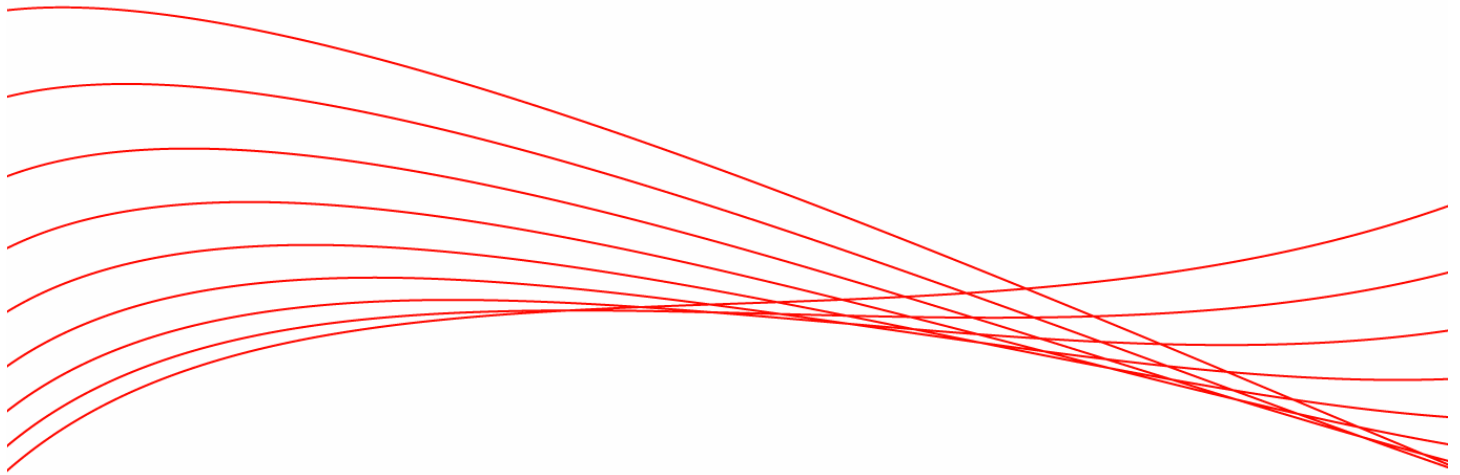


Traffic Management for the Enterprise



Introduction	2
The Importance of Traffic Management.....	2
Types of Network Traffic.....	3
Bursty traffic	3
Interactive traffic	3
Latency sensitive traffic.....	3
Non-real time traffic	4
Traffic Management: Standard vs. Best Practices	4
Traffic Management Technologies	5
XRMON and the Benefits	5
sFlow and the Benefits	6
Meeting Today’s Traffic Management Requirements –	8
ProCurve Networking Adaptive EDGE Architecture	8
ProCurve Traffic Management	9
ProCurve Traffic Management Products.....	9
ProCurve Manager Plus	10
Summary	11
For More Information	12

Introduction

Technology is intended to create efficiencies – not headaches. Indeed, emerging network technologies, such as gigabit Ethernet, wireless Local Area Networks (LANs), mobile network connections and Voice over Internet Protocol (VoIP) enable increased productivity. However, adopting new technology may seem – at first glance – to increase the complexity of both the network infrastructure and the network administrator’s job. This complexity can appear to intensify as more remote users log on, additional applications are extended to partners and customers, and different traffic types are flowing across a single network.

As the enterprise network infrastructure expands to support different types of traffic and users, traffic management becomes critical. Complete visibility into a network’s behavior becomes more important and more challenging. What is – or isn’t – happening throughout the network grid – including application performance, bandwidth utilization, network congestion and appropriate prioritization of user and application traffic – are questions that often go unanswered.

