

# Managing Network Bandwidth to Maximize Performance

*With increasing bandwidth demands, network professionals are constantly looking to optimize network resources, ensure adequate bandwidth, and deliver high performance. Often, buying more bandwidth is not a priority or an option due to limited budgets and pressure to reduce IT costs.*

*This white paper describes how to leverage best practices to monitor, baseline, and manage the network bandwidth and performance. It also highlights how to identify and eliminate issues such as unwanted traffic, unwanted protocols, and network problems with factory default switch configurations.*

## [Table of contents](#)

<b>Addressing common bandwidth consumption issues</b> .....	<b>2</b>
<b>Benefits of a highly-efficient network</b> .....	<b>2</b>
<b>Utilize best practices for a well-managed network</b> .....	<b>3</b>
<b>Preventing unwanted network traffic</b> .....	<b>3</b>
<b>Solution: portable integrated analyzer</b> .....	<b>4</b>
<b>Summary</b> .....	<b>6</b>

# Managing Network Bandwidth to Maximize Performance

Managing network bandwidth efficiently is a top-of-mind concern for many network engineers today. With increasing bandwidth demands, network professionals are constantly looking to optimize network resources, ensure adequate bandwidth, and deliver high performance. Yet uncontrolled network traffic such as personal IM or Skype – now with streaming video and its bandwidth implications – as well as oversubscribed WAN links can plague organizations and negatively impact network access. With limited budgets and the pressure to reduce IT costs, solving these problems by buying more bandwidth is often not a priority or an option. However, measures can be taken to effectively manage the existing network while improving and then maintaining optimal performance.

To ensure network performance, the network engineer must have full visibility into all activity occurring on the network – especially with user/application interaction – and how it is impacting bandwidth and availability. With this insight, network professionals can analyze utilization, maintain control, and meet the expected service level quality.

## Addressing common issues that consume bandwidth

Several common causes negatively impact bandwidth in the enterprise environment by “hogging” that bandwidth. A comprehensive, robust network analyzer can identify many of them, including:

1. Peer-to-peer (P2P) applications (for example, Gnutella and eDonkey)
2. Incorrectly configured connections between servers and clients
3. Skype or personal instant messaging (IM) software
4. Remote backups or downloads
5. Continuous streaming video
6. Incorrectly configured infrastructure devices (i.e. router and switch MTUs, switch port duplex settings)
7. Email with large data/document attachments
8. Unwanted protocols
9. Access to newsletters/websites with embedded animation/graphics

Identification of these sorts of activities is the first and most important step to solving the bandwidth issues, because usually once identified – the steps to address the issues are usually straightforward.

### Benefits of a highly-efficient network

Better insight into the network means more effective management of it. For example, employee productivity will increase, as users will be able to access the network at top speed. IT resources will be available for more strategic projects, as they won't be tied up at inopportune times to troubleshoot network access issues. Communication and data sharing will improve as users reduce high-bandwidth activities, ensuring high performance and availability to the network. And IT departments can host more centralized applications with resources properly allocated.

### Utilize best practices for a well-managed network

The first step in managing network bandwidth is developing policies that define access parameters and discourage activities such as streaming video. Employees may not even know how their activities are impacting others on the network; building awareness of common issues and guidelines can take the organization one step closer to a better managed network.

The next step is implementing the three best practices as described below:

- **Monitor:** Discover what is happening on the network in real-time
- **Baseline:** Document and report usage; define the current state of the network
- **Manage:** Improve performance based on the documentation and monitor progress

***IT will waste \$100 billion on network overspending by 2011. Companies should use WAN optimization tools to reduce network traffic, rather than purchase more bandwidth. WAN optimization tools can slash traffic by 60% to 80%.***

- Gartner analysts Mark Fabbi and Bob Hafner at the 2006 Gartner Symposium IT Expo

(Ref: <http://www.networkworld.com/news/2006/101206-gartner-network-overspending-waste.html> )

These best practices are easiest to implement using a portable integrated network analyzer with multiple capabilities. A portable tool can go to the actual source of a problem, and must be able to run numerous types of tests to quickly isolate the cause.

Network analyzers are the ideal solution for helping network professionals optimize network performance, improve efficiency, and reduce costs while improving reliability and security.

