ELEN 4017

Network Fundamentals

Lecture 23 & 24

Purpose of lecture

Chapter 4: Network Layer

- Internet Protocol
  - IP Addressing (contd)
  - Network Address Translation (NAT)
  - ICMP

An example

- The ISP advertises to Internet that all addresses **beginning with 200.23.16.0/20** belong to it.
- Thus routers outside of ISP can use the single address prefix. This is called **address aggregation**.
- Consider now that Organization number 1 wants to move to ISPs-R-Us.
- What would happen?

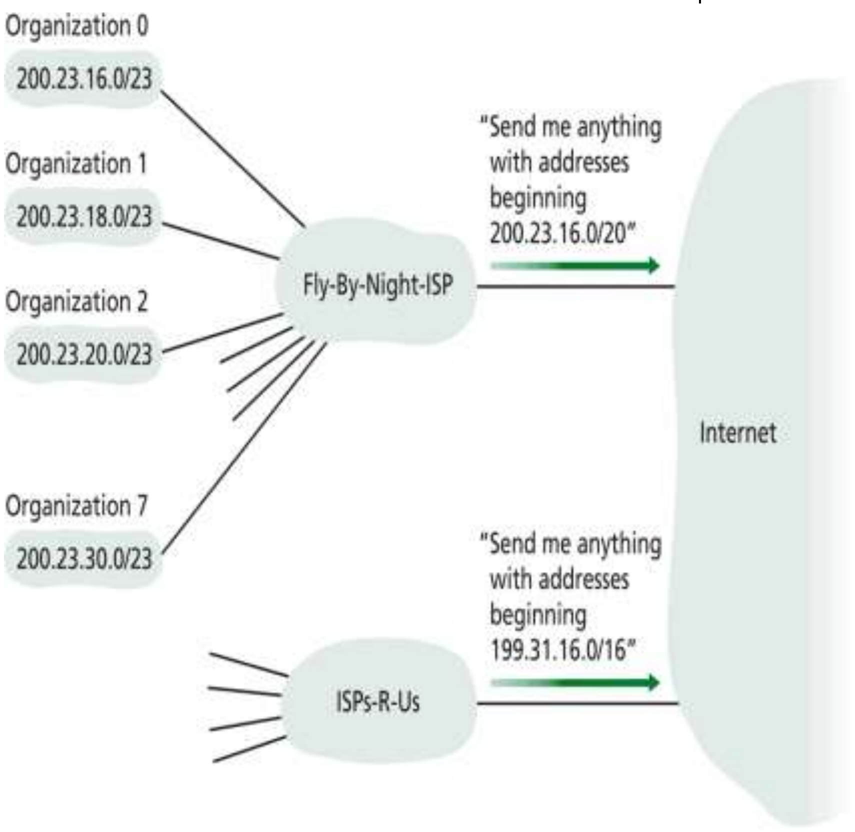


Figure 4.18 ♦ Hierarchical addressing and route aggregation

- In this case the ISPs-R-Us needs to amend their rule to include the new subnet.
- Importantly, Fly-By-Night does not need to change. Why?

