



# **Software Engineering in der industriellen Praxis (SEIP)**

**Dr. Ralf S. Engelschall**

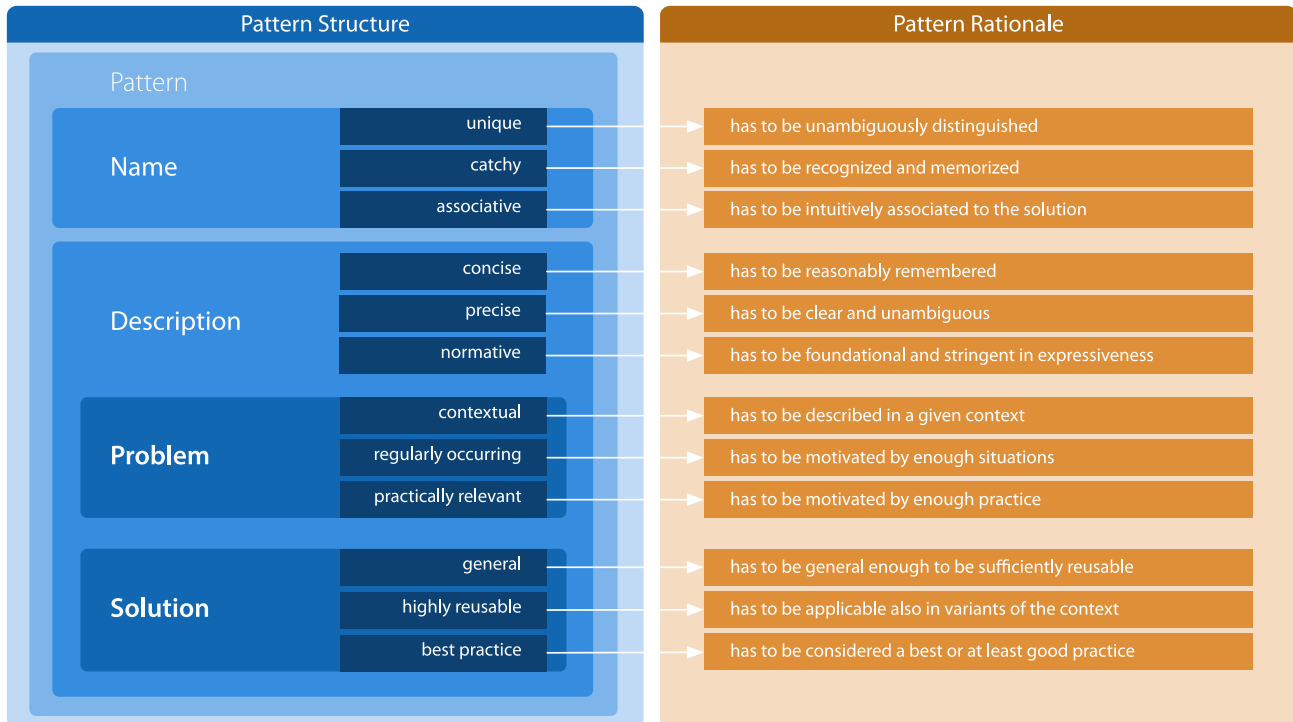
## Pattern Definition

**Pattern:** unique, catchy, and associative **Name** and concise, precise, and normative **Description** of a contextual, regularly occurring, and practically relevant **Problem** and a general, highly reusable, and best practice **Solution** for it.



AF 06.1

Indicate the version of the document (AF 06.1) and the version of the software (AF 06.1) used for the generation of the document. The document is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. For more information, please visit <https://creativecommons.org/licenses/by-nc-sa/4.0/>.



Definition eines **Architekturmusters**: einzigartiger, eingängiger und assoziativer Name und prägnante, präzise und normative Beschreibung eines kontextuellen, regelmäßig auftretenden und praktisch relevanten Problems und einer allgemeinen, hochgradig wiederverwendbaren und praxisbewährten Lösung für dieses Problem.

