

[NAT for IPv4 / Types of NAT](#)

Types of NAT

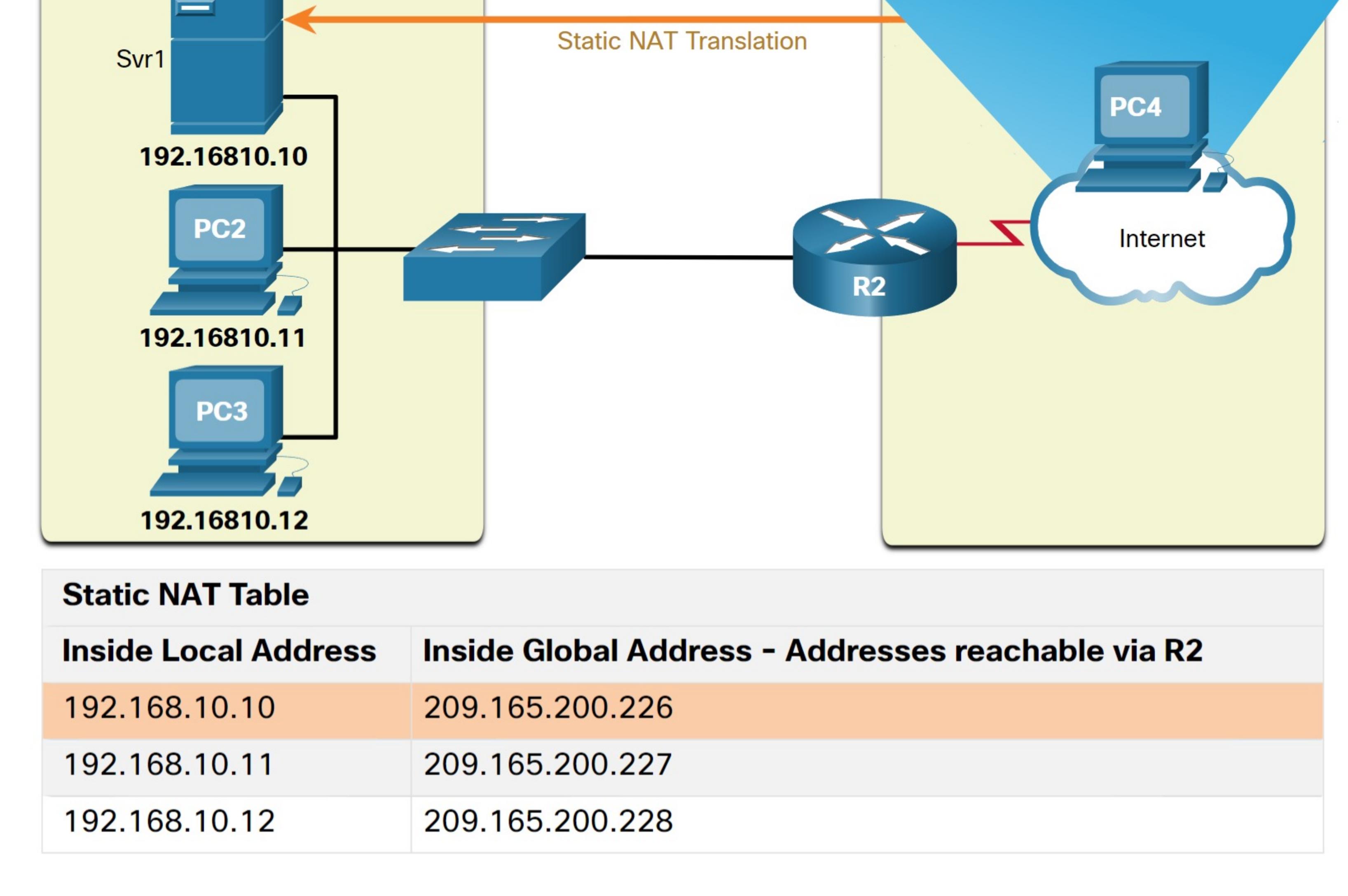
6.2.1

Static NAT

Now that you have learned about NAT and how it works, this topic will discuss the many versions of NAT that are available to you.

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant.

