Networks: Tutorial 10

Shinnazar Seytnazarov, PhD

Innopolis University

s.seytnazarov@innopolis.ru

February 18, 2022

Outline

- IP addressing
- Subnets
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)

IP Addressing

Any device in a computer network should be identified;

The IP network layer communication protocol requires each device (host or router) to have an IP address

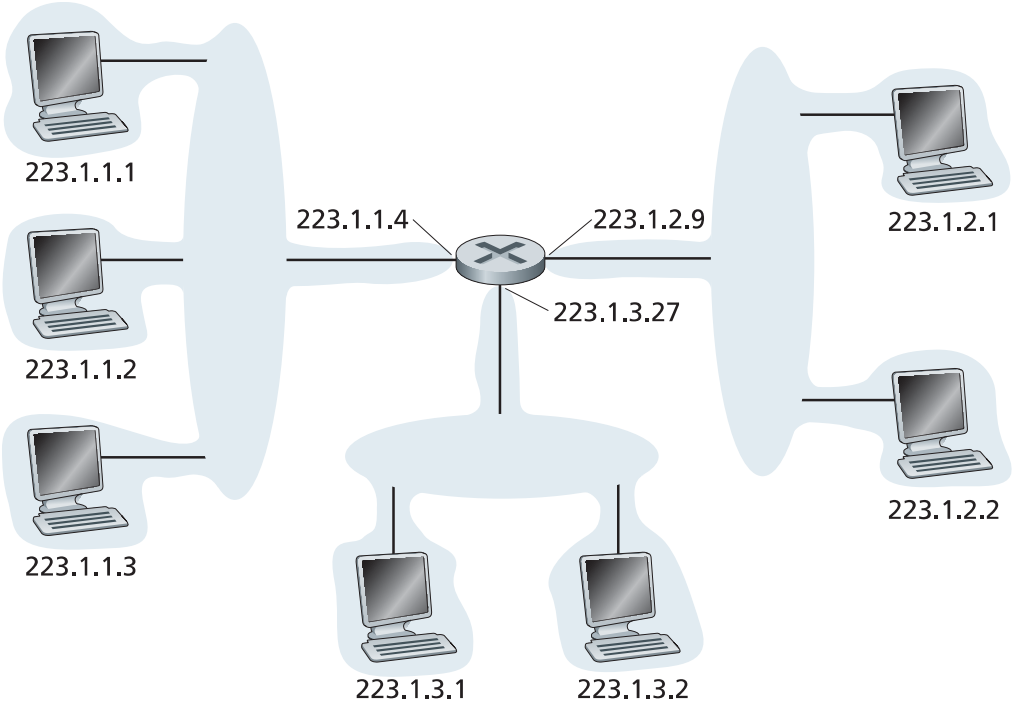
So, how IP addressing works?

IP Addressing

Any device in a computer network should be identified;

The IP network layer communication protocol requires each device (host or router) to have an IP address

So, how IP addressing works?

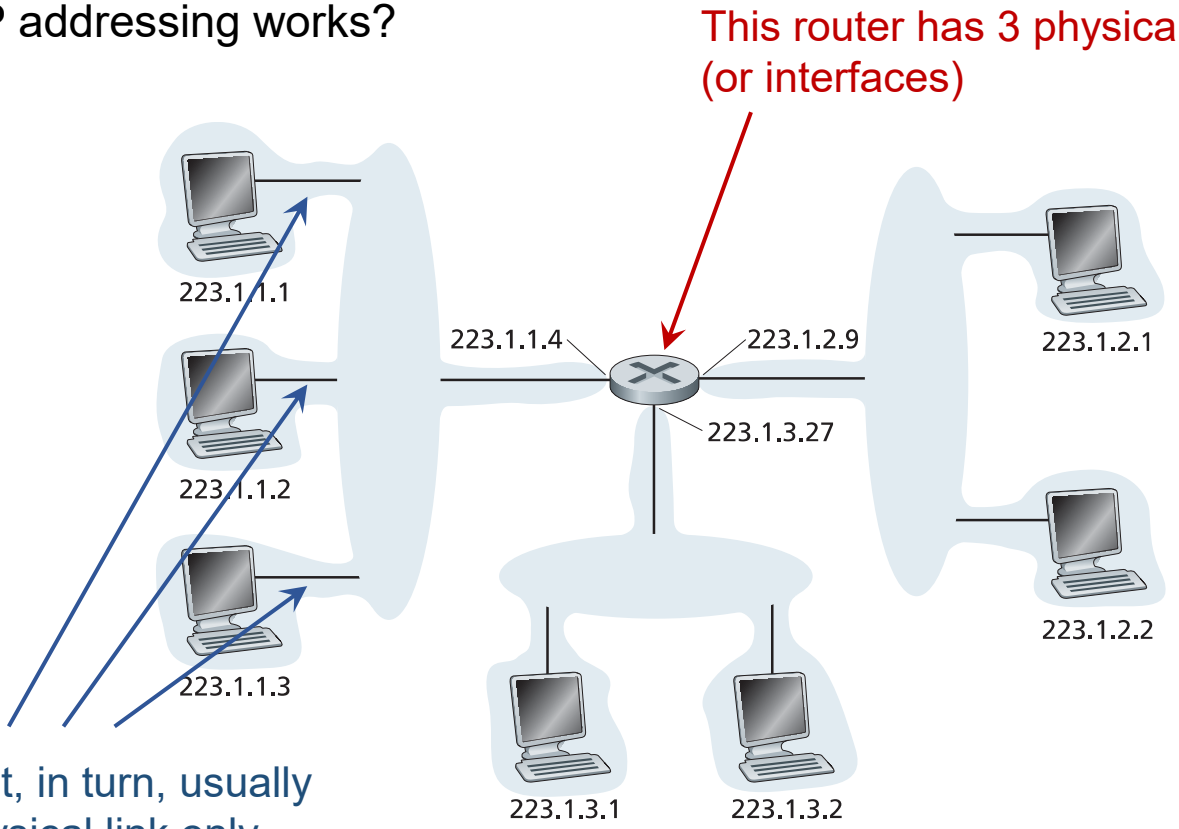


IP Addressing

Any device in a computer network should be identified;

The IP network layer communication protocol requires each device (host or router) to have an IP address

So, how IP addressing works?

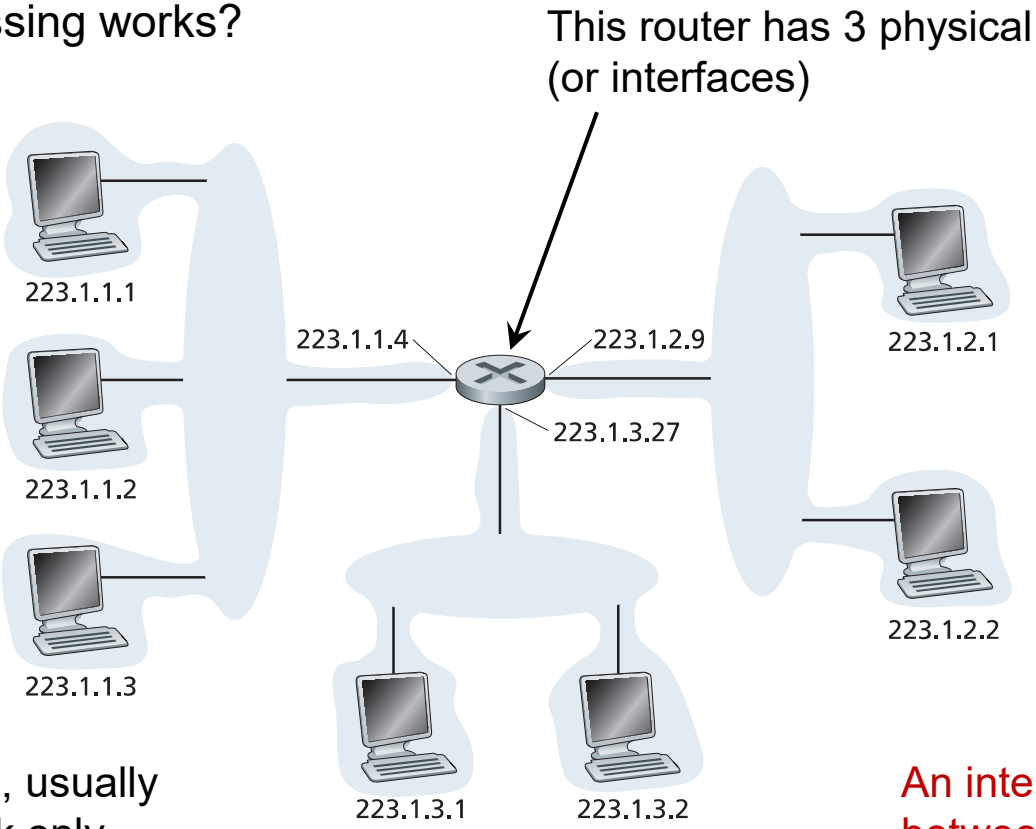


IP Addressing

Any device in a computer network should be identified;

The IP network layer communication protocol requires each device (host or router) to have an IP address

So, how IP addressing works?



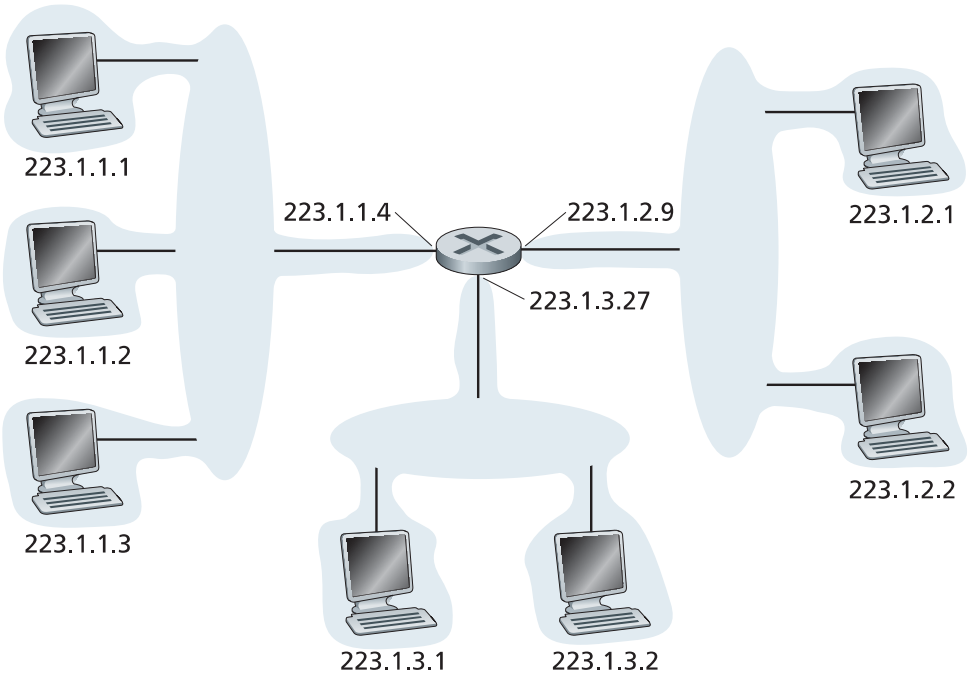
Each host, in turn, usually has 1 physical link only (and thus, an interface)

