Chapter 5. 802.11ac Planning

If you don't know where you're going, you'll end up someplace else.

—Yogi Berra

Although most of the discussion in this book has been about speed, the real value of 802.11ac to the network administrator is that it increases the capacity of a wireless network. Whether the network needs to serve more clients with today's level of throughput or today's client load with higher throughput, the solution is 802.11ac.

Several intersecting trends are driving the need for increased capacity. Many new devices are built around the assumption that 802.11 coverage is ubiquitous and therefore do not have an alternative LAN technology for accessing networks. Of these new devices, most of them are battery-operated and portable, and do not even have the capability to connect to wired Ethernet networks. As traffic shifts onto the wireless LAN, it must support new demands for connectivity. Increased numbers of devices is only the first part of a one-two punch being delivered by users. After connecting so many devices to wireless LANs, users then change the type of applications in use. With improved computing power and display technology, the user experience is becoming significantly more media-heavy, with a special emphasis on streaming multimedia and especially video support. Combine an increase in the number of devices with increased demand for capacity from each device, and you have a recipe for congestion unless greater capacity is in the cards. As the improved performance of 802.11ac becomes readily available in client devices, there will be user demand to take advantage of that speed.

Adoption of 802.11ac will likely happen more quickly than that of its predecessors. Improving speed is always welcome in networking, and many networks are built with a three- to five-year time horizon of service. Part of the planning process in building an 802.11ac network is to assess not only the current load on your network, but also the expected growth in demand for service to determine whether the increased density justifies using the highest-performance technology available. A strong industry focus on interoperability has made the transition to 802.11ac straightforward for network administrators as well.

Getting Ready for 802.11ac

802.11ac is evolutionary as much as it is revolutionary. Many of the design principles that have been used with previous technologies are still applicable, with a few minor changes to take advantage of new protocol features. The drivers to use 802.11ac are the same drivers that have justified every other network upgrade you have ever done:

Peak speed and/or throughput

> The most obvious driver for 802.11ac is the new higher speeds. Some applications require as much speed as the network can deliver, and these are obvious beneficiaries of the new technology. Increased use of video is a major driver of 802.11ac adoption, as is the increase in device density due to the widespread use of tablets and wireless LAN–equipped smartphones. Video is widely used throughout the spectrum of wireless LAN users, whether it is large and detailed images for patient care, instructional videos in the classroom, or wireless display technologies in corporate conference rooms. Higher speeds also enable additional point-to-point deployment scenarios and provide the capacity necessary to serve 802.11n clients with mesh backhaul connections.

Capacity

> With so much raw capacity, especially with wider channels, 802.11ac provides a superior level of service. In addition to the general efficiencies that the IEEE 802.11 working group builds into new specifications, products often add clever features to further extract capacity increases from the new physical layer. One common method of doing so is to bias transmissions toward frames that require shorter times to transmit. Even though 802.11ac can transmit large numbers of bits, the extremely high data rates mean that even very large amounts of data are transmitted faster than small packets were in 802.11b.

Latency

> Some applications benefit primarily from lower latency, especially real-time streaming applications such as voice, videoconferencing, or even video chat. Improving latency can be done by building a more efficient network, but often the best way to improve latency is to reduce the load on the network. 802.11 measures load by airtime utilization, so moving to faster physical layer standards improves latency by reducing the airtime load. Multi-user MIMO also has the potential to decrease network load by enabling parallel transmissions. Reducing latency means that even a few 802.11ac devices may benefit the entire network by decreasing airtime demand.

As part of the IEEE project authorization process, a task group in the formation process needs to discuss compatibility with previous technology standards. Early adopters of wireless LANs made significant investments in the technology, and the IEEE process is designed to protect that investment. Backward compatibility with prior 802.11 standards was a key consideration in the 802.11ac standardization process, and there was extensive work done in the protocol to ensure that 802.11ac would work with the many existing wireless LAN devices. In addition to physical-layer compatibility, 802.11ac has extensive MAC-layer compatibility, which enables newer 802.11ac devices to perform at their best even when surrounded by older devices. In fact, these functions were designed to enable a little bit of 802.11ac to speed up any network.

802.11ac was designed from the beginning to be compatible with prior standards (802.11n, 802.11a/g, and 802.11b). Don't let compatibility worries slow you down—adding 802.11ac speeds up any network, even if it has only a few 802.11ac client devices.

Even though 802.11ac is the future physical layer in wireless LANs, it will not be the only physical layer. APs that are sold as "802.11ac APs" will have one 5 GHz radio running 802.11ac, and they will also have a second 2.4 GHz radio running 802.11n. Even as 802.11ac becomes established, the 2.4 GHz band will continue to depend on the same 802.11n technology that has been used for the past several years.

Catching the 802.11ac Technology Wave

Early in the development of wireless LAN technology, a new PHY was brought to market all at once. With 802.11n, however, the standards started to become much more complex, and different levels of capability came to the market in distinct "waves" or "phases." Once the basic technical details are worked out, it can often be much easier to write a standard than to build a product. For example, the work required to add four-spatial-stream support into the 802.11n standard was relatively minimal after the basic ground rules were complete, but as of the 2013 publication date of this book, four-stream 802.11n devices have yet to be brought to market because of the engineering challenges involved in building the powerful DSP required to perform the spatial mapping while staying within the 15-watt 802.3af power limit.

802.11n came to the market in waves due to the overall complexity of the standard. 802.11ac will follow this well-worn path, with a rough estimate of the contents of the first two waves in Table 5-1. The first generation of 802.11ac delivers another jump in channel bandwidth, along with a new modulation. Taken together, these two features are enough to nearly double the speed of a typical three-stream client device. The second wave of 802.11ac will add even wider channels, four-stream support, and

beamforming. Although there is a temptation to focus on the headline rates only, beamforming has the potential to deliver significant gains in network capacity by improving the data rates at which most clients transmit. Not all transmissions occur at the fastest rate, so the beamforming boost can be substantial if it increases the data rates used by clients.

Table 5-1. 802.11ac technology waves

	Wave 1	Wave 2
Standard basis	802.11ac, draft 2.0	802.11ac, final version
Timeframe	Mid-2013	2014
Channel width	20, 40, and 80 MHz	Potential to add 160 MHz channels
Modulation support	Up to 256-QAM	Same as wave 1
Lowest 11ac speed	173 Mbps (20 MHz, 2-stream, 256-QAM)	Same as wave 1
Typical 11ac speed	867 Mbps (80 MHz, 3-stream, 256-QAM)	1.7 Gbps (160 MHz, 3-stream, 256-QAM)
Maximum 11ac speed	1.3 Gbps (80 MHz, 3-stream, 256-QAM)	3.5 Gbps (160 MHz, 4-stream, 256-QAM)
Beamforming	Yes (depending on underlying chipset)	Yes, possibly MU-MIMO

First wave 802.11ac versus second wave 802.11ac

A key decision in planning for 802.11ac is when to jump in and deploy widely. Unlike previous physical layers in 802.11, the first wave of 802.11ac does not offer a clear-cut compelling advantage for every user. First-wave 802.11ac products are now available, and derive their additional speed from two main protocol features. Getting the most out of the first wave of 802.11ac will require an environment that can use one or both of these features:

256-QAM

> The two top data rates in 802.11ac add 33% to the speed over 802.11n, but they require significantly higher signal-to-noise ratios. As a practical matter, such high SNRs require clean radio spectrum and short AP-to-client distances.

80 MHz channels

> Clean spectrum is required to allocate contiguous 80 MHz blocks, and even with Dynamic Frequency Selection (DFS) support, there will only be five available 80 MHz channels until the new spectrum discussed in the sidebar "Proposed Additional Spectrum for 802.11ac in the United States" becomes available. Five channels is enough to plan a network, but it will not be as easy as it was with the multitude of channels that were available in 802.11n.

In some environments, it is possible that neither of these features will provide a compelling reason for a widespread 802.11ac deployment. In that case, it still offers the highest available capacity and best support for high-density areas within your network. Table 5-2 compares the performance of the first two waves of 802.11ac.

Table 5-2. Performance comparison of 802.11ac waves

Protocol feature	First-wave gain over 802.11n	Second-wave gain over 802.11n
256-QAM data rates	1.33x	1.33x
80 MHz channels	2.1x	Same as first wave
160 MHz channels	Not available	4.3x
Up to eight spatial streams	No gain—first wave is 3 SS	1.33x—second wave is 4 SS
Multi-user MIMO	Not available	~2x?
TOTAL	**2.8x**	**~15x?**

Client Device Mix

As much as network administrators would like to believe that networks are their own reward, a network exists to get work done. The number, types, and capabilities of devices attached to the network are an important part of the planning process. One set of data for input into the planning process would be information on the existing devices attached to your wireless LAN today, and your existing wireless network management system should report the client mix in a variety of ways. However, in building a network, it is important to look ahead over the life of the network. In 2013, for example, only a few client devices will be 802.11ac-capable, but within a year 802.11ac will be widely available in client devices. Previous physical layers for wireless LANs have followed similar adoption trajectories. At first, the new technology is used in high-density and high-capacity areas; as those areas take hold, they support enough of a volume increase to drive down the cost of the new technology for everybody.

Table 5-3 shows the evolution of client capabilities as they move from 802.11n to the first wave of 802.11ac technology. Naturally, there will be departures from the table, but the general rule is that high-end laptops will use the fastest connectivity available while small battery-powered devices will use power-efficient single-stream interfaces. Low-end laptops fall somewhere in between and will typically settle for a less expensive wireless interface that has middle-of-the road capabilities. High-end tablets may also opt for two-stream interfaces.

Table 5-3. Effect of 802.11ac on client capabilities

Type of device	Radio type (in 2013 & earlier)	Channel width (2013 & earlier)	Data rate (2013 & earlier)	Radio type (2014)	Channel width (2014)	Data rate (2014)
Dual-band smartphone	802.11n, 1-stream	20 MHz	72 Mbps	802.11ac, 1-stream	20/40/80 MHz	Up to 433 Mbps
VoIP handset	802.11a/b/g or 1-stream 802.11n	20 MHz	54 Mbps	802.11a/b/g or 1-stream 802.11n/ac	20 MHz	Up to 87 Mbps
Tablet	802.11n, 1-stream	20/40 MHz	72 or 150 Mbps	802.11ac, 1-stream	20/40/80 MHz	Up to 433 Mbps
Netbook/low-end laptop	802.11n, 2-stream	40 MHz	Up to 300 Mbps	802.11ac, 2-stream	80 MHz	867 Mbps
High-end laptop	802.11n, 3-stream	40 MHz	Up to 450 Mbps	802.11ac, 3-stream	80 MHz	1.3 Gbps

Although 802.11ac is often dismissed as too power-hungry for mobile devices, single-stream 802.11 MIMO devices do not require significantly more power than their SISO predecessors. The main consumer of power in a MIMO device is the power-hungry digital signal processor that performs spatial mapping. By using only a single spatial stream, a portable device can reap significant benefits from 802.11ac's increased speed and wider channels without paying a significant power-consumption penalty. Although there will be an increase in power requirements to use wider channels, the trade-off is that transmissions go so much faster that the analog section is on for much less time. With a net battery life benefit, 802.11ac will be adopted widely in portable devices. In fact, 2013 saw the first introduction of an 802.11ac-capable smartphone.

