Is IPv6 over SP Wi-Fi a reality now?

Rajiv Asati, Distinguished Engineer (rajiva@cisco.com)
Ravi Shankar, Technical Leader (rshankar@cisco.com)
Cisco

Abstract

As Cable MSOs continue to exploit the fantastic opportunity with SP Wi-Fi and witness the exponential growth in their customer-base using the SP Wi-Fi services, they will soon have to decide whether to use public IPv4 addressing or private IPv4 addressing for the Wi-Fi Subscriber Equipments (UEs) used by their customer-base before the customers can avail of any free/paid services offered by the MSOs.

The reason is that most Cable MSOs have so far stuck with IPv4-only SP Wi-Fi designs/deployments, and most of them will run out of their public IPv4-address pools sooner or later (as soon as 2013-14 for some).

In this paper, we outline a strategy entailing IPv6 over SP Wi-Fi, discuss common challenges (that Cable MSOs face) with IPv6 in Wi-Fi and propose necessary solutions & technological evolutions for deploying IPv6 over SP Wi-Fi in Cable MSO networks.

TABLE OF CONTENTS

INTRODUCTION

Wi-Fi (an IEEE 802.11 family of standards [1]) is a pervasive & proven access technology that is now ubiquitously used indoors and outdoors. SP Wi-Fi, which primarily refers to an Wi-Fi system deployed and managed by a Service Provider (SP) for public access (aka community access) to SP network, is now commonly used by Cable Multi-System Operators (MSOs) to allow the customers/subscribers to benefit from the mobile consumption of Internet (and other) content. The MSOs are benefiting from SP

Wi-Fi to not only reduce the existing customer-attrition, but also attract new customers. MSOs can also offer the managed (and sometimes hosted) Wi-Fi services to other service providers (e.g. Mobile SPs).

As SP Wi-Fi continues to get widely deployed in MSO networks and get used more and more, MSOs must have to accommodate more and more devices/subscribers connecting to the networks, and use more and more IP addresses in addition to what MSOs already have/use for their triple-play services over wired access (e.g. Cable, Fiber).

> Imagine an SP Wi-Fi deployment having 10,000s of APs to serve 1,000,000s of subscriber devices. With 20% attachment rate, the MSO would need 210,000 IP addresses.

Noting the fact that almost all of the SP Wi-Fi deployments have been IPv4-only, and that many MSOs may not have enough IPv4 addresses left in very near future, it becomes obvious that operating SP Wi-Fi networks in an IPv4-only paradigm is quiet a significant business risk. While it is possible for MSOs to acquire additional IPv4 addresses from the RIR i.e. ARIN, they may not be able to do so once ARIN also runs out of its IPv4 addresses. Well, guess what, ARIN is already nearing the IPv4 address exhaustion [2].

This means something very obvious – Use IPv6. Of course, another obvious approach is to share each IPv4 address among number of customers.

MSOs must embrace/enable IPv6, no doubt about it. Of course, IPv6 enablement MUST NOT be done at the expense of IPv4. For all practical purposes, MSOs still need IPv4 (per customer or subscriber device) to ensure that IPv4-only devices and/or applications (aka apps) continue to work, despite having to dread the IPv4 address exhaustion. This means "Dual-stack IP addressing" (i.e. enable IPv6 while maintaining IPv4) of the customer/subscriber devices connecting to MSO Wi-Fi networks is MUST for now.

The key is to enable more and more subscribers/devices to use IPv6 for more and more content consumption, thereby limiting/reducing the need for IPv4, while ensuring customers' EXPERIENCE of content consumption.

SP WI-FI ARCHITECTURE

It is imperative to understand the SP Wi-Fi architecture as well as specific SP Wi-Fi components before dwelling into IPv6 specifics. This section provides a simplified overview of SP Wi-Fi architecture, which comprises of several building blocks:

1. Wi-Fi Access Points
2. Access Network
3. Metro/Aggregation Network
4. Wi-Fi Packet Core
5. Mobile Packet Core
6. Data Center

The Figure 1 illustrates such a simplified SP Wi-Fi architecture:

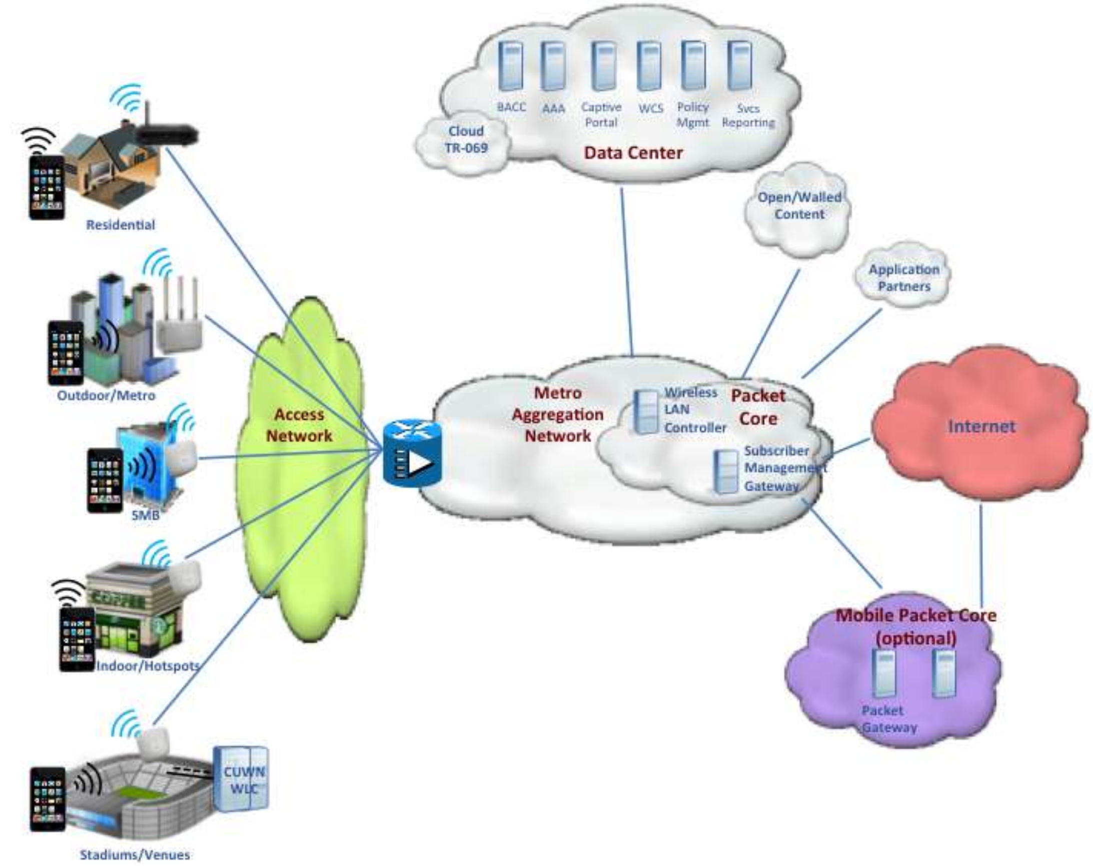

Figure 1 SP Wi-Fi Architecture – End-to-End (simplified)

The SP Wi-Fi architecture illustrated above contains the following building blocks:

1. Wi-Fi Access Points: The Wi-Fi Access Points may be either embedded with an ONU or cable modem (i.e. eDOCSIS device – also referred to as Cable Wi-Fi Gateway) or deployed separately from the CM or ONU.

2. Access Network: This is the DOCSIS based HFC network or xPON or Ethernet based Fiber network comprising CMTS or CCAP, Fiber Nodes, and CMs (or ONUs) providing network connectivity to/from the AP.

3. Metro/Aggregation Network: This is the network that CMTS uses to ultimately connect the subscribers 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. Wi-Fi Packet Core: WPC typically comprises one or more Wireless LAN

Controllers (WLC) and Subscriber Management Gateways.

   a. WLC – Responsible for control and management of Wi-Fi APs using CAPWAP protocol (IETF RFC 5415) and for mapping subscribers' traffic from Wi-Fi SSID to a virtual context e.g. VLAN by having tunnels to APs.

      Note that WLC is not expected to be present in the residential deployments of SP Wi-Fi.

   b. Subscriber Management Gateway: An IP point of attachment that functions as a Policy Enforcement Point (PEP). Specifically, the gateway is responsible for maintaining subscriber awareness (in form of sessions), enforcing the per-subscriber policy e.g. QoS & bandwidth limits, and providing the usage/accounting, DPI, etc.

      The gateway is also referred to as Intelligent Services Gateway (ISG) or Session Manager (SM) or Gateway.

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

6. Mobile Packet Core: This is optional, but it is needed for ensuring inter-technology (4G/3G to Wi-Fi, say) or inter-domain mobility. This includes 3GPP specific elements such as PDN Gateway (PGW) etc. pertaining to cellular networks.

To understand the SP Wi-Fi components and their functions a bit better, we need to drill down in the above high-level end-to-end SP Wi-Fi architecture. Figure 2 focuses on the SP Wi-Fi components and their functions:

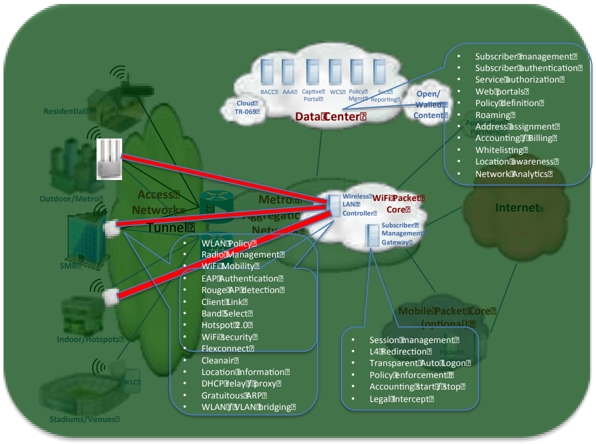

Figure 2 SP Wi-Fi Architecture - Functions

There are few points that are worth highlighting:

The WLC manages all the APs (including radio resources, SSIDs etc.) over the CAPWAP tunnels, and forwards/receives subscriber devices' IP traffic to/from Subscriber Management Gateway(s).

