SOLUTION BRIEF

MONITORING ACI FABRICS

With APCON IntellaView Network Visibility Solutions

Application Centric Infrastructure (ACI)

Cisco's Application Centric Infrastructure (ACI) provides network and data center architects/operators a new level of automation and scale. With ACI, there are new approaches to network-wide management and policy along with underlying protocols that affect monitoring options. This overview provides a framework of monitoring options along with insights to leveraging APCON's network visibility solutions to maximize the ROI of existing network/security tools.

APCON has developed solutions for a comprehensive approach to gain insight into physical, virtual, and cloud networks. The scalable family of IntellaFlex XR systems can accommodate evolving network fabrics, such as the Cisco ACI fabric and the need for higher-port-count 40G and 100G environments, all while providing packet processing functions to allow organizations to maintain ROI on their existing monitoring and security tool investments.

This Technical Brief will highlight options for holistic monitoring of Cisco ACI environments using APCON network visibility solutions. Leveraging new concepts within Cisco ACI fabrics and combined with packet processing, capture, VM analysis, and tool optimization features on the APCON platform allows best-of-breed capabilities for holistic network monitoring.

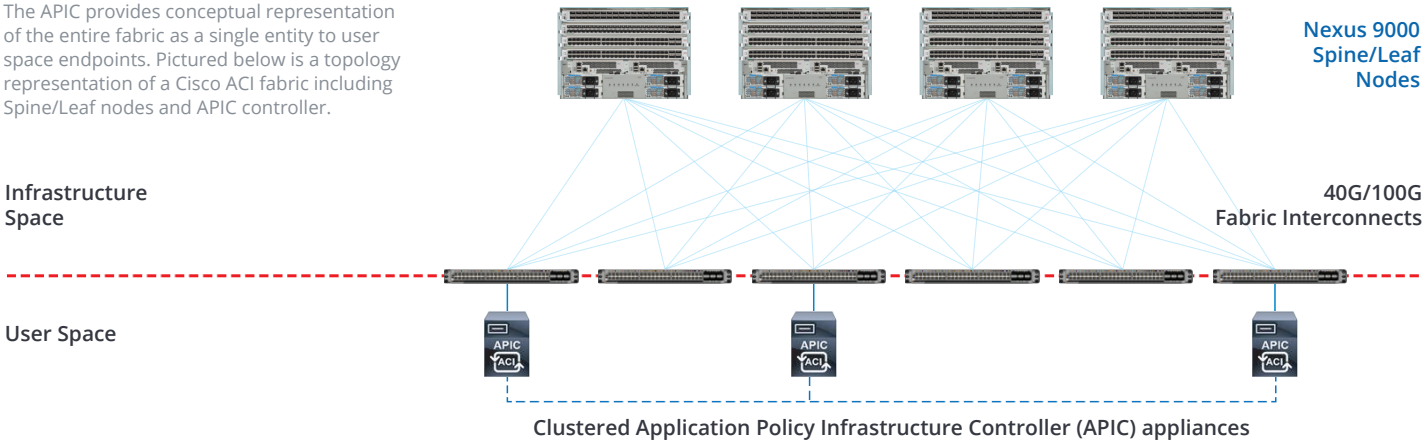
Concepts covered in this document include:

- Cisco ACI concepts/components
- Monitoring options using APCON network visibility solutions
- APCON Tool Optimization features
- Integrated APCON capture/VM analysis options

Cisco ACI concepts and components

Cisco ACI abstracts underlying component configuration via Application Network Profiles. Policies define interaction between Application Profiles and End Point Groups. Implemented in a leaf-spine fabric, routing is enabled between any two endpoints. In addition, overlay protocols such as a virtual extensible local area network (VXLAN) allow workloads to exist anywhere in the network. For management, the Application Policy Infrastructure Controller (APIC) manages and configures policy switches in the ACI fabric. The APIC is central control point for all policies and can rapidly provision or reconfigure hardware as needed.

The APIC provides conceptual representation of the entire fabric as a single entity to user space endpoints. Pictured below is a topology representation of a Cisco ACI fabric including Spine/Leaf nodes and APIC controller.



