Introduction to Network Isolation

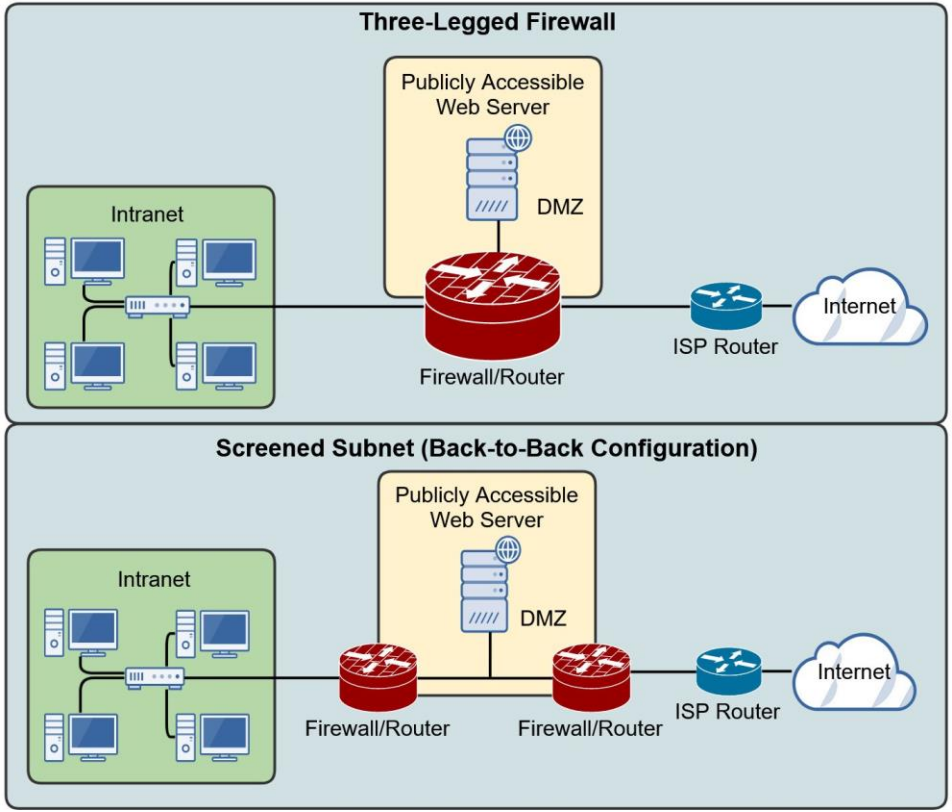
Network Segmentation & Isolation

- Network isolation, commonly referred to as network segmentation, is the process of breaking a large network up into separate smaller network segments.
- The goal is to be able to provide granular access control for each segment.
- We can accomplish this with:
  - Routers
  - Virtual LANs (VLANs)
  - Perimeter Networks (DMZ, Extranet)
  - Access Control Lists (ACLs)
  - And Additional Measures...

Demilitarized Zone (DMZ)