Most traffic management solutions available in the market have serious limitations: too expensive, difficult to use, overly taxing on bandwidth, and unable to scale with high-speed networks. ProCurve Networking by HP, however, addresses the traffic management requirements of today’s enterprise networks and overcomes the limitations of other solutions. Robust traffic management capabilities are integrated throughout the ProCurve portfolio, including:

- ProCurve Manager Plus Traffic Monitor, which shows detailed information on top sources of network traffic and connections on each network segment
- ProCurve Extended Remote Monitoring (XRMON), which is the technology used by the Traffic Monitor software in ProCurve Manager Plus
- sFlow, which has been incorporated into the ProCurve Routing Switch 9300m series and Switch 5300xl series

As a cornerstone of the ProCurve Networking Adaptive EDGE Architecture™, traffic management technologies enable companies to effectively administer networks of all shapes and sizes. In addition, they allow network administrators to make smart decisions about network access, traffic prioritization, traffic flows, and bandwidth optimization from one central management console and then easily propagate these decisions out to the edge of the network for enforcement.

This paper outlines ProCurve Networking traffic management solutions, which provide valuable insight into LAN performance – from the network core to the network edge.

The Importance of Traffic Management

The LAN has evolved from a transport mechanism to a strategic business tool for many companies. Three major and interdependent forces have driven this transformation: the Internet, an increasingly mobile workforce, and the convergence of multiple types of data traffic running through the same network.

As a result, networks are becoming more public, more extended, and more complex. Enterprises are being forced to understand and support new applications and new connection management solutions for their various constituencies – employees, partners, and customers.

In today’s connected business environment, straightforward and effective traffic management from the network core to the network edge is essential. Enterprises need a network infrastructure that scales to meet new business needs and manages added complexity in a cost-effective manner.

In addition, network administrators are expected to control the network in such a way that it is transparent to users. Essential information assets need to be instantly available around the clock. However, this is impossible to achieve without the right

tools to make smart, informed decisions. Most network administrators do not have simple, affordable tools that can quickly answer the following questions, regardless of the size of the network:

- Is network performance slowing down or becoming congested?
- Is a Network Interface Card (NIC) chattering, effectively clogging the network?
- What is the current network usage, and what has it been in the past hour?
- Which network routers are most active or over-utilized?
- Why is a server slow or inaccessible?
- Which users and applications are driving network traffic?
- Which users and applications are starving for bandwidth?
- How much bandwidth do I need for new applications?

Types of Network Traffic

Today's networks must accommodate an increasingly complex set of data traffic. Network traffic management tools enable network administrators to identify traffic types, users and applications, and facilitate the optimization of the network so all three components interact appropriately.

The first step toward network optimization is to understand where inefficiencies and problems are located, and why they are occurring.

The integration of various standards and technologies, such as XRMON and sFlow, combined with effective traffic management software tools, such as ProCurve Manager Plus, enables companies to effectively support various traffic types with optimum fault resolution, performance management, and capacity planning on all ports.

The following examples represent several types of network traffic that must be considered and supported:

Bursty traffic

Example: Large file downloads such as FTP, multimedia content (.wmv, .swf, .mov files) and graphic content (.jpg, .gif files).

Problem: Can result in spikes in bandwidth consumption, effectively starving other applications of bandwidth for a brief period of time. Interactive traffic and latency sensitive traffic are particularly susceptible to problems caused by bursty traffic.

Solution: Set a maximum constraint to limit access to bandwidth.

Interactive traffic

Example: Secure Socket Layer (SSL) transactions, Instant Messenger and Telnet sessions all consist of relatively short request/response, and generally support real-time interaction with end users.

Problem: Susceptible to competition for bandwidth, which can result in poor and unpredictable application response time.

Solution: Prioritize over less essential traffic and traffic that is less dependent on real-time response (such as e-mail).

Latency sensitive traffic

Example: Streaming applications, Voice over IP, and video conferencing all generate a steady stream of traffic, which consumes a significant amount of bandwidth.

Problem: Susceptible to competition for bandwidth, which can result in poor and unpredictable application response time. These applications can also easily saturate available bandwidth, effectively starving other applications.

Solution: Set minimum guarantees of access to bandwidth prioritized by business need, and set maximums to prevent any application from consuming too much bandwidth.

Non-real time traffic

Example: E-mail and batch processing applications are the predominant sources of non-real time traffic within the enterprise.

Problem: Can consume bandwidth that could be used by more business-critical applications.

