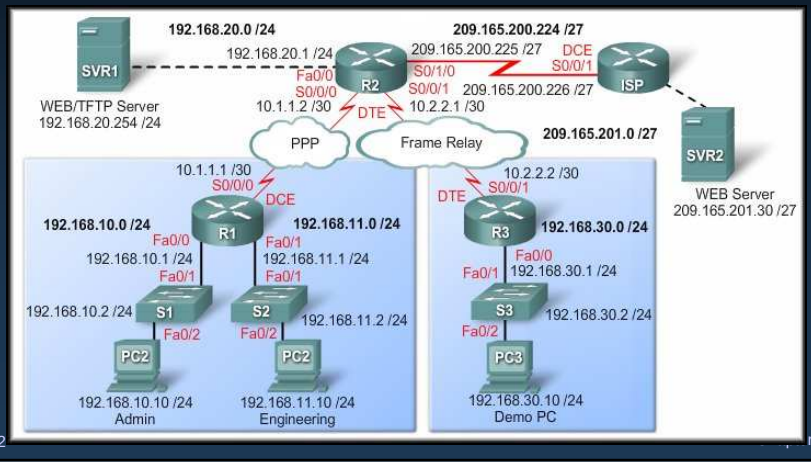
Chapter 8

Network Troubleshooting

Part I

Network Troubleshooting

Establishing the Network Performance Baseline



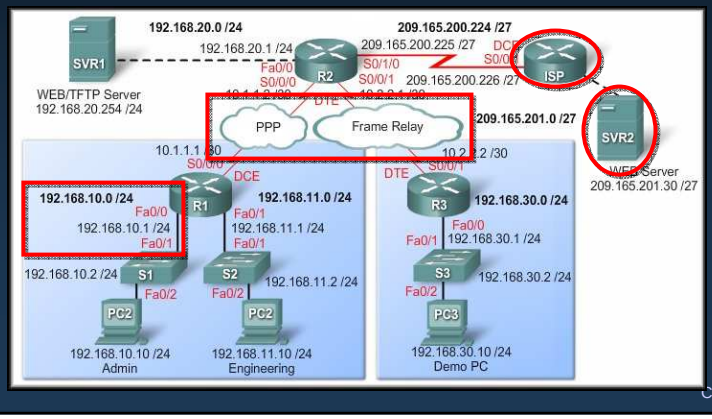
Establishing the Network Performance Baseline

- 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.

Device Name, Model	Interface Name	MAC Address	IP Address/Subnet Mask	IP Routing Protocol(s)
R1, Cisco 2611XM	fa0/0	0007.8580.a159	192.168.10.1 /24	EIGRP 10
	fa0/1	0007.8580.a160	192.168.11.1 /24	EIGRP 10
	s0/0/0	--- ---	10.1.1.1/30	OSPF
	s0/0/1	--- ---	Not Connected	
R2, Cisco 2611XM	fa0/0	0007.8580.a159	192.168.20.1 /24	EIGRP 10