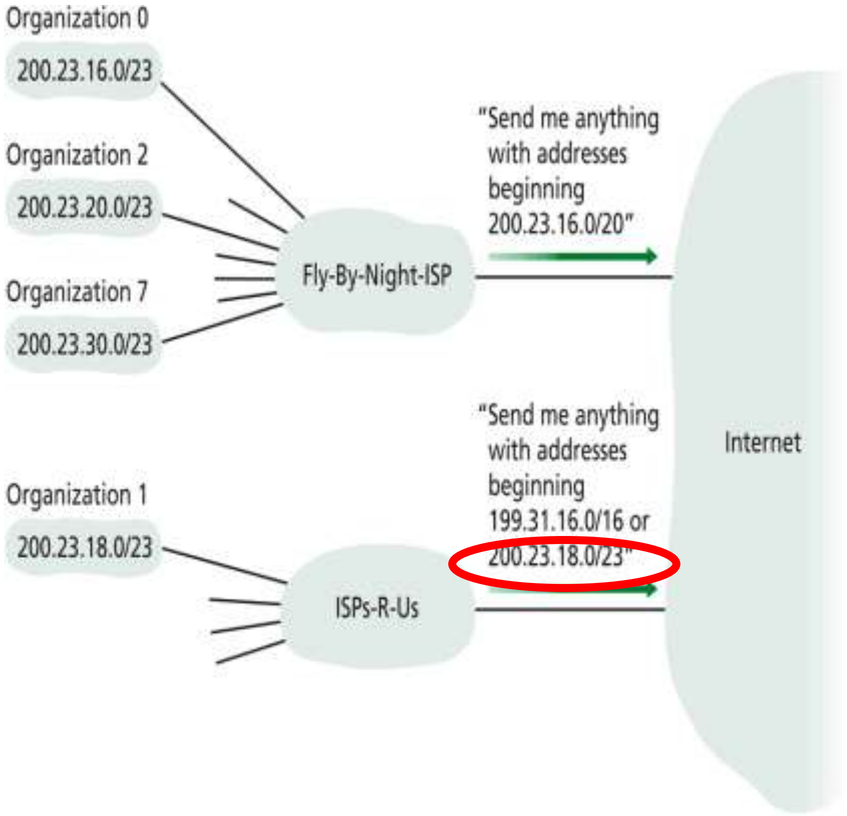


Figure 4.19 ♦ ISPs-R-Us has a more specific route to Organization 1

IP addressing: the last word...

Q: How does an ISP get block of addresses?

A: ICANN: Internet Corporation for Assigned Names and Numbers

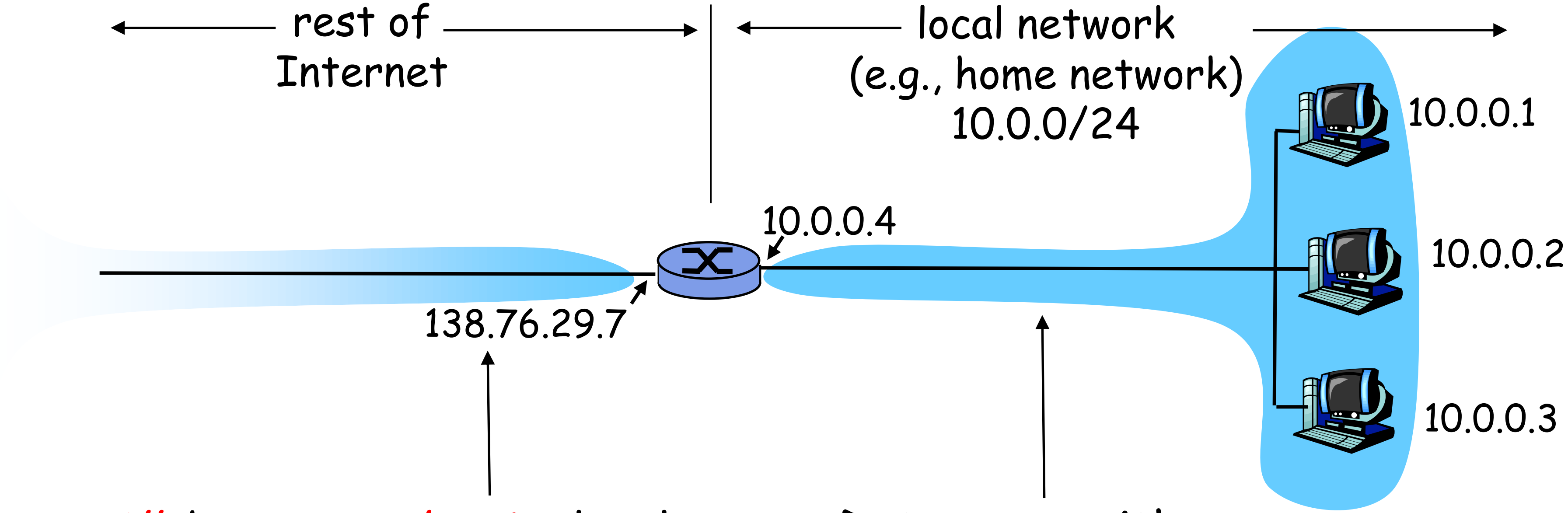
- allocates addresses
- manages DNS
- assigns domain names, resolves disputes

Purpose of lecture

Chapter 4: Network Layer

- Internet Protocol
  - IP Addressing (contd)
  - Network Address Translation (NAT)
  - ICMP

NAT: Network Address Translation



All datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7, **different source** port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT: Network Address Translation

- Motivation: local network uses just one IP address as far as outside world is concerned:
  - range of addresses not needed from ISP: just one IP address for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (**a security plus**).

