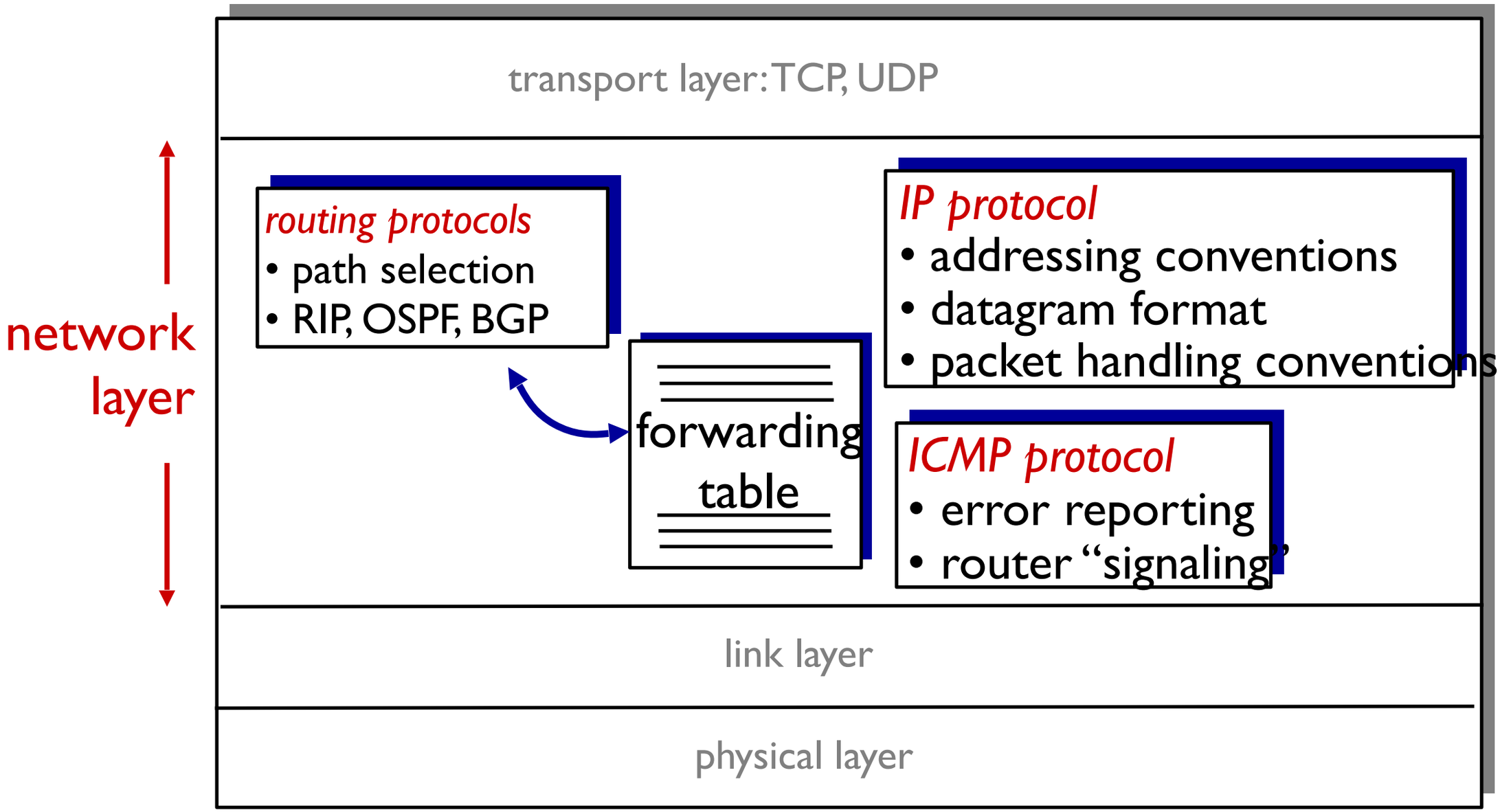
CN-Basic
L28

IP Packet Format

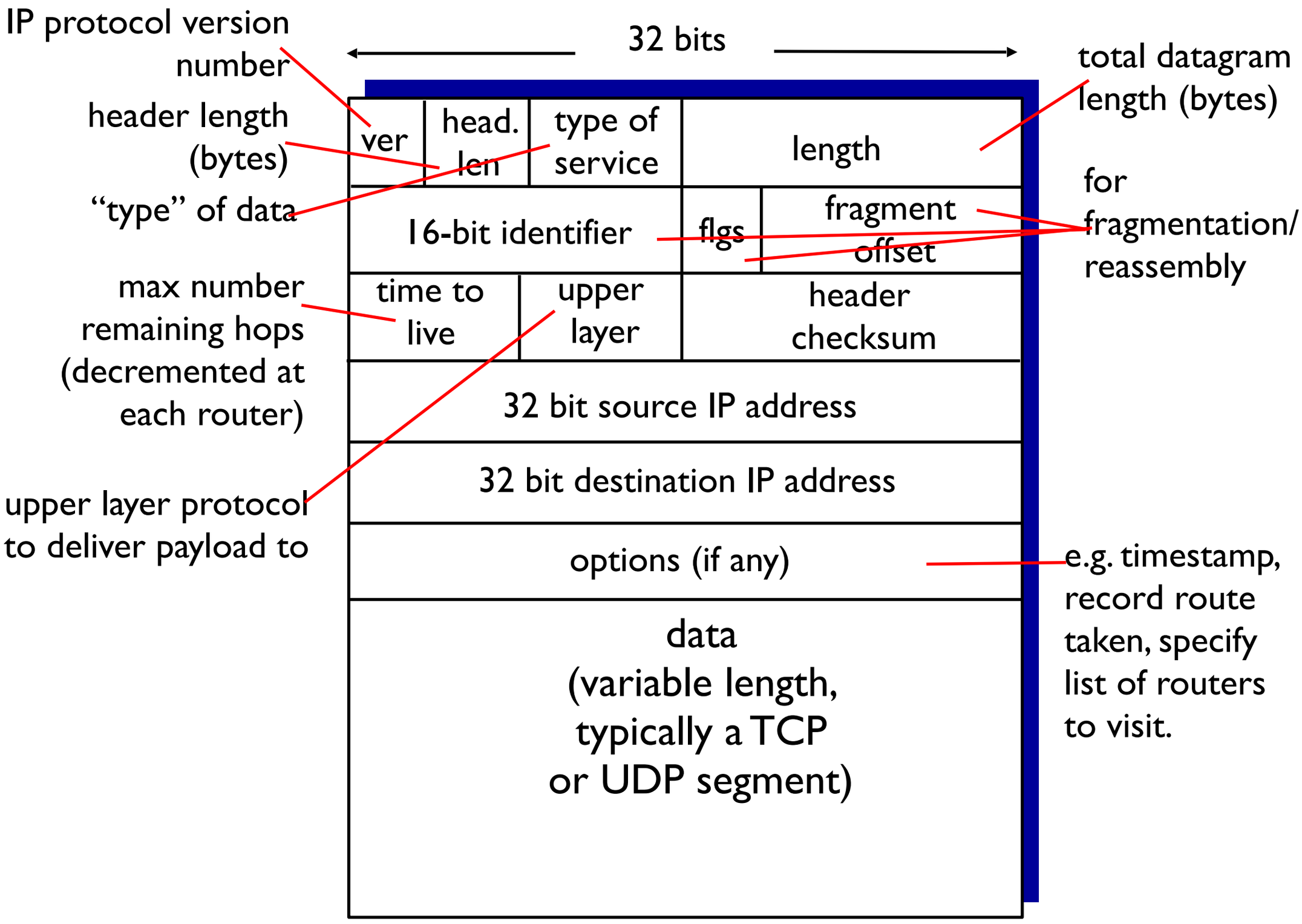
Dr. Ram P Rustagi
rprustagi@ksit.edu.in
http://www.rprustagi.com
https://www.youtube.com/rprustagi