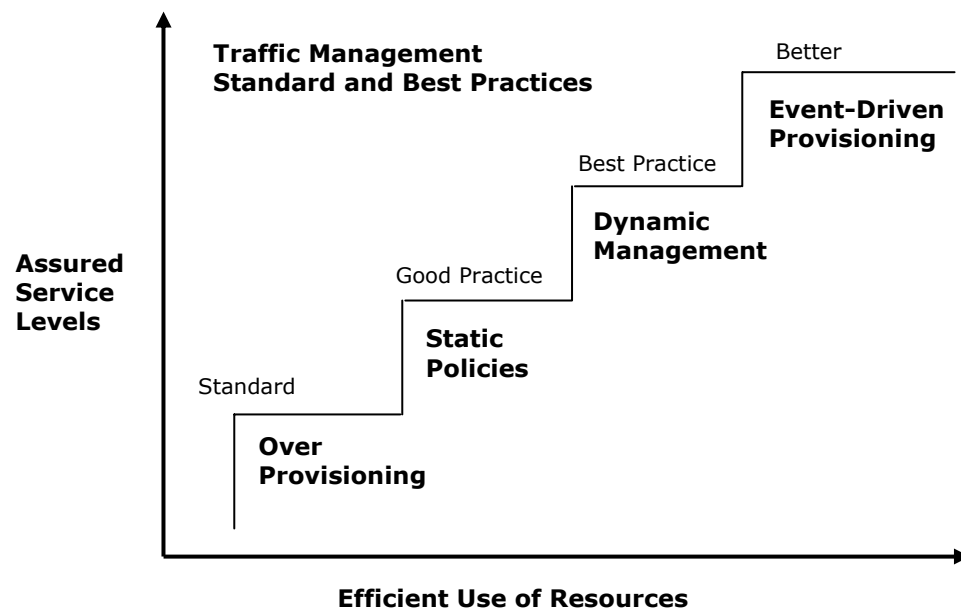
Solution: Schedule bandwidth assignment for non-business hours; set a maximum bandwidth constraint and low prioritization during business hours.

Traffic Management: Standard vs. Best Practices

Making well-informed decisions on how to monitor, manage, and fine-tune a business network begins with a traffic management infrastructure strategy built upon industry best practices. Understanding and implementing best practices to create assured service levels, and to create efficiencies across network resources, will help network administrators provision traffic and create intelligent networks.

By taking a look at how many businesses provision resources, it's easy to understand how service levels can be assured. The following (Figure 1.) highlights different network practices and outcomes for network service levels and efficient use of resources.

Figure 1. Assured Service Levels and Best Practices



Standard practice: Over provision

High capacity reduces possibility of network slowdown. (Downside: unnecessary expense)

Good practice: Static policies

Eliminate unnecessary traffic. (Downside: doesn't adapt to changing business needs)

Better practice: Dynamic management

Identify historical trends and patterns in order to appropriately set and enforce priorities. (Upside: meets business needs and centrally sets priorities with efficient, distributed enforcement)

Best practice: Event-driven provisioning

Smart, real-time assignment of resources based on user and application needs. (Upside: provides a hands-free, optimal allocation of network resources that tightly matches business requirements)

Traffic Management Technologies

Understanding the traffic traversing an enterprise network has always been a complex task, and the solutions for managing traffic have historically been very expensive. Traditionally, network traffic monitoring has been achieved using probes. This worked very effectively in shared networks where a single instrument can monitor all the traffic. However, with switched point-to-point networks, every port on a switch needs to be monitored to achieve the same visibility to network traffic. In addition, switches and routers make packet-forwarding decisions that affect the flow of traffic through a network. Understanding these traffic flows is critical to maintaining visibility to network use and misuse¹.

More than a decade ago, ProCurve set out to address these problems by inventing embedded sampling technology for network traffic, which is the basis of both XRMON and sFlow today.

By embedding a packet sampling technology into the network devices, Hewlett-Packard enabled network administrators to gather data across the entire network, instead of merely a few places where they could afford to install a network probe. This sampling technique also provided exact traffic level measurements and an accurate representation of who was causing the traffic, while adding minimal overhead to the network. Finally, packet sampling made it possible to provide a traffic management solution that scaled in accordance with increasing network speeds.

