

ULTRA-HIGH-SPEED PACKET PROCESSING FOR ADVANCED NETWORK MONITORING

INTELLAVIEW HYPERENGINE PACKET PROCESSOR



FEATURES

Advanced Packet Processing Solutions

High-Performance Service Engines:

- Up to four configurable service engines (100G max per engine)
- Real-time processing across 1G/10G/40G/100G feeds

Advanced Features Available On Each Engine:

- Packet Deduplication
- NetFlow Generation
- Traffic Shaping
- Pattern Matching
- Application Filtering
- Advanced Packet Slicing

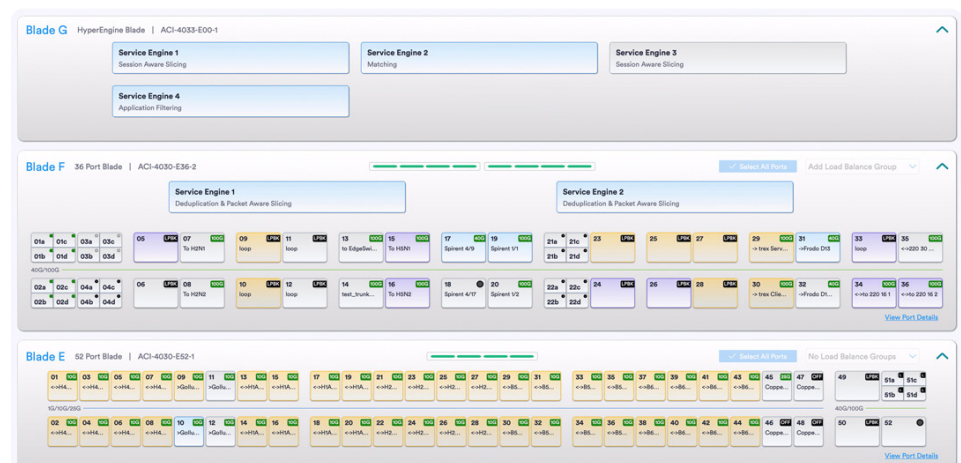
New Licensable Features:

- Application Filtering for 1600+ apps and 400+ protocols
- Session-Aware Slicing
- Pattern Matching for packets, sessions, or cross-packet
- Traffic Shaping eliminates tool oversubscription

The IntellaView HyperEngine Packet Processor enables the IntellaView platform to deliver advanced features for ultra-high-speed network infrastructures. It adds superior, industry-leading processing power for real-time packet processing and delivery of streamlined packet traffic to various network monitoring and security tools. This enhanced network visibility significantly increases the efficiency and effectiveness of network security, analytics, and performance monitoring solutions.

Each IntellaView HyperEngine blade adds up to 400G of high-performance processing service to IntellaView network visibility systems. Traffic sources can be aggregated to the HyperEngine Packet Processor to perform advanced processing.

The IntellaView HyperEngine offers four high-performance, multi-threaded network processors with flexible user-selectable service options. These service engines provide convenient configuration of advanced packet processing features including Packet Deduplication and NetFlow Generation for network monitoring.



HyperEngine Packet Processor includes four multi-threaded network processors, each supporting up to 100G capacity. Easily aggregate traffic from other blades for service processing.

PROCESSING FEATURES

Packet Deduplication

Complete visibility of large data center networks involves viewing traffic at several monitoring points. While this increases overall visibility, some packets will be monitored at multiple points creating duplicate packets that can overload network monitoring tools and affect reporting. Removing duplicate packets improves monitoring tool efficiency, accuracy, and data storage optimization. This enables monitoring tools to provide greater visibility while lowering overall costs.

The IntellaView HyperEngine blade, with up to 400G of processing capability, monitors every packet in the high-speed data stream to remove duplicates and improve tool efficiency. The HyperEngine blade enables duplicate matching across Layers 2, 3, and 4 headers, and supports a large, configurable window size of up to 500ms. Configurable options also include fields for a deduplication algorithm and inclusion/exclusion options for common encapsulations used in data centers. Another option allows the configuration to ignore particular Layer 4 TCP and/or UDP header fields. These configuration options provide additional flexibility to the user to customize what is actually considered a duplicate packet.

