

Switching IT: Troubleshooting 201

BY NEAL ALLEN

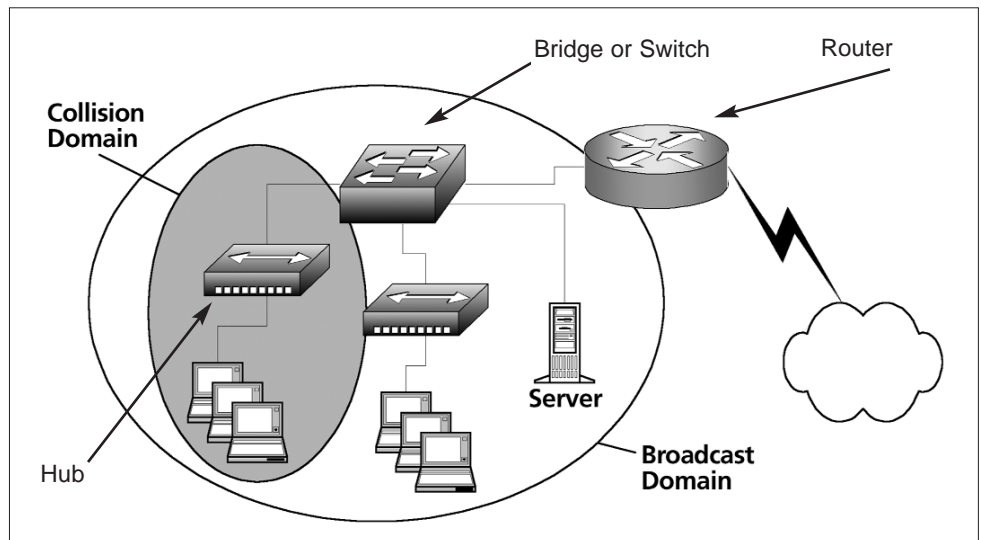
Ten years ago, the network was relatively simple. There were hubs, bridges, and routers. Each was a discrete box, readily identifiable from the others. Troubleshooting was also simple. If you were attached to a hub, then the rules for troubleshooting a collision domain applied.

At the point where the collision domain attached to a bridge, all errors stopped. Troubleshooting using a

protocol analyzer was the best available option, and was very effective once the user knew the basics of the network and the protocols in use.

Then switches appeared on the scene. A switch may act as an Open System Interconnection (OSI) Layer 2 bridge, or it may operate in one of several other modes that involve low-latency forwarding techniques. By implementing low latency forwarding techniques, the scope of the network that may be involved in an error is now equal to the broadcast domain. Regardless of forwarding technique, traffic is only forwarded to the “correct” port. Thus, using a protocol analyzer to monitor and troubleshoot becomes instantly ineffective in a switched environment. The protocol analyzer typically only sees broadcasts and traffic to unknown destinations when attached to any unused switch port.

A new generation of network analyzers can provide substantially faster solutions to networking problems. Active discovery tools using Simple Network Management Protocol (SNMP) for analysis, Remote Monitoring (RMON,) traffic analyzers, and a hybrid of



network and cable analyzers can be combined with traditional protocol analyzers to deliver unprecedented views into the network. Regardless of your tool of choice, there are 5 basic approaches that are generally applied to troubleshooting a switched environment:

- Access the switch console via remote login with an application such as Telnet or directly to the serial port. This is usually the same method used to configure the switch.
- Use SNMP to query the switch, usually from a network management platform.
- Install a Tap or Splitter, usually on an uplink. Then monitor the output from the Tap or Splitter with a protocol analyzer or other diagnostic tool.
- Configure a Mirror or Span port to get a copy of the traffic for analysis. The mirror can be configured to monitor the activity on one or more ports at the same time.
- Install a shared media hub between the problem device and the switch. Then monitor the collision domain with a protocol analyzer or other diagnostic tool.

