



Azaire™ Wireless Services Gateway

3GPP PDG, TTG and SeGW for Multi-Access Networks

The Azaire™ Wireless Services Gateway (WSG) is a 3GPP Packet Data Gateway (PDG), Tunnel Terminating Gateway (TTG), and Security Gateway (SeGW) as specified in the following 3GPP Release 6 Technical Specifications:

- TS 22.234 – Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking
- TS 23.234 - 3GPP system to Wireless Local Area Network (WLAN) interworking; System description
- TS 24.234 – 3GPP system to WLAN interworking; User Equipment (UE) to Network Protocols; Stage3.
- TS 29.161 - Wireless Local Area Network (WLAN) Access
- TS 29.234 - 3GPP system to WLAN interworking; Stage 3
- TS 33.234 – 3G Security; WLAN interworking security

The WSG performs the role of a mobile service provider edge gateway that works with the Azaire SCN-RAC serving as a 3GPP-compliant AAA Server to the HLR/HSS. The WSG supports a wide range of IP broadband access technologies including IWLAN, UMA and Femtocells to provide a rich blend of FMC services for the Mobile Network Operator.

COMMON PACKET DATA (APN) SERVICES

The WSG can be configured to connect to the mobile operator's GGSN using the 3GPP Gn interface (TTG mode) or directly to IP networks to provide APN based mobile data services (PDG mode).

The WSG interoperates with all major GGSNs in the market including Ericsson, Cisco, Nokia and Nortel to provide seamless access to GGSN based packet data services over broadband IP networks.

SIMULTANEOUS MULTI-SERVICE ACCESS

The WSG R5 supports simultaneous access to legacy GGSN based services in the TTG mode as well as new services directly from Wi-Fi in the PDG mode. This enables the dual-mode end subscriber to switch between GGSN based services and direct services on the same IPsec tunnel.



SERVICE AND APN SPECIFIC AUTHORIZATION

The Azaire SCN-RAC retrieves the user's subscription information from the HLR and forwards it to the WSG. This allows the WSG to validate the APN requested by the user and provide APN based services.

SECURE ACCESS

The IPsec tunnels between WLAN and the WSG provide the highest level of security over-the-air and through the public IP network. The WSG isolates the core network from unauthenticated WLAN traffic since only traffic from secure IPsec tunnels is forwarded. WSG supports both Internet Key Exchange (IKE) version 1 and version 2.

SIM-BASED AUTHENTICATION

The WSG relies on the subscribers to use a 3GPP Release 6 IWLAN compliant client/terminal. The client performs SIM or USIM based authentication (EAP-SIM or EAP-AKA) and sets up IPsec tunnels to the WSG which maps these to GPRS Tunneling Protocol (GTP). 3GPP IWLAN uses IKEv2 to facilitate secure exchange of Authentication messages between the UE Client and the 3GPP AAA server, such as the Azaire Service Control Node (SCN).



Azaire™ Wireless Services Gateway

VPN PASS THROUGH

The WSG supports APN-based GPRS VPNs through the GGSN or corporate VPN clients through the Internet.

NAT TRAVERSAL

The IPSec tunnel between the client and the WSG provides secure traversal of NAT/Firewalls thereby minimizing the need for dedicated Session Border Controller (SBC) for SIP traffic.

FIREWALL FEATURES

The WSG implements a stateful firewall to block most ports and services and plays the role of an inbound firewall to protect the un-tunneled traffic.

Additionally, the WSG is an outbound firewall which:

- Prevents traffic flood from the core network to the home zone.
- Prevents DoS attacks initiated from the Internet or any network element in the core network towards the unsecured WLAN network.

The WSG has enhanced firewall support for the following system/transport level protection mechanisms:

- IKEv2 protocol DoS protection
- IPSec setup rate limiting
- General System hardening – shut down disabled
- Allows Only Interface Specific Traffic
- Inner IP address spoof check.

