How can we gain the insights and control we need to optimize the performance of applications running on our network?
When used in combination with Cisco AVC-enabled devices, CA Network Flow Analysis provides the enhanced application-level visibility your network team needs to gain more control of the resources they manage—so they can optimize the network infrastructure for application performance, make more informed plans and investments and deliver more business value.
Executive Summary

Challenge

In the past few years, the use of cloud-based services, mobile devices and media-rich applications has expanded dramatically. These trends have served to put more strain on the network, lead to higher infrastructure costs and make the network more difficult, and critical, to manage. More than ever, the performance of your applications and business services is integrally bound to the performance of your network. Without enhanced visibility into the nature and behavior of applications running on their networks, administrators will lack the insights they need to ensure the network delivers optimal performance for the applications that matter most to the business.

Opportunity

CA Network Flow Analysis now offers support for Cisco Application Visibility and Control- (AVC) enabled devices, equipping your network teams with enhanced visibility into application behavior. As a result, administrators can gain improved control over the prioritization, routing, load balancing and optimization of application traffic in order to improve the user experience and reduce cost.

Benefits

CA Network Flow Analysis and Cisco AVC-enabled devices deliver the enhanced application awareness that helps network operations teams:

- Optimize the performance of applications and business services running on the network.
- Improve service levels through faster troubleshooting and remediation.
- Reduce costs and maximize the utilization of existing resources.
- Better align resources and investments with critical business services.
The Challenge

In recent years, there’s been an explosive proliferation in the usage of cloud services, mobile devices and streaming video. Each of these approaches serve to increase the load on networks—and the confluence of all this traffic makes managing networks both more challenging and more critical.

Now, more than ever, the performance of networks, applications and business services are fundamentally intertwined. Ultimately, a positive end-user experience is contingent upon a network infrastructure that’s optimized to deliver superior application and business service performance. However, to understand, manage and optimize networks today, new capabilities are required.

In the past, network monitoring and management was far less complex, with few applications to support, and each tied to specific ports and protocols. Now, more applications are going through same protocols and ports, making it harder to distinguish among different applications and services. While making this distinction is more difficult, it’s also increasingly critical. Some traffic may be essential to business performance, other applications may be lower priority, contrary to corporate policies or even malicious in nature. Further, the latency requirements of many applications can vary substantially. For example, when it comes to video conferencing, even slight delays can significantly degrade the user experience.

Therefore, to effectively govern your networks, it’s vital that administrators can discern between a user streaming their favorite TV show from Netflix or running an online meeting through WebEx, and manage resources and policies accordingly. Today, administrators have to go beyond basic network management and gain intelligent, application-level insights. Without deep application visibility, network administrators will be forced to contend with mounting challenges:

- In today’s complex networks, it is increasingly difficult and time consuming to isolate and troubleshoot performance issues.
- Understanding how network changes and new infrastructure investments will affect different applications is increasingly problematic, leading to suboptimal configurations and policies.

As a result, lower priority and personal user activities can hog resources, while the performance of critical business services suffers. Further, money gets wasted on underutilized infrastructure.

To effectively govern your networks, it’s vital that administrators can discern between a user streaming their favorite TV show from Netflix or running an online meeting through WebEx, and manage resources and policies accordingly.
The Opportunity

Combined, CA Network Flow Analysis and Cisco AVC-enabled devices provide the application-level visibility and capabilities your network teams need to more intelligently manage networks, so they can optimize performance, cost management, infrastructure management and more.

Introducing CA Network Flow Analysis

CA Network Flow Analysis provides real-time visibility into network activity, it reveals which applications and hosts are consuming the most bandwidth and it enables historical analysis of performance and utilization trends. With CA Network Flow Analysis, it is easy to gain the insights you need to optimize network service delivery, do more effective capacity planning and reduce costs. CA Network Flow Analysis delivers these key features:

• **Complete visibility.** CA Network Flow Analysis is designed to provide 100% visibility into network traffic, including host conversations, bandwidth capacity and consumption, application traffic patterns, QoS policies and anomaly detection. Users can browse reports and drill down to view detailed information, including any fields in a data packet from any monitored interface. In addition, CA Network Flow Analysis is integrated with CA Infrastructure Management, which provides IT teams with a unified interface for analyzing information on infrastructure performance, availability, flow, capacity, applications and voice and video.