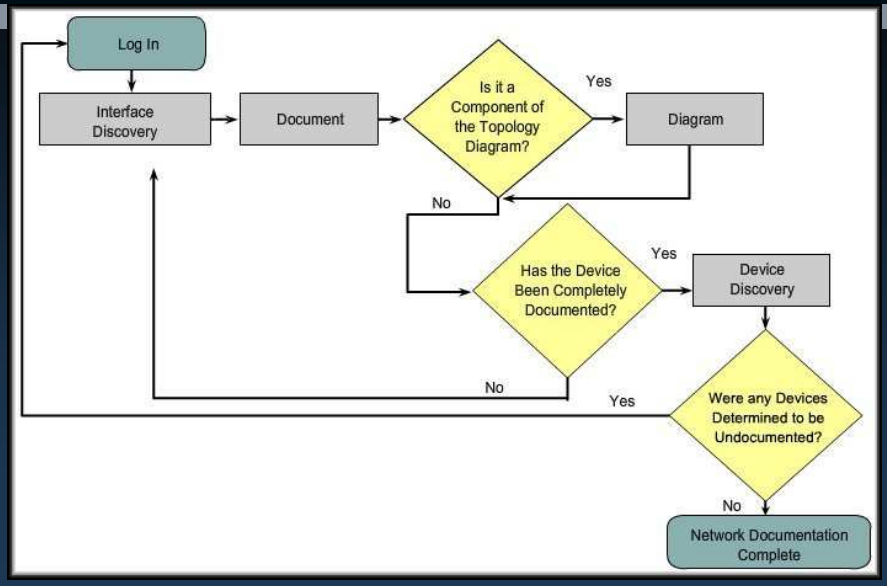
Switch Name, Model, Management IP Address	Port Name	Speed	Duplex	STP State (Fwd / Block)	Port Fast (Yes / No)	Trunk Status	Ether Channel (L2 or L3)	VLANs	Key
S1, Cisco WS-C3550-24-SMI, 192.168.10.2 /24	fa0/1	100	Auto	Fwd	No	On	L2	1	Connects to R1
	fa0/2	100	Auto	Fwd	No	On	L2	1	Connects to PC1
	fa0/3								Not Connected
	fa0/4								Not Connected

Documenting Your Network

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

Device Name (Purpose)	Operating System / Version	IP Address / Subnet Mask	Default Gateway Address	DNS Server Address	WINS Server Address	Network Applications	High Bandwidth Applications
SRV1 (Web/TFTP Server)	UNIX	192.168.20.254 /24	192.168.20.1 /24	192.168.20.1 /24		HTTP FTP	-
SRV2 (Web Server) co-located at ISP	UNIX	209.165.201.30 /27	209.165.201.1 /27	209.165.201.1 /27		HTTP	-
PC1 (Admin Term)	UNIX	192.168.10.10 /24	192.168.10.1 /24	192.168.10.1 /24		FTP Telnet	VoIP
PC2 (User PC – Engineering)	Windows XP Pro SP2	192.168.11.10 /24	192.168.11.1 /24	192.168.11.1 /24		HTTP FTP	VoIP
PC3 (Demo PC – Marketing)	Windows XP Pro SP2	192.168.30.10 /24	192.168.30.1 /24	192.168.30.1 /24		HTTP	Streaming Video VoIP

