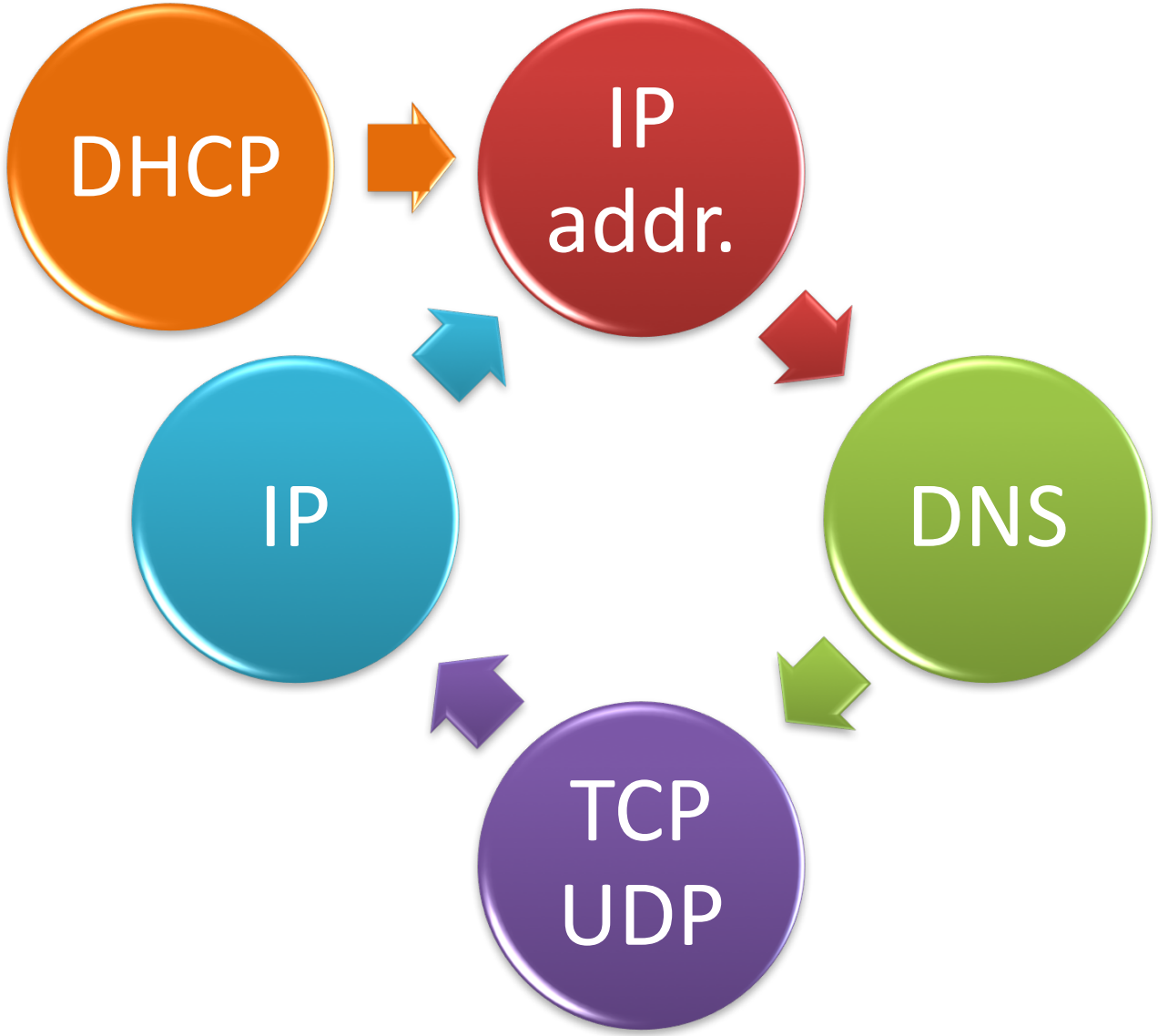
Higher layer protocols

- DHCP
- DNS
- Real time applications
- RTP

The hen or the egg?

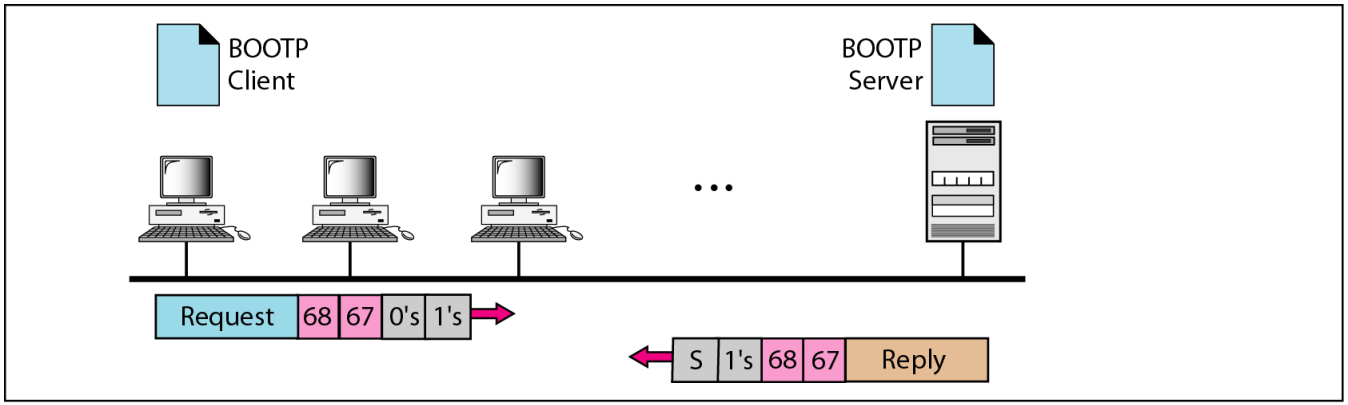


What to configure

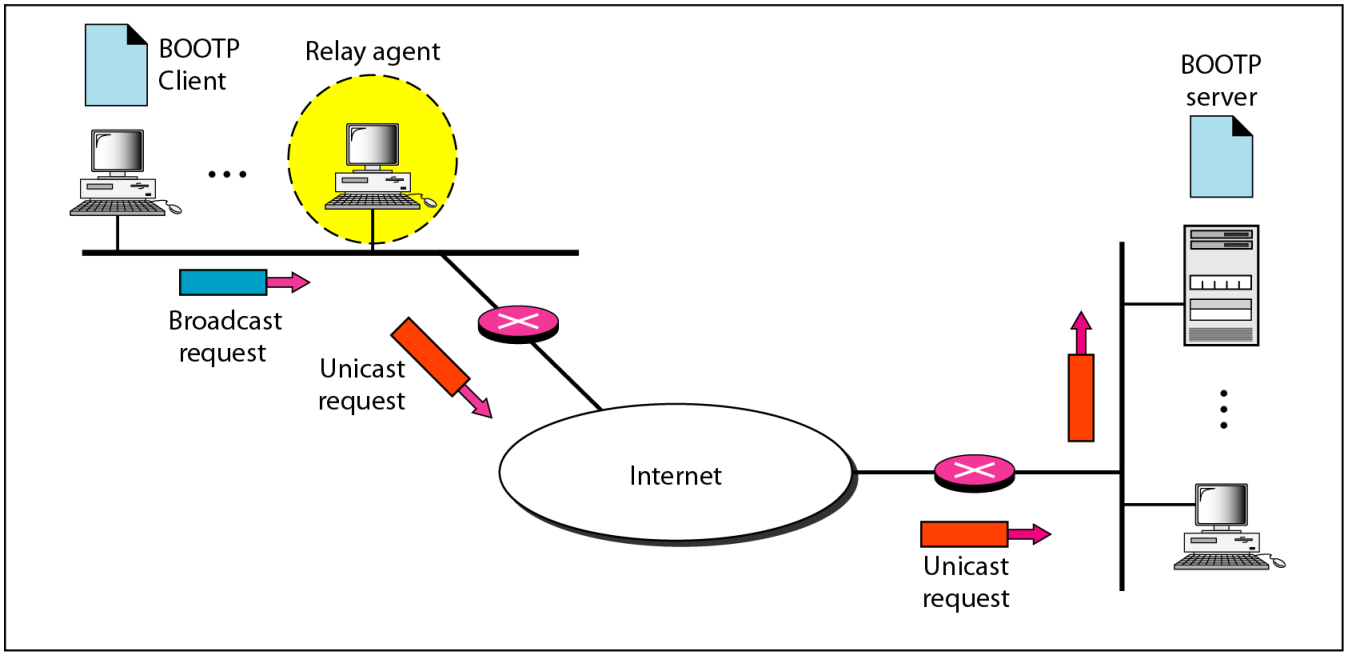
- IP address
- Net mask (specifies network id)
- Default Gateway (at least one)
- DNS server (at least one)
  - Server's IP address

- Other stuff
  - TFTP server
  - Configuration file
  - Executable image download

Obtaining an IP address (bootp – Bootstrap protocol)



a. Client and server on the same network



b. Client and server on different networks

Dynamic Host Configuration Protocol (DHCP)

- BOOTP
  - Not dynamic!
  - Server cannot reclaim IP address
- DHCP
  - IP address
    - Allocation from pool or static (mapping to e.g. MAC addr)
  - Network mask
  - Default gateway
  - DNS server(s)
  - Lease time

Dynamic Host Configuration Protocol (DHCP)

Internet protocol that enables dynamic allocation of IP addresses to hosts

Defined in RFC 2131

Was developed to deal with the shortage of IP addresses

Enables a local network to assign IP addresses from a pool of available IP addresses to hosts currently in use

- When a host is not in use, its IP address is returned to the pool managed by a DHCP server

Can also assign permanent IP addresses to some systems, such as servers, so that the address remains the same when the system is rebooted

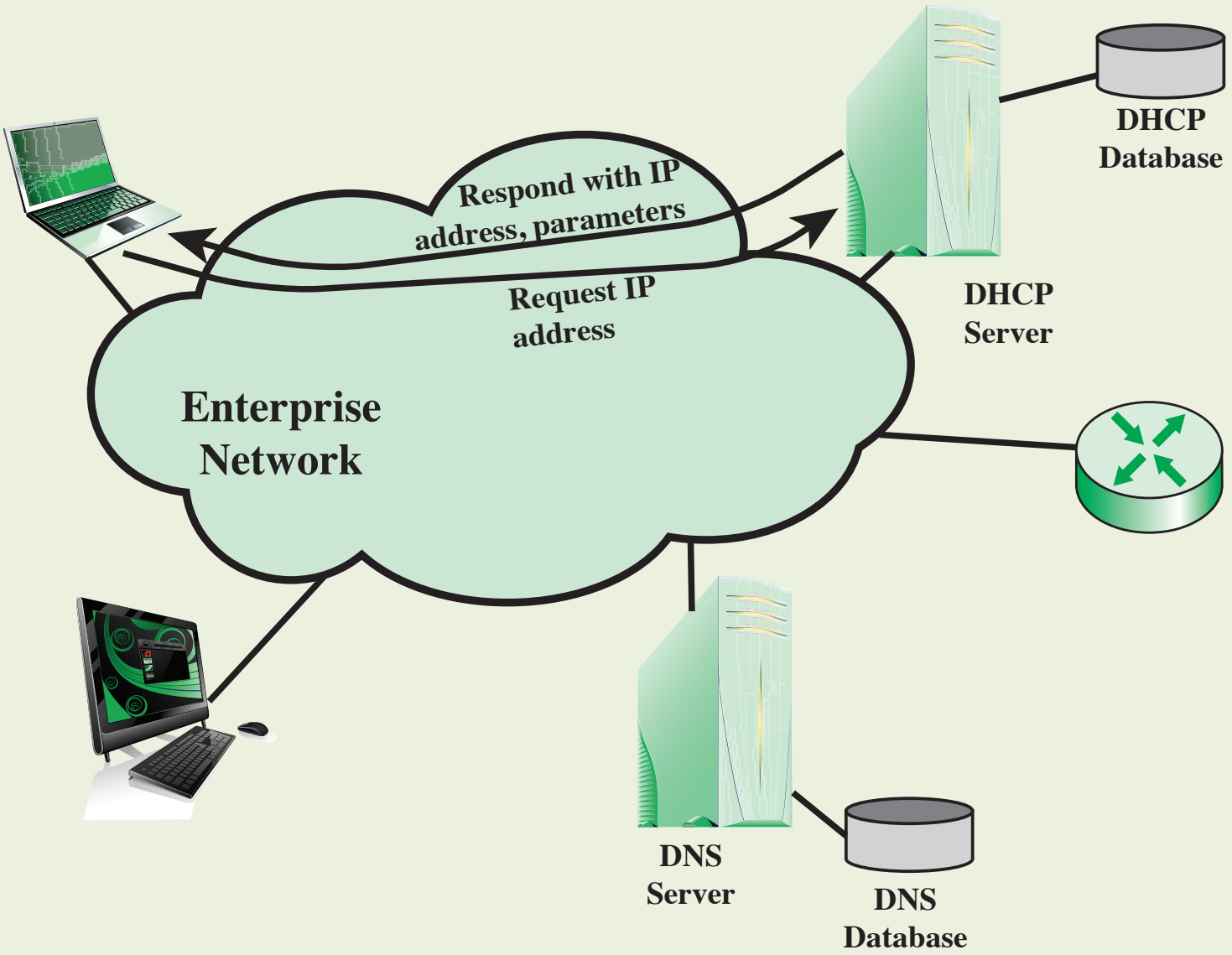


Figure 21.14 DHCP Role

The following DHCP messages are used for protocol operation: (reference only)

