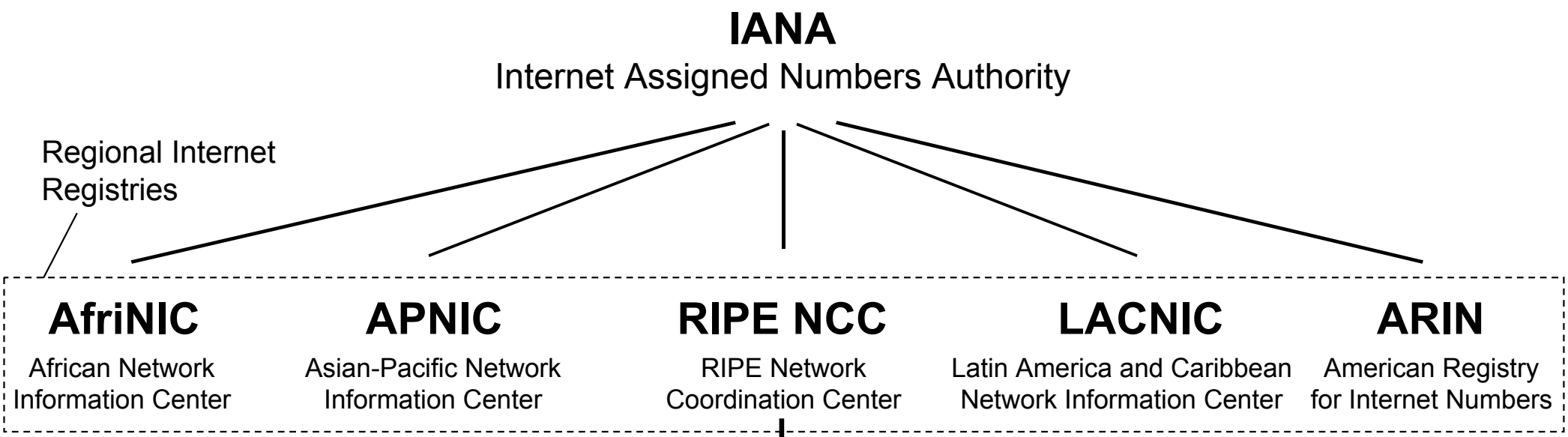
Further Addressing Issues

IP Address Assignment to Organizations/Netw. Providers



Address assignment examples:

- **DFN-Verein:** 6 x 16 bit prefix
  e.g. 193.174.0.0/16
- **BT-CONCERT:** 1 x 16 bit u. 1 x 19 bit prefix
  62.180.0.0/16
  195.182.96.0/19
- **VIA Networks:** 1 x 19 bit prefix
  212.14.64.0/19

IP Address Assignment within an Organization

- The partitioning of an organization's address range into subnets is performed according to the rules for structured address planning
- For assigning IP addresses there are 2 possible procedures:
  - **static IP address assignment**: the host is configured statically with a valid IP address and subnet mask (of the address range of the subnet it is connected to)
  - **dynamic IP address assignment:** when establishing a connection to the network, the host is dynamically assigned an IP address and subnet mask → **Dynamic Host Configuration Protocol (DHCP, RFC2131)**
    (Note: DHCP is part of many operating systems, successor of **bootp**)
- Motivation for dynamic address assignment (DHCP):
  - address shortage: more hosts than network addresses - but not all hosts are connected to the network at the same time
  - mobile hosts: hosts can be connected to different subnets of the organization - they receive an IP address from the corresponding subnet address range

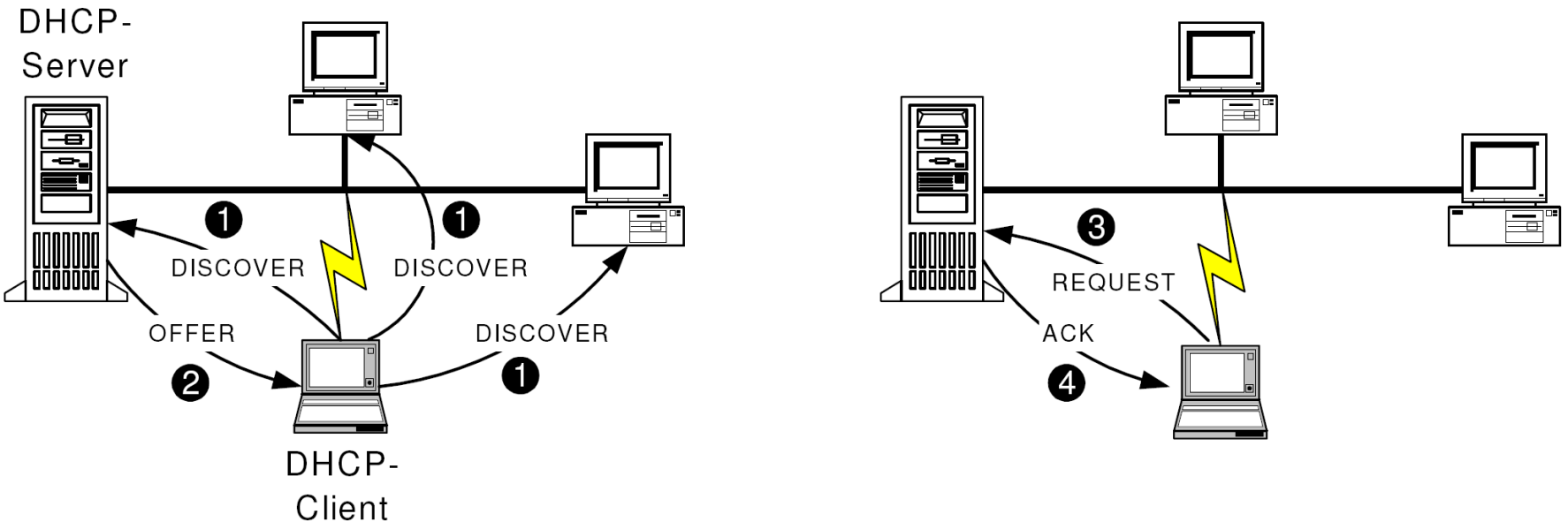
IP Address Assignment with DHCP - Mode of Operation

