Chapter 9: NAT for IPv4

Routing and Switching Essentials 6.0
Planning Guide

Chapter 9 - Sections

9.1 NAT Operation

9.2 Configure NAT

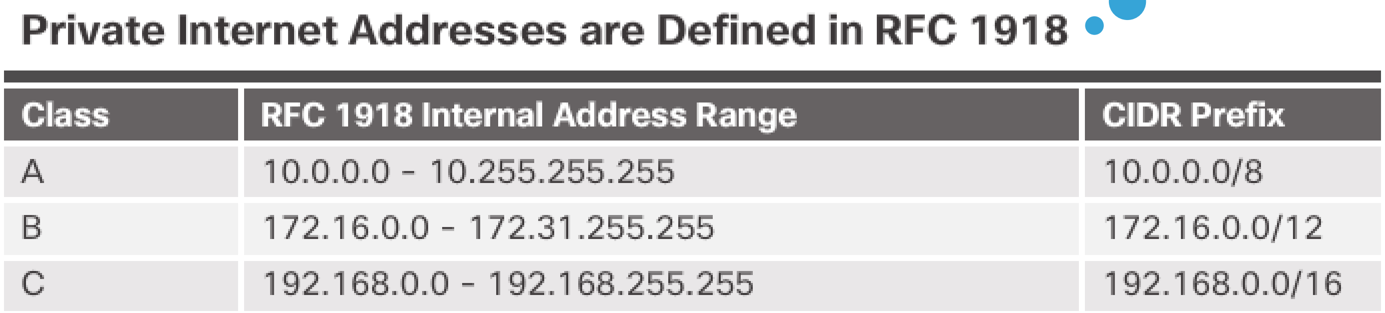
9.3 Troubleshoot NAT

9.4 Něco navíc

9.1 NAT Operation

IPv4 Private Address Space

Did you ever notice how all your labs were based on these addresses?



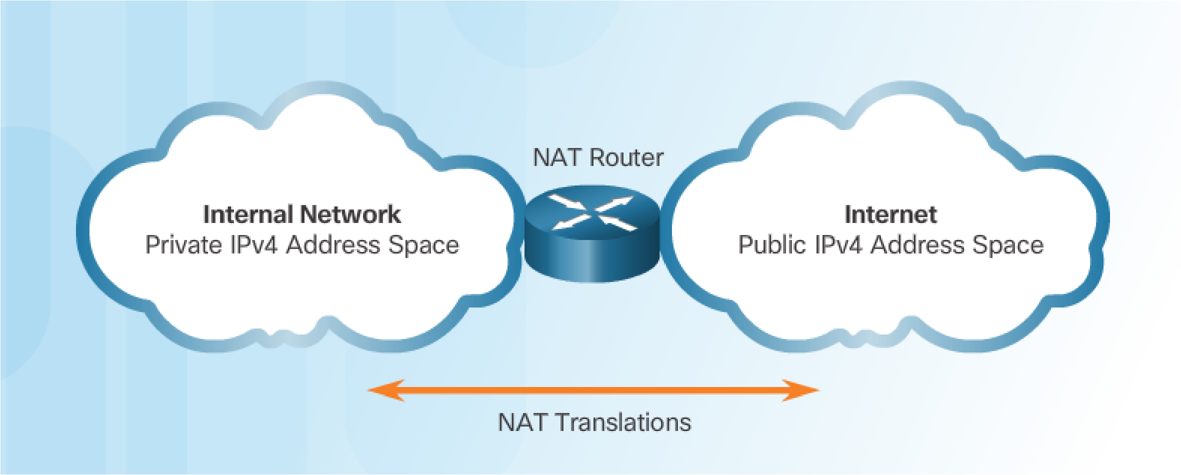
Private Internet Addresses are Defined in RFC 1918

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

These are the IP addresses you will see assigned to company devices.

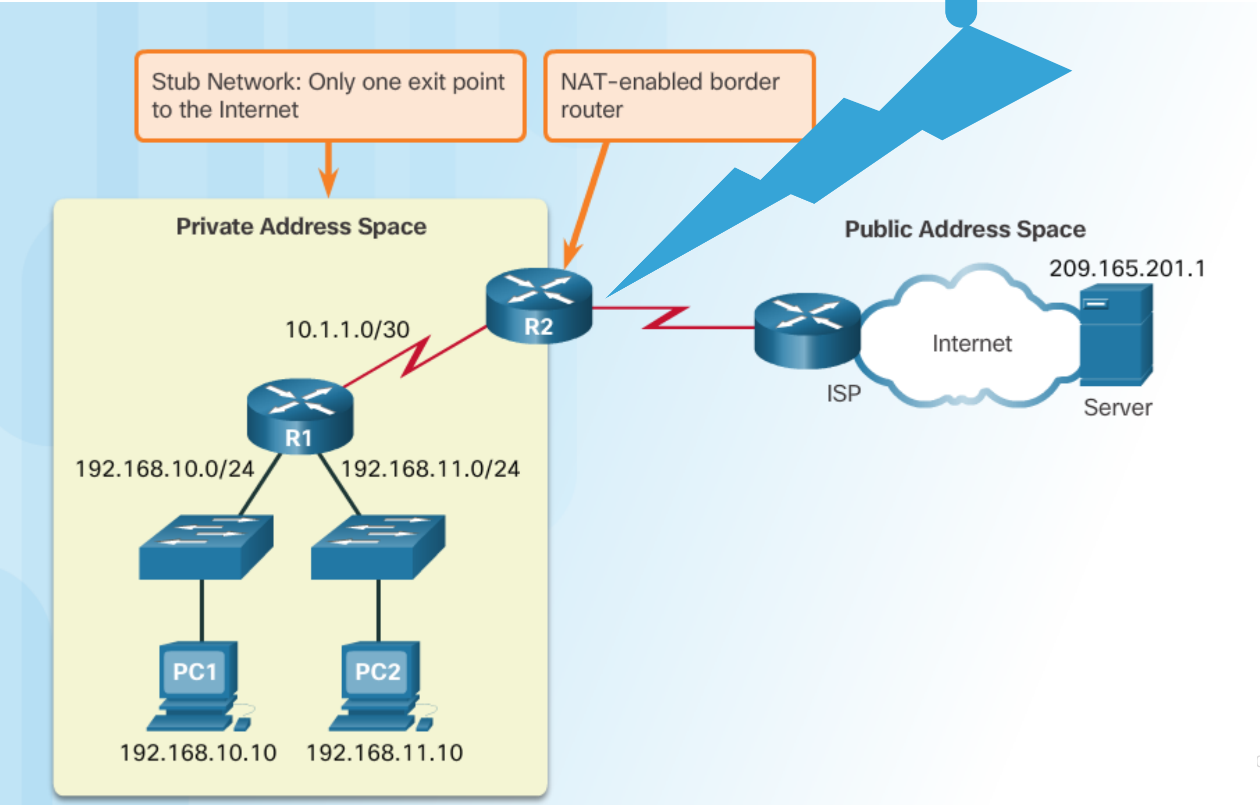
IPv4 Private Address Space (Cont.)

- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses to public addresses that can be routed over the Internet.
- One public IPv4 address can be used for thousands of devices that have private IP addresses.



What is NAT?

Important Concept—NAT is enabled on one device (normally the border or edge router)



Stub Network: Only one exit point to the Internet

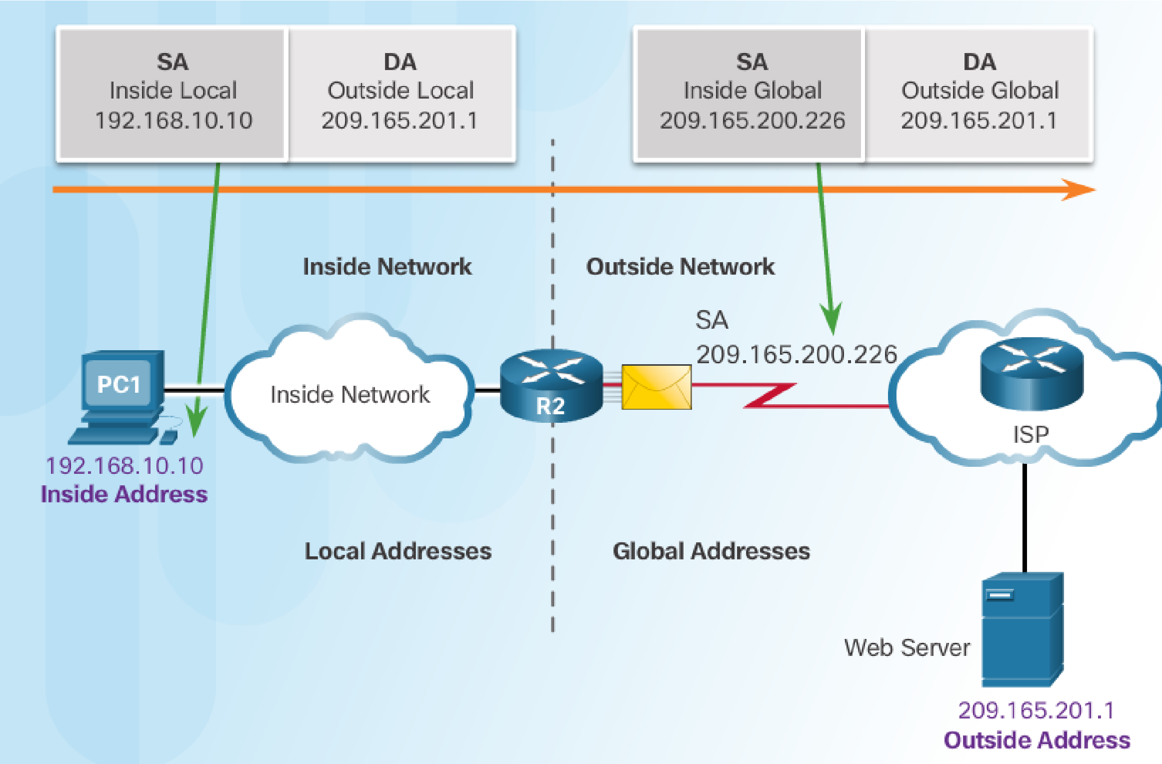
NAT-enabled border router

What is NAT?

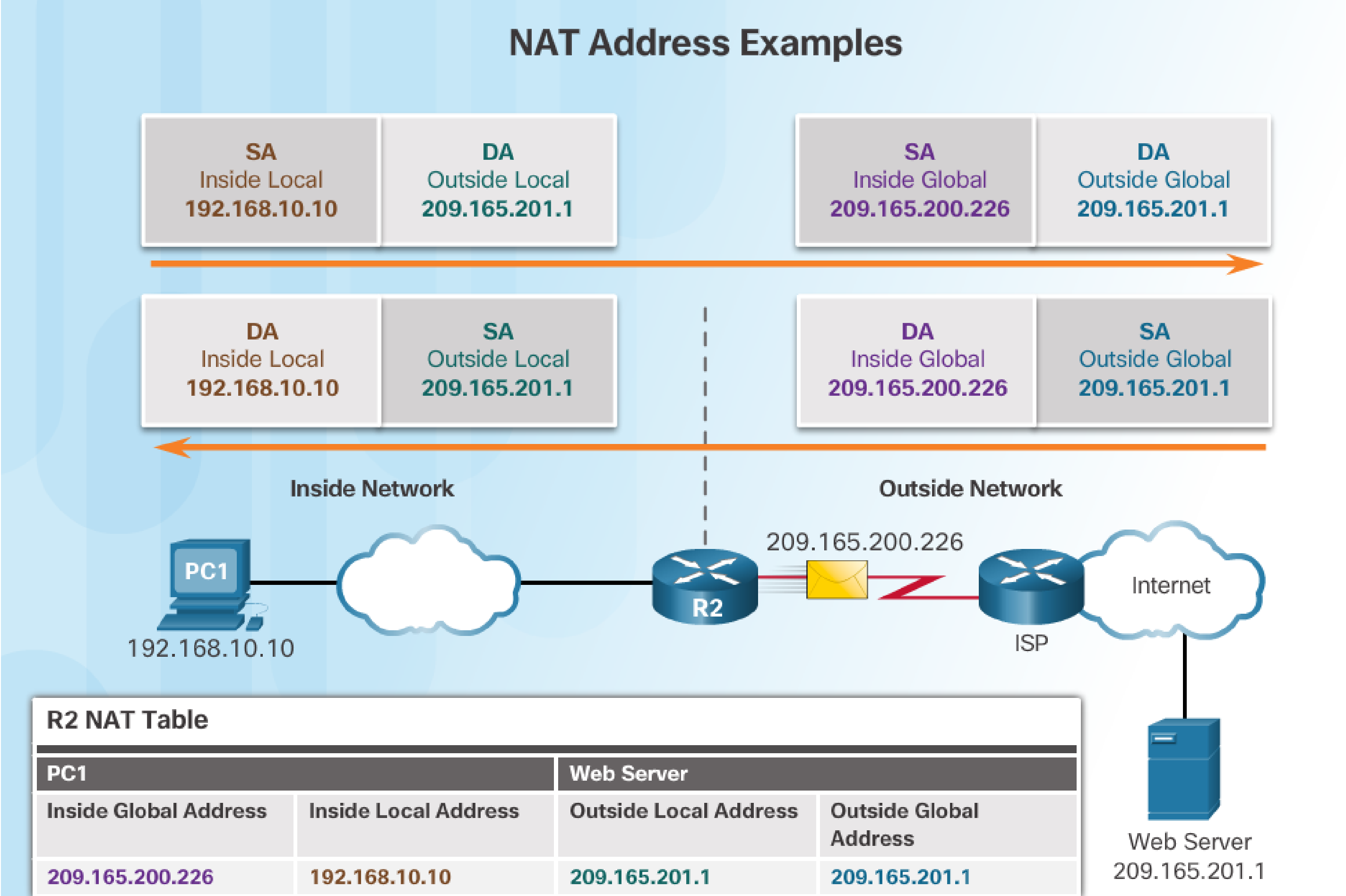
- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses used inside a company to public addresses that can be routed over the Internet.
- NAT hides internal IPv4 addresses from outside networks.
  - Companies use the same private IPv4 addresses so outside devices cannot tell one company’s 10.x.x.x network from another company’s 10.x.x.x network.
- A NAT-enabled router can be configured with a public IPv4 address.
- A NAT-enabled router can be configured with multiple public IPv4 addresses to be used in a pool or NAT pool for internal devices configured with private addresses.

NAT Terminology

- Four types of addresses: inside, outside, local, and global
  - Always consider the device that is having its private address translated to understand this concept.
  - **Inside address** – address of the company network device that is being translated by NAT
  - **Outside address** – IP address of the destination device
  - **Local address** – any address that appears on the inside portion of the network
  - **Global address** – any address that appears on the outside portion of the network



NAT Terminology (Cont.)



NAT Address Examples

SA	DA
Inside Local 192.168.10.10	Outside Local 209.165.201.1

SA	DA
Inside Global 209.165.200.226	Outside Global 209.165.201.1

DA	SA
Inside Local 192.168.10.10	Outside Local 209.165.201.1

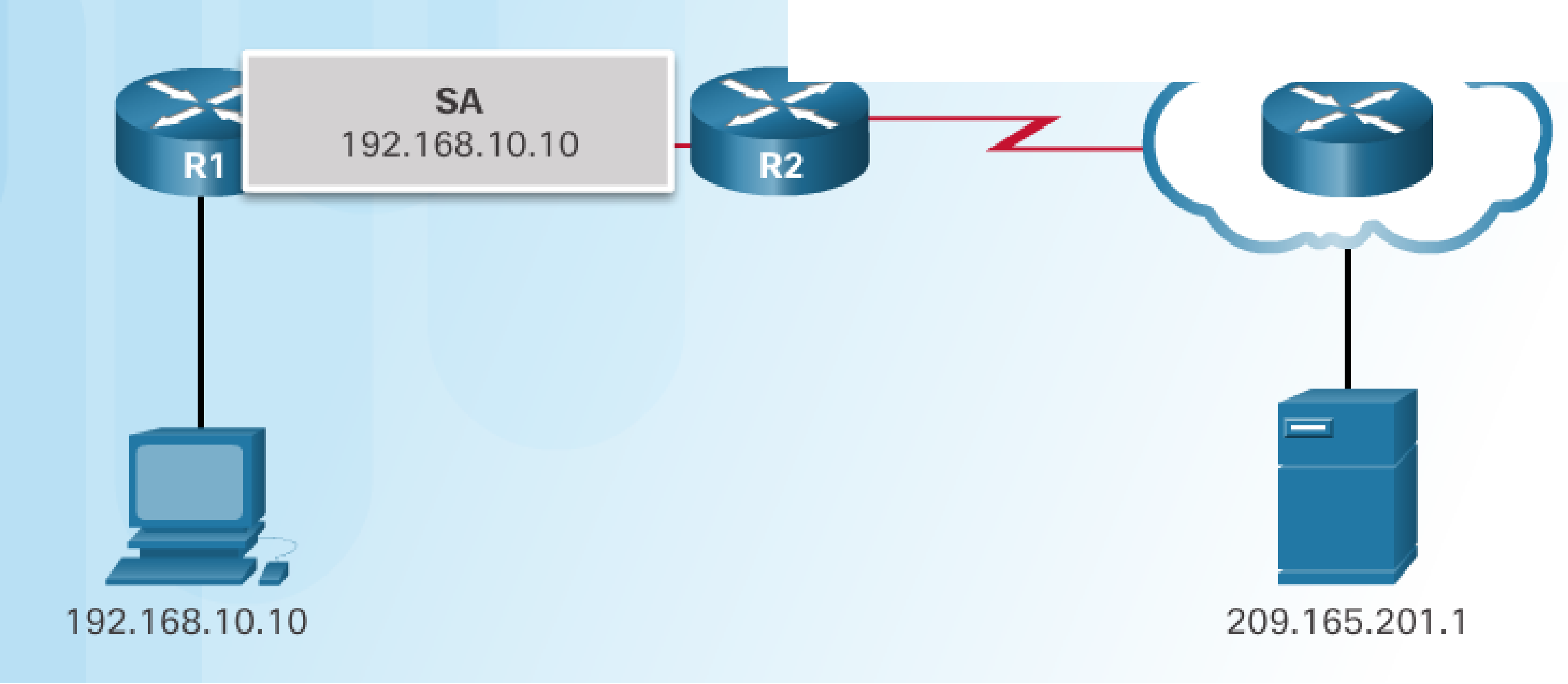
DA	SA
Inside Global 209.165.200.226	Outside Global 209.165.201.1

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

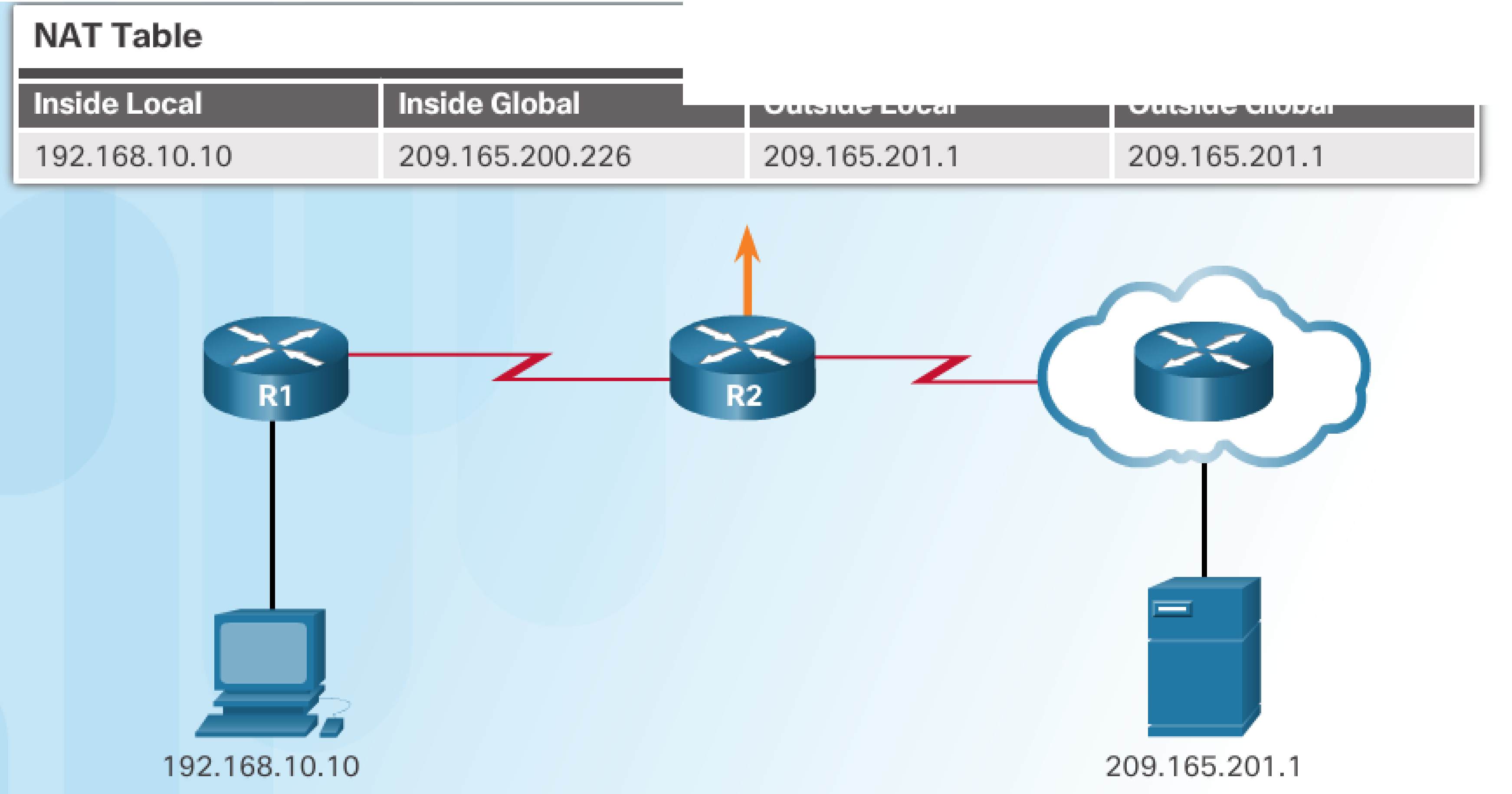
How NAT Works

1. The private (internal) IP address gets translated to a public IP address used to reach the external server.



How NAT Works

1. The private (internal) IP address gets translated to a public IP address used to reach the external server.



NAT Table

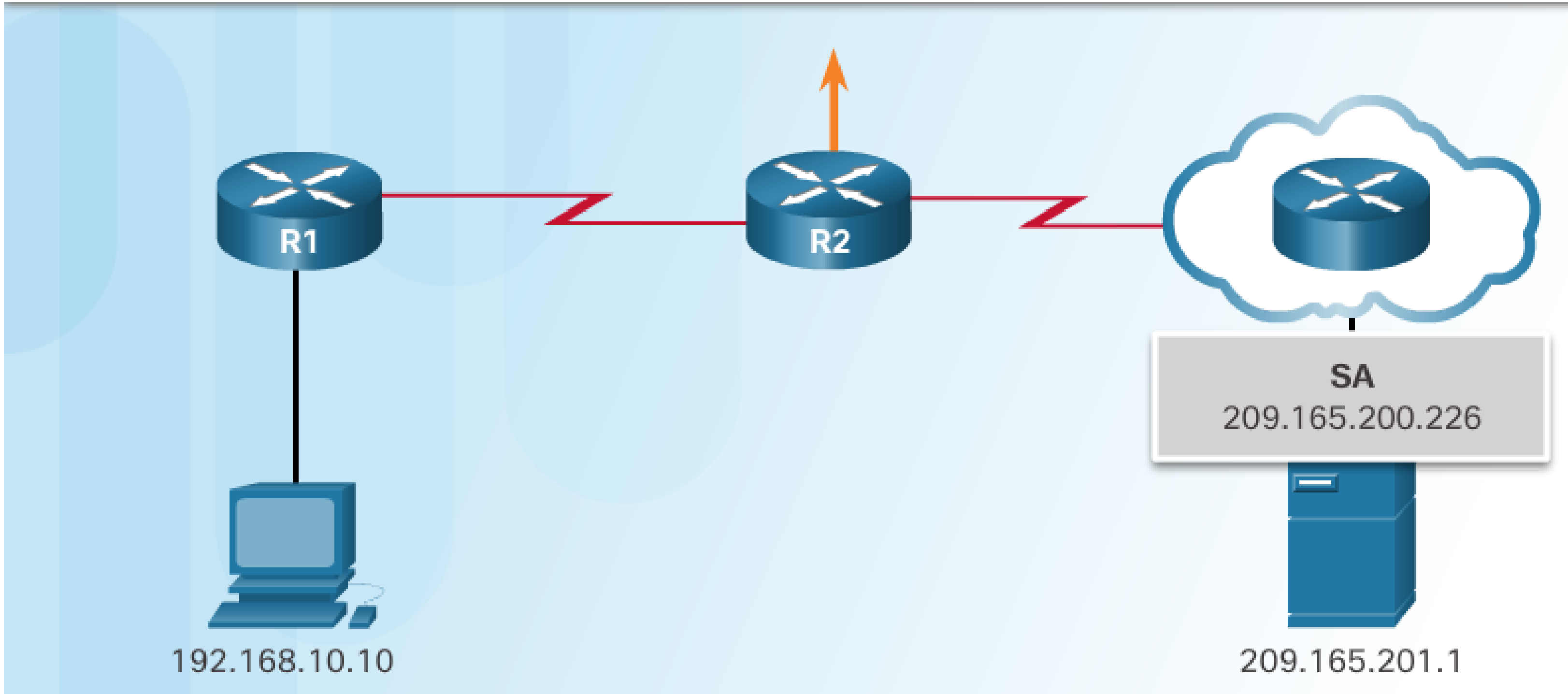
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

How NAT Works

1. The private (internal) IP address gets translated to a public IP address used to reach the external server.

NAT Table

Inside Local	Inside Global		
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

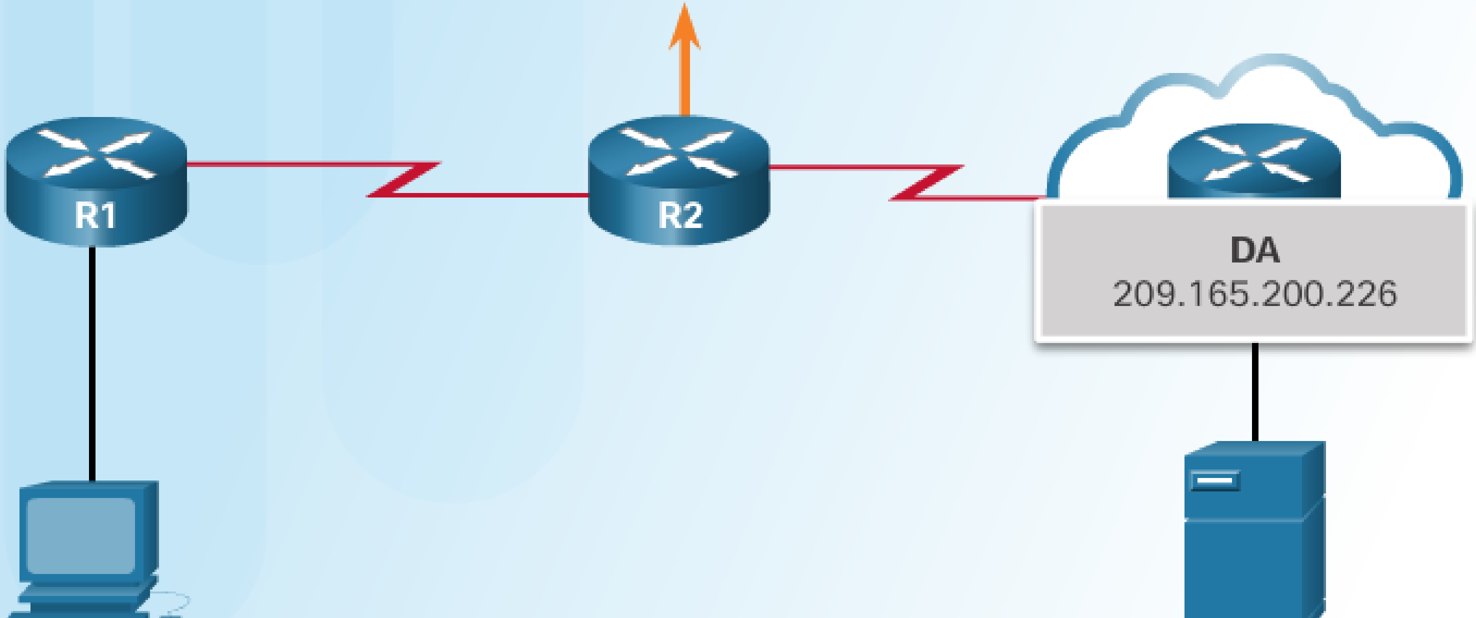


How NAT Works (Cont.)

