white paper

Smarter Wireless Networks for MSOs

INCREASING MSOS ROI WITHOUT DISRUPTING USER EXPERIENCE OR THE CORE NETWORK INFRASTRUCTURE

Overview

The rapid adoption and expansion of mobile Internet services is one of the biggest trends in telecommunications in the last ten years. Mobile Internet operation has the potential for significant business value to cable operators looking for new sources of revenue. However, this is not without risks. The messy, statistical world of radio-frequency communication in heterogeneous networks, combined with the intricacies of evolving mobile core network designs for subscriber management, client authentication, service policy definition and policy enforcement, can be daunting territory even for experienced radio access network engineers, let alone technical teams coming into the scene from the wireline access side.

IEEE 802.11 (Wi-Fi) is well suited as a data delivery service in Pico and Femto cell locations and is complimentary to cellular data networks such as WiMAX and LTE. Wi-Fi offers the following benefits for MSOs:

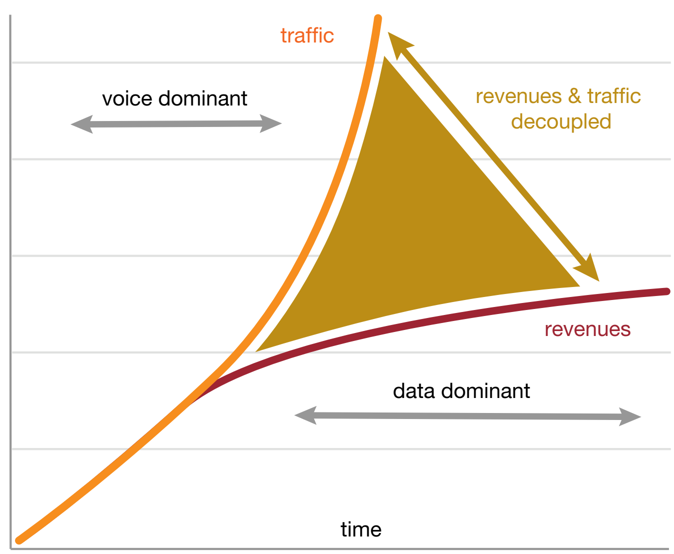
- 3G Offload – Most mobile devices with cellular data cards are also Wi-Fi capable
- New subscriber base – Many mobile devices are Wi-Fi-only
- Cost – Unlicensed spectrum, no spectrum license required for additional capacity

This paper focuses on the most important technical elements in wireless project exploration and execution — including advanced adaptive radio system design for high subscriber demand density environments, secure and seamless subscriber authentication, approaches to handoff and roaming and addressing the gap between mobile core integration standards and requirements in the real world of today's networks.

Smarter Wireless Networks for MSOs

INCREASING MSOS ROI WITHOUT DISRUPTING USER EXPERIENCE OR THE CORE NETWORK INFRASTRUCTURE

FIGURE 1: Decoupled Revenues and Traffic



Note: How Wi-Fi would contribute to revenue revolves around two main models: wholesale offering of the MSO network to MNOs (leasing, etc.) and using Wi-Fi to help promote the MSO as a Mobile Virtual Network Operator (MVNO).

Source: Unstrung Insider

Wi-Fi Models

Many operators are evaluating Wi-Fi and its usefulness to their network. Determining fitness can be based on one or more criteria but the real factor is how it impacts current and future revenue. Some recent, very well publicized, overloads of mobile operator data networks have raised the visibility of increasing subscriber demand for network capacity.

The Wholesale Model

One way to generate revenue is to leverage the Wi-Fi network as a value-add service to MNOs for their own branded networks. This requires a Wi-Fi infrastructure that can offer multiple, branded SSIDs and simple integration into both the MSO and MNO core for backend authentication, billing, etc. (See Figure 2)

The MVNO Model

As MSOs move towards a Mobile Virtual Network Operator (MVNO) model by adding cellular services to their portfolio, the ability to quickly expand and add coverage will be critical.

Voice subscribers demand coverage regardless of what the local spectrum landscape might look like. Increasing demand for wireless data services has, in many cases, exhausted local supplies of licensed spectrum. In many cases capacity can only be created with alternative solutions such as Wi-Fi.

Keys to successful implementation of either type of model (or both) requires the following:

- Wi-Fi access points (APs) – subscriber access
- Wireless mesh – backhaul
- Wireless point-to-point/multi-point – backhaul between mesh points and/or core
- WLAN network element manager – master view of Wi-Fi network
- Wireless services gateway – WLAN integration with mobile networking
- Femtocell CPE (indoor/outdoor) – femtocell subscriber access (optional)
- Authentication – seamless integration to core
- Roaming – fast and client-transparent roaming

Radio System Design

Wireless Architecture Types

There are four types of wireless architectures:

