ARCHITECTUAL APPROACHES FOR INTEGRATING SP Wi-Fi IN CABLE MSO NETWORKS

Rajiv Asati, Distinguished Engineer, rajiva@cisco.com
Sangeeta Ramakrishnan, Principal Engineer, rsangeet@cisco.com
Rajesh Pazhyannur, Technical Leader, rpazhyan@cisco.com

Abstract

Cable MSOs have an enticing opportunity with Wi-Fi residential and business services.

In this paper, we discuss the common requirements, challenges (that Cable MSOs face) and necessary architecture (that MSOs could use) for integrating SP Wi-Fi in Cable MSO networks to support both residential and hotspots use-cases. This paper also qualifies various architectural approaches for network transport in the context of DOCSIS access along with the time-to-market perspective, so as to enable MSOs to quickly capitalize on this opportunity.

1. INTRODUCTION

Wi-Fi is a pervasive & proven access technology that is commonly used by Homes and Enterprises around the world, and its usage by Service Providers (SPs) is gaining traction as well. SPs can use Wi-Fi to deliver one or more of the triple-play services (e.g Video, Voice, Data) to the customers indoor and outdoor, and enhance the customer/user experience (by allowing mobile consumption of content as well as access to data).

In fact, SPs, particularly, Mobile SPs have been leveraging Wi-Fi for better cost-efficiency and QoE. As the number of mobile devices keeps growing exponentially, it is expected that the Mobile network traffic would keep growing exponentially as well (studies have predicted a 18-fold increase in mobile data traffic in the next 5 years, as illustrated in `Figure 1`).

There will be 5B mobile devices and 2B M2M nodes
Global mobile traffic wil grow 26X to 6.3 EB/mo
Video will be 66% of all mobile traffic by 2015
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Cor

Source: Cisco Visual Networking Index (VNI) Global Mobile Data Forecast, 201

Unfortunately, most mobile SPs do not have enough licensed radio spectrum to accommodate this increase. Given that a large amount of traffic is consumed indoors (in homes, offices, public-spaces like hotels, café's, etc), where Wi-Fi connectivity is much more widely available than cellular, the usage & focus on Wi-Fi to offload traffic from cellular networks has greatly increased. In fact, 'Mobile Data Offload & Onload Video Whitepaper (published by Juniper Research in April 2011) predicts that Wi-Fi usage for mobile traffic offload could exceed ~1EB / month by 2015. This is illustrated in `Figure 2`.

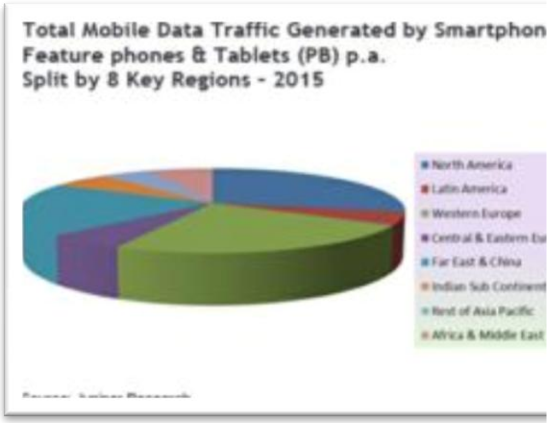


Figure 2 Mobile Traffic offload Prediction

Needless to say, Mobile SPs would need to acquire sites for installing Wi-Fi based macro-cells, and hence, mobile SPs are increasingly motivated to rely on other SPs/Providers offering the Wi-Fi based solutions.

Cable MSOs have a fantastic opportunity with Wi-Fi. In this paper, we discuss the common challenges (that Cable MSOs face) and necessary architecture (that MSOs could use) for integrating SP Wi-Fi in Cable MSO networks to support both residential and hotspots use-cases. We also qualify various architectural approaches for network transport in the context of DOCSIS access along with time-to-market perspective, so as to enable MSOs to quickly capitalize on this opportunity.

2. SP Wi-Fi: MSO REQUIREMENTS / CHALLENGES

SP Wi-Fi primarily refers to an 802.11 Wi-Fi system deployed and managed by a Service Provider (SP) for public access (aka community access) to its network for services such as High Speed Data Internet service. Public Access means that Wi-Fi is available to the customers of the SP and/or partner SPs and/or any customers. SPs may provide managed (and sometimes hosted) Wi-Fi services to other service providers (e.g. Mobile SPs).

SP Wi-Fi differs from general Wi-Fi e.g. Enterprise Wi-Fi (or Residential Wi-Fi) in three key aspects:

1. **Scale** – The number of APs and user clients tends to be very large – thousands to millions.
2. **Carrier Grade** – The high-availability and manageability aspects tends to be of carrier class (e.g. 5 9's)
3. **Multi-Vendor** – The existence of multiple vendor devices is expected – warranting the usage of standards based end-to-end architecture.

2.1 Use-Cases

SP WiFi architecture should be flexible enough to enable Cable MSO to serve one or more the following deployment use-cases:

1. **Residential** (Indoor) –re-use the Wi-Fi APs that are integrated with the (SP managed) residential gateways to provide public access Wi-Fi. In this case, the AP is located indoor (in a residential customer home).
2. **Metro** (Outdoor) –deploy Wi-Fi APs outdoor in public places to provide public access Wi-Fi. In this case, the APs are typically mounted on aerial cable strands, street-poles, roof-tops etc.
3. **HotSpot / SMB** (Indoor) –re-use the managed Wi-Fi service to SMBs such as coffee shops, bookstores, retail-stores etc., having 10s or 100s of employees, for both private and public access WiFi.
4. **HotSpot** (Outdoor) –deploy large concentration of APs in a relatively small area such as stadium, amphitheaters, parks etc. having large number of users in that area. The APs are usually located outdoor to offer public access Wi-Fi.

5. **Wholesale / offload** – allow partners' customers to access the Wi-Fi services, and/or backhaul mobile operators' customers traffic over the MSO infrastructure. In this case, the APs are located indoor and outdoor.

2.2 Access Point / 802.11 Radio

Access Point (AP) is the most fundamental element in the SP WiFi architecture. Hence, the AP requirements must be carefully assessed. The following are some of the key considerations for the Wi-Fi AP:

1. Coverage: refers to AP's range to = what throughput upto what distance. Coverage determines the number of APs required to cover a certain area. Naturally, 802.11n radio on AP is preferred for optimal coverage.
2. Capacity: refers to the maximum number of clients that AP can concurrently support/associate. Some prefer to define capacity in terms of maximum number of active users that can be supported with each user guaranteed a minimum throughput. Capacity directly influences the number of APs required to cover a certain area (e.g. the number of APs are determined by capacity requirements rather than coverage).
3. Interference Management: refers to AP's capability to continuously select the best radio channel (through constant monitoring since startup) while managing the radio interference so as to get the best radio performance. The interference could be generated by other Wi-Fi APs or by non Wi-Fi sources such as Bluetooth, DECT phones, Microwave etc. Naturally, techniques such as Beamforming to improve the signal strength received by the client, interference identification for reporting etc. become important.
4. Dual radio– refers to AP supporting simultaneous usage of 2.4GHz and 5GHz. This is particularly important for APs that are used for creating private and public WLANs. This should be controllable by the MSOs.

2.3 Security

Security is one of the most-pressing issues, as security threats such as snooping, Eavesdropping, session hi-jacking, session side-jacking, evil twin attack etc. expose the insecurity in WiFi networks that rely on open SSID. Hence, it is important to have secure SSID/WLAN.

Note that most SP Wi-Fi deployments have not used secured SSID because of lack of support on clients for EAP methods and/or complexity in distributing and managing user-security credentials. Hopefully, this will change with Hotspot2.0 recommendations. Please see more details on this here [Hotspot2.0].

Additionally, in case of residential SP WiFi, the AP must support at least one private WLAN/SSID for the residential customer's usage, and at least one public WLAN/SSID for public usage, for security reasons.

In summary, SP WiFi architecture should include user authentication and cryptography (e.g. WPA-2 Enterprise), as well as separate control and management of public and private WLANs so as to pave the way for 'Secure WLANs'.

2.4 Inter-Operator Roaming

It would be desirable to let the users use other MSOs' or SPs' Wi-Fi networks to get one or more services (such as high speed data connectivity to the Internet) when the users are roaming [Wi-Fi-Roam]. However, how would the customer's device know the right SSID (assuming more than one SSIDs) on the partner Wi-Fi network? If the users knew the right SSID, they may have to manually login and get authenticated so as to use partner Wi-Fi network. This is deemed not only inconvenient to the user, but also as a lost opportunity for the MSOs to influence users' network selection.

Once authenticated, then depending on the mobility requirement, home network or the partner network should assign the IP address to the user client device. If the roaming users managed to use partner Wi-Fi network, then they may get limited time before they are asked to re-authenticate, causing them another source of inconvenience. Lastly, as MSOs allow the roaming users, appropriate billing ruleset, Lawful Intercept etc. have to be enforced. Of course, this all assumes the MSOs to have struck the roaming agreements with other MSOs & SPs.

To address this challenge, IEEE 802.11u could be necessitated. Please see more details on this here [Hotspot2.0].

