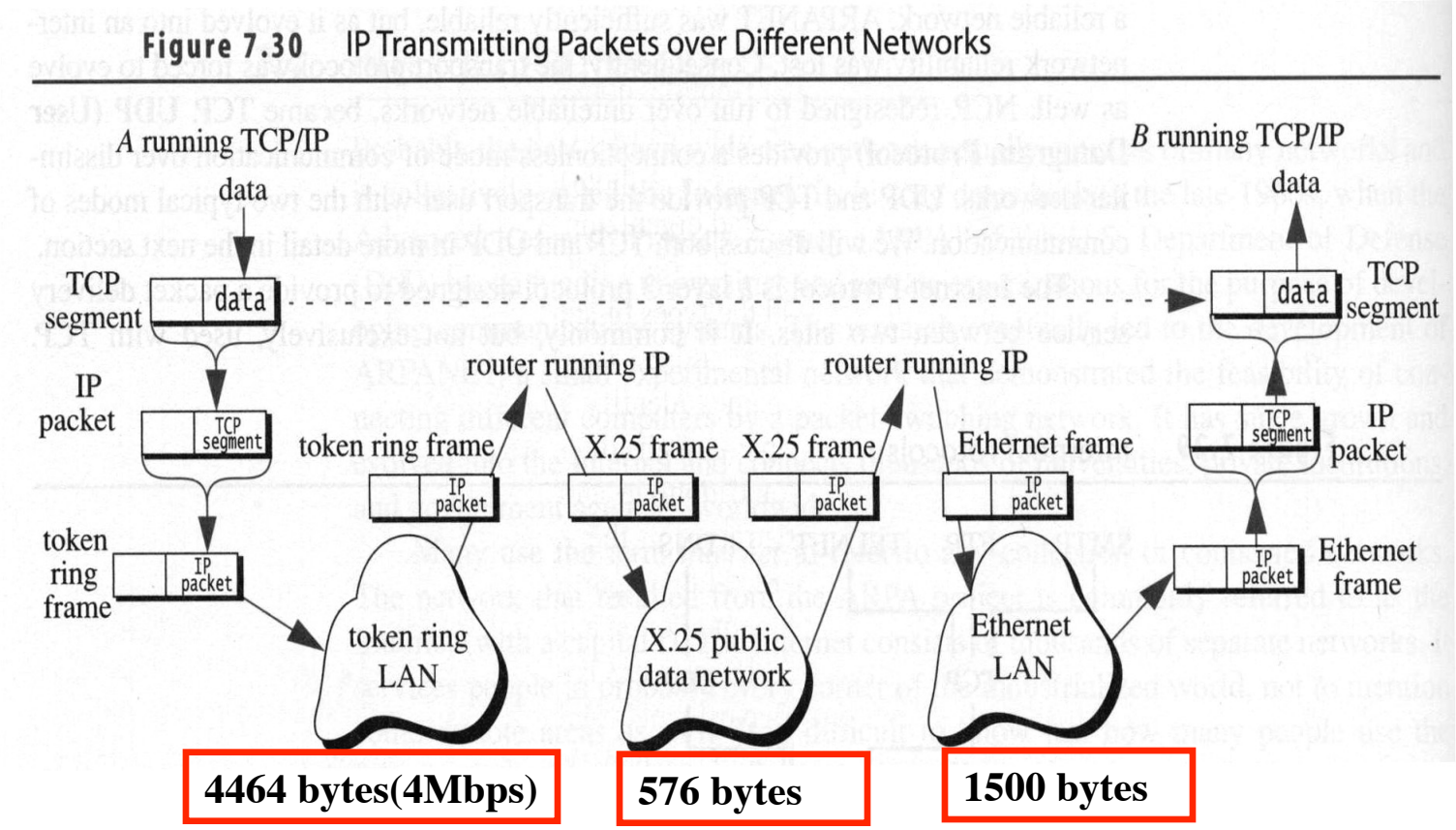
Lecture 18 Overview

- Last Lecture
  - Internet Protocol (1)
- This Lecture
  - Internet Protocol (2)
  - Source: chapters 19.1, 19.2, 22,1 22.2, 26.6
- Next Lecture
  - Transport Control Protocol (1)
  - Source: chapters 24.1, 24.3

