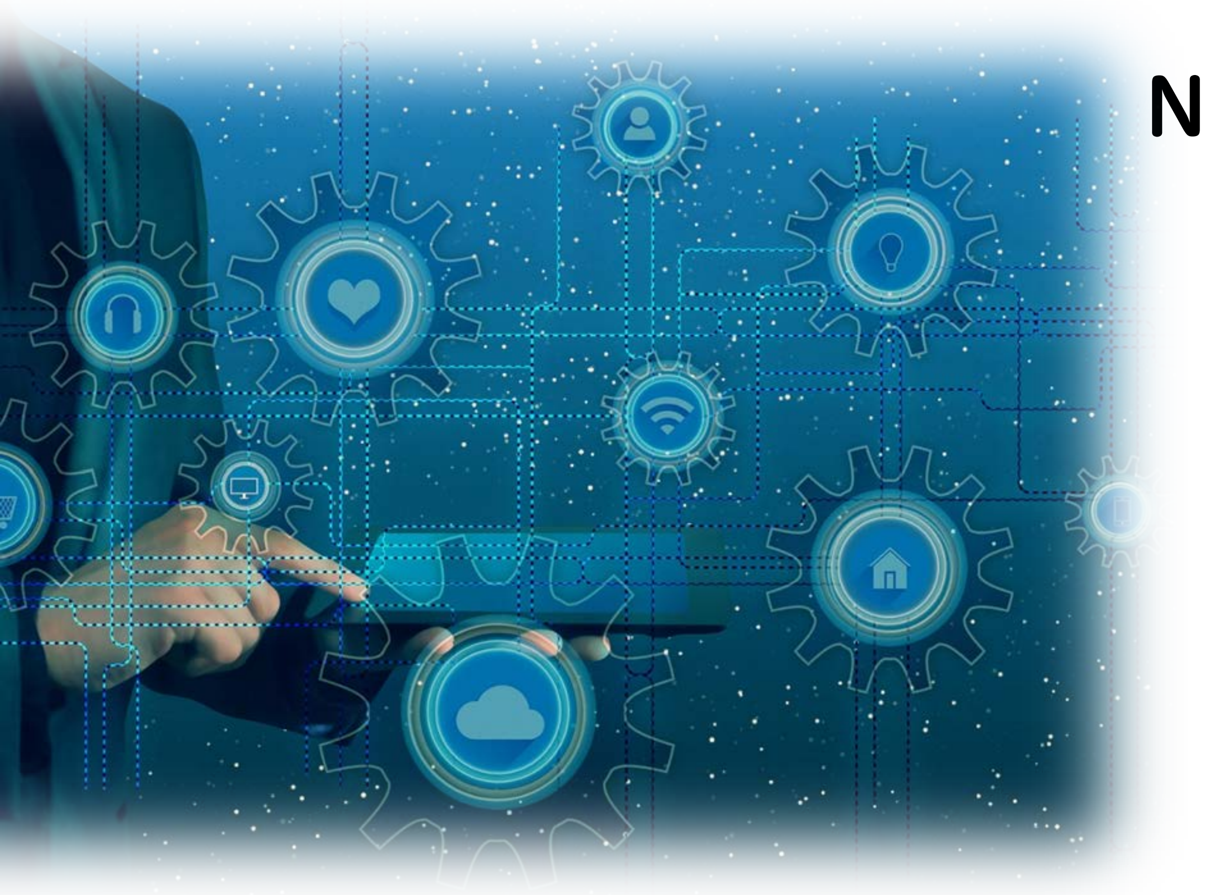
Lecture 4
Network Address Translation

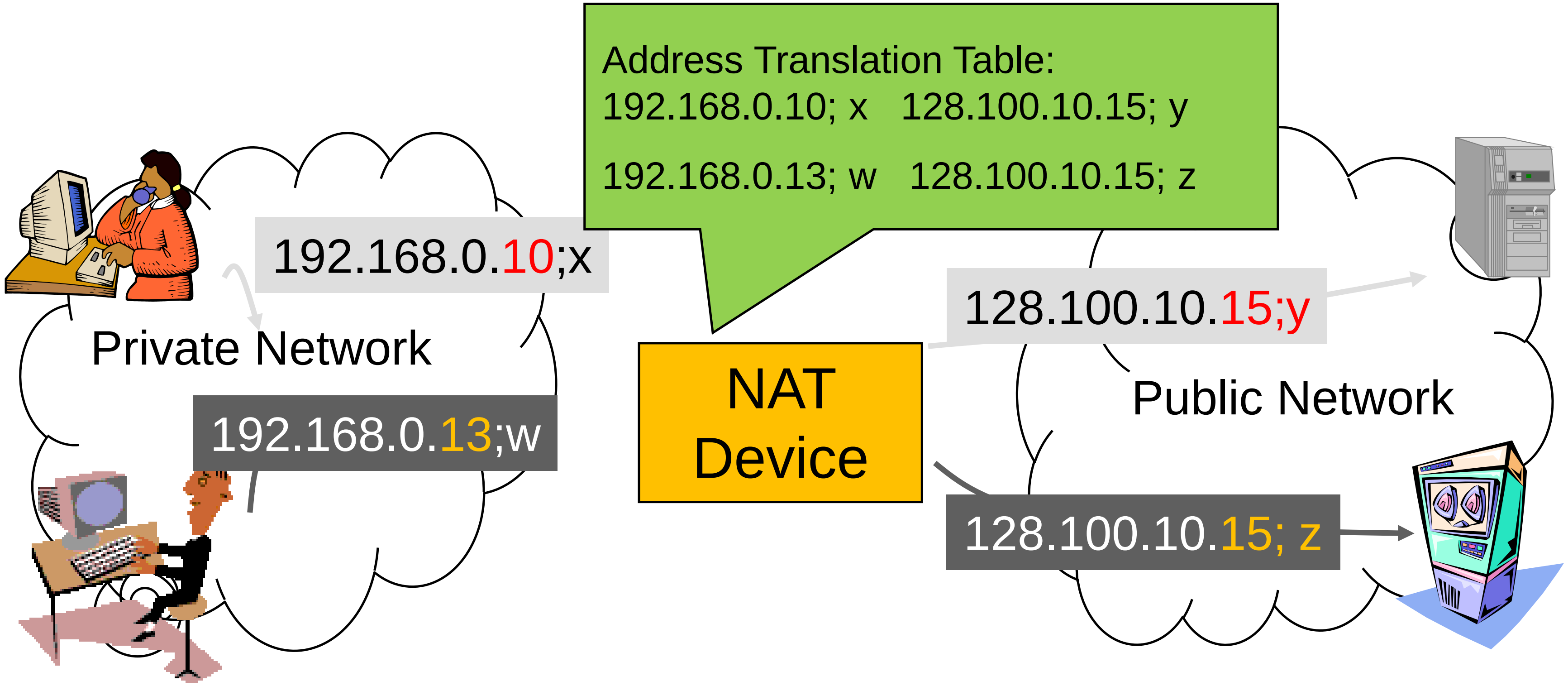


Network Address Translation

Network Address Translation (NAT)

- Class A, B, and C addresses have been set aside for use within private internets
  - Packets with private (“unregistered”) addresses are discarded by routers in the global Internet
- NAT (RFC 1631): method for mapping packets from hosts in private internets into packets that can traverse the Internet
  - A device (computer, router, firewall) acts as an agent between a private network and a public network
  - A number of hosts can share a limited number of registered IP addresses
    - Static/Dynamic NAT: map unregistered addresses to registered addresses
    - Overloading: maps multiple unregistered addresses into a single registered address (e.g. Home LAN)

NAT Operation (Overloading)



- **Hosts inside private networks generate packets with private IP address & TCP/UDP port #s**
- **NAT maps each private IP address & port # into shared global IP address & available port #**
- **Translation table allows packets to be routed unambiguously**

