Solution Brochure

Juniper Networks Mobile Packet Core Solution

Intelligent, Secure and Open IP Infrastructure for Highly Reliable Mobile Packet Core Networks

Mobile Packet Core Solution Overview

With the tremendous increase in mobile subscribers and an accelerated growth in network traffic, service providers are faced with a need to expand their networks to offer new and enhanced voice, data and video services. These mobile broadband services will demand a lot from the network: lower latency, higher network intelligence, greater bandwidth, additional security, quality of service (QoS), differentiation and more third-party interworking, to name just a few. As mobile networks move towards 3G network standards, and the circuit-switched networks get replaced by packet-switched networks, many service providers are turning to IP/MPLS technology as a common core for existing and next-generation services. Juniper's IP/MPLS solution enables service providers to preserve their current investments in Asynchronous Transfer Mode (ATM), Frame Relay and time-division multiplexing (TDM) networks, while developing a building block for next-generation services.

Challenges

IP/MPLS has become the mainstream technology for network cores due to its future flexibility, network scalability, and a reduction in the cost of new service deployment. However, there are several challenging factors that an operator needs to consider while making this transition.

- The IP/MPLS packet core must have at least the same level of quality of service, resiliency and High Availability (HA) as that of the existing TDM infrastructure. The operations and management of the network should meet existing Telco standards.
- It should protect investments in the traditional ATM, Frame Relay and TDM networks while offering an evolutionary path to Third-Generation Partnership Project (3GPP) and 3GPP2-enabled networks.
- Service providers should not only see a significant reduction in expenditure with this common multiservice core, but also a good addition to top-line growth due to faster introduction of new multimedia services.
- The IP/MPLS core should be open to evolving architectures such as WiMAX, full IP radio access network (RAN) and Long Term Evolution (LTE).
- The IP/MPLS packet core network should enable the service provider to effectively share revenue from content and media.
- As mobile services transition to IP, new security concerns must be addressed. Both users and services must be protected against threats previously known only in the public Internet.
- With IPv6 playing an important role in the end-to-end addressing of the new multimedia environments in IP Multimedia Subsystem and Fixed Mobile Convergence (IMS-FMC), MPLS should support a seamless integration of IPv6 with minimal network impact.
- IP/MPLS plug-and-play technology for intelligent and dynamic traffic engineering should fulfill the promise of a network running itself, leading to significant savings in operating costs.

Trends

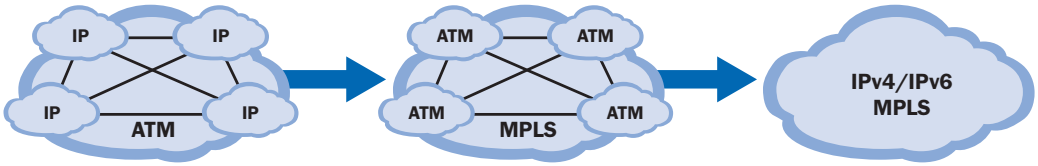

Figure 1: Mobile Operator Evolution to an IP/MPLS Mobile Packet Core

According to Analysys Research, mobile operator voice Average Revenue Per User (ARPU) in mature markets is down 5-15 percent over the past three years. To offset declining voice ARPU, service providers are offering new data services which are quickly increasing data ARPU. Data ARPU for most service providers now represents more than 10 percent of their total ARPU, and some service providers including NTT DoCoMo and China Mobile reportedly receive more than 20 percent of their ARPU from data services.

Juniper Networks Solution Portfolio for the Mobile Packet Core

For years, Juniper Networks has been helping wireless and wireline service providers evolve to a secure, converged IP infrastructure. Juniper products for service providers feature industry-leading IP expertise for intelligent and dependable mobile packet core networks, comprehensive and proven security, authorization and authentication, and open and scalable solutions to enable a flexible IP/MPLS core. In fact, 11 of the top 12 mobile service providers already employ Juniper's mobile solutions, and our products have been deployed in over 100 mobile networks worldwide.

