set ns [new Simulator]

set nf [open out.nam w]

$ns namtrace-all $nf

proc finish {} {

global ns nf

$ns flush-trace

close $nf

exec nam out.nam &

exit 0

}

set n0 [$ns node]

set n1 [$ns node]

$ns duplex-link $n0 $n1 1Mb 10ms DropTail

set tcp [new Agent/TCP]

$tcp set class\_ 1

$ns attach-agent $n0 $tcp

set sink [new Agent/TCPSink]

$ns attach-agent $n1 $sink

$ns connect $tcp $sink

set ftp [new Application/FTP]

$ftp attach-agent $tcp

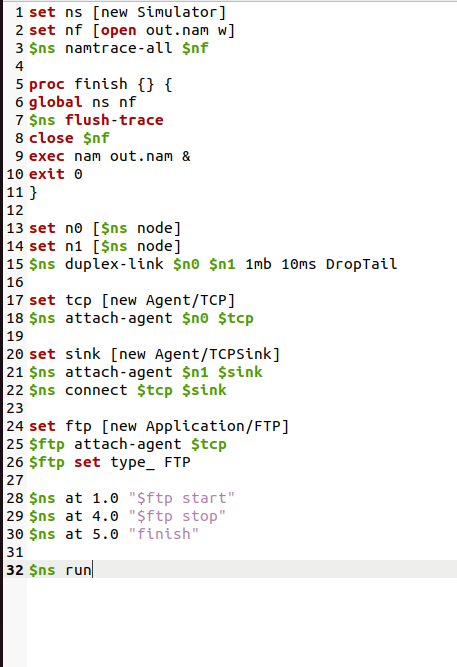
$ftp set type\_ FTP

$ns at 1.0 "$ftp start"

$ns at 4.0 "$ftp stop"

$ns at 5.0 "finish"

$ns run



Q: What is Wireshark?

A: Wireshark is a network protocol analyzer tool used for troubleshooting, analysis, and software development.

Q: How are the computers and printers in the college lab connected?

A: They are connected through a bus topology.

Q: What is the OSI model?

A: The OSI (Open Systems Interconnection) model is a conceptual model that standardizes the communication functions of a telecommunication or computing system.

Q: What is a computer network and why is it important?

A: A computer network is a group of interconnected devices that communicate with each other to share resources and information. It is important for sharing data, resources, and enabling communication and collaboration.

Q: What is the difference between LAN, MAN, and WAN?

A: LAN (Local Area Network) is a network that connects devices within a limited area, MAN (Metropolitan Area Network) is a network that connects devices within a larger area, and WAN (Wide Area Network) is a network that connects devices across a large geographical area.

Q: What is the OSI model and why is it important in computer networks?

A: The OSI model is a conceptual model that standardizes the communication functions of a telecommunication or computing system. It is important in computer networks for communication standardization and protocol development.

Q: What is TCP/IP and how does it relate to the OSI model?

A: TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of communication protocols that governs the exchange of data over the Internet. It relates to the OSI model in that both models have similar layers.

Q: What is a protocol and why is it important in computer networks?

A: A protocol is a set of rules that governs communication between devices on a network. It is important in computer networks to ensure that communication is standardized and efficient.

Q: What is a switch and how does it differ from a hub?

A: A switch is a networking device that forwards data packets between devices on a network. It differs from a hub in that it has more intelligence and can segment a network.

Q: What is a router and how does it work in a network?

A: A router is a networking device that forwards data packets between different networks. It works in a network by examining the destination address of a packet and determining the best route for it to take.

Q: What is a firewall and what is its role in network security?

A: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its role in network security is to protect against unauthorized access and attacks.

Q: What is NAT and how does it work in a network?

A: NAT (Network Address Translation) is a technique that allows devices on a private network to share a single public IP address. It works in a network by translating private IP addresses into public IP addresses.

Q: What is DNS and how does it work in a network?

A: DNS (Domain Name System) is a system that translates domain names into IP addresses. It works in a network by resolving domain names to IP addresses.

Q: What is DHCP and how does it work in a network?

A: DHCP (Dynamic Host Configuration Protocol) is a network protocol that dynamically assigns IP addresses to devices on a network. It works in a network by automatically assigning IP addresses to devices that connect to the network.

Q: What is a VPN and how does it work in a network?

A: A VPN (Virtual Private Network) is a secure network connection that allows remote access to a private network. It works in a network by encrypting data and creating a secure tunnel between the user and the network.

Q: What is wireless networking and how does it differ from wired networking?

A: Wireless networking is a type of computer networking that uses wireless signals to communicate between devices. It differs from wired networking in that it does not require physical cables to connect devices.

Q: What is the difference between IPv4 and IPv6?

A: IPv4 uses 32-bit addresses and can support up to 4.3 billion unique addresses, while IPv6 uses 128-bit addresses and can support up to 3.4×10^38 unique addresses.

Q: What is a subnet mask and how is it used in networking?

A: A subnet mask is used to divide an IP address into network and host portions. It is used in networking to determine which part of an IP address belongs to the network and which part belongs to the host.

Q: What is a gateway and how does it work in a network?

A: A gateway is a networking device that connects two different networks. It works in a network by forwarding data packets between the two networks.

Q: What is bandwidth and how is it measured?

A: Bandwidth refers to the amount of data that can be transmitted over a network in a given amount of time. It is measured in bits per second (bps) or multiples of bps such as kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).

Q: What is latency and how is it measured?

A: Latency is the amount of time it takes for a data packet to travel from its source to its destination. It is measured in milliseconds (ms) or microseconds (µs).

Q: What is a packet and how is it transmitted in a network?

A: A packet is a unit of data that is transmitted over a network. It contains information such as the source and destination addresses, as well as the data being transmitted. It is transmitted in a network by being encapsulated in headers and trailers that provide routing and error detection information.

Q: What is a MAC address and how is it used in networking?

A: A MAC (Media Access Control) address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. It is used in networking for addressing and identification purposes.

Q: In what context can we say that Wireshark is a network analyzer?

A: Wireshark can capture and analyze network traffic to help identify and troubleshoot network issues, making it a network analyzer tool.

Q: Explain all layers and their protocols in the OSI model.

A: The seven layers of the OSI model and their corresponding protocols are:

1. Physical Layer (protocols: Ethernet, Wi-Fi)
2. Data Link Layer (protocols: ARP, PPP, HDLC)
3. Network Layer (protocols: IP, ICMP, ARP)
4. Transport Layer (protocols: TCP, UDP)
5. Session Layer (protocols: SSL, TLS)
6. Presentation Layer (protocols: JPEG, MPEG)
7. Application Layer (protocols: HTTP, FTP, SMTP)

Q: What is the difference between HTTP and HTTPS?

A: HTTP (Hypertext Transfer Protocol) is a protocol used for transferring data over the web, while HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP that encrypts data using SSL/TLS to ensure secure communication.

Q: What is the difference between ipconfig and ifconfig?

A: Ipconfig is a command used in Windows to display network settings, while ifconfig is a command used in Linux/Unix-based systems to display and configure network settings.