An interface – a boundary between a network node and a physical link

For each network node, every interface has an associated IP address

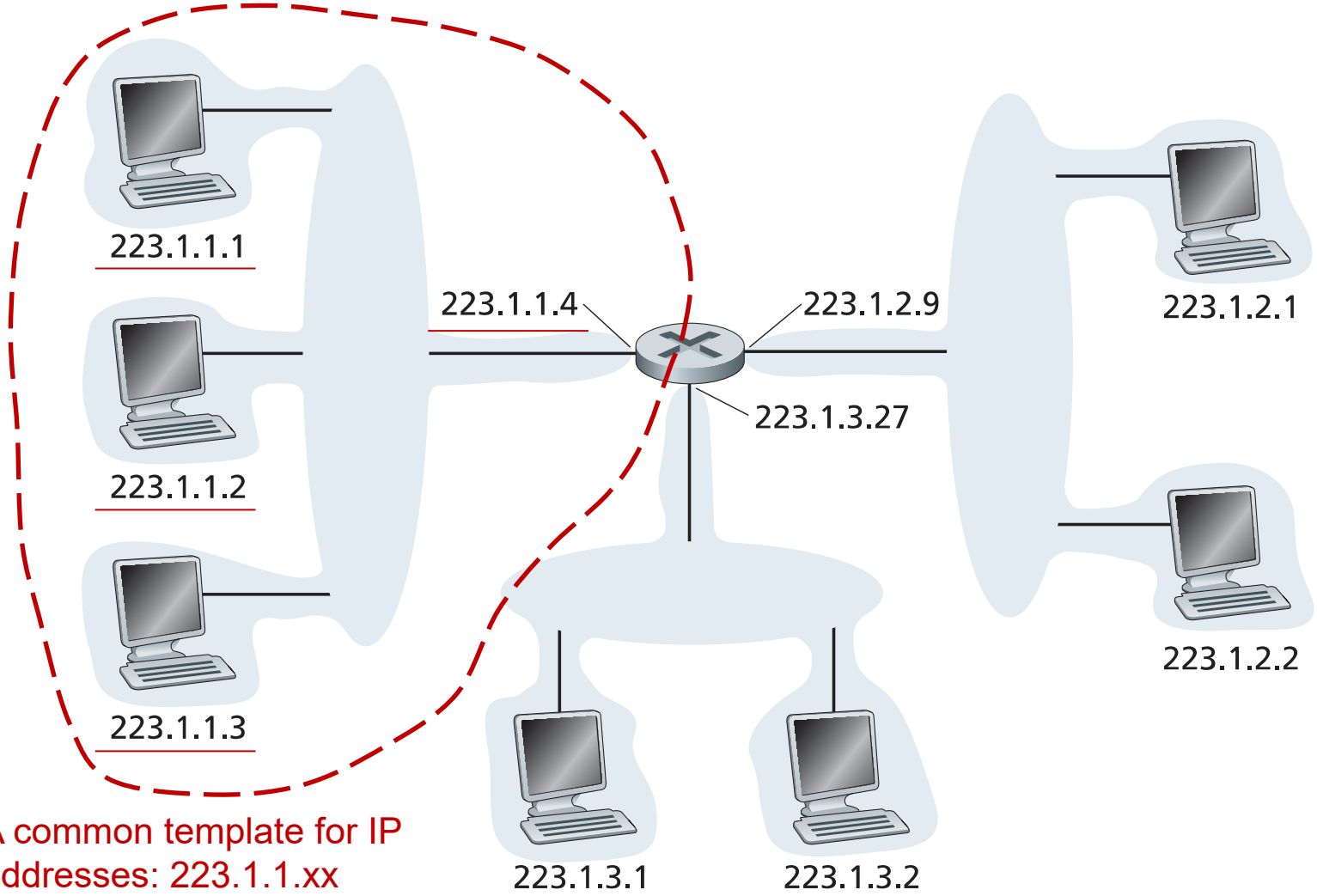
IPv4 Addressing: Summary

- IPv4 address is 32 bits long
- There are in total 2^{32} unique IPv4 addresses (that is around $4 * 10^9$ addresses)
- IP addresses are represented in dotted-decimal notation, e.g. 193.32.216.9, or in a binary notation
- In the global network, each interface on every host and router must have a globally unique IP address



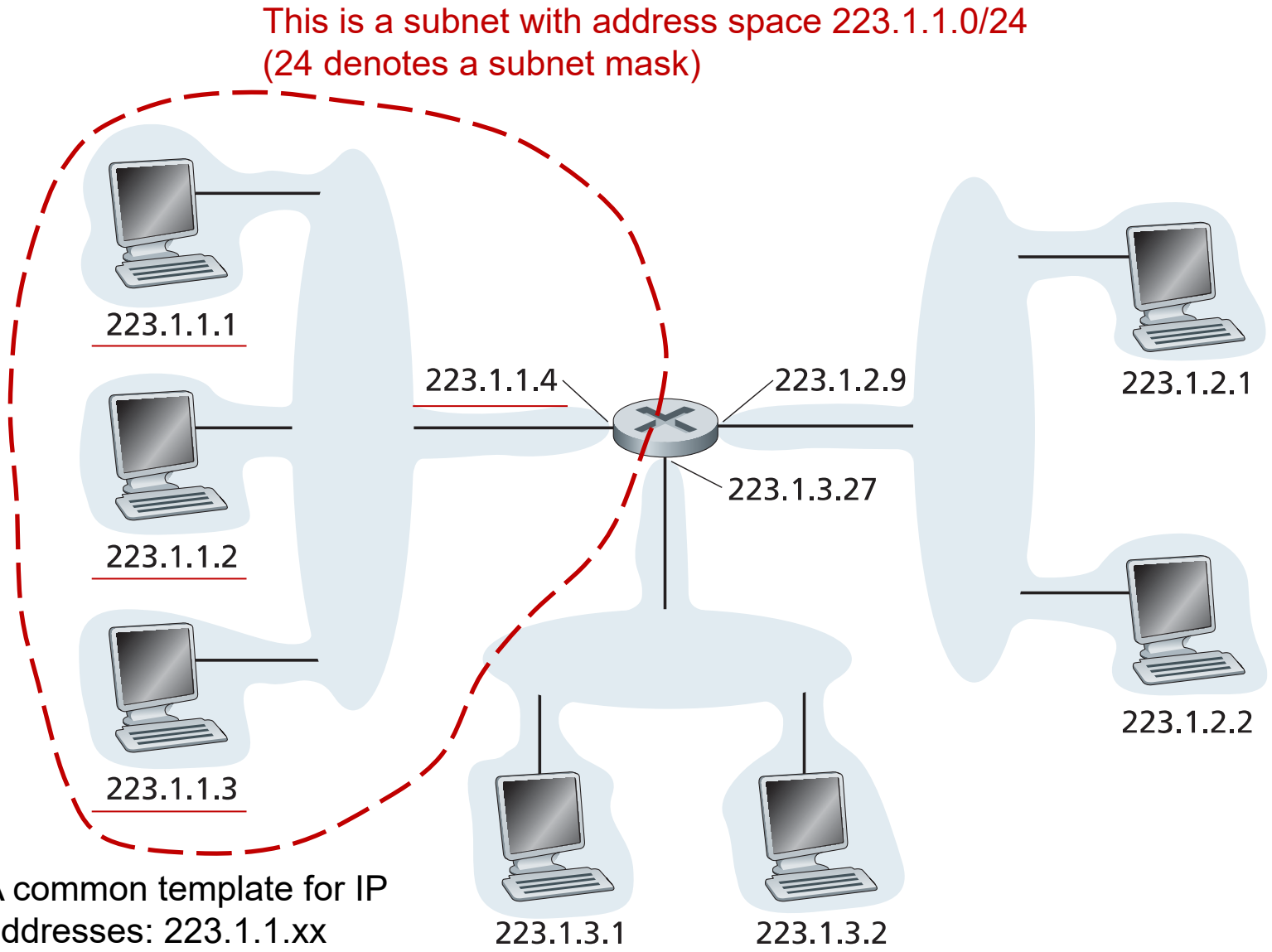
- There are devices having either one IP address (e.g. a typical host), or multiple IP addresses (e.g. a router)
- IP addresses should satisfy a set of constraints, as some IP addresses are reserved for special purposes, such as:
  - 255.255.255.255 – a broadcast IP address;
  - 0.0.0.0 – “this host” IP address, assigned to a host with no real IP address yet assigned;
  - 10.0.0.0/24 – the address space reserved for a private network
- IP addresses are distributed to ISPs by a global authority - Internet Corporation for Assigned Names and Numbers (ICANN), and its local branches

Subnets



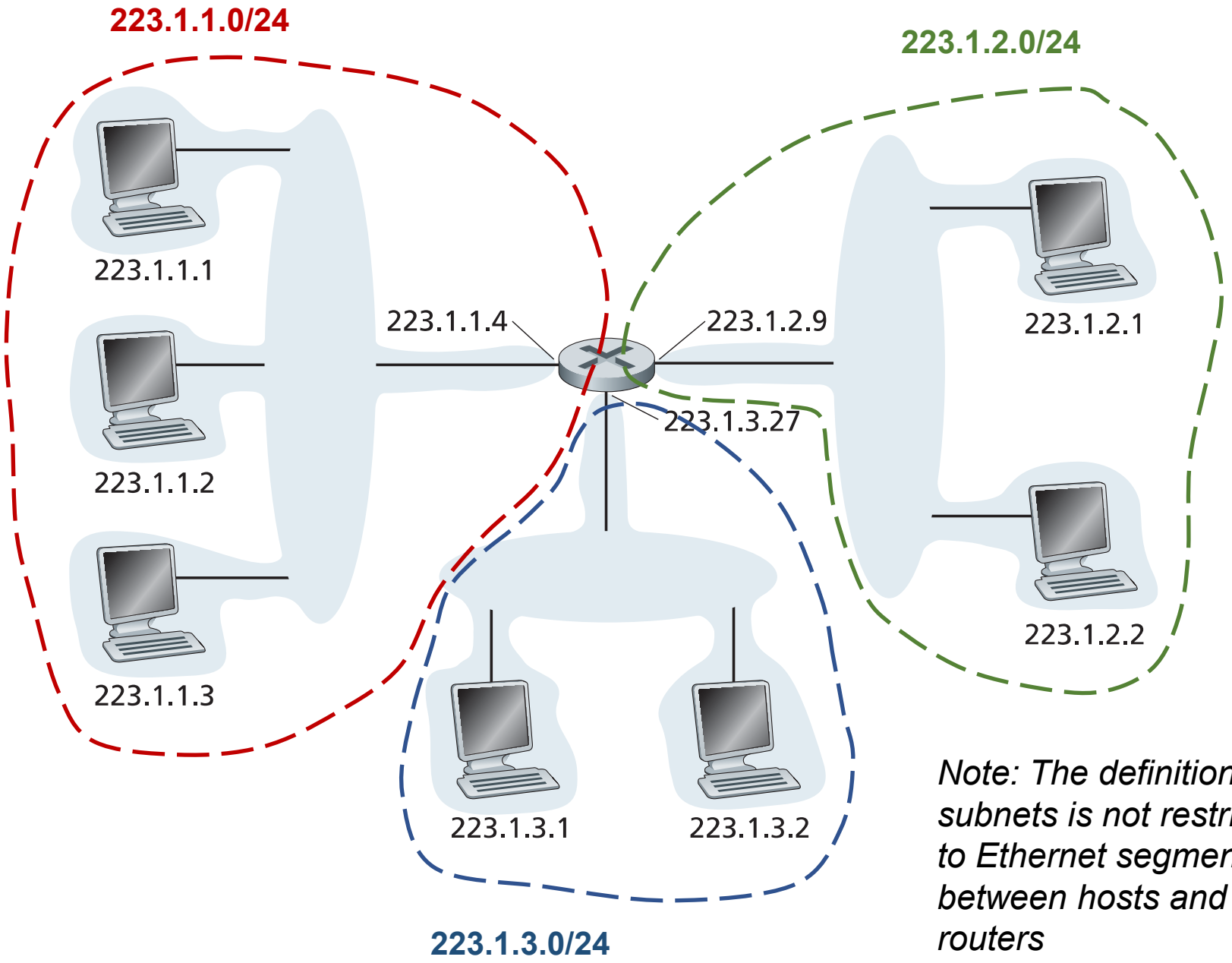
- A common template for IP addresses: 223.1.1.xx
- Direct interconnection between interfaces (no intermediate routers)