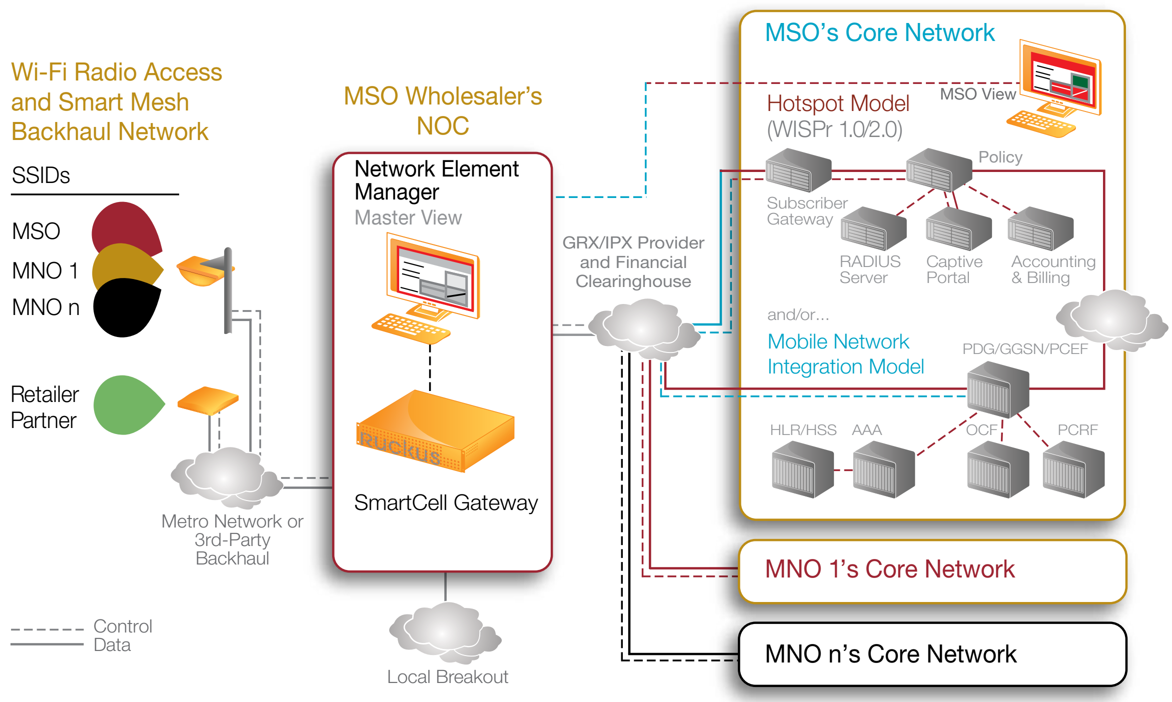
- Macro
- Micro
- Pico
- Femto

The use of **Macro** may be deployed as an above rooftop technology with a range of greater than 1 km. Macro architectures provide the backbone for a nationwide network. The use of **Micro**, for below rooftop, perhaps street level, is ideal for high capacity public areas like airports, stadiums, and shopping malls in less than 1 km coverage areas. **Pico** is well-positioned as a wireless architecture for large buildings serving small distance and subscriber counts. Finally, **Femto** may be considered for home or small office locations where distance, coverage and customer capacity are smaller than a Picocell.

Smarter Wireless Networks for MSOs

INCREASING MSOS ROI WITHOUT DISRUPTING USER EXPERIENCE OR THE CORE NETWORK INFRASTRUCTURE

FIGURE 2: Wholesale Wi-Fi Model



Integration with Hot Spot 2.0/802.11u capabilities

The Wi-Fi Standard

The 802.11 specifications are a series of IEEE standards for half-duplex wireless communications using the ISM (2.4 GHz) spectrum and U-NII 1, 2 and 3 (5 GHz). In Wi-Fi nomenclature, a device operating on the 2.4 GHz band is considered 802.11b (if using CCK modulation) or 802.11g (if using OFDM). A device operating on the 5 GHz band is 802.11a (OFDM).

A secondary designation is also used if a client device supports the IEEE 802.11n standard. This is an amendment to the original 802.11 standard that supports higher transmit rates. 802.11n introduces support for MIMO (Multiple-In, Multiple-Out) radios, channel bonding and other techniques that boost performance from 11 Mbps (802.11b) or 54 Mbps (802.11g or 802.11a) to a theoretical maximum of 600 Mbps. Devices that are compliant with this standard use a “n” designation, for example, 802.11bgn.

New Wi-Fi devices manufactured today are often 802.11n compliant. This standard is quickly overtaking older devices as a percentage of overall population and is expected to be the dominant client device radio choice in the near future. This is good news for operators looking to support client Wi-Fi devices – the faster speeds and enhancements of 802.11n are much more suited for high density and high performance deployments.

2.4 GHz Spectrum (802.11bgn)

The most common access radio type for Wi-Fi client devices is the ISM 2.4 GHz band, specifically 2412 through 2462 MHz.[1] Each channel is 20 MHz wide from the center frequency.[2] This yields three non-overlapping channels in 2.4 GHz – channels 1, 6 and 11.

5 GHz Spectrum (802.11an)

While the 2.4 GHz radio is the most common for client access, backbone/backhaul traffic typically utilizes the unlicensed 5 GHz spectrums. In the US, this comprises the lower, middle and upper U-NNI bands: 5.15–5.25 GHz, 5.25–5.35 GHz, and 5.725–5.825 GHz. 802.11a also uses a 20/40 MHz channel width and supports up to 12 non-overlapping channels.

1 As per US FCC regulations for the Americas regulatory domain. Other countries and organizations have different allowed spectrum ranges.
2 802.11n also supports 40 MHz wide channels.

TABLE 1

ADVANTAGES/DISADVANTAGES OF WI-FI VS. LICENSED SPECTRUM

	Wi-Fi (unlicensed)	Licensed Spectrum (WiMAX/LTE, etc.)
Transmit Speeds	Up to 450 Mbps[3]	Up to 100 Mbps
Duplex	Half	Full
Licensing requirements	None	Per local availability and regulatory approval
Licensing costs	None	Per local availability and regulatory approval
Interference	Varies	Minimal

Advantages/Disadvantages of Wi-Fi vs. Licensed Spectrum

There are a number of reasons why Wi-Fi is desirable as a wireless architecture. But there are some issues that must be considered before moving forward with a deployment.

The major advantage of Wi-Fi as compared to licensed spectrum technologies is that it is cheap and relatively easy to deploy since there is no spectrum purchase or licensing costs. The major downside of Wi-Fi is the flip side: because anyone can transmit, there is the potential for significant interference from other Wi-Fi networks. (See **Table 1**)

These shortcomings can often be overcome with careful planning and the right equipment selection. It is particularly important to take this into consideration before final site acquisition as some locations may be more prone to interference than others.

