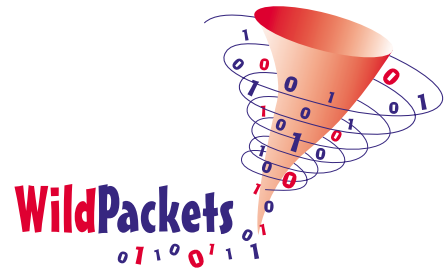
Applying EtherPeek to Switched Network Management



Applying EtherPeek to Switched Network Management

Contents

Introduction

There are numerous articles written concerning LAN analysis tools and their ability to provide the same degree of insight into switched network traffic as in a shared-media environment. This document attempts to characterize the switched infrastructure in the context of network protocol analysis and to show how WildPackets' EtherPeek can be used effectively to analyze and troubleshoot problems. This paper will further describe how EtherPeek can be a key tool in providing proactive network management in switched topologies and how analysis remains feasible and effective even when network traffic is segregated and isolated.

WildPackets, Inc. (formerly AG Group) developed the EtherPeek Ethernet LAN protocol analyzer in 1990 as a tool for capturing, decoding, and analyzing traffic in real-time for all devices in a LAN.

The structure of the LAN itself, however, has changed dramatically in the ensuing years. Armed with information about how to apply EtherPeek to this new structure, the network engineer can integrate the protocol analysis process into the overall spectrum of tools and utilities available for network troubleshooting and analysis. This array includes switch statistics, available through vendor-specific switch management software, and the industry-standard SNMP/RMON statistical and packet gathering tools available today.

Shared versus Switched Networks

In the 1980's, the networking marketplace saw the beginning of the migration away from shared, coaxial Ethernet to the realm of twisted pair, hub-based Ethernet networks. Both coaxial connectivity and early twisted-pair hubs created an infrastructure in which every station's transmissions were visible to every other station within what is referred to as a "collision domain." Bridges could connect a series of collision domains into a larger infrastructure called a "broadcast domain." A broadcast domain consists of all the interconnected stations that receive each other's broadcast and multicast packets and is an area bounded by routers. A router, therefore, forms the end of a broadcast domain and serves as the gateway into a different broadcast domain.

In a network where all stations in a collision domain "see" all traffic from all the other stations in the collision domain, we say that the network medium (the cable system) is "shared." That is, everyone must compete with everyone else to take turns accessing the medium for transmitting packets.

Protocol analysis in a shared-media environment is straightforward, as depicted in Figure 1, below. By simply attaching an analyzer at any point in a collision domain, one can acquire 100% of the transmitted packets from all stations within that domain.

Over the decade of the 1990's, the networking marketplace saw dramatic increases in desktop computing power. As application programs grew in complexity and sophistication, the need to send large quantities of data as quickly as possible grew proportionally. The shared-media environment forced all of these communicators to compete with each other for the use of the media. This proved to be an inadequate solution. To facilitate the demands of these increasingly complex networks, the industry experienced an evolution from shared media to switched network infrastructures. Today star-wired LANs using switches as the central connecting points are pervasive, creating large meshed network topologies.

While switched networks provide part of the solution for efficient use of the network media and infrastructure, they bring with them some inherent restrictions and limitations to the protocol analysis engineer. By their nature, switches do not forward all packets to all stations. Of course, broadcast and multicast packets continue to be forwarded out all ports of a switch and, therefore, reach all the stations in the broadcast domain. This is identical to the shared-media model. Directed frames, however, are forwarded in a much more intelligent manner. A "directed frame" is one with a specific Ethernet address as the destination target address. It is intended for only one recipient. The switch evaluates the Ethernet destination address on all incoming packets and forwards them only through the single port to which the intended target machine is attached.

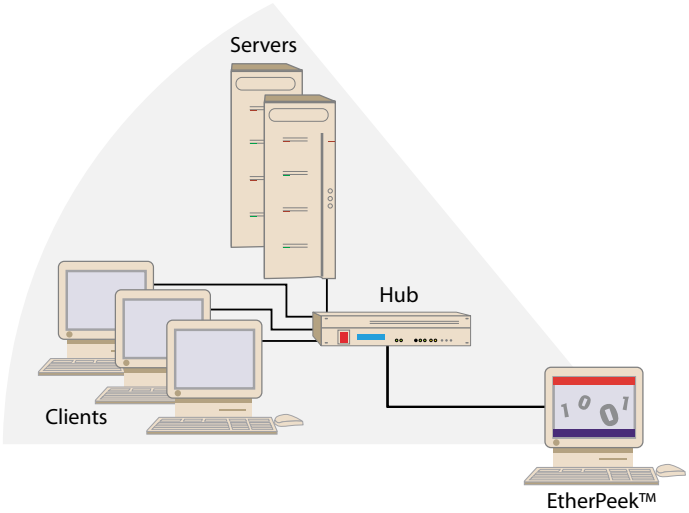


Figure 1. A shared-media network with EtherPeek

As a result of this behavior, the network benefits from a reduction in contention for network bandwidth and a corresponding reduction in Ethernet collisions and the resulting retransmissions. This can easily be seen if one considers a simple topology in which a single switch has two file servers and sixty workstations attached to it. At the same time that Workstation #1 is sending a packet to File Server #1, it is possible for Workstation #2 to send a packet to File Server #2. Neither workstation is required to wait for the other, as would have been the case in the older shared-media networking model.

