# Chapter 11: Network Address Translation for IPv4

**Routing And Switching**

Cisco | Networking Academy®

11

Do buttons on 10.1.1.2

# Chapter 11

11.0 Introduction

11.1 NAT Operation

11.2 Configuring NAT

11.3 Troubleshooting NAT

11.4 Summary

11

# Chapter 11: Objectives

- Describe NAT characteristics
- Describe the benefits and drawbacks of NAT
- Configure static NAT using the CLI
- Configure dynamic NAT using the CLI
- Configure PAT  using the CLI
- Configure port forwarding  using the CLI
- Configure NAT-PT (v6 to v4)
- Use show commands to verify NAT operation

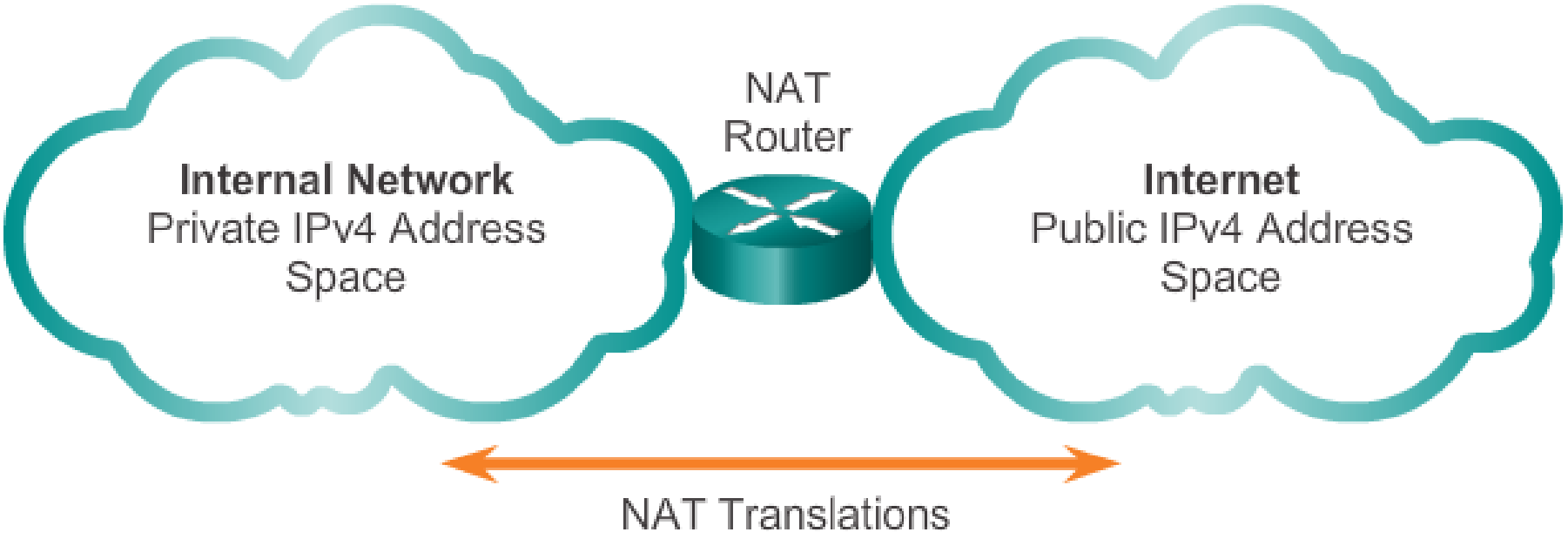
11.0.1.1

# IPv4 Private Address Space

- The IPv4 address space is not big enough to uniquely address all the devices that need to be connected to the Internet
- Network private addresses are described in RFC 1918 and are to designed to be used within an organization or site only
- Private addresses are not routed by Internet routers while public addresses are
- Private addresses can alleviate IPv4 scarcity but since they aren't routed by Internet devices, they need to be translated first.
- NAT is process used to perform such translation

11.0.1.1

# IPv4 Private Address Space




**Private Internet addresses are defined in RFC 1918:**

| Class | RFC 1918 Internal Address Range | CIDR Prefix |
|---|---|---|
| A | 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 |
| B | 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 |

11.1.1.1

Do buttons on 11.1.1.1

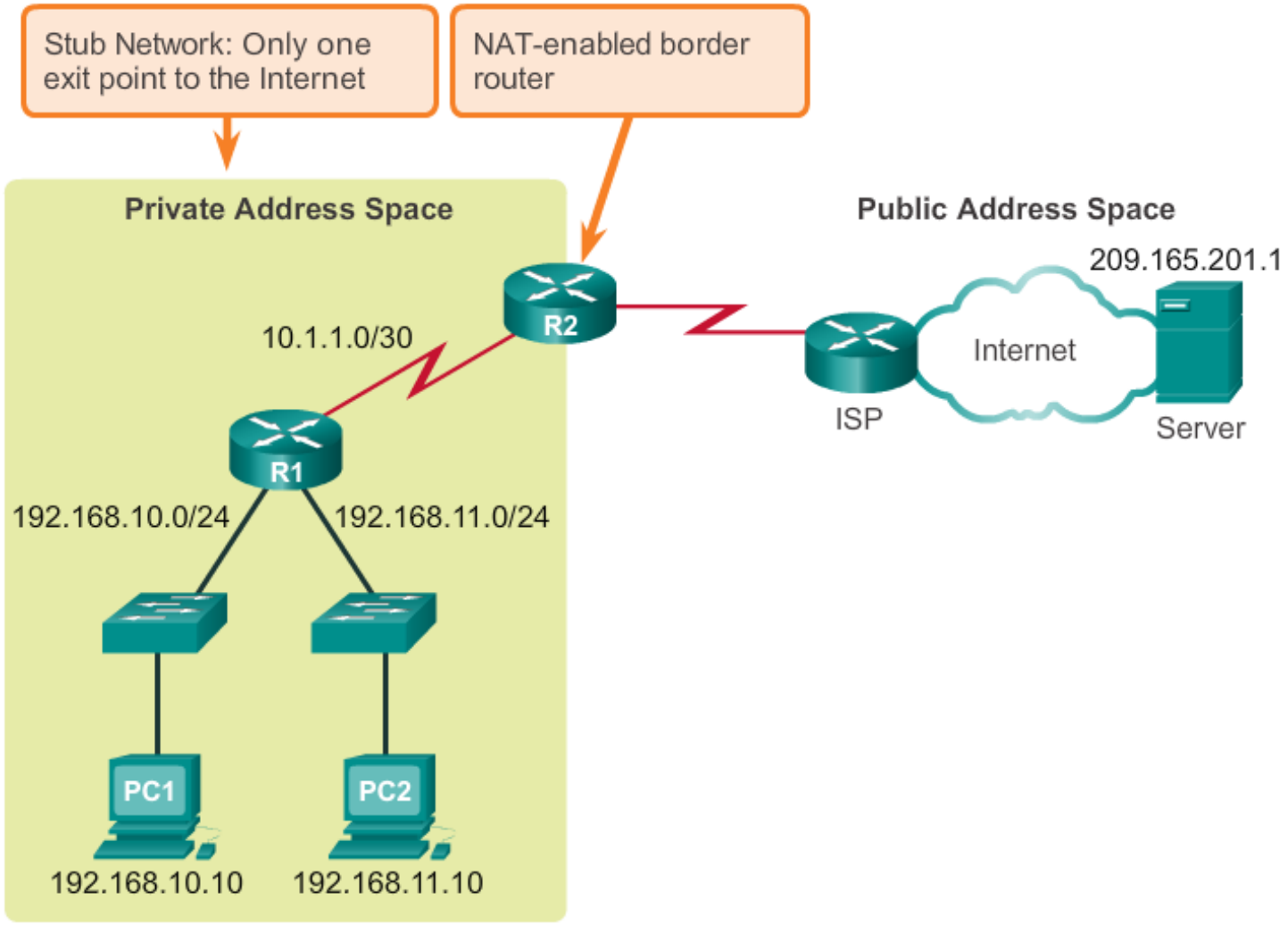
# What is NAT?

- NAT is a process used to translate network addresses
- NAT's primary use is to conserve public IPv4 addresses
- Usually implemented at border network devices such as firewalls or routers
- This allows the networks to use private addresses internally, only translating to public addresses when needed
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent/received to/from other organizations or the Internet, the border router translates the addresses to a public and globally unique address

11.1.1.2

## NAT Characteristics

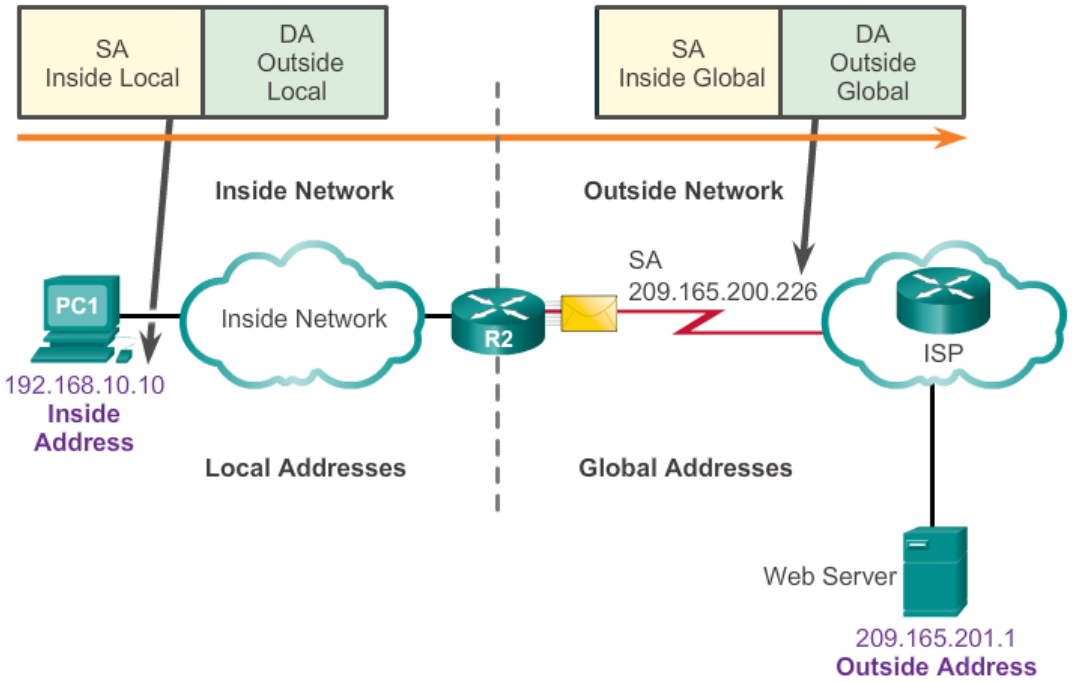
# What is NAT?




