Ethernet Switches

Faster Than a Speeding Hub

Laura Chappell

Editor's Note: Laura Chappell regularly speaks at NetWare Conferences and Exhibits, which are regional conferences hosted by NetWare Users International, North America. At each conference, Laura looks for solutions to common networking problems. Laura recently attended the Boston and Toronto conferences and found a solution to many users' network bandwidth problems—Ethernet switches.

The first time I saw a Kalpana switch in 1991, I had no idea how a switch worked or how it could improve network performance. I certainly had no idea that by 1996 the networking industry would be having a love affair with switch technology. This article briefly explains switch technology and describes some solutions for managing and troubleshooting networks that are connected by switches.

WHAT IS A SWITCH?

On a 10Base-T network, a hub connects devices, or stations, to form a network, as shown in Figure 1. When a station sends a request or reply to another station on the network, that communication, which is transmitted as an Ethernet packet, first travels through the hub. Like a multiport repeater, the hub then broadcasts the packet to each of its ports, regardless of the actual destination of the packet. For example, when Station A transmits a packet for the RESUME.DOC file to the SERV1 server, the packet passes through the hub, which then repeats the packet to all of the ports on the hub.

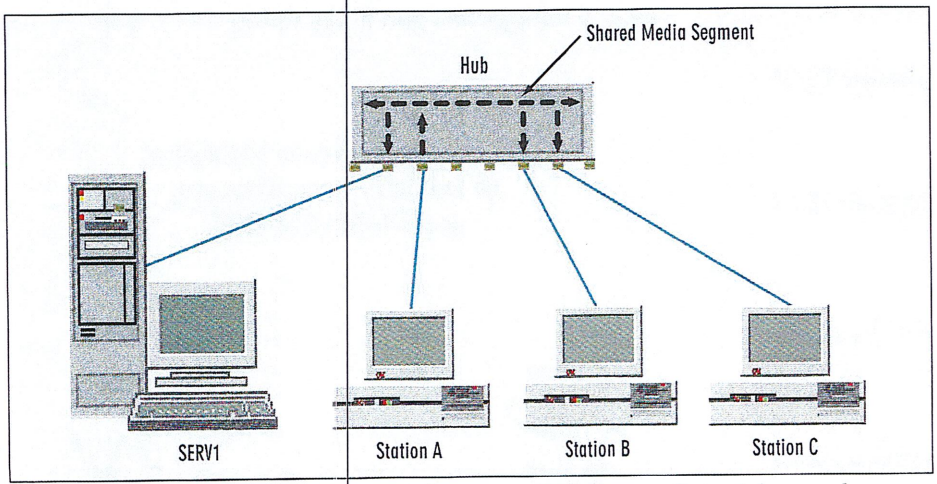

Illustration: Paul Johnson

Figure 1. *A hub repeats all requests to all ports on the hub, regardless of the actual destination of the request.*

Unfortunately, hubs have a shared media segment, which is essentially a single Ethernet bus on which all stations' communications must travel. (See Figure 1.) All stations connected to the hub must take turns sending packets on this "bus," sharing its 10 Mbit/s of bandwidth. For example, on a 48-port hub, a station competes with 47 other stations to send packets across 10 Mbit/s of bandwidth. If one station is sending packets across the segment, all other stations must wait until the segment is free.

Switches employ a different architecture to reduce bandwidth contention. Unlike a hub, a switch is an intelligent device that provides logical connections between stations. The switch maintains a table that lists all the stations connected to the switch by their hardware address and the port that corresponds to each station. When a packet passes through the switch, the switch reads the packet's destination address, refers to the table to determine the appropriate station's address and corresponding port, and then forwards the packet only to that port.

For example, when Station A transmits a packet addressed to SERV1, the switch reads the address on the packet, finds SERV1's address in the table, determines which port is connected to SERV1, and forwards the packet only to SERV1's port,

as shown in Figure 2. When Station A transmits a broadcast packet, the switch transmits the broadcast packet to all active ports.