Die Begründungen ist, daß ein **Architekturmuster**: eindeutig unterschieden werden muß, wiedererkannt und erinnert werden muß, intuitiv mit der Lösung assoziiert werden muß, sich gut merken lassen muß, klar und eindeutig sein muß, grundlegend und stringent in der Ausdrucksfähigkeit sein muß, in einem bestimmten Kontext beschrieben werden muß, durch genügend Situationen motiviert sein muß, durch genügend Praxis motiviert sein muß, um ausreichend wiederverwendbar zu sein auch allgemein genug sein muß, auch in Varianten des Kontexts anwendbar sein muß, und als beste oder zumindest gute Praxis angesehen werden muß.

**Architekturmuster** ermöglichen es einem insbesondere effizient zu kommunizieren (Name) und von den eingeflossenen Erfahrungen zu profitieren (Best Practice).

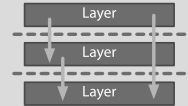
## Fragen

? Warum sind **Architekturmuster** interessant?

## Layering Principle

Horizontally split code or data into two or more logically, optionally also spatially, clearly distinct, isolating, named, and ranked Layers.

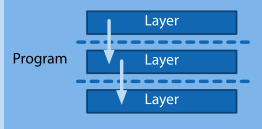
A Layer is not allowed to have relationships to or knowledge about any upper Layers. Additionally, for **Closed Layering**, each Layer is allowed to have relationships to and knowledge about the **directly** lower Layer only. In contrast to **Open Layering** or **Leaky Abstraction**, where each Layer is allowed to have relationships to and knowledge about **any** lower Layer.



### LR Layer

Split related code or data of a Program into two or more logically distinct domain- or technology-induced Layers.

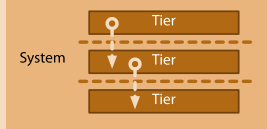
Rationale: Separation of Concern, Single Responsibility Principle, Mastering Complexity, Change Isolation, Functional Abstraction.



### TR Tier

Split related code or data of a System into two, three or more logically and spatially distinct, network-connected, domain- or technology-induced Tiers.

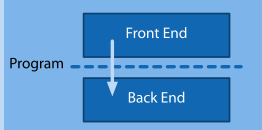
Rationale: Separation of Concern, Single Responsibility Principle, Mastering Complexity, Change Isolation, Functional Abstraction, Deployment Partitioning.



### FB Front End / Back End

Split the code of a Program into exactly two logical Layers: a user-facing Front End and a data-facing Back End.

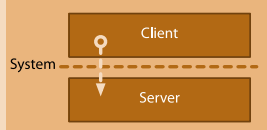
Rationale: Separation of Concern, Single Responsibility Principle, Mastering Complexity, Change Isolation, Functional Abstraction, Organisational Alignment.



### CS Client / Server

Split the code of a System into two spatially distinct, network-connected Layers, each forming a stand-alone Program: a user-facing and multi-instantiated (Rich) Client and a data-facing (and logically) single-instantiated (Thin) Server. Both contain a Front/Back End.

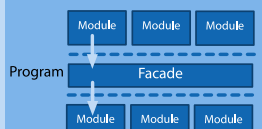
Rationale: Multi-User, User Computing Resource Leverage, Distributed Computing.



### FD Facade

Splice a domain-specific Facade Layer into two Layers of two or more Modules. The extra Facade Layer acts as a broker between the Modules.

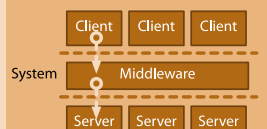
Rationale: Information Hiding, Cross-Cutting Concern Centralization, Functionality Orchestration, Authorization, Validation, Conversion.



### MW Middleware

Splice a domain-unspecific Middleware Layer into a Client/Server communication. The extra Layer is a stand-alone Program Tier and acts as a broker between Client and Server.

Rationale: Communication Peer Discovery Simplification, Transport Protocol Conversions, Network Topology Flexibility.



Beim **Layering** werden Code oder Daten in zwei oder mehr logische (**logically**) — ggf. auch “physikalische” (**spatially**) — **Layer** geschnitten. Diese Layer sind klar unterscheidbar (**clearly distinct**), von einander isoliert (**isolated**), benannt (**named**) und stehen in einer Rangordnung (**ranked**). Layer werden immer **horizontal** gezeichnet.

