WHITE PAPER

ixia

Cost-Effectively Scaling Visibility in the Enterprise

26601 Agoura Road, Calabasas, CA 91302 | Tel: 818.871.1800 | Fax: 818.871.1805 | www.ixiacom.com | 915-6602-01 Rev. A, July 2013

Table of Contents

Executive Summary

Enterprises need scalable and flexible networks that can adapt to the changing needs of the business world. Not only does the IT department need to add the right types of equipment (like monitoring tools, diagnostic tools, tools specific to company initiatives such as BYOD and private cloud, etc.), but they need to control costs at the same by adding the functionality exactly where and when it is needed.

Cutting edge technology from Ixia can be used to simplify the visibility of growing network complexities. The Ixia ControlTowerTM Network Visibility Architecture allows the IT department to add monitoring capability to improve network visibility. At the same time, the ControlTower architecture is the most flexible, powerful, and easy to use solution in the industry and enables positive ROI through improved network performance monitoring and network security tool enablement.

Managing Complexity Is A Constant Challenge

Today's enterprises continue to face the traditional challenges of cost containment, budget constraints and bandwidth constraints.

Today's enterprises continue to face the traditional challenges of cost, budget, and bandwidth constraints. The IT department must respond to these concerns with technology that solves problems AND is also on-budget – or preferably under budget.

Needless to say, this can be a tall order – especially as the amount of data passed on IP networks continues to increase and new business initiatives like BYOD and regulatory compliance expand. At the same time, new products and functionality are being added to the network. All of this creates more complexity, with a rate of increase that David Cappuccio of Gartner characterized at a 2012 Gartner Summit that for every 25% increase in functionality of a system, there is a 100% increase in complexity. It doesn't take too long for this additional complexity to become overwhelming.

In addition to the pain and cost of trying to decipher the network complexity, the complexity itself can be likened to a rolling fog that sweeps in to cloud the visibility of what is actually happening within your network. Simplification is the natural answer to complexity. But how do you achieve this simplicity while maintaining the functionality and flexibility that your customers (whether they're internal or external) want, and control costs at the same time?

One way is to introduce a scalable and flexible architecture that can adapt to the changing needs of your business. You need to be able to add equipment when you want and where you want, versus having to put the equipment where you have to (like in a centralized data center that might be far away from the customers that will actually use it). This "scalability on your terms" frees you from depending upon centralized, large-chassis deployments and gives you a valuable alternative: a flexible, scalable, distributed architecture that can adapt quickly to changing business needs and threats.

One area where this is particularly relevant is access to network performance and security monitoring tools. There are often network SPAN and TAP limitations that prevent you from placing the network tools exactly where you want, so network engineers are often forced to place the equipment at locations that are not optimal for traffic monitoring or for tool deployment.

A second way to counteract complexity is to simplify the management of the equipment that you do add. Managing your network elements should be intuitive, fast, and easy, using web-based GUI's that can connect to multiple boxes at one time. All too often you feel like you are being forced to manage your equipment serially, which takes more time – time that you don't have.

Ixia's ControlTower™ Network Visibility Architecture offers a network visibility switch and architecture that includes both approaches to simplicity – giving you exactly what you want:

- A cost effective monitoring switch that will increase visibility in your data network
- A flexible, distributed, or centralized architecture to scale the amount of monitoring ports you need, when you need them
- An architecture that gives you control over where you place your traffic monitoring tools within your network
- Management software that is easy to use and quickly configures the equipment

The Ixia ControlTower Solution

Ixia's new solution, the ControlTower architecture, is designed to deliver a plug and play solution that simplifies the deployment and management of network and application performance monitoring switches.

ControlTower is a new architecture enabling a flexible and scalable deployment of network monitoring switches. The management and control functionality is isolated to allow the controller unit (called a Supervisor) to manage and control other monitoring switches (called members) in the network. This model is similar to a software defined networking (SDN) architecture, where the Supervisor provides a centralized control and management point.

By doing this, multiple monitoring switches can be placed where they are needed in the network to optimize the network traffic distribution – but still have centralized command and control. This allows you to control costs (you add more ports as needed with the look and feel of one system) while also controlling the geographic location of the monitoring ports.

ControlTower solves the following problems for the IT department:

- Simplifies management for visibility switches and reduces management costs
- Increases visibility and, when combined with virtualized servers and network tools, allows enterprises to take advantage of both concepts to control their operational costs
- Increases access to distributed tools which streamlines tool costs and increases productivity

ControlTower functions in conjunction with Ixia's Network Tool Optimizer (NTO) monitoring switches. These switches allow the IT department to have open access to network information and distribute that information to a variety of diagnostic tools.