DHCPDISCOVER

- Client broadcast to locate available servers

DHCPOFFER

- Server to client in response to DHCPDISCOVER with offer of configuration parameters

DHCPREQUEST

- Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, for example, system reboot, or (c) extending the lease on a particular network address

DHCPACK

- Server to client with configuration parameters, including committed network address

DHCPNACK

- Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease has expired

DHCPDECLINE

- Client to server indicating network address is already in use. DHCP server should then notify sysadmin

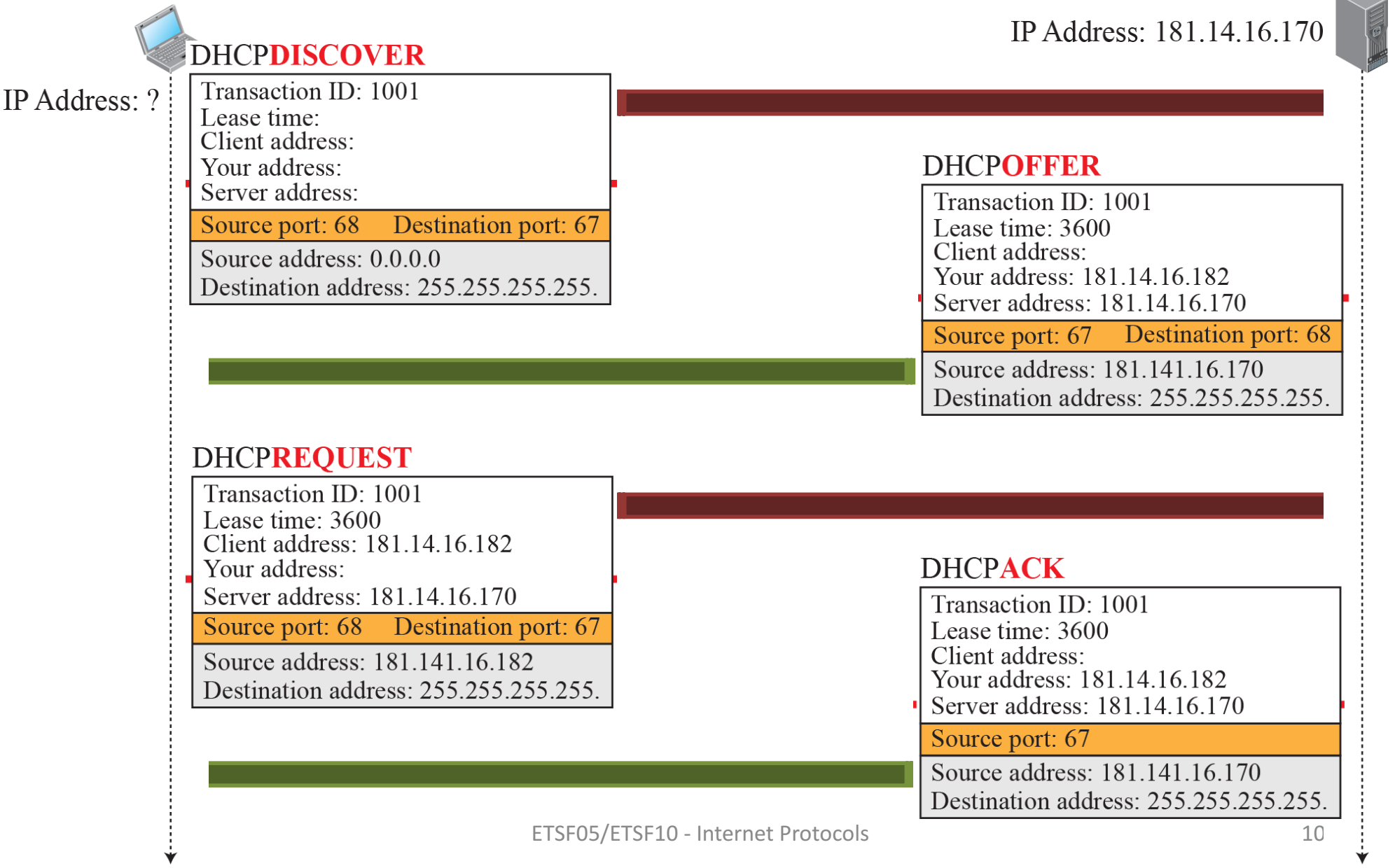
DHCPRELEASE

- Client to server relinquishing network address and canceling remaining lease

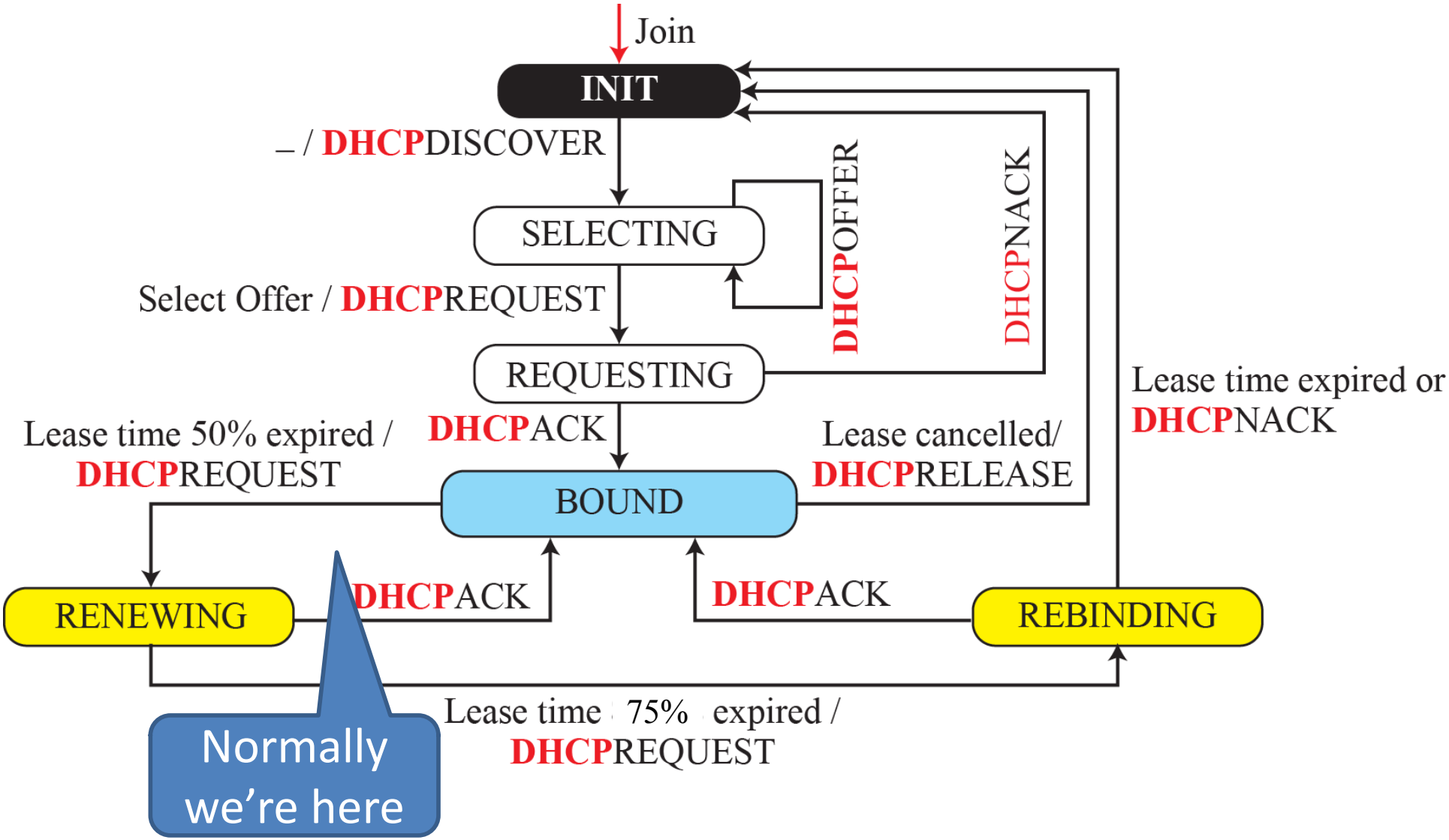
DHCPINFORM

- Client to server, asking only for local configuration parameters client already has externally configured network address

DHCP operation

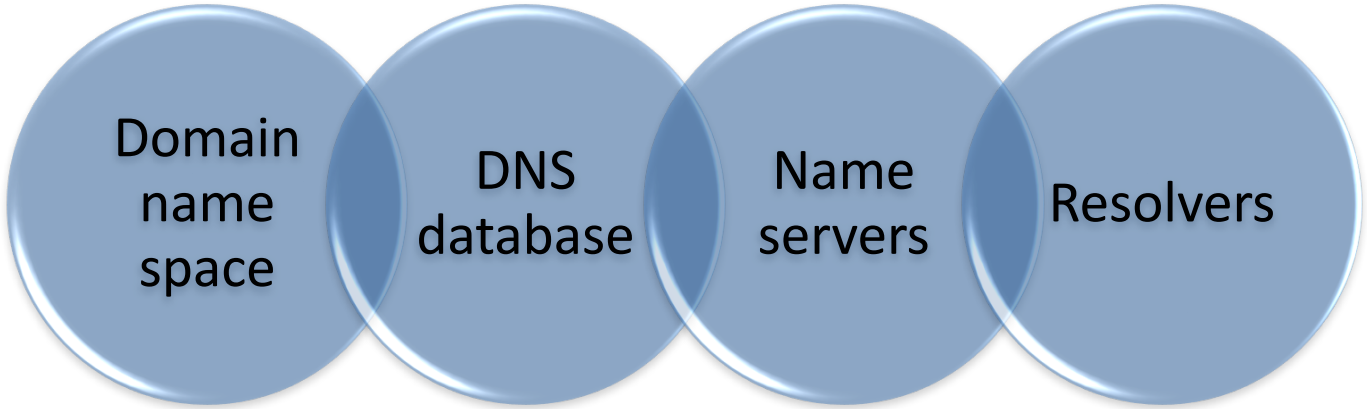


DHCP states


Join
INIT
– / DHCPDISCOVER
SELECTING
DHCPOFFER
DHCPNACK
Select Offer / DHCPREQUEST
REQUESTING
Lease time expired or DHCPNACK
Lease time 50% expired / DHCPREQUEST
DHCPACK
Lease cancelled/ DHCPRELEASE
BOUND
RENEWING
DHCPACK
DHCPACK
REBINDING
Lease time 75% expired / DHCPREQUEST
Normally we're here

Internet Directory Service
Domain Name System (DNS)

- A directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address
- Essential to the functioning of the Internet
- Defined in RFCs 1034 and 1035
- Four elements comprise the DNS:



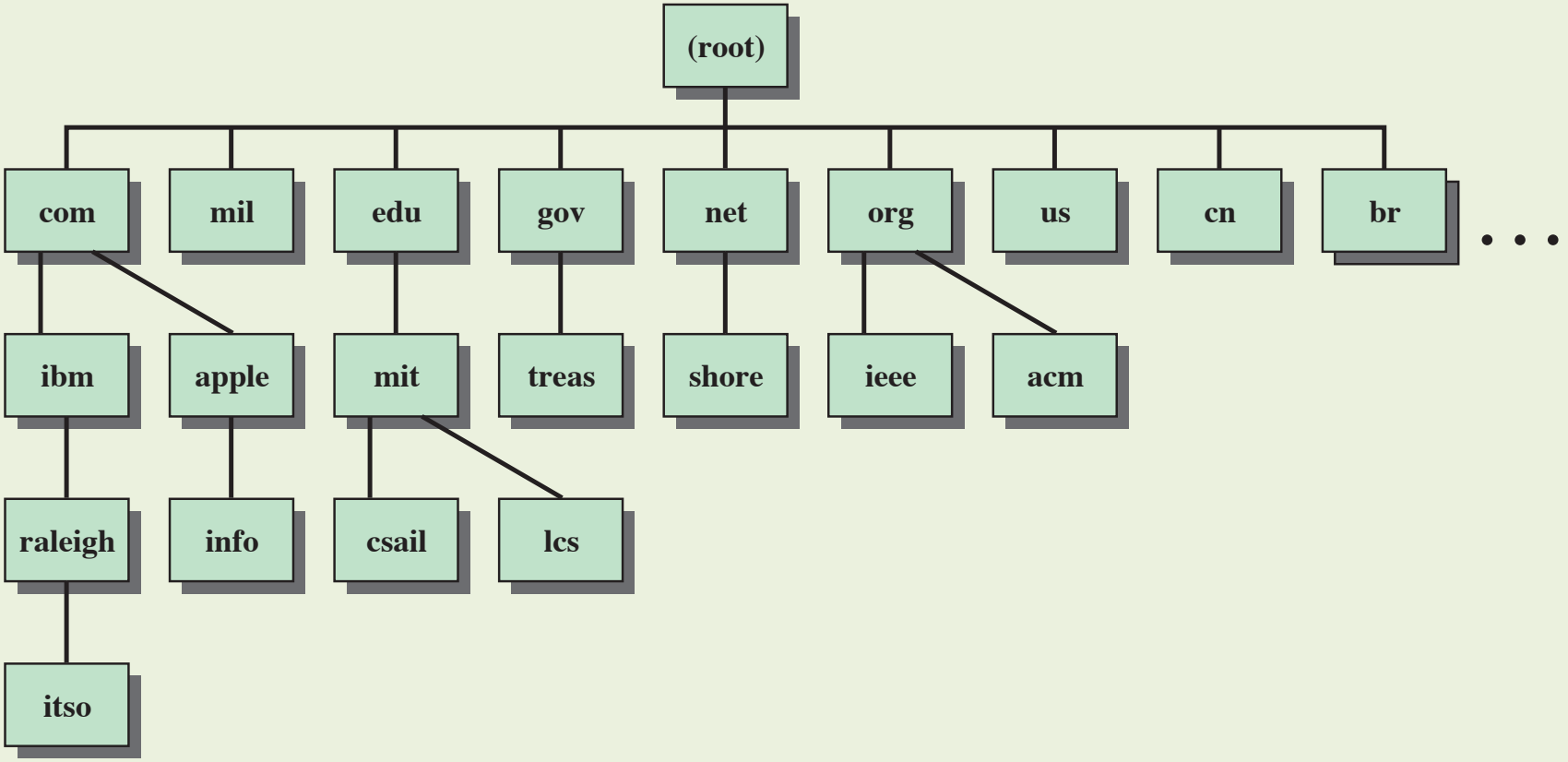


Figure 24.4 Portion of Internet Domain Tree

DNS Database

- Based on a hierarchical database containing **resource records** (RR) that include the name, IP address, and other information about hosts
- Key features:
  - Variable-depth hierarchy for names
  - Distributed database
  - Distribution controlled by the database

DNS resource records

(Domain Name, Type, Class, TTL, Value)

Type	*Interpretation of value*
A	A 32-bit IPv4 address (see Chapter 4)
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address (see Chapter 4)

See also Table 24.5 Resource Record Types
Figure 24.5 for record format

Domain name resolution

- Action of address mapping
  - Client = resolver
  - Server = DNS
- One server cannot have all the answers!
  - How to ask others?
  - What to do with the answer?
- Caching
  - Remember what you have learned

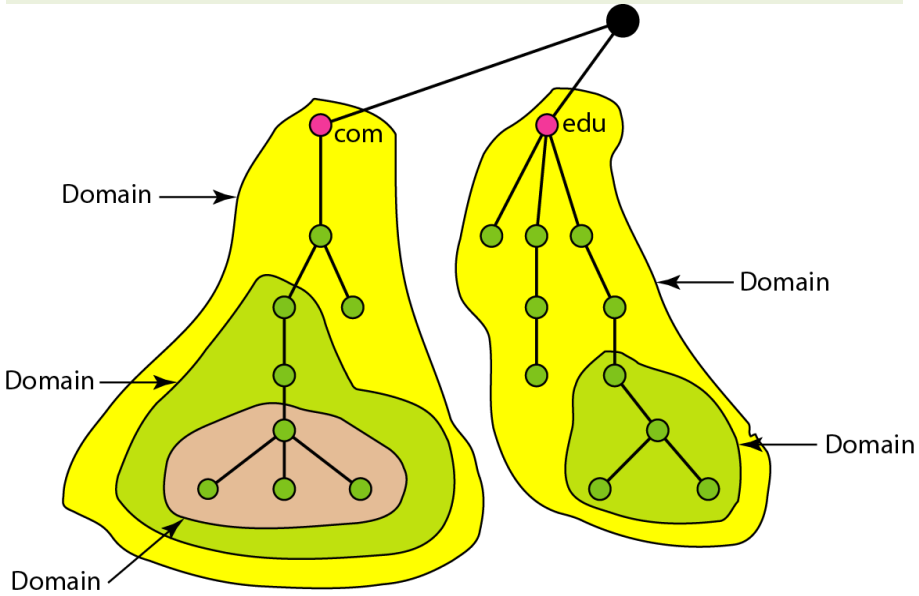
Domain

- Refers to a group of hosts that are under the administrative control of a single entity
- Organized hierarchically, so that a given domain may consist of a number of subordinate domains
- Names are assigned and reflect the hierarchical organization

