cphbusiness

COPENHAGEN BUSINESS ACADEMY





Networks Application Layer

Jens Egholm Pedersen <jeep@cphbusiness.dk>

Litterature:
http://en.wikipedia.org/wiki/Internet_protocol_suite
http://en.wikipedia.org/wiki/Domain_Name_System

Learning Goals

cphbusiness

Network	

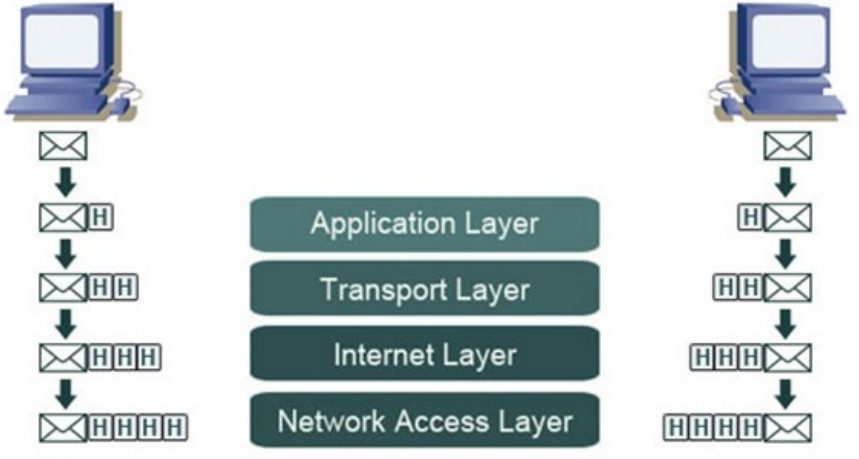
Main Topics	• TCP/IP and the OSI model
	• Network analysis/sniffing
	• Application Layer Protocols
	  • HTTP (Covered in another lesson)
	  • DNS
	  • DHCP

When this lesson is over you should be able to:	• Explain what a network protocol suite is • Describe the layers of the TCP/IP protocol system and the purpose of each layer • Describe the purpose of network sniffing/analysis tools, an use nslookup, ipconfig (ifconfig), ping, traceroute (tracert) and Wireshark for simple analysis scenarios • Give examples of popular Application Layer Protocols

cphbusiness

TCP/IP protocol suite

- A system of protocols
- TCP/IP maintained by the Internet Engineering task force (IETF)



