WHITE PAPER

ixia

A Paradigm Shift for Network Visibility:

Delivering Better Data for Better Decisions

Table of Contents

Introduction

As business networks continue to respond to user demands of access to more data, BYOD and the Internet of Things, a new chapter has opened for IT personnel. While much of the traffic that runs through service provider and enterprise networks is stateful and application-based, access to application and user data has been costly and often lacking. Simply looking at layers 2-4 of the OSI model no longer provides deep insight into the character of the traffic. While the Layer 2 – 4 data continues to have value, to really understand your network infrastructure and how to respond to customer demands, you need to see what applications are running and look at performance artifacts at the application layer, i.e. Layer 7 information.

At the same time that technologies like cloud and LTE are proliferating, the number of applications, both beneficial and malicious, are rapidly increasing and place further demands upon service providers and large enterprises. These organizations have to maintain constant vigilance to be able to respond in real time to eliminate network blind spots and identify hidden network applications so they can mitigate the network security threats from rogue applications and users.

Application intelligence (the ability to monitor packets based on application type and usage) is now available to provide the application and user insight that is desperately required. This technology is the next evolution in network visibility.

Application intelligence can be used to dynamically identify all applications running on a network. Distinct signatures for known and unknown applications can be identified and captured to give network managers a complete view of their network. In addition, well designed visibility solutions will generate additional (contextual) information such as geo-location of application usage, network user types, operating systems and browser types that are in use on the network.

As business networks continue to respond to user demands of access to more data, BYOD and the Internet of Things, a new chapter has opened for IT personnel.

As new network security threats emerge, application intelligence can correlate the applications with geography to identify compromised devices and malicious activities through Command and Control communications. IT managers can also use the application data to track fast growing applications and prevent outages and other performance impacts, especially in mobile service provider environments. This brand new visibility empowers customers with better data so they can make better decisions, which is accomplished by providing real-time application data to existing monitoring tools regarding the behaviors and locations of users and applications.

A fundamental requirement of the application intelligence technology to be useful is that the application data needs to be delivered/utilized any way a network manager wants it. This typically means in one of the three following formats:

1. Web-based API,
2. NetFlow (including extensions for the contextual content),
3. Or internal product dashboard

They key fact is that if customers have the data they need to distribute to their purpose-built monitoring tools to make those tools work better, those tools will deliver better insight into network anomalies, problems, and concerns.

Basic and Advanced Visibility

Before proceeding, let's look at what basic visibility is and compare that capability to application intelligence.

Basic Visibility – Network Packet Brokers

A network packet broker (NPB) is a device that directs network traffic from switch SPAN ports, taps, and/or between two connected routers and/or switches, and then manipulates that traffic by parsing and copying it to allow the more efficient use of network security and performance tools.

Every NPB must provide port mapping of network ports to monitoring ports, and usually offer the following basic features:

- A configuration interface, such as a graphical user interface (GUI) or command-line interface (CLI)
- Packet filtering, slicing, and de-duplication
- Traffic aggregation, regeneration, and load balancing
- Time-stamping

NPBs come in many flavors and with many different options and capabilities:

- Aggregation of monitored traffic from multiple links/segments
- Filtering and grooming of traffic to relieve overburdened monitoring tools
- Load-balancing traffic across a pool of tools
- Regeneration of traffic to multiple tools

A network packet broker (NPB) is a device that directs network traffic from switch SPAN ports, taps, and/or between two connected routers and/or switches, and then manipulates that traffic by parsing and copying it to allow the more efficient use of network security and performance tools.

