The Future Role of Media Gateways in All-IP Networks

A GENBAND Whitepaper
September 2008

By Glenn LeBrun, Sr. Director - Product Marketing
Andrew Bender, Sr. Director - Technical and Solutions Marketing

Introduction

Evolving Trends in Fixed and Mobile Networks

Contemporary communications networks are undergoing rapid changes. Networks that were circuit-based and voice-centric a decade ago have been optimized to carry packet-based voice, data, and video traffic. The key trends in all of these contemporary networks are: a) they are growing - in complexity, subscriber count, and bandwidth per user, b) they all provide services that rely upon being interconnected with each other, and c) they have a common long-term direction to converge on all-IP architectures.

These trends have ramifications for each of the network types that are operated by communications network operators. The various networks generally break-down into five main categories -- 1) fixed voice networks, 2) fixed data and video networks, 3) mobile voice networks, 4) mobile data and video networks, and 5) Fixed Mobile Convergence (FMC) networks. Each network type is examined below.

<u>Fixed Voice Networks</u>

Despite the accelerating growth of mobile networks and the increasing fixed line substitution by mobile, line counts in fixed voice networks have shown modest increases over the last five years, rising 18% over this period to a total of 1.3 billion lines at the end of 2007[1].

Fixed Core Network: The packetization of core voice traffic via Voice over IP (VoIP) was first implemented by some operators in private, controlled backbone networks. Use of VoIP yielded long-distance transport efficiencies and capitalized on new, affordable high capacity packet networks built to support the growth of the Internet. Now even more comfortable with the redundancy and resiliency of their IP networks, an increasing number of operators are migrating the traffic in their core fixed line voice networks to VoIP.

Fixed Access Network: Though most of the access lines in fixed voice networks continue to be served by conventional circuit-switched technology, a growing percentage of new lines are implemented using Voice over IP (VoIP). VoIP is being driven by the deployment of fiber-centric access technologies that enable Television, Video on Demand, and High Speed Internet, like Gigabit Passive Optical Networks (GPON), DSL-based Fiber-to-the-Node, and Cable Hybrid Fiber Coax.

As these access networks transition to VoIP, they are connecting into IP core networks, where the traffic is often transported as VoIP elsewhere in the network. As a result, a greater proportion of the traffic carried in fixed voice networks is becoming IP end-to-end. To further optimize their networks and reduce costs, some operators are pursuing native IP interconnection with other peer networks, rather than going through multiple TDM conversions as an intermediate, handoff methodology .

This continued growth of VoIP in both fixed line access and core networks is evidenced by the large total addressable market (TAM) identified for VoIP-based media gateways, softswitches, session border controllers, and other VoIP components, with forecasts exceeding $7 Billion annually by 2010[2].

---

[1] ITU World Telecommunication/ICT Indicators Database, July 2008
[2] Infonetics, 2008

Fixed Data/Video Networks

Consumer broadband lines have grown to over 400 million in 2008, with expectations to exceed 600 million by 2012[3]. At the time many of the networks that provide consumer broadband service were constructed, their primary value was to enable basic Internet access and related applications like web browsing or email. Internet-enabled applications have since expanded to include streaming media, file sharing, and interactive video, along with a steady stream of new "over the top" applications. All of these new uses of the Internet are creating new technical, interconnection, and interworking demands on the network.

Fixed broadband line growth is driven directly by demand for these new Internet applications, and increasingly by telco-oriented IP video services like IPTV. Many residential broadband networks are being implemented today with service tiers in excess of 30 Mbps, and have total capacity of up to 100 Mbps to the customer premises, to accommodate the growing demand for multimedia services.

The emergence of new traffic and content types, sophisticated policies to maintain Quality of Service (QoS) for multiple parallel (and competing) applications, and continually increasing call and session volumes are creating an expanding need for new network element capabilities to manage the traffic between content providers, users, and their networks.

