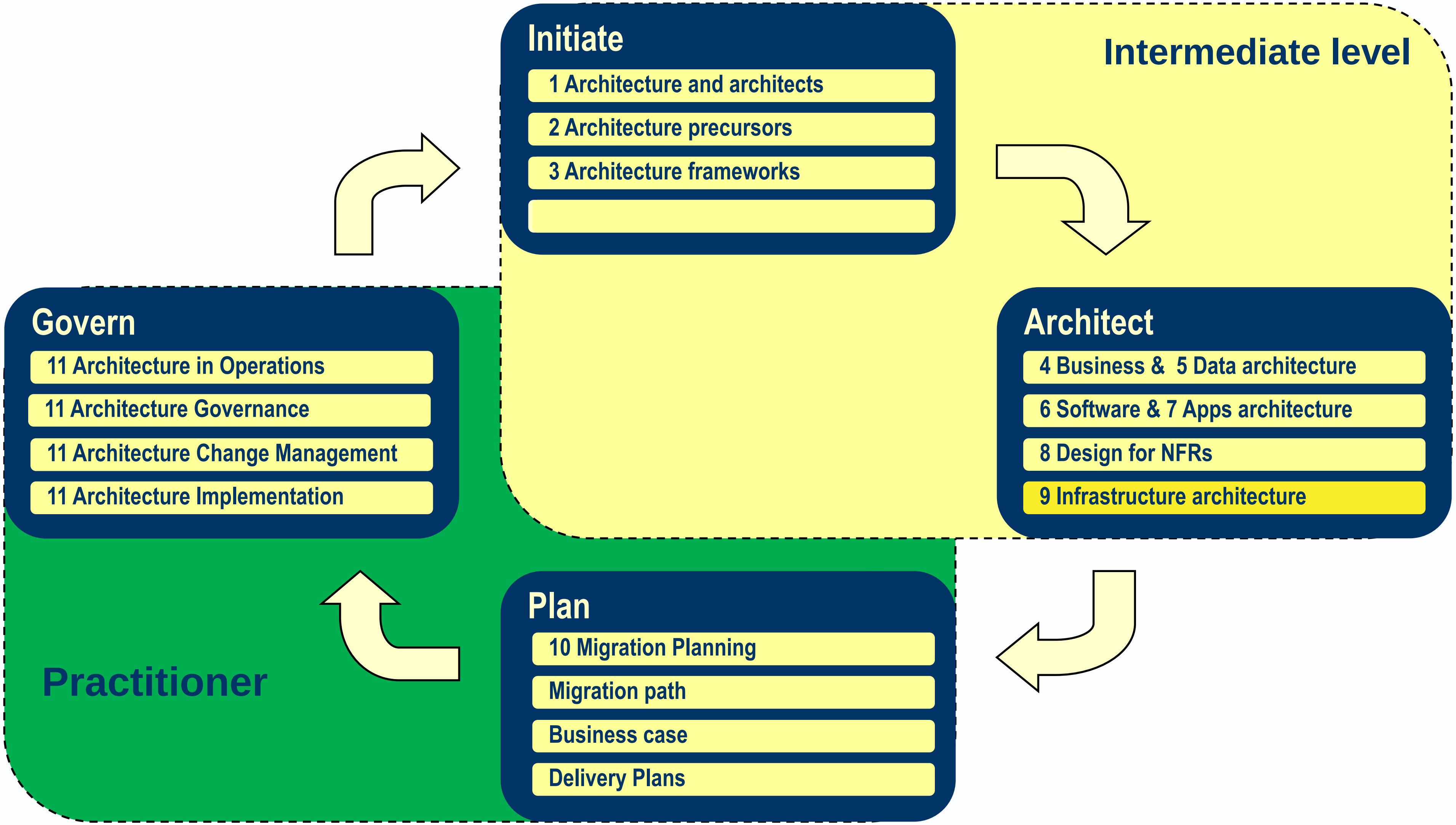
Avancier

Avancier Reference Model

Infrastructure Architecture (ESA 9)

9. Infrastructure architecture



Initiate

1 Architecture and architects

2 Architecture precursors

3 Architecture frameworks

Intermediate level

Architect

4 Business & 5 Data architecture

6 Software & 7 Apps architecture

8 Design for NFRs

9 Infrastructure architecture

Plan

10 Migration Planning

Migration path

Business case

Delivery Plans

Govern

11 Architecture in Operations

11 Architecture Governance

11 Architecture Change Management

11 Architecture Implementation

Practitioner

9: Infrastructure domain/view/layer

9.1: Foundation (rarely examined)

- Fig. 9.1 Base infrastructure architecture concepts

- **Platform service** [a service] that can be requested of a technology component by an application component or another technology component.
- E.g. transaction roll back, or user authentication.

- **Platform interface** [an interface] a collection of platform services accessible by applications; it identifies services, may provide access to them, and hides what performs them.
- It may be defined in the form of an API, or in a specific programming language.

- **Platform application** [a component] of generic infrastructure software.
- It is specified logically by the platform services it provides, and/or physically as a vendor/technology specific product that can be hired or bought.

- Examples: operating system, device driver, web server, data server, windowing system and message broker; also programming language and compiler.
- It may serve general non-functional requirements: e.g. identity management, data replication etc.

- **Node:**
- [a component] a computational resource upon which artifacts may be deployed for execution.
- Nodes can be interconnected through communication paths to define a network structure or topology.
- Nodes can be virtual or physical servers.
- Nodes can be nested.

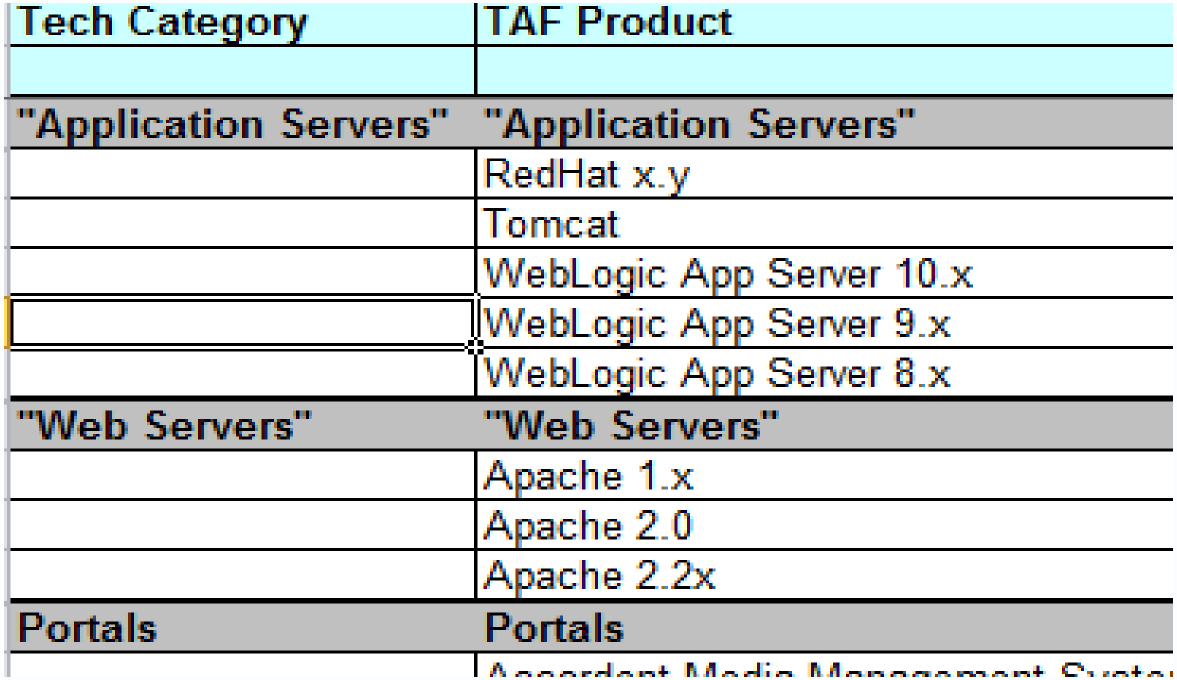
- **Communication network**
- [a structural view] of communication paths that enables computers and/or electro-mechanical devices to send and receive data.

9.2 Enterprise technology rationalisation

- **Application / technology matrix** [an artefact] that maps business applications to the platform applications and/or nodes they depend on.

Technology portfolio catalogue

- [an artefact] that lists platform component types in a baseline or target architecture.
- It is usually arranged under the hierarchical structure of an enterprise technology classification.



Tech Category	TAF Product
"Application Servers"	"Application Servers"
	RedHat x.y
	Tomcat
	WebLogic App Server 10.x
	WebLogic App Server 9.x
	WebLogic App Server 8.x
"Web Servers"	"Web Servers"
	Apache 1.x
	Apache 2.0
	Apache 2.2x
Portals	Portals
	Accordant Media Management Syste

ETC: Enterprise Technology Classification

- [a passive structure] for the organisation of a technology portfolio catalogue. E.g.
  - Client (user access) devices.
  - Generic user applications.
  - Operating systems.
  - Database management.
  - Middleware.
  - Software development.
  - Servers. Data storage.
  - Networks.
  - IT services management / operations.
  - Environment.
  - Security.

- **OS: Operating System** [a platform application] designed to enable programs to run on a computing device.
- (E.g. Windows, Windows Azure, Linux variants (SUSE & Red Hat), Unix variants (IBM AIX, HP UX, Oracle Solaris), IBM i (ex i5/OS, ex OS/400 on AS/400)).

