Juniper Networks **E320 Broadband Services Router**

The Evolution of Broadband

Broadband services are evolving beyond simple Internet access to advanced Triple Play services requiring Quality of Service (QoS) and a substantial increase in bandwidth per subscriber. The delivery of these services on a large scale requires a new generation of edge router, one that is optimized for deploying a vast range of innovative and converged voice, data, and multi-media services that simply cannot be cost effectively supported by earlier B-RAS (Broadband Remote Access Server) Platforms. To meet the stringent requirements of Triple Play services, Juniper has delivered the industry's most advanced Broadband Services Router (BSR).

E320 Broadband Services Router

Juniper Network's E320 is the first Broadband Services Router designed specifically to deliver Triple Play services to both corporate and residential subscribers. The E320 enables Service Providers to differentiate between their service offerings and those of their competitors through a unique blend of both hardware and software features that combine with enhanced QoS capabilities and substantial system capacity to enable both bandwidth scalability and subscriber density.

The E320 is a modular, carrier-class design with a passive midplane, active front-insert Line Modules (LM) and a high-reliability, rear-insert input/output adapter (IOA).

The E320 uses a distributed, multiprocessor architecture that allocates processing functions to each Line Module in the system to speed decision making and scale system growth. Unlike other routers with centralized processing architectures, the E320's distributed processing architecture allows Service Providers to incrementally add processing power as new subscribers or services are provisioned. This is critically important when maintaining service quality for existing customers and reduces the need to purchase additional routers due to diminishing performance.

The E320 system's innovative design provides a fast path for IP traffic by removing the route processor from the forwarding path and maintaining an entire routing table on each port. The E320's unique hardware architecture enables a complete search of the forwarding table for each packet, while maintaining wire speed performance. This design allows the system to avoid the non-deterministic performance of cache-based searches and the associated uncertainty in packet latency.

The E320 system design also supports wire-speed QoS handling; consequently, the system can examine, classify, and queue packets at wire speed. A scheduling function then regulates the packet flows onto the egress link based on the QoS policy assigned to each flow. All QoS policies for all flows are centrally configured and then distributed to each line module for on going execution. Because all QoS handling is distributed to the line modules, overall system performance is maintained even when additional line modules are added to the system. Regardless of the number of QoS policies or the volume of traffic, the system offers consistently high performance without compromise.

The E320 system makes use of application-specific integrated circuits (ASICs) in order to speed IP packet processing. The Juniper Networks custom ASICs, called the ESPII (edge service processor two), enable the E320 to meet the forwarding demands of the broadband edge.

Older-generation routers cannot cope with the processor demands of QoS functions, such as classification, queuing, and scheduling while routing packets at wire speed. The E320 overcomes these limitations with its hardware-assisted architecture.

The system's use of ESPII ASICs provides significant benefits to the Service Provider. ASICs help to:

- Reduce product size
- Reduce product cost, especially packet per second cost
- Increase packet-processing speeds dramatically by applying targeted power to hard-wired tasks

JUNOSe Software

JUNOSe is the operational software for the Juniper Networks market leading E-series family of Broadband Services Routers. The JUNOSe software architecture is modular, object oriented, and component-based to increase overall system reliability, ease software upgrades, and reduce new feature development time. In contrast to older monolithic software architectures, the modularity of the JUNOSe system architecture improves stability and reliability by ensuring that the behavior of one program module does not adversely affect others.

For increased reliability, JUNOSe incorporates leading resiliency technologies such as IETF graceful restart, hitless switchover, MPLS fast reroute, VRRP, APS and zero-touch Line Module failover to minimize or eliminate service disruption.

Quality of Service

Enabling QoS on a network allows preferential treatment of high priority traffic, whether it is low latency Voice over IP traffic, or a customer's mission critical data traffic. The ability for a service provider to differentiate traffic types for a customer provides new revenue opportunities, such as premium pricing for differentiated traffic treatment, or guaranteed bandwidth for assured delivery.