Features and Benefits

Juniper enables mobile service providers to build more cost-effective, flexible and scalable networks based on a common IP/MPLS infrastructure in order to increase overall profitability by:

- Allowing new, higher margin services to be introduced more economically, rapidly and flexibly than before.
- Reducing operating expenses associated with managing multiple networks and dependencies on different technologies.
- Deploying one operating system—JUNOS software—with a single code source and single implementation of features across the entire IP/MPLS infrastructure. JUNOS software offers an important means for service providers to streamline both support and operating costs.
- Leveraging existing investments to create bundled services.
- Providing a comprehensive VPN solution to integrate traditional technologies like ATM, Frame Relay and TDM.
- Maintaining a single AAA system for all users regardless of what network resources they use.
- Minimizing the security, reliability and scalability risks associated with traditional IP networks.
- Offering QoS and prioritization of traffic that enables service providers to partner with rich content/media providers to effectively share revenue from content/media services.

This flexible, service-oriented network infrastructure is "future-proof" in that it is built to adapt easily as technologies evolve, enabling service providers to deliver a sustainable set of innovative and secure services now and into the future.

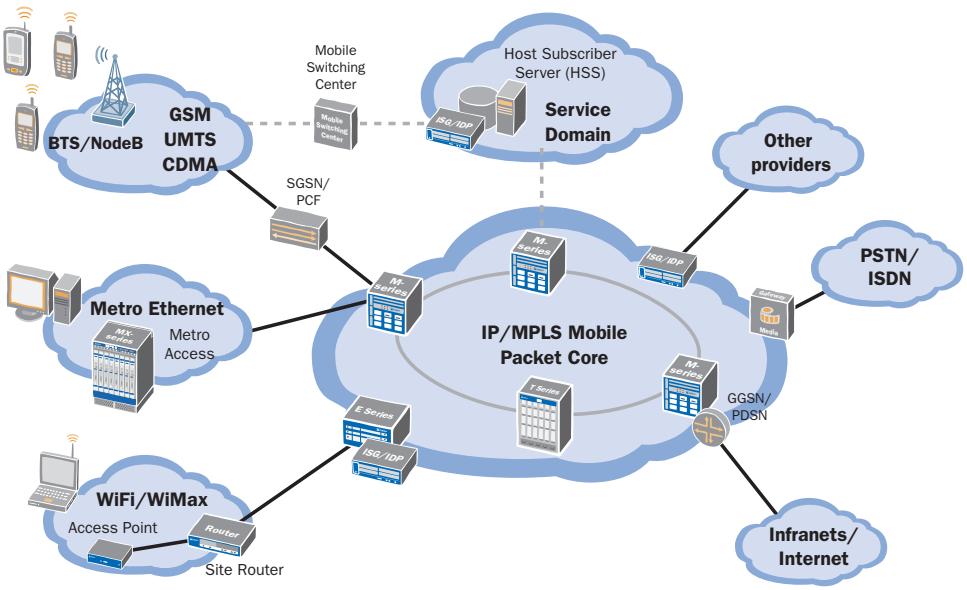

Figure 2: Juniper Enables Service Providers to Build an Intelligent, Secure and Open Mobile Packet Core

Juniper works closely with strategic partners to integrate our products into joint solutions designed to address the key challenges facing service providers as they migrate from circuit-switched technologies, from the introduction of mobile soft switching through the deployment of IP transport and the evolution to 3GPP, 3GPP2 and ETSI/TISPAN architectures. By employing open, standards-based interfaces, Juniper ensures compatibility not only with products from existing strategic partners, but also with new partner products and those offered by third-party equipment providers.

