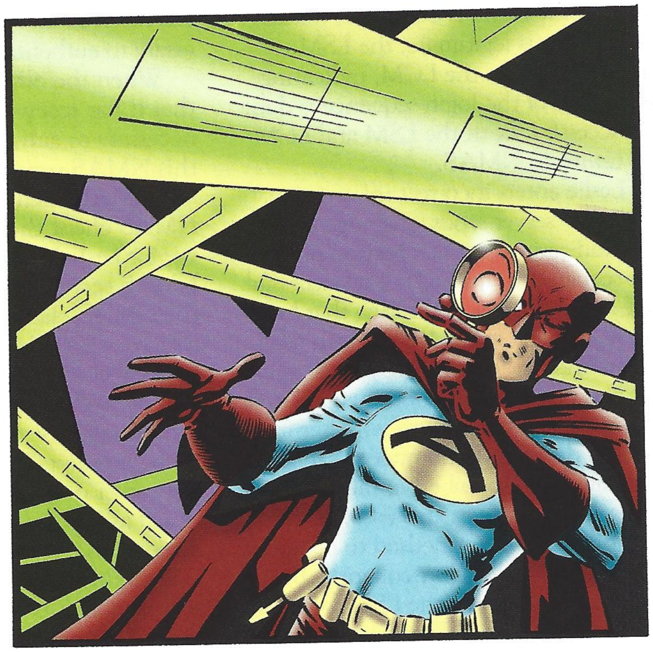
Laura Chappell

10 Tips for Creating a Network Analysis Report



If you have done onsite network analysis, you know that organizing the information gathered during an analysis session can be an overwhelming task. Since you may have thousands of packets and trend graphs to evaluate, you need to be selective in the information you present to your company or client, and you must create a visually appealing report. This article outlines 10 tips for creating a network analysis report. This article assumes you have some familiarity with network analysis and packet-level communications. In addition, you can read a sample network analysis report at http://www.netanalysis.org/references/0115rpt.zip. (For more information about network analysis, see *Introduction to Network Analysis*, which is available at http://www.podbooks.com.)

1. CREATE A TABLE OF CONTENTS WITH "MEAT"

I start creating my network analysis report by making a series of statements that are based on the company's concerns and the analysis results. It is important to use definite statements since these statements will be incorporated into a table of contents and will become the foundation for the network analysis report.

For example, suppose you are creating a network analysis report for a company called ABC Corp. and this company has the following questions regarding its network:

- How healthy are the numerous Token Rings?
- How effective is a heavily switched and bridged network design?
- Is IPX Routing Information Protocol (RIP) meeting the network needs or should NetWare Link Services Protocol (NLSP) be implemented?
- Why are the NetWare Core Protocol (NCP) connections sometimes denied?
- Is there any traffic that can be filtered from the network to improve bandwidth use?
- Are there any communications problems?

Keeping in mind the concerns ABC Corp. has, you can then use the information you discovered to create headings, which become an outline for your network analysis report. For example, you may create the following headings for ABC Corp.:

- No Sign of Overloaded Ring
- Good Ring Poll Process
- Low Token Error Count
- Card Failure Imminent
- Broadcasts Should Be Watched
- Strange Broadcast Blocking to Be Verified
- Routing: RIP Is Fine
- Dual Attached Server Questioned
- Packet Size Distribution Is Small
- Check SPX Timers
- General Connections Not Brought Down
- Unanswered Persistent Address Resolution Protocols (ARPs) Seen on the Network
- ARPing From 0.0.0.0
- Internet Control Message Protocol (ICMP) Redirects Indicate Problem

I have found that building the report from these series of statements makes the process go smoothly. After you have created these headings, you can use the following subheadings to break them down further:

- What is this technology all about?
- What did you find on the network?
- What should be done, or where can the company go for more information?

For example, perhaps a network analysis session revealed a high latency time between a client request and the server reply. It would be appropriate to include the following information:

Slow Response Time

Latency is time delay from one point to another point on a network. During my analysis of the network, I found that there is a high roundtrip latency time between a specific client and

Illustration: Norman Felchle

> the server. (See the sample report at http://www.netanalysis.org/references/0115rpt.zip.) The roundtrip time between a client request and a server reply takes much longer than other similar communications processes. During the network analysis, I found that the roundtrip latency time between station 1 and server FS2 is almost twice the delay of other similar communications. I have examined the communications further to find that station 1's data is taking a less direct route to FS2's network. Further examination of the client's bootup process and routing tables on the network should identify the cause of this routing inconsistency and increased latency delay.

It may also be nice to include a screen shot of the summary area (with timestamping) of relevant packets with this comment.