- A host joining a network searches for a DHCP server
- The DHCP server assigns a configuration to the host:
  - unused IP address
  - subnet mask
  - address of the Domain Name System server (DNS server)
  - address of the default router of the network (default gateway)
  - further optional parameters
- DHCP runs on IP/UDP port 67 (DHCP server) and port 68 (Client)

IP Address Assignment with DHCP - Types of Assignments

- **manually**: the network administrator keeps a mapping list (MAC address → IP address) on the DHCP server; the IP address is assigned to a host (as soon as it connects) for a long or unlimited time
- **automatic**: an unused IP address from the DHCP server's address pool is automatically assigned to the host for an unlimited time
- **dynamic**: an unused IP address is assigned to a host for a specific time defined by the host (**Lease-Time**); the reservation has to be renewed until then or the address will be revoked

IP Address Assignment with DHCP - Basic Principle



- The host (= DHCP client) sends a DHCP-DISCOVER (1) via (local) broadcast (to port 67 = bootp)
- A DHCP server responds with a DHCP OFFER (to port 68 of the DHCP client) and appends a possible network configuration (2)
- If the host accepts the configuration, it sends a DHCP-REQUEST (3) to the DHCP server (whose address is known now)
- If the DHCP server agrees, it responds with DHCP ACK (4)

IP Address Assignment with DHCP - Lease-Time

- In case of dynamic address assignment the host may only use the IP address for a specified time (lease time)
- 2 threshold times:
  - T_1 = 50% of the lease time
  - T_2 = 87,5% of the lease time
- After T_1 the host tries to renew the lease (by sending a DHCP REQUEST to the DHCP-Server)
- If there is no renewal (from the DHCP-Server) until T_2, the host requests a new DHCP server via broadcast (DHCP-DISCOVER)
- After the lease time passed the IP address may be assigned to other hosts without warning

IP Address Assignment with DHCP - DHCP Relay Agents

- Often it is too much effort to administrate a DHCP server for each subnet
- But the DHCP discovery via local broadcast is restricted to the local subnet (where the host resides)
- **DHCP Relay Agents** can forward requests to other subnets - in this case multiple subnets may share a DHCP server
- Modern routers integrate the DHCP Relay Agent service - no designated Relay Agent has to be administrated

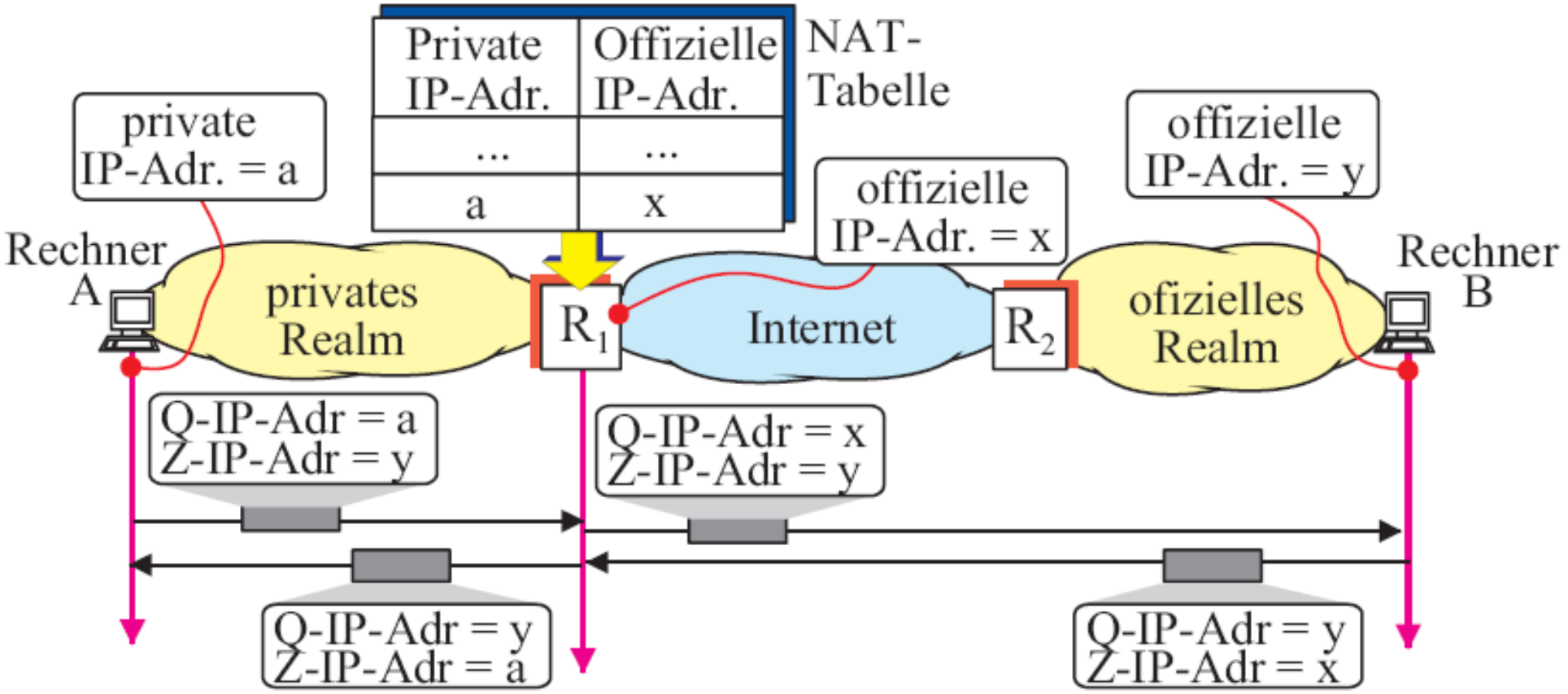
Network Address Translation (NAT)

