ALCATEL-LUCENT WLAN GATEWAY

FOUNDATION TO DELIVER A SUPERIOR CUSTOMER EXPERIENCE

APPLICATION NOTE

Alcatel·Lucent

ABSTRACT

Carrier Wi-Fi® technologies are playing an ever more important role in the mobile broadband strategies of telecom operators including fixed operators, multiple service operators (MSOs), mobile network operators (MNOs), mobile virtual network operators (MVNOs) and converged operators. Wi-Fi usage and the number of Wi-Fi access points are rapidly increasing and a range of carrier Wi-Fi market applications beyond hotspots is emerging. Operators are looking for new service revenues and competitive advantage by leveraging unlicensed Wi-Fi as an access technology and integrating their carrier Wi-Fi applications onto a common Wi-Fi core with carrier-grade infrastructure and systems.

With the goal of a simple, secure and seamless user experience, operators are actively looking to integrate their carrier Wi-Fi with wireless and wireline IP networks. As part of Alcatel-Lucent carrier Wi-Fi portfolio, the WLAN Gateway plays a key role in realizing this goal by anchoring the carrier Wi-Fi access infrastructure and providing the gateway to the IP based wireless and wireline services networks.

This Application Note describes several service deployment scenarios that leverage carrier Wi-Fi as an access technology, using the carrier-grade WLAN Gateway functionality of the Alcatel-Lucent 7750 Service Router (SR).

