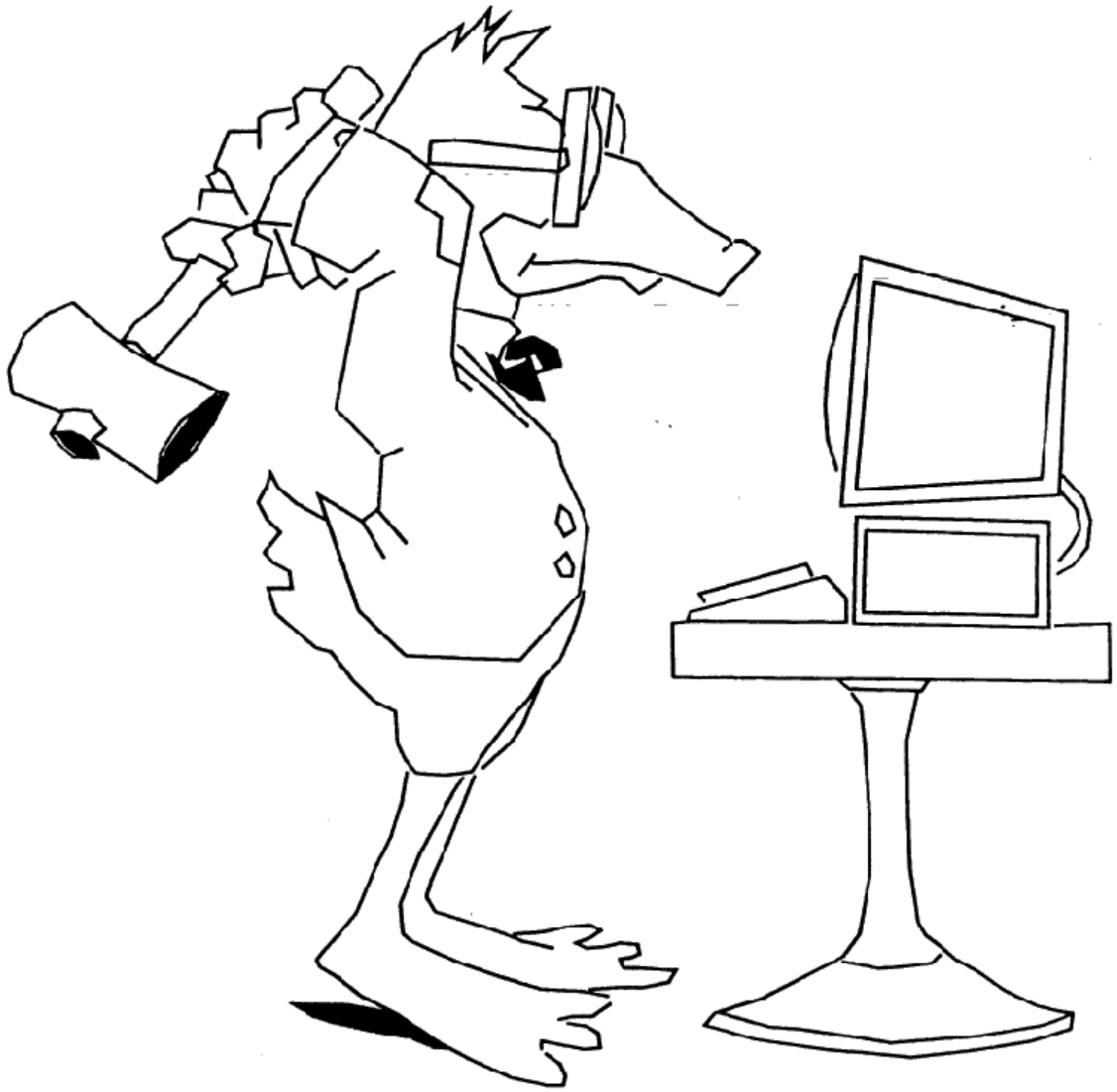
CoC ITA

Hochverfügbarkeitstechnologien in der IT

BMW Group

Hochverfügbarkeitstechnologien

CoC ITA



Hochverfügbarkeitstechnologien

CoC ITA

Agenda

- Einführung (Grundbegriffe, Kenngrößen etc.)
- Einordnung verschiedener HV-Technologien
- Cluster-Technologien
  HA-Cluster, Dispatched Cluster, Applikations-Cluster
- HV mit „virtuellen Maschinen“
- Hochverfügbare und katastrophensichere Netze
- Distributed File System (DFS)
- Software-Probleme und Gegenmaßnahmen
- Zusammenfassung
- Beantwortung von Fragen

