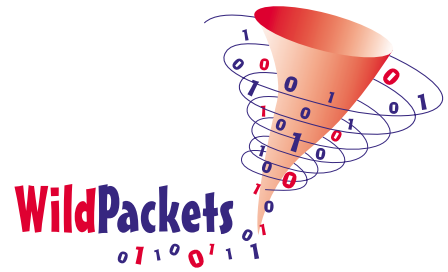
Using EtherPeek in the Enterprise Environment



Introduction

The evolution of enterprise networking means that optimal network management is more critical to the corporate business environment than ever before. According to research statistics published by Datamonitor, the global enterprise network management market will be worth nearly a billion dollars by 2002. How can today's network manager cope with the increasing complexity of the distributed networking environment?

This paper describes a simple solution to cost-effectively manage enterprise networks. WildPackets' EtherPeek packet analyzer, together with Netopia's Timbuktu, comprise a sophisticated method for monitoring performance across the enterprise network, from multiple local segments to a remote LAN.

Network Complexity

The more things change, the more they remain the same

It's no mystery: today's enterprise networks are more complex than ever. Though the complexity of competing standards, mixed topologies, immature protocols, and inferior technologies has given way to the domination of a simpler story – switched Ethernet, Cat 5 cabling, and TCP/IP – network complexity still reigns. In a period of only a few years, fiber and wireless transport media have emerged in the Enterprise. Hub-based topologies are yielding to switched-based topologies, as shown in Figure 1.

Networks are now designed to be modular and scalable. They must be load balanced, redundant, and have auto-recovery capabilities in the backbone.

Networks need to be application-aware and prioritize traffic based on content. With so many technological features available and so many hardware permutations possible, it is easy to go wrong.

If the network is designed properly, significant performance and reliability are achievable. If not, the result can be a network with lower performance, reliability, and manageability. Poor network design leads to situations where a misconfigured workstation may introduce errors that disable the entire domain.

Swapping out a hub for a switch might sound like a savvy response to the ubiquitous "network's slow" complaint, but realistically one must recognize that application design, the mix of network protocols, the placement and performance of servers and networking

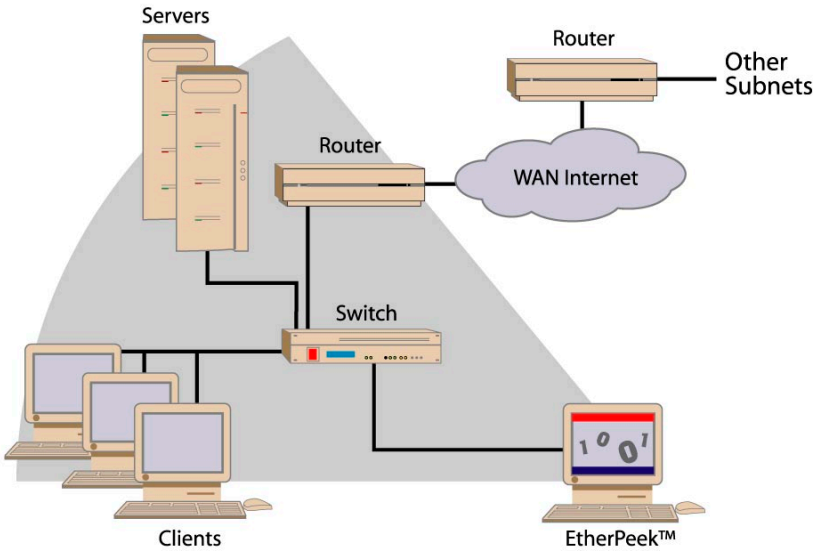


Figure 1. EtherPeek sees a segment of a switched network.

devices are at least as important as simply adding more bandwidth and switching capability to the network.

While personal computers increased personal productivity, it was the networking of these computers that revolutionized business processes with the accessibility of information and the speed with which it is shared. New technologies, new applications, and changes in network architecture continue to have major impacts on network performance. IT activities are now intricately tied to core business objectives. In fact, networks have never been more mission-critical than they are today.

It was difficult enough to convince the decision makers to buy the infrastructure, now you have to convince them to invest in tools to fix it!

As network managers race to re-architect existing segments to keep pace with the technology and outpace the demands of new applications coming online, IT budgets are under increased scrutiny. Managers and decision makers are under more pressure than ever to deliver high performance, low downtime, and to do it cost effectively. When network managers bring in LAN switches that promise 100Mb to the desktop, they need to show results.

Though network managers might hope that the ever-evolving nature of networking technology might lead to a simpler life, such has not been the case. The promise of zero-administration or self-healing networks is a pipe dream. New technology means redesigning the network. It means immature products and new problems.

New problems require new troubleshooting tools and techniques. Steep learning curves and high-priced kitchen-sink tools add to the difficulties for over-burdened IT professionals. Coupled with this fact is that it is increasingly difficult to find individuals with the skill set to manage today's networks.

