

LEARNING OUTCOMES:

- Students will be able to define Network Hardware
- Identify the fundamental devices of the computer network.
- Students will understand Network Architecture

OVERVIEW:

Network Hardware is the individual components of a network system that are responsible for transmitting data and facilitating the operations of a computer network. Although a network contains many hardware components, there are several basic categories that make up the complete operations of a network system. Hence are some of the different categories and how they contribute as a whole to the overall functioning of a network system.

DISCUSSION:


Network Hardware is as a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.

Today technology has penetrated its tentacles into every nook and corner of our lives. It has gone from being just an industry add-on to an inevitable necessity. As tech enablement is driving the industrial transformation, it's important for businesses to build a network that is secure, reliable and keeps the users in touch with their applications. The core of this very foundation is leveraged by the basic network hardware.

Network hardware plays a key role as industries grow as it supports scalability. It integrates any number of components depending on the enterprise's needs. Network hardware helps establish an effective mode of communication, thereby improving the business standards. It also promotes multiprocessing and enables sharing of resources, information, and software with ease.

Network equipment is part of advancement of the Ethernet network protocol and utilizes a twisted pair or fiber cable as a connection medium. Routers, hubs, switches, and bridges are some examples of network hardware.

Let's look at the **Fundamental Devices of a Computer Network.**

 **Modems** - enables a computer to connect to the internet via a telephone line. The modem at one end converts the computer's digital signals into analog signals and sends them through a telephone line. At the other, it converts

the analog signals to digital signals that are understandable for another computer.

✚ **Routers** - connects two or more networks. One common use of the router is to connect a home or office network (LAN) to the internet (WAN). It generally has a plugged in internet cable along with cables that connect computers on the LAN. Alternatively, a LAN connection can also be wireless (Wi-Fi-enabled), making the network device wireless. These are also referred to as wireless access points (WAPs).

✚ **Hubs, Bridges, and Switches** - are connecting units that allow multiple devices to connect to the router and enable data transfer to all devices on a network. A router is a complex device with the capabilities of hubs, bridges, and even switches.

- **Hubs** - a hub broadcast data to all devices on a network. As a result, it consumes a lot of bandwidth as many computers might not need to receive the broadcasted data. The hub could be useful in linking a few gaming consoles in a local multiplayer game via a wired or wireless LAN.
- **Bridges** - a bridge connects two separate LAN networks. It scans for the receiving device before sending a message. This implies that it avoids unnecessary data transfers if the receiving device is not there. Moreover, it also checks to see whether the receiving device has already received the message. These practices improve the overall performance of the network.
- **Switches** - a switch is more powerful than a hub or a bridge but performs a similar role. It stores the MAC addresses of network devices and transfers data packets only to those devices that have requested. Thus, when the demand is high, a switch becomes more efficient as it reduces the amount of latency.

✚ **Network interface card (NIC)** - is a hardware unit installed on a computer, which allow it to connect to a network. It is typically in the form of a circuit board or chip. In most modern machines, NICs are built into the motherboards, while in some computers, an extra expansion card in the form of a small circuit board is added externally.

✚ **Network cables** - cables connect different devices on a network. Today, most networks have cables over a wireless connection as they are more secure, i.e., less prone to attacks, and at the same time carry larger volumes of data per second.

✚ **Firewall** - is a hardware or software device between a computer and the rest of the network open to attackers or hackers. Thus, a LAN can be protected from hackers by placing a firewall between the LAN and the internet connection. A firewall allows authorized connections and

data-like emails or web pages to pass through but blocks unauthorized connections made to a computer or LAN.

NETWORK ARCHITECTURE

Network architecture is the design of a computer network. It framework for the specification of a networks physical components and their functional organization and configuration, its operational principles and procedures, as well as communication protocols used.

Network architecture design is more about optimizing its fundamental building blocks. These include four key components:

1. **Hardware** - refers to network devices that form the core of any network. These include user devices (laptops, PDAs, mobile phones), routers, servers, and gateways. The basic objective of any network architecture is to establish an efficient mechanism to transfer data from one hardware device to another.
2. **Transmission media** - encompasses all physical connections between network (hardware) devices. The properties of different transmission media determine the speed of data transfer from one endpoint to another. These can be wired and wireless. Wired media include physical wires or cables used for connections within a network, such as coaxial or fiber optics. On the other hand, wireless media operates on properties of microwave or radio signals, such as Wi-Fi or cellular.
3. **Protocols** - refer to the rules that govern data movement between network devices. Various machines on a network communicate with each other using this common protocol language. Without these protocols in place, it would be difficult for your iPhone to access a web page that is essentially stored on a Linux server. The nature of data decides the type of network protocol it needs to adopt. For example, transmission control protocol/internet protocol (TCP/IP) is used to connect to the internet, while file transfer protocol (FTP) is used for sending and receiving files to and from a server. Similarly, Ethernet protocol is used for connecting one computing device to another.
4. **Topology** - Network topology defines how the network is wired together and highlights the network's structure. This is important because variables such as distance between communicating devices can impact its data transfer speed, thereby affecting overall network performance. Several topologies exist, each with specific strengths and weaknesses. For example, consider a star topology. In this case, all the network devices are connected to a central hub. The strength of this

topology is such that any device can connect to the network easily. However, in situations when the central hub fails, the whole network can crash almost instantly. Another topology is that of a bus, where all devices are connected along a single pathway, termed as a bus. The bus resembles a highway that transports data from one endpoint to another. Although this topology is easy and affordable to implement, its performance can take a hit as more devices get added to the network. Today, most network architectures adopt a hybrid approach where different topologies are combined and blended to compensate for each one's weakness.

