Achieving Network Visibility For Cisco ACI Deployments

Introduction

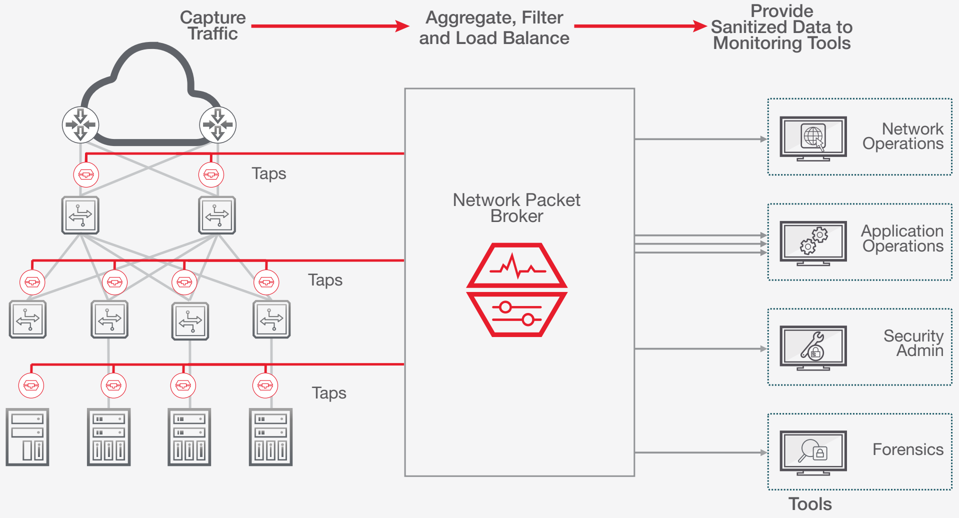
Software Defined Network (SDN) architectures like Cisco's Application Centric Infrastructure (ACI) are evolving and carry the promise of bringing improved application delivery to virtualized environments. Deploying ACI enhances business agility, reduces total cost of ownership (TCO), automates information technology (IT) tasks, and accelerates data center application deployments.

However, implementing ACI strains IT teams, which suddenly have to learn how to operate differently while maintaining the same level of security and performance as before.

Thus, incorporating a network visibility plan as a core component of an ACI deployment early in the planning process can help to ensure that the final deployment is easier to achieve and easier to manage.

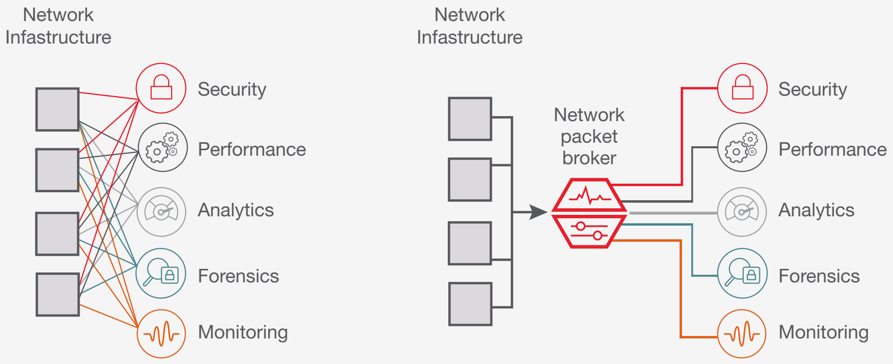
Adding to the strain are tools of all types used to monitor and ensure the health of a network. As the number of tools increases; the best practice is to adopt a network visibility solution in order to ensure that tools are receiving the data they need to perform. Thus, incorporating a network visibility plan as a core component of an ACI deployment early in the planning process can help to ensure that the final deployment is easier to achieve and easier to manage.

The goal of any visibility solution should ensure that the performance, monitoring, and security tools you have implemented to manage your network receive a complete end-to-end view of all your network data.