2. The translated public address is used by the server to send the requested information to the device that actually has a private IP address assigned to it.

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



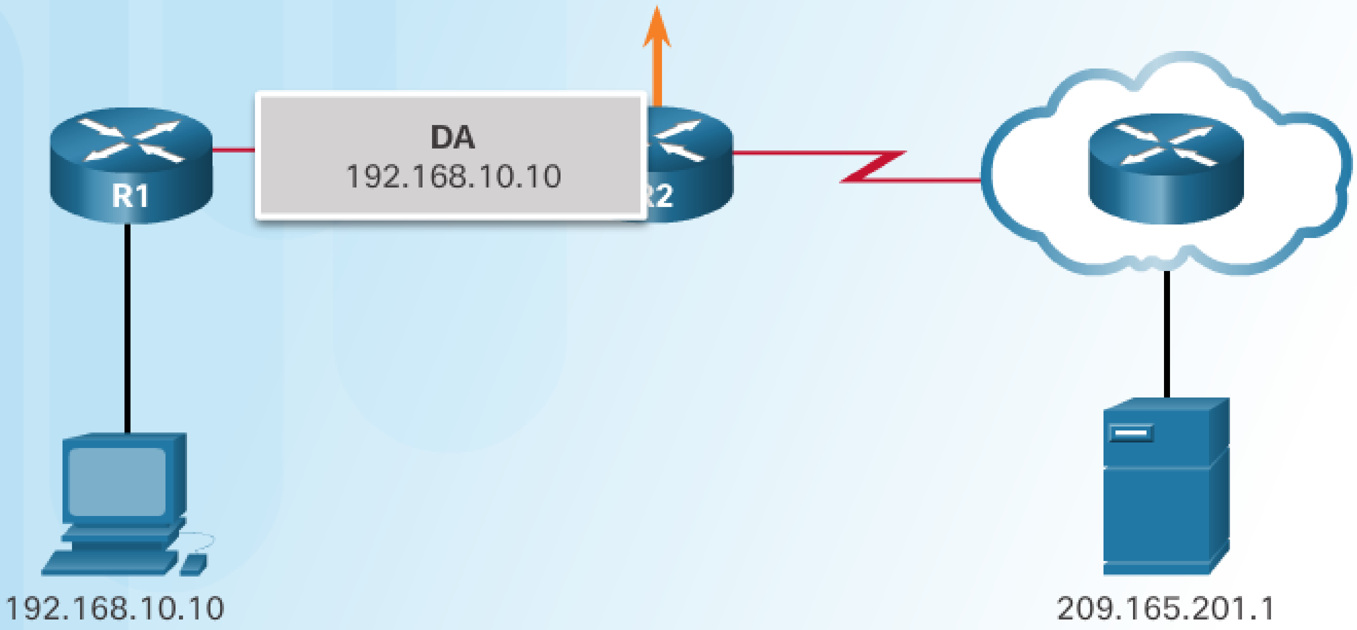
NAT Characteristics

How NAT Works (Cont.)

3. The NAT-enabled router consults the routing table to see what private address requested the data.

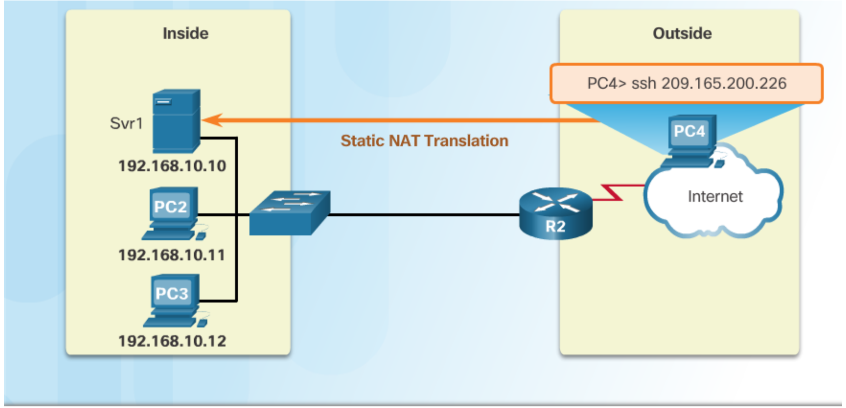
NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Static NAT

- Static address translation (static NAT) assigns one public IP address to one private IP address
- Commonly used for servers that need to be accessed by external devices or for devices that must be accessible by authorized personnel when offsite
- One-to-one address mapping between local and global addresses

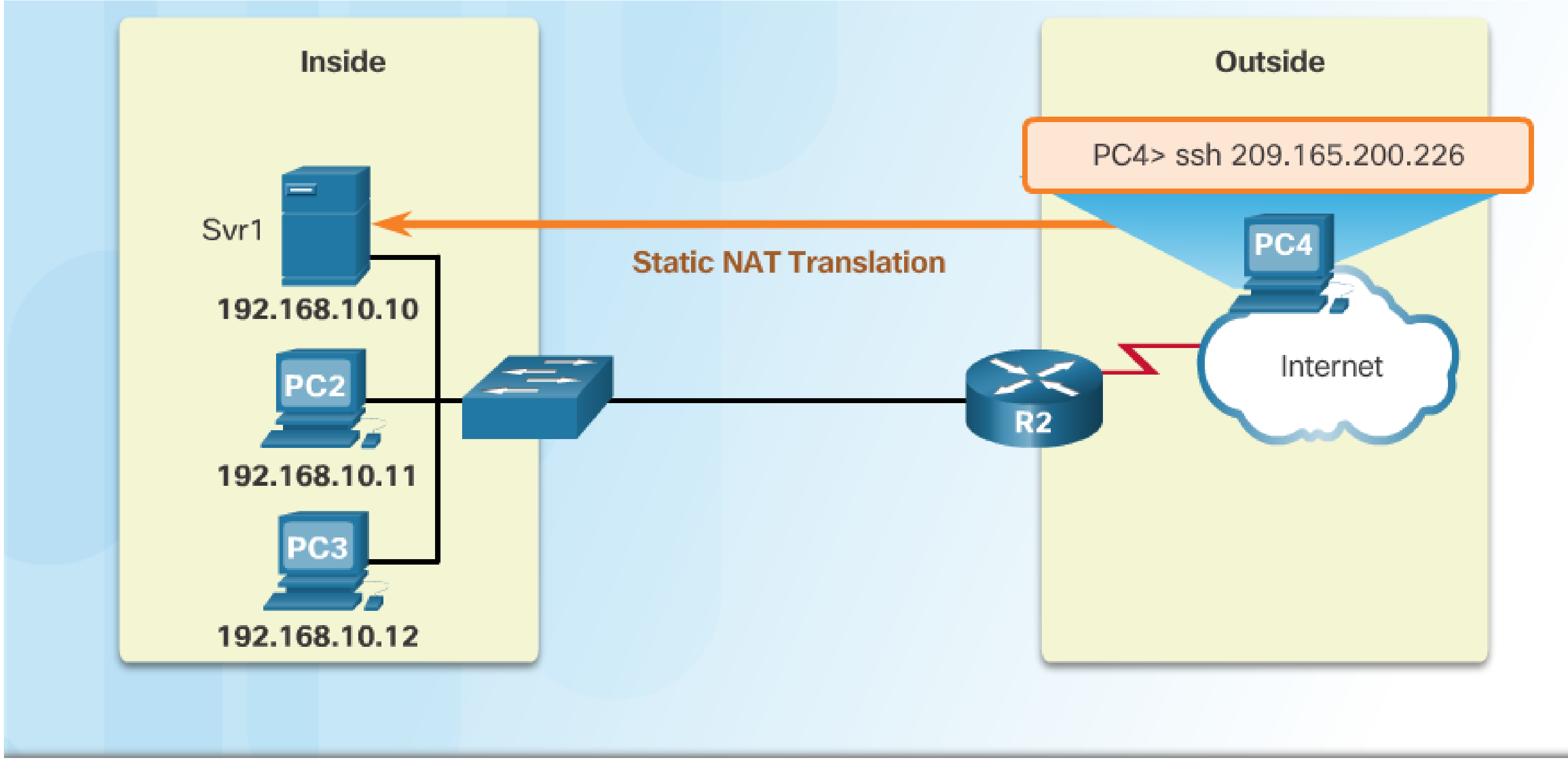


```
PC4> ssh 209.165.200.226
```

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

Static NAT



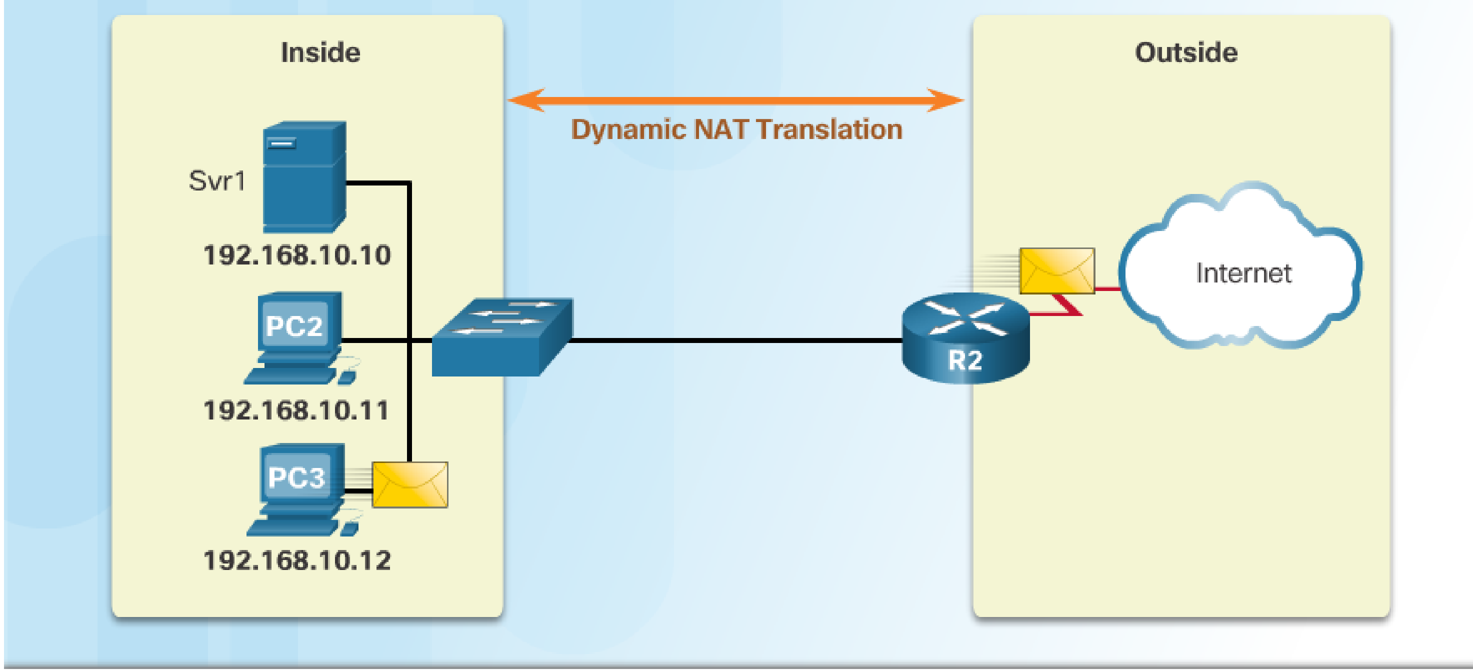
Static NAT Table

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

Dynamic NAT

- Dynamic NAT assigns a public IP address from a pool of addresses to each packet that originates from a device that has a private IP address assigned when that packet is destined to a network outside the company.
  - Addresses are assigned on a first-come, first serve basis
  - The number of internal devices that can transmit outside the company is limited to the number of public IP addresses in the pool.

Dynamic NAT

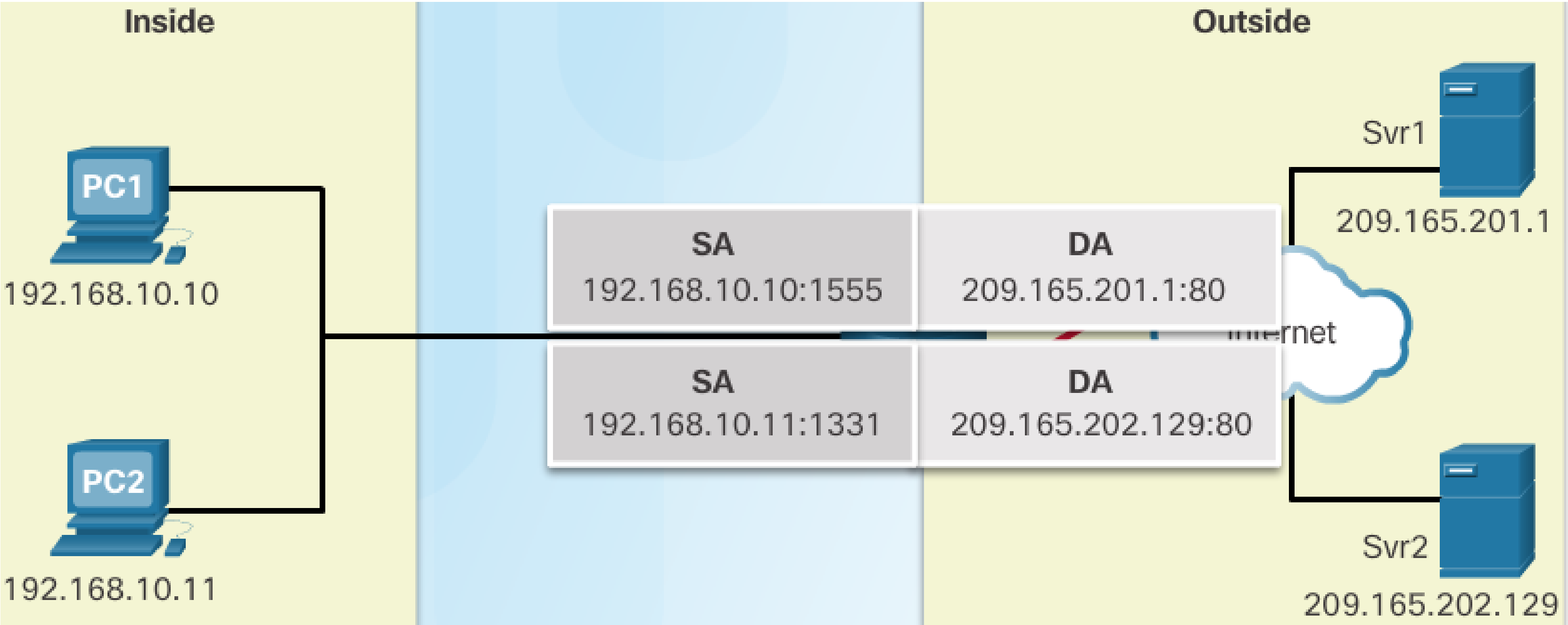


IPv4 NAT Pool

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

Port Address Translation (PAT)

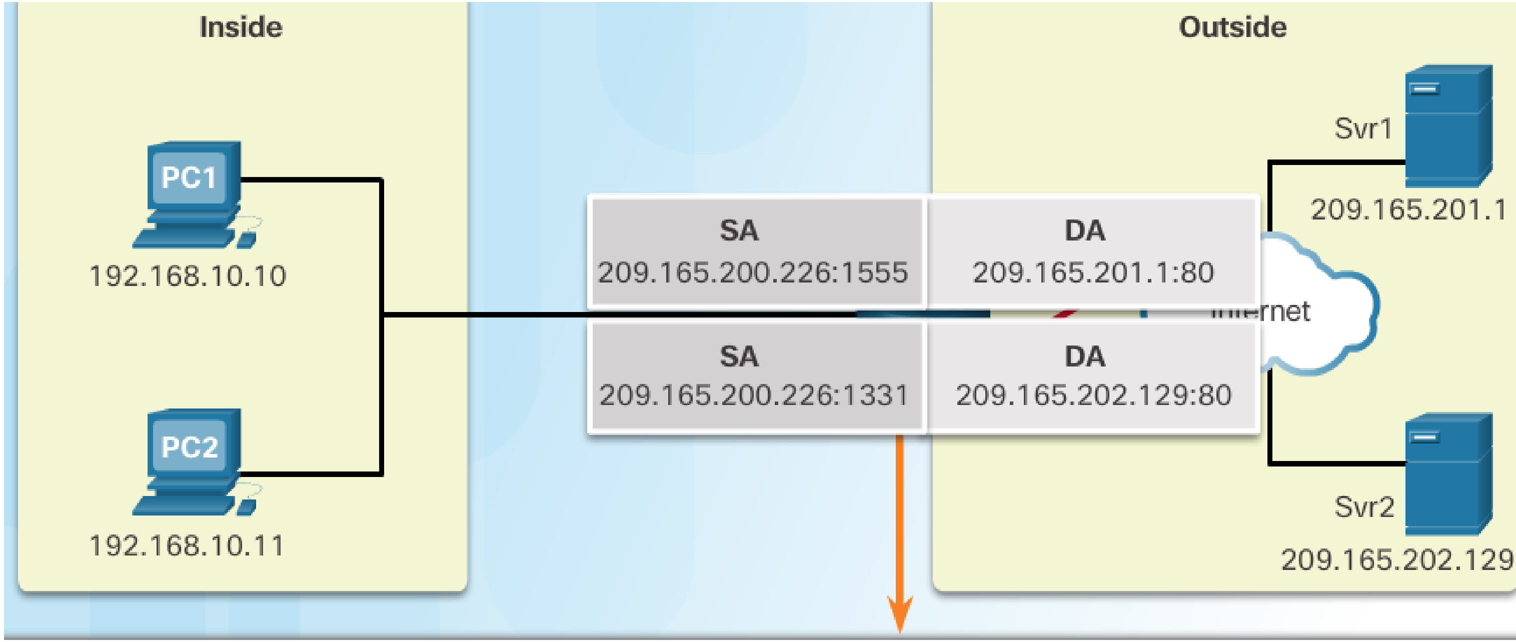
- PAT (otherwise known as NAT overload) can use one public IPv4 address to allow thousand of private IPv4 addresses to communicate with outside network devices.
- Uses port numbers to track the session



SA	DA
192.168.10.10:1555	209.165.201.1:80

SA	DA
192.168.10.11:1331	209.165.202.129:80

Port Address Translation (PAT)



SA	DA
209.165.200.226:1555	209.165.201.1:80
209.165.200.226:1331	209.165.202.129:80

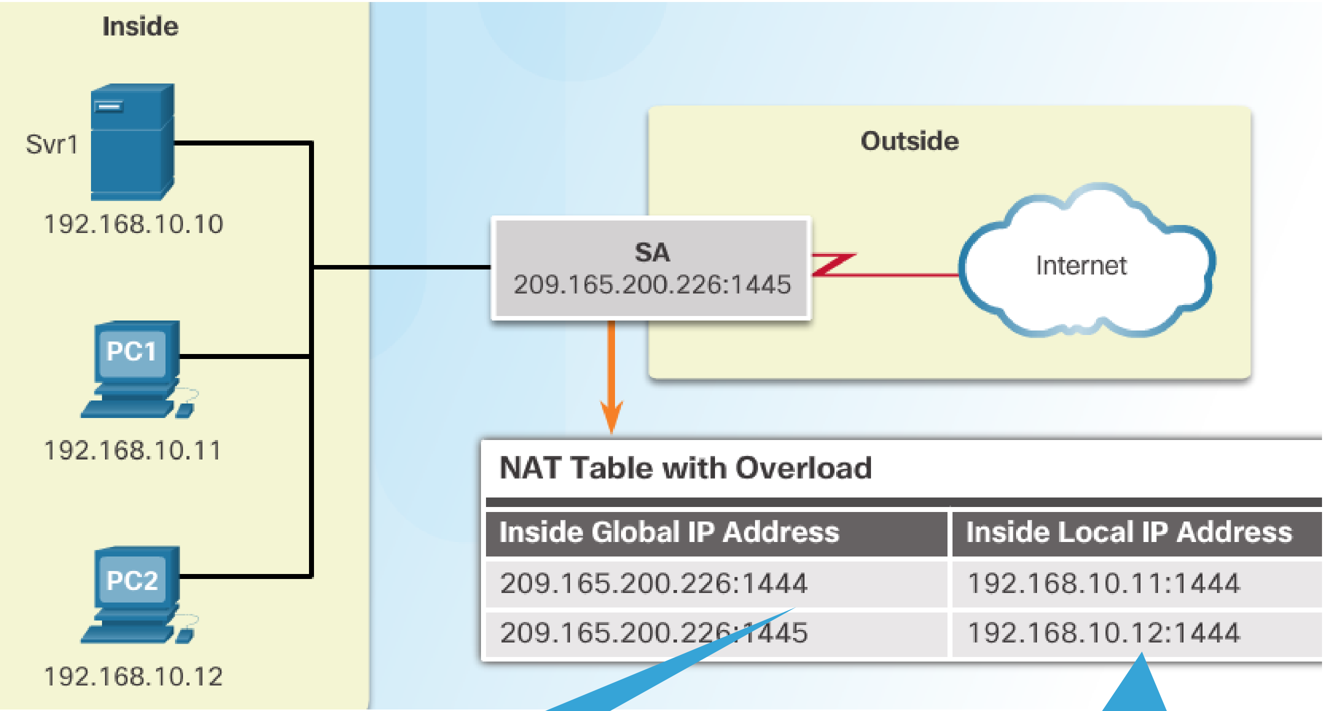
NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Next Available Port

- PAT tries to preserve the original source port number.
  - If that port number is already use, PAT will assign the first available port number for the appropriate port group
    - 0 - 511
    - 512 - 1023
    - 1024 - 65,535
  - When there are no more port numbers available, PAT moves to the next public IP address in the pool if there is one.

Next Available Port



NAT Table with Overload

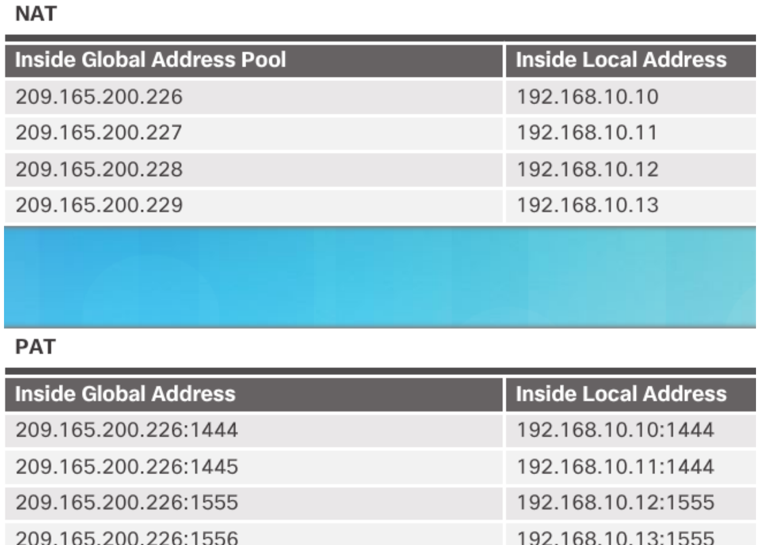
Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

2. Notice how PAT uses the same public address, but two different port numbers.

1. Notice how traffic is from two different internal devices using the same port number.

Comparing NAT and PAT

- Static NAT translates address on a 1:1 basis
- PAT uses port numbers so that one public address can be used for multiple privately addressed devices
  - PAT can still function with a protocol such as ICMP that does not use TCP or UDP



NAT

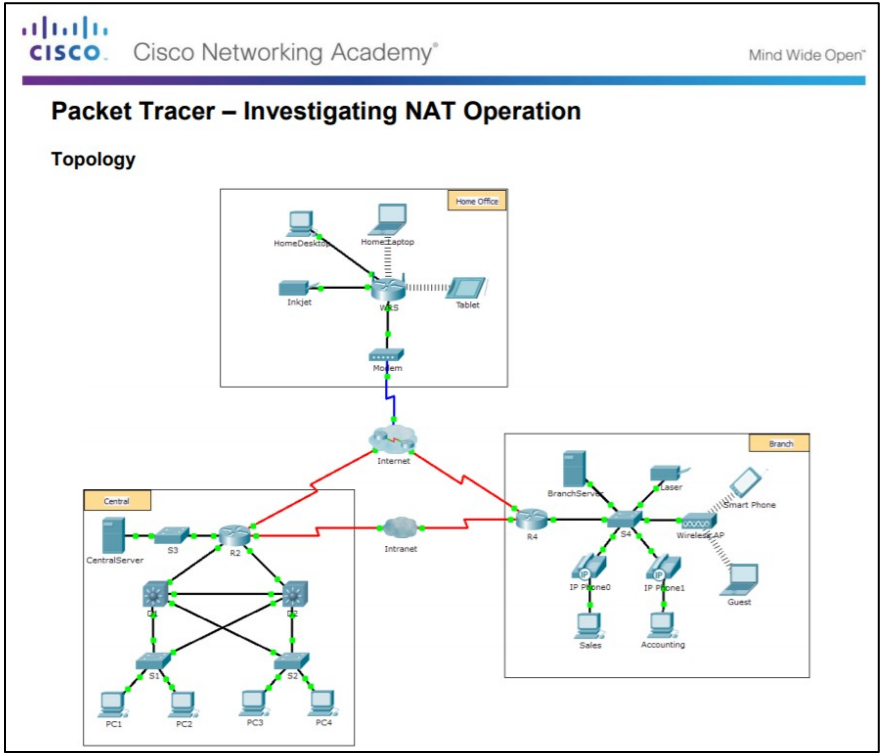
Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

Types of NAT

Packet Tracer – Investigating NAT Operation



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Investigating NAT Operation

Topology

Advantages of NAT

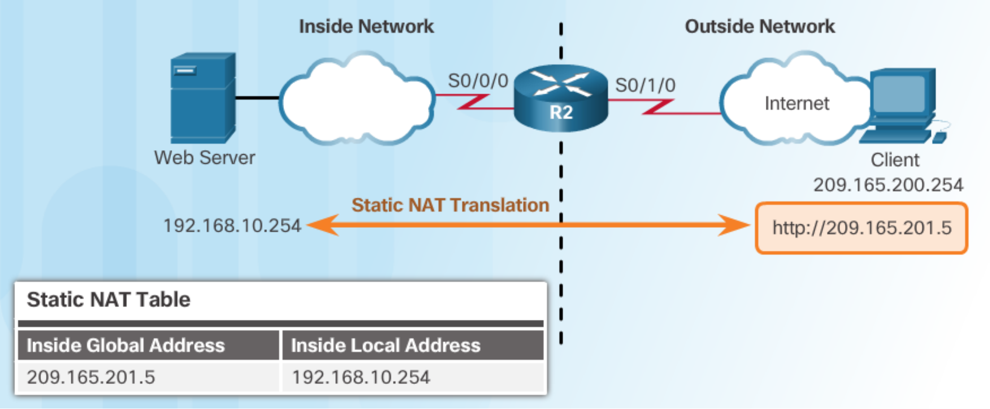
- **Conserves** the legally registered **addressing scheme**
  - *Every company can use the private IP addresses*
- Increases the **flexibility** of connections to the public network
  - *Multiple NAT pools, backup pools, and load-balancing across NAT pools*
- Provides **consistency** for internal network addressing schemes
  - *Do not have to readdress the network if a new ISP or public IP address is assigned*
- Provides network **security**
  - *Hides user private IPv4 addresses*

Disadvantages of NAT

- **Performance** is degraded.
  - The NAT-enabled border device must track and process each session destined for an external network.
- **End-to-end functionality** is degraded.
  - Translation of each IPv4 address within the packet headers takes time.
- **End-to-end IP traceability** is lost.
  - Some applications require end-to-end addressing and can‘t be used with NAT.
  - Static NAT mappings can sometimes be used.
  - Troubleshooting can be more challenging.
- **Tunneling becomes more complicated** (náročnější).
- Initiating **TCP connections can be disrupted**.

