Network Layers

Standardization Cruelty

This chapter introduces the layer concept widely used in data communication. Most famous is the ISO-OSI 7-layer model, which is also discussed in great detail here. By the way the interaction of layering and standardization is explained.

“The good thing about standards is that there are so many to choose from”

Andrew S. Tanenbaum

Standards

- We need networking standards
  - Ensure interoperability
  - Large market, lower cost (mass production)
- Vendors need standards
  - Good for marketing
- Vendors create standards
  - Bad for competitors, hard to catch up
- But: Slow standardization processes freeze technology...

We need standards. Unfortunately. Otherwise, each vendor would create what he wants and we would not be able to communicate accross networks. This situation occured very often in history. For example the United Nations initiated a world-wide Telephony standardization board, known as CCITT (today ITU-T). Or in the pre-Ethernet age, many vendors built completely incompatible LAN protocols.

Especially to force interoperability, many vendors for Internet-equipment initiated the TCP/IP Interoperability Conference in 1987, today known as "INTEROP".

Who Defines Standards?

- **ISO – Anything**
- **IETF – Internet**
- **ITU-T – Telco Technologies**
- **ATM Forum**
- **Frame Relay Forum**
- **IEEE – LAN Protocols**

The above slide mentions the most important standardization organizations.

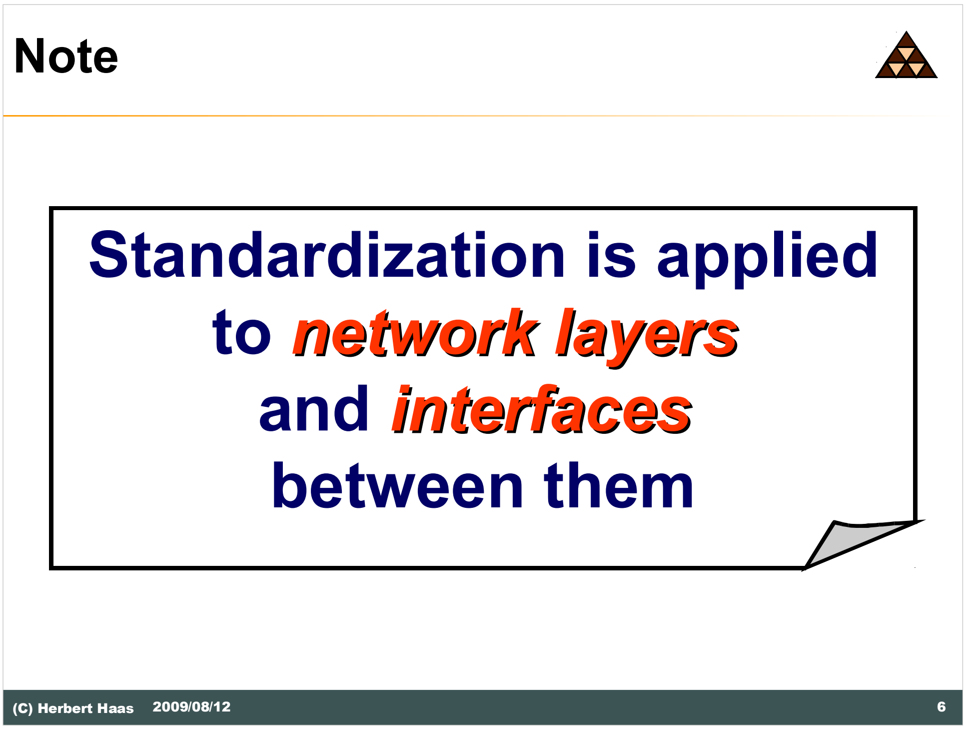
The Internet Engineering Task Force (IETF) is "actually" the most important technical organization for the Internet working groups and is organized in several areas. Area manager and IETF chairman form the IESG (Internet Engineering Steering Group). The IETF is also responsible to maintain the RFCs.

Standards Types

- De facto standards
  - Anyone can create them
  - E.g. Internet RFCs
- De jure standards
  - Created by a standardization organization
  - E.g. ISO/OSI, ITU-T

Not all standards are like the others. De facto standards are more flexible and speed-up the implementation. Usually everybody is allowed to extend them. The whole Internet is built on such loosely standards. Unfortunately misinterpretations can occur. (RFC's)

De jure standards are like acts of law. For example ITU-T standards explain nearly every detail implementers may ask.



The above sentence leads us to network layers. Break big problems into smaller ones and write standards for them ("divide and conquer"). Of course the interfaces between the layers must be standardized too. Eventually, multiple developers can work on different parts of the whole story.

Network Layers

- **Divide task of communication in multiple sub-tasks**
- **Hierarchically organized**
  - **Each layer *receives* services from the layer below**
  - **Each layer *serves* for the layer above**
- **Good for interoperability**
  - **Capsulated Entities and Interfaces**
- **But increases complexity**

Network layers are an abstraction to hide complexity. Layers are organized hierarchically, that is there is a predefined command direction. Imagine what would happen if we have a democratic model?

Note that network layers force a more complex development. Many high-performant communication technologies have been developed in an ad-hoc act, or alternatively consists of only a few layers.

Where to Define Layers

- Group functions (services) together
- When changes in technology occur
- To expose services
- To allow changes in protocol and HW
- To utilize existing protocols and HW

A good layering structure requires a intelligent grouping of functions. Ideally, technology improvements can be implemented immediately.

For example the X.25 packetizing algorithm, which is written in software and part of a network driver of the operating system can remain untouched, while the serial line hardware can be updated, and vice versa.

The ISO standardized anything–character sets, paper sizes, screws, ..., and network layers. In 1988 the US Government required any communication device to comply with the ISO/OSI model (GOSIP). Note that the non-OSI Internet was built much earlier, so many people expected the end of the Internet. But the Internet (which was created as nuclear-bomb resistant) not only survived the ISO/OSI model but also displaced many OSI-compliant protocols, such as CLNP.

Similarly, in Europe the "European Procedurement Handbook for Open Systems" (EPHOS) had been released.