See also: TCP/IP on Wikipedia

cphbusiness

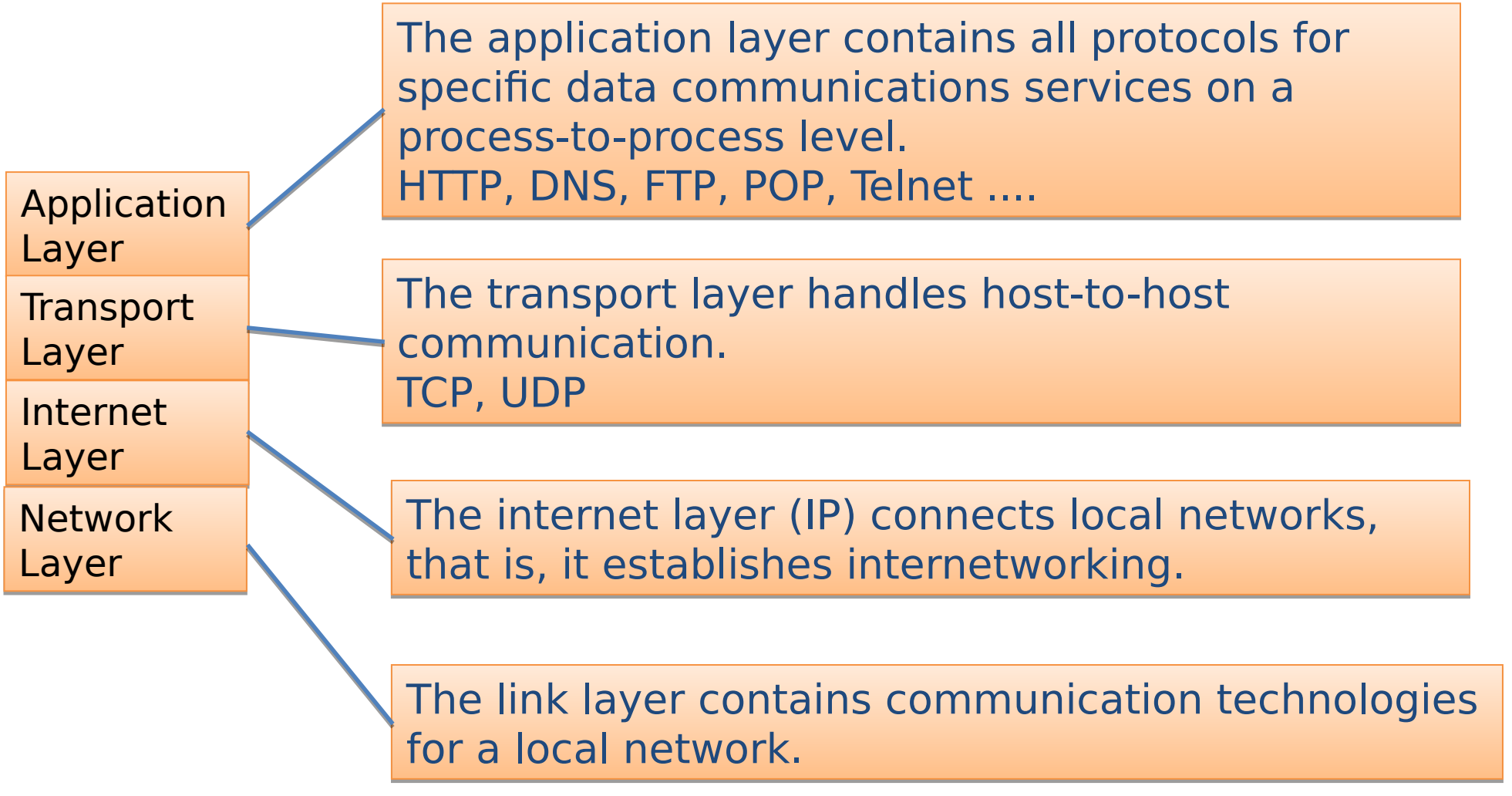
Network interface

- Interface between two pieces of equipment
  - Computer ↔ Router
- Typically a network card
  - But also a local virtual interface
  - If a server listens on localhost, who else sees it?
    - No one!
- One computer = many interfaces
  - Ethernet, Wifi, Loopback, etc.

See also: Network interface controller, Loopback interface

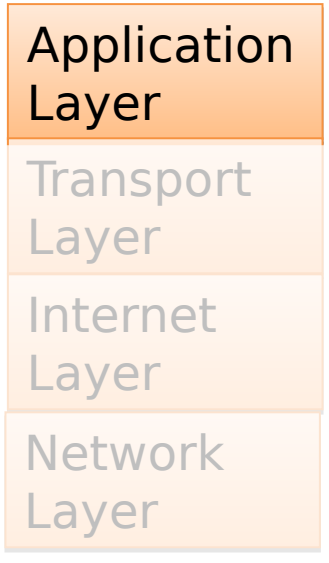
The TCP/IP Protocol Stack

cphbusiness



The Application Layer

cphbusiness



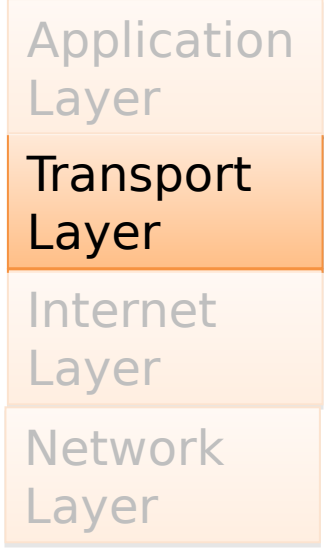
The application layer contains the higher-level protocols used by most applications for network communication.