Information on your device mix can be gathered from several sources. Naturally, knowledge of what has been purchased is an important source of information, but with the trend away from supporting exclusively corporate-owned devices, there is a need to gather information on all of the devices using the network. One constraint on the

adoption of 802.11ac is that it is supported only in the 5 GHz band, and a significant number of devices must be ready to move to the 5 GHz band to see strong benefits from 802.11ac.

Because 802.11ac is only available in the 5 GHz band, the benefits available depend on the number of 5 GHz–capable devices on the network.

One welcome development of 802.11ac is that it is driving increased use of the 5 GHz band. Many high-end client devices have begun to support 5 GHz operation with dual-band 802.11n interfaces, and these devices reward their users with improved connectivity. Use of the 5 GHz band has been restricted to high-end devices, in large part because it is still possible to be an "802.11n" device while supporting only one band. In order to label a device as "802.11ac," it will be necessary for that device to support the 5 GHz band, even though it is almost certain that a device labeled as "802.11ac" will also support 802.11n operation in the 2.4 GHz band.

Supporting client devices in the 5 GHz band requires a somewhat denser network deployment. If you have designed your network around the needs of coverage for the 2.4 GHz band, successfully moving to 802.11ac will require more APs.

Single-Stream Devices in 802.11ac

802.11ac offers significant benefits to single-stream devices. By extending the channel width up to 80 MHz, it makes substantial speed increases possible for single-stream devices, especially when there is sufficient uncongested spectrum available to transmit with wide channels. Looking forward to the next wave, multi-user MIMO has the potential to add significant performance to networks as well by transmitting to multiple single-stream clients at the same time. Unlike with 802.11n, there is no need to discount the gains of 802.11ac simply because of the presence of a significant number of single-stream client devices on the network. Even the first wave of 802.11ac APs will offer benefits to pre-11ac single-stream devices. As new generations of radio chips are produced, the performance will continue to improve, especially when MU-MIMO is available so multiple single-stream 802.11ac devices can receive transmissions simultaneously.

Application Planning

To be successful, the network must support the key applications that are in use. Many access points now offer some form of application visibility to augment your suppositions about the applications commonly used on the network, and can report on the throughput used by common applications. As an alternative to running application reporting on your network, Table 5-4 has a list of some of the most common applications that network administrators need to consider, along with the Wi-Fi Multimedia (WMM) access category that each application is typically assigned. WMM allows administrators to place traffic into four categories, with the higher-level categories receiving preferential access to the medium. In declining order of priority, traffic can be placed into queues for voice, video, best effort, or background traffic.

Table 5-4. Application throughput needs

Application	Recommended bit rate (Mbps, unless noted)	WMM access category
VoIP – voice transport	27 – 93 kbps (codec dependent)	Voice
VoIP – signaling (typically SIP)	5 kbps	Best effort
Remote display	150 kbps (without video), 1.8 Mbps (with video)	Video
Web conferencing	384 kbps – 1 Mbps	Video
FaceTime	0.9	Video
AppleTV video streaming	2.5 – 8	Video
High-definition video (compressed)	2 – 5	Video
High-definition video (uncompressed)	20	Video
High-definition video (uncompressed HDMI)	3.3 Gbps	Video
Standard-definition video	1 – 1.5	Video
Email/web browsing	0.5 – 1.0	Best effort
File sharing	5	Best effort
YouTube	0.9	Best effort
Network backup	Available capacity	Background

The applications in Table 5-4 are all based on unicast data. In many cases, 802.11 access points will convert multicast frames to unicast frames, and the same estimation technique can be used for multicast applications.

Application throughput requirements can be used to create a rough guide for the capacity requirements of an access point. None of the applications in Table 5-4 is the classic "killer app" that absolutely requires 802.11ac, but the increased use of video distribution highlights the more limited capacity of 802.11n. The easiest way to use application throughput requirements to estimate capacity requirements is to divide the total capacity of a device by the application's bit rate; this will give you a rough estimate of the capacity needed. Although an 802.11ac AP may be capable of nearly 1 Gbps of throughput, a single-stream tablet will be unable to use all of that capacity. For example, if a single-stream device is capable of 25 Mbps of TCP throughput, it will require approximately 4% of the available airtime of an access point to do standard emailing/web browsing (1 Mbps for the application divided by the 25 Mbps capacity). A dual-radio AP could support approximately 50 such devices running the application. For 802.11ac, there may be different capabilities in the 2.4 GHz 802.11n radio and the 5 GHz 802.11ac radio, provided the target devices can use at least some of the advanced 802.11ac protocol features.

Admission control

If a significant fraction of the anticipated traffic is in the high-priority voice and video queues, part of your equipment evaluation should be about whether *admission control* is a valuable addition to your network. When admission control is enabled, client devices must request access to high-priority queues. For example, before placing a voice call, a client must send a request to the AP to reserve capacity for a VoIP data stream. The AP can then determine whether there is sufficient airtime available to accept the device, and either reserve the capacity or reject the request to connect due to insufficient airtime. Admission control is available using a feature of the 802.11 protocol called the *Traffic Specification* (TSPEC), and products supporting this capability can be certified for *Wi-Fi Multimedia Admission Control* (WMM-AC) by the Wi-Fi Alliance interoperability certification program.

Physical Network Connections

As part of building an 802.11ac wireless edge, it is necessary to connect APs to the edge of the existing network. This involves two main tasks: physically connecting the AP to the edge of the network to provide data transport services to it, and providing sufficient power to start up the AP.

Backbone connectivity

Physical connections of 802.11ac devices to the backbone are a snap. APs work as bridges and connect to existing Ethernet backbones, so any existing Ethernet can readily be extended with 802.11. Even basic two-stream 802.11ac devices can easily push more than 100 Mbps, so a gigabit backbone is a practical requirement for an 802.11ac access layer. Although some products will support bonding of multiple links, Fast Ethernet just isn't fast enough to support 802.11ac. Upgrade your network edge to gigabit speed before installing 802.11ac.

Although 802.11ac is often described as "gigabit wireless," a gigabit Ethernet connection to the AP is sufficient for the first wave of 802.11ac products. 802.11 speeds are based on the data rate used to transmit the MAC frame, and do not include the effects of protocol overhead such as interframe spacing and the need to transmit PHY headers. Unlike Ethernet, 802.11 is a half-duplex medium. When an Ethernet link is described as 1 Gbps, it is capable of operating at 1 Gbps in both directions, whereas its 802.11 equivalent is capable of operating at 1 Gbps in both directions combined. Depending on network traffic, the wireless LAN may have more upstream or more downstream traffic, but the speed of the wireless LAN is the sum of the upstream and downstream directions. To make speed even more deployment-dependent, the top data rates in 802.11 are generally available only to clients with high signal-to-noise ratios, and there is a natural distribution of access speed because as devices increase in distance from the access point the speed decreases. For 802.11ac, speeds in excess of a gigabit require high-SNR links in order to use the 256-QAM modulation, and the natural spatial distribution of clients ensures that many clients will be operating at mid-range speeds.

In most networks, the protocol overhead plus the spatial distribution of client devices away from the AP will typically lead to a maximum practical throughput of about two-thirds of the headline rate. Apply that rule to a first-wave 802.11ac AP with a 1.3 Gbps radio in the 5 GHz band and a 450 Mbps 802.11n radio for the 2.4 GHz band, and the maximum practical throughput is slightly in excess of 1 Gbps. Even with atypical mixes of upstream and downstream traffic, fitting that into a single full-duplex Ethernet link is comfortable.

For the first wave of 802.11ac, make sure the Ethernet edge is gigabit, but don't worry about upgrading to 10-gigabit Ethernet access ports.

Capacity analysis for the connection of the access layer is an important component of ensuring sufficient backbone capacity. Although gigabit connections suffice for connecting access points in the first wave, the access layer switches themselves should have 10-gigabit uplink capacity to the core of the network to accommodate multiple 802.11ac APs. As the capacity of 802.11ac grows in successive waves, 10-gigabit uplink capacity will become even more important.

As part of planning a first-wave 802.11ac deployment, you will want to look ahead to the second wave in 2014. Cable infrastructure needs to support a wireless LAN for much longer than the lifetime of any particular generation of access points. With the second wave of 802.11ac, the speed will rise to 1.7 Gbps in 80 MHz channels and may be as high as 3.5 Gbps if 160 MHz channel support is introduced. With those speeds, a single gigabit link may no longer be sufficient.

Several options exist for supporting the increased capacity of the wireless LAN in the second wave. One is to handwave and say that gigabit connections are sufficient, much like some network administrators used Fast Ethernet to support early 802.11n APs. In many cases, the actual connection rates will be low enough that this might be viable, especially in coverage-oriented deployments.

If cable installation is required for your first-wave 802.11ac deployment, it is possible to lay the foundation for the second wave and beyond by installing two Ethernet cables to each AP location to support bonded connections. Be sure to use high-quality cables such as Category 6 or 7. The practical throughput of a 3.5 Gbps 802.11ac radio plus a 600 Mbps 802.11n radio is probably around 2.5 Gbps total at peak, but if the 160 MHz channel support is removed, the practical throughput is probably more like 1.5 Gbps, a speed well within reach of a dual bonded gigabit Ethernet connection. If you have an existing cable plant, it is likely to be expensive to return to the cable plant to add a second Ethernet link, but if the cable installation is new with the 802.11ac deployment, it's a good idea to install two cables just to be safe. The major cost of installing cable is labor, and the decision to install two cables will not add significantly to the cost.

For new cable plants to support 802.11ac, install two Ethernet cables. Bonded 1-gigabit Ethernet connections are future-proof and will support the second wave of 802.11ac.

Depending on your deployment scenario, there are additional reasons to consider two ports. As wireless LANs continue their march toward being the only access method for many devices, providing a highly redundant service becomes even more important. Dual-homed access points can draw power and connect to the network core through redundant paths, which may be attractive for certain types of deployments. For example, a financial firm that conducts trading operations or a health care organization supporting patient care and monitoring over a Wi-Fi network will want to carefully guard against even brief outages.

As 802.11ac continues to evolve, even higher speeds may be required. At the time this book went to press, 10-gigabit connections were only available over fiber cables. Fiber does not support power transmission, and thus is unlikely to be offered as an AP connection technology. There are efforts underway to supply power over 10 gigabit copper connections, but at the time this book was written, even 10-gigabit switches with copper connections were not very common.