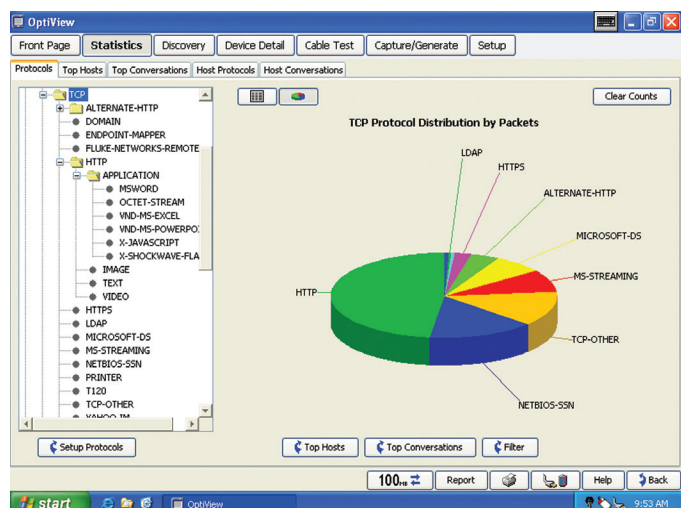
An analyzer gives network engineers visibility into network usage, so they can analyze traffic, document bandwidth usage, and know when and how to take action. Network analyzers come pre-configured with the analysis programs needed to quickly and effectively troubleshoot problems, whereas if network teams use laptops as protocol analysis tools they are faced with the time-consuming task of configuring these laptops with all the necessary software and keeping them updated. Integrated network analyzers are also compact and portable, and can be used to track switches and routers located at any physical location on the enterprise network. Laptops, on the other hand, can be heavy and bulky when used on location for troubleshooting.

### Best practices at work: prevent unwanted network traffic

Unwanted network traffic comes from several sources and often contributes to unnecessary processing by devices throughout the network. For example:

- P2P applications can rob WAN bandwidth from mission critical applications
- Unwanted protocols may indicate a legacy application or other incorrect device configuration
- Factory-default switch port settings may cause considerable amounts of unnecessary traffic and contribute to intermittent network sluggishness

Finding the sources of unwanted network traffic and taking steps to correct or eliminate the root causes can enhance network performance and help avoid future problems, but it can also be a time-consuming task without the proper tools and troubleshooting techniques. The following real-world examples illustrate common network bandwidth challenges, as well as how to identify and resolve them.



## Peer-to-peer traffic

With centralized servers and the move to web based applications, P2P traffic and instant messengers can easily rob WAN bandwidth from mission-critical applications. Therefore, it is necessary to identify these users. Trying to limit traffic is possible at the firewall, but the problem is that many P2P applications actually tunnel through HTTP and others just scan for an open port in the firewall. Attempting to control user PCs to prevent these applications from being installed is also an option, but this can be costly and difficult to manage. To get to the root of the problem, network engineers need deep packet inspection to be able to identify these applications and their source – especially streaming video and audio through HTTP that may occupy a significant amount of expensive WAN bandwidth.

Other applications may use dynamically assigned ports that make traditional port-based traffic analysis much less effective, so network engineers will need to filter on a specific signature to be able to identify these users. These capabilities are most accessible through an integrated network analyzer that can capture packet-level activity for more detailed analysis.

