VTP & NAT

Jirasak Sittigorn

Internetworking Standards & Technologies

Department of Computer Engineering, Faculty of Engineering

King Mongkut's Institute of Technology Ladkrabang

Cisco | Networking Academy®

Mind Wide Open™

- VTP (VLAN Trunking Protocol)
  - Benefits of VTP
  - VTP Operation
  - VTP configuration
  - Adding a switch to an existing VTP domain
  - VTP Pruning

VTP (VLAN Trunking Protocol)

- VTP is a messaging protocol that uses Layer 2 trunk frames to manage the addition, deletion, and renaming of VLAN on a single domain.
- VTP messages are encapsulated in either Cisco proprietary ISL or IEEE 802.1Q protocol frames and then passed across trunk links to other devices.
- NOTE: before creating VLANs on the switch, you must first set up a VTP management domain

Benefits of VTP

- **Before discussing VTP, it is important to understand that VTP is not necessary in order to configure VLANs or Trunking on Cisco Switches.**
- VTP is a Cisco proprietary protocol that allows VLAN configuration to be consistently maintained across a common administrative domain.
- VTP minimizes the possible configuration inconsistencies that arise when changes are made.
- Additionally, VTP reduces the complexity of managing and monitoring VLAN networks, allowing changes on one switch to be propagated to other switches via VTP.
- On most Cisco switches, VTP is running and has certain defaults already configured.

VTP Operation

- **VTP advertisements are transmitted out all trunk connections**, including ISL, IEEE 802.1Q, IEEE 802.10, and ATM LANE trunks.
- A critical parameter governing VTP function is the **VTP configuration revision number**.
- This 32-bit number indicates the particular revision of a VTP configuration.
- A configuration revision number **starts at 0 and increments by 1 with each modification until it reaches 4294927295, at which point it recycles back to 0 and starts incrementing again.**
- **Each VTP device tracks its own VTP configuration revision number VTP packets contain the sender's VTP configuration number.**
- This information determines whether the received information is more recent than the current version.
- If the switch receives a VTP advertisement over a trunk link, it inherits the VTP domain name and configuration revision number.
- **The switch ignores advertisements that have a different VTP domain name or an earlier configuration revision number.**

VTP Operation

- VTP switches operate in one of three modes:
  - Server
  - Client
  - Transparent

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- VTP servers can create, modify, delete VLAN and VLAN configuration parameters for the entire domain, and save VLAN configuration information in Catalyst NVRAM, and send VTP messages out to all trunk ports.

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- VTP clients cannot create, modify, or delete VLAN information.
- The only role of VTP clients is to process VLAN changes and send VTP messages out all trunk ports.
- The VTP client maintains a full list of all VLANs within the VTP domain, but it does not store the information in NVRAM.
- VTP clients behave the same way as VTP servers, but it is not possible to create, change, or delete VLANs on a VTP client.
- Any changes made must be received from a VTP server advertisement.

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

- Switches in **VTP transparent mode** forward VTP advertisements but ignore information contained in the message.
- A transparent switch will not modify its database when updates are received, nor will the switch send out an update indicating a change in its own VLAN status.
- Except for forwarding VTP advertisements, VTP is disabled on a transparent switch.
- There is also an "off" VTP mode in which switches behave the same as in the VTP transparent mode, except VTP advertisements are not forwarded.

VTP configuration

- VTP can be configured by using these configuration modes.
  - VTP Configuration in global configuration mode
  - VTP Configuration in VLAN configuration mode
- VLAN configuration mode is accessed by entering the **vlan database** privileged EXEC command.

- Determine the version number
- Choose the domain
- Choose the VTP mode
- Password protect the domain

VTP configuration

- **Step 1**: Determine the version number of VTP that will be utilized.
- **Step 2**: Decide if this switch is to be a member of an existing management domain or if a new domain should be created. If a management domain does exist, determine the name and password of the domain.
- **Step 3**: Choose a VTP mode for the domain.

VTP configuration - Version

VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp version 2
```

VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

- Two different versions of VTP can run in the management domain, VTP Version 1 and VTP Version 2. Two versions are not interoperable.
- **The two versions are not interoperable in the same VTP domain.**
- The major difference between the two versions is **version 2 introduces support for Token Ring VLANs.**
- If all switches in a VTP domain can run VTP Version 2, version 2 only needs to be enabled on one VTP server switch, which propagates it to other VTP switches in the VTP domain.
- Version 2 should not be enabled unless every switch in the VTP domain supports version 2.

VTP configuration - Domain and Password

VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

- The **domain name** can be between 1 and 32 characters.
- The **optional password** must be between 8 and 64 characters long.
- If the switch being installed is the first switch in the network, the management domain will need to be created.
- However, if the network has other switches running VTP, then the new switch will join an existing management domain.
- **Caution:** The **domain name** and **password** are case sensitive.

VTP configuration - Domain and Password

VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

- By default, management domains are set to a nonsecure mode, meaning that the switches interact without using a password.
- Adding a password automatically sets the management domain to secure mode.
- The same password must be configured on every switch in the management domain to use secure mode.

VTP configuration - VTP mode

VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp mode server
```

VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp server
```

Feature	Server	Client	Transparent
Source VTP Messages	Yes	Yes	No
Listen to VTP Messages	Yes	Yes	No
Create VLANs	Yes	No	Yes*
Remember VLANs	Yes	No	Yes*

*Locally Significant only

```
Switch#config terminal
Switch(config)#vtp mode [client|server|transparent]

Switch#vlan database
Switch(vlan)#vtp [client|server|transparent]
```

VTP Configuration - Overview

- VTP Configuration in global configuration mode:

```
Switch#config terminal
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Switch(config)#vtp domain cisco
Switch(config)#vtp password mypassword
```

- VTP Configuration in VLAN configuration mode:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
Switch(vlan)#vtp server
Switch(vlan)#vtp domain cisco
Switch(vlan)#vtp password mypassword
```

Verifying VTP

- This command is used to verify VTP configuration settings on a Cisco IOS command-based switch.

```
Switch#show vtp staus
VTP Version                     :2
Configuration Revision          :2
Maximum VLANs supported locally :68
Number of existing VLANs        :6
VTP Operating Mode              :Client
VTP Domain Name                 :cisco
VTP Pruning Mode                :Disabled
VTP v2 Mode                     :Enabled
VTP Traps Generation            :Disabled
MD5 digest                      :0x35 0x84 0x7B 0x04 0x3D
                                 0x55 0x3B 0xDA
Configuration last modified by 0.0.0.0 at 10-5-00 20:33:41
Switch#
```

Verifying VTP

- This command is used to display statistics about advertisements sent and received on the switch.

```
MDF_Switch#show vtp counters
VTP statistics:
Summary advertisments received          :4
Subset advertisments received           :1
Request advertisments received          :2
Summary advertisments transmitted       :7
Subset advertisments transmitted        :4
Request advertisments transmitted       :1
Number of config revision errors        :0
Number of config digest errors          :0
Number of V1 summary errors             :0
```

Adding a switch to an existing VTP domain

- Clear the configuration
- Clear the VTP file
- Power cycle the switch
- Configure VTP mode and domain
- Password protect the domain

- Use caution when inserting a new switch into an existing domain.
- In order to prepare a switch to enter an existing VTP domain, perform the following steps.
  - Delete the VLAN database, erase the startup configuration, and power cycle the switch.
  - This will avoid potential problems resulting from residual VLAN configurations or adding a switch with a higher VTP configuration revision number that could result in the propagation of incorrect VLAN information.
  - From the privileged mode, issue the **delete vlan.dat** and **erase startup-config** commands, then power cycle the switch.

