DevOps School

Lesson 06. Networks. IP-Addressing. IP-Networks

By Yuriy Bezgachnyuk, November 2021

softserve

AGENDA

- IP-Addressing
  - IPv4
- Tools
- IP-Networks
  - NAT
  - VPN

softserve

ADDRESSING

softserve

IP ADDRESS

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1998
Address Size	**32-bit** number	**128-bit** number
Address Format	Dotted **Decimal** Notation: **192.149.252.76**	**Hexadecimal** Notation: **3FFE:F200:0234:AB00: 0123:4567:8901:ABCD**
Profix Notation	**192.149.0.0/24**	**3FFE:F200:0234::/48**
Number of Addresses	2^{32} ~ 4 294 967 296	2^{128} ~ 340 282 366 920 938 463 374 607 431 768 211 456

softserve

IPv4

- IP-Address – unique logical address of 3rd level
  - Contained at the header of **IP-package** and identify the following:
    - Sender – Source Address (32)
    - Receiver – Destination Address (32)
- IPv4 length – 32 bits
- Form: decimal format with dots by octets 4 octets

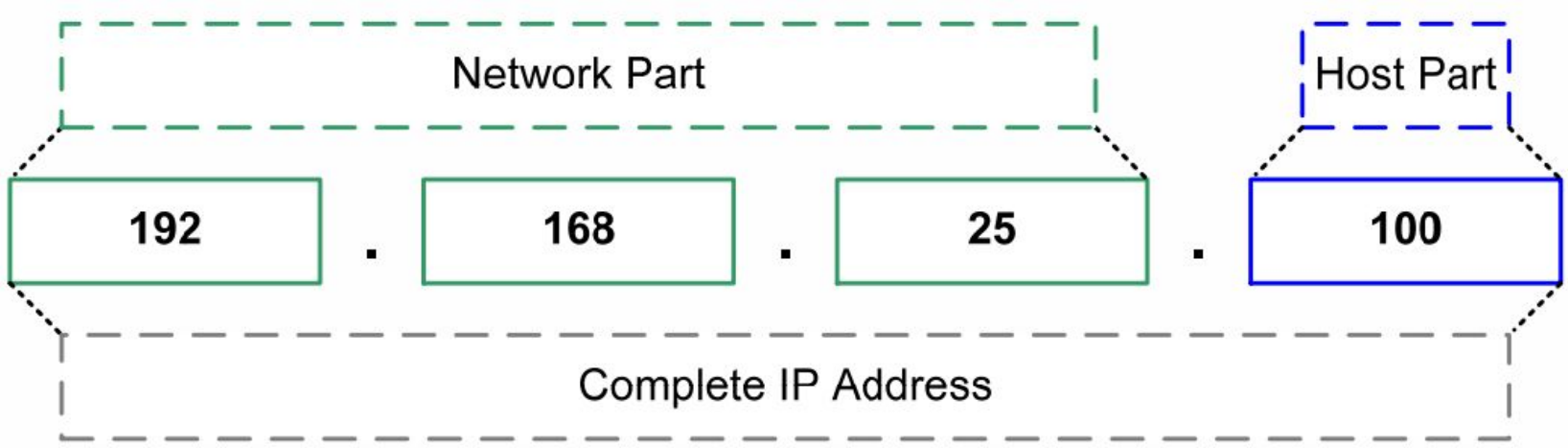
Format	IPv4 Address presentation	Size
Binary	11000000101010000001100101100100	32 bits
Binary	11000000 . 10101000 . 00011001 . 01100100	4x8 bits
Decimal Dotted	192 . 168 . 25 . 100	4x8 bits

softserve

IPv4 components

- Network part of address – **high** bits
  - **P** – the number of bits
  - Define the maximum number of networks
- The part of device address (Host Part) – **lower** bits
  - **N** – the number of bits
  - Define the maximum number of hosts in the network

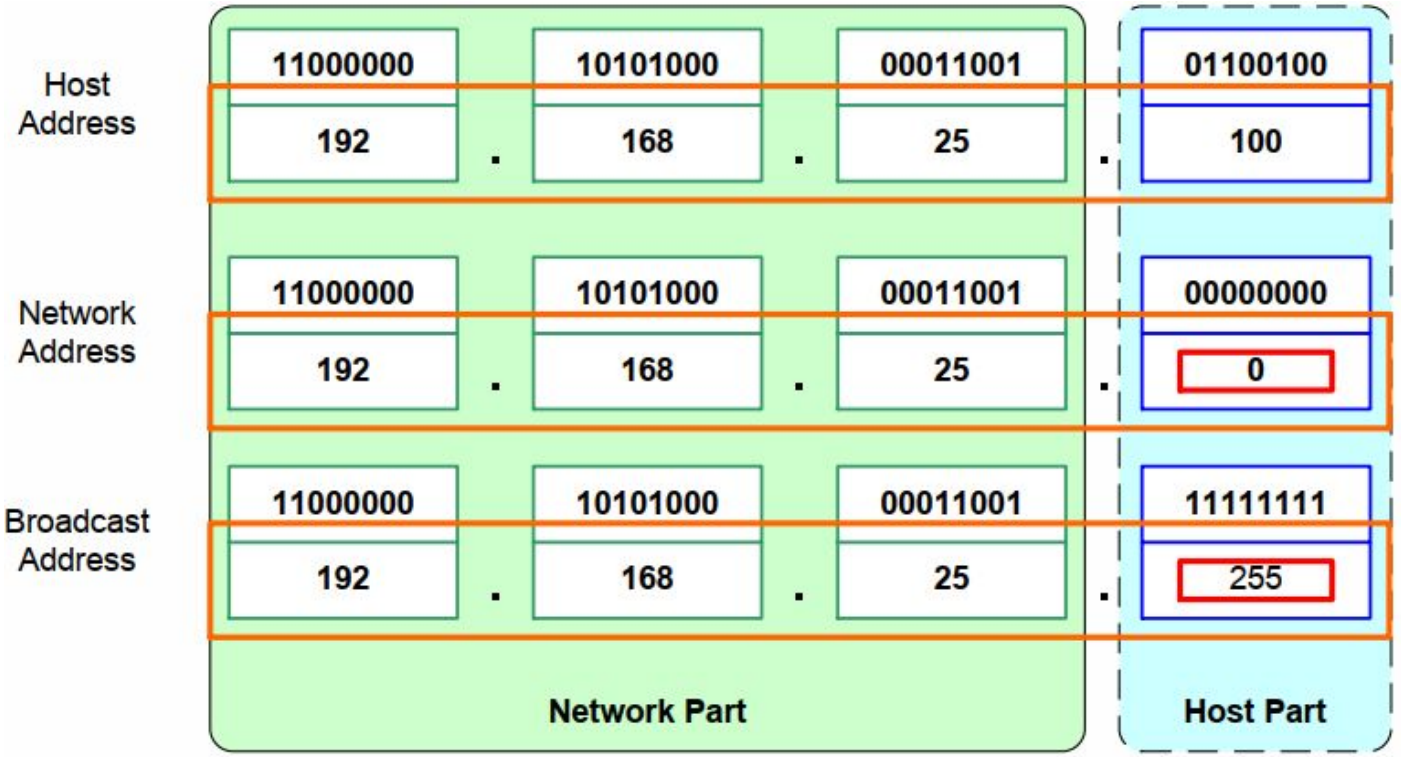
$$P + N = 32$$



softserve

IPv4 Address types

- **Host Address**
  - unambiguously identify **one** network **device** (*192.168.25.[1-254]*)
- **Network Address**
  - Identify all **subnet**
  - All bits of the Host part are **zero**
  - Using for routing (*192.168.25.0*)
- **Broadcast Address**
  - Specify **all devices** on a subnet
  - All Host part bits are **one**
  - Used to broadcast to all devices on the same network (*192.168.25.255*)



softserve

PREFIX

- **PREFIX** Length – number of bits of network part of whole address

$$N = 32 - PREFIX\_Length$$

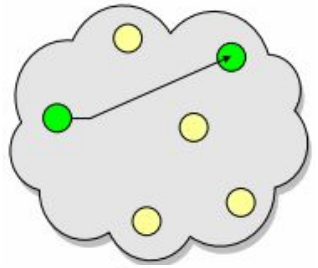
- Unambiguously identify:
  - Maximum number of devices in the network $2^N - 2$
  - Maximum number of networks (current level) 2^{Prefix_Length}
  - Addresses
    - Network
    - Broadcast