Ein Layer hat keine Beziehung (**relationship**) zu, oder Wissen (**knowledge**) über, irgendwelche Layer über ihm. Zusätzlich darf er, beim **Closed Layering**, eine Beziehung zu oder Wissen über den direkten Layer unter ihm haben. Außerdem darf er beim **Open Layering** bzw. der **Leaky Abstraction** sogar eine Beziehung zu oder Wissen über irgendwelche Layer unter ihm haben.

Falls sich das Layering über Netzwerk-Grenzen erstreckt oder eine “physikalische” Grenze durchbricht, spricht man nicht mehr von einzelnen Layern, sondern von **Tiers**.

Zerfällt ein Programm in einen vorderen bzw. auf das User-Interface fokussierenden Layer und einen hinteren bzw. auf Daten fokussierenden Layer, so spricht man bei den beiden Layern auch von **Front End** und **Back End** des Programms. Dies ist nicht zu verwechseln mit **Client** und **Server**, welche die zwei Tiers eines Systems über ihre speziellen Rollen benennt. Sowohl der Client als auch der Server sind eigenständige Programme mit jeweils einem Front End und einem Back End.

Eine sehr spezieller und prominenter Layer ist die **Facade**, welche innerhalb eines Programms die Module von zwei anderen Layern von einander trennt. Eine Variante der Facade auf Ebene eines Systems (statt auf der Ebene eines Programms) ist die **Middleware**, welche eine Client/Server-Kommunikation auftrennt.

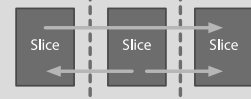
## Fragen

- ❓ Wie nennt man die entstehenden Einheiten, wenn Code oder Daten **horizontal** geschnitten werden?
- ❓ Was ist der Unterschied zwischen den Layer-Pärchen **Front/Back End** und **Client/Server**?

## Slicing Principle

Vertically split code or data into two or more logically, optionally also spatially, clearly distinct, named, and unranked slices.

The particular slicing should minimize the total amount of individual relationships between the resulting slices. Per type of relationship, there should be no cycle in the transitive relationships.



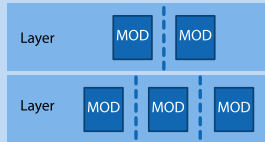
AF 063

Copyright © 2024, Technische Universität München (TUM). All rights reserved. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. For more information, see <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

### MOD Concerned Module

Split related code or data (usually across a single Layer) into two or more logically distinct domain- or technology-induced Modules.

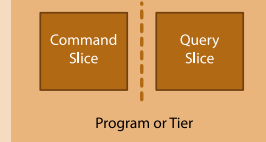
Rationale: Separation of Concern, Single Responsibility Principle, Mastering Complexity.



### CQRS Command-Query Responsibility Segregation

Split code and data of a Program (across all Layers) or a Tier into exactly two slices to segregate operations that read data (queries) from the operations that update data (commands).

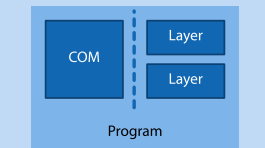
Rationale: Separated Scalability, Separated Data Access Patterns, Event Sourcing Approach.



### COM Common Slice

Factor out common or cross concern code or data of a Program (across all Layers) into a single spatially distinct, separate slice.

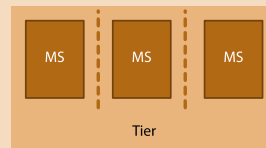
Rationale: Lack of Redundancy, Single Point of Truth, Reusability.



### MS Microservice

Split code and data of a Tier (across all Layers and Tiers) into two or more distinct, loosely-coupled, domain-enclosed, functional services, each forming a stand-alone Program.

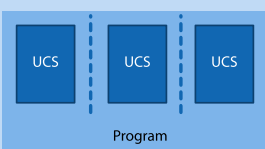
Rationale: Heterogeneity, Long-Term Large-Scale Maintenance, Replaceability, Resilience, (Scalability), (Easy Deployment), (Organizational Alignment), (Composability), (Reusability).



### UCS Use-Case Slice

Split the code and data of a Program (across all Layers) into two or more purely logical slices, one for each distinct, domain-specific Use-Case.

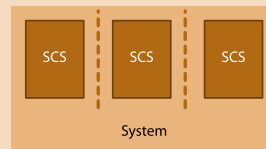
Rationale: Comprehensibility, Domain Alignment, Mastering Complexity.