EtherPeek in the Switched Network Environment

Now consider what happens when a network engineer attaches EtherPeek to some other port on the switch with the sixty workstations and two file servers just described, as shown in Figure 2. Since the packet from Workstation #1 is addressed to File Server #1, the switch only forwards that packet to the port to which File Server #1 is attached. The packet is not forwarded to the port to which EtherPeek is attached. EtherPeek does not see this packet, or any other packets that are directed to specific Ethernet destinations. This is the inherent nature of a switch and is normal, correct, and performance-enhancing behavior. If a workstation were to transmit a broadcast or multicast packet, then the switch would forward it out all of its ports. EtherPeek would be able to capture broadcast and multicast packets since all of these packets would be sent by the switch to the EtherPeek port and to all other ports.

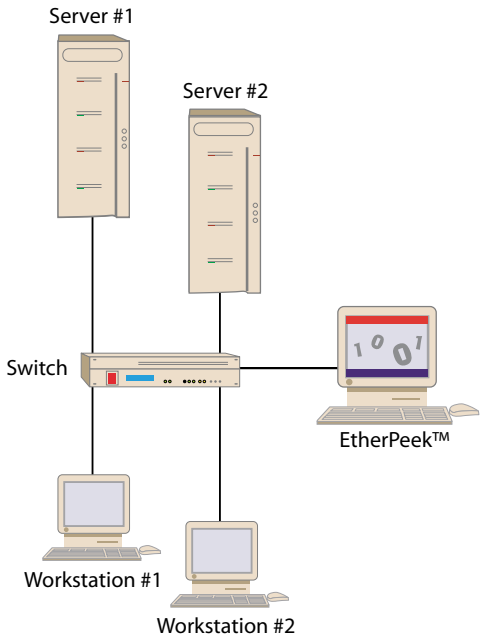


Figure 2. EtherPeek attached to a switched network.

To overcome this inherent behavior, and to allow protocol analyzers to be attached effectively to switches, the switch manufacturers have implemented a mechanism by which the switch administrator can select a port to be dedicated to the analysis process. This is done through the switch management software and implies that the particular model of switch supports this type of configuration. In addition, even if a switch does not support the selection of a particular port for use with an analyzer, there are ways to work around the restriction and still effectively connect EtherPeek for protocol analysis.

Configuring a Protocol Analysis Port

The most common term used to refer to the special port configured for use by a protocol analyzer is a "Mirror Port." In the Cisco environment, it is called a "Span Port." The table, below, shows a list of the terminology used by various vendors to refer to the configuration of a special protocol analyzer port in their switch equipment.

Imagine that a File Server is attached to Port #12 on a particular switch. For the sake of discussion, assume that EtherPeek is attached to Port #7 on the same switch. Through the switch management software a command is issued that "mirrors" Port #12 to Port #7. All traffic going in or out of Port #12 (to/from the File Server) is copied and sent out Port #7 (to EtherPeek). EtherPeek is now able to capture all traffic to and from the File Server. We say, "the File Server port is being mirrored."

There are a variety of port mirroring options available from various vendors and, although the essence of the mechanism is the same (mirrored traffic is sent to the analyzer port), the options and configuration parameters vary from vendor to vendor. It is important to consult the switch documentation to understand the capabilities and configurations required to activate port mirroring.

Vendor	Terminology
Xtreme Switches	Port Mirroring
CISCO	Port Spanning
3 COM	Roaming Analysis Port
XYLAN	Mobile Port
Nortel Networks	Copy Streaming
NetScout	Roving Port
Foundry Works	Port Mirroring

Mirroring Multiple Ports Simultaneously

It is possible, with some vendors' equipment, to mirror more than one port at a time. For example, several users may be complaining that they are having problems printing. EtherPeek could capture the traffic to and from all of the users if the switch mirrored each of the users' ports back to the EtherPeek port.

A Virtual LAN (VLAN) environment is another case in which specialized port mirroring may come into play. Imagine the switched network that was previously described. This network has two file servers and sixty workstations attached to a single switch. When implementing a VLAN, one may decide that 30 of the workstations and one of the file servers will be Network #1 and the other 30 workstations and the other file server will be Network #2. Hence, the administrator of the switch has created two separate broadcast domains and, therefore, two separate "virtual" networks from the devices attached to a single switch.