For networking hardware, the following components are needed to implement a Cisco ACI fabric:

- Nexus 9000 series switches running in ACI mode
- Application Policy Infrastructure Controller (APIC) deployed in clustered configuration

Topology features the following physical and virtual constructs:

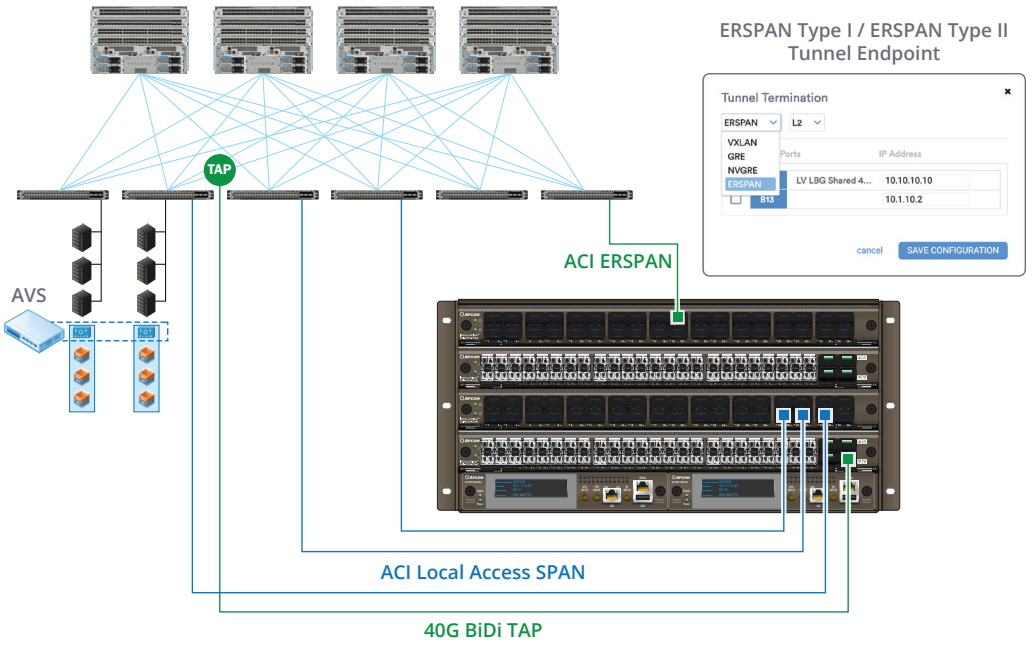
- The physical Spine and Leaf fabric architecture
- The ACI VXLAN overlay, which enables the decoupling from the physical network and the creation of virtualized L2 segments regardless of the endpoint location

Cisco ACI Traffic Monitoring

Cisco ACI presents network architects and operators with new levels of scale, automation, and ease of deployment. Understanding the monitoring options is important to complement these deployment innovations to attain comprehensive monitoring. Below is a high-level overview of how an APCON visibility solution can be used to complement a Cisco ACI deployment with conceptual options for gaining access to monitor feeds and data. Subsequent sections will cover these in more detail.

Topics will include:

- Cisco ACI SPAN types
- APCON use cases for capturing Cisco ACI SPAN traffic
- TAP options
- Cisco ACI Copy Services
- NetFlow Generation



Within a Cisco ACI fabric, placing TAP points between the spine and the leaf switches is an option to consider with additional setup covered later in this paper. It is important to note that TAP points will likely involve use of BiDi optics which are supported by APCON TAPs and QSFP ports. In addition, encapsulation and virtualization concepts are key considerations. A Cisco ACI Nexus fabric will normalize all traffic between leaf and spine by encapsulated Cisco Virtual Extensible LAN (VXLAN) protocol. APCON network visibility solutions optimize tool performance by factoring VXLAN in the deduplication hashing scheme and decapsulating VXLAN feeds. Previous monitoring concepts of TAP or SPAN rule of thumb still stand. It is important to consider some of the new options for Cisco ACI SPANs.

