ROUTER INTEGRATED APPLICATIONS

Service Overview

Service providers and enterprises offer an ever-increasing array of security, monitoring, voice, and video services. Unfortunately, each application and service is typically delivered using single service appliances, which creates significant network complexity and increases operational costs.

Juniper offers a portfolio of applications which run directly on Juniper's routing platforms. These router integrated applications ensure high service performance, resiliency, and scale, and they permit network consolidation by eliminating standalone appliances and the layers of management and administration needed to maintain them.

Product Description

Services and applications are typically delivered over the network using a combination of routers and a variety of appliances that host and monitor each service individually. In this model, service growth requires more appliances that inefficiently consume rack space and environmental resources such as power and cooling. Worse yet, adopting new services requires qualifying, integrating, and deploying new appliances in an expensive and time-consuming process that delays time to revenue. The end result is an inflexible and inefficient network environment where routers are surrounded by racks of service-specific appliances.

Juniper Networks overcomes the inefficiencies of appliance-based services with its Router Integrated Application portfolio. These applications are offered as optionally licensed software, and provide subscriber and service awareness, service monitoring, security, Network Address Translation (NAT) functions, application-layer load balancing, as well as a collection of link-layer services. These applications can be flexibly deployed on the Juniper Networks® MX Series 3D Universal Edge Routers, M Series Multiservice Edge Routers, and T Series Core Routers.

Juniper's router integrated application portfolio extends the value of Juniper Networks routers by flexibly and efficiently accommodating a wide range of applications while concurrently reducing or eliminating service-specific appliances and the layers of network and management complexity that they add, as well as related space and power requirements.

Architecture and Key Components

Router applications run directly on MX Series, M Series, and T Series routers. Router integrated applications are optionally licensed on these platforms via dedicated service cards, or DPCs that run the Trio chipset. Either approach ensures high performance, resiliency, and scale under all network conditions.

Service Cards

A variety of service cards are available for the MX Series, M Series, and T Series platforms. Multiple service cards are supported per routing platform to flexibly increase application performance, capacity, reliability, and scale.

Multiservices Dense Port Concentrator (MS-DPC)

The Multiservices DPC is a single slot service card that hosts applications on the Juniper Networks MX240, MX480, and MX960 3D Universal Edge Router. Each MS-DPC contains two Network Processing Units (NPUs), and each NPU can host the same or different applications as required.

Multiservices Physical Interface Card (MS-PIC)

The MS-PIC is a service PIC that hosts applications on the Juniper Networks M Series and T Series router platforms. A variety of MS-PICs are available for including versions compliant with Federal Information Processing Standards (FIPS).

- **MS-500**
  - The MS-500 works with Type 3 FPC.
- **MS-400**
  - The MS-400 works with Type 2 FPCs.
- **MS-100**
  - There are two versions of MS-100 service cards; each card works with Type 1 FPCs.

Trio-based MX Series 3D Universal Edge Routers and Modular Port Concentrators

A variety of router integrated applications are available 'inline'; that is, directly on Trio-chipset based MX Series products.

Inline services are available on the Trio chipset powered 16x10GbE DPC and Modular Port Concentrator, or MPC, for the MX240, MX480 and MX960. Additionally, the Trio chipset is built right into the Juniper Networks MX5, MX10, MX40, and MX80 3D Universal Edge Routers.

Product Options

Increase Efficiency with Compressed Real-Time Transport Protocol (CRTP)

CRTP compresses the 40-byte IP/UDP/RTP header down to two bytes, significantly reducing the overhead for small packets such as voice (typically 40-48 bytes depending on encoding scheme). By reducing packet headers to one-twentieth their original size, CRTP reduces the latency related to serialization, allowing service providers to offer VoIP services over low speed links. It also increases overall network resource efficiency.

Manage Resources with Dynamic Application Awareness

Dynamic Application Awareness uses packet inspection technology to enable the stateful detection, identification, and analysis of traffic on a per application basis. Dynamic Application Awareness enables differentiated services based on application criteria, ensures adherence to service-level agreements (SLAs), and maintains application fairness. Operationally, identifying layer traffic patterns and statistics supports capacity planning and service optimization activities.