Visibility is the term used to describe a data distribution layer that intelligently connects raw, unprocessed, incoming data to your analytics and security tools. It is not some sort of data analytics or monitoring application, or even deep packet inspection. Visibility is pure and simple data distribution with the ability to capture monitvoring data, groom that data as necessary, and load balance data flows to optimize security and network performance.

This is generally done by placing physical taps between network links throughout your network to unobtrusively capture all your network traffic. The monitoring data is then passed to a specialized network intelligent switch called a network packet broker (NPB) where all the data is aggregated, filtered, and processed prior to being sent to security and monitoring tools.



The end result is that tools receive all the data they need to see, and nothing that they do not.

Offload ACI Monitoring Traffic to a Dedicated Visibility Network

Challenge: ensure ACI is performing as desired

Deploying a dedicated network Visibility solution helps ensure your ACI deployment is performing as desired. The simple fact is you cannot monitor what you cannot see, and any errors that occur within ACI may not be seen by tools that are also managed within ACI. A dedicated network visibility solution that exists outside ACI is a critical ingredient to a successful ACI deployment.

Visibility Network

Utilizing visibility in an SDN is as important in non-SDN environments, if not more important. The practice of relying on only a few points in your network to capture data breaks down as you move to a SDN, like ACI. For instance, if you are only monitoring north–south traffic that may work today for some cases, but as you move to ACI, application workloads will be communicating between end point groups and therefore monitoring just north–south traffic will leave your tools blind. The simple fact is that critical links are not known ahead of time in an SDN; best practice is to obtain visibility into every network link. Switch Port Analyzer (SPAN) ports are to be avoided. They potentially impact your production traffic, are limited in number, and do not provide a consistent method to capture traffic across your entire networking domain.

Also, you need checks and balances against ACI to ensure the components are not failing. To obtain this, you need an external view of the situation using the tools you are most familiar with. Tapping each and every spline leaf connection ensures your monitoring tools see everything, while not negatively impacting your production network.[1]

Capturing Cisco ACI traffic for analysis

Traditional data center networks are built using a three-layer, hierarchical design consisting of access, aggregation, and core. However, this can be prone to bottlenecks, especially when uplinks between layers are oversubscribed.

For dynamic SDN environments, like Cisco ACI, where consistent network performance is paramount to applications; leaf-spine architectures provide a higher level of consistency.

With leaf-spine architectures, a series of leaf switches create the access layer, and connect to a series of spine switches in a mesh. Access-layer switches in this design are no more than one hop away from one another, thereby reducing latency and the potential of network bottlenecks across access-layer switches. The result increases the predictably and consistency of the amount of delay or latency for traveling information,

Why do I want a dedicated out-of-band visibility solution that lives outside Cisco ACI?

A solution that combines a dedicated out-of-band visibility solution with a Cisco ACI can provide several advantages[1], such as:

- Redirect monitoring traffic to a dedicated network, where performance bottlenecks and negative impacts on production networks are less of a concern
- Additional filtering and truncation control of monitored application traffic through a dedicated out-of-band network packet broker
- Consolidate and replicate monitoring traffic; allowing the use of multiple monitoring devices on the same traffic source

[1] Cisco Nexus Data Broker Integration with Cisco ACI

which is critical for environments like SDN, where consistency between the layers is critical to achieving consistent network and application workload performance.