Purpose

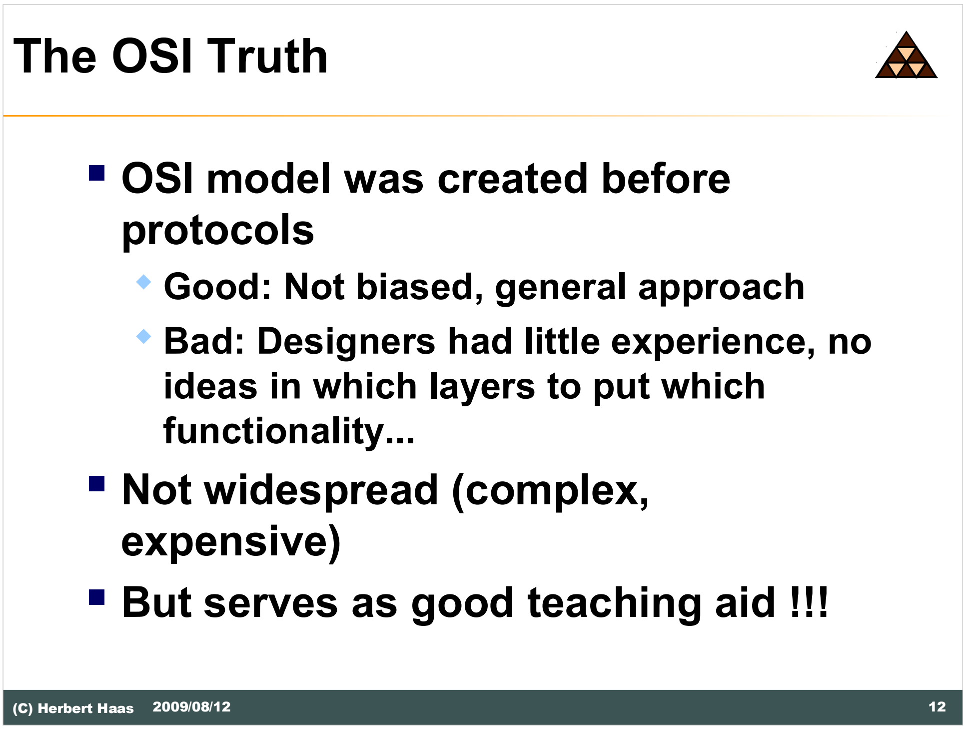
- OSI model *describes* communication *services* and *protocols*
- No assumption about
  - Operating system
  - Programming Language
- Practically, the OSI model
  - Organizes knowledge
  - Provides a common discussion base

Although every book of data communication mentions the ISO/OSI 7-layer model it is not that important in the real world: most technologies do not comply to this model. It is merely a reference model so that we can refer to it when we want to explain certain functions in our protocols. From this point of view the OSI model is indeed important today.

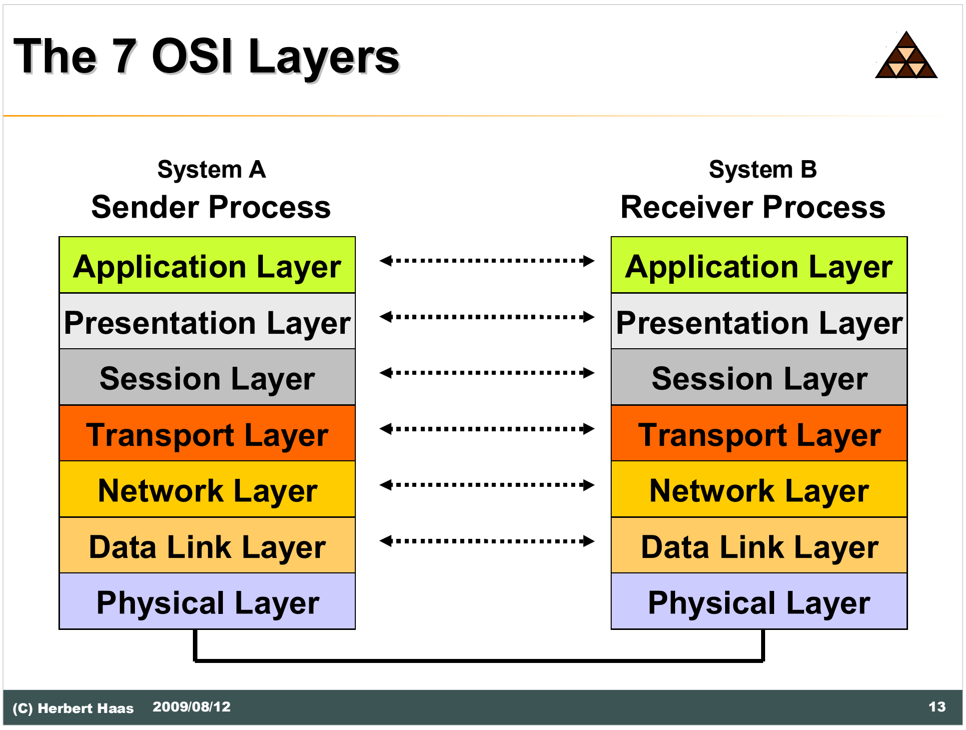
OSI Basics

- Point-to-Point, no shared media
- Nodes are called
  - End Systems (ES)
  - Intermediate Systems (IS)
- Each layer of the OSI model detects and handles errors (FCS)
- Dumb hosts and intelligent network
  - Compared with Internet: dumb network, intelligent hosts

The original OSI modes was created for point-to-point connections only (for example there was no specification for LAN-like shared media originally).



Although the OSI Model was created before the protocols, and so the complete model is very complex and not practically elaborated, its widely used today to define and category most of the important protocols. OSI is not biased because this reference framework is not associated with any particular vendor philosophy. OSI represents a general approach for describing data communication procedures but this property is often considered as a big disadvantage, because practical implementations typically can be described with a much simpler model and on the other hand the OSI architects had only little experience with real life implementations. Therefore, genuine OSI protocols are not really widespread today, because of its complexity. Nevertheless, the OSI model serves as reference frame when discussing or learning about protocols.



Because the communication between different systems can be a very complex task, OSI splits the communication aspects into smaller tasks. All layering is based on the OSI reference Model, which defines tasks and interactions of seven layers.

The user's data moves from the first layer (Application Layer) through all other layers. When two systems communicate with each other, then only the different layers talk. The application layer only talk with the application layer or the network layer only communicate with the network layer of system B. We can talk about a parallel communication between the layers. Every layer works for its own, it is not interested what the other layer does.

Physical Layer

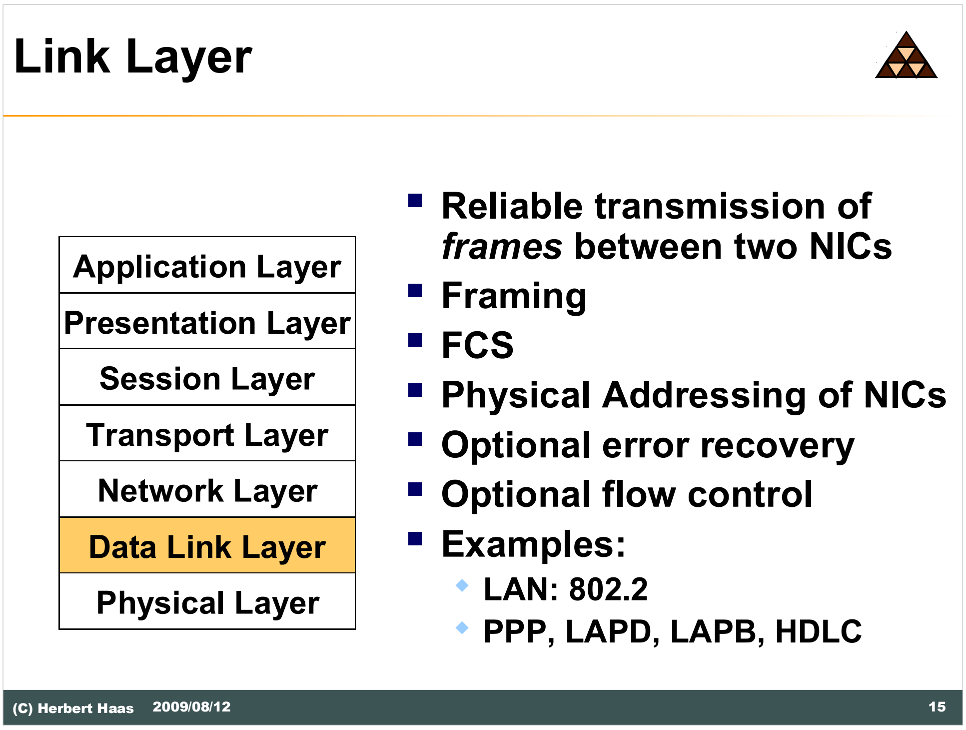
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