Carrier-Class Transport Infrastructure

Juniper routers built on IP/MPLS technology have made it possible to build packet networks that meet or exceed even the most stringent service provider requirements and can truly be considered telecom-grade. Such carrier-class networks depend on an intelligent, secure and open IP/MPLS infrastructure that integrates the transport of ATM and Frame Relay traffic into a multiservice mobile packet core network, while maintaining the quality associated with ATM and Frame Relay connectivity. Juniper's mobile packet core solution enables convergence of disparate networks via Layer 2 and Layer 3 VPNs, supports real-time data, makes mobile packet voice a reality, and enables other latency-sensitive IP applications such as IP signaling, gaming and mobile video.

Intelligent and Highly Reliable Mobile Networks

Juniper brings industry-leading IP expertise for intelligent and highly reliable mobile packet core networks, delivering 99.999 percent availability as measured by Telcordia. An IP/MPLS network enabled by Juniper Networks equipment supports voice, video and other real-time traffic by providing low-latency, low-jitter transport, and line rate forwarding under all conditions. Our industry-leading IP/MPLS feature set provides robust network management that includes auto-bandwidth, VPN support, traffic engineering and management, and failure detection.

High Availability Benefits

- Resilient VPN connectivity ensures that no calls are dropped, even when a failure occurs.
- Dynamic routing survives failures by automatically finding alternate routes to ensure IP telephony system availability.
- Automatic Protection Switching (APS) and Bidirectional Forwarding Detection (BFD), together with MPLS fast reroute (FRR), provide sub-second link restoration to ensure that voice calls are not interrupted if a transmission link or intermediate router fails.
- Redundant forwarding plane elements include duplicated switch matrix to maintain superior performance, even in the event of a failure.
- Nonstop routing (NSR) gives the ability of routing protocols to restart without the help of neighbors.
- Modularity of the JUNOS software, with each process running in a protected memory space, enables restarting without interruption to the other processes. Graceful Restart (GR) ensures that no data is lost during this restart.
- In Service Software Upgrades (ISSU) allows an upgrade to the JUNOS software image without having to take the router or network out of service.

Juniper Networks also makes dimensioning the IP/MPLS core far simpler since every interface can operate at full speed, whatever the traffic mix and conditions. Juniper routers achieve this through the extensive use of ASIC technology in the traffic forwarding plane, redundant switch matrix, a separate duplicated control plane (for route calculation purposes), and dedicated modules for advanced services such as IPSec security, Real-time Transport Protocol (RTP) compression or Legal Intercept. The result is a non-blocking architecture with very predictable throughput to meet the requirements of real-time voice traffic.

Quality of Service and Traffic Engineering

In order to provide telecom quality service, an IP/MPLS mobile packet core network must be capable of providing the service-level agreement (SLA) guarantees on delay-sensitive voice applications under any congestion conditions. Voice applications must meet all end-to-end SLA requirements of bandwidth, delay and jitter.

MPLS provides the ability to partition traffic and resources using VPN techniques. Packets entering the ingress routers in the network are classified and marked with identifiable DiffServ Code Points (DSCP). This classification is honored throughout the network on a per-hop basis, allowing delay-sensitive data such as voice to be given preferential treatment over other traffic. The other queues are not starved, however, and receive a proportion of the scheduler. Additionally, using techniques such as Weighted Random Early Detection (WRED), congestion can be avoided before it happens by slowing down the lower priority TCP connections. The Juniper DiffServ architecture accommodates the four user traffic profiles defined by 3GPP and 3GPP2, along with any additional signaling and management traffic in the network

IP/MPLS Traffic Engineering (TE) enables the network to compute the most desirable path from one node to another that meets all constraints of bandwidth and delay. MPLS TE increases network availability and QoS for the various traffic types by intelligently re-directing traffic over the core in the event of failures.

Performance Benefits

- Ensures that voice gets appropriate priority on the data network to deliver superior IP telephony application performance.
- Increases network efficiency by compressing voice packet headers over the WAN.
- ASIC-based hardware acceleration provides low-latency, low-jitter, HA packet transport for high quality voice, video and other real-time services.
- Dynamic QoS supports mission-critical voice and multimedia services as easily as best-effort Internet access.

