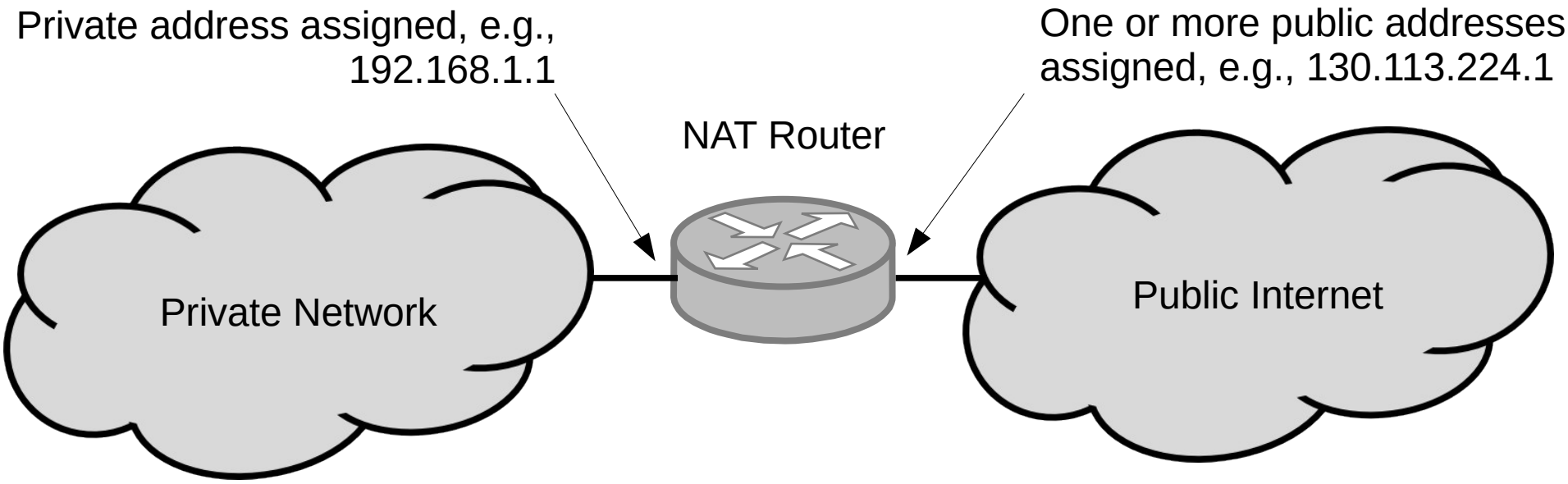
Network Address Translation (NAT)

Network Address Translation Scenario



Private address assignment, e.g., 192.168.1.0/24. Non-routable in the public Internet.

Public address assignment.