- Mechanical and electrical specifications
- Access to physical medium
- Generates Bit stream
- Line coding and clocking
- Examples
  - LAN: Ethernet-PHY, 802.3-PHY
  - WAN: X.21, I.400 (ISDN), RS-232

The Physical Layer generates the bit stream. This layer provides access to the physical medium by applying line coding (NRZ, Manchester, etc), synchronization (clocking, PLL), but also includes mechanical specifications. Layer 1 also can activate or deactivate the links between end systems (link management).

The physical part of the Ethernet NIC is called "PHY" and is perhaps the most complex entity of Ethernet because the PHY consists of a number of sublayers that care for interoperability with different Ethernet speeds (10, 100, 1000, 10000 Mbit/s) and codings (Manchester, 4B5B, 8B10B, ...). Note that there is a fundamental difference between "Ethernet" and IEEE "802.3": these are two separate LAN specifications but typically implemented on the same NIC—they just share the same topology and use the same media access strategy—most people are not aware of that.

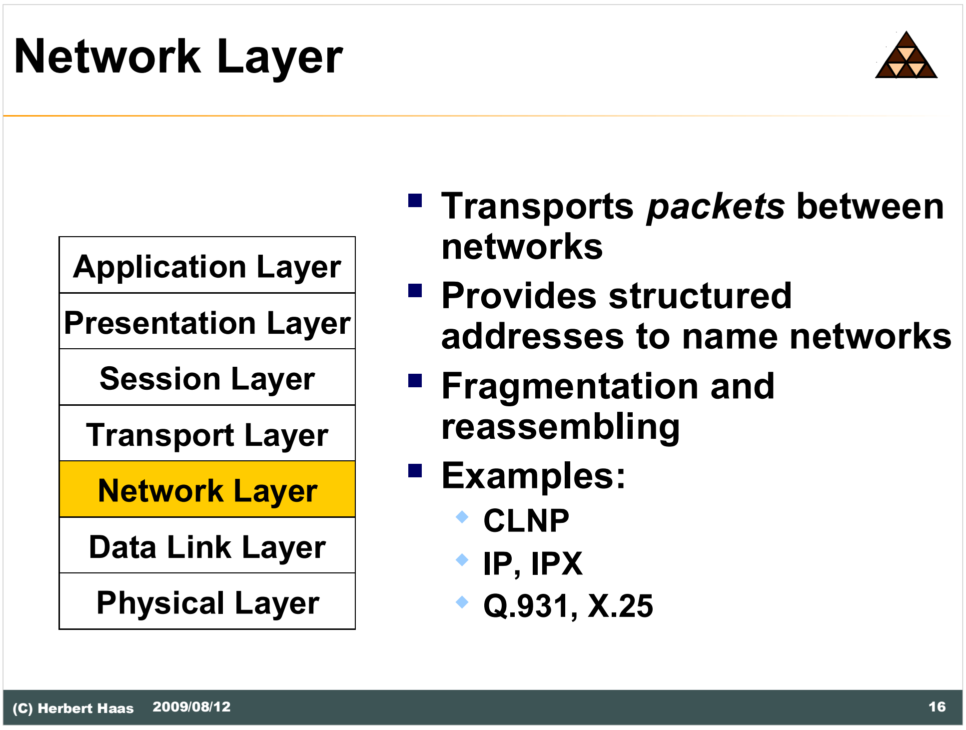
The X.21 is a typical and widely available interface on a Cisco router. The ISDN-layer 1 is specified in the ITU-T standard I.400 and describes both a 192 kbit/s synchronous multiplexing interface capable to transport 2 B channels and one D channel and secondly a high speed 2.048 Mbit/s interface capable to carry 30 B channels and one D channel. These ISDN specifics are presented in the N-ISDN chapter in more details. The old well-known Recommended Standard (RS) 232 specifies the classical serial interface found on many PCs and other peripheral devices.



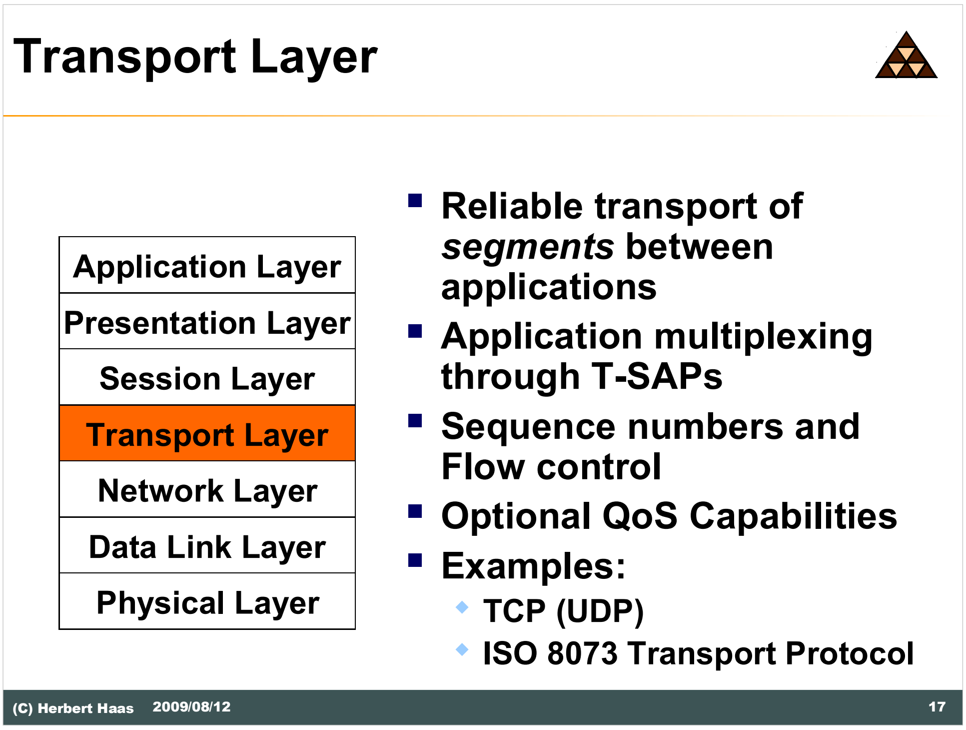
The data link layer builds the frame. In that way, framing or frame synchronization is the most important thing on layer 2. Where is the beginning of the frame ? Where is the end ? With a special Bit-Code the layer 2 protocols, such as HDLC or PPP, guarantee the framing of the data. That's important for the MTU (maximum transfer unit).