It is also possible, with some vendors' equipment, to mirror all traffic within a VLAN and have a copy of each packet transmitted in the VLAN sent to the analyzer port.

The Problem With Aggregate Bandwidth

In any situation where an analyzer port is going to receive mirrored traffic from more than one mirror port, there is a possibility that the overall aggregate of packets from all of the mirrored ports may exceed the bandwidth capacity of the analyzer's mirror port itself.

EtherPeek is attached using a 100 Mbps Ethernet connection to Port #7 on a switch. The switch is configured so that Port #12, #13, and #14 are mirrored onto Port #7. If the devices attached to the three-mirrored ports are each transmitting 45 Mbps (45% utilization on their individual 100 Mbps connections to the switch), then there will be 135 Mbps of aggregate traffic that the switch will try to send out Port #7 to EtherPeek. This will result in packets being dropped by the switch. The switch has no way to send 135 Mbps over a 100 Mbps Ethernet connection to EtherPeek.

If EtherPeek is going to be used with multiple port mirroring, then there must be consideration, and awareness, of the fact that packets exceeding the bandwidth capacity of the mirror port to which EtherPeek is attached will be dropped.

Analysis Of Non-Managed Switches

Some switches do not have switch management software running in them. Therefore, there is no way to mirror ports on these non-managed devices. In this case, it is necessary to insert a simple, repeating hub between the switch and the device being analyzed and then attach EtherPeek to the hub.

In the picture below, you see the way that EtherPeek would be attached to a non-managed switch if the clients were complaining that they had problems accessing the Server. The cable from a client to the Switch is unplugged and a simple repeating hub (a $40.00 4-port hub, for example) is inserted between the client and the Switch. EtherPeek is now attached to the Hub. Essentially a "Y"-cable has been created. EtherPeek can now capture all traffic between the client and the Switch.

This same logic could be applied if EtherPeek were being used to capture all traffic to and from the Server. The hub would be inserted between the Switch and the Server.

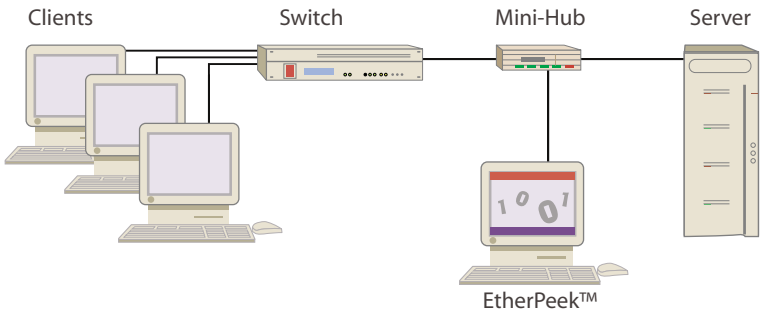


Figure 3. EtherPeek with a non-managed switch.

Remote Data Capture Utilities

Instead of using EtherPeek or any other full-featured protocol analyzer to capture packets from a network, there are a number of alternative ways to acquire a trace file. EtherPeek, for example, comes with a utility called "EtherHelp™" which performs remote, distributed packet capture for trouble-shooting and analysis. EtherHelp can be run from any machine in the network to capture a trace file that can then be analyzed by EtherPeek. EtherHelp allows filters and triggers to be set to restrict the traffic that is included in the captured file.

In the Unix/Linux arena, the TCPDUMP utility can create a trace file in much the same way that EtherHelp does. TCPDUMP files can be loaded into EtherPeek and analyzed.
In the realm of Simple Network Management Protocol (SNMP), there is a statistics-gathering software agent called an RMON Probe ("Remote Monitoring MIB"). This software may run inside a switch or router or it may run in a stand-alone probe device. RMON offers the ability to acquire a number of statistics concerning network utilization and also allows packets to be captured into a trace file. It is generally considered bad practice to use RMON probes for data capture because of the overhead and security concerns associated with such activities. EtherPeek cannot read an RMON packet capture file.

Files created by EtherPeek or EtherHelp are saved with the specialized information used by EtherPeek for decoding. They are given a."pkt" file extension. WildPackets has also developed a trace file conversion utility called "ProConvert" that will convert trace files from most other vendors' protocol analyzers into EtherPeek-readable format.

Attaching a remote data capture machine to a switched network is exactly like attaching EtherPeek. The requirements and constraints are identical. A switch port must be mirrored or a hub must be inserted to allow the remote capture machine to acquire directed frames.