Einführung

Definition

CoC ITA

Hochverfügbarkeit (HA = High Availability)

Unter Hochverfügbarkeit versteht man die Fähigkeit eines Systems, bei Ausfall einzelner Ressourcen (z.B. Server, Storage, Netzwerk, Software,...) seine Funktion ohne Eingriff von außen in relativ kurzer Zeit ohne Datenverlust wiederherzustellen.

Einführung

Katastrophenvorsorge (1)

CoC ITA

Katastrophenvorsorge

Vorsorge gegen den gleichzeitigen Ausfall mehrerer Systeme, beispielsweise eines gesamten Rechenzentrums, z.B. durch

Feuer, Wasser, Terroranschläge, Erdbeben.

Im K-Fall werden höhere Wiederanlaufzeiten sowie ein eingeschränkter Betrieb akzeptiert.

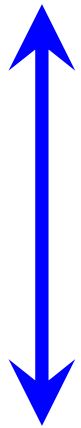
Einführung

Katastrophenvorsorge (2)

CoC ITA

- Backup an einen entfernten u. sicheren Ort
- Daten online zu einem entfernten Ort spiegeln
- Einsatz eines Notfall-Rechenzentrums eines Dienstleisters (Provider)
- Redundante Systeme in zwei getrennten Brandabschnitten
- Redundante Systeme in zwei getrennten Rechenzentren

einfache Maßnahmen mit geringer Vorsorgewirkung



aufwendige Maßnahmen mit hoher Vorsorgewirkung

Einführung

CoC ITA

Kenngrößen (1)

MTBF = „Mean Time Before Failure“

Mittlerer Zeitabstand zwischen dem Auftreten zweier aufeinander folgender Fehler

MTTR = „Mean Time To Repair“

Mittlerer Zeitbedarf für Erkennung, Diagnose, Reparatur, Inbetriebnahme

Systemverfügbarkeit $$A = \frac{MTBF}{MTBF + MTTR}$$

Einführung

Kenngrößen (2)

CoC ITA

Verfügbarkeit	entsprechende Downtime
99%	3,6 Tage Ausfall/Jahr
99,9%	8,76 Stunden Ausfall/Jahr
99,99%	52 Minuten Ausfall/Jahr
99,999%	5 Minuten Ausfall/Jahr
99,9999%	30 Sekunden Ausfall/Jahr
99,99999%	3 Sekunden Ausfall/Jahr

Einführung

Kriterien und Einflussfaktoren

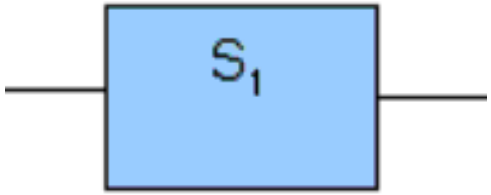
CoC ITA

- Hardware der beteiligten Systeme
- Software der beteiligten Systeme
- Gebäudetechnik im RZ
  - Klimaanlage im RZ, Unterbrechungsfreie Stromversorgung, Zugangskontrolle
- Verbindungen zwischen hochverfügbaren Systemen
  - LAN, SAN, WAN
- Sicherheit
  - Firewall, Virenschutz, Patch-Management
- Administration
  - Kompetenz + Vertrauenswürdigkeit der Administratoren

Einführung

CoC ITA

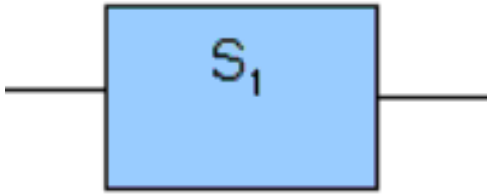
Berechnung der Verfügbarkeit (1)