9.2 Configure NAT

Configure Static NAT



Static NAT Table

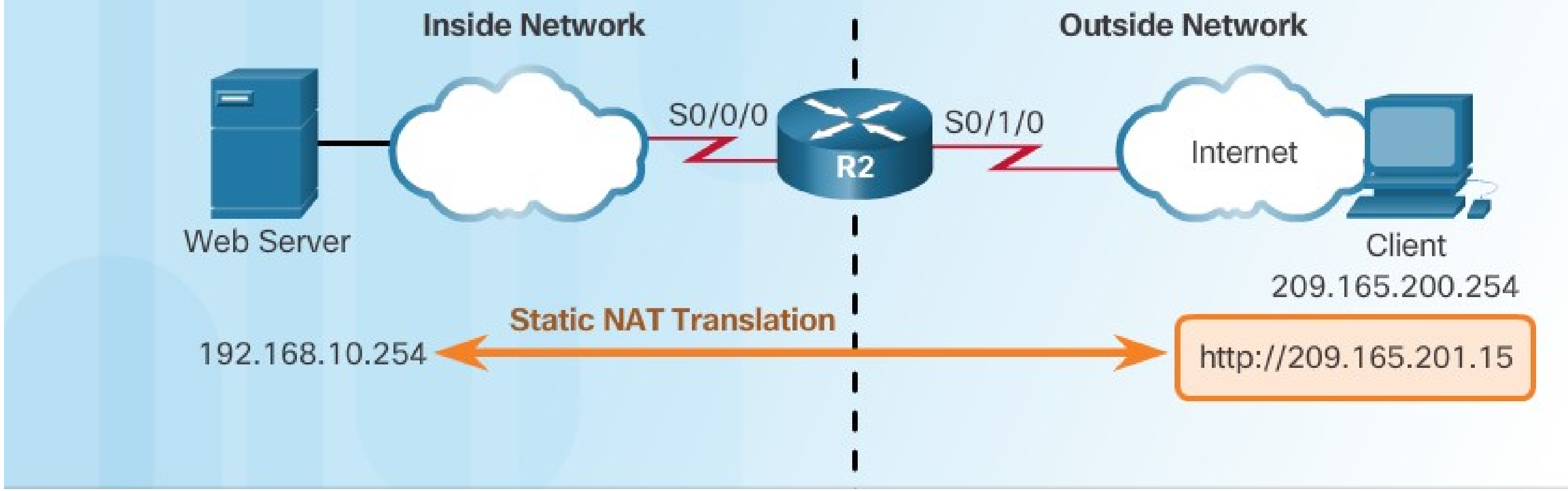
Inside Global Address	Inside Local Address
209.165.201.5	192.168.10.254

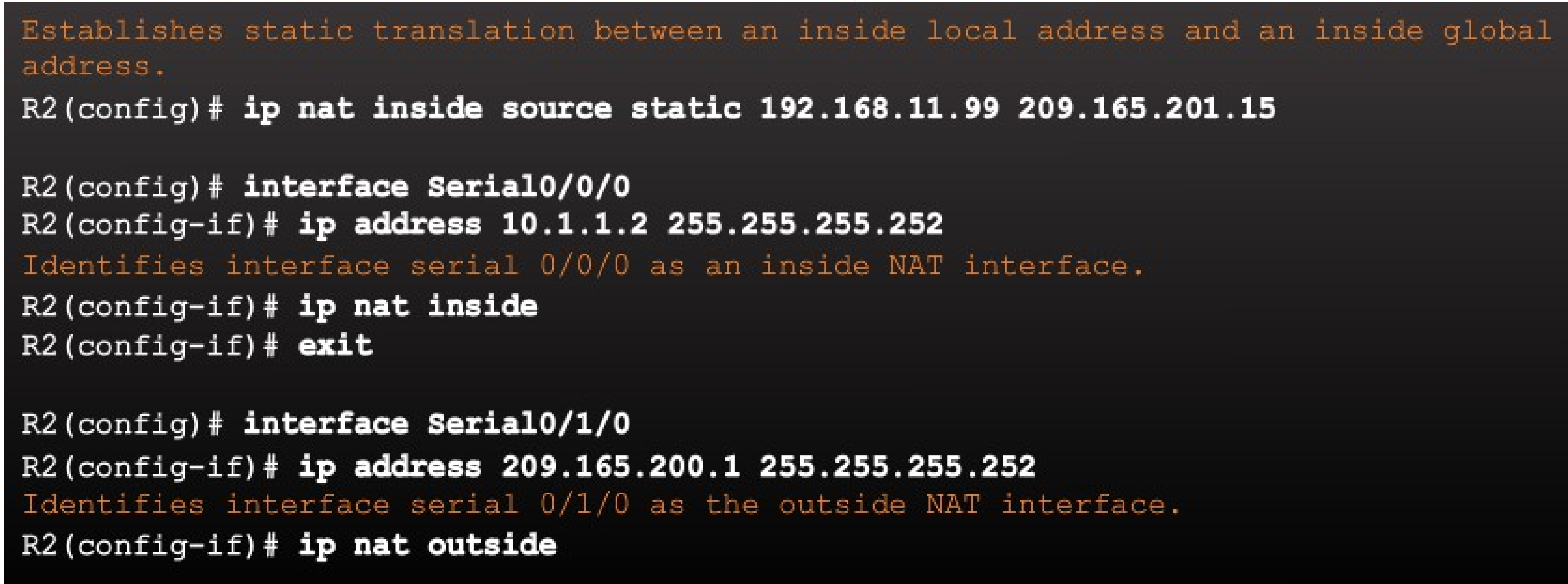
Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. `Router(config)#` **`ip nat inside source static`** *`local-ip global-ip`*	Enter the **`no ip nat inside source static`** global configuration mode command to remove the dynamic source translation.
2	Specify the inside interface. `Router(config)#` **`interface`** *`type number`*	Enter the **`interface`** command. The CLI prompt changes from `(config)#` to `(config-if)#`.
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`**	

Typická chyba!

Remember that any interface on the border router that is on the inside network must be configured with the **ip nat inside** command. This is a common mistake for those new to NAT.

Static NAT





```
Establishes static translation between an inside local address and an inside global
address.
R2(config)# ip nat inside source static 192.168.11.99 209.165.201.15

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 209.165.200.1 255.255.255.252
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Configuring Static NAT

Analyzing Static NAT

1. Client opens a web browser for a connection to a web server.

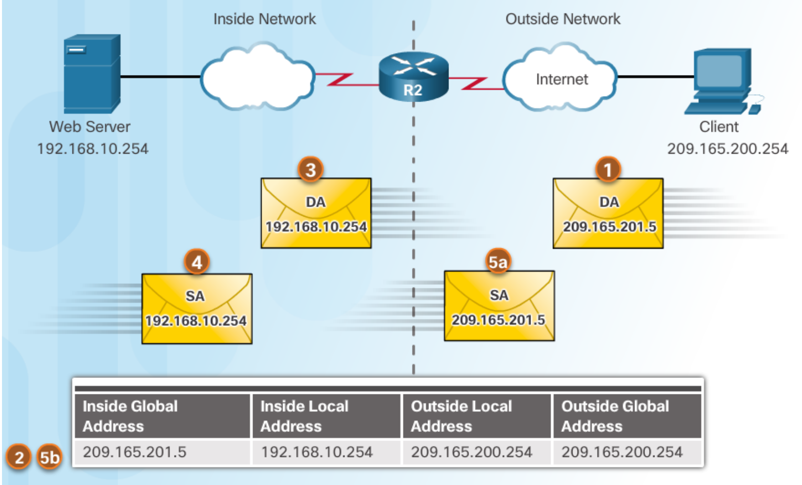
2. R2 receives the packet on the outside interface and checks the NAT table.

3. R2 replaces the inside global address with inside local address of 192.168.10.254 (the server's address).

4. Web server responds to the client.

5. (a) R2 receives the packet from the server on the inside address.
   (b) R2 checks NAT table and translates the source address to the inside global address of 209165.201.5 and forwards the packet.

6. The client receives the packet.



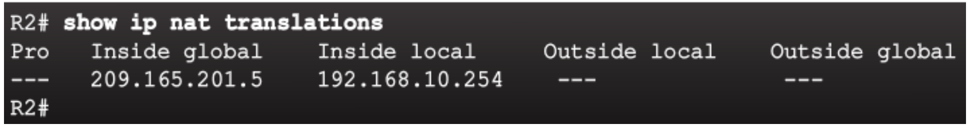
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.201.5	192.168.10.254	209.165.200.254	209.165.200.254

Configuring Static NAT

Verifying Static NAT

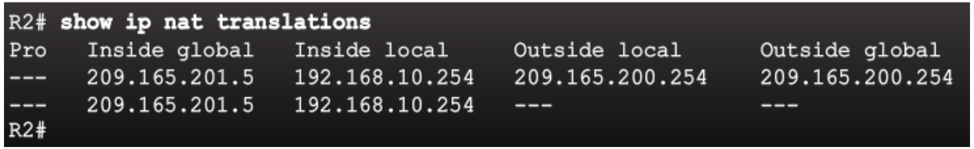
A best practice is to clear statistics when verifying that NAT is working.

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#
```

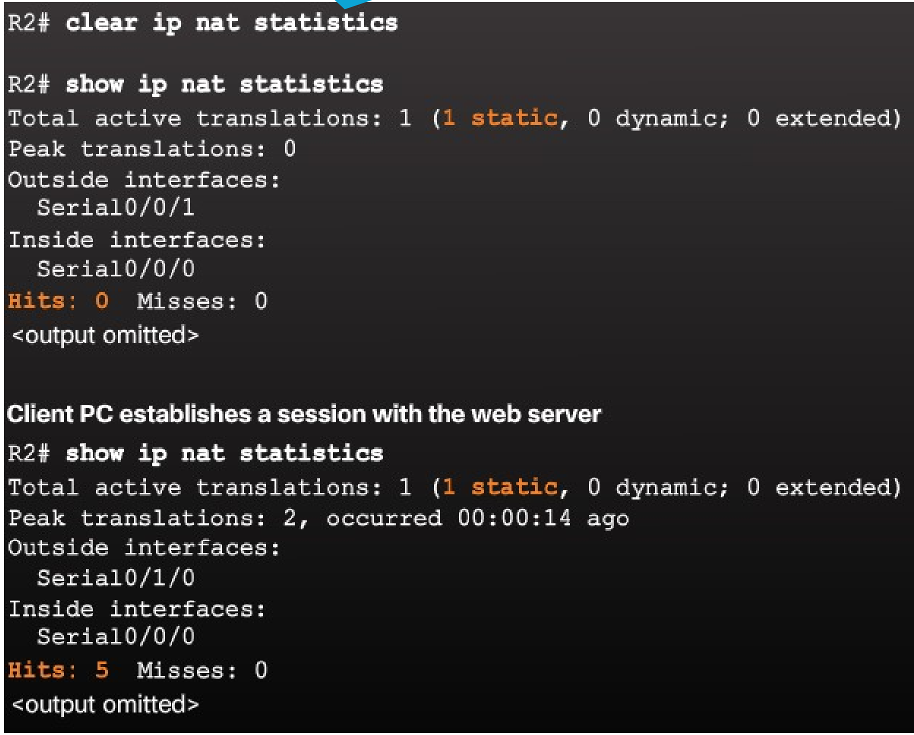
The static translation during an active session.



```
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
---   209.165.201.5   192.168.10.254  ---               ---
R2#
```

Important commands:

- **show ip nat translations**
- **show ip nat statistics**

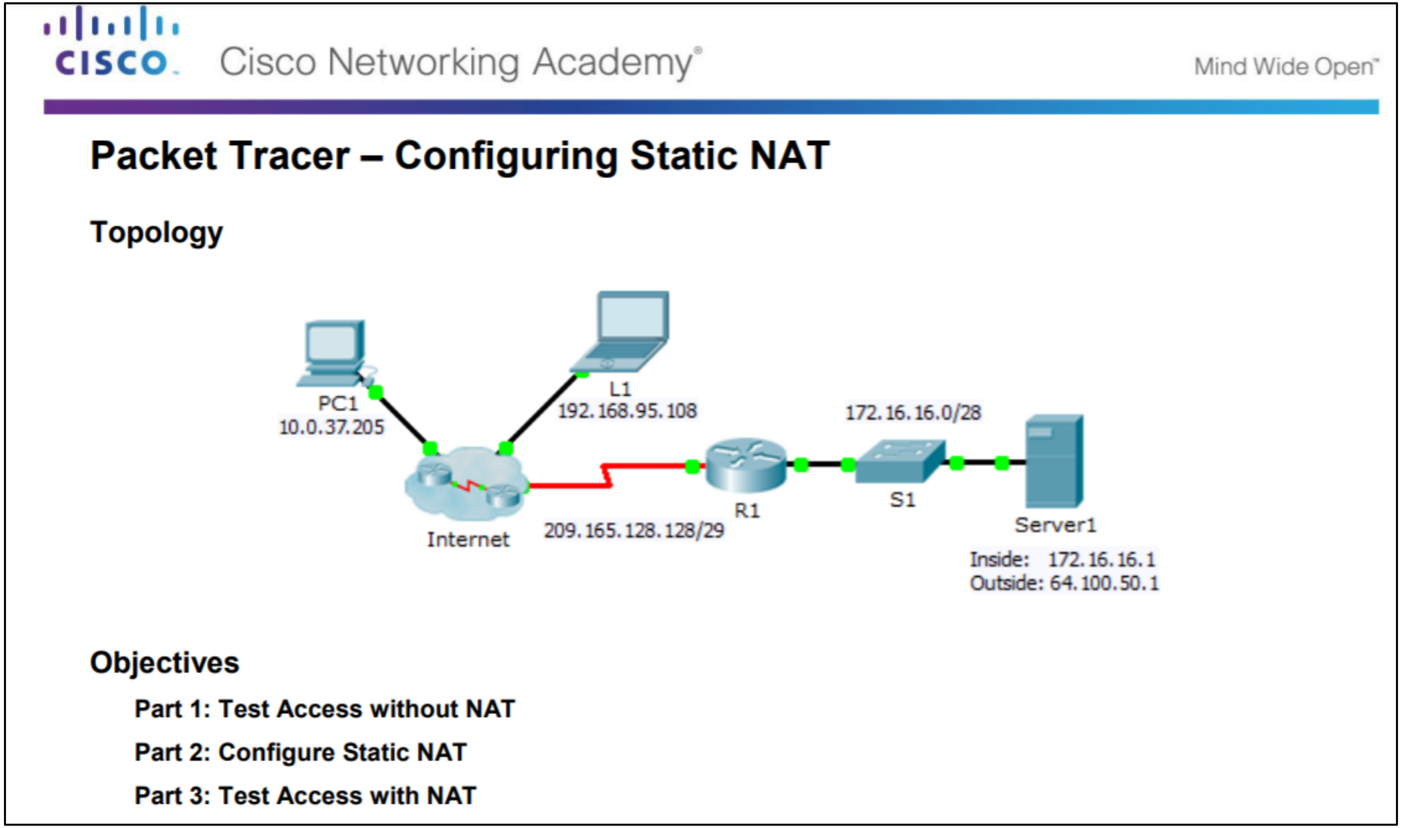


```
R2# clear ip nat statistics

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>
```

Packet Tracer – Configuring Static NAT



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Configuring Static NAT

Topology

PC1
10.0.37.205
L1
192.168.95.108
Internet
209.165.128.128/29
R1
172.16.16.0/28
S1
Server1
Inside: 172.16.16.1
Outside: 64.100.50.1

Objectives

Part 1: Test Access without NAT

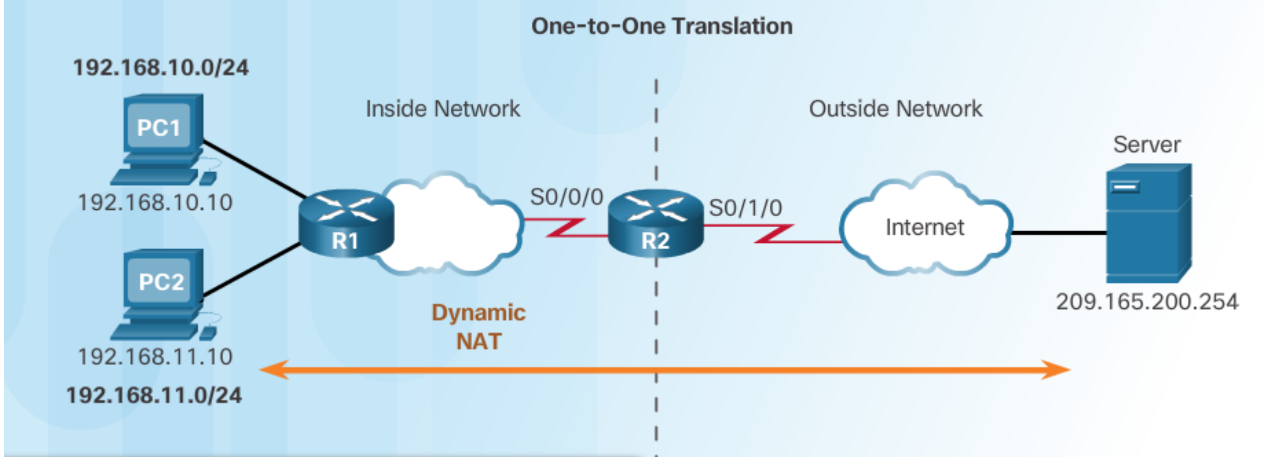
Part 2: Configure Static NAT

Part 3: Test Access with NAT

Configure Dynamic NAT

Dynamic NAT Operation

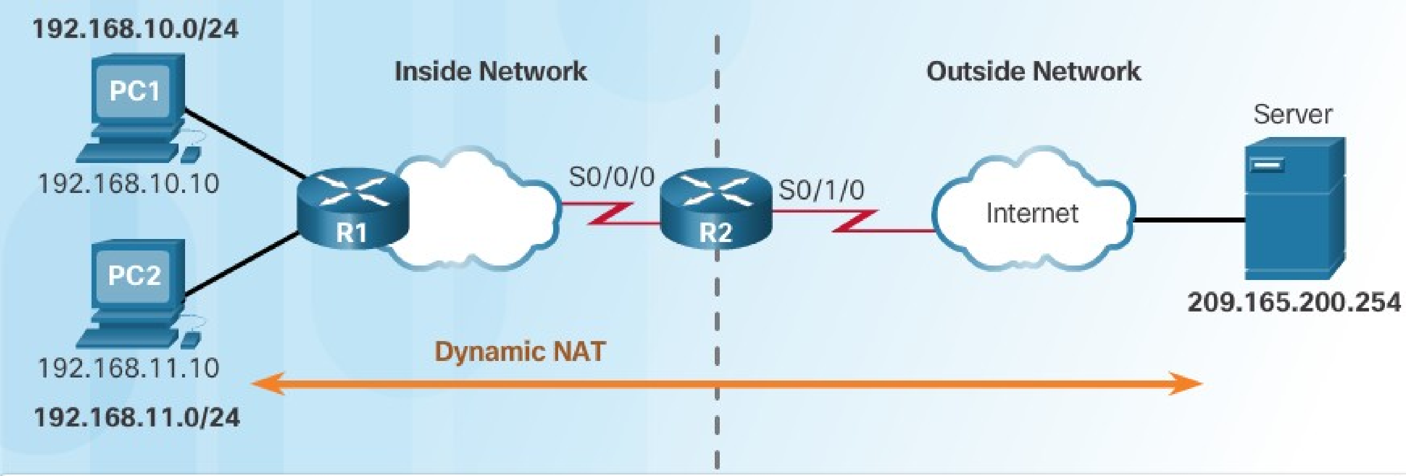
- Remember that dynamic NAT uses a pool of public IPv4 addresses.
- Use the same concepts of inside and outside NAT interfaces as static NAT.

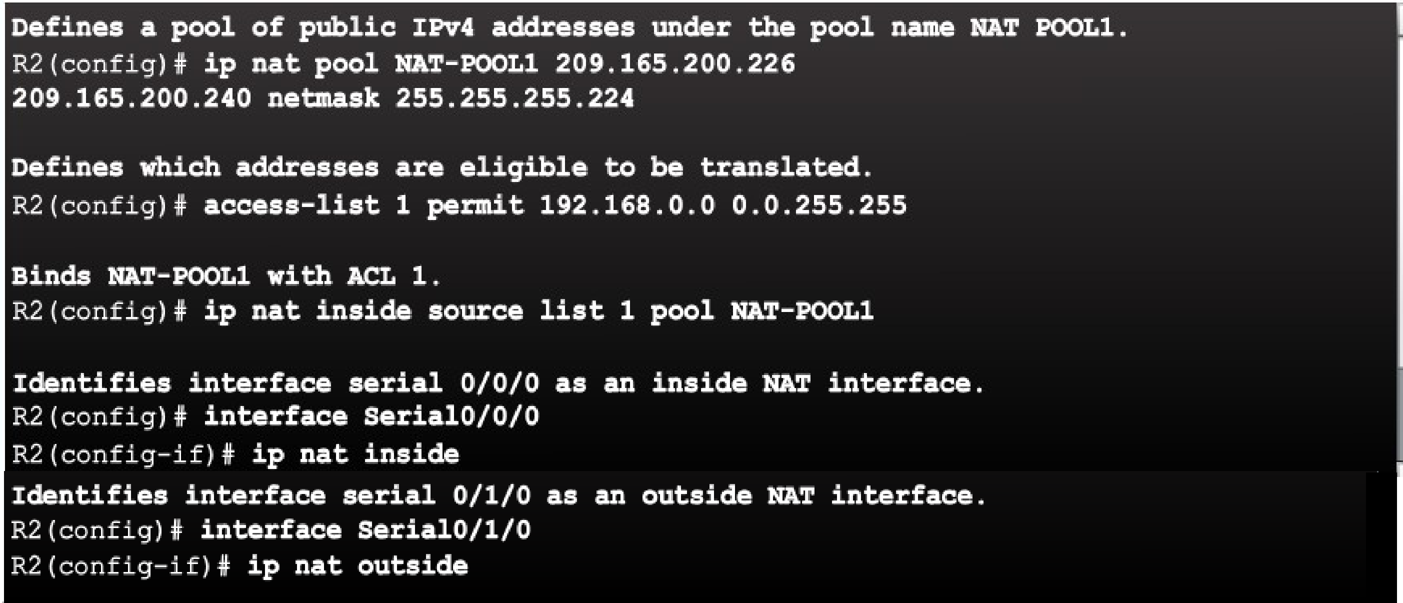


IPv4 NAT Pool

Inside Local Address Pool	Inside Global Address
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227
...	209.165.200.228
...	...
...	209.165.200.240

