White Paper

Building IMS-Capable Core Networks

Backbone Foundations for Fixed-Mobile Convergence

Alan Sardella
Solutions Marketing Manager

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200175-001 March 2006

Contents

Executive Summary

The need for new revenue-generating applications and services is one of the main drivers for IP Multimedia Subsystem (IMS). Mobility features provide great opportunities in this area, and some of the initial applications include presence services and Push-to-Talk over Cellular (PoC). Later applications will feature richer multimedia services such as video messaging and conferencing, and entertainment functions such as mobile IPTV. IMS also provides the functionality to bill and account for these services, and to roll them out quickly and cost-effectively.

The IMS environment also contributes to the convergence of disparate wireline and wireless networks, and allows more feature-rich services over both. The eventual promise is for subscribers to be able to access any network (wireless or wireline) from any device (computer, PDA, or cell phone) and be able to move seamlessly from one network to another. The advantages of this promise can be understood from Russ McGuire's "Law of Mobility."

As a networking standard, IMS was developed by the Third Generation Partnership Project (3GPP) and is therefore tied to mobile operators, although support for fixed networks has been added by the European Telecommunications Standards Institute (ETSI).[1] IMS is therefore a key environment in Fixed-Mobile Convergence (FMC) services, which will allow users to access a single suite of telephony and other services no matter where they are and how they are connected.

The foundational needs of IMS-compliant networks are much the same as the requirements of next-generation cores supporting any multiservice environment. These requirements include security, scalability, high performance, Quality of Service (QoS), high availability, and the ability to have policy smoothly applied with the integration of a control plane.

The logical foundation for packet processing in an IMS environment is a converged, virtualized, secure IP/MPLS backbone. Wireline service providers are already migrating along these lines with great success; they can maintain the performance and security advantages of discrete legacy systems, while provisioning and configuring a single shared infrastructure ready for next generation services. In addition, an IP/MPLS backbone supports session-based awareness to underpin an IMS environment, and multiple access technologies to allow the network to support advanced IMS services, such as video telephony and voice, data, and video over multiple sessions. Of course, these services introduce new security concerns, which are addressed by appliances such as firewalls, intrusion detection and prevention systems, and session border controllers.

Juniper brings together all the required multiservice and session-based capabilities into the Service Provider Infranet, which subscribes to a layered model similar to IMS, and has been a beacon for Juniper for years.   Juniper is uniquely positioned to address the needs of providers who want to build IMS-compliant networks today, or be positioned to build them tomorrow.

Introduction to IMS

IMS is a flexible, packet-based network architecture that allows network operators to quickly and cost effectively introduce multimedia and other profitable new services into their

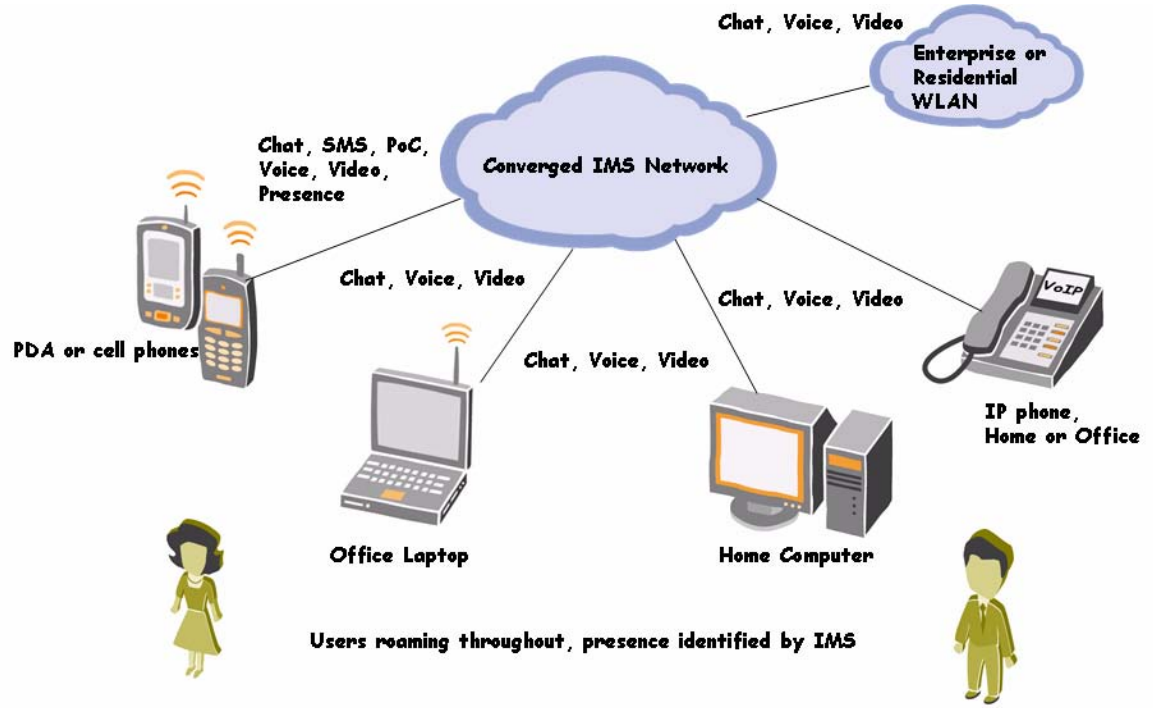
[1] The Telecoms and Internet converged Services and Protocols for Advanced Networks (TISPAN) is a standardization body of ETSI, specialized in fixed networks and Internet convergence. In a joint effort between the two groups, 3GPP Release 7 added support for fixed networks, by working together with TISPAN Release 1.

portfolios. The use of IMS architecture simplifies network operations and allows providers to focus on service introduction and business opportunity. For example, an IMS architecture could allow fixed and mobile users to communicate using voice, video, chat, and online gaming, and to take advantage of functionality such as Push to Talk over Cellular (PoC: the ability to quickly arrange meetings through a walkie-talkie mechanism), Instant Messaging (IM), and Presence (whether and how a user is available, and how the user wants to be contacted).

By itself, IMS does not specify any new services; rather, it provides a framework for network operators to build and launch their access-agnostic services. New applications, whether developed in-house or outsourced to third-party developers, can be integrated quickly onto IMS because of the nature of the architecture.

The following figure illustrates, at a high level, a converged IMS network that manages and controls the movement of subscribers between fixed and wireless networks.

Figure 1: A Simplified IMS Converged Network (Service Focus)



The IMS specifications define the functions to handle the signaling and user traffic for multimedia applications. Although some of the diagrams can look daunting, the functions are separated into logical layers, and many of the specified functions often reside in a single platform. Vendors have the flexibility to implement IMS functions in consolidated ways, and it is natural that platforms such as softswitches will combine many logically separate IMS call-processing functions, and that routers will take on some of the session-enforcement and gateway functionality in IMS.

