IPv6 Application Note:

3rd Generation WiFi – Carrier class secure mobility

Contributors

Jim Bound, jim.bound@hp.com
Chair IPv6 Technical Directorate http://www.ipv6forum.com
Chair of the North American IPv6 Task Force http://www.nav6tf.org
HP Fellow, Hewlett Packard Corporation

Junaid Islam, junaid@pegasysglobal.com
Member of the IPv6 Forum
Managing Partner, Pegasys Global Partners

Overview

WiFi is the hottest area in networking industry today for good reason. Many industry experts believe WiFi's ability to deliver Ethernet-like bandwidth to mobile compute devices will spur a new generation of consumer multimedia services like video conferencing as well provide a low cost strategy to improve in-building and off-net coverage cellular coverage. However before WiFi can be deployed as a carrier solution its poor manageability, security and mobility features need to be addressed.

WiFi's enterprise heritage has become a big challenge for service providers now wishing to provision large scale networks where thousands of access points need to connect millions of moving users. In order for WiFi to meet its full potential as a low cost carrier access solution it needs to develop a mechanism to provision thousands of Access Points without the hassle of manual configuration, a security model that extends the over-the-air benefits of 802.11i to a network level and a mobility scheme that allows users to roam without having to re-start their application at every hot spot. In short what WiFi needs is IPv6.

In preparing this paper it is the goal of the IPv6 Forum to show how the combination of WiFi innovation plus v6 network intelligence can be used to enable "carrier class secure mobility" in WiFi and thus allow service providers to take full advantage of this revolutionary technology.

The Next Step for WiFi – Carrier Class Secure Mobility

With an estimated 1 Billion cellular phones in use, mobile voice is one of the most successful technology deployments in human history. In fact, the only other technology with a similar growth curve is the Internet. Thus it is not surprising that many industry experts believe high speed mobile IP services (i.e. the marriage of mobile wireless technology combined with the global connectivity of IP) is the next big wave. However until recently, the only solution for service providers wishing to launch a high speed mobile IP offering was to either upgrade their existing 2G cellular infrastructure or deploy a 3G network – both expensive alternatives. But that has all changed now…

With the advent 802.11 networks (also known as WiFi) public service providers now have a low cost solution for enabling high speed mobile IP services. The enterprise level pricing of WiFi access points and their use of un-regulated spectrum has enabled service providers to quickly "light up" hot spots with relative ease. Unfortunately today's enterprise focused WiFi solutions do not lend themselves to cost effective deployment or high margin services

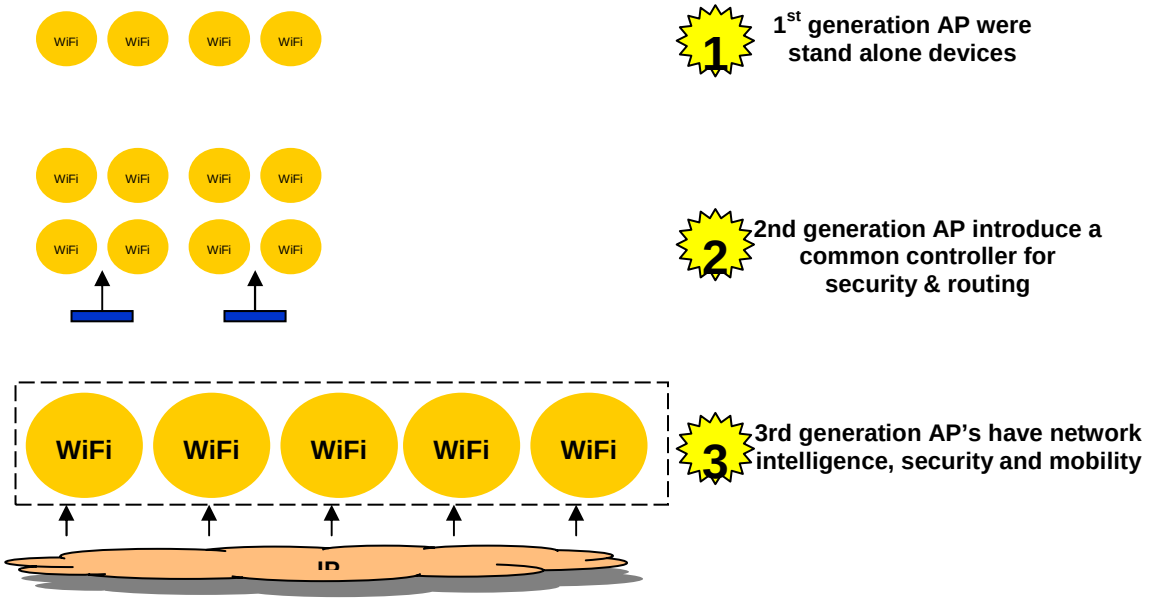
WiFi's enterprise heritage has become a big challenge for service providers now wishing to provision large scale networks and value add services. The current lack of provisioning features requires that every access point must be individually installed. The current lack of network security means that even if service providers use 802.11i for over-the-air encryption, network level security is not guaranteed. And finally the current lack of a mobility scheme requires that users manually re-establish a connection every time they roam from one hot spot to another. Thus given WiFi's current weaknesses it is not surprising that service providers are loosing money on their current hot spot investments.

