DATA SHEET

HIGH-SPEED PACKET PROCESSING FOR NETWORK VISIBILITY

IntellaView Advanced Features

Advanced Packet Processing Solutions That Drive Efficiency in Network Monitoring and Security

FEATURES

Packet Deduplication:

- High capacity: up to 600Gbps per HyperEngine processor blade; up to 400Gbps per 36-port blade and up to 3.2Tbps per 9RU system
- Configurable duplicate match criteria on layers 3 & 4
- Simultaneous IPv4/IPv6 deduplication
- Real-time processing across 1G/10G/25G/40G/100G feeds
- Capable of setting duplicate match that ignores encapsulation header

Packet Slicing:

- Real-time processing across 1G/10G/25G/40G/100G feeds
- New CRC calculated and appended
- Increase tool processing efficiency

NetFlow Record Generation:

- Generate traffic statistics
- Off-load processing from routers and production equipment
- Unsampled flow records contain data of every packet in the data stream for a complete representation of the traffic

Tunnel Initiation:

- Encapsulate GRE tunnel and direct traffic over IPv4/IPv6 networks
- Direct traffic between IntellaView at remote locations and IntellaView at the core data center
- Direct traffic to on-premises or cloud-based tools
- Available on every 10G/25G/40G/100G port

Tunnel Termination:

- Decapsulates tunnel traffic to ensure tool compatibility
- Supported protocols include: GRE, NVGRE, VxLAN, and ERSPAN I, II & III
- IntellaTap-VM virtual monitoring compatible

Protocol Header Stripping:

- Strips protocol header from packets for optimized tool processing
- New CRC calculated and appended
- Supported protocols include: GRE, NVGRE, VxLAN, VLAN, ERSPAN I, II & III, FabricPath, MPLS, MPLS PWE, MPLS over GRE

The IntellaView hybrid network visibility platform — with advanced, high-speed packet processing features — increases efficiency and visibility for security and performance monitoring solutions.

Next-generation data centers face a variety of network monitoring and security challenges. Duplicate packets create one of the biggest challenges for IT and security personnel, including monitoring tool oversubscription, false positives, and inaccurate performance reporting. It is estimated that network monitoring traffic can consist of up to 55 percent duplicate packets that diminish tool bandwidth, reduce storage availability, and decrease monitoring and security tool effectiveness. APCON's advanced high-speed packet processing features such as packet deduplication, packet slicing, and protocol header stripping can significantly reduce network traffic feeding to various network security and performance monitoring tools, resulting in increased utilization, effectiveness, and performance.

HIGH-SPEED PACKET PROCESSING FEATURES

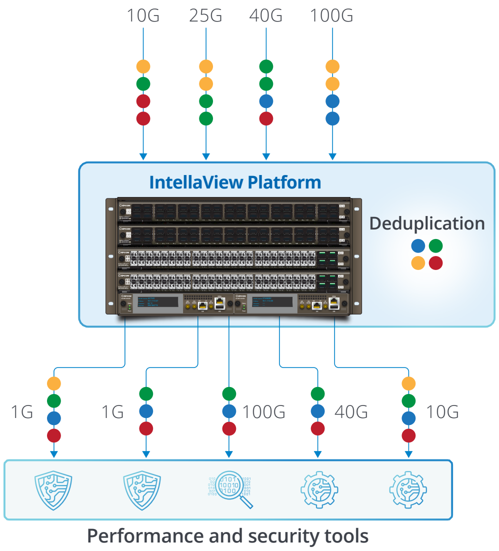
Packet Deduplication

Complete visibility of an enterprise data center 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 security and monitoring tools and affect reporting. Removing duplicate packets improves the efficiency and accuracy of these tools and reduces recording space requirements. This enables security and monitoring tools to provide greater visibility while lowering overall costs.