SPAN concepts in Cisco ACI

Cisco ACI introduces a new logical networking concept Endpoint Group (EPG) for mapping applications to the network. EPGs act as a collection of applications and components used for forwarding and policy definition. This is a key concept in enabling dynamic network provisioning as EPGs consume hardware resources only when member endpoints (tenants) are present. EPGs will expand or contract in real time as tenants and workloads move around a datacenter. There are monitoring concepts that still apply such as SPAN/ERSPAN.

SPAN Types in Cisco ACI

From an APCON monitoring setup perspective, it is critical to understand ERSPAN type based on SPAN type selected. Below is a brief description of SPAN types along with type methodology. The three SPAN options are as follows in Cisco ACI environments.

Access SPAN – Mirrors all traffic to and from leaf host ports locally with source and destination on the same leaf switch or across multiple leaf switches with a remote destination

Tenant SPAN – Mirrors all traffic to and from EPGs associated to a common tenant to a remote destination

Fabric SPAN – Mirrors all traffic to and from a spine switch to a remote destination

Access, Tenant, and Fabric SPANs use the encapsulated remote extension of SPAN (ERSPAN) Type I, while Fabric SPAN uses ERSPAN Type II. APCON supports all Cisco ACI SPAN types. Configuration of these SPAN and ERSPAN instructions can be found in the **Configuring SPAN chapter of the APIC NXOS CLI User Guide.**

The Cisco ACI SPAN options offer different levels of visibility. These factors are summarized below.

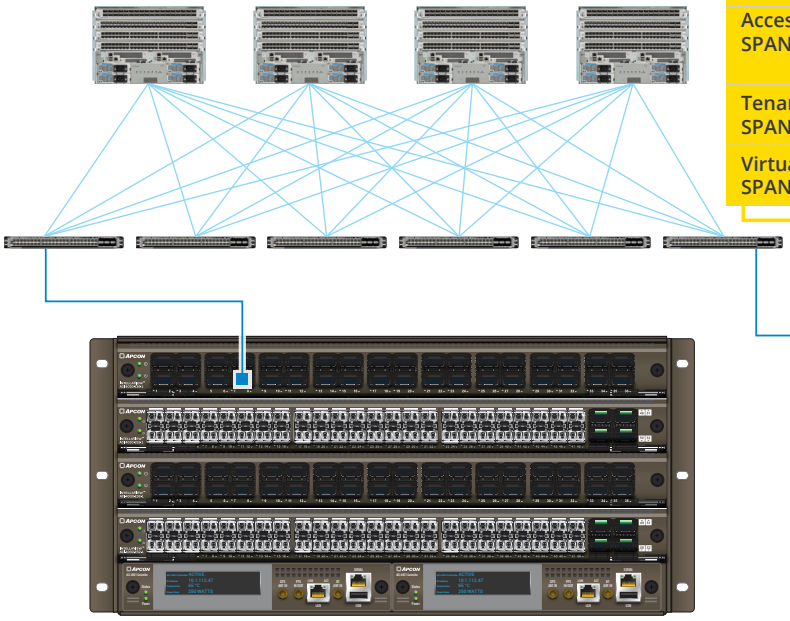
APCON platforms enable compatibility with all available SPAN and overlay options in a Cisco ACI environment.

Tenant SPAN	Fabric SPAN	Access SPAN
• Aggregates SPAN sessions across multiple switches • Mirrors traffic to/from specified Endpoint Group (EPG) • ERSPAN only • ERSPAN Type I encapsulation • No filtering possible	• Source must be fabric port • Mirrors traffic to/from Spine switches • ERSPAN only • ERSPAN Type II encapsulation • Supports aggregation of multiple switches • Filterable by private network or bridge domain	• Source must be host port • Mirrors traffic to/from Endpoints (Leaf switch host ports) • Local SPAN or ERSPAN • ERSPAN Type I encapsulation • Supports aggregation of multiple switches • Filterable by tenant, application profile, or EPG

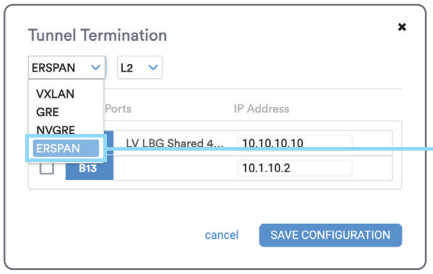
Cisco ACI SPAN sessions utilize ERSPAN Type I & II for export and can be terminated on HyperEngine or IntellaStore.