For WiFi to move beyond a commodity priced service it needs to first become a "carrier class secure mobile" infrastructure on which service providers can offer compelling services – in short WiFi needs to be enhanced with IPv6's connectivity, security and mobility. By enhancing WiFi technology with IPv6 network intelligence, service providers have the ability of creating a carrier class secure mobile infrastructure – one that offers the benefits of enterprise level pricing on the investment side yet the potential of high margin differentiated service revenue on the return side.

3rd generation WiFi – Carrier class secure mobility

WiFi technology has gone through a substantial evolution over the past few years. 1st generation WiFi products that had little or no network intelligence, and were used primarily to network home offices and conference rooms or to provision stand alone hot spots. Moreover the use of WEP and lack of management features meant that many enterprises avoided using 1st generation WiFi products all together, as the security and connectivity issues were too burdensome.

2nd generation WiFi solutions aimed to address the short comings of 1st generation products by connecting multiple access points to a dedicated Firewall/VPN switch to improve manageability and mobility via VLAN switching. While 2nd generation WiFi products were certainly a step up from dumb access points they are still inadequate for service provider environments where the scale of the network is many times greater than a typical office building. Moreover while VLAN switching is an adequate mobility solution within an enterprise site, for a service provider wishing to cover multiple city blocks, it simply does not scale.



For WiFi to become a carrier class solution it needs to offer security and mobility functionality comparable to that of cellular networks before it can be acceptable– and that is where IPv6's provides assistance.

3rd generation WiFi can best be described as the combination of WiFi technology plus IPv6 network intelligence to improve functionality with respect to connectivity, security, and mobility. Activity in 3rd generation WiFi solutions is primarily being driven by the needs of service providers for a highly scalable architecture that has the ability to support millions of roaming users across thousands of access points.

In the following section we will take a deeper look at how the "WiFi technology + v6 intelligence" formula is being used to create 3rd generation WiFi solutions. We will look at how intelligent access points + v6 is being used to lower the cost of deployment, how 802.11i + v6 is being used to provide network level security, and how VLAN switching + v6 is being used to provide seamless user mobility.