PREFIXES

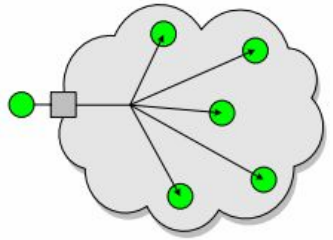
Names	Network + Prefix Length	Addresses	Number of Hosts in Network
Network	192.168.25.0/24	192.168.25.0 11000000.10101000.00011001.00000000	254
Host		192.168.25.1 11000000.10101000.00011001.00000001 ... 192.168.25.254 11000000.10101000.00011001.11111110	
Broadcast		192.168.25.255 11000000.10101000.00011001.11111111	
Network	192.168.25.0/25	192.168.25.0 11000000.10101000.00011001.00000000	126
Host		192.168.25.1 11000000.10101000.00011001.00000001 ... 192.168.25.126 11000000.10101000.00011001.01111110	
Broadcast		192.168.25.127 11000000.10101000.00011001.01111111	

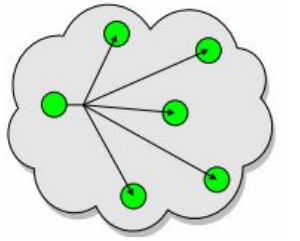
TYPE OF TRANSMISSION

- **Unicast** – individual transmission
  - Addressed to a single device (**the only one**)



- **Broadcast**
  - Addressed to **all** devices
    - Directed Broadcast – in remote subnet
    - Limited Broadcast – in local subnet

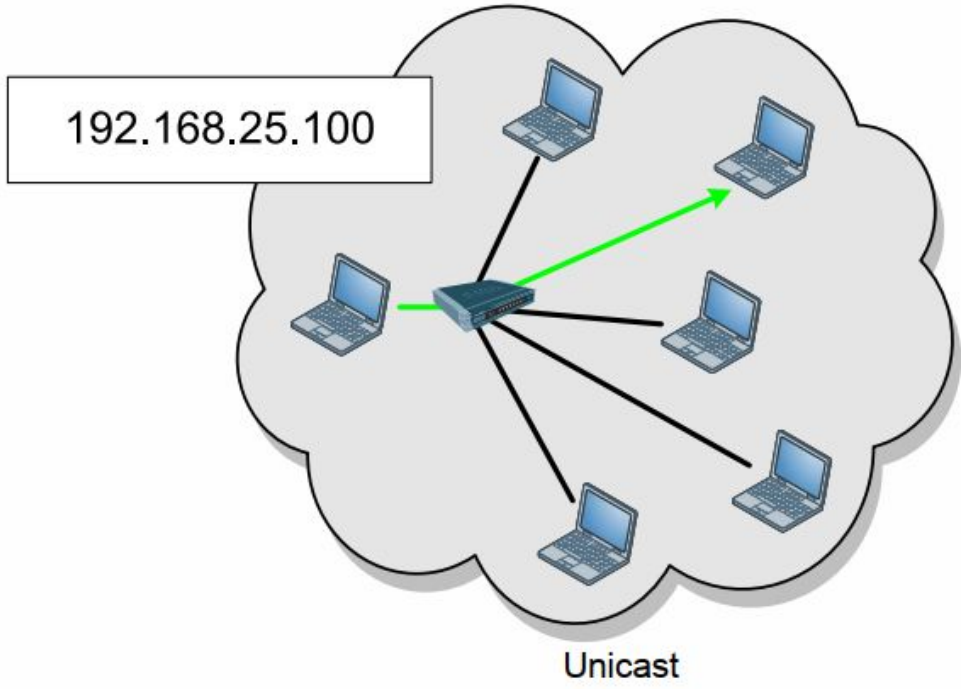




- **Multicast**
  - The sender sends data to a **group** of addresses (several)

UNICAST

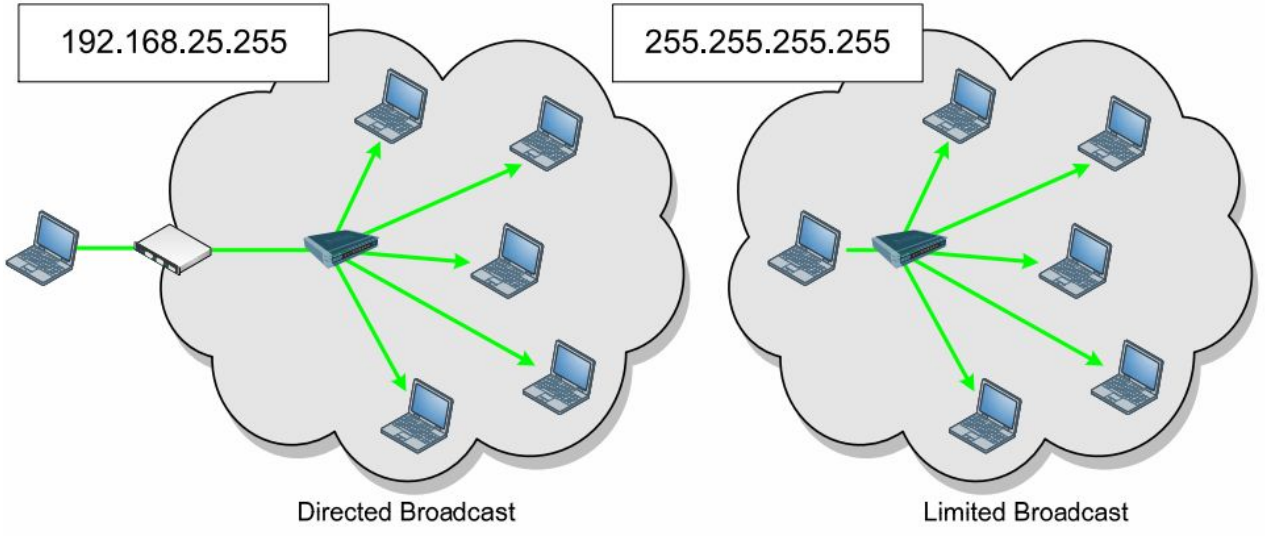
- Addressee:
  - One – separate device
  - Defined in the filed of IPv4 header (device)
    - Destination Address – logical address of the device



softserve

BROADCAST

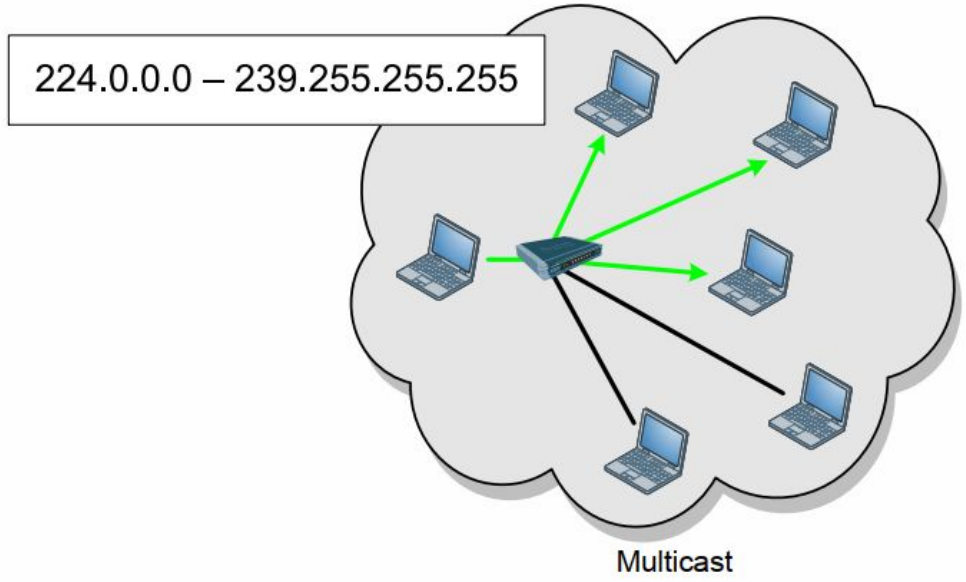
- Addressee
  - All devices in defined subnet
    - Local LAN (Limited Broadcast)
    - Remote LAN (Directed Broadcast)
  - Defined in the field of IPv4 header (subnet):
    - Destination Address – broadcast address of subnet