2. CREATE A VISUAL REPORT

The old saying "a picture is worth a thousand words" is especially true when you are creating a network analysis report. Network analysis is a visual art form. For example, the screen shot in Figure 1 depicts the most active six hosts (based on total bytes in or out). (See p. 26.) The addresses shown are their Media Access Control (MAC) addresses unless a name is known (in the case of Michael).

This graphic indicates that Michael's traffic accounts for one-half of all network communications. If other network factors (such as bandwidth utilization) indicate the network is reaching an overloaded status, you should examine the "top talkers" to determine if their activity is a one-time only process (such as backing up to the server) or a regular process (such as graphics-intensive downloads/uploads).

How do you create nice graphics for your network analysis report? A quality screen capture utility can do a much better job than the Export tools that are available in most network analyzers. I use SnagIt by TechSmith Corp., but other screen capture utilities are available. You should make sure that you choose a screen capture utility that can scroll down an open window and capture the entire contents. This capability is particularly important when you need to show complete packets that cannot fit onto one screen.

If you are building a network analysis report in Microsoft Word, you can double-click on the graphic to add labels that further link the art to your documented findings. (For examples of incorporating graphics into the text of a network analysis report, visit http://www.netanalysis.org/references/0115rpt.zip.)

3. INCLUDE A BASIC NETWORK MAP

Typically, I request a network map from the company before I go onsite. The map should include details such as network addresses, basic interconnecting devices, firewall locations, and building names.

If possible, you should edit the network map to indicate where you tapped into the network with your network analyzer. You should document any special analysis procedures that were required by the network layout. For example, if the network is highly switched, you should indicate

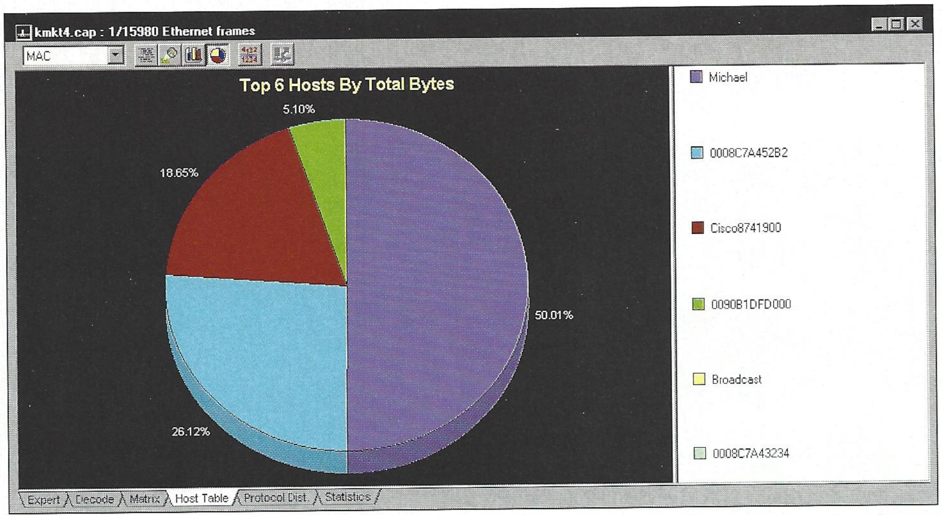


Figure 1. When Network Associates' Sniffer reported the top six hosts on this network, two hosts were inactive and, consequently, did not appear on the pie chart Sniffer created. You should explain such issues in your network analysis report.

whether or not you used port spanning or mirroring to analyze a switched segment.

If the company needs to create a network map, you may want to recommend using Visio Professional, which is the ultimate tool for creating network maps. (For more information about Visio Professional, visit http://www.visio.com.)

4. PROVIDE A NEXT STEP WHEN APPROPRIATE

Not all solutions are immediately evident when you examine network analysis results. If you do not have an immediate solution, you should recommend future steps the company should take to find a solution. For example, you may recommend the following:

- Follow-up analysis tests are required.
- The company should further analyze a particular area of communication.
- The company should ask its hardware or software vendors a list of questions you have compiled.
- If a particular problem is outside your field of expertise, you can recommend experts who have more experience in that area.

For example, I do not perform much Asynchronous Transfer Mode (ATM) analysis. If a network appears to have some ATM-related issues, I refer the company to an ATM expert whom I respect.

You may also want to acknowledge any company employees who participated in the onsite network analysis session. For example, the director of IS may have dedicated his or her time to following you around for the onsite network analysis. This acknowledgment not only gives credit to these employees but also indicates who might have additional information on the network analysis tasks and the process of obtaining results.