11.1.1.2

# NAT Terminology

- In NAT terminology, inside network is the set of devices using private addresses. Outside networks are all other networks
- NAT includes 4 types of addresses:
  - Inside local address
  - Inside global address
  - Outside local address
  - Outside global address




11.1.1.3

# NAT Terminology

- The terms, inside and outside, are combined with the terms local and global to refer to specific addresses

- Inside local address
- Inside global address
- Outside global address
- Outside local address

Explain each:

Private Address

Public Destination address

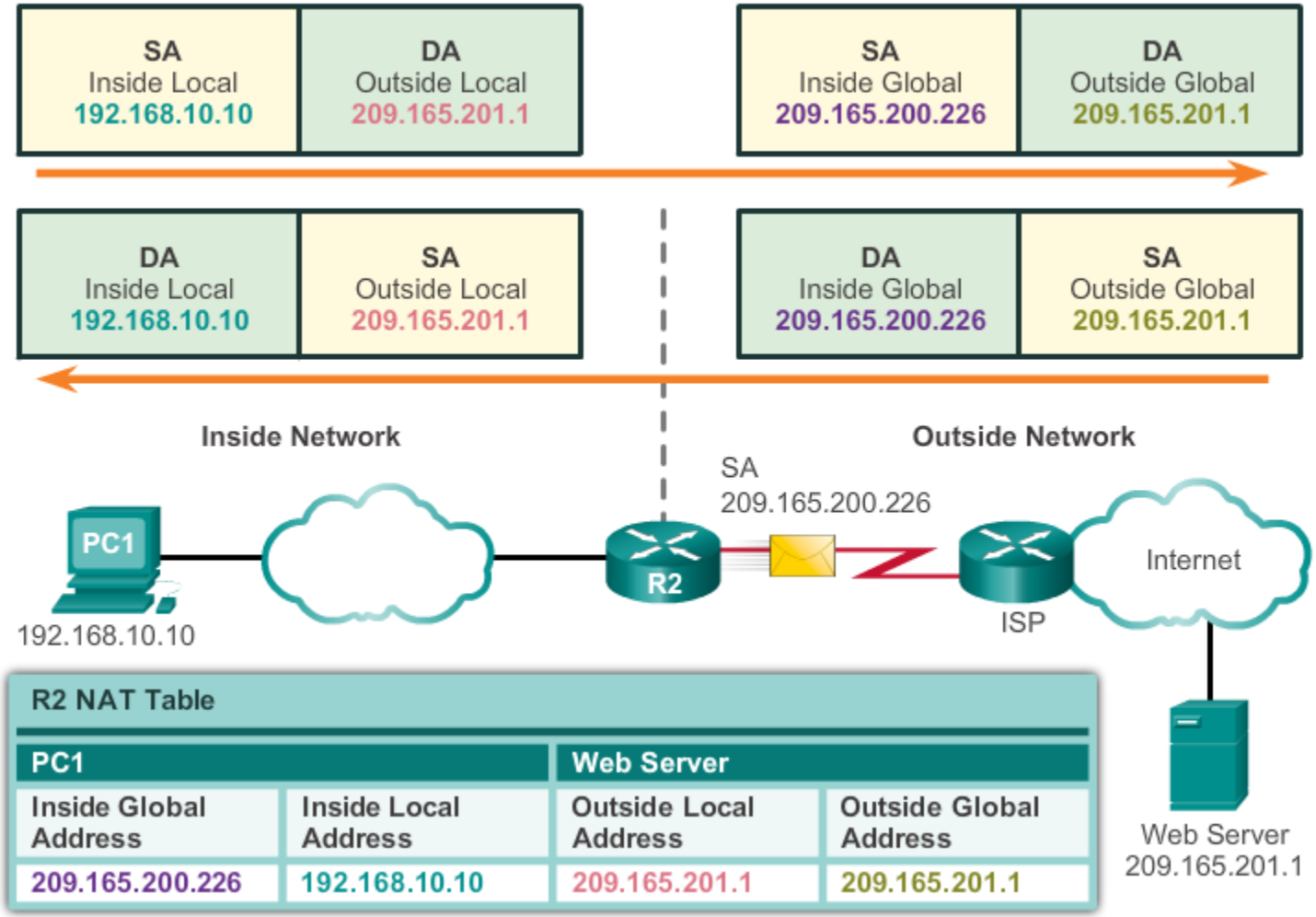
Packets private address is replaced with this address

Destination address on the internet

11.1.1.3

# How NAT Works

Explain the 4 address types

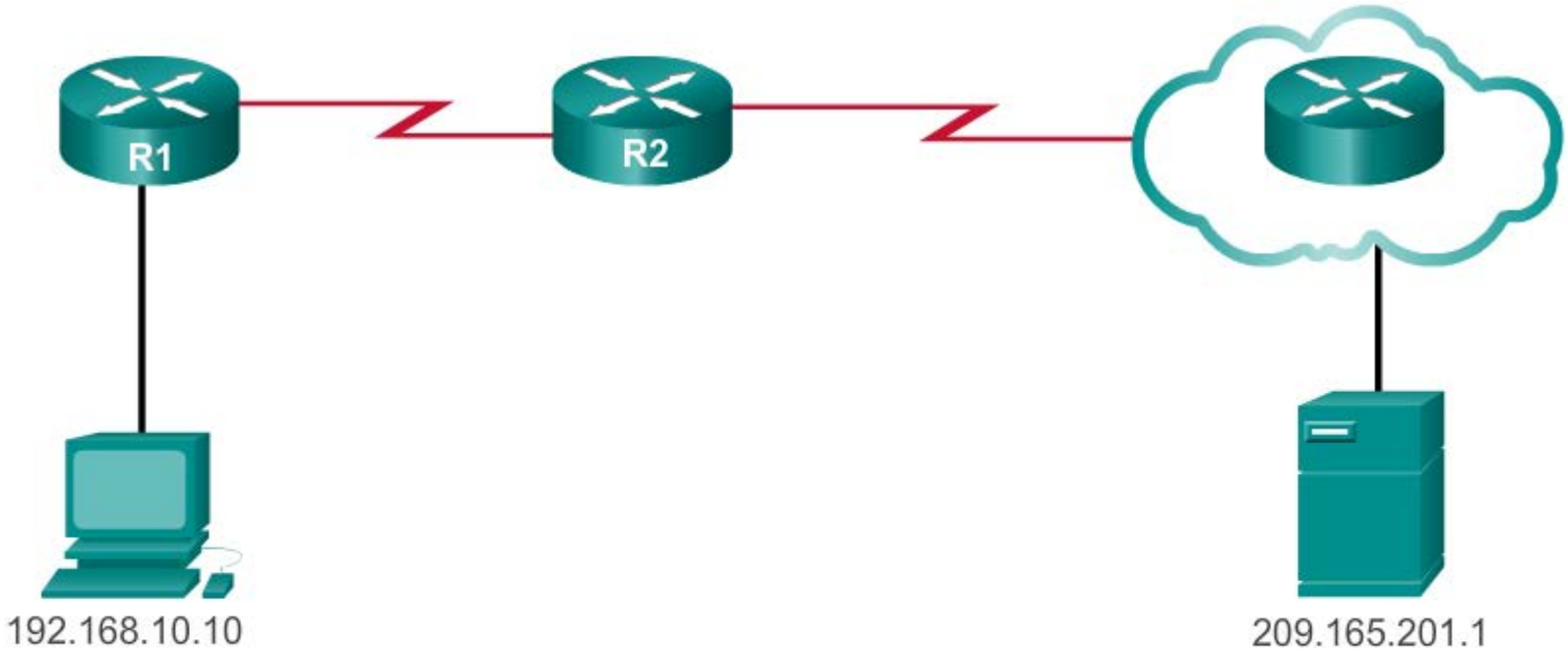



**R2 NAT Table**

| 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 |

11.1.1.4

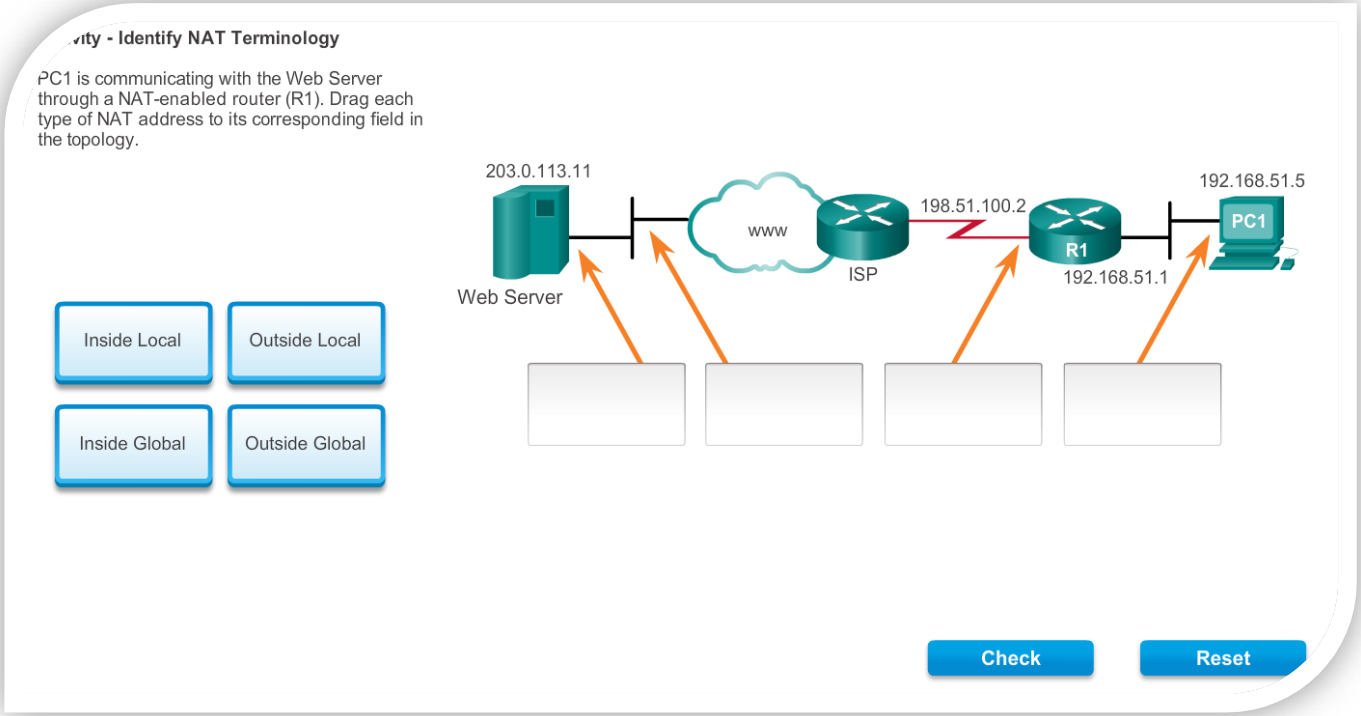
# How NAT Works




11.1.1.5

Do animation on 11.1.1.5

# 11.1.1.6 Activity - Identify the NAT Terminology




11.1.1.6

Do activity on 11.1.1.6

## Types Of NAT

# Static NAT

- Static NAT uses a one-to-one mapping of local and global addresses
- These mappings are configured by the network administrator and remain constant
- Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network
- A network administrator can SSH to a server in the inside network by point his SSH client to the proper inside global address

