Solution Overview

RUCKUS WAN Gateway - Microsegmentation Overview

March 2023

Table of Contents

Overview

This document will explain why microsegmentation is an important feature for many different verticals, and how RWG uses microsegmentation to assign clients to dedicated VLANs and subnets. RWG supports microsegmentation is several ways: per device, per room and per account.

FIGURE 1 – PER ROOM MICROSEGMENTATION

RWG includes a RADIUS server, and it acts as a NAC (Network Admission Control) to assign VLANs dynamically to wired or wireless clients. The solution uses WLANs configured with 802.1x Mac Bypass to send the client's authentication request to the RWG's RADIUS server. The RADIUS response includes the VLAN Tag Assignment (VTA) in the Access-Accept response.

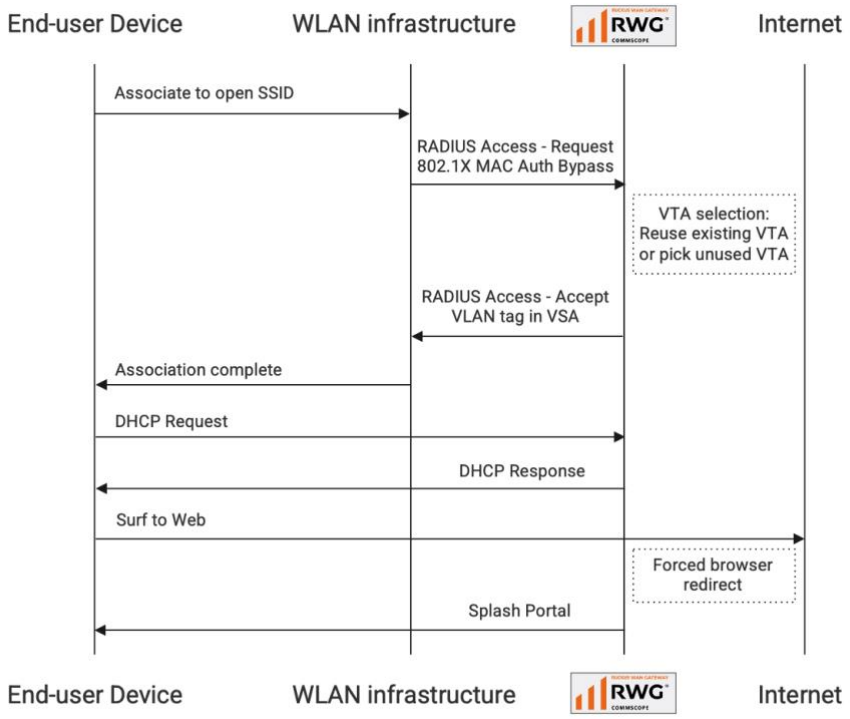


FIGURE 2 – 802.1X DYNAMIC VLANS FLOW

Why Microsegmentation

This diagram shows a perfectly reasonable architecture for your home – using a single IP subnet:

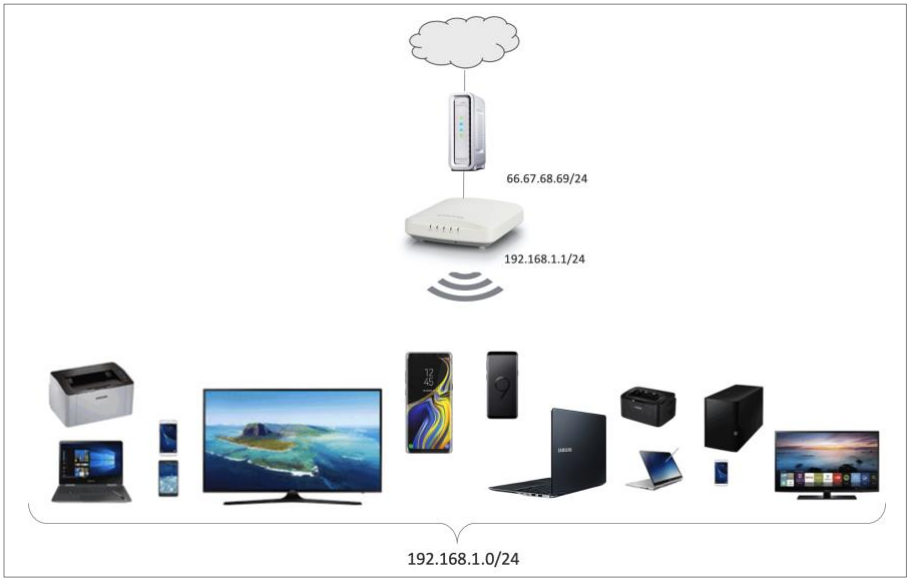


FIGURE 3 – HOME NETWORK USING A SINGLE IP SUBNET

This is good for your home network, but not for a shared network in your office, hotel or MDU/MTU. In the next diagram we have two IP subnets:

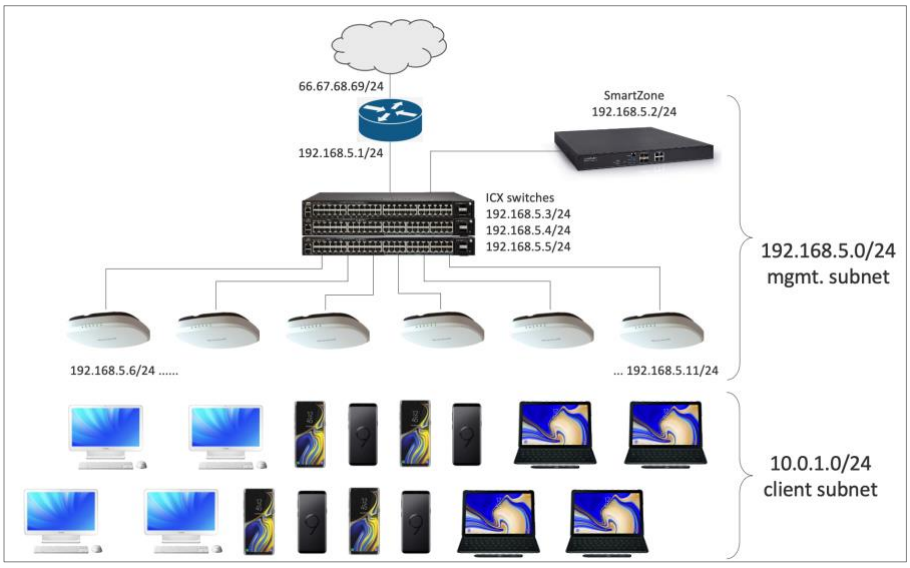


FIGURE 4 – ENTERPRISE NETWORK USING TWO SUBNETS

The infrastructure devices use one IP subnet for management, the users have their own IP subnet, and the IT personnel have access to both networks. This provides isolation between the client traffic and management traffic, but there is still no microsegmentation.

When RWG is used, the two networks are created in the LAN interface (igb3 in this example), along with two separate DHCP scopes:

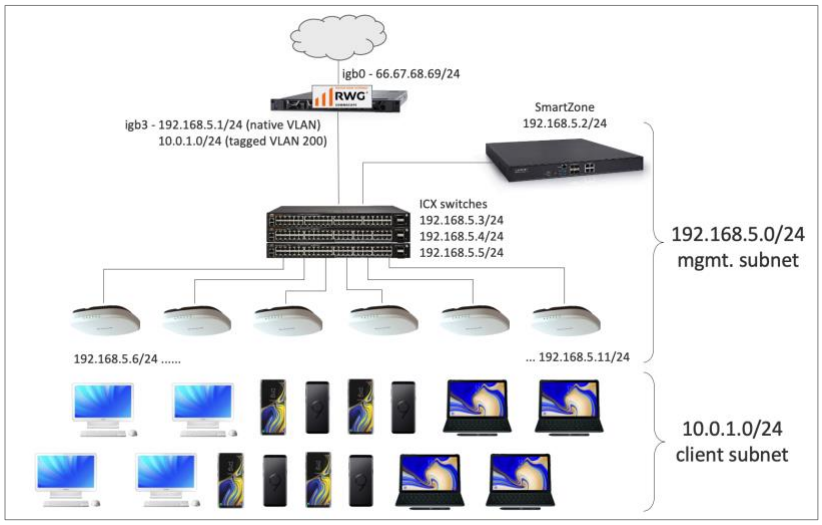
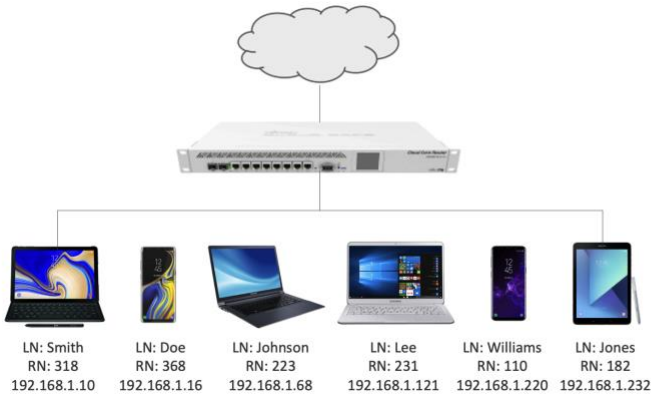


FIGURE 5 – RWG USING TWO LAN NETWORKS

Subnet 192.168.5.1/24 uses the native VLAN for management. The infrastructure devices acquire IP addresses from a DHCP scope in that subnet. The client subnet uses tagged VLAN 200 to provide addresses using the 10.0.1.0/24 DHCP scope.

Typical Hotel Network Using a Single Guest Segment

A typical hotel network often uses a single guest network, like the architecture used in an enterprise network. This is a terrible idea, but it's almost universal. The end-user population in a hotel is different - there is no control over the devices, and there is a high risk of bad actors.



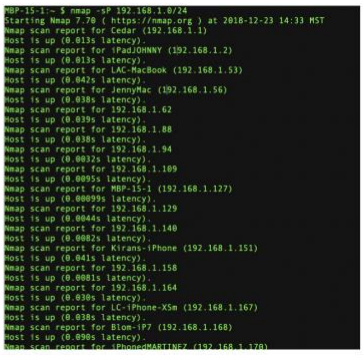


FIGURE 6 – HOTEL NETWORK AND NMAP SCAN

In the diagram above, a NMAP scan from any guest device in a 150-room hotel reveals the IP addresses of all guests and shows full connectivity among all guests.

A single segment for the hotel guests makes the network very vulnerable, and not scalable. Here are some of the drawbacks of that design:

- It's easy to crash the entire network. UDP attacks can flood the gateway (because there is only one gateway for all guests).
- A bad actor can install a rogue DHCP server.
- It's to intercept traffic. All guests are in the same VLAN, so it is easy to use TCP dump and perform Man-in-the-Middle and ARP poisoning attacks.
- It's easy to attack other nodes using TCP/UDP/ICMP flooding.
- The network does not scale. There is too much broadcast traffic, CSMA/CD and CSMA/CA can reach their limits quickly, and a single subnet leads to DHCP pool exhaustion.

A slightly better idea is to use L3 microsegmentation for the guests (/30 subnets), while still using a single VLAN. When using a /30 subnet there are two hosts addresses available per subnet: one is for the default gateway, and the other is for the guest.

Each client is placed in unique subnets, and that suppresses most of cross-end-user traffic. Each client has its own default gateway, so it is difficult to take entire network down.

