Update on Carrier Wi-Fi

The Rise of Cable Wi-Fi

A Technical Paper prepared for the Society of Cable Telecommunications Engineers
By

Steve Hratko
Director of Carrier Marketing
Ruckus Wireless
San Francisco, CA
650 620 9161
steve.hratko@ruckuswireless.com

Sebnem Ozer, Ph.D.
Principal Staff Systems Engineer
ARRIS Inc.
Horsham, PA
215 323 1154
sebnem.zorluozer@arrisi.com

Jerry Patton
Product Manager, Wi-Fi
ARRIS Inc.
Denver, CO
720 895 7154
jerry.patton@arrisi.com

Overview

The tremendous acceleration in mobile data traffic has been well documented over the years and continues in all geographies. Smartphones have become the de facto method by which most of the world consumes the Internet. The challenge for MSOs is how to best to profit from this trend. MSOs have great assets including extensive broadband HFC plant in most highly populated areas, and some of this plant is aerial which is great for mounting Wi-Fi APs. MSOs also have very strong customer relationships both with consumers and SMBs. There are several business models that MSOs are focusing on, with the primary one being to add Wi-Fi to their existing service bundle (Internet, voice, and video) to increase customer stickiness. This means less churn, which is a significant cost for most MSOs. A longer-term objective for many MSOs is to eventually enter into roaming arrangements with MNOs (mobile network operators) whereby their customers can use the MSO's Wi-Fi network to get connected to the Internet. The technology to enable massively scalable Wi-Fi roaming has arrived in the form of Hotspot 2.0, which will be discussed in more detail later in this paper. Once Hotspot 2.0 technology is in place, all that is left is to work out the financial settlements (if applicable) that are associated with roaming.

When deploying Wi-Fi technology, which has a very limited range, it is best to put the AP's where the people are. This means focusing on highly concentrated areas where large numbers of people congregate. These are often the same locations that MNOs are targeting for licensed small cell deployments. There are significant opportunities for MSOs to work with MNOs on these deployments.

One of the most compelling features of Wi-Fi technology is that it can be deployed by a wide variety of different entities including MNOs, MSOs, wireline providers as well as enterprises and public venues (Figure 1). This enables a level of densification to be achieved that goes far beyond what any service provider could accomplish on its own.

This paper will first explore the opportunity for carrier class Wi-Fi deployments by MSOs in a bit more detail. Some of the topics include:

- **Reliable wireless connectivity** without which nothing else really matters.
- **Hotspot 2.0 technology** to make the Wi-Fi roaming experience as seamless, secure, and automatic as with cellular
- **Scalable network architectures** with services to enable a compelling user experience once connected
- **Mastering the convergence of Wi-Fi and small cells** that will emerge in the latter part of 2014.

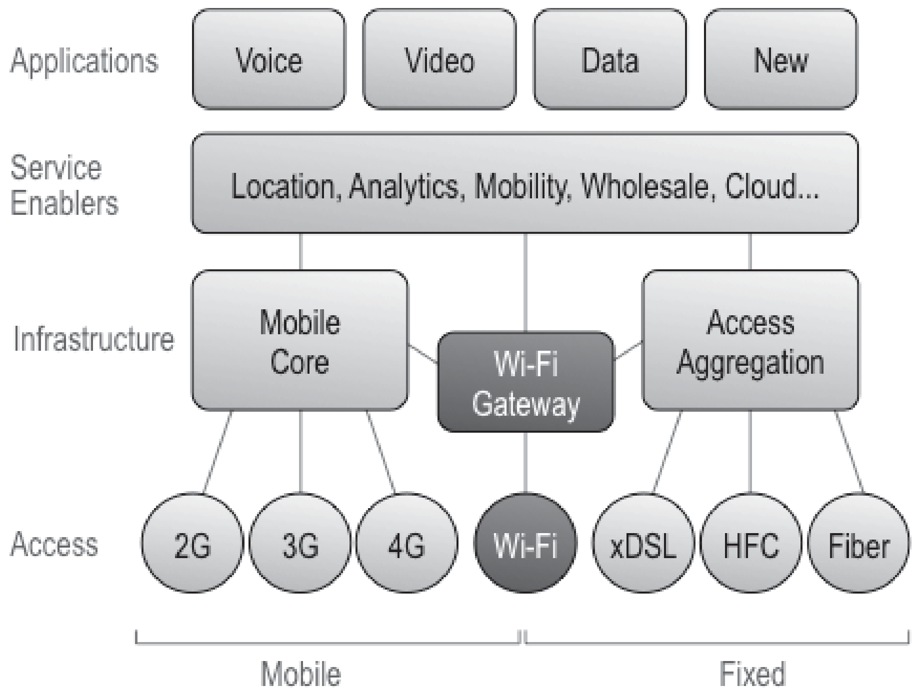

Figure 1 Carrier Class Wi-Fi System Deployment Architecture

We will then discuss the impact of new backhaul and back-office technologies on carrier class Wi-Fi services, mainly **converged edge router and multi-screen video platforms**. Better integration of Wi-Fi networks through the evolution of both Wi-Fi access and backhaul technologies will be addressed. We will conclude the paper by reiterating key elements for successful Carrier Wi-Fi deployments, integration and business opportunities for MSOs.

Leveraging Wi-Fi technology for greater competitive advantage

Reliable Wireless Connectivity

Reliable wireless connectivity is essential in any deployment because if you can't get connected and stay connected, nothing else really matters. A great deal of work has been done here over the past few years to make sure that the user can pick-up a solid signal, and a lot depends on where the APs are mounted.

One of the most compelling mounting locations for Wi-Fi AP's is on the aerial cable plant, where it exists. This enables MSO's to cover wide sections of city streets and, in many cases, reach users that are in buildings facing the street. The keys to a successful strand mount deployments are DOCSIS 3.0 support, environmental hardening, adaptive antenna technology, support for large numbers of users, and the ability to also provide backhaul and power to a small cell (more on this later).

Wi-Fi is also a great indoor technology that can support high-density public venues like airports, convention centers, hotels, stadiums, etc. The challenge with highly concentrated locations is that to get capacity, it is necessary to deploy large numbers of APs in a fairly confined area. This can introduce the potential for interference. The optimum solution for very high-density deployments is to make use of adaptive antenna technology, the large amount of unlicensed spectrum that is available, dual-mode devices, and a self-optimizing network architecture.

- **Adaptive antenna technology** can steer RF energy toward the user and away from neighboring APs that would see this as interference. The latter is very important in high-density design, as interference is often the limiting factor in a deployment. Adaptive antenna technology has been proven in high-density venues worldwide and offers a significant advantage over legacy solutions. As shown in the above drawing, the RF energy is shaped and directed in different ways for different user. This technology is especially effective on strand mounted APs and can increase the signal gain at the user's device by 6 dB (Figure 2).
- **Adaptive polarization diversity** is another key ingredient in a successful Wi-Fi deployment as it can increase the performance of the uplink. It is implemented in the Wi-Fi AP by having horizontally polarized and vertically polarized antennas to receive the user's transmission (Figure 3). This enables the AP to receive a strong signal regardless of the physical orientation of the user's mobile device.