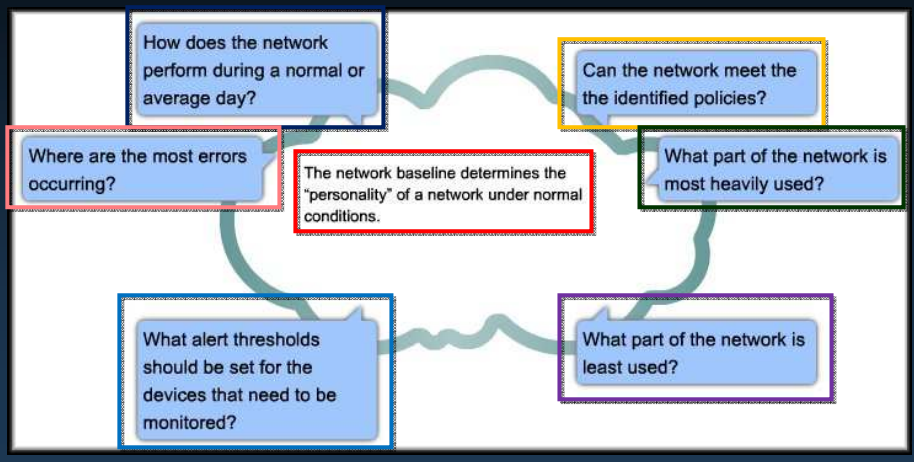
Network Documentation Process



Network Documentation Process

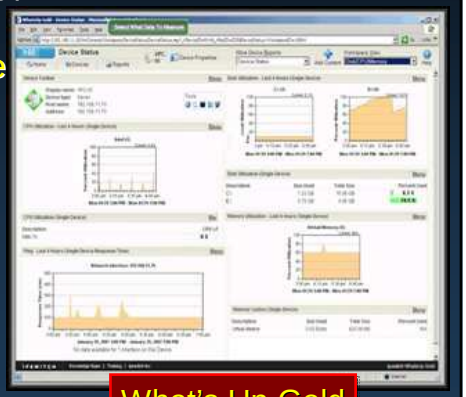
- Useful Commands:
  - ping: To test connectivity with neighbouring devices.
  - telnet: Log in remotely to a device for accessing configuration information.
  - show ip interface brief: To display the up or down status and IP address of all interfaces.
  - show ip route: To display the routing table 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?



Steps for Establishing a Network Baseline

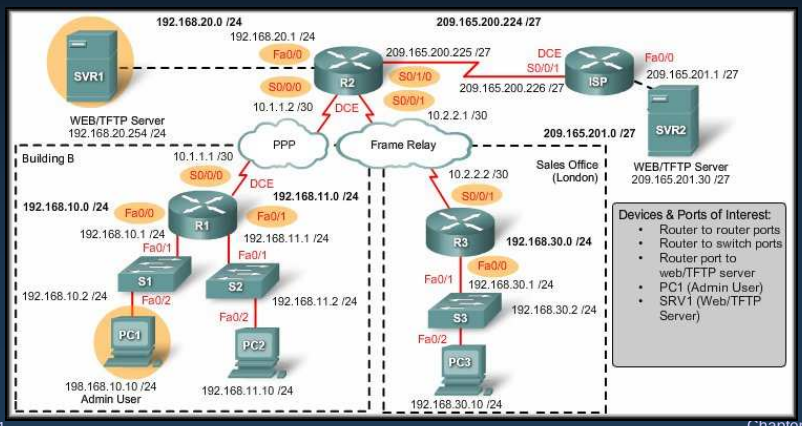
- Three Steps:
  - Step 1: Determine what types of data to collect.
  - Start by selecting a few variables that represent the defined policies.
  - If too many data points are selected, the amount of data can be overwhelming.
  - Generally, some good measures are interface utilization and CPU utilization.



What's Up Gold

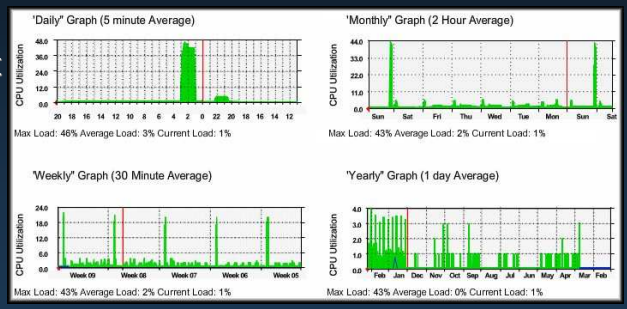
Steps for Establishing a Network Baseline

- Three Steps:
  - Step 2: Identify those key devices and ports for which performance data should be measured.



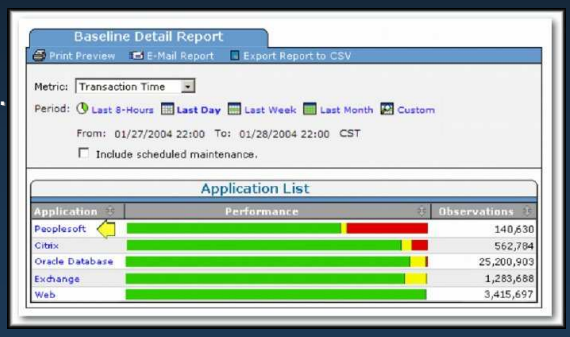
Steps for Establishing a Network Baseline

- Three Steps:
  - 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.