### SCS Self-Contained System

Split code and data of a System (across all Layers and Tiers) into two or more distinct, loosely-coupled, domain-enclosed, functional systems, each forming a stand-alone sub-System.

Rationale: Mastering Complexity, Heterogeneity, Resilience, Scalability, Easy Deployment, Organizational Alignment, Reusability, Replaceability.



Beim **Slicing** werden Code oder Daten in zwei oder mehr logische (**logically**) — ggf. auch “physikalische” (**spatially**) — **Slices** geschnitten. Diese Slices sind klar unterscheidbar (**clearly distinct**), voneinander isoliert (**isolated**) und benannt (**named**). Slices werden immer **vertikal** gezeichnet.

Slices im selben Layer sollten möglichst unabhängig voneinander sein. Im Falle von Beziehungen sollte zumindest kein Zyklus existieren. Es gibt verschiedene spezielle Varianten von Slices, die jeweils einen eigenen Namen haben.

**Concerned Modules** sind Slices eines Layers, welche ein bestimmtes fachliches oder technisches Anliegen umsetzen. **Common Package** ist ein Slice eines Tiers, wohin Gemeinsamkeiten anderer Layer verschoben wurden. **Use-Case Slices** sind Slices eines Tiers, die sich jeweils dediziert um bestimmte fachliche Anwendungsfälle kümmern.

Bei der **Command-Query Responsibility Segregation** Architektur wird ein Tier in zwei Slices für Commands/ Writes und Queries/ Reads getrennt. Ein **Microservice** ist ein Slice eines Tiers, welcher als getrenntes Programm ausgeführt ist und sich um eine abgeschlossene fachliche Funktionalität kümmert. Ein **Self-Contained System** ist ein Slice eines gesamten Systems, welches als getrenntes Sub-System ausgeführt ist.

## Fragen

- ❓ Wie nennt man die entstehenden Einheiten, wenn Code oder Daten **vertikal** geschnitten werden?
- ❓ Wie nennt man die Slices eines Tiers, welche als getrennte Programme ausgeführt sind, die sich jeweils um bestimmte fachlich abgeschlossene Funktionalitäten kümmern?

- ❓ Mit Hilfe welcher **Flow Architecture** kann man N Komponenten so miteinander verschalten, daß statt  $N \times (N - 1) / 2$  nur N Kommunikationswege entstehen?

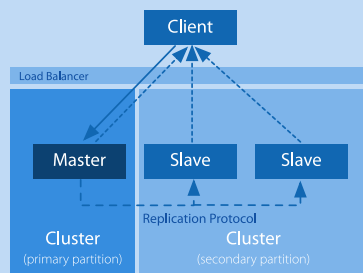


## Master-Slave (Static Replication)

Cluster of a single **Master** and multiple **Slave** nodes, where data is continuously copied from the Master to the Slave nodes in order to support high-availability (where a Slave will take over the Master role) in case of a Master outage and increased read performance (where regular read requests are also served by the Slaves).

In this static replication scenario the Master is usually assigned statically and in case of outages has to be reassigned usually semi-manually. Especially, the full reestablishment of the original Master assignment after a Master recovery usually is a manual process.

Examples: OpenLDAP Replication, PostgreSQL WAL Replication.

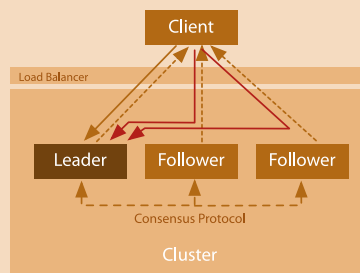


## Leader-Follower (Dynamic Replication)

Cluster of a single **Leader** and multiple **Follower** nodes, where data is written on the current Leader node and data read on both the current Leader and all Follower nodes. For writing data to the cluster, the Leader node performs a consensus protocol (e.g. RAFT, Paxos or at least Two-Phase-Commit) with the Followers and this way automatically and consistently replicates the data to the Followers.

In this dynamic replication scenario the Leader is usually automatically assigned by the cluster nodes through an election protocol and in case of outages is automatically re-assigned. There is usually no re-establishment of the original Leader assignment.

Examples: Apache Zookeeper, Consul, EtcD, CockroachDB, InfluxDB.