ControlTower is a new architecture enabling a flexible and scalable deployment of network monitoring switches.

With the new ControlTower architecture, a controller unit is introduced to separate management and control information for NTO's from the monitoring functionality. Multiple NTO's can be managed by one controller and creates one virtual system that has a high port density that is deployed where you need it. The off-loading of the management functions also improves the performance of the monitoring switches as well. The monitoring switches can be co-located or geographically separated – it's up to you.

The consolidated management functions help simplify the complexity within your data network. Management for the current architecture is consolidated for the monitoring switches. This means you can provision and manage multiple switches at one time with a single user interface that is intuitive and easy to use. The easy to use interface also decreases the amount of time needed to manage the switches – which allows you to spend more of your time on the value-added tasks that are actually important to you.

ControlTower Use Cases

The ControlTower technology has been optimized to deliver network visibility in three key enterprise environments.

The ControlTower technology has been optimized to deliver network visibility in three key enterprise environments:

- High density locations
- Distributed campus environments
- Distributed data centers

The high density single data center use case allows the IT department to rack and stack monitoring ports as needed. The ports can be added when you need them. You also have the flexibility of choosing how to deploy them within the data center. The following are two popular deployment methods:

- Top-of-Rack deployment
- End-of-Row deployment

As Figure 1 illustrates, ControlTower monitor switches can be deployed at the top of the equipment rack. This gives you the ability to aggregate monitoring data from all of the equipment within that rack, e.g. web servers, mail servers, databases, and applications. Another option is to co-locate most, if not all, of your diagnostic and test equipment within a single rack (so that the equipment is easy to locate and access) and then place the monitoring switch at the top of that rack.

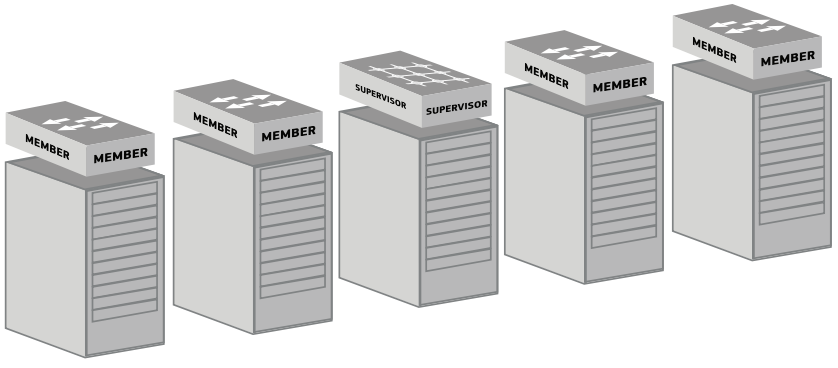

Figure 1 – ControlTower Deployment Example for Top-of-Rack

Figure 2 illustrates the second high density deployment method, which is to place the monitoring switches at the end of a row of equipment. This deployment method allows you to deploy network monitoring near an end-of-row aggregation point, which is common in many architectures, including those using Cisco Nexus switches. The data is then filtered at each member switch and consolidated for transmission back to your monitoring tools, minimizing the number of cable runs and ports needed in the data center.

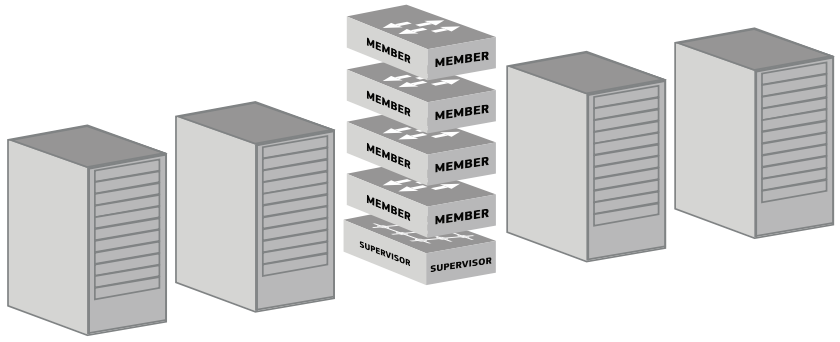

Figure 2 – ControlTower Deployment Example for End-of- Row

The Distributed Campus use case allows the IT department access to geographically dispersed tools across a campus environment. In this use case, tools can be located closer to users and the monitoring test points or consolidated in a centralized tool farm. This is particularly helpful in the campus environment because it allows IT personnel access to the data they need wherever they are located across the campus. It can also make configuration changes easier if tools and/or data spans connected to the monitoring equipment are routinely changed/configured.

The Distributed Campus use case allows the IT department access to geographically dispersed tools across a campus environment.

This use case is demonstrated in Figure 3.