In the figure, R2 is configured with static mappings for the inside local addresses of Srv1, PC2, and PC3. When these devices send traffic to the Internet, their inside local addresses are translated to the configured inside global addresses. To outside networks, these devices appear to have public IPv4 addresses.


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 is particularly useful for web servers or devices that must have a consistent address that is accessible from the Internet, such as a company web server. It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the Internet. For example, a network administrator from PC4 can use SSH to gain access to the inside global address of Srv1 (209.165.200.226). R2 translates this inside global address to the inside local address 192.168.10.10 and connects the session to Srv1.

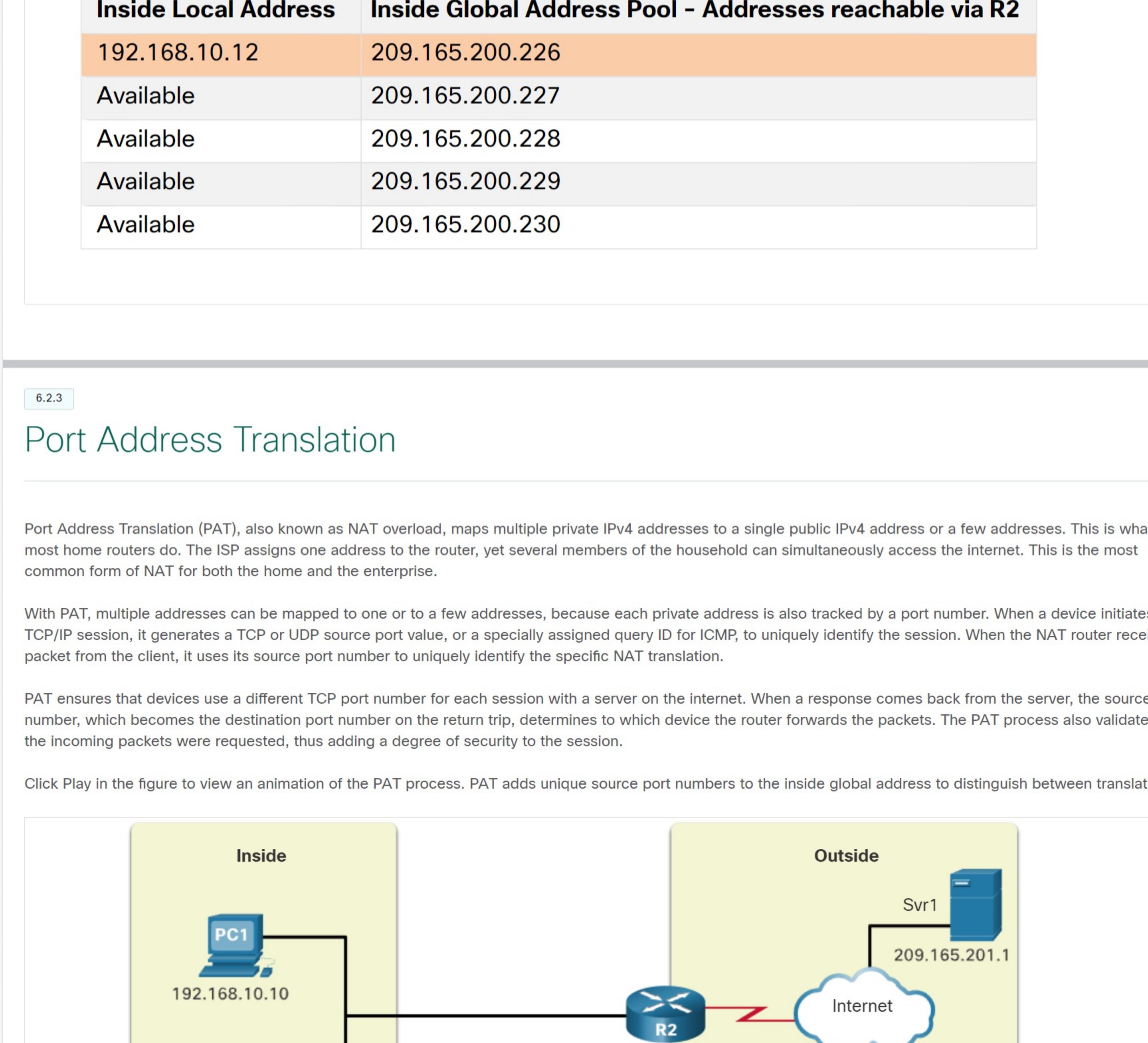
Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

6.2.2

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.