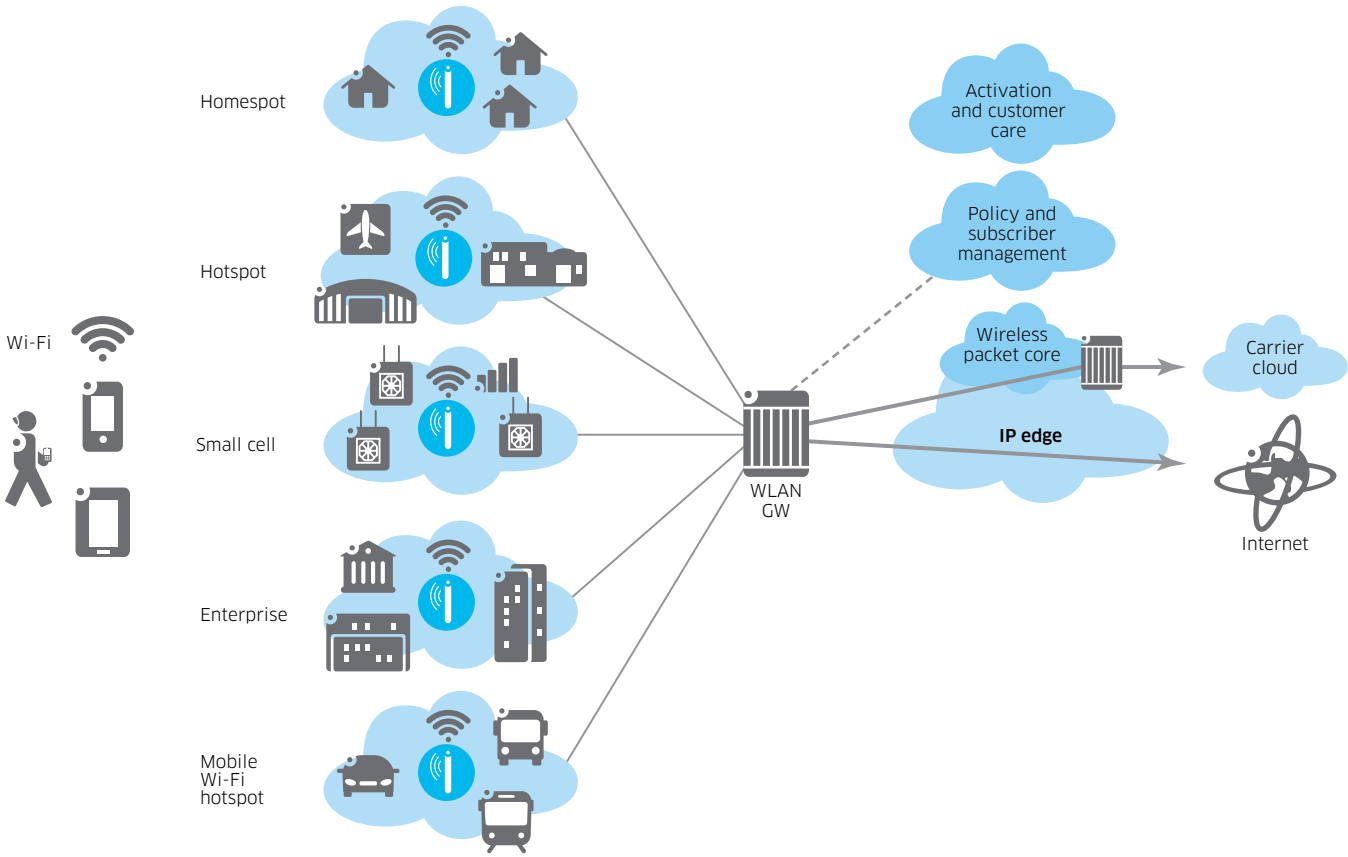
TABLE OF CONTENTS

1. LEVERAGING WI-FI ACCESS TECHNOLOGY

These days, no operator's mobile broadband strategy is complete without carrier Wi-Fi technologies. The potential for new revenue generation is compelling, and in many markets competitive positioning demands it.

Fixed operators are approaching carrier Wi-Fi from the perspective of community Wi-Fi, venue coverage and extended hotspot strategies. Mobile and converged operators are looking to integrate carrier Wi-Fi with their cellular networks to provide their users with with a seamless mobile broadband experience, which is best derived from secure and trusted connectivity across carrier Wi-Fi and cellular networks.

Figure 1. Carrier Wi-Fi market applications



In this dynamic environment, the suite of carrier Wi-Fi market applications is evolving rapidly. To date, some of the most widely adopted applications include:

- Homespot – sharing of residential Wi-Fi access points with guests and passers-by
- Hotspot – access to private, metro or citynet-based mobile broadband services from venues or urban areas such as restaurants, stadiums and parks
- Small Cell – access to licensed cellular and unlicensed Wi-Fi radio access infrastructures
- Enterprise – continued expansion of hosted Enterprise Wi-Fi infrastructures, as well as access to Wi-Fi within managed services from operators
- Mobile Wi-Fi Hotspot – carrier Wi-Fi access points that use cellular backhaul connections to support deployments in trains, public transport, and taxis

To support these market applications, operators are making strategic changes to their networks.

First of all, it has become a strategic imperative for operators to implement carrier-grade Wi-Fi core infrastructure and systems. They are also discovering the advantage of leveraging unlicensed Wi-Fi spectrum to expand their service footprints. While they are typically using carrier Wi-Fi access equipment from more than one vendor, they are ultimately integrating their carrier Wi-Fi applications onto a common carrier Wi-Fi core.

With these Wi-Fi network changes in place, operators can focus their attention on the delivery of a simple, secure and seamless user experience across wireline and wireless networks. The WLAN Gateway plays a critical role in making this happen. It requires advanced integrated gateway capabilities such as authentication, subscriber management, billing and anchoring of the user equipment (UE). It must also provide high bandwidth and aggregation, granular traffic conditioning, high density subscriber management and high availability. What's more, the WLAN Gateway must have the networking flexibility to concurrently support multi-vendor Wi-Fi access point (AP) infrastructure, and flexibly and efficiently integrate into the operator's IP network and business strategy.

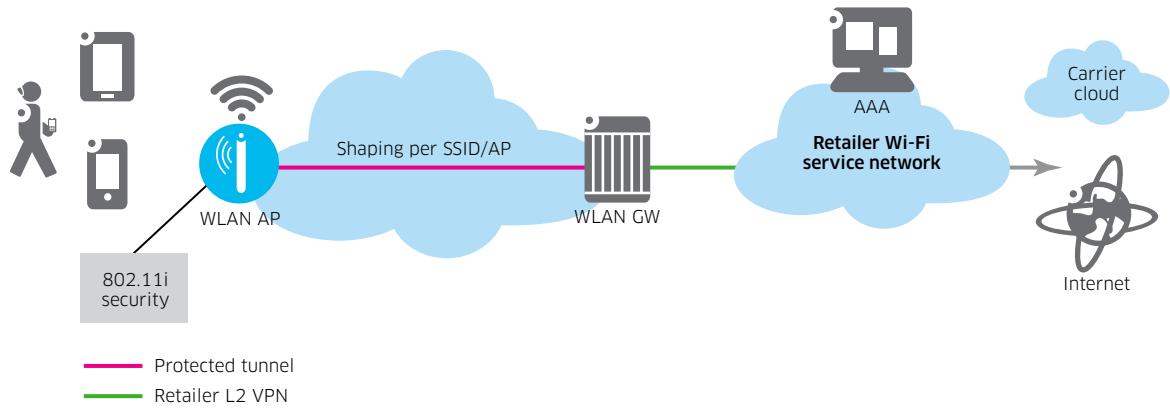
The following section describes three scenarios that demonstrate how an operator can meet the service and experience requirements of carrier W-Fi using the WLAN Gateway functionality of the Alcatel-Lucent 7750 Service Router (SR).

