

Acme Packet Net-Net 3820

data sheet

Overview

Acme Packet's Net-Net 3820 is a session border controller (SBC) or session routing proxy (SRP) solution for mid-range enterprise or service provider deployments. The Net-Net 3820 features Acme Packet's custom hardware design tightly integrated with Net-Net OS to provide the critical controls for delivering trusted, first-class interactive communications—voice, video and multimedia sessions—across IP network borders. The Net-Net 3820 complements Acme Packet's Net-Net 4500, 9200 and 14000 platforms and supports most of the SBC and SRP functions and features that are supported on Acme Packet's high-end platforms.

Solutions

In enterprise and contact centers the Net-Net 3820 secures the high quality delivery of a broad range of interactive communications services and applications ranging from basic VoIP to Service Oriented Architecture (SOA)-enabled unified communications. It secures the SIP/H.323 trunking border to service provider IP networks and the Internet border to remote offices, teleworkers and mobile employees. In extremely security-conscious organizations, the Net-Net 3820 even secures the border to the private VPN connecting other sites. The SIP and H.323 interworking capabilities of the Net-Net 3820 ensures interoperability with and between legacy IP PBX equipment and next-generation unified communications platforms. It controls session admission, IP PBX or UC server loads and overloads, IP network transport and SIP/H.323 session routing to assure SLAs and minimize costs. Regulatory compliance requirements are also satisfied with encryption ensuring session privacy and call/session replication for recording.

For government defense and security-focused agencies, the Net-Net 3820 meets the stringent requirements needed to comply with standards such as the U.S. Federal Information Processing Standard (FIPS). Acme Packet's implementations of SIP-TLS, IPsec, SSH and SFTP all comply with FIPS 140-2 without requiring special hardware. It also features configuration options to mitigate security vulnerabilities as required for products approved by the U.S. Defense Information Services Agency (DISA) to connect to Department of Defense networks.



Acme Packet Net-Net 3820

For fixed line and cable service providers, the Net-Net 3820 meets all session border control requirements for residential and business VoIP, SIP trunking and hosted PBX, unified communications (UC) or audio/video conferencing services. For mobile and fixed mobile convergence (FMC) service providers, the Net-Net 3820 controls femtocell, dual-mode handset and smart-phone access to IP interactive communications services and applications over next generation 3G, LTE and WiMAX networks. Service providers may also utilize the Net-Net 3820 for core SIP session routing or to control interconnect borders for peering services applications.

The Net-Net 3820 secures subscriber access and interconnect/peering borders and enables interoperability of heterogeneous endpoints, service infrastructure elements and networks to maximize service reach. It controls admission, overload, IP network transport and session routing to assure SLAs, maximize revenues and minimize costs. It efficiently routes SIP-based interactive communication sessions—voice, video, instant messaging and multimedia—within and between networks. Lastly, it enables regulatory compliance with emergency service (E911), national government priority service (GETS) and lawful intercept (CALEA) requirements.

For small to medium-sized service providers as well as enterprises requiring a highly available NEBS-compliant solution, the Net-Net 3820 offers a choice of single or dual AC or DC field-replaceable power supplies, as well as field replaceable fan packs. For services and applications requiring support for up to 8000 sessions, the Net-Net 3820 delivers the same hardware features and purpose-built architecture as high-end systems.

System capacity, performance and availability

The Net-Net 3820 platform supports up to 8,000 sessions, offers high availability operation for non-stop service and includes hardware acceleration options for encryption and QoS measurements. The Net-Net 3820 complements Acme Packet's Net-Net 4500 and 9200 platforms and delivers the following platform capabilities:

- Session capacity* – up to 8,000 simultaneous signaled sessions
- High-availability (HA) configuration – active/standby systems (1:1 redundancy) with check-pointing of signaling, media and configuration state for no loss of service
- In-line, wire-speed QoS measurement processor option
- Two-level encryption acceleration hardware options
 - Session set-up – IPsec tunnels and TLS sessions
 - Traffic encryption/decryption – IPsec and SRTP
- IPsec tunnel capacity
 - Up to 1,000 tunnels with manual keys
 - Up to 120,000 tunnels with IMS-AKA
- SIP-TLS capacity – up to 200,000 connections
- SRTP capacity – up to 8000 call legs
- Transcoding capacity – up to 7200 transcoded sessions
- Local route table entries – up to 1,000,000 routes
- Network interfaces – four active 10/100/1000 Mbps Ethernet interfaces (fiber or copper)
- System throughput – 5 Gbps
- Power supplies – single or dual field-replaceable AC or DC power supplies

* Performance and capacity vary by signaling protocol, call flow, codec, configuration and feature usage.