2.5 Mobility

Mobility is defined in many different ways, resulting in many different requirements. However, MSOs may not find all the mobility requirements to be important and/or applicable. A brief summary of mobility requirements is provided below:

- Fast Roaming: enables AP-to-AP handover user re-authenticate the user. Specifically, the re-association procedures are performed in parallel with key negotiation procedures, as per IEEE 802.1r.
- Micro-Mobility: In deployments with a small number of APs in a site (such as bookstore, restaurant) there is need to support mobility to reduce adverse impact on end user experience as they roam within the site. In most scenarios, when user walks out of the site, they will lose Wi-Fi coverage. Reconnecting to Wi-Fi in another location/site would typically result in users getting a different IP address.
- Macro-Mobility: In deployments where there is large contiguous area covered by Wi-Fi (such as outdoor APs) there is need for end users to maintain IP address as they roam between Wi-Fi APs. In such cases, the solution may need tunnels between centralized Wi-Fi aggregators (WLC, CMTS, MAG, etc) to provide this form of mobility
- Inter-Vendor Mobility: As mentioned earlier, SP Wi-Fi deployments tend to comprise network elements e.g. APs from different vendors, hence, it is important to ensure that mobility works between different vendors' APs. Further, in some scenarios, the vendors may provide overlapping Wi-Fi coverage.
- Inter-Technology Mobility: A significant portion of Wi-Fi devices are likely to have a cellular (3G/4G radio) as well. In some cases, it may be desirable to provide mobility as users roam between radio-technologies (between Wi-Fi and Cellular). Such mobility can be provided by using client based mobility mechanisms (Mobile IP, DSMIPv6) or network based mobility mechanisms (such as PMIPv6)..

While many of the above requirements may be reasonable, it is worth noting that continuous Wi-Fi coverage is a prerequisite of any form of mobility. Hence, mobility may not be possible everywhere or applicable, requiring careful justification.

2.6 Traffic Separation

As SP WiFi traffic is transported over the MSOs network infrastructure, traffic separation capabilities in the network especially on the access (e.g. DOCSIS) side will become critical.

2.6.1 Separation of HSD subscriber's traffic from SP Wi-Fi traffic

Most operators have bandwidth caps and tiers of service deployed whereby each subscribers' traffic is separately measured (for bandwidth cap purposes) and QoS is applied to ensure the traffic complies to the tier of service the user has subscribed to (example, 6Mbps down, 1Mbps up). Once the cable modem deployed at a business or home, is enabled for SP Wi-Fi, operators will want to ensure that the SP Wi-Fi users' traffic does not count towards the HSD subscriber's limits. Given that in DOCSIS the Service Flow is the unit on which accounting and QoS is applied, the architecture needs to ensure that the SP Wi-Fi traffic is mapped to a different service flow than that of the subscriber's HSD service flow. This mapping needs to be done both in the Upstream and Downstream directions.

An implicit challenge here is that needing specific US and DS classifiers may result in having unique CM config file for each modem. The chosen architecture must address this challenge.

2.6.2 Separation of Services per Fiber Node

The previous section discussed the separation of a single HSD subscriber's traffic from the SP Wi-Fi users attached to the same CM/AP. Additionally operators may want to ensure that a certain amount of bandwidth is set aside for HSD use versus SP Wi-Fi use across the entire Service Group. This would ensure that one service on an aggregate doesn't crowd out the other service on a Service Group. It would also be beneficial if any unused bandwidth provisioned for one service was made available for the other service to use as needed.

DOCSIS provides the Bonding Group construct which can be used to provide such a service separation between the two services. By using overlapping bonding groups across a set of RF channels, and steering HSD service flows to one Bonding Group and the SP Wi-Fi service flows to the other bonding group, operators can achieve such separation. Depending on how much bandwidth an operator wishes to set aside for each service, they can configure the bonding groups appropriately to achieve their goals.

2.7 Network Transport

SP WiFi services may need to be deployed over various types of access networks e.g. DOCSIS/HFC, EPON/Fiber etc. that are present in MSO networks. For example some operators are considering offering business services over EPON. The overall architecture chosen for deployment will need to be such that they are easily deployable across different access technologies. Hence the Access Point itself will need to support various backhaul technologies such as DOCSIS, EPON etc.

For utmost cost-effectiveness, it would be desirable to leverage the IP or MPLS (or 802.1 based carrier Ethernet) network transport that is already used by MSOs for other services. In fact, many MSOs have converged their networks (or on the path to do so) and been using MPLS technology for various services. The key is to choose the network transport that yields the simplification of SP WiFi architecture while satisfying other SP WiFi requirements that are important to the MSO.

2.8 Provisioning & Management

In particular, the WiFi APs should be automatically configured without needing any manual intervention for utmost cost-effectiveness (given the expected scale).

Thankfully, both DOCSIS cable modem and eDOCSIS[1] device already allows auto-

[1] An eDOCSIS device consists of an embedded DOCSIS cable modem (eCM) and one or more embedded Service/Application Functional Entities (eSAFEs) such as eAP, eRouter, eSTB, eMTA etc. There are already various vendors' eDOCSIS devices

configuration of cable modem (and DPOE allows auto-configuration of ONU) and integrated AP. Moreover, eDOCSIS device, by definition, has a single software image for the entire device.

However, if the chosen SP WiFi architecture requires each modem to rely on a unique config file, then it could become a provisioning challenge (as MSOs generally use a few cable modem config files across tens of thousands or millions of modems. This challenge can be solved if template based cable modem config file generation method is used.

For residential SP Wi-Fi deployments in particular the number of APs may well be as high as the number of deployed cable modems. Hence being able to provision at scale is critically important.

Needless to say that CMTS provisioning should not be needed on a per modem basis.

In summary, seamless integration of the WiFi provisioning (e.g. AP provisioning) into the existing provisioning infrastructure is going to be required for possible auto-provisioning of APs.

2.9 Subscriber Management

Like other services, SP WiFi services will also require subscriber management. This may include capabilities such as bandwidth accounting, quality of service, legal intercept etc. Such services will require a policy enforcement engine that is subscriber aware and learns the policies to be applied from a policy management system. All SP WiFi traffic will have to be routed through such a policy enforcement engine in order to provide the above-mentioned subscriber services.

Subscriber management could occur centrally in which case all traffic needs to be routed to the Subscriber Management Gateway. Different options are available to achieve this, and are discussed in more detail in the Transport Network section 4.1.

It is worth noting that for HSD services, such subscriber management capabilities are applied at the CMTS, hence no requirements to route HSD traffic to any other central entity really exist in MSO networks.

2.10 IPv6

Given the IPv4 address exhaustion becoming a reality for many MSOs & SPs sooner or later and given that SP Wi-Fi would involve 10,000s of APs and millions of users, it is imperative to have IPv6 in SP Wi-Fi usage from day 1. This means that IPv6 should be used not only for addressing users, but also for the underlying infrastructure (e.g. APs, CMTSs, PEs, etc.) irrespective of any IP tunneling is used or not. In other words, both user and AP addressing should be done using IPv6.

While using IPv4 is an option, MSOs would end up requiring many more bandaids (e.g. Carrier Grade NATs) to make it work in a large-scale environment, thereby negatively impacting CAPEX and OPEX associated with SP Wi-Fi.

2.10 Monetization

Once the basic SP Wi-Fi services (e.g. high speed data) get rolled out for the purposes such as customer retention, MSOs may increase the focus on monetization. This would require the architecture to be flexible enough to allow intelligent network to help with advanced services such as advertising, remote monitoring/security etc.

3. SP Wi-Fi ARCHITECTURE

(including 802.11n Wi-Fi Cable Gateway devices [Wi-Fi-GW]) in MSO deployments.

The SP Wi-Fi architecture needs to be flexible enough to satisfy some or all of the requirements (described in section 3) in an incremental & modular way. Such a flexibility would be an important trait to MSOs, since not every MSO would deem every requirements applicable to them day 1.

The SP Wi-Fi architecture needs to be flexible enough to satisfy some or all of the requirements (described in section 3) in an incremental & modular way. Such a flexibility would be an important trait to MSOs, since not every MSO would deem every requirements applicable to them day 1.

This section provides a simplified overview of SP Wi-Fi architecture, and focuses on the architectural approaches for transporting SP Wi-Fi traffic through the transport network while hinting at their flexibility. The Figure 3 below illustrates a high-level SP Wi-Fi architecture:

A SP Wi-Fi architecture illustrated above contains one or more of the following elements:

1. Wi-Fi Access Points: The Wi-Fi Access Points may be either embedded with a cable modem (as in outdoor or residential) i.e. eDOCSIS device (also referred to as Cable Wi-Fi Gateway) or deployed separately from the cable modem (as in many indoor hotspots).

2. Access Network: This is the DOCSIS based HFC network (or EPON or Ethernet based Fiber network) comprising CMTS or CCAP, Fiber Nodes, and CMs (or ONUs) providing network connectivity to/from the AP. The CMTS terminates DOCSIS connections from the cable modems as well as connects to the metro/aggregation Network.