VTP Pruning

- VTP pruning enhances network bandwidth use by reducing unnecessary flooding of traffic, such as broadcast, multicast, unknown, and flooded unicast packets, by default, VTP pruning is disabled.
- VLAN 1 (default) is always pruning ineligible.

```
Switch(vlan)#vtp pruning
To make specific VLANs pruning ineligible
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport trunk pruning vlan
                  remove vlan-id
```

NAT OPERATION

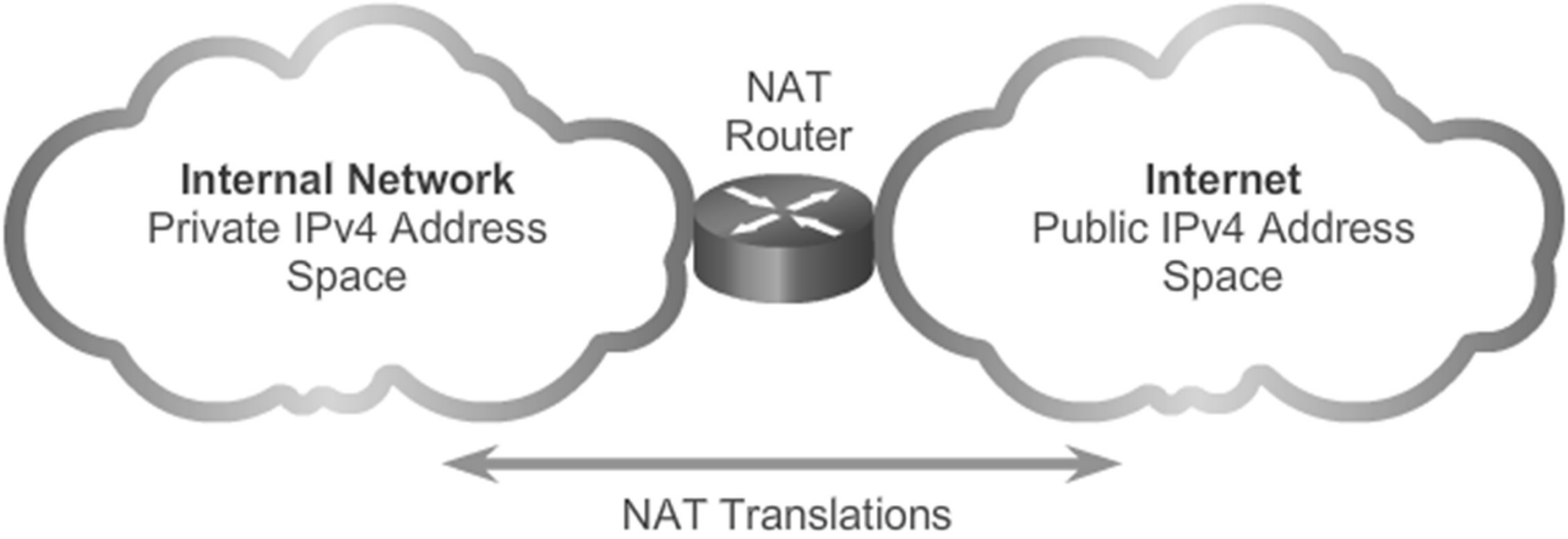
- NAT Characteristics
  - IPv4 Private Address Space
  - What is NAT?
  - NAT Terminology
  - How NAT Works
- Types of NAT
  - Static NAT
  - Dynamic NAT
  - Port Address Translation (PAT)
  - Comparing NAT and PAT
- Benefits of NAT
  - Benefits of NAT
  - Disadvantages of NAT

NAT Characteristics

- 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

NAT Characteristics

- IPv4 Private Address Space

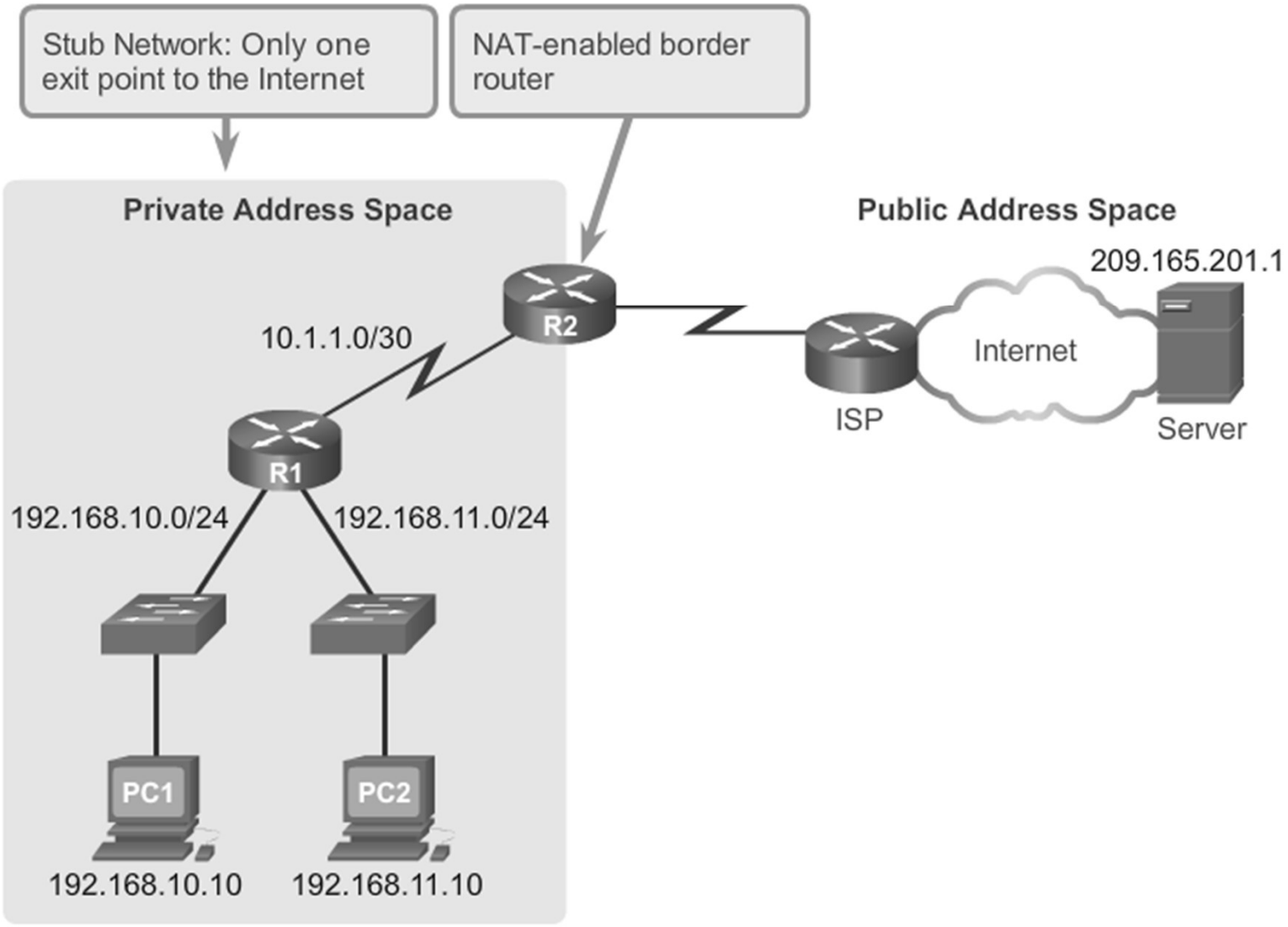


Private Internet addresses are defined in RFC 1918:

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

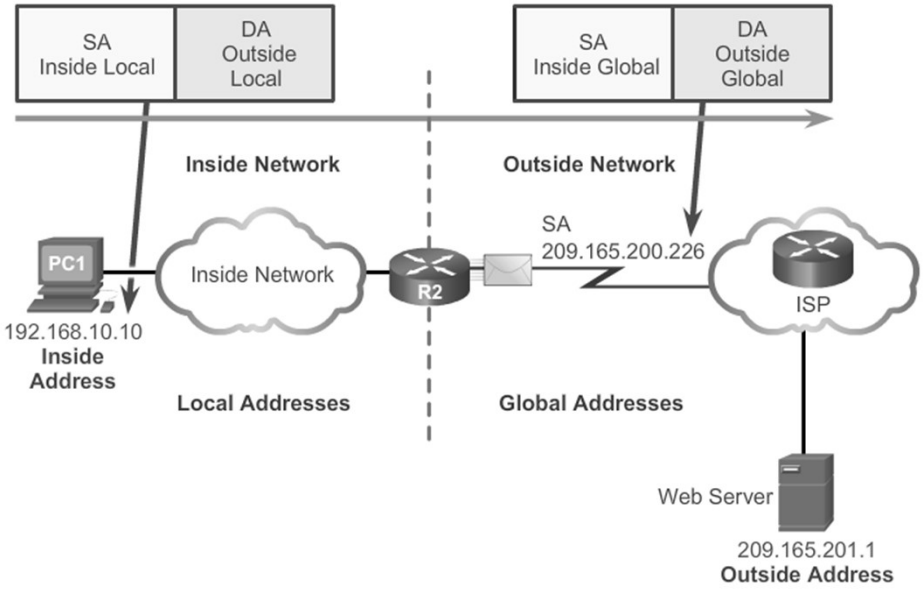
NAT Characteristics

- What is NAT?



