



# IMS Ready, and Raring to Go!

## Introduction

IMS architecture promises to bring a completely new world of voice, video, and data. Even the voice part of it will be something wildly different from today as vendors start talking about quad-play networks (land-line, cellular, video, and data) instead of triple-play. In fact, the Service Provider's (SP's) need to highlight the combined offerings of multiple voice technologies underpins the amazing transformations that we can expect to see—a world of seamless communication regardless of the access network. While it is easy to get caught up in the hype and possibilities, there is another side to the story. Even though IMS represents a vision of a standardized, simple, and scalable network, service providers are finding that increasing complexity, bandwidth requirements, and security concerns are stifling their ability to execute on that vision. End users demand high availability and high quality of service which cannot be solved by simply adding bandwidth.

Part of the issue is the fact that the IMS architecture is based on traditional data networking principles instead of traditional voice principles. IMS calls for a ubiquitous TCP/IP interlay between individual SPs and the services they provide—including voice services. While many SPs already offer data access in combination with voice, these two services are currently handled completely separately using different technology, experience, and equipment. Both the SPs and the traditional vendors they rely on don't necessarily have the technology, experience, and equipment needed to handle the challenges of an all IP network. Fortunately, F5 does; making TCP/IP applications fast, secure, and available is our primary focus.

## Increasing Complexity

Much like Service Oriented Architecture (SOA) is currently the buzz in the design and deployment of enterprise business applications, IMS architecture is designed to lower operational expenses (OpEx) and capital expenses (CapEx) associated with services deployment—as well as speed the development. Combined, this reduces the risks associated with attempting to define innovative new technologies. The modular design—again, almost exactly like SOA and Web 2.0—allows for the reuse of application pieces and the development of services that are simply unique combinations of other services, for example, Push-to-Talk over cellular combined with Instant Messaging.

SPs working towards IMS deployments, however, are finding some of the same hidden costs that enterprises are when dealing with SOA. The interplay between components, while reducing the number of systems, can dramatically increase the complexity in terms of troubleshooting and maintenance. When the systems were deployed in siloed environments, as has traditionally been the practice, the failure of a system only impacted the service silo in which it lived—now, a system failure impacts every service or blended service that uses it. This exacerbates the need for highly available sub-systems or components much like the Web services arena.

## Increasing Bandwidth Requirements

Similarly, the modular design of IMS, as well as the fact that voice and data no longer traverse separate networks, is posing an issue with bandwidth and quality of service (QoS). Again, while consolidating services into reusable components (like the Home Subscriber Service or HSS) greatly increases the efficiency of provisioning and reduces the OpEx and CapEx of the component, there is a significant increase in the amount of traffic to that centralized component. Now, instead of simply servicing a single silo, it must service all services needing it. This can cause significant issues in scale and performance. In addition, that increased traffic between components must also contend with the increased traffic of carrying all services across the same network—services with



varying levels of tolerance to latency and packet loss. This too presents issues with scale and performance of the individual applications, as well as the network as a whole.

### Security Challenges

Beyond the availability and performance challenges, SPs are also facing a security challenge. The IMS architecture is much more susceptible to attack and interference than the old fixed-line Telco business. First of all, by adopting all IP for the delivery of all services, IMS opens the SP up to all the same security vulnerabilities that any Internet application is confronted with—from denial-of-service attacks to application layer attacks. Second, just like many of the first SOA applications allow the users to create mash-ups of custom services, the IMS architecture has the same potential. This means that the services delivered by an SP may or may not reside within their own network. This opens the SP up to a host of new security issues—like how to handle billing and authentication issues when a user accesses an external service or to keep potentially sensitive information from other users of the network.

### Interoperability Within and Without

Finally, SPs who wish to implement IMS must deal with a host of interoperability challenges. For instance, the IMS architecture specifies the use of IPv6, primarily due to the vast number of IP addresses needed to handle the devices that might attach to an IMS network and the number of IMS networks that may evolve. Unfortunately, many of the traditional data networking devices and user equipment (UE) are incapable of handling IPv6 functionality. IMS is based on protocols like Session Initiation Protocol (SIP) and Real-Time Streaming Protocol (RTSP) which are not uniformly supported with the intelligence and control that web protocols (like hyper-text transfer protocol or HTTP) are. Additionally, while based on TCP/IP, IMS also relies on protocols like Stream Control Transmission Protocol (SCTP), which is almost unheard of in traditional data-networking implementations despite its advantages to similar technologies like Transmission Control Protocol (TCP).