Customize Services with Dynamic Subscriber Awareness

Dynamic Subscriber Awareness uses packet inspection technology and a subscriber database to enable the stateful detection, identification, and analysis of traffic on a per subscriber basis. This permits differentiated services based on subscriber policy, ensures adherence to SLAs, and enables subscriber/application fairness. Operationally, the identification of subscriber traffic patterns and statistics supports marketing and service optimization tasks.

Improve Security with IPsec Encryption

Juniper's IPsec encryption uses the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and triple Data Encryption Standard (3DES) to enable secure network communications. Enterprise customers can use IPsec to enhance end user security; while service provider's can use IPsec over third-party access links between the customer premise and their network edge, to add security to traffic over Layer 3 VPNs and to secure traffic transiting wholesale networks.

Protect the Network with Intrusion Prevention System (IPS)

Juniper Networks is a recognized leader in network security solutions, and our router integrated intrusion prevention system (IPS) provides comprehensive threat identification and mitigation from worms, trojans, spyware, and keyloggers. IPS increases network security and ensures continuous availability for business critical applications and services. Security statistics can be exported to reporting tools that support planning and forecasting activities.

Improve Operations Environment with J-Flow

J-Flow collects flow statistics which can be exported in standard cflowd v5, v8, and v9 flow record formats that are compatible with industry-standard flow collectors and applications. J-Flow can monitor traffic at the flow, department, or application level for customer billing or interdepartmental charge back purposes. It can also provide usage statistics for capacity and traffic engineering tasks or customer consulting services, and it can assist in tracking security violations.

Regulatory Compliance with Flow-Tap/Flow-Tap Lite, and Dynamic Flow Capture (DFC)

These applications intercept packets and forward copies to one or more content destinations based on filter criteria. Both applications offer access control via user classes and, importantly, filters do not add perceptible delay in the forwarding path, nor are filters installed by one user visible to others.

Boost Performance and Efficiency with Link Services

Link Services offer simultaneous support for enhanced multilink bundling and queuing, and link fragmentation and interleaving (LFI). Enhanced multilink features include End-to-End Multilink Frame Relay Implementation Agreement FRF.12, FRF.15, and FRF.16 support, which facilitate the efficient and cost-effective aggregation and bundling of Frame Relay links. Multilink Point-to-Point Protocol (MLPPP) support provides PPP over multiple discrete links such as N x T1/E1. Multiclass MLPPP is also supported to allow distinct quality of service (QoS) treatment of bundled MLPPP links.

LFI is an essential feature for latency sensitive services over low speed links, since it minimizes the delay and jitter that are characteristic of high payload packets. By breaking up large packets resulting from file transfers and interleaving smaller latency sensitive packets, serialization delay is minimized and overall service levels are significantly improved.

Add Scale and Security with Next-Generation Network Addressing Solutions and Carrier Grade NAT (CGN)

Juniper's NAT software supports static and dynamic address translation between private addresses and public IP addresses as well as Port Address Translation (PAT). A rich set of application-level gateways (ALGs) provides address translation for applications that have multiple flows (e.g., SIP, DNS, H.323, FTP, and ICMP), and class-of-service (CoS) support is made possible with rule-based DiffServ code point (DSCP) marking and forwarding class assignment.

Juniper Networks advanced CGN technologies help service providers thrive despite IPv4 address depletion (the IANA Global IPv4 address pool has been exhausted), and ensure coexistence and connectivity between IPv4 and IPv6 hosts and resources. Juniper supports a wide variety of CGN options, including DS-Lite, NAT 44(4), and NAT64, 6to4, and NAT-PT, providing a CGN toolbox that flexibly addresses the technical and business requirements of all types of service providers. Tunneling techniques such as 6rd are also supported.

Augment Security with Stateful Firewall

Juniper's stateful firewall software uses a per flow state table, IPv4/IPv6 packet inspection, and statistical modeling to identify, classify, count, and forward or filter packets on the data and/or control plane. The router integrated firewall can provide the first line of defense in a layered security architecture, efficiently offloading bulk stateful filtering from external firewalls in service provider and enterprise networks, or as a managed security service.

