“Troubleshooting the Broadcast IP Network”

Wayne M. Pecena, CPBE, CBNE
Texas A&M University
Educational Broadcast Services – KAMU FM-TV

Advertised Tutorial Scope:

This tutorial will provide a structured approach to IP network troubleshooting by using a layered approach modeled after the industry standard “OSI Networking” model. The layer design of the OSI model provides the perfect framework in which to build a structured troubleshooting approach focused upon the Data Flow layer functionality to quickly isolate the root cause issue.

Beginning at the physical level, practical techniques will be presented for fault isolation focused on the network medium or cabling. Progressing through the Data Link, Network, and Transport layers a focus will be placed upon using diagnostics built into off-the-shelf managed Layer 2 Ethernet switches and ending with Network and Transport layer performance troubleshooting techniques using protocol analysis.

Practical open-source Wireshark based protocol analysis examples will focus upon performance troubleshooting and overall network health monitoring. Troubleshooting IP networks, especially performance issues can often be a daunting task for the broadcast engineer.

Applying a structured approach with a focus on utilization of open-source tools where possible combined with a practical understanding of IP networking basics can lead to efficient and effective problem resolution and insuring a healthy IP network infrastructure for the broadcast facility.
Outline for This Afternoon:

- Applying a Logical Process to Troubleshooting
- Review of the IP Networking OSI Model
- Physical Layer
- Data Link Layer
- Network Layer and Above
- Taping Into the Network & Viewing Activity
- Takeaways, Questions, and Maybe Some Answers 😊

Major Topics To Be Covered:

- The Logical Troubleshooting Process
- Understanding the OSI Model Data Flow Layers
- Physical Layer Verification
- Data Link Layer Verification
  - Understanding Ethernet Switch Errors
  - Use of Common Open-Source Tools
- Network Layer and Above Verification
  - Layer 3 Protocols
  - Understanding ping & traceroute
- Taping into the Network
  - Getting Started with Wireshark
  - Wireshark Capture
  - Views
  - Creating Custom Pre & Post Wireshark Filters
  - Capture Analysis Examples
- Developing a Network Baseline
- Additional Useful Tools
- Takeaways, Questions, and Maybe Some Answers 😊
Applying a Logical Process to Troubleshooting

5 Things Required To Build a Network

- **Send** Host
- **Receive** Host
- **Message** or Data to Send Between Hosts
- **Media** to Interconnect Hosts
- **Protocol** to Define How Data is Transferred

*A Network is a Group of Host Devices That Share a Common Addressing Scheme
*A Host is Any Device That Can Be Connected to That Network*
Network Performance Factors

• # of Devices Connected to the Network
  – Host Interaction - Segment Utilization
  – Broadcast Traffic (broadcast domain)
  – QoS (priority – best effort)

• # of Locations
  – Centralized / Decentralized
  – Bandwidth Uniformity

• Industry Applications
  – File Size
  – Response / Latency

• Host Traffic Pattern
  – External Hosts (cloud)

Think Outside the Bandwidth Box:
  Latency
  Packet Loss
  TCP Retransmission(s)

Troubleshooting Steps

- Identify the Problem
- Probable Cause – Establish Theory
- Test
- Formulate Plan of Action
- Implement Plan
- Verify Outcome
- Document (establish preventative measures)

Is a Re-Boot Really Resolving A Problem?

Don’t Believe the User
(unless they totally confess)

Touch the Low Hanging Fruit First
(Do not overlook the simple things)

You Often Are Proving The Network Is Not At Fault

It’s NOT the Network
Simplified Troubleshooting Process

1. Problem Identification
2. Problem Diagnosis
3. Problem Resolution

Develop a Structured Approach (systematic) To Resolution

Avoid an Unstructured Approach

Review of IP Networking OSI Model Data Flow Layers

1. Physical
2. Data Link
3. Network
4. Transport
The OSI Model

Open Systems Interconnection (OSI) Model

Developed by the International Organization for Standardization (ISO)
A Conceptual Model – Abstract in Nature – Modular in Structure
Provides “Layer Swapping” – Partitions Communications Function
Defines How Data Traverses From An Application to the Network