3. Metro/Aggregation Network: The

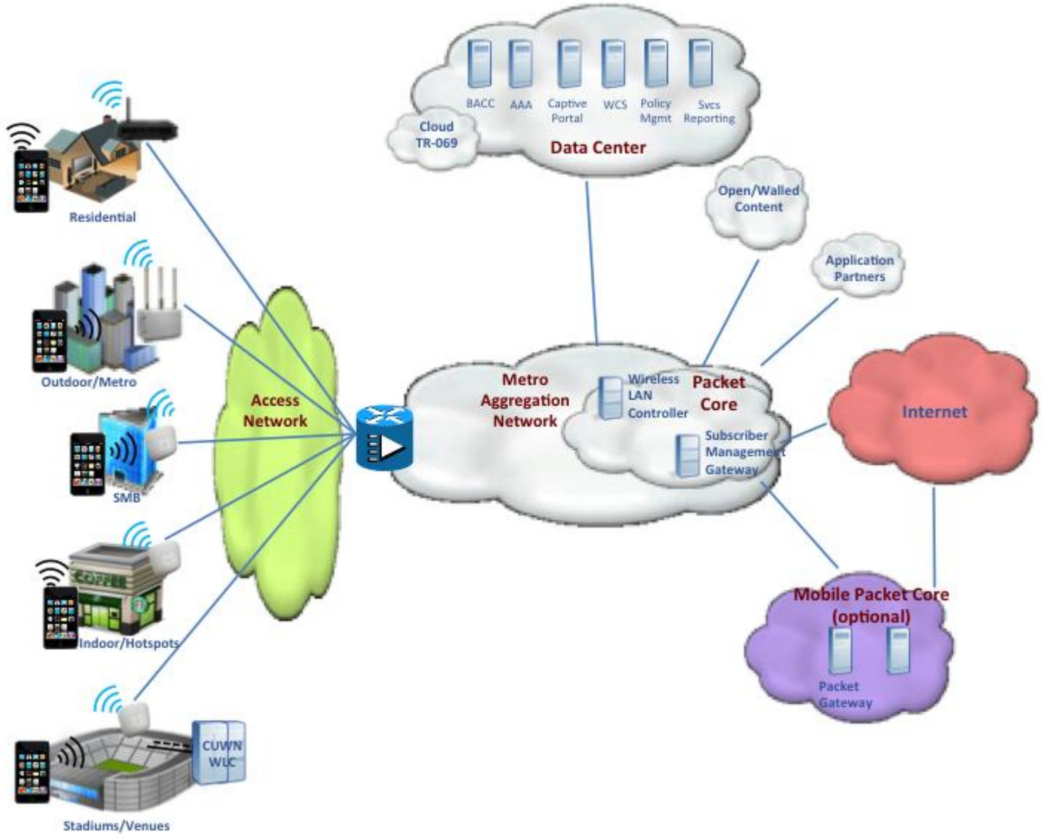


Figure 3 SP Wi-Fi Architecture (simplified)

network that CMTS uses to ultimately connect the users to the internet or partner networks or the open/walled-garden content. There may also be a regional and/or backbone network (not shown in the figure) between the metro network and internet. Metro network is usually an IP or IP/MPLS network (or sometimes a layer2 Ethernet/bridged network).

4. Wireless LAN Controller (WLC): The WLC is a centralized point of control and management of Wi-Fi APs using CAPWAP protocol (IETF RFC 5415). It tunnels data plane (user) traffic to/from the AP using the CAPWAP data plane tunnel (Please see section 3.1.1.2). It is part of the Wi-Fi packet core. It is worth pointing out that not all Wi-Fi APs are based on CAPWAP. Specifically, residential APs (i.e. eDOCSIS device) are not based on CAPWAP. This is better illustrated in the next section.

5. Subscriber Management Gateway: The Subscriber Management Gateway (dubbed as the centralized entity in this paper) is an IP point of attachment that functions as a Policy Enforcement Point (PEP). Specifically, the gateway is responsible to maintain user awareness and enforce of the relevant QoS settings, bandwidth limits, accounting, DPI, etc. The gateway is also referred to as Intelligent Services Gateway (ISG). It is part of the Wi-Fi packet core.

   It is worth pointing out that the Subscriber Management Gateway function could be implemented on the CMTS.

6. Data Center: The Service Network containing elements such as BAC, AAA, DNS, DHCP, Policy Servers and OSS/BSS elements providing network management and service management

7. Mobile Packet Core: This is optional, but it is needed for ensuring inter-technology (3G to Wi-Fi, say) or inter-domain mobility. This includes 3GPP specific elements such as PDN Gateway etc. pertaining to cellular network.

3.1 Network Transport Architecture

Wi-Fi AP connects wireless user devices to each other and/or to a wired network. In general[2], Wi-Fi AP is a layer2 bridge device that bridges Wi-Fi user devices' Ethernet frames between 802.11 wireless network (WLAN) and wired network (LAN). (One could relate AP to a Cable Modem, which is also a layer2 bridge device, but it bridges wired user devices' Ethernet frames between Ethernet network (LAN) and DOCSIS network).

> Due to subscriber management requirements described in section 2.9, the traffic from the Wi-Fi Access Points will need to be routed to a centralized entity located on the wired network for subscriber management. The subscriber management capability may reside on the WLC, ISG, MAG or even the CMTS depending on the chosen architecture.

This means that the Wi-Fi user device must have layer2 connectivity upto that centralized entity through the AP, even if AP and the centralized entity are multiple hops away from each other and reachable via the underlying network. If the underlying network

[2] A non-bridging AP will allow the association of wireless user clients, but will not allow connecting to a wired network.

is a layer2 network (i.e. Ethernet bridged network), then it is relatively simpler to ensure the needed layer2 connectivity between user devices and the centralized entity. However, if the underlying network is a layer3 network (e.g. IP or IP/MPLS network comprising routers), then it can get complicated, depending one the chosen architectural approach (there are number of architecture approaches, as discussed later in this section).

Before we discuss various architectural approaches, it is important to put the MSO network in the perspective. The underlying network in the context of a cable MSOs is commonly a layer3 network in which CMTS (or CCAP) presents itself as the layer3 next-hop (as well as layer2 next-hop) to the user devices behind the standalone modems (e.g. CM, ONU) or embedded modems [eDOCSIS] (i.e. eCM) acting as the bridge.

the underlying network infrastructure must facilitate the bidirectional connectivity between the Wi-Fi user device and the centralized entity acting as the first IP next-hop, wherever that entity is located. This can be done in number of ways, based on the chosen architecture and requirements.

This section discusses such architectural options while keeping Cable MSOs' network infrastructure in mind. While this section focuses on DOCSIS access, it is well applicable to EPON access given the DPoE relevance. The following network transport architectural approaches are qualified for backhauling SP Wi-Fi traffic:

1. IP tunneling from AP
2. BSoD L2VPN
3. BSoD L3VPN

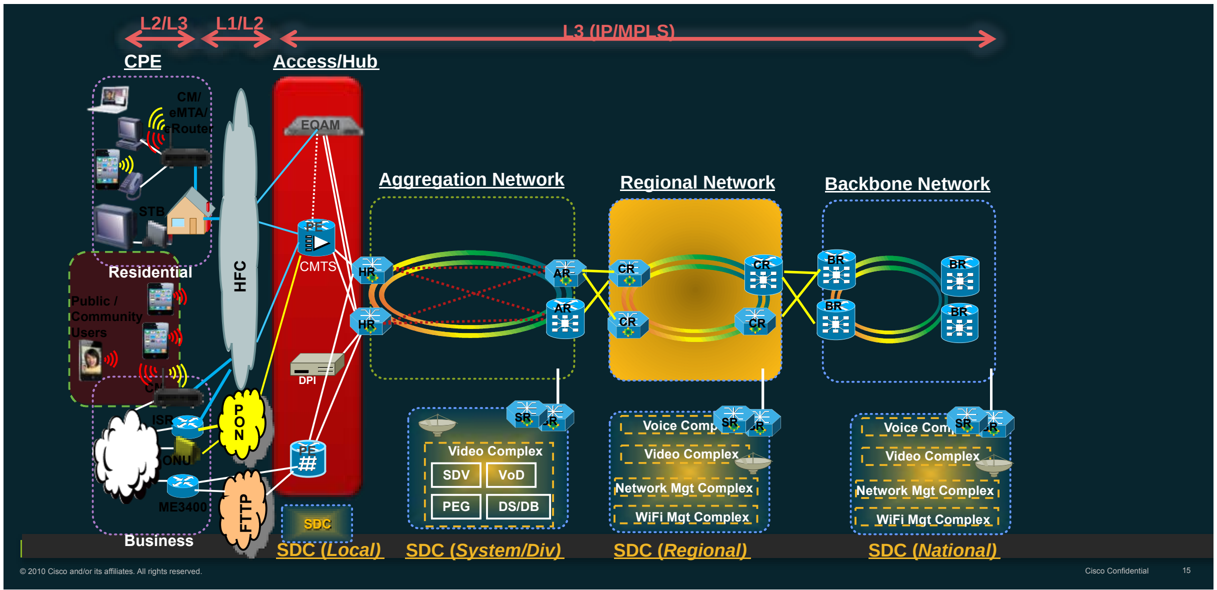


Figure 4: Reference network architecture (not showing SP Wi-Fi elements)

A reference Cable MSO network high-level diagram (not showing SP Wi-Fi elements) is shown in Figure 4.

