Level 8: NAPT



* If the PC @ 10.0.0.7 wants to start a connection with stackoverflow @ 151.101.1.69 either through a proxy or a transparent proxy or a NAPT translator.
  + The number of TCP connections between any PC on the subnet to stackoverflow is equal to the number of possible port numbers (65536)
  + Each new TCP connection between a PC on the subnet to a public IP address adds a new NAPT rule
  + A NAPT rule is garbage-collected either when a TCP connection is closed or the rule has not been used for a while
* However, what happens if stackoverflow @ 151.101.1.69 wants to start a connection with the PC @ 10.0.0.7? Or how to allow PC @ 10.0.0.7 to host a file server?
  + The dumbest way: have file servers on the public internet that are not behind NAPT, and upload any files to those public servers for sharing

Level 9a: P2P networking via public server

* Use one public server to hold the files between PCs behind NAPTs
* 
* How to achieve this without having the server to hold on to some files?

Level 9b: P2P networking via public proxy/relay/ TURN (Traversal Using Relays around NAPT)

* 
* What could we do if we don’t want to connect through any kind of relay server in between?

Level 9c: P2P networking via explicit NAPT rules (port forwarding)

* Why can’t two PCs talk to each other when they are both behind NAPT?
  + Their IP addresses are not meaningful on the public Internet
* Why can’t one PC connect to the NAPT on the other side?
* 
* If we add the NAPT rule to the NAPT @ 24.9.3.7 before the TCP Connection is started, then a direct TCP Connection can be established between the two PC behind NAPTs.

—----------------------------The following content was not part of the lecture—-----------------------------

There was some confusions around how the private src and public dst are set in a NAPT rule, and this is decided by the NAT implementations defined here: <https://www.rfc-editor.org/rfc/rfc3489#section-5>.

Say PC @ 10.0.0.7: 6101 starts a TCP connection to PC @ 24.9.3.7:1234 by sending a packet, the rule established would be:

* Full Cone

| private: | public : |
| --- | --- |
| src: \* : \* | src: 18.17.4.19: 2012 |
| dst: 10.0.0.7 : 6101 | dst: \* : \* |

* Restricted Cone

| private: | public : |
| --- | --- |
| src: \* : \* | src: 18.17.4.19: 2012 |
| dst: 10.0.0.7 : 6101 | dst: 24.9.3.7: \* |

* Port Restricted Cone

| private: | public : |
| --- | --- |
| src: \* : \* | src: 18.17.4.19: 2012 |
| dst: 10.0.0.7 : 6101 | dst: 24.9.3.7: 1234 |

* Symmetric

| private: | public : |
| --- | --- |
| src: 24.9.3.7: 1234 | src: 18.17.4.19: 2012 |
| dst: 10.0.0.7: 6101 | dst: 24.9.3.7: 1234 |