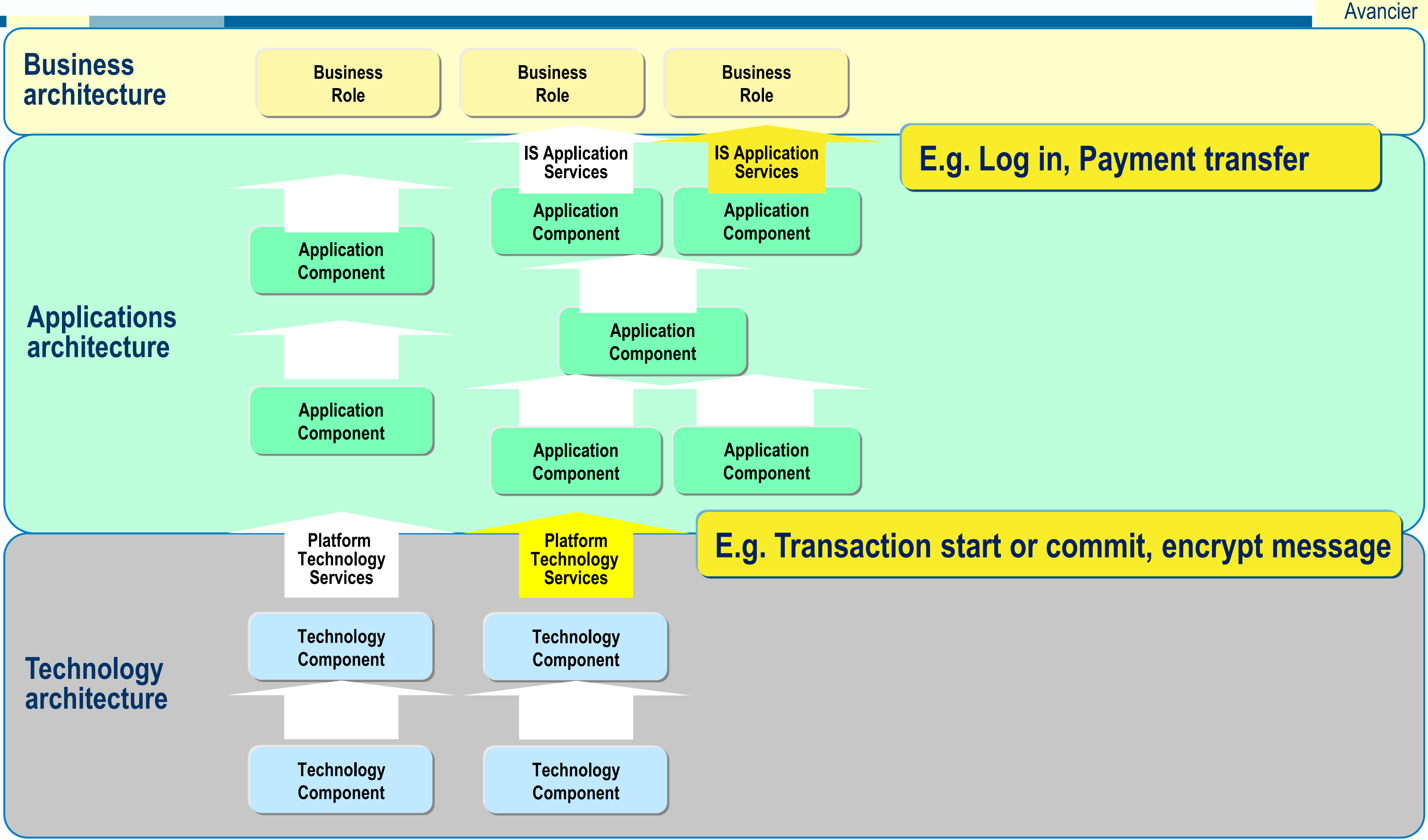
- **DBMS: Database Management System** [a platform application] designed to enable programs to store and retrieve persistent data.
- (E.g. DB2, SQL Server, Oracle, Sybase and Teradata.)

- **Middleware** [a platform application] designed to assist the interoperation of distributed applications components.
- (E.g. Message broker, Enterprise Service Bus, Transaction processing manager.)

TRM: Technical reference model

- [a passive structure] for organising the platform services provided by infrastructure technologies to applications.
- It may share its top-level structure with the ETC (above).
- It can provide a requirement specification for technology rationalisation.

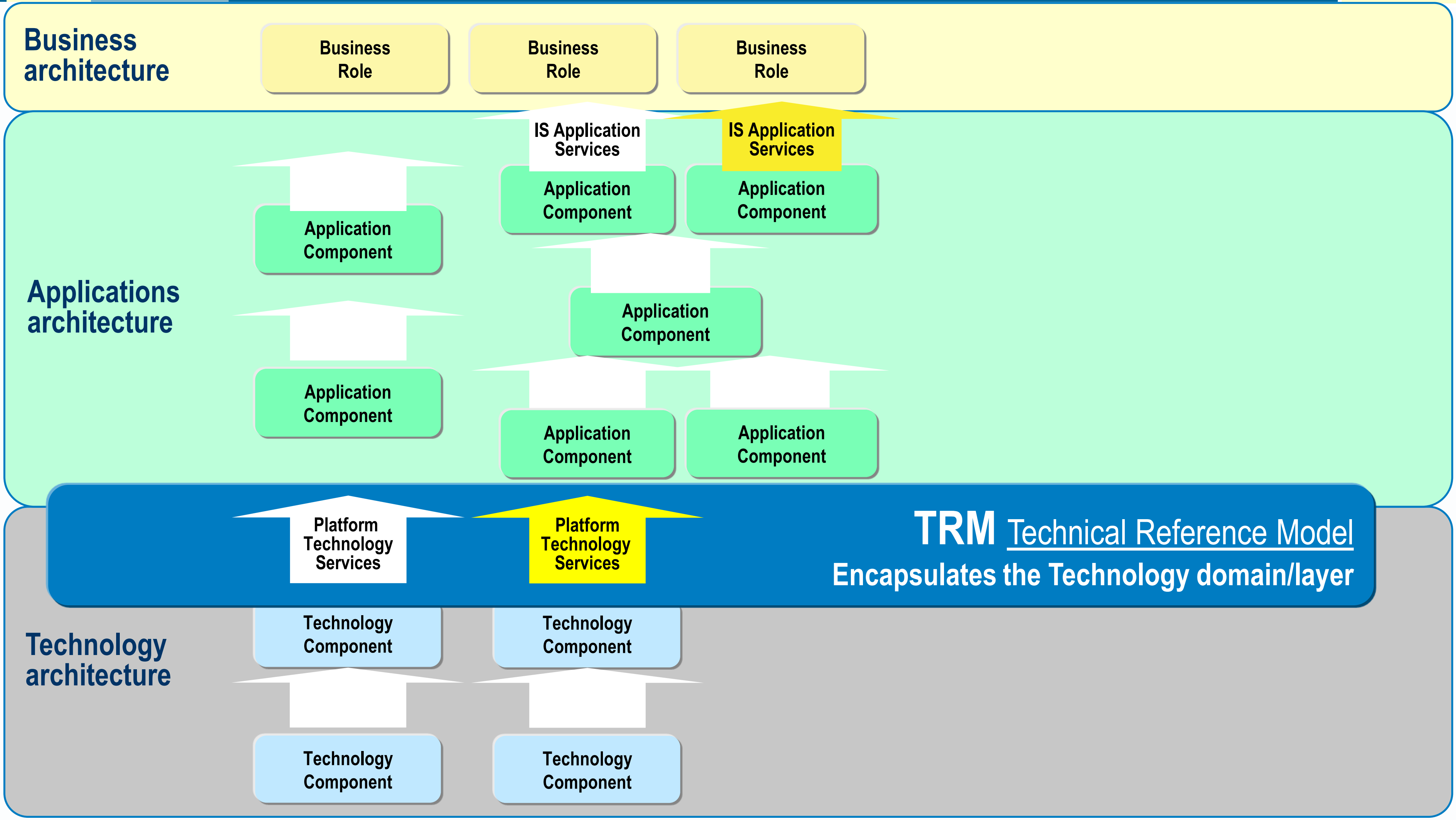
Two levels of service



E.g. Log in, Payment transfer

E.g. Transaction start or commit, encrypt message

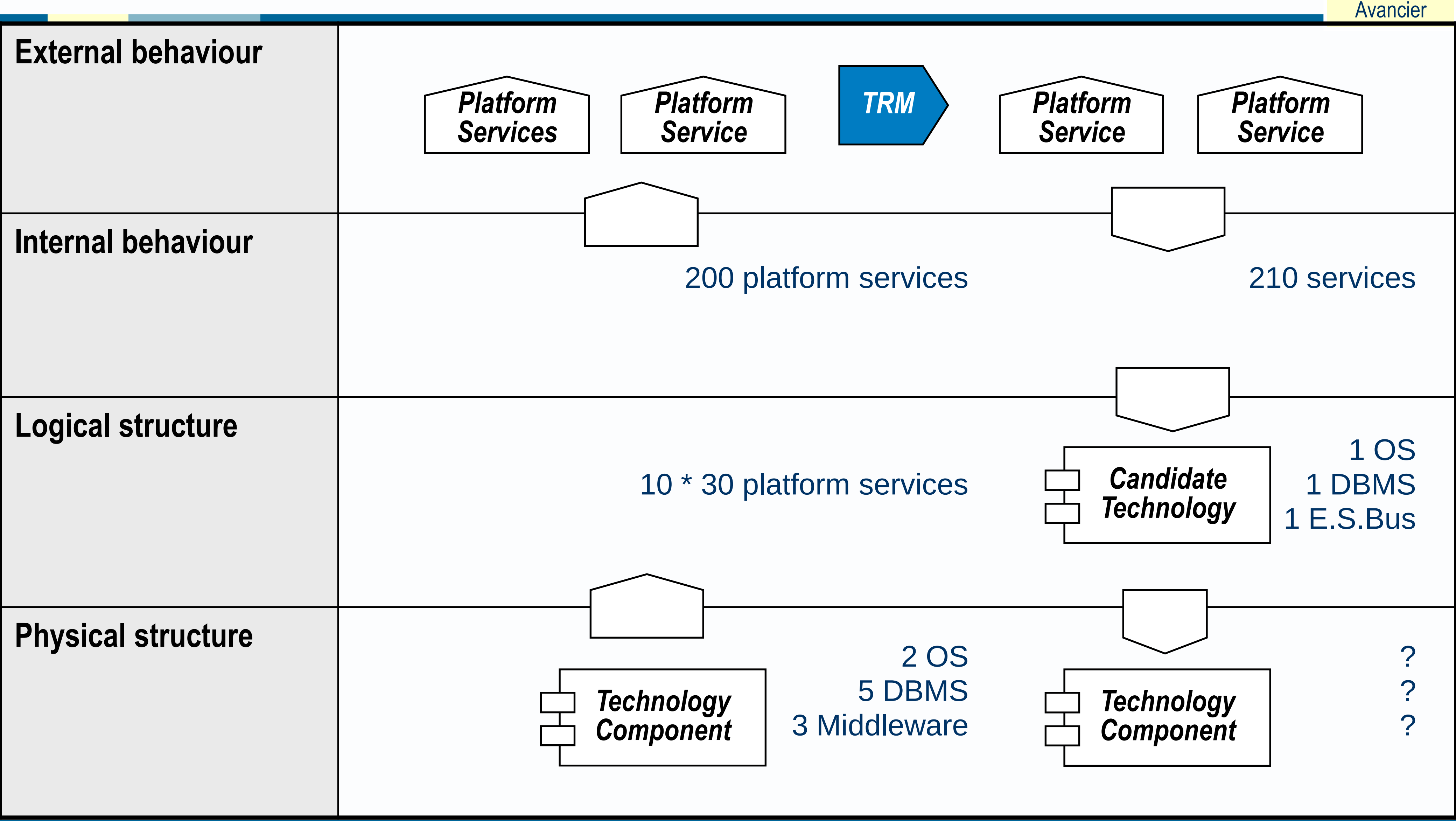
Using a Technical Reference Model to encapsulate infrastructure



Classify and catalog baseline technology services (as inTOGAF’s TRM)