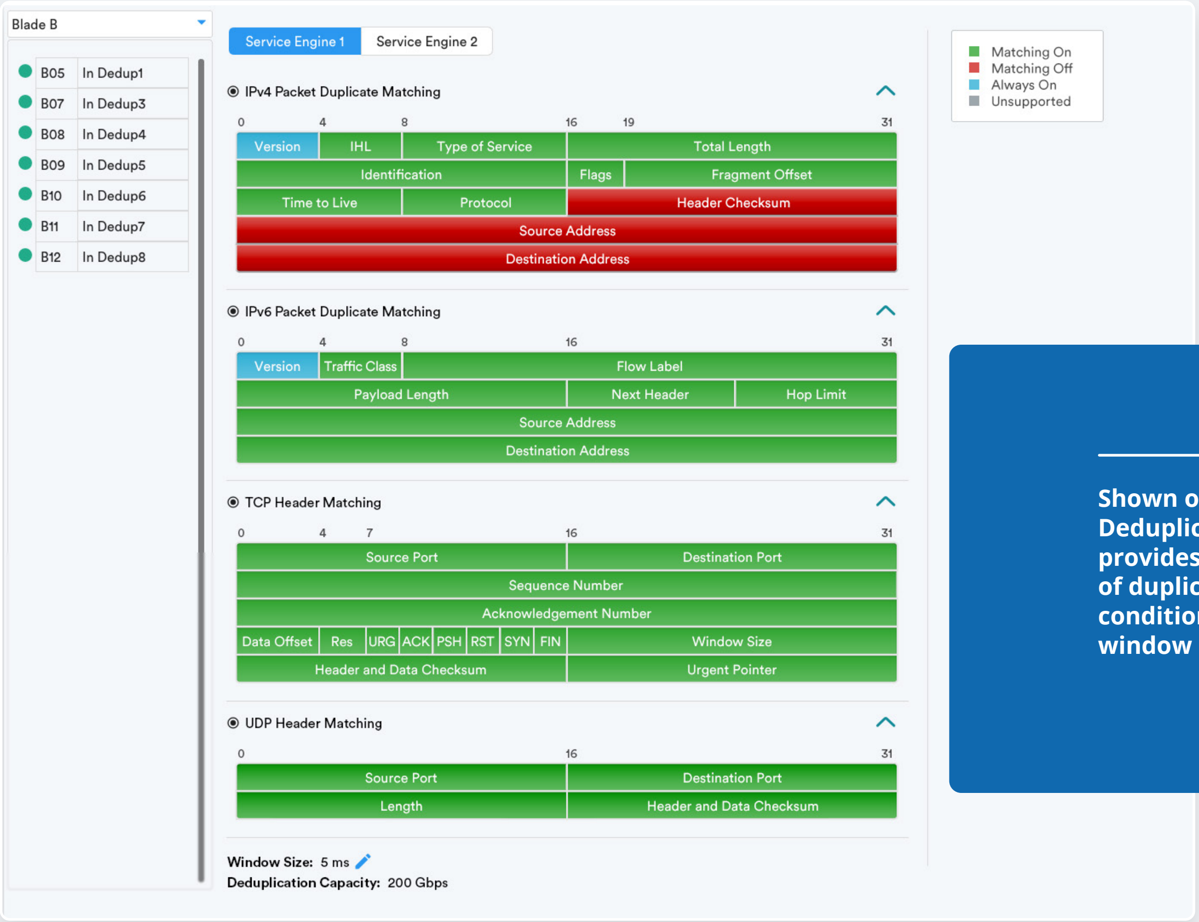
IntellaView can monitor every packet in the data stream to remove duplicates and improve tool efficiency. It enables duplicate matching across layers 3 and 4 headers. Configurable selections also include fields for the deduplication algorithm. Another selection allows configuration to ignore particular Layer 4 TCP and/or UDP header fields. These configuration selections provide additional flexibility to the user to customize what is actually considered a duplicate packet.

There are two deduplication Service Engines for each ACI-4030-E36-2 blade that offer a maximum of 400 Gbps deduplication capacity.

The IntellaView HyperEngine blade (ACI-4033-E00-1), with 600Gbps of processing capability, monitors every packet in the high-speed data stream to remove duplicates and improve tool efficiency. It supports a large, configurable window size of up to 500ms. It can be configured to have up to six deduplication Service Engines for each ACI-4033-E00-1 blade.