Dynamic NAT

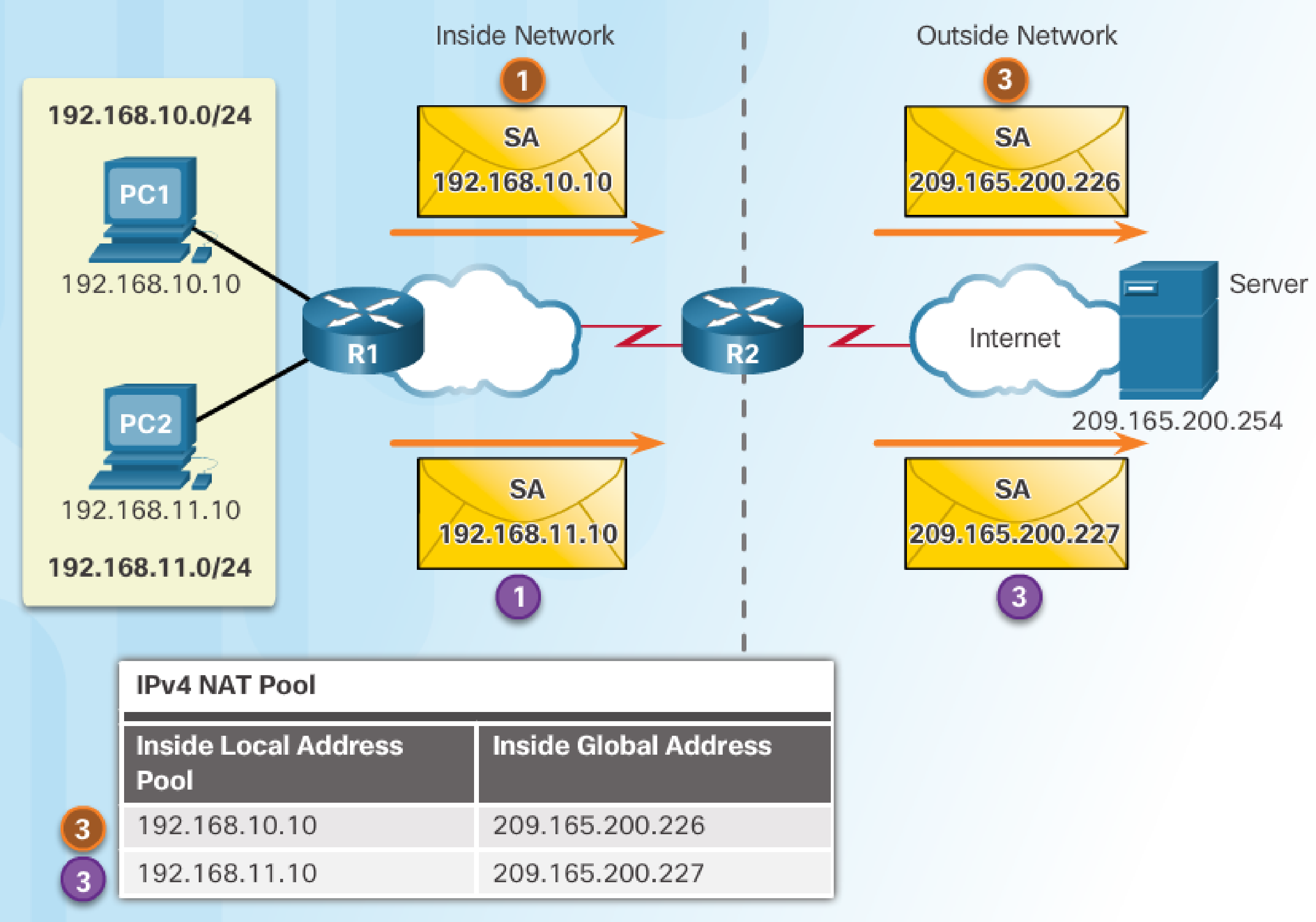




```
Defines a pool of public IPv4 addresses under the pool name NAT POOL1.
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224

Defines which addresses are eligible to be translated.
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255

Binds NAT-POOL1 with ACL 1.
R2(config)# ip nat inside source list 1 pool NAT-POOL1

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

Analyzing Dynamic NAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns a global address from the NAT pool and **creates a NAT table entry** for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address from the pool.



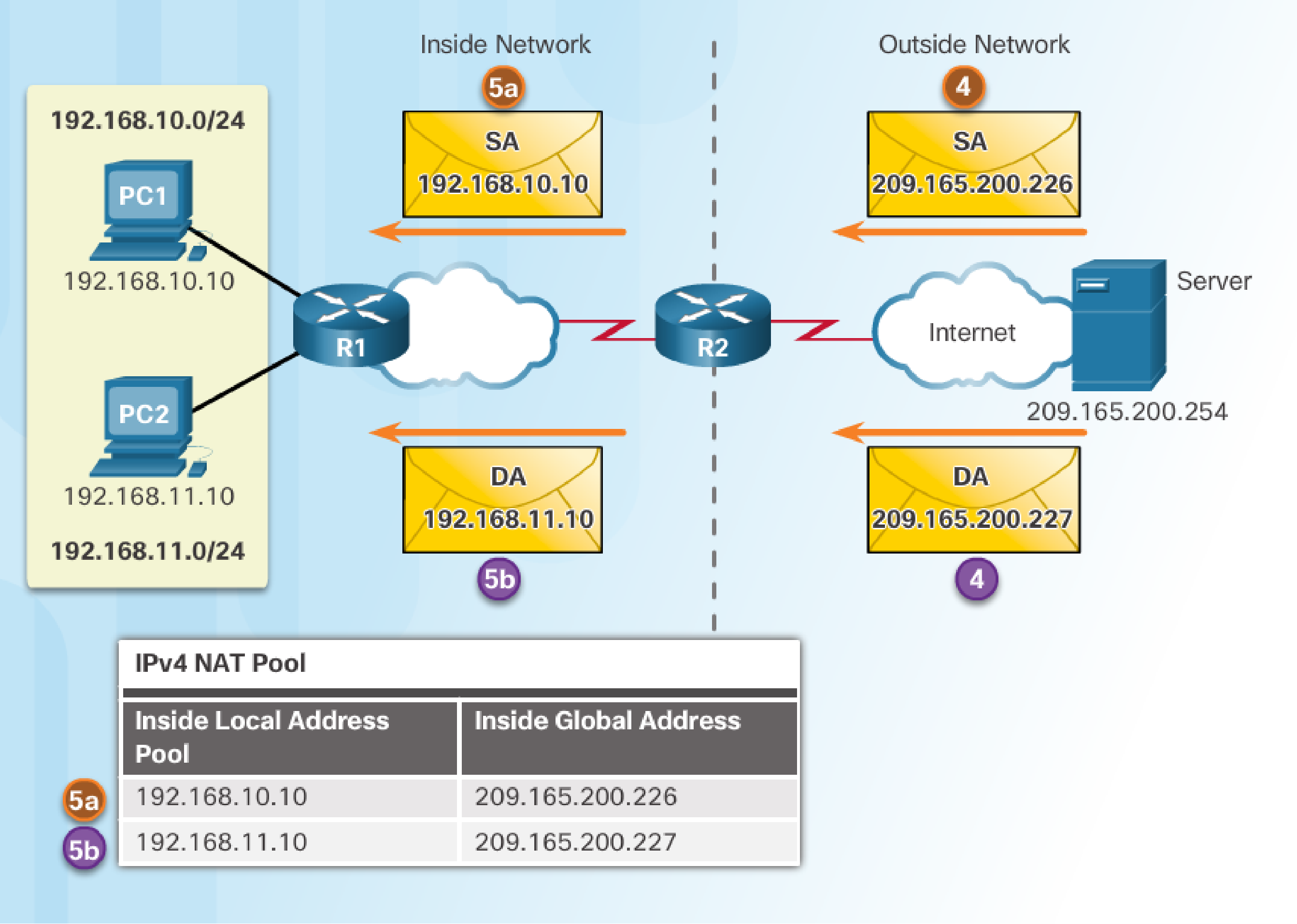
IPv4 NAT Pool

Inside Local Address Pool	Inside Global Address
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

Analyzing Dynamic NAT

4. The server responds to PC1 using the destination address of 209.165.200.226 (the NAT-assigned address) and to PC2 using the destination address of 209.165.200.227.

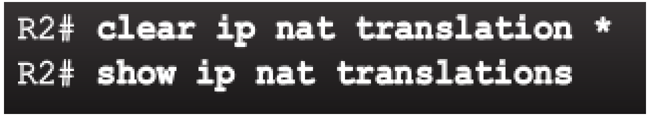
5. (a and b) R2 looks up each received packet and forwards based on the private IP address found in the NAT table for each of the destination addresses.



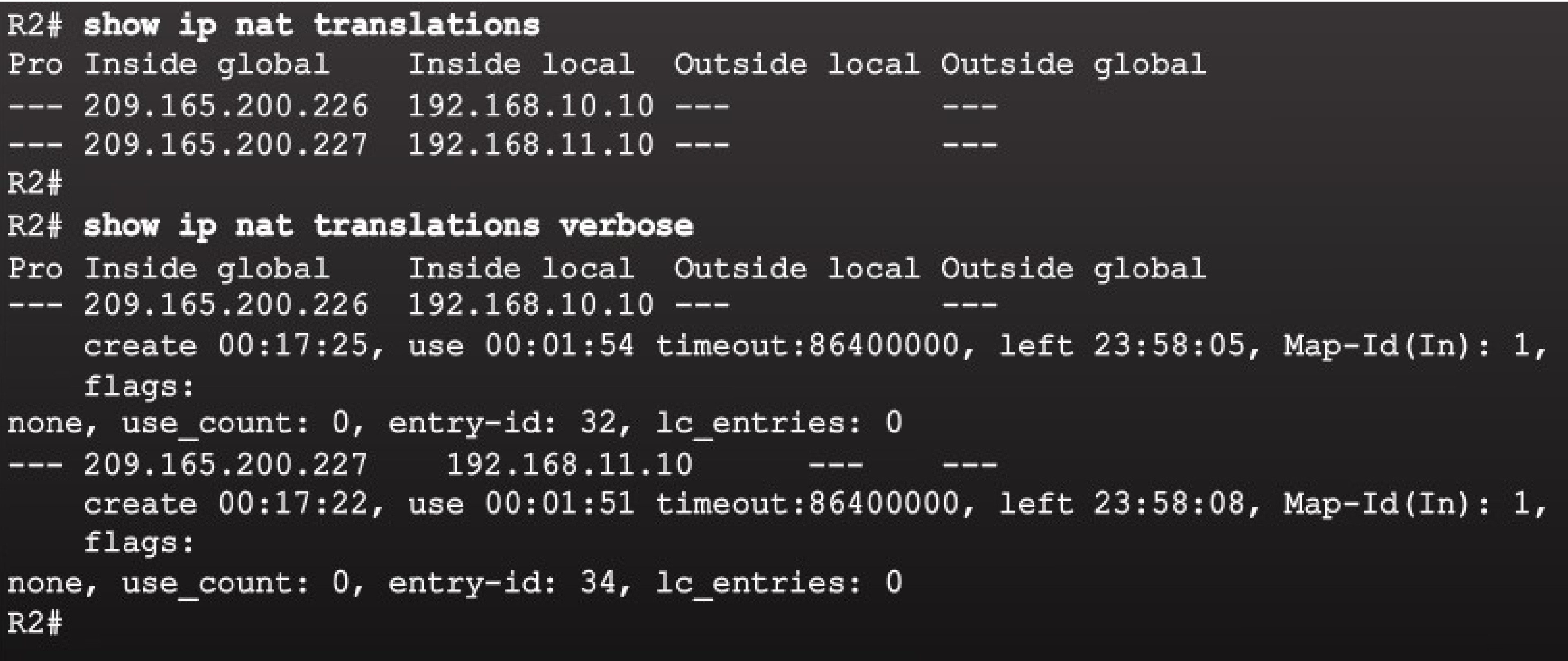
IPv4 NAT Pool

	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Verifying Dynamic NAT

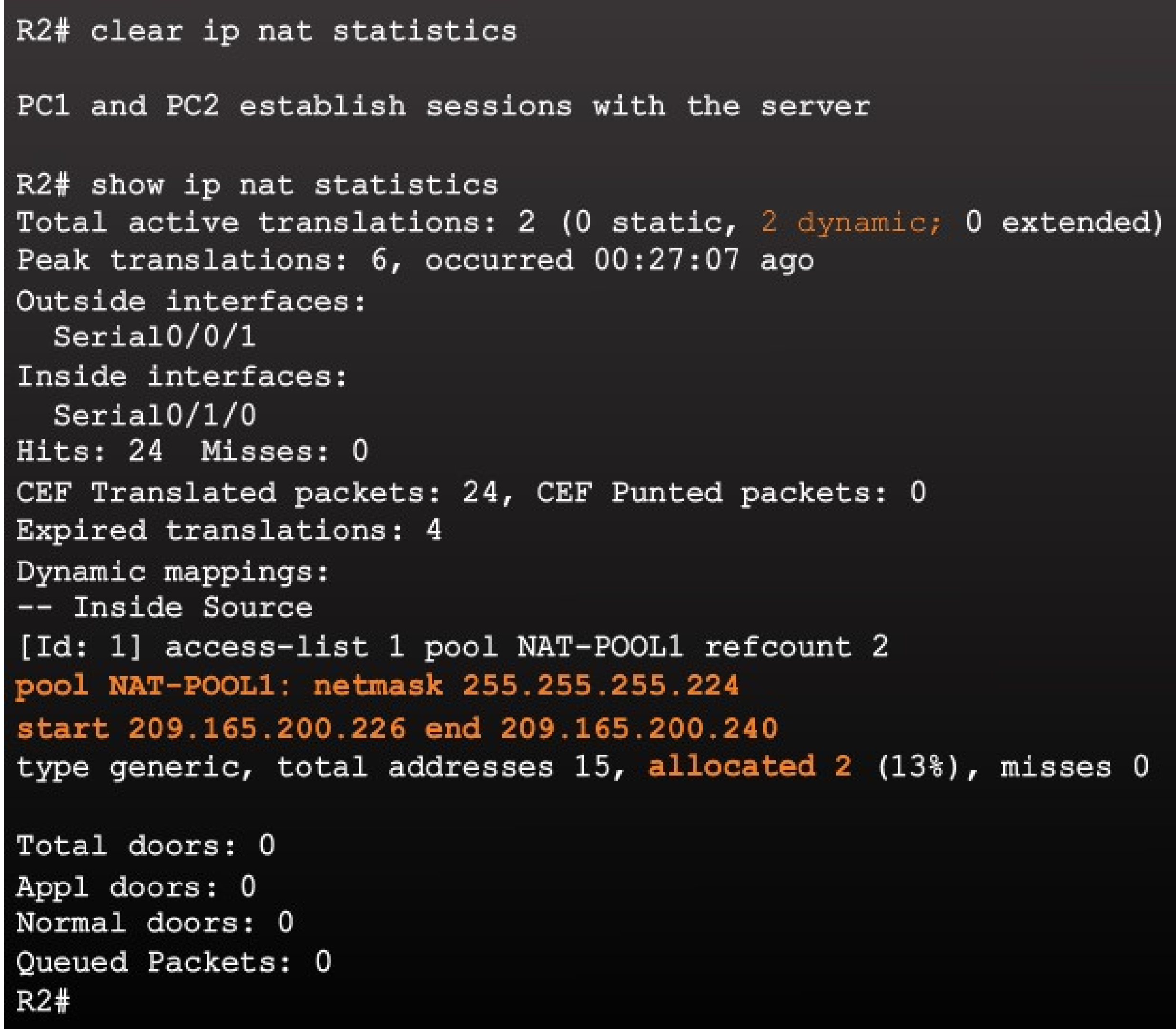


```
R2# clear ip nat translation *
R2# show ip nat translations
```



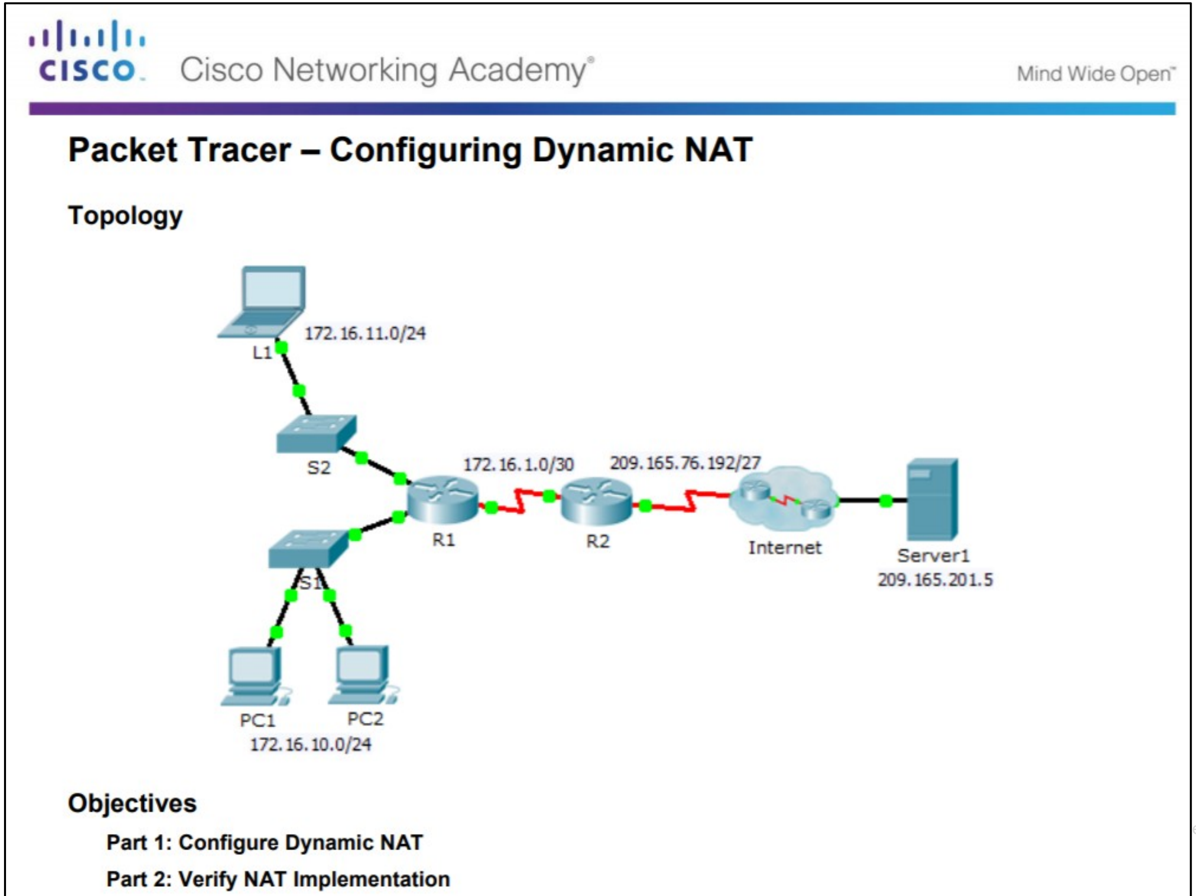
```
R2# show ip nat translations
Pro Inside global     Inside local   Outside local Outside global
--- 209.165.200.226  192.168.10.10 ---              ---
--- 209.165.200.227  192.168.11.10 ---              ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local   Outside local 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#
```

Verifying Dynamic NAT



```
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#
```

Packet Tracer – Configuring Dynamic NAT



Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Configuring Dynamic NAT

Topology

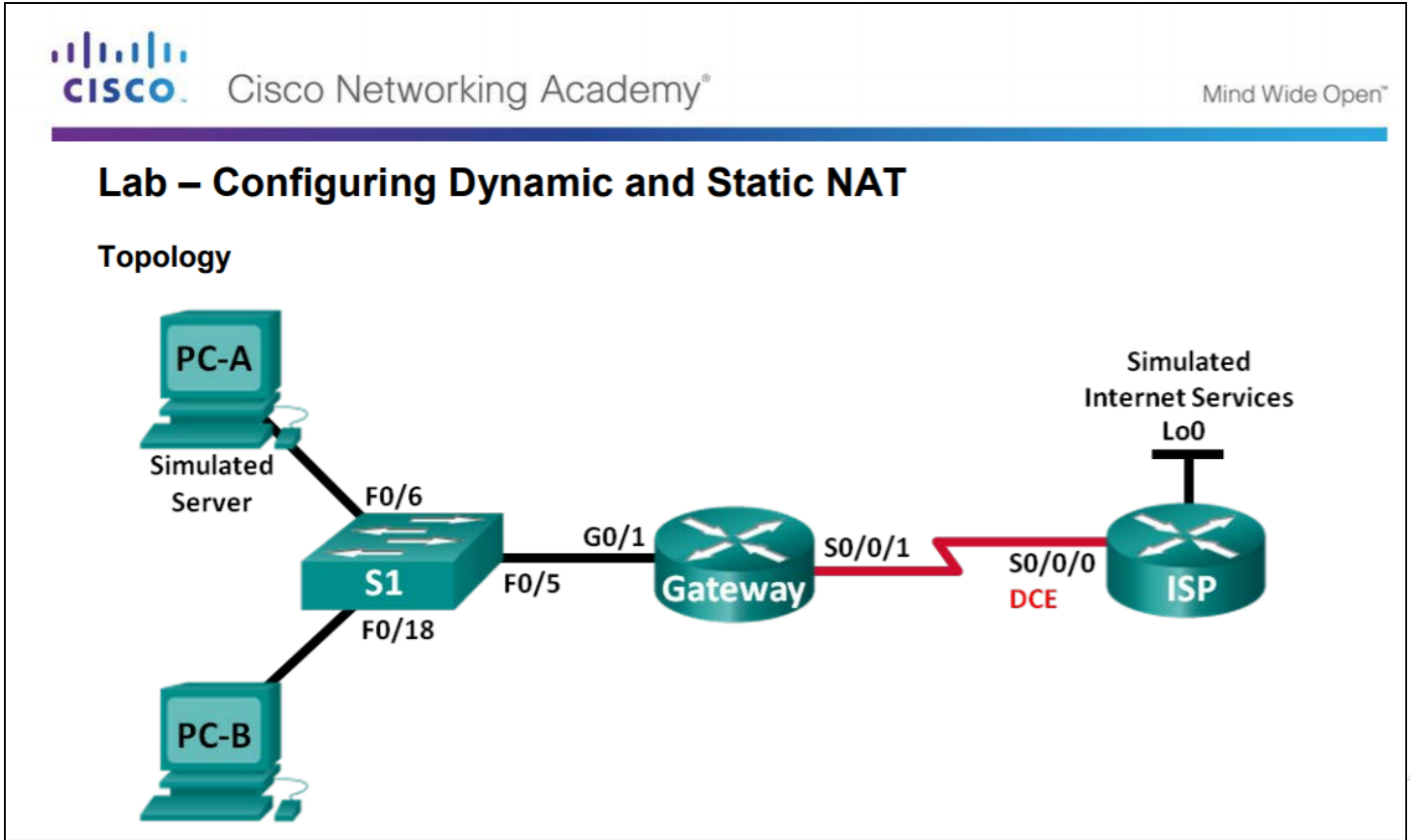
L1
172.16.11.0/24
S2
S1
R1
172.16.1.0/30
R2
209.165.76.192/27
Internet
Server1
209.165.201.5
PC1
PC2
172.16.10.0/24

Objectives

Part 1: Configure Dynamic NAT

Part 2: Verify NAT Implementation

Configuring Dynamic and Static NAT



Cisco Networking Academy®

Mind Wide Open™

Lab – Configuring Dynamic and Static NAT

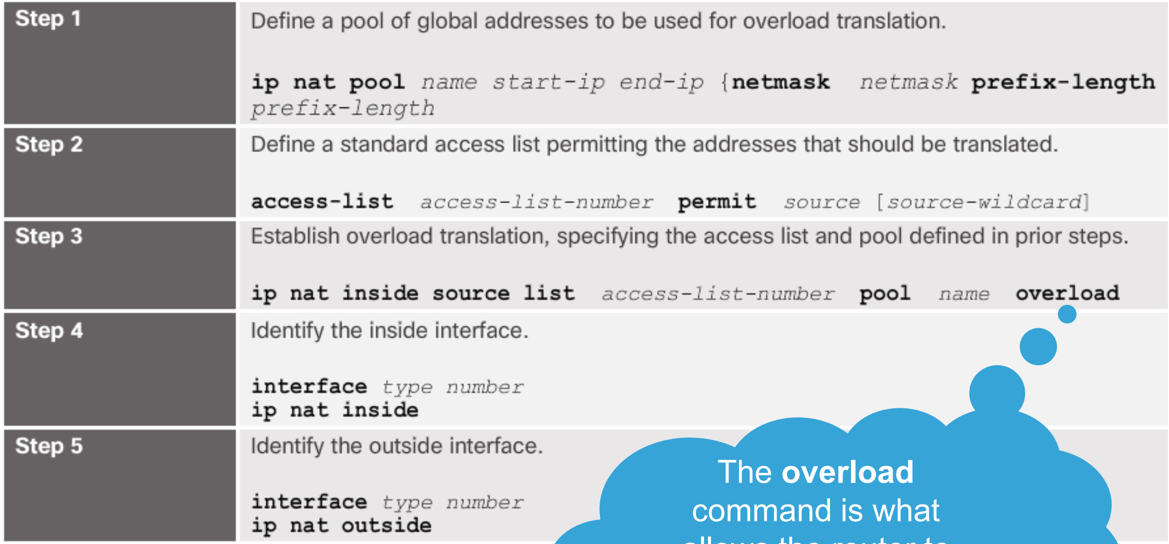
Topology

Configuring PAT: Address Pool

The pool contains the public addresses.

The ACL defines which private IP addresses gets translated.

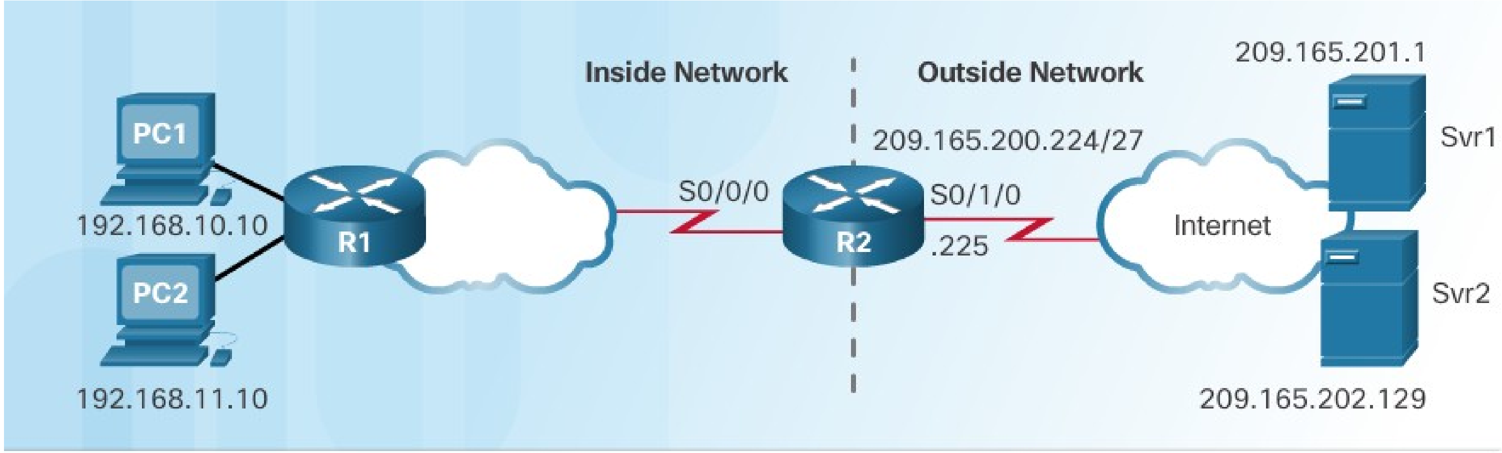
The **ip nat inside source list** *acl#* **pool** *name* **overload** command ties Step 1 with Step 2.

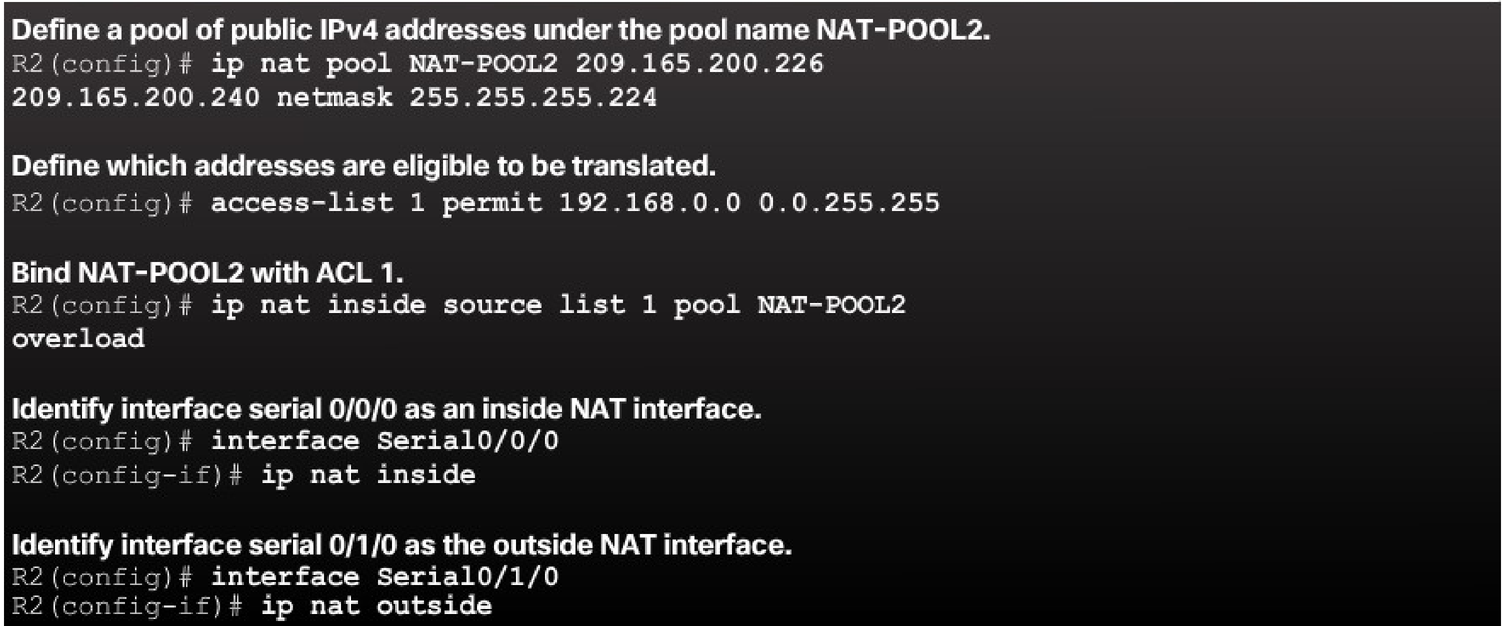


Step 1	Define a pool of global addresses to be used for overload translation. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* **prefix-length** *prefix-length*
Step 2	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *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**

The **overload** command is what allows the router to track port numbers (and do PAT instead of dynamic NAT).

Configuring PAT: 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
```

Configuring PAT: Single Address

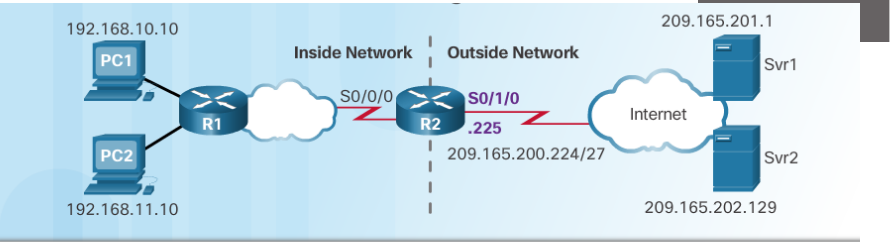
- When a public address is assigned to the external interface on the border router, that public address can be used for PAT and translate internal private IP addresses to the public IP address.

Still need an ACL to define which private IP addresses gets translated.

Instead of associating an ACL with a pool, the ACL is associated with an interface that has a public IP address assigned.

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**

The **overload** command is always needed for PAT.

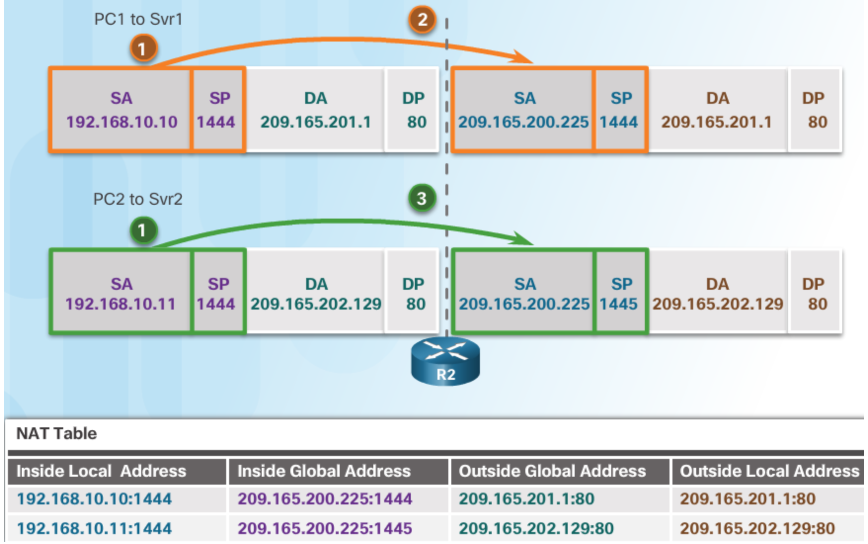


NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

Analyzing PAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns the IP address of the outside interface, **adds a port number**, and **creates a NAT table entry** for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address.



NAT Table

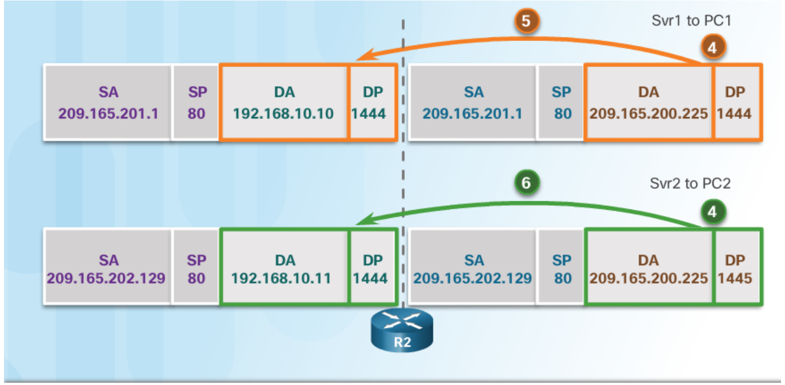
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Analyzing PAT

4. Each server responds to PC1 and PC2 using the destination address of the public address assigned to the external interface on the border router.

5. R2 looks up the received packet and forwards to PC1 because that is the private IP address found in the NAT table for the destination address and port number.

6. R2 looks up the received packet and forwards to PC2 because that is the private IP address found in the NAT table for the destination address and port number.

