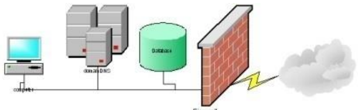
Management of Information Systems

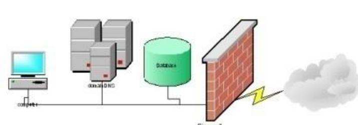
Dr Gusztáv Adamis
adamis@tmit.bme.hu

BME VIK TMIT



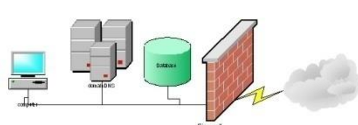
Refreshment

- Reference model, protocols
- IP bases
  - addresses, address classes
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP



OSI reference model

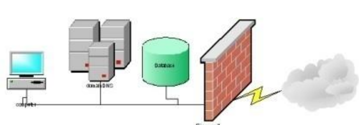
- 7 layers
  - Determines the tasks of the protocols used to control the communication among computers
  - Main goal: interoperation between devices of different suppliers
- Every layer uses ONLY the services of the layer below and provides service ONLY for the layer above
  - Protocol stack
  - SW / HW / combined implementation



Layer	Name		Function DATA SEGMENTS
7	Application	DATA	Application protocols, e.g. SMTP (e-mail – Simple Mail Transfer Protocol), HTTP (web), FTP (file transfer)
6	Presentation	DATA	Data presentation, encoding/decoding Data formats (e.g. MPEG), Character coding, compression, encryption
5	Session	DATA	Control of communication sessions (SCP – Session Control Protocol)
4	Transport	DATA SEG-MENTS	Data transfer between endpoints, reliability, virtual circuits, paths (e.g. TCP connections, port numbers)
3	Network	PACKETS	Logical addressing (e.g. IP addresses) and routing based upon them (routers)
2	Data Link	FRAMES	Interface (MAC) level addressing, Flow control, (bit)error detection & correction (bridge, switch)
1	Physical	BITS	Wire or fibre optic transmission medium among devices (hub)

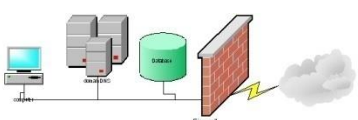
Layer characteristics

- Every layer uses the service of the underlying layer and offers service(s) to the higher layer
- The Interface between them determines the way of interaction/inter-communication
- Implementation details are hidden
  - Can be changed without an effect on the other layers (black box)
- Examples
  - Network topology and physical configuration/medium
  - Routing
  - Applications
  - New services/applications



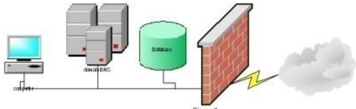
Protocols

- A module in the layered structure
- Set of rules that controls the communication between network elements
  - Applications, hosts, routers
- A Protocol Specification determines:
  - Interface to the higher layer (API)
  - „Interface” to peer entity
    - Message formats and possible sequences
    - Activities initiated by messages (Behaviour)



OSI 1. Physical layer

- Physical and electronic specification of the medium
  - Pin/connector structure
  - Electrical potential level (Volts)
  - Cable specifications, etc.
- Hub, repeater
- Main functions:
  - Physical connection establishment, release
  - Shared access to medium
  - Modulation/demodulation

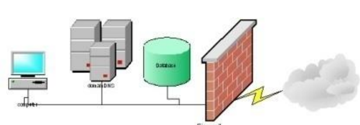


OSI 2. Data link layer

- Error-free transmission of messages (frames) between two neighbouring nodes
  - Framing
  - Indication and (optionally) correction of physical layer (~bit) errors
  - Hardware addressing (MAC addresses)
- Examples:
  - HDLC, LAPD, Aloha
- Bridge

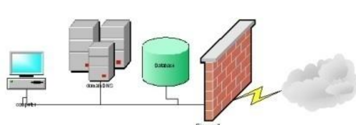
OSI 3. Network layer

- Transmission of messages between any nodes of the network (possibly through several networks)
  - Routing
  - Congestion control
  - SAR (Segmentation and reassembly)
  - Logical (IP) addressing
  - Traffic-based accounting
- Router



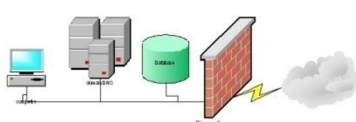
OSI 4. Transport layer

- Transparent transmission between users
- Connection establishment, reliability control (optionally)
- Virtual connections
- TCP



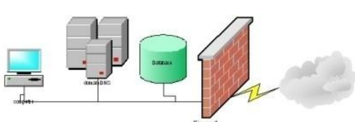
OSI 5. Session layer

- Dialogue management between end-users
  - Timer settings, termination, restart
  - Synchronization
  - Token management
- Actually log-in and log-off to and from the system



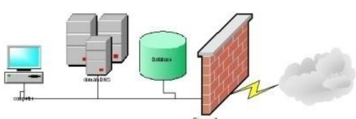
OSI 6. Presentation layer

- Ensures the data to be provided in an understandable format for the systems of of the end-users
  - Encoding, decoding
  - Code conversion (e.g. serial-XML)
  - Compressing/decompressing
  - Encryption



OSI 7. Application layer

- Communication between applications
  - negotiation
    - format
    - Security issues
    - synchronization
- HTTP, SMTP, FTP, Telnet

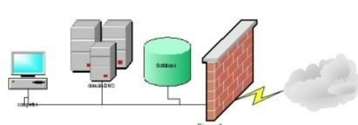


OSI – IP architecture

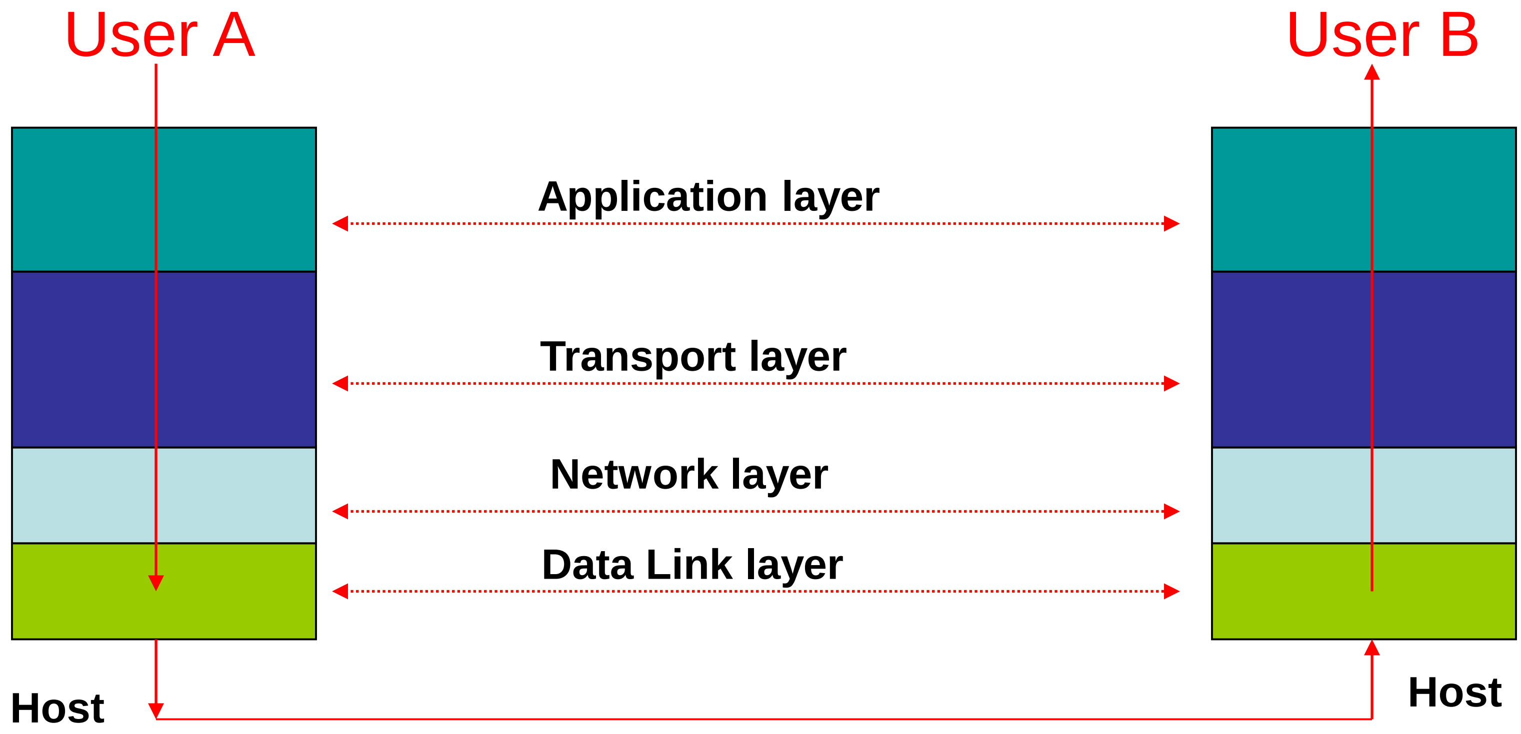
ISO/OSI	TCP/IP	Practical
Application	Application	Application
Presentation		
Session		
Transport	Transport Host-to-host (TCP/UDP/...)	TCP/UDP/...
Network	Internet (IP)	IP
Data link	Network interface Network access	LLC MAC
Physical		PCS & PMA PMD

IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
LLC: Logical Link Control

MAC: Medium Access Control
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

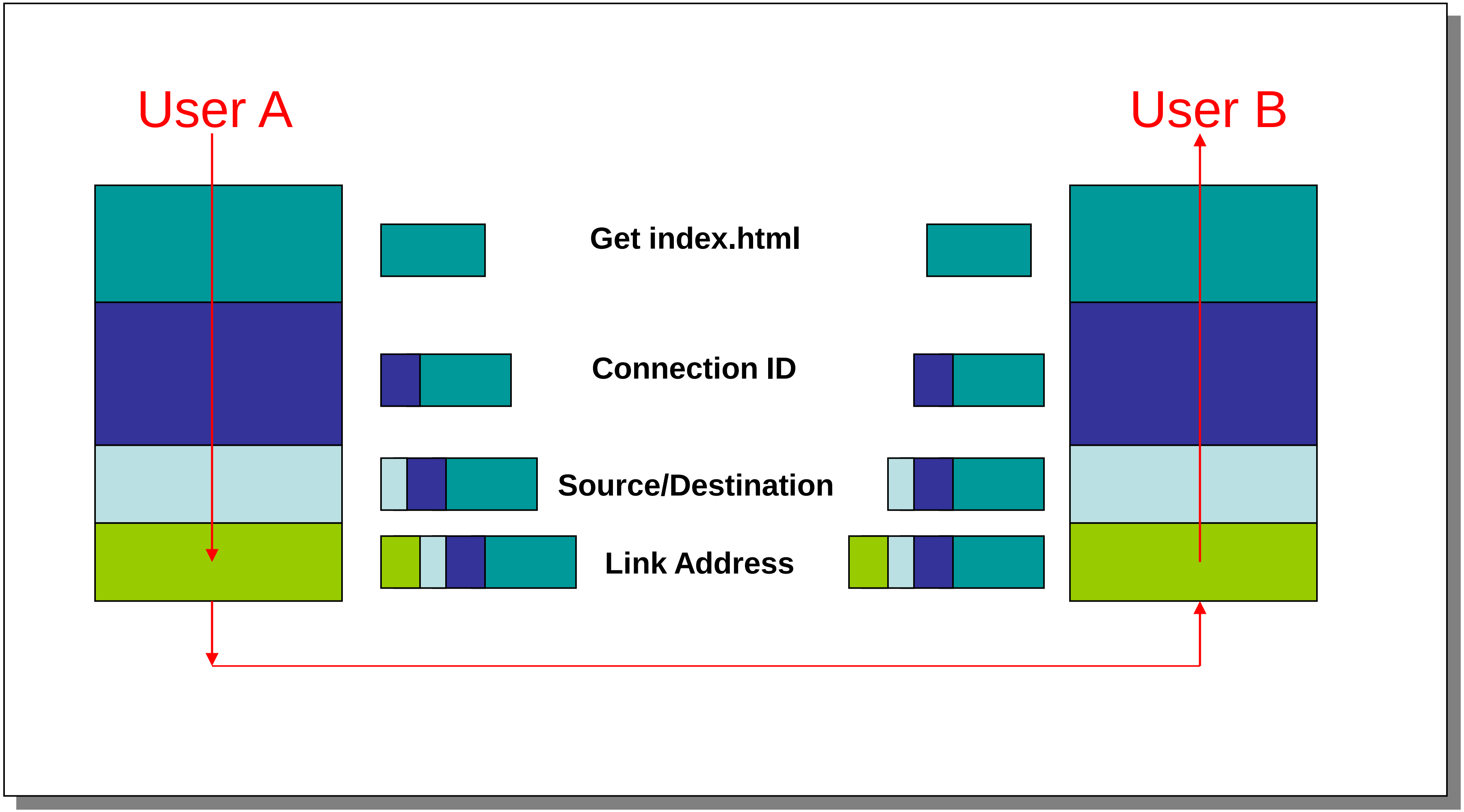


Layering



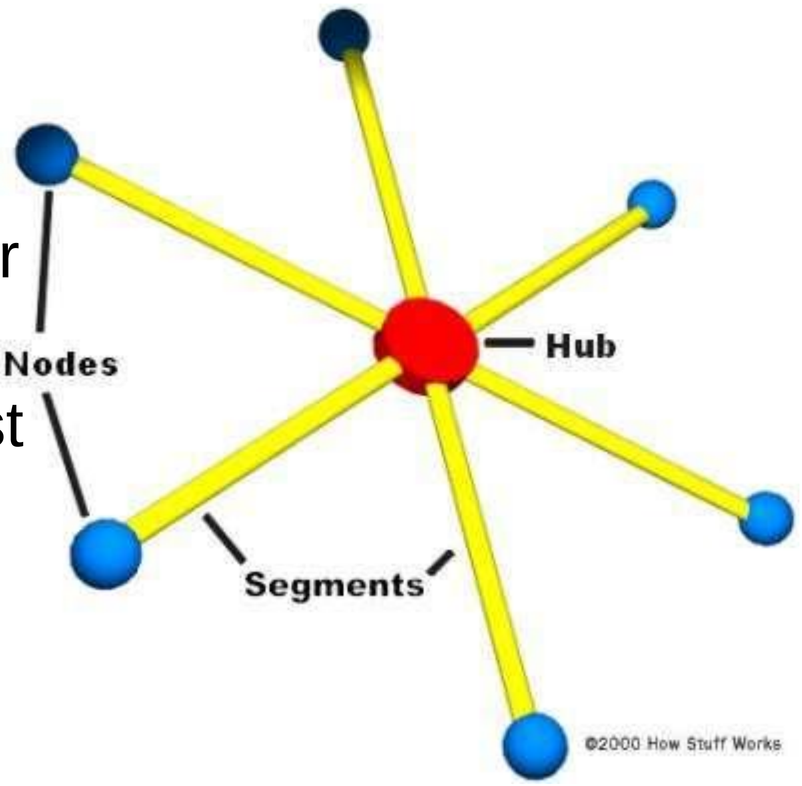
Layering: to simplify complex systems

Layering: Encapsulation



Hub, bridge, router, switch

- Hub
  - 1. (physical) layer
  - Broadcast
    - Input signal to all the other port,
    - No signal processing - fast
  - Ethernet with hub
    - Shared medium
      - -> collision detecting
      - -> waiting for resolving
      - -> shared bandwidth
      - -> half duplex



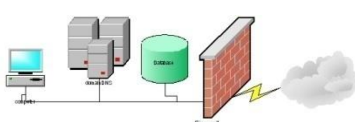
Hub, bridge, router, switch

- Bridge
  - 2. (data link) layer
  - Frame analysis, MAC (physical) address based routing
    - No collision, but slower procession
    - Dedicated internal connections
    - Since no broadcasting – multiple connections

      -> Dedicated (full) bandwidth
  - Transparent (adaptive bridges)
  - Source controlled
- But when is the hub better???

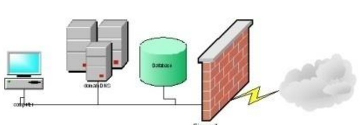
Hub, bridge, router, switch

- Router
  - 3. (network) layer
  - IP (!!) address based routing
  - Interconnects two or more IP *subnetworks*
  - Actually a special-purpose mainframe computer

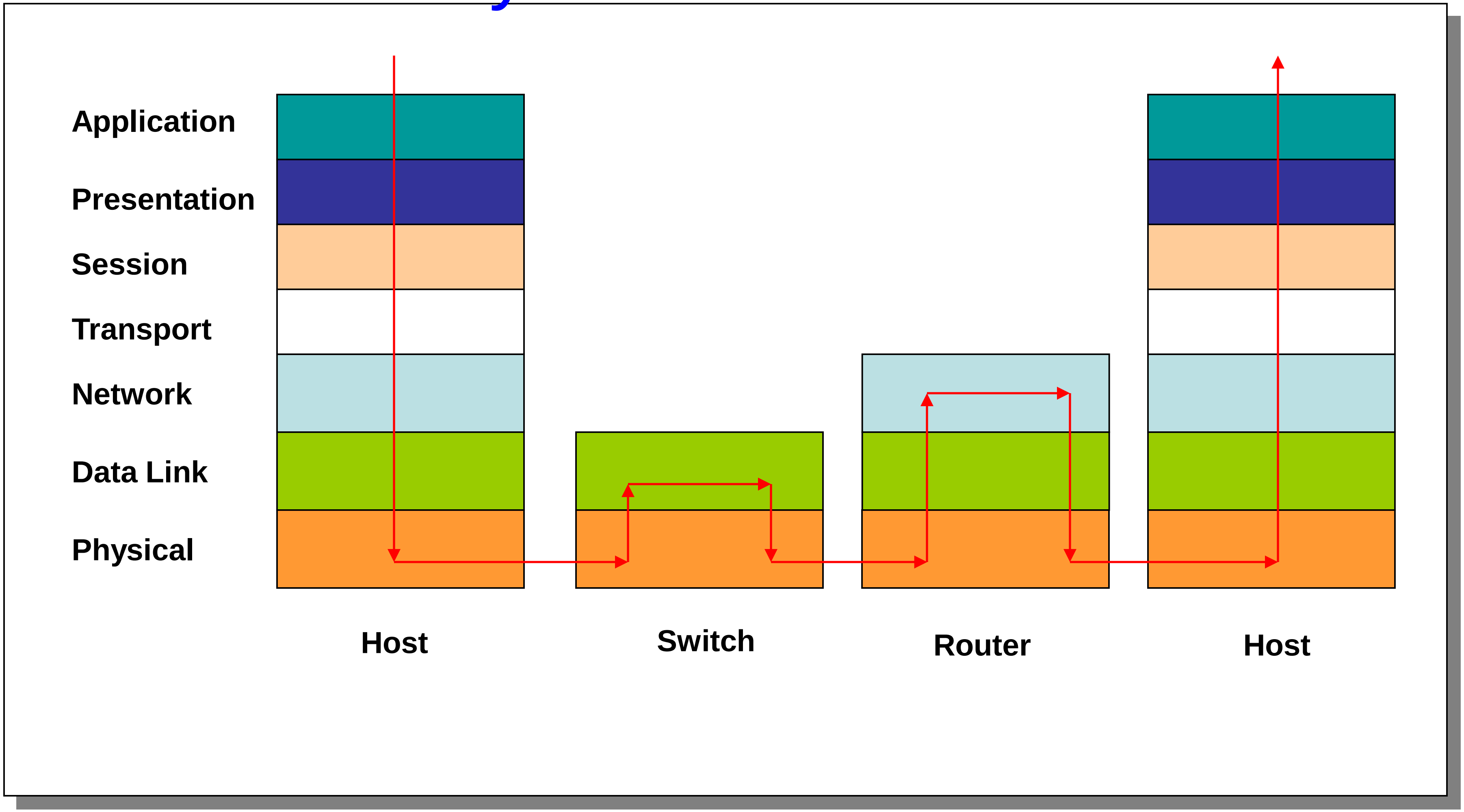


Hub, bridge, router, switch

- Switch
  - Commercial phrase
  - Typically used instead of bridge
  - But switches can work in higher layers, too
    - 4. (transport) layer:
      - NAT
      - load sharing based on TCP session
      - stateful firewall
    - 7. (application) layer
      - load sharing based on URL
      - application level transaction management

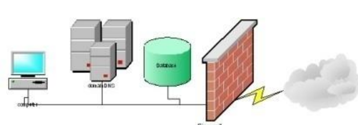


Places of the network equipments in a layered structure



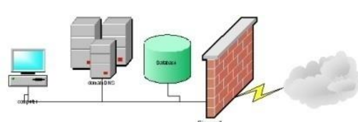
Layering

- Now, is it worth?
  - Mainly yes, but
  - Sometimes...
    - Nth layer duplicates the functions of an underlying layer (e.g.: error detection and correction),
    - Same piece of information needed in several layers
      (e.g.: time-stamp, Maximum Transmission Unit - MTU),
    - Price: power (speed, efficiency)