Power requirements

The electrical power requirements of 802.11ac will be higher than for previous 802.11 standards. Although 802.11ac radio chips are more efficient than prior chips, they are doing significantly more work. Additional spatial streams and wider channels require more sophisticated signal processing, so gains in power efficiency are outweighed by the new protocol capabilities. With higher data rates, frames are shorter and there is a significantly higher frame rate. All this adds up to higher resource requirements at the AP: more power for new radios, more buffer memory for frame operations, and higher-powered CPUs to do more to each packet at higher frame rates. As a result, 802.11ac APs are unable to work within the 13-watt budget of 802.3af.[39]

802.11ac APs will not offer full functionality with 802.3af, so part of the planning process should be to identify how to provide the required power to new APs.

Power options for 802.11ac are basically unchanged from previous generation of wireless LAN access points. The easiest way to provide additional power to run 802.11ac APs is to provide power using 802.3at (sometimes called "PoE plus"), a newer power standard that provides up to 25.5 watts at the end of a full-length Ethernet cable. 802.3at power is provided by many newer edge switches and can be added onto existing networks by using mid-span power injectors.

Alternatively, APs can be powered by DC power adapters if there are outlets readily available at the installation locations. If power outlets are unavailable, it will probably be quite expensive to add them to the best locations for AP installation, which are typically in the ceiling. Some products have the ability to draw power simultaneously from multiple power over Ethernet (PoE) connections, which enables these products to add two 13-watt 802.3af sources together for higher power draw. In most cases, the cost of running a second cable to existing AP mounting locations is prohibitive compared with that of purchasing mid-span injectors.

Security

802.11ac does not make fundamental changes to the 802.11 security architecture, nor does it introduce new features that require significant changes in your existing network security systems. Any network security devices in place for an existing wireless LAN will continue to work after an upgrade to 802.11ac unless they need to access the wireless medium directly. The biggest change to network security in 802.11ac might be based on the equipment you choose to use for 802.11ac—i.e., you might want to install equipment that offers new per-user capabilities that your previous network equipment did not.

Link-layer encryption

802.11ac does not support the use of anything other than AES-based encryption (CCMP and GCMP) to protect data frames.[40] To take advantage of the fast data rates in 802.11ac, you will have to retire any TKIP-based networks. Many 802.11ac devices will continue to support TKIP for client operations, but when doing so will limit transmission rates to pre-802.11ac data rates. To lift the cap on network capacity, you will need to convert the network over to a new encryption method.

Many 802.11ac devices will support TKIP, but will only do so with older performance-limiting 802.11a/b/g rates.

One method of transitioning away from TKIP is to run parallel networks on the same infrastructure by duplicating an existing TKIP network on newer APs. By monitoring the usage of the TKIP network, it is possible to determine when enough older devices have been retired and the TKIP-compatible network may be decommissioned. As an

alternative to parallel networks, both encryption protocols can be run simultaneously on the same SSID, which is sometimes called *mixed-mode operation*. In a mixed-mode network, the encryption method must be supported by all clients—in this case, this means the lowest common security denominator of TKIP will be used, which will limit performance, especially for applications that make extensive use of broadcast and multicast traffic.

Fast roaming

Real-time applications such as voice and videoconferencing require uninterrupted access to the radio medium, even when moving between APs. Therefore, the ability to move connections rapidly between APs is critical for real-time applications such as voice and videoconferencing. When security must be included as part of the handoff between APs, there are two major implementation paths. Opportunistic Key Caching (OKC) moves the master key between APs and is widely available in network equipment. The 802.11r specification also provides a guaranteed fast transition capability and is the foundation of the Wi-Fi Alliance's Voice-Enterprise certification program.

Management frame protection

In 2009, the 802.11 working group ratified 802.11w, a standard for the protection of management frames. Unicast management frames are protected with CCMP and encrypted to prevent eavesdropping, while broadcast management frames are authenticated with the Broadcast/Multicast Integrity Protocol (BIP). 802.11ac has no mandates regarding management frame protection, but it is likely that the initial 802.11ac products will be some of the first available products with management frame protection. Therefore, you should consider whether to use management frame protection on your network. Management frame protection can be operated in one of two modes:

Management frame protection capable

> In this mode, an AP will advertise that it can protect management frames. If a client that supports management frame protection attaches to the network, the AP will encrypt management traffic to it.

Management frame protection required

> In this mode, an AP advertises not only that it can protect management frames, but also that clients must support the capability to use the network. If a client is unable to support management frame protection, it will not be allowed to connect to the network.

Management frame protection is potentially a worthwhile capability if you are using devices that make extensive use of management frames, such as devices that support the Wi-Fi Alliance's Voice-Enterprise certification.

Authentication

802.11ac made no changes to the 802.1X authentication framework. Any user authentication system that works with 802.11a/b/g/n networks will also work with an 802.11ac network.[41] EAP-based authentication is designed to work on top of many different physical layers, and therefore it does not require any changes when moving to 802.11ac. Connections between the wireless network and the user account system should not need to be redesigned.

Additional Planning Considerations

Wireless networks do not have many vendor-independent management tools and protocols. An important part of planning a network and evaluating equipment is to assess the vendor management tools that are typically tightly integrated with the APs. Management tools typically perform both configuration management and ongoing monitoring.

To develop a way of assessing products, it will help to devise usage scenarios for what the network must support. Almost universally, a wireless network needs to support employee access as well as guest access. Commonly, employee access will be differentiated in some fashion, such as by user role or device type. Contractors and consultants may be given even more restricted access.

Guest management

Wireless networks are so useful that they often are key infrastructure for additional services offered by the IT team. One of the most notable examples is guest services, which may be composed of guest registration, authentication, and billing, or some subset of the three. Now that mobile devices almost universally use wireless LANs to access the network, wireless LAN deployments are often used to provide guest access to visitors. An adjunct to many wireless LAN deployments is a guest management system that is used to manage accounts for visitors.

Guest management systems have recently taken on a related role as a differentiator between corporate-owned devices and employee-owned devices. Enthusiasm for bring-your-own-device (BYOD) programs is based on the productivity increases that flow from putting information quite literally in the hands of users. Designing a technical architecture for a BYOD program is a book topic in itself; one of the core technical problems that must be solved is finding a way to distinguish corporate-owned devices from employee- or visitor-owned devices so that different policies can be applied to these sets of devices. In addition to flexible security models and policies, a BYOD program may require building a network that requires a significantly higher level of service due to increases in device density.

Intrusion detection

Wireless intrusion detection systems were once considered a standard part of the network administrator's toolkit, due to the relatively weak security mechanisms available to wireless LAN devices in the era before 2003. The improved cryptographic capabilities available for both data protection and management frame security have mitigated known attacks, and most wireless LAN system vendors have moved to integrate containment capabilities into their product lines by controlling the wired network.

802.11ac Radio Planning

With planning complete, it's time to pick out equipment to build the network. Developing solid requirements, as outlined in the previous section, is an important step in understanding what the network needs to do. Many of those requirements can be translated into a tentative plan that helps guide selection of hardware. Good project management practices are somewhat iterative. Begin with a rough estimate of your network requirements, and short-list vendors that can help meet your requirements. Bring in demonstration equipment to prove out the basic design, and gather information to refine your rough estimate. Above all, don't be afraid to put some load on your network as you are proving the concepts.

Available Radio Channels

802.11ac uses the 5 GHz spectrum exclusively, and at the time this book went to press, it had 22 available 20 MHz channels for use. In deployment practice, 14 of those channels require the use of Dynamic Frequency Selection (DFS) to protect radar operations. At an 80 MHz channel width, however, the number of available channels

shrinks to just five, and three of those five channels require DFS support. Although the number of channels is reduced substantially, five channels is still sufficient to provide channel separation in almost any area that will see a wireless LAN deployment. Once the proposed spectrum expansion described in Chapter 2 is finalized, four more 80 MHz channels will be added.

Coverage and Capacity Estimates

An important step in the planning process is to estimate the number and type of APs that you will need to build your network. The AP count can be estimated for a network that provides basic coverage, or it can be estimated based on the capacity or transaction requirements identified for the network. Both types of estimates are important, especially for dense networks that have significant numbers of hot spots with high user density. "Coverage-oriented" networks provide basic connectivity for a low density of devices and can be built successfully without advanced features. Increasingly, however, networks are being built around capacity, and 802.11ac is the core technology that will enable the next generation of "capacity-oriented" networks. If you are not building a network around high capacity, you probably do not need 802.11ac. Table 5-5 is a basic comparison of the two approaches to building a network.

Table 5-5. Network characteristics

Attribute	Low-density network	High-density network
Number of clients supported per AP	Low	High
Typical distance between APs	Higher	Lower
Floor area covered by an AP	5,000 square feet (500 square meters) or more	2,000–3,000 square feet (200–300 square meters)
802.11 physical layer type	802.11n	802.11ac
Typical signal strength and signal-to-noise ratio in AP handoff area	–80 dBm (about 20 dB SNR)	–67 dBm or higher (about 33 dB SNR)
Radio design	Optimized for area of coverage	Optimized for throughput per unit of coverage area
Target frequency band	2.4 GHz (sometimes 5 GHz)	5 GHz
Load balancing/band steering	Not needed due to common lack of dual-band client devices	Required
Quality of service	Not needed	Required
Application mix	Light usage of best effort data	Voice and/or video are present

Even within a single network, both approaches may be used depending on the area. When planning out a network, designers will need to mix the two approaches to make it successful. Stairwells and hallways are often areas where users need connectivity while in transit, but the user density and application demands of the typical stairwell are quite small compared to those of conference rooms, auditoriums, and office space. In such sparsely used areas, it is acceptable to design for lower capacity and a more moderate signal quality, perhaps even using less expensive 802.11n access points.

Turning the raw data of network devices and applications into a running network requires combining the data on network goals with your knowledge of the physical space. To do so, run through a checklist like the following:

1. Get plans for the area the wireless LAN needs to cover. Many buildings have blueprints available as computer-aided drafting (CAD) files, but CAD-based processing is overkill in most cases. When you get the building plans, make sure that either they are to scale, or the planning tool you are using allows scaling of the drawings. For drawings that do not have a scale, it is possible to get a rough scale by labeling a doorway as 3 feet (1 meter) wide, or by taking the external dimensions of the building.

2. Divide up the physical space into areas of differing capacity based on your judgment of expected usage of the network. In corporate environments, areas where high capacity should drive the layout include conference rooms, offices, and cubicles. In educational settings, capacity drivers include classrooms and lecture halls. In hospitals, areas where wireless LANs support critical care drive capacity, especially when used with high-capacity applications like imaging. Be sure to account for the types of clients in use in each area, and include plans for growth. As your clients transition from one- and two-stream 802.11n clients to 802.11ac clients, the demands on the network will grow.

   If you're expecting to support significant usage, be sure to have usage estimates to match. Do not be afraid of building too much coverage at this point—it is usually harder to expand a network than to cut it back.