Steps for Establishing a Network Baseline

- Measuring Network Performance Data:
  - In simpler networks, the baseline tasks may require a combination of manual data collection and simple network protocol inspectors.

Command	Description
show version	Shows uptime, version information for device software and hardware.
show ip interface [brief]	Shows all the configuration options that are set on an interface. Use the **brief** keyword to only show up/down status of IP interfaces and the IP address is of each interface.
show interface *[interface_type interface_num]*	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 0/0).
show ip route	Shows the contents of the routing table.
show arp	Shows the contents of the arp table.
show running-config	Shows current configuration.
show port	Shows the status of ports on a switch.
show vlan	Shows the status of VLANs on a switch.
show tech-support	Runs other show commands, and provides many pages of detailed output, designed to be sent to technical support. Also useful for other purposes.

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 their time.
  - Using efficient troubleshooting techniques shortens overall troubleshooting time.
  - Two extreme approaches to troubleshooting almost always result in disappointment, delay, or failure.

General Approach to Troubleshooting

- 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

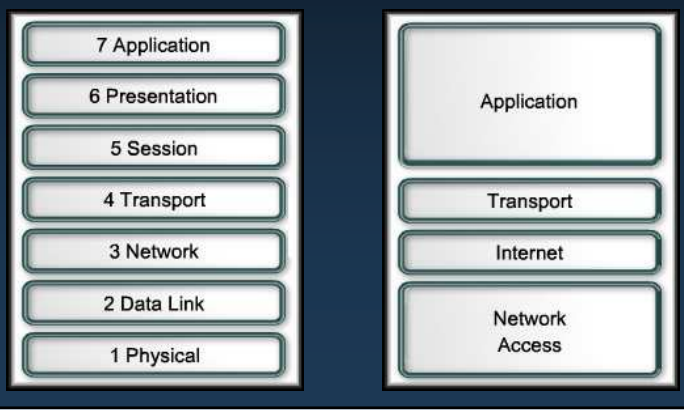
- At the other extreme is the impractical, or **caveman**, approach.
  - The caveman's first instinct is to start **swapping cards; changing cables; changing out or upgrading software and increasing bandwidth** until, miraculously, the network begins operating again.
  - This does not mean that the network 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.**

General Approach to Troubleshooting

- 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.

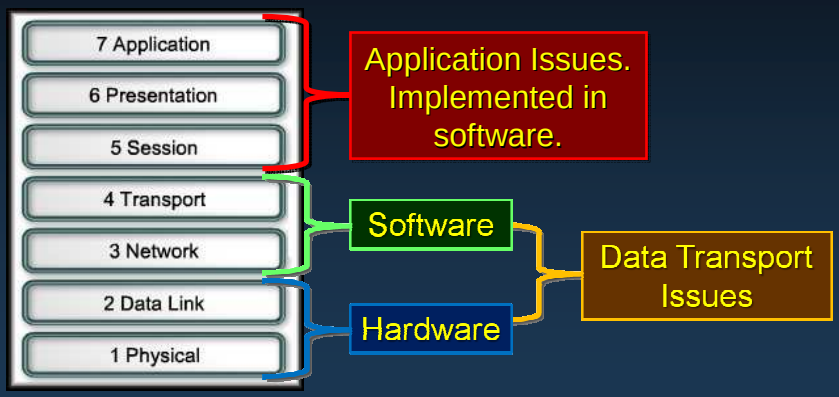
Using Layered Models for Troubleshooting

- 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.