As discussed earlier, if the underlying network is a layer3 network (e.g. IP or IP/MPLS network comprising routers), then

While each of the above architectural approaches are described in detail in the subsequent sections, the Figure 5 below briefly illustrates them with their data plane specifics and how they relate to one of key AP capabilities:

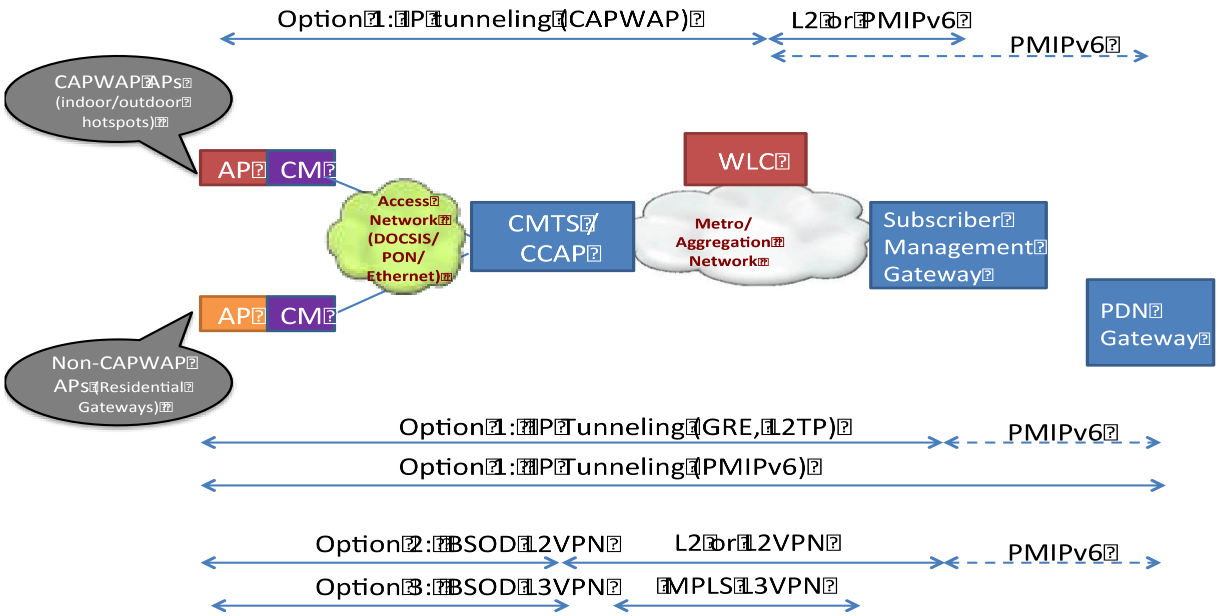

Option 1: IP tunneling (CAPWAP)
L2 or PMIPv6
PMIPv6
CAPWAP APs (indoor/outdoor hotspots)
AP
CM
WLC
Access Network (DOCSIS/ PON/ Ethernet)
CMTS/ CCAP
Metro/ Aggregation Network
Subscriber Management Gateway
AP
CM
PDN Gateway
Non-CAPWAP APs (Residential Gateways)
Option 1: IP Tunneling (GRE, L2TP)
PMIPv6
Option 1: IP Tunneling (PMIPv6)
Option 2: BSOD L2VPN
L2 or L2VPN
PMIPv6
Option 3: BSOD L3VPN
MPLS L3VPN

Figure 5 Network Transport Architectural Approaches - Data Plane

- CAPWAP APs: The traffic to/from AP is IP tunneled to the WLC using CAPWAP. The traffic between the WLC and Subscriber Gateway is a L2/802.1Q. PMIPv6 usage is optional.

- Non-CAPWAP APs: The traffic to/from AP is either tunneled over the network (option 1) or forwarded natively (option 2 or 3). PMIPv6 usage is optional.

The next section discusses each of the above network transport architectural options in details.

3.1.1 IP Tunneling from AP

There are number of options within this particular architectural approach that leverages IP tunneling from AP itself so as to tunnel the Wi-Fi traffic (either at layer2 or layer3) through the network.

3.1.1.1 PMIPv6

The architectural approach here is to build an over-the-top IP tunnel between AP and a remotely located centralized entity, using GRE over IP. In this approach, the data plane comprises “IPv4|v6 over GRE over IPv4|v6 over Ethernet [over DOCSIS (or PON)]” in the last-mile access and “IPv4|v6 over GRE over IPv4|v6” (over MPLS, if existed) in rest of the network (upto that centralized entity).

PMIPv6 is well standardized at the IETF [RFC5213] and [RFC5844]. PMIPv6 involves Mobility Access Gateway (MAG) and Local Mobility Anchor (LMA). LMA is defined to be the topological anchor point i.e. home agent for the Mobile Node’s (e.g. Wi-Fi user device's) IP prefix(es) and manages MN’s binding state via MAG. MAG manages mobility-related signaling for the MN that is attached to its access link. It is responsible for tracking the MN's movements to and from the access link and for signaling to the LMA.

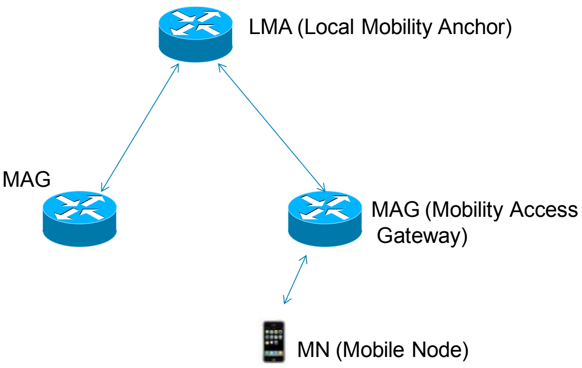
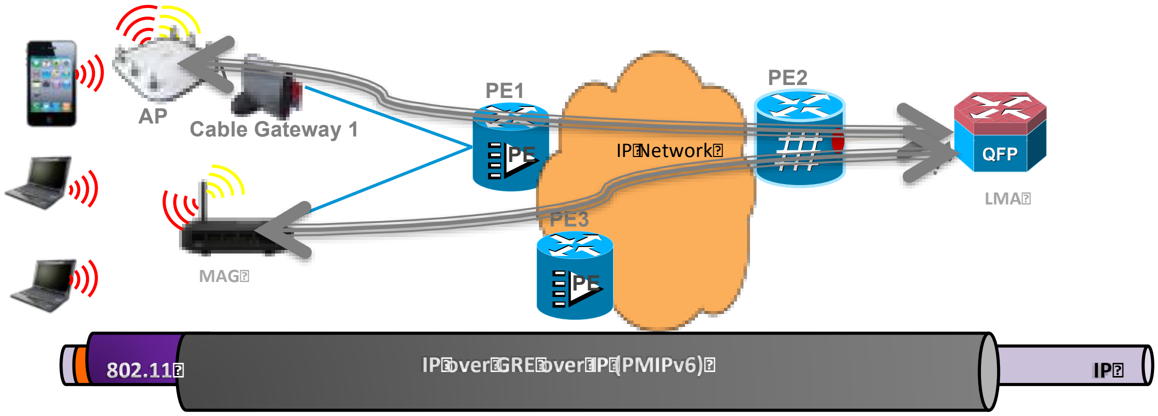


Figure 6 PMIPv6 Components

Error! Reference source not found. above illustrates PMIPv6 components.

While GRE over IP is commonly used tunnel mode, PMIPv6 also allows for other tunnel modes such as 'Ethernet over IPv6 over IPv6', Ethernet over UDP over IPv4 etc.



PMIPv6 is the only protocol that is claimed to qualify SP WiFi (with 802.1x/EAP) as the 'trusted non-3GPP access' and ensure mobility in every scenario.

Using PMIPv6 based architectural approach, an AP (acting as the MAG) uses PMIPv6 protocol messages to inform the LMA about the Wi-Fi user device (e.g. Mobile Node) getting attached. This allows AP/MAG and LMA to install (or update) the corresponding forwarding entries for the IP address assigned to the Wi-Fi user device. AP/MAG terminates user's layer2 and sends/receives user's IP traffic over the PMIPv6 tunnel. In other words, AP/MAG acts as the IP next-hop/gateway for the Wi-Fi user. While the Wi-Fi user is connected to AP/MAG at layer2, its IP address is anchored the LMA. This allows IP mobility, when the Wi-Fi user roams and changes AP/MAG attachments.

Figure 7 illustrates PMIPv6 tunneling applicability for SP Wi-Fi in sample MSO network topology.
It is important to highlight that instead of enabling PMIPv6 (MAG function) at the AP (as shown in this particular approach), it can

be instead enabled on ISG, WLC or CMTS (as shown in other architectural approaches e.g. BSoD L2VPN) in an incremental manner for mobility.