5. ASSUME THE READER HAS LITTLE KNOWLEDGE OF NETWORK ANALYSIS

You should find out who will be reading the network analysis report you create and then tailor the report accordingly. In general, however, you should assume that the reader is not familiar with protocol analysis or packet-level communications. You should explain terms specific to protocol analysis such as latency or persistent ARPs. However, these definitions should be fairly high level, rather than technical. That is, anyone reading the report should be able to understand the definition.

Although you should assume the reader is not an analyst, you must also be careful not to offend the reader by providing information that is too basic. For example, don't define networking or explain the history of the Internet.

In some cases, you may want to provide references to third-party materials for more information. For example, if you are commenting on a vendor's nonstandard method of handling ARP queries, you may refer the reader to Request for Comments (RFC) 826, which explains ARP communications over Ethernet media. (You can download this RFC from http://www.ietf.org/rfc/rfc0826.txt.)

6. ASSUME THE READER HAS NO TIME

The toughest part of building a report is assuming that the reader has no time to review a detailed report. At the beginning of the report, you should create a one-page summary that highlights the key points contained in the report. As I write network analysis reports, I often imagine the Chief Technology Officer (CTO) checking out the report for a cursory overview of the information the company paid for. Obviously, CTOs are extremely busy, so I make sure the summary is concise and easy to read.

Remember to address any concerns the company may have. As mentioned earlier, I specifically ask the company about their concerns before going onsite. I then address these concerns within the report as the first set of issues.

7. INCLUDE SPECIFIC PACKET REFERENCES

Keep track of the trace files you reference in the network analysis report, and refer to trace files with specific names and packet numbers. For example, you could refer to trace files and packet numbers as follows:

"As you can see in Figure 1 [packet 1 of trace ICMP.TR1], the router is redirecting the user's client back to itself. This behavior clearly indicates a problem on the network since redirections should be pointing devices to another routing device."

In most cases, you will want to include a CD or a diskette with your report to provide the company with the original trace files. The company may want to review these files at a later time.

8. BUILD THE REPORT FROM THE BOTTOM UP

As a network administrator, you have been trained by the Open Systems Interconnection (OSI) model to view communications from the physical/data link layer up. Organizing your network analysis report in this way is good because more readers will be able to understand the lower-layer findings. The upper-layer findings typically require a more advanced reader and may bog down the report in mucky details.

For example, in the sample report online at http://www.netanalysis.org/reference/0115rpt.zip, you will note that the report starts with the health of the Token Ring and Ethernet segments examined. The report then moves through the multiprotocol broadcast/multicast issues and the protocol stacks (IPX/SPX and TCP/IP). Finally, the report addresses the application and upper-layer protocol issues and any miscellaneous concerns.

9. SUBMIT SOFT-COPY REPORT

I submit my soft-copy report in Word format and allow the company to edit the report. After all, the company has paid for the report and is the rightful owner of all information contained therein. I also send several bound hard-copy reports via overnight express to ensure that upper management receives quality color copies.

Typically, you should keep the report under 30 pages. At the 20-page mark, the readers' eyes begin to water, and readers start dozing off.

10. CONSIDER YOUR REPORT HIGHLY CONFIDENTIAL

The information you place in your network analysis report typically documents a network's design, its strong points, and its weak points. Consider the report confidential and encrypt it if you are sending it across the Internet.

Trace files should also be considered confidential since the data portion of the packets often contains readable data from the network. Understandably, many companies also want their network addressing scheme to be kept confidential.

In some situations, I may create a "For Your Eyes Only" addendum to the report. This addendum addresses network security concerns. I typically hand this report only to the key contact at the company. He or she can distribute this highly classified information as needed.

THE SAMPLE REPORT

The sample report at http://www.netanalysis.org/references/0115rpt.zip was derived from an actual network analysis report on a mixed Ethernet/Token Ring network that supports IPX/SPX and TCP/IP. I have edited the addresses, contact names, and any identifying characters/information to protect the confidentiality of the company.

This sample report was submitted following an onsite network analysis training session, so the report lacks some of the introductory technology information under each heading. For example, the "Good Ring Poll Process" section should include a short blurb on the purpose and typical timing of the ring poll process. Since this information was explained in the onsite network analysis training, it was not repeated in the report.

A network analysis report contains all of the information gained from the thousands of packets and mounds of data you have accumulated. The report should be useful enough and informational enough to be used as a handout for a presentation if you desire to use it as such.

Of course, you can create network analysis reports in numerous different formats. I am always interested in viewing network analysis reports. If you have a format or formula that works well for you and want to share it, please send it to me at lchappell@netanalysis.org.

Laura Chappell is the author of TCP/IP Analysis and Troubleshooting, *a new pod book now available from http://www.podbooks.com.*