- Application: use of private IP addresses within an organization and translation of these private addresses to one or multiple public addresses to the outside (Internet)
- Benefits:
  - no address shortage within the organization's network → simplified address planning
  - "hiding" of internal hosts from the outside: no externally initiated communication possible as internal IP addresses are not visible from outside
- NAT types (RFC2663):
  - 1:1 mapping between public and private IP addresses: **traditional NAT**
  - 1:n mapping between a public and n private IP addresses: **NAT with SUA** (Single User Account feature), also known as **NAPT** (Network Address Port Translation) and **PAT** (Port Address Translation) or **IP-Masquerading**

Network Address Translation (NAT) - Traditional Mode

- Each organization-internal host are assigned two IP addresses: one private (internal) and one (possibly dynamically assigned) public (external) address; the host only knows and uses the private address
- Only the router (Gateway) at the border between the internal network and the external Internet knows both addresses and maintains a mapping table that allows to map between both addresses:
  - static mapping: fixed mapping between public and private address
  - dynamic mapping: on-demand mapping of private to public address (in case a host demands communication to the outside; only valid during the external communication)
- Because usually there are less external addresses available than internal hosts, in classical NAT only a subset of the hosts may connect to the Internet simultaneously

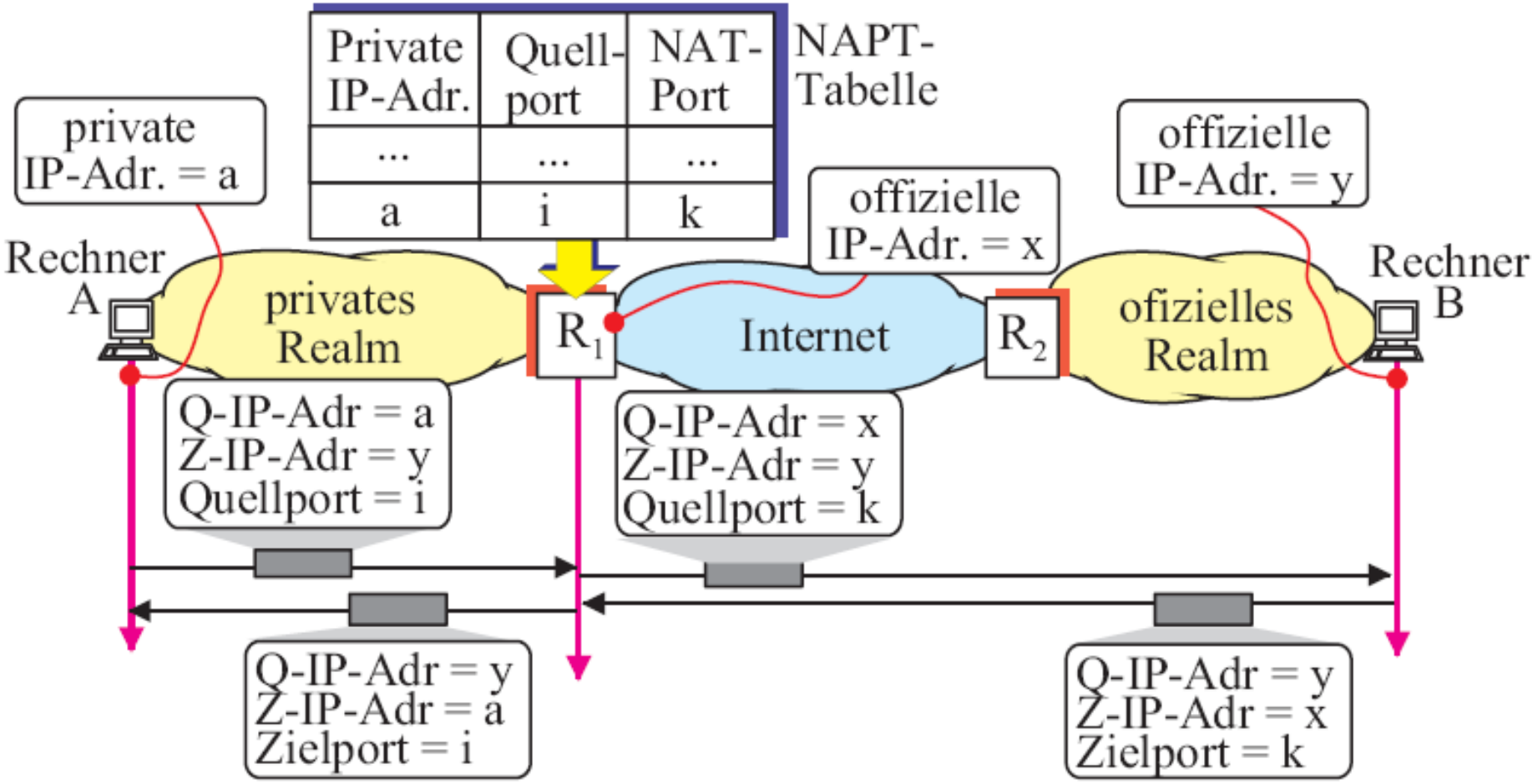
Network Address Translation (NAT) - Traditional Mode