In the figure, PC3 has accessed the Internet using the first available address in the dynamic NAT pool. The other addresses are still available for use. Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.


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

6.2.3

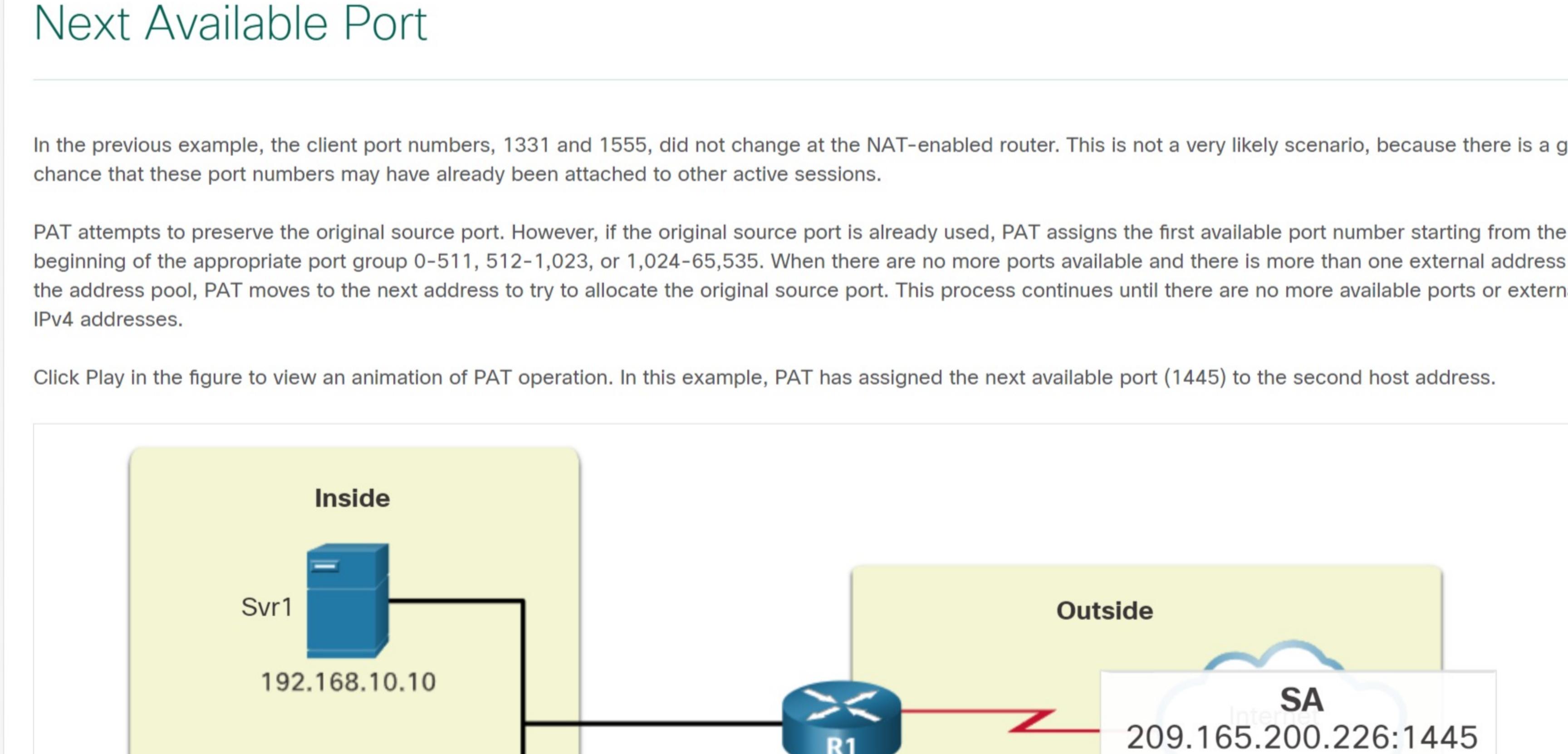
Port Address Translation

Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses. This is what most home routers do. The ISP assigns one address to the router, yet several members of the household can simultaneously access the Internet. This is the most common form of NAT for both the home and the enterprise.