Networking Focus

Application Layers
- Application
- Presentation
- Session

Data Flow Layers
- Transport
- Network
- Data Link
- Physical

Application
Presentation
Session
Transport
Network
Data Link
Physical

1. Physical
   - Interfaces to Physical Network, Moves Bits Onto & Off Network Medium
2. Data Link
   - Provides Network Access Control, Physical Address (MAC), & Error Detection
3. Network
   - Provides Internetwork Routing (path), Provides Virtual Addressing (IP)
4. Transport
   - Manages End-End Connections, TCP, UDP, & Flow Control
The Protocol Data Unit

Layer | PDU |
------|-----|
4     | Segment |
3     | Packet |
2     | Frame |
1     | Bit |

1101001101111101100101010010001000010101010110001111111111

Encapsulation & De-Encapsulation
Network Addressing

• **Layer 2 PHYSICAL ADDRESS:**
  – MAC Address – 6 Bytes – Hexadecimal Notation - **00:12:3F:8D:4D:A7**
  – Fixed “Burned-in-Address” – Assigned by NIC Mfg.
  – Local in Scope

• **Layer 3 VIRTUAL ADDRESS**
  – IP Address – 4 Bytes (IPv4) – Doted-Decimal Notation – **165.95.240.185**
  – Based Upon Network
  – Globally Unique
Frame & Packet Flow Through a Network

MAC Address Changes As Frame Passes Through the Network
IP Address Does Not Change (unless NAT involved)

Physical Layer Verification

Interfaces to Physical Network, Moves Bits Onto & Off Network Medium
Ethernet Is the Standard Today!

- Conceptually Based Upon “ALOHA NET”
  - Developed as a “Wireless” Network by Norman Abramson & colleagues
  - Developed & Deployed at the University of Hawaii in 1971
- Later Re-Defined at Xerox PARC in 1973 to Become “Ethernet”
  - Bob Metcalf & David Boggs “Fathers of Ethernet”

Ethernet Media Evolution

“Thick-Net” Vampire Tap

“Thin-Net”

Topology Also Migrates from “Bus” to “Star” Based
### Many Types of Ethernet

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet GBIC &amp; SFP Modules</td>
<td></td>
</tr>
<tr>
<td><strong>“Giga-Bit Interface Converter”</strong> - GBIC Transceiver - SC Fiber Connector</td>
<td></td>
</tr>
<tr>
<td><strong>“Single Form-factor Pluggable”</strong> – SFP / SFP+ / XFP (mini GBIC) Transceiver - LC Fiber Connector</td>
<td></td>
</tr>
<tr>
<td><strong>Copper or Optical Based</strong> Transceiver to Provide Flexible Physical Interface</td>
<td></td>
</tr>
</tbody>
</table>

- **GBIC**
  - GBIC Transceiver - SC Fiber Connector
  - Single Form-factor Pluggable (SFP) / XFP (mini GBIC)
  - Transceiver - LC Fiber Connector

- **Copper or Optical Based**
  - Transceiver to Provide Flexible Physical Interface

---

**Ethernet GBIC & SFP Modules**

- "Giga-Bit Interface Converter" - GBIC Transceiver - SC Fiber Connector
- "Single Form-factor Pluggable" – SFP / SFP+ / XFP (mini GBIC) Transceiver - LC Fiber Connector
- **Copper or Optical Based** Transceiver to Provide Flexible Physical Interface
Copper Cable Test Terminology

- Understand What You Are Testing
  - The “Standard” Needed
  - The “Application” Involved

