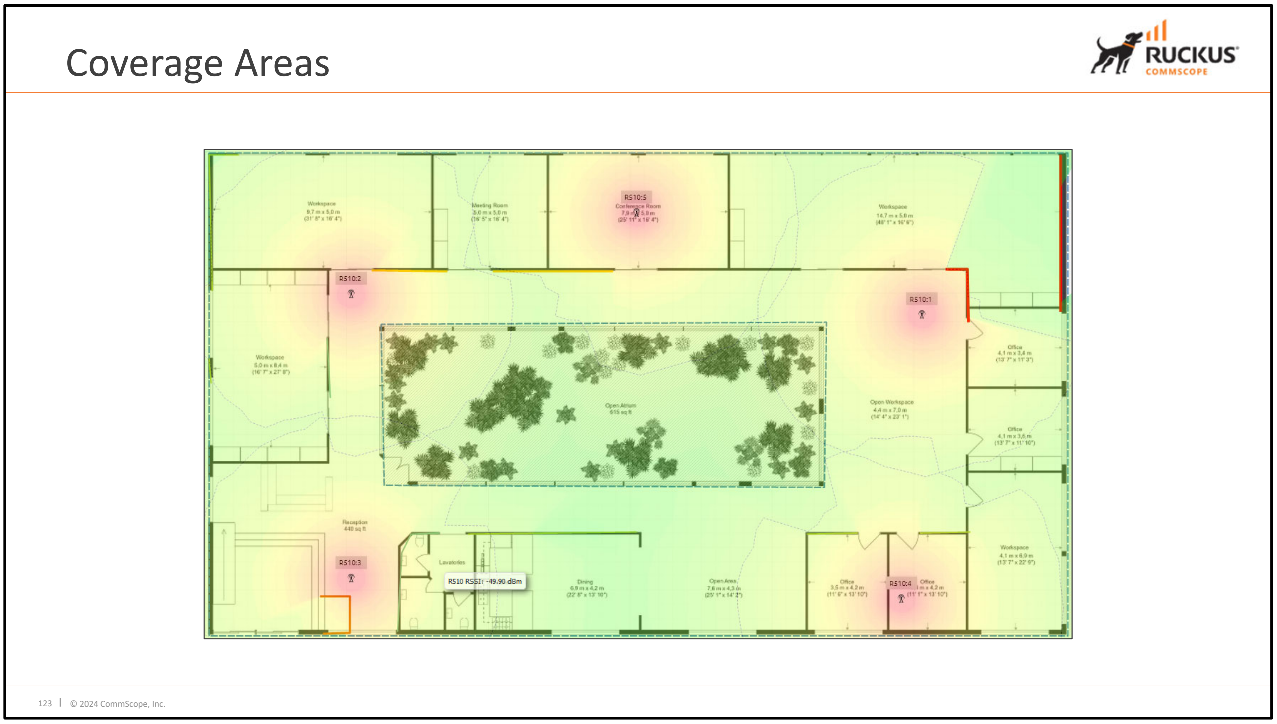
Traffic and load planning

Environmental Concerns

The WLANs you design will be working within different building types, around different neighboring networks and will be exposed to different sources of interference. Some of this information can be learned from discussions with your stakeholders. Other pieces of information can only be learned by conducting a physical site survey.

Different requirement areas will have different wall types and different numbers of walls and other obstructions. Not all WLANs are built within the same types of buildings or open areas. You will need to determine what the objects in the airspace are going to do to your wireless signals, block them completely, attenuate them, refract or diffract them.

You will also need to find the frequencies of any non-802.11 sources of interference so that they may be avoided in your design. Additionally, you will need to know the temperature ranges, weather elements and dust expected of the WLAN requirement areas to determine the type of APs to deploy and if the APs will need protective enclosures.



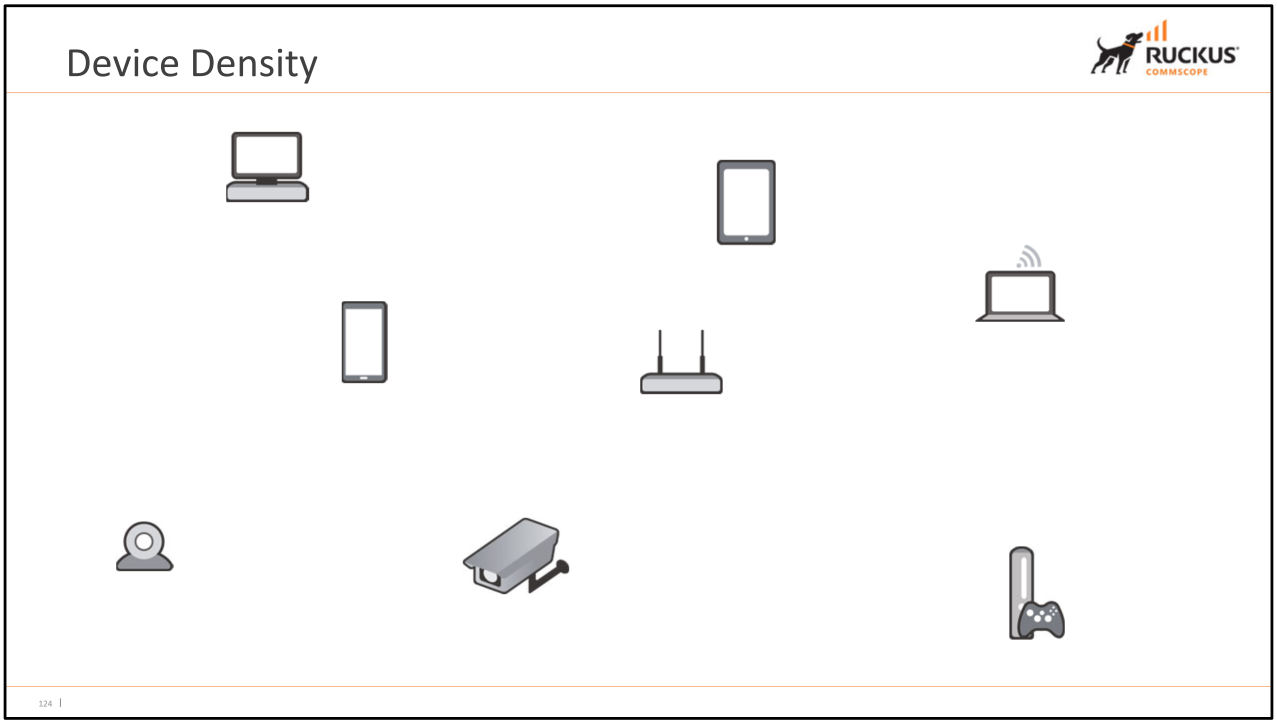
Coverage Areas

123 | © 2024 CommScope, Inc.

Coverage areas are the spaces in which the design must purposely provide Wi-Fi. Each area may have it's own requirements for wireless usage. Some areas are populated by guest, some by staff only and others may be a mixture of both. The requirements for a warehouse are most assuredly different than those found in patient care areas of a hospital.

The needs of guests in a coffee shop or lobby are different than those of the users within an enterprise office space. More often than not, the designs with which you work will have multiple coverage areas with differing requirements. You must gather the requirements for each of the coverage areas and design for them separately.

A good way to look at what the industry has called coverage areas for years is to treat and call them requirement areas instead. This will help you and your customers better understand why some areas of the same size use different numbers of and or models of access points.

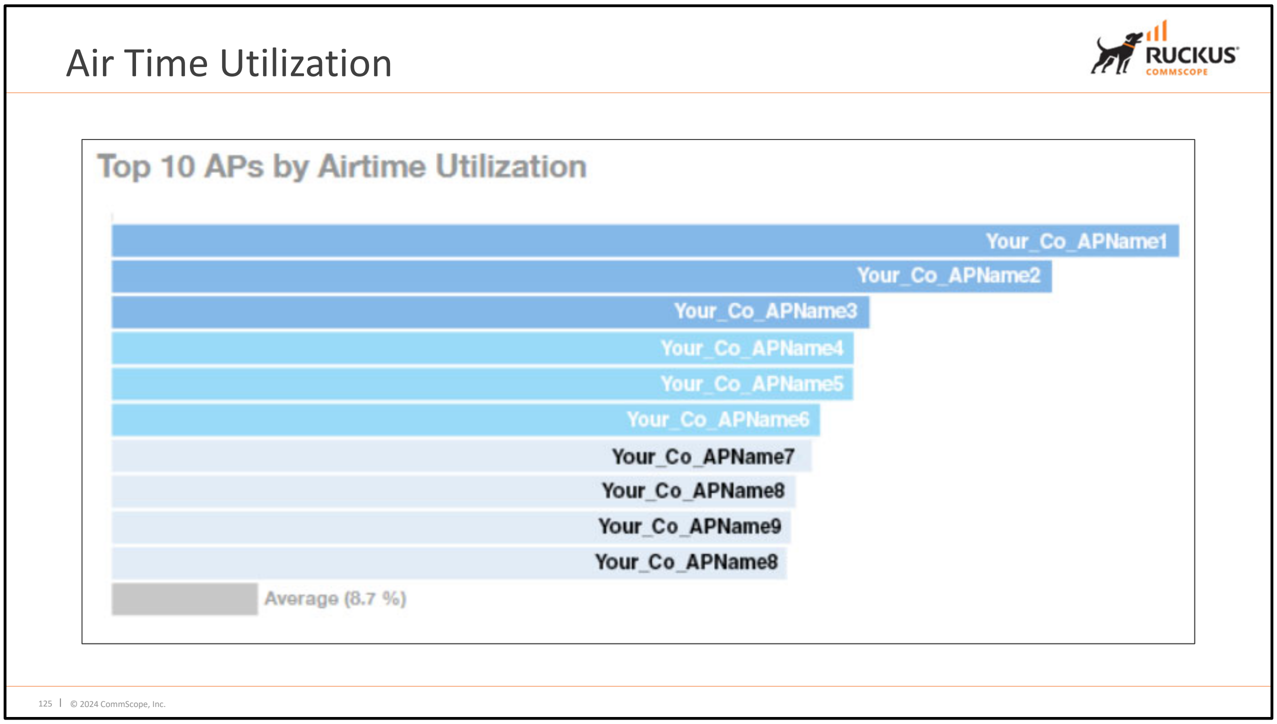


Device Density

124 |

Device density is the number of client devices present within a service set area. In home networks, that number can be relatively small. Whereas in a stadium, that number is quite large. You must design around the number of and types of devices on your WLAN. They all need to access the network and most likely have different abilities and requirements.

Some deployments may have requirement areas that have differing device density. Each area needs to be designed based upon it’s individual requirements. You should not design based upon an average or simply plan for the highest or lowest possible device density everywhere. Each device must contend for the medium. So in higher density deployments you will need more APs to break up the collision domains into smaller sizes. This helps increase user satisfaction and reduces hidden node, near-far and retransmission issues.

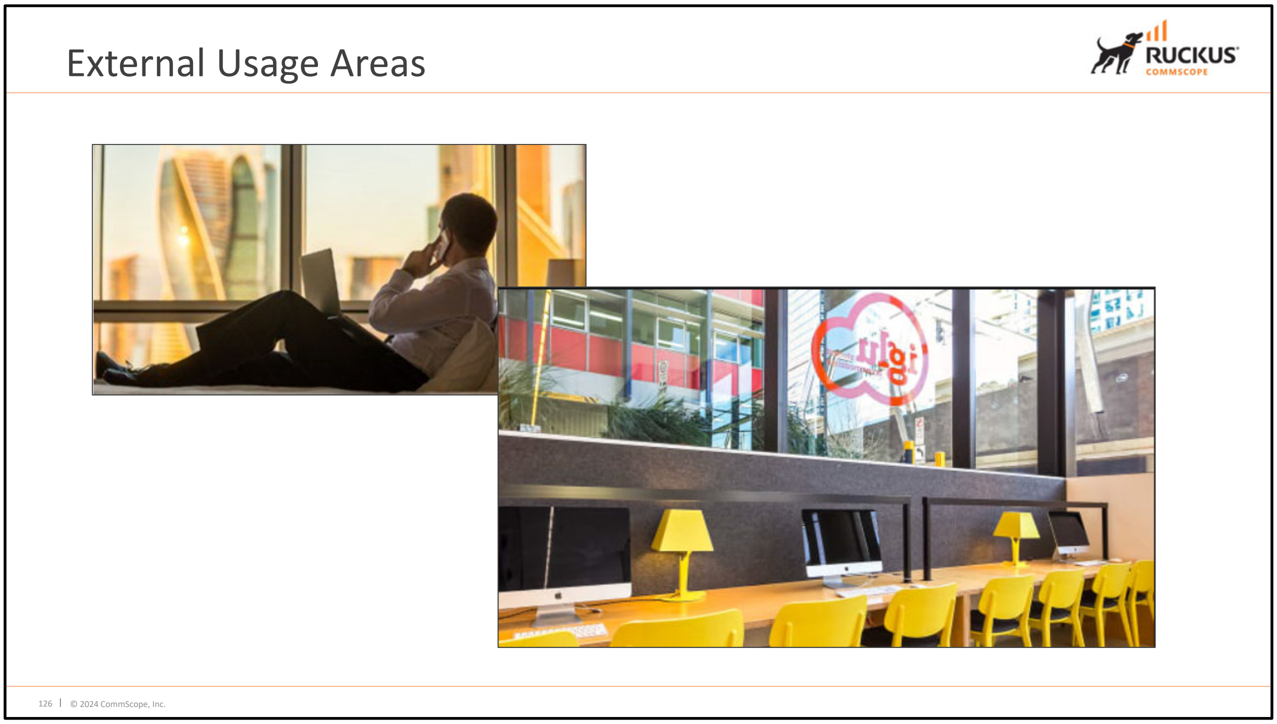


Air Time Utilization

125 | © 2024 CommScope, Inc.

Air time utilization is one of the most important factors in determining the success of a WLAN. Air time utilization is a key metric in measuring and assessing your WLAN health. There are two main influencers of air time utilization, external RF interference (non-WiFi energy) and the medium contention.

If it is too high, some applications will suffer or cease to function. For example, Voice applications require a 50% or greater free air time to work properly. If air time utilization exceeds 50%, these applications will begin to suffer. Planning properly for air time utilization is required for good WLAN design.



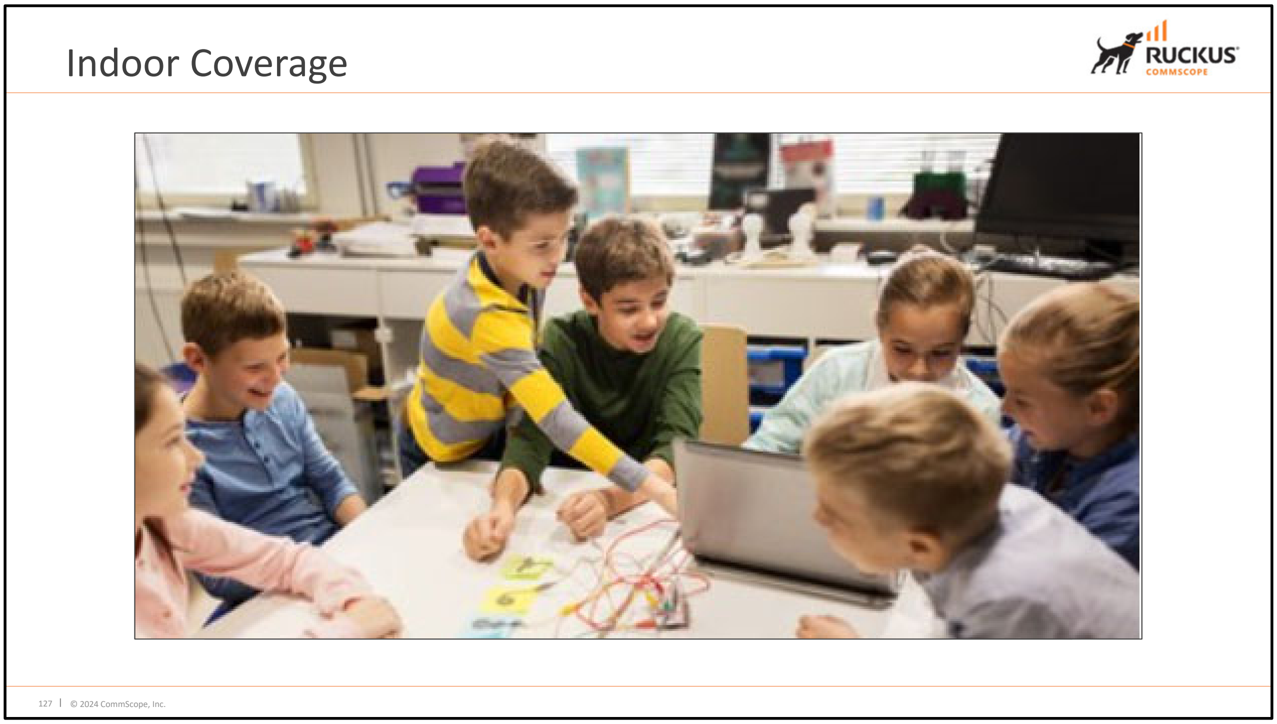
External Usage Areas

126 | © 2024 CommScope, Inc.

More often than not, an area that supports guest access will also support internal use to keep internal device traffic protected by organizational standards and to keep internal devices and users from using the external or guest network. You may, however, encounter a design requiring only guest access in a given space to force internal users to be within the confines of other parts of the property. Customers will state that they need to provide guest networking in some areas but not in others. This is normal today.

Older networks did not provide guest Wi-Fi, forcing guests to use designated Ethernet ports for Internet access. Just like internal users, external users do not want to be tethered anymore, forcing the design to include guest Wi-Fi in some locations.

These locations started out as the lobby and meeting rooms then expanded into other areas where guests were allowed to wander. In hospitality, this started in the lobby, meeting rooms and conference centers but rapidly spread into the guest rooms, poolside, and all other common spaces. When designing a guest network for external devices, there are several things to keep in mind beyond the obvious connectivity.



Indoor Coverage

127 | © 2024 CommScope, Inc.

You may have a WLAN with multiple requirement areas defined with vastly different device and user needs. In a school for example, students have different needs than teachers and both groups have different needs than staff. The auditorium and stadium will have different needs than the classrooms.

Additionally, indoor deployments usually have more environmental design influences than outdoor deployments. Indoors you must design so that the signals are able to be used despite the walls, filing cabinets, people, water effects, elevators, wiring closets, stairwells, HVAC systems and sources of non-802.11 interference such as microwaves, X-10 cameras, alarm systems and other RF generating devices.

To over come the various influences in the indoor environment, it is important to identify the necessary frequency type, AP's power, ideal AP's location and the pattern of the wireless signals from the antenna. Additionally, you must also make any APs you deploy look nice or not be seen. People want to use the network not look at it. Ascetics are increasingly important for indoor deployments.

That is why in most indoor environments, excluding manufacturing and logistics, you will need to design using internal antenna APs. Indoors, it is common to mount the APs above the ceiling tiles, thus hiding them from view. In addition to being untethered, people also expect the network to look nice.

RUCKUS COMMSCOPE

Product selection for solution

Transportation WLAN Considerations

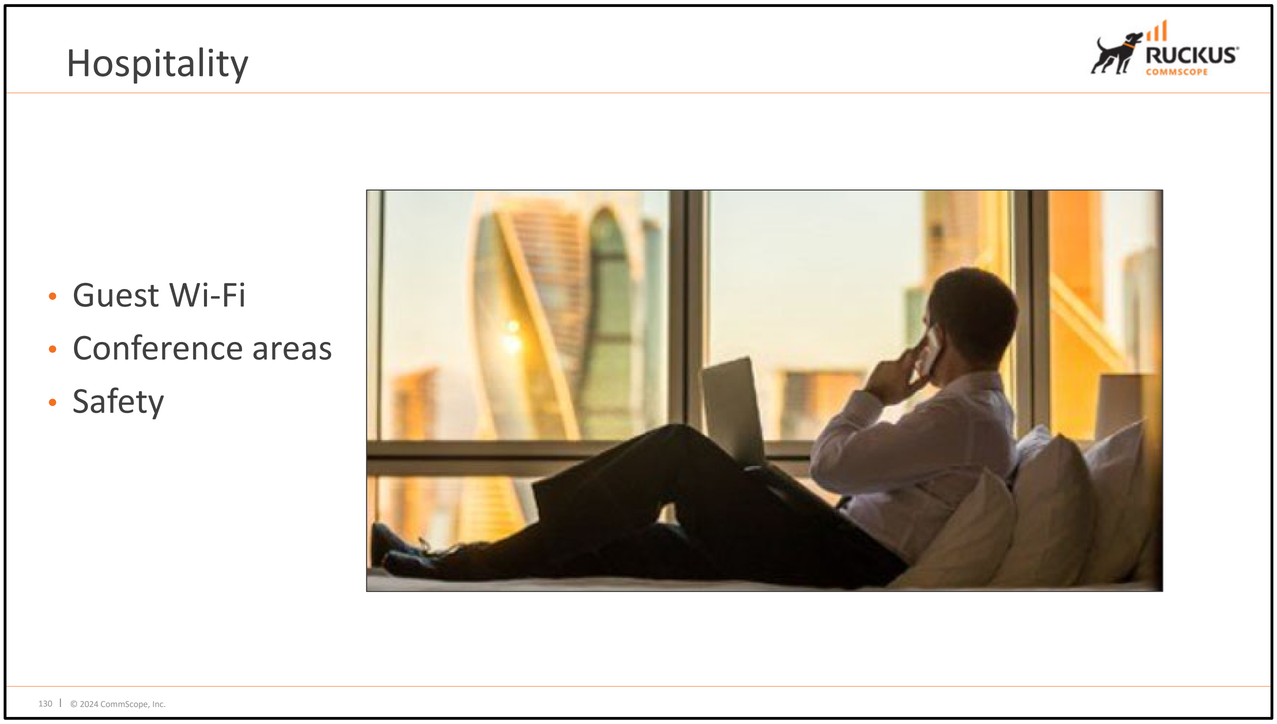
129 | © 2024 CommScope, Inc.

The areas for which Wi-Fi will be used in this environment are smaller than you would find in a typical fixed network but have their own set of challenges.

The devices used onboard aircraft must meet the aviation standards for their use, for safety reasons, as may
those deployed for use on busses, trains or in cars. The placement of APs on aircraft, busses and trains may simply be a matter of allowed mounting points and not a matter of what you learn in a physical site survey.

Often the APs used will have their own cellular radios for connecting to a backhaul. Some bus networks connect to the Internet via
the municipal Wi-Fi provided by the city.

Many school districts provide Wi-Fi on their buses to allow students access to resources for study. This enables students who may
not have an Internet connection at home additional Internet time for their learning.

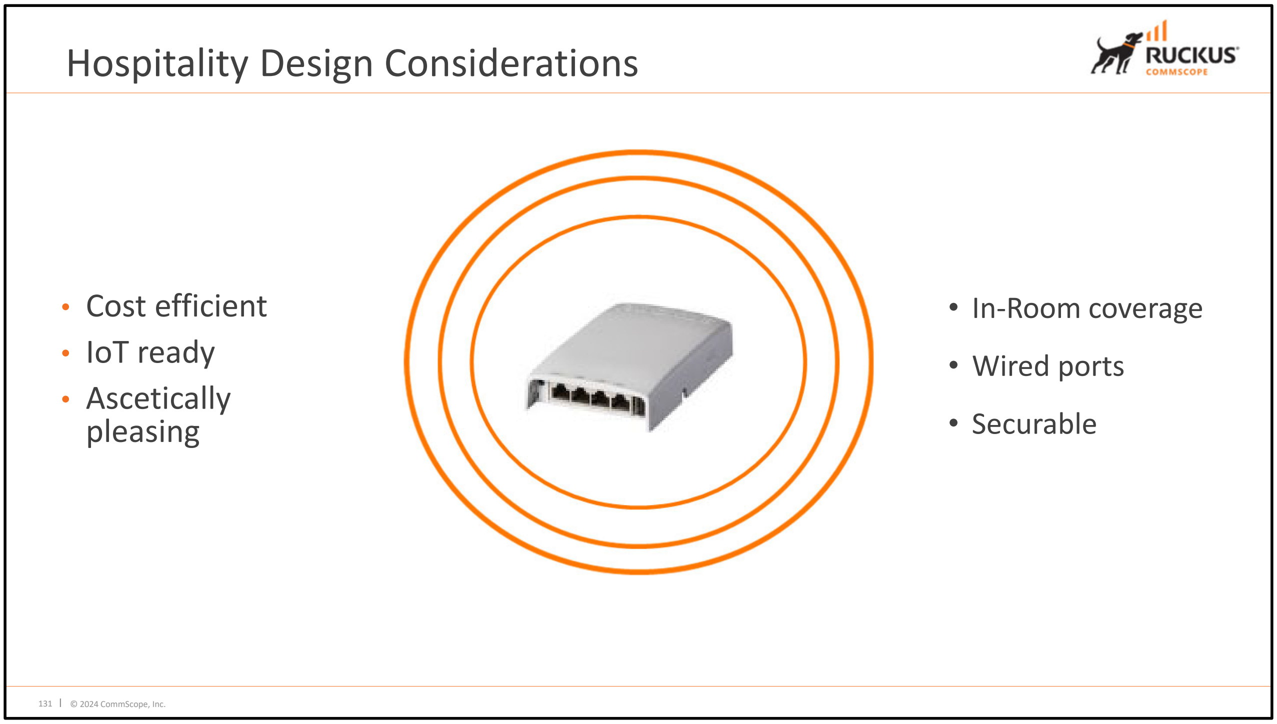


Hospitality

- Guest Wi-Fi
- Conference areas
- Safety

Today's business and leisure travelers expect high-speed Internet connectivity for their smart devices everywhere. 83% of hotel guests take the time to report a bad Wi-Fi experience, and 36% won't rebook that property if they have had one. If hotels do not provide guests with fast, reliable Internet connections, they are unlikely come back or recommend the property to others.

RUCKUS's wired and wireless solutions are the gold standard for hospitality worldwide. There's a reason why 70% of the hospitality market—and 86% of the world's luxury properties—rely on RUCKUS Smart Wi-Fi. Guest Wi-Fi is an expected amenity. Some hotels charge for it, others include it with your stay and some offer premium access for additional fees. However, all major hotel chains do provide guest Wi-Fi today. In early deployments in hospitality, the Wi-Fi may have only been found in common areas like the lobby and conference rooms. Now it is in every guest room, conference room, restaurant, lounge, fitness center, business center and even in outdoor areas like pool side. Hotels realized years ago that to attract guest they needed to add phones and televisions in their rooms. Today, it is Wi-Fi. Wi-Fi is even part of a Safety plan in most hotel chains. It enables smart locks and cameras to be used in enhancing security for both guests and staff alike.



Hospitality Design Considerations

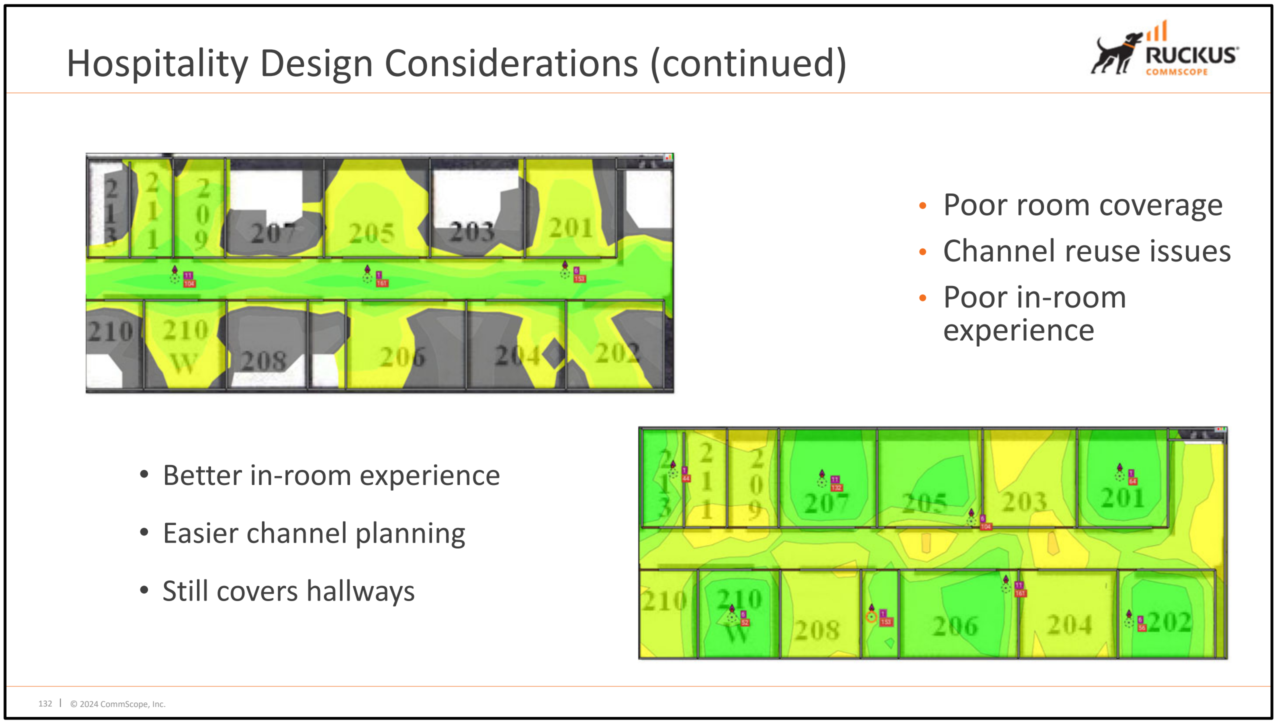
- Cost efficient
- IoT ready
- Ascetically pleasing

- In-Room coverage
- Wired ports
- Securable

131 |

Due to the increased device density found in hospitality, the way you design for Wi-Fi in hotels has changed. Some hotels to save money used to deploy a few APs per floor in the halls to achieve a coverage only plan. Sure there was Wi-Fi in each room, but it was not a good network design. Guest quickly began to stay in hotels where the Wi-Fi was designed for throughput, airtime utilization and device density. They did not know what was required of the design to make this happen. They only knew that when they stayed in some hotels the Wi-Fi worked better than in others.

So, how do you achieve the goal of good Wi-Fi in hospitality? You design and implement for airtime utilization, device density and throughput. This may mean using an AP in every guest room. That sounds very expensive at first but is really not. You can design for one wall mounted AP in each guest room to provide both wired and wireless connectivity. These very affordable AP and switch in one units allow you to deliver the full range of in-room services while dramatically reducing cabling, installation time, and construction costs. These devices have low gain antennas, reducing the cell size of each AP and assisting you in making a solid channel use plan for a high volume of APs deployed in such an area. They also have wired ports to provide connectivity to things such as phones and televisions, reducing wiring costs.



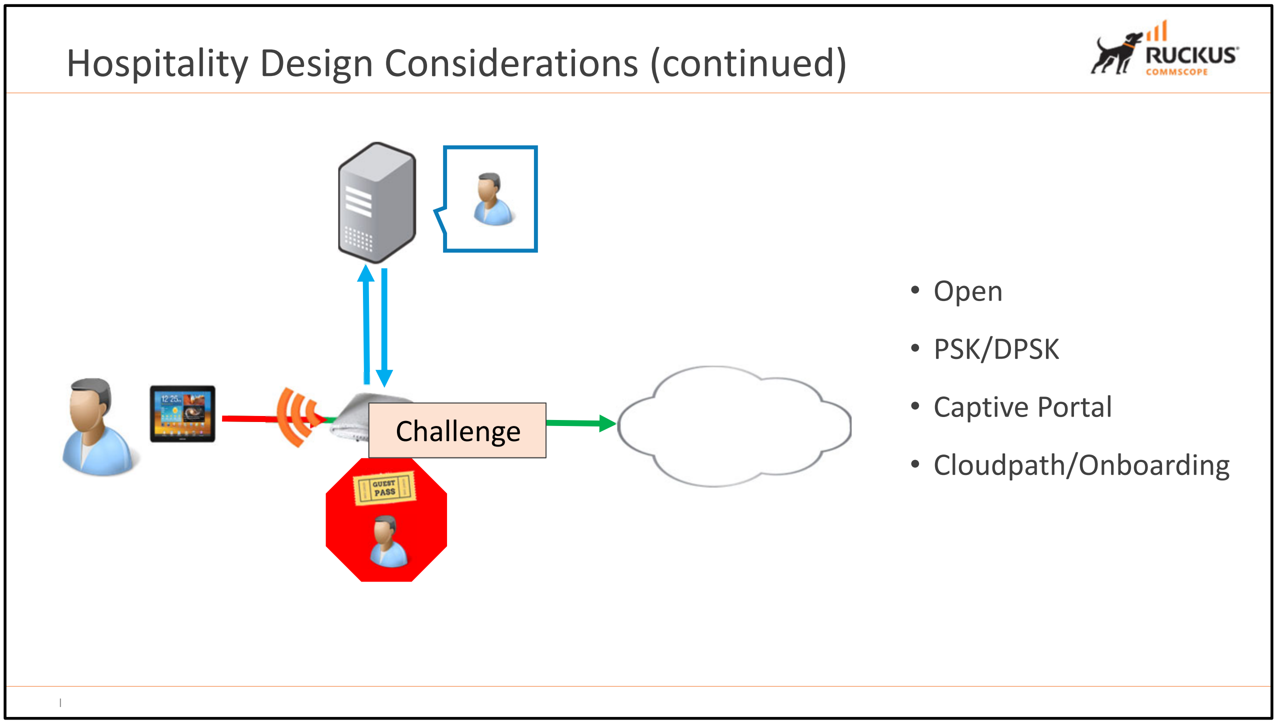
Hospitality Design Considerations (continued)

- Poor room coverage
- Channel reuse issues
- Poor in-room experience

- Better in-room experience
- Easier channel planning
- Still covers hallways

When using one wall mounted AP per room, you remove the need for APs in hallways. APs placed in the hallway do not only look bad but also provide poor connectivity to devices in rooms, due to hidden nodes, poor channel reuse options and near far problems. Using these smaller APs in each guest room will allow you to provide better in-room user experience and reduce costs of wiring and hardware. Their use can also offer coverage in the halls, if needed. This design also greatly reduces your site survey and design time.

You should still conduct a physical site survey to locate sources of non-802.11 interference and neighboring networks as well as to potentially locate any rogue devices. Other areas of the hotel may require different AP model types, because their intended uses are different and will better meet the needs of those requirement areas.

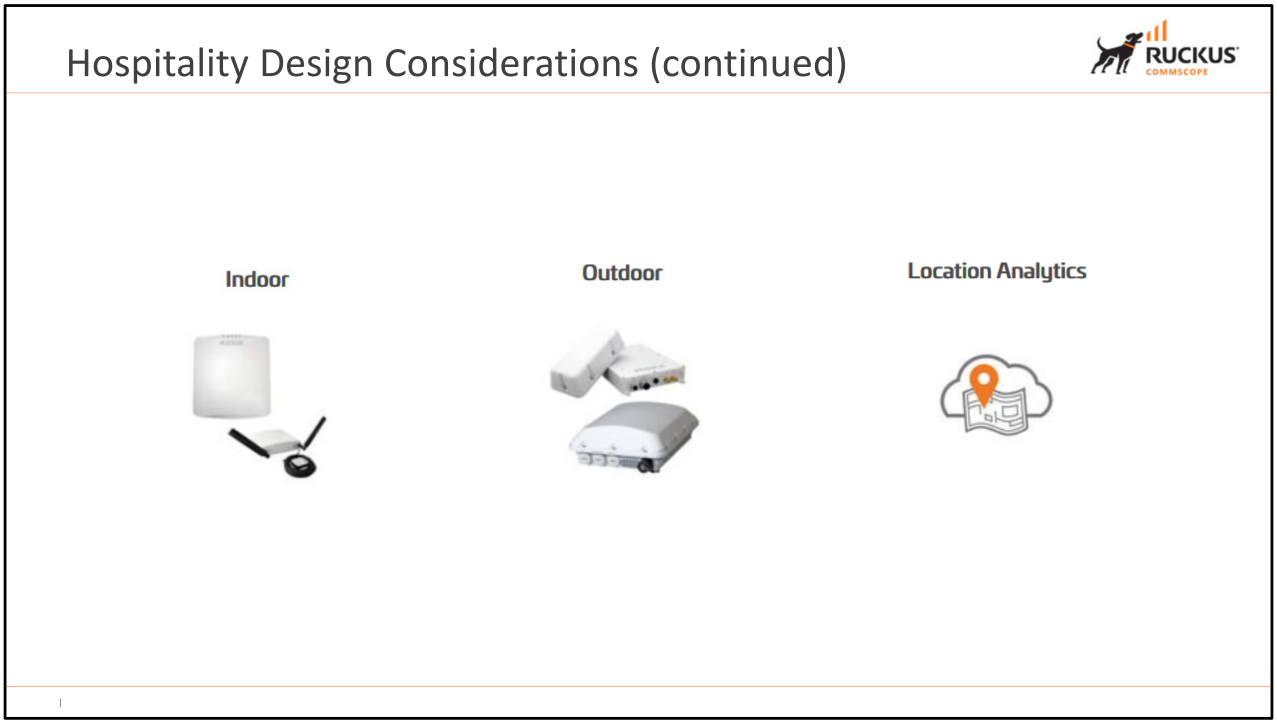


Hospitality Design Considerations (continued)

- Open
- PSK/DPSK
- Captive Portal
- Cloudpath/Onboarding

Authentication for hotel guests vs. staff is also a consideration when implementing within the hospitality vertical. There are many ways hotels choose to do this from

Open networks, requiring no authentication at all, to the use of an onboarding solution such as Cloudpath. No matter the authentication method you choose, you should strive to make it's use as easy as possible for the guests, not only in this vertical but also in all others. Guest defiantly want a good user experience when using the network. That begins with the WLAN being easy to join. The hotel staff members, for the most part, are not IT professionals and should not be involved in connecting guest devices to the network. The method chosen should require the least amount of staff-guest interaction for authentication that meets your customer's guest security policies.



Hospitality Design Considerations (continued)

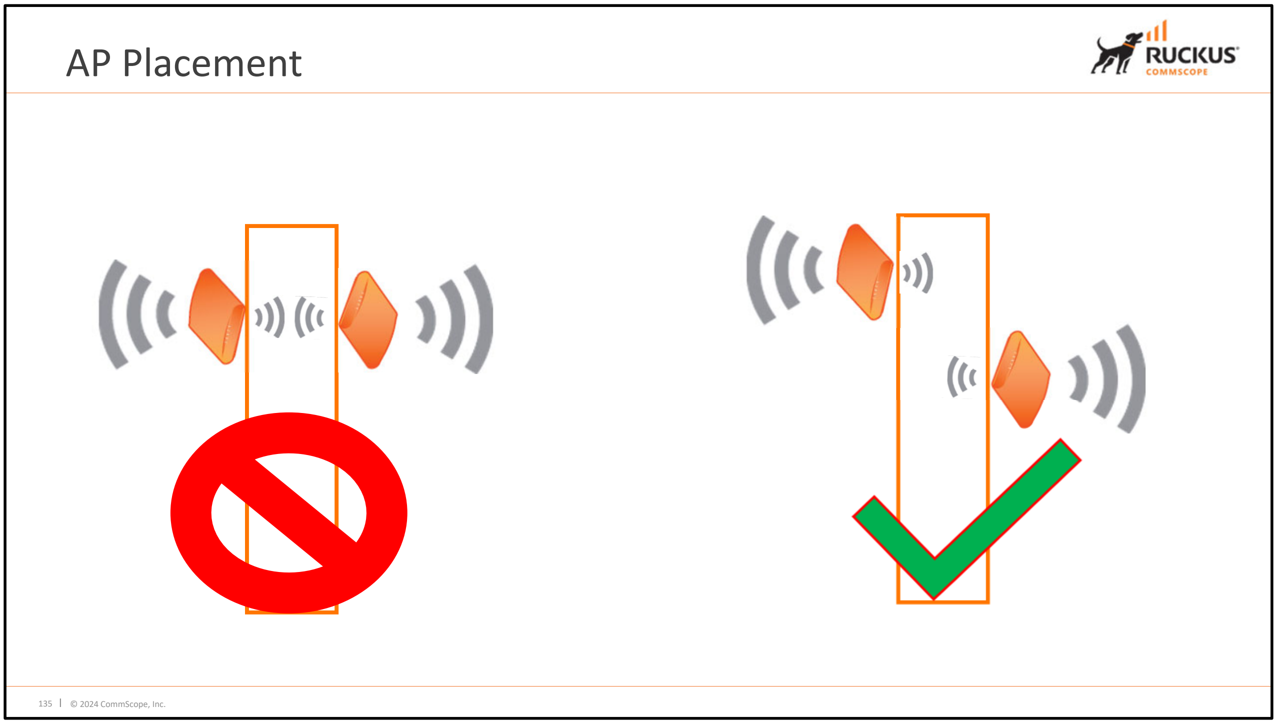
Indoor

Outdoor

Location Analytics

Hospitality Wi-Fi usually involves coverage for both indoor and outdoor locations. Your design should treat different portions of the property as separate requirement areas. You will need to plan for the use of multiple AP models within a hotel deployment, some for indoor areas in and beyond guest rooms and some for outdoor areas such as poolside.

When deploying a new network or updating an older one, it is a good idea to discuss using APs which support the latest protocols. You never know what device types guest will want to use on the network. Supporting the latest protocols helps to ensure guest satisfaction and to prolong the life of the WLAN. Additionally, you may need to plan for the use of non-Wi-Fi wireless communications such as Zigbee, for door locks etc. and Bluetooth Low Energy, for BLE Beaconing used in convention centers and resorts in assisting guest in finding amenities and meeting rooms. You may even need to plan for additional services for your customer to collect information about where the Wi-Fi is being used. Selecting APs for different use across the entire property is more difficult than selecting a single AP model for an office area.



AP Placement

Students and teachers alike will have their own devices, in addition to the devices provided by the school system, much like BYOD networks. Schools usually have very tight budgets. Some people advocate one AP or more per classroom while others try to cover more rooms with fewer APs. The best practice is to provide enough APs to ensure all the devices can connect in your requirement areas and have the desired amount of airtime just as in any other environment. This may mean more than one AP in a class or one AP for a few classrooms.

Each school should be evaluated on its needs. Higher education, colleges and universities, demands Wi-Fi too but also has large lecture halls and dorm rooms to cover, making them a hybrid design which combines classrooms, large venue, office space and a hospitality like environment as well. Students expect good Wi-Fi in the dorms for learning but also expect it for online gaming. Remember, the students are the customer of the higher education facility. Their expectations should be part of your design. You will find yourself using multiple design strategies in higher education. As for AP placement, the dorms should be treated like hotel rooms. You may use wall plate APs in each dorm room and other APs to cover common areas and outdoor space.

In addition to the cabling issues discussed earlier, the physical location in each room matters too. As you can see in this illustration, the APs are mounted back to back on opposite sides of the wall. This is a bad practice. The rear lobes of an AP will cause EMI for the AP on the opposite side of the wall. It is better to offset the APs as much as possible or mount them from the ceiling to avoid rear lobe interference and improve your channel usage.

Client Device Carts

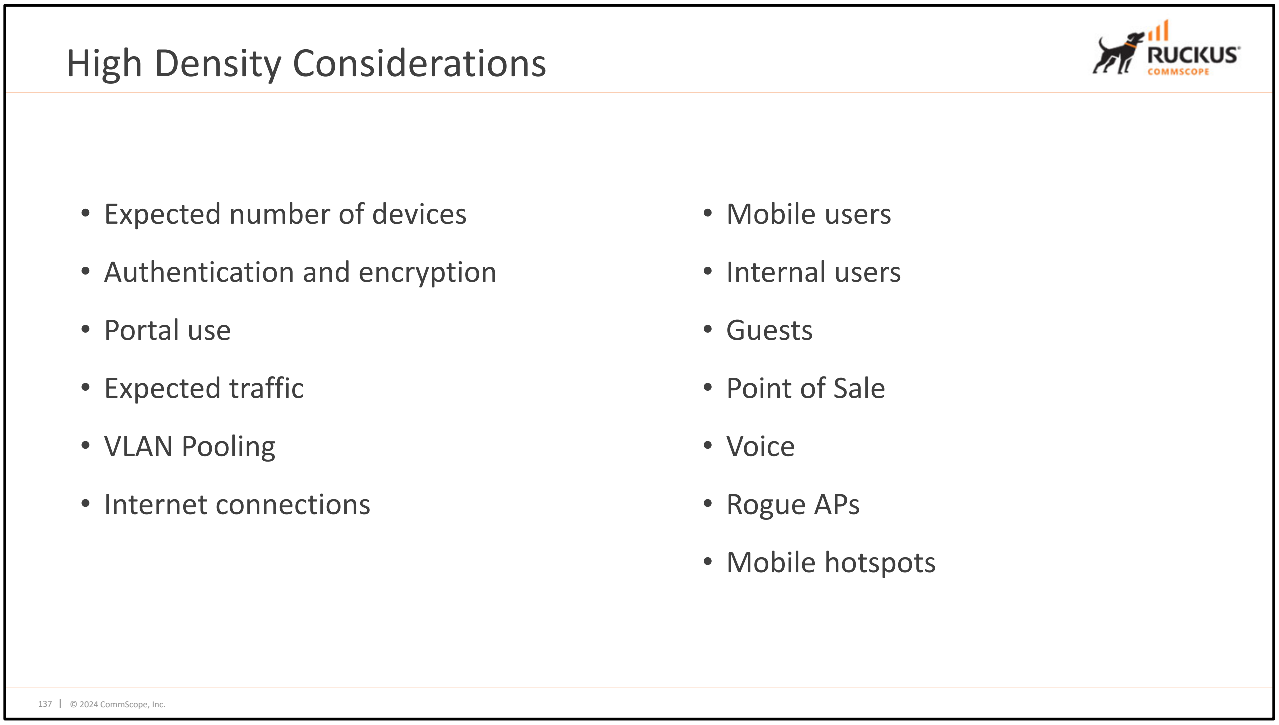
- Once popular
- Still in use
- Most likely stocked with legacy client stations

- Sudden increased client count
- Sudden increased airtime utilization
- Possible addition of an AP in the space

136 | © 2024 CommScope, Inc.

You should determine in your information gathering if the school uses device carts. These were once a very popular way to provide a room full of students with laptops or tablets. They are still in use but are not so popular as they once were.

What will these do to your WLAN? They can suddenly add 30 or more laptops or tablets in a room. These devices may only support legacy technologies, impacting your WLAN configurations. They may add an AP into the space. They will allow for increased airtime utilization where deployed.



High Density Considerations

- Expected number of devices
- Authentication and encryption
- Portal use
- Expected traffic
- VLAN Pooling
- Internet connections

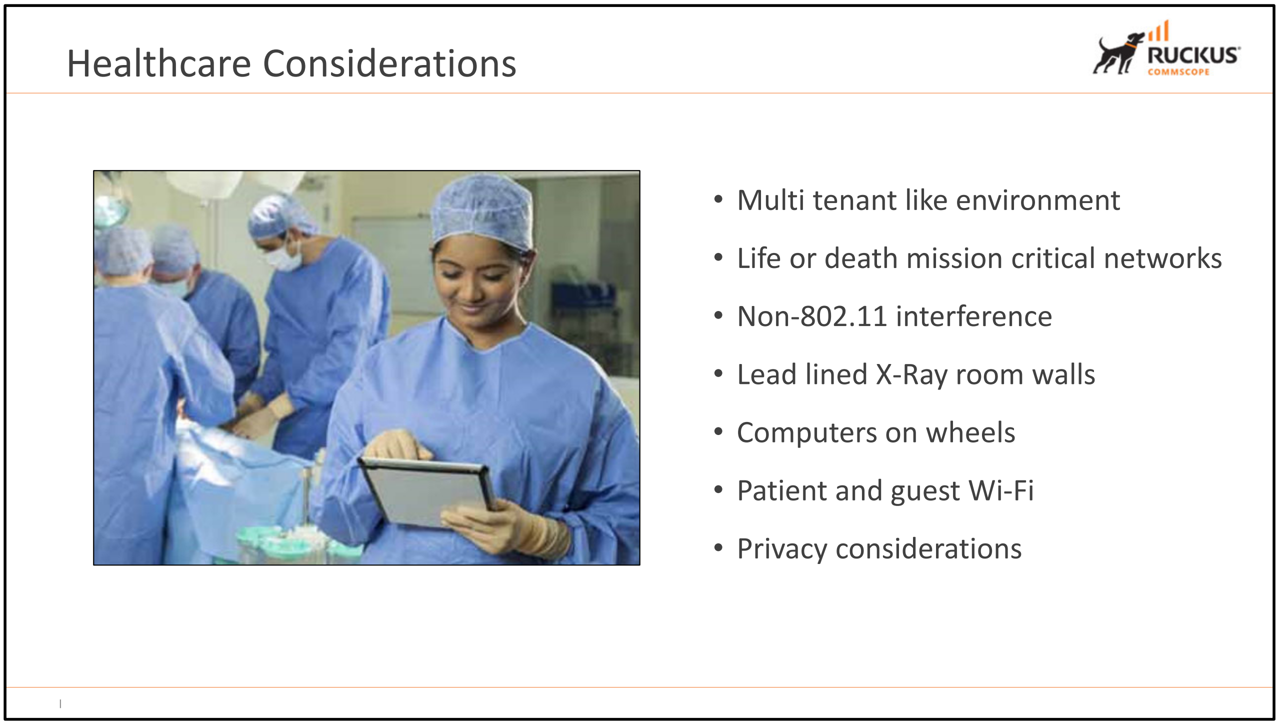
- Mobile users
- Internal users
- Guests
- Point of Sale
- Voice
- Rogue APs
- Mobile hotspots

137 | © 2024 CommScope, Inc.

Designing and deploying for a high-density environment has many things in common with other designs, such as the expected number of devices and devices types, decisions the authentication and encryption to be used, the bands to be supported, captive portal use, expected traffic and Internet connection needs. Everything is just on a much larger scale. You will also need to take into account the human bodies in the space. Humans are mostly liquid and will block propagation of RF signals. Large dense crowds will have an effect on Wi-Fi, something you may not encounter in simple office deployments. A part of all designs should be the number of devices simultaneously connected to and passing traffic through a single AP radio. Although the radios used in APs can support many connections, you really have to worry about throughput.

Devices simply connected but not passing traffic take up device count but do not impact traffic. A small number of very active devices may take up a lot of airtime. This holds true in all deployments. In high density deployments you will need to properly design for load balancing across the Aps and within the wired network too. The methods of client load balancing are well covered in the RASZA 200 course. Even though you are designing a WLAN, you can not forget that the WLAN must use the wired network too.

If you are in a stadium, for example, you may have decided to use many small APs mounted in lockable enclosures under the seats to cover small sections of the seating areas along with APs mounted on walls and or poles as additional coverage allowing you to break up the collision domains into smaller pieces, giving you better airtime utilization. You may have a great channel plan or be using ChannelFly. However, if you do not segment the user traffic on the wired side, there will still be problems.



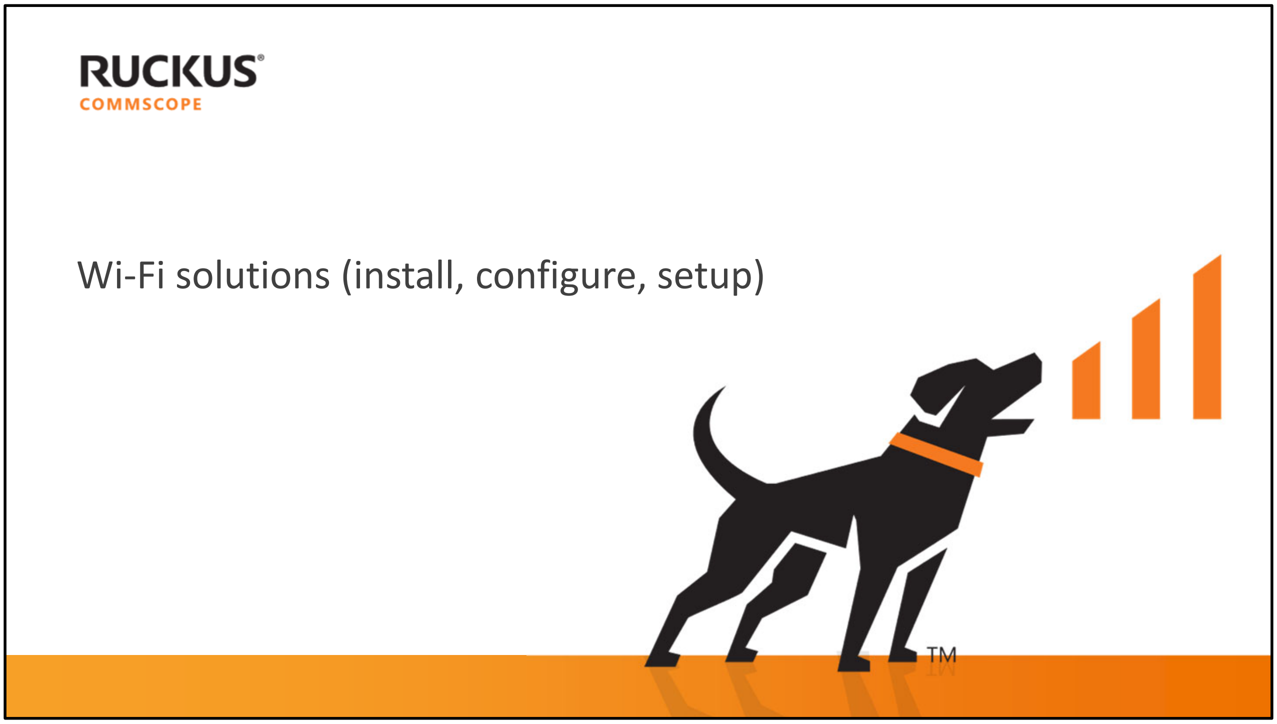
Healthcare Considerations

RUCKUS
COMMSCOPE

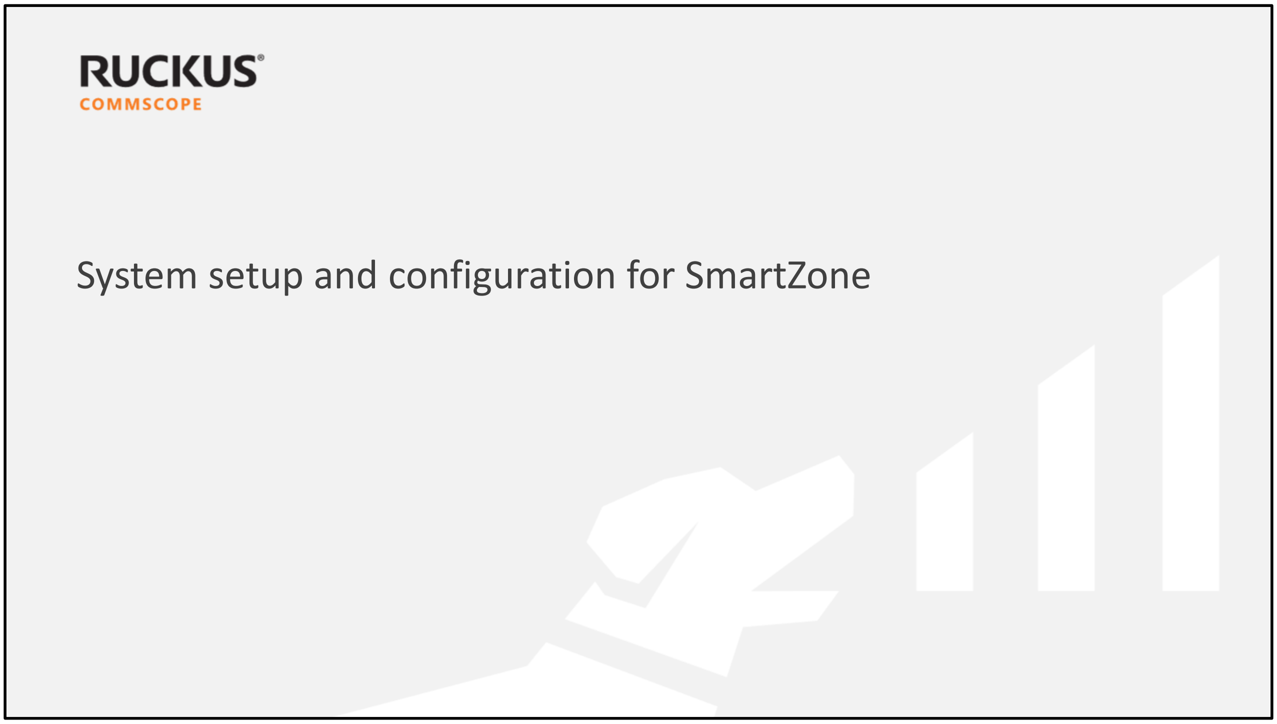
- Multi tenant like environment
- Life or death mission critical networks
- Non-802.11 interference
- Lead lined X-Ray room walls
- Computers on wheels
- Patient and guest Wi-Fi
- Privacy considerations

From small clinics to large hospitals, Wi-Fi has become a part of patient care and satisfaction. Healthcare, however, is a difficult vertical within which to design and build WLANs. Most hospitals are really multi-tenant buildings, with several medical groups, insurance companies, small businesses, patients and guests all wanting Wi-Fi.

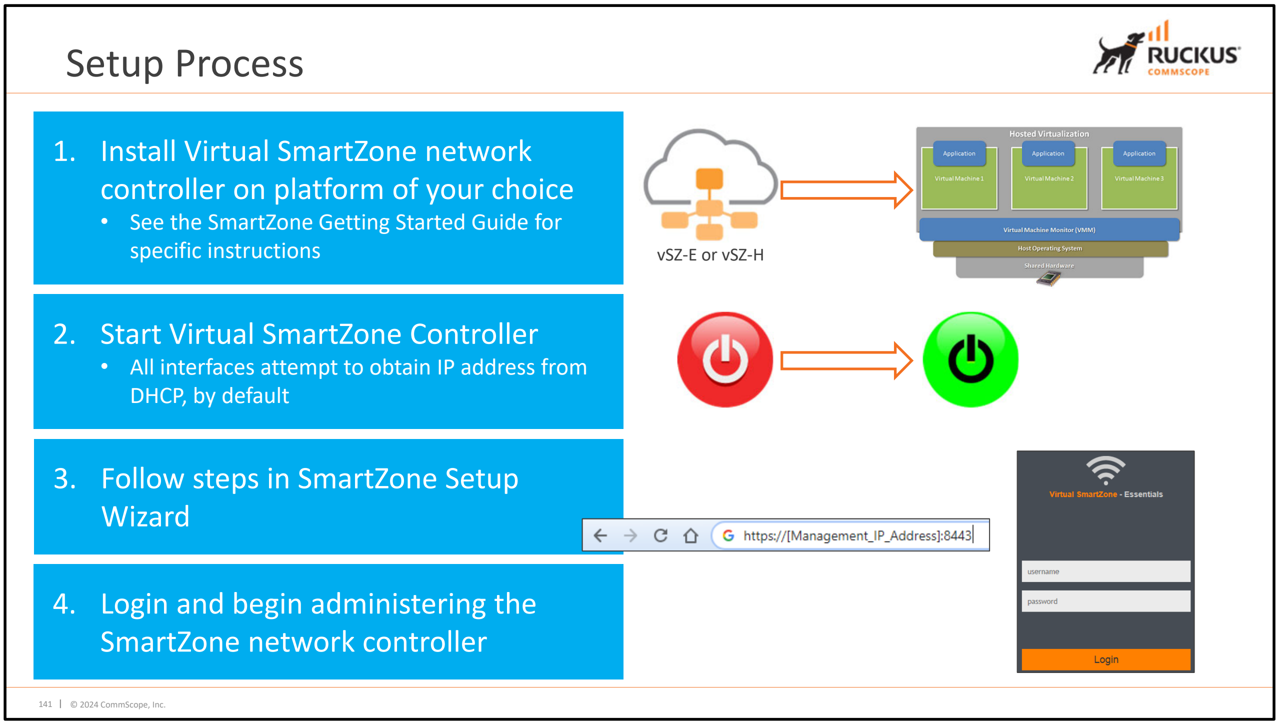
If there is no coordination of Wi-Fi usage, planning will be difficult. In addition to increased contention, co-channel interference, high airtime utilization and legacy device support requirements, this is also a challenging RF environment having many sources of non-802.11 interference. Designing for a hospital may be the most if not one of the most challenging designs you will ever encounter.



Wi-Fi solutions (install, configure, setup)



System setup and configuration for SmartZone



Setup Process

1. Install Virtual SmartZone network controller on platform of your choice
   - See the SmartZone Getting Started Guide for specific instructions
2. Start Virtual SmartZone Controller
   - All interfaces attempt to obtain IP address from DHCP, by default
3. Follow steps in SmartZone Setup Wizard
4. Login and begin administering the SmartZone network controller

141 | © 2024 CommScope, Inc.

Step 1: Install the Virtual SmartZone network controller on platform of your choice

- See the SmartZone Getting Started Guide for specific instructions

Step 2: Start the Virtual SmartZone Controller

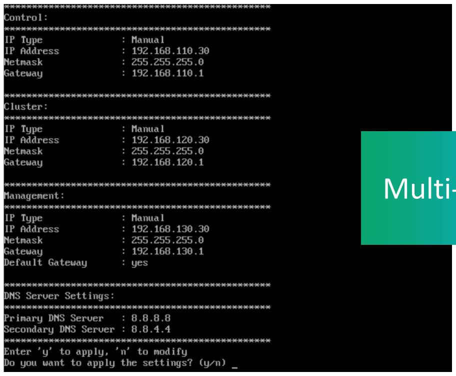
- By default, all interfaces on the controller will attempt to obtain IP address from a DHCP. If IP addresses are successfully obtained, you connect to the IP address of the Management interface as shown and proceed to the next step.
  If IP addresses are not obtained, the CLI Initial Setup must be performed. (see next page for details).
- Additionally, if you are configuring a 1 NIC setup, you must go into the VM after the appliance is deployed, but before it is booted to remove the extraneous NICs. You can do this by unchecking “power on automatically” on the virtual machine import wizard.

Step 3: Follow the steps in the SmartZone Setup Wizard to define cluster and system information.

Step 4: Login and begin administering the SmartZone network controller.

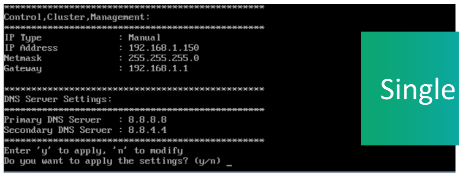
CLI Initial Setup

- If DHCP server is not available, CLI setup must be performed
- CLI initial setup allows you to:
  - Specify edition: Essentials or High Scale
  - Assign IP addresses



```
************************************************
Control:
************************************************
IP Type              : Manual
IP Address           : 192.168.110.30
Netmask              : 255.255.255.0
Gateway              : 192.168.110.1

************************************************
Cluster:
************************************************
IP Type              : Manual
IP Address           : 192.168.120.30
Netmask              : 255.255.255.0
Gateway              : 192.168.120.1

************************************************
Management:
************************************************
IP Type              : Manual
IP Address           : 192.168.130.30
Netmask              : 255.255.255.0
Gateway              : 192.168.130.1
Default Gateway      : yes

************************************************
DNS Server Settings:
************************************************
Primary DNS Server   : 8.8.8.8
Secondary DNS Server : 8.8.4.4
************************************************
Enter 'y' to apply, 'n' to modify
Do you want to apply the settings? (y/n) _
```

Multi-NIC

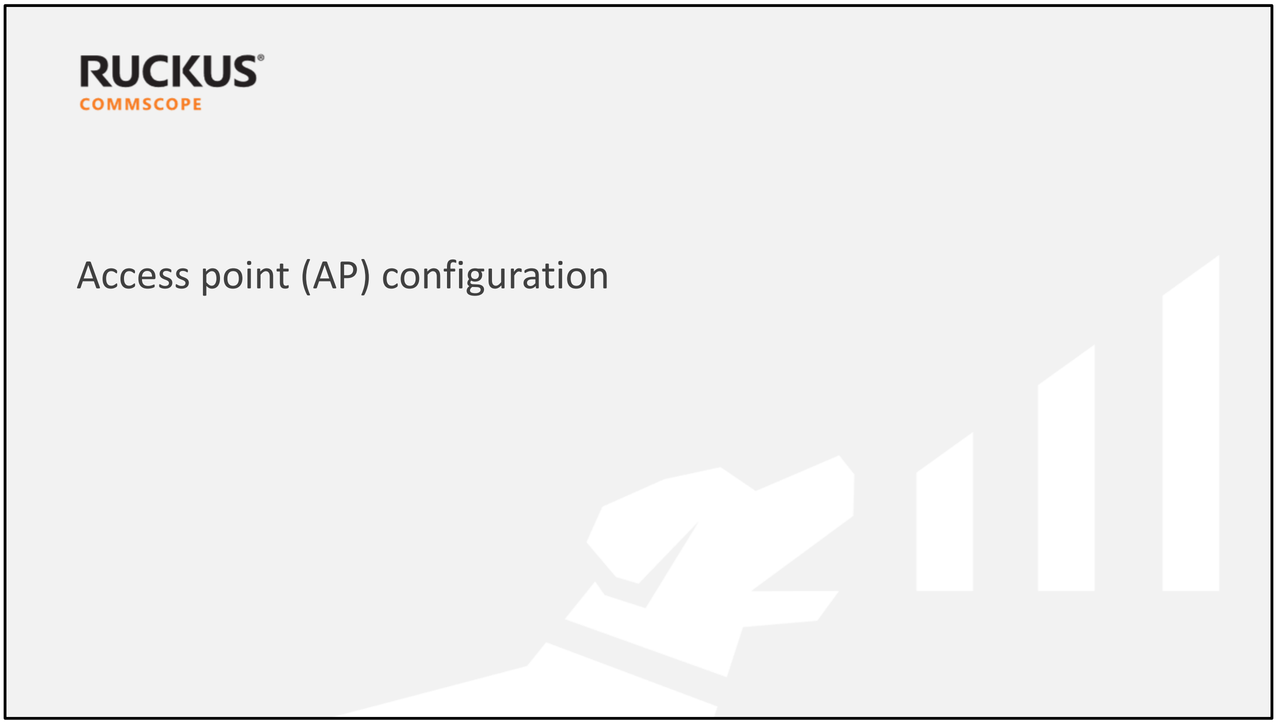


```
************************************************
Control,Cluster,Management:
************************************************
IP Type              : Manual
IP Address           : 192.168.1.150
Netmask              : 255.255.255.0
Gateway              : 192.168.1.1

************************************************
DNS Server Settings:
************************************************
Primary DNS Server   : 8.8.8.8
Secondary DNS Server : 8.8.4.4
************************************************
Enter 'y' to apply, 'n' to modify
Do you want to apply the settings? (y/n) _
```

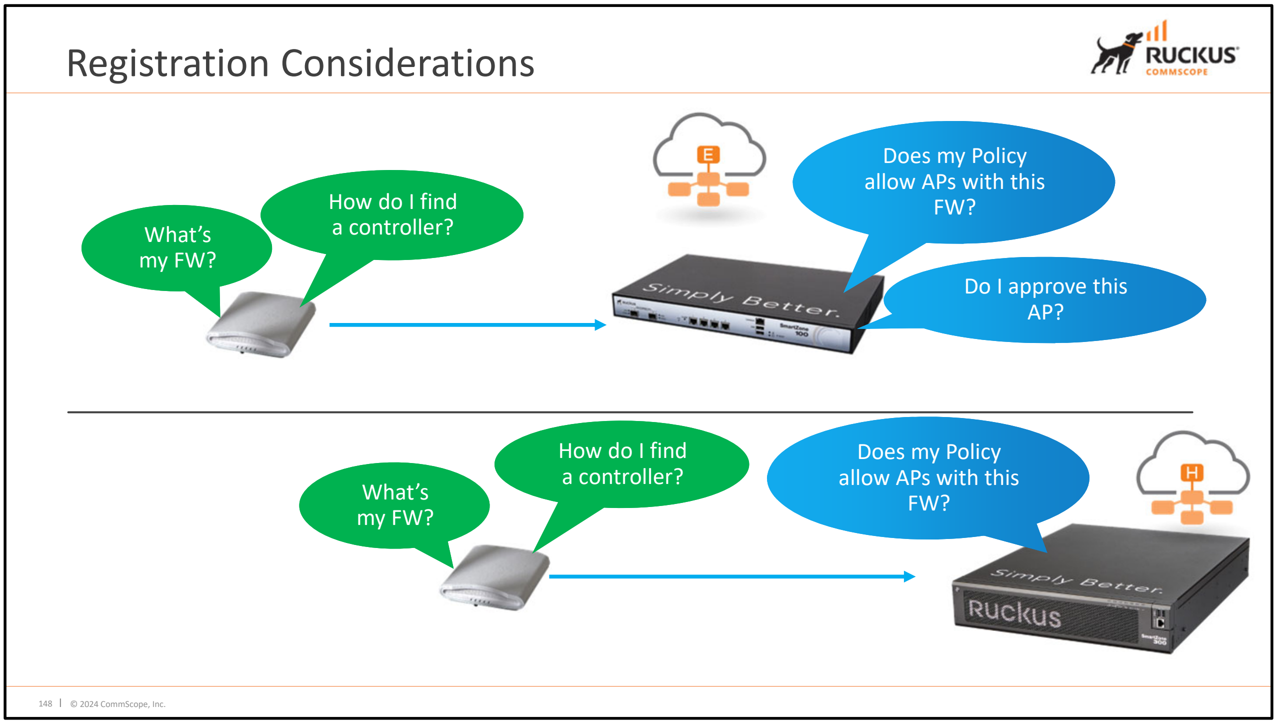
Single NIC

If there is no DCHP server available for the Management interface, the CLI setup utility must be run. The CLI can be accessed through the VM management platform or the console interface of the SmartZone 100 or 300 hardware platform.

During the initial setup on a Virtual SmartZone you will define whether the network controller will run as an Essentials or High Scale edition (This is determined by the hardware in the physical platforms). Then you will configure IP addresses based on the number of discovered virtual interfaces on the virtual machine. After completion, a summary page will be displayed allowing you to confirm the settings.



Access point (AP) configuration

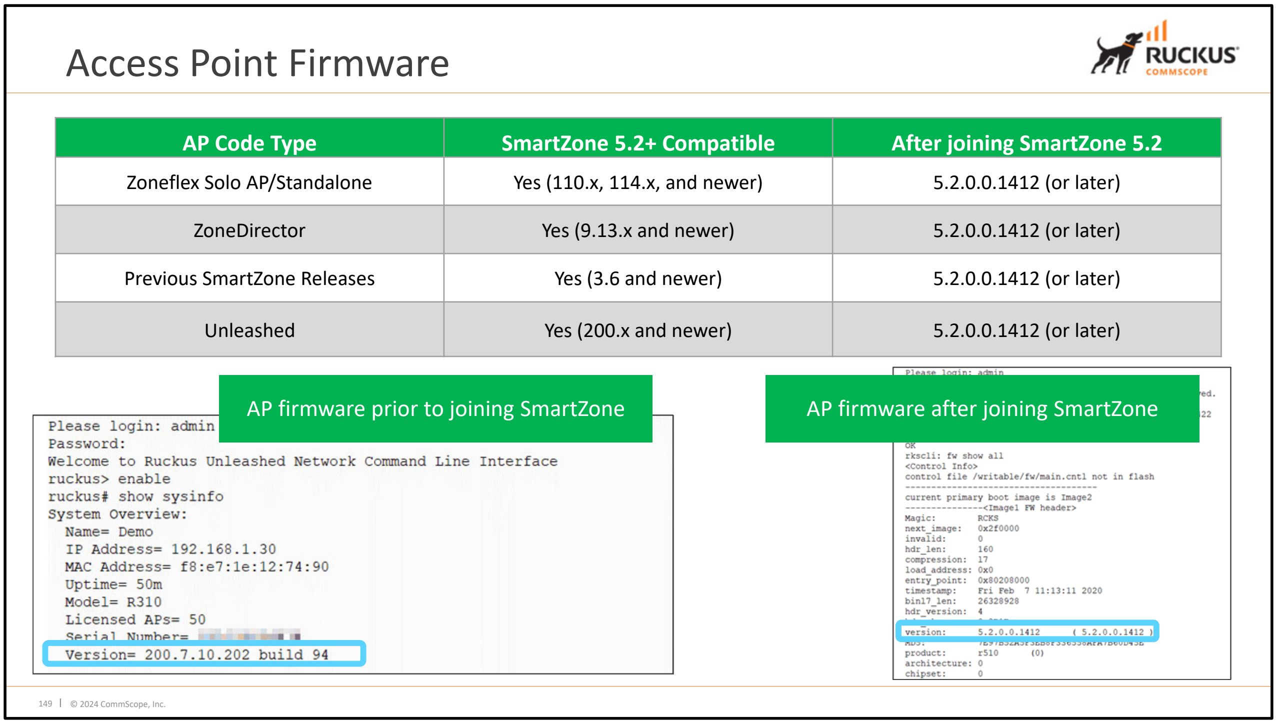


Registration Considerations

RUCKUS COMMSCOPE
E
What's my FW?
How do I find a controller?
Does my Policy allow APs with this FW?
Do I approve this AP?
Simply Better.
SmartZone 100
H
What's my FW?
How do I find a controller?
Does my Policy allow APs with this FW?
Simply Better.
Ruckus
148 | © 2024 CommScope, Inc.

Before attempting to register Access Points to a controller, there are some questions that need to be considered:

- What firmware is the Access Point running and how will that influence its connection to a controller?
- How will the Access Point find the controller address? Should this be a manual or automated process?
- Does the Controller Policy allow the Access Points to connect?
- Does the SmartZone Essentials policy require you to manually approve Access Points?



Access Point Firmware

AP Code Type	SmartZone 5.2+ Compatible	After joining SmartZone 5.2
Zoneflex Solo AP/Standalone	Yes (110.x, 114.x, and newer)	5.2.0.0.1412 (or later)
ZoneDirector	Yes (9.13.x and newer)	5.2.0.0.1412 (or later)
Previous SmartZone Releases	Yes (3.6 and newer)	5.2.0.0.1412 (or later)
Unleashed	Yes (200.x and newer)	5.2.0.0.1412 (or later)

AP firmware prior to joining SmartZone

```
Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# show sysinfo
System Overview:
  Name= Demo
  IP Address= 192.168.1.30
  MAC Address= f8:e7:1e:12:74:90
  Uptime= 50m
  Model= R310
  Licensed APs= 50
  Serial Number= [redacted]
  Version= 200.7.10.202 build 94
```

AP firmware after joining SmartZone

```
Please login: admin
OK
rkscli: fw show all
<Control Info>
control file /writable/fw/main.cntl not in flash
-------------------------------------
current primary boot image is Image2
---------------<Image1 FW header>
Magic:        RCKS
next_image:   0x2f0000
invalid:      0
hdr_len:      160
compression:  17
load_address: 0x0
entry_point:  0x80208000
timestamp:    Fri Feb  7 11:13:11 2020
bin17_len:    26328928
hdr_version:  4
version:      5.2.0.0.1412      ( 5.2.0.0.1412 )
MD5:          7E97B52A5F3EB8F336558AFA7B60D45E
product:      r510      (0)
architecture: 0
chipset:      0
```

149 | © 2024 CommScope, Inc.

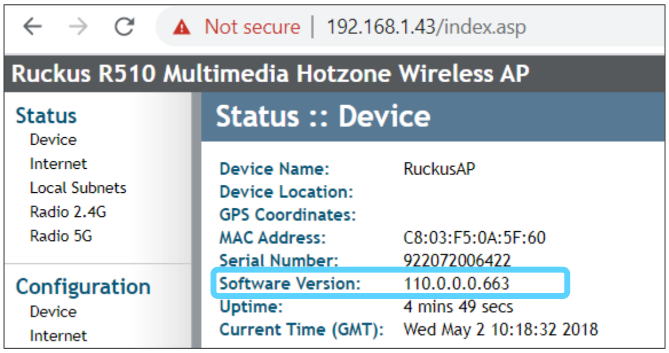
You may see the code that the Access Point runs referred to as either "software" "or "firmware". These phrases are used interchangeably. We will refer to the Access Point and Controller code as "firmware".

As mentioned previously the first consideration for AP registration is the AP's firmware. In order to connect an AP to SmartZone release 5.2 it must be running supported versions of the following firmware types:

- Solo AP firmware
- Zone Director firmware
- Previous Release SmartZone firmware
- Unleashed firmware

Once an AP has successfully connected to a SmartZone instance, SmartZone will replace the firmware on the AP with SmartZone firmware . Once the SmartZone firmware is loaded, previous methods of AP management (for example; unleashed) will no longer be available unless those firmware types are re-established.

Access Point Firmware and Banks



Ruckus R510 Multimedia Hotzone Wireless AP

Status :: Device

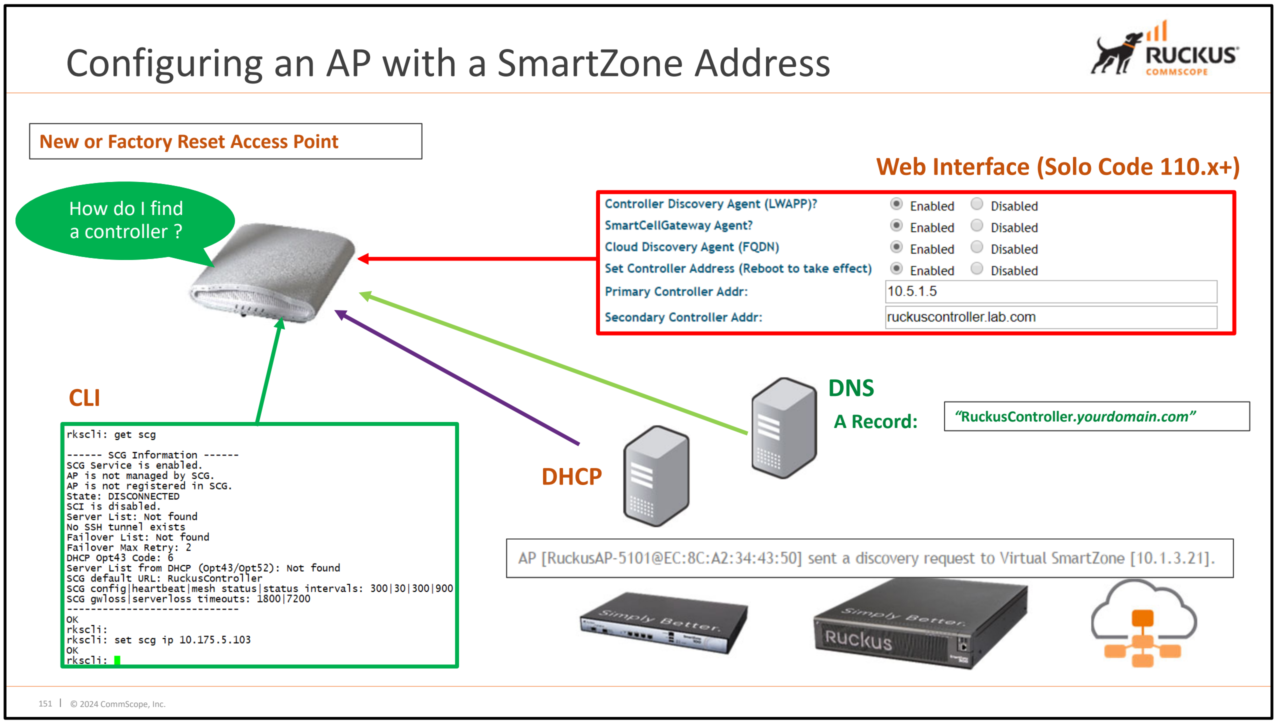
```
Device Name:          RuckusAP
Device Location:
GPS Coordinates:
MAC Address:          C8:03:F5:0A:5F:60
Serial Number:        922072006422
Software Version:     110.0.0.0.663
Uptime:               4 mins 49 secs
Current Time (GMT):   Wed May 2 10:18:32 2018
```

What's my firmware?

RUCKUS Access Points

- Ship with code 110.x (March 2020)
- Store firmware in two locations:
  - Bank 1
  - Bank 2
- Upgrade firmware when joining:
  - ZoneDirector – to ZD firmware
  - SmartZone – to SmartZone firmware

Before registering Access Points to the controller, the first step is to identify the firmware currently running on the Access Points. At the time this course was created (March 2020) new Access Points shipped from the factory have code 110.x pre-installed. If the AP was ordered with Unleashed firmware from the factory (which is possible depending on which AP SKU was selected) additional commands are required for the registration process.



Configuring an AP with a SmartZone Address

New or Factory Reset Access Point

Web Interface (Solo Code 110.x+)

Controller Discovery Agent (LWAPP)?	● Enabled	○ Disabled
SmartCellGateway Agent?	● Enabled	○ Disabled
Cloud Discovery Agent (FQDN)	● Enabled	○ Disabled
Set Controller Address (Reboot to take effect)	● Enabled	○ Disabled
Primary Controller Addr:	10.5.1.5	
Secondary Controller Addr:	ruckuscontroller.lab.com	

CLI

```
rkscli: get scg

------ SCG Information ------
SCG Service is enabled.
AP is not managed by SCG.
AP is not registered in SCG.
State: DISCONNECTED
SCI is disabled.
Server List: Not found
No SSH tunnel exists
Failover List: Not found
Failover Max Retry: 2
DHCP Opt43 Code: 6
Server List from DHCP (Opt43/Opt52): Not found
SCG default URL: RuckusController
SCG config|heartbeat|mesh status|status intervals: 300|30|300|900
SCG gwloss|serverloss timeouts: 1800|7200
-----------------------------
OK
rkscli:
rkscli: set scg ip 10.175.5.103
OK
rkscli:
```

DHCP

DNS

A Record: "RuckusController.yourdomain.com"

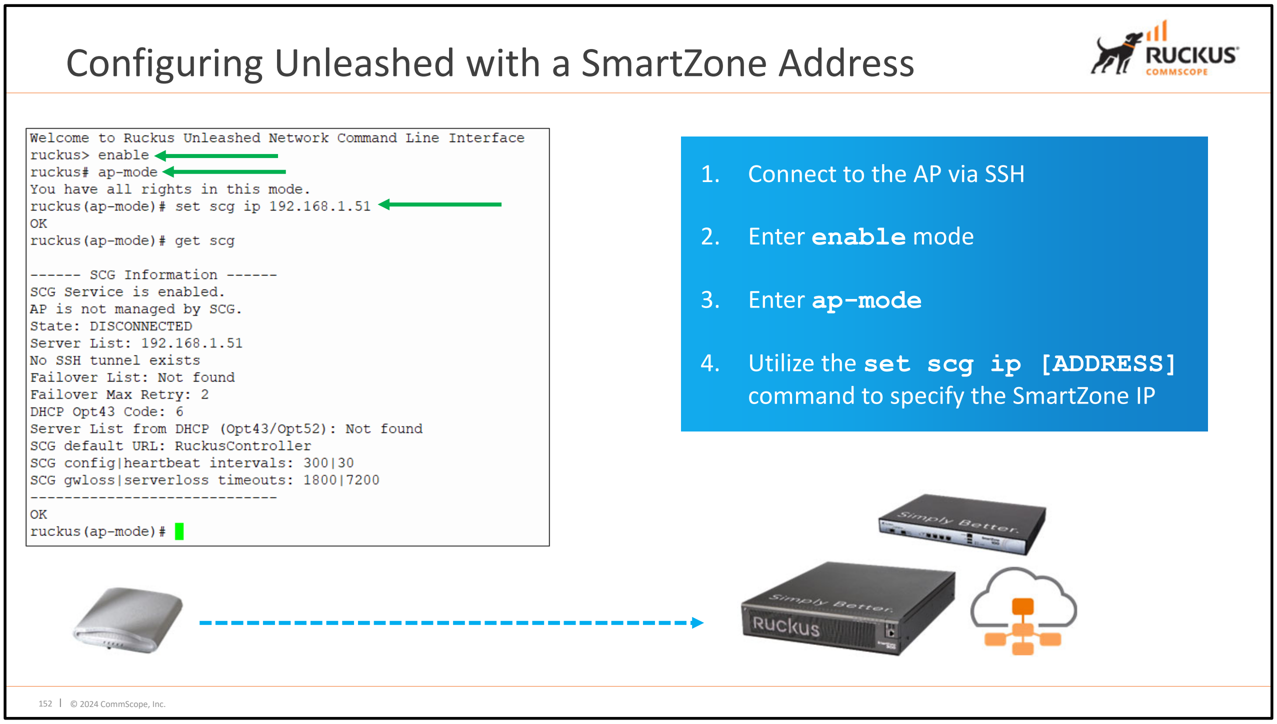
```
AP [RuckusAP-5101@EC:8C:A2:34:43:50] sent a discovery request to Virtual SmartZone [10.1.3.21].
```

151 | © 2024 CommScope, Inc.

Access Points have a number of ways to acquire the IP address of the controller:

- **Web Interface**: The Access Point web interface provides an option to specify a primary and secondary controller address. These can be specified as IP addresses or DNS names. After entering the address, the Access Point may prompt the Administrator for a restart, depending on the code version.
- **CLI**: The controller address can be manually entered via CLI as shown in the previous slide
- **DHCP**: The controller address can be supplied automatically using the scope options in DHCP.
- **DNS**: If your AP is obtaining DHCP, but you don't want to use scope options, a DNS A Record will provide the name resolution of the controller – however you must also ensure the correct Domain Name is supplied within the DHCP scope.

When an Access Point contacts the controller, a message appears in the event log.



Configuring Unleashed with a SmartZone Address

```
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)# set scg ip 192.168.1.51
OK
ruckus(ap-mode)# get scg

------ SCG Information ------
SCG Service is enabled.
AP is not managed by SCG.
State: DISCONNECTED
Server List: 192.168.1.51
No SSH tunnel exists
Failover List: Not found
Failover Max Retry: 2
DHCP Opt43 Code: 6
Server List from DHCP (Opt43/Opt52): Not found
SCG default URL: RuckusController
SCG config|heartbeat intervals: 300|30
SCG gwloss|serverloss timeouts: 1800|7200
-----------------------------
OK
ruckus(ap-mode)#
```

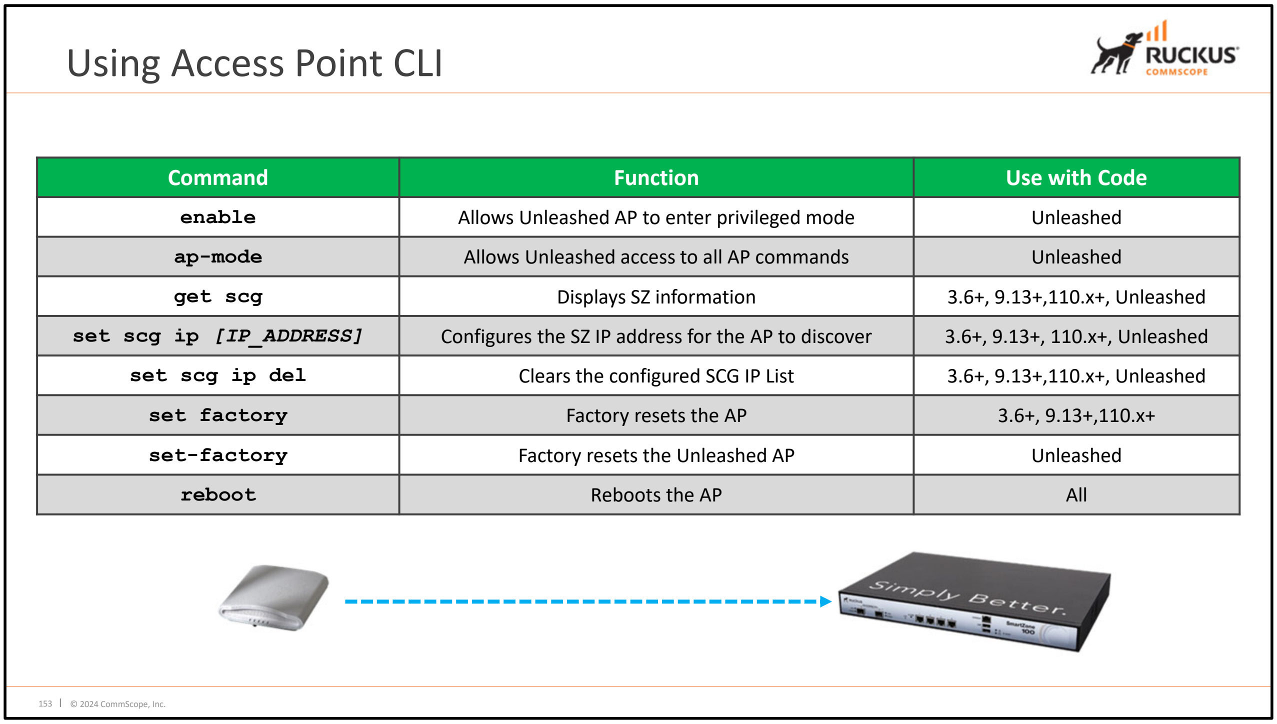
1. Connect to the AP via SSH
2. Enter **`enable`** mode
3. Enter **`ap-mode`**
4. Utilize the **`set scg ip [ADDRESS]`** command to specify the SmartZone IP

152 | © 2024 CommScope, Inc.

Unleashed APs do not provide the ability to configure SmartZone addressing from within the GUI. CLI commands must be used:

1. Connect to the Unleashed AP via SSH
2. Enter `enable` mode on the AP
3. Additionally enter ap-mode which allows access to all AP commands
4. Execute the set scg ip [address] command, specifying the IP of the SmartZone

The AP will initiate contact with SmartZone and will have it's firmware reloaded depending on some additional variables.



Using Access Point CLI

Command	Function	Use with Code
`enable`	Allows Unleashed AP to enter privileged mode	Unleashed
`ap-mode`	Allows Unleashed access to all AP commands	Unleashed
`get scg`	Displays SZ information	3.6+, 9.13+,110.x+, Unleashed
`set scg ip [IP_ADDRESS]`	Configures the SZ IP address for the AP to discover	3.6+, 9.13+, 110.x+, Unleashed
`set scg ip del`	Clears the configured SCG IP List	3.6+, 9.13+,110.x+, Unleashed
`set factory`	Factory resets the AP	3.6+, 9.13+,110.x+
`set-factory`	Factory resets the Unleashed AP	Unleashed
`reboot`	Reboots the AP	All

153 |

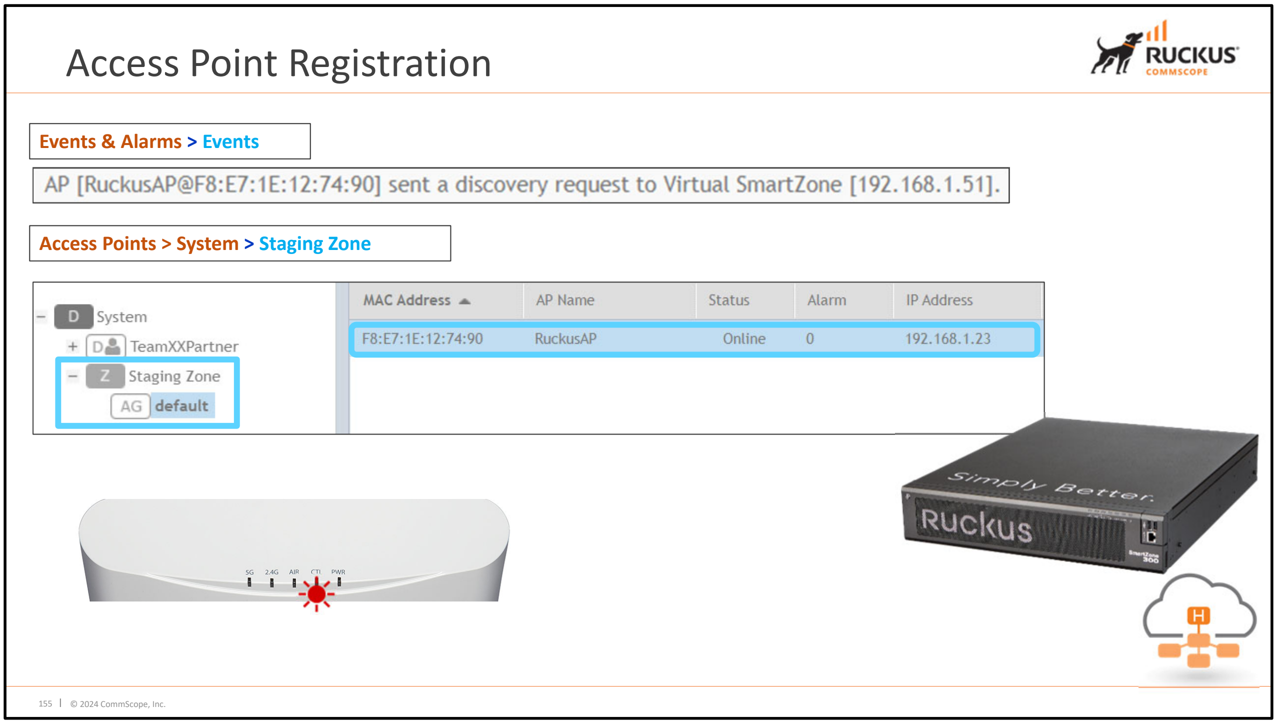
Shown is a summary of CLI commands used on an Access Point when manual configuration is needed to establish connectivity to SmartZone.

The most common CLI commands you will use to connect an Access Point to a SmartZone controller are:

- **`get scg`** - Displays SmartZone controller configuration information (if any exists)
- **`set scg ip [IP_ADDRESS]`** - Configures the SmartZone IP address for the Access Point to discover. Multiple controllers IPs can be configured, and NAT addressing can be specified.
- **`set scg ip del`** - Clears the configured SCG list.

Finally, it's useful to know how to factory reset or reboot an Access Point – the commands for this are:

- **`set factory`** - Factory resets the Access Point.
- **`reboot`** - Reboots the AP.