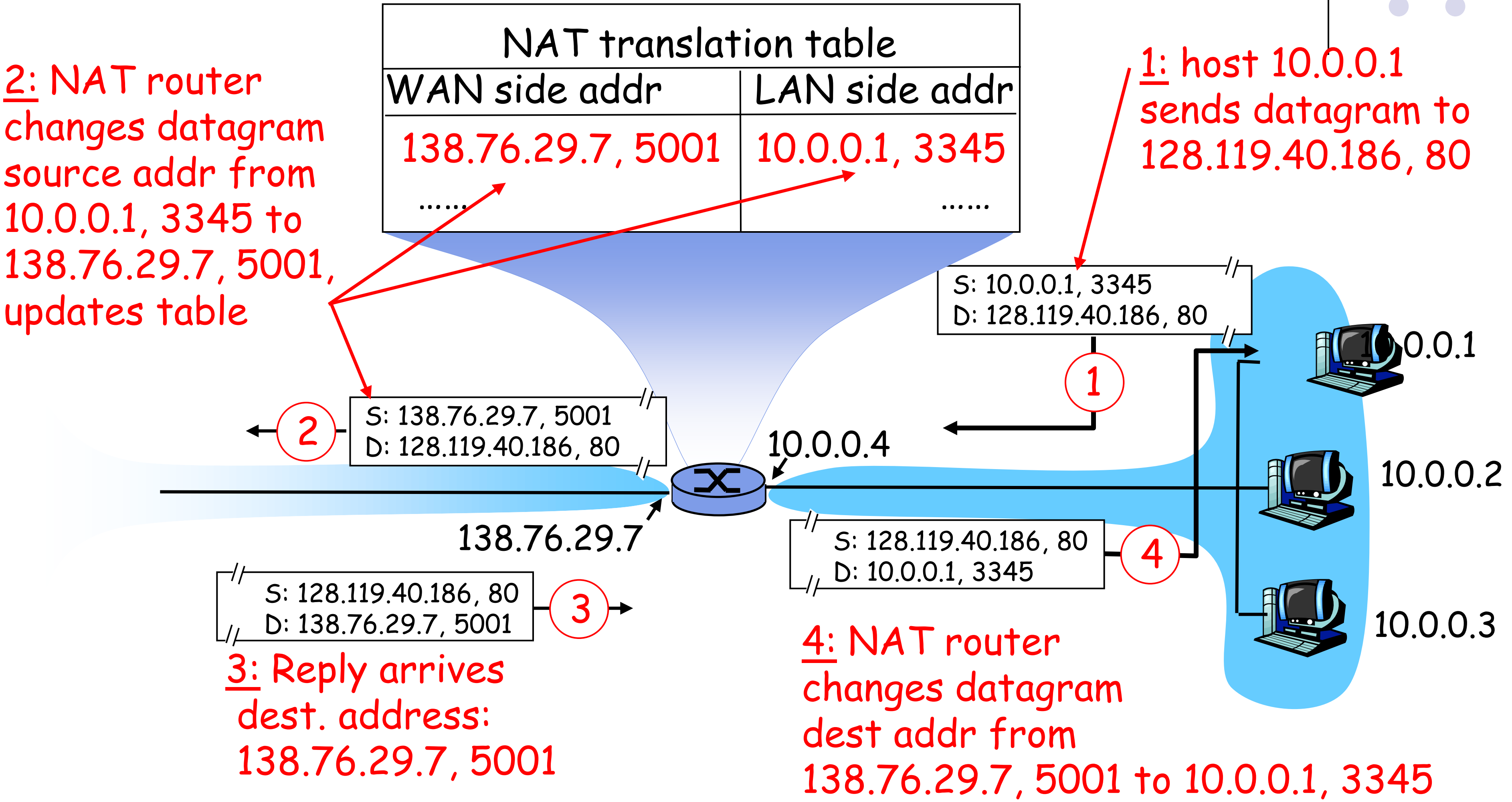
NAT: Network Address Translation

Implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)

  . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr.
- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair
- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: Network Address Translation



NAT translation table	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

1: host 10.0.0.1 sends datagram to 128.119.40.186, 80

S: 10.0.0.1, 3345
D: 128.119.40.186, 80

S: 138.76.29.7, 5001
D: 128.119.40.186, 80

S: 128.119.40.186, 80
D: 138.76.29.7, 5001

S: 128.119.40.186, 80
D: 10.0.0.1, 3345

3: Reply arrives dest. address: 138.76.29.7, 5001

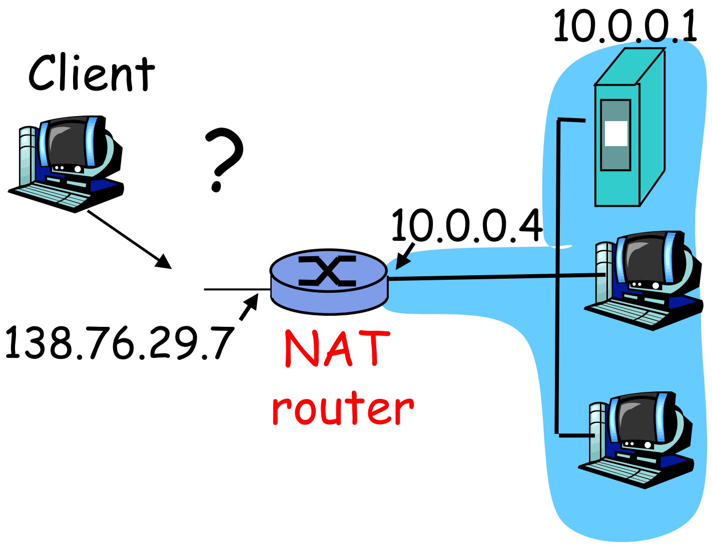
4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

NAT: Network Address Translation

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, eg, P2P applications
  - address shortage should instead be solved by IPv6

NAT traversal problem

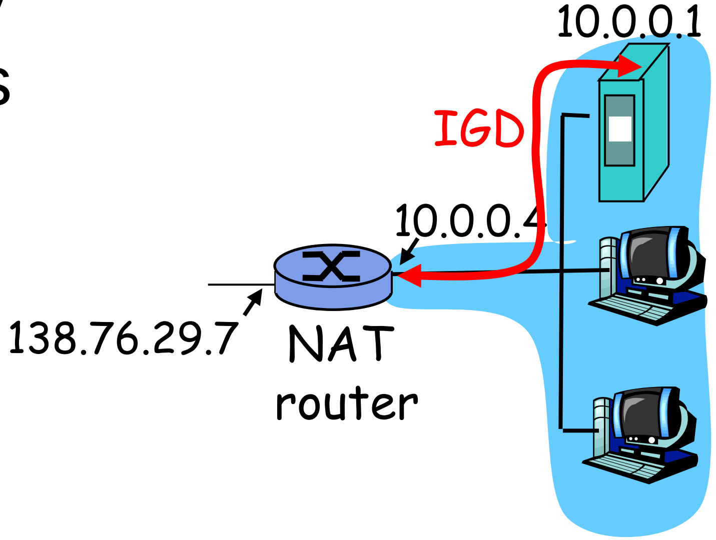
- client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client can’t use it as destination addr)
  - only one externally visible NATted address: 138.76.29.7
- solution 1: statically configure NAT to forward incoming connection requests at given port to server
  - e.g., (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