Example of Mobile Network Traffic Classification by Type

Payload Type	Per Hop Behavior	Characteristics	Queue Settings
Routing and MPLS Protocols	NC or CSC	Network Control traffic	Small fixed bandwidth
Voice and CS data traffic	EF	Expedited Forwarding – high priority traffic with guaranteed minimum bit rate and low latency requirements	Strict high priority queue
SS7 signaling, GTP-C	AF11	Assured Forwarding – a group of per-hop behavior PHBs with forwarding assurance, providing differentiated precedence and loss probability Second Digit after AF defines the drop priority	Queue with guaranteed bandwidth (different priority settings)
PS Streaming	AF12		
Available for non-mobile traffic classes	AF2[1..3]		
	AF3[1..3]		
	AF4[1..3]		
O&M (background)	BE	Software upgrades, bulk File Transfer Protocol (FTP) of statistics	Best-effort queue
O&M (high priority)	AF11	Configuration management, traps, alerts, SSH	Queue with guaranteed bandwidth (different priority settings)
PS Interactive best-effort	BE	Best-effort traffic	Best-effort queue

MPLS Plug-and-Play

Plug-and-play is a very important concept that Juniper has taken from the LAN world and applied to MPLS networks to significantly reduce the configuration burden in the network. The notion of plug-and-play has contributed to Ethernet's success and Juniper believes that the benefits of plug-and-play can be achieved by adapting it to different technologies. Juniper's implementation of MPLS plug-and-play builds on three key concepts: intelligent routers, unnumbered interfaces, and script automation. This collection of techniques for provisioning infrastructure is designed to reduce the configuration burden, bring a greater degree of order and meaning to the network, and reduce the probability for configuration errors. Juniper routers are intelligent enough to allow for most of the provisioning to take place in the network, and in a Juniper routed environment, much of it can be fully automated, removing complex device configuration and Operations Support Systems (OSS) configuration requirements.

Juniper Networks provides industry-leading intelligent and dynamic traffic-engineering tools to service providers to allow automatic congestion control and low-latency path tracking. Some of the key benefits of this feature are:

- Automatic (pre-configured) running of protocols on each interface
- Automatic assignment of interface "addresses" and other forwarding information (labels)
- Auto-discovery of VPN endpoints (IP, pseudowire, virtual private LAN service-VPLS)
- Auto-discovery of multicast sources and receivers
- Automatic enforcement of security policies
- Auto-mesh and auto-bandwidth for RSVP-TE
- Automatic protection of links and/or nodes

Deployment Models

There are two types of deployment scenarios proposed by Juniper Networks for the 3GPPP environments. The first model shown below in Figure 3 is known as the "Provider Edge (PE)" model and has a simplified architecture for service providers that are building an IP/MPLS core primarily for voice. The reduced network elements have the advantage of a lower CAPEX and simplified network management. However, there is a lack of administrative granularity due to the absence of a clear separation between the LAN and WAN segments in the network.

The MX routers are used as PE devices, providing connectivity to all of the Mobile Network elements on the LAN side (that is, all nodes within the MSS environment), and a full IP/MPLS feature on the core side.

