



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Troubleshooting Guideline

Cisco | Networking Academy[®]
Mind Wide Open[™]

Task 1: Read this document. This document contains basic troubleshooting techniques/ steps/ commands.

Task 2: (Assignment) Complete and submit: (Submission via Moodle:- 21/06/2021)

Based on your acquired skills from all the lab works, complete the following.

Complete the Packet Tracer Task and submit. (File is available in Moodle)

LAB Objectives

Understand troubleshooting methods.

Requirements

- Use Packet Tracer

Troubleshooting

Introduction:

Troubleshooting is the process of identifying, locating, and correcting problems. Documentation is part of the troubleshooting process and should include the following:

- o ***A detailed description of the problem***
- o ***Steps taken to determine the cause of the problem***
- o ***Steps used to correct the problem***

When gathering information, talk to the user and try to determine how much of the network is affected by the issue.

To find out the nature of problem: *End-user reports and Problem verification report*

Always check the equipment details:

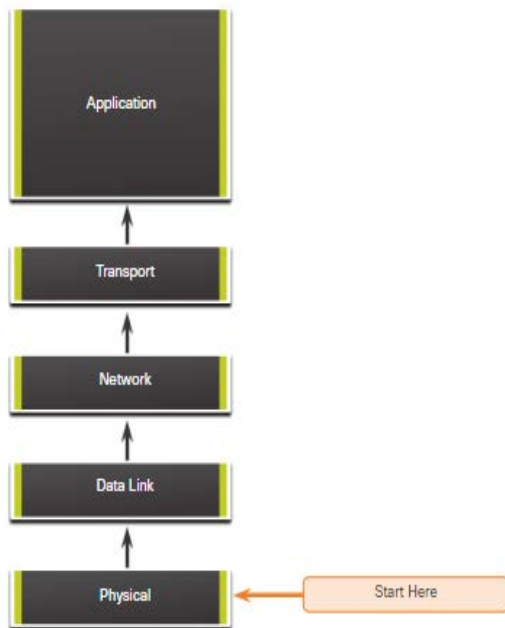
- o Manufacturer, Make / model, Firmware version
- o Operating system version, Ownership / warranty information

Check configuration and topology

- o Physical and logical topology
- o Configuration files and Log files

Check previous troubleshooting steps taken and results achieved.

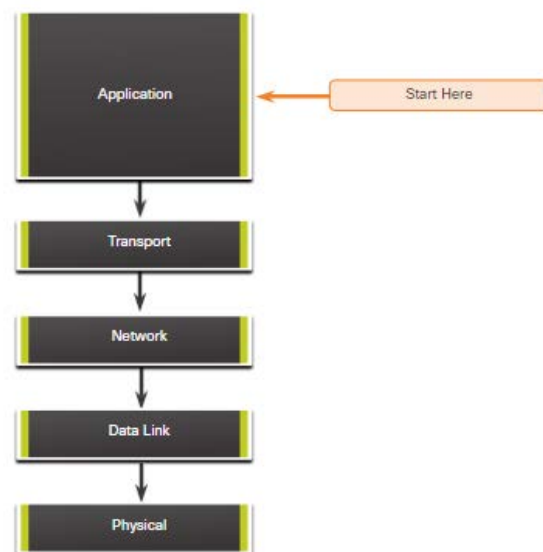
Bottom up Approach



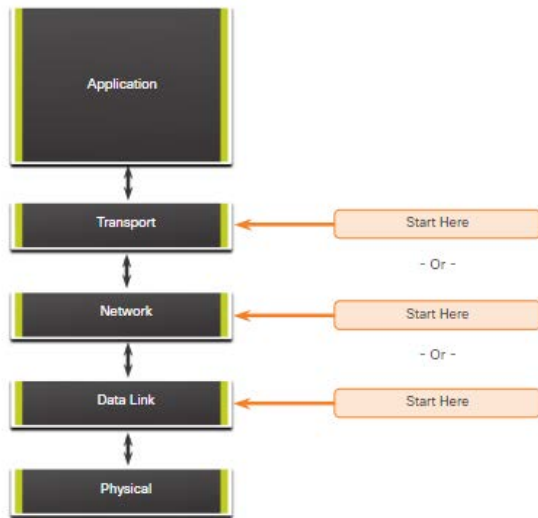
1. Start with the physical layer and the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified.
2. A good approach to use when the problem is suspected to be a physical one.
3. Most networking problems reside at the lower levels, so implementing the bottom-up approach is often effective.
4. A disadvantage is it requires that you check every device and interface on the network until the possible cause of the problem is found. It is also difficult to determine which devices to start examining first.

Top Down Approach

1. Start with the end-user applications and move down through the OSI layers.
2. End-user applications of an end system are tested before tackling the more specific networking pieces.
3. Use this approach for simpler problems or when you think the problem is with a piece of software. The challenge is to determine which application to start examining first.
4. Disadvantage is it requires checking every network application until the possible cause of the problem is found.