Because a switch is intelligent and provides each station with almost dedicated bandwidth, networks connected by switches are fast and efficient. To increase speed even more, switch manufacturers are producing switches with both 10 Mbit/s ports and a 100 Mbit/s port. You connect your most active network device, such as a server or router, to the 100 Mbit/s port, and connect all other stations to the 10 Mbit/s ports.

Switches do have one disadvantage: They cost significantly more than hubs do. For example, 3Com Corporation's SuperStack LinkBuilder FMS II Stackable Hub with 12 10 Mbit/s ports has a suggested retail price of U.S. $499, and the 24-port version has a suggested retail price of U.S. $899. On the other hand, 3Com Corporation's SuperStack LinkSwitch 1000 Switch with 12 10 Mbit/s ports and one 100 Mbit/s port has a suggested retail price of U.S. $2,699, and the 24-port version has a suggested retail price of U.S. $3,699.

TYPES OF SWITCHES

Ethernet switches typically use one of two types of forwarding technologies: cut-through or store-and-forward.

Cut-Through Switches

If a switch uses cut-through technology, it begins forwarding a packet to the appropriate destination port after it receives the first six bytes of the packet. (The first six bytes contain the packet's destination address field.) The delay introduced by the switch, or the latency period, is minimal because the switch holds the packet for only a six-byte timeframe (approximately 4.8 microseconds) before forwarding it.

Although a cut-through switch does improve performance, it has one major drawback: It begins forwarding a packet before it can determine the packet's validity. In Ethernet, the cyclical redundancy check (CRC) field, which determines whether the packet is valid or corrupted, appears at the end of the packet.

If a station is transmitting corrupted packets, a cut-through switch forwards these corrupted packets. If a cut-through switch interprets a corrupted packet as a broadcast packet, the switch will forward the corrupted packet to all stations connected to the switch. Transmitting corrupted packets can cause serious congestion and time-outs on the network.

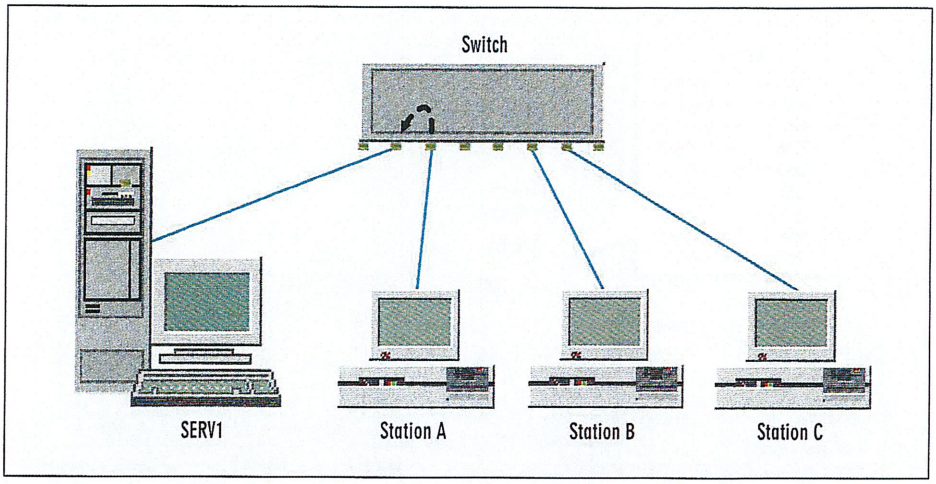

Figure 2. A switch forwards a request directly to the destination station, rather than broadcasting the request to all stations connected to the switch.

Store-and-Forward Switches

If a switch uses store-and-forward technology, it stores the entire packet before forwarding it. As a result, the switch can check the packet's CRC field to determine if the packet is valid or corrupted. Unlike a cut-through switch, a store-and-forward switch does not forward corrupted packets.