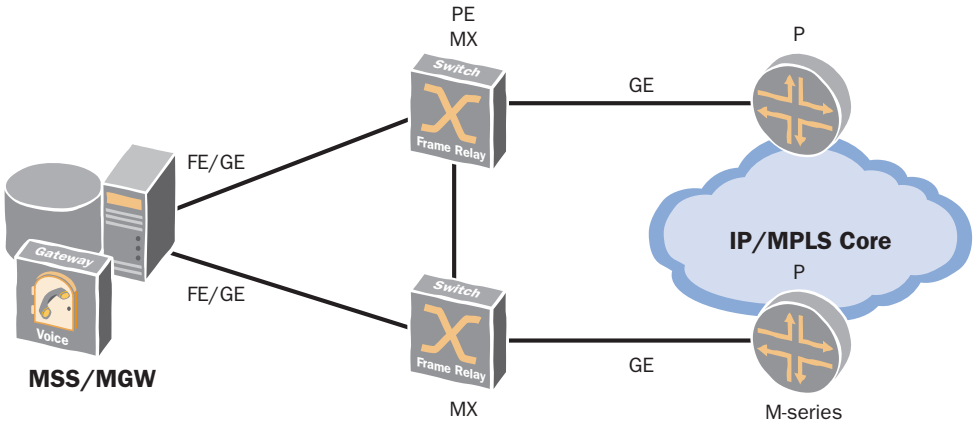

Figure 3: The Juniper PE Model

The second model shown below in Figure 4 is known as the "Customer Edge (CE)" model and has a clear differentiation between the LAN and WAN segments. This provides for better operational flexibility due to the separation of the site switches which connect the various network elements to the MPLS edge boxes. This model is best suited for situations where different organizations are responsible for the site connectivity and WAN, or for service providers that already have a multipurpose IP/MPLS core. The increased number of network elements carries with it the disadvantage of a higher CAPEX and extra management. In this model, the MX-series routers are used as CE devices and, depending on the connectivity type, the PE devices are either MX- or M-series routers.

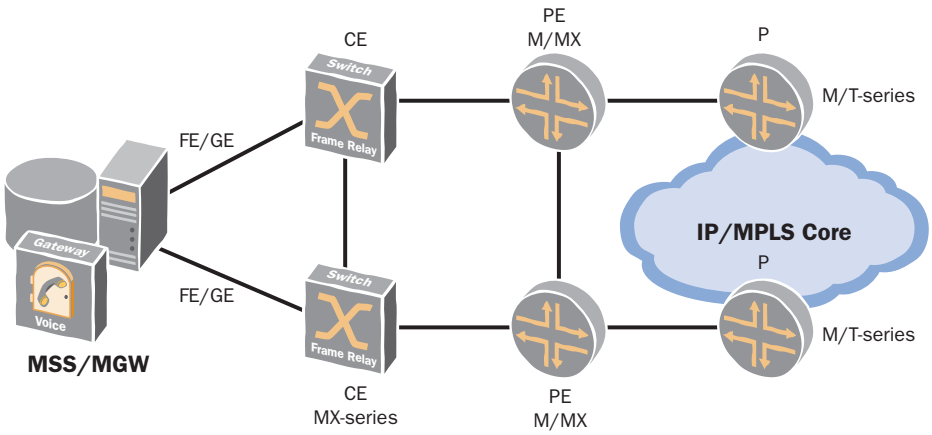

Figure 4: The Juniper CE Model

Comprehensive and Proven Security for Mobile Networks

Since the consequences of, for example, a Distributed Denial of Service (DDoS) attack are so great—potentially interrupting thousands of voice calls and other high revenue and critical services—it is essential that DoS security be provided at all layers of the mobile network, from the network layer to the application layer. Application-level threats (viruses, hacking, vulnerability exploits) against user devices and threats to infrastructure operating systems must also be mitigated. In addition, session-based data and multimedia applications and services mix different access types (WiFi, WiMAX, cable, DSL and others), making cross-network session awareness and session-protection crucial.

Juniper Networks mobile packet core network solutions include pervasive security that protects the infrastructure as well as applications. As an industry leader with a full range of security products, Juniper secures 23 of the world's top 30 mobile service provider networks and protects 8 of the top 12 mobile networks from General Packet Radio Service (GPRS) attacks. Our best-in-class network security is designed to handle voice as well as data traffic, to secure converged networks, and to protect Global System for Mobile Communications (GSM)/GPRS and Code Division Multiple Access (CDMA) network interfaces. Our security platforms also include support for new protocols such as GPRS tunneling protocol (GTP), SIGTRAN, and Session Initiation Protocol (SIP).