Mobile Voice Networks

Mobile voice services are growing at a much faster rate than their fixed line equivalents; this is due in part to the rapid adoption in emerging markets. The use of mobile phones has skyrocketed, with over three billion users today and more than five billion forecasted by 2011[4]. Mobile subscribers now outnumber fixed line subscribers by more than 3 to1 on a global basis, with similar proportions in mature, saturated markets as well as emerging ones.[5]

In response to this growth, operators must continue to invest to expand mobile voice networks; at the same time, mobile saturation is approaching -- with continual price competition due to multiple operators in each market, making less revenue available per unit of service. This inevitable commoditization of basic mobile service results in two major competitive responses for operators - 1) reduce total costs per subscriber by migrating services to a common IP basis, and 2) increase average revenue per user (ARPU) through new services such as mobile data services and related applications.

Mobile Data/Video Networks

A vast majority of the mobile subscriber base is served by second generation (2G) GSM mobile networks with intrinsically limited data capacity, where voice and Short Message Service (SMS) are the only widely available applications.

Though voice usage remains the primary source of revenue for mobile operators, data services are beginning to contribute an increasing proportion of overall revenue, with up to 20% of total mobile carrier revenues now derived from data.[6] Even in emerging markets, potential subscriber demand for data and information services has been demonstrated by

---

[3] Strategy Analytics, 2008
[4] Infonetics, 2008
[5] ITU, 2008
[6] Giga Omni Media, 2008

the success of Short Message Service (SMS) with an amazing 2.3 trillion messages sent in 2008[7].

The subscriber appetite for enhanced mobile data services has been created by the success and growth of Internet applications, originally supported by the rise of fixed broadband networks. Email and web browsing have become pervasive Internet applications, and were the first to migrate to mobile devices. However, the adoption of these services was initially limited by the constraints of basic 2G mobile data services like GPRS and 1xRTT which are not capable of "broadband" speeds (greater than 256kbps).

Third-generation (3G) mobile data networks and other and high-speed wireless options like WiFi and WiMax are now being actively deployed to address the bandwidth requirements of mobile Internet applications. While this is occurring, the demands of Internet applications are also changing, as new applications like streaming media and file sharing have overtaken basic web browsing and email in the overall balance on Internet traffic.[8]

Operators have provided decisive evidence that subscribers with a combination of a sophisticated Internet-capable mobile device and adequate high speed data network support will generate significant sustainable increases in utilization. Increases of more than 30 times for this subscriber class have been reported.[9]

Market research also indicates that significant demand exists for mobile video, with about 500 million mobile subscribers expected to be regular viewers of streaming or broadcast videos on mobile handsets by 2010[10]. Although 3G high-speed networks have captured less than 10% of the global subscriber base thus far, the dynamics of new applications are already driving the industry to consider the transition to Long Term Evolution (LTE). LTE networks offer yet higher data bandwidth potential and an all-IP architecture optimized for data applications.

The presence of Internet applications, and the open mobile device platforms that support them, are a significant departure from the trusted, "walled garden" architectures that were originally used to build mobile core networks. These changes present new security risks and traffic management challenges for mobile operators that are compounded as network speeds increase.

Femtocells and WiFi

Fixed Mobile Convergence (FMC) services have gained popularity with mobile operators as an inexpensive and practical way to extend the indoor coverage of existing wireless networks and increase total subscriber capacity. However, the most compelling reason for FMC deployment may be the prospect for using the mobile core network to extend high speed data access into the home or business in support of new high-bandwidth Internet applications.

Because mobile phones are increasingly used as a "main line" in the home or business, up to 40% of all voice calls are made in these locations. However, due to inadequate mobile coverage in residential and suburban locations or structural interference in buildings or homes, service performance and voice quality often suffers. In order to provide complete coverage in these locations, two types of FMC offerings are being pursued by mobile

---

7 Gartner, 2008
8 Giga Omni Media, 2008
9 Unstrung, 2008
10 ABI, 2008

carriers -- those that use licensed spectrum controlled by the operators via a Femtocell, and unlicensed wireless data networks comprised of WiFi “hotspots”.

Femtocell networks include a small, in-home base station that consumers connect to their home broadband network. These devices provide mobile voice and data network access inside the building where they are installed. The femtocell uses a customer’s fixed broadband access to send mobile voice, data, and signaling traffic in licensed frequency bands back to the mobile operator’s core network in a security-encrypted tunnel.