Subnets



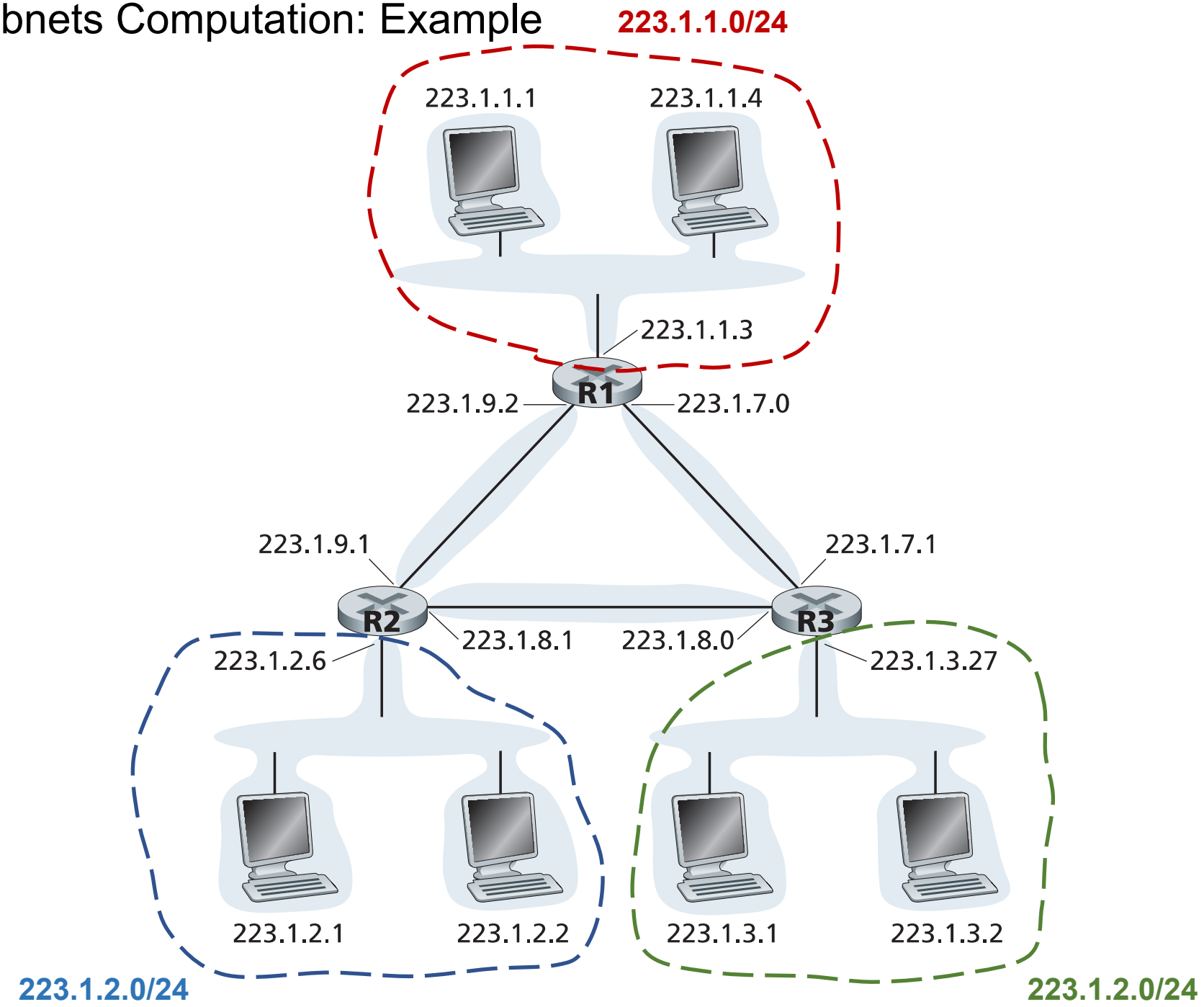
- A common template for IP addresses: 223.1.1.xx
- Direct interconnection between interfaces (no intermediate routers)

Subnets



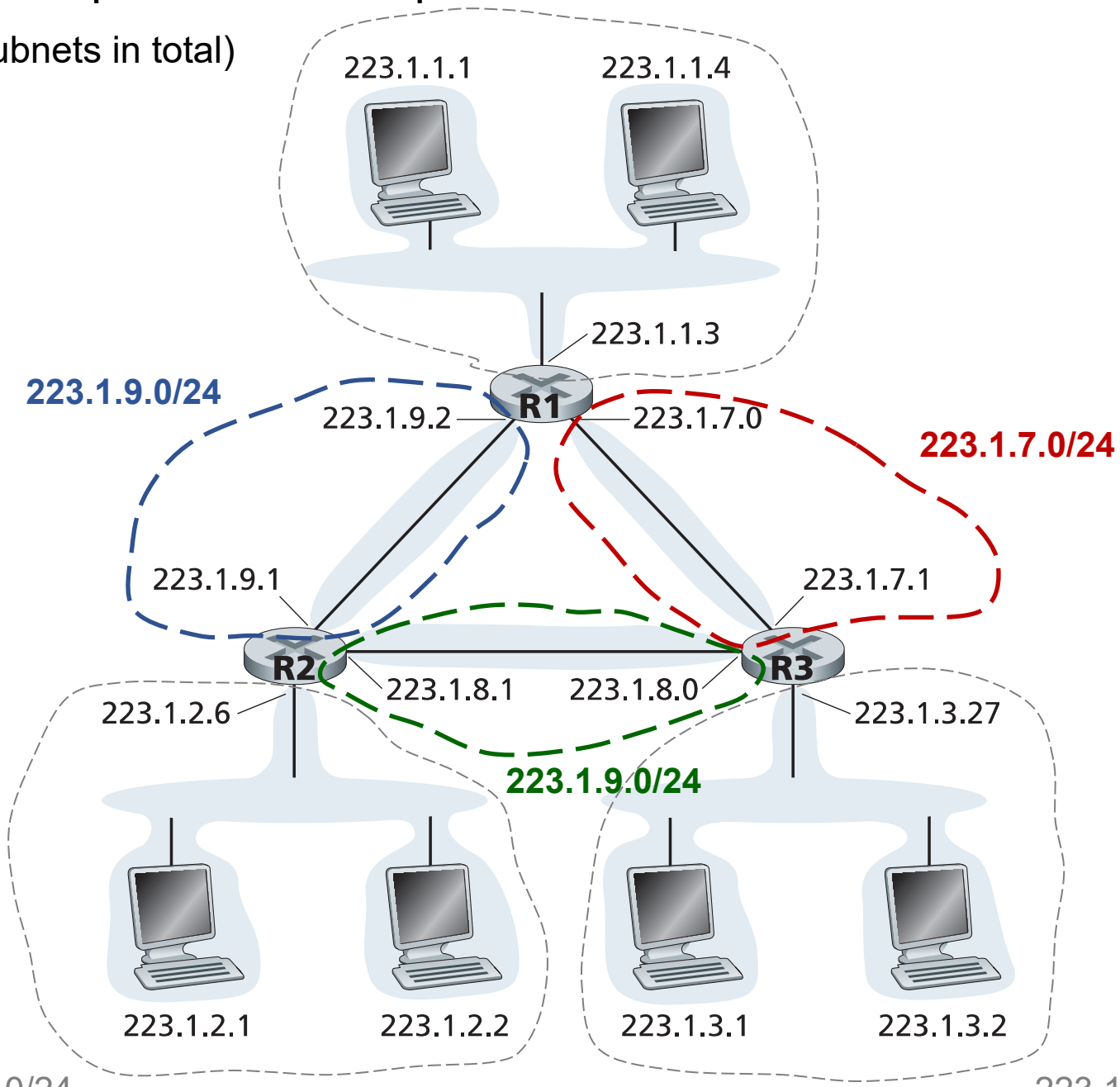
Note: The definition of subnets is not restricted to Ethernet segments between hosts and routers

Subnets Computation: Example



Subnets Computation: Example

(We get 6 subnets in total)



So, how IP addresses are assigned?

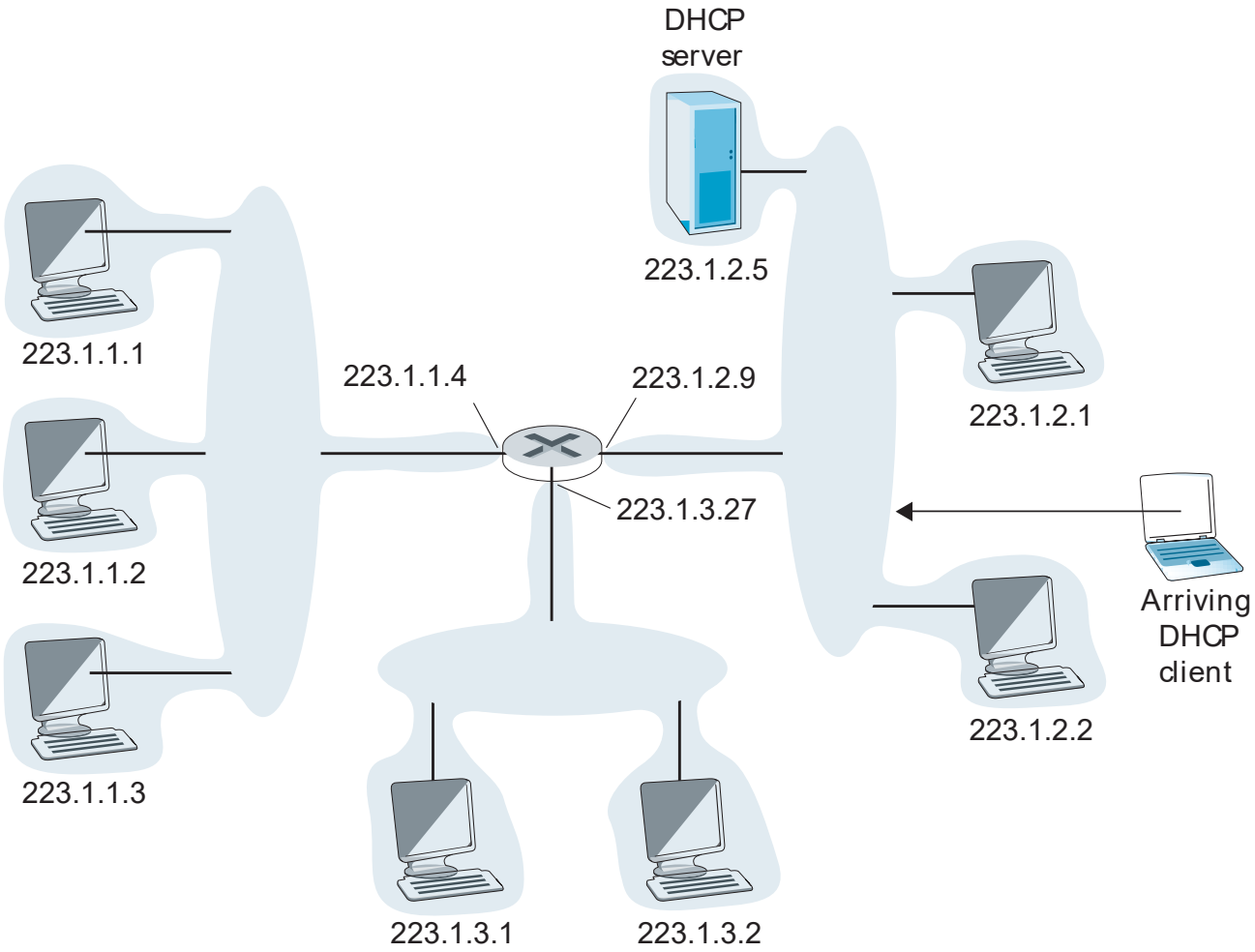
There are several stages:

1) Global authority – ICANN – allocates blocks of IP addresses to ISPs
2) ISPs assign IP addresses either statically or by using DHCP servers:
    1) To routers – usually by hand, by using special tools;
    2) To hosts – usually dynamically, by using DHCP server(s)

Dynamic Host Configuration Protocol (DHCP) Server

Procedure to assign an IP address to a new host:

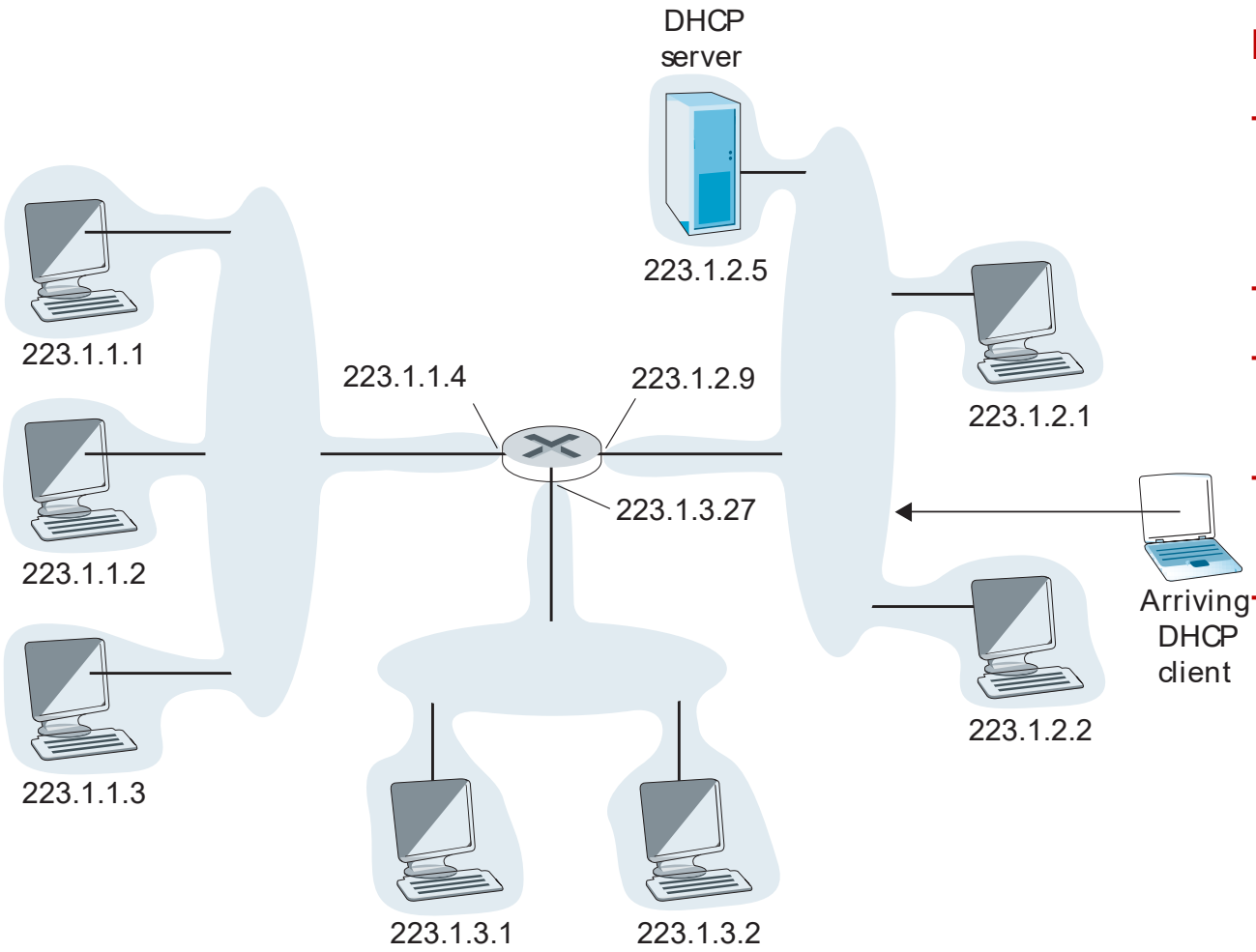
1) A joining host must discover a DHCP server first, so it sends a broadcast message, that is received by all other nodes, including a DHCP server;
2) DHCP server chooses some available IP address, and broadcasts it into a network;
3) A client host might get several offers of IP addresses, in case of multiple DHCP servers on a network;
4) A client makes a choice, echoing a message with a chosen IP, and DHCP acknowledges;



Dynamic Host Configuration Protocol (DHCP) Server

Procedure to assign an IP address to a new host:

1) A joining host must discover a DHCP server first, so it sends a broadcast message, that is received by all other nodes, including a DHCP server;
2) DHCP server chooses some available IP address, and broadcasts it into a network;
3) A client host might get several offers of IP addresses, in case of multiple DHCP servers on a network
4) A client makes a choice, echoing a message with a chosen IP, and DHCP acknowledges



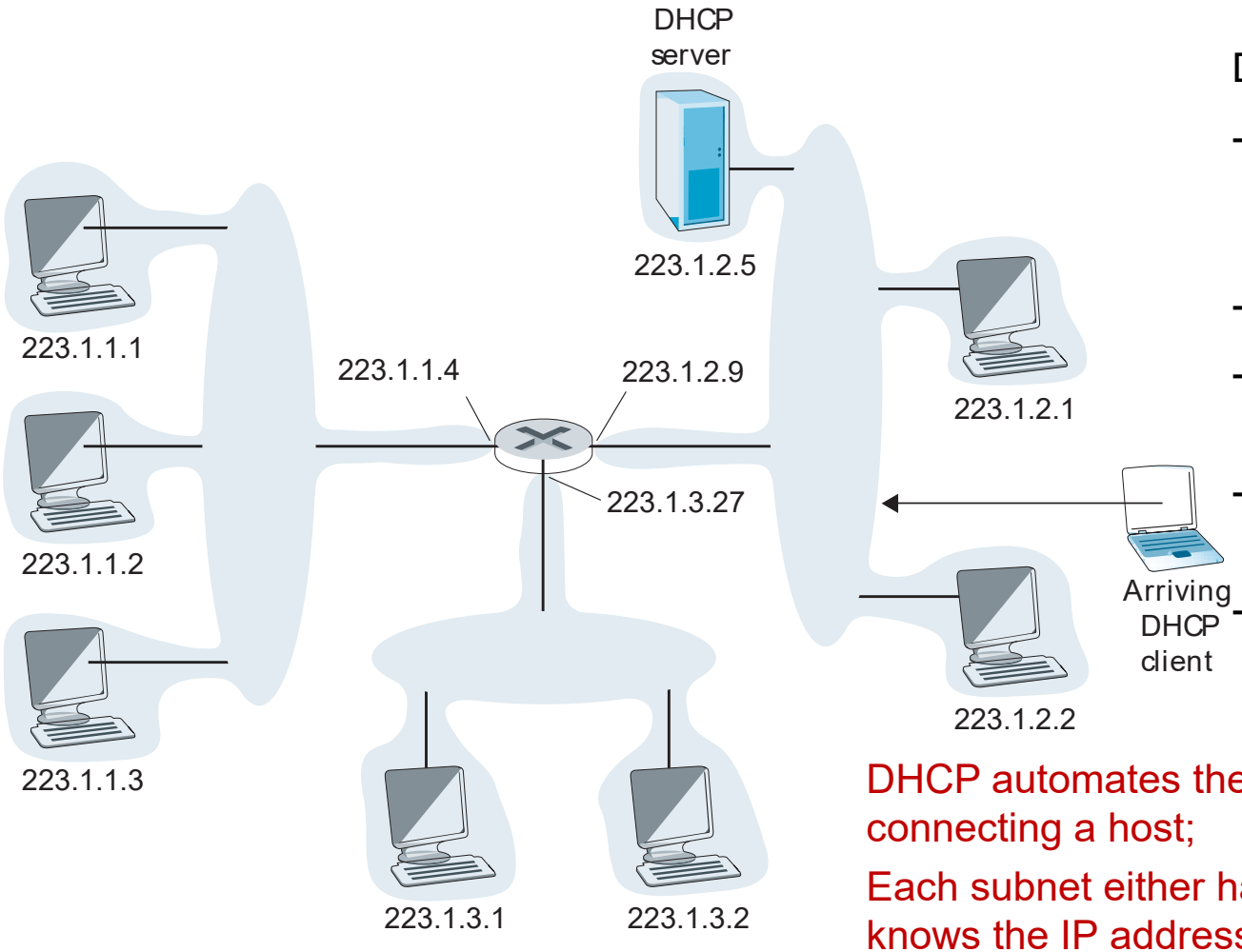
DHCP provides:

- IP address (static or temporary, with a limited IP lease time);
- DHCP IP address;
- The address of the first-hop router (default gateway);
- The address of a local DNS server;
- Subnet address mask

Dynamic Host Configuration Protocol (DHCP) Server

Procedure to assign an IP address to a new host:

1) A joining host must discover a DHCP server first, so it sends a broadcast message, that is received by all other nodes, including a DHCP server;
2) DHCP server chooses some available IP address, and broadcasts it into a network;
3) A client host might get several offers of IP addresses, in case of multiple DHCP servers on a network
4) A client makes a choice, echoing a message with a chosen IP, and DHCP acknowledges



DHCP provides:

- IP address (static or temporary, with a limited IP lease time);
- DHCP IP address;
- The address of the first-hop router (default gateway);
- The address of a local DNS server;
- Subnet address mask

DHCP automates the network-related aspects of connecting a host;

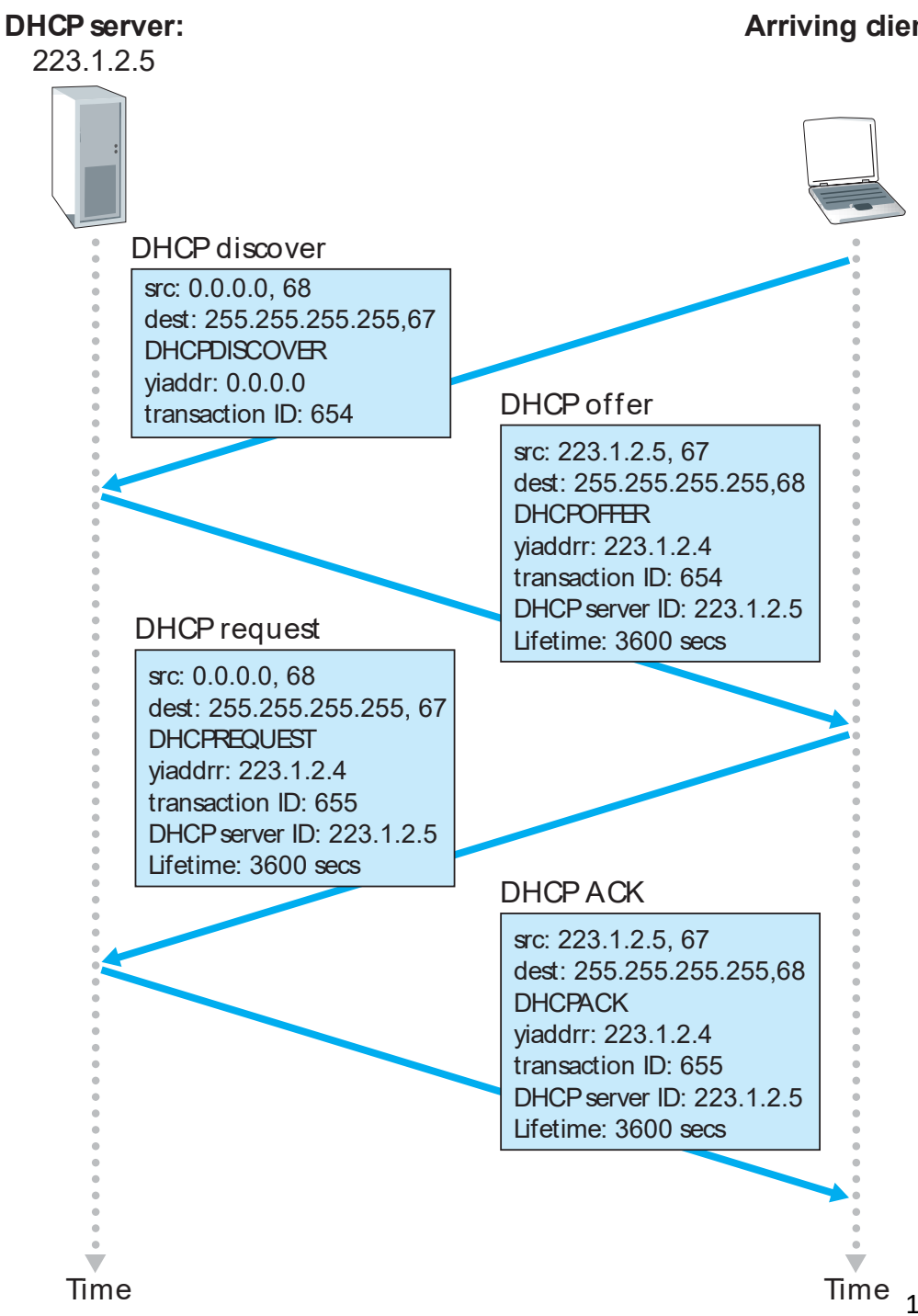
Each subnet either has a DHCP server, or a router knows the IP address of a DHCP server