Wi-Fi Radio Network Components

As mentioned earlier, the radio components of the Wi-Fi network can be itemized as follows:

- **Wi-Fi Access Points (APs)** – subscriber access
- **Wireless Mesh** – backhaul
- **Wireless Point-to-Point/Multi-point** – backhaul between mesh points and/or core
- **Centralized Wi-Fi Management**

Each of these components has a vital role within the architecture as a whole. Key considerations for each of these will be the specific installation and RF environment, performance, load and capacity requirements and cost.

Wi-Fi Access Point Selection

From a subscriber's point of view, the most visible component of the network is the access radio of the AP. The ability to connect and seamlessly (and speedily) access mobile applications on demand is crucial for subscriber satisfaction and retention. Thus, the selection of the AP should be based on deliverable performance as much as any given feature. Of particular concern is the AP's performance in high-density networks. Many WLAN manufacturers tout performance numbers based on single client rate over range in ideal situations. This is not realistic and is not an accurate predictor of Wi-Fi performance in a deployed operator network. An analysis of high-density performance characteristics yields the following requirements:

1. Support for 802.11n
2. AP performance (transmit/client connection speeds)
3. Ability to support 100+ client connections[4]
4. Airtime Fairness to ensure equal client access to the medium
5. Active interference detection and mitigation (on channel and off)
6. Quality of Service (QoS) for prioritized application delivery such as streaming video and voice

3 Although the 802.11n standard provides for speeds up to 600 Mbps, the typical speed as implemented by most vendors today is 300 Mbps for 2 streams, and 450 Mbps for 3 streams.

4 Connection here is defined as an associated device which may not necessarily be actively transmitting.

802.11n Support

There are many Wi-Fi product offerings on the market today that claim to meet the needs of MSOs. Most APs on the market are 802.11n-capable. From this common starting point, however, capabilities and performance vary widely.

AP Performance

Most Wi-Fi APs use radio chipsets from a short list of chipset manufacturers (Atheros, Marvell, etc.). But this does not mean they have the same performance characteristics. Some radios are more tightly integrated with the rest of the hardware than others, which can yield substantial benefits. In particular, antennas are a major distinguishing factor in AP performance.

The major differences in Wi-Fi antennas lie in: signal gain, directionality and polarization. A typical access radio AP antenna is omnidirectional, typically 2 – 4 dBi signal gain, and vertical linear polarization. Such similarity implies similar performance.

Directional antennas can offer far greater range and higher client connection speeds due to the increased signal gain from a more tightly focused signal. While these traits are desirable, the narrow beamwidth (often 10-30°) drastically reduces the effective coverage area. This results in more APs required and is usually not desirable.

One interesting variation on this problem of signal gain vs. coverage is smart antenna arrays. These arrays are comprised of multiple directional antennas.[5] The array is designed such that the antenna system, as a whole, can provide 360° coverage. However transmission to a client is done with a combination of directional antennas that are focused in the client's location relative to the AP. This results in a directional beam of RF energy. The directionality of the transmission allows for increased signal gain and increased range.

The higher signal gain also results in higher transmit rates for clients. This is an ideal situation as it provides the advantages of directional, high-gain antennas with omnidirectional coverage. Higher client connection rates also mean clients can get on and off the air faster for each transaction executed – leaving more airtime for other clients (higher density). Support for more clients at greater range can dramatically reduce overall network costs in hardware costs as well as the number of sites required and installation costs.

Client Density

However not all APs may be able to support very high client densities. A review of many Wi-Fi AP's datasheets indicates they are capable of supporting up to 256 clients or more. The ability to allow 256 client associations does not necessarily translate into 256 active client connections.

Ideally, a Wi-Fi technology should not only support at least one hundred clients, it should also be able to move traffic through most - if not all – one hundred. This is not a simple task and requires intelligence both in the AP software and hardware. It also requires the other items in the list to satisfactorily deliver high-density performance.

Airtime Fairness

If there are one hundred devices associated to a single radio, there should be a mechanism to ensure none of the clients is hogging all of the bandwidth and, conversely, none of the clients.

Interference Detection and Mitigation

As noted, Wi-Fi operates on unlicensed spectrum. This means operators must share spectrum with other Wi-Fi networks as well as non-Wi-Fi devices that may also be using the same frequencies.

The absence of a single authority to coordinate channel assignments and spectrum use makes interference a significant factor in performance. The ability of an AP to detect and mitigate RF interference will play a crucial role in the number subscribers per AP, the coverage area and overall throughput performance. A reduction in any of these numbers means more APs in the final design, i.e. more site acquisitions, installation, hardware purchases, backhaul, power, permits, etc.

There are several mechanisms currently used by WLAN vendors to mitigate interference, these include changing channels (assuming there is a better channel available), changing power level (reduce cell size), and adaptive antenna solutions.