WiFi networks can be used by dual mode phones with radio systems that interface to both existing mobile macrocell networks, as well as unlicensed WiFi networks that provide Internet access. WiFi-based FMC solutions rely on an encrypted tunnel that originates from the subscriber’s terminal to send the mobile voice and data traffic back to the mobile operator’s core network, when the device is connected to a WiFi network.

Data performance in the macrocell network is determined by signal quality and active user density. The distance of subscriber devices from the base station, losses from building penetration, and interference from other subscribers all affect the signal quality. Active users sharing a given sector or cell must compete for channel capacity at the base station and potentially in the backhaul network as well.

Modern air interface standards make use of advanced modulation techniques that continue to improve the amount of radio spectrum required per unit of link bandwidth, the maximum transfer speeds available, and the range at which a given speed can be achieved. However, as the macrocell networks gain higher capacities for data speeds, these improvements are more than counteracted by the congestion generated by additional subscribers and new multimedia applications.

Both Femtocell and WiFi FMC approaches offer a significant increase in data bandwidth available per subscriber by limiting the number of active users that share radio channel capacity, and by offering a dedicated base station at short range with maximum link performance. Forecasts for Femtocell and WiFi FMC offerings predict an extremely rapid growth in users, from a few million today to over 150 million by 2012[11].

Commonalities and Issues in Evolving Networks

As the value of information, communications, and entertainment grows, so do the transport networks. Yet as networks have grown over the years -- and as demand for information has increased -- networks have had to become much more efficient with regard to costs and technologies.

In the recent past, fixed and mobile networks were exclusively based in circuit technology. The service provider controlled all traffic within a secure walled garden and had complete control over the networks upon which the traffic traveled. Voice traffic generally took a path from location A to location B over intermachine trunks, which are the voice trunks between telephone exchange switches. Signaling traffic often took a different path to ensure, for instance, that a call was not needlessly connected to a location when the called phone was already in use, or to look up a terminating phone number from an 800 database.

---

[11] ABI Research, 2008

Though early telecommunications networks were based in analog technologies, this began to change with the rise of the digital age in the 1970's. In the latter part of the digital age, methods of transport were being refined such that fixed and mobile networks were capable of handling higher data speeds. Emerging from the latter part of the digital age were the early packet technologies like frame relay and ATM. The most current packet technology, and the one that has been globally-accepted for all future networks, is IP. IP is very efficient, cost-effective, and can accommodate nearly all types of communications traffic and higher-level applications and services, so it is the natural transport protocol as speeds and services continue to increase.

IP networks are the most current technology, but they must still maintain some of the key attributes of earlier circuit technologies:

- IP networks must maintain security to ensure that service is not stolen and that information is not compromised or otherwise disrupted.
- IP networks must be managed so that their transactions, phone calls, or "sessions" -- the connecting of one location with another or multiple others -- have a defined level of continuity, reliability, and quality.
- Networks must also have policy enforcement ensure that operating rules are followed and are in conformance with service contracts. This applies to all services -- from those as simple as plain old telephone voice service (POTS) to very complex services like advanced data applications or video conferencing.

Integrating VoIP Networks. Since older circuit networks are now giving way to more efficient IP-based networks, a common problem has arisen: "How do we connect these new IP networks to the older circuit networks - and still maintain the session management, policy enforcement, and security that we had in those networks?" In the last decade, telecom manufacturers, academia and standards bodies have devised various methods to provide solutions to this problem. As shown in the Figure 1 below, voice networks of today are primarily comprised of islands of VoIP surrounded by oceans of circuit voice networks. In addition to many other functions, media gateways serve to mediate the traffic between the two disparate networks, ensuring that circuit voice traffic -- including both the signaling and voice (or "bearer") traffic is converted between VoIP and circuit (or TDM).