3. Estimate your capacity and coverage needs. For each capacity area in your plan, the estimate requires multiple calculations. When planning networks, I use several metrics to come up with an AP count and draw upon my own experience in blending them or choosing between them. Most importantly, for a high-capacity area, ensure that the 5 GHz band coverage is sufficient. For maximum throughput, neighboring APs should not be located on the same channel and should be located as far as possible from adjacent channels.[42] 802.11ac is only supported in the 5 GHz band in large part because of these advantages. To estimate 5 GHz coverage, you can use a planning toolset to design coverage with at least a 30 dB SNR. Or, if you know you know the noise floor within your environment, you can design the coverage around a signal strength based on that SNR. In some cases, the manufacturers of devices that you are targeting for support can supply design criteria. Many voice device vendors, for example, will suggest that a network be designed around a signal strength of –67 dBm.

   Another estimate of capacity is based on rough back-of-the-envelope calculations of airtime. As described in "Application Planning", you can get an extremely rough estimate of the amount of airtime a device will need by comparing its total TCP throughput to the application requirements. With a guess at the number of clients and the airtime consumption of each, you can derive an estimate of the number of APs required.

   For example, if there are 30 tablets in a classroom and each tablet requires 4% of the available airtime, then two radios are required.[43]

   To get more precise estimates of your AP capacity requirements, more accurate test tools are available. Traffic generators can be programmed with either simulated applications or application profiles, then installed and run on test devices to simulate your deployment. In deployments with extensive tablet usage, be sure to run the traffic generator on a tablet because it is a single-stream device, often with an antenna system of average performance. Verifying performance for older physical layers (802.11a and 802.11n) may also be important for networks that need to support large numbers of older devices.

4. For each area that has been estimated separately, add together each area's AP count to come up with a total.

As a hard-won piece of practical knowledge, I have found that in most networks that support general office work and do not have special demands for high throughput, a standard dual-radio AP can cover about 3,000 square feet. The per-AP coverage area has hovered around 3,000 square feet since the days when 802.11b devices transmitting at 11 Mbps were considered state of the art. As wireless LAN capacity has increased, users have moved more applications onto the wireless LAN and begun to demand much higher quality service.

Initial 802.11ac AP mounting locations

Cabling is one of the biggest costs in placing APs, and the approach to determining where to put 802.11ac APs will depend on the extent to which there is existing cabling infrastructure available to support the network. Reusing an existing cable plant will save a substantial amount of money because the cost of labor for cabling installation can be roughly comparable to the cost of the access points themselves.

If 802.11ac is replacing an existing network based on earlier technology (802.11a/b/g/n), start by reusing existing cabling and surveying the area to measure coverage. If the signal quality is sufficient the existing mounting locations should be acceptable, although a few additional APs may be required to boost capacity in "hot spots" where the highest data rates are required. One factor to watch out for when swapping out older APs for 802.11ac APs is that if the network is very old and was designed around 2.4 GHz coverage, the shorter range of 5 GHz coverage may not be sufficient to provide the desired connectivity.

APs are cheap, and staff time is expensive. Usually, it will be more cost-effective to replace existing APs in their current locations and add further capacity if necessary than to take the time to deliberately re-survey a location for a new 802.11 standard.

If, on the other hand, you are building a wireless network for the first time, the initial mounting locations should be computed with some form of planning software. Many product vendors will assist in the determination of AP locations as part of a project bid process, often by using wireless LAN planning tools. If you use software to perform a "virtual" site survey, keep in mind that there is no substitute for performing either a manual survey with an AP powered on and measured manually by a target client device, or a rigorous post-deployment survey to validate the estimates produced by the planning software. When using software tools, keep in mind that many basic tools lack the ability to specify user or device density, so be ready to modify the results of a simulated site survey to adjust them to your environmental expectations. For example, some tools will attempt to provide high-quality coverage throughout a designated coverage area, and it is up to you to move coverage from sparsely used areas such as hallways and stairwells into the real target usage areas, such as conference rooms and classrooms.

An upgrade to 802.11ac is also an ideal time to add capacity if needed. One of the ways in which 802.11ac increases speed is the new 256-QAM modulation, but 256-QAM requires high signal-to-noise ratios. 256-QAM will not work through a wall, so if one of the objectives of your deployment is to increase the peak throughput available, it may be necessary to consider putting APs within line of sight of every place that clients may gather. Planning tools can often estimate the effects of installing additional APs for capacity purposes, and may help with setting transmit power levels.

5 GHz coverage and 802.11ac-only APs

802.11ac accentuates the difference in radio range between the 2.4 GHz band and the 5 GHz band. A good rule of thumb is that the range of a radio is inversely proportional to the square of its operating frequency.[44] Physical layers at 5 GHz will naturally have a much shorter range than at 2.4 GHz. In a network designed for 802.11ac capacity, generally the APs will be placed where they are needed for 5 GHz coverage. In a network designed for 802.11ac capacity, the network will be quite dense because of the high SNR requirements to support the 256-QAM rates (MCS 8 and 9). As a result, there are likely to be places in your network where a dual-radio device does not make sense. Figure 5-1 illustrates one example of this. Four APs are used to provide high-quality 802.11ac coverage. However, due to the longer usable range of 2.4 GHz radio signals, even when turning the power down, three APs are sufficient to provide coverage at 2.4 GHz. One of the APs does not need to activate its 2.4 GHz radio.

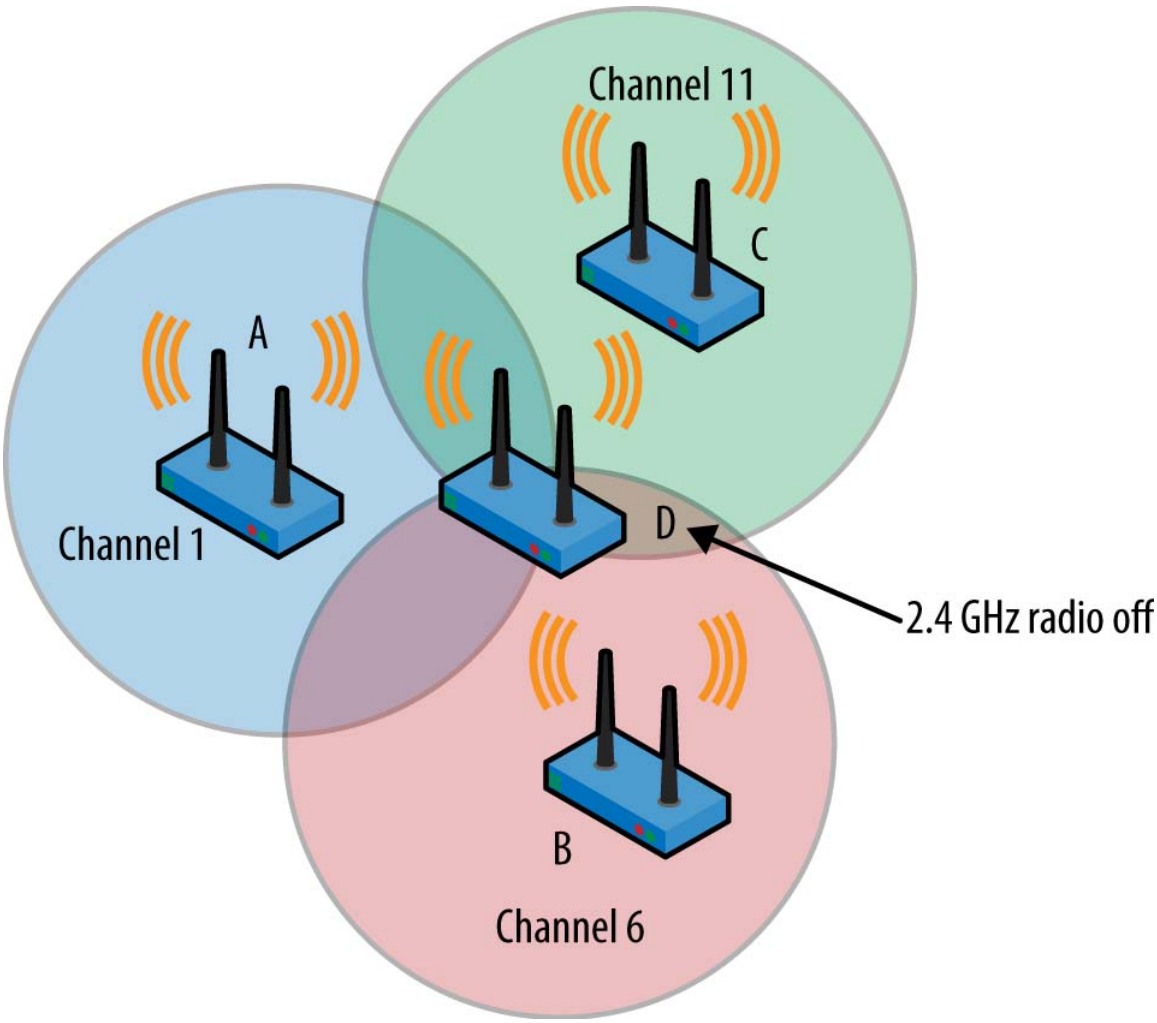

Figure 5-1. 2.4 GHz coverage completeness

A common method of adding 802.11ac capacity to an existing network is to add an 802.11ac radio to a place in space where 5 GHz coverage needs improvement. Such "infill" APs need only be 5 GHz–capable, but should come from the same vendor as the dual-radio devices already used on your network to ensure that the roaming, band steering, and load-balancing capabilities work with the rest of the network. With 802.11ac having much shorter range, the capacity-enhancing infill AP is likely going to be an increasingly large component of your network architecture. If the newly added AP has dual radios, the 2.4 GHz radio can be used as a full-time sensor. Applications for sensors are varied, but they include full-time wireless security sensors and dedicated spectrum monitors. Some vendors can use such radios as client devices to test actual performance.

Equipment Selection

With an estimate of the number of APs and their tentative initial locations, it is time to start picking out an actual implementation, rather than working with generic APs. At a high level, APs connect the free-flowing wireless world with the high-performance, fixed-in-place wired world. After reviewing your network requirements and determining what constraints drive the logical architecture, it's time to pick out your access point hardware. Access points all perform the same basic function in that they shuttle frames between radio networks and Ethernet LANs, but there can be tremendous differences in cost and functionality. Comparing access points on the basis of price alone may prevent you from discovering a critical feature that improves your ability to manage and run the network. If you're building a network of more than just a handful of access points, you probably want to look beyond the hardware available at electronics stores and at highly functional APs. Here are some things you may want to consider:

Wi-Fi Alliance interoperability certification

> In June 2013, the Wi-Fi Alliance launched an interoperability program for 802.11ac. Ensuring that your product vendor has successfully passed interoperability testing is not an absolute guarantee of interoperability, but it is a strong statement that the manufacturer believes in interoperability and has taken steps to ensure compatibility with a wide variety of client devices. To check on the certification status of a product, visit the Wi-Fi Alliance website and click on the "Wi-Fi CERTIFIED Products" button on the lefthand side of the page.