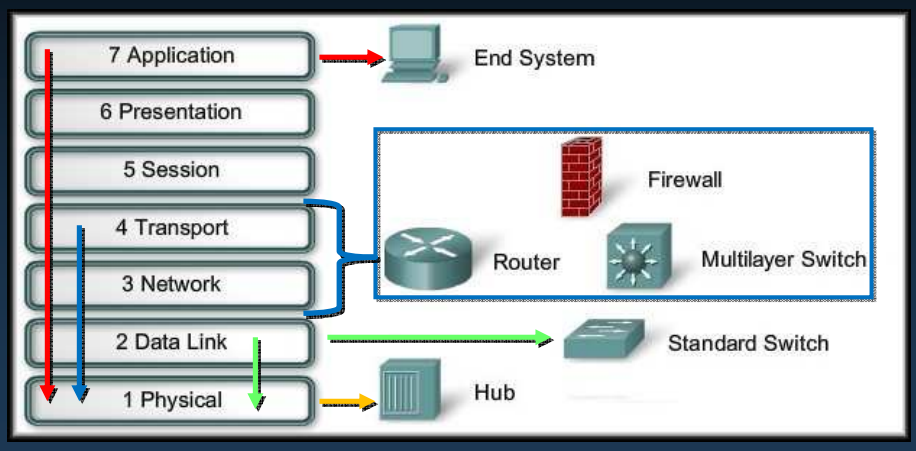
Using Layered Models for Troubleshooting

- OSI Reference Model:



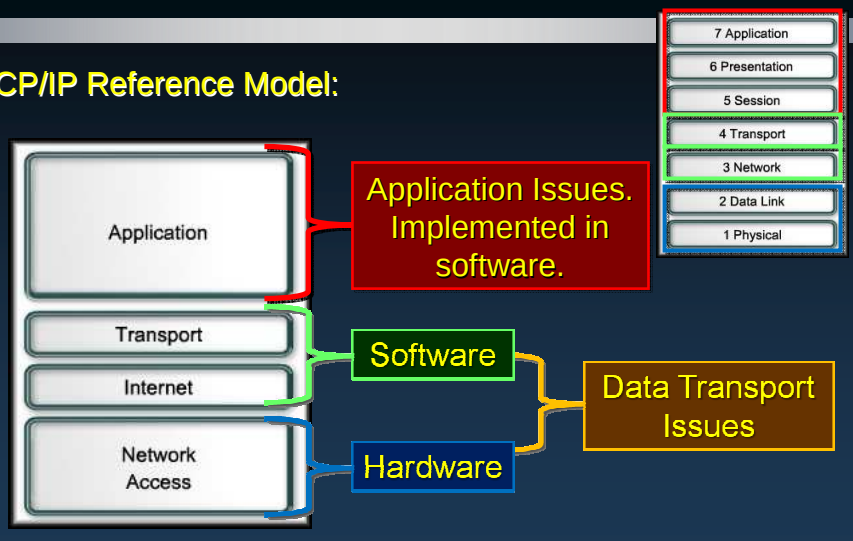
Using Layered Models for Troubleshooting

- Devices and the OSI Model:



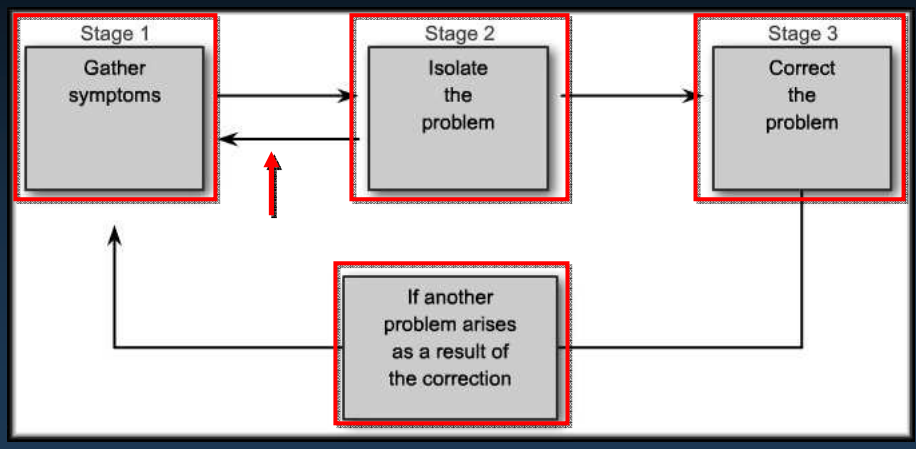
Using Layered Models for Troubleshooting

