Chapter 8
Network Troubleshooting

Part I

Network Troubleshooting

Establishing the Network Performance Baseline
Establishing the Network Performance Baseline

- To efficiently diagnose and correct network problems, a network engineer needs to know:
  - How the network has been designed.
  - The network’s expected performance.
- This information is captured in the network documentation.

Network documentation usually includes 3 components:
- Network Topology Diagram.
- Network Configuration Table.
- End-system Configuration Table.

Documenting Your Network

- Network Topology Diagram:
  - Graphical representation of a network, illustrating how each device in a network is connected and its logical architecture.
Documenting Your Network

### Network Configuration Table:
- **Contains accurate, up-to-date** records of the hardware and software used in a network.

<table>
<thead>
<tr>
<th>Device Name, Model</th>
<th>Interface Name</th>
<th>MAC Address</th>
<th>IP Address/Subnet Mask</th>
<th>IP Routing Protocol(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1, Cisco 2611XM</td>
<td>fa0/0</td>
<td>00:07:0500:109</td>
<td>192.168.10.1/24</td>
<td>EIGRP 10</td>
</tr>
<tr>
<td></td>
<td>fa0/1</td>
<td>00:07:0500:160</td>
<td>192.168.11.1/24</td>
<td>EIGRP 10</td>
</tr>
<tr>
<td></td>
<td>e0/0/0</td>
<td></td>
<td>10.1.1.1/24</td>
<td>OSPF</td>
</tr>
<tr>
<td>R2, Cisco 2611XM</td>
<td>fa0/0</td>
<td>00:07:0500:109</td>
<td>192.168.20.1/24</td>
<td>EIGRP 10</td>
</tr>
</tbody>
</table>

### End-System Configuration Table:
- **Contains baseline records of the hardware and software used in end-system devices.**

<table>
<thead>
<tr>
<th>Device Name (Purpose)</th>
<th>Operating System / Version</th>
<th>IP Address / Subnet Mask</th>
<th>Default Gateway Address</th>
<th>DNS Server Address</th>
<th>WINS Server Address</th>
<th>Network Applications</th>
<th>High Bandwidth Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV2 (Web Server)</td>
<td>UNIX</td>
<td>209.165.201.128/27</td>
<td>209.165.201.1/27</td>
<td>209.165.201.1/27</td>
<td>HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC1 (Admin/Engineer)</td>
<td>UNIX</td>
<td>192.168.10.12/24</td>
<td>192.168.10.1/24</td>
<td>192.168.10.1/24</td>
<td>FTP Telnet, VoIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC2 (User Eng)</td>
<td>Windows XP Pro SP2</td>
<td>192.168.11.10/24</td>
<td>192.168.11.1/24</td>
<td>192.168.11.1/24</td>
<td>HTTP, VoIP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Documentation Process

- **Useful Commands:**
  - **ping**: To test connectivity with neighbouring devices.
  - **telnet**: Log in remotely to a device for accessing configuration information.
  - **show ip interface brief**: To display the up or down status and IP address of all interfaces.
  - **show ip route**: To display the routing table in a router to learn the directly connected neighbors, more remote devices (through learned routes), and the routing protocols.
  - **show cdp neighbor detail**: To obtain detailed information about directly connected Cisco neighbor devices.
Why Establish a Network Baseline?

- How does the network perform during a normal or average day?
- Where are the most errors occurring?
- What alert thresholds should be set for the devices that need to be monitored?
- Can the network meet the identified policies?
- The network baseline determines the “personality” of a network under normal conditions.
- What part of the network is most heavily used?
- What part of the network is least used?

Steps for Establishing a Network Baseline

- Three Steps:
  - Step 1: Determine what types of data to collect.
  - Start by selecting a few variables that represent the defined policies.
  - If too many data points are selected, the amount of data can be overwhelming.
  - Generally, some good measures are interface utilization and CPU utilization.

What’s Up Gold
Steps for Establishing a Network Baseline

- Three Steps:
  - Step 2: Identify those key devices and ports for which performance data should be measured.
  - Step 3: Determine the baseline duration.
    - At least seven days to capture any daily or weekly trends.
    - Should last no more than six weeks.
    - Generally, a two to four week baseline is adequate.
Steps for Establishing a Network Baseline

- **Measuring Network Performance Data:**
  - Sophisticated network management software is often used to baseline large networks.
  - Fluke Network SuperAgent.
  - Netscout’s Sniffer Pro.
  - HP Openview.

