3GPP I-WLAN

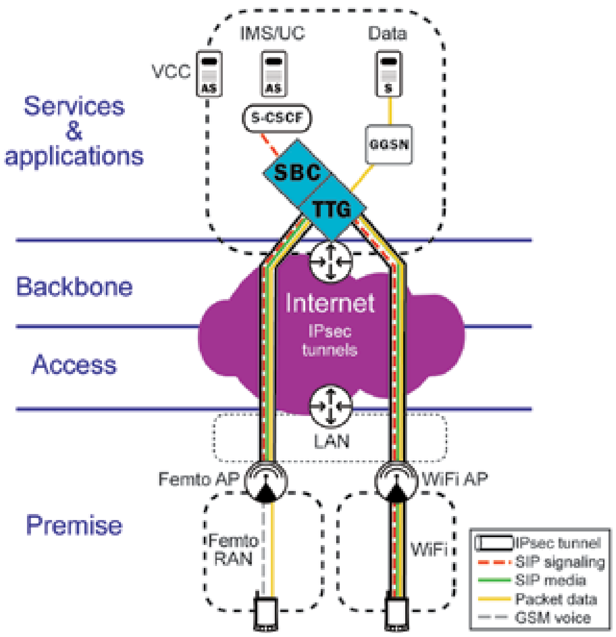
solutions note

3GPP I-WLAN

Mobile operators are turning to multiple fixed-mobile convergence (FMC) approaches to increase revenue opportunities and customer loyalty. One approach to FMC involves the 3GPP Interworking-Wireless LAN (I-WLAN) architecture to improve radio coverage and reduce backhaul costs. This architecture uses IPsec tunnels to deliver SIP-based services and packet data services over untrusted WiFi access networks with backhaul over the Internet or a managed network. Optionally, these services can be delivered via a femtocell to existing GSM/GERAN endpoints with the femtocell providing GSM-SIP signaling interworking.

Solution

Deployed at the access border of the SIP or IMS service network, Acme Packet's Net-Net® MSG and SBC are designed to satisfy all the critical requirements for delivering voice and data services securely over the untrusted Internet and WiFi access networks. They may be deployed as two separate products or as one integrated product.



Net-Net MSG I-WLAN

Acme Packet's Net-Net MSG functions as an 3GPP I-WLAN Tunnel Terminating Gateway (TTG) and is responsible for controlling IPsec tunnels used to transport SIP interactive communications and packet data services to the endpoint or femtocell.

Security – Acme Packet's Net-SAFE® function secures SIP interactive communications and packet data services.

- Access control
  - Authenticate endpoints via 3GPP Wm interface to AAA servers
  - Permit or deny access to anonymous users
- Confidentiality & privacy
  - Support IPsec tunnel mode encryption/decryption of SIP interactive communications and packet data services over untrusted access network to ensure confidentiality, prevent identity theft and mitigate service theft
- TTG DoS/DDoS protection
  - Protect TTG from DoS/DDoS attack and other malicious attacks - IPsec, L3 / L4
  - Protect TTG from non-malicious overloads
  - Allow trusted/authenticated users access while under DoS attack or overload
  - Dynamically accept or reject traffic based on device behavior

Applications

Using I-WLAN, GSM mobile operators and MVNOs can further facilitate fixed-mobile substitution by delivering voice and packet data services into areas with poor radio coverage using two different types of access points:

- WiFi access points supporting dual mode SIP/WiFi and GSM/GERAN (GSM EDGE Radio Access Network) endpoints
  - SIP-based services - voice, video and interactive communications
  - Packet data services
- Femtocell access points supporting existing GSM/GERAN endpoints
  - Circuit-switched voice services
  - Packet data services

- Monitoring and reporting
  - Monitor and report on alarms for attacks and overloads
  - Audit trails for attack response & fraud investigation
  - Provide secure monitoring & management access to protect from unauthorized personnel

Service reach maximization – Acme Packet Net-Net MSG provides NAT traversal and virtualization to extend subscriber reach and types of services supported