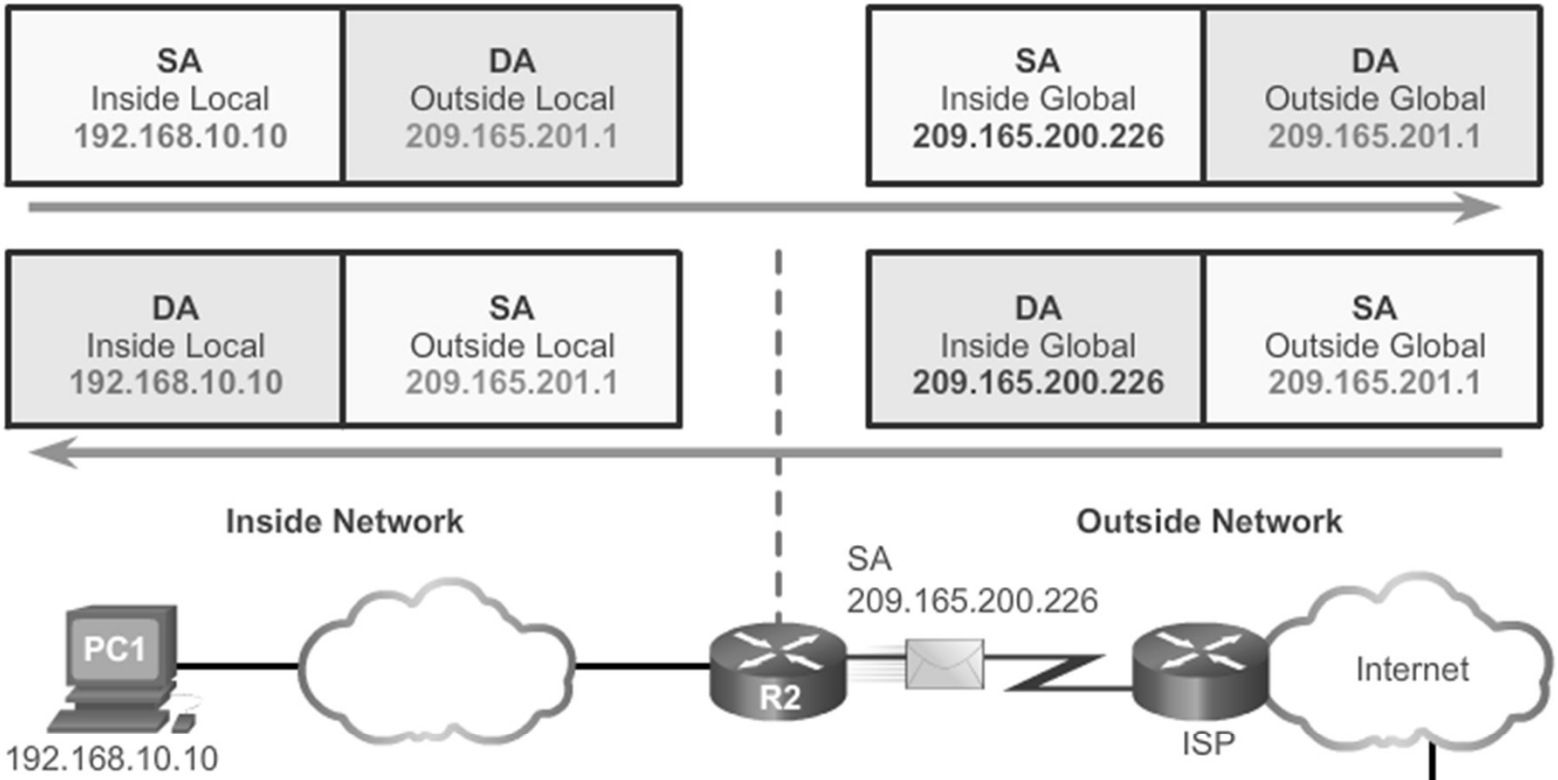
NAT Characteristics

- 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



NAT Operation

- NAT Terminology

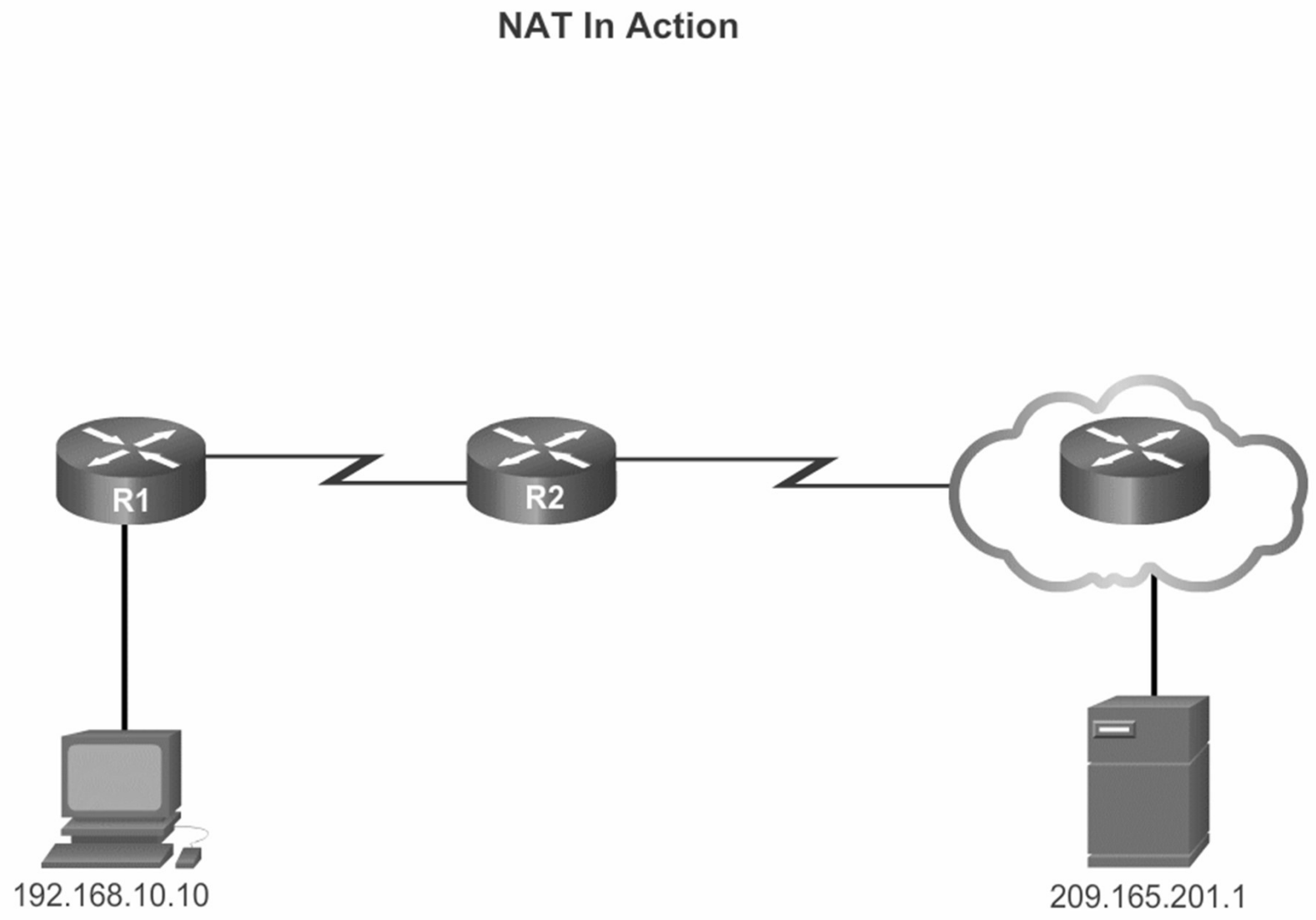


R2 NAT Table

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 Characteristics

- How NAT Works



Types of NAT

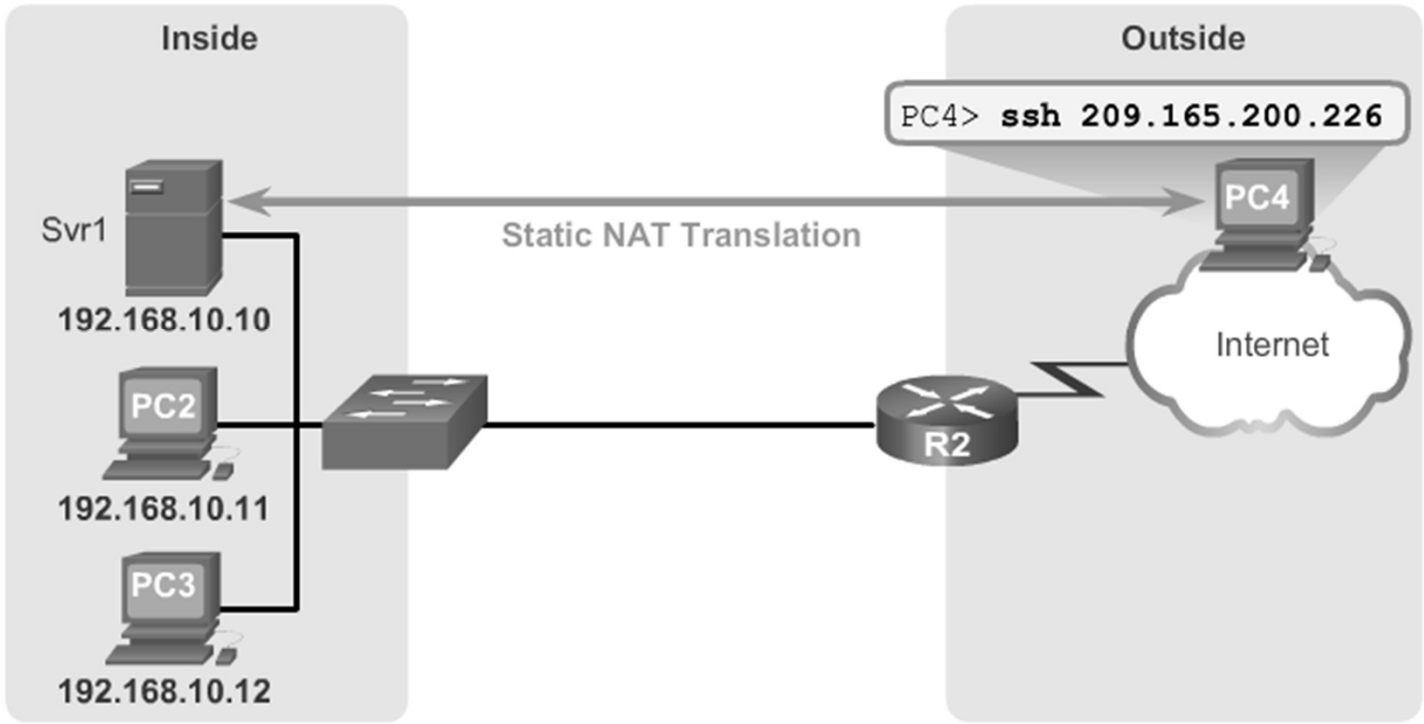
- Static NAT
  - Static NAT uses a one-to-one mapping of local and global addresses
  - These mappings are configured by the network administrator and remain constant
  - Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network
  - A network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

