Introduction and Lecture Overview

- This is a free, complete course for the CCNA from Jeremy's IT Lab.
- This lecture covers NAT — Network Address Translation.
- NAT is a very important topic for the CCNA exam and for real-world network engineering.
- NAT is used to translate the source and/or destination IP address of a packet to a different IP address.
- NAT is covered in exam topic 4.1, which says you must be able to configure and verify inside source NAT using static and pools.
- What will be covered in this lecture:
  - Private IPv4 addresses — IP addresses which you are free to use in your internal networks and which don't have to be globally unique.
  - An introduction to NAT and its purpose.
  - Static NAT, one type of NAT you need to know for the CCNA, and how to configure it.
- This lecture is part 1 of NAT. NAT is split into two lectures instead of one long lecture because it's an important topic that shouldn't be rushed.
- Day 45 will cover some additional NAT topics you need to know for the CCNA.
- Watch until the end of the lecture for a bonus practice question from Boson Software's ExSim, the best practice exams for the CCNA.

Private IPv4 Addresses

- This is review from the IPv6 lectures in this course, but IPv4 doesn't provide enough addresses for all devices that need an IP address in the modern world.
- The long-term solution to this problem is to switch to IPv6, but changing networks all over the world from IPv4 to IPv6 is no simple task.

- Before we switch completely over to IPv6, there are some short-term solutions to this problem, which have actually extended the lifespan of IPv4 quite a lot.
  - The first one, which you already know, is CIDR — Classless Inter-Domain Routing.
    - With CIDR, we can forget about the rigid IPv4 address classes and are free to use any prefix length with any address, no need to think about classes.
  - The other two very important solutions, which will be covered in this lecture, are private IPv4 addresses and NAT.

RFC 1918 and Private Address Ranges

- RFC 1918 specifies the following IPv4 address ranges as private.
- **Note:** 'RFC' means Request For Comments. These are the documents that are used to set standards for the Internet.
- The first private IPv4 address range is **10.0.0.0/8**, which includes **10.0.0.0 to 10.255.255.255**.
- The second one is **172.16.0.0/12**, which includes **172.16.0.0 to 172.31.255.255**.
- Finally, there is **192.168.0.0/16**, which includes **192.168.0.0 to 192.168.255.255**.
- These address ranges are recognizable because the professor uses them a lot in the course for example networks and labs.
- These ranges specify one range of addresses from class A, one range of addresses from class B, and one range of addresses from class C.

Why the Prefix Lengths Differ from Classful Expectations

- Some might be thinking: 'why is the class B range /12? Isn't class B /16? And why is the class C range /16? Isn't class C /24?'
  - The answer is that these are simply address ranges.
  - **Example:** 172.16.0.0/12 just specifies a range of addresses from 172.16.0.0 to 172.31.255.255, and you're free to divide up those addresses however you want and use them in your network.
  - **Example:** Likewise, 192.168.0.0/16 just specifies a range of addresses from 192.168.0.0 to 192.168.255.255, and once again you are free to divide up those addresses in any way you want.
- In any case, don't be too attached to the concept of address classes. In modern networks everyone uses CIDR, Classless Inter-Domain Routing, so address classes are a thing of the past.

Using Private IPv4 Addresses

- RFC 1918 specifies the following IPv4 address ranges as private:
  10.0.0.0/8 (10.0.0.0 to 10.255.255.255)
  172.16.0.0/12 (172.16.0.0 to 172.31.255.255)
  192.168.0.0/16 (192.168.0.0 to 192.168.255.255)
- You are free to use these addresses in your networks. They don't have to be globally unique.

- You are free to use these addresses in your networks, and they don't have to be globally unique.

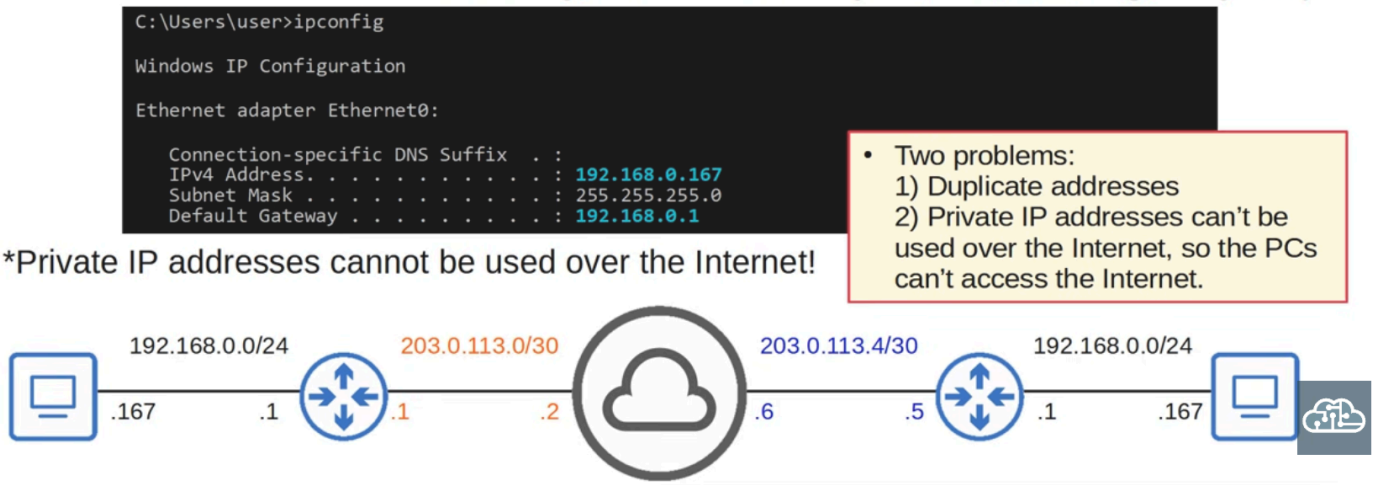
- **Example:** If you're watching this lecture from a PC in your home, it's almost certainly using a private IP address.
    - The professor's PC has the IP address 192.168.0.167, and its default gateway, the router, is 192.168.0.1.
    - Your PC might have the exact same IP address as the professor's PC, or at least it might be in the same subnet, 192.168.0.0/24.