Video Monitoring and Analysis with StreamScope eRM

Service providers and cable operators can use StreamScope eRM to identify and isolate video quality issues at the Media Delivery Index (MDI) and MPEG layers, which reduces troubleshooting time and expensive truck rolls. StreamScope eRM was developed by Triveni Digital, a Juniper Technology Alliance partner and a recognized leader in advanced digital video solutions. Triveni Digital used the Junos SDK to integrate its video monitoring technology with Junos OS.

Monitoring IP, VPN, and VoIP Services with Telchemy ePM (TePM)

TePM provides comprehensive monitoring capabilities for a wide range of IP, VPN, and VoIP services in support of service planning, troubleshooting, and quality assurance. TePM was developed by Telchemy Inc., a Juniper Technology Alliance partner and a recognized leader in advanced VoIP monitoring solutions. Telchemy used the Junos SDK to integrate its technology with Junos OS.

Tunnel Services for Efficient Scale

Juniper's tunnel services software offers a variety of encapsulation schemes such as IP over IP, Physical Interface Module sparse mode (PIM SM), generic routing encapsulation (GRE), and L2TP network server (LNS). These encapsulation schemes ensure efficient traffic distribution and communications over a range of network architectures and protocols.

Features and Benefits

FEATURE	DESCRIPTION	BENEFITS
Router integrated applications	Service cards and the applications they host are directly supported on M Series and T Series routers.	· Investment protection in routers. · Lower OpEx bv reducing the space, power, and cooling resources consumed by appliances. · Reduce design complexity associated with appliance interconnect and port mirroring to external probes.
Service flexibility	Service cards host the optionally licensed Junos OS application software portfolio.	· Apply services to any flow over any interface. · Group applications to address unique requirements where and when needed.
Service performance and scale	Service cards provide dedicated service processing, and scale is easily supported by adding service cards.	· Deploy applications where and when wanted. · Lower service start-up costs and cost-effectively scale services as needed. · Decouples service capacity from the network interface—apply service to any flow in router. · No additional equipment or cabling is required.
High availability (HA)	Multiple redundancy schemes are supported.	· Increased service resiliency and uptime. · Select level of redundancy to fit needs.
Consistent operations and administration	Multiple configuration and management options are available. Single service card architecture supports all services (cards are NOT service specific).	· Junos OS command-line interface (the same CLI that supports the MX Series) is used to configure all service card supported applications, including those developed by partners. · Juniper Networks Junos® Space applications can also be utilized. · Simplifies sparing and maintenance tasks.
Next-generation network addressing and CGN	Rich support for IPv6 coexistence transition and IPv4 depletion mitigation tools, including DS-Lite and NAT44(4), as well as 6rd.	· Avoid IPv4 address exhaustion while maintaining current architecture. · Enables IPv4/IPv6 coexistence. · Line rate IPv6 performance. · High CGN capacity per platform. · Toolbox approach flexibly accommodates varied technical and business requirements.
CRTP	Compresses IP/UDP/RTP headers.	· Provides highly efficient VoIP services. · Reduces VoIP latency over low speed links.
Dynamic Application Awareness	Identifies traffic on a per application basis.	· Enable differentiated services. · Ensure adherence to SLAs. · Improve operational environment. · Control and direct traffic over network based on application layer information. · Collects statistics on a per application basis in support of operations tasks.
Dynamic Subscriber Awareness	Identifies traffic on a per subscriber basis.	· Enable differentiated services. · Ensure adherence to SLAs. · Control and direct traffic over network based on subscriber identity and privileges. · Collects statistics on a per subscriber and per application basis in support of operations tasks.
J-Flow monitoring[1]	Identifies traffic on a per subscriber basis.	· Enable SLA accounting and charge backs. · Improve capacity and traffic planning activities. · Supports consulting services. · Track security violations. · Compatible with standard flow collectors.
Flow-tap and dynamic flow capture	Collects flow statistics for export in standard v5, v8, and v9 flow records.	· Flexible deployment models. · Increases security threat detection. · For Communications Assistance for Law Enforcement Act (CALEA) support, filtering doesn't add perceptible service delay and filters installed by a user are invisible to others.

[1]J-Flow cflowd v10 is available directly on Trio-based Dense Port Concentrator cards (DPCs) for the MX Series 3D Universal Edge Routers.