The WLC can either be L2 or L3 connected to the Subscriber Management Gateways. In either connectivity, all subscriber traffic must be forced through the Subscriber Management Gateway (so as to identify the subscriber, enforce policies, account for usage, perform Legal Interception etc.). To do so,

- In case of L2 connectivity, subscriber's default IP gateway is pointed to the Gateway's IP address
- In case of L3 connectivity, other IP routing mechanisms are used

The Subscriber Management Gateway terminates and manages subscriber sessions that are created dynamically when subscribers get online. Sessions are created as unauthenticated until subscriber credentials are verified and appropriate services are installed. Once authenticated, subscribers are allowed access into the network for the authorized content consumption.

SP WI-FI: IPV6 TOUCHPOINTS

IPv6 enablement in the SP Wi-Fi architecture can be divided in two categories – IPv6 enablement for Wi-Fi subscribers, and IPv6 enablement for Infrastructure.

The latter category is for enabling IPv6 in the network infrastructure independent of subscribers' usage of IPv6 (or IPv4). For example, AP and WLC communicating (CAPWAP) over IPv6.

The former category is for enabling IPv6 for the subscribers independent of the network infrastructure. This category requires a lot many more devices (besides the subscriber devices) in the Data Center to be enabled with IPv6. For example, AAA (or BSS) servers accommodating subscriber device' IPv6 address usage during authentication.

The figure below illustrates the IPv6 touch-points:

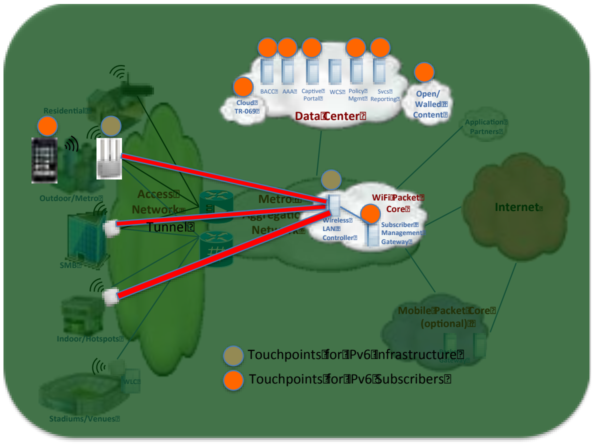

Figure 3 SP Wi-Fi Architecture: IPv6 Touchpoints

Unlike IPv4, IPv6 allows a device to have multiple IPv6 addresses. Hence, it is important to track all the IPv6 addresses per device and enable seamless mobility for them when the subscriber's device moves within the mobility domain.

> A mobility domain is defined as a contiguous area of Wi-Fi coverage in which a subscriber can move seamlessly and maintain IP session continuity.

The essential requirement for seamless mobility is that it should be transparent to the subscriber device (i.e. Wi-Fi Client) and it should allow the device to keep and use the original IP characteristics (IP address, default GW, DNS and DHCP services) after the move.

IPV6 CHALLENGES & SOLUTIONS

IPv6 enablement in the SP Wi-Fi architecture can lead to a number of challenges for any deployment. This section describes those challenges as well as current solutions.

IPv6 Address Assignment – SLAAC vs DHCPv6

In SP Wi-Fi, each subscriber device must be assigned at least one global IPv6 address in a dynamic manner. To do so, there are two options – SLAAC (Stateless Auto Address Configuration) and DHCPv6.

Challenge*: Use SLAAC or DHCPv6?*

SLAAC is stateless, hence, it scales better than DHCP(v6), which is stateful (address assignment). More importantly, SLAAC is ubiquitously supported on almost all subscriber devices, whereas DHCPv6 is not.

Despite its simplicity and ubiquitous support, SLAAC is not quite useful until unless one of the following two is also used for conveying DNS configuration information to the devices: (1) Router Advertisement (RA) option for DNS [RFC6106], (2) Stateless DHCPv6 [RFC3736]. At the time of writing this paper, the second option i.e. Stateless DHCPv6 has better support on various subscriber devices than that of the first option.

DHCPv6 support for address assignment on the subscriber devices is not as ubiquitous as that of SLAAC. For ex, many Android devices (e.g. Samsung Galaxy 7’’ tablet with Android 4.1.0+) don’t support DHCPv6 for address assignment. Nonetheless, DHCPv6 allows the addresses to be centrally managed for ongoing allocation to the subscribers.

So, which protocol to use in a deployment?

Solution*: Use SLAAC (along with Stateless DHCPv6) short-term/medium-term.*

It is worth pointing out that given the recommendation to enable dual-stacking on subscriber devices, they would be provided with the IPv4 DNS server addresses anyway (and DNS allows A and AAAA record look up over both IPv4 and IPv6), so IPv6 DNS server address is not mandatory to ensure IPv6 usage. This takes care of a small percentage of devices not supporting stateless DHCPv6.