Private IPv4 Addresses Cannot Be Used Over the Internet

- Important point: private IP addresses cannot be used over the Internet.
- Your ISP, Internet Service Provider, will drop traffic to or from private IP addresses.
- You may be wondering: if private IP addresses can't be used over the Internet, how can you access the Internet from your PC? That's where NAT comes in.

Demonstration: The Problems Without NAT

- RFC 1918 specifies the following IPv4 address ranges as private:
  10.0.0.0/8 (10.0.0.0 to 10.255.255.255)
  172.16.0.0/12 (172.16.0.0 to 172.31.255.255)
  192.168.0.0/16 (192.168.0.0 to 192.168.255.255)
- You are free to use these addresses in your networks. They don't have to be globally unique.



- **Example:** On the left is the professor's PC, 192.168.0.167, connected to the router, 192.168.0.1. Somewhere across the Internet there is another PC connected to a router, and they have the same IP addresses.

- Without NAT, there are two big problems:
  - The first problem is that there are duplicate addresses. If there is a packet traveling over the Internet with the destination address 192.168.0.167, which PC will it go to? The professor's PC? Or the other one with the same IP address?
  - The second problem is that private IP addresses can't even be used over the Internet, so the PCs can't access the Internet.

How NAT Solves Both Problems

- NAT solves both of these problems.
- **Example:** Although the PCs and the routers' internal interfaces have identical private addresses, perhaps the professor's router's external interface has the public IP address 203.0.113.1, and the other router has the public IP address 203.0.113.5.
- Important: Although the private IP addresses aren't unique, the public IP addresses must be unique.
- When the professor's PC needs to reach destinations over the Internet, NAT will allow it to borrow the unique public IP address of the router, or another public IP address configured for NAT.
- Not just the professor's PC, but all other devices in the home can use that same single public IP address to access the Internet, all at the same time.
- So the professor's PC can borrow the router's IP address and communicate over the Internet using 203.0.113.1, and the other PC can communicate over the Internet using 203.0.113.5.
- NAT will be explained next.

Key Points to Remember About Private IPv4 Addresses

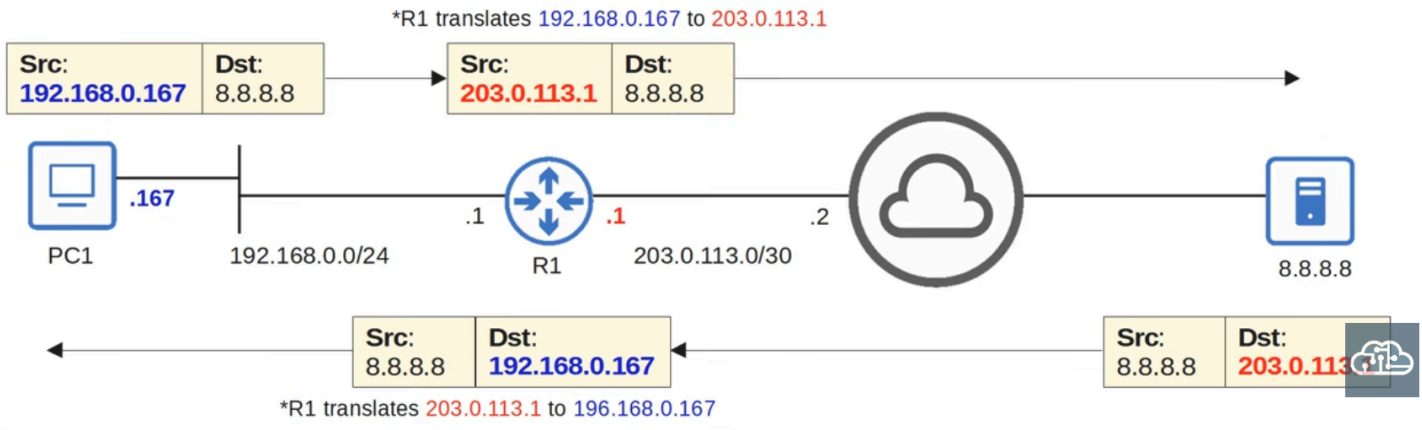
- Remember the RFC number: 1918.
- Remember the three private IP address ranges.
- Remember that they can't be used over the Internet.

Introduction to NAT

- NAT is used to modify the source and/or destination IP addresses of packets.

- There are various reasons to use NAT, but the most common reason is to allow hosts with private IP addresses to communicate with other hosts over the Internet.
- This is in addition to allowing multiple internal hosts to share a single public IP address, but the professor will demonstrate how that works in Day 45.
- There are also various types of NAT, but for the CCNA you have to understand source NAT and how to configure it on Cisco routers.