Packets are processed from multiple ports to remove duplicates, directing traffic of interest to security and performance monitoring tools.



Blade B

● B05	In Dedup1
● B07	In Dedup3
● B08	In Dedup4
● B09	In Dedup5
● B10	In Dedup6
● B11	In Dedup7
● B12	In Dedup8

Service Engine 1 | Service Engine 2

🟩 Matching On
🟥 Matching Off
🟦 Always On
⬜ Unsupported

◉ IPv4 Packet Duplicate Matching

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

◉ IPv6 Packet Duplicate Matching

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

◉ TCP Header Matching

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

◉ UDP Header Matching

0 16 31
Source Port | Destination Port
Length | Header and Data Checksum

Window Size: 5 ms
Deduplication Capacity: 200 Gbps

Shown on the left is the Deduplication screen that provides full customization of duplicate match conditions and configurable window size in milliseconds.

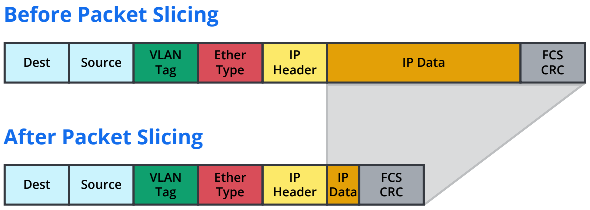
Protocol Header Stripping

Data packets are often encapsulated using various protocol headers which help these packets reach their ultimate destination. This is particularly important for hybrid environments spanning cloud, virtualized, and on-premise infrastructures. However, these protocol headers are not needed or used by various monitoring, diagnostic, and security tools. By stripping away the header information, overhead is reduced and such tools can operate at maximum efficiency. Types of protocol headers that can be stripped on the IntellaView blade include GRE, NVGRE, VxLAN, VLAN, ERSPAN I, II & III, FabricPath, MPLS, MPLS PWE, and MPLS over GRE. For certain protocols (GRE and VxLAN), the IntellaView can also perform both Deduplication and Protocol Header Stripping on each packet as it passes through the IntellaView blade.

Packet Slicing

The Packet slicing feature of IntellaView can remove confidential information to comply with regulatory requirements and leave the packet headers intact. Legislation such as HIPAA, PCI and others demand data confidentiality; stripping sensitive payload data from packets before they go to monitoring tools ensures that any sensitive data is not stored outside secure boundaries. Packet slicing increases tool utilization while reducing data volume, creating greater efficiency, security, and reduction in costs.

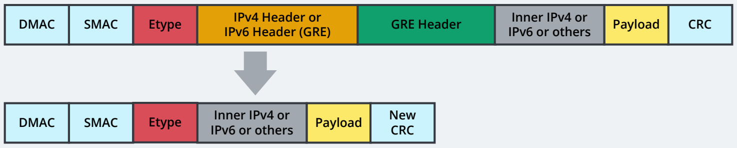
IntellaView supports packet slicing on all packets at line rate. Network engineers may configure each port on the blade to truncate each packet that passes through the port to a preset number of bytes, to reduce bandwidth load at the monitoring device, or to remove sensitive data from the monitoring stream. A new checksum (CRC) is calculated and appended.



Packets are sliced at a defined number of bytes to reduce bandwidth load at security and monitoring devices and/or to remove sensitive data.

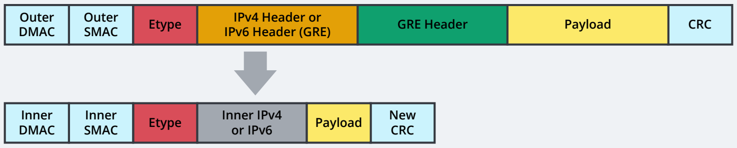
Protocol Stripping

GRE I Stripping the outer IP and GRE headers

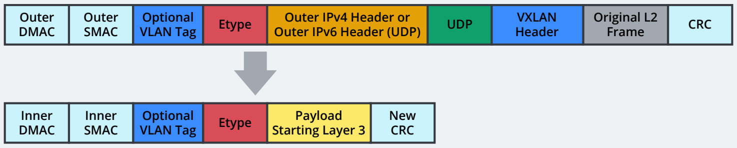


DMAC
SMAC
Etype
IPv4 Header or IPv6 Header (GRE)
GRE Header
Inner IPv4 or IPv6 or others
Payload
CRC
DMAC
SMAC
Etype
Inner IPv4 or IPv6 or others
Payload
New CRC