2. WLAN SERVICE DEPLOYMENT SCENARIOS

2.1 Layer 2 Wholesale Wi-Fi Service

In this initial scenario, a wireline or wireless operator with a carrier Wi-Fi service footprint can partner with retail service providers, MSOs, MNOs or MVNOs for use of their carrier Wi-Fi infrastructure, as shown in Figure 2.

Figure 2. Layer 2 Wholesale Wi-Fi Service



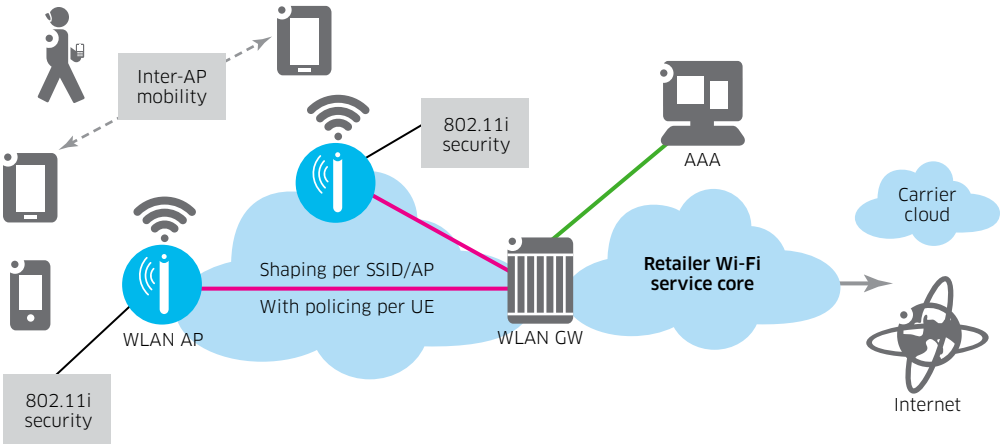
The WLAN Gateway provides a Layer 2 connection from the AP back to the retailer. All UE requests and traffic are passed back to the retailer as Layer 2 traffic. The retail service provider has the direct business relationship with end users and retains responsibility for issues such as user authentication and IP address assignment.

The WLAN Gateway can perform ingress and egress shaping on the service set identifier (SSID) based on the Service Level Agreement (SLA) with the retailer.

2.2 Retail Carrier Wi-Fi Service/Layer 3 Wholesale

A wireline or wireless operator can allow carrier Wi-Fi access through a retail SSID, as shown in Figure 3.

Figure 3. Retail Carrier Wi-Fi/Layer 3 Wholesale



In this scenario, the carrier Wi-Fi service operator has the business relationship with end users, so the retailer needs mechanisms to authenticate the end user, assign an IP address, and create a user context for accounting and billing.

The following descriptions of these mechanisms refer to retail carrier Wi-Fi service, and apply equally to the provisioning of a Layer 3 wholesale service. The difference is only in who owns the back-end authentication and accounting servers.

2.2.1 User authentication

The WLAN Gateway supports both portal-based and Extensible Authentication Protocol (EAP) user authentication mechanisms.

Portal-based authentication is the familiar mechanism found in public hotspots where, after attaching to the carrier Wi-Fi service SSID, the user opens a web browser and is redirected to an authentication page to enter user credentials.

EAP is an authentication framework frequently used in wireless networks and point-to-point connections. It requires no user intervention and instead allows for seamless authentication of UEs based on unique device identifiers. In IEEE 802.11 (Wi-Fi), the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) standards have adopted IEEE 802.1X,[1] with five EAP types as the official authentication mechanisms: EAP-TLS, EAP-SIM, EAP-AKA, LEAP, EAP-TTLS.

2.2.2 IP address assignment

The WLAN Gateway supports IP address assignment using various methods, including a local Dynamic Host Configuration Protocol (DHCP) server in the 7750 SR, DHCP relay, DHCP proxy and RADIUS.

2.2.3 UE context and policing

The WLAN Gateway creates a UE context for accounting and billing based on information obtained from the policy server during authentication. As it does in the Layer 2 wholesale

1 IEEE 802.1X: *Standard for local and metropolitan area networks — Port-Based Network Access Control*, February 5, 2010

service, it performs ingress and egress shaping per SSID and, because the UE is anchored in the WLAN Gateway, it also supports hierarchical ingress and egress policing of the UE within the shaped SSID.