IP - Internet Protocol

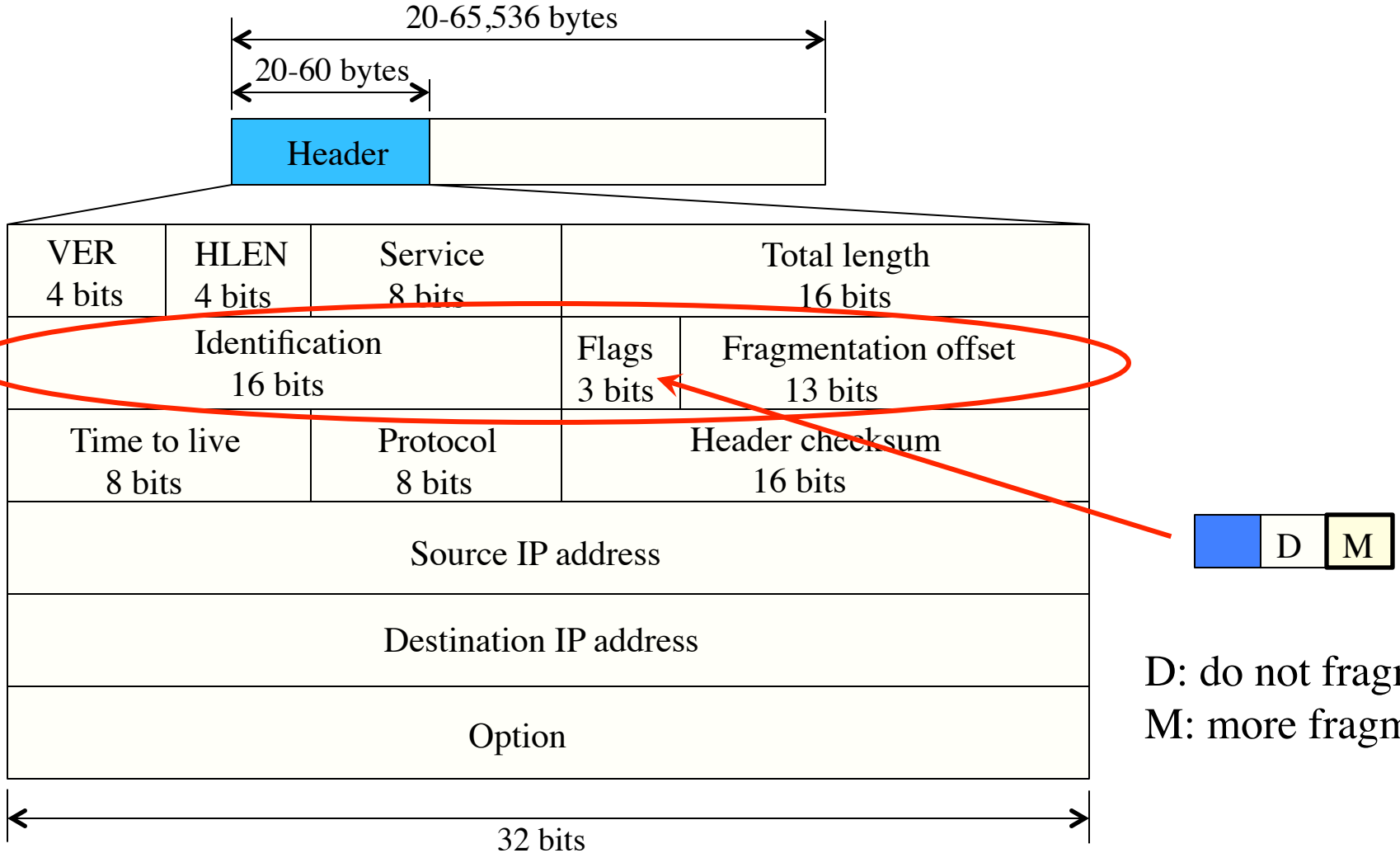
- Different networks allow different maximum packet sizes. Those sizes are called **maximum transfer units (MTUs)**.