softserve

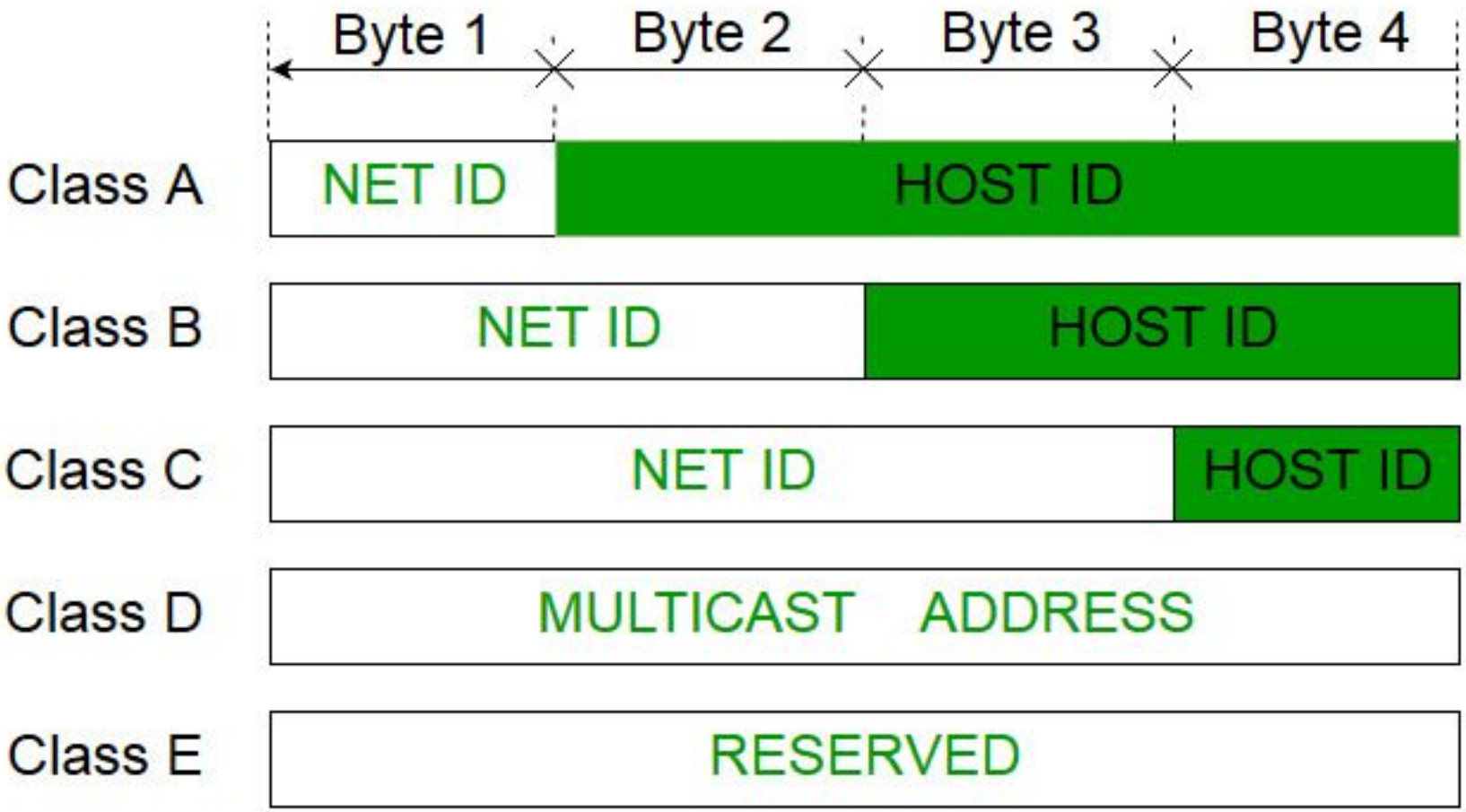
MULTICAST

- Addressee:
  - Selected group of devices
  - Defined in the filed of IPv4 header
    - Destination Address – separate reserved group