2.2.4 Inter-AP mobility

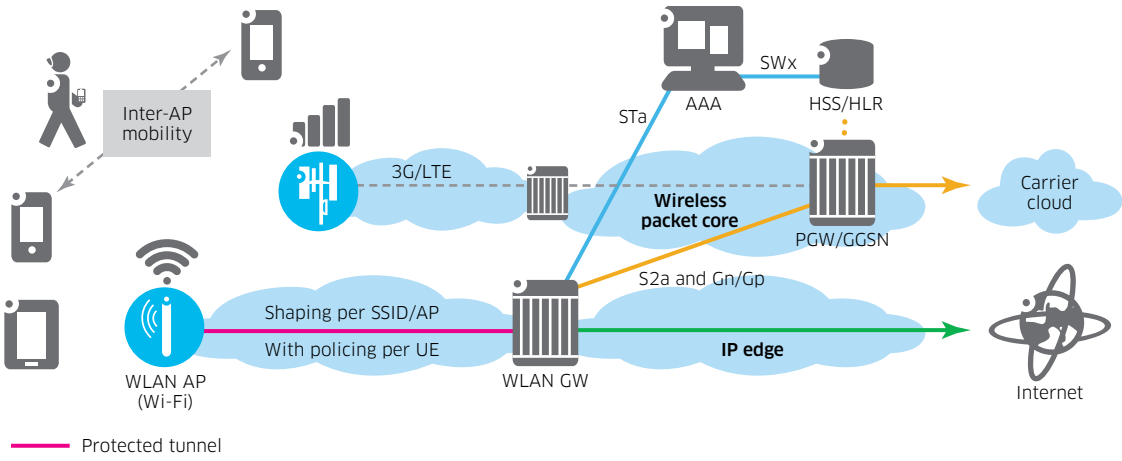
The WLAN Gateway supports Wi-Fi inter-AP mobility for a UE that moves between APs and WLAN Gateways within the carrier Wi-Fi service. When the UE traffic moves to a new AP-to-WLAN Gateway tunnel, the WLAN Gateway either seamlessly switches the UE connection if anchored on the same WLAN Gateway, or detects the UE connection if it moves between WLAN Gateways. The UE can avoid full re-authentication and re-association if the AP and UE support IEEE 802.11 Pairwise Master Key (PMK) caching or if the APs implement IEEE 802.11r[2] or IEEE 802.11i Opportunistic Key Caching (OKC).

2.3 Carrier Wi-Fi – Cellular Intermobility

Carrier Wi-Fi – Cellular Intermobility presents another retail carrier Wi-Fi service opportunity for MNOs and MVNOs. The operators can use the WLAN Gateway to ensure seamless connectivity and mobility between carrier Wi-Fi access networks and cellular infrastructure. The WLAN Gateway obtains the UE IP address from the mobile core so the WLAN Gateway can preserve the UE IP address, whether it is on carrier Wi-Fi or as the UE moves between the carrier Wi-Fi and the cellular networks.

In the scenario illustrated in Figure 4, the carrier Wi-Fi network is used as an alternative radio access network for the MNO or MVNO subscribers.

Figure 4. Carrier Wi-Fi – Cellular Intermobility



As in the retail carrier Wi-Fi service scenario above, both portal-based and EAP authentication are supported.

For each UE in the service, the WLAN Gateway creates a subscriber instance, so hierarchical policing of UE carrier Wi-Fi traffic is supported within the shaping per SSID in the AP.

Unlike the other scenarios described, in this case the WLAN Gateway auto-creates the UE subscriber context by communicating with the mobile core to retrieve the authentication and other subscriber parameters. This allows MNOs and MVNOs to maintain a familiar operating model, and to provide their subscribers with access to service experiences across the 3G/4G cellular network (for example, mobile portal, parental controls, and pre-paid charging).

