Hardware and Network Servicing Level III

Based on August, 2011, Version3 Occupational Standard (OS)

Module Title: **Identifying and Resolve Network Problems**

LG Code : **EIS HNS3 M08 1220 LO (1-3) LG (27-29)**

TTLM Code : **EIS HNS3 TTLM08 1220v1**

December 2020

Bishoftu, Ethiopia

Contents **Page**

LG #27	LO # 1- Implement regular network monitoring
Instruction sheet	

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Setting up an appropriate log to monitor network activity
- Using network tools to benchmark the network and to establishing a reference point
- Reviewing documents and logs regularly to facilitate network tuning
- Making recommendations to management for additional network resources

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Set up log to monitor network activity
- Use network tools to benchmark the network and to establishing a reference point
- Review documents and logs regularly to facilitate network tuning
- Make recommendations to management for additional network resources

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If your performance is satisfactory proceed to the next learning guide,

Information sheet 1. Setting up an appropriate log to monitor network activity

Network monitoring refers to the practice of overseeing the operation of a computer network using specialized management software tools. Network monitoring systems are used to ensure availability and overall performance of computers (hosts) and network services. These systems are typically employed on larger scale corporate and university IT networks.

Key Features in Network Monitoring

A network monitoring system is capable of detecting and reporting failures of devices or connections. It normally measures the processor (CPU) utilization of hosts, the network bandwidth utilization of links, and other aspects of operation. It will often send messages (sometimes called watchdog messages) over the network to each host to verify it is responsive to requests. When failures, unacceptably slow response, or other unexpected behaviour is detected, these systems send additional messages called *alerts* to designated locations (such as a management server, an email address, or a phone number) to notify system administrators.

The term **network monitoring** describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

Network Monitoring Tools

Networks are the fundamentals behind businesses worldwide. It plays a pivotal role in serving your employees for administrative purposes and your clients across the continents. The networks help you keep information in a centralized location - accessible to those who need and restrict every other inbound request. So how do you provide continuous top-notch end user experience and maintain your rapidly evolving network? Only by monitoring the availability, health, and performance of your networks over time.

The need for network monitor tools

The importance of networks in a business environment is immense, employing sophisticated, network performance monitoring tools is vital. With a network monitoring solution, you can avoid potential network pitfalls.

- Network monitoring solutions aid IT admins by:
  - ✓ Providing complete visibility into the IT infrastructure
  - ✓ Keeping them updated of the network's state in real time
  - ✓ Identifying issues before the end users are affected
  - ✓ Tracking and troubleshooting performance issues early

Apart from the above, with the help of network monitoring systems, admins can now make more informed IT decisions which help in improving business continuity.

- **Requirements of a network monitoring tool**

While selecting a network monitoring tool for your IT environment, it is important to weigh in your current requirements and also your future needs. Some of the essential elements that a network monitoring tool requires are:

- ✓ Real time monitoring
- ✓ Comprehensive monitoring capabilities
- ✓ Scalability
- ✓ Automation
- ✓ User Management

Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools -- especially when it comes to measuring accurate end-to-end response time because they limit round trip visibility.

Status request failures - such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved - usually produce an action from the monitoring system. These actions vary - an alarm may be sent to the resident system admin, automatic fail over systems may be activated to remove the troubled server from duty until it can be repaired.

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

1. Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
2. Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
3. Maintenance is concerned with performing repairs and upgrades for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
4. Provisioning is concerned with configuring resources in the network to support a given service.
5. Set appropriate log to monitor and notify problems

Self-Check1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

I. Choose the best answer

1._____ is capable of detecting and reporting failures of devices or connections

A. network monitoring system B. network tools C. monitoring tool D) none

2. All are the essential elements that a network monitoring tool except one

A. scalability B. Moral C. Automation D. user management

Part II fill the blank space

3. Write at least two network monitoring solutions aid IT admins

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____ Rating:

Information sheet 2. Setting up an appropriate log to a management Information Base

Management Information Base

MIB stands for Management Information Base, is a hierarchical database that defines the information that an SNMP management system can request from an agent using Simple Network Management Protocol. A management information base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol. The format of the Management information base is defined as part of the SNMP.

How MIB Works

A Management Information Base is a collection of manageable network objects. These objects are a logical representation of physical networking components that are SNMP-enabled (such as computers, hubs, routers, switches, and networking software). MIBs contain information about the configuration of these networking components, such as the version of the software running on the component, the IP address or port number, and the amount of available disk space for storage. MIBs function as a kind of directory containing the logical names of the network resources and their configuration parameters that are managed by SNMP.

Because every MIB is a member of the MIB hierarchy, you can uniquely identify a MIB for each network component. The name is represented using a standard dotted naming system.

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in provided space

Part II fill the blank space

1. _____ is a collection of manageable network objects
2. SNMP stands for _____

3. List at least three components of physical network (3 point)

_____
_____
_____
_____

Note*:* Satisfactory 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating:

Information sheet 3. Use network tools to establishing a reference point

Network Tools

Network tools and utilities enable you to manage your networks with greater efficiency and less network troubleshooting overhead. These tools aid in efficiently detecting network issues, diagnosing their cause and locality, and mitigating and resolving them. This helps ensure the stability of your network environment to keep users from the hassles that come with device connectivity issues. These network tools for Windows and Linux, like SNMP Ping and DNS Resolver, aid in validating network sources, addresses, devices, and more.

Network tools have become a network admin's go-to solution for efficiently troubleshooting network issues. With networks continually evolving, generic network tools and utilities are no longer sufficient for carrying out network diagnosis and debugging. Network admins have started shifting towards ad hoc network tools and utilities to manage complex network infrastructures. Network tools and utilities come in handy when conducting network monitoring and reconnaissance. These reliable network tools ensure effective network monitoring, diagnosis, and management, each network tool aiding a specific network operation.

This diverse tool set includes free network utility tools under the following categories:

- Network Discovery tools
- Network Diagnostic tools
- Address Management tools
- SNMP tools
- System Utilities

Network Tools & Utilities

Network tools aid in various network operations and inspections that has to be carried out to identify the cause of a specific network issue.

Network tools includes

Network Discovery tools: Get a more comprehensive view of your network with free network discovery tools, such as Ping and SNMP Ping. The network discovery tools efficiently discovers your network resources without any additional requirements by integrating with your existing network environment.

Network Diagnostic tools: Diagnose and troubleshoot network issues. Resolve network problems such as issues with network connectivity, health, latency, and so on with a network tool like Trace Route.

SNMP Tools: Efficiently monitor your SNMP-enabled devices with tools such as MIB Module Viewer, MIB Node Viewer, and Community Checker.

System Utilities: Get detailed insight and monitor your system information, CPU, and more with other system utilities.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Choose the best answer from the given alternatives

1. What command would be used to establish network connectivity? (2point)

   A. IPCONFIG /all B. IPCONFIG /release C. IPCONFIG /renew

   D. IPCONFIG /register dns

2. Which IP address will invoke the TCP/IP loopback function? (2point)

   A. 127.0.0.1 B. 10.0.0.1 C. 169.192.0.1 D. 172.254.0.1

3. _____ enable you to manage your networks with greater efficiency and less network troubleshooting overhead (2point)

   A. Network Diagnostic tools B. Network tools and utilities

   C. SNMP Tools D. Address Management tools

4._____ is to translate domain names into IP Addresses, which computers can understand.

   A. DHCP B. ping

   C. DNS D. Internet Explorer web browser

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____

Rating:

Information sheet 4. Review documents and logs regularly to facilitate network tuning

- **Documentation review criteria include three areas of focus:**
  - ✓ Review is used for the "generalized" level of accuracy, that is, a high-level inspection looking for required content and for any obvious errors, omissions, or inconsistencies.
  - ✓ Study is used for the "focused" level of accuracy, that is, an inspection that includes the intent of "review" and adds a more in-depth inspection for greater evidence to support a determination of whether the document has the required content and is free of errors, omissions, and inconsistencies.
  - ✓ Analyse is used for the "detailed" level of rigor, that is, an examination that includes the intent of both "review" and "study," adding a thorough and detailed analysis for significant grounds for confidence in the determination of whether required content is present and the document is correct, complete, and consistent.

Documentation review is intended to determine the flow of information across the business process, and map how the data from the raw data sources is transformed into the ultimate information product.

- Constructing an information production flow diagram is valuable for many reasons:
  - ✓ It provides an information-centric view of the ways that business processes are executed.
  - ✓ It focuses on multiple uses of data and information across information system and business process boundaries.
  - ✓ It reduces the concentration on functional requirements in deference to enterprise data and information requirements across the organizations.
  - ✓ It documents the way that information flows across business processes and can be used to identify the best locations for inspecting data quality and identifying flaws before any business impacts can occur.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in provided space

Part II short answer

1. List at most two reasons to constructing an information production flow diagram (3 point)

   _____

   _____

   _____

   _____

2. _____ is intended to determine the flow of information across the business process, and map how the data from the raw data sources is transformed into the ultimate information product.(2point)

Note: Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____

Rating:

Information sheet 5. Make recommendations to management for additional network resources

Recommendations may be combined or, in long reports, presented in separate sections. If there are no recommendations to be made as a result of the network resources Always address limitations and suggest how they might be overcome in future network resources. Flow reversal had no significant effect compared with steady flow. Further network resources are recommended to determine the maximum achievable enhancement.

However, some general comparisons can be made between network resources in the geographical sub-region:

- size of the current collection and availability of a budget in order to maintain acquisitions;
- network resource facilities and equipment;
- level of professional training of network resource;
- significant donor funding for information activities;

Self-Check 5	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Short Answer Question

1. List at least 4 recommended network resources or devices and positively influencing multiple outcomes organization can benefit by prioritizing the actions first.

_____

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____

Rating:

LG #28	LO #2 Troubleshoot Network problems

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Addressing help desk and other support services
- Using various tools and knowledge of network topology and protocols
- Advising users and clients of progress and solutions
- Completing support documentation

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Address help desk and other support services
- Use various tools and knowledge of network topology and protocols
- Advise users and clients of progress and solutions
- Complete support documentation

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.

2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If your performance is satisfactory proceed to the next learning guide,

Information sheet 1 Addressing help desk and other support services

A **help desk** is a resource intended to provide the customer or end user with information and support related to a companies or institution's products and services. The purpose of a help desk is usually to troubleshoot problems or provide guidance about products such as computers, electronic equipment, and network devices.

Issues can arise at numerous points along the network**.** Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on. By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.

- There are many ways designed to identify network problems.
  - ✓ using tools to identify and solve network problems
  - ✓ advice users and clients on time
  - ✓ complete support documentation
- **SUPPORT SERVICES**

The term "support" refers to actions taken on behalf of users rather than those taken on equipment and systems. Support denotes activities that keep users working or help users improve the ways they work. Included under support might be such items as:

- ✓ providing "Help Desks" and other mechanisms for resolving problems and offering guidance (e.g., automated information systems and searchable frequently-asked-question (FAQ) databases)
- ✓ offering initial and ongoing training on equipment and software
- ✓ identifying external resources, including websites, consultants, and volunteers as appropriate
- ✓ integrating instruction and technology, usually through observation and personal interaction between a teacher and a technology coordinator
- ✓ integrating administration and technology, usually conducted through specialized consultants or software/systems vendors

How to Enable Event Viewer

The Windows Event Viewer allows previewing of logged events. Anytime a significant event takes place on your Windows 7 machine, a log entry is added. It is recommended to view these events through Event Viewer, even when the system if functioning properly, to get an idea of the computer's normal state. Therefore, when a problem occurs, it will be easier to identify events that are out of place. Checking the Event Viewer for logged errors can help identify and diagnose the problem.

Self-Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Short Answer Question

1. List three ways designed to identify network problems

_____

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating: _____

Information sheet 2 Using various tools and knowledge of network topology and protocols

Physical Network Topologies

A physical network topology shows the physical layout of the devices connected to the network. Knowing how devices are physically connected is necessary for troubleshooting problems at the Physical Layer, such as cabling or hardware problems.

Physical network topologies typically includes

Device types

- Models and manufacturers of devices
- Locations
- Operating system versions
- Cable types and identifiers
- Cabling endpoints

Logical Network Topologies

A logical network topology shows how data is transferred on the network. Symbols are used to represent network elements such as routers, servers, hubs, hosts, and security devices. Logical network topologies typically include;

- Device identifiers
- Static and default routes
- Interface identifiers
- WAN technologies
- Routing protocols
- IP addresses and subnet masks
- Data-link protocols

In addition to network diagrams, other tools may be needed to effectively troubleshoot network performance issues and failures.

Troubleshooting is the process of identifying, locating and correcting problems that occur. Experienced individuals often rely on instinct to troubleshoot. However, there are structured techniques that can be used to determine the most probable cause and solution.

When a problem occurs on an enterprise network, troubleshooting that problem quickly and efficiently is very important to avoid extended periods of downtime. Many different structured and unstructured problem-solving techniques are available to the network technician.

These include:

- Top-down
- Trial-and-error
- Bottom-up
- Substitution
- Divide-and-conquer

Most experienced network technicians rely on the knowledge gained from past experience and start the troubleshooting process using **a trial-and-error** approach. Correcting the problem in this manner saves a great deal of time.

When a situation requires a more structured approach, most network personnel use a layered process based on the OSI or TCP/IP models. The technician uses previous experience to determine if the issue is associated with the lower layers of the OSI model or the upper layers. The layer dictates whether a top-down or bottom-up approach is appropriate.

- **Basic Network Problems**
  - ✓ **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened or can be physically damaged.
  - ✓ **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.
  - ✓ **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem and other configuration issues, network fault may arise and the services will get affected.
  - ✓ **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.
  - ✓ **Traffic overload:** If the link is over utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload condition the device will start behaving abnormally.

- ✓ **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

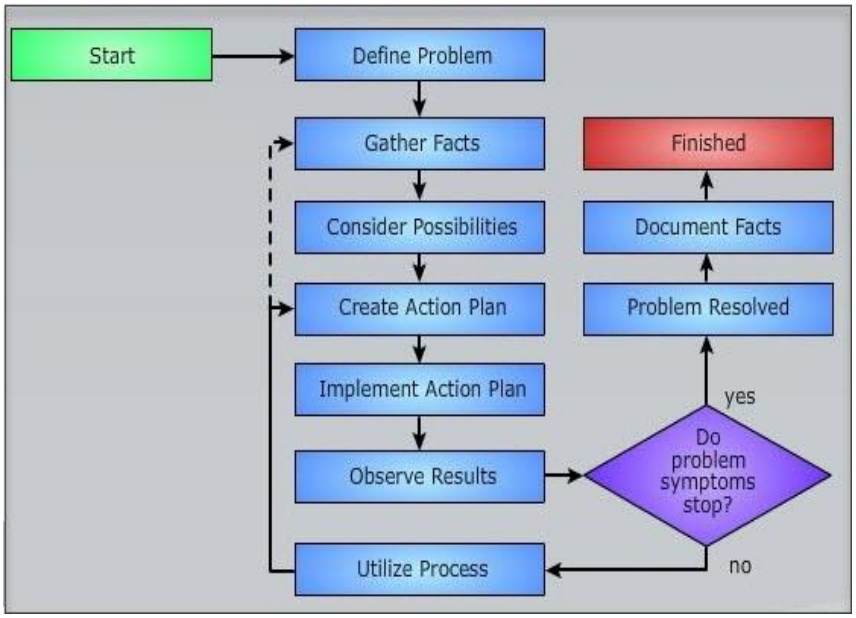


Figure 2.1 Network Troubleshooting Flowchart

When approaching a problem situation, follow the generic problem-solving model, regardless of the type of troubleshooting technique used.

- Define the problem
- Gather facts
- Deduce possibilities and alternatives
- Design plan of action
- Implement solution
- Analyse results

If the first pass through this procedure does not determine and correct the problem, repeat the process as necessary.

Document the initial symptoms and all attempts at finding and correcting the cause. This documentation serves as a valuable resource should the same or similar problem occur again. It is important to document even failed attempts, to save time during future troubleshooting activities.

When troubleshooting, proper documentation must be maintained. This documentation should include as much information as possible about:

- The problem encountered
- Steps taken to determine the cause of the problem
- Steps to correct the problem and ensure that it will not reoccur

Document all steps taken in troubleshooting, even the ones that did not solve the issue. This documentation becomes a valuable reference should the same or similar problem occur again.

Gathering Information

When a problem is reported, verify it and determine the extent. Once the problem is confirmed, the first step in troubleshooting is to gather information.

Gathering information

One of the first ways to gather information is to question the individual who reported the problem as well as any other affected users. Questions can include: end user experiences, observed symptoms, error messages and information about recent configuration changes to devices or applications.

Next, collect information about any equipment that may be affected. This can be gathered from documentation. A copy of all log files and a listing of any recent changes made to equipment configurations is also necessary. Other information on the equipment includes the manufacturer, make and model of devices affected, as well as ownership and warranty information. The version of any firmware or software on the device is also important because there may be compatibility problems with particular hardware platforms.

Information about the network can also be gathered using network monitoring tools. Network monitoring tools are complex applications often used on large networks to continually gather information about the state of the network and network devices. These tools may not be available for smaller networks. Once all necessary information is gathered start the troubleshooting process.

Software Utilities for troubleshooting connection

A number of software utility programs are available that can help identify network problems. Most of these utilities are provided by the operating system as command line

interface commands. The syntax for the commands may vary between operating systems.

Some of the available utilities include:

- ipconfig - Displays IP configuration information
- ping - Tests connections to other IP hosts
- tracert - Displays route taken to destination
- netstat - Displays network connections
- nslookup - Directly queries the name server for information on a destination domain

Ipconfig

Ipconfig is used to display the current IP configuration information for a host. Issuing this command from the command prompt will display the basic configuration information including: IP address, subnet mask and default gateway.

Ipconfig /all

The command ipconfig /all displays additional information including the MAC address, IP addresses of the default gateway and the DNS servers. It also indicates if DHCP is enabled, the DHCP server address and lease information.

How can this utility assist in the troubleshooting process? Without an appropriate IP configuration, a host cannot participate in communications on a network. If the host does not know the location of the DNS servers it cannot translate names into IP addresses.

Ipconfig /release and ipconfig /renew

If IP addressing information is assigned dynamically, the command ipconfig /release will release the current DHCP bindings. Ipconfig /renew will request fresh configuration information from the DHCP server. A host may contain faulty or outdated IP configuration information and a simple renewal of this information is all that is required to regain connectivity.

If after releasing the IP configuration, the host is unable to obtain fresh information from the DHCP server, it could be that there is no network connectivity. Verify that the NIC has an illuminated link light, indicating that it has a physical connection to the network. If

this does not solve the problem, it may be an issue with the DHCP server or network connections to the DCHP server.

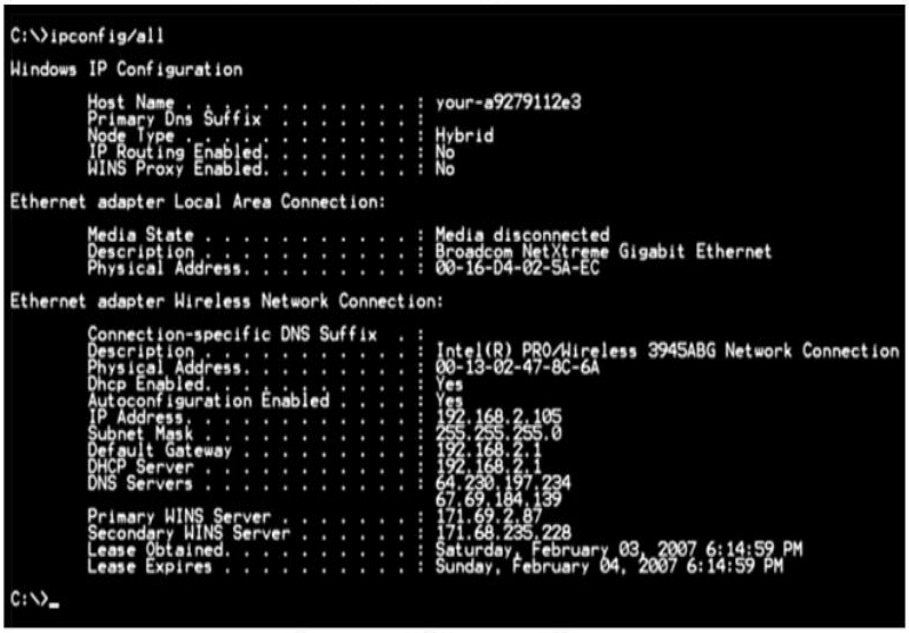


Figure 2.2 ipconfig display information

Operation sheet- 1 **Windows Client Configuration**

You will need the following

- **Window 7**
- **Window server 2008 or above**

Steps

Step 1: Start both Windows Server 2008 R2 and Windows 7 vms. At first, you will not login to Windows 2008 Server as of yet, only to the Windows 7 machine

Step 2: View network card configuration using the ipconfig command

Step 3: Change the IP address of the Windows 7 machine

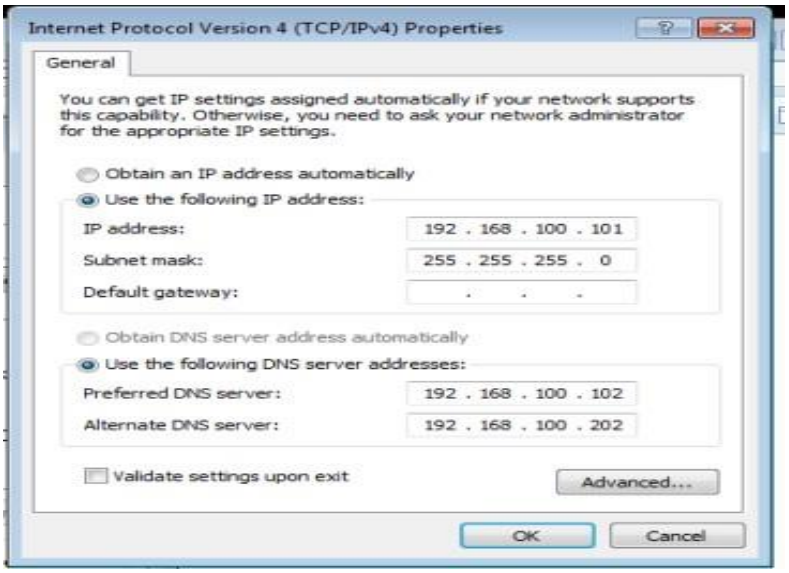


Fig. 2.3 Internet Protocol version 4(TCP/IPV4) properties

Step 4: Verify the new IP address. Use the ipconfig command to verify that the IP address has changed.

Step 5: Change Windows 7 machine back to the original address

Step 6: Ping the Windows Server machine from the Windows 7 PC

Step 7: Change IP address of Windows Server 2008 machine and try and ping Windows

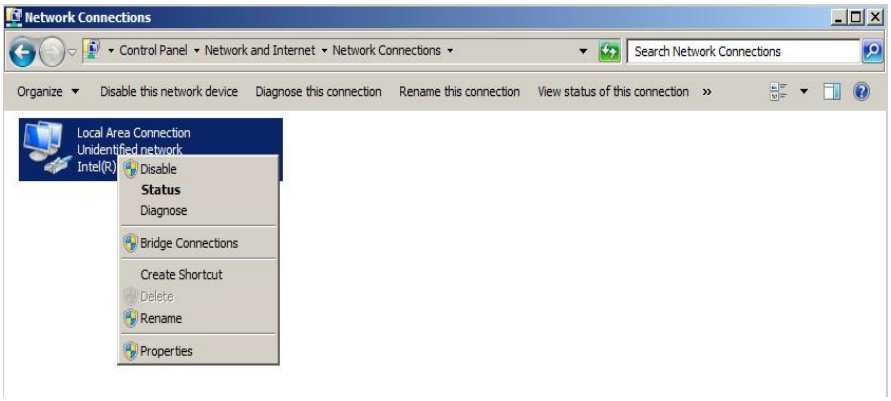


Fig. 2.4 network connection properties

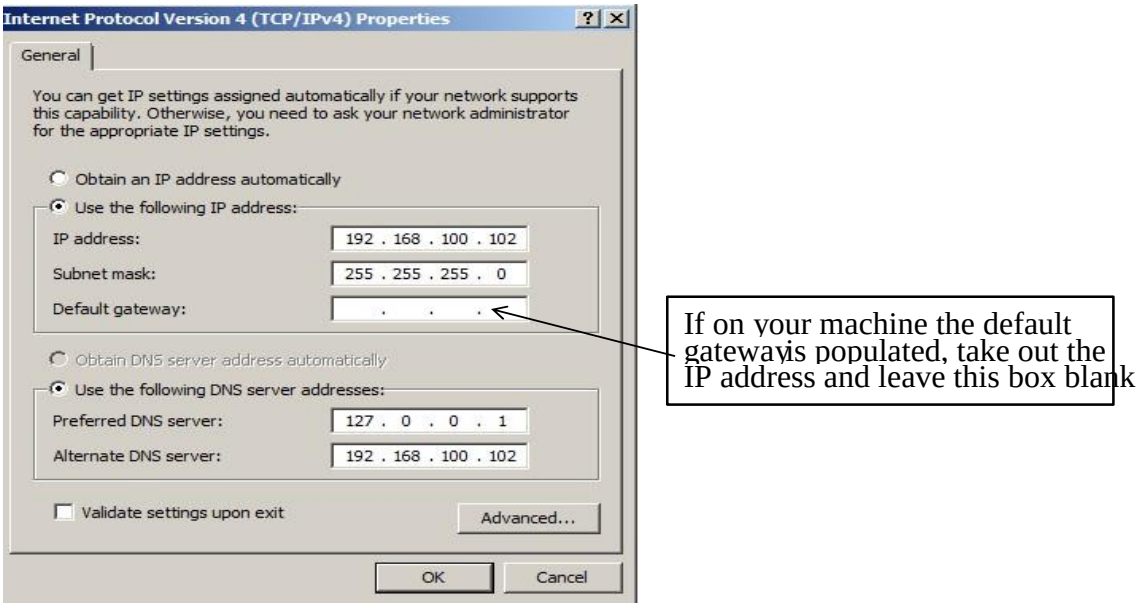


Fig. show Default getaways options

Step 8: Ping Windows Server 2008 machine from Windows 7 machine after IP address on Windows Server 2008 machine is changed.

Step 9: Change subnet mask of Windows Server 2008 Machine and ping from Windows 7 machine

Step 10: Put IP and Subnet Mask address back to their pre lab setting and view and modify the ARP table.

Ping

If the IP configuration appears to be correctly configured on the local host, next, test network connectivity by using ping. Ping is used to test if a destination host is reachable. The ping command can be followed by either an IP address or the name of a destination host, as for example:

ping 112.168.7.5

ping www.cisco.com

When a ping is sent to an IP address, a packet known as an echo request is sent across the network to the IP address specified. If the destination host receives the echo request, it responds with a packet known as an echo reply. If the source receives the echo reply, connectivity is verified.

If a ping is sent to a name, such as www.cisco.com, a packet is first sent to a DNS server to resolve the name to an IP address. Once the IP address is obtained, the echo request is forwarded to the IP address and the process proceeds. If a ping to the IP address succeeds, but a ping to the name does not, there is most likely a problem with DNS.

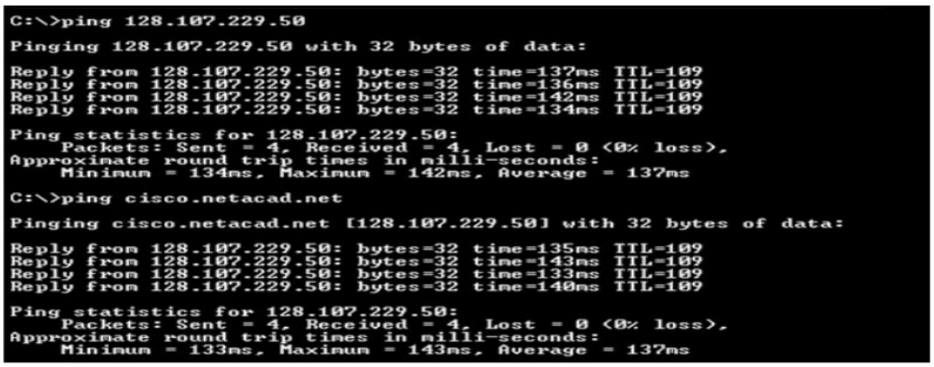


Fig. 2.5 Ping display results

If pings to both the name and IP address are successful, but the user is still unable to access the application, then the problem most likely resides in the application on the destination

Operation sheet- 2 testing the network connection using command prompt

1. From the Windows Start menu, click Run.
2. Type CMD and click OK.
3. Do this step on both computers.
4. In the command prompt of the source computer, then press Enter. For example, PING 10.0.0.2 Understanding the results:

5. Each PING test makes 4 tries, and gives back a response for each attempt.

If the response looks like this, the test is successful.

```
Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=64
Reply from 10.0.0.2: bytes=32 time=1ms TTL=64
Reply from 10.0.0.2: bytes=32 time=1ms TTL=64
Reply from 10.0.0.2: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Fig. 2.6 shows ping test successful response

If the response looks like either of these examples, the test failed.

```
Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Fig. 2.7 shows ping test failed display

Tracert

The ping utility can verify end-to-end connectivity. However, if a problem exists and the device cannot ping the destination, the ping utility does not indicate where the connection was actually dropped. To accomplish this, another utility known as tracert must be used.

The Tracert utility provides connectivity information about the path a packet takes to reach the destination and about every router (hop) along the way. It also indicates how long a packet takes to get from the source to each hop and back (round trip time). Tracert can help identify where a packet may have been lost or delayed due to bottlenecks or slowdowns in the network.

The basic tracert utility will only allow up to 30 hops between a source and destination device before it assumes that the destination is unreachable. This number is adjustable by using the -h parameter. Other modifiers, displayed as Options in the graphic, are also available.

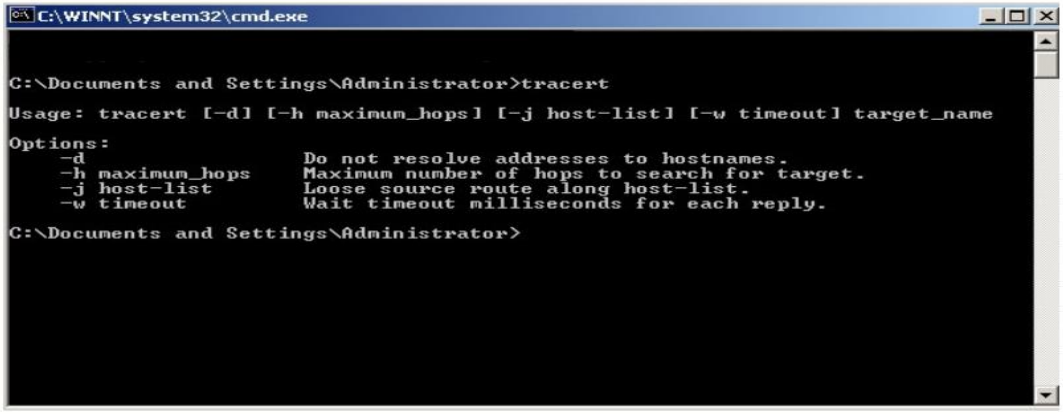


Fig. 2.8 Shows Tracert test failed display

Netstat

Sometimes it is necessary to know which active TCP connections are open and running on a networked host. Netstat is an important network utility that can be used to verify those connections. Netstat 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. This is because they can indicate that something or someone is connected to the local host. Additionally, unnecessary TCP connections can consume valuable system resources thus slowing down the host's performance. Netstat should be used to examine the open connections on a host when performance appears to be compromised.

Many useful Options are available for the netstat command.

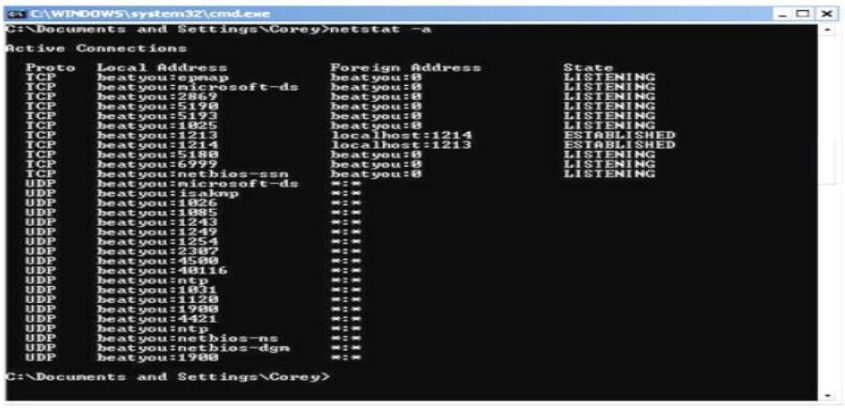


Fig. 2.9 Netstat test failed display

Nslookup

When accessing applications or services across the network, individuals usually rely on the DNS name instead of the IP address. When a request is sent to that name, the host must first contact the DNS server to resolve the name to the corresponding IP. The host then uses IP to package the information for delivery.

The nslookup utility allows an end-user to look up information about a particular DNS name in the DNS server. When the nslookup command is issued, the information returned includes the IP address of the DNS server being used as well as the IP address associated with the specified DNS name. Nslookup is often used as a troubleshooting tool for determining if the DNS server is performing name resolution as expected.

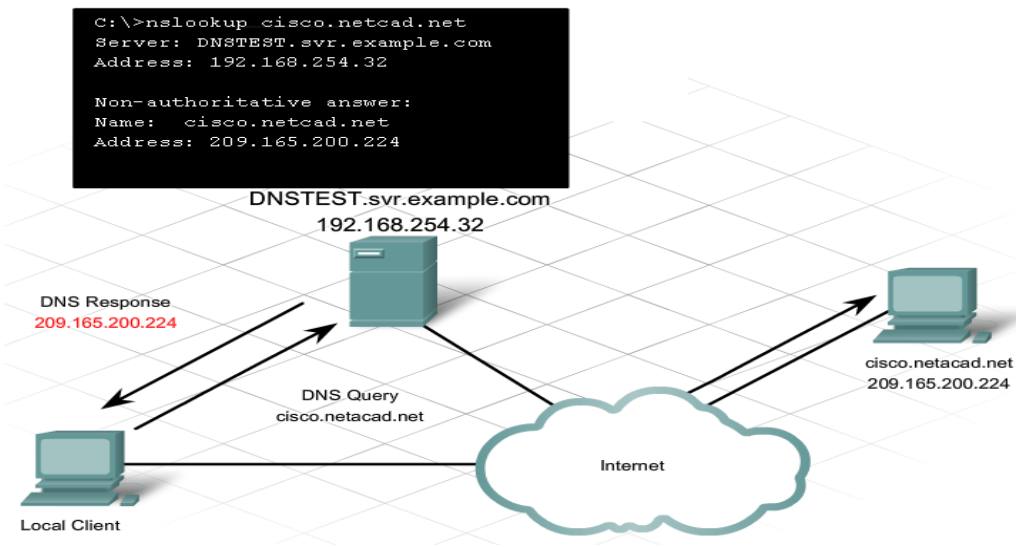


Fig. 2.10 **Nslookup** display

Troubleshooting Tools

Tone Generator and Tone Locator

Ideal situation

Telecommunications closet ports, wire terminations all labelled properly

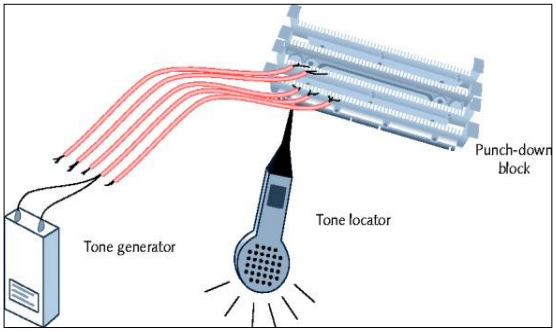
Reality

Telecommunications closet disorganized, poorly documented

Tone generator (toner)

Issues signal on wire pair**Tone locator (probe)**

- Emits tone when electrical activity detected



Probe kit

- Generator and locator combination

  Fox and hound

Fig.2.11 Tone generator

Fiber optic continuity tester

- Issues light pulses on fiber
- Determines whether pulses reached other end
- Tests the cable

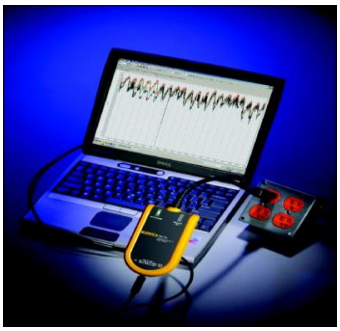


Fig. 2.12 Fiber optic continuity tester

Butt Set

Lineman's handset, telephone test set

- Butt into telephone conversation
- Rugged, sophisticated telephone

Uses Determine if line functioning

- Receiving signal, picking up noise affecting signal
- Sophisticated butt sets
- Perform rudimentary cable testing tester
- Detecting dial tone on line

Fig.2.13 Butt set telephone

Operation sheet 2 Disable TCP/IP on computer

Problems: TCP/IP disabled.

To disconnect TCP/IP on computer

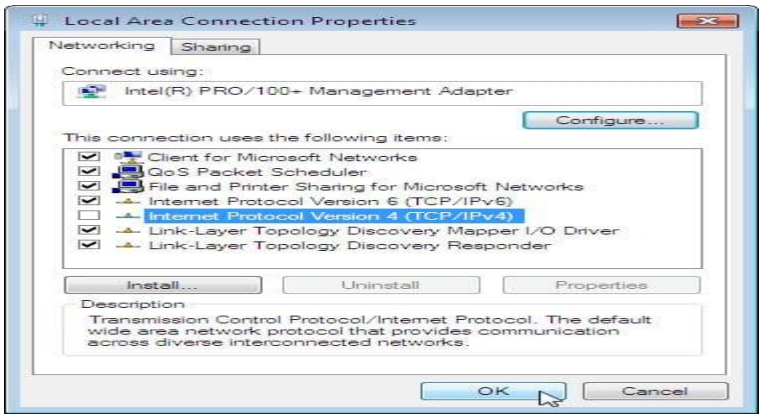


Fig.2.15 Ethernet properties

Click **Start** ---▸ **Control Panel** ---▸ **Network and Sharing Center** ---▸ Click **Change adapter settings** ---▸ double-click the desired network adaptor---▸ click **Properties**.

Unselect **Internet Protocol Version 4 (TCP/IPv4)**---▸ **OK**.

Software troubleshooting

NTLDR:- stands **NT l**oa**d**e**r** is the boot loader for all releases of Windows NT operating system up to and including Windows XP and Windows Server 2003. NTLDR is typically run from the primary hard disk drive, but it can also run from portable storage devices such as a CD-ROM, USB flash drive, or floppy disk. NTLDR can also load a non NT-based operating system given the appropriate boot sector in a file.

NTLDR requires, at the minimum, the following two files to be on the system volume:

- NTLDR, the main boot loader itself
- NTDETECT.COM, required for booting an NT-based OS, detects basic hardware information needed for successful boot

NTLDR is launched by the volume boot record of system partition, which is typically written to the disk by the Windows FORMAT or SYS command.

Windows NT was originally designed for ARC-compatible platforms, relying on its boot manager support and providing only osloader.exe, a loading program accepting ordinary command-line arguments specifying Windows directory partition, location or boot parameters, which is launched by ARC-compatible boot manager when a user chooses to start specific Windows NT operating system. However, because the x86 lacked any of the ARC support, the additional layer was added specifically for that platform: custom boot manager code presenting text menu allowing the user to choose from one or more operating system and its options configured in boot.ini configuration file, prepended by special Start up module which is responsible for some preparations such as switching the CPU to the protected mode. When a user chooses an operating system from the boot menu, the following command-line arguments are then passed to the part of the osloader.exe common to all processor architectures:

Fig. 2.16 shows: NTLDR missing window XP

Causes of NTLDR Error

This error has been known to occur as a result of one of the following causes:

Cause 1: Computer is booting from a non-bootable source

Sometimes this error can be caused if a computer tries to boot from a non-bootable source, such as a floppy disk or a flash drive. This usually happens if that computer's BIOS boot sequence is configured incorrectly.

Cause 2: NTLDR-related files are corrupt or missing

On Windows XP, Windows 2000, and Windows 2003 Server this error may appear if any of boot-related files (NTLDR, NTDETECT.COM and Boot.ini) are missing or corrupt. These files are normally hidden and system protected, but they can still go bad because of user errors, power outages, or virus attacks.

Cause 3: The bootable volume has its active partition set incorrectly Similar to the previous cause, this error may occur if a bootable disk's active partition is set incorrectly. For example, let's assume that the user's PC has a bootable volume with two primary partitions. The first partition is active, and has the operating system files, NTLDR + the NTLDR boot loader code set. The second partition is inactive, and has only the NTLDR boot loader code set without the NTLDR itself, probably as a leftover from a previous Windows installation. If the user sets the second partition as active instead of the first one, then the system tries to load from a second partition, looks for the NTLDR file, is unable to find it on this volume, and then halts the loading process, displaying an error screen.

Cause 4: Wrong boot sector code is installed

Windows Vista, Windows 7, Windows 8, Windows 8.1 and Windows 10 use a newer version of loader called BOOTMGR, but this error can still appear if the older NTLDR-compatible master boot code is applied to the bootable partition. That is usually caused by errors made while configuring the boot loader manually.

Cause 5: Too many files in the root folder

HAL (Hardware Abstraction Layer) serves as an interface between a system's hardware and software, providing a consistent hardware platform on which to run applications. When a HAL is employed, applications do not access hardware directly but access the abstract layer provided by the HAL. For example, responding to an interrupt is quite different on a machine with an Advanced Programmable Interrupt Controller than on one without. The HAL provides a single function for this purpose that works with all kinds of interrupts by various chipsets, so that other components need not be concerned with the differences. In Windows, HAL is implemented in hal.dll, and when this file is either missing on corrupt, the boot process halts, or an error screen is displayed. . Hal.dll file can become missing, damaged, corrupted or deleted because of numbers of reasons and it will get in notice when you install or run some application and ends with hal.dll missing or hal.dll not found the error.

Here is an example of "HAL is missing or corrupt" error screen for Windows XP:

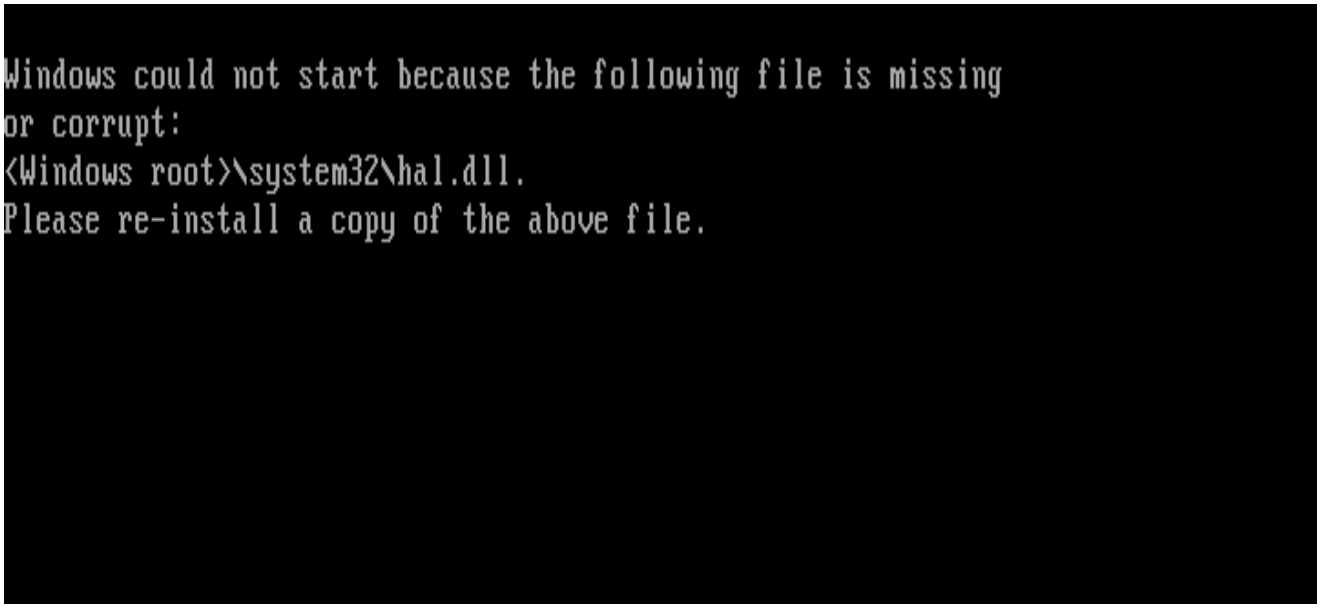


Fig 2. 17 shows HAL is missing or corrupt" error screen for Windows XP

Hal.dll errors in Windows 7, Windows 8, Windows 10, may appear in one of several different ways:

- Windows could not start because the following file is missing or corrupt: C:\Windows\system32\hal.dll. Please re-install a copy of the above file.
- Cannot find \Windows\System32\hal.dll
- C:\Windows\System32\Hal.dll missing or corrupt
- Windows failed to load because the HAL is missing, or corrupt. Status: 0xc000000f
- Windows failed to start. A recent hardware or software change might be the cause.

Hal.dll errors always display shortly after the computer is started but before Windows fully starts.Hal.dll errors in Windows XP are usually caused by different issues than in later versions of Windows. Please see How to Fix Hal.dll Errors in Windows XP instead.

Cause of Hal.dll Errors

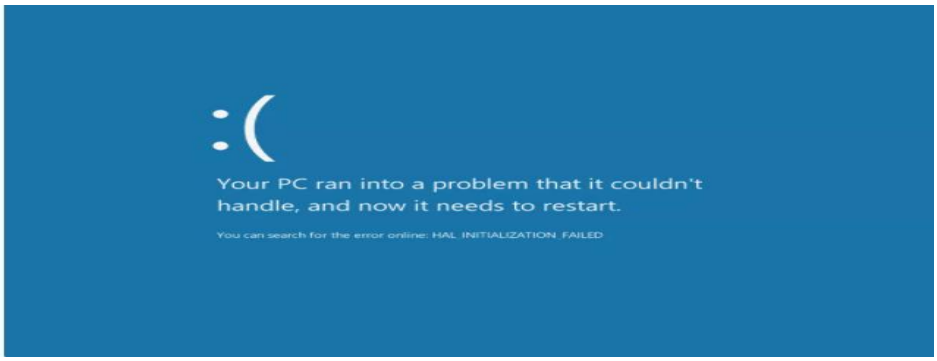


Fig. 2.18 shows A Blue Screen of Death in Windows 8.

Operation sheet 3. Repairing NTLDR missing

Operation title: - Repairing NTLDR missing

Purpose	To acquire the trainees with assembling cream separator operation and maintenance practice
Equipment ,tools and materials	Supplies and equipment needed or useful for fitting and adjusting cream senator include these: • Computer • CD/DVD which have operating system
Conditions or situations for the operations	• All tools, equipment's and materials should be available on time when required. • Appropriate working area/Lab to repair.
Procedures	1. Insert the Windows XP install CD 2. Restart the computer and boot from the CD 3. Press any key to boot from the CD 4. Press **R** when the Windows Options menu is loaded to access **Repair Console** 5. After this step, log into Windows by pressing **1** using the Administrator password 6. Use the following commands to copy the NTLDR and NTDETECT.COM files from the Windows installation disk to the hard disk: 7. Copy D:\i386\ntldr C:\ 8. Copy D:\i386\ntdetect.com C:\ 9. Where D:\ is the install CD's drive letter and C:\ is the Windows XP

	partition's drive letter 10. Once these files are copied, remove the Windows installation disc from the disc drive 11. Restart the PC 12. Restart your computer
Precautions	• Care should be taken while connecting with electric adjusting computer • Preparing materials, tools and equipment are according to instruction given
Quality criteria	• Did personal protective equipment worn while repairing computer machine

Operation sheet 3. Repairing Hal.dll missing

Operation title: - Repairing Hal.dll missing

Purpose	To acquire the trainees with assembling cream separator operation and maintenance practice
Equipment ,tools and materials	Supplies and equipment needed or useful for fitting and adjusting cream senator include these: • Computer • CD/DVD which have operating system
Conditions or situations for the operations	• All tools, equipment's and materials should be available on time when required. • Appropriate working area/Lab to repair.
Procedures	1. Restart your computer. 2. Press any key to boot into the CD when you see the "Press any key to boot from CD" message. 3. Press R to start **Recovery Console** when the Options screen appears. 4. Type in your Administrator password followed by the Enter key to submit it. 5. You'll reach the Command Prompt now, type the following command, where D:\ is your CD's drive letter and C:\ is the letter of the drive you installed Windows to: 6. expand D:\i386\hal.dl_ C:\Windows\system32\ 7. Press Y when you are asked if you want to overwrite this file and then hit Enter to submit the command. 8. Restart your computer.

Precautions	• Care should be taken while connecting with electric adjusting computer • Preparing materials, tools and equipment are according to instruction given
Quality criteria	• Did personal protective equipment worn while repairing computer machine

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Marching column A with column B

	column A		**column A**
1	Ping _____	A.	Displays IP configuration information
2	Tracert _____	B.	Tests connections to other IP hosts
3	Nslookup _____	C.	Displays route taken to destination
4	Ipconfig _____	D.	Displays network connections
5	Netstat _____	E.	Directly queries the name server for information on a destination domain

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____

Lap Test 1	Practical Demonstration

Task 1. When you turn on the computer it boots regularly and displays on the monitor/screen the message **"NTLDR file is missing"** press Ctrl+Delete. Solve this problem. (Assume that the computer should not be formatted.)

Instruction: - Repair your computer system properly.

- Recover the system file missed.

Task 2. Write the symptoms of NTLDR missing

Information sheet 3. Advising users and clients of progress and solutions

An improvement must offer an obvious advantage over whatever it replaces, or potential users will have little incentive to use it. The more visible the costs of an innovation (financial, convenience, the need to learn new skills), the greater the importance of making potential benefits and rewards apparent. These benefits include expanded influence over work (stopping a production line), increased value of work, greater recognition (being part of a valued implementation team), solution of a long standing problem and preservation of jobs.

A solved may pay off for an organization as a whole but not for individuals in any form they can recognize. That is why it is so important to make these benefits visible through encouragement from supervisors as well as through explicit and timely feedback on how the innovation is affecting workers' output. In general, the faster the positive feedback to users, the more visible the benefits will be.

It is clear that all the benefits of the new system increased to the organization, not to the individuals who used it. The organization's supported, indeed mandated, use of the new system, but the reward structure militated against it.

Network Monitoring Solution

To really know your network, you need a network monitoring solution that can tell you what you need to know – in real time and from anywhere, anytime.

For businesses of all sizes, you also need a solution that's easy to use, quick to deploy, and offers low total cost of ownership – yet also delivers all the features you need. You need a solution with comprehensive capabilities and the same reliability you expect from your network. If you want your network running at high availability, you need a demonstrated solution that you can depend on as well.

Remember, you're monitoring a lot of network components and you're collecting a lot of information. In order to see things clearly and quickly, you need a solution that displays this data – including a network map, report data, alerts, historical information, problem areas, and other useful information – as a network operating center (NOC) dashboard. Aside from making troubleshooting easier, this will help you to leverage historical network data to understand trends in device usage, network usage, and overall network capacity to enable more accurate and effective network design and planning.

And while your network generally stays in one location, your employees sometimes travel. Regardless, you need to be able to access your network monitoring solution anywhere, anytime. For that matter, different people will need to access the system for different reasons, and not everyone should be able to access the same level of information. You need a solution that affords role-based views, that assigns levels of permissions based on the user's function in the organization. Finally, you should look for a solution that supports multiple methods of monitoring devices. SNMP (Simple Network Management Protocol) is a flexible technology that lets you manage and monitor network performance devices, troubleshoot problems, and better prepare for future network growth. Many network devices support SNMP, making it easy to monitor them using a solution that supports SNMP.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Write true if the sentence is correct or false in sentence is wrong

1. Network monitoring including a network map, report data, alerts, historical information, problem areas, and other useful information network operating _____
2. SNMP is a flexible technology that lets you manage and monitor network performance devices, troubleshoot problems _____

II. Short answer

3. Write at least 4 the Key Benefits of Network Monitoring

_____

_____

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating: _____

Information sheet 4. Completing support documentation

Network documentation is an important part of any troubleshooting process. Network documentation should include a normal or baseline measurement of network performance against which potential problems can be judged.

The performance baseline can include the types of traffic normally expected, as well as the volume of traffic to and from servers and network devices. The baseline should be documented just after the network is installed, when it is running optimally. Baseline performance should be re-established after any major changes to the network are implemented.

Additionally, documentation such as topology maps, network diagrams and addressing schemes can provide valuable information when a troubleshooter is trying to understand the physical layout of the network and the logical flow of information.

Why is documenting considered the most important?

Documentation is a useful record because it can lead to the elimination of an entire set of suspect problems. Over time, documentation tracks all the changes or modifications made to a system. If the next system problem is evaluated by a different technician, as often happens in large corporate environments, records of previous repairs are invaluable troubleshooting tools; they educate the technician on the previous state of the machine.

There are specific questions regarding the network server that a technician should ask in the event of a problem.

List four of these questions:

- When was the last time that the network server was operational?
- What has changed since the last time the network server was operational?
- What hardware or software has been recently added to the network server?
- Who first reported the problem with the network server?

- Where is the network server logbook?

How is the failure of the network server affecting the operation of the corporation?

When troubleshooting, documentation should be maintained during the troubleshooting process. This documentation can be a valuable reference and can be used when future issues arise.

Good troubleshooting documentation should include:

- Initial problem
- Steps taken to isolate the problem
- Results of all steps taken, both successful and unsuccessful
- Final determined cause of the problem
- Final problem resolution
- Preventative measures

- **Using outside source for help**

During the troubleshooting process, the troubleshooter is unable to determine the problem and its resolution, it might be necessary to obtain assistance from outside sources. Some of the most common sources for help include:

- ✓ Previously kept documentation
- ✓ Online FAQs (Frequently Asked Questions)
- ✓ Colleagues and other network professionals
- ✓ Internet forums

- **Using the Help Desk**

The helpdesk is the end-user's first stop for assistance. The helpdesk is a group of individuals with the knowledge and tools required to help diagnose and correct common problems. It provides assistance for the end-user to determine if a problem exists, the nature of the problem, and the solution.

Many companies and ISPs establish helpdesks to assist their users with networking problems. Most large IT companies run helpdesks for their individual products or technologies

Documented network is easier to troubleshoot

Some of the important things you should consider as potential candidates for documenting include the following:

- A logical map of the network.
  - ✓ This may or may not match up with the physical way the network is laid out.
- A physical map of the network.
  - ✓ This documentation should describe each physical component and illustrate the ways in which the different components are connected.
- Cabling and patch panel information.
  - ✓ When you've got hundreds of cables in a wiring closet patching together different physical segments, you'll need to know which cable connects this to that.
- Default settings for computers and other devices on the network. A spreadsheet is good for this.
  - ✓ An application that manages servers, network components, and client computers is even better.
- Listings of applications and the computers or users that make use of them, as well as software versions, patch levels, and so on.
- Be sure to know who to contact for a particular application. If you are a network administrator, you are primarily responsible for the underlying network.
  - ✓ If a particular application is failing, but the network is up and running, you need to know who to call. There should always be a contact on your list for application managers. A network manager can do only so much.
- Information about the user accounts, and associated permissions and rights, for the users and user groups on the network.
- A network overview.
  - ✓ It's nice to be able to give a new user a document that explains what she needs to know about the network.

- ✓ This should be a short document telling the user such things as which drives are mapped to her computer, and which printers offer what features.
- ✓ This should not be an extensive document such as the physical and logical maps described earlier in this list.

- Problem reports.
  - ✓ Keep track of problems as they arise, and document the cause and remedy.
  - ✓ No need to solve the same problem twice! This also includes outage reports—keeping track of unscheduled downtime for a computer or network device can tell you over time just how capable the device is.
  - ✓ A logical map of the network shows the relationships between components and the flow of information through the network.
  - ✓ A physical map of the network tries to approximate on paper a representation of how each component of the network is connected to the network.
    - For example, a logical map for a Windows network might show computers grouped by domains, even though the computers are not located physically in the same part of the network.
  - ✓ A physical map would show the location of each of the computers, the hub or switch to which they are connected, and so on. In general, logical maps can be used to help isolate configuration or application problems, whereas physical maps can be used to isolate a problem that affects only a portion of the network, perhaps a single computer or other device.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Write true if the sentence is correct or false in sentence is wrong

1. Helpdesk is the end-user's first stop for assistance _____
2. A physical map of the network is the physical way the network is laid out. _____
3. Initialize the problem is the first step of troubleshooting documentation_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____

Rating:

LG # 29	LO #3- Carry out maintenance support on identified problem

Instruction sheet

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- Conducting diagnostic tests around identified problem
- Completing maintenance in the line with organizational guidelines
- Obtaining new components as part of the resolution
- Storing or disposing components

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Conduct diagnostic tests around identified problem
- Complete maintenance In the line with organizational guidelines
- Obtain new components as part of the resolution
- Store or disposing components

Learning Instructions:

Read the specific objectives of this Learning Guide.

1. Follow the instructions described below.
2. Read the information written in the “Information Sheets”. Try to understand what are being discussed. Ask your trainer for assistance if you have hard time understanding them.
3. Accomplish the “Self-checks” which are placed following all information sheets.
4. Ask from your trainer the key to correction (key answers) or you can request your trainer to correct your work. (You are to get the key answer only after you finished answering the Self-checks).
5. If your performance is satisfactory proceed to the next learning guide,
6. Perform “the Learning activity performance test” which is placed following “Operation sheets” ,
7. If your performance is satisfactory proceed to the next learning guide,
8. If your performance is unsatisfactory, see your trainer for further instructions or go back to “Operation sheets

Information sheet 1. Conducting diagnostic tests around identified problem

Network diagnostics tools

One of the most important abilities for a network professional to develop is the ability to efficiently troubleshoot network problems. Good network troubleshooters are always in high demand. When troubleshooting, many technicians use the OSI and TCP/IP networking models to help isolate the cause of a problem. Logical networking models separate network functionality into modular layers. Each layer of the OSI or TCP/IP model has specific functions and protocols. Knowledge of the features, functions, and devices of each layer, and how each layer relates to the layers around it, help a network technician to troubleshoot more efficiently.

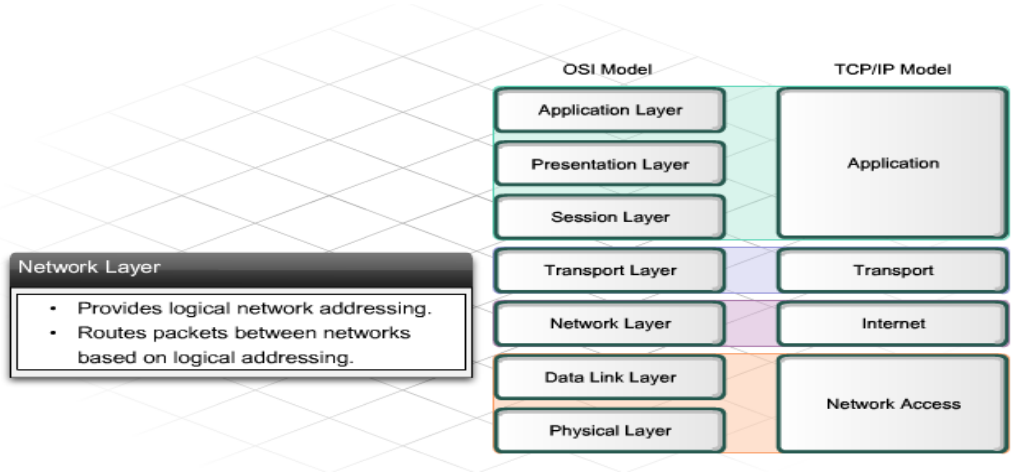


Fig. 3.1 OSI and TCP/IP model summary

Network Diagnostics Tools are simple software for real-time monitoring and fast configuring of network devices, components, and appliances that can cause critical issues when they go down. Some diagnostic software gather data useful for network forensic analysis and investigation with inspection of packet data, allowing tracking of intrusion or other causes of network events.

The Network Diagnostic Tool is a client/server program that provides network configuration and performance testing to a user's desktop or laptop computer.

The system is composed of a client program (command line or java applet) and a pair of server programs (a webserver and a testing/analysis engine). Both command line and web-based clients communicate with a Web enhanced server to perform these diagnostic functions. Multi-level results allow novice and expert users to view and understand the test results.

Network Diagnostic Tool is a single stream performance measurement of a connection's capacity for "bulk transport" NDT (Network Diagnostic Tool) measures "single stream performance" or "bulk transport capacity". NDT reports upload and download speeds and latency metrics.

For example test the speed and health of your Internet connection to Box, follow these steps to run a **Connection Diagnostics** test from within your Box account:

- Open the **Account** menu by clicking the profile image (or initials) in the upper-right corner. Click **Account Settings**.
- Select the "**Diagnostics**" tab
- Under the "**Connection Diagnostics**" section, click the "**Run Test**" button

This will run a multi-step connection test to see if your connection is at an optimum level. When the test completes, you will see a short summary of test results.

Because most problems have simple causes, developing a clear idea of the problem often provides the solution. Unfortunately, this is not always true, so in this section we begin to discuss the tools that can help you attack the most intractable problems. Many diagnostic tools are available, ranging from commercial systems with specialized hardware and software that may cost thousands of dollars, to free software that is available from the Internet. Many software tools are provided with your UNIX system. You should also keep some hardware tools handy.

To maintain the network's equipment and wiring, you need some simple hand tools. A pair of needle-nose pliers and a few screwdrivers may be sufficient, but you may also need specialized tools. For example, attaching RJ45 connectors to unshielded twisted pair (UTP) cable requires special crimping tools.

Self-Check 1	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

Fill Blank pace

1. _____Tools are simple software for real-time monitoring and fast configuring of network devices, components, and appliances that can cause critical issues when they go down.
2. _____is the process of identifying, locating and correcting problems that occur.

II. Short answer

3. What is network diagnostics tools?

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____ Rating:

Information sheet 2. Completing maintenance in the line with organizational guidelines

Maintenance procedures and other work-related documents should identify preconditions and precautions, provide clear instructions for work to be done, and be used to ensure that maintenance is performed in accordance with the maintenance strategy, policies and programmes. The procedures should normally be prepared in cooperation with the designers, the suppliers of equipment, and the personnel conducting activities for quality assurance, radiation protection and technical support. They should be technically accurate, properly verified, validated, authorized and periodically reviewed.

Priority should be given to amending and updating procedures in a timely manner. A mechanism should be implemented which enables users to feedback suggestions for the improvement of procedures based on the organization rules and guide lines.

Maintenance instructions issued to crafts men should be compiled in accordance with quality assurance requirements and should point out the risk impact of the work with equipment and personnel safety and identify the counter measures to be taken and specify the post-maintenance/modification testing required. The required level of skill and methods of procedure use should be stated. Routine activities involving skills that qualified personnel usually possess may not require detailed step-by-step instructions; they should nevertheless be subject to control by means of organization rules and guidelines procedures.

Maintenance services

When discussing the maintenance of the physical aspects of the technology throughout its life span (generally 3-5 years for most equipment and applications), it makes sense to think seriously about what maintenance requirements actually entail. The term "maintenance" refers to those preventive, diagnostic, updating, replacement, and repair procedures that an organization undertakes to keep its technology working effectively

and efficiently. Maintenance can be provided either by persons who are employees of the organization or through outside contractors.

Maintenance items might include:

- ✓ replacing wear-and-tear parts and consumable supplies
- ✓ repairing or replacing faulty components
- ✓ cleaning equipment
- ✓ monitoring the condition and functionality of networks and equipment, including testing website access and links
- ✓ redeploying equipment
- ✓ updating or upgrading hardware and software, including installing new versions of the operating system
- ✓ backing up stored files
- ✓ documenting trends and patterns in the use of applications or equipment
- ✓ removing and disposing of equipment and applications

Hardware maintenance

The steps to be followed when carrying out maintenance of hardware will depend on the device being maintained and the problem with it. Most hardware products should have comprehensive technical and user manuals, help screens and websites to assist in this

You need to have access to and examine closely the recommended procedures and documentation when carrying out hardware maintenance. All maintenance is usually recorded on a log. This is used for statistical reports to improve any future repairs on network components, and for budgeting estimates. You also need to follow OH&S guidelines to ensure you do not cause any injury to yourself or damage any of the computer components.

All tools and components need to be available before you start the task. When any form of maintenance is required, it should be done at a time that is less disruptive to users.

Software maintenance

Again there are many tasks in maintaining servers and computer software and these will be described in the associated manuals. It is less likely that there will be specific procedures and documentation needs for these processes, so you would need to review the organisation's procedures manual to determine what is needed.

You need to ensure that software will run on the hardware that it is to be installed on. It also needs to be compatible with other software on the computer. Networked software needs to be tested from various computers on the network before being released to users.

Replacement and repair with minimal disruption

When maintenance takes place, users should be faced with only minimal disruption. The period when no one can use the computers is known as downtime.

If work cannot be done outside of normal operating hours, a schedule should be designed to minimise disruption by performing tasks at the least busy times. This needs to be done by surveying users, or having them log times on the schedule that best suit them. If the work affects all staff they need to be alerted well in advance of the proposed maintenance schedule. The maintenance should be carried out when the least number of users will require the system, and at a time when disruption will not cause problems for the company.

Sometimes scheduling in advance may not be possible. A disk crash or system breakdown often occurs when least expected. In many cases the computer or component is required to be up and running within a very short period, and expectations by users can be unrealistic. The conditions laid out for such instances in the service level agreement can set realistic times in advance. More importantly, preventative maintenance, including the resources for up-date and upgrades, may hopefully prevent such events as crashes or system breakdowns and the disruption they can cause. Having simple contingency plans can also avoid disruption.

Self-Check 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

II. Short answer

1. Write four maintenance items used during maintenance services

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating: _____

Information sheet 3. Obtaining new components as part of the resolution

Obtaining new components

Continuous interaction with clients is crucial to determine exactly what they require on their network to meet their organisational needs. The help desk data base can also often inform IT staff as to what might need to be purchased to overcome consistent problems or improve work flow. New components may of course also be required because of breakdowns.

Once you have decided that new components are required, you need to contact vendors that stock the component, obtain information as to warranty and licensing as well as any technical specifications needed to check that the component is compatible with other hardware and software on the network. For fragile components, the delivery method and packaging of the component must be appropriate and agreed upon also.

After this, the recommendations would normally need to be documented and submitted to a supervisor or manager for approval.

Self-Check 3	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

I. Short answer

1. Write at least three hardware network components?

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating: _____

Information sheet 4. Storing or disposing components

Stores Components

The cost of materials is one of the largest elements of cost. Proper storing of materials is very important to prevent losses from damage, pilferage and deterioration in quality of materials. The stores must, therefore, be properly organised and equipped for the handling of raw materials.

Material stored in maintenance store rooms can be grouped into five categories:

Major Spares these are the "insurance" items that are stocked for specific plant equipment to guard against prolonged equipment downtime. It's not uncommon for about half the dollar value of maintenance stores material to be made up of spare parts. The items in this category are:

- High cost, when compared with the cost of other stock items
- Entire assemblies/subassemblies for "vendor only" repairable items
- Specialized for use on one or a limited number of equipment items
- May be difficult to obtain promptly from suppliers
- Likely to have longer average turnover intervals than other stock items
- Used in equipment for which prolonged downtime is considered costly or unsafe Compared with the relative certainty of normal stock usage, the need for major spares or spare parts is somewhat of a gamble.

Computer network components are the major parts which are needed to install the software. Some important network components are NIC, switch, cable, hub, router, and modem. Depending on the type of network that we need to install, some network components can also be removed.

Disposal

It is important that equipment disposal procedures do not inadvertently compromise information or networks. Devices which have been involved in providing security functionality for a network are likely to retain sensitive information within them, even when powered down. The goal is to ensure that devices are unlikely to contain any

recoverable user information, and will not be able to reconnect to the encrypted network.

The following recommendations should be applied to all equipment involved in providing the encrypted network service:

1. All certificates associated with a device (including operational, management and maintenance) should be revoked prior to device disposal.
2. Any other credentials associated with a device should be changed or revoked as appropriate.
3. The advice in our secure sanitization of storage media guide should be followed for any devices that have handled decrypted information.
4. Factory resets or device wiping should be employed as a general precaution.

Packaging must be created to encourage its safe and easy disposal by consumers. Packaging should also be designed to reduce environmental hazards including reducing toxicity and dangers to flora and fauna.

Waste Disposal

(1) The waste that cannot be re-used, processed or used as a source of energy shall be disposed by using special operations for waste disposal

(2) Prior to the disposal, the waste shall be subjected to physical, chemical, thermal or biological treatment in order to reduce its quantity, volume and negative impact on the environment and on human life and health.

(3) Before a waste disposal operation is started, the waste shall be selected and classified according to the List of Wastes.

(4) The waste that cannot be selected and classified according to the List of Wastes must be assessed for its hazardous characteristics in order to decide how this waste shall be handled.

(5) The disposal of waste shall be performed at specially designated sites and locations, as well as in specially constructed premises and installations intended for waste disposal that have obtained A or B integrated environmental permit.

Self-Check 4	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet in the provided space

1. **I. Short answer**
2. Explain the similarity and difference between disposal and storing waste with example?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Note*:* Satisfactory rating 100%

You can ask your teacher for the copy of the correct answers.

Score = _____
Rating: _____

Reference

- CCNP(R): Cisco Internetwork Troubleshooting Study Guide (642-831) (Author Pfund, Todd Lammle, Sybex)
- Networking Bible (Author Barrie Sosinsky)
- CCNP(R): Cisco Internetwork Troubleshooting Study Guide (642-831) (Author Pfund, Todd Lammle, Sybex)
- Networking Bible (Author Barrie Sosinsky)
- MCSE: Windows Server 2003 Active Directory Planning, Implementation, and Maintenance Study Guide (70-294) 2nd edition (Author James Chellis)
- Network Know-How: An Essential Guide for the Accidental Admin (Author John Ross Dr)
- www.vincenzobruno.it
- https://www.premiumexam.net
- https://resources.intenseschool.com
- https://networklessons.com
- https://en.wikipedia.org/wiki/NTLDR
- https://www.networknet.nl/apps/wp/archives/671
- https://neosmart.net/wiki/ntldr-is-missing/
- https://www.insan4it.net/2010/07/windows-server-2008-ntldr-is-missing.html
- https://neosmart.net/wiki/hal-dll-missing-corrupt/

AKNOWLEDGEMENT

We wish to extend thanks and appreciation to the many representatives of TVET instructors who donated their time and expertise to the development of this TTLM.

We would like also to express our appreciation to Federal Technical and Vocational Education and Training Agency (FTVET), Oromia TVET Bureau, TVET College/ Institutes, who made the development of this TTLM with required standards and quality possible.

This TTLM is developed on December 2020 at Bishoftu Bin International hotel.

The trainers who developed the TTLM

No	Name of Trainer	College Name	Edu. Background	Address	
				Mob.	Email
1	Abebe Mintefa	Ambo TVET College	MSc.	0929352458	tolabula@gmail.com
2	Frew Atkilt	Bishoftu Polytechnic College	MSc.	0911787374	frew.frikii@gmail.com
3	Tewodiros Girma	Sheno TVET College	MSc.	0912068479	tedimutd@gmail.com
4	Tsedale Mengiste	Dukem TVET College	MSc.	0912076643	tmmeng2005@gmail.com
5	Zerihun Abate	Sebeta Polytechnic College	MSc.	0911858358	zedoabata2017@gmail.com

Answer Key LO1
Self-check 1

1. A
2. B
3. - Providing complete visibility into the IT infrastructure

   - Keeping them updated of the network's state in real time

   - Identifying issues before the end users are affected

   - Tracking and troubleshooting performance issues early

Self-check 2

1. Management Information Base
2. Simple Network Management Protocol
3. computers, hubs, routers, switches, and networking software

Self-check 3

1. A
2. A
3. B
4. C

Self-check 4

1.

- It provides an information-centric view of the ways that business processes are executed.
- It focuses on multiple uses of data and information across information system and business process boundaries.
- It reduces the concentration on functional requirements in deference to enterprise data and information requirements across the organizations.
- It documents the way that information flows across business processes and can be used to identify the best locations for inspecting data quality and identifying flaws before any business impacts can occur

2. Documentation review

Self-check 5

1. Pay attention to operational realities.
2. Prioritize based on risk analysis.
3. Be realistic about security staffing.
4. Automate routine tasks

Answer Key LO2

Self-check1

- using tools to identify and solve network problems
- advice users and clients on time
- complete support documentation

Self-check 2

1. B
2. C
3. E
4. A
5. D

Self-check 3

1. True
2. True
3.

- Maintaining full network visibility
- Discovering security threats
- Predicting and preventing network downtime
- Observing bandwidth utilization
- Reducing mean time to repair (MTTR)
- Testing changes to a network or device
- Generating network performance reports
- Documentation review

Self-check 4

1. True
2. True
3. True

Answer Key LO3

Self-check 1

1. Network Diagnostics
2. Troubleshooting
3. Network Diagnostics Tools are simple software for real-time monitoring and fast configuring of network devices, components, and appliances that can cause critical issues when they go down. Some diagnostic software gather data useful for network forensic analysis and investigation with inspection of packet data, allowing tracking of intrusion or other causes of network events. The Network Diagnostic Tool is a client/server program that provides network configuration and performance testing to a user's desktop or laptop computer.

Self-check 2

1. - replacing wear-and-tear parts and consumable supplies
   - repairing or replacing faulty components
   - cleaning equipment
   - monitoring the condition and functionality of networks and equipment, including testing website access and links
   - redeploying equipment
   - updating or upgrading hardware and software, including installing new versions of the operating system
   - backing up stored files

Self-check 3

Hardware component Routers, Bridges, Hubs, Repeaters, Gateways, switches

Self-check 4

- Storing of materials is very important to prevent losses from damage, pilferage and deterioration in quality of materials. The stores must, therefore, be properly organized and equipped for the handling of raw materials.
- It is important that equipment disposal procedures do not inadvertently compromise information or networks. Devices which have been involved in

providing security functionality for a network are likely to retain sensitive information within them, even when powered down.