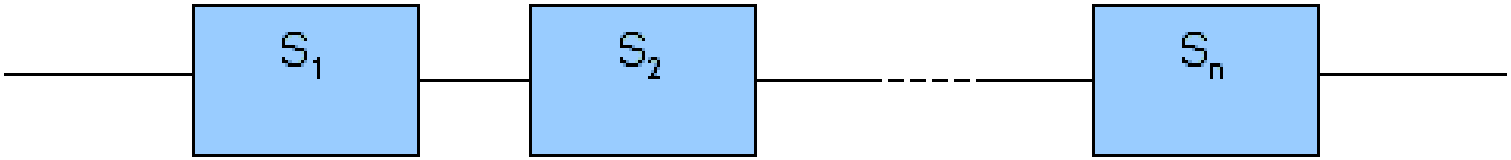
$$A_1 = \frac{MTBF}{MTBF + MTTR}$$

Einführung

Berechnung der Verfügbarkeit (2)



$$A_1 = \frac{MTBF}{MTBF + MTTR}$$

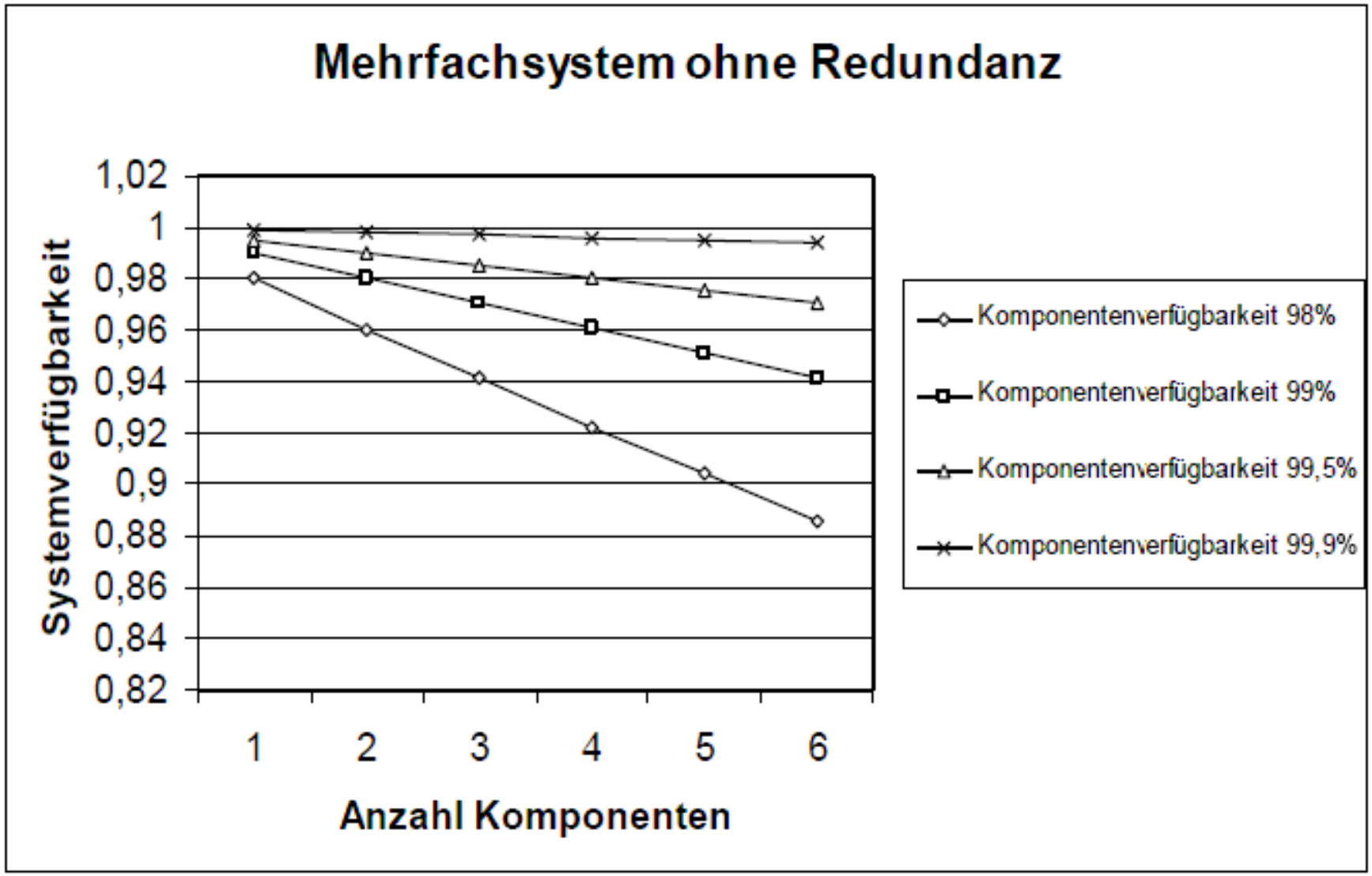