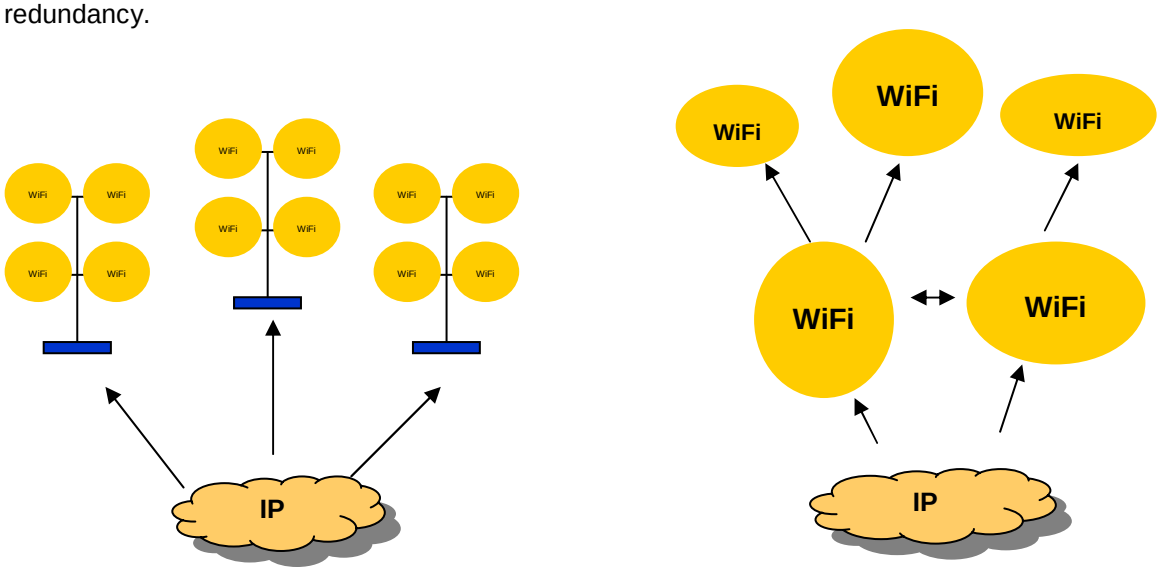
Access Point Provisioning

Deploying hundreds or thousands of access points can be a very difficult task for service providers especially when one considers that every node must be individually configured. Even with 2nd generation WiFi solutions that have the ability to configure multiple access points from a single switch, deployment can be extremely arduous as the hub-spoke topology often doesn't reflect the environment one has to work with. For example while finding an Ethernet port to connect an access point is not a problem when one is working in an office building, out on the street corner it is another issue. Ideally WiFi needs to have a more flexible and autonomous deployment model that leverages whatever connectivity a service provider is able to get.

To address the shortcomings of 2nd generation WiFi switches and access points, service providers are now experimenting with intelligent 3rd generation access points that have the ability to discover the presence of other nodes autonomously and connect with them either via wired or over-the-air trunks. This feature allows intelligent access points to dynamically determine the topology for their local access point cluster.

By enhancing intelligent access points with IPv6's stateless node discovery capability we are able to take the benefits of local cluster discovery to the next level. Stateless node discovery extends the benefits of access point auto-discovery to a network level by enabling adjacent clusters of radios to determine their optimal topology and build a resilient mesh.

The illustration below highlights the difference between a 2nd and 3rd generation access point deployment. On the left side we have a view of a 2nd generation network where access points must be manually configured and the topology options are limited by the fact that the switches function as network connection points. On the right side we have a view of a 3rd generation WiFi network where intelligent access points are able to discover adjacent nodes and dynamically determine their optimal routing topology. Moreover the 3rd generation network is able to dynamically provision wireless trunks to adjacent nodes in order to improve load balancing and redundancy.