SPAN Type	Source	Filter	Destination
Fabric SPAN	Fabric port	• Bridge domain • Private network	Remote (ERSPAN Type II)
Access SPAN	Access port	• Tenant • Application profile • Endpoint group	Remote (ERSPAN Type I)
Tenant SPAN	Endpoint group	—	Remote (ERSPAN Type I)
Virtual SPAN	VM interface	—	Remote (ERSPAN Type I)

Configuring SPAN sessions from Cisco ACI deployments



ACI SPAN sessions centrally configured on APIC Controller



Leverage any IntellaView port to terminate sessions

For the Cisco ACI environment, the following shows a conceptual setup to configure the SPAN source from within the Cisco ACI environment via APIC and configuring an APCON installation to receive and decapsulate this feed.

Implementing APCON Network Visibility

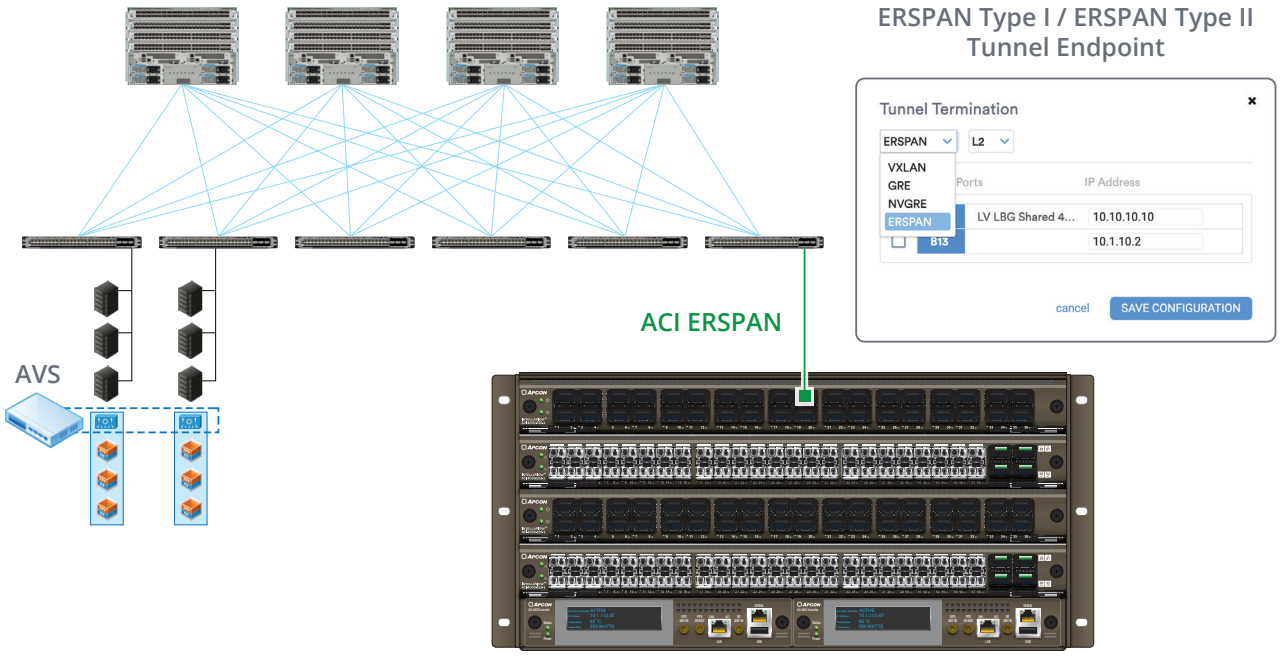
Receiving SPAN Types on APCON IntellaView Platform
Tenant, Fabric, or Access SPANs are centrally configured on Cisco APIC. Configuring ERSPAN Type I or II requires a destination IP address set on an APCON port. APCON supports ERSPAN decapsulation options on any ports. IntellaView blades terminate tunneled traffic as required by Cisco ACI and virtual network environments. This includes support for decapsulation of all current ACI transport protocols.