11.1.2.1

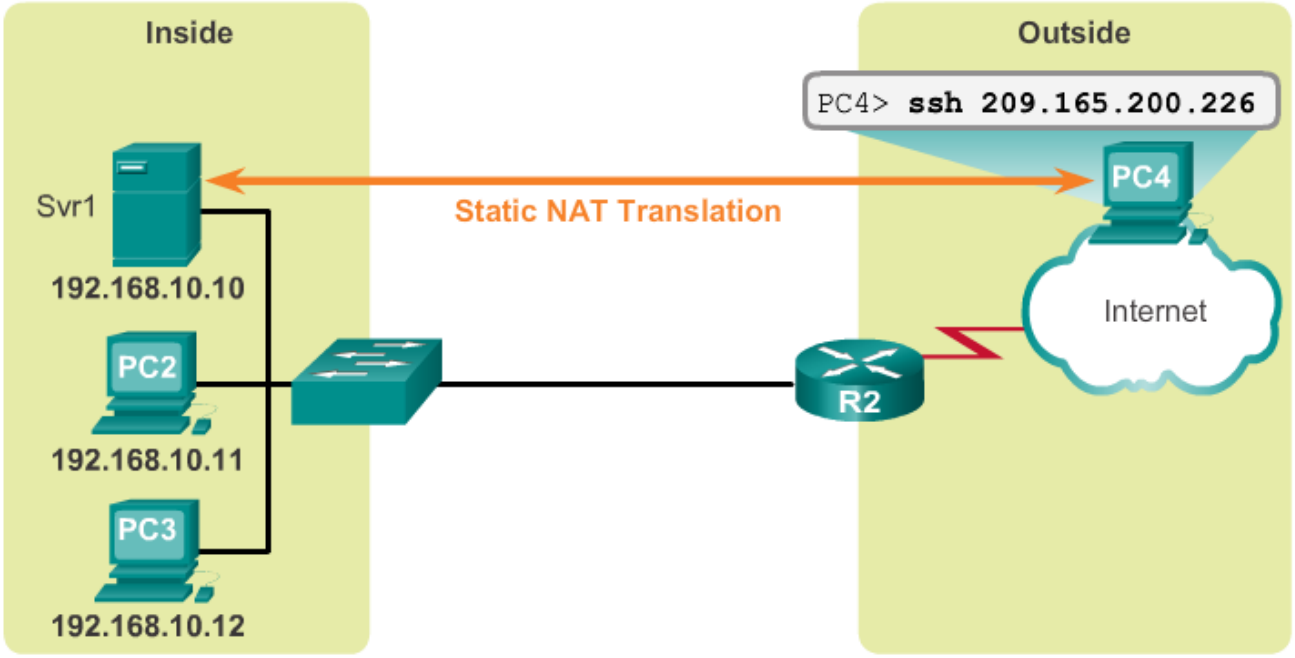
## Types Of NAT

# Static NAT

**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 |




11.1.2.1

## Types Of NAT

# Dynamic NAT

- Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis
- When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool
- Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions

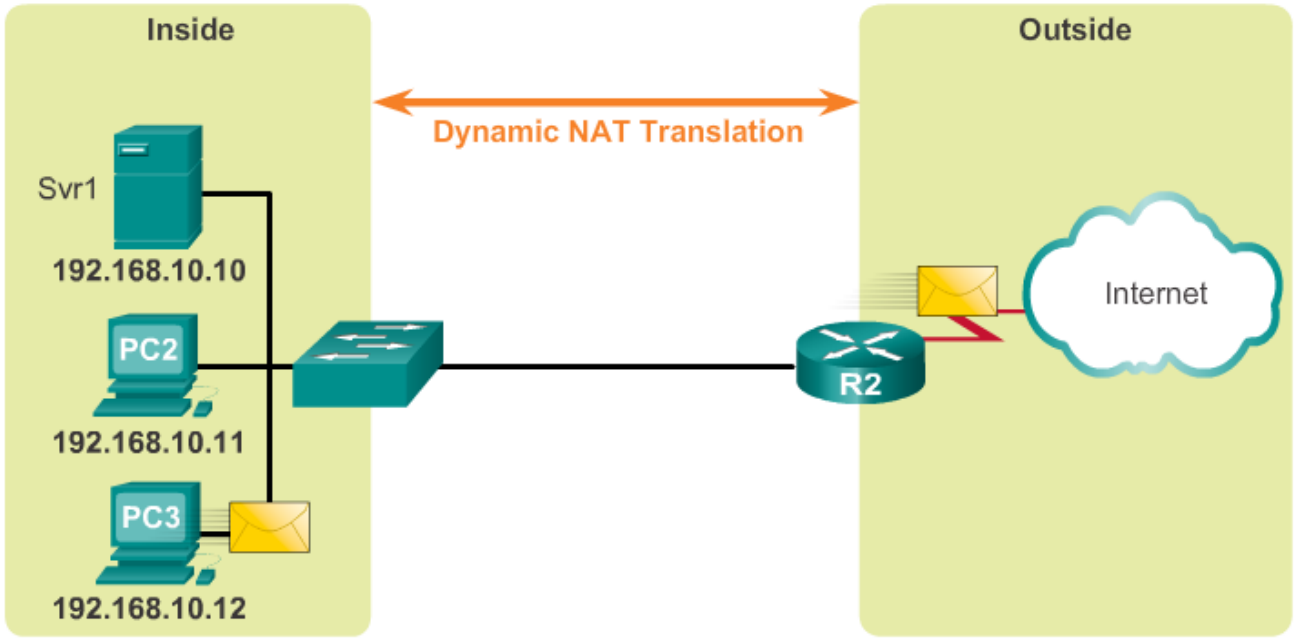
11.1.2.2

## Types Of NAT

# Dynamic NAT

**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 |



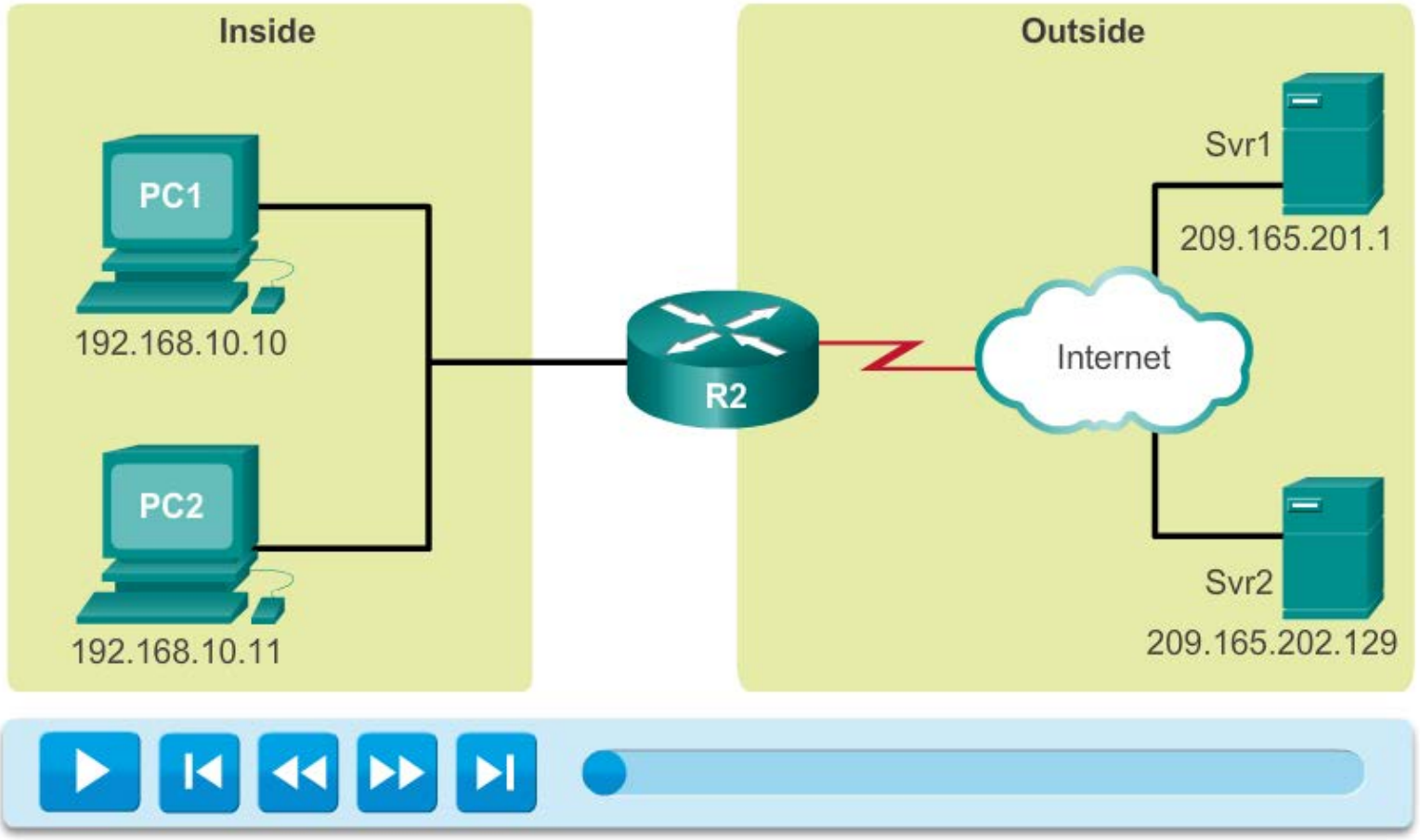

11.1.2.2

# Port Address Translation NAT (PAT)

- PAT maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
- PAT uses the pair source port and source IP address to keep track of what traffic belongs to what internal client
- PAT is also known as NAT overload
- By also using the port number, PAT is able to forward the response packets to the correct internal device
- The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session