Source NAT Demonstration



- **Example:** PC1's IP address is 192.168.0.167, and it wants to communicate with the server at 8.8.8.8.
    - PC1 creates a packet with source IP 192.168.0.167 and destination 8.8.8.8.
    - PC1 sends the packet to its default gateway, R1.
    - This is where the NAT happens. R1 translates the source IP address from 192.168.0.167 to 203.0.113.1, the IP address of its external interface.
    - That's why it's called 'source' NAT, because it translates the source IP address.
    - **Note:** In this case R1 translated PC1's IP to the IP address of its own interface, 203.0.113.1, but that's only one option. There are many different kinds of NAT.
    - **Note:** The professor will cover this type of NAT, where the router's interface IP address is used, in the next lecture, Day 45.
    - Static NAT, which will be covered in this lecture, doesn't use the router's IP address; it uses a separate address.
    - R1 then sends the packet out to the Internet and it arrives at its destination, 8.8.8.8.
    - The server sends a reply. The source is 8.8.8.8, and the destination is 203.0.113.1.
    - The s]
    - erver sends the packet to R1, which then reverses the translation. 203.0.113.1 is translated ba['**Note:** Although in this case the destination IP is being changed, this isn't destination NAT. R1 is just reverting the previously translated address back to PC1's actual IP address.
    - The server's response reaches PC1.

Transition to Static Source NAT

- That was a brief introduction to NAT, specifically source NAT, translating the source IP address of a packet.
- Next, the professor looks deeper into one specific kind of source NAT: static source NAT.

Static NAT

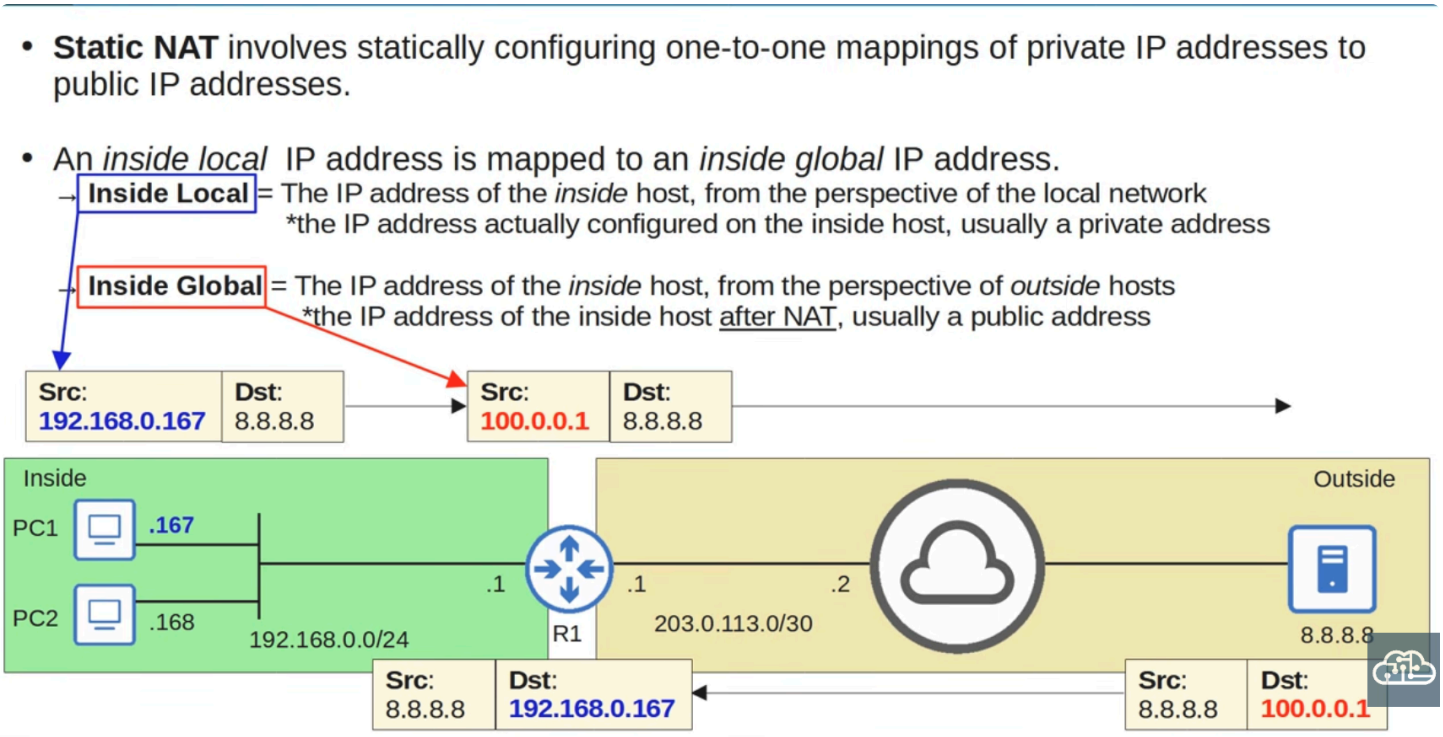
- Static NAT involves statically configuring one-to-one mappings of private IP addresses to public IP addresses.

