IntelliNet’s Converged Data Offload Gateway delivers an innovative architecture that supports multiple data offload solutions on a single platform. Since most data offload implementations leverage easily and cheaply accessible public IP networks for backhaul, the primary function of this gateway is to enable simple, seamless, highly secure access to subscribers as they roam between trusted mobile networks and untrusted public networks. The Gateway is wireless interface agnostic supporting the two most popular access methods – femtocell as well as Wi-Fi. More importantly, as the network operators migrate to next generation LTE networks, the Gateway takes on the role of the e-PDG while maintaining backward compatibility with 2G/3G networks. This allows operators to seamlessly upgrade their networks. An important feature of the solution is that it is completely standards based.

The Wi-Fi Offload Gateway is a carrier-grade platform which can support both standards based and innovative approaches to interworking with cellular networks. The product builds routing intelligence on traffic from a Wi-Fi path based on operator provided policy. The traffic can be extended either to the cellular core network or to the internet. Since the operator’s core network requires a trusted device access, the gateway also enables authentication to the core network and secure transport access.

Interworking WLAN for Data Offload 3GPP standards introduced the specifications for interworking WLAN with cellular networks. These standards continue the progression to enabling WLAN connectivity to the evolved packet core for LTE-4G networks. The standards-based infrastructure makes a compelling case to support the infrastructure for the data offload path. Unlike UMA, IWLAN was carefully designed to support rich data services such as streaming audio and video over the unlicensed spectrum. The fundamental bridge that IWLAN provides is to build a trusted relation between a non-cellular entity with the core network. This is critical since the Wi-Fi path is not secure.

Operators can either leverage Wi-Fi to their advantage or make it a liability for network bypass Mobile Data Offload for 3G Networks IWLAN utilizes the SIM based identity of the user device to provide a common authentication scheme as deployed in a GSM/UMTS network. Having authenticated the user, the next step is to setup a secure transport on which signaling and traffic can be encrypted.

IWLAN is therefore able to provide two modes of interworking. Using a Tunnel Terminating Gateway (TTG), it can expose operator hosted services typically behind a GGSN and accessible through an APN. The TTG terminates the Wi-Fi transport tunnel and extends it to GGSN connectivity. In the second mode, utilizing a Packet Data Gateway (PDG), it can provide an access to the packet data network or the internet services itself. The advantage is that this mode can offload GGSN traffic as well. Both modes are capable of applying service based local policy for enforcing QoS. By utilizing underlying IP-mobility based methods, it can provide seamless handoff between the cellular and Wi-Fi networks.
Wi-Fi Offload Gateway

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

SIM-BASED AUTHENTICATION
The Wi-Fi Offload Gateway 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 Gateway which maps these to GPRS Tunneling Protocol (GTP). 3GPP IW-LAN uses IKEv2 to facilitate secure exchange of Authentication messages between the UE Client and the 3GPP AAA server.

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

FIREWALL FEATURES
The Wi-Fi Offload Gateway implements a stateful firewall to block most ports and services and plays the role of an inbound firewall to protect the un-tunnled traffic. Additionally, the Gateway 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 Wi-Fi Offload Gateway 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
The Wi-Fi Offload Gateway 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 Wi-Fi Offload Gateway applies QoS by copying the ToS or Diffserv code-point from the IP headers of the data traffic to the outer IP header after IPsec encapsulation.

CARRIER-CLASS MANAGEABILITY & DEPLOYABILITY
The Offload Gateway 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 Wi-Fi Offload Gateway supports retrieval of statistics per subscriber to enable operators to conduct audit trails and to settle billing disputes.

HIGH AVAILABILITY (HA) FEATURES
The Wi-Fi Offload Gateway 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

www.intellinet-tech.com
Wi-Fi Offload Gateway

SCALABLE PERFORMANCE & LOAD BALANCING

The Wi-Fi Offload Gateway is a scalable system based on the industry standard ATCA platform. It 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 Wi-Fi Offload Gateway software is licensed according to the maximum number of concurrent subscribers supported. Options are available to fully populate the Offload Gateway 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 Offload Gateway 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

RAPID INTEGRATION WITH EXISTING OSS

Since most network interfaces are internal to the Wi-Fi Offload Gateway, the Mobile Operator can manage the entire chassis as a single entity. The Gateway's 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.