The Internet network layer

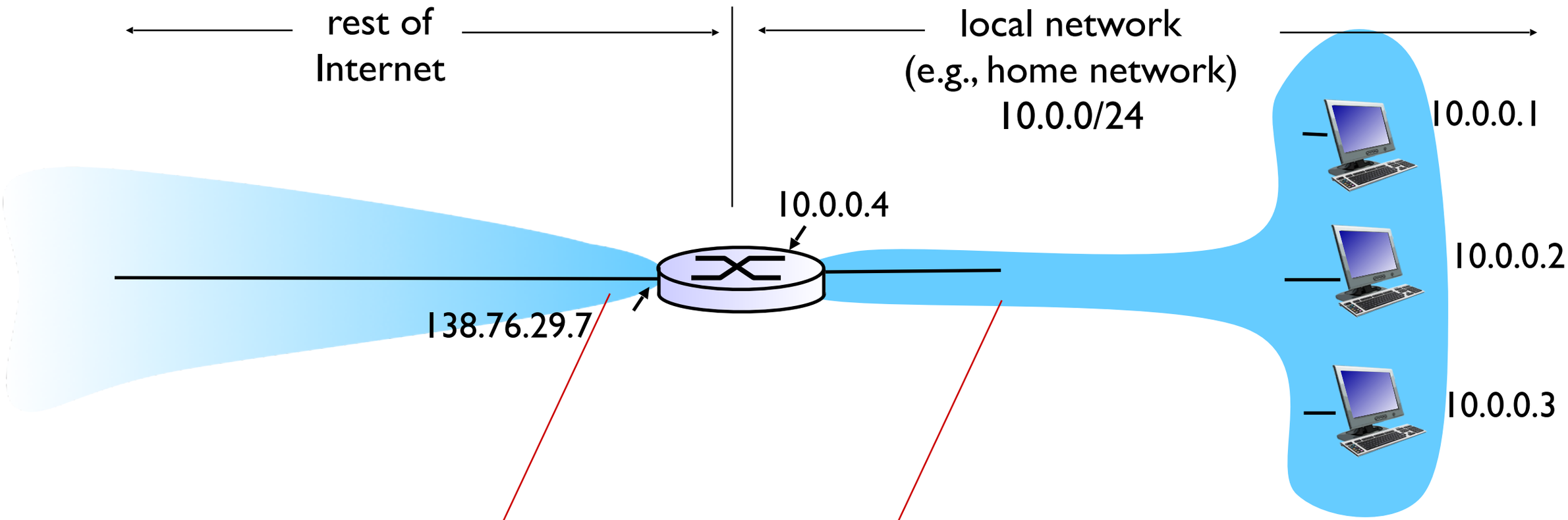
host, router network layer functions:



IP datagram format



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

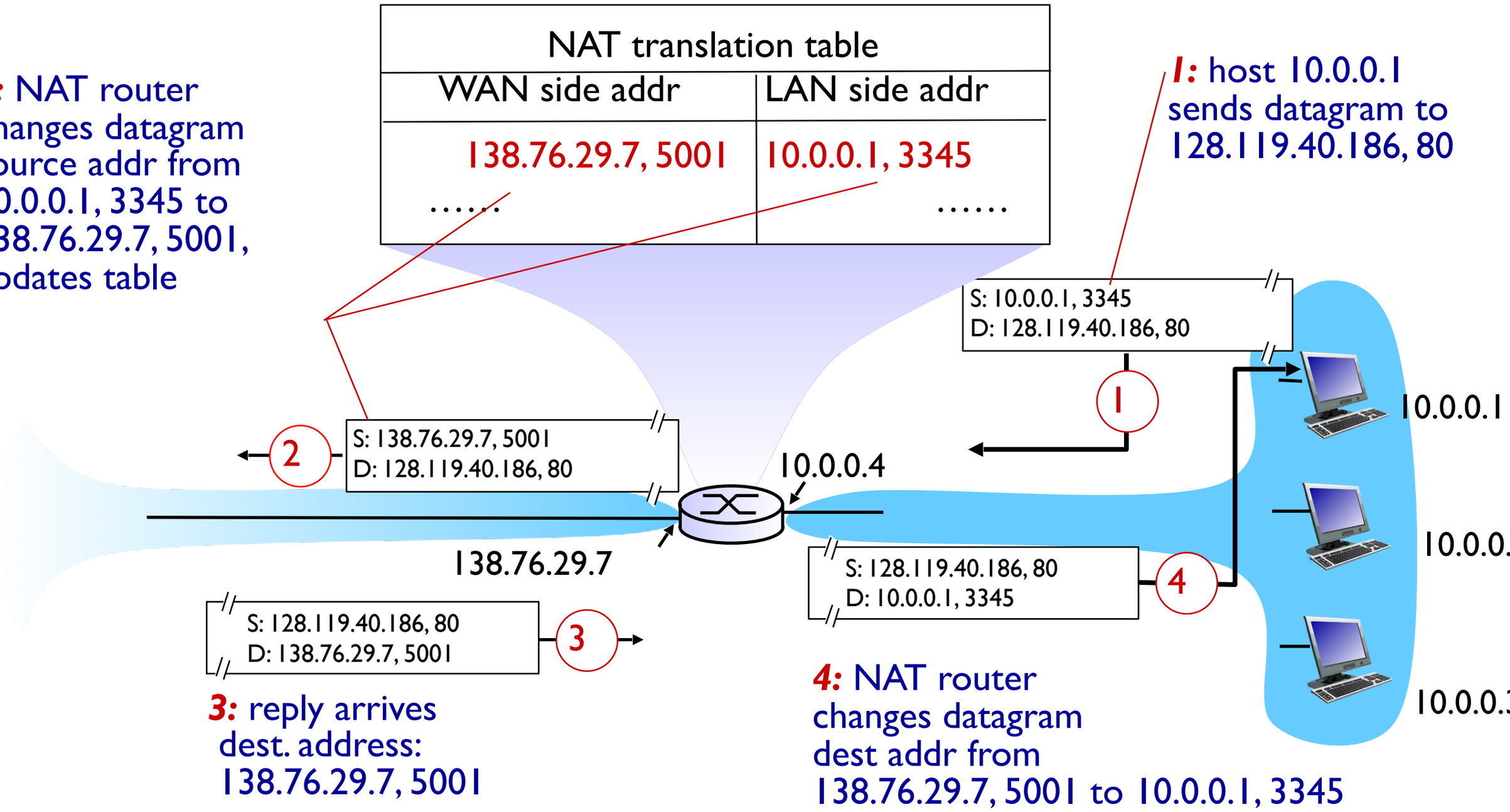
implementation: NAT router must:

- *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



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

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
  - address shortage should be solved by IPv6
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - NAT traversal: what if client wants to connect to server behind NAT?

ICMP: internet control message protocol

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Query Messages:

Type	Code	description
0/8	0	Echo reply/request (ping)
13/14	0	Timestamp request/reply
10/9	0	Router solicitation/advt