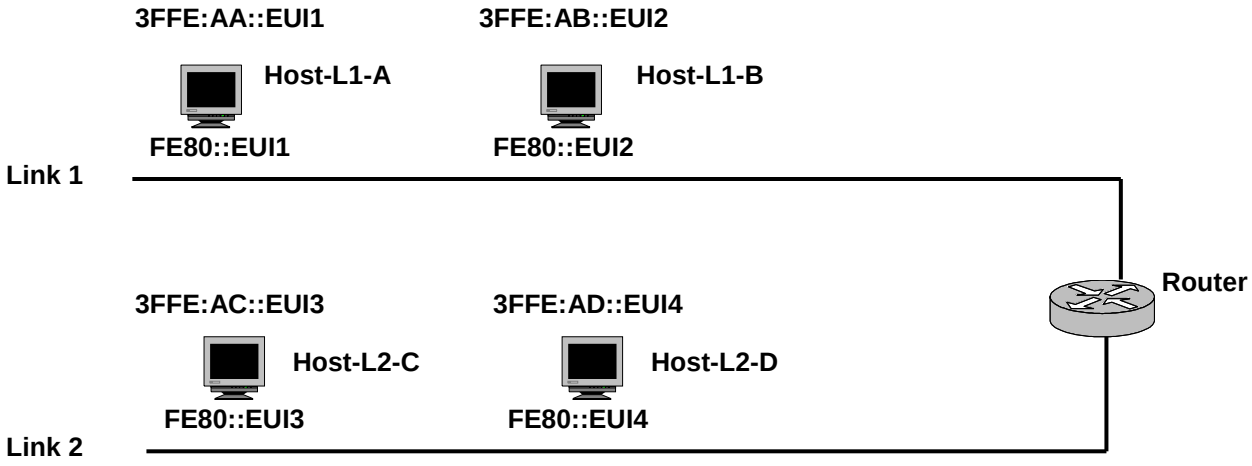


IPv6 Stateless Node Discovery– the foundation for Access Point auto-configuration
When IPv6 features like stateless node discovery are embedded into 3rd generation access points, adjacent clusters of access points can autonomously determine their optimal connectivity, load balancing and redundancy scheme without any operator configuration.

Internet Protocol version 6 (IPv6)[RFC 2460], when used as the IP Protocol, nodes can discover each other and form IPv6 addresses to communicate on an 802.11 network using what is called Neighbor Discovery [RFC 2461] and Stateless Auto-configuration [RFC 2462]. IPv6 supports a robust stateless node discovery paradigm, which provides the following features:

- Discover the presence of nodes on the network
- Discover the Data link Layer of nodes on the network
- Discover Routers on the network
- Discover Link Configuration Parameters on the network

These features then permit an IPv6 node to obtain and maintain information about the accessibility of another node on the network for communications. Node discovery is the predecessor to the node obtaining an address from IPv6 auto-configuration. This core IPv6 feature also permits nodes to communicate on networks where there are no routers within an ad hoc environment.



Multicast used for link segment packet Communications

The diagram above depicts an IPv6 multiple link segment network connected by a router. Each IPv6 node has a Link-Local (FE80::) and Global Address (3FFE::) assigned to the node for communications in the above diagram. An IPv6 node when booted on an IPv6 Link first creates a Link-Local address by taking the architecturally defined prefix in Neighbor Discovery FE80, and appending an End User Identifier (EUI), determined by the access point, to that prefix. This Link-Local address is then verified on the link that it is not duplicated with other Link-Local addresses on that nodes Link.

The IPv6 node then uses the Link-Local address to send on the IPv6 Link Neighbor Solicitations, enabling other nodes on that Link will see those multicast Solicitations, and then return Neighbor Advertisements. After this communications process all access point's on the IPv6 Link can now communicate without the use of servers or routers in a stateless manner.

The IPv6 nodes will also listen for Router Advertisements on the IPv6 Link (or send Router Solicitations), which provide address prefixes, link configuration parameters, and information on whether to use a Stateless or Statefull method for address assignment and to locate additional network configuration parameters using the Dynamic Address Configuration Protocol for IPv6 (DHCPv6) [RFC 3315].