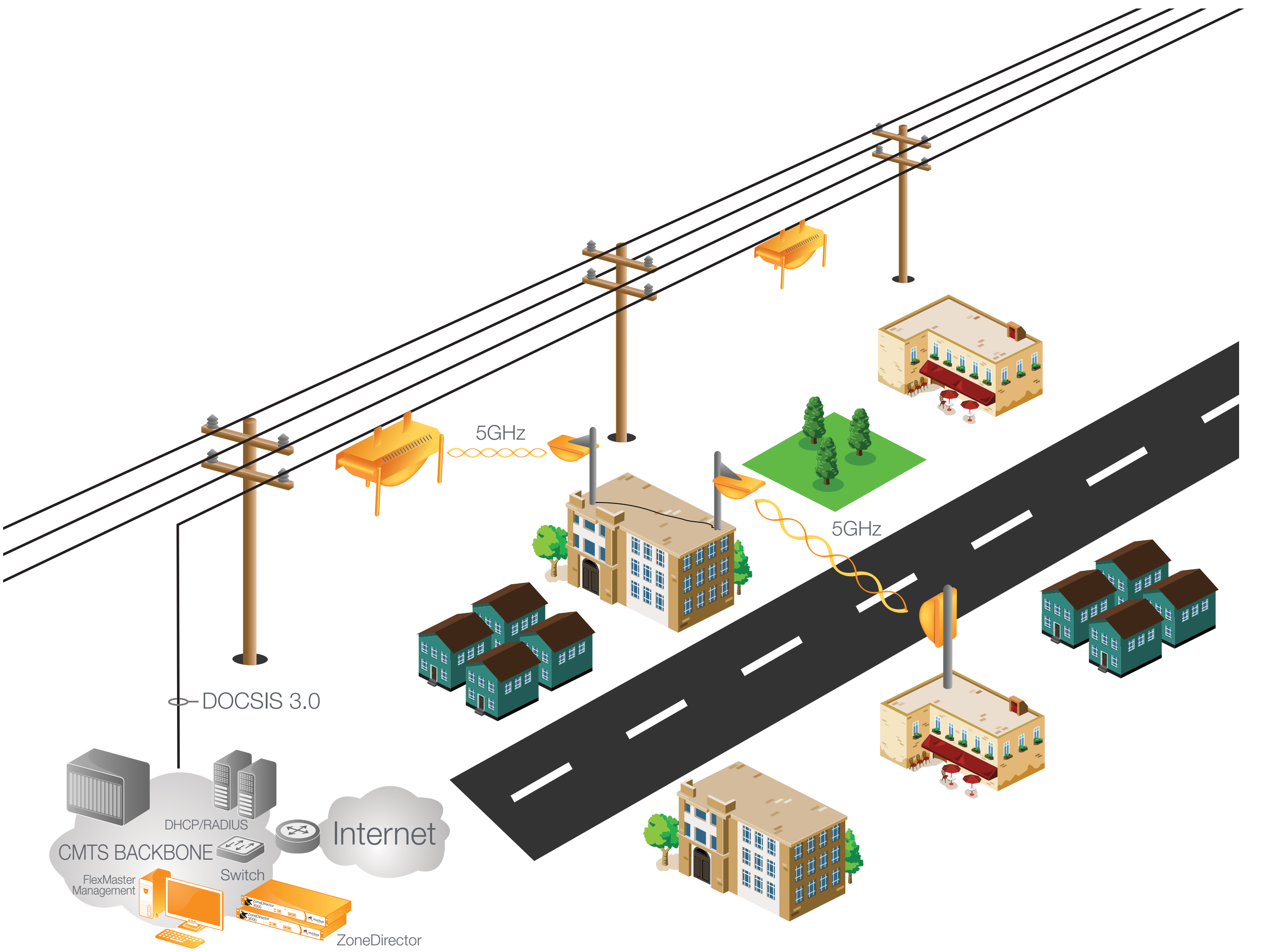
Switching channels is a popular option that is supported by nearly all Wi-Fi technologies. If the AP detects less interference on a different channel it simply changes to that channel. This reduces overall interference and improves performance. The downside of this technique is that it doesn't help if there are no better channels available. If an AP is experiencing excessive interference and all other channels are similarly busy no

5 In this case, multiple antennas refers to more than two antennas per radio chain.

Smarter Wireless Networks for MSOs

INCREASING MSOS ROI WITHOUT DISRUPTING USER EXPERIENCE OR THE CORE NETWORK INFRASTRUCTURE

FIGURE 3: MSO/Cable Operator Networks



improvements can be achieved. In a relatively sparse RF environment (e.g. rural) this mechanism can work very well. However, most suburban and urban areas already have high utilization of Wi-Fi spectrum. Another solution is needed. A final approach, which is the most promising to the problem of interference is adaptive (smart) antennas.

Most access radio antennas on APs are intended to cover a 360° (omnidirectional) area. Thus, when the AP is transmitting to a client device it is broadcasting in all directions, not just towards the client. This causes unwanted RF, which increases the overall RF interference levels.

FIGURE 4: Omnidirectional Antenna

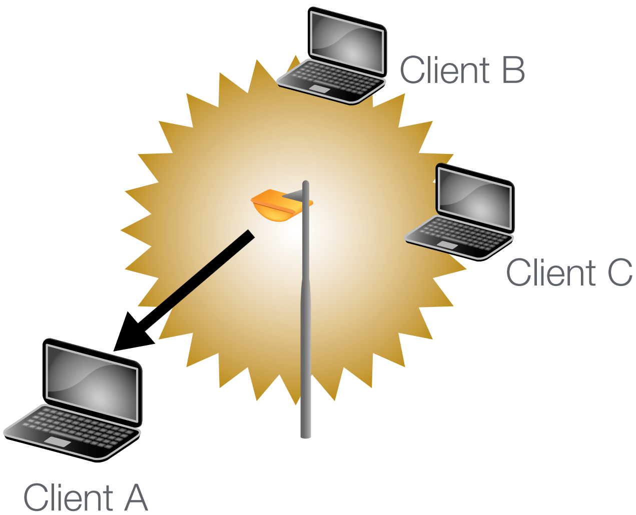


Figure 4 show how an AP transmitted to client A is also unintentionally transmitting towards clients B and C; causing unwanted interference.

Adaptive antennas employ an array of multiple directional antennas in order to form beams. Rather than transmit in an omnidirectional pattern, a combination of directional antennas can form a beam towards the active client. RF is therefore focused in that direction only. This capability is called "antenna-based beamforming" and is currently supported in some AP technologies. This should be distinguished from "chip-based beamforming" discussed later.