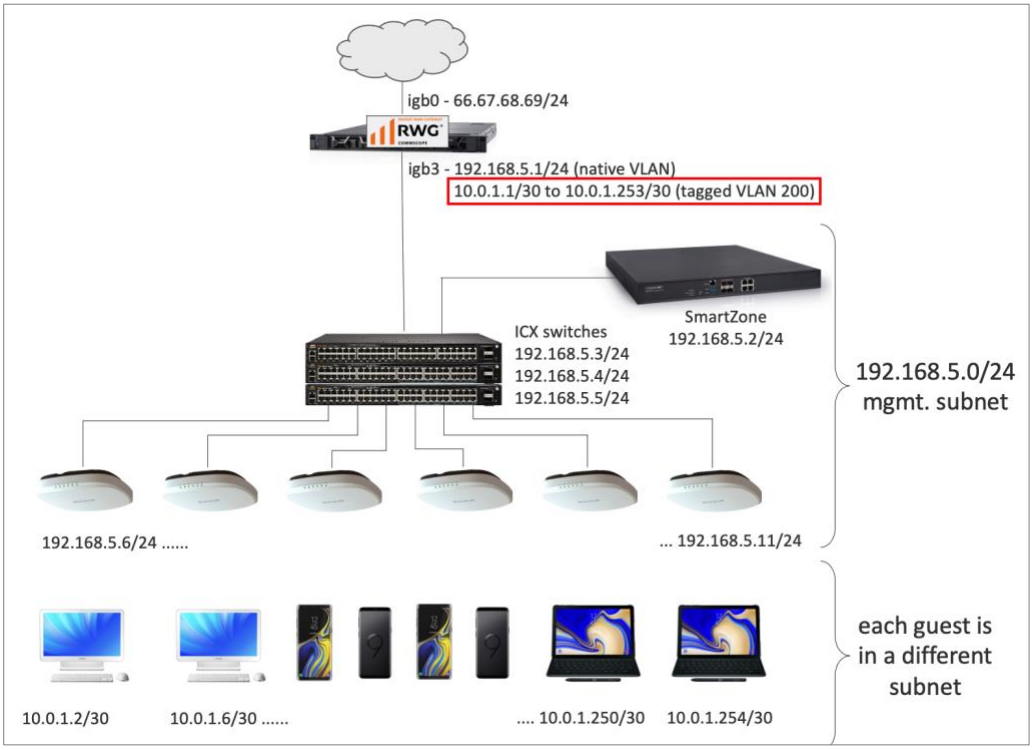


FIGURE 7 – HOTEL NETWORK USING A /30 SUBNET FOR THE GUESTS

Using RWG to Configure L3 Microsegmentation

It is possible to configure L3 microsegmentation in almost any platform, but that might be a lot of work. You need to create all /30 network interfaces, then create a DHCP server and one DHCP pool for each subnet.

FIGURE 8 – ADDING IP SUBNETS AND DHCP SCOPES MANUALLY

Using RWG you can create 64 or 4,000 subnets and DHCP pools with just one click. The following configuration creates 64 subnets and DHCP pools under VLAN 200, starting at subnet 10.0.1.1/30:

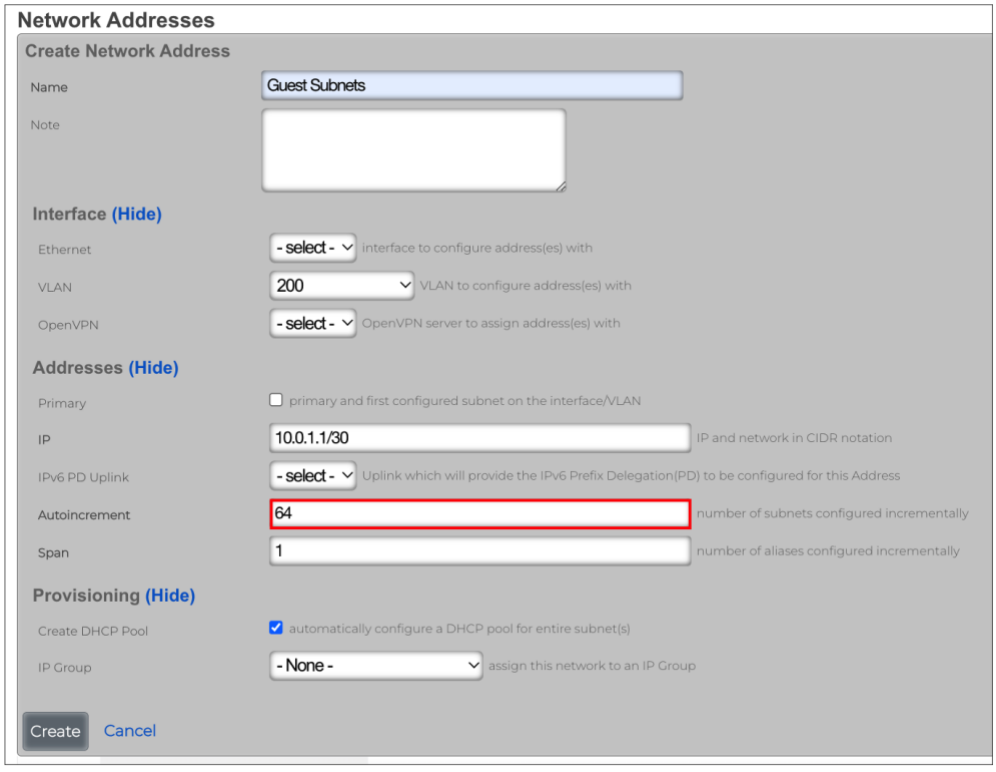


FIGURE 9 – CREATING IP SUBNETS AND DHCP SCOPES USING RWG

Even though we are still using a single VLAN, /30 subnets fixes a lot of problems:

Problem	Using /30 subnets
UDP attacks can flood the gateway	Harder, because there are many default gateways now
A bad actor installs a rogue DHCP server	This is still a problem, because there is only one VLAN
Man-in-the-Middle attacks	Harder, because there are many default gateways now
TCP/UDP/ICMP flooding to other nodes	Can be controlled using L3 firewalls
Too much broadcast traffic	Still a problem
CSMA/CD and CSMA/CA limits	Still a problem
DHCP exhaustion	Solved

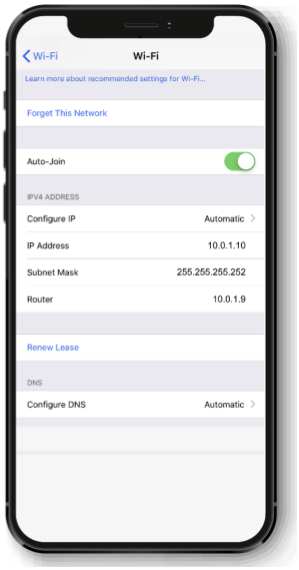


FIGURE 10 – PROBLEMS SOLVED BY USING /30 SUBNETS

The True Solution: Per-Device VLAN and IP Subnet Microsegmentation

The recommended design uses one VLAN per device, each using a separate /30 subnet.

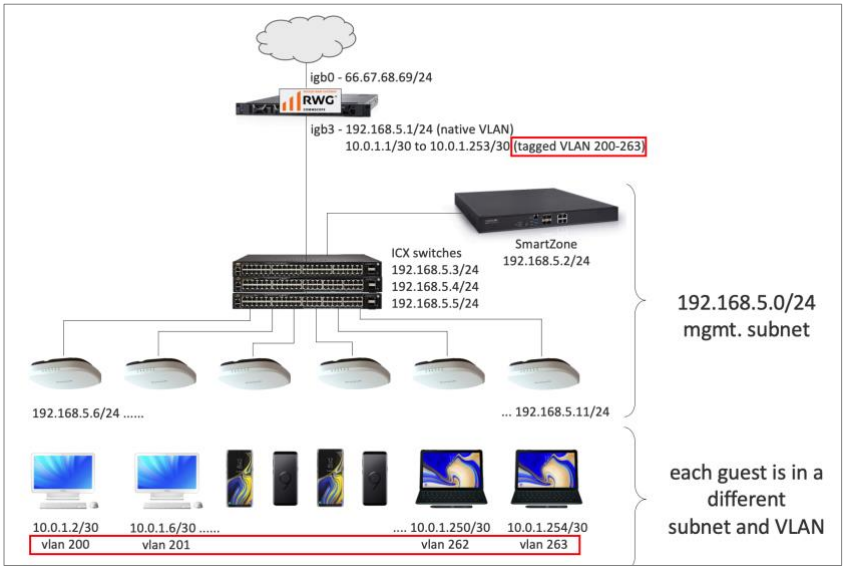


FIGURE 11 – PROBLEMS SOLVED BY USING /30 SUBNETS

In the diagram above, interface **igb3** is configured with 64 tagged VLANs (200-263), and each will be associated to a different subnet. For example, VLAN 200 has subnet 10.0.1.2/30, vlan 201 has subnet 10.0.1.6/30, and so on.

You can configure L2 and L3 microsegmentation in RWG with two clicks. In the example below, the **Guest VLANs** start at 200, and each VLAN will contain only one subnet from **Guest Subnets**.

The **Create Guest VLANs** form is used to create a range of vlans starting with VLAN ID 200. The **Create Network Address** form is used to create IP subnets that will be associated with the Guest VLANs and create a DHCP for each subnet automatically.

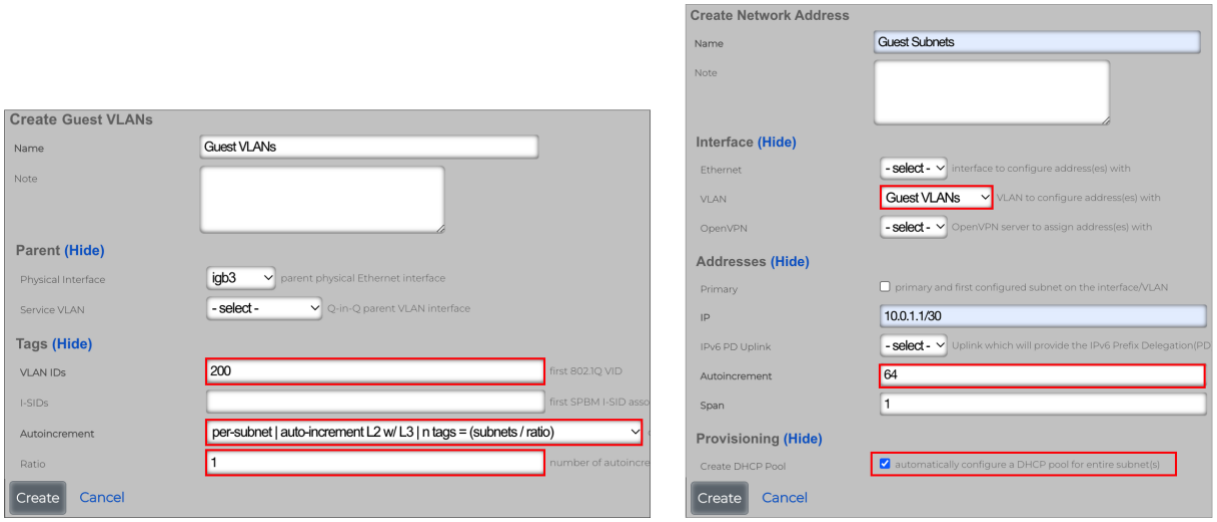


FIGURE 12 – CONFIGURING L2 AND L3 MICROSEGMENTATION WITH 2 CLICKS

RWG also configures the WLAN and the RADIUS profile in SmartZone with only one click. The WLAN uses 802.1x with MAC authentication bypass.