The MSOs should resort to alternate methods such as (RADIUS) accounting start records to keep track of IPv6 addresses used by the subscriber devices for compliance & lawful intercept purposes.

Multiple IPv6 Addresses with SLAAC

When SLAAC is used for IPv6 address assignment, each subscriber device is provided (by the Gateway) an IPv6 prefix (of prefix-length = 64), which could be a dedicated to a device or shared among a number of devices.

Challenge*: Use Dedicated vs. Shared IPv6 Prefix?*

In case of a dedicated IPv6 prefix, each subscriber device gets a unique global IPv6 prefix and uses it to assign one or more global IPv6 addresses to itself.

In case of a shared IPv6 prefix, a number of subscriber devices get a common global IPv6 prefix and use it to assign one or more global IPv6 addresses.

The shared IPv6 prefix approach causes the Gateway to store each device's each IPv6 address in the routing/forwarding table, thereby increasing the size of the IPv6 routing table by 3-8 times (as a device may assign multiple IPv6 addresses). Moreover, as the device changes its IPv6 address (due to privacy extensions), the control plane traffic (Neighbor Discovery traffic corresponding to Duplicate Address Detection (DAD)) would unnecessarily consume the precious Wi-Fi bandwidth and cause the router to keep on updating the routing/forwarding table with more than one routes per device. This arguably is sub-optimal and unnecessary.

Solution*: Dedicated IPv6 prefix (of length = 64).*

A dedicated IPv6 prefix helps to keep a single routing/forwarding entry per device.

Also, it helps to identify an individual subscriber device's IPv6 traffic based on its prefix instead of any of its individual IPv6 addresses. This allows Gateway to use a single IP session per subscriber device and provide accounting simplicity.

Location Based Services

When SLAAC is used for IPv6 address assignment, each subscriber device is provided (by the Gateway) an IPv6 prefix (of prefix-length = 64), which could be a dedicated to a device or shared among a number of devices. In SP Wi-Fi, location based services rely on the hardcoded AP's location information to proximate the subscriber device's location

Challenge*: Location based services may fail with IPv6 when SLAAC is used for address assignment.*

In IPv4-only SP Wi-Fi, location based services can be offered by letting the web portal initiate a DHCPv4 lease query for the subscriber IPv4 address and receive the DHCP option 82 information (that would convey the corresponding AP location, as inserted by the WLC acting as a DHCP relay agent during the IPv4 address assignment to the subscriber device) to figure out the subscriber device's approximate location.

In IPv6 enabled SP Wi-Fi, location based services would not work, if DHCPv6 is not involved in address assignment. So, the portal cannot determine location based on source IPv6 address of the subscriber device.

Solution*: Determine Location based on VLAN and AP mapping.*

When subscriber devices are L2 connected to the 'Subscriber Management Gateway', all traffic from a set of APs can be mapped to specific VLANs. Location is then determined by virtue of incoming VLAN's by defining different captive portals per VLAN. This is illustrated in the figure below:

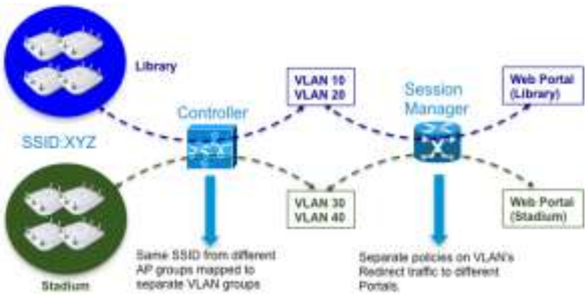
Library
SSID:XYZ
Stadium
Controller
VLAN 10
VLAN 20
VLAN 30
VLAN 40
Session Manager
Web Portal (Library)
Web Portal (Stadium)
Same SSID from different AP groups mapped to separate VLAN groups
Separate policies on VLAN's Redirect traffic to different Portals.

Figure 4 Location based Service - IPv6 Solution

The ‘Subscriber Management Gateway’ would need to have different redirection portals defined on incoming VLAN’s and location relevance is based on redirection to the right instance of the portal.

Other options include out of band mechanisms for location relevance such as accounting start records sent from WLC to a database that have both the IPv6 address of the subscriber device and the associated AP name or location string.

Multiple IPv6 Addresses & IP Sessions

Unlike IPv4, IPv6 allows multiple IPv6 addresses per interface when an IPv6 prefix (shared or dedicated) is assigned to the subscriber device.

Challenge*: Subscriber Management Gateway may create multiple IP sessions for the same subscriber device.*

IPv6 address that is used by the subscriber during the web authentication is associated with the ‘session’ on Subscriber Management Gateway and all traffic from the subscriber is identified based on this source IPv6 address. When the Wi-Fi Client has multiple IPv6 addresses and could potentially use different ones, it becomes necessary to associate all Wi-Fi Client IPv6 addresses with the existing session. Otherwise, the Gateway may create multiple sessions for the same device, impacting the overall session scale.