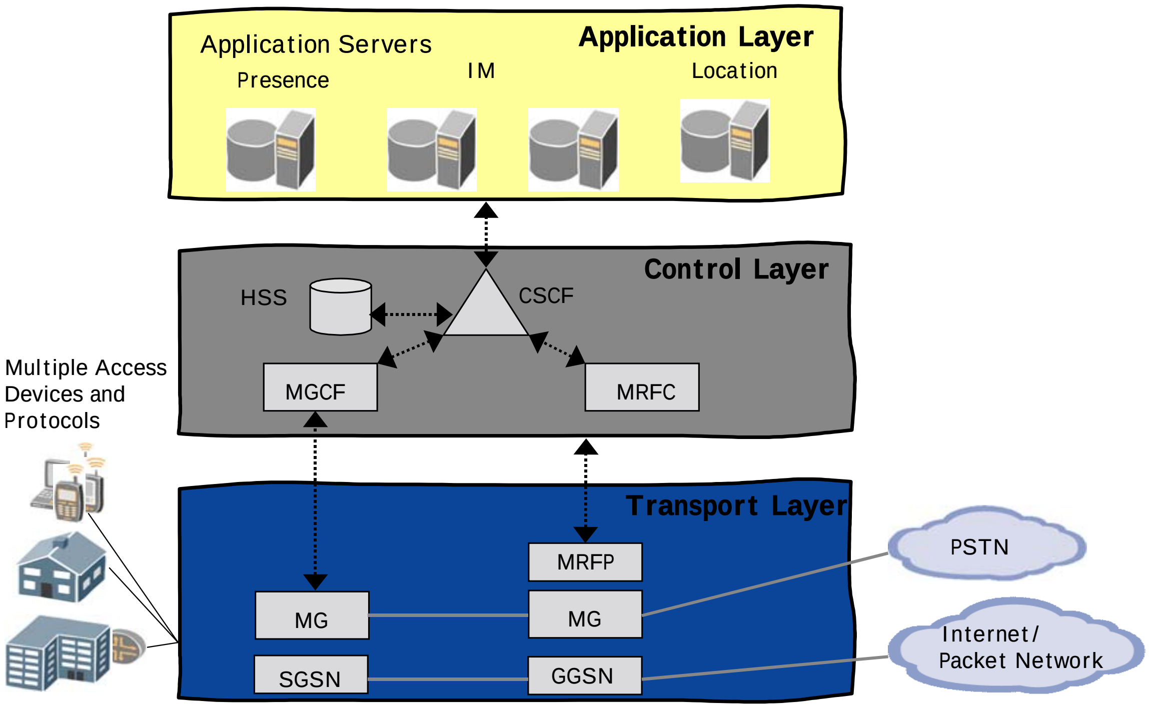
The main signaling protocol in IMS is the Session Initiation Protocol (SIP). SIP is the proposed standard today for multimedia communication between users interacting with voice, video and instant messaging. In IMS, the use of SIP facilitates interconnectivity between fixed and mobile networks. The requirements of provisioning and managing a SIP session can be very complex – much moreso than managing packets or even data flows. This will be discussed below in the *Session Provisioning, Control and Security* section.

The IMS Layered Model

IMS is described in a layered model; the three layers are the Application Layer, the Control Layer, and the Transport Layer. This is in fact a departure from traditional telecommunications networks, where signaling, transport, and applications are frequently integrated into single switches. This layered approach is aligned with other modem Next Generation Network (NGN) architectures, such as the Juniper Service Provider Infranet.

A high level view of the IMS architecture is shown in the following figure.

Figure 2: High Level View of IMS Architecture



Note: All acronyms in the diagrams in this paper are defined in the IMS Acronym Glossary at the end.

More details on the functions of these layers and the devices commonly found in them are given in the following sections.

Transport Layer

The *Transport Layer* provides the core network architecture of the General Packet Radio Service (GPRS), which consists of support nodes for data services:

- A Serving GPRS Support Node (SGSN) for data services to mobile stations, and
- A Gateway GPRS Support Node (GGSN) for gateways to the Internet or other data networks such as corporate WANs.

The Multimedia Resource Function Processor (MRFP) provides relevant multimedia resources (conferencing, announcements, interactive voice response, etc.). There is also an interface to connect the provider network to its internal Accounting and Billing Systems. The media gateways (MG) provide conversion between packet and circuit switched networks.

In general, this layer is where routers and switches, security firewalls, and optical transport reside, along with gateways translating between protocols and between packet and circuit based traffic. Security is particularly important in the Transport Layer, and Denial of Service (DoS) attacks must be parried through standard router hardening practices such as line rate packet filtering, rate limiting, flow replication and monitoring, and unicast reverse path forwarding (uRPF). To ensure session uptime, stateful firewall support on both native appliances and routers is also critical.

The nature of routing and switching is sophisticated with IMS, because the services and policies that enable transport require specific adaptations within the network infrastructure. Thus, the routing that occurs within the IMS transport layer is dependent on service quality variables such as Quality of Service (QoS), high availability (HA), and congestion and session management. The policies that set these features, often on a per-session basis, are set in a higher layer (the Control Layer) and enforced in the Transport Layer.

The need for ubiquitous access is illustrated on the Transport Layer. To take full advantage of the value of IMS services, devices will access the network over many technologies such as cellular, data, 3G, Wi-Fi, WiMax, DSL, fixed IP access, PSTN etc.

Note: It should be noted that even after an IMS rollout, there will still be large quantities of legacy voice traffic going through the core backbone. TDM and ATM will coexist with IMS, and will need in fact to interwork with it.

Control Layer

The *Control Layer* provides session control and management, and is responsible for setting up and taking down packet sessions. It also contains the information on subscriber authentication, service authorization, and location. This layer is essentially the “brains” of IMS, making the generic policy decisions that are enforced in the Transport Layer.

The Control Layer includes the SIP servers that register user devices and route signaling messages between them to set up sessions (this is referred to as the Call Session Control Function or CSCF). The CSCF interacts with the Home Subscriber Server (HSS), which is the database containing subscriber profiles and preferences.

The border gateways on the Control Layer allow different networks to interoperate with each other. The Media Gateway Control Function (MGCF) and Multimedia Resource Function Controller (MRCF) interact with the CSCF and control the media gateways and media resources.

Application Layer

The *Application Layer* hosts application and content services. This includes data centers of application servers, web servers, etc. Also included here are generic service enablers that manage service elements like user groups and presence. These service elements connect to users through the control plane. Most of the new multimedia applications or application enablers, such as presence and location (where a subscriber is) are supported by the Application Layer.