With the embedded agents on most ProCurve devices, a network administrator can track traffic levels across all segments of the network. And through network management applications, such as ProCurve Manager Plus, traffic issues and the responsible nodes are easily identified, located, and isolated. With such information, the network administrator can take the appropriate action to resolve the issue.

ProCurve network management products use the embedded traffic sampling technologies to present the user with in-depth traffic analysis. Technology integrated into the ASICs of ProCurve switches and routing switches provides the ProCurve Manager Plus management station with real-time traffic updates. ProCurve Manager can automatically select the sampling device for each measured segment on the network. Once the devices to be monitored are selected, the management station begins receiving samples of the relevant traffic information. From this information, the Traffic Monitor displays a utilization percentage, which can further yield the "top talkers" on that segment along with MAC addresses, IP addresses, Source and Destination ports, and connection and protocol information.

XRMON and the Benefits

XRMON is a sampling technology that has been embedded into ProCurve network devices for more than 12 years. Formerly known as Embedded Advanced Sampling Environment (EASE), XRMON samples network traffic, captures traffic levels and users across the entire network, and adds very little overhead to the infrastructure.

¹ Reves, Joseph, Panchen, Sonia. "Traffic Monitoring with Packet-Based Sampling for Defense against Security Threats." Page 1. 2002. White paper.

XRMON is completely unobtrusive, with the network taking no appreciable performance hit when conducting the sampling strategy. This aspect can be a significant benefit for the many situations where general network traffic patterns are the only necessity. Since only packet headers are sampled it is secure; not only because it uses a fraction of sample packets captured, but also because the samples are randomly selected XRMON will not allow eavesdropping on a conversation.

With the sampling rate adjusted once per hour, ProCurve XRMON is statistically accurate to a 95 percent confidence level. This accuracy is more than adequate for traffic flow analysis for network planning and top-down network troubleshooting. Problems are identified quickly so that segment-specific troubleshooting can be performed with a network analyzer. And because ProCurve XRMON is a sampling technology that requires very little in terms of system resources, it is easily scalable to monitor switched and shared high-speed technologies, such as Gigabit Ethernet, 100Base-T and FDDI.

sFlow and the Benefits

An Internet Engineering Task Force (IETF) draft standard for network traffic monitoring and accounting, sFlow represents a monitoring technology that gives complete visibility into the use of networks and enables network resource optimization. sFlow and XRMON are very similar; in fact, it is reasonable to say that sFlow is an evolution of XRMON. Therefore, many of the same benefits exist. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch, router or stand-alone probe) and a central data collector, referred to as the sFlow Analyzer.

The sFlow Agent uses sampling technology to capture traffic statistics and packet headers from the device it is monitoring. sFlow Datagrams are used to immediately forward the sampled traffic statistics to an sFlow Analyzer for analysis (see Figure 2. sFlow in Operation)². The architecture and sampling techniques used in the sFlow monitoring system are designed to provide continuous site-wide (and network-wide) traffic monitoring for high-speed switched and routed networks. sFlow specifically addresses issues associated with³:

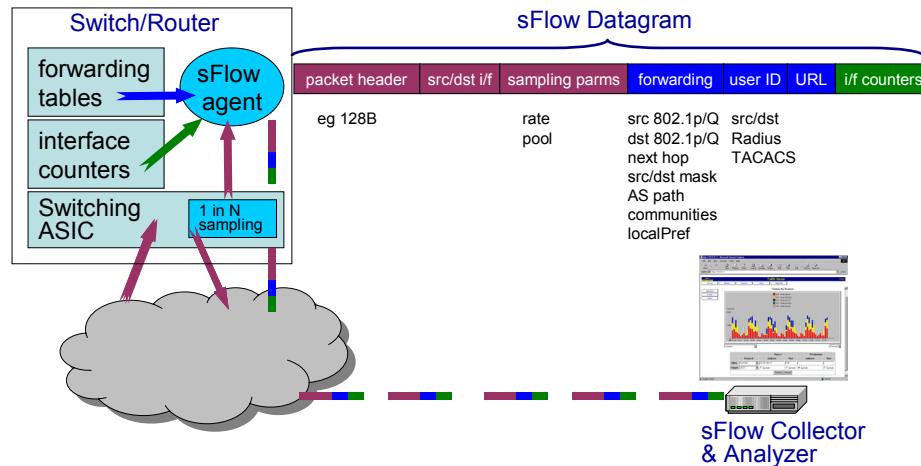
- Accurately monitoring network traffic at Gigabit speeds and higher
- Scaling to manage tens of thousands of agents from a single point
- Extremely low-cost agent implementation