Unfortunately, because the store-and-forward switch must hold the entire packet in memory before forwarding it, latency time increases. The latency time depends on the size of the packet since the entire packet must be stored before the switch can forward it.

ANALYZING SWITCHED TRAFFIC

Although switches can improve performance and decrease traffic, they do affect how you troubleshoot Ethernet networks. For example, if a network has a 10Base-T hub, you can connect Novell's LANalyzer for Windows to the hub and take advantage of the way the hub forwards packets to every port. You can eavesdrop on all communications between stations and use these communications to troubleshoot performance problems.

If the network has a switch, however, a LANalyzer for Windows station can hear only broadcast traffic and its own communications. To monitor traffic on a network connected by a switch, you must purchase a switch management solution. To choose the best solution for your network, you should consider the size of your network and your budget.

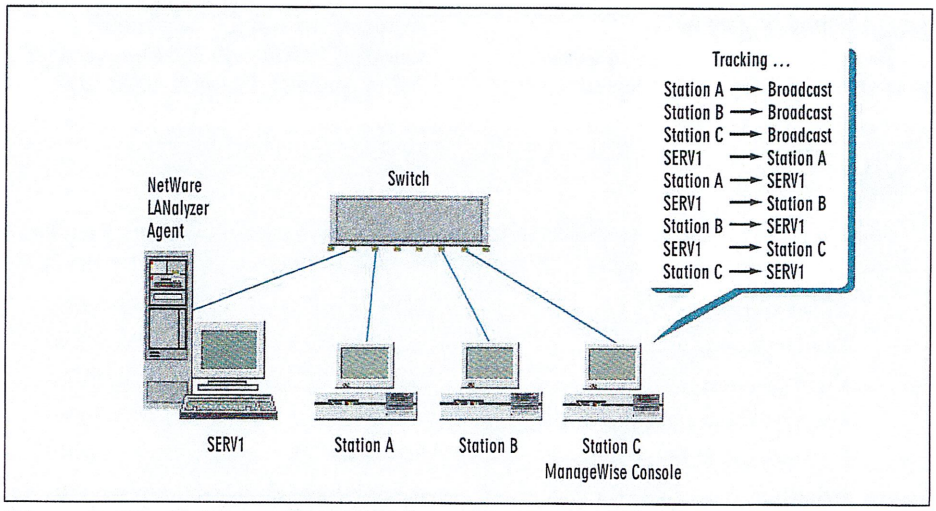

Figure 3. Novell's ManageWise LANalyzer Agent NLM tracks all communications to and from the server, regardless of whether the network includes a switch.

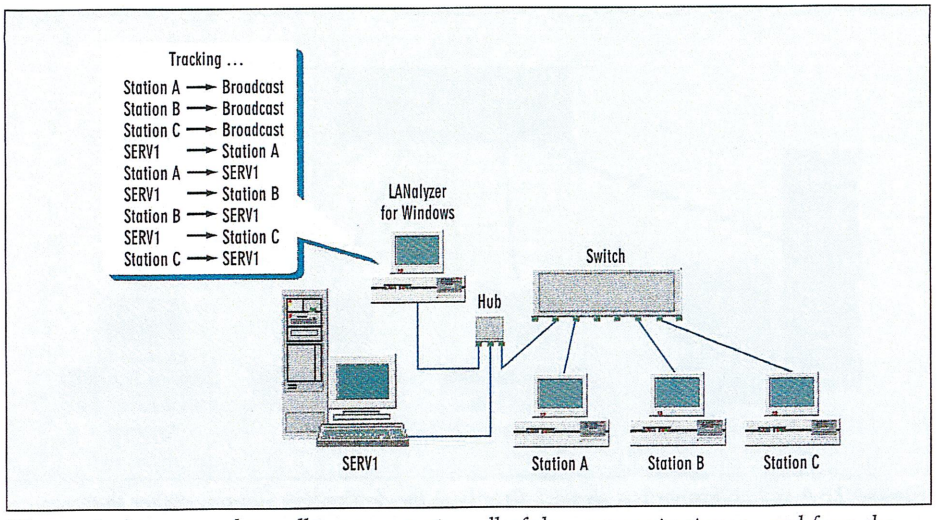

Figure 4. An external tap allows you to view all of the communications to and from the NetWare server.