• **Insights for proactive management.** CA Network Flow Analysis features patented anomaly detection capabilities that help your administrators proactively find and address performance and security risks. CA Network Flow Analysis automatically observes networks, collecting data from diverse sensors across the infrastructure, and then establishes patterns and identifies when behaviors deviate from normal. Through these capabilities, your administrators can more quickly identify the anomalies that can indicate the existence of misconfigurations, malicious attacks, poor service levels and other problems. Further, CA Network Flow Analysis provides the workflows and resources that help you do fast research and troubleshooting when anomalies occur. CA Network Flow Analysis also provides longer-term views to help identify patterns over the course of days, weeks and months.

Cisco AVC also features support for application mapping through NBAR2, Cisco’s innovative deep packet inspection (DPI) technology, which enables identification of more than 1,000 applications.
CA Network Flow Analysis and Cisco AVC

Through its support of Cisco AVC-enabled devices, CA Network Flow Analysis enables administrators to harness rich, application-level insights in managing their networks. Cisco AVC leverages core technologies found in the Cisco ASR 1000 Series Aggregation Services Routers, the Cisco Integrated Service Routers Generation 2 (ISR G2) and Cisco Wireless Controllers. Instead of requiring an additional hardware device or platform, Cisco AVC integrates with existing devices at the management layer, reducing network footprint, simplifying network operations, and reducing total cost of ownership.

Cisco AVC also features support for application mapping through NBAR2, Cisco’s innovative deep packet inspection (DPI) technology, which enables identification of more than 1,000 applications. The information collected by Cisco AVC-enabled devices is exported into CA Network Flow Analysis through open standard formats, such as NetFlow Version 9 and IP information export (IPFIX). Further, administrators can create, edit and delete NBAR2 application mapping rules in the CA Network Flow Analysis console.

Joint Solution: Key Capabilities

With CA Network Flow Analysis and Cisco AVC, administrators can leverage NBAR2 in several key ways:

• **Application accounting.** Users can get a snapshot of applications traversing a given interface, along with traffic rate and volume, which can be tracked both by bytes and packet units.

• **Classification.** With these combined solutions, administrators can identify traffic by NBAR2 application signature. This allows organizations to set per-application policy controls, including quality of service. For example, an enterprise administrator can limit traffic rates for consumer-focused applications like Netflix, Pandora and iTunes, or guarantee bandwidth for business applications like WebEx, Office 365 and SharePoint.

• **Reporting.** Through CA Network Flow Analysis, operations teams can leverage a range of reports, including:
  - NBAR2 session reports, which validate traffic and markings in raw data.
  - Application response time reports, which deliver information on response time metrics for applications, clients and servers.
  - WAAS (wide area application services) segment reports, which provide pass-through information that helps administrators determine why a given flow is not optimized.
Joint Solution Advantages

CA Network Flow Analysis and Cisco AVC provide a powerful solution for discovering and controlling applications within the network. The solutions enable administrators to gain much deeper insight into which applications are running in their networks and their performance characteristics. Using layer 3-7 information, Cisco AVC identifies applications and exports data to CA Network Flow Analysis for management and reporting. Through these solutions, administrators can:

- Set, track and validate application traffic policies to enable continued refinements.
- Guarantee, limit or prioritize bandwidth for specific applications.
- Do intelligent path selection based on technological and business performance requirements.
- Configure rules to identify NBAR2 application traffic, combine traffic for multiple applications or separate NBAR2 traffic from other traffic.

With these capabilities, administrators can establish much more intelligent control over network usage and take the steps necessary to improve application performance.

The Benefits

With CA Network Flow Analysis and Cisco AVC, network operations teams can quickly gain the visibility and intelligence they need to understand network performance within the context of the applications and services running on the network. In addition, they can gain the controls they need to put these insights to work to fulfill a range of objectives:

- **Boost service levels.** Administrators can track and optimize the applications that users interact with, and reduce the incidence of downtime and performance issues. Plus, when issues arise, they can leverage the powerful tools and timely and detailed information they need to resolve problems more quickly.

- **Better manage costs and resources.** With CA Network Flow Analysis and Cisco AVC, your operations teams can start to more effectively understand, predict and meet changing resource demands. They can track performance trends in order to make more informed investment decisions, so resources acquired deliver maximum improvement.

- **Deliver more business value.** CA Network Flow Analysis and Cisco AVC help your team identify and track the performance of applications running on the network and prioritize resource allocations for the services with the highest business impact. As a result, the solutions help your organization more consistently deliver the service levels the business requires, helping fuel improved business performance.
Conclusion

Improving how applications perform in today’s networks is more critical and more challenging than ever. With CA Network Flow Analysis and Cisco AVC, your operations teams can gain the visibility and controls they need to understand network and application behavior, and employ the policies, configurations and investments that help make sure the most critical business services continue to perform optimally.