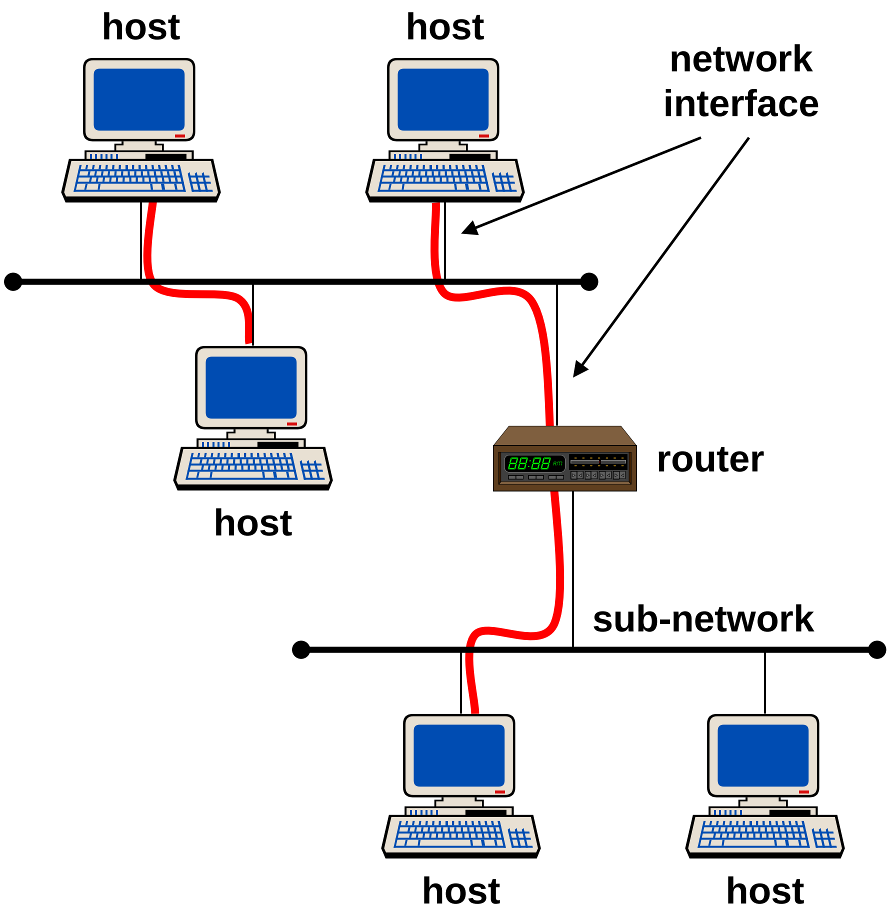


IP refreshment

- IP bases
  - Addresses, address classes
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP



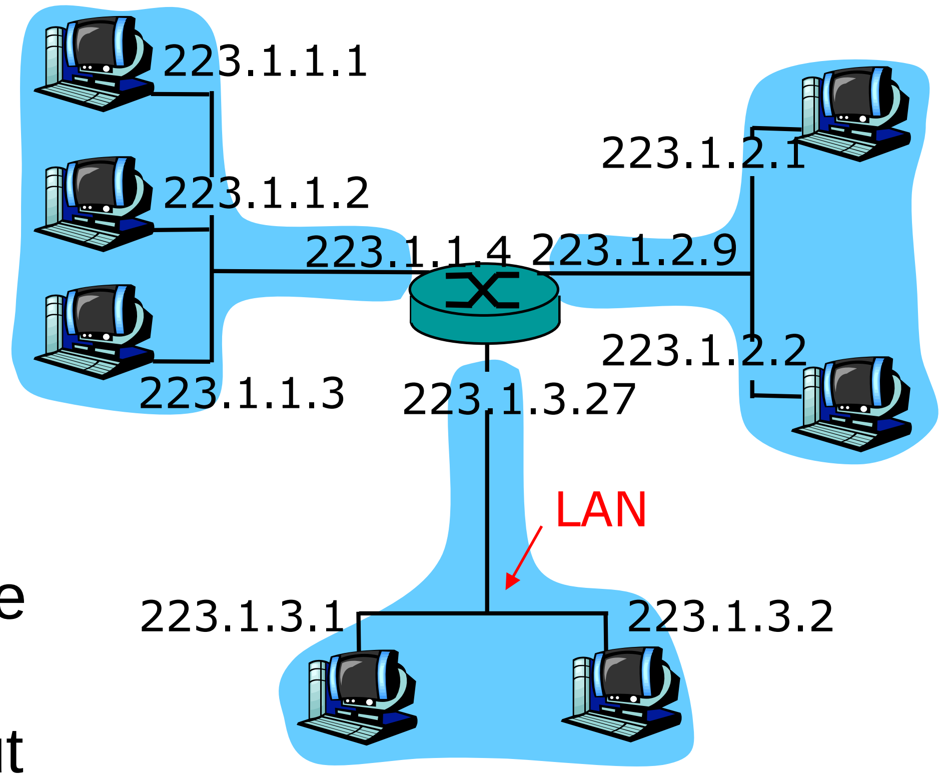
Elements of an IP network



- **Host**: communication endpoint
- **Sub-network**: physical network, the connected nodes can communicate directly
- **Router**: transmits the messages between hosts of different sub-networks
- **Interface**: connection point of a node to a sub-network

IP addresses, networks

- IP address:
  - network address (high order bits)
  - host address (low order bits)
- *Network?* (from point of IP)
  - interface with the same network address
  - interconnection without a router between these devices

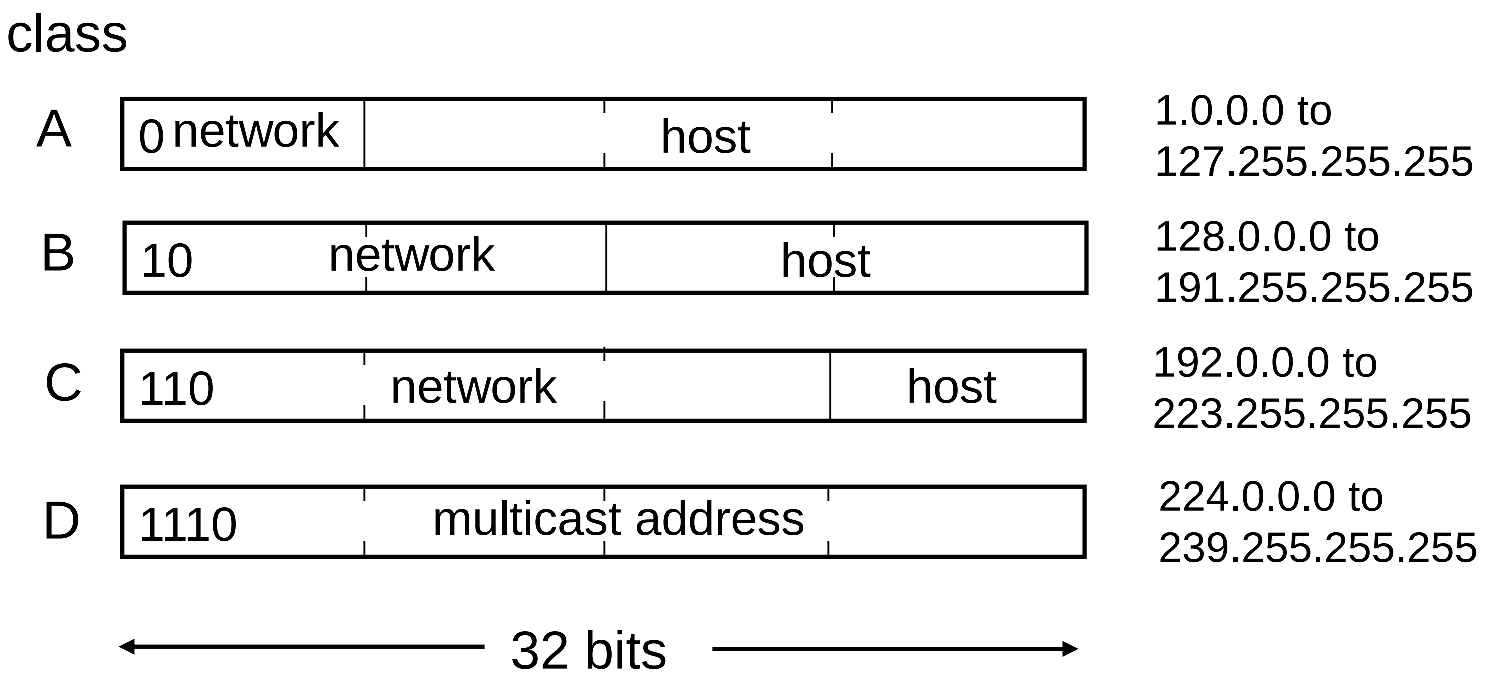


24 bits long network addresses

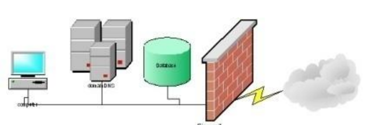
10011000	10000010	11110110	00000010
152	130	246	2

→ **152.130.246.2** ← **dotted decimal notation**

IP address classes

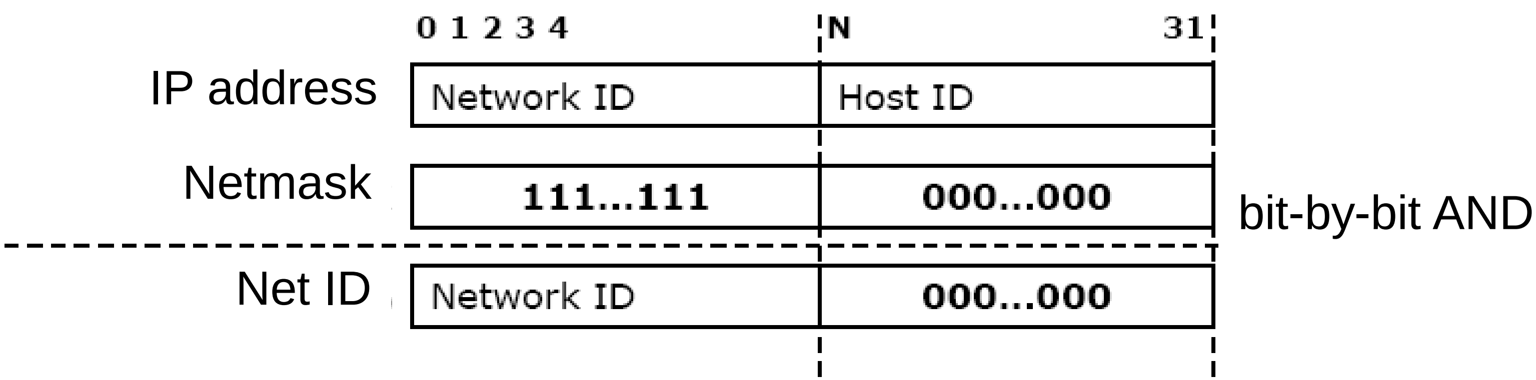


- Theoretically 2^{32} (~4.3 billion) addresses, but in practice only ~3.3 billion
- Not flexible enough – consumes the IP address space ☹
- Solution: CIDR: Classless Inter-Domain Routing



Netmask

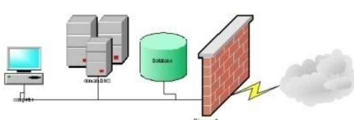
- Netmask starts with as many 1s as long is the network part of the address
- Netmask determines the size of the sub-networks



Netmask

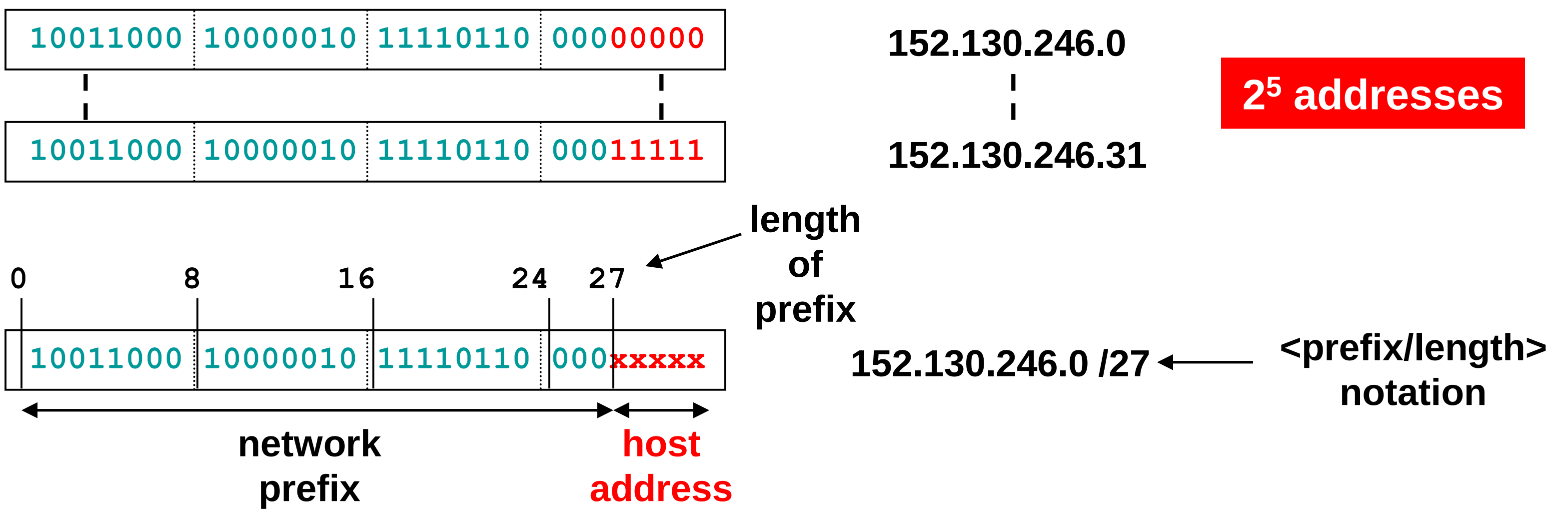
- Example:
  - BME network
    - IP address range: 152.66.x.x : 255.255.0.0
  - TMIT sub-network
    - IP address range : 152.66.244.x : 255.255.255.0
- 255.255.255.0 –> 24 bit netmask : C class

- If the network part can be anything, not only 8,16, 24 -> netmask can determine the length -> size of the network



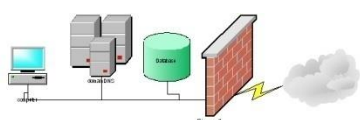
Variable Length Subnet Mask

Assign continuous IP address blocks to sub-networks



Special IP Addresses

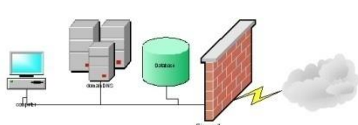
- Host ID all 0 host part: address of the (sub-)network
  - e.g. 152.66.244.0
    - Cannot be assigned to hosts
- Host ID all 1 host part: broadcast address
  - Last address of a sub-network:
    - e.g. 152.66.244.255
  - Standard allows to use 255.255.255.255, too
  - Broadcast message: to all hosts of a sub-network
- 127.0.0.0-127.255.255.255: loop-back network (delivered to the sending host itself)
  - 127.0.0.1: own address of the local host



Private IP Address Ranges

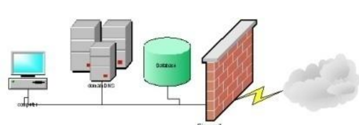
Size	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	description[
24-bit block	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

Private addresses are non-routable



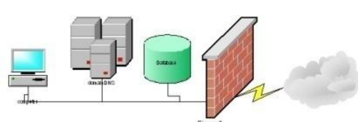
Exercise

- 152.130.246.128/28
  - how many IP addresses does it contain?
  - max. how many hosts does it contain?
  - what is the broadcast address?
- Netmask 28 bits -> 32-28=4 bits host part
  - 2^4=16 IP addresses
  - 16-2=14 host address (network + broadcast address!)
  - 10001111 -> 128+15=143 -> 152.130.246.143



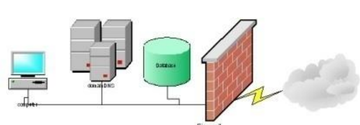
DHCP

- Dynamic Host Configuration Protocol
- Makes it possible for a machine to get an IP address from the network
- DHCP may provide other network parameters, too:
  - Gateway, DNS server
- Disadvantage: a machine can get different addresses at different times



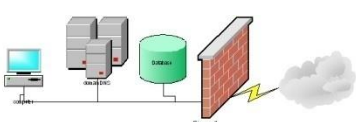
MAC address

- Media Access Control (Extended Unique Identifier)
  - EUI-48 or MAC-48: 48 bit long,
  - EUI- 64: 64 bit long address
  - 12 hexa digit notation: **00-09-6B**-26-ED-37
  - Manufacturers stores them on the cards (**first part assigned by IEEE to the manufacturers** - OUI)
    - OUI: Organizational Unique Identifier
  - 2^{48} combinations (281 thousand billion)
    - Ethernet
    - Bluetooth
    - ATM
  - EUI-64: IPv6

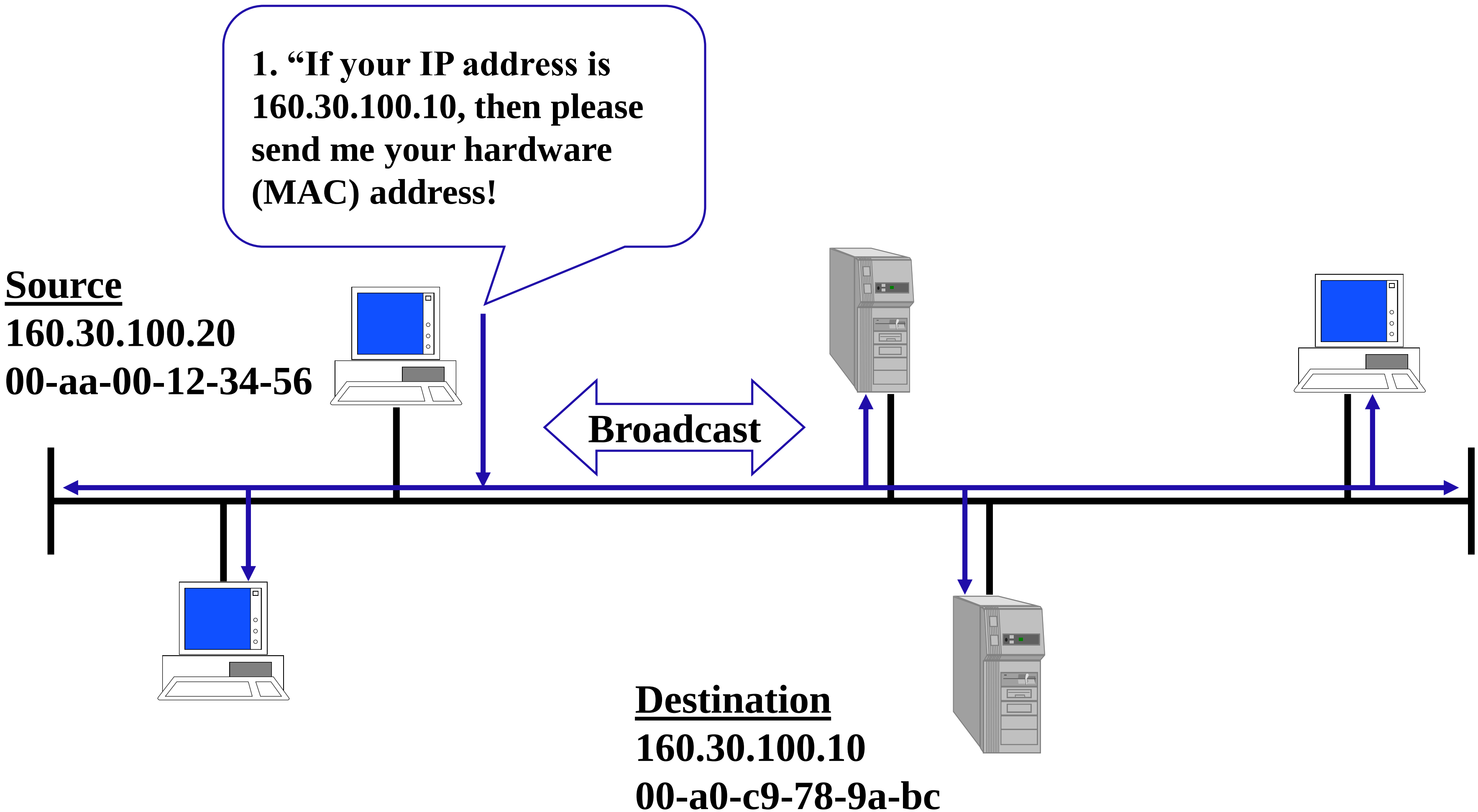


ARP – Address Resolution Protocol

- Source must know the hardware address (MAC address) of the destination before IP packets can be sent to it
- ARP is a method that assigns a hardware address to an IP address
- ARP determines the hardware address of the requested IP address by a broadcast message sent on the sub-network
- ARP stores the hardware-IP address assignments in a cache; this is how it can use them later on
- It can be displayed by a Windows **`arp -a`** command