DHCP Client-Server Interaction

Recap:

255.255.255.255 – broadcast destination IP;

0.0.0.0 – “this host” source IP

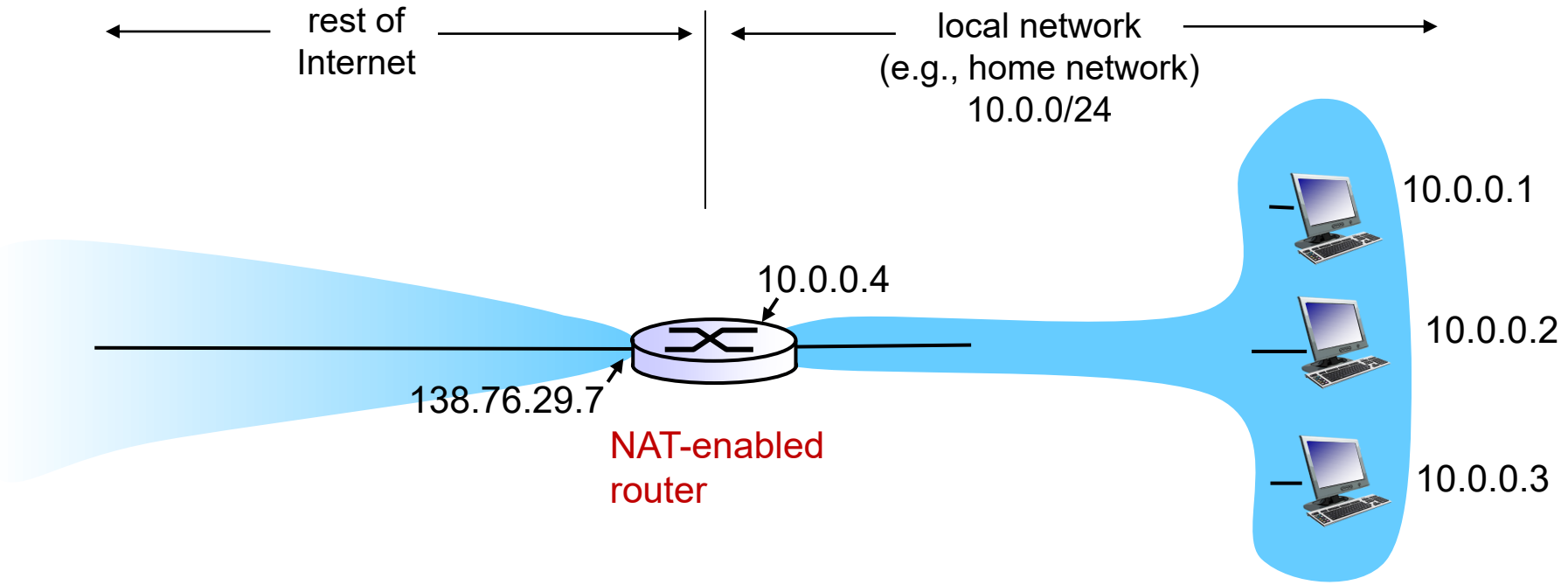


Network Address Translation (NAT)

Every IP-cable device needs an IP address;

There is a shortage of the available IPv4 addresses;

Solution – NAT, that allows to spend only 1 public IP address for a subnet

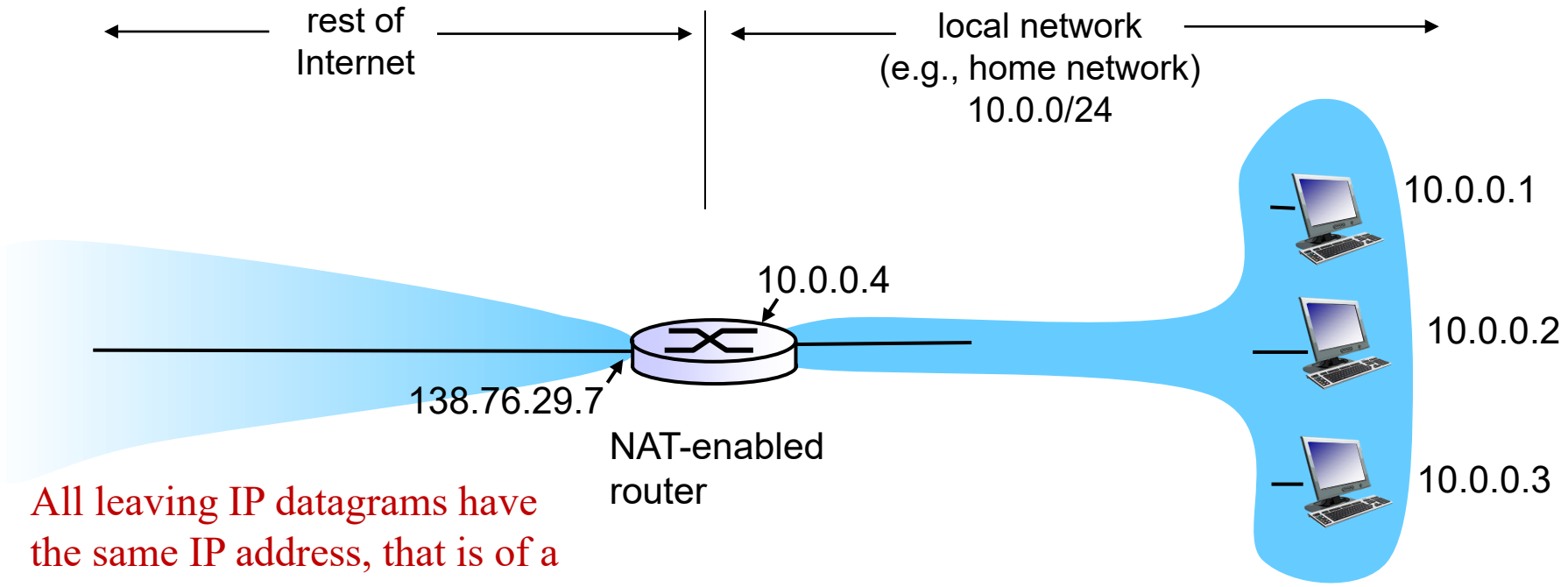


Network Address Translation (NAT)

Every IP-cable device needs an IP address;

There is a shortage of the available IPv4 addresses;

Solution – NAT, that allows to spend only 1 public IP address for a subnet



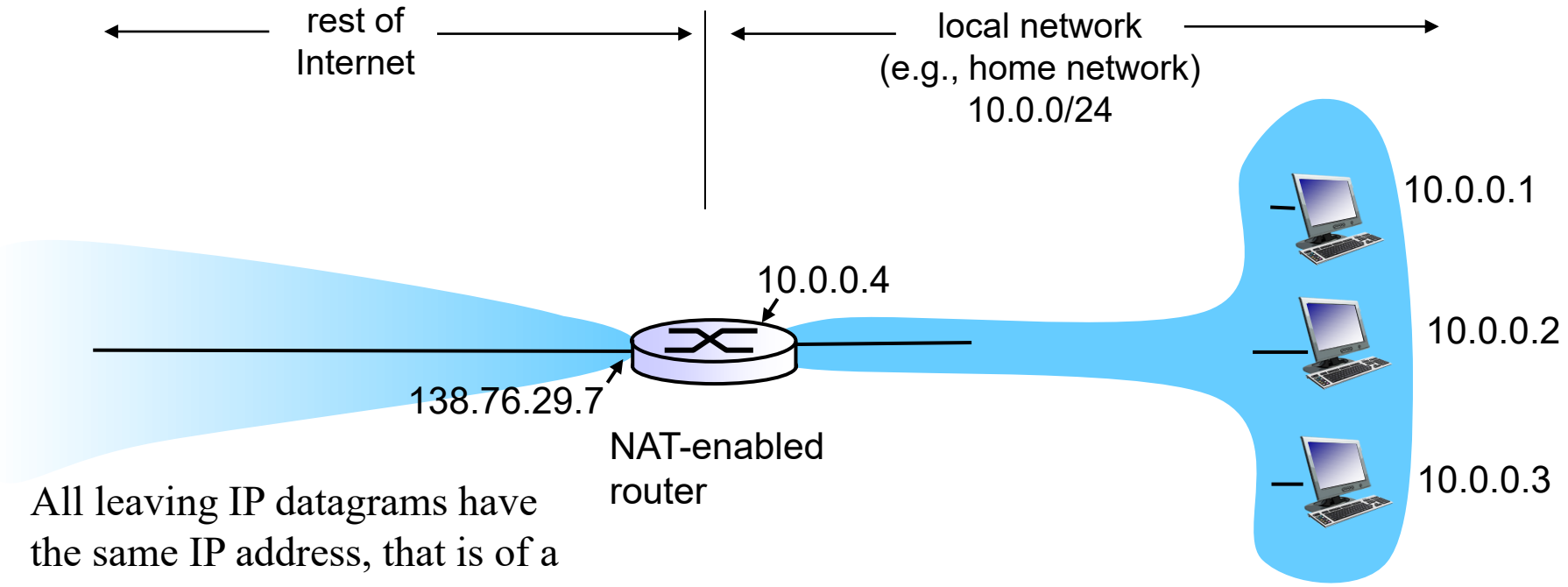
All leaving IP datagrams have the same IP address, that is of a NAT router

Network Address Translation (NAT)

Every IP-cable device needs an IP address;

There is a shortage of the available IPv4 addresses;

Solution – NAT, that allows to spend only 1 public IP address for a subnet



All leaving IP datagrams have the same IP address, that is of a NAT router

138.76.29.7 – a public IP address

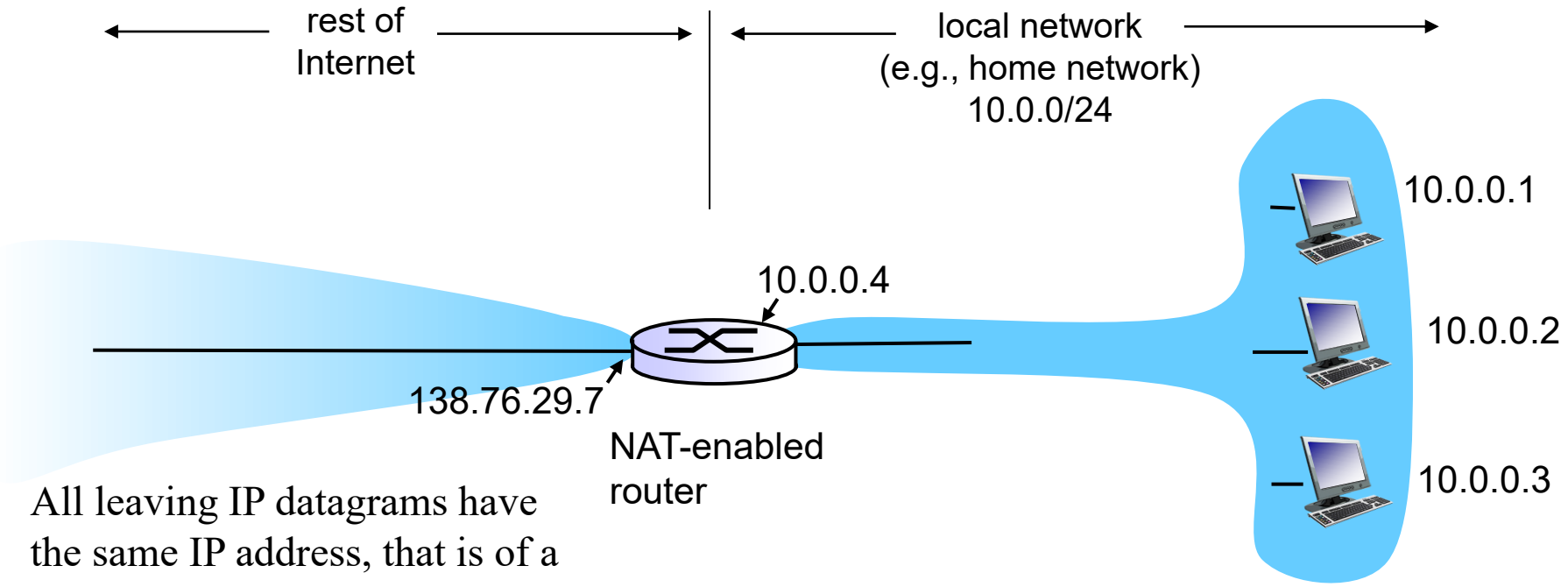
10.0.0.0/24 – private IP addresses

Motivation for Network Address Translation (NAT)