In addition to dedicated security appliances such as the Juniper Networks Integrated Security Gateway 2000 (ISG 2000), Juniper routers are also hardened against attacks. Features such as line rate packet filtering, unicast Reverse Forwarding Path (uRPF), flow monitoring and IPSec VPNs are all available in our router product family.

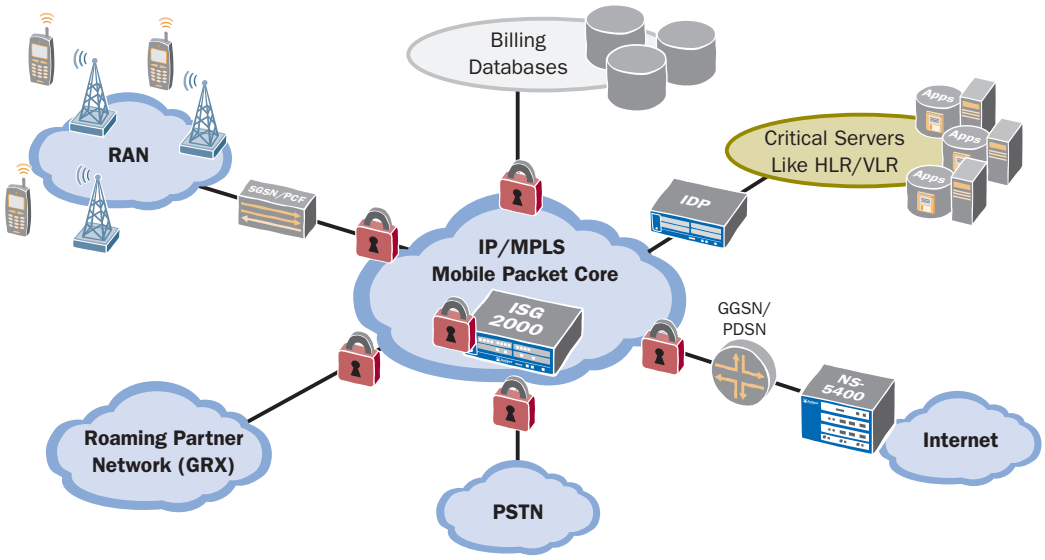

Figure 5: Juniper Networks Provides Comprehensive Security for the Entire Mobile Operator Network

Table 2 summarizes some of the security features that Juniper Networks offers for securing mobile operator networks:

Table 2: Securing Wireless Operator Networks

Security Feature	Benefit
Detects and thwarts attacks on Gi, Gp, Ga, Gn interfaces	Increased service uptime
Overbilling attack protection	Satisfied customers and operator revenue protection
Security for traffic to roaming partners	Enhanced roaming solution offering, seamless service
Virtualization support	Built for Mobile Virtual Network Operator (MVNO) support to lower CAPEX
Deep Inspection, antivirus, and firewall support on Gi interface	Quickly complete trial and deploy new services with full confidence in the security of your network

Next-Generation Mobile Networks

Looking to the future of network evolution, the introduction of the IP Multimedia Subsystem (IMS) and Fixed Mobile Convergence (FMC) as a service enabler will demand an intelligent, secure and open IP/MPLS core network. And the evolution towards mobile broadband technologies like HSPA (High Speed Packet Access), Long Term Evolution (LTE) and WiMAX will further increase the demand for a high capacity, highly reliable IP core network.

IPv6 over G-MPLS

IPv6 will be a key technology for next-generation networks. It will provide the end-to-end addressing requirements of IMS-FMC needed by the new multimedia environments for mobile devices and residential VoIP. With Generalized MPLS (G-MPLS) running in the mobile packet core, IPv6 can be enabled as another service without having an impact on the core of the network—no software/hardware upgrades, configuration changes or degradation in performance of the other services. Juniper offers key features to support 6PE and 6VPE for IPv6 transport over a G-MPLS core.

Optical Transport with G-MPLS

The widespread deployment of dense wavelength-division multiplexing (DWDM)-based optical transport systems in the core network, to satisfy the tremendous need and increase in capacity demand, has led network planners to reconsider traditional approaches to provisioning and network restoration, and plan integration of the optical layer into the MPLS infrastructure.

