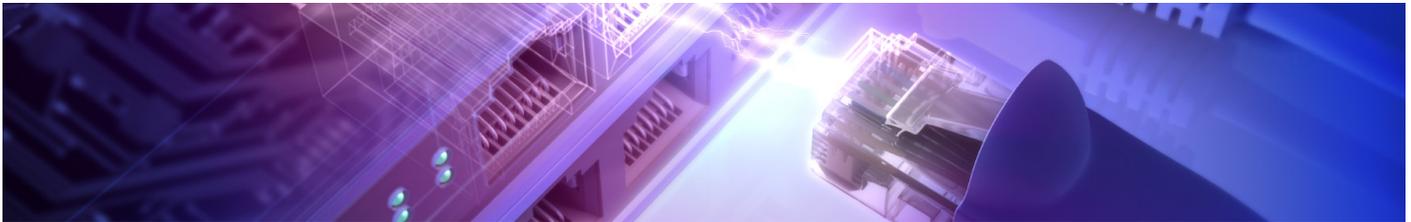


SSG + WLC = Successful Carrier WiFi deployment



INTRODUCTION

This document serves to present the case of the key benefits of using ANTLabs Service Selection Gateway (SSG) in conjunction with a wireless LAN controller (WLC) when deploying Carrier WiFi. At ANTLabs, we advocate a 3-layer architecture of policy management, subscriber management and radio frequency (RF) management.

SUBSCRIBER MANAGEMENT

The key benefits of using a dedicated gateway is the flexibility and power available to you as a service provider. In today's current environment, the ability to be able to respond to the constantly changing customer demands and fancies is not just a luxury, but a given in order to be commercially viable. New handsets and devices are launched at a pace previously unheard of in as recent times as 5 years ago. The speed of innovation in consumer devices and the operating systems that power them is only getting faster. Hence to remain relevant and to thrive in such a dynamic environment, the infrastructure that the service provider puts in place needs to be flexible to adapt to all these on-going changes.

The following are the unique ways in which the SSG is able to value add to the critical subscriber management functions over the WLC. Each will be elaborated on in more details in this white paper.

Zero Config Networking & Enhanced IP Management

- Adapt and allow all devices to connect to the network
- Prevent IP collision, IP spoofing, MAC spoofing

Multiple Authentication & Provisioning Methods

- Support varied business models for revenue generation

Dynamic bandwidth policies

- Improve quality of service and user experience
 - Encourage usage
 - Reduce unnecessary bandwidth upgrades
- Provide differentiated service level for up-sell opportunities

Flexible Usage Accounting and Billing

- Create varied WiFi plans easily

Integrated Lawful Intercept

- Pinpoint user and activity easily without consulting multiple systems
- Enable Business Analytics

Seamless Roaming

- Allow seamless roaming across multiple WLCs with minimal performance impact

Reliability

- Slow down heavy users, and not blackout service
- Anti-DOS
- Anti-SPAM

Key Benefits

1. Improve WiFi usage and end user adoption
2. Reduce Cost (less support issues and unnecessary upgrades)
3. Increase Revenue from WiFi network
4. Comply to legal requirements and gain business insights

Zero-configuration Networking and Enhanced IP Management

There's a saying in the public WiFi space: "If your users cannot connect, then you cannot collect (revenue)". This is never truer when it comes to the subscriber management, especially in the competitive visitor-based network space. This is almost foundational when it comes to building any kind of public access WiFi network, yet it is frequently overlooked by most planners, until it comes back to "bite them" in poor subscriber experience and poor service take up.

By **zero-configuration networking**, we mean that as long as the subscriber has a network setting on this device that can work at some network (be it at his home or in his office), then he should be able to connect and use the Carrier WiFi without having to make changes to his device settings. This deals with a wide gamut of network settings from his IP, gateway and DNS to his proxy settings, if used. ANTLabs' patented Tru'Connect technology delivers on this aspect of quality of experience (QoE).