The advantages of this approach are – (a) scales extremely well, (b) provides IP mobility for all scenarios, (c) integrates with 3GPP based cellular network

The disadvantages of this approach are – (a) requires MAG function as well as user management/control on AP/Modem – increased complexity on residential modems/gateways, (b) requires unique config file per modem for DS classification, (c) subjected to fragmentation and reassembly on last-mile access, (d) prohibits 5-tuple classification for QoS in the network, (e) results in sub-optimal multicast replication (e.g. network capacity wastage) if multiple user devices consume the multicast content

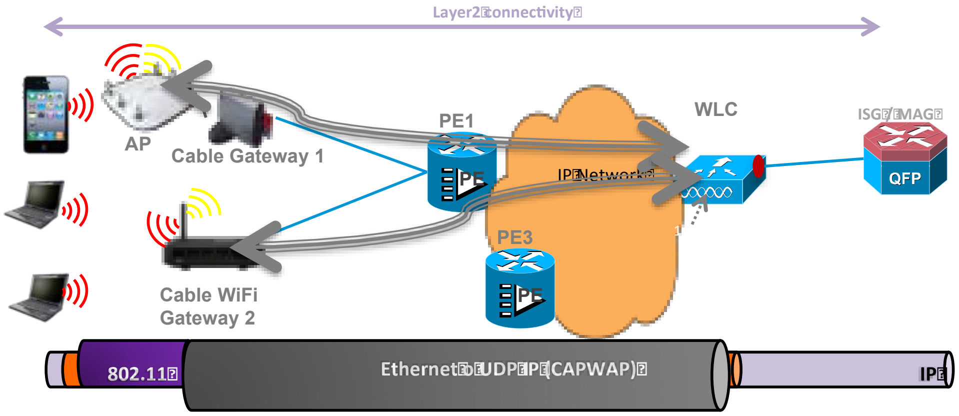
3.1.1.2 CAPWAP

The architectural approach here is to deliver the WiFi 802.11 traffic to a remotely located centralized entity e.g. Wireless LAN Controller (WLC), using UDP over IP. In this approach, the data plane comprises users' "Ethernet over UDP over IPv4|v6 over Ethernet [over DOCSIS (or PON)]" in the last-mile access and "Ethernet over UDP over IPv4|v6" (over MPLS, if existed) in rest of the network (upto WLC). UDP port is a well-known port 5247.

CAPWAP is well standardized at the IETF [RFC5415] and [RFC5416].

CAPWAP is a de facto protocol for Control and Provisioning of APs, and extensively used in most SP Wi-Fi deployments use-cases.

Figure 8 illustrates CAPWAP tunneling applicability for SP Wi-Fi in sample MSO network topology:



Using this approach, an AP establishes a CAPWAP tunnel (i.e. UDP over IP tunnel) with WLC (e.g. centralized entity). The 802.11 frames sent by the user device are forwarded by AP over the CAPWAP tunnel to WLC, which decapsulates the CAPWAP header and forwards the user device' IP packet using IP forwarding lookup. If the IP destination of the packet is another WiFi user device, then the IP packet is encapsulated in the 802.11 header and placed on the CAPWAP tunnel towards the appropriate AP. If the IP destination of the packet is on the wired network, then the IP packet is forwarded as usual.

The returning traffic gets subjected to the IP forwarding lookup, and gets placed on the appropriate CAPWAP tunnel, which is terminated at the AP. AP then delivers the 802.11 frames to the WiFi user device.

CAPWAP provides fragmentation and reassembly as per the path MTU discovery done by both AP and WLC, and allows for optional encryption using DTLS. CAPWAP also allows for PMIPv6 integration, as/if/when desired. This means that PMIPv6 elements (e.g. MAG and LMA) can incrementally be introduced, in which the MAG function can be enabled at the WLC.

The advantages of this approach are – (a) provides network administrators with a structured and hierarchical model to control & configure the APs, (b) controls hand-offs between AP during user roaming = foundation for mobility (c) works with layer2 or layer3 network, (d) allows 802.11 link-layer control, (e) works with NAT

The disadvantages of this approach are – (a) CAPWAP is not deemed useful for the residential APs, (b) network capacity wastage due to unnecessary multicast replication at WLC may happen if multiple user devices consume the multicast content

3.1.1.3 GRE

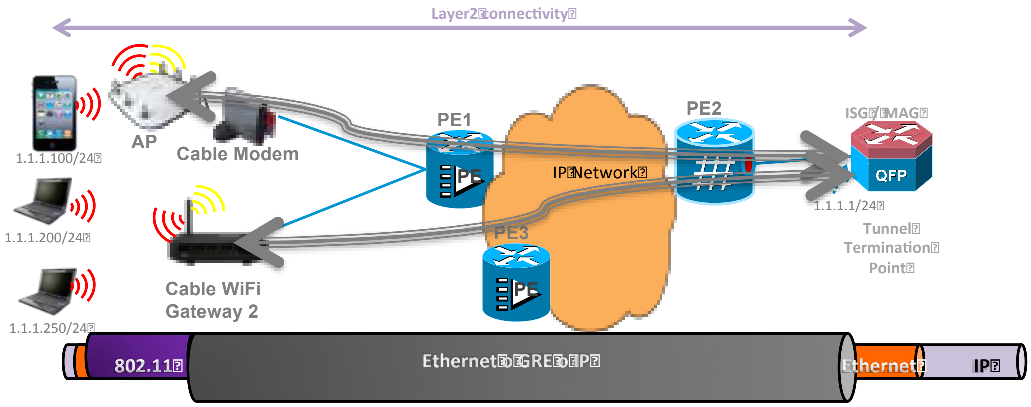
The architectural approach here is to build an over-the-top IP tunnel to deliver the Wi-Fi user device's Ethernet traffic between AP and a remotely located centralized entity (i.e. tunnel termination entity), using GRE. This approach requires IP connectivity between AP and the centralized entity. In this approach, the data plane comprises users' "Ethernet over GRE over IPv4|v6 over Ethernet [over DOCSIS (or PON)]" in the last-mile access and "Ethernet over GRE over IPv4|v6" (over MPLS, if existed) in rest of the network (upto that centralized entity).

> While Ethernet over GRE over IP usage is not well known or used, it is standardized at the IETF [RFC1771].

Figure 9 illustrates GRE tunneling applicability for SP Wi-Fi in sample MSO network topology.

Using this approach, an AP establishes a GRE tunnel with the remote L2TP tunnel concentrator (e.g. centralized entity) and sends/receives Wi-Fi user device's Ethernet frames, over GRE (over IP) tunnel. It is important to note that GRE doesn't require a control channel and can be set up in a stateless manner without requiring any tunnel configuration.

The advantages of this approach are – (a)



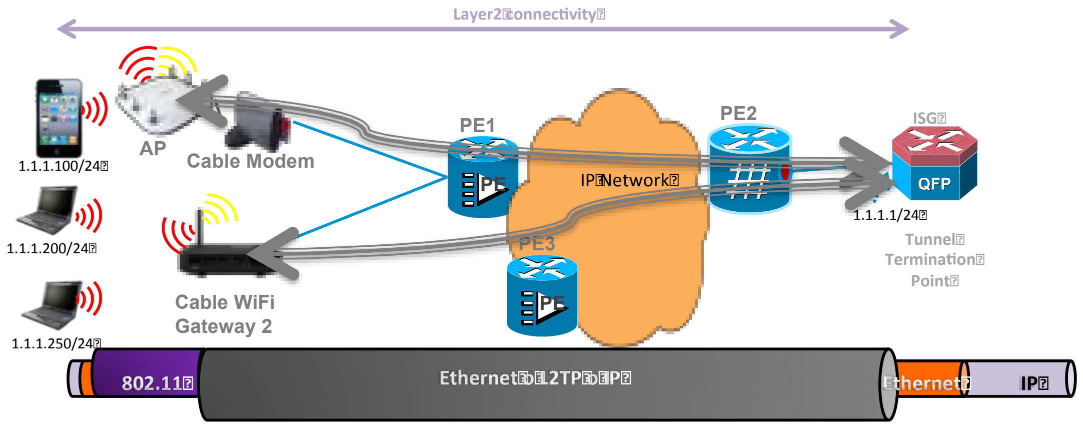
maintains simplicity on AP or Gateways (b) scales well (if stateless tunneling is used, (c) maintains subscriber management/control at the remotely located centralized entity (e.g. tunnel termination point) based on IP, (d) provides IP mobility natively within the Layer 2 domain, (e) can integrate with PMIPv6 (by having the MAG function on the tunnel termination point) to provide macro-mobility.

The disadvantages of this approach are – (a) does not integrate with 3GPP and doesn't provide mobility in all scenarios, (b) requires unique config file per modem for DS classification, (c) relies on IP tunneling, (d) subjected to fragmentation and reassembly on last-mile access, (e) prohibits 5-tuple classification for QoS in the network, (f) results in sub-optimal multicast replication (e.g. network capacity wastage) if multiple user devices consume the multicast content

3.1.1.4 L2TP

The architectural approach here is to build an over-the-top Layer 2 circuit (over IP network) to deliver the Wi-Fi traffic (e.g. Ethernet frames) between AP and a remotely located centralized entity (i.e. tunnel termination entity), using Layer 2 Tunneling Protocol (L2TP). This approach requires IP connectivity between AP and the centralized entity. In this approach, the data plane comprises users' "Ethernet over L2TP over IPv4|v6 over Ethernet [over DOCSIS (or PON)]" in the last-mile access and "Ethernet over L2TP over IPv4|v6" (over MPLS, if existed) in rest of the network (upto that centralized entity).