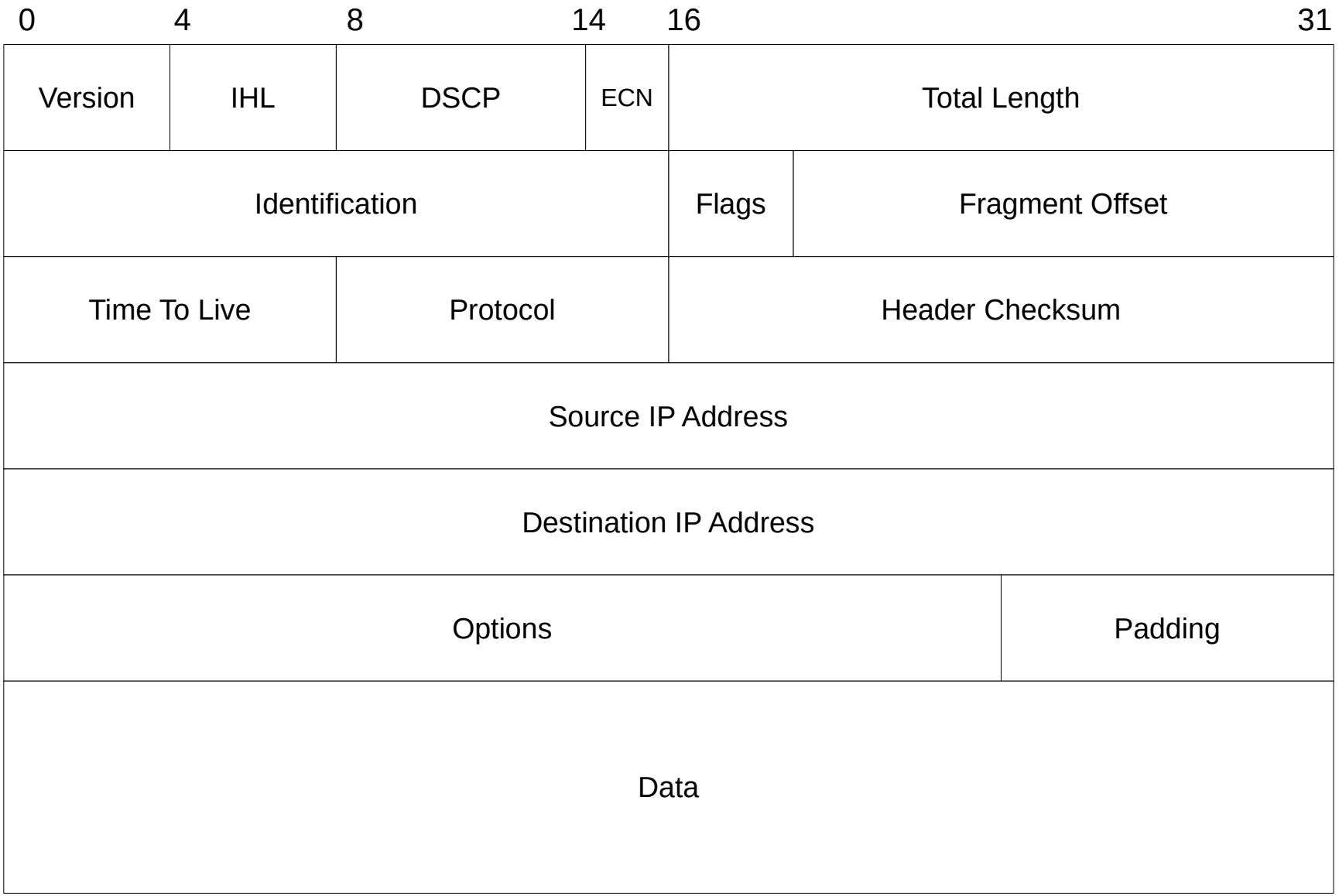
Network Address Translation (NAT)

- Is a mechanism for mitigating the depletion of IPv4 addresses. Allows hosts with private IP addresses to share public IP addresses.
- NAT is very common and often combined with firewalls. Broadband routers typically contain this functionality.
- Since translation is performed, a client can change its ISP without having to change any internal IP addresses. The translation merely has to change.
- There are two main variations:
  - Network Address Translation (NAT) (Layer 3)
  - IP Masquerading (also referred to as Network Address and Port Translation (NAPT) (Layers 3/4)