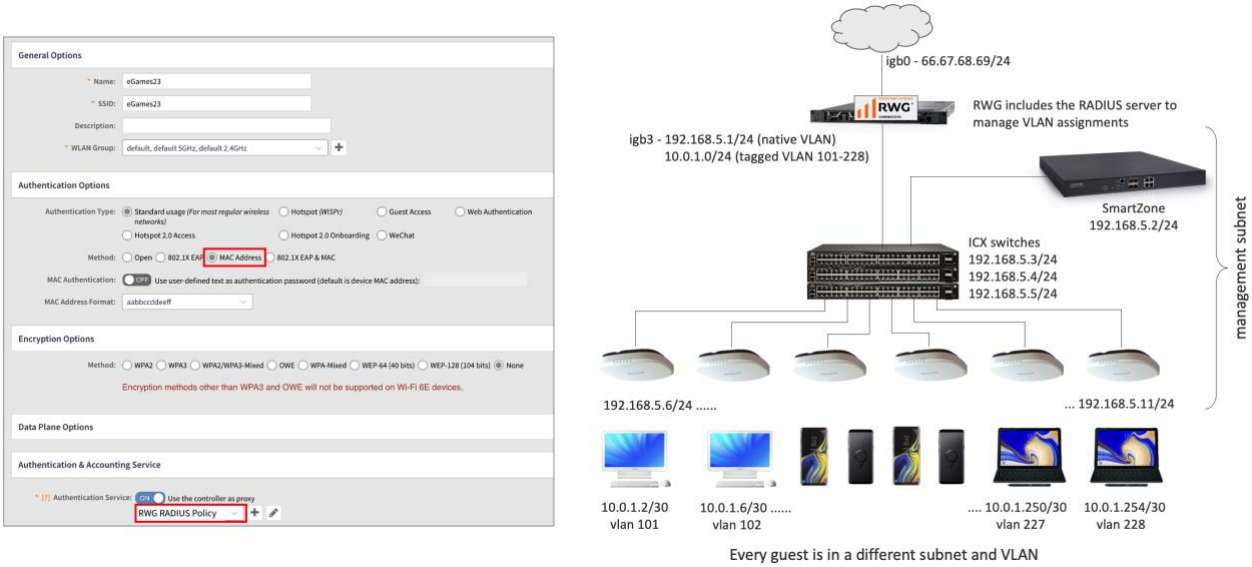


FIGURE 13 – RWG CONFIGURES THE WLAN AND RADIUS PROFILE IN SMARTZONE WITH ONE CLICK

In wireless networks using microsegmentation with one VLAN and IP subnet per client device, most of the issues are solved:

Problem	Using L2 & L3 Microsegmentation
UDP attacks can flood the gateway	Harder, because there are many default gateways
A bad actor installs a rogue DHCP server	Ineffective, because there are separate VLANs
Man-in-the-Middle attacks	TCP dump reveals nothing, so MITM attacks are impossible. Packet captures only reveal traffic between the host and its unique default gateway
TCP/UDP/ICMP flooding to other nodes	Very difficult, because of separate VLANs
Too much broadcast traffic	Broadcasts greatly reduced because of separate VLANs
CSMA/CD and CSMA/CA limits	Network capacity increases
DHCP exhaustion	Already solved by L3 segmentation

FIGURE 14 – PROBLEMS SOLVED BY L2 & L3 MICROSEGMENTATION

Microsegmentation for Wired Devices

L2 & L3 microsegmentation can also be used for wired devices. One approach is to configure the VLAN assignments statically at the switch ports, but that is very labor intensive.

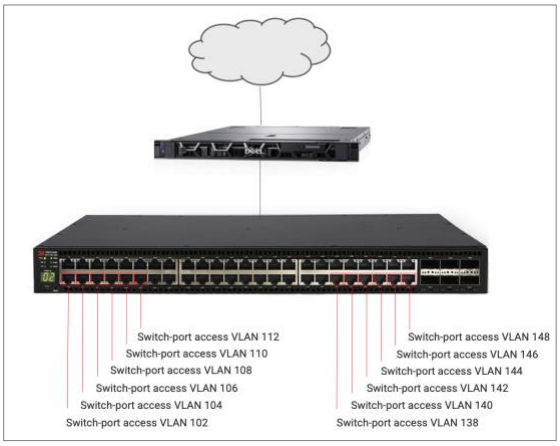


FIGURE 15 – WIRED DEVICES MICROSEGMENTATION USING STATIC VLANS

Again, a better approach is to use dynamic VLANs configured with 802.1x. At the global level, an ICX switch needs the following configuration lines:

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius-server host 192.168.5.1 key supersecretkey
```

At the port level, every switch port uses 802.1x and MAC Address Bypass (MAB) to authenticate against the RADIUS server running in RWG and receive a dynamic VLAN assignment.

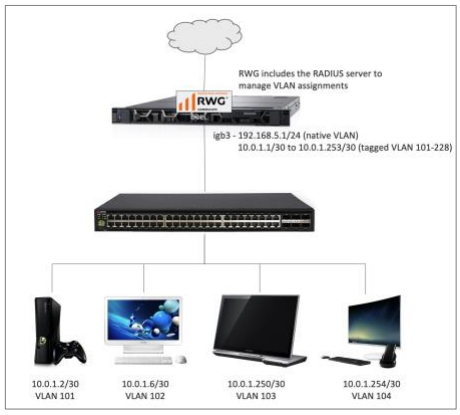


FIGURE 16 – WIRED DEVICES MICROSEGMENTATION USING DYNAMIC VLANS

Use Cases

Personal Area Networks

Personal Area Networks (PAN) is a hospitality marketing term. RWG implements PANs using L2 & L3 dynamic VLAN microsegmentation.

RWG can be integrated with PMS platforms from the main hotel chains, including MICROS FIAS. The guest authentication can use DPSKs or a splash portal and landing portal where the guest enters their credentials (typically the room number and guest's last name).

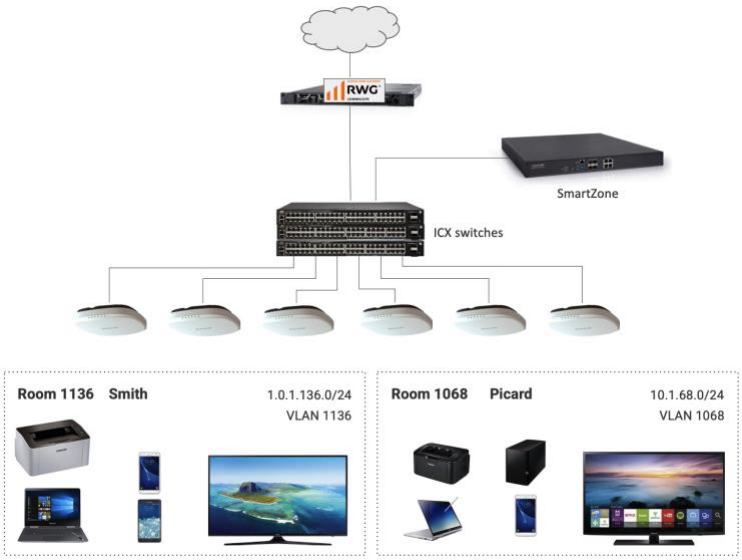


FIGURE 17 – PERSONAL AREA NETWORK IN HOTEL ROOMS

PANs can extend beyond the room walls. The **virtual room** boundary is independent of the physical space. For example, it allows a guest to stream media on a NAS located in a unit to a tablet in the laundry, or to reverse stream an Xbox in a room to a tablet in the gym or pool.

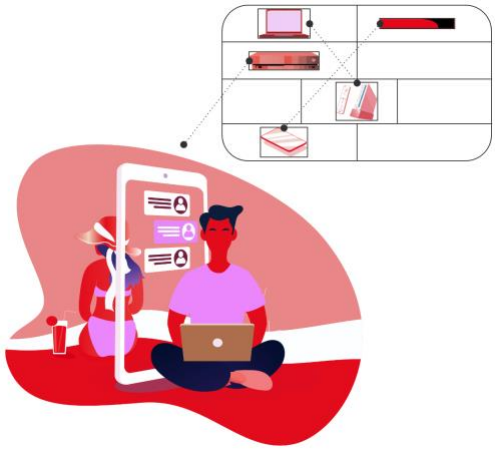


FIGURE 18 – A VIRTUAL ROOM

Using DPSKs

As an alternative to using unsecured SSIDs and portals for authentication, RWG can use WLANs with DPSKs to move each guest to a dedicated VLAN and IP subnet. In this use case a single encrypted SSID is broadcasted throughout the entire property, and the guests in each room have a single DPSK. All guest devices can use the same DPSK. The guest can only see their own traffic, and casting and AirDrop always work.

Using DPSKs, no portals are required for accessing the Wi-Fi network. In addition, the major PMS platforms can be used integrated with RWG.

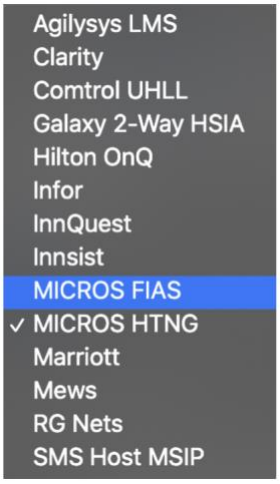


FIGURE 19 – PMS SUPPORTED BY RWG

RWG can pre-generate DPSKs using the PMS guest database. The DPSKs can use any combination of the guest room number and last name (or other fields) like:

Room: 328 Last Name: Smith	Room: 286 Last Name: Lee Last Name: Meyer
Valid PSKs:	**Valid PSKs:**
328smith	286lee
328SMITH	286Lee
328Smith	lee286
smith328	Lee286
Smith328	286meyer
SMITH328	286MEYER
... etc.	... etc.

