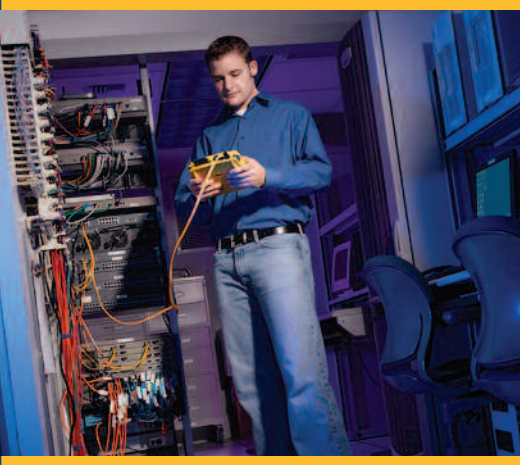
Eliminating sources and causes of unwanted network traffic

Your network may have the capacity and efficiency of an eight-lane expressway on a sunny Sunday morning. Just like this lightly-loaded highway, your network traffic moves quickly without bottlenecks; obstacles can be avoided, detours are few and far between and the occasional bursts of traffic are easily absorbed.

But what if some of the cars on your highway are in poor repair? As others speed down the road, the poorly running cars are starting to clog some of the lanes. The highway is in great shape but as more of these cars in bad repair take up more lanes, the entire highway experiences a slow down in speed.

Unwanted network traffic comes from several sources and often contributes to unnecessary processing by devices throughout the network affecting the "open highway" for your users.



For example:

- Excessive broadcast traffic affects end stations that need to determine if the traffic is relevant
- Unwanted protocols may indicate an obsolete or other incorrect device configuration
- Using factory-default switch port settings may be causing considerable amounts of unnecessary traffic and contributing to intermittent network sluggishness

Finding the sources of unwanted network traffic and taking steps to correct or eliminate the root causes can enhance network performance and help avoid future problems, but it can also be a time-consuming task without the proper tools and troubleshooting techniques.

Fluke Networks' EtherScope™ Network Assistant can be used to quickly identify unwanted network traffic and the device(s) that are contributing to the problem. EtherScope also provides statistics to help you understand the impact on your network and tests to determine if configuration changes are having the desired effect.

Excessive Broadcasts

Broadcast traffic is a necessary part of virtually every network but since each end station that receives a broadcast packet may need to do some processing, it is desirable to reduce the overall volume of broadcast traffic. Excessive broadcasts could also indicate a hardware or configuration problem or even a potentially malicious activity. In a typical network, the amount of broadcast traffic may be very small or could potentially overload the network. The first step is to measure the amount of broadcast traffic, then determine if it is excessive for your situation. EtherScope tracks traffic by type and MAC. You can quickly see which devices are generating the most broadcast traffic. EtherScope includes an automated device discovery

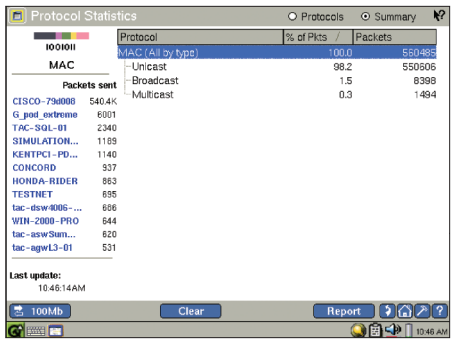


Figure 1: Traffic statistics by type and MAC.

capability and will associate received network traffic with the source device to create a "Top Talkers" view. By using this view and selecting "Broadcasts," you can instantly view the top sources of broadcast traffic.

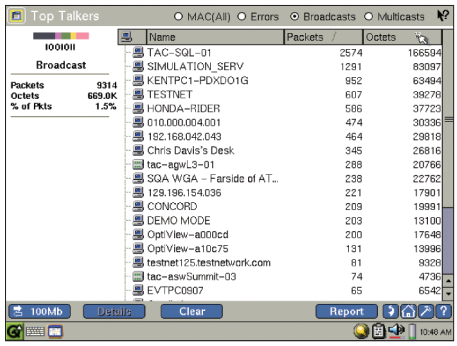


Figure 2: Top Talkers view.

EtherScope also discovers the Layer 2 topology of your network. During the discovery process, EtherScope determines the switch and switch port that connects end devices

Visibility to identify and eliminate unwanted traffic.

to the network allowing you to take appropriate action which may include temporarily disabling the switch port while the problem is being investigated.