Fragmentation

- If an IPv4 router receives a packet larger than the MTU of the network, it must break up the packet into fragments.
- The identification, flags, and fragment offset fields are used in this process.
  - Identification – the identification of packet.
  - Flag field
    - The second bit is called the *do not fragment* bit
    - The third bit is called *more-fragments bit* (mfb), indicating if there are more fragments following the current one
  - Fragment offset field - offset of the fragment in the packet's data field (Units of 8 bytes)
- When fragmented, each fragment has its own header
  - Which fields in the header need to be changed?

IP Packet Format (revisit)



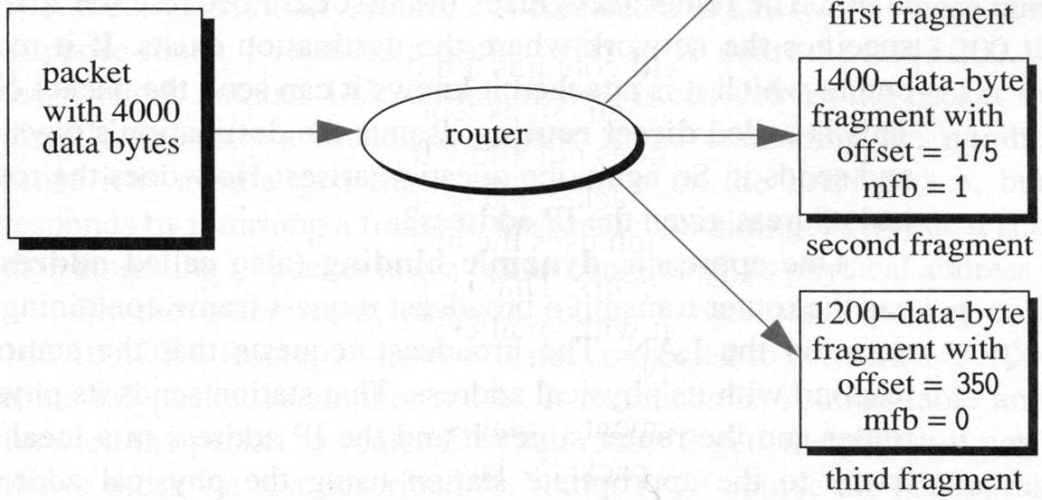
D: do not fragment
M: more fragments

Fragmentation (cont.)

Figure 7.34 Packet Fragmentation

MTU =1420

IP_Header =20



Fragments all have the same identification, source, and destination fields.

Demo: http://aboelela.site/profile/projects/net-seal/animations/ip-fragmentation/

Problems with IPv4

- Address depletion
  - 2^{32}=4.3 billion addresses
  - Many organizations got a class B network.
- Can not meet the requirement of multimedia applications
  - No constant bit rate guarantee
- Does not have good support for host mobility
- Not secure enough

IPv6

- IPv6 was developed to overcome these problems
  - Can co-exist with IPv4
- Major goals of IPv6
  - Make it possible for a host to roam without changing its address
  - Allow the protocol to evolve in the future
  - Permit the old and new protocols to coexist for years