2 IEEE 802.1r: *Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS)* Transition, July 15, 2008

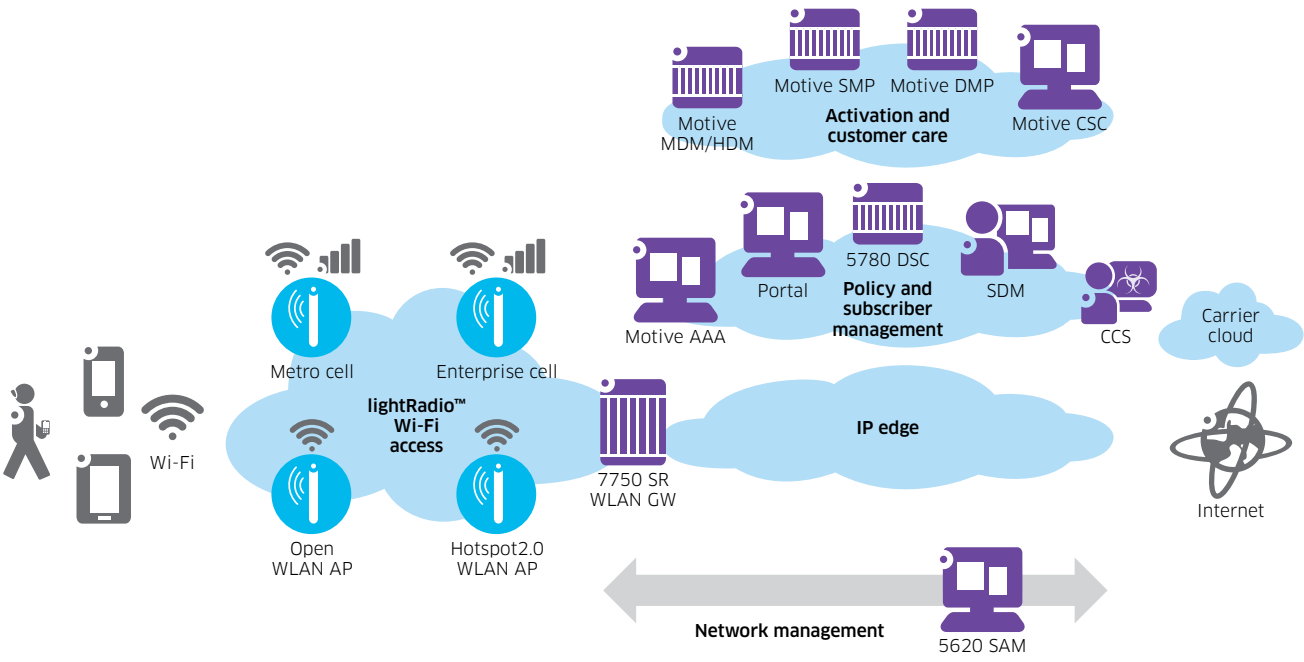
The WLAN Gateway supports the 3GPP model (SAMOG) in which the UE carrier Wi-Fi data traffic is tunneled in GPRS Tunneling Protocol (GTP) v1 or v2 back to the packet data network gateway/ gateway GPRS support node (PGW/GGSN) that serves as the anchor point for the UE. Used extensively in mobile networks, GTP headers contain useful bearer and policy information that the WLAN Gateway leverages in conjunction with IEEE 802.11e Wi-Fi Multimedia (WMM) to extend a common policy model across cellular and carrier Wi-Fi.

As an enhancement to GTP tunneling all UE traffic back to the mobile core, the WLAN Gateway also supports Selective IP Traffic Offload (SIPTO) local breakout. Policy defined UE traffic can be selected and then directly interconnected either to the required network resources that reside within the wireline network or to the Internet. The remaining UE traffic continues to be tunneled back to PGW/GGSN. In both cases, accounting can be unified at the mobile core.

3. ALCATEL-LUCENT WLAN GATEWAY FUNCTIONALITY

Alcatel-Lucent offers a comprehensive carrier Wi-Fi portfolio that addresses both wireline and wireless provider requirements. Subsets of the architecture can be deployed depending on the objectives of the carrier Wi-Fi service. The Alcatel-Lucent WLAN Gateway is a key component of the portfolio and addresses requirements to anchor multi-vendor carrier Wi-Fi access infrastructures to support a range of carrier Wi-Fi market applications.

Figure 5. Alcatel-Lucent carrier Wi-Fi portfolio



The Alcatel-Lucent WLAN Gateway is delivered on the 7750 SR platform, which is an industry leader in the next-generation edge service router product class. The 7750 SR architecture enables high-density service interfaces with low power consumption per bit transported, and provides the ability to support processing-intensive gateway services concurrently with no compromise between performance and advanced service delivery.

3.1 Traffic conditioning through aggregating and shaping Wi-Fi traffic

The WLAN Gateway aggregates Wi-Fi traffic from the multi-vendor WLAN AP infrastructures and applies Quality of Service (QoS) traffic shaping to and from the APs. The degree to which the WLAN Gateway interacts with individual subscriber traffic depends on whether the Wi-Fi service is wholesale or retail. Retail services generally have more individual subscriber traffic visibility and the WLAN Gateway creates a state for each subscriber instance. In instances where the WLAN Gateway creates a Wi-Fi subscriber context, the Alcatel-Lucent 7750 SR can hierarchically police the subscriber traffic within the AP-level traffic shaping.

