NETWORK CONCEPTS

1.8 Implement the following network troubleshooting methodology:

Network Troubleshooting Procedure

1. Establish the symptoms.
2. Identify the affected area.
3. Establish what has changed.
4. Select the most probable cause.
5. Implement a solution.
6. Test the result.
7. Recognize the potential effects of the solution.
8. Document the solution.

Establish the Symptoms

- Determine exactly what is going wrong, and note the effect of the problem on the network.
- Assign a priority to the problem.
- In a large network environment, it is essential to establish a system of priorities that dictate which calls get addressed first.
- Most often, the severity of the problem determines who gets attention first.

Rules for Establishing Priorities

- Shared resources take precedence over individual resources.
- Network-wide problems take precedence over workgroup or departmental problems.
- Departmental issues should be rated according to the function of the department.
- System-wide problems take precedence over application problems.

Identify the Affected Area

- See if the problem can be duplicated.
- Network problems that you can easily duplicate are far easier to fix, primarily because you can easily test to see if your solution was successful.
- Having the user reproduce the problem can sometimes lead to the solution.
- If the problem can be duplicated, you can start determining the actual source of the problem

Establish What Has Changed

- When a computer or other network component that used to work properly now does not work, some change has probably occurred.
- Major changes, such as the installation of new hardware or software, are obvious possible causes of the problem.
- Tracking down the source of a networking problem can often be a form of detective work, and learning to "interrogate" your "suspects"

Select the Most Probable Cause

- Follow this axiom: when you hear hoofbeats, think horses, not zebras.
- When you look for possible causes of a problem, start with the obvious first.
- Work methodically and document everything you check so that you do not duplicate your efforts.

Implement a Solution

- After you have isolated the problem, determine if it is caused by hardware or software.
- If it is a hardware problem, you might replace the faulty unit or use an alternate.
  - Example: for a communication problem, you might replace network cables until you find one that is faulty.
  - Example: if the problem is in a server, you can replace components until you

Test the Results

- After you resolve the problem, you should return to the beginning of the process and repeat the task that originally caused the problem.
- If the problem no longer occurs, you should test the other functions related to the changes you made to ensure that fixing one problem has not created another.
- Repeat the procedures you used to duplicate the problem exactly, to ensure that the

Document the Solution

- Begin documenting your actions as soon as the user calls for help.
- A well-organized support organization uses a system to register each problem call as a trouble ticket that eventually contains
  - A complete record of the problem
  - The steps taken to isolate and resolve the problem
- A support organization often operates by using tiers.
  - Calls come in to the first tier.
  - If the problem is complex or the first-tier technician cannot resolve it, the call is escalated to the second

Summary

- Identifying network components
  - Computers have a variety of ports, some of which are implemented by the motherboard and others by expansion cards.
  - Computers use many different types of connectors fortheir various interfaces, and in some cases the same connector type can provide different functions

Software troubleshooting tools

- The Eight Steps
- ARP
- IPconfig
- Netstat
- Nbtstat
- Ping
- Tracert
- Traceroute
- MTR
- Nslookup
- -dig
- -host
- -route