High-bandwidth, business critical applications such as e-commerce, ERP, HR, supply chain management, manufacturing, etc., are network dependent. Network downtime and poor performance can have drastic effects on the business' bottom line.

All of these aspects of today's complex networks mean that getting ahead of the curve is more difficult than ever. Network analysis tools need to help determine capacity, establish baselines, identify bottlenecks, and even identify application deficiencies that affect performance. More than ever network managers need simple-to-use and distributable tools that can be used to monitor networks, as well as provide real time, useful troubleshooting analysis. And, more than ever, network managers need cost-effective tools that can be justified to management.

As networks gain in visibility, the tools to manage them must be efficient and cost effective.

In a Nutshell

- **Your company or client has a major investment in network infrastructure.**
- **It's paid off. Network applications reach around the globe.**
- **Don't look now: the network is mission-critical.**
- **Delays and downtime cost big bucks.**
- **It's hard to find good help these days!**
- **New applications are in the pipeline.**
- **The warehouse wants wireless.**
- **"Hey, the network's slow."**
- **Budgets are due...**
- **ROI?**

Simple Solutions for Complex Networks

WildPackets provides a comprehensive set of tools that allow you to cost-effectively manage your increasingly complex enterprise network. WildPacket's EtherPeek, TokenPeek, and AiroPeek set the industry standard for ease-of-use while delivering superior diagnostic and analytic capabilities at an affordable price. By certifying Netopia's Timbuktu for use with WildPackets award winning* tools, WildPackets provides the ability to achieve high quality statistical analysis in a distributed fashion, whether you need to analyze multiple segments in your local datacenter or troubleshoot network problems on a remote LAN.

Timbuktu is the leading enterprise solution for cross platform remote control. With Timbuktu, network managers can deploy EtherPeek, or the distributed capture agent EtherHelp, throughout the enterprise, allowing engineers to manage and troubleshoot LAN segments wherever they exist.

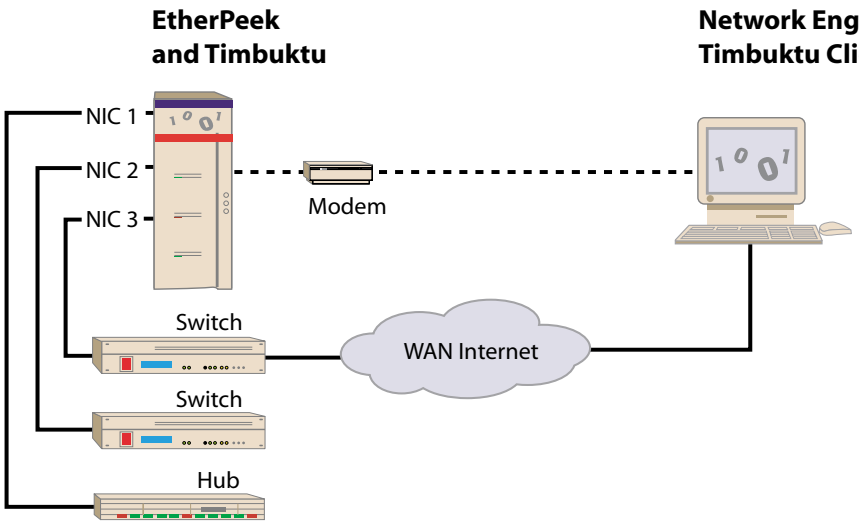
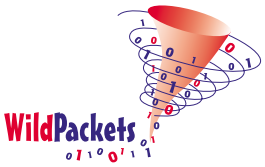


Figure 2. EtherPeek and Timbuktu utilizing multiple NICs.

* EtherPeek™ was awarded PC Magazine Editors' Choice Award, May 3, 2001; 5 Mice rating from Editors and Lab of MacWorld Magazine, January 2000; "Product of the Year" award from LAN Magazine, 1994; and "Best New Network Product" Editor's Choice Award from MacWorld Magazine, 1993.



Key Benefits of Timbuktu

- **High level of security**
- **Out of band modem access if network down**
- **Industry leading interface**
- **Centralized administration**
- **Multiple concurrent consoles**

With EtherPeek's uniquely modular architecture, coupled with Timbuktu, network managers have the ability to remotely perform sophisticated diagnostic tests, monitor network traffic and events, trace illicit network activities, and perform trending, as well as test and debug network hardware and software. Well-known for its friendly graphical interface, EtherPeek sets the industry standard for ease-of-use while offering all the expert troubleshooting capabilities you expect.

EtherPeek's powerful packet filtering mechanism, used real-time or after capture, isolates traffic by specific node, protocol, error type and/or packet content. EtherPeek's simple "Make Filter" and "Select Related" commands allow you to immediately create and filter for specific network traffic by highlighting a packet line. Real-time network statistics depict traffic in terms of overall utilization, nodes, conversations and protocols. History statistics provide performance data through traffic captured for a specified time interval.

