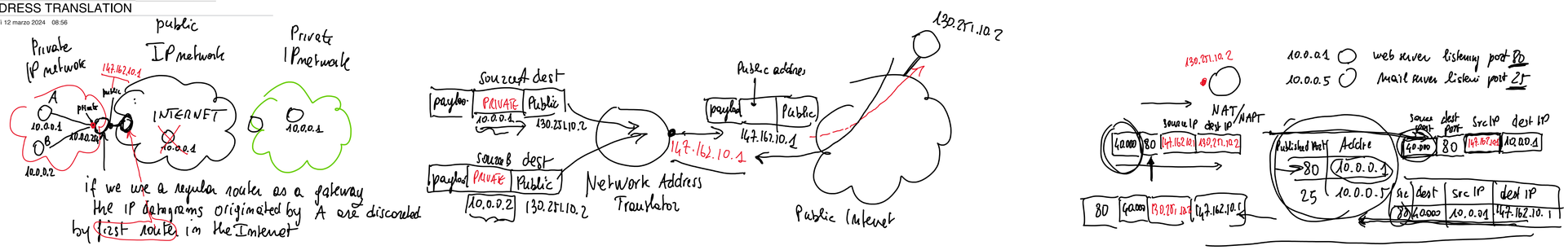
4.4 PRIVATE ADDRESSING - NETWORK ADDRESS TRANSLATION

martedì 12 marzo 2024 08:56



Hosts within enterprises that use IP can be partitioned into three categories:

Category 1: hosts that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 2: hosts that need access to a limited set of outside services (e.g., E-mail, FTP, netnews, remote login) which can be handled by mediating gateways (e.g., application layer gateways). For many hosts in this category an unrestricted external access (provided

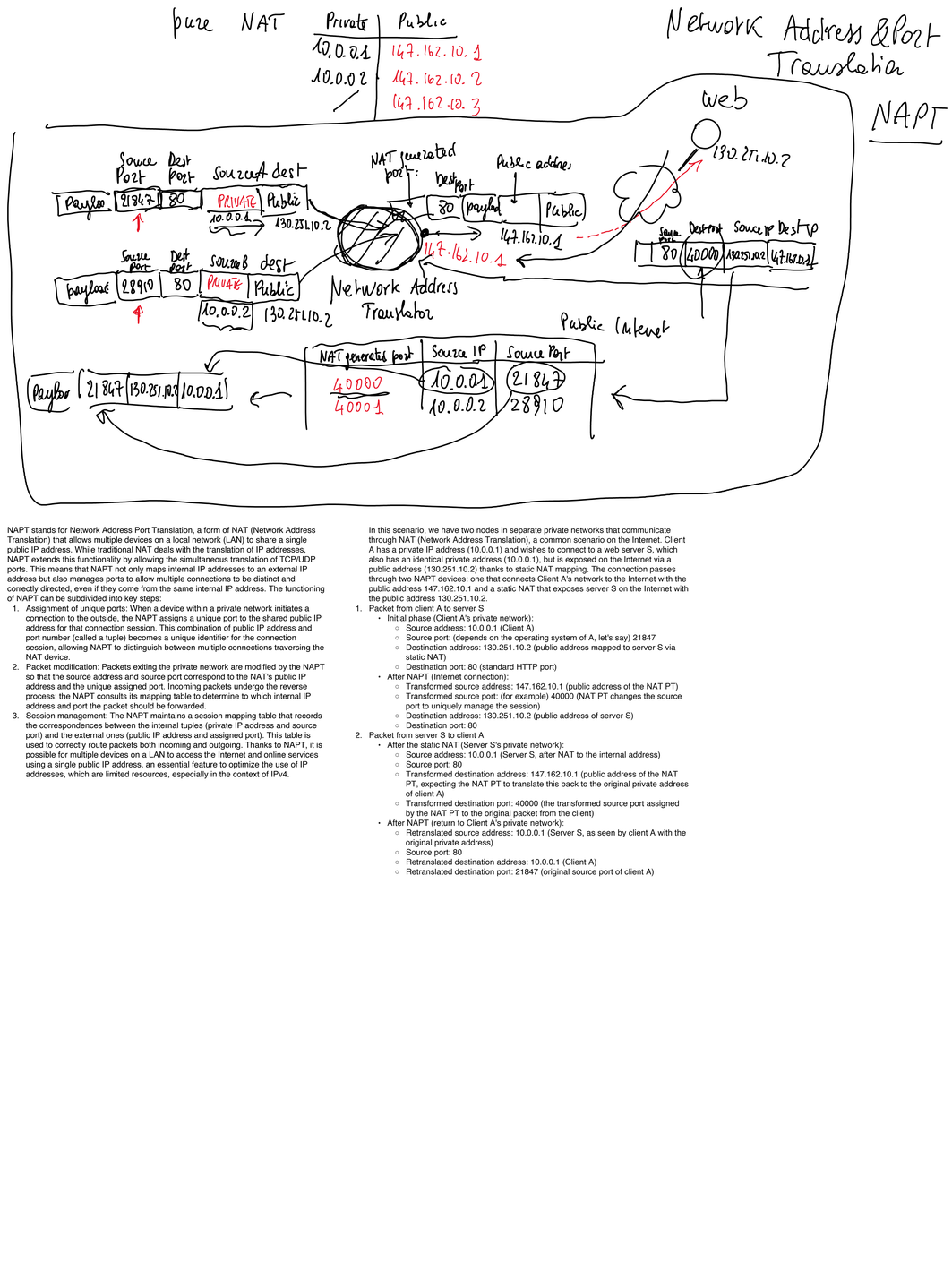
undesirable for privacy/security reasons. Just like hosts within the first category, such hosts may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 3: hosts that need network layer access outside the enterprise (provided via IP connectivity); hosts in the last category require IP addresses that are globally unambiguous.