Also frame checking, correction of transmission errors on a physical link, is implemented on layer 2. There are also a physical address of the network interface cards. This address is transported with the data link layer too (e.g. MAC-Address with Ethernet).

Error recovery and flow control may be realized in connection-oriented mode.



The network layer builds the so-called "packet". Layer 3 transports the packets between the different networks. Therefore layer 3 needs structured and routable addresses to find the right networks. IP is the most important Layer 3 protocol today (IPv4 has a structured 4 byte address). The OSI Connectionless Network Protocol (CLNP) is another example for a layer-3 protocol but it is not so widely used today, except some Telcos and Carriers use it for internal purposes. IPX has been developed by Novell in order to extend Novell networks over different data-link layer worlds. Q.931 is the ISDN layer 3 carried over the D-channel and is used for signaling purposes. Basically Q.931 conveys the telephone numbers and other service parameters. The classical packet-switched WAN standard X.25 actually specifies only the layer 3 of this technology and is used to set up a number of virtual calls over an asynchronous link layer (LAPB).



The transport layer is necessary to build a logical connection to the application in order to send data in so-called "segments". With the help of port numbers (by TCP and UDP), a layer 4 protocol guarantees the transport of the segments to the right application. These port numbers are called T-SAPs in the OSI world. The transport layer optionally takes care about flow control, reliable transmission between end systems, and is most important for QoS capabilities. Flow control requires connection oriented mode.

Session Layer

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

- **Provides a user-oriented connection service**
  - ***Synchronization Points***
- **Little capabilities, usually not implemented or part of application layer**
  - **Telnet: GA and SYNCH**
  - **FTP: re-get allows to continue an interrupted download**
  - **ISO 8327 Session Protocol**

The Session Layer coordinates and controls dialogue between different end systems. This layer is only seldom or sparsely implemented. For example a Telnet server gives the sending permission to the Telnet client via a Go Ahead (GA) sequence. Using the BRK-Key, a SYNCH sequence is triggered and the server must synchronize with the client by flushing the buffered stream. FTP keeps track of the data blocks transmitted and is able to continue an interrupted session from this checkpoint on.

Session protocols are important with telephony applications such as H.323 which employs H.225 to establish sessions. Another example is the IETF Session Initiation Protocol (SIP). The ISO 8327 is an OSI basic connection oriented session protocol specification.

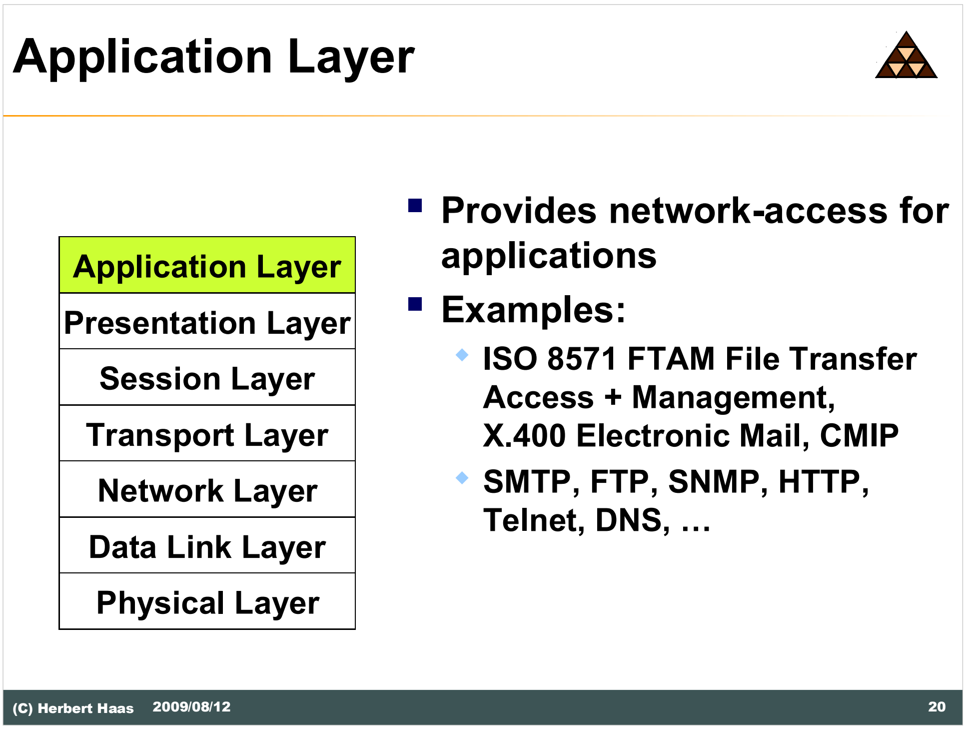
Presentation Layer

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

- **Specifies the data representation format for the application**
- **Examples:**
  - **MIME (part of L7) and UUENCODING (part of L7)**
  - **ISO: ASN.1 and BER**

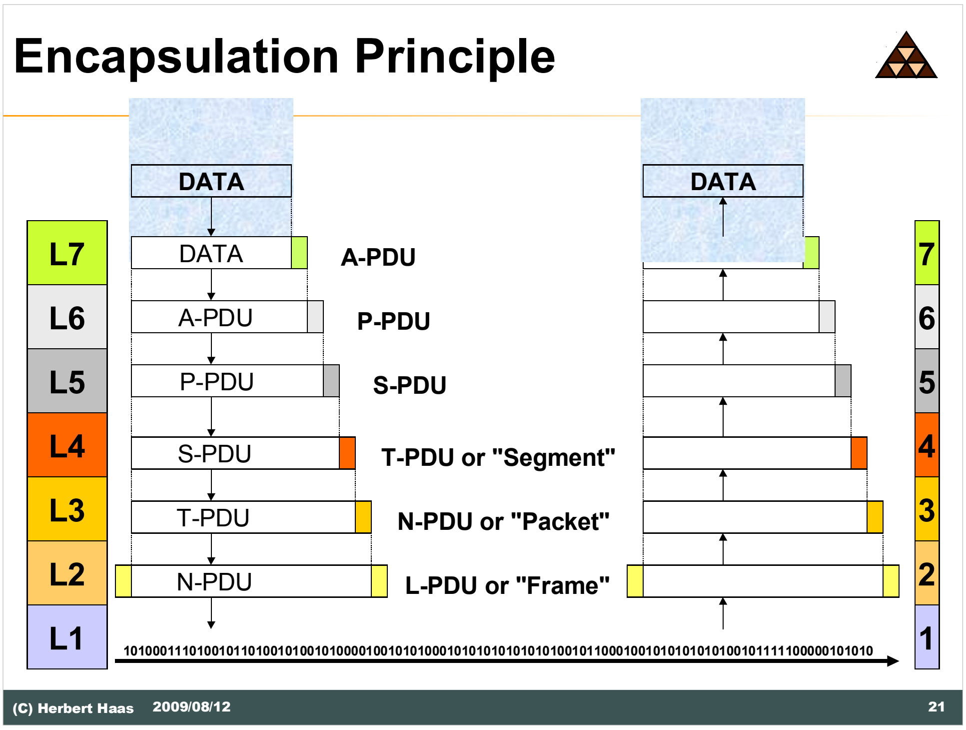
The layer 6 is responsible for common language between end systems. The presentation layer specifies the "meaning" of the data and how each byte should be interpreted.