L2TPv2 is standardized at the IETF [RFC2661], whereas L2TPv3 is standardized at the IETF [RFC3931]. Figure 10 illustrates L2TP tunneling applicability for SP Wi-Fi in sample MSO network topology.



Using this approach, an AP establishes an L2TP tunnel with the remote L2TP tunnel concentrator (e.g. centralized entity) and sends/receives Wi-Fi user device's Ethernet frames, over L2TP (over IP) tunnel. It is important to note that L2TP requires a control channel to establish the tunnel.

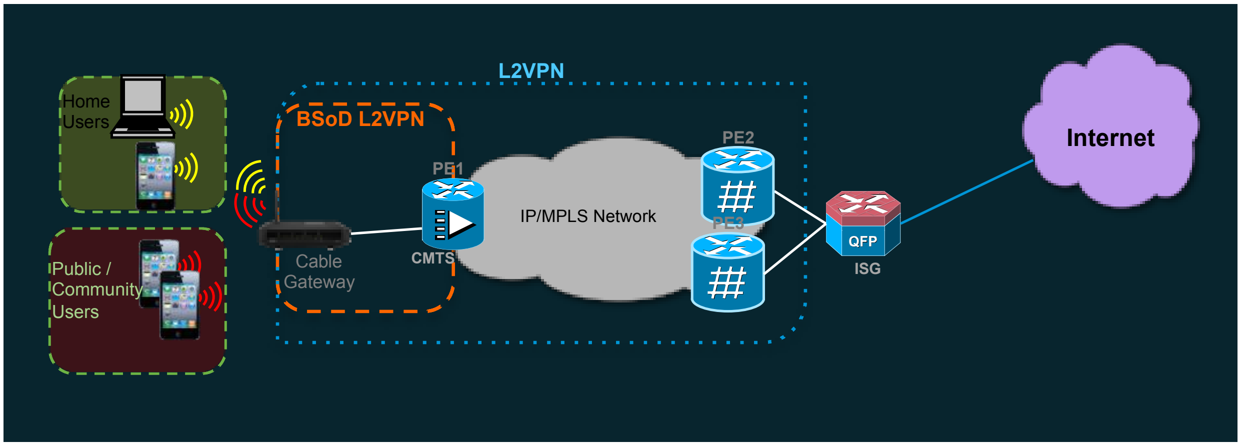
This architectural approach allows for PMIPv6 integration, as/if/when desired by the MSO to achieve mobility between Wi-Fi and Wi-Fi as well as cellular and Wi-Fi. This means that PMIPv6 elements (e.g. MAG and LMA) can incrementally be introduced in the

MSO network, in which the MAG function can be enabled at the L2TP tunnel concentrator.

The advantages of this approach are – (a) has its own control channel, (b) can make use of a cookie for added security

The disadvantages of this approach are – (a) does not scale (beyond few thousand tunnels), (b) requires unique config file per CM for proper DS classification, (c) does not integrate with 3GPP and doesn't provide mobility in all scenarios by itself,

3.1.2 BSoD L2VPN



The idea in this architectural approach is very simple – use Layer 2 VPN to deliver the Wi-Fi traffic to a remotely located centralized entity at layer2 (without requiring any IP lookup). In this approach, the data plane comprises Ethernet [over DOCSIS (or PON)] in the last-mile access and Ethernet over MPLS (or just Ethernet) in rest of the network (upto the centralized entity).

Thankfully, Layer 2 VPN is a well known and well used option in many MSO deployments already, given that CableLabs standardized the Layer 2 VPN over DOCSIS in form of BSoD L2VPN [BSODL2VPN] and enabled many MSOs to use Layer 2 VPN to serve business customers with Metro Ethernet services (e.g. MEF (E-LINE, E-LAN, E-TREE), TLS etc.) when the VPN sites are attached to the HFC access. It is becoming quite useful for other purposes such as traffic separation for different services.

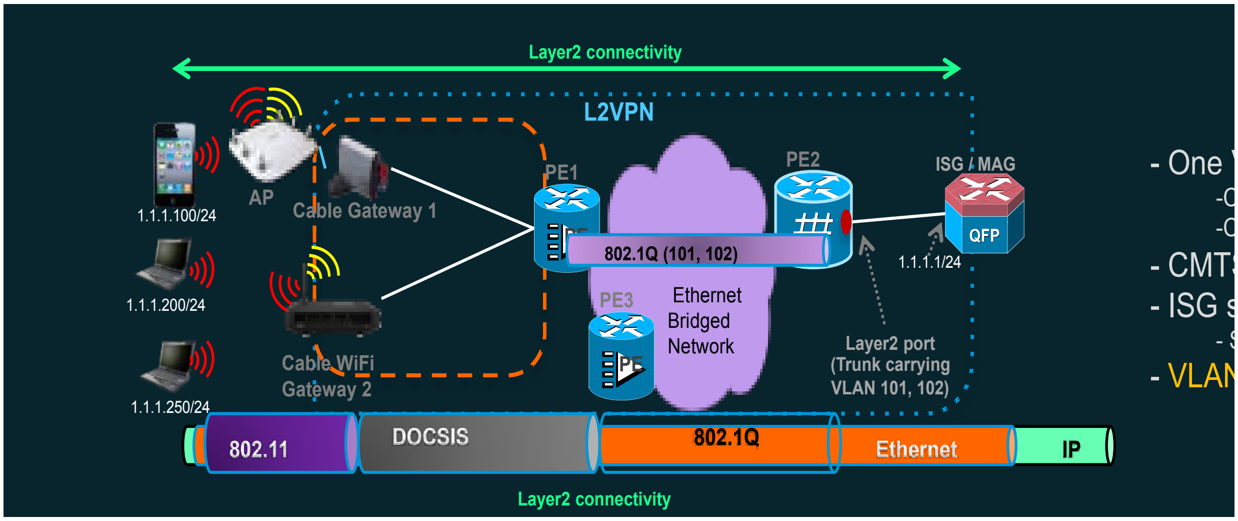
`Figure 11` illustrates L2VPN applicability in sample MSO network topology. It is important to note that the service-flows used for SP Wi-Fi (e.g. Public/Community users) are different from the ones used by the residential users. This automatically allows for traffic separation and IP prefix/address assignment separation between SP Wi-Fi users and residential users (throughout the network).

Using BSoD L2VPN, a CM is able to classify the upstream traffic (received from the AP) using SSID (in case of embedded CM) or VLAN (in case of standalone CM) present in the Ethernet frames, and forward the traffic over a particular DOCSIS service-flow (e.g. impose DOCSIS Header on the received Ethernet frame) to the CMTS. A CM is also able to forward the downstream traffic (received from the CMTS on a particular DOCSIS service-flow) to the AP (e.g. remove DOCSIS header and retrieve Ethernet frame).

Using BSoD L2VPN, a CMTS is able to forward the upstream traffic (received from the CM) on its uplink e.g. NSI towards the centralized entity, after removing the DOCSIS header and imposing an 802.1Q or 802.1AD or MPLS header, as per what MSO chose (and set in the config file). CMTS is also able to forward the downstream traffic (received from the network/centralized entity) after removing the 802.1Q or 802.1AD or MPLS header, to the Cable Modem on a particular DOCSIS downstream service-flow. It is important to highlight that the downstream Classification can be done by the CMTS without needing any CM config file dependency.

`Figure 12` illustrates using BSoD L2VPN using 802.1Q encapsulation variant. The figures below illustrate using BSoD L2VPN using MPLS encapsulation variants.

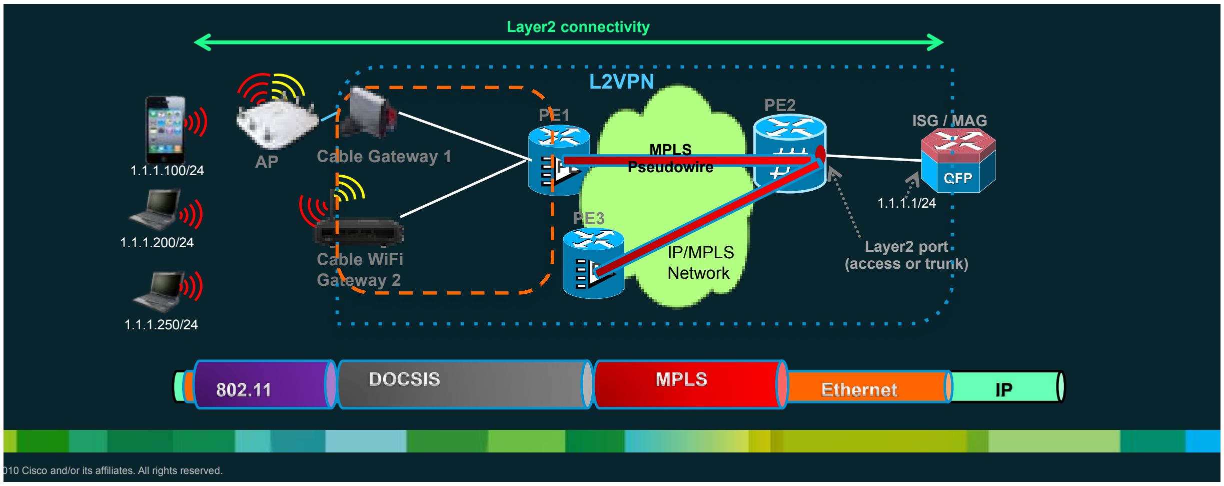
BSoD L2VPN does not require any tunneling from AP or CM, resulting in zero overhead on DOCSIS RFI, hence, avoiding any fragmentation/reassembly possibility, and also resulting in leveraging what's already supported in deployed MSO networks.