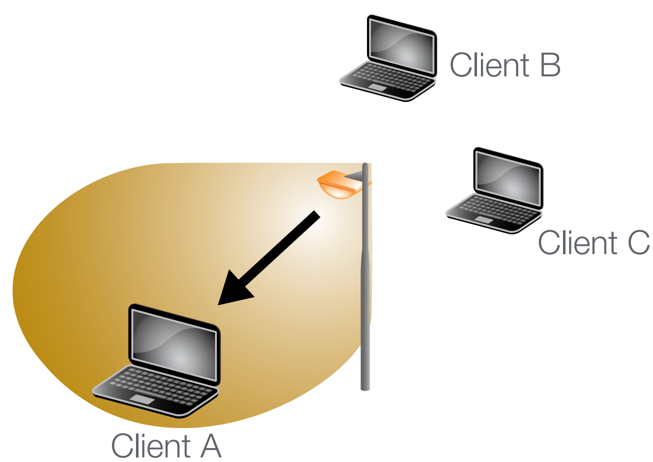
Adaptive antenna beam formation has the advantage of not only increased signal gain (all RF energy is focused on the target device), it also reduces interference. It's important to point out that this kind of adaptive antenna requires multiple directional antenna elements. Omnidirectional antennas cannot create a targeted directional beam toward a single client while simultaneously mitigating RF energy (noise) in the other directions (see Figure 6), showing symmetrical beam patterns created by omni antennas employing chip-based beamforming].

There are some Wi-Fi APs that incorporate a beamforming technology based on TxBF, which is part of the 802.11n standard.[6] This is very different from the antenna-based beamforming described above. In TxBF – also called chip-based beamforming – multiple omnidirectional antennas are used to correlate transmission signals. The result is, ideally, a point in which the signals are cumulative and additional signal gain is created. This can focus more energy towards a client, but it does not eliminate RF interference. Due to the symmetrical nature of the omni antenna pattern, RF interference may be received from the direction opposite the targeted client (see Figure 6).

In comparison, adaptive antenna arrays are particularly well suited to interference mitigation. With multiple antenna combinations to choose from, the signal with the best SNR (Signal to Noise Ratio) can be used. Also, reducing RF waste by not transmitting where the client is not located allows more antenna gain to be placed on the intended recipient.

Outdoor deployments will always encounter RF interference. Therefore the ability to mitigate and reduce interference in a deployment is one of the most important factors possible. Evaluation of a Wi-Fi solution should always include realistic environments. Lab testing, which typically has a very clean RF environment, is not necessarily an indicator of future success in the field.

FIGURE 5: Adaptive Antenna Beam Formation



6 Because multiple signals are correlated, TxBF requires a MIMO (Multiple-Input, Multiple-Out) capable AP.

FIGURE 6: Transmit Beamforming (chip-based)

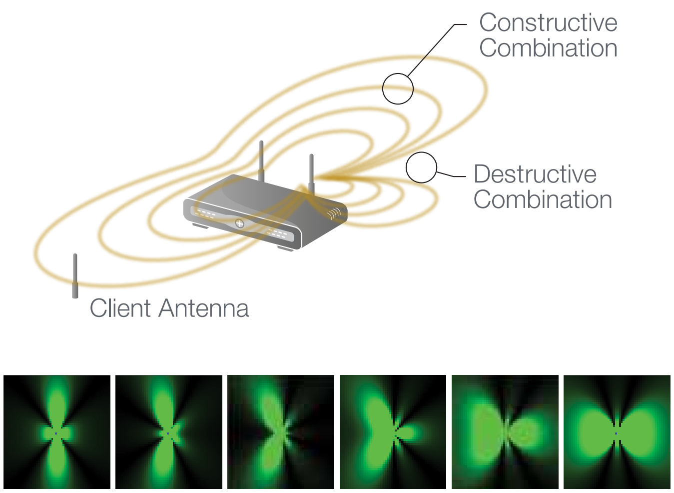
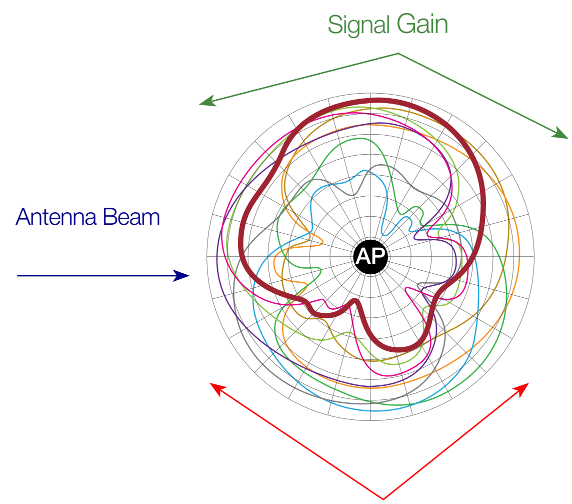


FIGURE 7: Interference Mitigation



Quality of Service (QoS)

A differentiator among wireless offerings to subscribers is content and application access. Different applications will require different levels of network access; for example, streaming video and voice must be prioritized over email to ensure acceptable performance.

The 802.11e[7] amendment to the Wi-Fi standard describes QoS mechanisms to protect sensitive data from other, non-delay sensitive traffic. 802.11e mandates AP support for four transmission queues: voice (highest priority), video, data and background. Note that the standard itself only requires one set of queues for the entire WLAN. The preferred approach is to implement these queues on a per-client basis at the AP.

Wi-Fi Mesh and Point-to-Point/Multi-Point Bridge Selection

So far, this discussion has been primarily about subscriber access performance. However many of the points made so far, in particular with reference to radio/antenna performance, hold true. The greater the performance, at range, of a mesh node or bridge, the better overall network performance will be.

RF Performance

It cannot be emphasized enough the importance of proper AP RF engineering as outlined in the previous section. Everything that follows from here on assumes great AP RF performance. **No feature can make up for an AP that cannot provide outstanding RF coverage.**

The best RF performance, as seen to date, has been based on adaptive antenna array technology. This provides the best performance, least interference and RF mitigation. In an ever-changing Wi-Fi RF landscape, these features are a critical way an MSO can future-proof their Wi-Fi investment.