Session Border Controller (SBC) configurations

The Net-Net 3820 supports two Acme Packet SBC configurations, the integrated Net-Net Session Director (SD) and decomposed Net-Net Signaling Firewall (SF), which delivers SIP signaling security and other control functions.

With comprehensive support for SIP, H.323, SIP-H.323 interworking, MGCP/NCS and H.248 signaling and media sessions, Net-Net OS for the Net-Net 3820 offers proven signaling interoperability with all major softswitches, IMS CSCF elements, SIP servers, H.323 gatekeepers, call agents, application servers, media servers, media gateways, IP PBXs, UC servers and numerous IP-based voice and video endpoints.

Net-Net 3820 SBCs can also be configured to operate as members of a Net-Net SBC cluster when used in conjunction with Acme Packet's Net-Net 4500 Session-aware Load Balancer (SLB). Acme Packet Net-Net SBC clusters support up to 2 million subscribers without requiring architectural forklifts or network disruptions. Net-Net SBC clusters support all Net-Net SBC configurations.

Session Routing Proxy (SRP) configuration

The Net-Net 3820 Session Router (SR) is a session routing proxy that consolidates and simplifies the routing of SIP-based voice, video, instant messaging and multimedia sessions within and between mobile, fixed-line and transit networks to help service providers reduce capital and operating expenditures while optimizing service revenue.

In Acme Packet's Open Session Routing Architecture (OSR), the Net-Net 3820 SR works in conjunction with best-of breed routing database products and services from Acme Packet partners. These complementary product vendors and service providers offer centralized routing databases and database provisioning tools for dynamic route selection. The Net-Net 3820 SR queries these databases using industry-standard ENUM, SIP and DNS protocols. The Net-Net 3820 SR's local route tables may also be provisioned by Acme Packet's Net-Net Route Manager Central (RMC).

The Net-Net 3820 SR dynamically routes sessions between all types of borders, including access and interconnects, IP and TDM. More specifically, it routes sessions between stateful service control elements such as Acme Packet SBCs, wireless Mobile Switching Centers (MSC), IMS subscriber call control elements and softswitches controlling media gateways. Since the source and destination SIP signaling elements are session-stateful, the Net-Net SR can operate in a stateless or transaction-stateful mode to maximize its performance.

Common functions

Net-SAFE™, Acme Packet's SBC security framework, is supported via the tight integration of the Net-Net 3820 hardware and Net-Net OS software. Net-SAFE features powerful denial-of-service/distributed denial-of service protection at the layer 3, layer 4, IPsec and SIP signaling level, and intrusion detection/prevention capabilities. Other security features support dynamic access control, topology hiding, privacy and confidentiality, service infrastructure DoS/DDoS protection, virus and SPIT protection, and fraud prevention.

Net-Net Central, our next-generation management platform, delivers highly-scalable configuration and fault, performance and security management for Acme Packet products and solutions. Its flexible high-availability architecture accommodates very large networks and provides extensibility for hosting advanced management application add-ons. Through its dashboard summary and multiple configuration views, Net-Net Central facilitates flow-through provisioning, capacity planning and comprehensive performance and fault-monitoring with "at-a-glance" status indicators that simplify real-time network-wide management. Through standard interfaces including SNMP, SFTP, XML and SOAP, Net-Net Central also integrates with OSS/BSS ecosystems to deliver advanced service fulfillment, service assurance, billing and mediation.

Net-Net 3820 Network Interface Units

The rear slot of the Net-Net 3820 accommodates a single Network Interface Unit (NIU) module. Net-Net 3820 NIUs are offered in a variety of configurations to address a wide range of network, service and application scenarios. All Net-Net 3820 NIUs include four Ethernet interfaces for signaling, media and data traffic. The NIUs also integrate the system alarm and management interfaces, including those used for the physical configuration of high-availability (HA) system pairs.

Net-Net 3820 NIUs are offered with the following interface speeds and connection types

- 10/100/1000 Mbps with copper RJ45 connectors
- 10/100/1000 Mbps via small form factor-pluggable (SFP) copper transceiver
- 1 Gbps via with small form factor-pluggable (SFP) connectors for copper or fiber optic transceiver connectivity

Encryption and QoS monitoring and reporting options

To meet the demands of scalable, high-quality interactive communications, Net-Net 3820 NIUs offer a variety of on-board hardware and processor options designed to offload the 3820 CPU from processor-intensive functions such as security and QoS monitoring and reporting.