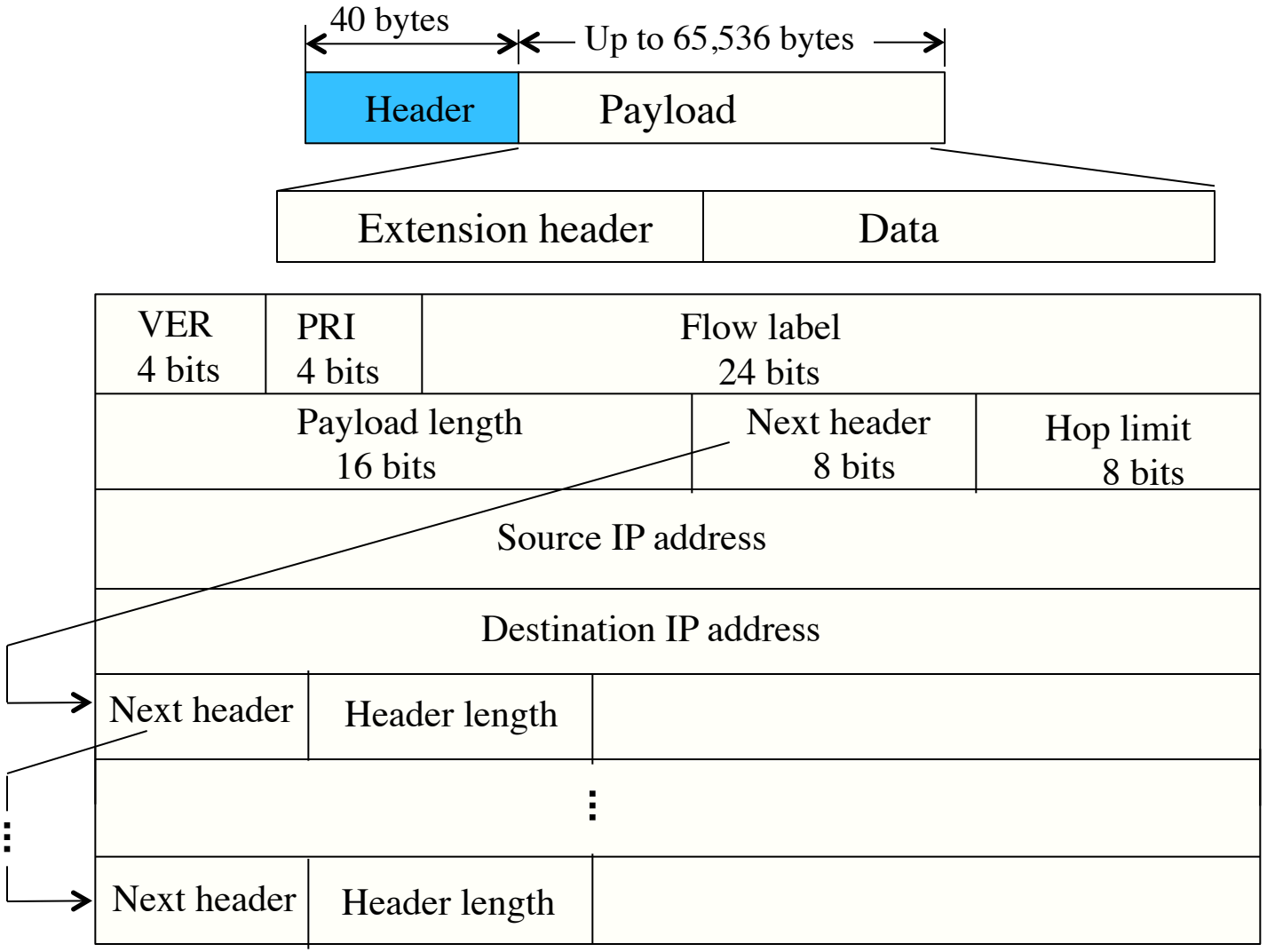
IPv6 Addresses

- IPv6 addresses are 128 bits long
  - Hexadecimal Colon Notation

    12AB:0000:0000:CD30:0000:0000:0000:0000
  - There are $2^{128} = 3*10^{38}$ in total.
  - If the entire earth, land and water, were covered with computers, IPv6 would allow $7*10^{23}$ IP addresses per square meter.
- Only a small part of the address space has been allocated so far.

https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

IPv6 Packet Format



IPv6 Packet Header

- Version field (4 bits)
  - Value 4 for IPv4; value 6 for IPv6
- Priority field (4 bits)
  - Used in congestion control. Values above 7 are for real-time or multimedia applications.
  - Low priority packets will have longer delay when congestion occurs.
- Flow label field (24 bits)
  - Allows a source and destination to set up a pseudoconnection with particular properties and requirements.
  - In effect, it attempts to combine the flexibility of a datagram and virtual circuit.

IPv6 Packet Header (cont.)

