Fair bandwidth usage among service subscribers

PacketController QoS solution can mitigate excessive bandwidth consumption by high-usage users, thereby promoting equitable and efficient utilization of network resources. By specifying source and destination IP addresses and leveraging Deep Packet Inspection (DPI) to identify application types, it becomes possible to impose limits on both uplink and downlink bandwidth, as well as the number of concurrent connections.

By leveraging Deep Packet Inspection (DPI), organizations can gain application-level visibility to classify over 3,000 applications across more than 40 categories. This provides granular insight into network traffic—including encrypted traffic—which is essential for enforcing effective policies. Analyzing these traffic trends facilitates strategic network planning, delivers deeper business intelligence, and supports enhanced compliance with Law Enforcement Agency (LEA) requirements, while also opening up opportunities for service monetization.

The PacketController AP500 is a 2RU dual-power appliance for 400G networks with available license at 400/520Gbps and provides a cost-effective yet powerful solution for large size ISPs.

Leveled Fairness Control

By restricting the bandwidth of high-usage subscribers during peak periods, telecommunications carriers can ensure fairer distribution of network resources, ultimately boosting customer satisfaction. Additionally, this approach allows for tiered control, enabling carriers to apply differentiated policies to various subscriber groups.

User-Level QoS with Radius Accounting Message Integration

By using the Radius attributes of accounting message form external Radius server, AP series supports identity-aware traffic shaping and it automatically maps user identity to its currently assigned IP address (either IPv4 or IPv6 or both).

Application Identification and Control

Deep Packet Inspection technology offers comprehensive application awareness by identifying and visualizing applications currently running on the network, monitoring their operational status, and empowering administrators to enforce per-application bandwidth and communication policies.

IPv4 to IPv6 Transition

Provides the measurement and management of IPv4 and IPv6 traffic simultaneously for operators of all access technologies.

DDoS Mitigation

PacketController helps you detect and mitigate Distributed Denial of Service (DDoS) attacks. Its IP anomaly filtering can protect against numerous types of attacks.

Carrier-class Gi/SGi Firewall

Protect subscribers and shield mobile core infrastructure from cyberattacks at the Gi/SGi and RAN to ensure uninterrupted operations. Consolidating security functions and CGNAT helps efficient operation and enables optimized performance.

Carrier-Grade Performance

- 1GE, 10GE, 25GE, 40GE, 100GE and 400GE ports
- Up to 520Gbps on one single hardware appliance
- Up to 750M concurrent sessions on one single hardware appliance

Bandwidth Management

- Rate limit on throughput, packet per second, connections
- Time based bandwidth management
- Monthly quota management
- DPI Management
- Web Filtering (GEO and Websites)
- High performance logging
- Subscriber Portal
- Integration with Radius accounting message for user-level traffic shaping

Networking

- Layer 2/Layer 3 support
- BGP+
- BGP Multi-path (ECMP)
- IS-IS v4/v6, OSPF v2/v3
- RIP v2/ng
- VLAN (802.1Q, QinQ)
- BFD
- Static routes & path monitoring
- Policy based routing (PBR)
- Link aggregation (802.1AX), LACP
- VXLAN
- NVGRE
- IPv4 NAT/NAPT
- IPv6 NPAT
- ACL
- Port mirroring

Flexible Licensing

- "Pay-as-you-grow" license on hardware
- From 200Mbps to 520Gbps

Extensibility

- N+M Clustering (Active-Standby, Active-Active)
- Multitenancy (Partition) Support

Firewall

- Stateful Layer 4 network firewall
- Gi/SGi firewall
- L7 application-aware firewall and visibility
- L4–L7 services consolidation
- Application layer gateways (DNS, ESP, FTP, ICMP, PPTP, RTSP, SIP, TFTP)

DDoS Protection

- Flood attack protection: SYN cookies, TCP/UDP/ICMP flood protection, DNS/HTTP flood protection
- Protocol attack protection: invalid packets, anomalous TCP flag combinations, packet size validation (ping of death)
- Resource attack protection: slowloris, slow POST, sockstress, fragmentation

Management/Monitoring

- Dedicated management port (CLI, Telnet, SSH, WUI)
- Dedicated management routing table
- Dedicated control CPU
- SNMP v1/2/3
- RBAC with AAA (LDAP, Radius, TACACS+ support)
- 802.1ab LLDP
- sFlow/IPFIX/Netflow v9
- Syslog

AP500 Hardware Platform Specification

Available License	
Throughput	400/520 Gbps
Performance	
Throughput	520Gbps
Full TCP CPS	7.5M
Concurrent Sessions	750M
Rules	128K
Partitions	512
Hardware Specification	
Processor	2 x Intel 36-core CPU
Memory	512GB
Storage	SSD (2 backup SSDs)
Hardware Acceleration	ASIC
Management Ports	Ethernet Management Port, RJ-45 Console Port
Default Network Interfaces	2 x 1GbE Copper Management
Pluggable Modules	Dual-Port 10GbE Fiber (SFP+) Quad-Port 10GbE Fiber (SFP+) Dual-Port 25GbE Fiber (SFP28) Dual-Port 40GbE Fiber (QSFP+) Dual-Port 100GbE Fiber (QSFP+) Dual-Port 400GbE (QSFP-DD)
Dimensions	500mm (W) x 600mm (D) x 88mm (H)
Weight	28 kgs
Power Supply	Hot swap Dual Power Supply
Cooling Fan	Hot swap Fans
Rails	Sliding Rails
Operating Environment	Temperature: 0-40 °C (32-104 °F) Humidity: 5% to 95%

All PacketController Hardware Appliances support N+M active-standby/active-active clustering deployment.
The specifications, performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

©Copyright 2026 PacketController Networks (www.packetcontroller.com). All rights reserved. PacketController are trademarks of PacketController Networks.