Title:
How To Build A Simple Open-Source Distributed Protocol Analyzer

Word Count:
519

Summary:
This is the way that Network General (the creator of Sniffer ®) has deployed Distributed Sniffer ® since the beginning. While the product that you are using may be from another or Open-Source vendor,(i.e. Ethereal ®/ WireShark ®), this process is time honored and as such, is considered to be “Best Practice.”

This design is meant to assure that the NIC that is listening to the Monitor is not sending any packets itself. The Monitor Card should have no protocols bound to its...

Keywords:
Sniffer, Wireshark, Protocol, Analysis, Performance, Test, Troubleshoot, Flow, Application, TCP/IP

Article Body:
This is the way that Network General (the creator of Sniffer ®) has deployed Distributed Sniffer ® since the beginning. While the product that you are using may be from another or Open-Source vendor,(i.e. Ethereal ®/ WireShark ®), this process is time honored and as such, is considered to be “Best Practice.”

This design is meant to assure that the NIC that is listening to the Monitor is not sending any packets itself. The Monitor Card should have no protocols bound to itself and listens in promiscuous mode. Additionally, the PC should be as passive as possible and not phoning home to vendors because of unnecessary software it has loaded.

One process is to take a company’s standard laptop and customize it by removing anything that is not needed to support the role of a Protocol Analyzer. Any software that is not part of the laptops OS requirements should be un-installed. Once the laptop has been stripped down this way, load the Open Source Protocol Analyzer of your choice and test it.

Once testing is satisfactorily completed, save an Image of the laptop to be used to generate other Open Source Laptop Protocol Analyzers.

System Requirements:

Pentium 4 or higher.

1GB Memory or higher.

2 NICs. One of which is 100Mbs (not Gigabit) to be used as the Monitor Card. (NOTE: This process is not appropriate for Gigabit Monitoring.)

Remote Control Software (i.e. VNC) that supports File Transfers from the laptop acting as a Protocol Analyzer to the PC used by the Network Transaction Analyst.

Two NICs:

1st NIC – Monitor Card – No IP bound to the card. This card just listens in promiscuous mode. It is the one that is attached to the Monitor Port in the Switch. This should be a 100 Mbs NIC.

2nd NIC – Transport Card – IP is bound (static) so that this card can be used on the Intranet to access the remote control function of the PC. This can be Gigabit if that is all that is available.

Other Configuration Issues:

No Management Software (SMS, Radia, etc.) enabled. No management of this device other than remote control.

Virus Protection (only if it is considered mandatory by company policy). However, this laptop should have no email client or any other software that will want to connect to the Internet (with the possible exception of Time Services). A Firewall rule can always be created to enforce its isolation from the public Internet except on approved sockets.

A Time Server should be in place to keep the various Protocol Analysis Laptops in sync. This can be an Internet source if Company Policy permits or a local Intranet source.

The laptop should not be a member of the Company Domain. One logs into the PC itself, locally or via remote control.
All Mirrors in switches are to be bi-directional.

Consider creating a shared folder to act as a Trace File depository. This is not required, but can be helpful as these files can easily grow too large for many corporate email policy size limits.

Use WinZip on the Laptop to allow compression of the large trace files to speed up transfer.