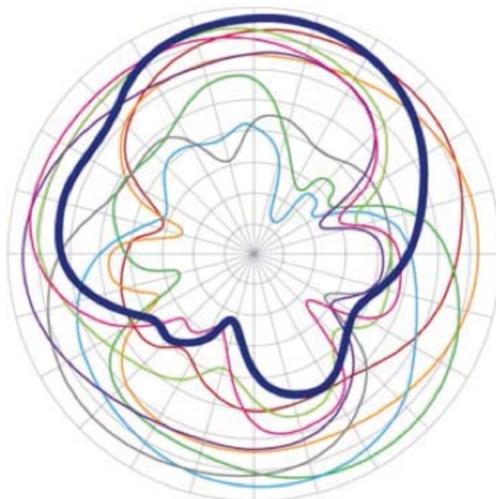

Figure 2 Adaptive antenna patterns

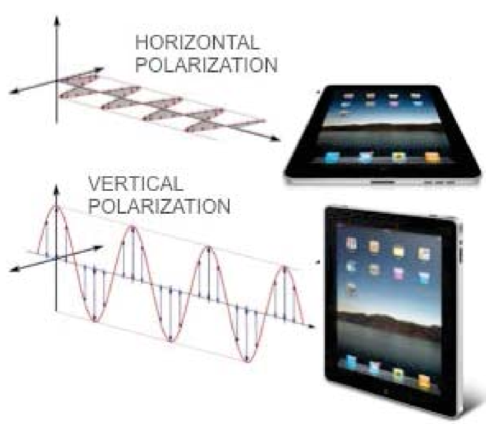

Figure 3 Adaptive polarization diversity

- In high-density deployments there is no such thing as too much spectrum, and Wi-Fi has access to **upwards of 600 MHz** in many geographies. This far exceeds the licensed spectrum that a mobile operator would have in a major metro area. In many indoor deployments, the venue owner can exercise a great deal of control over what gets deployed in their building, which can help keep unlicensed bands from getting congested.
- Almost all data-centric wireless devices (laptops, tablets, and smartphones) now **support the 5 GHz band**, which will greatly improve network throughput in high-density deployments.
- **Self-optimizing network** technologies like ChannelFlyTM enable APs deployed in close proximity to automatically select the optimum channel for the situation based on realizable capacity, and switch channels as circumstance dictate. One factor that changes the RF characteristics of a venue is the ebb and flow of the crowd, as people do absorb RF energy. SON technologies like ChannelFly are absolutely essential to enabling massively scalable Wi-Fi networks to be rolled out quickly and with a minimum amount of network planning. When this is combined with technology that allows APs to be automatically configured, it makes large deployments fairly straightforward.
- **Strand mounted DOCSIS compatible APs that can power external devices** are a critical ingredient in any MSO deployment. Aerial plant, where it exists, is a nearly perfect place to mount Wi-Fi APs (and small cells) as it provides site acquisition, power, and broadband backhaul. The ability of these devices to provide power-over-Ethernet (out) enables them to also support small cells. The latter has become a very interesting opportunity for MSOs, as MNOs look to rapidly build-out a small cell network to increase their network densification.
- **802.11r and 802.11k technology** to greatly improve the user experience during a handoff scenario. Now as the user moves about in a large venue such as a stadium, it will be possible to quickly hand them off from AP to AP as they move about. This technology impacts both the network and the mobile devices and is addressed with 802.11r. Another specification from the IEEE addresses load balancing, where the network will move subscribers around in the coverage area to better address loading in the network. This work is called out in 802.11k.
- **802.11ac is also on the verge of entering the carrier market** and in the right situations they can provide a real performance boost (Figure 4). 11ac uses new modulation techniques, greater channel bonding, and even more RF streams to push throughput up above 1 Gbps. Very few devices actually need this kind of performance, but it does enable the user to get on and off the airlink quickly, which enables even more users to be supported by the same AP. This technology will start to emerge in 2014 as it does require new APs and new devices. 11ac will not always be the right solution as it gets its great throughput through channel bonding, and there will be those situations where more non-overlapping channels will trump the need for higher speed.

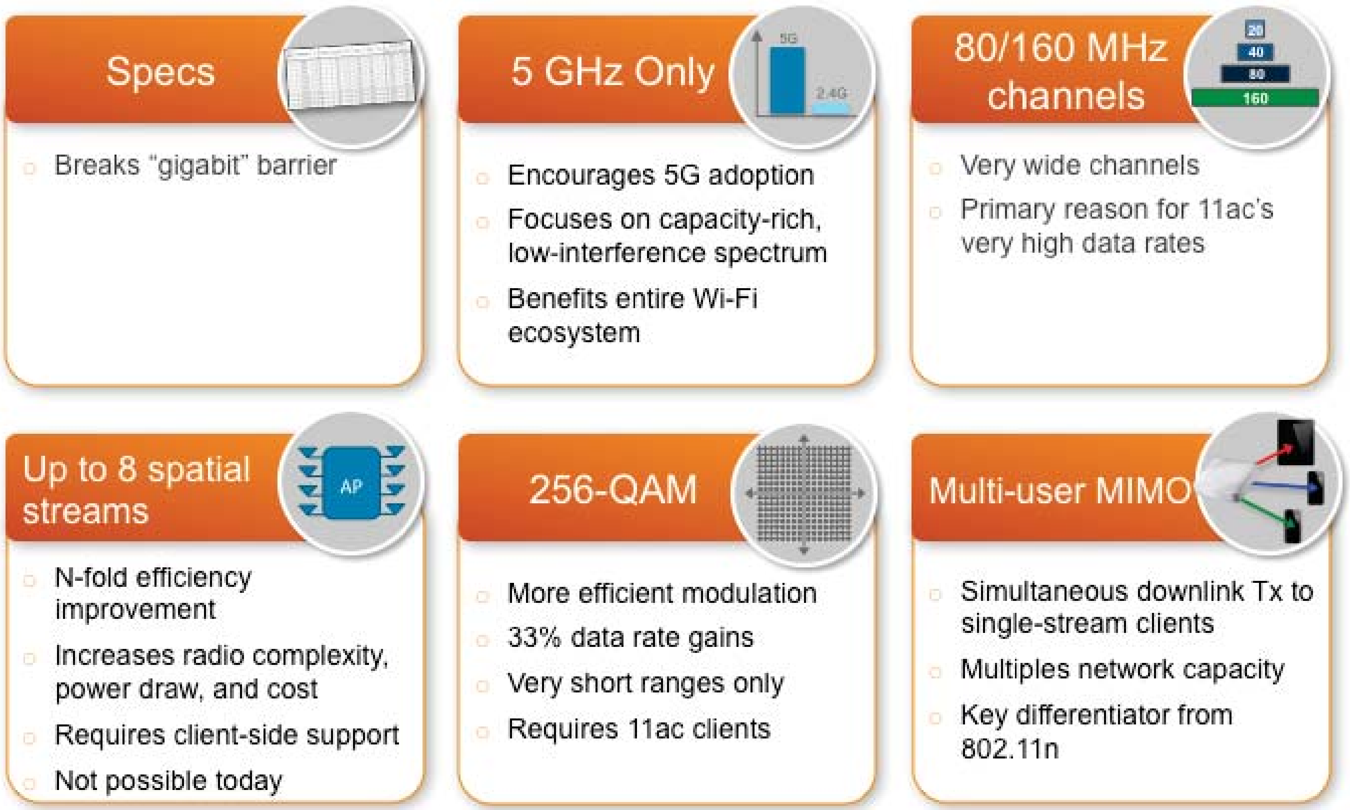

Figure 4 IEEE 802.11ac overview

Hotspot 2.0: Automating and Securing the Wi-Fi Connection Experience

Reliable wireless connectivity is only the first step in a compelling user experience. Next up, is to enable the user to get automatically connected wherever they might be, and that includes a coffee shop in their hometown or a city on the other side of the world. This is very much the mobile phone experience that we all enjoy when getting off an airplane just about anywhere in the world. The Wi-Fi Alliance is driving an initiative called Hotspot 2.0 to address this challenge. Ruckus has been a leader in the HS2.0 work in the WFA, and it's an essential part of the Ruckus SmartCell Architecture.

The first release of HS2.0 provides support for automatic network discovery and selection along with automatic authentication (aka roaming). In this process, a HS2.0 enabled mobile device can have a dialog (pre-association) with a HS2.0 enabled AP for the purpose of discovering its capabilities, the most important of which include:

- The domain name of the network operator that is providing that AP. If it is the same as the user's home network then the user can move straight to authentication. No roaming required.
- If it is different, then the mobile device needs to discover the roaming relationships that are supported by that AP.
- Other capabilities that can be discovered include backhaul bandwidth, loading on the backhaul, name of the AP operator, authentication method, etc.