- **Note:** It doesn't have to be private to public. You can NAT any address to any other address, but to keep things simple, think of it as mapping one private IP to one public IP.
- An inside local IP address is mapped to an inside global IP address.

Inside Local and Inside Global Addresses

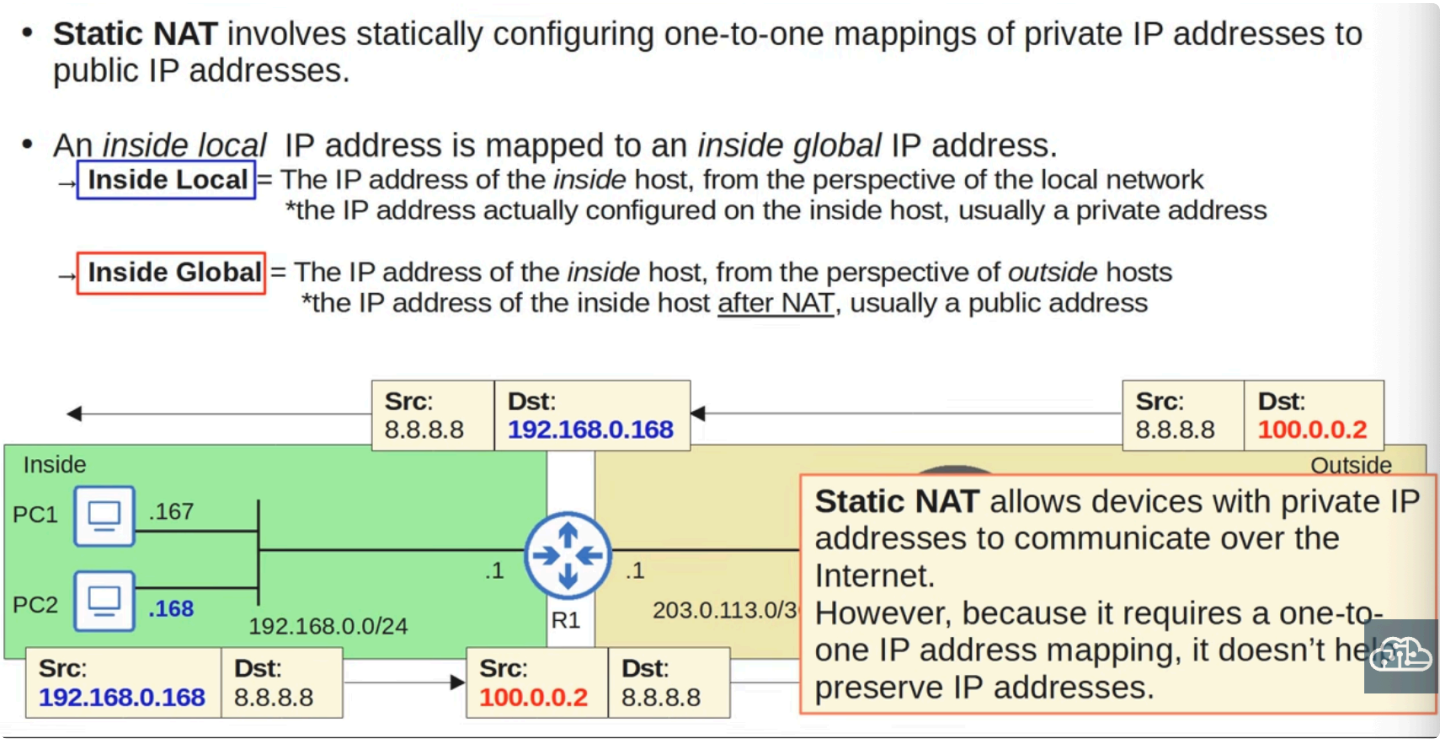
- These are two important terms to understand, not just for static NAT but for all types of NAT.
- 'Inside' refers to the router's internal network, as opposed to outside networks such as the Internet.
- **Inside local address:** The IP address of the inside host, from the perspective of the local network.
  - It's the IP address actually configured on the inside host, which is usually a private IP address.
- That 'inside local' address is translated to an **inside global address**:
  - The IP address of the inside host from the perspective of 'outside' hosts, hosts outside of the local network.
  - It's the IP address of the inside host after NAT, and is usually a public IP address.

Static NAT Demonstration



- **Example:** PC1 wants to communicate with the server at 8.8.8.8.
  - PC1 makes a packet with destination IP address 8.8.8.8 and source IP address 192.168.0.167.
  - This is the inside local address — it's the IP address actually configured on PC1, and it is indeed a private IP address.
  - PC1 sends the packet to its default gateway R1, which performs source NAT to change it to, for example, 100.0.0.1.
  - **Note:** In static NAT, R1's interface IP is not being used. 100.0.0.1 is a separate public IP address reserved just for PC1.
  - This is the inside global IP of PC1. It's PC1's IP address after NAT is performed, and it's a public IP address.
  - R1 sends the packet over the Internet to 8.8.8.8, which then sends the reply.
  - **Note:** From the server's perspective, it's communicating with IP address 100.0.0.1, even though PC1's actual IP address is 192.168.0.167.
  - So, the 'inside global' address is the IP address of the inside host, PC1, from the perspective of outside hosts, for example the server. It's not the actual IP address configured on PC1.
  - R1 reverses the translation back to PC1's inside local address and sends it to PC1.