This is particularly true with regards to network capacity and latency. Other requirements include:

- Self-organizing Network (SON) capability with self-healing/optimization
- Automatic (zero-touch) RF management
- Wi-Fi tuned for high-reliability backhaul
- Predictive, adaptive mesh topology
- High performance over range
- GPS and IEEE 1588v2 PTP timing capable
- Wired & Wi-Fi combined in single mesh topology
- Enable AP clustering for capacity aggregation

7 A complementary standard frequently mentioned in conjunction with 802.11e is WMM (Wi-Fi Multi- Media). This is an interoperability certification offered by the Wi-Fi Alliance and is based on 802.11e.

Interference Mitigation in the Mesh

Like individual APs, RF interference is a significant factor in Wi-Fi mesh and bridging. These devices typically use highly directional antennas, however the greater distances involved increases their susceptibility to interference. Anything that reduces the chances of interference across the backhaul greatly improves overall performance network stability.

Self-Organizing Networks

A Wi-Fi network must respond to rapidly changing environments, from both within and outside the organization deploying that network. For example, as MSOs increase their Wi-Fi network footprint, they will be adding new APs and expanding the mesh. Fine tuning these changes by hand is a daunting task that can consume hundreds of person-hours a year.

A good Wi-Fi network should be able to adapt to changes automatically and self-organize around those changes. This can free up valuable person-hours that can be better used elsewhere. It also dramatically improves rollout time – technicians can install new nodes in a matter of minutes instead of hours. Automatic organization also includes self-healing around failures – again, reducing the need for truck rolls and technicians on poles.

Wi-Fi Network RF management

All Wi-Fi deployments will require both dynamic adjustments to changing environmental conditions as well as administrative configuration. These tasks should be presented in a simple manner than can easily be learned by NOC personnel and higher-level engineers alike.

Because of the large scale involved in MSO/MNO deployments, a high-touch Wi-Fi solution that requires direct configuration of each individual AP, mesh node or bridge is simply not practical or realistic.

Automated RF Channel Planning

Reducing day-to-day operator maintenance and management tasks is critical to the success of a WLAN deployment. Many licensed spectrum networks require intensive, time-consuming channel planning and maintenance. Wi-Fi networks, due to their use of unlicensed spectrum, can require daily – perhaps hourly – monitoring and management of channel usage. This is highly undesirable.

An ideal WLAN network has a central management point capable of monitoring RF capacity and interference and adjusting channels as necessary automatically. By not requiring direct operator intervention, the network can drive fast adaption to a changing wireless landscape and increase overall performance and maintain SLA.

Centralized Multi-Tenant Management

As MSO's rollout their networks to MNOs, they may need to support multiple MNO access to the Wi-Fi network for monitoring, management, troubleshooting and reporting. These are key to MNO rollout success. However access to a centralized management platform should not mean MNOs have access or visibility to other MNO networks. Therefore, the Wi-Fi management platform must support a multi-tenant model that gives each MNO visibility and management of their specific network; SSIDs, statistics, SLA, etc. Management and monitoring of the overall WLAN network itself is reserved for the MSO.

Automated Firmware and Configuration

Any new network infrastructure represents tremendous effort to design, deploy and manage. Those management tasks include updating the WLAN nodes with new configuration as well as firmware updates. Many Wi-Fi technologies support a reduced or zero-touch management plan for their APs. The management server serves not only as a central management point, but also a single place to push new configuration profiles and firmware updates to the network nodes. This reduces truck rolls and expensive, hands-on management. Automatically propagating the same configuration/firmware to multiple devices also reduces the chances of operator error and misconfigurations.