² <http://sflow.org/about/index.php>

³ Footnote 3

Figure 2. sFlow in Operation

sFlow (RFC 3176) in Operation



Embedded in ProCurve hardware, sFlow technology helps create network visibility by:

- Capturing detailed, comprehensive traffic data across the entire network infrastructure
- Sending data in raw format so the information can be analyzed on a real-time basis or on demand
- Restricting device and network overload

In addition, sFlow saves money. Because the technology is embedded in the device ASICs, there is no additional cost associated with equipment. sFlow can also help control network service costs by ensuring the network traffic remains within service level agreement (SLA) guidelines, and can be used to formulate a history of network utilization so it is possible to allocate costs per user.

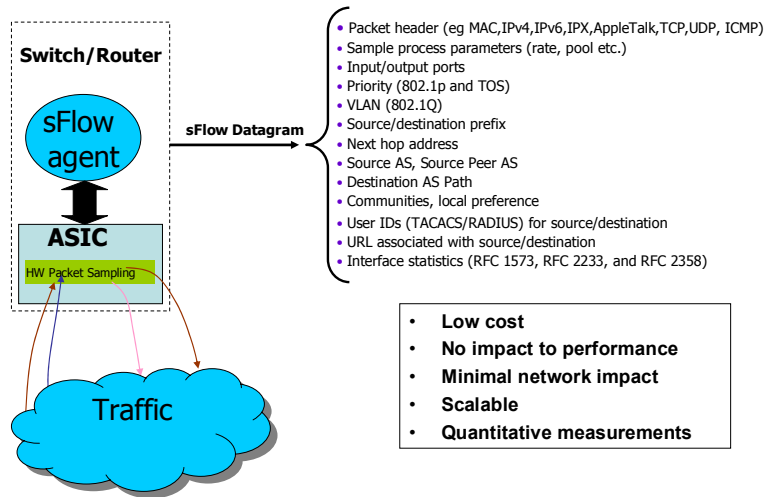
In summary, sFlow monitoring technology gives complete visibility into the use of networks, enabling performance optimization, accounting/billing for usage and defense against security threats.

(see Figure 3. sFlow Summary⁴)

⁴ <http://sflow.org/about/index.php>

Figure 3. sFlow summary

sFlow (RFC 3176) – Summary



Meeting Today's Traffic Management Requirements – ProCurve Networking Adaptive EDGE Architecture

The ProCurve Networking Adaptive EDGE Architecture™ was developed to secure the future of ProCurve customers by delivering the best central command with control to the edge. With control to the edge, companies can provide secure, robust functionality to support all current and future traffic and application types.

By definition, it is the network edge where users and applications connect, where traffic enters and exits the network, and where the network must determine how that traffic is handled.

The edge is where security priorities and policies must be enforced, where the user connects after being authenticated at a central command resource.

Without control to the edge, decisions about security and traffic must be deferred to the network core, impacting core performance and scalability, while at the same time requiring more bandwidth in all parts of the network – driving up cost and complexity. In addition, this opens the network to security attacks between the points where access is physically attained and where authorization is granted.

Control to the edge places selected functions from Layers 2, 3, and 4, and higher functions in edge switches. These switches control access and traffic flows to ensure the increasing set of applications can function correctly and concurrently without interference. Adaptive EDGE networks support both centralized cores and distributed cores with equal facility, because both core configurations can enforce the key decisions made at the edge.