Static NAT: PC2 Example



- **Example:** What if PC2 also wants to communicate over the Internet with 8.8.8.8?
  - Static NAT is defined as being 'one-to-one'.
  - On R1, PC1's private IP address 192.168.0.167 is mapped to the public IP address 100.0.0.1. That's a one-to-one mapping.
  - If PC2 also wants to reach 8.8.8.8, it will need its own IP address.
  - The router would not allow the professor to map both PC1 and PC2's IP addresses to 100.0.0.1 using static NAT.
  - In this case, the professor configured R1 to translate PC2's IP address, 192.168.0.168, to 100.0.0.2.
  - 192.168.0.168 is the inside local address, the actual IP address configured on PC2.
  - 100.0.0.2 is the inside global address, PC2's IP address after NAT.
  - The server sends the reply to 100.0.0.2, and R1 translates it back to 192.168.0.168 and sends the reply back to PC2.
- That's basically how static NAT works.

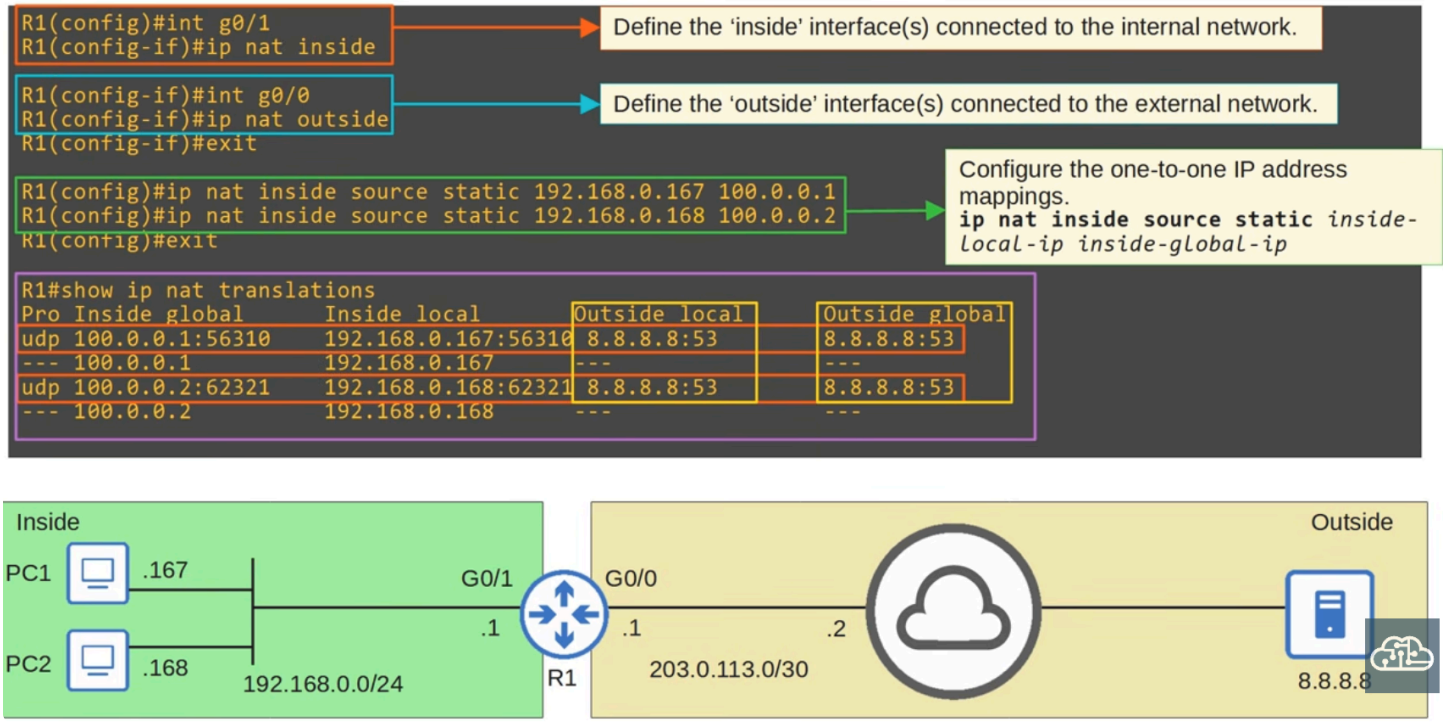
Limitations of Static NAT

- Static NAT allows devices with private IP addresses to communicate over the Internet.
- However, because it requires a one-to-one IP address mapping, it doesn't really help preserve IP addresses.
- If each internal device needs its own public IP address anyway, you might as well just configure a public IP address on the device itself.
- So, although there are reasons to use static NAT, for the professor's purposes it's not the most useful kind of NAT.

Static NAT Configuration

- Only a few commands are needed to configure static NAT.

Define the Inside and Outside Interfaces



- First, define the inside interface or interfaces by using the `ip nat inside` command from interface configuration mode.
- In this network, R1's inside interface is G0/1, connected to the internal network.