User Interface Services	Transaction Processing Services	Operating System Services	Software Engineering Services
Graphical Client/Server services	Starting a transaction	Kernel Operations	Programming Language services
Display Objects services	Co-ordination of recoverable resources in a transaction	Command Interpreter and Utility services	Object Code Linking services
Window Management services	Committing or rolling back transactions	Batch Processing services	CASE Environment and Tools services
Dialogue Support services	Controlling timeouts on transactions	File and Directory Synchronization	Graphical User Interface (GUI) Building services
Printing services	Chaining transactions together		Scripting Language services
Computer-Based Training and Online Help services	Monitoring transaction status		Language Binding services
Character-Based services			Run-Time Environment services
			Application Binary Interface services
Graphics and Imaging Services	**Data Management Services**	**Network Services**	**OO Provision of Services**
Graphics services	Data Dictionary/Repository services	Electronic Mail services (send, receive…)	Object Request Broker (ORB) services
Graphical Object Management services	Database Management System (DBMS) services	Distributed Data services	Implementation Repository services
Drawing services	OO Database Management System (OODBMS) services	Distributed File services	Installation and Activation services
Imaging functions	File Management services	Distributed Name services	Interface Repository services
	Query Processing functions	Distributed Time services	Replication services
International Operation Services	Screen Generation functions	Remote Process (Access) services	Common Object services
Character Sets and Data Representation services	Report Generation functions	Remote Print Spooling and Output Distribution services	Change Management services
Cultural Convention services	Networking/Concurrent Access functions	Enhanced Telephony functions	Collections services
Local Language Support services	Warehousing functions	Shared Screen functions	Concurrency Control services
		Video-Conferencing functions	Data Interchange services
		Broadcast functions	Event Management services
		Mailing List functions	Externalization services
			Licensing services
Data interchange services	**Location and Directory Services**	**System and Network Management Services**	Lifecycle services
Document Generic Data Typing and Conversion services	Directory services	User Management services	Naming services
Graphics Data Interchange services	Special-Purpose Naming services	Configuration Management (CM) services	Persistent Object services
Specialized Data Interchange services	Service Location services	Performance Management services	Properties services
Electronic Data Interchange services	Registration services	Availability and Fault Management services	Query services
Fax services	Filtering services	Accounting Management services	Relationship services
Raw Graphics Interface functions	Accounting services	Security Management services	Security services
Text Processing functions		Print Management services	Start-Up services
Document Processing functions	**Security Services**	Network Management services	Time services
Publishing functions	System Entry Control services	Backup and Restore services	Trading services
Video Processing functions	Security Management services	Online Disk Management services	
Audio Processing functions	Audit services	License Management services	
Media Synchronization functions	Access Control services	Capacity Management services	
Multimedia Processing functions	Non-Repudiation services	Software Installation services	
Information Presentation and Distribution functions	Trusted Recovery services	Trouble Ticketing services	
Hypertext functions	Encryption services		
	Trusted Communication services		

Overview of the rationalisation approach



External behaviour

Platform Services

Platform Service

TRM

Platform Service

Platform Service

Internal behaviour

200 platform services

210 services

Logical structure

10 * 30 platform services

Candidate Technology

1 OS
1 DBMS
1 E.S.Bus

Physical structure

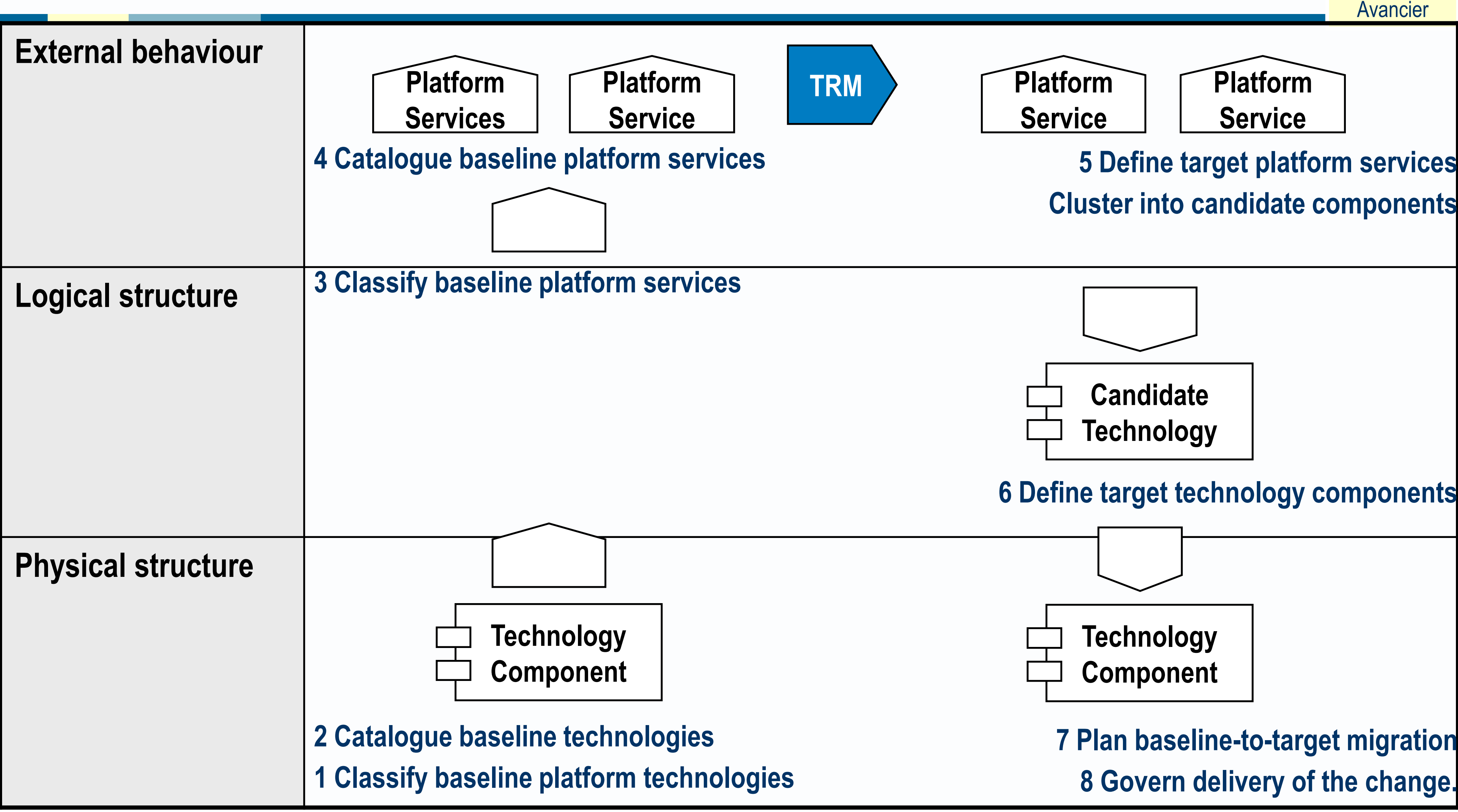
Technology Component

2 OS
5 DBMS
3 Middleware

Technology Component

?
?
?

Technology architecture rationalisation (BCS RM style)



External behaviour

Platform Services

Platform Service

TRM

Platform Service

Platform Service

4 Catalogue baseline platform services

5 Define target platform services

Cluster into candidate components

Logical structure

3 Classify baseline platform services

Candidate Technology

6 Define target technology components

Physical structure

Technology Component

Technology Component

2 Catalogue baseline technologies

1 Classify baseline platform technologies

7 Plan baseline-to-target migration

8 Govern delivery of the change.

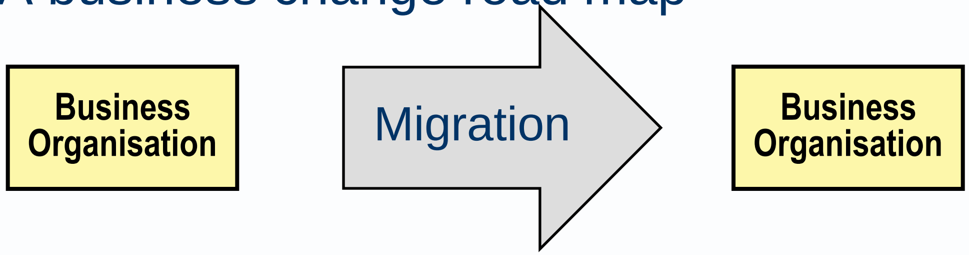
Technology rationalisation

► [a technique] for studying the services provided by a baseline technology infrastructure and defining a de-duplicated target architecture.

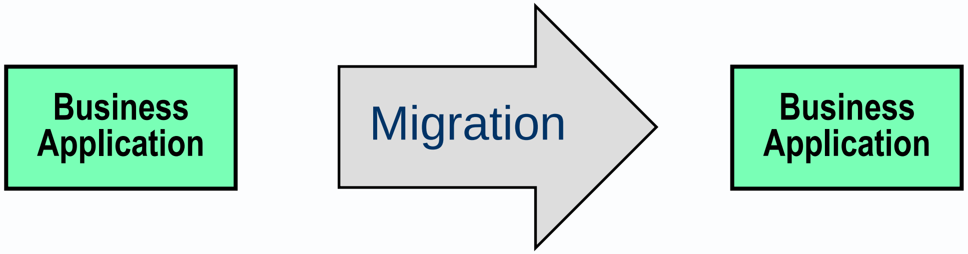
1. Understand the baseline
   - Classify and catalog baseline technologies (see ETC)
   - Classify and catalog baseline technology services (see TRM)
2. Review the context and motivations
3. Design the target
   - Define target technology services
   - Define target technology components
4. Plan baseline-to-target migration
5. Govern delivery of the change.

Review and coordinate road maps

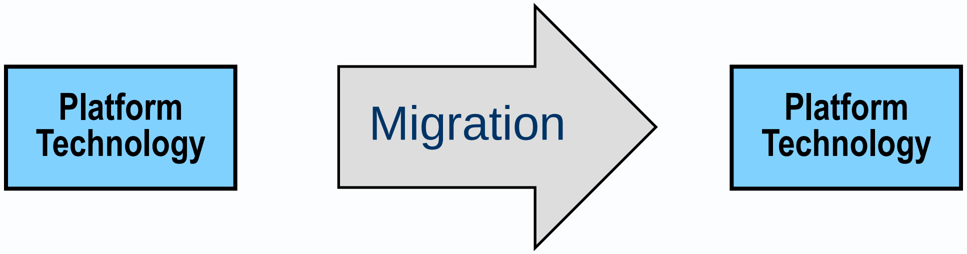
- A business change road map



- An application road map



- A platform technology road map



App	2016	2017	2018	2019
ERP 1	Ignore	Ignore	Remove	
ERP 2			Deploy	Improve
CRM 1	Remove			
CRM 2	Deploy	Improve	Prize	Prize
Billing	Prize	Prize	Prize	Prize
DW/BI	Improve	Improve	Improve	Improve
Timesheet	Ignore	Rewrite	Prize	Prize

- **Virtual machine** [a platform application] of software that enables application programs to run above – decoupled from - the underlying operating system and/or hardware processor. It enables applications to be moved between different operating systems and/or processors. It enables server consolidation.
-
- **Server consolidation** [a work process] a programme of work to deploy currently deployed applications to fewer servers, usually involving virtualisation.