Access Point Registration

Events & Alarms > Events

```
AP [RuckusAP@F8:E7:1E:12:74:90] sent a discovery request to Virtual SmartZone [192.168.1.51].
```

Access Points > System > Staging Zone

- D System
  - D TeamXXPartner
  - Z Staging Zone
    - AG default

MAC Address ▲	AP Name	Status	Alarm	IP Address
F8:E7:1E:12:74:90	RuckusAP	Online	0	192.168.1.23

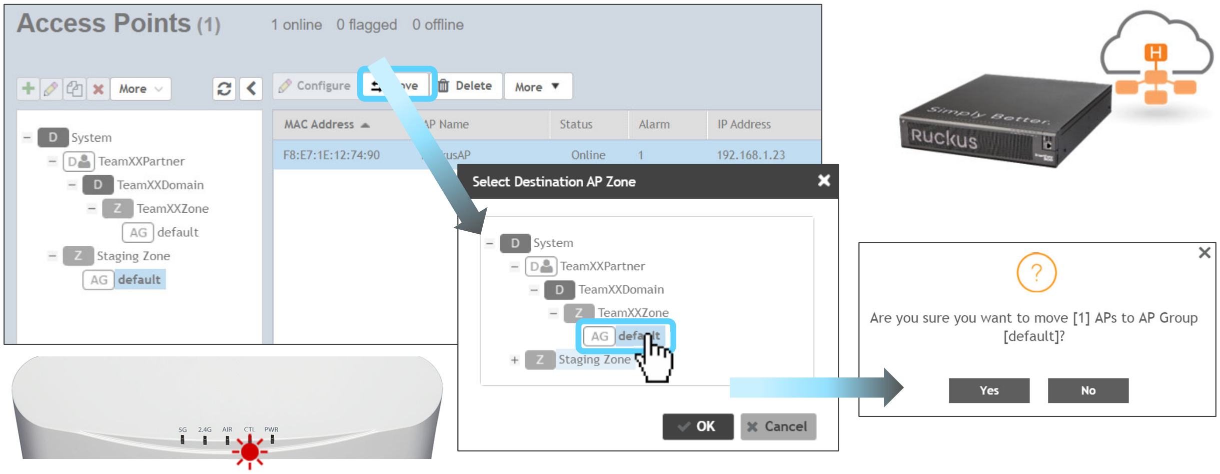
155 | © 2024 CommScope, Inc.

As with Essentials, when the Access Point establishes a communication with a High Scale controller, an entry will appear in the Event Log showing a Discovery request was made, this can take a few moments to appear, however as this is a High Scale controller, the Access Point will register into the Default Access Point Group in the Staging Zone.

The Access Points can be viewed in their Zones, under **Configuration > Access Points**. Selecting the Zone name will show the Access Points in that Zone. Without any special configuration, all Access Points will join the Default Access Point Group in the Staging Zone.

Access Point Registration – Moving APs to Zones

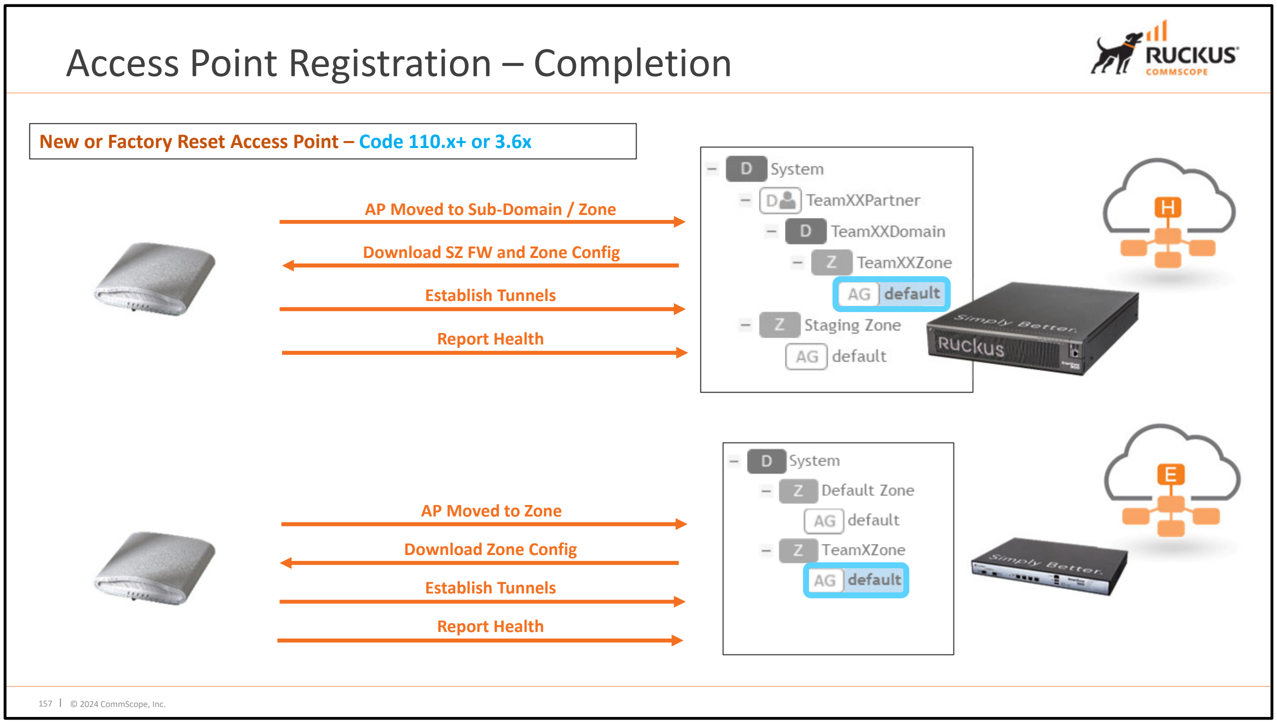
Access Points > System > Staging Zone > Default AG > [Access_Point_MAC]



156 | © 2024 CommScope, Inc.

The Access Points can now be moved to their respective Zone. An Access Points is moved by first highlighting it within its current Zone, and selecting **Move**.
A list will appear showing all of the Domains. Double click on any Domain to show the Subdomains and Zones, and select the target Zone from the list. If you choose the Zone as the destination for the AP move, it will be placed into the default Access Point group for the Zone. If other Access point groups exist under the zone APs can be specifically placed directly into the group.

When the Zone is chosen, the controller displays a warning to confirm the move. Once confirmed, the Access Point is moved into the Zone. Now the Access Point completes registration by downloading the Zone firmware and configuration, through this process you will see the AP CTL light rapidly blink green. Once processing is complete the CTL light on the AP should remain solid green.



Access Point Registration – Completion

New or Factory Reset Access Point – Code 110.x+ or 3.6x

AP Moved to Sub-Domain / Zone

Download SZ FW and Zone Config

Establish Tunnels

Report Health

AP Moved to Zone

Download Zone Config

Establish Tunnels

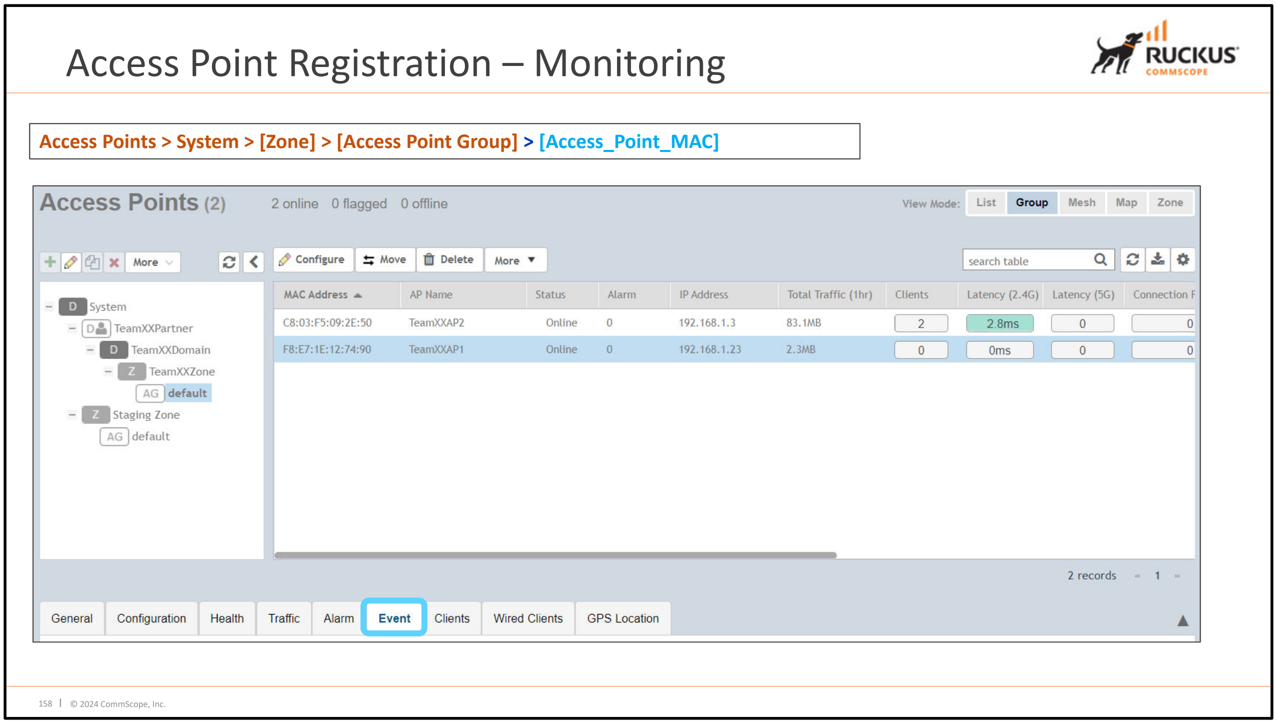
Report Health

157 | © 2024 CommScope, Inc.

On the High Scale controller, the Administrator moves the Access Point to the target Subdomain and Zone. On Essentials, the Administrator moves the Access Point to its target Zone. The procedure the Access Points follow is:

- In High Scale the Access Point now downloads the firmware. In Essentials the firmware is downloaded as soon as the AP is approved. Both Essentials and High Scale applies the configuration for the Zone at this point.
- The Access Point establishes the control tunnel connection, and, if configured, the data tunnel connections.
- The Access Point is now operational and sends status and statistics to the controller.

The registration process can take some time to complete, especially over WAN links that may have some latency, so it is important to allow enough time for the Access Points to complete registration fully.



Access Point Registration – Monitoring

Access Points > System > [Zone] > [Access Point Group] > [Access_Point_MAC]

Access Points (2) 2 online 0 flagged 0 offline

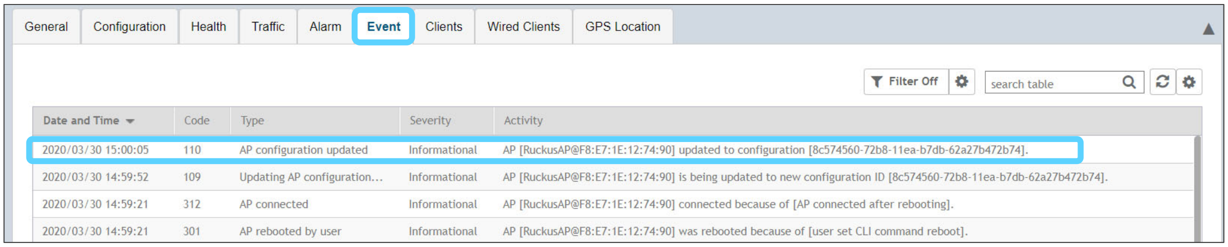
MAC Address	AP Name	Status	Alarm	IP Address	Total Traffic (1hr)	Clients	Latency (2.4G)	Latency (5G)	Connection F
C8:03:F5:09:2E:50	TeamXXAP2	Online	0	192.168.1.3	83.1MB	2	2.8ms	0	0
F8:E7:1E:12:74:90	TeamXXAP1	Online	0	192.168.1.23	2.3MB	0	0ms	0	0

2 records « 1 »

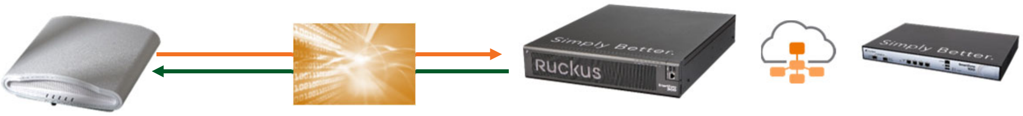
When the Access Points are undergoing and completing registration, you can view their progress by checking the Event Log. In order to do this, highlight the Access Point you wish to view. Then refer to the bottom sub-menu, event tab.

Access Point Registration – Viewing Events

Access Points > System > [Zone] > [Access Point Group] > [Access_Point_MAC] > Event

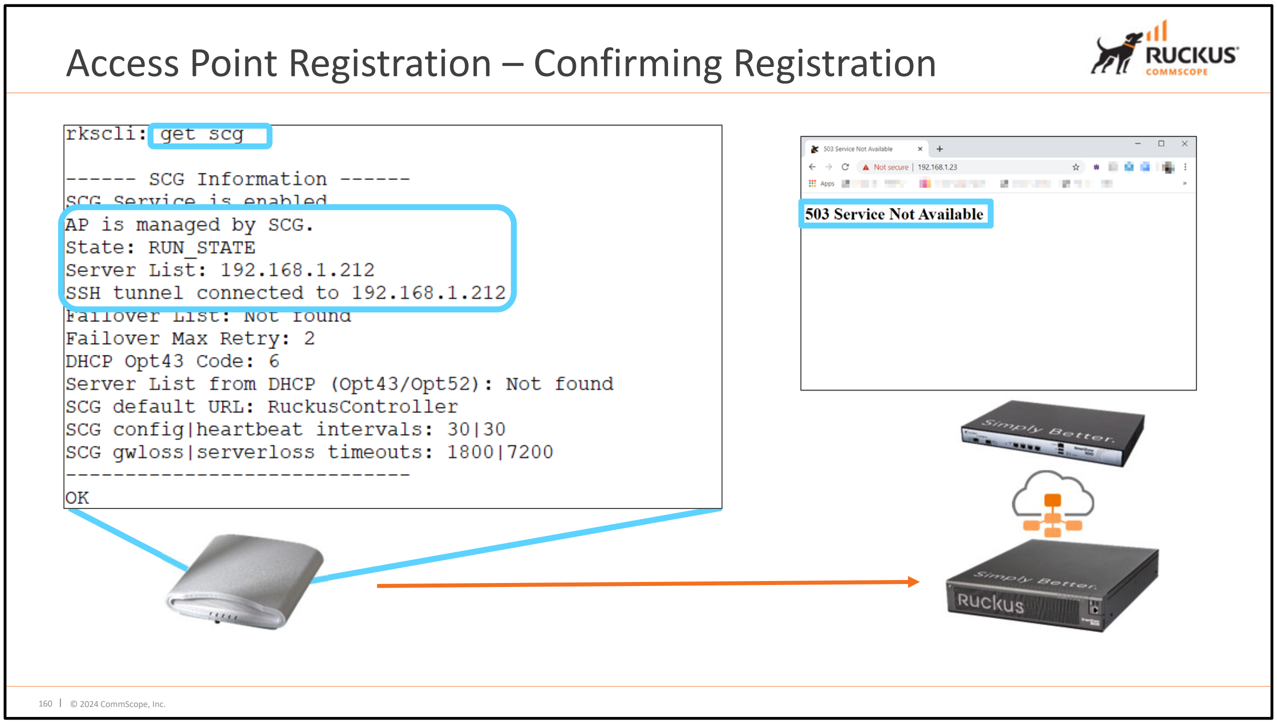


Date and Time	Code	Type	Severity	Activity
2020/03/30 15:00:05	110	AP configuration updated	Informational	AP [RuckusAP@F8:E7:1E:12:74:90] updated to configuration [8c574560-72b8-11ea-b7db-62a27b472b74].
2020/03/30 14:59:52	109	Updating AP configuration…	Informational	AP [RuckusAP@F8:E7:1E:12:74:90] is being updated to new configuration ID [8c574560-72b8-11ea-b7db-62a27b472b74].
2020/03/30 14:59:21	312	AP connected	Informational	AP [RuckusAP@F8:E7:1E:12:74:90] connected because of [AP connected after rebooting].
2020/03/30 14:59:21	301	AP rebooted by user	Informational	AP [RuckusAP@F8:E7:1E:12:74:90] was rebooted because of [user set CLI command reboot].



When a specific AP is selected, the lower menu towards the bottom of the page shows a number of tabs with AP specific information.

Selecting the **Event** tab will show events related to this Access Point. Here you will see the events logged as the Access Point completes registration. The registration process can take some time due to the upload and installation of new firmware, so you should take care to ensure that registration has enough time to complete. When you see “updated to configuration” as the last step, you know that registration has completed successfully.



Access Point Registration – Confirming Registration

```
rkscli: get scg

------ SCG Information ------
SCG Service is enabled
AP is managed by SCG.
State: RUN_STATE
Server List: 192.168.1.212
SSH tunnel connected to 192.168.1.212
Failover List: Not found
Failover Max Retry: 2
DHCP Opt43 Code: 6
Server List from DHCP (Opt43/Opt52): Not found
SCG default URL: RuckusController
SCG config|heartbeat intervals: 30|30
SCG gwloss|serverloss timeouts: 1800|7200
-----------------------------
OK
```

503 Service Not Available

160 | © 2024 CommScope, Inc.

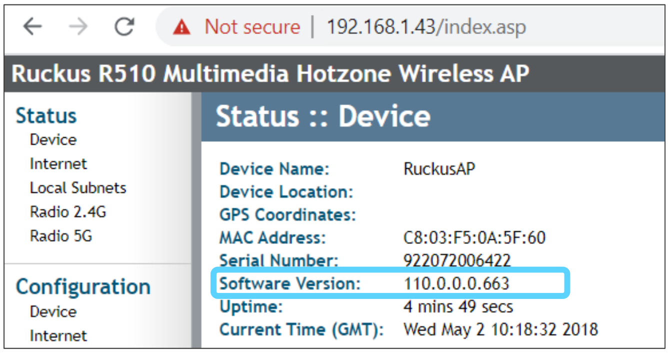
Once the Access Point has completed registration to the controller, the Access Point CLI can be accessed. The login details will no longer be the default *super/sp-admin*, but will be the AP Login credentials you specified when you created the Zone configuration.

Once logged in, the Access Point can be checked with the command `get scg`. After successful registration, the following details should be displayed:

- AP is managed by SCG
- **State**: RUN_STATE
- **Server List**: The IP addresses of the SmartZone Node
- **SSH Tunnel**: The SSH tunnel connected and to which node

Once an Access Point is managed by a controller it will refuse direct connections to the web interface. The web interface is disabled as a security feature.

Access Point Firmware and Banks



Not secure | 192.168.1.43/index.asp

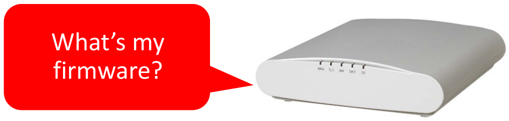
Ruckus R510 Multimedia Hotzone Wireless AP

Status
- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G

Configuration
- Device
- Internet

Status :: Device

Device Name: RuckusAP
Device Location:
GPS Coordinates:
MAC Address: C8:03:F5:0A:5F:60
Serial Number: 922072006422
Software Version: 110.0.0.0.663
Uptime: 4 mins 49 secs
Current Time (GMT): Wed May 2 10:18:32 2018



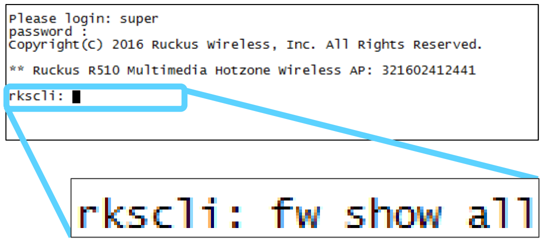
RUCKUS Access Points

- Ship with code 110.x (March 2020)
- Store firmware in two locations:
  - Bank 1
  - Bank 2
- Upgrade firmware when joining:
  - ZoneDirector – to ZD firmware
  - SmartZone – to SmartZone firmware

Before registering Access Points to the controller, the first step is to identify the firmware currently running on the Access Points. At the time this course was created (March 2020) new Access Points shipped from the factory have code 110.x pre-installed. If the AP was ordered with Unleashed firmware from the factory (which is possible depending on which AP SKU was selected) additional commands are required for the registration process.

CLI Command: fw show all

Command	Function
`fw show all`	Displays the firmware installed



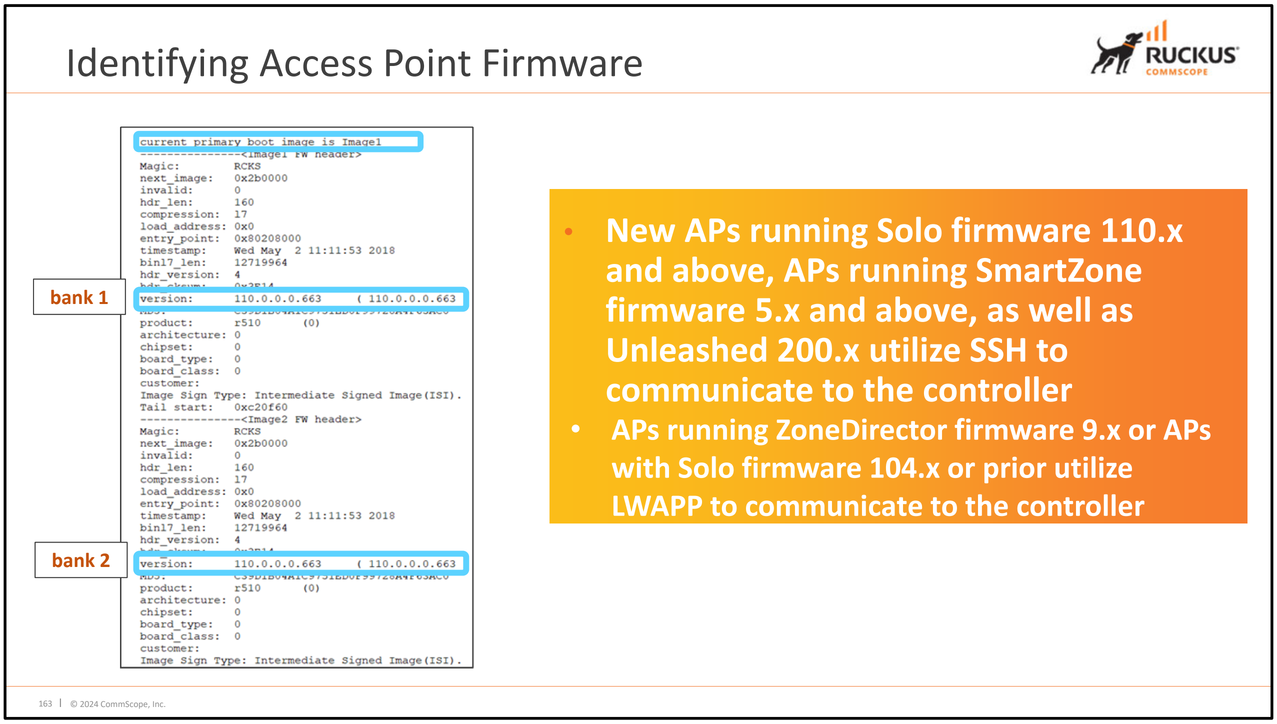
```
Please login: super
password :
Copyright(C) 2016 Ruckus Wireless, Inc. All Rights Reserved.

** Ruckus R510 Multimedia Hotzone Wireless AP: 321602412441
rkscli: 
```

```
rkscli: fw show all
```

- SSH to the AP
  - default user: *super*
  - default password: *sp-admin*
- Enter the command
  - **`fw show all`**

The firmware installed on the Access Point can be viewed from the CLI. The default username is **super**, and the default password is **sp-admin**. If the default credentials do not allow for successful login, it’s likely the Access Point has been previously connected to a controller and should be factory reset.

After logging in at the CLI, the command **`fw show all`** will display the installed firmware.



Identifying Access Point Firmware

bank 1

bank 2

```
current primary boot image is Image1
---------------<Image1 FW header>
Magic:         RCKS
next_image:    0x2b0000
invalid:       0
hdr_len:       160
compression:   17
load_address:  0x0
entry_point:   0x80208000
timestamp:     Wed May  2 11:11:53 2018
bin17_len:     12719964
hdr_version:   4
hdr_cksum:     0x3F14
version:       110.0.0.0.663      ( 110.0.0.0.663
MD5:           C39D1B04A1C9751ED0F99720A4F65AC0
product:       r510      (0)
architecture:  0
chipset:       0
board_type:    0
board_class:   0
customer:
Image Sign Type: Intermediate Signed Image(ISI).
Tail start:    0xc20f60
---------------<Image2 FW header>
Magic:         RCKS
next_image:    0x2b0000
invalid:       0
hdr_len:       160
compression:   17
load_address:  0x0
entry_point:   0x80208000
timestamp:     Wed May  2 11:11:53 2018
bin17_len:     12719964
hdr_version:   4
hdr_cksum:     0x3F14
version:       110.0.0.0.663      ( 110.0.0.0.663
MD5:           C39D1B04A1C9751ED0F99720A4F65AC0
product:       r510      (0)
architecture:  0
chipset:       0
board_type:    0
board_class:   0
customer:
Image Sign Type: Intermediate Signed Image(ISI).
```

- **New APs running Solo firmware 110.x and above, APs running SmartZone firmware 5.x and above, as well as Unleashed 200.x utilize SSH to communicate to the controller**
- **APs running ZoneDirector firmware 9.x or APs with Solo firmware 104.x or prior utilize LWAPP to communicate to the controller**

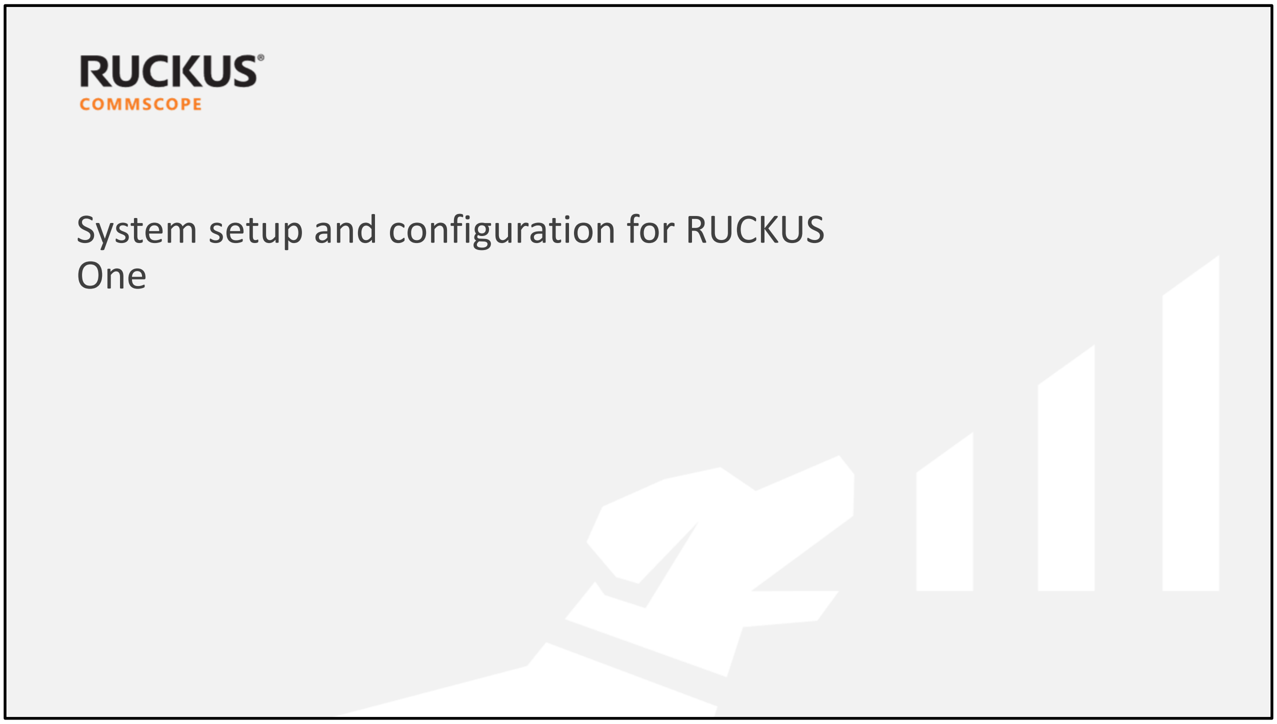
163 | © 2024 CommScope, Inc.

When identifying the Access Point firmware, take note of the following:

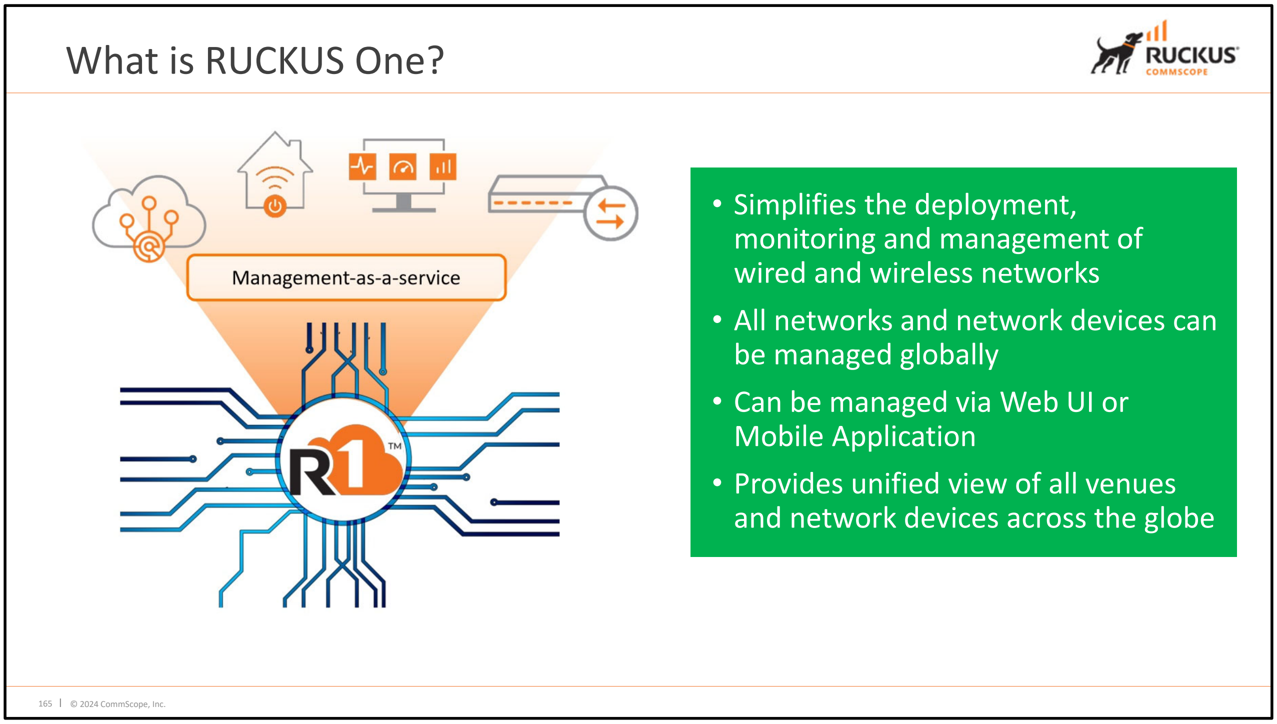
- The Access Point displays which image the Access Point booted from.
- Displays the two firmware images stored on the Access Point, in Bank 1 and Bank 2.

If mixed code is displayed, the Access Point could be either have been the subject of an incomplete or failed registration or has had a manual firmware upgrade to one bank only. Once the Access Point knows where to find the controller, it will attempt to contact the controller using a discovery process. The method used to connect to the controller depends on the APs installed firmware. By default, the SmartZone controller communicates with Access Points using SSH.

AP Firmware considerations for implementations using LAGs including following these steps to avoid losing IP connectivity:
1. Disable secondary port of the LAG in the AP
2. Disable Bonding on the AP using AP CLI
3. Upgrade the AP Zone
4. Enable LAG using controller GUI
5. Enable secondary port on the AP
6. Disable the secondary port from the switch



System setup and configuration for RUCKUS One


Management-as-a-service
R1 TM

What is RUCKUS One?

- Simplifies the deployment, monitoring and management of wired and wireless networks
- All networks and network devices can be managed globally
- Can be managed via Web UI or Mobile Application
- Provides unified view of all venues and network devices across the globe

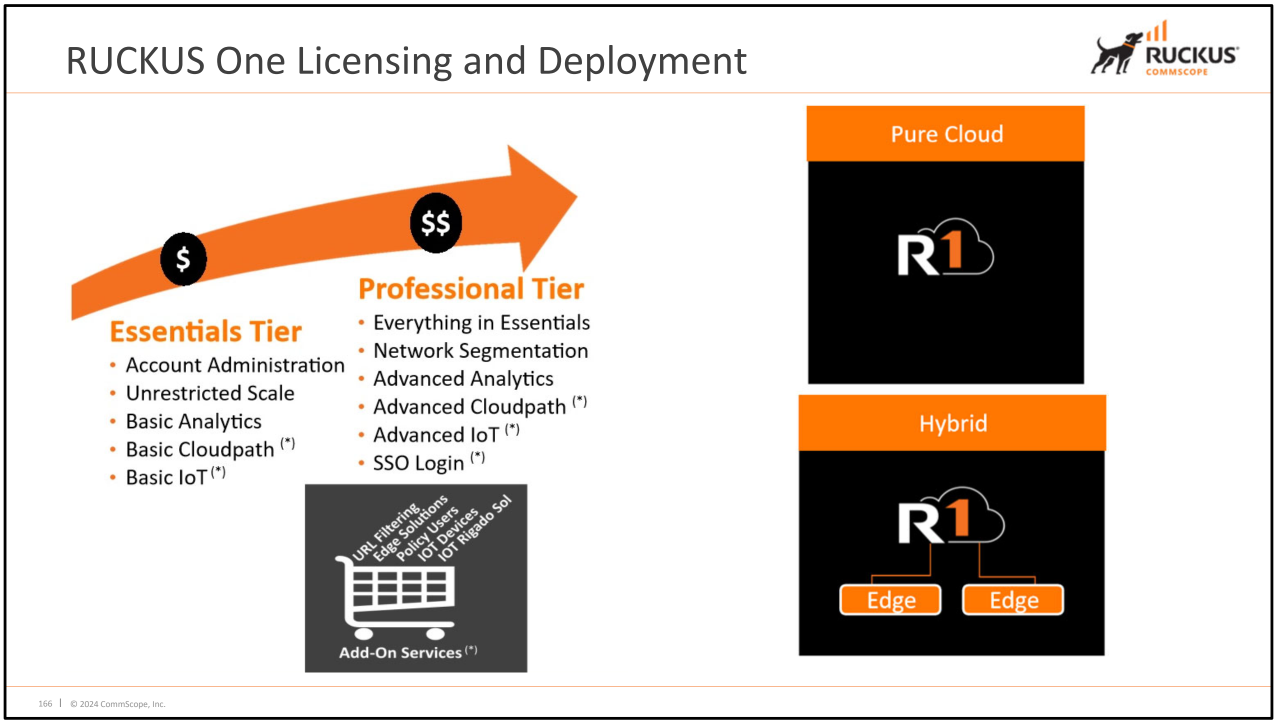
165 | © 2024 CommScope, Inc.

Let’s understand what is RUCKUS One. RUCKUS one is an AI-driven, converged network management-as-a-service platform. It simplifies the deployment, monitoring, and management of your wired and wireless networks.

With RUCKUS one you can manage all your networks across multiple sites, and network devices from any part of the globe using the web interface or mobile app. Administrators get a unified view of all venues, as well as connected APs, switches and the clients. Simplifies the deployment, monitoring and management of wired and wireless networks.

Some of the unique feature of RUCKUS One includes:

- Unified Enterprise Network Management
- High Scalability
- Service Catalog
- AI and ML driven Network Assurance
- Flexibility
- RESTful APIs



RUCKUS One Licensing and Deployment

Essentials Tier

- Account Administration
- Unrestricted Scale
- Basic Analytics
- Basic Cloudpath (*)
- Basic IoT (*)

Professional Tier

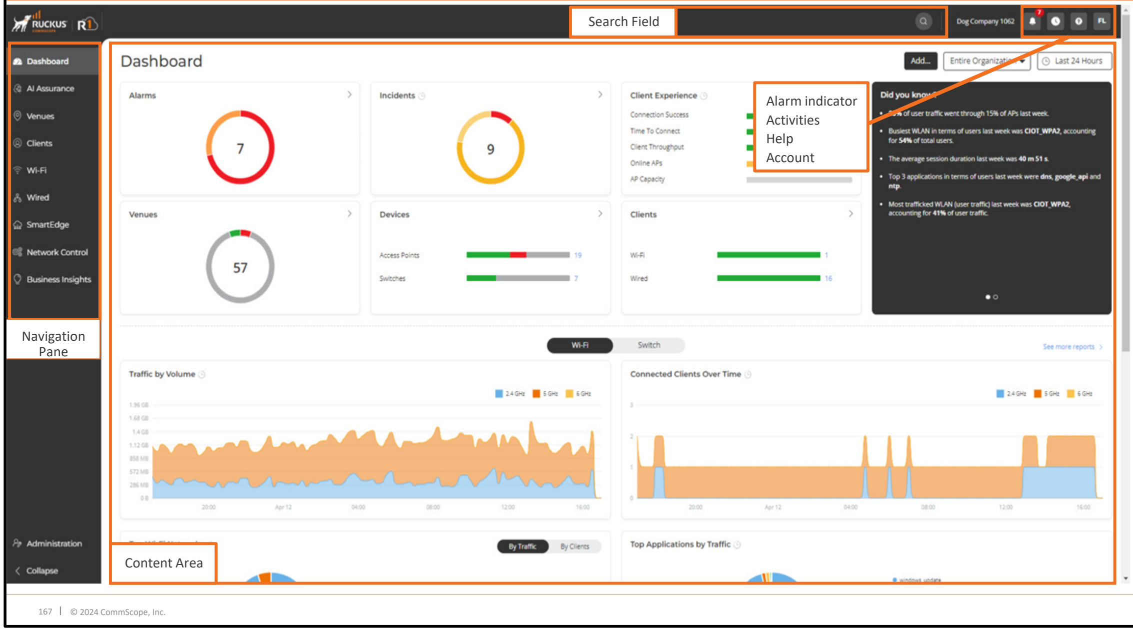
- Everything in Essentials
- Network Segmentation
- Advanced Analytics
- Advanced Cloudpath (*)
- Advanced IoT (*)
- SSO Login (*)

166 | © 2024 CommScope, Inc.

RUCKUS One platform delivers flexible licensing model to meet a variety of business needs. Tiered subscriptions - Essential and Professional - enable enterprises and managed service providers (MSPs) to adopt subscription level that is most aligned with their business needs. Individual add-on services layered on top of subscription tier enable enterprises and MSPs to spend efficiently. Consumption based subscription enables enterprises and managed service providers to utilize subscriptions to meet their peak / short term surge without having to over-subscribe and over-spend for those corner cases. Ability to pause subscriptions when needed ensures that enterprises and managed services providers reap maximum value out of their subscriptions.

RUCKUS One offers flexible deployment models - cloud, hybrid (cloud with edge services), or on-prem.

Dashboard



Did you know?

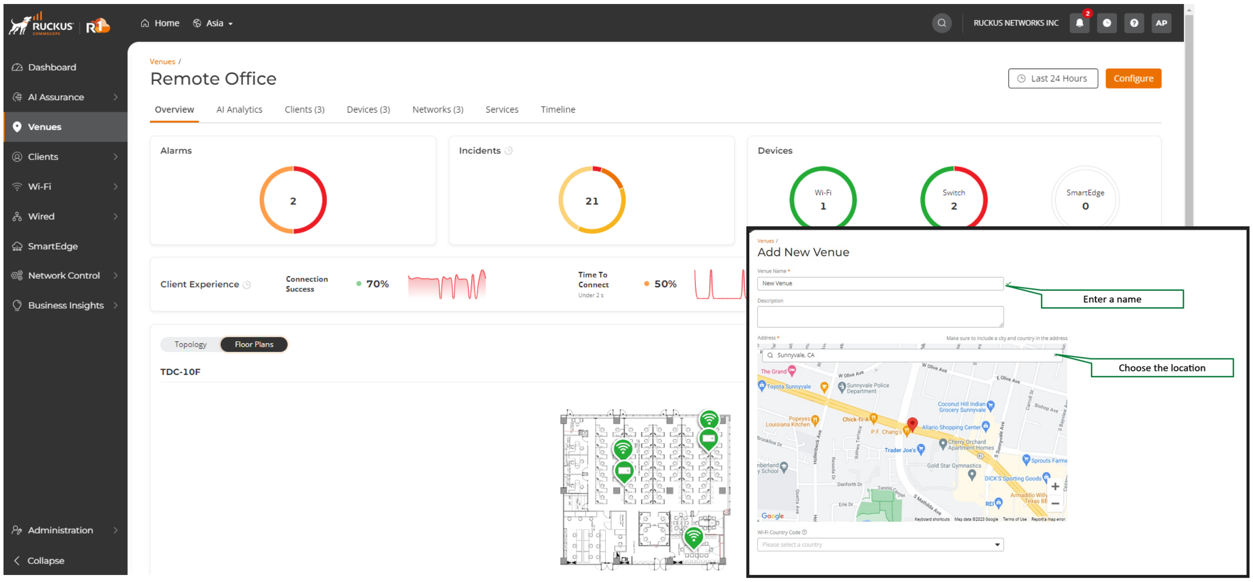
- [illegible] of user traffic went through 15% of APs last week.
- Busiest WLAN in terms of users last week was **CIOT_WPA2**, accounting for **54%** of total users.
- The average session duration last week was **40 m 51 s**.
- Top 3 applications in terms of users last week were **dns, google_api** and **ntp**.
- Most trafficked WLAN (user traffic) last week was **CIOT_WPA2**, accounting for **41%** of user traffic.

167 | © 2024 CommScope, Inc.

The RUCKUS One web interface is a graphical user interface (GUI) for managing and monitoring your network devices, venues, and wireless networks. By default, the Dashboard information is displayed when you log in. Primary Elements of the RUCKUS One GUI includes:

- **Navigation Pane** - Use the navigation bar to go through the main pages of the portal.
- **Content area** - When a user selects an option from the navigation pane, the related information displays in the content area. By default, the information show on the screen is displayed when you login.
- **Search field** - Used to search for matches in venues, APs, switches, venues, and networks.
- **Alarm indicator** - Displays a list of Administrator activities that have occurred, including the time the activity occurred and the status of the activity.
- **Activities** – Displays a list of events including an audit log of the steps taken as part of the Activity, as well as the time required to perform each action and the success or failure of each step within the activity.
- **Help** - Displays a list of links to the RUCKUS One online resources such documentation center, how-to-videos, support and assistance page, training site and about RUCKUS one page.
- **Account** - Consists links for managing your account.

Venues



Add New Venue

Venue Name *: New Venue

Description

Address *: Sunnyvale, CA

Wi-Fi Country Code: Please select a country

Enter a name

Choose the location

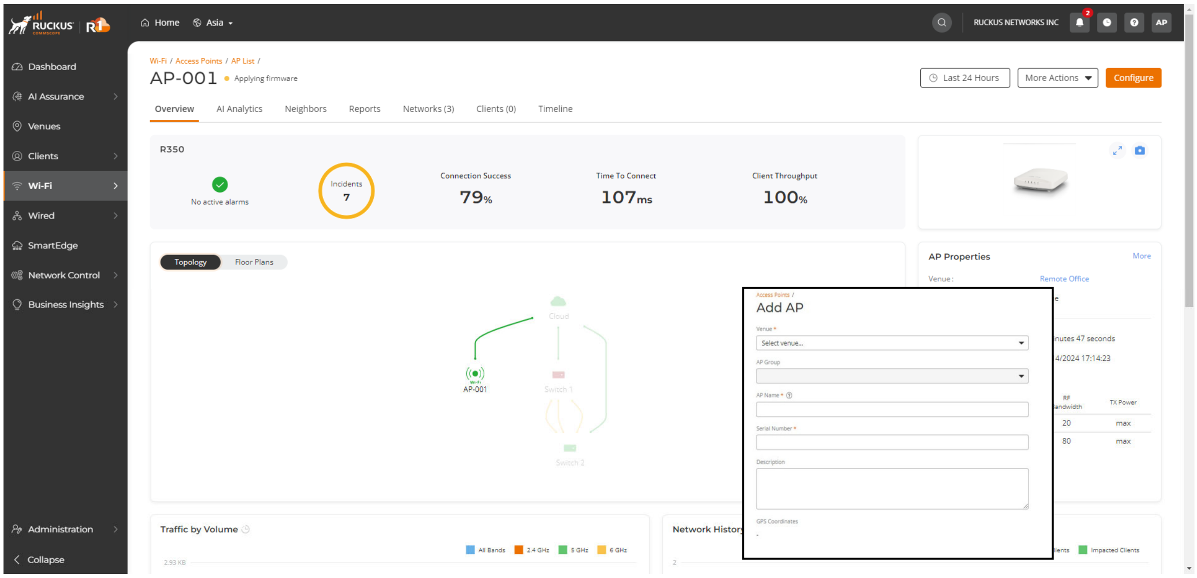
168 | © 2024 CommScope, Inc.

Venues are the primary resource managed by RUCKUS One. A venue represents a physical space where networking devices are deployed. Venues can vary in size from a small room to a large multi-floor building.

While each venue may have multiple networking devices, each networking device can belong to only one venue. Venue configurations override AP group settings and individual AP settings.

To add a new Venue, you need enter a name and choose the location on the maps.

Access Points



Wi-Fi / Access Points / AP List /

AP-001 ● Applying firmware

R350

No active alarms

Incidents 7

Connection Success 79%

Time To Connect 107ms

Client Throughput 100%

AP Properties — More

Venue : Remote Office

RF Bandwidth	TX Power
20	max
80	max

Access Points /

Add AP

Venue *

Select venue...

AP Group

AP Name *

Serial Number *

Description

GPS Coordinates

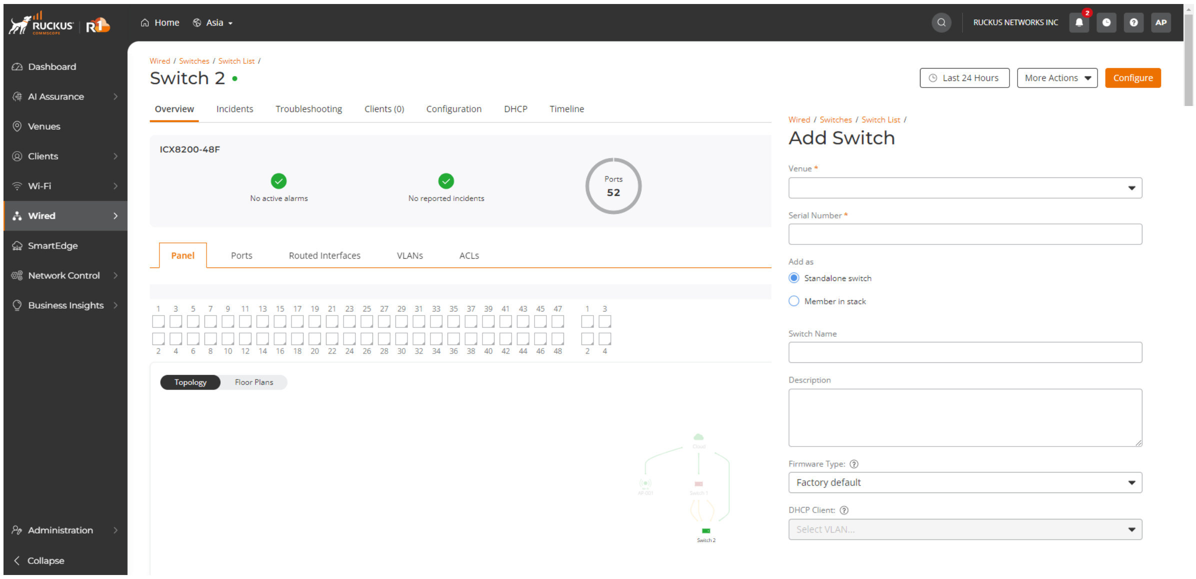
-

169 | © 2024 CommScope, Inc.

You can view a summary of all APs that you have added to your RUCKUS One account and check all of their statuses from a single page. Click an AP name to view details about the AP. The Access Points page appears with a number in brackets indicating how many APs are in your account.

To add an access point you need enter a name, the serial number of the AP and select a venue. An AP can be part of a single venue, it cannot be added to multiple venues.

Switches



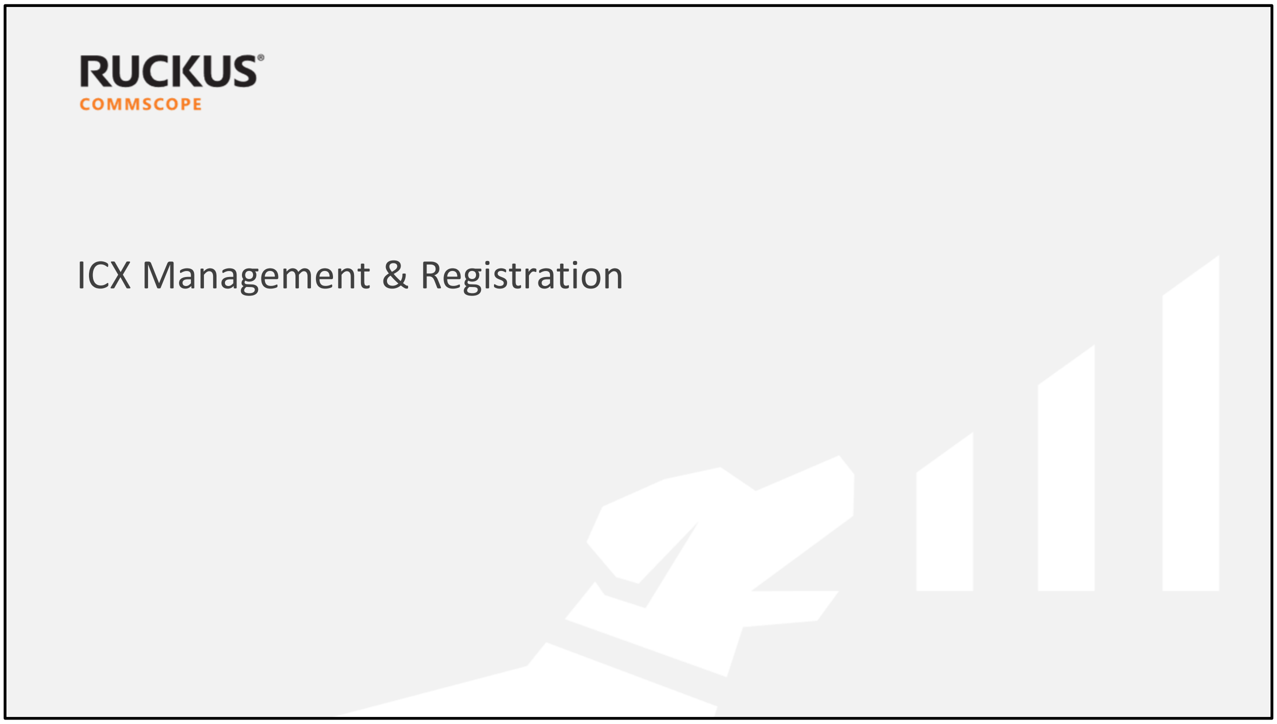
Add as: ● Standalone switch ○ Member in stack

Firmware Type: Factory default

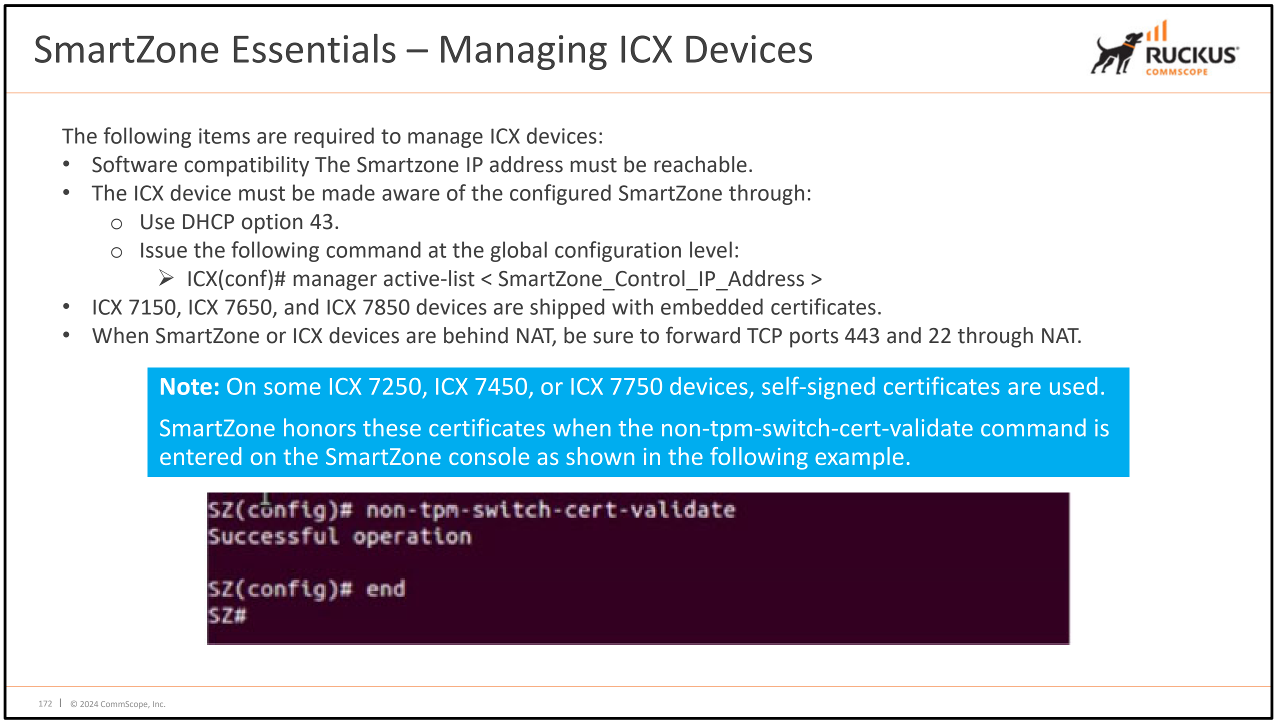
You can onboard a FastIron ICX switch from the RUCKUS one web interface and also using the RUCKU One Mobile App. When an ICX switch added with a version that is earlier than ICX version 08.0.92b, RUCKUS One upgrades the switch to the most current version of the ICX version. The minimum ICX Switch firmware supported is ICX 8.0.90d.

To add a new switch, you need enter a name, the serial number of the switch and select a venue. A Switch can be part of a single venue, it cannot be added to multiple venues.

Note: If a switch is running an older version than 8.0.90d, it will not connect to the Cloud. From the switch CLI, use the show version command to view the software version the switch is running.



ICX Management & Registration



SmartZone Essentials – Managing ICX Devices

The following items are required to manage ICX devices:

- Software compatibility The Smartzone IP address must be reachable.
- The ICX device must be made aware of the configured SmartZone through:
  - Use DHCP option 43.
  - Issue the following command at the global configuration level:
    - ICX(conf)# manager active-list < SmartZone_Control_IP_Address >
- ICX 7150, ICX 7650, and ICX 7850 devices are shipped with embedded certificates.
- When SmartZone or ICX devices are behind NAT, be sure to forward TCP ports 443 and 22 through NAT.

Note: On some ICX 7250, ICX 7450, or ICX 7750 devices, self-signed certificates are used.

SmartZone honors these certificates when the non-tpm-switch-cert-validate command is entered on the SmartZone console as shown in the following example.

```
SZ(config)# non-tpm-switch-cert-validate
Successful operation

SZ(config)# end
SZ#
```

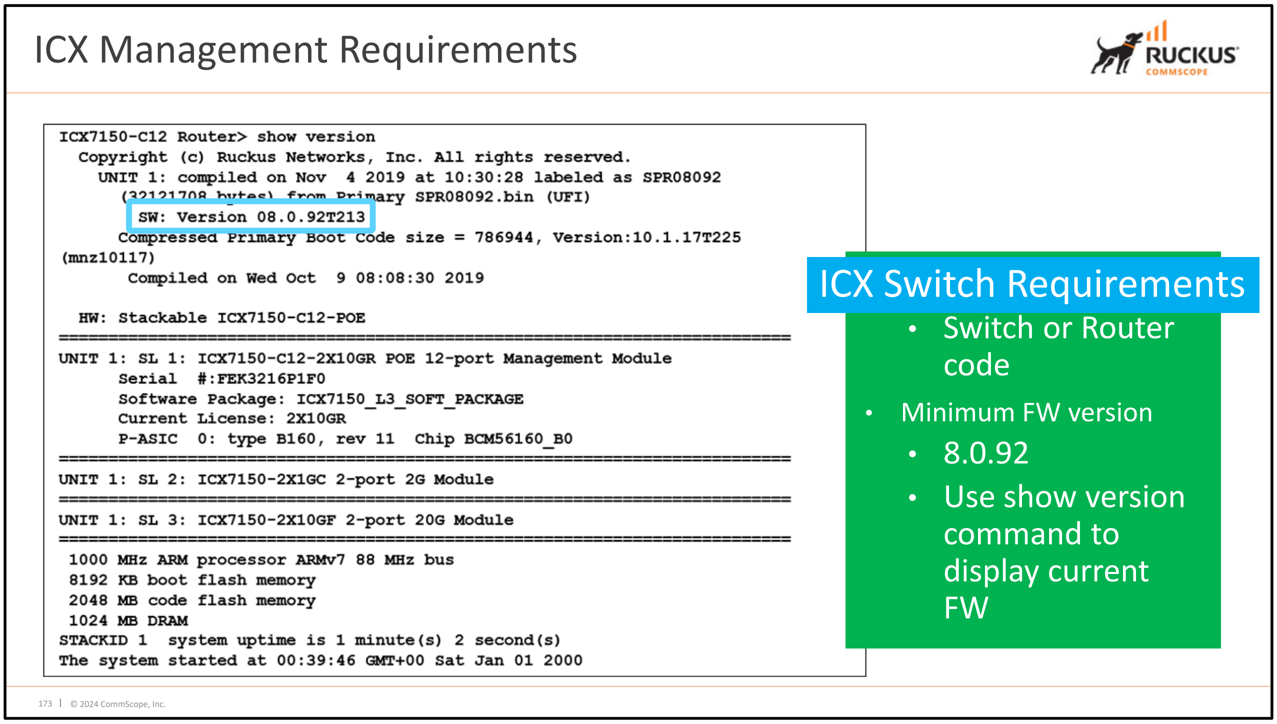
172 | © 2024 CommScope, Inc.

ICX devices running either router or switch images can be managed by SmartZone.
The following items are required to manage ICX devices:

- Software compatibility requirements (refer to the ICX-Management Feature Support Matrix)
- The Smartzone IP address must be reachable by the ICX device through the Management interface or through switch or router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of two ways:
  - Configure the DHCP server to use DHCP option 43.
  - Issue the following command at the global configuration level:

    ICX(conf)# manager active-list < SmartZone_Control_IP_Address >
- ICX 7150, ICX 7650, and ICX 7850 devices are shipped with embedded certificates that are used for authentication withSmartZone.
- When SmartZone or ICX devices are behind NAT, be sure to forward TCP ports 443 and 22 through NAT.

Note: On some ICX 7250, ICX 7450, or ICX 7750 devices, self-signed certificates are used. SmartZone honors these certificates when the `non-tpm-switch-cert-validate` command is entered on the SmartZone console as shown in the following example.



ICX Management Requirements

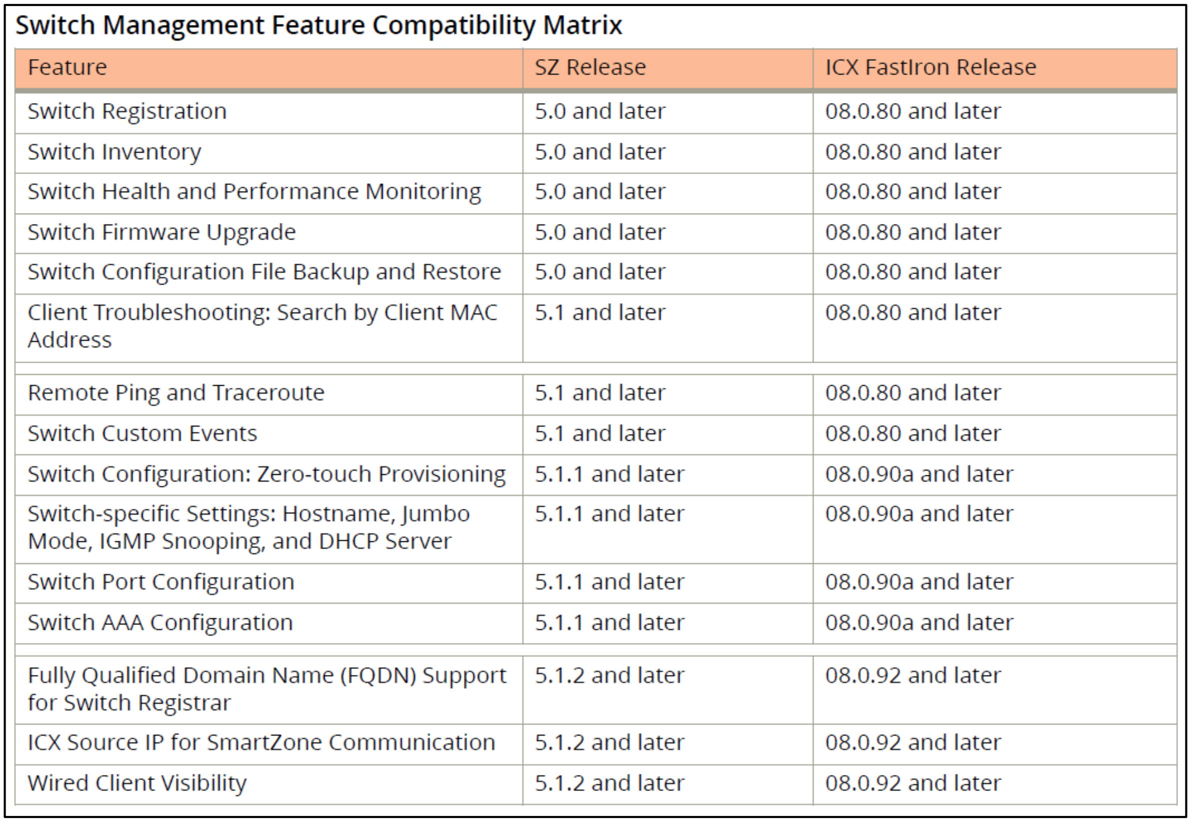
```
ICX7150-C12 Router> show version
  Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 1: compiled on Nov  4 2019 at 10:30:28 labeled as SPR08092
      (32121708 bytes) from Primary SPR08092.bin (UFI)
        SW: Version 08.0.92T213
      Compressed Primary Boot Code size = 786944, Version:10.1.17T225
(mnz10117)
       Compiled on Wed Oct  9 08:08:30 2019

  HW: Stackable ICX7150-C12-POE
==========================================================================
UNIT 1: SL 1: ICX7150-C12-2X10GR POE 12-port Management Module
      Serial  #:FEK3216P1F0
      Software Package: ICX7150_L3_SOFT_PACKAGE
      Current License: 2X10GR
      P-ASIC  0: type B160, rev 11  Chip BCM56160_B0
==========================================================================
UNIT 1: SL 2: ICX7150-2X1GC 2-port 2G Module
==========================================================================
UNIT 1: SL 3: ICX7150-2X10GF 2-port 20G Module
==========================================================================
 1000 MHz ARM processor ARMv7 88 MHz bus
 8192 KB boot flash memory
 2048 MB code flash memory
 1024 MB DRAM
STACKID 1  system uptime is 1 minute(s) 2 second(s)
The system started at 00:39:46 GMT+00 Sat Jan 01 2000
```

ICX Switch Requirements

- Switch or Router code
- Minimum FW version
  - 8.0.92
  - Use show version command to display current FW

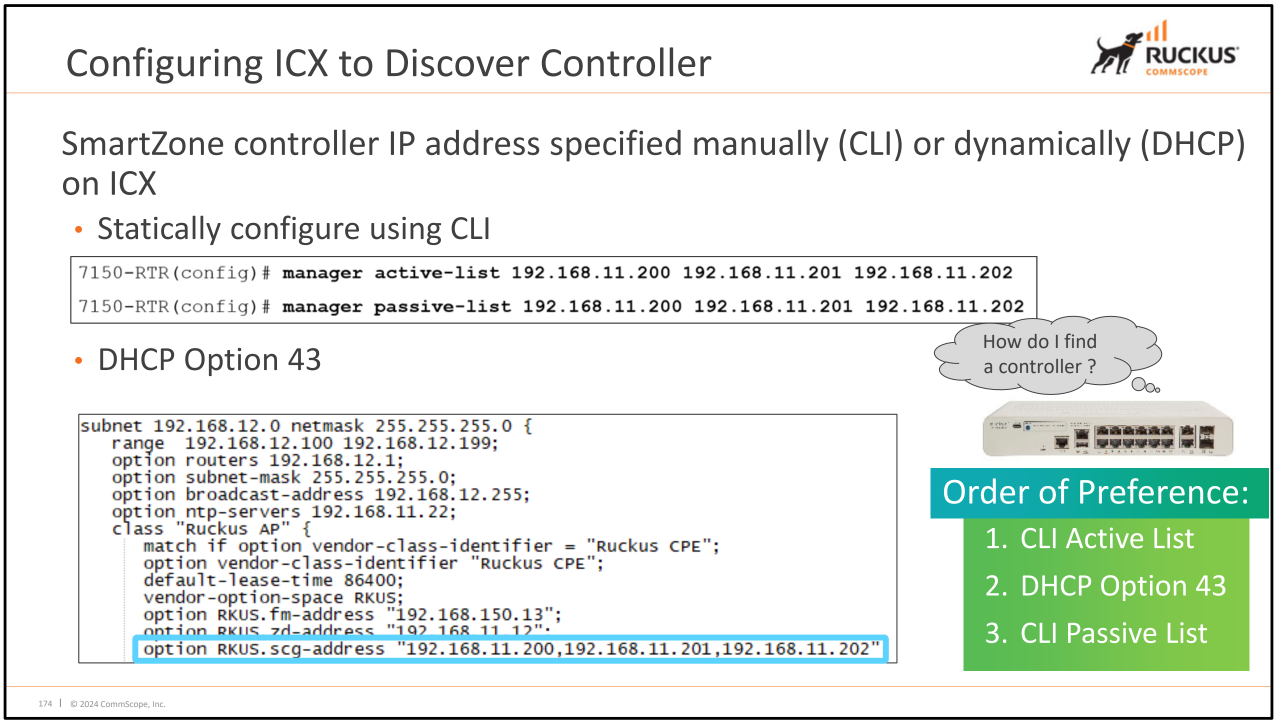
173 | © 2024 CommScope, Inc.

The features covered have specific requirements on the SmartZone controller and the managed ICX device. For all the featured described, the ICX switch must be in the 7000 series, can be running switch or router code, and is required to run a minimum of v8.0.92 FW. While some of the read-only features are available with previous versions of firmware, this course is entirely based on a minimum of v8.0.92. The firmware version on a switch can be verified by using the **`show version`** command.



Switch Management Feature Compatibility Matrix

Feature	SZ Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Switch Configuration: Zero-touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Fully Qualified Domain Name (FQDN) Support for Switch Registrar	5.1.2 and later	08.0.92 and later
ICX Source IP for SmartZone Communication	5.1.2 and later	08.0.92 and later
Wired Client Visibility	5.1.2 and later	08.0.92 and later



Configuring ICX to Discover Controller

SmartZone controller IP address specified manually (CLI) or dynamically (DHCP) on ICX

- Statically configure using CLI

```
7150-RTR(config)# manager active-list 192.168.11.200 192.168.11.201 192.168.11.202
7150-RTR(config)# manager passive-list 192.168.11.200 192.168.11.201 192.168.11.202
```

- DHCP Option 43

```
subnet 192.168.12.0 netmask 255.255.255.0 {
   range  192.168.12.100 192.168.12.199;
   option routers 192.168.12.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.12.255;
   option ntp-servers 192.168.11.22;
   class "Ruckus AP" {
      match if option vendor-class-identifier = "Ruckus CPE";
      option vendor-class-identifier "Ruckus CPE";
      default-lease-time 86400;
      vendor-option-space RKUS;
      option RKUS.fm-address "192.168.150.13";
      option RKUS.zd-address "192.168.11.12";
      option RKUS.scg-address "192.168.11.200,192.168.11.201,192.168.11.202"
```

Order of Preference:

1. CLI Active List
2. DHCP Option 43
3. CLI Passive List

In order for an ICX switch to register to a SmartZone controller it must know the IP address of one or more controllers. There are two ways this can occur for on-premises controllers, manually configured using the ICX command line interface (CLI) or using DHCP Option 43.

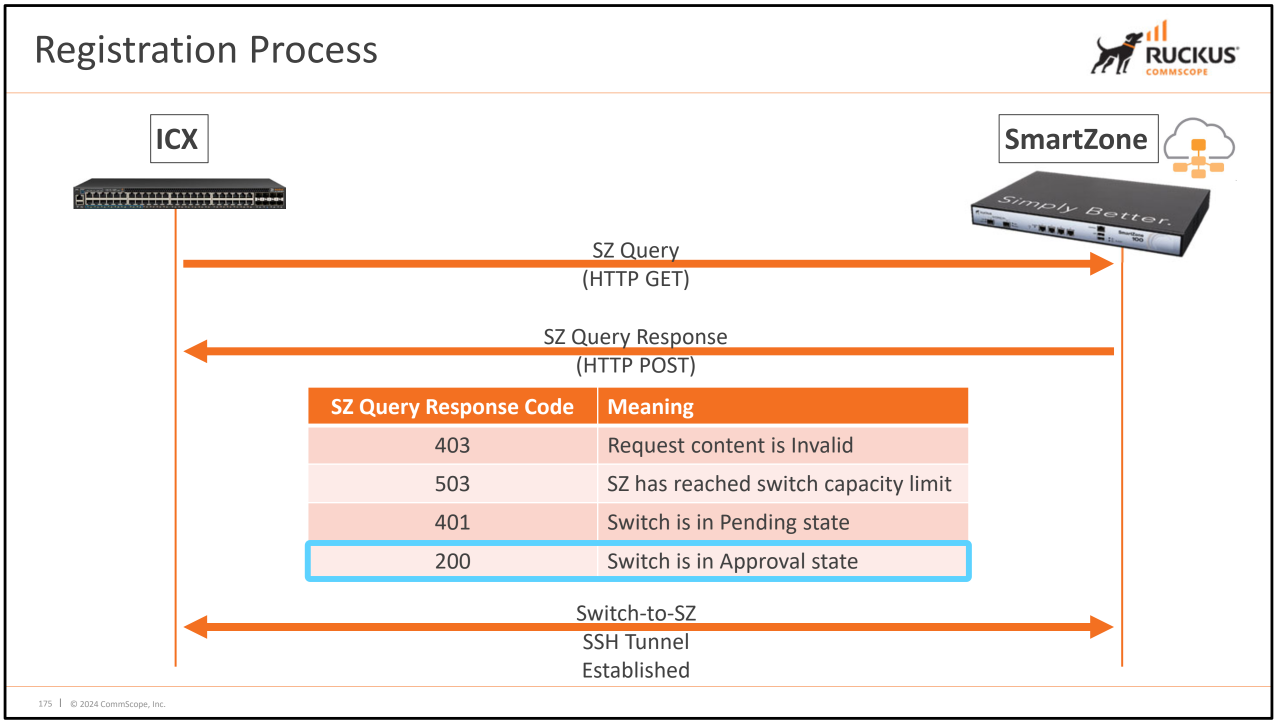
There are two CLI options, along with DHCP, for defining the controller IP address. Each of these are processed in a specific order, which is:

1. CLI Active list
2. DHCP Option 43
3. CLI Passive list

When configuring through the ICX CLI, active controllers can be specified using the **`manager active-list`** command, followed by one or more controller IP addresses, by priority.

Alternatively, the controller's IP address can be provided through DHCP Option 43. The addresses can be defined in the "Ruckus AP" class using the "RKUS.scg-address" option, as shown here.

A passive list of controllers is also configured via the CLI. This is accomplished with the **`manager passive-list`** command, followed by one or more controller IP addresses, by priority. These controllers will only be used if there are no active controllers and no DHCP-learned controllers. Typically, a passive list is used when you prefer DHCP but also desire a fallback.



Registration Process

SZ Query Response Code	Meaning
403	Request content is Invalid
503	SZ has reached switch capacity limit
401	Switch is in Pending state
200	Switch is in Approval state

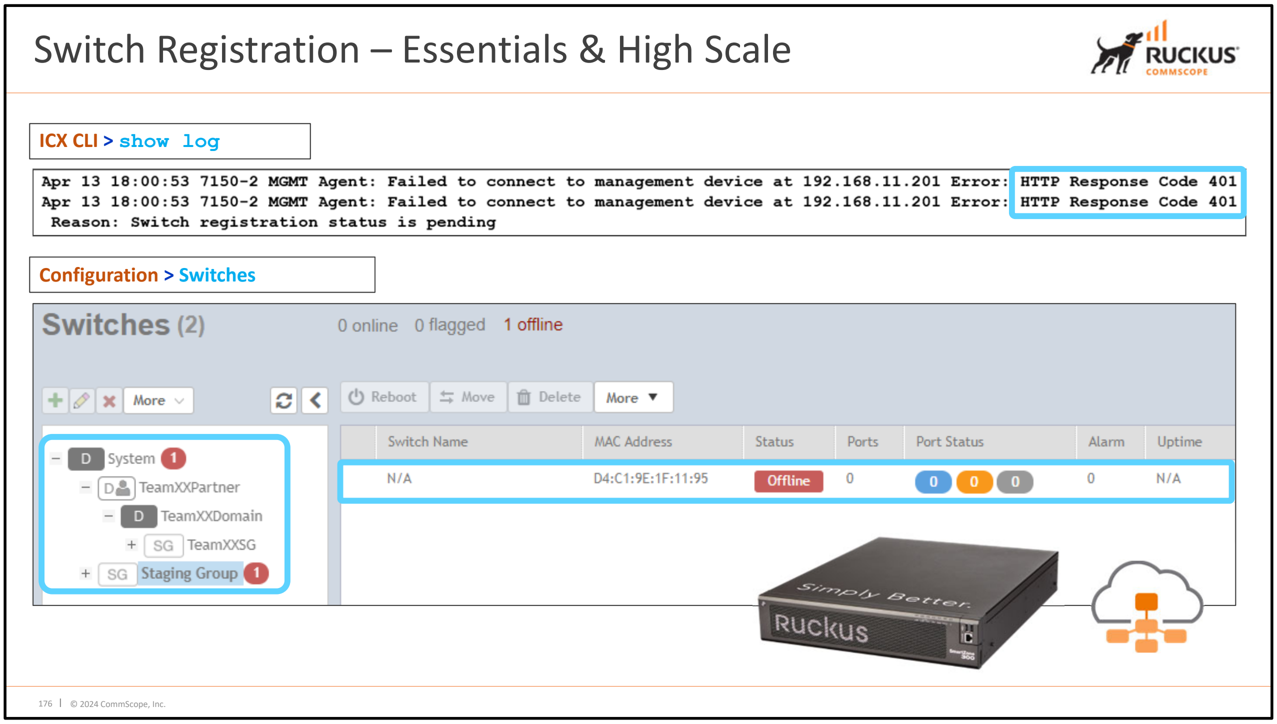
175 | © 2024 CommScope, Inc.

Once an ICX switch has the IP address of the controller, it begins sending SZ queries in the form of an HTTP GET message. The information contained in the HTTP GET message will determine action by the controller. The result, in the form of a response code, will be sent back to the ICX switch in an HTTP POST message.

Here are the possible response codes and their meanings:

- A response code of 403 indicates the content in the SZ Query is invalid and cannot be processed.
- A response code of 503 simply indicates the SmartZone controller has reached its capacity of licenses for managed switches and cannot accept the new query.
- A response code of 401 indicates the SmartZone has accepted the query and has placed the switch in a PENDING state. This is the state a switch will be in when it is placed in the default switch group. Until it is moved to a non-default switch group, it will remain in a PENDING state.
- A response code of 200 indicates that the switch is in the APPROVAL state. This is the final successful state achieved when a switch is either manually or due to a Registration Rule moved to a non-default switch group. Upon reaching an APPROVAL state, SSH keys are exchanged and tunnels are established between the ICX switch and the SmartZone controller allowing full management functionality.

The functionality described here is the same for the Essentials and High Scale editions of the SmartZone controller.



Switch Registration – Essentials & High Scale

ICX CLI > show log

```
Apr 13 18:00:53 7150-2 MGMT Agent: Failed to connect to management device at 192.168.11.201 Error: HTTP Response Code 401
Apr 13 18:00:53 7150-2 MGMT Agent: Failed to connect to management device at 192.168.11.201 Error: HTTP Response Code 401
 Reason: Switch registration status is pending
```

Configuration > Switches

Switches (2) 0 online 0 flagged 1 offline

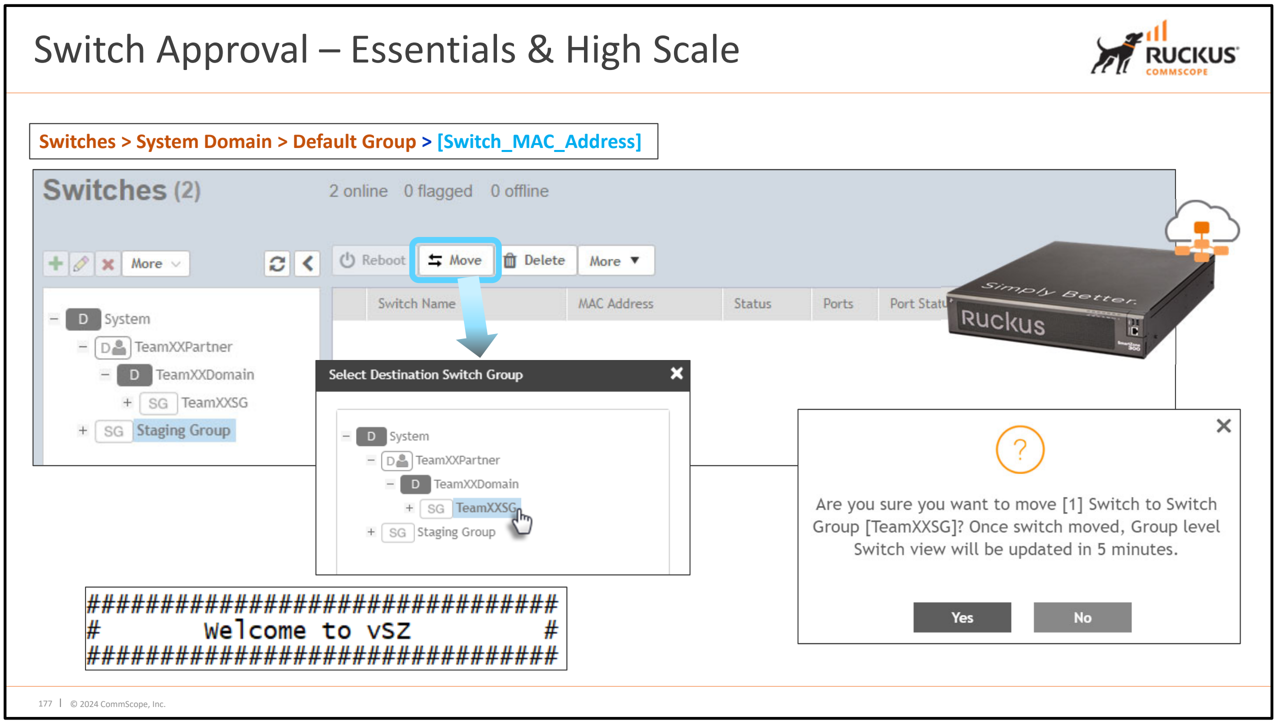
Switch Name	MAC Address	Status	Ports	Port Status	Alarm	Uptime
N/A	D4:C1:9E:1F:11:95	Offline	0	0 0 0	0	N/A

176 | © 2024 CommScope, Inc.

When an ICX switch establishes communication with the controller, an entry will appear in the switches syslog showing an SZ Query “failed” with a response code of 401.

This is labelled a failure by the HTTP protocol due to the code number, but in this case it is actually a step towards success because it indicates the switch has been placed into the Default Switch Group or Staging Group in the System Domain, depending on controller version.

This can be verified in the SmartZone web interface under **Configuration > Switches**. Without any special configuration, all Switches will join the Default Switch Group or Staging Group (Essentials or High Scale, respectively) in the System Domain unless the switch license capacity has been reached.



Switch Approval – Essentials & High Scale

Switches > System Domain > Default Group > [Switch_MAC_Address]

Are you sure you want to move [1] Switch to Switch Group [TeamXXSG]? Once switch moved, Group level Switch view will be updated in 5 minutes.

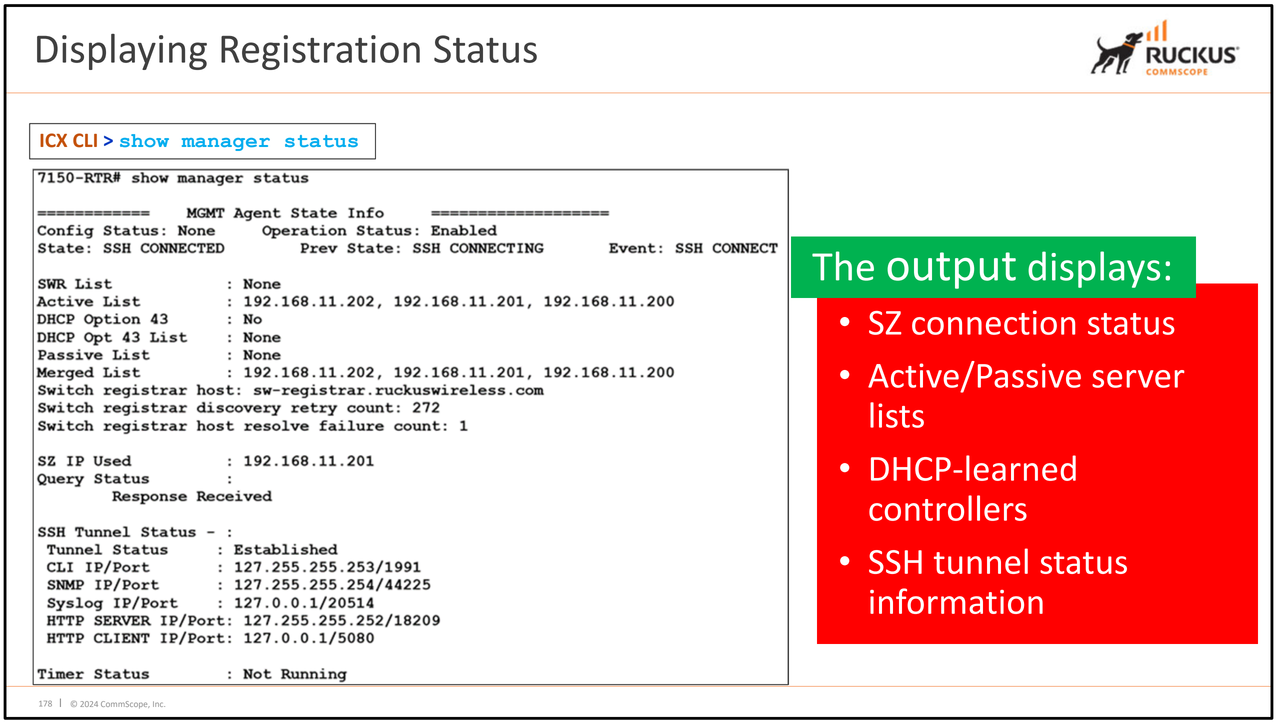
```
################################
#          Welcome to vSZ      #
################################
```

177 | © 2024 CommScope, Inc.

To leverage full management functionality of an ICX switch, you must move it from the Default Switch Group to an non-default group. This is accomplished by selecting the switch in the Default Group and clicking the **Move** button.

This will open a dialog where you can select the destination Switch Group. Clicking OK will open another dialog confirming you wish to move the switch.

Upon successful movement to the destination Switch Group the switch be removed from the Staging Group and the alarm states will clear. Lastly, the ICX switch console will display a “Welcome to vSZ” message indicating it has successfully moved and established the SSH tunnel to the controller.



Displaying Registration Status

ICX CLI > `show manager status`

```
7150-RTR# show manager status

============     MGMT Agent State Info      ===================
Config Status: None     Operation Status: Enabled
State: SSH CONNECTED         Prev State: SSH CONNECTING       Event: SSH CONNECT

SWR List            : None
Active List         : 192.168.11.202, 192.168.11.201, 192.168.11.200
DHCP Option 43      : No
DHCP Opt 43 List    : None
Passive List        : None
Merged List         : 192.168.11.202, 192.168.11.201, 192.168.11.200
Switch registrar host: sw-registrar.ruckuswireless.com
Switch registrar discovery retry count: 272
Switch registrar host resolve failure count: 1

SZ IP Used          : 192.168.11.201
Query Status        :
        Response Received

SSH Tunnel Status - :
 Tunnel Status     : Established
 CLI IP/Port       : 127.255.255.253/1991
 SNMP IP/Port      : 127.255.255.254/44225
 Syslog IP/Port    : 127.0.0.1/20514
 HTTP SERVER IP/Port: 127.255.255.252/18209
 HTTP CLIENT IP/Port: 127.0.0.1/5080

Timer Status        : Not Running
```

The output displays:

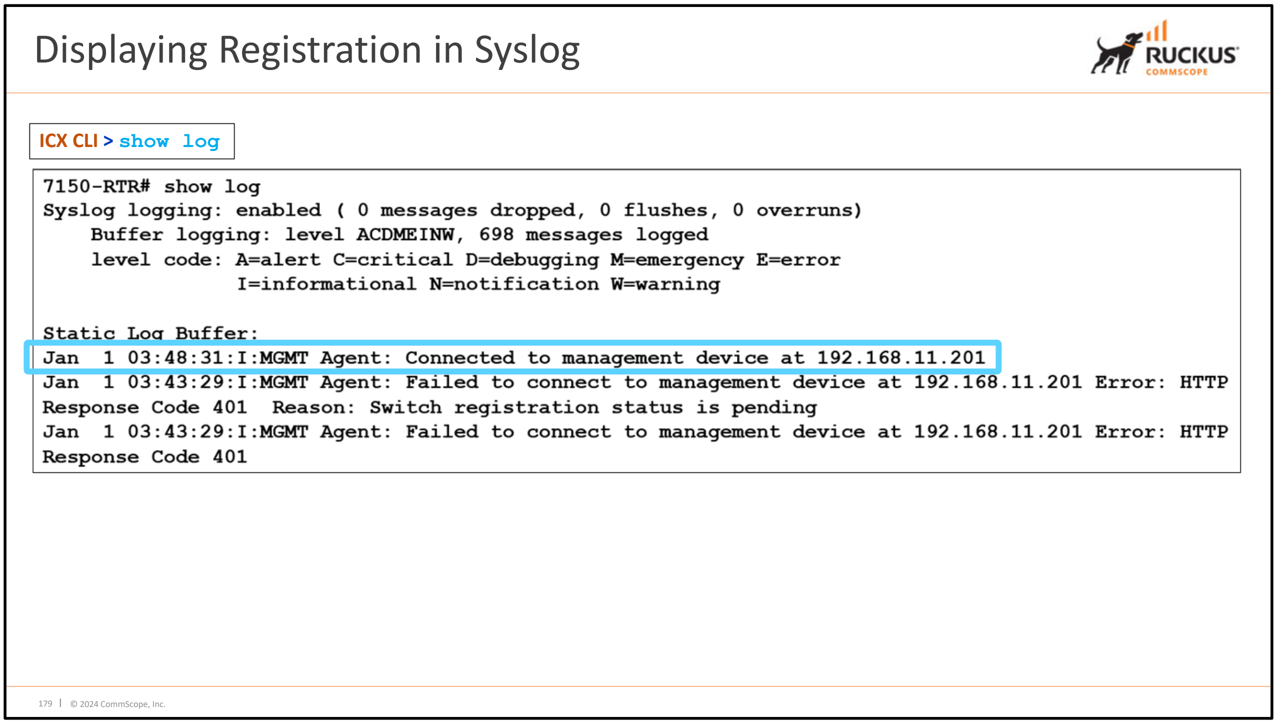
- SZ connection status
- Active/Passive server lists
- DHCP-learned controllers
- SSH tunnel status information

178 | © 2024 CommScope, Inc.

From the ICX CLI, the **`show manager status`** command can provide potentially useful information about the state of the switch-to-controller connection.
It also displays information about the available controllers and the sources they were learned from.

Finally, it also shows the status of the SSH tunnel and unique IP addresses and ports used for each management protocol.

In the example output, you may notice that the SZ IP used is the second controller in the merged list. Since the list is processed sequentially, this would likely be a scenario where the first controller in the list is unreachable.



Displaying Registration in Syslog

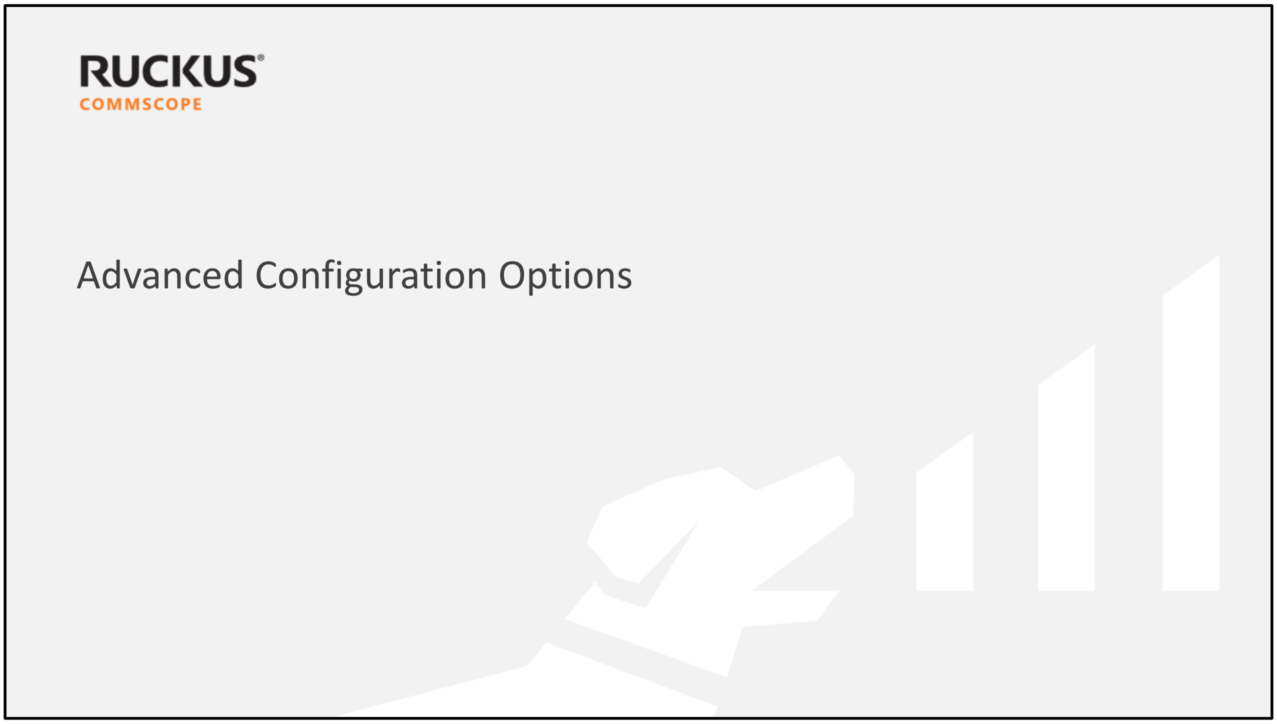
ICX CLI > `show log`

```
7150-RTR# show log
Syslog logging: enabled ( 0 messages dropped, 0 flushes, 0 overruns)
    Buffer logging: level ACDMEINW, 698 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning

Static Log Buffer:
Jan  1 03:48:31:I:MGMT Agent: Connected to management device at 192.168.11.201
Jan  1 03:43:29:I:MGMT Agent: Failed to connect to management device at 192.168.11.201 Error: HTTP
Response Code 401  Reason: Switch registration status is pending
Jan  1 03:43:29:I:MGMT Agent: Failed to connect to management device at 192.168.11.201 Error: HTTP
Response Code 401
```

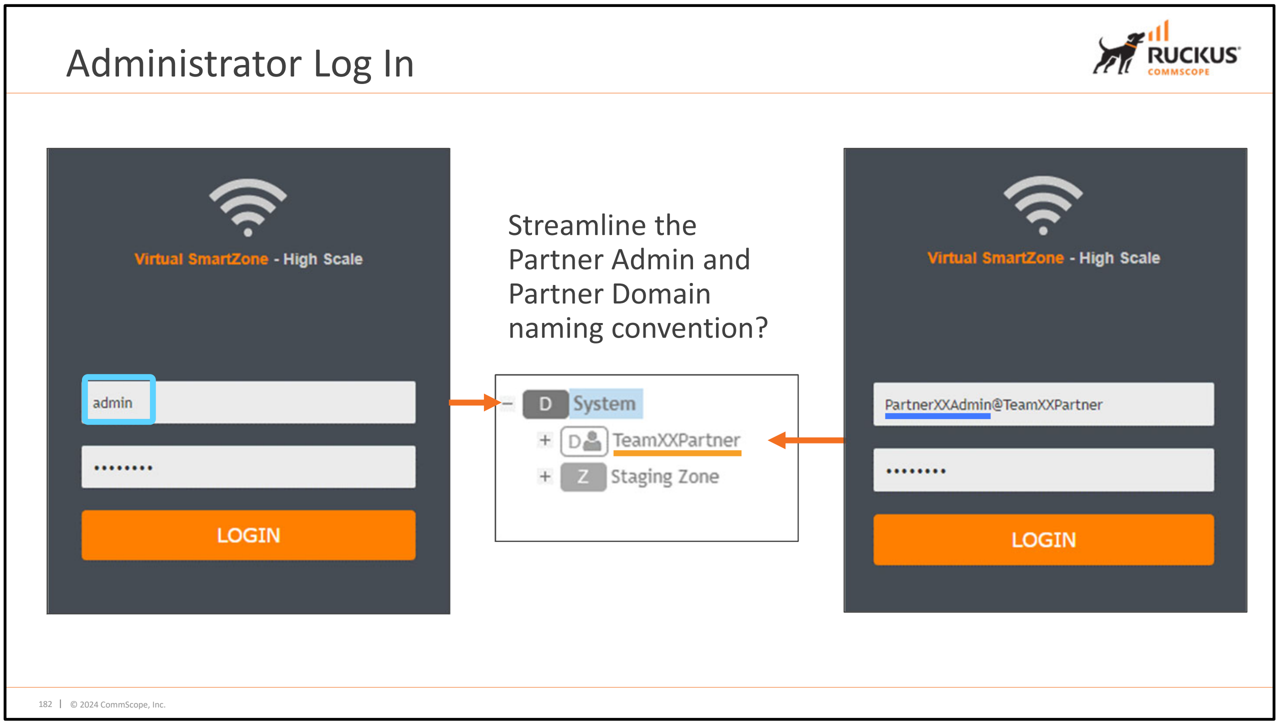
Also from the ICX CLI is the **`show log`** command. The output of this command displays information for query messages sent by the ICX. Here we see two failed connections while the switch was still in the Default/Staging Group leading up to the successful connection to SmartZone controller. These can be helpful in potential registration troubleshooting scenarios.