The CM config file includes TLVs that describe the mapping of one or more SFs with L2VPN designated for SP Wi-Fi. The config file does not need anything per-modem or AP specific to ensure the DS classification of the SP Wi-Fi traffic.

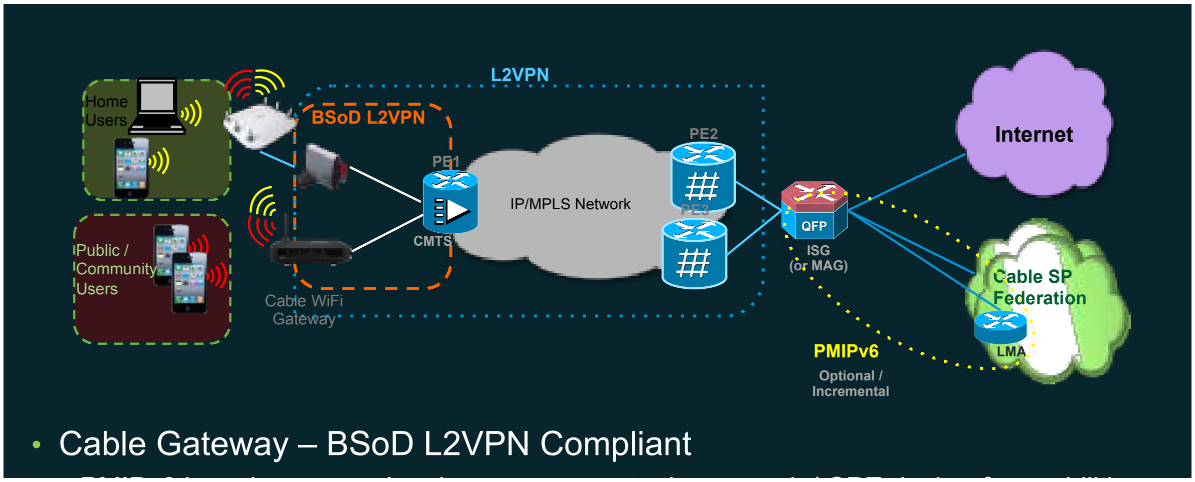
BSoD L2VPN with 802.1Q encap requires one VLAN per CM (if using P2P L2VPN) or one VLAN per network (if using P2MP L2VPN) for SP Wi-Fi.

BSoD L2VPN with MPLS encap



requires one MPLS pseudowire per CM (if using P2P L2VPN) or one MPLS pseudowire per CMTS (if using P2MP L2VPN) for SP Wi-Fi.

What’s really nice about this architectural approach is that it allows for PMIPv6 integration, as/if/when desired by the MSO to infuse mobility during Wi-Fi and Wi-Fi as well as cellular and Wi-Fi handoff. This means that PMIPv6 elements (e.g. MAG and LMA) can incrementally be introduced in the MSO network without changing the existing L2VPN setup, as illustrated in Figure 14:



- Cable Gateway – BSoD L2VPN Compliant

The advantages of this approach are: (a) Works in the existing deployments, (b) downstream classification is possible without any config file dependency, (c) Separate traffic management for SP Wi-Fi users and residential users, (d) common config file pertaining to SP Wi-Fi for the CMs with P2MP L2VPN, (e) Seamless mobility in all scenarios is possible with PMIPv6 integration, as/if necessary, (f) requires no fragmentation/reassembly on the last-mile access = better data-plane throughput

The disadvantages of this approach are: (a) unique CM config file per modem if P2P L2VPN is used (note thathe upcoming BSoD L2VPN specification changes (CableLabs work underway) will no longer require unique CM config file, thanks to the dynamic discovery of remote PEs), (b) dynamic SF (e.g. DSx) support may not be available, (c) does not integrate with 3GPP and doesn’t provide mobility in all scenarios.

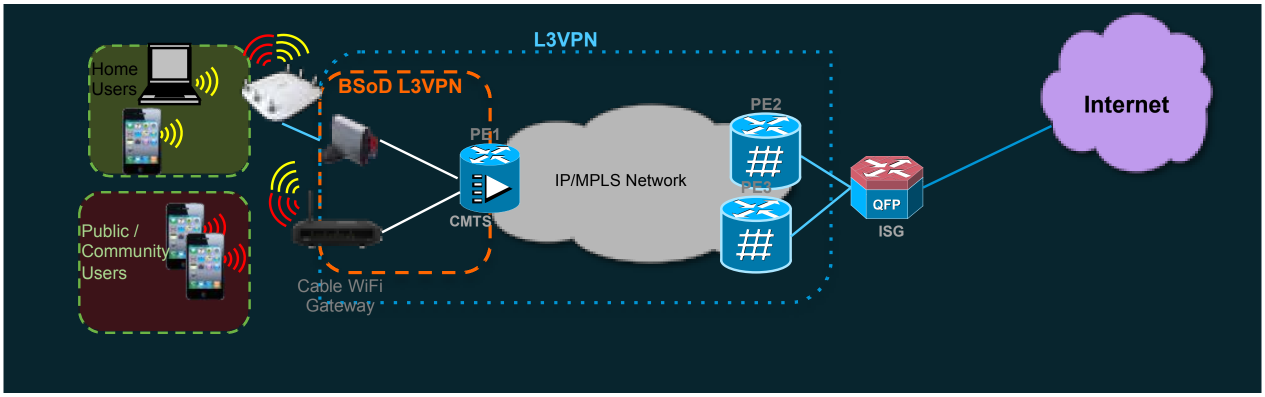
3.1.3 L3VPN

IP/VPN [RFC4364] is one of the most used technologies in SP networks (Wireline or Mobile) for internal purposes (e.g. network virtualization) and/or external purposes (e.g. Business L3VPN service).

This architectural approach allows the CMTS to terminate layer2 and use Layer 3 VPN to deliver the Wi-Fi traffic to remotely located centralized entity at layer3. In this approach, the data plane comprises ‘IP over Ethernet over DOCSIS (or PON)’ in the last-mile access and ‘IP over MPLS’ in rest of the network.

CableLabs standardization of L3VPN is underway (IP/VPN working group).

Figure 15 illustrates L3VPN applicability in sample MSO network topology.



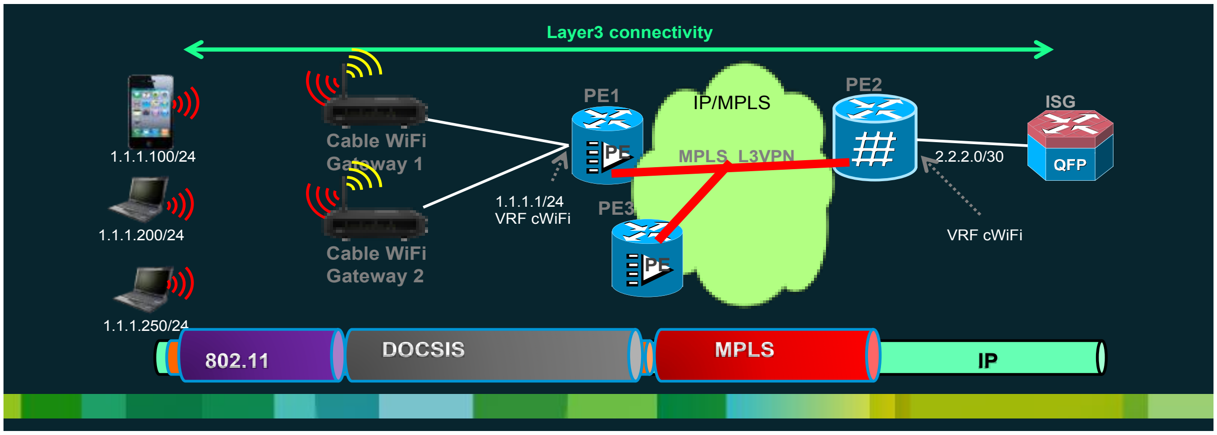
It is important to note that the service-flows used for SP Wi-Fi (e.g. Public/Community users) are different from the ones used by the residential users. This automatically allows for traffic separation and IP prefix/address assignment separation between SP Wi-Fi users and residential users.