In parallel, automate the management and optimisation of the infrastructure services based on well-defined policies.

9.3: Solution technology elements and definition

- **Device** [a node] with processing capability upon which artifacts may be deployed for execution. E.g. application server, client workstation, mobile device, embedded device. Devices can be nested.
- **Execution environment** [a node] on which components can be deployed in the form of executable artifacts. E.g. OS, workflow engine, database system, and J2EE container. Execution environment instances are assigned to device instances. Execution environments can be nested (e.g. database nested in an operating system).
- **Communication path:** an association or channel between two nodes, through which they are able to exchange signals and messages.

Deployment

- **Deployable artifact:** a development deliverable (source file, script, executable, database table etc.) that is deployable to a node instance.
- It may be nested, so a component and its descriptor can deployed inside one artifact instance to a node instance.

- **Deployed artifact:** an artifact that has been deployed to one or more deployment targets.

- **Deployment:** the allocation of one artifact to one deployment target (defined at the type level or instance level).

Software deployment diagram [an artefact]

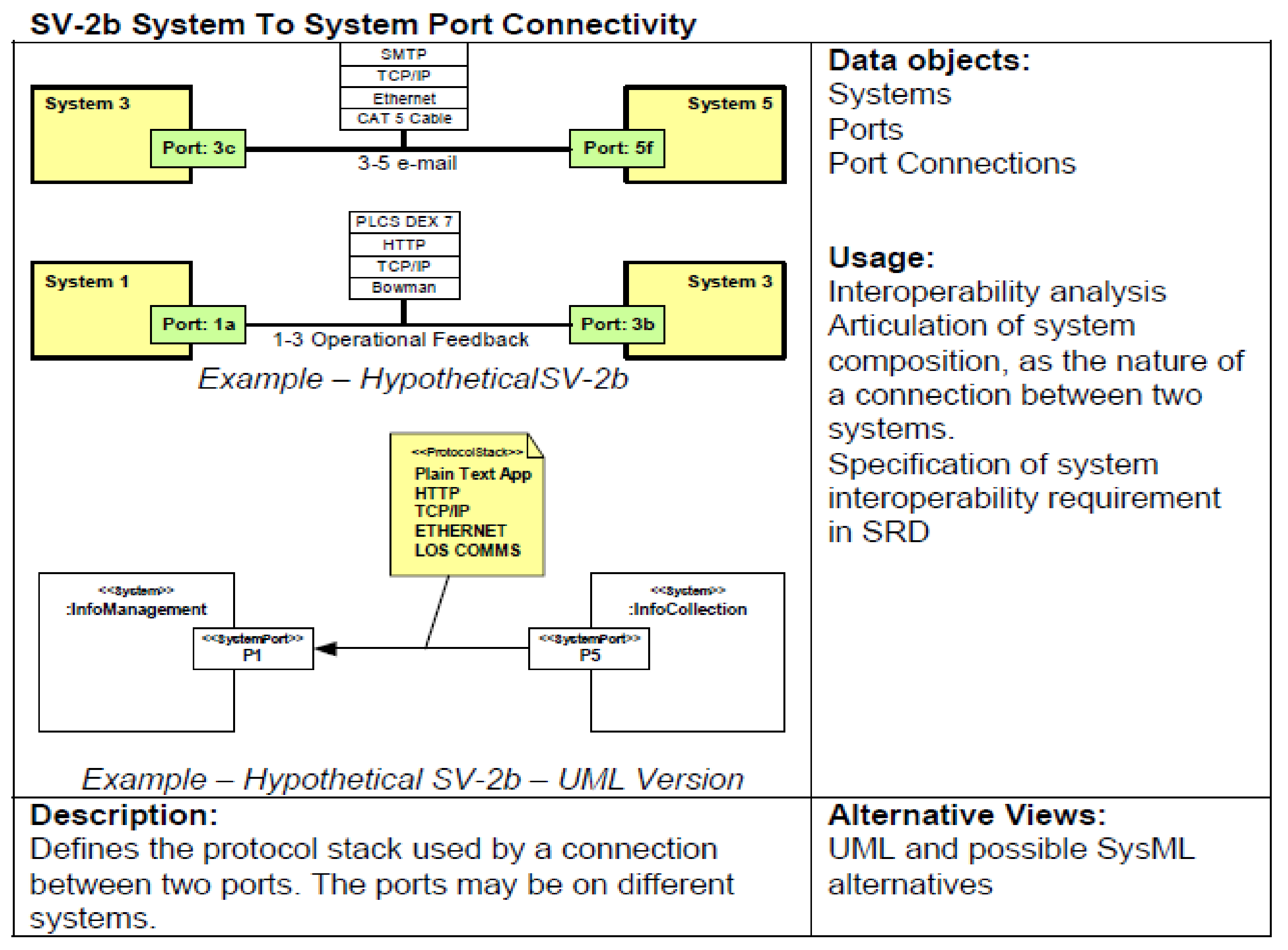
- that shows deployments of application and other software components to execution environments and nodes (virtual and/or physical).

Hardware configuration diagram [an artefact]

- that shows the devices and indicates where they are connected by communication paths.

Communications engineering diagram [an artefact]

- that shows devices, and is focused on detailing the network components, sometimes annotated with IP addresses.



SV-2b System To System Port Connectivity

Example – HypotheticalSV-2b

Example – Hypothetical SV-2b – UML Version

Data objects:
Systems
Ports
Port Connections

Usage:
Interoperability analysis
Articulation of system composition, as the nature of a connection between two systems.
Specification of system interoperability requirement in SRD

Description:
Defines the protocol stack used by a connection between two ports. The ports may be on different systems.

Alternative Views:
UML and possible SysML alternatives

Solution technology definition [a technique]

- a process to define the platform application environment(s) needed to support and run application(s).
- It should start by addressing show stoppers at the top and bottom of the technology stack.
- Is the end user able and willing to use the client-end device? Is data available from data servers when needed?
- It progresses from a logical applications architecture through progressively more physical views to hardware and network diagrams.

- It may proceed as follows:
  1. Identify the context and requirements for the platform technologies
  2. Establish baseline opportunities and constraints
  3. Define client nodes and data server or source nodes (show stoppers)
  4. Define intermediate web and app nodes.
  5. Map software components to nodes (with I/O protocols and connections)
  6. Map virtual nodes to physical nodes
  7. Define network(s) to connect the nodes
  8. Refine to handle non-functional requirements
  9. Define additional non-production environments
  10. Govern deployment and transition from development into operations.

9.4: Communication networks and protocols

Network scopes

- **PAN**: **Personal Area Network** [a communication network] typically carried or worn by a person. The reach of a wireless PAN varies from a few centimetres to a few meters.

- **LAN**: **Local Area Network** [a communication network] under the control of a local network administrator, usually within a building or closely connected buildings.

- **MAN**: **Metropolitan Area Network** [a communication network] optimized for a block of buildings, or an entire city, and likely to use leased lines.

- **WAN**: **Wide Area Network** [a communication network] that connects computers and networks over long distances, usually employs leased lines or the Internet.

VPN: Virtual Private Network [a communications network]

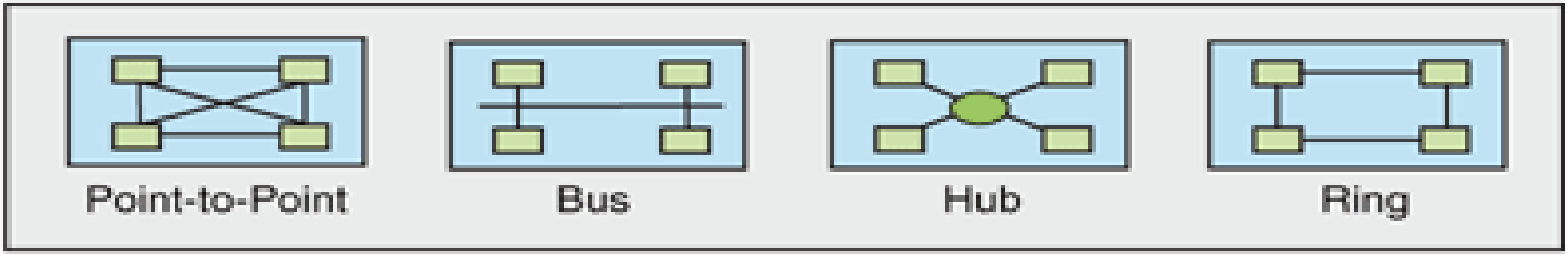
- in which communication between nodes is carried by connections within some larger network instead of by physical wires.
- Usually uses the Internet or other WAN but feels like a LAN.
- The data link-layer protocols of the virtual network are said to be tunnelled through the wider network.

Cloud computing:

- an architecture that features services provided by a service provider to a customer over a WAN.
- It is defined using contracts that hide what performs the remote services.
- The service provider may pool the necessary resources.

- **Software as a Service:** provision of use cases (e.g. order capture and payment validation) from a business application owned by a service provider; the customer owns only the data.
- **Platform as a Service:** provision of platform services (e.g. message delivery or transaction rollback) from a platform application owned by a service provider; the customer owns the business application as well as the data.
- **Infrastructure as a Service:** provision of basic computing technology services, processor speed and memory, by a remote service provider.

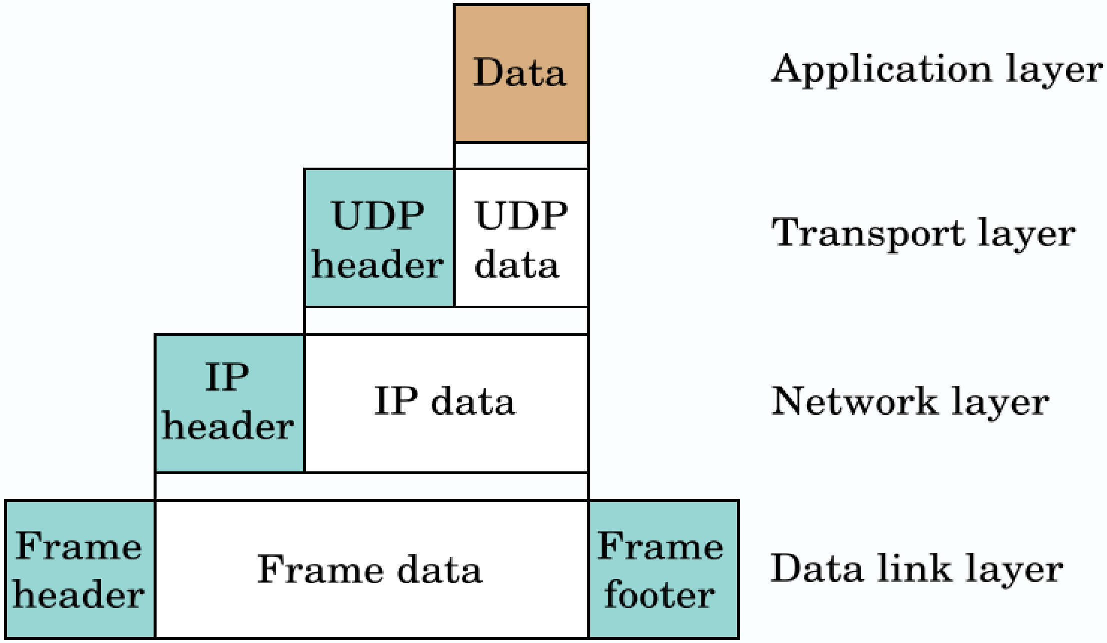
Topology

- [a pattern] for the shape of a network, or communication routes over it. A shape that connects nodes or constrains communications routes over a network.
- 

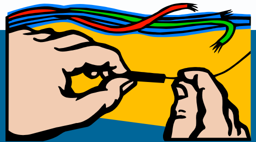
- **Point-to-point (aka mesh)** [a topology] in which one node sends a message directly to another node; other end-point nodes are unaware of this.
- **Bus** [a topology] in which each node listens to all messages sent by other nodes, and filters out unwanted ones.
- **Hub** [a topology] in which each node sends and receives messages via a central node.
- **Ring** [a topology] in which nodes pass a message around in a circular fashion until it arrives at the intended destination node.