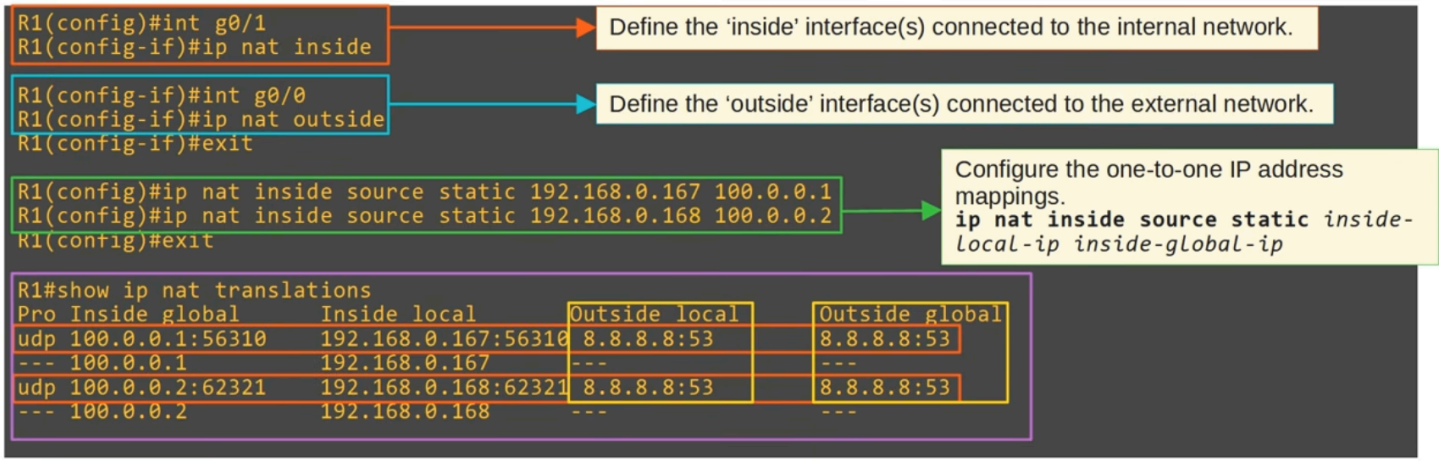
```
R1(config)# interface g0/1
R1(config-if)# ip nat inside
```

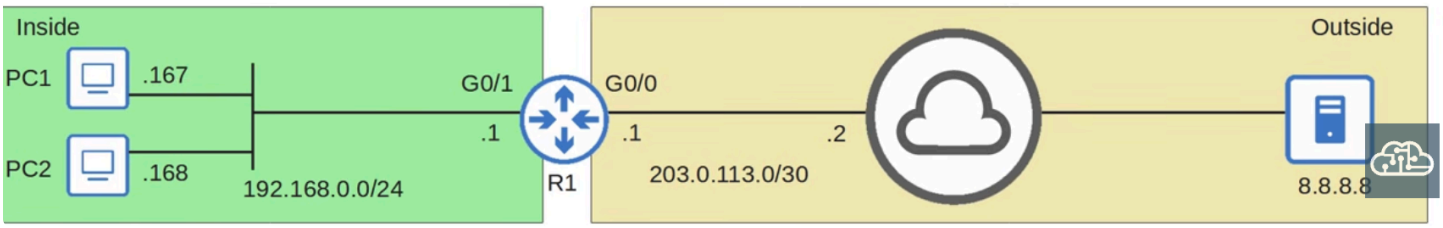
- Likewise, the professor used the `ip nat outside` command on G0/0 to define it as the outside interface.

```
R1(config)# interface g0/0
R1(config-if)# ip nat outside
```

- R1 will perform NAT on traffic traveling from the inside interface, G0/1, to the outside interface, G0/0.

Configure the One-to-One IP Address Mappings





- Then configure the one-to-one IP address mappings.

- The command is **`ip nat inside source static`**, followed by the inside local IP address and then the inside global IP address.

```
R1(config)# ip nat inside source static 192.168.0.167 100.0.0.1
R1(config)# ip nat inside source static 192.168.0.168 100.0.0.2
```

- PC1's IP address will be translated to 100.0.0.1, and PC2's will be translated to 100.0.0.2.
- **Note:** Because these are public IP addresses, to use them you have to actually own them; they must be registered to you or your company. You can't just freely use any public IP address you want, like you can with private IP addresses.

Verifying Static NAT: SHOW IP NAT TRANSLATIONS

- Finally, the professor used the command **`show ip nat translations`**. This is a very useful show command for NAT.

Verification:

```
R1# show ip nat translations
```

- Important points about the output:

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---
```

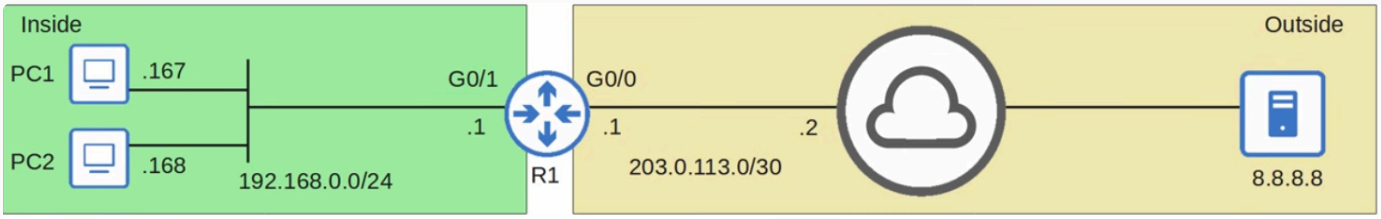
  - When static NAT is used, you will see the entries permanently displayed in the translations table.
  - Inside global is displayed first on the left, then inside local — the opposite of what the professor personally thinks it should be.
  - These two entries are permanent, but whenever NAT is actually performed on R1, when the addresses are actually translated, dynamic entries for those translations will also appear in this table.
  - **Example:** The professor sent some traffic from PC1 and PC2 to 8.8.8.8, so you can see these two dynamic entries.
- Columns from left to right:

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---
```