Features and Benefits (continued)

FEATURE	DESCRIPTION	BENEFITS
IPS	Identifies and mitigates network threats.	• Improve network and control plane security. • Increase service availability by blocking worms, trojans, spyware, keyloggers, and other threats. • Collect comprehensive statistics for security management, planning, and reporting tools.
IPsec encryption	Support for AES, DES, and 3DES.	• Enhance end user security. • Improve security over access links and wholesale networks.
Link Services	Simultaneous support for enhanced multilink bundling and queuing, and link fragmentation and interleaving (LFI).	• Efficient Frame Relay aggregation. • Enables bundled Point-to-Point Protocol (PPP) transport over multiple discrete links with QoS treatment per link. • Provides highly efficient multiplay service delivery without sacrificing QoS.
Stateful firewall	Identify, classify, count, and forward or filter packets on the data and/or control plane based on policy.	• Extend firewall to H.323, FTP, Session Initiation Protocol (SIP), and Internet Control Message Protocol (ICMP). • Help layer defenses by efficiently offloading bulk stateful filtering from external firewalls. • Underpin managed security service.
StreamScope eRM	Proactively identifies and isolates digital television (DTV) faults through the comprehensive analysis of both IP layer packets and MPEG layer streams.	• Comprehensive multilayer analysis and real-time video QoS score based on service quality and deviation from standards and norm. • Ability to identify and filter impairments by severity focuses troubleshooting efforts. • MX Series routers can take automated actions based on StreamScope eRM triggers. • Scales to support over 800 standard definition channels using 200+ video quality rules.
Telchemy ePM	Provides comprehensive, router integrated active IP, VPN, and VoIP service monitoring and troubleshooting capabilities.	• Improve service monitoring and planning. • Employ advanced troubleshooting tools. • Maintain IP, VPN, and VoIP service quality.
Tunnel services	Supports a wide variety of encapsulation mechanisms, including IP over IP, PIM SM, and GRE.	• Transport L3 VPNs in non-MPLS networks. • Virtual private LAN service (VPLS) support via virtual tunnel interfaces. • LNS tunnel termination for L2TP clients.

Specifications

MS-DPC and MS-PIC Certifications and Approvals

Safety

- CAN/CSA-C22.2 No. 60950-00/UL 60950 (Third Edition)
- Safety of Information Technology Equipment
- EN 60950, Safety of Information Technology Equipment

Certifications

- FIPS 140-2 Level 1 certification
- Stateful firewall - ICSA certified

Electromagnetic

- EMC AS / NZS 3548 Class A (Australia/New Zealand)
- BSMI Class A (Taiwan)
- EN 55022 Class A Emissions (Europe)
- FCC Part 15 Class A (USA)
- VCCI Class A (Japan)
- Immunity EN-61000-3-2 Power Line Harmonics
- EN-61000-4-2 ESD

Electromagnetic (continued)

- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

Network Equipment Building System (NEBS)

- GR-63-CORE; NEBS, Physical Protection
- GR-1089-CORE; EMC and Electrical Safety for Network Telecommunications Equipment
- SR-3580 NEBS Criteria Levels (Level 3 Compliance)

European Telecommunications Standardization Institute (ETSI)

- ETS-300386-2 Telecommunications Network Equipment Electromagnetic Compatibility Requirements

Application Software Specifications

CRTP

- CRTP (RFC 2508)

Dynamic Application Awareness

- Dynamically redirects new flows to subscriber database
- Uses deep packet inspection, signature database, and well known addresses and ports to identify applications associated with a flow
- Configures forwarding plane to take an action on packets (forward or drop, rate limit, mark) associated with the flow based on policy
- Collects statistics on a per application basis in support of operational tasks
- Can be deployed upstream from a Broadband Network Gateway (BNG) or gateway GPRS support node (GGSN), or in conjunction with Dynamic Subscriber Awareness to correlate application usage with subscriber information

Dynamic Subscriber Awareness

- Dynamically redirects new flows to subscriber database
- Checks subscriber ID against policy database
- Configures forwarding plane to forward, rate limit, mark, or drop packets associated with flow based on policy
- Can be used in conjunction with Dynamic Subscriber Awareness to correlate application usage with subscriber information

Flow monitoring and accounting[1]