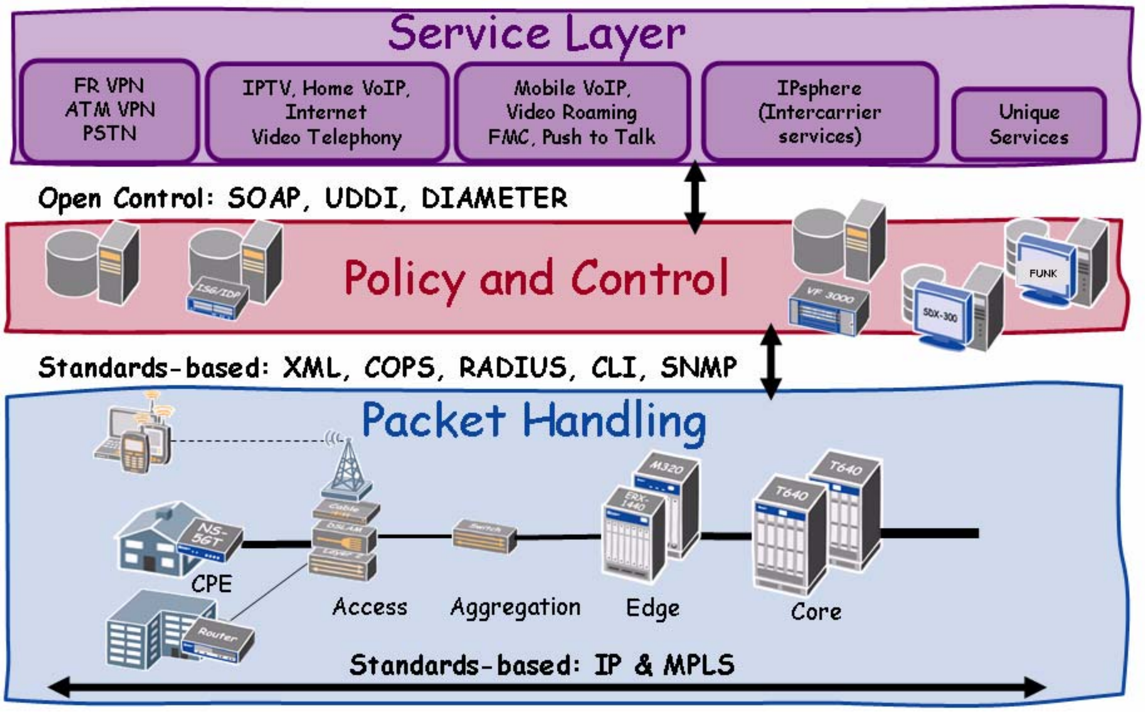
The Infranet Layered Model

Juniper has led the industry in building networks with similarly layered architectures (to IMS) for its entire history. Juniper Infranets are very much aligned with requirements of IMS. In particular, layers allow scaling of the infrastructure and encourage standardized interfaces to be used. This allows a best-of-breed approach and healthy vendor competition at all layers. Ultimately, providers can more easily support valuable services.

Infranets offer complementary functionality to IMS, and in conjunction with the work of the IPsphere Forum (www.ipsphere.org), add cohesion to interprovider relationships, creating business context for the functionality provided by IMS.

The following diagram shows the architecture for Juniper's Service Provider Infranet; the inter-provider signaling functionality of the Services Plane will be fulfilled by the efforts of the IPsphere Forum. The northbound interfaces of the Infranet's Policy and Control layer will allow integration with services found on the Application Layer of IMS.

Figure 3: Juniper's Service Provider Infranet Architecture



Transport plane functionality is the foundation of IMS— strong underlying IP packet processing is required for the new services of IMS to succeed. On the service and control planes, Juniper provides products in the areas of session control, security, management, and application acceleration. Of course, Juniper is also partnering at these layers to provide best of breed, end to end solutions for IMS and for value added services.

As part of the Service Provider Infranet, Juniper is grouping traffic processing capabilities into *feature packs* that will provide enhancements to basic connectivity, legacy services, poly-play networks, session-based services, service publishing and so forth. This modularity allows service providers to choose the right set of functions that adapt to, and enhance, their current network, without requiring unnecessary network redesign.

The Core Network and the Transport Layer

The requirements of core networks to support an IMS Transport Layer are very similar to the needs of any next generation, multiservice core network and are fulfilled by proven IP/MPLS routing and security platforms.

It is necessary for advanced traffic processing platforms, in both the security and routing domains, to populate the transport plane of IMS architectures. The primary requirements are:

- **Scale:** These networks will be some of the biggest in the world, so mechanisms for scaling to very large amounts of traffic are essential.
- **Policy Driven:** The ability to dynamically control almost any aspect of the forwarding and routing elements from the layer above (that is, on request of the softswitches and other elements in the control layer).
- **Performance:** These networks have voice, video, and other real-time traffic flowing on them all the time, so low latency and jitter, and line-rate forwarding under all control conditions is required.
- **QoS:** Services on IMS networks will range from best-effort delivery to mission-critical voice and other media, and the network must be able to address this entire range with the appropriate quality of service.
- **Security:** Since the consequences of, for example, a DDoS attack are great (potentially interrupting thousands of voice calls and other high-revenue and critical services), it’s essential that DoS security be provided at the network (IP) through application (worm propagation, spam) layer. In addition, application level threats (virus, hacking, vulnerability exploits) against user devices, and threats to infrastructure operating systems, must be mitigated.
- **Availability:** For the same reasons as above, networks and their elements must be very highly available.
- **Flexibility:** As IMS, and service provider networks in general, are generally multi-vendor environments, adherence to open standards and the ability to be agile and customizable is critical.

The best approach for building the foundation of an IMS environment involves creating a secure, converged IP/MPLS network that is agile and flexible enough to allow IMS functionality to be incrementally implemented as it becomes available.

Foundational Features of the Core Network

Both mobile and wireline network operators are concluding that consolidating their separate networks onto a single IP/MPLS backbone will provide a robust, scalable solution for meeting the needs of next-generation service-oriented environments such as IMS.

Converge, Virtualize, and Secure

While access networks may remain heterogeneous, service providers are migrating their core networks to a single, consolidated IP/MPLS infrastructure.

An IP/MPLS core provides a great deal of flexibility and a solid platform for future services to be added to the network. The result is a less costly, more flexible network that is demonstrably compliant with privacy standards, and can be easily augmented to provide new services.

The converged infrastructure must be secured. Service provider networks of all descriptions are under constant attack. Routers and their interfaces, as well as routing protocols, and network management, are all critical network components, and must work securely. Fundamentally, these security requirements include:

- Clean separation of the control and forwarding plane, with rules limiting access to control plane
- uRPF: Assurance that a packet that arrives on an interface came from a host that is reachable through that interface (and is dropped if it did not)
- Rate limiting to break connections that are involved in DoS attacks
- Packet filtering, to ensure that packets intended for a destination (such as a router's control plane) that they are unauthorized for are dropped
- Flow replication and monitoring, to identify attacks and prepare for mitigation before they become serious
- IDP (intrusion detection and prevention) at Internet gateways, and a firewall plus IDP in the path used to communicate between mobile devices
- Administrative separation of policy decisions on the Control Layer and enforcement on the Transport Layer

The next step is to virtualize resources on this converged IP/MPLS backbone. This virtualization comes in the form of MPLS VPNs, both at Layer 2 and Layer 3. MPLS VPNs are secure and reliable, and the benefits of migrating to MPLS can be immediately realized.

Layer 3 MPLS VPNs allow operators to consolidate various network services onto a common IP/MPLS infrastructure. VPNs also allow a more rapid introduction of the value of MPLS into the existing IP infrastructure. The benefits of migrating to MPLS can be immediately realized as individual network sites are MPLS enabled with VPNs. These sites can immediately take advantage of features such as MPLS fast-reroute and traffic engineering (including per-hop Class of Service – CoS – behaviors as well as DiffServ TE) while interoperating with the existing IP network.