NPBs tend to be more sophisticated (and more expensive) than basic taps. Generally, NPBs possess the following capabilities:

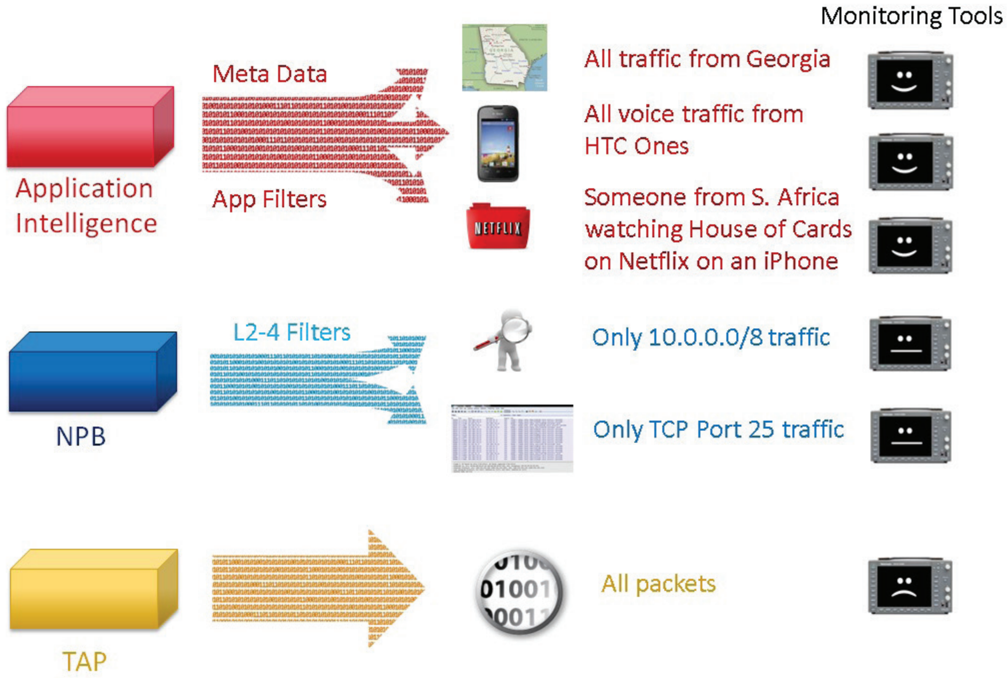
- Fault tolerance. Fault-tolerance minimizes network downtime in the event of NPB failure, connected device failure, or power loss.
- Traffic grooming. Traffic grooming ensures that only relevant traffic is routed to connected monitoring tools. This helps to make sure that tools are only receiving traffic they are supposed to, and increases general monitoring efficiency by prevent the tool form being overwhelmed by extraneous data.
- Packet optimization. Packet optimization modifies captured packets in order to increase the efficiency of network security and performance tools connected to NPBs. Such optimizations include time-stamping, packet de-duplication, protocol stripping, etc.

Application Intelligence – Advanced Visibility

Application intelligence delivers real-time application data to monitoring tools so that users have more accurate application data in order to make better decisions. It does this by providing rich data on behavior and location of users and applications, in any format needed – raw packets, filtered packets, or metadata. This allows IT teams to identify hidden network applications, mitigate network security threats from rogue applications and user types, and reduce network outages and/or improve network performance due to application data information.

Application intelligence delivers real-time application data to monitoring tools so that users have more accurate application data in order to make better decisions.

As the following diagram illustrates, while Taps and SPANs deliver the full data stream to monitoring tools, this places a heavy processing burden on those tools. Once an NPB is introduced, duplicate packets and non-relevant packets can be removed so that the monitoring tools have a lesser burden to deal with. Once Application Intelligence is added, application and user information that can be difficult or even impossible for external monitoring tools to gather, can be readily supplied to those monitoring tools. Those tools can then spend their full processing power to focus on data correlation, long term trending and data storage.



The Evolution of Visibility

When application intelligence is integrated into a Network Packet Broker, the full visibility improvements can be realized and the application data can be distributed to the specialized network monitoring tools for maximum benefit.

Application intelligence possess the following abilities:

- Dynamic- and signature-based application detection and monitoring
- Combine traditional NPB capabilities with application detection and intelligence
- Track applications by bandwidth, session, and geography
- Monitor and report on application failure and success rates
- Support the ability to collect IP network traffic as it enters or exits an interface (such as Cisco's NetFlow).

What is Driving the Network Visibility Paradigm Shift?

Apps, Apps, and More Apps

The general ubiquitousness of mobile computing in general life now means that the use of networks, network access, and applications over networks has exponentially risen. The need for both applications as services and on-demand use is increasing network traffic immeasurably.