Divide and Conquer Method



1. Select a layer and test in both directions.
2. Start by collecting user experiences of the problem, document the symptoms and then, using that information, make an informed guess as to which OSI layer to start your investigation.
3. When a layer is verified to be functioning properly, it can be assumed that the layers below it are functioning.
4. **Work up the OSI layers.** If an OSI layer is not functioning properly, the administrator can work down the OSI layer

model. For example, if users cannot access the web server, but they can ping the server, then the problem is above Layer 3. If pinging the server is unsuccessful, then the problem is likely at a lower OSI layer.

Define Problem	Type of Problem	Troubleshooting Method
Determine the type of problem.	Software-oriented	Top-Down Method
Analyze the symptoms.	Hardware/Cable-oriented or Complex	Bottom-Up Method
Apply previous experiences.	New Problem	Divide-and-Conquer Method
	Experienced Before	

Take the time to select the most effective network troubleshooting method. Software problems are often solved using a top-down approach. Hardware-based problems are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method. Otherwise, the bottom-up approach may be used.

Common Problems

A large proportion of networking problems are related to physical components or problems with the physical layer. Physical problems are concerned mainly with the hardware aspects of computers and networking devices, and the cables that interconnect them. Physical problems do not include the logical (software) configuration of devices.

Some of the more common Layer 1 problems include the following:

- ✓ Device receiving power? (turned off or unplugged)
- ✓ Loose network cable connection
- ✓ Incorrect cable type
- ✓ Faulty network cable
- ✓ Faulty wireless access point

Ensure there are no errors showing on any LEDs that display the connectivity status. If on-site, visually inspect all network cabling and reconnect cables to ensure a proper connection. If using wireless, verify that the device is operational and settings are configured correctly.

Your senses could help!!! To find out if

- ✓ Cables which are not connected
- ✓ Cables connected to the wrong port
- ✓ Loose cable connections
- ✓ Damaged cables and connectors
- ✓ Use of the wrong type of cable
- ✓ View condition and function of various network devices with LEDs.
- ✓ Feel for overheated components as well as to detect mechanical problems with devices such as cooling fans.
- ✓ Devices create a small vibration in the component that can be detected using touch.
- ✓ Smell can detect components which are overheating.
- ✓ Burning insulation or components is very distinct.
- ✓ Taste is directly related to the sense of smell because both use the same receptors such as tasting the acridness of something burning.



- ✓ Used to detect major problems such as electrical issues and the proper operation of cooling fans and disk drives.
- ✓ All devices have characteristic sounds and any change from the normal sounds usually indicate a problem of some sort.
- ✓ Examine LEDs (link lights) that indicate the current state or activity of a piece of equipment or connection.

Note: The exact configuration and meaning of LEDs varies between manufacturers and devices.

- ✓ Typical LEDs include ones for power, system, WLAN, wired ports, and internet (labeled WAN in the figure), USB, and Quick Security Setup (QSS, also known as Wi-Fi Protected Setup [WPS] that is a security risk).
- ✓ A **normal condition** is for these LEDs to flash indicating that traffic is flowing through the port.
- ✓ A **solid green light** typically indicates that a device is plugged into the port, but no traffic is flowing.

No light typically indicates one or more of the following:

- ✓ Nothing is plugged into the port.
- ✓ There is an issue with the wired or wireless connection.
- ✓ A device or port has failed.
- ✓ There is a cabling issue.
- ✓ The wireless router is improperly configured, for example, a port was administratively shut down.
- ✓ The wireless router has a hardware fault.
- ✓ The device does not have power.

Troubleshooting Commands

Most of these utilities are provided by the operating system as command line interface (CLI) commands. The syntax for the commands may vary between operating systems.

Some of the available utilities include:

Ipconfig

- ✓ Displays IP configuration information.
- ✓ **ipconfig**: Used to display IP configuration information such as IP address, subnet mask, and default gateway
- ✓ **ipconfig /all**: Includes MAC address, DNS server(s), and DHCP information
- ✓ **/release** - used to let go of the current DHCP bindings
- ✓ **/renew** - used to obtain new DHCP bindings

```
C:\> ipconfig/release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
    Default Gateway . . . . . :
```

```
C:\> ipconfig/renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : lan
    Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
    IPv4 Address. . . . . : 10.10.10.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.1
```

ping (Most used network utility)

- ✓ Tests whether or not network devices are reachable
- ✓ Echo request message used to send the packet
- ✓ Echo reply verifies connectivity
- ✓ Request timed out or general failure is an indication of failure
- ✓ A ping to a name like www.cisco.com verifies not only connectivity, but DNS as well.
- ✓ If neither a ping to an IP address, nor a ping to the name is successful, then network connectivity along the path to the destination is most likely the problem.
- ✓ **Try to ping the default gateway.** *If the ping to the default gateway is successful, the problem is not local. If the ping to the default gateway fails, the problem resides on the local network.*

Note: A ping may fail due to the firewall on the sending or receiving device, or a router along the path that is blocking the pings.