- **Cable Verification**
  - Basic Continuity (wiremap) & TDR

- **Cable Certification**
  - Demonstrates Compliance With Standard

- **Cable Qualification**
  - Evaluate Ability to Support Specific Bandwidth

- Testing Provides Assurance

<table>
<thead>
<tr>
<th>Name</th>
<th>Frequency</th>
<th>Ethernet Signal Supported</th>
<th>Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat 5</td>
<td>1 - 100MHz</td>
<td>10/100Base T</td>
<td>Stpc, RJ45</td>
</tr>
<tr>
<td>Cat5a</td>
<td>1 - 100MHz</td>
<td>10/100Base T, Gigabit Ethernet</td>
<td>Stpc, RJ45</td>
</tr>
<tr>
<td>Cat6</td>
<td>1 - 250MHz</td>
<td>10/100Base T, Gigabit Ethernet</td>
<td>Stpc, RJ45</td>
</tr>
<tr>
<td>Cat6a</td>
<td>1 - 500MHz</td>
<td>10/100Base T, Gigabit Ethernet, 10Gig Ethernet</td>
<td>Stpc, RJ45</td>
</tr>
<tr>
<td>Cat7</td>
<td>1 - 600MHz</td>
<td>10/100Base T, Gigabit Ethernet, 10Gig Ethernet</td>
<td>Stpc, TERA</td>
</tr>
<tr>
<td>Cat7a</td>
<td>1 - 1600MHz</td>
<td>10/100Base T, Gigabit Ethernet, 10Gig Ethernet</td>
<td>Stpc, TERA</td>
</tr>
</tbody>
</table>

Cable Wiring Faults Often Found

- **Continuity Issues / In-Correct Paring**
  - Reversed Pair: No pin-pin continuity
  - Transposed Pair: Twisted pair on wrong pins
  - Split Pair: TX/RX pair twist not maintained
EIA-568A vs 568B

Color Standard
EIA 568A

<table>
<thead>
<tr>
<th>NC</th>
<th>RX+</th>
<th>RX-</th>
<th>TX+</th>
<th>TX-</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Color Standard
EIA 568B

<table>
<thead>
<tr>
<th>NC</th>
<th>RX+</th>
<th>RX-</th>
<th>TX+</th>
<th>TX-</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

IEEE Standardized:

- 802.3af: 13w device power (minimum 44 V DC and 350 mA)
- 802.3at “PoE+”: 26w device power
- 802.3bt “PoE++”: 49w (type 3) or 96w (type 4) device power

Power Over Ethernet - PoE

- Allows Data & DC Power To Be Carried on the Same UTP Cable
- IEEE Standardized:
Twisted Pair Cabling Test Tools
Cisco Ethernet Switch TDR
(available on select models)

- test cable-diagnostics tdr interface xx/x

```
Switch test cable-diagnostics tdr interface gi/0/1
TDR test started on interface gi/0/1
A TDR test can take a few seconds to run on an interface
Use "show cable-diagnostics tdr" to read the TDR results.
```

```
Switch sh cable-diagnostics tdr int gi/0/1
TDR test last run on: March 01 00:00:00
```

<table>
<thead>
<tr>
<th>Interface Speed</th>
<th>Local Pair</th>
<th>Pair length</th>
<th>Remote Pair</th>
<th>Pair status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi/0/1 auto</td>
<td>Pair A</td>
<td>20 +/- 4 meters N/A</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>Pair B</td>
<td>20 +/- 4 meters N/A</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pair C</td>
<td>21 +/- 4 meters N/A</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pair D</td>
<td>20 +/- 4 meters N/A</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fiber Optics Verification

- Common FO Tests:
  - Continuity
  - Loss
  - Connector Face Inspection

- Advanced FO Tests:
  - OTDR
Fiber Optics Test Devices

- Power Meter
- Light Source
- OTDR (Optical Time Domain Reflectometer)
- Connector Inspection Microscope

Optical Guidelines

Example Loss Budget – Actual Levels Dependent Upon Specific Optical TX & RX Devices

- 1.0 dB / km – 1310nm MM
- 0.5 dB / km – 1310nm SM
- 0.3 dB / connector
- 0.3 dB / connector

-3 to -9 dB
-9 to -19 dB

Too Much RX Power Can Be Detrimental As Not Enough - Attenuate
Common Layer 1 Faults

**Copper Cabling Aspects:**
- Continuity Problems (open, shorts, crossed)
- Wrong Cable for Application
- Improper RJ-45 Installation
- Excessive "Un-Twist"
- Excessive Connections (connector blocks)
- Excessive Segment Length

**Fiber Cabling Aspects:**
- Damaged Fiber
- Improper Connector Installation
- Dirty Connectors
- Component Aging
Data Link Layer Verification