Every IP-cable device needs an IP address;

There is a shortage of the available IPv4 addresses;

Solution – NAT, that allows to spend only 1 public IP address for a subnet



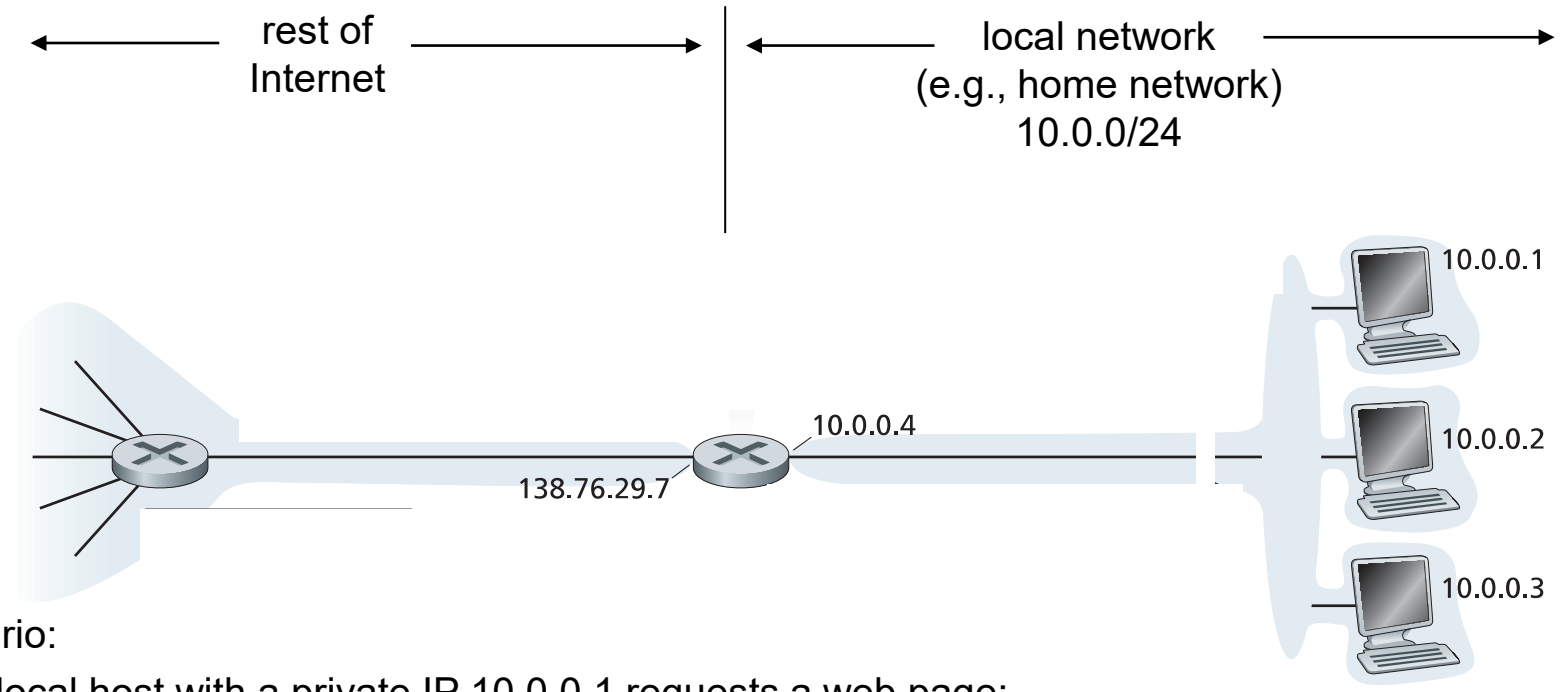
All leaving IP datagrams have the same IP address, that is of a NAT router

138.76.29.7 – a public IP address

10.0.0.0/24 – private IP addresses

The usage of a NAT-enabled router allows to reserve only 1 public IP address for an entire subnet

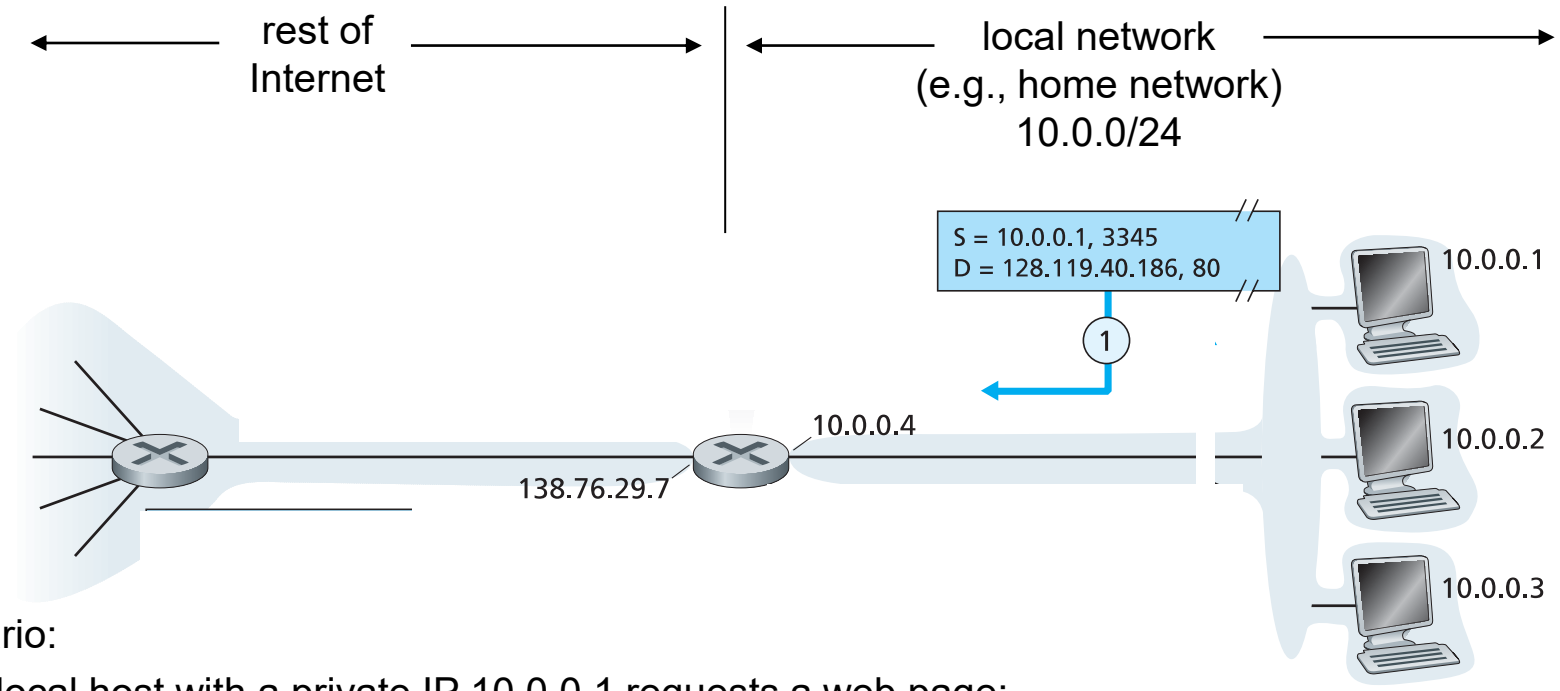
Network Address Translation (NAT): The Principle of Work



Scenario:

1) A local host with a private IP 10.0.0.1 requests a web page;

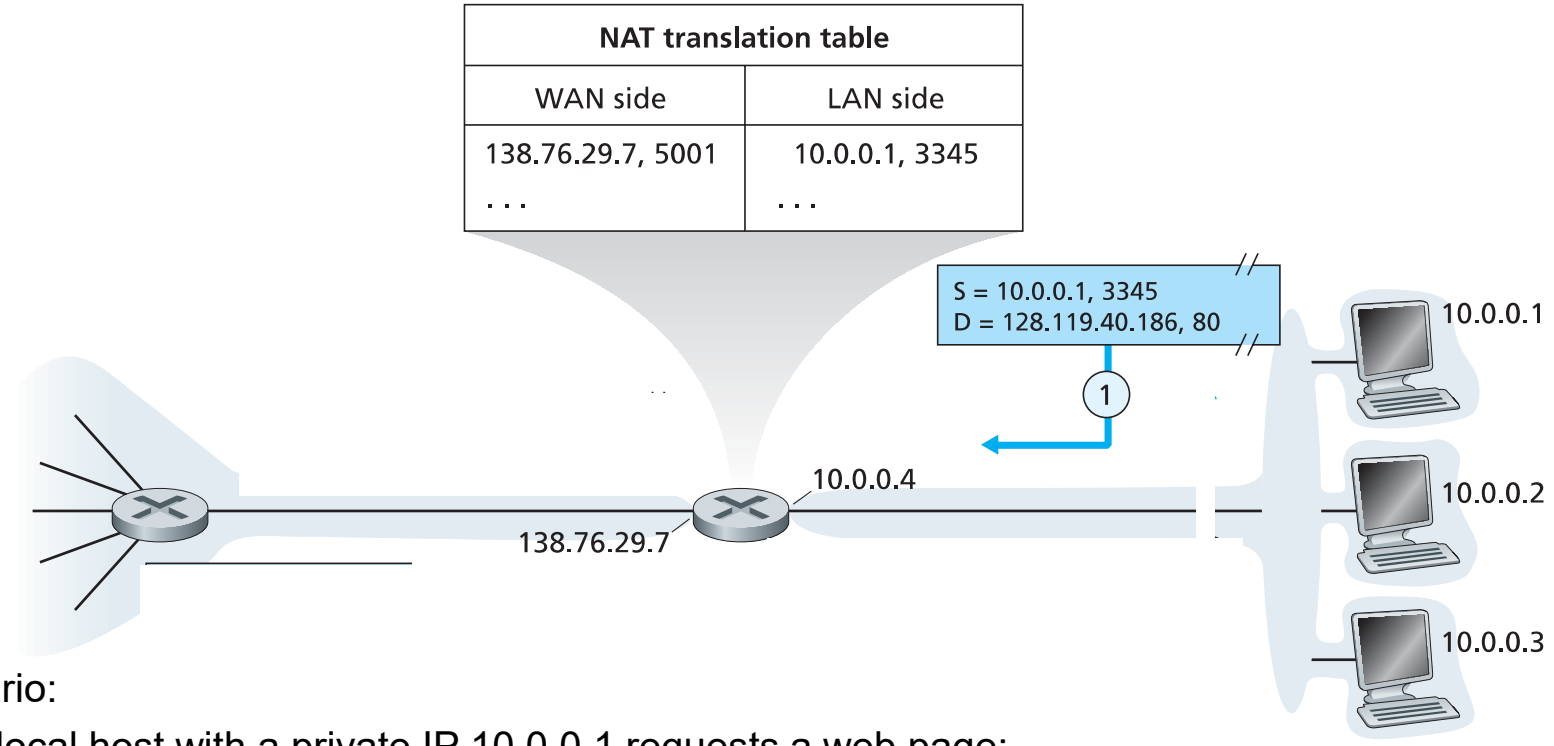
Network Address Translation (NAT): The Principle of Work



Scenario:

1) A local host with a private IP 10.0.0.1 requests a web page;
2) That host assigns to its IP datagram request an arbitrary source port number, e.g. 3345;
3) IP datagram is sent into LAN;