11.1.2.3

# PAT Process

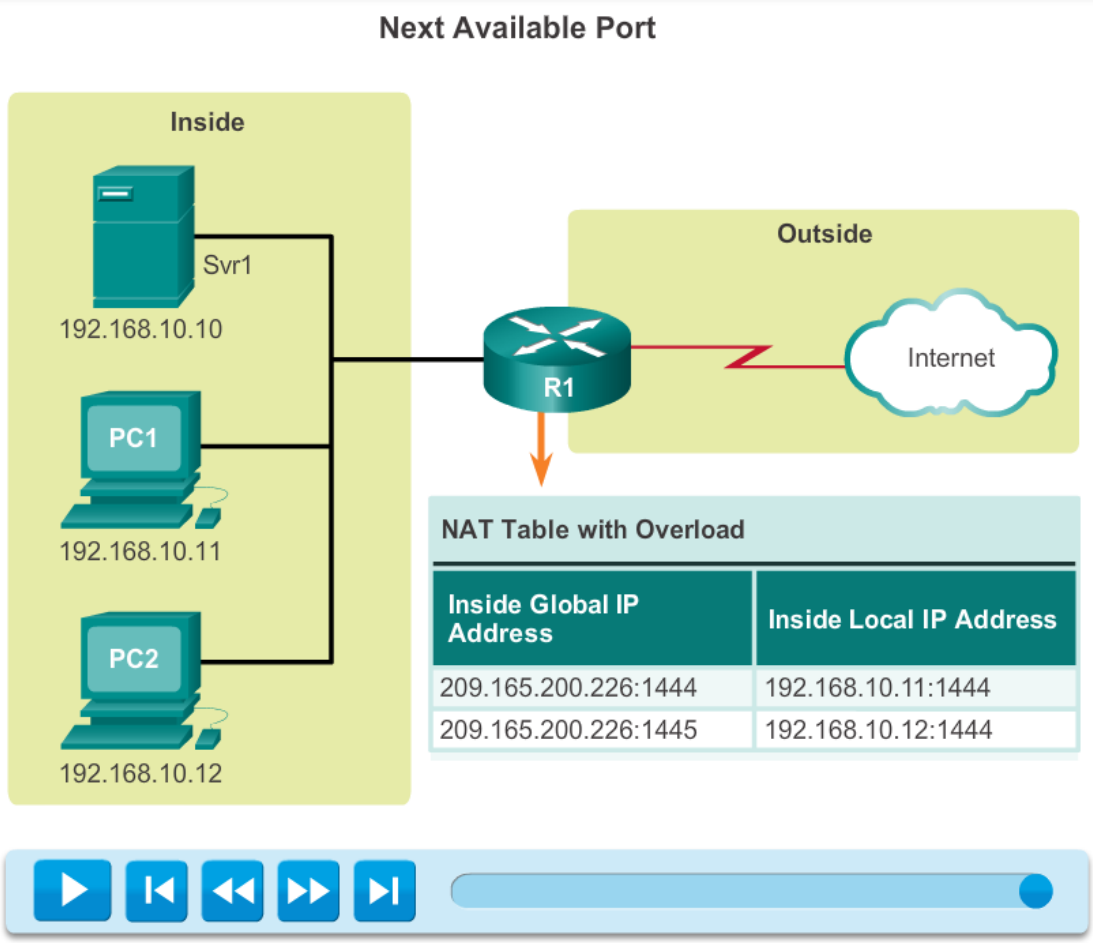



11.1.2.3

Do animation on 11.1.2.3

PAT

# Next Available Port




11.1.2.4

Do animation on 11.1.2.4

# Comparing NAT and PAT

- NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses
- PAT modifies both the address and the port number
- NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address given by the host on the public network
- With PAT, there is generally only one or a very few publicly exposed IPv4 addresses
- PAT is also able to translate protocols that don't use port numbers such as ICMP. Each one of these protocols are supported differently by PAT

11.1.2.5

# Benefits of NAT

## Benefits 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

11.1.3.1

# Disadvantages of NAT

## 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

11.1.3.2

# Configuring Static NAT

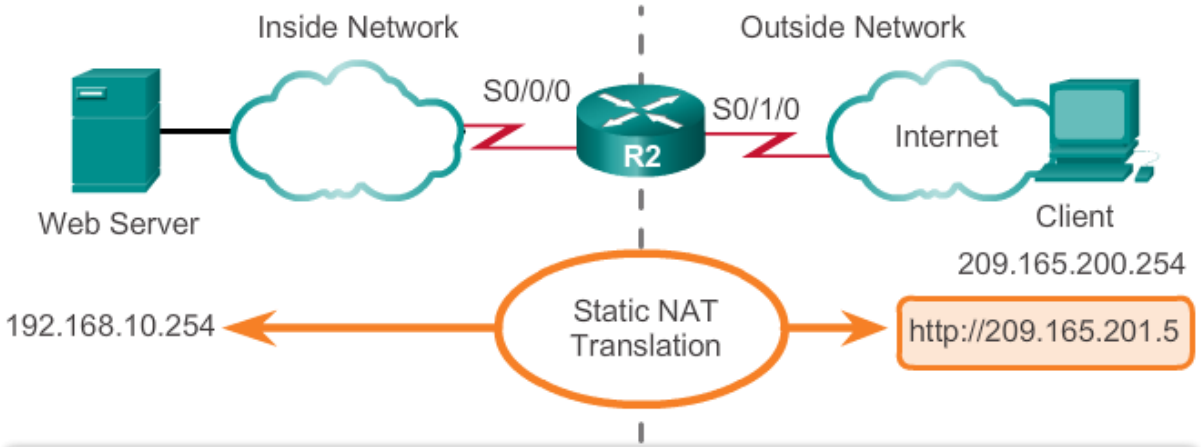
- There are two basic tasks when configuring static NAT translations:
  - Create the mapping between the inside local and outside local addresses
  - Define which interface belong to the inside network and which belong to the outside network