Data coded according to application layer protocols are then encapsulated into a transport layer protocol (such as TCP or UDP), which in turn use lower layer protocols to effect actual data transfer.

Application layer protocols generally treat the transport layer (and lower) protocols as black boxes which provide a stable network connection across which to communicate, although the applications are usually aware of key qualities of the transport layer connection such as the end point IP addresses and port numbers

The Transport Layer

cphbusiness



The transport layer establishes host-to-host connectivity.

Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers).

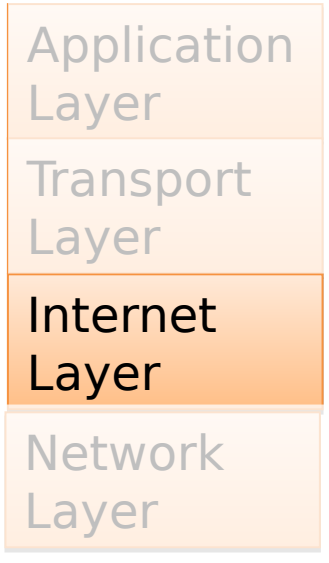
The two major protocols in this layer are:

- **TCP** (Transmission Control Protocol)
  a connection-oriented protocol that addresses numerous reliability issues to provide a reliable connection
  - ❖ data arrives in-order
  - ❖ data is error free
  - ❖ duplicate data is discarded
  - ❖ lost/discarded packets are resent
  - ❖ includes traffic congestion control
- **UDP** (User Datagram Protocol)
  a connectionless unreliable datagram protocol.

What address information would you expect to find at this layer?

The Internet Layer

cphbusiness



- Provides logical addressing so that data can pass among subnets of different types.
- Provides packet routing, the task of sending packets of data (datagrams) from source to destination by sending them to the next network node (router) closer to the final destination
- Relates physical addresses (used at the Network Access layer) to logical addresses.

What address information would you expect to find at this layer?

The Network Layer

cphbusiness

- Application Layer
- Transport Layer
- Internet Layer
- **Network Layer**

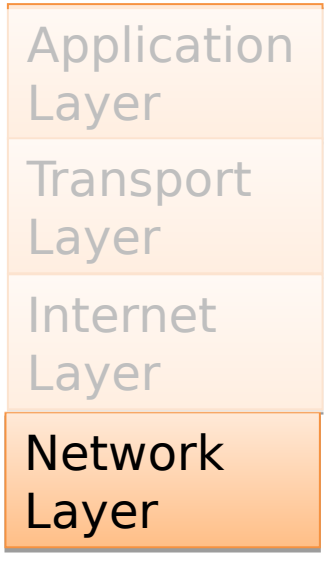
The link layer is the networking scope of the local network connection to which a host is attached. As a result TCP/IP is able to be implemented on top of virtually any hardware networking technology.

The link layer is used to move packets between the Internet layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.

What address information would you expect to find at this layer?

A network frame

cphbusiness



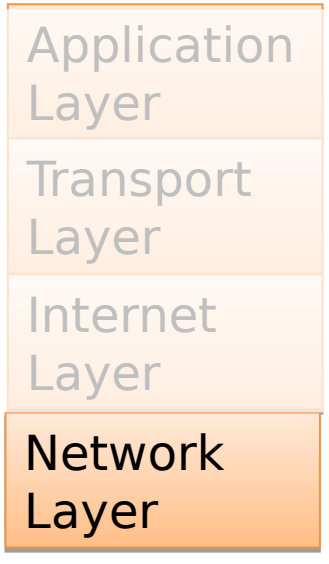
- The smallest transmission unit in networking and telecommunications
- Consists of a header and a packet

- Separated by tiny pauses so the hardware can tell frames apart
  - 100 Gb/s: 0.96ns