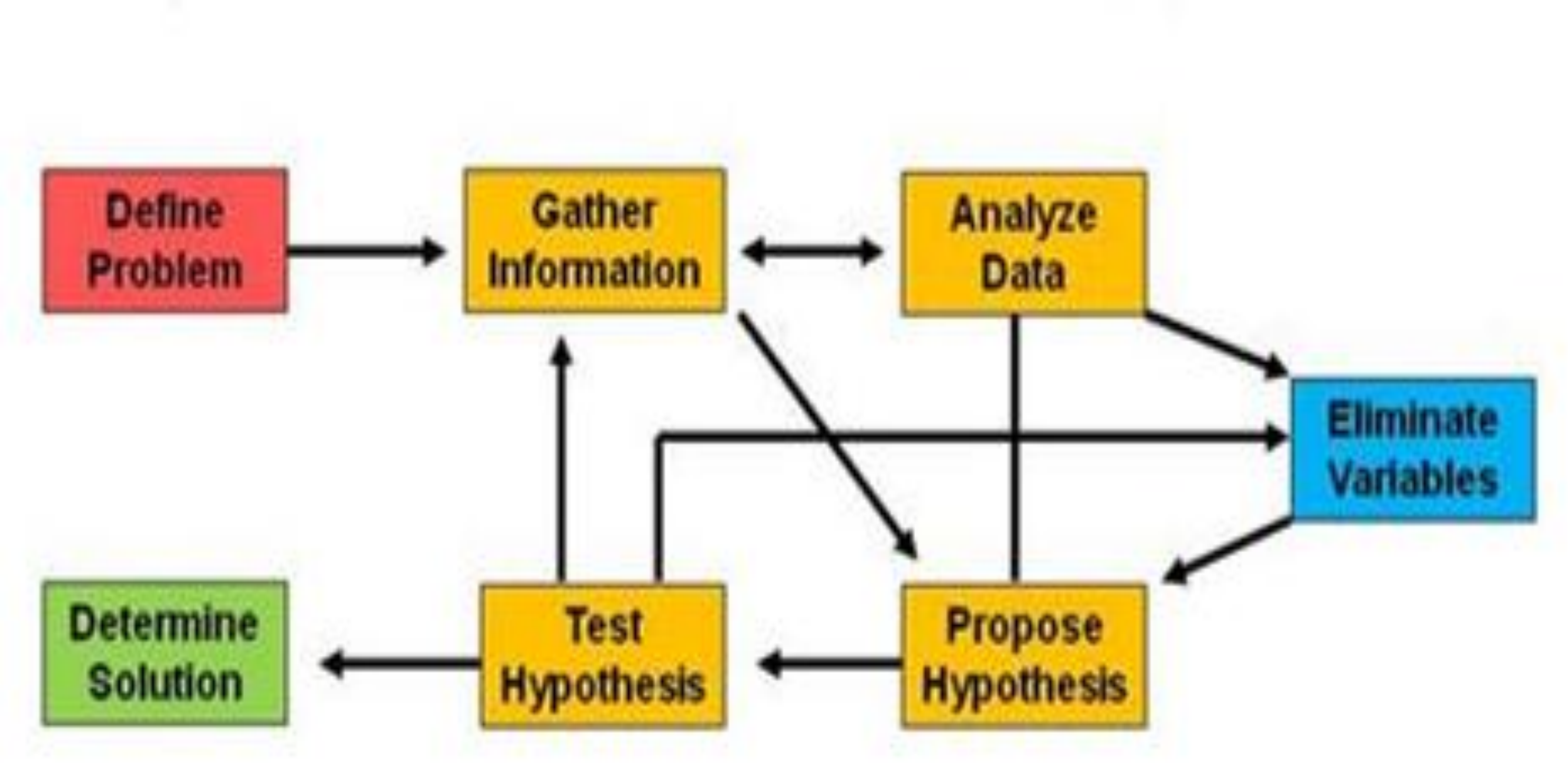
Troubleshooting

- The process of solving a problem or determining an issue.
- Troubleshooting often involves the process of elimination, where a technician will follow a set of steps in order to determine the problem or resolve the problem.

Troubleshooting

- It is intended to be independent from the document processing system used. The aim is to achieve accurate documentation from life cycle to control.

Troubleshooting



Troubleshooting

- One of the skills a network administrator must have is the ability to effectively troubleshoot network problems.
- To emphasize the importance of network troubleshooting, Cisco has dedicated an entire exam to the topic as part of the Cisco Certified Network Professional (CCNP) certification.