Solution*: Use MAC address for creating a single IP session per subscriber device.*

A common unique identifier such as a device MAC address can be used to identify a session, but this requires that the Wi-Fi Client be L2 connected to the Subscriber Management Gateway, either directly or through a tunneling mechanism.

This is deemed advantageous for another benefit – having a single session and consolidated accounting records for both IPv4 and IPv6 traffic.

If the subscriber device can not be L2 connected, then an alternate mechanism where every subscriber device gets a dedicated IPv6 prefix could be utilized, so the traffic from the device can be identified based on the common prefix instead of individual IPv6 addresses. Needless to say that such a mechanism would ensure a single IP session for IPv6.

Dual-Stack IP Sessions

Challenge*: Subscriber Management Gateway may not create a single IP session.*

Gateway may create separate IP sessions – one for IPv4 traffic and another for IPv6 traffic from/to the same subscriber device, depending on the Gateway implementations. This can impact the session scale.

Solution*: Use MAC address for creating a single IP session per subscriber device*

A common unique identifier such as a device MAC address can be used to identify a session, but this requires that the Wi-Fi Client be L2 connected to the Subscriber Management Gateway, either directly or through a tunneling mechanism.

If the subscriber device can not be L2 connected, then this challenge can not be solved – two sessions must have to be created on the Gateway.

IPv6 Multicasting & IPv4-only Devices

IPv6 fundamentally relies on Multicasting such that the (Neighbor Discovery (including Router Discovery)) messages are sent to few or every subscriber device in the WLAN domain, thereby consuming the precious Wi-Fi radio resources.

***Challenge**: Inefficient Wi-Fi radio utilization due to Multicasting.*

If the number of IPv6 enabled devices is less than that of IPv4-only devices in a given WLAN, then IPv6 multicasting to all nodes may sub-optimally consume Wi-Fi radio resources.

In IPv4 over SP Wi-Fi, the WLC usually acts as the DHCP relay and as the proxy for the subscriber devices' ARP requests. ARP requests for Wi-Fi Client MAC addresses are never sent across the backhaul network. Similar optimization is not available for IPv6.

***Solution**: Use IPv6 unicasting for Router Advertisements and let WLC respond to NS messages using local ND cache.*

If all subscriber devices are not dual-stacked (e.g. IPv6 enabled), then it would be better to deliver IPv6 Router Advertisement messages (from Gateways) as IPv6 unicast messages only to those devices that are dual-stacked, so as to save the Wi-Fi radio resources as well as the backhaul infrastructure resources.

To do so, the APs and WLCs will have to be aware of the subscriber device type (IPv6 enabled or not) and unicast the RA messages to the IPv6 enabled devices. Additionally, just like with IPv4, the WLCs would have to be IPv6 aware and respond to NS (Neighbor Solicitation) messages coming from the devices using its local ND cache. NS messages for IPv6 addresses of devices are used by the Gateway as a keepalive mechanism to detect when the device has disconnected from the network. Subscriber management gateway uses NS messages for IPv6 addresses of clients as a keepalive mechanism. These messages are multicast by the subscriber management gateway, and must be responded to by the Wireless LAN controller instead of being sent downstream across the backhaul network and then across the radio network by the AP.

This yields better performance overall.

IPv6 Wi-Fi Client Mobility

It is commonly expected that some of the subscribers would move while connected to the Wi-Fi network and it would be desirable to not let their IP communication get interrupted due to the move.

***Challenge**: IPv6 session persistency during the move within a mobility domain.*

Unlike IPv4 SP Wi-Fi network in which Discover Network Attachment (DNAv4) protocol is used by the Wi-Fi Clients to check its connectivity to the same L2 network during the move and ensure continuing with its existing IPv4 address, IPv6 has no such provisions.

With SLAAC based IPv6 address assignment, the Wi-Fi Client must have to receive the same prefix being advertised (in RA message) in order to maintain its IPv6 address. If the Wi-Fi Client sees a different prefix, then it will assign another new IPv6 address and deprecate the previous IPv6 address, eventually impacting the ongoing TCP/UDP sessions (due to upstream and/or downstream traffic not getting correctly forwarded by the Gateway to the Wi-Fi Client).

***__Solution__**: Deliver the original RA (and IPv6 prefix) to the Wi-Fi Client after the move.*

When a Wi-Fi Client moves from one AP to the next, it will receive the same RA, if it is on the same (WLC-Gateway) VLAN after the move as before the move. However, after the move, if the Wi-Fi Client is attached to an AP on a different (WLC-Gateway) VLAN, then the Wi-Fi Client move will have to be tracked and the RA from the original VLAN will still have to be sent to the Wi-Fi Client so it can continue to use its existing address and via the previous default router, where the IP session existed.