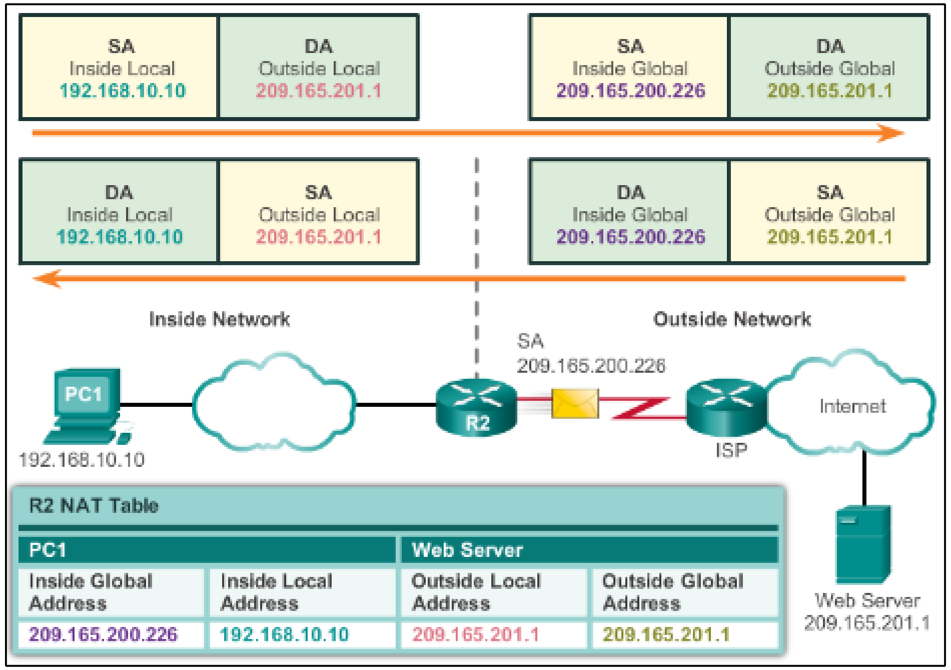
Routable and Nonroutable Addresses

- Nonroutable Address [RFC 1918]
    - Internet Router ignore the following addresses.
        - 10.0.0.0 – 10.255.255.255
        - 172.16.0.0 – 172.31.255.255
        - 192.168.0.0 – 192.168.255.255
    - Millions of networks can exist with the same nonroutable address.
    - “Intranet” : Internal Internet
    - NAT (Network Address Translation) router
    - Side benefit : “Security”

NAT Operation

NAT Characteristics

- IPv4 Private Address Space
  - 10.0.0.0 /8, 172.16.0.0 /12, and 192.168.0.0 /16
- What is NAT?
  - Process to translate network IPv4 address
  - Conserve public IPv4 addresses
  - Configured at the border router for translation
- NAT Terminology
  - Inside address
    - Inside local address
    - Inside global address
  - Outside address
    - Outside local address
    - Outside global address



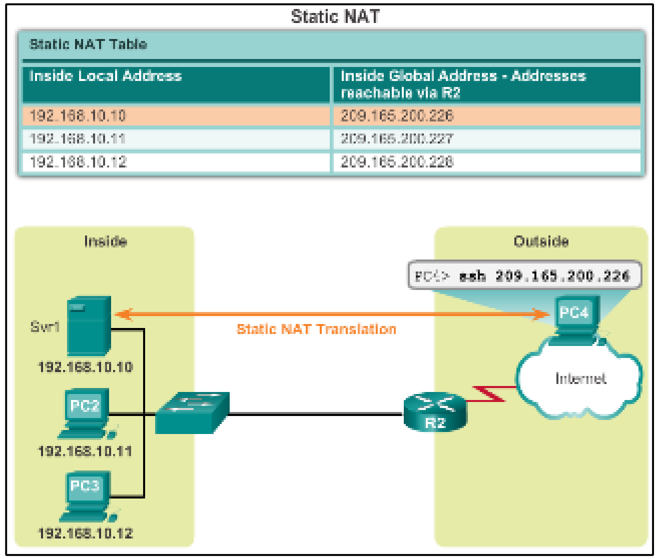
R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

NAT Operation

Types of NAT

- Static NAT
  - One-to-one mapping of local and global addresses
  - Configured by the network administrator and remain constant.
- Dynamic NAT
  - Uses a pool of public addresses and assigns them on a first-come, first-served basis
  - Requires that enough public addresses for the total number of simultaneous user sessions
- Port Address Translation (PAT)
  - Maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
  - Also known as NAT overload
  - Validates that the incoming packets were requested
  - Uses port numbers to forward the response packets to the correct internal device

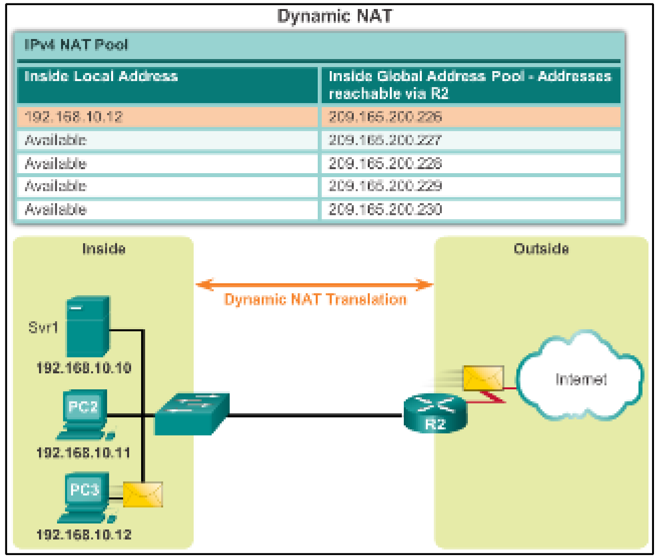


Static NAT

Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

```
PC4> ssh 209.165.200.226
```



Dynamic NAT

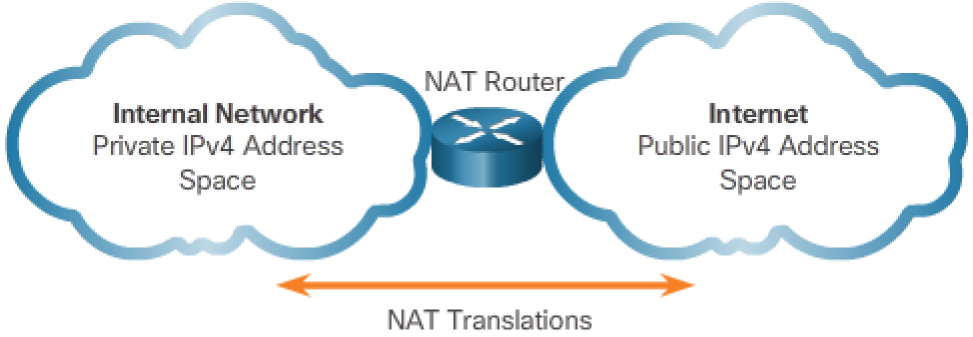
IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