Troubleshooting

- **The eight steps**

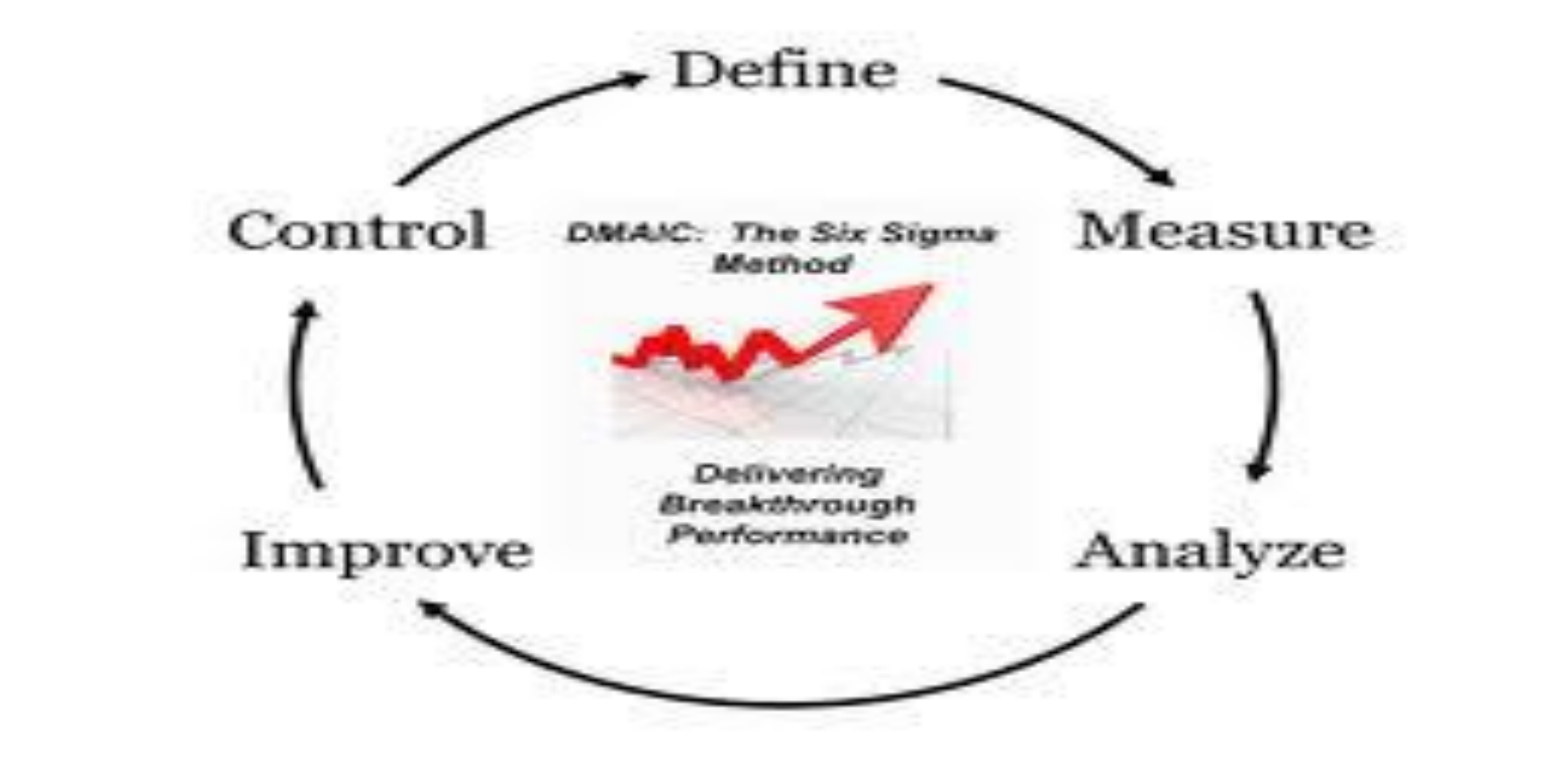
  The most important part of troubleshooting any problem is to divide the tasks of problem resolution into a systematic process of elimination.

  - Define the problem.
  - Gather detailed information.
  - Consider probable cause for the failure.

Troubleshooting

- Devise a plan to solve the problem.
- Implement the plan.
- Observe the results of the implementation.
- Repeat the process if the plan does not resolve the problem.
- Document the changes made to solve the problem.

Troubleshooting


Define
Measure
Analyze
Improve
Control
DMAIC: The Six Sigma Method
Delivering Breakthrough Performance

Troubleshooting

- Using the Scientific Method when troubleshooting may not be the swiftest path to a resolution.
- But it is the most certain path to resolving complex problems and finding a permanent fix.
- The Scientific Method can be applied to any troubleshooting situation.