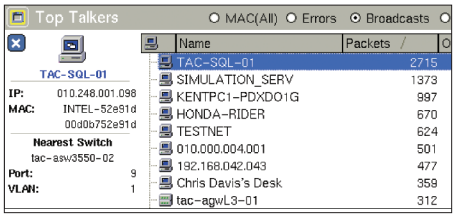


Figure 3: Top Talker nearest switch detail.

Unwanted Protocols

As networks and the services they provide evolve and servers or user machines are replaced and upgraded, the likelihood of passing unwanted, often obsolete protocols within the network increases. Each situation is unique, but knowing where to look and having a tool that shows not only which devices are using a particular protocol but where they are connected to the network is critical.

EtherScope monitors all network traffic and automatically provides protocol statistics for an extensive list of protocol types and TCP and UDP ports. Combining protocol statistics with device discovery provides a simple way to determine what protocols are running on your network and who is using them. Click on the offending protocol to locate the top source devices. Click on a device to locate the offender on your network.

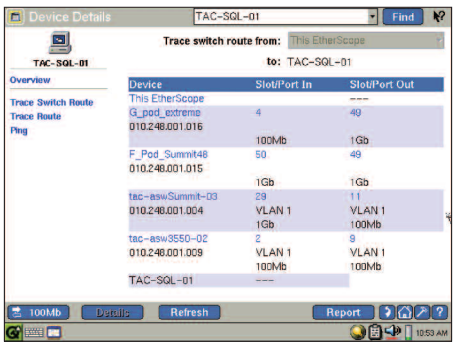


Figure 4: Trace switch route.

EtherScope only displays those protocols that are actually detected to simplify the display. If a packet cannot be resolved to a known port number, it is sorted into an "other" category, for example "Other TCP." This helps locate users who may be running undesirable applications or be infected with a virus.

The device discovery feature in EtherScope includes a mechanism that can greatly enhance the results when used within networks that utilize a management or administrative VLAN for segregating user data from infrastructure traffic. Normally devices in a different VLAN are not visible to the discovery processes. By allowing users to create a list of devices in the management VLAN, EtherScope can provide a complete Layer 2 connectivity picture through switches to end user devices making it easier to locate sources of unwanted protocols.

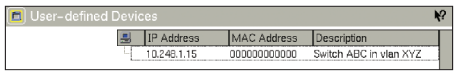


Figure 5: Device details.

Factory Default Switch Configurations

Unwanted network traffic and even temporary network problems can occur as a side effect of factory default settings in a normally healthy network. Consider Spanning-Tree Protocol (STP) used in almost every switched network. Most vendors enable spanning tree on each switch port by default. This is a reasonable choice as it makes it easy to quickly connect a new device and also protects the network from forwarding loops as the network grows. When the state of an interface changes, for example connectivity to another switch is lost, STP utilizes a special Bridge Protocol Data Unit (BPDU) called a Topology Change Notification (TCN). This mechanism works very efficiently in a stable network and the presence of TCNs is normally not an issue.

A problem that can cause unexpected consequences is when the spanning tree is enabled on ports that do change state frequently. Since a TCN is generated when a port that was in the forwarding state goes down or when a port transitions to the forwarding state, including each time an end user connects to the network, the TCN process starts and affects each bridge in the spanning tree. In the worst case of a large network with many users connecting and disconnecting, the network can be in topology change status almost constantly. The impact on the network is that the bridge forwarding aging time (nominally 5 minutes) is reduced to an effective 15 seconds which can lead to a very high level of flooding as switches re-learn each link.

If you want to change a factory default switch port setting, you can use EtherScope's Telnet or Terminal Emulator functionality to access the switch and set port configurations. Consult your switch documentation for the applicable switch configuration commands.

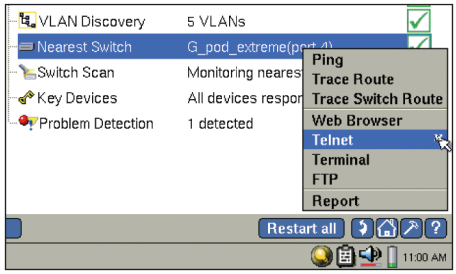


Figure 6: Access telnet or terminal emulator functionality to change switch configurations.

Conclusion

Unwanted network traffic is not only a nuisance to users, it can also cause confusion when troubleshooting hard-to-find network problems. Understanding the possible causes and sources for unwanted traffic can be an important part of keeping a network clean and running efficiently. Combining the knowledge of where and what to look for with automated tools such as Fluke Networks' EtherScope Network Assistant allows you to become a powerful problem solver.

Printed in U.S.A. 2/2005 2435321 A-ENG-N Rev A