Do buttons on 11.2.1.1
Students do button 4 for practice

11.2.1.1

# Configuring Static NAT

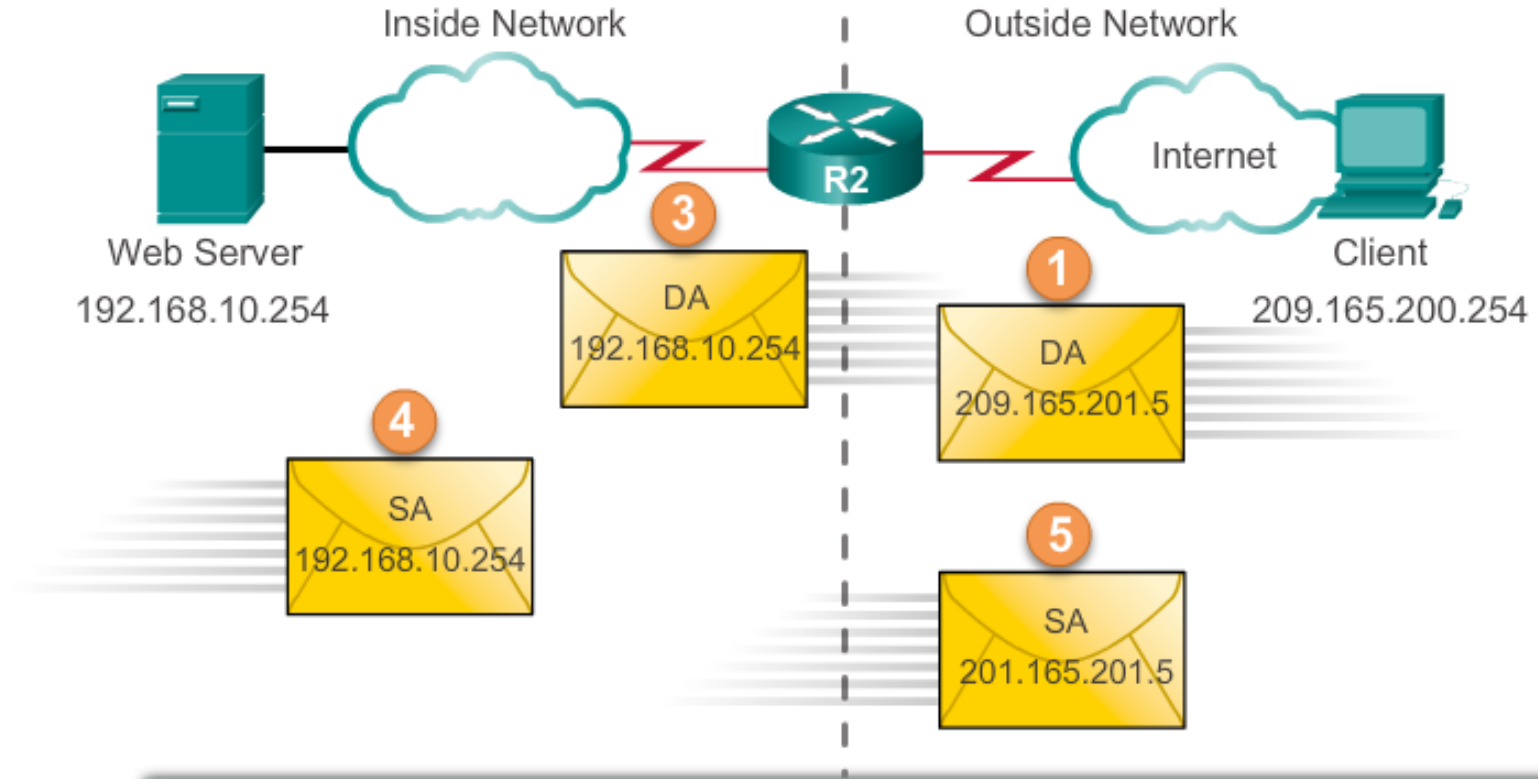
## Example Static NAT Configuration




```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

11.2.1.1

# Analyzing Static NAT




**NAT Table**

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

2 5

11.2.1.2

# Verifying Static NAT

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

11.2.1.3

## Configuring Static NAT

# Verifying Static NAT

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

**Client PC establishes a session with the web server**

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

11.2.1.3

# 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 won't be able to communicate to any external networks if no addresses are available in the pool

11.2.2.1

# Configuring Dynamic NAT

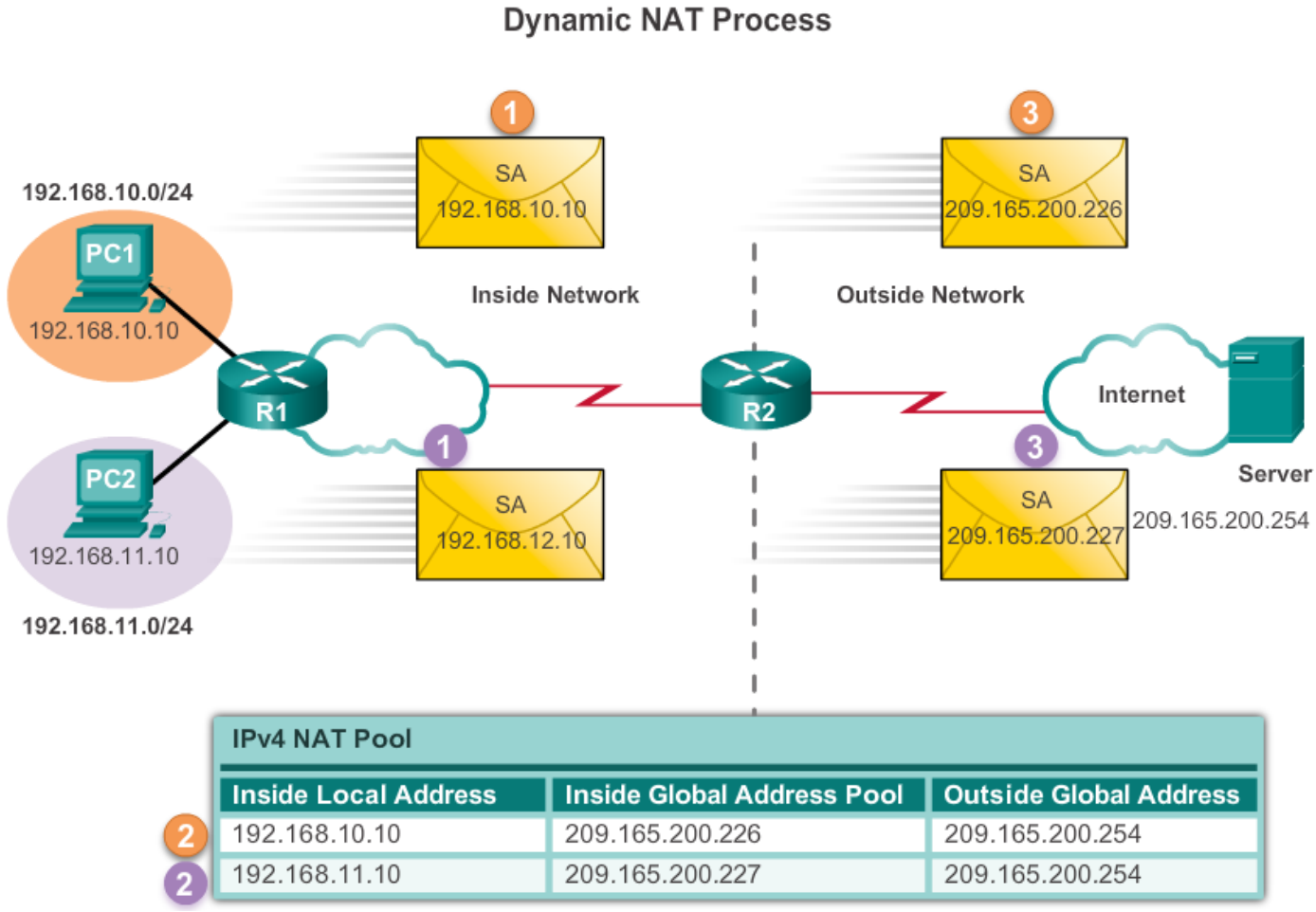
## Dynamic NAT Configuration Steps

| Dynamic NAT Configuration Steps | |
|---|---|
| **Step 1** | Define a pool of global addresses to be used for translation.<br>**ip nat pool** *name start-ip end-ip*<br>{<br>**netmask***netmask* \| **prefix-length** *prefix-length*<br>} |
| **Step 2** | Define a standard access list permitting the addresses that should be translated.<br>**access-list** *access-list-number* **permit** *source [source-wildcard]* |
| **Step 3** | Establish dynamic source translation, specifying the access list and pool defined in prior steps.<br>**ip nat inside source list** *access-list-number* **pool** *name* |
| **Step 4** | Identify the inside interface.<br>**interface** *type number*<br>**ip nat inside** |
| **Step 5** | Identify the outside interface.<br>**interface** *type numbe*<br>**ip nat outside** |

11.2.2.2

Do buttons on 11.2.2.2
Students do button 4 for practice

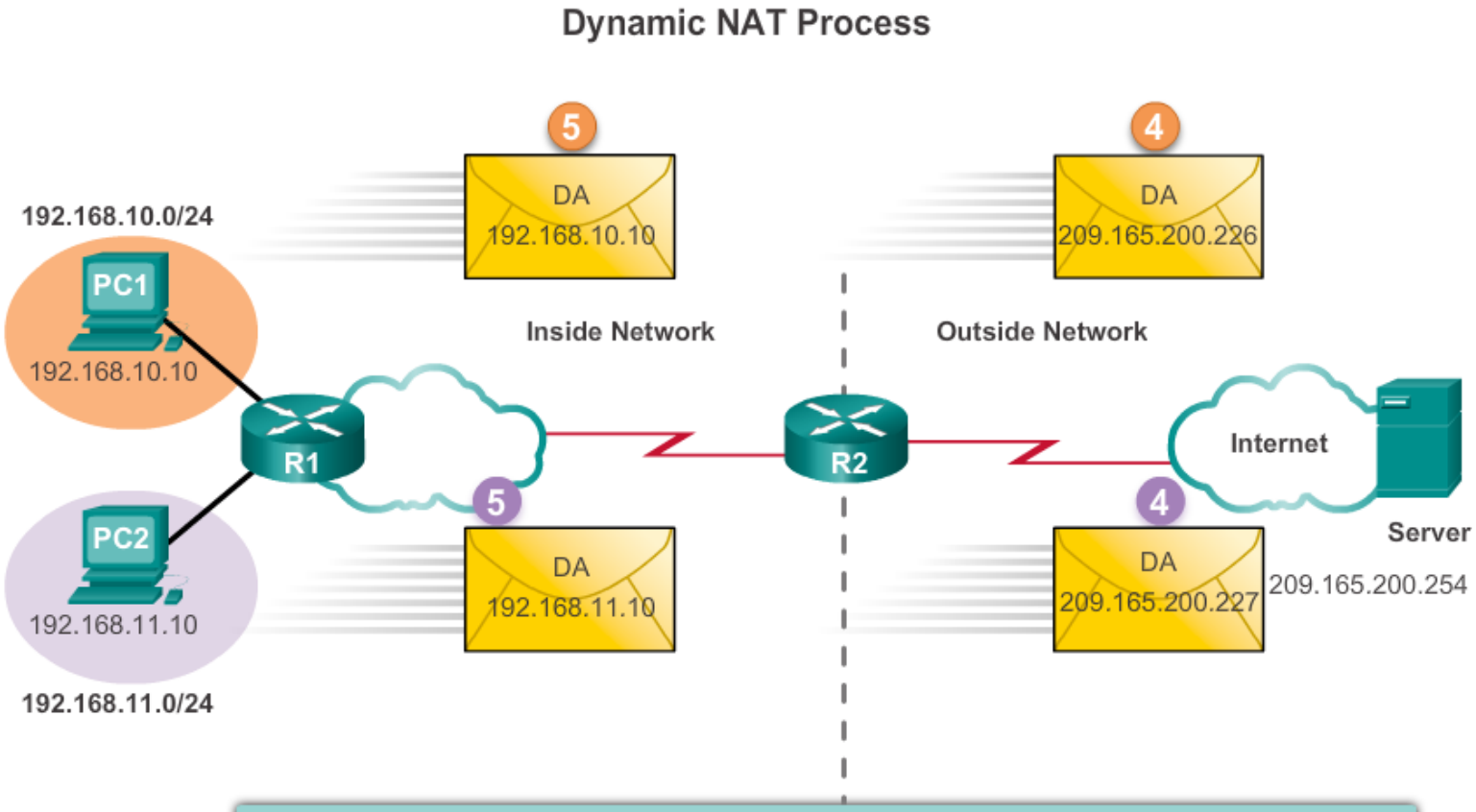
# Analyzing Dynamic NAT




11.2.2.3

Do buttons on 11.1.2.3

# Analyzing Dynamic NAT




**IPv4 NAT Pool**

| | Inside Local Address | Inside Global Address Pool | Outside Global Address |
|---|---|---|---|
| 5 | 192.168.10.10 | 209.165.200.226 | 209.165.200.254 |
| 5 | 192.168.11.10 | 209.165.200.227 | 209.165.200.254 |

11.2.2.3

# Verifying Dynamic NAT

## Verifying Dynamic NAT with show ip nat translations

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

11.2.2.4

Do buttons on 11.1.2.4

# Verifying Dynamic NAT

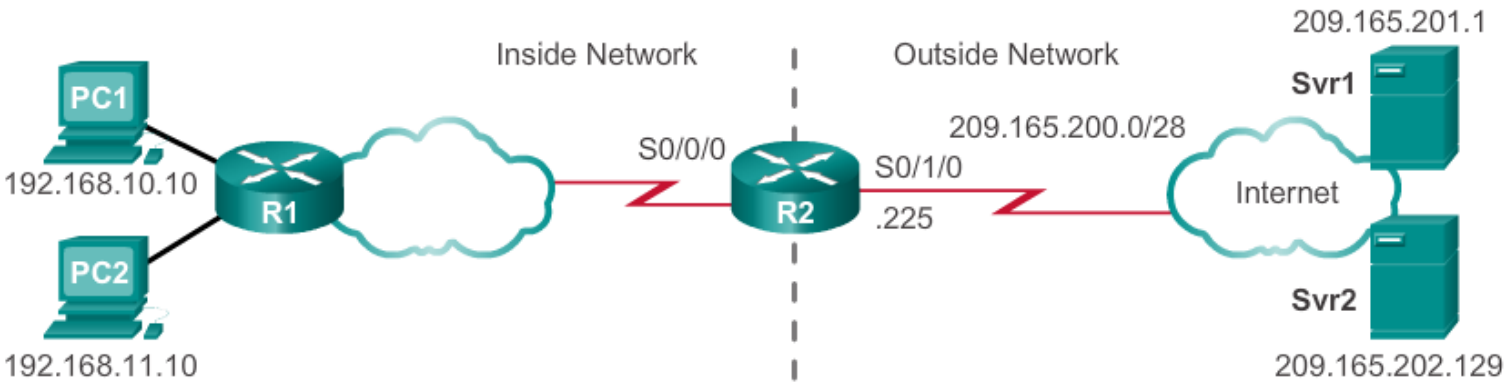