Net-Net 3820 1Gbps NIUs with SFP interfaces can accommodate on-board processor options for IPsec and SRTP encryption, QoS monitoring and reporting, or both.

On-board encryption acceleration hardware enables secure communications without compromising end user or subscriber quality of experience (QoE).

QoS monitoring and reporting hardware monitors and measures each media flow through the system, calculating quality scores (such as Mean Opinion Score, or MOS), and aggregating the information into data for transmission to external reporting or accounting systems. On-board QoS monitoring and measurement is also utilized for real-time functions such as QoS-based routing and load balancing, also without compromising end user or subscriber quality of experience (QoE).

Net-Net 3820 advanced function NIUs

Net-Net 3820 advanced function NIUs help the Net-Net 3820 deliver a combination of performance, capacity and functionality unmatched by other platforms in its class. With a distributed, multi-processor approach that leverages the latest DSP and multi-core processors, the Net-Net 3820 is capable of performing many of the functions offered by our high-end chassis-based system, the Net-Net 9200, at the reduced capacity levels required by many enterprises as well as smaller service providers.

Transcoding NIU

Acme Packet's Transcoding NIU for the Net-Net 3820 delivers a low to mid-range hardware-based transcoding solution that complements the high-capacity transcoding offered on our Net-Net 9200 platform. With this NIU, the Net-Net 3820 supports up to 7200 transcoded sessions. The Transcoding NIU also includes features QoS monitoring and reporting hardware for both transcoded and non-transcoded sessions. The Net-Net 3820 Transcoding NIU may be populated with up to twelve transcoding modules, each supporting up to 600 transcoded sessions, for pay-as-you-grow scalability.

Enhanced Traffic Control NIU

Acme Packet's Enhanced Traffic Control (ETC) NIU offers a unique and highly-advanced design, with enhanced capabilities that address a wide range of next-generation services and applications. The ETC NIU is a high-performance multi-processor engine for the Net-Net 3820 that combines multiple hardware-accelerated functions including:

- High-capacity SRTP encryption
- High-capacity termination for SIP-TLS
- Separate, dedicated processors for high capacity IPsec encryption and TCP termination
- Integrated hardware for QoS monitoring and reporting

The extensible multi-core, multi-processor architecture of the ETC NIU is also capable of supporting additional applications and functions as new requirements emerge.

Net-Net 3820 specifications	
Chassis	<ul style="list-style-type: none"> • 1U, rack-mount • Front – power and HA status LEDs, physical system reset pinhole, console • Rear – one network interface unit slot (signaling, media and management interfaces) • Power supplies – single or dual AC or DC, field replaceable • Optional mounting brackets for front/rear or center-mount in 19” or 23” rack
Memory	<ul style="list-style-type: none"> • 2 GB for active configuration and logs • 256 MB internal flash memory for runtime image and backup configurations • Optional storage expansion module for local CDR backup
Content addressable memory (CAM)	<ul style="list-style-type: none"> • 128K entries for static & dynamic ACLs, media control rules and ARP entries
Encryption options	<p>TLS</p> <ul style="list-style-type: none"> • Software-based encryption for low capacity TLS sessions • Secure Services Module (SSM) hardware accelerator option for high capacity TLS sessions <p>SRTP</p> <ul style="list-style-type: none"> • Network Interface Unit (NIU)-based encryption processors <p>IPsec</p> <ul style="list-style-type: none"> • Tunnel set-up – software-based for use of manual keys; Secure Services Module (SSM) hardware accelerator option for use of dynamic keys • Traffic encryption – NIU-based encryption processors
Network interface units (NIU)	<p>Supports network interfaces for signaling, media and data</p> <p>Basic NIUs and options</p> <ul style="list-style-type: none"> • Four 10/100/1000 Mbps Ethernet copper ports (RJ-45 connector) • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports (requires SFP transceivers) • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports with inline IPsec/SRTP encryption processors (requires SFP transceivers) • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports with inline QoS measurement processors (requires SFP transceivers) • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports with inline IPsec/SRTP encryption and QoS measurement processors (requires SFP transceivers) <p>Transcoding NIU</p> <ul style="list-style-type: none"> • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports (requires SFP transceivers) • Up to twelve on-board transcoding digital signal processor (DSP) modules • Inline QoS measurement processors <p>Enhanced Traffic Control NIU</p> <ul style="list-style-type: none"> • Four 1000 Mbps Ethernet fiber or four 10/100/1000 Mbps copper ports (requires SFP transceivers) • Integrated high-capacity encryption (IPsec, SRTP, TLS) processors • Inline QoS measurement • Integrated hardware-based SIP-TLS and TCP processing <p>NIU management interfaces – included on all NIU options</p> <ul style="list-style-type: none"> • Two 10/100/1000 Mbps interfaces with RJ-45 for HA node configurations • One 10/100/1000 Mbps interface with IPsec encryption processor and RJ-45 for management networks (Optional IPsec encryption of management interface via encryption capable NIU) • One RS-232 serial console interface with RJ-45 connector (only rear or front interface may be used at any time) • One alarm interface with RJ-45 connector
Front panel management interfaces	<ul style="list-style-type: none"> • One RS-232 serial console interface with RJ-45 connector (only rear or front interface may be used at any time) • One USB 2.0 interface • LEDs for displaying power and HA status • Physical system reset pinhole