IP management in the Carrier WiFi is another frequently overlooked area but critical to a successful Carrier WiFi service. Most WLCs have limited capabilities when it comes to IP management using its built-in DHCP server. This necessitates the deployment of an additional DHCP server to overcome this limitation. The SSG, on the other hand, has a robust and powerful built-in DHCP server, able to support over 2000 leases per second even with 32K DHCP IPs. Working in conjunction with its zero-configuration networking capabilities, it allows very efficient use of IPs by requiring only a single pool of IPs to support multiple VLANs. It also includes other useful features like MAC spoofing detection and the ability to dynamically change the user equipment (UE) IP from a NAT-ed IP to a routed IP.

Multiple Authentication & Provisioning Methods

Once subscribers are able to connect to the network, the next problem presents itself: identifying the subscriber in order to grant appropriate service. While the WLC can support a few commonly used authentication methods like RADIUS, 802.1x and complimentary access, it is not able to meet the varied needs of service providers in a full-fledged Carrier WiFi. This is simply because of the different deployment environments that service providers face:

- **Hospitality deployments:** requiring integration with property management system for account provisioning and authentication.
- **Exhibitions centres:** requiring credit card based provisioning, authentication and billing.
- **Transportation hubs like airports and train stations:** requiring integration with roaming aggregators and their login applications used by their subscribers

This issue is further compounded by the need to deal with the problem of account provisioning. This is most obvious in a corporate Carrier WiFi environment. Having to activate IT or MIS to create a temporary account in the WLC each time a visitor requires Internet access in the meeting rooms can almost be a full time job in itself, especially for a large MNC headquarters. ANTLabs' solution to this common issue is to simply place a few IP-based account printers at strategic locations. These account printers can then be used by the receptionist to create different account types by pushing the appropriate buttons.

Dynamic Bandwidth Policies

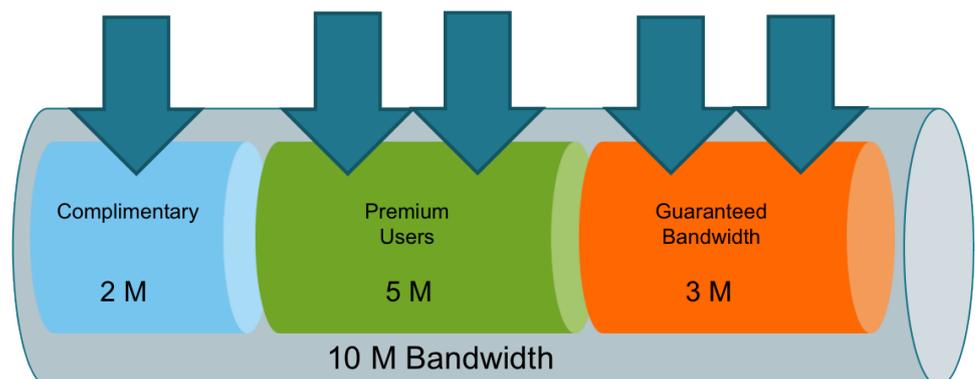
After subscribers are authenticated and we know who they are, we can then deliver different experience to them, based on their profile. This is especially important for a commercial Carrier WiFi service. It allows the service provider to maximise revenue but charging different amounts, according to the need and ability of the subscriber to pay. This creates a win-win situation as subscribers can then enjoy the QoE they have opted and paid for, while service providers are rewarded for offering differentiated services to meet different subscriber demands.

In this respect, the SSG and WLC can play highly complementary roles in order to deliver on this QoE. The WLC can focus on its key strengths of managing the limits WiFi spectrum, preventing a small group of subscribers from hogging most of the RF bandwidth. The SSG will then focus on its strength of subscriber management and manage the limited Internet bandwidth. The SSG can do this through 4 modes:

- **Per client rate limits.** This most basic mode caps the amount of bandwidth a subscriber can get at any point. However, it does not prevent a subscriber from being starved of bandwidth by other more aggressive clients.
- **Equal bandwidth among clients.** This other standard mode ensures that all subscribers will get an equal share of available bandwidth under congestion conditions.
- **Multi-tier QoS with application traffic prioritization.** This optionally available mode applies 3 tiers of priority subscribers: a guaranteed bandwidth tier, a premium tier and a complimentary tier. The guaranteed tier offers all subscribers in that tier a share of the guaranteed bandwidth. The premium tier is able to “eat into” other tiers allocation of total bandwidth if that allocation is not utilised. In addition, this tier will allocate more bandwidth to “interactive applications” (like web surfing) and latency bandwidth sensitive applications (like VoIP, video etc.). The complimentary tier is the lowest priority and is a best effort allocation of all remaining bandwidth.
- **Multi-tier QoS with per client rate limit.** This optional mode is very similar to the previous mode except that for the modified handling of premium tier subscribers: a rate limit can be applied instead of application traffic prioritization.



All Hotel Guests Exhibition Attendees Conference Attendees VIPs Hotel Staff



Flexible Usage Accounting and Billing

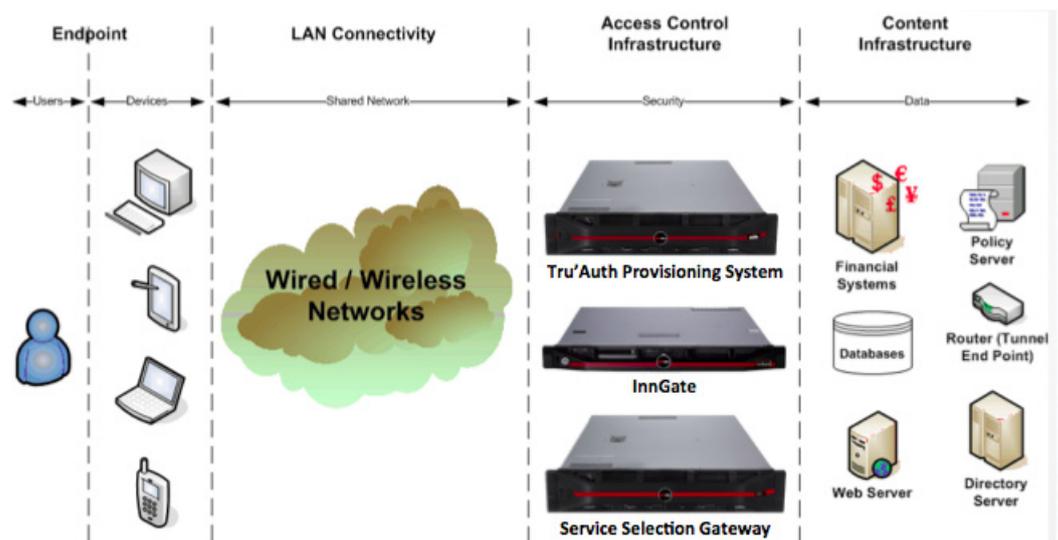
The need to support different accounting and billing modes is also critical to the success of a Carrier WiFi service. This is another area the power and flexibility of the SSG outshines the WLC. While the WLC can typically handle time-based accounting: terminate a subscribers account after a certain amount of time after initial login, more varied usage accounting methods are needed. The SSG is able to support the following accounting methods:

- **Fixed duration.** This time-based mode of accounting terminates the subscriber's access after the pre-determined duration of time has elapsed, after first login.
- **Stored duration.** This time-based mode of accounting will terminate the subscriber's access only after his cumulative login time exceeds his allocated quota. This is very much like how prepaid mobile usage is accounted.
- **Stored volume.** This mode of accounting relies on the volume of traffic generated by the subscriber. Upon hitting the traffic quota, the SSG will terminate the subscriber's access.
- **Fair-use.** This mode is a combination of both time and volume accounting methods. The subscriber has a both a time and volume quota and his account is consumed upon reaching either quota first.

Integrated Lawful Intercept

In today's security conscious environment, law enforcement agencies have placed the onus onto service providers to make sure they are able to provide required information on subscribers' usage to aid in their investigations. This tedious requirement is made much more complicated due to the way a WLC-only type network is deployment. Any request for information has to be manually correlated between the NAT firewall router's logs and RADIUS session logs and this needs to be done for all sessions of a single subscriber. This is extremely time consuming and error prone.