- cflowd v5
- cflowd v8
- cflowd v9

Intrusion prevention system (IPS)

- Anomaly-based attack detection
- Active and expired flow recording
- System logging
- SYN-cookie activation
- Attack detection mechanisms include application signature support for 100Bao, Aimstar, Applejuice, Ares, BitTorrent, DirectConnect, eDonkey2000, FastTrack, Freenet, GoBoogy, GnucleusLAN, Gnutella, Gnutella2, HotLine, ICQ, IRC, Jabber/XMPP, Joltid PeerEnabler, Kademlia, KuGoo, Kuro, MMS, MSNPv10, MSNPv11, MSNPv12, MSNPv13, Mute, Napster, Oscar (AOL), OpenFT (giFT), Poco, QQ, Real-Time Streaming Protocol (RTSP), SCTP, Skybe, Soribada, Telsa, TOC (AOL) WinNY, WPNP, Yahoo IM, Peercast, IceShare, Freecast, Soulseel, Xunlei, and many others.

IPsec encryption

- Encryption Algorithms (RFC 2405, RFC 2410)
  - AES (128, 192, and 256 bit)
  - 3DES
  - DES
  - Null
- Authentication Hash Algorithms (RFC 2403, RFC 2404)
  - Message Digest 5 (MD5)
  - SHA-1
  - Fully qualified domain name (FQDN)
  - IPv6 for IPsec (RFC 2460)
- Internet Key Exchange (IKE) Modes
  - Main/aggressive mode supported for IKE security association (SA) setup
  - Quick mode supported for IPsec SA setup
  - Digital certificates (X.509) VeriSign
  - Entrust

Link Services

- Multilink support
  - MLPPP (RFC 1990)
  - MCMLPPP (RFC 2686)
  - MLFR (FRF.15)
  - MLFR (FRF.16)
- LFI protocol support
  - LFI over PPP (RFC-1990)
- LFI over MLPPP bundles
  - FRF.12 via FRF.15 encapsulation

NAT and Carrier Grade NAT

- RFC2663 – NAT44 and NAPT44
- RFC4787 – UDP Behave
- RFC5382 – TCP Behave
- RFC5508 – ICMP Behave
- RFC6146 – Stateful NAT64
- RFC5969 – 6rd
- Draft-ietf-softwire-dual-stack-lite – DS-Lite
- RFC2766 – NAT-PT
- RFC3056 6to4
- Draft-kuarsingh-v6ops-6to4-provider-managed-tunnel – 6to4-PMT
- Draft-ietf-behave-lsn-requirements – Common requirements for CGN devices

Stateful firewall

- Stateful packet filtering
- Checks for the packets in IP stack
- Assists in the detection of denial-of-service (DoS) attacks
- Firewall for inter-VPN traffic
- TCP intercept, flow, and session limits
- Stateful Firewall/NAT ALGs include BOOTP, DCE RPC and DCE RPC portmap, Exec, FTP, H.323, ICMP, IIOP, login, NetBIOS, NetShow, RealAudio, RPC and RPC portmap, RTSP, shell, SNMP, SQLNet, Trivial File Transfer Protocol (TFTP), traceroute, WinFrame, and SIP

StreamScope eRM

- Media Delivery Index (MDI) IETF RFC 4445, including MDI DF:MLR values and overall byte count
- SNMP, RFC 1067
- MPEG 2 encoding using MPEG 2 transport streams
- MPEG 4/H.264/AVC encoding using MPEG 2 transport streams
- MPEG 4/H.264/AVC encoding using Real-Time Transport Protocol (RTP) transport
- MPEG layer analysis includes:
  - Flow identification, including SA/DA, ports, RTP source, and interface index
  - MPEG2 PID data, including packet counts, type (video, audio, SCTE 35), and buffer analysis
  - MPEG2 program information, including total packet count and peak cell rate (PCR) analysis data
  - MPEG2 table sections along with reception statistics
  - Program Service Information (PSI) with PAT and program path maximum transmission (PMT)
  - Digital Video Broadcasting/Service Information (DVB/SI) tables
- Monitors Advanced Television Systems Committee (ATSC) and ATSC A/78 transport stream verification, including ATSC Program and System Information Protocol (PSIP) tables
- SCTE-142 Recommended Practice for Transport Stream Verification