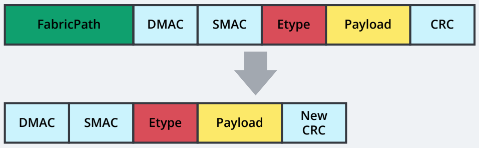
NVGRE I Stripping the outer Ethernet, outer IP, and GRE headers



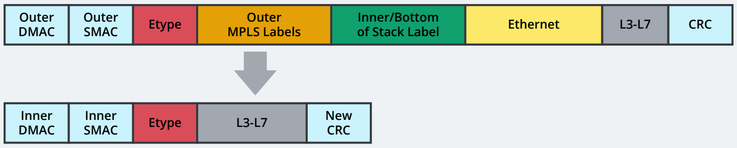
VXLAN I Stripping the outer MAC, outer IP, UDP, and VXLAN headers



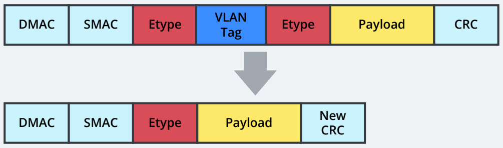
Cisco FabricPath I Stripping the Cisco FabricPath header



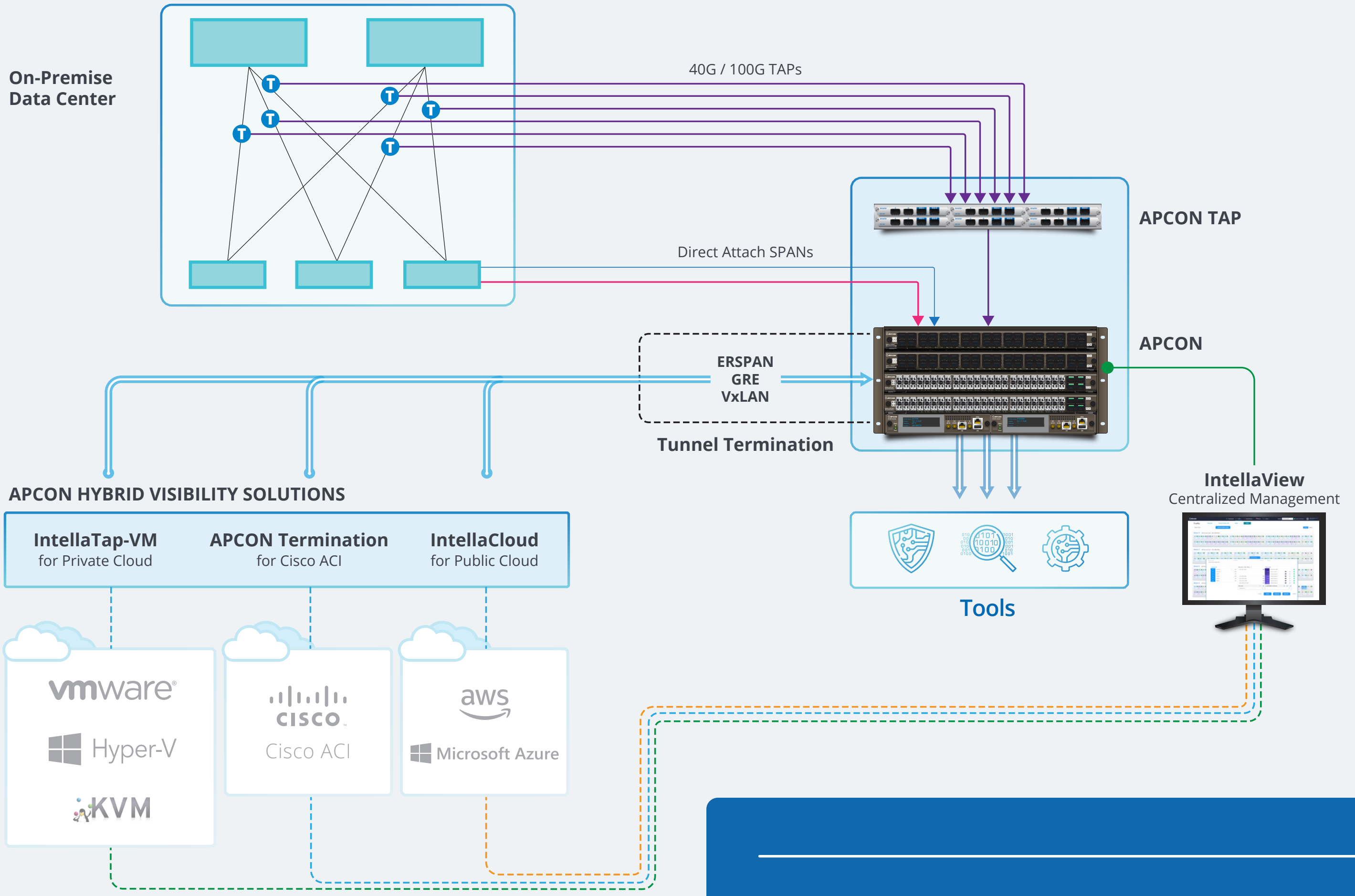
MPLS I Stripping outer MAC, MPLS Etype, all outer MPLS labels, and inner/bottom label