RUCKUS
COMMSCOPE
TM

RUCKUS SmartZone WLAN Configuration



Advanced Configuration Options



Administrator Log In

Virtual SmartZone - High Scale
admin
••••••••
LOGIN
D System
D TeamXXPartner
Z Staging Zone
Virtual SmartZone - High Scale
PartnerXXAdmin@TeamXXPartner
••••••••
LOGIN

Streamline the Partner Admin and Partner Domain naming convention?

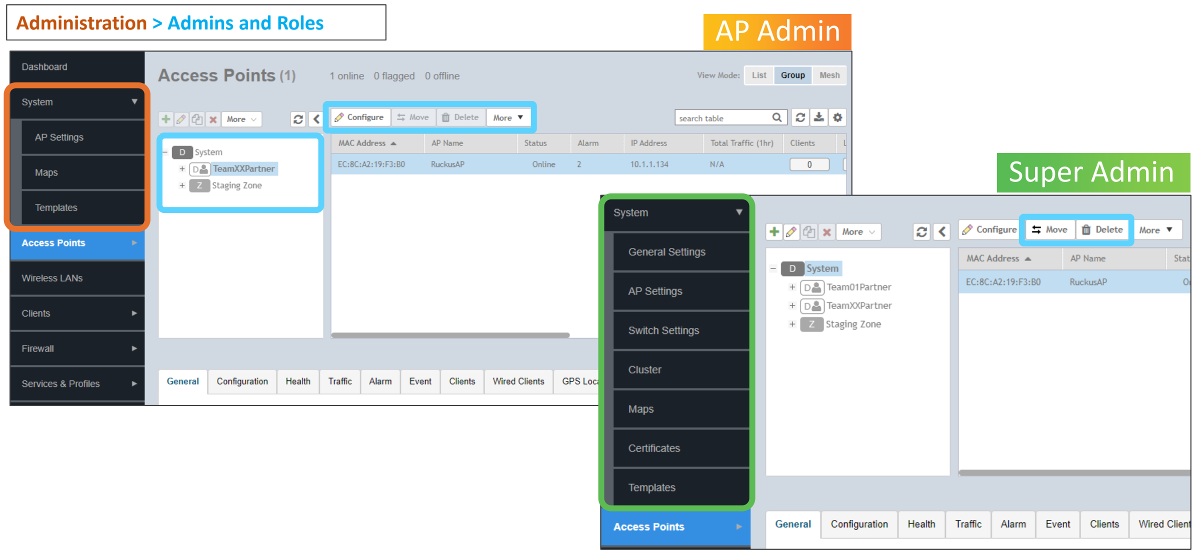
182 | © 2024 CommScope, Inc.

When logging in to High Scale Controller, there are two options available. The first is to log on to the System Domain. Logging in to the System Domain provides access to resources within the System Domain which includes Subdomains and Zones with the rights set by the assigned permission.

The second option is to log in to a Subdomain or Partner Domain. When logging in to a Subdomain or Partner Domain, you need to also specify the Domain in the login username by adding @[Domain_Name]. This will provide you with access to that partner domain and provide the rights assigned to that username.

Administrator Login – Interface Differences

Administration > Admins and Roles



183 | © 2024 CommScope, Inc.

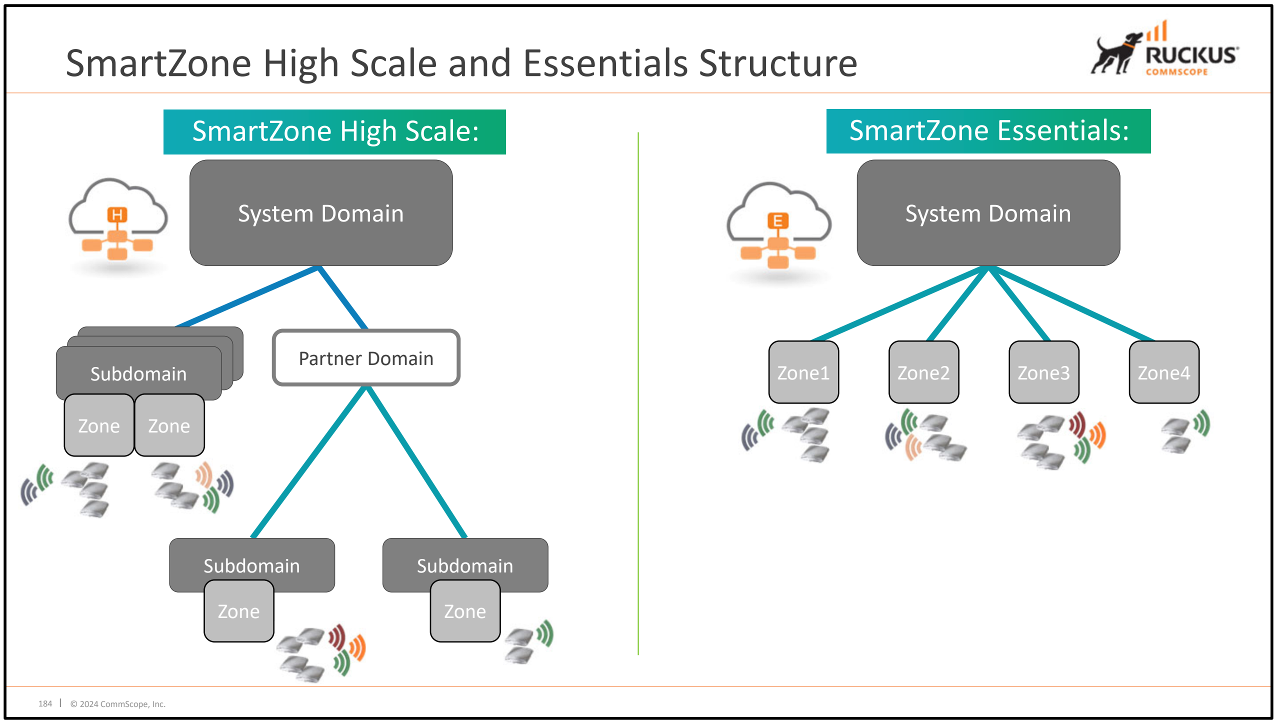
When you log in with your alternative Administrator account you will see a number of differences based on the Group settings that apply to the logged in account.

In this example, the Administrator is logging in with AP Admin Permissions, and has selected the **Access Point** menu. Note the following:

- The left-hand menu buttons have changed. Buttons have been removed that relate to system settings that the AP Administrator is not permitted to see.
- Only the Partner Domain and its Subdomains and Zones are visible.
- The Staging Zone is still visible
- The **Move** and **Delete** options for Access Point configuration are greyed out.

Clearly there will be many differences in the web interface and available options depending on the logged in Administrator and Group permissions.

You should ensure you fully explore these options and test comprehensively before deploying Administrator accounts.



SmartZone High Scale and Essentials Structure

SmartZone High Scale:

System Domain

Subdomain

Partner Domain

Zone

Zone

Subdomain

Subdomain

Zone

Zone

SmartZone Essentials:

System Domain

Zone1

Zone2

Zone3

Zone4

184 | © 2024 CommScope, Inc.

The most important of the differences between High Scale and Essentials is in the structure. SmartZone High Scale controllers are based on Domains.

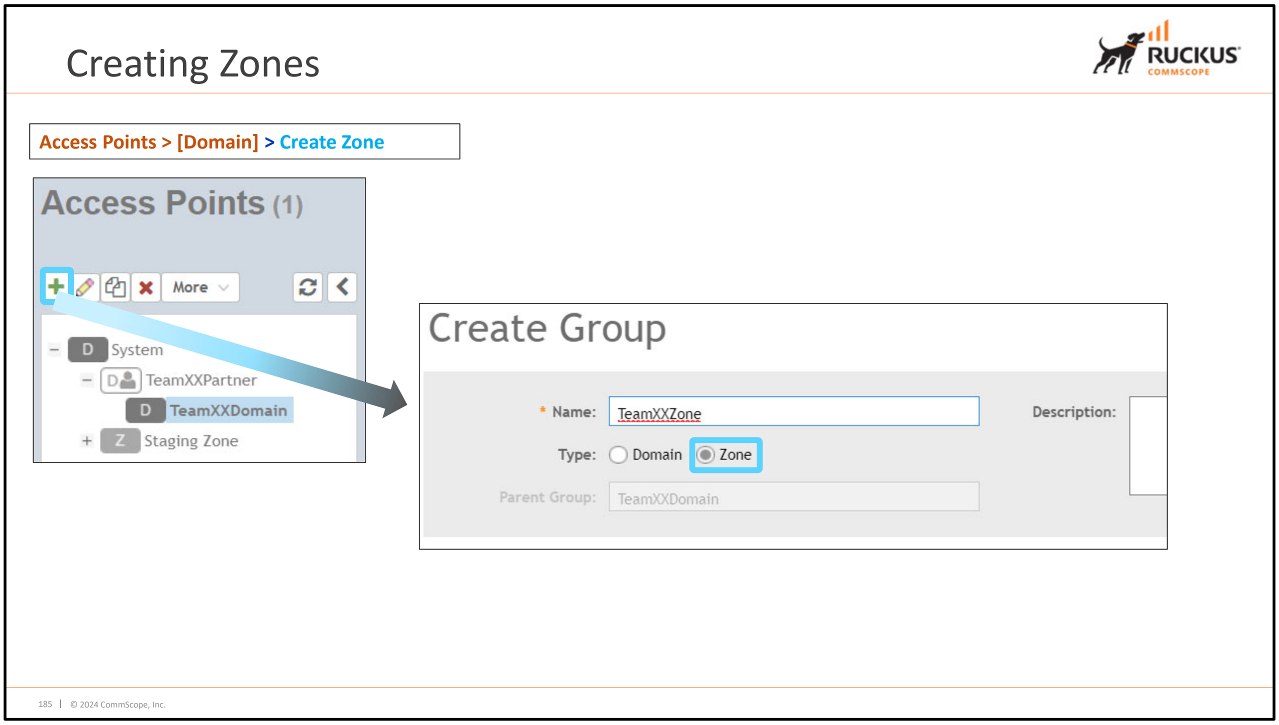
Domains represent administration boundaries. SmartZone High Scale is designed for large scale deployments, and you can create additional Subdomains to which you can delegate administration. Subdomains will inherit a number of settings from the System Domain.

You can also create Partner Domains. Partner Domain Administrators have autonomy and control over operations and functions within the Partner Domain and can customize some settings rather than inherit them from the System Domain. Partner Domains are ideal for Managed Service Providers and can themselves contain Subdomains.

Once Partner Domains and Subdomains have been created, the next step is to create the Zones. Whereas Domains represent administrative boundaries, Zones determine the configuration and behavior of the Access Points .

SmartZone Essentials is based on a single System Domain. As Domains represent administration boundaries, there is a single point of administration, though you can add additional Administrators with customized rights.

You can NOT create Subdomains or Partner Domains. You can, however, create multiple Zones. Remember that Zones determine the configuration and behavior of the Access Points .



Creating Zones

Access Points > [Domain] > Create Zone

Create Group

* Name: TeamXXZone

Type: ○ Domain ● Zone

Parent Group: TeamXXDomain

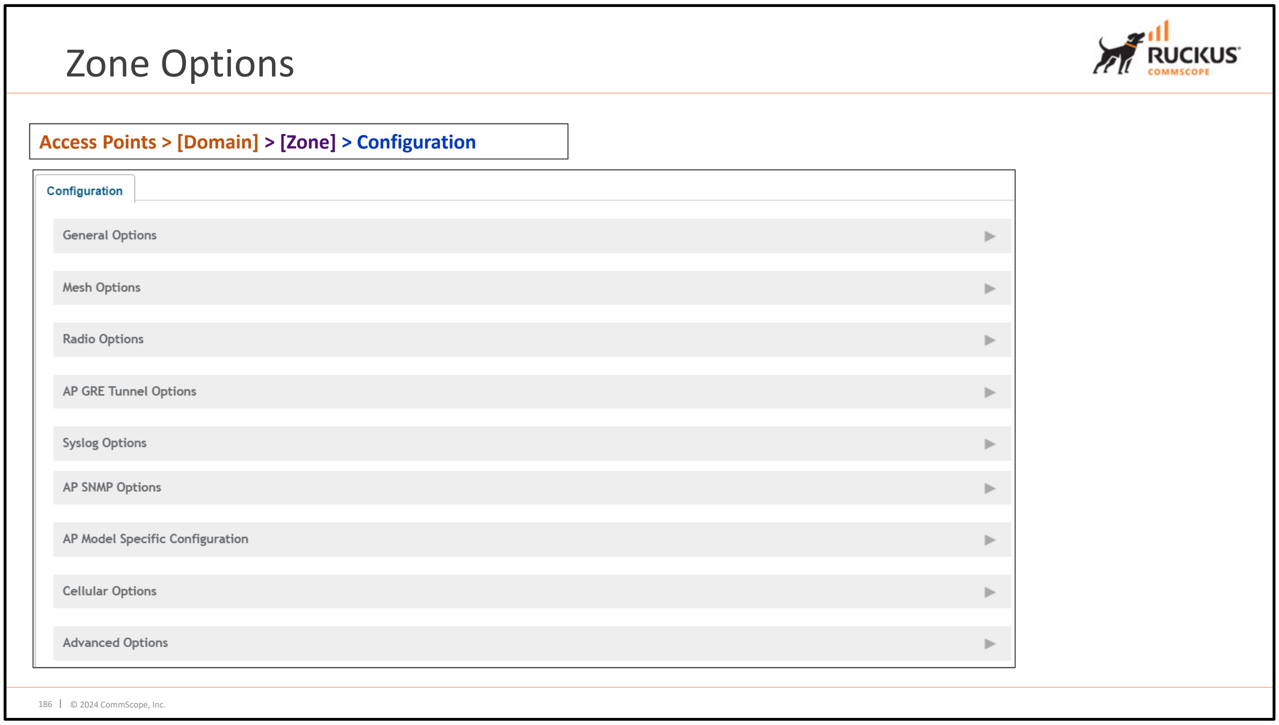
Description:

185 | © 2024 CommScope, Inc.

In order to create a Zone, navigate to **Access Points.**

On High Scale controllers, you can create a Zone under the System Domain, a Partner Domain, or a Subdomain of either. Where the Zone is created is determined by which Domain is selected/highlighted when Zone is created.

Selecting the **"+"** icon opens a new **Create Group** window. In this case, "Group" can refer to either a new Subdomain or a new Zone. **Domain** is selected by default. By selecting **Zone**, you will create a new Zone and will be required to edit the Zone settings.



Zone Options

Access Points > [Domain] > [Zone] > Configuration

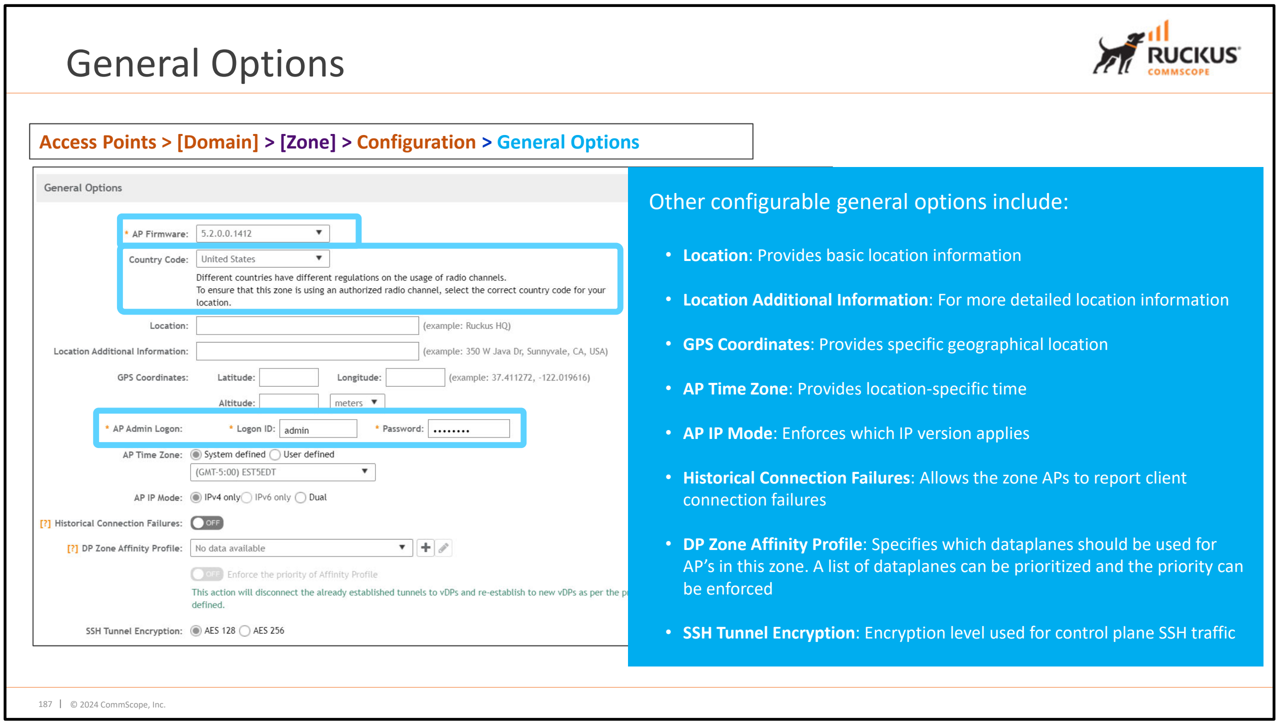
Configuration

- General Options
- Mesh Options
- Radio Options
- AP GRE Tunnel Options
- Syslog Options
- AP SNMP Options
- AP Model Specific Configuration
- Cellular Options
- Advanced Options

186 | © 2024 CommScope, Inc.

When you create a Zone, there are a number of options you are able to configure: **General Options**

- **Mesh Options**
- **Radio Options**
- **AP GRE Tunnel Options**
- **Syslog Options**
- **AP SNMP Options**
- **AP Model Specific Configuration**
- **Cellular Options**
- **Advanced Options** – As the name implies contains the most comprehensive settings and brings in many different AP features.



General Options

Access Points > [Domain] > [Zone] > Configuration > General Options

General Options

* AP Firmware: 5.2.0.0.1412 ▼

Country Code: United States ▼

Different countries have different regulations on the usage of radio channels.
To ensure that this zone is using an authorized radio channel, select the correct country code for your location.

Location: (example: Ruckus HQ)

Location Additional Information: (example: 350 W Java Dr, Sunnyvale, CA, USA)

GPS Coordinates: Latitude: Longitude: (example: 37.411272, -122.019616)

Altitude: meters ▼

* AP Admin Logon: * Logon ID: admin * Password: ••••••••

AP Time Zone: ● System defined ○ User defined

(GMT-5:00) EST5EDT ▼

AP IP Mode: ● IPv4 only ○ IPv6 only ○ Dual

[?] Historical Connection Failures: OFF

[?] DP Zone Affinity Profile: No data available ▼

OFF Enforce the priority of Affinity Profile

This action will disconnect the already established tunnels to vDPs and re-establish to new vDPs as per the p
defined.

SSH Tunnel Encryption: ● AES 128 ○ AES 256

Other configurable general options include:

- **Location**: Provides basic location information
- **Location Additional Information**: For more detailed location information
- **GPS Coordinates**: Provides specific geographical location
- **AP Time Zone**: Provides location-specific time
- **AP IP Mode**: Enforces which IP version applies
- **Historical Connection Failures**: Allows the zone APs to report client connection failures
- **DP Zone Affinity Profile**: Specifies which dataplanes should be used for AP’s in this zone. A list of dataplanes can be prioritized and the priority can be enforced
- **SSH Tunnel Encryption**: Encryption level used for control plane SSH traffic

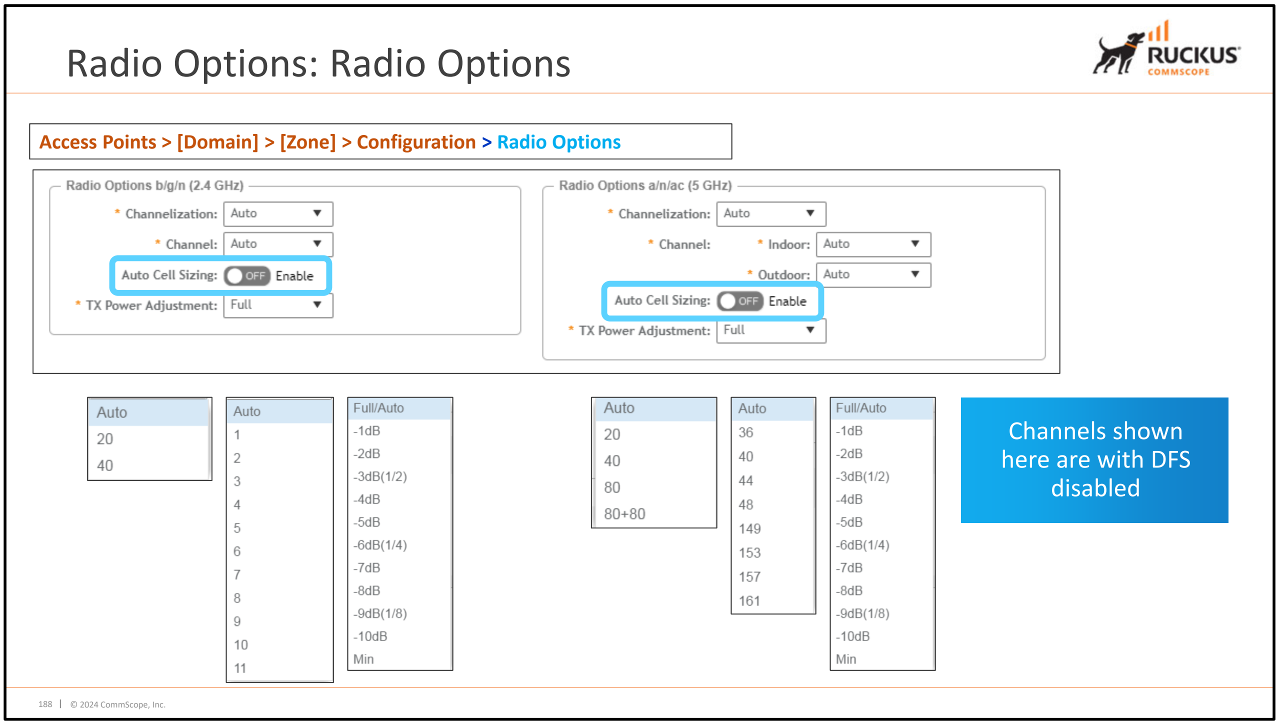
187 |

The SmartZone Zone General Options have a number of settings. The most important are:

- **AP Firmware**: The firmware you will deploy to the Zone to enable new features or address any security vulnerabilities. You will be able to choose from the versions of firmware that have been uploaded to the controller from its first build and subsequent upgrades. This setting is required, but will be populated with a default value based on the controller version.
- **Country Code**: The Country Code sets the channels and port settings. Using the correct country code critical because it ensures that APs use only authorized radio channels.
- **AP Admin Logon**: Configures the CLI logon, used to remotely administer APs. These settings are required and have no default values.

Other configurable options include:

- Location information fields to provide detailed information on zone location as well as provide GPS coordinates
- AP Time zone
- AP IP Mode
- Historical Connection Failures to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.
- Zone Affinity profile options to specify which dataplanes should be used for AP’s in this zone. The list of dataplanes can be prioritized, and the priority enforced by setting the **Enforce the Priority of Affinity Profile** slider to **ON**.
- And SSH tunnel encryption options for the control plane traffic



Radio Options: Radio Options

Access Points > [Domain] > [Zone] > Configuration > Radio Options

Radio Options b/g/n (2.4 GHz)

- * Channelization: Auto
- * Channel: Auto
- Auto Cell Sizing: OFF Enable
- * TX Power Adjustment: Full

Radio Options a/n/ac (5 GHz)

- * Channelization: Auto
- * Channel: * Indoor: Auto
- * Outdoor: Auto
- Auto Cell Sizing: OFF Enable
- * TX Power Adjustment: Full

Channels shown here are with DFS disabled

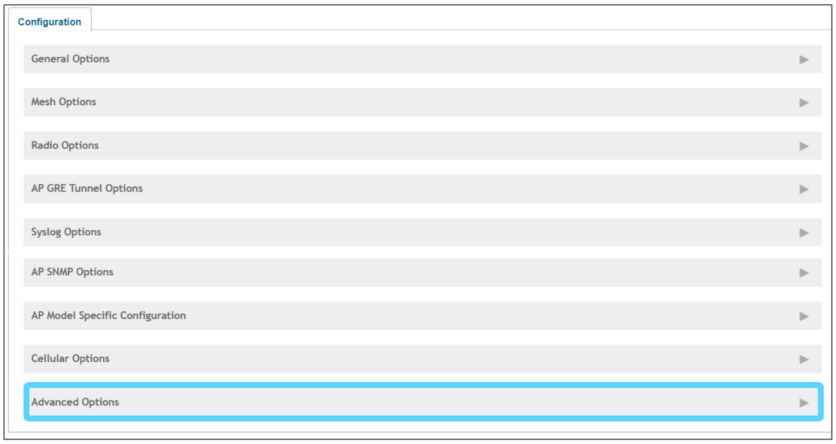
188 | © 2024 CommScope, Inc.

The second available setting is related to the radio transmissions, and is appropriately labelled **Radio Options**.
There are four settings:.

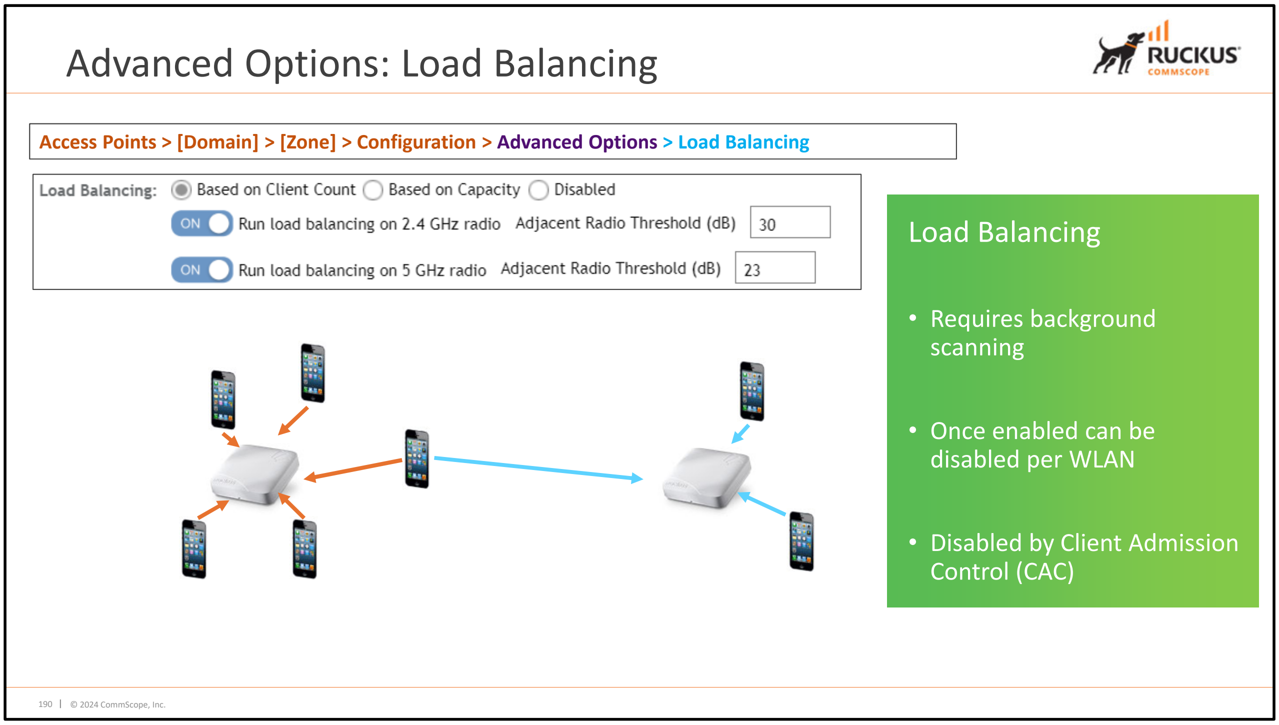
- **Channelization: Auto**, **20** or **40** for 2.4GHz, **Auto**, **20**, **40**, **80** or **80+80,** and if DFS channels are enabled **160** for 5GHz. When set to **Auto**, the Access Points will automatically select the channel width.
- **Channel: Auto** or **specific channel**. When set to **Auto**, the controller will select the channels that each Access Point will use based on the environment in which the Access Point is placed. Selecting a specific channel configures all of the Access Points within the Zone to use that channel. The channels specified in the **Channel Range** options will still be available for background scanning.
- **Auto Cell Sizing** is disabled by default. However when enabled it allows the APs to adjust their own transmit power levels in relation to other APs that are heard in the environment. This can help minimize RF overlap and interference. **Background Scanning** must be enabled under the WLAN advanced settings to make use of this feature. Turning on Auto Cell Sizing disables the ability to manually set TX power.
- **TX Power Adjustment: Full** to **Min**. You can choose to reduce the maximum transmit power used by the Access Point from the default.
  - The **Full/Auto** setting represents this highest transmission power allowed according to the regulation domain and the Access Point model.
  - The dB scale represents by how much the transmission power is decreased relative to Full.
  - The **Min** setting is the lowest possible transmission value that the Access Point can make. This depends on the model and chipset, and is commonly 0dBm

Advanced Zone Options

Access Points > [Domain] > [Zone] > Configuration > Advanced Options



The Zone **Advanced Options** relate mostly to the behaviour of the Access Point radios. The following is a summary of some of the key settings.



Advanced Options: Load Balancing

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Load Balancing

Load Balancing: ● Based on Client Count ○ Based on Capacity ○ Disabled

ON Run load balancing on 2.4 GHz radio Adjacent Radio Threshold (dB) 30

ON Run load balancing on 5 GHz radio Adjacent Radio Threshold (dB) 23

Load Balancing

- Requires background scanning
- Once enabled can be disabled per WLAN
- Disabled by Client Admission Control (CAC)

190 | © 2024 CommScope, Inc.

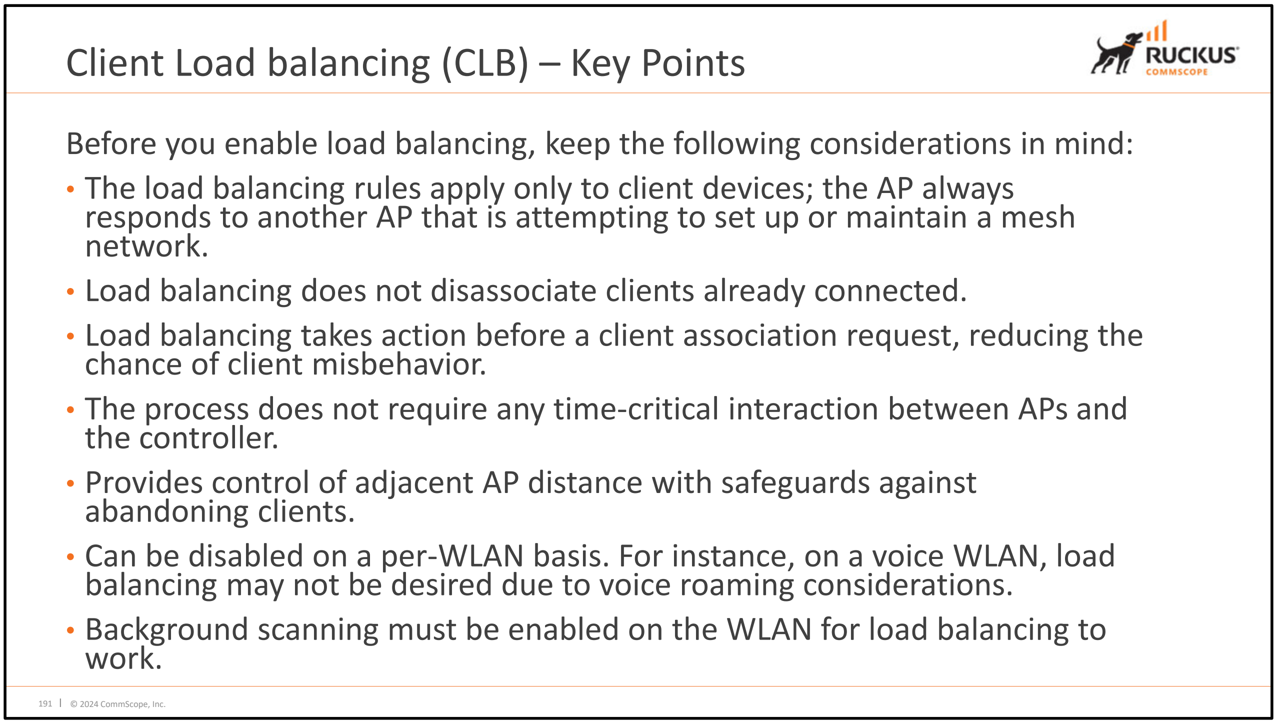
Load Balancing balances client load across Access Points. With options to balance:

- **Based on Client Count** – which allows configurations for both load balancing and band balancing based on numbers of clients associated or,
- **Based on Capacity** – which allows configurations for load balancing only based on AP capacity
- Disabling Load Balancing disables load and band balancing

Load Balancing requires Background Scanning and once enabled, it can be can be disabled per WLAN.
Load Balancing is disabled when Client Admission Control is in use.

When joining a WLAN, a client naturally attempts to connect to the access that appears to have the strongest signal. With Load Balancing enabled, the favored Access Point does not allow the connection, and the client connects instead to an alternative Access Point. The configurable thresholds are used to determine the SNR of an adjacent Access Point before Load Balancing will be applied.

Client Load Balancing is disabled by default and as with many of the system settings, it's recommended leave the default settings in place unless extensive testing and analysis can be performed.



Client Load balancing (CLB) – Key Points

Before you enable load balancing, keep the following considerations in mind:

- The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- The process does not require any time-critical interaction between APs and the controller.
- Provides control of adjacent AP distance with safeguards against abandoning clients.
- Can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.
- Background scanning must be enabled on the WLAN for load balancing to work.

191 |

Before you enable load balancing, keep the following considerations in mind:

The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.

Load balancing does not disassociate clients already connected.

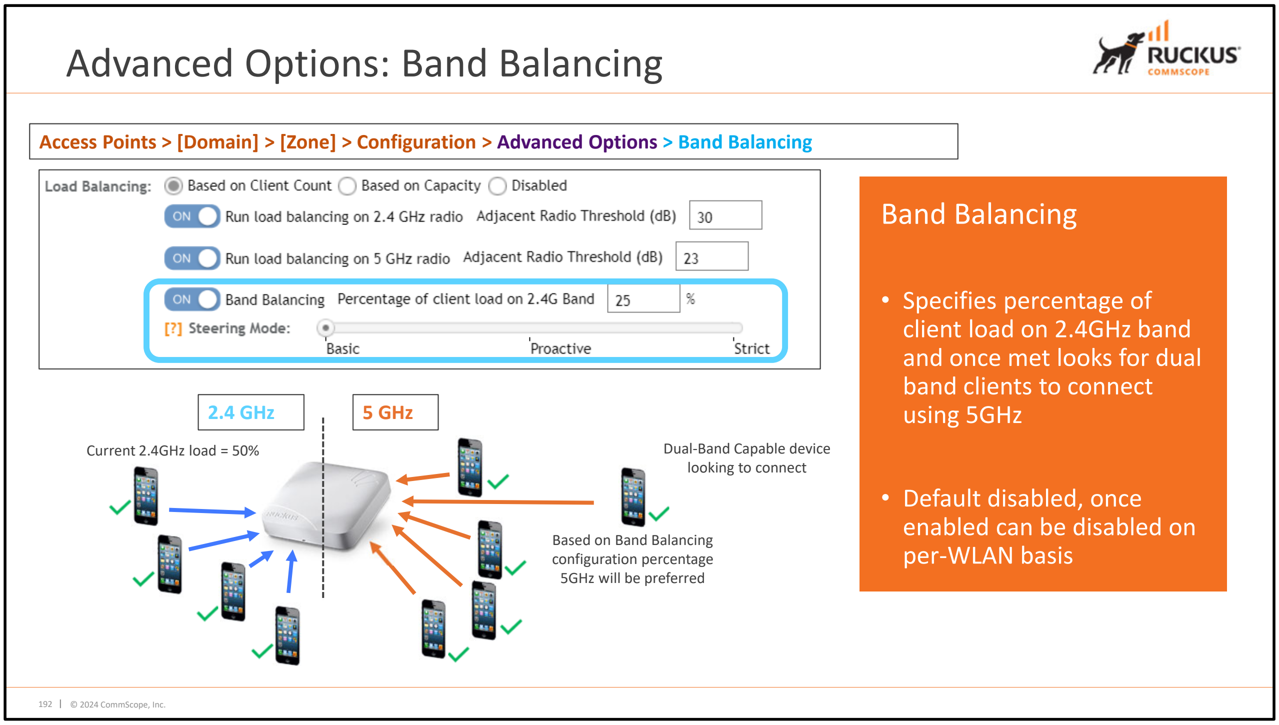
Load balancing takes action before a client association request, reducing the chance of client misbehavior.

The process does not require any time-critical interaction between APs and the controller.

Provides control of adjacent AP distance with safeguards against abandoning clients.

Can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.

Background scanning must be enabled on the WLAN for load balancing to work.



Advanced Options: Band Balancing

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Band Balancing

Load Balancing: ● Based on Client Count ○ Based on Capacity ○ Disabled

ON Run load balancing on 2.4 GHz radio Adjacent Radio Threshold (dB) 30

ON Run load balancing on 5 GHz radio Adjacent Radio Threshold (dB) 23

ON Band Balancing Percentage of client load on 2.4G Band 25 %

[?] Steering Mode: Basic Proactive Strict

2.4 GHz
5 GHz
Current 2.4GHz load = 50%
Dual-Band Capable device looking to connect
Based on Band Balancing configuration percentage 5GHz will be preferred

Band Balancing

- Specifies percentage of client load on 2.4GHz band and once met looks for dual band clients to connect using 5GHz
- Default disabled, once enabled can be disabled on per-WLAN basis

192 | © 2024 CommScope, Inc.

Band Balancing, balances the client load across the Access Point radios. Band Balancing is not to be confused with Band Steering.

Band Steering was originally implemented by many vendors to encourage WLAN devices to use 5GHz channels. This was due to the perceived greater signal strength of 2.4GHz over 5GHz transmissions.

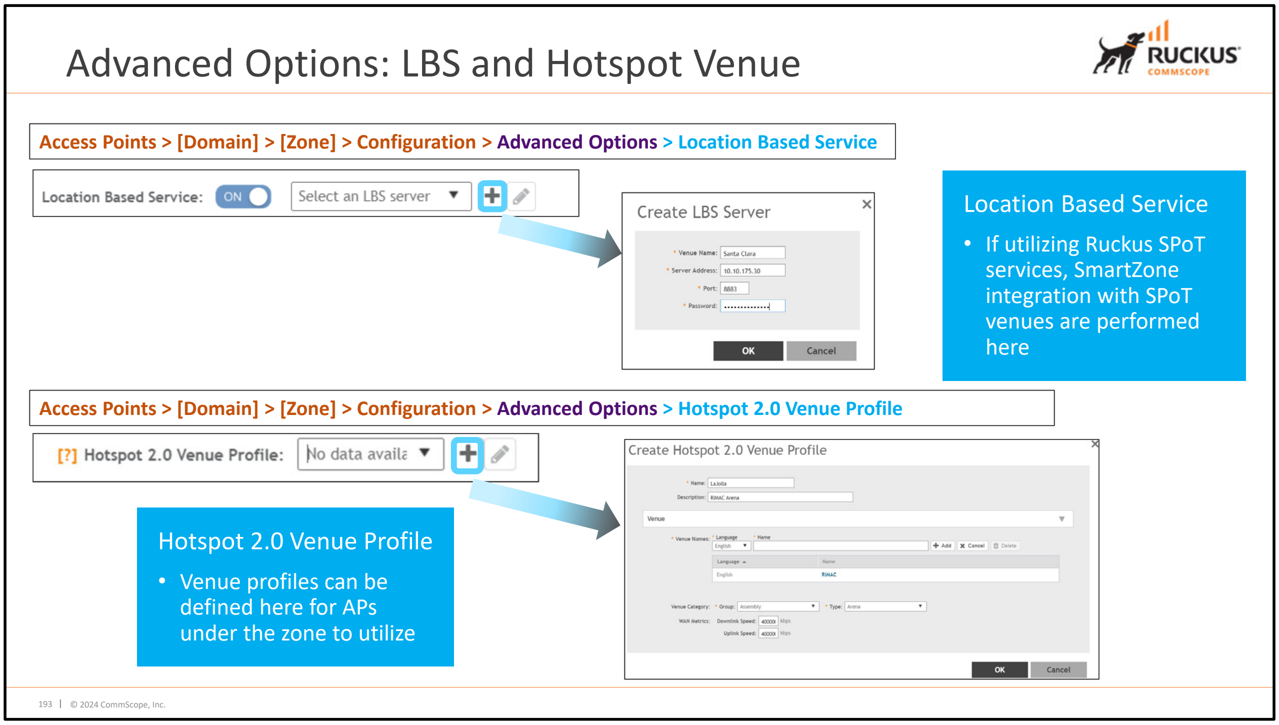
Many modern devices will now look to connect on the channel that offers the greatest throughput. With 802.11n, ac and ax, devices are able to use channels wider than 20MHz in 5GHz, so they naturally favour 5GHz.

Band Balancing encourages dual-band clients to connect to 5 GHz radios when the configured percentage threshold is reached.

You can use the slider to actively control associated stations to meet certain band distribution requirements allowing for dynamic band balancing:

- **Basic**: during heavy load conditions, this option withholds probe and authentication responses in order to balance clients.
- **Proactive**: uses the Basic configuration in addition to actively re-balances clients using the 802.11v BSS Transition Management (BTM).
- **Strict**: uses the Proactive configuration in addition to forcefully re-balances clients using the 802.11v BTM.

Band Balancing is disabled by default, and once enabled can be disabled per individual WLAN.



Advanced Options: LBS and Hotspot Venue

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Location Based Service

Location Based Service: ON | Select an LBS server ▼

Create LBS Server

- Venue Name: Santa Clara
- Server Address: 10.10.175.30
- Port: 8883
- Password: ••••••••••••••

Location Based Service

- If utilizing Ruckus SPoT services, SmartZone integration with SPoT venues are performed here

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Hotspot 2.0 Venue Profile

[?] Hotspot 2.0 Venue Profile: No data availa ▼

Create Hotspot 2.0 Venue Profile

- Name: LaJolla
- Description: RIMAC Arena

Venue

- Venue Names: Language: English ▼ Name:

Language	Name
English	RIMAC

- Venue Category: Group: Assembly ▼ Type: Arena ▼
- WAN Metrics: Downlink Speed: 40000 kbps
- Uplink Speed: 40000 kbps

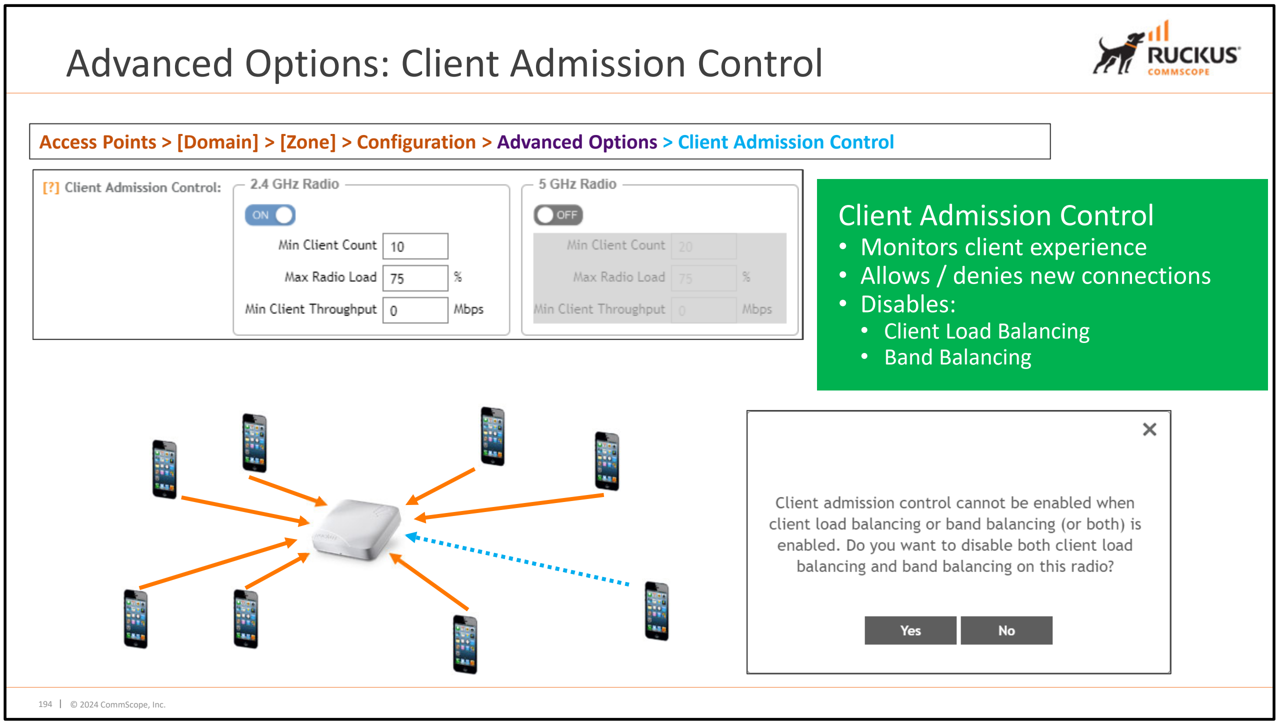
Hotspot 2.0 Venue Profile

- Venue profiles can be defined here for APs under the zone to utilize

193 | © 2024 CommScope, Inc.

Enabling **Location Based Services** enables Ruckus Smart Positioning Technology (SPoT) integration with SmartZone. Once a venue has been created within SPoT, the venue information is then applied here.

HotSpot 2.0 Venue Profiles allows administrators to configure a Hotspot venue which will be utilized by APs in this zone. Hotspot Venue Profiles can also be configured by navigating to **Services & Profiles > Hotspot 2.0** and selecting the zone.



Advanced Options: Client Admission Control

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Client Admission Control

[?] Client Admission Control:

	2.4 GHz Radio		5 GHz Radio	
	ON		OFF	
Min Client Count	10		20	
Max Radio Load	75	%	75	%
Min Client Throughput	0	Mbps	0	Mbps

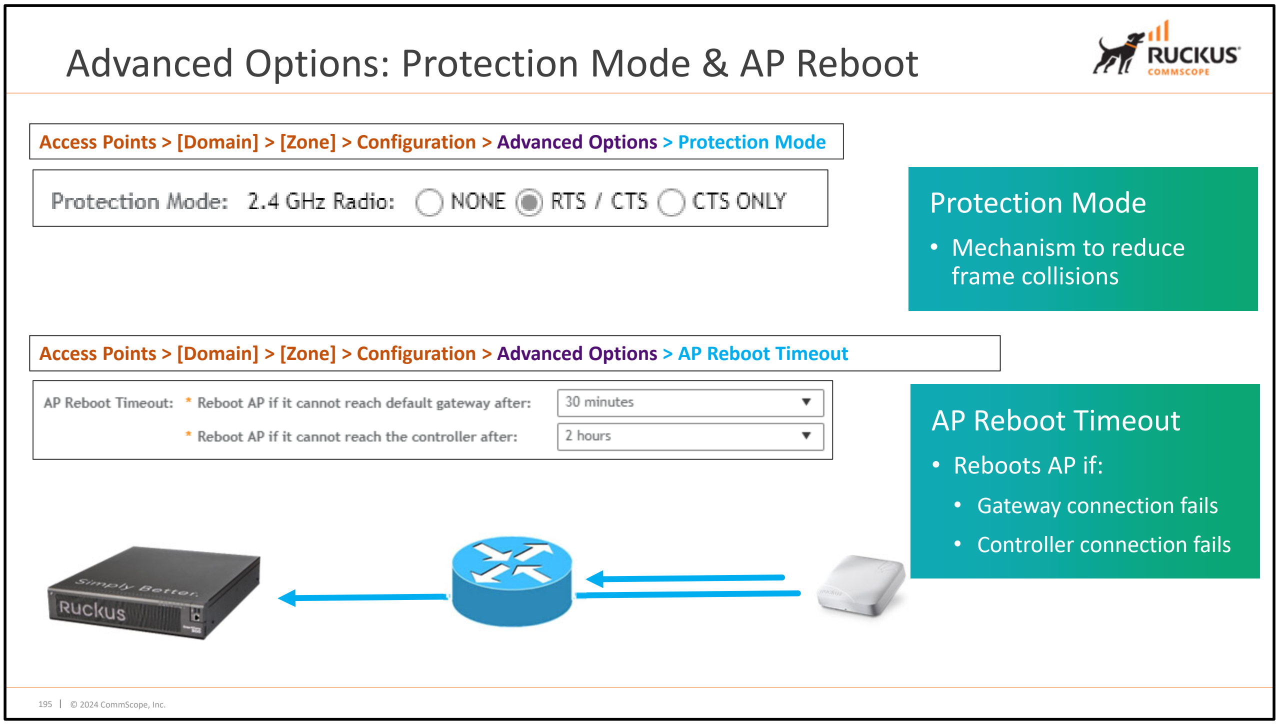
Client Admission Control
- Monitors client experience
- Allows / denies new connections
- Disables:
  - Client Load Balancing
  - Band Balancing

Client admission control cannot be enabled when client load balancing or band balancing (or both) is enabled. Do you want to disable both client load balancing and band balancing on this radio?

194 | © 2024 CommScope, Inc.

Client Admission Control is used to allow or deny new client connections based on the available Quality of Experience for currently connected clients.
When Client Admission Control is enabled, Access Points use algorithms based on the configurable settings on order to permit or deny client connections. Use of **Client Admission Control** disables **Client Load Balancing** and **Band Balancing**.

If enabled on a Zone, a message asks to confirm that you wish to disable load balancing and band balancing. If **Yes** is selected, CAC will be enabled and Client Load Balancing and/or Band Balancing will be disabled.



Advanced Options: Protection Mode & AP Reboot

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Protection Mode

Protection Mode: 2.4 GHz Radio: ○ NONE ● RTS / CTS ○ CTS ONLY

Protection Mode
- Mechanism to reduce frame collisions

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > AP Reboot Timeout

AP Reboot Timeout: * Reboot AP if it cannot reach default gateway after: 30 minutes
* Reboot AP if it cannot reach the controller after: 2 hours

AP Reboot Timeout
- Reboots AP if:
  - Gateway connection fails
  - Controller connection fails

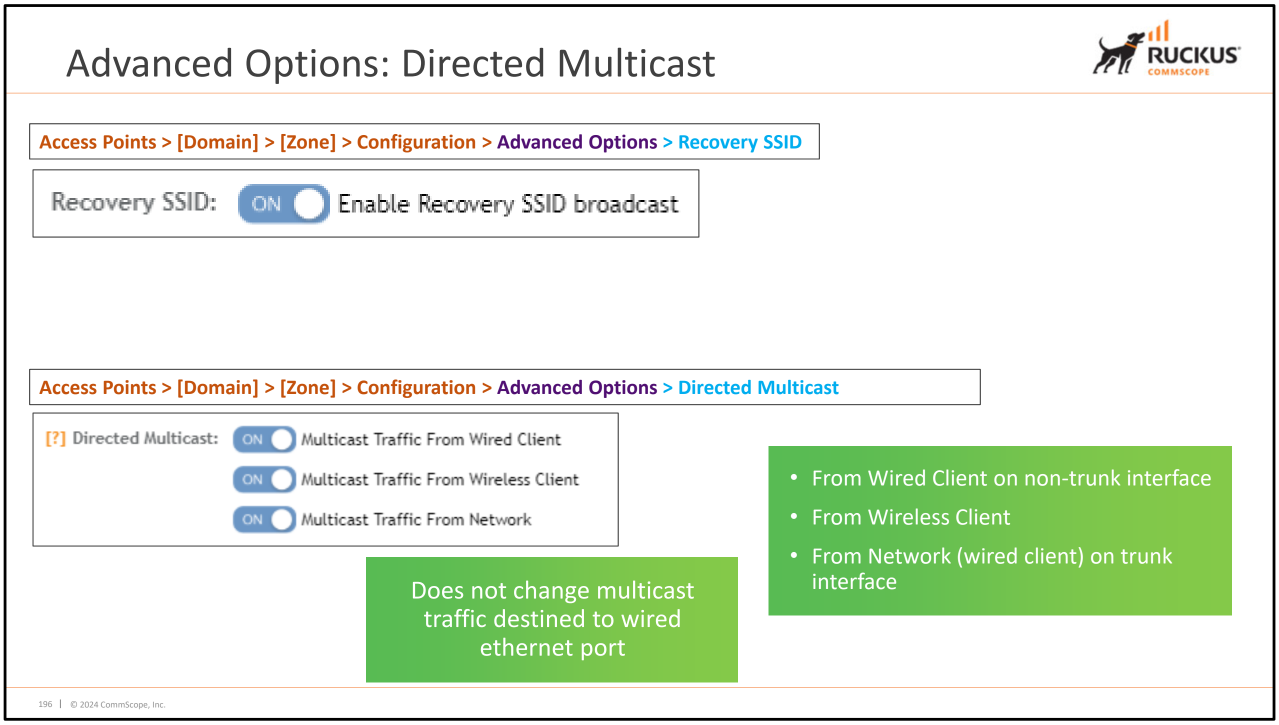
195 | © 2024 CommScope, Inc.

Protection Mode allows you to set the mode a 2.4 GHz radio will use to reduce collisions. These settings control how 802.11 devices know when they should communicate with another device and by default RTS/CTS is used. In most instances this setting should be left at the default value.

AP Reboot Timeout, which is enabled with the default values shown here, will reboot an Access Point if the Access Point detects loss of connectivity. The AP will reboot if:

- It loses connection to its default gateway or
- Loses connectivity to the controller

You can disable the AP reboot by setting both of the timers to 0 (Never Reboot). These timers should be set according to your redundancy strategy and your WLAN settings and requirements.



Advanced Options: Directed Multicast

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Recovery SSID

Recovery SSID: ON Enable Recovery SSID broadcast

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Directed Multicast

[?] Directed Multicast: ON Multicast Traffic From Wired Client
ON Multicast Traffic From Wireless Client
ON Multicast Traffic From Network

Does not change multicast traffic destined to wired ethernet port

- From Wired Client on non-trunk interface
- From Wireless Client
- From Network (wired client) on trunk interface

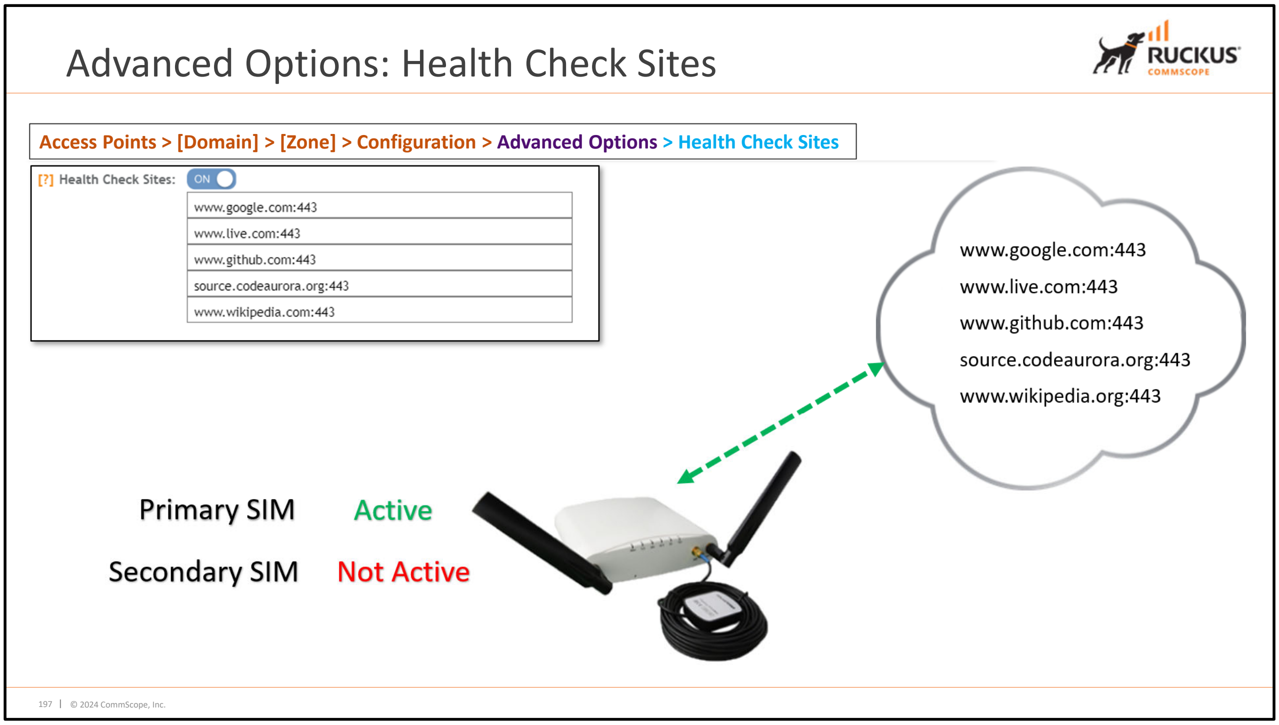
196 | © 2024 CommScope, Inc.

The **Recovery SSID** option allows you to disable the broadcasting of the Recovery, or island, SSID for APs in the zone. The default setting is for the recovery SSID to be enabled. This recovery SSID allows APs to broadcast a WLAN that gives administrators the ability to connect directly to the AP when in range.

Directed Multicast transfers multicast traffic as unicast packets to enhance the performance in wireless networks. This cuts down on multicast flooding in the WLAN. There is no change to the multicast traffic if the destination port is the wired Ethernet port, only WLAN destinations.

Three options have been added to control multicast conversion and all three are enabled by default:

- **Wired Client** – Enables multicast-to-unicast conversion from wired client on a non-trunk interface
- **Wireless Client** – Enables multicast-to-unicast conversion from wireless client
- **Network** – Enables multicast-to-unicast conversion from wired client on a trunk interface



Advanced Options: Health Check Sites

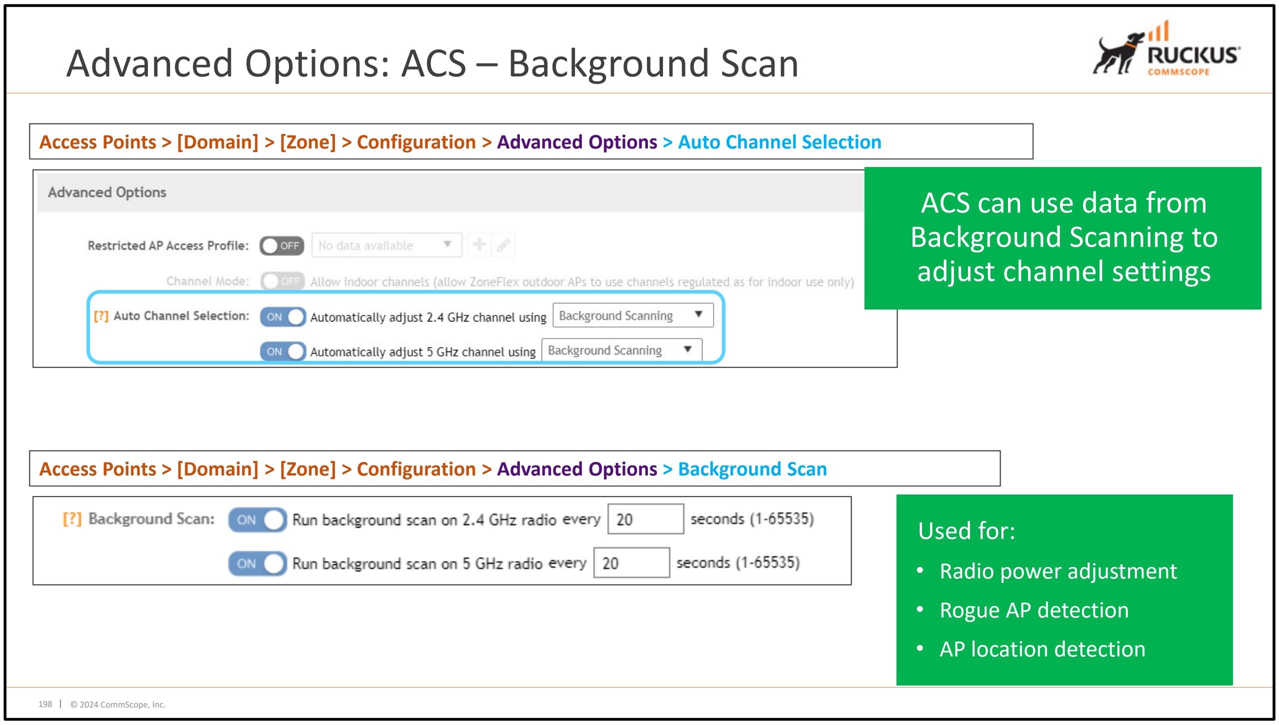
Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Health Check Sites

[?] Health Check Sites: ON

- www.google.com:443
- www.live.com:443
- www.github.com:443
- source.codeaurora.org:443
- www.wikipedia.com:443

Primary SIM	Active
Secondary SIM	Not Active

The **Health Check Sites** option is disabled by default, but once enabled allows for modification of the sites listed. These sites are used by Ruckus M510 access points to validate the internet connectivity of their cellular networks **,** if these sites are unavailable on their primary SIM failover to the secondary SIM would occur.



Advanced Options: ACS – Background Scan

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Auto Channel Selection

Advanced Options

Restricted AP Access Profile: OFF No data available

Channel Mode: OFF Allow indoor channels (allow ZoneFlex outdoor APs to use channels regulated as for indoor use only)

[?] Auto Channel Selection: ON Automatically adjust 2.4 GHz channel using Background Scanning

ON Automatically adjust 5 GHz channel using Background Scanning

ACS can use data from Background Scanning to adjust channel settings

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Background Scan

[?] Background Scan: ON Run background scan on 2.4 GHz radio every 20 seconds (1-65535)

ON Run background scan on 5 GHz radio every 20 seconds (1-65535)

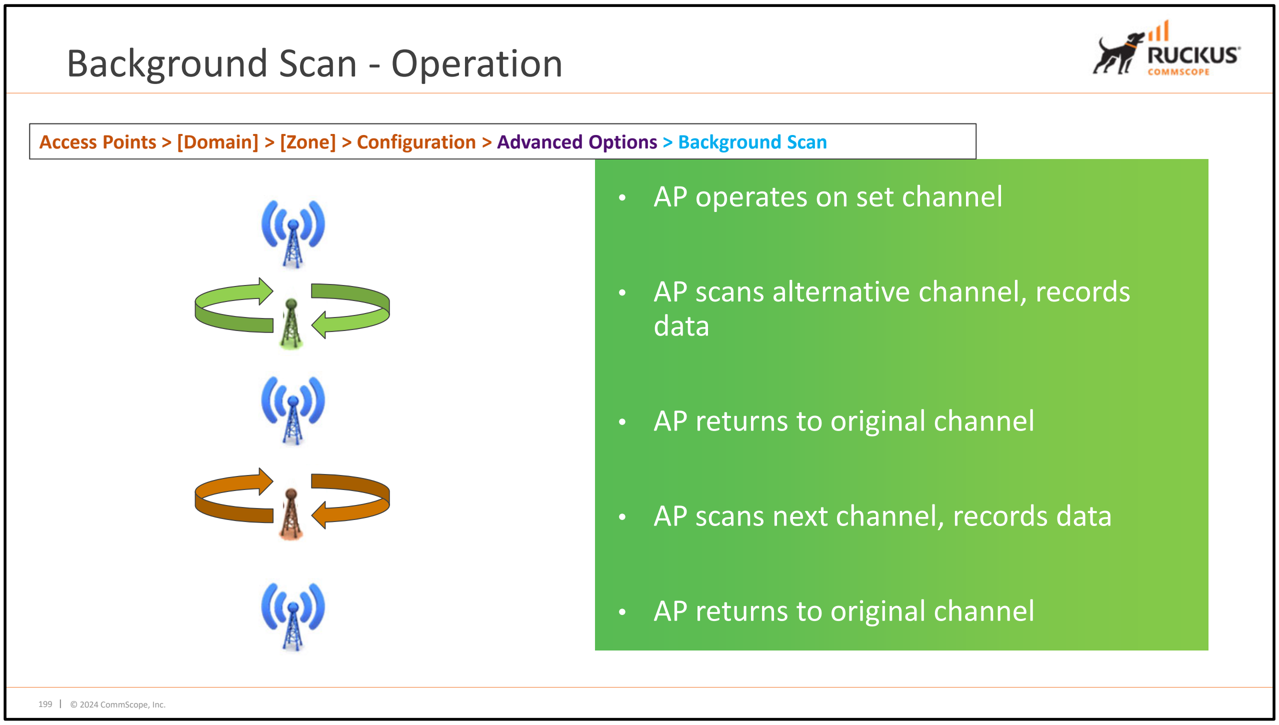
Used for:

- Radio power adjustment
- Rogue AP detection
- AP location detection

198 | © 2024 CommScope, Inc.

Auto Channel Selection sets how the channels will auto-adjust to RF problems in the environment. There are two options available – **Background Scanning**, or **ChannelFly**.

Background Scanning:, which is the default setting, is the process of having an Access Point temporarily go off channel in order to gather information on the surrounding WLAN environment, and then return. Background Scanning takes place by default, and runs every 20 seconds unless you configure otherwise. The data recorded during Background Scanning is used for Radio Channel and Power Adjustment, Rogue Access Point Detection and Access Point Location Detection. With Background Scanning enabled, Auto Channel Selection provides the option to use the data from Background Scanning to adjust channel settings to optimize WLAN operations.



Background Scan - Operation

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Background Scan

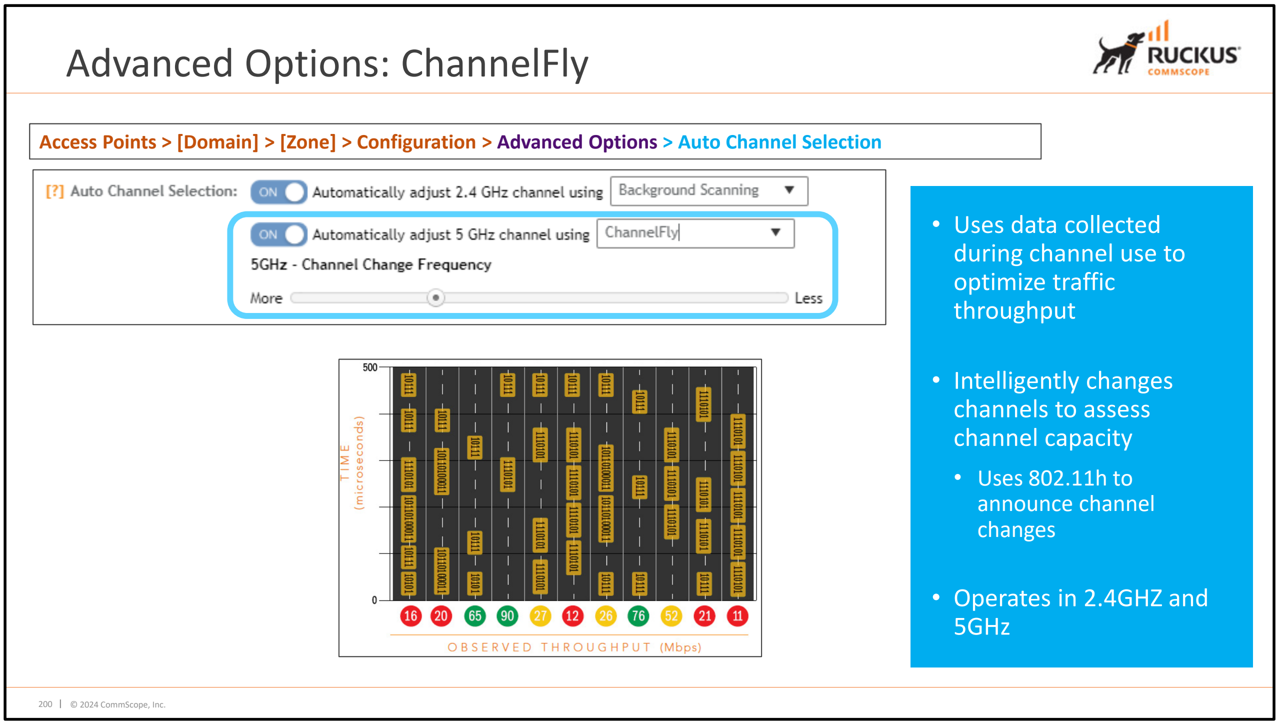
- AP operates on set channel
- AP scans alternative channel, records data
- AP returns to original channel
- AP scans next channel, records data
- AP returns to original channel

199 | © 2024 CommScope, Inc.

Background scanning is relatively simple service and operates as follows:

- The Access Point operates on a set channel
- The Access Point scans an alternative channel and records data
- The Access Point returns to the original channel
- The Access Point scans the next channel and records data
- The Access Point returns to the original channel

Background Scanning is invisible to the client stations who continue to operate on the Access Point’s normal channel and is required for operation of other features such as **Auto Cell Sizing** and **Rogue AP Detection**



Advanced Options: ChannelFly

Access Points > [Domain] > [Zone] > Configuration > Advanced Options > Auto Channel Selection

[?] Auto Channel Selection: ON Automatically adjust 2.4 GHz channel using Background Scanning

ON Automatically adjust 5 GHz channel using ChannelFly

5GHz - Channel Change Frequency

More ○ Less

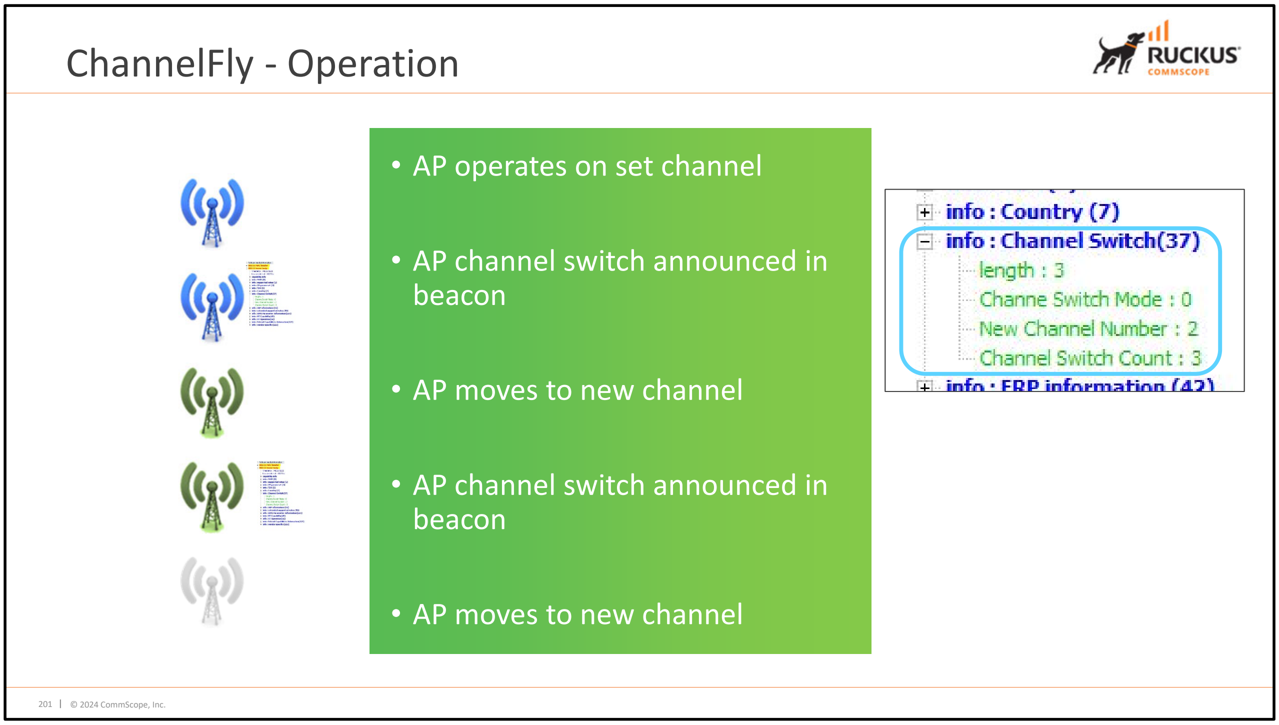
- Uses data collected during channel use to optimize traffic throughput
- Intelligently changes channels to assess channel capacity
  - Uses 802.11h to announce channel changes
- Operates in 2.4GHZ and 5GHz

200 | © 2024 CommScope, Inc.

ChannelFly changes the channel periodically and records performance data on the channel. The data recorded is used to determine the channels that offer the best potential throughput. The metrics gained using ChannelFly can be used to by Auto Channel Selection.

When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and Ruckus mesh nodes in the 2.4 GHz and/or 5 GHz bands.

Selecting the **Channel Change Frequency** determines how often ChannelFly will change channel. This setting is applied uniquely per antenna if enabled on both 2.4 and 5 GHz.



ChannelFly - Operation

- AP operates on set channel
- AP channel switch announced in beacon
- AP moves to new channel
- AP channel switch announced in beacon
- AP moves to new channel

```
+ info : Country (7)
- info : Channel Switch(37)
    length : 3
    Channe Switch Mode : 0
    New Channel Number : 2
    Channel Switch Count : 3
+ info : ERP information (42)
```

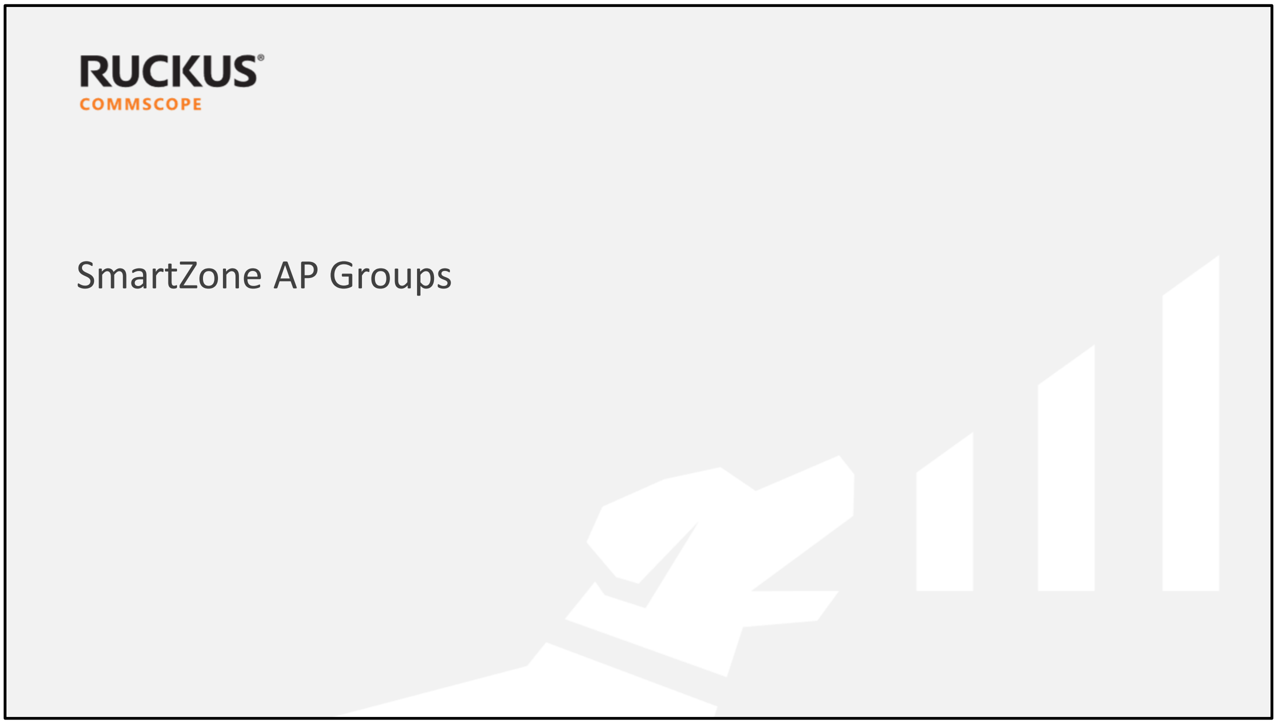
201 | © 2024 CommScope, Inc.

ChannelFly operates by regularly changing the Access Point to a new channel by following this process:

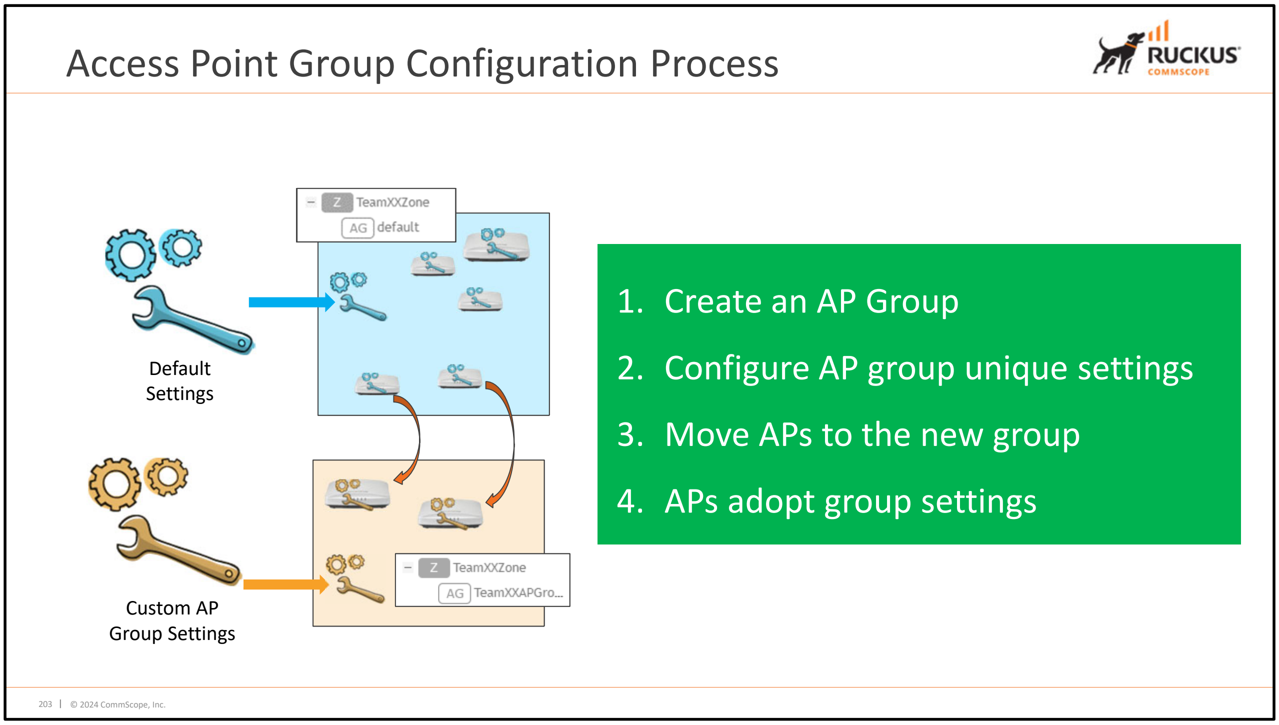
- The Access Point operates on set channel
- The channel switch is announced in beacon
- The Access Point moves to new channel
- The channel switch is announced in beacon
- The Access Point moves to new channel

There are two important things to consider when using ChannelFly. The first is that when using ChannelFly, Background Scanning is still being performed. The choice is only which of the two is used to provide the metrics used for Auto Channel Selection. The second point is that ChannelFly can be enabled per band – 2.4GHz or 5GHz (or both).

ChannelFly can take some time to effectively analyze the environment, and it’s not suitable for every environment. If you want to utilize ChannelFly, you should ensure you leave enough time for the system to settle, and that you monitor network performance to ensure that the client experience is not affected adversely.



SmartZone AP Groups



Access Point Group Configuration Process

1. Create an AP Group
2. Configure AP group unique settings
3. Move APs to the new group
4. APs adopt group settings

Access point groups can be used to define configuration options and apply them to groups of APs at once, without having to individually modify each AP's settings.

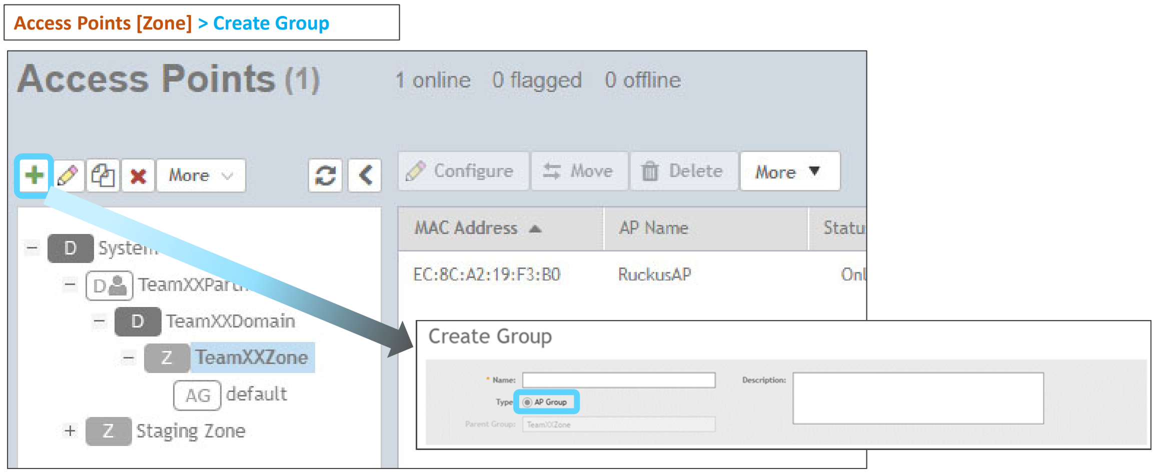
For each group, administrators can create a configuration that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

Access Points adopt the settings of the zone and the group to which they belong. Without any other consideration, this is the Default Access point Group.

In order to apply different custom settings to a group of APs within the zone you can use custom Access Point Groups.
The process to of creating and using custom Access Point Groups is as follows:

1. Create the custom AP Group
2. Configure the custom settings
3. Move the Access Points to the new group
4. The Access Points adopt the group settings of the group

Create an AP Group



MAC Address	AP Name	Statu
EC:8C:A2:19:F3:B0	RuckusAP	Onl

Create Group

* Name:

Description:

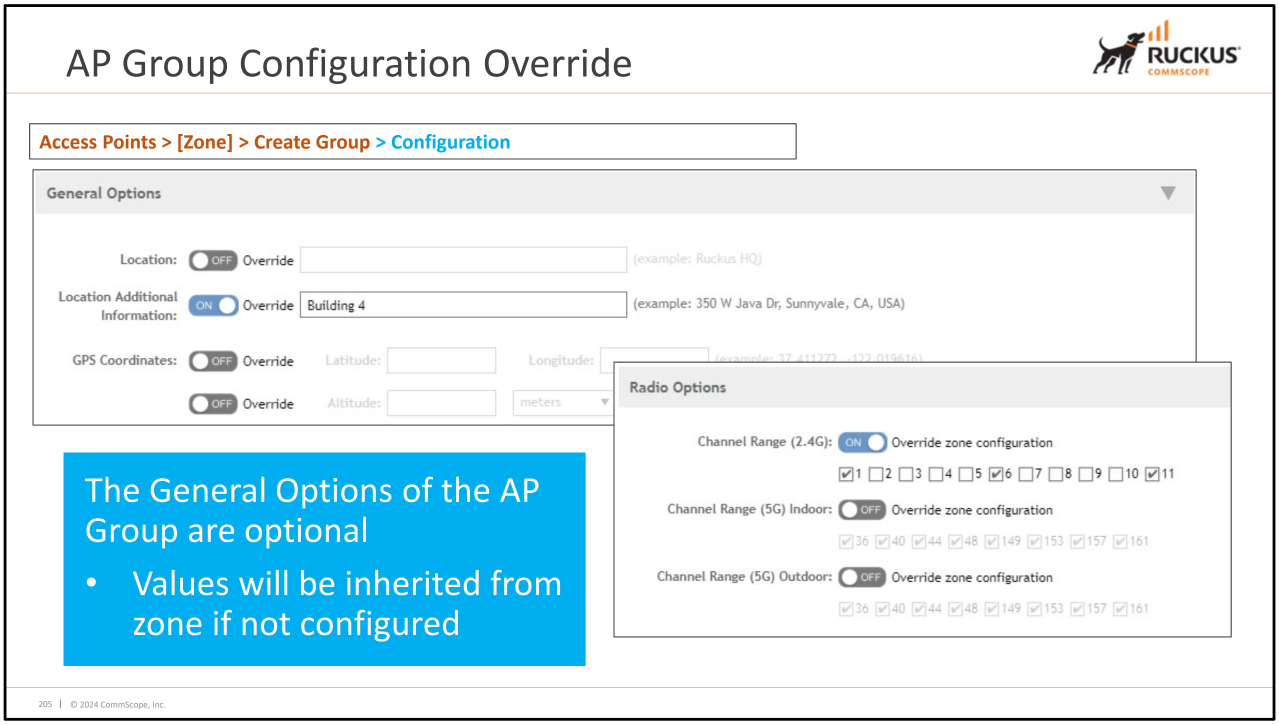
Type ● AP Group

Parent Group: TeamXXZone

AP Groups are managed in the same location as the Domains and Zones. To create a new AP Group, select the Domain and Zone from the **System** list, and select the **add (+)** button.

Start by entering a name for the group. Notice that under **Type**, the **AP Group** is selected. Once you enter these settings you'll move forward to the group configuration options.

The AP Group being created will inherit settings from the Zone that it is created in. This administratively created AP group has the ability to override the Zone settings.



AP Group Configuration Override

Access Points > [Zone] > Create Group > Configuration

General Options

Location: OFF Override (example: Ruckus HQ)

Location Additional Information: ON Override Building 4 (example: 350 W Java Dr, Sunnyvale, CA, USA)

GPS Coordinates: OFF Override Latitude: Longitude: (example: 37.411272, -122.019616)

OFF Override Altitude: meters

Radio Options

Channel Range (2.4G): ON Override zone configuration

☑1 □2 □3 □4 □5 ☑6 □7 □8 □9 □10 ☑11

Channel Range (5G) Indoor: OFF Override zone configuration

☑36 ☑40 ☑44 ☑48 ☑149 ☑153 ☑157 ☑161

Channel Range (5G) Outdoor: OFF Override zone configuration

☑36 ☑40 ☑44 ☑48 ☑149 ☑153 ☑157 ☑161

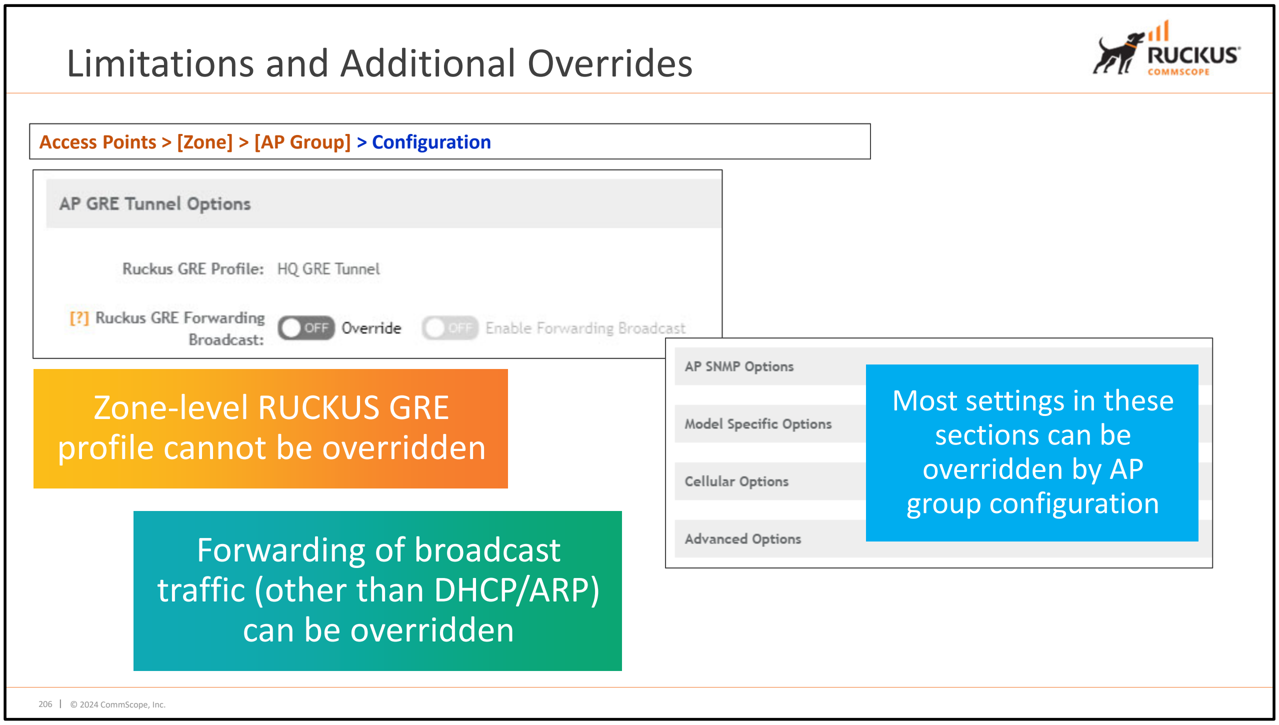
The General Options of the AP Group are optional

- Values will be inherited from zone if not configured

205 | © 2024 CommScope, Inc.

A newly created AP group inherits settings from the zone configuration but these can be overridden for specific settings you wish to change. Sliding the **Override** selector to “On” allows you to modify the field. This applies to all available configuration options.

In the example here, Location Additional Information setting is configured to override the Zone configuration for the same setting and applies it only to APs in this group. As another example, you can override the zone radio settings for each radio type.