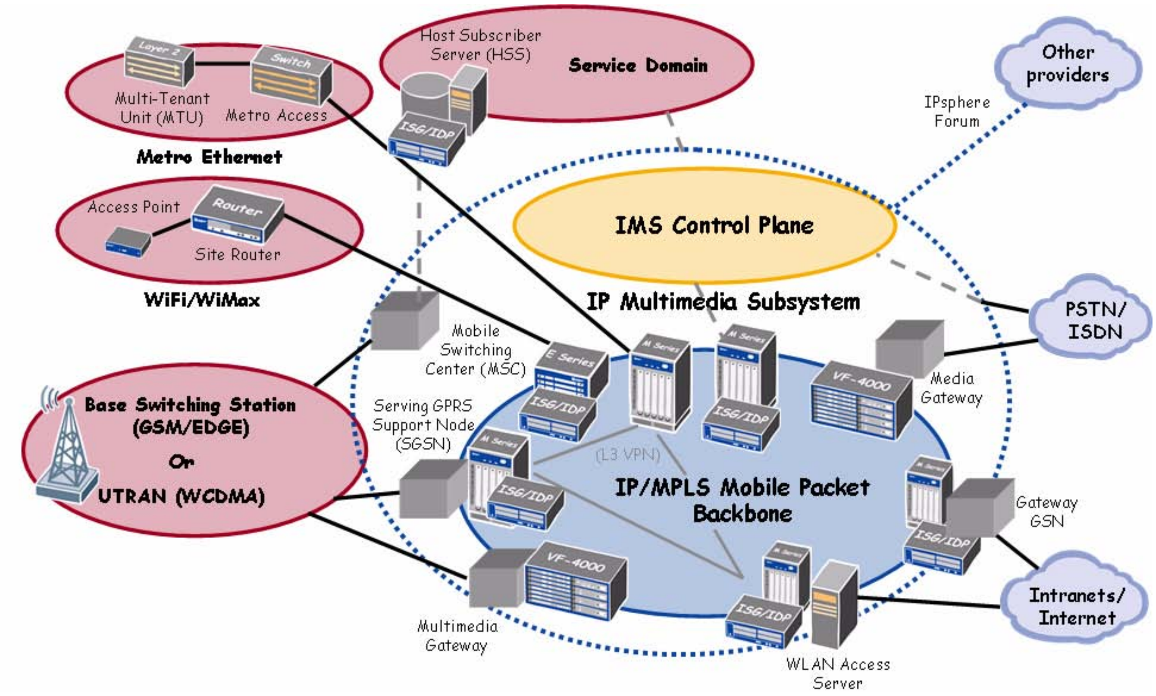
A further advantage of virtualizing in this way is that network operators configuring for IMS get their own dedicated space on the converged network. With the secure isolation of the VPN, the operator's IMS team can perform all of their provisioning in this space. It's a logical virtualization of resources, fully available to the IMS team.[2]

[2] For specific information on the benefits of MPLS VPNs to mobile operators, see the white paper entitled, *Introducing MPLS Layer 3 VPNs in Mobile Operator Networks* at http://www.juniper.net/solutions/sp/mobile.html.

Juniper facilitates an easy migration of legacy circuits to VPNs with the Infranet Legacy Services feature pack, a collection of services enabling Ethernet, Frame Relay and ATM to traverse the multiservice backbone in Layer 2 VPNs. These VPNs maintain QoS, availability, and operations of the original service, with the same clean traffic separation they enjoyed with a Frame Relay or an ATM circuit, but which can be maintained in a far more straightforward manner. At this point, other virtualized services such as QoS and DiffServ TE are also very easy to maintain, as they are configured within the VPN.

The following diagram shows the role that converged IP/MPLS core can play in providing the foundation for creating an IMS environment.

Figure 4: IP/MPLS Core Backbone Serving the Needs of IMS



At this point, operators can work on creating a secure IMS service infrastructure. Every server farm, from the CSCF to the servers on the Application Layer, can be secured with high performance firewalls and intrusion detection and prevention (IDP). The same holds true for other servers on the Control Layer such as DNS servers and AAA servers (which may be associated with the HSS function).

The Transport Layer contains similar requirements. Both individual GPRS nodes, and of course GPRS peering points, need to be secured with firewall (GPRS aware) packet filtering, intrusion detection and prevention (IDP), and optionally with IPSec VPNs. This virtualization allows a single platform to support multiple customers.

Protecting servers is critical for a variety of reasons. For instance, billing is going to be a large facet of all the increased services that are offered, and overbilling can be a critical problem that could bring down the fundamentals of your whole IMS network (angry customers, bad press, and so forth).

A converged infrastructure will make billing models easier to support, and Service Level

Agreements (SLA) easier to propose and to enforce. And finally, security can be more consistently applied to a converged core: the process of containing security threats will be much easier to maintain than it would be on dissimilar equipment.

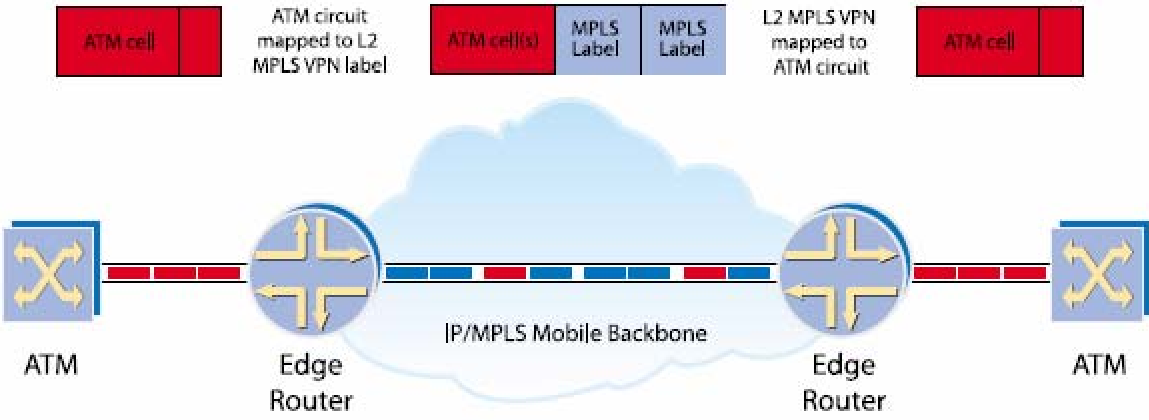
As IMS will support service delivery over multiple access networks, the edge into the multiservice backbone must have very high-density interfaces and subscriber management. The interfaces may be to aggregate WiFi, WiMax, or DSL, and they will all need to be secured.

Case Study: Implementing a Mobile Backbone Network

A European mobile operator needed to consolidate multiple separate networks into a consolidated core and expand its mobile backbone network. The operator wanted to collapse multiple networks onto a converged IP/MPLS network, and have the services be scalable with IPv6 capability.

Using Juniper routers to perform this migration provided the operator with an established strategy that permitted (in the short term) the coexistence of their existing ATM infrastructure through interworking with IP/MPLS VPNs. The operator then had a network that was then ready to support the infrastructure for a next-generation environment such as IMS. As shown below, the provider greatly expanded its ability to support access types from disparate networks by implementing Layer 2 MPLS VPNs, which allowed them to consolidate traffic from PPP, ATM, Frame Relay and other sources onto the IP/MPLS backbone.