Preparing ACI traffic for tool ingestion

When it comes to ensuring your tools can see ACI traffic, there are three considerations:

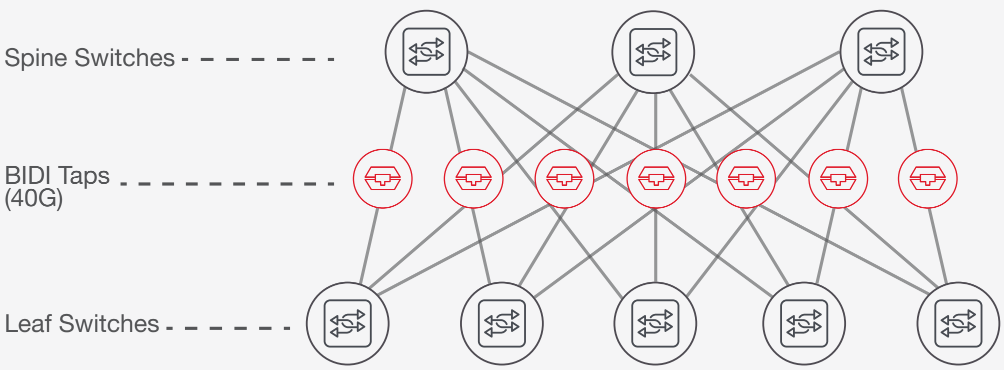
1. Removing Duplicate Traffic caused by spine-leaf architectures
2. Stripping VxLAN headers
3. Ensure tools see everything

First, placing network taps within an ACI architecture creates a significant amount of duplicate traffic which should be removed before forwarding to tools. This will result in significant tool costs if not performed. Next, Cisco ACI networks rely on encapsulating all communications within Virtual Extensible Local Area Network (VxLAN) tunnels. When capturing the traffic via a network tap, the header is going to remain, and it must be stripped before any tool can access it. Finally, Cisco ACI utilizes spine-leaf architectures where east–west traffic flows in high volumes; tapping each link creates a huge amount of unpredictable traffic.

How many visibility blind spots can your monitoring platform handle? **ZERO.**

Each monitoring tools requires 100% of all network data to work effectively. Even Cisco's whitepaper on Cisco ACI integration with its data broker product recommends, in high traffic situations, "offloading all monitoring traffic to a dedicated network may be beneficial," because of "fewer visibility blind spots".

Spine / Leaf Data Center Network Architecture



Tapping Cisco ACI networks is the best and most effective method to capturing ACI traffic for out-of-band analysis. Other approaches like utilizing SPAN ports are susceptible to dropping data, which could result in your monitoring, security and performance tools not receiving the data the need to perform their job, thus creating a visibility blind spot.

No artificial limitations on packet processing

NPBs are great at processing packet data. Their job is to make the data that is captured easier for your tools to consume. They can remove duplicate packets, strip headers such as VxLAN headers, add timestamping information, or slice the packet payloads to reduce data volumes send to tools, making them much more efficient.

Network Packet Brokers within most visibility solutions today can strip headers of network packets. However, can you combine this stripping with other advanced features without restriction? For instance, what if you (or a higher level SDN orchestration layer) wants to add another packet processing operation to your ACI traffic? Will it be able to, or will it require additional hardware?

A visibility solution that requires you to reference a compatibility table in their operations guide to ensure that the combinations of packet processing operations you want to perform is supported is going to be much harder, if not impossible to integrate with SDN controller. Simply put, these type of artificial limitations on feature combinations complicate any integration with an orchestration or control layer; this includes SDN controllers like APIC. Additionally, as your ACI environment deployment matures, these types of restrictions create complexities that prevent automation.