- **In simpler networks, the baseline tasks may require a combination of manual data collection and simple network protocol inspectors.**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Shows uptime, version information for device software and hardware.</td>
</tr>
<tr>
<td>show ip interface [brief]</td>
<td>Shows all the configuration options that are set on an interface. Use the brief keyword to only show updown status of IP interfaces and the IP address is of each interface.</td>
</tr>
<tr>
<td>show interface [interface_type interface_num]</td>
<td>Shows detailed output for each interface. To show detailed output for only a single interface, include the interface type and number in the command (e.g. ethernet 1/0).</td>
</tr>
<tr>
<td>show ip route</td>
<td>Shows the contents of the routing table.</td>
</tr>
<tr>
<td>show arp</td>
<td>Shows the contents of the arp table.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows current configuration.</td>
</tr>
<tr>
<td>show port</td>
<td>Shows the status of ports on a switch.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Shows the status of VLANs on a switch.</td>
</tr>
<tr>
<td>show tech-support</td>
<td>Runs other show commands, and provides many pages of detailed output, designed to be sent to technical support. Also useful for other purposes.</td>
</tr>
</tbody>
</table>
**Final Thoughts**

- To most Network Administrators, documentation is a:

  But (no pun intended), it is **absolutely necessary** for a well designed, well implemented and well maintained network.

**Network Troubleshooting**

Troubleshooting Methodologies and Tools
General Approach to Troubleshooting

- Network engineers, administrators, and support personnel realize that troubleshooting is a process that takes the greatest percentage of their time.
  - Using efficient troubleshooting techniques shortens overall troubleshooting time.
  - Two extreme approaches to troubleshooting almost always result in disappointment, delay, or failure.

At one extreme is the theorist, or rocket scientist, approach.
- The rocket scientist analyzes and reanalyzes the situation until the exact cause at the root of the problem has been identified.
- While this process is fairly reliable, few companies can afford to have their networks down for the hours or days that it can take for this exhaustive analysis.
**General Approach to Troubleshooting**

- At the other extreme is the impractical, or caveman, approach.
  - The caveman's first instinct is to start swapping cards; changing cables; changing out or upgrading software and increasing bandwidth until, miraculously, the network begins operating again.
  - This does not mean that the network is working properly, just that it is operating.
  - It may achieve a change in symptoms faster, but it is not reliable nor does it find the root cause of the problem.

- The better approach is somewhere in the middle using elements of both.
  - It is important to analyze the network as a whole rather than in a piecemeal fashion.
  - A systematic approach minimizes confusion and cuts down on time otherwise wasted with trial and error.
  - This is where a well documented and maintained network will save you both time and money.
Logical networking models, such as the OSI and TCP/IP models, separate network functionality into modular layers.

When troubleshooting, these layered models can be applied to the physical network to isolate network problems.

**OSI Reference Model:**

- Application Issues. Implemented in software.
- Data Transport Issues
- Software
- Hardware
Using Layered Models for Troubleshooting

- Devices and the OSI Model:

- TCP/IP Reference Model:
General troubleshooting can be broken down into 4 stages.

Point to Ponder: Which is worse?
The right answer to the wrong problem.
Or
The wrong answer to the right problem.
Troubleshooting Methods:

- Start with the physical components of the network and move up through the layers.
- A good approach to use when the problem is suspected to be a physical one.

General Troubleshooting Procedures

- Troubleshooting Methods:
  - Start with the end-user applications and move down the layers of the OSI model.
  - This approach is good for simpler problems or when you think the problem is with a piece of software.
• **Troubleshooting Methods:**
  - Start by collecting user experience of the problem and make an informed guess as to which OSI layer to start your investigation.
  - *e.g.* If users can’t access the web server and you can ping the server, then you know that the problem is above Layer 3.

**General Troubleshooting Procedures**

- Take the time to select the most effective network troubleshooting method.
- **For Example:**
  - Two IP routers are not exchanging routing information.
  - The last time this type of problem occurred it was a protocol issue.
  - You choose the divide-and-conquer troubleshooting method.
  - You begin testing the TCP/IP-related functions at the Data Link Layer and move up.
### General Troubleshooting Procedures

#### Gathering Symptoms:

- **Analyze existing symptoms**
- **Contact external administrator**

![Diagram showing troubleshooting process]

- **Determine ownership**
  - **Is the problem within the autonomous system?**
  - **Yes**
  - **Narrow scope**
  - **Determine symptoms**
  - **Document symptoms**

- **Solve problem and document the solution**
  - **Yes**
  - **Can the problem be solved using the documented symptoms?**
  - **Yes**
  - **No**