NAT Operation

NAT Advantages

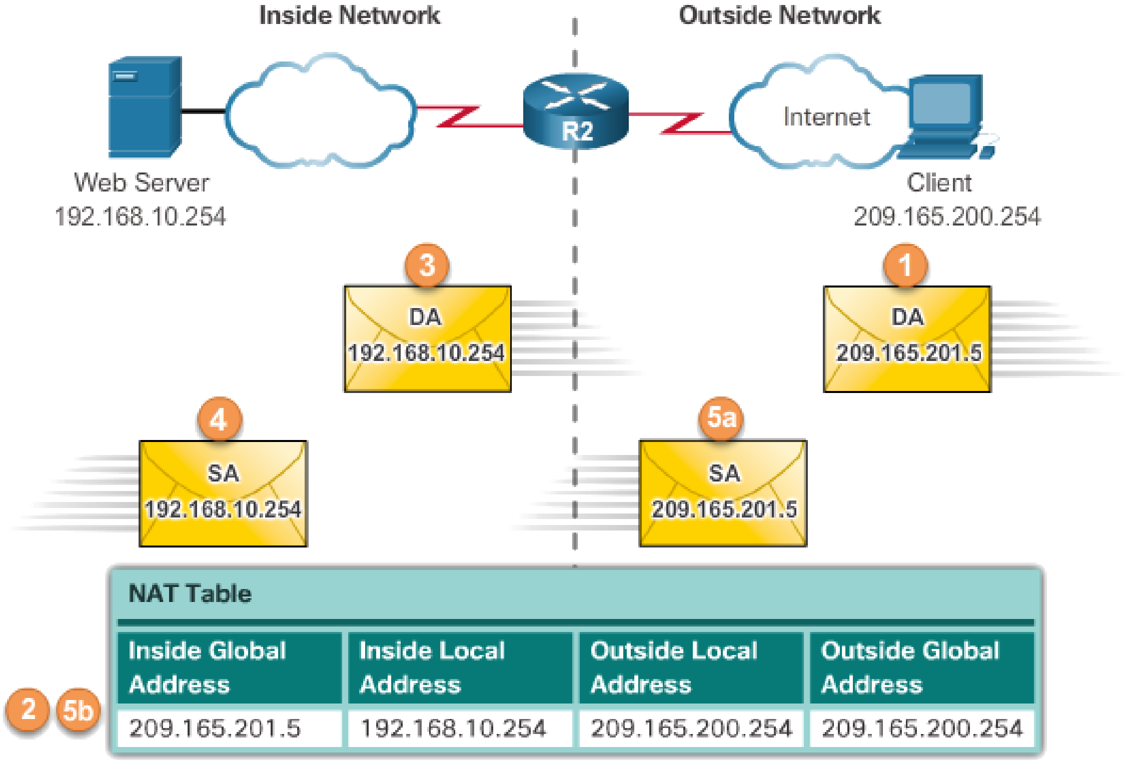
- Advantages of NAT
  - Conserves the legally registered addressing scheme
  - Increases the flexibility of connections to the public network
  - Provides consistency for internal network addressing schemes
  - Provides network security
- Disadvantages of NAT
  - Performance is degraded
  - End-to-end functionality is degraded
  - End-to-end IP traceability is lost
  - Tunneling is more complicated
  - Initiating TCP connections can be disrupted



Configuring Static NAT

- Configuring Static NAT
  - Create the mapping between the inside local and inside global addresses
    - `ip nat inside source static` *`local-ip global-ip`*
  - Define which interfaces belong to the inside network and which belong to the outside network
    - `ip nat inside`
    - `ip nat outside`
- Analyzing Static NAT
- Verifying Static NAT

```
show ip nat translations
show ip nat statistics
clear ip nat statistics
```