NAT traversal problem

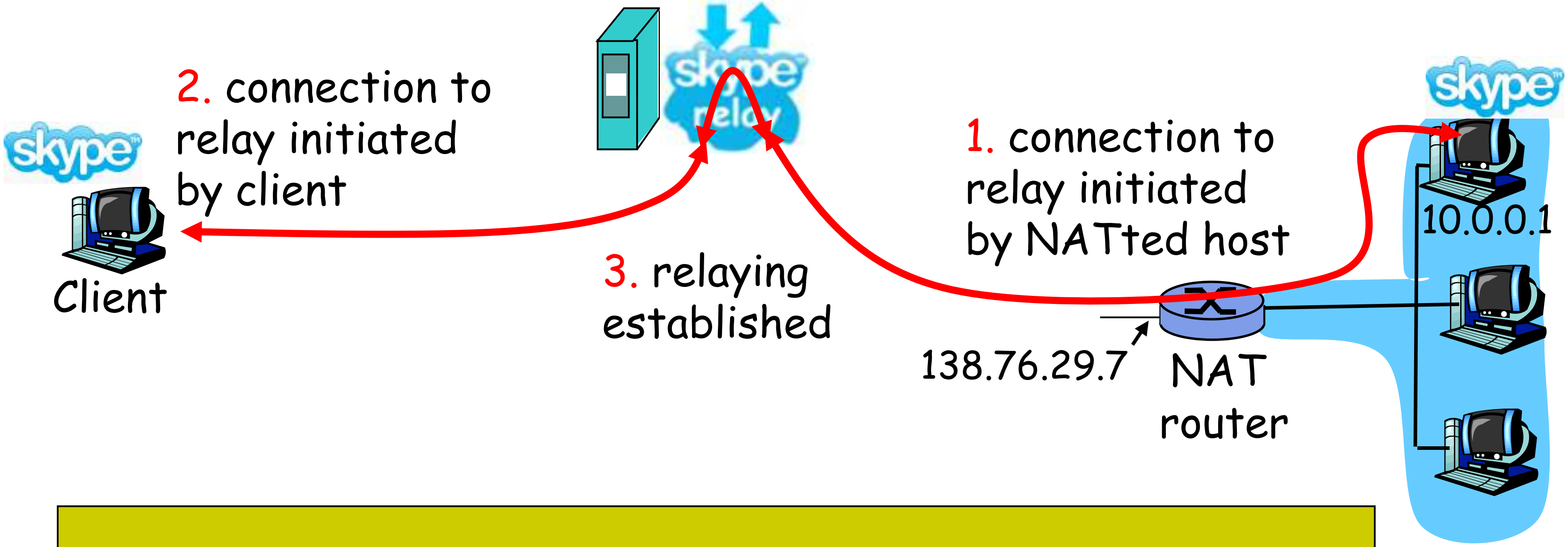
- solution 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Allows NATted host to:
  - learn public IP address (138.76.29.7)
  - add/remove port mappings (with lease times)

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



skype relay
2. connection to relay initiated by client
skype
Client
3. relaying established
1. connection to relay initiated by NATted host
skype
10.0.0.1
138.76.29.7
NAT router

Or if 1 client is not behind a NAT, can ask the other party to contact him directly

Purpose of lecture

Chapter 4: Network Layer

- Internet Protocol
  - IP Addressing (contd)
  - Network Address Translation (NAT)
  - ICMP