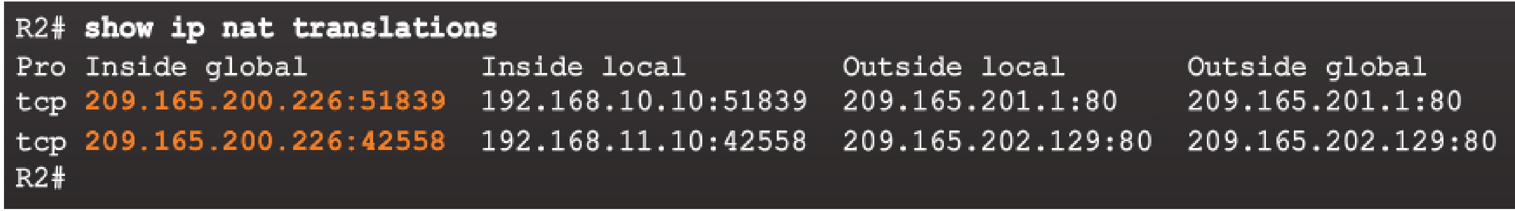


NAT Table

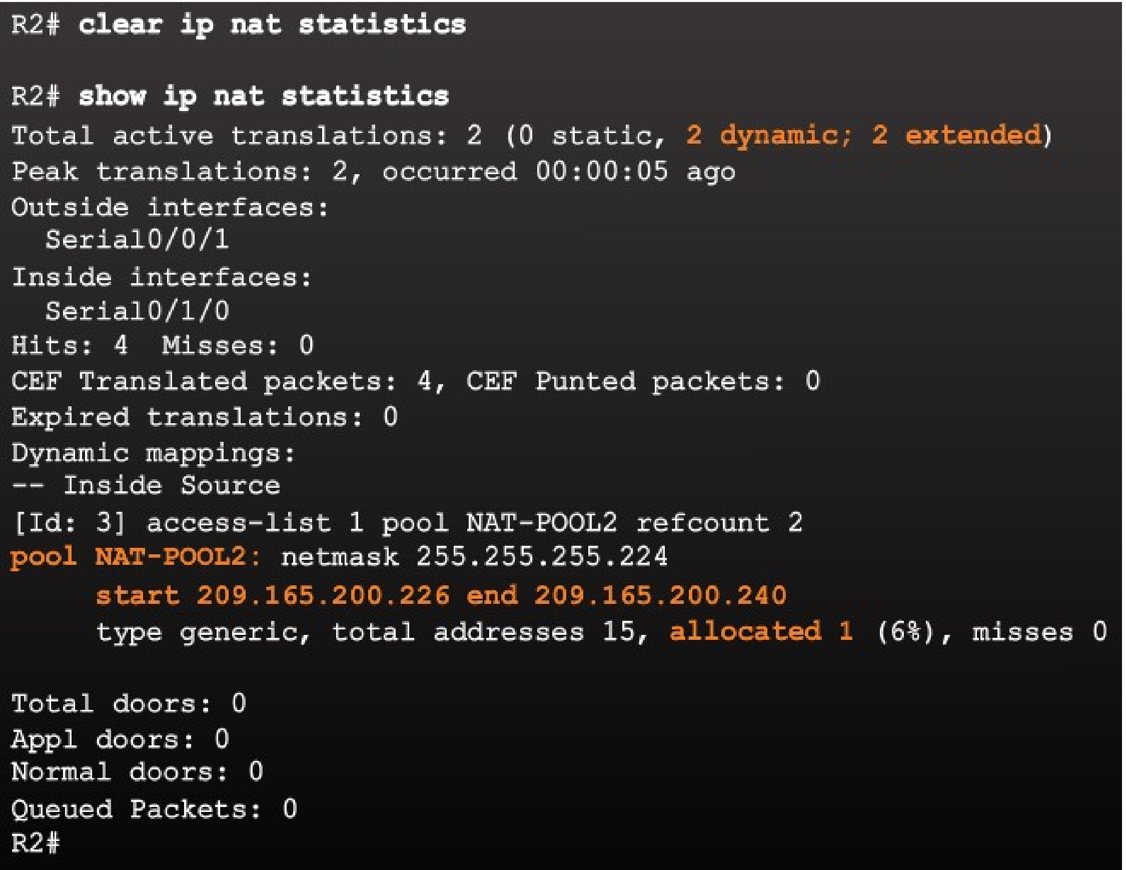
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Configure PAT

Verifying PAT

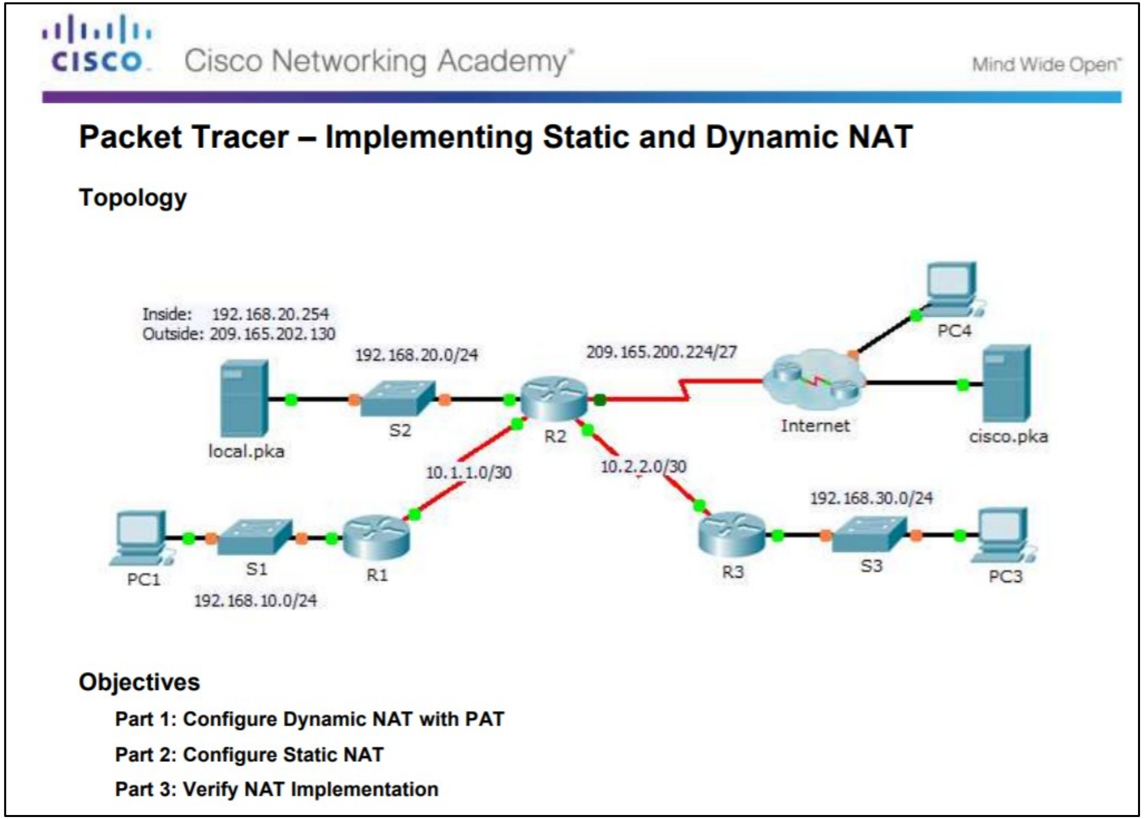


```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local         Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80      209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80    209.165.202.129:80
R2#
```



```
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

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

Packet Tracer – Implementing Static and Dynamic NAT



Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Implementing Static and Dynamic NAT

Topology

Inside: 192.168.20.254
Outside: 209.165.202.130
192.168.20.0/24
209.165.200.224/27
PC4
local.pka
S2
R2
Internet
cisco.pka
10.1.1.0/30
10.2.2.0/30
192.168.30.0/24
PC1
S1
R1
R3
S3
PC3
192.168.10.0/24

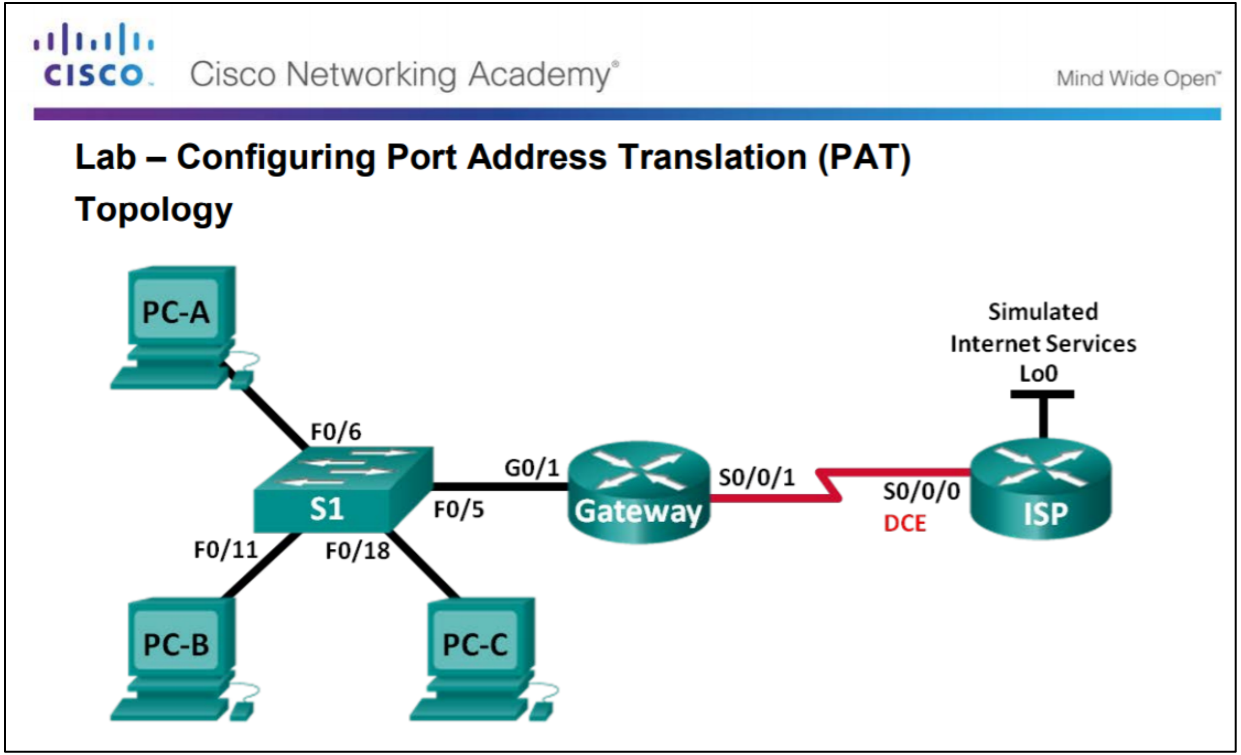
Objectives

Part 1: Configure Dynamic NAT with PAT

Part 2: Configure Static NAT

Part 3: Verify NAT Implementation

Configuring Port Address Translation (PAT)



Cisco Networking Academy®

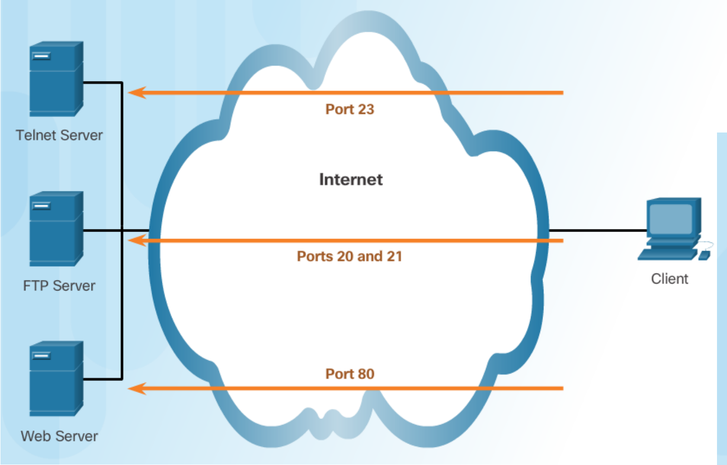
Mind Wide Open™

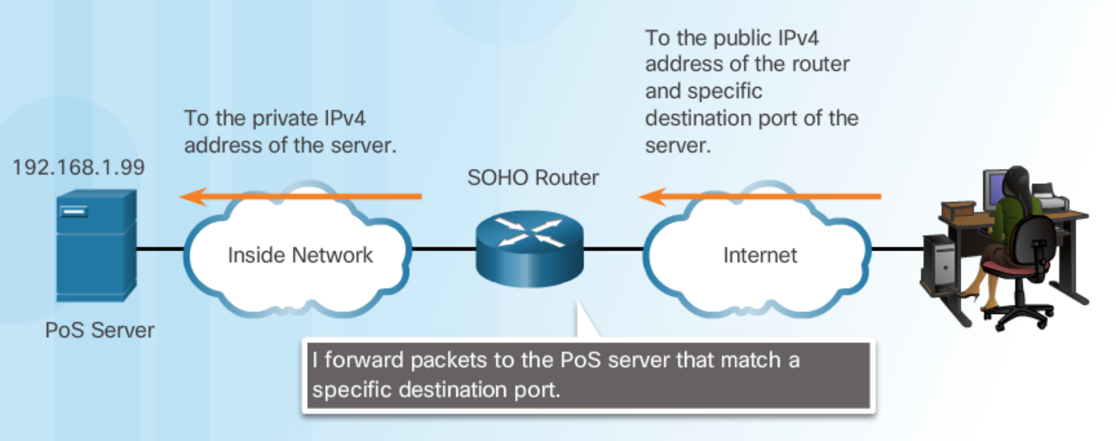
Lab – Configuring Port Address Translation (PAT)

Topology

Port Forwarding

- Port forwarding allows an external device to reach a device on a specific port number and the device is located on an internal (private) network.
  - Required for some peer-to-peer file-sharing programs and operations such as web serving and outgoing FTP
  - Solves the problem of NAT only allowing translations for traffic destined for external networks at the request of internal devices.

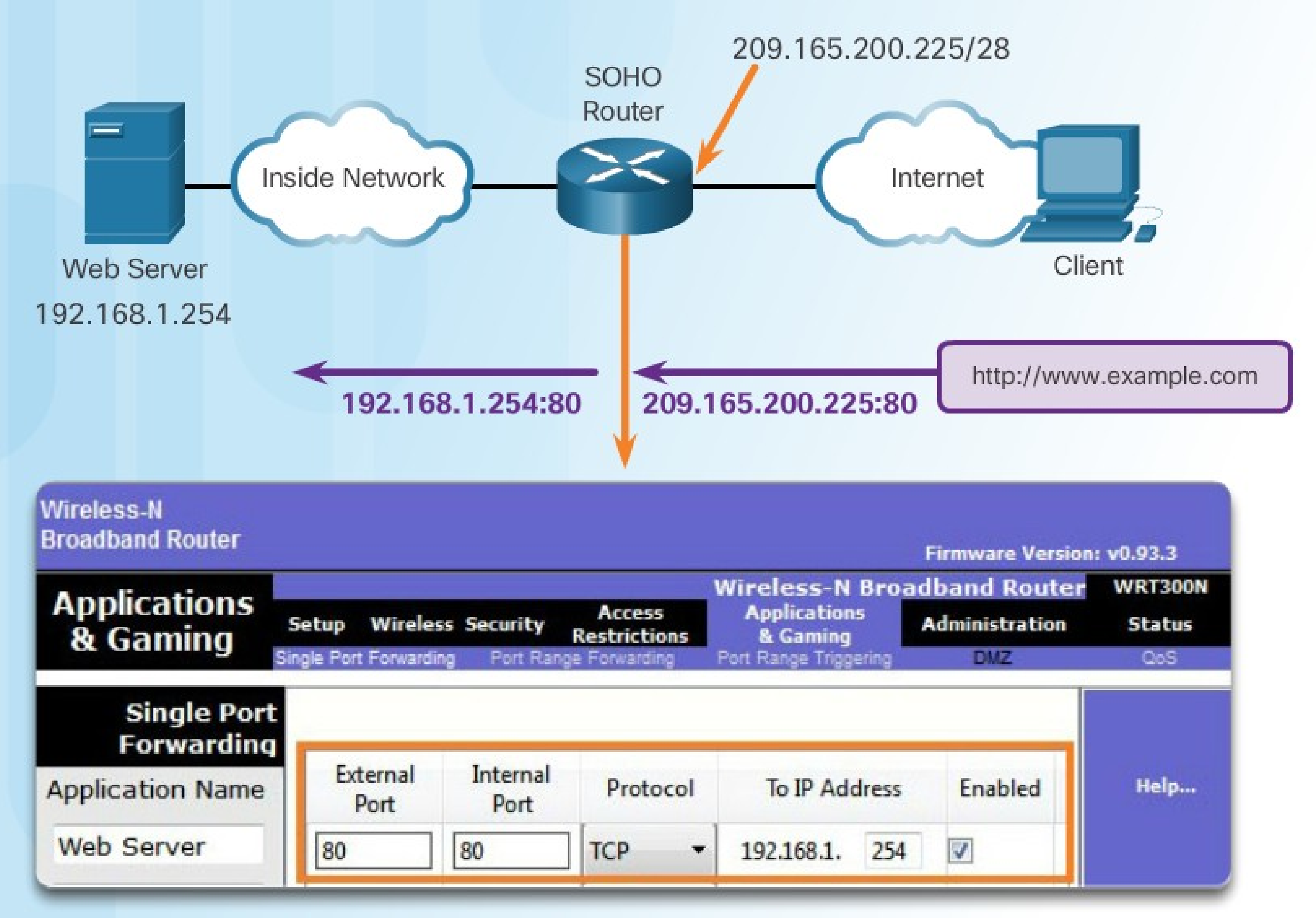



To the public IPv4 address of the router and specific destination port of the server.
To the private IPv4 address of the server.
192.168.1.99
SOHO Router
Inside Network
Internet
PoS Server

I forward packets to the PoS server that match a specific destination port.

Wireless Router Example

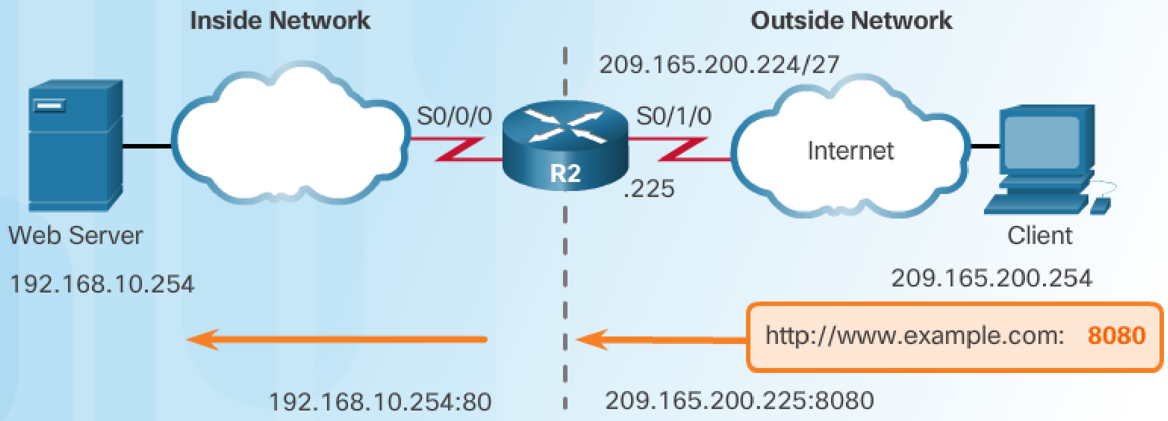
- Port forwarding can be enabled for specific applications
  - Must specify the inside local address that requests should be forwarded to



Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
Web Server	80	80	TCP	192.168.1. 254	☑

Configuring Port Forwarding with IOS

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```



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
```

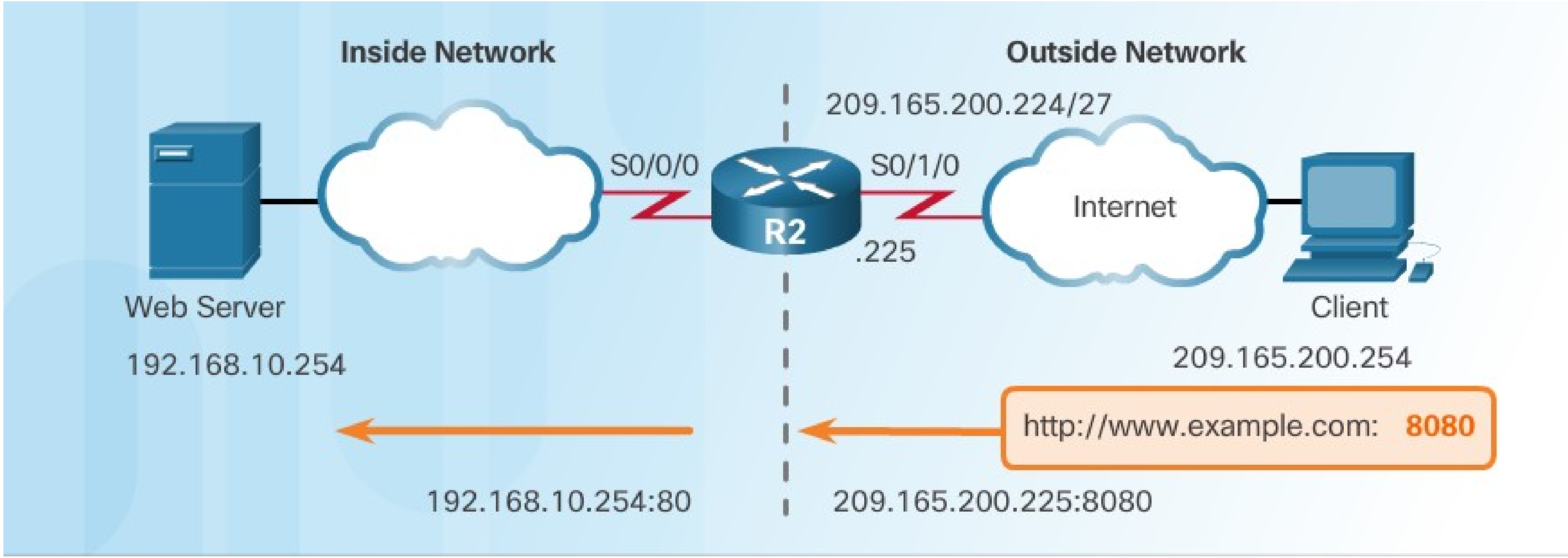
Identifies interface serial 0/0/0 as an inside NAT interface.

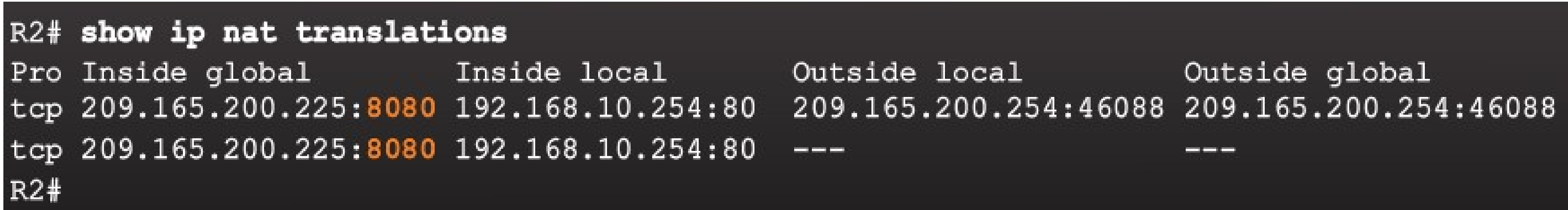
```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

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

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

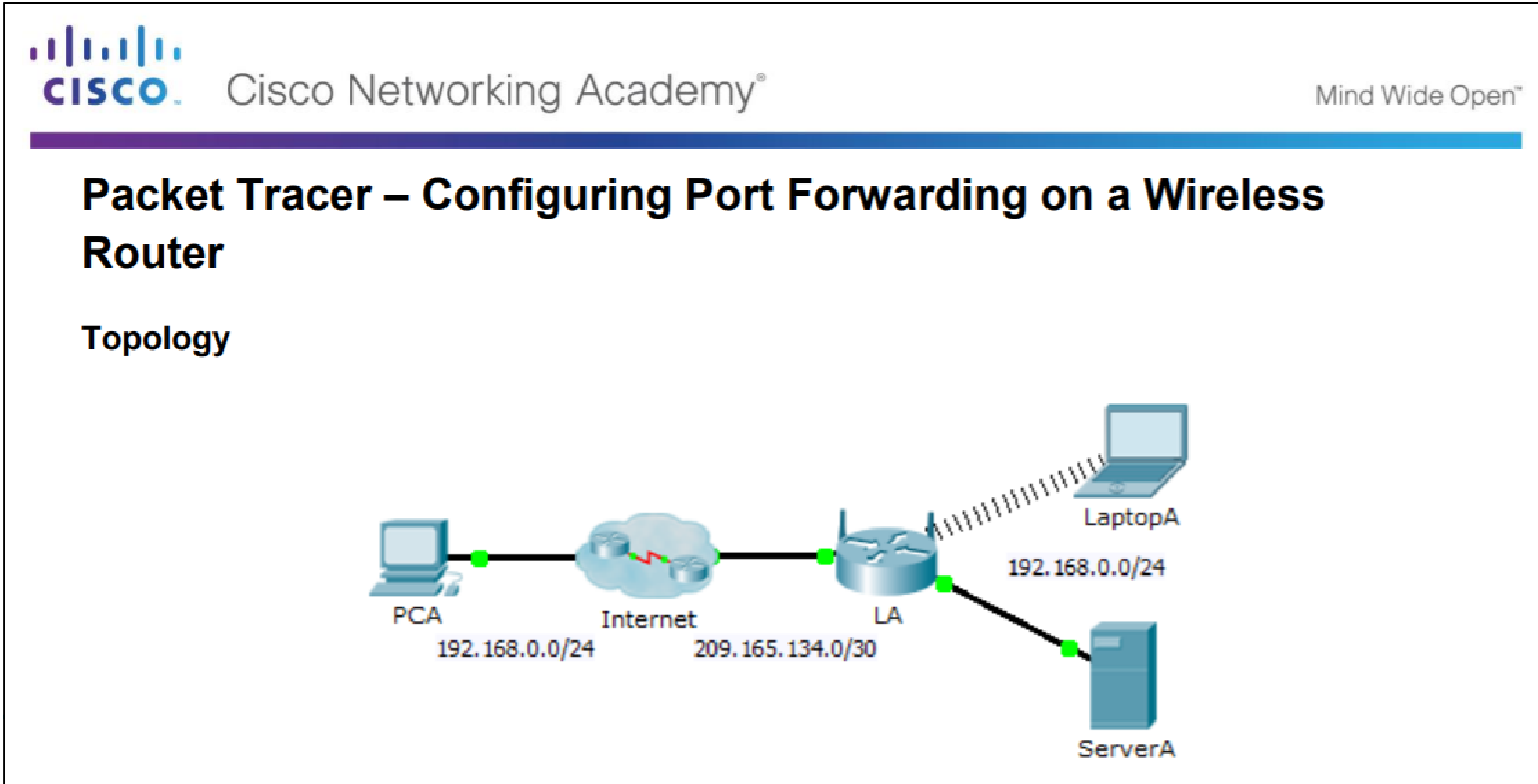
Kontrola