This means that the traffic to and from the Wi-Fi Client, including ND messages, will have to be tunneled between the old and new WLCs to keep the Wi-Fi Client and the Gateway transparent to the move. This is possible because the WLCs in the same mobility domain exchange mobility messages to keep track of Wi-Fi Client movement. In case of L3 roams, the Wi-Fi Client remains anchored at its home WLC by tunneling all traffic to and from the Wi-Fi Client between the foreign and home WLC. The figure below shows IPv6 Wi-Fi Client mobility:

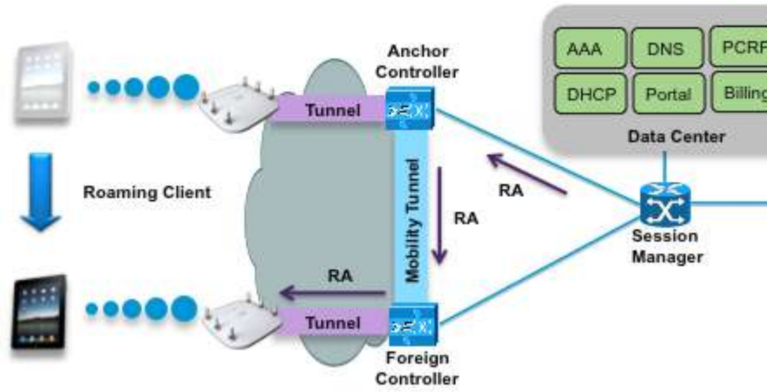

Figure 5 IPv6 SP Wi-Fi Client Mobility

The RA (Router Advertisement) is tunneled through the mobility tunnel between Anchor and Foreign WLC and unicasted to the Wi-Fi Client. Similarly, DHCPv6 and NDP messages are also processed at the anchor WLC through the dynamically established mobility tunnel.

IPv6 Default Routing & Gateway Selection

IPv6 routers (e.g. Subscriber Management Gateways) send ICMPv6 RA (Router Advertisement) messages to “all nodes” multicast address at a regular interval so as to inform all hosts of the router presence and characteristics, and to provide hosts with parameters they need to function properly on the network.

A host that wants to find out immediately what routers are present may send a RS (Router Solicitation), which will prompt listening routers to send out RA’s. RS is sent to the “all routers” multicast address. RA in response to a RS goes unicast back to the device that sent the RS, and is called a unicast RA.

***Challenge**: High-Availability and Load-sharing of Subscriber Management Gateways.*

In IPv6 SP Wi-Fi deployment, the Wi-Fi Clients typically choose their default gateways based on router preference included in the Router Advertisements. When there are multiple RAs of equal priority, Wi-Fi Clients usually choose the router that sent the very first RA as their default gateway.

In SP Wi-Fi deployments, it is preferable to load balance Wi-Fi Clients across multiple Subscriber Management Gateways. Wi-Fi Clients sessions are established on the Subscriber Management Gateway based on their selection of the default gateway. In the case of IPv4, default gateway selection is enforced by DHCP configuration. With IPv6, the Wi-Fi Clients select their own default gateway and all subscriber sessions could end up on the same Subscriber Management Gateway.

***Solution**: Use VRRP with or without IPv6 default Router Priorities.*

Set RA priorities (High, medium, low) on the Subscriber Management Gateways in order to influence the selection of default gateways. Wi-Fi Client traffic for the same SSID is load balanced on a per subscriber basis across a set of VLAN's. One Subscriber Management Gateway will have a "high" priority set for one or more VLAN's in the set and have a lower priority on the remaining VLANs. IPv6 traffic can be load balanced across a redundant set (N:1 or 1:1) of Subscriber Management Gateways.

The figure below shows an overview of load balancing and redundancy for IPv6 Wi-Fi Clients:

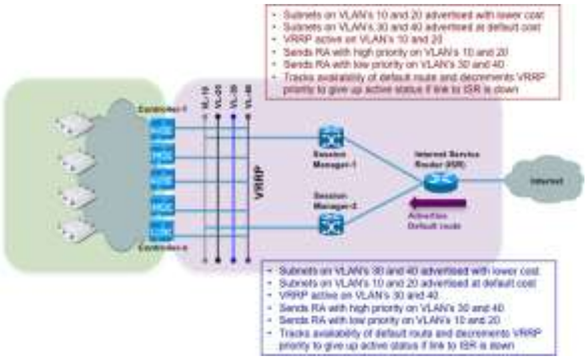
Subnets on VLAN's 10 and 20 advertised with lower cost
Subnets on VLAN's 30 and 40 advertised at default cost
VRRP active on VLAN's 10 and 20
Sends RA with high priority on VLAN's 10 and 20
Sends RA with low priority on VLAN's 30 and 40
Tracks availability of default route and decrements VRRP priority to give up active status if link to ISR is down
Controller-1
VL-10
VL-20
VL-30
VL-40
WLC
WLC
WLC
WLC
WLC
Controller-n
VRRP
Session Manager-1
Session Manager-2
Internet Service Router (ISR)
Advertise Default route
Internet
Subnets on VLAN's 30 and 40 advertised with lower cost
Subnets on VLAN's 10 and 20 advertised at default cost
VRRP active on VLAN's 30 and 40
Sends RA with high priority on VLAN's 30 and 40
Sends RA with low priority on VLAN's 10 and 20
Tracks availability of default route and decrements VRRP priority to give up active status if link to ISR is down