High performance

> Performance is not just a matter of the rate at which products push data. Many products are capable of pushing "air rate" data speeds, but only corporate-grade APs have "air rate" performance while providing a sophisticated feature set under heavy load. As with many other areas of networking technology, vendors of corporate-grade hardware invest much more heavily in software tuning because their products are used in deployments where more than just the number of bits per second matters. This investment pays dividends in providing high data rates at longer ranges from the AP with higher numbers of active client devices.

Hardware quality and robustness

> Corporate-grade devices are designed to be used for many years before replacement, and therefore are often designed with future expandability in mind. Components are selected with a view toward quality and long life, instead of basing decisions primarily on cost. Sophisticated antennas or other radio frontend components may be used to improve the quality of the network, either in terms of throughput or coverage. Radios will be enabled on all available channels, even though the cost of regulatory compliance before using DFS channels can be substantial, and software supports automatic configuration of radio channel selection. Some deployment areas may require specialized hardware designs due to either very high or very low operating temperatures.

Software functionality, upgradability, and quality

> Generally speaking, more expensive devices have significantly more functionality, with advanced features in several areas. Vendors regularly plan for the release of such features, and it is common for new features to be provided midway through a product's life cycle. Understanding the future functionality that might be delivered and whether your deployment would benefit from planned features allows you to consider new features appropriately in the decision process. Additionally, extensive QA testing is used to ensure that corporate-grade devices can be run for months at a time under heavy loads.

Antenna options

> Internal antennas allow an AP to be self-contained and to blend smoothly into the aesthetic environment. External antennas typically have higher gain, which improves range. In a deployment based on area of coverage instead of density, or a deployment in a challenging radio environment, selecting the right external antenna can make the difference between a poor-quality network and a successful one. External antennas are also frequently used for outdoor deployments. Picking the right external antenna is still something of an art, and the antenna must be matched to the performance characteristics of the AP. A high-gain antenna will dramatically increase the transmit range of an AP, but if the AP has low receive sensitivity, the high-gain antenna will cause more problems than it solves.[45] Product manufacturers are responsible for obtaining regulatory authorization for each type of external antenna used, so a larger selection of external antennas indicates more extensive regulatory testing.

Power options

> Consumer-grade devices are typically powered with a "wall wart" transformer and must be installed close to existing electrical outlets, while corporate-grade devices can draw power from the device at the other end of the Ethernet cable. Power over Ethernet enables placement of devices in out-of-the way locations, and can be used to provide power even on very high ceilings.

Security

> Security is not just about providing solid encryption, though that is the obvious starting point. Corporate-grade products offer flexible authentication through RADIUS and directory interfaces, per-user VLAN mapping, traffic filtering and queuing, and built-in captive web portals for web-based authentication. Fast roaming support extends the basic encryption to support mobile applications.

Quality of service

> At the most basic level, quality of service support involves compliance with the Wi-Fi Multimedia (WMM) certification requirements, which divides traffic on the air into four classes of differing priority. More complex queuing systems can be used to improve service quality for voice devices, or to ensure that airtime is balanced fairly between network users.

Manageability

> If you are reading this book, you need centralized management. Evaluate management tools for a wireless network in the same way you evaluate management tools for a wired network. Ensure that the management software provides something beyond simple configuration management and can report on the overall state of the network.

Network Architecture for 802.11ac

Throughout the evolution of wireless LAN technology, there have been a number of approaches to adding the wireless LAN access layer onto an existing wired backbone network. Most approaches share two fundamental attributes, and they remain unchanged by 802.11ac. Fundamentally, 802.11 provides MAC-layer (or, after the OSI

nomenclature, “layer 2”) mobility. As an 802.11 station moves throughout the coverage area of the network, from the perspective of the routing and switching infrastructure it remains in a fixed spot. All commercially available products that support large-scale networks have extended the fundamental MAC-layer mobility to encompass the entire network, sometimes even going so far as to make a single subnet available in many different locations with VPN technology. Additionally, ever since the 2006 introduction of WPA2, the 802.1X security framework (sometimes also called “WPA2-Enterprise” after the Wi-Fi Alliance certification program) has provided strong authentication and transparent encryption to client devices. The 802.1X framework offers network administrators the capability of designing network authentication around user-specific policies, often assigning a bundle of access rights (variously called a “profile” or a “role”) to users upon connection to the network.

Many network administrators are familiar with the concept of protocol layering and the Open Systems Interconnection (OSI) model. Network protocols are often classified by where they fit in the OSI model. Less well known, but just as important, is the separation of network technologies into *planes*, as shown in the depth dimension of Figure 5-2. Each plane has its own protocol layers, of course, but each plane also has a specialized purpose. Common planes include the following:

Data plane (sometimes called the “forwarding plane”)

> Protocols in the data plane move bits from one location to another and are concerned with moving frames from input interfaces to output interfaces. In an IP network, the main data plane protocols are TCP and IP, with applications such as HTTP riding on top of the network and transport layers.

Management plane

> The management plane provides protocols that allow network administrators to configure and monitor network elements. In an IP network, SNMP is a protocol in the management plane. A vendor’s configuration application would also reside in the management plane; wireless LANs may use CAPWAP as a transport protocol in the management plane. Without exception, large-scale IP networks use centralized management and thus have a centralized management plane. The management plane of the network is responsible for planning and implementation, policy definition, and ongoing monitoring.

Control plane

> The control plane helps make the network operate smoothly by changing the behavior of the data plane. An IP network uses routing protocols for control, while switched networks use the spanning tree protocol. The control plane of a wireless LAN is responsible for ensuring mobility between access points, coordinating radio channel selection, and authenticating users, among other tasks. The control plane is also responsible for enforcing policy.

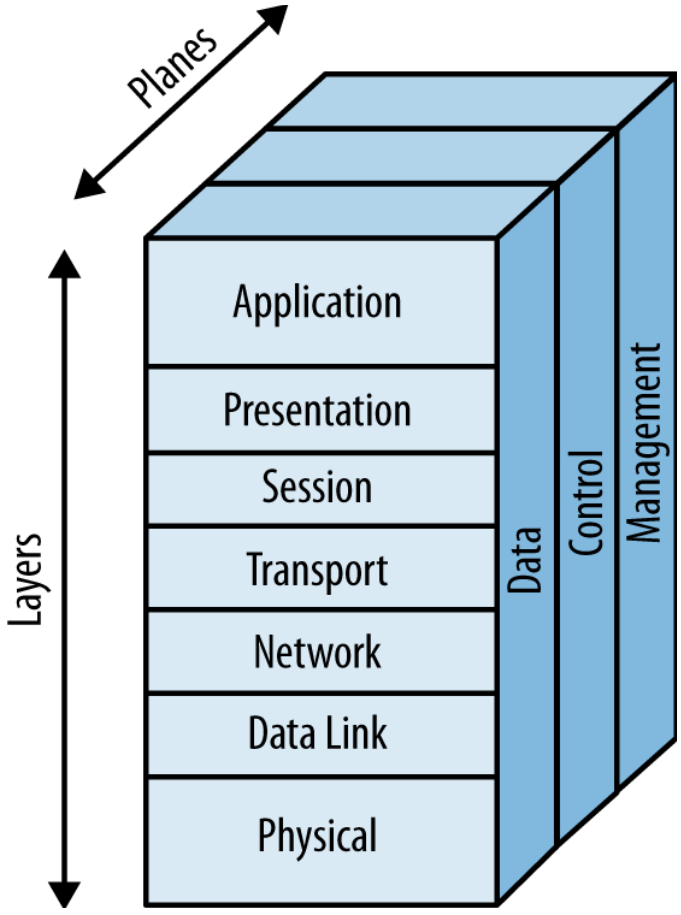

Figure 5-2. Network protocol architecture: layers and planes

Wireless networks can be classified based on the location of the control plane, and much of the development across the history of wireless LANs has been about refinements to the control plane. Early wireless LANs were built out of completely independent APs. The management plane was practically nonexistent (consisting of the APs’ serial ports and, in a highly engineered network, perhaps a terminal server), and the control plane was not unified. Networks based on autonomous APs did not automatically select channels and did not always support smooth handoff between APs without proprietary protocol extensions at both ends of the link.

The development of wireless LAN controllers a decade ago led to a redesign in the way that networks were built, with the control and management planes being centralized in this new piece of the network. In a typical controller-based deployment, the access points have limited functionality without a connection to the controller. Authenticating and authorizing users is handled by the controller, as are algorithms that provide RF management functions such as channel selection. Centralized management and control made much larger networks possible, and essentially, nearly every large-scale network built prior to the emergence of 802.11n was built using a controller-based architecture. In addition to the control and management planes, early controller-based network architectures centralized the data plane as well. All data from APs was forwarded through the controller; this is often referred to as a *network overlay* because the wireless network was separate from the existing core network and

existed as a layer on top of the existing core. In effect, the controller took on the role of a distribution switch for users attached to APs and provided mobility by serving as an anchor for the logical point of attachment. Early applications of wireless LANs were driven by application-specific traffic, not general-purpose user access, which made the overlay model acceptable to network administrators.

With the emergence of higher-speed wireless network technologies, there was a shift in how wireless LANs were used: rather than simply being small one-off deployments to automate processes, they became general-purpose access methods. Add-on PC cards were replaced by 802.11 interfaces integrated into the motherboard. With the standardization of 802.11n and 802.11ac traffic volumes have increased dramatically, due to both the higher speeds and the increase in the number of wireless devices attached to a typical network. As network load increased, centralized forwarding through controllers became a traffic bottleneck. Many vendors responded to the bottleneck by moving the forwarding decision out of the controller and back to the AP at the edge of the network, an approach often referred to as *distributed forwarding* because the data plane function has moved from the controller out to the AP, and, in fact, back to a parallel location with wired traffic. Although this architecture looks superficially similar to autonomous APs, it is typically paired with centralized management. Increased processing power also made varying control plane implementations possible, enabling distributed AP architectures to handle typical control functions by working among themselves.

Architecture comparison

Building a "micro-network" of an AP or two is easy. With a small number of APs, it is acceptable to manage the APs individually. Upgrading to 802.11ac is also straightforward: take out your existing 802.11a/b/g/n APs and replace them with 802.11ac APs. At such a small scale, almost anything will work. At some point, however, the overhead of managing individual devices will be too great. At this point, you are building a small- or medium-sized network. These networks have just as much to gain from 802.11ac.

Prior to the introduction of distributed APs, most networks needed a centralized control plane to handle the loads imposed by large numbers of users, and the choice between autonomous APs and controller-based APs was a straightforward one that was almost always resolved in favor of the more advanced centralized control plane. With the explosion of 802.11 devices now available, network architects have designed higher and higher capacity networks, stressing the centralized control plane. Early controller-based networks were able to use a single controller as the focal point for both the control and the data plane, but that assumption no longer holds.