See also : Frame (networking), Data Link Layer (OSI)

cphbusiness

Network layer

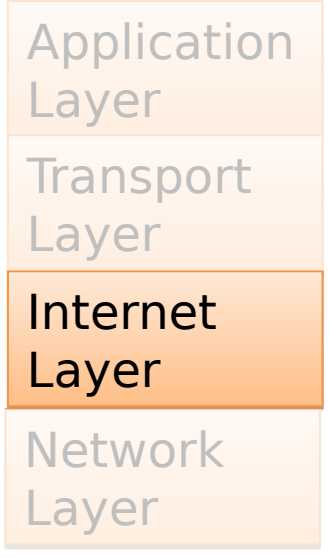


- Physical or logical network
- ARP
  - Maps IP to MAC
- MAC
  - Handles frames
- PPP
  - Direct connection between two hosts

See also : Network layer on Wikipedia

cphbusiness

Internet layer



- Transports packages
- IP
- IPsec
  - Encrypts IP packages
- ICMP
  - Network requests and errors
  - Fx traceroute or ping

See also : Internet Layer on Wikipedia

cphbusiness

Ping and traceroute

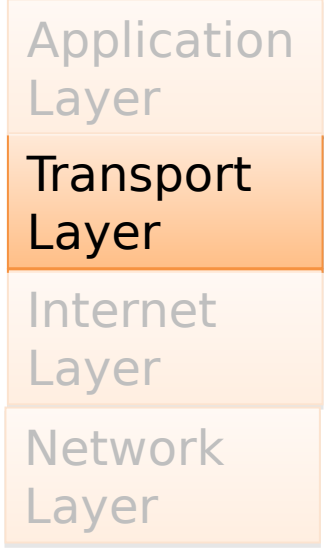
- `ping google.com`

- `traceroute google.com`

See also: Ping on wikipedia, Traceroute on Wikipedia

cphbusiness

Internet layer

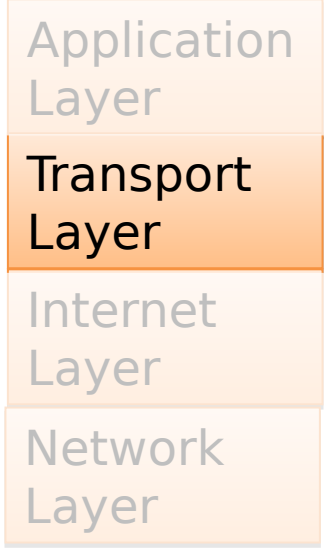


- Host-to-host communication
- TCP
- UDP

See also : Internet Layer on Wikipedia

cphbusiness

Package sniffing



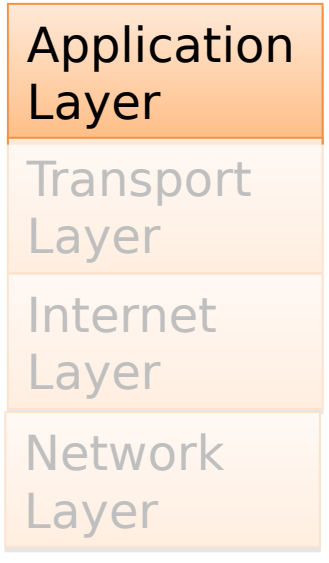
- Transport layer sends packages
- These can be sniffed!
  - Wireshark example

See also : Internet Layer on Wikipedia

cphbusiness

Application layer

- Process-to-process communication
- A lot !



See also : Application layer on Wikipedia

Application Layer Protocols

cphbusiness

DHCP - DHCPv6 – **DNS** – FTP – **HTTP** - IMAP – IRC – LDAP – MGCP – NNTP – BGP – NTP – POP – RPC – RTP – RTSP – RIP - SIP – SMTP – SNMP – SOCKS - SSH - Telnet - TLS/SSL ...