With PAT, multiple addresses can be mapped to one or a few addresses, because each private address is also tracked by a port number. When a device initiates a TCP/IP session, it generates a TCP or UDP source port value, or a specially assigned query ID for ICMP, to uniquely identify the session. When the NAT router receives a packet from the client, it uses its source port number to uniquely identify the specific NAT translation.

PAT ensures that devices use a different TCP port number for each session with a server on the Internet. When a response comes back from the server, the source port number, which becomes the destination port number on the return trip, determines to which device the router forwards the packets. The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session.

Click Play in the figure to view an animation of the PAT process. PAT adds unique source port numbers to the inside global address to distinguish between translations.



As R2 processes each packet, it uses a port number (1331 and 1555, in this example) to identify the device from which the packet originated. The source address (SA) is the inside local address with the TCP/UDP assigned port number added. The destination address (DA) is the outside global address with the service port number added. In this example, the service port is 80, which is HTTP.

For the source address, R2 translates the inside local address to an inside global address with the port number added. The destination address is not changed but is now referred to as the outside global IPv4 address. When the web server replies, the path is reversed.

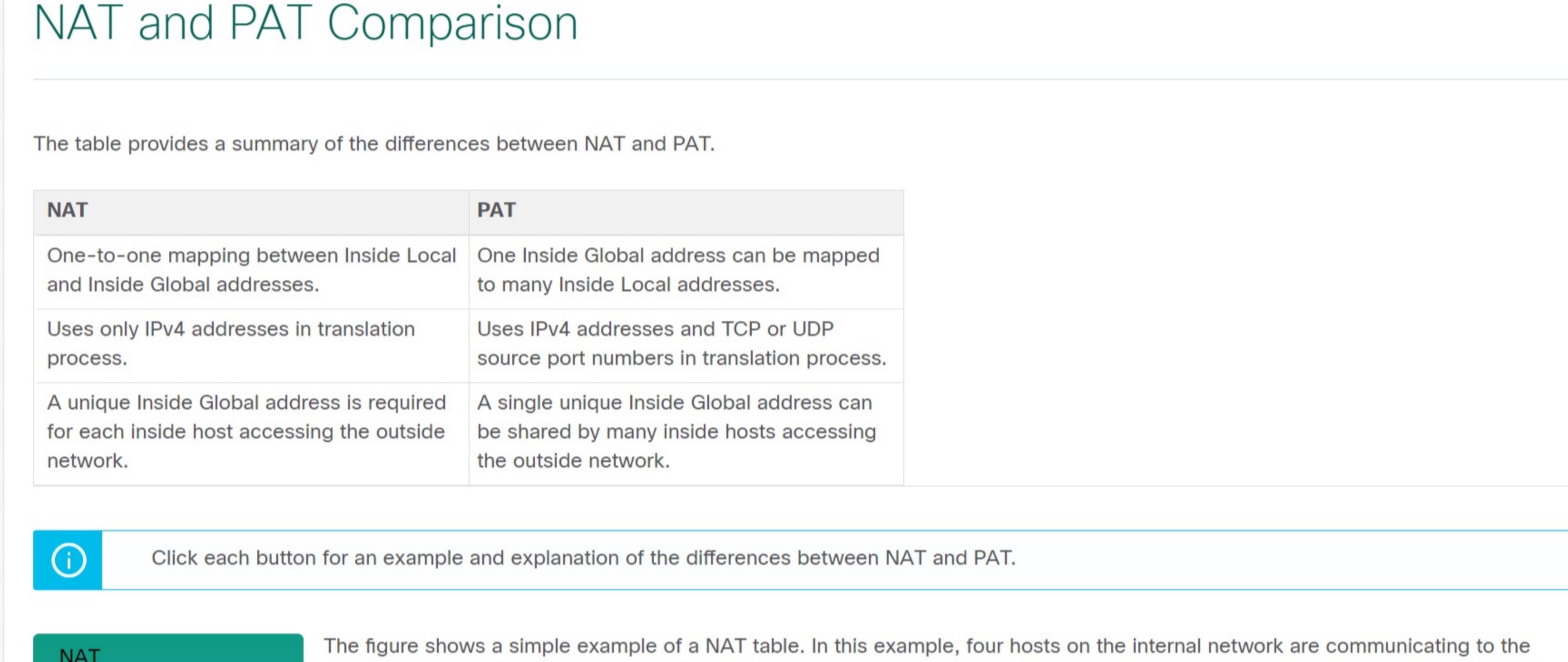
6.2.4

Next Available Port

In the previous example, the client port numbers, 1331 and 1555, did not change at the NAT-enabled router. This is not a very likely scenario, because there is a good chance that these port numbers may have already been attached to other active sessions.