IPv4 Packet Duplicate Matching

ON ⬆

0	4	8	16	19	31
Version		IHL		Total Length	
Identification				Fragment Offset	
Time to Live		Protocol		Header Checksum	
Source Address					
Destination Address					

IPv6 Packet Duplicate Matching

OFF ⬆

0	4	8	16	24	31
Version		Traffic Class		Flow Label	
Payload Length			Next Header		Hop Limit
Source Address					
Destination Address					

TCP Header Matching

ON ⬆

0	4	7	16	31					
Source Port			Destination Port						
Sequence Number									
Acknowledgement Number									
Data Offset	Res	URG	ACK	PSH	RST	SYN	FIN	Window Size	
Header and Data Checksum							Urgent Pointer		

Packet Deduplication
Select any service engine to view configuration. Shown here is the deduplication screen that provides full customization of duplicate match conditions and time window size.

NetFlow Generation V5, V9, and IPFIX

The HyperEngine blade monitors network traffic and is an ideal source for generating NetFlow records. It can off-load processing from routers and other production equipment to increase efficiency and save costs; plus, consolidating NetFlow sources reduces network traffic and simplifies the monitoring architecture.

Connect any system traffic to the four service engines for NetFlow source processing of unsampled or sampled traffic flow records. The unsampled flow records contain data of every packet in the data stream for a complete representation of the traffic.

The diagram illustrates the data flow for NetFlow generation. On the left, a 'PHYSICAL DATACENTER' sends '100G Traffic' to the 'INTELLAVIEW HYPERENGINE (APPLICATION ANALYTICS)'. The HyperEngine processes this traffic and sends '10G' streams to three categories of 'EXISTING TOOLS': Security Tools, Load Balancing, and Performance Tools. Simultaneously, the HyperEngine sends 'IPFIX Records' to a 'RECORD COLLECTOR'. The IPFIX records include Flow Record Data, Application ID, App Group ID, and Session Data.

NetFlow Generation

Process packets from multiple ports to remove duplicates or generate NetFlow records, directing traffic of interest to security and performance tools.



Traffic Shaping

With the Traffic Shaping feature (sometimes referred to as “rate limiting”) of IntellaView’s HyperEngine, traffic can be limited to a user-specified average rate by buffering packets that exceed that rate. The buffered data is released at a steady, even flow so it remains at or below the target bandwidth of the appliance to avoid tool oversubscription.


Traffic Shaping offers tool-saving capabilities to maintain optimum traffic flow, especially when certain appliances are not designed to handle traffic above a specific rate for extended periods. Additionally, tools typically have minimal buffer space, so packets are dropped if a tool is bombarded with more traffic than it can handle. Aside from dropping packets, a tool that is overwhelmed may be unable to properly perform its functions.

Each one of the HyperEngine service engines can buffer millions of packets — shared across all connections — to ensure your existing tools are not overburdened by data speeds that fluctuate above a tool’s optimum rate.

123 *** Pattern Matching

This feature of the IntellaView HyperEngine allows SecOps and NetOps teams to match packet contents and filter for specific traffic. Users can create search parameters on individual packets and sessions to identify data based on patterns in any part of the packet payload. APCON’s Pattern Matching uses regular expressions (regexs) to match packet contents in near real time. The HyperEngine also draws on deep packet inspection technology (DPI) to help data centers’ security tools receive only the packets they need. After finding pattern matches, packets can be masked, passed, or dropped as appropriate to comply with privacy guidelines and to safeguard the network.

Pattern Matching is a vital part of ensuring privacy standards and compliance established in regulations such as HIPAA and PCI by identifying and masking sensitive data. This feature can search for specific data patterns such as social security numbers or credit card numbers. Once a pattern is identified, the matched data can be masked and the packet forwarded; or the packet can be dropped, or simply forwarded unchanged. Another use of this feature is searching for known virus threats or other types of potentially dangerous traffic, then forwarding any identified packets directly to a security tool. The Pattern Matching feature also allows the import of a regular expression signature file to simplify configuration.



Layer 7 Application Filtering

With IntellaView’s HyperEngine packet processor, users can identify and filter network traffic for Layer 7 applications and protocols. Any of its four service engines can leverage advanced DPI (deep packet inspection) and heuristics to identify over 1,600 applications and more than 400 protocols in real time with a high degree of accuracy and virtually no false positives.

Empower your SecOps and NetOps teams to maximize the efficiency of your monitoring and security tools by filtering out low-risk, high-bandwidth applications like YouTube, Facebook, Skype, etc. Inspecting flows to identify specific applications or protocols can save money by preventing existing tools from becoming overburdened, even as traffic increases.