Figure 5: Layer 2 MPLS VPNs Consolidate Multiple Access Types



Many customers have already converged onto a virtualized, secure IP/MPLS backbone in this way and are now preparing to build IMS environments off these core networks. As services scale, they need to continue their transformation and migration by increasing their access and also scaling to handle their increase in the number of sessions, with session security, session awareness, and application interworking. As IMS is launched, they will have to address another phase of security threats to secure the processing of features such as presence and

IM.[3]

Launching IMS Services

As IMS deployment ramps up, there will be more and more subscribers wanting varied access types – examples include WiFi, WiMax, dedicated broadband and leased line access. Some of these users (for example DSL, WiMax, and Wi-Fi) will require basic subscriber management – including authentication, address allocation, and resource authorization. In addition to access density and interface types, there is the question of scaling sessions and services. Furthermore, all access types will have to be secured with threat mitigation solutions to handle threats such as DDoS. Juniper delivers these features in the Infranet Poly-Play feature pack.

Potential for running applications on handsets that are normally associated only with a PC and a wireline connection – Instant Messaging (IM) is one instance of this. One can be reached on chat more easily in a mobile device such as a cell phone or PDA.

This is a very rich enhancement to the IM application: if one end of the IM conversation is a desktop and the other is a PDA, then an access-agnostic core network capable of finding these devices is of great value. And this value only increases if the application turns to conferencing, with a combination of users who may be mobile (on both cell or WLAN), using a dedicated leased line for a business, and using broadband access from homes or businesses.

The increased value of applications when they can be accessed by a user the road, or outside the range of a fixed device, has recently been termed the "Law of Mobility"; it states "Mobility exponentially increases the value of any product."[4] This law also notes that the potential to build mobility into products and applications is becoming more cost effective, and that businesses and consumers can take advantage of these trends will parallel Moore's Law (of computing) and Metcalf's Law (of the Internet).[5]

The Law of Mobility shows itself in many ways. For instance, if a mobile handset user taking advantage of a corporation's IP Centrex or hosted PBX service, one could envision a scenario such as this: an employee is walking into her office building talking on a mobile handset, and as soon as she gets to her desk, the call can be transferred to her IP-enabled desk phone, still controlled by the same SIP server. The call quality can be improved and the other advantages of being on the desk phone (or a soft phone) are now realized. All phone access is unified and converged, and users can be located and can access phone messages, email, and other contact logs using a variety of devices, and from a single data store.

Other examples of session-based applications made possible by widespread IMS deployment include the following:

- Push to watch, text, or stream, as well as "click to talk" from a workstation
- Messaging with voice, video, and unified communications
- Instant conferencing for voice, video, and chat

[3] For more information, see the case study entitled, *Implementing a Mobile Backbone Network* at http://www.juniper.net/solutions/sp/mobile.html.
[4] For more information, see the whitepaper entitled *The Law of Mobility* by Russ McGuire at http://www4.sprint.com.
[5] For a recent article comparing these laws, see *Moore's Law, Metcalfe's Law; now McGuire's* at http://www.networkworld.com/columnists/2006/011606briere.html.

- Multiparty gaming with voice and mobility
- Other presence services such as find me, follow me, and report availability status
- IP Centrex, hosted PBX, and virtual assistant
- Other entertainment services such as IPTV or VoD over the Internet

There are other considerations regarding session-based services that are best served on a converged network. Regulatory requirements are an example; these include Lawful Intercept, E911, Primary Line Services, and Equal Access.

These types of advanced applications will have high revenue potential but may also be difficult to manage. They will often need the support of partnerships between handset providers and network operators. At times, cooperation may be needed between competing providers in order to partner for best advantage.

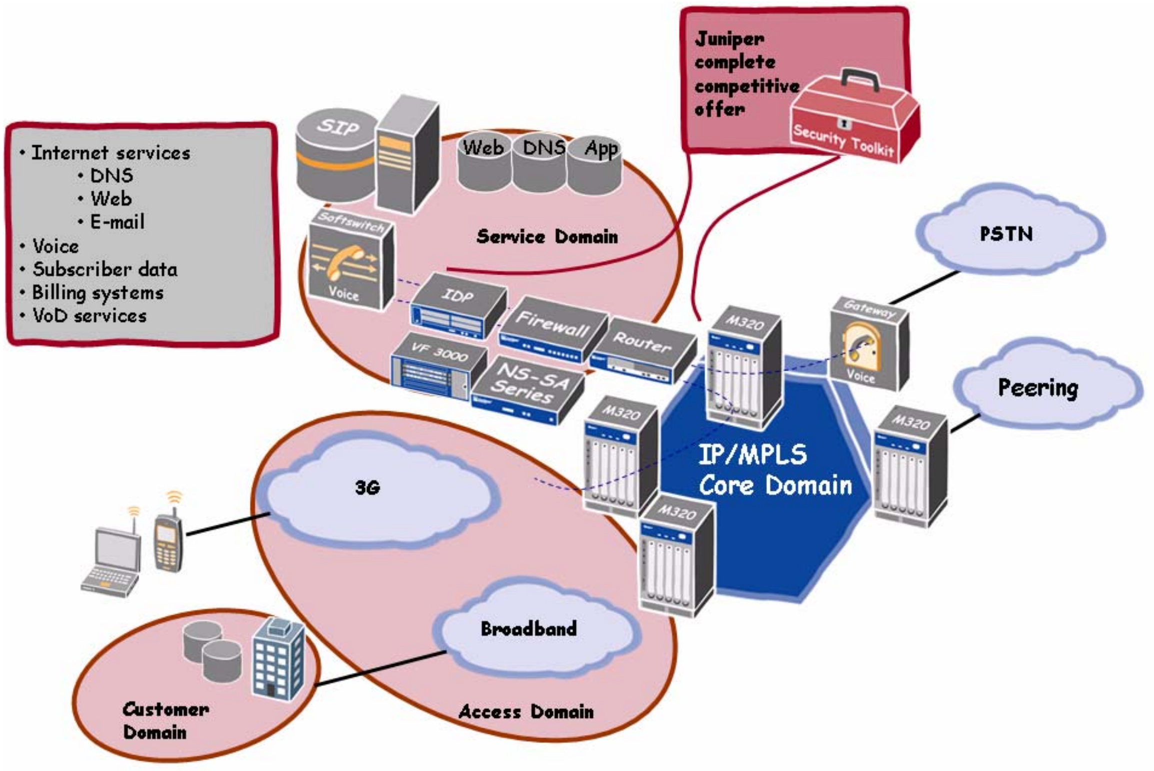
The federation-oriented capabilities of industry forums such as IPsphere are also likely to play a role here, as one operator may choose to outsource local access to another operator who has the published the ability to provide special access to a select group within a certain region. Providers may also choose to federate in terms of sharing SIP sessions; one may terminate the session and pass it to another.

Securing Services and Infrastructure

As compared to wireline-only services, security issues become more complex when mobility is added to the connectivity picture. There are many new entry points for security threats, and there is a new mobile infrastructure to attack. Attacks may be against FMC-related applications and services (such as attempts to infiltrate authentication, home location, and billing), as well as on the infrastructure equipment (where network or signalling attacks may be a concern) or on the servers themselves, where the threats involve traditional virus attacks. In fact, this last threat can apply equally to handsets and mobile devices.