Tools we will use this semester

cphbusiness

- nslookup
- ipconfig (MAC ➡ ifconfig)
- Ping
- Netstat ➡
- TraceRoute (Windows tracert)

(Telnet can sometimes be useful to check if a port is blocked by your ISP, or to "test" a TCP server (your chat server) without a client)

The Domain Name System

cphbusiness

The *Domain Name System,* or DNS, is a globally distributed, scalable, reliable, dynamic database, used to map between hostnames and IP addresses, and to provide electronic mail routing information.

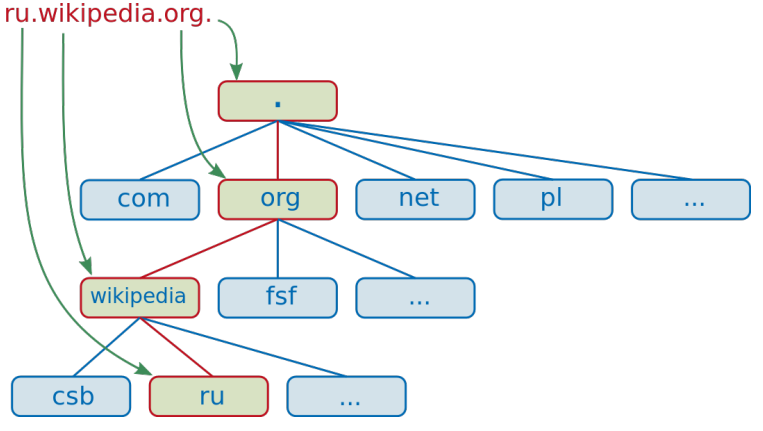
Basically three components are involved:
•A Domain Name Space
•Servers making the Domain Name Space available
Clients which query the servers about the name space

cphbusiness

Domain name

- Read from right to left
- Fully qualified domain name (FQDN)
  - Begins with the root domain "."

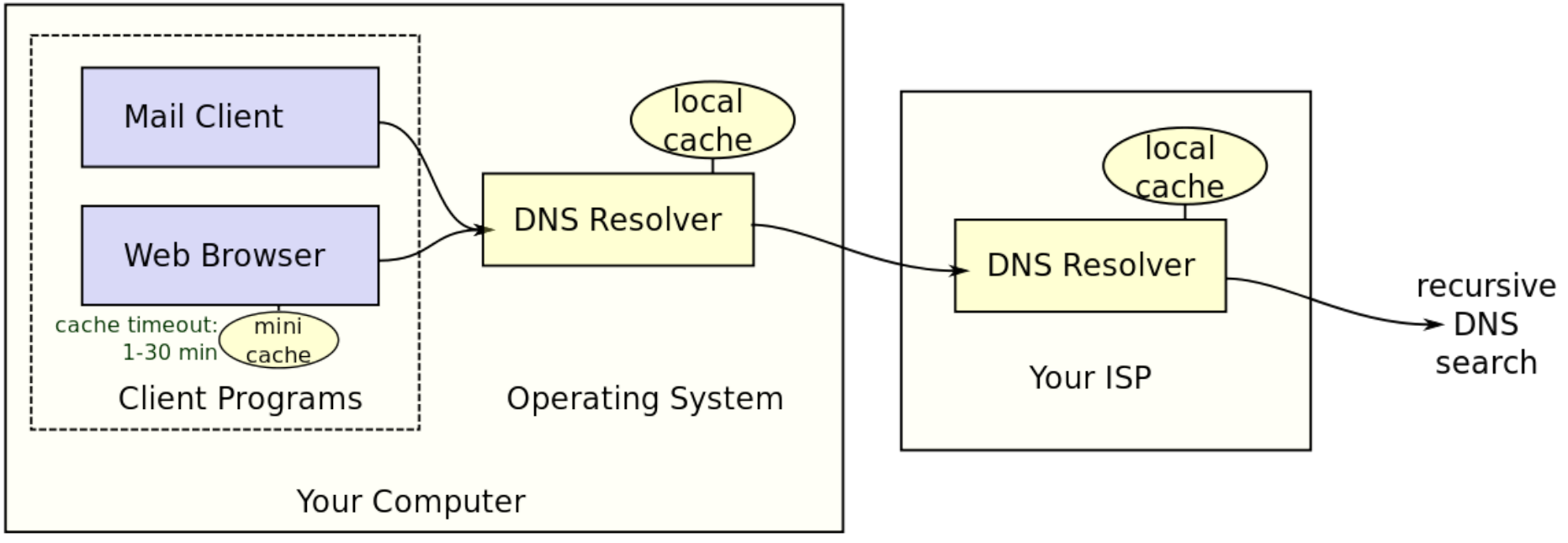
1) Root domain
2) Top-level domain
3) Second or third level