Network Address Translation (NAT) - NAPT

- If only one external (public) IP address is available, the classical NAT is inappropriate
- To use one public address for multiple hosts, a further distinguishing criterion has to be applied → use of the source port number to uniquely identify a host
- Basic principle:
  - the gateway router replaces the private IP address of the host with the public IP address and the source port number (that only has local meaning and can be arbitrarily chosen by the host) with a new port number which is uniquely mapped to the host's IP address (mapping table: new port number → host IP address and original port number); Note: in this case the gateway router has to recalculate the header checksum
  - the communication partner in the Internet responds to the public IP address and new port number
  - the gateway router can derive the private host IP address and original port number according to its mapping table
- Problem: some applications require public IP addresses or port numbers (for externally initiated communication) (e.g. ftp, SIP)

Network Address Translation (NAT) - NAPT



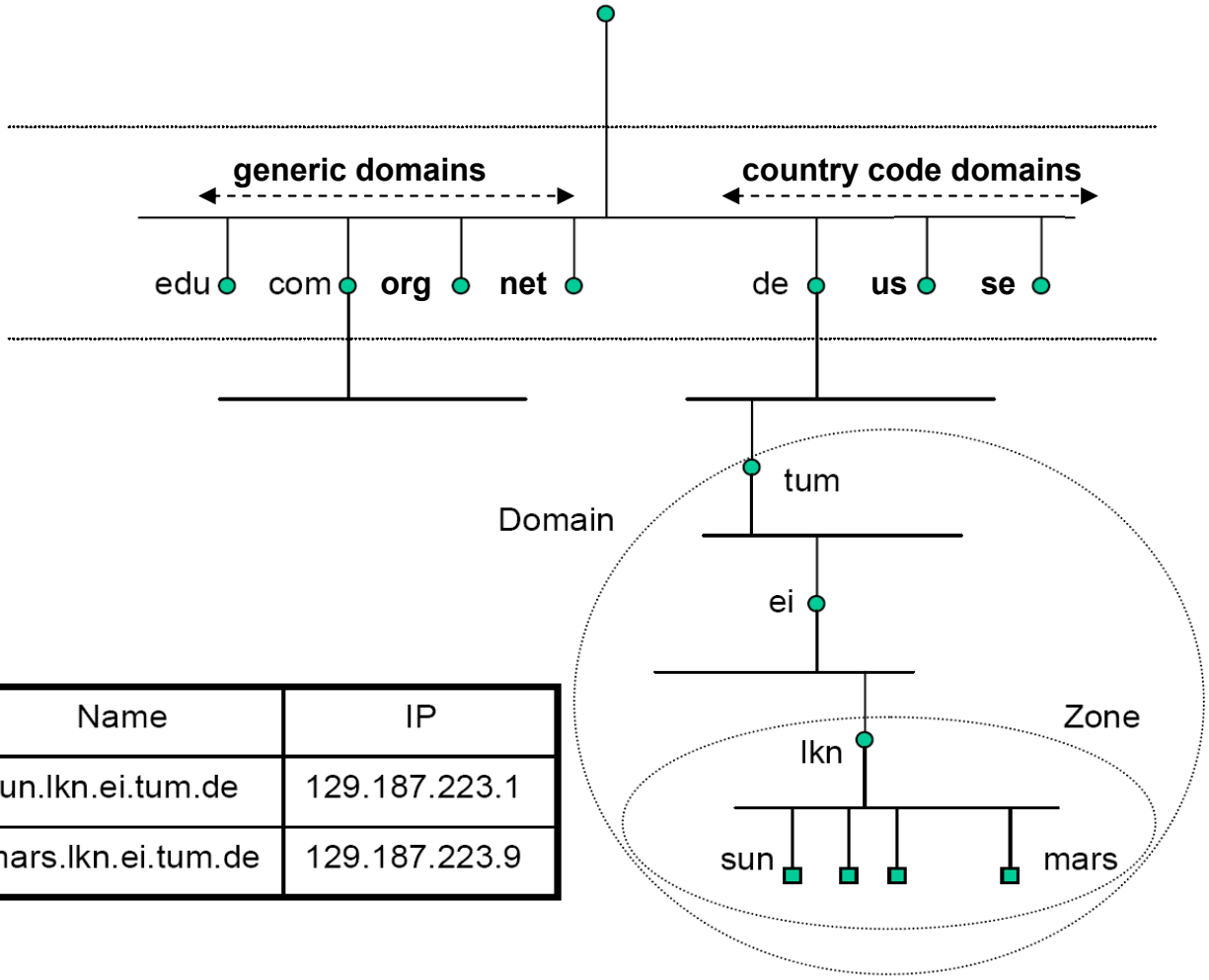
Names and Addresses in the Internet

- Definition **“address"**:
  - hints the route to the destination - usually refers to a location
- Definition **“name"**:
  - identifies a resource independent of its location (“resource ID")
- Names and addresses in the Internet:
  - **IP address**: tells in which network a system (Host, Router, Server etc.) is located; assigned per network interface; required for routing
  - **Domain name**: identifies a system in the Internet without referring to a location (i.e. the network it is connected to); the mapping between domain name and IP address of a system is performed by the Internet **Domain Name System (DNS);** benefit: users can memorize names more easily than IP addresses
  - **Resource name**: identifies a unique resource (e.g. website in case of WWW) on the Internet; typical resource names are **URIs** (Uniform Resource Identifier) and **URLs** (Uniform Resource Locator)