```
R2# show ip nat translations
Pro Inside global        Inside local       Outside local         Outside global
tcp 209.165.200.225:8080 192.168.10.254:80  209.165.200.254:46088 209.165.200.254:46088
tcp 209.165.200.225:8080 192.168.10.254:80  ---                   ---
R2#
```

Packet Tracer – Configuring Port Forwarding on a Wireless Router



Cisco Networking Academy®

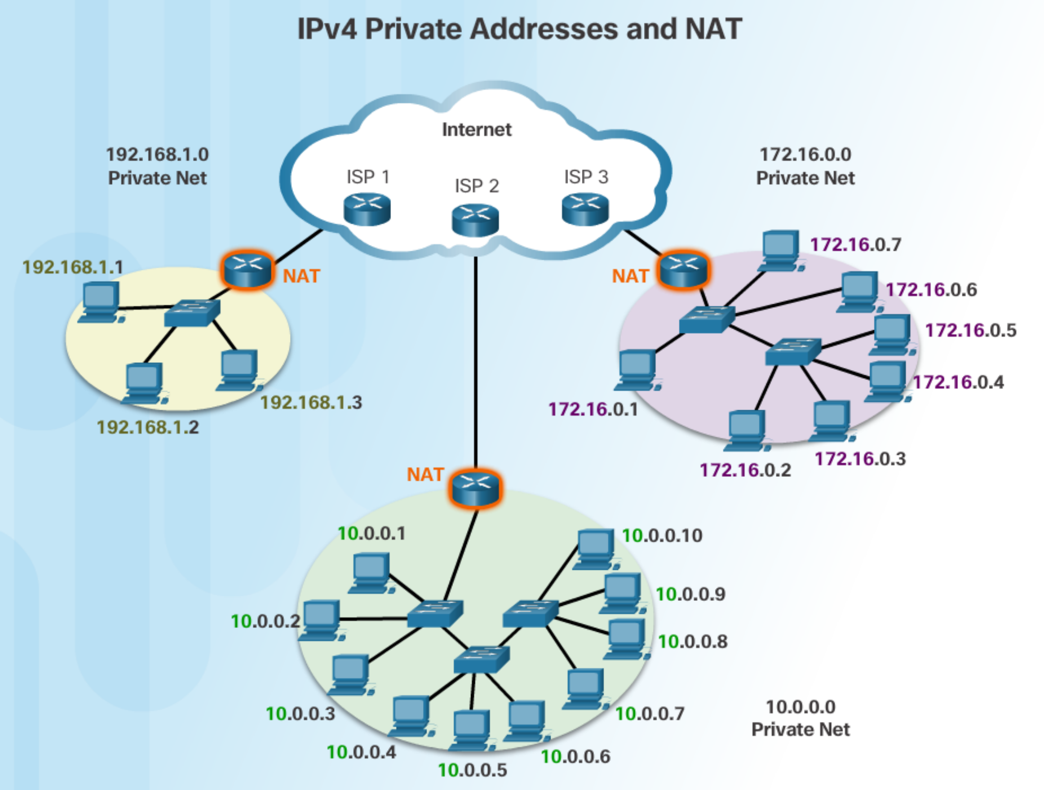
Mind Wide Open™

Packet Tracer – Configuring Port Forwarding on a Wireless Router

Topology

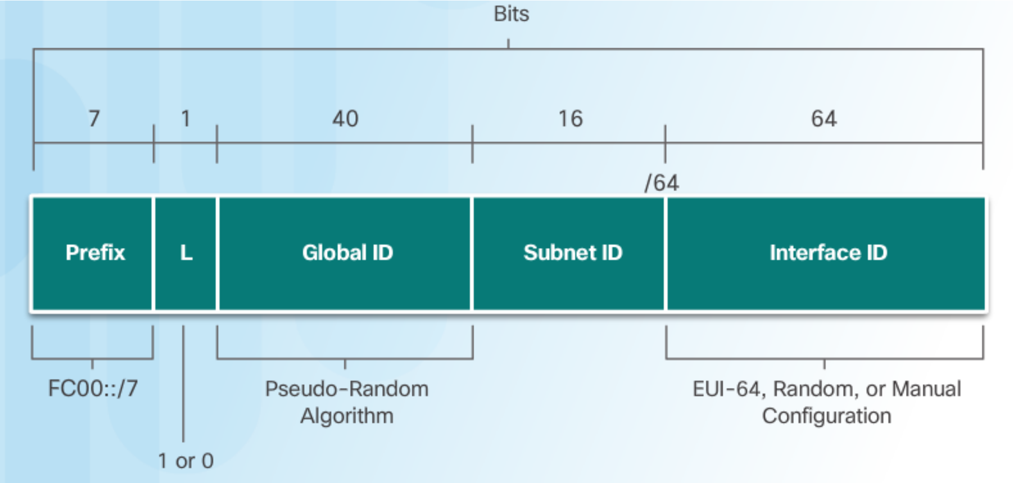
NAT for IPv6?

- IPv6 was developed with the intention of making NAT for IPv4 unnecessary
- IPv6 does have its own form of NAT
  - IPv6 has its own private address space



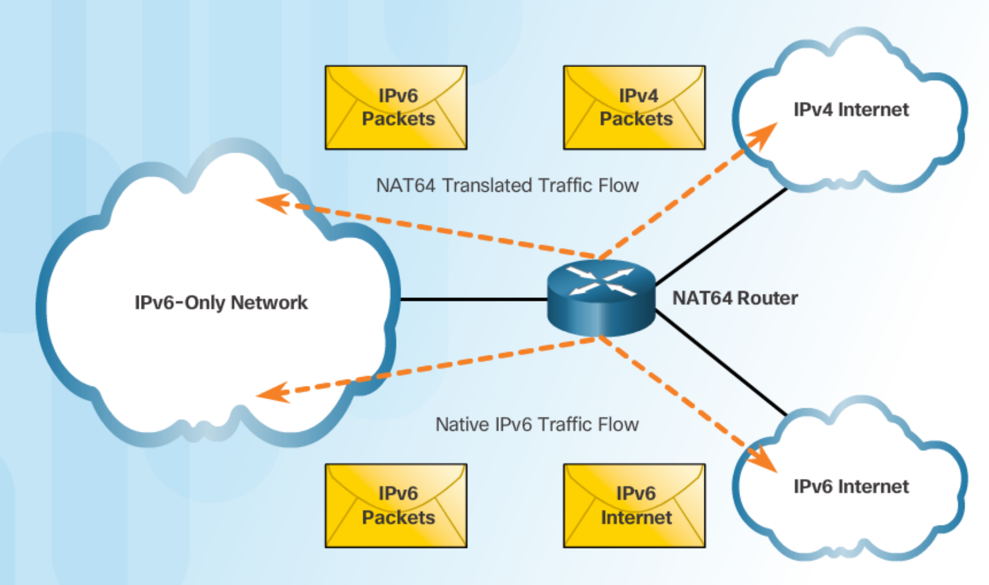
IPv6 Unique Local Addresses

- IPv6 unique local addresses (ULAs) are similar to IPv4 private addresses
  - ULAs are to provide IPv6 address space for communications within a local site.
  - First 64 bits of a ULA
    - Prefix of FC00::/7 (FC00 to FDFF)
    - Next bit is a 1 if the prefix is locally assigned
    - Next 40 bits define a global ID
    - Next 16 bits is a subnet ID
  - Last 64 bits of a ULA is the interface ID or host portion of the address
- Allows sites to be combined without address conflicts
- Allows internal connectivity
- Not routable on the Internet



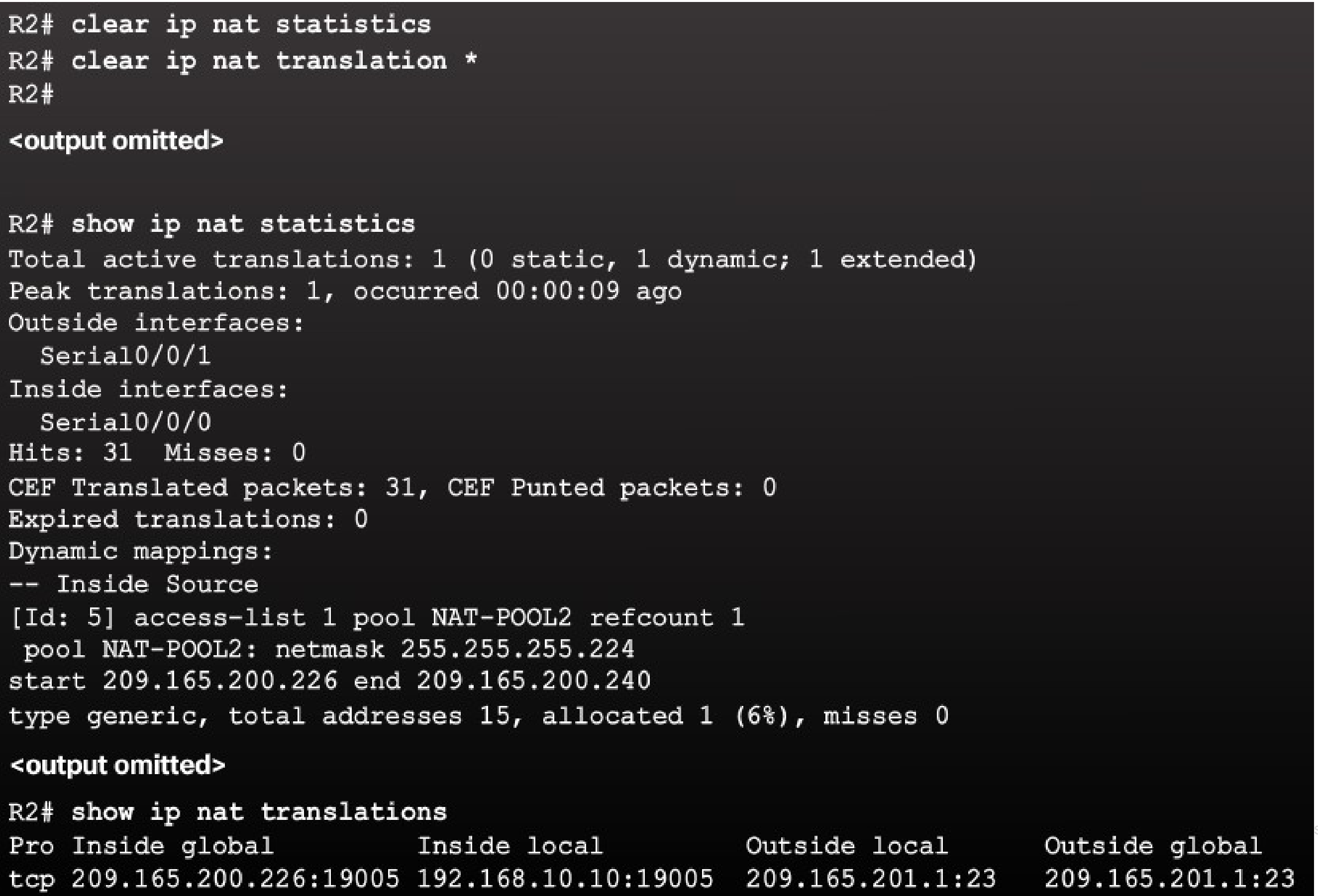
NAT for IPv6

- Provide access **between IPv6-only and IPv4-only** networks (not translating private address to public addresses as NAT for IPv4 was)
- Techniques available
  - **Dual-stack** – both devices run protocols for both IPv4 and IPv6
  - **Tunneling** – Encapsulate the IPv6 packet inside an IPv4 packet for transmission over an IPv4-only network
  - **NAT for IPv6** (translation)
    - Should not be used as a long term strategy
    - The older Network Address Translation-Protocol Translation (NAT-PT)
    - **NAT64**

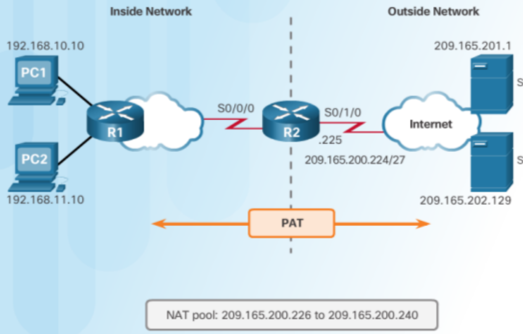


9.3 Troubleshoot NAT

The show ip nat Commands



```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
<output omitted>

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
```



1. Determine what NAT is supposed to achieve and compare with configuration. This may reveal a problem with the configuration.

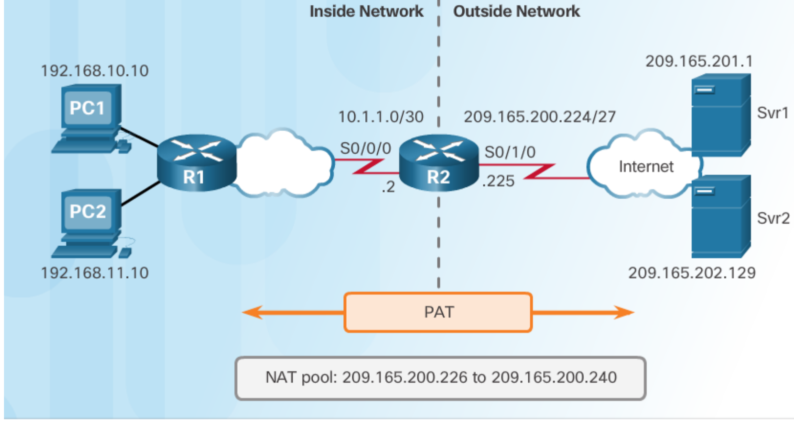
2. Verify translations using the **show ip nat translations** command.

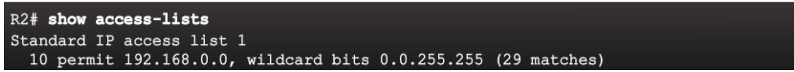
3. Use the **clear** and **debug** commands to verify NAT.

4. Review what is happening to the packet and verify routing.

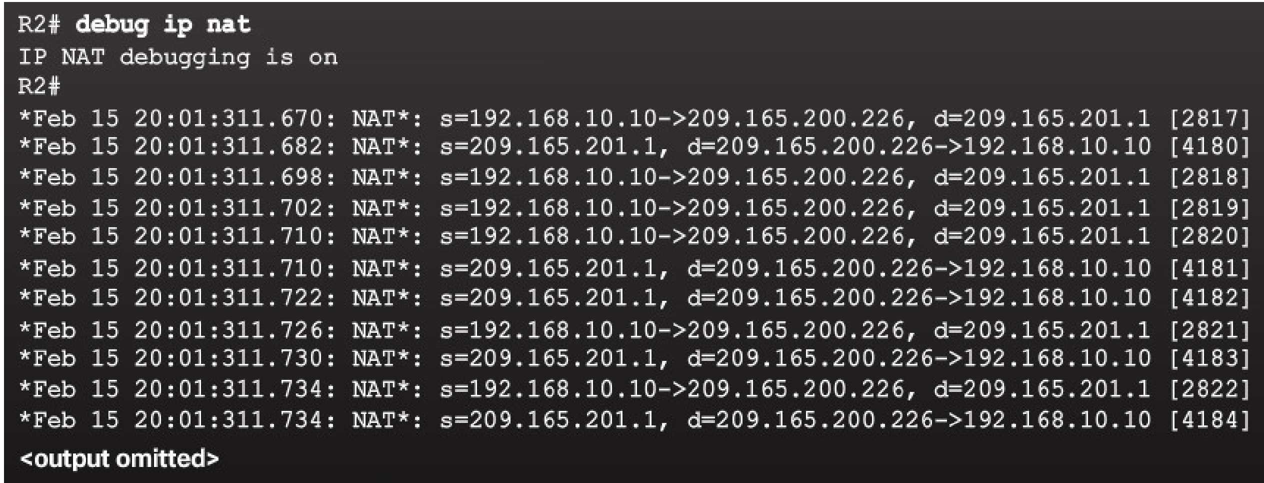
The debug ip nat Commands

- Common commands
  - **debug ip nat**
  - **debug ip nat detailed**
- Output symbols and values
  - * - The translation is occurring in the fast-switched path
  - **s=** - Source IPv4 address
  - **a.b.c.d--->w.x.y.z** – Source a.b.c.d is translated to w.x.y.z.
  - **d=** - Destination IPv4 address
  - **[xxxx]** - IPv4 identification number
- Check the ACL to ensure the correct private addresses are designated.



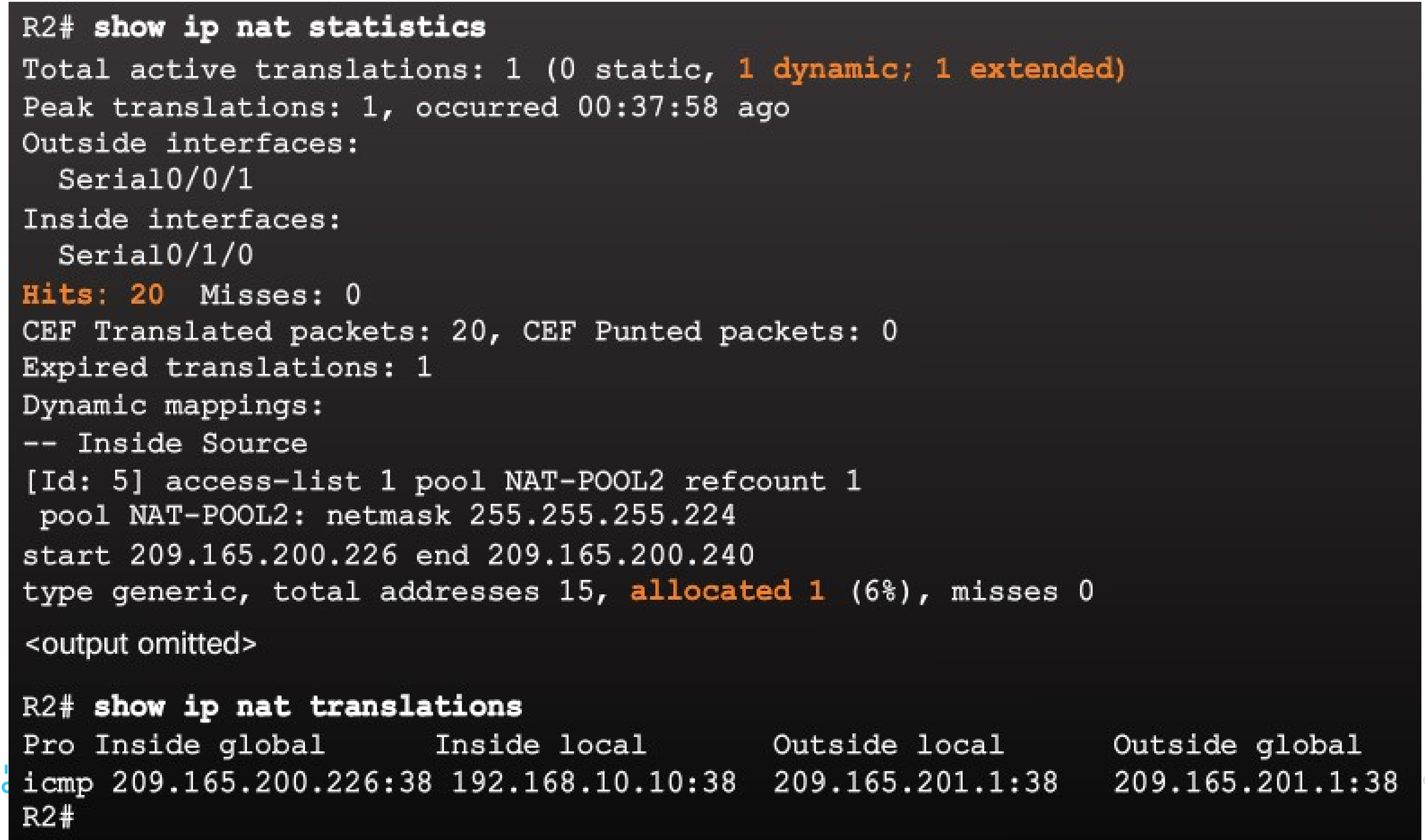


```
R2# show access-lists
Standard IP access list 1
  10 permit 192.168.0.0, wildcard bits 0.0.255.255 (29 matches)
```



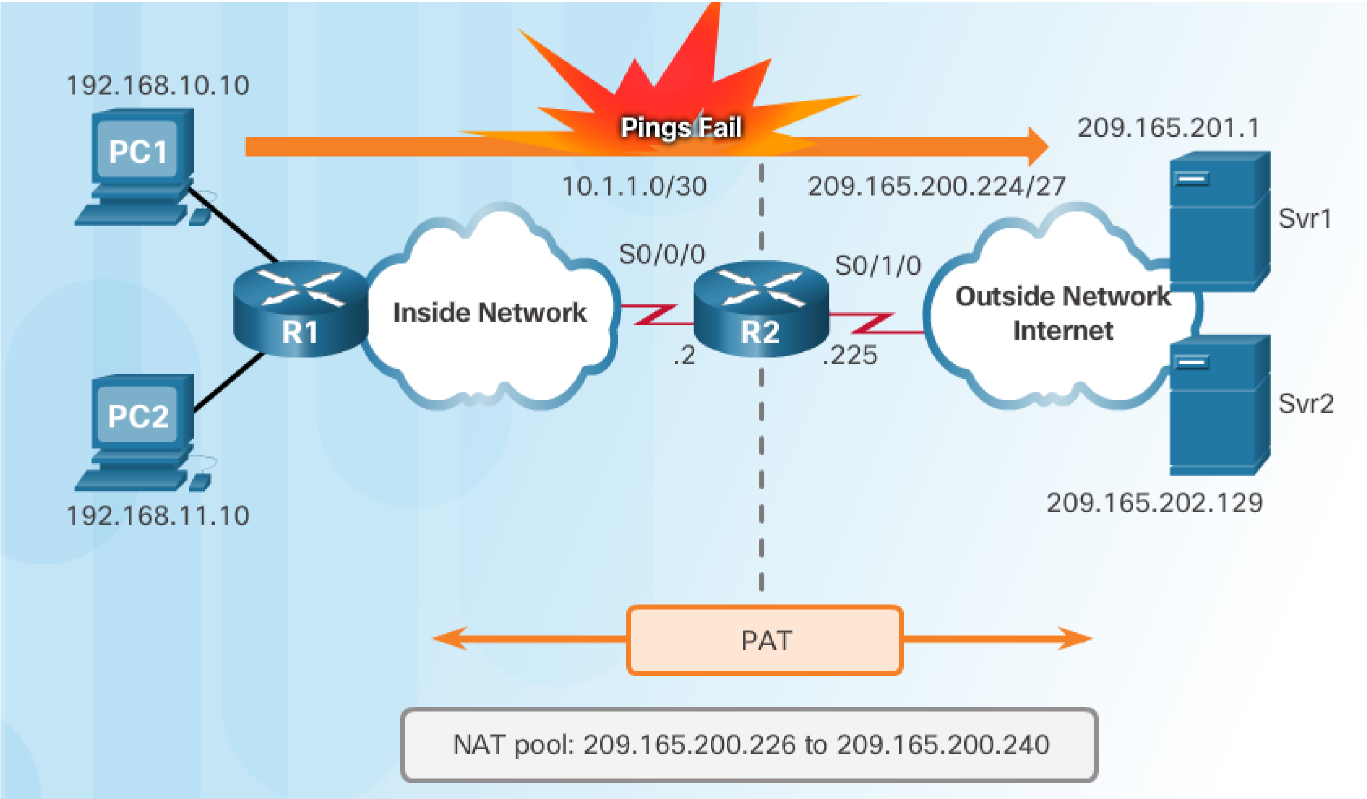
```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1  [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1  [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>
```

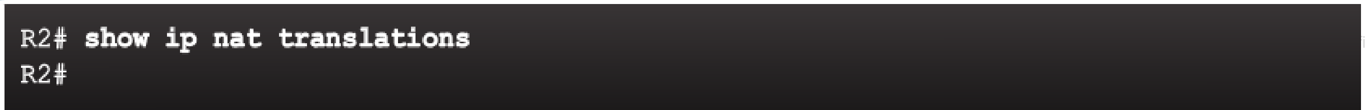
NAT Troubleshooting Scenario: překlady by měly vypadat takto:



```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:37:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 20  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 1
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
icmp 209.165.200.226:38 192.168.10.10:38  209.165.201.1:38   209.165.201.1:38
R2#
```

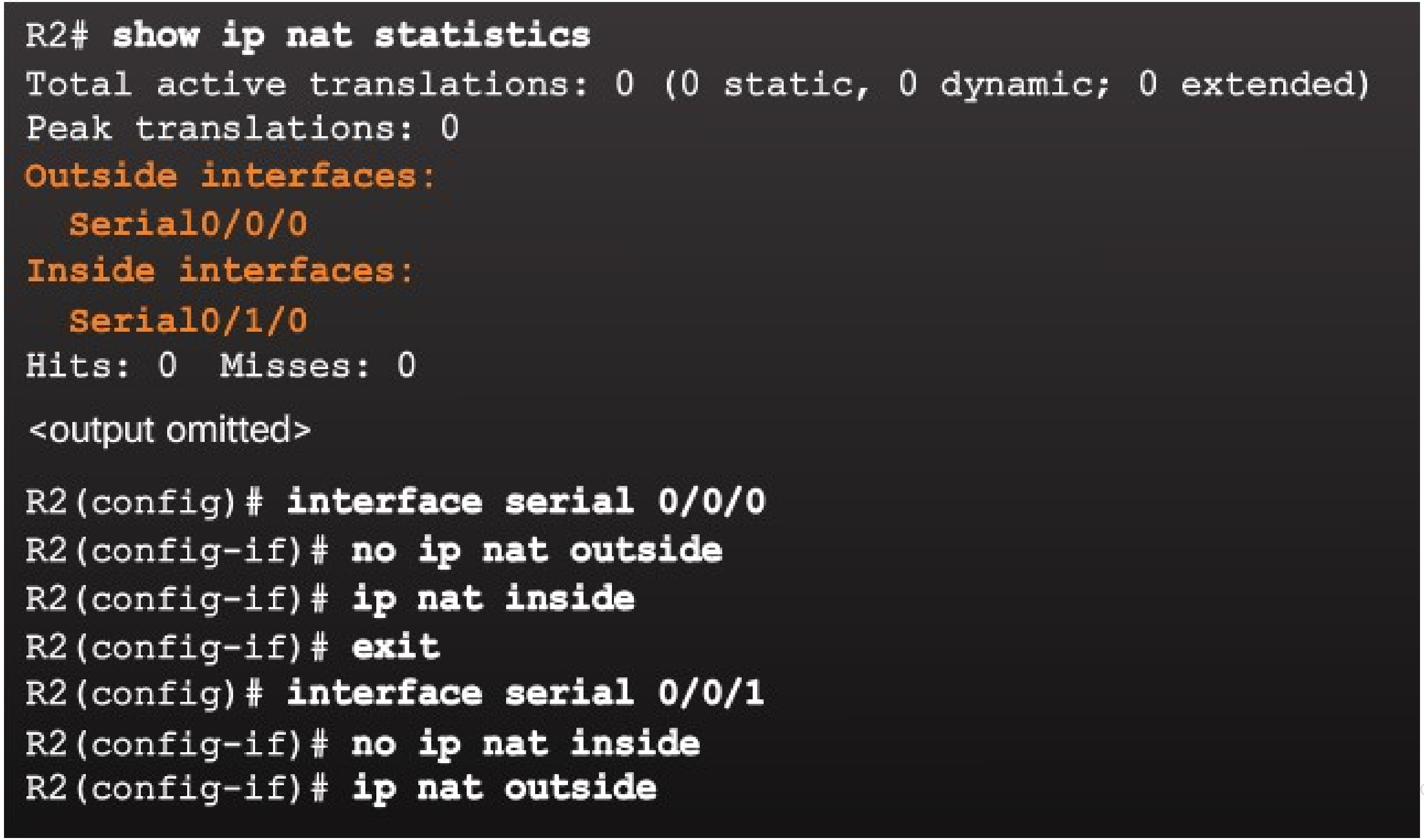
NAT Troubleshooting Scenario: interní počítač není schopen kontaktovat externí server, tabulka překladů vypadá takto: nic





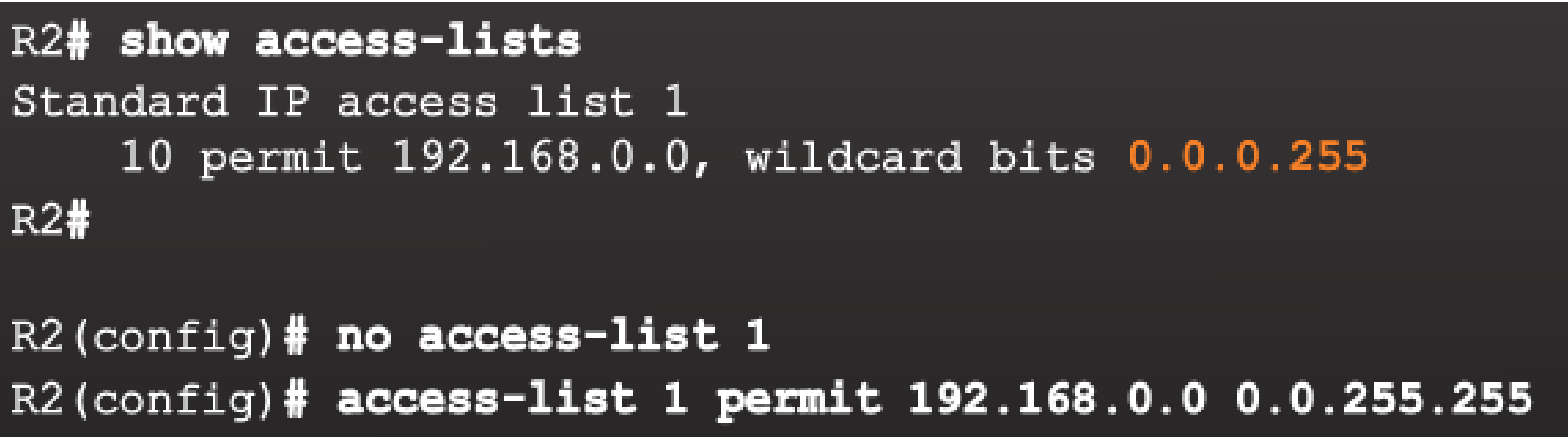
```
R2# show ip nat translations
R2#
```

NAT Troubleshooting Scenario: můžete mít prohozeny rozhraní



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

<output omitted>

R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```

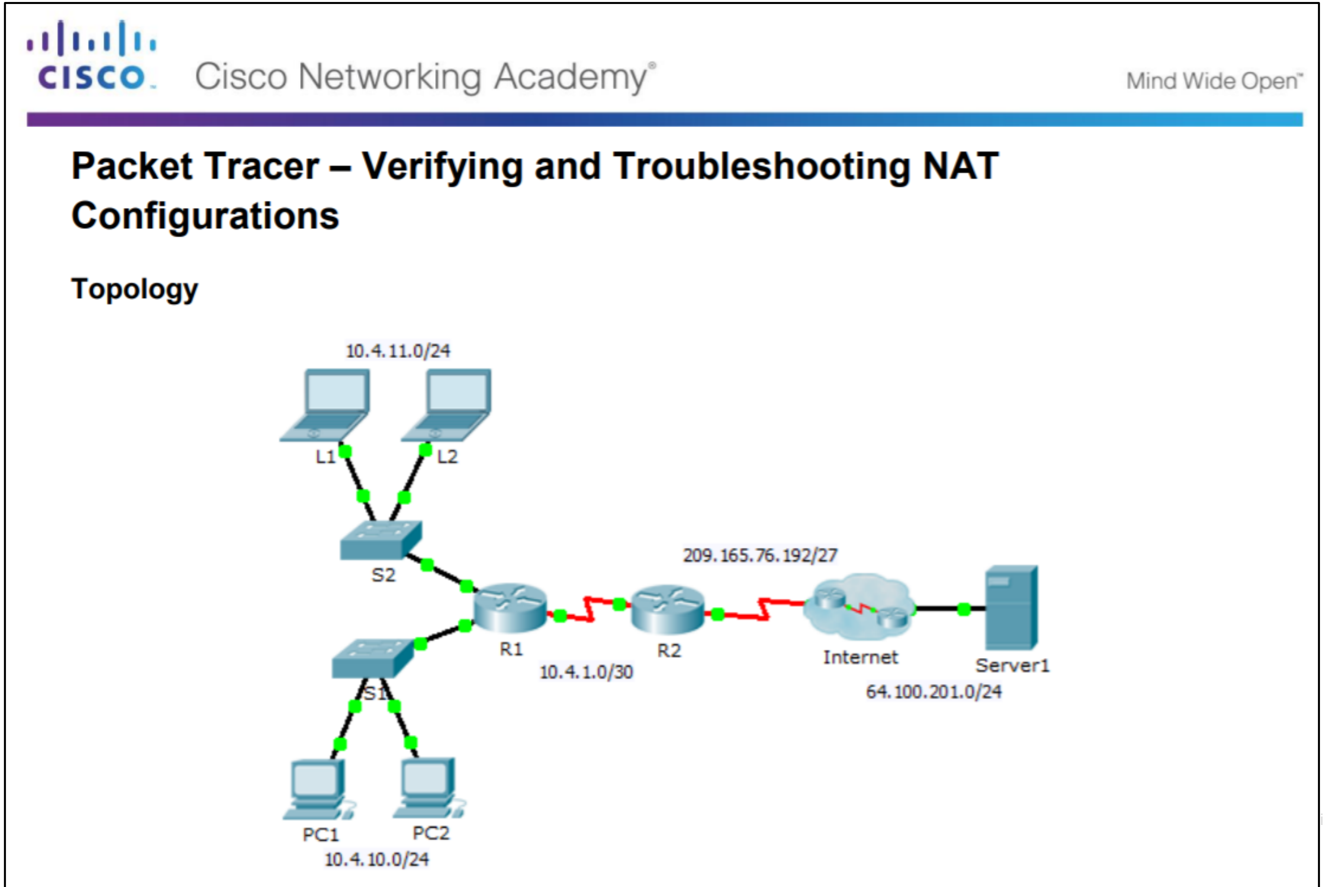
NAT Troubleshooting Scenario: může být blbě ACL