Network layer [a view]

- a level in a hierarchy of communication layers, corresponding to layers of platform applications.

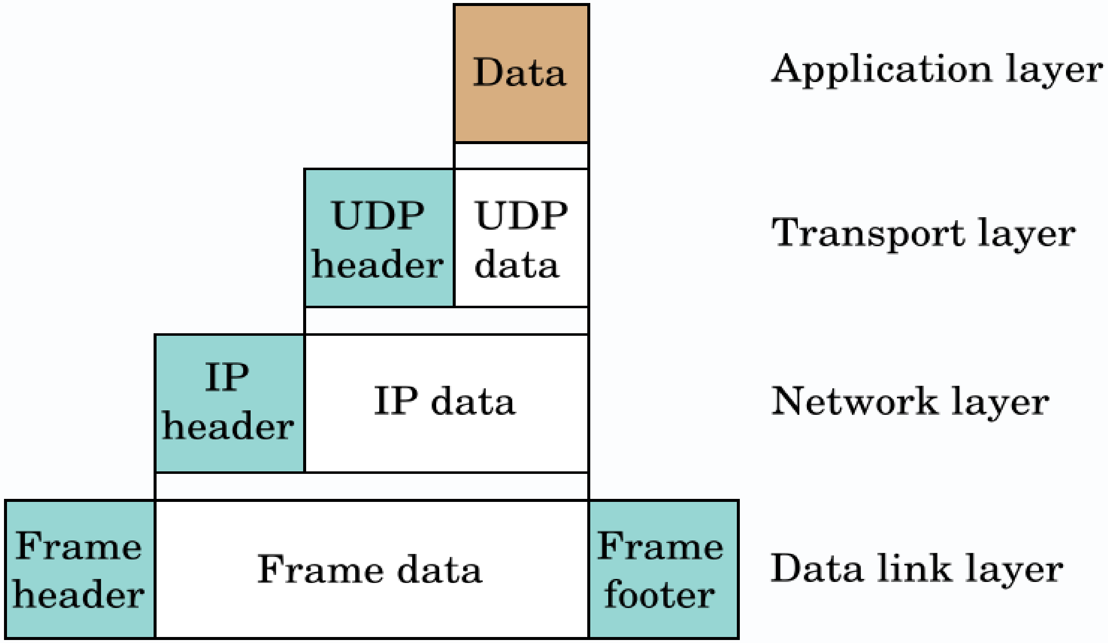

Data
UDP header
UDP data
IP header
IP data
Frame header
Frame data
Frame footer

Application layer
Transport layer
Network layer
Data link layer


Physical layer

Protocol [a standard]

- for the process and rules used by message senders and receivers when they exchange messages via transport mechanisms, or by end points in a telecommunication exchange. May include a standard format for the header preceding the message, the footer following the message, and the sequence in which messages are exchanged.



Data

Application layer

UDP header

UDP data

Transport layer

IP header

IP data

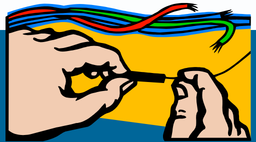
Network layer

Frame header

Frame data

Frame footer

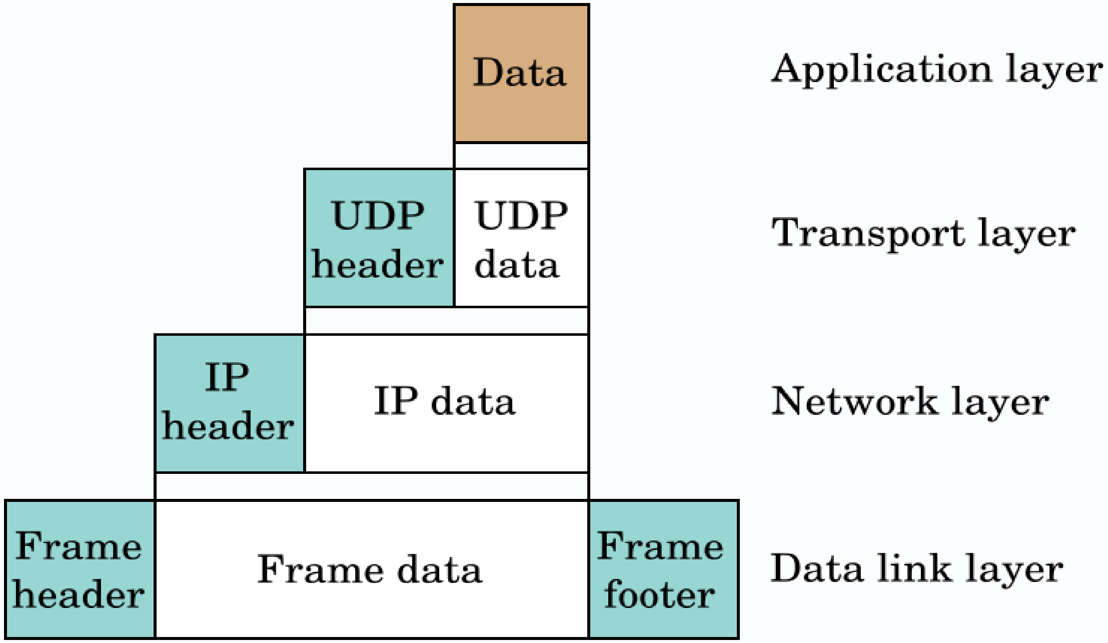
Data link layer

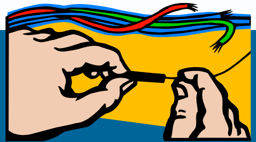


Physical layer

Protocol Stack [a pattern]

- that arranges protocols in layers, corresponding to layers of platform applications. The best known protocol stacks are probably OSI and TCP/IP.

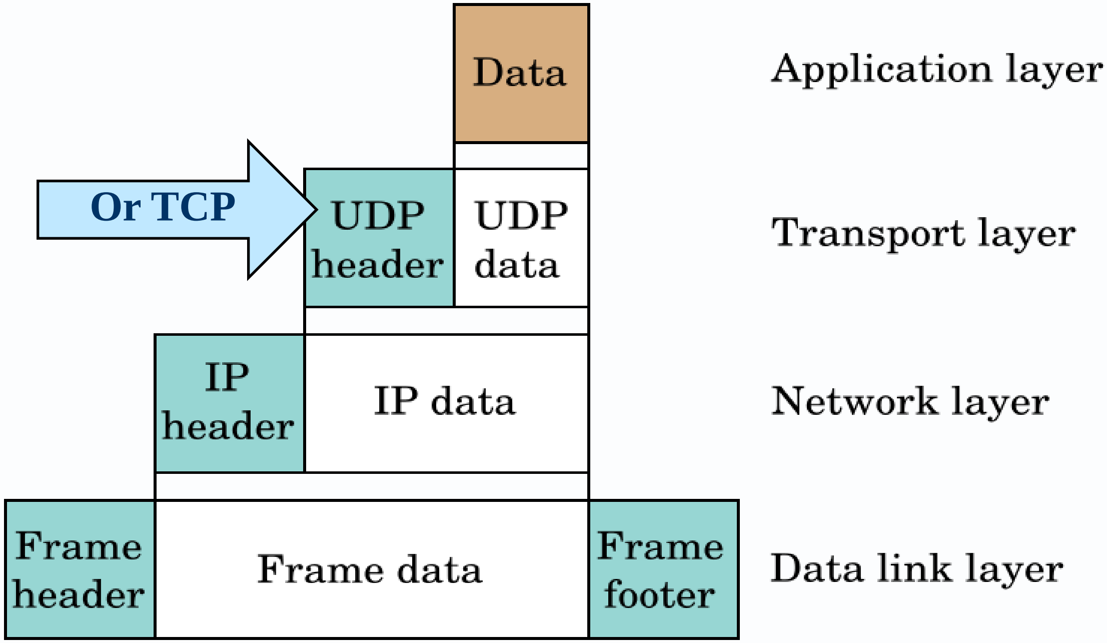


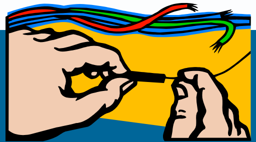


Physical layer

TCP/IP 5 layer stack [a protocol stack]

- nowadays more commonly discussed than the old 7-layer OSI model:

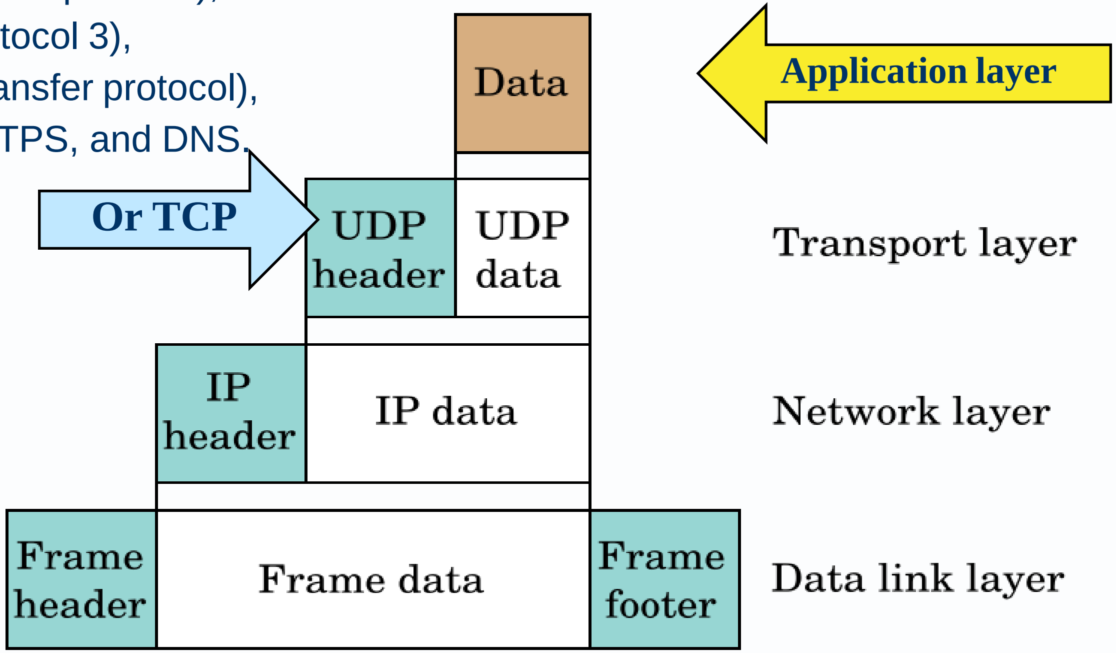




Physical layer

Application layer [a network layer]

- the top layer. It provides services to identify communication partners and quality of service, authenticate users, ensure privacy, and identify constraints on data syntax.
- Popular application layer protocols include
- FTP (file transfer protocol),
- HTTP (hypertext transfer protocol),
- POP3 (post office protocol 3),
- SMTP (simple mail transfer protocol),
- also RPC, SOAP, HTTPS, and DNS.