Names and Addresses - Domain Name System (DNS)

- Characteristics of DNS:
  - distributed database with a hierarchy of **Name Servers** in the Internet
  - protocol at application layer which governs the communication with name servers; uses UDP, port number 53
  - client server model; server may forward requests to other servers
  - also used by protocols at application layer to resolve names (HTTP, SMTP, FTP etc.) - DNS is a core function in the Internet
  - key task: resolve domain names to IP addresses
  - domain names are structured hierarchically and represent one or multiple IP addresses

Names and Addresses - DNS Namespace Structure



Name	IP
sun.lkn.ei.tum.de	129.187.223.1
mars.lkn.ei.tum.de	129.187.223.9

Root Domain

Top Level Domains (TLD)

Domains

Hosts

Names and Addresses - DNS Namespace Structure

- Domain associations:

generic TLDs (gTLD)
.com = commercial
.net = administrative organizations
.org = other organizations
.int = international organizations
.edu = education (de facto US only)
.gov = government (US only)
.mil = military (US only)

→ **76% of all domains**

country code TLDs (ccTLD)
.de = Germany
.fr = France
.uk = United Kingdom
.at = Austria
.au = Australia
.....
country code acc. to ISO 3166

→ **24% of all domains**

Names and Addresses - DNS Name-Server Hierarchy

- Types of name servers:
  - **Root Name Server**
    - contain only entries for Top Level Domains (TLD)
    - only 13 root name servers worldwide
    - root name server locations see: http://www.root-servers.org
  - **Top-Level Domain (TLD) Name Server**
    - server responsible for the TLD
    - contain entries about the autoritative name server of a TLD
  - **Autoritative Name Server**
    - each host is registered at such a server
    - is often also the local name server in its network
  - **Local Name Server**
    - usually each organization (company, university, provider) maintains a local name server
    - a request is always sent to the local server first (default server)

Names and Addresses - DNS Name-Server Hierarchy

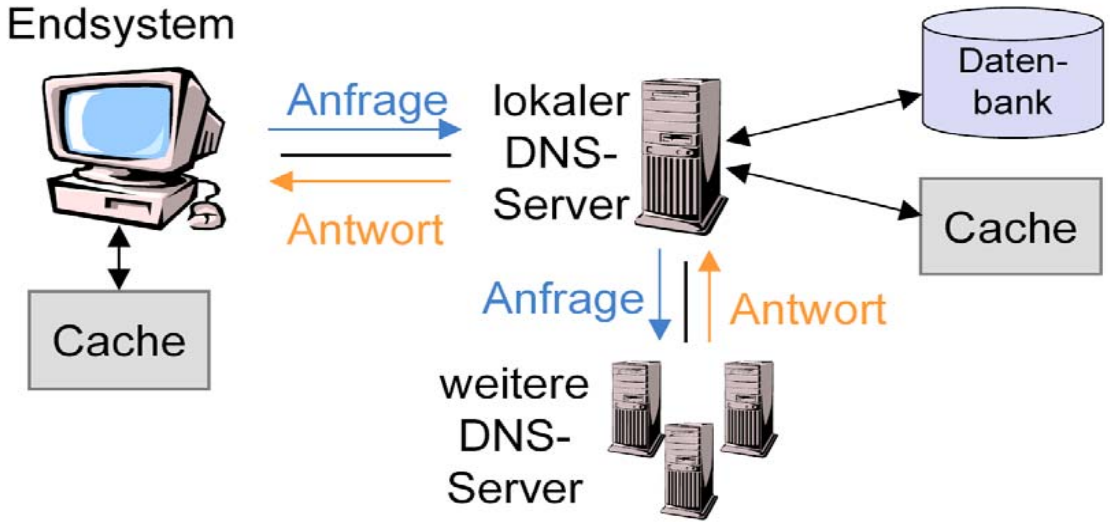
- Name servers in each hierarchy layer (= domain) do:
  - know one root name server
  - know name servers for the hierarchy layers below
  - contain entries they are responsible for (i.e. for entries within their domain); they have the authority to assign names within their domain
  - the results of previous requests are cached; the storage duration is governed by a timeout (typically multiple days)

Names and Addresses - DNS Resolver

- Applications that use the DNS name service use a so-called **Resolver**
- The Resolver knows the IP addresses of one or multiple local name servers; their addresses are either statically assigned by the network administrator or dynamically via DHCP
- The Resolver asks its local name server and provides the answer to the respective application

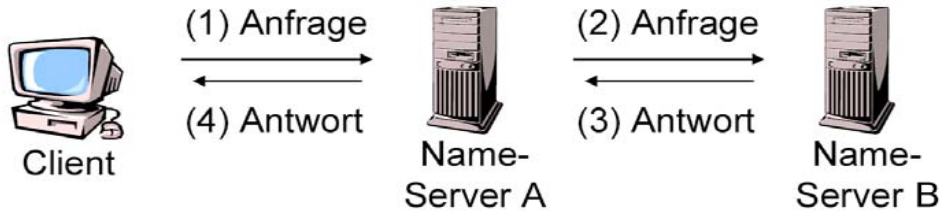
Names and Addresses - Procedure of a DNS Query

- In case a host does not have a reply cached, it queries a local name server
- The local name server replies with entries from:
  - its local database (if it is autoriative)
  - its own cache if previous queries are cached
  - other name servers (in case the local name server has no own info)