From <https://www.rfc-editor.org/rfc/rfc1918>

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255 (10/8 prefix)
172.16.0.0	-	172.31.255.255 (172.16/12 prefix)
192.168.0.0	-	192.168.255.255 (192.168/16 prefix)



NAPT stands for Network Address Port Translation, a form of NAT (Network Address Translation) that allows multiple devices on a local network (LAN) to share a single public IP address. While traditional NAT deals with the translation of IP addresses, NAPT extends this functionality by allowing the simultaneous translation of TCP/UDP ports. This means that NAPT not only maps internal IP addresses to an external IP address but also manages ports to allow multiple connections to be distinct and correctly directed, even if they come from the same internal IP address. The functioning of NAPT can be subdivided into key steps:

1. Assignment of unique ports: When a device within a private network initiates a connection to the outside, the NAPT assigns a unique port to the shared public IP address for that connection session. This combination of public IP address and port number (called a tuple) becomes a unique identifier for the connection session, allowing NAPT to distinguish between multiple connections traversing the NAT device.
2. Packet modification: Packets exiting the private network are modified by the NAPT so that the source address and source port correspond to the NAT's public IP address and the unique assigned port. Incoming packets undergo the reverse process: the NAPT consults its mapping table to determine to which internal IP address and port the packet should be forwarded.
3. Session management: The NAPT maintains a session mapping table that records the correspondences between the internal tuples (private IP address and source port) and the external ones (public IP address and assigned port). This table is used to correctly route packets both incoming and outgoing. Thanks to NAPT, it is possible for multiple devices on a LAN to access the Internet and online services using a single public IP address, an essential feature to optimize the use of IP addresses, which are limited resources, especially in the context of IPv4.

In this scenario, we have two nodes in separate private networks that communicate through NAT (Network Address Translation), a common scenario on the Internet. Client A has a private IP address (10.0.0.1) and wishes to connect to a web server S, which also has an identical private address (10.0.0.1), but is exposed on the Internet via a public address (130.251.10.2) thanks to static NAT mapping. The connection passes through two NAPT devices: one that connects Client A's network to the Internet with the public address 147.162.10.1 and a static NAT that exposes server S on the Internet with the public address 130.251.10.2.

1. Packet from client A to server S
   - Initial phase (Client A's private network):
     - Source address: 10.0.0.1 (Client A)
     - Source port: (depends on the operating system of A, let's say) 21847
     - Destination address: 130.251.10.2 (public address mapped to server S via static NAT)
     - Destination port: 80 (standard HTTP port)
   - After NAPT (Internet connection):
     - Transformed source address: 147.162.10.1 (public address of the NAT PT)
     - Transformed source port: (for example) 40000 (NAT PT changes the source port to uniquely manage the session)
     - Destination address: 130.251.10.2 (public address of server S)
     - Destination port: 80
2. Packet from server S to client A
   - After the static NAT (Server S's private network):
     - Source address: 10.0.0.1 (Server S, after NAT to the internal address)
     - Source port: 80
     - Transformed destination address: 147.162.10.1 (public address of the NAT PT, expecting the NAT PT to translate this back to the original private address of client A)
     - Transformed destination port: 40000 (the transformed source port assigned by the NAT PT to the original packet from the client)
   - After NAPT (return to Client A's private network):
     - Retranslated source address: 10.0.0.1 (Server S, as seen by client A with the original private address)
     - Source port: 80
     - Retranslated destination address: 10.0.0.1 (Client A)
     - Retranslated destination port: 21847 (original source port of client A)