CN Tut 1 Activity

1. What is a port?

In computer networking, a port is a virtual endpoint for data transmission, allowing multiple services to operate on a single device by distinguishing traffic intended for different applications.

2. What is a port number?

A port number is a numerical identifier in the transport layer protocols (like TCP or UDP) that specifies a particular process or service on a device, directing incoming and outgoing data to the correct application.

3. What is an ip address?

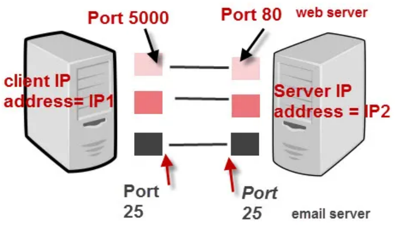
An IP address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol, serving two main functions: host identification and location addressing.

4. What is the use of ip address and port number if searched together?

Combining an IP address with a port number identifies a specific service on a particular device within a network, facilitating accurate data routing to the intended application. Together they form a socket.

5. What kind of services can be obtained by a socket?

Sockets can be used to obtain the following kinds of services:
Connection-oriented services, such as TCP: These services offer reliable, bidirectional communication between a client and a server, with guarantees about delivering data in order and without loss.
Connectionless services, such as UDP: These services are faster and offer message-based communication, but there is no guarantee of reliability or order.

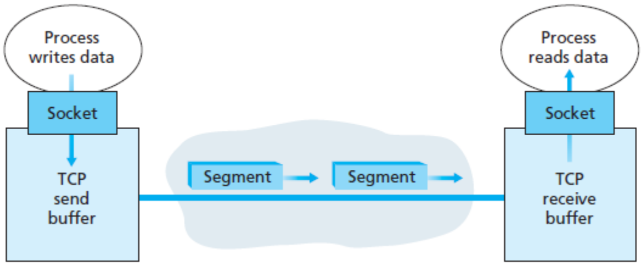


IP Address + Port number = Socket

TCP/IP Ports And Sockets

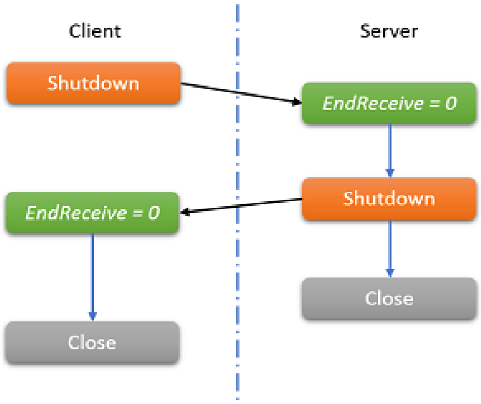
6. Mechanism to connect and disconnect:

Connection-oriented mechanism (TCP):
Connection Process:
Client sends a connection request to the server using a connect() call.
Server listens for requests using bind() and listen() and accepts the connection using accept().
A persistent connection is maintained until explicitly closed.



Reliable delivery is guaranteed.

Examples: File transfers, web browsing, and email.
Disconnection Process:
Either party can initiate disconnection using a close() or shutdown() call.



7. How can we determine the time-to-leave of a socket?

Message-based control
Applications can use ICMP messages to determine when packets are dropped because their TTL has expired.

Timeout-based control:
Set a timeout on a socket using options like SO_RCVTIMEO or SO_SNDTIMEO that limit how long a socket waits for send/receive operations.If the time-out is met, the operation fails, which indicates the TTL or response time exceeded.

Threshold-based control:
TTL can be configured explicitly by the use of the IP_TTL at the socket level so as to specify the number of hops a packet could make before being discarded.
Use C's setsockopt() or its corresponding options in the Python's socket library for TTL configuration.

Case Study: Identifying Packet Drop Rate and Network Consistency Through Cisco Packet Tracer

Introduction
The case study has been discussed on how Cisco Packet Tracer can identify the rate of a packet drop and the consistency of the network. Cisco Packet Tracer is a simulation tool used extensively in the designing and simulating network topologies, allowing the user to test and analyze network behaviors without the use of physical hardware. Through the use of several network devices, such as routers, switches, PCs, and others, in Packet Tracer, network administrators and students can replicate real-world scenarios, including packet loss, latency, and other factors that influence network performance.

Objective
The main objective of this case study is to demonstrate how Packet Tracer can help identify packet drop rates and assess network consistency under various conditions, including network congestion, faulty equipment, and misconfigured devices.

