Network Activity1:

We need to search for:

-Difference between router and switch devices.

-What is the routing table?

-What is the difference between public and private IP?

-Difference between public and private subnets

-Threat-mitigation methods

What Is a Router ?

The router is basically an interconnecting device that connects two or more computer networks. It makes use of an **internet protocol (IP)** and assumes that all of the attached devices on the networks use the same communication architecture and protocols.

What Is Switch in Networking ?

A switch is a device that provides bridging functionality with greater efficiency. A switch mainly acts as a **multiport** bridge to connect devices or segments in a LAN.
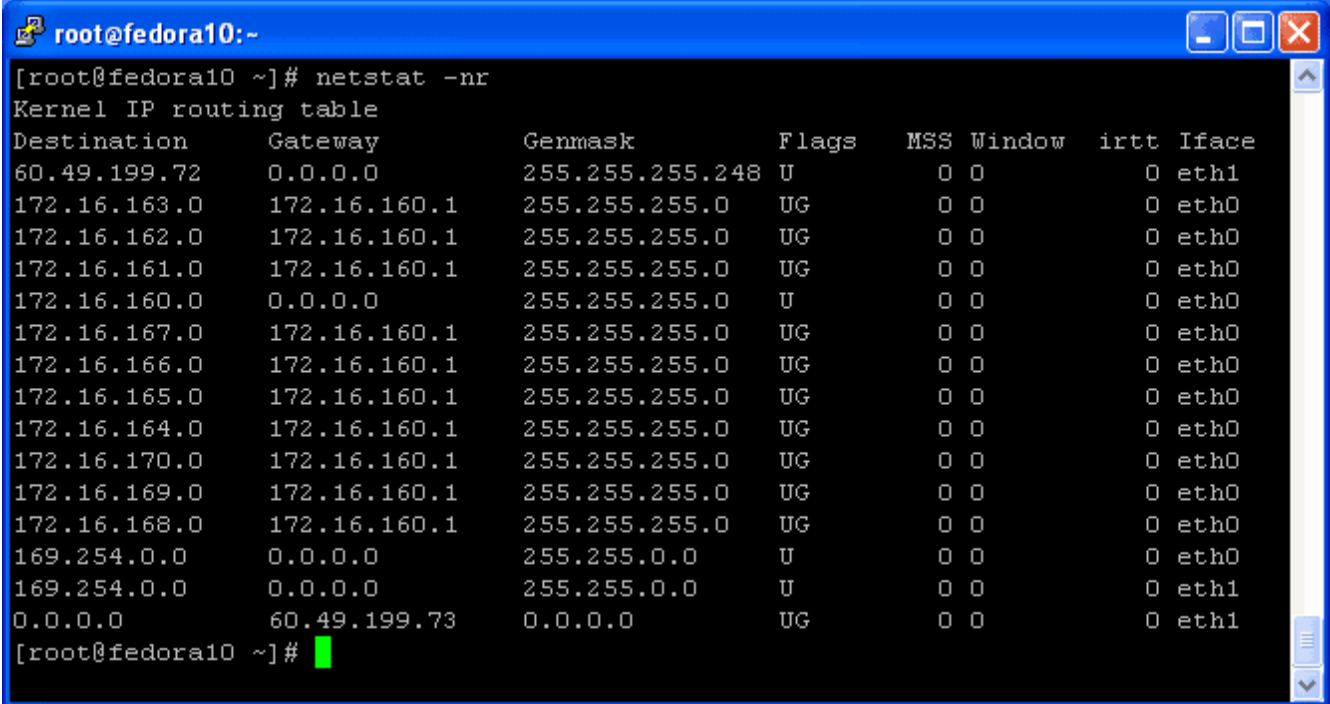
The switch has a **buffer** (refer figure below) for each link to which it is connected. When it receives any packet, it stores the packet in the buffer of the receiving link and checks for the address to find the outgoing link.

Switch

Source: https://electronicsguide4u.com/what-is-a-router-switch-and-gateway-in-networking/
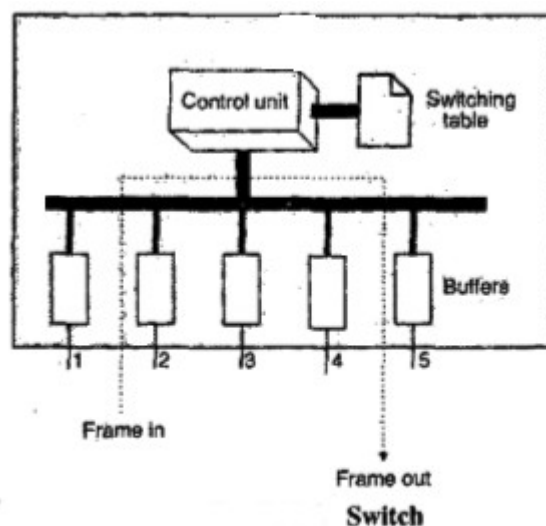
What is the routing table?

A Routing Table is an internal table that a computer or router uses to determine which router interface to send packets to, based on their destination network addresses.

```
root@fedora10:~

[root@fedora10 ~]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask          Flags   MSS Window  irtt Iface
60.49.199.72    0.0.0.0         255.255.255.248  U         0 0          0 eth1
172.16.163.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.162.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.161.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.160.0    0.0.0.0         255.255.255.0    U         0 0          0 eth0
172.16.167.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.166.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.165.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.164.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.170.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.169.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
172.16.168.0    172.16.160.1    255.255.255.0    UG        0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0      U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0      U         0 0          0 eth1
0.0.0.0         60.49.199.73    0.0.0.0          UG        0 0          0 eth1
[root@fedora10 ~]#
```

There are two different methods for populating a routing table with routes: using static routing, or dynamic routing.