**Media Access Control (MAC) Address**

- **Organization Unique Identifier (OUI):** 24 bits
- **Mfg. Assigned:** 24 bits
- **6 hexadecimal digits:** 6 hexadecimal digits

OUI A4:67:06 = Apple, Inc.

http://www.wireshark.org/tools/oui-lookup.html

MAC Address Formats
Always 48 Bits – Expressed as Hexadecimal

Can Be Represented in Several Formats:

00:A0:C9:14:C8:29

00-A0-C9-14-C8-29

00A0.C914.C829

The Layer 2 Ethernet II (DIX) Frame

An Ethernet II (DIX) Frame

Invalid FRAME Lengths:
< 64 BYTES = "RUNT" FRAME
> 1518 BYTES = "GIANT" FRAME

Note—Preamble Not Used in Frame Length Calculation

Be Aware That Other Frame Types Exist!
Adding the VLAN Tag

**ETHERNET FRAME**

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION MAC ADDRESS</th>
<th>SOURCE MAC ADDRESS</th>
<th>TYPE</th>
<th>DATA</th>
<th>CRC</th>
</tr>
</thead>
</table>

**802.1Q ETHERNET FRAME**

<table>
<thead>
<tr>
<th>PREAMBLE</th>
<th>DESTINATION MAC ADDRESS</th>
<th>SOURCE MAC ADDRESS</th>
<th>802.1Q TAG</th>
<th>TYPE</th>
<th>DATA</th>
<th>CRC</th>
</tr>
</thead>
</table>

**4 bytes**

802.1Q TAG

TPID "0x8100" PRI CF I VLAN ID

**VLAN ID = 12 bits Yields 4,096 Possible VLANs**

---

**Ethernet Auto-Negotiation**

- **Auto Configuration of Port Duplex & Speed**
  - Utilizes Ethernet FLP & NLP Bursts
- **Duplex**: Half Duplex or Full Duplex
- **Speed**: 10 / 100 / 1000 Mbps
- **Insure Both Endpoint Devices Are Set to Auto**
  - 10 Mbps Full Duplex is Not a Valid Mode
  - 100 Mbps Half Duplex Indicates Auto-Negotiation Failure
- **IMHO Best Practice – Static Configure Infrastructure**
  - Duplex Mismatch = Poor Performance = CRC Errors
  - Be Careful Depending Upon Auto-Negotiation

![Half-Duplex](image)

Sending Information

![Full-Duplex](image)

Sending and Receiving Information
Duplex Mismatch Result

When Duplex Mismatch Occurs:
High Collision Rate Results, thus Performance Reduced

Cisco Switchport Metrics
Common Layer 2 Faults

- Failed or Intermittent Host NIC
- Failed or Intermittent Switch Port
- Duplex Mismatch
- Excessive Errors

Use “Managed” Switch Port Capabilities To Verify Operation
Network Layer and Above Verification

The IPv4 Packet Header

- Version (4)
- Header (4)
- Precedence / Type (8)
- Length (16)
- Identification (16)
- Flag (3)
- Offset (13)
- Time to Live (8)
- Protocol (8)
- Header Checksum (16)
- Source IP Address (32)
- Destination IP Address (32)
- Options & Padding (0 or 32)
- Packet Payload (Transport Layer Data)
IPv4 Header Fields of Interest

- **Version** – Indicates IPv4 or IPv6
- **Length** – Datagram Length (20 – 65,535 bytes) Usually (5) 32-bit words
- **Flag** – Indicates if a Packet Can Be Fragmented
- **Time to Live “TTL”** – Maximum “hop” Distance the Packet Can Travel
- **Protocol** – Indicates upper layer protocol (TCP, UDP, ICMP as examples)
- **Source Address** – Address of “sending” Host
- **Destination Address** – Address of “receiving” Host
- **Options & Padding** – Fills Packet With Bits to End Packet On a 32-Bit Boundary

---

Is My IP Address Correct?