- TCP/IP Reference Model:



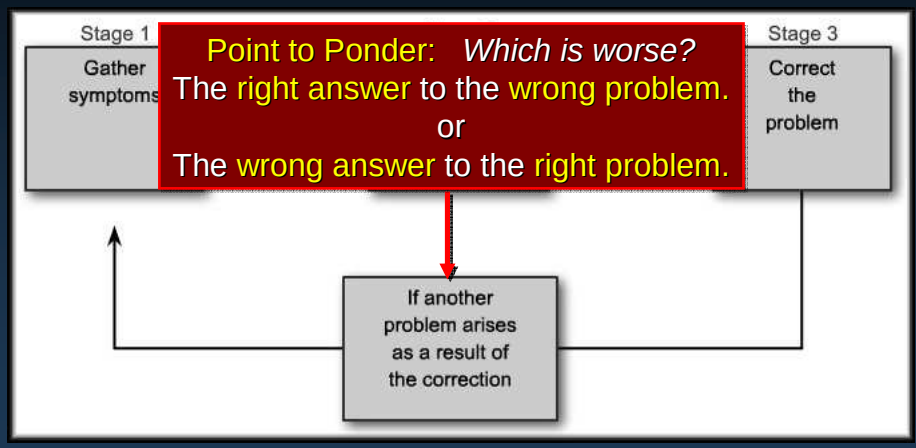
General Troubleshooting Procedures

- General troubleshooting can be broken down into 4 stages.



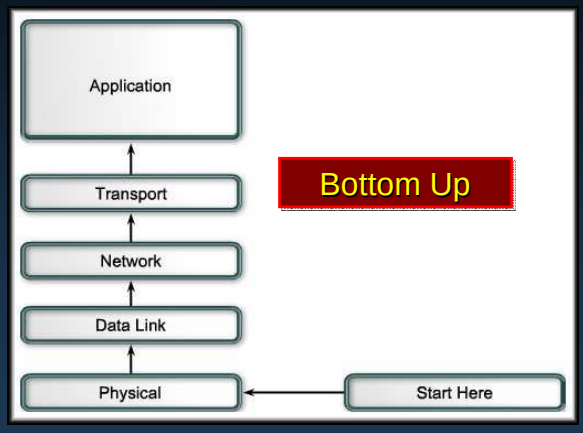
General Troubleshooting Procedures

- General troubleshooting can be broken down into **4 stages**.



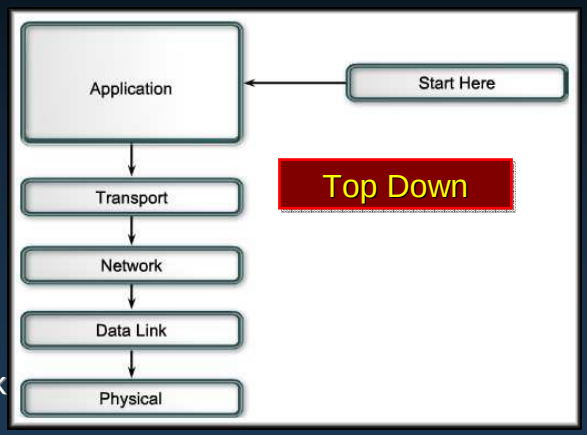
General Troubleshooting Procedures

- 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.



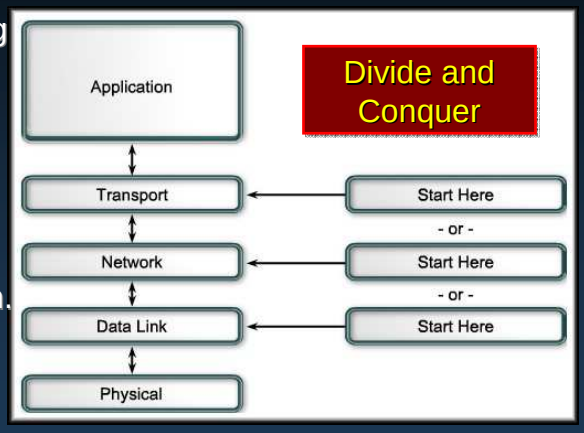
General Troubleshooting Procedures

- 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.