Once an AP has been selected, the mobile device will automatically connect to the network using 802.1x with EAP (extensible authentication protocol). There are many EAP methods of which the following are required for HS2.0 compatibility:

- If a mobile device has a Subscriber Identity Module (SIM), then EAP-SIM as defined in RFC-4186
- If a mobile device has a UMTS Subscriber Identity Module (USIM), then EAP-Authentication and Key Agreement (AKA) as defined in RFC-4187. EAP-AKA' (RFC-5448) support will be required in a follow-on release.
- All mobile device must support EAP-Transport Layer Security (TLS) as defined in RFC-5216 and which uses an X.509 digital certificate
- All mobile device must support EAP-Tunneled Transport Layer Security (TTLS) as defined in RFC-5281) and which uses username and password, with a server side certificate

Mobile devices will use their existing mobile credentials when they are being authenticated back to the HLR/HSS in their home network. Hotspot 2.0 also specifies that the Wi-Fi airlink be encrypted using 802.11i. This addresses a security vulnerability with captive portal based authentication, which does not encrypt the airlink. 802.1x/EAP and 802.11i are both part of the Wi-Fi Alliance's WPA2-enterprise certification, which is standard on today's smartphones.

All Ruckus AP's and controllers are Hostpot 2.0 capable and any Ruckus 802.11n AP in the field can be upgraded to support HS2.0. HS2.0 capable smartphones have begun to ship from the major vendors with the Samsung Galaxy S4 being first out of the gate in May of 2013. And with the industry expected to ship 800 million smartphones this year, it will not take long for the technology to sweep through the industry. The actual HS2.0 equipment certification program in the Wi-Fi Alliance is called PasspointTM.

In Figure 5, we show a user in a visited network having their authentication request proxied back to the home network. The visited network could be an MNO, MSO, enterprise, wireline operator, public venue, or basically any entity with a broad Wi-Fi footprint. The impact of Hotspot 2.0 on Wi-Fi networks will be profound, and it will impact all device types.

In many ways the MSOs have been at the vanguard of the move to seamless Wi-Fi roaming with the work of the Cable Wi-Fi roaming alliance here in the US. Five major MSOs have banded together to allow each MSO's subscribers to roam on their combined network. This is a great example of the power of roaming, and with Hotspot 2.0 this approach become infinitely scalable. Not only can MSOs roam with each other but with MNOs, wireline operators, public venues, private enterprises, and the list goes on.

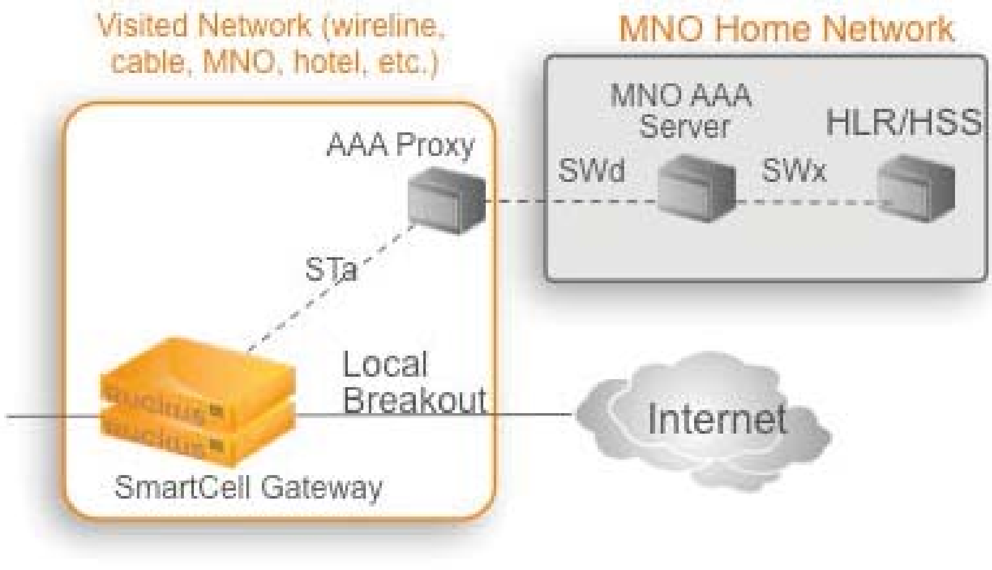

Figure 5 Routing the authentication request back to the home network

A Compelling Services Infrastructure for MSOs

The Ruckus SmartCell Architecture (Figure 6) is well suited to carriers of all types, and especially to MSOs. It consists of Wi-Fi access points, WLAN controllers, WLAN gateways, and selected value added services. The WLAN controller provides a variety of radio resource management (RRM) functions for Ruckus access points including:

- Management of access points
- Management of security associations
- Automatic channel selection, which enables each AP to select the most appropriate channel for that situation
- AP-AP handoff as a user moves about in the coverage area and much more

The WLAN gateway function sits between the Wi-Fi RAN (controllers and APs) and the end network, which is usually the Internet. A steering function can be enabled to direct traffic to either the mobile packet core or to a service complex and from there to the Internet. (Note: the former only applies to MNO deployments). The service complex would include support for authentication and address assignment along with charging, policy enforcement, DPI, lawful intercept, and the collection of network statistics amongst other things.

Wi-Fi RANs can be built with equipment from a single vendor or they can be multi-vendor. In a multi-vendor architecture the operator could typically deploy APs (and the WLAN controllers that support those APs) from a number of different vendors, and direct all Wi-Fi traffic to flow through a WLAN gateway to the Internet. Connectivity between WLAN controllers and WLAN gateways can be via GRE, PMIP, or QinQ to name a few of the possible protocols. GRE is the recommended protocol, but other approaches are certainly valid. The recommended approach in Wi-Fi RAN network design is to connect APs to the gateway by way of the controller, and not have the APs connected directly to the gateway. This approach greatly simplifies multi-vendor interoperability, as it is only necessary for the WLAN controllers to interoperate with the WLAN gateways (and leaves the APs out of the equation). The interfaces that are **open and interoperable** in Wi-Fi RANs include the 802.11 airlink, the S2a/Gn interface to the core (only for MNOs), IP interface into the Internet, and of course RADIUS (or Diameter).