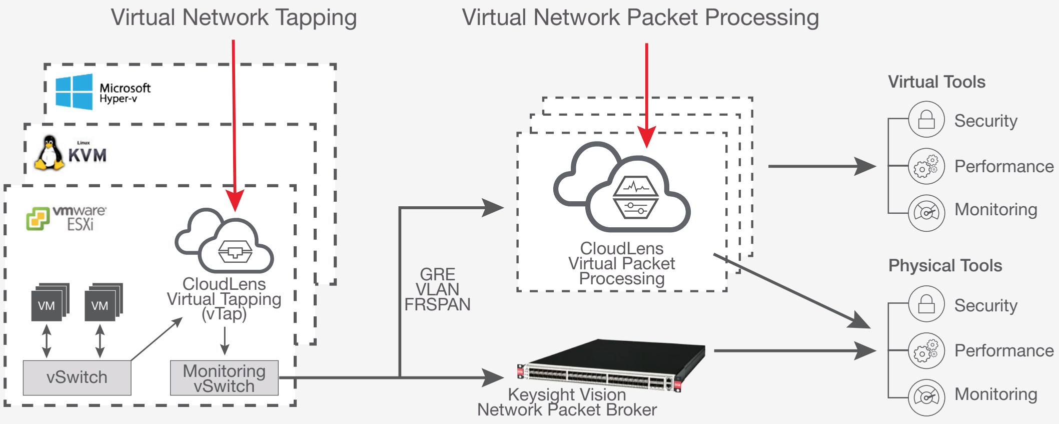
Instead, a visibility solution that allows any combination of advanced filtering features without restriction is more desirable, not only for integration, but also for the health of your network. A visibility solution that is easy to manage without artificial limitations allows you to focus on "what" is the right data to provide your monitoring tools, rather than wasting your time determining "how" to get it there.

Integrating visibility with Cisco ACI works by replacing human components with automation. When defining visibility rules, any visibility solution that requires you to cross-reference an advanced feature compatibility table in their user guide should be a warning sign that their products are substantially harder to integrate with any SDN, including Cisco ACI.

Inspect virtual machine network traffic

One of the key drivers for SDN was virtualization. It therefore makes sense to ensure your visibility solution has the capacity to capture virtual network traffic for the purposes of routing it to tools.

Also, as additional visibility resources are needed, the visibility fabric should scale capacity without the need to rack-and-stack physical hardware.



Keysight CloudLens allows for the capture of both public and private virtual network traffic for filtering, aggregation and processing with or without the need for a physical network packet broker. It allows for horizontal scale through the capability to programmatically stand-up new virtual packet processing resources as needed, without the need for network operation teams to rack-and-stack new physical hardware.

Capture traffic via top-of-rack switches

Another method for capturing data within an ACI network is through data aggregation at the switch level, where top-of-rack switches aggregate data before forwarding.

Section Summary

Concern	Keysight Solution
What is the best way to capture ACI traffic? Critical links are not known ahead of time, and as part of my Cisco ACI network, I installed Cisco bidirectional (BiDi) technology. How do I capture this type of traffic?	**BiDi FlexTaps** Place Keysight BiDi FlexTaps between spine and leaf switches, which are advantageous to SPAN ports, because they capture a complete copy of the data and are not susceptible to packet loss.
If I tap into Cisco ACI network Traffic how will my tools keep up? How can my existing security and monitoring tools keep up with the increased traffic caused by tapping Cisco ACI 40G links?	**Utilize High Performance NPBs** Utilize Keysight high-performance Vision NPBs to load-balance and filter traffic amongst all your tools.
How do I deal with the duplicate packets tapping spine-leaf networks create? How do I remove the duplicate packet “noise” that comes with placing taps within spine-leaf networks?	**NPBs remove duplicate packets** Our Vision NPBs remove duplicate network packets from tapped Cisco ACI traffic, providing your tools an end-to-end view of Cisco ACI network traffic.
How do I get my monitoring platform access to VxLAN Traffic? If I tap ACI networks, I will receive a complete copy of the packet data, including the VxLAN header. My tools cannot strip VxLAN headers, so they will have no ability to process this tapped data.	**NPBs Strip VxLAN Headers** Our Vision NPB’s strip VxLAN headers from traffic tapped in Cisco ACI environments, providing your tools a complete view of Cisco ACI network traffic.
How do I capture virtual network traffic? How do I ensure I am seeing VM traffic as part of my solution to monitor ACI deployments?	**CloudLens provides virtual network visibility** Keysight CloudLens provides a complete view of both public and private virtual network traffic, providing tools a view into VM-to-VM network traffic.