Limitations and Additional Overrides

Access Points > [Zone] > [AP Group] > Configuration

AP GRE Tunnel Options

Ruckus GRE Profile: HQ GRE Tunnel

[?] Ruckus GRE Forwarding Broadcast: OFF Override OFF Enable Forwarding Broadcast

Zone-level RUCKUS GRE profile cannot be overridden

Forwarding of broadcast traffic (other than DHCP/ARP) can be overridden

AP SNMP Options

Model Specific Options

Cellular Options

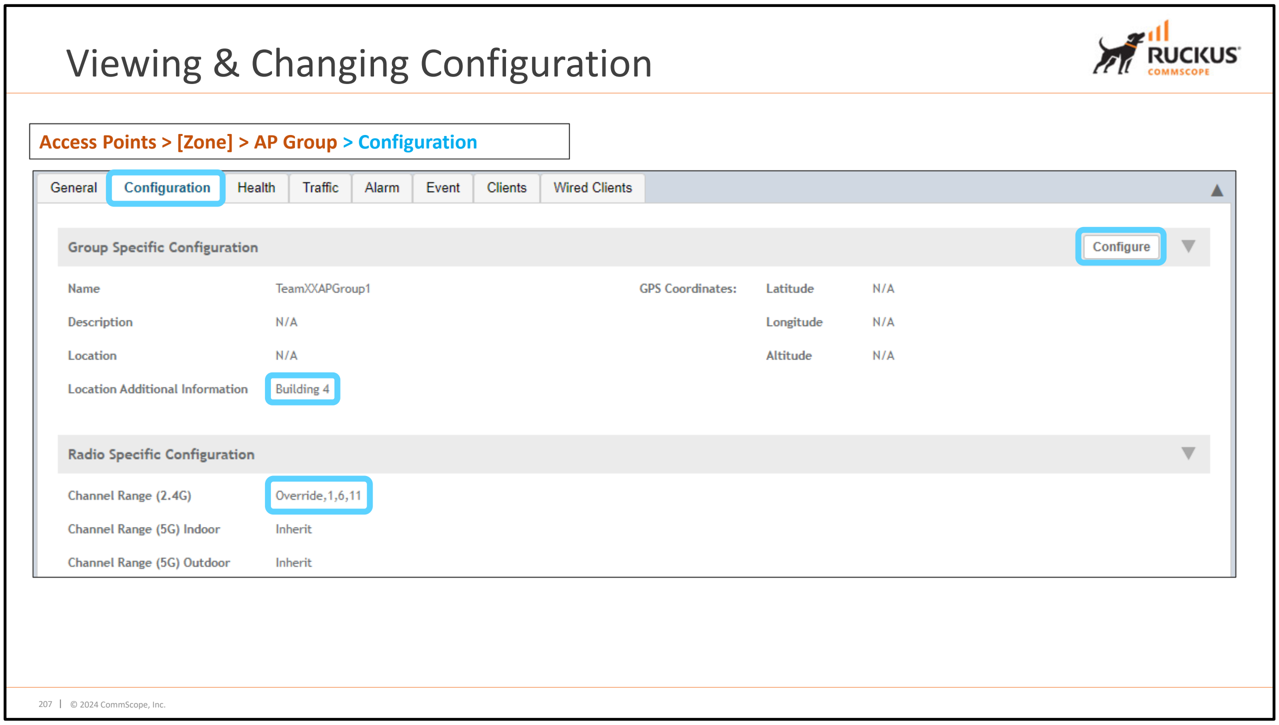
Advanced Options

Most settings in these sections can be overridden by AP group configuration

206 | © 2024 CommScope, Inc.

In the AP GRE Tunnel configuration section, RUCKUS GRE tunnel profiles are inherited from the zone and cannot be overridden in an AP group. However, an override by the AP group can effect the broadcast traffic other than ARP and DHCP from being forwarded.

In the remaining configurations sections of an AP group can have the inherited zone configuration overridden through the standard process of toggling the Override switch and adjusting the configuration option to the desired setting.



Viewing & Changing Configuration

Access Points > [Zone] > AP Group > Configuration

Group Specific Configuration

Name	TeamXXAPGroup1	GPS Coordinates:	Latitude	N/A
Description	N/A		Longitude	N/A
Location	N/A		Altitude	N/A
Location Additional Information	Building 4			

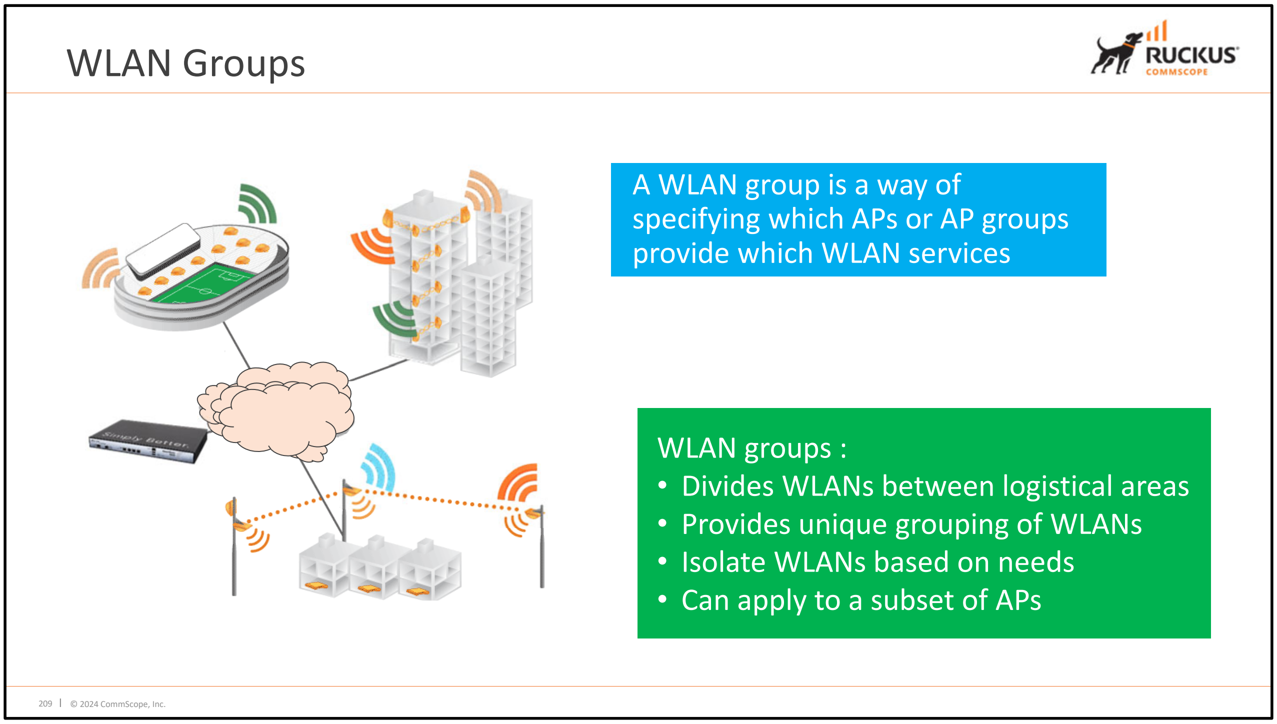
Radio Specific Configuration

Channel Range (2.4G)	Override,1,6,11
Channel Range (5G) Indoor	Inherit
Channel Range (5G) Outdoor	Inherit

207 | © 2024 CommScope, Inc.

Once AP Group settings have been made, you can highlight the AP group, and select the **Configuration** tab to view the settings. Configuration that was set in the AP group overrides the zone configuration and is reflected on the Configuration tab. To make further changes to the AP group, select the **Configure** button.

SmartZone WLAN Groups



WLAN Groups

A WLAN group is a way of specifying which APs or AP groups provide which WLAN services

WLAN groups :

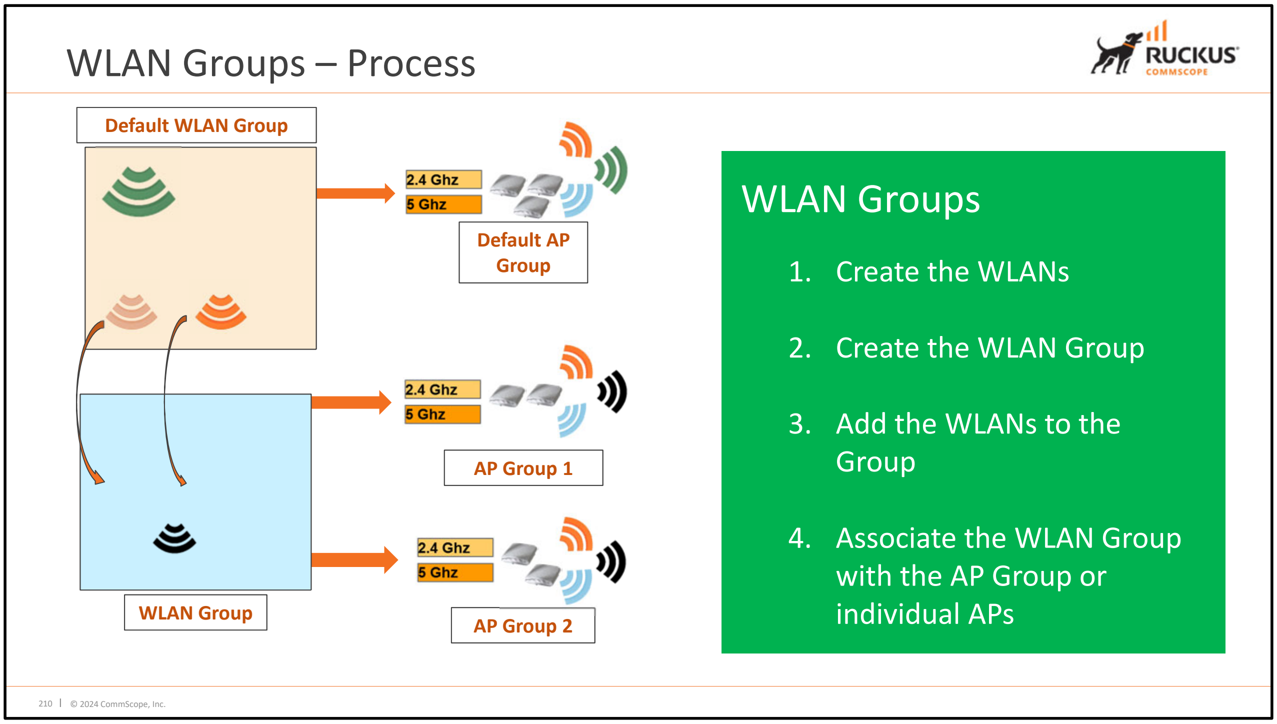
- Divides WLANs between logistical areas
- Provides unique grouping of WLANs
- Isolate WLANs based on needs
- Can apply to a subset of APs

209 | © 2024 CommScope, Inc.

While AP groups provide foundational functions and features of its AP members WLAN groups provide the SSIDs the APs will service. With WLAN groups APs can be divided up into groupings of SSIDs based on their logistical area, isolation WLANs or even “one off” WLAN requirements. With WLAN groups you can uniquely place WLAN broadcasts in their needed places while minimizing WLAN reach.

Examples: ALL APs within the stadium can have similar configuration (AP Groups) however different areas would have unique WLAN requirements. In the stands would not need a vendor SSID but the corridors would. Putting the vendor SSID in a separate WLAN group then associating it with the appropriate APs provide effective means of SSID isolation.

As for the building you might want to provide a visitor SSID in the lobby but would not need it in the upper floors. Possible vendors in the bottom floor also could have their SSID only broadcast in their area but not in the rest of the building. Cameras or other devices that only reside a few places within the building could be served as well by associating the APs in their proximity with a WLAN group that contains their required SSIDs.



WLAN Groups – Process

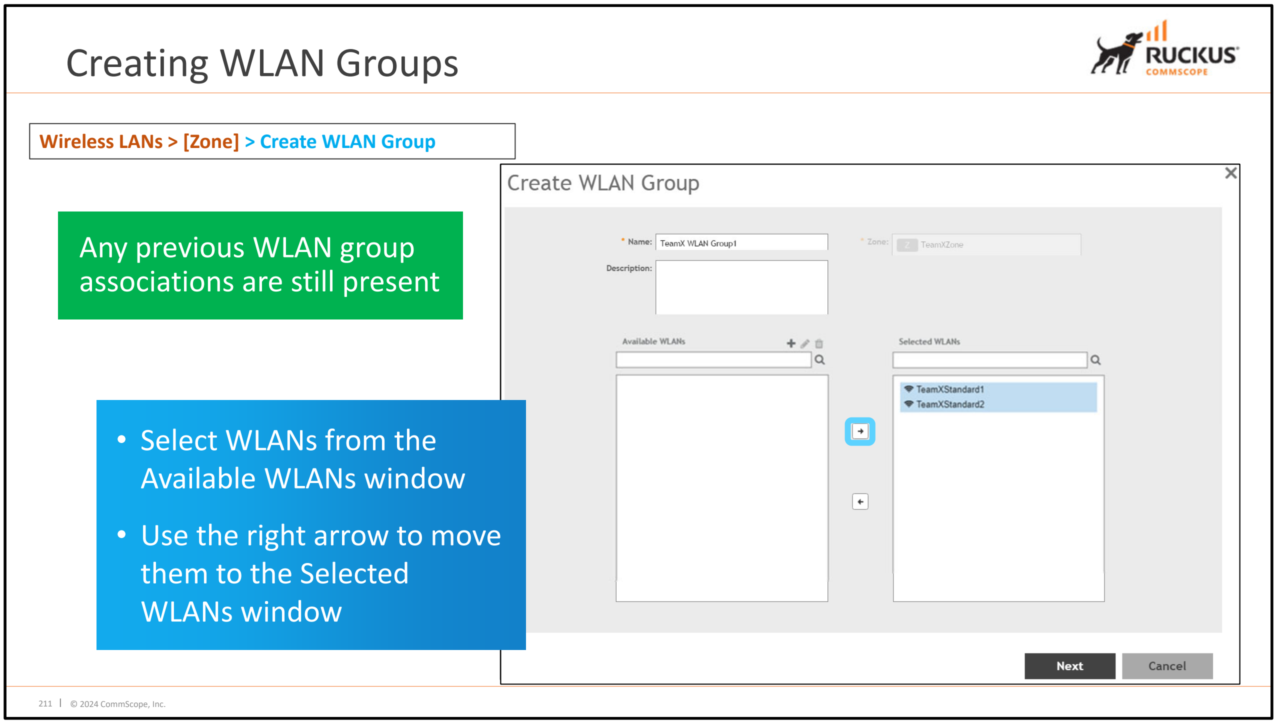
WLAN Groups

1. Create the WLANs
2. Create the WLAN Group
3. Add the WLANs to the Group
4. Associate the WLAN Group with the AP Group or individual APs

210 | © 2024 CommScope, Inc.

The process for creating WLAN Groups is similar to that for Access Point Groups. However, unlike Access Points, which can only belong to a single AP group, WLANs can be a member of more than one WLAN group.

You first need to create your WLANs which has already been discussed. Next, create a new WLAN Group and add the preferred WLANs to that WLAN Group. The final step is to apply the WLAN group to a AP group or to individual APs radios.



Creating WLAN Groups

Wireless LANs > [Zone] > Create WLAN Group

Any previous WLAN group associations are still present

- Select WLANs from the Available WLANs window
- Use the right arrow to move them to the Selected WLANs window

Create WLAN Group

* Name: TeamX WLAN Group1

* Zone: TeamXZone

Description:

Available WLANs

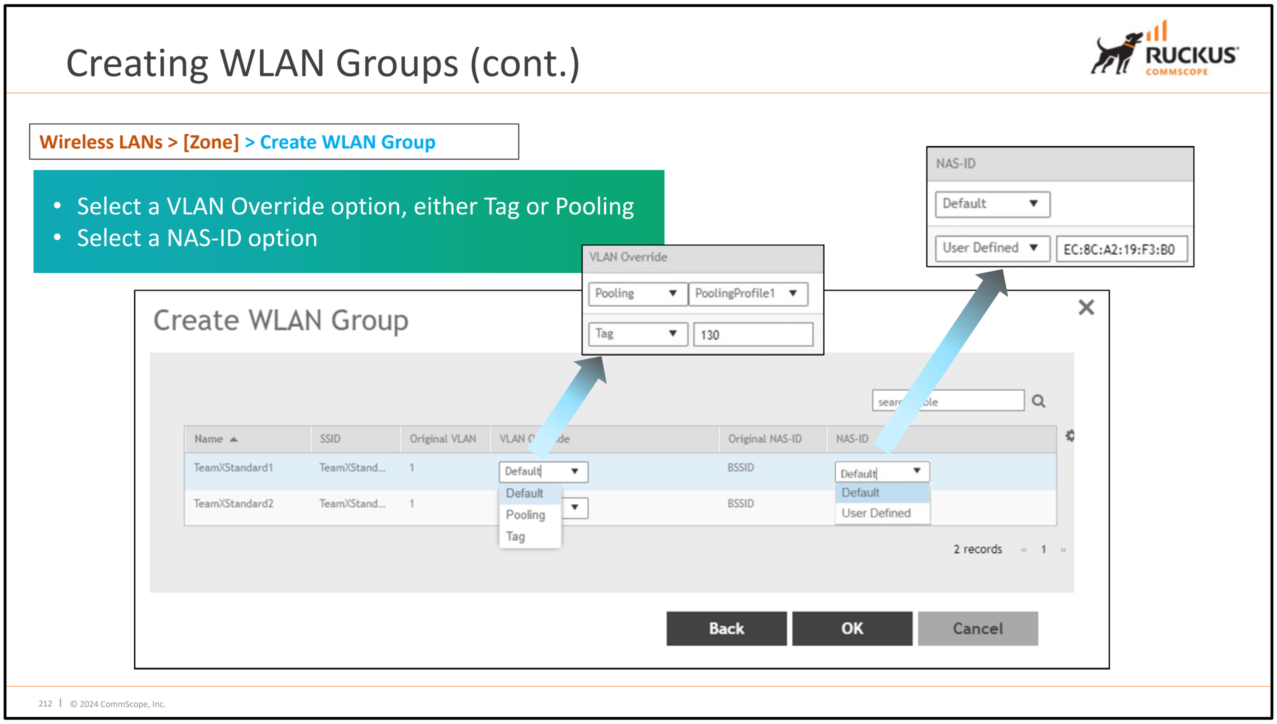
Selected WLANs

TeamXStandard1
TeamXStandard2

211 | © 2024 CommScope, Inc.

Once the WLAN group page opens, name the WLAN Group and select the desired WLANs from the **Available WLANs** window on the left. Use the **arrow** to move the highlighted WLANs to the **Selected WLANs** window and then press Next.

Remember, WLANs can be part of multiple WLAN Groups. Previously created WLANs that you have added to your new named group are still members of the Default WLAN Group. You have to manually remove them from the Default WLAN Group if you want them to only be in your new group.



Creating WLAN Groups (cont.)

Wireless LANs > [Zone] > Create WLAN Group

- Select a VLAN Override option, either Tag or Pooling
- Select a NAS-ID option

Create WLAN Group

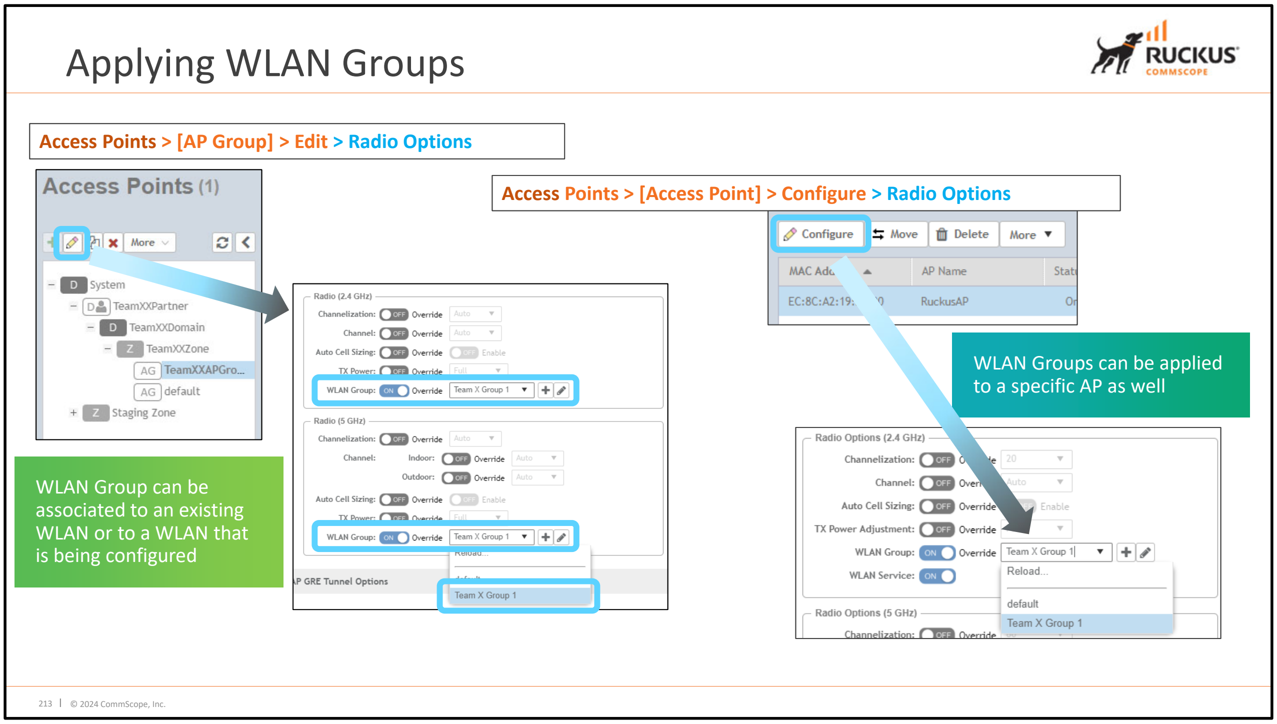
Name	SSID	Original VLAN	VLAN Override	Original NAS-ID	NAS-ID
TeamXStandard1	TeamXStand...	1	Default	BSSID	Default
TeamXStandard2	TeamXStand...	1		BSSID	

2 records

VLAN Override: Pooling, PoolingProfile1; Tag, 130

NAS-ID: Default; User Defined, EC:8C:A2:19:F3:B0

The next options include VLAN override and NAS ID options that apply only to this WLAN group. VLAN override provides options to either use the default value assigned to the WLAN itself, associate a VLAN pool profile (which you will learn about next) or simply assign a VLAN tag for the clients to be assigned to, which will be different then the default VLAN tag of the WLAN. The NAS ID allows you to set a value for the AP to communicate with the RADIUS server. Options include using the AP MAC address or any User-defined address to allow the RADIUS server to identify the request source.



Applying WLAN Groups

Access Points > [AP Group] > Edit > Radio Options

Access Points > [Access Point] > Configure > Radio Options

WLAN Group can be associated to an existing WLAN or to a WLAN that is being configured

WLAN Groups can be applied to a specific AP as well

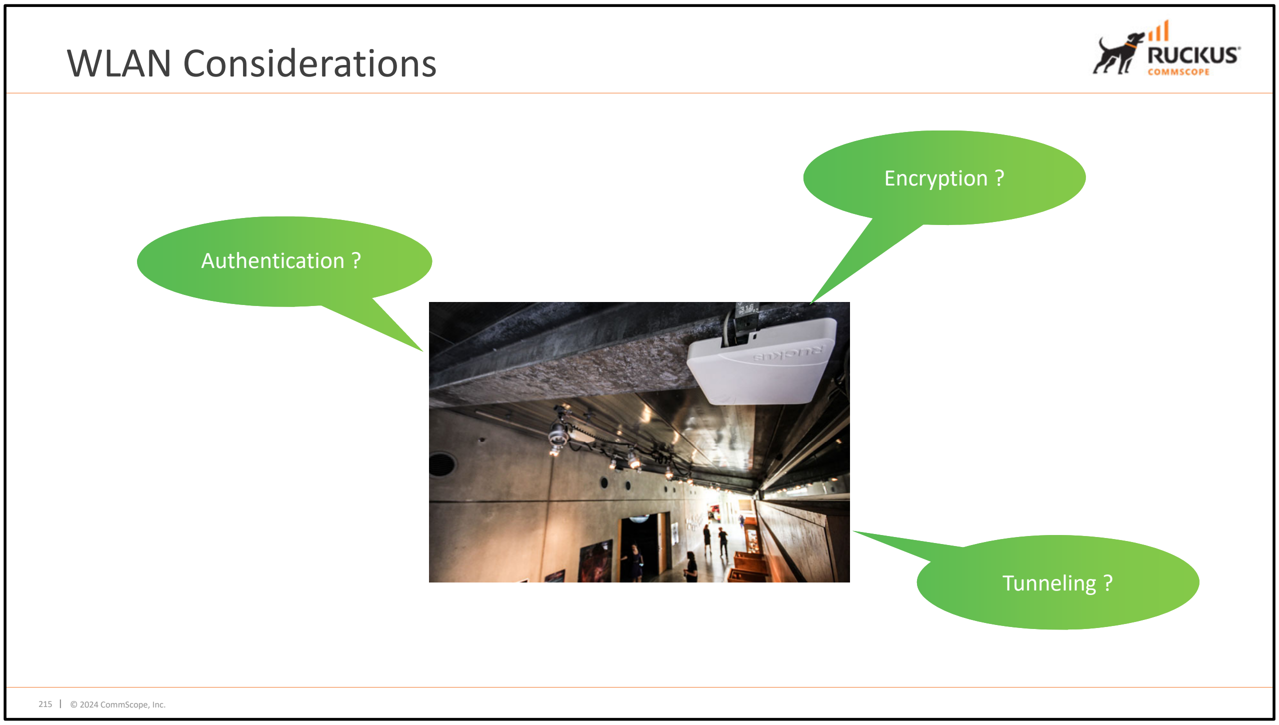
Access Points (1)
More
System
TeamXXPartner
TeamXXDomain
TeamXXZone
TeamXXAPGro...
default
Staging Zone
Radio (2.4 GHz)
Channelization: OFF Override Auto
Channel: OFF Override Auto
Auto Cell Sizing: OFF Override OFF Enable
TX Power: OFF Override Full
WLAN Group: ON Override Team X Group 1
Radio (5 GHz)
Channelization: OFF Override Auto
Channel: Indoor: OFF Override Auto
Outdoor: OFF Override Auto
Auto Cell Sizing: OFF Override OFF Enable
TX Power: OFF Override Full
WLAN Group: ON Override Team X Group 1
Reload...
default
Team X Group 1
AP GRE Tunnel Options
Configure
Move
Delete
More
MAC Add...
AP Name
Stat...
EC:8C:A2:19:...
RuckusAP
Radio Options (2.4 GHz)
Channelization: OFF Override 20
Channel: OFF Override Auto
Auto Cell Sizing: OFF Override Enable
TX Power Adjustment: OFF Override
WLAN Group: ON Override Team X Group 1
WLAN Service: ON
Reload...
default
Team X Group 1
Radio Options (5 GHz)
Channelization: OFF Override
RUCKUS
COMMSCOPE

213 | © 2024 CommScope, Inc.

You can apply a WLAN Group to an Access Point Group, either when you create the AP Group or later by editing the AP Group. Under the AP Group, enable the **Override zone configuration** option, then select the WLAN Group to be applied to this AP Group. You'll need to do this for each radio, so be sure to configure both 2.4GHz and 5GHz which can both match or be members of different WLAN groups.

If a WLAN Group hasn't been created yet, you can do that now by clicking the **+** sign.
A WLAN group can be applied to a specific AP as well as its specific radios. This is effective when you might have an isolated location that is the only place a WLAN needs to be broadcast.

Configuring Wireless LANs



WLAN Considerations

Authentication ?

Encryption ?

Tunneling ?

215 |

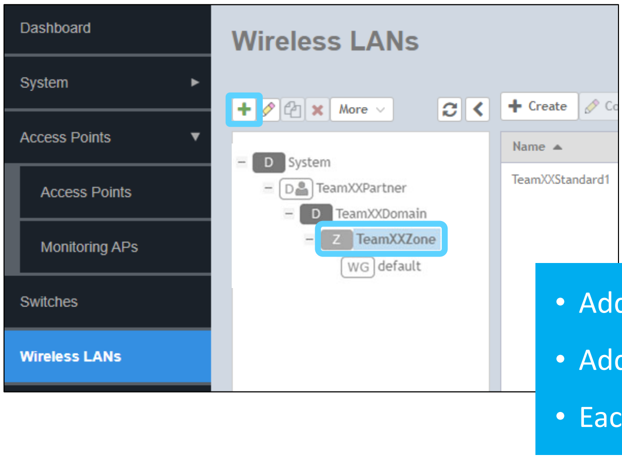
Before setting up WLANs, you need to consider some of the things that will impact WLAN operations.

- How will users authenticate?
- What type of encryption should be offered?
- Should traffic be tunneled?

This list is by no means complete. However, it provides a good starting point for the kind of things you need to consider.

Wireless LANs

Wireless LANs > [Zone] > Wireless LANs

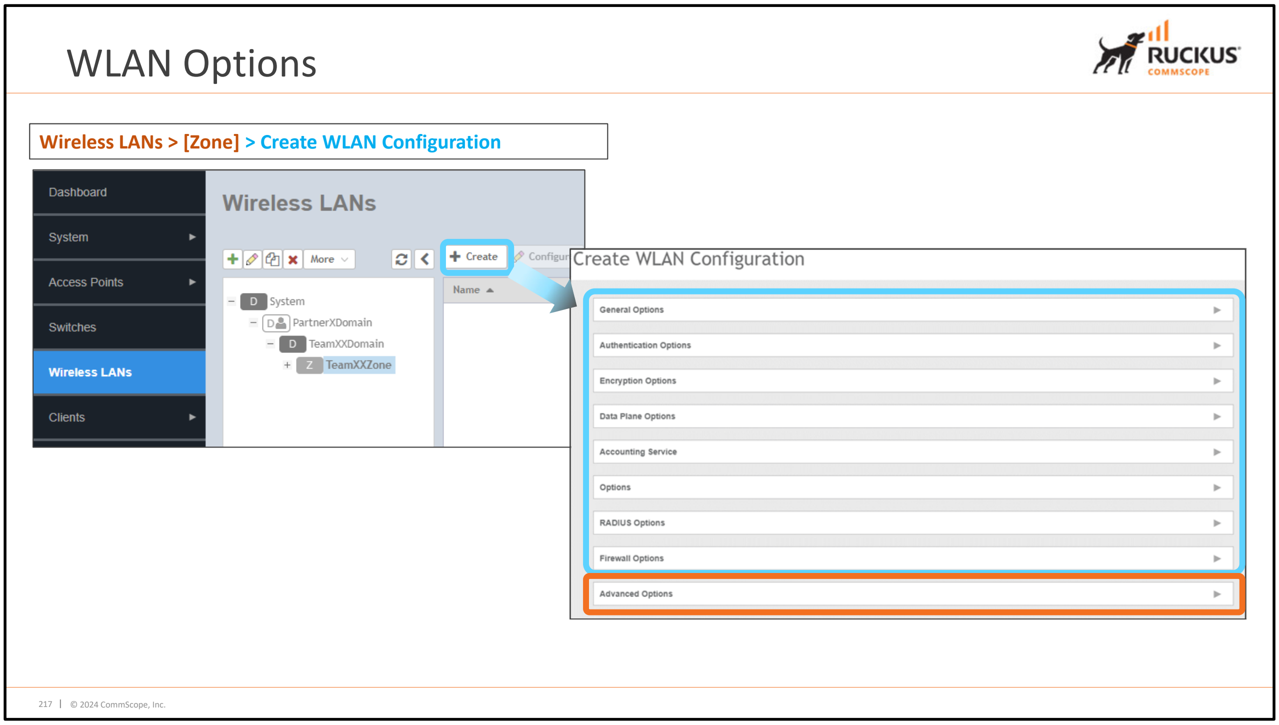


- Add a WLAN Group using the add (+) icon
- Add WLAN Groups at the Zone level
- Each Zone has a default WLAN group (WG)

216 | © 2024 CommScope, Inc.

You can create a WLAN by selecting a Zone where you would like to create the WLAN Group and **add (+)** icon. Each zone has a default group that any WLANs created will be placed in unless a custom group is created and selected at the time of the WLAN creation.

Once custom WLAN groups are created WLANs can be placed in both the default and the custom WLAN group or can be exclusively placed in the custom group or vice versa. WLAN Groups relate to WLANs so they must be created at the Zone level. A WLAN Group can include a maximum of 27 member WLANs. For dual radio APs, each radio can be assigned to only one WLAN Group (single radio APs can be assigned to only one WLAN Group).

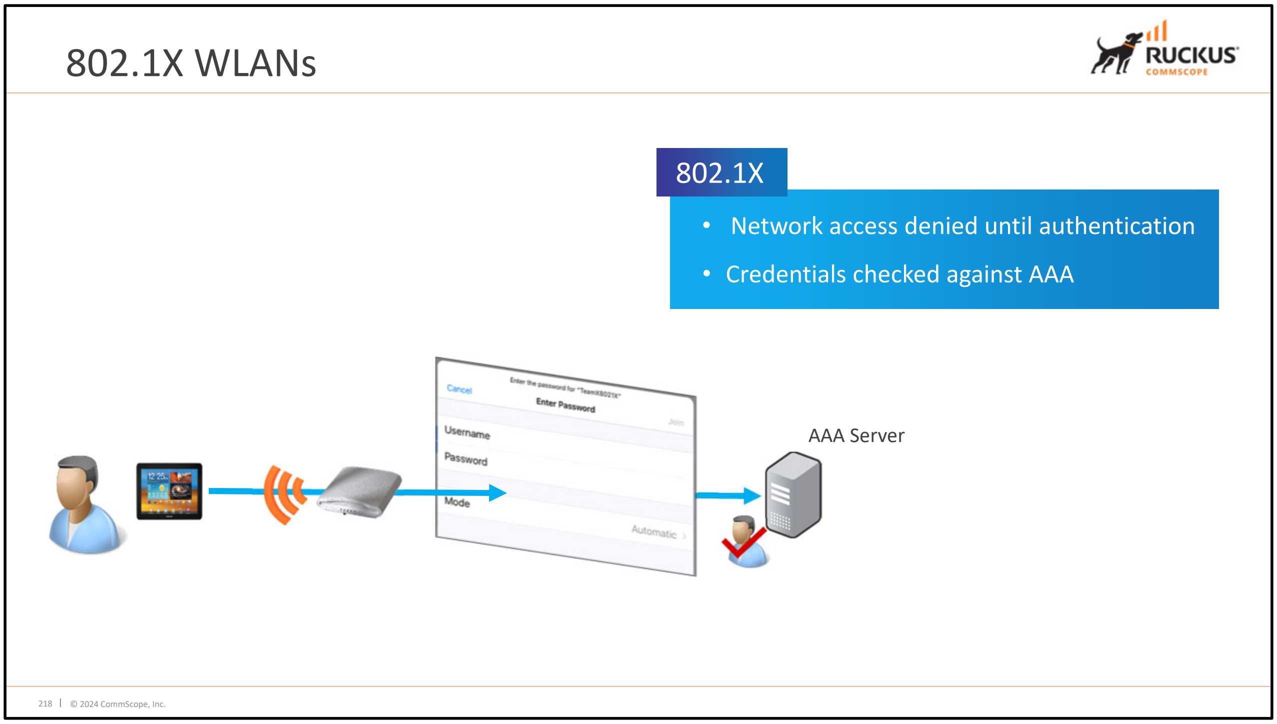


WLAN Options

Wireless LANs > [Zone] > Create WLAN Configuration

217 | © 2024 CommScope, Inc.

Once the zone is selected click create to start configuring your wireless LAN
When creating a new WLAN, you will perform configuration tasks in two major areas – A collection of general settings, and the **Advanced Options**.



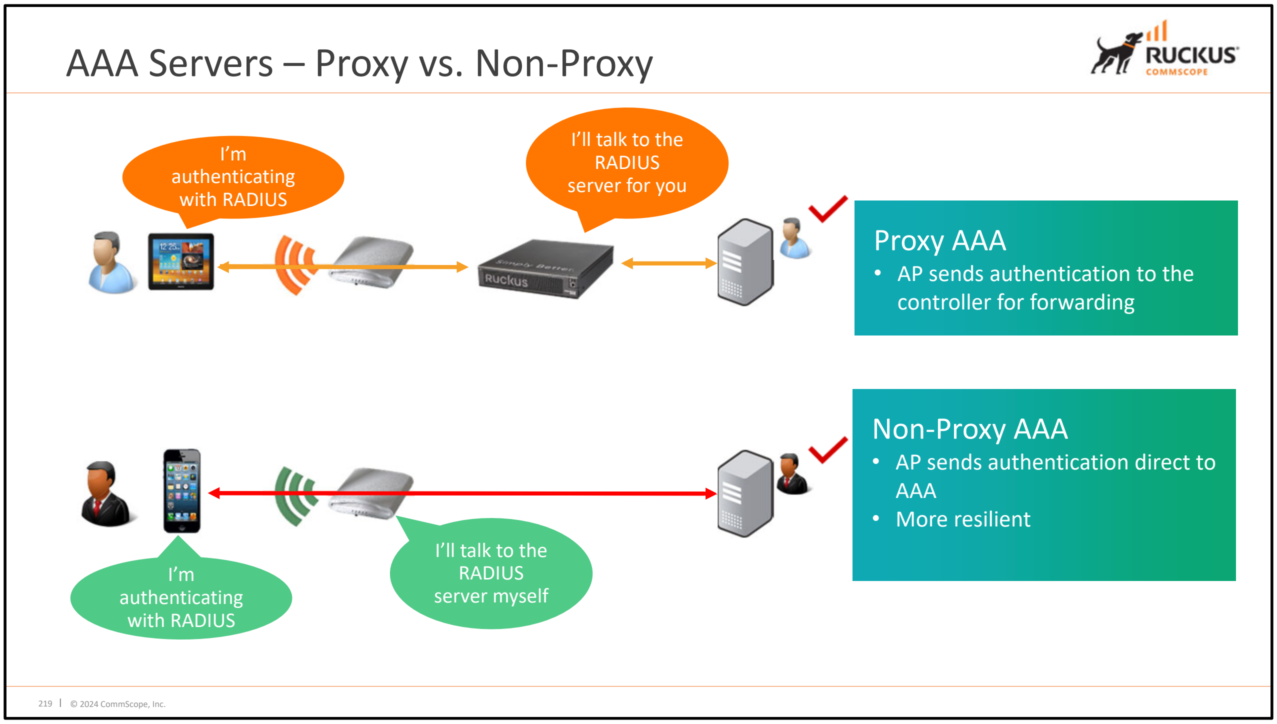
802.1X WLANs

802.1X

- Network access denied until authentication
- Credentials checked against AAA

218 | © 2024 CommScope, Inc.

In order to use 802.1X, you'll need a supporting authentication server.
When the user attempts to gain access to the network they are prompted to enter a username and password, at which point the AAA server checks these credentials against its database. If it finds a matching account and the password is correct, the user can continue their connection.



AAA Servers – Proxy vs. Non-Proxy

I'm authenticating with RADIUS

I'll talk to the RADIUS server for you

Proxy AAA

- AP sends authentication to the controller for forwarding

Non-Proxy AAA

- AP sends authentication direct to AAA
- More resilient

I'm authenticating with RADIUS

I'll talk to the RADIUS server myself

219 | © 2024 CommScope, Inc.

In order to understand the AAA services available to SmartZone controllers, you need to understand the difference between Proxy and Non-Proxy AAA Authentication.

With Proxy AAA, the authentication is managed from the controller and the controller communicates with the AAA server. In the example shown a wireless user authenticating via RADIUS with Proxy enabled will send it's request to the SmartZone controller who will in turn send the request on to the authentication server. The success or failure of the authentication is then sent from the authentication server to the SmartZone and back through the AP to the client.

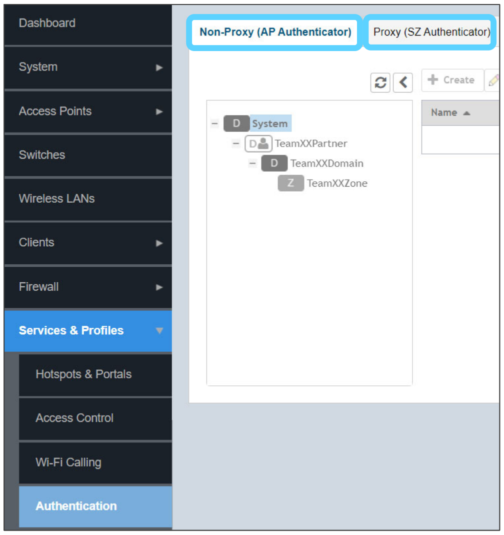
With Non-Proxy AAA, the authentication is managed between the Access Point and the AAA server directly; the controller is not part of the authentication process.

Creating AAA Servers

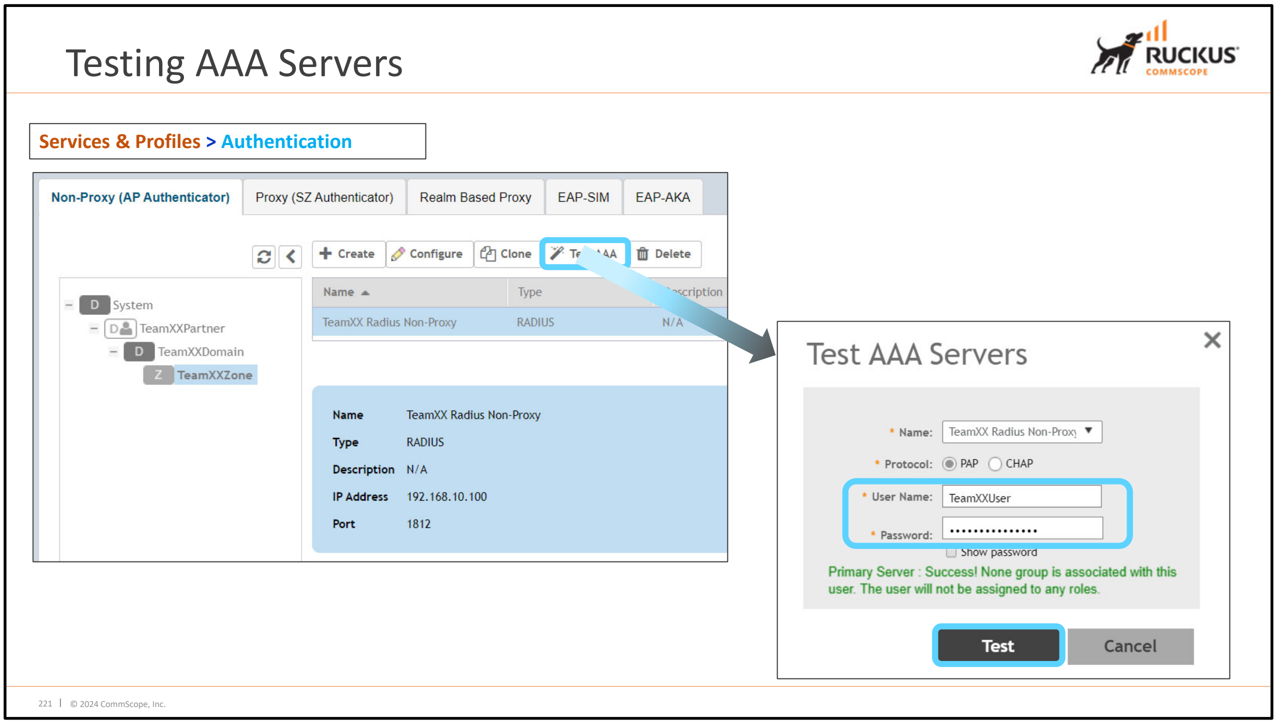
Services & Profiles > Authentication

Proxy and Non-Proxy AAA Servers provide user authentication:

- RADIUS
- Active Directory
- Lightweight Directory Access Protocol (LDAP)



Proxy and Non-Proxy servers are configured under **Services & Profiles > Authentication**. The servers provide user authentication using RADIUS, Active Directory and LDAP.



Testing AAA Servers

Services & Profiles > Authentication

Name	Type	Description
TeamXX Radius Non-Proxy	RADIUS	N/A

Name TeamXX Radius Non-Proxy
Type RADIUS
Description N/A
IP Address 192.168.10.100
Port 1812

Test AAA Servers

* Name: TeamXX Radius Non-Proxy
* Protocol: ● PAP ○ CHAP
* User Name: TeamXXUser
* Password: •••••••••••••••
□ Show password

Primary Server : Success! None group is associated with this user. The user will not be assigned to any roles.

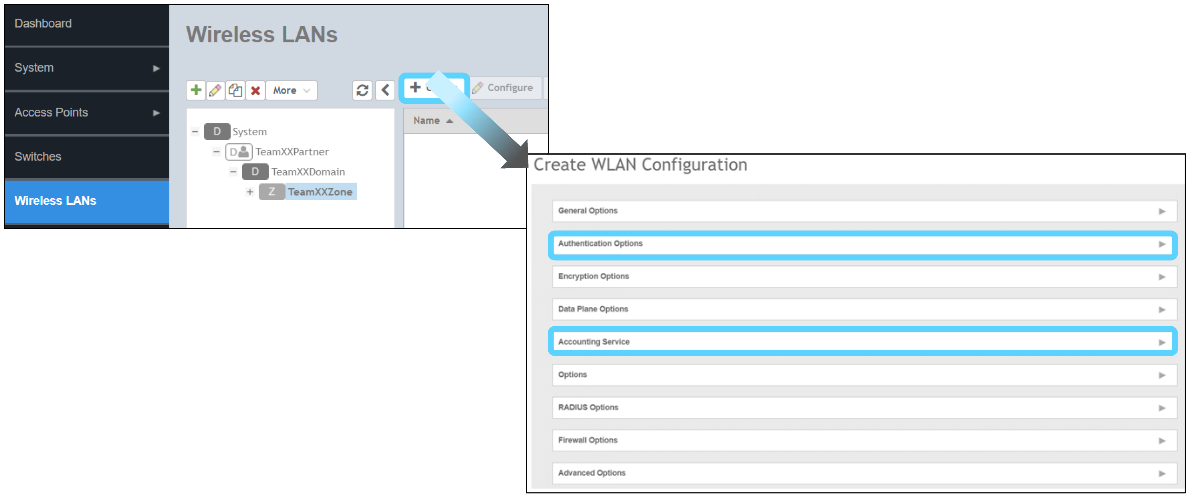
221 | © 2024 CommScope, Inc.

You can test communication to the AAA servers by selecting either a Non-Proxy or Proxy AAA server and selecting Test AAA.
 Provide credentials for the account you would like to validate and select the TEST button. A message indicating success or failure will appear within the test window

For Non-Proxy AAA, remember that this specific test is made directly from the controller to the AAA server. A successful test from the controller is not a guarantee that the Access Point will be able to connect successfully.
For Proxy AAA, you're testing from the controller itself, and if all is well, you should expect to see a Success message and clients should be able to authenticate
To fully test, you need to authenticate from a device connected to an Access Point.

Creating an 802.1X WLAN

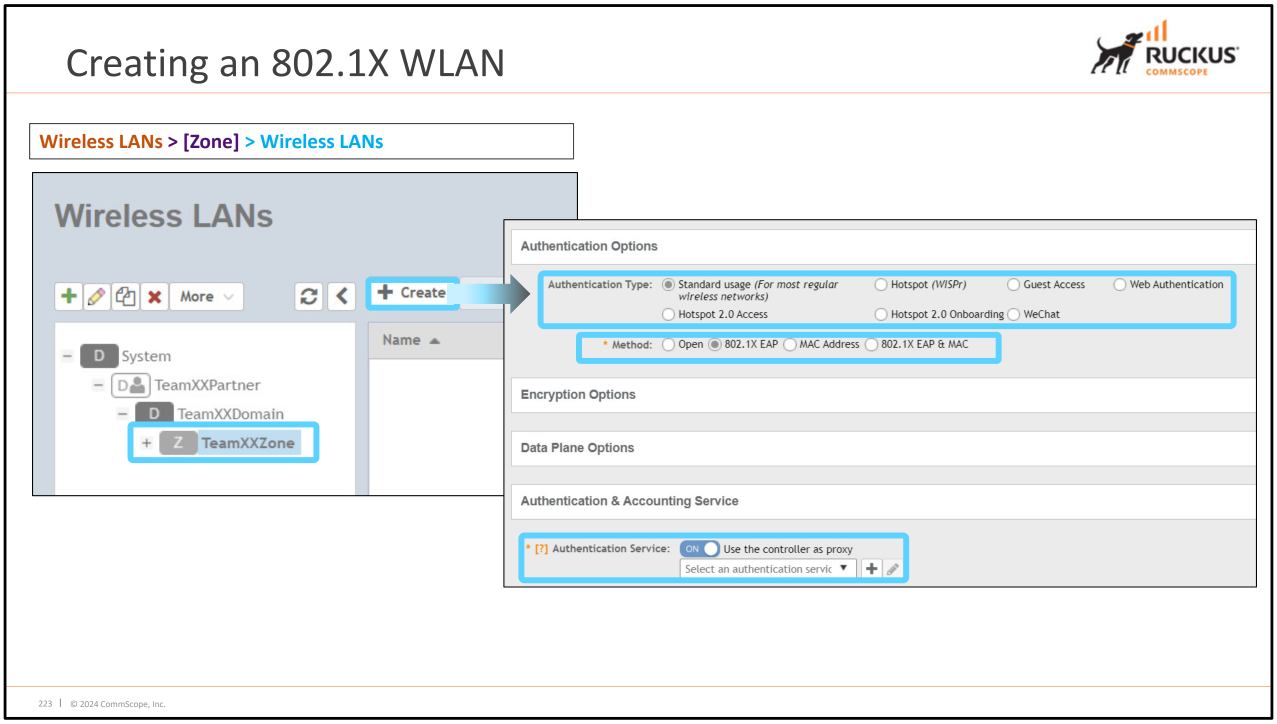
Wireless LANs > Create WLAN Configuration



222 | © 2024 CommScope, Inc.

You learned previously that when creating a new WLAN, you will perform configuration tasks in two major areas – a collection of general settings, and the Advanced Options.

When creating a new 802.1X authenticated WLAN, the configurable parameters necessary are under the Authentication Options as well as Accounting Services sections. We'll look at those now.



Creating an 802.1X WLAN

Wireless LANs > [Zone] > Wireless LANs

Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ○ Open ● 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

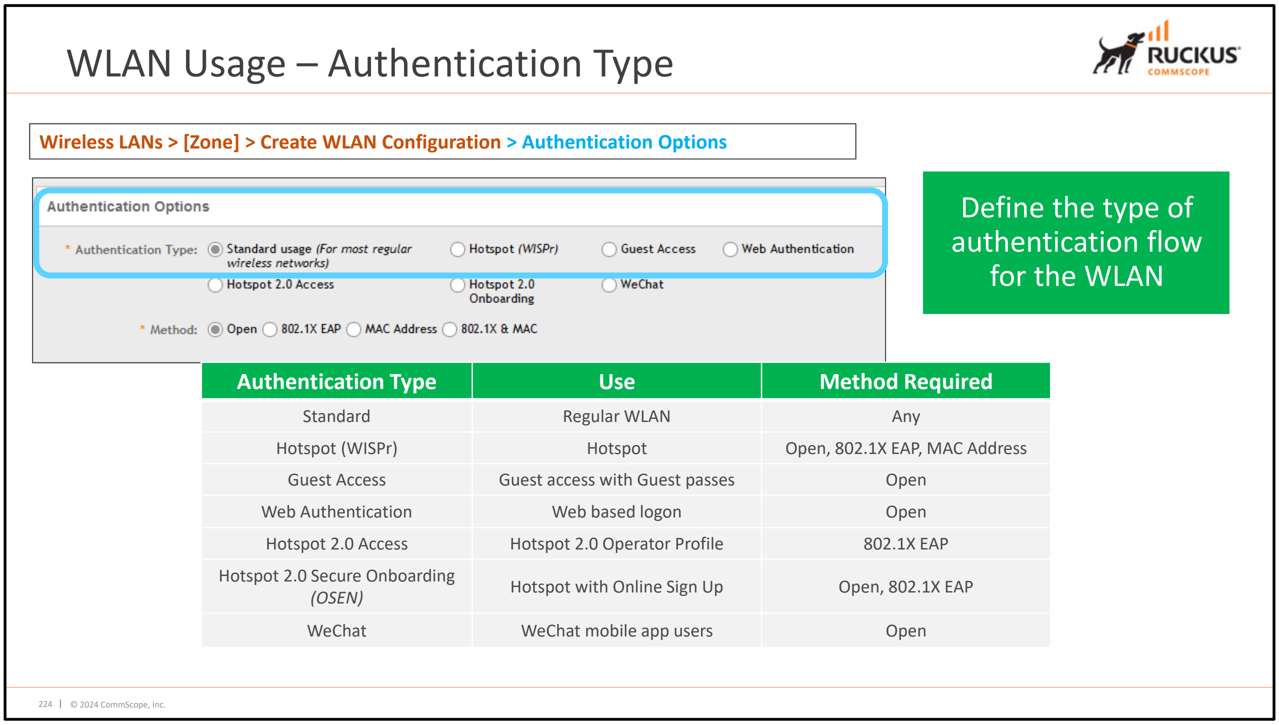
* [?] Authentication Service: ON Use the controller as proxy

Select an authentication servic ▼

Begin by selecting the Zone where you would like to your define your 802.1X WLAN and click **Create**.

When configuring an 802.1XWLAN, use the following settings:

- **Authentication Type**: Standard usage
- **Method**: 802.1X EAP
- **Authentication and Accounting Server**: select Use the controller as Proxy when configuring for Proxy AAA, or deselect if using a Non-Proxy AAA service.
- Select the server name from the drop-down list.
  If a server does not exist you can configure one here by clicking the +



WLAN Usage – Authentication Type

Wireless LANs > [Zone] > Create WLAN Configuration > Authentication Options

Authentication Options

* Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ● Open ○ 802.1X EAP ○ MAC Address ○ 802.1X & MAC

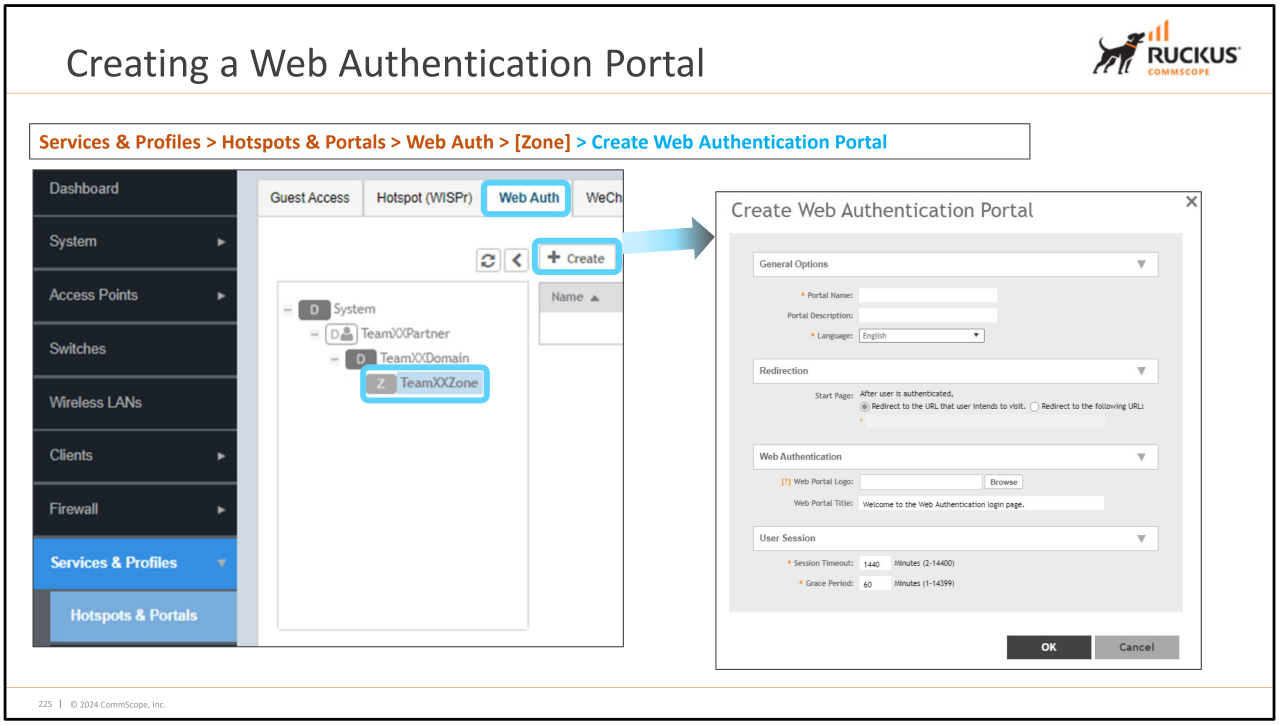
Define the type of authentication flow for the WLAN

Authentication Type	Use	Method Required
Standard	Regular WLAN	Any
Hotspot (WISPr)	Hotspot	Open, 802.1X EAP, MAC Address
Guest Access	Guest access with Guest passes	Open
Web Authentication	Web based logon	Open
Hotspot 2.0 Access	Hotspot 2.0 Operator Profile	802.1X EAP
Hotspot 2.0 Secure Onboarding *(OSEN)*	Hotspot with Online Sign Up	Open, 802.1X EAP
WeChat	WeChat mobile app users	Open

224 |

When it comes to authentication, you have several options on how the user can identify themselves. We will concentrate on the first 4 methods that include:

- **Standard WLANs** – regular WLANs where the user is usually pre-identified by either their MAC or possibly a pre-shared key (PSK)
- **Hotpot (WISPr)** – Hotspot with authentication provides the ability for a onboarding user to be limited in their access until they are able to authenticate by an onboarding system such as Cloudpath. Once they are registered their access limitations (walled garden) is lifted.
- **Guest Access** – Guest access WLANs provide the ability to authenticate guests by the process of redirecting them to enter a Guest Access Portal where either guest passes were issued prior to their connection attempt or they can provide other means of identification such as SMS .
- **Web Authentication** – Unlike Guess Access Web Authentication provides a web based login to allow pre-defined users to authenticate using username/password process.



Creating a Web Authentication Portal

Services & Profiles > Hotspots & Portals > Web Auth > [Zone] > Create Web Authentication Portal

Create Web Authentication Portal

General Options

* Portal Name:

Portal Description:

* Language: English

Redirection

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit. ○ Redirect to the following URL:

Web Authentication

[?] Web Portal Logo: Browse

Web Portal Title: Welcome to the Web Authentication login page.

User Session

* Session Timeout: 1440 Minutes (2-14400)

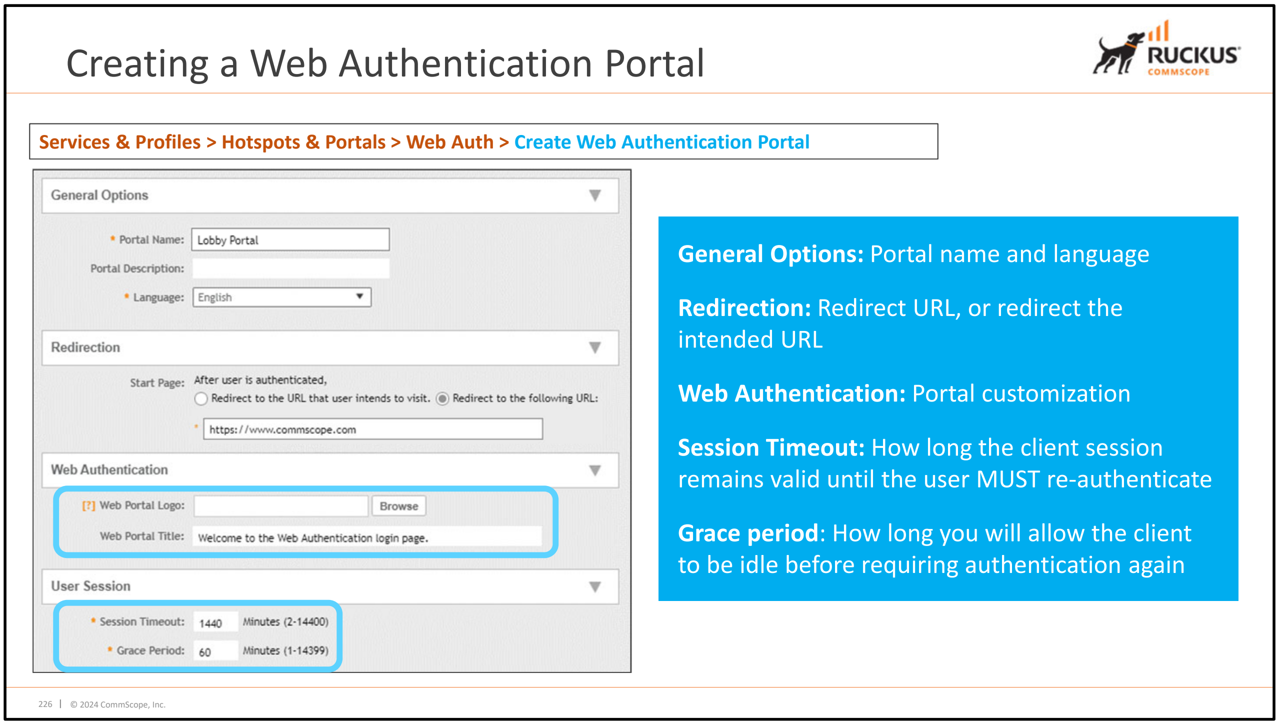
* Grace Period: 60 Minutes (1-14399)

OK Cancel

225 | © 2024 CommScope, Inc.

To create a Web Authentication portal, begin under **Services and Profiles > Hotspots and Portals**, and ensure the **Web Auth** tab is selected.
Web Authentication Portals are created at the Zone level so select the specific zone you intend to implement the Web Authorization portal. Once the Zone is selected select **Create**.

Web Auth portals will need to be created in each zone that requires Web Auth services.



Creating a Web Authentication Portal

Services & Profiles > Hotspots & Portals > Web Auth > Create Web Authentication Portal

General Options

* Portal Name: Lobby Portal
Portal Description:
* Language: English

Redirection

Start Page: After user is authenticated,
○ Redirect to the URL that user intends to visit. ● Redirect to the following URL:
* https://www.commscope.com

Web Authentication

[?] Web Portal Logo: Browse
Web Portal Title: Welcome to the Web Authentication login page.

User Session

* Session Timeout: 1440 Minutes (2-14400)
* Grace Period: 60 Minutes (1-14399)

General Options: Portal name and language

Redirection: Redirect URL, or redirect the intended URL

Web Authentication: Portal customization

Session Timeout: How long the client session remains valid until the user MUST re-authenticate

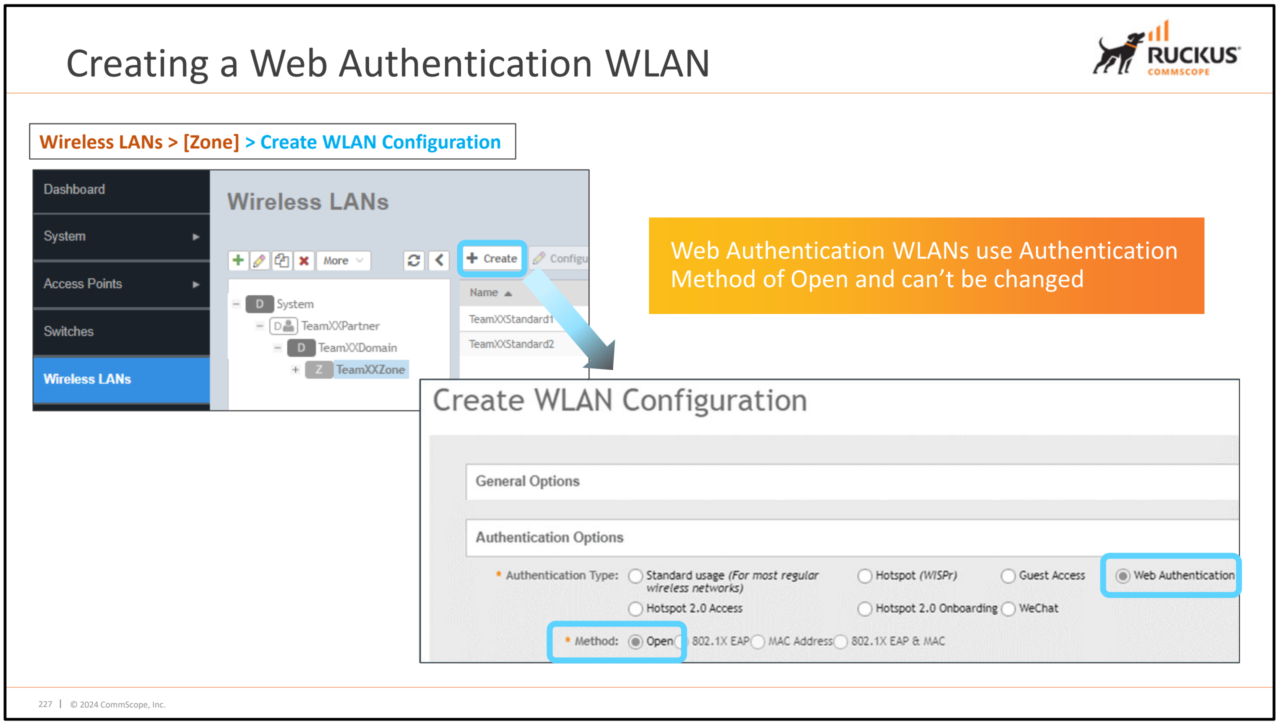
Grace period: How long you will allow the client to be idle before requiring authentication again

226 | © 2024 CommScope, Inc.

You begin creating a Web Authentication portal by giving it a name and a description, select the language you would like to be displayed to the user.

In the Redirection section, decide if you want users to continue to the web page they were trying to visit, or if they should be redirected to a specific page once they have successfully authenticated.

Personalization of the Web Auth portal can be achieved by adding a logo along with a unique title to help identify to users the purpose and/or authentication requirements.
In the User Session section, the session timeout determines how long the session can remain valid until the user MUST re-authenticate. This timeout sets a virtual timer for the client where they can reconnect successfully multiple times before they are required to re-authenticate. The grace period defines how long you will allow the client to be idle before authenticating again.



Creating a Web Authentication WLAN

Wireless LANs > [Zone] > Create WLAN Configuration

Web Authentication WLANs use Authentication Method of Open and can't be changed

Create WLAN Configuration

General Options

Authentication Options

* Authentication Type: ○ Standard usage (*For most regular wireless networks*) ○ Hotspot (*WISPr*) ○ Guest Access ● Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ● Open ○ 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

227 | © 2024 CommScope, Inc.

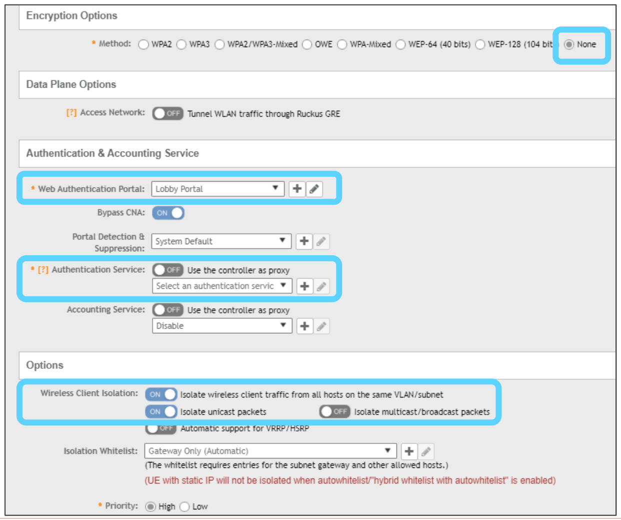
The next option is to select the authentication method which identifies the mechanism or object that will be used to identify the connecting user. Options of 802.1X provide the ability to reach out to a backend authenticator providing authorization for access. Depending on the Authentication Type selected, the user might need to be pre-registered or, you can provide other means for the user to identify themselves such as a Hotspot, Guest Access or Web Authentication. Methods such as MAC Address provides authentication of the device connecting or, a combination of both user and device authentication can be used. The default setting for any of the Authentication types of a newly configured WLAN is **Open**. When other methods other than open are used then additional identification of authentication services will be required. As such when these other methods are selected, you will see further down on the WLAN configuration the Authentication Server settings that appear. SmartZone configuration is dynamic allowing various requirements to appear depending on prior selections. 802.1X and MAC address authentication types are good examples where additional configuration appears when they are selected.

Once you have created the Web Authentication portal, you can apply it to a Web Authentication WLAN.

Under WLAN configuration, select Create and choose Web Authentication as the Authentication Type. When Web Authentication is selected, the Authentication Method is set to Open and can't be changed. Remember, this is 802.11 authentication, and isn't related to the process of user authentication. If you are unsure how this operates, check out the RUCKUS Wireless Fundamentals (RWF 100) course on the RUCKUS training website.

Applying the Web Authentication Portal to a WLAN

Wireless LANs > [Zone] > Create WLAN Configuration



Encryption Options

* Method: ○ WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bit ● None

Data Plane Options

[?] Access Network: OFF Tunnel WLAN traffic through Ruckus GRE

Authentication & Accounting Service

* Web Authentication Portal: Lobby Portal

Bypass CNA: ON

Portal Detection & Suppression: System Default

* [?] Authentication Service: OFF Use the controller as proxy
Select an authentication servic

Accounting Service: OFF Use the controller as proxy
Disable

Options

Wireless Client Isolation: ON Isolate wireless client traffic from all hosts on the same VLAN/subnet
ON Isolate unicast packets OFF Isolate multicast/broadcast packets
OFF Automatic support for VRRP/HSRP

Isolation Whitelist: Gateway Only (Automatic)
(The whitelist requires entries for the subnet gateway and other allowed hosts.)
(UE with static IP will not be isolated when autowhitelist/"hybrid whitelist with autowhitelist" is enabled)

* Priority: ● High ○ Low

- Encryption: None
- Web Authentication Portal name, or create one
- Authentication Server
  - Non-Proxy
  - Proxy

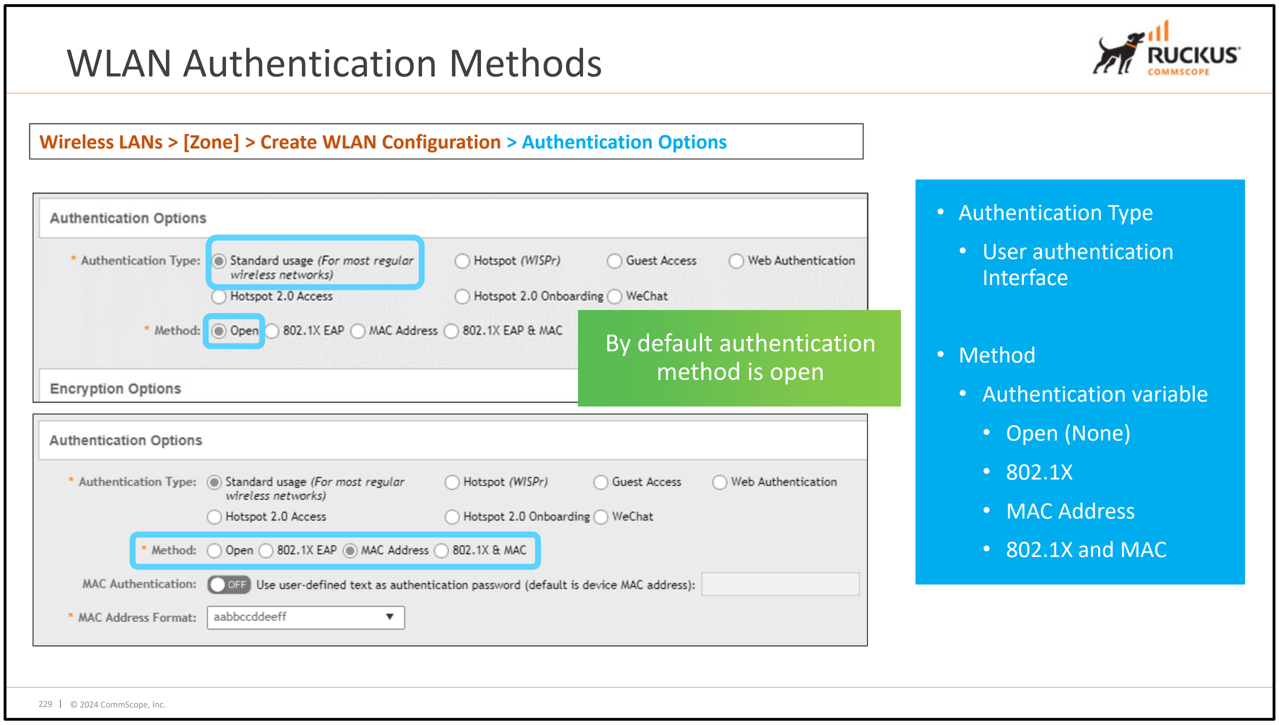
Wireless Client Isolation can be enabled to provide additional security

After selecting **Web Authentication** as the Authentication Type, you'll notice some of the options change below:

- Encryption is set to None by default.
- Under **Authentication & Accounting Service**, select the Web Authentication Portal from the drop down list or create a new Web Authentication Portal by selecting the '+' button next to the drop-down box.
- Finally, choose whether to use a Proxy or Non-Proxy AAA server, and specify the AAA server you will use to authenticate against from the drop down list.

Note that Wireless Client Isolation can be enabled on Web Authentication WLANs to increase security of clients connected to the WLAN.

Note: The Portal Detection and Suppression option above the Authentication service aids with device that use a form of Captive Network Assistant services that can detect if a device is behind a portal based WLAN and can cause disconnect prior to the authentication requirements performed. This feature is beyond the scope of this class but more details can be found in the SmartZone documentation.



WLAN Authentication Methods

Wireless LANs > [Zone] > Create WLAN Configuration > Authentication Options

Authentication Options

* Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ● Open ○ 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

Encryption Options

By default authentication method is open

Authentication Options

* Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ○ Open ○ 802.1X EAP ● MAC Address ○ 802.1X & MAC

MAC Authentication: OFF Use user-defined text as authentication password (default is device MAC address):

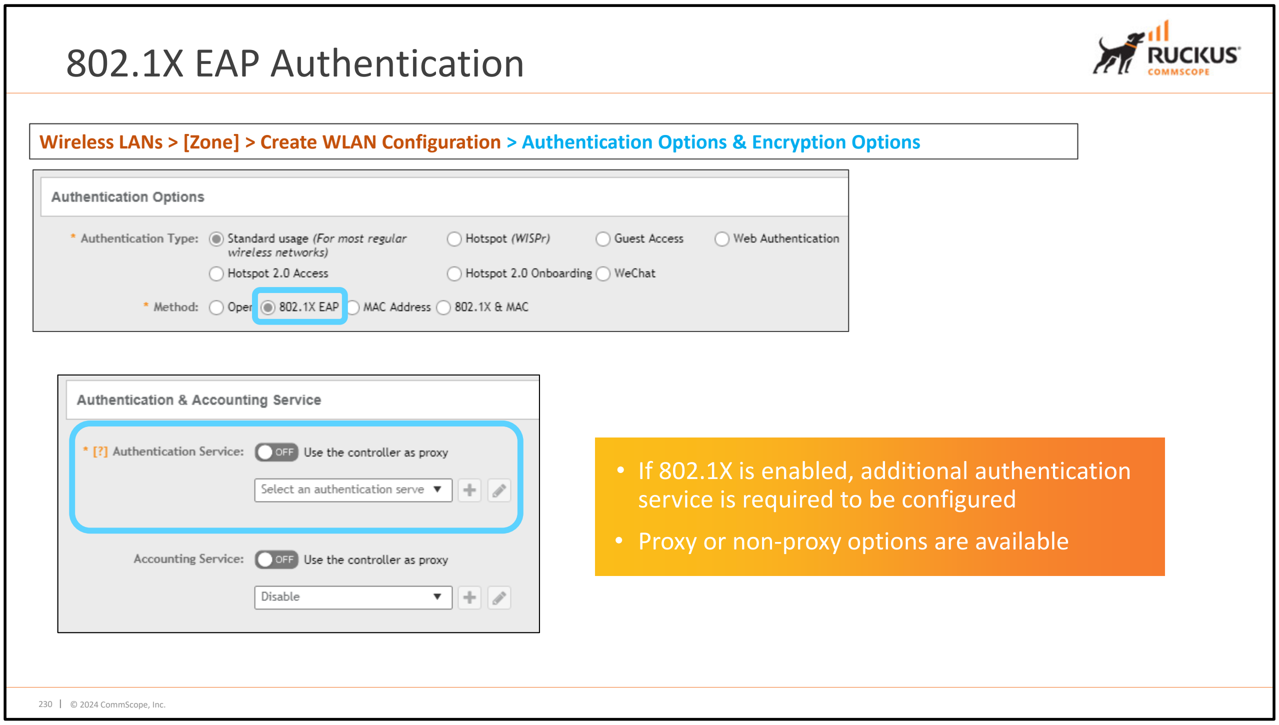
* MAC Address Format: aabbccddeeff

- Authentication Type
  - User authentication Interface
- Method
  - Authentication variable
    - Open (None)
    - 802.1X
    - MAC Address
    - 802.1X and MAC

The next option is to select the authentication method which identifies the mechanism or object that will be used to identify the connecting user. Options of 802.1X provide the ability to reach out to a backend authenticator providing authorization for access.

Depending on the Authentication Type selected, the user might need to be pre-registered or, you can provide other means for the user to identify themselves such as a Hotspot, Guest Access or Web Authentication. Methods such as MAC Address provides authentication of the device connecting or, a combination of both user and device authentication can be used. The default setting for any of the Authentication types of a newly configured WLAN is **Open**.

When other methods other than open are used then additional identification of authentication services will be required. As such when these other methods are selected, you will see further down on the WLAN configuration the Authentication Server settings that appear. SmartZone configuration is dynamic allowing various requirements to appear depending on prior selections. 802.1X and MAC address authentication types are good examples where additional configuration appears when they are selected.



802.1X EAP Authentication

Wireless LANs > [Zone] > Create WLAN Configuration > Authentication Options & Encryption Options

Authentication Options

* Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ○ Open ● 802.1X EAP ○ MAC Address ○ 802.1X & MAC

Authentication & Accounting Service

* [?] Authentication Service: OFF Use the controller as proxy

Select an authentication serve

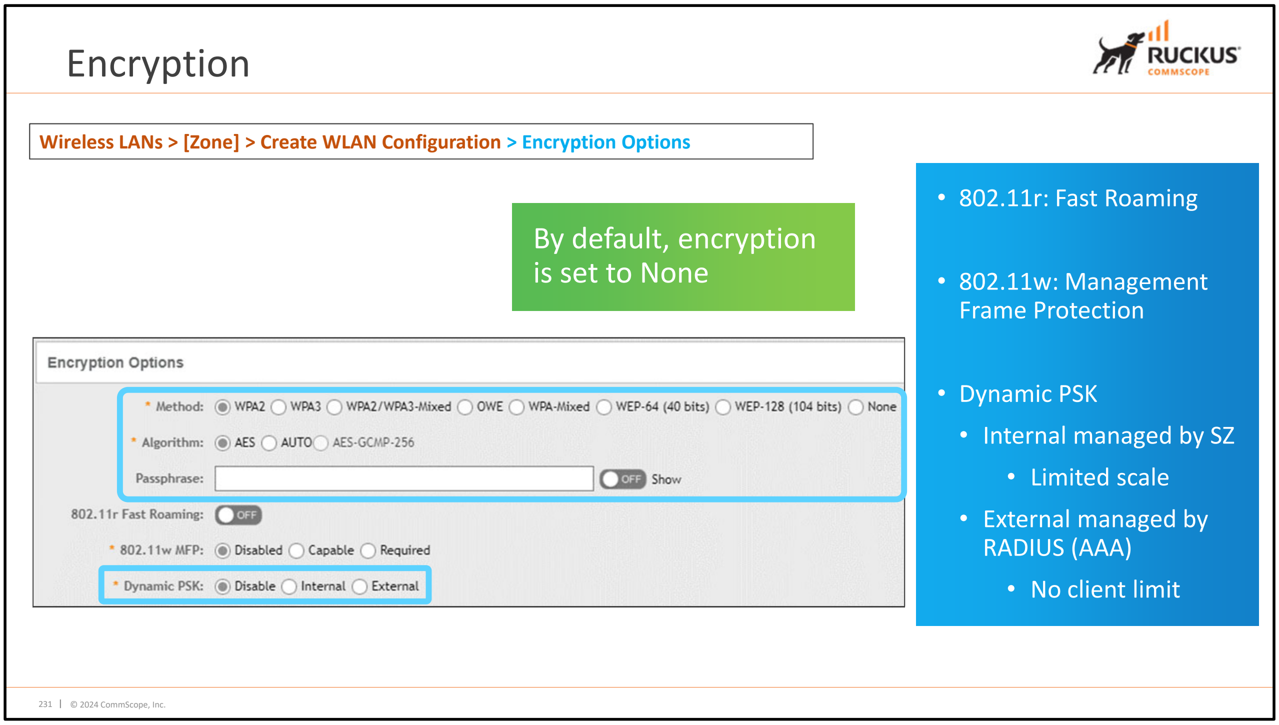
Accounting Service: OFF Use the controller as proxy

Disable

- If 802.1X is enabled, additional authentication service is required to be configured
- Proxy or non-proxy options are available

230 | © 2024 CommScope, Inc.

802.1X Authentication requires an authenticator to verify the credentials of the client. Therefore, you must configure an **Authentication Service for the controller** (when used as a Proxy) or have the **AP**, the user is connected, to directly contact the authenticator service. Optionally you can configure an Accounting Service (AAA authentication) to report connection, disconnection and total data used by clients.



Encryption

Wireless LANs > [Zone] > Create WLAN Configuration > Encryption Options

By default, encryption is set to None

Encryption Options

* Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

Passphrase: OFF Show

802.11r Fast Roaming: OFF

* 802.11w MFP: ● Disabled ○ Capable ○ Required

* Dynamic PSK: ● Disable ○ Internal ○ External

- 802.11r: Fast Roaming
- 802.11w: Management Frame Protection
- Dynamic PSK
  - Internal managed by SZ
    - Limited scale
  - External managed by RADIUS (AAA)
    - No client limit

231 | © 2024 CommScope, Inc.

Moving down on the WLAN configuration, the default setting for encryption options is None. If you choose an encryption method, then additional settings for each method will become available as shown here for WPA2.

You can also select whether to support **802.11r** Fast Roaming, which is a setting commonly used in VoIP deployments.
802.11w offers Management Frame Protection and can be enabled however the understanding of this feature is an advanced topic.

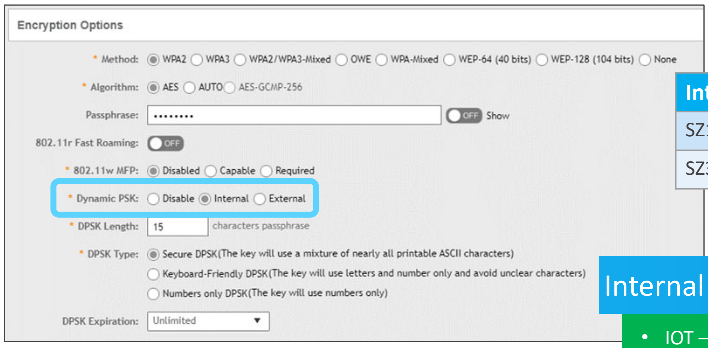
Dynamic PSK is a RUCKUS proprietary method of providing unique per-user or per device Pre-Shared keys for WLAN encryption. DPSKs are used to provide secure wireless access, and eases the process of managing encryption keys. Individual DPSKs can be deleted in the event of a student/employee leaving the organization, or their device being lost or stolen without impacting other users of the WLAN.

An Internal DPSK which is managed within the controller, contains records and DPSK of each user and is limited in the number of DPSKs that can be assigned.

External DPSKs are maintained by the RADIUS server where RADIUS protocols are used to authenticate the user and includes a users DPSK value within the RADIUS response (access accept message). External DPSK does not have a limit on the amount of users it can support.

Internal Dynamic Pre-Shared Key (DPSK)

Wireless LANs > [Zone] > Create WLAN Configuration > Encryption Options



Encryption Options

* Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

Passphrase: ········· OFF Show

802.11r Fast Roaming: OFF

* 802.11w MFP: ● Disabled ○ Capable ○ Required

* Dynamic PSK: ○ Disable ● Internal ○ External

* DPSK Length: 15 characters passphrase

* DPSK Type: ● Secure DPSK(The key will use a mixture of nearly all printable ASCII characters)
○ Keyboard-Friendly DPSK(The key will use letters and number only and avoid unclear characters)
○ Numbers only DPSK(The key will use numbers only)

DPSK Expiration: Unlimited ▼

Internal DPSK	Total DPSKs	DPSKs Per Zone
SZ100, vSZ-E	20,000	10,000
SZ300, vSZ-H	100,000	10,000

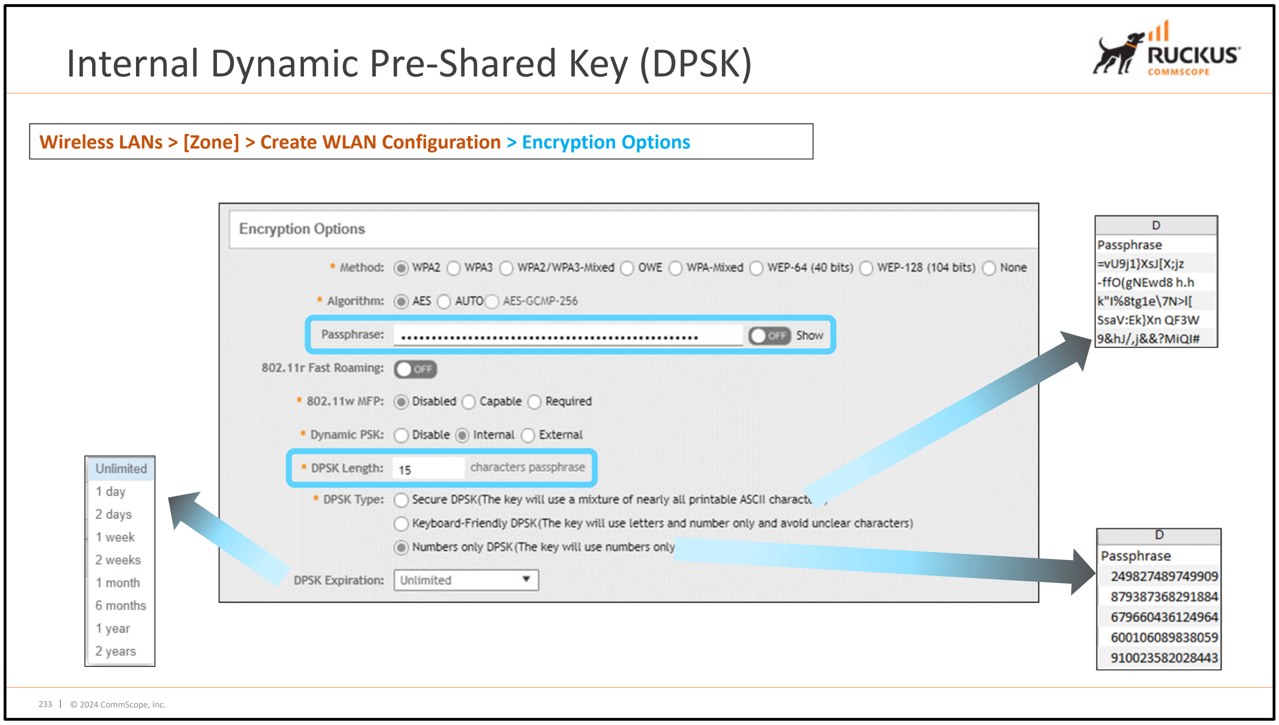
Internal DPSK provides benefits for:

- IOT – Headless devices (devices w/o a proper web browser)
- Education – May not have a RADIUS server
- Legacy Device – Legacy devices may not support 802.1X
- Mobility Devices – Easy to use (no onboarding) and faster roaming compared to 802.1X

232 |

Ruckus patented Dynamic PSK (DPSK) enhances client security by automating randomized passphrase keys for use with each device. SmartZone Internal DPSK deployment can support up to 100,000 DPSKs, with up to 10,000 per zone. Group DPSK, user-specified passphrase and number-only DPSK configurable options further enhance client security and organization policy. Group DPSK allows the ability to create a DPSK “pool” that can be shared by multiple devices, with up to sixty-four Group DPSKs in a zone. Administrators can also specify a number-only DPSK, which makes guest or other “easy entry” scenarios more user-friendly.

In External DPSK deployments, the DPSK is maintained by the Radius Server (AAA) and Radius protocols are used to authenticate the client. The client is authenticated by the open authentication WLAN - WPA/WPA2 encryption where the controller uses the RADIUS server which will respond to a successful authentication, the DPSK will be included in the Access Accept message. There is no limitation on the number of DPSK supported in this mode.



Internal Dynamic Pre-Shared Key (DPSK)

Wireless LANs > [Zone] > Create WLAN Configuration > Encryption Options

Encryption Options

* Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

Passphrase: •• OFF Show

802.11r Fast Roaming: OFF

* 802.11w MFP: ● Disabled ○ Capable ○ Required

* Dynamic PSK: ○ Disable ● Internal ○ External

* DPSK Length: 15 characters passphrase

* DPSK Type: ○ Secure DPSK(The key will use a mixture of nearly all printable ASCII charact

○ Keyboard-Friendly DPSK(The key will use letters and number only and avoid unclear characters)

● Numbers only DPSK(The key will use numbers only

DPSK Expiration: Unlimited ▾

D
Passphrase
=vU9j1}XsJ[X;jz
-ffO(gNEwd8 h.h
k"I%8tg1e\7N>l[
SsaV:Ek}Xn QF3W
9&hJ/,j&&?MiQI#

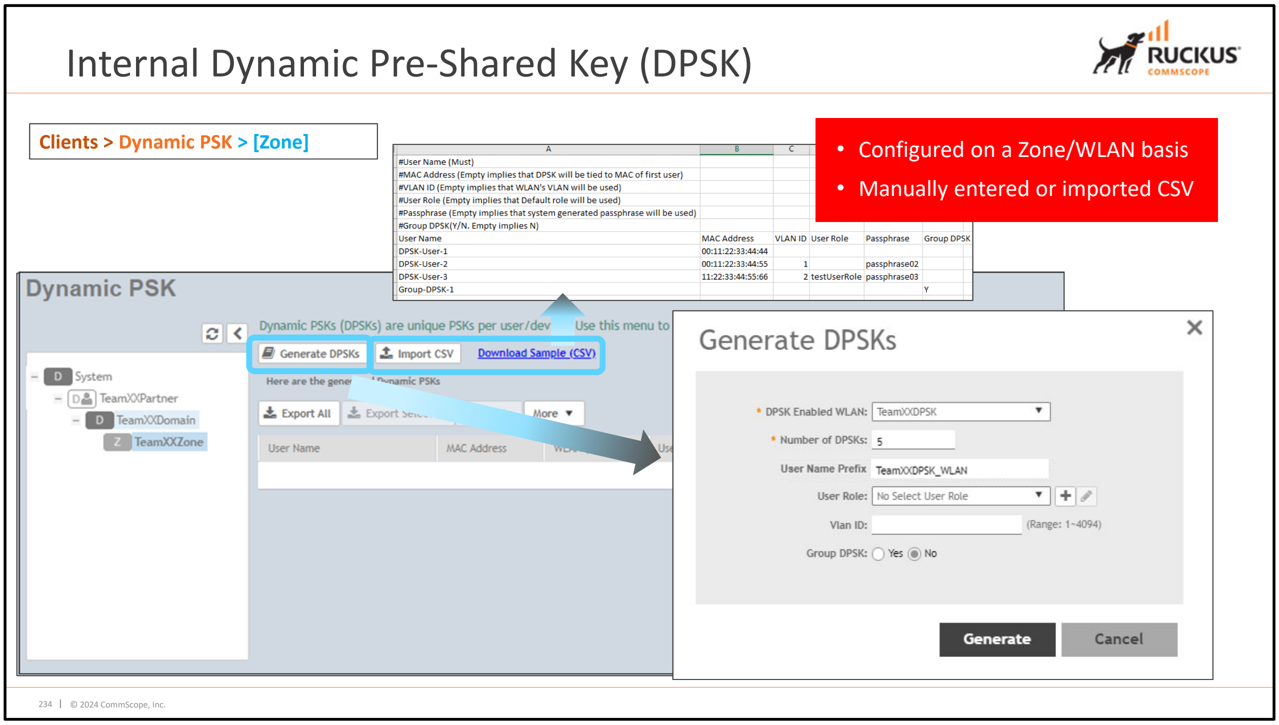
D
Passphrase
249827489749909
879387368291884
679660436124964
600106089838059
910023582028443

233 | © 2024 CommScope, Inc.

If internal DPSK is chosen, then you will be given the ability to customize the DPSK characteristic requirements for the DPSK WLAN you are configuring. Note that the passphrase configured above is required but never used since DPSKs are going to be used by clients instead of this configured PSK, you should create a complex "seed" passphrase that will be difficult to guess since it should not be used by any clients.

These internal DPSK settings include the DPSK length where the default DPSK value is 62 however you can be adjusted to meet your specifications. Keep in mind that if clients are going to be entering this manually a lower number might be beneficial to keep it user friendly. The WiFi Alliance suggests that a PSK should be at least 18 characters which includes a mixture of upper- and lower-case letters and symbols to ensure security.

Keep in mind that devices you may be deploying on this WLAN such as IOT or headless devices (no browser capabilities) do not support some or all special characters. Therefore, you might need to adjust the DPSK passphrase type that you want to use for the WLAN. Three options are available which include Secure DPSK, Keyboard Friendly DPSK and Numbers only DPSK to allow you to customize depending on your deployment needs. Finally you can also select how long the DPSK will be valid on the WLAN before it will expire and the user will need to renew with a new key.



Internal Dynamic Pre-Shared Key (DPSK)

Clients > Dynamic PSK > [Zone]

- Configured on a Zone/WLAN basis
- Manually entered or imported CSV

A	B	C			
#User Name (Must)					
#MAC Address (Empty implies that DPSK will be tied to MAC of first user)					
#VLAN ID (Empty implies that WLAN's VLAN will be used)					
#User Role (Empty implies that Default role will be used)					
#Passphrase (Empty implies that system generated passphrase will be used)					
#Group DPSK(Y/N. Empty implies N)					
User Name	MAC Address	VLAN ID	User Role	Passphrase	Group DPSK
DPSK-User-1	00:11:22:33:44:44				
DPSK-User-2	00:11:22:33:44:55	1		passphrase02	
DPSK-User-3	11:22:33:44:55:66	2	testUserRole	passphrase03	
Group-DPSK-1					Y

Generate DPSKs

- * DPSK Enabled WLAN: TeamXXDPSK
- * Number of DPSKs: 5
- User Name Prefix TeamXXDPSK_WLAN
- User Role: No Select User Role
- Vlan ID: (Range: 1~4094)
- Group DPSK: ○ Yes ● No

Internal DPSK keys are generated and maintained within SmartZone by navigating to **Clients> Dynamic PSK**. Once a zone is selected the click Generate DPSK to populate the DPSK for a WLAN. The fields that appear are:

DPSK Enabled WLAN: If multiple DPSK enabled WLANs are deployed in the zone you will be able to use the drop down list to select the one you would like to add DPSK entries for.
Number of DPSKs: This is the amount of DPSKs you are going to add to the WLAN DPSK pool.