Core Integration

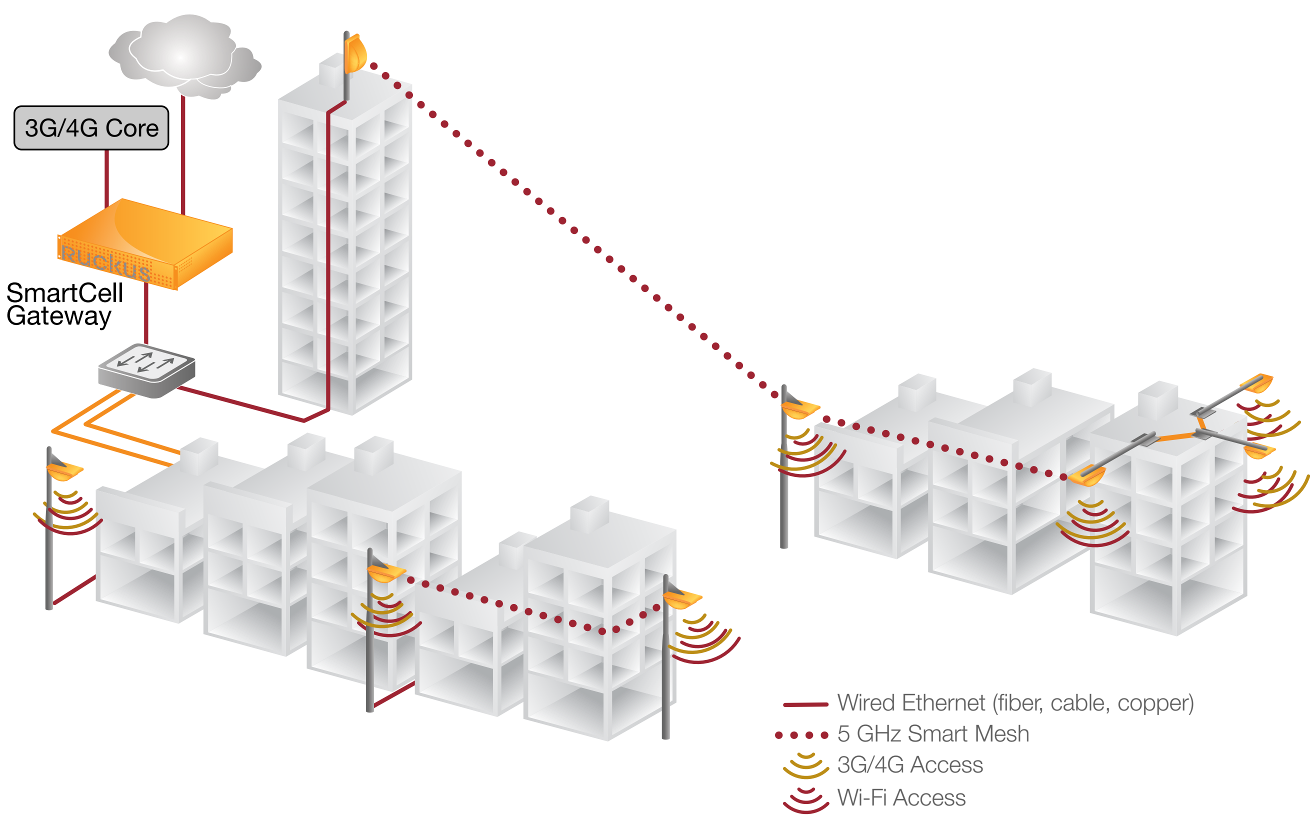
Core Services and the Wi-Fi Network

Second only in importance to superior RF performance, is the ability to tightly couple the Wi-Fi network into the existing core infrastructure. Not only does this help provide a seamless subscriber experience, it also helps reduce costs: simpler deployment, maintenance equates to fewer man-hours and cost savings. It also helps reduce troubleshooting time and maintain SLAs – existing tools and procedures to troubleshoot core issues will remain relatively similar, which reduces mean time to fix.

Smarter Wireless Networks for MSOs

INCREASING MSOS ROI WITHOUT DISRUPTING USER EXPERIENCE OR THE CORE NETWORK INFRASTRUCTURE

FIGURE 8: Integrated Mesh Backhaul



The primary pieces of core integration for Wi-Fi include:

- SmartCell Gateway – the demarcation between Wi-Fi management and services and the rest of the core
- Authentication – subscriber authorization
- Client roaming – seamless, transparent subscriber experience
- Billing – accounting and payment

SmartCell Gateway Relationship to the Core

From a logical point of view, the SmartCell Gateway (SCG) sits between the Wi-Fi network and the core. For tunneled WLAN data entering the core, it may also be the packet data gateway. This gateway is situated on the home (MSO) network and operates as a multi-tenant platform for MNOs.

Key features of SCG integration should include:

- Support for tunneled data (encrypted or unencrypted) as well as local breakout
- AAA Proxy support
- Scalable, high performance data throughput

Support for these functions allows an MSO to easily add Wi-Fi to the existing infrastructure without requiring traffic reengineering or new authentication/integration models. Instead, the existing structure is leveraged with very minimal change. This has significant benefits to the MSO looking to deploy a cost-effective Wi-Fi network with minimal upfront cost or changes.

The logical model can then be extended into a realized wholesale architecture capable of supporting a large number of operators as individual entities.

TABLE 2

GLOSSARY OF TERMS AND DEFINITIONS	
3G Networks	Third generation of mobile systems also known as International Mobile Telecommunications-2000 (IMT-2000) specifications
4G Networks	4G is the short name for fourth-generation wireless, the ITU-R organization specified the IMT-Advanced (International Mobile Telecommunications Advanced) requirements for 4G standards.
CCK	Complimentary Code Keying – modulation scheme used in 802.11b wireless networks in order to increase achievable data rates from 2Mbps to 11Mbps
CM	Cable modem – connects a computer or local network to broadband Internet service through the same cable that supplies cable television service
CMTS	Cable modem termination system – a DOCSIS network device that manages and communicates with many Cable Modems.
CPE	Customer Premises Equipment—Communications equipment that resides in the customer's premises.
DoCSIS	Data Over Cable Service Interface Specification-- an international telecommunications standard that permits the transmission of internet protocol communications transfer over an existing Cable TV (CATV) system.

Billing

Authentication has already been discussed in an earlier section, but so far very little has been said about billing. Subscribers not only need a seamless way of authentication, the operator needs a seamless way to handle account status. This includes billing (tiered billing, pay as you go, monthly billing, overage costs, etc.). Therefore the SmartCell Gateway must be able to look up and enforce any required billing that results from subscriber login and access. This is a dynamic process that requires flexibility from the gateway.

Subscriber Authentication

Any subscriber-based service offering requires authentication to ensure only paying customers have access to the network. All MSOs and MNOs typically have an authentication and billing system in place. It is important then that a Wi-Fi extension of the existing infrastructure be seamless and transparent.

- Automatic, secure authentication and roaming
- Enabled by SSID & authentication protocol configuration
- Easy-to-use push configuration
- Utilize mobile OS to auto-detect and authenticate features
- Do not require a separate connection manager application