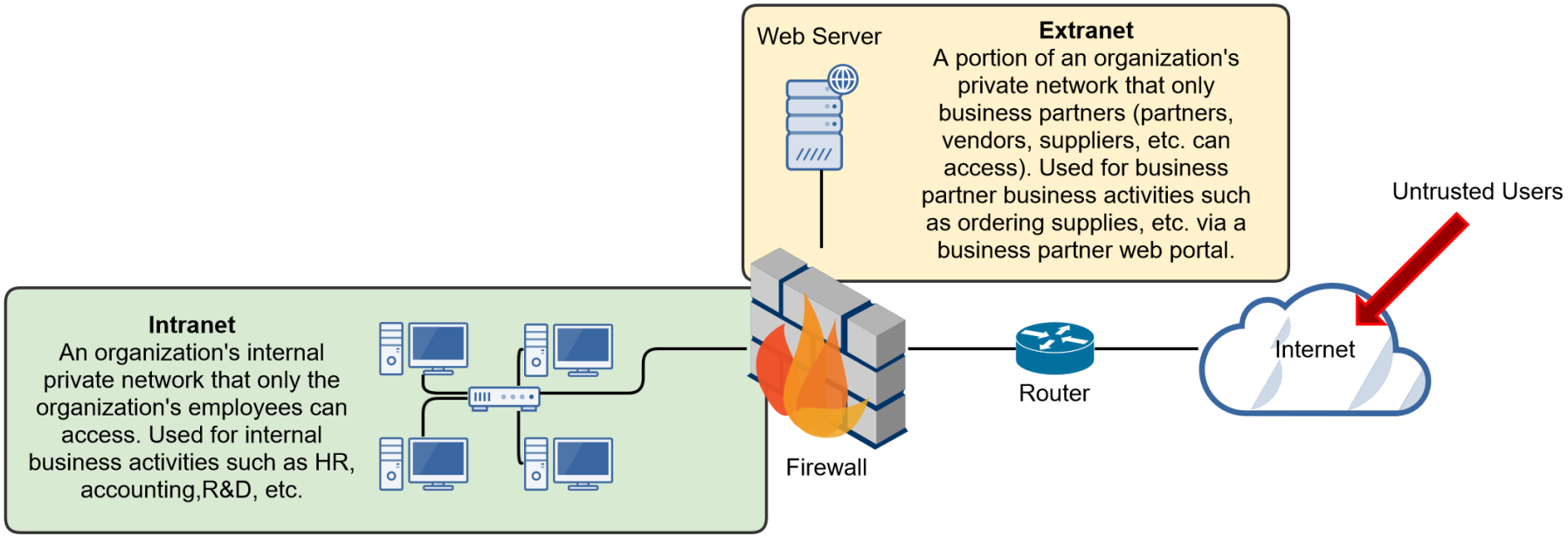
Demilitarized Zone (DMZ)

- A perimeter network designed to be securely separated from an organization's private internal network (intranet).
- Commonly called a DMZ (demilitarized zone).
- Allows untrusted users outside an organization's LAN (intranet) to access specific services located within the DMZ.
  - Public Web Site(s)
  - Trivial FTP Server for File Downloads (drivers, software, etc.)
  - Public Email Service (Gmail, etc.)
- Also blocks such users from gaining access to the organization's intranet.



Basic Network Zones

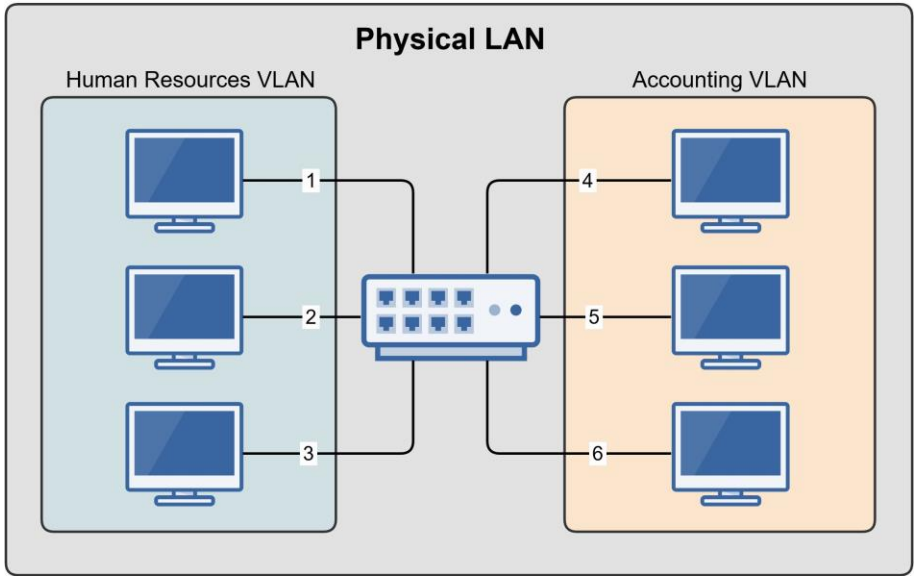
Intranet, Extranet and the Internet



Virtual LANs (VLANs)

Virtual LANs (VLANs)