VLAN I Stripping all VLAN tags (up to 8 tags)



APCON's IntellaView performs protocol stripping on any port, up to 288 40G or 100G ports in a 9RU chassis.



IntellaView is part of APCON's hybrid network visibility solution which also includes IntellaTap-VM and IntellaCloud, providing tunnel termination to monitor high-speed, high-volume traffic of interest.

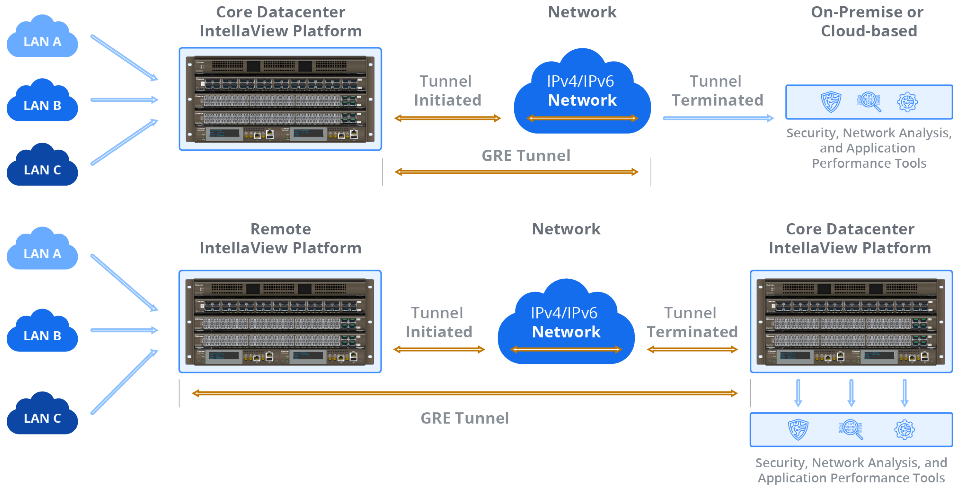
Tunnel Termination

Terminating encapsulated tunnel traffic enables multiple applications including virtual network monitoring. The IntellaTap-VM virtual TAPs use tunnel encapsulation to forward VM traffic of interest to the monitoring network while the Tunnel Termination feature decapsulates the tunnel traffic to ensure tool compatibility. The IntellaView Tunnel Termination supports multiple types of tunnels including GRE, NVGRE, VxLAN, and ERSPAN Types I, II, and III.