Domains, subdomains, zones

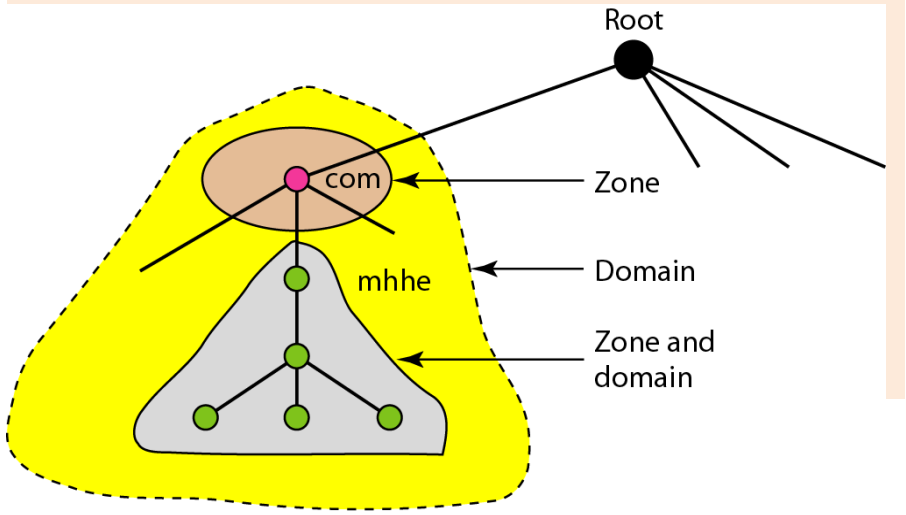
Domain

- Subtree of DNS

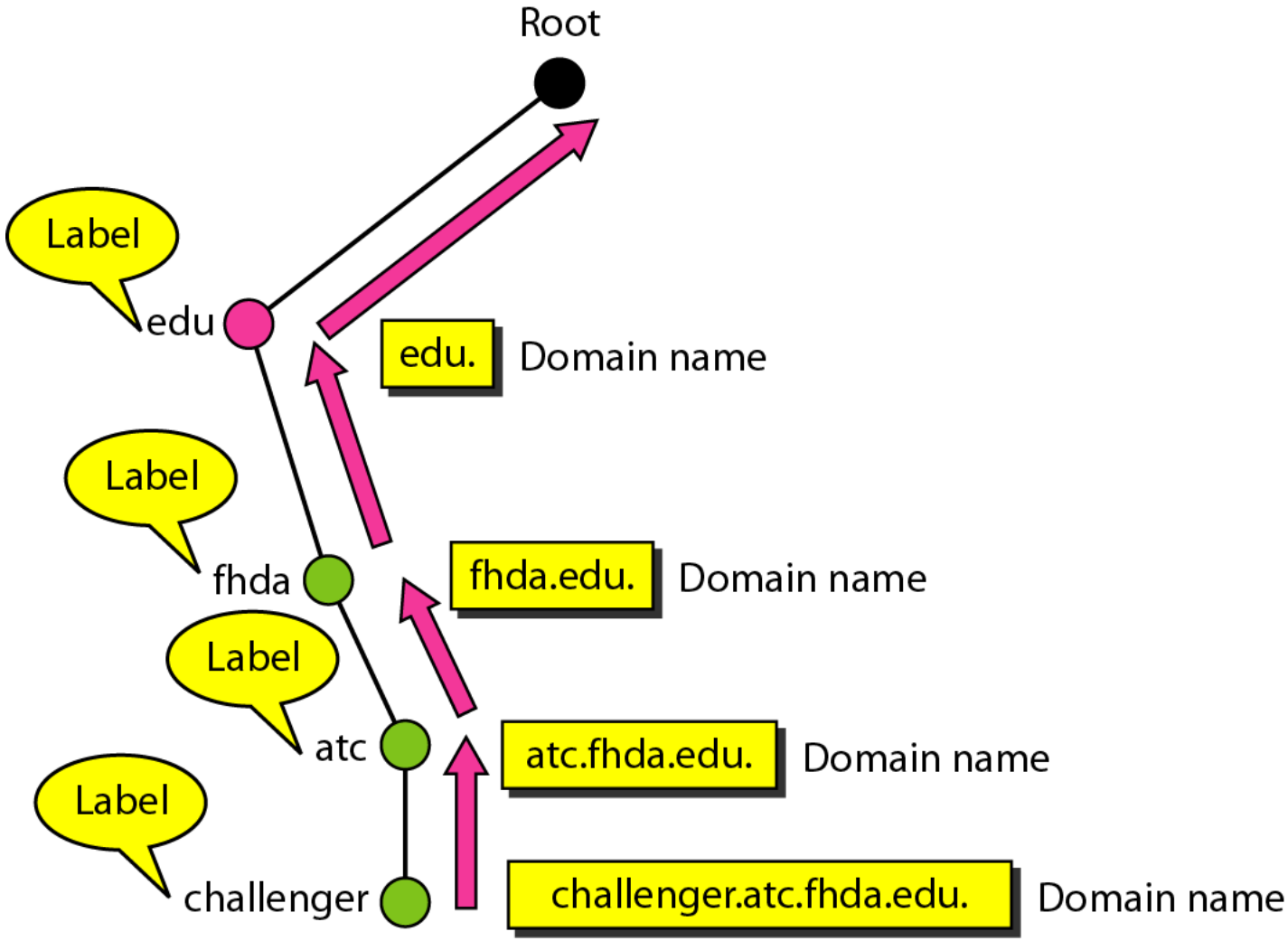


Zone

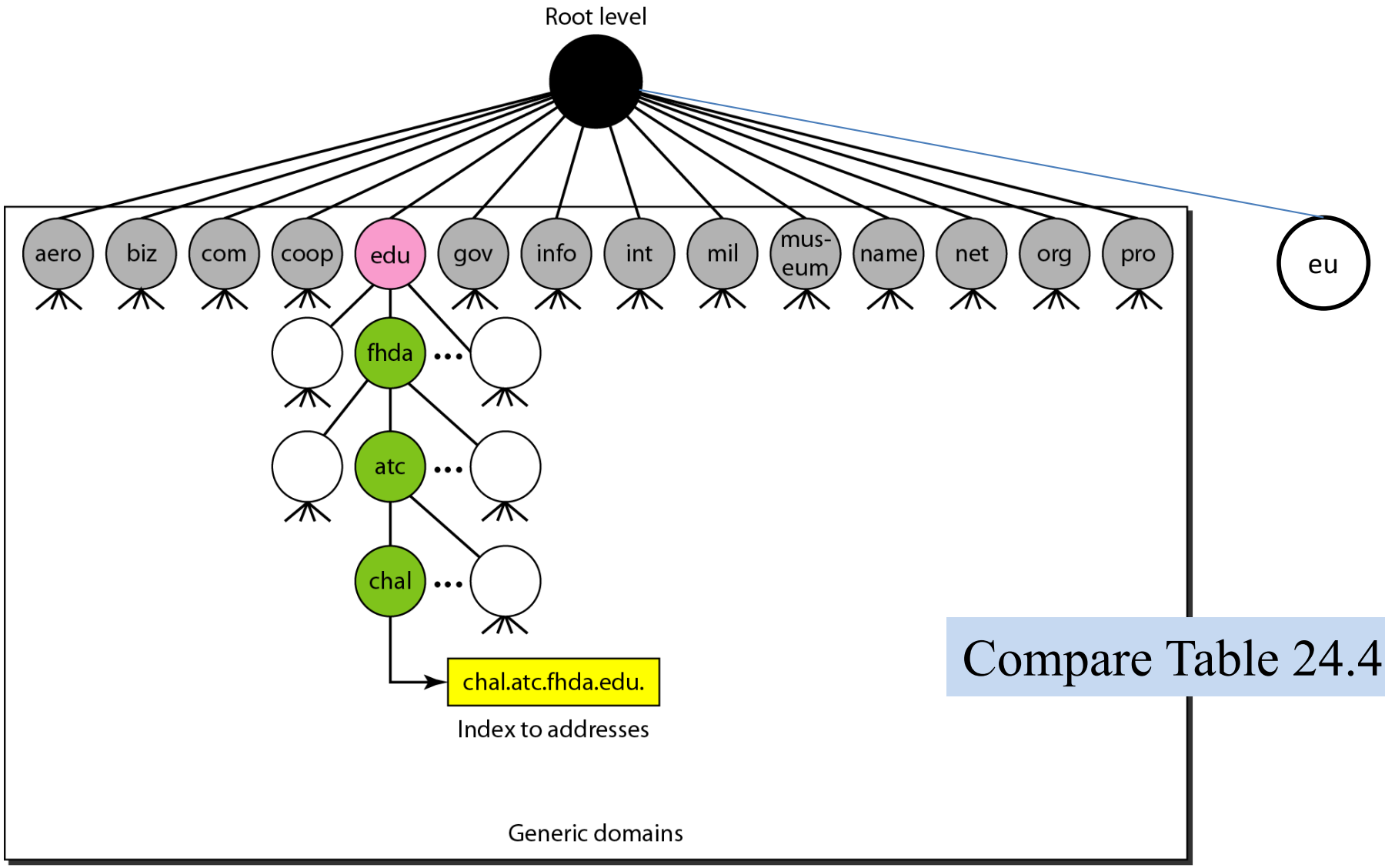
- Servers' control area



Domain names and labels

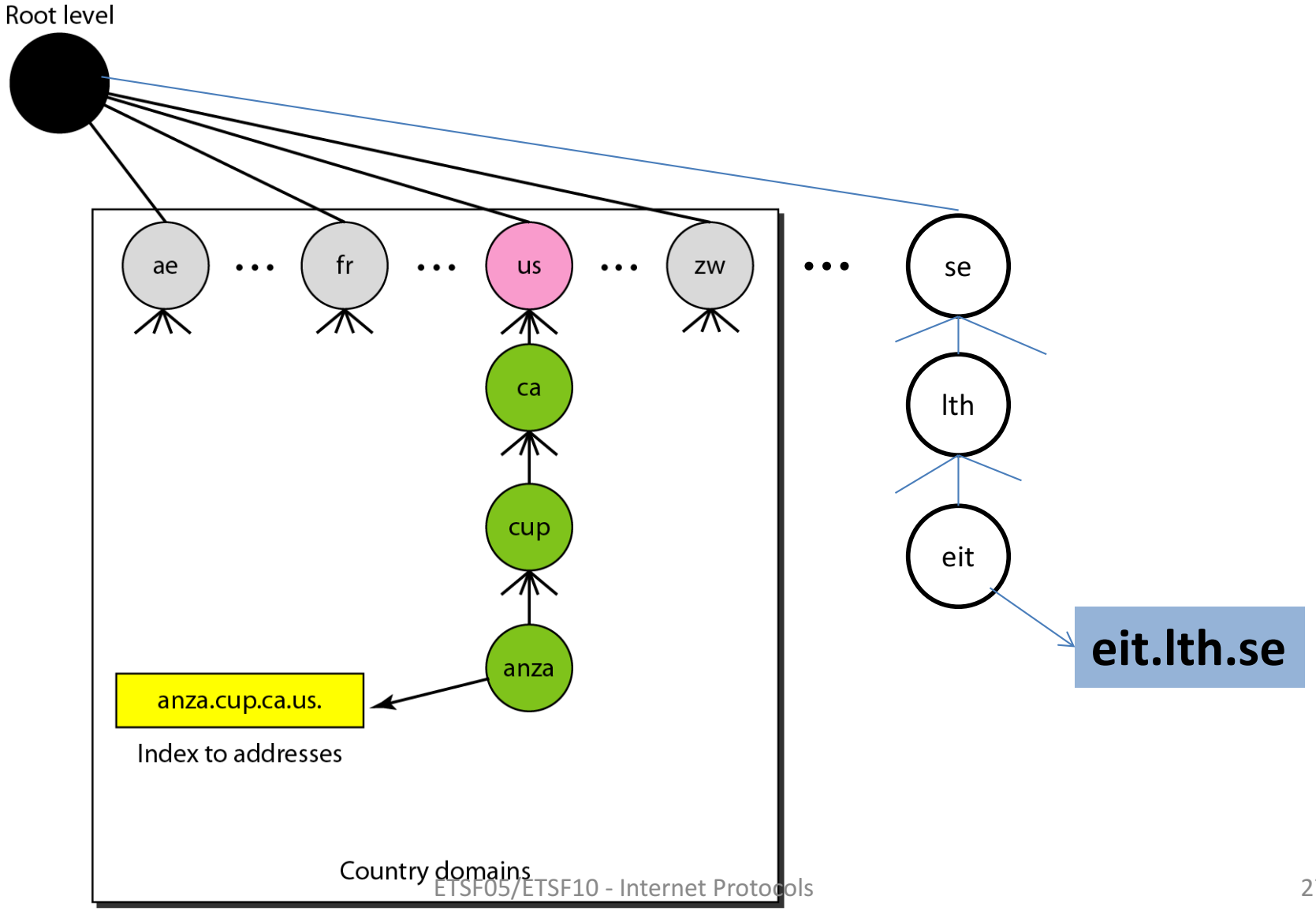


Generic domains



Compare Table 24.4

Country domains



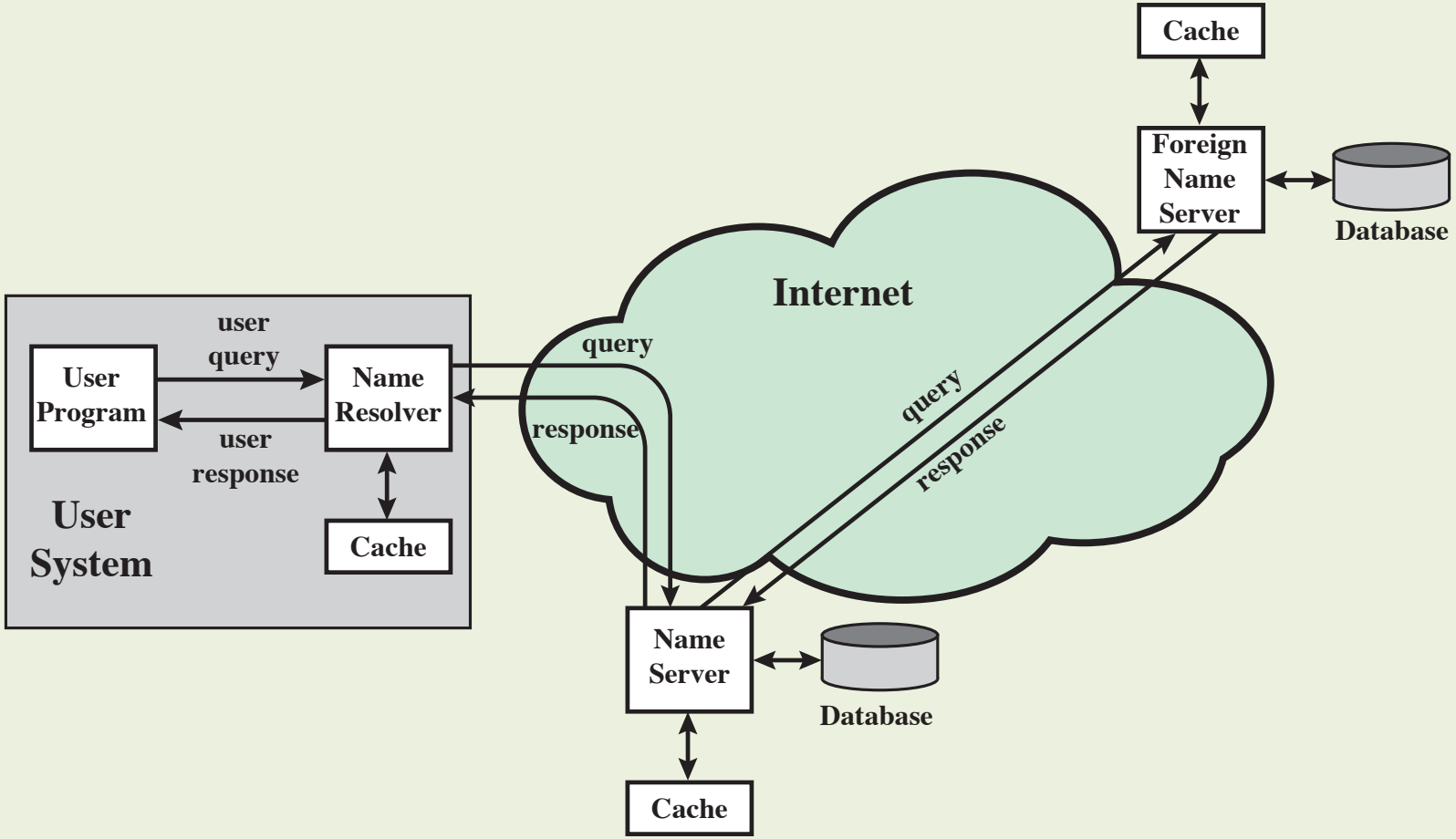
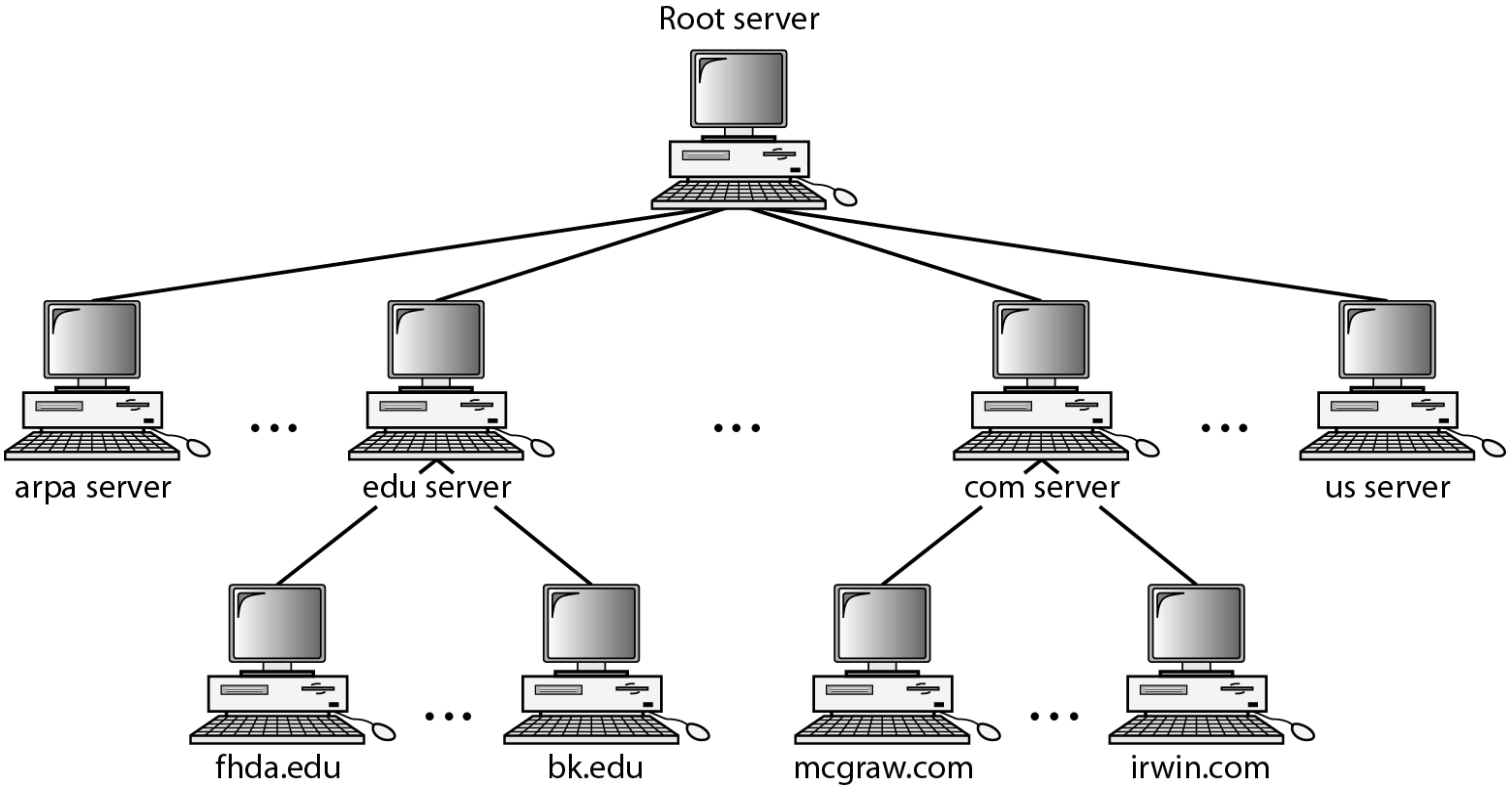