StreamScope eRM (continued)

- SCTE18 EAS which defines an Emergency Alert Signaling for cable TV systems
- SCTE35 Digital Program Insertion (DPI) tables, enabling monitoring of targeted advertisements
- Full analysis performed according to ETR 101 290 specification

TePM voice and IP monitoring

- VoIP test call generation to other TePM Agents and standard-based SIP endpoints
- RTP stream generation according to RFC3550
- Real-Time Transport Control Protocol SR/RR (RFC3550) and RTCP XR VoIP (RFC3611)
- 10, 20, 30 ms packet intervals (up to 100 ms for some tests)
- Selectable pre-encoded payloads for G.711, G.729A codecs
- "Thin call" option with zero length payload
- Call setup using SIP signaling
- Measurement of incoming RTP stream
- Inserts packet impairments into outgoing stream, including independent and bursty packet loss
- Generation of multiple concurrent streams
- Configurable minimum and maximum call duration and inter-call time interval
- Integrated UDP traceroute function to detect route followed by call
- Network application test capabilities for synthetic network application transaction generation
- Dynamic Host Configuration Protocol (DHCP) availability and response time tests
- Domain Name System (DNS) availability and response time tests
- HTTP availability and response time tests
- Point of presence (POP) availability and response time tests
- SMTP availability and response time tests
- Reports availability and performance per application layer (IP, UDP/TCP, session, transaction)
- Identification of the layer at which performance failure occurs
- Network testing capabilities for IP addressable devices such as a server or router
- Ping and traceroute
- Hop-by-hop tests, with congestion detection, duplex mismatch detection, and available bandwidth estimation results

Tunnel services and LNS

- GRE, including enhanced functions such as pre-fragmentation, key stamping, and verification
- IP-IP
- PIM-SM, PIM-SIM-DM
- Virtual tunnel interfaces
- Multicast tunnel interfaces
- L2TP Network Server (LNS)
  - Interface to authentication, authorization, and accounting (AAA) system (RADIUS)
  - PPP and L2TP termination
  - Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) for authentication
  - Terminates L2TP into VPN routing and forwarding tables (VRFs)

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services.**

Ordering Information

Service Cards for M Series and T Series Platforms

MODEL NUMBER	DESCRIPTION
Multiservices PICs	
PE-MS-100-1	Multiservices PIC Type 1 with 1 Gbps DRAM for the M7i and M10i
PE-MS-100-1-FIPS	Multiservices PIC Type 1 with 1 Gbps DRAM, FIPS version for the M7i and M10i
PB-MS-100-1	Multiservices PIC Type 1 with 1 Gbps DRAM for the M40e, M120, M320, T320, T640, and T160
PB-MS-100-1-FIPS	Multiservices PIC Type 1 with 1 Gbps DRAM, FIPS version for the M40e, M120, M160, and M320
PB-MS-400-2	Multiservices PIC Type 2 with 2 Gbps DRAM for the M40e, M120, M320, T320, T640, and T1600
PB-MS-400-2-FIPS	Multiservices PIC Type 2 with 2 Gbps DRAM, FIPS version for the M40e, M120, M160, and M320
PC-MS-500-3	Multiservices PIC Type 3 with 3.5 Gbps DRAM for the M120, M320, T320, T640, and T1600
PC-MS-500-3-FIPS	Multiservices PIC Type 3 with 3.5 Gbps DRAM for the M40e, M120, M160, and M320

Junos OS Application Software

MODEL NUMBER	DESCRIPTION
Compressed Real-Time Protocol	
S-CRTP	CRTP license (requires MS-PIC for the M7i, M10i, M40e, M120, M320, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
Dynamic Application Awareness	
S-ATO	Application Traffic Optimization service license for policy enforcement and application statistics; license includes deep packet inspection and policy mechanisms (requires MS-PIC for the M120 and M320, or the MS-DPC for the MX240, MX480, and MX960)
Dynamic Subscriber Awareness	
S-PTSP	Dynamic Subscriber Awareness license based on packet trigger subscriber policy (PTSP) (requires MS-DPC for the MX240, MX480, and MX960)
Intrusion Prevention System	
S-IDP	IPS license for intrusion prevention software with policy enforcement (requires MS-PIC 400 or MS-PIC 500 for M120 and M320 or the MS-DPC for the MX240, MX480, and MX960)
Flow-Tap, Flow-Tap Lite, and Dynamic Flow Capture	
S-DFC-100K[2]	Dynamic Flow Capture software license (requires MS-PIC for the M320, T640, T320, and T1600)
S-SFM-FLOWTAP-IN	Software license for secure flow mirroring service—MX Series only