User Name: Leave it blank if you want the controller to auto-generate the user name, or enter the user name manually that might help identify their membership in the DPSK list.

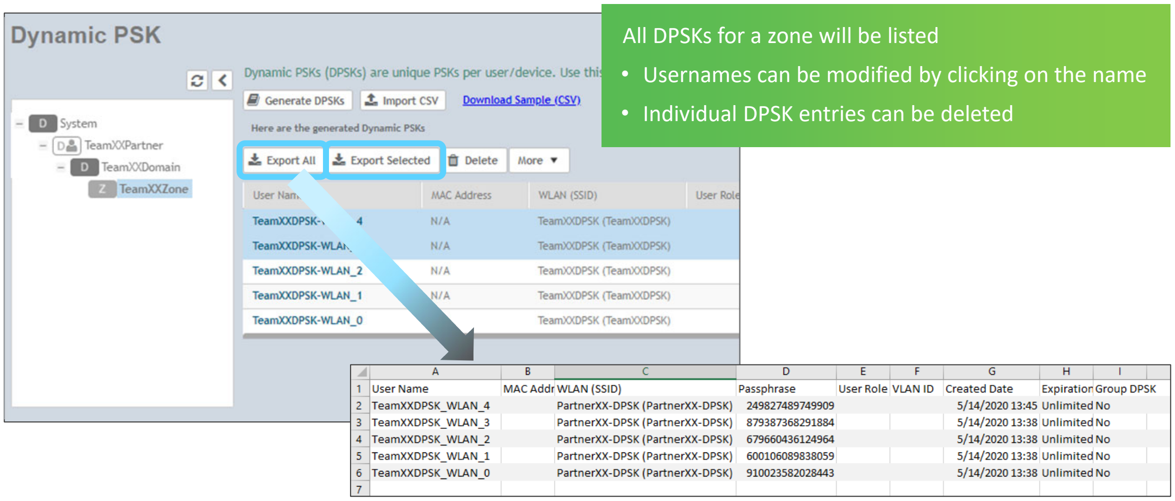
Passphrase: Leave it blank if you want the controller to auto-generate the passphrase, or enter the passphrase manually.

User Role: If you have created user roles, select the user role that you want to assign to the device to manipulate the VLAN or other values assigned to the user role.

VLAN ID: Type a VLAN ID within the range 1-4094 that you would like the user to be associated with. If you leave blank it will assign them to the VLAN configured on the WLAN.

Internal Dynamic Pre-Shared Key (DPSK)

Clients > Dynamic PSK > [Zone]



Dynamic PSKs (DPSKs) are unique PSKs per user/device. Use this

Here are the generated Dynamic PSKs

User Nam	MAC Address	WLAN (SSID)	User Role
TeamXXDPSK-4	N/A	TeamXXDPSK (TeamXXDPSK)	
TeamXXDPSK-WLA	N/A	TeamXXDPSK (TeamXXDPSK)	
TeamXXDPSK-WLAN_2	N/A	TeamXXDPSK (TeamXXDPSK)	
TeamXXDPSK-WLAN_1	N/A	TeamXXDPSK (TeamXXDPSK)	
TeamXXDPSK-WLAN_0		TeamXXDPSK (TeamXXDPSK)	

All DPSKs for a zone will be listed

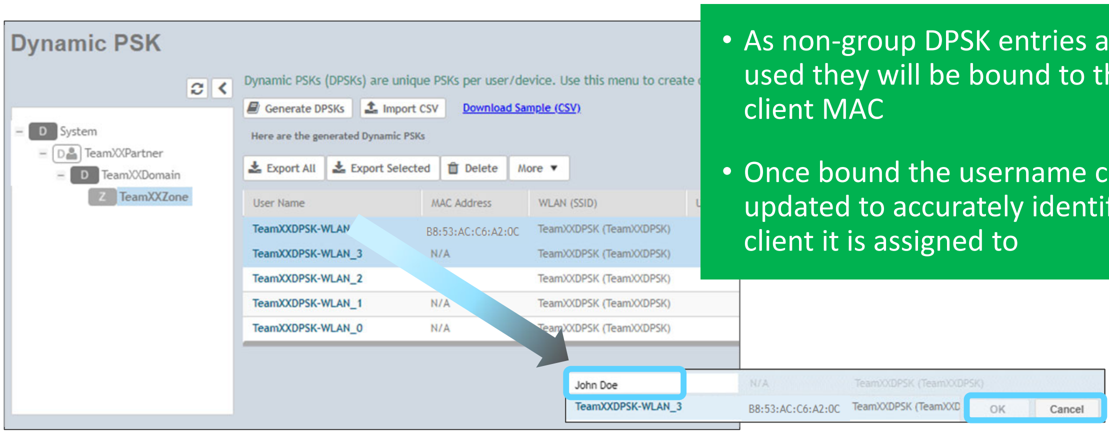
- Usernames can be modified by clicking on the name
- Individual DPSK entries can be deleted

	A	B	C	D	E	F	G	H	I
1	User Name	MAC Addr	WLAN (SSID)	Passphrase	User Role	VLAN ID	Created Date	Expiration	Group DPSK
2	TeamXXDPSK_WLAN_4		PartnerXX-DPSK (PartnerXX-DPSK)	249827489749909			5/14/2020 13:45	Unlimited	No
3	TeamXXDPSK_WLAN_3		PartnerXX-DPSK (PartnerXX-DPSK)	879387368291884			5/14/2020 13:38	Unlimited	No
4	TeamXXDPSK_WLAN_2		PartnerXX-DPSK (PartnerXX-DPSK)	679660436124964			5/14/2020 13:38	Unlimited	No
5	TeamXXDPSK_WLAN_1		PartnerXX-DPSK (PartnerXX-DPSK)	600106089838059			5/14/2020 13:38	Unlimited	No
6	TeamXXDPSK_WLAN_0		PartnerXX-DPSK (PartnerXX-DPSK)	910023582028443			5/14/2020 13:38	Unlimited	No
7									

Once the DPSK are generated they will be listed with their details. To gather the DPSK values that were generated you can select the entries you would like to export and click the Export Selected button. Optionally you can export all the entries for the zone by clicking on the Export all button. Both will download a CSV file that can then be used to distribute the DPSKs.

Internal Dynamic Pre-Shared Key (DPSK)

Clients > Dynamic PSK > [Zone]



Dynamic PSK

Dynamic PSKs (DPSKs) are unique PSKs per user/device. Use this menu to create

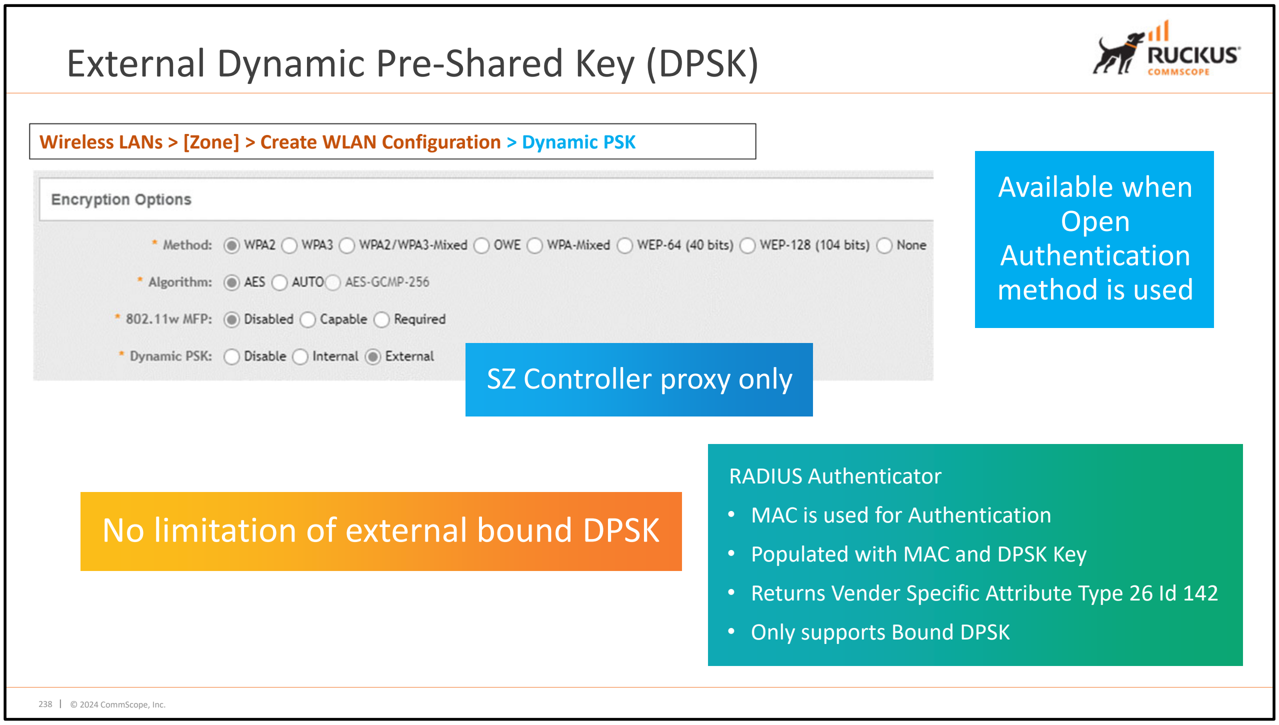
Here are the generated Dynamic PSKs

User Name	MAC Address	WLAN (SSID)
TeamXXDPSK-WLAN	B8:53:AC:C6:A2:0C	TeamXXDPSK (TeamXXDPSK)
TeamXXDPSK-WLAN_3	N/A	TeamXXDPSK (TeamXXDPSK)
TeamXXDPSK-WLAN_2		TeamXXDPSK (TeamXXDPSK)
TeamXXDPSK-WLAN_1	N/A	TeamXXDPSK (TeamXXDPSK)
TeamXXDPSK-WLAN_0	N/A	TeamXXDPSK (TeamXXDPSK)

John Doe	N/A	TeamXXDPSK (TeamXXDPSK)
TeamXXDPSK-WLAN_3	B8:53:AC:C6:A2:0C	TeamXXD

- As non-group DPSK entries are used they will be bound to the client MAC
- Once bound the username can be updated to accurately identify the client it is assigned to

As clients connect they will convert the unbound DPSK entries to bound and their MAC address will be populated by the DPSK that was used. You can click on the DPSK username and update the current value making it easier to identify the user of the bound DPSK. If any DPSK is selected and deleted from the list the user will no long be able to use that key to authenticate to the WLAN.



External Dynamic Pre-Shared Key (DPSK)

Wireless LANs > [Zone] > Create WLAN Configuration > Dynamic PSK

Encryption Options

* Method: ● WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

* 802.11w MFP: ● Disabled ○ Capable ○ Required

* Dynamic PSK: ○ Disable ○ Internal ● External

Available when Open Authentication method is used

SZ Controller proxy only

No limitation of external bound DPSK

RADIUS Authenticator

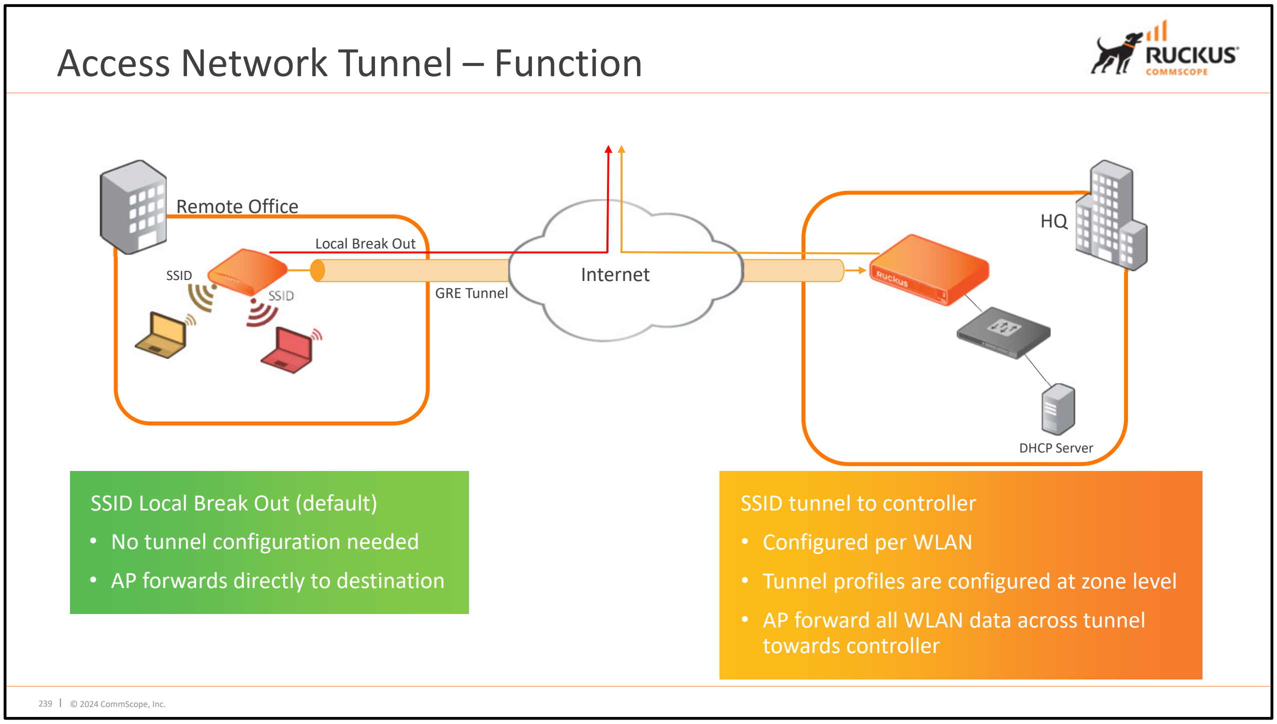
- MAC is used for Authentication
- Populated with MAC and DPSK Key
- Returns Vender Specific Attribute Type 26 Id 142
- Only supports Bound DPSK

238 | © 2024 CommScope, Inc.

As mentioned previously RUCKUS Networks introduced a concept unique to the industry and building on the capabilities of DPSK, known as External DPSK. The SZ controller will send Access-Request messages to the RADIUS server using the MAC as authentication.

The RADIUS server will respond with a Access Accept message which includes the RUCKUS Vendor Specific Attribute ID 142 containing the DPSK value the device is to use. Because the RADIUS server responds with the DPSK value it needs to be populated with the MAC and assigned DPSK of each specified device which means all DPSKs are in the bound state since they are specifically assigned.

RADIUS is currently the only supported AAA authenticator for DPSK and the SZ controller must be used as a proxy when external DPSK is used. For more details on DPSK and more information on how to deploy it, refer to the RUCKUS website.



Access Network Tunnel – Function

SSID Local Break Out (default)

- No tunnel configuration needed
- AP forwards directly to destination

SSID tunnel to controller

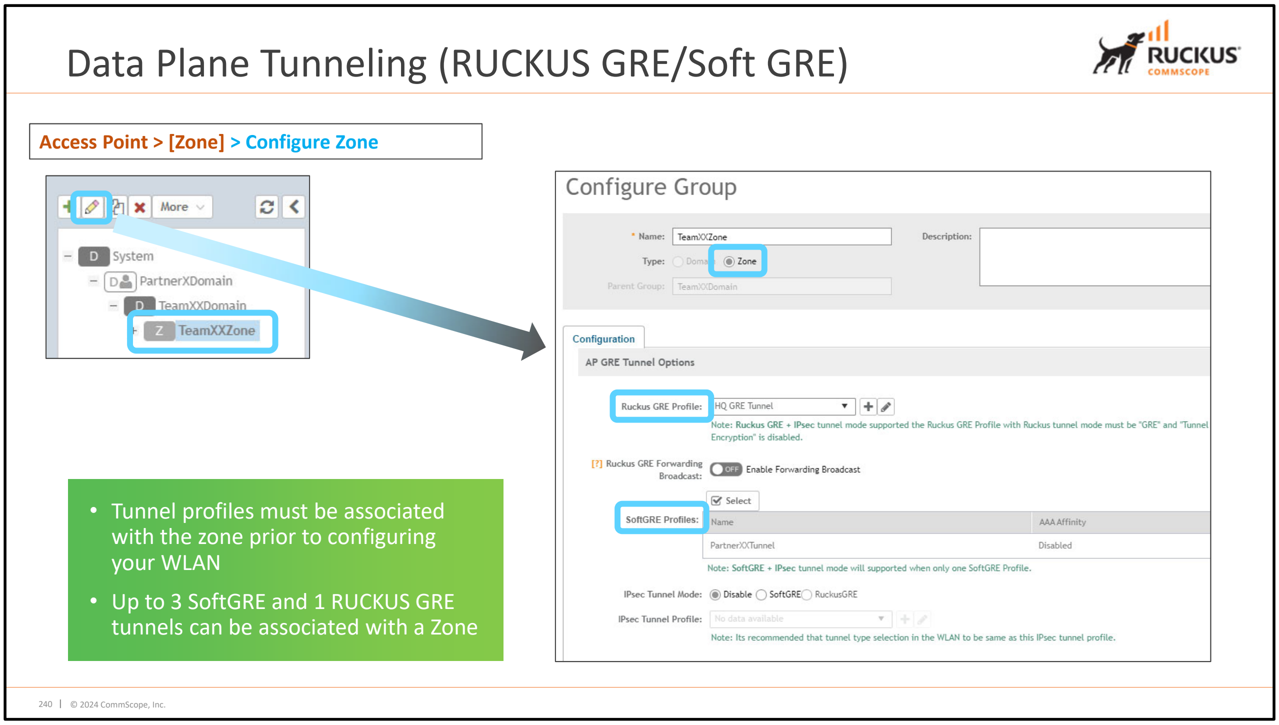
- Configured per WLAN
- Tunnel profiles are configured at zone level
- AP forward all WLAN data across tunnel towards controller

239 | © 2024 CommScope, Inc.

As we continue down the WLAN configuration we will see tunnel options. Let’s look at the effect of enabling a tunnel for a WLAN. Without tunnelling, an Access Point passes traffic straight to the Internet. This is normal for most deployments.

However, there are occasions where traffic or security policies require that traffic be sent to the controller. VoIP is probably the scenario you are most familiar with, where connections require fast BSS transitions. You may also use tunnelling in conjunction with data monitoring (lawful intercept) or to allow access the resources that are remote to the AP however not so with the controller.

In order to enable WLAN tunneling at the WLAN level, you need to have already configured a tunnel interface, either a physical interface or a virtual Data Plane. You also need to have a tunnel profile created under **Services & Profiles > Tunnels & Ports**.



Data Plane Tunneling (RUCKUS GRE/Soft GRE)

Access Point > [Zone] > Configure Zone

Configure Group

* Name: TeamXXZone

Type: ○ Domain ● Zone

Parent Group: TeamXXDomain

Description:

Configuration

AP GRE Tunnel Options

Ruckus GRE Profile: HQ GRE Tunnel

Note: Ruckus GRE + IPsec tunnel mode supported the Ruckus GRE Profile with Ruckus tunnel mode must be "GRE" and "Tunnel Encryption" is disabled.

[?] Ruckus GRE Forwarding Broadcast: OFF Enable Forwarding Broadcast

SoftGRE Profiles: ☑ Select

Name	AAA Affinity
PartnerXXTunnel	Disabled

Note: SoftGRE + IPsec tunnel mode will supported when only one SoftGRE Profile.

IPsec Tunnel Mode: ● Disable ○ SoftGRE ○ RuckusGRE

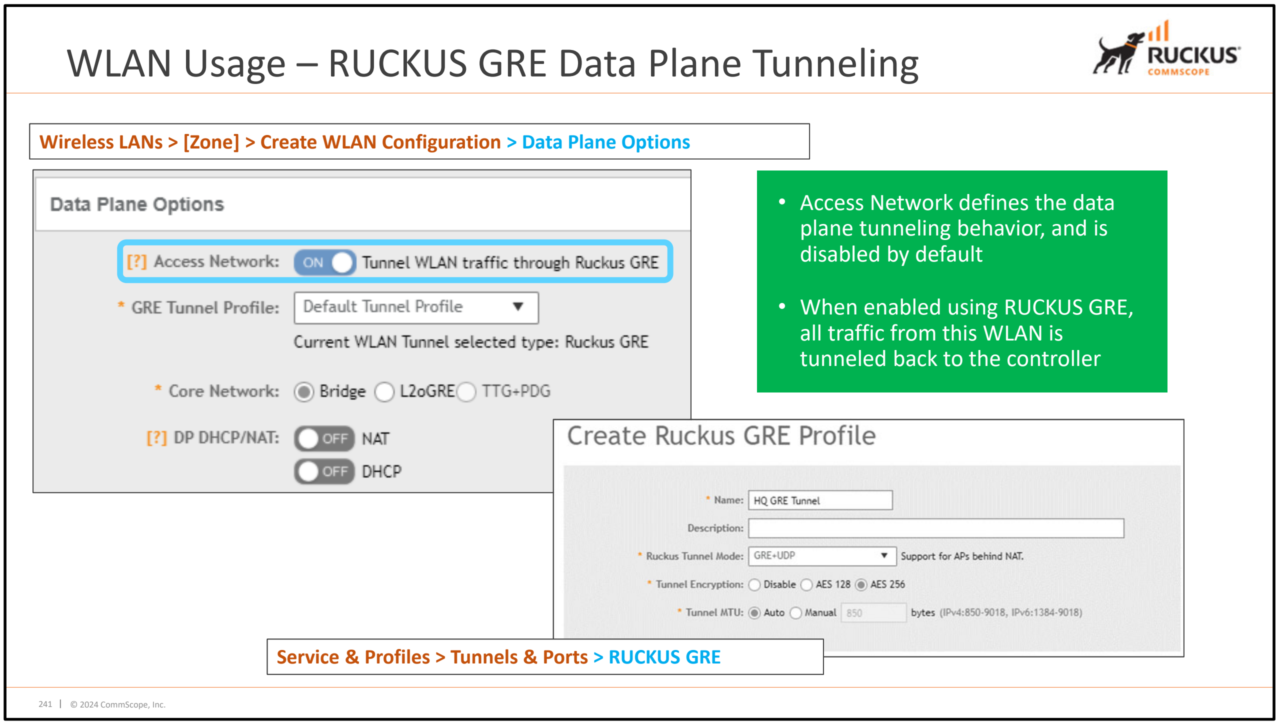
IPsec Tunnel Profile: No data available

Note: Its recommended that tunnel type selection in the WLAN to be same as this IPsec tunnel profile.

- Tunnel profiles must be associated with the zone prior to configuring your WLAN
- Up to 3 SoftGRE and 1 RUCKUS GRE tunnels can be associated with a Zone

240 | © 2024 CommScope, Inc.

Prior to configuring a WLAN to use either a RUCKUS GRE or soft GRE tunnel, they must be associated with the zone your WLAN resides in. One RUCKUS GRE tunnel can be selected and up to 3 softGRE tunnels can be selected within a zone. Once configured under the zone the tunnels will be available for selection within the WLAN configuration.



WLAN Usage – RUCKUS GRE Data Plane Tunneling

Wireless LANs > [Zone] > Create WLAN Configuration > Data Plane Options

Data Plane Options

[?] Access Network: ON Tunnel WLAN traffic through Ruckus GRE

* GRE Tunnel Profile: Default Tunnel Profile ▼

Current WLAN Tunnel selected type: Ruckus GRE

* Core Network: ● Bridge ○ L2oGRE ○ TTG+PDG

[?] DP DHCP/NAT: OFF NAT

OFF DHCP

- Access Network defines the data plane tunneling behavior, and is disabled by default
- When enabled using RUCKUS GRE, all traffic from this WLAN is tunneled back to the controller

Create Ruckus GRE Profile

* Name: HQ GRE Tunnel

Description:

* Ruckus Tunnel Mode: GRE+UDP ▼ Support for APs behind NAT.

* Tunnel Encryption: ○ Disable ○ AES 128 ● AES 256

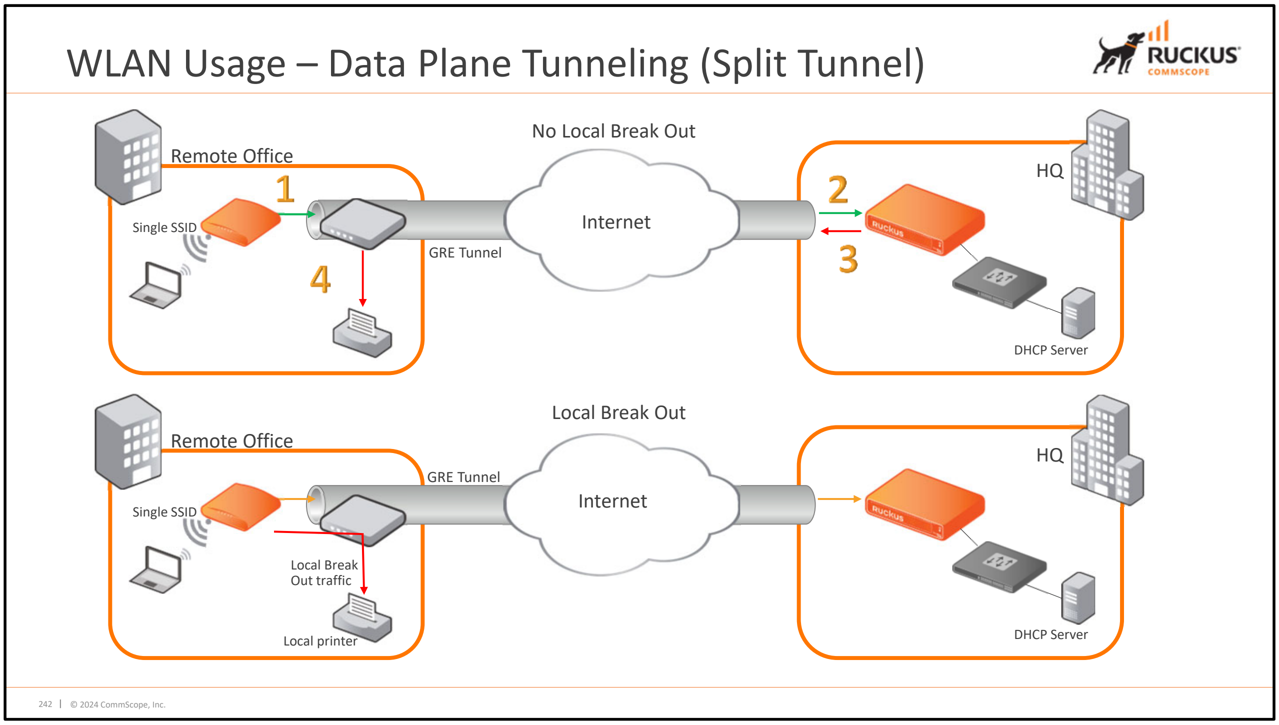
* Tunnel MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

Service & Profiles > Tunnels & Ports > RUCKUS GRE

241 | © 2024 CommScope, Inc.

Tunnel selection for a WLAN is under the **Data Plane Options** allowing to set up tunnelling for the WLAN traffic.

The default is disabled; that is, traffic is not tunnelled and performs local breakout forwarding. To enable tunnelling select the **Tunnel WLAN traffic through GRE tunnel** to forward traffic from this WLAN back to the controller or a configured dataplane. When tunneling through a RUCKUS GRE tunnel using the bridge Core Network option additional choices including Core Network, Data Plane DHCP/NAT are available.



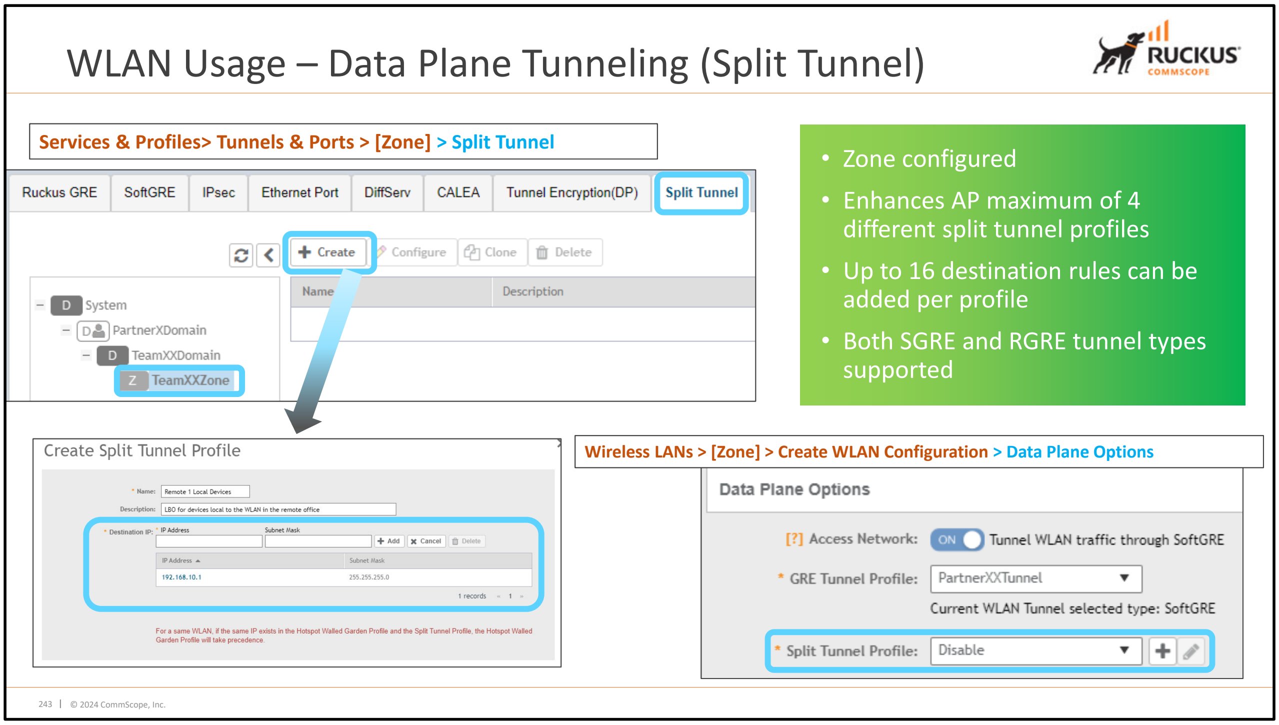
WLAN Usage – Data Plane Tunneling (Split Tunnel)

242 | © 2024 CommScope, Inc.

Currently for a specific user, an AP supports the tunneling of all user traffic OR sending that user's traffic out the AP WAN interface.

Split tunneling provides the ability to split traffic based on configured destination IPs/subnets. Up to 16 IP ACLs are configured within a split tunnel profile and can be applied to the AP WLAN. WLAN client packets that match the ACL will be sent out and returned locally (LBO) on the AP WAN interface. Network device sourced in the AP's local network will not initiate connection to client in the tunneled WLAN.

For split tunneling to work correctly wireless Client will need to receive IP address from DHCP Server from the remote end of the tunnel.
It is the operator's responsibility to guarantee that the IP address rule specified for the split LBO traffic is reachable from the AP management interface and VLAN.



WLAN Usage – Data Plane Tunneling (Split Tunnel)

Services & Profiles> Tunnels & Ports > [Zone] > Split Tunnel

- Zone configured
- Enhances AP maximum of 4 different split tunnel profiles
- Up to 16 destination rules can be added per profile
- Both SGRE and RGRE tunnel types supported

Create Split Tunnel Profile

* Name: Remote 1 Local Devices

Description: LBO for devices local to the WLAN in the remote office

* Destination IP: * IP Address | Subnet Mask | + Add | ✖ Cancel | Delete

IP Address ▲	Subnet Mask
192.168.10.1	255.255.255.0

1 records « 1 »

For a same WLAN, if the same IP exists in the Hotspot Walled Garden Profile and the Split Tunnel Profile, the Hotspot Walled Garden Profile will take precedence.

Wireless LANs > [Zone] > Create WLAN Configuration > Data Plane Options

Data Plane Options

[?] Access Network: ON Tunnel WLAN traffic through SoftGRE

* GRE Tunnel Profile: PartnerXXTunnel

Current WLAN Tunnel selected type: SoftGRE

* Split Tunnel Profile: Disable

243 | © 2024 CommScope, Inc.

To configure a split tunnel navigate to **Services & Profiles > Tunnels & Ports > Split tunnel**.
Select the zone you would like to configure split tunneling options and click create
a. In the **Name** field, type a name for the split tunnel profile.
b. Optionally you can add a brief **Description** in the description field
c. In the **IP Address** field, enter the destination IP address.
d. In the **Subnet Mask** field, enter the destination IP subnet mask.
e. Click **Add** to add the destination IP details after each entry. Remember up to 16 can be configured
f. Click **OK**.

NOTE

To configure a RUCKUSGRE or SoftGRE split tunnel it must be enabled on the WLAN before mapping it to a Split Tunnel Profile.
As you can see there are edit, clone or delete options to manage the split tunnel profiles.
Once your profile has been configured under your **WLAN configuration > dataplane options** you can select your split profile option within the WLAN configuration.

Advanced Options Overview

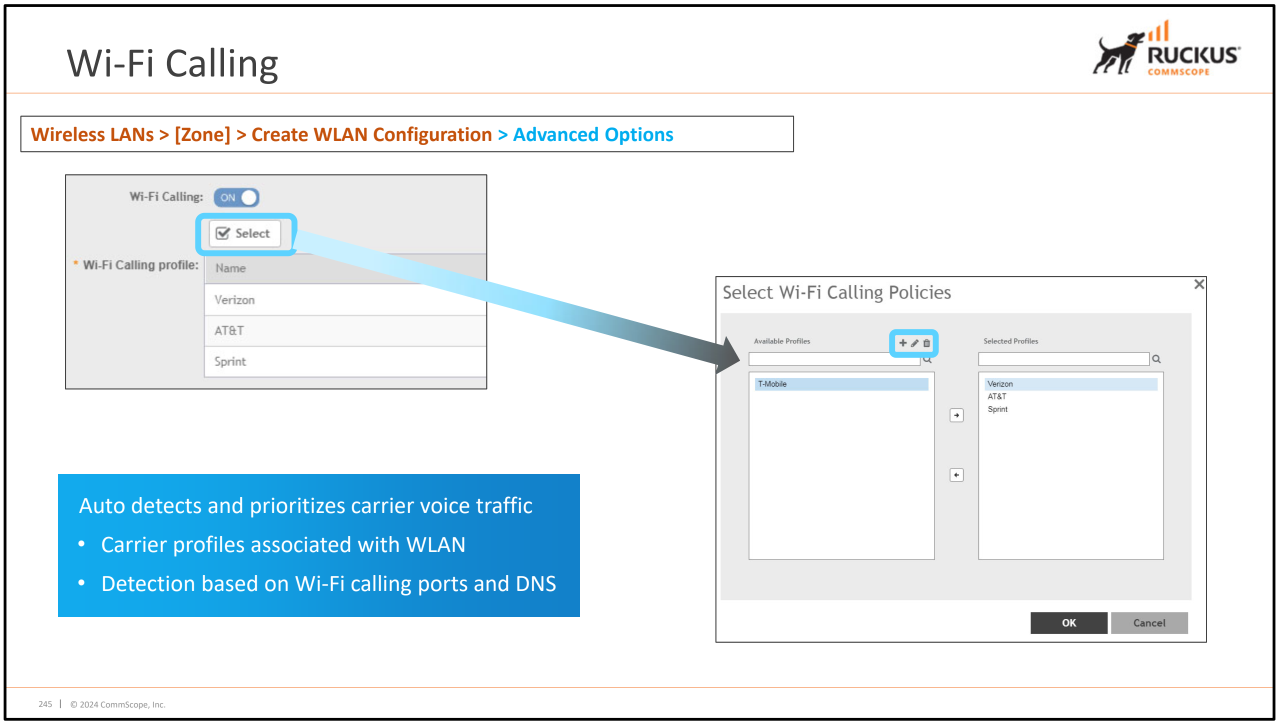
Wireless LANs > [Zone] > Create WLAN Configuration > Advanced Options

Fine tune the WLAN including:

- Wi-Fi Calling
- Client Fingerprinting
- VLAN pooling
- Load/band balancing
- QoS Mapping
- Scheduling

244 |

Under **Advanced Options**, you will find a range of additional settings that give you a high degree of control over the way the WLAN functions.



Wi-Fi Calling

Wireless LANs > [Zone] > Create WLAN Configuration > Advanced Options

Wi-Fi Calling: ON

Auto detects and prioritizes carrier voice traffic

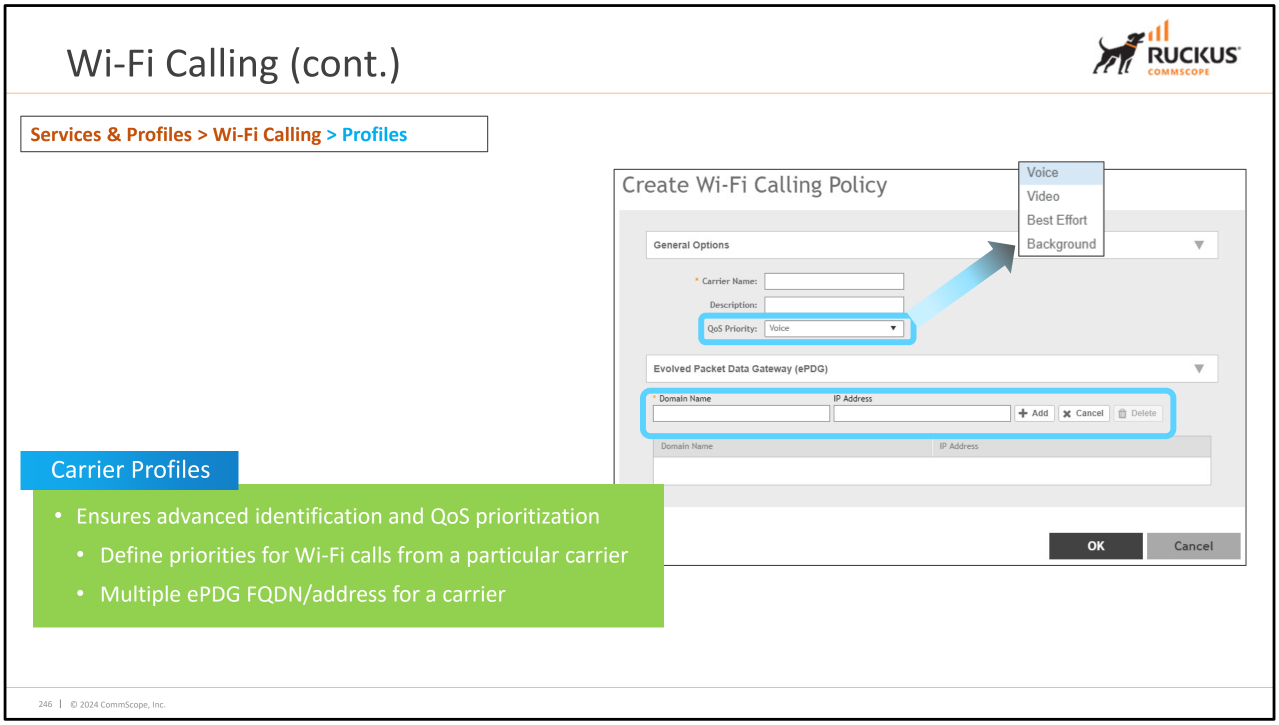
- Carrier profiles associated with WLAN
- Detection based on Wi-Fi calling ports and DNS

245 | © 2024 CommScope, Inc.

Smartphones have the ability to connect to their carrier and establish calls through the local Wi-Fi connection by establishing an IPSec tunnel for their WiFi calling feature. Configuring WiFi Calling allows a WLAN to auto detect and prioritize the voice traffic over other network data traffic. The detection is based on the common Wi-Fi calling port and DNS configured values.

Multiple FQDN addresses along with a priority can be configured for each carrier. Seamless roaming across multiple APs is supported and can be used in Local Breakout (LBO) Tunnel, VLAN and Mesh designs.

Only the selected profiles within a WLAN will be supported by the WiFi calling feature. You can select preconfigured profiles to be used for a WLAN or add them using the buttons at the top.



Wi-Fi Calling (cont.)

Services & Profiles > Wi-Fi Calling > Profiles

Create Wi-Fi Calling Policy

General Options

* Carrier Name:

Description:

QoS Priority: Voice

Evolved Packet Data Gateway (ePDG)

* Domain Name	IP Address

Carrier Profiles

- Ensures advanced identification and QoS prioritization
  - Define priorities for Wi-Fi calls from a particular carrier
  - Multiple ePDG FQDN/address for a carrier

246 | © 2024 CommScope, Inc.

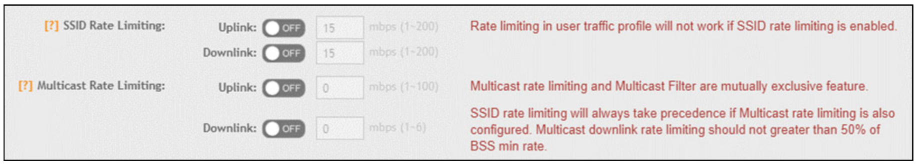
Profiles can be preconfigured and associated with the WLAN of your choice. Each carrier profile can have a defined priority and how their Wi-Fi clients calling packets are handled within the WLAN. Each carrier will need to have a profile configured identifying their FQDN optionally or IP addresses of their Evolved Packet Data Gateway. Many carriers use multiple ePDGs therefore multiple entries can be applied to a carriers profile. For more details concerning WiFi calling please refer to the SmartZone Admin Guide.

https://ruckus-support.s3.amazonaws.com/private/documents/2832/Wi-Fi%20calling%20Deployment%20Guide.pdf?AWSAccessKeyId=AKIAJM3QLNNKLOV235TQ&Expires=1588877120&Signature=SiND%2FQsEwy9Y0RAnf1EtWTEpbhw%3D

SSID Rate Limiting

Wireless LANs > Create WLAN Configuration > Advanced Options

Enforces an aggregate rate limit for all users of the WLAN providing the ability to identify Unicast or Multicast



[?] SSID Rate Limiting: Uplink: OFF 15 mbps (1~200)

Downlink: OFF 15 mbps (1~200)

Rate limiting in user traffic profile will not work if SSID rate limiting is enabled.

[?] Multicast Rate Limiting: Uplink: OFF 0 mbps (1~100)

Downlink: OFF 0 mbps (1~6)

Multicast rate limiting and Multicast Filter are mutually exclusive feature.

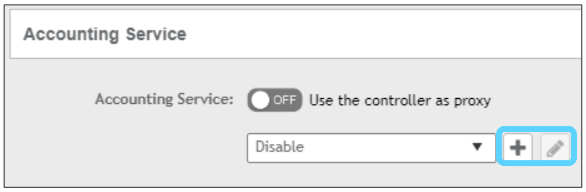
SSID rate limiting will always take precedence if Multicast rate limiting is also configured. Multicast downlink rate limiting should not greater than 50% of BSS min rate.

247 | © 2024 CommScope, Inc.

SSID Rate Limiting imposes a rate limit on the devices using the WLAN. You can also impose rate limits using Firewall Policies. However, in order for Firewall policies to function you need to have **SSID Rate Limiting** disabled.

Accounting Service

Wireless LANs > Create WLAN Configuration > Accounting Service



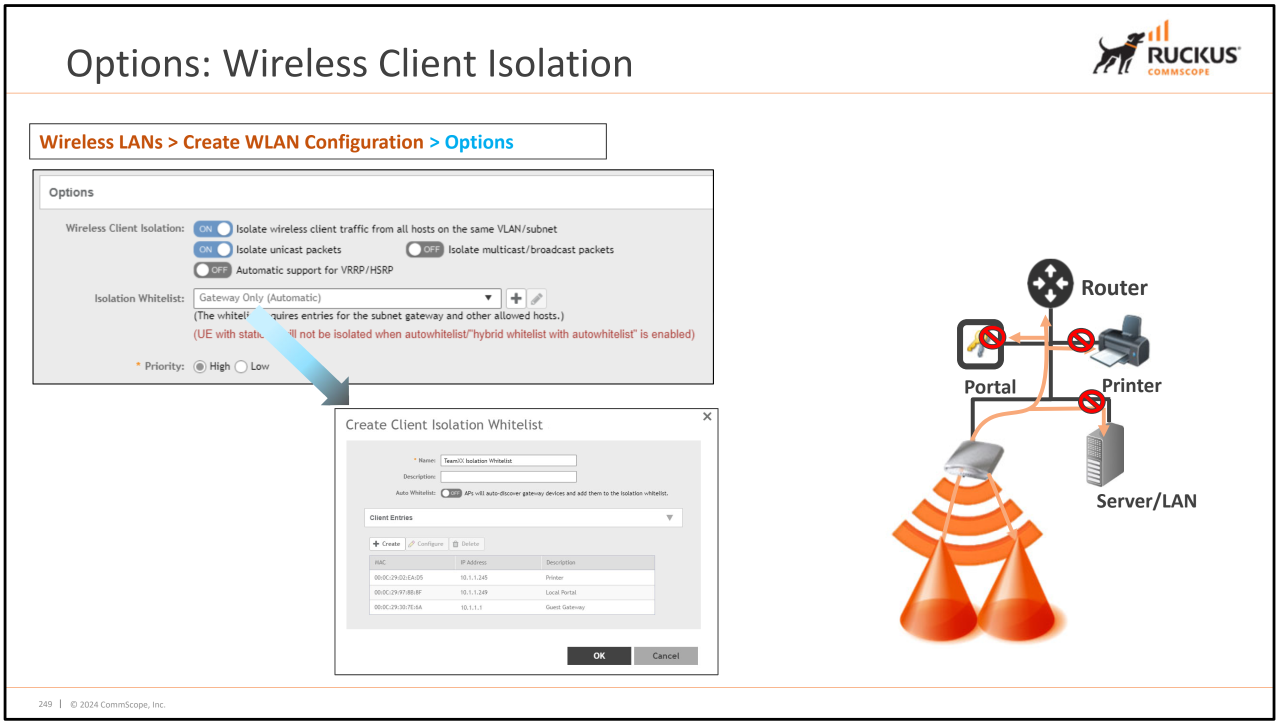
Accounting Service

Accounting Service: OFF Use the controller as proxy

Disable

- Specifies server to send accounting messages
  - Disabled by default
- Server options
  - Proxy based
    - Sent by controller
  - Direct
    - Sent by AP directly

Specifies the server used for accounting messages. By enabling Proxy, accounting messages are sent by the controller. In a non-proxy mode, the AP will communicate accounting messages directly. Pre-existing accounting servers can be chosen from the drop down menu or one can be configured using the + sign. The server displayed in the drop down field can be edited by selecting the pencil icon.



Options: Wireless Client Isolation

Wireless LANs > Create WLAN Configuration > Options

Options

Wireless Client Isolation: ON Isolate wireless client traffic from all hosts on the same VLAN/subnet

ON Isolate unicast packets — OFF Isolate multicast/broadcast packets

OFF Automatic support for VRRP/HSRP

Isolation Whitelist: Gateway Only (Automatic) ▼ +

(The whiteli quires entries for the subnet gateway and other allowed hosts.)

(UE with static ill not be isolated when autowhitelist/"hybrid whitelist with autowhitelist" is enabled)

* Priority: ● High ○ Low

Create Client Isolation Whitelist

* Name: TeamXX Isolation Whitelist

Description:

Auto Whitelist: OFF APs will auto-discover gateway devices and add them to the isolation whitelist.

Client Entries

MAC	IP Address	Description
00:0C:29:D2:EA:D5	10.1.1.245	Printer
00:0C:29:97:8B:8F	10.1.1.249	Local Portal
00:0C:29:30:7E:6A	10.1.1.1	Guest Gateway

249 |

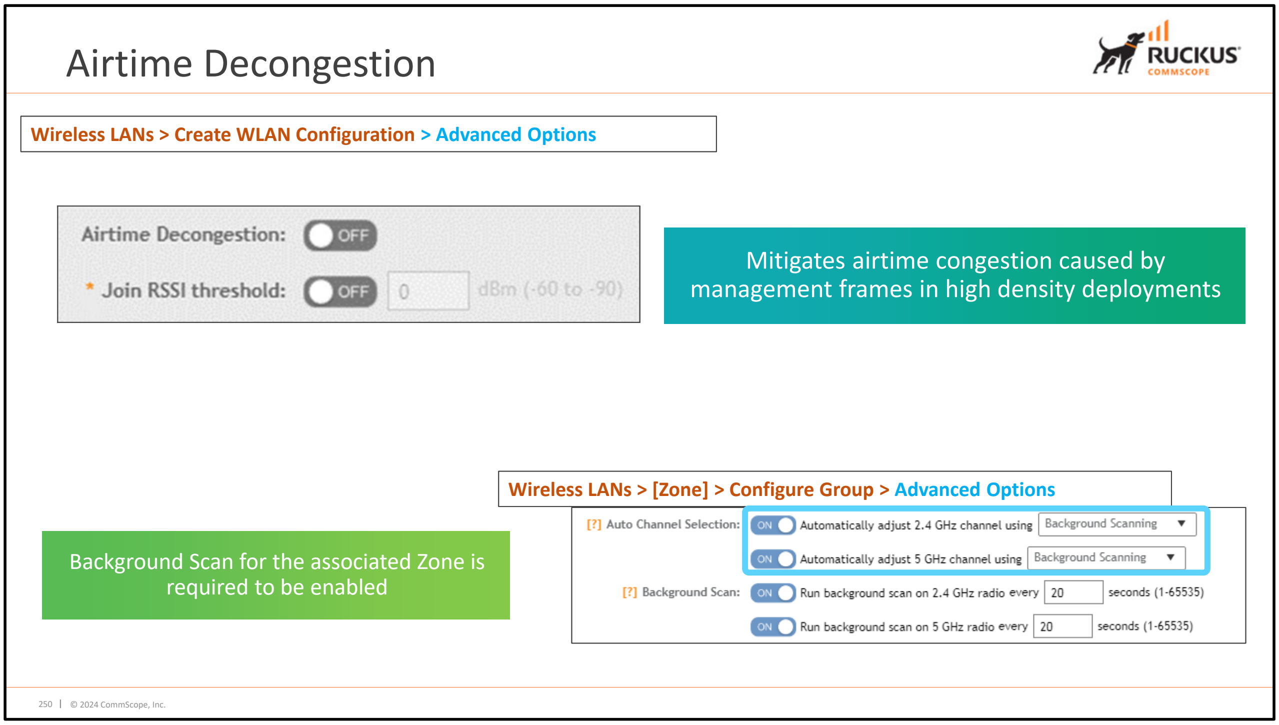
Wireless Client Isolation is disabled by default on standard WLANs, but is enabled on other WLAN types. A best practice is to always check the settings.

- **Disabled** - devices are able to see all other devices on the subnet.
- **Enabled** - devices are blocked from seeing other devices on the VLAN/subnet.

Customized access by the use of the Whitelist allows you to control what devices users can access such as a specific printer or portal. You can customize device access within a WLAN by configuring whitelists. A default whitelist is created which allows gateway access through autodiscovery of the gateway of the WLAN or you can configure your own list by clicking on the "+" or navigating to **Services & Profiles > Access Control > Client Isolation Whitelist**.

Additional options that appear when enabled include the ability to isolate unicast or multicast/broadcast traffic on the WLAN. Automatic support for VRRP/HSRP allowing the gateways to be identified can be enabled as well.

You can also select a priority for client traffic which is set to High by default. Priority relates to SmartCast Traffic Quality of Service. The default for all WLANs is **High**. You may select **Low** if you are working with advanced QoS settings and want to influence network traffic, however this is an advanced subject. If it's something you're interested in, you should refer to the RUCKUS website for more information on SmartCast.



Airtime Decongestion

Wireless LANs > Create WLAN Configuration > Advanced Options

Airtime Decongestion: OFF

* Join RSSI threshold: OFF 0 dBm (-60 to -90)

Mitigates airtime congestion caused by management frames in high density deployments

Wireless LANs > [Zone] > Configure Group > Advanced Options

[?] Auto Channel Selection: ON Automatically adjust 2.4 GHz channel using Background Scanning ▼

ON Automatically adjust 5 GHz channel using Background Scanning ▼

[?] Background Scan: ON Run background scan on 2.4 GHz radio every 20 seconds (1-65535)

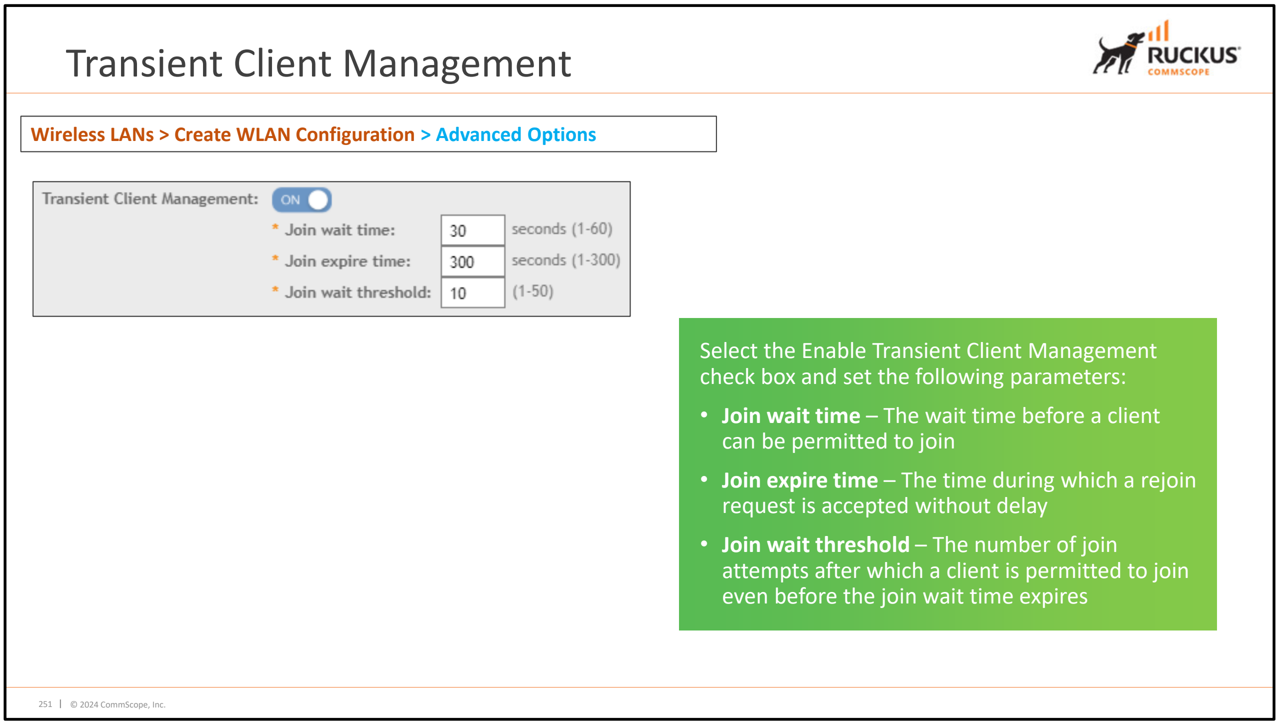
ON Run background scan on 5 GHz radio every 20 seconds (1-65535)

Background Scan for the associated Zone is required to be enabled

250 | © 2024 CommScope, Inc.

The **Airtime Decongestion** feature optimizes the Wi-Fi management traffic in a network where the amount of management traffic can potentially consume a significant portion of airtime thereby reducing the amount of time available for user data traffic. This feature controls the RSSI threshold setting for Transient Client Management. Enabling this feature disables the **RSSI threshold** configuration in **Transient Client Management**.

To ensure proper function confirm that **Background Scan** is enabled.



Transient Client Management

Wireless LANs > Create WLAN Configuration > Advanced Options

Transient Client Management: ON

* Join wait time: 30 seconds (1-60)

* Join expire time: 300 seconds (1-300)

* Join wait threshold: 10 (1-50)

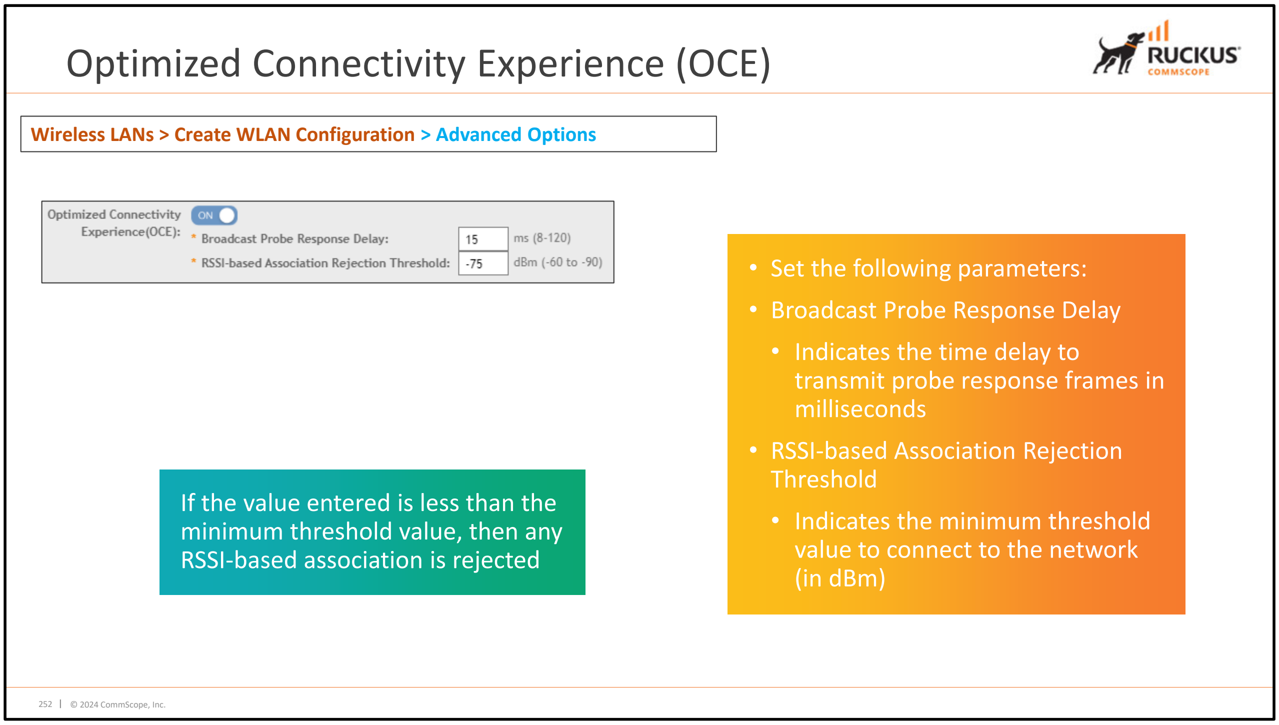
Select the Enable Transient Client Management check box and set the following parameters:

- **Join wait time** – The wait time before a client can be permitted to join
- **Join expire time** – The time during which a rejoin request is accepted without delay
- **Join wait threshold** – The number of join attempts after which a client is permitted to join even before the join wait time expires

251 | © 2024 CommScope, Inc.

The Transient Client Management feature allows only those clients that stay within the AP's coverage region for a minimum period of time to associate with the AP and use the service. Simply put it discourages transient clients (such as passing motorists or train passengers passing through a station) from joining the network in environments where passing traffic will not attempt to connect once discovered.

Transient Client management uses statistical methods to delay the association of transient clients to an AP. Select the **Enable Transient Client Management** check box and set the parameters that provides the best to tune configuration parameters based on typical observed dwell times and RSSI of transient clients.



Optimized Connectivity Experience (OCE)

Wireless LANs > Create WLAN Configuration > Advanced Options

Optimized Connectivity Experience(OCE): ON
- * Broadcast Probe Response Delay: 15 ms (8-120)
- * RSSI-based Association Rejection Threshold: -75 dBm (-60 to -90)

If the value entered is less than the minimum threshold value, then any RSSI-based association is rejected

- Set the following parameters:
- Broadcast Probe Response Delay
  - Indicates the time delay to transmit probe response frames in milliseconds
- RSSI-based Association Rejection Threshold
  - Indicates the minimum threshold value to connect to the network (in dBm)

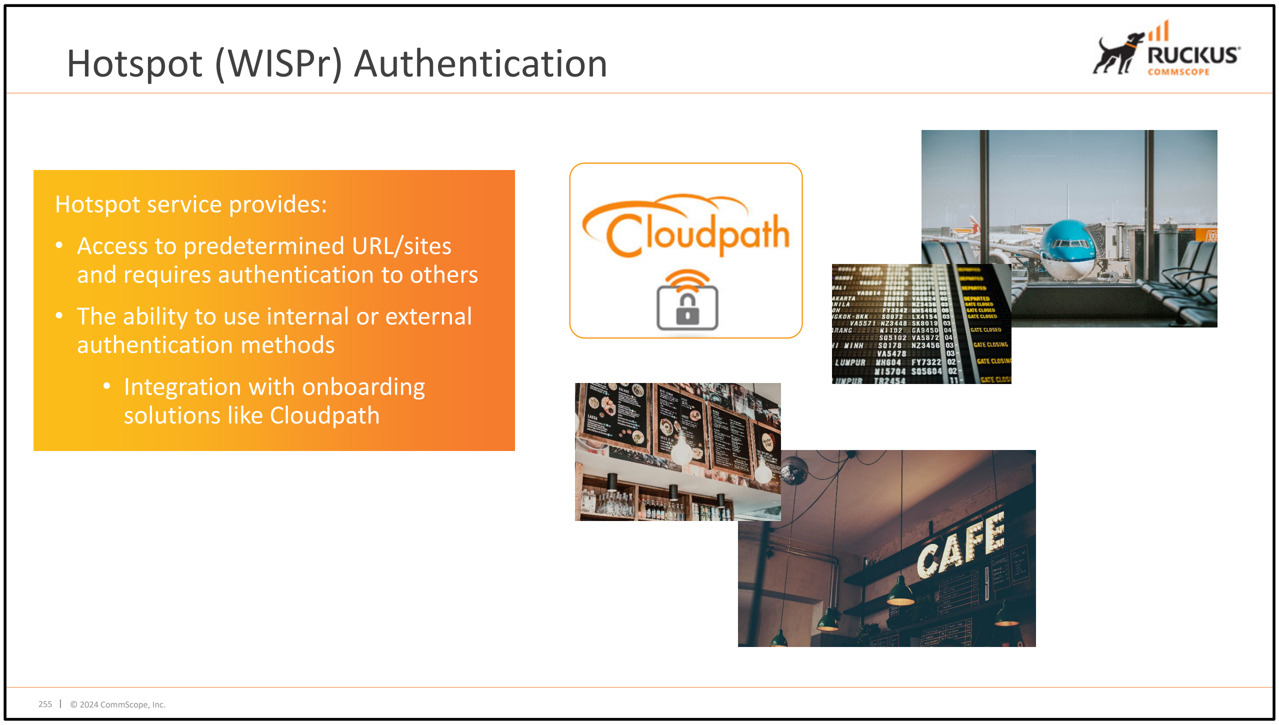
252 | © 2024 CommScope, Inc.

Optimized Connectivity Experience (OCE) delivers a better overall connectivity experience by enabling probe response suppression and by preventing devices with marginal connectivity to join the network.

When OCE is enabled, the affected APs and stations are excluded from Airtime Decongestion and Transient Client Management, resulting in reduction in probe response. Probe response suppression optimizes airtime for data traffic. OCE solves connectivity issues by rejecting any association with clients with poor signals.

SmrtZone Security and access control features

Configuring security policies



Hotspot (WISPr) Authentication

Hotspot service provides:

- Access to predetermined URL/sites and requires authentication to others
- The ability to use internal or external authentication methods
  - Integration with onboarding solutions like Cloudpath

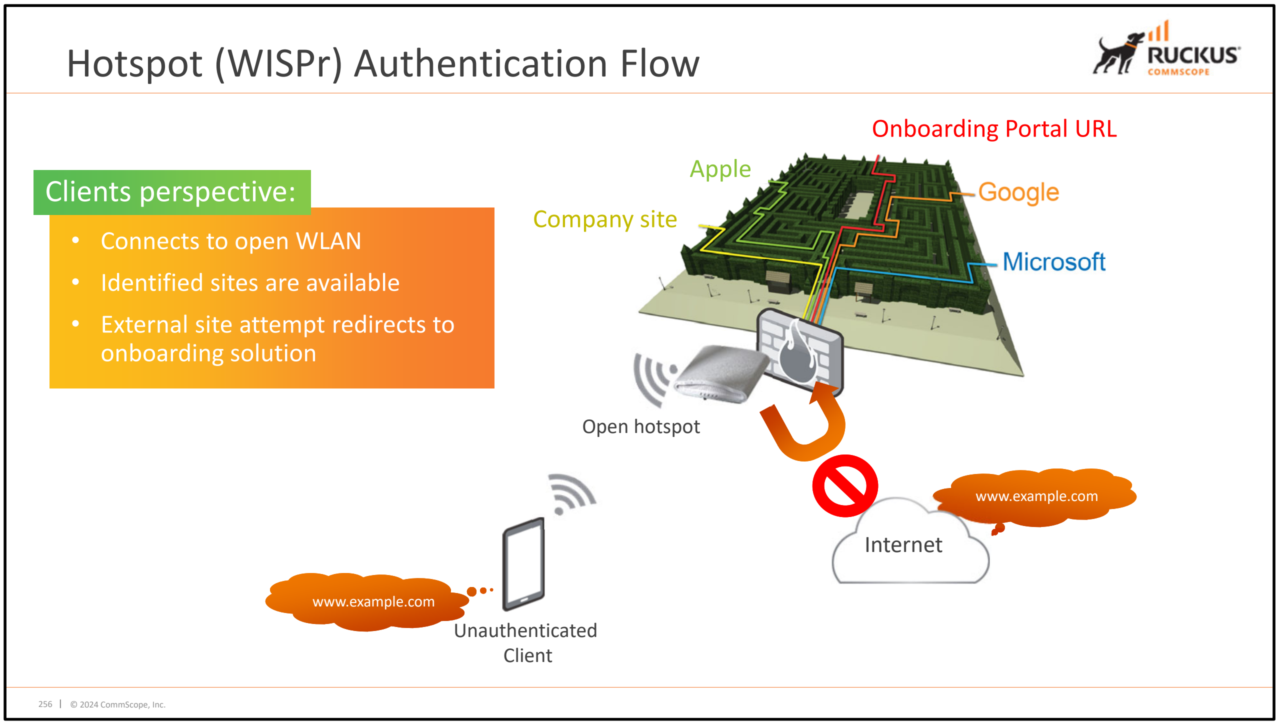
Cloudpath
CAFE

255 | © 2024 CommScope, Inc.

Hotspot WLANs known as Wireless Internet Service Providers roaming (WISPr) are similar to Web Authentication WLANs however, you have the additional option of specifying a “Walled Garden”. A Walled Garden allows you to give access to a select group of websites while requiring authentication for the rest. It also allows flexibility to either use a SZ internal authentication system or an external solution such as RUCKUS Networks Cloudpath onboarding solution. Using onboarding solutions like Cloudpath provides a self service automated onboarding process which is very effective when large amount of devices such as colleges or a large enterprise needs to effectively onboard and manage users. Other effective uses for a Hotspot service is:

When you want users to be able to access your website while on premises for things such as company instructions or directory access. It can be effective for museums for admission information or current exhibits or as simple as a menu for café all accessible without having to authenticate however still protecting access to other public sites.

Other options could be for airports where they want to have the flight status boards or terminal maps accessible but require authentication for outside sites or even charge for public access.



Hotspot (WISPr) Authentication Flow

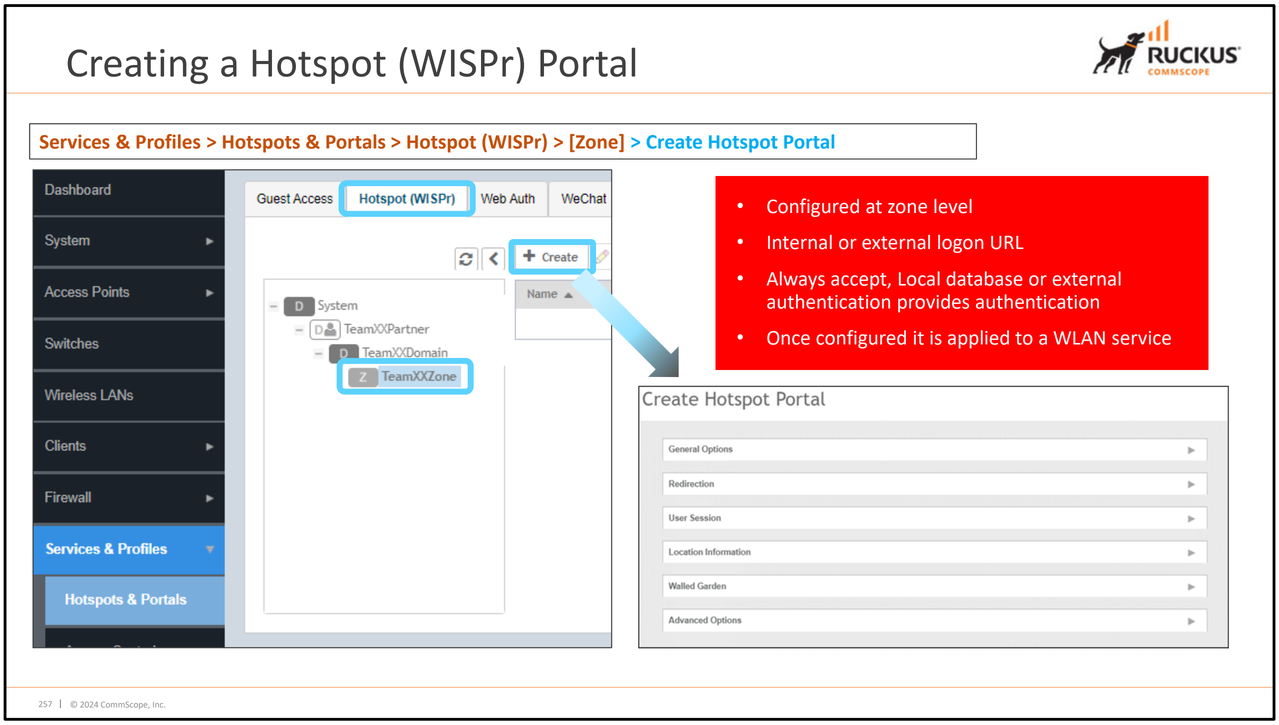
Clients perspective:

- Connects to open WLAN
- Identified sites are available
- External site attempt redirects to onboarding solution

256 | © 2024 CommScope, Inc.

The process starts with an open hotspot allowing users to connect. Once connected it is determined if the user has been previously authorized and if not they are placed in the walled garden allowing access to only sites identified. If the user attempts to access a site outside the walled garden list then they are redirected to an onboarding or authentication page where they can enter their credentials or onboard their device.

Onboarding solutions like Cloudpath provide other authentication options like the ability to use OAuth authentication from social media sites such as Facebook, Google or LinkedIn before they are allowed to access public URLs.



Creating a Hotspot (WISPr) Portal

Services & Profiles > Hotspots & Portals > Hotspot (WISPr) > [Zone] > Create Hotspot Portal

- Configured at zone level
- Internal or external logon URL
- Always accept, Local database or external authentication provides authentication
- Once configured it is applied to a WLAN service

Hotspot WISPr portals are created under **Services & Profiles > Hotspots & Portals**, and this time selecting the **Hotspot (WISPr)** tab.

Hotspot WISPr Portals are created at the Zone level, so select the Zone where you would like to have the portal and click **Create**

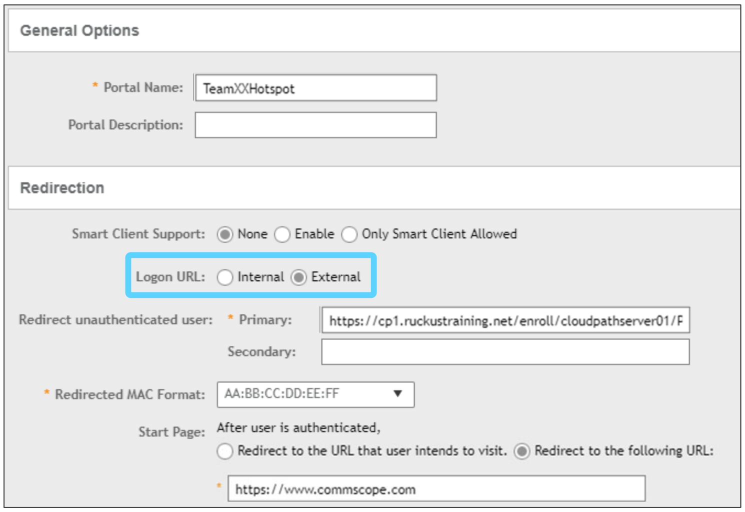
Options allow you to use either the internal site within SmartZone which will prompt for user credentials or an external site that will provide that service. When using an external site you will configure a redirect towards that site when a client is not previously authenticated or their access has expired.

There are choices on which to use for authentication sources. One option (**Always Accept)** Grants access to all users and is typically used when only acceptance of terms of service is required for WLAN access. Other options include using the local database which is manually populated in SmartZone. The last option is to use an external authentication service which is configured under Services & Profiles > Authentication where RADIUS, Active Directory and LDAP services can be configured.

Once the Hotspot service is configured it is then associated with a WLAN to direct unauthorized users to the correct portal for authentication.

Configuring a Hotspot (WISPr) Portal

Services & Profiles > Hotspots & Portals > Hotspot (WISPr) > [Zone] > Create Hotspot Portal



General Options

* Portal Name: TeamXXHotspot

Portal Description:

Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user: * Primary: https://cp1.ruckustraining.net/enroll/cloudpathserver01/F

Secondary:

* Redirected MAC Format: AA:BB:CC:DD:EE:FF

Start Page: After user is authenticated,
○ Redirect to the URL that user intends to visit. ● Redirect to the following URL:

* https://www.commscope.com

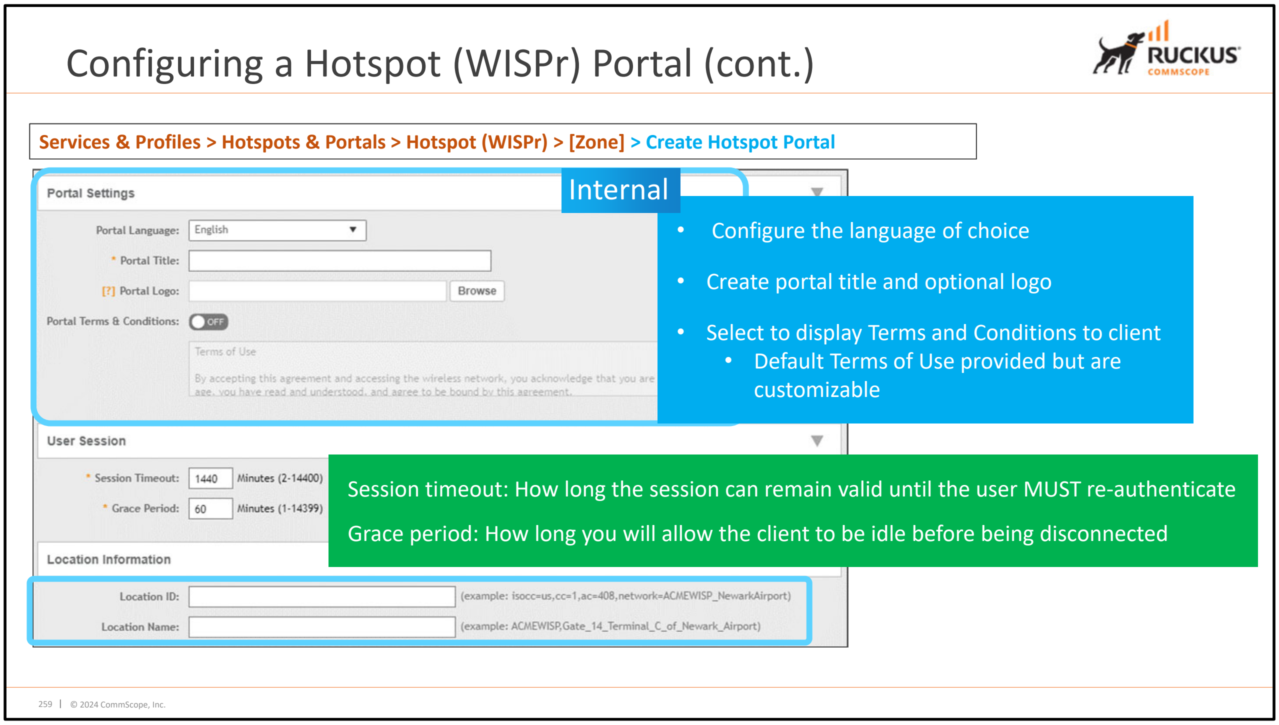
- Provide a portal name
- Logon URL
  - Internal Logon
    - SmartZone portal
  - External Logon
    - 3rd party portal
- 3rd Party Redirect of unauthenticated user
  - Primary & Secondary
- Start Page
  - Redirect URL

258 | © 2024 CommScope, Inc.

Under the General Options window giving your Hotspot (WISPr) Portal an Identifiable name and optionally, a description.

Under the Redirection section, select the login URL you plan to use for the users. This can be the internal, inbuilt portal in the SmartZone which requires the naming, language selection and optional logo, or you can refer the authentication to an external logon server. If an external URL is chosen you'll need to specify at least one external URL. There is also an option to configure a secondary redirect server if the primary server is not reachable allowing unauthenticated users will be redirected to the secondary server.

Finally, decide if you want users to continue to the web page they were trying to visit, if they should be redirected to a specific page.



Configuring a Hotspot (WISPr) Portal (cont.)

Services & Profiles > Hotspots & Portals > Hotspot (WISPr) > [Zone] > Create Hotspot Portal

Portal Settings

Portal Language:	English ▾
* Portal Title:	
[?] Portal Logo:	Browse
Portal Terms & Conditions:	OFF

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are age, you have read and understood, and agree to be bound by this agreement.

User Session

* Session Timeout:	1440	Minutes (2-14400)
* Grace Period:	60	Minutes (1-14399)

Location Information

Location ID:		(example: isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport)
Location Name:		(example: ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport)

Internal

- Configure the language of choice
- Create portal title and optional logo
- Select to display Terms and Conditions to client
  - Default Terms of Use provided but are customizable

Session timeout: How long the session can remain valid until the user MUST re-authenticate

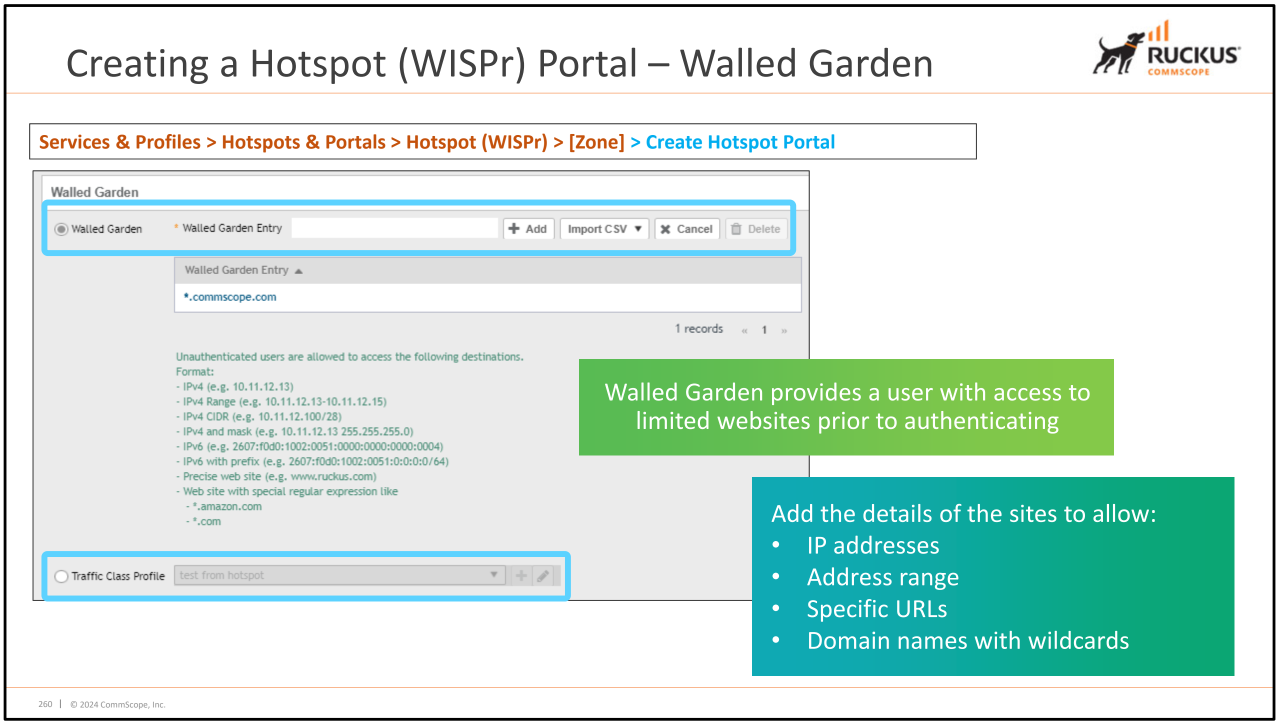
Grace period: How long you will allow the client to be idle before being disconnected

259 | © 2024 CommScope, Inc.

If an internal URL is chosen previously for client redirection, additional portal settings will be required which include the preferred language to be displayed along with a portal title and optional logo. If no customized logo is chosen the RUCKUS logo will be used instead. The portal terms of use can be enabled and displayed to the user for approval and can be customized to fit the organizations requirements.

For both internal or external in the User Session section, specify the user session timeout and grace period in minutes. The default times are shown in the example.

- The Session Timeout specifies how long the session can remain valid until the user MUST re-authenticate.
- The Grace Period specifies how long you will allow the client to be idle before being disconnected.



Creating a Hotspot (WISPr) Portal – Walled Garden

Services & Profiles > Hotspots & Portals > Hotspot (WISPr) > [Zone] > Create Hotspot Portal

Walled Garden

● Walled Garden * Walled Garden Entry

Walled Garden Entry ▲
*.commscope.com

1 records « 1 »

Unauthenticated users are allowed to access the following destinations.
Format:
- IPv4 (e.g. 10.11.12.13)
- IPv4 Range (e.g. 10.11.12.13-10.11.12.15)
- IPv4 CIDR (e.g. 10.11.12.100/28)
- IPv4 and mask (e.g. 10.11.12.13 255.255.255.0)
- IPv6 (e.g. 2607:f0d0:1002:0051:0000:0000:0000:0004)
- IPv6 with prefix (e.g. 2607:f0d0:1002:0051:0:0:0:0/64)
- Precise web site (e.g. www.ruckus.com)
- Web site with special regular expression like
  - *.amazon.com
  - *.com

○ Traffic Class Profile: test from hotspot

Walled Garden provides a user with access to limited websites prior to authenticating

Add the details of the sites to allow:
- IP addresses
- Address range
- Specific URLs
- Domain names with wildcards

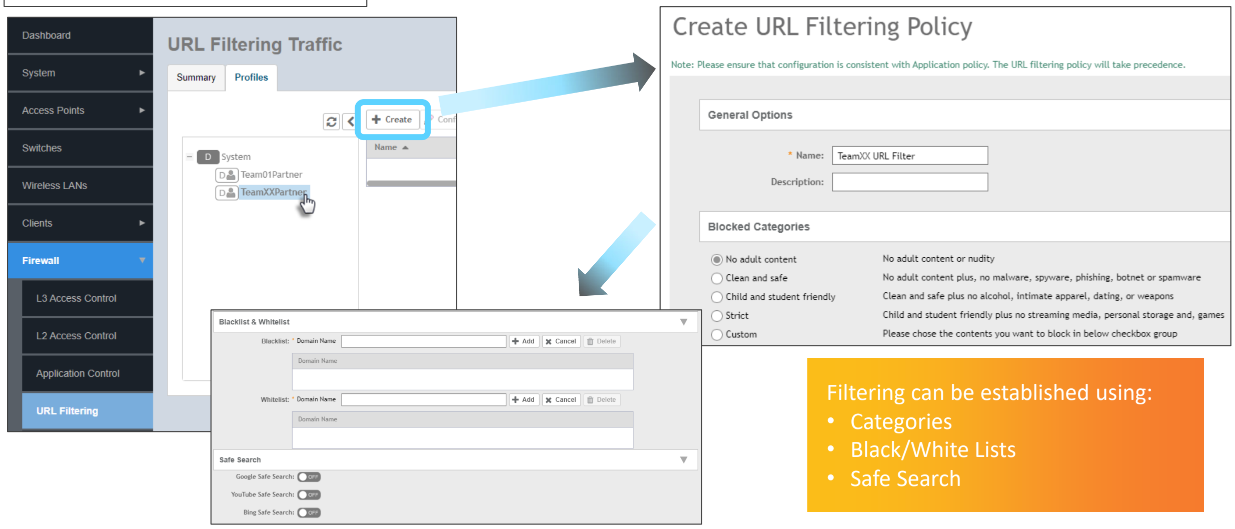
260 | © 2024 CommScope, Inc.

The Walled Garden provides the user with access to identified websites prior to requiring authentication. This can be used to allow access to certain internal websites or specific access. As mentioned before if used with Cloudpath the walled garden would include access to the device app stores to allow the download of the install app of Cloudpath or for other uses. To allow access to a site you simply add the URL of the sites you want to allow. You can specify IP addresses, IP address ranges, specific URLs, or domain names with wildcards.

Optionally you can use a Traffic Class Profile which has been developed to accommodate the Express WiFi service a Facebook offering to mobile network operators and internet service providers to help them better provide fast, affordable, reliable, and scalable internet access for everyone. More details about Facebooks expresswifi can be found at expresswifi.fb.com/about or in SmartZone documentation. Once all these objects for the WISPr hotspot portal has been configured click save and you can now associate it to a WLAN interface which we will do next.

URL Filtering Policy

Firewall > URL Filtering > Profiles



Create URL Filtering Policy

Note: Please ensure that configuration is consistent with Application policy. The URL filtering policy will take precedence.

General Options

* Name: TeamXX URL Filter

Description:

Blocked Categories

● No adult content	No adult content or nudity
○ Clean and safe	No adult content plus, no malware, spyware, phishing, botnet or spamware
○ Child and student friendly	Clean and safe plus no alcohol, intimate apparel, dating, or weapons
○ Strict	Child and student friendly plus no streaming media, personal storage and, games
○ Custom	Please chose the contents you want to block in below checkbox group

Blacklist & Whitelist

Blacklist: * Domain Name [ ] Add Cancel Delete

Domain Name

Whitelist: * Domain Name [ ] Add Cancel Delete

Domain Name

Safe Search

Google Safe Search: OFF

YouTube Safe Search: OFF

Bing Safe Search: OFF

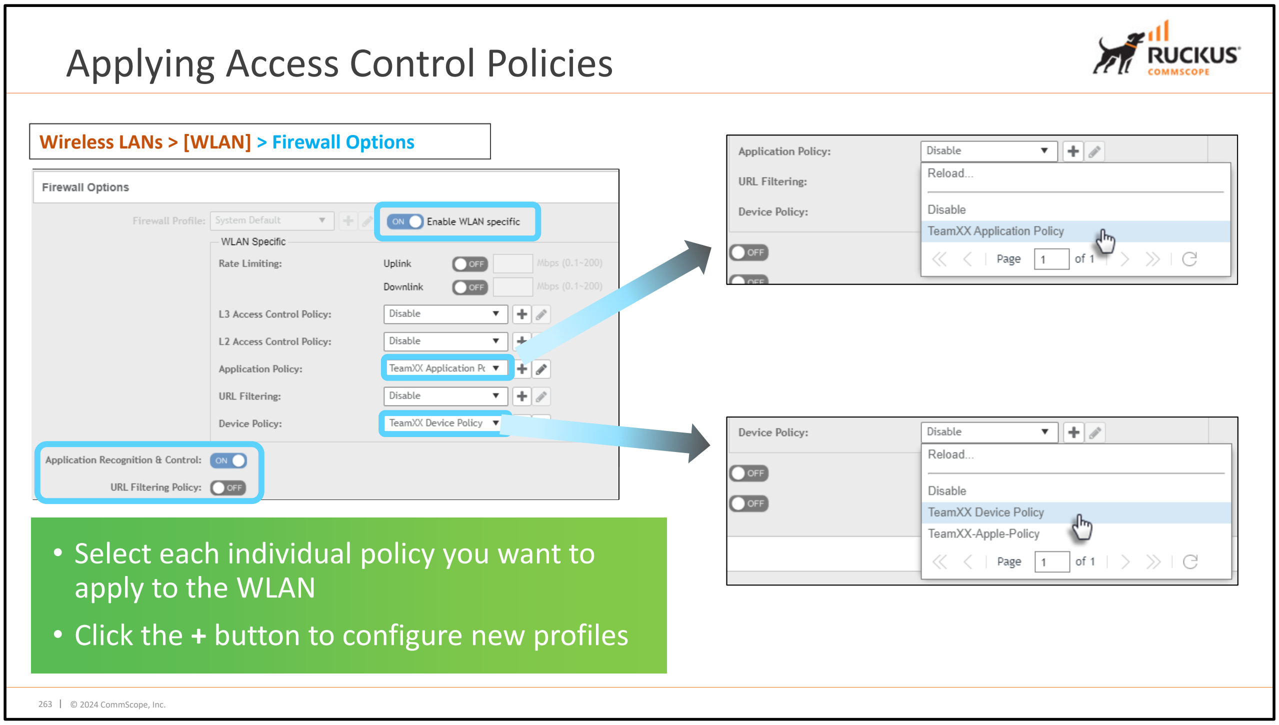
Filtering can be established using:
- Categories
- Black/White Lists
- Safe Search

262 | © 2024 CommScope, Inc.

The URL filtering feature allows for the blocking of inappropriate websites that you can define. A unique URL filtering policy can be created or pre-existing URL settings can be applied. When this policy is applied to a WLAN, filtering of identified traffic within the URL filtering policy will be applied.

To configure a URL filtering policy, navigate to Firewall > URL Filtering, select the Profiles tab, select the domain where the policy will be available and then click Create. To define the filtering policy, you can identify URLs by categories, set up black or white lists and employ safe search options.

URL filtering requires a separate URL license which can be added over time. Please refer to the SZ administrators guide for more details about URL filtering and licensing.



Applying Access Control Policies

Wireless LANs > [WLAN] > Firewall Options

Firewall Options

Firewall Profile: System Default

ON Enable WLAN specific

WLAN Specific

Rate Limiting: Uplink OFF Mbps (0.1~200)

Downlink OFF Mbps (0.1~200)

L3 Access Control Policy: Disable

L2 Access Control Policy: Disable

Application Policy: TeamXX Application Pc

URL Filtering: Disable

Device Policy: TeamXX Device Policy

Application Recognition & Control: ON

URL Filtering Policy: OFF

Application Policy: Disable

URL Filtering:

Device Policy:

Reload...

Disable

TeamXX Application Policy

Page 1 of 1

Device Policy: Disable

Reload...

Disable

TeamXX Device Policy

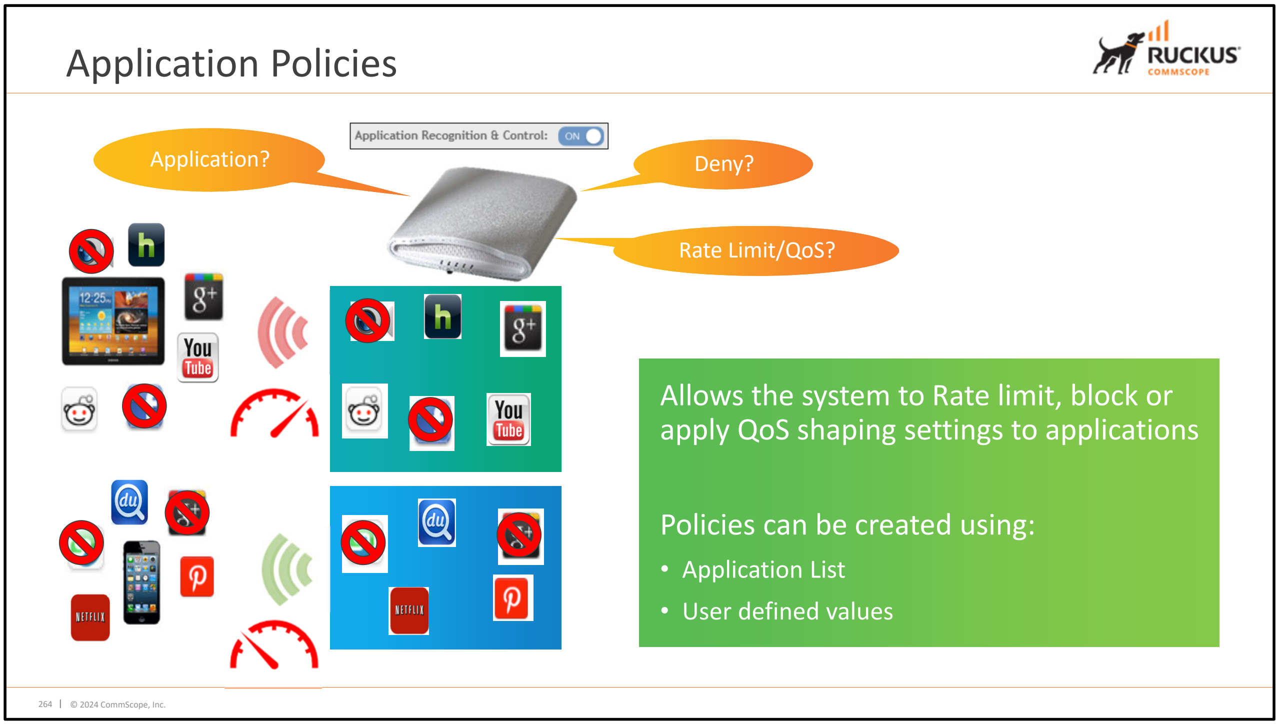
TeamXX-Apple-Policy

Page 1 of 1

- Select each individual policy you want to apply to the WLAN
- Click the **+** button to configure new profiles

263 | © 2024 CommScope, Inc.