In the Internet the presentation layer uses ASCII coding and the meaning of the data is specified by a so-called "Multipurpose Internet Mail Extension" (MIME) header. MIME is used by SMTP (Email) and HTTP (Web browsing) for example. UUENCODING is one example of how to transform 8-bit-bytes into 7-bit-bytes and it is typically used with Internet Mail attachments. The ISO/OSI world generally uses the "Abstract Syntax Notation Language Number One" (ASN.1) as common presentation layer. This language is used to specify data structures and contents. On the wire the data is transmitted using the "Basic Encoding Rules" (BER).



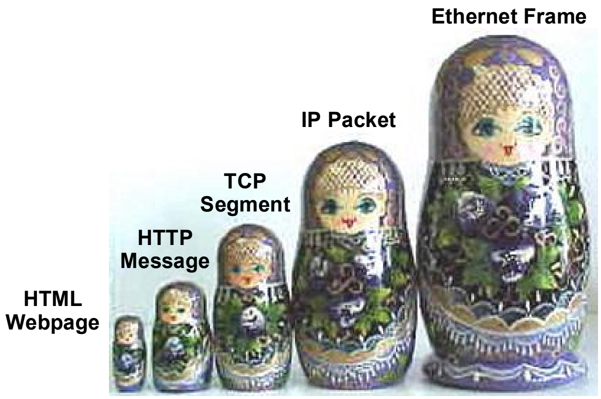
The Application layer supports user with common network applications. For example: file transfer or virtual terminals. Layer 7 also supports basic network procedures in order to implement distributed applications (e.g. transaction systems). Note that the application layer is not identical with the application! The application itself "sits" upon the application layer and uses the service primitives provided by the application layer to access the network.

Application layer protocols either use "inline" or "inband" control sequences (as it is used with Telnet), where control bytes are mixed with the data stream, or it might use a predefined frame structure, consisting of header and body. Another method is to open a dedicated logical control connection only to exchange control information (as it is used with FTP).



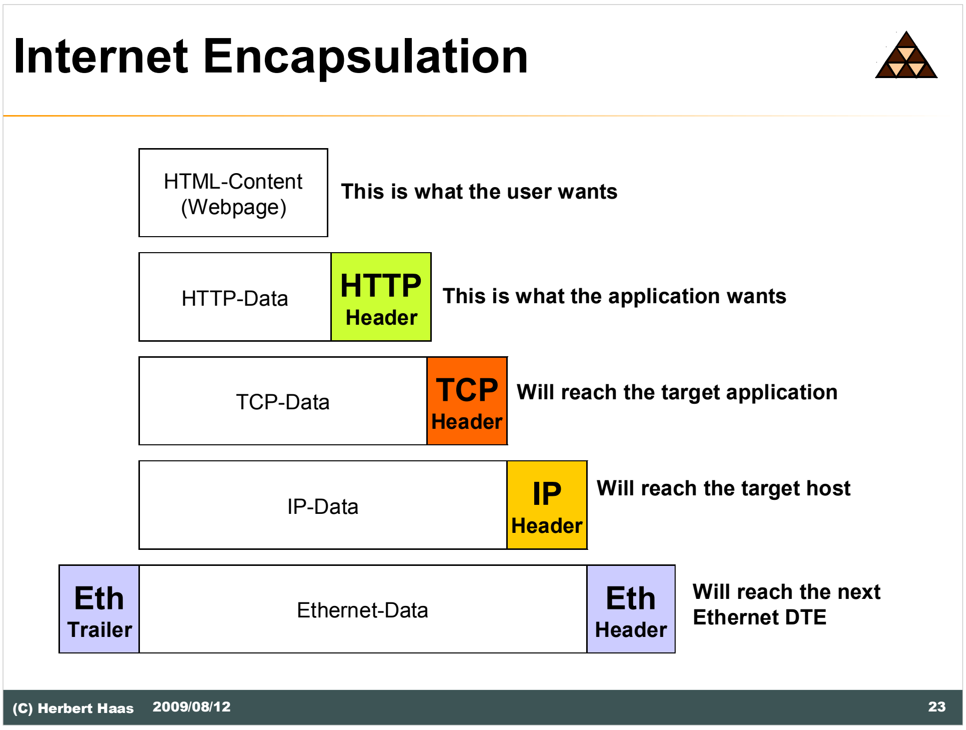
The data moves through all 7 layers. Every layer add his own header. The data with layer 4,5,6 and 7 header is called “segment”. A segment plus layer 3 header is called “packet”. The so called “frame” (data plus six headers) will be transport over layer 1 to the destination system. Then the frame will moves through all 7 layers again, and in each station a header will be removed.

Practical Encapsulation



The idea of encapsulation is fundamental in the data communication world. Adjacent layers encapsulate or decapsulate information by adding/removing additional "overheads" or "headers" in order to implement layer-specific functionalities. The whole process can be regarded as Matroschka-puppet principle.

In our example let's suppose a webserver sends a webpage (HTML code) to a client. The webpage is carried via the Hyper Text Transfer Protocol (HTTP) which provides for error and status messages, encoding styles and other things. The HTTP header and body is carried via TCP segments, which are sent via IP packets. On some links in-between, the IP packets might be carried inside Ethernet frames.



In our example let's suppose a webserver sends a webpage (HTML code) to a client. The webpage is carried via the Hyper Text Transfer Protocol (HTTP) which provides for error and status messages, encoding styles and other things. The HTTP header and body is carried via TCP segments, which are sent via IP packets. On some links in-between, the IP packets might be carried inside Ethernet frames.

OSI Speak (1)

- **Entities**
  - **Anything capable of sending or receiving information**
- **System**
  - **Physically distinct object which contains one or more entities**
- **Protocol**
  - **Set of rules governing the exchange of data between two entities**

Entities:

Any hardware or software module that acts upon a single layer is called an "entity". Several entities exist peer to peer within a given layer and are capable to communicate which each other. This type of communication is referred as "horizontal" communication -- this is actually what we mean when we talk about a "protocol".

System:

Several entities make up a "system". For example a PC is a "system" because it consists of the entities Ethernet PHY entity, MAC entity, LLC entitiy, IP entity, TCP entity, and several L7 entities. A system is merely a term that reflects the physically separation of groups of entities.

Protocol:

We already described the meaning of protocol above together with the definition of a entity, but a protocol can be explained more simple: A protocol is a set of rules that are necessary to exchange data in an ordered and unmistakable way.