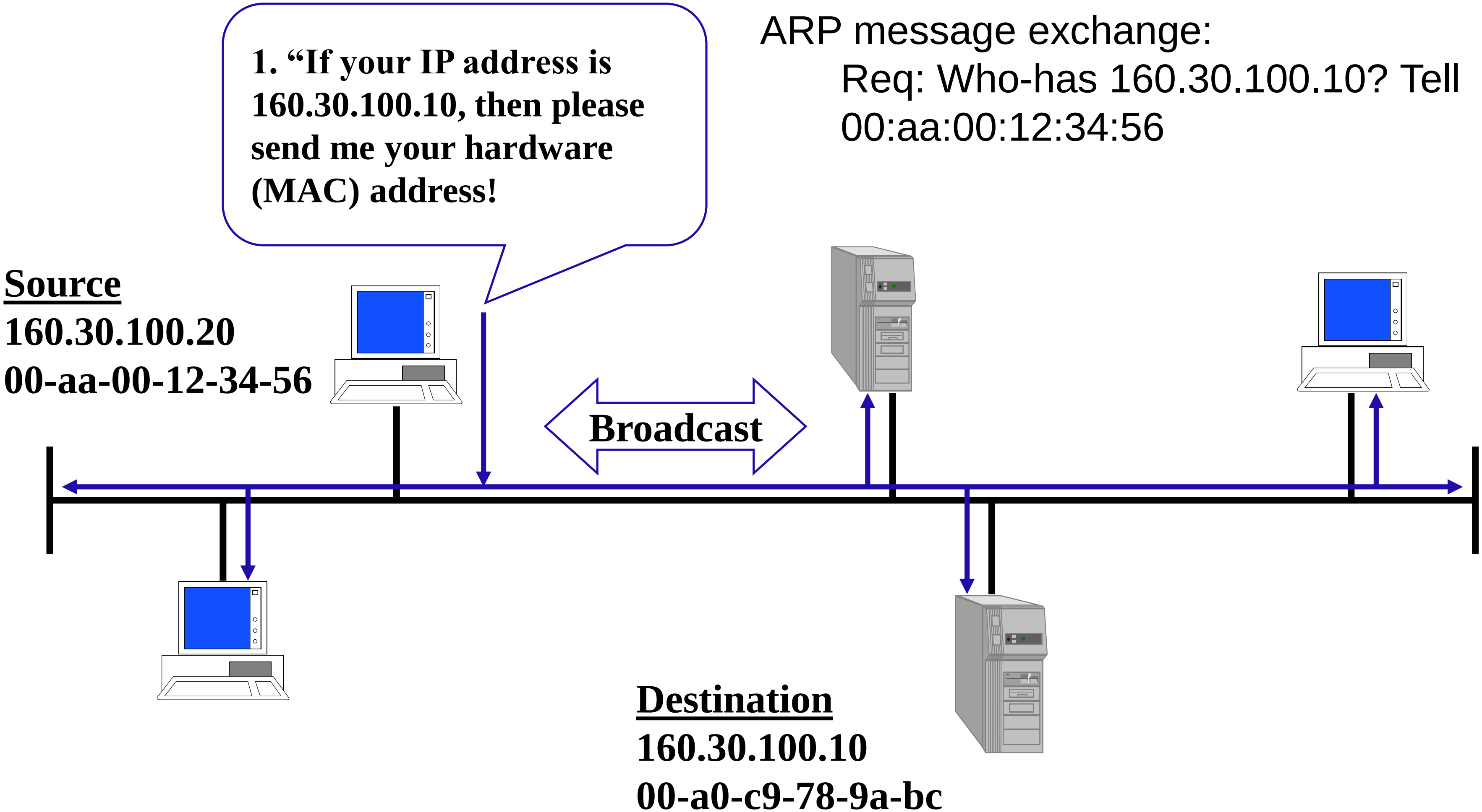
Address Resolution Protocol



Address Resolution Protocol

ARP message exchange:

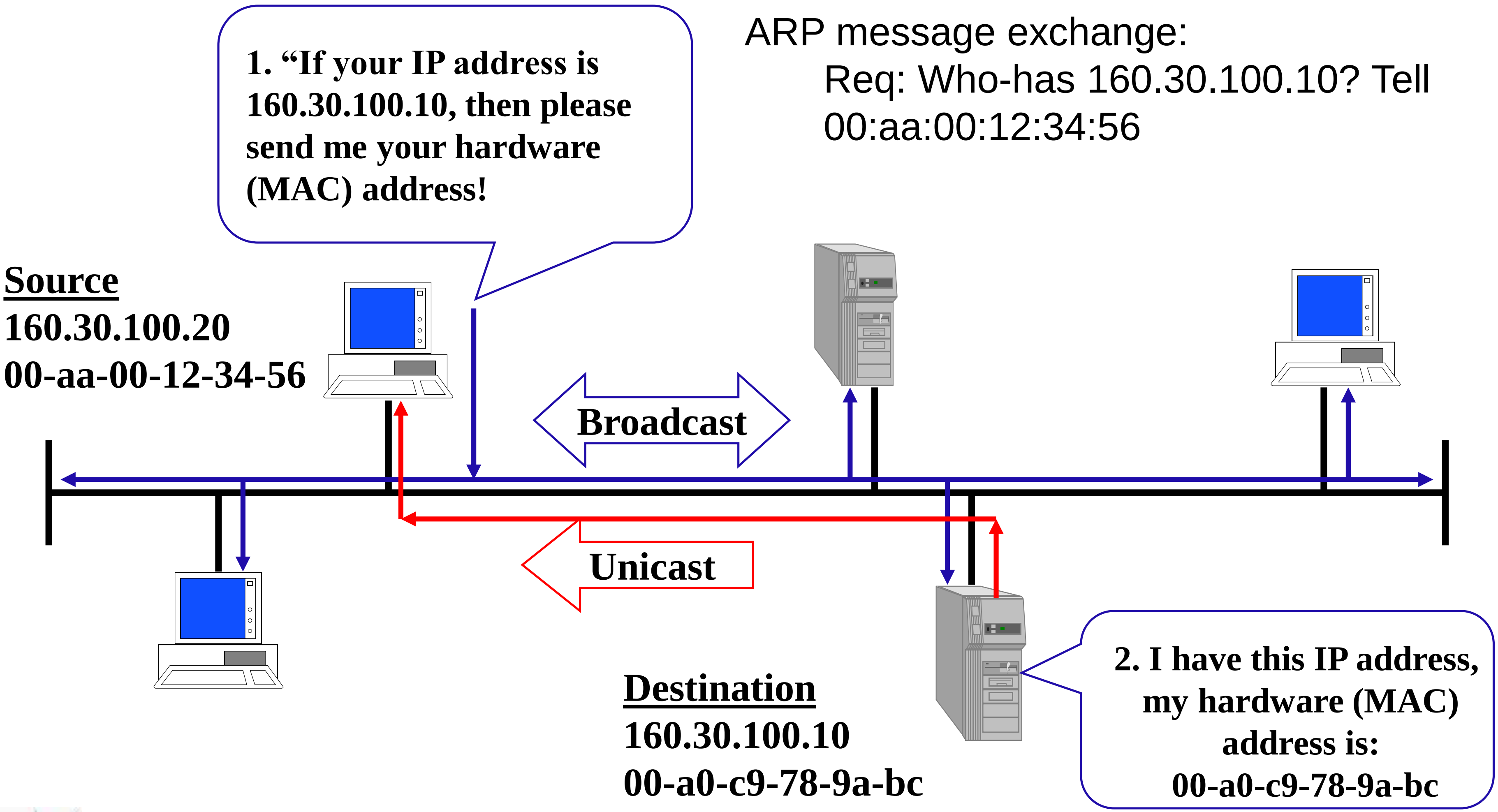
Req: Who-has 160.30.100.10? Tell 00:aa:00:12:34:56



Address Resolution Protocol

ARP message exchange:

Req: Who-has 160.30.100.10? Tell 00:aa:00:12:34:56

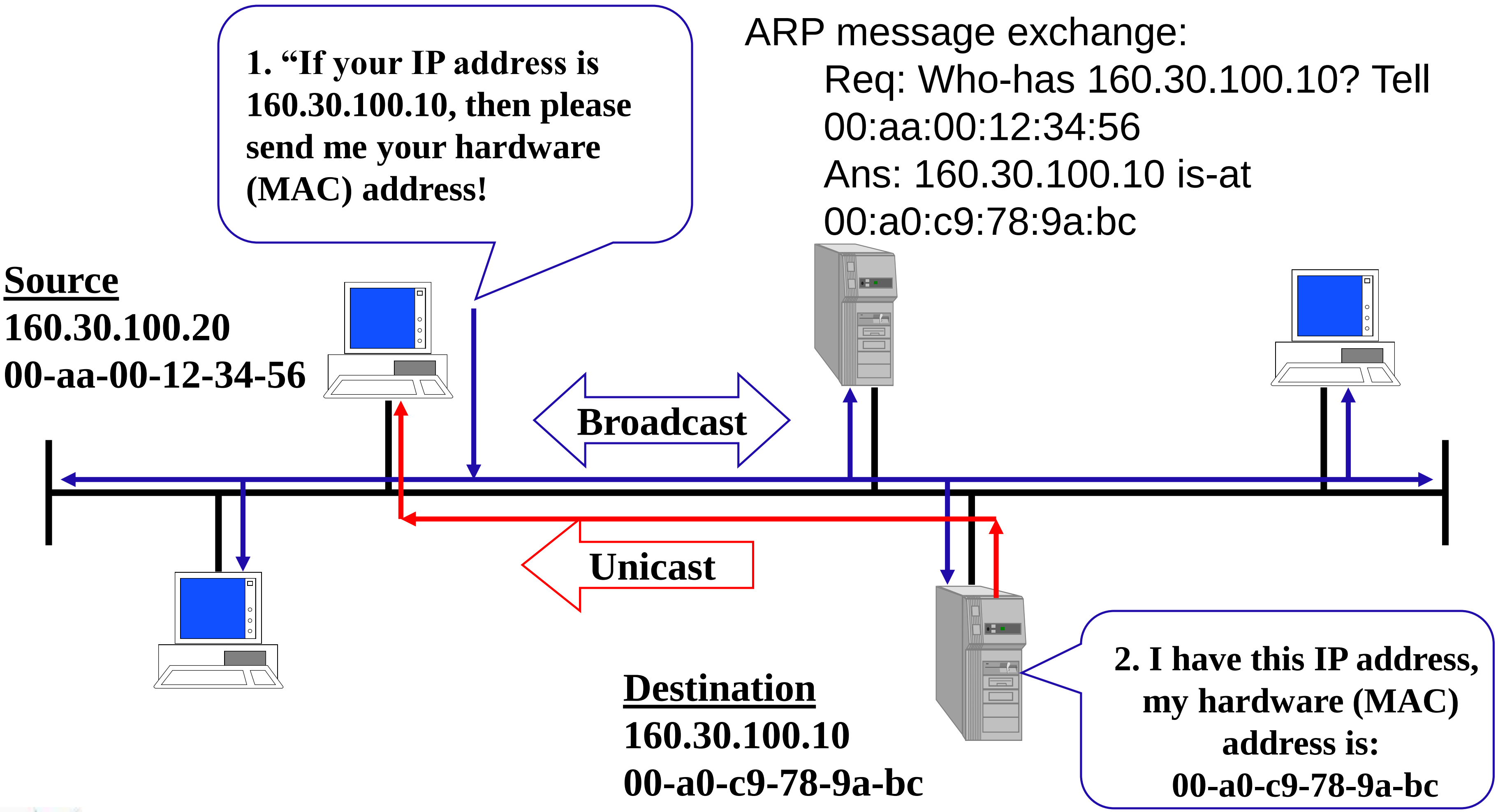


Address Resolution Protocol

ARP message exchange:

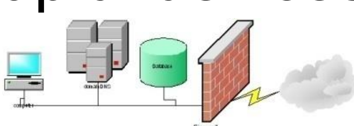
Req: Who-has 160.30.100.10? Tell 00:aa:00:12:34:56

Ans: 160.30.100.10 is-at 00:a0:c9:78:9a:bc



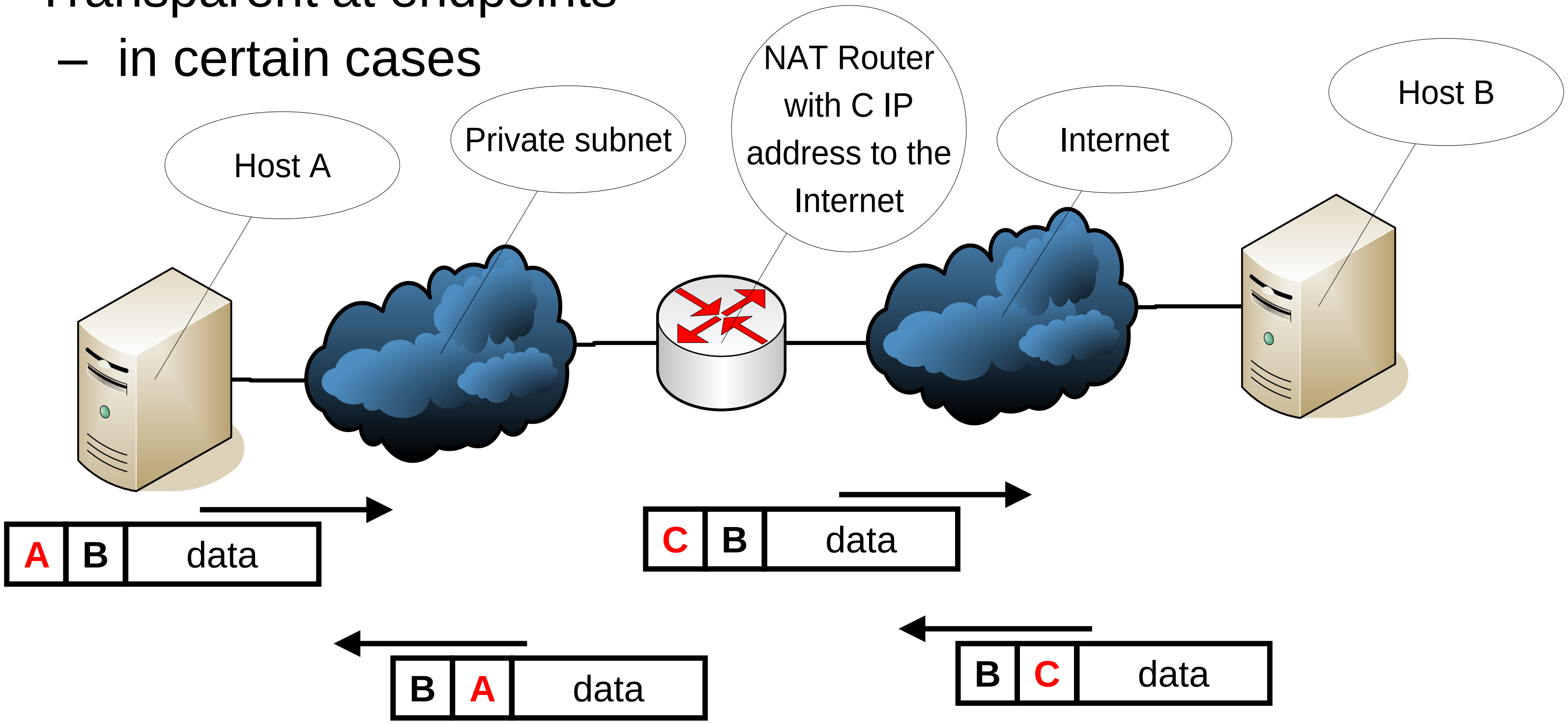
RARP - Reverse Address Resolution Protocol

- RARP assigns IP address to a hardware (MAC) address
- RARP makes it possible to a newly started machine to propagate its Ethernet address by a broadcast request
  - „My 48-bit Ethernet address is 00-a0-c9-78-9a-bc. Does anyone know my IP address?”
- RARP server detects the request and sends the requested IP address back
  - DHCP
  - For ‘stupid’ devices, e.g. printer

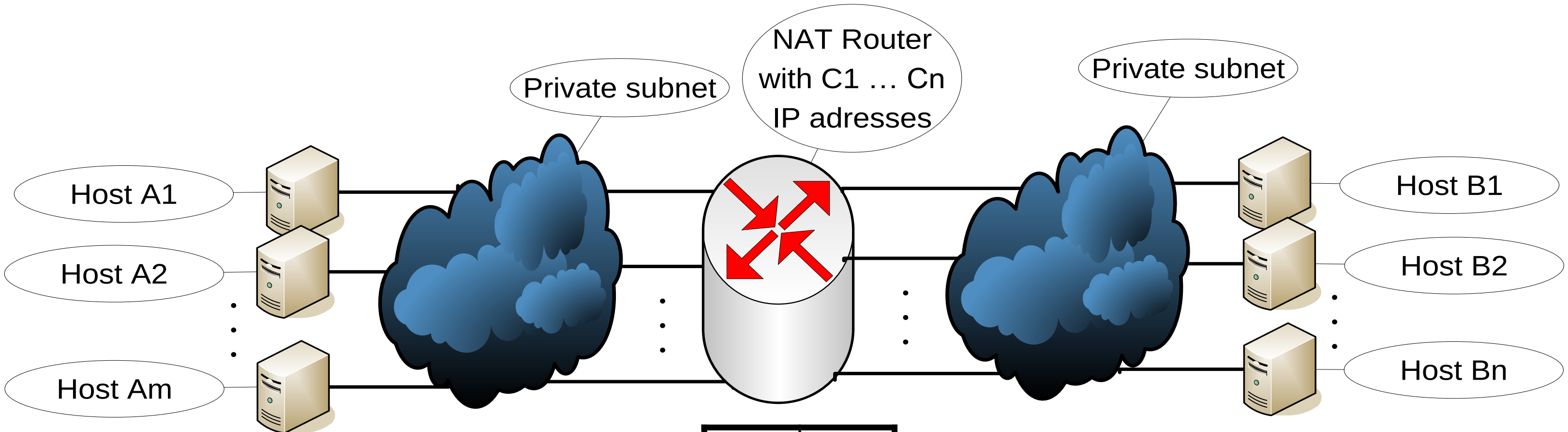


NAT - Network Address Translator

- The IP Network Address Translator (RFC1631) (1994)
- Connecting Private Networks to Internet
- L3 (IP layer) level conversion
- Transparent at endpoints
  - in certain cases

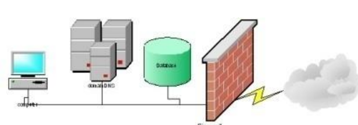


NAT – with more hosts (m=n)



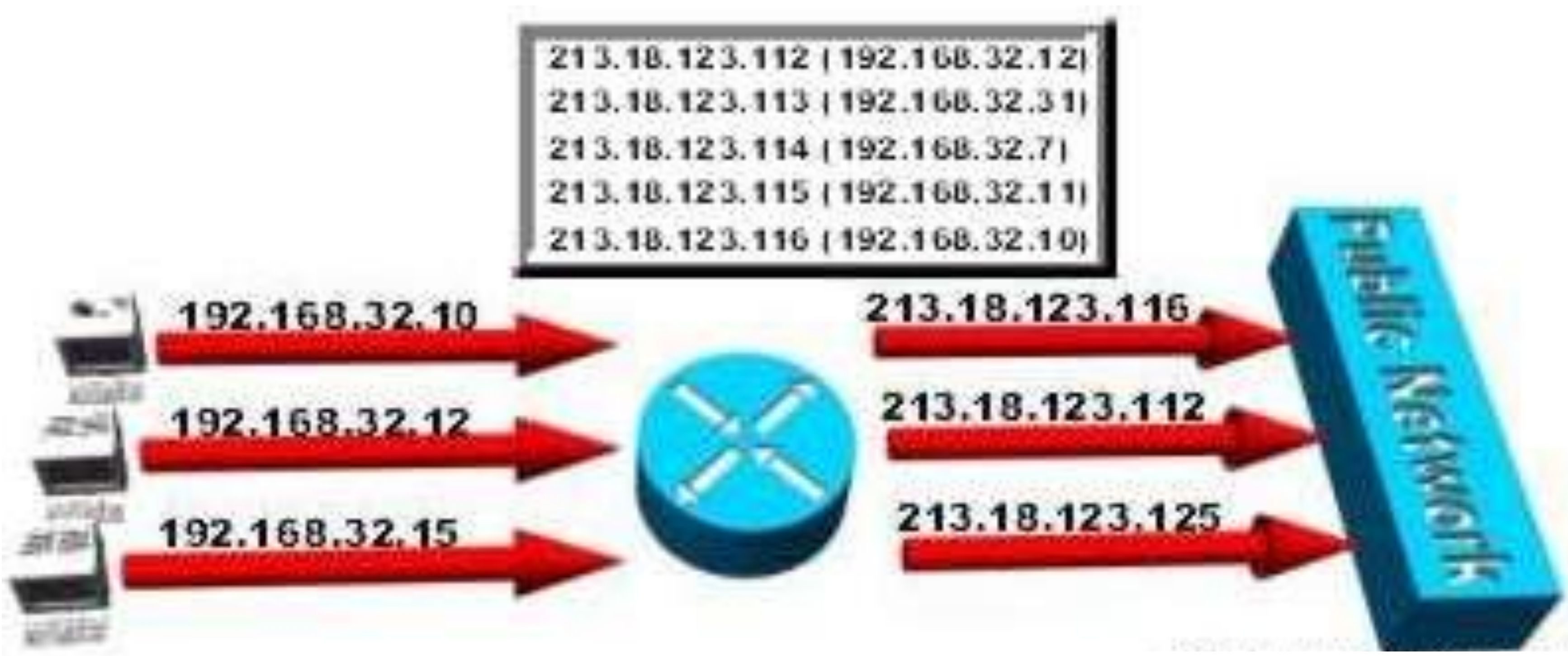
A1	**C1**
A2	**C2**
…	**…**
Am	**Cn**

- # of private addresses = # of public addresses available for the router
- Assignment can be
  - static
  - dynamic
    - to increase protection