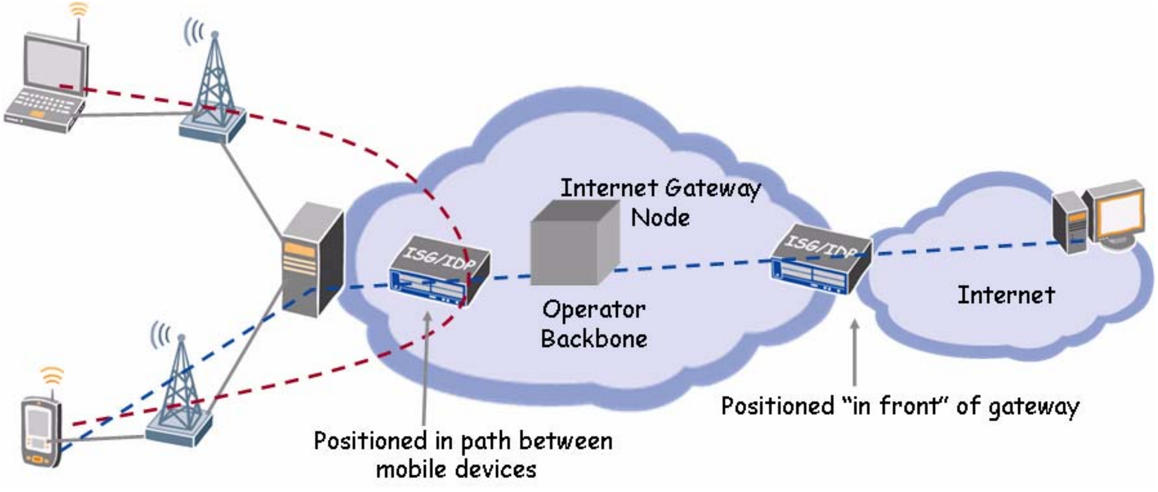
Juniper's security toolkit includes IDP and firewall services, as well as session border controllers.

Figure 6: Securing the Services



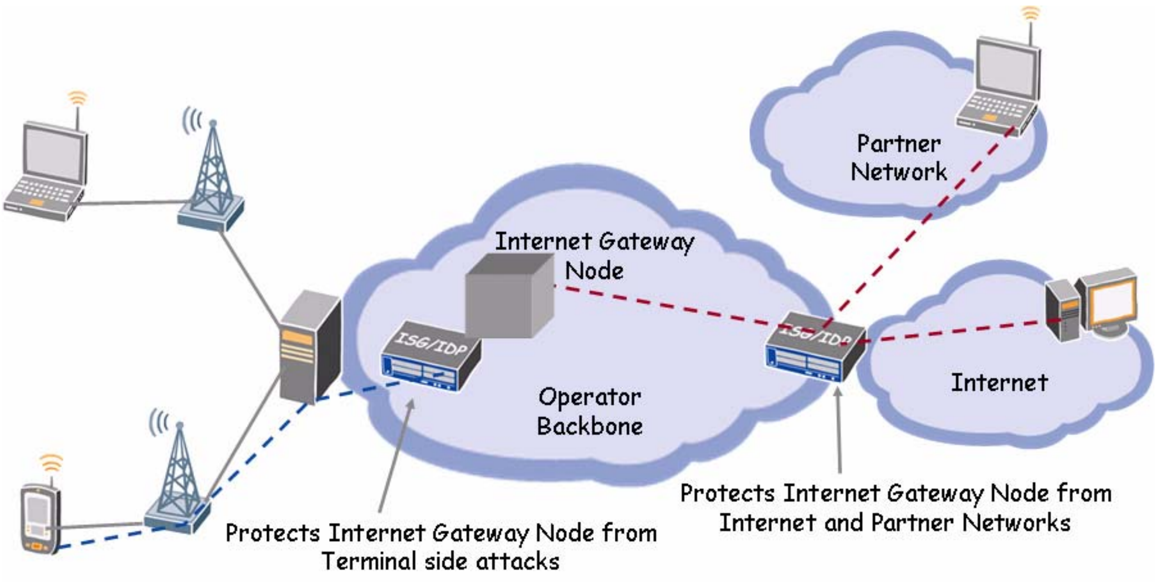
Operator networks are subject to a variety of different threats, which may be (perhaps unwittingly) propogated by end-user devices, and which involve threats to either these devices or to server farms. As the following figure shows, these threats are effectively neutralized with firewall and IDP functionality, either positioned in front of the Internet gateway or along a path between two communicating devices.

Figure 7: End Terminal Security


Internet Gateway Node
ISG/IDP
ISG/IDP
Operator Backbone
Internet
Positioned "in front" of gateway
Positioned in path between mobile devices

There are additional issues with gateway nodes providing connectivity to either the Internet or to partner networks. These nodes need a highly scalable and redundant security solution. In the solution diagram below, a very high capacity IDP/Firewall device (the Juniper Networks ISG) protects the Internet gateway node from terminal side attacks, while the other ISG protects the Internet gateway node from the Internet and partner networks.

Figure 8: Operator Node Security

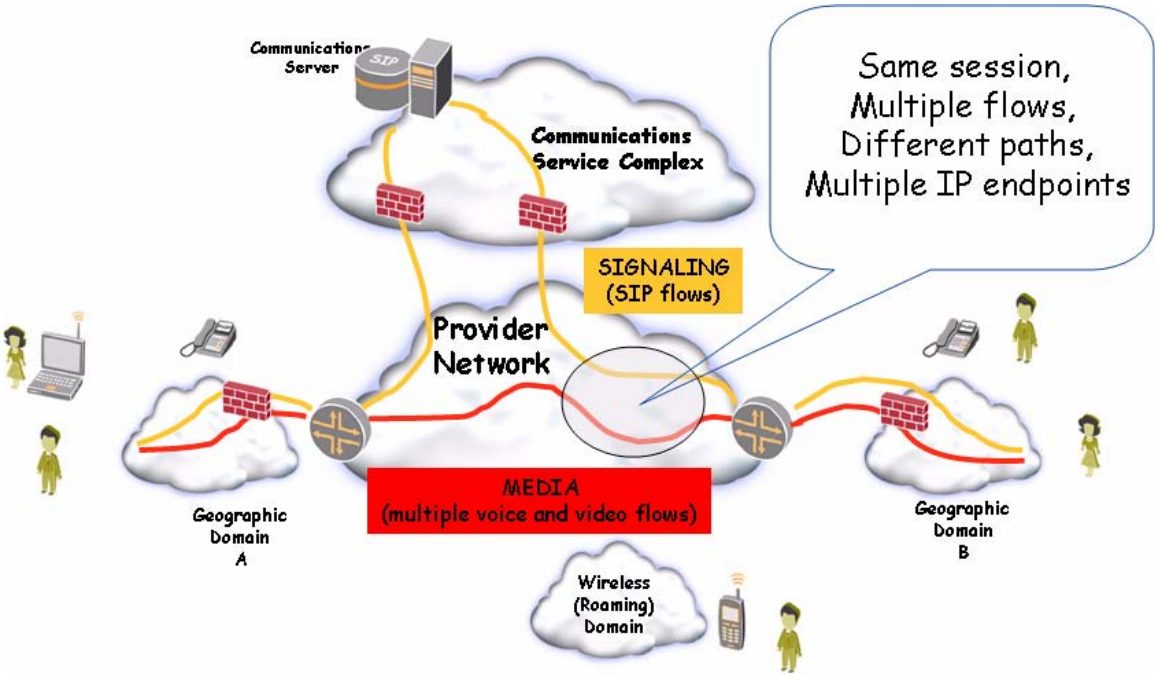

Partner Network
Internet Gateway Node
ISG/IDP
ISG/IDP
Operator Backbone
Internet
Protects Internet Gateway Node from Internet and Partner Networks
Protects Internet Gateway Node from Terminal side attacks

The Juniper Networks service provider portfolio provides many best-of-breed security platforms with stateful inspection and policy enforcement, denial of service (DoS) attack protection, and over billing attack protection to reduce risk levels. Additional literature on these platforms and their applicability to mobile networks or to converged fixed/wireless networks may be found on the Juniper Networks website[6].