Troubleshooting

- Troubleshooting problem analysis and root cause determination require patience, determination, and experience.

- It is important to fully investigate the problem and collect all relevant data in order to begin troubleshooting on the correct path.

Troubleshooting

View the ARP table - ARP (windows)

- Displays and modifies entries in the Address Resolution Protocol (ARP) cache.

- Which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses.

Troubleshooting

View IP configuration Information

- IPconfig(windows 2000 and higher)

- In computing, ipconfig (internet protocol configuration) in Microsoft Windows is a console application that displays all current TCP/IP network configuration.

- Values can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings

Troubleshooting

View IP configuration Information

- IPconfig(Linux)

- Ifconfig is a system administration utility in Unix-like operating systems for network interface configuration.

- The utility is a command line interface tool and is also used in the system startup scripts of many operating systems.

Troubleshooting

View IP configuration Information

- IP Configuration Protocol is used by computers for requesting Internet Protocol parameters,such as an IP address from a network server.

- The protocol operates based on the client-server model.

- Most residential network routers receive a globally unique IP address within the provider network.

Troubleshooting

View IP configuration Information

- When a computer or other networked device connects to a network, its DHCP client software in the operating system sends a broadcast query requesting necessary information.

- Any DHCP server on the network may service the request.

Troubleshooting

View IP and Routing Statistics

- Netstat (Windows)

- Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing)

- Routing tables and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics

Troubleshooting

View IP and Routing Statistics

- Netstat (Windows)

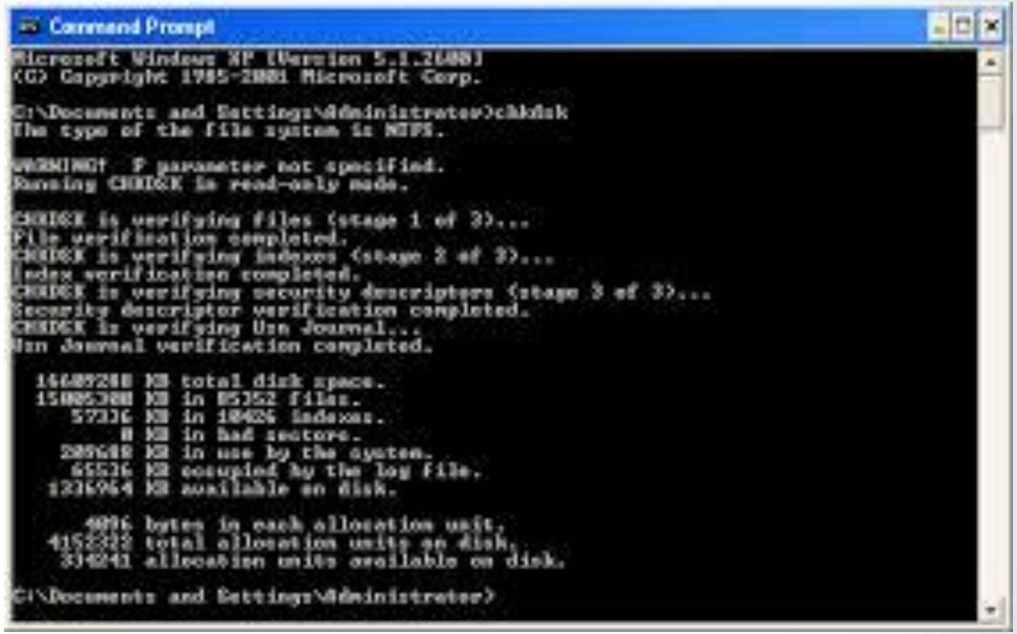
- Is available on Unix-like operating systems including OS X, Linux, Solaris, and BSD.

- Is available on Windows NT-based operating systems including Windows XP, Windows Vista, Windows 7 and Windows 8.

View IP and Routing Statistics

- Netstat (Windows)

- It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.



Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>chkdsk
The type of the file system is NTFS.