Each of these approaches has positive and negative aspects, and none of them are perfect. You will probably have to employ several of them depending on the troubleshooting situation.

Neal Allen, a technology specialist for Fluke Networks, plays a critical role in beta testing, strategic partnerships, and event logistics. He has been involved in the design, installation, and troubleshooting of networks for more than 15 years.

SNMP

If security is enabled at the switch or anywhere along the way, it may not be possible to talk to the switch to obtain statistics.

Most useful information may be obtained from standard Management Information Bases (MIBs) instead of private MIBs, though not all switches support standard MIBs. Also, not all standard MIBs are well implemented by all switches. Private MIBs provide a view into new features and functionality that the standard MIBs don't know about, such as rate limiting.

The primary job of the switch is to forward traffic, not answer SNMP queries. Under high traffic loads and/or high traffic bursts, many switches will temporarily stop updating SNMP statistics, and may even stop recording them briefly.

SNMP queries add traffic to a network that you are already troubleshooting for some sort of performance problem, this is an especially important consideration if a Wireless Area Network (WAN) link is involved. They also require some level of Central Processing Unit performance from the switch, which impacts the switches ability to forward traffic.

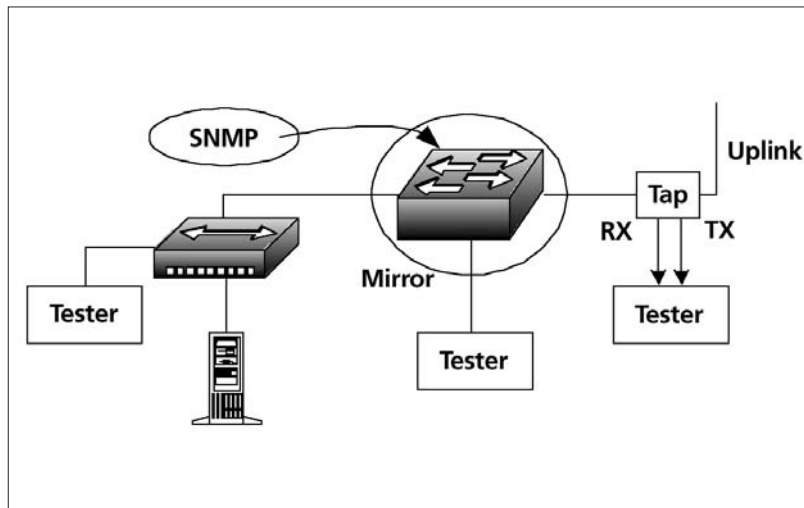
Tap or Splitter

Taps provide a view into both half and full duplex links, but monitoring a full duplex link requires an expensive 2-port analyzer unless you are willing to see only one side of a conversation at a time. Not all traffic on a switch passes through the uplink, which is often where the tap is installed.

Installation of a Tap requires that the link be disconnected for a short period of time, which further impacts performance on the network.

Shared Media Hub

As with the Tap, installing a hub only gives you a view of the traffic passing through a single port—not the whole switch.



Shared media means half duplex. Placing a hub on a full duplex link is likely to result in worse performance than the problem you were already troubleshooting.

Not all hubs are OSI Layer 1 repeaters. You may not see what you are expecting,

especially if the “hub” is really a small and inexpensive switch itself.

Installing the hub means adding 2 additional points of failure: the hub, and another cable.

Once a shared media hub is installed almost any monitoring tool may be used to troubleshoot the problem, including protocol analyzers.

Mirror or Span

Only traffic from the ports being mirrored will appear on the configured mirror port. You still need to have a pretty good idea where the problem is. Also, many switches do not permit traffic to be transmitted into the output mirror port, resulting in a listen-only situation.

Operating a mirror will usually reduce the performance of the switch by some amount.

Even if you guessed correctly on which port(s) to mirror, the forwarding technique employed by the switch may prevent you from seeing the error(s) that are causing the problem you are troubleshooting. Errors are not generally forwarded by switches—though some techniques permit certain errors to be forwarded.