$$A_{ges} = A_1 \bullet A_2 \bullet \ldots \bullet A_n$$

Einführung

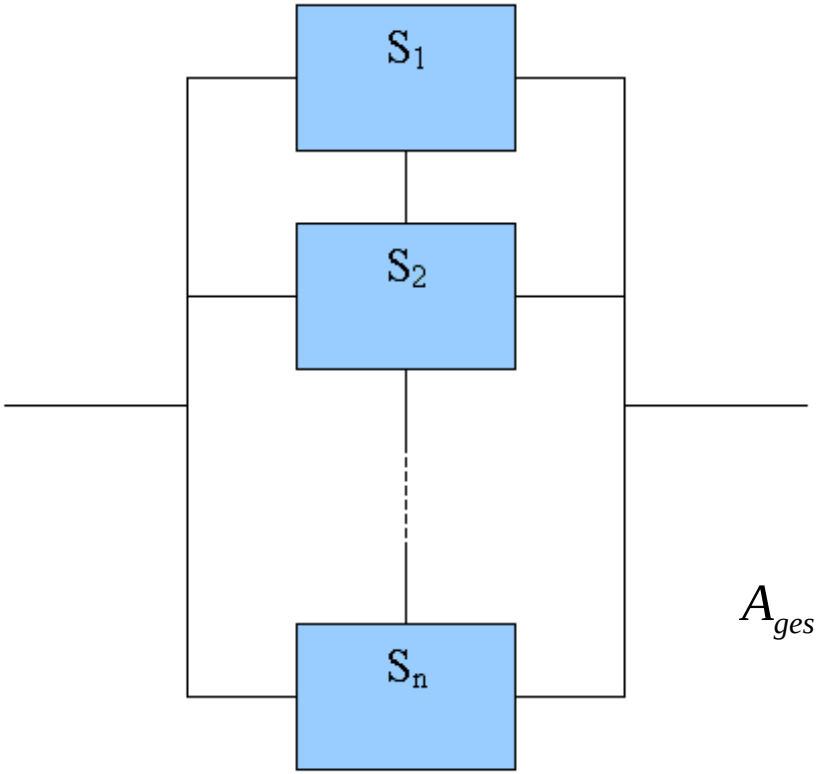
CoC ITA

Berechnung der Verfügbarkeit (3)



Einführung

Berechnung der Verfügbarkeit (4)