FIGURE 20 – DPSKS GENERATED FROM THE PMS DATABASE

Any valid DPSK will take the guests to their dedicated VLAN and IP subnet.

The following diagram shows the authentication flow for a network using an external PMS with pre-generated DPSKs.

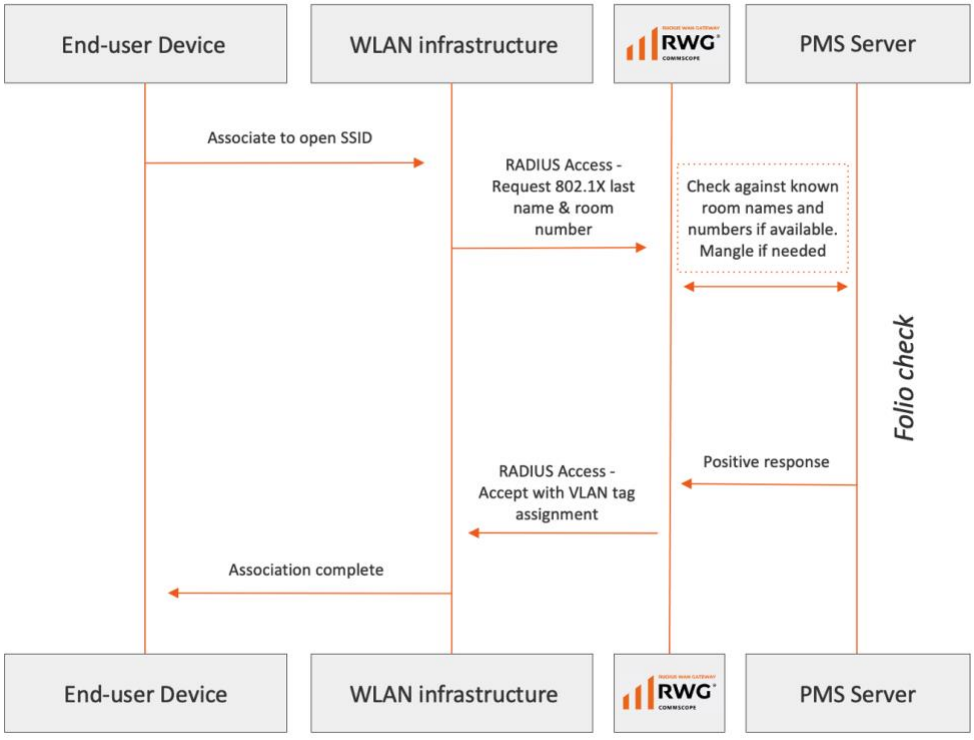


FIGURE 21 – SOLUTION FLOW USING EXTERNAL PMS AND DPSKS

Using Authentication Portals

Instead of using DPSKs, the client can use authentication portals to connect to the Wi-Fi network. The process might start with an open network that takes the guests to a splash portal that places them in a shared onboarding VLANs with limited access and less speed.

After the guests register using their room number and last name, they reach a landing portal and they are placed in a dedicated VLAN with full access, and maybe other options to increase the access speed or different services. Multiple VLAN pools and RADIUS realms might be required for that solution.

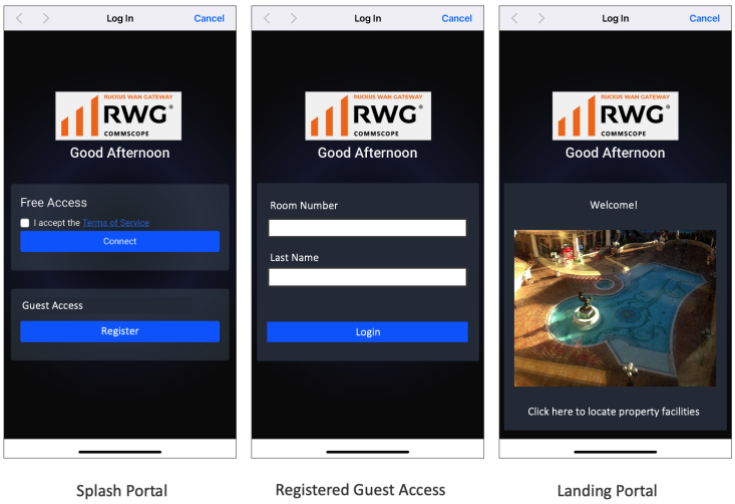


FIGURE 22 – AUTHENTICATION USING PORTALS

Residential Gateways

The diagram below shows a typical physical residential gateway architecture using DOCSIS/MoCA. Public IP addresses are distributed amongst the physical residential gateways. There is one residential gateway per subscriber network, NAT'd to a single public IP address with configurable port forwarding and DMZ.

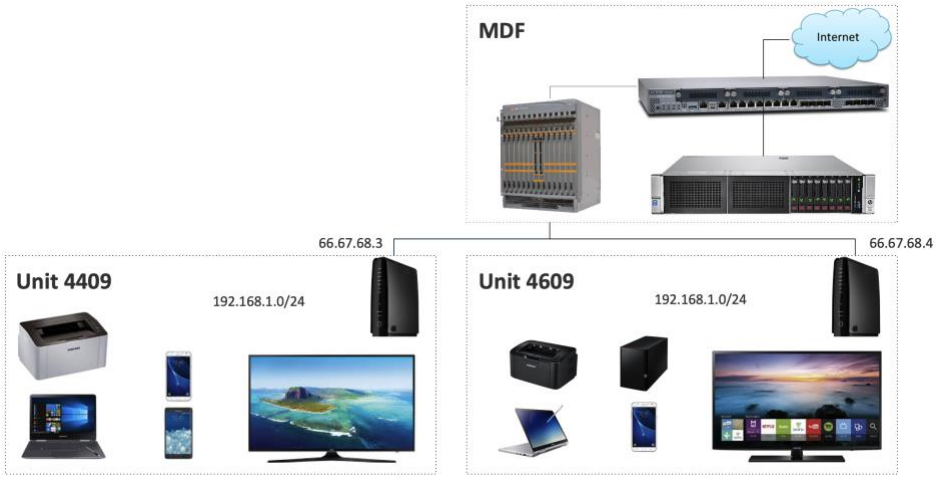


FIGURE 23 – RESIDENTIAL GATEWAY ARCHITECTURE

vRG is a RWG marketing term for a virtualized residential gateway in MDU networks. A vRG is a RWG configured like a PAN, but with different public IP addresses for each unit. Multiple public IP addresses and NAT pools are configured at the RWG WAN uplink. The public IP addresses are bound on-demand.

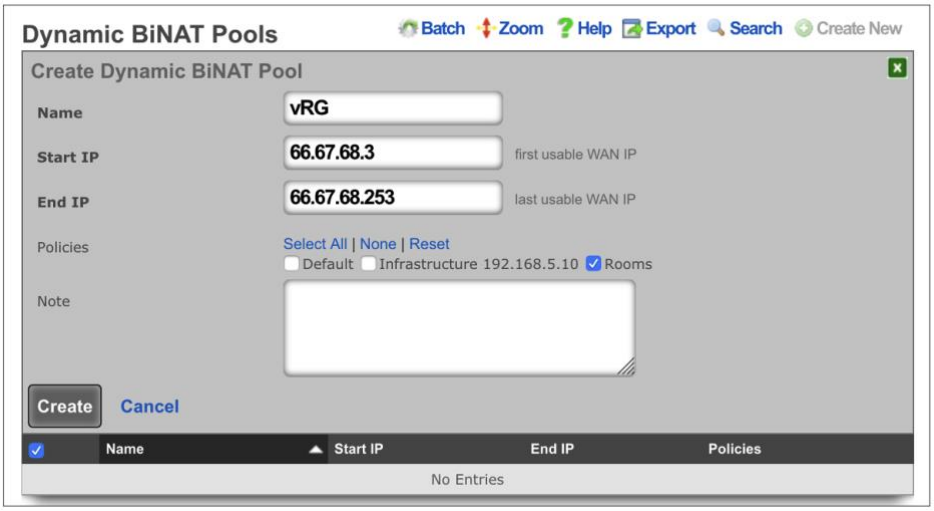


FIGURE 24 – CONFIGURATION OF BINAT POOLS IN A VRG

eSports

Some games require the players to be on the same VLAN.

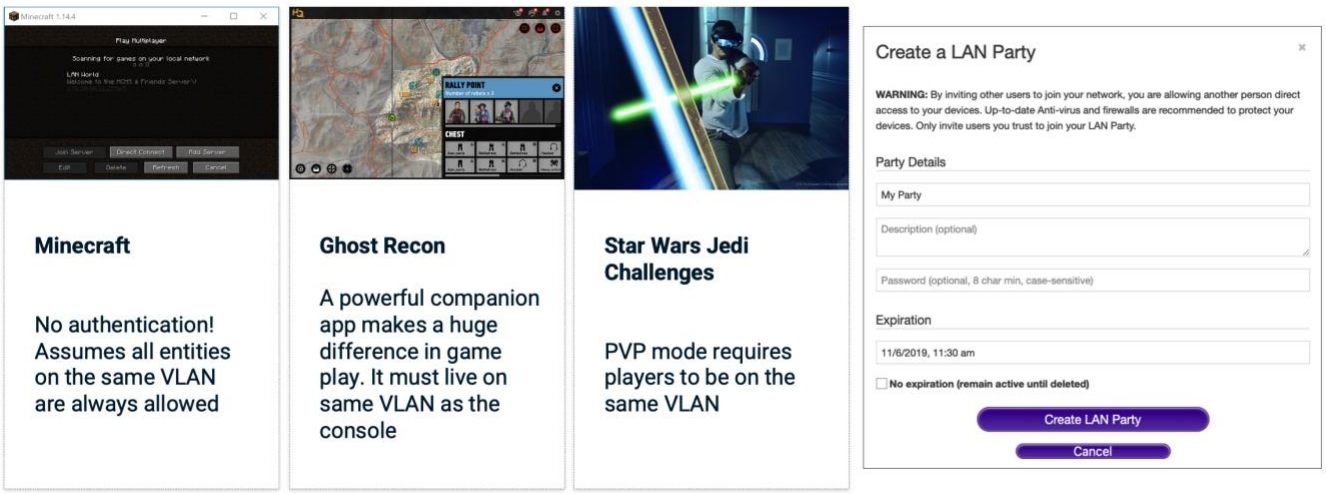


FIGURE 25 – ESPORTS SAME VLAN REQUIREMENT

RWG includes a feature called LAN Party, which brings people together temporarily in a microsegment to support collaboration, gaming, and education. AirDrop, casting, and games will work temporarily between the authorized users.

Conclusion

The Old Way to Configure Microsegmentation