If the combined activity on the mirrored port(s) exceeds the total output capacity of the mirror port, then traffic will be discarded without notification. You will unknowingly miss potentially critical traffic while you are troubleshooting.

Despite the various positive and negative aspects of the common switch troubleshooting techniques, you will have to use them. There simply are not a lot of alternatives. The good thing is that all of the issues that cause problems for troubleshooting also help to keep the rest of the network running even when one or more

users are experiencing problems. Beware: there are some recent developments in switching technology that should be considered during the troubleshooting process.

Rate Limiting

Some switches permit configuration of limits on how much bandwidth a particular user, protocol, or address is permitted. Other users, protocols, or applications may consume the entire capacity of the connection. Thus, web access between two adjacent ports of the same switch may crawl along at 5 MBPS despite being connected at 100 MBPS, while a File Transfer Protocol (FTP) download proceeds at near wire-speed across the same connection. The anticipated reaction is to assume that the web server is experiencing problems, when in fact it is the intentional configuration of the switch. Short of logging into the switch configuration management screens, this type of configuration is nearly impossible to detect.

Load Balancing

Some switches are designed to perform load balancing. The troubleshooting impact of this is that you know where the traffic entered the switch, but you may have difficulty predicting where it should come out. Unless you can check the switch configuration, this can be difficult to troubleshoot.

OSI Layer 3, 4, 5-7 Forwarding Functionality

Switches have become much faster and smarter. The front-end silicon is now able to perform many routing functions without passing the traffic up to software for routing decisions. The software is usually more multi-functional, but the hard-

ware is much faster. Troubleshooting in this environment is not the same as troubleshooting a collision domain or broadcast domain problem. Unless you can check the switch configuration, this can be difficult to troubleshoot.

VLANs

A simple Virtual Local Area Network (VLAN) configuration assigns a set of ports to be a broadcast domain. To pass traffic between 2 VLANs on the same switch usually requires a trip to a router, possibly located on another blade in the switch or an entirely separate device.

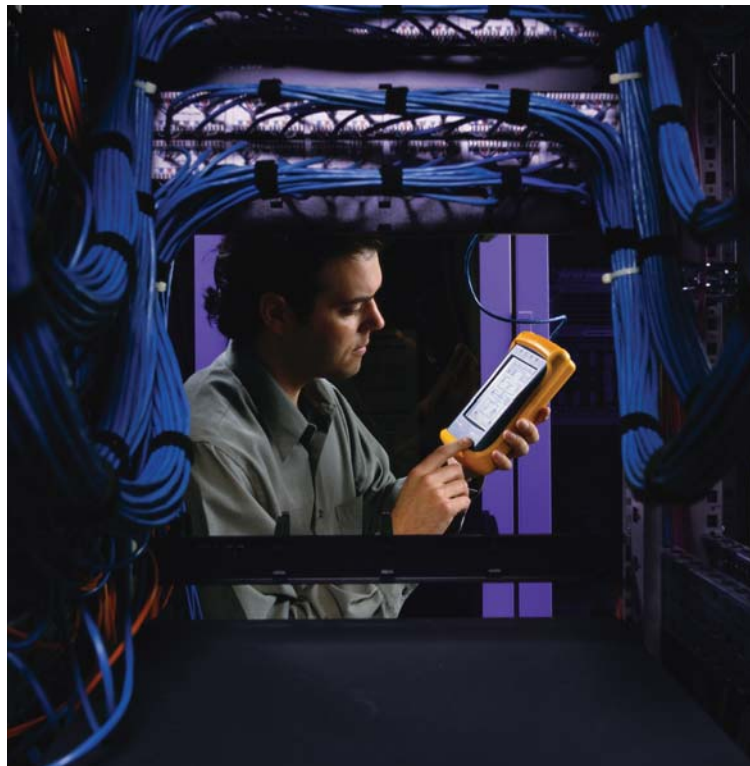
More complex configurations can assign the VLAN dynamically based on port, address, or other criteria. This may mean that the troubleshooting tool must assume the identity of the problem station in order to effectively troubleshoot the problem.