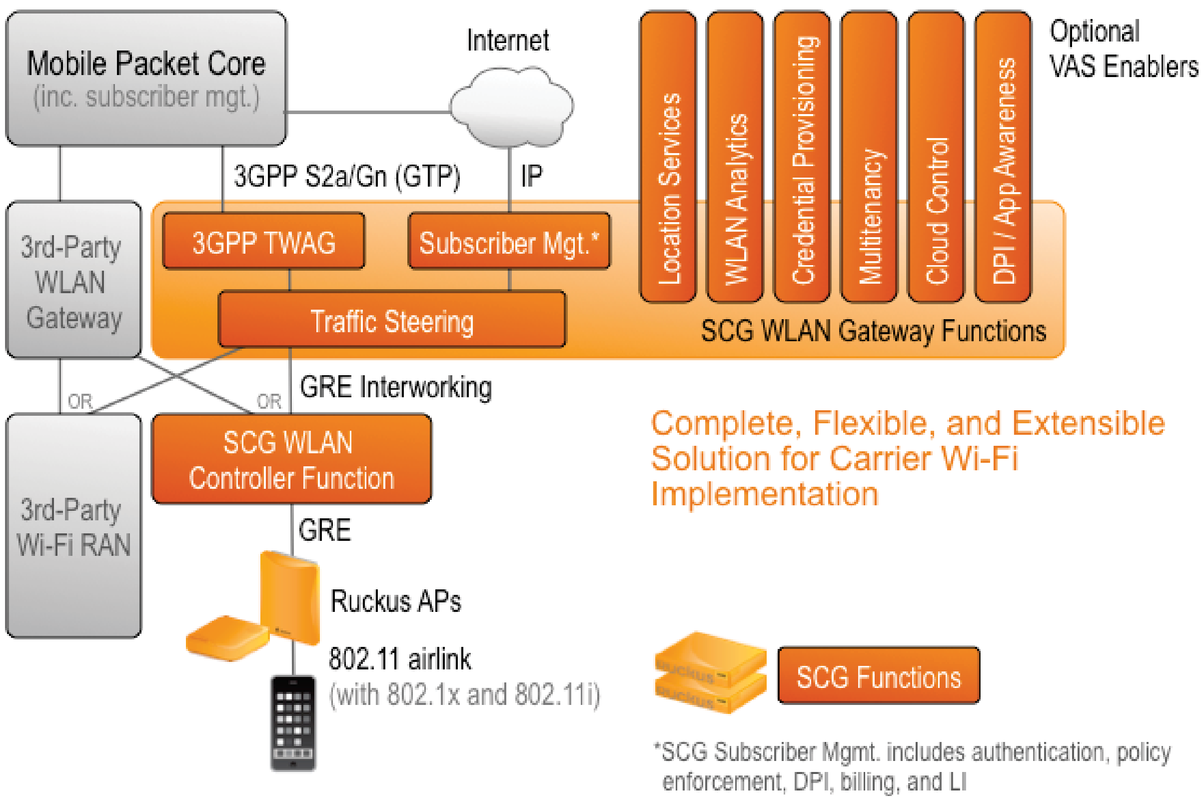

Figure 6 SmartCell Architecture

The Scaling Challenge

The design of the WLAN Gateway is key to enabling a very scalable deployment, as it is what aggregates traffic coming from APs and WLAN controllers located across the coverage area. It is also where services are provided, and they must scale as well. A good target is to focus on WLAN gateways that can scale to at least 30,000 APs and 300,000 subscribers. This provides a very good starting point for network capacity. It is also important that network services can also scale and one of the more important ones is the collection of statistics. In the SmartCell Architecture this is done with SmartCell Insight.

SmartCell Insight is an application that runs on VMware and provides visibility, trend analysis, and reporting for Wi-Fi RANs. It does this by collecting data from the network on access point usage that can be used to better gauge the success of a Wi-Fi RAN deployment and help in planning for network expansion. A wide variety of metrics are gathered and these are loaded into the system's database engine, which can then be searched to produce a wide variety of reports. SmartCell Insight has a set of standard reports, and it also supports custom report generation. Data from this system can also be passed to upstream analytics engines via a variety of industry standard APIs.

Working with MNOs on Small Cell Deployments

The MSOs are uniquely positioned to enable the broad based rollout of small cells by leveraging their extensive broadband HFC footprint. MSOs in many parts of the world are already generating a substantial amount of revenue by backhauling traffic from macro cells, and the potential exists to do the same for small cells. Where the MSO story is especially compelling, is where they have aerial plant as they can provide not just broadband backhaul but also site acquisition and power. There is no other scenario where the outdoor small cell deployment path is as clean as when there is aerial cable plant. Other outdoor deployment options usually include light poles, traffic lights, sides of buildings, bus stops, phone booths, etc.

The first step in enabling a hosted small cell service for an MNO is to deploy high-end DOCSIS compatible strand mounted Wi-Fi APs on the aerial plant. Many MSOs are already well down this path with extensive strand mounted Wi-Fi deployments. If the right Wi-Fi APs are deployed, it becomes very straightforward to then go back and add small cells. These devices can be directly attached to the Wi-Fi APs, which provide backhaul and power. A good choice here is the Ruckus ZoneFlex 7781cm, which is a dual-band, 3-stream, DOCSIS 3.0 AP that has been environmentally hardened and can supply PoE (power-over-Ethernet) for a small cell. By focusing on a mechanical attachment instead of integrating the radios together at the circuit board level, it becomes much easy for the MSO to deploy the small cell that is preferred by the MNO partner. Options here include small cells from the major RAN vendors as well as small cells from a variety of smaller vendors. The small cells will connect to the DOCSIS enabled AP via Ethernet, which will backhaul data traffic and provide power to the unit (PoE). This saves the cost and expense of having the small cell vendor integrate a DOCSIS modem into their unit. The same unit that might be deployed on a light pole or the side of a building can also be used on an MSO cable strand (Figure 7 and Figure 8).

Figure 7 Strand mounting a Wi-Fi AP and a small cell

Figure 8 Light pole mounting a Wi-Fi AP and a small cell

One of the advantages in deploying small cells off of a Wi-Fi platform is that it allows the MSO to sell a managed small cell service to all the MNOs in an area. This is possible because a small cell will transmit over a much greater distance than a Wi-Fi AP. The latter is usually good for about 100 meters and the former could easily go 500 meters or more depending on output power. This means that a particular MNO may only need to attach to every 5 Wi-Fi APs in the MSO network leaving the other 4 to accommodate other MNOs.

When deploying is areas where there is no overhead plant, the options for site acquisition, power, and backhaul are much more challenging. A great mounting asset in an urban street canyon without overhead plant are street lights. These are always found in downtown city centers, and they have AC power (in many cases they are always hot).

Clearly there is a lot of value in the convergence of these two radio technologies, but what are the impacts on the network? In Figure 9, we see how the different functions are handled back in the network. The Wi-Fi AP passes Wi-Fi traffic back to the SCG in the MSO core, and the small cell communicates with MME and Serving Gateways in the MNO's core network. The two cores are parallel and owned by different operators. They only come together out on the strand.

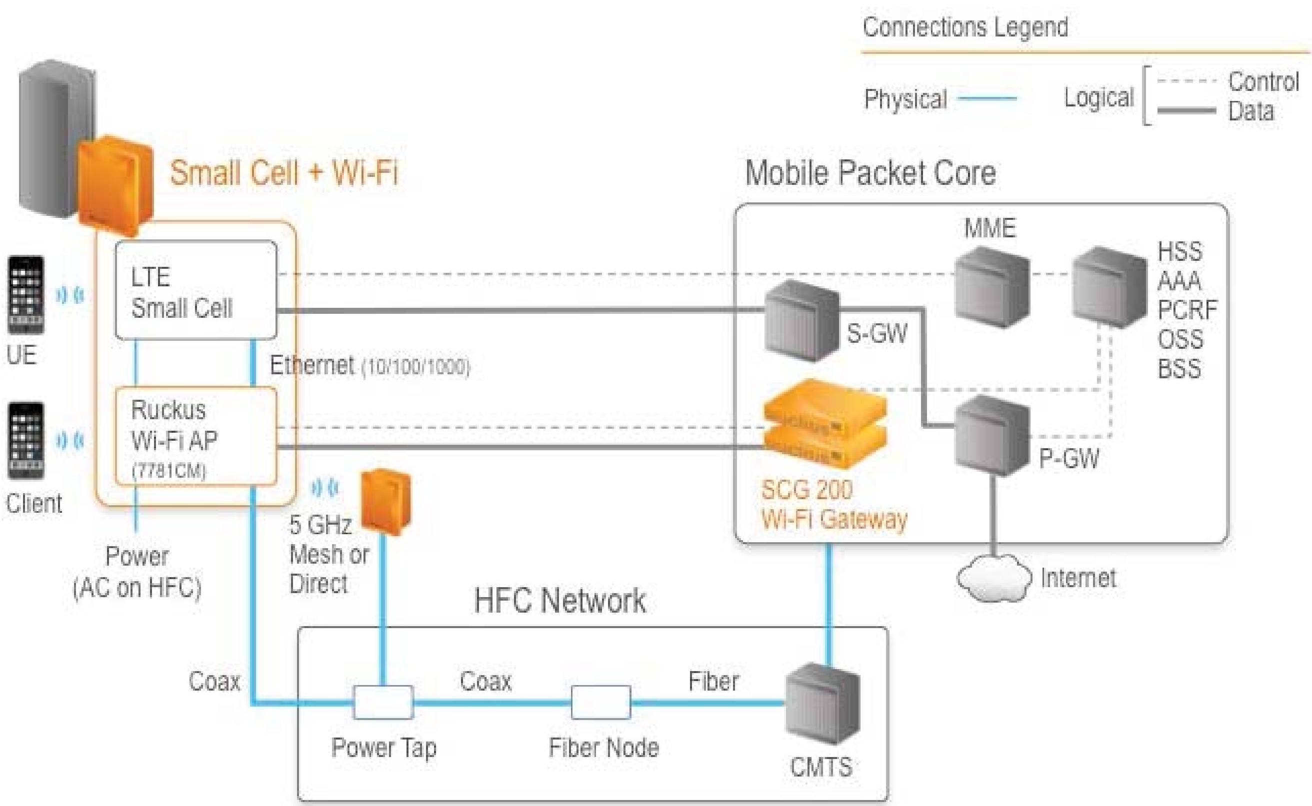

Figure 9 Small Cell access and core network

Updates and Upgrades for Backhaul Networks of Public Wi-Fi Systems

MSOs want to have one network and service management platform that is access network and vendor agnostic while innovation can continue at every aspect of the system. Software defined networks and network virtualization are ongoing related work for data centers and provider networks. Service providers', especially cable operators', networks and systems are very different than data centers. Based on cable operator's current status and future requirements, an evolutionary strategy with planned transitions and hybrid structures is preferred. MSOs can leverage their existing hardware/firmware assets while integrating new solutions with appropriate interfaces and APIs [1].