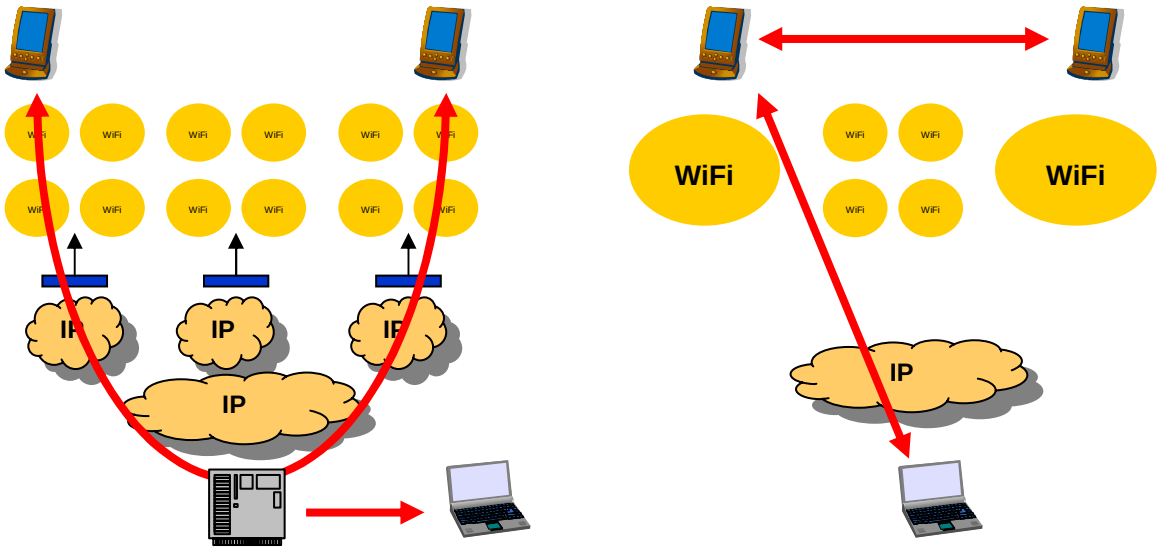
Application Security

There are two security issues that need to be addressed before WiFi can become a carrier access solution; the first is assuring the privacy of the data transmitted over-the-air, the second is protecting the network itself against intrusion. Because mobility is an essential aspect of WiFi networks, old techniques that rely on stable, hardwired connections between users and network connection points are no longer sufficient to assure proper access control. Moreover WiFi networks are orders of magnitude more vulnerable to MAC (Media Access Control) address spoofing than wired LANs.

To address air interface security1st generation WiFi products used WEP as a security solution which relied on using a simple shared key to encrypt message payloads. Unfortunately the WEP protocol transmitted the key along with every packet enabling simple monitoring programs like Air Snort to de-encrypt user traffic by breaking the relatively short key. As a response to WEP's flaws 2nd generation products migrated to 802.1x to eliminate the transmittal of the key and incorporate a longer key. Moreover work in now under way for a 3rd generation security solution based on AES within the 802.11i standard.

While 802.11i secures the air link it doesn't address the issue of network level application security – that is where IPv6 comes in. By combining AES 802.11i with v6 we are able to enhance the security to a network level by providing trusted end to end connectivity between mobile users.

The illustration below highlights the difference between a 2nd and 3rd generation WiFi networks. On the left side we have a view of a 2nd generation network where the lack of strong over the air security and NAT means that user traffic can be intercepted at multiple points. On the right side we see how 802.11i when combined with v6's end to end connectivity guarantees application security because no third parties can view the encrypted payload. Moreover the end to end connectivity model also provides a more efficient use of bandwidth for multimedia services like video conferencing.



IPv6 end to end connectivity – the foundation for network security

IPv6's large address space supports end to end application connectivity and security between two nodes across a network without the use of NAT. Strict end to end connectivity ensures that only trusted parties are able to view packets - not ISPs, routers, switches, network manager stations, nor snooping clients. Moreover, when using IPSec end to end all that is exposed is the Header and Options fields' information.

Current use of NAT in IPv4 networks is a major security flaw because both parties cannot initiate connections with each other over a network. Whether using asymmetric NAT or symmetric NAT users cannot initiate a connection with the other party because they have a private address on their Intranet. This means when a node wants to communicate out of their Intranet, a NAT software or hardware function (usually on a router) must accept the connection and then rewrite the sending nodes packet with an IP source address that is visible to destination network. The NAT function then must maintain state so that when a responding packet appears, NAT can rewrite the IP destination address so the packet can be sent to the original sending node on the Intranet. NAT presents a major hole for IPsec it uses the IPv4 address to create the security association. When the NAT function rewrites the IP address of a packet that association is lost and the packet cannot be authenticated or decrypted by the receiving node.

Also NAT does not provide security, but only translation of the IP addresses as described above. An attacker can capture a packet to a NAT function, rewrite the header, and then put whatever data it chooses for the attack behind the IP header, and the NAT function would not know or check the packet for this attack. The packet would be delivered to the node with the alterations by the attacker from the network path into the NAT function.

IPv6 permits two wireless nodes to obtain and share IPsec keys from an authority securely using key management and then use IPsec to authenticate or encrypt packets sending them across the wireless network (Access Points, Routers, etc). The packets are delivered solely based on the IPv6 destination address in the IPv6 header. If AAA is being used for authentication to enter or leave a Wireless network then IPsec with v6 can also be used to secure that communication. This permits multi-level security when communicating with the IP network layer within a WiFi network. .

It should be noted that a firewall can still used to verify incoming and outgoing packets by using v6 header information and an out of band identification mechanism on the network (e.g. Smart Card, Guard Key Software on the node) without breaking the strict end-to-end trust model.
.