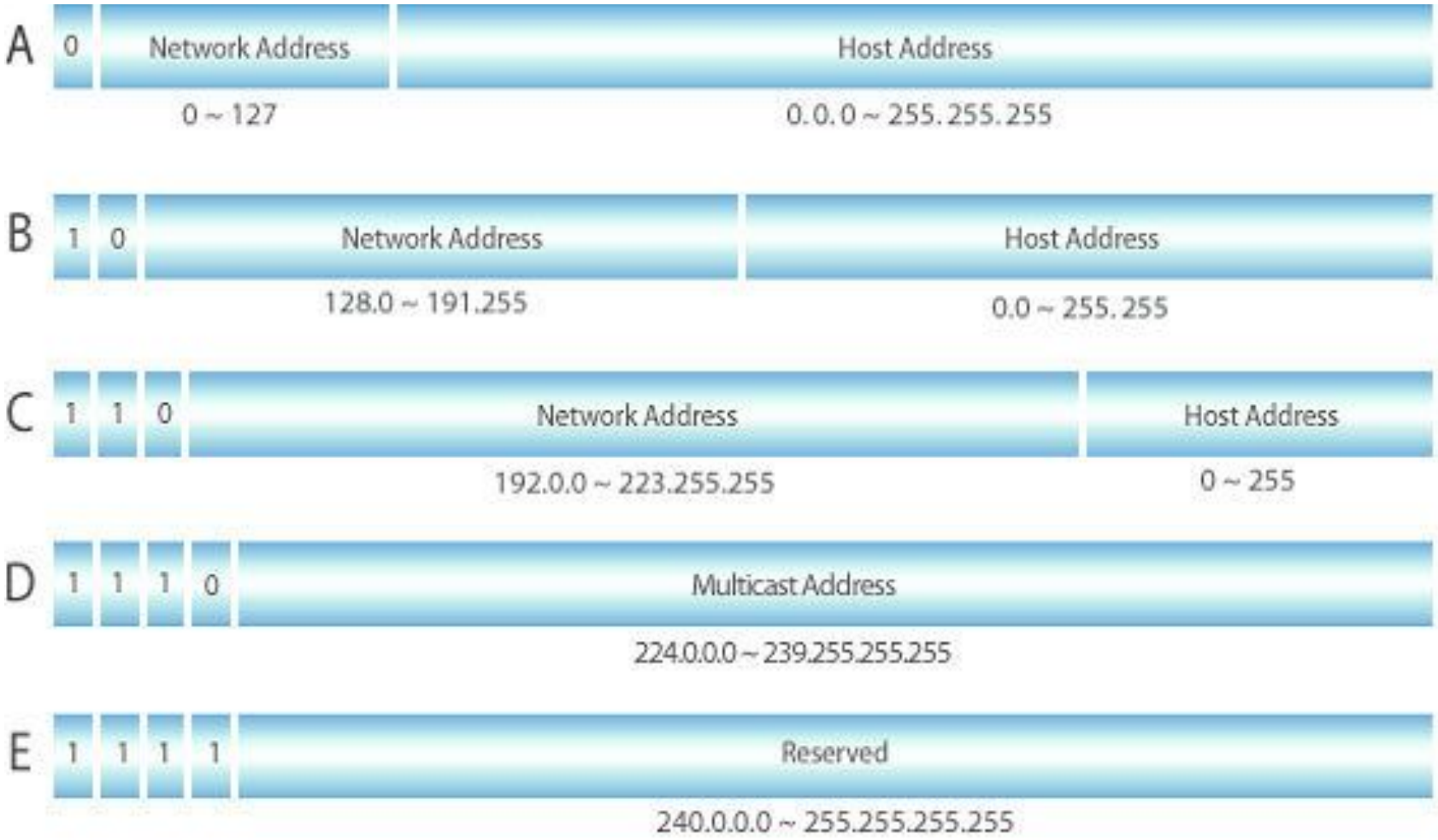
softserve

IPv4 Host Addresses



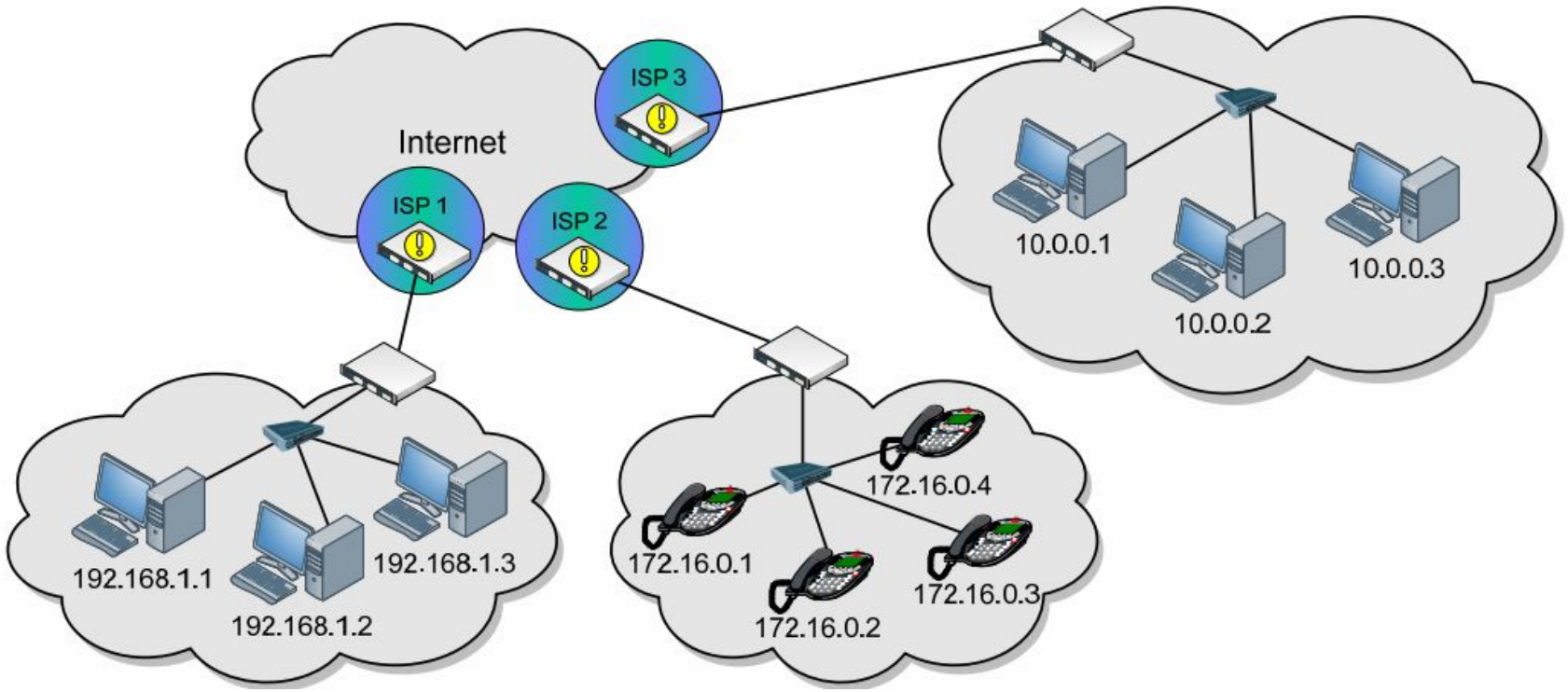
softserve

IPv4 Host Addresses



softserve

IPv4 Host Addresses



- Private
  - Class A: 10.0.0.0/8
  - Class B: 172.16.0.0/12
  - Class C: 192.168.0.0/16

softserve

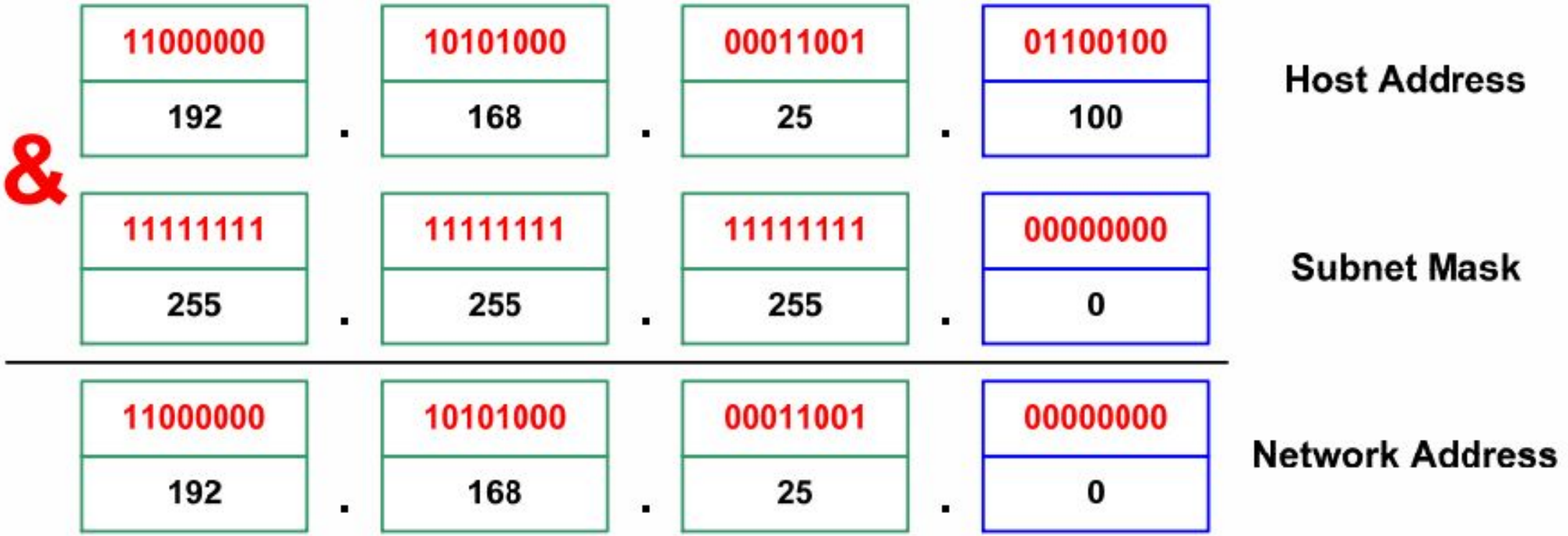
SPECIAL ADDRESSES

- Network Addresses
- Broadcast Addresses
- Default Route
  - 0.0.0.0
  - Reserved: 0.0.0.0/8
- Loopback Address
  - 127.0.0.1
  - Reserved: 127.0.0.0/8
- Link-Local Addresses
  - 169.254.0.0/16
- TEST-NET Addresses
  - 192.0.2.0/24

SUBNET MASK

- **Subnet mask** – 32-bit number which show range of IP-addresses that located in one subnet
  - 1 – subnet bits (inseparable, from left to right)
  - 0 – device bits (inseparable, from right to left)
- A **subnet mask** is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s.
- In this way, the subnet mask separates the IP address into the network and host addresses.

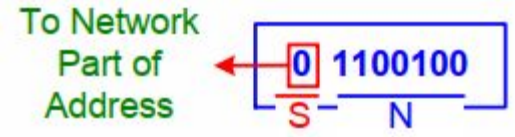
SUBNET MASK

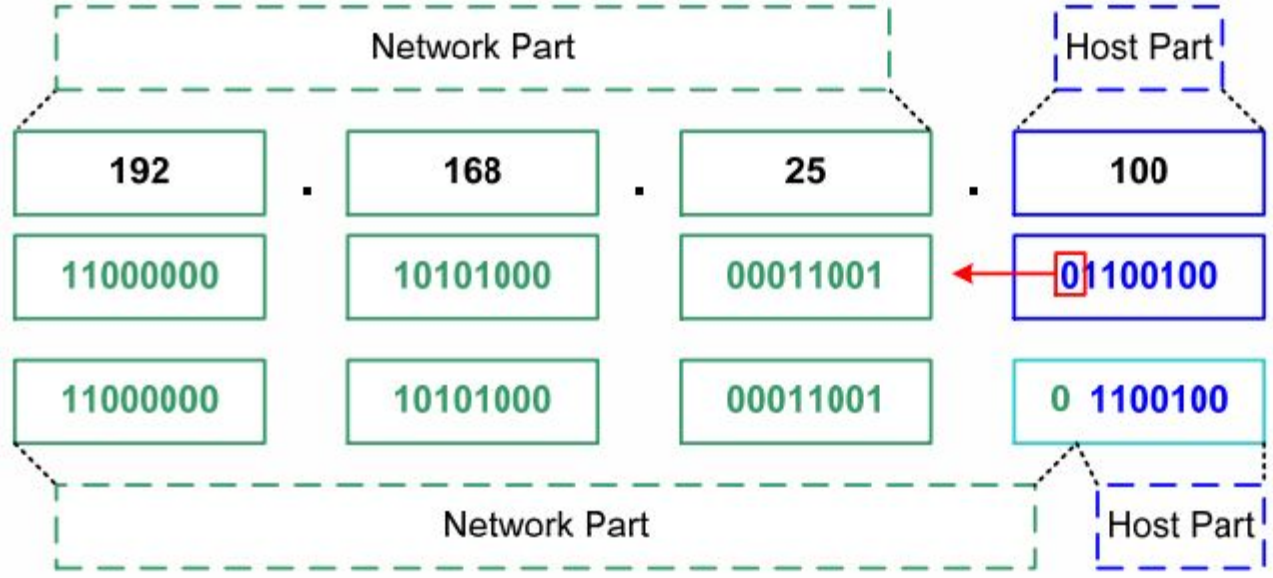


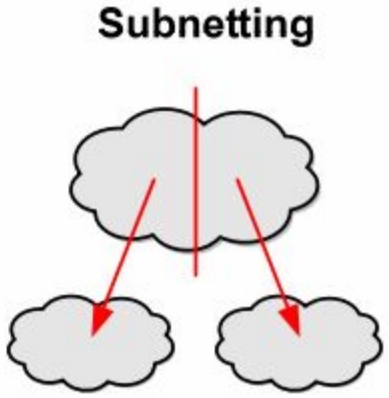
softserve

SUBNETTING

- Subnetting (dividing on subnets) – creating logical subnets from one block of addresses (network)
  - Borrowing bits into the network part of the address (S bit)
  - Number of subnets 2^s
  - Maximum number of devices in the network $2^N - 2$