- NAT traversal
  - Enable services to traverse premise-based NAT devices by using UDP encapsulation
- Virtualization
  - Support multiple logical MSGs in single physical system for separation of services - I-WLAN and UMA, residential and enterprise, retail and wholesale, or multiple mobile virtual network operator (MVNO) customers

Net-Net SBC

Acme Packet's Net-Net SBC is responsible for controlling SIP sessions between the SIP service core and the SIP endpoint or femtocell. It provides critical control in five functional areas:

Security – Acme Packet's Net-SAFE® security function mitigates all SIP service security threats

- SBC DoS/DDoS protection
  - Protect SBC from DoS/DDoS attack and other malicious attacks - SIP signaling, SIP media, L3 / L4
  - Protect SBC from non-malicious overloads
  - Allow trusted/authenticated users access while under DoS attack or overload
  - Dynamically accept or reject traffic based on device behavior
- Access control
  - Permit access to from authorized/registered users; permit or deny access to anonymous users
  - Dynamically accept or reject traffic based on device behavior
  - Accept media only for authorized sessions
- Topology hiding
  - Hide core service network topology to prevent directed attacks
- Virus, worm & SPIT protection
  - Protect network from malicious attachments, prevent malformed messages from overloading resources
  - Restrict usage to prevent automated dialing/ unwanted sessions
- Service infrastructure DoS prevention
  - Prevent DoS/DDoS attacks from reaching core service infrastructure
  - Protect core from signaling overload attacks by enforcing call rate limiting, message rate limiting and code gapping policies
- Fraud prevention
  - Perform signaling and media validation by authenticating and authorizing users
  - Enforce service contract per-user/device and prevent piggy-back usage
- Monitoring and reporting
  - Monitor and report on alarms for attacks and overloads
  - Audit trails for attack response & fraud investigation
  - Provide secure monitoring & management access to protect from unauthorized personnel

Service reach maximization - Acme Packet Net-Net SBCs provides numerous address and protocol translation capabilities to maximize the types of endpoints, service infrastructure and network topologies supported

- IP address and telephone number translation/manipulation
  - Bridge IP address spaces - private-public, private-private, IPv4-IPv6
  - Perform prefix, suffix, and other telephone number manipulations
- SIP protocol translations and fix-ups
  - Provide SIP protocol normalization and repair
  - Interwork SIP transport protocols - UDP, TCP, SCTP
  - Translate SIP response codes between SIP service core and access network

SLA assurance – Acme Packet's Net-Net SBCs provide features to assure service quality and service availability during abnormal busy periods or network events

- Session admission control
  - Admit sessions based upon signaling & bandwidth constraints per user, network or SIP session agent to ensure resource availability
  - Interface to external policy servers and bandwidth managers
- Overload protection & control
  - Load balance SIP signaling traffic based on number of sessions or rate of sessions
  - Reject or divert traffic based upon destination number to control mass calling events
- Failure detection, traffic re-route and recovery
  - Monitor performance and availability of L3 router, SIP registrar, SIP session agent
  - Re-route or re-distribute traffic based upon performance degradation or failure
  - Manage avalanche SIP registration events resulting from power outages or registrar failures by statefully managing endpoint re-registration process and load
- Transport control
  - Assign QoS marking/VLAN mapping based on application, source address or destination address

Revenue & profit protection – Acme Packet Net-Net SBCs ensure service infrastructure resources are used efficiently

- Accounting
  - Generate CDRs for billing or network planning
- Service theft protection
  - Police media bandwidth per session based upon authorized codec
  - Terminate inactive session with session timers to free-up network and system resources
  - Ensure only authorized sessions receive correct QoS and resource allocation

Regulatory compliance - Acme Packet Net-Net SBCs provide functions required to comply with government regulations for IP interactive communications

- Emergency session handling
  - Prioritize, retrieve location information and route emergency/ E911 sessions
  - Interface to external location servers (CLF)
- Lawful intercept
  - Replicate & deliver signaling (call data) and media (call content) for lawful intercept

acme packet

71 Third Avenue
Burlington, MA 01803 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com

3/13/08