```
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
R2#

R2(config)# no access-list 1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

NAT Troubleshooting Commands

Packet Tracer – Verifying and Troubleshooting NAT Configurations



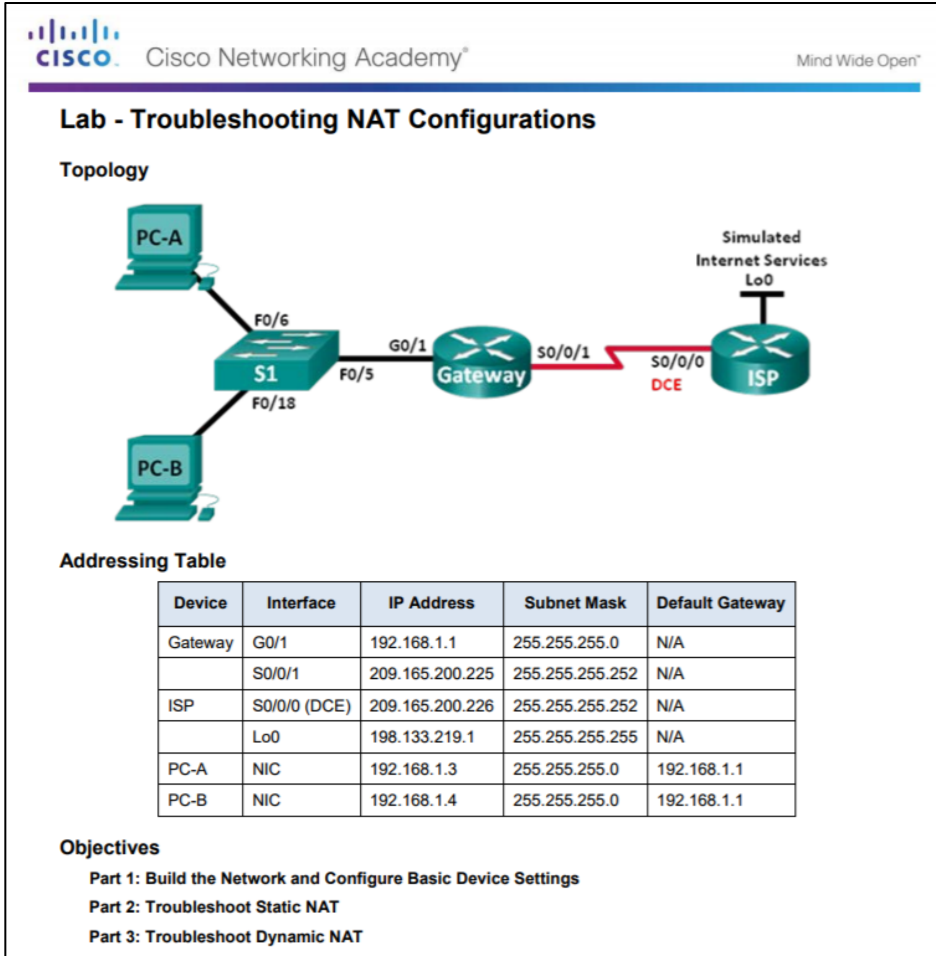
Cisco Networking Academy®

Mind Wide Open™

Packet Tracer – Verifying and Troubleshooting NAT Configurations

Topology

Troubleshooting NAT Configurations



Cisco Networking Academy® Mind Wide Open™

Lab - Troubleshooting NAT Configurations

Topology

PC-A
PC-B
S1
F0/6
F0/5
F0/18
G0/1
Gateway
S0/0/1
S0/0/0
DCE
ISP
Simulated Internet Services
Lo0

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Static NAT

Part 3: Troubleshoot Dynamic NAT

Proxy a NAT

Typy proxy

CGI (Common Gateway Interface) Proxy – CGI proxy se používají hlavně pro přístup na webovou stránku, která je blokována firemními společnostmi, vzdělávací institucí atd. CGI proxy skryjí naši IP adresu a předávají webové stránky URL serveru proxy serveru, aby získali přístup na tyto stránky. Například stránky sociálních médií budou blokovány v různých korporátních společnostech, vzdělávací instituce CGI proxy nám pomáhají v přístupu na stránky.

Transparentní proxy – Transparentní proxy, který se představuje jako proxy server, ale nezakrývá aktuální IP adresu klienta. Klient proto neví, zda používají server proxy nebo ne. Pomáhá dostat se přes blok IP, ale uživatel nemá žádnou anonymitu.

Anonymous Proxy - Anonymní proxy server pomůže skrýt IP adresu klienta, ale představí jej jako proxy server. Pomůže vám určit anonymitu přes IP a poskytne nesprávnou IP adresu přístupovým webům.

High Anonymity Proxy – tento proxy server je nejbezpečnější a poskytuje uživateli úplnou anonymitu. Skrývá IP adresu klienta a sám funguje jako zařízení.

Co je proxy z bezpečnostního hlediska?

- Proxy server je počítač, který funguje jako **prostředník mezi internetem a uživatelským počítačem**. Umožňuje počítači uživatele nepřímé připojení k jiným síťovým službám.

- Proxy server se používá hlavně pro skrytí aktuální polohy uživatele a sdílení internetového připojení mezi více uživateli.

- Když používáme proxy server, klientské počítače se nejprve připojí k proxy serveru a poté pošlou požadavek. Proxy server nejprve zkontroluje v keši, zda požadavek již neproveden dříve. Pokud nebyl, nový je požadavek odeslán na internet z proxy serveru.

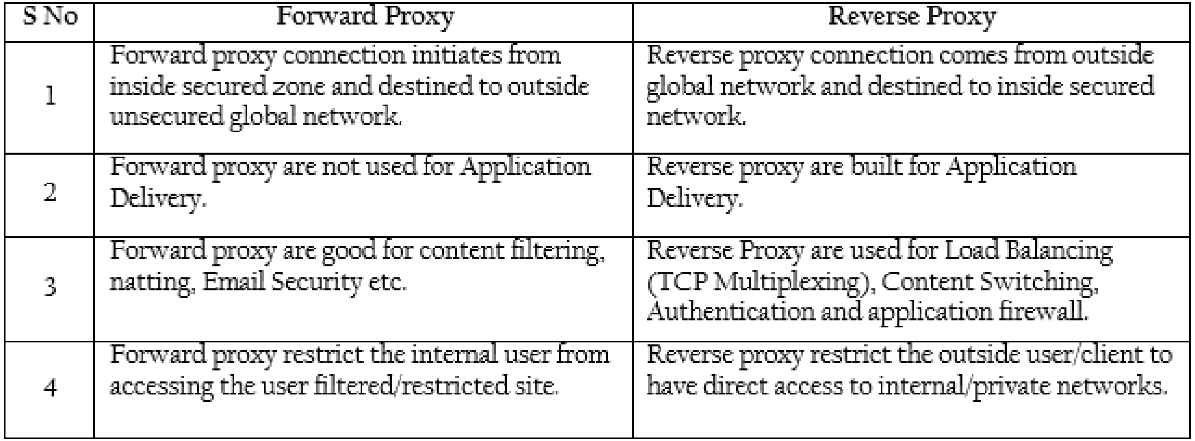
Výhody proxy

- Snižuje náklady na internet, protože může být sdílen s více klienty.

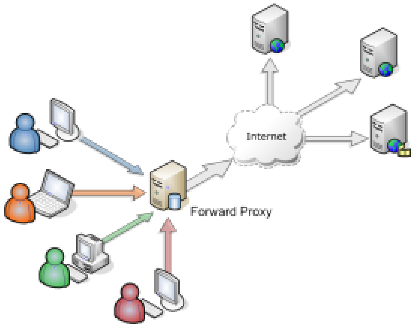
- Může být použit v rámci VPN spojení, což vám pomůže skrýt aktuální polohu a pomoci zobrazit umístění podle našich preferencí.

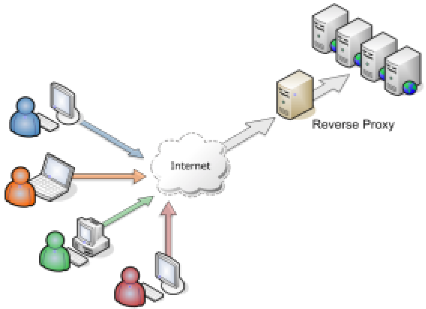
- Lze aplikovat filtr, čímž zlepšují bezpečnostní funkce.

Rozdíly forward proxy – reverse proxy

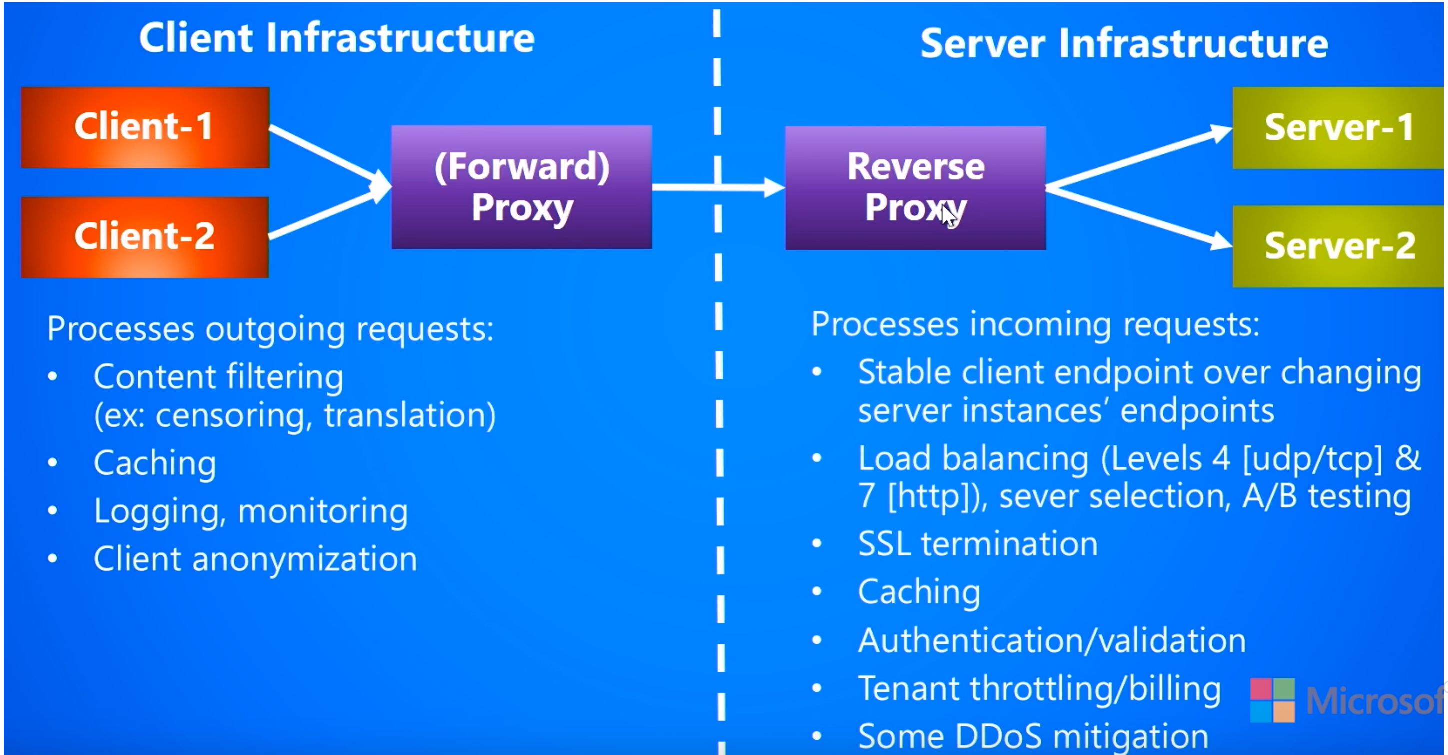


S No	Forward Proxy	Reverse Proxy
1	Forward proxy connection initiates from inside secured zone and destined to outside unsecured global network.	Reverse proxy connection comes from outside global network and destined to inside secured network.
2	Forward proxy are not used for Application Delivery.	Reverse proxy are built for Application Delivery.
3	Forward proxy are good for content filtering, natting, Email Security etc.	Reverse Proxy are used for Load Balancing (TCP Multiplexing), Content Switching, Authentication and application firewall.
4	Forward proxy restrict the internal user from accessing the user filtered/restricted site.	Reverse proxy restrict the outside user/client to have direct access to internal/private networks.





Pohled Microsoftu



Client Infrastructure

Client-1

Client-2

(Forward) Proxy

Processes outgoing requests:

- Content filtering (ex: censoring, translation)
- Caching
- Logging, monitoring
- Client anonymization

Server Infrastructure

Reverse Proxy

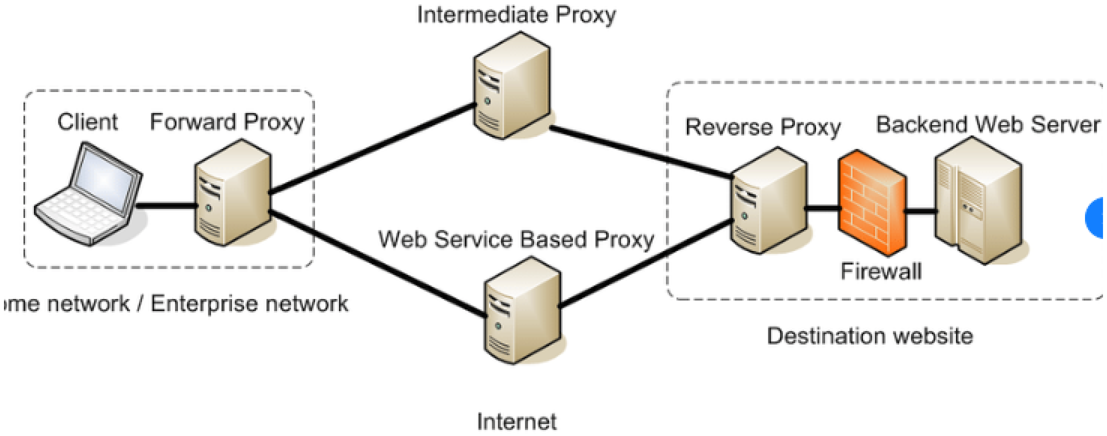
Server-1

Server-2

Processes incoming requests:

- Stable client endpoint over changing server instances' endpoints
- Load balancing (Levels 4 [udp/tcp] & 7 [http]), sever selection, A/B testing
- SSL termination
- Caching
- Authentication/validation
- Tenant throttling/billing
- Some DDoS mitigation

Kam firewall



K čemu lze forward proxy použít

- Content Filtering
- eMail security
- NAT’ing
- Compliance Reporting

K čemu lze reverse proxy použít

- Application Delivery including:
- Load Balancing (TCP Multiplexing)
- SSL Offload/Acceleration (SSL Multiplexing)
- Caching
- Compression
- Content Switching/Redirection
- Application Firewall
- Server Obfuscation
- Authentication

Co blokuje jedna US firma na forward proxy

- familypostcards2008.com (Storm Worm virus)
- facebook.com
- playboy.com
- wikipedia.org

forward proxy software (server side)

PHP-Proxy

cgi-proxy

glype

Internet censorship wiki: List of Web Proxies

reverse proxy software for HTTP (server side)

- apache mod_proxy (can also work as a forward proxy for HTTP)
- nginx (used on hulu.com, spam sites, etc.)
- HAProxy
- lighthttpd
- perlbal portfusion
- pound

reverse proxy software for TCP (server side)

balance

delegate

pen

portfusion

python director

Rozdíl proxy a NAT

- 'Proxy' označuje aplikaci vrstvy 7 na referenčním modelu OSI. Překlad síťových adres (NAT) je podobný proxy, ale pracuje ve vrstvě 3.

- V konfiguraci klienta vrstvy-3 NAT je konfigurace brány dostatečná. Pro klientskou konfiguraci proxy vrstvy 7 však musí být cílem paketů, které klient vygeneruje, vždy proxy server (vrstva-7), pak proxy server přečte každý paket a zjistí skutečný cíl.

- Vzhledem k tomu, že NAT pracuje na vrstvě 3, je méně náročný na zdroje než proxy vrstvy 7, ale také méně flexibilní.

- Srovnáme-li tyto dvě technologie, můžeme se setkat s terminologií známou jako „transparentní firewall“. Transparentní brána firewall znamená, že proxy používá výhody proxy vrstvy 7 bez znalosti klienta. Klient předpokládá, že brána je NAT ve vrstvě 3 a nemá žádnou představu o vnitřku paketu, ale prostřednictvím této metody se pakety vrstvy 3 odesílají pro účely vyšetřování do proxy serveru vrstvy 7.

Tor onion proxy software

- Tor (zkratka pro Onion Router) je systém, který má umožnit online anonymitu. Klientský software Tor směruje internetový provoz prostřednictvím celosvětové sítě serverů dobrovolníků, aby se utajilo umístění uživatele nebo jeho použití od někoho, kdo provádí sledování sítě nebo analýzu provozu. Pomocí Tor je obtížnější sledovat činnost na internetu, včetně „návštěv na webových stránkách, online příspěvcích, okamžitých zprávách a dalších komunikačních formátech“, zpět uživateli. Jeho cílem je chránit osobní svobodu, soukromí a schopnost provádět důvěrné obchodní činnosti tím, že jejich internetové aktivity budou monitorovány.

Problém s NAT

Velký problém je s NAT. Otázkou je, kde je umístěno proxy:

- uvnitř vnitřní sítě (v rámci lokální LAN);

- v rámci vnější sítě a z vnitřní sítě se je třeba k němu přihlašovat;

- dvě administrativní domény jsou spolu propojeny, každá má vlastní proxy.

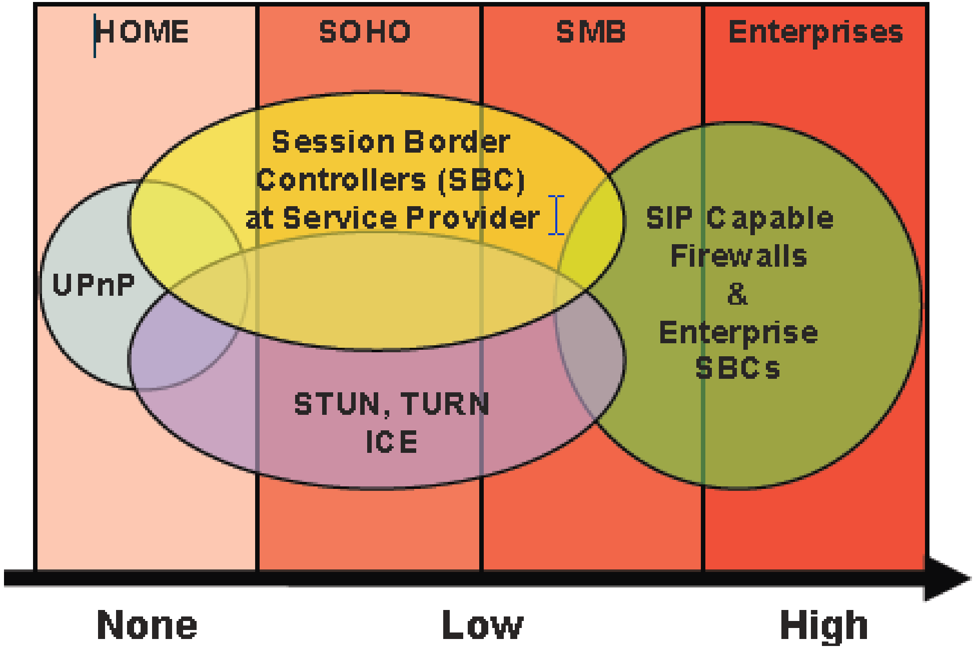
.

Nejnepříjemnější je vnější proxy

- Jeho privátní IP adresa je z privátní sítě (např. 10.1.1.100) a přichází k proxy v příkazu INVITE spolu s jeho SIP adresou (např. pepa@hp.cz).
- Odpověď OK pak nenalezne příjemce. Možným řešením je použití transportního protokolu TCP anebo protokolu STUN.
- A nejlepším řešením je NAT vůbec pokud možno nepoužívat – což je i jeden z argumentů pro přechod na IPv6.

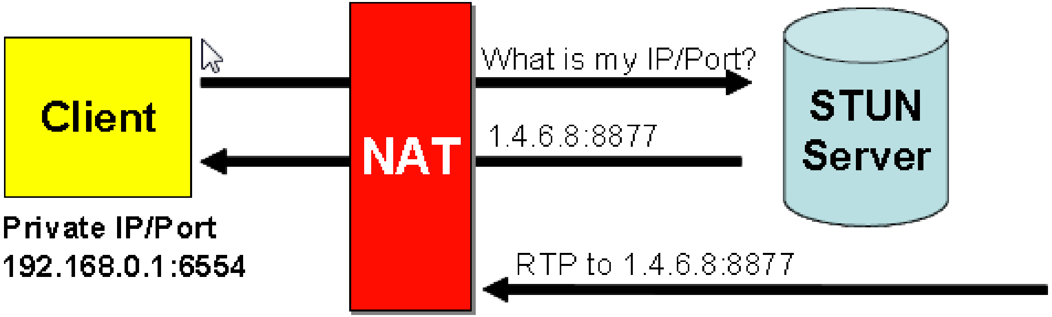
Kdy STUN a kdy firewall?

STUN – Simple traversal of UDP through NATs


HOME
SOHO
SMB
Enterprises
Session Border Controllers (SBC) at Service Provider
UPnP
SIP Capable Firewalls & Enterprise SBCs
STUN, TURN ICE
None
Low
High

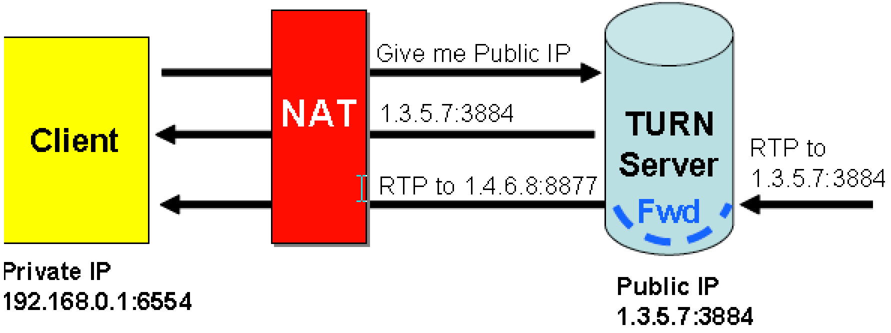
STUN
(Simple/Session Traversal of UDP through NATs)

- Dvojice adres „server-reflexivní“
- Obvykle u ISP jako služba
- STUN2 xoruje k adrese nonce
- Klient je cloněn pouze nepříliš bezpečným NAT a je vystaven útokům kohokoliv, kdo odchytá STUN provoz
- Nezajišťuje symetrický NAT, kdy mezi unikátními IP adresami a porty odesilatele a příjemce misí být unikátní i dvojice na NATu (jen pro ně).