- Essentially LANs within a LAN
  - Physical Switch → Multiple Virtual Switches
- Break up a large “physical” LAN into several smaller “logical” LANs.
- Accomplished with managed switches.
- Assign specific switch interfaces (ports) to specific virtual LANs.
  - Human Resource VLAN (Interfaces 1, 2, 3)
  - Accounting VLAN (Interfaces 4, 5, 6)
- Benefits of VLANs
  - Reduces Broadcast Domains
  - Segments Network by Role
  - Increases Security
  - Devices Cannot Communicate with Other VLANs
  - Group Devices by Need, Not Physical Location

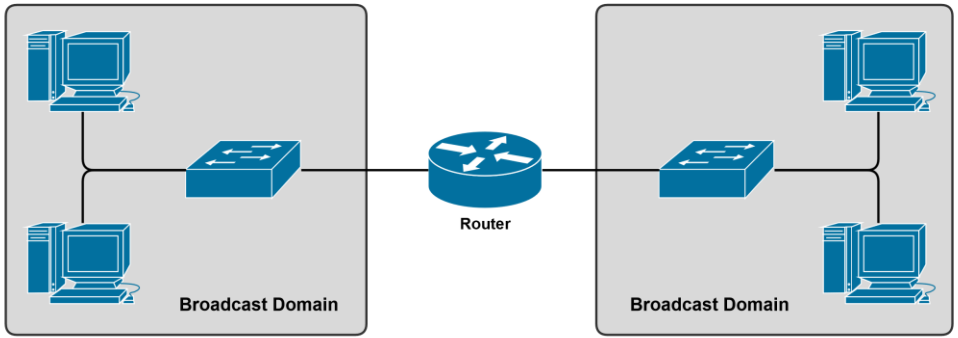


Routers

INSTRUCTOR
ALTON

Routers

- Used to Connect Different Networks Together
- Routes Traffic Between Networks using **IP Addresses**
- Uses Intelligent Decisions (Routing Protocols) to Find the Best Way to Get a Packet of Information from One Network to Another.
- **OSI Layer 3 Device**
  - Layer 3 = Router
  - Layer 2 = Switch
  - Layer 1 = Hub

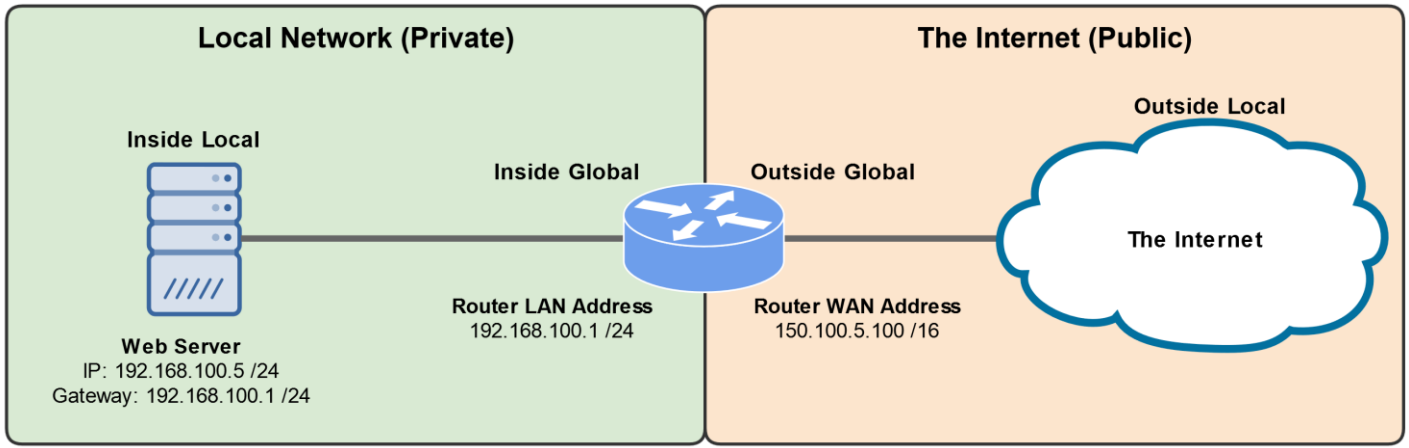


Network Address Translation (NAT)