GRE Tunnel Initiation

The GRE Tunnel Initiation offers the ability to receive incoming traffic flows, encapsulate each packet and redirect the traffic to another destination, either on-premises or in the cloud. Traffic can also be directed between remote locations and the core data center.

When combined with IntellaTap-VM and Titan, the GRE Tunnel Initiation provides a unified virtual and physical monitoring solution that delivers complete hybrid network visibility and improves monitoring and security tool efficiency.

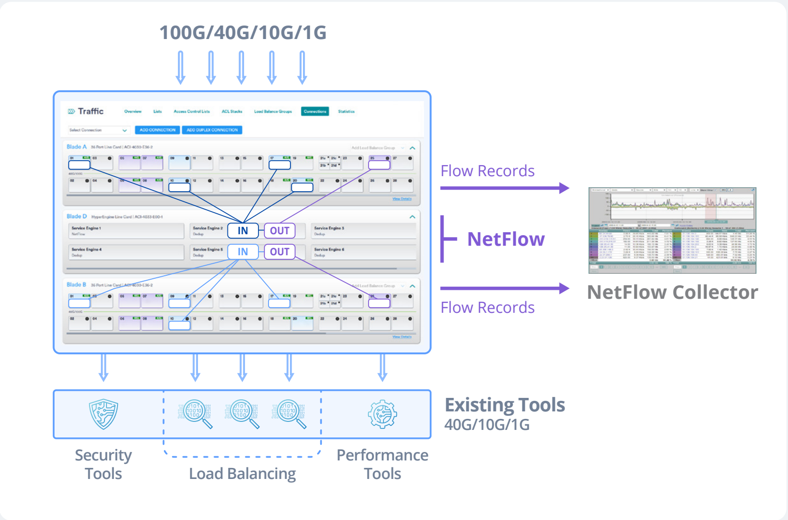


(Top) To on-premises or cloud-based tools
(Bottom) Between remote locations and the IntellaView at the core datacenter

NetFlow V5, V9 and IPFIX

The HyperEngine 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.

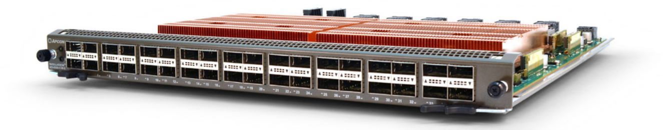
Connect any system traffic to the six service engines for NetFlow source processing of unsampled or sampled traffic flow records. The unsampled flow records contain data of every packet in the data stream for a complete representation of the traffic.



NetFlow Generation with IntellaView HyperEngine

INTELLAVIEW BLADES

The APCON IntellaView consists of the ACI-4030-E36 and the ACI-4030-E52 Multi-Function Blades and ACI-4033-E00 HyperEngine Packet Processor Blade. The aggregation and filtering technology of the multi-function blades make it easy to monitor high-speed networks. With the broadest range of advanced features including packet slicing, protocol stripping, load balancing, port tagging, tunnel termination, tunnel initiation, packet deduplication (ACI-4030-E36-2 blade or ACI-4033-E00-1 blade only) and NetFlow generation (with ACI-4033-E00-1 blade), network engineers are confident the right traffic is delivered to the right tools all the time.



40G and 100G Port Density

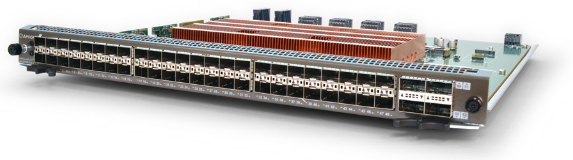
The ACI-4030-E36 blade is a highly flexible packet aggregation switch that includes the following port and density options.

- The ACI-4030-E36 blade supports 36 × 40/100G front panel ports capable of supporting 40G and 100G QSFP28 fiber modules.
- The QSFP28 ports support port breakout. Port breakout breaks one 40G port into 4 × 10Gbps ports or one 100G port into 4 × 25Gbps ports.
- The ACI-4030-E36-2 blade includes a hardware module that supports the Packet Deduplication feature.
- Supported features include Port Tagging, Packet Slicing, Protocol Header Stripping, Tunnel Termination, Tunnel Initiation, and Packet Deduplication (E36-2 only).