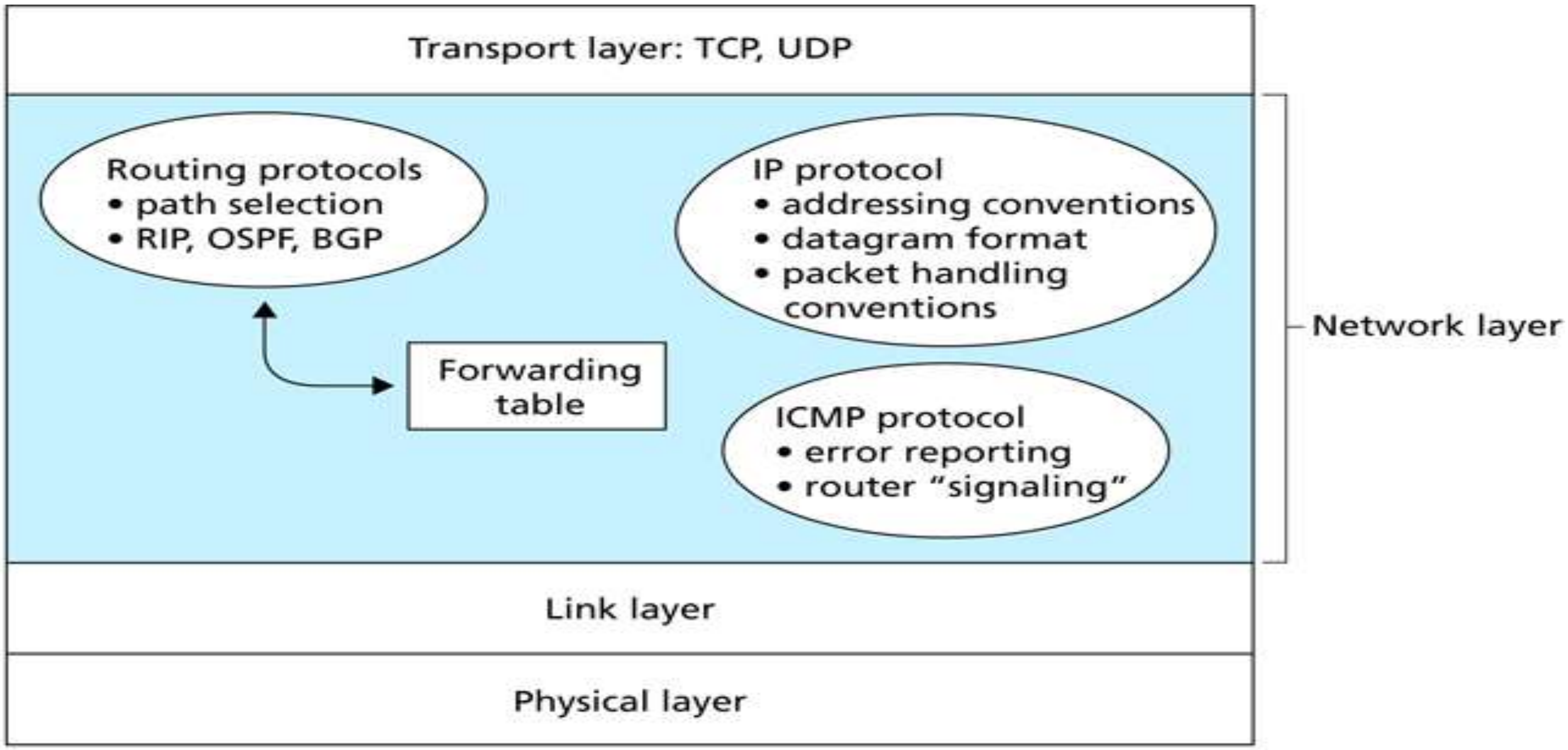
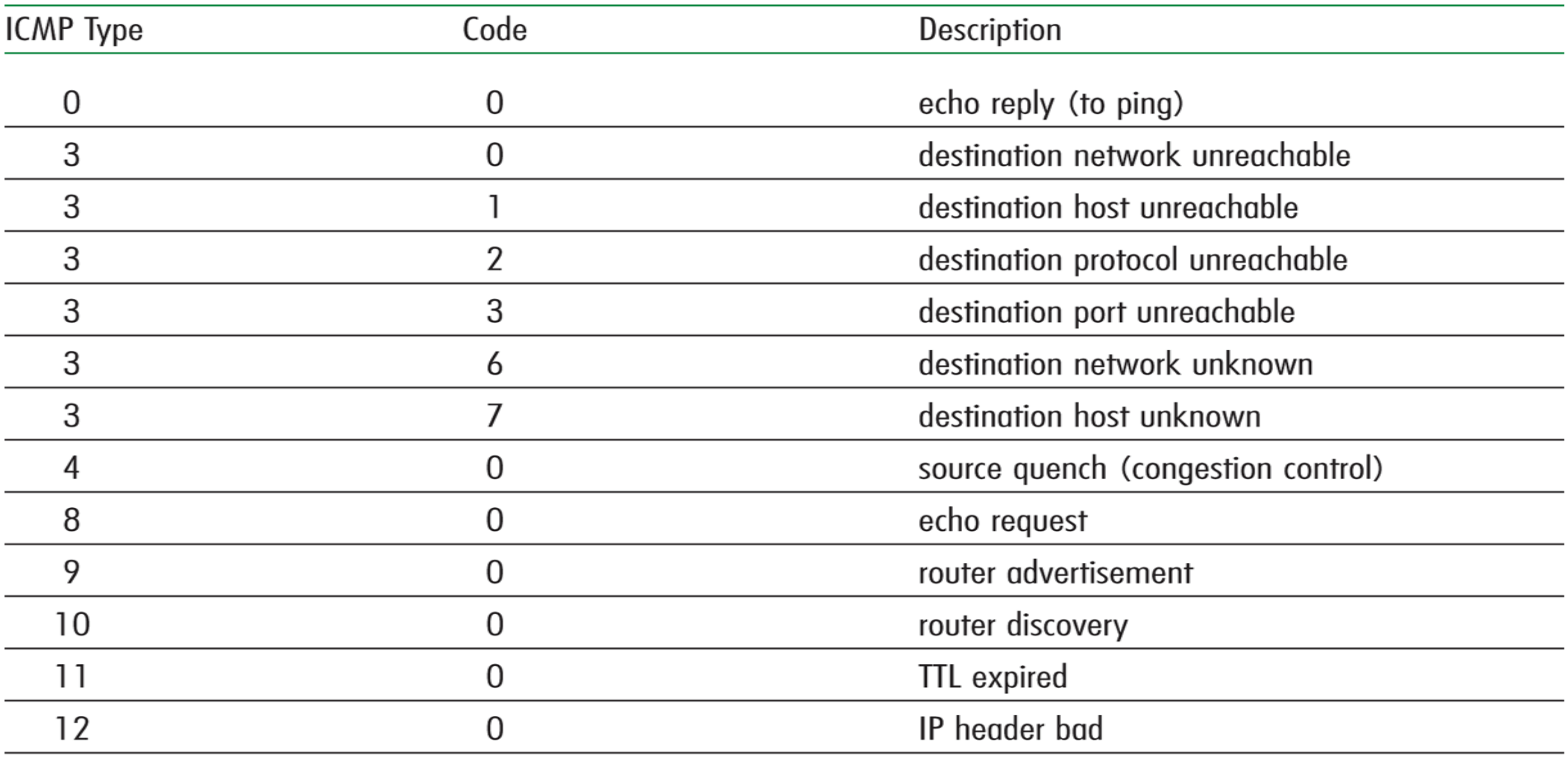