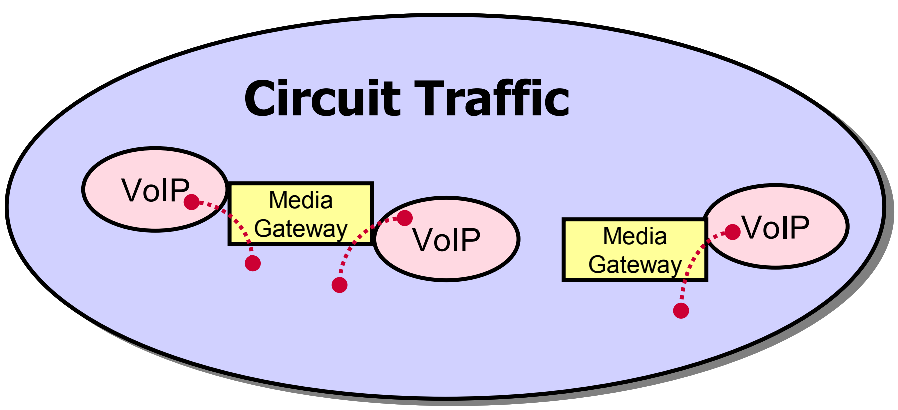

Figure 1. Current voice networks.

Similarly, softswitches are used to manage the control and feature aspects of these voice sessions. As this technology evolves to the generally agreed upon standard of IP Multimedia Subsystem (IMS), the softswitch is disaggregated into other signaling and control components, though media gateway functions generally remain intact.

Networks are changing, however, as the cycles of change become more compressed with rapid improvements in technology. In contrast to islands of VoIP surrounded by oceans of circuit networks, an evolution is occurring to islands of circuit-switched voice surrounded by oceans of diverse IP networks that are carrying multimedia sessions such as voice, data, and video applications. Though media gateways and softswitches or IMS cores will continue to manage voice transactions between the circuit and VoIP networks for a long time to come, there is also a growing need to manage transactions at the borders between these various IP networks.

IP-to-IP transactions occur at three primary borders. One border exists in the network core, where operator networks typically connect to other service provider networks. The second exists between operator networks and end customer networks. The third is between the operator and application providers that deliver content through the network to their subscribers.

Unlike legacy circuit networks where traffic flow was structured and homogeneous, IP traffic is inherently heterogeneous with a diverse set of protocols and network configurations that require complex interworkings and policy control over IP sessions. IP is not tied to any specific network facility, so traffic needs to be intelligently routed and managed, and IP is also very open, exposing network borders to the security risks inherent in the Internet.

When these diverse IP networks meet at network borders, extensive interworking, protocol repair, and normalization is required to ensure smooth session flow. In addition, a complex set of security risks must be managed to prevent service theft, ensure session integrity, protect policies and SLAs, and provide network predictability and session confidentiality.

Emerging Session Management and Policy Enforcement Needs in IP-Based Networks. In contrast to circuit networks, IP networks create increasing levels of complexity. Where circuit networks had over 100 years of standardization, IP networks have until recently not had the benefit of standardization. This means that -- even though all traffic takes the form of IP -- there are many variations on how the traffic is handled within an IP packet.

For example, certain protocols are used to manage voice and multimedia sessions. Older protocols like H.323 are in common use in IP PBX systems worldwide, but the new SIP-based protocols used in service provider networks are incapable of communicating with these systems directly. Even SIP, as new as it is, has many variants that require some type of mediation so that two SIP sessions may talk to each other.

Another example is policy enforcement. If a multimedia session like video gaming is requesting a particular bandwidth or network priority level, policy enforcement will ensure that the network does not violate its own policies for managing other sessions. In contrast to circuit networks, where pre-designated policies typically manage bandwidth constraints on the physical facility (e.g., PRI), more flexible IP network policy enforcement allows packets with differing policies to ride simultaneously through the network or "cloud".

Emerging Security Needs in IP-Based Networks. Just like circuit network communications, IP-to-IP communications require some level of session management and policy enforcement, but security is particularly important due to the open nature of IP. Circuit networks were inherently secure, since both the signaling and content traffic were under tight control. IP networks, on the other hand, may be vulnerable to Internet-like attacks, including denial of service attacks, viruses and worms, theft of service, and other risks that threaten to significantly compromise network integrity.