A CM is able to classify the upstream traffic (received from the AP) using SSID (in case of embedded CM) or VLAN (in case of standalone CM) present in the Ethernet frames, and forward the traffic over a particular DOCSIS service-flow (e.g. impose DOCSIS Header on the received Ethernet frame) to the CMTS. A CM is also able to forward the downstream traffic (received from the CMTS on a particular DOCSIS service-flow) to the AP (e.g. remove DOCSIS header and retrieve Ethernet frame).

Using IP/VPN, a CMTS is able to forward the upstream traffic (received from the CM) on its uplink e.g. NSI to the network (or towards the centralized entity, if present), after removing the DOCSIS header and imposing an MPLS header. A CMTS is also able to forward the downstream traffic (received from the IP/MPLS network or centralized entity) after removing the MPLS header, to the Cable Modem on a particular DOCSIS downstream service-flow. It is important to note that the downstream Classification can be done by the CMTS without needing any CM config file dependency (e.g. per-CM or per-AP classifier).

The CM config file includes TLVs that describe the mapping of SFs with L3VPN designated for SP Wi-Fi (e.g. cWi-Fi in the figure above).

Figure 16 illustrates the data plane utilized when IP/VPN is used for SP Wi-Fi.



The advantages of this approach are: (a) CMTS could become the per-user policy enforcement point (with or without MAG function), (b) common config file pertaining to SP Wi-Fi for the CMs, (c) downstream classification is possible without any config file dependency, (c) the Wi-Fi traffic could follow the IP routing right from the CMTS, if needed, ((d) Wi-Fi users can be served by any DHCP server, (e) dynamic SF (e.g. DSx) support is available, (f) Seamless mobility is possible if the Wi-Fi user gets handed-off between APs served by the same CMTS

The disadvantages of this approach are: (a) Seamless Mobility is not possible all the time, since IP address preservation can not be guaranteed upon AP hand-off from one CMTS to another (without some additional complexity), (b) does not integrate with 3GPP, (c) cablelabs standardization not completed yet

Like L2VPN, L3VPN does not require any tunneling from AP or CM, resulting in zero overhead on DOCSIS RFI, hence, avoiding any fragmentation/reassembly possibility, and also resulting in leveraging what's already supported in deployed MSO networks.

3.1.4 Future Possibilities

In the previous section, although transport options are discussed as three discrete options, there are various other ways to achieve the requirements set out earlier. For example the benefits of PMIPv6 can be derived without the tradeoffs of tunneling by implementing the MAG in the network. Of course such an architecture brings its own set of tradeoffs. Similarly if subscriber management is implemented at the edge of the network it may eliminate the need for L2VPN/L3VPN architectures that are used to route traffic to a centralized entity. Such advanced architectures and solutions are outside the scope of this paper and are not discussed in any further detail here.

3.1.5 Comparison of Transport Options

The table below compares the three architectural approaches for network transport:

Table 1 Comparison of Various approaches

		IP Tunneling (from AP)	L2VPN	L3VPN
1	CableLabs Standardized	No	Yes	In progress[3]
2	Available	No[4]	Yes	Yes
3	Data Plane (Last-Mile Access)	User Ethernet frame over GRE|L2TP over IP over Ethernet over DOCSIS	User Ethernet frame over DOCSIS	User Ethernet frame over DOCSIS
4	Data Plane (Network)	User Ethernet frame over GRE|L2TP over IP (over MPLS)	User Ethernet frame over .1Q or .1AD or MPLS	User IP packet over MPLS
5	Overhead on Last-Mile Access	Yes	No	No
6	Requires Unique CM config file per Modem	Yes	Yes/No	No
7	User Awareness	ISG, MAG	ISG, MAG	CMTS or ISG
8	CMTS/CCAP Uplink/NSI needs?	IP	802.1Q Trunk, or IP/MPLS	IP/MPLS
9	DOCSIS Upstream Classifier?	IP Address	SSID or VLAN tag	SSID or VLAN tag
10	DOCSIS Downstream Classifier?	IP Address	MPLS label or VLAN tag	MPLS label or VLAN tag
11	DOCSIS Fragmentation & Reassembly (on CMTS, CM)	Yes	No	No
12	5-Tuple[5] based Classification by CMTS	No	Yes	Yes
13	5-Tuple based Classification by other routers	No	No	Yes
14	Mobility (WiFi-WiFi)	Yes	Yes[6]	Yes/No[7]
15	Mobility (WiFi-Cellular)	Yes	Yes	No
16	Accounting/DPI/LI possible at CMTS?	No	Yes	Yes

[3] CableLabs Standardization progressing in IPVPN Working Group

[4] Except L2TP, none of the IP tunneling variants seem to be available at the moment on the Modem / Gateway

[5] 5-Tuple = Src IP, Dest IP, Proto, Src Port, Dest Port

[6] May Require PMIPv6 Integration

[7] Seamless mobility as long as AP handoff doesn't change the CMTS.

4.0 CONCLUSION

A number of network transport options for SP Wi-Fi are discussed in this paper. Some of them are already deployed, whereas some of them are being considered for deployment.

The architectural options that help simplify the SP Wi-Fi architecture and harvest network intelligence would provide not only the cost-effectiveness, but also enable monetization opportunities. Monetization is where the next

REFERENCES

[Wi-Fi-Roam]CableLabs Wi-Fi Roaming Architecture and Interfaces Specification
[Wi-Fi-GW] CableLabsWi-Fi Requirements for Cable Modem Gateways
[eDOCSIS] CableLabseDOCSIS Specification
[DPOE] CableLabsDOCSIS Provisioning of EPON Specification 1.0
[BSODIPVPN] CableLabs IP VPN
[BSODL2VPN] CableLabs Business Services over DOCSIS Layer 2 VPN Specification
[Hotspot2.0]WFA
http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns673/white_paper_c11-649337.html.
[RFC4364] IETF BGP/MPLS IP Virtual Private Networks (VPNs)

ABBREVIATIONS

AP	Access Point
BSOD	Business Services over DOCSIS
CAPWAP	Control and Provisioning of Wireless Access Points
CM	Cable Modem
CMTS	Cable Modem Termination System
DPI	Deep Packet Inspection
GRE	Generic Routing Encapsulation
LI	Legal Intercept
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
PMIPv6	Proxy Mobile IPv6
WLC	Wireless LAN Controller

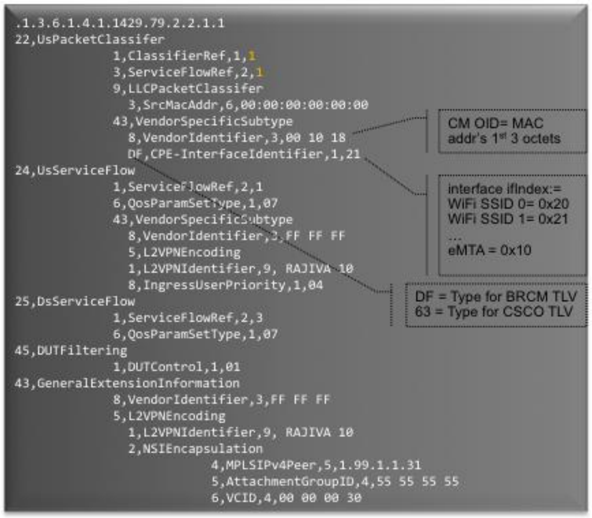
ACKNOWLEDGEMENTS

The author wishes to thank colleagues at Cisco for help and support in writing this paper.

APPENDIX

SP Wi-Fi using BSoD L2VPN – Sample Config file

A sample eCM config file for BSoD L2VPN having SSID-SF mapping is shown below



```
.1.3.6.1.4.1.1429.79.2.2.1.1
22,UsPacketClassifer
             1,ClassifierRef,1,1
             3,ServiceFlowRef,2,1
             9,LLCPacketClassifer
               3,SrcMacAddr,6,00:00:00:00:00:00
             43,VendorSpecificSubtype
               8,VendorIdentifier,3,00 10 18
               DF,CPE-InterfaceIdentifier,1,21
24,UsServiceFlow
             1,ServiceFlowRef,2,1
             6,QosParamSetType,1,07
             43,VendorSpecificSubtype
               8,VendorIdentifier,3,FF FF FF
               5,L2VPNEncoding
               1,L2VPNIdentifier,9, RAJIVA 10
               8,IngressUserPriority,1,04
25,DsServiceFlow
             1,ServiceFlowRef,2,3
             6,QosParamSetType,1,07
45,DUTFiltering
             1,DUTControl,1,01
43,GeneralExtensionInformation
             8,VendorIdentifier,3,FF FF FF
             5,L2VPNEncoding
               1,L2VPNIdentifier,9, RAJIVA 10
               2,NSIEncapsulation
                       4,MPLSIPv4Peer,5,1.99.1.1.31
                       5,AttachmentGroupID,4,55 55 55 55
                       6,VCID,4,00 00 00 30
```

CM OID= MAC addr's 1st 3 octets

interface ifIndex:=
WiFi SSID 0= 0x20
WiFi SSID 1= 0x21
...
eMTA = 0x10

DF = Type for BRCM TLV
63 = Type for CSCO TLV