Cisco SPAN Guidelines and Restrictions

There are specific configurations needed when setting up SPAN monitor feeds on Cisco ACI environments.

- SPAN traffic competes with user traffic for switch resources. To minimize the load, configure SPAN to copy only the specific traffic that you want to analyze.
- A SPAN source will take an entire port for monitoring traffic from external sources.
- Tenant and Access SPANs use the encapsulated remote extension of SPAN (ERSPAN) Type I, while Fabric SPAN uses ERSPAN Type II.
- ERSPAN destination IPs must be learned in the fabric as an endpoint.
- SPAN supports IPv6 traffic but the destination IP for the ERSPAN cannot be an IPv6 address.

Refer to the **Cisco APIC Troubleshooting Guide** for more information.



Deployment Options: ACI ERSPAN Deployment

For ERSPAN deployments, one or more IP addressable ports will be exposed to the Cisco ACI fabric and connected to an APCON IntellaView port. The blade will provide the functionality to set IP destination addresses and decapsulate appropriate ERSPAN Type feeds. SPAN feeds will be configured from the Cisco ACI environment. Once set, defined traffic from anywhere in the fabric will be sent to the specified APCON destination port.

Within the IntellaView GUI, set the "Tunnel Termination" option with the appropriate IP address and De-Encapsulate option.

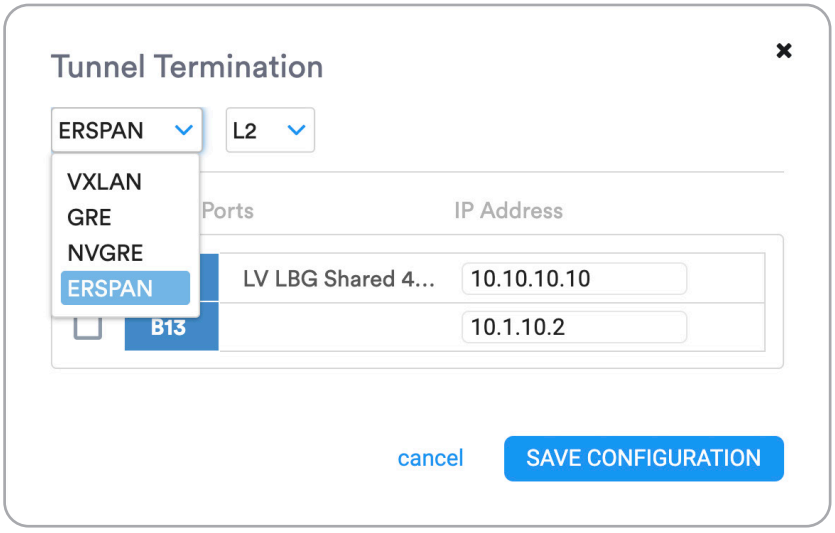
APCON Network Visibility Solution

ACI-4030-E36-2-1: Multi-Function Blade

- Supports 36 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation
  - Deduplication