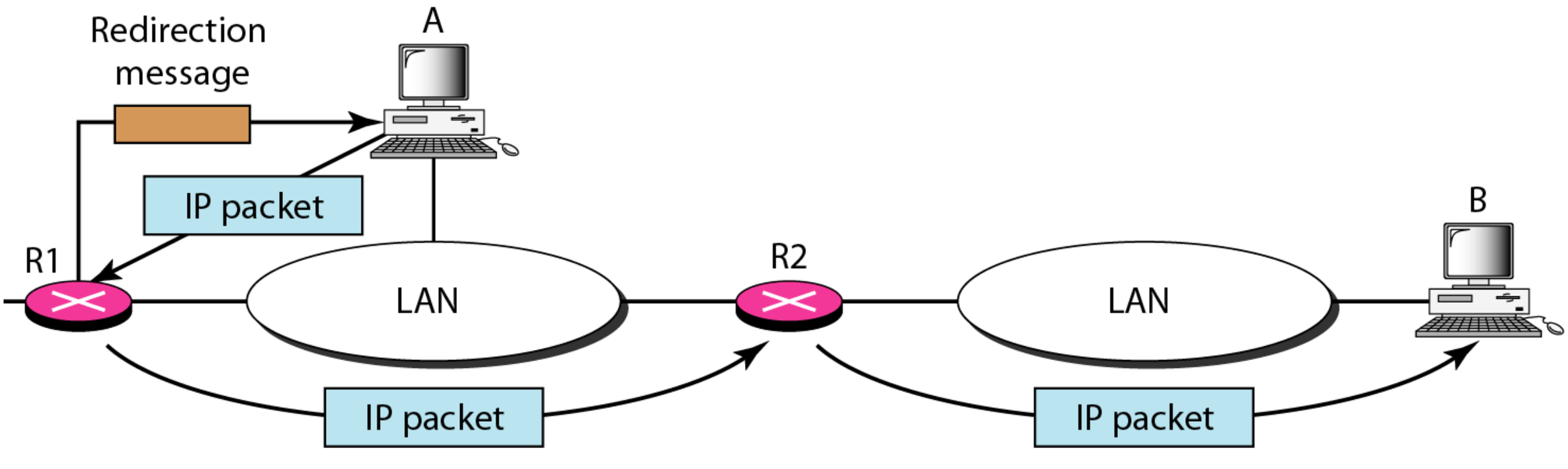
Error Reporting Messages

3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
5	0	Redirect
11	0	TTL expired
12	0	bad IP header

ICMP Messages

- Few points to note
  - –No ICMP error msg will be generated for
    - Response to datagram carrying an ICMP error message
    - Fragmented datagram that is not the first fragment
    - Datagram having multicast address
    - Datagram having special address e.g.
      - –`127.0.0.1`, or `0.0.0.0`

ICMP Redirect



Src: Forouzan - Data Communication and Networking

ICMP PMTU Discovery

- It is a mechanism
  - **It is not a protocol**
- Mechanism
  - Intermediate router informs the sender
    - error : destination not reachable
    - code : Fragmentation required
- IP Fragmentation is avoided in general
- Path MTU (PMTU) discovery is used
  - To find the max segment size for a given path
- Fragment is a costly process
  - Especially for NAT address
    - is configured by default in any enterprise

ARP - Address Resolution Protocol

- Packet delivery to a host requires two addresses
  - Logical address - IP Address
  - Physical address - MAC address
- Need to find mapping from logical to physical
  - ARP is used - RFC 826