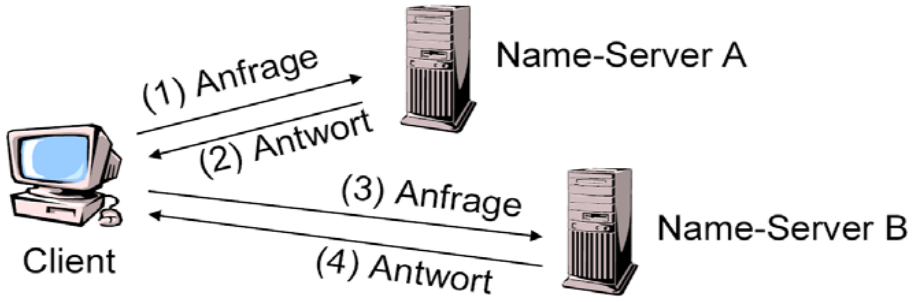


Names and Addresses - Types of DNS Queries

- Recursive query:
  - in case the queried server does not know the answer, it requests further servers until it can respond with an answer
  - benefit: less overhead for the client because the name resolving is done by the servers

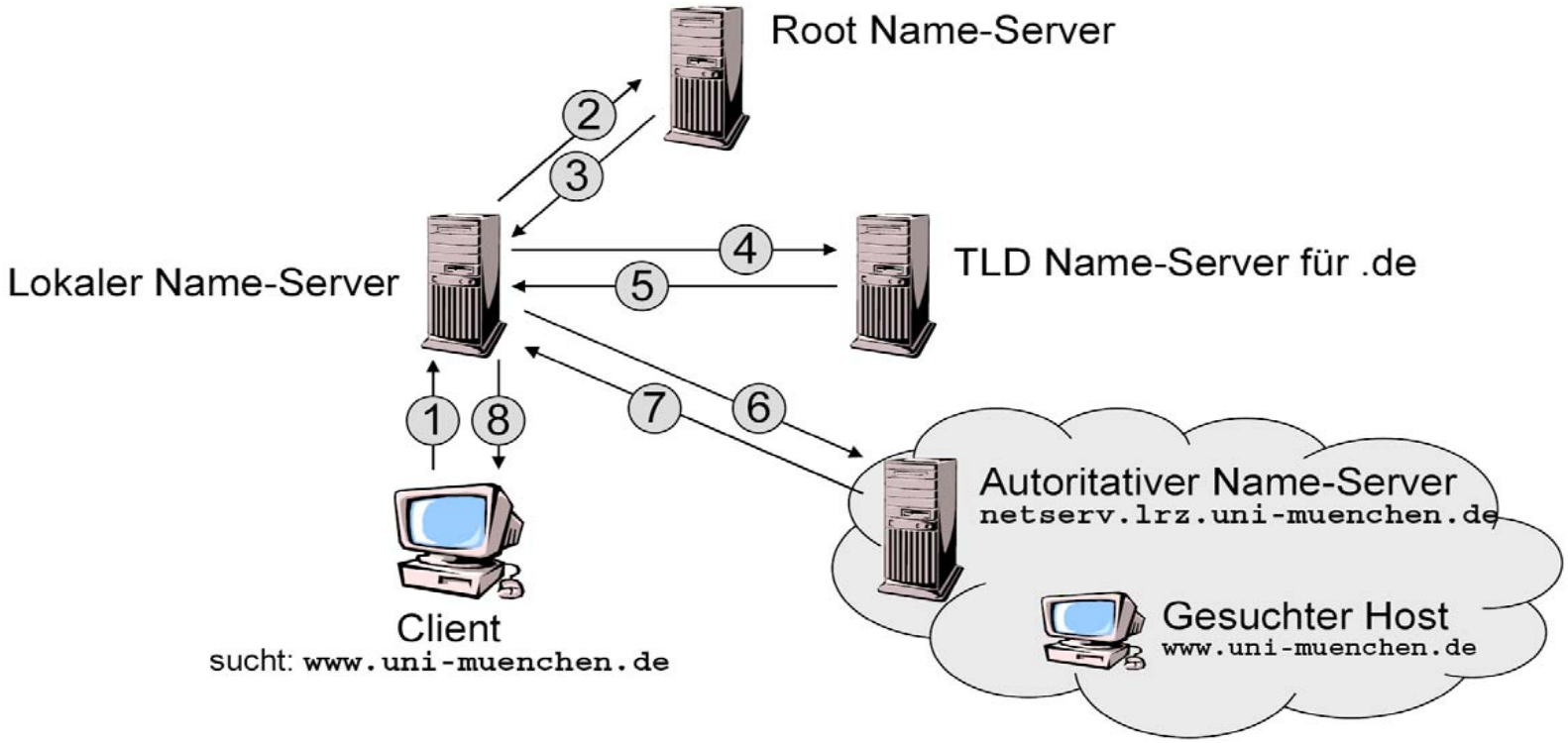


- Iterative query:
  - in case the queried server does not know the answer, it can provide references to other servers; the client itself will query these servers
  - benefit: less overhead for the name server that was initially queried



Names and Addresses - DNS Query Example

- Example: http://www.uni-muenchen.de is queried by the web browser of a client host



- typically a client queries its local name server recursively, the local name server then queries other servers iteratively

Names and Addresses - DNS Resource Records (RR)

- Data related to domain names is stored as so-called **Resource Records (RR)** in the databases of the name servers
- The name server replies contain one or more RRs
- RR format: (Name, Value, Type, TTL)
- RR Types:
  - type = A or type = AAAA