While MSOs make transition to the next generation networks and service platforms, services to support and resources to allocate based on specific business models will determine the strategy. In this and following sections, we will focus on two aspects of backhaul and back-office systems that will interact with Public Wi-Fi networks. We will discuss converged edge router and multi-screen video platform solutions that will help service providers to better integrate and benefit from Public Wi-Fi networks. Both converged edge router and multi-screen video platforms share common design features that will enable combined and hybrid solutions while some of the functionality may be virtualized and abstracted. The transition will depend on functionality and effective way to provide it (e.g. as a headend firmware vs. cloud operation).

The support for new services and higher bandwidth demand of subscribers shape the future of HFC networks. Public Wi-Fi networks had limited impact due to relatively low bandwidth cap deployments and best effort data delivery. However, the impact will be bigger as deployments and roaming models are changing, higher bandwidth Wi-Fi access is available and new tiered services may be offered.

As discussed in the previous sections, higher bandwidth and more flexible service integration are available with new Wi-Fi hardware and functionality. Similarly, higher bandwidth and flexible network and service support are also targets for current HFC access and headend network components, including converged edge routers (Figure 1).

Today, IEEE 802.11n APs integrated with 8x4 CMs are being deployed for outdoor metro and hotspot networks. With IEEE 802.11ac, CMs with more channel bonding will be used (24x8 is available today). MSOs can upgrade their CMTS with the system that has higher channel bonding capability when their HFC network usage (including subscriber home, business, community and Public Wi-Fi) requires the transition (Figure 2).

The next step would be to change to multiservice platforms (such as CCAP and CER) [5] that can support HSD, VoIP, VoD, SDV and IP Video over a unified network (Figure 2). The main advantages are:

- Having video and data over a unified network enables less expensive and more effective resource, network and service management: Today, Cable Wi-Fi bandwidth planning, resource and network management are handled separately. The new platform will enable better integration of management components and support for differentiated traffic treatment for Public Wi-Fi services. Service types may be mixed to increase network utilization while meeting service quality requirements.
- Higher bandwidth with less cost (more channel bonding): Both best effort with higher bandwidth (e.g. IEEE 802.11ac) and carrier grade services (e.g. video, voice over Wi-Fi) may be supported. MSOs may continue to deploy networks with higher DOCSIS 3.0 channel bonding on new multiservice platforms and make a transition to new access options such as DOCSIS 3.1.
- Transport agnostic (e.g. DOCSIS and EPON): Carrier Wi-Fi nodes with coax and fiber backhauls may be deployed and served from the same platform for different deployment models.
- Common design objectives with video and subscriber management platforms: This will facilitate integrated policy and charging for Wi-Fi traffic and dynamic service provisioning
- Ready for IP migration: MSOs can start by combining QAM, HFC and IP on the same platform while converging to IP. More provider’s services will be available for multiple devices over Wi-Fi networks.