## Verifying Dynamic NAT with show ip nat statistics

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

11.2.2.4

# Configuring PAT: Address Pool

## Example PAT with Address Pool




Define a pool of public IPv4 addresses under the pool name NAT-POOL2.
R2(config)# **ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224**
Define which addresses are eligible to be translated.
R2(config)# **access-list 1 permit 192.168.0.0 0.0.255.255**
Bind NAT-POOL2 with ACL 1.
R2(config)# **ip nat inside source list 1 pool NAT-POOL2 overload**

Identify interface serial 0/0/0 as an inside NAT interface.
R2(config)# **interface Serial0/0/0**
R2(config-if)# **ip nat inside**

Identify interface serial 0/1/0 as the outside NAT interface.
R2(config)# **interface Serial0/1/0**
R2(config-if)# **ip nat outside**

Do buttons on 11.2.3.1
Students do button 3 for practice

11.2.3.1

# Configuring PAT: Single Address

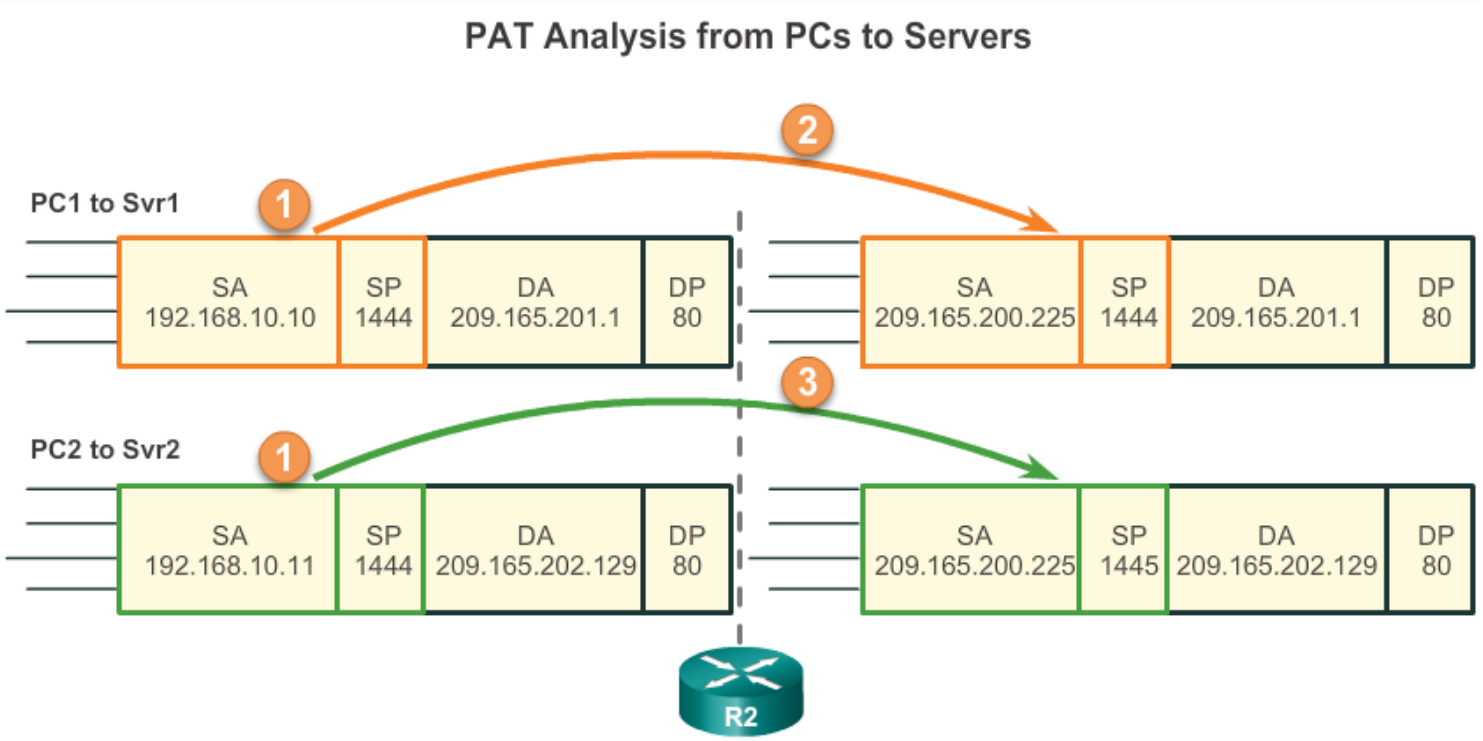
| | |
|---|---|
| **Step 1** | Define a standard access list permitting the addresses that should be translated.<br><br>**access-list** *access-list-number* **permit** *source*[*source-wildcard*] |
| **Step 2** | Establish dynamic source translation, specifying the ACL, exit interface and overload options.<br><br>**ip nat inside source list***access-list-number***interface** *type number* **overload** |
| **Step 3** | Identify the inside interface.<br><br>**interface** *type number*<br>**ip nat inside** |
| **Step 4** | Identify the outside interface.<br><br>**interface** *type number*<br>**ip nat outside** |

Do buttons on 11.2.3.2
Students do button 3 for practice

11.2.3.2

## Configuring Port Address Translation (PAT)

# Analyzing PAT



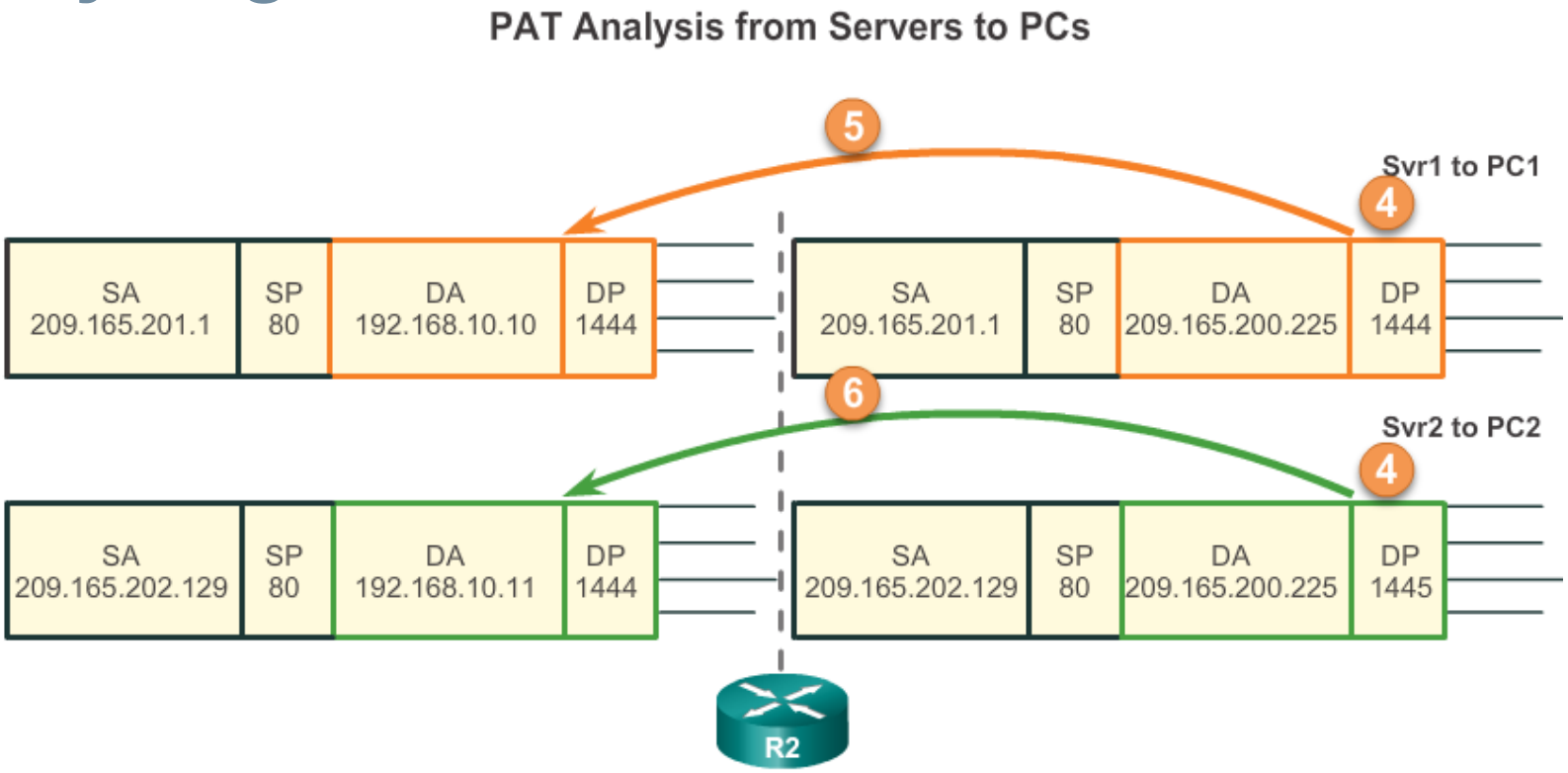

**NAT Table**

| Inside Local Address | Inside Global Address | Outside Global Address | Outside Local Address |
|---|---|---|---|
| 192.168.10.10:1444 | 209.165.200.226:1444 | 209.165.201.1:80 | 209.165.201.1:80 |
| 192.168.10.11:1444 | 209.165.200.226:1445 | 209.165.202.129:80 | 209.165.202.129:80 |

11.2.3.3

Do buttons on 11.2.3.3

# Analyzing PAT




**NAT Table**

| Inside Local Address | Inside Global Address | Outside Global Address | Outside Local Address |
|---|---|---|---|
| 192.168.10.10:1444 | 209.165.200.226:1444 | 209.165.201.1:80 | 209.165.201.1:80 |
| 192.168.10.11:1444 | 209.165.200.226:1445 | 209.165.202.129:80 | 209.165.202.129:80 |

11.2.3.3

# Verifying PAT

## Verifying PAT Translations