MODEL NUMBER	DESCRIPTION
J-Flow	
S-ACCT	J-Flow license (requires MS-PIC for the M7i, M10i, M40e, M120, M320, T320, T640, and T1600 or MS-DPC for MX240, MX480, and MX960)
S-ACCT-5M	J-Flow license for up to 5 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-10M-UPG	J-Flow license upgrade from 5 to 10 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-10M	J-Flow license for up to 10 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-15M-UPG	J-Flow license upgrade from 10 to 15 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-15M	J-Flow license for up to 15 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-20M-UPG	Upgrade from 15 to 20 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-20M	J-Flow license for up to 20 million flows (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-25M-UPG	Upgrade from 20 to 25 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-25M	J-Flow license for up to 25 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-30M-UPG	Upgrade from 25 to 30 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-30M	J-Flow license for up to 30 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-35M-UPG	Upgrade from 30 to 35 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-35M	J-Flow license for up to 35 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-40M-UPG	Upgrade from 35 to 40 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-40M	J-Flow license for up to 40 million flows for MX Series routers (requires MS-DPC for MX240, MX480, and MX960)
S-ACCT-JFLOW-CHASSIS	Chassis-wide J-Flow software license (requires MPC or MS-DPC on MX960 router)
S-ACCT-JFLOW-IN	Software license for in-line J-Flow on MPCs for the MX240, MX480, and MX960
S-ACCT-JFLOW-IN-10G	Software license for 10 Gbps of J-Flow traffic (requires an MPC on MX80 routers)
S-ACCT-JFLOW-IN-5G	Software license for 5 Gbps of J-Flow traffic (requires an MPC on MX80 routers)

[2]DFC license does not require MS-DPC for chassis-based MX Series routers.

MODEL NUMBER	DESCRIPTION
J-Flow (continued)	
S-COLLECTOR-100K	Software license for passive monitoring flow collector application supporting 100,000 packets per second (100,000 pps) throughput for the M320, T640, T320, and T1600
S-MONITOR-1M	Software license for passive monitoring for J-Flow supporting 1 million flows (requires MS-PIC for the T320, T640, and T1600)
IPsec and IKE	
IPsec	Security services license (requires the MS-PIC for the M7i, M10i, M40e, M120, M320, T320, T640, T1600, and TX Matrix)
S-ES	Security services license (requires the MS-PIC for the M10i, M7i, M5, M120, M160, M20, M320, M40e, T320, T640, and T1600)
S-ES-2K	Software license that supports 2,000 IKE sessions (requires the MS-DPC for the MX240, MX480, and MX960)
S-ES-4K-UPG	Software license upgrade from 2,000 to 4,000 IKE sessions (requires the MS-DPC for the MX240, MX480, and MX960)
S-ES-4K	Software license that supports 4,000 IKE sessions (requires the MS-DPC for the MX240, MX480, and MX960)
ES-6K-UPG	Software license upgrade from 4,000 to 6,000 IKE sessions (requires the MS-DPC for the MX240, MX480, and MX960)
S-ES-6K	Software license that supports 6,000 IKE sessions (requires the MS-DPC for the MX240, MX480, and MX960)
Link Services	
S-LSSL-4	Link Services software license that supports up to 4 multilink bundles (requires the MS-PIC for the M7i, M10i, M120, M20, M320, M40e, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
S-LSSL-256	Link Services software license that supports up to 255 multilink bundles per chassis (requires the MS-PIC for the M7i, M10i, M20, M40e, M120, M320, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
S-LSSL-255-UPG	Link Services software upgrade license from 64 to 255 multilink bundles per chassis (requires the MS-PIC for the M7i, M10i, M20, M40e, M120, M320, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
S-LSSL-1023	Link Services software license up to 1,023 multilink bundles per chassis (requires the MS-PIC for the M7i, M10i, M20, M40e, M120, M320, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
S-LSSL-1023-UPG	Link Services software upgrade license from 255 to 1,023 multilink bundles per chassis (requires the MS-PIC for the M7i, M10i, M20, M40e, M120, M320, T320, T640, and T1600, or the MS-DPC for the MX240, MX480, and MX960)
S-SERVICES-SFO	Stateful failover for services (MLPPP only) (requires the MS-PIC for the M7i, M10i, M20, M40e, M120, M320, T320, T640, and T1600)