Data

Application layer

Or TCP

UDP header

UDP data

Transport layer

IP header

IP data

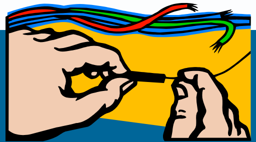
Network layer

Frame header

Frame data

Frame footer

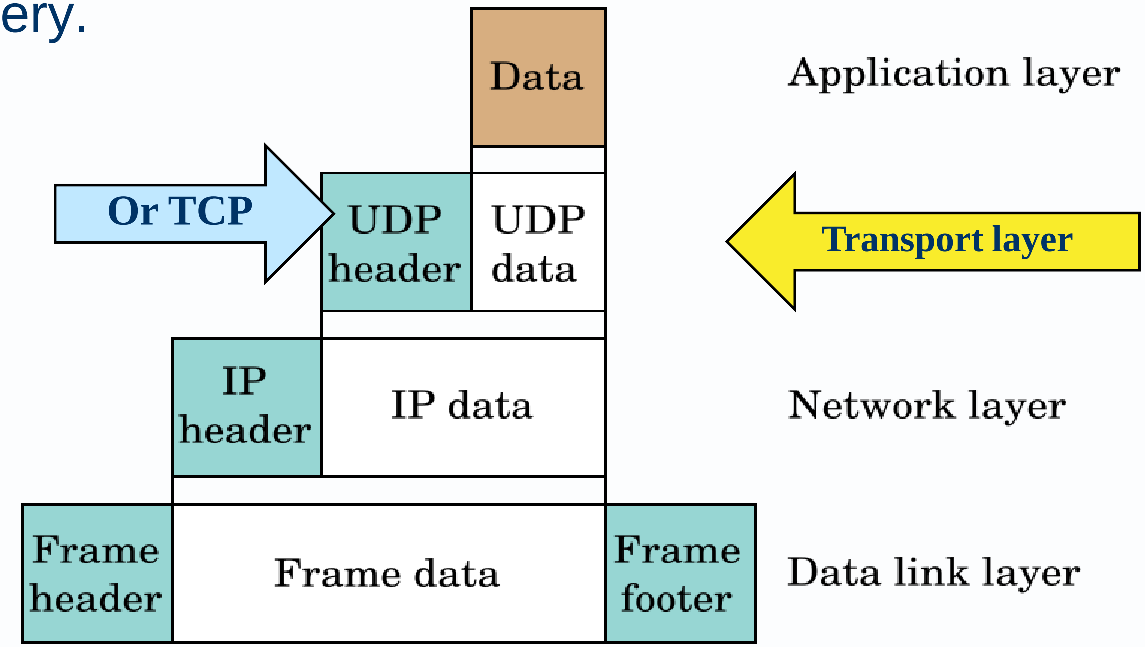
Data link layer



Physical layer

Transport layer [a network layer]

- that manages the end-to-end message delivery.
- TCP (transmission control protocol) and UDP (user datagram protocol) have a checksum to ensure data flow integrity.
- TCP ensures complete data transfer or else times out.
- By contrast, UDP is a lightweight protocol that does report failed message delivery.



Data

Application layer

Or TCP

UDP header

UDP data

Transport layer

IP header

IP data

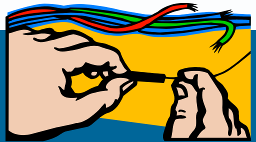
Network layer

Frame header

Frame data

Frame footer

Data link layer



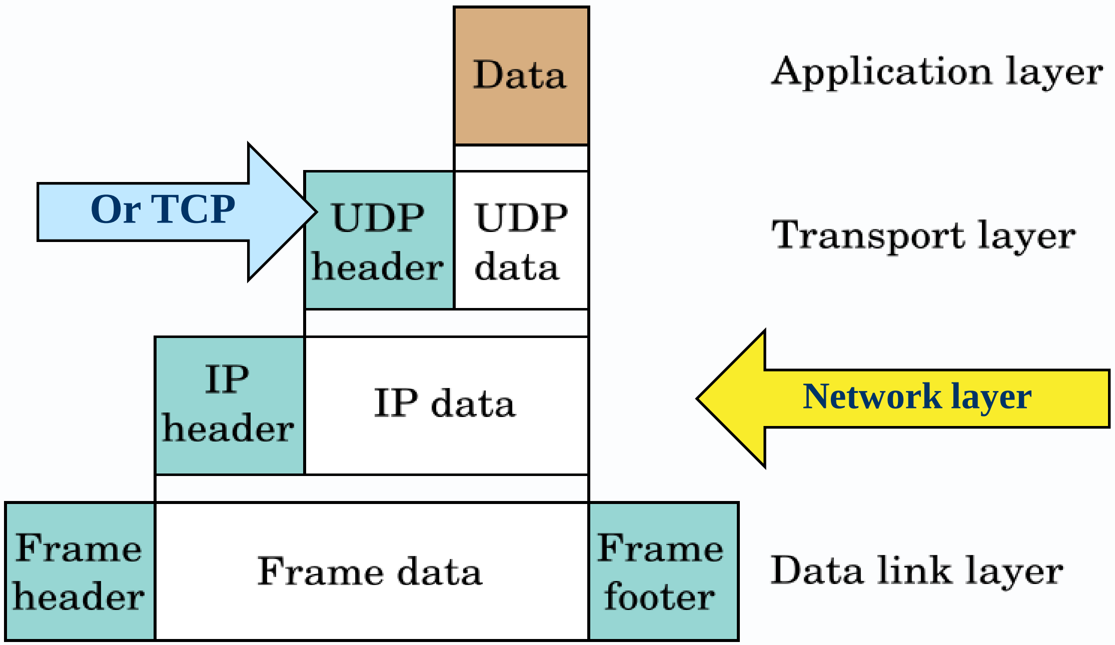
Physical layer

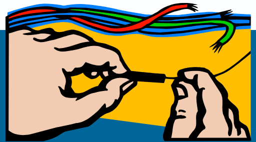
Transport level e.g. TCP v UDP

	Transmission Control Protocol	User Datagram Protocol
Protocol	connection-oriented	connectionless
Connection	requires handshaking to set up end-to-end connection.	no effort to set up a dedicated end-to-end connection.
Reliability	**Reliable** - either no missing data, or, in case of multiple timeouts, the connection is dropped.	**Unreliable** - no concept of acknowledgment, retransmission and timeout.
Ordering	**Ordered** - when data packets arrive in the wrong order, the TCP layer holds data until the earlier data can be rearranged and delivered	**Not ordered** - the order in which packets arrive cannot be predicted.
Weight	**Heavy** - requires three packets just to set up a socket, before any actual data can be sent.	**Light** – simpler and faster
Unit	**Streaming** - Packets may be split or merged into bigger or smaller data streams arbitrarily.	**Datagrams** - Packets have definite bounds and no split or merge into data streams may exist.

Network layer [a network layer]

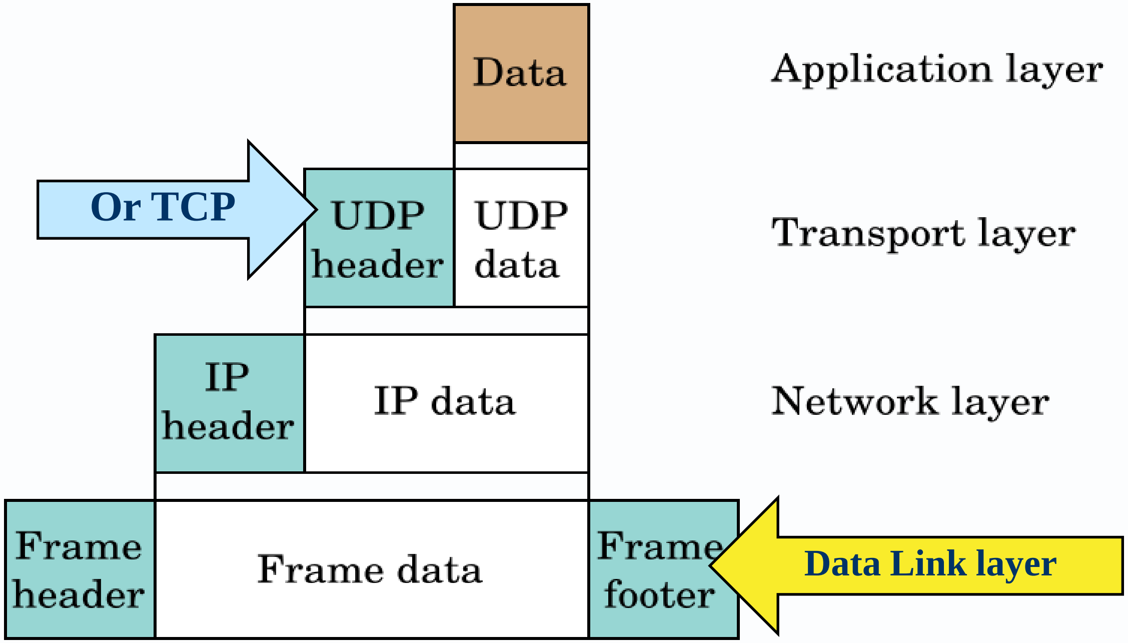
- that handles the routing and forwarding of data at the packet level.
- It sends outgoing transmissions in the right direction to the right destination.
- It receives incoming transmissions. E.g. IP is the dominant network layer protocol.

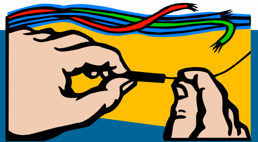



Physical layer

Data transport layer [a network layer]

- at which data is transported around the physical network modes by network communications software.
- It may, e.g., do bit-stuffing for strings of 1's in excess of 5 etc.
- E.g. Wi-Fi. Ethernet (based on a bus topology) and
- Token passing (based on a ring topology).