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



Types of NAT

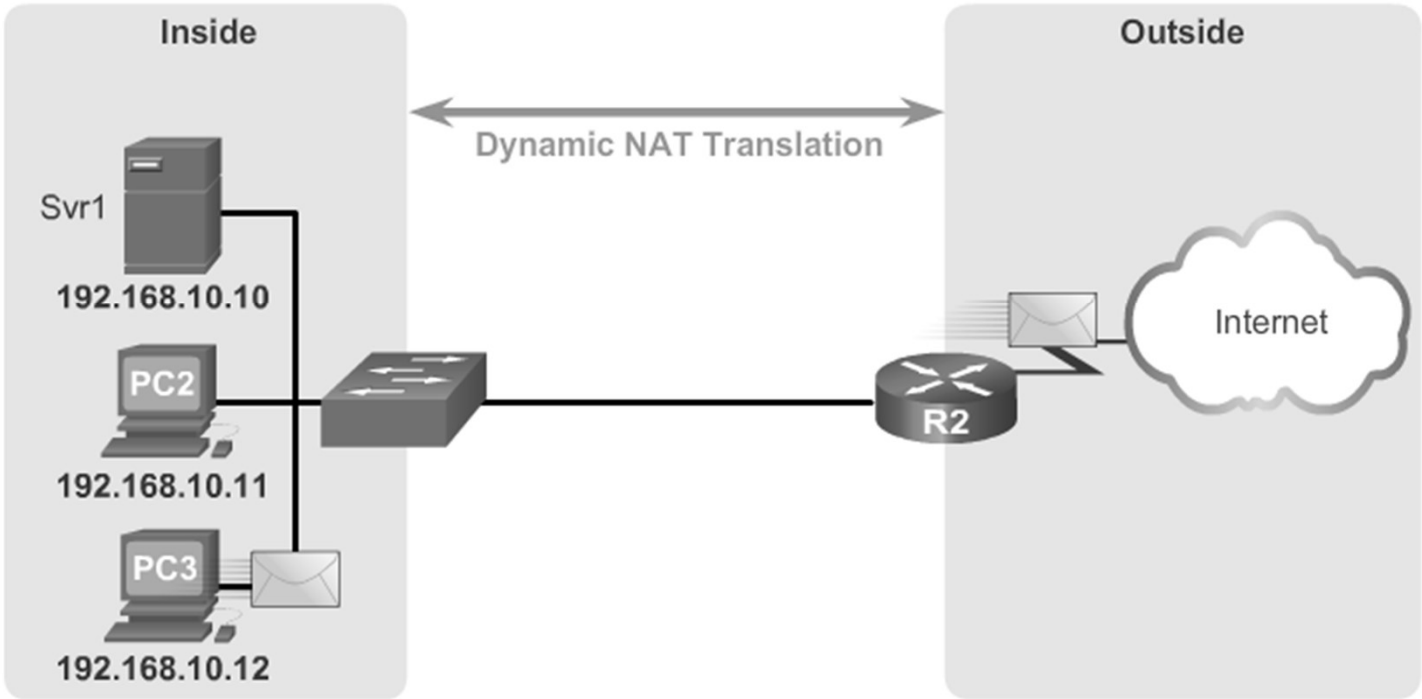
- Dynamic NAT
  - Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis
  - When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool
  - Dynamic NAT requires that enough public addresses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

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



Types of NAT

- 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

Types of NAT

- 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

Benefits & Disadvantages 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

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 NAT

- Configuring Static NAT
  - Configuring Static NAT
  - Analyzing Static NAT
  - Verifying Static NAT
- Configuring Dynamic NAT
  - Dynamic NAT Operation
  - Configuring Dynamic NAT
  - Analyzing Dynamic NAT
  - Verifying Dynamic NAT
- Configuring Port Address Translation (PAT)
  - Configuring PAT: Address Pool
  - Configuring PAT: Single Address
  - Analyzing PAT
  - Verifying PAT
- Port Forwarding

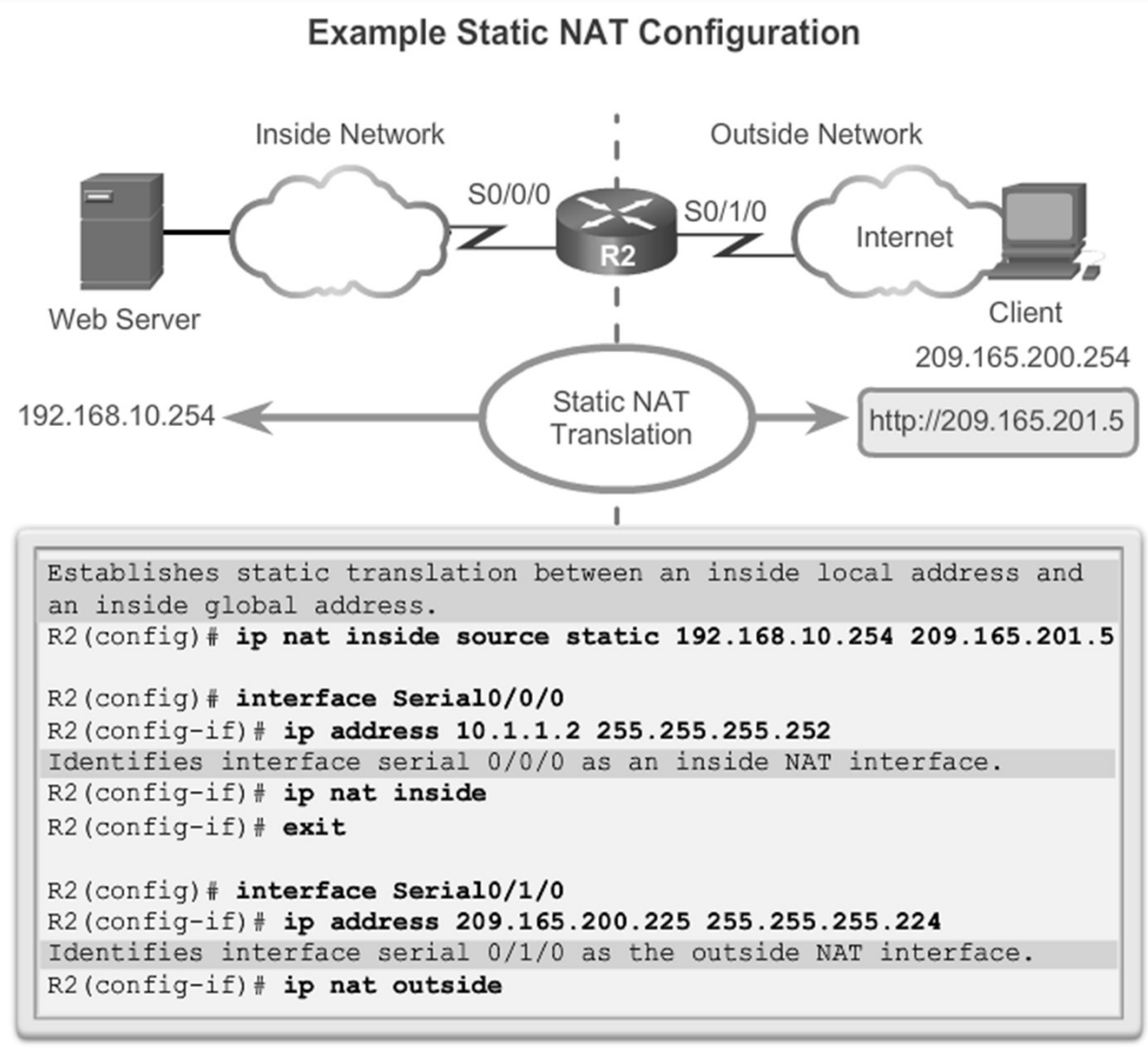
Configuring Static NAT

- 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

Step	Action
1	Establish static translation between an inside local address and an inside global address. `Router(config)# ip nat inside source static local-ip global-ip`
2	Specify the inside interface. `Router(config)# interface type number`
3	Mark the interface as connected to the inside. `Router(config-if)# ip nat inside`
4	Exit interface configuration mode. `Router(config-if)# exit`
5	Specify the outside interface. `Router(config)# interface type number`
6	Mark the interface as connected to the outside. `Router(config-if)# ip nat outside`