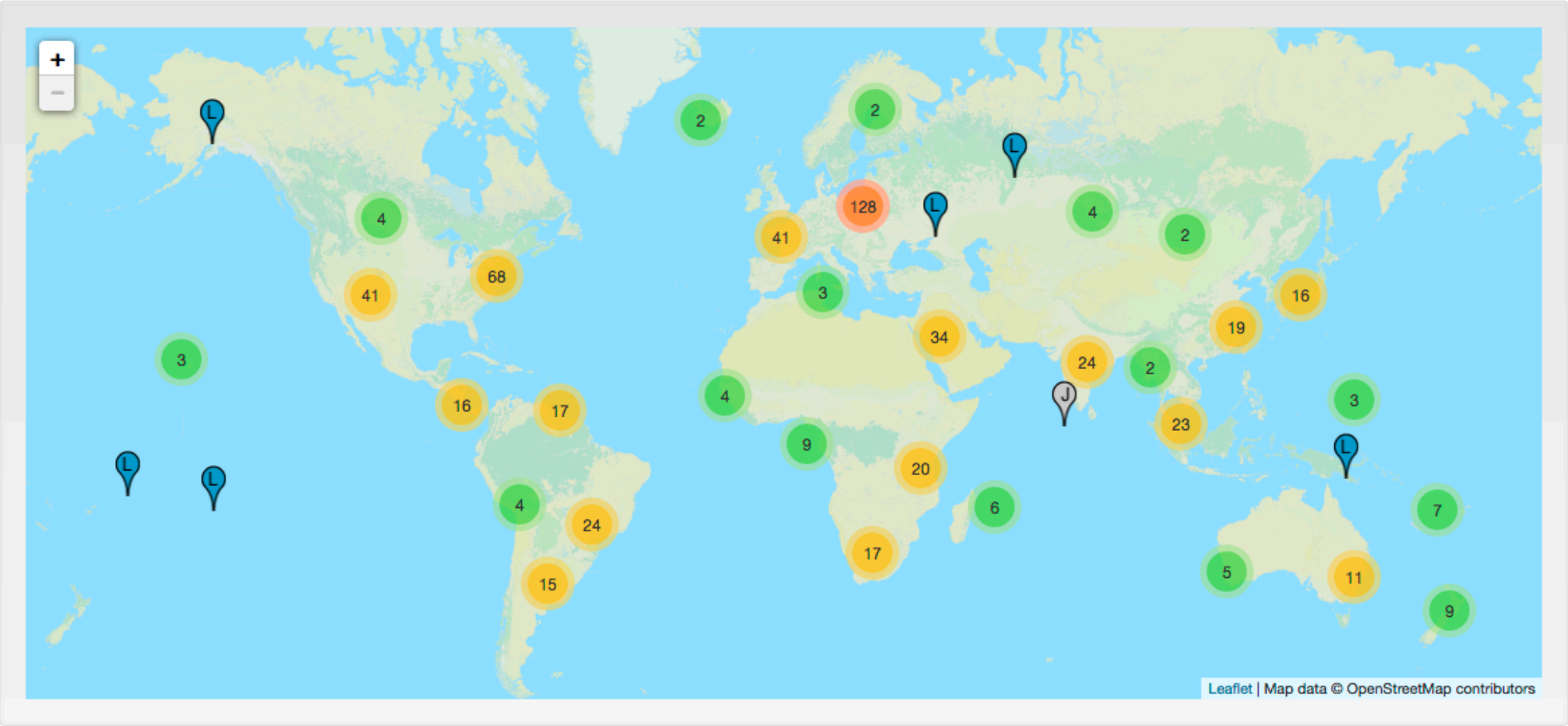
Figure 24.6 DNS Name Resolution

Hierarchy of domain name servers



- 13 root servers

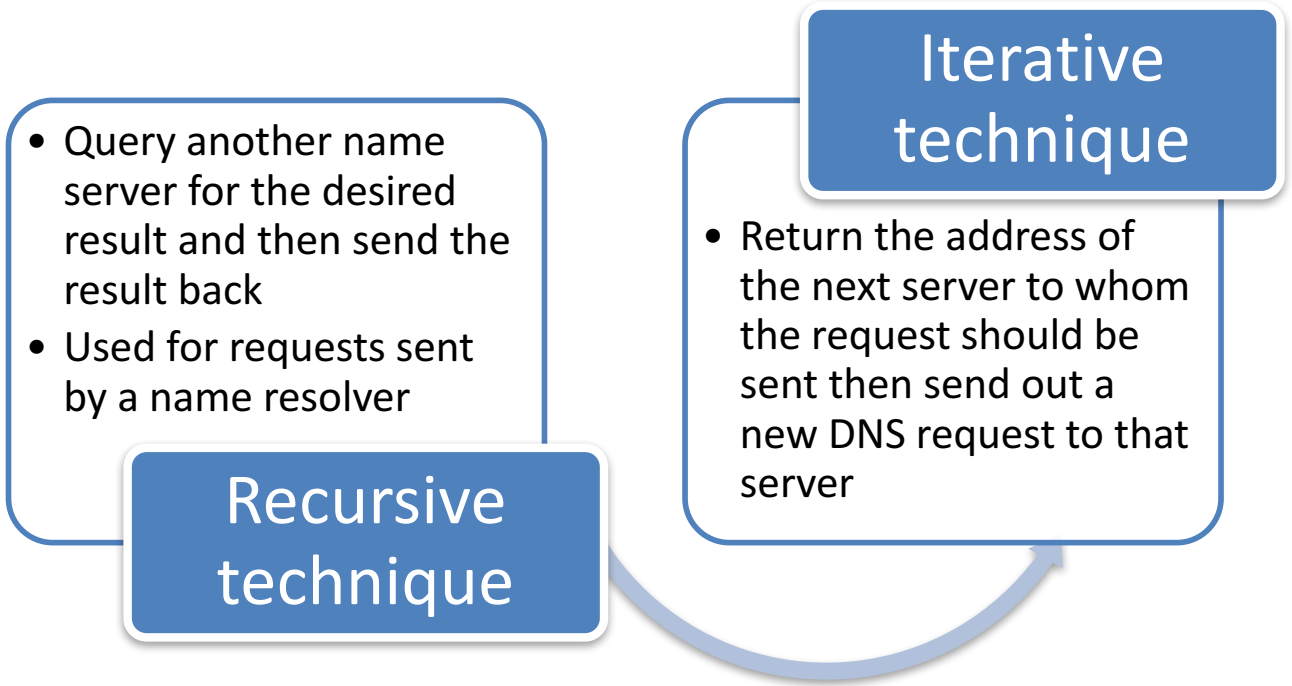
www.root-servers.org



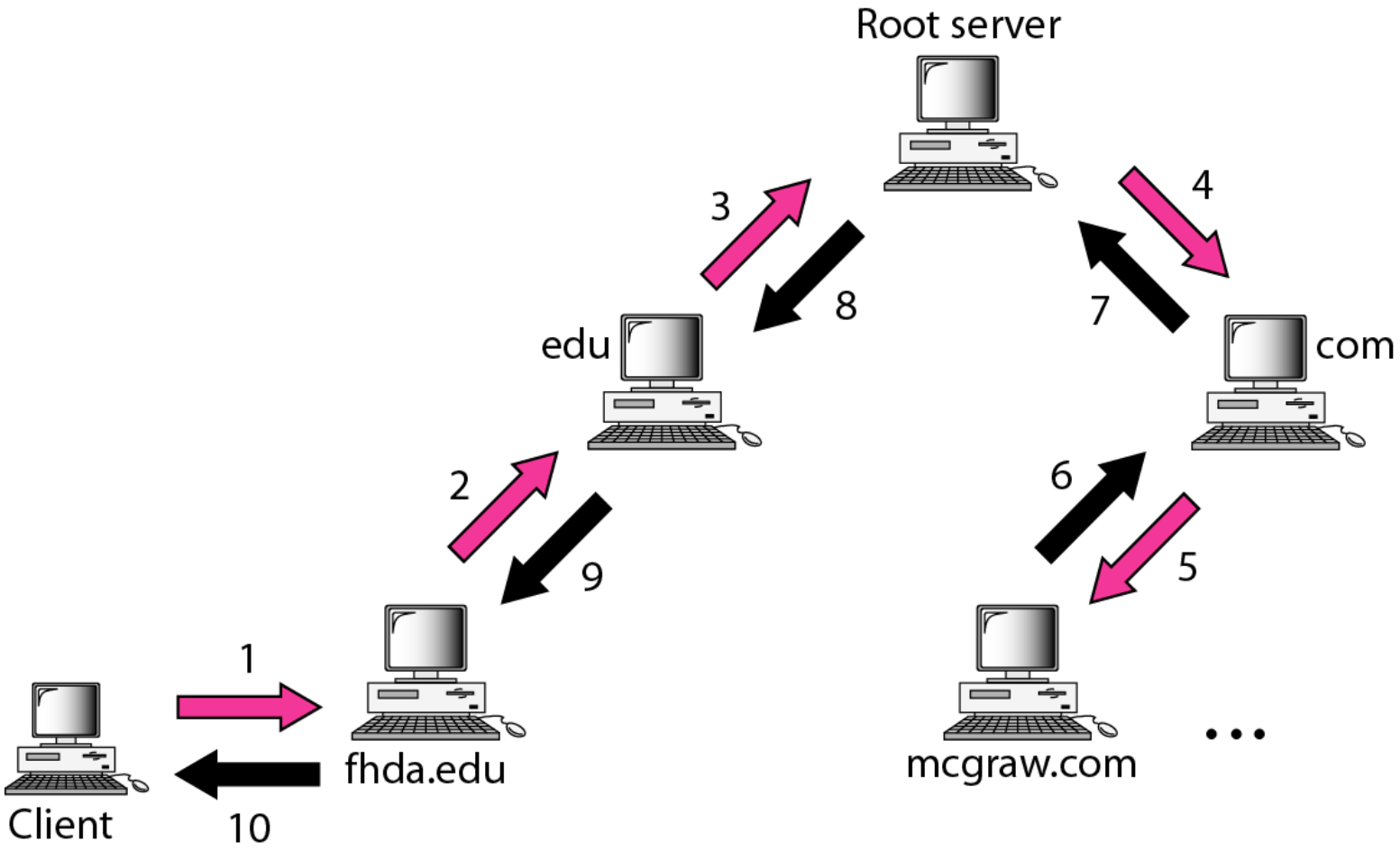
- 13 root servers: A, B, C, D, E, F, G, H, I, J K, L, M
- Implemented by total 641 servers

Name Resolution

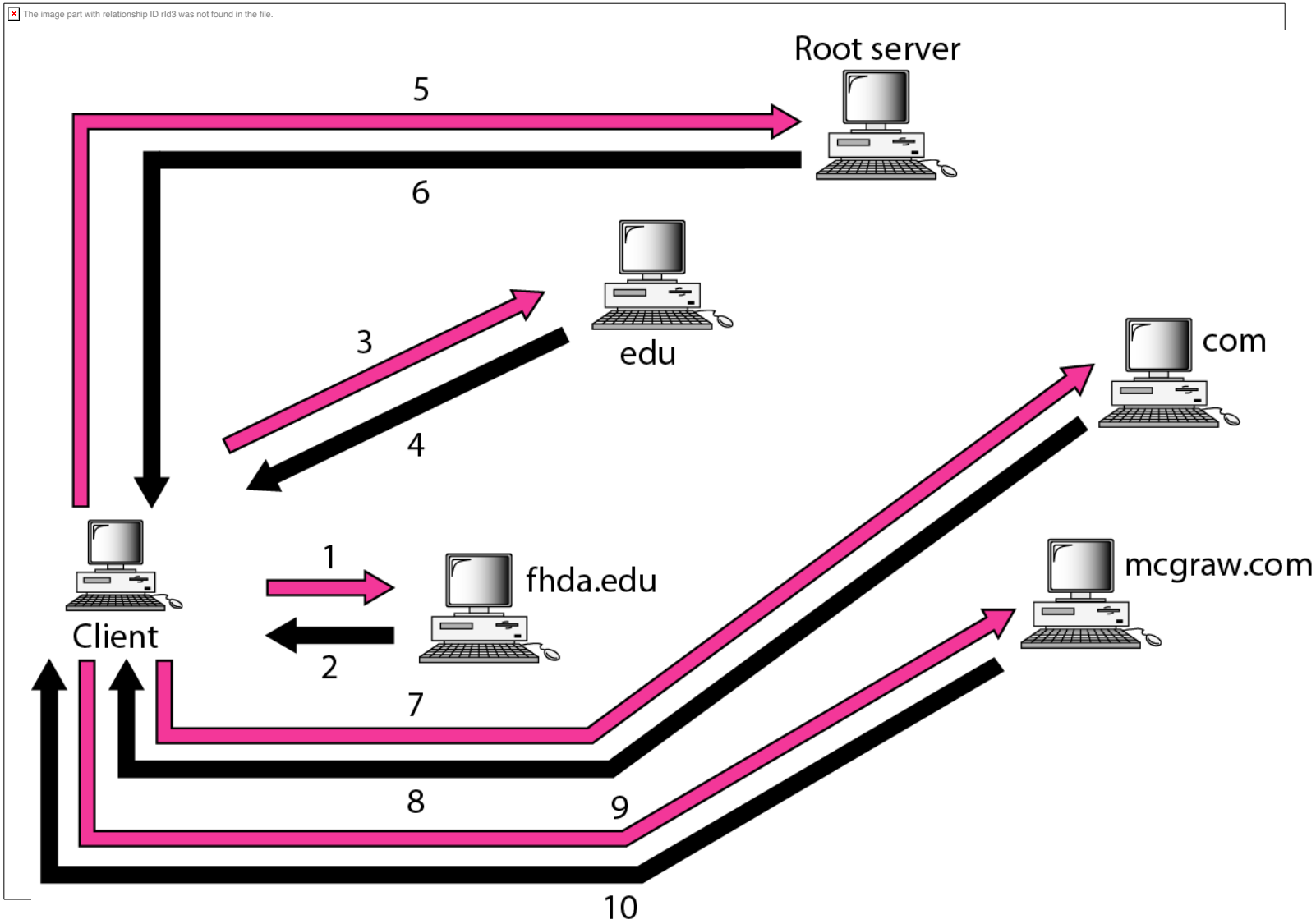
- Each query begins at a name resolver located in the user host system
- If the resolver does not have the requested name in its cache, it sends a DNS query to the local DNS server
- Resolvers use UDP for single queries and TCP for group queries



Recursive resolution



Iterative resolution



Manual lookup (on UNIX like)

Lookup

> host lu.se

lu.se has address 130.235.52.5

lu.se has IPv6 address 2001:6b0:16:1:5ee:bad:c0de:1002

lu.se mail is handled by 10 mx.lu.se.