Network Address Translation (NAT)

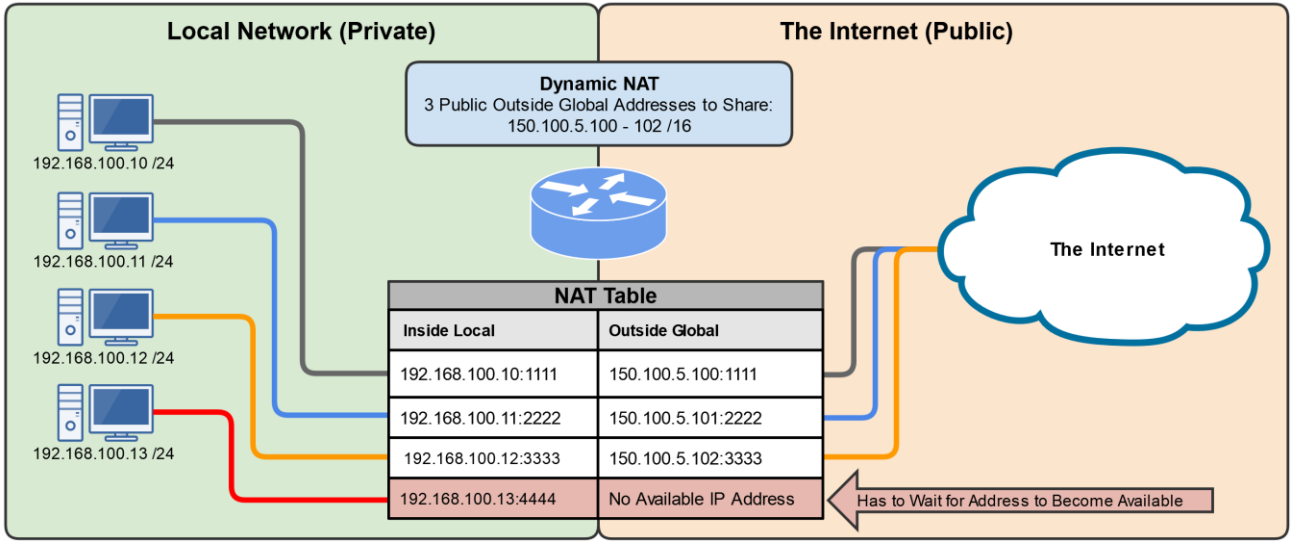
- NAT translates private IP addresses to public IP addresses, allowing us to map private IP addresses to public IP addresses:
  - To help preserve scarce public IPv4 addresses
  - To help increase network security
- With NAT, the private IP address of a network device is hidden from devices outside of its LAN.
- Three are three forms of NAT:
  - Static NAT (SNAT)
  - Dynamic NAT (DNAT)
  - Port Address Translation (PAT)
- Border network devices, such as routers, proxy servers, and firewalls can utilize NAT.

Static NAT (SNAT)



- One-to-One relationship, where one private IP is statically configured to one public IP address.
- Commonly used as a means to “hide” the IP address of a publicly available device, such as a web server.