Figure 6 VRRP and Load-sharing

The same SSID is load balanced across a group of VLAN's on a per subscriber basis by the set of WLC's. Depending on the VLAN's assigned to Wi-Fi Clients, they will choose the Subscriber Management Gateway with the higher priority RA as their default router. Downstream traffic to the Wi-Fi Client will routed by the ISR (Internet Services Router) through the correct Subscriber Management Gateway based on route preferences at the ISR. When a subscriber-facing interface goes down, VRRP will ensure that Wi-Fi Client traffic will be processed by the redundant Subscriber Management Gateway and traffic symmetry (through the same Subscriber Management Gateway) will be maintained after route convergence at the ISR. Downtime is limited to VRRP and route convergence.

Transparent Auto-Logon (TAL)

Auto Logon (TAL) is used to enhance the subscriber experience by recognizing the Wi-Fi Client and bypassing the authentication requirement for a previously authenticated subscriber using the same device for a fixed time period, say 48 hours. As long as the subscriber accesses the network at least once during the set period, he/she will not have to authenticate on the network again since their identity is maintained in the network.

TAL is done by caching a unique ID – typically the MAC address of the Wi-Fi Client and then authorizing subsequent access against this cache based on the source MAC address of the incoming packet.

***Challenge**: Multi-hop L3 connectivity between subscriber device and Gateway.*

When subscribers are L2 connected, the Subscriber Management Gateway has access to the Wi-Fi Client's MAC address and can attempt an authorization. If the Wi-Fi Client is L3 connected and using an IPv4 address, the Subscriber Management Gateway uses a DHCP lease query to obtain the MAC address of the Wi-Fi Client. When, the Wi-Fi Client is L3 connected and has an IPv6 address (Stateless or SLAAC), the Gateway has no visibility into the Wi-Fi Client MAC address and cannot attempt an authorization

***Solution**: Enforce L2 connectivity or DHCPv6.*

To ensure TAL, IPv6 Wi-Fi Clients will have to be L2 connected to the Subscriber Management Gateway, so that they can be authorized using their MAC addresses. Alternatively, stateful DHCPv6 will have to be enforced so the Subscriber Management Gateway can use a DHCPv6 lease query to determine Wi-Fi Client MAC address for authorization.

P2P Applications and First Hop Security (FHS)

Peer-to-Peer communications must be allowed in a public SP Wi-Fi network to support many P2P applications like Skype, instant messaging, chat etc.

***Challenge**: P2P communications allowance may also allow Layer 2 connectivity among the Wi-Fi clients.*

If any WLC implementations require having all Wi-Fi clients with Layer 2 connectivity (to each other) for supporting P2P communications, then such implementations can introduce security vulnerabilities in an IPv6 network such as clients sending out RA's or responding to DHCPv6 messages..

***Solution**: Enable FHS solutions and force ALL P2P communications through the Subscriber Management Gateway*

FHS enablement would provide RA Guard - block all RA messages from all Wi-Fi clients, DHCPv6 Guard - recognize and block DHCPv6 responses from all clients, Source Guard - drop all traffic not sourced from client's IP address etc. Since the WLC responds to NS messages with entries in the local ND cache, it is possible to always force all Peer to Peer communication through the Gateway, which is the optimal place to enforce the policies and account for traffic usage.

Lawful / Legal Intercept (LI)

Cable MSOs are almost always required, as part of their regulatory compliance obligations, to keep a history of the IP addresses used by the subscribers, before placing any interception tap.

Challenge*: Tracking and logging use of IPv6 addresses*

With SLAAC, IPv6 addresses are self assigned and each device can have (and use) multiple IPv6 addresses. Unfortunately, there is no centralized address management to log IPv6 addresses used by subscribers with SLAAC (and stateless DHCPv6).

Solution*: Use out of band techniques to log and track IPv6 address usage*

One approach is to use the accounting start and stop records (RADIUS) that have client MAC addresses and IPv6 / IPv4 addresses and sometimes, even user names. These records will have to be generated as soon as a client gets assigned an IPv6 address and records will have to be stored in a database for historical reference / tracking for a period of time in accordance with regulatory compliance requirements.

There are other methods being discussed to address this issue. Please refer to this IETF draft - http://tools.ietf.org/html/draft-asati-dhc-ipv6-autoconfig-address-tracking-00

Prepaid Subscriptions

Prepaid subscriptions are offered based on time or volume or a combination of the two. All subscriber traffic and usage, regardless of IPv4 or IPv6 must be accounted for.

Challenge*: Real time computation of usage and quota enforcement for dual-stack clients*

If there are two different sessions for IPv4 and IPv6 traffic, then accounting records will have to be reconciled (by the accounting/billing server) in real time to compute usage and enforce quotas. This can pose increasing difficulty to the accounting/billing server and sacrifice the accuracy of enforcement.