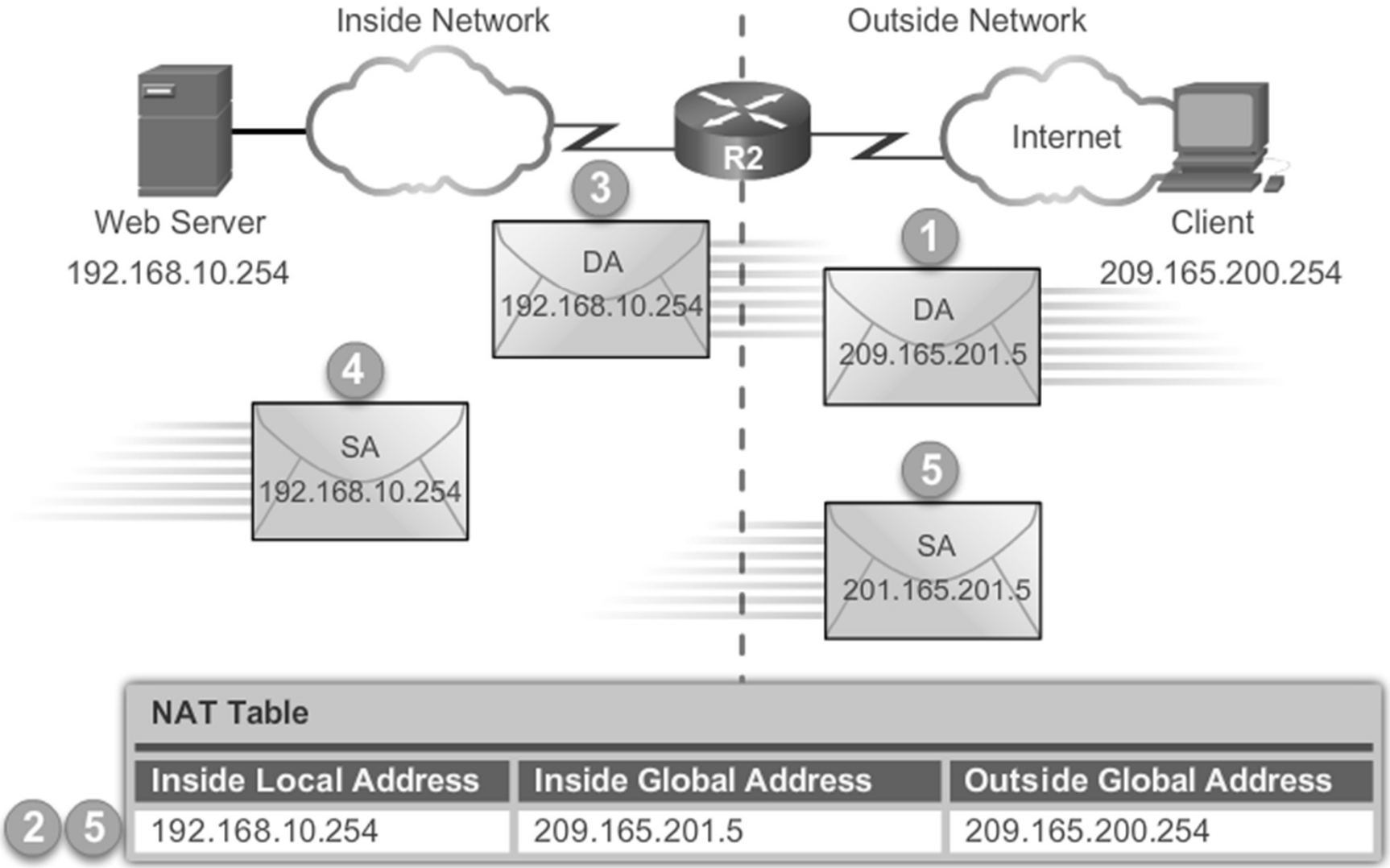
Configuring Static NAT

- Configuring Static NAT



Configuring Static NAT

- Analyzing Static NAT

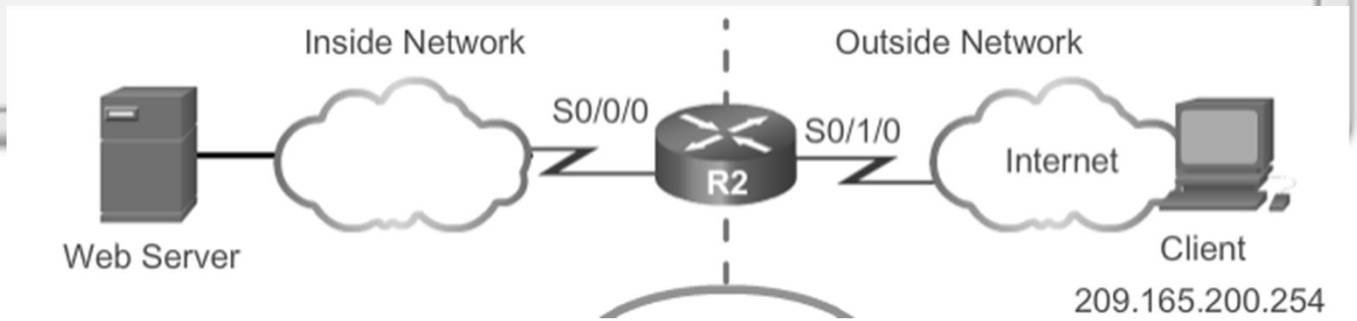


Configuring Static NAT

- 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#
```

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>
```