Security risks are substantially minimized where networks are mostly small islands of VoIP surrounded by large islands of circuit switched traffic, since all traffic is either circuit-to-circuit or circuit-to-IP, and the media gateway sits on the border between the very secure TDM network and the relatively insecure IP network. The media gateway is not a typical attack point, nor is it particularly vulnerable to attacks.

However, as the transition continues to smaller islands of circuit voice surrounded by oceans of IP multimedia traffic, security problems grow. Both the signaling (or control) traffic and the media (voice, data, video) are susceptible to attacks.

Though malicious attacks often occur, not all attacks are intentional. For instance, a single IP phone could become "sick" and inadvertently bombard the network controllers with a steady stream of registrations or call attempts, causing a network tie-up and preventing valid callers or sessions from getting through. Security issues like this can occur whether the sessions are voice, data, or video.

Risk Locations in the Network. With any network, as speeds and interface options increase, so do the risks. For example, content typically comes from somewhere other than the service provider's network -- generally the open Internet. Viruses, worms, and other security risks can occur at the interface between the operator and the Internet content providers -- commonly known as the "Network-to-Network Interface" or NNI. If these risk elements pass from the Internet - or other IP networks -- into the operator's IP-based network core, substantial harm could come to the network itself or to the voice, data, or video traffic carried within it.

Similarly, content is increasingly being created by end users for consumption at other locations like the Internet. This meet-point between the user's device and the operator network is usually termed the user-to-network interface or "Access-to-Network Interface" (ANI). Since any Internet user can create any Internet content and widely distribute it, the ANI presents additional risk.

A femtocell is another example of an ANI, and is likely to become a major point of risk exposure into the mobile network, since content sent via a femtocell rides the Internet for some portion of the journey. Just like content that originates in the Internet, however, end user-created content that crosses the ANI has the potential to include elements that can either harm or clog the network.

Session Border Controllers. Session border control technology is used in networks to mitigate security risks, to ensure that sessions are managed properly, and to enforce defined policies. Session Border Controllers (SBCs) are the platforms that are used to provide these functions, enabling smooth communications between multiple end points in IP communications. The location and function of SBCs are illustrated in Figure 2.

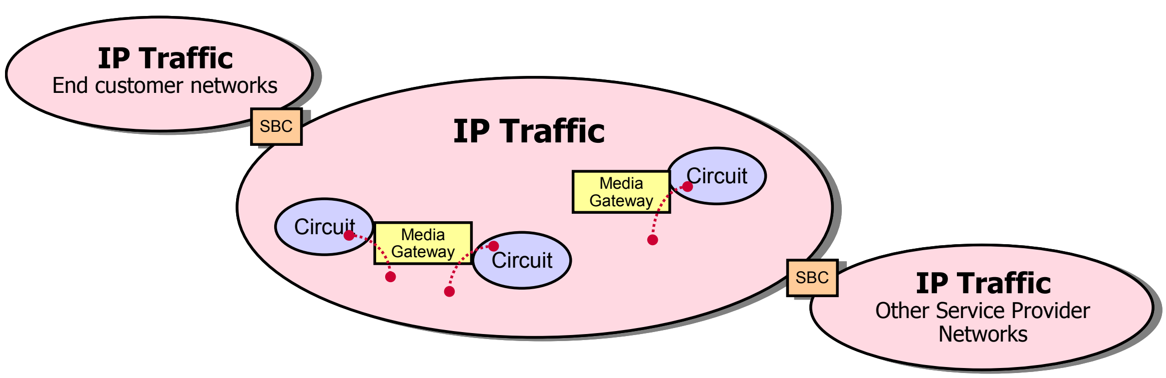

Figure 2. Session Border Controllers

Like the media gateways and call control elements that manage IP-to-circuit communications, SBCs play a similar role in IP-to-IP communications. They provide session management, policy enforcement, and security, along with other functions like Lawful Intercept and advanced routing.