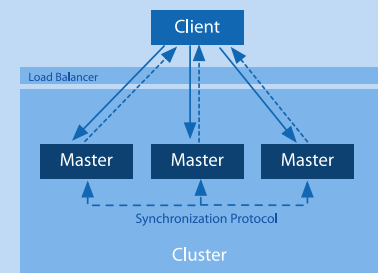


## Master-Master (Synchronization)

Cluster of multiple **Master** nodes, where data is read and written on any Master node concurrently. The Master nodes either use Strict Consistency through writing to a mutual-exclusion-locked shared storage concurrently or use Eventual Consistency in a Shared Nothing storage scenario where they continuously synchronize their local data state to all other nodes with the help of a synchronization protocol.

The synchronization protocol usually is based on either Conflict-Free Replicated Data Types (CRDT) or at least Operational Transformation (OT). In any scenario, data update conflicts are explicitly avoided.

Examples: ORACLE RAC, MySQL/MariaDB Galera Cluster, Riak, Automerge/Hypermerge.



→ Write Operation  
--- Read Operation

Bei den **Cluster Architectures** wird der Zusammenschluss von Rechnerknoten zu einem Cluster adressiert.

Bei der **Master-Slave** Architektur handelt es sich um eine statische Replikation der Daten von einem Master Server auf einen oder mehrere Slave Server. Die Clients können Lesezugriffe an alle Server senden, müssen aber Schreibzugriffe ausschließlich über den Master laufen lassen. Dies wird üblicherweise dazu verwendet, um die Read Performance zu steigern.

Bei der **Leader-Follower** Architektur handelt es sich um eine Art dynamische Replikation der Daten von einem Leader Server auf einen oder mehrere Follower Server. Die Clients können sowohl Lese- als auch Schreibzugriffe an alle Server senden. Da nur der Leader Server die Schreibzugriffe bearbeiten darf, leiten die Follower Server diese, intern und für den Client intransparent, an den Leader Server weiter.

Dies ist auch der Unterschied zu Master-Slave: der Leader wird über ein Leader Election Protocol (bei einem Ausfall des aktuellen Leader Servers) automatisch und dynamisch zwischen allen Servern festgelegt. Der Vorteil ist, daß sich Leader-Follower für die Clients wie Master-Master anfühlt, der Cluster aber keine aufwändige Konfliktlösungsstrategie wie bei Master-Master umsetzen muss.

Bei der **Master-Master** Architektur handelt es sich um eine echte Synchronisation der Daten zwischen zwei oder mehr gleichberechtigten Master Server. Die Clients können sowohl Lese- als auch Schreibzugriffe an beliebige Master Server richten. Die Master Server müssen dazu aber intern eine aufwändige Konfliktlösungsstrategie umsetzen, um gleichzeitige Änderungen an denselben Daten aufzulösen.

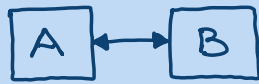
## Fragen

- ❓ Welche einfache **Cluster Architecture** kann man einsetzen, wenn die Read-Performance einer Server-Anwendung gesteigert werden soll?



**PTP**   **Point-to-Point**

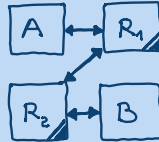
Communicate between two network nodes in a point-to-point fashion, usually through a direct link.



**Rationale:** simple communication where both nodes know about each other and can directly reach each other.

## RTG Routing

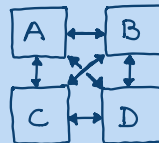
Communicate between two network nodes in a point-to-point fashion, but by routing the network packets over intermediate forwarding nodes (routers).



**Rationale:** simple communication where both nodes know about each other, but cannot directly reach each other.

**P2P** Peer-to-Peer

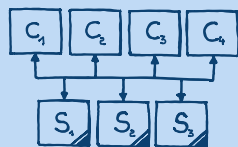
Communicate between multiple network nodes (usually all in the client and server role at the same time) without involving a central hub node (in the role of a server) — except for the initial network entry discovery.



**Rationale:** communication without central control (although a seed peer is required).

**C/S**    **Client/Server**

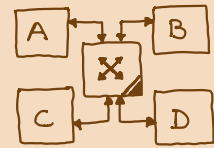
Communicate between multiple nodes in the client role (making requests, and usually with ephemeral addresses) and multiple nodes in the server role (serving responses, and usually with fixed addresses).