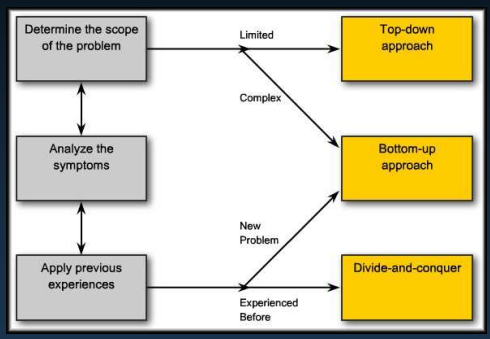
General Troubleshooting Procedures

- 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.



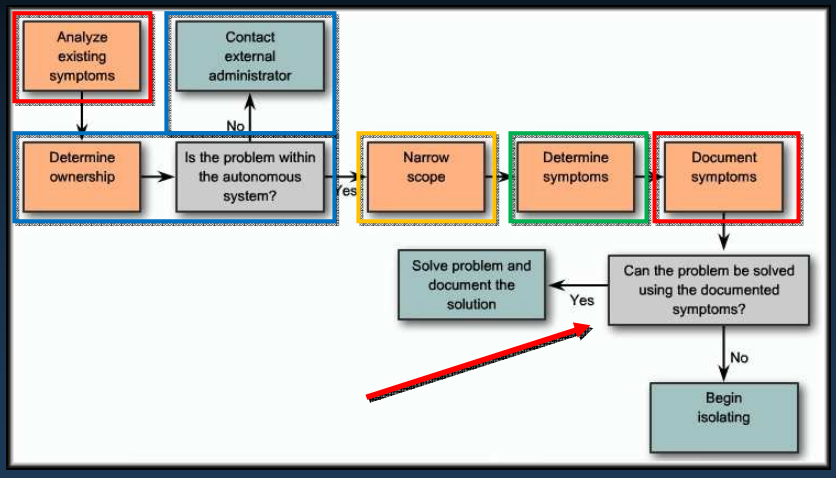
General Troubleshooting Procedures

- 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:



General Troubleshooting Procedures

- Gathering Symptoms: Useful troubleshooting commands.

Command	Description
ping *{host | ip-address}*	Sends an echo request packet to an address, then waits for a reply. The *host | ip-address* variable is the IP alias or IP address of the target system.
traceroute *{destination}*	Identifies the path a packet takes through the networks. The destination variable is the hostname or IP address of the target system.
telnet *{host | ip-address}*	Connects to an IP address using the Telnet application.
show ip interface brief	Displays a summary of the status of all interfaces on a device.
show ip route	Displays the current state of the IP routing table.
show running-config interface	Displays contents of currently running configuration file for a particular interface.
[no] debug ?	Displays a list of options for enabling or disabling debugging events on a device.
show protocols	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol.

General Troubleshooting Procedures

- Questioning Users:

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

General Troubleshooting Procedures

- Questioning Users:
  - 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.

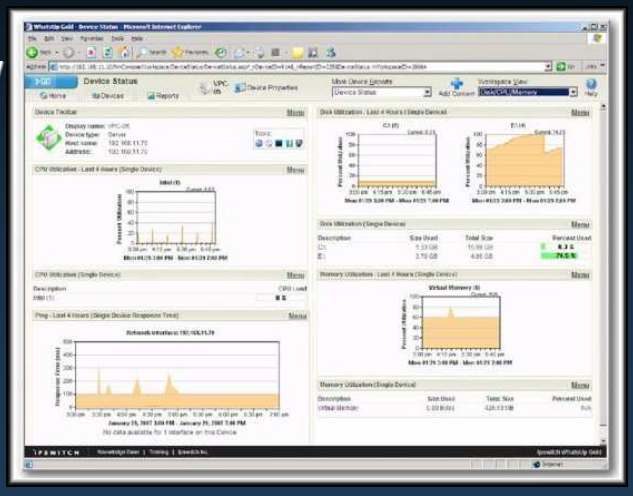
Point to Ponder: *Which is worse?*
The right answer to the wrong question.
or
The wrong answer to the right