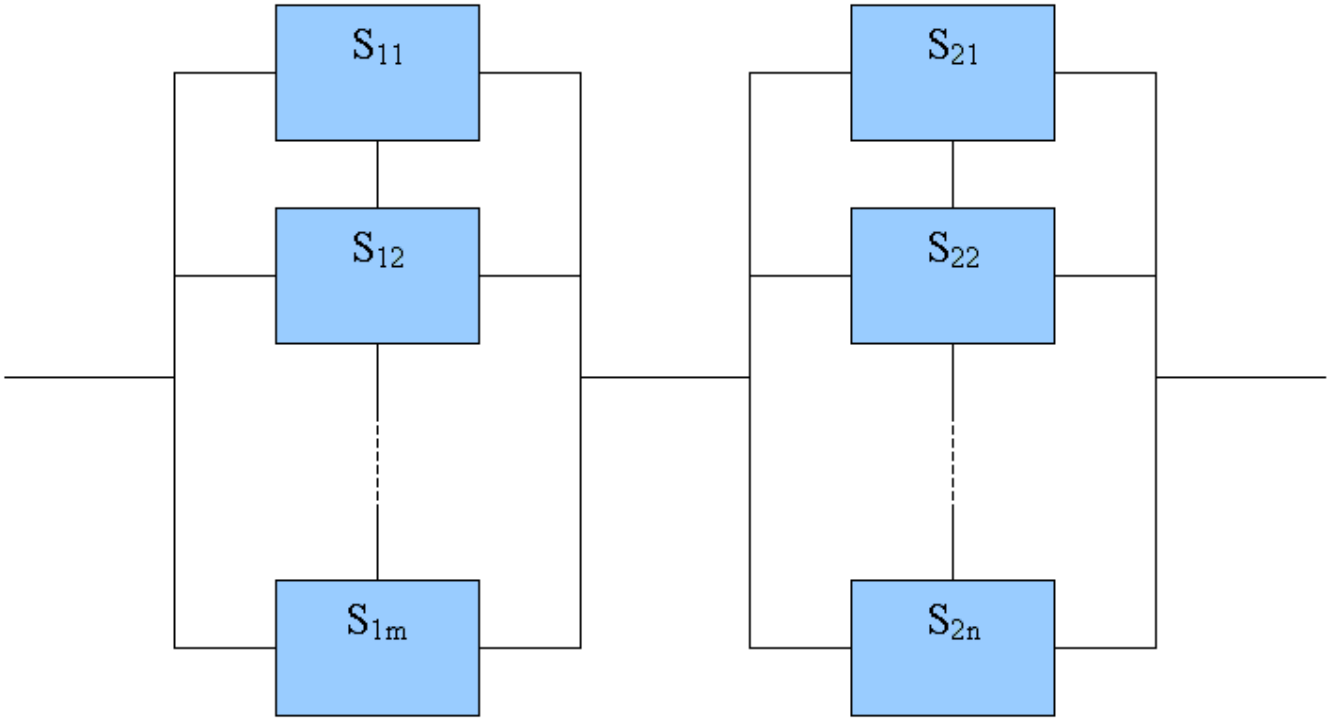


$$A_{ges} = 1 - (1 - A_1) \bullet (1 - A_2) \bullet \ldots \bullet (1 - A_n)$$

Einführung

CoC ITA

Berechnung der Verfügbarkeit (5)