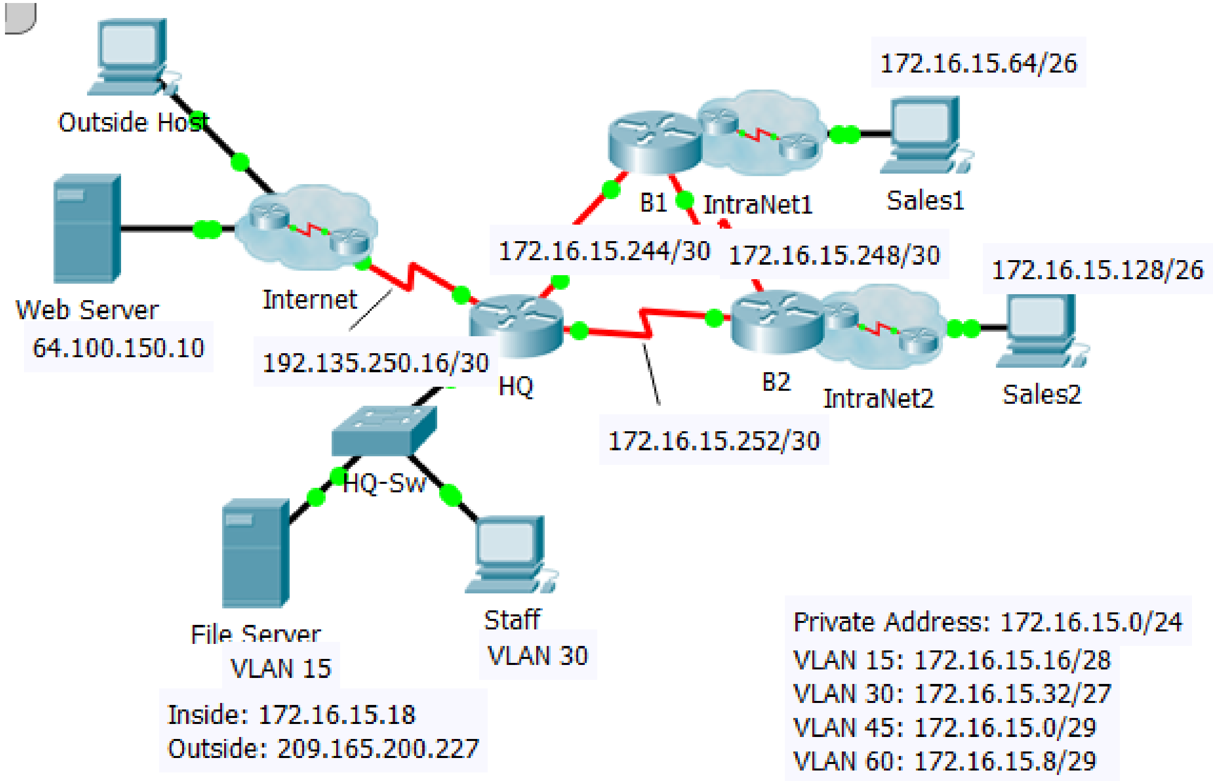


NAT Table

Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.201.5	192.168.10.254	209.165.200.254	209.165.200.254

NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
```



Inside: 172.16.15.18
Outside: 209.165.200.227

Private Address: 172.16.15.0/24
VLAN 15: 172.16.15.16/28
VLAN 30: 172.16.15.32/27
VLAN 45: 172.16.15.0/29
VLAN 60: 172.16.15.8/29

Configuring Dynamic NAT

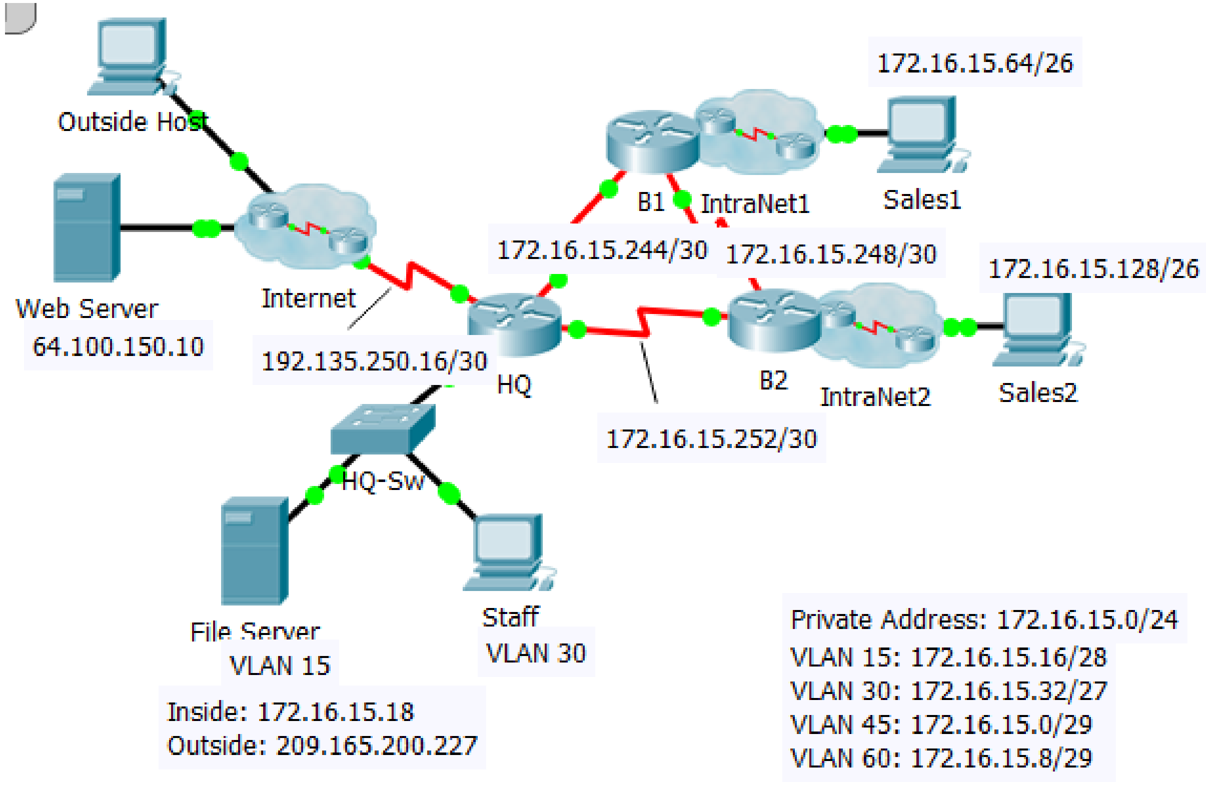
- Dynamic NAT Operation
  - The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come, first-served basis.
  - With dynamic NAT, a single inside address is translated to a single outside address.
  - The pool must be large enough to accommodate all inside devices.
  - A device is unable to communicate to any external networks if no addresses are available in the pool.

Configuring Dynamic NAT (Cont.)

- Configuring Dynamic NAT
  - Create the mapping between the inside local and inside global addresses
    - **`ip nat pool`** *`name start-ip end-ip`* `{`**`netmask`** *`netmask`* `|` **`prefix-length`** *`prefix-length`*`}`
  - Create a standard ACL to permit those addresses to be translated
    - **`access-list`** *`access-list-number`* **`permit`** *`source`* `[`*`source-wildcard`*`]`
  - Bind the ACL to the pool
    - **`ip nat inside source list`** *`access-list-number`* **`pool`** *`name`*
  - Identify the inside and outside interfaces
    - **`ip nat inside`**
    - **`ip nat outside`**

NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
```



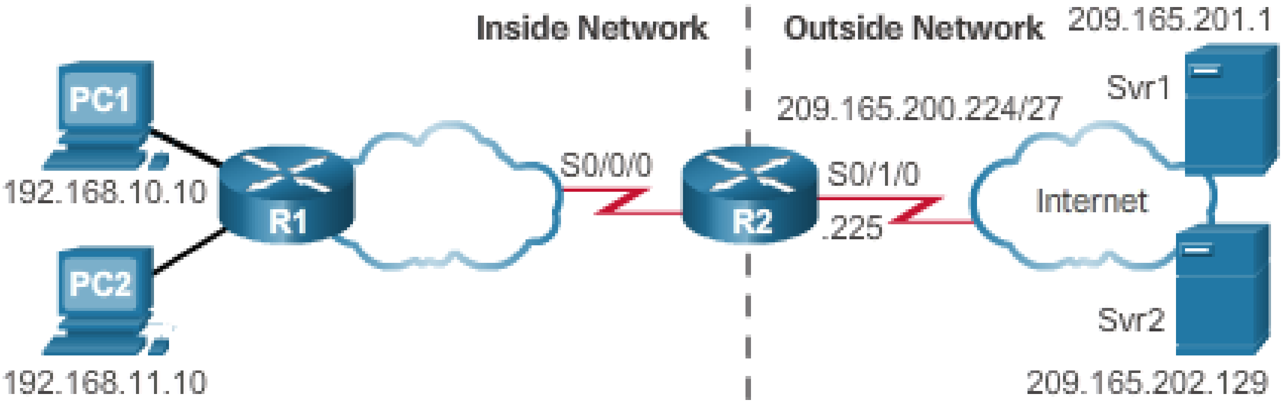
Inside: 172.16.15.18
Outside: 209.165.200.227

Private Address: 172.16.15.0/24
VLAN 15: 172.16.15.16/28
VLAN 30: 172.16.15.32/27
VLAN 45: 172.16.15.0/29
VLAN 60: 172.16.15.8/29

Configuring Port Address Translations (PAT)