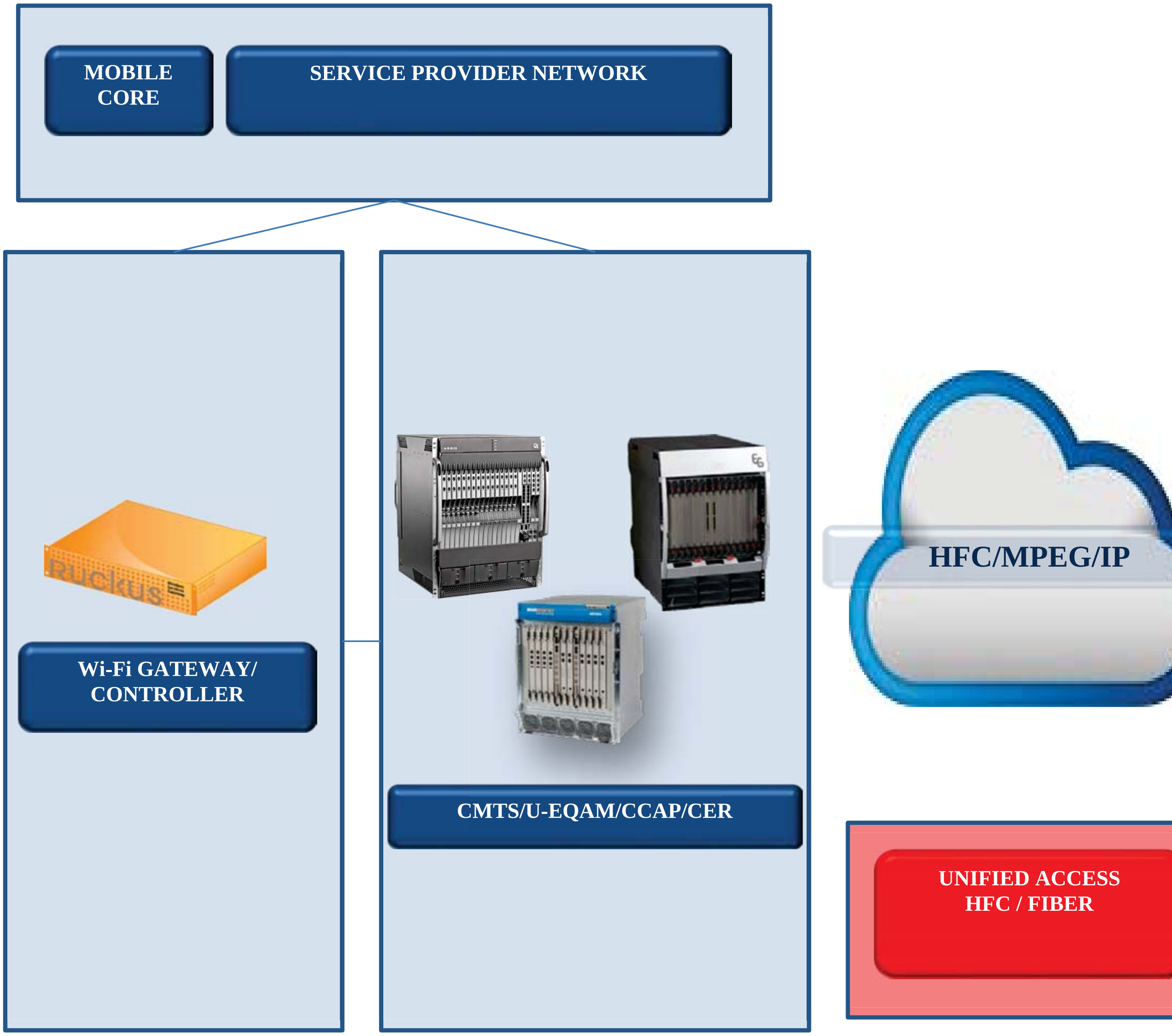

Figure 10 Access backhaul options with CMTS Edge Router Evolution

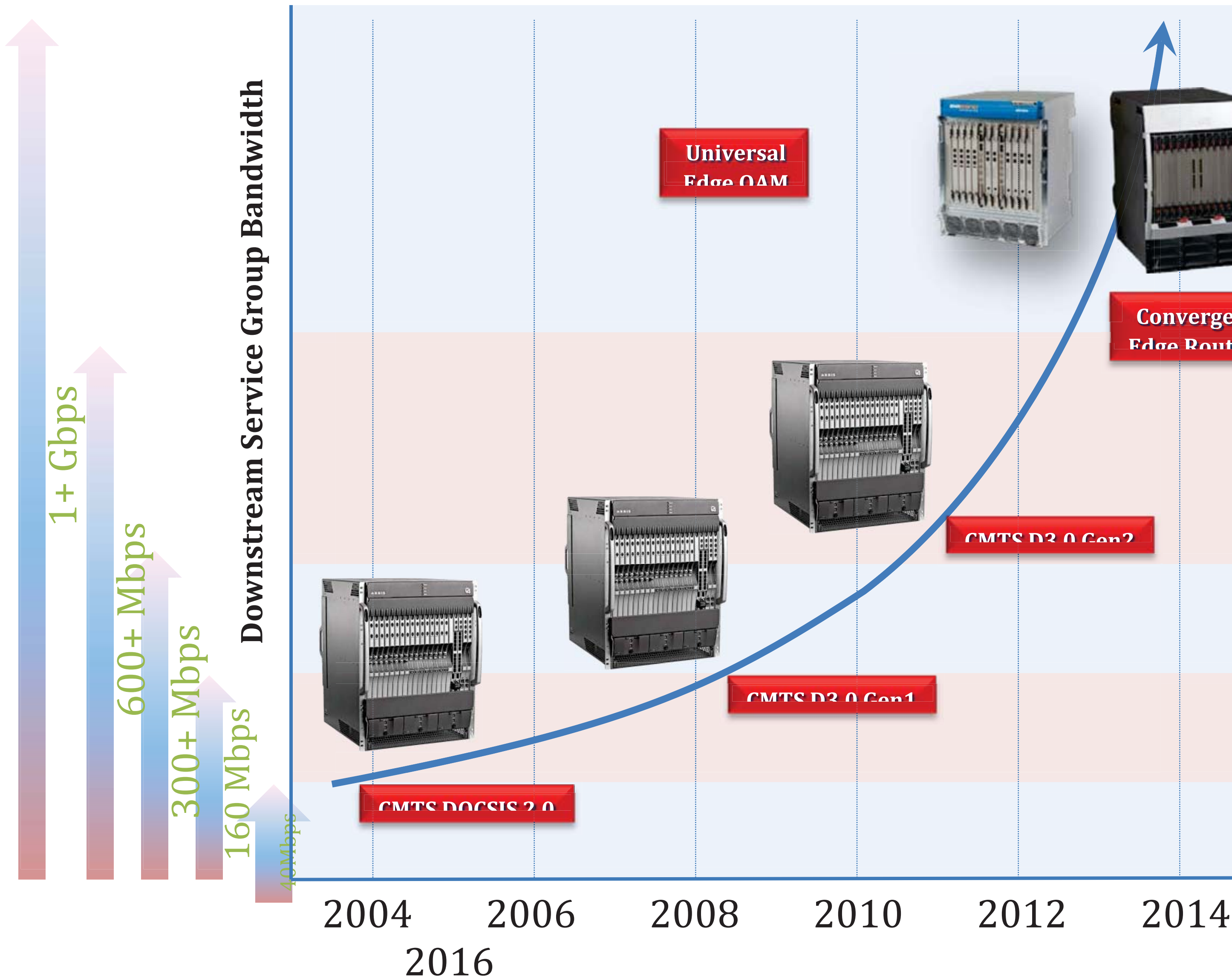

Figure 11 CMTS Edge Router Evolution

Video over Public Wi-Fi Systems

Today, most of the existing Cable Public Wi-Fi networks offer best effort data as a free service to subscribers or with fixed plan rates to non-subscribers. However, MSOs aim to extend their Wi-Fi services as a result of recent deployment successes and proliferation of new Wi-Fi devices and applications. Voice and video over Wi-Fi are services of interest for both service providers and end users. Video applications may include managed video and premium content from live channels and VOD (along with bundled services), OTT video, mobile video offload and local streaming (e.g. local news streaming).

Subscribers recently started to enjoy live programming and video on demand content when they are away from home. There are crucial network and service features that impact the extension of TV Everywhere:

- User authentication and content protection: Digital Rights Management, robust authentication and secure content delivery must be provided in a way where the user can have a unified, simplified and seamless sign on for multiple platforms while content piracy and theft of service are prevented.
- Access to content: Interactive, personalized and fast means of finding and discovering content on multiple devices must be provided.
- Carrier Video Quality of Experience: Consistent quality adapted to multi-screen viewing in dynamic environments (e.g. Wi-Fi networks with different interference and congestion levels) and networks (e.g. MSO's home and partner's visited networks with corresponding SLAs) must be provisioned. This also requires effective monitoring and diagnostics solutions.
- Integrated policy and charging functionality: Usage/time based policy management and charging must be provided for tiered services including recording at visited networks.
- Business intelligence and user behavior analytics: Correlating content, user, device, location and time and large scale data mining for advertising and other location based services.

The solution is a combination of network and service platforms including multi-screen video platforms, Carrier Wi-Fi networks and unified backhaul, service and backoffice management. Figure 3 displays the main system blocks of the solution.

In Figure 3, video user may be a subscriber at home or away from home or a roaming partner's subscriber with multiple device options. HFC / Wireless access components include Carrier Wi-Fi nodes (AP + CM) or small cells connected to CMTS/CCAP/CER over HFC networks. Traffic is mostly tunneled (except for home users) to a wireless controller and/or mobility gateway that terminates the secure tunnel and may be also connected to mobile core network. Wireless controllers also manage and provision APs. CMTS/CCAP/CER is connected to the headed network and may also be connected to PCMM network components [2],[3] for dynamic wireless services. Traffic from the wireless controller is directed to an access controller with differentiated connections (e.g. VPNs) for different services. Access controller may be the policy enforcement point (can be integrated within wireless controller / mobility gateway) that communicates with service and subscriber management platform. Service and subscriber management platform includes both wireless and video services. For wireless services, interfaces to partner MSOs backoffice (e.g. through proxy AAA) and mobile core network (e.g. SIM servers) may exist. Video access and management components are shown in Figure 4.