The E320 supports per subscriber based hierarchical queuing and scheduling in ASIC hardware. The following capabilities are supported on the E320:

- Up to 8 hardware queues per subscriber interface to support multiple traffic types
- Rate-limiting of individual queues, logical interfaces and physical interfaces
- Prioritization of traffic types per subscriber (e.g. Voice, Video, Internet) and the requisite assignment to specific queues for appropriate QoS treatment

- Scheduling based on either round robin, weighted round robin, or strict priority
- DiffServ-based traffic classification (Assured Forwarding and Expedited Forwarding Per Hop Behavior)
- Random Early Discard and Weighted Random Early Discard within each hardware queue
- Prioritization of traffic between different subscriber interfaces (e.g. business vs. residential) to ensure "fairness" between subscribers

The E320 can use the flexibility of hierarchical QoS to differentiate traffic for individual subscribers. Hardware based functionality ensures consistent wire rate performance as services are scaled up.

Subscriber Management and "Zero Touch Provisioning"

Juniper Network's E320 provides "zero touch provisioning", essentially auto-detecting the encapsulation protocol (e.g. PPPoE, PPPoATM, DHCP or IP) on an ATM VC or Ethernet VLAN, and then authenticating the session via Radius. For DHCP authentication, option 82 and the physical device's MAC address can be forwarded to the Radius server. This provides the same subscriber management capability currently used for PPP to also be utilized for DHCP subscriber access.

The wide range of subscriber management features on the E320 gives service providers the flexibility to support access methods, authentication and policy management options that suit their operational and market requirements.

The E320 is designed to be access agnostic, a services edge platform that can aggregate of thousands of logical IP interfaces, regardless of the access protocol of the interface. IP access via the following encapsulation protocols are supported:

- IP/PPP
- IP/FR
- IP/ATM
- IP/PPP/FR
- IP/PPP/ATM
- IP/PPPoE/FR
- IP/PPPoE/ATM
- IP/PPP/SONET/SDH (POS)
- IP/VLAN
- IP/Ethernet
- IP/PPPoE/VLAN
- IP/PPPoE/Ethernet

The E320 can support multiple DHCP and PPPoE sessions on a single Ethernet VLAN or ATM VC. Each DHCP or PPPoE session has its own logical IP interface, address and policies. This flexibility allows service providers to deploy a variety services to end customers via multiple logical IP interfaces on the same L2 circuit. For example, delivery of video and internet traffic to an end customer could be done via multiple PPPoE or DHCP sessions in the same Layer 2 (VLAN or VC) circuit, with traffic differentiation between PPPoE and DHCP sessions.

- User identification is a critical component of dynamic access networks. Identification is required:
- to apply intelligent policies (e.g. QoS for different traffic types)
- policy management to control which services are available to a user, and charge appropriately, and
- to quickly find sources of attacks and protect the network and resources from these attacks.

Policy Management

The E320 supports IP session-based policies that can be applied to both ingress and egress traffic. Policies can be applied to each IP session statically via configured Profiles, or dynamically via Radius during session authentication or with Juniper Networks SDX Service Deployment System.

The E320 supports per subscriber policies that allow granular control of IP traffic. Policies are applied to individual IP sessions and use multi-field classifiers to identify traffic based on attributes contained within IP headers. Policy actions include:

- **Color:** Mark traffic green, yellow or red to signify discard priority once inside a hardware queue. WRED uses different discard thresholds for each of these colors.
- **Filter:** Drop packets matching the classifier, can be used to enforce security.
- **Forward:** Forward traffic matching the classifier.
- **Log:** Log traffic matching the classifier, can be used for security monitoring.
- **Mark:** Change the TOS/Precedence/DiffServ settings in the IP header or Ethernet 802.1p settings.
- **Next Hop/Interface:** Override routing table and specify alternate outgoing interface.
- **Rate-Limit-Profile:** Ingress traffic policing with multiple rates defined. Committed, conformed and exceeded traffic can be assigned a color (green, yellow or red) to signify discard priority for WRED under congestion scenarios.
- **Traffic-class:** Assign traffic based on classifier to a specific QoS (e.g. strict priority, multi-media, interactive, best effort, etc). Traffic in each traffic class for a subscriber can be placed in a different hardware queue for QoS and scheduling.

