Nalini Elkins'
TCP/IP Trace Reading and Introduction to Troubleshooting on z/OS

Do you have the responsibility for TCP/IP problem resolution? When you get a trace, are you clear on what it can tell you or are you mystified? Do you want to brush up on how exactly the core Internet protocols (TCP, IP, UDP and ICMP) work? Can you tell if you have implemented your TCP profile parameters properly from traces? Are you implementing Enterprise Extender? Do you know how to decode the EE headers (ABR, ANR Labels, HPR, LLC)?□□

We will spend much of the time in this class in labs reading trace after trace showing various aspects of the core Internet protocols both in normal situations and in abnormal. The more experience you have with traces, the more you will become comfortable and adept at resolving many problems in the TCP/IP network. We will use case studies from real situations to see how such problems manifest themselves and have been resolved.

We will also discuss how hacks work in the TCP/IP environment. How do security violations such as TCP SYN Flood, SMURF, or UDP packet storm really work? Which part of the protocol is exploited? Are you at risk? In this class, you will learn about such security violations and how to prevent them.

Nalini Elkins, an experienced TCP/IP network performance expert, with many years in network management and working with IBM, will teach you practical TCP/IP diagnostic skills. You will learn how to identify protocol and performance problems, whether originating from TCP/IP system setup, application problems or hardware failures. You will receive detailed explanations on how to interpret packet traces and how to resolve problem situations.

Consider this class as being dedicated to deeply and fundamentally understanding the TCP, UDP, IP, and ICMP protocols via trace analysis.

Audience

This 3-1/2 day seminar is designed for systems programmers who are responsible for troubleshooting, performance measurement, security, analysis, or tuning of their installation's TCP/IP network, socket applications and TCP/IP stack. You will leave class knowing how to read a packet trace for the core IP protocols (TCP, UDP, IP, and ICMP). Most importantly, you will have an understanding of the protocols and how they interrelate to transport data. Then, when you look at a trace - you will understand what you are seeing. You can then find and eliminate potential trouble spots or problems in your TCP/IP stack, network or socket applications.

TCP/IP

Connecting the World

This class is for you…

- o If you want to troubleshoot your TCP/IP stack, socket applications or network
- o If you want to know how your TCP stack can be attacked
- o If you are an experienced diagnostician, but want to see what problems other installations have had
- o If you are a novice network analyst, or new to the field of TCP/IP networking and need to learn how the core Internet Protocols work to effectively diagnose problems in your TCP/IP stack and socket applications
- o If you are implementing Enterprise Extender and want to know how to diagnose problems

Class Overview

This intensive seminar is designed to provide the attendee with an understanding of how to use packet traces to diagnose problems with the TCP/IP network, socket applications, and TCP/IP stack. It is designed to guide you in learning the basic concepts of TCP/IP network diagnosis by teaching you a step-by-step approach to trace reading. You will learn how to analyze traces for TCP, UDP, IP and ICMP protocols, for FTP, TN3270, CICS, WebSphere, HTTP Server, and other socket applications. You will learn to analyze various TCP/IP profile and setup parameters for z/OS and also Windows and Linux. You will learn where the security vulnerabilities are of the core Internet protocols and how to protect your installation.

The strength of this seminar not only comes from the information learned, but from the analysis you can perform on your own data during the seminar week.

Class Participation

During this class you will analyze your own data and installation setup.

Each student is strongly encouraged to bring packet trace data and TCP profile examples from their installation. Shortly after you enroll in the seminar you will be provided data collection instructions for the data you will be examining in class. Analysis and class exercises will make use of this data.

During the class week Nalini Elkins will be available to help review the data, to answer questions, and provide expert feedback. You can think of this as a week that you've scheduled specifically to understand how the core Internet Protocols are implemented in your TCP/IP network.

Seminar Highlights

Detailed explanations on how to interpret packet traces and how to fix many commonly seen problems are provided.

1. Optionally, your individual system trace reports can be evaluated which includes a written recommendation report. This service is the equivalent of an expert reviewing your installation data and providing a detailed explanation.

30 Los Helechos
Carmel Valley, CA 93924
(831) 659-8360
sales@inside-products.com
www.inside-products.com

Development Center
30 Los Helechos
Carmel Valley, CA 93924

2. You will learn to identify performance problems, whether originating from the TCP/IP network system setup parameters, from socket applications, or network hardware.
3. You will learn if you have security holes in your TCP/IP stack as we have found in many systems

Prerequisite

A basic understanding of z/OS, TCP/IP, and networks is assumed.

Seminar Dates and Location and Prices

For dates and locations and prices, please contact sales@inside-products.com or call our office at 831-659-8360. Seminars are regularly offered in the USA, Europe, and Australia.

For More Information…

For more information on this or other seminars, including prices and locations, please contact:

Inside Products, Inc.
30 Los Helechos
Carmel Valley CA 93924

Phone: 831-659-8360
Fax: 831-659-8360

Email: nalini_elkins@inside-products.com or
Email: sales@inside-products.com
Web: www.inside-products.com

Please do not hesitate to call if you would like more information or details on this seminar.

In-house

All seminars are available for in-house instruction.

Instructor

Nalini Elkins, of Inside Products, Inc., (www.inside-products.com), is a recognized leader in the field of computer performance measurement and analysis. In addition to being an experienced software product designer, developer, and planner, she is a formidable businesswoman. She has been the founder and co-founder of two start-ups in the high-tech arena.

During her career Nalini served in groups responsible for network performance design, analysis, troubleshooting, and systems programming. The classes Nalini produces and instructs, and the

products she develops are designed with the needs of systems programmers as a key requirement. Nalini has an excellent understanding for the needs of system programmers because she was in their shoes for many years.