Session Provisioning, Control and Security

On every layer of the Infranet, special features are needed to provide certain services relevant to IMS. A primary example is session provisioning and control. To control sessions, networks need extra intelligence (typically at the network edge) to control multiple dynamic flows, IP endpoints, network paths, and a separate control and media plane. An example of this extra complexity is shown in the following figure.

Figure 9: Sessions are More Complex to Provision and Manage

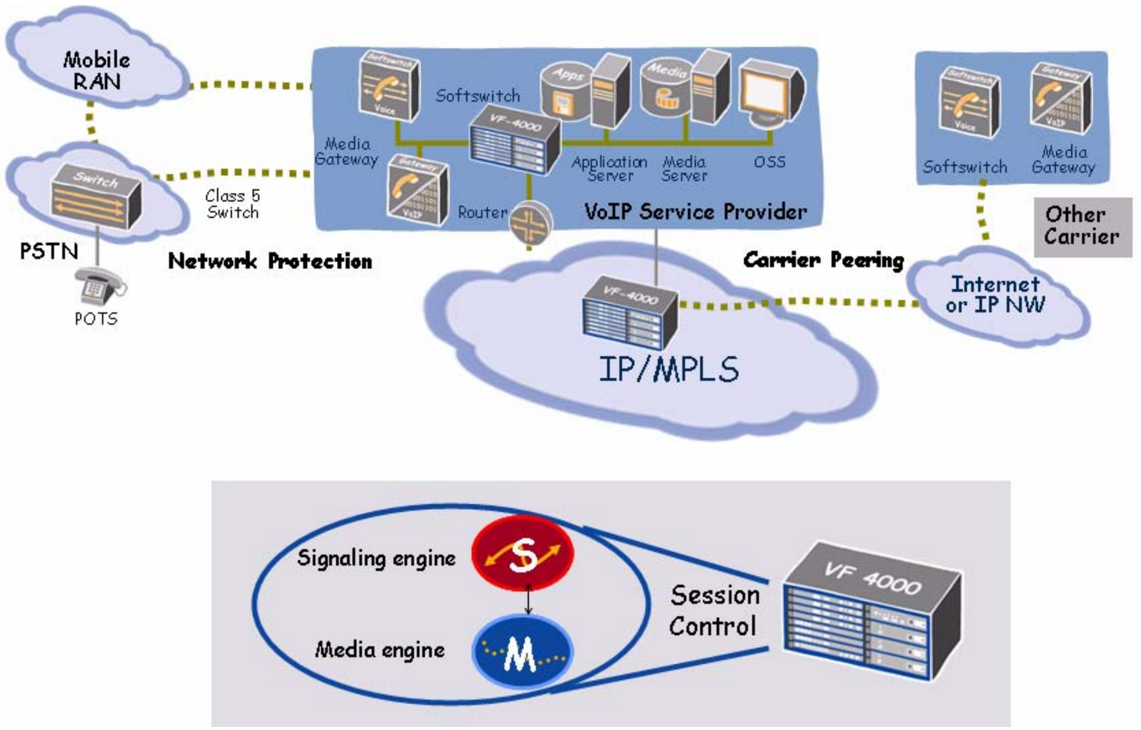

Communications Server
SIP
Communications Service Complex
Same session, Multiple flows, Different paths, Multiple IP endpoints
SIGNALING (SIP flows)
Provider Network
MEDIA (multiple voice and video flows)
Geographic Domain A
Geographic Domain B
Wireless (Roaming) Domain

While routers and switches make decisions based on header fields within individual packets, and sometimes on a flow basis within a single flow, session control involves awareness and decisions based on multiple flows, on both signaling and bearer channels.

Juniper Networks VF-Series session border controllers are deep packet processing devices that support both signaling and media streams (for all common VoIP protocols) to classify, measure, and manipulate each packet for the management and reporting of VoIP traffic. The following diagram shows the session-based network protection and secure carrier peering capabilities of the VF-Series solution.

[6] For more information, see *Evolving Security Needs in the Mobile World* (www.juniper.net/solutions/literature/white_papers/200146.pdf) as well as *GPRS Threats and Security Recommendations* (http://www.juniper.net/solutions/literature/white_papers/200074.pdf) and *Infrastructure Security Gateway for GPRS Networks* (http://www.juniper.net/solutions/literature/solutionbriefs/351041.pdf).

Figure 10: VF-Series Network Protection and Carrier Peering



The threats between the core backbone and the voice (and/or mobile) network shown above include DoS, service theft, hacking, tampering and fraud, and the intrusion of unauthorized users. VF-based security includes media firewalling (via negotiated ports), signalling validation, DoS protection, registration and dialog security, and topology hiding.

For peering and wholesaling, the concerns are billing verification, access control, and topology hiding. In addition to session security across routing domains, the VF provides call routing and load balancing, and applies policies to the call routing processes. The VF also provides access and admission control and QoS.

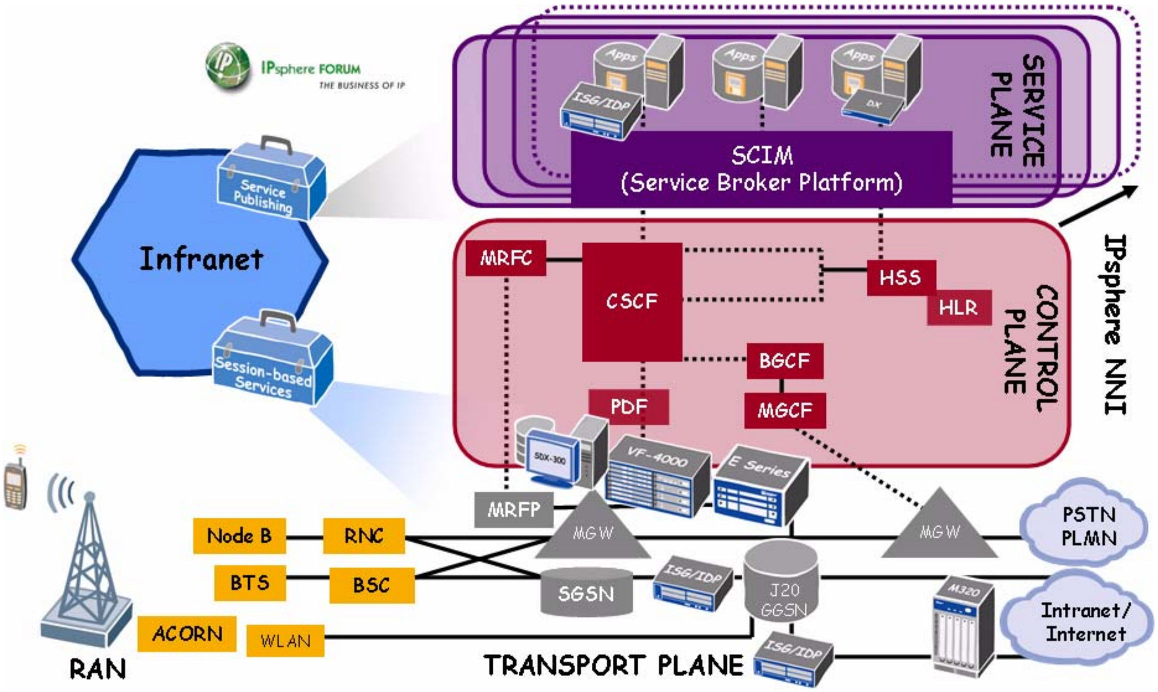
VF-Series session border controllers also provide effective solutions for NAT traversal, and VPN/VLAN address translation.[7]

Infranet Feature Pack Mapping to IMS Architecture

The following diagram shows how the Infranet feature packs provide the multiservice network and support IMS, and also illustrates Juniper's product positioning in the IMS environment.