The typical way to configure microsegmentation requires lots of manual setups:

- Setup the router with the correct VLANs.
- Setup the switches with the correct VLANs.
- Setup the NAC rules to drop devices into the correct VLANs.
- Setup your wireless controller to point to the RADIUS server for AAA.
- Setup your wireless access points to connect to the wireless controller.
- VLANs must match on the router, switches, wireless controllers, and APs.
- Create many VLANs is very time-consuming. Many errors might arise, like mismatches or incorrect start or end of the VLAN range.
- The DHCP pools must match the VLANs. Configuration errors might also arise:
- **Off-by-one** problems where DHCP pools for most VLANs are present... except one.
- Changes to VLAN configs but forgetting to make matching change to DHCP server.
- RADIUS/SSID/NAC rules configuration must match. Some common errors include:
- The shared secret is off by one character or has a space character before or after.
- IP address of the RADIUS server is misconfigured.
- The WLAN SSID must be programmed into the wireless controller, and it must match what the RADIUS realm expects.

It takes days to get everything right during the initial deployment, and if you make a change you need to be careful, otherwise everything will break.

The New Way - Using RWG to Configure Microsegmentation

Using RWG you enter the configuration data exactly once. All VLANs, IP subnets and DHCP scopes are configured with just a few clicks. The SmartZone controller and ICX switches are adopted by RWG, and they are configured automatically.

RWG will configure the WLAN and RADIUS profile in the SmartZone controller, and all required VLANs in the ICX switches to support the microsegmentation design.

There is never any duplicated data entry at any time, and there is a dramatic reduction in deployment time and complexity. Here is the actual measured deployment result for one SmartZone controller, 15 ICX switches, 300 APs and 500 VLANs:

- **Without RWG:** more than 1 day
- **Using RWG:** 90 minutes

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

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

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

www.ruckusnetworks.com

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

RUCKUS®
COMMSCOPE