**Rationale:** communication with central orchestration, control and data storage.

## BUS Bus/Broker/Relay

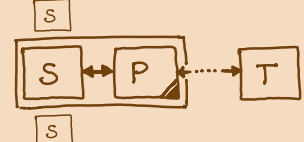
Communicate between multiple nodes with the help of a central packet forwarding hub node in a star network topology.



**Rationale:** decouple communication nodes:  
instead of Point-to-Point (PTP)  
communications between **all** nodes, there  
are just PTP communications with the hub.

## FPR (Forward) Proxy

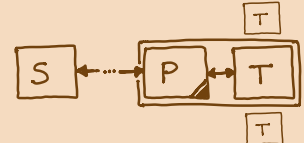
Communicate between two nodes by using an intermediate forwarding proxy node in front of the source node.



**Rationale:** bridge network topology constraints (segmented networks); caching at source side; auditing of communication.

## RPR Reverse Proxy

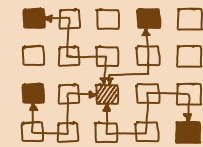
Communicate between a source and a target node by using a masquerading proxy node directly in front of the target node.



**Rationale:** load balancing for multiple target nodes; caching at target side; auditing of communication; security shielding of target nodes; protocol conversions.

**VPN**    **Virtual (Private) Network**

Communicate between nodes in a logical star network topology on top of an arbitrary physical routed network topology.



**Rationale:** secure private network overlaying an unsecure public network; simplify network topology.

Bei den **Networking Architectures** wird die Netzwerk-topologische Kommunikation zwischen Rechnerknoten adressiert. Der einfachste Weg ist eine **Point-to-Point** Kommunikation über eine direkte Verbindung der Knoten.

Üblicherweise geht die Kommunikation heute aber über ein Netzwerk von Knoten, bei dem die einzelnen Nachrichten mit Hilfe von **Routing** über Zwischenknoten ausgetauscht werden.

Kommunizieren alle Knoten in sowohl Client- als auch Server-Rolle direkt miteinander, so spricht man von einer **Peer-to-Peer** Architektur. Sind einige Knoten nur in der Client-Rolle und andere nur in der Server-Rolle, so spricht man von einer **Client/Server** Architektur.

Um mehrere Knoten miteinander kommunizieren zu lassen, ohne daß diese sich jeweils kennen und adressieren müssen, nutzt man üblicherweise einen zentralen **Bus/Broker** Knoten und eine Stern-Topologie.

Sind zwischen Quelle (Source) und Ziel (Target) Zwischenknoten aktiv, welche als Stellvertreter (**Proxy**) in der Kommunikation agieren und nicht nur wie ein **Router** die Netzwerk-Pakete weiterleiten, spricht man entweder von einer (**Forward**) **Proxy** oder **Reverse Proxy** Situation. Ersteres, wenn der Proxy auf Seite des Quellknotens agiert, letzteres, wenn der Proxy als Stellvertreter des Zielknotens agiert.

Zusätzlich kann ein sogenanntes **Virtual Private Network** etabliert werden, bei dem ein logisches abgesichertes "Overlay Network" über ein physikalisches Netzwerk gelegt wird.

## Fragen


- ❓ Mit welcher **Network Architecture** kann man mehrere Knoten miteinander kommunizieren lassen, ohne daß diese Knoten sich jeweils untereinander genau kennen müssen?
- ❓ Wie nennt man einen Rechnerknoten, der als Stellvertreter für einen Zielknoten agiert?



**UCT Unicast** (one-to-one)

Communicate messages from one source to exactly one destination node. The destination node is explicitly and individually addressed.


**Rationale:** private communication between exactly two nodes which both know each other beforehand.



**ACT Anycast** (one-to-any)

Communicate messages from one source to one of many destination nodes. The picked destination node usually is the network-topology-wise "nearest" or least utilized node in a group of nodes.

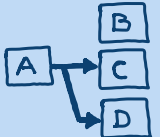
**Rationale:** Unicast, optimized for network failover scenarios, load balancing and CDNs.



**MCT Multicast** (one-to-many)

Communicate messages from one source to many destination nodes. The destination nodes usually form a group and are usually not individually addressed.