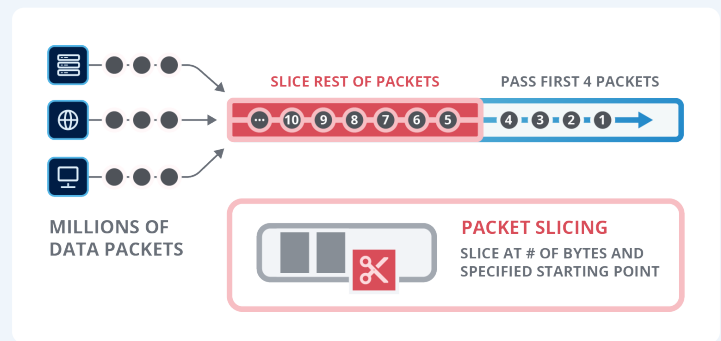
With Layer 7 Application Filtering, you get complete control over the traffic traversing your network by identifying protocol types, standard applications, and apps with security flaws or known vulnerabilities.



Advanced Packet Slicing

The Packet Slicing feature removes packet payload that is not necessary for certain network performance analysis and analytic tools, thus increasing the efficiency and effectiveness of these tools. It also ensures data privacy for compliance with regulations such as HIPAA and PCI.

The Session-Aware Slicing feature allows a certain number of packets in a session to pass through unsliced, before slicing all remaining packets in the session. A session is defined as a time-delimited, two-way link that enables the exchange of information between two or more entities. This is useful if you want to see the initial, unencrypted packets that establish a TLS/SSL session, and then slice the remaining packets.



Session-Aware Slicing

Session-Aware Packet Slicing allows the first specified packets to pass and slices remaining session based on user-configurable attributes.

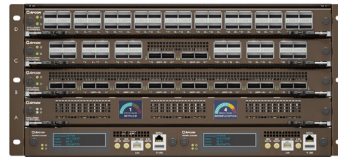
INTELLAVIEW NETWORK VISIBILITY PLATFORM



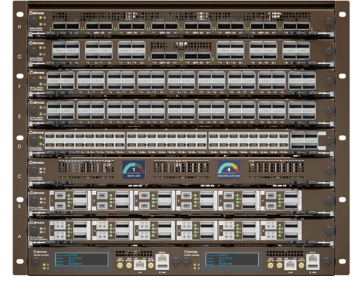
1.5RU | Single blade



3RU | Up to 2 blades



5RU | Up to 4 blades



9RU | Up to 8 blades

The IntellaView HyperEngine blade is a piece of APCON's IntellaView network visibility platform and is compatible with all IntellaView chassis. The HyperEngine blade is best suited for use in the 3RU, 5RU, and 9RU chassis.

The IntellaView blade-swappable chassis platform consists of the ACI-4010-AC 1.5RU, ACI-4020-AC 3RU, ACI-4040-AC 5RU, and ACI-4080-AC 9RU chassis. The 3RU, 5RU, and 9RU chassis can be configured with two front-facing controller cards with a touchscreen to provide failover operation for uninterrupted continuity, and much more.

The 3RU, 5RU, and 9RU chassis can be configured with up to six next-generation switch fabric cards, providing full mesh connectivity with the blades through the backplane, and offering a dramatic increase in bandwidth potential, with up to five times more than the previous generation products. The more fabric cards you install inside the chassis, the higher the blade-to-blade traffic bandwidth.

IntellaView HyperEngine Blade Specifications | ACI-4033-E00

Processing Performance	Up to four service engines; total 400G*
Memory	64GB of DDR4 per service engine
Licensed Services:	Packet Deduplication, NetFlow Generation, Pattern Matching, Traffic Shaping, Application Filtering, Advanced Packet Slicing
Weight	16.5 lbs (7.5 kg)
Power	750-900 Watts / 2560-3072 BTU
Dimensions	17.24" W × 17.46" D × 1.63" H (43.78 W × 44.32 D × 4.11 H cm)
Temperature	Operating: 32 to 113 °F (0 to 45 °C); Storage: -40 to 158 °F (-40 to 70 °C)
Relative Humidity	Operating: 10-85%; Storage: 0-95% non-condensing

*Performance indicates the network processor capacity. Actual performance varies by the selected feature and packet size.



APCON, Inc. • 9255 SW Pioneer Court, Wilsonville, Oregon 97070
 +1 503-682-4050 • 1-800-624-6808 • @APCON • company/APCON • apcon.com
 © 2020-2024 APCON, Inc. All Rights Reserved. APCON is a registered trademark of APCON, Inc.

19063-0724