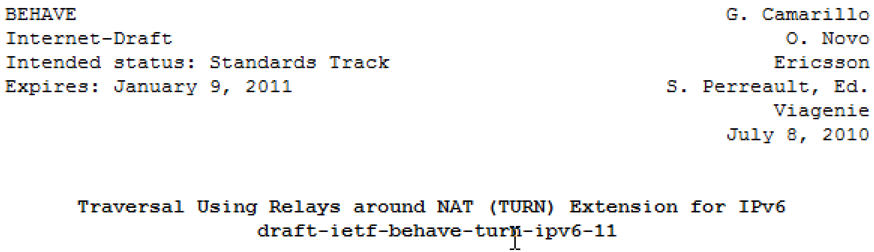


TURN
(Traversal Using Relay NAT)

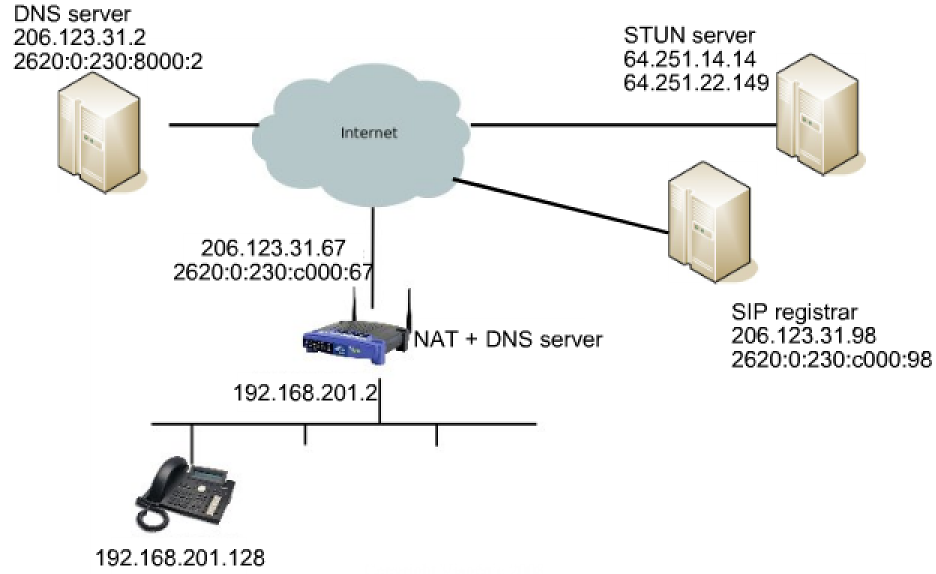
- Metoda náročná na šířku pásma
- Server musí být blízko NATu a k dispozici po celou dobu komunikace
- Zajišťuje symetrický NAT



TURN je součást migrace do IPv6



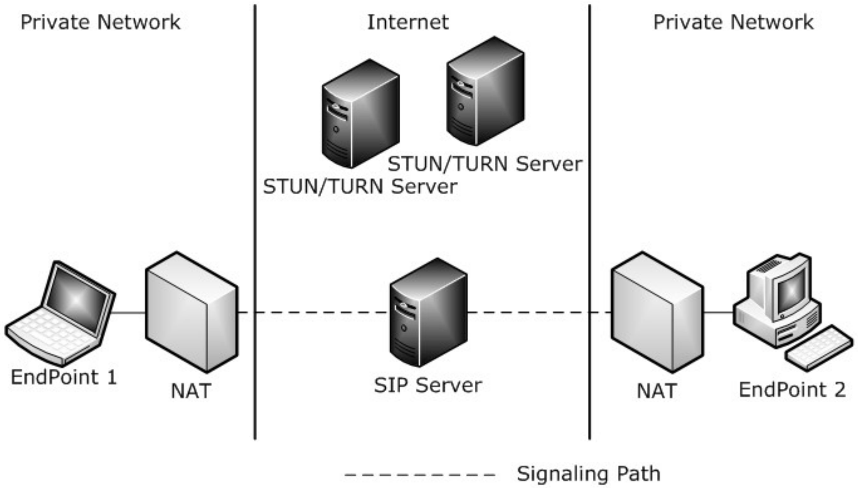
```
BEHAVE                                                    G. Camarillo
Internet-Draft                                                 O. Novo
Intended status: Standards Track                              Ericsson
Expires: January 9, 2011                            S. Perreault, Ed.
                                                              Viagenie
                                                          July 8, 2010


     Traversal Using Relays around NAT (TURN) Extension for IPv6
                    draft-ietf-behave-turn-ipv6-11
```



ICE
(Interactive Connectivity Establishment)

- Využívá STUN i TURN podle nastavené priority
- Zprostředkovává je volanému prostřednictvím CDP
- Po navázání spojení zastaví jejich použití

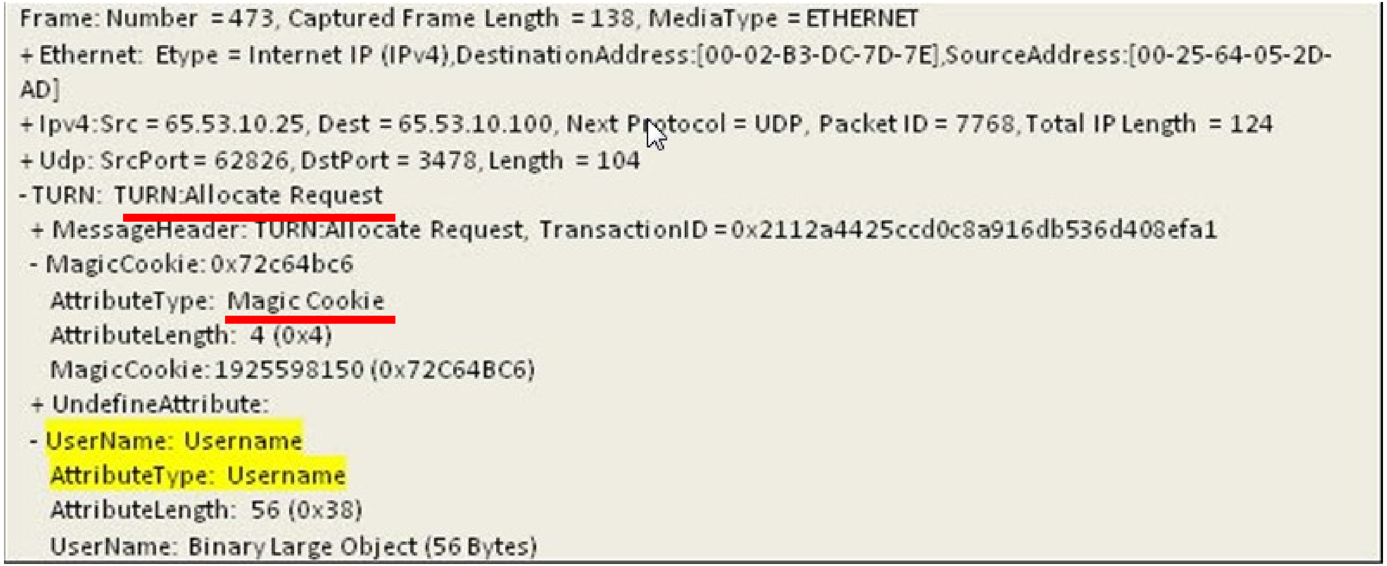
Microsoft Office Communications Server 2007 R2, A/V Edge Server
je rozšířen o STUN/TURN, blíže Mike Atkins v „Troubleshoot STUN with TURN
in Office Communications Server 2007 R2“ v http://blogs.technet.com z prosince 2010



Microsoft ICE z roku 2008 – 1. krok

Klient posílá požadavek na STUN/TURN server

Klient STUN posílá *TURN Allocation request* na A/V Edge Server

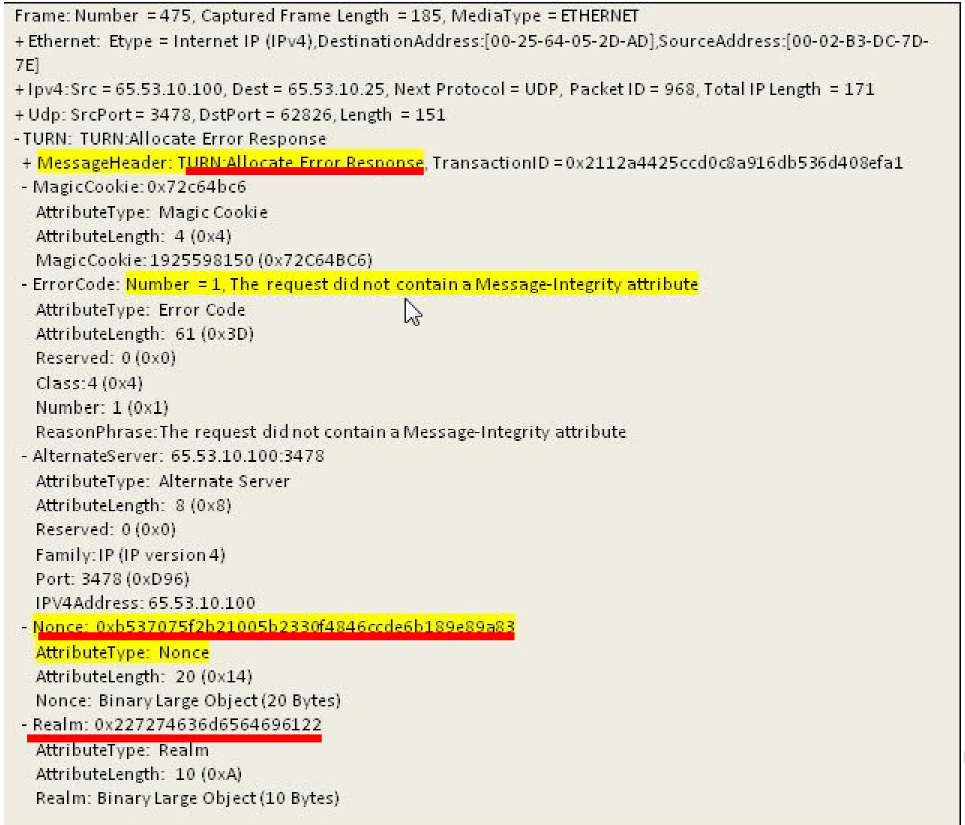


```
Frame: Number =473, Captured Frame Length =138, MediaType =ETHERNET
+Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-02-B3-DC-7D-7E],SourceAddress:[00-25-64-05-2D-
AD]
+Ipv4:Src =65.53.10.25, Dest =65.53.10.100, Next Protocol = UDP, Packet ID = 7768, Total IP Length = 124
+Udp: SrcPort = 62826, DstPort = 3478, Length = 104
-TURN: TURN:Allocate Request
 +MessageHeader: TURN:Allocate Request, TransactionID =0x2112a4425ccd0c8a916db536d408efa1
 -MagicCookie: 0x72c64bc6
   AttributeType: Magic Cookie
   AttributeLength: 4 (0x4)
   MagicCookie: 1925598150 (0x72C64BC6)
 +UndefineAttribute:
 -UserName: Username
   AttributeType: Username
   AttributeLength: 56 (0x38)
   UserName: Binary Large Object (56 Bytes)
```

Záznam: Microsoft Network Monitor 3.4

2. krok

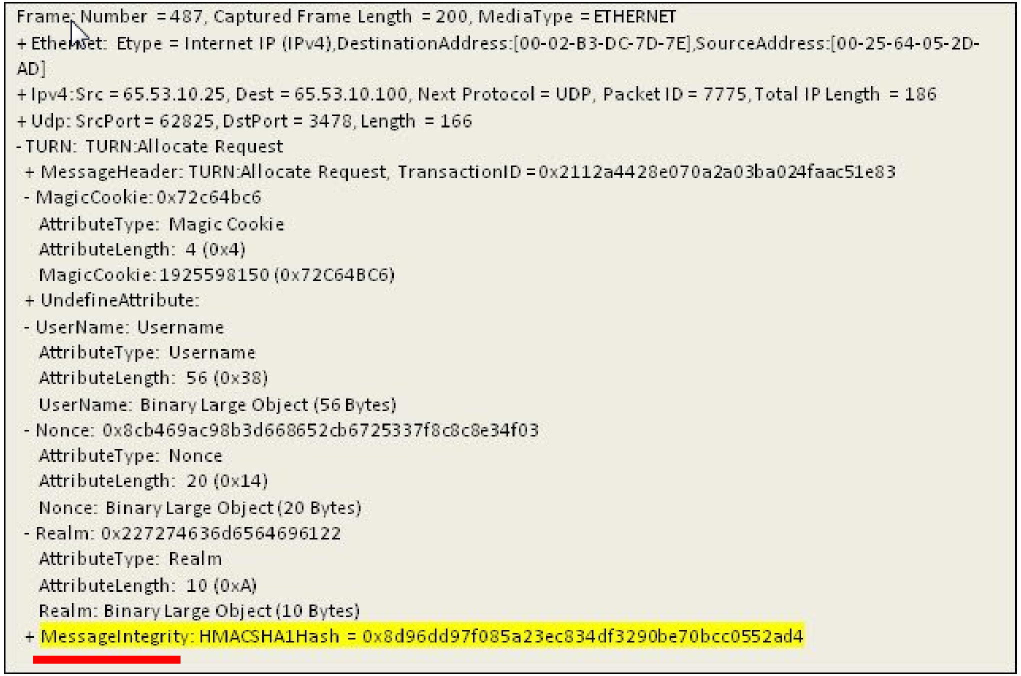
Odpověď STUN/TURN serveru



```
Frame: Number  = 475, Captured Frame Length  = 185, MediaType = ETHERNET
+ Ethernet:  Etype = Internet IP (IPv4),DestinationAddress:[00-25-64-05-2D-AD],SourceAddress:[00-02-B3-DC-7D-
7E]
+ Ipv4:Src = 65.53.10.100, Dest = 65.53.10.25, Next Protocol = UDP, Packet ID = 968, Total IP Length  = 171
+ Udp: SrcPort = 3478, DstPort = 62826, Length  = 151
- TURN:  TURN:Allocate Error Response
 + MessageHeader: TURN:Allocate Error Response, TransactionID = 0x2112a4425ccd0c8a916db536d408efa1
 - MagicCookie: 0x72c64bc6
    AttributeType:  Magic Cookie
    AttributeLength:  4 (0x4)
    MagicCookie: 1925598150 (0x72C64BC6)
 - ErrorCode: Number  = 1, The  request did not contain a Message-Integrity attribute
    AttributeType:  Error Code
    AttributeLength:  61 (0x3D)
    Reserved:  0 (0x0)
    Class: 4 (0x4)
    Number:  1 (0x1)
    ReasonPhrase: The request did not contain a Message-Integrity attribute
 - AlternateServer:  65.53.10.100:3478
    AttributeType:  Alternate Server
    AttributeLength:  8 (0x8)
    Reserved:  0 (0x0)
    Family: IP (IP version 4)
    Port: 3478 (0xD96)
    IPV4Address: 65.53.10.100
 - Nonce:  0xb537075f2b21005b2330f4846ccde6b189e89a83
    AttributeType:  Nonce
    AttributeLength:  20 (0x14)
    Nonce:  Binary Large Object (20 Bytes)
 - Realm: 0x227274636d6564696122
    AttributeType:  Realm
    AttributeLength:  10 (0xA)
    Realm: Binary Large Object (10 Bytes)
```

3. krok

Výpočet MI a její odeslání na STUN/TURN server



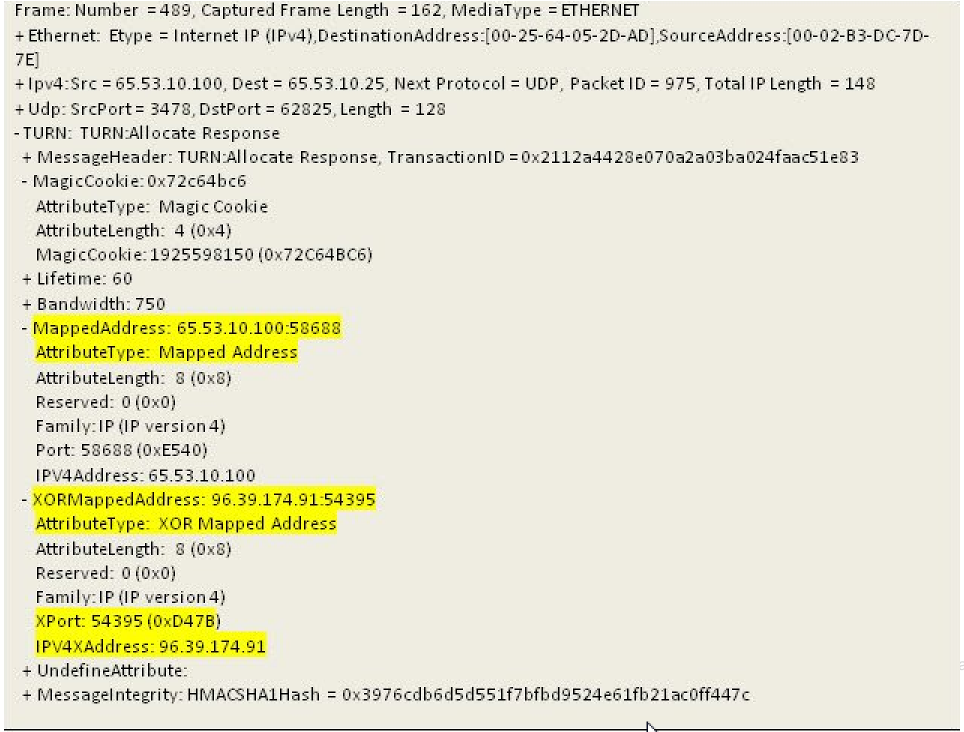
```
Frame: Number  = 487, Captured Frame Length  = 200, MediaType = ETHERNET
+ Ethernet:  Etype = Internet IP (IPv4),DestinationAddress:[00-02-B3-DC-7D-7E],SourceAddress:[00-25-64-05-2D-
AD]
+ Ipv4:Src = 65.53.10.25, Dest = 65.53.10.100, Next Protocol = UDP, Packet ID = 7775, Total IP Length  = 186
+ Udp: SrcPort = 62825, DstPort = 3478, Length  = 166
- TURN:  TURN:Allocate Request
 + MessageHeader: TURN:Allocate Request, TransactionID = 0x2112a4428e070a2a03ba024faac51e83
 - MagicCookie: 0x72c64bc6
   AttributeType:  Magic Cookie
   AttributeLength:  4 (0x4)
   MagicCookie: 1925598150 (0x72C64BC6)
 + UndefineAttribute:
 - UserName:  Username
   AttributeType:  Username
   AttributeLength:  56 (0x38)
   UserName:  Binary Large Object (56 Bytes)
 - Nonce:  0x8cb469ac98b3d668652cb6725337f8c8c8e34f03
   AttributeType:  Nonce
   AttributeLength:  20 (0x14)
   Nonce:  Binary Large Object (20 Bytes)
 - Realm: 0x227274636d6564696122
   AttributeType:  Realm
   AttributeLength:  10 (0xA)
   Realm: Binary Large Object (10 Bytes)
 + MessageIntegrity: HMACSHA1Hash = 0x8d96dd97f085a23ec834df3290be70bcc0552ad4
```

Message-Integrity = MD5(username ":" realm ":" SASLPrep(password))

kde SASL (Simple Authentication and Security Layer) je obecná metoda ověřování v protokolech klient/server
SASLprep – reprezentace jmen a hesel pro SASL - viz RFC 4013

4. krok
Server STUN/TURN odpovídá vzdálenému klientu

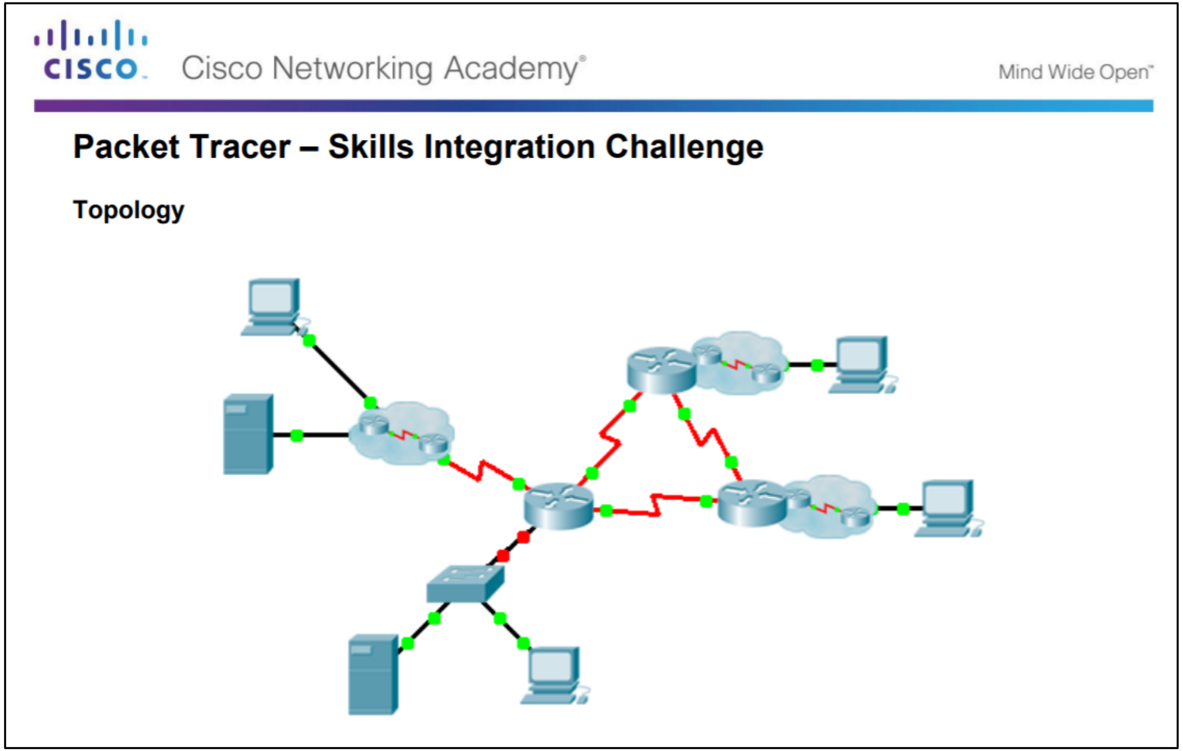
- Server STUN/TURN odesílá paket Allocate Response, v ní hodnotu časovače, šířky pásma…
- XORMappedAddress je počítána XORem z MagicCookie z 1. kroku



```
Frame: Number  = 489, Captured Frame Length  = 162, MediaType = ETHERNET
+ Ethernet:  Etype = Internet IP (IPv4),DestinationAddress:[00-25-64-05-2D-AD],SourceAddress:[00-02-B3-DC-7D-
7E]
+ Ipv4:Src = 65.53.10.100, Dest = 65.53.10.25, Next Protocol = UDP, Packet ID = 975, Total IP Length  = 148
+ Udp: SrcPort = 3478, DstPort = 62825, Length  = 128
- TURN:  TURN:Allocate Response
  + MessageHeader: TURN:Allocate Response, TransactionID = 0x2112a4428e070a2a03ba024faac51e83
  - MagicCookie: 0x72c64bc6
     AttributeType:  Magic Cookie
     AttributeLength:  4 (0x4)
     MagicCookie: 1925598150 (0x72C64BC6)
  + Lifetime: 60
  + Bandwidth: 750
  - MappedAddress: 65.53.10.100:58688
     AttributeType:  Mapped Address
     AttributeLength:  8 (0x8)
     Reserved:  0 (0x0)
     Family: IP (IP version 4)
     Port: 58688 (0xE540)
     IPV4Address: 65.53.10.100
  - XORMappedAddress: 96.39.174.91:54395
     AttributeType:  XOR Mapped Address
     AttributeLength:  8 (0x8)
     Reserved:  0 (0x0)
     Family: IP (IP version 4)
     XPort: 54395 (0xD47B)
     IPV4XAddress: 96.39.174.91
  + UndefineAttribute:
  + MessageIntegrity: HMACSHA1Hash = 0x3976cdb6d5d551f7bfbd9524e61fb21ac0ff447c
```

9.4 Chapter Summary

Packet Tracer - Skills Integration Challenge



Cisco Networking Academy®

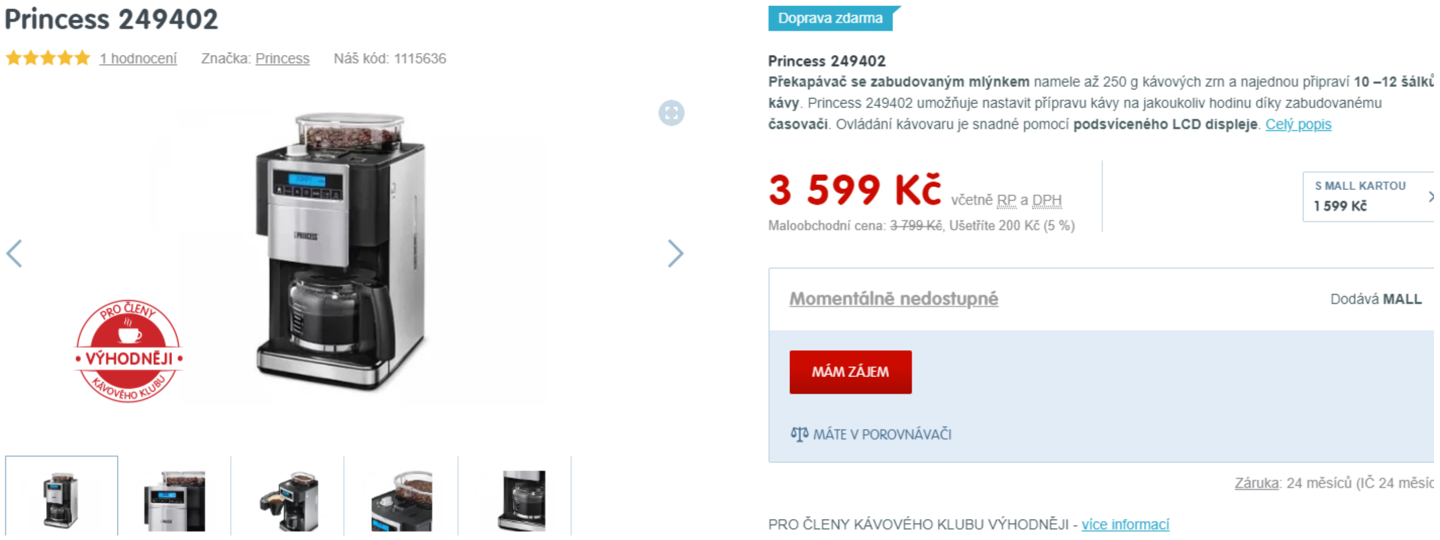
Mind Wide Open™

Packet Tracer – Skills Integration Challenge

Topology

Conclusion

- Explain how NAT provides IPv4 address scalability in a small to medium-sized business network.
- Configure NAT services on the edge router to provide IPv4 address scalability in a small to medium-sized business network.
- Troubleshoot NAT issues in a small to medium-sized business network.



Princess 249402

★★★★★ 1 hodnocení Značka: Princess Náš kód: 1115636

Doprava zdarma

Princess 249402

Překapávač se zabudovaným mlýnkem namele až 250 g kávových zrn a najednou připraví **10 –12 šálků kávy**. Princess 249402 umožňuje nastavit přípravu kávy na jakoukoliv hodinu díky zabudovanému **časovači**. Ovládání kávovaru je snadné pomocí **podsvíceného LCD displeje**. Celý popis

3 599 Kč včetně RP a DPH

Maloobchodní cena: ~~3 799 Kč~~, Ušetříte 200 Kč (5 %)

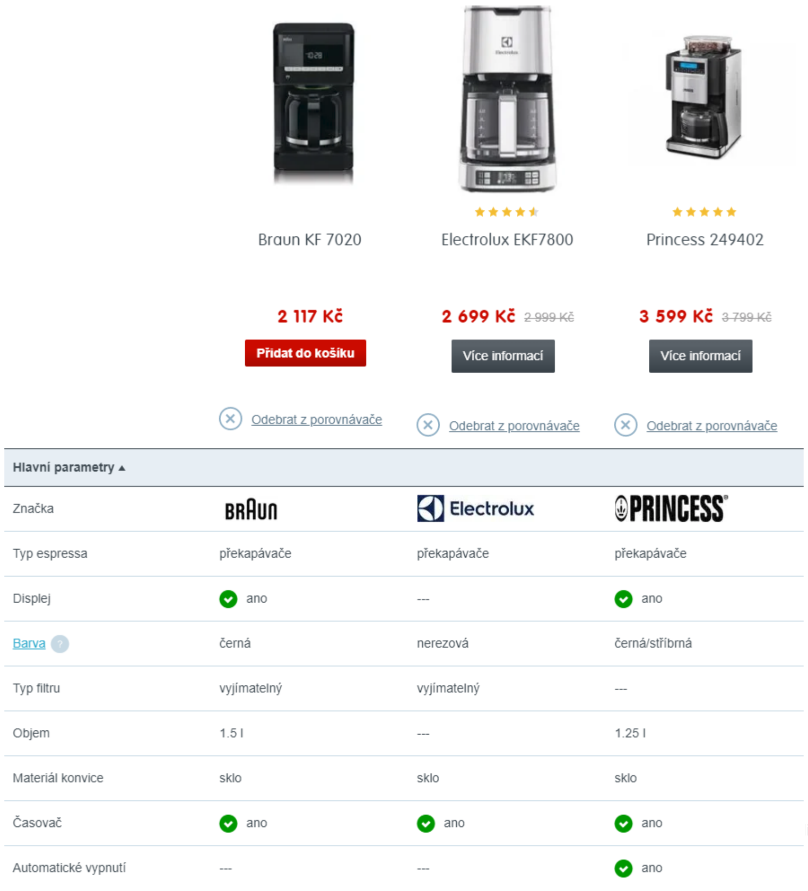
S MALL KARTOU 1 599 Kč

Momentálně nedostupné Dodává **MALL**

Záruka: 24 měsíců (IČ 24 měsíc

PRO ČLENY KÁVOVÉHO KLUBU VÝHODNĚJI - více informací

https://www.mall.cz/porovnani?sectionId=EB036



	Braun KF 7020	★★★★½ Electrolux EKF7800	★★★★★ Princess 249402
	2 117 Kč	2 699 Kč ~~2 999 Kč~~	3 599 Kč ~~3 799 Kč~~
	Přidat do košíku	Více informací	Více informací
	⊗ Odebrat z porovnávače	⊗ Odebrat z porovnávače	⊗ Odebrat z porovnávače
Hlavní parametry ▲			
Značka	BRAUN	Electrolux	PRINCESS
Typ espressa	překapávače	překapávače	překapávače
Displej	✓ ano	---	✓ ano
Barva ?	černá	nerezová	černá/stříbrná
Typ filtru	vyjímatelný	vyjímatelný	---
Objem	1.5 l	---	1.25 l
Materiál konvice	sklo	sklo	sklo
Časovač	✓ ano	✓ ano	✓ ano
Automatické vypnutí	---	---	✓ ano