WARNING!  F parameter not specified.
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 3)...
Index verification completed.
CHKDSK is verifying security descriptors (stage 3 of 3)...
Security descriptor verification completed.
CHKDSK is verifying Usn Journal...
Usn Journal verification completed.

  16689288 KB total disk space.
  15005308 KB in 85352 files.
     57336 KB in 10426 indexes.
         0 KB in bad sectors.
    209648 KB in use by the system.
     65536 KB occupied by the log file.
   1336964 KB available on disk.

      4096 bytes in each allocation unit.
   4152322 total allocation units on disk.
    334241 allocation units available on disk.

C:\Documents and Settings\Administrator>
```

Troubleshooting

View NetBIOS over TCP/IP Information

- Nbtstat (Windows)

- NetBIOS over TCP/IP (NBT, or sometimes NetBT) is a networking protocol.
- It allows legacy computer applications relying on the NetBIOS API to be used on modern TCP/IP networks.
- When properly configured, NBT allows those applications to be run on large TCP/IP networks.

View NetBIOS over TCP/IP Information
- Nbtstat (Windows)

- In NetBIOS, each participant must register on the network using a unique name of at most 15 characters.

- It is interesting to note that NBNS is one of the first proper dynamic peer-to-peer distributed name registration services.

Troubleshooting

Test host to host connectivity

- Ping

- Ping is a networking utility program or a tool to test if a particular host is reachable.

- It is a diagnostic that checks if your computer is connected to a server.

Troubleshooting

Test host to host connectivity

- Ping

- A ping test is a method of checking if the computer is connected to a network.

- It also determines the latency or delay between two computers. It is used to ensure that a host computer, which your computer tries to access, is operating.

Troubleshooting

Identify the path between two hosts

- Tracert (Windows)

- Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP).

- Echo Request messages the destination with incrementally increasing Time to Live (TTL) field values.

Troubleshooting

Identify the path between two hosts

- Tracert (Windows)

- The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination.

Troubleshooting

Identify the path between two hosts

- Tracert (Windows)

- The near-side interface is the interface of the router that is closest to the sending host in the path.

- Used without parameters, Tracert displays help.

- This can speed up the display of Tracert results

Troubleshooting

Identify the path between two hosts

- Traceroute (Linux)

- The Internet is a large and complex aggregation of network hardware, connected together by gateways.

- Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult.

Troubleshooting

Identify the path between two hosts

- MTR (Linux)

- MTR combines the functionality of the traceroute and ping programs in a single network diagnostic tool.

- As MTR starts, it investigates the network connection between the host MTR runs on and HOSTNAME.

Troubleshooting

Test host to host connectivity using ARP

- ARPing (Linux)

- Ends IP and/or ARP pings the ARPing utility sends ARP and/or ICMP requests to the specified host and displays the replies.
- The host may be specified by its hostname, its IP address, or its MAC address.
- This program is only able to run as root. Make it setuid if you like.

Troubleshooting

Test Name Resolution

- Nslookup (windows and linux)

- Nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

Troubleshooting

Test Name Resolution

- dig (linux,this is the preferred tool on linux)

- dig (domain internet groper): A tool for system administrators, dig sends DNS queries at the target server and decodes the replies.

- It is part of the BIND DNS server from the Internet Software Consortium.

Troubleshooting

Test Name Resolution

- dig (Linux, this is the preferred tool on Linux)

- It is also popular with hackers because it allows fine-tuned queries to be crafted.

- Key point: Hackers like to run the following command in order to query the version of BIND:

Troubleshooting

Test Name Resolution

- host (Linux)

- The purpose of assigning names to IP numbers is to make them easier for people to remember.

- In reality, an IP address identifies a network interface associated with a device such as a network card.

Troubleshooting

View and modify the routing table

- route

- Route is a command used to view and manipulate the TCP/IP routing table in both Unix-like and Microsoft Windows operating systems.

- Manual manipulation of the routing table is characteristic of static routing.

Troubleshooting

View and modify the routing table

- route

- In Linux distributions based on 2.2.x Linux kernels.
- The ipconfig and route commands are operated together to connect a computer to a network.
- Used to define routes between computer networks.