> host –t A lu.se

lu.se has address 130.235.52.5

Reverse

> host 130.235.52.5

5.52.235.130.in-addr.arpa domain name pointer lb3v1.net.lu.se.

Dynamic DNS

- Host may move around
  - Change of IP address
- New domains may emerge
  - Binding (IP address ↔ Name)
  - DHCP updates primary DNS server
  - Primary server updates zone
  - Secondary servers notified

DNSsec

- Provides
  - Message authentication
- Protect against
  - Forged or manipulated data
- No confidentiality

- Digital signature

Real-time audio/video

- One-way communication
  - IPTV, Internet Radio
  - Over The Top (OTT)
- Two-way communication (interactive)
  - IP telephony
  - Voice over IP (VoIP)
  - Video conferencing

Compare On Demand Services

- Audio/Video
- Not real-time
- TCP and buffering
- Example:
  - Youtube
  - Spotify
  - Play Channels

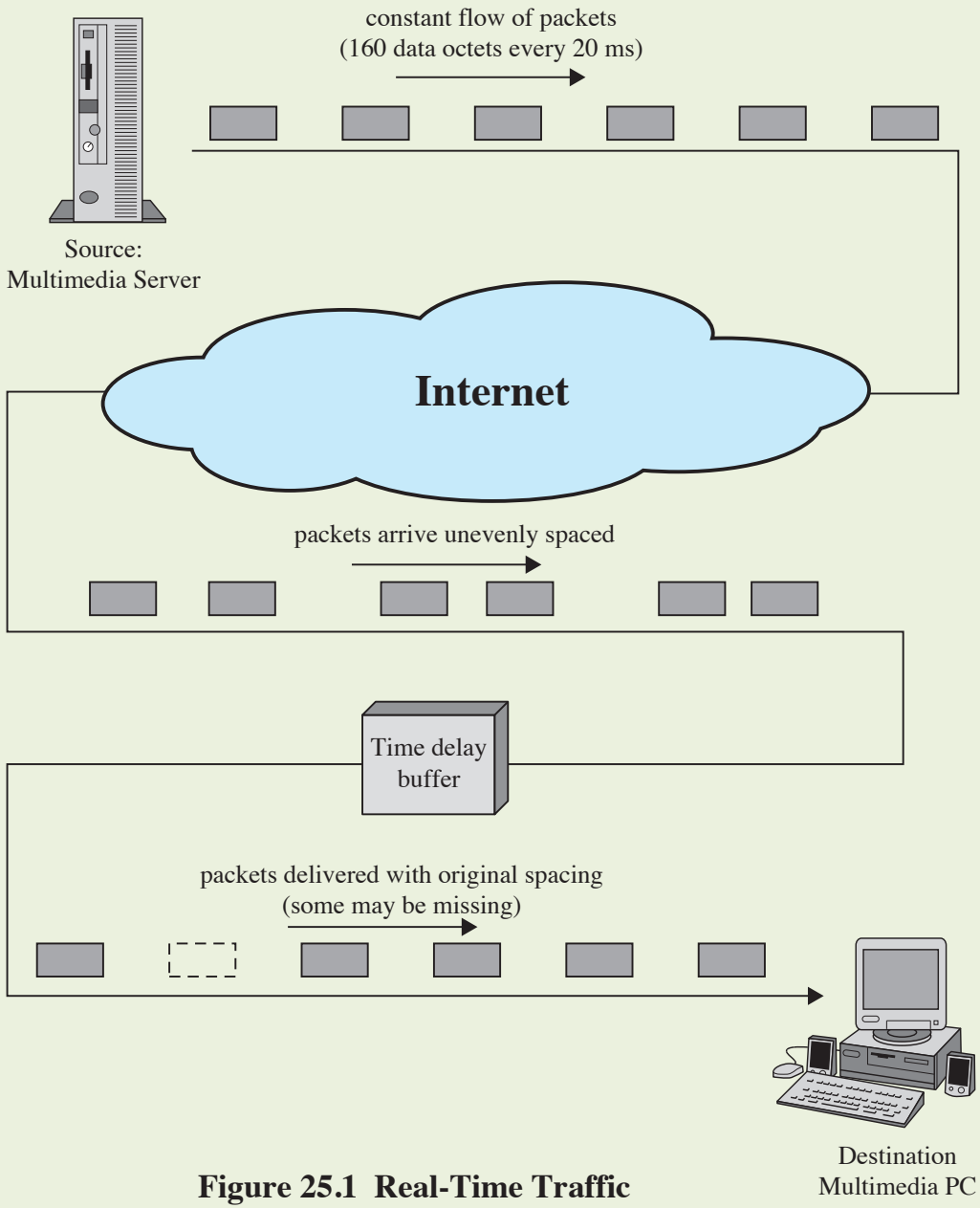
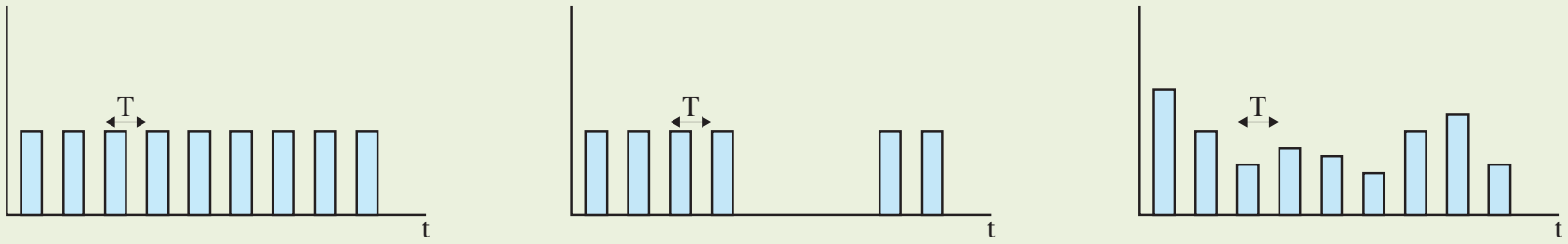


Figure 25.1 Real-Time Traffic



(a) Continuous data source

(b) Voice source with silent intervals

(c) Compressed video source

Figure 25.2 Real-Time Packet Transmission (based on [ARAS94])

Requirements for Real-Time Communication

- Low jitter (delay variations)
- Low latency
- Ability to aggregate non-real-time and real-time services
- Adaptable to dynamically changing network and traffic conditions
- Good performance for large networks and large numbers of connections
- Modest buffer requirements within the network
- Effective capacity utilization
- Low overhead in header bits per packet
- Low processing overhead per packet within the network and at the end system

Hard Versus Soft Real-Time Applications

Soft

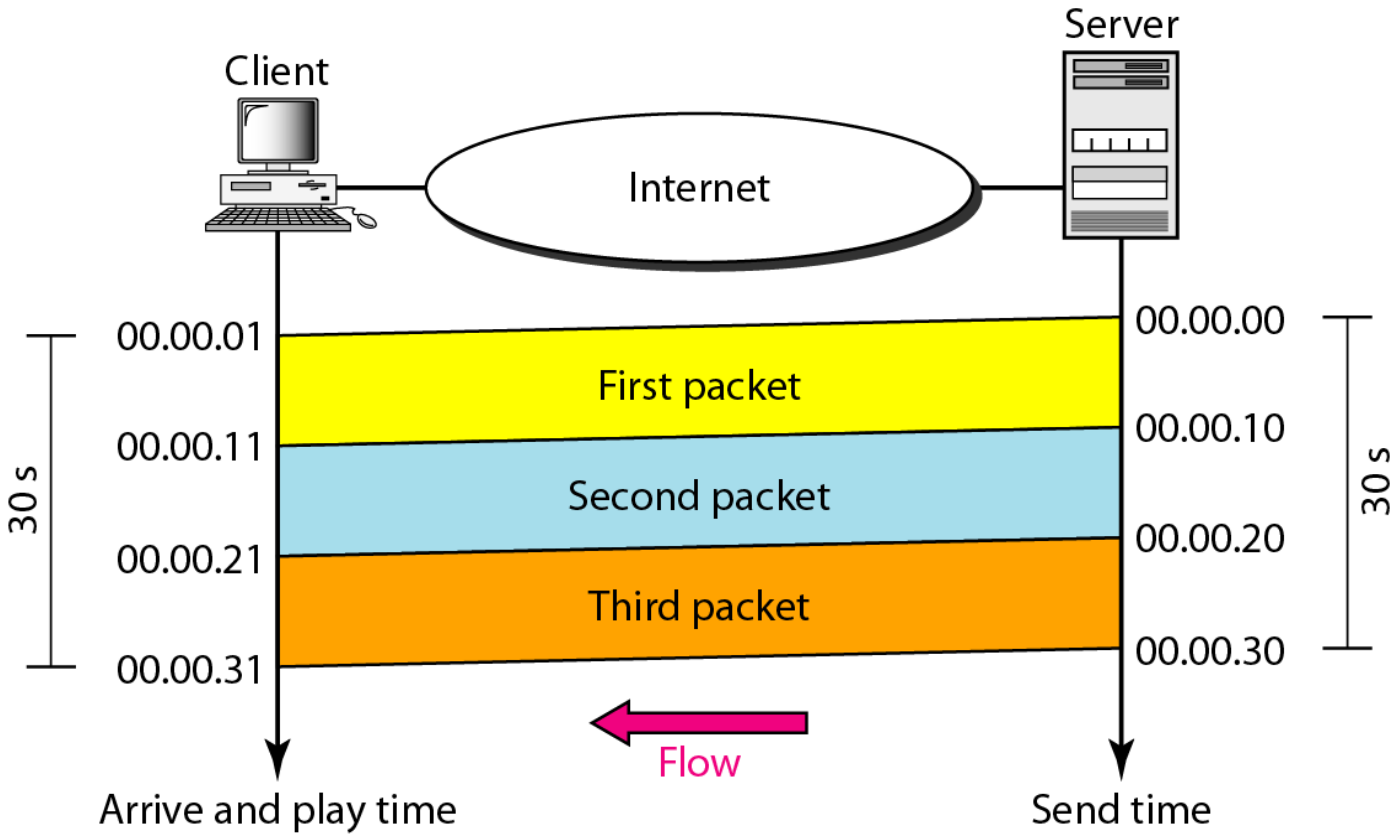
- Can tolerate loss of some portion of data
- Impose fewer requirements on the network, therefore permissible to focus on maximizing network utilization, even at the cost of some lost or misordered packets

Hard

- Zero loss tolerance
- A deterministic upper bound on jitter and high reliability takes precedence over network utilization considerations

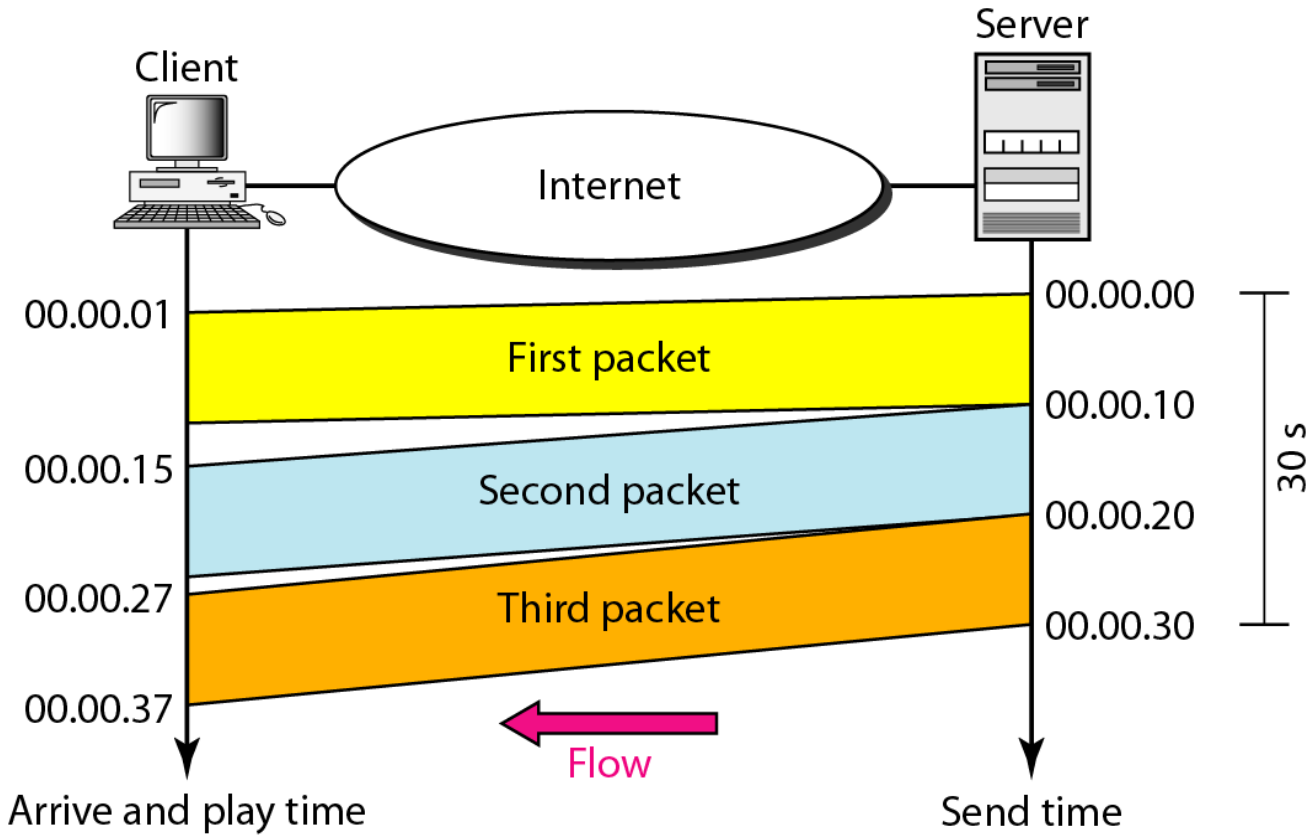
Time relationship

- Just delay? No problem!(?)