- **Begin isolating**

---

### Useful troubleshooting commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping (host</td>
<td>ip-address)</td>
</tr>
<tr>
<td>traceroute (destination)</td>
<td>Identifies the path a packet takes through the network. The destination variable is the hostname or IP address of the target system.</td>
</tr>
<tr>
<td>telnet (host</td>
<td>ip-address)</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>Displays a summary of the status of all interfaces on a device.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the current state of the IP routing table.</td>
</tr>
<tr>
<td>show running-config interface</td>
<td>Displays contents of currently running configuration file for a particular interface</td>
</tr>
<tr>
<td>[no] debug ?</td>
<td>Displays a list of options for enabling or disabling debugging events on a device.</td>
</tr>
<tr>
<td>show protocols</td>
<td>Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.</td>
</tr>
</tbody>
</table>
Questioning Users:

<table>
<thead>
<tr>
<th>Guidelines</th>
<th>Example End-user Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask questions that are pertinent to the problem.</td>
<td>What does not work?</td>
</tr>
<tr>
<td>Use each question as a means to either eliminate or discover possible problems.</td>
<td>Are the things that do work and the things that do not work related?</td>
</tr>
<tr>
<td>Speak at a technical level that the user can understand.</td>
<td>Has the thing that does not work ever worked?</td>
</tr>
<tr>
<td>Ask the user when the problem was first noticed.</td>
<td>When was the problem first noticed?</td>
</tr>
<tr>
<td>Did anything unusual happen since the last time it worked?</td>
<td>What has changed since the last time it did work?</td>
</tr>
<tr>
<td>Ask the user to recreate the problem, if possible.</td>
<td>Can you reproduce the problem?</td>
</tr>
<tr>
<td>Determine the sequence of events that took place before the problem happened.</td>
<td>When exactly does the problem occur?</td>
</tr>
</tbody>
</table>

My tips:
- Remember that users are now used to technological advances.
  - There are very few, if any, “dumb users” anymore.
- Don’t portray yourself as a know-it-all. If you do, you can expect the least amount of co-operation.
- Be specific in your questions at the user’s level.

Point to Ponder: Which is worse? The right answer to the wrong question. or The wrong answer to the right question.
A wide variety of software and hardware tools are available to make troubleshooting easier.

- Gather and analyze symptoms of network problems.
- Provide monitoring and reporting functions.
- Establish the network baseline.
  - Network Management Systems (NMS).
  - Knowledge Bases.
  - Baselining Tools.
  - Protocol Analyzers.

Software Troubleshooting Tools

- Network Management Systems (NMS).
  - CiscoView
  - HP Openview
  - Solar Winds
  - What's Up Gold
  - Device level monitoring / configuration.
  - Graphic display.
Software Troubleshooting Tools

**Knowledge Bases:**
- On-line network device vendor knowledge bases have become indispensable sources of information.
- Vendor based knowledge bases are a vast pool of searchable experience based information.

**Baselining Tools:**
- Can help draw network diagrams, help to keep network software and hardware documentation up-to-date and help to cost effectively measure baseline network bandwidth use.
Software Troubleshooting Tools

- **Protocol Analyzers:**
  - A protocol analyzer decodes the various protocol layers in a recorded frame and presents this information in a relatively easy to use format.
  - Filter traffic.
  - Reporting.
  - Wireshark.
  - Sniffer Pro.

Hardware Troubleshooting Tools

- **Network Analysis Module:**
  - Cisco Catalyst 6500 series switches and Cisco 7600 series routers.
Hardware Troubleshooting Tools

- **Digital Multimeters:**
  - Digital multimeters (DMMs) are test instruments that are used to directly measure electrical values of voltage, current, and resistance.

Hardware Troubleshooting Tools

- **Cable Testers:**
  - Cabling testers can be used to detect broken wires, crossed-over wiring, shorted connections and improperly paired connections.
Hardware Troubleshooting Tools

- **Cable Analysers:**
  - Cable analyzers are multifunctional handheld devices that are used to test and certify copper and fiber cables for different services and standards.
  - Distance to performance defects.
  - Identify corrective actions.
  - Graphically display crosstalk and impedance behavior.

Hardware Troubleshooting Tools

- **Portable Network Analyzers:**
  - Portable devices for troubleshooting switched networks and VLANs.
  - Plug in anywhere on the network.
  - Switch port to which the device is connected and the average and peak utilization.
  - Discover VLAN configuration, identify top network talkers and analyze network traffic.
Portable Network Analyzers:
- Portable devices for troubleshooting switched networks and VLANs.
- Plug in anywhere on the network.
- Switch port to which the device is connected and the average and peak utilization.
- Discover VLAN configuration, identify top network talkers and analyze network traffic.

Hardware Troubleshooting Tools

Plume Networks OptiView™ Series III Integrated Network Analyzer