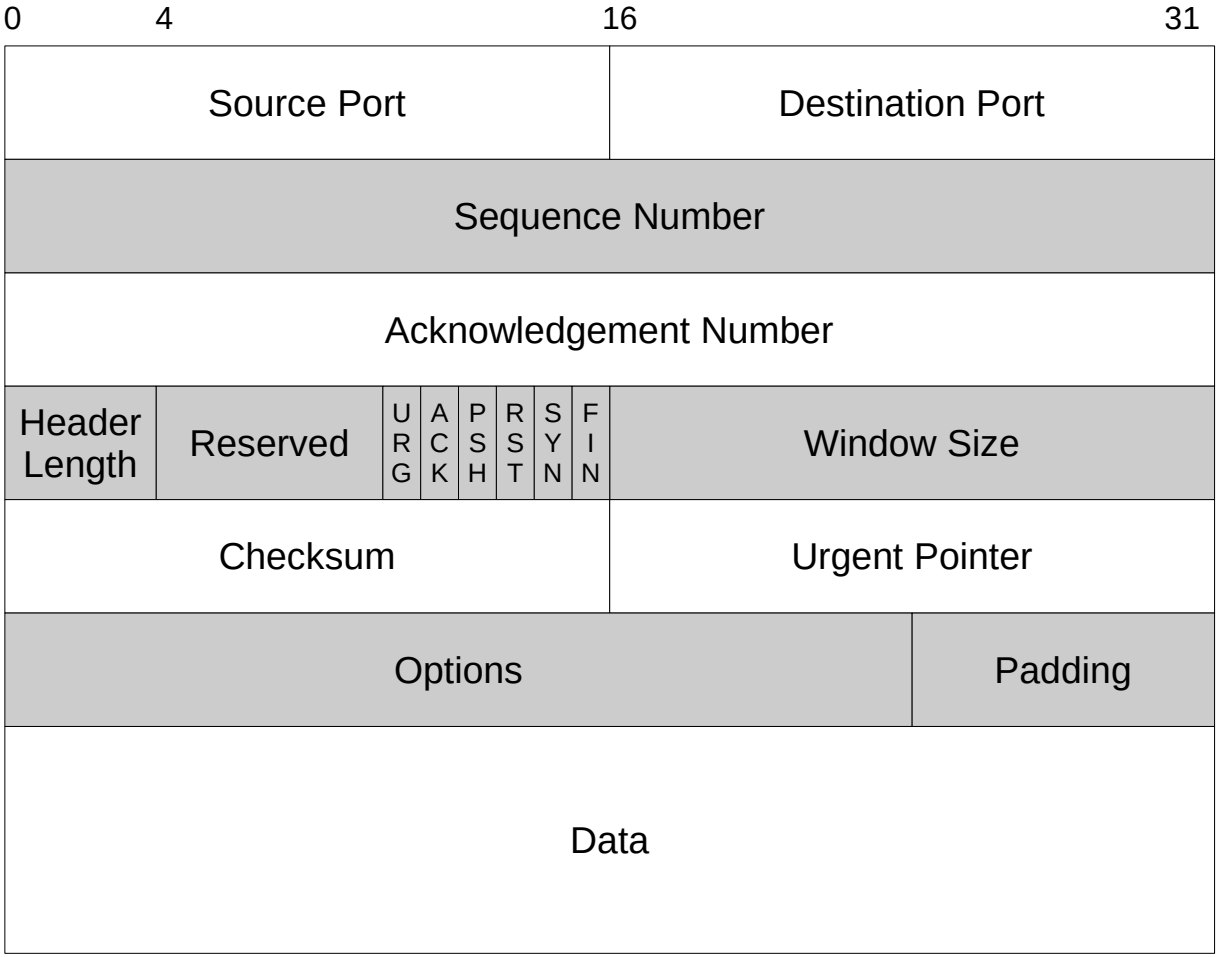
NAT and IP Masquerading

- In general NAT can be called upon to translate Npriv private addresses into Npub public addresses. There are three different situations.
  - Npriv = Npub. A fixed translation can be made between each private IP address and each public one (not a very interesting case)
  - Npriv > Npub. The translation can be dynamic with the private nodes sharing the public addresses but only Npub mappings are possible.
  - Npriv > Npub = 1. In this case all private addresses are translated into a single public address. TCP/UDP port numbers are used to identify the translation. This is referred to as Network Address and Port Translation (NAPT) or IP Masquerading.

IP (Layer 3)


0
4
8
14
16
31
Version
IHL
DSCP
ECN
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options
Padding
Data

TCP Segment Format
(Layer 4!)