3.2 Networking flexibility

Based on the Alcatel-Lucent Service Router Operating System (SR OS), the WLAN Gateway delivers the networking flexibility to anchor a range of multi-vendor carrier Wi-Fi market applications infrastructure. It has capabilities such as soft Generic Routing Encapsulation (GRE), as well as virtual LAN (VLAN) and QinQ to integrate with both existing and new multi-vendor carrier Wi-Fi market application access infrastructures. In addition, it provides the gateway to IP services networks and delivers a range of IP networking capabilities such as VPNs, MPLS, BGP and OSPF based control, IPv4 and IPv6 support, and 3GPP GPRS Tunnel Protocol to integrate into the mobile operator's packet core.

With this networking flexibility, operators are able to keep options open to accommodate a variety of business and deployment strategies. For example, a business strategy focused on cost-containment might require that user data traffic originating at a large venue — such as a stadium or perhaps in out-of-territory deployments — must not be backhauled to the retail service provider network. In a scenario such as this, the Alcatel-Lucent WLAN Gateway can locally interconnect the user traffic to the Internet or other ISP networks through its Service Router capabilities — such as peering, BGP, and carrier grade Network Address Translation (NAT) — or connect the user traffic directly to business or infrastructure virtual networks using its range of VPN capabilities.

3.3 Enhanced subscriber management mechanisms

The WLAN Gateway supports mechanisms to coordinate with the provider's back-end subscriber, policy and billing infrastructure for authentication as well as parameters to create subscriber context such as:

- Per-subscriber authentication (web authorization or EAP based)
- Advanced subscriber access management
- Service personalization through per-subscriber service context policies
- Quota management or credit control
- Carrier Wi-Fi mobility
- Lawful Intercept

The WLAN Gateway has advanced subscriber access management features that optimize resources and protect legitimate Wi-Fi network users. For example, "migrant" Wi-Fi users can automatically associate with an SSID within range, and thus consume an IP address and network resources, even though they do not intend to connect. The WLAN Gateway uses L2 aware Carrier-grade NAT, which allows the sharing of inside IP address between subscribers as well as constrained access until authentication is completed. In this way, the WLAN Gateway can handle large numbers of "migrant" Wi-Fi users without impact to authenticated active users.

The WLAN Gateway also provides a seamless network experience for the user whether the service is carrier Wi-Fi only or combined with a wireline or wireless service subscription. In the case of carrier Wi-Fi retail services, the subscriber context exists on the WLAN Gateway. Optionally, the WLAN Gateway can coordinate with a mobile provider's core infrastructure by interconnecting with a packet network gateway or a gateway GPRS support node. For a carrier Wi-Fi service, the WLAN Gateway provides mechanisms to allow for inter-AP and inter-WLAN Gateway mobility. This ensures that the carrier Wi-Fi service user may move seamlessly within the carrier Wi-Fi infrastructure or between the carrier Wi-Fi and the cellular RAN infrastructure.

3.4 High availability and OAM

Through the 7750 SR OS the WLAN Gateway delivers high availability from the perspectives of network resiliency and platform redundancy. It offers high availability within a 7750 SR platform and between 7750 SR platforms that could be collocated or geographically dispersed.

The WLAN Gateway is managed by the Alcatel-Lucent 5620 Service Aware Manager (SAM). The 5620 SAM provides integrated management capabilities for Alcatel-Lucent carrier Wi-Fi and for the underlying backhaul and transport networks. Its capabilities allow:

- Increased service deployment agility through automation
- Proactive monitoring and management across multiple network layers
- Integration into existing BSS/OSS through flexible, open APIs

3.5 Integrated advanced gateway capabilities

The Alcatel-Lucent 7750 SR can support a full range of IP service edge features simultaneously with the WLAN Gateway's integrated advanced gateway capabilities, including:

- Dual-stack IPv4 and IPv6 for both network infrastructure and high-scale subscriber support
- Lawful Intercept at high scale and high bandwidth for carrier Wi-Fi subscribers
- Policy interfaces, such as RADIUS and Diameter, to support the application of carrier Wi-Fi policies
- Carrier-grade NAT (supporting NAT44, NAT64 and Layer 2-aware NAT) for easy use of private network addresses
- Subscriber accounting and credit control methods including XML-based accounting files, RADIUS accounting and Diameter credit control for real-time charging service support
- IPsec tunnel termination and public key infrastructure (PKI) to secure AP tunnels for untrusted aggregation networks (note that the 7750 SR is also deployed as a high-scale and high-bandwidth 3GPP Security Gateway in leading mobile networks)

In addition, Application Assurance on the WLAN Gateway extends the service depth of the Alcatel-Lucent 7750 SR by enabling visibility and intelligent control for IP applications including extensive per-application, per-subscriber, or per-VPN Layer 2 and Layer 3 service policies. This allows enhanced and personalized QoS-managed application performance and provides a platform for carrier Wi-Fi monetization with service capabilities such as in-browser notification for banner advertisement, URL filtering/parental control, and stateful firewalls. These capabilities enable operators to differentiate consumer, business and mobile service offerings.