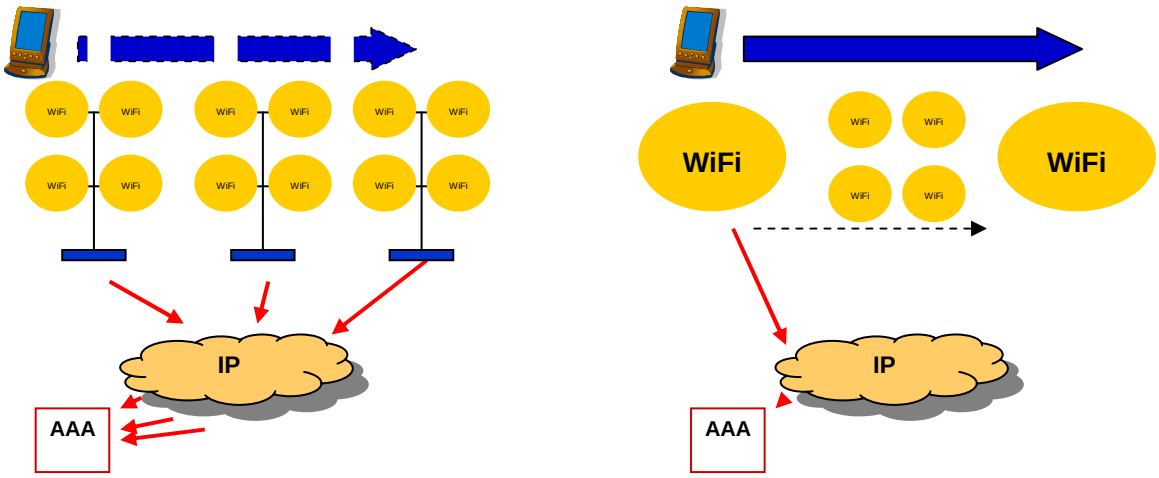
Mobility

The third important component of how v6 is able to facilitate a 3rd generation WiFi solution is through enabling seamless mobility for users. With 1st generation access points users were forced to re-authenticate themselves every time they moved within their office. 2nd generation WiFi solutions addressed the complete lack of mobility by providing a VLAN switch to maintain sessions by switching user traffic back to the original WiFi switch port they're on. While VLAN solution is adequate as an Enterprise solution where mobility is "in-building" phenomena, in a service provider environment where users are likely to travel from one cluster of hot spots to another it is far from adequate.

In order to improve mobility service providers are now trialing access points that have VLAN switches built into them. This feature has the benefit of enabling adjacent access points to maintain sessions by switching traffic amongst themselves without the need of a separate switch. However still does not address the issue to network mobility – and that is where v6 comes in.

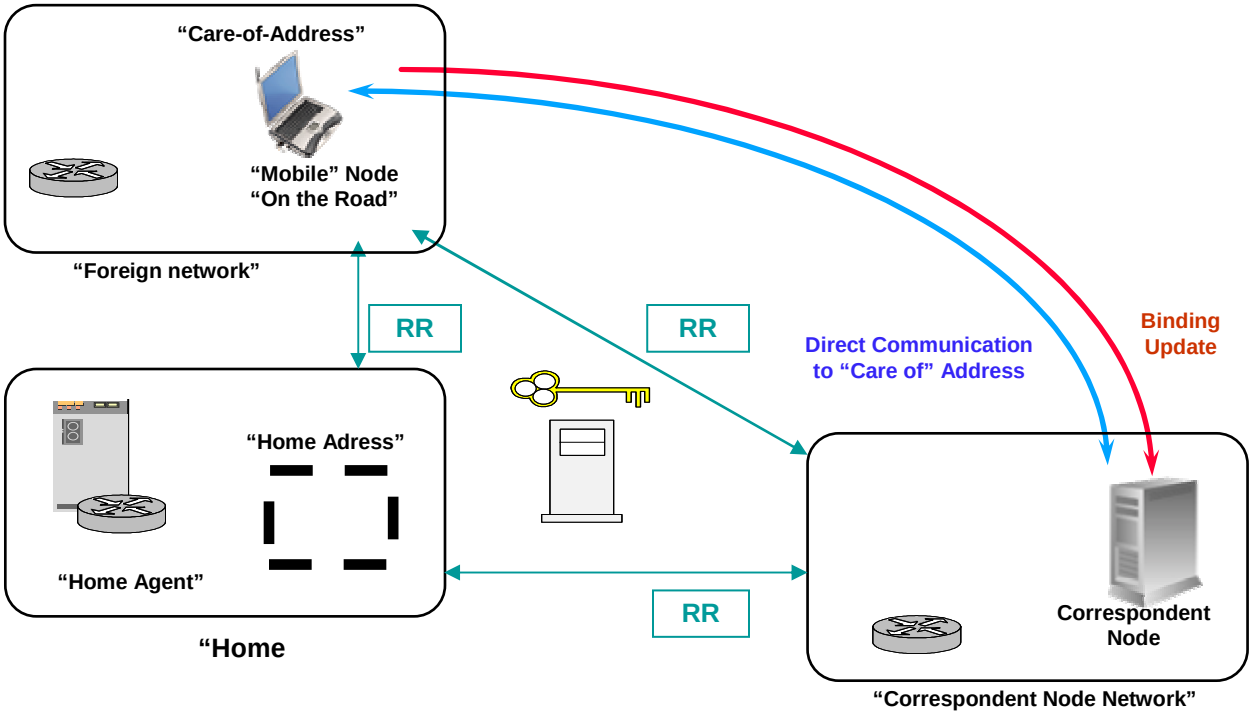
By enhancing embedded VLAN switching in access points with v6 we are able to extend the benefits of local mobility to a network level by Mobile IPv6. MIPv6 enables the seamless of IP sessions so that users can travel from their home to their office to a hot spot without having to re-start an application.