Table 5-6 compares the three basic types of APs described in this section. In reality, there is some overlap between these architectures when they are implemented in products. It is likely that a large-scale network at any speed—especially one supporting critical applications—will require some degree of decentralization, either by moving some of the data plane functions to the edge of the network, moving some of the control plane functions to the edge of the network, or both. All three architectures are capable of supporting any set of network requirements, but the cost and availability of the resulting network may vary.

Table 5-6. Architecture comparison

Attribute	Autonomous APs	Controller-based APs	Distributed APs
Location of data plane	Distributed, enabling high network performance.	Centralized, potentially limiting performance to the forwarding capacity of a controller. Good mobility support because devices attach through the controller.	Distributed, enabling high network performance. Many products have features to assist with mobility.
Location of management plane	Depends on product; often distributed, imposing very high staff costs.	Centralized, lowering operational expenses.	Depends on product; often centralized, enabling lower operational expenses.
Location of control plane	Distributed, if it exists. Nonexistent control plane limits flexibility of security and radio management.	Centralized, with high functionality for radio management and user management.	Distributed. Functionality of control plane depends on vendor implementation.

Selecting a network architecture

Management plane

If you are building a network consisting of more than a handful of APs, there is no consideration. Centralized management is a must, if only because maintaining consistent policy configuration across multiple devices is easier when you can change network-wide policies and apply them to devices from a central location, similar to the way that centralized management tools for wired networks allow policies to affect the configuration on many devices. Some early wireless LAN products lacked centralized management, but these were quickly replaced by products that could be used with a centralized management system. Many flavors of centralized management exist, with wide variations in functionality and cost. Even though centralized management was formerly only accessible to large-scale networks, the emergence of the software-as-a-service "rental" model may offer you the ability to use a full-featured management system at an affordable cost for a small network.

Centralized management is nonnegotiable beyond just a few access points.

Data plane

The forwarding plane of wireless networks has been the subject of significant developments over the past five years. When 802.11 first reached the market, it was comparatively slow. Using the centralized forwarding path in Figure 5-3 did not impose a significant penalty on the network because wireless LAN speeds were slow enough for the choke point to keep up. When most 802.11 packets needed nearly 200 microseconds of preamble to begin transmission, the extra latency of a trip across the network core was barely noticeable. As the speed of 802.11 has increased, though, it has become harder and harder for the centralized forwarding point to keep up.

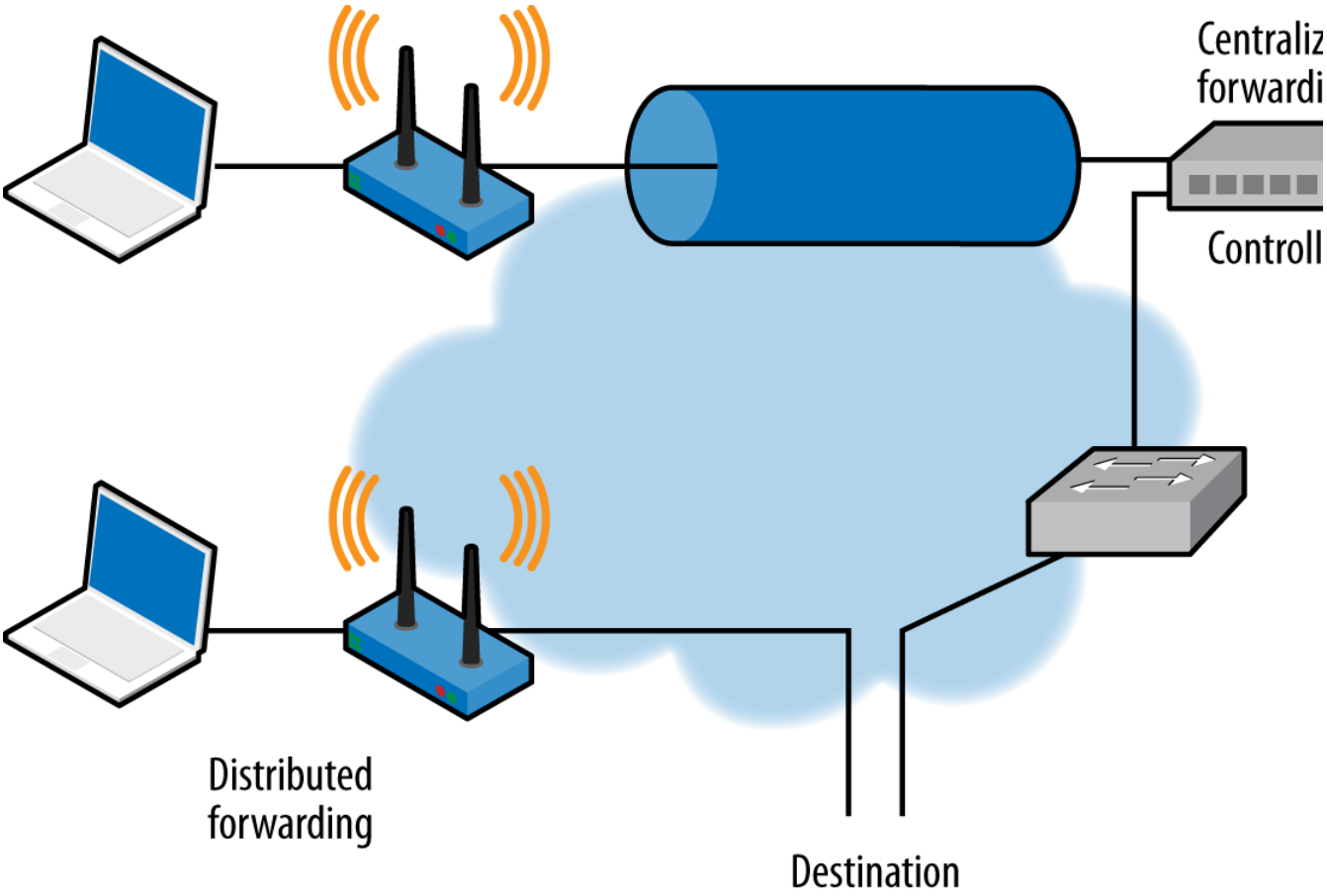

Figure 5-3. Types of forwarding paths

In practice, there is not a sharp divide between products on the market that offer a centralized forwarding path and those that offer a direct forwarding path at the access point. When controllers are used, the resulting networks may offer the choice of sending traffic either through the centralized forwarding point or directly from the AP at the network edge. As speeds have increased, the ability to offload data forwarding to the edge of the network has helped keep controllers from becoming bottlenecks on their networks. At the other end of the spectrum, APs that are generally used in distributed forwarding deployments typically offer the ability to make any VLAN accessible throughout the network by using an AP-to-AP tunnel.

The increased speeds of 802.11ac make AP-level forwarding much more attractive, especially when combined with the potential of multi-user MIMO to dramatically increase data traffic in the future.

Tunnels through the network, whether between an AP and controller or between APs, must be constructed in a way that is compatible with existing restrictions on frame size. Client devices will generally send and receive maximum-length Ethernet frames of 1,500 bytes (though they may of course use 802.11 protocol features to aggregate several of these frames together). Transporting a maximum-length Ethernet frame across an intermediate network requires either that the network support larger frames or that the tunneling protocol manage fragmentation of the client data frame plus a tunnel header.

Control plane

In a wireless LAN, the control plane maintains the logical network attachment of the client, which includes its security information, the state of any user access rights or service quality guarantees, as well as path information on how the wireless network enables data to reach the client. The control plane also manages coordination between APs for tasks such as radio management and providing network-wide quality of service. Control plane design is one of the most fertile grounds for experimentation in wireless LAN design. The location of the control plane makes an important contribution to the overall reliability and resiliency of the network. Building fully redundant wireless networks requires both resilient data forwarding and resilient control capabilities.

Most large-scale networks were originally built on centralized control plane technologies, which required that APs be in continuous contact with a control point. Many centralized control planes are now moving toward either a split control plane (where functions are shared between the controller and APs) or a more fully distributed control plane. Distributed control planes can be cheaper, especially when designing for distributed networks with many remote sites. Neither the distributed nor the centralized type of control plane is inherently more resilient; a distributed control plane protocol can be resilient by design, while a centralized control plane may require spare controllers.

Carefully evaluate the trade-offs between a centralized versus a distributed control plane from the perspectives of functionality, reliability, and cost.

Hardware Considerations

The Wi-Fi Alliance is an industry association of companies that collectively drive the development of wireless LAN technology. The Alliance is best known for the Wi-Fi CERTIFIED interoperability testing program that began in 2000. When development begins on new physical layer technologies such as 802.11ac, the Wi-Fi Alliance has a certification program to ensure that these emerging technologies are built with interoperability available from the first version. Once testing is complete and a product is awarded certification, it can be looked up at the Wi-Fi Alliance certified product listing. Each product is also given an *interoperability certificate* that details the individual product features that have been certified.[46]

Mandatory tests

Every device submitted for 802.11ac certification must pass a series of basic tests. The features that are expected to be supported include:

5 GHz operation

> 802.11ac is a 5 GHz–only specification. All tests in the Wi-Fi Alliance certification program require operation at 5 GHz. This is in contrast to the 802.11n Wi-Fi Alliance certification program, in which 5 GHz capabilities were optional.

Channel width of 20, 40, and 80 MHz

> The initial version of the 802.11ac certification requires support of all the available channel widths up to 80 MHz. Again, this is in contrast to the Wi-Fi Alliance's 802.11n certification program, which covered only 20 MHz and 40 MHz channels (with 40 MHz channels being optional).

Dynamic bandwidth signaling

> In addition to requiring support of multiple channel widths, the 802.11ac certification test plan requires demonstrated interoperability for the dynamic bandwidth signaling protocol features described in "Dynamic Bandwidth Operation (RTS/CTS)".

Support of MCS 0 through 7 (up to 64-QAM)

> Modulation of up to 64-QAM is required of all devices seeking 802.11ac certification.

Minimum number of spatial streams

> APs must support at least two streams before being allowed to claim 802.11ac certification; no such rule applies to client devices. There is an exception for "mobile APs," which are battery-powered devices like the Novotel Mi-Fi. Battery-powered APs are allowed to implement only a single spatial stream. The number of tested spatial streams is likely to be placed on the interoperability certificate.

A-MPDU reception

> Any Wi-Fi CERTIFIED 802.11ac device must be able to receive A-MPDU frames. A-MPDU support is typically provided within the radio chip itself, so support for this option is widespread. Devices under test are allowed to self-describe the A-MPDU size supported, so it is impossible to determine the density of back-to-back MPDUs supported.

A-MSDU reception

> In addition to A-MPDU aggregation, to receive certification devices must support A-MSDU reception.

Security: TKIP & WEP negative tests

> 802.11ac devices may not use TKIP or WEP to protect frames sent at 802.11ac data rates. The certification program includes "negative tests," which are tests to ensure that WEP and TKIP cannot be used with 802.11ac data rates. Many products implement data rate limits when WEP or TKIP is configured, so that if an 802.11ac network is configured for TKIP, its components will avoid using data rates higher than 54 Mbps.