Solution*: Enforce a single dual-stack session per device by having L2 connectivity between client and Subscriber Management Gateway*

With L2 connectivity between clients and Subscriber Management Gateway, session identification could be based on subscriber MAC address and all traffic to and from the subscriber (IPv4 and IPv6) will have the same identity making it easier to enforce volume or time based quotas real time. This has the added advantage of reducing the total number of sessions to be managed by the Subscriber Management Gateway.

Service Based Billing

MSOa may like the option of differentiated billing based on services consumed by the subscribers. Video, for example, could be billed at a different rate than voice. Similarly, access to MSO content could be provided at a reduced rate or tiered billing rate based on blocks of bandwidth consumption over a period of time.

Challenge*: Consolidated accounting for services, regardless of whether they were consumed with IPv4 or IPv6*

Typically, services are independent of the type of stack (IPv4 or IPv6) used and in the case of dual-stack clients, the same services could be consumed using both IPv4 and IPv6. An example would be to identify a RTP stream for differentiated billing. RTP can run over both IPv4 and IPv6 because it contains no specific assumptions about the capabilities of the lower layers, except that they provide framing.

***<u>Solution</u>**: Leverage QoS policies having both IPv4 and IPv6 traffic classes*

In Quality of Service design, Service flows (Services) are generally identified using characteristics from L4 through L7 and must include the option to match both IPv4 and IPv6 traffic classes. A service flow is set of traffic classes and is part of the services definition. When the services are installed for the subscriber on the Subscriber Management Gateway, an accounting start record, identifying the service name is sent. Interim accounting and accounting stop records are sent for all traffic that matches characteristics defined in all of the traffic classes associated with the service flow.

EVOLUTIONS

As we understand and assess the challenges, it becomes important to think outside the box and evolve IPv6 usage in SP Wi-Fi for further optimization. The below points discuss few such optimization opportunities:

1. If DAD could be disabled in case of a dedicated IPv6 prefix per subscriber device, then it would significantly reduce the control plane traffic on the Wi-Fi. Because the Gateway controls the prefix assignment, it can obviate the possibility of duplicate address assignment.

This would be helpful in the context of challenge described in section 4.6

2. If the device could acquire new IPv6 prefix/address after the move (from one AP (and WLC) to another AP (and WLC)) while keeping the old one(s), then tunneling of the control plane (i.e. original RA) and the data plane traffic could be limited to the existing IPv6 connections, while allowing the new IPv6 connections to use the new IPv6 prefix/address.

This would be helpful in the context of the challenge described in section 4.7, since the device would eventually stop using the old IPv6 prefix/addresses and could let go of them. This would cut down on having to tunnel the traffic from WLC to WLC and pave the way for optimal control plane and data plane traffic forwarding.

3. IP address logging is a critical prerequisite for Lawful Interception. When SLAAC is used for IPv6 address assignment, then IP address logging could fail. If the logging can still be done by the DHCP server (even if SLAAC is used), then it would be operationally beneficial to the MSOs. Thankfully, such a solution [4] is now discussed at the IETF DHC working group.

IPV6 STRATEGY / RECOMMENDATIONS

It is important to summarize the recommendations for IPv6 enabled SP Wi-Fi deployments:

1. Focus on IPv6 enablement for subscriber devices followed by infrastructure
2. Use Dual-stacking (i.e. IPv4 + IPv6) on subscriber devices
3. Leverage SLAAC for IPv6 address assignment (along with stateless DHCPv6) in short-term/medium-term and (stateful) DHCPv6 in long-term
4. Use a dedicated IPv6 prefix per subscriber device
5. Use one single IP session per subscriber device (whether dual-stacked or not)
6. Consider Unicast Router Advertisement
7. Preserve device's IP address during Mobility events, if possible
8. Use VRRP and VLANs on Subscriber Management Gateways for better high-availability and load-sharing
9. Prefer L2 connectivity between devices and Gateways (instead of multi-hop L3 connectivity)
10. Enforce First-Hop Security on WLC and Gateways, as well as subscribers' P2P communication via Gateways
11. Use HTTP redirection instead of L4 redirection
12. Leverage 'MAC address' as the IP session classifier
13. Log IPv6 addresses per subscriber.

SUMMARY

Is IPv6 over SP Wi-Fi a reality now? The answer is YES.

While there are obvious challenges to enabling IPv6 in SP Wi-Fi, there are solutions. There are certainly opportunities for optimization for further evolving IPv6 adoption in SP Wi-Fi networks. We urge the MSOs to start developing the strategy for enabling IPv6 in their SP Wi-Fi deployments (and pave the way for reducing the need for Carrier Grade NAT (CGN)44).

REFERENCES

[1] IEEE 802.11

[2] https://www.arin.net/resources/request/ipv4_countdown.html

[3] http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns673/data_sheet_c78-707266.html

[4] http://tools.ietf.org/html/draft-asati-dhc-ipv6-autoconfig-address-tracking-00