POLICY MANAGEMENT & QOS

WSG R5 supports the following Policy and QoS features to enable operators to offer the flexibility to manage network bandwidth based on application level flows from the subscriber:

- Policy Management support through Access Control Lists (ACLs)
- Flow classification with DSCP Marking
- Bandwidth policing per user
- Queuing and scheduling based on HTB & SFQ
- Congestion avoidance using RED
- Shallow Packet Inspection and Traffic Shaping
- Identify flows and apply flow specific policies

The WSG applies QoS by copying the ToS or Diffserv codepoint from the IP headers of the data traffic to the outer IP header after IPSec encapsulation.

CARRIER-CLASS MANAGEABILITY & DEPLOYABILITY

The WSG provides numerous features for operators to ease the deployability and manageability of the entire solution.

PER SUBSCRIBER STATISTICS

In addition to providing per ATCA blade statistics, the WSG supports retrieval of statistics per subscriber to enable operators to conduct audit trails and to settle billing disputes.

HIGH AVAILABILITY (HA) FEATURES

The WSG is a high availability system designed for reliability. Every subsystem is hot swappable with either active and standby subsystems or load balanced subsystems. Any single failure does not lead to loss in capacity or performance:

- Dual redundant Management, Load Balancing & Switch Fabric blades
- Hot swappable Application blades can be configured in dual redundant 1:1 mode
- Dual feed power input into redundant Power Entry Modules (PEMS)
- Redundant fans

SCALABLE PERFORMANCE & LOAD BALANCING

The WSG is a scalable system based on the industry standard ATCA platform. The WSG (Release 5) supports up to 300,000 concurrent subscriber IPSec/IKEv2 tunnels (with future software upgrades to support 400,000) and an aggregate throughput of 650 Megabits per-second on a fully loaded 1+1 redundant ATCA platform. The WSG software is licensed according to the maximum number of concurrent subscribers supported. Options are available to fully populate the WSG chassis with up to 8 Application blades configured in 1:1 redundant mode.

The ATCA technology ensures future upgrades to higher performance blades and hardware-acceleration daughter cards. The blade models within the WSG are:

- Non-HA Configuration - 1 Management blade, 1 Load Balancing blade and 1 Application blade,
- HA Configuration - Dual redundant Management, Load Balancing blades & Application blades configured in 1:1 mode



Azaire™ Wireless Services Gateway

ACCOUNTING RECORDS

The WSG forwards accounting information to the Azaire SCN. The WSG supports the option of providing interim accounting records to the SCN. This feature enables the SCN to send the Intermediate CDRs to the CGF. Interim CDRs are useful for fraud prevention, reconciliation and in case the final CDR is lost or corrupted. The SCN uses this information to generate accounting records in different formats including RADIUS accounting records, S-CDR, G-CDR, and W-CDR.

The accounting records include Radio Access Technology (RAT) type to allow differentiated billing for different access technologies without allocating additional APNs.

RAPID INTEGRATION WITH EXISTING OSS

Since most network interfaces are internal to the WSG, the Mobile Operator can manage the entire chassis as a single entity. The WSG multi-protocol SNMP agent (V1, V2 or V3) is designed for rapid integration into the carrier's existing Operations Support Systems (OSS). This agent can be used by any SNMP based Network Management System (NMS) to provide complete Fault, Configuration, and Performance management. The IntelliNet SCN-OMC can be deployed as a standalone Element Management System (EMS), or integrated with the major NMS platforms such as HP OpenView.



email: sales@intellinet-tech.com

Corporate Headquarters

1990 W. New Haven Ave.
Suite 303
Melbourne, FL 32904 USA
Tel: + 1 321 726 0686
Fax: + 1 321 726 0683

Development Centers

413/4 Oxford Towers
139 Airport Road
Bangalore - 560017 India
-
40 Shuman Blvd., Suite 256
Naperville, IL 60563 USA

Copyright © 2009 IntelliNet Technologies, Inc., all rights reserved. IntelliNet Technologies, IntelliSS7, Accelero, Convero, Azaire, Azaire Networks, the Azaire Networks logo, MobiFlex and IP-CNP are registered trademarks of IntelliNet Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. Specifications are subject to change without notice.



www.intellinet-tech.com