


## Acme Packet session border controllers

Acme Packet Net-Net session border controllers (SBC) provide critical control functions to deliver trusted, first-class interactive communications—voice, video and multimedia sessions—across IP network borders. They support multiple applications in service provider, enterprise, government and contact center networks—from SIP trunking to hosted VoIP enterprise and residential services to fixed-mobile convergence.

SBC platforms by market

Markets	Net-Net 2600 & Net-Net OS-E	Net-Net 3800	Net-Net 4250	Net-Net 4500 & ATCA blade	Net-Net 9200
					
Enterprise	*	*	*	*	*
Gov't defense/ security sectors		*		*	
Contact center	*	*	*	*	*
Service provider		*	*	*	*

Our Net-Net family of SBCs leverage Net-Net OS, our operating system environment, and supports several different integrated and decomposed SBC configurations on our hardware platforms—the Net-Net 2600, 3800, 4000, and 9200 series systems and the Net-Net 4500 ATCA blade. Our software-only SBC platform, Net-Net OS-E, supports an integrated SBC configuration for enterprises and contact centers on Acme Packet-certified third-party servers.

Acme Packet Net-Net SBCs deliver the industry's richest session border control functionality in terms of architectural flexibility, signaling protocol breadth, control function and feature depth, and carrier-class availability and manageability.

**Architectural flexibility** - integrated SBC with signaling & media control, decomposed SBC with media control only and/or signaling control, access SBC with or without P-CSCF, interconnect SBC

**Multi-protocol signaling** - SIP, H.323, MGCP/NCS, H.248, RTSP, SIP-H.323 & H.323 interworking; SIP & H.323 load balancing & routing; H.248 distributed SBC control

**Integrated, hardware-software-based DoS/DDoS protection** - dynamic SBC self-protection against layer 3 / 4, IPsec and signaling protocol-related attacks and overloads

**Control functions & features** - over 500 configuration parameters for control in the areas of security, service reach maximization, SLA assurance, revenue & cost management and regulatory compliance

**Carrier-class high availability (HA)** - check-pointing of media, signaling & configuration state ensures no loss of active calls, or call state required for NAT traversal, session handling (transfer/hold, etc.) or accounting

**Management** - embedded browser-based configuration and call tracing, EMS, SAS, CLI, HTTPS, SSH, telnet, FTP, XML, RADIUS, SNMP, syslog, secure management

## SBC configurations

Acme Packet SBCs may be configured with signaling and media control integrated in a single system (integrated SBC) or with signaling and media control divided across separate systems (decomposed SBC). Acme Packet offers the following SBC configurations:

- **Net-Net Session Director (SD)** - integrated SBC with multi-protocol signaling and media control
- **Net-Net Border Gateway (BG)** - decomposed SBC with media control only, uses H.248 control interface to master Acme Packet Session Controller or third-party SIP signaling element
- **Net-Net Session Controller (SC)** - decomposed SBC with SIP signaling control only, uses H.248 control interface to slave Acme Packet Border Gateway or third-party media proxy/relay
- **Net-Net Signaling Firewall (SF)** - decomposed SBC with SIP signaling security and other control functions

The table below illustrates the SBC configurations supported by each Acme Packet platform.

Acme Packet platforms by SBC configuration

Net-Net SBC configuration	Net-Net 2600 & Net-Net OS-E	Net-Net 3800	Net-Net 4250	Net-Net 4500 & ATCA blade	Net-Net 9200
					
SD	*	*	*	*	*
SC			*	*	*
BG			*	*	*
SF			*	*	*

## SBC functions & features

### Security

- SBC DoS/DDoS protection
  - Protect SBC from DoS/DDoS attack and other malicious attacks
  - Protect SBC from non-malicious overloads
  - Allow trusted/authenticated users access while under DoS attack
  - Dynamically accept or reject traffic based on device behavior
- Access control
  - Filter specific devices or whole networks on a per application basis
  - Permit access to known devices or networks
  - Permit access to from authorized/registered users; permit or deny access to mask users
  - Dynamically accept or reject traffic based on device behavior
  - Accept media only for authorized sessions
- Topology hiding & privacy
  - Hide core topology to prevent directed attacks and preserve confidentiality
  - Mask user information for privacy and confidentiality
  - Protect users and service provider infrastructure from eavesdroppers, identity thieves and fraud
  - Secure L2 and L3 VPN customers by maintaining security isolation between VPNs; support inter-VPN sessions
  - Support inter-VPN sessions; monitor media for intra-VPN sessions for lawful intercept or fraud prevention
- Virus, worm & SPIT protection
  - Protect network from malicious attachments, prevent malformed messages from overloading resources
  - Restrict usage to prevent automated dialing/unwanted sessions
- Service infrastructure DoS prevention
  - Prevent DoS attacks from reaching core service infrastructure
  - Protect core from signaling overload attacks by enforcing call rate limiting, message rate limiting and code gapping policies