See also : Network Address Translation on Wikipedia

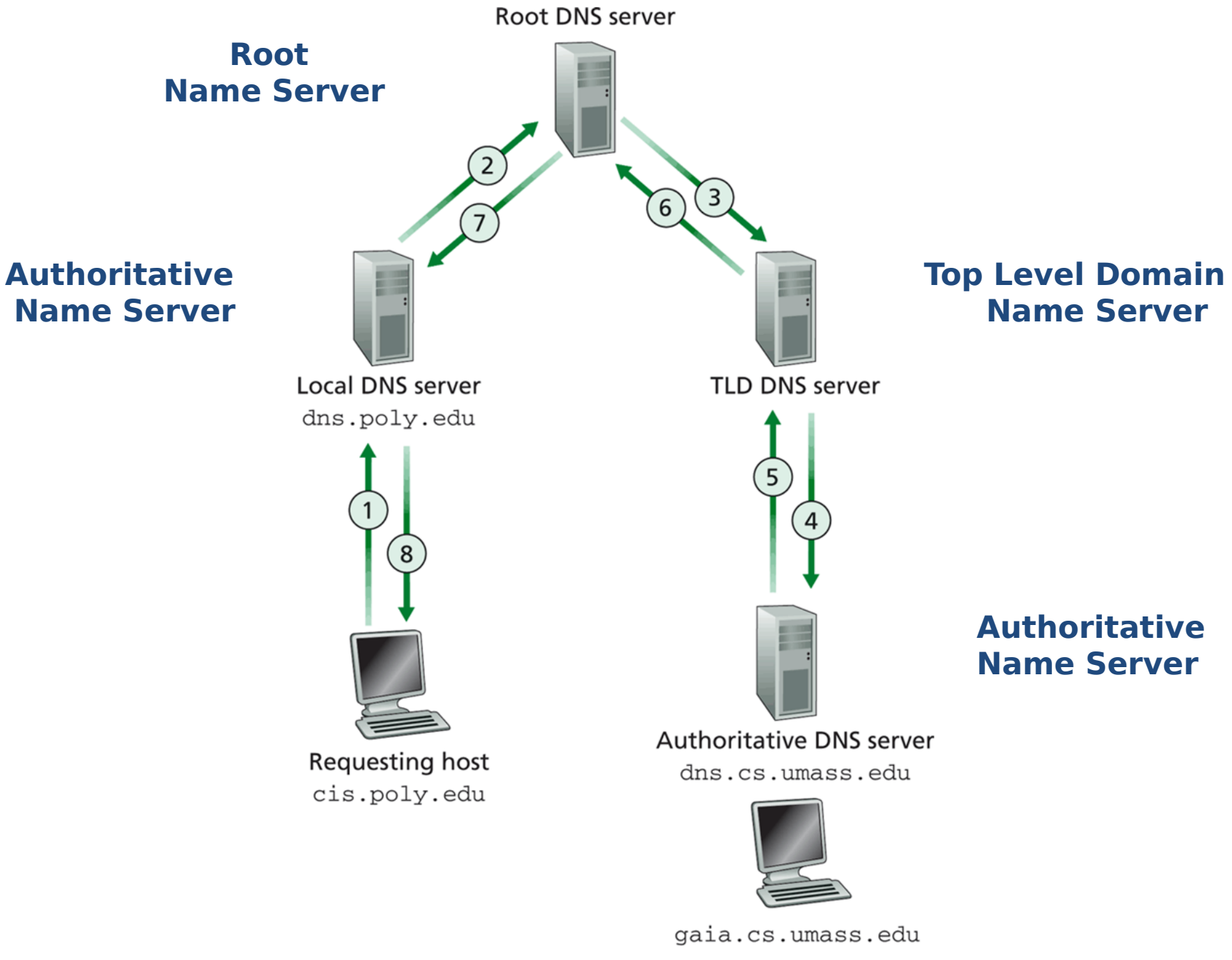
DNS Resolving

cphbusiness



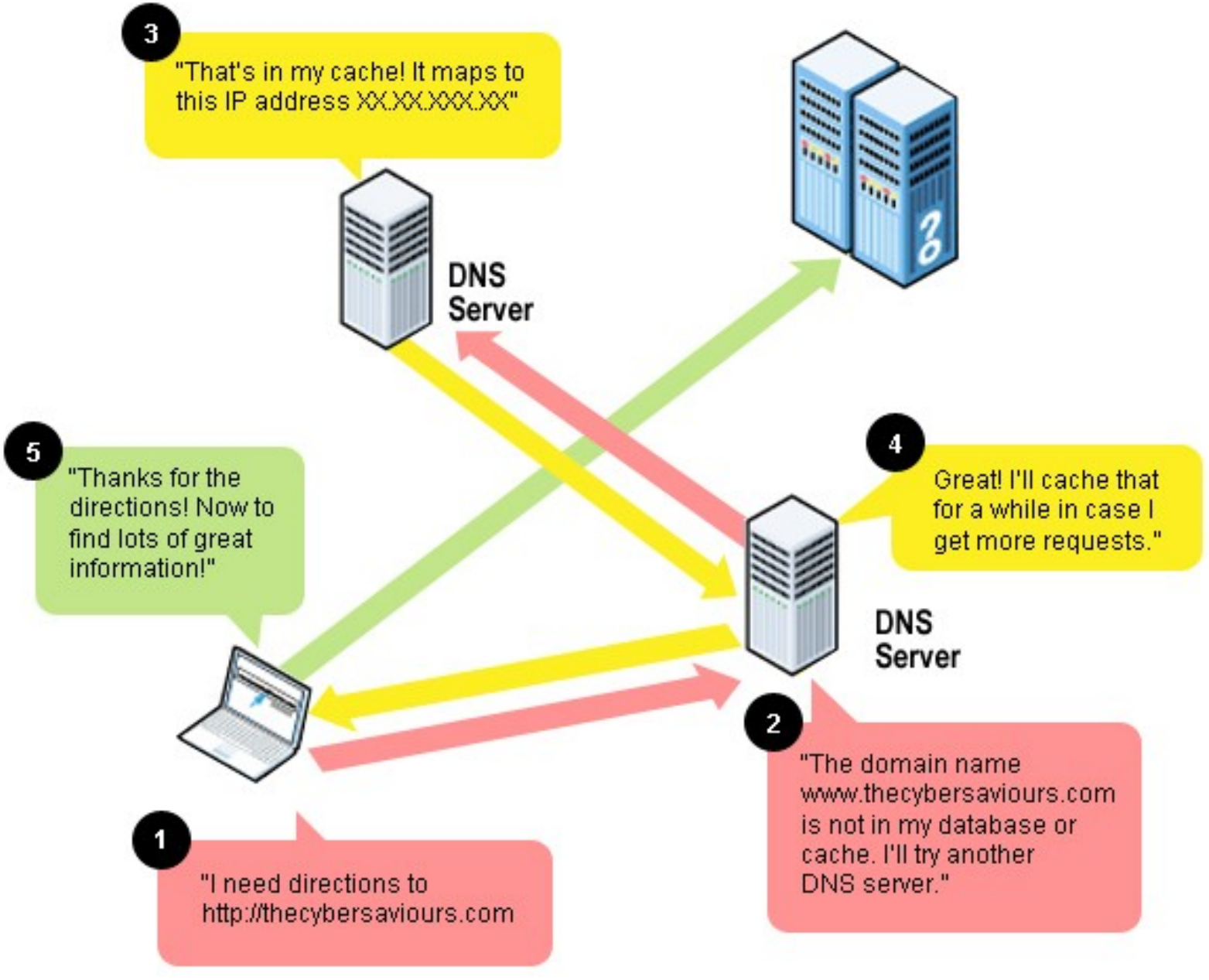
Recursive DNS search

cphbusiness



DNS Caching

cphbusiness



cphbusiness

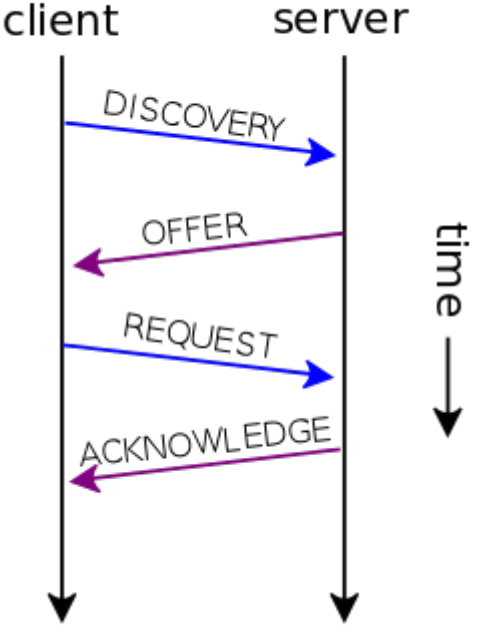
nslookup

- `nslookup google.com`

- Who sets these addresses ?

DHCP

- Dynamic Host Configuration Protocol
- Dynamically distributes addresses and subnetmasks, gateway etc.



See also: DHCP on Wikipedia

DHCP - Operation

cphbusiness

- When a DHCP-configured client connects to a network, it sends a broadcast query requesting necessary information to a DHCP server.
- The DHCP server manages a pool of IP addresses and information such as default gateway, domain name, and so forth.
- On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and parameters, such as the subnet mask and the default gateway.