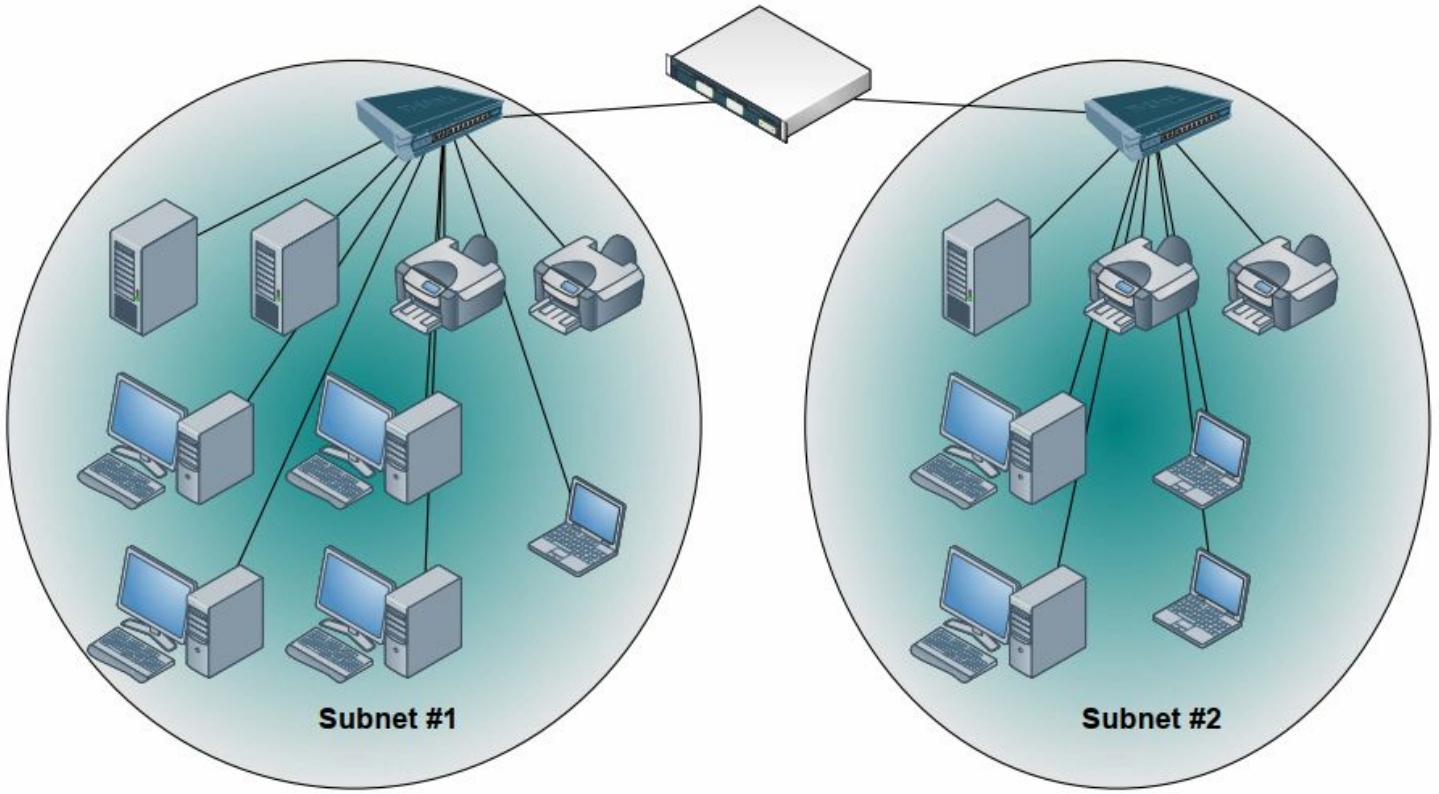




softserve

SUBNETTING

- Advantages
  - Simplified management
  - Simplification of addressing
  - Simplification of routing
  - Minimizing network load (traffic localization)
- Criteria
  - Geographic location
  - Appointment
  - Responsibility (property)



softserve

IPv6

- An IPv6 protocol address consists of 128 bits
  - `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`
  - each letter x is a hexadecimal digit representing 4 bits
- Part of the bits on the left (depending on the prefix) indicate the network, the remaining bits on the right identify the device
- IPv6 does not use subnet masks as they would be very long, instead a **prefix** is used
- The `/64` prefix means the first 64 is the network and the rest is the host.

IPv6

- To shorten an address, rules must be applied in succession.

  `2001:0DB0:0000:123A:0000:0000:0000:0030`

- Leading zeros are removed;
- If the hextet consists of only zeros, then it is replaced by one zero

  `2001:DB0:0:123A:0:0:0:30`

- One longest group is selected, consisting of completely zero hextetsthe longest sequence is `":0:0:0:"` and is replaced by two colons `"::"`

  `2001:DB0:0:123A::30`

softserve

IPv6. Loopback

- Used to send a packet to itself

  `127.0.0.1`

- There is only one cyclic address

  `0000:0000:0000:0000:0000:0000:0000:0001`

- short version

  `::1`

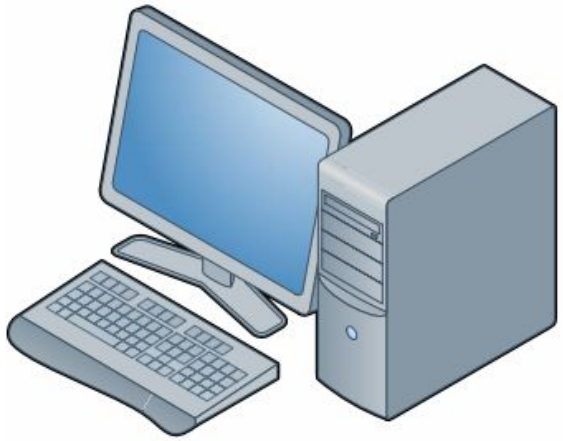
- The corresponding virtual physical interface is named LOOPBACK.

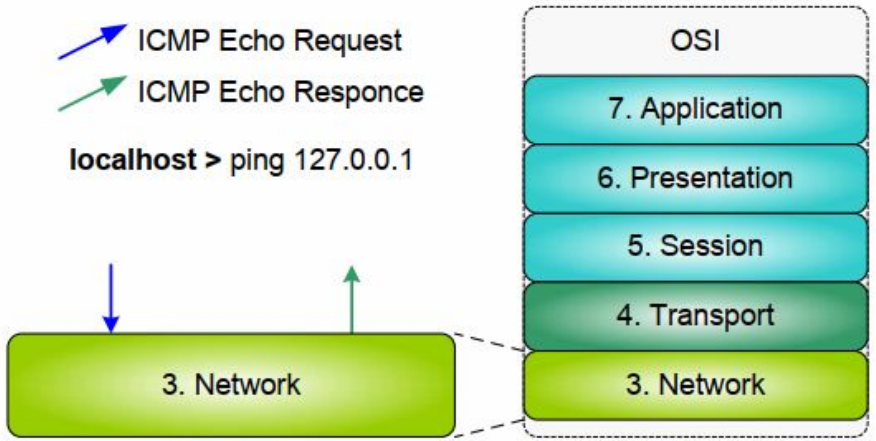
NETWORK TOOLS

softserve

NETWORK TEST (LOOPBACK)

- **Ping** – utility for testing IP-connection
  - **ICMP** – Internet Control Message Protocol
    - ICMP Echo Request
    - ICMP Echo Reply
- Testing local stack TCP/IP (127.0.0.1 – Loopback)
  - Reflect the state of the network layer (local)
  - Doesn't say anything about the underlying levels
  - Doesn't say anything about the correctness of the network settings (IP, Mask, Gateway, …)