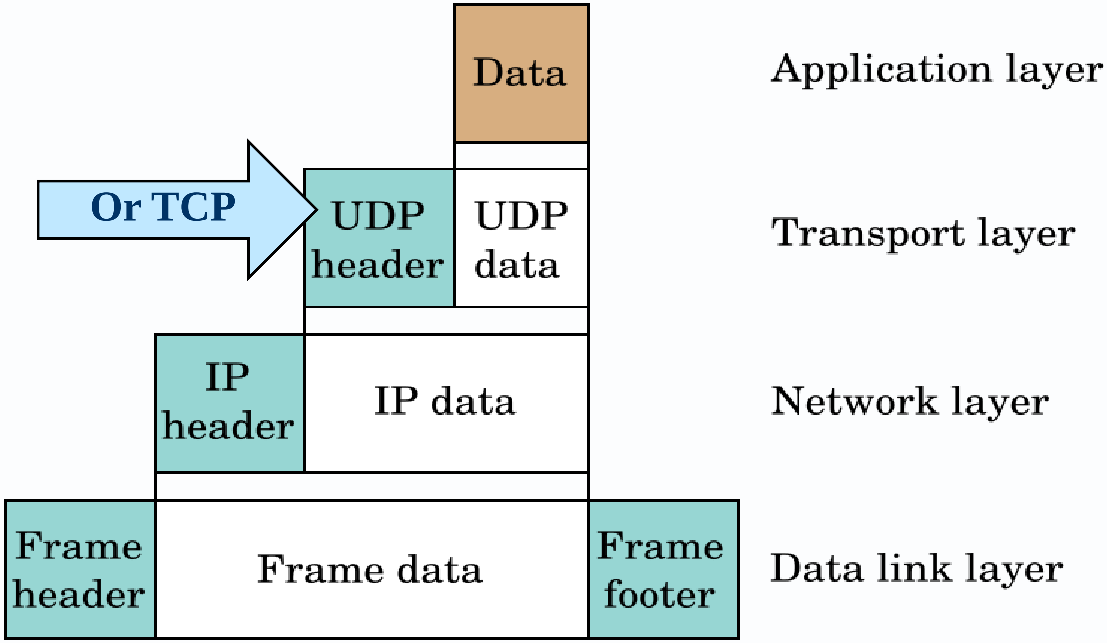




Physical layer

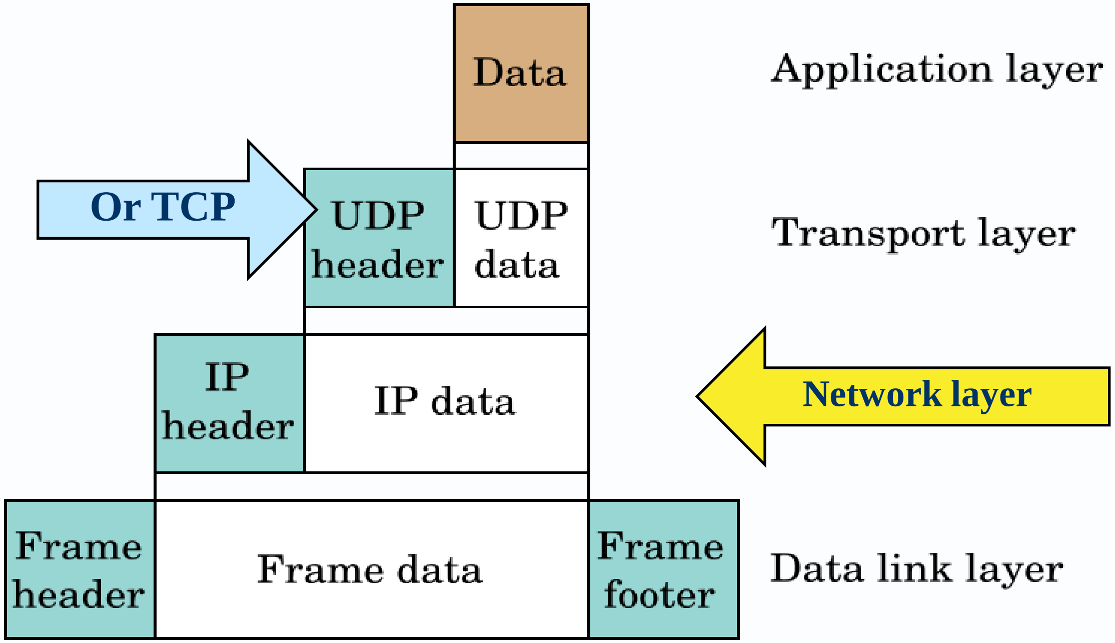
Physical layer [a network layer]

- at the bottom, connecting nodes by a physical medium.
- It conveys the bit stream through the network at the electrical and mechanical level - provides the hardware means of sending and receiving data on a carrier.
- E.g. Modems,
- Optical fiber,
- Coaxial cable,
- Twisted pair.



IP (Internet Protocol) [a protocol]

- a network layer protocol that sends data across a packet-switched internetwork, using IP addresses; the most prominent feature of the Internet.



Data

Application layer

Or TCP

UDP header

UDP data

Transport layer

IP header

IP data

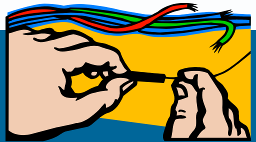
Network layer

Frame header

Frame data

Frame footer

Data link layer



IP address [a property]

- a logical identifier, assigned to a node in a network that uses the Internet Protocol for communication.
- It is divided into two sections:
  - the first identifies a local network;
  - the second identifies a node on that network.

- An IP4 address is made from four 8-bit parts, often presented as four decimal numbers.

- An IP6 address is made from eight 16-bit parts, often presented as eight hexadecimal numbers.
- The range of IP6 addresses is enough to uniquely address every computer, but sub-netting and network address translation remain useful.

NAT: Network address translation [a technique]

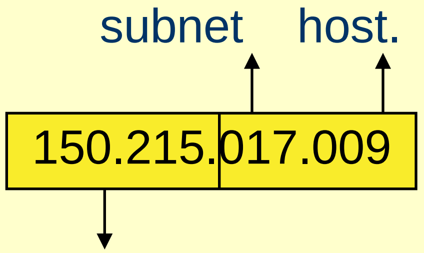
- used to separate the private internet address space within a LAN from the public internet.
- Most NAT systems enable multiple computers on a private network to access the internet using a single public IP address.

Two ways around the limited IP address range

- Network Address Translation
- The router is given
  - A public IP address
  - A configurable list of local IP addresses

- Common addresses
  - 192.168.0.0
    - (255.255.255.0)
  - 172.68.0.0
    - (255.255.0.0)
  - 10.0.0.0
    - (255.0.0.0)

- Subnet
  - Use the second (host) part of the IP address to identify both

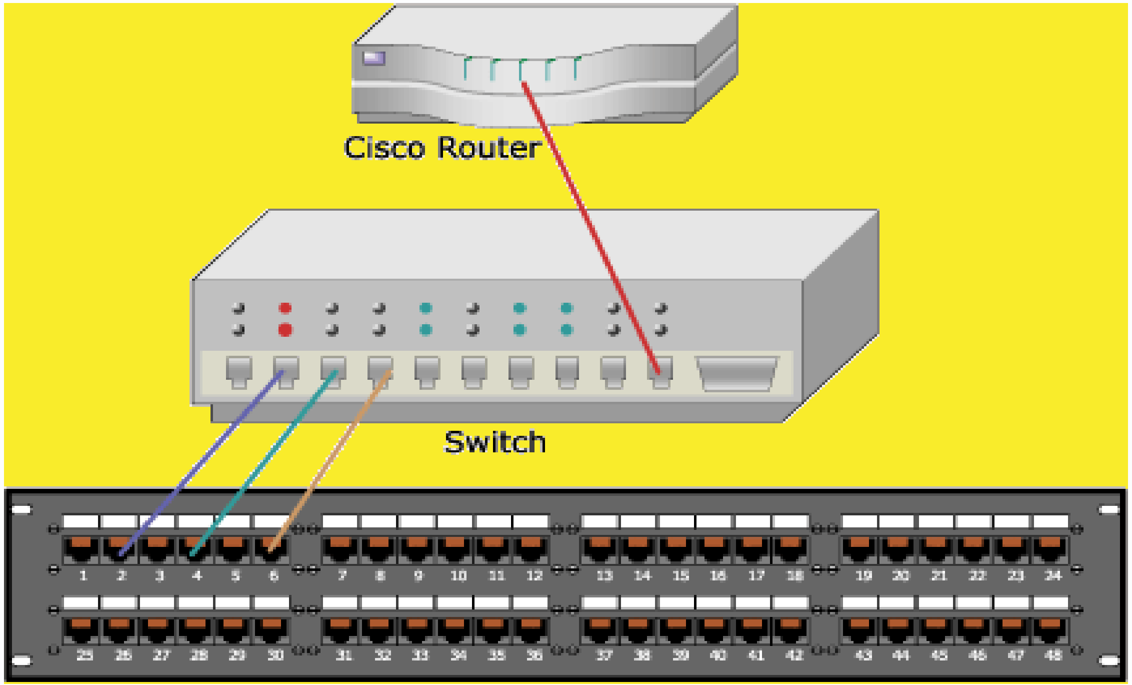


  - The network address

- **Convergence (of telecommunication media)**: the trend that enables one operating platform to supply many media. It enables equipment providers to combine voice, data and images in services offered to the user.

- **VoIP: Voice over IP system** [a component] of IP Telephony that is promoted as offering lower network installation and management costs, lower voice phone tariffs and mobility of phone numbers.

9.5 Connecting applications over networks



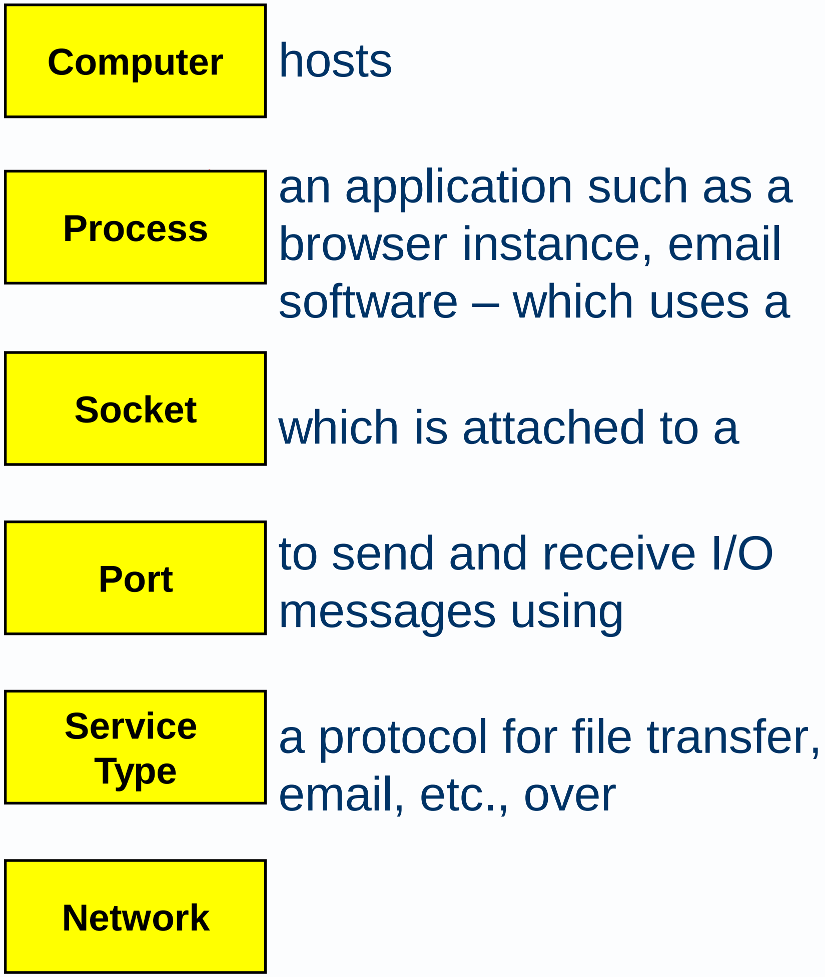
Process (computer sense):

- an application (or program instance) running on a computer (as can be seen in the "Task Manager" on a lap top).
- Each has a process number.
- At run-time, one process can use several sockets to send and receive different kinds of I/O data.