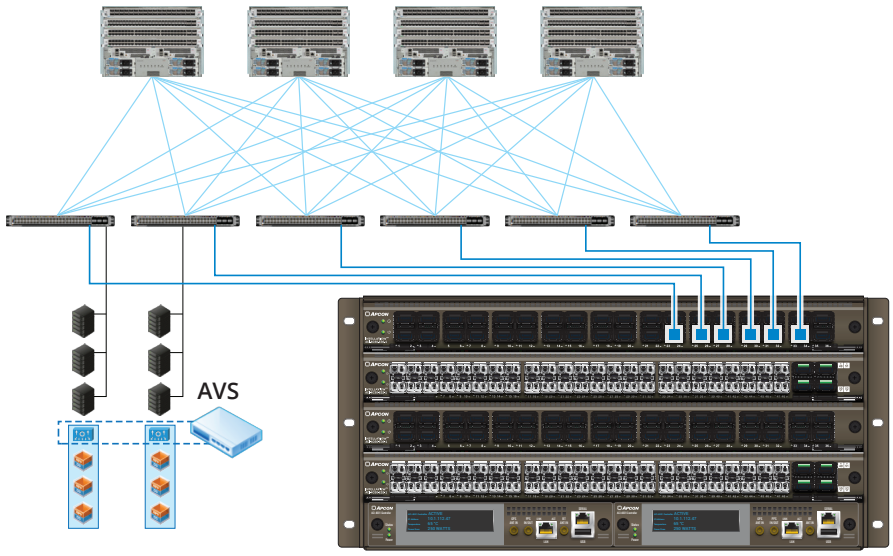
ACI-4030-E52-1-1: Multi-Function Blade

- Supports 48 ports of 1G/10G/25G
- Supports 4 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation



Cisco ACI Local SPAN Deployment

For local SPAN deployments in Cisco ACI, a SPAN session is typically set on each of the leaf switches providing local monitor feeds from across the ACI fabric. Standard ports are used on the APCON IntellaView platform to receive feeds with appropriate 1G/10G/25G/40/100G port rate setting. The SPAN feeds will be configured from Cisco ACI environment.



APCON Network Visibility Solution

ACI-4030-E36-2-1: Multi-Function Blade

- Supports 36 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation
  - Deduplication

ACI-4030-E52-1-1: Multi-Function Blade

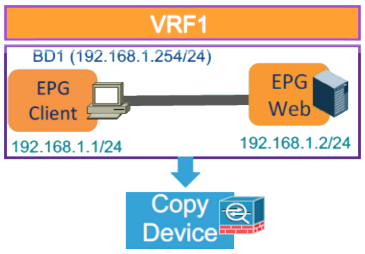
- Supports 48 ports of 1G/10G/25G
- Supports 4 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation

Cisco ACI Copy Services

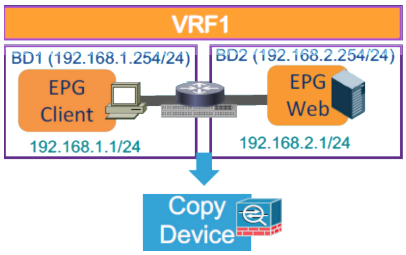
The Cisco ACI copy services feature is new starting with ACI 2.0 Release. Unlike SPANs that duplicate traffic, copy services enable selectively copying traffic of interest between endpoint groups based on established user-defined contracts.

In addition, copy services do not add encapsulation headers to the copied traffic. It is recommended to check hardware specifications for availability (Nexus 9300-EX or newer).

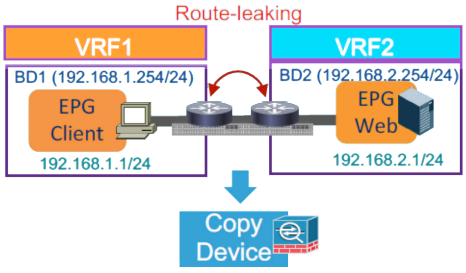
Copy Service Deployment Options



End Point Group (EPG) in the same (L2 Bridge domain) BD.