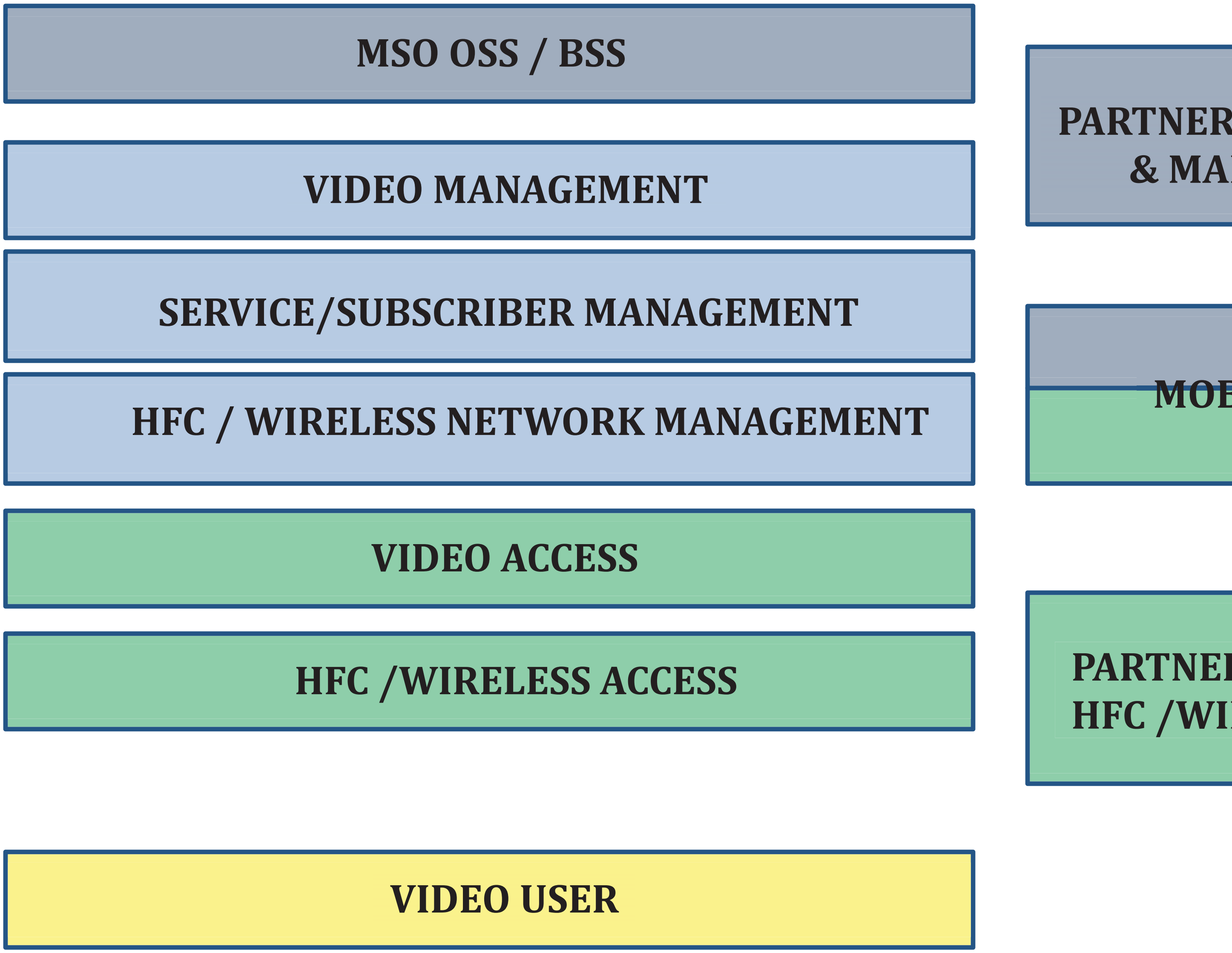

Figure 12 Main system blocks of managed video over Wi-Fi networks

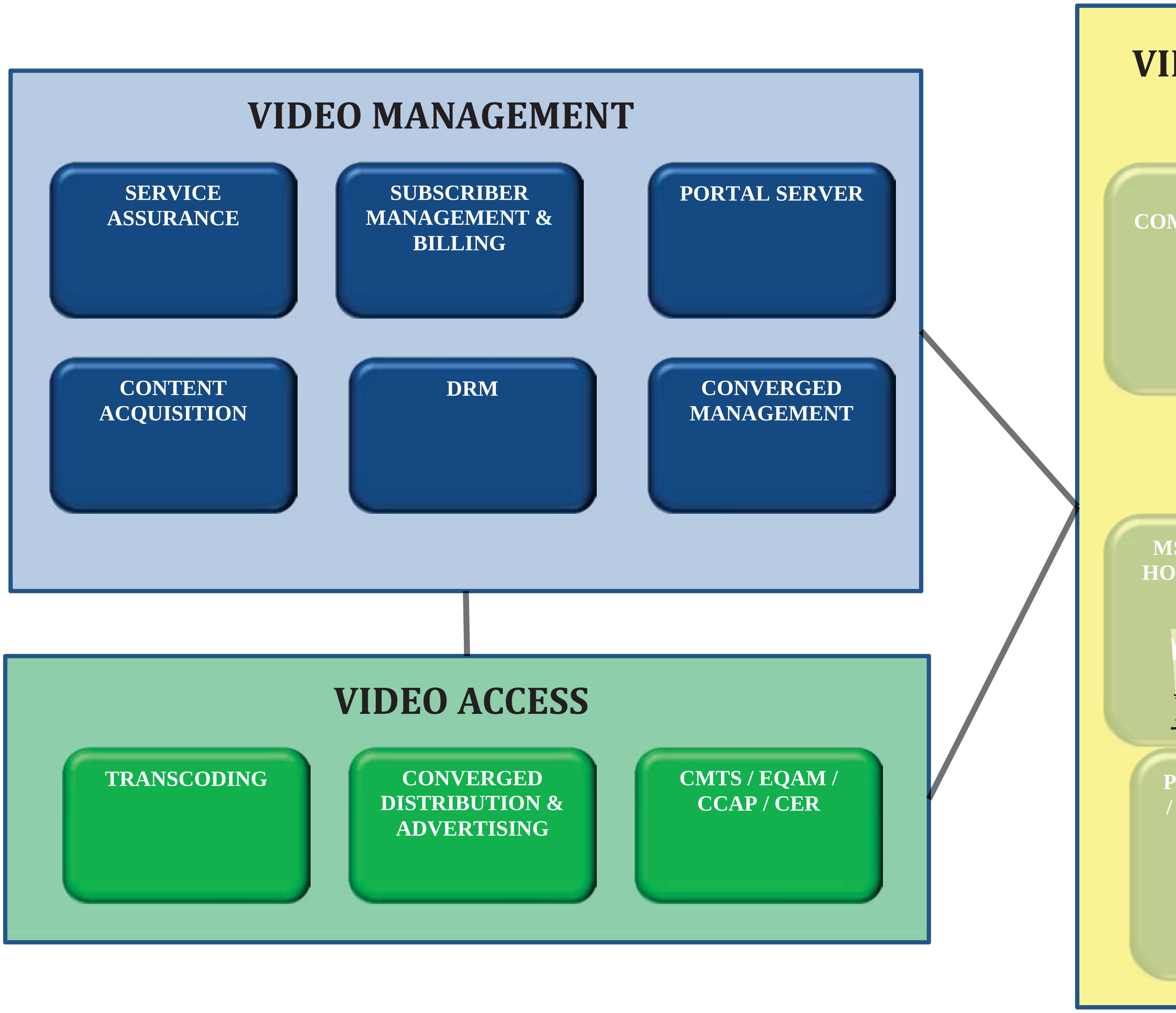

Figure 13 Video management and access network blocks

The solution architecture blocks in Figure 3 must meet service providers, programmers and end-users' requirements. Users want to access both networks and services seamlessly anytime, anywhere and with any device. Although home users and on the go user cases have similar device and service requirements users in metro/hotspot Wi-Fi networks have different mobility and handoff cases. The solution should cover both seamless network transition and service continuity depending on the deployment. As discussed in section X, Public Wi-Fi networks enable users to seamlessly roam between partner providers' networks and handoff between same (e.g. AP to AP) and different access technologies (e.g. Wi-Fi and 3G/4G). Similarly, users want to find, access and display content seamlessly and easily without dealing with multiple apps/plug-ins, players and logins depending on the device. Video management and access components shown in Figure 4 enable optimization of video streaming for the end device while integrated wireless service management ensures end-to-end quality provisioning and service continuity. Both network components (e.g. APs) and subscriber authentication must be provided. Carrier Wi-Fi nodes are authenticated and wireless traffic is protected through secure tunnels as explained in section [X]. In addition, secure video service access and delivery and DRM solutions with integrated subscriber management ensure the wireless users' credentials and video rights.

Due to different channel and usage characteristics (e.g. interference and congestion levels), QoE provisioning in metro/hotspot Wi-Fi networks has different requirements than home Wi-Fi networks. Increased bandwidth (i.e. IEEE 802.11ac as discussed in section [x] and new CMTS/CCAP/CER and CMs as discussed in section [y]) along with new video compression techniques (e.g. HEVC) are promising better video quality. However, due to high dynamics of public Wi-Fi networks, interference mitigation, congestion control and WMM functionalities are crucial. On the HFC network side, static or dynamic QoS may be provisioned (e.g. through COPS protocol between CMTS and policy server) [3]. Carrier Wi-Fi nodes along with subscriber management can classify the traffic based on interface, MAC/IP addresses, IP protocols, port numbers, heuristics and different policies can be applied based on classification per SSID, tunnel, VLAN , TOS.