```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local       Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80    209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80  209.165.202.129:80
R2#
```

11.2.3.4

Do buttons on 11.2.3.4

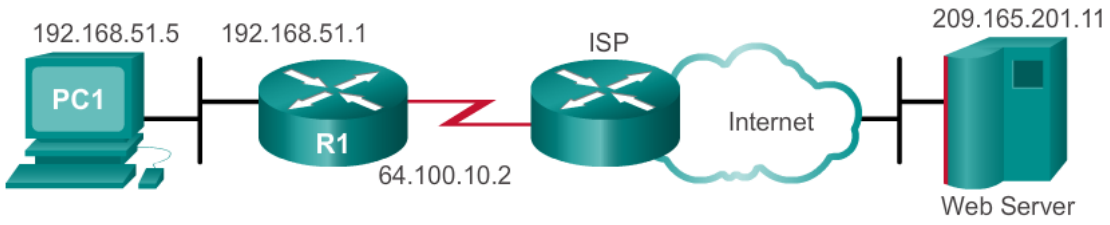
# Configuring Port Address Translation (PAT)
# 11.2.3.5 Activity - Identify the Address Information at Each Hop

**Activity - Identify Address Information at Each Hop**

PC1 is communicating with the Web Server through a NAT-enabled router (R1). Follow this communication one hop at a time to determine how the source address (SA), destination address (DA), and port number changes along the way. Select Button 2 now to get started.

1
2
3
4
5

**Network Topology**

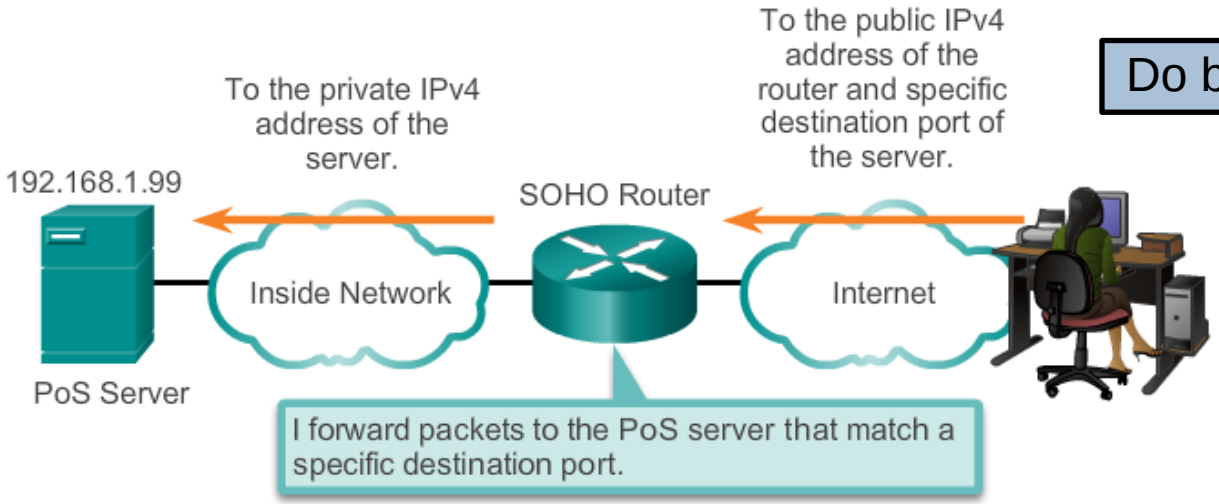



11.2.3.5

Do activity on 11.2.3.5

# Port Forwarding

- Port forwarding is the act of forwarding a network port from one network node to another
- A packet sent to the public IP address and port of a router can be forwarded to a private IP address and port in inside network
- This is helpful in situations where servers have private addresses, not reachable from the outside networks

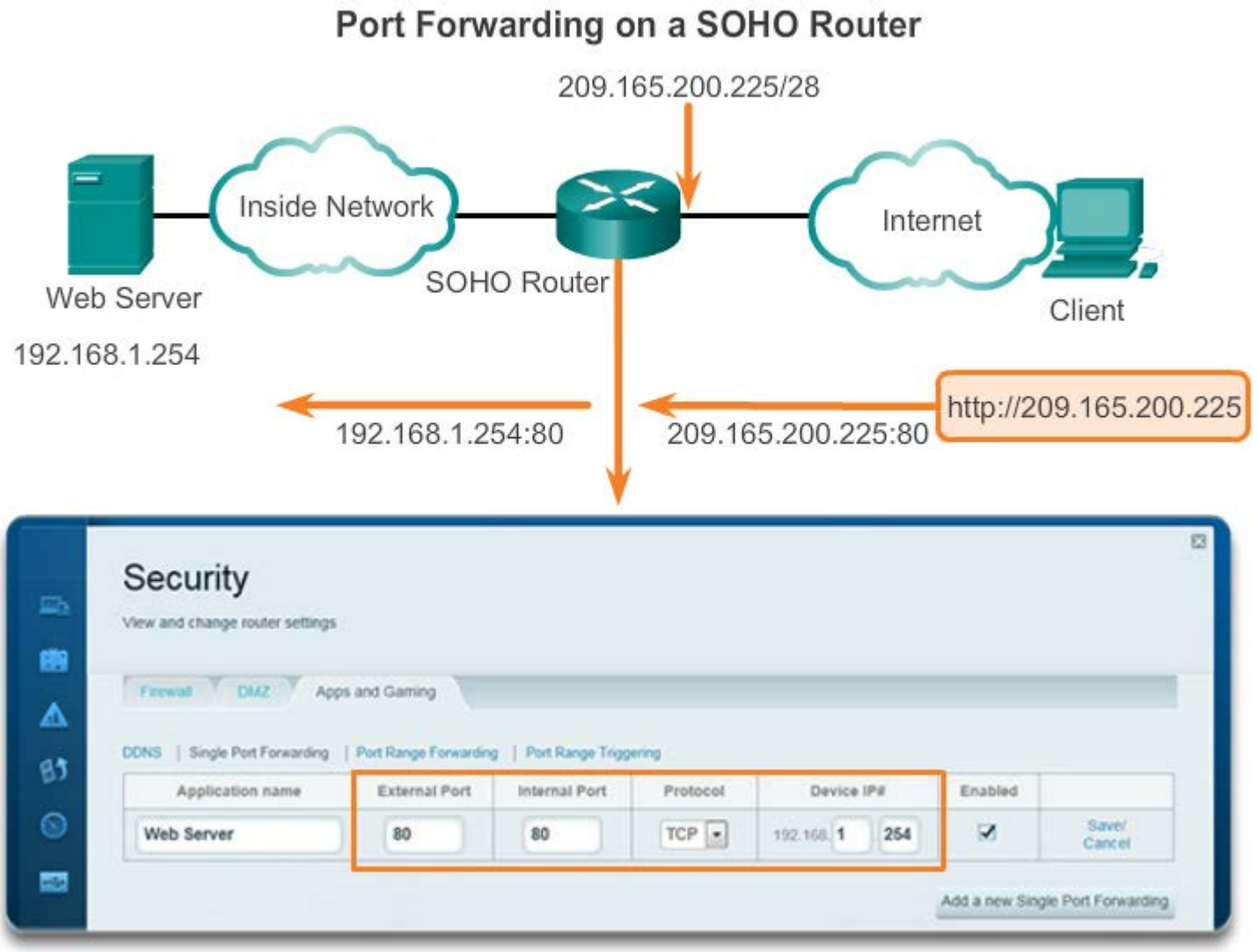



Do buttons on 11.2.4.1

11.2.4.1

## Port Forwarding

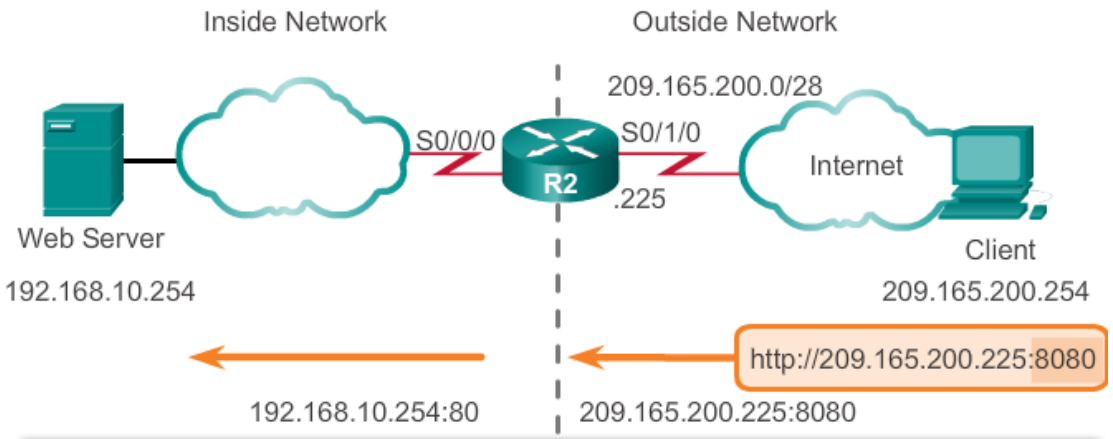
# SOHO Example




11.2.4.2

# Configuring Port Forwarding with IOS

- In IOS, Port forwarding is essentially a static NAT translation with a specified TCP or UDP port number




Establishes static translation between an inside local address and local port and an inside global address and global port.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

11.2.4.3

Do buttons on 11.2.4.3

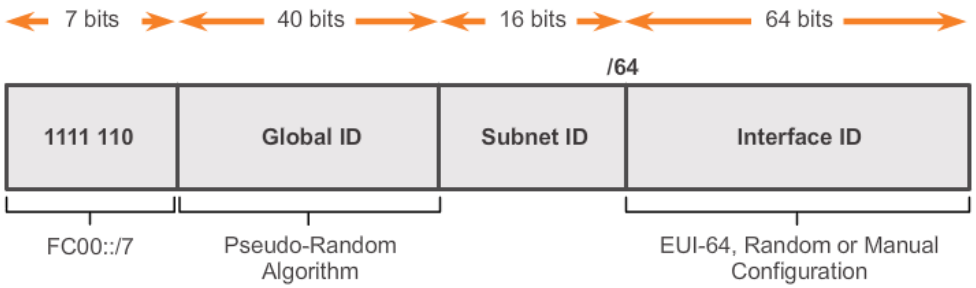
# NAT for IPv6?

- NAT is a workaround for IPv4 address scarcity
- IPv6 with a 128-bit address provides 340 undecillion addresses
- Address space is not an issue for IPv6
- IPv6 makes IPv4 public-private NAT unnecessary by design
- However, IPv6 does implement a form of private addresses and it is implemented differently than they are for IPv4

11.2.5.1

# IPv6 Unique Local Addresses

- IPv6 unique local addresses (ULA) is designed to allows IPv6 communications within a local site
- ULA is not meant to provide additional IPv6 address space
- ULA have the prefix FC00::/7, which results in a first hextet range of FC00 to FDFF
- Unique local addresses are defined in RFC 4193
- ULAs is also known as local IPv6 addresses (not to be confused with IPv6 link-local addresses)



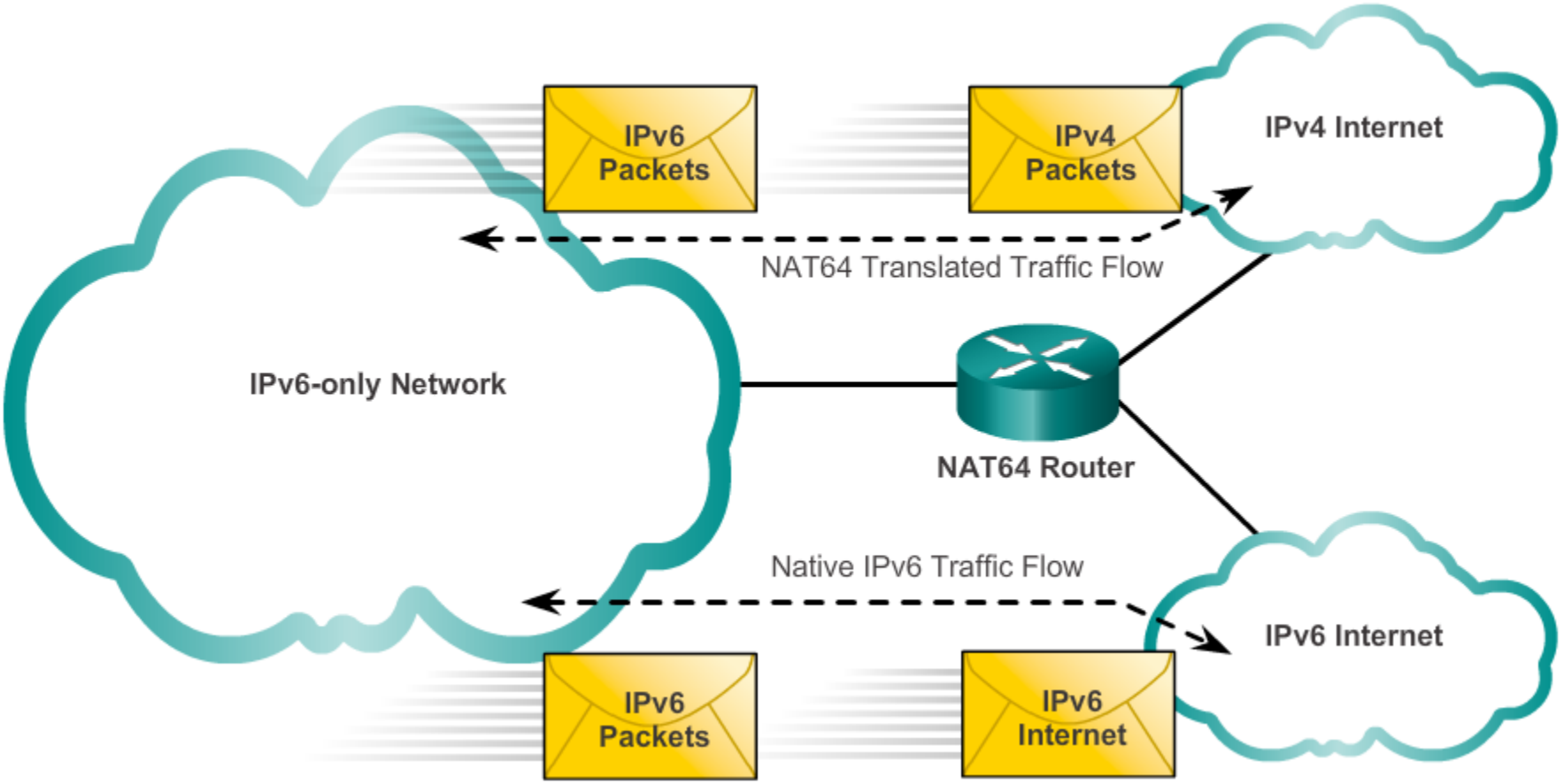

11.2.5.2

# NAT For IPv6

- IPv6 also uses NAT but in a much different context
- In IPv6, NAT is used to provide transparent communication between IPv6 and IPv4
- NAT64 is not intended to be a permanent solution. It is meant to be a transition mechanism
- Network Address Translation-Protocol Translation (NAT-PT) was another NAT based transition mechanism for IPv6 but is now deprecated by IETF
- NAT64 is now recommended

11.2.5.3

# NAT For IPv6




11.2.5.3

# Troubleshooting NAT: Show commands