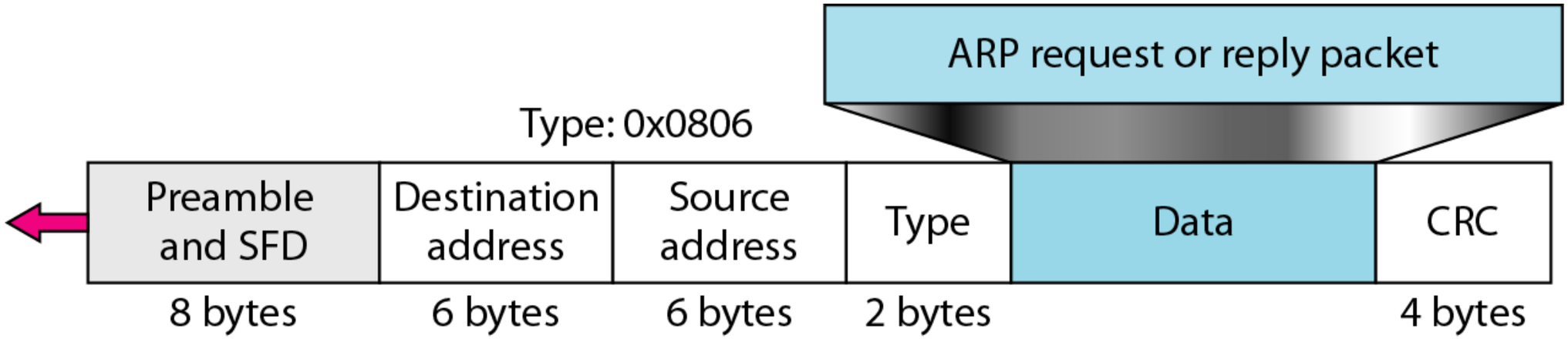
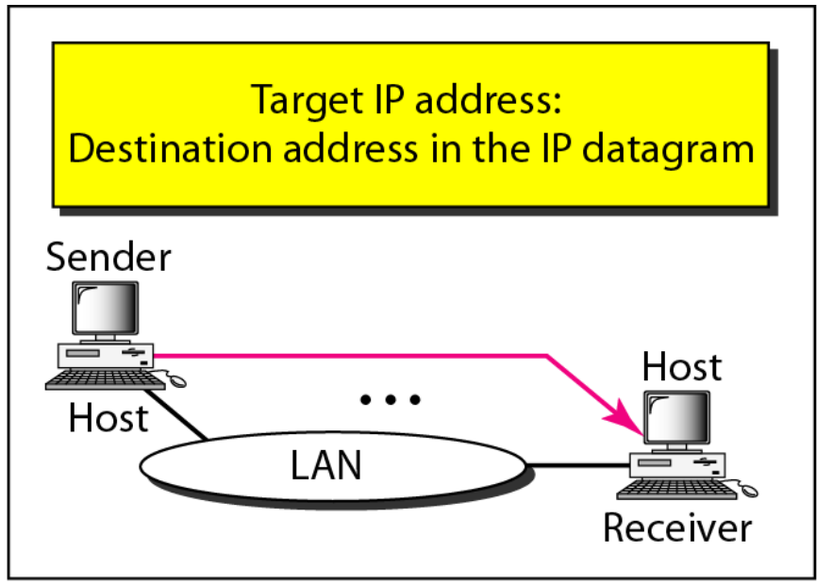
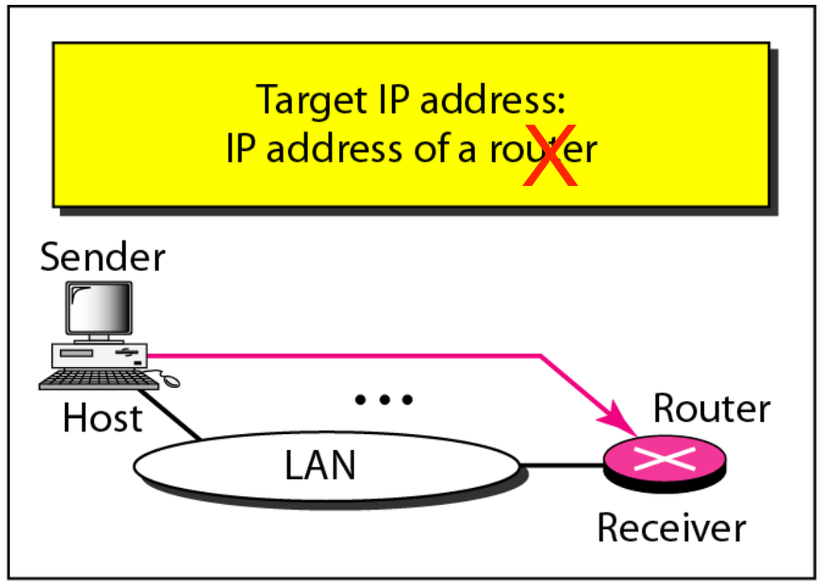