✓

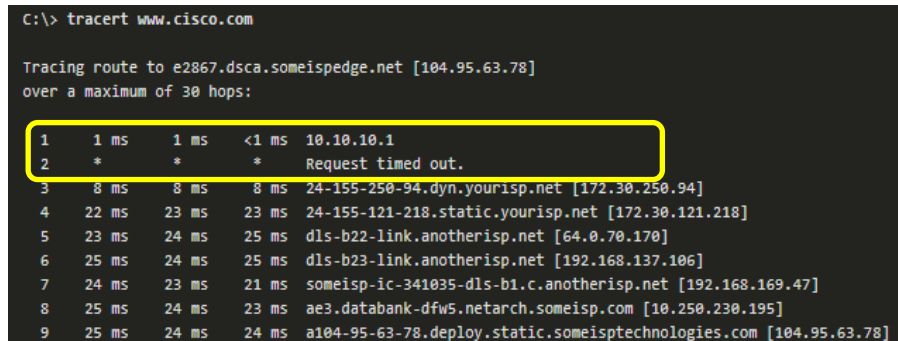
netstat - Displays network connections.

- ✓ The netstat command is used to verify active TCP connections and lists the protocol in use, the local address and port number, the foreign address and port number, and the state of the connection.
- ✓ Unexplained TCP connections can pose a major security threat because they can indicate that something or someone is connected to the local host.
- ✓ Unnecessary TCP connections can consume valuable system resources thus slowing down the host.

tracert

- ✓ The **ping** command does not indicate where a connection drops if it fails. Use **tracert** (Microsoft and Linux) or **tracert** (Cisco and other OSES) to provide connectivity information about the path a packet takes to reach the destination and about every router (hop) along the way.
- ✓ Indicates how long a packet takes to get from the source to each hop and back (round trip time).
- ✓ Used to identify where a packet may have been lost or delayed due to bottlenecks or slowdowns.

Note: Notice in the output here the 2nd hop failed. This is most likely due to a firewall configuration on that device which does not permit responding packets from the **tracert** command.



```
C:\> tracert www.cisco.com

Tracing route to e2867.dsca.someispedge.net [104.95.63.78]
over a maximum of 30 hops:

  0  1 ms    1 ms    <1 ms   10.10.10.1
  1  *        *        *       Request timed out.
  2  8 ms    8 ms    8 ms    24-155-250-94.dyn.yourisp.net [172.30.250.94]
  3  22 ms   23 ms   23 ms    24-155-121-218.static.yourisp.net [172.30.121.218]
  4  23 ms   24 ms   25 ms    dls-b22-link.anotherisp.net [64.0.70.170]
  5  25 ms   24 ms   25 ms    dls-b23-link.anotherisp.net [192.168.137.106]
  6  24 ms   23 ms   21 ms    someisp-ic-341035-dls-b1.c.anotherisp.net [192.168.169.47]
  7  25 ms   24 ms   23 ms    ae3.databank-dfw5.netarch.someisp.com [10.250.230.195]
  8  25 ms   24 ms   24 ms    a104-95-63-78.deploy.static.someisptechnologies.com [104.95.63.78]
```

However, the device does forward the packets to the next hop.

nslookup

- ✓ When a network device is being configured, one or more DNS server addresses are provided that the DNS client can use for name resolution.
- ✓ Usually the ISP provides the addresses to use for the DNS servers.
- ✓ When a user application requests to connect to a remote device by name, the requesting DNS client queries the name server to resolve the name to a numeric address.

- ✓ Nslookup allows the user to manually query the name servers to resolve a given host name.
- ✓ Can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.
- ✓ When issued, the default DNS server configured for your host is displayed. The name of a host or domain can be entered at the **nslookup** prompt.
- ✓ Directly queries the name server for information on a destination domain.

Learnings from tutorials done so far:

- ✓ Build a Simple Network
- ✓ Understand and configure IP Address
- ✓ Use Ping/ Trace route Utility to check the connection status
- ✓ Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.
- ✓ Analyze a MAC address to determine the manufacturer.
- ✓ Analyze the Wired and Wireless Network connection.
- ✓ Analyze Address Resolution Protocol (ARP).
- ✓ Connect to a Wireless Router and configure the basic settings in a wireless router
- ✓ Use nslookup command to understand the url to ip conversion
- ✓ Build a Small Network, do basic configurations and establish a successful network connectivity.
- ✓ Use simulated/real time environment in packet tracer.
- ✓ Configure Switches and Routers: IP Interfaces, Line Configurations, Passwords
- ✓ Troubleshoot a simple network.