**IP Addressing “Rules”**

- Each Network MUST Have a Unique Network ID
- Each Host MUST Have a Unique Host ID
- Every IP Address MUST Have a Subnet Mask
  - Implied for a Classful Network
  - Explicit Stated for Classless Network
- An IP Address Must Be Unique Globally If Host on the Public Internet

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.1.100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
2-Part IPv4 Address

VLSM

- Allows Mask to Be Determined on a “Bit Basis”
  - Remember: Classful Addressing Specified Network/Host Boundary
  - Classless Addressing Allows Network/Host Boundary to Be Specified at an Individual Bit

19 Subnet Mask Bits = 255.255.224.0
Primary TCP/IP System Protocols:

- **ARP** – Address Resolution Protocol
  - Maps an IP Address to a MAC Address
- **DHCP** – Dynamic Host Configuration Protocol
  - Provides Host IP Configuration Information
- **DNS** – Domain Name System
  - Translates a Host Name to an IP Address
- **ICMP** – Internet Control Message Protocol
  - *The “Tattle Tale” Protocol*
Understanding ICMP (ping & traceroute foundation)

- The “Internet Control Message Protocol”
  - ICMPv4 defined by RFC-792 & 2463
  - ICMPv6 defined by RFC-2463
- An Error Messaging & Information Reporting Scheme:
  - Error Messages
  - Query Messages
- Reports ONLY to the Sending Host

---

“ping” Packet Internet Groper

Send Hosts Sends ICMP “echo request”
Destination Host Replies ICMP “echo reply”
Round-Trip Times Returned

Keep In Mind - “ping” is a basic “reachability” test
Using “ping”

- **LINUX**
  
  ```
  w deadline] [-f flooded] [-I interface] [-M hint] [-a (host) | -n (IP)] [-s sendbuf] [-T timeout] [-
  w ...] destination
  ```

- **Windows**
  
  ```
  ```

---

“traceroute”

**RFC 1812**

- The Most Widely Used Network Diagnostic Tool / The Most Widely Misunderstood Network Diagnostic Tool

- **How?**
  
  - Send Host Transmits 3 UDP Packets to Receive Host With TTL = 1 (port typical 33434)
  - First Hop Router Sends icmp TTL Exceeded
  - Send Host Transmits 3 UDP Packets to Receive Host With TTL = 2
  - Second Hop Router Sends icmp TTL Exceeded
  - Send Host Transmits 3 UDP Packets to Receive Host With TTL = 3
  - Third Hop Router Sends icmp TTL Exceeded
  - Send Host Transmits 3 UDP Packets to Receive Host With TTL = 4
Understanding “traceroute”

Windows Command Screen “tracert”

What is Up?

Limitations of “ping” & “traceroute”

- **ICMP May Be Blocked Within Networks**
- **Routers May Limit ICMP Processing (interfaces limited)**
- **Realize Layer 2 Devices Will Not Be Seen**
- **Protocol Utilized by traceroute Can Impact Results (UDP, ICMP, TCP)**
- **Understand:**
  - traceroute Forward Path Route is Displayed (return path may be different)
  - traceroute returns Round-Trip Latency
- **Understand Traceroute Latency:**
  - Latency Increase May Not Be Significant
  - Latency Increase Must Continue Increasing for Additional Hops To Be of Concern
The “Loopback” Interface
Test Local IP Stack and Network Adapter

- The “Loop-Back” Address
  - IPv4 Loopback: **127.0.0.1**
    - Actually Any 127.0.0.0/8 Address Works OR the Range of 127.0.0.1 to 127.255.255.255
  - IPv6 Loopback: **::1**

```
ping 127.2.3.4
PING 127.2.3.4: 56 data bytes
64 bytes from 127.2.3.4: icmp_seq=0 ttl=64 time=0.106 ms
64 bytes from 127.2.3.4: icmp_seq=1 ttl=64 time=0.095 ms
64 bytes from 127.2.3.4: icmp_seq=2 ttl=64 time=0.106 ms
64 bytes from 127.2.3.4: icmp_seq=3 ttl=64 time=0.095 ms
--- 127.2.3.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

```
ping ::1
PING ::1: 56 data bytes
64 bytes from ::1: icmp_seq=0 ttl=64 time=0.095 ms
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.095 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.095 ms
--- ::1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Taping Into the Network
Viewing Network Activity