    Name = host name, Value = IPv4 or IPv6 address of the host
  - type = NS

    Name = domain, Value = IP address of autoritative servers for this domain (= server that knows how IP addresses of this domain can be retrieved)
  - type = CNAME

    Name = alias hostname, Value = canonical host name

    with that the canonical name of a host can be obtained
  - type = MX

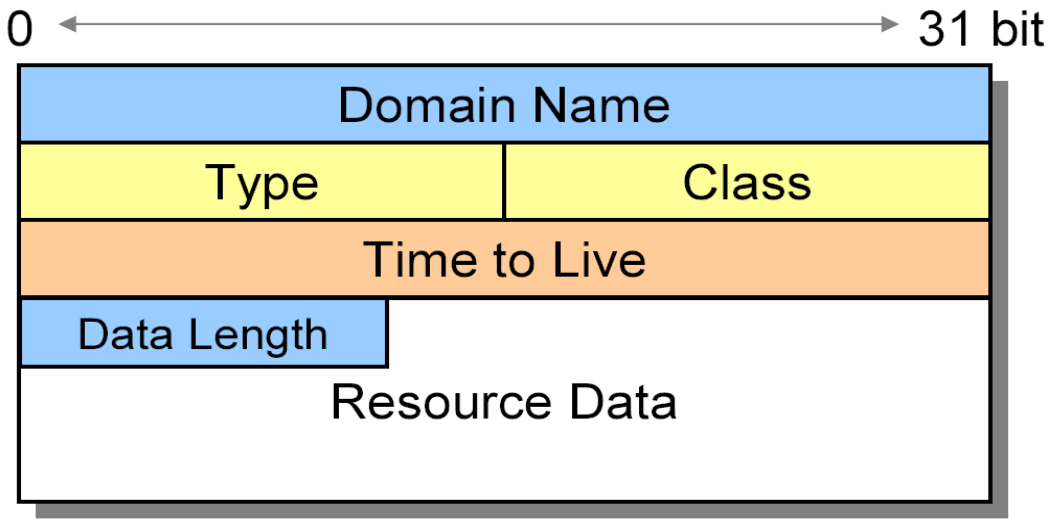
    Name = alias host name, Value = hostname of an email server

Names and Addresses - DNS Resource Records Details

- Types of Resource Records (RRs):

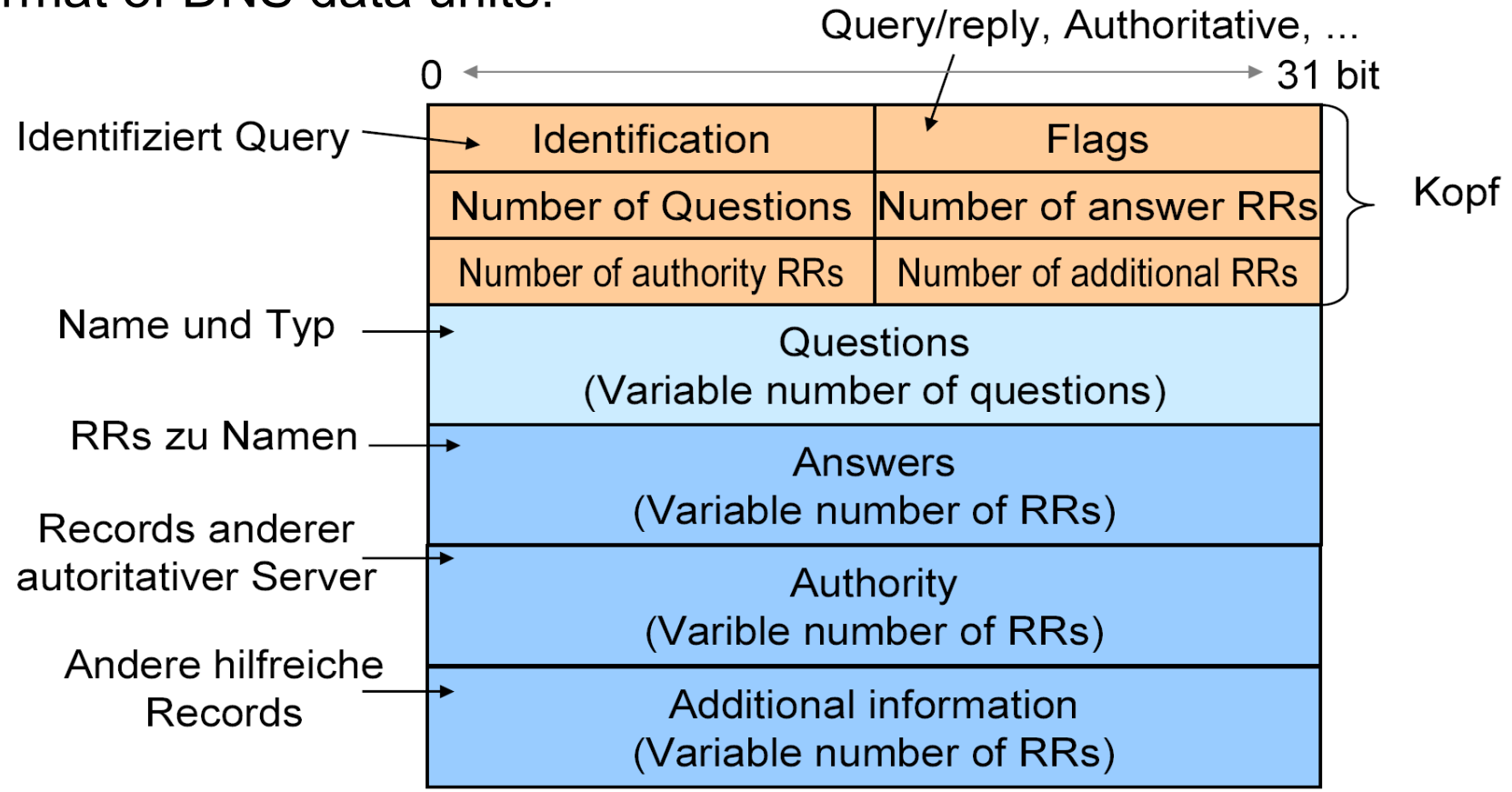
Typ	Beschreibung
A bzw. AAAA (Address)	Abbildung Name auf IPv4/IPv6-Adresse
MX (Mail Exchange)	E-Mail-Server einer Domäne
NS (Nameserver)	Nameserver einer Domäne
CNAME (Canonical Name)	„Alias“-Namen für Rechner/Domänen
PTR (Pointer)	Abbildung IP-Adresse auf Name
HINFO (Host Info)	Zusätzliche Informationen (CPU, ...)