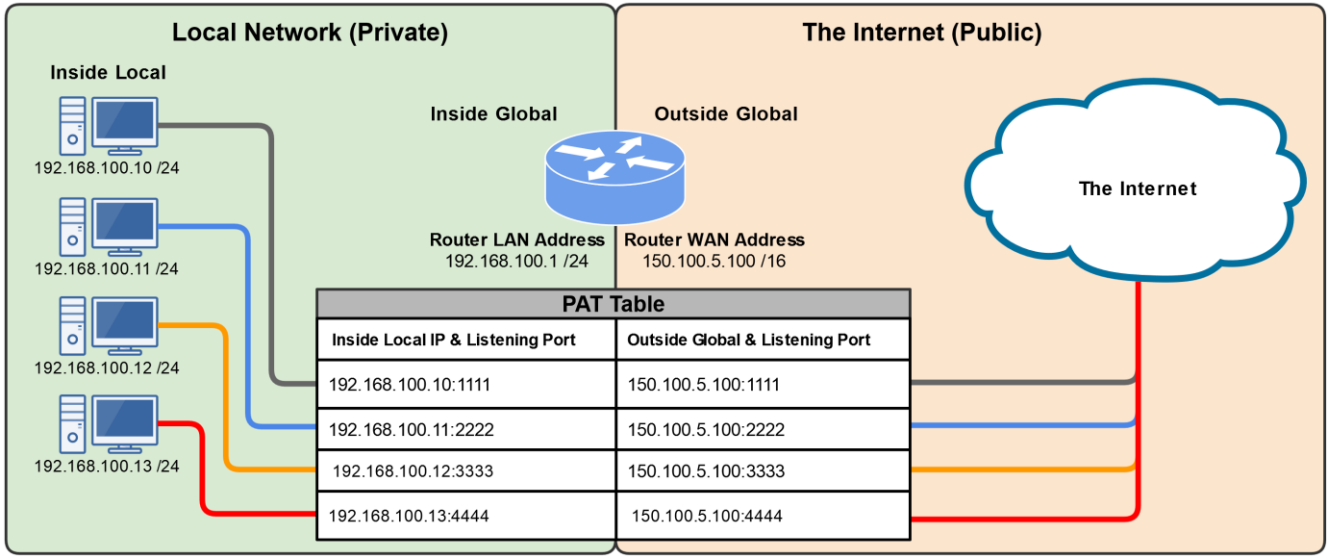
Dynamic NAT (DNAT)



- Many-to-Many relationship, where many private IP addresses have access to a pool of public IP addresses.
- If the pool of IP addresses is all in-use, other devices in the local private network must wait for them to become available.

INSTRUCTOR
ALTON

Port Address Translation (PAT)



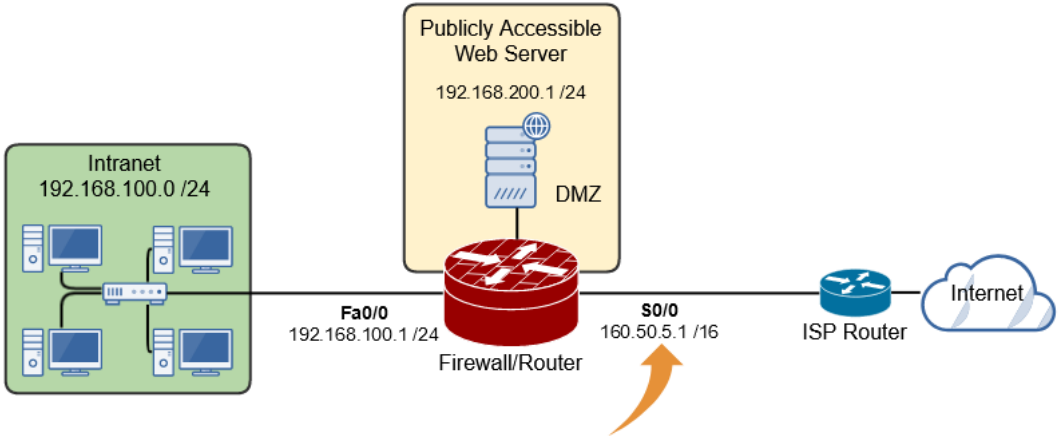
- Many-to-One relationship, where all devices on the local private network utilize a single public IP Addresses.
- Ports are used to link each connection to a specific dynamic port number.
- Very common in small business and home networks.

Access Control Lists (ACLs)

INSTRUCTOR
ALTON

Access Control Lists (ACLs)

- Access Control Lists are a network security feature used to create allow/deny network rules to filter network traffic.
- They can be set for both incoming and outgoing traffic on a variety of devices, such as:
  - Routers
  - Firewalls
  - Proxy Servers
  - End-Devices



Interface	IP Address	Port	Rule
S0/0	192.168.100.0 - 255 /24	0 - 65535	Deny
S0/0	192.168.200.1 /24	0 - 79, 81 - 65535	Deny
S0/0	192.168.200.1 /24	80	Permit