NAT vs IP Masquerading

- NAT
  - A host behind the NAT router sends a packet with source address/port, (s_addr, s_port), to a public Internet destination address/port, (d_addr, d_port).
  - The NAT router is configured with a pool of public addresses that are shared by the private network hosts.
  - If this host address is not in the NAT's address translation table, the NAT router selects an unused public address from the pool, p_addr, and replaces the (s_addr, s_port) with (p_addr, s_port) in the packet. (Note that s_port in packet does not change).

NAT vs IP Masquerading

- NAT
  - The NAT router records the mapping, s_addr ↔ p_addr in its address translation table.
  - When packets arrive from the Internet, the destination address is looked up in the translation table and the reverse substitution of the destination address is made, i.e., p_addr → s_addr.
  - When subsequent packets are sourced from host s_addr, the source address is translated using the translation table entry, i.e., s_addr → p_addr.
  - NOTE: NATing does not modify higher layer (> Layer 3) packet headers, e.g., TCP or UDP.

NAT vs IP Masquerading

- NAT
  - NATing is one-to-one, i.e., one private address is mapped to one public address only. The private host holds that address until it is returned to the address pool. This is typically done using timeouts based on a lack of network activity.
  - If there are more private hosts than addresses in the public address pool, blocking may occur.
- IP Masquerading
  - This is a many-to-one address/port translation, i.e., many private hosts can share the same single public IP address.

NAT vs IP Masquerading

- IP Masquerading
  - A host behind the NAT router sends a packet with source address/port, (s_addr, s_port), to a public Internet destination address/port, (d_addr, d_port).
  - The NAT router may only have a single public address, p_addr, which is shared by all private network hosts.
  - If this host address/port is not in the router's adddress/port translation table, the NAT router replaces the (s_addr, s_port) with (p_addr, e_port) in the packet, where e_port is an arbitrarily selected (and unused) port number.
  - The remote host will respond with packets using destination address/port (p_addr, e_port).