Ultimately, the Adaptive EDGE Architecture enables highly available meshed networks – a grid of functionally uniform switching devices – to scale out to virtually unlimited dimensions and performance due to the distributed decision-making of control to the edge. Moreover, the EDGE architecture facilitates comprehensive traffic management throughout an enterprise infrastructure.

The ProCurve Networking Adaptive EDGE Architecture focuses on:

- Traffic monitoring to control bandwidth optimization throughout the network grid
- Integration of industry-standard virtual LAN (VLAN) and industry-standard security constructs to provide “out of the box” access management unavailable on non-EDGE ports
- Complementary implementation of industry-standard traffic routing and Layer 2 meshing, providing path failover and multi-path load balancing for robust reliability
- Unparalleled range of traffic prioritization features to provide traffic type coexistence and quality of services functions, virtually eliminating the need for custom network design architectures to ensure support of current and future voice, video and content delivery applications
- Centralized command of the edge for easy implementation of user security and application policies

ProCurve Traffic Management

ProCurve is uniquely positioned to provide traffic management solutions that are highly reliable and affordable, and optimized for security, mobility, and the convergence of voice, video and data applications.

ProCurve solutions deliver superior network traffic management capabilities, including:

- Identification of network congestion within a network
- Precise network policing of network traffic, from the network edge where the user connects to the network core

ProCurve network management solutions provide traffic management modules that utilize embedded packet sampling technologies to provide the network administrator with an in-depth view of the traffic levels across all ProCurve ports. The traffic management modules also offer the ability to drill down to see who is responsible for network traffic, so that it is possible to not only see when a problem exists, but also who is causing the problem.

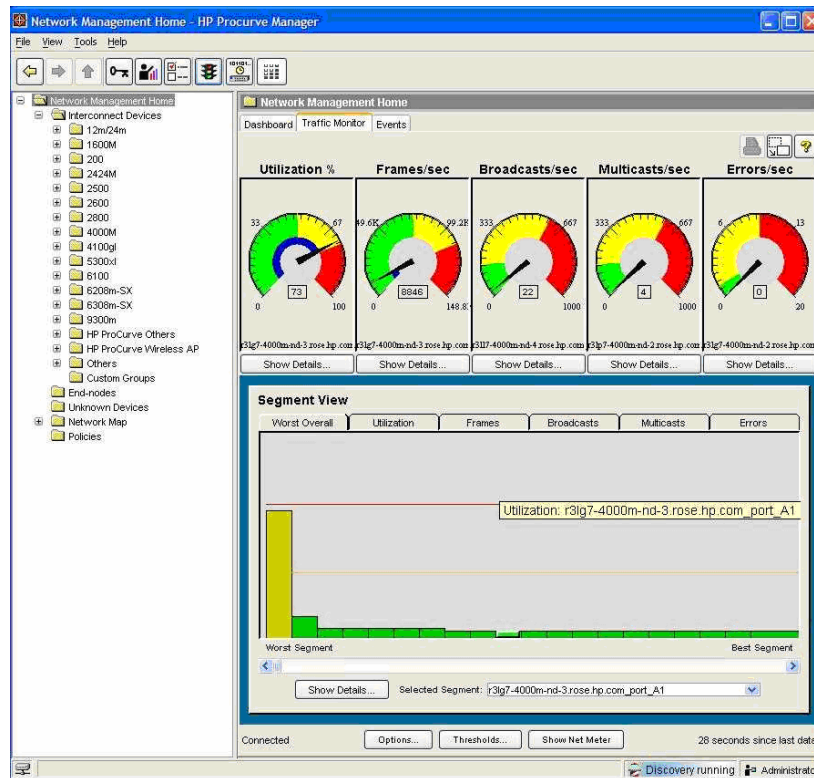
ProCurve Traffic Management Products

ProCurve offers a range of products that include and support traffic management technology (see Figure 4). All ProCurve Networking solutions enable end-to-end traffic management capability, providing complete network visibility from the core to the edge (see Figure 5).