To apply individual policies to a WLAN, turn on the **Enable WLAN specific** option. Each policy type now has a drop-down box to select one of the pre-configured policies to apply or a new policy can be created by clicking the + sign. As with Firewall Profiles, Application Recognition & Control and URL Filtering must be enabled for an application or URL filtering policy, respectively, to be enforced.



Application Policies

Allows the system to Rate limit, block or apply QoS shaping settings to applications

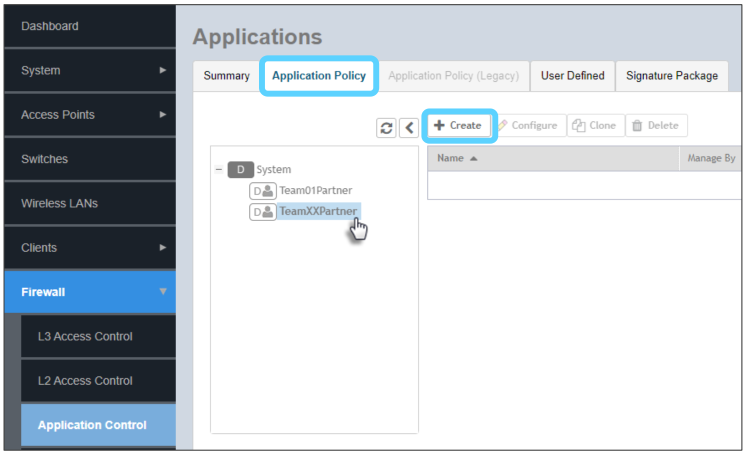
Policies can be created using:

- Application List
- User defined values

Application policies allow you to leverage the information collected through Application Recognition & Control. Because the applications can be identified and monitored, you can control access to them. Application policies provide you with a mechanism to block specific applications. Alternatively, you can apply rate limiting or Quality of Service settings to allow high-speed throughput to one policy while limiting bandwidth to another.

Creating Application Policies

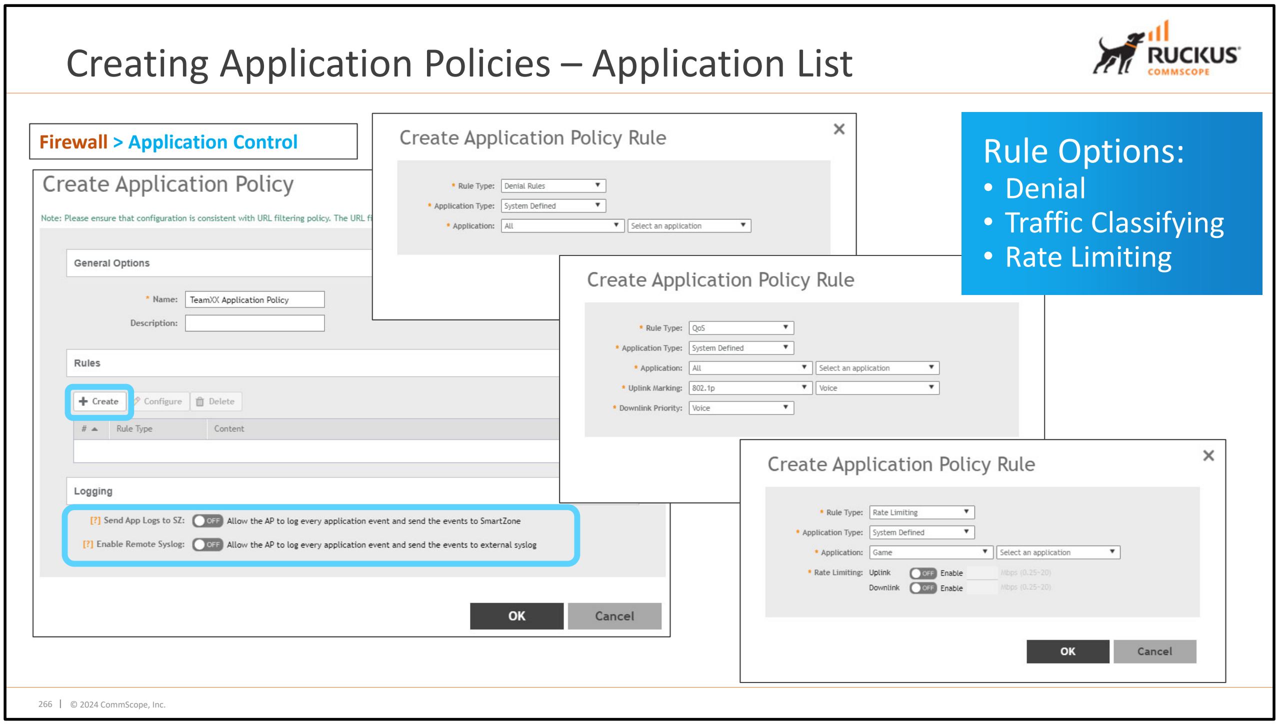
Firewall > Application Control > Application Policy



- Configured at the Domain level in High Scale deployments
- Application list or User Defined application control
- Multiple rules can be applied under a single policy

265 |

Like L2/3 Access policies, Application policies are configured from the domain perspective. As mentioned, the policies can be configured using a system defined application list or by a User Defined application rule. However’ both can be included in a single application policy. To create your application policy, select your domain and click the Create button.



Creating Application Policies – Application List

Firewall > Application Control

Create Application Policy

Note: Please ensure that configuration is consistent with URL filtering policy. The URL fi

General Options

* Name: TeamXX Application Policy

Description:

Rules

Logging

[?] Send App Logs to SZ: OFF Allow the AP to log every application event and send the events to SmartZone

[?] Enable Remote Syslog: OFF Allow the AP to log every application event and send the events to external syslog

Create Application Policy Rule

* Rule Type: Denial Rules

* Application Type: System Defined

* Application: All | Select an application

Create Application Policy Rule

* Rule Type: QoS

* Application Type: System Defined

* Application: All | Select an application

* Uplink Marking: 802.1p | Voice

* Downlink Priority: Voice

Create Application Policy Rule

* Rule Type: Rate Limiting

* Application Type: System Defined

* Application: Game | Select an application

* Rate Limiting: Uplink OFF Enable Mbps (0.25~20)

Downlink OFF Enable Mbps (0.25~20)

Rule Options:

- Denial
- Traffic Classifying
- Rate Limiting

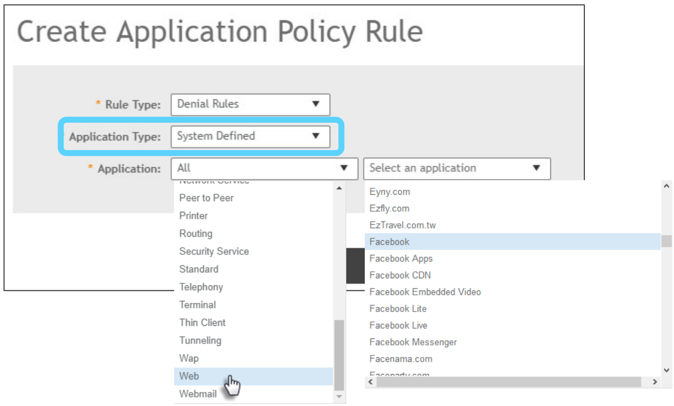
266 |

In the Create Application Policy window that appears, provide a name for the policy. Next, rules can be defined by selecting **Create** under the **Rules** section. Rule options include Denial Rules, QoS and Rate limiting which we will look at in more detail in the following slides.

Optionally, you can send App Logs to SZ as well as sending logging information to an external syslog system. Prerequisites must be configured to allow these operations, including the enabling of SmartZone event management and an external syslog server defined under **System > General Settings > Syslog**.

Creating Application Policies – Deny Rules

Firewall > Application Control > Application Policy > Create Application Policy Rule



Create Application Policy Rule

* Rule Type: Denial Rules

Application Type: System Defined

* Application: All

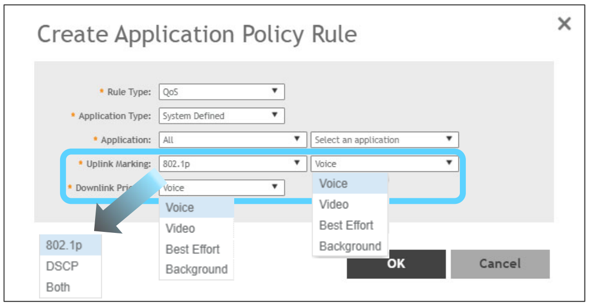
Select an application

- Rule Type: Denial Rules
- Use a system defined or user defined application
  - For a system defined application, choose the desired application
- The rule is added to the Application Policy

Selecting the **Rule Type** to **Denial Rules** Select an **Application Type**, either **System Defined** or **User Defined**. For a system defined application, choose the desired application from the **Application** drop-down list. When you select a category, for instance **Web**, the applications list will display only web-based applications like Facebook or other websites. Choose the desired application and click **OK**. The rule is added to the list, and can be edited or deleted.

Creating Application Policies – QoS

Firewall > Application Control > Application Policy > Create Application Policy Rule



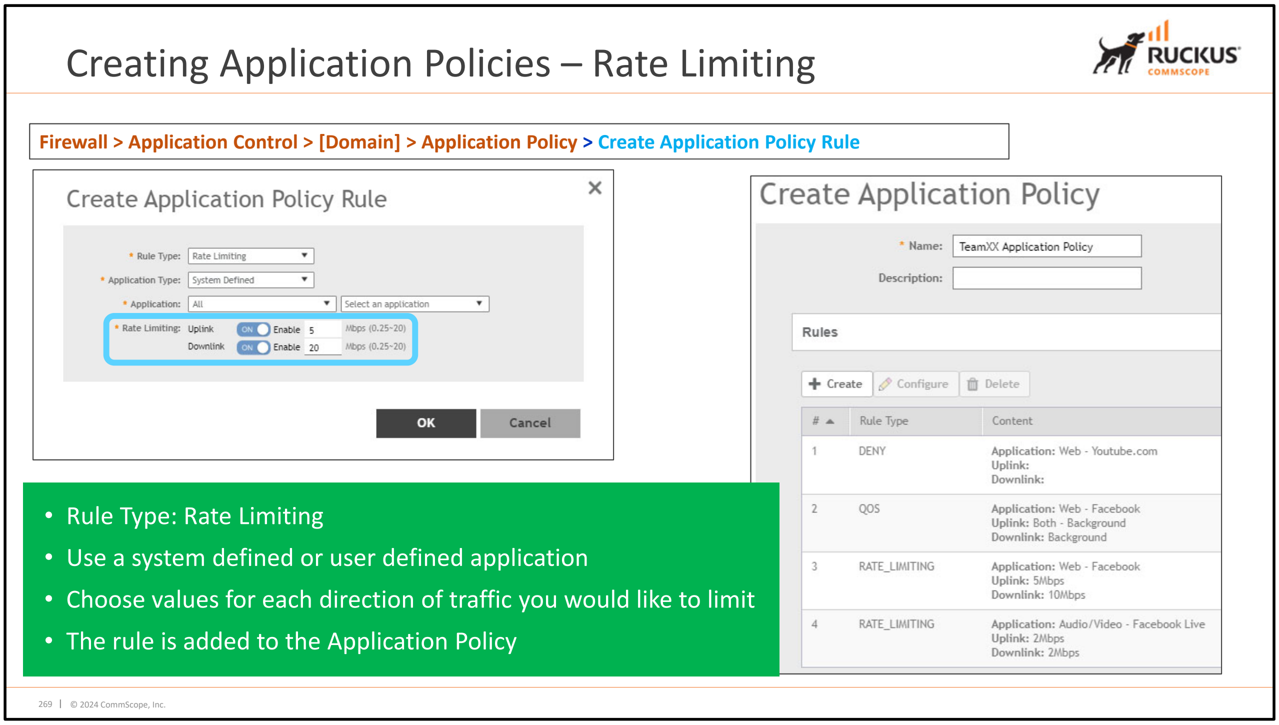
Create Application Policy Rule

- Rule Type: QoS
- Application Type: System Defined
- Application: All | Select an application
- Uplink Marking: 802.1p | Voice
- Downlink Priority: Voice

- Rule Type: QoS
- Use a system defined or user defined application
- Select Uplink Marking for client traffic
- Select Downlink Priority Marking
- The rule is added to the Application Policy

|

For QoS marking, select the Rule Type as QoS, then select the applications you want to filter. Options allow you to select the type of markings either 802.1p, DSCP or both and then the value placed on the traffic. Likewise you can separately choose the downlink marking of the traffic as it is sent out to the client. Once configured click **OK** and the rule is added to the list where it can be edited or deleted here.



Creating Application Policies – Rate Limiting

Firewall > Application Control > [Domain] > Application Policy > Create Application Policy Rule

Create Application Policy Rule

- * Rule Type: Rate Limiting
- * Application Type: System Defined
- * Application: All | Select an application
- * Rate Limiting: Uplink ON Enable 5 Mbps (0.25~20)
- Downlink ON Enable 20 Mbps (0.25~20)

- Rule Type: Rate Limiting
- Use a system defined or user defined application
- Choose values for each direction of traffic you would like to limit
- The rule is added to the Application Policy

Create Application Policy

* Name: TeamXX Application Policy

Description:

Rules

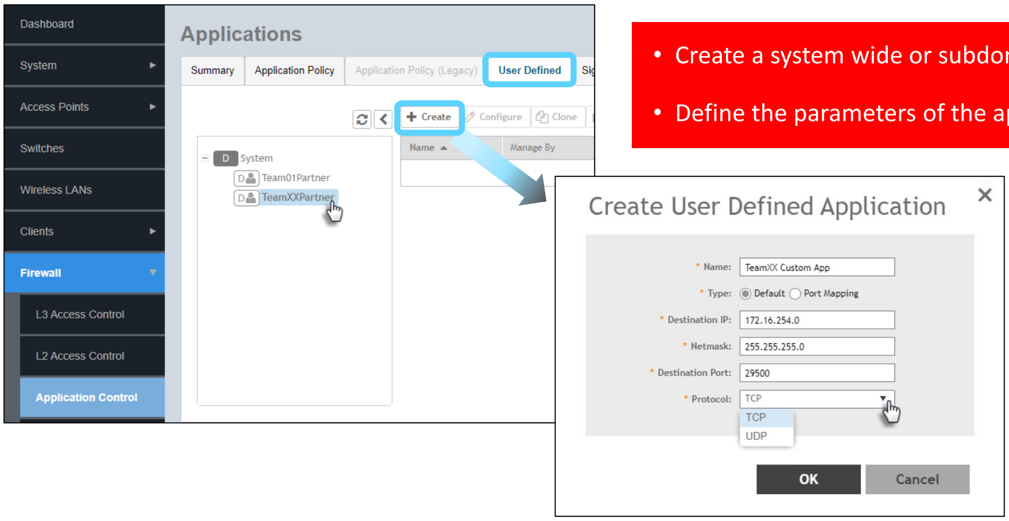
#	Rule Type	Content
1	DENY	**Application:** Web - Youtube.com **Uplink:** **Downlink:**
2	QOS	**Application:** Web - Facebook **Uplink:** Both - Background **Downlink:** Background
3	RATE_LIMITING	**Application:** Web - Facebook **Uplink:** 5Mbps **Downlink:** 10Mbps
4	RATE_LIMITING	**Application:** Audio/Video - Facebook Live **Uplink:** 2Mbps **Downlink:** 2Mbps

269 | © 2024 CommScope, Inc.

When using the **Rate Limiting** option, select an Application to be filtered, then select the rates you would like to control for the app. Once your values have been entered click **OK**. The rule is added to the list and can be edited or deleted. Also note that multiple rules for the same application can be configured within a policy imposing multiple aspects of control over it.

User Defined Application

Firewall > Application Control > [Domain] > User Defined



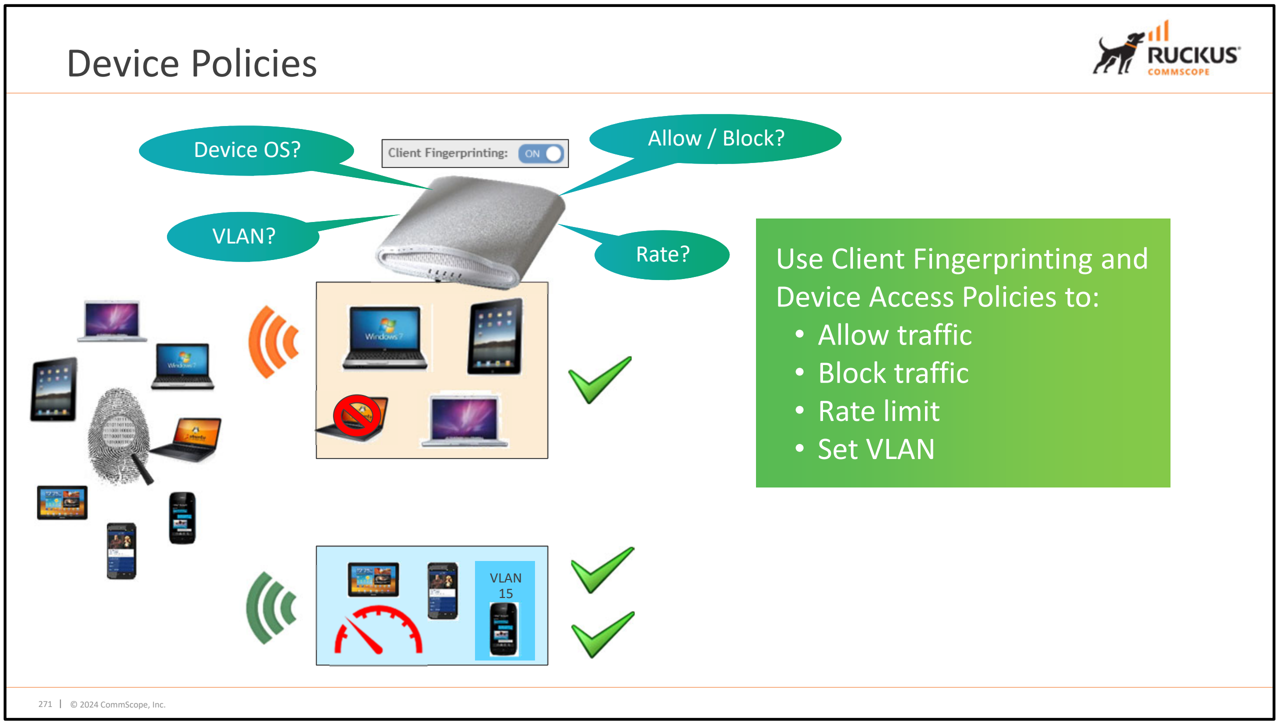
Create User Defined Application

- * Name: TeamXX Custom App
- * Type: ● Default ○ Port Mapping
- * Destination IP: 172.16.254.0
- * Netmask: 255.255.255.0
- * Destination Port: 29500
- * Protocol: TCP

- Create a system wide or subdomain application
- Define the parameters of the application

Sometimes the system isn’t able to identify the application. This is common when devices are accessing a proprietary device or service. In this case, you can create a User Defined application to identify the traffic destination by name. The Dashboard will use the configured name in displaying the application.

To create a user defined application, navigate to Firewall > Application Control, select the User Defined tab, then the domain and click Create. In the window that appears, enter a name for the application along with its details and click OK to save it.



Device Policies

Device OS?

Client Fingerprinting: ON

Allow / Block?

VLAN?

Rate?

VLAN 15

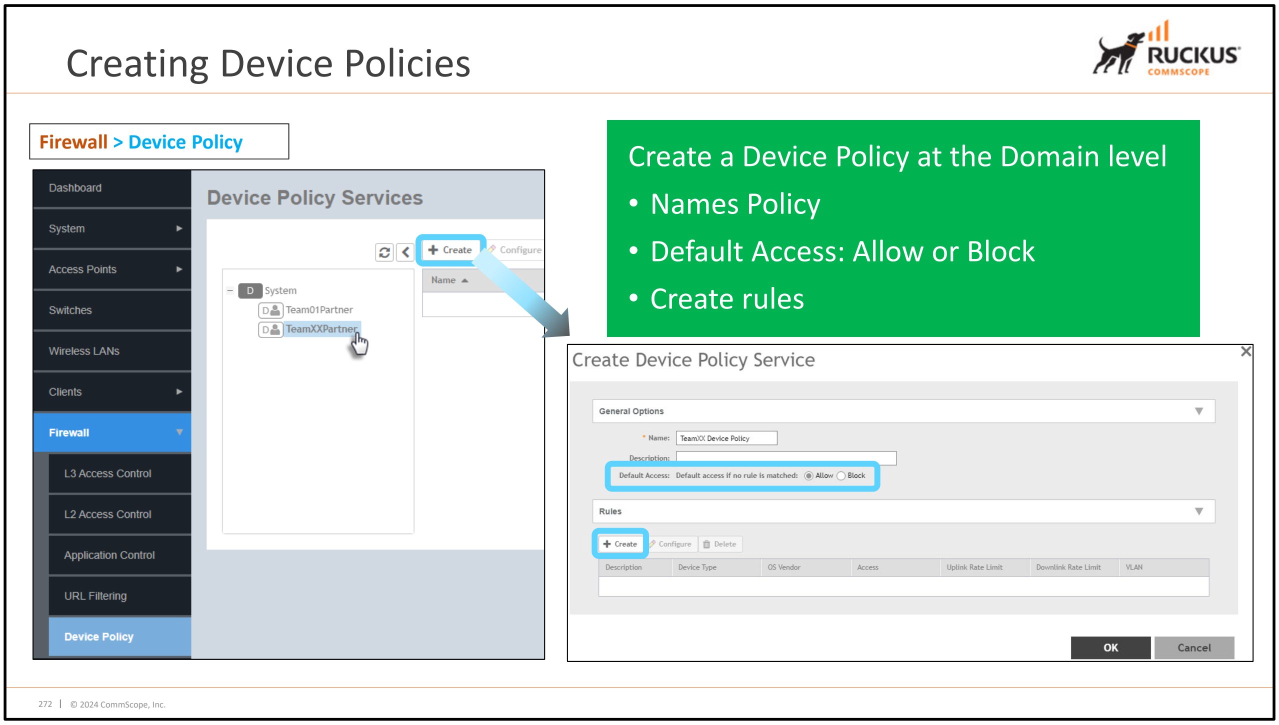
Use Client Fingerprinting and Device Access Policies to:

- Allow traffic
- Block traffic
- Rate limit
- Set VLAN

271 | © 2024 CommScope, Inc.

Device OS Policies allow you set policies based on the identified operating system type.

- With **Client Fingerprinting** enabled, the SmartZone will attempt to identify the client device type by OS.
- You can add rules to the policy allow or block traffic based on device type.
- You can apply rate limiting to specific device types only.
- You can assign specific device types to a VLAN.



Creating Device Policies

Firewall > Device Policy

Create a Device Policy at the Domain level

- Names Policy
- Default Access: Allow or Block
- Create rules

Create Device Policy Service

General Options

* Name: TeamXX Device Policy

Description:

Default Access: Default access if no rule is matched: ● Allow ○ Block

Rules

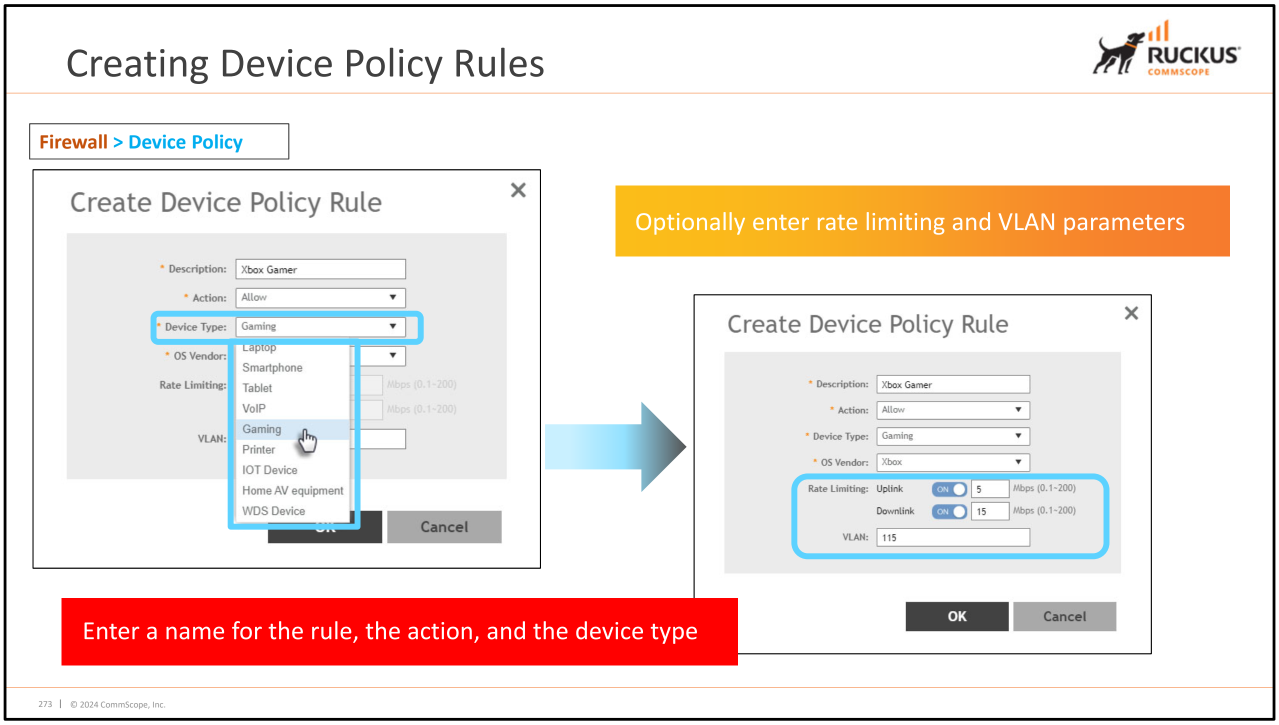
Description	Device Type	OS Vendor	Access	Uplink Rate Limit	Downlink Rate Limit	VLAN

272 |

To create an OS Policy, go to **Firewall > Device Policy**.

Device Policies are created at the domain level. To create a new Device Policy, select a Domain and click **Create**.

Enter a name for the policy and specify the default access of allow or block if no rule is met. Click **Create** to add the rules.



Creating Device Policy Rules

Firewall > Device Policy

Create Device Policy Rule

- * Description: Xbox Gamer
- * Action: Allow
- * Device Type: Gaming
- * OS Vendor:
- Rate Limiting: Mbps (0.1~200) / Mbps (0.1~200)
- VLAN:

Optionally enter rate limiting and VLAN parameters

Create Device Policy Rule

- * Description: Xbox Gamer
- * Action: Allow
- * Device Type: Gaming
- * OS Vendor: Xbox
- Rate Limiting: Uplink ON 5 Mbps (0.1~200)
- Downlink ON 15 Mbps (0.1~200)
- VLAN: 115

Enter a name for the rule, the action, and the device type

273 | © 2024 CommScope, Inc.

Enter a name, and under **Action**, select whether this is an Allow or Block rule. Remember, this will need to be consistent with the default access rule.

Select the device type from the drop-down list as well as the OS vendor you are wanting to control.

Optionally you can configure rate limiting and a VLAN for the rule. Click Ok and it will be added to the Device policy. Once all the devices you want to control are entered into the policy it will be ready to be applied to a WLAN.

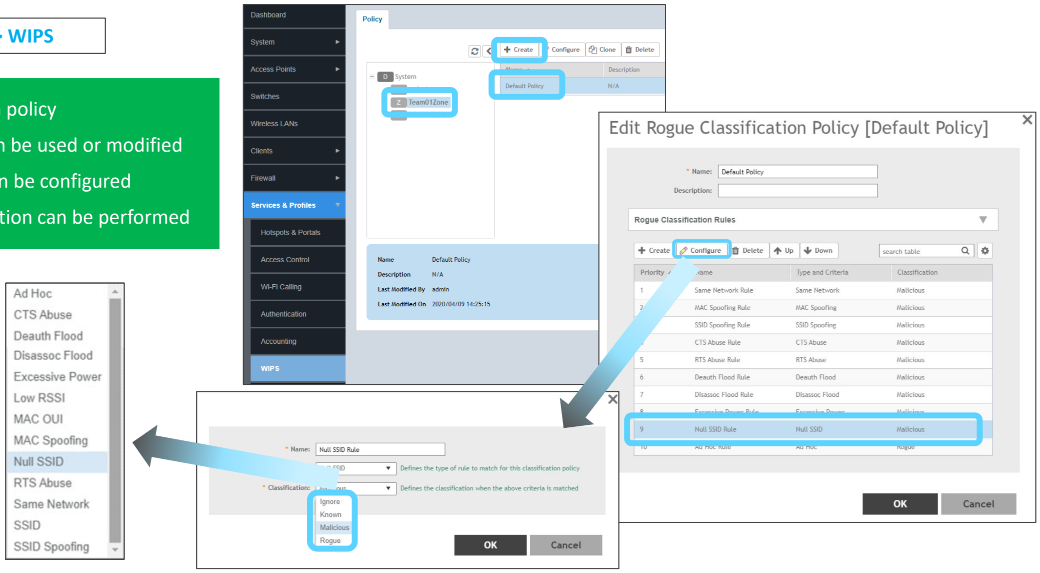
Rouge Device Detection

Rogue Device Policies

Services & Profiles > WIPS

Rogue Classification policy

- Default policy can be used or modified
- Custom policy can be configured
- Manual classification can be performed



Name: Default Policy
Description: N/A
Last Modified By: admin
Last Modified On: 2020/04/09 14:25:15

Edit Rogue Classification Policy [Default Policy]

* Name: Default Policy
Description:

Rogue Classification Rules

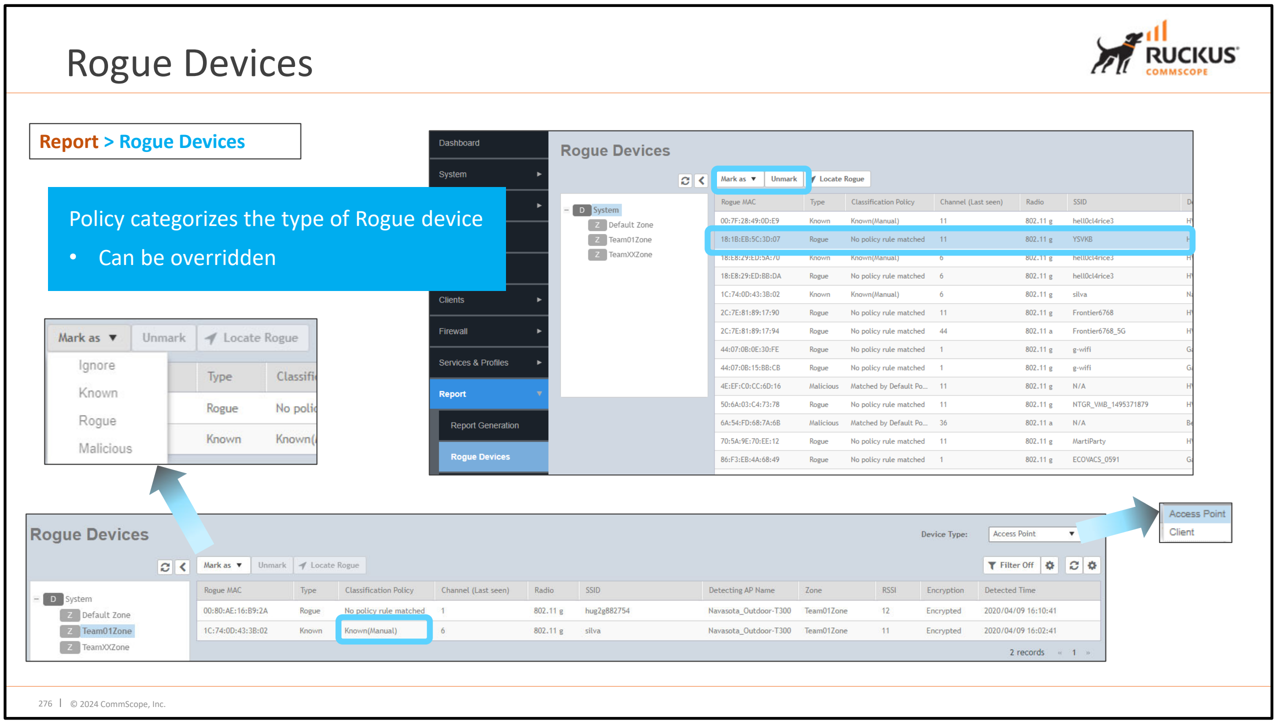
Priority	Name	Type and Criteria	Classification
1	Same Network Rule	Same Network	Malicious
2	MAC Spoofing Rule	MAC Spoofing	Malicious
	SSID Spoofing Rule	SSID Spoofing	Malicious
	CTS Abuse Rule	CTS Abuse	Malicious
5	RTS Abuse Rule	RTS Abuse	Malicious
6	Deauth Flood Rule	Deauth Flood	Malicious
7	Disassoc Flood Rule	Disassoc Flood	Malicious
8	Excessive Power Rule	Excessive Power	Malicious
9	Null SSID Rule	Null SSID	Malicious
10	Ad Hoc Rule	Ad Hoc	Rogue

* Name: Null SSID Rule
Null SSID — Defines the type of rule to match for this classification policy
* Classification: Malicious — Defines the classification when the above criteria is matched

Rogue devices "if detection is enabled in AP or wireless LAN Zones" can be detected and categorized with the Rogue Classification Policy. These policies are configured under **Services & Profiles** within each zone level where the detection and policy is to be applied.

You can either use the existing default policy (which can be modified) or configure your own to advise how detected devices are categorized based on the devices behavior or configurations.

There are many classification rules that can be configured customizing how the detected devices are identified in the Rogue list. Once the profile is configured it can be applied to a WLAN Zone guiding its WLAN members on Rogue detection. Manual classification or adjustment to previously identified devices from the policy is possible which we will see next.



Rogue Devices

Report > Rogue Devices

Policy categorizes the type of Rogue device

- Can be overridden

Type	Classifi
Rogue	No polic
Known	Known(

Rogue Devices

Rogue MAC	Type	Classification Policy	Channel (Last seen)	Radio	SSID
00:7F:28:49:0D:E9	Known	Known(Manual)	11	802.11 g	hell0cl4rice3
18:1B:EB:5C:3D:07	Rogue	No policy rule matched	11	802.11 g	YSVKB
18:E8:29:ED:5A:70	Known	Known(Manual)	6	802.11 g	hell0cl4rice3
18:E8:29:ED:BB:DA	Rogue	No policy rule matched	6	802.11 g	hell0cl4rice3
1C:74:0D:43:3B:02	Known	Known(Manual)	6	802.11 g	silva
2C:7E:81:89:17:90	Rogue	No policy rule matched	11	802.11 g	Frontier6768
2C:7E:81:89:17:94	Rogue	No policy rule matched	44	802.11 a	Frontier6768_5G
44:07:0B:0E:30:FE	Rogue	No policy rule matched	1	802.11 g	g-wifi
44:07:0B:15:BB:CB	Rogue	No policy rule matched	1	802.11 g	g-wifi
4E:EF:C0:CC:6D:16	Malicious	Matched by Default Po...	11	802.11 g	N/A
50:6A:03:C4:73:78	Rogue	No policy rule matched	11	802.11 g	NTGR_VMB_1495371879
6A:54:FD:68:7A:6B	Malicious	Matched by Default Po...	36	802.11 a	N/A
70:5A:9E:70:EE:12	Rogue	No policy rule matched	11	802.11 g	MartiParty
86:F3:EB:4A:68:49	Rogue	No policy rule matched	1	802.11 g	ECOVACS_0591

Rogue Devices

Rogue MAC	Type	Classification Policy	Channel (Last seen)	Radio	SSID	Detecting AP Name	Zone	RSSI	Encryption	Detected Time
00:80:AE:16:B9:2A	Rogue	No policy rule matched	1	802.11 g	hug2g882754	Navasota_Outdoor-T300	Team01Zone	12	Encrypted	2020/04/09 16:10:41
1C:74:0D:43:3B:02	Known	Known(Manual)	6	802.11 g	silva	Navasota_Outdoor-T300	Team01Zone	11	Encrypted	2020/04/09 16:02:41

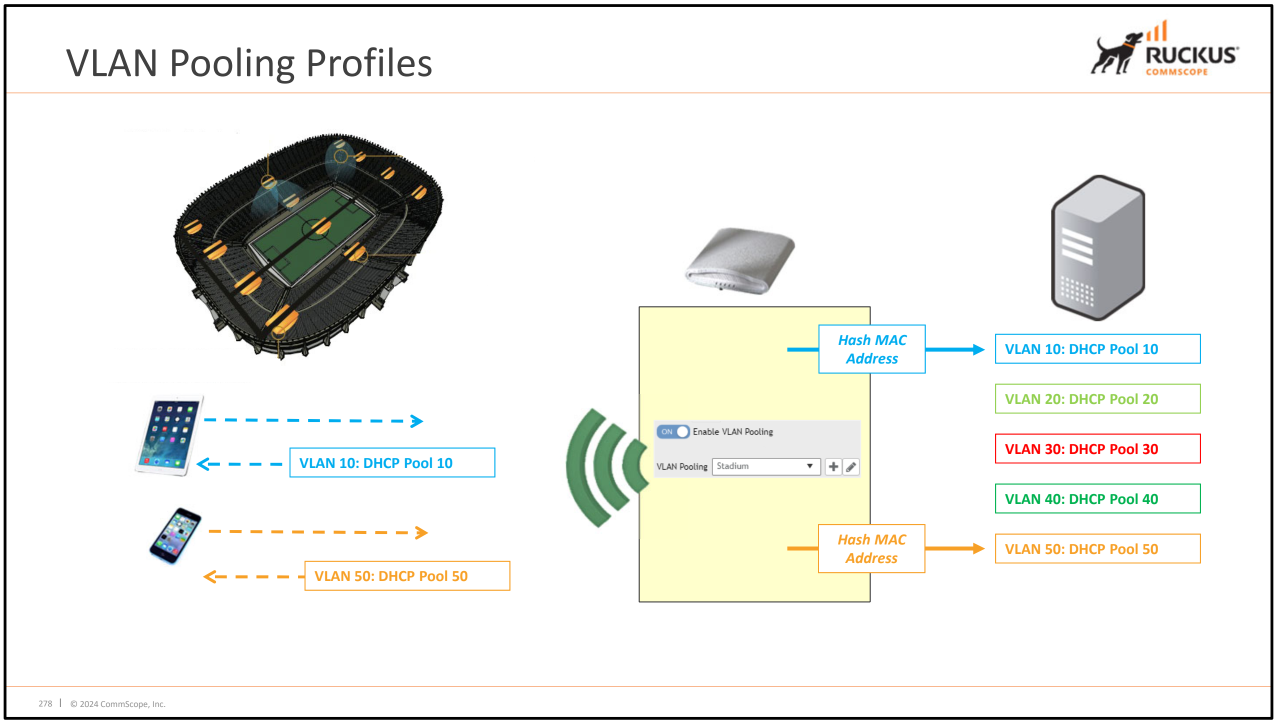
2 records « 1 »

276 | © 2024 CommScope, Inc.

Detected Rogue devices are listed under **Report > Rogue Devices** and each will be marked with a type based on the default rule policy if a custom policy has not been configured. Marking Rogue devices after they have been identified by the default policy can be manually overridden by selecting the device and choose “Mark as”, then select your option. Devices can also be set as Unmarked by selecting the unmarked button after a device has been selected. Rogue devices are listed as either access points or Clients and each list can be selected by using the drop down option on the top right of the list.

RUCKUS
COMMSCOPE

VLAN Pooling

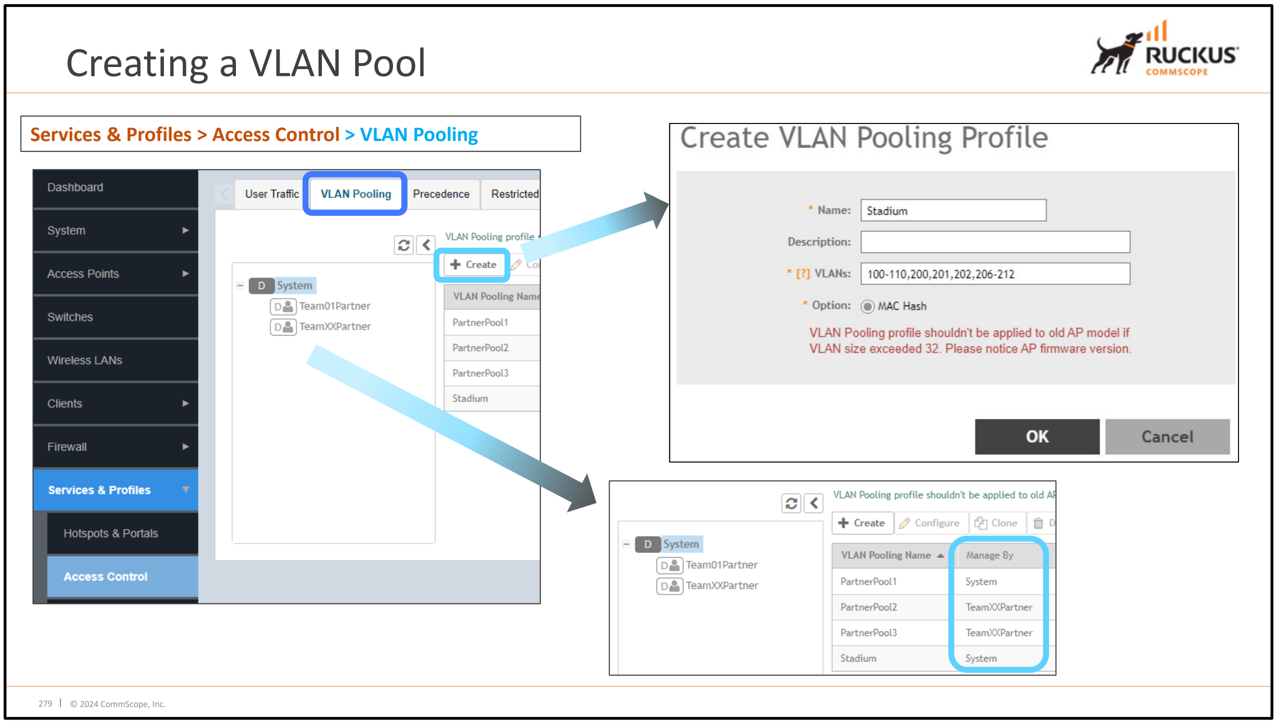


VLAN Pooling Profiles

278 | © 2024 CommScope, Inc.

VLAN Pooling allows you to run multiple different DHCP pools in a single WLAN. You'll use this in high-density deployments when you have a lot of clients. The AP uses a hash algorithm to assign incoming devices to different VLAN pools.

In our example, the first station connects. The AP hashes the MAC address, and the result maps to the first configured VLAN, VLAN 10. The client receives an IP address from VLAN 10 to the station. The second station connects, and the hashed MAC address maps to the VLAN 50. The client receives an IP address from VLAN 50.
Because the hash algorithm always provides the same result, each station will always be assigned to the same VLAN. Large deployments will have enough diversity between MAC addresses to ensure the clients are evenly balanced across the pools.



Creating a VLAN Pool

Services & Profiles > Access Control > VLAN Pooling

Create VLAN Pooling Profile

* Name:	Stadium
Description:	
* [?] VLANs:	100-110,200,201,202,206-212
* Option:	● MAC Hash

VLAN Pooling profile shouldn't be applied to old AP model if VLAN size exceeded 32. Please notice AP firmware version.

OK Cancel

VLAN Pooling profile shouldn't be applied to old AP

VLAN Pooling Name	Manage By
PartnerPool1	System
PartnerPool2	TeamXXPartner
PartnerPool3	TeamXXPartner
Stadium	System

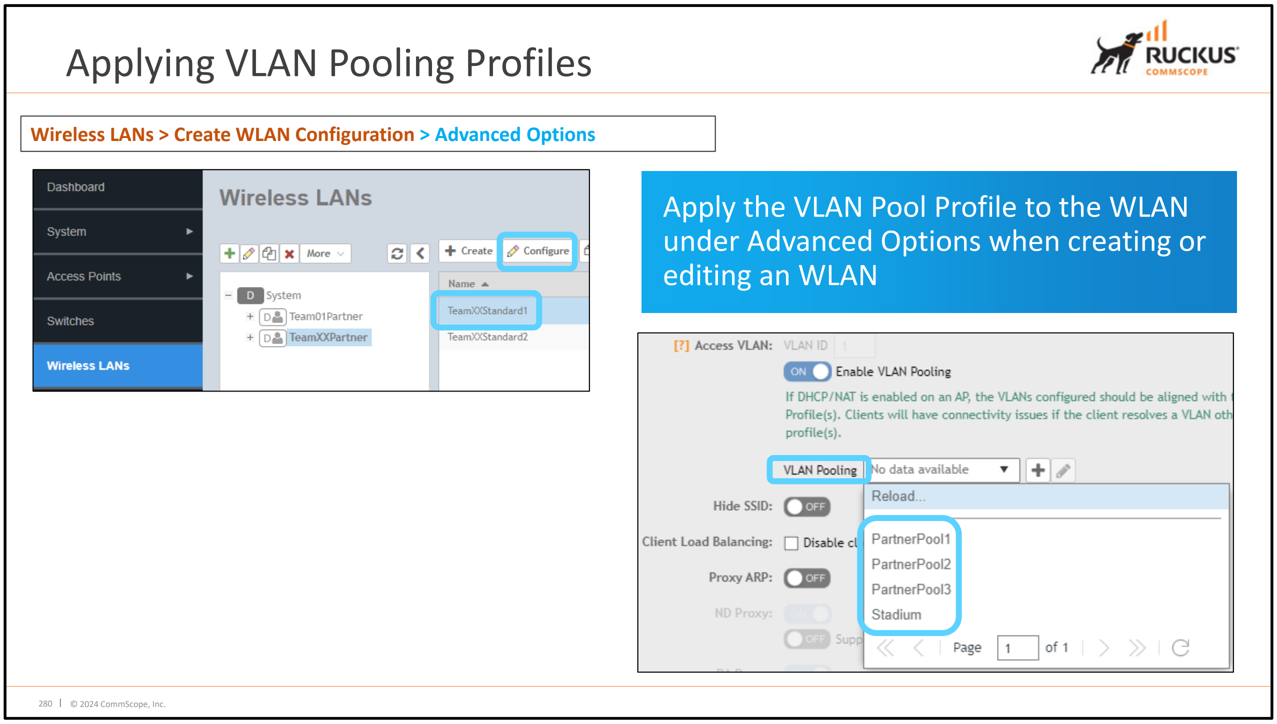
279 | © 2024 CommScope, Inc.

Previously you saw that you can enable VLAN Pooling under the **Advanced Options** when creating a WLAN.

To create a VLAN Pooling Profile navigate to **Services & Profiles > Access Control** and select the **VLAN Pooling** tab, Select the zone you want to configure the pool in then select **Create**.

Name the profile and add the VLANs. The **MAC Hash** option is selected by default. Each VLAN pool can contain up to 32 VLANs, and a maximum of 64 VLAN pools can be created. Each WLAN can be configured with a single VLAN Pool.
AP models supporting 11ac wave 2 and higher supports a maximum of 64 VLANs. Other AP models support up to 32 VLANs.

VLAN pooling profiles can be associated with domains however if created at the system level they are available for all domains. Therefore when creating profiles be careful to select the domain in which you want the profile to be available.



Applying VLAN Pooling Profiles

Wireless LANs > Create WLAN Configuration > Advanced Options

Apply the VLAN Pool Profile to the WLAN under Advanced Options when creating or editing an WLAN

[?] Access VLAN: VLAN ID 1

ON Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with t Profile(s). Clients will have connectivity issues if the client resolves a VLAN oth profile(s).

VLAN Pooling: No data available

Hide SSID: OFF

Client Load Balancing: □ Disable cl

Proxy ARP: OFF

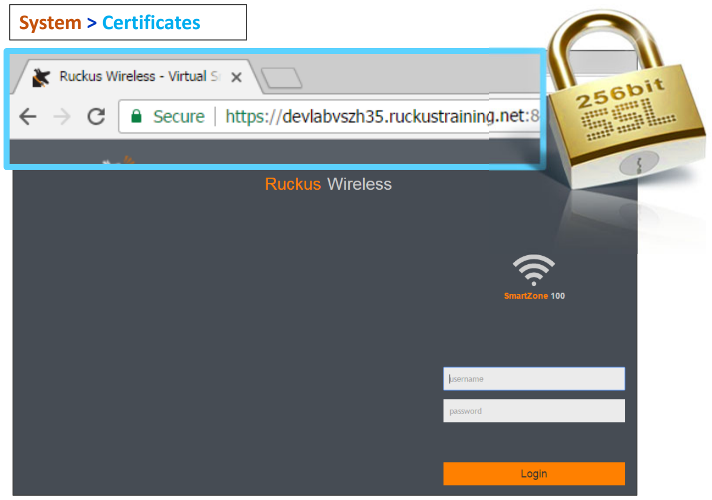
Once you have created your VLAN Pooling Profiles, you can add them to your WLANs. You'll need to return to the **Wireless LANs** menu.
You can add VLAN pools to WLANs as you create them or edit an existing WLAN. In this case we are selecting the WLAN (**TeamXXStandard1**) we want to add a pool and select configure.

Add the VLAN Pooling Profile under the **Advanced Options** menu.
Notice that when the *TeamXXPartner WLAN* is selected in the Wireless LANs menu, both the system-level VLAN Pools as well as the Partner domain pools are available in the VLAN Pooling list.

Certificates

Certificates

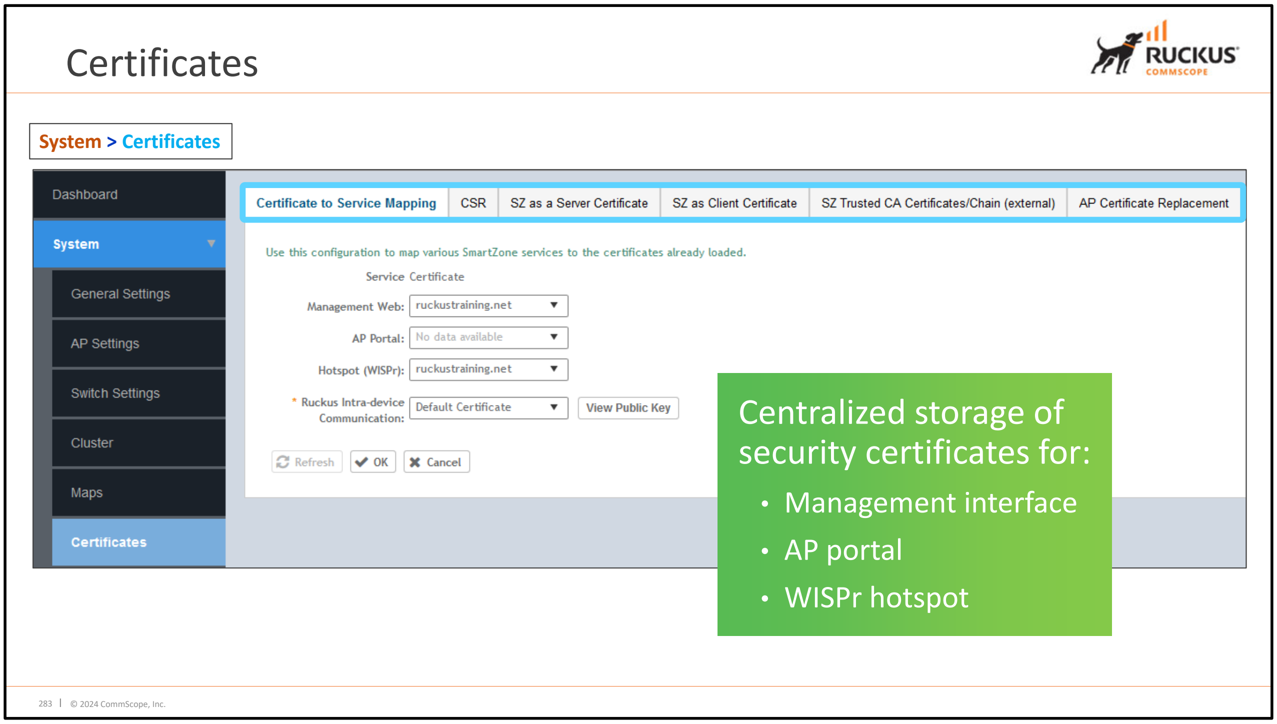
System > Certificates


Ruckus Wireless - Virtual S
Secure
https://devlabvszh35.ruckustraining.net:8
256bit
SSL
Ruckus Wireless
SmartZone 100
username
password
Login

- Default self-signed certificate is created during setup
- Some services may experience problems when using self-signed certificates
- Trusted Certificate verifies the controller

Devices use certificates during authentication to verify the identity of the controller and for additional secure connections. The system creates a default self-signed certificate during system setup. However, some services may experience problems when using self-signed certificates.

It’s an established best practice, as well as a RUCKUS recommendation, to use trusted certificates for verifying SmartZone resources.



Certificates

System > Certificates

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: ruckustraining.net

AP Portal: No data available

Hotspot (WISPr): ruckustraining.net

* Ruckus Intra-device Communication: Default Certificate

Centralized storage of security certificates for:

- Management interface
- AP portal
- WISPr hotspot

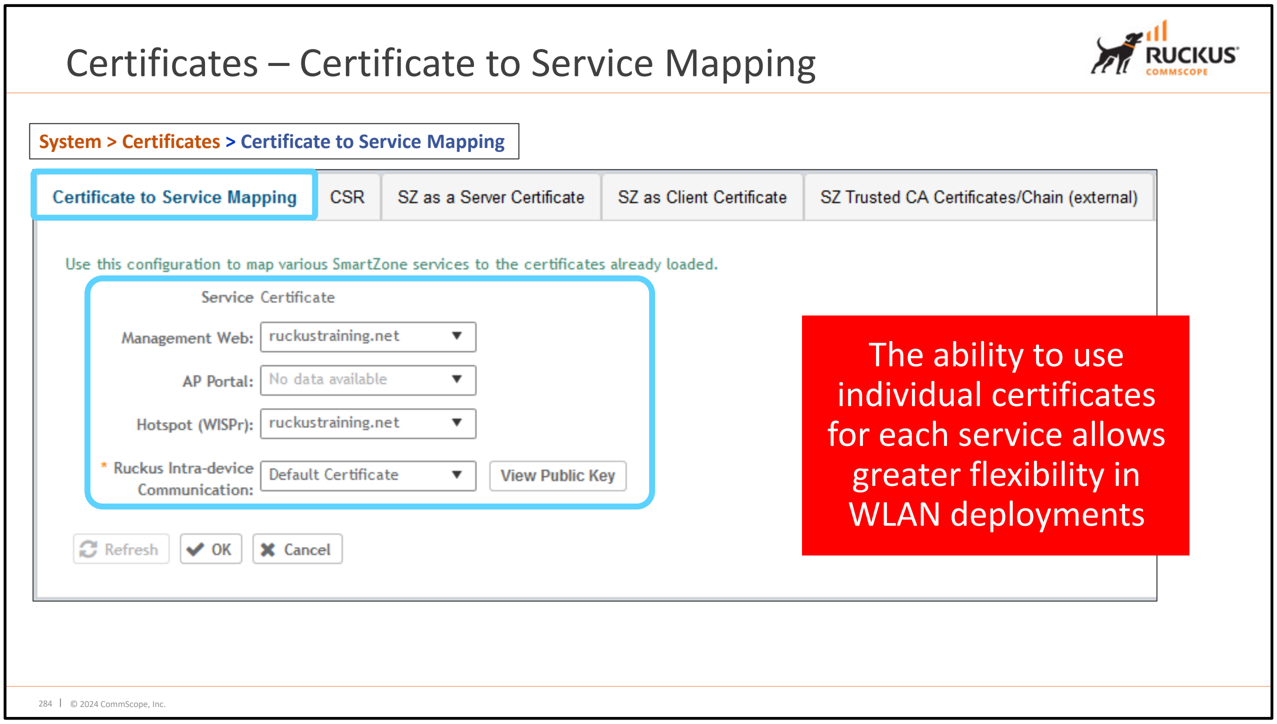
283 | © 2024 CommScope, Inc.

All the security certificates that the controller uses for its web interface, AP portal, and hotspots are managed from a central storage.

By default, a RUCKUS-signed SSL certificate (or security certificate) exists in the controller. However, because this default certificate is signed by RUCKUS and is not recognized by most web browsers, a security warning appears whenever you connect to the web interface or users connect to the AP portal or a hotspot. To prevent these security warnings from appearing, you can import an SSL certificate that is issued by a recognized certificate authority (CA).

You can view certificate configurations under **System > Certificates**. There are a number of options available for configuring certificates:

- **Certificate to Service Mapping**: Allows you to specify which certificate will map to which service.
- **CSR**: Allows you to generate a Certificate Signing Request.
- **SZ as a Server Certificate**: Import certificates for when the SmartZone controller is the server.
- **SZ as a Client Certificate**: Import certificates for when the SmartZone controller is the client.
- **Trusted CA Certs (Chain)**: Imports a Trusted CA Chain into the controller.
- **AP Certificate Replacement**: Used to replace AP certificates.



Certificates – Certificate to Service Mapping

System > Certificates > Certificate to Service Mapping

Certificate to Service Mapping
CSR
SZ as a Server Certificate
SZ as Client Certificate
SZ Trusted CA Certificates/Chain (external)

Use this configuration to map various SmartZone services to the certificates already loaded.

Service	Certificate
Management Web:	ruckustraining.net
AP Portal:	No data available
Hotspot (WISPr):	ruckustraining.net
* Ruckus Intra-device Communication:	Default Certificate

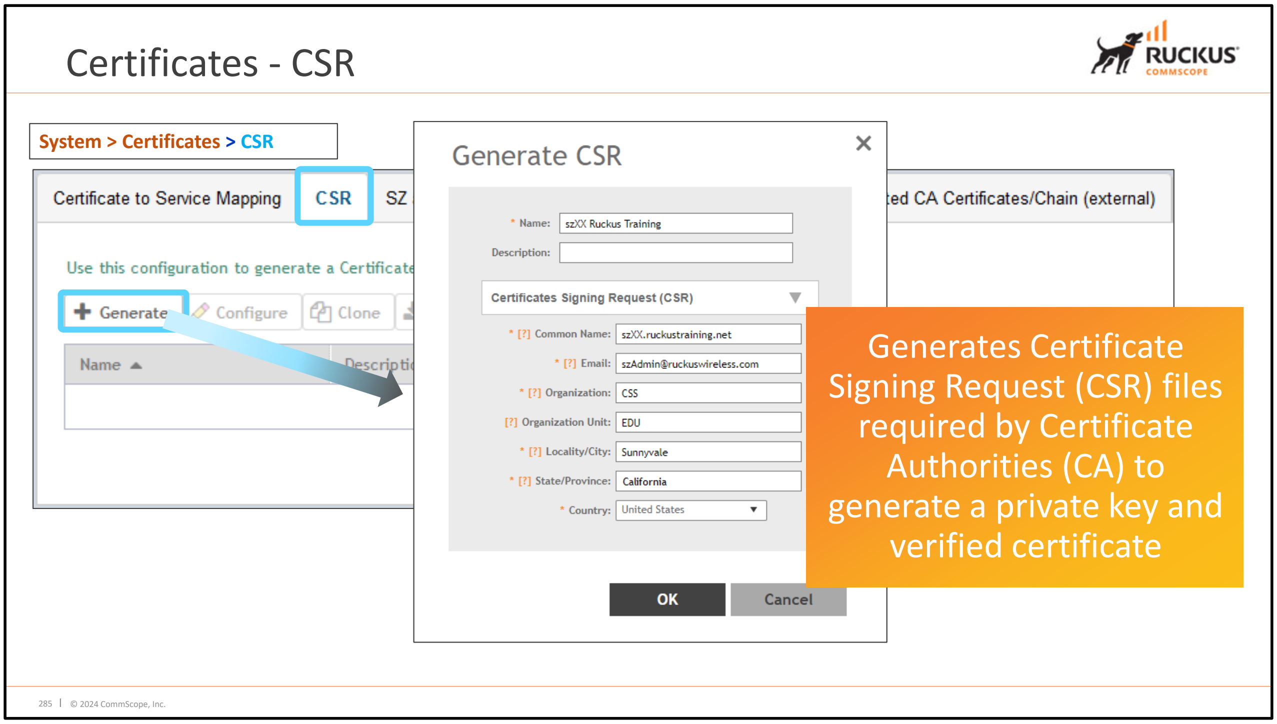
The ability to use individual certificates for each service allows greater flexibility in WLAN deployments

284 | © 2024 CommScope, Inc.

The **Certificates to Service Mapping** specify which certificates will be used for each of the specified services. This gives you the freedom to use unique certificates that are more appropriate to the service you are providing rather than using a single, default certificate for all.

These are the services which can be uniquely assigned certificates for access:

- **Management Web**: The certificate used when accessing the web interface
- **AP Portal**: The certificate used by Web Auth WLANS and Guest Access WLANs.
- **Hotspot WISPr**: The certificate used by WISPr WLANs.
- **RUCKUS Intra-device Communications**: The certificate used for Access Point control traffic.



Certificates - CSR

System > Certificates > CSR

Certificate to Service Mapping
CSR
SZ
ted CA Certificates/Chain (external)
Use this configuration to generate a Certificate
Generate
Configure
Clone
Name
Descripti

Generate CSR

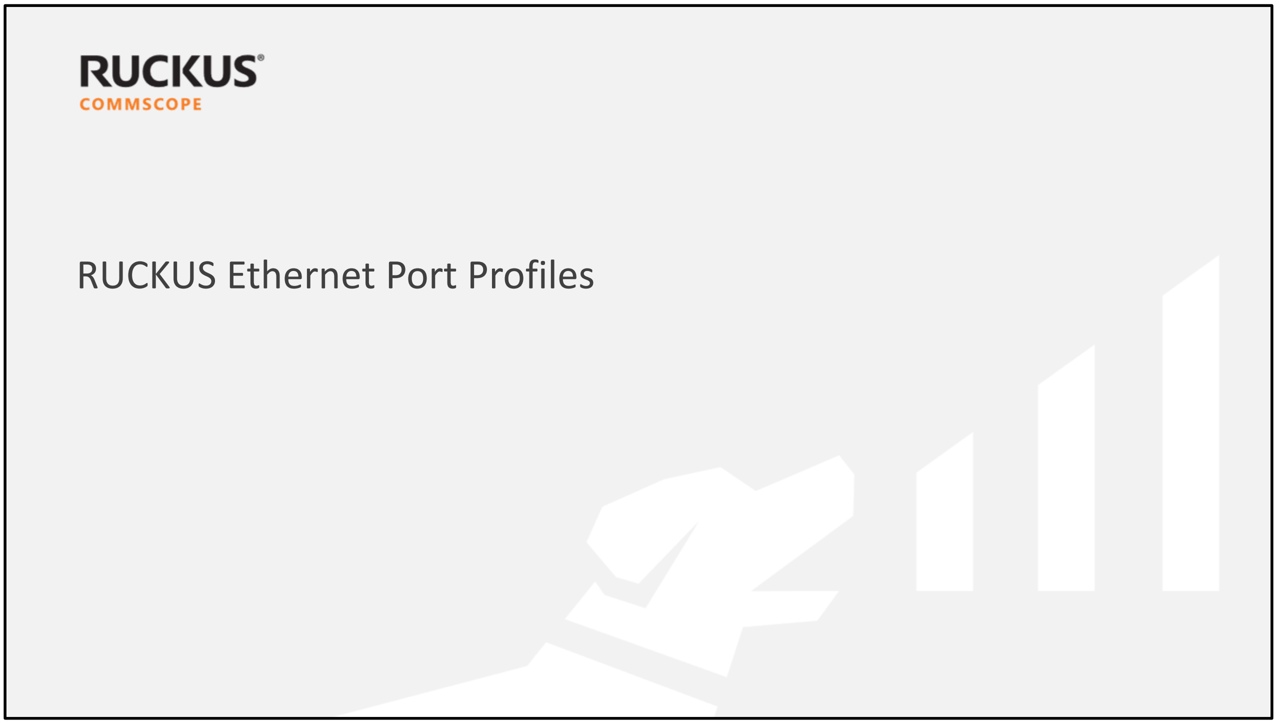
- * Name: szXX Ruckus Training
- Description:

Certificates Signing Request (CSR)

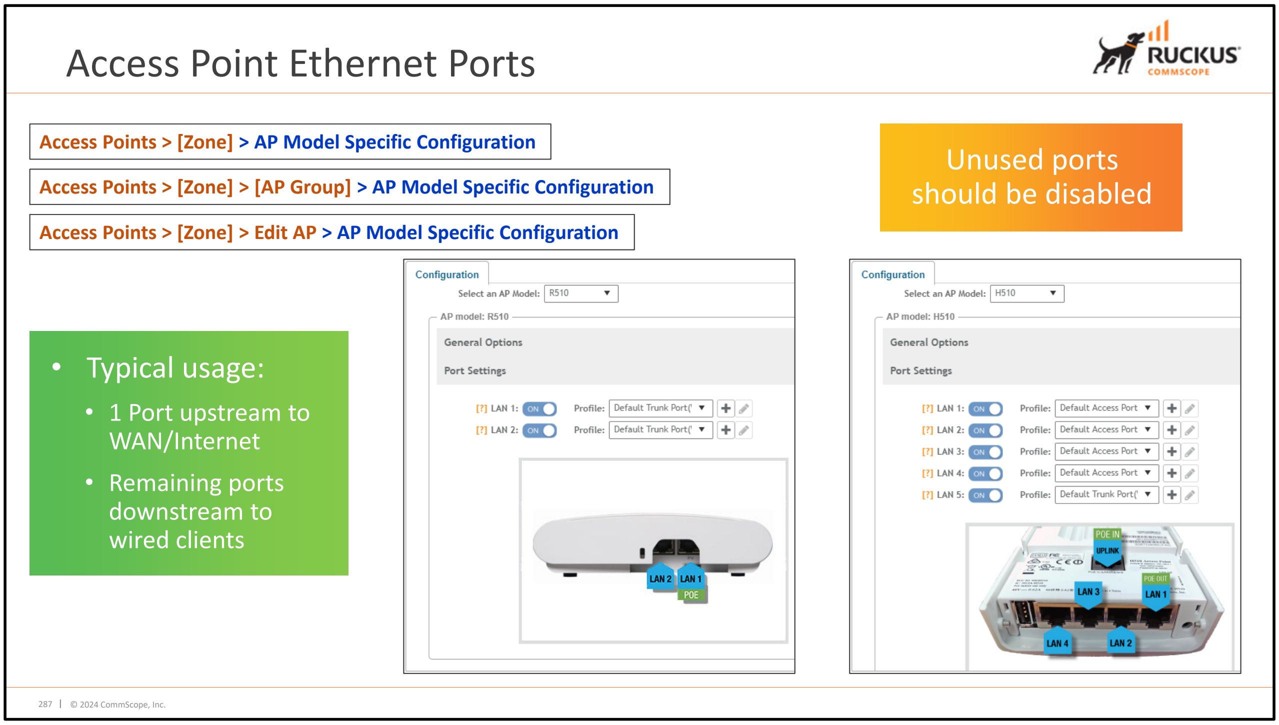
- * [?] Common Name: szXX.ruckustraining.net
- * [?] Email: szAdmin@ruckuswireless.com
- * [?] Organization: CSS
- [?] Organization Unit: EDU
- * [?] Locality/City: Sunnyvale
- * [?] State/Province: California
- * Country: United States

Generates Certificate Signing Request (CSR) files required by Certificate Authorities (CA) to generate a private key and verified certificate

The **Certificate Signing Request** tab is used to generate a Certificate Signing Request (CSR). A CSR is used to generate the files required for ordering a trusted certificate from an external Certificate Authority (CA). In a CSR request you are required to supply various pieces of information which will be used to generate a compressed zip containing a .csr file and a .pem file. Your certificate provider will require one of these files, depending on which RFC they adhere to, in order to generate your private key and assign you a certificate. The returned certificate can then be installed on SmartZone controller in the **SZ as a Server Certificate** tab and can then be assigned to specific service.



RUCKUS Ethernet Port Profiles



Access Point Ethernet Ports

Access Points > [Zone] > AP Model Specific Configuration

Access Points > [Zone] > [AP Group] > AP Model Specific Configuration

Access Points > [Zone] > Edit AP > AP Model Specific Configuration

Unused ports should be disabled

- Typical usage:
  - 1 Port upstream to WAN/Internet
  - Remaining ports downstream to wired clients

Configuration

Select an AP Model: R510

AP model: R510

General Options

Port Settings

[?] LAN 1: ON Profile: Default Trunk Port('

[?] LAN 2: ON Profile: Default Trunk Port('

Configuration

Select an AP Model: H510

AP model: H510

General Options

Port Settings

[?] LAN 1: ON Profile: Default Access Port

[?] LAN 2: ON Profile: Default Access Port

[?] LAN 3: ON Profile: Default Access Port

[?] LAN 4: ON Profile: Default Access Port

[?] LAN 5: ON Profile: Default Trunk Port('

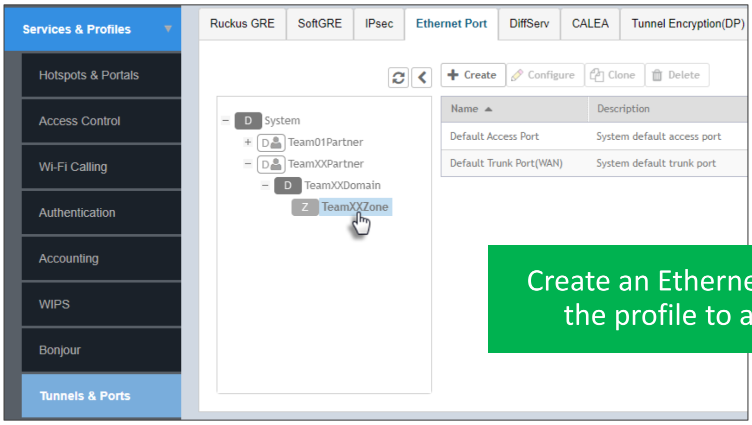
It is important to understand the wired connections that allow wireless clients to access services beyond the AP itself. RUCKUS APs come in many different configurations with a different number of Ethernet ports. These ports can be disabled and configured in the AP Model Specific Configuration section of a zone, an AP group or on an individual AP. It is most common for an AP to use one port for connecting upstream to the WAN, the Internet and the SmartZone controller. The remaining ports can then be connected downstream to wired network clients.

To disable an individual Ethernet port, simply toggle the slider to the OFF position. It definitely a best practice to disable any unused Ethernet ports on an access point.

Additionally, a port profile, defining the operational functionality of the port, can be selected from the drop-down menu. The SmartZone controller has two port profiles that are available to all APs. These are the Default Trunk Port (WAN) and Default Access Port.

Ethernet Port Profiles

Services & Profiles > Tunnels & Ports > Ethernet Port

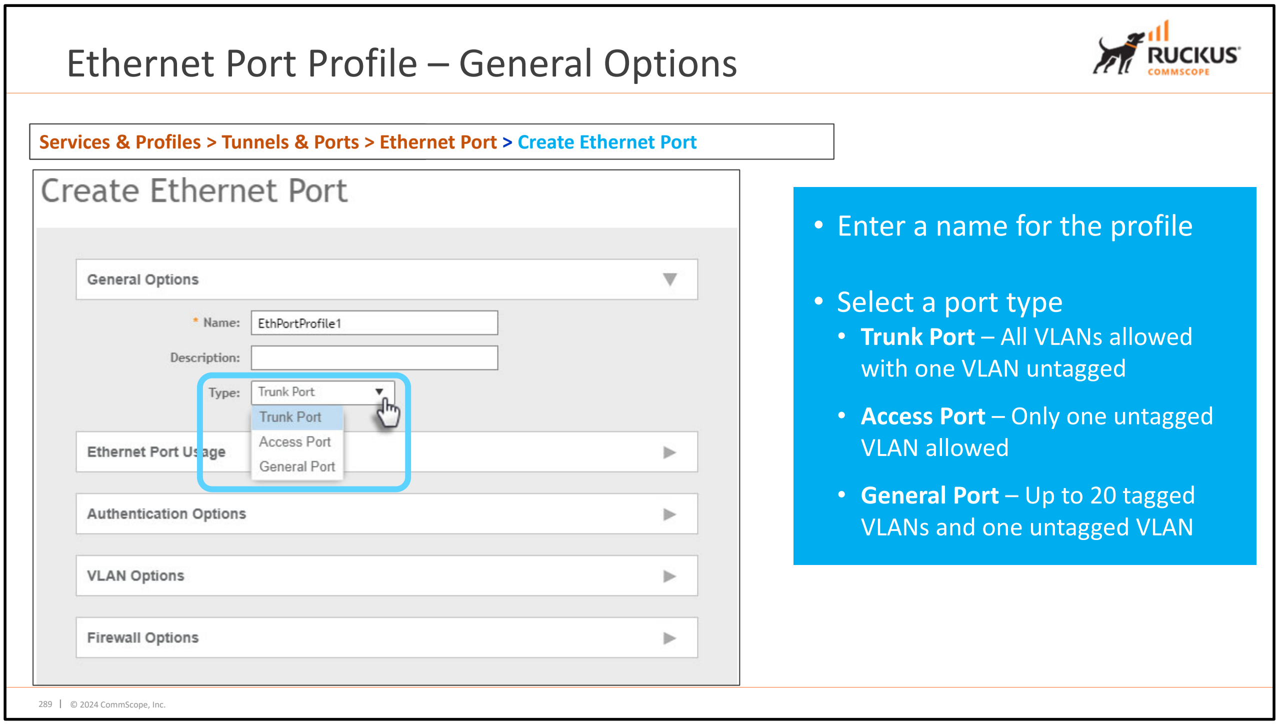


Name	Description
Default Access Port	System default access port
Default Trunk Port(WAN)	System default trunk port

Create an Ethernet Port Profile, then apply the profile to a single AP or AP group

Port profiles define the behaviour of the Ethernet ports on an AP. In order to apply a Port Profile to an Access Point or Access Point Group, you need to create the profile first. This is done under **Services & Profiles > Tunnels & Ports > Ethernet Port** and configured at the zone level. By default an access port and trunk port profile are created and can be applied to Ethernet ports of an AP. If you require unique VLAN assignments, tunnelling or 802.1X authentication then a custom profile will need to be created.

When you create a new profile, various settings allow you to tune how it will behave. You can then apply the profile to a single AP or AP Group.



Ethernet Port Profile – General Options

Services & Profiles > Tunnels & Ports > Ethernet Port > Create Ethernet Port

Create Ethernet Port

General Options

* Name: EthPortProfile1

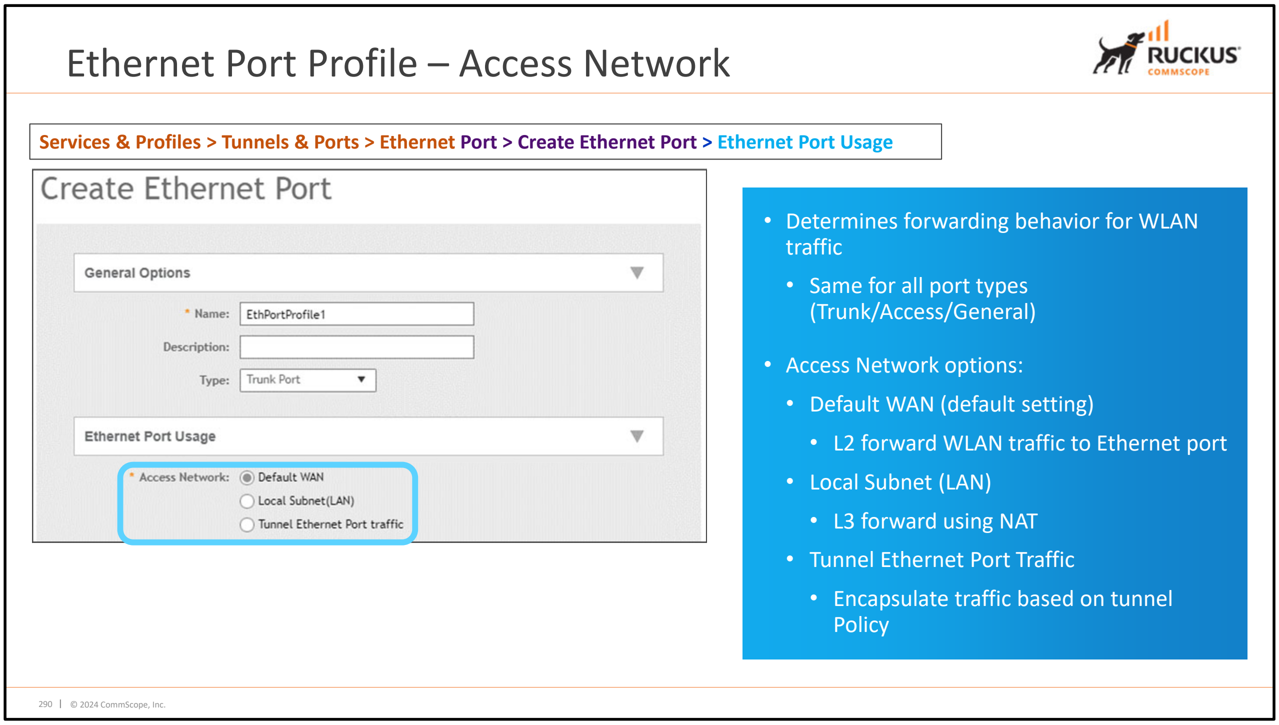
Description:

Type: Trunk Port

- Enter a name for the profile
- Select a port type
  - **Trunk Port** – All VLANs allowed with one VLAN untagged
  - **Access Port** – Only one untagged VLAN allowed
  - **General Port** – Up to 20 tagged VLANs and one untagged VLAN

289 |

Start by giving the Port Profile a name, and then select the type of port. The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port or General Port. Let’s take a look at each one of the port types.



Ethernet Port Profile – Access Network

Services & Profiles > Tunnels & Ports > Ethernet Port > Create Ethernet Port > Ethernet Port Usage

Create Ethernet Port

General Options

* Name: EthPortProfile1

Description:

Type: Trunk Port

Ethernet Port Usage

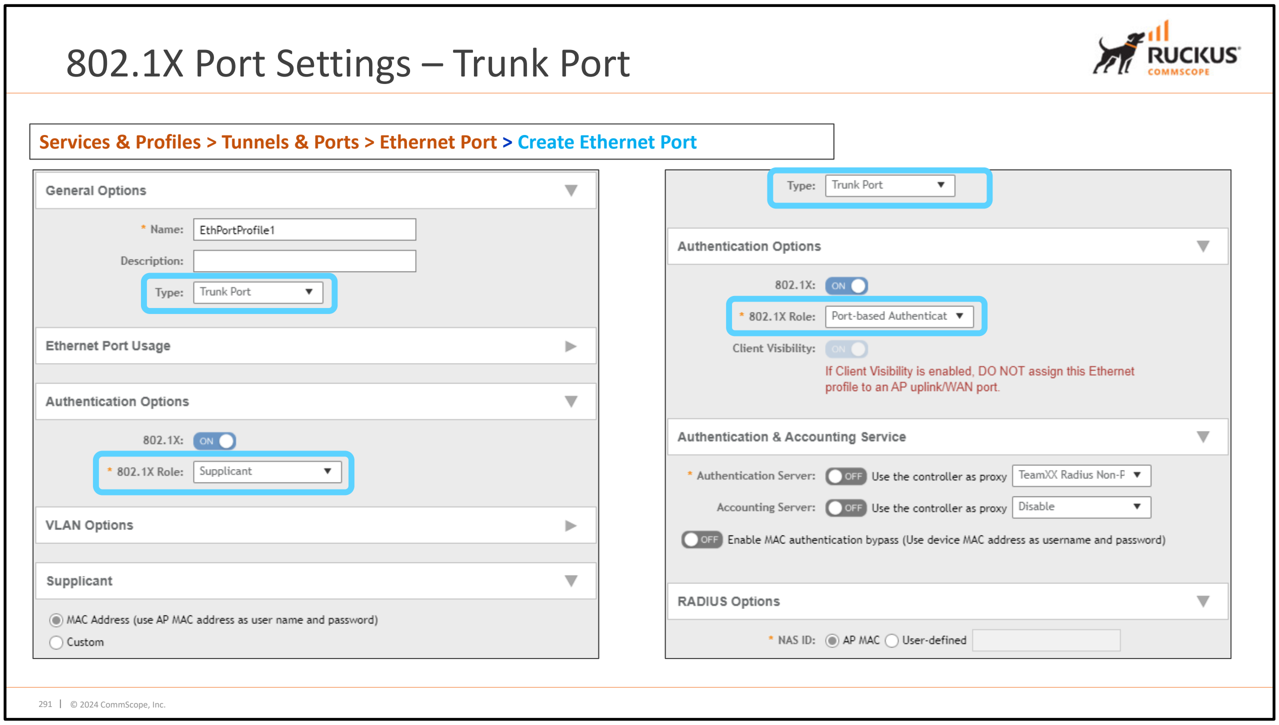
* Access Network: ● Default WAN
○ Local Subnet(LAN)
○ Tunnel Ethernet Port traffic

- Determines forwarding behavior for WLAN traffic
  - Same for all port types (Trunk/Access/General)
- Access Network options:
  - Default WAN (default setting)
    - L2 forward WLAN traffic to Ethernet port
  - Local Subnet (LAN)
    - L3 forward using NAT
  - Tunnel Ethernet Port Traffic
    - Encapsulate traffic based on tunnel Policy

290 | © 2024 CommScope, Inc.

Under the Ethernet Port Usage section, the Access Network option is used to specify how traffic from AP WLANs will be forwarded to an Ethernet port where this profile is applied.

- **Default WAN**: The default setting, forwards data arriving on AP WLANs to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding.
- **Local Subnet (LAN)**: This setting allows routing of wireless data to its destinations using Layer 3 network address translation (NAT).
- **Tunnel Ethernet Port Traffic**: Uses Layer 2 Tunneling Protocol to deliver encapsulated data based on the tunnel profile selected.



802.1X Port Settings – Trunk Port

Services & Profiles > Tunnels & Ports > Ethernet Port > Create Ethernet Port

General Options

* Name: EthPortProfile1

Description:

Type: Trunk Port

Ethernet Port Usage

Authentication Options

802.1X: ON

* 802.1X Role: Supplicant

VLAN Options

Supplicant

● MAC Address (use AP MAC address as user name and password)

○ Custom

Type: Trunk Port

Authentication Options

802.1X: ON

* 802.1X Role: Port-based Authenticat

Client Visibility: ON

If Client Visibility is enabled, DO NOT assign this Ethernet profile to an AP uplink/WAN port.

Authentication & Accounting Service

* Authentication Server: OFF Use the controller as proxy TeamXX Radius Non-F

Accounting Server: OFF Use the controller as proxy Disable

OFF Enable MAC authentication bypass (Use device MAC address as username and password)

RADIUS Options

* NAS ID: ● AP MAC ○ User-defined

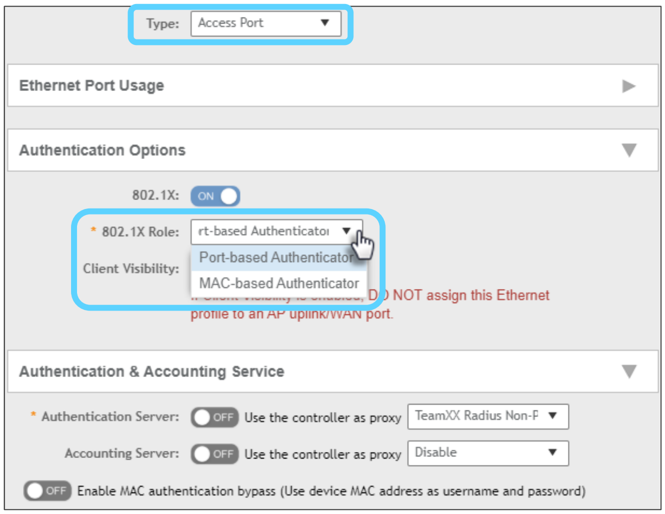
291 | © 2024 CommScope, Inc.

When 802.1X is enabled on Trunk port, there are two 802.1X roles available:

- **Supplicant** – Can use the APs MAC address or a custom value as the username and password for authentication
- **Port-based Authentication** – Here you must specify the server used for authentication on this network. When you select **Use the controller as proxy**, requests will flow through the controller. In non-proxy mode, the AP will communicate directly with the authentication server without going through the controller. In both cases, a previously configured authenticator must be selected from the dropdown list. RADIUS options are also required for this 802.1X role.

802.1X Port Settings – Access Port

Services & Profiles > Tunnels & Ports > Ethernet Port > Create Ethernet Port



Type: Access Port

Ethernet Port Usage

Authentication Options

802.1X: ON

* 802.1X Role: rt-based Authenticator

Port-based Authenticator

MAC-based Authenticator

Client Visibility:

DO NOT assign this Ethernet profile to an AP uplink/WAN port.

Authentication & Accounting Service

* Authentication Server: OFF Use the controller as proxy TeamXX Radius Non-P

Accounting Server: OFF Use the controller as proxy Disable

OFF Enable MAC authentication bypass (Use device MAC address as username and password)

802.1X on Access ports allows two roles:

- Port-based Authentication
- MAC-based Authentication

Both require Authentication and RADIUS options to be defined

292 | © 2024 CommScope, Inc.

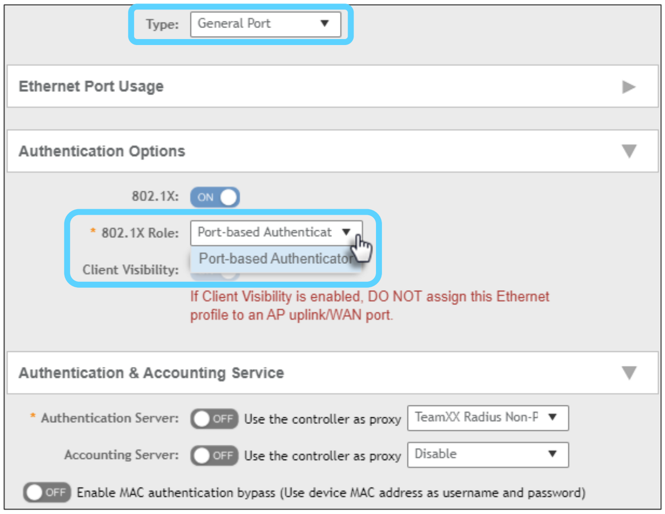
When 802.1X is enabled on an **Access** port, there are two 802.1X roles available:

- **MAC-based Authentication**
- **Port-based Authentication**

In both cases you have to set an authenticator from a preconfigured authentication service. The difference between Port-based and MAC-based is with a Port-based Authenticator, only a single MAC host must be authenticated for all hosts to be granted access to the network. If you select MAC-based Authenticator, each MAC address host is individually authenticated. RADIUS options are also required for this 802.1X role.

802.1X Port Settings – General Port

Services & Profiles > Tunnels & Ports > Ethernet Port > Create Ethernet Port



Type: General Port

Ethernet Port Usage

Authentication Options

802.1X: ON

* 802.1X Role: Port-based Authenticat

Port-based Authenticator

Client Visibility:

If Client Visibility is enabled, DO NOT assign this Ethernet profile to an AP uplink/WAN port.

Authentication & Accounting Service

* Authentication Server: OFF Use the controller as proxy TeamXX Radius Non-P

Accounting Server: OFF Use the controller as proxy Disable

OFF Enable MAC authentication bypass (Use device MAC address as username and password)

- 802.1X on General ports only allows Port-based Authentication
- Like Trunk and Access ports, Authentication and RADIUS options are required

293 | © 2024 CommScope, Inc.

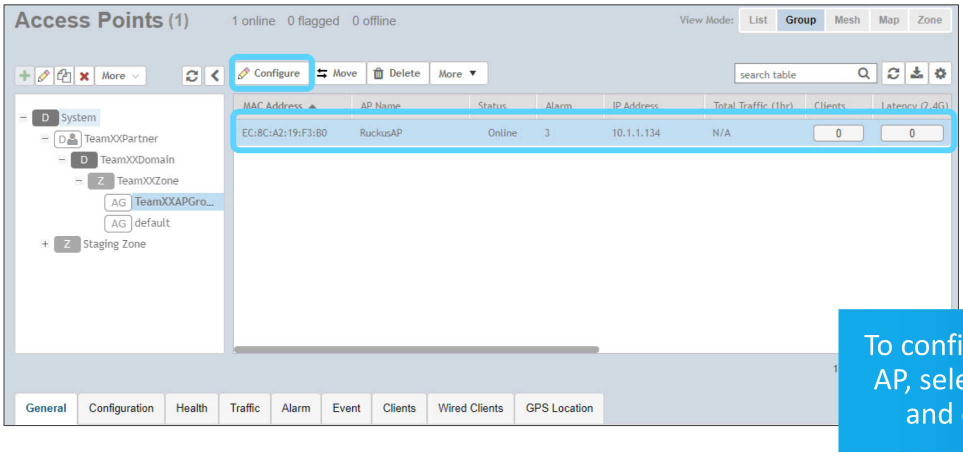
When 802.1X is enabled on a **General** port, there is only one 802.1X role available:

- **Port-based Authentication**

This option will require you to specify the server used for authentication on this network A previously configured authenticator must be selected from the dropdown list. RADIUS options are also required for this 802.1X role.

Individual Access Point Settings

Access Points > Access Points



MAC Address	AP Name	Status	Alarm	IP Address	Total Traffic (1hr)	Clients	Latency (2.4G)
EC:8C:A2:19:F3:B0	RuckusAP	Online	3	10.1.1.134	N/A	0	0

To configure an individual AP, select it from the list and click **Configure**

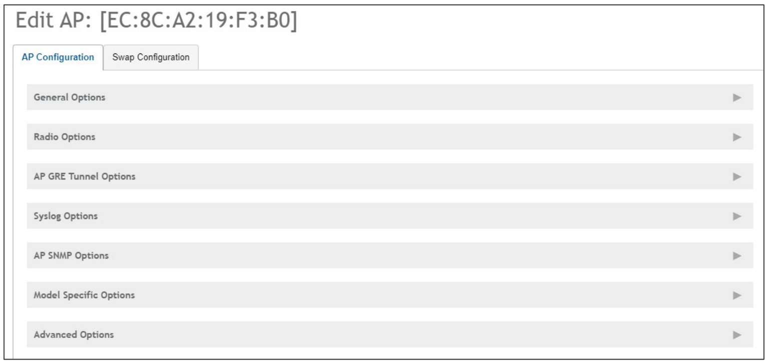
294 | © 2024 CommScope, Inc.

If you want to apply a specific configuration to a single Access Point only, use **Individual AP Settings**. These settings define the configuration for a specific Access Point and will override any Zone, AP Group, or model specific settings.

To configure individual settings, select an AP from the list and select **Configure**.

Configuring Individual APs

Access Points > Access Points > Edit AP



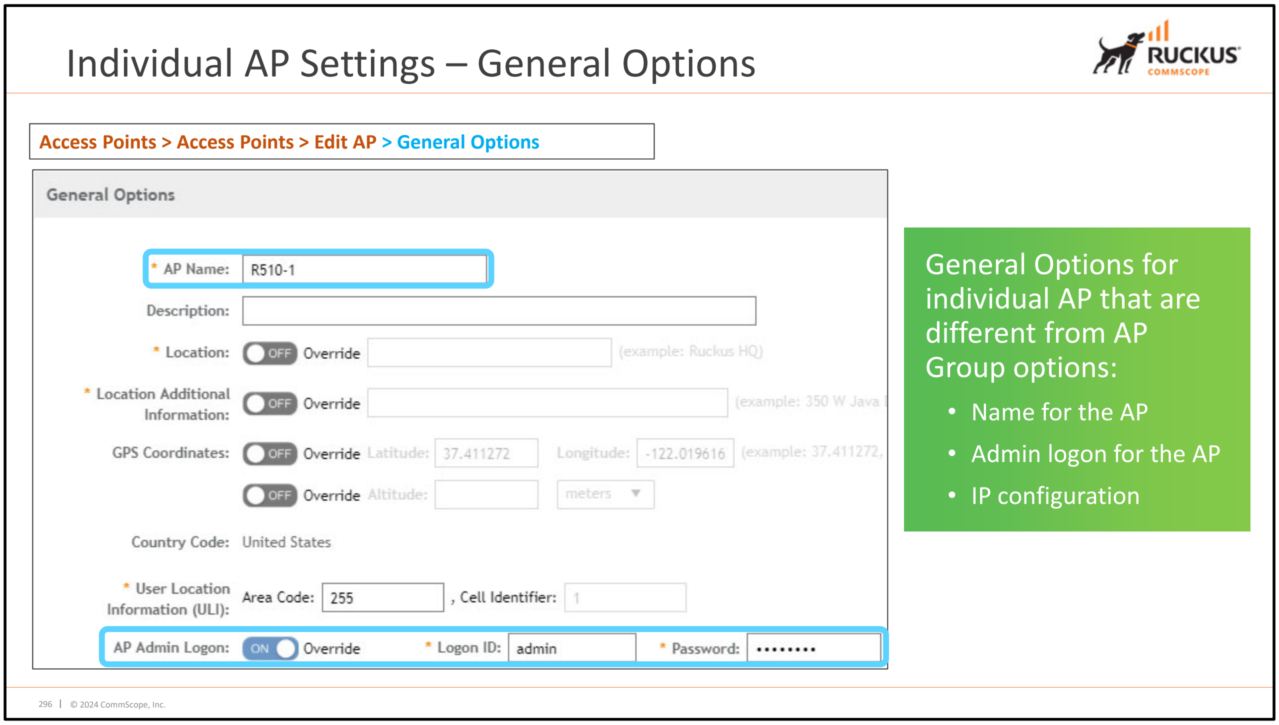
Edit AP: [EC:8C:A2:19:F3:B0]

- Individual AP settings override Zone and AP Group settings
- Only General Options and Radio Options contain additional configuration capabilities found in AP Groups
- Settings are identical to AP Group settings for:
  - AP SNMP Options
  - Model Specific Options
  - Advanced Options

295 | © 2024 CommScope, Inc.