Security

It is critical that routers in broadband networks provide the highest level of security against attacks while ensuring predictable and reliable performance. Broadband routers need to identify, suppress and prevent attacks from affecting end user services. Denial of Service (DoS) attacks are intended to take a router out of service by consuming processing cycles on invalid packets until the processing resources are exhausted. These attacks include the well known network based TCP SYN flood, SMURF and Ping of Death. Usually the source of these attacks is hidden using address spoofing (i.e. changing the source address of the attack packet).

The E320 has independent processing sites for both the forwarding plane and the control plane, which means that forwarding performance is not impacted by network overhead such as route processing. In addition to the performance benefits, this design has proven to be superior when guarding against security attacks such as DoS attacks. With the forwarding plane independent of the control plane, the E320 is able to control both the type of traffic and the amount of each traffic type that is processed at any given time. This granular control provides a security system that is unique to the E320. DoS attacks can be detected and prevented without any impact to forwarding performance.

The E320 supports source address validation for all packets entering the router. If the source address of the packet has been spoofed, the packet will be dropped thereby ending the threat at its roots.

Lawful Intercept Support

New emphasis on regulations for monitoring data traffic as it crosses carrier networks makes Lawful Intercept (LI) a crucial issue for service providers. As concern over everything from global terrorism to electronic fraud grows, the ability to capture traffic and isolate it for in-depth analysis has taken on much greater importance. With law enforcement authorities requiring the capability to focus in on individual subscriber flows and monitor where data traffic is coming from, where it's headed, and what it might contain, carriers have

no choice but to implement technology that allows that kind of close inspection—without impacting performance or the integrity of customer traffic.

Many broadband platforms support the management and monitoring of mirrored ports only at the Command Line Interface. Also, mirroring can only be enabled after the user logs in and the IP interface is created. For mobile users, it is hard for an administrator to predict the ingress point for a given user in order to enable mirroring. The static configuration of earlier broadband routers does not work well in an environment where users login and logout frequently. These issues make Lawful Intercept cumbersome and time consuming especially when there are a large number of routers in the network.

The E320 overcomes these limitations through its support of RADIUS Initiated Mirroring. RADIUS-based mirroring uses RADIUS and Vendor Specific Attributes (VSA) rather than CLI commands to identify a user whose traffic is to be mirrored. This method is dynamic; the mirroring is configured and enabled separately from the user's session. Service Providers can use a single RADIUS server to mirror multiple routers in their network.

RADIUS-based mirroring can be pre-configured such that mirroring is automatically initiated when the specified user logs on or a dynamic decision to mirror traffic can be initiated by RADIUS for a user that is already logged on. This makes RADIUS-based mirroring an excellent solution for broadband networks and for mirroring mobile users. This method also enables L2TP traffic to be at the L2TP access concentrator (LAC). If the L2TP network server (LNS) and the LAC belong to different service providers, RADIUS-based mirroring at the LAC allows the mirroring to take place close to the user's domain. The E320's mirroring feature is initiated without regard to the user location, router, interface, or type of traffic.

Multicast

As many multi-media services will be delivered across an IP multicast network, it is critical that each multicast stream is processed efficiently to eliminate any degradation of service. The E320's advanced architecture has been optimized to deliver high performance, IP multicast services to support these multi-media services including video, gaming and other high bandwidth applications. The E320 delivers efficient, high performance multicast processing by performing the multicast replication both within the switch fabric and on the egress line cards. This architecture delivers the lowest jitter, highest multicast performance and scale possible and is orthogonal to the rich H-QoS capabilities on E320. The separation of forwarding and control planes allows the E320 to quickly process IGMP packets to support sub-second "JOINS" and "LEAVES" for responsive channel changing services even when system is under full load.