In most Cable Wi-Fi systems, cable and Wi-Fi segments are separate in terms of network and resource management. However, services like carrier quality video require end-to-end control over heterogeneous networks which may be very different in nature in terms of resource dynamics. The heterogeneous networks require QoS mapping at the network boundaries for service and session continuity. Therefore, service management has to make sure wireless, HFC access and backhaul networks are configured and policies are enforced seamlessly. This may require deeper packet inspection at network segments. End-to-end resource management is a challenge in terms of supporting high quality user experience while maximizing network utilization. Since the user may be visiting roaming partner's network, appropriate SLAs must be provisioned for video services. This issue is specific to Public Wi-Fi networks and users may observe quality degradation without realizing he/she is in a visited network as authentication and handoffs are seamlessly made. Due to this issue and the fact that Public Wi-Fi networks have higher dynamics, traditional video streaming protocols may not be adequate. Complexity is another issue as ideal resource management for Cable Wi-Fi systems would require real time analysis and monitoring of Wi-Fi links, which may not be always feasible.

Air-time fairness in Wi-Fi access networks is an important feature for medium sharing. However, MAC, network/IP and application level interactions and different backoff and rate adaptation mechanisms adopted at each level makes harder to control the overall video quality. Today client based adaptive bit rate video applications are widely used, among them HTTP Live Streaming (Apple – HLS), Internet Information Services – Smooth Streaming (Microsoft – HSS), and HTTP Dynamic Streaming (Adobe – HDS) as de-facto industry standards and MPEG Dynamic Adaptive Streaming over HTTP (MPEG-DASH) as the standardized adaptive streaming specification. While these protocols work better on dedicated mediums they may create unfairness, instability and poor utilization without being able to differentiate the problem (congestion vs. channel errors and channel access problems due to greedy users/applications). In shared mediums, end-user devices can not have the full network view and differentiation of problem cause is much harder. However, they are a good indicator when end-user/device is experiencing problems. The overall control protocol should adapt to user's video application requirements (e.g. bit rate per screen for a specific video), access and backhaul link conditions, user policy and device specific applications (such as client-based adaptive rate streaming). Network based adaptive bit rate algorithms are more appropriate for Public Wi-Fi networks with a central view of end-to-end network resources [4]. However, having an accurate view of the network in a timely manner and differentiate location and device specific issues is a big challenge. Especially, diagnostics and monitoring during roaming to visited networks will be broken Therefore, a more optimized solution is a network based adaptive resource management system that is assisted with client based adaptive rate algorithms for carrier quality video transmission over Cable Wi-Fi systems.

An integrated policy and charging functionality will enable MSOs to monetize video over Public Wi-Fi networks. MSOs may choose usage or time based policies at both home and visited networks depending on their business models.

Business intelligence and user behavior analytics at both wireless and video management side are required for MSOs to benefit from their video services over Public Wi-Fi networks. Wireless data help the service providers for optimization and planning of both network and services. Integrated wireless and video usage data will help MSOs to correlate content, user, device, location and time for advertising and location based services. This in turn would help both MSOs and programmers to secure rights agreements based on solid business models. While home users analytics are used for personalization of services, Public Wi-Fi networks in addition have localized and aggregated content and behavior intelligence that open new doors for location based business opportunities (e.g. advertisement, mobile offload, advanced retail applications etc...).

Conclusions

Wi-Fi deployments represent a great opportunity for the world's MSOs. It allows them to leverage their extensive broadband HFC networks as well as aerial plant where it exists. The business opportunities from that point on are many and varied and usually start by increasing customer stickiness and build from there.

The key elements that are required for a successful deployment usually start with reliable RF connectivity.

- Reliable Wi-Fi connectivity based on adaptive antenna technology can provide increased signal gain toward the user, and greater interference mitigation. This technology has been proven in carrier deployments and 3rd party testing all over the world. Adaptive antennas are only the beginning.
- Hotspot 2.0 technology will have a huge impact on Wi-Fi networks as it makes the process of roaming a seamless, automatic, and secure as with cellular. The MSOs have already made great strides here in the roaming consortiums that they've formed in the US market. With Hotspot 2.0 that approach becomes infinitely extensible as now the world of roaming can include operators, enterprises, and public venues of all types and from all geographies.
- A scalable network architecture that can also scale in its ability to provide network services. Such an architecture should also encompass licensed small cells as they emerge. Wi-Fi and small cells will combine to bring huge amounts of data traffic back into the network. The surge in data demand is only beginning (Figure 14).

For more information on the Ruckus SmartCell Architecture please visit [6].

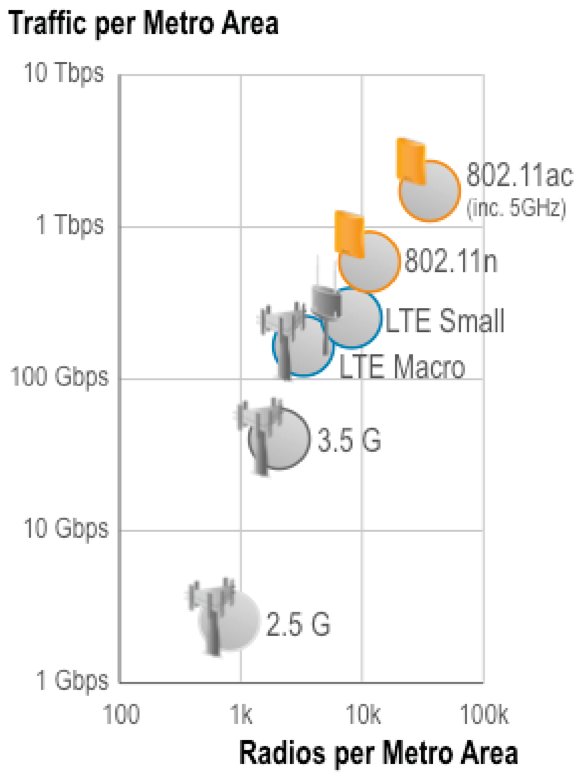

Figure 14 Wi-Fi traffic Volumes

MSOs will benefit from integrated solutions that combine innovative Wi-Fi and HFC access, subscriber/service management and multi-screen video platform solutions. The integration will enable MSOs to offer new services over Public Wi-Fi networks while transitioning to higher bandwidth networks, IP transport and unified network and service management systems.

Bibliography

[1] Nandiraju Nagesh, Ozer Sebnem, "Applying the Software Defined Networking Paradigm to MSO Commercial networks", The Cable Show - NCTA 2013", June, 2013

[2] CableLabs Wi-Fi Specification, "Wi-Fi Requirements for Cable Modem Gateways", WR-SP-WiFi-GW-I02-120216

[3] Cable Europe Wi-Fi Specification, "Cable Wi-Fi projects; Public Wi-Fi Services", CEL-TR-WIFI-V1.1

[4] Howald Robert, Ozer Sebnem, Nandiraju Nagesh, "Delivering Pixel Perfect", The Cable Show Spring Technical Forum, May, 2010

[5] Emmendorfer Michael, Cloonan Tom, "Examining the Future Evolution of the Access Network", 2013 Spring Technical Forum, June 2013.

[6] www.ruckuswireless.com

Abbreviations and Acronyms

AKA	Authentication and Key Agreement
AP	Access Point
CCAP	Converged Cable Access Platform
CER	Converged Edge Router
CM	Cable Modem
CMTS	Cable Modem Termination System
DOCSIS	Data Over Cable Service Interface Specification
EAP	Extensible Authentication Protocol
GRE	Generic Routing Encapsulation
HLR	Home Location Register
HSS	Home Subscriber Server
MNO	Mobile Network Operator
MSO	Multisystem Operator
QoE	Quality of Experience
RADIUS	Remote Access Dial In User Service
SIM	Subscriber Identity Module
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security