G-MPLS has emerged as a next-generation networking protocol for providing an intelligent optical control plane for optical networks. G-MPLS is considered a superset of MPLS, as it extends the forwarding and control planes to include not only packet-based and cell-based, but also synchronous optical network (SONET), DWDM, and fiber-based network elements.

Juniper's mobile packet core network solutions do more than just build an infrastructure for your current needs. They create a future-proof infrastructure that supports seamless migration to emerging IMS-FMC applications. Because our solutions are fully compliant with standards issued by major groups such as 3GPP and 3GPP2, they will enable you to evolve your network as next-generation architectures continue to develop.

Summary—Juniper's Intelligent, Secure and Open Mobile Core Solution

Service provider networks are multi-vendor environments, making agility and adherence to open standards critical factors. To realize the full benefits and value of using MPLS, service providers must be able to manage the delivery, availability and performance of the MPLS network, and this adds new challenges for traditional network management tools.

Juniper is committed to non-proprietary and open standards as defined by Internet Engineering Task Force (IETF), International Telecommunication Union Telecommunication Standardization (ITU-T), Third-Generation Partnership Project (3GPP & 3GPP2), ETSI/TISPAN, and other standards groups. Standards-based interfaces that leverage third-party open source solutions (OSS) make Juniper Networks routers easily manageable and rapidly deployable. We protect existing mobile operator ATM and Frame Relay infrastructure investments by providing graceful, standards-based migration to IP/MPLS—for example, through our support for Layer 2 and Layer 3 pseudowires and ATM to MPLS interworking.

Juniper Networks is the market leader in building flexible, service-oriented packet networks. Whether you are a GSM/GPRS operator, a CDMA operator, or even an Unlicensed Mobile Access (UMA) or WiFi/WiMAX service provider, an intelligent, secure and open IP/MPLS infrastructure with products from Juniper Networks will enable you to adapt easily as technologies evolve, allowing you to deliver a sustainable set of innovative and secure services today and into the future. To learn more, contact us today or visit http://www.juniper.net/wireless.

Table 3: Summary of Key Features for Juniper Networks Mobile Packet Core Solutions

Intelligent	Secure	Open
• Full MPLS feature set, including traffic engineering and management, failure detection and fast reroute • Sub-millisecond detection and recovery from IP link failures • QoS to prioritize traffic based on application and service requirements • IPv4 and IPv6 support over a common core • Monitors IP transport, dynamically adjusting policies to allow, prioritize and even block network traffic based on user, service and network demands • MPLS plug-and-play to reduce network configuration and complexity • 11 of the top 12 mobile networks are Juniper customers	• Provides protection for all points of the network • Protects assets from DoS, DDoS and other network attacks • Protects end users from viruses, worms and trojans • Protects traffic at transport layer via firewall and Deep Inspection techniques • Protects voice and other SIP-based traffic via policy enforcements, back-to-back user agent and topology hiding • Secures traffic of many types, including Stream Control Transmission Protocol (SCTP) and SIP • Protects control layer via SIP and H.323 application layer gateways (ALGs) • Protects SIP-based application servers and end users via Intrusion Detection and Prevention (IDP)	• Committed to non-proprietary and open standards as defined by IETF, ITU-T,3GPP, 3GPP2, ETSI/TISPAN and other major standards bodies • Industry-leading QoS, SLA, Call Admission Control (CAC) features enable various applications on the mobile core to help retain familiar ATM experiences for smoother evolutionary path to IP • Industry-leading IPv6 capabilities with IPv4 to IPv6 migration support • Toolkits that enable integration with partners and third-party vendors via open, standards-based interfaces such as DIAMETER, COPS, SOAP, and XML • Committed to developing cost-effective, flexible, best-in-class solutions in conjunction with strategic partners

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Juniper Your Net™

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.

150047-003 Feb 2008