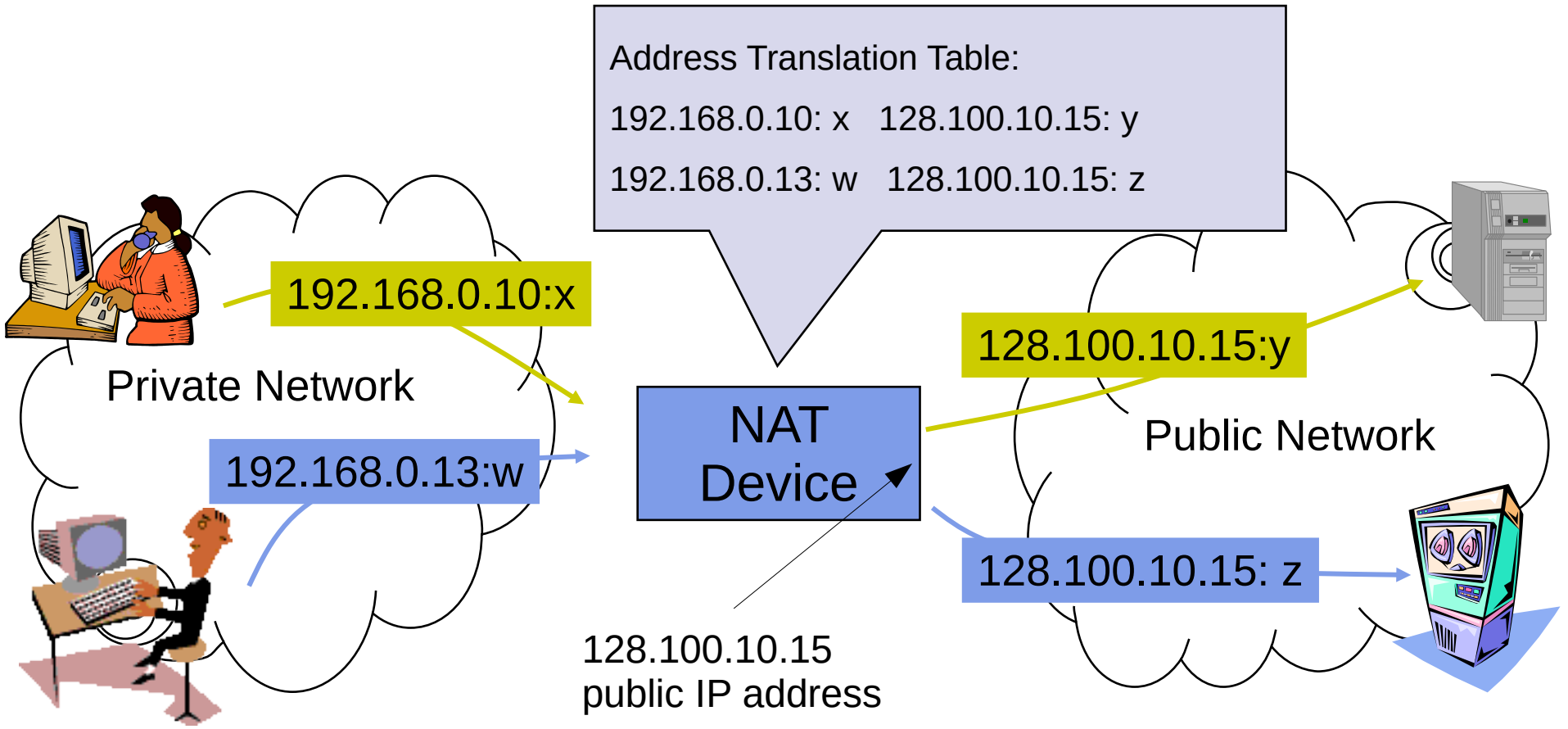
NAT vs IP Masquerading

- IP Masquerading
  - The router records the mapping, (s_addr, s_port) ↔ (p_addr, e_port), in its address/port translation table.
  - When packets arrive from the Internet, the destination address/port is looked up in the translation table and the reverse substitution of the destination address/port is made, i.e., (p_addr, e_port) → (s_addr, s_port).
  - When subsequent packets are sourced from host with (s_addr, s_port), the source address/port is translated using the translation table entry, i.e., (s_addr, s_port) → (p_addr, e_port).
  - NOTE: IP Masquerading manipulates layer 4 packet header contents, i.e., the TCP and UDP port numbers.

NAT vs IP Masquerading

- IP Masquerading
  - Uses a unique port number (e_port value, above) for each network connection sourced and there are 64K possible port numbers. It is unlikely that they will be depleted (although it has happed with certain gaming software).

NAPT Operation



- Hosts inside private networks generate packets with private IP address and TCP/UDP port numbers.
- NAT maps each private IP address and port number into shared global IP address and available port #
- Translation table allows packets to be routed unambiguously.

NAT Demonstation

Network Address Translation

- Port numbers are intended for addressing processes, not hosts.
- It is not possible to initiate contact with a host behind a NAT router. Devices are generally more secure.
- Violates end-to-end semantics since the NAT router is manipulating port numbers at layer 4.
- The proper solution is to use IPv6, which has 128-bit addresses.
- Isolates local (NATed) address assignment from public assignment, e.g., can change ISPs without local network address reassignment. Or, local addresses can be changed without external notification.