- Format:



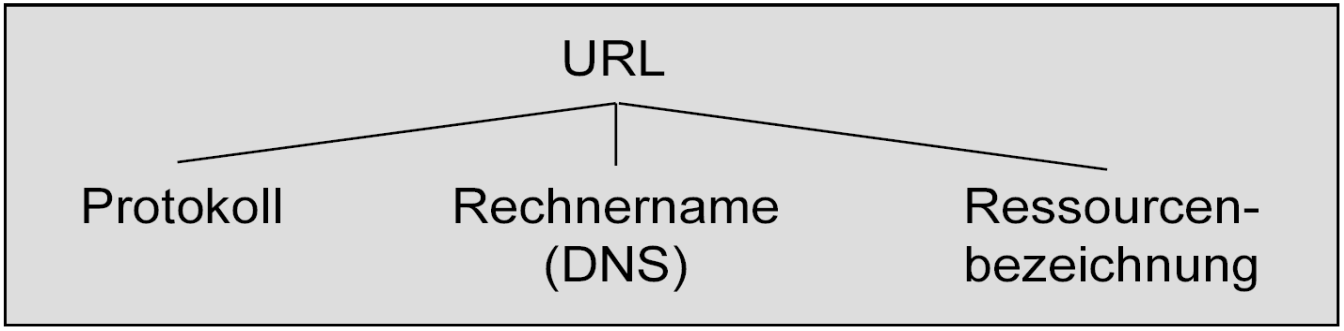
Names and Addresses - DNS Data Units

- Types of DNS data units:
  - Query
  - Reply
- Format of DNS data units:



Names and Addresses - URI/URLs

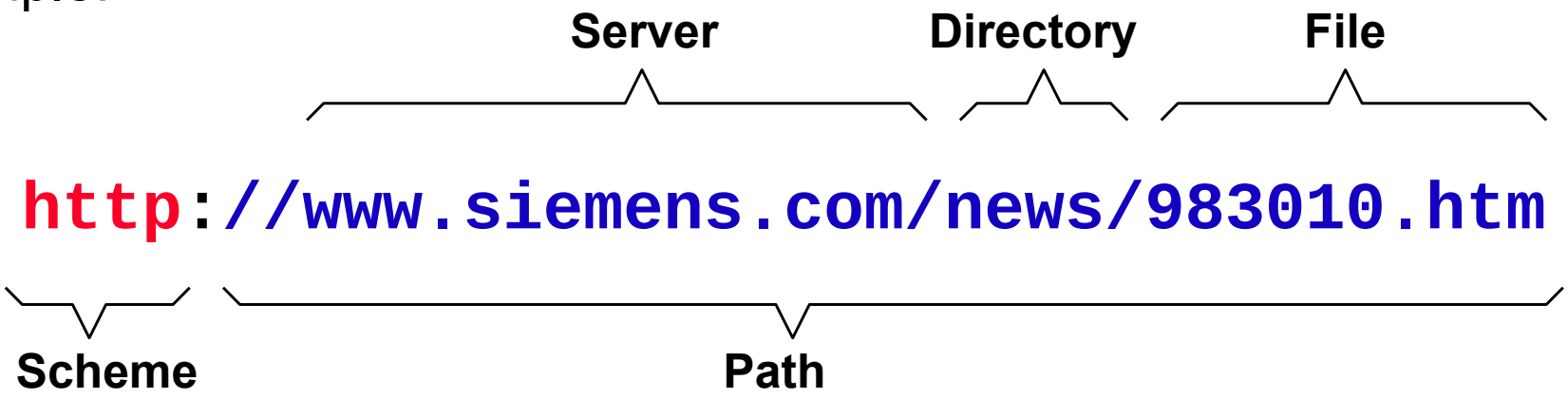
- **Uniform Resource Identifier / Locator (URI / URL)**
  - compact representation of a resource on the Internet (including the access method)
  - used by different Internet applications, e.g. WWW, FTP, Email
  - components:



  - the resource name identifies an accessible object on the server:
    - for WWW: website
    - for FTP: file
    - for Email: email recipient (i.e. email address)

Names and Addresses - URI/URLs

- A URL is a URI for objects in the Internet that might be accessed by using some existing protocol
- Abstract syntax of a URL: **<scheme>:<scheme specific part>**
- Example:



ftp	File Transfer protocol
http	Hypertext Transfer Protocol
gopher	The Gopher protocol
mailto	Electronic mail address
news	USENET news
nntp	USENET news using NNTP access
telnet	Reference to interactive sessions
wais	Wide Area Information Servers
file	Host-specific file names
prospero	Prospero Directory Service