Developing a Methodology for Switched Network Analysis

The guiding principle for analyzing a switched network is "You cannot see all of the traffic at the same time." This is a reflection of the fundamental distinction between the shared-media networks of the 1980's and today's switched infrastructures.

The methodology for analysis in a switched network environment focuses on two fundamental types of problems:

1. **You have a suspect:** A particular user, server, router, or other device is suspected of having, or causing, a problem

2. **You do not have a suspect:** There is a need to assess the overall characteristics, performance, and statistical measurements related to the network as a whole.

When a suspect station is being analyzed, the methodology is relatively simple. It is only necessary to mirror (or insert a hub) to capture all of the traffic to and from the suspect station. Analysis then proceeds in a normal manner.

When no suspect is identified, it becomes critical that the statistics and other management information provided directly by the switch be examined. Managed switches will report a broad spectrum of statistical information concerning network performance and protocol behavior. Since the switch itself can "see" 100% of the traffic passing through it, the statistics and other information provided by the switch become the key piece of an overall network assessment.

Of course, when measuring the baseline performance in a network it makes sense to expand on the basic switch statistics by capturing packets (by mirroring or with a hub) from each of the file servers and routers on the network. In general, all users will be communicating with the servers or through the routers. Hence, while there may be several hundred users, there will probably be a much smaller number of servers or routers. The job of individually measuring traffic characteristics and protocol behavior from each server and router may seem onerous, but that is the consequence of accepting the benefits of switched network engineering as opposed to coaxial Ethernet or simple hubs.

Summary and Conclusions

Through the use of port mirroring or the introduction of a mini-hub, a network engineer can effectively use EtherPeek to analyze traffic in a switched Ethernet environment. EtherPeek does not stand alone, however, in the networking professional's toolkit. Data collection utilities and the assessment of switch statistics augment the spectrum of analysis capabilities.

EtherPeek captures all of the traffic to and from a suspect station through the correct application of port mirroring or placement of a mini-hub. Switch statistics provide a basis for the assessment of a switched network as a whole.

This document has focused on the switched network aspects of applying EtherPeek to the protocol analysis task. WildPackets' product mix includes other types of associated utilities and tools that further expand and augment EtherPeek's capabilities. These include WebStats™ Analysis Module for collecting advanced TCP/IP, web-related statistics, and NetSense™ expert analysis tool that uses advanced algorithms to locate problems in trace files that may be buried or may be outside the experience of the analyst. NetSense provides "expert system" functionality to enhance EtherPeek's decoding and reporting features.

WildPackets provides a comprehensive solution to analyze and troubleshoot today's complex, sophisticated switched network infrastructures. When the features, capabilities, and price point of WildPackets' solutions are explored, it is reasonable to have every networking professional armed with the entire suite of EtherPeek analysis tools.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

On-Site Consulting

When protocol analysis support is needed at your site, the network experts at WildPackets will work with you and your support team to resolve network problems.

Performance Baseline and Network Capacity Planning Report

When it is necessary to know the real performance and capacity issues facing your network, a WildPackets consultant can create a baseline report, from a simple evaluation of a single critical server or router up to an assessment of your overall network infrastructure.

Infrastructure Design Analysis Services

The network experts at WildPackets can help you sort through the details of multi-vendor proposals for hardware and software installation and systems integration, providing you with an unbiased, third party perspective on your proposed network planning,

Remote Consulting Services

WildPackets' Remote Consulting Services may resolve challenging network problems for you without requiring an on-site visit. Our protocol analysis experts will accurately analyze specific trace files you send in to them or capture live traffic from your network and provide a general characterization of network performance and potential problems.

WildPackets Academy

WildPackets Academy offers the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers and support staff. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for both Ethernet networks and 802.11b wireless LANs. WildPackets Academy also provides instruction and testing for the industry-standard **NAX™ (Network Analysis Expert) Certification.**

For complete course descriptions and scheduling information, please visit www.wildpacketsacademy.com.

Live Online Quick Start Program

WildPackets now offers one-hour online QuickStart Programs on using EtherPeek and AiroPeek, led by a Professional Services Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

WildPackets, Inc.

Since its inception in 1990, WildPackets has been developing affordable tools designed to simplify the complex tasks associated with designing, maintaining, troubleshooting and optimizing computer networks. In the past eighteen months, WildPackets has acquired two key partner organizations and greatly expanded its product development expertise and professional services capabilities in the process. WildPackets customers include Ameritech, Cisco Systems, Lucent Technologies, Microsoft, National Institutes of Health, Yahoo! and others. Strategic partners include Cisco Systems, Symbol Technologies and Agere Systems.

WildPackets, Inc.
2540 Camino Diablo
Walnut Creek, CA 94596
Tel 925-937-7900
Fax 925-937-2479
www.wildpackets.com