Troubleshooting Tools

- 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.

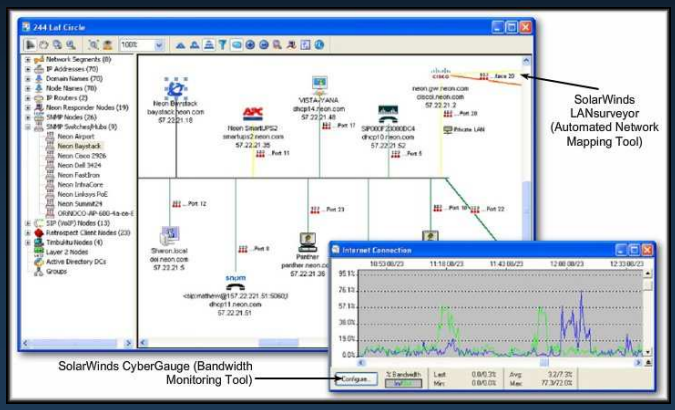


Software Troubleshooting Tools

- **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.

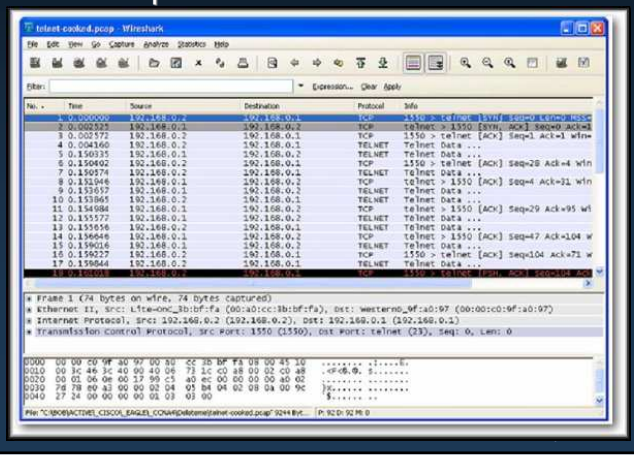
Software Troubleshooting Tools

- **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.

Fluke 179 Digital Multimeter

Hardware Troubleshooting Tools

- Cable Testers:
  - Cabling testers an be used to detect broken wires, crossed-over wiring, shorted connections and improperly paired connections.


Fluke Networks LinkRunner Pro Tester

Fluke Networks CableIQ Qualification Tester

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.

Fluke Networks DTX Cable Analyzer

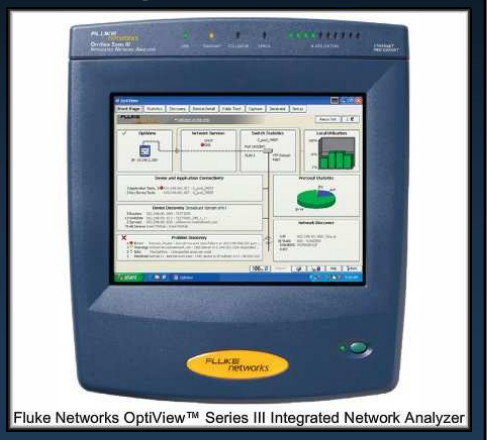
Hardware Troubleshooting Tools

- 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.

Fluke Networks OptiView™ Series III Integrated Network Analyzer

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.



Fluke Networks OptiView™ Series III Integrated Network Analyzer