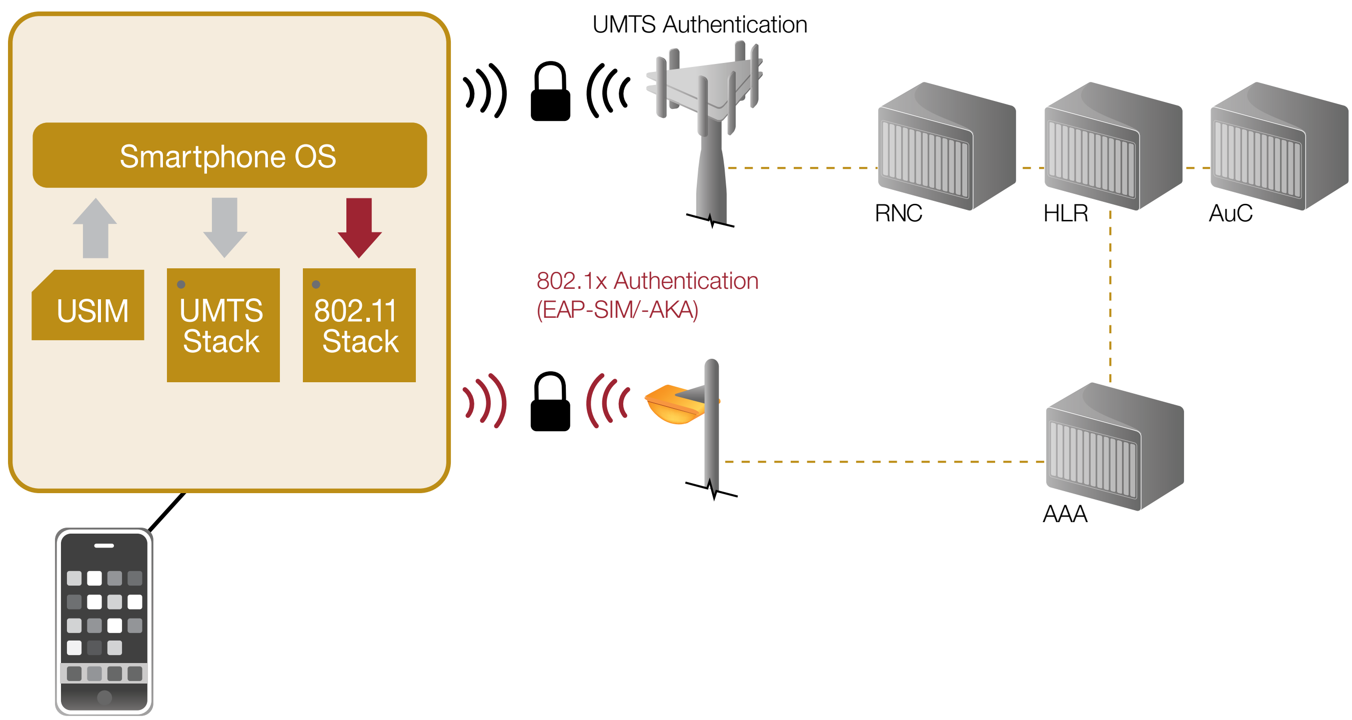
Common Client Authentication Types

An essential part of this authentication scheme is EAP-SIM and EAP-AKA. These authentication protocols are a standardized way to meet most of the needs listed above. They allow transparent authentication using existing SIM credentials. These methods also eliminate the requirement for a separate connection manager. Since most mobile devices support auto-detection and use of Wi-Fi networks, integration with a Wi-Fi infrastructure is relatively simple in this respect.

Of course not all mobile devices have SIM cards, (laptops, iPads, tablets, etc.). In these cases an alternate authentication method is required.

The key to a successful design and implementation lies in easy integration with the core. This should include as little modification to the core as possible. The above approaches to subscriber authentication are very typical and supported by most AAA servers and services within the core.

FIGURE 9: Authentication to the Core



Roaming

The integration of cellular and Wi-Fi networks ultimately involves integration at both the client and the core network. Guaranteeing a seamless subscriber experience requires a Wi-Fi network that can accept a device roaming from the cellular network without requiring manual intervention.

Clients today are capable of detecting available Wi-Fi networks and initiating a switch. From there it is up to the Wi-Fi system to complete the authentication tasks that give the device admission to the network. The previous section discussed several authentication mechanisms that may be used to authorize subscriber devices. But there is more to roaming than authentication. Also important are:

- How quickly a client can move from one AP to another
- IP persistence – allow the client to keep the same IP address within a local area

Wi-Fi Traffic Offload

As part of core integration, a WLAN gateway must have the ability to offload traffic from the APs to the Internet or tunnel the traffic back into the core. Corebound traffic needs to be handled in different ways, depending on the particular MSO/MNOs model: local-breakout or centralized tunnel data (encrypted or unencrypted). This flexibility is a must to support current as well as future needs.

Since the gateway will see both control plane traffic (from the APs) as well as client originated traffic, a logical partitioning of traffic is necessary to keep each type isolated from the other.

TABLE 3

AUTHENTICATION APPROACHES

Attributes	EAPSIM/AKA	MAC/PSK	MAC	UAM
Subscriber Identification	USIM	MAC address	MAC address	User name and password
Air interface Encryption	AES (derived from UMSIM)	AES (derived from PSK)	None	None
UE Requirements	USIM, 802.1X, EAP-SIM/AKA	WPA2	None	None
AP Requirements	WPA2	WPA2	WISPr	WISPr
Interference	Varies	High (transparent to subscriber)	High (transparent to subscriber)	Minimal
Convenience	High (transparent to subscriber)	Medium	Low	Low (requires subscriber input)
Security Strength	High	Non-SIM devices	Non-SIM devices	Temporary guest access

Client IP Address Roaming and Persistence

As subscribers move from node to node within a network, it is important to reduce or eliminate the need for the device to drop and reacquire an IP address. Re-acquiring an IP address is time-consuming and can adversely impact the subscriber experience. When a device roams from one AP to another nearby AP, it needs to take its IP address with it. This type of roaming represents significant sophistication on the part of the WLAN gateway. It needs to coordinate the initial acquisition of an address (DHCP option 82, for example) from the correct range of available addresses and ensure that address is maintained throughout the local network.

IP persistence not only improves subscriber experience, it also improves the MSO/MNO's ability to track a particular device for management, billing and troubleshooting purposes.

Summary

Wi-Fi can be a very good fit for MSOs looking to expand their capacity, footprint, services and revenue. Many new solutions in the MSO market have emerged to meet this growing need.

To ensure a successful deployment, MSOs need to understand Wi-Fi's background – how it developed out of the enterprise and unlicensed spectrum and evolved into what it is today. Taking the next step into the operator market will require new features and capabilities from Wi-Fi solutions.

A product line that is primarily focused on the enterprise may not be able to function well in a carrier/operator environment. There are significant scaling issues as well as core integration features that are different for carrier/operator environments.

Ruckus® Simply Better Wireless.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

www.ruckuswireless.com