OSI Speak (2)

- **Layer**
  - **A set of entities**
- **Interface**
  - **Boundary between two layers**
- **Service Access Point (SAP)**
  - **Virtual port where services are passed through**

Layer:

A "layer" in the OSI jargon is a set of entities--but do not confuse layers with systems! The entities of a layer reside on the same hierarchy level and a single layer comprises several systems. On the other hand a system comprises several layers but typically only one (or a limited number) of entities are available on each layer of a system. For example: In order to communicate in the Internet, all devices must support layer 3 (the IP layer). That is, each system must provide at least one IP-entity.

Interface:

An "interface" is simply the logical boundary between two layers. Note that interfaces are typically not physically visible because they represent the boundary between two layers at a whole. The local representation of an interface is called a "Service Access Point" or SAP. The Service Access Point is one of the most frequently used terms in data communication and simply reflects the piece of hardware or software that acts as an interface between two layers. The previously OSI-interface is meant globally, while the SAP has local meaning, i. e. at one system. A SAP is a practical term, in some technologies such as IEEE 802.2 it is just a field in the header indicating the destination and source layer. If you use an Ethernet NIC with an AUI interface, than this electrical interface can be also considered a SAP because "service primitives" are passed through this interface. Service Primitives are explained below...

Service Access Point:

An "Interface Data Unit" (IDU) is practically spoken the piece of data that is passed through a SAP to the next layer's entity. It contains ICI and SDU which is described below. When an IDU is passed through a SAP to the next layer, this layer extracts and processes the Interface Control Information (ICI).

OSI Speak (3)

- **Interface Data Unit (IDU)**
  - **Data unit for vertical communication (between adjacent layers of same system)**
- **Protocol Data Unit (PDU)**
  - **Data unit for horizontal communication (between same layers of peering systems)**

Interface Data Unit:

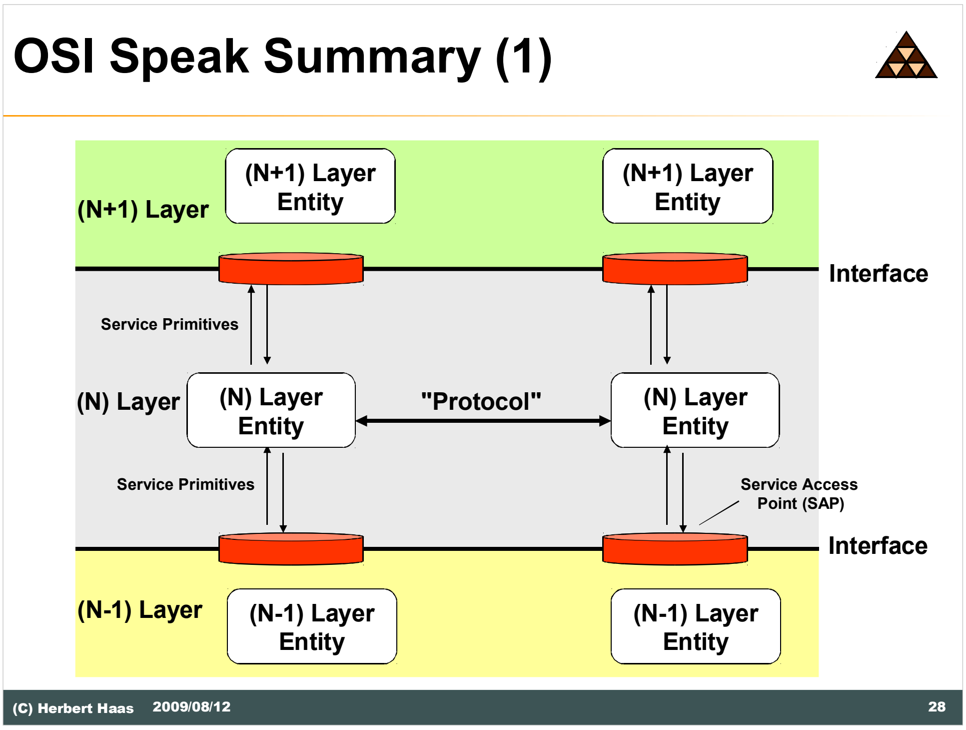
An "Interface Data Unit" (IDU) is practically spoken the piece of data that is passed through a SAP to the next layer's entity. It contains ICI and SDU which is described below. When an IDU is passed through a SAP to the next layer, this layer extracts and processes the Interface Control Information (ICI). Note that data is passed through a SAP using "service primitives". Service primitives are functions that are implementation specific (for example an API) and are used to pass data from one layer to another on the same system. These service primitives actually pass on these IDUs.

Protocol Data Unit:

The SDU actually represents the payload plus headers for upper layers. The SDU is transported horizontally with an header used at this layer. Both SDU and Header is called a "Protocol Data Unit" (PDU). The PDU is the most often used term of all these terms mentioned here. At least you should remember the PDU.

OSI Speak (4)

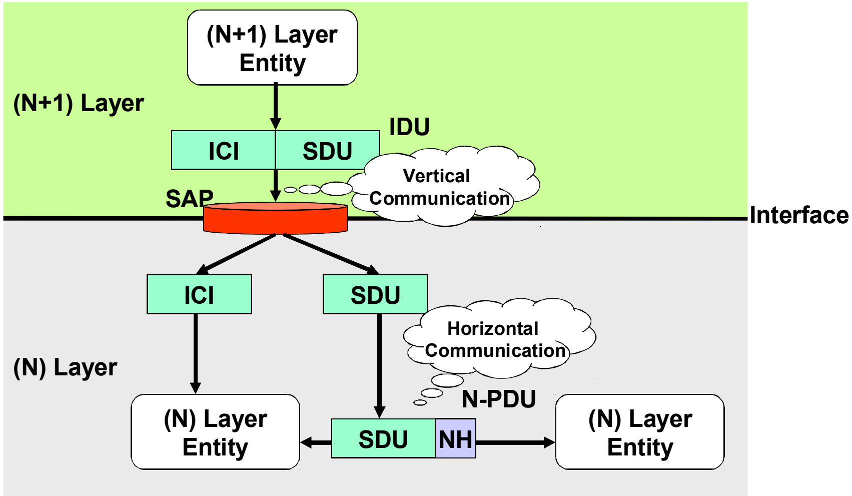
- Interface Control Information (ICI)
  - Part of IDU
  - Destined for entity in target-layer
- Service Data Unit (SDU)
  - Part of IDU
  - Destined for further communication
  - Contains actual data ;-)



The ISO/OSI model defines four service primitives: request, indication, response and confirm.

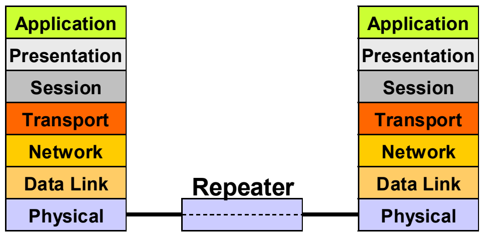
Note that the service primitives are only used for vertical communication.