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

Configuring Dynamic NAT

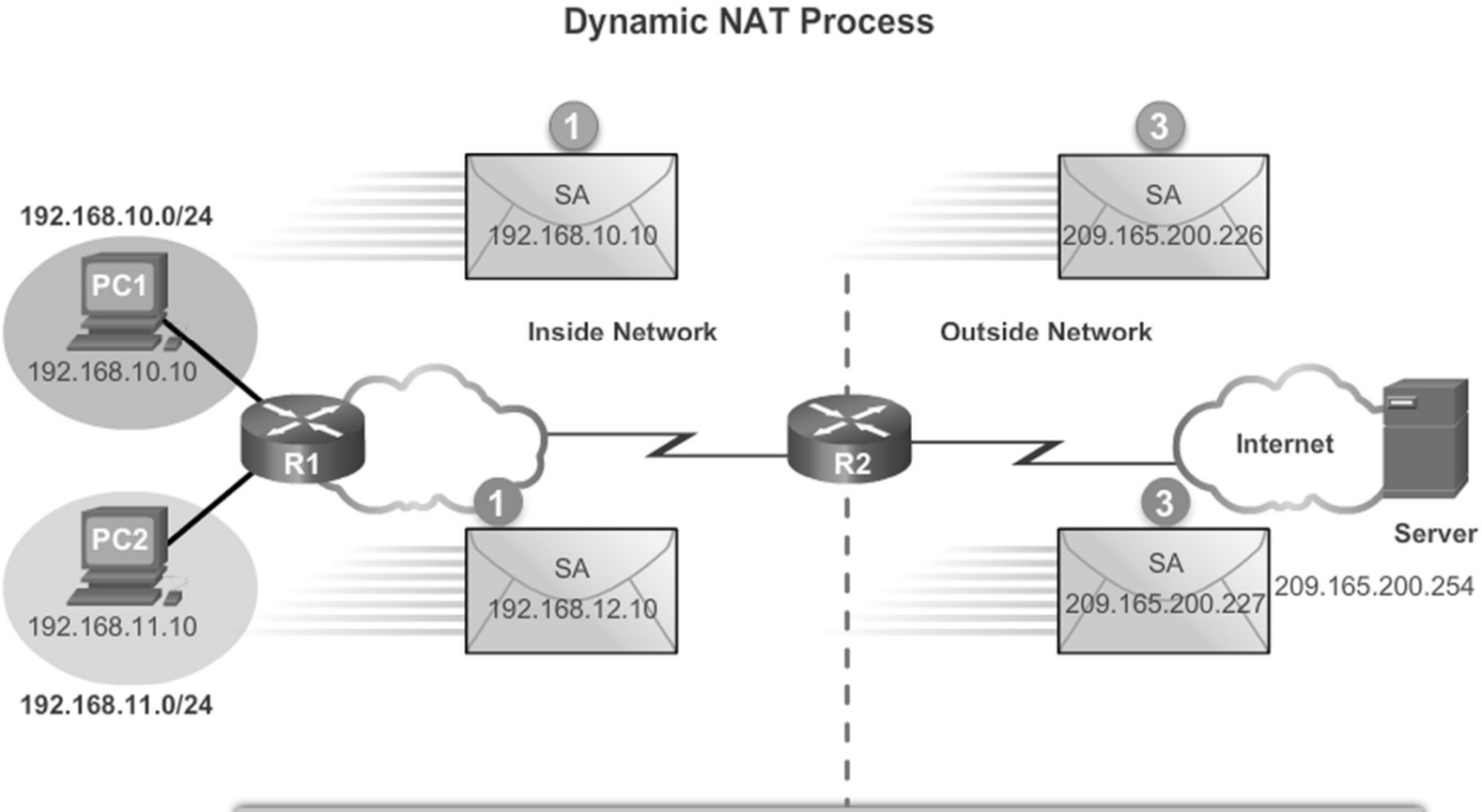
- Configuring Dynamic NAT

Dynamic NAT Configuration Steps

Dynamic NAT Configuration Steps	
Step 1	Define a pool of global addresses to be used for translation. **ip nat pool** *name start-ip end-ip* { **netmask***netmask* | **prefix-length** *prefix-length* }
Step 2	Define a standard access list permitting the addresses that should be translated. **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. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 5	Identify the outside interface. **interface** *type number* **ip nat outside**

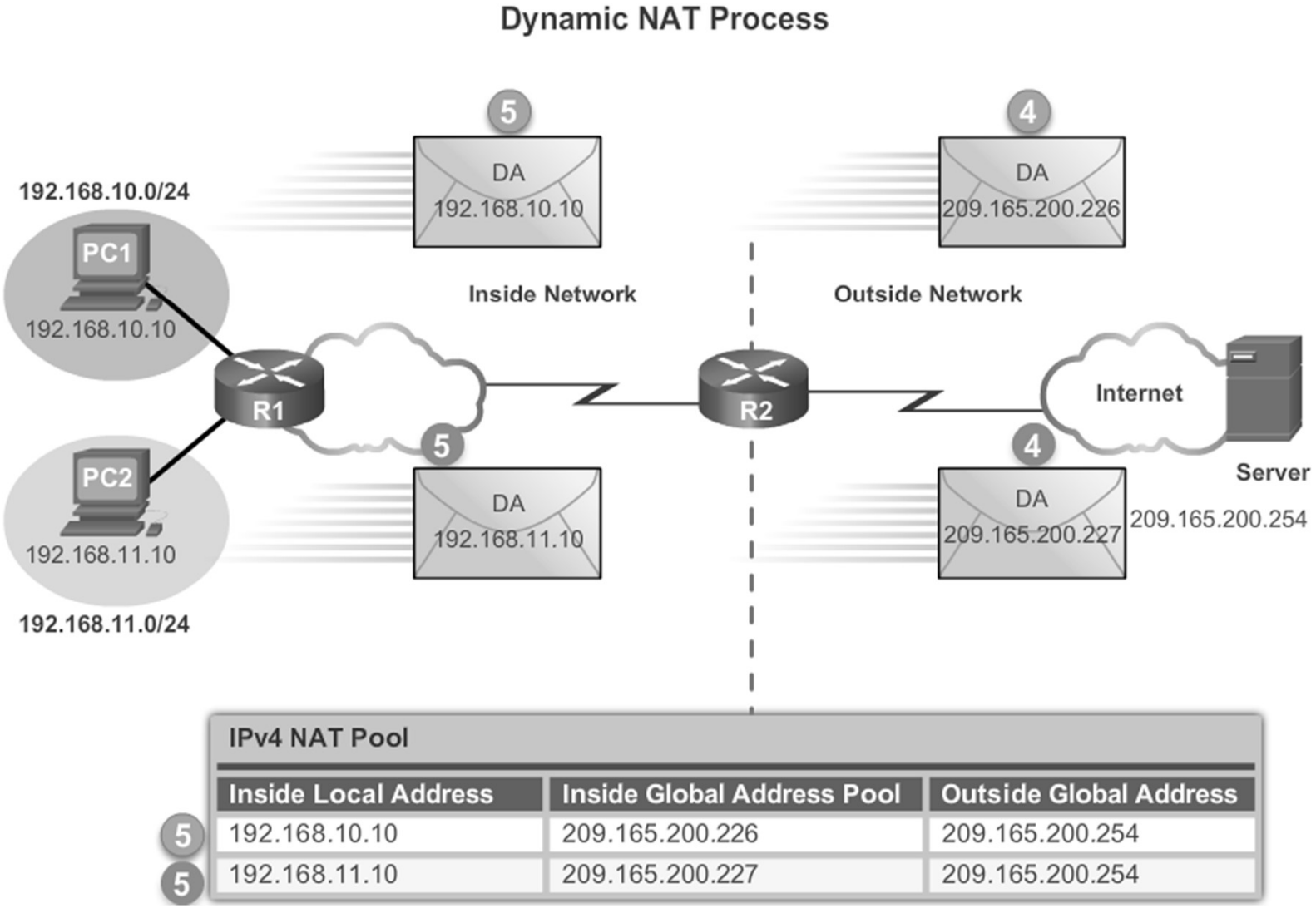
Configuring Dynamic NAT

- Analyzing Dynamic NAT



Configuring Dynamic NAT

- Analyzing Dynamic NAT



Configuring Dynamic NAT

- 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#
```

Configuring Dynamic NAT

- 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#
```