## Unwanted or legacy protocols

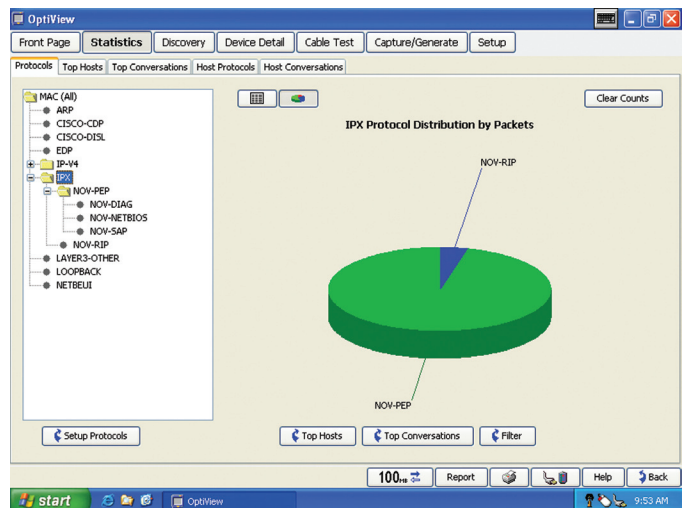
As networks and the services they provide evolve, and servers or user machines are replaced and upgraded, the likelihood of passing unwanted, often obsolete protocols within the network increases. Each situation is unique, but with an integrated network analyzer, network professionals will know where to look. The tool can show not only which devices are using a particular protocol but also where they are connected to the network. For example, in the IPX protocol suite, RIP and SAP packets are broadcast every 60 seconds, even if no change has occurred anywhere in a route or service. In many devices, especially printers, IPX protocols are enabled by default. Therefore, combining protocol statistics with device discovery capabilities, such as with an integrated network analyzer tool, provides a simple way to determine which protocols are running on the network and who is using them.

## Factory default switch configurations

Unwanted network traffic and even temporary network problems can occur as a side effect of factory default settings in a normally healthy network. For example, consider Spanning-Tree Protocol (STP) which is used in almost every switched network. Most vendors enable spanning tree on each switch port by default. This is a reasonable choice as it makes it easy to quickly connect a new device and also protects the network from forwarding loops as the network grows. When the state of an interface changes, for example when connectivity to another switch is lost, STP utilizes a special Bridge Protocol Data Unit (BPDU) called a Topology Change Notification (TCN). This mechanism works very efficiently in a stable network and the presence of TCNs is normally not an issue.

But this can become a problem causing unexpected consequences when the STP is enabled on ports that do change state frequently. Since a TCN is generated when a port that was in the forwarding state goes down or when a port transitions to the forwarding state, including each time an end user connects to the network, the TCN process starts and affects each bridge in the spanning tree. In the worst case, where a large network with many users are connecting and disconnecting, the network can be in topology change status almost constantly. The impact on the network is that the bridge forwarding aging time (normally 5 minutes) is reduced to an effective 15 seconds which can lead to a very high level of flooding as switches re-learn each link. Understanding the possible causes and sources for this type of flooding is possible through an integrated network analyzer and can be an important part of keeping a network clean and running efficiently.

Unwanted network traffic is not only a nuisance to users; it also causes confusion when troubleshooting hard-to-find network problems. Combining the knowledge of where and what to look for with an automated tool such as Fluke Networks' OptiView Series III Integrated Network Analyzer allows network engineers to become highly capable problem solvers in a network environment.



## Simplify best practices with the OptiView™ Series III Network Analyzer

The OptiView Series III Integrated Network Analyzer from Fluke Networks is an integrated, comprehensive tool that combines multiple functions in one portable device, so network professionals can go directly to the source of a problem and analyze numerous possible causes. The OptiView Analyzer also aids network professionals with monitoring, baselining and managing the network.

### Monitor

With the OptiView Analyzer, network professionals can discover which protocols and applications are running on the network, track the top hosts/users and which applications they are running, and determine which applications are unwanted. Network engineers can monitor WAN traffic and identify unauthorized applications that are running over the WAN. They can also quickly and easily identify multicasters, broadcasters or select top conversations to determine which hosts may be over-utilizing resource bandwidth.