**Protocol Analysis**

- Wireshark - Analyses of “Live” & “Recorded” Network Activity
- “Open Source” Protocol Analyzer Application
- Often Referred to as a “Sniffer” ©
- Developed in 1998 as “Ethereal”
- Renamed in 2006 Due to Trademark Issues
- Useful To:
  - “See” Host Activity on a Network
  - Isolate Performance Issues
  - Understand Application Interaction/Configuration
  - Network Benchmarking

---

Obtain & Install “Wireshark”

- Available for Windows, Mac OSx, & Linux
- Download (current v2.0.1): [www.wireshark.org](http://www.wireshark.org)
- Be Sure to Include Libraries:
  - WinPcap (Windows)
  - Libpcap (Unix/Linux)
- Install
- Start Wireshark
- Select Interface
- Click “Start”
- CTRL+E will Stop
- You Have Created a PCAP File!
- View & Analyze Results
- Save For Later Analysis
**NIC “Promiscuous” Mode**

“Promiscuous” Mode
Processes All Frames Received

**Wireshark Host Requirements**

- Apple OSx, Debian GNU/Linux, FreeBSD, Mandriva Linux, NetBSD, Red Hat Enterprise/Fedora Linux, and several others.
- 64-bit AMD64/x86-64 or 32-bit x86 processor.
- 400 MB available RAM. Larger capture files require more RAM.
- 300 MB available disk space. Capture files require additional disk space.
- 1024x768 (1280x1024 or higher recommended) resolution / 16 bit color minimum.
- A supported Network Interface

Keep in Mind:
Capturing on a 100 Mbps network can produce hundreds of megabytes of capture data in a very short time. A fast processor, lots of memory and disk space is always a good idea.
Where to Tap?

- **Problem** Nature Often Determines:
  - At Problem Host
  - At Destination Host
  - Mid-Network Locations
- **Accessibility** May Also Drive Tap Point

_**Remember:** Interfaces are Bi-Directional_

**Keep in Mind the PDU**
How to Tap Ethernet & Capture Packets

• Can Be Challenging!
• How to Capture?
  – UTP Ethernet:
    • Physical Passive Tap
    • Active Tap
  – Optical Ethernet:
    • Physical Passive Tap
    • Active Tap
  – Ethernet Switch Port Mirror
  – Run Wireshark on Client Host

Active Tap Devices
Selecting the Tap Point:

**Problem** Nature Often Determines:
- At Problem Host
- At Destination Host
- Mid-Network Locations

**Accessibility** May Also Drive Tap Point

---

Shared Media Approach

10/100 Mbps Maximum – Half-Duplex Only

It Was Simpler In The Past

Half-Duplex Shared Media Networks Not Commonplace Today
Switched Media Approach

Switched Media “Hub” Approach

Normal Ethernet Switch Operation Prevents Network Traffic Between Host A and Host B To-Be-Seen by the Wireshark Capture Host

Works, But Downgrading Network To Half-Duplex Ethernet Switch Now Sees 2-MAC Addresses (problem if switch-port security is enabled)
Switched Media “Tap” Approach

Works, but often costly especially when GigE UTP or optical network involved

Switched Media “Monitor Port” Approach

Recommended Approach (where possible)
Keep In Mind!

Limitations:
“Bad” Frames Not “Mirrored”
No VLAN Tags Passed
Caution With RTP Network Traffic

Remember:
Tapping a Network Can Be Challenging!

Cisco Ethernet Switch “SPAN Port”

```
config t
monitor session 1 source interface fa0/1
monitor session 1 source interface fa0/23
monitor session 1 destination interface fa0/14
exit
```
HP Procurve Ethernet Switch “Port Mirror”

config
mirror-port 14
int 1, monitor (int 1-12, monitor)
int 23, monitor
show monitor
exit

My Favorite Tap Approaches

GS105Ev2
GigE, Port Mirror, VLAN, Cable Check
Amazon $ 41.40
Creating Custom Wireshark Views

Captured Packet(s)
Selected Header
Data Decoded
Payload Data
Decoded Hexadecimal & ASCII
Filtering

• Capture Filters
  – Selectively Capture Packets
  – Pre-Capture Configuration
  – Minimizes Amount of Captured Data

• Display Filters
  – Applied When Viewing
  – Allows Focusing on Attribute(s)
  – All Data is Retained