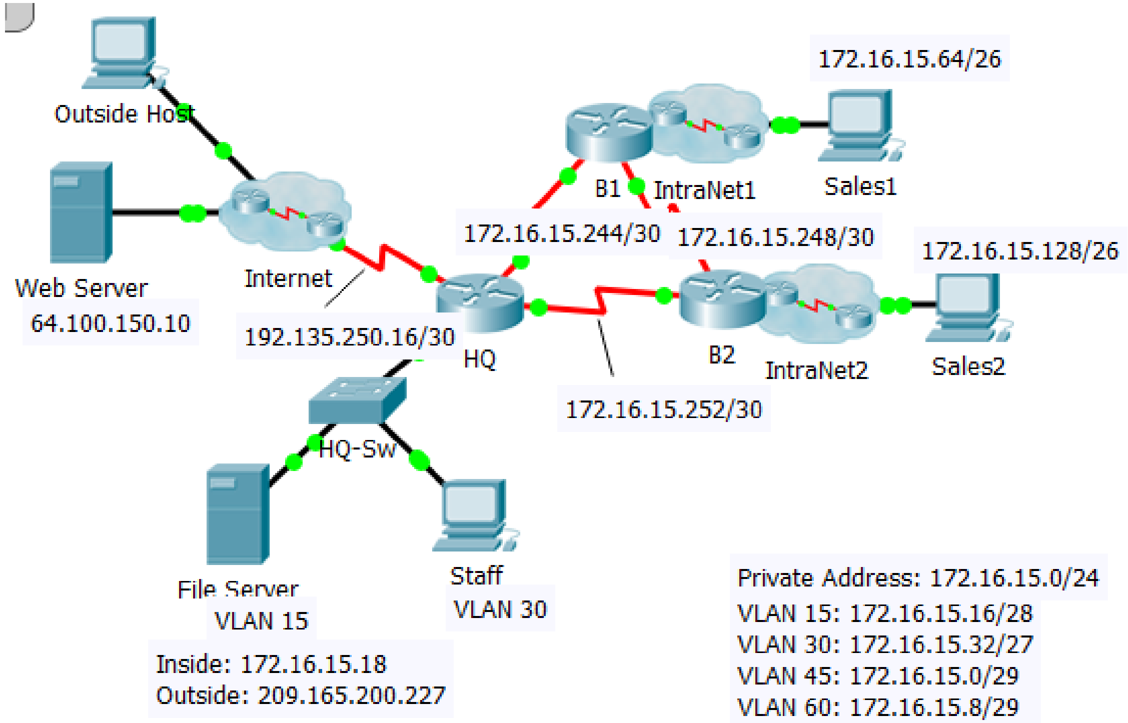
- Configuring PAT: Address Pool
  - Create the mapping between the inside local and inside global addresses
    - **ip nat pool name** *start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
  - Create a standard ACL to permit those addresses to be translated
    - **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
  - Bind the ACL to the pool
    - **ip nat inside source list** ***access-list-number*** **pool** ***name*** ***overload***
  - Identify the inside and outside interfaces
    - **ip nat inside**
    - **ip nat outside**