  - On the left is the 'Pro', protocol column, indicating that UDP was used.
  - Then the inside global address column. Notice that next to each IP address there is a colon followed by a number. What do you think that number is? It's the port number.
  - **Note:** For static NAT, you don't have to pay too much attention to the port numbers, but in Day 45 the professor will look at PAT, Port Address Translation, and you'll see the importance of these port numbers for NAT.
  - Next is the inside local address column. Notice that, even though the IP addresses have been translated, R1 doesn't translate the port numbers when using static NAT. They remain the same.

Outside Local and Outside Global

- These last two columns introduce two new terms, outside local and outside global.
- The **outside local** address is the IP address of the outside host from the perspective of the local network.



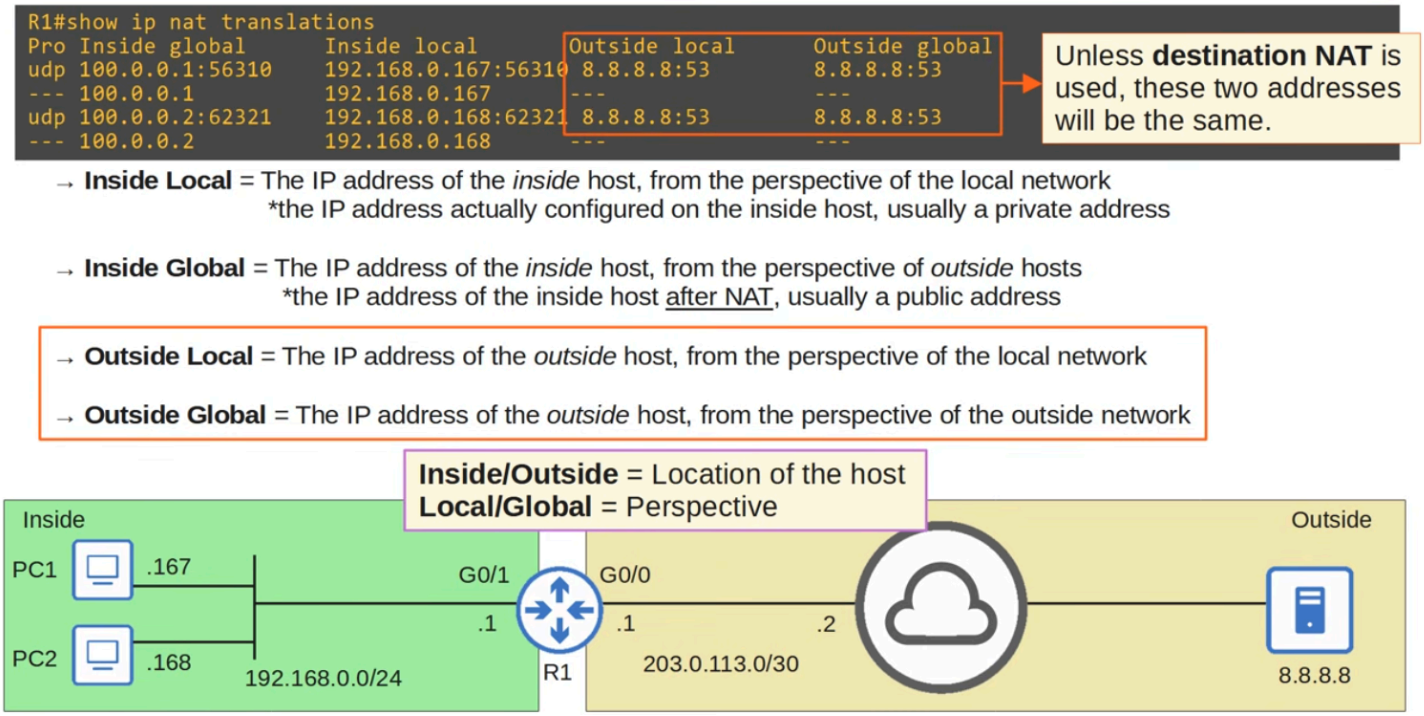
  - **Example:** From PC1's perspective, the server's IP address is 8.8.8.8, so that's the outside local IP address.
- The **outside global** address is the IP address of the outside host from the perspective of the outside network, the outside hosts.

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---
```

Unless **destination NAT** is used, these two addresses will be the same.

  - **Example:** In this case, the server's actual IP address is 8.8.8.8, so as you can see both of these are the same — the outside local address and the outside global address.
- Unless destination NAT is used, these two addresses will always be the same.
  - **Note:** Destination NAT is beyond the scope of the CCNA exam, so for the professor's purpose you can expect these two to always be the same.
- By the way, notice that the port number is also indicated for these, and they're using port 53.
- So, what service did PC1 and PC2 use to access the server? They used DNS, which uses UDP port 53, and sometimes TCP port 53.

Understanding the Four NAT Terms



- These four terms — inside local, inside global, outside local, and outside global — can be a little confusing, but make sure you understand the difference.
- 'Inside' and 'outside' indicate the location of the host, on the inside network or the outside network.
    - PC1 and PC2 are 'inside', and the server at 8.8.8.8 is 'outside'.
- Local and global, on the other hand, indicate the perspective.
    - 'Local' means from the perspective of the local, inside network.
    - 'Global' means from the perspective of the global, outside network.
    - **Example:** 192.168.0.167 is PC1's IP address from the perspective of the local network, and 100.0.0.1 is PC1's IP address from the perspective of the global network.

Clearing NAT Translations

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---

R1#clear ip nat translation *

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 100.0.0.1          192.168.0.167      ---                 ---
--- 100.0.0.2          192.168.0.168      ---                 ---
```