- Payload length field (16 bits)
  - Tells how many bytes follow the 40-byte header (max. 64k bytes)
- Next header field (8 bits)
  - Tells which of the six extension headers, if any, follows this one.
  - If this header is the last IP header, the Next header field tells which transport protocol handler (TCP/UDP) to pass the packet to.
- Hop limit field (8 bits)
  - Is the same as the time-to-live field in IPv4 and decrements on each hop.
  - When it hits zero, the packet is dropped.
- Source/Destination address fields (128 bits)

IPv6 Extension Headers

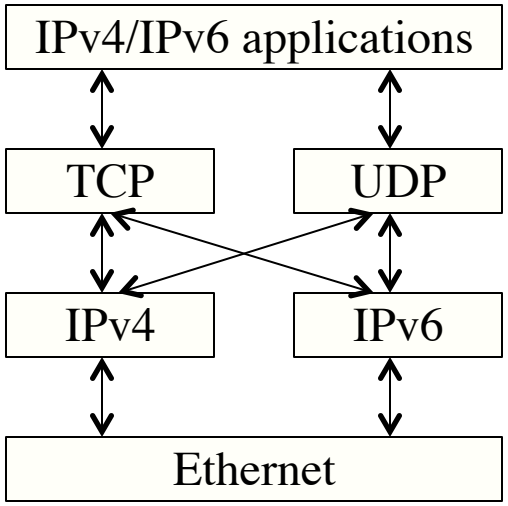
- IPv6 implements several extension headers to allow more options.
  - Authentication header - for IP authentication
  - Destination options - provides info for the destination
  - Fragmentation header - provides information in the event that packet fragments must be reassembled
    - Only the original source can fragment.
    - Intermediate routers cannot fragment.
  - Hop-by-hop header - provides information that each router must examine
  - Routing header - provides additional routing information
  - Security header - indicates the packet's payload has been encrypted

Differences Between IPv4 and IPv6

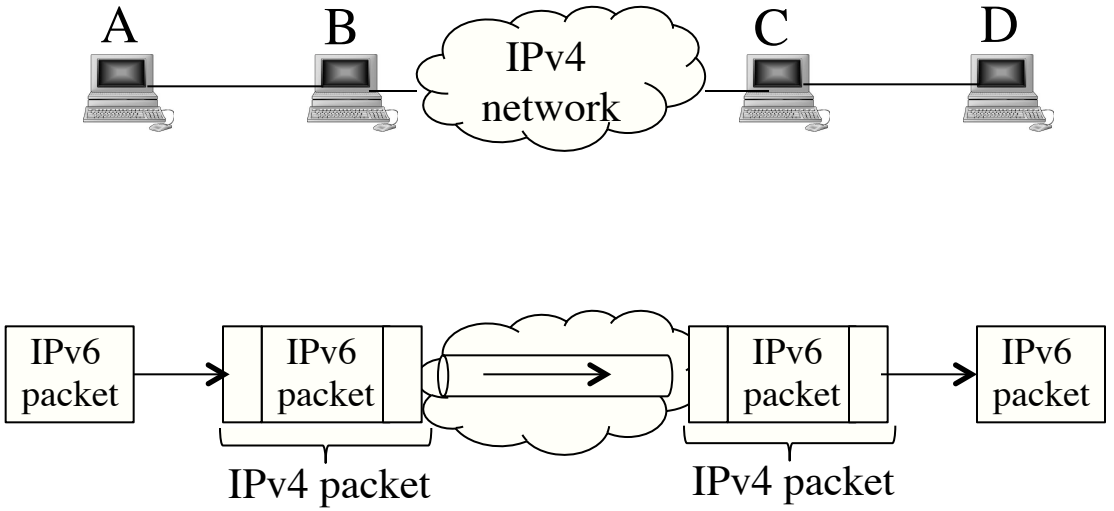
- IP address length
  - IPv4 addresses have 32 bits; IPv6 addresses have 128 bits
- Packet header
  - IPv4 header contains 13 fields. IPv6 has only 8 fields
  - No header checksum in IPv6
  - TTL is replaced by hop limit.
  - …
- Fragmentation is not allowed at routers in IPv6
- IPv6 has better support for options
- IPv6 supports more security (authentication and privacy)
- IPv6 pays more attention to type of service (flow label)
- …

Compatibility with IPv4

- IPv4 will still be around for some time.
- What happens when an IPv6 packet has to pass through a IPv4 router?



Dual stack



Tunnelling

Domain Name System (DNS)

- Converts IP names (ASCII strings) into IP addresses.
- A hierarchical, domain-based naming scheme implemented using a distributed database system.