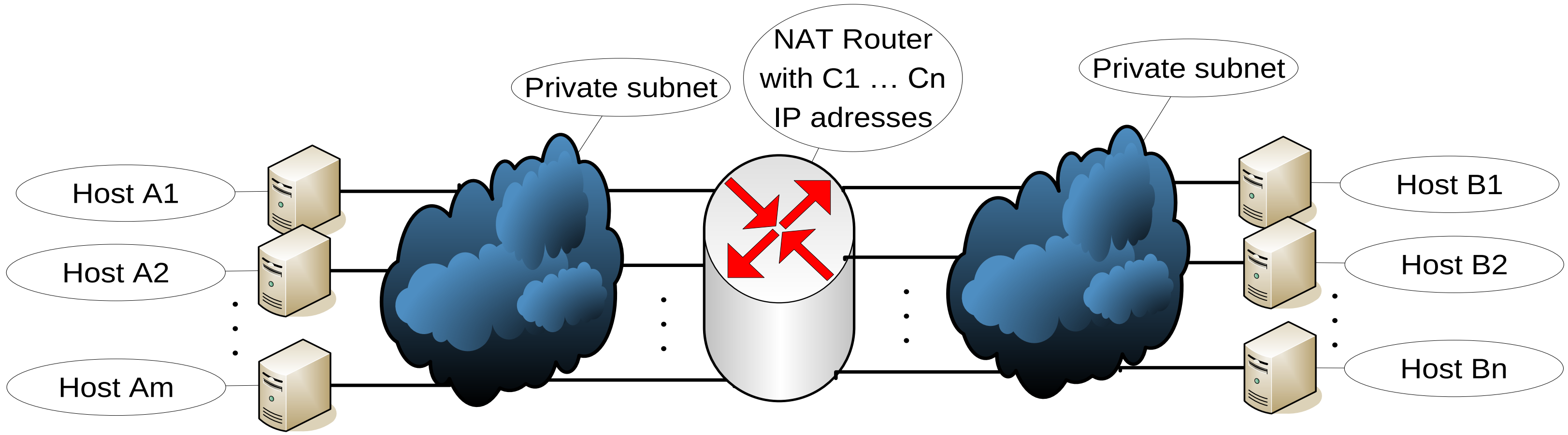


Static NAT example

Dynamic NAT example



NAT – with more hosts (m>n)

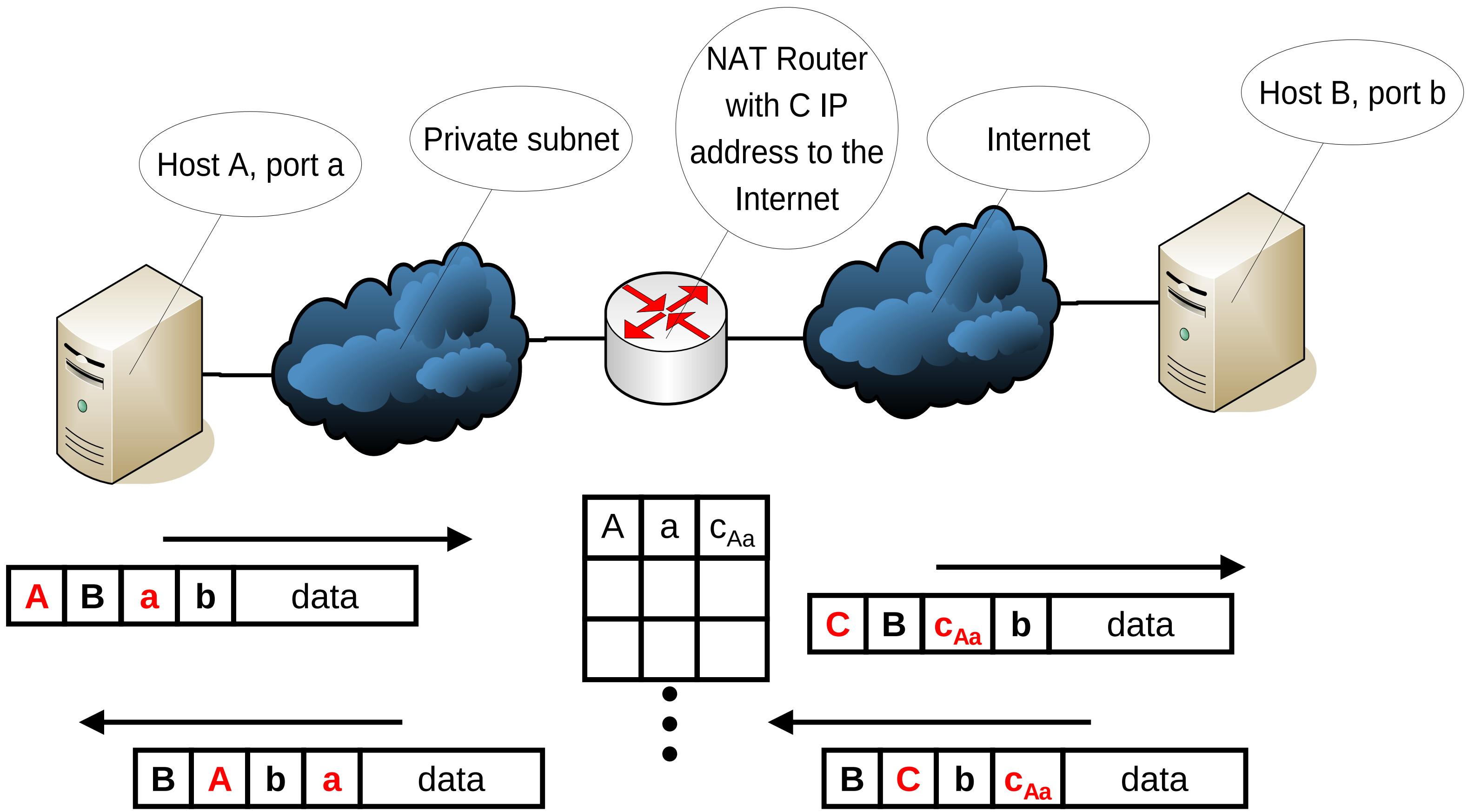


A1	**C1**
A2	**C2**
…	**…**
Am	**Cn**

- Needs an assignment strategy
  - if not enough (m>n)???
    - Typically n =1
  - static: more than one private addresses for one public
    - reverse traffic can not be routed to proper server
  - dynamic: use the next idle public address
    - not enough addresses if every server has a connection at the same time

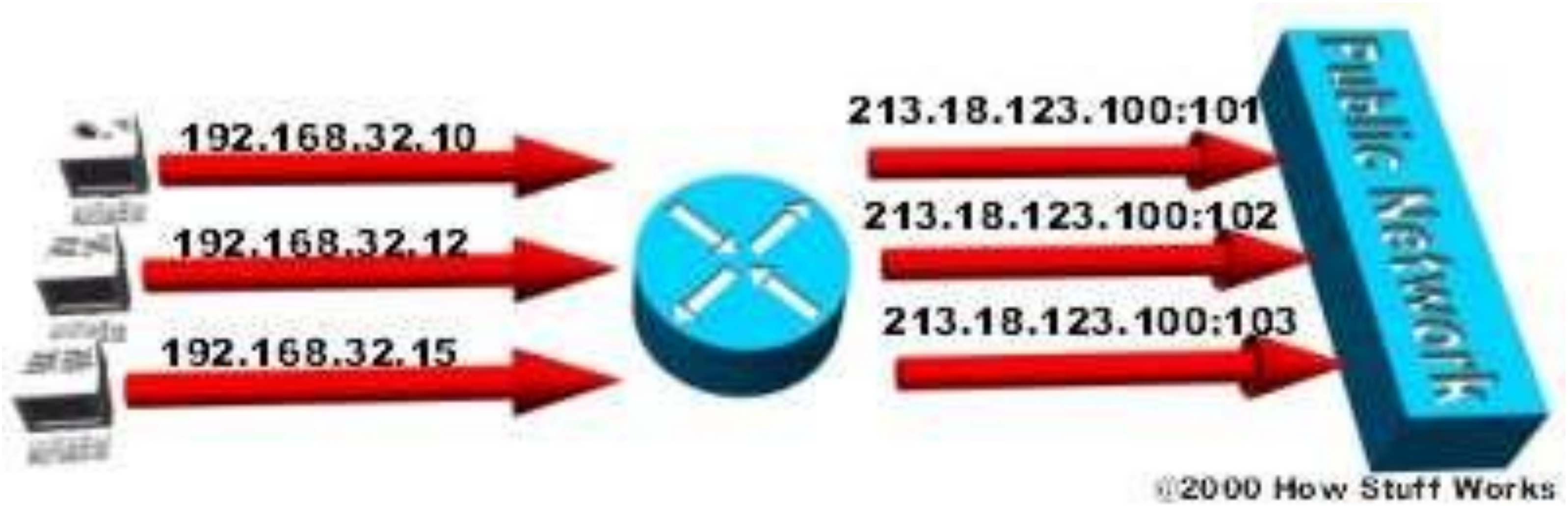
NAT + port translation

- Network Address Port Translation (NAPT)

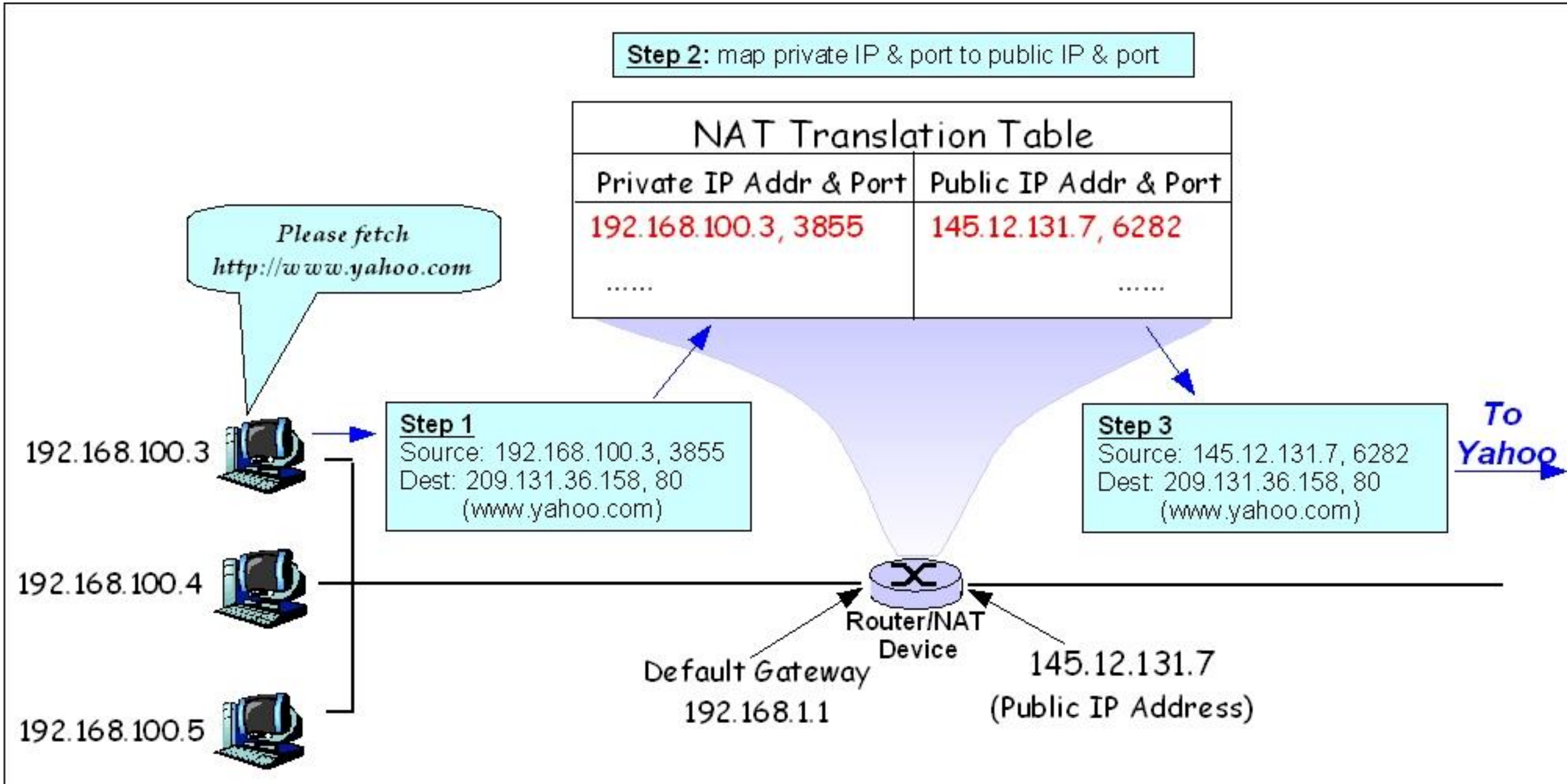


NAPT example

- Table:
  - DRAM (Dynamic RAM)
  - 4MB ~26000 connections

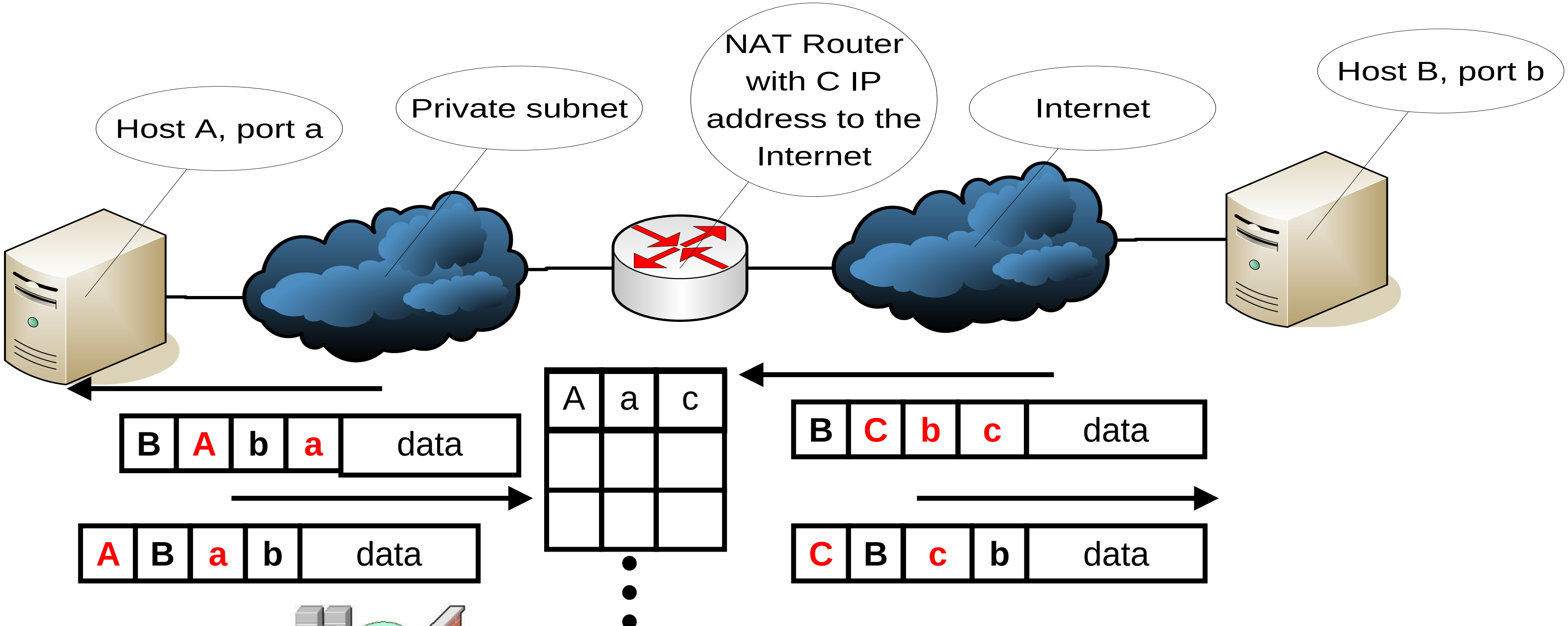


NAPT example



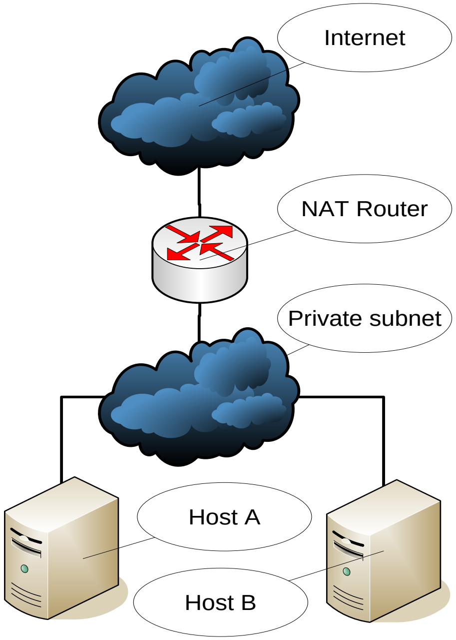
NAPT – virtual server

- Export the internal server with static NAPT assignment
  - looks like if the NAPT server provided the service
    - to every port
    - to selected port(s)
      - restriction for not allowed traffic



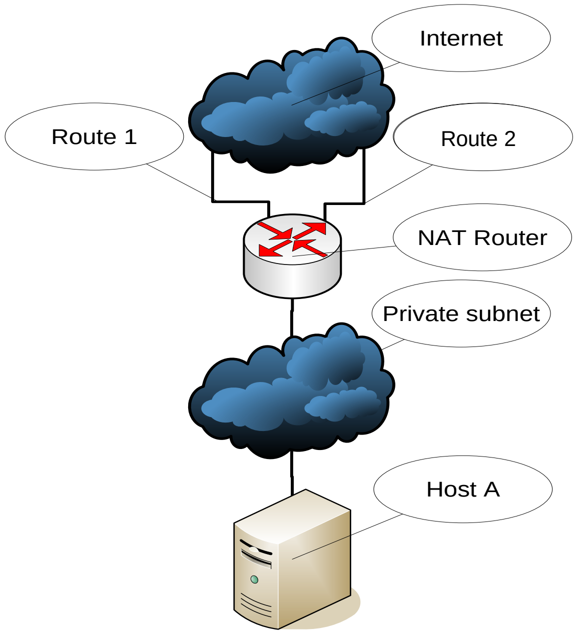
NA(P)T – optimisation

- More internal server
  - Load sharing/balancing
  - Internal structure hidden - modifiable



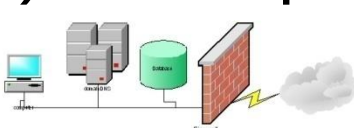
NA(P)T – optimisation

- More interfaces
  - Reliability
  - Multi-homing
    - Typically with different ISPs



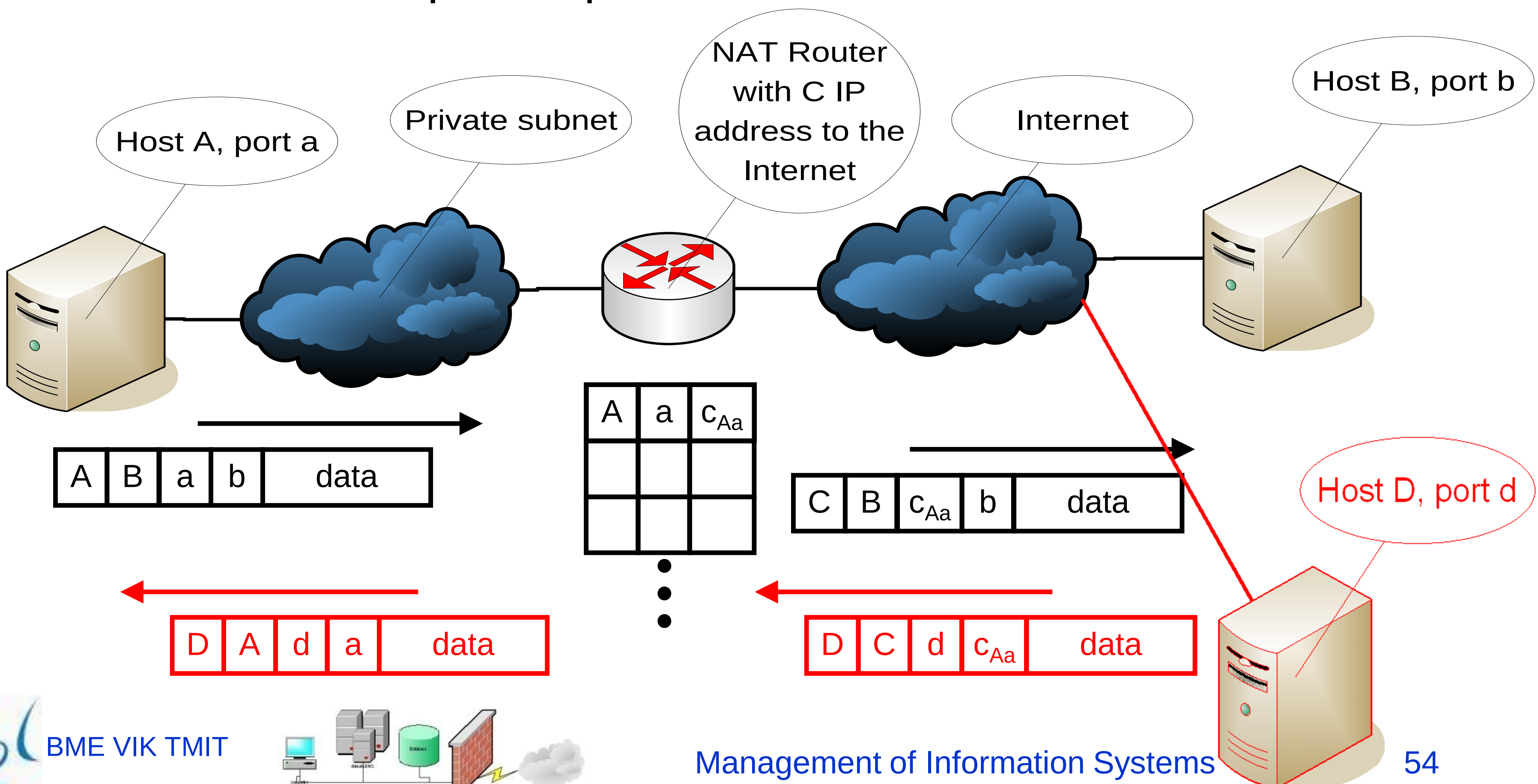
NA(P)T – firewall

- Allows only internally initiated connections
  - Disables “outer” connections – only replies to internal connections allowed
- BUT: inbound mapping
  - “Let you in” only from specific devices/IP addresses
  - E.g. working from home
  - Must be configured in advance
- NAPT ≠ proxy server
  - NA(P)T transparent for servers