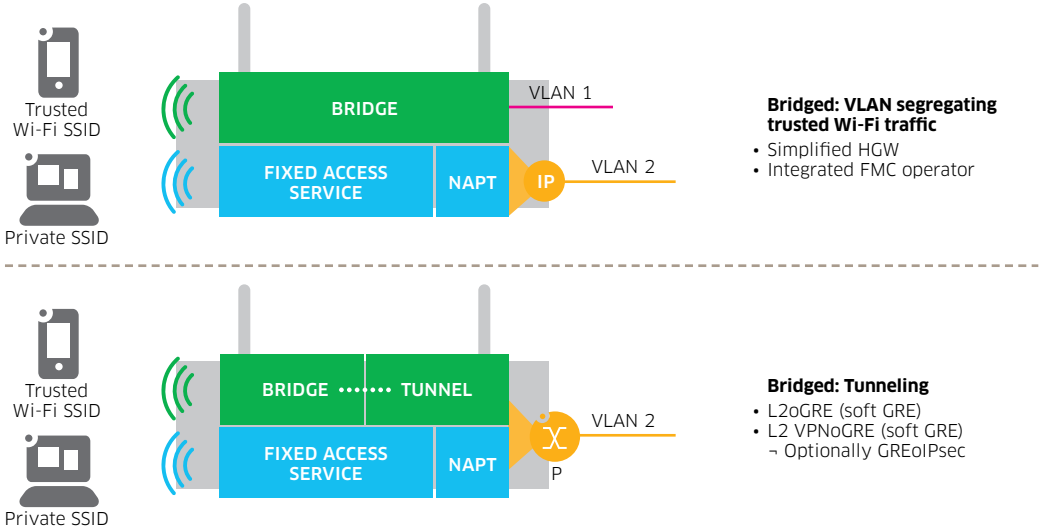
3.6 Carrier Wi-Fi access tunneling capabilities

End user devices or user equipment connect to the network via a tunnel that is established between WLAN APs and the WLAN Gateway, with the AP responsible for placing the UE sessions into the tunnel. For thin APs that use an Access Controller (AC) to control multiple APs in a WLAN zone, the tunnel is created between the AC and the WLAN Gateway.

The tunnel model imposes no new requirements on the UE, so tunneling can address the installed base of UEs. There is an AP requirement to support any tunneling mechanism chosen. So far, this discussion has referred to generic APs and UEs, however the AP can reside within a managed home gateway, and the tunneling is conceptually the same.

The tunnel model accommodates different access methods, as shown in Figure 6.

Figure 6. Alcatel-Lucent 7750 SR WLAN Gateway to AP tunneling protocols



Within each of the main tunneling approaches, there are several alternatives for encapsulation and/or encryption.

3.6.1. Encapsulation and Layer 2 bridged tunneling

Alcatel-Lucent lightRadio Wi-Fi supports a variety of encapsulation methods between the AP/home gateway (HGW) and the WLAN Gateway, as shown in Figure 6. Alcatel-Lucent believes that bridged tunneling with Layer 2 over GRE (L2oGRE) or Layer 2 virtual private network (VPN) over GRE (L2VPNoGRE) offers the most flexible solution. The use of GRE also aligns with the 3GPP standards around the integration of carrier Wi-Fi with the cellular network packet core.

3.6.2 Support for IPv4 and IPv6

An advantage to using a Layer 2 tunnel is that the tunnel is agnostic as to whether it is transporting IPv4 or IPv6. A dual-stack IPv4/IPv6 UE can be supported across the tunnel and the AP need not be IPv6-aware. In contrast, a routed tunneling mechanism requires a complete IPv4 and IPv6 dual stack in the network or the added complexity of implementing 4to6/6to4 transition mechanisms. The Alcatel-Lucent 7750 SR supports IPv4 and IPv6 and is fully capable of supporting routed tunneling, but Layer 2 tunneling is a more elegant and scalable solution.

3.6.3 Support for wholesale Layer 2 WLAN services

Layer 2 tunneling also lends itself to wholesale Layer 2 WLAN services, which routed tunneling cannot support. In the case where the AP is owned by a wholesale provider, a single tunnel from the AP to the WLAN Gateway can support multiple retailer WLAN SSIDs

that can, for example, be delimited with IEEE 802.1Q VLAN tags.[3] Efficient use of tunnels aids in the overall scale of the solution. In addition, a Layer 2 service allows the use of Layer 2-aware NAT,[4] which greatly simplifies Wi-Fi IP address management.