These challenges are only compounded by the potential open nature of IMS to interface and provide blended services across SP domains. While an individual SP may be able to select and implement technology that perfectly matches each other in capability and TCP/IP implementation, they cannot account for the differences of the equipment used by other SPs or the myriad of devices that may access the services they offer.

### The F5 Difference

F5 is the world leader in Application Delivery Networking. F5 is the de facto standard in many of today's SOA deployments because of the intelligence, agility, and manageability that F5 equipment provides these architectures in making SOA a reality, enabling SOA to deliver on its promises. With full support for SIP, RTSP, and SCTP, F5 is ready to be the same cornerstone of IMS deployments.

### IMS-Ready Intelligent Load Balancing/High Availability

As IMS application rollouts move from first office deployments to full launch, service providers need a way to scale these applications for millions of users, while at the same time ensuring that the applications are always available.

The flexibility of TMOS has allowed F5 to extend the LB/HA of the BIG-IP® Local Traffic Manager™ (LTM) to the protocols that run in an IMS network. This means that the LTM can intelligently load balance equipment such as application servers (AS), call session controllers (CSCF), media gateways (MG), signaling gateways (SG), session border controllers (SBC), video



streaming servers, and so on with the same alacrity and agility that it handles HTTP in the Web services world.

While load balancing helps achieve the scalability necessary, the real *intelligence* comes from the health monitoring specific to the IMS protocols. Built-in health monitoring for SIP and RTSP makes it quick to implement monitors that check the health of the *service*. This is much more than a PING that verifies that the server is responding; it is an application level monitor that proves the service is up and available. Additionally, custom health monitoring can be used to structure these monitors to perfectly fit the application.

This intelligent LB/HA ensures that the multimedia applications are always available, and enables service providers to scale their IMS network efficiently.

### IMS Ready Full Proxy

Leveraging the full-proxy TMOS architecture, BIG-IP LTM is able to act as a translator to fix internetworking problems between varying IMS equipment at the TCP and UDP level. BIG-IP LTM now has specific iRules triggers designed specifically for SIP and RTSP enabling IMS traffic to be inspected and transformed at the connection level. Also, as previously mentioned, the full-proxy aids in protocol sanitization and standardization between components.

IMS requires lots of IP address space, and some providers will need to look towards IPv6 to be able to deploy IMS. An SP can begin to deploy IPv6 in the network without replacing application servers by placing them behind BIG-IP LTM. BIG-IP LTM can act as an IPv4/IPv6 gateway and give service providers an easy migration path to IPv6. In the same way, BIG-IP LTM can help translate between other SP networks or standard Internet services without the need to worry about which version of IP they are running.

### IMS Infrastructure Security

The same F5 technology used to protect HTTP applications is IMS-ready, ensuring that your IMS infrastructure is always secure. Having been proven on the front-lines of many of today's largest Internet sites, the LTM has specific Denial-of-Service (DoS) attack protection and provides many of the function of a Topology Hiding Internetworking Gateway (THIG). As a full-proxy implementation (see next section), the LTM also eliminates many protocol-based attack vectors by providing protocol sanitization as well.

Transport Layer Security (TLS) or Security Sockets Layer (SSL) are common technologies used to provide confidentiality and integrity services to Internet traffic. BIG-IP LTM enables you to add these technologies to the IMS implementation while offloading the processor overhead from the service, thus not only providing security but improving scalability and performance.

### IMS-Ready Carrier-Class Hardware

Service providers, especially traditional Telcos, have specific requirements for hardware that's deployed in their network. BIG-IP LTM has options available to meet these demands, including:

- A NEBS compliant BIG-IP LTM 6400 option
- DC and redundant power supply options
- High reliability, redundant failover configurations

Best of all, many SPs already have F5 equipment certified and deployed with their data networks helping to ease the transition between existing services and IMS architecture.



### Conclusion

The allusions to the fact that IMS architecture, in design and implementation, is nearly identical to SOA within the enterprise application development market are not without merit. In fact, with the exception of the actual protocols used (SOA using Web services protocols and IMS using SIP/RTSP/SCTP) they have nearly the same goal and exactly the same issues; availability, performance, and security.

By extending the capabilities of the F5 suite of products—like BIG-IP Local Traffic Manager—to include pre-built support of the core IMS needs, F5 is positioned to bring the same ease of design, deployment, and management to IMS that we have in enterprise architectures for more than a decade. F5 provides security, performance, and availability to IP networks; F5 is IMS Ready, and raring to go.