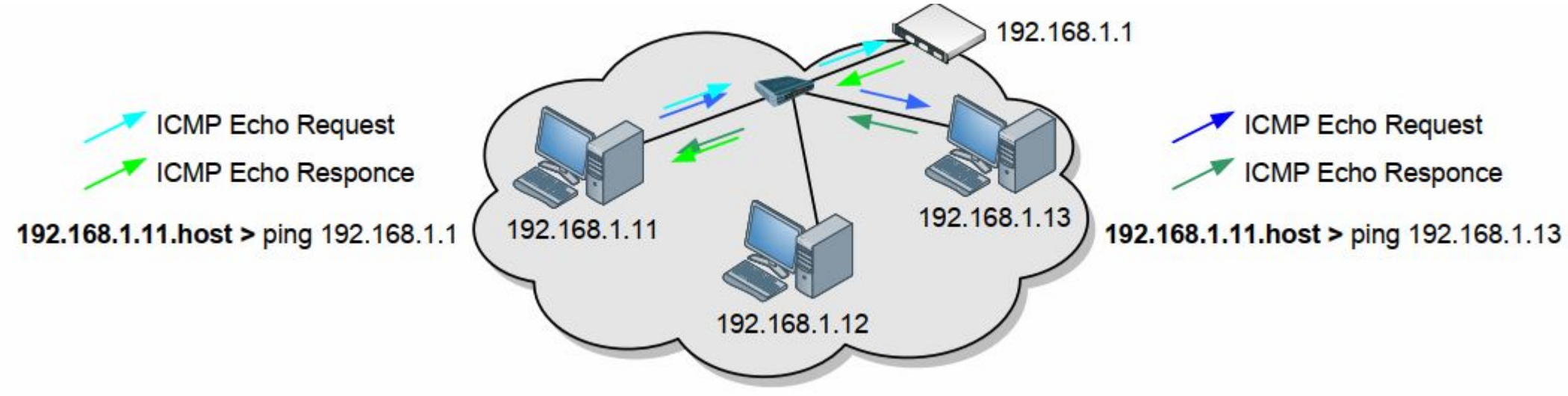




softserve

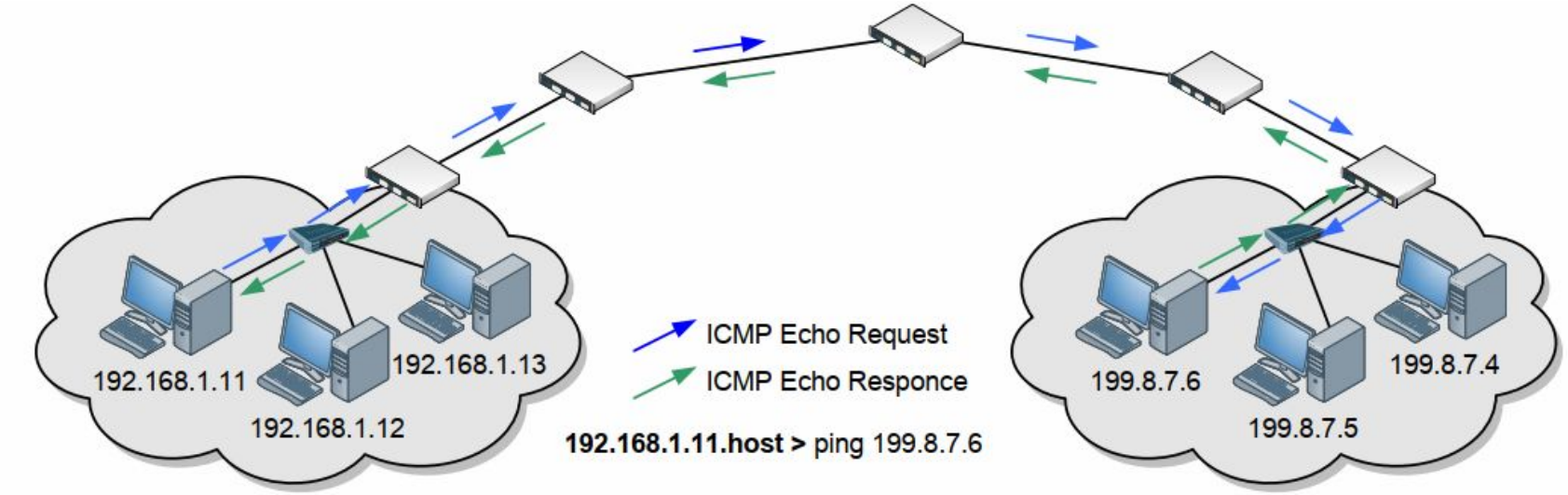
NETWORK TEST (LOCAL)

- Testing local network (IP, Gateway)
  - Checking workability of gateway
  - Functioning of whole stack TCP/IP
  - Functioning of Hub/Switch
  - Functioning of LAN



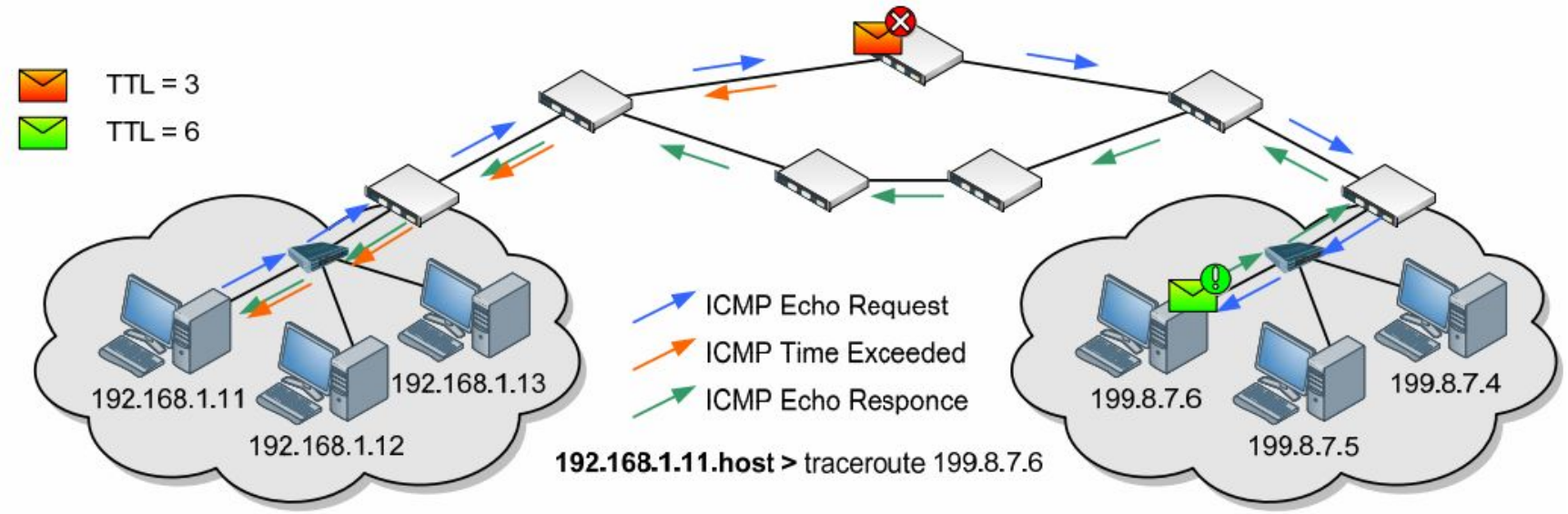
NETWORK TEST (REMOTE)