Figure 4.12 ♦ A look inside the Internet's network layer

ICMP

- ICMP is used by hosts and routers to communicate network layer information to each other.
- You have encountered the message **“Destination network not reachable”**. Originates from ICMP.
- At some point an IP router was unable to find a path to the host specified. That router **generated a type-3 ICMP message** and forwarded it to your host.
- ICMP is considered part of IP, but **strictly speaking it is just above IP**. This is because ICMP messages are carried over IP (similar to TCP/UDP).

ICMP Message Types



ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

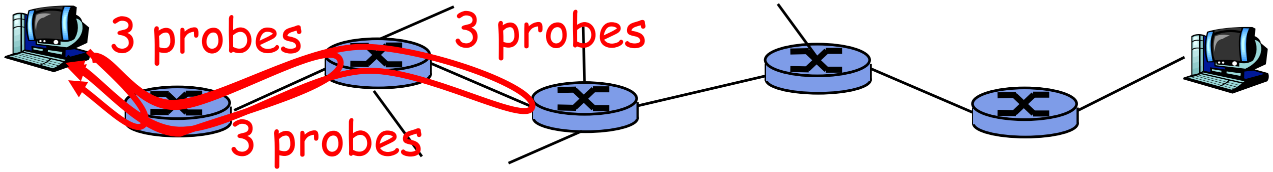
Figure 4.21 ◆ ICMP message types

Ping

- Ping is a tool to test if a host is reachable across a network.
- The client sends a **type-8 Code 0 (echo request)** message to a specified host.
- The destination server responds with an echo reply.
- Typically the OS also maintains a timer so that you can gauge the RTT for the ping.

Traceroute

- Traceroute is a program used to **trace the route** taken by an IP packet.
- It achieves its operation by **sending a series of IP datagrams to the destination using an unlikely port number**.
- Importantly it **increments the TTL value** for each datagram.
- Consider the **nth datagram reaching router n**. The router will detect that the **TTL has expired**, **discard the packet and send an ICMP warning message back to source (type 11 code 0).** This ICMP packet contains the **routers IP address**.
- This continues until the destination is reached and the port is unreachable.


3 probes
3 probes
3 probes