Figure 4: ProCurve Traffic Management Products

ProCurve Product	Traffic Management Technology
ProCurve Manager Plus	Centralized traffic monitoring
ProCurve Routing Switch 9300m series	sFlow and XRMON (EP Blades only)
ProCurve Switch 5300xl series	sFlow and XRMON
ProCurve Switch 3400 series	XRMON and sFlow
ProCurve Switch 2800 series	XRMON and sFlow
ProCurve Switch 2500 series	XRMON

Figure 5. ProCurve Network Management: ProCurve Manager



ProCurve Manager Plus

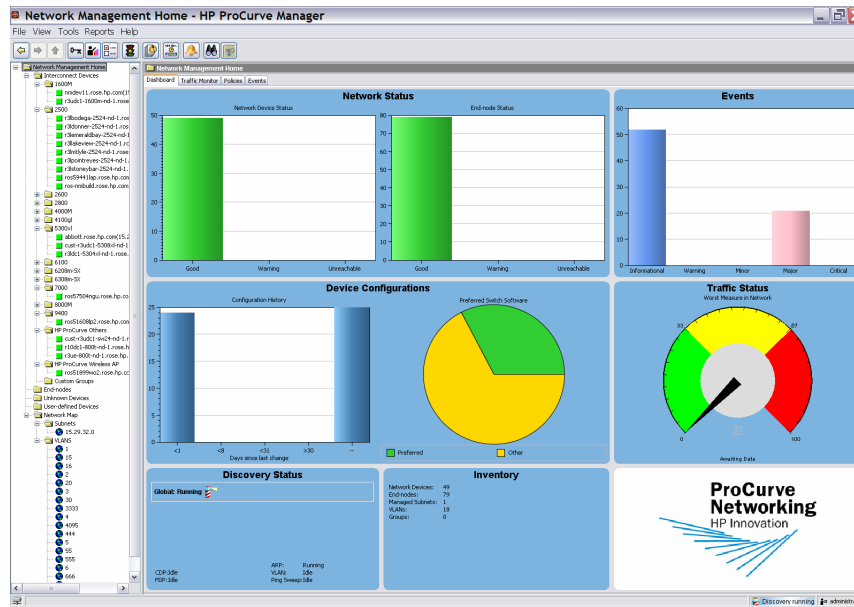
ProCurve Manager Plus is a complete, Windows-based network management solution that provides both basic and advanced management features for ProCurve devices. It allows users to discover, configure, monitor, and troubleshoot ProCurve devices. ProCurve Manager Plus includes features such as configuration management, VLAN management, in-depth traffic monitoring, group and policy management, and automated software updates.

ProCurve Manager Plus leverages patented sampling technologies to continually monitor traffic data in a low overhead manner that does not inhibit business-related traffic.

With this functionality, ProCurve Manager enables the user to easily drill down to see what is happening on the network, where it is happening, and who is driving that network traffic. For example, the network administrator can view a list of the top five users on any segment during any minute in the past hour, and can instruct the network to monitor all segments or only the network segments that are most business critical.

All in all, ProCurve Manager Plus provides an easy-to-use central console to consolidate traffic views across the network (see Figure 6). This is the critical first step to enabling network administrators to optimize network utilization and match network service levels to business needs.

Figure 6. ProCurve Manager Plus



Summary

As enterprises add new network applications, support remote users, implement different types of traffic, and extend to partners and customers, having complete visibility into an infrastructure's behavior becomes increasingly important and challenging. More than ever, straightforward and effective traffic management from the network core to the network edge is essential to business success.

ProCurve provides traffic management solutions that are highly reliable, affordable, and optimized for security, mobility, and the convergence of voice, video and data applications. An integral part of the ProCurve Adaptive EDGE Architecture, ProCurve's traffic management tools collect, measure and analyze bandwidth data – enabling network administrators to quickly identify issues, isolate problems, and optimize resource utilization. ProCurve Networking by HP solutions meet customer needs by consistently delivering on the value propositions of high availability, affordability, security, ease-of-use, and interoperability.

For More Information

To learn more about ProCurve Networking by HP solutions, contact your local ProCurve sales representative or visit our website at: www.procurve.com.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

XXXX-XXXXEN, 5/2005