The settings applied to an individual AP are almost identical to the AP Group settings we just discussed, with a few minor differences. Let’s review the available options.
The General Options and Radio Options tabs contain some settings that are only found through individual AP configuration.

Most other settings that can be overridden are that same as in the AP group and zone.



Individual AP Settings – General Options

Access Points > Access Points > Edit AP > General Options

General Options

* AP Name: R510-1

Description:

* Location: OFF Override (example: Ruckus HQ)

* Location Additional Information: OFF Override (example: 350 W Java

GPS Coordinates: OFF Override Latitude: 37.411272 Longitude: -122.019616 (example: 37.411272,

OFF Override Altitude: meters ▼

Country Code: United States

* User Location Information (ULI): Area Code: 255 , Cell Identifier: 1

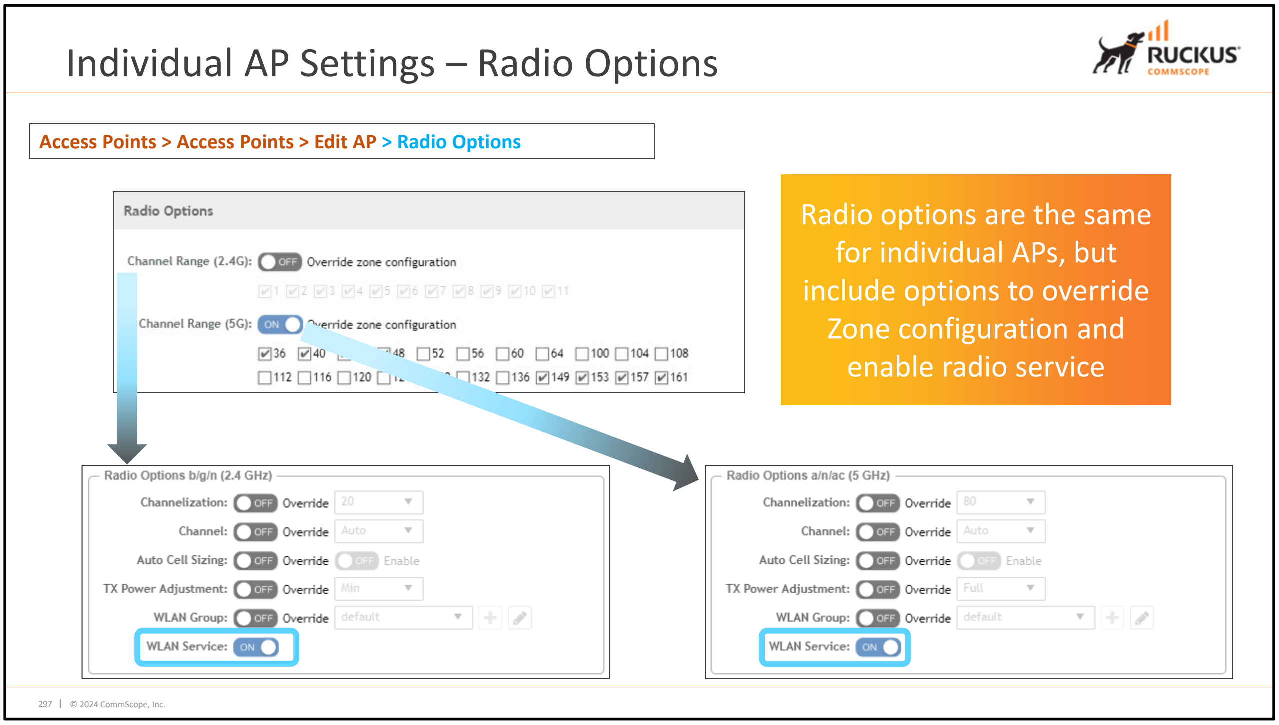
AP Admin Logon: ON Override * Logon ID: admin * Password: ••••••••

General Options for individual AP that are different from AP Group options:

- Name for the AP
- Admin logon for the AP
- IP configuration

296 | © 2024 CommScope, Inc.

In the General Options section of an individual access point's configuration, you can fine-tune the Access Point name, modify the admin login settings and change the AP's IP information. All of these changes are unique to the AP itself and items like the name and IP information simply cannot applied by a group policy.



Individual AP Settings – Radio Options

Access Points > Access Points > Edit AP > Radio Options

Radio Options

Channel Range (2.4G): OFF Override zone configuration

☑1 ☑2 ☑3 ☑4 ☑5 ☑6 ☑7 ☑8 ☑9 ☑10 ☑11

Channel Range (5G): ON Override zone configuration

☑36 ☑40 48 □52 □56 □60 □64 □100 □104 □108

□112 □116 □120 □132 □136 ☑149 ☑153 ☑157 ☑161

Radio options are the same for individual APs, but include options to override Zone configuration and enable radio service

Radio Options b/g/n (2.4 GHz)

Channelization: OFF Override 20

Channel: OFF Override Auto

Auto Cell Sizing: OFF Override OFF Enable

TX Power Adjustment: OFF Override Min

WLAN Group: OFF Override default

WLAN Service: ON

Radio Options a/n/ac (5 GHz)

Channelization: OFF Override 80

Channel: OFF Override Auto

Auto Cell Sizing: OFF Override OFF Enable

TX Power Adjustment: OFF Override Full

WLAN Group: OFF Override default

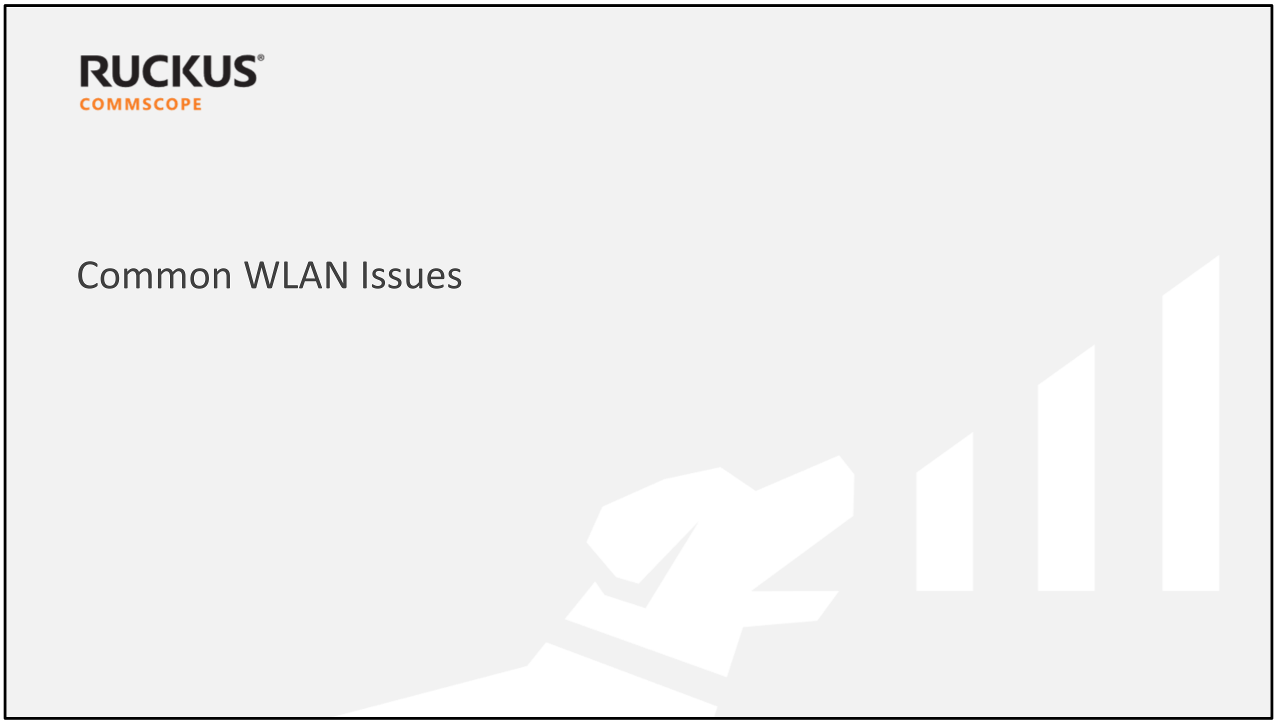
WLAN Service: ON

297 | © 2024 CommScope, Inc.

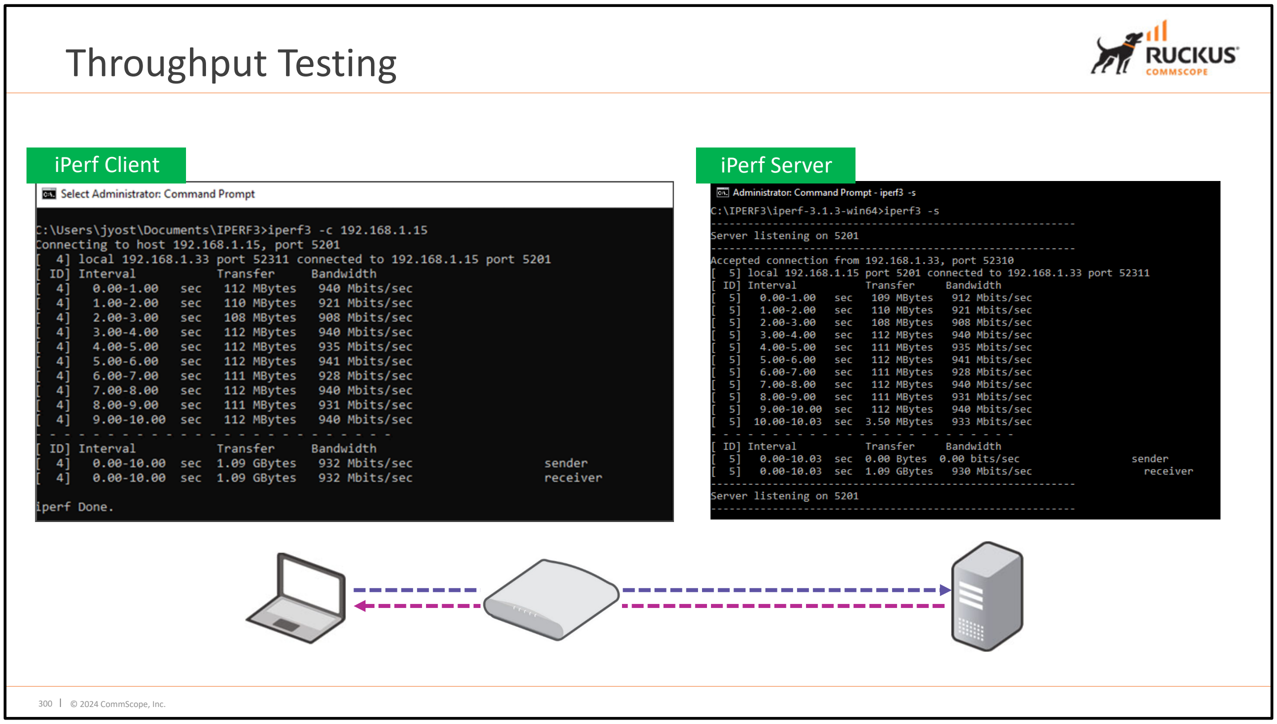
The settings in the Radio Options are similar to the group and zone options. One big difference is that now you have the additional option to disable the WLAN service on the radio. It important to note that this is only place in entire SmartZone hierarchy where an individual wireless radio can be disabled, preventing connectivity on any WLANs.

While disabling the WLAN service will stop WLANs from being available, the Access Point will continue to perform scanning.

Wi-Fi solution troubleshooting and repair



Common WLAN Issues


Select Administrator: Command Prompt
Administrator: Command Prompt - iperf3 -s

Throughput Testing

iPerf Client

```
C:\Users\jyost\Documents\IPERF3>iperf3 -c 192.168.1.15
Connecting to host 192.168.1.15, port 5201
[  4] local 192.168.1.33 port 52311 connected to 192.168.1.15 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec   112 MBytes   940 Mbits/sec
[  4]   1.00-2.00   sec   110 MBytes   921 Mbits/sec
[  4]   2.00-3.00   sec   108 MBytes   908 Mbits/sec
[  4]   3.00-4.00   sec   112 MBytes   940 Mbits/sec
[  4]   4.00-5.00   sec   112 MBytes   935 Mbits/sec
[  4]   5.00-6.00   sec   112 MBytes   941 Mbits/sec
[  4]   6.00-7.00   sec   111 MBytes   928 Mbits/sec
[  4]   7.00-8.00   sec   112 MBytes   940 Mbits/sec
[  4]   8.00-9.00   sec   111 MBytes   931 Mbits/sec
[  4]   9.00-10.00  sec   112 MBytes   940 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  1.09 GBytes   932 Mbits/sec                  sender
[  4]   0.00-10.00  sec  1.09 GBytes   932 Mbits/sec                  receiver

iperf Done.
```

iPerf Server

```
C:\IPERF3\iperf-3.1.3-win64>iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 192.168.1.33, port 52310
[  5] local 192.168.1.15 port 5201 connected to 192.168.1.33 port 52311
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec   109 MBytes   912 Mbits/sec
[  5]   1.00-2.00   sec   110 MBytes   921 Mbits/sec
[  5]   2.00-3.00   sec   108 MBytes   908 Mbits/sec
[  5]   3.00-4.00   sec   112 MBytes   940 Mbits/sec
[  5]   4.00-5.00   sec   111 MBytes   935 Mbits/sec
[  5]   5.00-6.00   sec   112 MBytes   941 Mbits/sec
[  5]   6.00-7.00   sec   111 MBytes   928 Mbits/sec
[  5]   7.00-8.00   sec   112 MBytes   940 Mbits/sec
[  5]   8.00-9.00   sec   111 MBytes   931 Mbits/sec
[  5]   9.00-10.00  sec   112 MBytes   940 Mbits/sec
[  5]  10.00-10.03  sec  3.50 MBytes   933 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.03  sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-10.03  sec  1.09 GBytes   930 Mbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

300 |

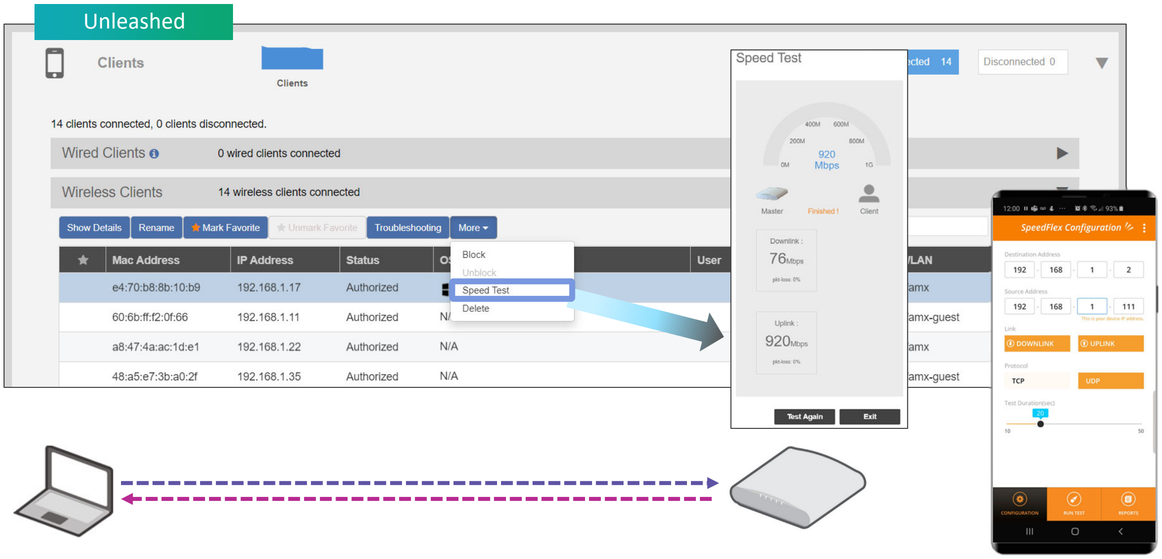
Although the most common bottleneck to any network wired or wireless is the WAN uplink, you may be required to perform throughput testing to validate the WLAN's bandwidth capabilities. Tools such as iPerf allow you to perform client / server bi-directional bandwidth testing. Measuring wireless bandwidth is done by configuring an 802.11 connected device as the client as well as configuring a server on the wired network behind the AP.

Commands are entered from each device and measurements are taken showing the bandwidth for each interval of the testing process. Additional iPerf filters can be applied to tests to adjust things like TCP window size, to setup bursting, configure a number of parallel streams or to use UDP protocols.

When testing WLAN throughput keep in mind typical throughput observed will not mirror 802.11 data rates. This is due to the overhead of contention protocols, as well as many other factors. The WLAN aggregate throughput should be expected to be around 50% of the advertised rate. This will vary between lab, new and existing deployments.

Based on the results of your testing you may need to determine why the client is operating at a lower than expected speed. This could be due to any number of factors including distance to the AP, negotiated modulation rates, or even number of users connected to the access point.

RUCKUS Speed Test



14 clients connected, 0 clients disconnected.

Wired Clients 0 wired clients connected

Wireless Clients 14 wireless clients connected

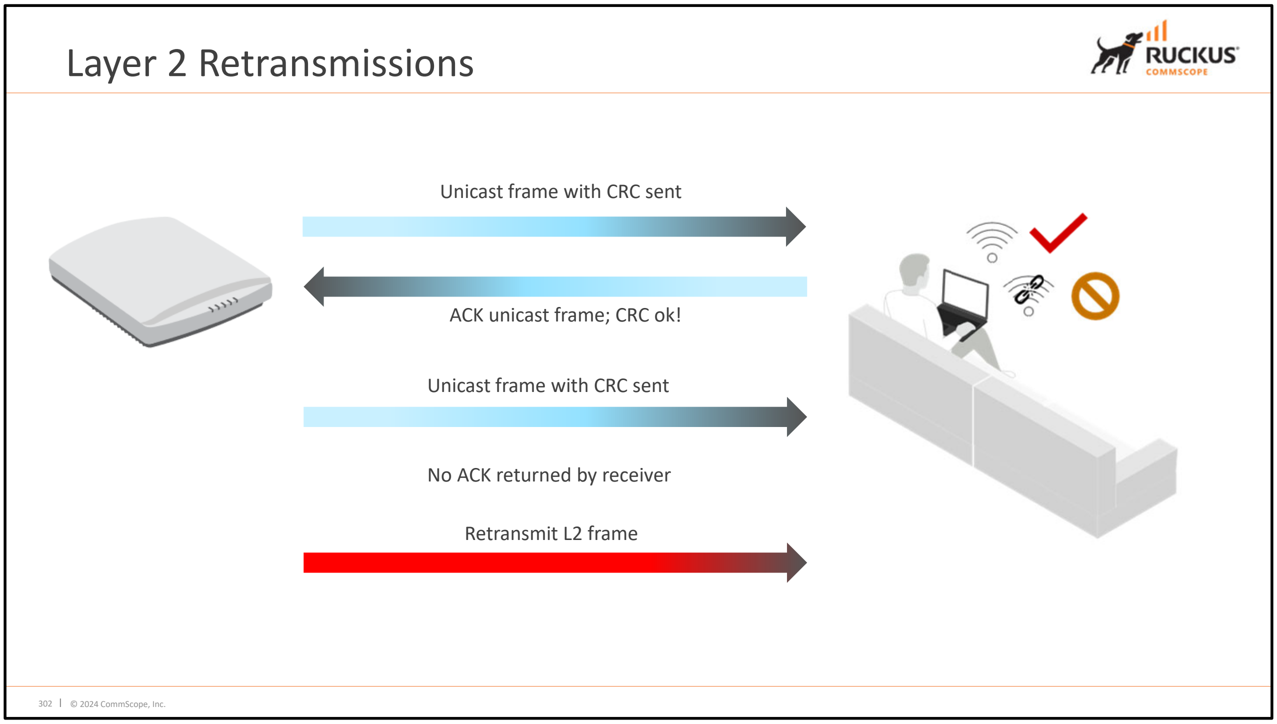
★	Mac Address	IP Address	Status	O	User	/LAN
	e4:70:b8:8b:10:b9	192.168.1.17	Authorized			amx
	60:6b:ff:f2:0f:66	192.168.1.11	Authorized	N/		amx-guest
	a8:47:4a:ac:1d:e1	192.168.1.22	Authorized	N/A		amx
	48:a5:e7:3b:a0:2f	192.168.1.35	Authorized	N/A		amx-guest

Destination Address: 192 . 168 . 1 . 2

Source Address: 192 . 168 . 1 . 111

RUCKUS provides the ability to validate client throughput by utilizing speed testing tools built into SmartZone as well as Unleashed. Rather than the client/server method used by iPerf, Speed test for unleashed tests bandwidth directly between the client and the AP.

From either SmartZone or Unleashed select the wireless client you wish to test and choose ***more***. From the drop down menu choose ***Speed Test*** , additional plug-ins may be required, once installed choose ***start*** to begin the test. SpeedFlex is also available as a mobile app available from the Apple app store or google play store, which allows you to perform a speed test from your handheld device to any SmartZone, Unleashed or Cloud Managed AP.



Layer 2 Retransmissions

Unicast frame with CRC sent

ACK unicast frame; CRC ok!

Unicast frame with CRC sent

No ACK returned by receiver

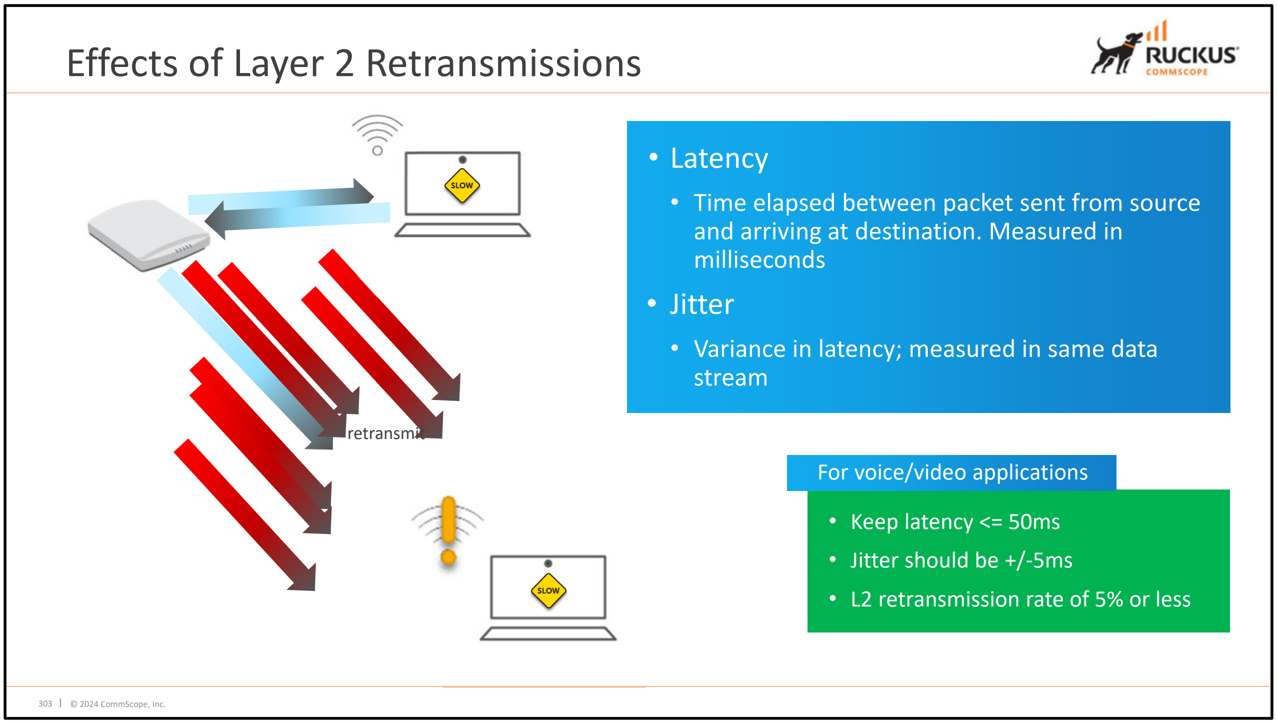
Retransmit L2 frame

302 | © 2024 CommScope, Inc.

802.11 retransmissions occur at Layer 2 but are typically a symptom of a Layer 1 problems or other WLAN design issues. In either case, retransmissions affect WLAN performance. A retransmission occurs when 802.11 frames fail their cyclic redundancy check (CRC) after being received and no acknowledgement is sent back to the transmitting device.

In normal operation the 802.11 radio will send unicast frames that will include a CRC in the trailer. The receiver will use the CRC to validate the integrity of the data received. If the CRC passes, the frame was not corrupted during transit and the receiver will send back an acknowledgement (ACK) frame to the transmitter.

However, when there is collision of RF in the air or otherwise corruption of the frame, the receiver will not be able to pass the CRC check on the unicast frame and as such will not send back an ACK to the transmitter. This causes the transmitter to retransmit the frame. These retransmissions consume additional airtime and create additional overhead to process and retransmit.



Effects of Layer 2 Retransmissions

- Latency
  - Time elapsed between packet sent from source and arriving at destination. Measured in milliseconds
- Jitter
  - Variance in latency; measured in same data stream

For voice/video applications

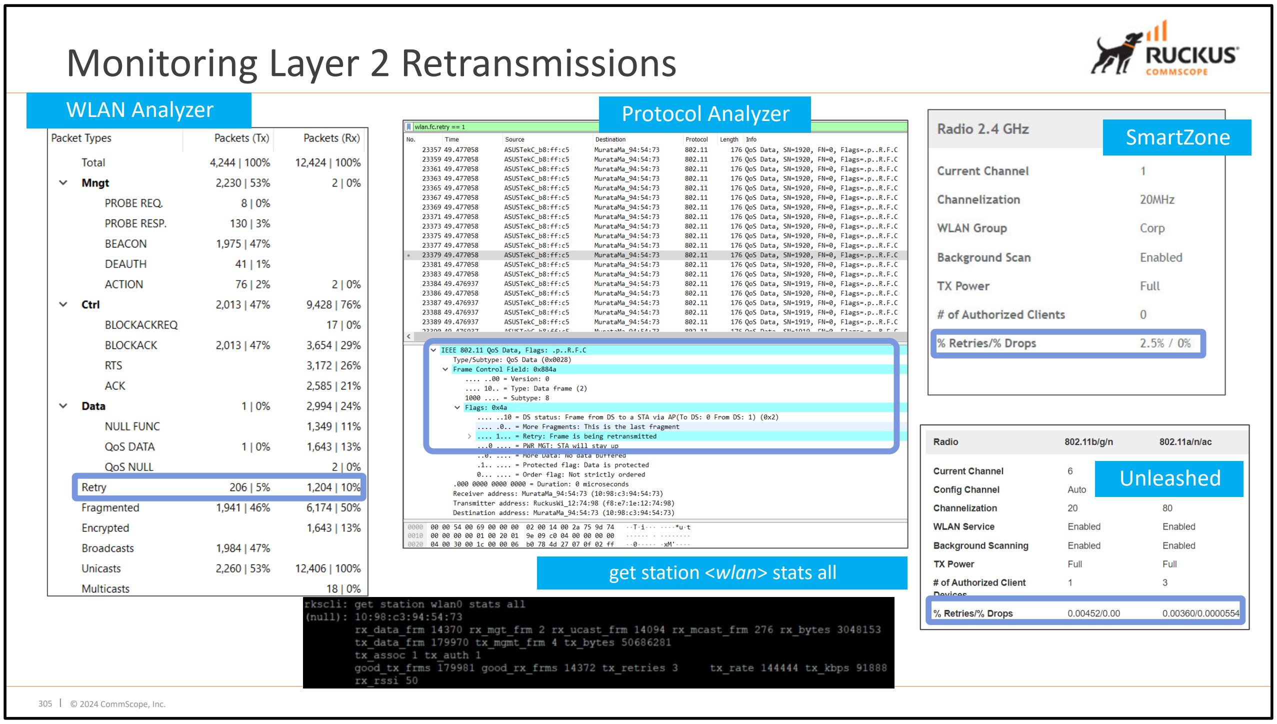
- Keep latency <= 50ms
- Jitter should be +/-5ms
- L2 retransmission rate of 5% or less

303 | © 2024 CommScope, Inc.

Retransmissions themselves are not abnormal especially in the 2.4GHz space. However, it is when these Layer 2 retransmissions increase in scale that they become an issue and negatively impact the WLAN. These impacts can bee seen in the form of increased airtime consumption and decreased quality.

Increases in airtime consumption due to excessive retransmits will reduce the overall throughput of your WLAN. Excessive L2 retransmissions also impact the ability to provide a consistent delivery of traffic which sensitive applications such as VoIP and video streaming require. Retransmits can reduce quality and introduce echo or gaps in the video stream.

These quality issues are caused because of the increase of latency and jitter, due to the retransmissions. Latency is the time it takes for packets to be delivered from the source to the destination measured in milliseconds. Jitter is variation of the latency. For instance packets steadily arriving at 30ms packet after packet make for a smooth audio-visual stream. However when packets start coming in at 150ms, the next at 200ms, the next at 170ms, that variation is called jitter and it can break up the quality of the voice or video application. Jitter buffers, which used by client devices to help alleviate the effect of this cannot compensate for large amounts of retransmits on the WLAN.



Monitoring Layer 2 Retransmissions

WLAN Analyzer

Packet Types	Packets (Tx)	Packets (Rx)
Total	4,244 | 100%	12,424 | 100%
Mngt	2,230 | 53%	2 | 0%
PROBE REQ.	8 | 0%	
PROBE RESP.	130 | 3%	
BEACON	1,975 | 47%	
DEAUTH	41 | 1%	
ACTION	76 | 2%	2 | 0%
Ctrl	2,013 | 47%	9,428 | 76%
BLOCKACKREQ		17 | 0%
BLOCKACK	2,013 | 47%	3,654 | 29%
RTS		3,172 | 26%
ACK		2,585 | 21%
Data	1 | 0%	2,994 | 24%
NULL FUNC		1,349 | 11%
QoS DATA	1 | 0%	1,643 | 13%
QoS NULL		2 | 0%
Retry	206 | 5%	1,204 | 10%
Fragmented	1,941 | 46%	6,174 | 50%
Encrypted		1,643 | 13%
Broadcasts	1,984 | 47%	
Unicasts	2,260 | 53%	12,406 | 100%
Multicasts		18 | 0%

Protocol Analyzer

```
wlan.fc.retry == 1
No.    Time       Source              Destination          Protocol  Length Info
 23357 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23359 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23361 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23363 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23365 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23367 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23369 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23371 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23373 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23375 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23377 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23379 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23381 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23383 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23384 49.476937  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1919, FN=0, Flags=.p..R.F.C
 23386 49.477058  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1920, FN=0, Flags=.p..R.F.C
 23387 49.476937  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1919, FN=0, Flags=.p..R.F.C
 23388 49.476937  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1919, FN=0, Flags=.p..R.F.C
 23389 49.476937  ASUSTekC_b8:ff:c5   MurataMa_94:54:73    802.11    176 QoS Data, SN=1919, FN=0, Flags=.p..R.F.C

IEEE 802.11 QoS Data, Flags: .p..R.F.C
   Type/Subtype: QoS Data (0x0028)
   Frame Control Field: 0x884a
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
      Flags: 0x4a
         .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
         .... .0.. = More Fragments: This is the last fragment
         .... 1... = Retry: Frame is being retransmitted
         ...0 .... = PWR MGT: STA will stay up
         ..0. .... = More Data: No data buffered
         .1.. .... = Protected flag: Data is protected
         0... .... = Order flag: Not strictly ordered
   .000 0000 0000 0000 = Duration: 0 microseconds
   Receiver address: MurataMa_94:54:73 (10:98:c3:94:54:73)
   Transmitter address: RuckusWi_12:74:98 (f8:e7:1e:12:74:98)
   Destination address: MurataMa_94:54:73 (10:98:c3:94:54:73)

0000  00 00 54 00 69 00 00 00  02 00 14 00 2a 75 9d 74   ··T·i··· ····*u·t
0010  00 00 00 00 01 00 20 01  9e 09 c0 04 00 00 00 00   ······ · ········
0020  04 00 30 00 1c 00 00 06  b0 78 4d 27 07 0f 02 ff   ··0····· ·xM'····
```

SmartZone

Radio 2.4 GHz	
Current Channel	1
Channelization	20MHz
WLAN Group	Corp
Background Scan	Enabled
TX Power	Full
# of Authorized Clients	0
% Retries/% Drops	2.5% / 0%

Unleashed

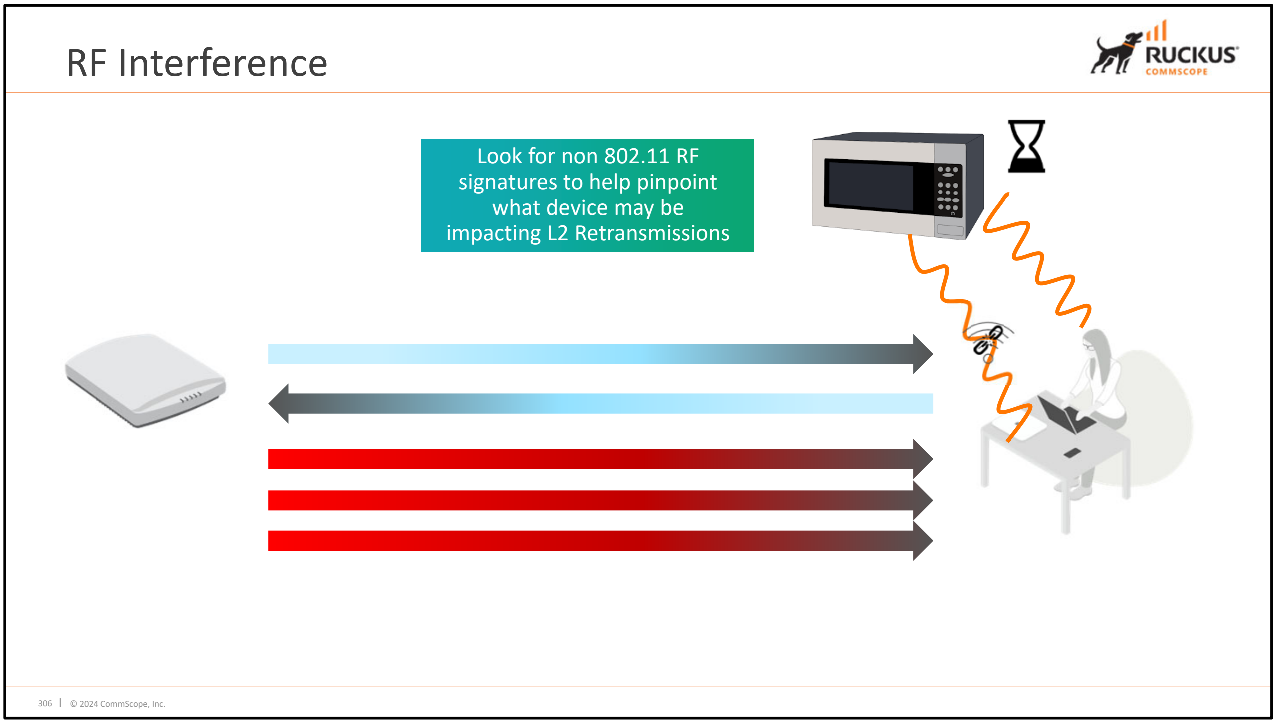
Radio	802.11b/g/n	802.11a/n/ac
Current Channel	6	
Config Channel	Auto	
Channelization	20	80
WLAN Service	Enabled	Enabled
Background Scanning	Enabled	Enabled
TX Power	Full	Full
# of Authorized Client Devices	1	3
% Retries/% Drops	0.00452/0.00	0.00360/0.0000554

get station <*wlan*> stats all

```
rkscli: get station wlan0 stats all
(null): 10:98:c3:94:54:73
        rx_data_frm 14370 rx_mgt_frm 2 rx_ucast_frm 14094 rx_mcast_frm 276 rx_bytes 3048153
        tx_data_frm 179970 tx_mgmt_frm 4 tx_bytes 50686281
        tx_assoc 1 tx_auth 1
        good_tx_frms 179981 good_rx_frms 14372 tx_retries 3     tx_rate 144444 tx_kbps 91888
        rx_rssi 50
```

305 | © 2024 CommScope, Inc.

You can utilize layer 2 protocol analyzers to obtain a view into the layer 2 retransmits for a specific client, WLAN or access point. Many network management systems and controllers such as RUCKUS SmartZone and Unleashed include the ability to look at L2 retries for all APs they manage as simple percentage from the perspective of an individual APs radio. Utilizing the ‘get station’ CLI command you can check the tx_retries for a specific WLAN and/or client. Keep in mind exceeding a 20% retransmission rate will usually impact performance on the WLAN.



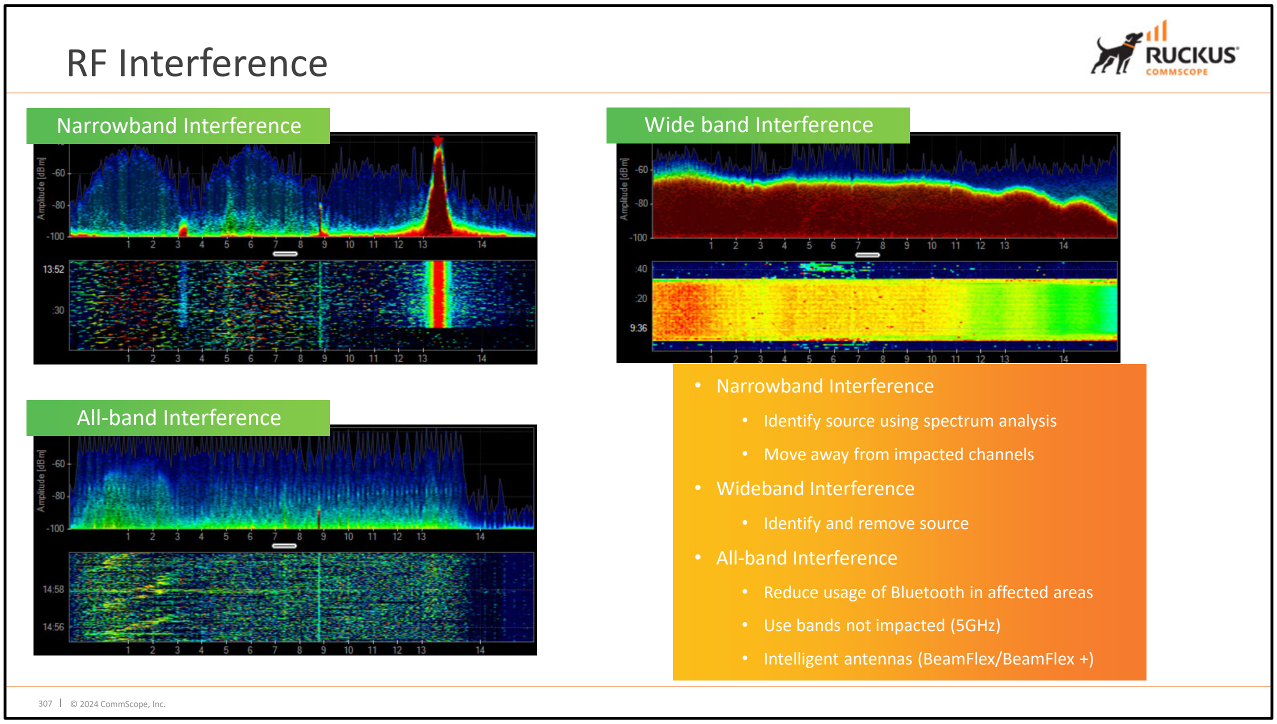
RF Interference

Look for non 802.11 RF signatures to help pinpoint what device may be impacting L2 Retransmissions

306 | © 2024 CommScope, Inc.

Non 802.11 RF interference is the major contributor to Layer 2 retransmissions. This can corrupt the frames in the air making the receiver fail the CRC check or even block it from receiving the frame at all. You will need to identify these RF sources in your environment by using spectrum analysis tools to identify the RF signature of the device causing the interference.

In the example shown here we’re only seeing Layer 2 retransmits intermittently. As soon as the microwave turns off the connection stabilizes and continues to operate normally. If there is a pattern to when your Layer 2 retransmits are occurring, use that information to help identify the cause of the interference.



RF Interference

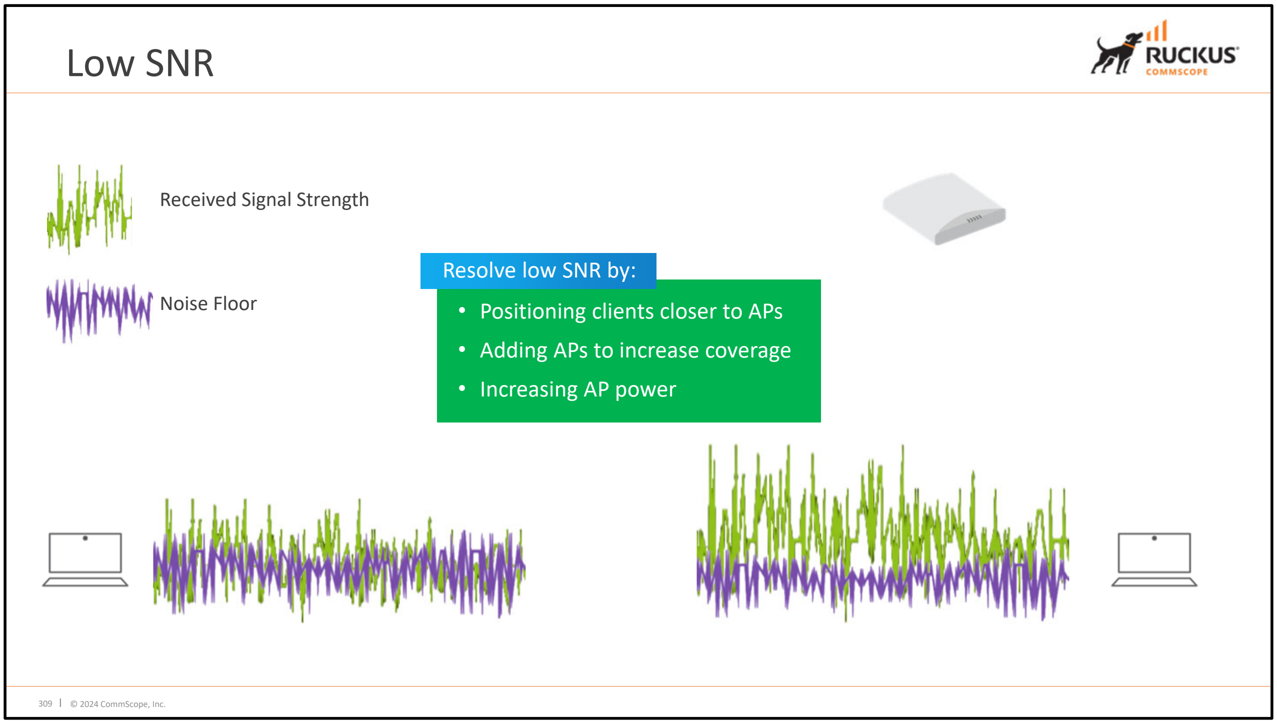
- Narrowband Interference
  - Identify source using spectrum analysis
  - Move away from impacted channels
- Wideband Interference
  - Identify and remove source
- All-band Interference
  - Reduce usage of Bluetooth in affected areas
  - Use bands not impacted (5GHz)
  - Intelligent antennas (BeamFlex/BeamFlex +)

307 | © 2024 CommScope, Inc.

RF interference is another common source of WLAN issues in Layer 1 which can be propagated by 802.11 and non-802.11 sources. In the case of non-802.11 RF interference it can completely drown out 802.11 radios effectively denying service to them. In the case of 802.11 RF interference the amplitude is such that other 802.11 radios sense the energy during a clear channel assessment and defer transmissions. Both are something that you should look to avoid but understand how to deal with. RF interference is typically categorized into one of three types, narrowband, wideband and all-band.

Narrowband interference is a high amplitude signal that impacts a single or multiple channels. Typically this is caused by cordless phones, video cameras, wireless mice, keyboards and some microwaves. The resolution in these cases is to use spectrum analysis to identify where the interference occurs and move your channel settings away from it.

Wideband interference is where a signal with high amplitude is seen across all channels in the band. This can be caused by some microwaves, remote controlled drones, healthcare equipment and even purpose-built jammers. Using a spectrum analyzer to identify the source of the interference and removing it (in cases where this is feasible) from the environment is a valid resolution.



Low SNR

Received Signal Strength

Noise Floor

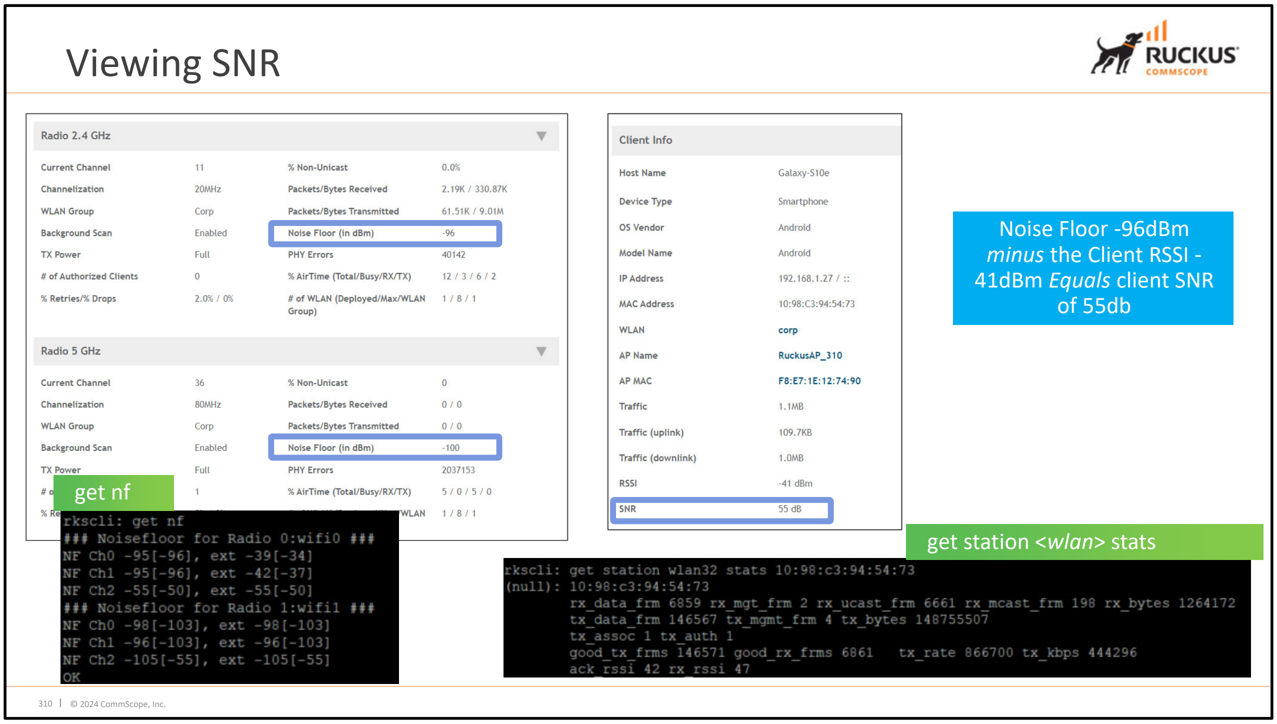
Resolve low SNR by:

- Positioning clients closer to APs
- Adding APs to increase coverage
- Increasing AP power

309 | © 2024 CommScope, Inc.

A low signal-to-noise ratio is another common cause of Layer 2 retransmissions. If noise floor and received signals are too close to the same level the client will have a low SNR and the data transmissions can become corrupt resulting in Layer 2 retransmits.

In the example shown the laptop on the right maintains a good SNR with signal strength well above the noise floor. However the laptop on the left if further away and it's received signal is not as strong causing a much lower SNR. We can resolve low SNR by repositioning the clients closer to the AP to obtain a stronger signal. This is not however always possible or feasible, in which case you could add an additional AP to provide stronger coverage to the device on the left. You could also increase the AP power, however this should not be the first option and should be done cautiously, as doing so can introduce additional problems such as increased co-channel interference, hidden nodes, and increased AP utilization.



Viewing SNR

Radio 2.4 GHz

Current Channel	11	% Non-Unicast	0.0%
Channelization	20MHz	Packets/Bytes Received	2.19K / 330.87K
WLAN Group	Corp	Packets/Bytes Transmitted	61.51K / 9.01M
Background Scan	Enabled	Noise Floor (in dBm)	-96
TX Power	Full	PHY Errors	40142
# of Authorized Clients	0	% AirTime (Total/Busy/RX/TX)	12 / 3 / 6 / 2
% Retries/% Drops	2.0% / 0%	# of WLAN (Deployed/Max/WLAN Group)	1 / 8 / 1

Radio 5 GHz

Current Channel	36	% Non-Unicast	0
Channelization	80MHz	Packets/Bytes Received	0 / 0
WLAN Group	Corp	Packets/Bytes Transmitted	0 / 0
Background Scan	Enabled	Noise Floor (in dBm)	-100
TX Power	Full	PHY Errors	2037153
# o	1	% AirTime (Total/Busy/RX/TX)	5 / 0 / 5 / 0
% Re		WLAN	1 / 8 / 1

get nf

```
rkscli: get nf
### Noisefloor for Radio 0:wifi0 ###
NF Ch0 -95[-96], ext -39[-34]
NF Ch1 -95[-96], ext -42[-37]
NF Ch2 -55[-50], ext -55[-50]
### Noisefloor for Radio 1:wifi1 ###
NF Ch0 -98[-103], ext -98[-103]
NF Ch1 -96[-103], ext -96[-103]
NF Ch2 -105[-55], ext -105[-55]
OK
```

Client Info

Host Name	Galaxy-S10e
Device Type	Smartphone
OS Vendor	Android
Model Name	Android
IP Address	192.168.1.27 / ::
MAC Address	10:98:C3:94:54:73
WLAN	corp
AP Name	RuckusAP_310
AP MAC	F8:E7:1E:12:74:90
Traffic	1.1MB
Traffic (uplink)	109.7KB
Traffic (downlink)	1.0MB
RSSI	-41 dBm
SNR	55 dB

Noise Floor -96dBm *minus* the Client RSSI -41dBm *Equals* client SNR of 55db

get station <*wlan*> stats

```
rkscli: get station wlan32 stats 10:98:c3:94:54:73
(null): 10:98:c3:94:54:73
        rx_data_frm 6859 rx_mgt_frm 2 rx_ucast_frm 6661 rx_mcast_frm 198 rx_bytes 1264172
        tx_data_frm 146567 tx_mgmt_frm 4 tx_bytes 148755507
        tx_assoc 1 tx_auth 1
        good_tx_frms 146571 good_rx_frms 6861   tx_rate 866700 tx_kbps 444296
        ack_rssi 42 rx_rssi 47
```

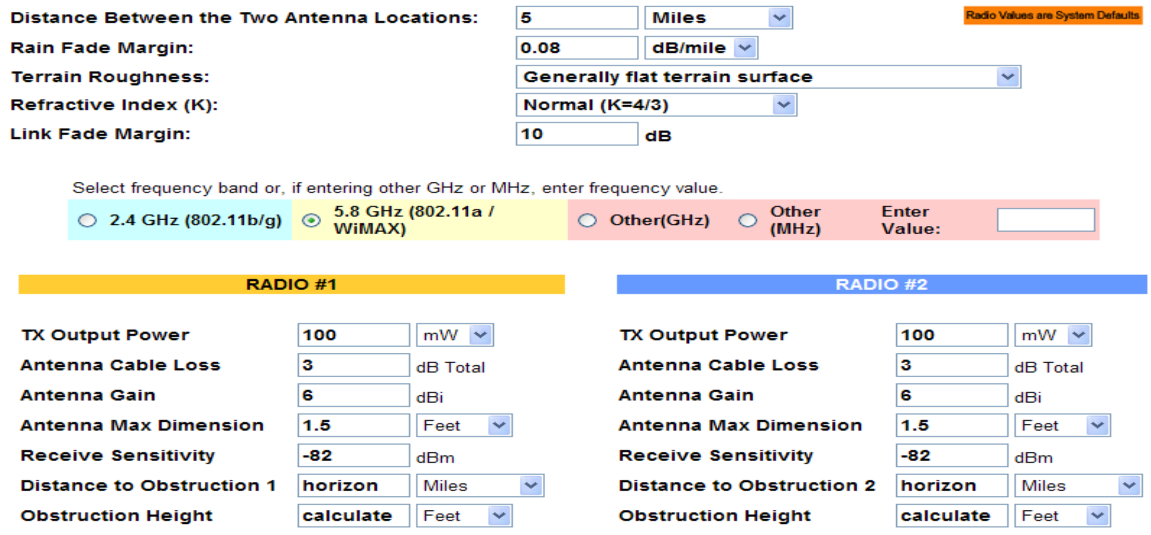
310 | © 2024 CommScope, Inc.

So how do we know if we have bad SNR? We defined good ranges of SNR and stated that the SNR should be at least 20dB, and ideally 25dB over the noise floor for good performance. RUCKUS SmartZone includes the ability to look at the noise floor from an AP perspective, per radio and also tracks client RSSI and displays the SNR value. The SNR is calculated for you, but the simple math takes the noise floor and subtracts the client RSSI. In this case the client is on 2.4 GHz and so we have an SNR of 55dB, which is excellent, but in this scenario the device is mere feet from the AP. As we know with more distance the SNR will go down.

Alternatively, you can obtain data from the CLI to calculate what the SNR would be from an AP and client perspective. From the AP you can run the command get nf to obtain a list of SNRs per radio. Running this command gives the noise floor values for both 2.4 displayed as wifi0 and 5 GHz displayed as wifi1.

To obtain the RSSI from a client perspective you can run the get station command to display RSSI values of all or specific clients connected to a specific radio.

Online RF Calculators



Radio Values are System Defaults

Distance Between the Two Antenna Locations:	5	Miles
Rain Fade Margin:	0.08	dB/mile
Terrain Roughness:	Generally flat terrain surface	
Refractive Index (K):	Normal (K=4/3)	
Link Fade Margin:	10	dB

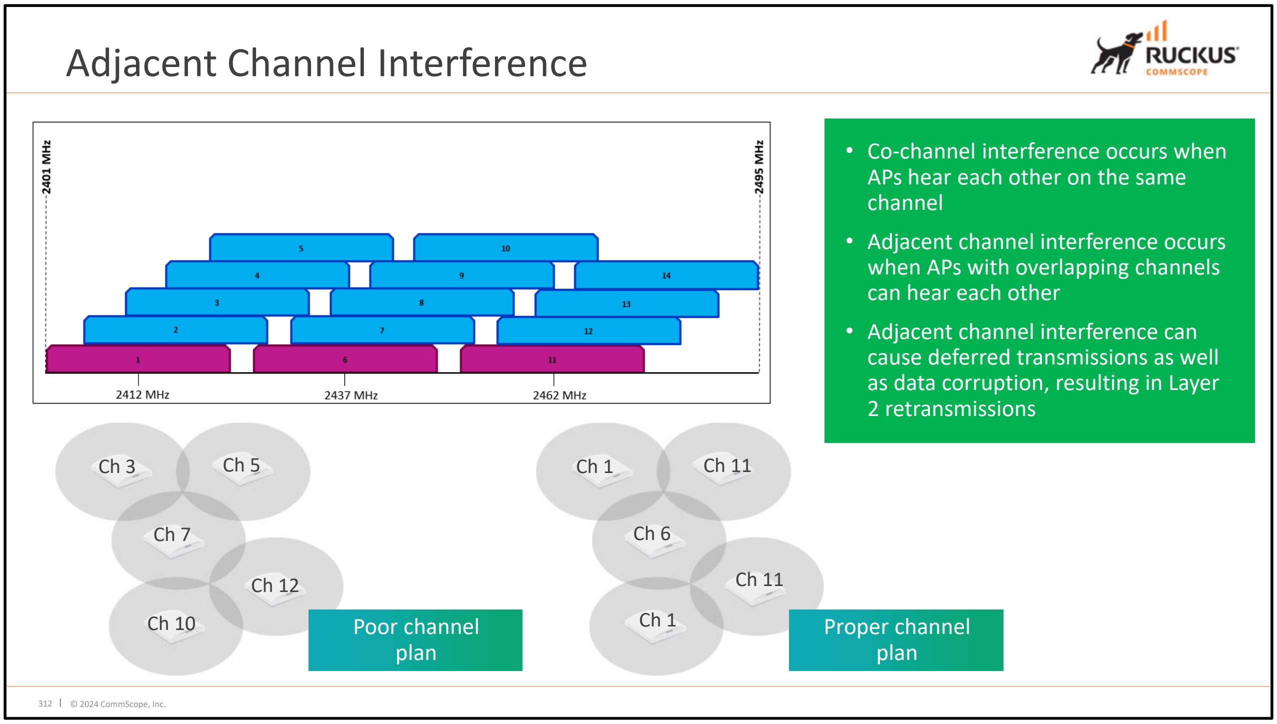
Select frequency band or, if entering other GHz or MHz, enter frequency value.

○ 2.4 GHz (802.11b/g) ● 5.8 GHz (802.11a / WiMAX) ○ Other(GHz) ○ Other (MHz) Enter Value:

RADIO #1			RADIO #2		
TX Output Power	100	mW	TX Output Power	100	mW
Antenna Cable Loss	3	dB Total	Antenna Cable Loss	3	dB Total
Antenna Gain	6	dBi	Antenna Gain	6	dBi
Antenna Max Dimension	1.5	Feet	Antenna Max Dimension	1.5	Feet
Receive Sensitivity	-82	dBm	Receive Sensitivity	-82	dBm
Distance to Obstruction 1	horizon	Miles	Distance to Obstruction 2	horizon	Miles
Obstruction Height	calculate	Feet	Obstruction Height	calculate	Feet

311 |

There are free online link budget calculators just like the dBm to mW tools. The one shown here is from Connect802.com. You can find many other calculators online for things such as path loss, Fresnel zone clearance.

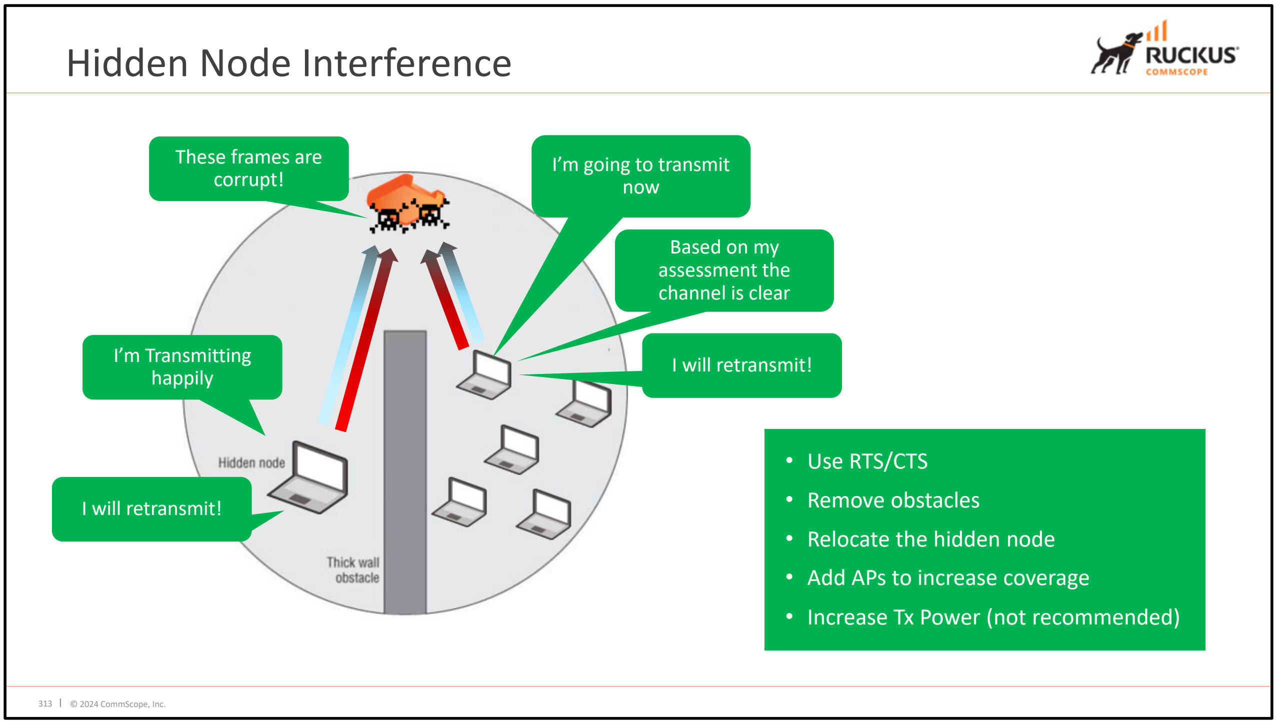


Adjacent Channel Interference

- Co-channel interference occurs when APs hear each other on the same channel
- Adjacent channel interference occurs when APs with overlapping channels can hear each other
- Adjacent channel interference can cause deferred transmissions as well as data corruption, resulting in Layer 2 retransmissions

312 | © 2024 CommScope, Inc.

Adjacent channel interference is caused when using channels that overlap in the frequency space, particularly in the 2.4 GHz band. As shown in the channel graph above you can see that many channels in this frequency overlap. Using channels that overlap in your channel plan will lead to adjacent channel interference and cause deferred transmissions as well as data corruption and cause Layer 2 retransmissions. Adjacent channel interference can be avoided with proper channel planning using non-overlapping channels.



Hidden Node Interference

These frames are corrupt!
I'm going to transmit now
Based on my assessment the channel is clear
I'm Transmitting happily
I will retransmit!
Hidden node
I will retransmit!
Thick wall obstacle

- Use RTS/CTS
- Remove obstacles
- Relocate the hidden node
- Add APs to increase coverage
- Increase Tx Power (not recommended)

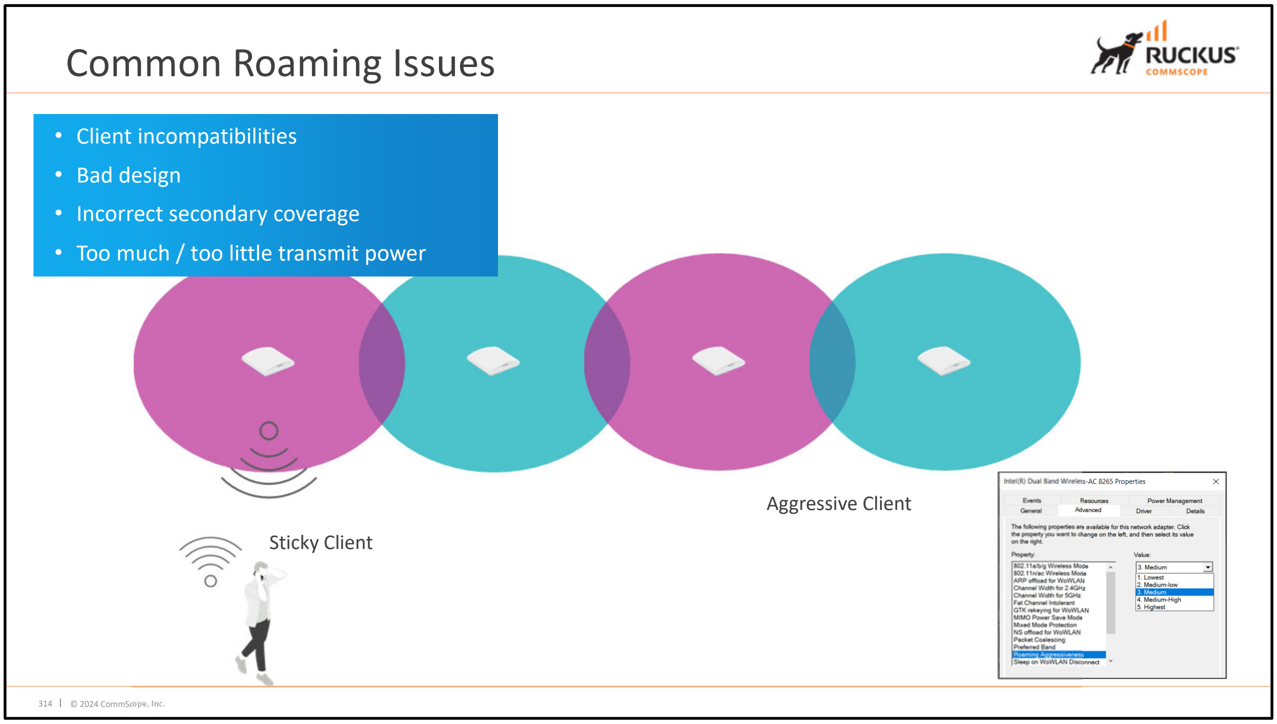
313 | © 2024 CommScope, Inc.

Hidden nodes can also cause Layer 2 retransmits because these hidden nodes are not heard by other stations when performing a clear channel assessment (CCA). The result being that other stations successfully perform the CCA and begin transmitting. When this occurs with stations in the same frequency, transmission is corrupted and layer 2 retransmission begins. The hidden node will continue to corrupt transmissions for the stations on the other side of the wall because it cannot hear their CCA. The result of this is an increase in Layer 2 retransmissions which slows throughput and adds latency.

There are several causes for hidden nodes, in this example it is a thick wall, but be other obstacles in the physical environment. Alternatively, if you had an AP with high Tx power and two stations at opposite ends of the RF cell, those stations may not be able to hear each other and again the hidden node interference would occur. Some of these issues can be attributed to poor WLAN design or changes in the environment over time.

You may be clued into a hidden node problem by users complaining of slow Wi-Fi. Using a protocol analyzer you can identify an increased retransmission rate for one node, this would be the hidden node. Once you have identified the hidden node there are several options available to resolve it.

Request-to-Send/Clear-to-Send (RTS/CTS) can be used ether temporarily or permanently to resolve hidden node problems. Typically the use of RTS/CTS decreases throughput because it adds additional processing to the AP, but in some cases use of RTS/CTS may increase throughput if collisions and retransmits were high.



Common Roaming Issues

- Client incompatibilities
- Bad design
- Incorrect secondary coverage
- Too much / too little transmit power

Intel(R) Dual Band Wireless-AC 8265 Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 802.11a/b/g Wireless Mode
- 802.11n/ac Wireless Mode
- ARP offload for WoWLAN
- Channel Width for 2.4GHz
- Channel Width for 5GHz
- Fat Channel Intolerant
- GTK rekeying for WoWLAN
- MIMO Power Save Mode
- Mixed Mode Protection
- NS offload for WoWLAN
- Packet Coalescing
- Preferred Band
- Roaming Aggressiveness
- Sleep on WoWLAN Disconnect

Value: 3. Medium

1. Lowest
2. Medium-low
3. Medium
4. Medium-High
5. Highest

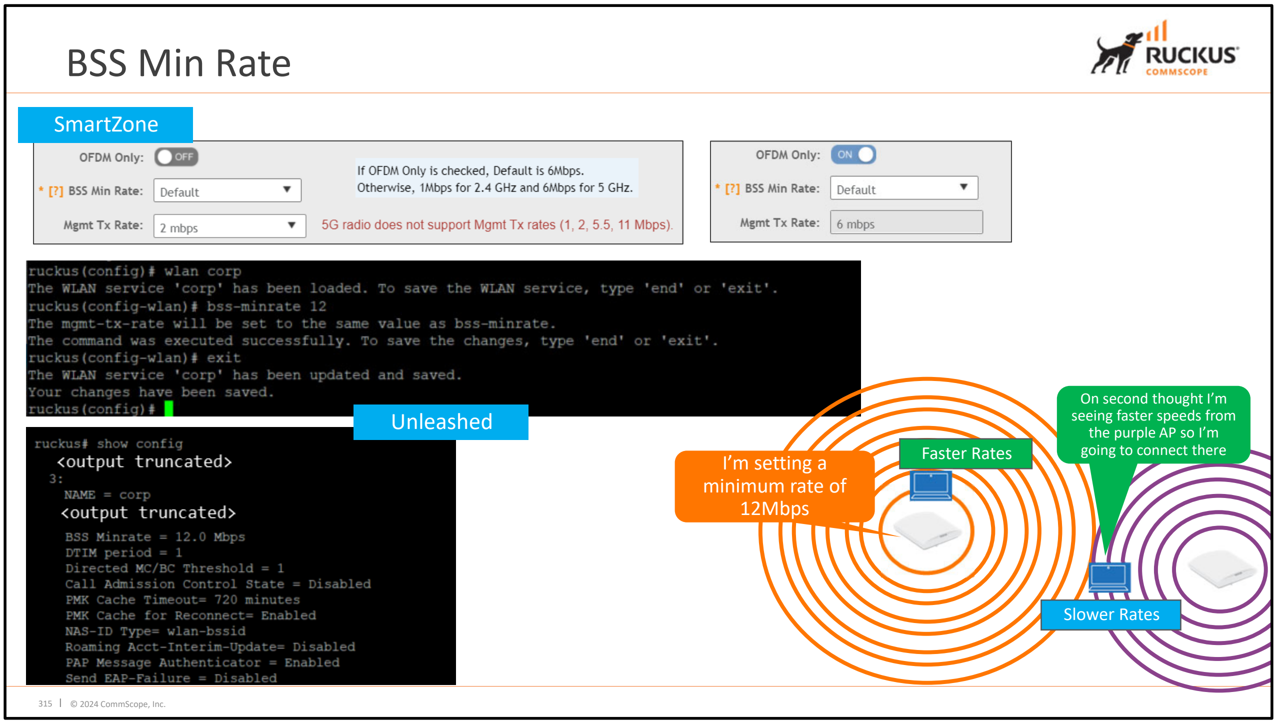
314 | © 2024 CommScope, Inc.

Roaming is typically a decision the client station makes as it moves through the WLAN, although there are ways an AP can influence roaming. Clients typically look at signal strength, SNR, missed beacons and retries when making their decision to roam. Most commonly roaming problems stem from client drivers or client device incompatibility. You should be aware of variance in devices and capabilities in your environment.

Bad WLAN design can result in poor roaming as well. For instance mounting APs close to corners in a hallway can make signal drop quickly when clients turn a corner or coverage can bleed through floors causing devices to connect to APs in the floor above or below. It is important to make sure that you have proper secondary coverage. Typically an RF coverage overlap of 15-20% is recommended.

APs with too much transmit power can cause clients to roam to them unnecessarily. APs with not enough transmit power may not provide the coverage intended and cause clients to roam prematurely or find themselves in a dead zone with no coverage.

A clients roaming aggressiveness can also be problematic. Too high and the client will hop between APs even though the signal strength is stable. Too low and the client becomes sticky and refuses to roam even though a better signal is available.



BSS Min Rate

SmartZone

OFDM Only: OFF

* [?] BSS Min Rate: Default

Mgmt Tx Rate: 2 mbps

If OFDM Only is checked, Default is 6Mbps.
Otherwise, 1Mbps for 2.4 GHz and 6Mbps for 5 GHz.

5G radio does not support Mgmt Tx rates (1, 2, 5.5, 11 Mbps).

OFDM Only: ON

* [?] BSS Min Rate: Default

Mgmt Tx Rate: 6 mbps

```
ruckus(config)# wlan corp
The WLAN service 'corp' has been loaded. To save the WLAN service, type 'end' or 'exit'.
ruckus(config-wlan)# bss-minrate 12
The mgmt-tx-rate will be set to the same value as bss-minrate.
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-wlan)# exit
The WLAN service 'corp' has been updated and saved.
Your changes have been saved.
ruckus(config)#
```

Unleashed

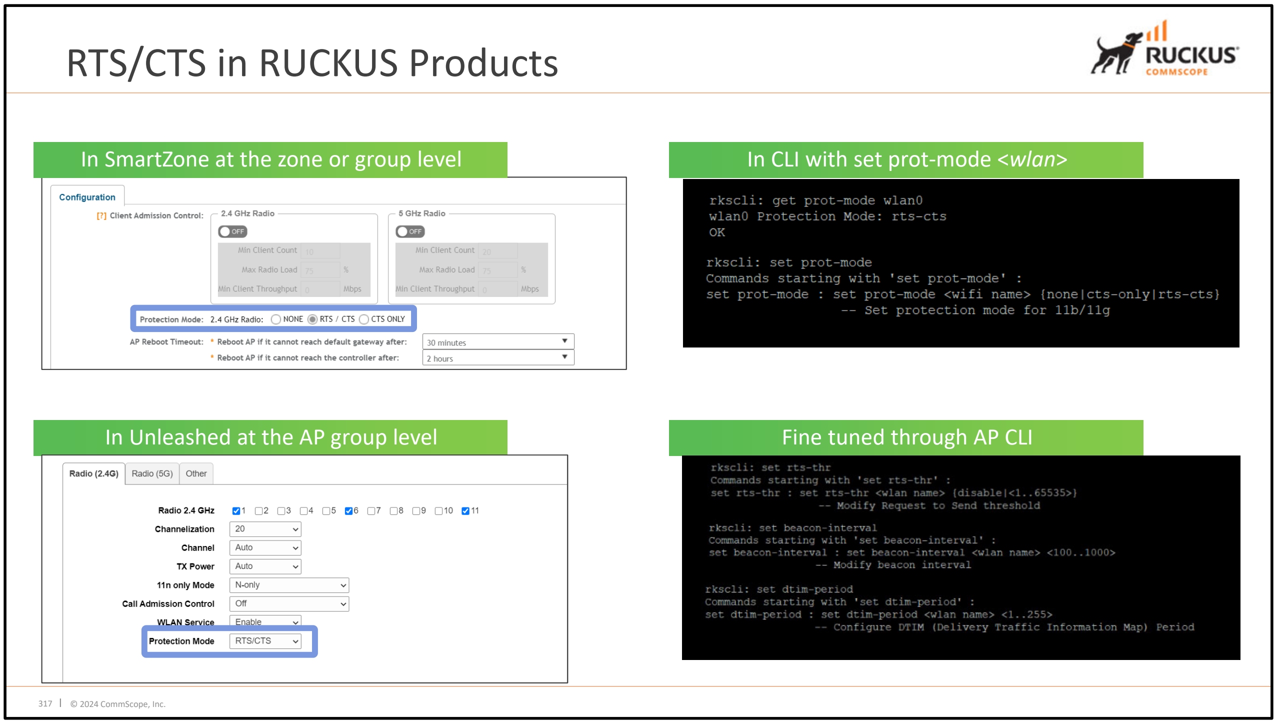
```
ruckus# show config
   <output truncated>
  3:
    NAME = corp
    <output truncated>
    BSS Minrate = 12.0 Mbps
    DTIM period = 1
    Directed MC/BC Threshold = 1
    Call Admission Control State = Disabled
    PMK Cache Timeout= 720 minutes
    PMK Cache for Reconnect= Enabled
    NAS-ID Type= wlan-bssid
    Roaming Acct-Interim-Update= Disabled
    PAP Message Authenticator = Enabled
    Send EAP-Failure = Disabled
```

I'm setting a minimum rate of 12Mbps
Faster Rates
On second thought I'm seeing faster speeds from the purple AP so I'm going to connect there
Slower Rates

In some cases client roaming aggressiveness cannot be configured. Smartphones and tablets for example may not allow for the modification to the frequency in which they perform background scanning. In other cases a client will not roam even though the signal from another AP is better and provides better throughput.

As mentioned previously. Roaming is a client decision, but it can be influenced by APs. Once such way that an AP can influence a client to roam is by adjusting the minimum rate at which devices can connect. As we know devices closer to the AP have better RSSI values and the stronger signal will give those devices a better connection with higher throughput. Clients at the edge of coverage cell can negotiate slower rates as little as 1Mbps. However in setting a minimum rate, devices wanting to step down below the minimum defined rate would not be able to do so and would look to roam to an AP with better coverage rather than persist with a slow connection.

This minimum rate is called the basic service set minimum rate, or, BSS min rate. In RUCKUS products this rate is defined at the WLAN level and can be configured to 1, 2, 5.5, 12 and 24 Mbps. It is important to know the least capable devices in your network before adjusting this rate as it could impact the ability for lesser capable clients to connect. Also it is a best practice to select a mandatory data rate (such as 12, and 24) as not all of the optional rates (such as 18) are supported by all clients. By default in SmartZone the BSS min rate is configured as 1Mb for 2.4GHz and 6Mb for 5GHz.



RTS/CTS in RUCKUS Products

In SmartZone at the zone or group level

Configuration

[?] Client Admission Control:

2.4 GHz Radio			5 GHz Radio		
OFF			OFF		
Min Client Count	10		Min Client Count	20	
Max Radio Load	75	%	Max Radio Load	75	%
Min Client Throughput	0	Mbps	Min Client Throughput	0	Mbps

Protection Mode: 2.4 GHz Radio: ○ NONE ● RTS / CTS ○ CTS ONLY

AP Reboot Timeout: * Reboot AP if it cannot reach default gateway after: 30 minutes

* Reboot AP if it cannot reach the controller after: 2 hours

In CLI with set prot-mode <*wlan*>

```
 rkscli: get prot-mode wlan0
 wlan0 Protection Mode: rts-cts
 OK

rkscli: set prot-mode
Commands starting with 'set prot-mode' :
set prot-mode : set prot-mode <wifi name> {none|cts-only|rts-cts}
                 -- Set protection mode for 11b/11g
```

In Unleashed at the AP group level

Radio (2.4G) | Radio (5G) | Other

Radio 2.4 GHz ☑1 □2 □3 □4 □5 ☑6 □7 □8 □9 □10 ☑11

Channelization: 20

Channel: Auto

TX Power: Auto

11n only Mode: N-only

Call Admission Control: Off

WLAN Service: Enable

Protection Mode: RTS/CTS

Fine tuned through AP CLI

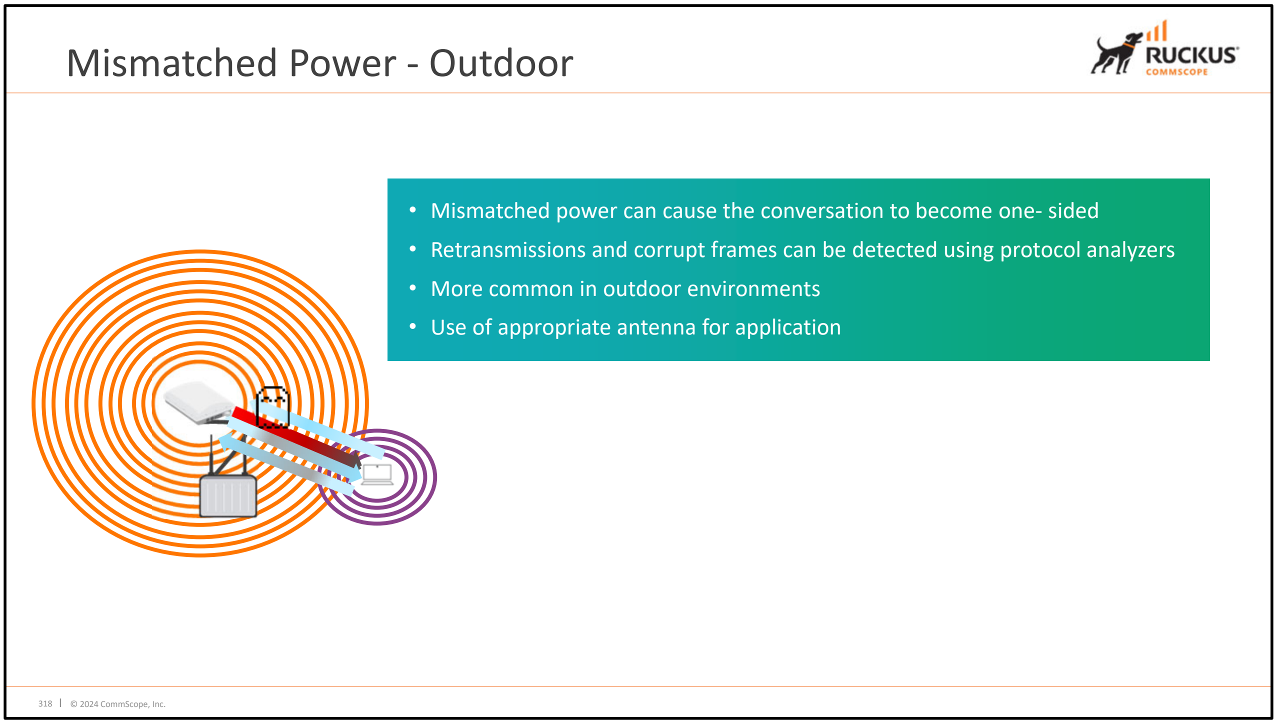
```
 rkscli: set rts-thr
 Commands starting with 'set rts-thr' :
 set rts-thr : set rts-thr <wlan name> {disable|<1..65535>}
                  -- Modify Request to Send threshold

 rkscli: set beacon-interval
 Commands starting with 'set beacon-interval' :
 set beacon-interval : set beacon-interval <wlan name> <100..1000>
                  -- Modify beacon interval