- Testing connections with remote network (device)
  - Gateway capability (WAN, Internet)
  - Functioning of intermediate equipment (and software)
  - Functioning of final addressable device (and software)
- Restrictions
  - Gateway capability (WAN, Internet)
  - Prohibition / Rejection ICMP datagrams
  - Difficulty of routes



softserve

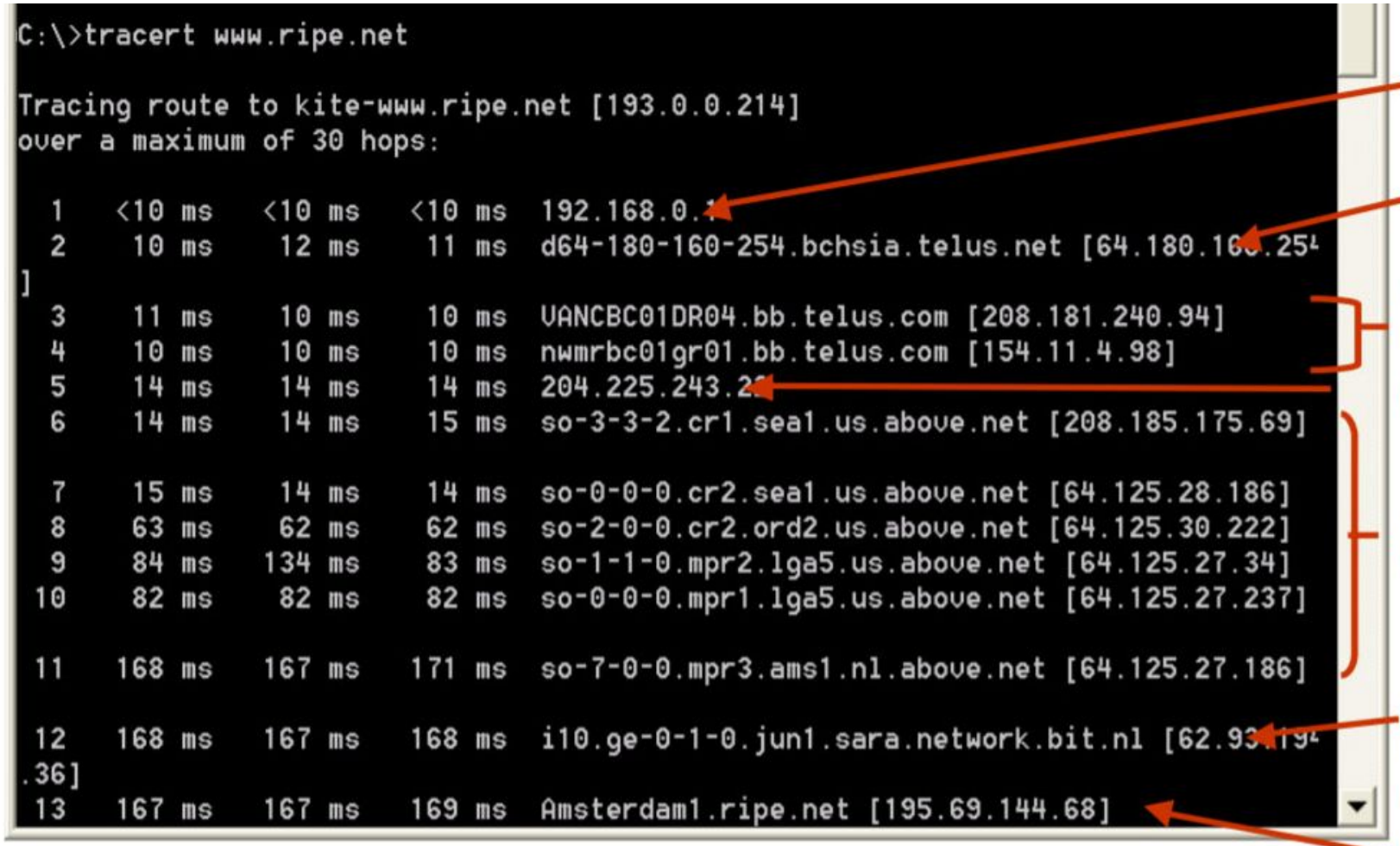
TESTING ROUTE



- **Traceroute** (in windows tracert) – utility for showing the path
  - ICMP
    - Echo Request
    - Time Exceeded
  - Displaying the path (s) of packages
  - Display network delay time (round trip time)

softserve

TESTING ROUTE



softserve

TESTING ROUTE

- Local router. The first lines of the traceroute results will indicate your gateway's IP address.
- PoP router. A Point of Presence (PoP) is the local access point of your ISP. This access point helps your device establish a connection with the internet.
- Source Tier 2 ISP Network. Your request might be routed to a regional ISP (like Comcast or Cox), which services a limited geographic area.
- IXP. An Internet Exchange Point (IXP) is a physical location where ISPs and other network providers connect to exchange internet traffic.
- Tier 1 ISP Network. These ISP providers are considered the backbone of the internet because they own the infrastructure to carry most of the traffic themselves.

IP-NETWORK TECHNOLOGIES

softserve

IP-NETWORK TECHNOLOGIES

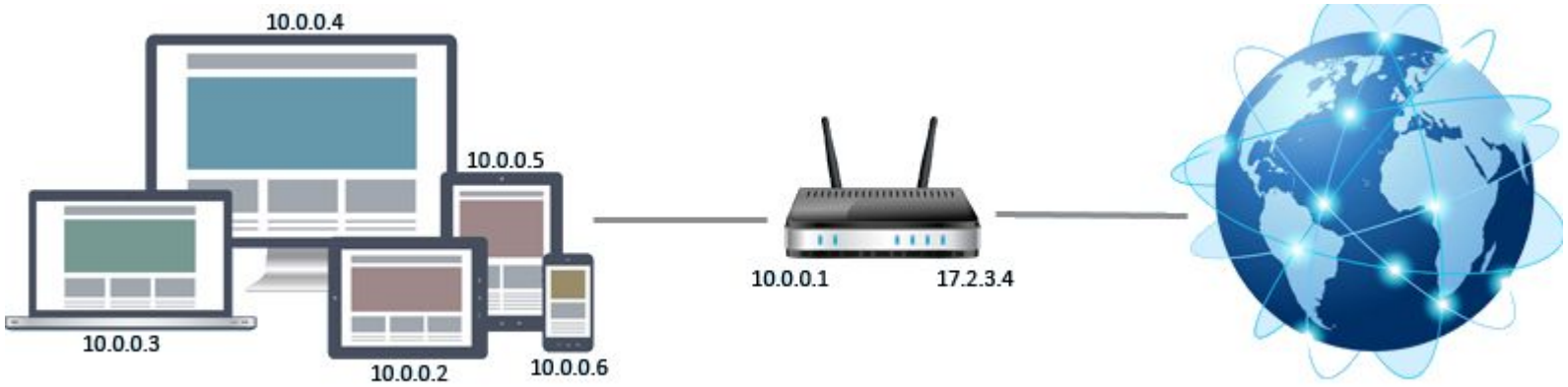
- Network Address Translation (NAT)
- Demilitarized zone (DMZ)
- Virtual Private Network (VPN)

NETWORK ADDRESS TRANSLATION

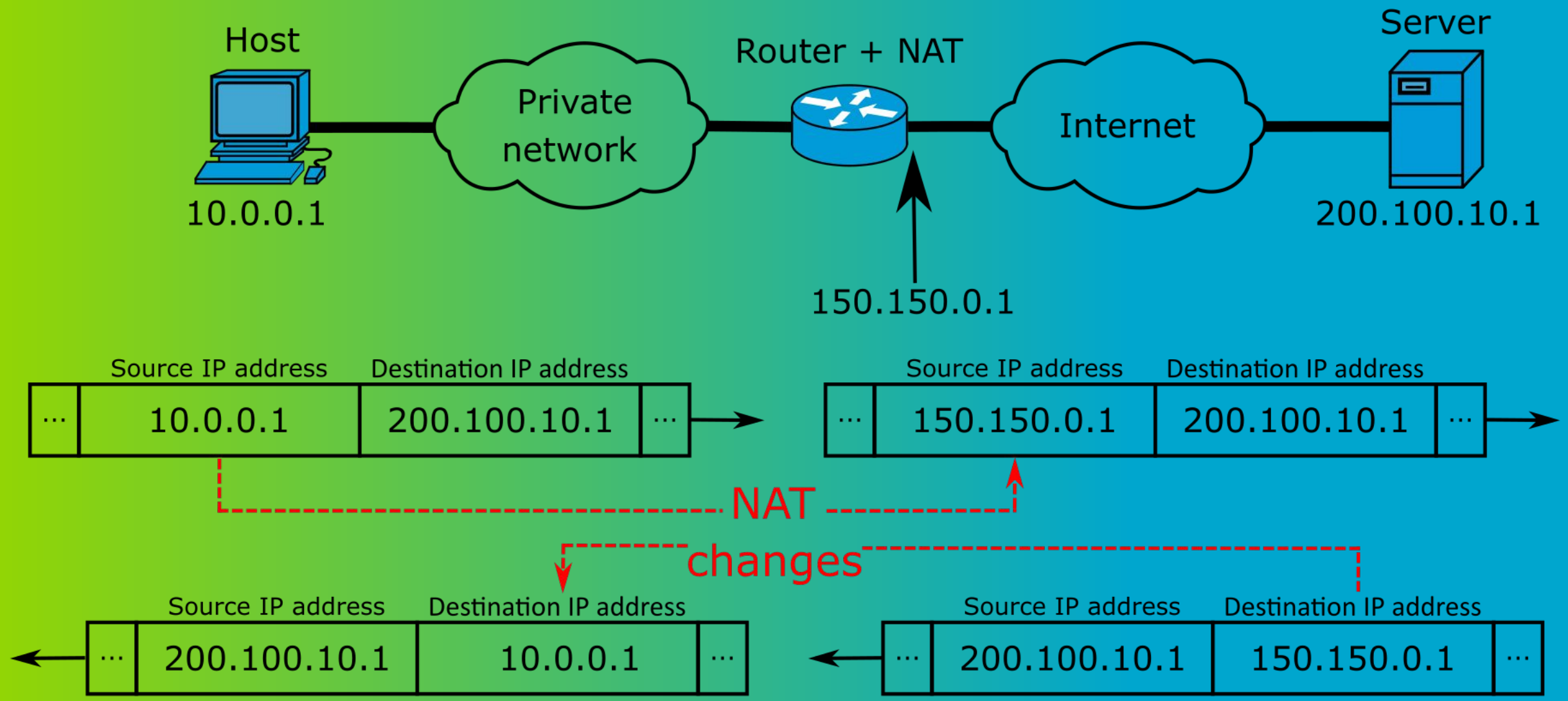
- **Network Address Translation (NAT)** – technology of address translation
  - **Rewriting** IP addresses and ports as the packet passes through intermediate network device