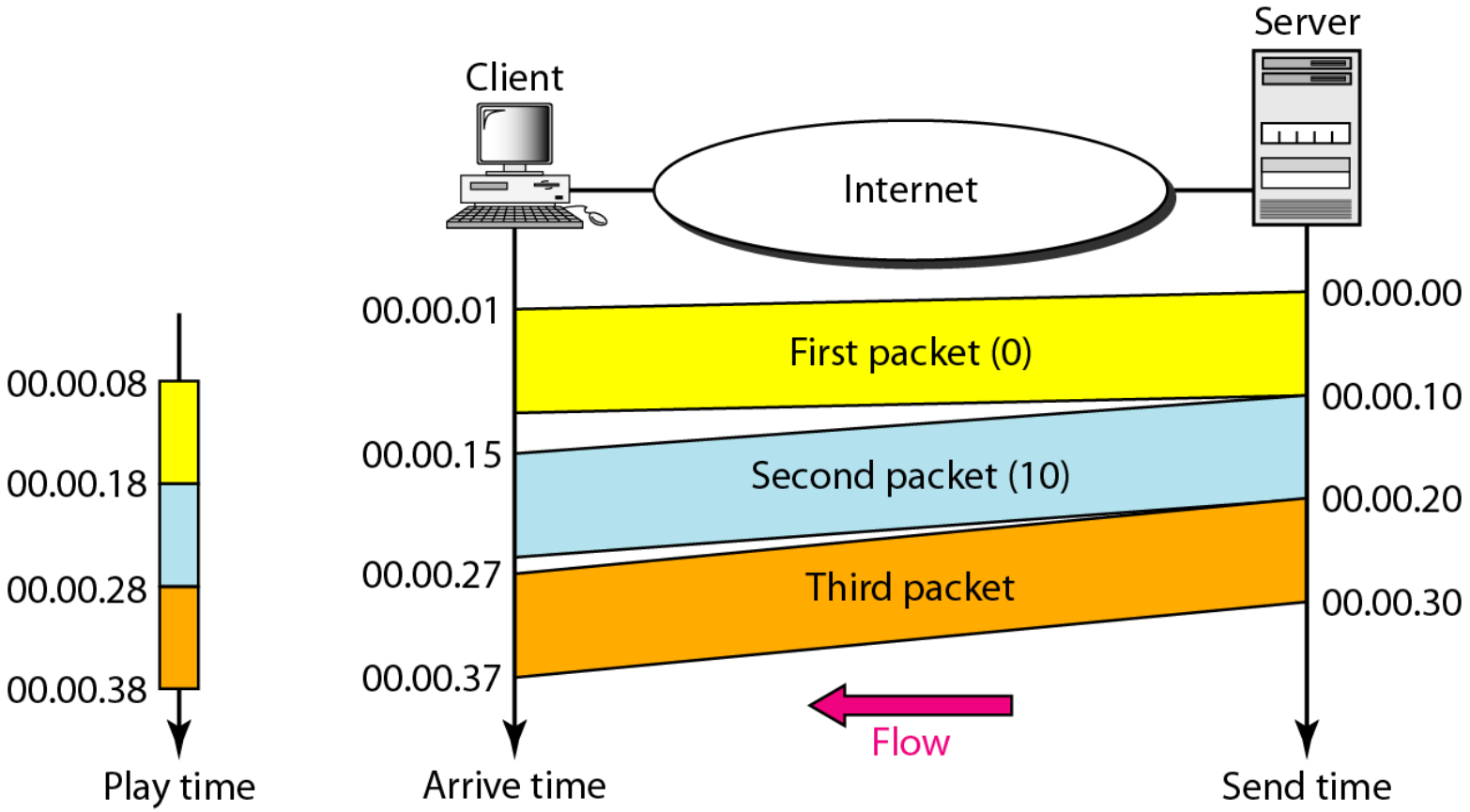
Packet Delay Variation (PDV)/Jitter

- Undesired variation in delay

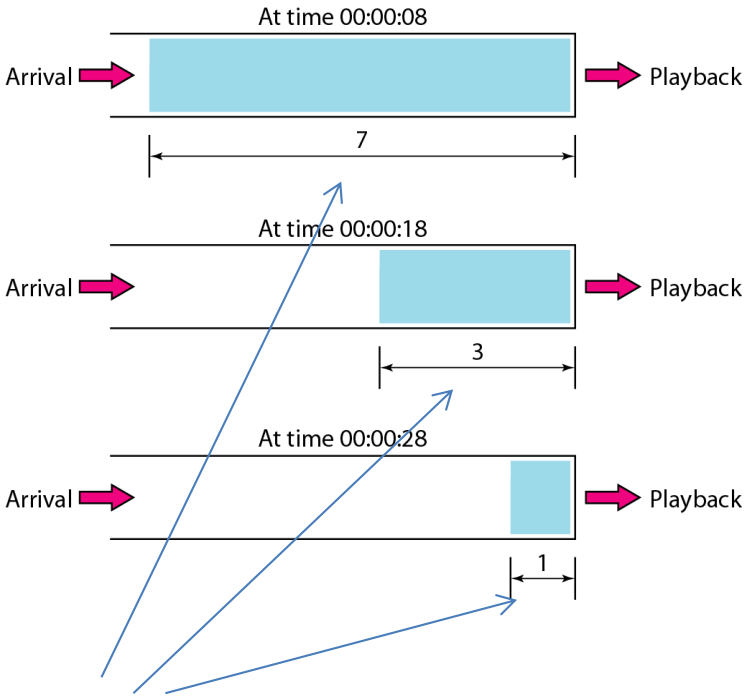


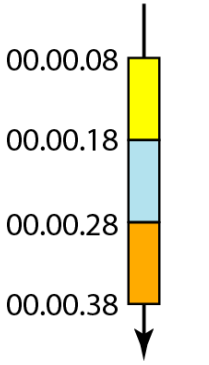
Timestamps

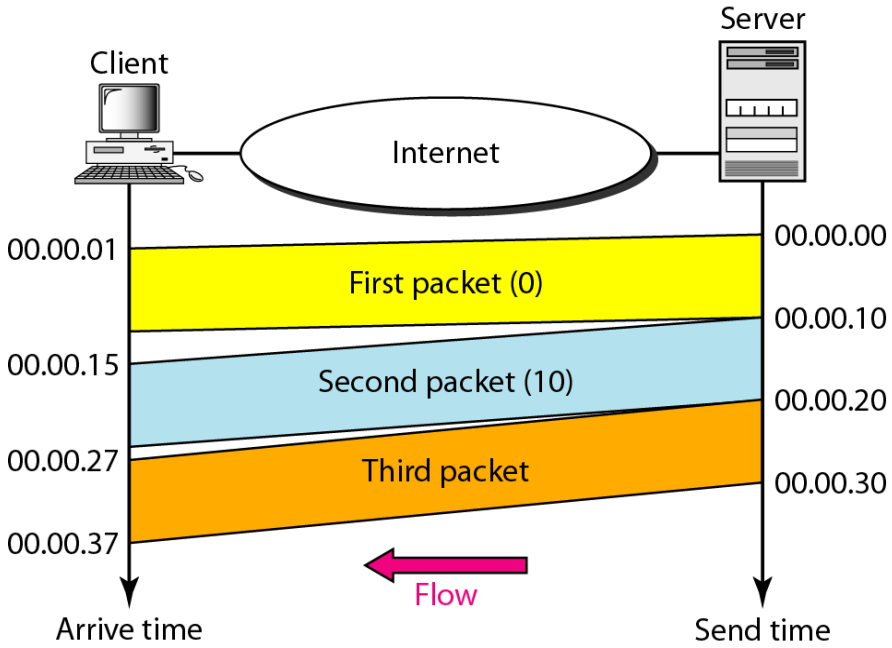
- Separation of arrival time from playback time



Playback buffer







Playout delay – permissable network delay

Still not good enough!

- Packets can be delivered out of order.
- Packets can be dropped on their way.
- Timestamps do not detect lost packets.

Sequence numbers

- More support:
  - Multicast? Translation? Mixing?

Summary and comparison

Real Time Performance Requirements

- Sensitive to:
  - Delay
  - Jitter
- Not so sensitive to:
  - Packet loss
  - Corrupted packets

vs.

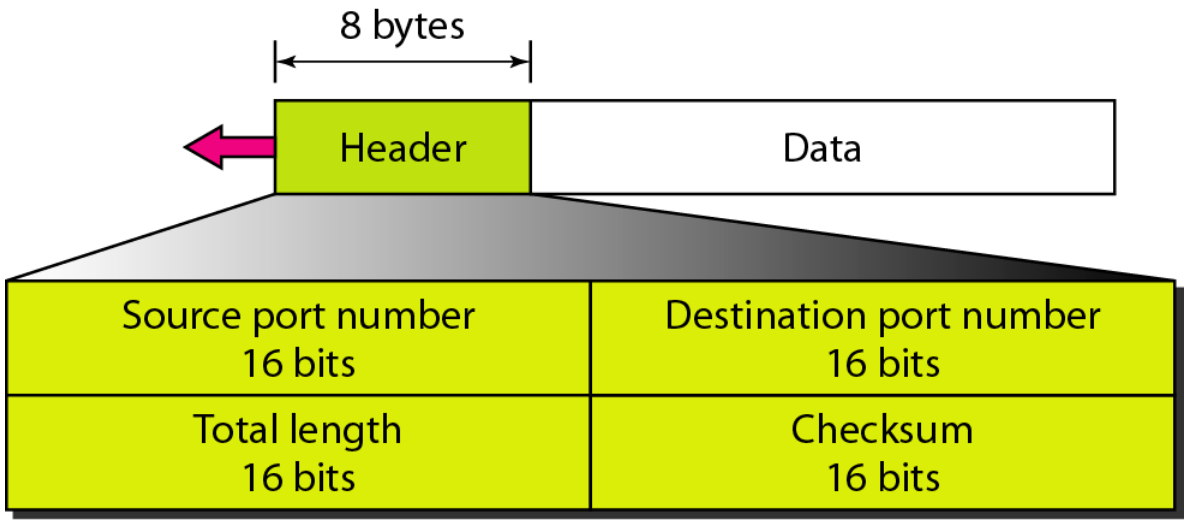
Characteristics of TCP

- Sensitive to:
  - Lost or corrupted packets
- Not so sensitive to:
  - Delay
- No multicasting!

So, what about UDP?