Easily identify "talkative" nodes or "chatty" protocols generating unnecessary traffic. Discover which protocols consume the most bandwidth and which nodes communicate most frequently. Or check to see how a router is handling traffic during peak hours.

Timbuktu provides multi-platform control of remote installations, including zero administration deployment, centralized management, and several layers of security specifically designed for today's enterprise environment. The network manager can easily deploy, configure, monitor, and update remote EtherPeek installations throughout the enterprise. The network manager then utilizes the same EtherPeek interface to which he or she is accustomed, as if the network resources were local. Only mouse and keyboard movements are sent over the network. Further, Timbuktu takes advantage of advanced caching technology to allow minimal consumption of the network resources and maximize performance.

Timbuktu has features that not only meets IS security needs, but also provides the flexibility to work with existing security measures such as firewalls, Virtual Private Networks (VPN), PAP, CHAP, Point-to-Point Tunneling Protocol (PPTP), SecureID™, etc.

Timbuktu security features include:

- Master Password configuration to prevent any changes to the security specifications on a machine.
- Can be configured to use Windows NT and Windows 2000 security directly, allowing administrators to leverage the security already deployed within their environment or use built in username/password controls.
- Utilizes a Site Key Generator that enforces the established security policies, e.g. disabling various features, modifying the TCP ports used, requiring Site Keys in order to connect to users, and restricting modifications after the initial installment and configuration.
- Supports secure screen blanking on remote machines. When this option is enabled, a remote control session will automatically blank the screen on the host, preventing the disclosure of any sensitive or confidential information to somebody with physical access to the machine.

Using Timbuktu's dial-up capability, network engineers can attach to a remote EtherPeek out-of-band when the network is down. A second adapter can be added to the EtherPeek/Timbuktu box for high-speed out-of-band access. Simply connect the second adapter to a separate segment. As shown in Figure 2, you can add multiple adapters to monitor multiple segments. Add one card per switch (up to the limit your hardware supports). When you start EtherPeek, simply choose which adapter to monitor.

Alternatively, use a matrix switch to choose the switch you wish to manage, as shown in Figure 3.

Summary

Using EtherPeek with Timbuktu in the enterprise environment is a viable option for network professionals. Network engineers can capture and analyze data in real-time, just as if they were using EtherPeek locally. They can manage multiple remote sessions simultaneously. Capture files can easily be transferred locally for historical baselining or off-line troubleshooting.

With EtherPeek + Timbuktu, network professionals can spend their time managing the infrastructure and planning for the future rather than flying to remote locations, conveniently and remotely diagnosing and troubleshooting network performance throughout the enterprise.

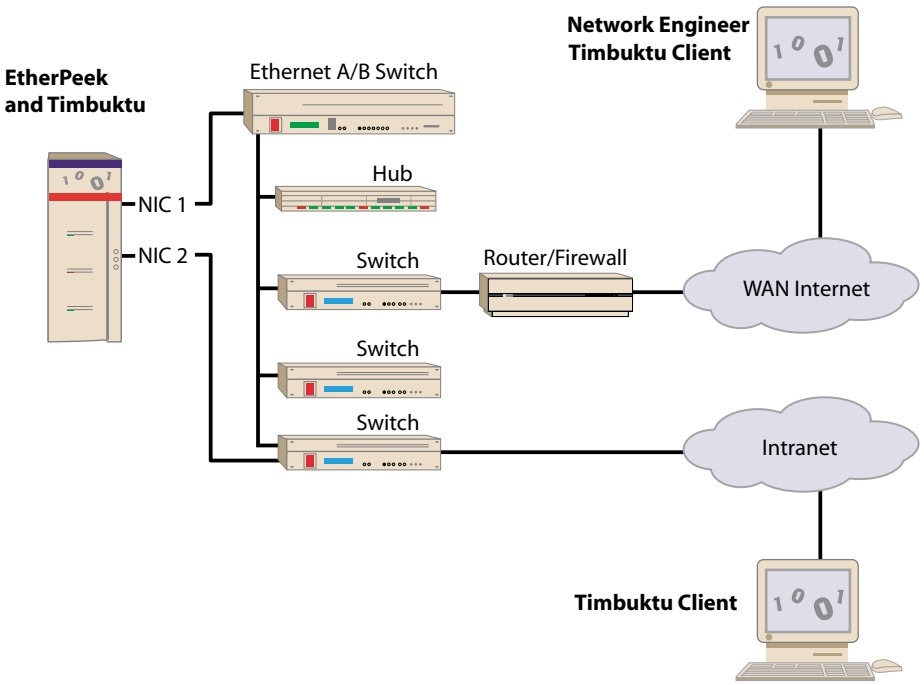


Figure 3. EtherPeek and Timbuktu utilizing an Ethernet A/B switch.