8 Challenges of Network Hardware Today

1. Physical connectivity challenges

Defective cables and connectors on a network can generate errors on the network devices to which they are connected. The problem aggravates due to a broken or malfunctioning cable. The issue can even crop up on the outside of the LAN infrastructure. Damage to a copper cable or fiber optic connector can significantly reduce the volume of data it can transfer. It can also lead to considerable packet loss.

2. Malfunctioning hardware devices

Network issues can arise due to malfunctioning network equipment, including firewalls, routers, switches, and wireless access points. The possible reasons for this could be bad configurations, faulty connections, or even disabled devices. It is essential to ensure that all the devices on the network are configured appropriately, as misconfiguration issues can affect different parts of the network, thereby impacting its performance. Such a challenge can be countered by paying close attention to all the devices and switches to verify if they are working normally.

3. DNS issues

Domain name system (DNS) is analogous to a directory for the internet, and every internet-connected device matches domain names with the IP addresses of the websites. Computers can connect to other devices via the internet and look up websites through their IP addresses. As you enter the domain name in a web browser, the DNS finds the content connected to that domain.

4. Temperature issues

Most hardware failures occur due to an abnormal spike in temperature. Abnormal heating or cooling in network units can cause the abrupt shutting down or freezing of hardware systems, which eventually results in their failure. As network devices compute large quantities of data, the optimal temperature needs to be maintained to function efficiently.

5. Ventilation problems

As the temperature of the network equipment rises, the performance and speed of its operation slow down. It can even break down in some cases. Poor ventilation arising due to inappropriate device arrangement or wrongful fan setup may not be able to tackle or handle the extra heat produced by network devices. This can worsen and have an adverse effect on network productivity.

6. Overutilization of capacity

Exploiting the surplus capacity of network equipment can slow it down considerably, thereby leading to performance lag. This is one of the prominent network hardware challenges where devices with limited computing resources are overburdened with the excess workload. Such challenges can be tackled by controlling the overutilization of device capacity by resorting to workload division and distribution among other network devices.

7. Fluctuation in power supply

Corroded cable connections or other external factors can lead to notable fluctuations in power supply. In some cases, there can be a sudden surge in power supply, which can cause unplanned outages. Such events can lead to short circuits that can impact the performance of an individual device or the entire network.

8. Battery overuse

The efficiency of a battery takes a hit once 80% of its energy is utilized. Draining the battery can cause cache data loss or a sudden device or server shutdown. Moreover, low-capacity batteries lack power efficiency and have a short shelf life. Such battery units can affect the overall capability of the device and, in turn, affect the entire network.

Top 10 Best Practices of Network Hardware Management for 2022

1. Opt for multi-vendor support

Modern networks comprise heterogeneous approaches to increase their capability compared to traditional homogeneous networks. Along with default vendor-supported systems, businesses are embracing custom-configured devices that provide specific business solutions. Thus, hardware monitoring practices should support multi-vendor devices irrespective of vendor or configuration barriers.

2. Prioritize critical alerts

Network hardware issues should be prioritized considering two factors: the criticality of the device and the significance of the underlying issue. Additionally, hardware problems are managed by several parties spread across teams and even geographies. It is crucial to push the alerts to the right teams through the right channels in such cases. This creates a well-defined fault resolution path that is properly regulated and managed and will help resolve hardware faults faster and in an optimized manner.

3. Proactively monitor and troubleshoot

Instead of resolving hardware problems after an issue occurs, practicing proactive measures to avoid hardware failure in the initial stage can save a lot of time and resources. Technicians should be alerted in advance based on preemptive hardware device monitoring and management. This will ensure that issues are addressed before they worsen and damage the organizational network.

4. Gain deeper visibility

Hardware issues require an in-depth understanding of the root cause of the problem to resolve them without impacting the network's overall performance. Hence, one has to gain deeper visibility into the performance of hardware devices to address the minutest problems. Technicians can easily diagnose and fix issues in network hardware devices if they have access to the tiniest details of the hardware devices. This not only improves hardware efficiency but ensures that the network is not affected by hardware problems.

5. Automate basic tasks

L1/L2 troubleshooting operations and fundamental maintenance tasks are quite repetitive. These are time- and resource-consuming activities. As such, automating such tasks can give technicians the liberty and more time to focus on critical hardware alerts that require immediate remedial action. Moreover, technicians also need to keep a tab on the interruptions or failures that may occur in these automated tasks. In simple words, a healthy blend of manual and automation can help in resolving hardware issues quickly.

6. Ensure clarity on hardware dependencies & processes

Failure in one hardware device implies that another device dependent on it will face significant performance degradation. In some cases, it may even lead to the failure of a series of hardware devices. Thus, to prevent total network outage, it is vital to keep track of connectivity along all the hardware devices in the network.

7. Troubleshoot cable connectivity issues

The cables used for network connections differ depending on the required connectivity type. For example, connectivity between a router and a computer is enabled with a crossover cable. Hence, it is crucial to ensure that a suitable cable is used to make a physical connection between any two network devices.

8. Handle faulty ports

In a faulty port scenario, one needs to check that the port or interface on which the link is established is not off or shut down. Verifying the duplex mode and data transfer speed can also help. Additionally, when the port is running fine, but still the problem exists, you can check the indicator lights on each device.

9. Verify traffic overload

In situations where there is more traffic than the carrying capacity at a link or interface, it may start behaving abnormally. Thus it is vital to verify traffic overload at a link or interface by inspecting the volume of data packets at a given time on the link under consideration. This ensures the smooth running of hardware devices on the network.

10. Troubleshoot routing problems

While routing data packets on a network, the possibility of fault occurrence is high. Hence, plans for resolving issues can be laid down depending on the fault type. Floating data packets from source to destination hosts can become rogue if the wrong routing protocol is used to find the route to the next hop.

EXERCISES:

1. What does network hardware mean?
2. What is network architecture?