Distributed Analysis Solution

A distributed analysis solution, such as Novell's ManageWise, allows you to manage all your network devices from a central console. Information about network traffic and performance travels from the ManageWise LANalyzer Agent NetWare loadable module (NLM) across the network to the central console on which you can view, manage, and configure your local and remote network devices.

Most NetWare communications are client-server communications: A station sends request packets to a server, and the file server transmits replies. By installing a ManageWise LANalyzer Agent NLM on a NetWare file server, you can track all communications to and from that server, regardless of whether a switch forwarded the packets. (See Figure 3 on p. 51.)

Monitor Port Solution

Some switches include a monitor port that may support a company's proprietary network analyzer or a third-party network analyzer, such as Network General's Sniffer.

A monitor port allows you to analyze network communications in one of three ways: port tapping, circuit tapping, or switch tapping. Port tapping enables the network analyzer to monitor all communications to and from a specific port. Circuit tapping enables the analyzer to look at a specific conversation between two switch ports. Switch tapping enables the analyzer to look at all of the communications flowing through the switch.

The following switches offer a monitor port solution:

- Bay Networks, Inc.'s Model 28000 Series switches and Model 3000 with 3328 host module switch
- Cisco Systems' Catalyst 5000 (with software version 2.1 or greater), Catalyst 1200 (with software version 3.0 or greater), Catalyst 1700, and EtherSwitch EPS-2115M
- SMC's EliteSwitch ES/1 and EliteSwitch ES/1 ATX
- 3Com Corporation's SuperStack LinkSwitch 2200 Switch and LANplex 2016, 2500, and 6000

Standalone Network Analyzer

On a network that has only two or three switches, you can add an external tap to the server's port. An external tap is a hub with at least three ports. You simply plug your server, a switch, and a network analyzer such as Novell's LANalyzer for Windows into these ports, and the network analyzer allows you to listen to all communications between the server and its clients. (See Figure 4.)

An external tap works with any switch and offers the same functionality as ManageWise and the LANalyzer Agent NLMs do. You can purchase a four- or five-port hub from SMC or Farallon Communications, Inc. for approximately U.S. $90.

CONCLUSION

If your hub is a bottleneck on your network or if you need high-bandwidth support, using a switch will improve network performance and allow you to use your existing cabling, network interface boards, and drivers. If you want to investigate switch technology, you may want to start with the products mentioned in this article. (For more information, see "Switch Companies.")

Laura Chappell researches, writes, and lectures on NetWare protocol performance, troubleshooting, and optimization. She is the coauthor of several books published by Novell Press. You can reach Laura at lchappell@imagitech.com.

Switch Companies

Several companies demonstrated switch products at the Boston and Toronto NetWare Conferences and Exhibits. For more information about these products, contact the following companies, or visit their booth at the next NetWare Conference and Exhibits.

3Com Corporation	1-800-NET-3COM	1-408-764-5000	http://www.3com.com
Bay Networks, Inc.	1-800-231-4213	1-408-988-2400	http://www.baynetworks.com
Cisco Systems	1-800-859-2726	1-408-526-4000	http://www.cisco.com
Farallon Communications, Inc.		1-510-814-5100	http://www.farallon.com
Network General	1-800-SNIFFER	1-415-473-2000	http://www.ngc.com
Novell	1-800-NETWARE	1-801-429-5588	http://www.novell.com
SMC	1-800-SMC-4YOU	1-516-435-6000	http://www.smc.com