HyperEngine Packet Processor

The HyperEngine blade delivers advanced features for ultra-high-speed network infrastructure. It adds superior, industry-leading processing power (600Gbps) to the IntellaView for real-time packet processing and enhanced network visibility with significantly increased efficiency and effectiveness of the network security, analytics and performance monitoring solutions.

- 6 configurable service engines.
- Real-time processing across 1G/10G/40G/100G feeds.
- Deduplication
- NetFlow generation



1/10/25G and 100G Port Density

The ACI-4030-E52 blade is a highly flexible packet aggregation switch that includes the following port and density options.

- 48 SFP+ ports capable of supporting 1G, 10G, or 25G.
- 4 QSFP28 ports capable of supporting 40G or 100G.
- The QSFP28 ports support port breakout. Port breakout breaks a 40G port into 4 × 10Gbps ports or a 100G port into 4 × 25Gbps ports using breakout cables.
- Supported features include Packet Slicing, Protocol Header Stripping and Tunnel Termination, Tunnel Initiation, and Packet Deduplication (E36-2 only).

ORDERING INFORMATION

Part Number	Description
ACI-4030-E36-1	IntellaView 36 Port Blade – Supports 36 × 40/100G ports
ACI-4030-E36-2-1	IntellaView 36 Port Blade w/ Advanced Feature Module – Supports 36 × 40/100G ports (includes Advanced Feature Module) – Includes Deduplication Software License (ACI-9300-002)
ACI-4030-E52-1-1	IntellaView 52 Port Blade – Supports 48 × 1/10/25G ports – Supports 4 × 40/100G ports
ACI-4030-001	Advanced Feature Module for ACI-4030-E36-1 blade – Enables upgrade of ACI-4030-E36-1 blade to ACI-4030-E36-2 blade – ACI-4030-E36-1 must be returned to APCON for upgrade – Software Licenses Sold Separately
ACI-4033-E00-1-1	IntellaView HyperEngine High-Speed Packet Processor
ACI-9300-002	Deduplication Software License for ACI-4030-E36-2 blade
ACI-9300-004	IntellaView Tunnel Management License (includes Tunnel Initiation and Tunnel Termination)
ACI-9300-010	IntellaView Protocol Stripping License
ACI-9300-012	IntellaView Packet Slicing License
ACI-9300-014	IntellaView Advanced Services Bundle License (includes Tunnel Management, Protocol Stripping, and Packet Slicing Licenses)
ACI-9330-002	Deduplication Software License for ACI-4033-E00-1-1 HyperEngine blade
ACI-9330-004	IntellaView NetFlow Generation License for ACI-4033-E00-1-1 HyperEngine blade

APCON SOLUTIONS

APCON leverages its proprietary IP and deep expertise to provide flexible, focused solutions across

- **Government**
- **Healthcare**
- **Higher Education**
- **Financial Services**
- **Manufacturing**
- **Telecommunications**

APCON solutions provide the flexibility and means to gain visibility to data more efficiently, resulting in savings across the board, including time, resources, and maintenance.

SERVICE AND SUPPORT

APCON's professional services team of certified engineers has years of experience optimizing network visibility strategies for businesses across the globe. In addition to providing installation assistance of existing analysis tools, this team proudly provides around-the-clock troubleshooting services and support.

ABOUT APCON

A privately held corporation, APCON is headquartered near Portland, Oregon, where it has operated since 1993. APCON's in-house staff manages product design and development, manufacturing, quality assurance and final testing, customer training and long-term servicing of its solutions — whether for a system with a single switch or a global installation that spans across multiple geographical or cloud locations.

APCON
Solutions for Networks

APCON, Inc. ▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070
+1 503–682–4050 ▪ 1–800–624–6808 ▪ **apcon.com**
@APCON ▪ company/APCON