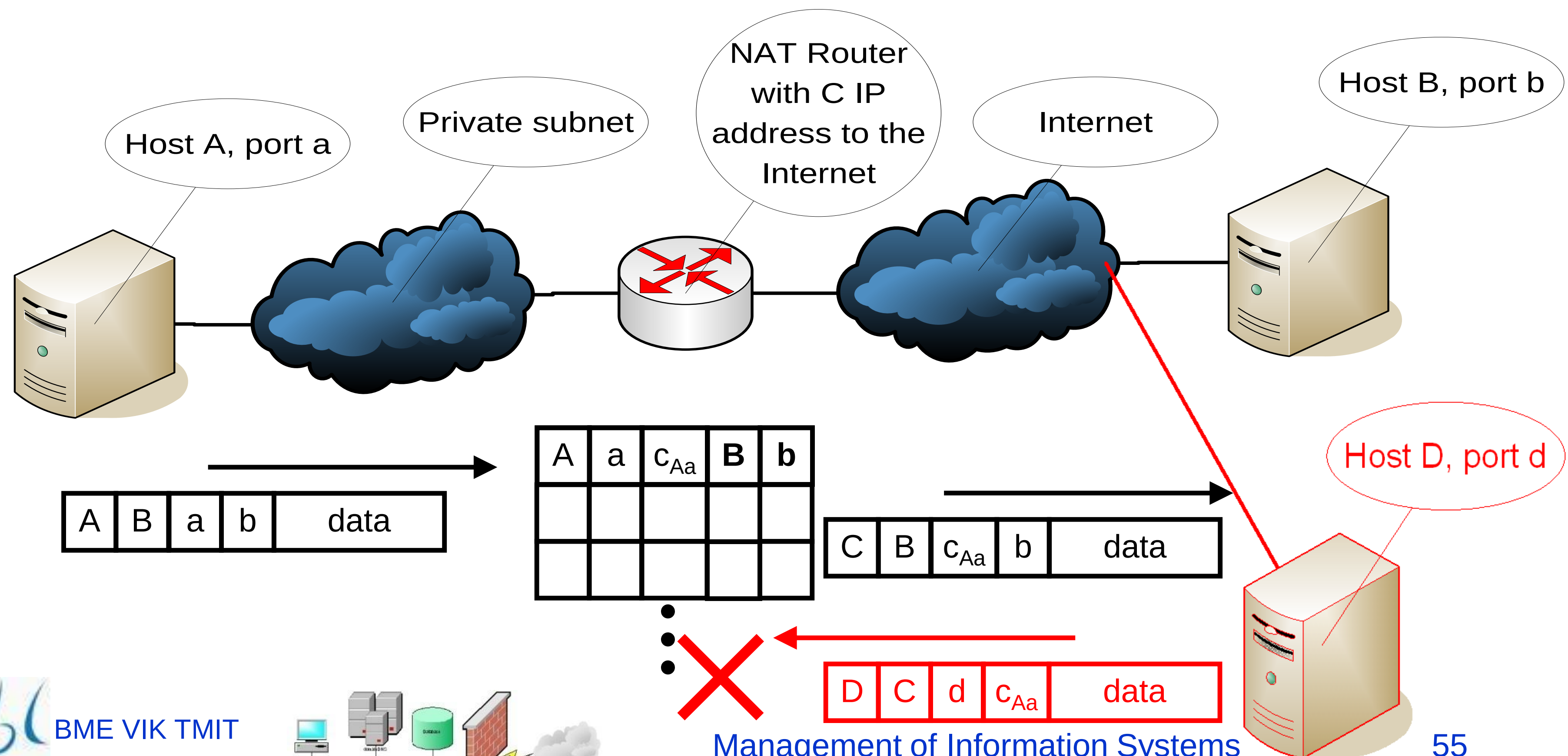
NAPT – security

- Dynamical entries
  - but they may be scanned (and so reached) during lifetime
  - not a NAPT-specific problem



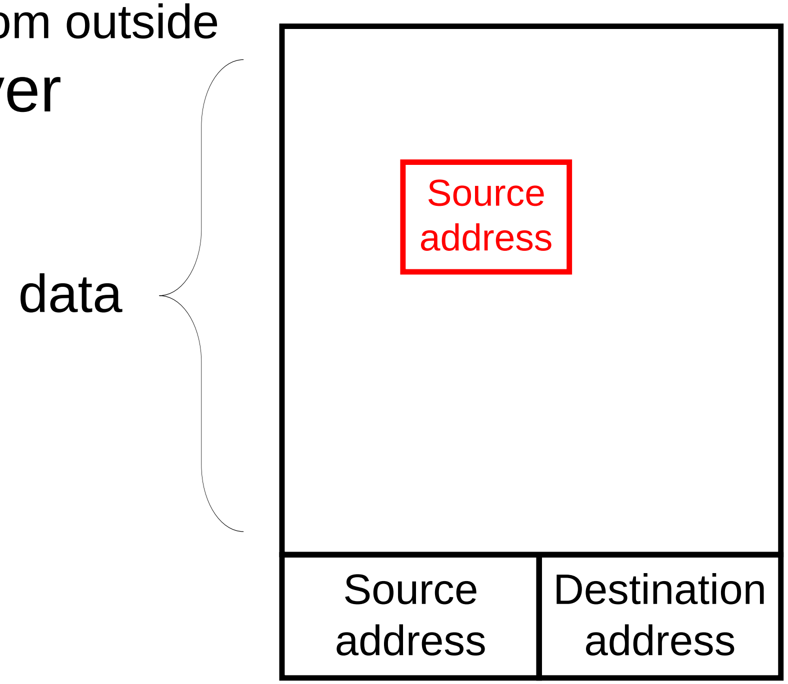
NAPT – security extension

- Extended with the remote IP address
- Simple firewall



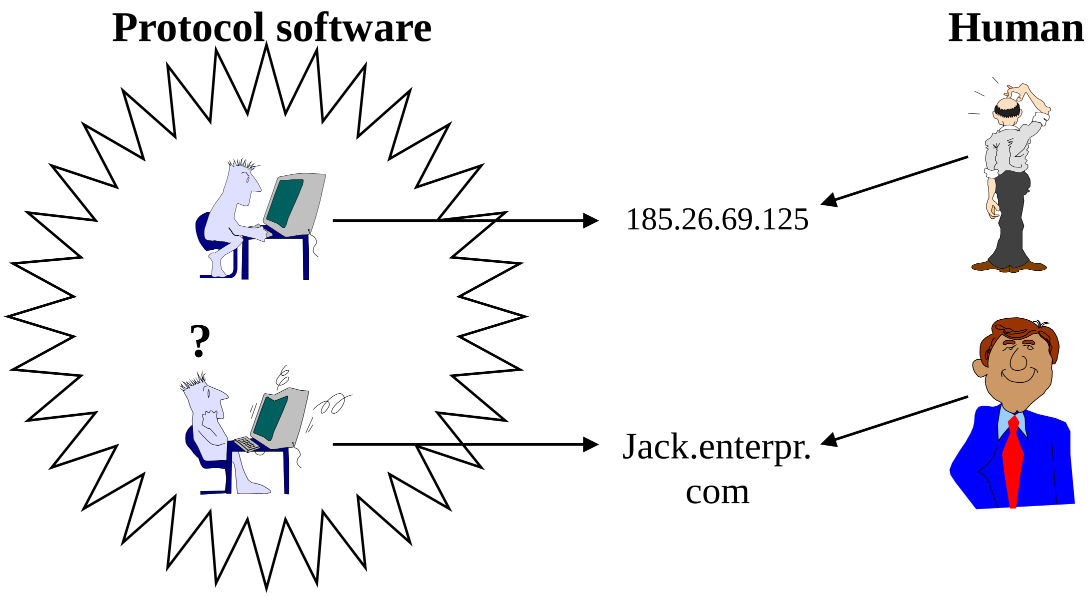
NAT problems

- Impossible to open a secondary connection
  - Not possible to initiate a transaction from outside
- IP address in the application layer
  - Routing protocols
  - DNS
  - FTP
  - H.323
  - SIP
  - HTTP (absolute URL)
  - etc…



- Solution
  - IP addresses must be replaced also in the application layer (e.g. in data part of an IP packet)
    - violates the OSI layering concept
    - application proxy at a NAT router

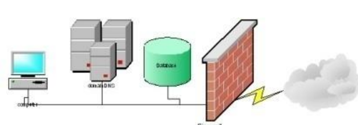
Domain Name System (DNS)



- For a human it is hard to remember an IP address
  - But convenient for software using IP protocol
- For a human symbolic names are more natural
  - But software using IP protocol struggles with them

DNS continued

- Name of a computer – IP address database
- Hierarchical structure
- Distributed database, distributed control
- Structured names
- Widely supported by different operating systems
- Two main domain types:
  - General (7, all of 3 letters)
  - Countries (of 2 letters)
- Disadvantage: static, manual administration

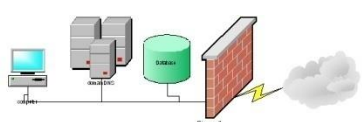


DNS Namespace

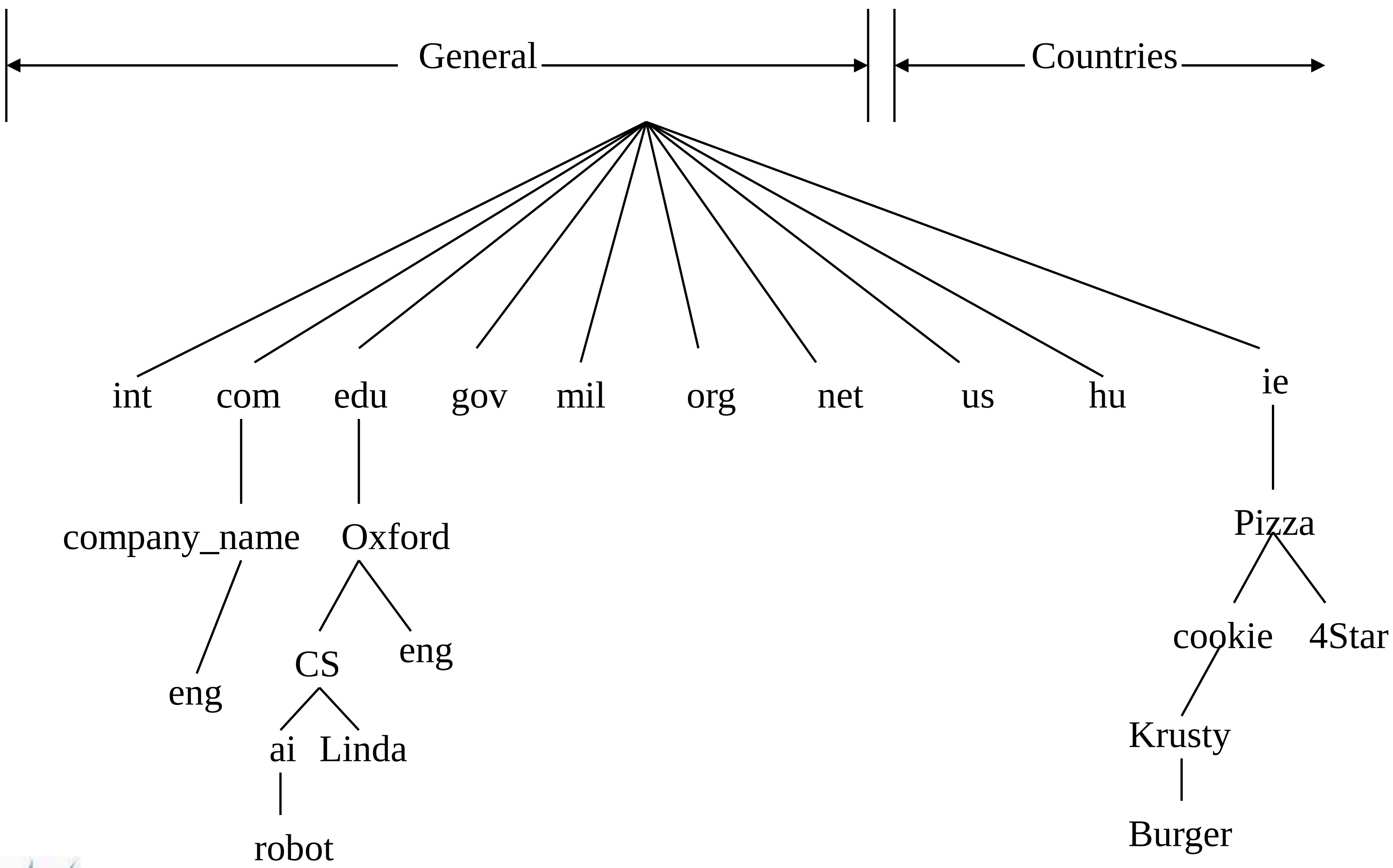
- General domains:
  - (Most of them may only be registered only within U.S., but e.g. `.com` can be registered anywhere)

Domain	*Description*
.com	Commercial organisations
.edu	Educational institutions
.gov	Government organisations
.mil	Military group
.net	Major network support centre
.org	Organisations other than those above
.int	International organisations