Virtual High-Speed Ports

Many switches permit combining several lower speed ports to form a single logical higher speed port. This is sometimes known as EtherChannel, though it is not limited to a single vendor, or a single Ethernet speed. Taps are available to monitor multiple physical links joined into a logical port, but it requires special software and hardware.

Redundancy

Switches inherently offer Spanning Tree as an OSI Layer 2 means of maintaining and managing parallel network paths. If anything goes wrong with the way parallel paths are handled, a broadcast storm often results and brings the broadcast domain to a halt. A variety of troubleshooting issues surround Spanning Tree prob-



lems, but the solution is simply to disconnect one of the parallel connections. Finding the problem parallel connection is the challenge. Furthermore, since switches also double as routers depending on the options loaded with the switch operating system or the installed hardware, the issue of standby ports becomes something to worry about. Various acronyms found include Virtual Router Redundancy Protocol (VRRP), Hot Standby Router Protocol (HSRP) and Extreme Standby Router Protocol (ESRP). All of them describe how two or more switches may be used in parallel, blocking traffic until such time as the active switch fails.

In some instances the parallel path is constantly active, but unused. Other configurations permit the unused path to be tested and then held “down” until needed, or both paths to be load balanced and used continuously. On occasion all paths are kept up and load balanced until a failure closes a path. To troubleshoot in this environment requires some knowledge of the configuration, or at least the presence of the parallel path. Independent actions by the dynamic Layer 2 protocols and the dynamic Layer 3 protocols can sometimes prevent the “active” port at the other layer from receiving traffic.

Asymmetrical Routed Paths

Similar to redundancy issues, parallel routed paths may create problems. Depending on the network configuration, it is possible to have asymmetrical paths in operation. Traffic can leave on one path and return on another. This situation may cause connection oriented protocols like Transmission Control Protocol (TCP) to receive packets out of order, which may result in retransmissions (apparent as a slow response to the user).

Unusual Frame Types

Many switches now offer vendor proprietary links to “improve” performance. These usages include all sorts of innovative solutions to distance, speed, or performance challenges.

Two examples include Jumbo Frames and Long Reach Ethernet (LRE), neither “standard” is supported

by the 802.3 Ethernet standard at this time. Many diagnostic tools cannot be directly connected to a port using a non 802.3 technology.

Shortening the Troubleshooting Cycle

There are a considerable number of challenges that network support staff must overcome when troubleshooting switched networks. Awareness of the potential problems is paramount to a successful troubleshooting episode, and the list of potential troubleshooting challenges continues to grow.

Each additional feature that is introduced into switching technology creates a new troubleshooting challenge.

None of the challenges are insurmountable, but continued education is critical. Once aware of the challenge it, becomes a relatively simple matter of selecting the right tool or tools for the problem at hand. Gone are the days of using a single tool to solve most problems, however, the suite of features available from the range of available tools is growing right alongside the increasing catalog of switch features. ■

“Awareness of the potential problems is paramount to a successful troubleshooting episode, and the list of potential troubleshooting challenges continues to grow.”

An Acronym Guide

- CPU**—Central Processing Unit
- ESRP**—Extreme Standby Router Protocol
- FTP**—File Transfer Protocol
- HSRP**—Hot Standby Router Protocol
- LRE**—Long Reach Ethernet
- MIB**—Management Information Bases
- OSI**—Open System Interconnection
- RMON**—Remote Monitoring
- SNMP**—Simple Network Management Protocol
- TCP**—Transmission Control Protocol
- VLAN**—Virtual Local Area Network
- VRRP**—Virtual Router Redundancy Protocol
- WAN**—Wireless Area Network