Power	
AC power option	<ul style="list-style-type: none"> • Single or dual field-replaceable power supplies • Dual power supplies are redundant and load sharing, 300 VA max • Voltage: Autoranging 100-240 VAC wide input with power factor correction • Frequency: 50/60 Hz • Current: 3A x 2 rating • Cable: 2.0 meter 18 AWG 3-wire cable, with 3-lead IEC-320 receptacle on the power supply end, and a country-dependent plug on the power source end
-48 VDC power option	<ul style="list-style-type: none"> • Single or dual field-replaceable power supplies • Dual power supplies are redundant and load sharing, 300 VA max • Voltage: -48 VDC (+- 10%) nominal in North America. Maximum range is -40VDC to -60 VDC • Current: 7A x 2 rating • Cable: 18 AWG recommended minimum, with at least 3 conductors rated for at least 140° F (60° C)
-72 VDC power option	<ul style="list-style-type: none"> • Voltage: -72 VDC nominal in Russia • Cable: 18 AWG recommended minimum, with at least 3 conductors rated for at least 140° F (60° C)
Physical	
Dimensions	<ul style="list-style-type: none"> • 1.72 in H x 17.10 in W x 19.00 in D (not including mounting hardware) • 4.37 cm H x 43.43 cm W x 48.26 cm D (not including mounting hardware)
Weight	<ul style="list-style-type: none"> • 19 lbs (8.62 kg) fully configured
Colors	<ul style="list-style-type: none"> • Front panel - Midnight black with Glacier blue trim
Temperature	<ul style="list-style-type: none"> • Operating: 32°F to 104°F, 0°C to +40 °C • Storage: -4°F to 149°F, -20°C to +65 °C
Relative humidity	<ul style="list-style-type: none"> • 10 to 85%, non-condensing
Air flow	<ul style="list-style-type: none"> • 50 cfm front to back
Heat dissipation	<ul style="list-style-type: none"> • 100W (341 BTU/hour) typical, 200W (682 BTU/hour) maximum
Power dissipation	<ul style="list-style-type: none"> • 100W typical, 200W maximum
Regulatory	<ul style="list-style-type: none"> • Product bears CE¹ marking indicating compliance with the 99/5/EC directive, which includes EN and IEC standards for safety and EMI
Safety	<ul style="list-style-type: none"> • US: UL² 60950-1, 2nd edition • Canada: CSA³ 60950-1-07, 2nd edition • EU: EN⁴ 60950-1:2006
EMC	<ul style="list-style-type: none"> • US: FCC⁵ Part 15 (CFR 47) Class A limits • Canada: ICES⁶-003 Issue 4, Class A limits • EU: EN 55022:2006 +A1:2007 Class A limits • Australia: CISPR 22 and C-Tick • Japan: VCCI⁷ Class A limits
Immunity	<ul style="list-style-type: none"> • EU: EN 300 386 v1.4.1
NEBS compliance	<ul style="list-style-type: none"> • GR-63 • GR-1089 • SR-3580 – Level 3
U.S. Department of Defense Security	<ul style="list-style-type: none"> • FIPS 140-2 compliant • Defense Information Systems Agency (DISA) Unified Communications Requirements (UCR) compliant • Listed – DISA Unified Capabilities Approved Product List (UCAPL)
<p>¹CE = European Compliance ²UL = Underwriters Laboratory ³CSA = Canadian Standards Association ⁴EN = European Norm ⁵FCC = Federal Communications Commission ⁶ICES = Interference-Causing Equipment Standard ⁷VCCI = Voluntary Control Council for Information Technology Equipment</p>	



100 Crosby Drive
Bedford, MA 01730 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com

© 2011 Acme Packet, Inc. All rights reserved. Acme Packet, Session-Aware Networking, Net-Net and related marks are trademarks of Acme Packet. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Acme Packet without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Acme Packet assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Acme Packet, Acme Packet has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.

09/08/11