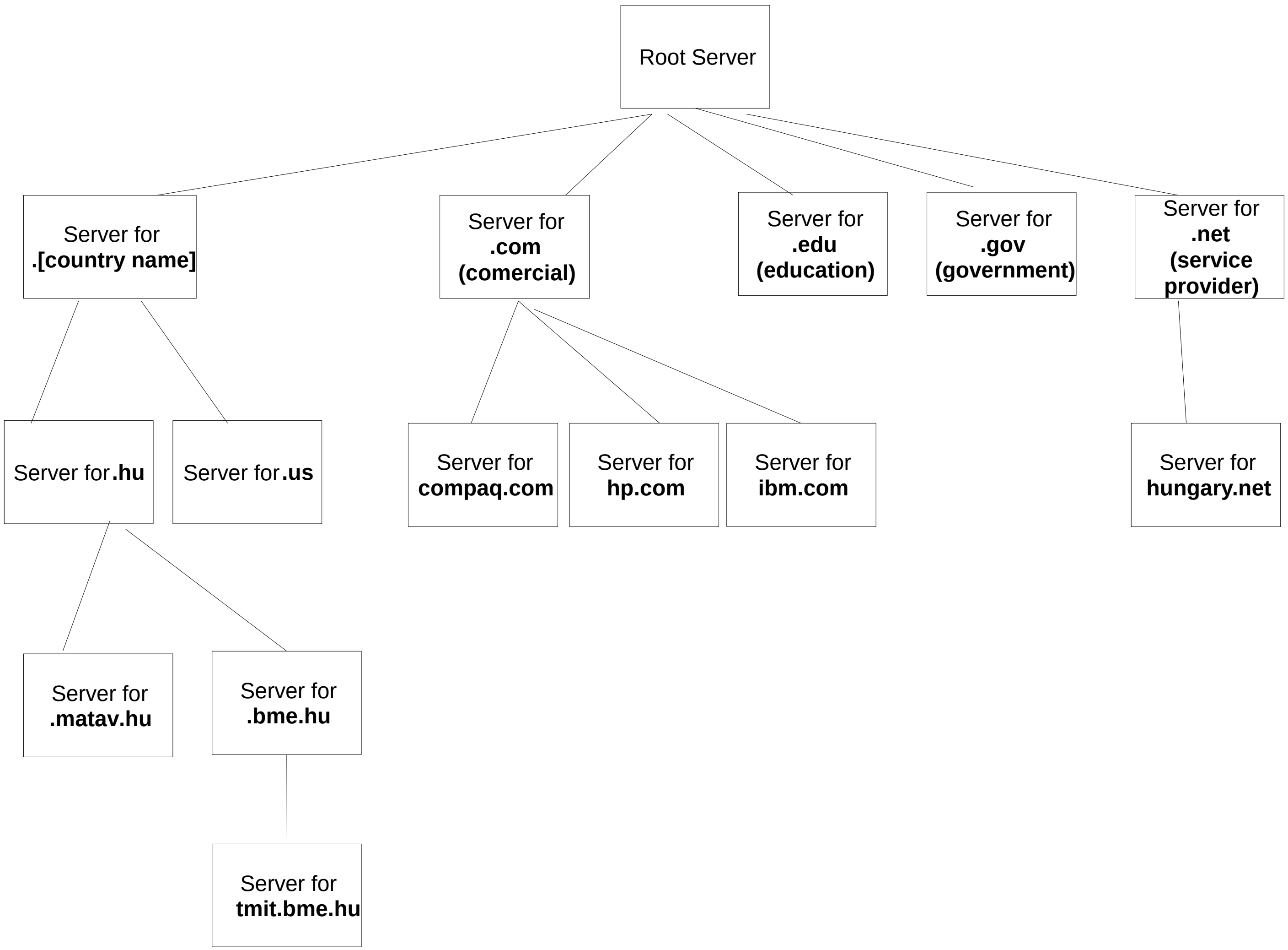
- Countries:
  - e.g.: .hu .us .fr .de



Internet Domain Namespace

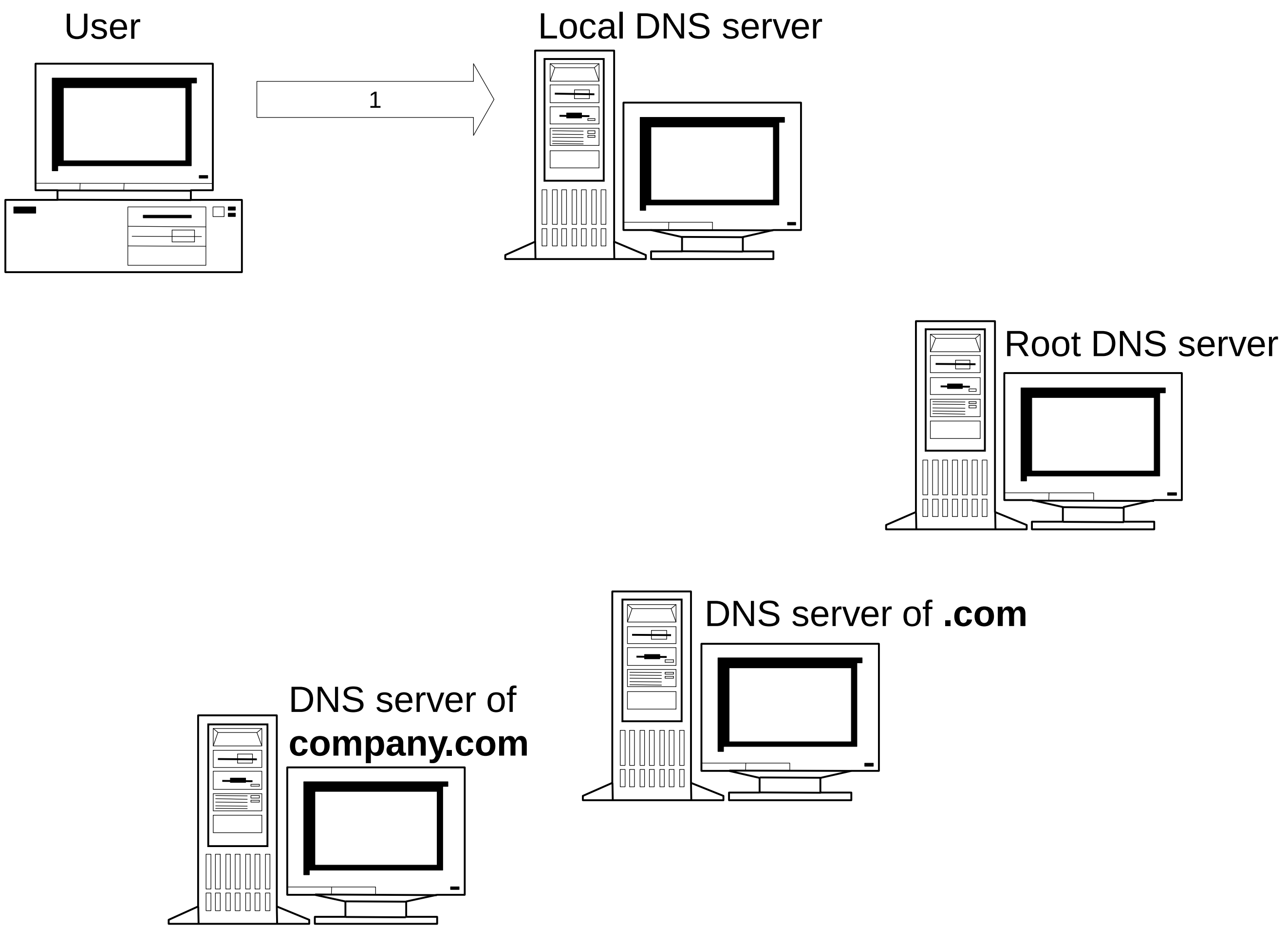


Domain Name Resolution



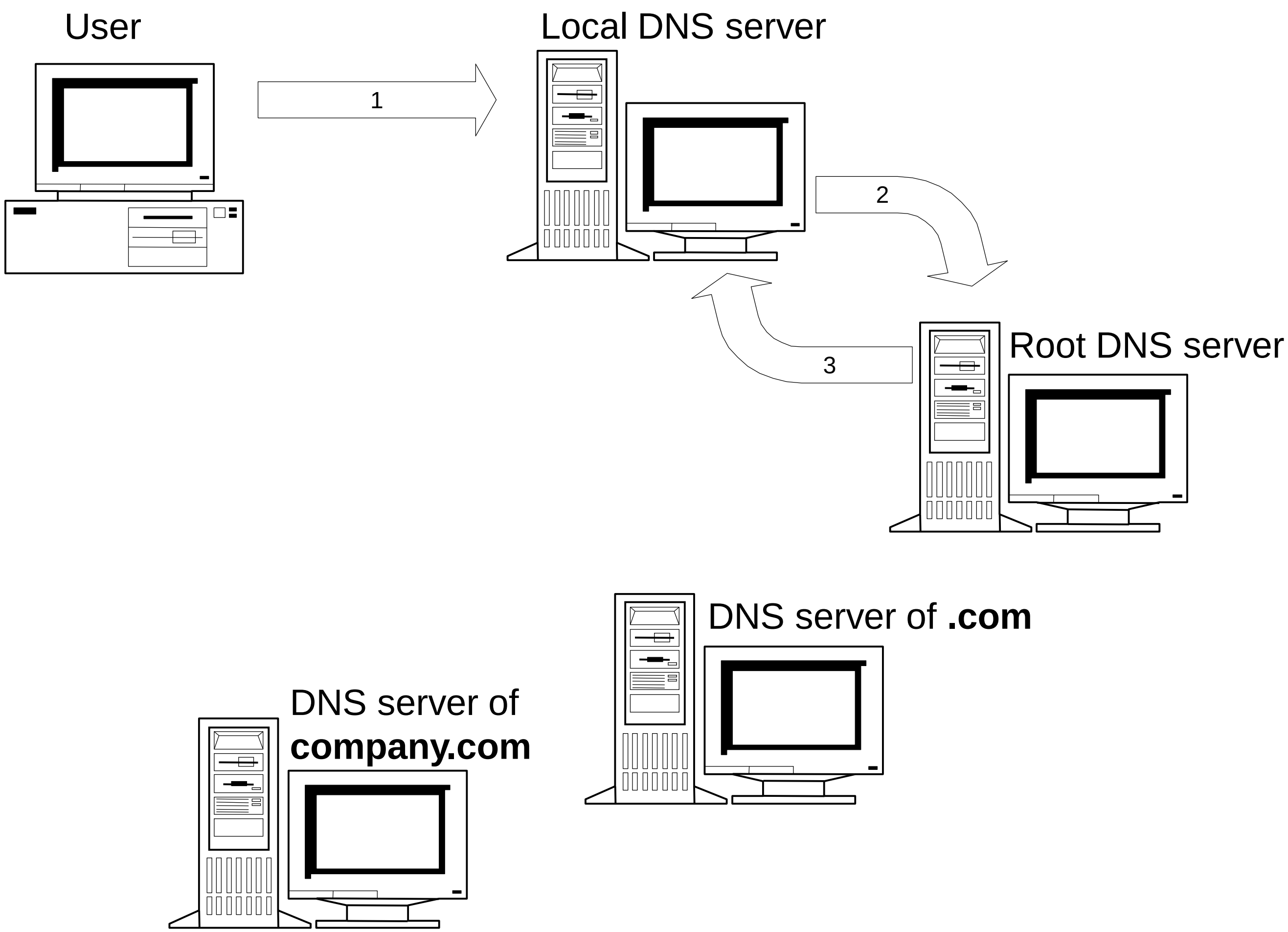
DNS Address Resolution

(Steps of resolution of `anybody.company.com` **domain name**



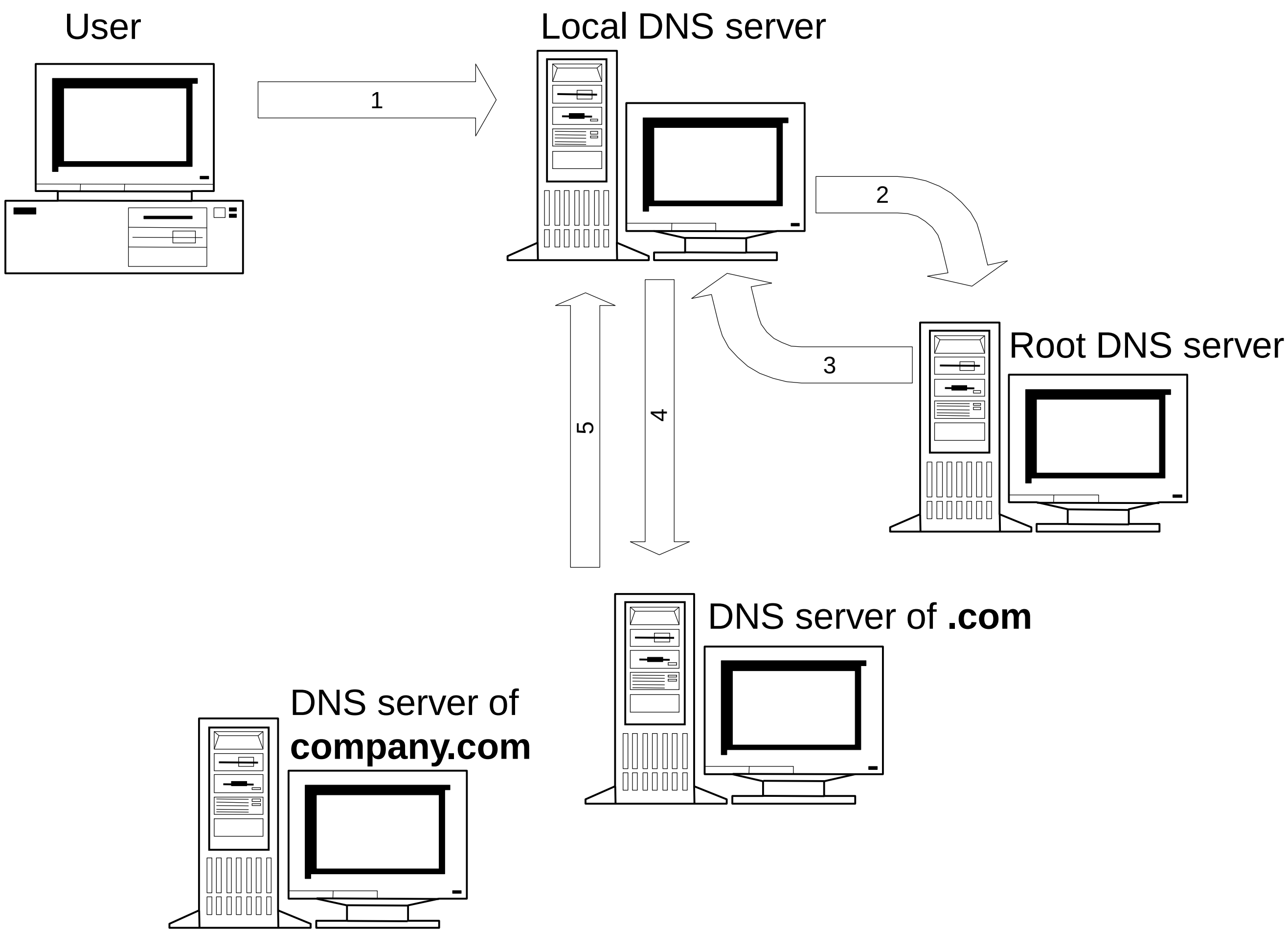
DNS Address Resolution

(Steps of resolution of `anybody.company.com` **domain name**



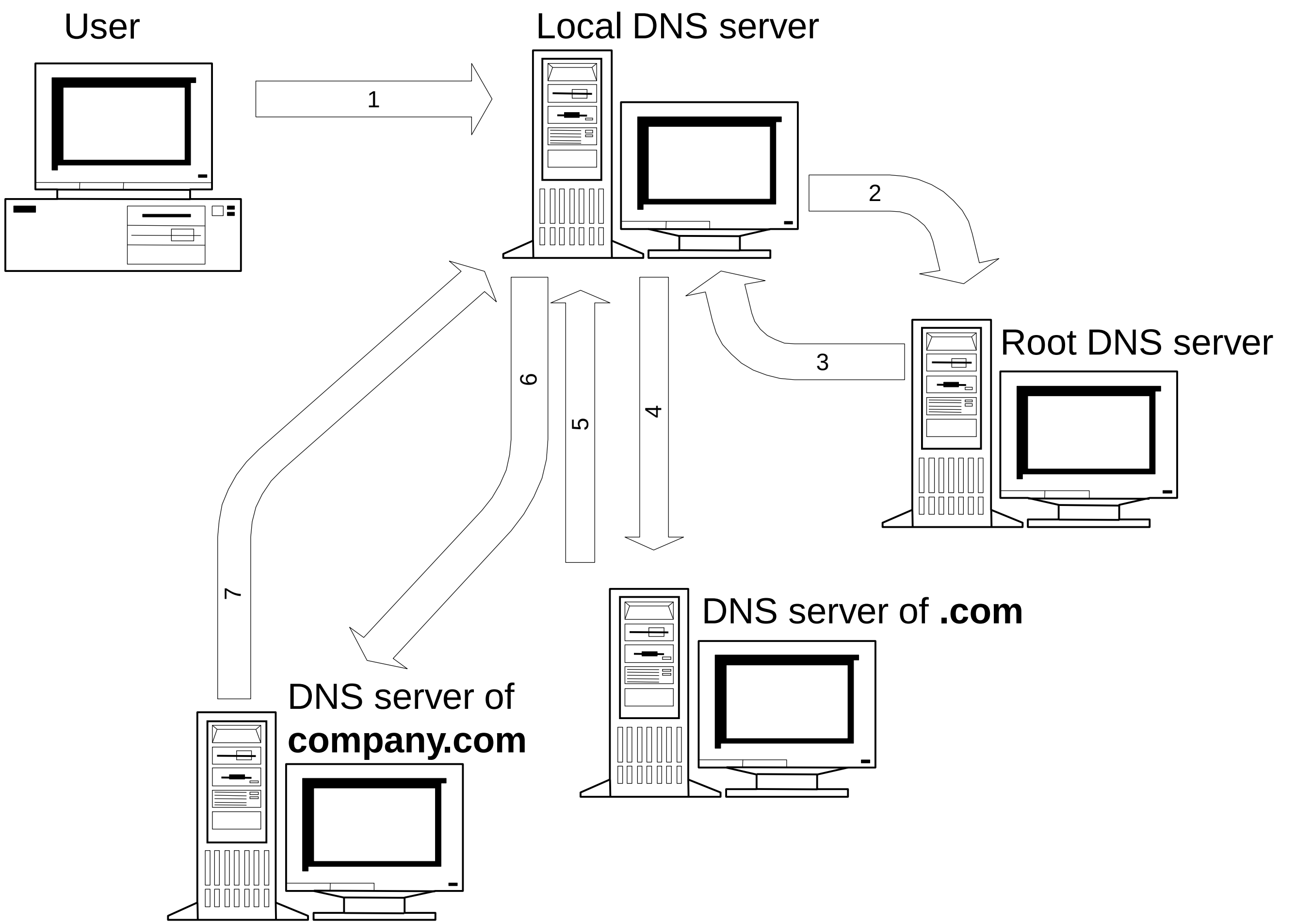
DNS Address Resolution

(Steps of resolution of `anybody.company.com` **domain name**



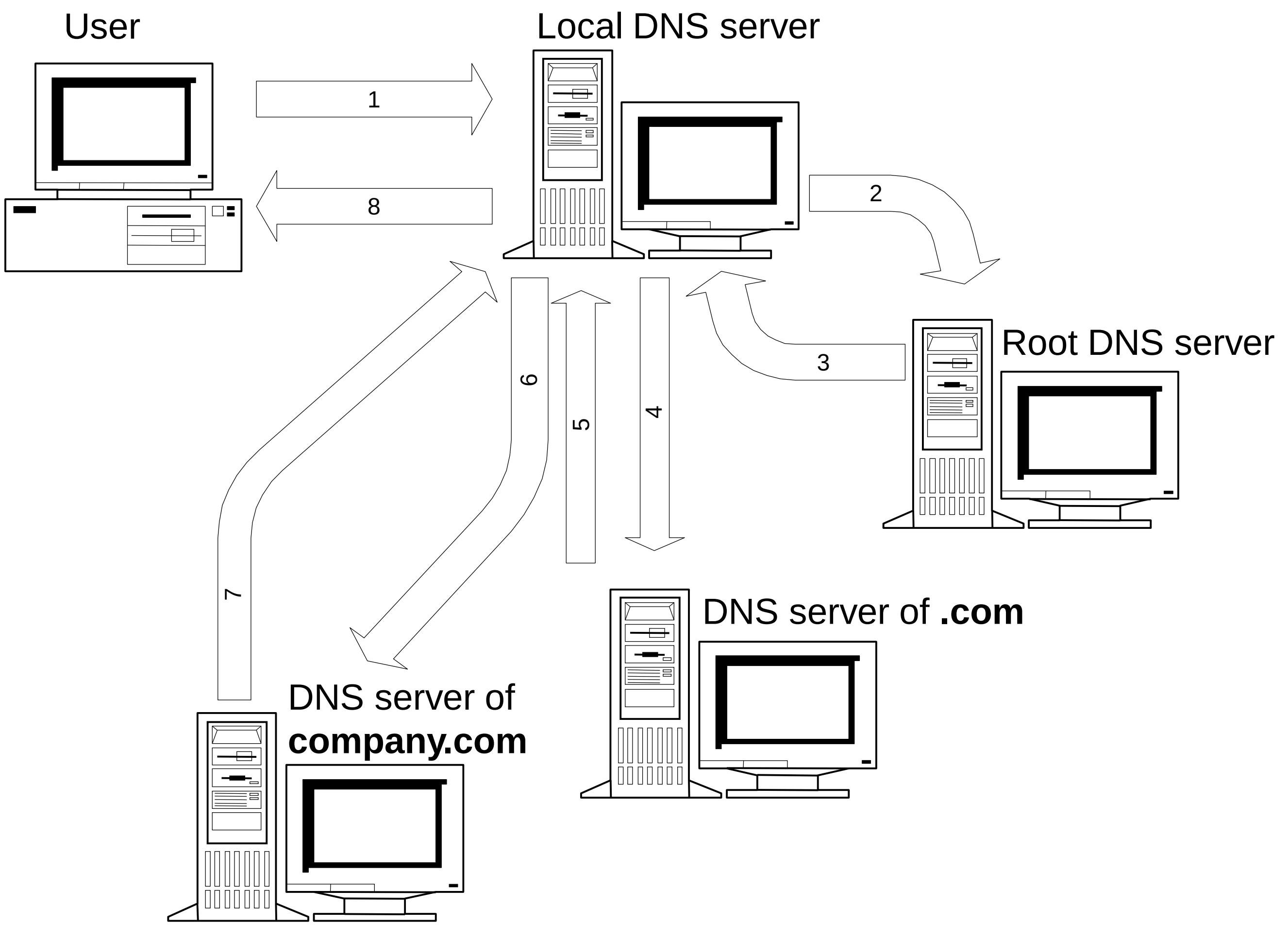
DNS Address Resolution

(Steps of resolution of anybody.company.com **domain name**



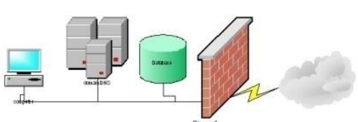
DNS Address Resolution

(Steps of resolution of `anybody.company.com` domain name



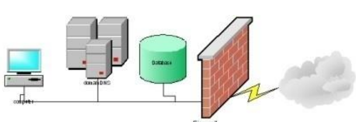
DNS Caching

- DNS servers store the lately resolved names to reduce Internet traffic and increase the efficiency
- The local server returns by the information stored in the cache, but marks it as „non-authoritative” (~not for sure valid), and gives the address of the server that stores the exact binding
- If the efficiency (speed) is important, the client accepts the non-authoritative information
- If the accuracy is important, the client turns to the „authority” server and verify that the binding between name and address is still valid
- Whenever an authority responds to a request, it includes a Time To Live (TTL) value in the response that specifies how long it guarantees the binding to remain

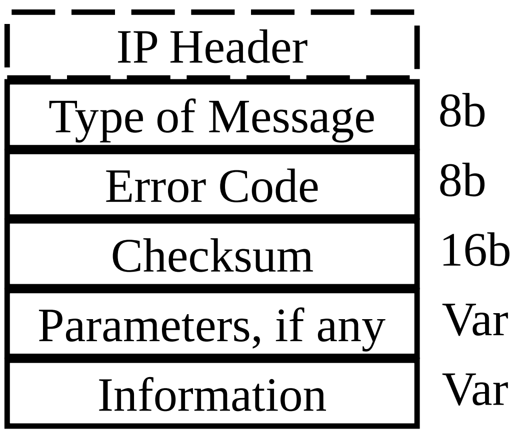


Internet Control Message Protocol, ICMP

- Transmission of error reports and IP layer control messages
- ICMP messages are carried as IP packets and are therefore unreliable
- Most widely used „debugging” tool
  - Ping, traceroute



Message types and format

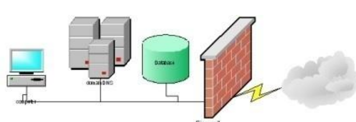


TYPE FIELD	ICMP Message Types
0	**Echo Reply**
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	**Echo Request**
11	**Time exceeded for a packet**
12	Parameter problem on a packet
13	Timestamp request
14	Timestamp reply
15	Information request (obsolete)
16	Information reply (obsolete)
17	Address mask request
18	Address mask reply

Ping

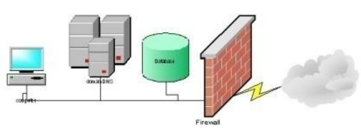
- Ping: for testing the aliveness of a device
  - accessibility of a terminal
  - round trip time (RTT)
  - length of route (in terms of hop-s)
  - optionally record route

```
Ping alpha [152.66.246.10] with 32 bytes of data:

Reply from 152.66.246.10: bytes=32 time=114ms TTL=250
Reply from 152.66.246.10: bytes=32 time=26ms TTL=250
Reply from 152.66.246.10: bytes=32 time=23ms TTL=250
Reply from 152.66.246.10: bytes=32 time=27ms TTL=250

Ping statistics for 152.66.246.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 114ms, Average = 47ms
```