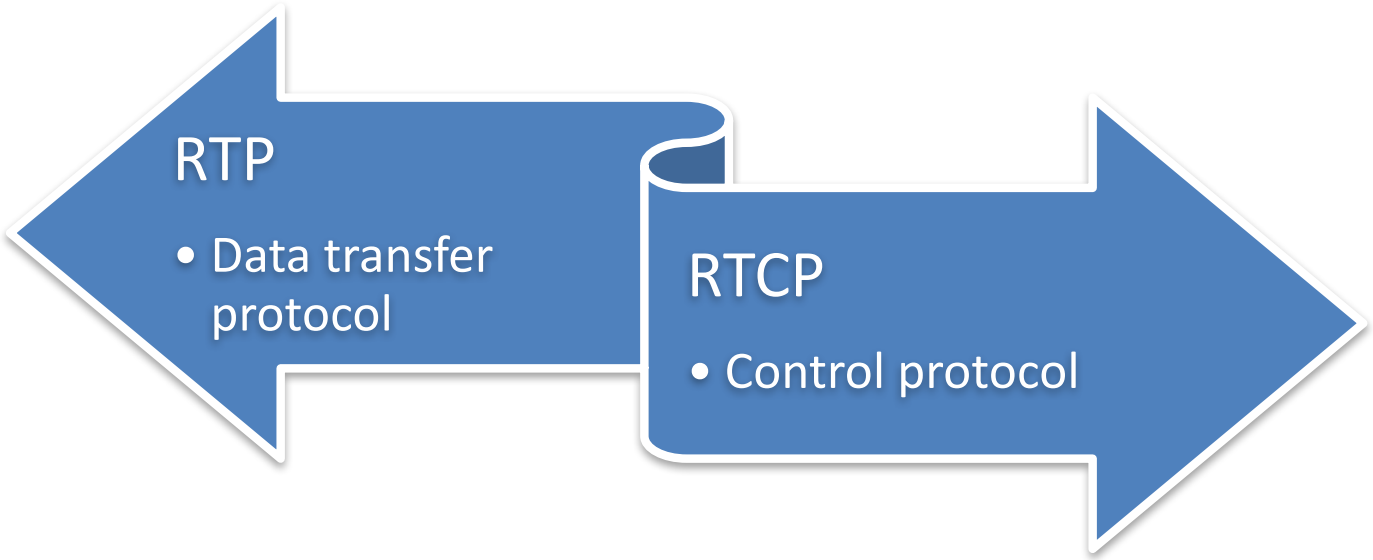
UDP header format

- Checksum optional
- No numbering
  - No relation between datagrams

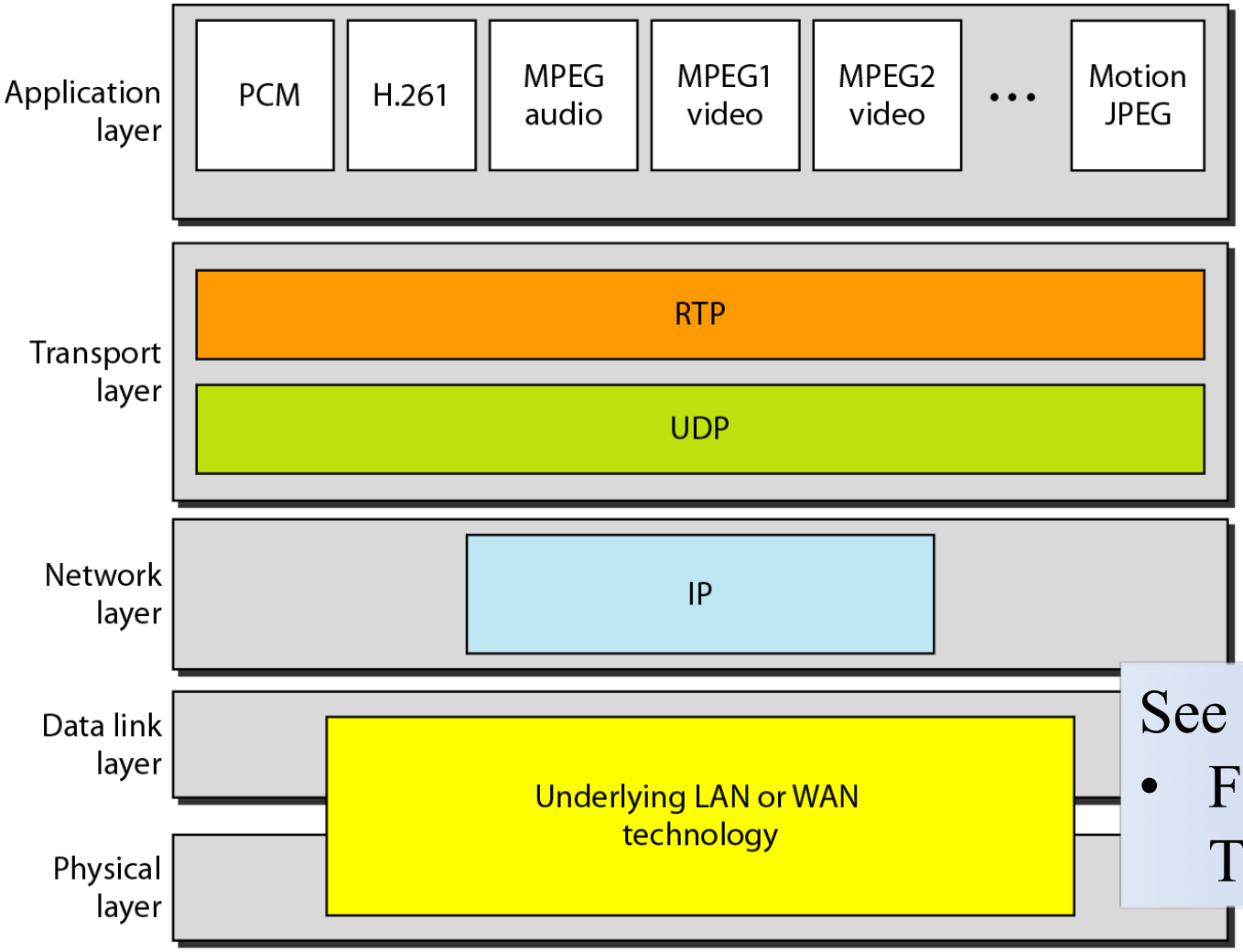


Real-Time Transport Protocol (RTP)

- Defined in RFC 3550
- Best suited to soft real-time communication
- Lacks the necessary mechanisms to support hard real-time traffic
- Two protocols that make up RTP are:



Real-time Transport Protocol



See
- Fig 25.7 RTP Header
  Table 25.1 Payload types

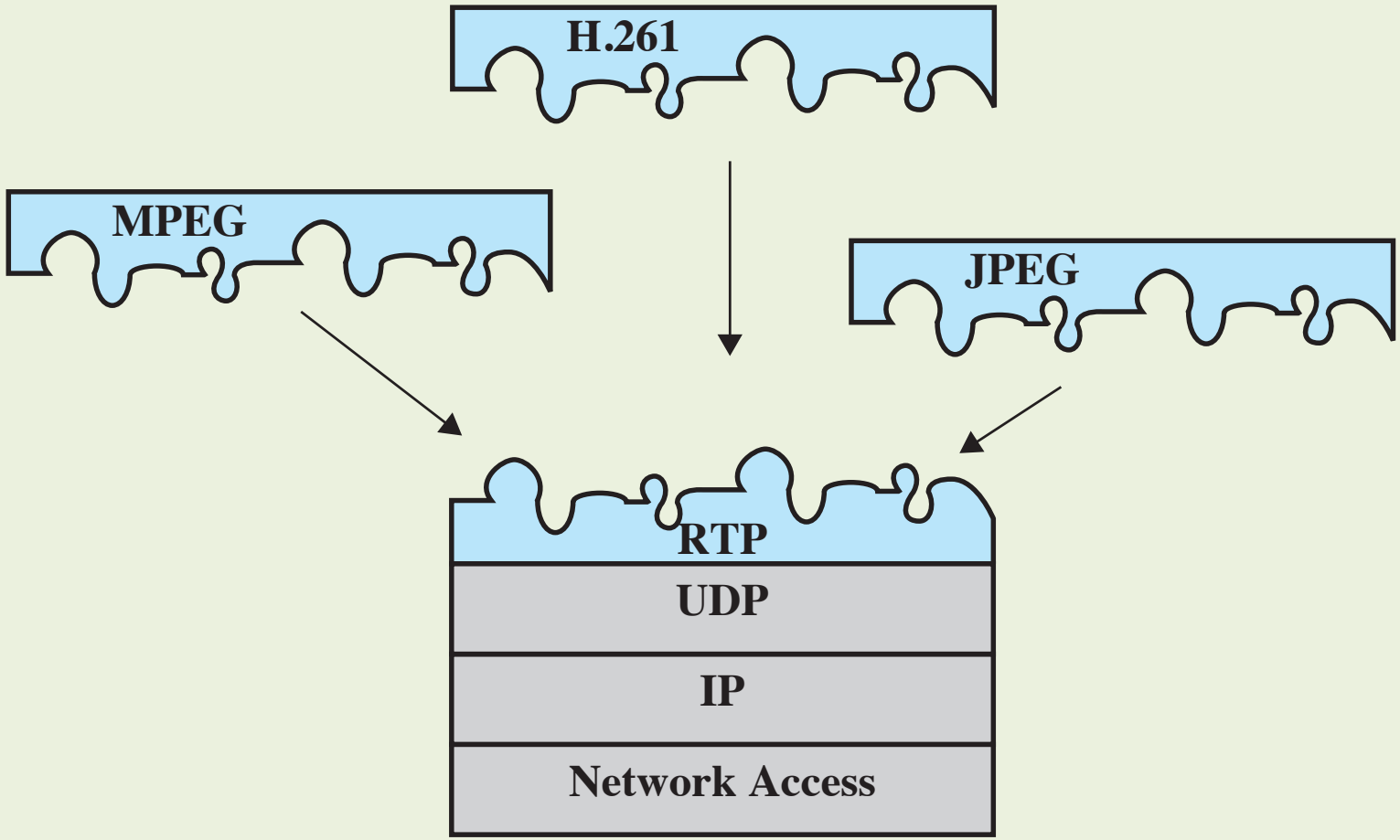


Figure 25.6 RTP Protocol Architecture [THOM96]

RTP Concepts

- RTP supports the transfer of real-time data among a number of participants in a **session**
  - A session is a logical association among two or more RTP entities that is maintained for the duration of the data transfer
    - Defined by:
      - RTP port number
      - RTCP port number
      - Participant IP addresses

Real-time Transport Protocol

- RTP handles real-time traffic
- No delivery mechanism
  - Uses UDP/IP
- Contributions
  - Time-stamping
  - Sequencing
  - Mixing

RTP Relays

- A relay operating at a given protocol layer is an intermediate system that acts as both a destination and a source in a data transfer
- Two kinds:
  - Mixer
  - Translator

Mixer

- RTP relay that receives streams of RTP packets from one or more sources, **combines** these streams, and forwards a new RTP packet stream to one or more destinations
- May change the data format or simply perform the mixing function
- Provides the timing information in the combined packet stream and identifies itself as the source of synchronization
- Example: Audio / video session with several participants

Translator

- A simple device that produces one or more outgoing RTP packets for each incoming RTP packet
- May **change** the format of the data in the packet or use a different lower-level protocol suite to transfer from one domain to another
- Examples of translator use include:
  - Convert a video to a lower quality format
  - If an application-level firewall prevents the forwarding of RTP packets, two translators can set up tunnel
  - Replicate an incoming multicast RTP packet and send it to a number of unicast destinations

Real-time Transport Control Protocol (RTCP)

- RTP only carries data
  - Sessions initialised by SIP (Session Initiation Protocol)

- RTCP carries control messages
  - Flow control
  - Service quality
  - Feedback to source

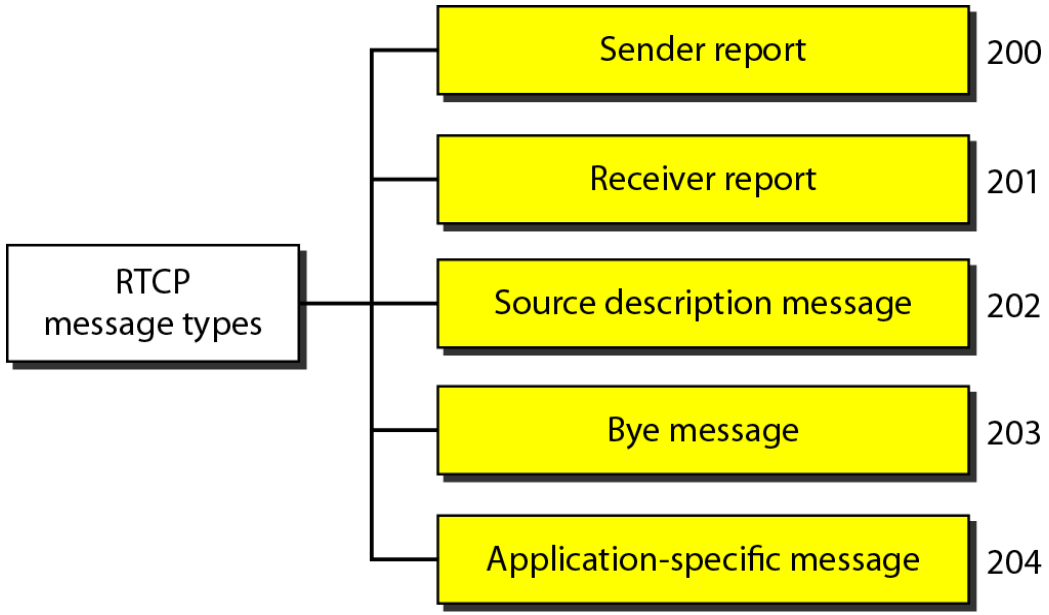
Sender report

- Sent by active senders
  - Periodical
- Statistics
  - Transmission
  - Reception
- Absolute timestamp
  - Receivers can synch RTP messages
    - Important for audio and video

Receiver report

- Sent by listeners
  - Not sending RTP packets
  - Feedback about QoS

And others…



Some multimedia applications

Two-way

- Skype
- Webex
- Adobe Connect
- Zoom
- …

One-way

- Youtube
- Netflix
- Spotify
- Play channels
  - Free or subscribed
- …

Many of these use TCP!

Problem

- The user often expects the same, or better, QoE than terrestrial broadcast
- Internet based applications has to cope with
  - Best effort
  - Cramped access networks
  - Bad channels
    - DSL
    - WiFi
    - Mobile