Plan for Integrated Management

At some point, integrating visibility with a Cisco ACI/APIC is going to be required. Nobody wants to manage separate interfaces. In this section, we discuss the challenges considerations of incorporating visibility with SDN’s.

Self-maintaining visibility

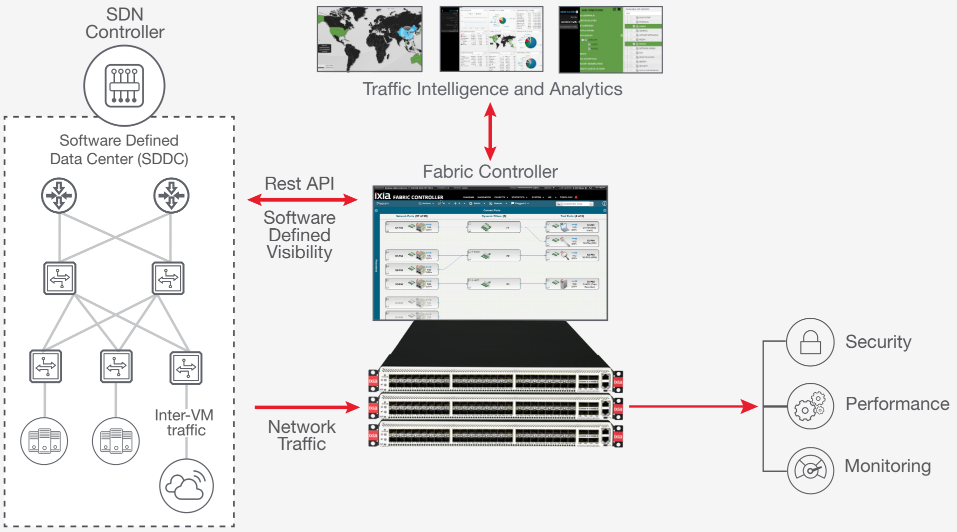
Visibility architectures enable filter rules that define what should happen to the traffic arriving on a network port before forwarding on to a security, monitoring, or analytics tool.

However, once a filter rule is used for an existing network port, then the logic to utilize it for another filter can become complex. SDN controllers will have no concept of visibility and filter rules; they therefore have no understanding of how to remedy them. So, when considering how to integrate visibility with SDN, it is critical to look for a visibility solution that is easy to configure and manage, so that it can operate in a self-sustaining manner wherein conflicts and problems are handled automatically and without human intervention being necessary.

Filter rule overlaps are a necessary evil of flow mapping architectures, and commonly include the notion of a loopback port. This model is complex and not SDN-friendly. Keysight's dynamic filter compiler was designed to automatically handle overlapping filter rules for users. It has the added benefit of making SDN integration a much more elegant process.

Single point of control across all visibility elements

For an SDN controller to connect and send instructions to a visibility platform, there must be a way to aggregate all visibility elements, such as NPBs, and manage them collectively. Keysight Fabric Controller (IFC) allows centralized control, monitoring, and management of a global security and monitoring fabric comprised of many NPBs, including advanced features and functionality. It is resilient and extends full control through open APIs.



Keysight Fabric Controller (IFC) allows for centralized management of multiple NPBs, where all ports and interconnects are managed in a single pane of glass. This allows a single place for a SDN orchestration layer to integration with a visibility layer. Combined with Keysight's self-maintaining, consistent zero packet loss visibility; Keysight Network Visibility can integrate IFC directly with Cisco APIC.