The illustration on the benefits of MIPv6 below highlights the difference between a 2nd and 3rd generation WiFi networks. On the left side we have a view of a 2nd generation network where as a user moves from one hot spot to another he must re-authenticate himself whenever moves out side an cluster of access points. On the right side we have a view of a 3rd generation network where the user experiences seamless connectivity as he travels across multiple hot spots through a combination of embedded switching within an access point cluster and MIPv6 session re-establishment when entering new networks.



Mobile IPv6 – a mechanism for application mobility
Mobile IP permits users to remain connected across wireline (e.g. Ethernet, xDSL) and wireless (e.g. 802.11, Cellular, Satellite) networks while roaming from one network to another. This permits the user to stay connected in route to the airport from home, rather than shutting down their PDA/Laptop at home, and reconnecting at the WiFi location at the airport.

The diagram on the following page illustrates the multiple phases of a Mobile IPv6 connection. On the Home network a Mobile Node receives its Home Address as any IPv6 node. The Mobile Node registers that address with the Home Agent, which is a router that keeps the location information for the Mobile Node when it moves to a Foreign Network. The home agent also stores the Mobile Nodes Care-of-Address when the Mobile Node is away from Home. A peer node that the Mobile Node communicates with is defined as the Correspondent Node (which may be stationary or mobile).



Security between the Mobile Node and Home Agent can be accomplished using the IP Security Protocol (IPsec) Architecture [RFC 2411]. This permits secure communications between the Mobile Node and the Home Agent. When a Correspondent Node receives a packet from a Mobile Node it first checks its binding caches to see if it has a cache of the Mobile Nodes Care-of-Address, and if it does not the Correspondent Node will send the packet to the Mobile Nodes Home Address. The Home Agent will receive all packets sent to the Mobile Node when it is away from home and then tunnel the packet to the Mobile Nodes new location.

One powerful feature of v6is that it enables a Mobile Node and Correspondent Node to communicate directly, without going through a Home Agent, by the use of the Mobile IPv6 Route Optimization. In the diagram above that is done using a procedure defined as Return Routability (RR) within the Mobile IPv6 protocol in which the network path between the Mobile Node and Correspondent Node is secured through the RR procedure. Once this happens packets can be directly forwarded between the communicating parties without the need of the Home agent.

Putting it all together – Carrier class WiFi Network

Taking a step back, we can see how v6 enhanced 3rd generation WiFi network might operate.