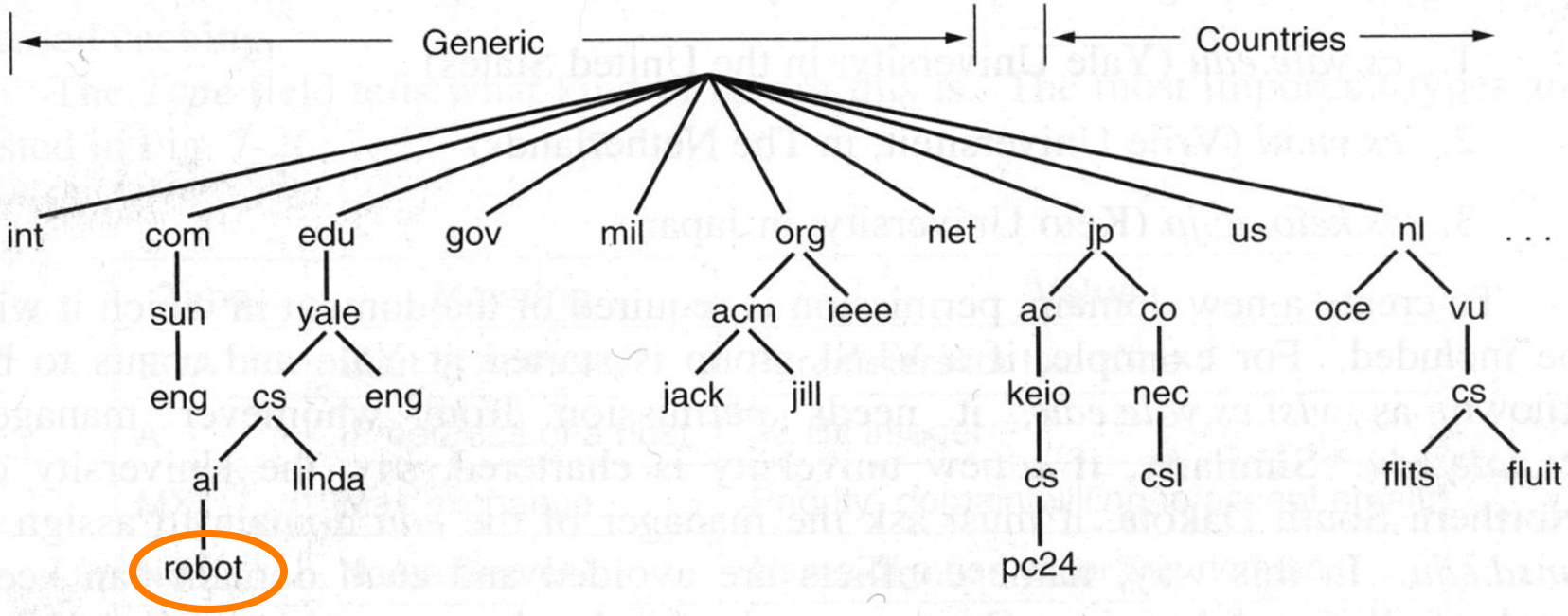


Fig. 7-25. A portion of the Internet domain name space.

DNS (cont.)

- DNS Name Space
  - Divided into non-overlapping zones.
  - Each zone contains some part of the tree and also contains name servers holding the information about that zone.