- You can clear all of the dynamic translations in the NAT translation table with `clear ip nat translation *`.

```
R1# clear ip nat translation *
```

- Even though the professor only configured static NAT, not dynamic NAT, each time the static NAT entries are actually used, dynamic entries are added to the NAT translation table for those translations.
- When PC1 and PC2 stop communicating with 8.8.8.8, these dynamic entries will eventually time out and be removed from the NAT translation table, but this command allows you to manually clear the table.
- Notice that, after using that command, the two dynamic entries are gone, but the static entries remain.

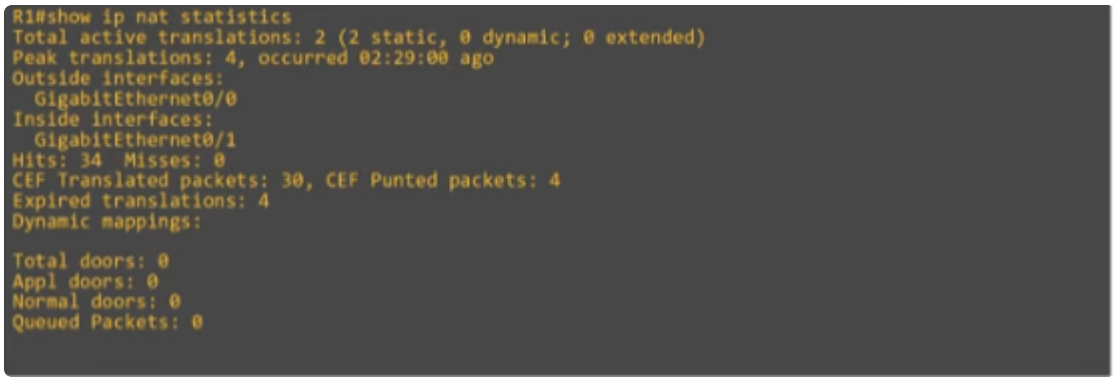
```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 100.0.0.1:56310    192.168.0.167:56310 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.1          192.168.0.167      ---                 ---
udp 100.0.0.2:62321    192.168.0.168:62321 8.8.8.8:53         8.8.8.8:53
--- 100.0.0.2          192.168.0.168      ---                 ---

R1#clear ip nat translation *

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 100.0.0.1          192.168.0.167      ---                 ---
--- 100.0.0.2          192.168.0.168      ---                 ---
```

- These static NAT entries won't time out and can't be deleted unless you remove the `ip nat inside source static` commands from the router.

Verifying Static NAT: SHOW IP NAT STATISTICS



- The last command the professor showed is `show ip nat statistics`.

Verification:

```
R1# show ip nat statistics
```

- Walkthrough of the first few lines of the output:
  - Total active translations 2, and both of them are static.
  - Since the professor just cleared the dynamic entries, there aren't any at the moment.
  - As for extended entries, the professor will explain them in Day 45.
  - Peak translations is 4 — that's the highest number of translations that have been in R1's NAT table.
  - Here you can see the outside interface, g0/0, and the inside interface, g0/1.

Command Review and Practice RecommendationNAT Commands — Quick Reference

Command	What it does
`ip nat inside`	Marks an interface as the **internal/private** side of NAT.
`ip nat outside`	Marks an interface as the **external/public** side of NAT.
`ip nat inside source static <inside-local> <inside-global>`	Creates a permanent **1-to-1 Static NAT** mapping between a private and public IP.
`show ip nat translations`	Displays the router's current **NAT translation table**.
`show ip nat statistics`	Shows NAT statistics, including inside/outside interfaces and number of translations.
`clear ip nat translation *`	Deletes **all dynamic NAT translations** from the NAT table.

- These are the new commands from this lecture.
- If you don't remember any of these commands, make sure to go back in the lecture to review.
- The professor recommends practicing these configurations either by making your own labs in Packet Tracer, or by trying the practice labs.
- The static NAT lab will be in the next lecture.

Review of Today's Lecture

- First, the professor introduced private IPv4 addresses.
  - Remember the three private IP address ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- Then the professor gave an introduction to NAT in general.
  - NAT allows routers to modify the source and/or destination addresses of packets.
  - But for the CCNA, you just need to learn source NAT.
- Then we looked at one type of source NAT: static source NAT.
  - Static source NAT involves manually configuring one-to-one mappings of private IP addresses to global IP addresses.
- Finally, we looked at how to configure static NAT.
  - Static NAT configuration is fairly simple. Just specify the inside and outside interfaces, and then configure the IP address mappings.
- The professor thinks that the bigger challenge of this lecture is understanding those four terms: inside local, inside global, outside local, and outside global.
- We'll cover NAT again in the next lecture, so if some things are unclear, don't worry about it.
