System and Network Administration

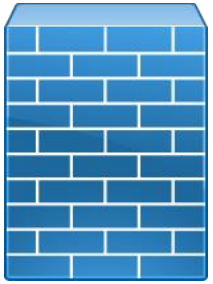
Network Hardware

Virtual ethernet interfaces

Network Devices

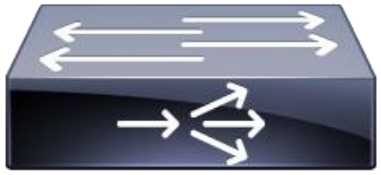
Router

Proxy



Firewall

Switch



Load balancer

Switches

Switch: A device with multiple network ports that combines multiple physical network segments into a single logical network.

- Creates dedicated connections involving only two hosts in a transmission.
- Sends individual packets to specific destination host based on their physical (MAC) addresses.
- Security protections provided by switches:
  - Can limit access to specific ports based on MAC address.
  - Can implement flood guards to protect against DoS attacks.
  - Can implement loop prevention to shut down network loops.

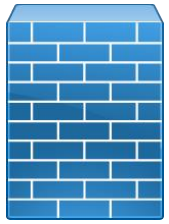
Routers

Router: A device that connects multiple networks that use the same protocol.

- Can determine most efficient path for network traffic to take.
- Most routers will not forward broadcast traffic.

Access control list: A set of rules for blocking or allowing traffic.

- Router can filter network traffic through **ACLs** and block unwanted traffic.
- One type of Firewall technique



Proxy

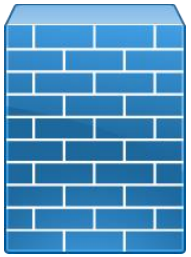
A device that acts on behalf of one end of a network connection when communicating with the other end of the connection.

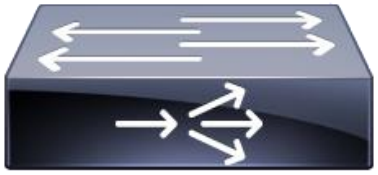
- Used as a way to filter content.
- Forward proxies intercept client traffic before it leaves the internal network.
- Reverse proxies intercept traffic coming from an external network.
  - Intended to protect destination servers from compromise.
- Proxies can modify traffic or just forward it.
- Some proxies are multi-purpose and have application-level awareness.

Firewall

Firewall: A device that protects a system or network by blocking unwanted traffic.

- Predefined rule sets (**ACLs**) determine what traffic to block.
- Connection information can be saved to a log for monitoring.
- Types of firewalls:
  - Host-based
  - Network-based
  - Web application



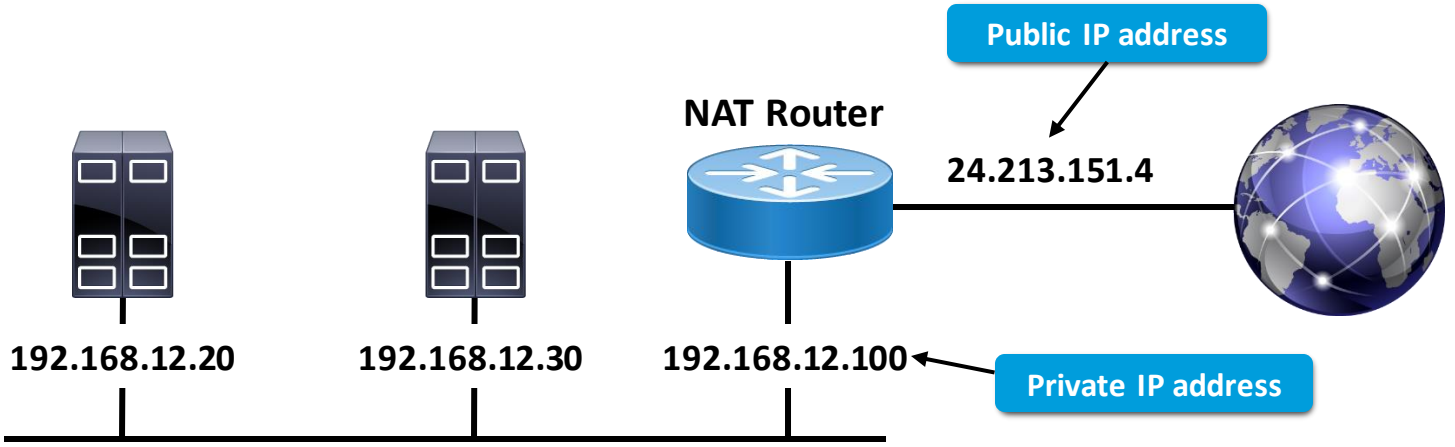


Load Balancer: A device that distributes traffics to various servers to balance CPU and memory use

Network Address Translation

A service that translates between different IP addressing schemes, such as between public and private IP addresses.

- Offers simple security by concealing internal addresses from the Internet.
- Packets sent by router to the Internet appear to come from the public address.




Q
&
A

Virtual ethif

- Virtual interfaces allows you to use multiple IPs on a single physical network interface
- The main advantage is that you don't need to have a physical adapter for each IP, but instead you can create multiple virtual interfaces (aliases) for a single physical card.
- Done to allow webservers to host multiple SSL encrypted web sites on a single webserver, or to allow VPNs to communicate on a dedicated IP address
- Two primary means of creating virtual IPs on a Linux host:
  - Ifconfig
  - iproute2

Virtual ethif - ifconfig

- Assuming that the interface being used is eth1, This command will create a virtual interface for eth0 with a name of eth1:0

```
ifconfig eth1:0 192.168.1.28
```

- This command creates an apparent separate device from eth1 with it's own IP address, netmask, and broadcast address.
- no gateway – usually only one gateway per machine.
- To remove it use ifconfig with the down option for the device:

```
ifconfig eth1:0 down
```

Virtual ethif - ifconfig

- Update the routing table using arping, to bind the physical interface MAC to the virtual interface IP address

```
arping -q -U -c 3 -I eth1 192.168.1.28
```

- This can now be used to host services and servers, fielding connections to clients or other hosts.
- These changes made will be lost when the machine is rebooted.
  - Add the commands to the network up and down scripts

Virtual ethif - iproute2

- The iproute tool set is tremendously powerful: one can easily perform complex tasks on the network stack of any Linux host with this tool
- Its power is its great flexibility, and with great flexibility comes great complexity - however, it has particular advantages for managing virtual interfaces
- The description of the ip command from the man pages describes this suite well:

ip - show / manipulate routing, devices, policy routing and tunnels

Virtual ethif - iproute2

- To create a virtual interface

```
ip addr add 192.168.1.28 dev eth1
```

- To see all IP addresses that are assigned to an interface

```
ip addr show dev eth1
```

- Or leave off `dev ethN` to get the same for all interfaces on the system (it is not possible to do this with ifconfig)
- To remove the virtual interface

```
ip addr del 192.168.1.28/32 dev eth1
```

- Note that the device must be specified when creating and deleting. While the subnet mask may be specified for the deletion, it is not required.


Q
&
A