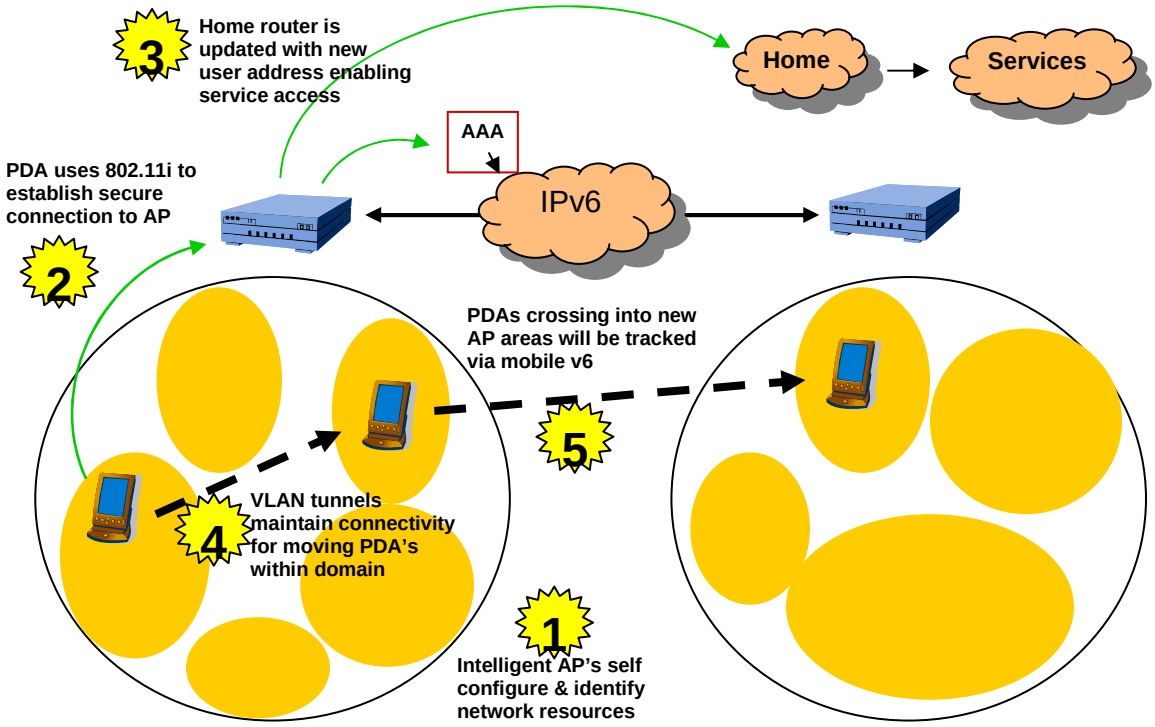
1/ Intelligent access points leverage v6 stateless node discovery to determine the local topology and work in conjunction with other access points to define the best connectivity, load balancing and redundancy plan.

2/ Users can now authenticate themselves using 802.11i to set up a secure link to their local access point which in turn contacts an AAA server to verify accessibility.

3/ Once authenticated, the access point contacts the home agent for the user with their new care of address. This enables the user to re-join active IP sessions that he may have been previously using.

4/ As users roam within a local cluster of access points VLAN switching is used to maintain connectivity across wired and wireless trunks.

5/ For users who move outside an access point cluster into a new group, Mobile IPv6 re-establishes active sessions without the need for application re-starts.



Closing thoughts…

The global reach of the Internet now enables service providers to launch multimedia services anywhere there is adequate broadband connectivity. Unfortunately this also implies that unless service providers develop compelling services that they will become bit pipes for their competitors. Thus the key to survival and success in this era of near ubiquitous connectivity is to develop a strong core competence in IP mobility and multimedia services – and this is where IPv6 can play a powerful role.

As the example of 3rd generation WiFi shows us, IPv6 can be used to improve the productivity of network elements by enhancing their level of connectivity, security and mobility. IPv6 is more than just a longer address field but a more intelligent approach to build carrier class networks. Features like stateless node discovery when combined with WiFi innovations like wireless backhaul allow service providers to deploy network assets more intelligently than possible through manual configuration.

Looking to the future, IPv6 allows service providers to enter new markets and deploy new services with greater speed than ever before by providing a common foundation for multimedia services. By significantly improving connectivity, security and mobility to their network assets, IPv6 allows services providers to create new applications without having to re-develop connectivity features every time they wish to create a new service.

For further reading please refer to www.ipv6forum.com