PAT attempts to preserve the original source port. However, if the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0-511, 512-1,023, or 1,024-65,535. When there are no more ports available and there is more than one external address in the address pool, PAT moves to the next address to try to allocate the original source port. This process continues until there are no more available ports or external IPv4 addresses.

Click Play in the figure to view an animation of the PAT operation. In this example, PAT has assigned the next available port (1445) to the second host address.



In the animation, the hosts have chosen the same port number of 1444. This is acceptable for the inside address, because the hosts have unique private IPv4 addresses. However, at the NAT router, the port numbers must be changed; otherwise, packets from two different hosts would exit R1 with the same source address. This example assumes that the first 420 ports in the range 1,024 - 65,535 are already in use, so the next available port number, 1445, is used.

When packets are returned from outside the network, if the source port number was previously modified by the NAT-enabled router, the destination port number will now be changed back to the original port number by the NAT-enabled router.

6.2.5

NAT and PAT Comparison

The table provides a summary of the differences between NAT and PAT.

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local addresses.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each Inside host accessing the outside network.	A single unique Inside Global address can be shared by many Inside hosts accessing the outside network.

Click each button for an example and explanation of the differences between NAT and PAT.

NAT	PAT
The figure shows a simple example of a NAT table. In this example, four hosts on the internal network are communicating to the outside network. The left column lists the addresses in the global address pool that are used by NAT to translate the Inside Local address of each host. Note the one-to-one relationship of Inside Global addresses to Inside Local addresses for each of the four hosts accessing the outside network. With NAT, an Inside Global address is needed for each host that needs to connect to the outside network.	

Note: NAT forwards the incoming return packets to the original Inside host by referring to the table and translating the Inside Global address back to the corresponding Inside Local address of the host.

Inside Global Address 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

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

209.165.200.226:1446 192.168.10.13:1444

209.165.200.226:1447 192.168.10.14:1444

209.165.200.226:1448 192.168.10.15:1444

209.165.200.226:1449 192.168.10.16:1444

209.165.200.226:1440 192.168.10.17:1444

209.165.200.226:1441 192.168.10.18:1444

209.165.200.226:1442 192.168.10.19:1444

209.165.200.226:1443 192.168.10.20:1444

209.165.200.226:1444 192.168.10.21:1444

209.165.200.226:1445 192.168.10.22:1444

209.165.200.226:1446 192.168.10.23:1444

209.165.200.226:1447 192.168.10.24:1444

209.165.200.226:1448 192.168.10.25:1444

209.165.200.226:1449 192.168.10.26:1444

209.165.200.226:1440 192.168.10.27:1444

209.165.200.226:1441 192.168.10.28:1444

209.165.200.226:1442 192.168.10.29:1444

209.165.200.226:1443 192.168.10.30:1444

209.165.200.226:1444 192.168.10.31:1444

209.165.200.226:1445 192.168.10.32:1444

209.165.200.226:1446 192.168.10.33:1444

209.165.200.226:1447 192.168.10.34:1444

209.165.200.226:1448 192.168.10.35:1444

209.165.200.226:1449 192.168.10.36:1444

209.165.200.226:1440 192.168.10.37:1444

209.165.200.226:1441 192.168.10.38:1444

209.165.200.226:1442 192.168.10.39:1444

209.165.200.226:1443 192.168.10.40:1444

209.165.200.226:1444 192.168.10.41:1444

209.165.200.226:1445 192.168.10.42:1444

209.165.200.226:1446 192.168.10.43:1444

209.165.200.226:1447 192.168.10.44:1444

209.165.200.226:1448 192.168.10.45:1444