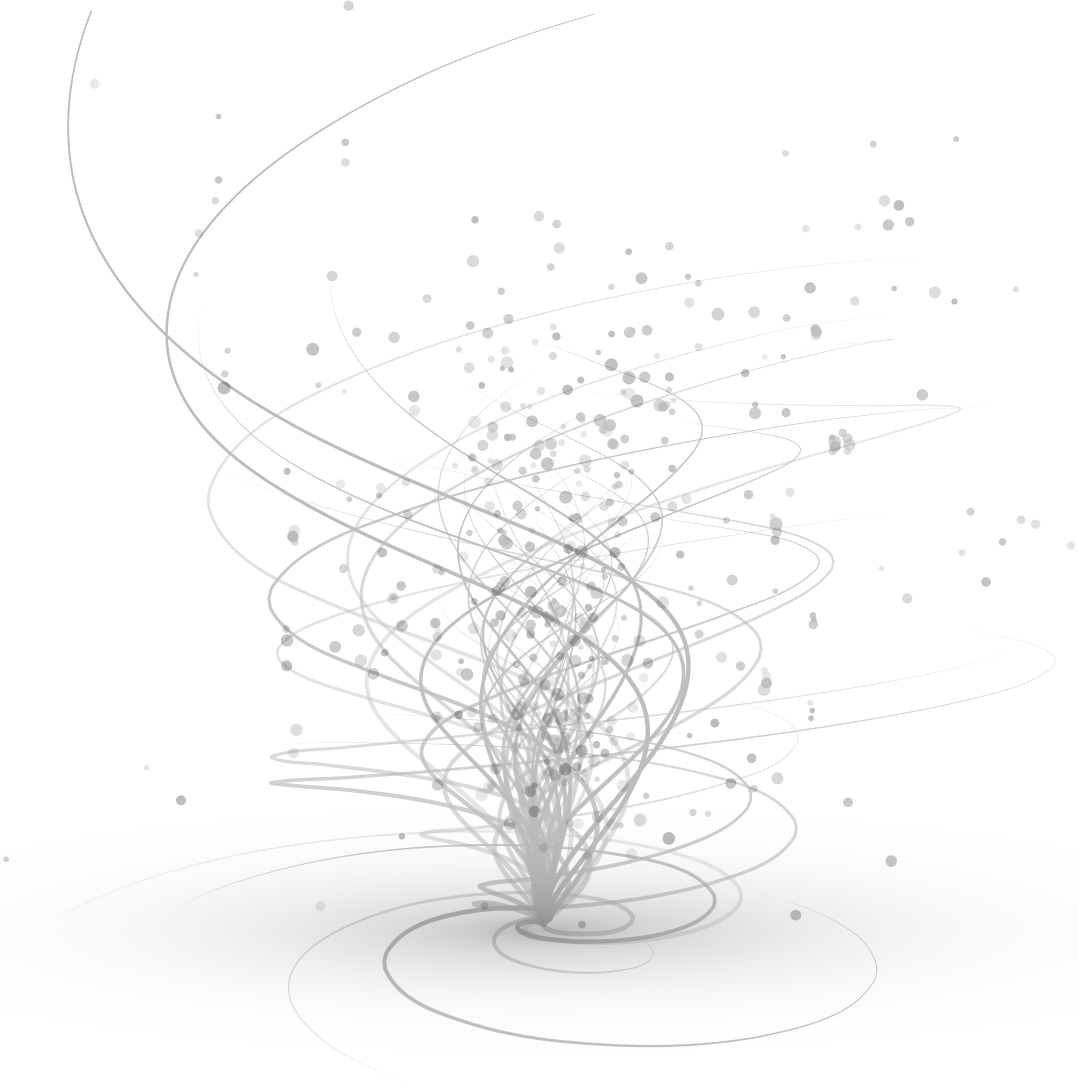
Consistent visibility

Visibility blind spots are bad for not only ensuring your SDN is performing to specifications, but also for when it comes time to relinquish control of your visibility solution to a larger orchestration layer. Dropping visibility data randomly due to load or changes in traffic patterns presents a variability that may not be visible to the SDN controller, and may cause system inaccuracies.