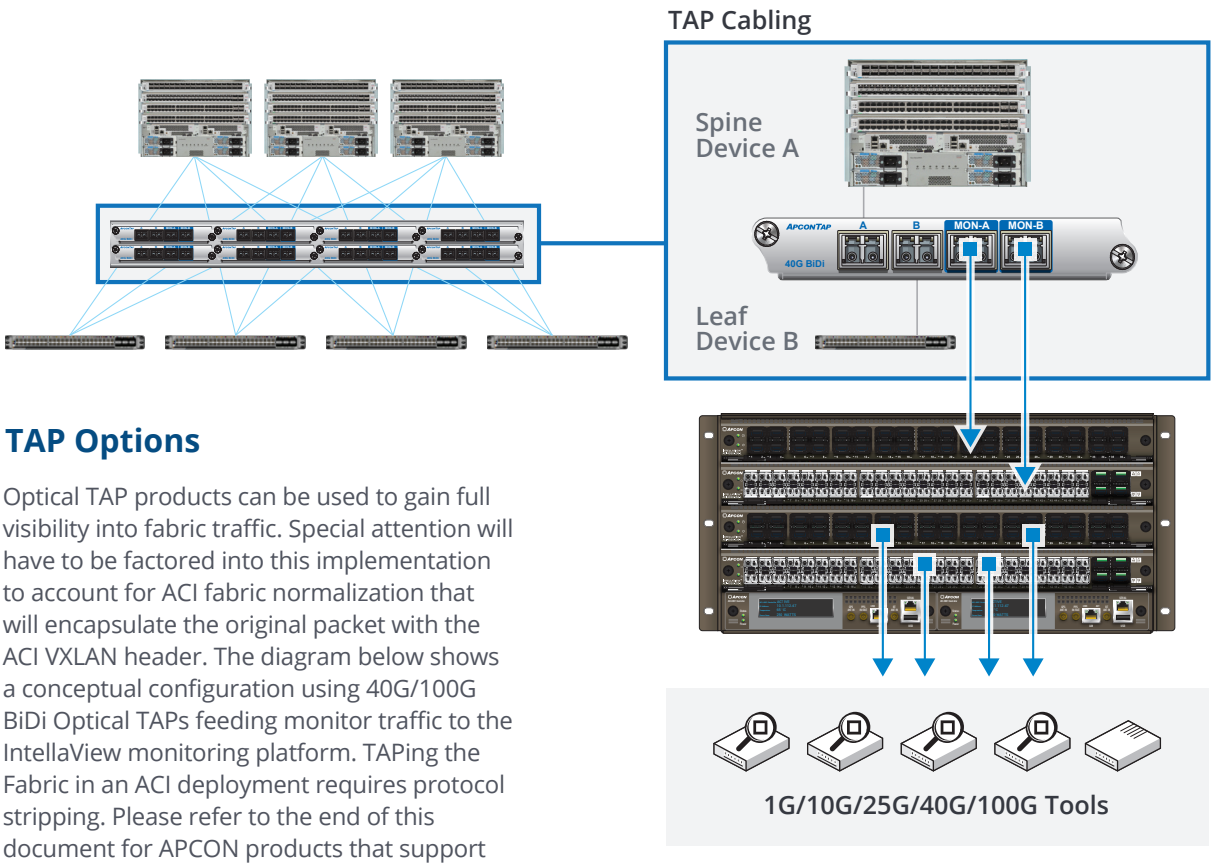


EPG in different BD under the same VRF (L3 route between L2). VRF is Cisco VPN mechanism to route between VLAN, yet maintaining separate IP domain.



EPG in different BD and different VRF.

Specific setup options can be found in the **Cisco Configuring Copy Services** documentation.



TAP Options

Optical TAP products can be used to gain full visibility into fabric traffic. Special attention will have to be factored into this implementation to account for ACI fabric normalization that will encapsulate the original packet with the ACI VXLAN header. The diagram below shows a conceptual configuration using 40G/100G BiDi Optical TAPs feeding monitor traffic to the IntellaView monitoring platform. TAPing the Fabric in an ACI deployment requires protocol stripping. Please refer to the end of this document for APCON products that support ACI Advanced Feature sets.

APCON TAP and Network Visibility Solution

ACI-0540-000: ApconTap Chassis

- Holds up to 6 ApconTap modules

ACI-0540-XXX: ApconTap Modules (4 ports per module)

- 40G MM
- 100G MM
- 40G SM
- 100G MM
- 40G BiDi
- 100G BiDi

ACI-4030-E36-2-1: Multi-Function Blade

- Supports 36 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation
  - Deduplication

ACI-4030-E52-1-1: Multi-Function Blade

- Supports 48 ports of 1G/10G/25G
- Supports 4 ports of 40G/100G
- Advanced Features:
  - Protocol Stripping
  - Port Tagging
  - Packet Slicing
  - Tunnel Termination
  - Tunnel Initiation

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**

17050-0621