The huge challenge facing network managers and operators today is how to efficiently and effectively monitor incidents and problems that come with the use and performance of applications and services traveling across networks. This is due in part to the complexity of today's network environments combined with the lack of visibility introduced by the latest round of technologies – such as server virtualization, cloud computing, and software defined networks.

The huge challenge facing network managers and operators today is how to efficiently and effectively monitor incidents and problems that come with the use and performance of applications and services traveling across networks.

Security

With the increase of cloud computing, virtualization, and application use, today's networks are constantly evolving and increasingly vulnerable to new risks, threats, and uncertainties. The days of hacking only for fun are dead and gone. Today's network security threats are a big business – motivated by financial gain and much more sophisticated, prevalent, and insidious than in the past. There are now whole communities dedicated to the sole purpose of cracking network security, many of which have gained international notoriety (i.e., Anonymous and DERP), who also share infiltration technology within their group and distribute their discoveries online.

With the increase of cloud computing, virtualization, and application use, today's networks are constantly evolving and increasingly vulnerable to new risks, threats, and uncertainties.

Many governments are also employing so-called "white hat" hackers to either prevent attacks on friendly networks, or perpetrate them on other countries. Countless examples of the back-and-forth between governments make news daily (the attacks on Iran's nuclear capabilities, the ongoing attacks originating in China on the United States, etc.).

IT security professionals are struggling to keep up with the ever-escalating war between those trying to break in, and those trying to keep them out. Although vendors do their best (and it is a pretty good effort) in providing network security tools to defend against the latest cyber threats, implementing those tools is an ongoing challenge. Couple this with the lurking specter of undiscovered application coding flaws and vulnerabilities waiting to be exploited, and you can see the daunting level of what security professionals are being asked to accomplish.

The Value of Application Intelligence

Application intelligence, working in tandem with other monitoring tools, gives better visibility into the impact network traffic has on network performance. While packet monitoring gives one critical perspective, knowing what types, and the character of, application traffic provides another important monitoring tool. One of the biggest advantages application intelligence provide is insight into the packet flow across the network.

In packet switching networks, packet flow (also known as traffic or network flow) is a sequence of packets from a source computer to a destination, which may be another host, a multicast group, or a broadcast domain. RFC 2722 defines traffic flow as "an artificial logical equivalent to a call or connection." RFC 3697 defines traffic flow as "a sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination that the source desires to label as a flow. A flow could consist of all packets in a specific transport connection or a media stream. However, a flow is not necessarily 1:1 mapped to a transport connection."

Packets from protocols can be grouped into flows as well. There are transport protocols, and some protocols use layer 4 as a transport. For example, HTTP traffic is carried by TCP/IP and creates a flow as the connection is built and torn down. Understanding the packet flow is crucial, since packets from one flow often need to be handled differently from others, by means of separate queues in switches, routers and network adapters, to achieve traffic shaping, fair queueing or quality of service (QoS).

This packet monitoring is used to analyze packet types. What application intelligence allows you to do is look at the type of application creating the packet flow, and monitoring the packets based on that distinction. In essence, rather than just examining the packet type, it uses some deep packet inspection techniques to see inside the packet itself, characterize the packet based on the application data contained therein, and then make decisions based on the application or applications that are using the packet flow. It allows traffic monitoring to be done at OSI layers 4-7, as well as 1-3.

What application intelligence allows you to do is look at the type of application creating the packet flow, and monitoring the packets based on that distinction.

- Knowing what applications are traversing the network can be crucial in keeping your network functioning and safe. Application intelligence allow you to:
- Deploy dynamic application intelligence capabilities to identify hidden or unknown network applications and user types.
- Strengthens network security by correlating applications with geography to highlight suspicious connections.
- Increases early warning capabilities by delivering better information to monitoring tools so as to minimize downtime.
- Track granular information on application success and failure rates (even for internal applications).
- Leverage application intelligence knowledge to get accurate and detailed application signatures.