The SSG's Lawful Intercept module makes this troublesome task much easier and efficient, by providing a log entry for every single connection made. Each log entry will show the login user name, the UE MAC, source IP and port, destination IP and port, and NAT-ed IP and port. If the connection was a HTTP connection, the URL and browser user agent is also logged down.



SCALABILITY

As more subscribers get onto the Internet bandwagon and with each of them potentially carrying more than one device, the scalability of the chosen infrastructure for the VBNs is an important selection criterion.

Point-level Scalability

Each SSG is able to scale to support up to 20,000 concurrent subscribers, on a 2U rack space footprint. To support so many subscribers, the SSG supports 10GE interfaces for high throughput. In addition, it can support multiple WAN interfaces through its multi-WAN module for improved performance and reliability. This level of performance and scalability are typically not found in a WLC.

System-level Scalability

When your subscriber exceeds the capacity of a single (pair) of SSGs, multiple sets of SSGs can be aggregated and seamless roaming across this cluster of SSG can be achieved through session aggregation within Tru'Auth (AAA and Policy Server).

RELIABILITY

Finally all these capabilities and performance will not mean much if the overall system keeps breaking down, hence reliability features are also important. Here, the SSG also excels, to ensure maximum service uptime.

Firstly, the SSG comes with built-in defensive functions to protect itself against malicious attacks. These capabilities are again not found in a WLC.

- **Rate-limit of the number of HTTP & TCP sessions** that a single device can open to the gateway. This will ensure that no single device can open excessive TCP / HTTP sessions to the gateway and starve out other devices.
- **DNS and ARP rate-limit.** This feature prevents the gateway from being overwhelmed by bogus DNS / ARP requests.
- **SYN Flood protection.** This feature prevents a malicious user from hogging up all port resources on the SG by ignoring SYN packets that are not responded to when the SG sends a challenge to sender
- **Anti-SPAM features:**
 - **Total recipient limit.** By limiting the total number of recipient for each mail, this makes spamming more inconvenient for intentional spammers and effectively blocks of virus-initiated SPAM.
 - **Invalid sender domain blocking.** Another common practise of spammers is to fake an invalid sender domain so any bounced mail does not impact his mail server. This check again makes it that much harder for spammers to generate SPAM.
 - **Concurrent SMTP connection limit.** This limit can be set on a per user and global basis. This prevents a spammer from making multiple connections to the SG to send out SPAM.
- **Size & Recipient limit for each outgoing mail.** These configuration limits the size of each outgoing mail that can be sent out by a user. This prevents hogging of the WAN bandwidth as a result of trying to deliver a very large email attachment. It also prevents a user from sending mails to too many recipients.

- 
- **Rate limiting of email sending.** A “number of email” threshold is set on the SG. For each delivery of the same mail above this limit, the SG will add a “threshold delay” before accepting a delivery request to a new target email address. This effectively slows down rate of delivery and prevents chocking up the WAN link with email traffic.

Next, with full synchronization of configuration and subscriber sessions between active and stand-by SSGs, automated fail-over from faulty master to stand-by SSG, multi-WAN redundancy of Internet link, subscribers will be minimally affect in the event of single point failures in any part of the network.

CONCLUSION

All in all, the SSG provides a much richer subscriber experience and a quality of experience that a WLC on its own will not be able to deliver. However, when each layer of infrastructure plays its part well, from the WLC for its RF management capability, to the SSG for its subscriber management capability and finally to the policy server, the subscriber will have a truly enjoyable experience.

For more information visit www.antlabs.com.

Copyright Information

© 2013, Advanced Network Technology Laboratories Pte Ltd (ANTlabs). All rights reserved.

This document is protected by copyright. No part of this document may be reproduced in any form by any means without prior written authorization of ANTlabs and its licensors, if any. The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

TRADEMARKS

Windows and Microsoft are registered trademarks of Microsoft Corporation © All other product names mentioned herein are the trademarks of their respective owners.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENT. ANT LABS MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.