rkscli: set dtim-period
Commands starting with 'set dtim-period' :
set dtim-period : set dtim-period <wlan name> <1..255>
                 -- Configure DTIM (Delivery Traffic Information Map) Period
```

317 | © 2024 CommScope, Inc.

RTS/CTS is enabled by default and can modified to disable the protection altogether or switch to CTS-only mode. CTS only mode (or CTS-to-Self) is better for mixed mode environments and provides less protection against hidden nodes and collisions. However CTS only has the benefit of less overhead and offers higher potential throughput.

In SmartZone the protection mode can be set within the advanced settings of the Zone or AP Group. In Unleashed the mode is set at the AP group level.

These settings can also be verified at an individual AP level with CLI commands. Additionally through the AP CLI you can modify settings, such as enabling a RTS/CTS threshold, which determines at what packet length the function is triggered. Or change the beacon and delivery traffic indication message (DTIM) rates.



Mismatched Power - Outdoor

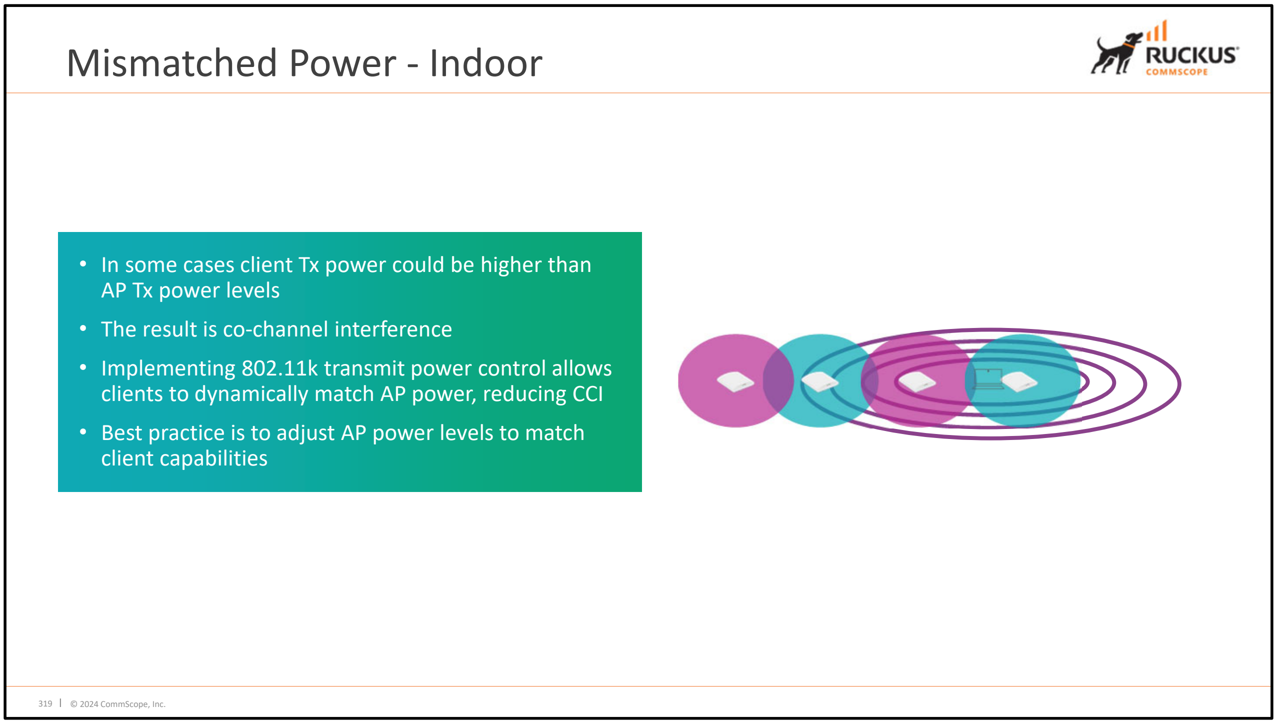
- Mismatched power can cause the conversation to become one- sided
- Retransmissions and corrupt frames can be detected using protocol analyzers
- More common in outdoor environments
- Use of appropriate antenna for application

318 | © 2024 CommScope, Inc.

The AP in this scenario can transmit a unicast frame to a client and because it is transmitting at (100mW), the client will hear it. However the client will attempt to respond with an ACK, but its transmitted power is only 20mW and as such, the AP never receives it and so begin Layer 2 retransmits.

You wont typically see this in high density deployments because those APs usually operate at much lower power levels, it is more likely you might encounter this in an outdoor setting. You can diagnose a power mismatch by using a protocol analyzer looking for corrupt frames, listening near the AP you would see corruption versus listening near the client where you would not detect corruption.

In this case a solution could be to deploy an antenna with increased gain, rather than running at full power levels. Increasing an APs gain not only amplifies the transmitted signal it also amplify the signal received as we discussed in the RUCKUS Wireless Fundamentals course.



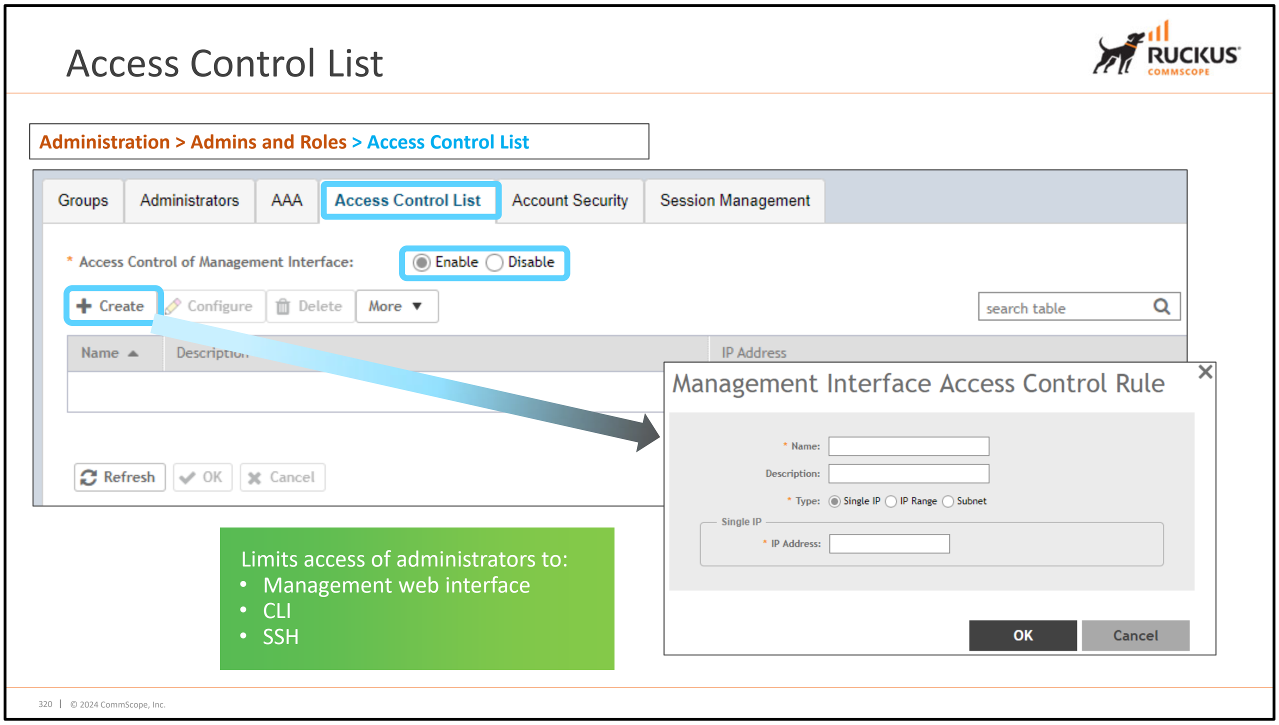
Mismatched Power - Indoor

- In some cases client Tx power could be higher than AP Tx power levels
- The result is co-channel interference
- Implementing 802.11k transmit power control allows clients to dynamically match AP power, reducing CCI
- Best practice is to adjust AP power levels to match client capabilities

As previously discussed, for indoor deployments, radios are typically set to transmit at one quarter to one eighth of their full power. This leaves APs able to perform in these environments as little as 10mW (or 10dBm) of transmit power. The client we used in the previous example had a transmit power of 20mW (or 13dBm), and while that does not seem like much of a difference it can have an impact on CCI. Couple that with the fact that many mobile devices can transmit at those power levels and they are moving around your WLAN.

For these high density deployments, a best practice is to design your WLANs AP power levels to match client capabilities. This will help ensure that clients are seeing the strongest signals from the closest APs.

In other scenarios you could look to implement Transmit Power Control (TPC) to tell clients dynamically to match the transmit power of the AP, of course these features need to be supported on the AP and client.



Access Control List

Administration > Admins and Roles > Access Control List

* Access Control of Management Interface: ● Enable ○ Disable

Management Interface Access Control Rule

* Name:

Description:

* Type: ● Single IP ○ IP Range ○ Subnet

Single IP

* IP Address:

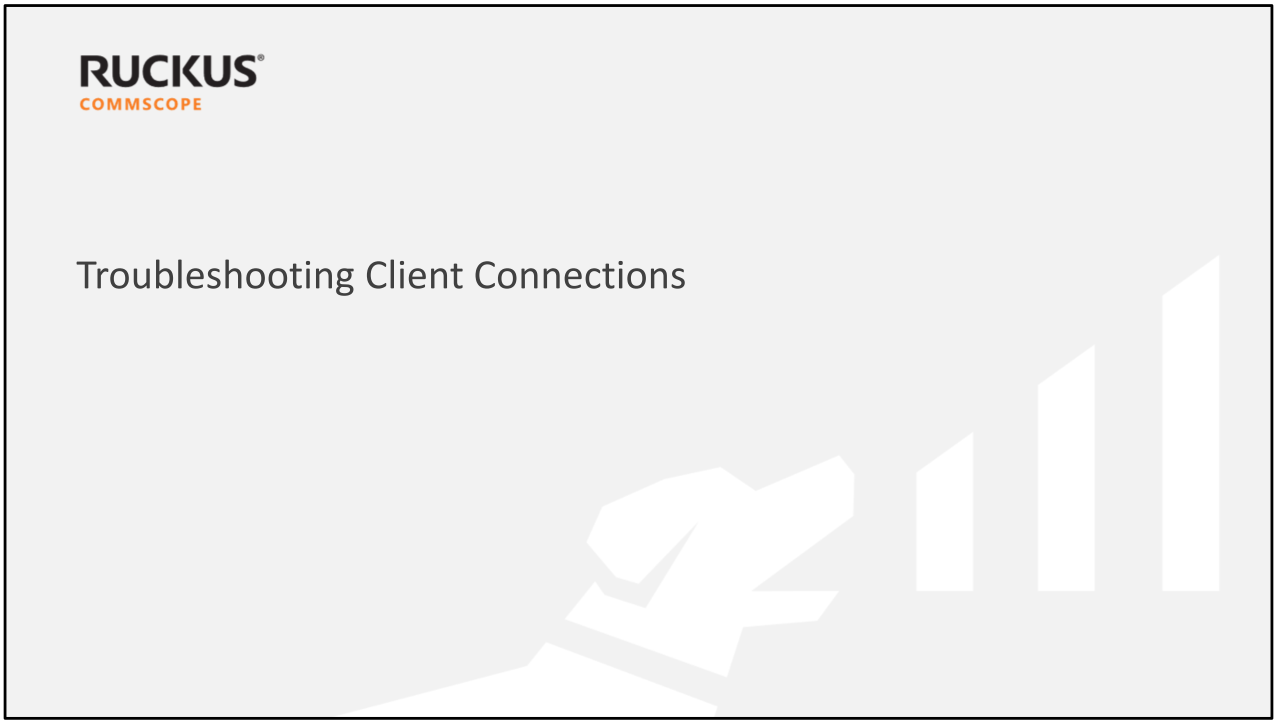
Limits access of administrators to:

- Management web interface
- CLI
- SSH

The **Access Control List** tab allows you to secure SSH/CLI access as well as the management web interface by restricting access to connections from:

- **A Single IP Address**
- **An IP Range**
- **An IP Subnet**

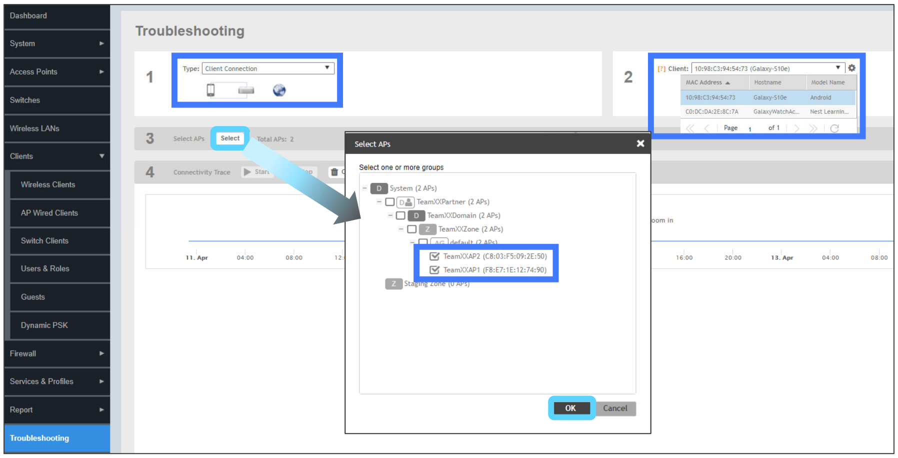
If you enable the Access Control List, the management web interface will be limited by the source IPs configured. Additionally the SSH port for communications to the Management interface changes from port 22 to port 8022. This does not change the SSH port on the Control interface, which is used for controller-to-AP communications.



Troubleshooting Client Connections

Troubleshooting – Client Connection

Troubleshooting > Client Connection



Troubleshooting

1 Type: Client Connection

2 [?] Client: 10:98:C3:94:54:73 (Galaxy-S10e)

MAC Address	Hostname	Model Name
10:98:C3:94:54:73	Galaxy-S10e	Android
C0:DC:DA:2E:8C:7A	GalaxyWatchAc...	Nest Learnin...

Page 1 of 1

3 Select APs Select Total APs: 2

4 Connectivity Trace

Select APs

Select one or more groups

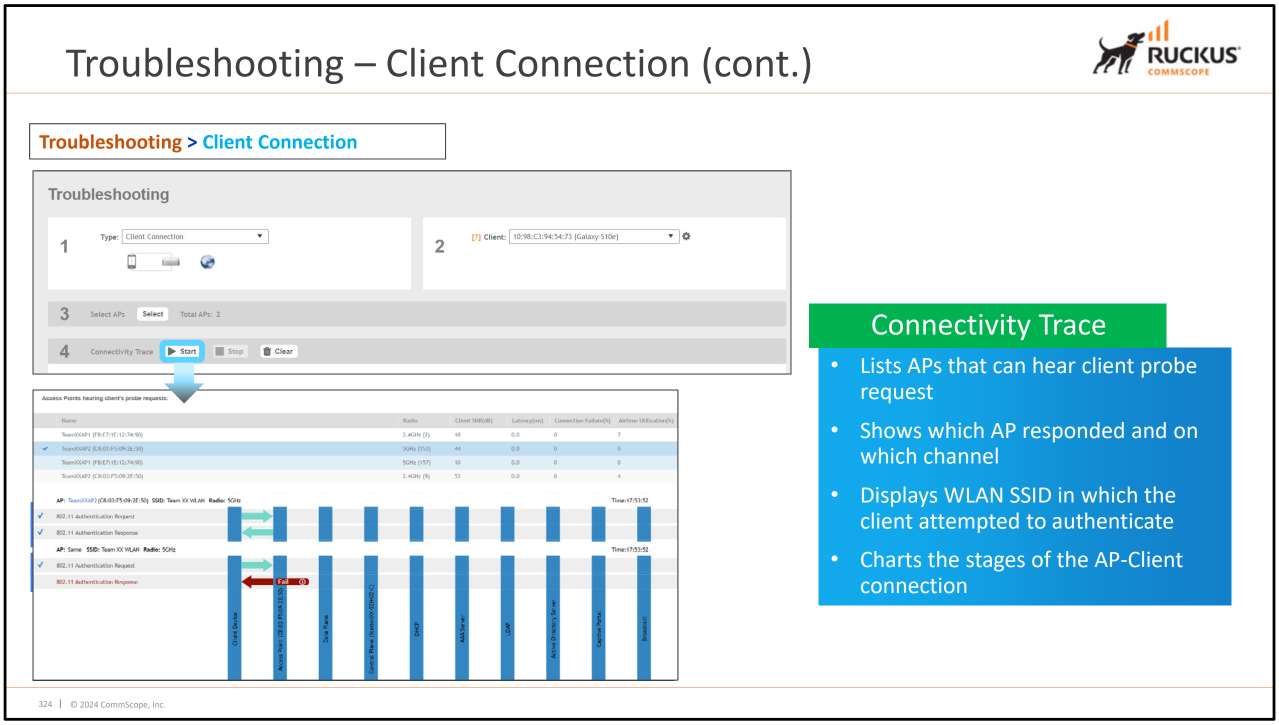
- D System (2 APs)
  - □ D TeamXXPartner (2 APs)
    - □ D TeamXXDomain (2 APs)
      - □ Z TeamXXZone (2 APs)
        - □ AG default (2 APs)
          - ☑ TeamXXAP2 (C8:03:F5:09:2E:50)
          - ☑ TeamXXAP1 (F8:E7:1E:12:74:90)
  - Z Staging Zone (0 APs)

- Set the **Type** as “Client Connection”
- Select **Client** from list; Alternatively enter full MAC address of client
- **Select** the APs in which to monitor for probe requests

323 | © 2024 CommScope, Inc.

Administrators can utilize SmartZone troubleshooting tools in real time to help diagnose problems clients may be experiencing with connectivity. Selecting **Troubleshooting** from the navigation menu allows the administrator to select which type of real-time evaluation they would like to perform. We will begin by looking at the **Client Connection**.

Next, we will select the client in which we would like to monitor, please take note that in the case of a client that has never successfully connected you can enter the full MAC Address of the client in the client field. The next step is to click **Select** and then choose which APs we will look for this client connection on and then choose **OK**.
Once the client and APs have been defined the connectivity trace is ready to be ran.



Troubleshooting – Client Connection (cont.)

Troubleshooting > Client Connection

Troubleshooting

1 Type: Client Connection

2 [?] Client: 10:98:C3:94:54:73 (Galaxy-S10e)

3 Select APs Select Total APs: 2

4 Connectivity Trace ▶ Start ■ Stop 🗑 Clear

Access Points hearing client's probe requests:

	Name	Radio	Client SNR(dB)	Latency(ms)	Connection Failure(%)	Airtime Utilization(%)
	TeamXXAP1 (F8:E7:1E:12:74:90)	2.4GHz (2)	18	0.0	0	7
✓	TeamXXAP2 (C8:03:F5:09:2E:50)	5GHz (153)	44	0.0	0	0
	TeamXXAP1 (F8:E7:1E:12:74:90)	5GHz (157)	10	0.0	0	0
	TeamXXAP2 (C8:03:F5:09:2E:50)	2.4GHz (9)	53	0.0	0	4

AP: TeamXXAP2 (C8:03:F5:09:2E:50) SSID: Team XX WLAN Radio: 5GHz Time:17:53:52

✓ 802.11 Authentication Request

✓ 802.11 Authentication Response

AP: Same SSID: Team XX WLAN Radio: 5GHz Time:17:53:52

✓ 802.11 Authentication Request

802.11 Authentication Response

Connectivity Trace

- Lists APs that can hear client probe request
- Shows which AP responded and on which channel
- Displays WLAN SSID in which the client attempted to authenticate
- Charts the stages of the AP-Client connection

324 | © 2024 CommScope, Inc.

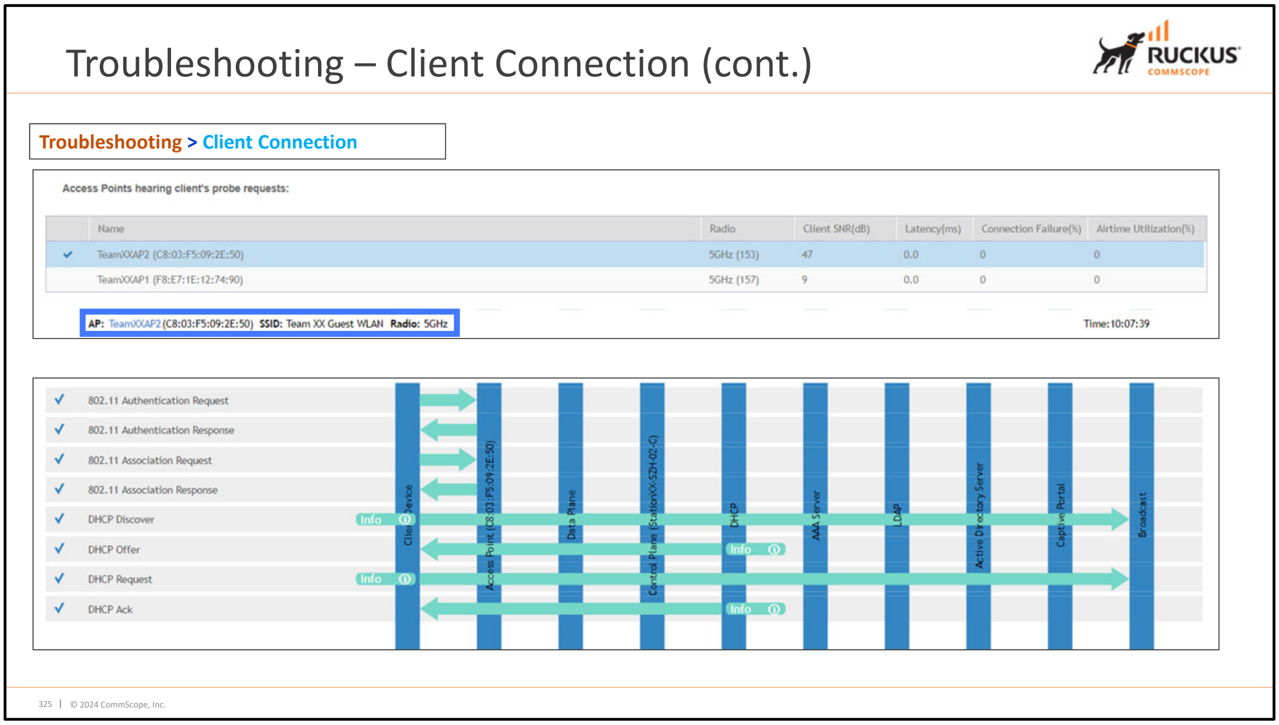
Continuing from the previous slide we are ready to begin our Connectivity Trace by selecting the **Start** button.

At this time live data begins to populate presuming that the selected client is actively attempting to connect on the APs we specified as the live trace is running. The first thing shown is a list that hear the clients probe requests (for both 2.4 and 5 GHz). The AP is highlighted and marked with a check which identifies the AP and radio this request was accepted on. Additional details such as Radio Channel, Client Signal-to-Noise-Ratio, latency, Connection Failures and Airtime Utilization are shown for APs that can hear the clients request.

Further down in the live capture we can see details of the authentication attempt, such as the AP that responded, which SSID the client attempted to connect to, on which radio it attempted to connect to and at what time. We then see the initial 802.11 Authentication request come from the client device to the Access Point.

The AP responds to the Client, and this particular WLAN is configured with WPA3 which requires a password to join. The Client responds to the AP with a password, which has been entered incorrectly.

The AP then rejects the authentication attempt as shown by the “Failed” flag. This demonstrates that the failure is completely between the client and AP at this point, there were no further authentication servers in play nor did a 4-way handshake or DHCP requests take place.



Troubleshooting – Client Connection (cont.)

Troubleshooting > Client Connection

Access Points hearing client's probe requests:

	Name	Radio	Client SNR(dB)	Latency(ms)	Connection Failure(%)	Airtime Utilization(%)
✓	TeamXXAP2 (C8:03:F5:09:2E:50)	5GHz (153)	47	0.0	0	0
	TeamXXAP1 (F8:E7:1E:12:74:90)	5GHz (157)	9	0.0	0	0

AP: TeamXXAP2 (C8:03:F5:09:2E:50) **SSID:** Team XX Guest WLAN **Radio:** 5GHz

Time:10:07:39

✓ 802.11 Authentication Request
✓ 802.11 Authentication Response
✓ 802.11 Association Request
✓ 802.11 Association Response
✓ DHCP Discover
✓ DHCP Offer
✓ DHCP Request
✓ DHCP Ack

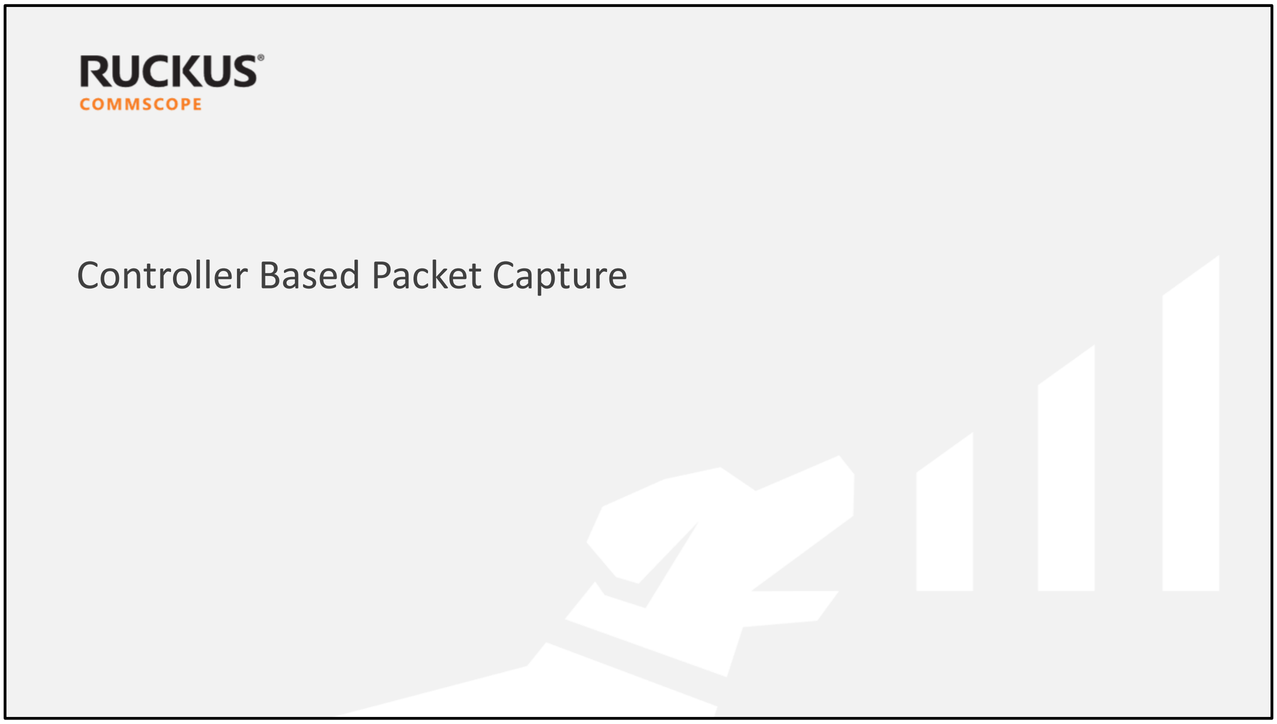
325 | © 2024 CommScope, Inc.

In this example we see that the APs are only hearing client probe requests on the 5GHz radio chain, and that the AP (shown highlighted with a check mark) with the best SNR to the client is the device that received the initial 802.11 request from the client.

We can also see the SSID that the client is connecting to. The flow diagram then depicts the step-by-step information exchange between the devices during the connection process. In this exchange we can see that we went through the 802.11 Authentication and Association phase, meaning we were able to successfully connect to the AP. The client then performed a DHCP Discovery broadcast, which was followed by a DHCP Offer, a DHCP Request, and finally a DHCP Ack. At this point the client has successfully connected and received an IP address.

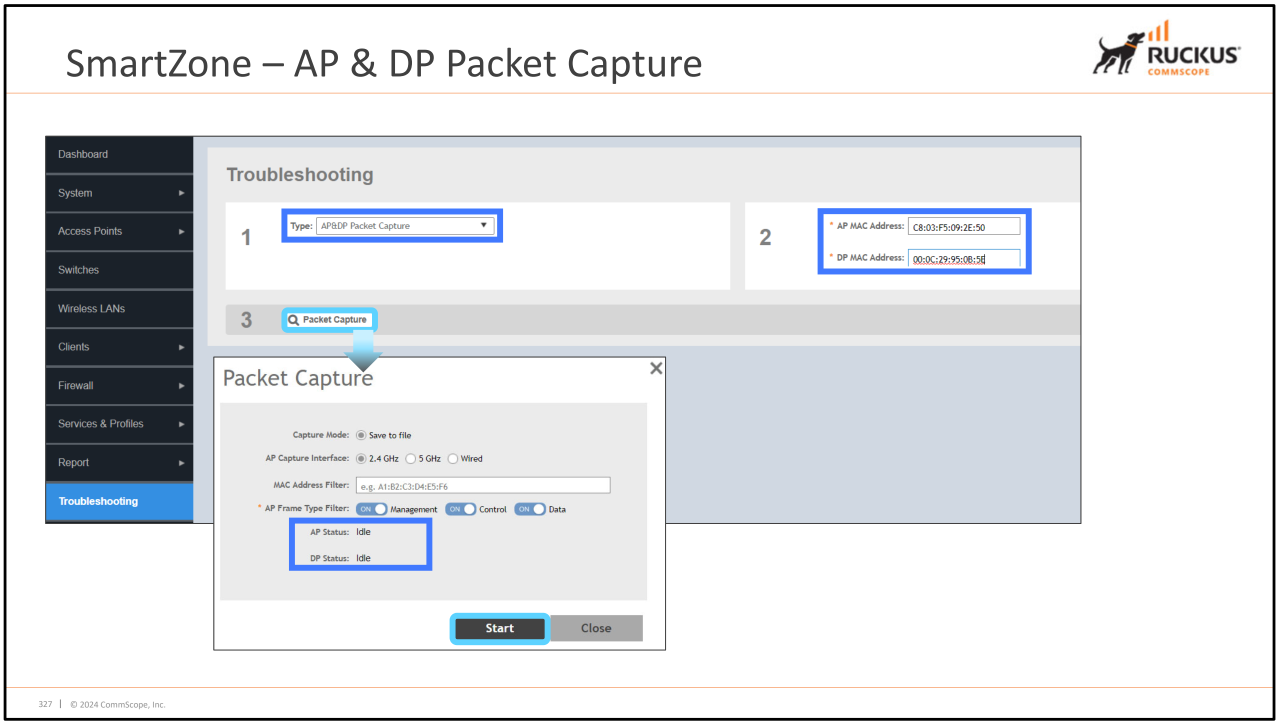
If there were alternate methods of authentication in use for this connection, such as Radius or Active Directory, we would have been able to see those specific requests in the flow and troubleshoot any issues that were displayed.

Additionally, Visual Connection Diagnostics (VCD) is a troubleshooting tool allows you to focus on a specific client device and its connection status. Its intuitive interface tracks the step-by-step progress of the client's connection through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, and roaming



RUCKUS
COMMSCOPE

Controller Based Packet Capture



SmartZone – AP & DP Packet Capture

Troubleshooting

1 Type: AP&DP Packet Capture

2 * AP MAC Address: C8:03:F5:09:2E:50
* DP MAC Address: 00:0C:29:95:0B:5E

3 Packet Capture

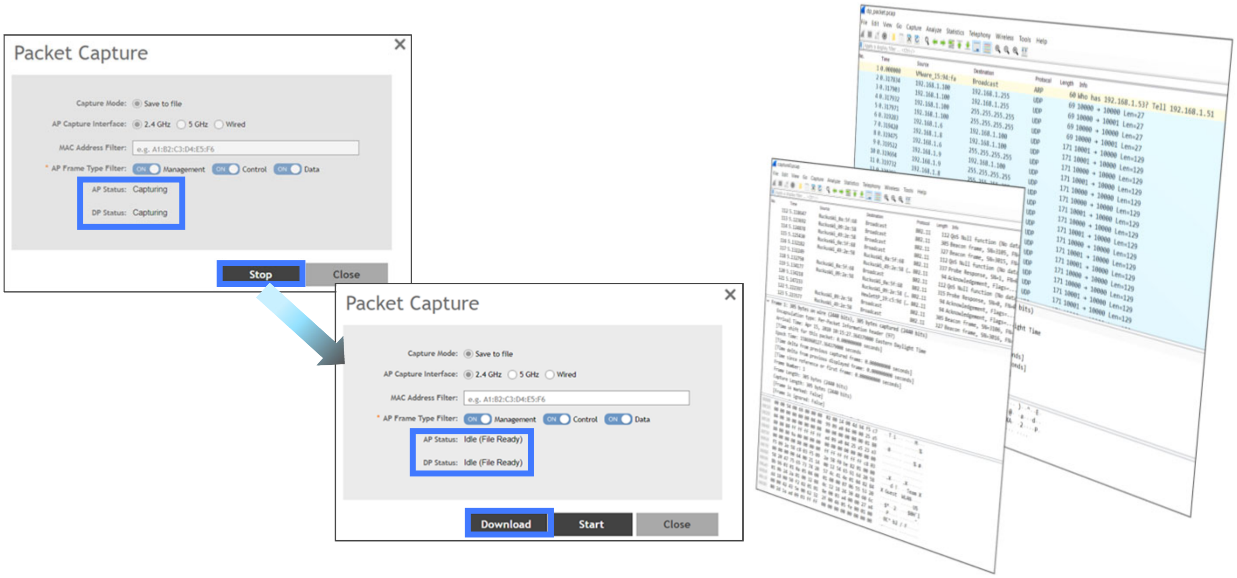
Packet Capture

Capture Mode: ● Save to file
AP Capture Interface: ● 2.4 GHz ○ 5 GHz ○ Wired
MAC Address Filter: e.g. A1:B2:C3:D4:E5:F6
* AP Frame Type Filter: ON Management ON Control ON Data
AP Status: Idle
DP Status: Idle

327 | © 2024 CommScope, Inc.

Access Point and Dataplane Packet captures allow engineers to gather PCAP files for both AP and Dataplane interfaces providing useful packet level inspection directly at the source. Administrators can specify the MAC Address for the access point and/or dataplane interfaces they are looking to capture traffic on and click **Packet Capture.** Specify which interface you want the AP capture to run on, by selecting either 2.4 GHz, 5 GHz, or Wired. Additionally, You can limit the AP capture by specifying a MAC Address to filter against, as well as optionally filtering traffic by Management, Control or Data traffic types.

SmartZone – AP & DP Packet Capture (cont.)



Packet Capture

Capture Mode: ● Save to file

AP Capture Interface: ● 2.4 GHz ○ 5 GHz ○ Wired

MAC Address Filter: e.g. A1:B2:C3:D4:E5:F6

* AP Frame Type Filter: ON Management ON Control ON Data

AP Status: Capturing

DP Status: Capturing

Packet Capture

Capture Mode: ● Save to file

AP Capture Interface: ● 2.4 GHz ○ 5 GHz ○ Wired

MAC Address Filter: e.g. A1:B2:C3:D4:E5:F6

* AP Frame Type Filter: ON Management ON Control ON Data

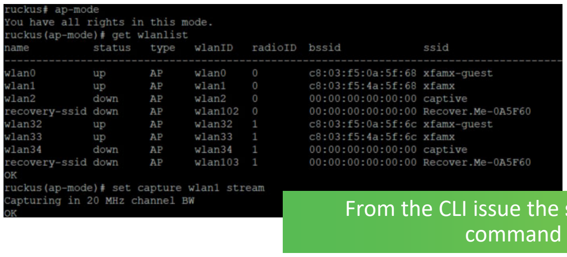
AP Status: Idle (File Ready)

DP Status: Idle (File Ready)

Once a capture is running the AP and/or DP status will change to “Capturing”. Note: Only one diagnostic packet capture operation can be run at a time, even if run from different user accounts. Anyone starting a new capture will stop the previous capture operation.

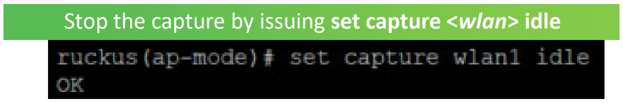
Once you are finished with the capture click **Stop**. The Status will return to Idle (File Ready). You can then download the zipped packet captures. Once downloaded and extracted the capture files can be opened and analyzed.

AP Packet Capture – CLI



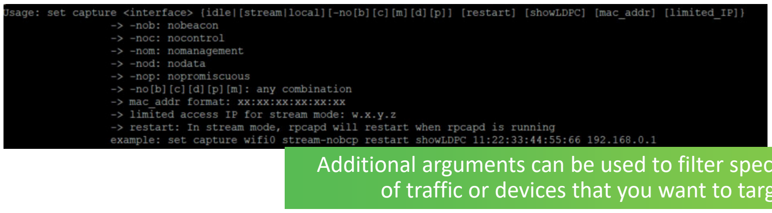
```
ruckus# ap-mode
You have all rights in this mode.
ruckus(ap-mode)# get wlanlist
name          status   type   wlanID   radioID  bssid             ssid
------------------------------------------------------------------------------------------
wlan0         up       AP     wlan0    0        c8:03:f5:0a:5f:68 xfamx-guest
wlan1         up       AP     wlan1    0        c8:03:f5:4a:5f:68 xfamx
wlan2         down     AP     wlan2    0        00:00:00:00:00:00 captive
recovery-ssid down     AP     wlan102  0        00:00:00:00:00:00 Recover.Me-0A5F60
wlan32        up       AP     wlan32   1        c8:03:f5:0a:5f:6c xfamx-guest
wlan33        up       AP     wlan33   1        c8:03:f5:4a:5f:6c xfamx
wlan34        down     AP     wlan34   1        00:00:00:00:00:00 captive
recovery-ssid down     AP     wlan103  1        00:00:00:00:00:00 Recover.Me-0A5F60
OK
ruckus(ap-mode)# set capture wlan1 stream
Capturing in 20 MHz channel BW
OK
```

Stop the capture by issuing **set capture <*wlan*> idle**



```
ruckus(ap-mode)# set capture wlan1 idle
OK
```

From the CLI issue the **set capture <*wlan*> stream** command from AP mode



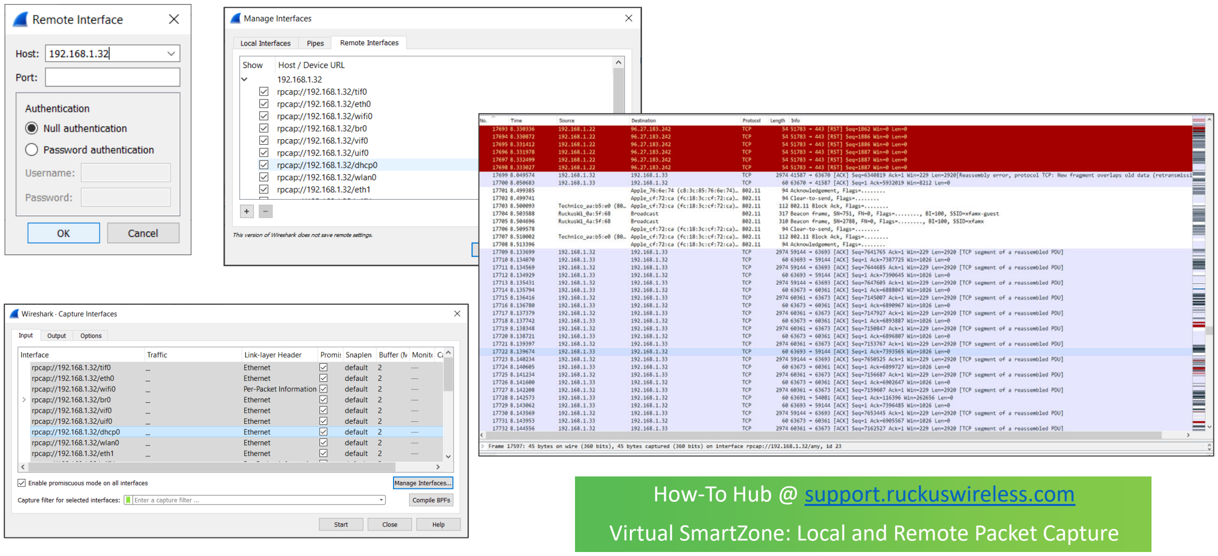
```
Usage: set capture <interface> {idle|[stream|local][-no[b][c][m][d][p]] [restart] [showLDPC] [mac_addr] [limited_IP]}
                -> -nob: nobeacon
                -> -noc: nocontrol
                -> -nom: nomanagement
                -> -nod: nodata
                -> -nop: nopromiscuous
                -> -no[b][c][d][p][m]: any combination
                -> mac_addr format: xx:xx:xx:xx:xx:xx
                -> limited access IP for stream mode: w.x.y.z
                -> restart: In stream mode, rpcapd will restart when rpcapd is running
                example: set capture wifi0 stream-nobcp restart showLDPC 11:22:33:44:55:66 192.168.0.1
```

Additional arguments can be used to filter specific types of traffic or devices that you want to target

329 | © 2024 CommScope, Inc.

Capturing packets from an AP CLI is also possible. Once connected to an APs CLI interface, enter ap-mode and use the command get wlanlist to show the networks for this specific AP. Use the set capture <wlan> stream command to begin streaming. Optionally additional arguments can be used to filter specific types of traffic or devices that you want to target. Once streaming is complete be sure to stop the stream with the set capture <wlan> idle command.

AP Packet Capture – CLI



Remote Interface

Host: 192.168.1.32

Port:

Authentication

● Null authentication

○ Password authentication

Username:

Password:

Manage Interfaces

Show	Host / Device URL
	192.168.1.32
☑	rpcap://192.168.1.32/tif0
☑	rpcap://192.168.1.32/eth0
☑	rpcap://192.168.1.32/wifi0
☑	rpcap://192.168.1.32/br0
☑	rpcap://192.168.1.32/vif0
☑	rpcap://192.168.1.32/uif0
☑	rpcap://192.168.1.32/dhcp0
☑	rpcap://192.168.1.32/wlan0
☑	rpcap://192.168.1.32/eth1

This version of Wireshark does not save remote settings.

```
No.   Time     Source               Destination                   Protocol Length Info
17693 8.330336 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1862 Win=0 Len=0
17694 8.330872 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1886 Win=0 Len=0
17695 8.331412 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1886 Win=0 Len=0
17696 8.331978 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1887 Win=0 Len=0
17697 8.332499 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1887 Win=0 Len=0
17698 8.333027 192.168.1.22         96.27.183.242                 TCP      54 51783 → 443 [RST] Seq=1887 Win=0 Len=0
17699 8.049574 192.168.1.32         192.168.1.33                  TCP    2974 41587 → 63670 [ACK] Seq=6340819 Ack=1 Win=229 Len=2920[Reassembly error, protocol TCP: New fragment overlaps old data (retransmissi
17700 8.050683 192.168.1.33         192.168.1.32                  TCP      60 63670 → 41587 [ACK] Seq=1 Ack=5932019 Win=8212 Len=0
17701 8.499385                      Apple_76:6e:74 (c8:3c:85:76:6e:74)… 802.11 94 Acknowledgement, Flags=........
17702 8.499741                      Apple_cf:72:ca (fc:18:3c:cf:72:ca)… 802.11 94 Clear-to-send, Flags=........
17703 8.500093 Technico_aa:b5:e0 (80… Apple_cf:72:ca (fc:18:3c:cf:72:ca)… 802.11 112 802.11 Block Ack, Flags=........
17704 8.503588 RuckusWi_0a:5f:68    Broadcast                     802.11  317 Beacon frame, SN=751, FN=0, Flags=........, BI=100, SSID=xfamx-guest
17705 8.504696 RuckusWi_4a:5f:68    Broadcast                     802.11  310 Beacon frame, SN=2788, FN=0, Flags=........, BI=100, SSID=xfamx
17706 8.509578                      Apple_cf:72:ca (fc:18:3c:cf:72:ca)… 802.11 94 Clear-to-send, Flags=........
17707 8.510002 Technico_aa:b5:e0 (80… Apple_cf:72:ca (fc:18:3c:cf:72:ca)… 802.11 112 802.11 Block Ack, Flags=........
17708 8.513396                      Apple_cf:72:ca (fc:18:3c:cf:72:ca)… 802.11 94 Acknowledgement, Flags=........
17709 8.133699 192.168.1.32         192.168.1.33                  TCP    2974 59144 → 63693 [ACK] Seq=7641765 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17710 8.134070 192.168.1.33         192.168.1.32                  TCP      60 63693 → 59144 [ACK] Seq=1 Ack=7387725 Win=1026 Len=0
17711 8.134569 192.168.1.32         192.168.1.33                  TCP    2974 59144 → 63693 [ACK] Seq=7644685 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17712 8.134929 192.168.1.33         192.168.1.32                  TCP      60 63693 → 59144 [ACK] Seq=1 Ack=7390645 Win=1026 Len=0
17713 8.135431 192.168.1.32         192.168.1.33                  TCP    2974 59144 → 63693 [ACK] Seq=7647605 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17714 8.135794 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6888047 Win=1026 Len=0
17715 8.136416 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7145007 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17716 8.136780 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6890967 Win=1026 Len=0
17717 8.137379 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7147927 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17718 8.137742 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6893887 Win=1026 Len=0
17719 8.138348 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7150847 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17720 8.138721 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6896807 Win=1026 Len=0
17721 8.139397 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7153767 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17722 8.139674 192.168.1.33         192.168.1.32                  TCP      60 63693 → 59144 [ACK] Seq=1 Ack=7393565 Win=1026 Len=0
17723 8.140234 192.168.1.32         192.168.1.33                  TCP    2974 59144 → 63693 [ACK] Seq=7650525 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17724 8.140605 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6899727 Win=1026 Len=0
17725 8.141234 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7156687 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17726 8.141600 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6902647 Win=1026 Len=0
17727 8.142208 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7159607 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17728 8.142573 192.168.1.33         192.168.1.32                  TCP      60 63691 → 54081 [ACK] Seq=1 Ack=116396 Win=262656 Len=0
17729 8.143062 192.168.1.33         192.168.1.32                  TCP      60 63693 → 59144 [ACK] Seq=1 Ack=7396485 Win=1026 Len=0
17730 8.143569 192.168.1.32         192.168.1.33                  TCP    2974 59144 → 63693 [ACK] Seq=7653445 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
17731 8.143953 192.168.1.33         192.168.1.32                  TCP      60 63673 → 60361 [ACK] Seq=1 Ack=6905567 Win=1026 Len=0
17732 8.144556 192.168.1.32         192.168.1.33                  TCP    2974 60361 → 63673 [ACK] Seq=7162527 Ack=1 Win=229 Len=2920 [TCP segment of a reassembled PDU]
> Frame 17597: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface rpcap://192.168.1.32/any, id 23
```

Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Promis	Snaplen	Buffer (M	Monit	Ca
rpcap://192.168.1.32/tif0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/eth0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/wifi0	_	Per-Packet Information	☑	default	2	—	
rpcap://192.168.1.32/br0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/vif0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/uif0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/dhcp0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/wlan0	_	Ethernet	☑	default	2	—	
rpcap://192.168.1.32/eth1	_	Ethernet	☑	default	2	—	

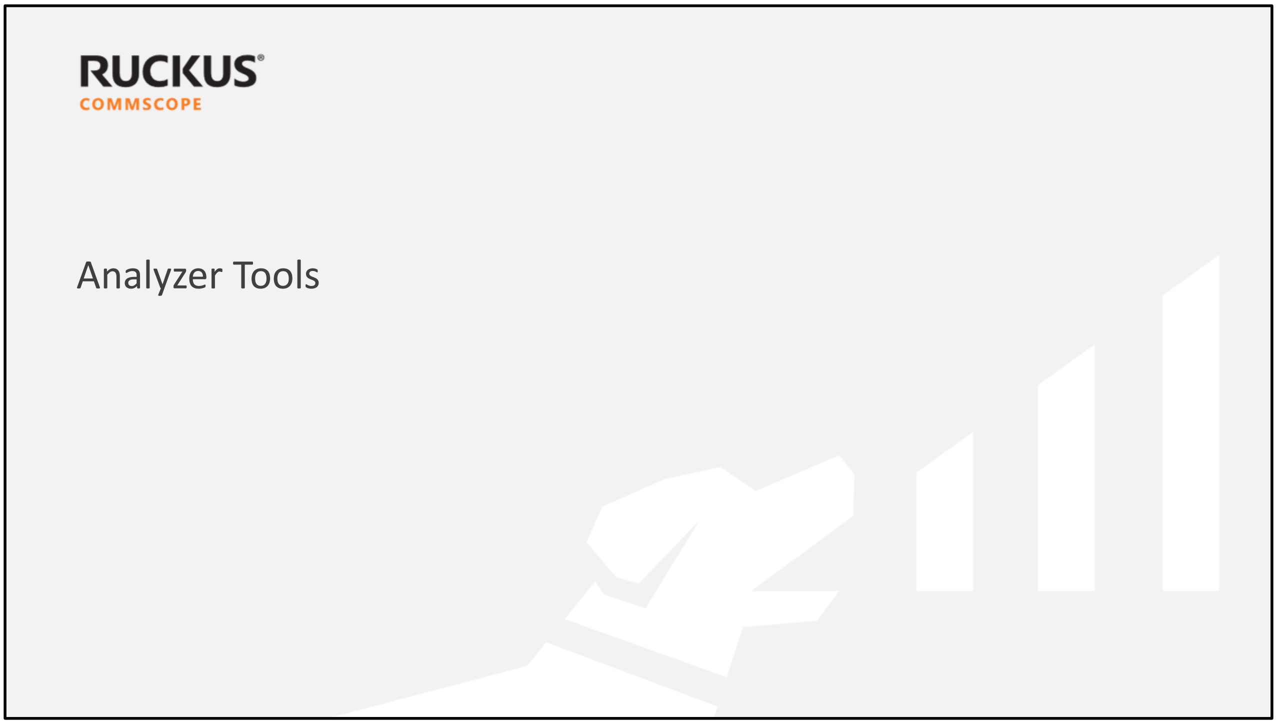
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

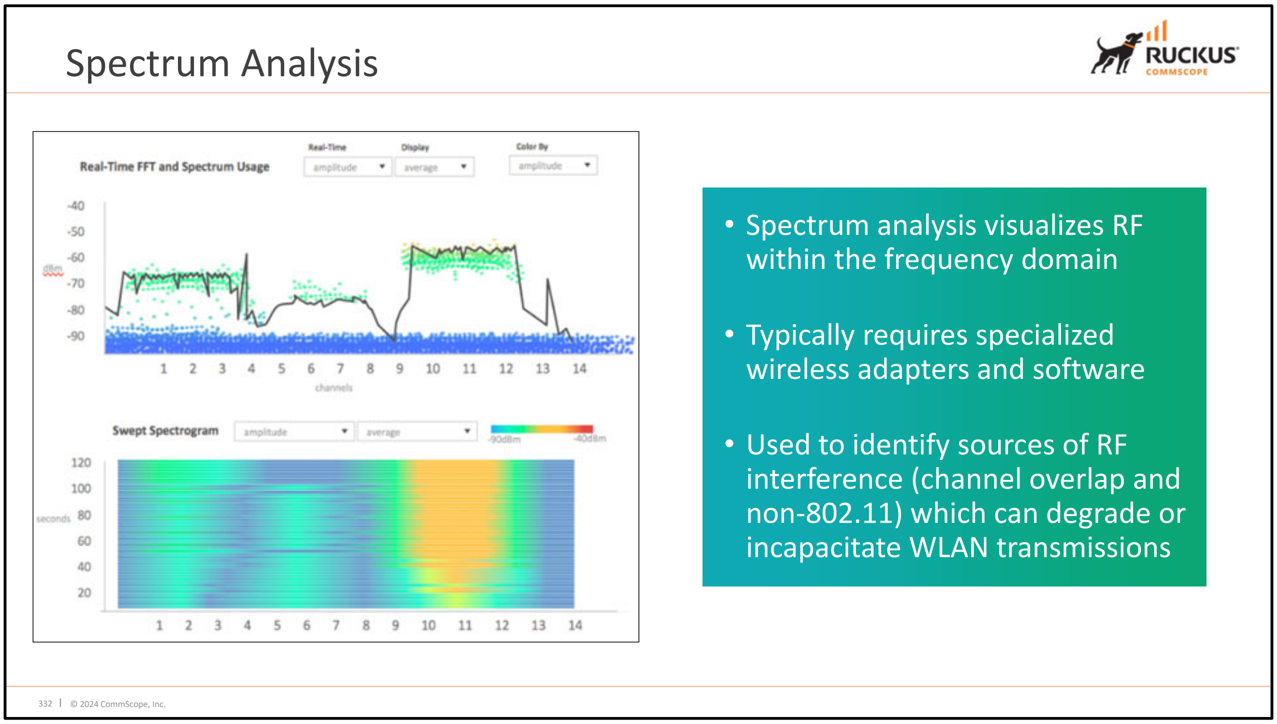
How-To Hub @ support.ruckuswireless.com

Virtual SmartZone: Local and Remote Packet Capture

Once the stream has been initiated from the AP we can add a remote capture interface with WireShark. In this case 192.168.1.32 is the IP of the AP that we started capture on. Once queried all available interfaces can be added as capture interfaces and capture can begin. To learn how to perform the steps of setting up remote capture interfaces visit the Ruckus How-To Hub at support.ruckuswireless.com and look for the video under the SmartZone section titled “Troubleshooting SmartZone: Local and Remote Packet Capture”.



Analyzer Tools



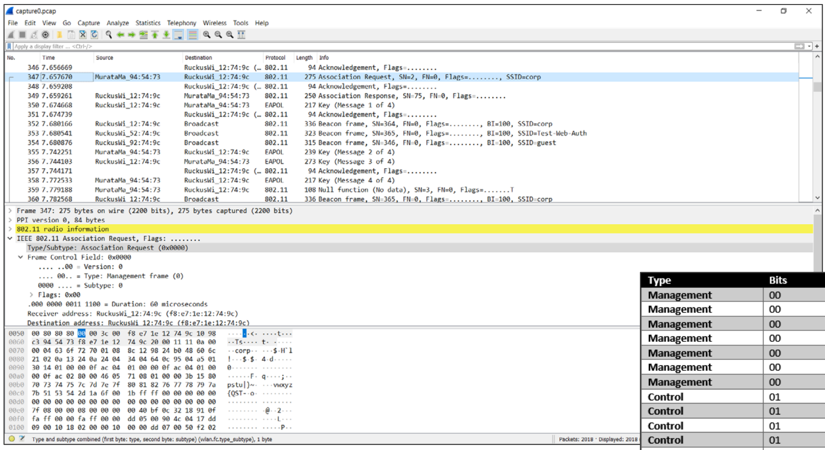
Spectrum Analysis

- Spectrum analysis visualizes RF within the frequency domain
- Typically requires specialized wireless adapters and software
- Used to identify sources of RF interference (channel overlap and non-802.11) which can degrade or incapacitate WLAN transmissions

Spectrum analyzers are used to visualize and measure RF within the frequency domain. We discussed frequency domains, time domains, and their relation to each other in the RUCKUS Wireless Fundamentals 100 course. A spectrum analyzer can help identify sources of non-802.11 transmissions that may be causing interference within layer 1 of your WLAN environment. Interference can come from devices on overlapping channels in 2.4 GHz and from non-Wi-Fi devices in any band where your devices are operating. It is interference because there is no contention just RF energy. Interference reduces the performance of the wireless network, by causing retransmissions due to the collision of wireless frames with the “noise” in the space. Therefore, it is important to monitor the spectrum usage in a particular area and efficiently allocate the spectrum as needed to wireless devices.

In order to perform spectrum analysis, you must have a wireless adapter capable of scanning the frequencies in your WLAN deployment as well as software to record and display the results. As we will discover, most RUCKUS APs include the ability to act as a spectrum analyzer. This RUCKUS feature is particularly helpful as it can be performed remotely without needing an engineer on-site.

Protocol Analyzers


capture0.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source              Destination            Protocol  Length Info
  346 7.656669                      RuckusWi_12:74:9c (… 802.11     94 Acknowledgement, Flags=........
  347 7.657670  MurataMa_94:54:73   RuckusWi_12:74:9c    802.11    275 Association Request, SN=2, FN=0, Flags=........, SSID=corp
  348 7.659208                      RuckusWi_12:74:9c (… 802.11     94 Acknowledgement, Flags=........
  349 7.659261  RuckusWi_12:74:9c   MurataMa_94:54:73    802.11    250 Association Response, SN=75, FN=0, Flags=........
  350 7.674668  RuckusWi_12:74:9c   MurataMa_94:54:73    EAPOL     217 Key (Message 1 of 4)
  351 7.674739                      RuckusWi_12:74:9c (… 802.11     94 Acknowledgement, Flags=........
  352 7.680166  RuckusWi_12:74:9c   Broadcast            802.11    336 Beacon frame, SN=364, FN=0, Flags=........, BI=100, SSID=corp
  353 7.680541  RuckusWi_52:74:9c   Broadcast            802.11    323 Beacon frame, SN=365, FN=0, Flags=........, BI=100, SSID=Test-Web-Auth
  354 7.680876  RuckusWi_92:74:9c   Broadcast            802.11    315 Beacon frame, SN=346, FN=0, Flags=........, BI=100, SSID=guest
  355 7.742251  MurataMa_94:54:73   RuckusWi_12:74:9c    EAPOL     239 Key (Message 2 of 4)
  356 7.744103  RuckusWi_12:74:9c   MurataMa_94:54:73    EAPOL     273 Key (Message 3 of 4)
  357 7.744171                      RuckusWi_12:74:9c (… 802.11     94 Acknowledgement, Flags=........
  358 7.772533  MurataMa_94:54:73   RuckusWi_12:74:9c    EAPOL     217 Key (Message 4 of 4)
  359 7.779188  MurataMa_94:54:73   RuckusWi_12:74:9c    802.11    108 Null function (No data), SN=3, FN=0, Flags=.......T
  360 7.782568  RuckusWi_12:74:9c   Broadcast            802.11    336 Beacon frame, SN=365, FN=0, Flags=........, BI=100, SSID=corp

> Frame 347: 275 bytes on wire (2200 bits), 275 bytes captured (2200 bits)
> PPI version 0, 84 bytes
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  v Frame Control Field: 0x0000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0000 .... = Subtype: 0
    > Flags: 0x00
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: RuckusWi_12:74:9c (f8:e7:1e:12:74:9c)
    Destination address: RuckusWi_12:74:9c (f8:e7:1e:12:74:9c)

0050  00 80 80 80 00 00 3c 00  f8 e7 1e 12 74 9c 10 98   ·····<· ····t···
0060  c3 94 54 73 f8 e7 1e 12  74 9c 20 00 11 11 0a 00   ··Ts···· t· ····
0070  00 04 63 6f 72 70 01 08  8c 12 98 24 b0 48 60 6c   ··corp·· ···$·H`l
0080  21 02 0a 13 24 0a 24 04  34 04 64 0c 95 04 a5 01   !···$·$· 4·d·····
0090  30 14 01 00 00 0f ac 04  01 00 00 0f ac 04 01 00   0······· ········
00a0  00 0f ac 02 80 00 46 05  71 08 01 00 00 3b 15 80   ······F· q····;··
00b0  70 73 74 75 7c 7d 7e 7f  80 81 82 76 77 78 79 7a   pstu|}~· ···vwxyz
00c0  7b 51 53 54 2d 1a 6f 00  1b ff ff 00 00 00 00 00   {QST-·o· ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  7f 08 00 00 08 00 00 00  00 40 bf 0c 32 18 91 0f   ········ ·@··2···
00f0  fa ff 00 00 fa ff 00 00  dd 05 00 90 4c 04 17 dd   ········ ····L···
0100  09 00 10 18 02 00 00 10  00 00 dd 07 00 50 f2 02   ········ ·····P··

Type and subtype combined (first byte: type, second byte: subtype) (wlan.fc.type_subtype), 1 byte    Packets: 2018 · Displayed: 2018
```

- Layer 2 analysis of 802.11 frame exchanges
- Client based captures depend on capability of wireless adapters
- RUCKUS APs allow for direct capture (initiated through SmartZone or AP CLI)

Type	Bits	Subtype	Bits
Management	00	Beacon	1000
Management	00	Association Request	0000
Management	00	Association Response	0001
Management	00	Authentication	1011
Management	00	Deauthentication	1100
Management	00	Action	1101
Management	00	Action No Ack	1110
Control	01	Control Wrapper	0111
Control	01	Block Ack Request (BlockAckReq)	1000
Control	01	Block Ack (BlockAck)	1001
Control	01	PS-Poll	1010
Control	01	RTS	1011
Control	01	CTS	1100
Control	01	Acknowledgement (ACK)	1101
Data	10	Standard Data Frame	0000
Data	10	Null Data Frame	0100
Data	10	QoS Data	1000
Data	10	QoS Null Data Frame	1110

https://www.semfionetworks.com/uploads/2/9/8/3/29831147/wireshark_802.11_filters_-_reference_sheet.pdf

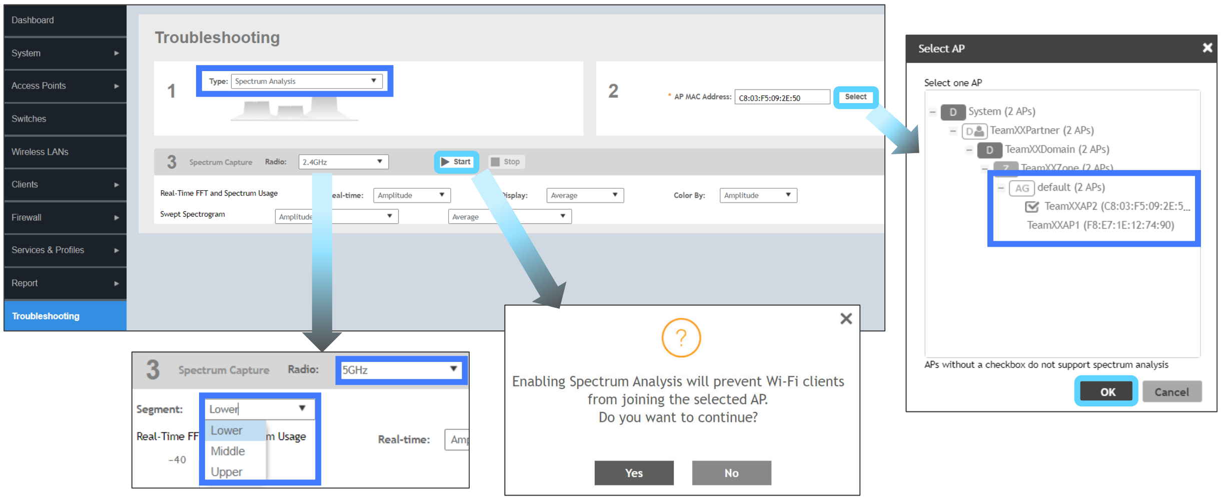
While spectrum analyzers provide a look into RF or layer 1 issues within a WLAN deployment. Protocol analyzers allow you to capture the packets being sent over the air and decode them for analysis. A common protocol analyzer popular among administrators is Wireshark, however there are other WLAN protocol analyzers available.

These tools are used to diagnose layer 2 issues in a WLAN by allowing you to look at the 802.11 frame exchanges between APs and clients. The three major frame types for 802.11 being Management, Control and Data. As shown in the screenshot Wireshark is displaying a capture with no filters applied, however filtering the capture to narrow down the results is most always a good idea. There are many filters that can be applied to narrow the capture display such as MAC address, BSSID, SSID, and 802.11 frame type. A link to the most common 802.11 filters for wireshark is shown here.

RUCKUS COMMSCOPE

RUCKUS Built-in Troubleshooting Tools

SmartZone – Spectrum Analysis



Type: Spectrum Analysis

* AP MAC Address: C8:03:F5:09:2E:50

Radio: 2.4GHz

Real-Time FFT and Spectrum Usage — Real-time: Amplitude — Display: Average — Color By: Amplitude

Swept Spectrogram — Amplitude — Average

Select one AP

- System (2 APs)
  - TeamXXPartner (2 APs)
    - TeamXXDomain (2 APs)
      - TeamXXZone (2 APs)
        - default (2 APs)
          - ☑ TeamXXAP2 (C8:03:F5:09:2E:5…
          - TeamXXAP1 (F8:E7:1E:12:74:90)

APs without a checkbox do not support spectrum analysis

Radio: 5GHz

Segment: Lower

Enabling Spectrum Analysis will prevent Wi-Fi clients from joining the selected AP. Do you want to continue?

336 | © 2024 CommScope, Inc.

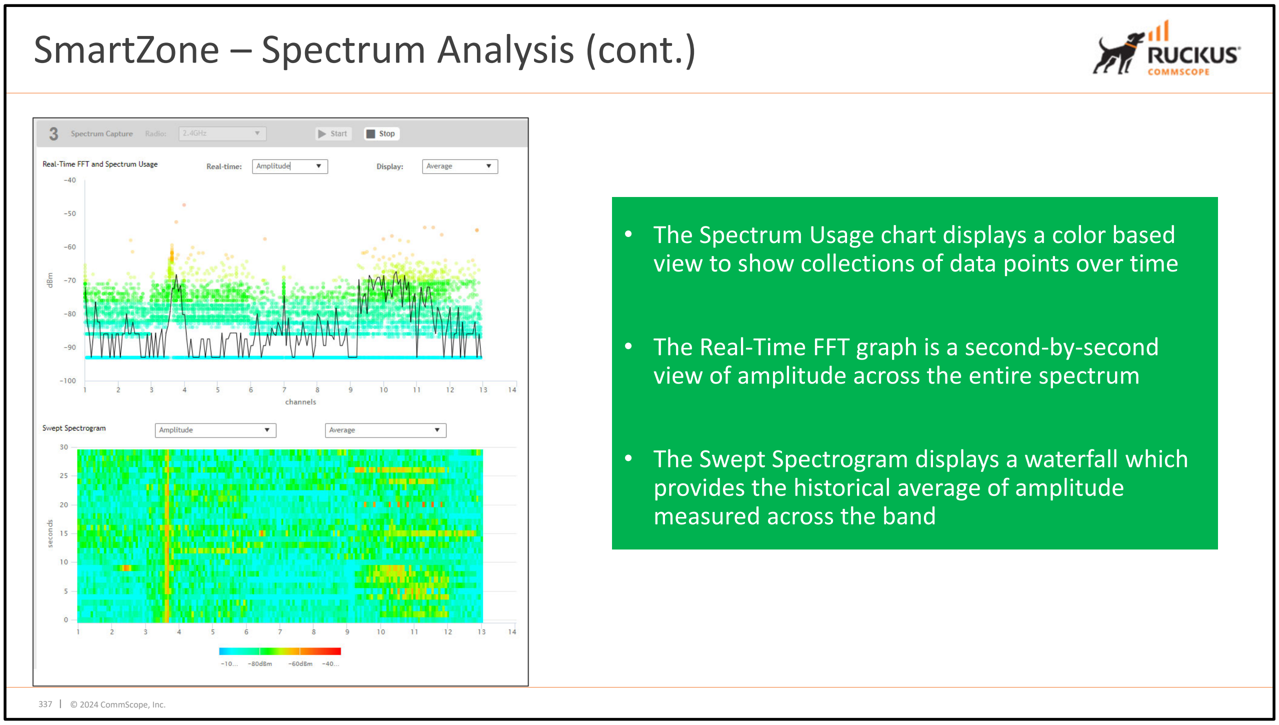
RUCKUS SmartZone WLAN controllers have several built-in tools to help with troubleshooting. SmartZone spectrum analysis allows administrators to place most Ruckus APs models into Spectrum-Mode which directs APs to transmit spectrum data back to the controller.

The steps to perform this process from SmartZone are simple. Once logged into SmartZone begin by navigating to **Troubleshooting** and selecting **Spectrum Analysis.**
Then **Select** the AP to place into Spectrum-Mode. APs that do not have a checkbox, do not support being placed into Spectrum-Mode. Once the selection is made choose **OK**.

Next select the **Radio** whose band you want to analyze, the default is 2.4GHz. If 5GHz is selected you must also select the segment of the 5GHz spectrum that you wish to analyze which is broken into three groups:
Lower – for channels 36 to 64
Middle – for channels 100 to 144
Upper – for channels 149 to 165

The Real-Time FFT and Swept Spectrogram options change the way the charts are displayed and can be adjusted in real-time while the capture is running.
Once the selections have been made and you are ready to begin the capture press **Start** and accept the message which states that clients will be unable to join this AP while spectrum analysis is running.

SmartZone – Spectrum Analysis (cont.)



Radio: 2.4GHz

Real-time: Amplitude

Display: Average

Amplitude

Average

- The Spectrum Usage chart displays a color based view to show collections of data points over time
- The Real-Time FFT graph is a second-by-second view of amplitude across the entire spectrum
- The Swept Spectrogram displays a waterfall which provides the historical average of amplitude measured across the band

337 |

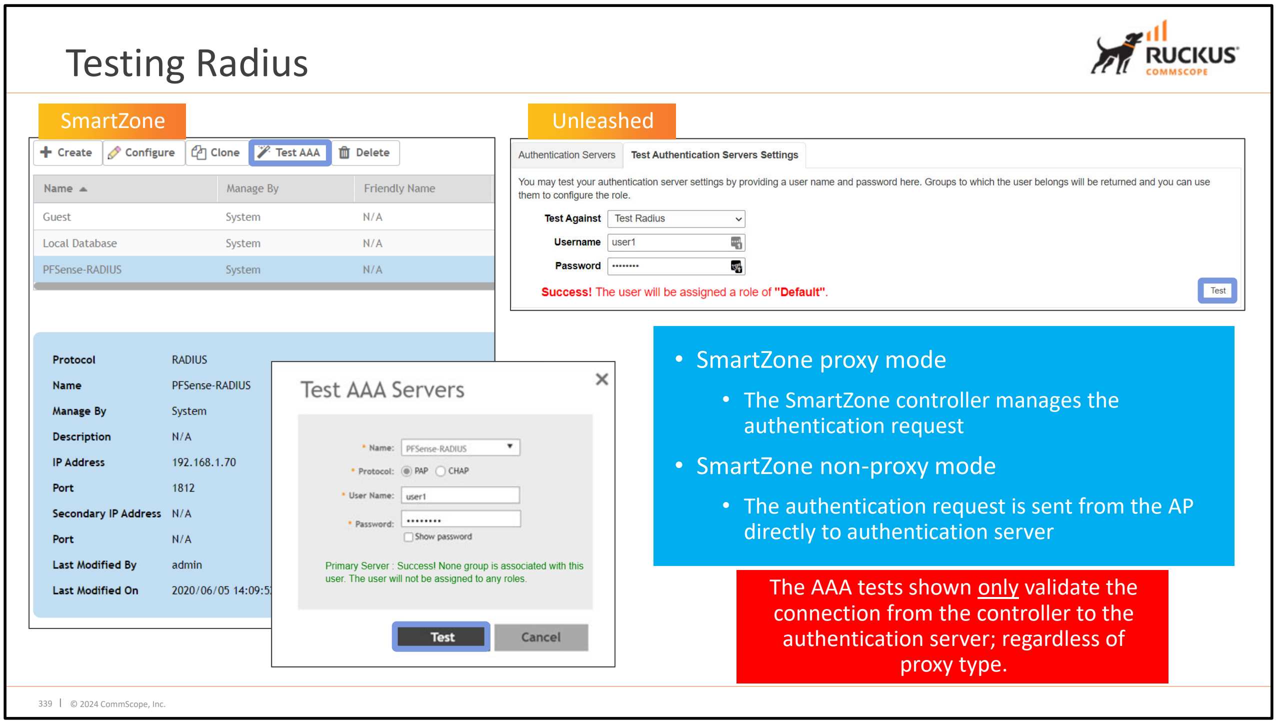
As Spectrum Analysis runs the charts will begin to populate with data. The Spectrum Usage chart displays a color based view to show collections of data points over time. As more samples are collected at the specific frequency and amplitude the colors of the points change. In this amplitude based view warm (yellow/red) colors depict higher amplitude, while cooler colors (green/blue) depict lower amplitude.

From this specific graph we can see that the AP is most strongly detecting 2.4 GHz signals at a point between channel 3 and channel 4 as well as across channels 10, 11 and 12.

The black line shown in the Real-Time Fast Fourier Transform (FFT) graph is a second-by-second update of measured data across the entire band. Within this view the average energy measured is displayed for the current sample period.

The Swept Spectrogram displays a waterfall of color over time, where each horizontal line represents one sample period. The waterfall displays a running historical average of amplitude measured across the band.

In the example shown we can tell a few things about the RF environment from the view of this AP. This AP is detecting a device very strongly in between channels 3 and 4. While this is due to a wireless mouse that is very close to the AP in this lab environment, if we saw this in a deployment, we would want to make sure that we are either staying away from that channel (most channel plans for 2.4 GHz use 1, 6, and 11 anyway) or correct the source of the interference.



Testing Radius

SmartZone

Name	Manage By	Friendly Name
Guest	System	N/A
Local Database	System	N/A
PFSense-RADIUS	System	N/A

Protocol	RADIUS
Name	PFSense-RADIUS
Manage By	System
Description	N/A
IP Address	192.168.1.70
Port	1812
Secondary IP Address	N/A
Port	N/A
Last Modified By	admin
Last Modified On	2020/06/05 14:09:5

Test AAA Servers

* Name: PFSense-RADIUS

* Protocol: ● PAP ○ CHAP

* User Name: user1

* Password: ••••••••

□ Show password

Primary Server : Success! None group is associated with this user. The user will not be assigned to any roles.

Unleashed

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against: Test Radius

Username: user1

Password: ••••••••

Success! The user will be assigned a role of "Default".

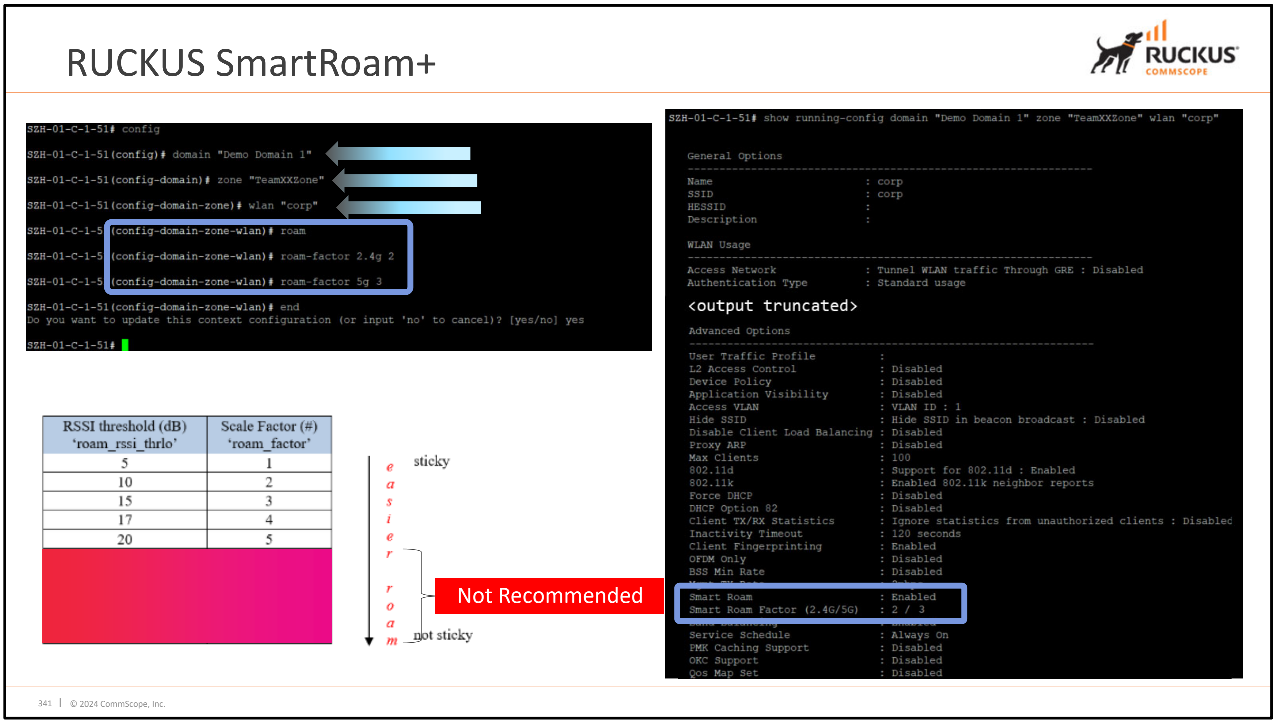
- SmartZone proxy mode
  - The SmartZone controller manages the authentication request
- SmartZone non-proxy mode
  - The authentication request is sent from the AP directly to authentication server

The AAA tests shown only validate the connection from the controller to the authentication server; regardless of proxy type.

339 | © 2024 CommScope, Inc.

RUCKUS SmartZone and Unleashed provide tools to help validate the connectivity to authentication servers. This will help ensure the target authentication server is online, the ports are open, the shared secret is valid, and that the authentication servers connection to the user database is functioning. Specify a username and password that you wish to use for the test and press “test”. If everything is functioning correctly you should be met with a success message.

You should be aware that SmartZone allows you to configure authentication servers in proxy or non-proxy mode. If using proxy mode, the setup on the authentication server will include setting the controller as a NAS (client) whereas using non-proxy mode, each individual AP would need to be configured as a NAS (client). It is important to understand that the authentication tests shown here only validate the connection from the controller to the authentication server. A successful test here does not mean that a non-proxy authentication attempt will be successful.



RUCKUS SmartRoam+

```
SZH-01-C-1-51# config

SZH-01-C-1-51(config)# domain "Demo Domain 1"

SZH-01-C-1-51(config-domain)# zone "TeamXXZone"

SZH-01-C-1-51(config-domain-zone)# wlan "corp"

SZH-01-C-1-5 (config-domain-zone-wlan)# roam

SZH-01-C-1-5 (config-domain-zone-wlan)# roam-factor 2.4g 2

SZH-01-C-1-5 (config-domain-zone-wlan)# roam-factor 5g 3

SZH-01-C-1-51(config-domain-zone-wlan)# end
Do you want to update this context configuration (or input 'no' to cancel)? [yes/no] yes

SZH-01-C-1-51#
```

```
SZH-01-C-1-51# show running-config domain "Demo Domain 1" zone "TeamXXZone" wlan "corp"


  General Options
  ----------------------------------------------------------------
  Name                        : corp
  SSID                        : corp
  HESSID                      :
  Description                 :

  WLAN Usage
  ----------------------------------------------------------------
  Access Network              : Tunnel WLAN traffic Through GRE : Disabled
  Authentication Type         : Standard usage
  <output truncated>
  Advanced Options
  ----------------------------------------------------------------
  User Traffic Profile           :
  L2 Access Control              : Disabled
  Device Policy                  : Disabled
  Application Visibility         : Disabled
  Access VLAN                    : VLAN ID : 1
  Hide SSID                      : Hide SSID in beacon broadcast : Disabled
  Disable Client Load Balancing  : Disabled
  Proxy ARP                      : Disabled
  Max Clients                    : 100
  802.11d                        : Support for 802.11d : Enabled
  802.11k                        : Enabled 802.11k neighbor reports
  Force DHCP                     : Disabled
  DHCP Option 82                 : Disabled
  Client TX/RX Statistics        : Ignore statistics from unauthorized clients : Disabled
  Inactivity Timeout             : 120 seconds
  Client Fingerprinting          : Enabled
  OFDM Only                      : Disabled
  BSS Min Rate                   : Disabled
  Smart Roam                     : Enabled
  Smart Roam Factor (2.4G/5G)    : 2 / 3
  Service Schedule               : Always On
  PMK Caching Support            : Disabled
  OKC Support                    : Disabled
  Qos Map Set                    : Disabled
```

RSSI threshold (dB) 'roam_rssi_thrlo'	Scale Factor (#) 'roam_factor'
5	1
10	2
15	3
17	4
20	5

While defining bss min rates can help clients roam seamlessly to APs offering better speeds, RUCKUS SmartRoam+ can be used to remove a stuck client from an AP by sending a disassociation frame to the client if its signal falls below the defined roam factor for the WLAN .

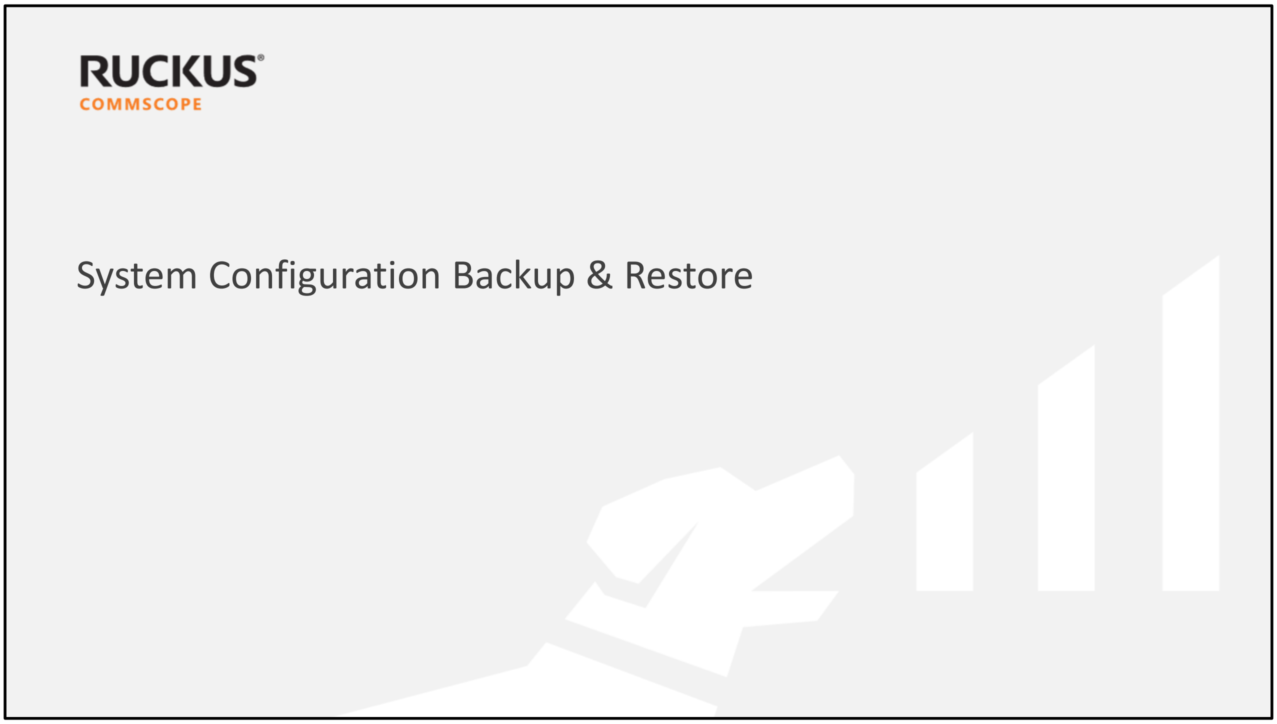
SmartRoam can only be enabled only through CLI commands and in this example we are showing the configuration from a SmartZone highscale perspective.

Once you have specified the domain, zone and wlan enable SmartRoam with the **roam** command and specific the **roam-factor** per radio. This roam factor sets the threshold in which the AP will consider using SmartRoam to disconnect a client. At a roam factor of one if the clients SNR falls below 5dB the AP will send a deauth frame to the client. The lower the roam factor the stickier the client.

It is recommended to use conservative roam factors to as you begin to implement SmartRoam, the use of values over 5 are not recommended.
You can validate the configuration and check the status of SmartRoam by issuing the show running-config command specifying any applicable domain, zone and wlan

RUCKUS
COMMSCOPE

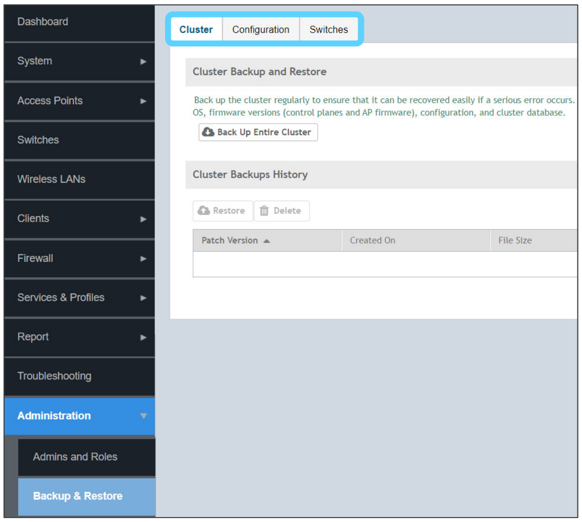
RUCKUS Wi-Fi solution management



System Configuration Backup & Restore

Creating a Configuration Backup

Administration > Backup & Restore



Back up the cluster regularly to ensure that it can be recovered easily if a serious error occurs. OS, firmware versions (control planes and AP firmware), configuration, and cluster database.

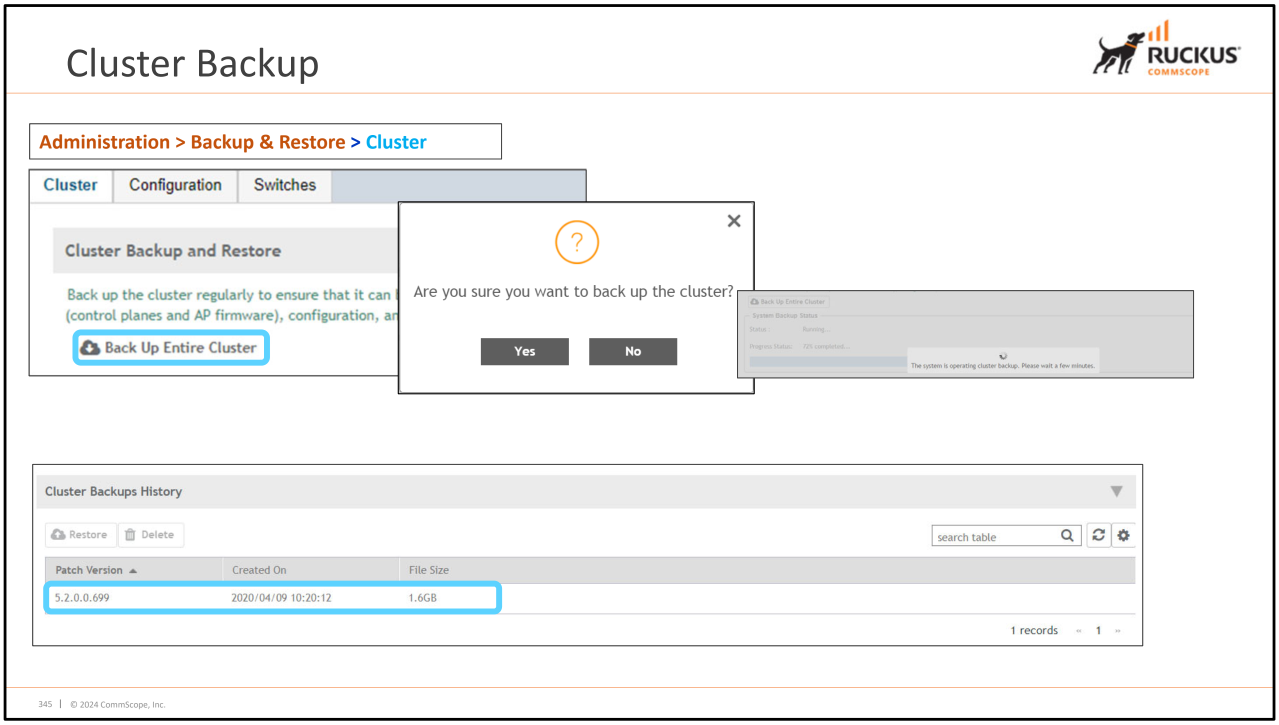
Backup and restore options

- Entire cluster
- Configuration (individual system)
- Switches

344 | © 2024 CommScope, Inc.

The Backup and Restore settings are found under **Administration > Backup & Restore**.

Here you’ll see three tabs – **Cluster, Configuration** and **Switches**. Let’s look at each in turn.



Cluster Backup

Administration > Backup & Restore > Cluster

Cluster Backup and Restore

Back up the cluster regularly to ensure that it can
(control planes and AP firmware), configuration, ar

Are you sure you want to back up the cluster?

System Backup Status

Status : Running...

Progress Status: 72% completed...

The system is operating cluster backup. Please wait a few minutes.

Cluster Backups History

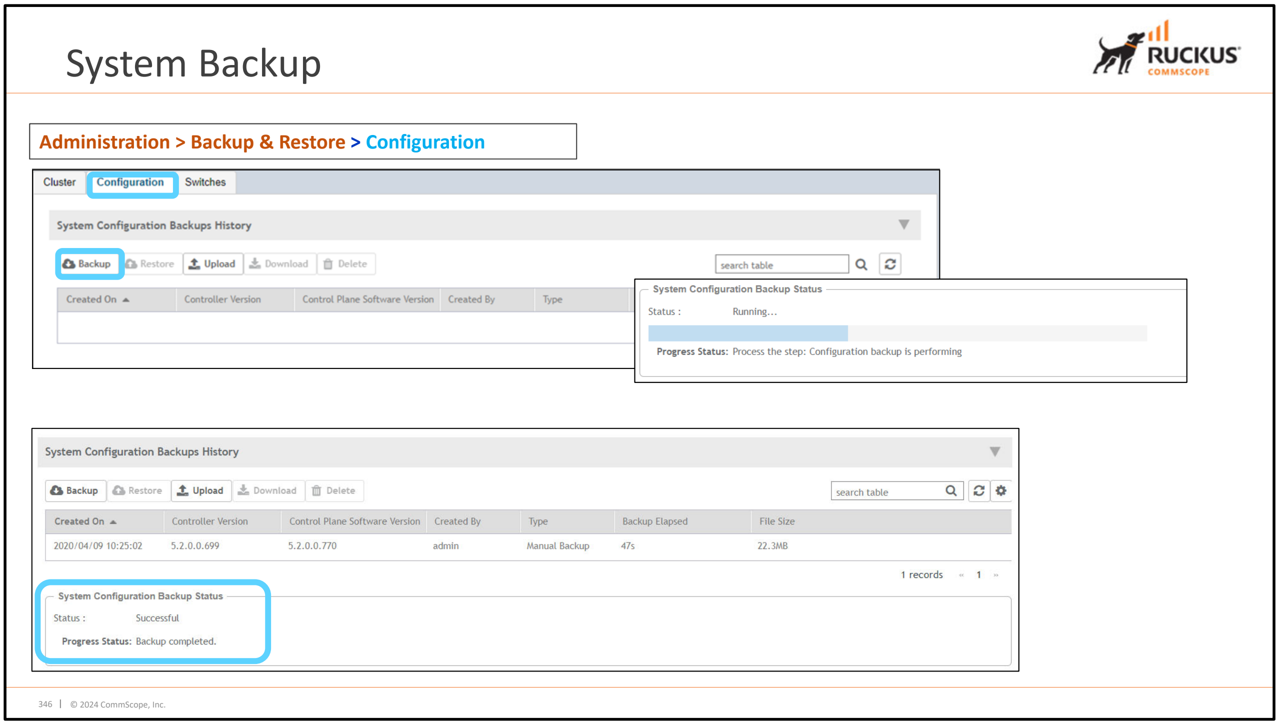
Patch Version	Created On	File Size
5.2.0.0.699	2020/04/09 10:20:12	1.6GB

1 records « 1 »

From the **Cluster** menu, select **Back Up Entire Cluster** to perform a system backup of the cluster settings.

You'll see a standard warning, and then the status of the backup as it runs. Once completed, you will see the backup in the history window.

Be aware that the the cluster will go into maintenance mode during the backup process.



System Backup

Administration > Backup & Restore > Configuration

Created On ▲	Controller Version	Control Plane Software Version	Created By	Type

System Configuration Backup Status

Status : Running...

Progress Status: Process the step: Configuration backup is performing

Created On ▲	Controller Version	Control Plane Software Version	Created By	Type	Backup Elapsed	File Size
2020/04/09 10:25:02	5.2.0.0.699	5.2.0.0.770	admin	Manual Backup	47s	22.3MB

1 records « 1 »

System Configuration Backup Status

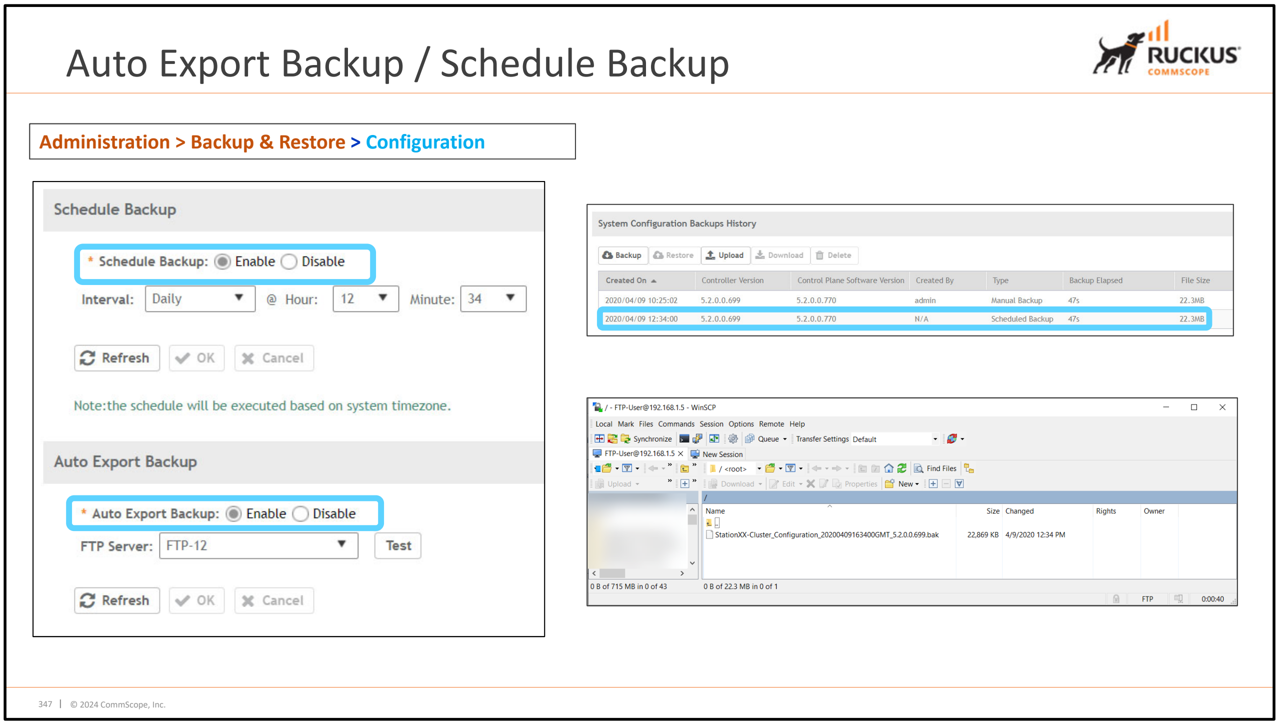
Status : Successful

Progress Status: Backup completed.

346 | © 2024 CommScope, Inc.

To backup the system configuration, use the **Configuration** tab. Click **Backup**, and the status of the backup will display.

When the backup is finished, you'll see an entry in the history log. You'll also see the status will be displayed as *Successful* and *Backup completed*.



Auto Export Backup / Schedule Backup

Administration > Backup & Restore > Configuration

Schedule Backup

* Schedule Backup: ● Enable ○ Disable

Interval: Daily @ Hour: 12 Minute: 34

Note:the schedule will be executed based on system timezone.

Auto Export Backup

* Auto Export Backup: ● Enable ○ Disable

FTP Server: FTP-12

System Configuration Backups History

Created On	Controller Version	Control Plane Software Version	Created By	Type	Backup Elapsed	File Size
2020/04/09 10:25:02	5.2.0.0.699	5.2.0.0.770	admin	Manual Backup	47s	22.3MB
2020/04/09 12:34:00	5.2.0.0.699	5.2.0.0.770	N/A	Scheduled Backup	47s	22.3MB

/ - FTP-User@192.168.1.5 - WinSCP

/

Name	Size	Changed	Rights	Owner
..				
StationXX-Cluster_Configuration_20200409163400GMT_5.2.0.0.699.bak	22,869 KB	4/9/2020 12:34 PM		

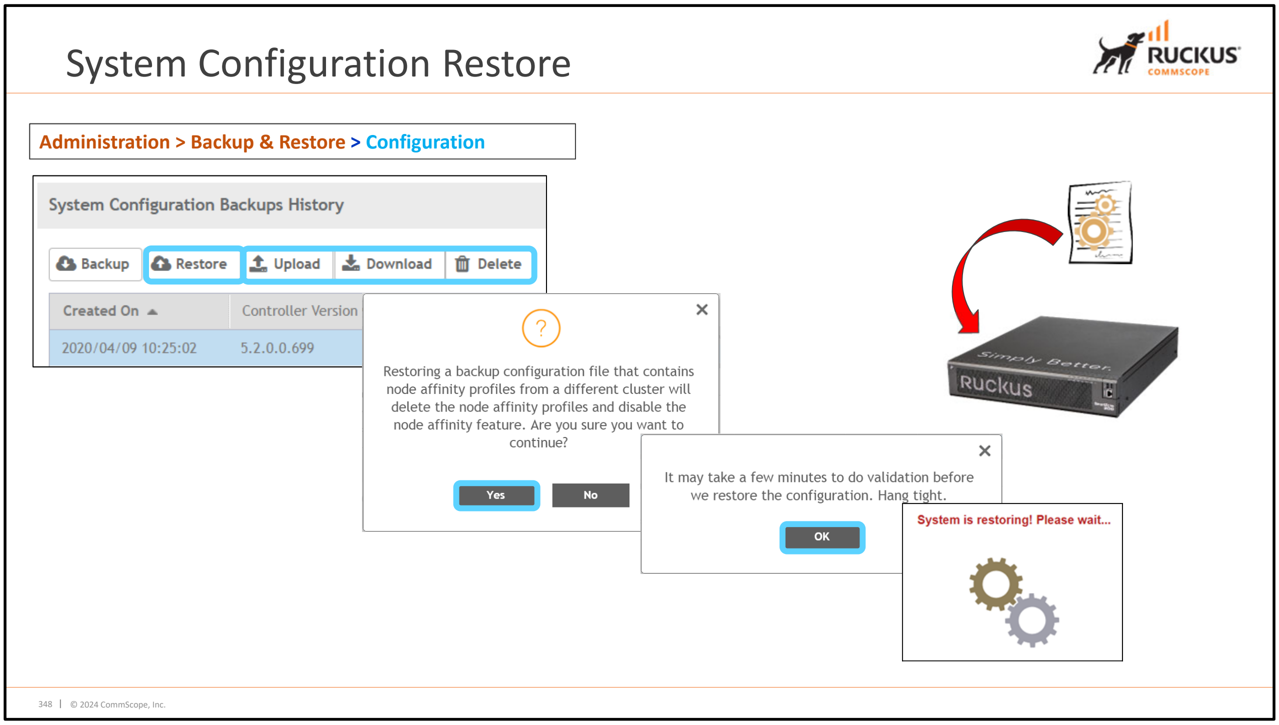
0 B of 715 MB in 0 of 43

0 B of 22.3 MB in 0 of 1

FTP 0:00:40

347 | © 2024 CommScope, Inc.

You can enable the ability to schedule configuration backups to run at a specific times according to a daily, weekly or monthly intervals. Additionally, you can choose to have these backups auto export to an FTP server by selecting an existing FTP server from the drop down list. FTP servers are created under the **SYSTEM** section of SmartZone. These will show up as “Scheduled Backup” in the history and appear as .bak files on the FTP server.



System Configuration Restore

Administration > Backup & Restore > Configuration

System Configuration Backups History

Created On ▲	Controller Version
2020/04/09 10:25:02	5.2.0.0.699

Restoring a backup configuration file that contains node affinity profiles from a different cluster will delete the node affinity profiles and disable the node affinity feature. Are you sure you want to continue?

It may take a few minutes to do validation before we restore the configuration. Hang tight.

System is restoring! Please wait...

Once backups have been made, you will see them listed under **System Configuration Backups**. From here, you can select to upload, or download or delete a backup file, or to perform a restore.

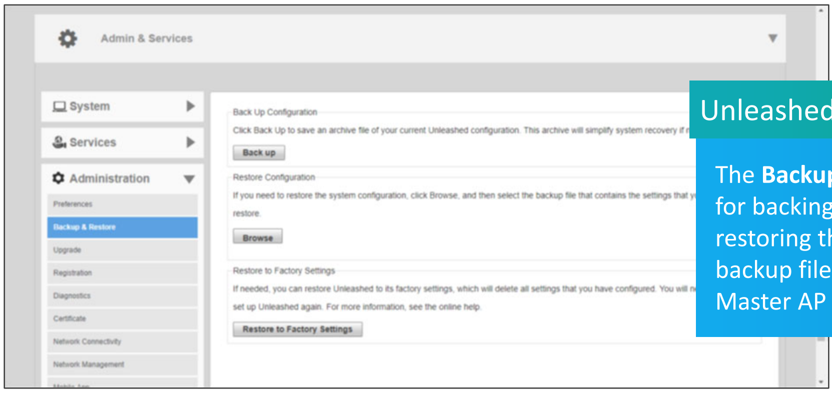
If you choose to restore the system config, you will see the standard warning. Selecting to continue shows the progress of the restore.

The cluster restore process may take several minutes to complete. When the restore process is underway, the controller logs you off the web interface automatically, and you won't be able to log back in until the restore is complete.

If you log in and the web interface displays the message "**Cluster is out of service. Please try again in a few minutes**", wait for three minutes and the Dashboard will appear shortly. The message appears because the controller is still initializing its processes.

For instance, existing configuration backups can be used to build a new vSZ platform in the case of a failed vSZ system, or to replicate a production vSZ cluster in a lab environment.

Unleashed Configuration Backup & Restore



Back Up Configuration

Click Back Up to save an archive file of your current Unleashed configuration. This archive will simplify system recovery if r

Restore Configuration

If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that y

restore.

Restore to Factory Settings

If needed, you can restore Unleashed to its factory settings, which will delete all settings that you have configured. You will n

set up Unleashed again. For more information, see the online help.

Unleashed Backup & Restore

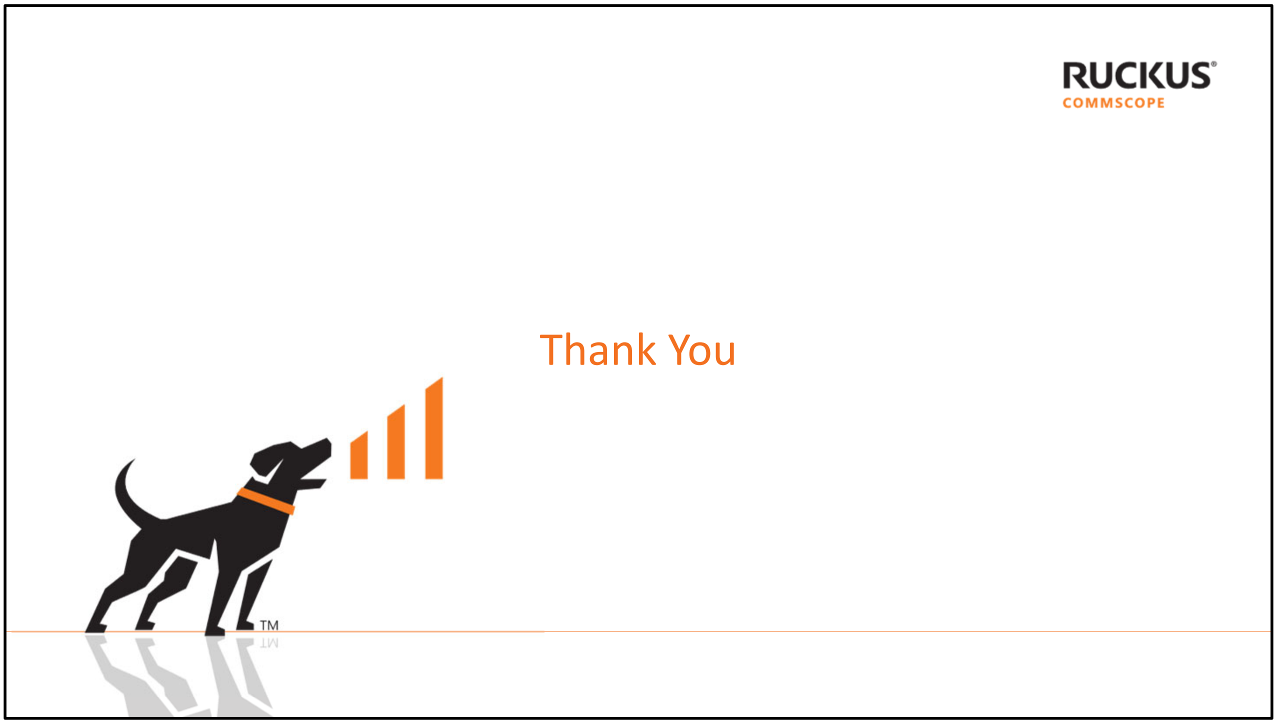
The **Backup & Restore** page provides options for backing up your current configuration, restoring the configuration from a previous backup file, or restoring the Unleashed Master AP to factory settings.

The backup is a small encrypted file with a .bak extension saved to the filename and location of your choosing.

To restore settings from a backup file, click **Browse**, then select your backup file, and click **Open**. Once the .bak file has been uploaded to Unleashed, select one of three restore options for your Unleashed network.

Options include:

- Restore Everything
- Restore Everything except system name and IP address
- Restore only WLAN settings, ACLs, roles, users, country code and system time



Thank You