Another growing issue for network operators is signal storms. As smartphone sales surge and become more enmeshed in daily life, the dynamics of mobile communications are clearly changing. People are now spending more time using non-voice applications such as games, email, text messaging and social media. The sheer number of times these applications contact the network as a background task is creating major problems for operators, increasing signaling loads significantly and causing network outages. Accurately visualize network spikes due to application use can be used for network capacity for better resource dimensioning, outage prevention and improved performance for customers.

Furthermore, how monitoring gathers data can be problematic. Many software solutions (such as Cisco's NetFlow) use can use a sampling algorithm to gather a sample of packet data. While sampling is available for NetFlow it's not a requirement – the reality is that operators tend to now like t like sampled data (especially security people). I has to do with the limitations of sampling algorithm.

Most sampling algorithms collect single packets (or groups of packets) at a specified interval. It's like only reading every 64th word in an article. At the end of it, you might have an inkling of the article's gist (or at least what it might pertain to), but little else. Network analysts don't want one out of every 64 packets, they want one out of every one.

If you get enough packets over a long enough period, you can gather fairly useful data. However, if you're trying to pin down an intrusion that occurred via a single HTTP request, you need a much fuller picture. Sampling technology simply doesn't provide that information.

Another benefit to knowing the types of application traffic on the network is improved monitoring resource efficiency. Without knowing the application information for a traffic flow, all the packets in the flow must be sent to the monitoring tool. This can cause the tool's resources to be overwhelmed. Rather than sending all packets in a flow to a monitoring tool that needs to find HTTP applications (for example), with an application intelligence that is able to identify specific application traffic you can ONLY send HTTP application traffic to that network tool.

Using the application intelligence, you can deliver better information to monitoring tools and minimize monitoring resource downtime

Another benefit to knowing the types of application traffic on the network is improved monitoring resource efficiency.

Finally, application aware monitoring allows for a better integration with automation. As data centers and data center traffic becomes more and more complex, automation is becoming a more and more valuable resource for network operators. Being able to have network monitoring tools respond quickly to perceived traffic scenarios with pre-configured responses allow for operators to identify and deal with network issues rapidly – before they affect network performance. By tuning these response to application traffic, operators can better immunize the network from application traffic that affects performance, responding to changes at the application level.

Application Intelligence Use Cases

So how can application intelligence be used to increase the efficiency and effectiveness of network monitoring (as well as network security). Generally speaking, application intelligence should demonstrate the features such as:

- Dynamic application identification to automatically information about known/unknown/hidden applications on any network
- Application identification and geo-location of application, handset type, OS, browser type, and other key user data
- Delivers data to a data collector (such as NetFlow or IPIXP to perform traffic analytics that help minimize network outages

The following sections will highlight use scenarios where application intelligence can provide information to monitoring device that will help improve network performance.

Profile the Network

A network profile is an inventory of all the assets and services used by a network. A network profile is useful to network administrators to make better decisions about how configuration changes, service and application deployment, and upgrades could affect the rest of the network. For example, security administrators can evaluate the profile for assets that violate policy and for any suspicious activity.

As the profile changes over time, network operators and defenders can monitor for emerging concerns. This, in turn, can lead to policy changes and reallocation of network resources.

Most modern data-center applications, running over networks with unusually high bandwidth and low latency, should have great communication performance. However, often these applications experience low throughput and high delay between the front-end, user-facing servers – as well as the back-end servers that perform other operations. Troubleshooting network performance problems is hard.

Application intelligence can help to profile a network by identifying application performance issues, traffic flows across the network, and how application traffic affects overall network performance.

Determine and locate source of network spikes

One of the most common things that can kill network performance is a huge spike in traffic that overwhelms resources. Examples of this can be a particularly popular news story, video, or game that hits the market at a specific time, and everybody tries to access it at once. These types of events can slow down or even disable an otherwise functioning network.

One of the most common things that can kill network performance is a huge spike in traffic that overwhelms resources.

With an application intelligence, monitoring tools can observe if there is a sudden spike in a specific type of application traffic – and then take action to either mitigate the effect or alert the proper people that can address the issue. Application intelligence can monitor application bandwidth explosions, and use the data to track fast growing applications.