Example PAT with Address Pool



NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
```



Inside: 172.16.15.18
Outside: 209.165.200.227

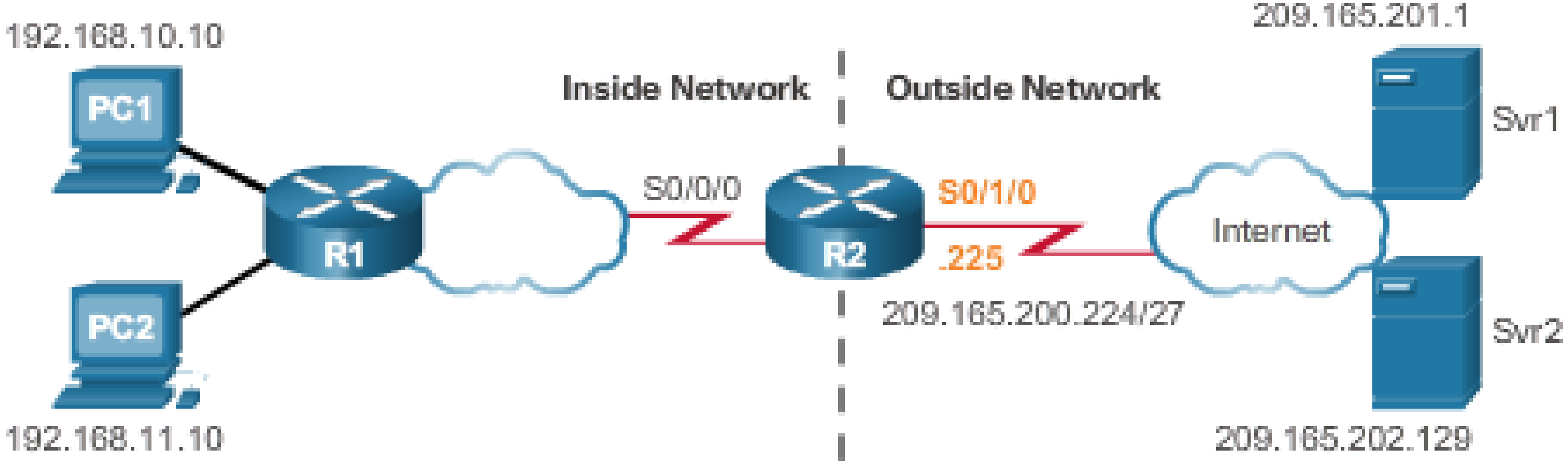
Private Address: 172.16.15.0/24
VLAN 15: 172.16.15.16/28
VLAN 30: 172.16.15.32/27
VLAN 45: 172.16.15.0/29
VLAN 60: 172.16.15.8/29

Configuring NAT

Configuring Port Address Translations(PAT)(Cont.)

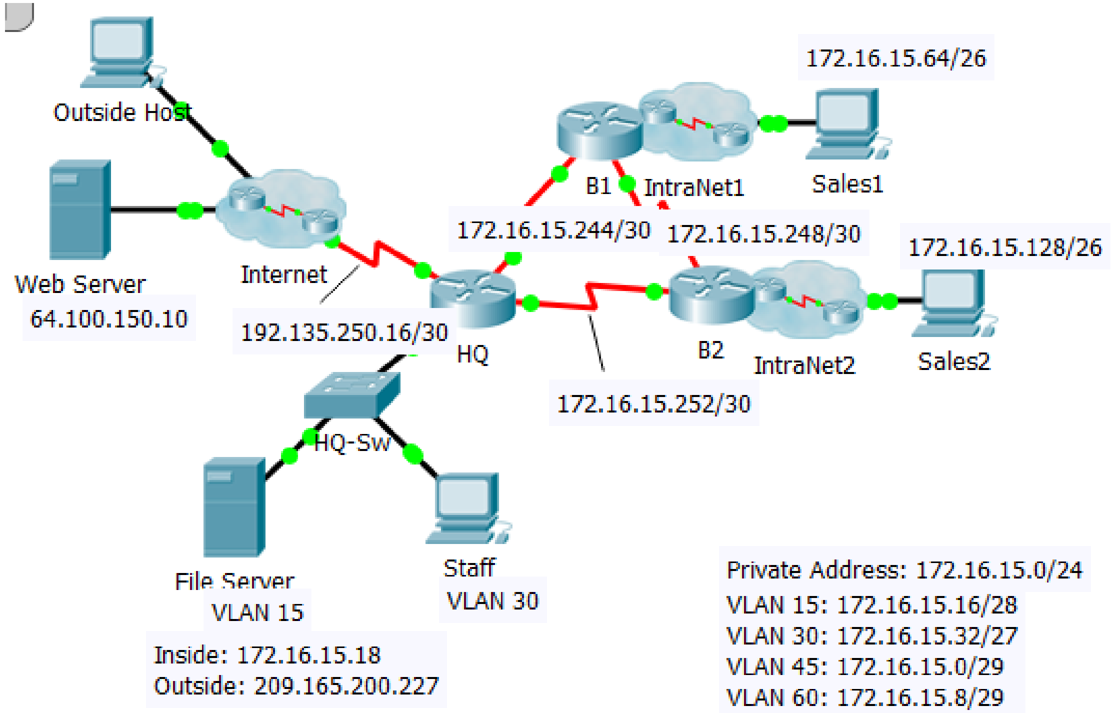
- Configuring PAT: Single Address
  - Define a standard ACL to permit those addresses to be translated
    - **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
  - Establish dynamic source translation, specify the ACL, exit interface, and overload option
    - **ip nat inside source list** *access-list-number* **interface type** *name* **overload**
  - Identify the inside and outside interfaces
    - **ip nat inside**
    - **ip nat outside**

PAT with Single Address



NAT – Sample Configuration

```
access-list 1 permit 172.16.15.0 0.0.0.255
ip nat pool TEST 209.165.200.225 209.165.200.226 netmask 255.255.255.252
ip nat inside source list 1 pool TEST overload
[ip nat inside source list 1 s 0/1/0 overload]
ip nat inside source static 172.16.15.18 209.165.200.227
interface s0/0/0
  ip nat inside
interface s0/0/1
  ip nat inside
interface s0/1/0
  ip nat outside
```



Outside Host
172.16.15.64/26
B1
IntraNet1
Sales1
Web Server
64.100.150.10
Internet
172.16.15.244/30
172.16.15.248/30
172.16.15.128/26
192.135.250.16/30
HQ
B2
IntraNet2
Sales2
172.16.15.252/30
HQ-Sw
File Server
VLAN 15
Staff
VLAN 30
Inside: 172.16.15.18
Outside: 209.165.200.227
Private Address: 172.16.15.0/24
VLAN 15: 172.16.15.16/28
VLAN 30: 172.16.15.32/27
VLAN 45: 172.16.15.0/29
VLAN 60: 172.16.15.8/29