Fig Src: Forouzan - Data Communication and Networking, SIE

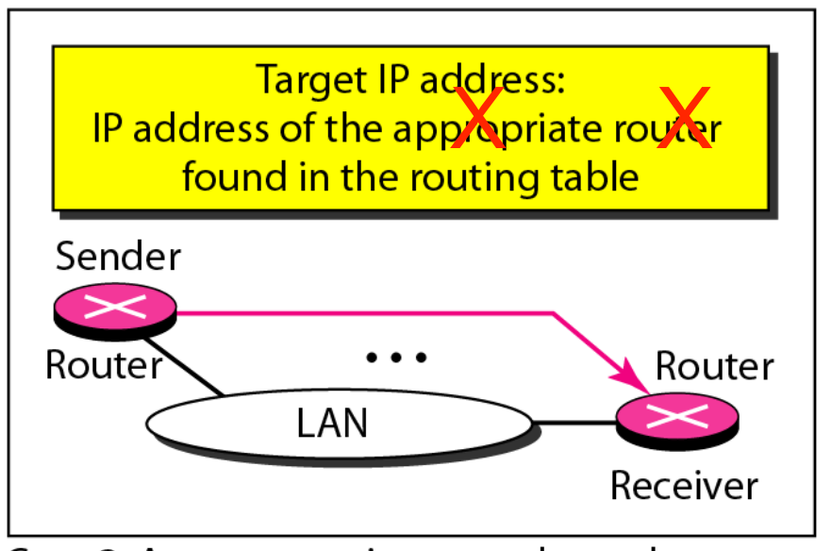
ARP - 4 cases



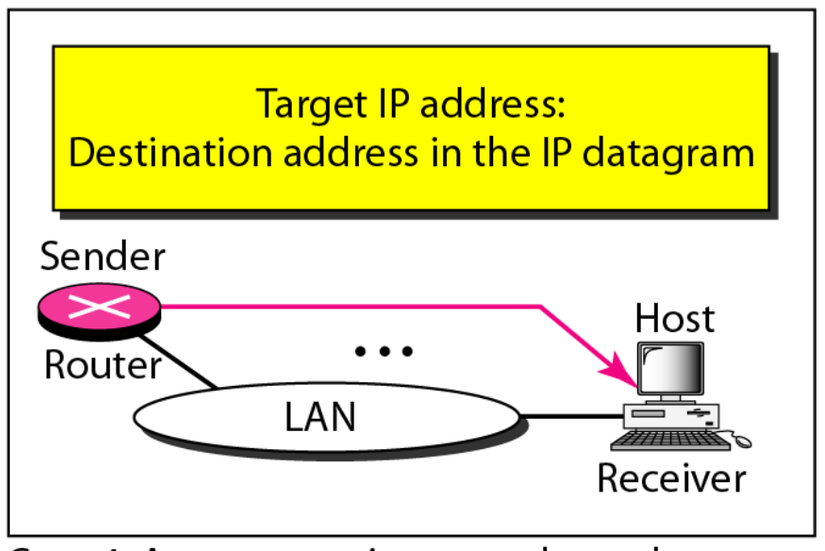
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

Src: Forouzan

ARP

- ARP Request and Reply
  - ARP Request is broadcast
  - ARP Reply is Unicast
- Other forms of ARP
  - Proxy ARP (RFC 1027)
  - Reverse ARP (RFC 903)
  - Gratuitous ARP

Reverse ARP

- Reverse ARP (RARP)
  - RFC 903
  - Used for diskless stations
- Organization does not have enough IP Address
  - Target as MAC Bcast does not cross the router
  - Needs one RARP server for each subnet
- BOOTP
  - Improvement over RARP
  - Has a relay agent to forward across network
  - Has static mapping of MAC to IP
    - Manageability issues
- DHCP - replaces BOOTP

Summary

- IP Packet Format
- ICMP
- NAT
- ARP
  - Reverse ARP
  - BOOTP
  - DHCP