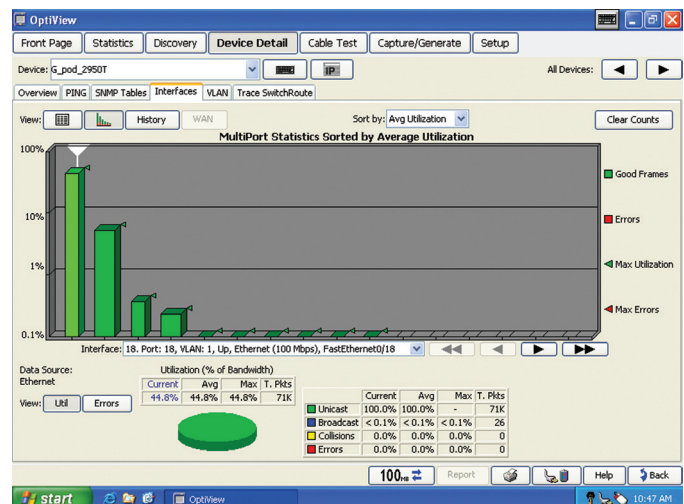
### Baseline

Once the network team has a full audit of activity on the network, a baseline can be documented to set the service level quality expectations. The team can define appropriate protocol usage, detail user activity, and determine normal WAN utilization. Network engineers can detect over-utilization and excessive errors, and locate inactive switch ports to determine if performance problems are related to link speed mis-configurations or to the number of hosts on a port. Network professionals can then use the OptiView Analyzer to eliminate unwanted applications through deep traffic analysis, differentiating between specific audio, video, image or data applications. Once this is complete, the IT team can take a snapshot of the network to determine normal operation. This not only includes monitoring traffic levels, but also involves checking on the utilization of switch ports, router and WAN interfaces. While performing this task, network professionals can also check for errors on switch ports, indicating configuration errors such as duplex mismatches. It is important to document the results in this stage so that the network team has a reference point that can be used when users make reports of a slow network.

### Manage

Monitoring the network periodically is much easier when working off of baseline data, and reports can be pulled quickly through the portable OptiView Analyzer user interface. The tool makes it simple to ensure unwanted traffic has not returned and that all changes are validated.

The OptiView Series III Integrated Network Analyzer enables network professionals to identify applications utilizing link bandwidth – including those that use dynamically assigned port numbers – in order to see and validate the impact of applications on bandwidth



### Get superior capabilities with a single, portable integrated tool

The OptiView Series III Integrated Network Analyzer provides full functionality on an advanced, portable tool. To accomplish the same level of analysis without the OptiView Analyzer would typically require several different tools, including:

- SNMP polling tool
- Wire speed, hardware packet capture tool
- Protocol analyzer
- Traffic monitoring tool
- Host management utilities (telnet/ssh) tool

usage. The tool also lets network engineers determine who is using which applications. Specific capabilities allow network engineers to:

- Perform application analysis in real-time on Gigabit links (capture not required)
- Determine the specific endpoints (server, host) for each application using the application.
- Perform a layer 3 or layer 2 trace route to identify where the endpoint is connected to the switch/router interface
- Differentiate between specific audio, video, image, and data applications, and show the level of bandwidth usage of each
- Monitor WAN link utilization and error rates on ISDN, Frame Relay, T1/E1, T3, ATM and SONET
- Identify overloaded switch ports, ports with error traffic
- Locate inactive switch ports to balance loads and network segmentation
- Identify all protocols in use via traffic analysis, to discover and eliminate legacy protocols by locating the hosts transmitting them
- Verify network capacity and test capacity between remote sites using throughput testing at full Gigabit rates

### Summary

With increasing bandwidth demands, network professionals are constantly looking to maximize network efficiency, ensure adequate bandwidth, and deliver high network performance. Adhering to best practices using the OptiView Series III Integrated Network Analyzer can help network engineers increase employee productivity, free up IT resources, and improve communication and data sharing. In addition, leveraging best practices to monitor, baseline, and manage the network can help network engineers proactively approach issues such as P2P traffic, unwanted protocols, and network problems with factory default switch configurations.

### The business case for a portable, integrated network analyzer

The OptiView Series III Integrated Network Analyzer helps network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. It gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. No other portable tool offers this much vision and all-in-one capability to help you:

- Deploy new technologies and applications
- Manage and validate infrastructure changes
- Solve network and application performance issues
- Secure the network from internal threats

It shows you where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of the OptiView Analyzer to give you vision and control of your network. To learn more about OptiView, go to [www.flukenetworks.com/optiview](http://www.flukenetworks.com/optiview).

#### NETWORK SUPERVISION

**Fluke Networks**  
P.O. Box 777, Everett, WA USA 98206-0777

**Fluke Networks** operates in more than 50 countries worldwide. To find your local office contact details, go to [www.flukenetworks.com/contact](http://www.flukenetworks.com/contact).

©2007 Fluke Corporation. All rights reserved.  
Printed in U.S.A. 6/2007 2805664 H-ENG-N Rev A