Optional tests

In addition to the mandatory tests described in the previous section, the certification program includes a number of optional capabilities, each of which is called out on the interoperability certificate:

MCS 8 & 9 (256-QAM support)

> When the radio link has sufficient signal quality, products that implement 256-QAM can achieve throughput of 30% higher than the mandatory MCS rates.

Short guard interval at 80 MHz

> Short guard intervals boost throughput by about 10%, and their use is widely supported in chipsets. An optional short guard interval test was defined for use with 802.11n, and the 802.11ac certification extends that test to the wider 80 MHz channels.

Space-time block coding (STBC)

> STBC allows a signal to travel farther because it uses all of the MIMO signal processing gains to increase range. STBC was not widely implemented when it debuted with 802.11n, and remains optional with 802.11ac.

Transmission of A-MPDUs

> Support for sending A-MPDUs is optional. This is the only aggregation test; the certification testing does not validate A-MSDU behavior.

LDPC

> The low-density parity check adds a coding gain of about 2 dB. It is optional within the specification, but a valuable capability when used with 256-QAM to eke out as much performance as possible from the radio link.

Single-user (SU) transmit beamforming

> Single-user transmit beamforming offers a potential gain of about 3–5 dB.

Modular Access Point Design

Like 802.11n before it, 802.11ac comes with a "roadmap" and several phases to be passed through before full capability is delivered. Some vendors have delivered modular radios they refer to as "future-proof" because the radio modules can be upgraded. Unfortunately, for customers the effect of modular APs is that you purchase one AP for the price of two and a half APs, and typically get substandard performance as a bonus for spending the extra money.

When building a modular AP, designers start with a chassis that accepts upgraded radios. The chassis defines the system resources available for the life of the product. (As far as I know, no modular AP has been produced with an upgradable processor card like those used in switches and routers.) Designers must build in extra CPU and memory to provide enough power to accommodate later upgrades. As a buyer, you pay for more of an AP than you need at the start to get the extra resources now. Modular APs often cost 50% more than their fixed-configuration counterparts: you pay for extra system resources now to preserve the option of upgradeability down the road.

With luck, product designers have guessed correctly at system specifications. If the future generation of hardware turns out to be more capable and resources fall short, performance will be sluggish, or the vendor will need to eliminate features and deliver a subpar product. Over the lifetime of a modular AP, the state of the art will change enough to invalidate design assumptions. An AP chassis designed before the conception of emerging features will potentially have the resources to power an 802.11ac upgrade, but it will miss out on any features that became commonplace after the chassis was designed. Modular APs suffer from the same problem as other modular products—the performance is determined by the overall system, and making just one component better rarely results in the promised performance benefit.

Another drawback is that when you go to upgrade a modular AP, there is by definition only one seller. With vendor lock-in, the cost of the upgrade module may be equivalent to the cost of a new fixed-configuration AP, designed from the ground up for current demands. Frequently, purchasers of modular APs find that by the time they are ready to change modules, newer fixed-configuration APs cost less but offer greater functionality.

All this might be worth it if modular APs saved operational costs, but they do not. Installing modules often requires more work than changing a fixed-configuration AP because the modular AP needs to be unmounted, altered, and remounted. In some cases, a new mounting bracket is needed to ensure the new antennas in the upgraded module are aligned correctly. The staff cost for adding modules is usually at least as much, and probably more than, that of just replacing APs with newer models.

Building an 802.11ac Network

Building a network may begin with detailed information gathering to make a good prediction of the number and location of APs required, or it may be more iterative, where a few APs are used to "test the waters" with a deployment in a key gathering spot for users. In iterative deployments, using the management capabilities of the wireless LAN system you are evaluating is a good way to obtain feedback on your assumptions. Is the client mix what was expected? Are the supposed key applications the most commonly used applications?

Channel Selection

At first glance, 802.11ac's addition of yet another channel width would seem to complicate the configuration process because it means network designers must manage yet another parameter with backward compatibility implications. However, the design of 802.11ac's channel coexistence mechanisms provides a rough guideline to channel allocation. Because 802.11ac clients can measure the available bandwidth, an 802.11ac network can take up as much capacity as is available, and two 802.11ac networks sharing the same frequency space can share the wide channels.

Figure 5-4 shows how a network can be built with minimum channel overlap. For the purpose of the figure, each AP's frequency space is represented by a "stack" of bars, where the shortest bar is the primary 20 MHz channel, the next-longest bar is the primary 40 MHz channel, and the longest bar is the primary 80 MHz channel. When two APs share a channel, the relevant bar is blended between two colors.

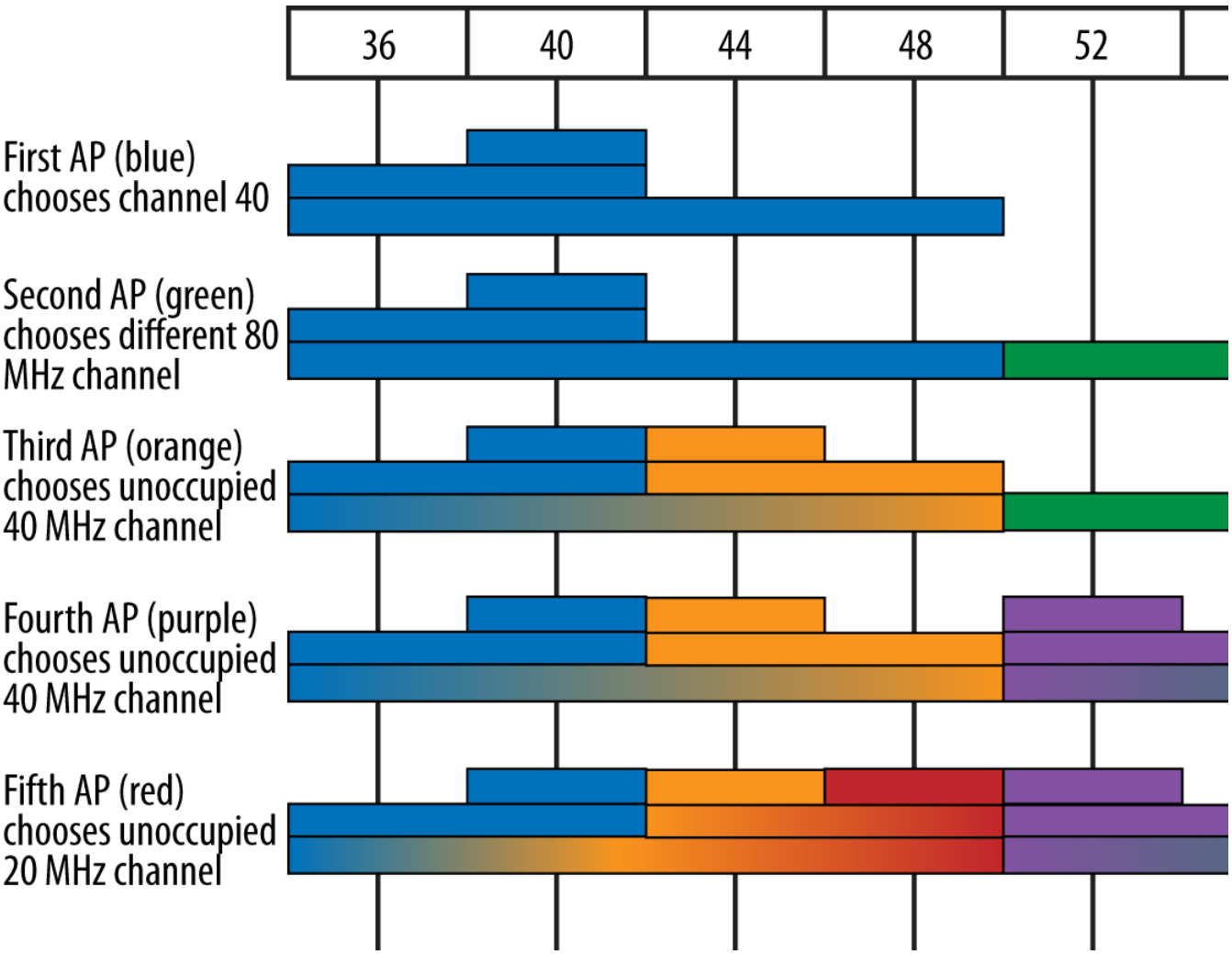

Figure 5-4. Channel addition algorithm for 802.11ac

The figure shows a network being brought up in the following steps:

1. When the first AP is powered up, it is straightforward. There is no existing network, and therefore the AP can choose any channel. In the figure, the AP represented by blue bars chooses channel 40. It will therefore take channel 40 for its 20 MHz transmissions, channels 36 and 40 for its 40 MHz transmissions, and channels 36 through 48 for its 80 MHz transmissions.

2. The second AP poses no problems, either. There is a free 80 MHz channel from channels 52 through 60, so the AP represented by green bars chooses, say, channel 60. (All four channels will choose the non-overlapping 80 MHz channel, so they are all equivalent.)

3. When the third AP, represented by orange bars, is added, it has no free 80 MHz channel. Therefore, it needs to choose a minimum-interference channel. Stepping down from the desired 80 MHz channel width, the orange AP can choose the 40 MHz channel of channels 44 and 48. The overlap between the orange and blue APs is shown by the way that the 80 MHz channel is blended between orange and blue.

4. The addition of the fourth AP, represented by purple, takes a similar path as the addition of the orange AP in the previous step. It has no free 80 MHz channel, so it must choose the least-overlapping 40 MHz channel. The only unoccupied 40 MHz channel is channels 52 and 56, so it chooses either of those two primary 20 MHz channels as its operating channel. The figure shows it choosing channel 56.

5. Finally, when the fifth AP (represented by the color red) comes up, it cannot choose an unoccupied 80 MHz channel or an unoccupied 40 MHz channel. Therefore, it must choose a free 20 MHz channel. In the figure, it is shown occupying channel 48. The 40 MHz channel composed of channels 40 and 48 is blended between orange and red to show that it is being shared between those two APs, and the 80 MHz channel is blended between blue, orange, and red to show that all three APs share the 80 MHz channel.

This process illustrates one important advantage of 802.11ac: supporting multiple channel widths at the same time enables 802.11ac clients to “burst” capacity when it's available. Network administrators should design their networks for minimum channel overlap for wide channels, and let the narrower transmissions fall where they must to accomplish that goal. Keeping the wide 80 MHz channels as free as possible will enable as many fast transmissions as possible from 80–MHz-capable clients and is a worthy goal.

When laying out a network, do not limit yourself to 20 MHz channels. Lay out the network using the widest channels possible and spread out the selected channels as much as possible.

Practically speaking, an extensive deployment of 40 or 80 MHz channels requires support for the worldwide harmonized radio band (channels 100 to 144 in Figure 2-3). Using these channels requires that the AP support Dynamic Frequency Selection. DFS capabilities are required by radio regulators in each individual country, and support is tested as part of the government certification process required to sell radio devices.