OSI Speak Summary (2)



Layer 1 Devices

- Adapts to different physical interfaces
- Amplifies and/or refreshes the physical signal
- No intelligence
- Repeater, Hub, NT1



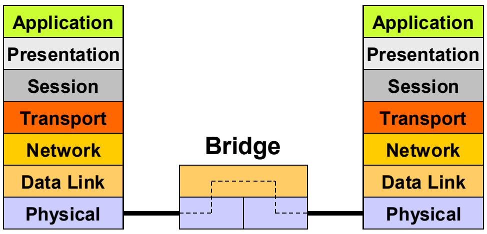
(C) Herbert Haas 2009/08/12 30

To connect different system with each other we need special devices. If you want to connect two systems only per physical layer you need a so called “hub” or “repeater”.

This kind of devices are not intelligence and only used to amplifies or refresh the physical signal, or to connect systems with different physical interfaces.

Layer 2 Devices

- Filter/Forwards frames according Link Layer Address
- Incorporates Layer 1-2
- LAN-Bridge ("Switch")

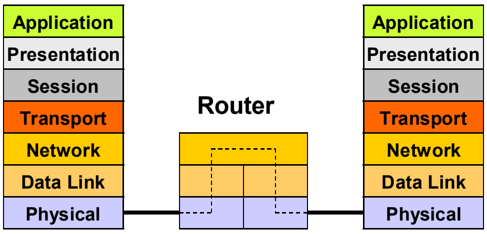


A so called “bridge” or “switch” is a device to connect systems per data link layer. This kind of devices determine the physical layer and can forward datagram's according the link layer address. For example: MAC address with Ethernet. Note that a bridge utilizes two or more physical layer entities (NICs) that is a bridge is able to convert encodings and signal-rates.

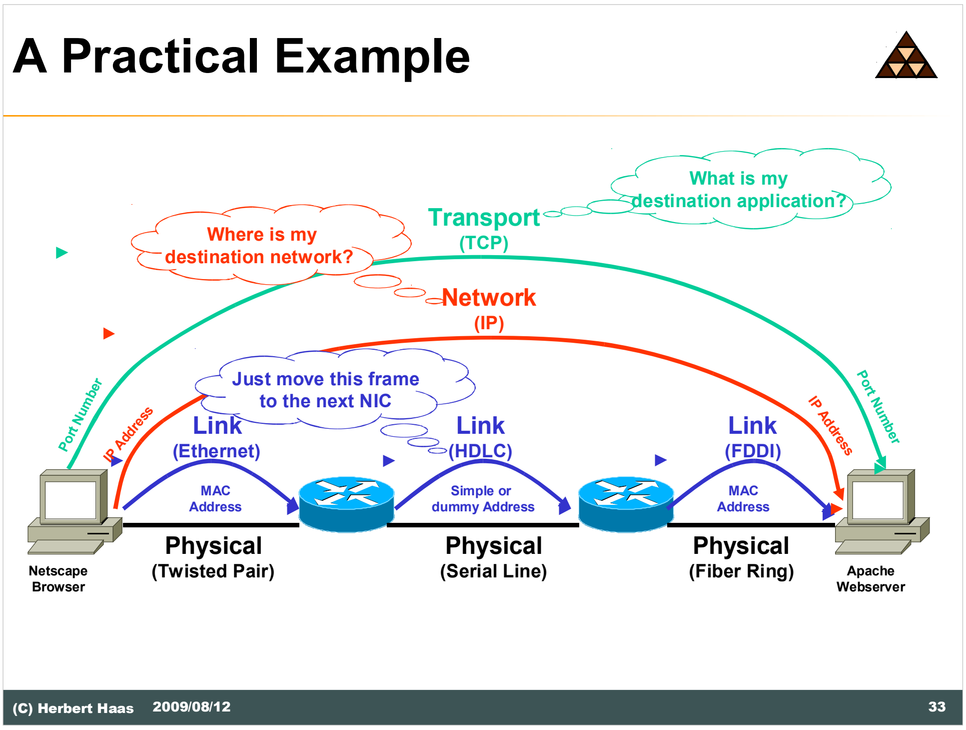
Note the difference between “bridge” and “switch”: A bridge is implemented in software, whereas a switch is built in hardware. Today only switches are used, because they are much faster.

Layer 3 Devices

- "Packet Switch" or "Intermediate System"
- Forwards packets to other ***networks*** according ***structured*** address
- Terminates Links
- Router, WAN-Switch

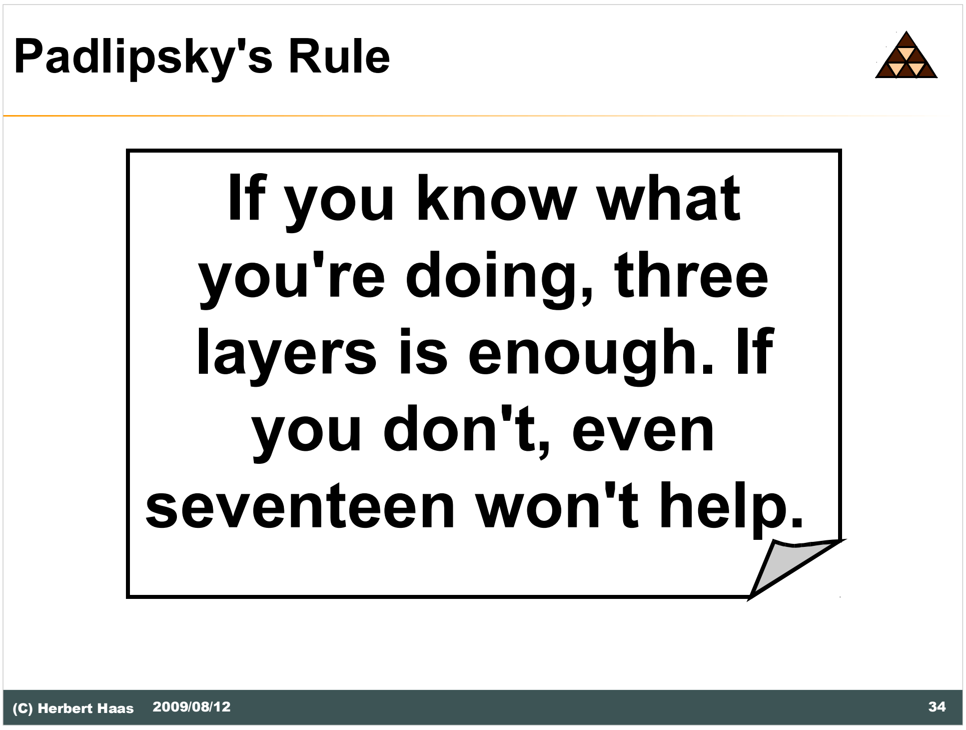


The most important device in the Internet is the so called "router". A router consists of several layer 1 and layer 2 entities and a single layer 3 entity, thus it can forward packets to other networks according structured addresses (remember IP-Addresses). By terminating layer 1 and 2 a router is able to connect total different network technologies with each other. For example: on one side there is Ethernet on the other side ATM.