Easily debugged

You should be prepared to handle situations where the SDN controller is out of sync with your visibility solution. When this happens, it is important to have a visibility management interface that is clear and easy to understand, so that the person debugging it does not have to be the original author. When dealing with fewer visibility solutions that include the challenge of overlapping filter rules, there is generally a lot of pen-and-paper logic that must be manually figured out. This logic is entered as filter rules, but the logic that was originally derived is lost; making it hard to understand why and how it was originally configured. This can be a large roadblock to SDN integration with visibility, simply because it can be a huge challenge to debug.

Visibility solutions that process data using software are hindered by their architecture to process data sequentially, and thus, are susceptible to dropping network data before reaching your tools.



Section Summary

Concern	Keysight Solution
When my SDN changes, how will change be reflected in my visibility platform? In my current visibility solution, it is complicated to add or change my visibility, usually requiring an operator to program. How can my network visibility by automated in such an environment?	**Self-Maintaining Visibility** Visibility rules, which describe how captured traffic flows to your monitoring platform, are executed sequentially in nature. A change in any filter rule may inadvertently impact existing rules, resulting in your monitoring platform receiving incomplete or incorrect data (visibility blind spot). Keysight's dynamic filter compiler handles all filter rule complexities automatically, allowing for new tools to be added, modified, or replaced, as needed. Established data flows to tools remain unchanged, ensuring consistency and allowing an SDN controllers like APIC to send change requests without restriction.
How do I scale visibility when it has limitations? When changing visibility rules to include additional features like deduplication, header stripping, or packet slicing, my visibility solution requires me to add other modules. How will that operate in an SDN where my visibility instrumented by a separate control and orchestration layer?	**No Artificial Limitations on Packet Processing** Keysight visibility solution allows any combination of advanced filtering features without restriction or performance impact. Any existing visibility paths can be modified to include additional packet processing rules without concern that the operation may require additional packet processing hardware. Thus, Keysight visibility allows SDN controllers to scale, without artificial restrictions seen within other network processor-based (software-based) visibility solutions.
How do I debug problems? When I have out-of-sync issues between my SDN controller (APIC) and visibility, how will I be able to quickly determine where the error is? What if I cannot understand how the visibility platform was programmed because of all the logic that was used?	**Easily Understood Interface** Since Keysight's visibility solution is self-maintaining, there are no hidden rules in place, and thus, complexities are greatly reduced. When debugging out-of-sync issues between your SDN and visibility, Keysight visibility does not require knowledge of the hidden rules in order to manage it. Thus, the person debugging Keysight visibility does not need to be the same person who programmed it, which reduces MTTR and increases adoption.
How do I ensure my visibility management scales with my SDN? My reason for adopting an SDN like Cisco ACI was to allow my environment to scale as needed to meet the demands of my production workloads. How do I ensure my visibility remains manageable at scale?	**IFC Provides Software Defined Visibility at Scale** Keysight visibility, utilizing its capability to be self-maintaining, can act as a stateful participant in a higher-level orchestration layer by taking commands from an SDN controller and operating deterministically and consistently without artificial restrictions. IFC maintains manageability at scale by providing centralized management of multiple NPBs and allowing for a single APIC integration point.

Conclusion

Software Defined Networking (SDN), like Cisco Application Centric Infrastructure (ACI), is an innovative approach to network architecture that provides the ability to create a whole new class of functionality. The deployment of SDN can be an intricate and challenging task where the ability to develop sustainable solutions is paramount. Offloading ACI monitoring traffic to a dedicated out-of-band visibility solution has many advantages; however, maintaining visibility introduces complexity, so care must be taken in selecting a solution that scales with your SDN environment.

Keysight visibility solutions are designed to be the highest-performing and easiest-to-use solutions on the market. Visibility filter resolution, no filter rule restrictions, and zero packet loss architectures have the added benefit of making Keysight visibility solutions natively more easily integrated with SDN controllers, including Cisco Application Policy Infrastructure Controller (APIC).

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:
www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES