Common Preventative Maintenance Techniques Used for Networks

Network Maintenance

There are common preventive maintenance techniques that should continually be performed for a network to operate properly. In an organization, if one computer is malfunctioning, generally only that user is affected. But if the network is malfunctioning, many or all users are unable to work.

Preventive maintenance is just as important for the network as it is for the computers on a network. You must check the condition of cables, network devices, servers, and computers to make sure that they are kept clean and are in good working order. One of the biggest problems with network devices, especially in the server room, is heat. Network devices do not perform well when overheated. When dust gathers in and on network devices, it impedes the proper flow of cool air and sometimes even clogs the fans. It is important to keep network rooms clean and change air filters often. It is also a good idea to have replacement filters available for prompt maintenance. You should develop a plan to perform scheduled maintenance and cleaning at regular intervals. A maintenance program helps prevent network downtime and equipment failures.

As part of a regularly scheduled maintenance program, inspect all cabling. Make sure that cables are labeled correctly and labels are not coming off. Replace worn or unreadable labels. Always follow the company’s cable labeling guidelines. Check that cable supports are properly installed and no attachment points are coming loose. Cabling can become damaged and worn. Keep the cabling in good repair to maintain good network performance. Refer to wiring diagrams if needed.

Check cables at workstations and printers. Cables are often moved or kicked when they are underneath desks. These conditions can result in loss of bandwidth or connectivity.

As a technician, you may notice that equipment is failing, damaged, or making unusual sounds. Inform the network administrator if you notice any of these issues to prevent unnecessary network downtime. You should also be proactive in the education of network users. Demonstrate to network users how to properly connect and disconnect cables, as well as how to move them, if necessary.

Basic Troubleshooting Process for Networks

Applying the Troubleshooting Process to Networks

Network problems can be simple or complex, and can result from a combination of hardware, software, and connectivity issues. Computer technicians must be able to analyze the problem and determine the cause of the error to repair the network issue. This process is called troubleshooting.
To assess the problem, determine how many computers on the network are experiencing the problem. If there is a problem with one computer on the network, start the troubleshooting process at that computer. If there is a problem with all computers on the network, start the troubleshooting process in the network room where all computers are connected. As a technician, you should develop a logical and consistent method for diagnosing network problems by eliminating one problem at a time.

Follow the steps outlined in this section to accurately identify, repair, and document the problem. The first step in the troubleshooting process is to identify the problem. The figure shows a list of open-ended and closed-ended questions to ask the customer.

After you have talked to the customer, you can establish a theory of probable causes. The figure shows a list of some common probable causes for network problems.

After you have developed some theories about what is wrong, test your theories to determine the cause of the problem. The figure shows a list of quick procedures that can determine the exact cause of the problem or even correct the problem. If a quick procedure does correct the problem, you can then verify full system functionality. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.

### Step 1: Identify the Problem

| Open-ended questions | • What problems are you experiencing with your computer or network device?  
|                      | • What software has been installed on your computer recently?  
|                      | • What were you doing when the problem was identified?  
|                      | • What error message have you received?  
|                      | • What type of network connection is the computer using?  
| Closed-ended questions | • Has anyone else used your computer recently?  
|                      | • Can you see any shared files or printers?  
|                      | • Have you changed your password recently?  
|                      | • Can you access the Internet?  
|                      | • Are you currently logged into the network? |

### Step 2: Establish a Theory of Probable Cause

| Common causes of network problems | • Loose cable connections  
|                                  | • Improperly installed NIC  
|                                  | • ISP is down  
|                                  | • Low wireless signal strength  
|                                  | • Invalid IP address |

### Step 3: Test the Theory to Determine Cause

| Common steps to determine cause | • Check that all cables are connected to the proper locations.  
|                                 | • Unseat and then reconnect cables and connectors.  
|                                 | • Reboot the computer or network device.  
|                                 | • Login as a different user.  
|                                 | • Repair or re-enable the network connection.  
|                                 | • Contact the network administrator.  
|                                 | • Ping your default gateway.  
|                                 | • Access a remote web page such as http://www.cisco.com. |
After you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution. The figure shows some sources you can use to gather additional information to resolve an issue.

After you have corrected the problem, verify full functionality and, if applicable, implement preventive measures. The figure shows a list of the steps to verify the solution.

In the final step of the troubleshooting process, document your findings, actions, and outcomes. The figure shows a list of the tasks required to document the problem and the solution.

### Identify Common Problems and Solutions

Network problems can be attributed to hardware, software, or configuration issues, or to some combination of the three. You will resolve some types of network problems more often than others. The figure is a chart of common network problems and solutions.
<table>
<thead>
<tr>
<th>Identify the Problem</th>
<th>Probable Causes</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC LED lights are not lit.</td>
<td>The network cable is unplugged, bad, or damaged.</td>
<td>Reconnect or replace the network connection to the computer.</td>
</tr>
<tr>
<td>User cannot telnet into a remote device.</td>
<td>• The remote device is not configured for Telnet access.</td>
<td>• Configure the remote device for Telnet access.</td>
</tr>
<tr>
<td></td>
<td>• Telnet is not allowed from the user or a particular network.</td>
<td>• Allow Telnet access from the user or the network.</td>
</tr>
<tr>
<td>Older laptop cannot detect the wireless router.</td>
<td>• The wireless router/access point is configured with a different 802.11 protocol.</td>
<td>• Configure the wireless router with a compatible protocol for the laptop.</td>
</tr>
<tr>
<td></td>
<td>• The SSID is not being broadcast.</td>
<td>• Configure the wireless router to broadcast the SSID.</td>
</tr>
<tr>
<td></td>
<td>• The wireless NIC in the laptop is disabled.</td>
<td>• Enable the wireless NIC in the laptop.</td>
</tr>
<tr>
<td>Computer has an IP address of 169.254.x.x.</td>
<td>• The network cable is unplugged.</td>
<td>• Reconnect the network cable.</td>
</tr>
<tr>
<td></td>
<td>• The router is powered off or the connection is bad.</td>
<td>• Ensure the router is powered on and is properly connected to the network.</td>
</tr>
<tr>
<td></td>
<td>• The NIC is bad.</td>
<td>• Replace the NIC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Release and renew the IP address on the computer.</td>
</tr>
<tr>
<td>Remote device does not respond to a ping request.</td>
<td>• Windows firewall disables ping by default.</td>
<td>• Set the firewall to enable the ping protocol.</td>
</tr>
<tr>
<td></td>
<td>• The remote device is configured to not respond to ping requests.</td>
<td>• Configure the remote device to respond to the ping request.</td>
</tr>
<tr>
<td>One user can log into the local network but cannot access the Internet.</td>
<td>The gateway address is incorrect.</td>
<td>Ensure the correct gateway address is assigned to the NIC.</td>
</tr>
</tbody>
</table>
The network is fully functional and the wireless laptop connection is enabled, but the laptop cannot connect to the network.

- The laptop wireless capability is turned off.
- The external wireless antenna is misaligned.
- The laptop is out of wireless range.
- Interference from other wireless devices using the same frequency range.

- Enable laptop wireless capability using the wireless NIC property or the Fn key along with the multi-purpose key.
- Realign the external wireless antenna to pick up the wireless signal.
- Move closer to the wireless router/access point.
- Change wireless router to a different channel.

A Windows 7 computer, just connected to a network with only Windows 7 computers, cannot view shared resources.

- Incorrect workgroup.
- Incorrect network location.
- Has not joined the homegroup.
- Network Discovery and File Sharing is turned off.

- Change workgroup name.
- Change network location to Home Network.
- Join the homegroup.
- Turn on Network Discovery and File Sharing.

A user cannot map a drive over the network.

- Incorrect workgroup.
- Network Discovery and File Sharing is turned off.

- Change workgroup name.
- Turn on Network Discovery and File Sharing.

Summary

This chapter introduced you to the fundamentals of networking, the benefits of having a network, the ways to connect computers to a network, and the planning, implementation, and upgrading of networks and network components. The different aspects of troubleshooting a network were discussed with examples of how to analyze and implement simple solutions. The following concepts from this chapter are important to remember:

- A computer network is composed of two or more computers that share data and resources.

- There are several different network types called LAN, WLAN, PAN, MAN, and WAN.

- In a peer-to-peer network, devices are connected directly to each other. A peer-to-peer network is easy to install, and no additional equipment or dedicated administrator is required. Users control their own resources, and a network works best with a small number of computers. A client/server network uses a dedicated system that functions as the server. The server responds to requests made by users or clients connected to the network.
• The network topology defines the way in which computers, printers, and other devices are connected. Physical topology describes the layout of the wire and devices, as well as the paths used by data transmissions. Logical topology is the path that signals travel from one point to another. Topologies include bus, star, ring, mesh, and hybrid.

• Networking devices are used to connect computers and peripheral devices so that they can communicate. These include hubs, bridges, switches, routers, and multipurpose devices. The type of device implemented depends on the type of network.

• Networking media can be defined as the means by which signals, or data, are sent from one computer to another. Signals can be transmitted either by cable or wireless means. The media types discussed were coaxial, twisted pair, fiber-optic cabling, and radio frequencies.

• Ethernet architecture is now the most popular type of LAN architecture. Architecture refers to the overall structure of a computer or communications system. It determines the capabilities and limitations of the system. The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implement the CSMA/CD access control method.

• The OSI reference model is an industry-standard framework that divides the functions of networking into seven distinct layers: application, presentation, session, transport, network, data link, and physical. It is important to understand the purpose of each layer.

• The TCP/IP suite of protocols has become the dominant standard for the Internet. TCP/IP represents a set of public standards that specify how packets of information are exchanged between computers over one or more networks.

• A NIC is a device that plugs into a motherboard and provides ports for the network cable connections. It is the computer interface with the LAN.

• Resources are shared over a network when computers belong to the same workgroup and homegroup.

• Testing network connectivity can be accomplished with CLI tools like ping, ipconfig, net, tracert, and nslookup.

• The three transmission methods to sending signals over data channels are simplex, half-duplex, and full-duplex. Full-duplex networking technology increases performance because data can be sent and received at the same time. DSL, cable, and other broadband technologies operate in full-duplex mode.

• Network devices and media, such as computer components, must be maintained. It is important to clean equipment regularly and use a proactive approach to prevent problems. Repair or replace broken equipment to prevent downtime.
• Many safety hazards are associated with network environments, devices, and media.

• Make network design decisions that will meet the needs and the goals of your customers.

• Select network components that offer the services and capabilities necessary to implement a network based on the needs of the customer.

• Plan network installations based on the needed services and equipment.

• Upgrading a network may involve additional equipment or cabling.

• Prevent network problems by developing and implementing a comprehensive preventive maintenance policy.

• When troubleshooting network problems, listen to what your customer tells you so that you can formulate open-ended and closed-ended questions that will help you determine where to begin fixing the problem. Verify obvious issues, and try quick solutions before escalating the troubleshooting process.