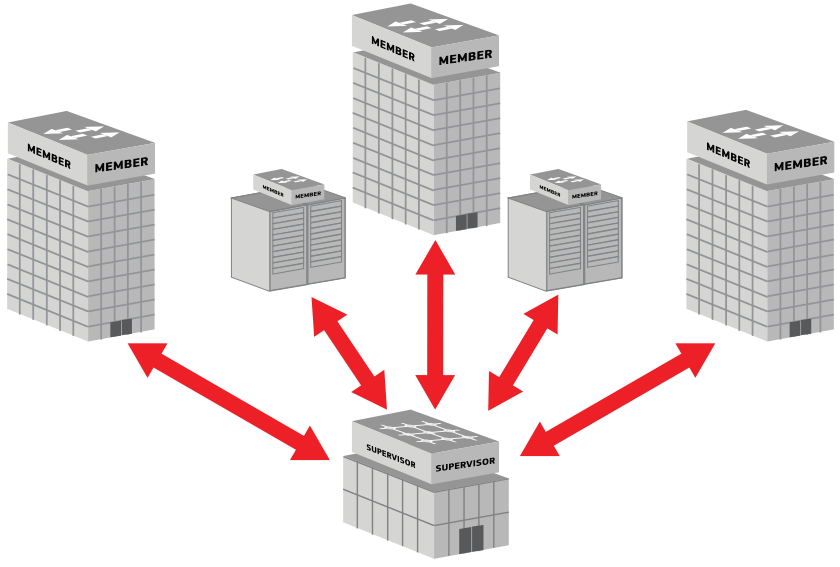

Figure 3 – ControlTower Deployment Example for a Distributed Campus

The changing nature of security threats is driving a significant change in the way that security administrators must maintain vigilance across their networks. No longer are hackers content with simply defacing or bringing down a site with a Denial of Service (DoS) attack. A second benefit of the distributed campus use case is that this design architecture allows IT personnel to respond rapidly to security threats in a campus environment.

The well-publicized rise of Advanced Persistent Threats and their use for long-term, deep penetrations into networks with the goal of stealing intellectual property and valuable customer data means that perimeter-only defenses are now inadequate. Effective security requires monitoring of segments across the enterprise network for potential information theft and malware transmission. However, it's simply not cost effective to deploy security tools on every network segment, especially in a multi-building enterprise campus. And even if it were, administering and collecting all of the relevant security data would be a daunting task.

Here, also, the ControlTower architecture presents a solution. Network administrators can deploy a central "tool farm" of cost-effective, high-capacity security tools and distribute and monitor ControlTower cluster members across the buildings and segments. This allows for collecting interesting traffic and bringing it back to the security tool farm for inspection. If the monitored segments offer too much bandwidth for a single tool to analyze, Ixia's solution can transparently load-balance data across multiple tools.

Besides the improved access to tools benefit, Ixia's ControlTower maximizes flexibility for private and public cloud environments where virtualized workloads can migrate and traffic patterns change rapidly.

The third fundamental use case is that of a Distributed Data Center, where you might want to expand your private cloud architecture in addition to enabling quick and easy access to your existing tool farm (especially for application performance management and access to security analysis tools).

Besides the improved access to tools benefit, Ixia's ControlTower maximizes flexibility for private and public cloud environments where virtualized workloads can migrate and traffic patterns change rapidly.

For example, consider adding a VMWare cluster pools in a new row of your data center. With a traditional network monitoring switch, the only methods of extending your visibility network to this pool would be to choose between limited visibility (adding another stand-alone switch with more management complexity) or adding multiple, expensive home-runs to your current switch. With ControlTower you can simply place a ControlTower Member switch in the new location, add it into the ControlTower cluster via one 40GE link, and then manage it as a part of your existing NTO infrastructure.

This ability to seamlessly expand your visibility network when and where you need it is a unique benefit of the ControlTower architecture. Since it runs the NTO software, connecting these new ports to your application performance monitor or security tools is as easy as drag-and-drop with our simple GUI interface.

Summary

Whether it's increasing bandwidth demands, a rapid build out of public or private cloud hosting facilities, the sharp rise in the number of segments requiring monitoring, or flexibility in deployment across a distributed geography, Ixia has developed a solution designed to meet current and future needs. Easy to manage Ixia solutions enable easy expansion and growth.

Easy to manage Ixia solutions enable easy expansion and growth.

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

Other Ixia Contacts
Info: info@ixiacom.com
Investors: ir@ixiacom.com
Public Relations: pr@ixiacom.com
Renewals: renewals@ixiacom.com
Sales: sales@ixiacom.com
Support: support@ixiacom.com
Training: training@ixiacom.com

For more information see http://www.ixiacom.com/