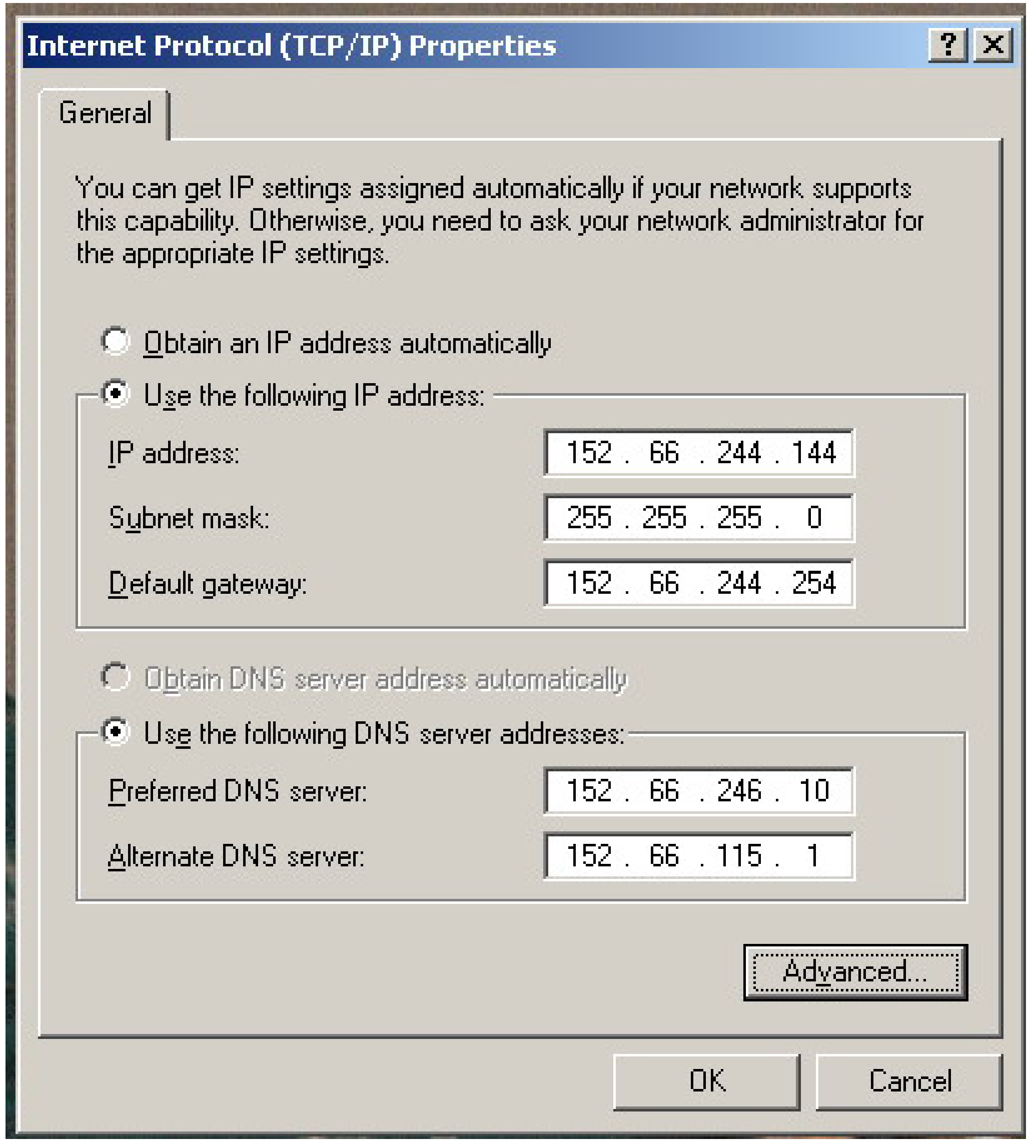


IP settings

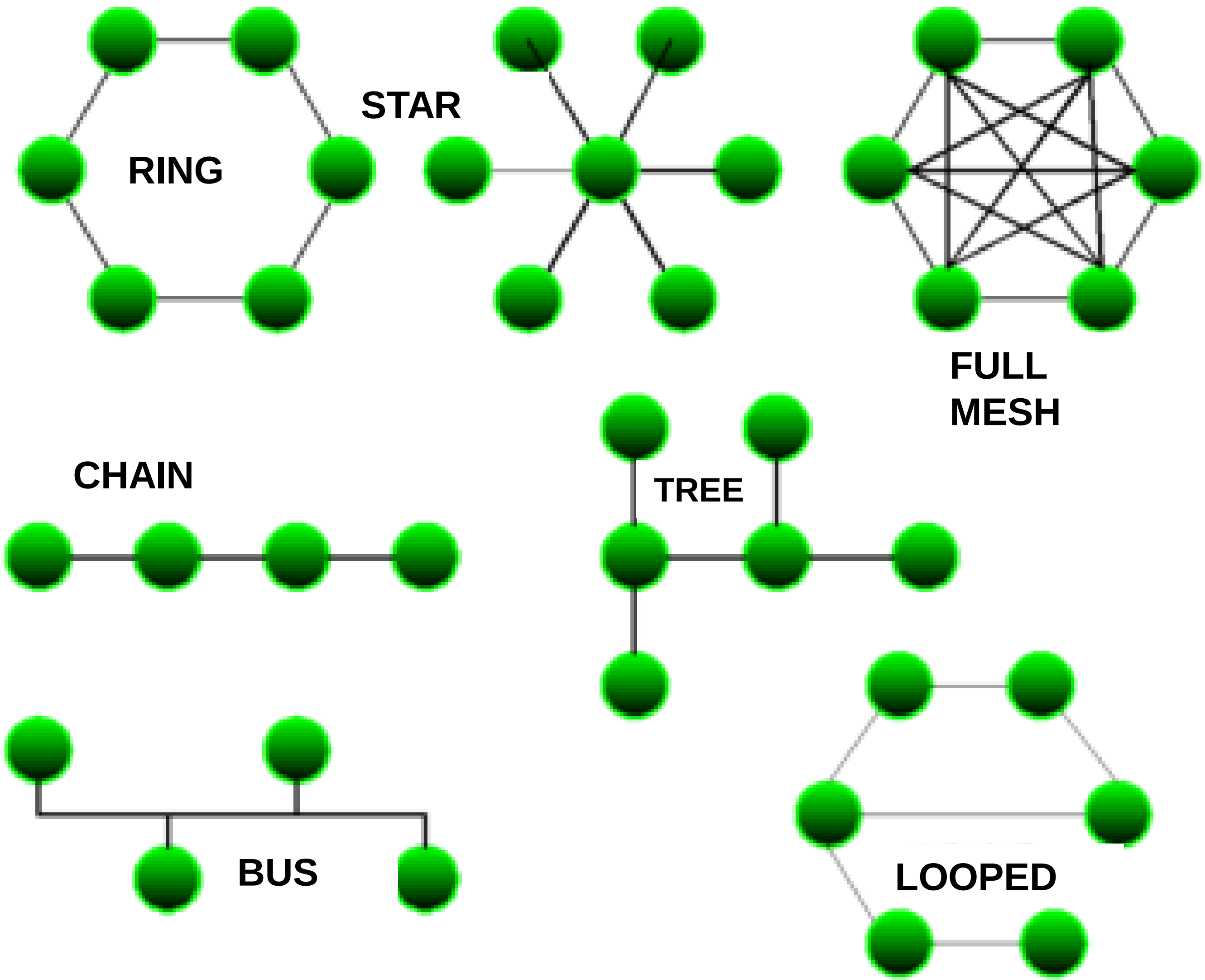
- Basic settings on a computer
  - IP address/netmask
  - Default gateway
  - DNS server
- Extended settings
  - Default domain name
  - More DNS servers



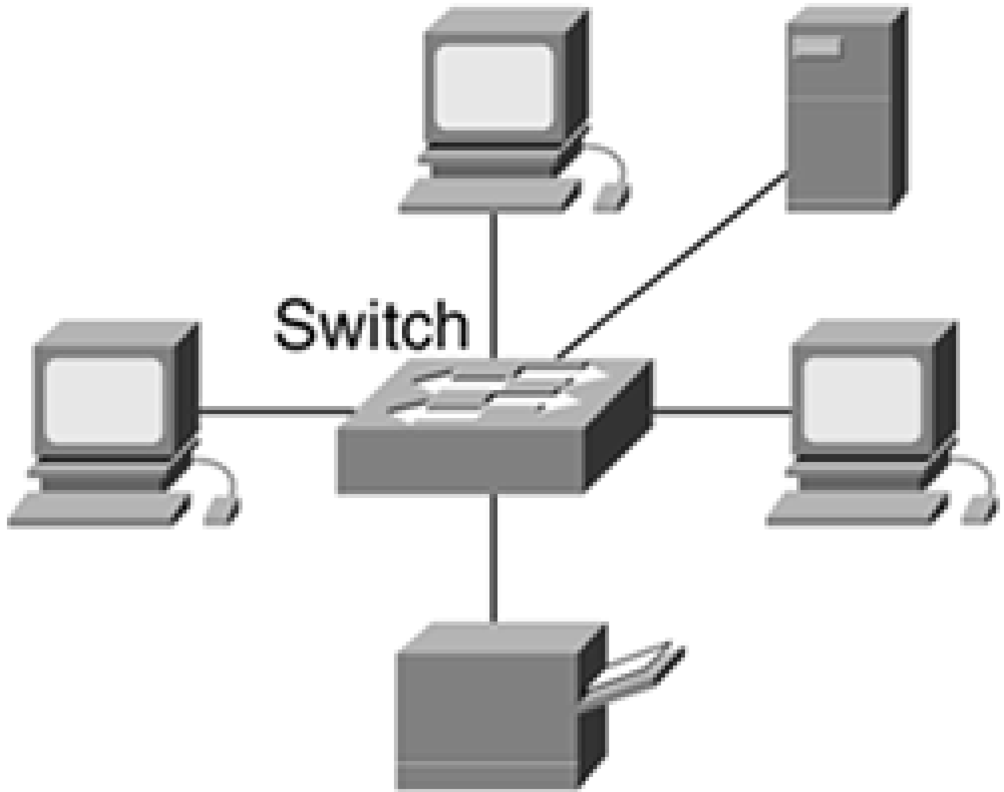
Fixed IP address



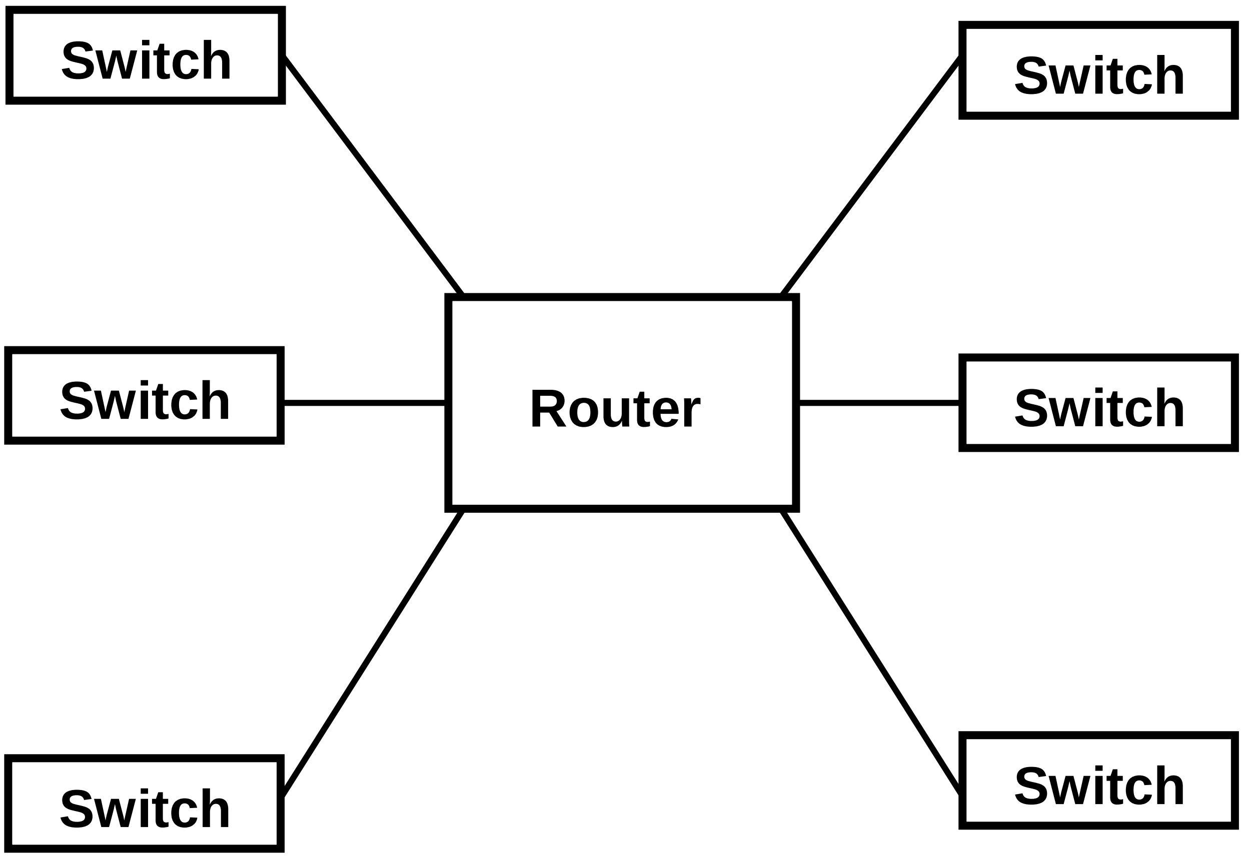
Network Topologies



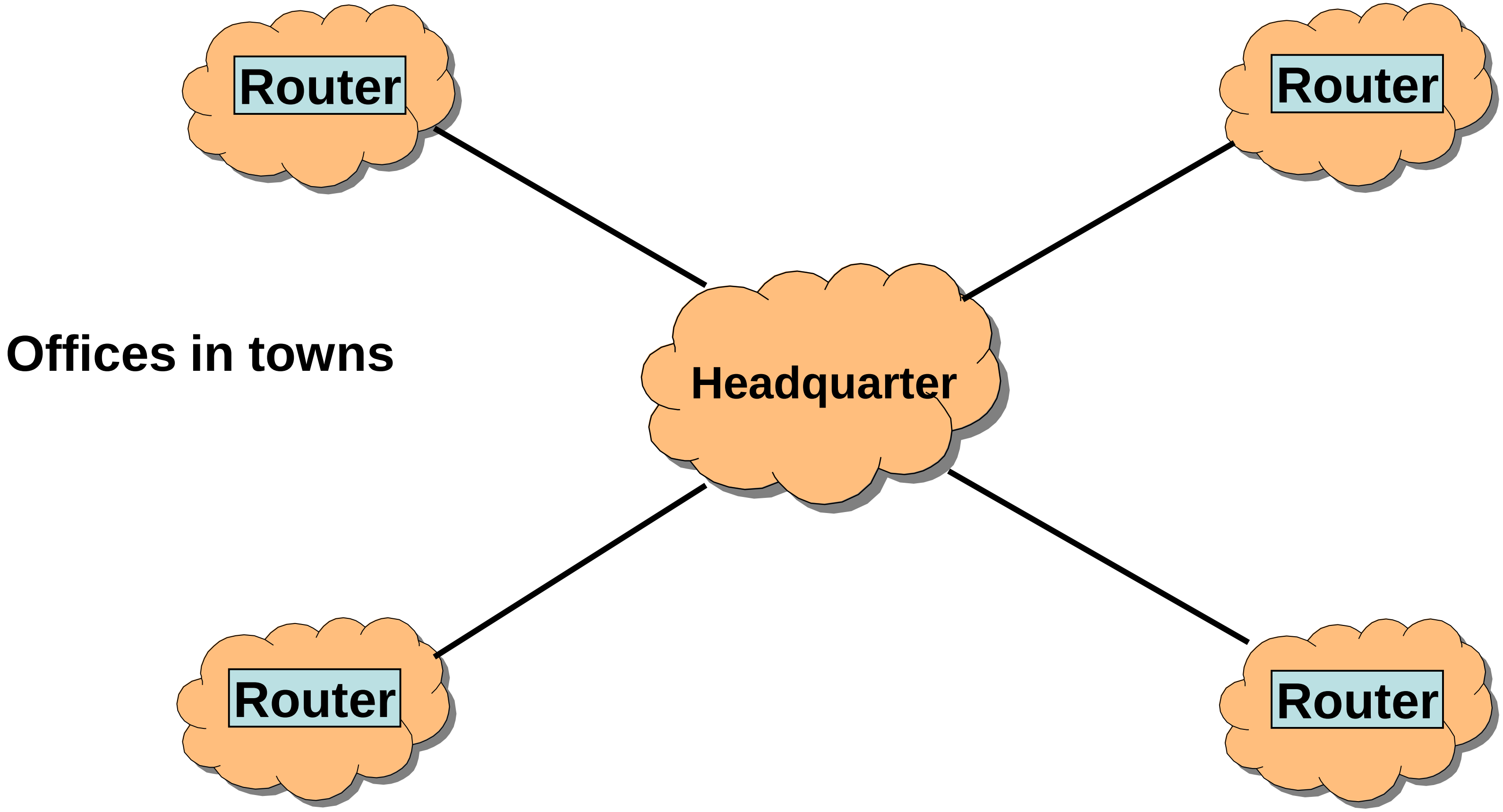
Simple Star LAN



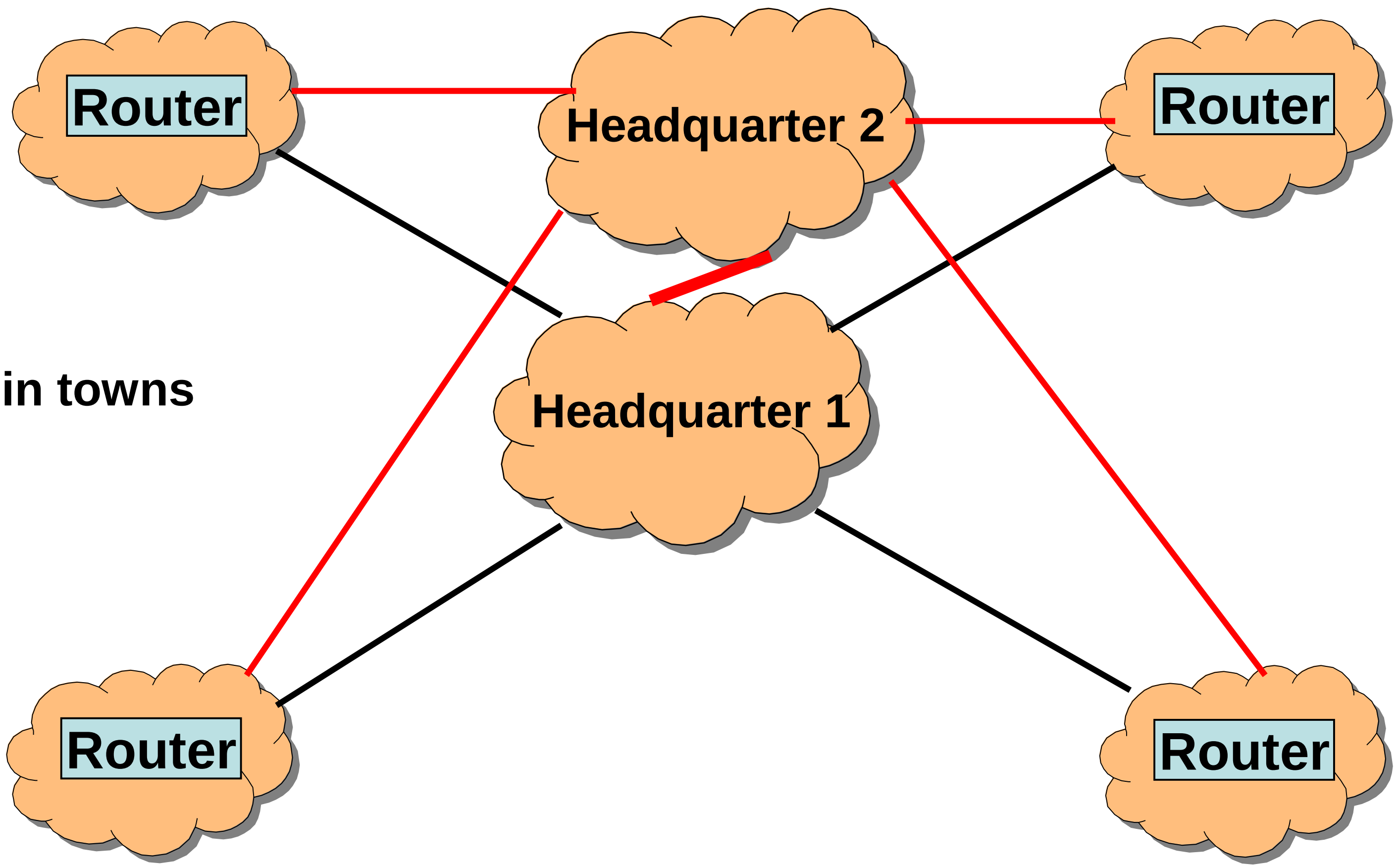
LAN, Campus Network - Star



WAN – Star

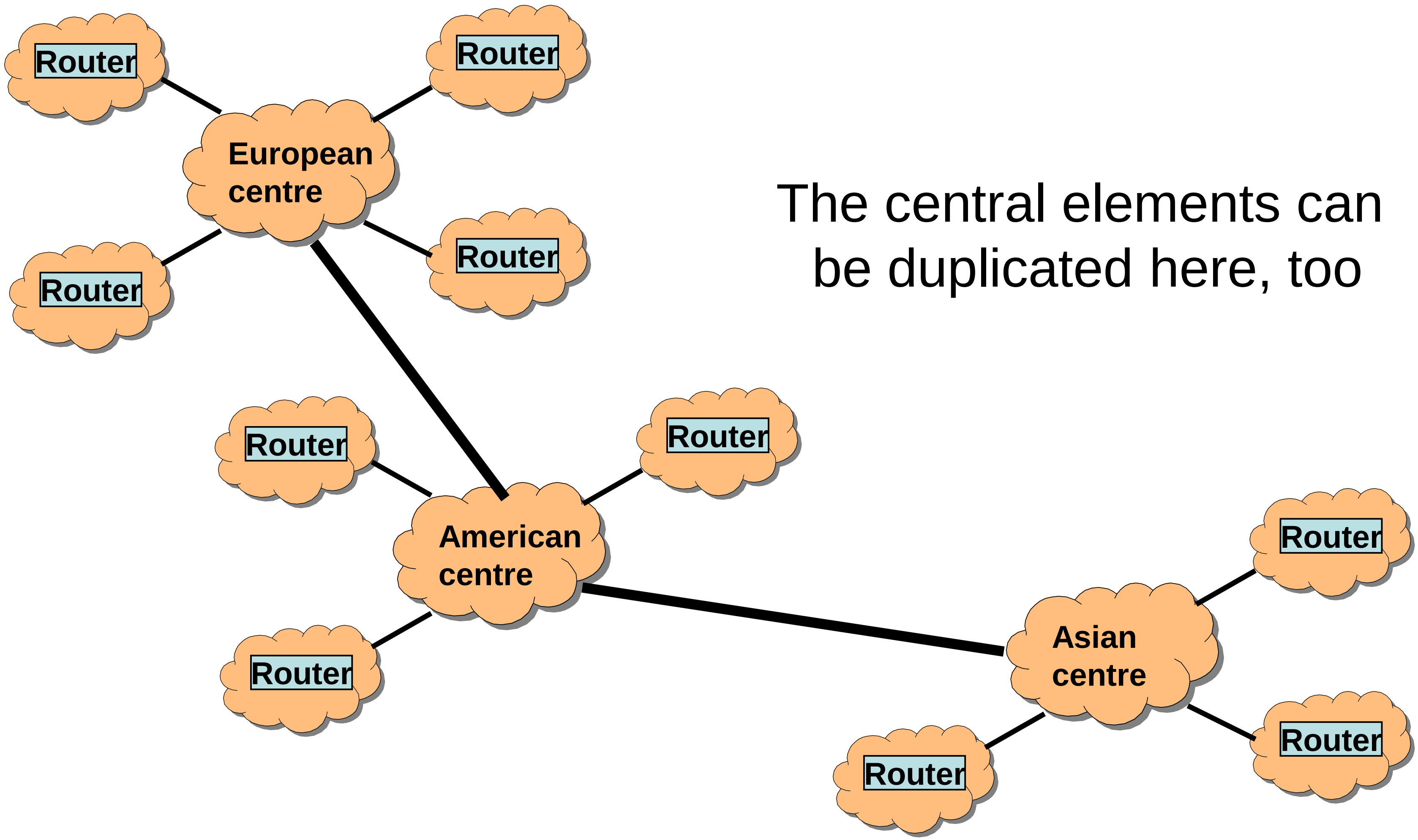


WAN – Star with duplicated centre



Offices in towns

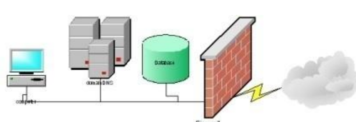
Multiple Star (Tree)



