Multi-SSID Deployment Considerations

This article provides recommendations for implementing multiple SSIDs in the same wireless environment and discusses the effect it can have on wireless performance.

Below are our general recommendations when deploying multiple SSIDs on a single physical AP:

- No more than 3 SSIDs should be enabled on any single AP.
- Each SSID should have band-steering enabled.
- Legacy bit rates should be disabled on each SSID.
- Only enable an SSID on an AP if needed.
- APs whose coverage areas overlap should not be on the same channels.
- Each SSID should be configured to tag a separate VLAN.

Interference and Channel Utilization

Channel utilization

APs and wireless clients on the same channel who are also within range of each other form a single broadcast domain, similar to an Ethernet hub. All devices can hear each other's transmissions and if any two devices transmit at the same time, their radio signals will collide and become garbled resulting in data corruption or complete frame loss. If there is an excessive amount of collisions, data would never be transmitted successfully and the wireless network would be unusable.

To avoid collisions, 802.11 wireless devices use a listen before speaking approach when accessing the wireless medium. Specifically, devices perform a Clear Channel Assessment (CCA) by listening to see if another device is actively transmitting on the channel before attempting to send its own frames. When a device detects another transmission in progress, it will perform a random back-off for a short period of time after which it would perform another check before attempting to transmit again. If the channel is clear after a check, the device can access the channel and send some data. As the number of devices needing to transmit frames increase on the channel, congestion can occur to the point where devices spend more time receiving than sending.

Interference

When two wireless devices transmit at the same time, their radio signals will collide and become garbled. 802.11 devices on the same channel use a CCA check to avoid these collisions. However, the CCA check may not detect a
transmission occurring on a different channel that also has some frequency overlap on the channel the check is being performed on. In this case, two 802.11 devices on different channels that overlap may transmit at the same time causing a collision and possible data corruption or frame loss. This is called interference because one device's transmission interferes with another device's transmission.

As the number of interfering devices increase, so does the potential for frame loss. The 802.11 standard uses a reliable transport mechanism where each sent data frame must be ACK'd by the receiver to ensure the frame was not lost in transit or corrupted. If the sender does not receive an ACK, it must re-transmit the same frame until an ACK is received. Re-transmissions result in slower speeds because it takes longer to successfully send a single frame.

**Consequences of Multiple SSIDs**

One frequently overlooked aspect of wireless networking is that a network administrators can control interference and channel utilization generated by their own managed wireless system. Dashboard allows admins the ability to enable multiple SSIDs on a single physical AP (Access Point). Each SSID that is enabled on a given AP is called a VAP (Virtual AP). VAPs behave as their own independent AP, operating on the channels the physical AP is set to. Therefore enabling 5 SSIDs on a single AP in Dashboard is nearly identical to deploying 5 physical APs with one SSID each. Normally, multiple SSIDs are used to provide different types of wireless network access to different device types and user classes. The downside of enabling more SSIDs is that it creates more channel utilization due to overhead.

**Overhead from Management Frames**

Beacons and probe response are two types of required wireless management frames that can increase channel utilization. Beacon frames are used by the VAP to advertise the SSID and inform connected clients that frames are waiting for delivery. Each VAP must send a beacon every 100ms at the lowest supported data rate so all clients can receive it. The date rate is 1Mbps by default with 802.11b/g/n and 6Mbps on 802.11a/n.

Wireless clients can also discover available wireless networks using probe requests. When a VAP receives a probe request, it will respond with a probe response for the the SSID which contains the wireless capabilities. Probe requests and responses are always sent at the lowest supported data rates with 1Mbps 802.11b/g/n and 6Mbps on 802.11a/n.

As the number of wireless networks operating on a specific channel increase so does the amount of beacon frames and probe responses. Take a scenario where there are two physical APs on the same channel each with a single SSID. Both APs will transmit one beacon frame every 100 ms and when any client sends a probe request on that channel, each AP will send a probe response. This would not cause much overhead. However take the same two physical APs each with 4 SSIDs. Now 8 VAPs are independently sending beacon frames every 100ms and any time a client sends a probe request, 8 probe responses are transmitted. This example does not begin to take into account neighboring WiFi system management frames, wireless data transfers, or non-802.11 interference (such as microwaves and cordless phones). WiFi Revolution, a team of wireless experts, has put together a [SSID overhead calculator](#) which allows an admin to calculate the amount of overhead based on the number of VAPs and APs.

The two configurations below can be used to increase the data lowest supported data rate and decrease probe
responses on the 2.4Ghz band.

- **Disabling legacy bit rates:** This feature allows the administrator to set the lowest supported data rate to 6Mbps on a per-SSID basis. Although it may reduce the connectivity options of 802.11b clients, it does increase the data rate of beacons and probe responses. Therefore these transmissions consume less airtime.

- **Band Steering:** When band steering is enabled, dual-band (2.4GHz and 5GHz) APs only reply to probe requests on the highest supported frequency band for the client. This reduces the number of probe responses on 2.4GHz by pushing clients to 5Ghz where supported.

## Deploying Multiple SSIDs

The key to successful WiFi deployment is eliminating SSID redundancy. Redundancy occurs when multiple SSIDs are deployed providing different types of access, but the configurations used could allow for them to be consolidated into a single SSID. With the Cisco Meraki system, multiple SSIDs are only needed when NAT mode is required instead of Bridge mode or there are different wireless encryption requirements such as no encryption, WEP, or WPA2.

Below is a common deployment scenario:

- **Guest SSID:** This SSID will normally have no encryption. It is configured to provide internet access to clients while keeping them isolated from the corporate network using NAT mode and firewall rules. A bandwidth limit is also used to prevent guest clients from hogging bandwidth. APs whose coverage cells extend into guest areas should have this SSID enabled. It also shouldn't use legacy data rates and have band steering enabled.

- **Internal SSID:** This SSID should be for trusted users. The SSID will use encryption (WPA2-PSK or WPA2-Enterprise) and network access via bridge mode. Different VLANs, firewall rules, traffic shaping and bandwidth limits can be based on user or device class and can be assigned using **Group Policy**. APs whose coverage cells extend into internal areas should have this enabled. It also shouldn't use legacy data rates and have band steering enabled.

- **Legacy:** If necessary, an SSID for legacy devices that use legacy encryption or data rates can be enabled. This SSID will normally use bridge mode with VLANs and should only be enabled in areas where legacy devices exist. While band steering should be enabled, and legacy bit-rates disabled, this SSID can be an exception if required to support the legacy clients.

The **Per-AP availability** feature allows an administrator to enable SSIDs on a per-AP basis. Using this, more than 3 SSIDs can exist within a network, but each is only active on the APs where it is needed, thus keeping the total active SSIDs on any given AP within 3.

Another suggestion is to configure APs in a Dashboard network to use non-overlapping channels (1, 6, and 11 on 2.4Ghz radios), and in areas where two APs are within range, reduce their transmit power.

If your network requires different network access, traffic, and security controls based on user or device class, **Group Policy** is the most versatile way an administrator can apply bandwidth limits, traffic shaping, L3/L7 firewall rules, VLANs and Splash page settings on a per-client or per-user basis. Group Policy can be assigned to clients at the globally, per-
SSID, or based on RADIUS attributes.