```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
```

Host 192.168.10.10 telnets to server at 209.165.201.1

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:09 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 31  Misses: 0
CEF Translated packets: 31, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
```

<output omitted>

```
R2# show ip nat translations
Pro Inside global         Inside local         Outside local      Outside global
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23   209.165.201.1:23
R2#
```

11.3.1.1

Do buttons on 11.3.1.1

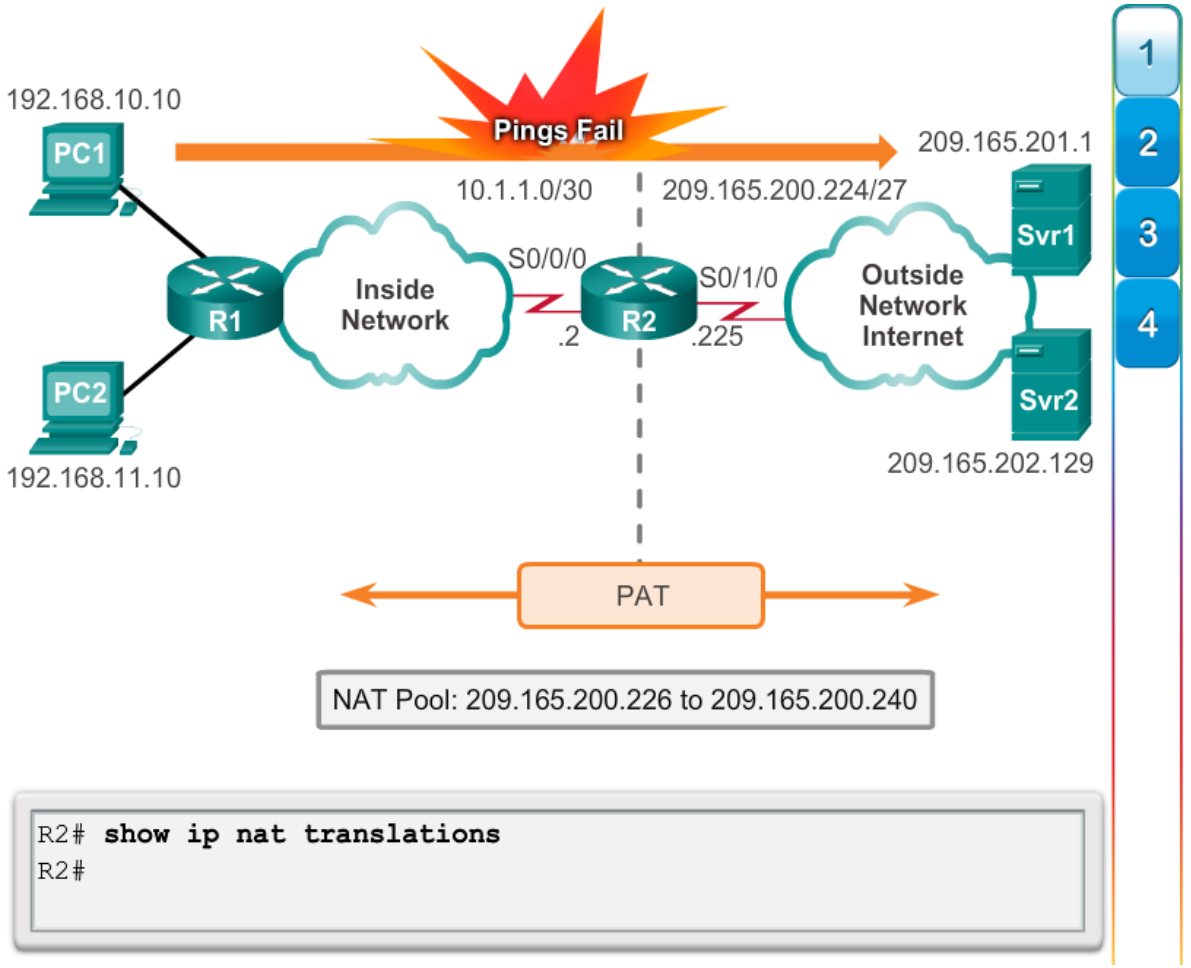
# Troubleshooting NAT: Debug command

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2818]
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2819]
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2820]
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4181]
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4182]
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2821]
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4183]
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2822]
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4184]
output omitted
```

11.3.1.2

Do buttons on 11.3.1.2

# Troubleshooting NAT: Debug command




11.3.1.3

Do buttons on 11.3.1.3

# Chapter 11: Summary

- This chapter has outlined how NAT is used to help alleviate the depletion of IPv4 address space.
- NAT conserves public address space and saves considerable administrative overhead in managing adds, moves, and changes.
- This chapter discussed NAT for IPv4, including:
- NAT characteristics, terminology and general operations
- The different types of NAT including static NAT, dynamic NAT, and NAT with overloading
- The benefits and disadvantages of NAT

11.4.1.3

# Chapter 11: Summary (cont)

- The configuration, verification and analysis of static NAT, dynamic NAT, and NAT with overloading
- How port forwarding can be used to access an internal devices from the Internet
- Troubleshooting NAT using **show** and**debug** commands
- How NAT for IPv6 is used to translate between IPv6 addresses and IPv4 addresses

11.4.1.3

Cisco | Networking Academy®

Mind Wide Open™

tAdA