Configuring PAT

- Configuring PAT: Address Pool

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

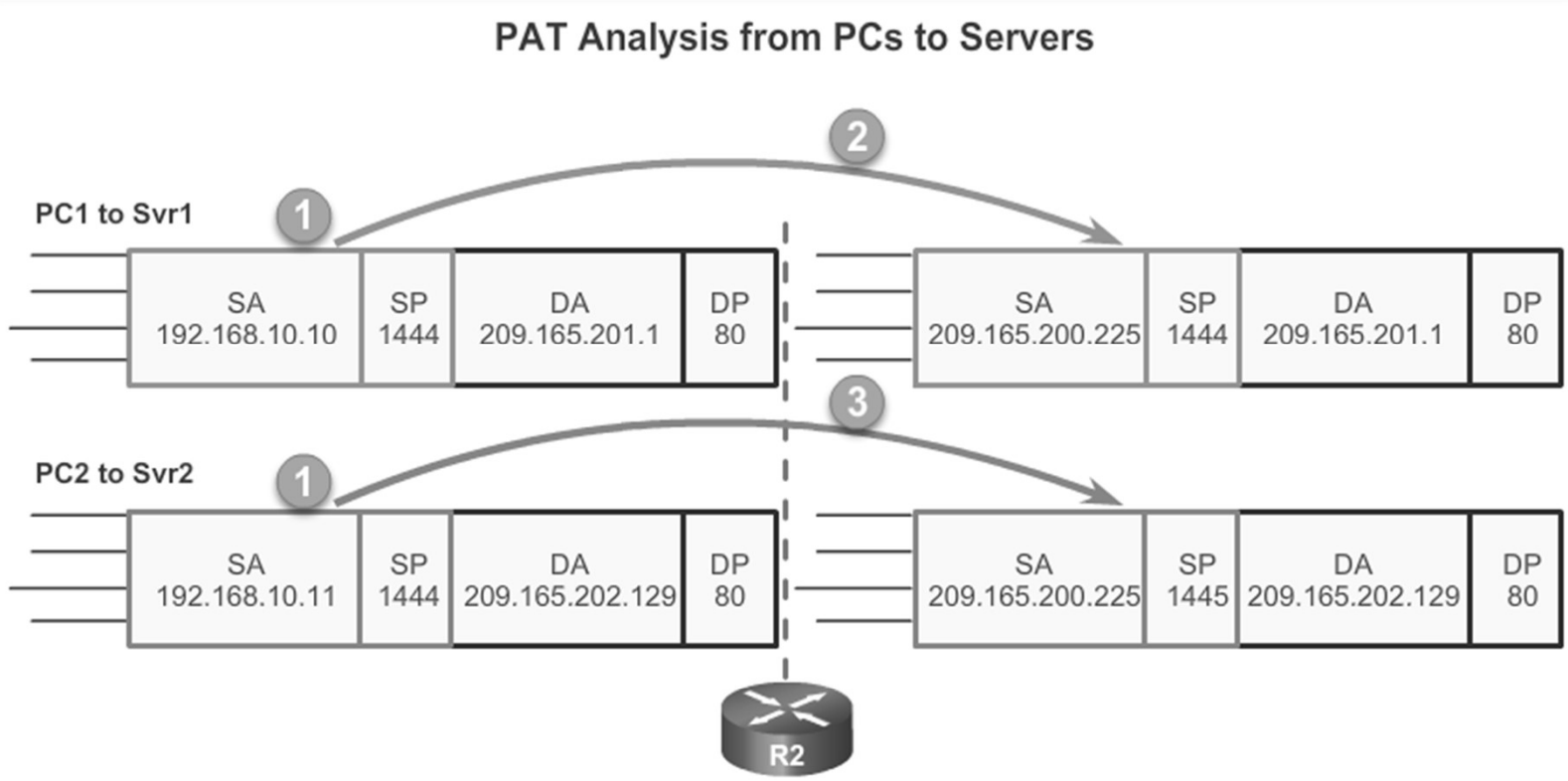
Configuring PAT

- Configuring PAT: Single Address

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

Configuring PAT

- Analyzing PAT

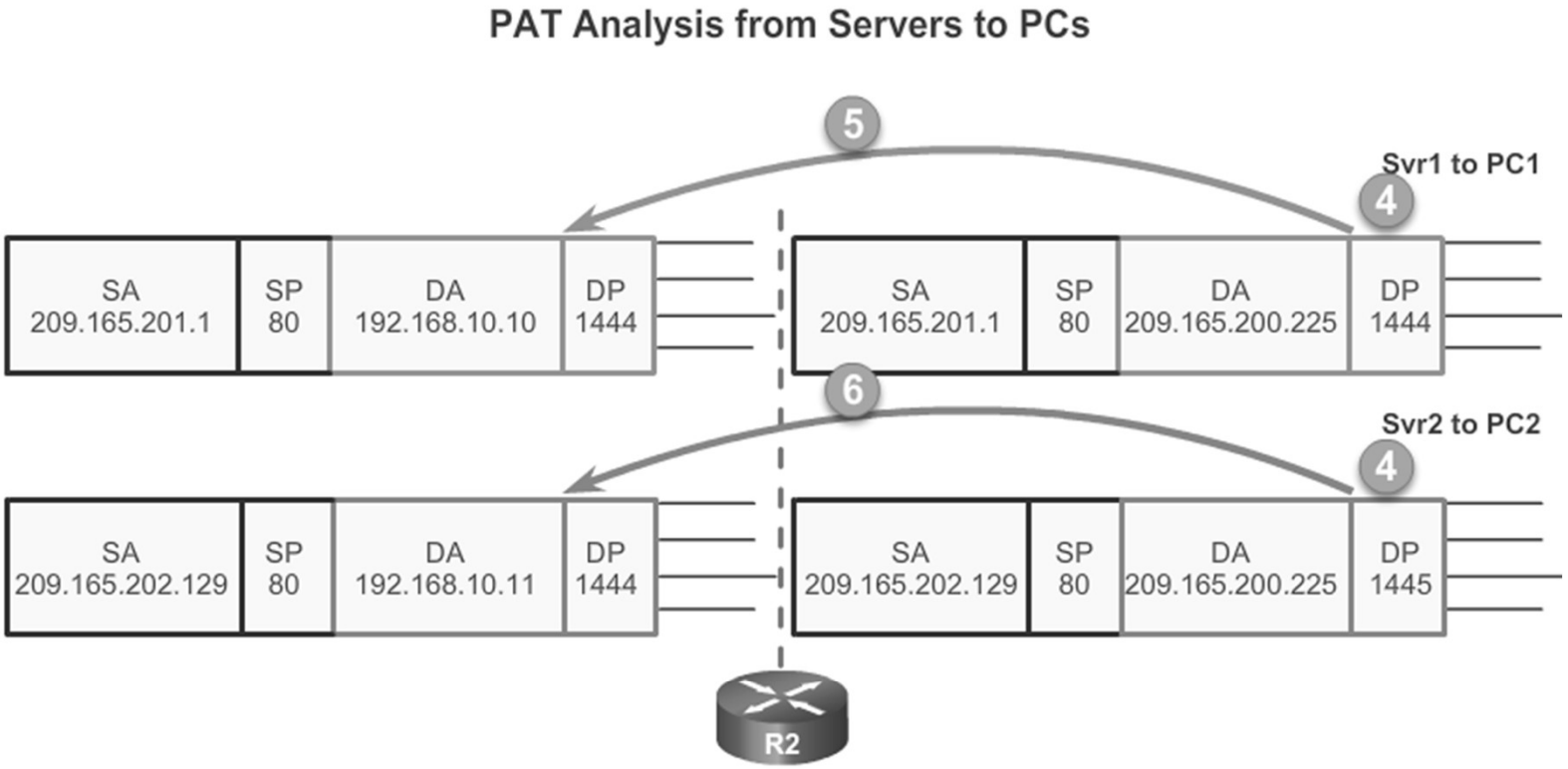


NAT Table

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

Configuring 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

Configuring PAT

- 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#
```

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 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
```

Questions and Answers