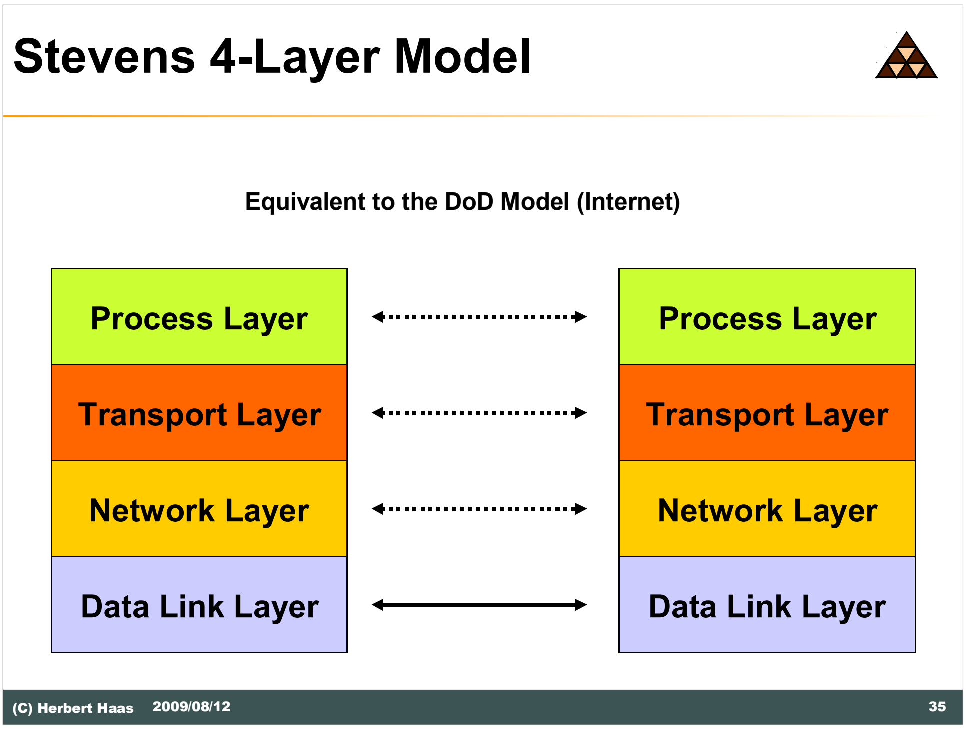


In the picture above you see a good example in which "symbolic" way the different layers talk with each other. The link layer only searches for the right NIC address. IP only wants to the destination network, and TCP is the protocol to communicate between applications. Most importantly, notice that packets are sent over different link layer technologies such as Ethernet, HDLC, or FDDI. Exactly this is the reason why a common network layer is needed to allow communication over different "networks" (=links).

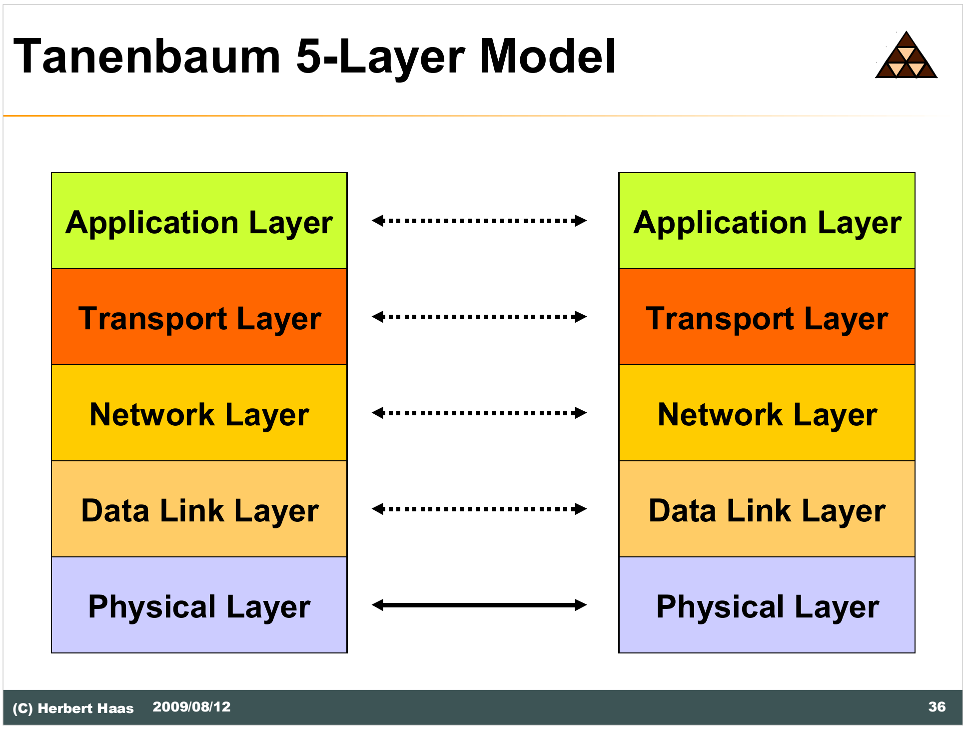
Don't be confused about the different usages of the term "network". People say "network" and mean "bunch of devices interconnected with each other". To be more exact, a network is identified by a unique network identifier, such as the network-ID of the IP-address. Since a contiguous link layer implementation (such as an Ethernet LAN) can have assigned a single IP net-ID, each link can be regarded as network.



Until now we discussed the famous OSI seven layer reference model, but real implementations typically consist of a subset of this 7-layer model. On the one hand, not all OSI layers are necessary in real-world applications, on the other hand, many important technologies had been created before the OSI standard.



The picture above shows the W. Stevens 4 layer model which is used also in the Internet. The Internet layer model is also called "Department of Defense" (DoD) model.



The famous computer scientist Andrew S. Tanenbaum defined a more practical approach utilizing five layers. Other than the DoD or Stevens 4-layer model the physical specifications are defined in a separate layer.

Summary

- Network layers ensures interoperability and eases standardization
- ISO/OSI 7 layer model is an important reference model
- Practical technologies employ a different layer set, but it's always possible to refer to OSI

The Internet perspective is implement it, make it work well, then write it down.

The OSI perspective is to agree on it, write it down, circulate it a lot and now we'll see if anyone can implement it after it's an international standard and every vendor in the world is committed to it.

One of those processes is backwards, and I don't think it takes a Lucasian professor of physics at Oxford to figure out which.

Marshall Rose, "The Pied Piper of OSI"

Quiz

- Explain layer-2 capabilities!
- What could be the task of a layer-4 device ?
- What is a "gateway"?
- How does the (N) layer tell (N+1) layer that it has data to hand over ?
- Why have OSI protocols not been successful on market ?

Hints

- Q1: Framing, Protection, Access,...
- Q2: Layer 4 device might deal with QoS, sequencing and flow control
- Q3: According to OSI a layer 1-7 device, according to IETF a router.
- Q4: Using Service Primitives (Indicate)
- Q5: OSI is too complex and general, several fields in headers might have variable length, sometimes ignores byte- and word-delineation, ...