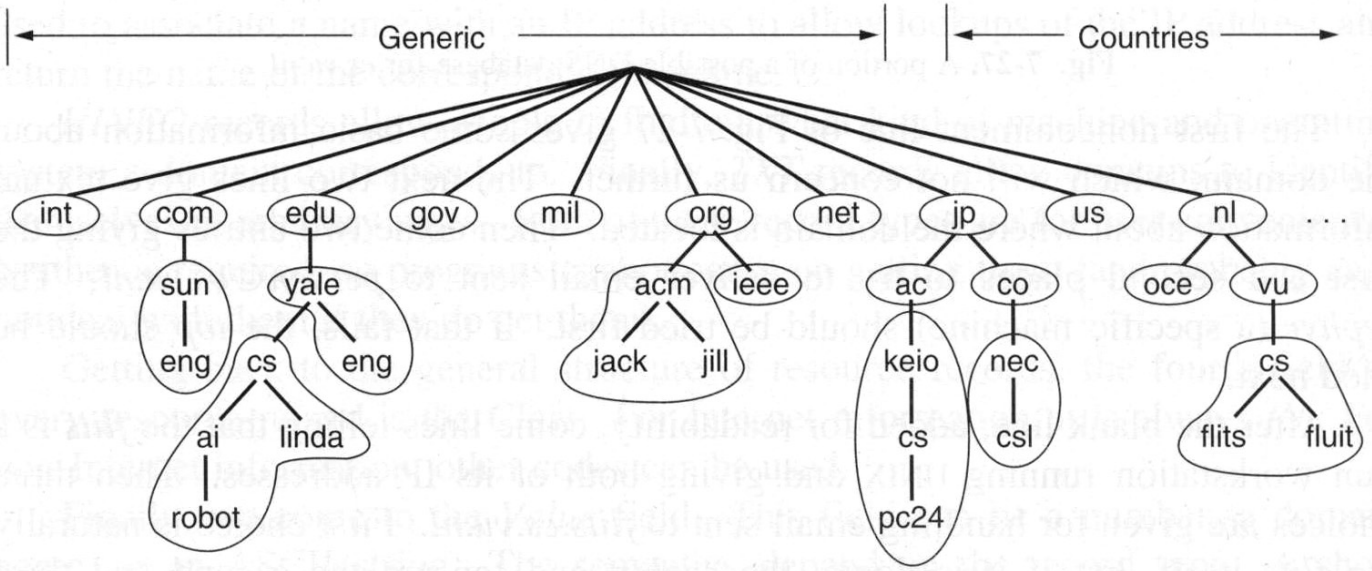


Fig. 7-28. Part of the DNS name space showing the division into zones.

DNS (cont.)

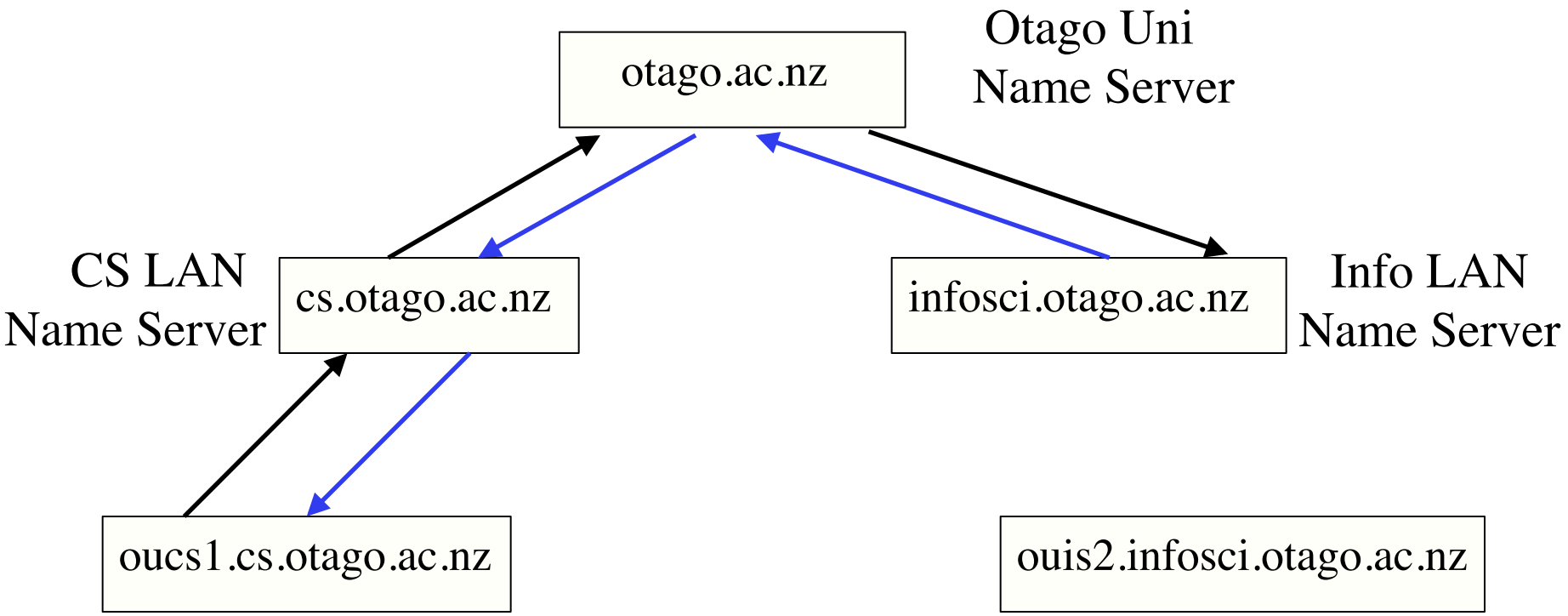
- DNS database is distributed among the name servers.
  - Each zone has at least one name server which maintains a file containing IP names and addresses of all workstations in the zone.
  - There are 13 root level name servers that know all the top level name servers.
  - Recursive Resolution
    - If a host has a query about an IP name, it passes the query to one of the local name servers.
      - If the IP name falls under the zone of that name server, it returns the IP address of the name to the host.
      - If the IP name is remote and no info about the name is available, the name server sends a query to another server (the parent usually) and wait for response.
    - The same procedure is repeated until the query is finally resolved. Then the response travels back to the requesting client.