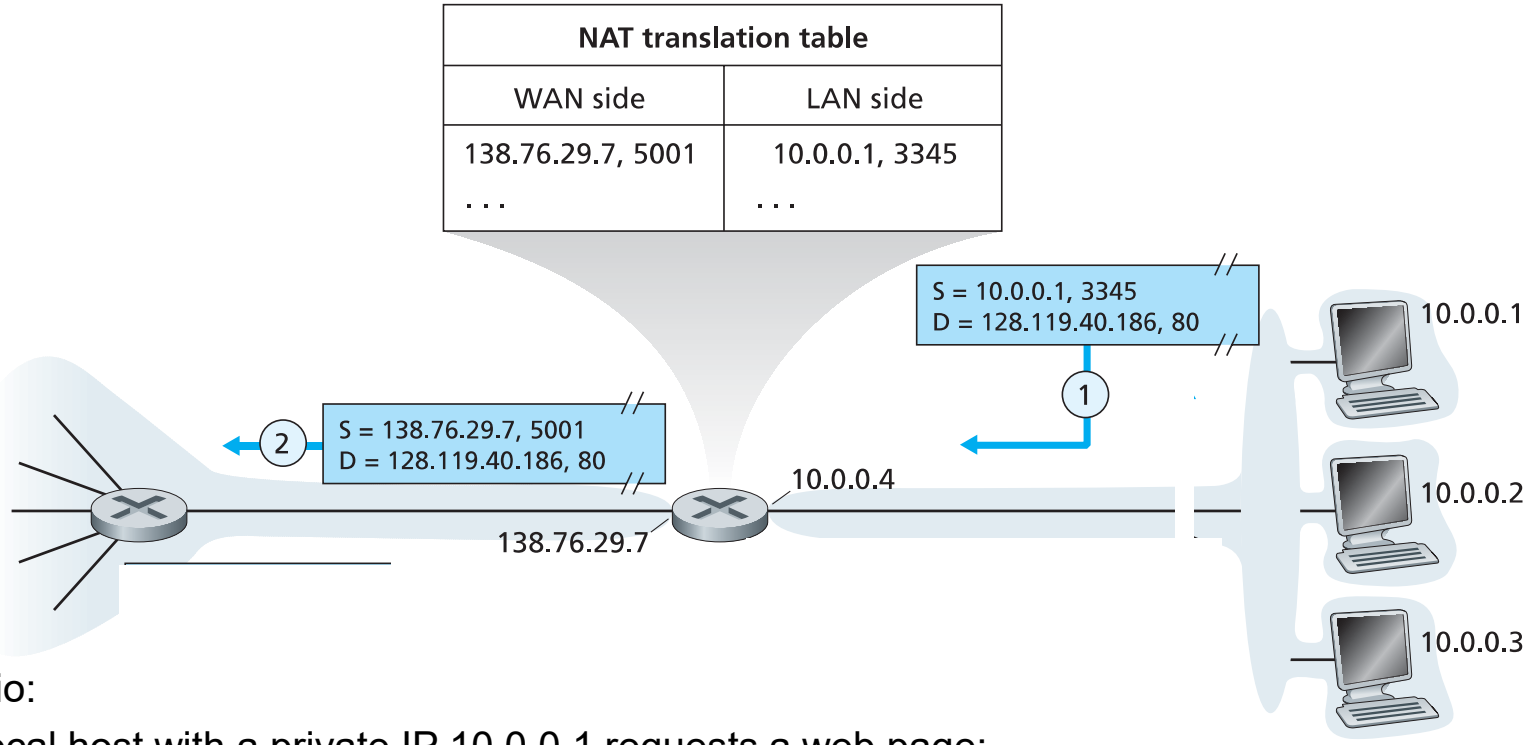
Network Address Translation (NAT): The Principle of Work



Scenario:

1) A local host with a private IP 10.0.0.1 requests a web page;
2) That host assigns to its IP datagram request an arbitrary source port number, e.g. 3345;
3) IP datagram is sent into LAN;
4) Router receives it, replaces the private IP 10.0.0.4 with its public IP 138.76.29.7, as well as generates a random new port number, e.g. 5001;
5) Router adds an entry into its NAT table, that port 5001 corresponds to host 10.0.0.1, and sends the modified IP datagram into the global network;

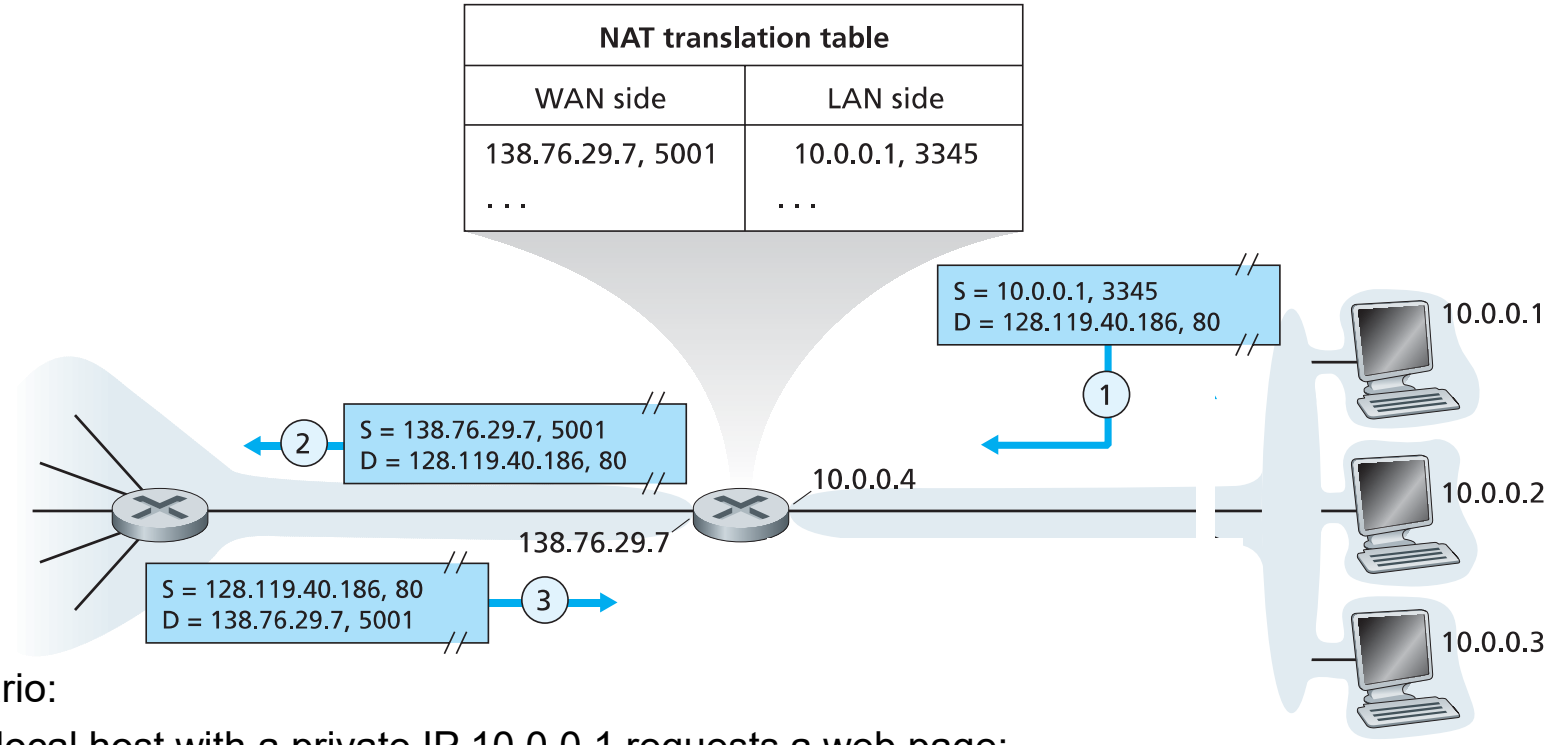
Network Address Translation (NAT): The Principle of Work



Scenario:

1) A local host with a private IP 10.0.0.1 requests a web page;
2) That host assigns to its IP datagram request an arbitrary source port number, e.g. 3345;
3) IP datagram is sent into LAN;
4) Router receives it, replaces the private IP 10.0.0.4 with its public IP 138.76.29.7, as well as generates a random new port number, e.g. 5001;
5) Router adds an entry into its NAT table, that port 5001 corresponds to host 10.0.0.1, and sends the modified IP datagram into the global network;
6) A destination host knows nothing, that an IP datagram has been modified;

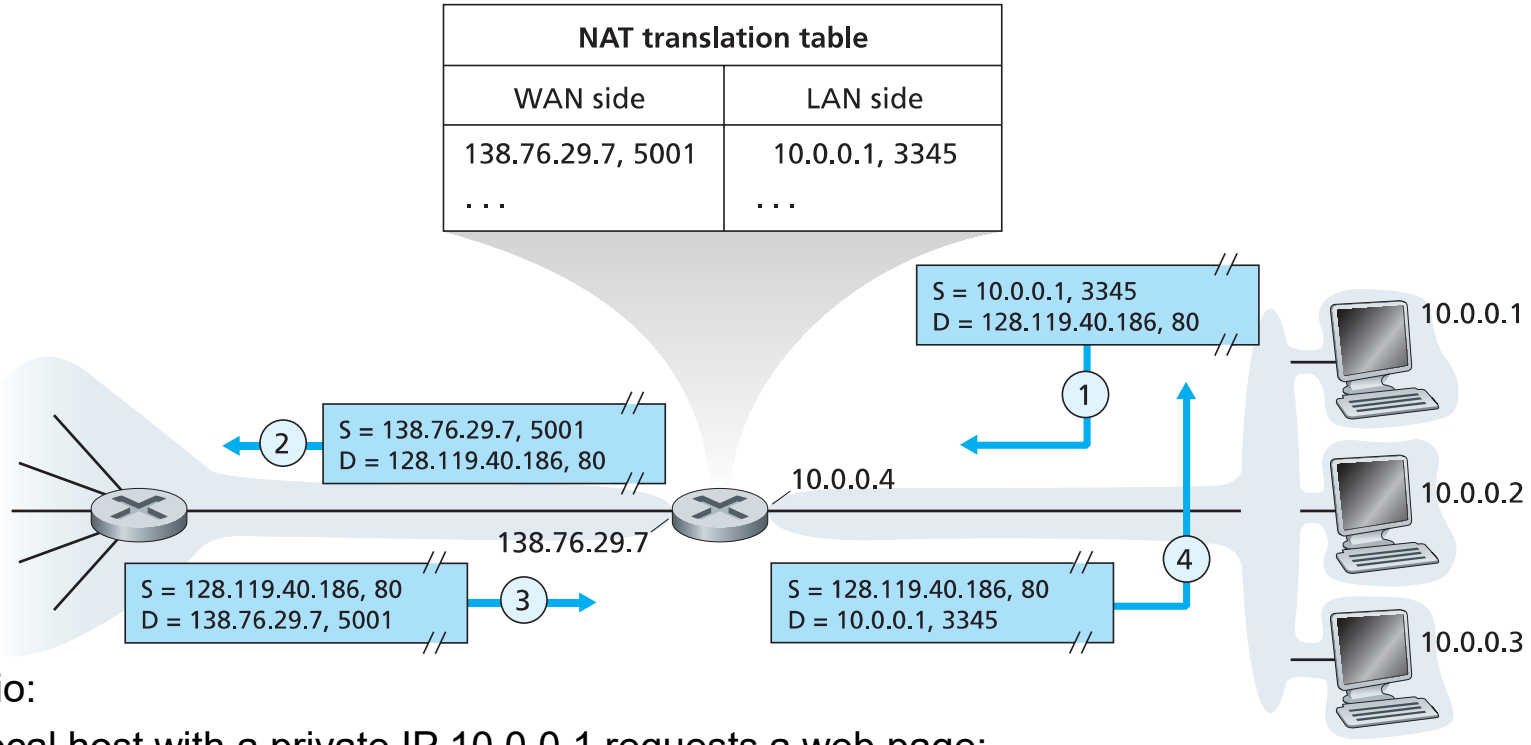
Network Address Translation (NAT): The Principle of Work



Scenario:

1) A local host with a private IP 10.0.0.1 requests a web page;
2) That host assigns to its IP datagram request an arbitrary source port number, e.g. 3345;
3) IP datagram is sent into LAN;
4) Router receives it, replaces the private IP 10.0.0.4 with its public IP 138.76.29.7, as well as generates a random new port number, e.g. 5001;
5) Router adds an entry into its NAT table, that port 5001 corresponds to host 10.0.0.1, and sends the modified IP datagram into the global network;
6) A destination host knows nothing, that an IP datagram has been modified;
7) When a response comes back to the router, it checks the port number, and determines a local IP from its NAT table

Network Address Translation (NAT): The Principle of Work



Scenario:

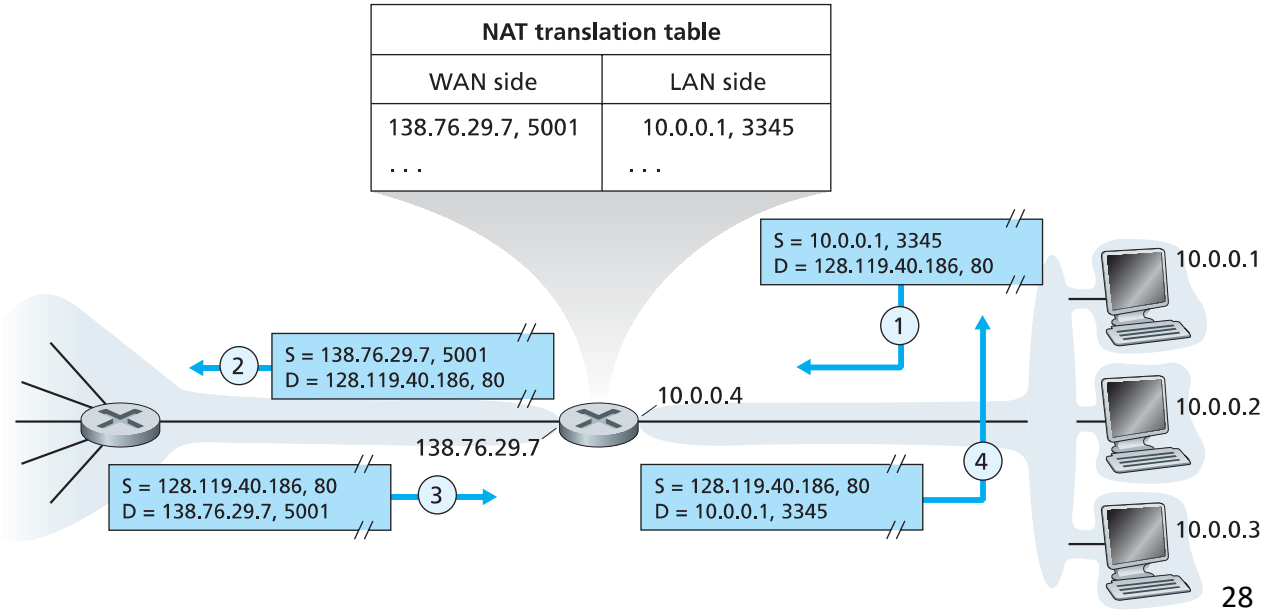
1) A local host with a private IP 10.0.0.1 requests a web page;
2) That host assigns to its IP datagram request an arbitrary source port number, e.g. 3345;
3) IP datagram is sent into LAN;
4) Router receives it, replaces the private IP 10.0.0.4 with its public IP 138.76.29.7, as well as generates a random new port number, e.g. 5001;
5) Router adds an entry into its NAT table, that port 5001 corresponds to host 10.0.0.1, and sends the modified IP datagram into the global network;
6) A destination host knows nothing, that an IP datagram has been modified;
7) When a response comes back to the router, it checks the port number, and determines a local IP from its NAT table

Key advantages of NAT:

- A reduced number of public IP addresses needed;
- An increased security for local hosts

Objections against NAT:

- The misuse of ports (Ports should be used to address processes, not hosts);
- Routers should process packets up to layer 3 (not to modify IP and port number);
- The violation of the end-to-end communication concept;
- IPv6 should be used, to overcome shortage of IPv4 addresses, rather than using such tricks;
- NAT interferes with P2P applications (P2P file sharing, P2P voice-over-IP, as these apps need to establish a direct TCP connection)



Key advantages of NAT:

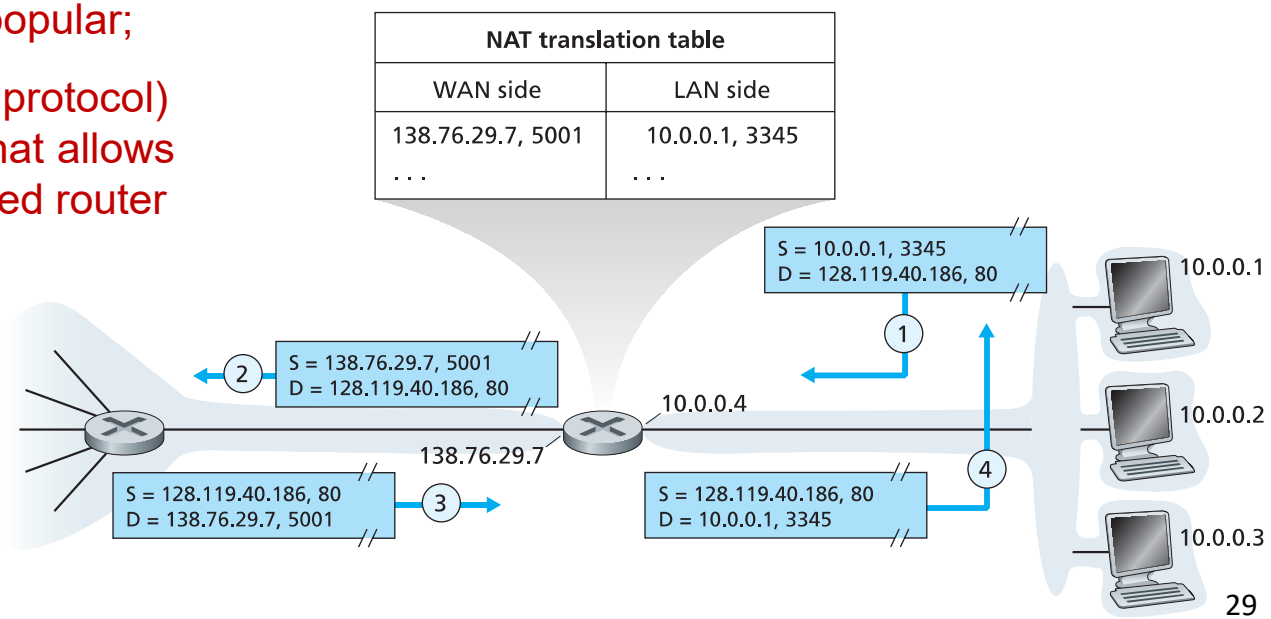
- A reduced number of public IP addresses needed;
- An increased security for local hosts

Objections against NAT:

- The misuse of ports (Ports should be used to address processes, not hosts);
- Routers should process packets up to layer 3 (not to modify IP and port number);
- The violation of the end-to-end communication concept;
- IPv6 should be used, to overcome shortage of IPv4 addresses, rather than using such tricks;
- NAT interferes with P2P applications (P2P file sharing, P2P voice-over-IP, as these apps need to establish a direct TCP connection)

Anyway, NAT becomes widely popular;

UPnP (Universal Plug and Play protocol) has been recently introduced, that allows to discover a nearby NAT-enabled router

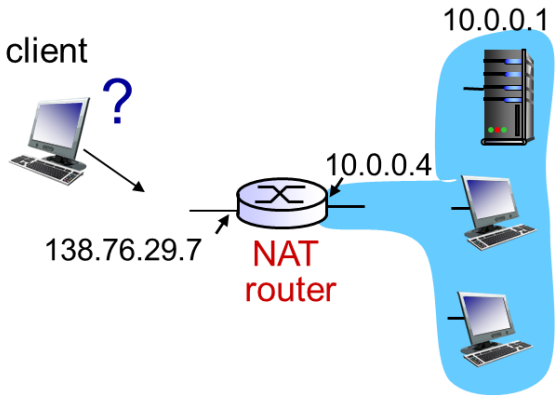


NAT Traversal Problem

- Client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can't use it as destination addr)
  - only one externally visible NATed address: 138.76.29.7

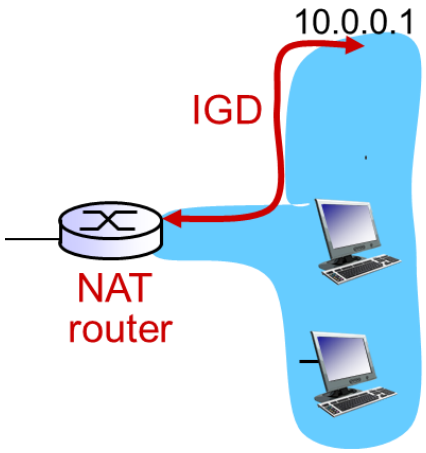
Solution1: statically configure NAT to forward incoming connection requests at given port to server

e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



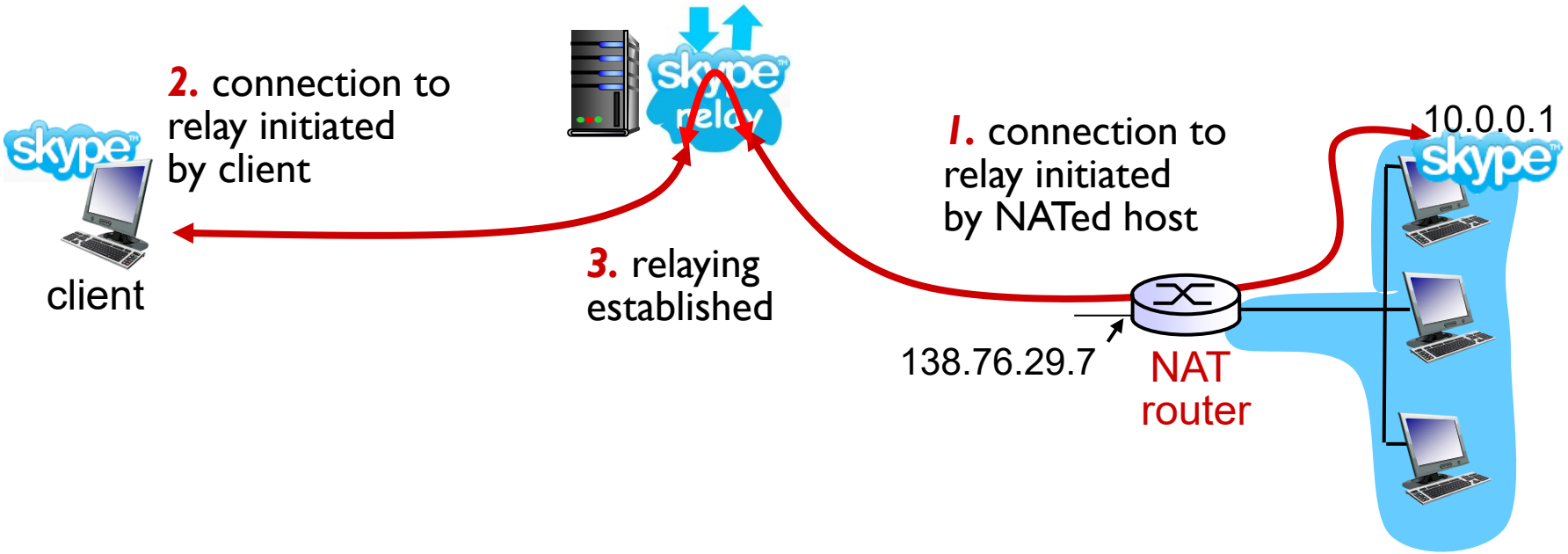
- *Solution 2:* Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATed host to:
  - learn public IP address (138.76.29.7)
  - add/remove port mappings (with lease times)

  i.e., automate static NAT port map configuration



NAT Traversal Problem

- *Solution 3:* relaying (used in Skype)
  - NATed client establishes connection to relay
  - external client connects to relay
  - relay bridges packets between to connections



Acknowledgment

These slides are prepared with the help of Artem Burmyakov and Muhammad Fahim