Computer	hosts
Process	an application such as a browser instance, email software – which uses a
Socket	which is attached to a
Port	to send and receive I/O messages using
Service Type	a protocol for file transfer, email, etc., over
Network	

Service Type [a protocol]

- for a computer to send or receive one particular kind of I/O data (such as file, web pages or email).
- One service type can be delivered via different ports.



Computer hosts

Process an application such as a browser instance, email software – which uses a

Socket which is attached to a

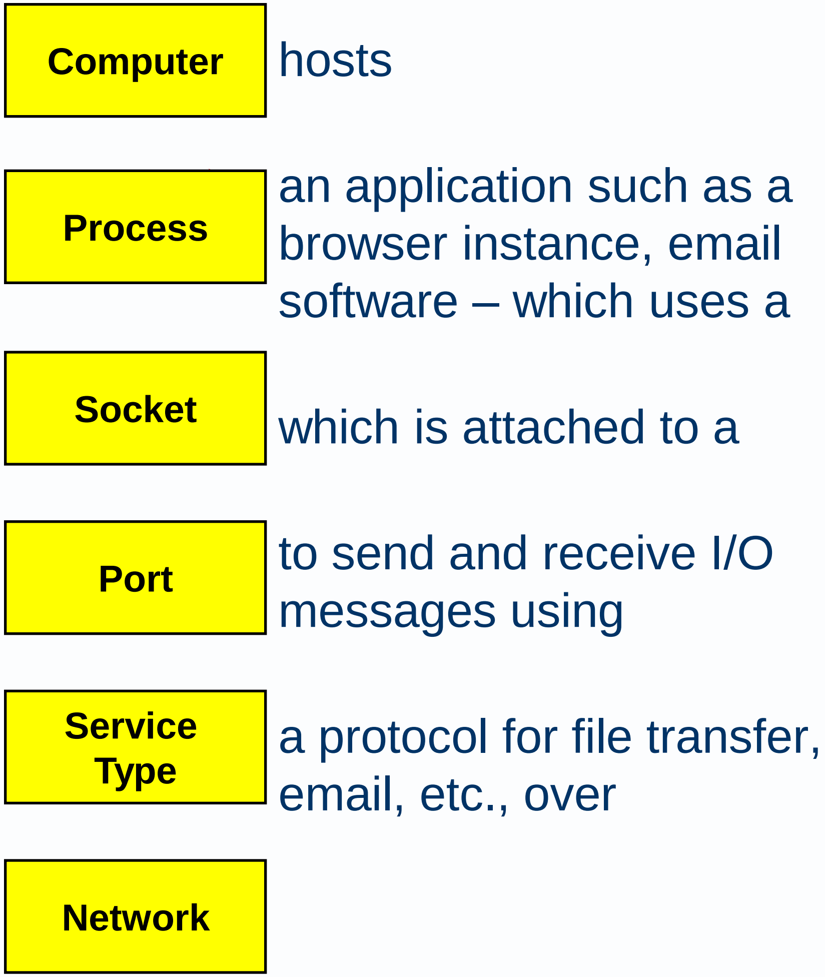
Port to send and receive I/O messages using

Service Type a protocol for file transfer, email, etc., over

Network

NIC [a component]

- a network interface card or network adapter that can connect a computer to a network.
- At its simplest, one NIC is assigned one MAC address by the manufacturer at the factory, and is assigned one logical IP address by an engineer or the run-time environment.
- The IP address on a NIC can be assigned many ports.



Computer hosts

Process an application such as a browser instance, email software – which uses a

Socket which is attached to a

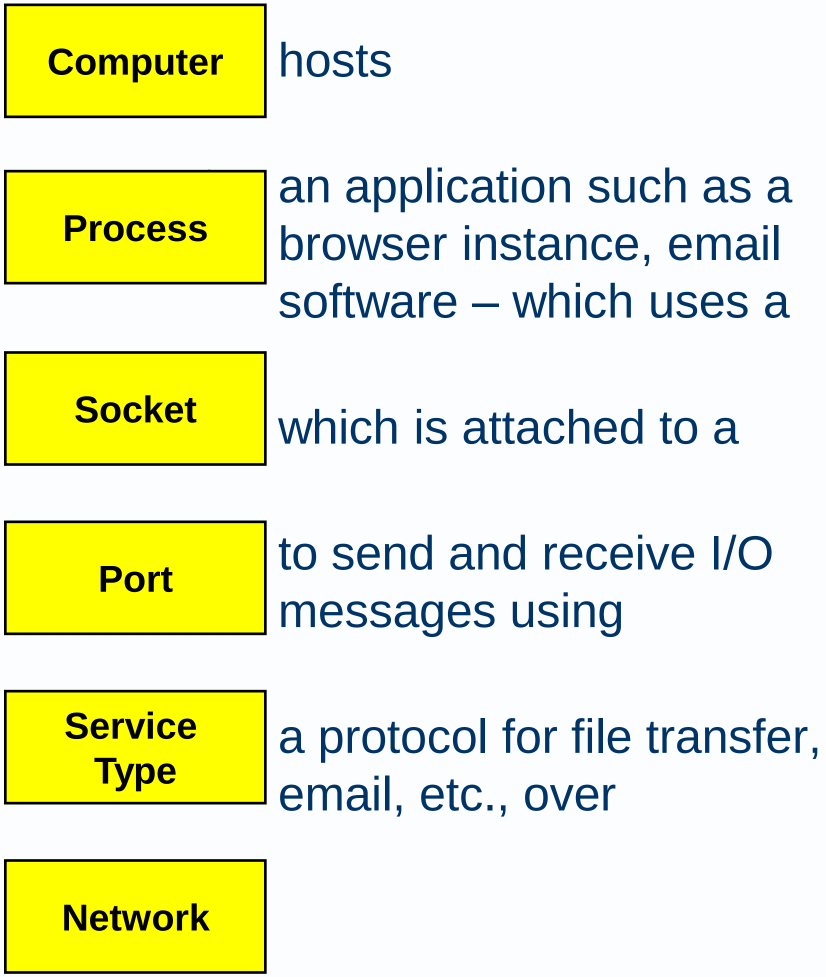
Port to send and receive I/O messages using

Service Type a protocol for file transfer, email, etc., over

Network

Port [a component]

- that is assigned to one IP address for the purpose of sending or receiving I/O data using one service type.
- The choice of port number can be made an engineer or by the run-time environment.
- An international standard defines default port numbers for servers sending and receiving data via specific service types. E.g.
- An HTTP (unsecured) server listens for messages on port 80.
- An HTTPS (secured) server listens for messages on port 443.
- An SMTP server sends email using port 25.
- A POP3 server listens for email using port 110.



Computer hosts

Process an application such as a browser instance, email software – which uses a

Socket which is attached to a

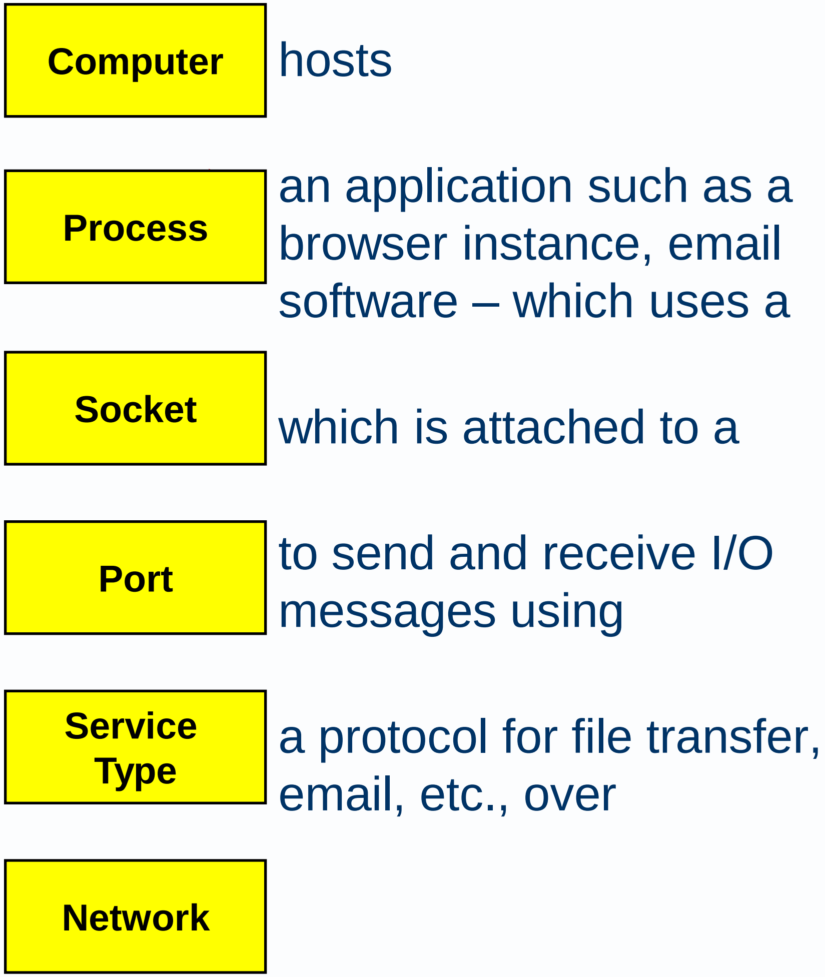
Port to send and receive I/O messages using

Service Type a protocol for file transfer, email, etc., over

Network

Socket [a component]

- that holds data about the use of one port by one process.
- It is identified by a process number and a port number (which has in turn been assigned to a logical network address and a service type).
- E.g. an HTTP server listens for messages on port 80 at a particular IP address, and creates a socket for each process that sends a message. Sockets are reused over time.



Computer hosts

Process an application such as a browser instance, email software – which uses a

Socket which is attached to a

Port to send and receive I/O messages using

Service Type a protocol for file transfer, email, etc., over

Network