[7] For more information on VF-Series session border controllers, see http://juniper.net/products/sbc/.

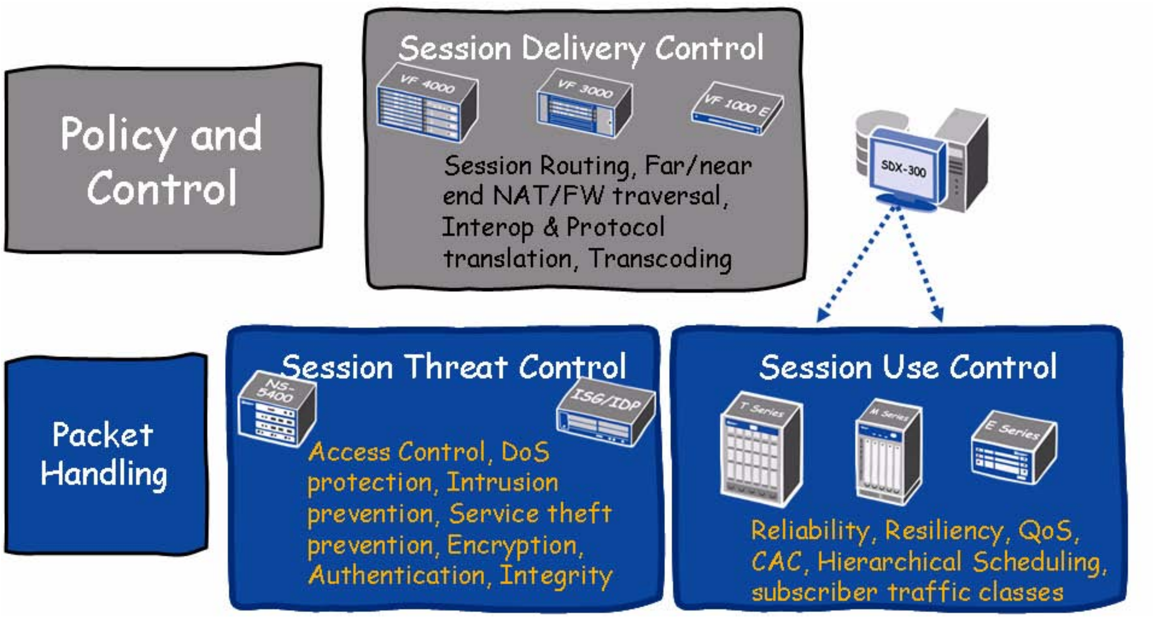
Figure 11: IMS Architecture with Infranet and Juniper Products



Juniper’s feature packs provide coordinated features and functionality, across wide portfolios, that have been tested together, and that when released to providers support the appropriate business services to the requirements of next generation networks. In the case of IMS, the most relevant feature packs will provide session-based services and federation services (largely through a connection to IPsphere).

The session-based services delivery (via the session feature pack) provides delivery, use, and threat control (see figure below). Essentially, these services provide a complete session-enabled network infrastructure. The following figure illustrates some of this functionality and the products that are relevant to it.

Figure 12: Session Pack Features for Delivery, Use and Threat Control


Policy and Control
Session Delivery Control
VF 4000
VF 3000
VF 1000 E
Session Routing, Far/near end NAT/FW traversal, Interop & Protocol translation, Transcoding
SDX-300
Packet Handling
Session Threat Control
NS-5400
ISG/IDP
Access Control, DoS protection, Intrusion prevention, Service theft prevention, Encryption, Authentication, Integrity
Session Use Control
T Series
M Series
E Series
Reliability, Resiliency, QoS, CAC, Hierarchical Scheduling, subscriber traffic classes

In addition to ensuring highly efficient session-based service, Juniper's session pack provides for differentiated services creation (in terms of QoS, security and connectivity), and highly granular security and threat containment.

Conclusion

Juniper provides traffic processing for the top 25 worldwide services providers, as well as security solutions to 23 of the top 30 wireless carriers; 9 of the top 10 mobile carriers also use Juniper's routing and aggregation products. Providers are confident that building and enhancing networks with Juniper's Service Provider Infranet will ensure guaranteed network performance and security for value-added applications. The Service Provider Infranet includes the session-oriented features and the service awareness that an IMS network requires.

The requirements of IMS-compliant networks, particularly on the Transport Layer, are directly in line with what Juniper has been providing in advanced traffic processing capabilities from its inception. The foundation for creating an IMS environment, in both the wired and the mobile spaces, is the creation of a converged, secure, virtualized core network, based on IP/MPLS. This foundation allows the control and application layer capabilities of IMS to be securely woven into the network. It also provides the basis for the high density and variable access requirements of a networking environment that provides the benefits of mobility to the largest number of subscribers.

IMS Acronym Glossary

3GPP/3GPP2: Third Generation Partner Project (2)

AF: Application Function

BGCF: Breakout Gateway Control Function

BGF: Border Gateway Function

CNI: Customer to Network Interface

COPS: Common Open Policy System

CSCF: Call State Control Function (may be Proxy-CSCF, Interrogating-CSCF, or Service-CSCF)

ETSI: European Telecommunications Standards Institute

GGSN: Gateway GPRS Support Node

GPRS: General Packet Radio Service

GTP: GPRS Tunneling Protocol

HSS: Home Subscriber Server

HLR: Home Location Register

ICI: Intercarrier interface

IMS: IP Multimedia Subsystem

Infranet: Infrastructure network

MGCF: Media Gateway Control Function

MGW: Media Gateway

MMS: Multimedia Messaging Service

MPLS: Multiprotocol Label Switching

MRFC: Multimedia Resource Function Controller

PDF: Policy Decision Function

PEF: Policy Enforcement Function

PEI: Policy Enforcement Interface

PoC: Push to Talk over Cellular

SCIM: Service Capability Interaction Manager

RACF: Resource Allocation and Control Function

RCEF: Resource Control and Enforcement Function

RSVP: Resource Reservation Protocol

SGSN: Serving GPRS Support Node

SIP: Session Initiation Protocol

SNI: Service to Network Interface

SOA: Service Oriented Architecture

SOAP: Simple Object Application Protocol

SPDF: Service Policy Decision Function

TISPAN: Telecom and Internet Services and Protocols for Advanced Networks (working group under ETSI)

UMTS: Universal Mobile Telecommunications System

UTRAN: UMTS Terrestrial Radio Access Network

WCDMA: Wideband Code Division Multiple Access

XML: Extended Markup Language