MODEL NUMBER	DESCRIPTION
Telchemy ePM (TePM)	
S-TEPM-CTRLR-VOIP	Software license for one TePM Controller
S-TEPM-CTRL-ADD-1	Software license for one TePM Agent (requires TePM Controller (S-TEPM-CTRLR-VOIP) and MS-PIC for M7i, M10i, M120, M320, and M40e, or MS-DPC for the MX240, MX480, and MX960)
S-TEPM-CTRL-ADD-100	Software license for 100 TePM Agents (requires TePM Controller (S-TEPM-CTRLR-VOIP) and MS-PIC for M7i, M10i, M120, M320, and M40e, or MS-DPC for the MX240, MX480, and MX960)
S-TEPM-CTRL-ADD-25	Software license for 25 TePM Agents (requires TePM Controller (S-TEPM-CTRLR-VOIP) and MS-PIC for M7i, M10i, M120, M320, and M40e, or MS-DPC for the MX240, MX480, and MX960)
S-TEPM-CTRL-ADD-5	Software license for 5 TePM Agents (requires TePM Controller (S-TEPM-CTRLR-VOIP) and MS-PIC for M7i, M10i, M120, M320, and M40e, or MS-DPC for the MX240, MX480, and MX960)
Stateful Firewall and NAT (including Carrier Grade NAT)	
S-SERVICES-SFO	Stateful failover for MLPPP only (requires MS-PIC for M10, M7i, M5, M120, M160, M20, M320, M40e, T320, and T640)
S-NAT-FW-SINGLE	NAT/firewall license, single instance (requires MS-PIC for M7i, M10i, M40e, M120, M320, T320, T640, and T1600)
S-NAT-FW-MULTI	NAT/firewall license, multi-instance (requires MS-PIC for M7i, M10i, M40e, M120, M320, T320, T640, and T1600)
S-SFW	Stateful firewall license (requires MS-DPC for the MX240, MX480, and MX960)
S-NAT	Stateful NAT license (requires MS-DPC for the MX240, MX480, and MX960)
Stateful Firewall and NAT (including Carrier Grade NAT)	
VAS-ERM-LTU	StreamScope eRM license (requires MS-DPC for the MX240, MX480, and MX960)
Tunnel Services and L2TP Network Services (LNS)[3]	
S-TUNNEL	Software license for tunnel services (requires the MS-PIC for the M7i and M10i)
S-LNS-2K	Software license for 2,000 L2TP LNS sessions (requires the MS-PIC for the M7i, M10i, and M120)
S-LNS-4K-UPG	L2TP LNS license upgrade from 2,000 to 4,000 sessions (requires the MS-PIC on the M120)
S-LNS-4K	Software license for 4,000 L2TP LNS sessions (requires the MS-PIC for the M7i, M10i, and M120)
S-LNS-8K-UPG	L2TP LNS license upgrade from 4,000 to 8,000 sessions (requires the MS-PIC for the M7i, M10i, and M120)
S-LNS-8K	Software license for 8,000 L2TP LNS sessions (requires the MS-PIC for the M7i, M10i, and M120)
S-LNS-16K-UPG	L2TP LNS license upgrade from 8,000 to 16,000 sessions (requires the MS-PIC for the M120)
S-LNS-16K	Software license for 16,000 L2TP LNS sessions (requires the MS-PIC for the M120)

[3]Tunnel services are also available directly on Trio-based DPCs for the MX Series 3D Universal Edge Routers.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Notes

Corporate and Sales Headquarters
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

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

1000382-001-EN June 2011

Printed on recycled paper