DNS (cont.)

- Example
  - A host `oucs1.cs.otago.ac.nz` wants to know the IP address of the host `ouis2.infosci.otago.ac.nz`
  - `oucs1.cs.vu.nl` sends a query to the local name server `cs.otago.ac.nz`. Since `ouis2.infosci.otago.ac.nz` is a remote host, `cs.otago.ac.nz` knows nothing about it.
  - The server `cs.otago.ac.nz` sends the query to a upper-level name server `otago.ac.nz.`
  - The `otago.ac.nz` server may not know `ouis2.infosci.otago.ac.nz`, but it at least knows its child `infosci.otago.ac.nz`. So it sends the query to the name server `infosci.otago.ac.nz`, which has the requested information and sends the answer hop by hop back to the originator `oucs1.cs.otago.ac.nz`

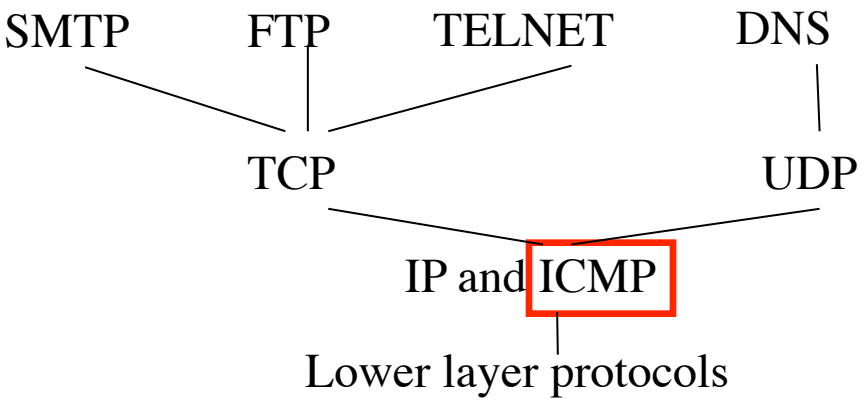
DNS (cont.)

Recursive Resolution



Internet Control Message Protocol (ICMP)

- When a router receives an IP packet and finds errors, what should it do?



  - ICMP is used by the routers to report errors and unexpected events, test the state of the network, perform congestion control, and router updates.
  - The Internet is closely monitored by the routers using ICMP.
  - Congestion control is performed using choke packets.

Internet Control Message Protocol (cont.)

- Typical control messages sent by ICMP:
  - Destination unreachable
  - Time exceeded
  - Parameter problem
  - Source quench
  - Redirect
  - Echo request
  - Echo reply
  - Timestamp request
  - Timestamp reply

Summary

- Packet fragmentation
- IPv6
- DNS
- ICMP