With this knowledge, monitoring systems can prevent localized or global outages, especially in mobile service provider environments. Customers can use this product to create empirical data to identify bandwidth usage, trending, and growth needs

Analyze, Troubleshoot, and Predict BYOD Effects and Issues

One of the biggest issues facing network operators in the age of mobile devices is the “bring your own device” (BYOD) phenomenon. Unregulated devices suddenly linked to your network and using it in ways that are unauthorized or just unexpected can wreak havoc on network performance. Understanding what is happening on the network in such cases is crucial to maintaining a functioning network.

Application intelligence allows you to understand device impact and user trend behavior. You can capture rich user and behavioral data about the applications that are running, and determine how, when, and where users are employing them.

Application intelligence allows you to use operating system information troubleshoot and predict BYOD effects. For example, only a small amount of users with an OS (iPhone 4) may use an application, while a substantial amount of users with a different OS (iPhone 5) use the same application. An application intelligence allows you to collect user information about browser types on the network that are used for each application.

All of this data allows you to intelligently plan for network upgrades and user migration.

Capacity Planning

Planning for your network capacity needs can be the difference between a smoothly functioning network, and a disastrous mess of a network. If a network is under-provisioned, users will not have access to needed services and applications when it is crucial.

Having the right data about who, when, when, and how the network is being used allows you to make smart decisions about how to allocate limited network resources.

Application intelligence can provide the exact data you need to know who is using the network, what applications are being run, and from what location they are being accessed. A good application intelligence provides the geo-location of application traffic to see application bandwidth and data distribution across the network. With the right tool, geo-location capability can be very granular and allows identification beyond country, state, and town down to even neighborhood locations.

Tag Groups to Filter for Specific Information (Applications) Across the Network

The biggest variable in any network is not the hardware, the design, or even the traffic (though all of those are a factor). No, the biggest variable in a network are the users employing it.

The biggest variable in any network is not the hardware, the design, or even the traffic (though all of those are a factor). No, the biggest variable in a network are the users employing it. They are the ones that create the demand for resources, the traffic flows, and the security threats that plague network operators on a daily basis.

Application intelligence allows network operators to audit for security policy infractions, and verify network user activity is following set policies. For example, users may be using a webmail service (such as Gmail) that bypasses the network anti-virus protocols that was set up for the corporate email system (Outlook).

Application intelligence also allows for protection against known bad websites. As an example, you could verify how many users on the network are still connecting to sites susceptible to Heartbleed.

Specific types of traffic, and the users who send it, sometimes must be monitored in order to gather data on network usage – or to verify that network policies are being correctly maintained. With the ability to monitor traffic based on application, network operators have another tool in their bag to verify that they can control network resources.

Deploy an Early Warning System to Prevent Unpredictable Floods on Popular Applications (the Application Tsunami Effect)

Nothing beats being prepared and ready when it comes to solving problems. Oftentimes in networking, the solution boils down to how fast can a network situation be detected and diagnosed – and how quickly that information can be acted upon. Getting an accurate picture of what is happening in the network in real-time, and understanding exactly what is causing it, allows a network operator to turn a potential network disaster into a mere nuisance.

Application intelligence, with its ability to monitor traffic based on application type, allows a savvy network operator to prepare for network "tsunamis" from specific applications or event – setting up alerts or actions ahead of time.

Conclusion

The world is changing, and the networks that keep us connected are changing with it. More and more people are using networks for more and more functions – networking is a deeply interwoven part of our everyday life. With this use, comes increased demands and needs. Networks are changing and adapting rapidly to meet these needs.

Network operators must monitor all aspects of their networks to maintain functionality. That includes monitoring applications along with the critical parts of application deliver – servers, services, and applications are used across the network. Recognizing and reacting to easily identifiable, trouble-making applications can mean the difference between functioning and flailing. Operators must proactively head off application issues with deep capacity planning.

Application intelligence help you always get the right alert at the right time, with no alert storms that leave you guessing about the real problem.

Network operators must monitor all aspects of their networks to maintain functionality. That includes monitoring applications along with the critical parts of application deliver – servers, services, and applications are used across the network.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

915-6634-01 Rev. A, May 2014