Tools and Setup
Cisco Packet Tracer: A network simulation software that can be used to design and test network topologies.
Network Devices: Routers, switches, and end devices (PCs).
Traffic Generation: Utilize tools like ping, traceroute, and traffic generators available in Packet Tracer to generate real-time network traffic.
Simulation Mode: Packet Tracer allows the user to switch between real-time mode and simulation mode, which is critical for observing packet flow, drop rates, and latency.
Steps to Determine Packet Drop Rate
Network Design:

Start with designing a simple network topology using Packet Tracer. Design a network with two routers connected to each other on both sides via a switch with multiple PCs on each side of the network.

Pretend PCs are configured to send data packets to each other in this network by using a ping command or any traffic-generating tool.

Configure IP Addresses and Routing:

Assign all devices in the network with their respective ip addresses.

Set up static or dynamic routing to ensure that packets can traverse from one end device to another. Make sure to simulate routing protocols such as OSPF or RIP, if necessary.

Traffic Generation and Monitoring:

Use the "ping" command to send ICMP packets between devices. This is the most common way to generate traffic in a network.

Enable simulation mode in Packet Tracer. From this mode, you can see every packet's route and industry.

Open the "Event List" and check if the packets are actually being transmitted without dropping or whether they are dropping.

Packet Drop Analysis

While in simulation mode, when a ping or flow of traffic is initiated, Packet Tracer displays how each packet moves through the devices in the network. A packet drop will be seen due to a problem in the network, which could be either:

Congested links

Routing of packets or networks is incorrect.

There is faulty hardware such as a malfunctioning router or switch.

Packet loss will be indicated by missing packets in "Event List" and by the messages "TTL Expired, meaning it takes too long to reach the destination.

Testing Consistency of Networks

Consistency is how steady the network can be, in terms of performance over time. You could test with multiple pings to simulate traffic over long periods. By changing the number of packets sent and the interval, you see how the network tends over different periods.

You measure the RTT for each ping. A stable network may have relatively steady RTTs, but it could be unstable, causing packets to just drop, where RTTs are not constant.

Identifying Causes of Packet Loss:

In case of packet drops, identify the following problems:

Network Congestion: Overuse of the link can result in network congestion, causing packets to be dropped.

Faulty Configuration: In case of a problem in routing tables or IP configurations, packets might be misrouted or dropped.

Hardware Problems: Network devices or links malfunctioning might be causing the packet loss.

Security Features: Firewalls or ACLs may be blocking specific traffic.

Use of Other Networks in Packet Tracer

Packet Tracer lets you simulate any network environment, whether a simple LAN or WAN, an Internet-based network, and so on, just using simulated devices. Well, there's no such direct interaction with actual networks (Kali Linux or a system in general) inside Packet Tracer, but you can:

Simulate networks using any kind of devices that behave the same as actual networks.

Integrate the simulated networks with the actual systems using VPN or other simulated protocols.

Use tools such as Wireshark or Kali Linux (used for penetration testing) in conjunction with Packet Tracer for further advanced analysis. For instance, you could run a virtual instance of Kali Linux alongside Packet Tracer and then simulate attack scenarios to test the security of your network.

Packet Tracer and Kali Linux Integration

While Packet Tracer is only meant for network simulation, Kali Linux is a mighty tool for penetration testing and security analysis. Since you cannot have Kali Linux directly integrated into Packet Tracer, there are a few ways you can have them work in tandem:

External Traffic Simulation: Run Kali Linux on a separate machine or VM and generate traffic to or from a network that Packet Tracer simulates. This allows you to see how Packet Tracer will behave in real-world traffic conditions and security scenarios.

Network Security Testing: Conduct a vulnerability test by using Kali Linux to create a DoS attack, for instance, and view how Packet Tracer will behave when a packet is lost or the network faces congestion or a routing failure.

Packet Capture Analysis: Though packet capture features are simple in Packet Tracer, you could run Wireshark on a separate Kali Linux and still capture packets flowing from the network simulated by Packet Tracer to gain an overview of what the network does - packets that dropped, latency, etc., security weaknesses, and others.

Conclusion

Cisco Packet Tracer is a great simulation and analysis tool for network performance, including packet drop rates and network consistency. With the simulation feature of Packet Tracer, one can test and troubleshoot the configuration of networks in a controlled environment. Though Packet Tracer is not supported by external network systems such as Kali Linux, their use together in a real-world testing environment could give better insights into the behavior, security, and performance of the network under various conditions.