NAPT Performance Issues

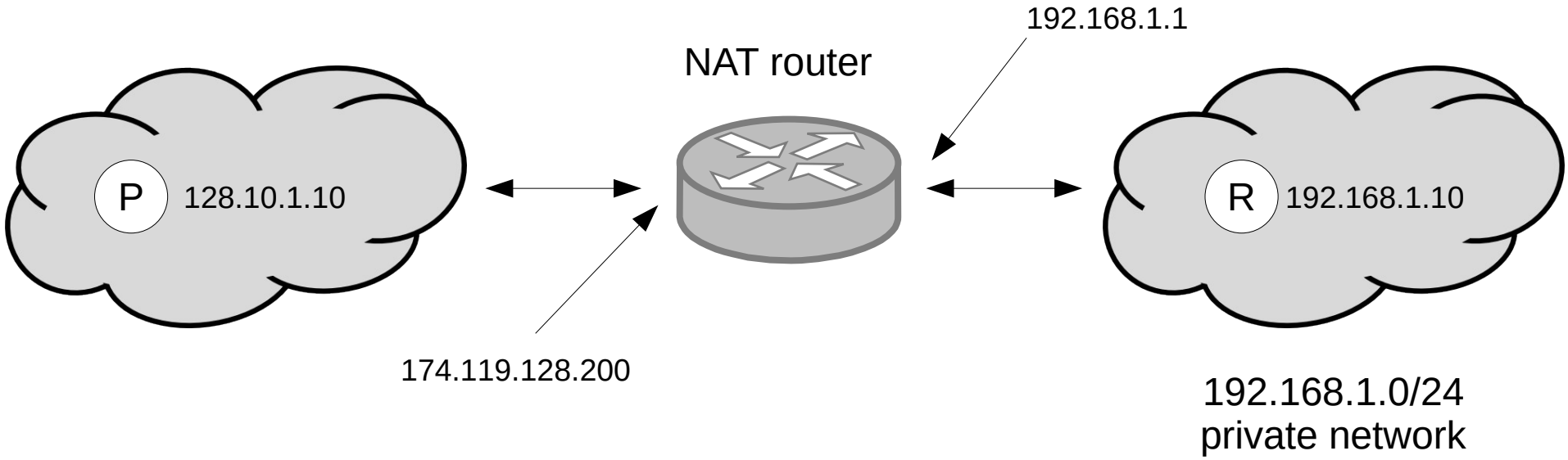
- Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
- Modifying port number requires that NAT boxes recalculate TCP checksum
- Fragmentation: Care must be taken that a datagram that is fragmented before it reaches the NAT device is not assigned a different IP address or different port numbers for each of the fragments.

NAT

- NAT destroys universal end-to-end reachability of hosts on the Internet.
- A host in the public Internet often cannot initiate communication to a host in a private network.
- The problem is worse, when two hosts that are in a private network need to communicate with each other.

NAT Traversal

- NATed hosts are inherently "client-only".
- How can an Internet host connect to a host that is behind a NATed firewall?