Network Tuning and Optimization

Part of monitoring the network is watching for conditions that will lead to substandard service, and, if possible, applying new configurations to network devices to improve performance and functionality. Fundamentally, the 802.11 MAC manages airtime. APs turn available airtime into bits sent to and from the network. Performance tuning in 802.11ac uses similar techniques to performance tuning in previous physical layers: reduce airtime contention whenever possible, and work to pack as many bits as possible into each available microsecond.

With its emphasis on technologies that assist in improving dense networks, 802.11ac APs will be packed together quite tightly. Reducing the coverage area of each AP is an important way of providing more radio capacity, but it is by no means the end of the story. Even though the 2.4 GHz band is not capable of supporting 802.11ac, it still has an important role to play as a source of capacity in busy networks. When serving areas with maximum density, enable *load-balancing* features in your wireless network equipment. Many products support multiple forms of load sharing to optimize network performance. Identifying 802.11ac clients, especially those capable of wide channel operations, and moving them to 802.11ac radios will be an important component of boosting network capacity. In high-capacity areas, multiple adjacent APs on nearby channels will need to share capacity.

Many manufacturers select default settings that are generally good for data networking and will deliver acceptable performance for web-based applications and email. In fact, many APs include a feature that gives priority to high-speed 802.11ac frames because they move data much more quickly than the older 802.11a/b/g/n frames. When transmitting a 1,500-byte Ethernet frame, 802.11ac is lightning-fast compared to its predecessors, especially if a wider channel is available for the transmission. Preferential treatment for fast 802.11ac frames has the apparent effect of speeding up the network for 802.11ac users with only minimal impact to users of older devices. The ability of a network to treat traffic differently to serve the overall user population is often called “airtime fairness” because when the throughput is optimized for the entire client population, the result is "fair.”

One important performance tuning technique that is no longer available to 802.11ac network administrators is control of data rates. In 802.11a/b/g/n, it was possible for network administrators to control which data rates were supported. To avoid devices falling back to airtime-hungry low data rates, network administrators often disable low data rates. Deactivating low rates often has another second desirable side effect in that it encourages devices to move off APs with marginal connections toward better APs. However, the 802.11ac protocol does not offer control of individual data rates. Devices must support all non-256-QAM data rates, and the only control offered by the protocol in the MAC capability information element (see “The VHT Capabilities Information element”) is over the 256-QAM rates.

The 802.11ac protocol does not provide the capability to control individual data rates. The only choices available in the protocol are supporting MCS 0–7, MCS 0–8, or MCS 0–9.

Voice

In contrast to data-oriented networks, some special configuration may be helpful for networks that support extensive amounts of voice traffic. Voice traffic is demanding because it cannot be buffered, so many of the efficiency enhancements in 802.11ac are not used by voice handsets. The core of voice tuning is reducing latency for as much traffic as possible. Here are some of the techniques that can be used:

QoS configuration: enable Wi-Fi Multi-Media (WMM) and priority queuing

> WMM is a quality-of-service specification that can dramatically improve the quality of voice at the receiver. Not all vendors turn on WMM by default, or even make voice the highest-priority traffic type. The single most important configuration change you can make to support higher-quality voice calls is to ensure that WMM is enabled. Some vendors also have an option for strict priority scheduling, which delivers frames in order to the receiver.

Enable admission control (WMM-AC)

> Admission control requires voice client devices to request capacity for a call before enabling the call to be established. For example, a voice handset using G.711 could request that the AP allocate 80 kbps of capacity. The AP is then free to accept the request and reserve capacity, or reject the request due to a lack of capacity.

Enable fast roaming

> Multiple techniques for fast roaming may be used, but the most common are opportunistic key caching (OKC) and 802.11r. Check with your voice client vendor to figure out which of them are supported.

Increase data rate used for Beacon frame transmission

Voice handsets are often very aggressive in roaming between APs, so tuning efforts will focus on decreasing the effective coverage area of APs and reducing large areas of coverage overlap. One of the most effective ways of limiting the effective range of an AP is to make its Beacon transmissions travel a shorter distance. While it is not possible to design a radio wave that stops at a certain distance, increasing the data rate of Beacon frames can be used to limit the effective range of the network. Typically, the Beacon rate will be set at a minimum of 24 Mbps, and sometimes even higher. (802.11a/g rates should be used because many voice handsets do not use 802.11n.)

Shorten DTIM interval

Many voice products use multicast frames for control features or push-to-talk (PTT) features. Multicast frames are held for transmission until the DTIM is transmitted.[47] Many APs will ship with a DTIM of 3, so multicast transmissions are delivered after every third Beacon. Setting the DTIM to 1 makes multicast delivery more frequent, at the cost of some battery life on handsets that need to power on after every Beacon to receive multicasts.

Reduce retry counters

Voice applications are highly sensitive to latency. 802.11 will automatically retry failed transmissions, but retransmissions take additional time. In voice transmission, frames should arrive on time or not at all. Using network capacity to retransmit frames after the target delivery time does not improve call quality, but it can delay other voice frames in the transmit queue. Somewhat counterintuitively, reducing the frame retry count can improve overall latency, and therefore voice quality.

Multicast

Multicast applications are often similar to voice applications in terms of the demands placed on the network. Multicast traffic streams are often video, and may not be easily buffered if they are real-time streams. Furthermore, multicast traffic has a lower effective quality of service than unicast traffic on a wireless LAN because multicast frames are not positively acknowledged. In a stream of unicast frames, each frame will be acknowledged and retransmitted if necessary. Multicast transmission has no such reliability mechanism within 802.11, so a stream of multicast frames may not be received and there is no protocol-level feedback mechanism to report packet loss. Here are some steps you can take to optimize multicast transmissions:

Shorten the DTIM interval

Just as with voice, many multicast applications depend on receiving data promptly. Setting the DTIM interval as low as possible improves the latency of multicast delivery.

Increase the data rate for multicast frames

By default, many products will select a low data rate, often 2 Mbps, for multicast transmissions in an effort to be backward compatible. While this is a laudable goal, and the choice of 2 Mbps was reasonable during the 802.11b-to-802.11g transition in 2004, low data rates for multicast no longer serve that goal. Unless there are critical applications running on 2 Mbps devices, or there are a large number of such old devices on the network without any upgrade path, you should increase the multicast data rate to reduce airtime contention. Many APs can automatically set the multicast data rate to the minimum data rate used for unicast frames to associated clients, or even the minimum unicast rate for clients in the multicast group. With 802.11ac, it is no longer possible to disable the low MCS rates, so the best that can be done is to disable the low data rates for previous physical layers.

Enable multicast-to-unicast conversion

Some APs implement a feature that converts a single multicast frame into a series of unicast frames. Multicast frames must be transmitted at a rate that can be decoded by all receivers and therefore is often relatively slow. Unicast frames can be transmitted much faster if the receivers are close to the AP. A series of positively acknowledged unicast frames may take approximately the same amount of airtime, but have significantly greater reliability.

Internet Group Management Protocol (IGMP) snooping

One of the best ways to limit the load imposed by multicast traffic is to ensure that it is not forwarded on to the radio link if no clients are listening. Many APs implement IGMP snooping, and even if your APs do not, IGMP snooping can be configured on the switched network connecting the APs. IGMP snooping monitors membership in multicast groups and only forwards multicast traffic if there are listeners to the stream.

Checklist

When planning a network, use the following checklist:

Client count, density, and mix

Gather information on the number of clients you expect to use the network, and, if possible, what their capabilities are. A good estimating rule is that an 802.11ac AP can serve around 30–60 clients with acceptable service, depending on the application. Identify peak data rates that each client will support.

Applications

Identify the key applications that must be supported on the network. Ensure that these applications are tested during any proof-of-concept demonstration and before the final acceptance testing of the new network. Application requirements may also be used to guide the planning process by working to estimate the number of APs needed and ensuring appropriate APs to serve high-density areas.

Backbone switching

Upgrade to gigabit Ethernet at the network edge to connect your APs, and make sure that the access layer has 10-gigabit uplinks into the core. Check whether jumbo frame support is required. 10-gigabit Ethernet will not be required for AP connections for the first wave of 802.11ac, but make sure it is part of your plans as 802.11ac develops. Any new cable runs for 802.11ac should include two cables.

Power requirements

Supply power to the AP mounting locations. This will need to be PoE+ (802.3at) for full functionality, so either upgrade edge switches to use higher power or obtain mid-span injectors to supply sufficient power to run your chosen AP hardware.

Security planning

802.11ac does not support TKIP or WEP for security. If your network is not already on CCMP (WPA2), consider moving the network to use CCMP to avoid needing to reconfigure client devices for the proof of concept.

After planning the network, as you move into the design and deployment phases, use the following checklist:

Architecture

> The easy choice in architecture is that the management plane must be centralized. In most cases, a hybrid data plane that blends aspects of both a distributed data plane and centralized forwarding will be the right choice. Carefully evaluate the trade-offs for the location of the management plane based on application requirements and cost.

Hardware selection

> Select hardware that meets your requirements for performance and functionality and is certified by the Wi-Fi Alliance to ensure interoperability.

Coverage and capacity planning

> Based on the anticipated user density and application mix, come up with tentative AP mounting locations. Many tools are available to assist with this process, some of which are free. When laying out the network, pick the widest "native" channel width for 802.11ac.

---

[39] Many 802.3af power injectors are able to supply substantially more power than the specification requires, through a combination of high-quality components, shorter-than-maximum-length cable runs, and high-quality cabling. Even taken together, though, these sources of headroom are only good for a few watts. The increased resources demanded by 802.11ac require more than just a few watts, so headroom won't save you from a power upgrade.

[40] CCMP is sometimes used interchangeably with the name of the Wi-Fi Alliance certification program that tests for CCMP interoperability: Wi-Fi Protected Access, version 2 (WPA2).

[41] See Chapter 22 in *802.11 Wireless Networks: The Definitive Guide* for a detailed discussion of building a user authentication system for your wireless LAN.

[42] With three channels, it is not possible to lay out a network where neighboring APs do not use adjacent channels. This constraint is one of the many reasons why the 2.4 GHz band is not a good choice for a capacity-oriented network.

[43] If 30 devices each require 4% of the available airtime, you will need 30 x 4% = 120% of the available airtime, or 1.2 radios. Because there is no such thing as a fractional radio, round up (or, in a spreadsheet, use the "ceiling" function).

[44] One of the reasons why the TV white space standardization effort is exciting is that the TV spectrum was around 700 MHz, giving it a range that can be measured in kilometers instead of meters.

[45] Receive sensitivity is not commonly reported on data sheets but may be available in the FCC test reports for equipment that you are considering.

[46] At the time this book was written, no 802.11ac interoperability certificates were yet available.

[47] For more information on the operation of the DTIM, see Chapter 8 in *802.11 Wireless Networks: The Definitive Guide*.

Prev Chapter 4. Beamforming in 802.11ac | Home | Next Glossary