Today's SBCs are commonly used at the signaling layer. As networks become more complex, however -- with more types of media and a more comprehensive need to analyze, control, and route traffic -- SBCs are increasingly being used to secure and control the actual voice, data, or video media itself.

Managing Network Complexity in Standardized Architectures

Today's SBCs are often stand-alone platforms that are commonly deployed at the primary IP-to-IP connection points in the network -- the Network-to-Network Interface (NNI) and the Access-to-Network Interface (ANI). For many service providers, these stand-alone platforms have sufficient capacity and extensive security, policy enforcement, and session management capabilities to be used for long periods of time in evolving networks.

Service providers, however, are facing tremendous challenges in dealing with the onslaught of network changes required to provide an ever-increasing number of revenue producing, IP-centric services. IMS is a classic example of these changes. It is a well-defined architecture, but it has a relatively large number of functional elements, including SBCs and media gateways (or their variants). In addition, each element has its own defined interfaces and interoperability with other elements. As a result of these complexities, many operators have been reluctant to quickly deploy these networks.

Not only do the new architectures create significant capital expenditure (CapEx) burdens for all of this new equipment, but service providers are also concerned about the complexity of managing many single purpose elements in the network. Facing substantial operational costs every time they deploy a new type of network element, many service providers are looking for platforms that provide multiple, simultaneous features to help them reduce the complexity and minimize the number of "touch points" that an IP packet requires as it traverses the network.

Evolving Gateway Roles in IP Networks. Due to their advanced media handling capabilities, the latest generation of gateways is particularly suited to resolve network complexity issues, integrating media gateway, SBC, and media server functions in order to minimize the number of discrete elements required in the network:

- **Media processing**: Because a gateway must perform high touch processing on the information that goes through it, it is built with tremendous hardware capabilities for media processing. This takes the form of a high bandwidth backplane capacity that maximizes packet throughput, and a multi-slot, multi-purpose chassis that can accommodate many Digital Signal Processors (DSPs) or Network Processing Units (NPUs) for advanced packet processing to perform SBC functions like session management, policy enforcement, and security.
- **Transcoding and Media Adaptation**: The processing capacity of the gateway also makes it a logical platform for providing various media adaptation functions that are required in IP networks for a variety of reasons. For example, fixed and mobile access networks are often bandwidth-constrained, resulting in many different,

incompatible codecs that encode and decode the voice content for more efficient routing over the IP network. As a result, one voice path using a G.711 codec may need to connect to another voice path using a G.729 codec, requiring a DSP or NPU from a gateway to provide the translation.

The IP network itself and any end user devices attached to it can result in other voice quality impairments -- including as delay, jitter, echo, and packet loss. Due to the rich media processing and interworking capabilities in the latest generations of gateways, they are the natural platform for providing advanced acoustic echo cancellation and other voice quality enhancements to mitigate these impairments.

- **Media Resource Functions**: Other media resource functions are often best-suited for gateways, including announcements, tones, and simple conferencing -- leaving the heavier media processing for more centralized platforms like media servers.
- **Network Location**: Gateways are often physically located at key IP interconnection points in the network, making them a convergence platform for consolidating elements. Integrating these multiple functions is a natural extension of both what the gateway is able to do, as well as where the gateway sits in the network.

  An additional benefit of using gateways for these functions -- in lieu of very centralized elements -- is that these high volume processing needs can be distributed farther down in the network -- where some gateways are already located and where the traffic itself either originates or terminates. This means that traffic is not needlessly routed through the network to expensive centralized elements for media processing.
- **Fixed and Mobile Integration:** Gateways that support both fixed and mobile codecs, protocols, and interfaces can be important migration platforms for operators -- enabling true network convergence for operators that have both network types. In addition, gateways can also provide critical functionality to enable Fixed Mobile Convergence in femtocell or WiFi networks, including secure IPSec tunnel termination and other security and media adaptation functions.
- **Network Integration**: Since media gateways are generally the first network elements for interconnecting diverse networks, they are often already extensively deployed. This broad deployment means that they are commonly integrated into Network Management Systems (NMS). As a result, thus simplifying the process of integrating new features into an existing gateway platform.