• Which One to Use?
  – Reason for Capturing Dictates Proper Filter Use
  – Use “Capture” Filter When You Know What You Are Looking For
  – Remember: You Can’t Display What Has Not Been Captured!
Using “Capture” Filters

Useful “Capture” (pcap) Filter Examples

- ip
- tcp
- udp
- host 165.95.240.130
- host 165.95.240.128/26
- host 165.95.240.128 mask 255.255.255.192
- src net 165.95.240.128/26
- dst net 165.95.240.128/26
- port 80
- not broadcast and not multicast

http://www.tcpdump.org/manpages/p pcap-filter.7.html
Using “Display” Filters

Useful “Display” Filter Examples

- eth.addr==00:19:c8:c8:22:7f
- ip
- ip.addr==165.95.240.130
- ip.addr==165.95.240.130 or ip.addr==165.95.240.129
- tcp
- tcp.port==80
- udp
- udp.port==50000
- http

http://www.firstdigest.com/2009/05/wiresharks-most-useful-display-filters/
TCP 3-Way Handshake

Find the 1st SYN Packet:  “Edit>Find Packet”
Enter “tcp.flags.syn==1”
Right Click on Packet – Select “Follow TCP Stream”

ICMP Example
Streaming Media Example

Developing a Network Baseline
Baseline Performance

www.networkuptime.com/tools/enterprise

Wireshark Statistics
Additional Tools

Commercial Tools
Fluke Networks “Clearsight”

http://www.klos.com/products/packetvault/

Takeaways, Questions, and Maybe Some Answers 😊

https://nmap.org/zenmap/
Takeaway Points & Concepts

• Establish a "Structured" Troubleshooting Approach
  – Avoid “Shooting from the Hip” Approach(s)
• Use the OSI Model as a Guide to a Structured Approach
  – Work You Way Up the “IP Stack”
    • Verify Layer 1 Physical Connectivity
    • Verify Layer 2 Connectivity is Error Free
    • Verify Layer 3 Inter-Networking
    • Use Protocol Analysis to “See” Network activity
• **80% of Network Problems is Physical Infrastructure Based**
  – Standards Not Properly Applied
  – Installation Guidelines Not Adhered To
  – Don’t Loose Sight of **100m** Ethernet UTP Segment Limit!

---

Takeaway Points & Concepts

• Use Protocol Analysis to “See” Network Host Interaction”
• “Wireshark” Is The Most Popular Protocol Analyzer
• Understanding the OSI Model & TCP/IP Protocol Action is Key to Understanding Wireshark Results
• Understand How & Where to Capture Network Activity
• “Filtering” is Essential to Find the Needle in the Haystack
  – Capture Filters (minimize captured data)
  – Display Filters (minimize displayed info)
• Customize Your Wireshark Views
• Verify Everything Yourself
• Caution Trusting What You Are Told!
My Favorite Reference Texts:

1. The Illustrated Network
2. Network Warrior
3. Ethernet: The Definitive Guide

Further Wireshark Study

- Wireshark Network Analysis
- Wireshark Essentials
- Wireshark 101

https://wiki.wireshark.org/

https://www.wireshark.org/docs/wsug_html/
Section 4
Information Technology Systems

Chapter 2: Information Technology and the Broadcast Plant
Chapter 3: Network System Overview
Chapter 4: Data and Frequency Troubleshooting
Chapter 5: Remote Development, and More Standards for Video Transport and Internet Standard Networks

Flowchart For Problem Resolution

Is It Working?

Do It

YES

NO

Did You Mess With It?

YES

YOU IDIOT!

NO

Anyone Else Known?

YES

You're SCREWED!

NO

Can You Blame Someone Else?

YES

NO

Will It Blow Up in Your Hands?

YES

Look The Other Way

NO

NO PROBLEM!

NO PROBLEM!
SBE National Elections

July 25 - August 25

Thank You For Your Vote for SBE Board Member!

Wayne M. Pecena CPBE, CBNE
SBE Board of Directors – Executive Committee Member
Education Committee Chair
Since 2012
Thank You for Attending!

Wayne M. Pecena  
Texas A&M University  
w-pecena@tamu.edu

979.845.5662