- Fraud prevention
  - Perform signaling and media validation by authenticating and authorizing users
  - Enforce service contract per-user/device and prevent piggy-back usage
- Monitoring and reporting
  - Monitor and report on alarms for attacks and overloads
  - Audit trails for attack response & fraud investigation
  - Provide secure monitoring & management access to protect from unauthorized personnel

#### Service reach maximization

- NAT traversal
  - Enable incoming and outgoing calls to traverse premise-based NAT devices by discovering public/external IP addresses for signaling and media or keeping NAT pinholes open for signaling
- Address translation
  - Bridge IP address spaces - private-public, private-private, IPv4-IPv6
  - OLIP/VPN bridging and aggregation eliminates the need to backhaul VPN links to core session control elements and signaling NAT function
- Telephone number & URI manipulation
  - Enable prefix, suffix, wildcard and other telephone number manipulations to enhance/control session routing
- Protocol translations and fix-ups
  - Signaling - provide protocol normalization, repair and interworking for SIP to SIP, H.323 to H.323, SIP to H.323, SIP to SIP-T, SIP to SIP-I, SIP-I to SIP-T
  - Transport - provide support & interworking for UDP, TCP, SCTP
  - Encryption - provide support & interworking for none, TLS, MTLS, IPsec, SRTP
  - Response codes - correct SIP & H.323 response code translations between networks/service providers
- Transcoding, transrating & DTMF translations
  - Transcoding - translation for wireline and wireless codecs
  - Transrating - mediate between variations in rate (e.g. 10ms to 30ms)
  - DTMF extraction / interworking - enable conversion from in-band to out of band signaling

#### SLA assurance

- Session admission control
  - Admit sessions based upon signaling & bandwidth constraints per user, network or session agent to ensure resource availability
  - Interface to external policy servers and bandwidth managers
- Overload protection & control
  - Load balance traffic based on number of sessions or rate of sessions
  - Reject or divert traffic based upon destination number to control mass calling events
- Failure detection, traffic re-route and recovery
  - Monitor performance and availability of L3 router, SIP registrar, SIP session agent
  - Re-route or re-distribute traffic based upon performance degradation or failure
  - Manage avalanche SIP registration events resulting from power outages or registrar failures by statefully managing endpoint re-registration process and load
- Transport control
  - Assign QoS marking/VLAN mapping based on application, source address or destination address
  - Release media peer-peer media between endpoints
- Quality reporting and quality-based routing
  - Measure QoS (latency, jitter and packet loss) and ASR per session
  - Append QoS and ASR information to CDR

- Route sessions based on observed QoS - jitter, loss, latency - or answer seizure ratio (ASR)
- Call replication for call recording - for contact center session handling quality assessments

#### Revenue & cost optimization

- Accounting
  - Generate CDRs for billing or network planning
  - Diameter, RADIUS or file-based accounting
- Service theft protection
  - Police media bandwidth per session based upon authorized codec
  - Terminate inactive session with session timers to free-up network and system resources
  - Ensure only authorized sessions receive correct QoS and resource allocation
- Routing
  - Least cost routing (LCR) - enables policy-based session control based on route cost
  - ENUM-based routing - increases routing infrastructure scalability and reduces PSTN costs
  - Carrier code-based routing - enables policy based session control based on prefix or carrier code
  - Industry-standard ENUM, SIP, XML and DNS interfaces to third-party routing databases
  - Large local route tables for static, localized routing decisions
- Codec stripping & re-ordering
  - Normalize codec at border to simplify core service network and routing

#### Regulatory compliance

- Emergency session handling - E-911
  - Prioritize, retrieve location information and route emergency/E911 sessions with enhanced QoS (3GPP E-CSCF)
  - Interface to external location servers (3GPP CLF)
- Priority session handling - Government Emergency Telecommunications Service (GETS)
  - Prioritize and route priority sessions with enhanced QoS
- Lawful intercept
  - **Replicate & deliver signaling (call data) and media (call content) for lawful intercept**
- Session replication for recording - for quality control and regulatory compliance requirements