Evolving Definitions of Gateways. The telecommunications industry has long known the term "media gateway" as representing a network element that performed various types of media processing at the IP and TDM network borders. With advanced packet processing on-board the latest generation of media gateways, this definition has expanded to other gateway capabilities for the mediation of traffic at the borders of packet networks.

However, the multi-slot, multi-functional nature of media gateways is also resident in another industry standard form factor -- specifically the Advanced Telecom Computing Architecture (ATCA). An ATCA platform allows for multiple, often inter-related features and functions to be integrated onto a single chassis. Like media gateways, ATCA platforms are highly scalable to meet the needs of growing networks.

An ATCA platform is also an excellent alternative for deploying advanced IP network service capabilities. For example, an operator may have a need for massively scalable femtocell Security Gateway that supports a million or more active IP tunnels. The simple integration of additional Security Gateway modules into the ATCA chassis allows the operator to scale to meet these needs. If the same or adjacent applications also require additional session management, policy, or security, Session Border Controller modules can be added to the platform to perform those functions.

Application Flexibility. The key to successful deployments of new services depends upon the specific operator need. Where media gateways features are needed for mediating communications at the borders of IP and TDM networks, they can also be flexible enough to mediate and normalize traffic at IP to IP network borders. Where specific IP to IP mediation, security, or intelligent routing is required, the multi-slot ATCA choice may be the best alternative. Selecting a telecommunications vendor that can offer each of these alternatives gives the operator significant flexibility to deploy their networks according to their needs, improving time-to-market, revenue-generation capabilities, and network efficiencies.

About GENBAND

GENBAND is a market leader and pioneer in connecting, securing, and enabling efficient communications between network borders. The company's carrier class line of gateway and security products provide interconnection and migration solutions at the borders of circuit and IP networks, as well as advanced security and session management at the borders where IP networks meet.