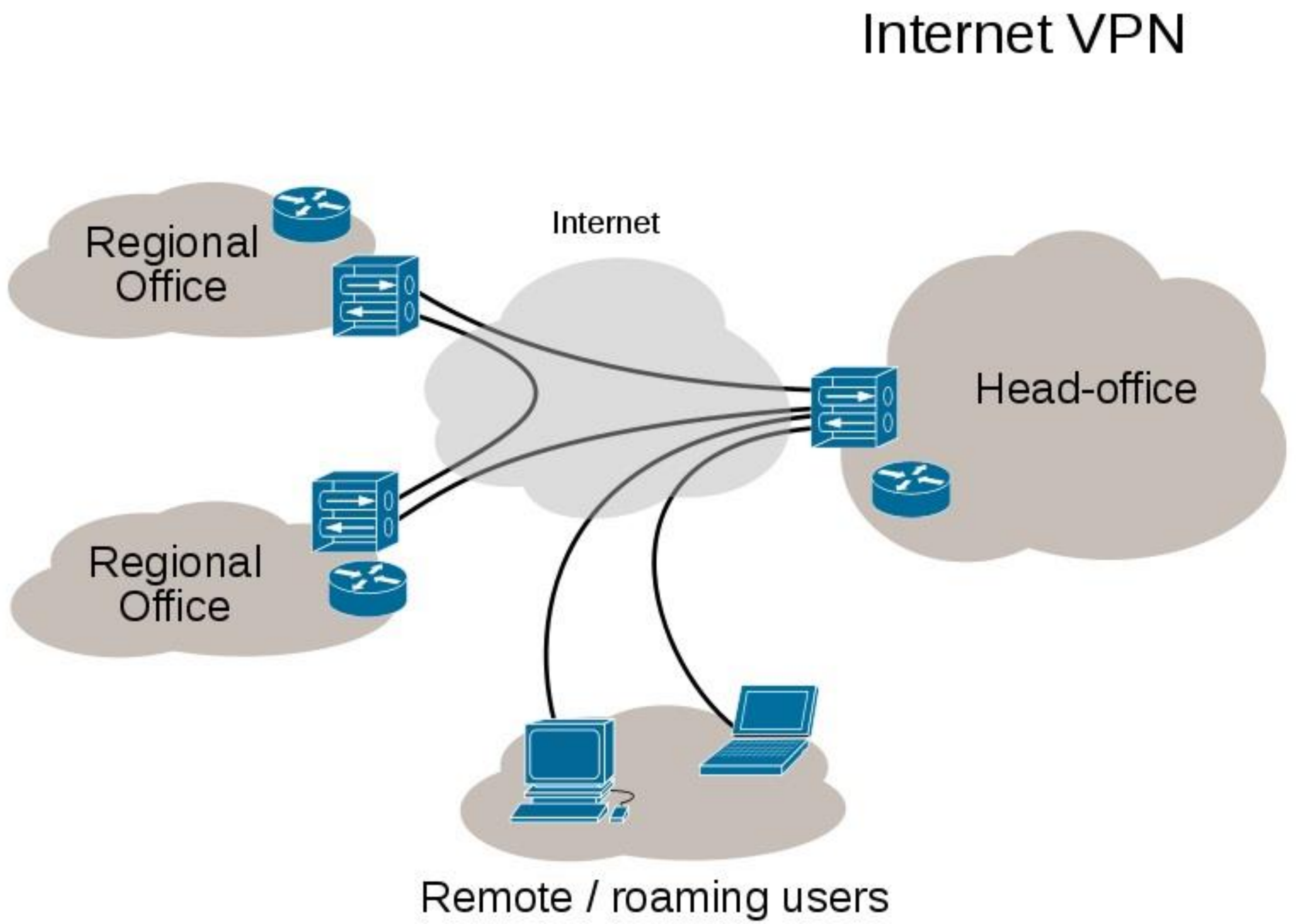
The central elements can be duplicated here, too

Decentralised (distributed) networks

- Chain
  - In case of error: two separated parts
- Ring
  - In case of error: becomes a chain
- Looped
  - Between (certain) nodes two connections
- Full mesh
  - Everybody with everybody else
  - Most reliable but most expensive
    - n*(n-1)/2 connections



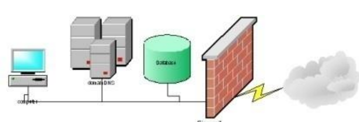
Virtual Private Network



- Transmit data through Internet
  - Not secure
- Leased line
  - Expensive
- VPN
  - Encryption, tunneling

VPN benefits

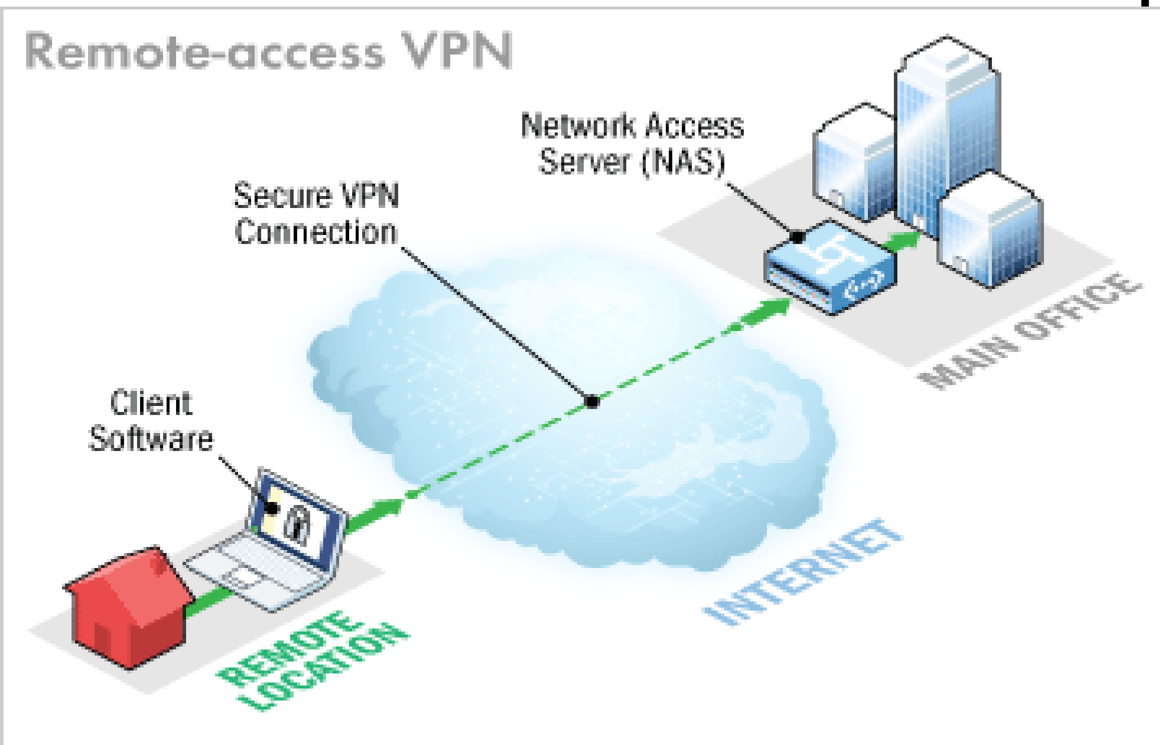
- Extended connections across multiple geographic locations without using a leased line
- Improved security for exchanging data
- Flexibility for remote offices and employees to use the intranet over an existing Internet connection as if they're directly connected to the network
- Savings in time and expense for employees to commute if they work from virtual workplaces
- Improved productivity for remote employees



VPN features

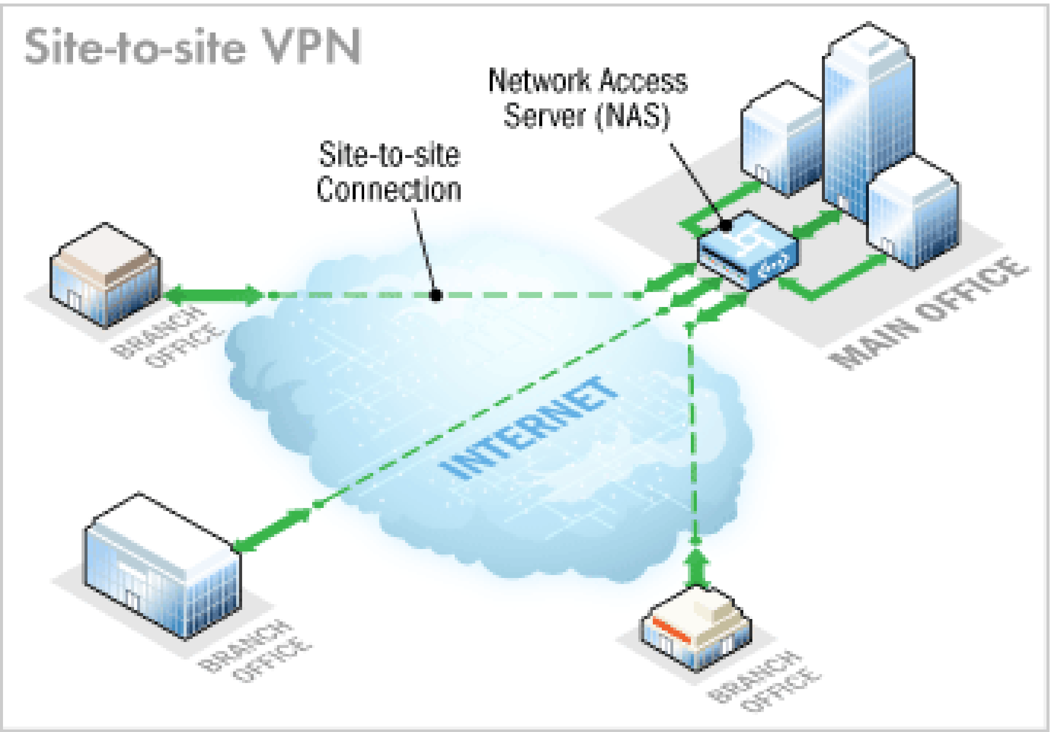
- Security
  - VPN protects data on public network: intruders unable to read or use it
- Reliability
  - Employees/Remote Offices able to connect to VPN at any time
  - VPN provides the same quality of connection for each user even at maximum number of simultaneous connections
- Scalability
  - As a business grows possible to extend without replacing the VPN technology

Remote-Access VPN



- Connects users
  - Network Access Server (Media Gateway, Remote-Access Server)
  - Client software

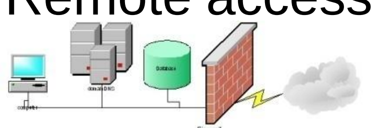
Site-to-site VPN



- Multiple fixed locations
  - Intranet-based
  - Extranet-based
- No need for a client software
- VPN Concentrators
  - (NAS)

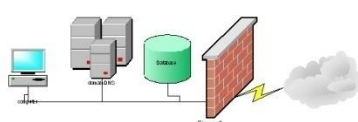
VPN Concentrator

- Network Access Server
  - VPN (tunneling capable) router
  - Sets up and maintains each tunnel in a remote-access VPN
  - Ensures end-to-end delivery of data
  - Encapsulation (tunneling)
    - Packs user data into an other packet
    - Control header
  - Encryption
    - IPSec
      - Site-to-site
    - SSL
      - Remote access



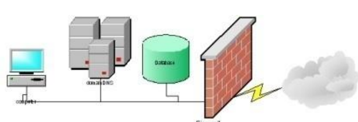
VPN Concentrator

- Firewall
  - What type of traffic can pass through from the Internet onto a LAN and on what TCP and UDP ports
- AAA Server
  - Confirms who you are (authentication)
  - Identifies what you're allowed to access over the connection (authorization)
  - Tracks what you do while you're logged in (accounting)

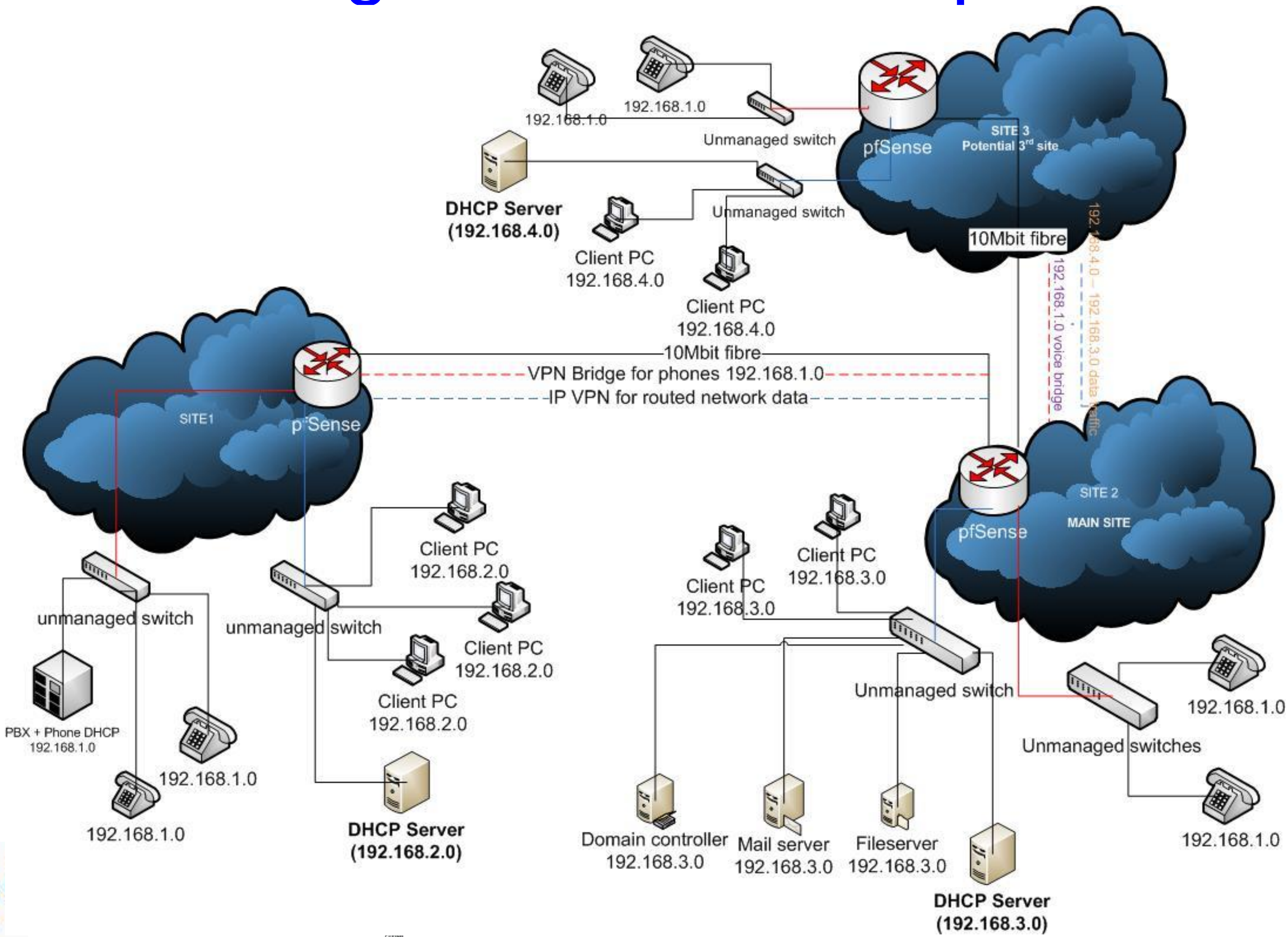


Physical and logical network maps

- Physical:
  - Routes, numbers, types (coaxial, fibre optic) of cables, exact places of endpoints
  - Redundancy (if exists): exact identification of substitutional lines
- Logical:
  - Logical network topology: network identifiers, (numbers, names), speeds
  - Routing protocols used
  - Administrative domains (if more)
- Importance of labeling
- Both logical and physical maps must indicate the boundaries of the network
  - Logical and physical connections to other networks

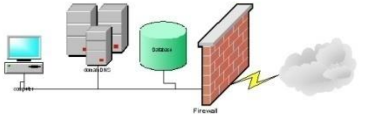


Logical network map



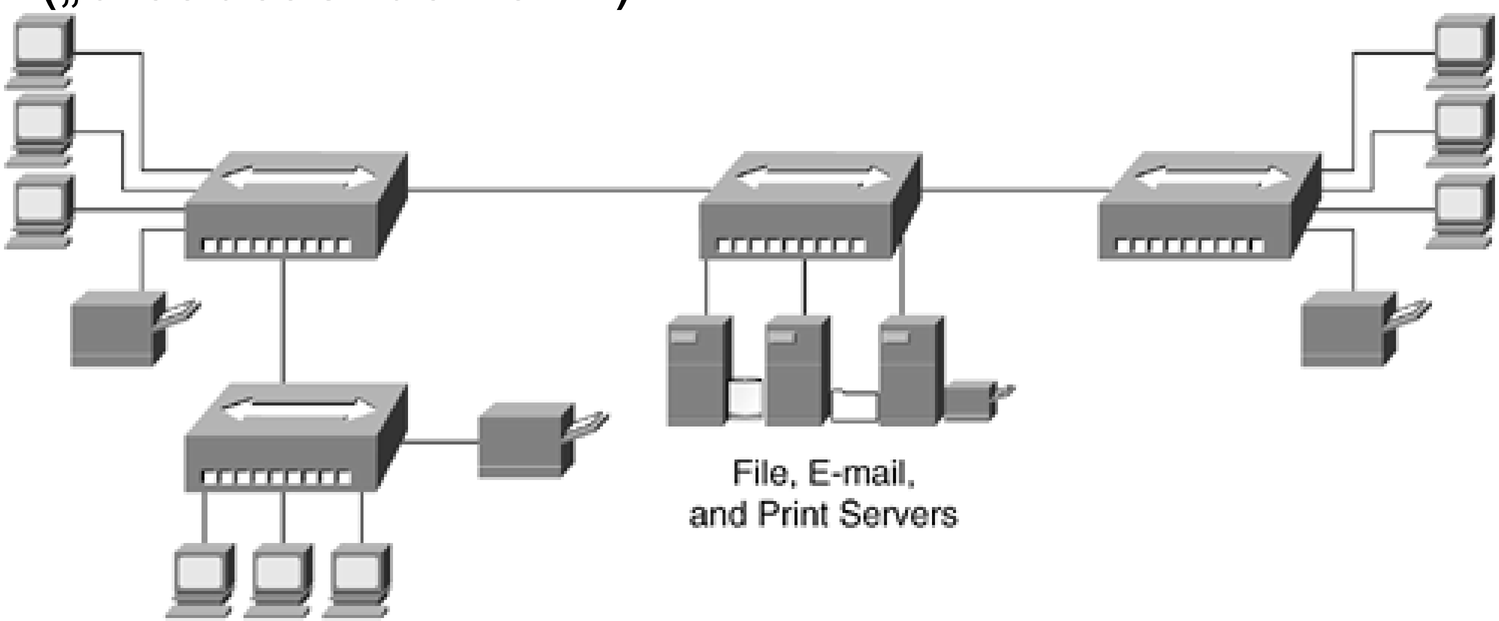
Logical topology

- Network map
- 3rd and above layer devices (router)
- Every sub-network managed by a 2nd layer unit (switch) is a unit („cloud”)
- Sizing (capacity, speed) is determined typically on the basis of the logical topology
  - Routing plan must harmonize with it



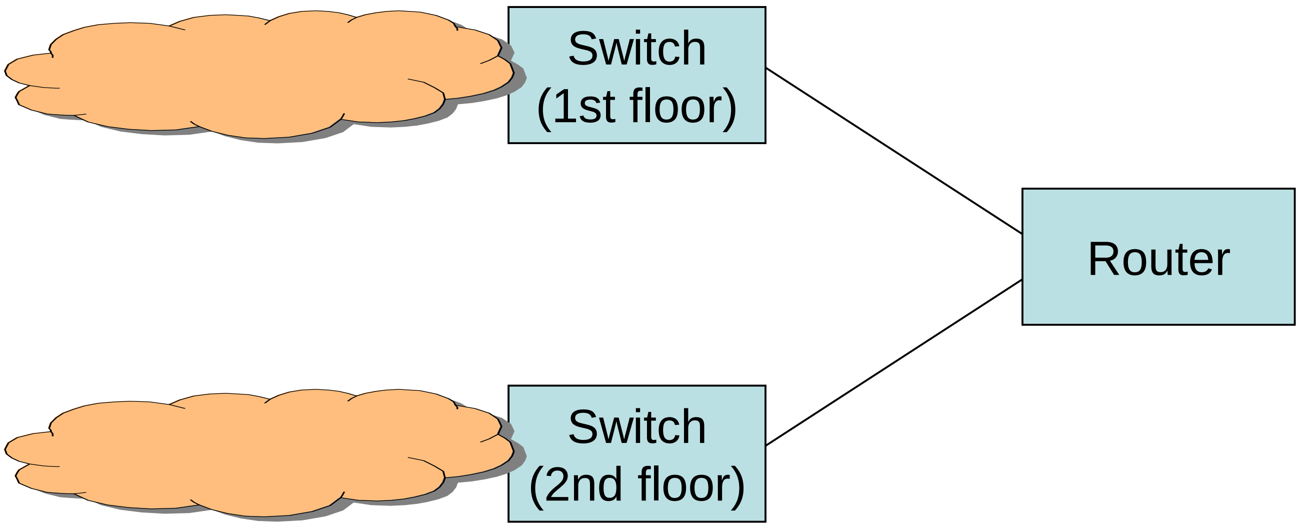
Typical logical topologies

- Flat topology
  - 3rd layer equipments (router) only at boundaries
  - Every device in the same IP address space („broadcast domain”)



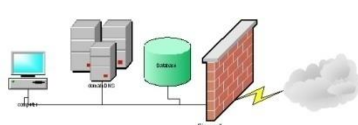
Typical logical topologies

- Location-based topology
  - One-one sub-network at every floor (with own IP address space)



Typical logical topologies

- Functional-group based topology
  - Flat networks according to logical groups, independently from physical location (sales, engineers, managers, marketing)
  - Services (print, file- and nameserver, authentication) typically by groups
  - Sub-networks are connected to the main network by 3rd layer equipments (router)



Demarcation Points

- Definition:
  - Demarcation point is the boundary between the organization and a utility (telephone, network provider, etc.) company
- Responsibility (errors, cabling, etc.):
  - To demarcation point – utility company
  - From demarcation point – organization
- Advisable properly labeling the demarcation points – to be able to show at any time to the technicians of the utility company