Static routing

Static route is the term applied to any route in a routing table that has been manually coded (entered). For example, when the routing requirements between networks are very simple, routing tables can easily be coded directly into the host to provide all connectivity requirements.

Static routing has limitations when networks become larger. The number of routes can become difficult to manage. Also, networks can change: routers can become unavailable, causing certain routes to be unusable. At the same time, new routes can become available and these must manually be added to the routing table before they can be utilized. To overcome such limitations, dynamic routing can be used.

Dynamic routing

Dynamic routing involves the usage of routing protocols to communicate information about the status of routes and interfaces. z/OS supports two types of dynamic routing protocols: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Sources:

https://networkencyclopedia.com/routing-table/

https://www.ibm.com/docs/en/zos-basic-skills?topic=layer-routing-tables-protocols

What is the difference between public and private IP?

Key Difference: Private IP addresses are the addresses used for identification of a device within a network. They are not valid on the internet. On the other hand, Public IP addresses are for the devices accessible on the internet.
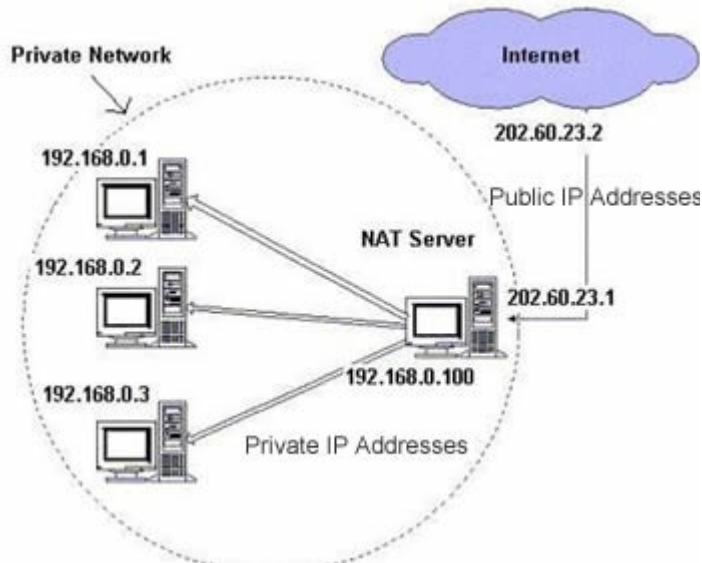
IP address or Internet Protocol is the number which acts as an identifier for the devices connected together in a computer network. Computers use IP addresses to identify each other and data is sent from one computer the other. It is a unique or exclusive number. This number is also known as IP number.

Public IP addresses include all other IP addresses which do not include any of the private IP addresses reserved by Internet standard groups. It can be accessed over the internet. A device is only accessible within a local area network by using a private IP address. However, if one of the devices in LAN wants to be accessible over the internet, then in that case this device must be connected to the internet by using a public IP address.

Comparison between Public IP and Private IP address:

	Public IP Address	**Private IP Address**
Definition	Used for identification of a home network to the outside world	Used for identification of a network device inside the home network
Uniqueness	It is unique throughout the entire network	Two or more separate networks can have same private IP addresses assigned to different computers
Example	202.60.23.1	192.168.0.3
Usage	Used on the Internet or other WAN	Used on a Local Area Network; for computers not directly connected to the internet

source: http://www.differencebetween.info/difference-between-public-ip-and-private-ip-address

Difference between public and private subnets:

Public Subnet

A public subnet will be used for instances that need a public IP to be accessible from the internet. The way we make it a public subnet is to associate a custom route table and add a route to the internet, with an internet gateway as a target.

In a Public Subnet:

- Communication is allowed from subnet to internet.
- Communication is allowed from internet to subnet.

A private subnet is used for instances that do not need to be directly reachable from the internet. For the best security, it's important to keep backend instances and databases private.

Public Subnet vs Private Subnet

Any subnet which has a route to an internet gateway is called a **public subnet**.

An **Internet Gateway** enables internet communication for subnets.

Any subnet which **DOES NOT** have route to an internet gateway is called a **private subnet**

sources:

https://www.oreilly.com/library/view/designing-aws-environments/9781789535549/fa751615-4bb5-4d85-b1a7-00808ec69533.xhtml

https://cloud.in28minutes.com/aws-certification-public-subnet-vs-private-subnet

Threat-mitigation methods:

Mitigation strategies are used by many companies and public-sector entities to isolate and minimize the damage or impact of a threat until a problem can be counter-measured. As such, these strategies vary however the National Security Agency (NSA) of the US Government utilizes a list of its Top 10 Cybersecurity Mitigation Strategies:

- Update and Upgrade Software Immediately
- Defend Privileges and Accounts
- Enforce Signed Software Execution Policies
- Exercise a System Recovery Plan
- Actively Manage Systems and Configurations
- Continuously Hunt for Network Intrusions
- Leverage Modern Hardware Security Features
- Segregate Networks Using Application-Aware Defenses
- Integrate Threat Reputation Services
- Transition to Multi-Factor Authentication

source:

https://www.hypr.com/mitigation/