- The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts.
- Upon disconnecting, the IP address is returned to the pool for use by other clients

cphbusiness

Network Address Translation

- With subnets comes local IPs
- How can hosts reach local Ips?
  - A gatekeeper switches addresses!

See also : Network Address Translation on Wikipedia

cphbusiness

The IP package

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

How do you translate a package from one network to another?

- You switch the source and destination addresses

cphbusiness

Network Address Translation

1) Local machine sends package
2) Router sees package and replaces source IP with the router's own IP
3) Remote host replies to router
4) Router sees reply and replaces destination IP with local IP

See also : Network Address Translation on Wikipedia

traceroute

- Linux: `traceroute google.com`
- Windows: `tracert google.com`

traceroute

- Linux: `traceroute google.com`
- Windows: `tracert google.com`

- Who sees your traffic?
  - Everyone!

netstat

- `netstat`
- Active connections (sockets) on your machine
- Who opens these?
  - Active connections on your computer

Learning Goals

cphbusiness

Network	

Main Topics	• TCP/IP and the OSI model
	• Network analysis/sniffing
	• Application Layer Protocols
	  • HTTP (Covered in another lesson)
	  • DNS
	  • DHCP

When this lesson is over you should be able to:	• Explain what a network protocol suite is • Describe the layers of the TCP/IP protocol system and the purpose of each layer • Describe the purpose of network sniffing/analysis tools, an use nslookup, ipconfig (ifconfig), ping, traceroute (tracert) and Wireshark for simple analysis scenarios • Give examples of popular Application Layer Protocols