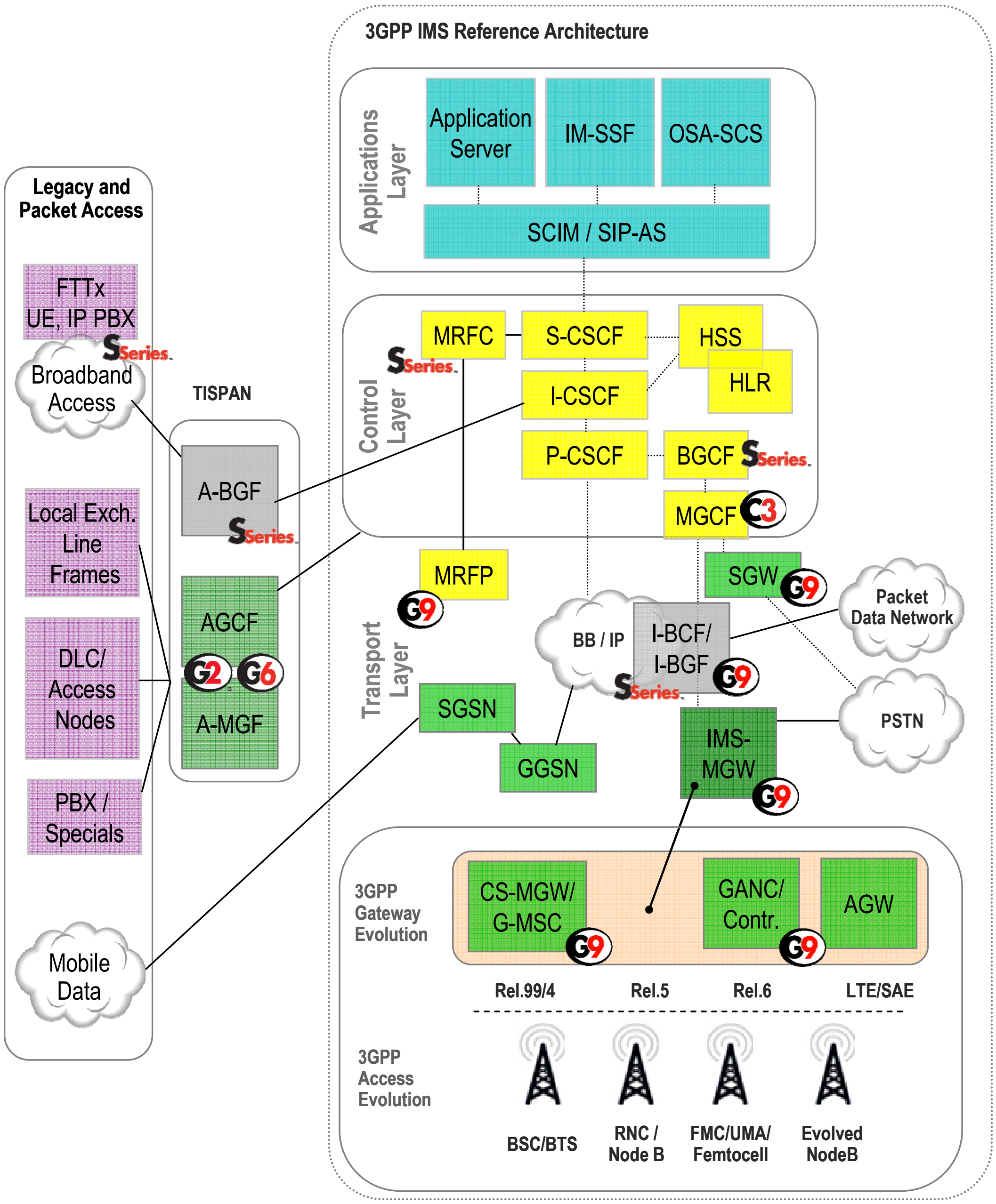

Figure 3. GENBAND Products in IMS Networks

GENBAND's three product lines of IMS-ready gateways and controllers provide significant value at the rapidly growing network edge -- where IP networks border other IP networks or legacy circuit networks.

G-Series: The G-Series includes the G9 Converged Gateway, G6 Universal Gateway, and G2 Compact Gateway.

The G9 is a high-density, carrier class trunking, access, signaling, and IP gateway that is purpose-built for use in mobile, fixed line, and converged operators' packet and circuit-switched networks. The G9 has a massively scalable backplane and is built from the latest generation of multipurpose DSP, computing, and media processing components. It has both IP and TDM switch fabrics for seamless interworking at the borders of networks including TDM to TDM, TDM to packet, and packet to packet. Extremely versatile, the G9 supports advanced architectures as defined by 3GPP, 3GPP2, and TISPAN NGN, among others -- and it provides a variety of solutions in GSM, UMTS, CDMA, Fixed Mobile Convergence (FMC), and fixed line networks. A state-of-the-art migration platform, the G9 gateway has an open Mc interface allowing operators to transition to IP Multimedia Subsystem (IMS) networks and the all-packet future, providing continuous long-term value, cost reduction, and revenue generation for service providers.

The G6 is a carrier class, mid-sized multipurpose gateway, purpose-built for highly reliable VoIP, that simultaneously supports multiple IP service architectures, and the G2 Compact Gateway is a small, hardened gateway for service provider and enterprise VoIP networks.

S-Series: The S-Series platforms include the S2 and S9 Integrated Border Gateways and the S3 Session Border Controller. The S3 offers extensive security, policy enforcement, and session management capabilities, delivering secure carrier class, real-time communications for mobile and fixed service providers at IP network borders.

The S2 and S9 are 2 and 14-slot ATCA platforms with multiple functions provided in the form of chassis modules, including the Session Border Controller and the Security Gateway for the S2 and S9. The SBC for S2 and S9 delivers security, policy enforcement, and session management for real-time communications in mobile and fixed service provider networks. The Security Gateway for S2 and S9 provides security, user authentication, mobile-IP connectivity management, secured tunnel management, policy enforcement, and accounting for operators' fixed mobile convergence (FMC) solutions, including femtocells and WiFi/WLAN.

C-Series: The C-Series includes the C3 Signaling Controller that offers fully featured, advanced routing and control solutions to manage complex interworking for fixed and mobile network operators at the TDM/circuit and packet network borders.