High Availability

With the evolution of broadband multi-media services such as voice and video underway, the level of reliability required on broadband networks is comparable to the reliability associated with global voice networks. With this in mind, the E320 is designed for continuous availability and consistent high performance to achieve the availability levels required by Service Providers to support multi-media applications.

Hardware Design

The E320 provides redundancy on all major subsystems, including control plane redundancy as well as line module and port-level redundancy on the data plane. The control plane consists of the route processor function which is 1:1 redundant and the distributed switch fabric which is 1:4 redundant. Unlike other Broadband Services Routers, the E320 offers 1:N Line Module redundancy which provides the highest level of protection while minimizing CapEx expenditures required to achieve hardware redundancy. The IOA's can be protected via Automatic Protection Switching (APS). In addition, all common equipment such as fans and power are redundant assuring that there is no single point of failure.

Software Design

The E320's JUNOSe operational software is based upon a high-performance modular, object oriented design. Each program module has access to shared system resources, including memory, packet buffers, and processor cycles. This approach improves stability and reliability by ensuring that the behavior of one module does not adversely affect the others.

The combination of carrier-grade hardware and innovative software design helps decrease the time and complexity of maintenance functions, lowering overall operational costs and increasing subscriber satisfaction.

IPv6

IPv6 has become an essential part of broadband service and entertainment offerings for a variety of reasons: Growing number of broadband customers, proliferation of broadband devices and their remote management capabilities. The E320 is well suited for those environments and supports IPv6 natively: IPv6 fast-path forwarding and routing, IPv6-based subscriber management, policy and QoS - just to name a few.

The smooth migration from IPv4- to IPv6-based services is guaranteed through the dual-stack capabilities of the E320 and JUNOSe. A given subscriber can have both IPv4 and IPv6 sessions in parallel, which are auto-sensed and controlled by a single policy server entity such as RADIUS or Juniper's SDX policy manager. IPv6 specifics such as NCPv6 and DHCP-Prefix Delegation are tightly integrated into the suite of subscriber management features. IPv6 Multicast in conjunction with MLDv1 and MLDv2 is the building block for IPv6-based TV services and is accompanied by a rich set of IPv6 packet classification, policy, hierarchical QoS, tunneling and DOS prevention functions.

E320 Components

The primary components of the E320 include; the Switch Route Processor (SRP) modules, the Switch Fabric Modules (SFM), Line Modules (LM), and Input Output Adapters (IOA). Line Modules can be used for access or uplink ports. Access line modules receive traffic from low-speed circuits, and the system routes the traffic onto higher-speed uplink line modules and then to the core of the network. Line Modules act as frame forwarding engines for the physical interfaces on the IOAs.

SRP Module

Switch route processor (SRP) modules perform system management, routing table calculations and maintenance, forwarding table computations, statistics processing, configuration storage, and other control plane functions. The SRP module determines which line modules are physically present in the chassis and monitors and controls vital functions on the line modules.

SRP IOA

The SRP IOA is a single corresponding input/output adapter that interfaces with the SRP module(s) through the system's midplane. The same SRP IOA works with all SRP modules.

SFM Module

The switch fabric modules (SFMs) work with the SRP module(s) to create a distributed shared memory switching fabric for the router. Each SFM module has its own memory and power adapter. Like the SRP module, the SFM module contains a single fabric slice.

Line Modules (LMs)

Line modules (LMs) act as frame forwarding engines for the physical interfaces, which are the IOAs, and process data from different types of network connections. In the current release, a single line module pairs with all available IOAs.

I/O Adapters (IOAs)

Most input/output adapters (IOAs) provide the physical interconnection to the network via small form-factor pluggable transceivers (SFPs). Insert each IOA into the back of the system, directly behind a line module. Each Line Module can support up to two half-height IOA's.