Nalini has also developed an expert system for diagnosing network hardware problems. The marketing rights for this product were sold to Boole & Babbage (which was later taken over by BMC). Nalini then joined Boole to further develop and support this product. After some time at Boole, Nalini joined some other Boole employees in co-founding a new company - Applied Expert Systems.

As Technical Co-founder, Nalini helped to design and develop a number of products in the SNA and TCP/IP network management area. These products included expert systems for SNA diagnostics, web performance diagnostics, TCP/IP routing diagnosis and TCP/IP network management. She was the Chief Developer of the product IBM first marketed as NetView Performance Monitor for TCP/IP.

Nalini now has her own company, Inside Products, Inc. (www.inside-products.com), which designs, develops and markets network management and Linux management software. The products are Inside the Stack TCP/IP monitor, TCP Problem Finder and TCP Response Time Monitor. Inside Products also provides consulting to resolve network problems such as FTP throughput, socket application performance and TCP/IP tuning. Inside Products has international distributors in Australia, Germany, Switzerland, the United Kingdom, Belgium, Netherlands, Luxemburg and Brazil.

Nalini has published numerous articles in publications such as zJournal, Technical Support, Xephon's TCP/IP Update, and Enterprise Systems Journal. Nalini is also a regular speaker at SHARE, both national and regional Computer Measurement Groups (CMGs), and variety of international conferences.

Nalini can be contacted directly at Nalini_Elkins@Inside-Products.com

Seminar Outline

The following is a high level outline for this seminar. Since the seminar is constantly being updated, actual seminar content and flow may vary slightly from this outline.

TCP/IP Network Performance Introduction

1. TCP/IP network fundamentals
2. Core Internet protocols (TCP, IP, UDP, ICMP)
3. Common RFC's
4. Mainframe TCP architecture (USS, socket applications, TCP/IP Profile, BPX parms)
5. Socket applications, well-known ports (Telnet, FTP, SMTP, Web server)
6. What can we learn with traces?

Connecting the World

How to Take a Packet or Socket Trace

1. What kinds of traces are there?
2. How to start the external writer task.
3. How to format and print a trace
4. How to use the Network Management API to provide traces
5. How to use the SNMP Packet trace MIB

How to Analyze Enterprise Extender

1. How do the multiple headers work? (SNA, HPR, UDP, and IP)
2. How do headers indicate performance?
3. How do Adaptive Rate-Based (ARB) headers and flow control work?
4. ARB slowdown
5. EE keep alive

How to Analyze a Trace for TCP Protocol Problems

1. How does the TCP open sequence work?
2. Lab: Read traces with the TCP open sequence for TN3270, CICS, WebSphere, FTP, etc.
3. Negotiating and setting MTU, window and other parameters in the open sequence
4. Data transmHow do Adaptive Rate-Based (ARB) headers and flow control work?ission implementation i
5. How does TCP congestion window work?
6. How do TCP duplicate acks, retransmissions, and retransmit timers work?
7. Lab: Read traces for normal data transmission for TN3270, CICS, FTP, WebSphere, etc.
8. Lab: Read traces with problems with congestion window, duplicate acknowledgments, and retransmits
9. How does the TCP close sequence work?
10. Lab: Read traces with the TCP close sequence (from server and client)
11. Why is TCP reset used?
12. Lab: Read traces with TCP resets.
13. Case studies

TCP/IP Profile parameters

1. What are they?
2. How do they impact performance?
3. What can go wrong?
4. Case studies to illustrate settings
5. Setting TCP parameters in other platforms such as Windows or Linux

TCP Hacks and Security Violations

1. What they are: TCP SYN Flood, SMURF, UDP Packet Storm, etc
2. What part of the protocol is exploited
3. How to prevent and detect security violations

How to Analyze a Trace for UDP Protocol Problems

1. How does the UDP protocol work?
2. Lab: Read traces with the UDP connections for SNMP, DNS, etc.

30 Los Helechos
Carmel Valley, CA 93924
(831) 659-8360
sales@inside-products.com
www.inside-products.com

INSIDE PRODUCTS
Thinking Inside the Box
Development Center
30 Los Helechos
Carmel Valley, CA 93924

3. UDP flow
4. Unnecessary UDP traffic from Windows, Linux
5. Lab: Read traces with the NetBios UDP connections from SQL Server
6. UDP profile parameters - what are they?
7. How do they impact performance?
8. What can go wrong?

How to Analyze a Trace with ICMP Protocol

1. How does the ICMP protocol work?
2. Lab: Read traces with ICMP protocol messages for problems caused by UDP.
3. Lab: Read traces with ICMP protocol messages for problems caused by TCP.

How to Analyze a Trace for IP Protocol Problems

1. How does the IP protocol work?
2. Lab: Read traces with UDP over IP protocol
3. Lab: Read traces with TCP over IP protocol
4. How does PATHMTUDISCOVERY work?
5. IP profile parameters - what are they?
6. How do they impact performance?
7. What can go wrong?

Analyzing Socket Application Problems

1. TCP sockets,
2. FTP,
3. Web server applications,
4. TN3270,
5. Response time,
6. LDAP server,
7. Parameters to manage sessions (timemark, etc.)

Analyzing Response Time for TCP and UDP

1. What are round trip time, round trip variance, end-to-end times, network times, and host times?
2. How can we define a 'transaction' from a trace?
3. How can we match packets to get end-to-end, host, and network response time?
4. Lab: Use traces to match response times for TN3270, CICS, FTP, etc.
5. Statistical analysis of response time - what is best for what problems?
6. How do we think about UDP response time?
7. What is a UDP 'transaction'?
8. Lab: Use traces to match response times for TN3270, CICS, FTP, etc.
9. Statistical analysis of response time - what is best for what problems?