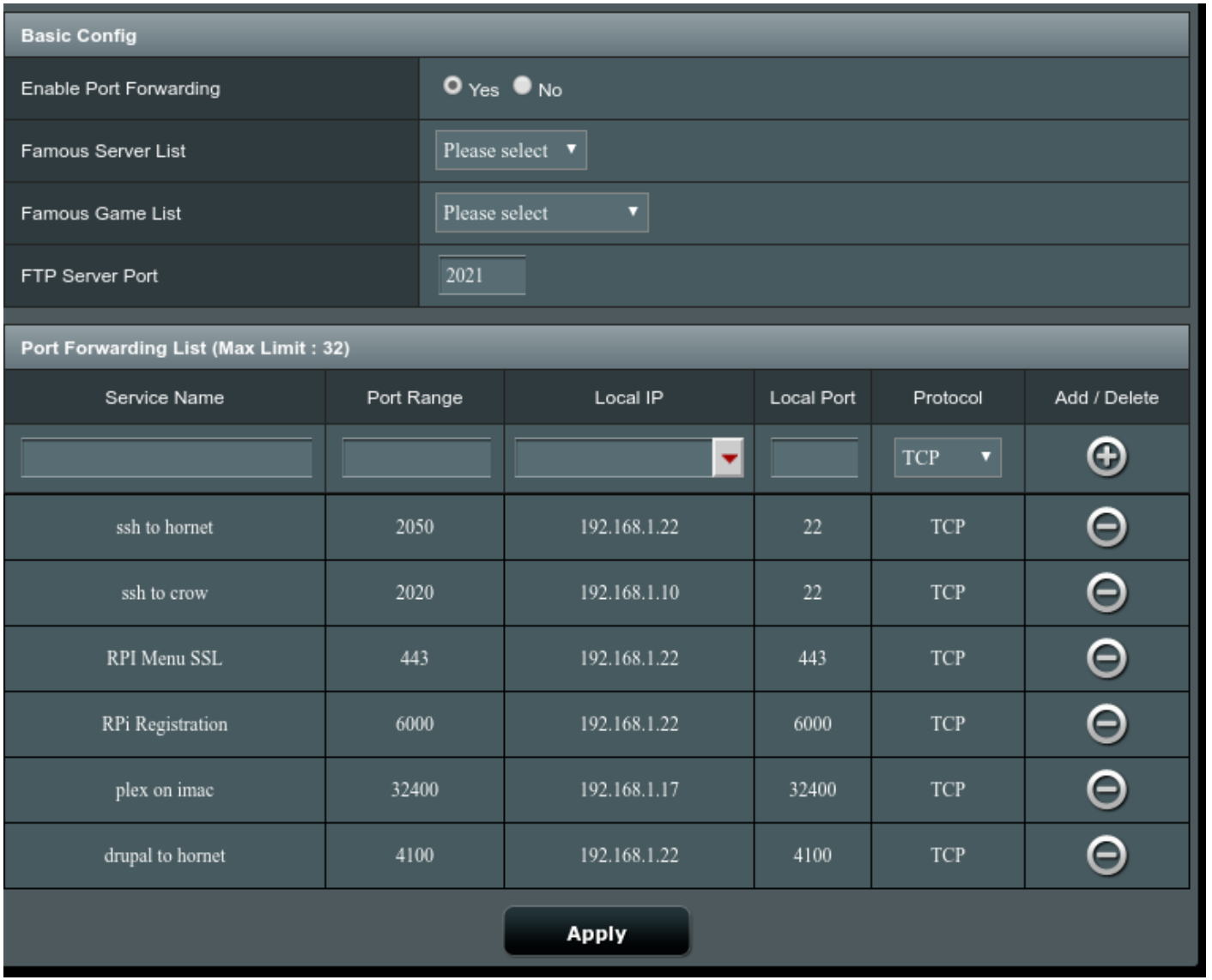


NAT Traversal

- (Some) Solutions:
  - statically configure the NAT router to forward incoming connection requests on a given port to the server/port, i.e., "Port Forwarding".
  - e.g., In the above example, if host R is running a web server on address/port (192.168.1.10, 80), the NAT could be configured so that any incoming TCP connection to address/port (174.119.128.200, 90) would be forwarded to (192.168.1.10, 80). The web server could then be accessed from a browser using the format:

    http://174.119.128.200:90/<remaining URL>

Router Port Forwarding Example



Basic Config

Enable Port Forwarding	Yes / No
Famous Server List	Please select
Famous Game List	Please select
FTP Server Port	2021

Port Forwarding List (Max Limit : 32)

Service Name	Port Range	Local IP	Local Port	Protocol	Add / Delete
				TCP	
ssh to hornet	2050	192.168.1.22	22	TCP	
ssh to crow	2020	192.168.1.10	22	TCP	
RPI Menu SSL	443	192.168.1.22	443	TCP	
RPi Registration	6000	192.168.1.22	6000	TCP	
plex on imac	32400	192.168.1.17	32400	TCP	
drupal to hornet	4100	192.168.1.22	4100	TCP	

Apply

NAT Traversal

- (Some) Solutions:
  - Use a Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. The allows a NATed host to:
    - learn public IP address
    - add/remove port mappings (with lease times). i.e., automate static NAT port map configuration
  - Host relaying
    - NATed client establishes connection to relay
    - external client connects to relay
    - relay routes packets between the two connections
    - this is used in Skype