3.6.4 Soft GRE

The Alcatel-Lucent WLAN Gateway offers mechanisms for GRE tunnels to be automatically created when devices attach to the AP, eliminating the need for each AP to be explicitly provisioned on the WLAN Gateway. Because this "soft GRE" is stateless and the tunnel contexts are created based on need, the WLAN Gateway does not need to maintain states for unused tunnels, thus improving the solution's scalability.

3.6.5 Hop-by-hop security

There is no loss in data security because the traffic can be secured on a hop-by-hop basis. IEEE 802.11i security and encryption protocols can be used to secure traffic between the UE and the AP, and the tunnel between the AP and the WLAN Gateway can be secured with IPsec by running GRE over IPsec (GREoIPsec). Corporate VPN access is also compatible because it allows end-to-end encryption. In contrast, alternate implementations may require double IPsec encryption by the UE.

5. CONCLUSION

For operators looking to fulfill their service expansion strategies by including carrier Wi-Fi capabilities, Alcatel-Lucent offers a complete and scalable portfolio. By integrating an industry-leading set of WLAN Gateway capabilities on the field-proven Alcatel-Lucent 7750 Service Router platform, Alcatel-Lucent provides operators with a platform on which to monetize carrier Wi-Fi. The WLAN Gateway delivers the performance operators need to enhance their wholesale and retail offerings with carrier-grade Wi-Fi services and achieve the strategic advantage of simple, secure and seamless user experience.

For more information on Alcatel-Lucent carrier Wi-Fi, visit www.alcatel-lucent.com/solutions/carrier-wifi

3 IEEE 802.1Q: Standard for Local and metropolitan area networks — *Virtual Bridged Local Area Networks*, May 19, 2006
4 IETF *Layer 2-Aware NAT.* draft-miles-behave-l2nat-00, March 4, 2009

6. REFERENCES

1. 3GPP TS 23.402: *Architecture enhancements for non-3GPP accesses*. Release 11. March 2012. http://www.3gpp.org/ftp/Specs/html-info/23402.htm

2. IEEE 802.1Q: *Standard for Local and metropolitan area networks* — Virtual Bridged Local Area Networks. May 19, 2006. http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

3. IEEE 802.1r: *Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition.* July 15, 2008.

4. IEEE 802.1X: *Standard for local and metropolitan area networks — Port-Based Network Access Control.* February 5, 2010. http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

5. IEEE 802.11 (WPA2): *Wireless Local Area Networks*. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

6. IETF *Layer 2-Aware NAT*. draft-miles-behave-l2nat-00. March 4, 2009. http://tools.ietf.org/html/draft-miles-behave-l2nat-00

8. ACRONYMS

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5620 SAM	Alcatel-Lucent 5620 Service Aware Manager
5780 DSC	Alcatel-Lucent 5780 Dynamic Services Controller
7750 SR	Alcatel-Lucent 7750 Service Router
7750 SR MG	Alcatel-Lucent 7750 Service Router Mobile Gateway
8650 SDM	Alcatel-Lucent 8650 Subscriber Data Manager
8950 AAA	Alcatel-Lucent 8950 Authentication, Authorization and Accounting server
9471 WMM	Alcatel-Lucent 9471 Wireless Mobility Manager
AA	Application Assurance
AAA	Authentication, Authorization and Accounting
AC	Access Controller
AP	access point
BGP	Borger Gateway Protocol
CCS	Convergent Charging System
CDN	content delivery network
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
FMC	fixed-mobile convergence
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GREoIPsec	GRE over IPSec
GTP	GPRS Tunneling Protocol
GW	gateway
HLR	Home Location Register
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security
L2oGRE	Layer 2 over GRE
L2VPNoGRE	Layer 2 VPN over GRE
LTE	long term evolution
MNO	mobile network operator
Motive AAA	Motive Authentication, Authorization and Accounting Server
Motive CSC	Motive Customer Service Console
Motive DMP	Motive Data Management Platform
Motive MDM/HDM	Motive Mobile Device Manager/ Home Device Manager
Motive SMP	Motive Service Management Platform
MSO	multiple service operator
MVNO	mobile virtual network operator
NAPT	network address port translation
NAT	Network Address Translation
OKC	Opportunistic Key Caching
OSPF	Open Shortest Path First
PGW	packet data network gateway
PKI	public key infrastructure
PMK	Pairwise Master Key
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SaMOG	S2a Mobility based on GPRS Tunneling Protocol
SLA	Service Level Agreement
SR OS	Alcatel-Lucent Service Router Operating System
SSID	service set identifier
UE	User Equipment
VLAN	virtual local area network
VPN	virtual private network
Wi-Fi	Wireless Fidelity
WLAN	wireless local area network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
XML	Extensible Markup Language

Alcatel·Lucent