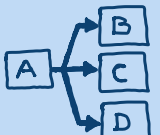
**Rationale:** node communication where destination nodes dynamically change or where total traffic should be reduced.



**BCT Broadcast** (one-to-all)

Communicate messages from one source to all available destination nodes. The destination nodes usually are implicitly defined by the extend of the local communication network segment.

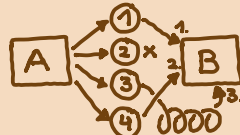
**Rationale:** spreading out messages to all available nodes for potential responses.



**DGR Datagram** (Single Packet)

Communicate messages as an unordered set of single packets, usually without any network congestion control, retries or other delivery guarantees.

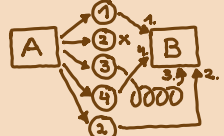
**Rationale:** simple low-overhead communication without prior communication establishment (handshake).



**STR Stream** (Sequence of Packets)

Communicate messages as an ordered sequence (stream) of packets, usually with network congestion control, retries and delivery guarantees (at-most-once, exactly-once, at-least-once).


**Rationale:** reliable communication between nodes.



**PLL Pull** (Request/Response, RPC)

Communicate by performing a request (from the client node) and pulling a corresponding response (from the server node).

**Rationale:** Remote Procedure Call (RPC) like Unicast or Anycast communication.



**PSH Push** (Publish/Subscribe, Events)

Communicate by "subscribing" to "channels" of messages (on one or more receiver nodes or on an intermediate hub) once and then publishing events to those "channels" (on the sender node) multiple times.

**Rationale:** event-based Multicast or Broadcast communication.



Bei den **Communication Architectures** wird die Kommunikationsart zwischen Komponenten adressiert. Man unterscheidet primär vier verschiedene Arten des Nachrichtenversands: beim **Unicast** sendet ein Quellknoten an exakt einen direkt adressierten Zielknoten. Beim **Anycast** sendet ein Quellknoten an eine Gruppe von potenziellen Zielknoten, die Nachricht wird aber nur an einem Zielknoten aus der Gruppe zugestellt.

Beim **Multicast** sendet ein Quellknoten ebenfalls an eine Gruppe von Zielknoten, die Nachricht wird aber an allen Zielknoten aus der Gruppe zugestellt. Beim **Broadcast** sendet ein Quellknoten an alle erreichbaren Zielknoten, ohne daß diese konkreten Zielknoten dem Quellknoten bekannt sind.

Bei der Art der Nachrichten unterscheidet man zwei Varianten: beim **Datagram** besteht jede Nachricht aus exakt einem Netzwerkpaket und beim Versand mehrerer Nachrichten werden keine Garantien gegeben, ob und in welcher Reihenfolge die Nachrichten beim Zielknoten ankommen werden. Im Gegensatz dazu, besteht beim **Stream** eine Nachricht aus einer Sequenz von Netzwerkpaketen und dabei werden verschiedene Garantien gegeben:

Bei Paketstaus auf Zwischenknoten wird beim **Stream** ggf. die Quelle gedrosselt. Bei Paketverlust werden Pakete erneut versandt. Und man erhält ggf. die Kontrolle darüber, ob das Paket am Zielknoten maximal einmal, genau einmal, oder mindestens einmal zugestellt wird.

Man unterscheidet üblicherweise zwei Modi der Client/Server-Kommunikation: beim **Pull**-Modus sendet der Client eine Anfrage und der Server sendet eine Antwort. Der Server kann hierbei insbesondere nicht (ohne vorherige Anfrage) eine Nachricht proaktiv versenden. Beim **Push**-Modus sendet der Client vorab eine Nachricht an den Server, um bestimmte Arten von Nachrichten zu abonnieren. Danach kann jederzeit der Server eine Nachricht an alle dafür abonnierten Clients senden.

Üblicherweise wird **Pull** über **Unicast/Anycast** und als **Stream** implementiert, beispielsweise im Protokoll HTTP. **Push** wird dagegen üblicherweise über **Multicast/Broadcast** als **Datagram** implementiert, beispielsweise im Protokoll DHCP.

## Fragen

- ❓ Welches bekannte Web-Protokoll nutzt eine auf **Unicast, Stream** und **Pull** basierende Kommunikation?