E320 Broadband Services Router Specifications

Weight

Chassis only	88 lb (39.9 kg)
Chassis fully configured	Approximately 215 lb (97.5 kg)

Dimensions

With cable management bracket and bezels	24.5 (H) x 19 (W) x 28 (D) inches 62.23 x 48.26 x 71.12 cm
Chassis only	24.5 (H) x 19 (W) x 25 (D) inches 62.23 x 48.26 x 63.5 cm

Environmental Requirements

	NEBS GR-63-CORE compliant
Ambient operating temperature	• Long term: 41° to 104° F (5° to 40° C) • Short term: 23° to 122° F (–5° to 50° C)
Ambient operating humidity	• Long term: 5% to 85% (noncondensing) • Short term: 5% to 95% (noncondensing)
Ambient storage temperature	–40° to 158° F (–40° to +70° C), 95% relative humidity
Ambient storage humidity	5% to 95% (noncondensing)

Heat Dissipation

DC Input	4800 W, 16380 BTU/hour maximum
Voltage	–40° to –72° VDC

NOTE: If the voltage rises above –40 VDC, the system will power off. The system will not power on again until the input voltage reaches –43 +/– 0.5 VDC.

Current	100 A @ –48 VDC
Power	4800 W maximum
Redundancy (input power)	2 independent line feeds

Space Requirements

- 3 feet (90 cm) behind router or rack
- No space requirements for sides of units or rack
- Do not block air vents on front or back of the router

Airflow

An integral air plenum directs router's exhaust air below the router and out the back.

NEBS Certification

- SR-3580 (FD-15): Network Equipment Building System (NEBS) Criteria Levels, Issue 1, November 1995
- GR-63 (LSSGR, FD-15): Network Equipment Building System (NEBS) Requirements: Physical Protection, Issue 1, October 1995
- GR-1089 (LSSGR, FD-15): Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment, Issue 2, Revision 1, February 1999

Safety Agency Certification

- AS/NZS 3260:1993, Safety of Information Technology Equipment Including Electrical Business Equipment
- CAN/CSA C22.2, No. 60950-00, 3rd Edition, Safety of Information Technology Equipment
- EN60825-1, Safety of Laser Products - Part 1: Equipment Class, Requirements, and User's Guide (2001)
- EN60950:2000, 3rd Edition, Safety of Information Technology Equipment
- IEC 60950-1(2001-10) Ed. 1.0 Information technology equipment - Safety - Part 1: General requirements
- Low Voltage Directive (73/23/EEC)
- UL 60950, 3rd Edition, Safety of Information Technology Equipment

Electromagnetic Emissions Agency Certification

- AS/NZS 3548:1995 (CISPR 22 Class A)
- EMC Directive (89/336/EEC)
- EN55022 Class A (CISPR-22 Class A)
- EN55024, Annex C for WAN Equipment Performance Criteria A, B, and C
- ETSI 300-386, Telecommunication Network Equipment; ElectroMagnetic Compatibility (EMC) requirements
- FCC Part 15 Class A
- IECS-003 Issue 3 Class A
- VCCI (Voluntary Control Council for Interference by Information Technology Equipment)

Telecommunications Certification

- ACA TS 016-1997
- CTR13 – Commission Decision of 9 July 1997 on a common technical regulation for attachment requirements for terminal equipment interface for connection to 2048 kbit/s digital structured ONP leased lines: 97/521/EC – OJ No. L215 Vol. 40, August 1997
- CTR24 – Commission Decision of 9 September 1997 on a common technical regulation for attachment requirements for terminal equipment interface for connection to 34 Mbit/s digital unstructured and structured leased lines: 97/639/EC – OJ No. L271 Vol. 40, 3 October 1997
- FCC PART 68
- IECS-003 Issue 3 Class A
- PD7024 – Essential requirements for terminal equipment intended for connection to unstructured digital leased circuits of the public telecommunications network using a CCITT recommendation G,703 interface at a rate of 2048 kbit/s with a 75 ohm unbalanced presentation, 1994
- RTTE Directive (1999/5/EEC)

Juniper® NETWORKS

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.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

100103-002 May 2006