- **Types:**
  - Source NAT (SNAT)
  - Destination NAT (DNAT)
  - Port Address Translation (PAT)

- **Address Translation Concepts**
  - Static NAT
  - Dynamic NAT
  - Masquerading



softserve


Host
Private network
Router + NAT
Internet
Server
10.0.0.1
150.150.0.1
200.100.10.1
Source IP address
Destination IP address
10.0.0.1
200.100.10.1
150.150.0.1
200.100.10.1
NAT
changes
Source IP address
Destination IP address
200.100.10.1
10.0.0.1
Source IP address
Destination IP address
200.100.10.1
150.150.0.1

softserve

TYPES & CONCEPTION NAT [1]

- **Source NAT (SNAT)**:
  - Providing access from a local network (private, private, closed) to the Internet (public network)
  - The request is initiated from the internal network
- **Destination NAT (DNAT)**:
  - Providing access from the Internet to the local network
  - The request is initiated from the external network
  - The request is forwarded to a specific internal host
- **Port Address Translation (PAT)**:
  - Associates the public address and port with the internal address and port (access to internal services from the outside)
  - Often called "port forwarding"

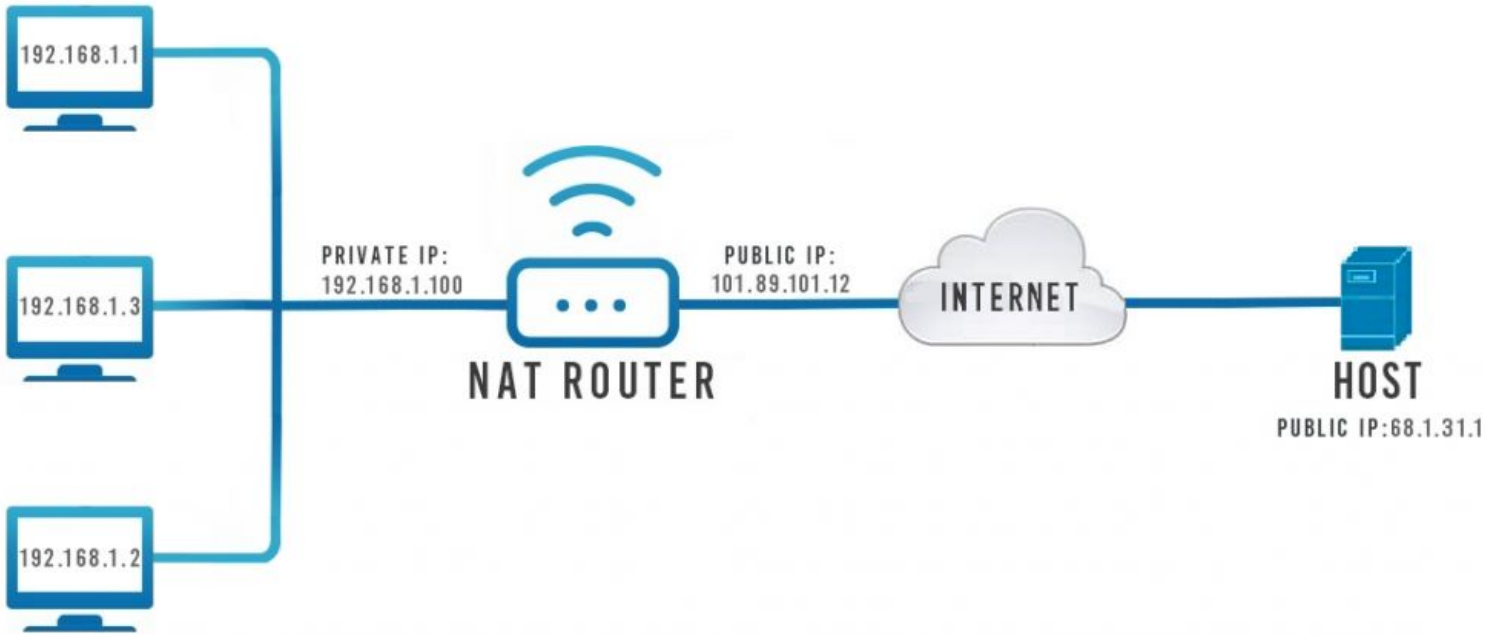
TYPES & CONCEPTION NAT [2]

- **Static NAT**:
  - Links one private address to one public address
- **Dynamic NAT**:
  - Associates many private addresses with a pool of public ones
- **Masquerading**:
  - Subtype of Source NAT
  - The external address is not explicitly indicated, but determined automatically (for the specified interface)
  - Used for dynamic "white" addresses

PORT ADDRESS TRANSLATION (PAT)

- **Port Address Translation (PAT)**, this is where each client uses the *same IP* address but uses a different port.
  - A good example is access to a web server. Users from a private address, say in the 10.0.0.0 network, have their individual addresses translated to just one legal IP address but separate port numbers between 1024 and 65535.
- They can all have separate conversations with a web server having just one address and destination port of 80 (HTTP).
  - This applies just as well if one user has several sessions with the same web server, the different port numbers distinguish the sessions.

PAT



NAT TABLE

INSIDE PRIVATE IP:PORT	INSIDE PUBLIC IP:PORT	OUTSIDE PUBLIC IP:PORT
192.168.1.1:9688	101.89.101.12:8801	68.1.31.1:23
192.168.1.2:1253	101.89.101.12:5123	68.1.31.1:23
192.168.1.3:1025	101.89.101.12:102	68.1.31.1:23

softserve

NAT: ADVANTAGES / DISADVANTAGES

ADVANTAGES	DISADVANTAGES
Saving IP-addresses: One “**white**” (**external**, public) IP-address serves many “gray” (hidden, internal) addresses	Not all protocols can work with NAT
Restricting access to the internal network from the public (SECURITY)	Complication of the work of the intermediate device
Hiding the internal network architecture	Additional complexities of user identification
	Multiple connections from one IP
	Problems accessing the internal network from the outside

VIRTUAL PRIVATE NETWORK (VPN)

- Virtual Private Network (VPN) – network built on top of another network
  - Typically, the underlying network is public (untrusted)

- VPN Building Options:
  - **Intranet VPN** – Integration into a single secure network several distributed networks of one organization (interaction through open channels)
  - **Remote Access VPN** – secure communication between corporate network segment and single user
  - **Client / Server VPN** – protection of transmitted data between two nodes (not networks) of the corporate network; authorized access to certain resources

VPN: ADVANTAGES / DISADVANTAGES

ADVANTAGES	DISADVANTAGES
Tunneling network traffic	Excess traffic
Encryption of transmitted data	
Authentication, authorization and accounting	
Hiding the internal network architecture from the public network	
Providing remote (mobile) users with authorized access to local network resources	
Creation of virtual networks	

TERMS and ABBREVIATIONS

- IPv4
- Reserved Addresses
- Unicast
- Broadcast
- Multicast
- NAT
- NAT: PAT
- Subnet mask
- Subnetting
- Ping
- Traceroute
- VPN

softserve

REFERENCES & SOURCES

https://www.ietf.org/rfc/rfc1631.txt – NAT

softserve


TO
THE
FUTURE
softserve