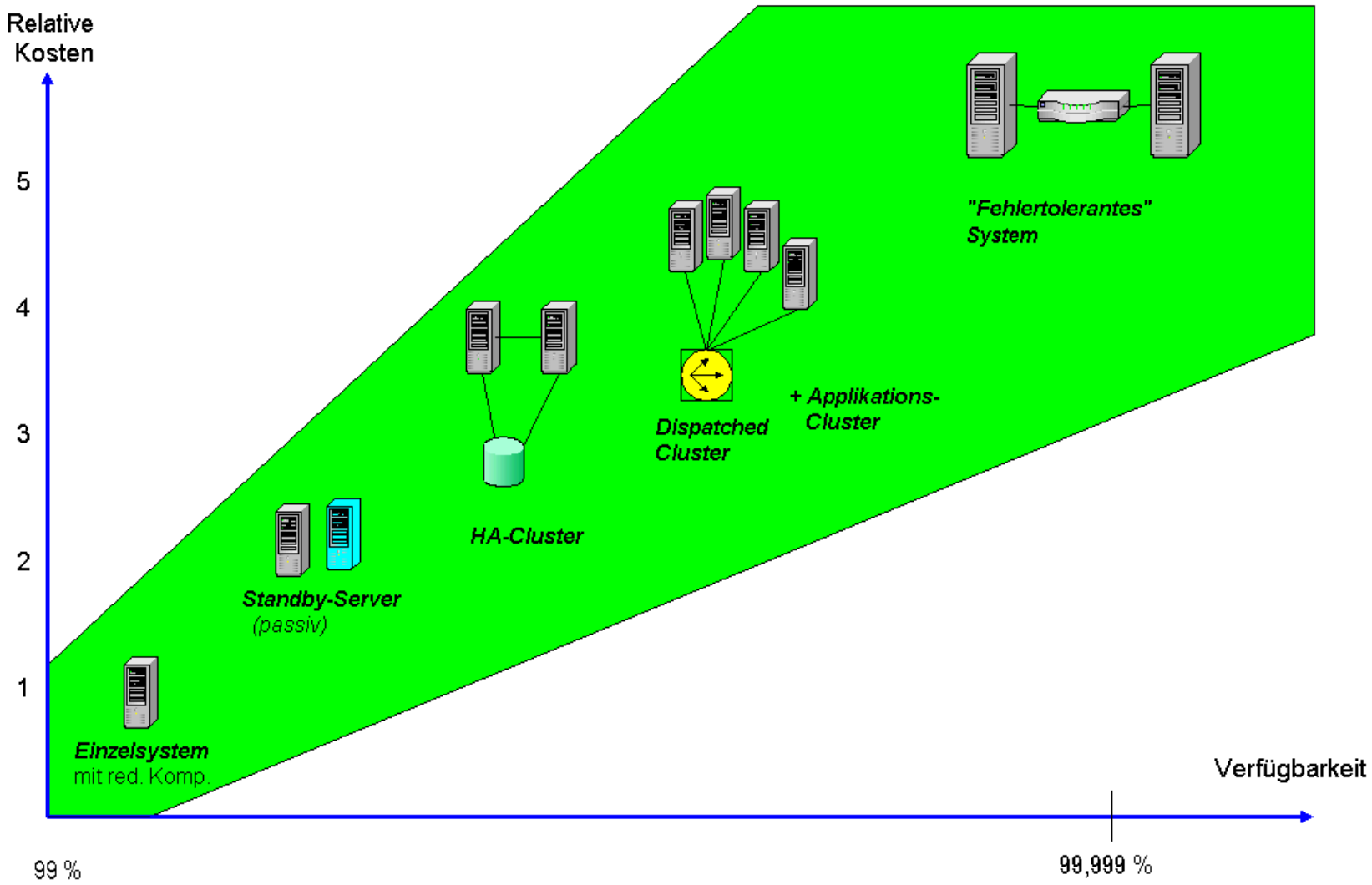


$$A_{ges} = A_{1ges} \bullet A_{2ges}$$

$$A_{ges} = (1-(1-A_{11}) \bullet (1-A_{12}) \bullet \ldots \bullet (1-A_{1n})) \bullet (1-(1-A_{21}) \bullet (1-A_{22}) \bullet \ldots \bullet (1-A_{2n}))$$

Einordnung verschiedener HV-Technologien

CoC ITA



Einzelsystem mit redundanten Komponenten Beispiele

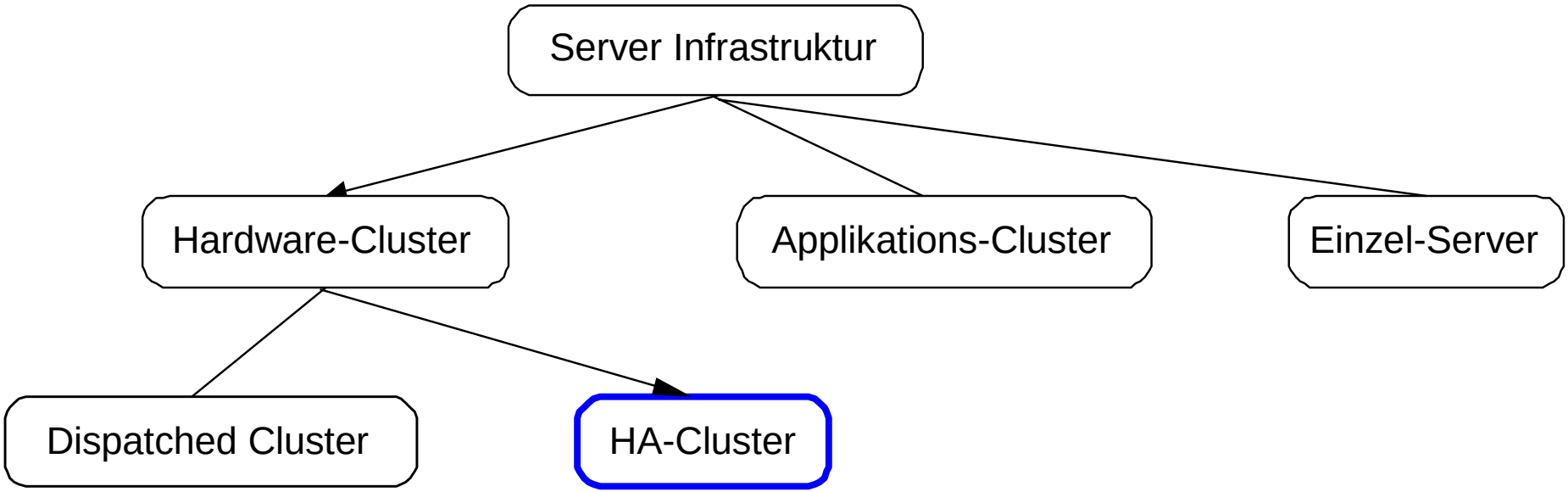
CoC ITA

- **Server**
  Redundante Netzteile, Lüfter, NICs, HBAs, ECC-Speicher

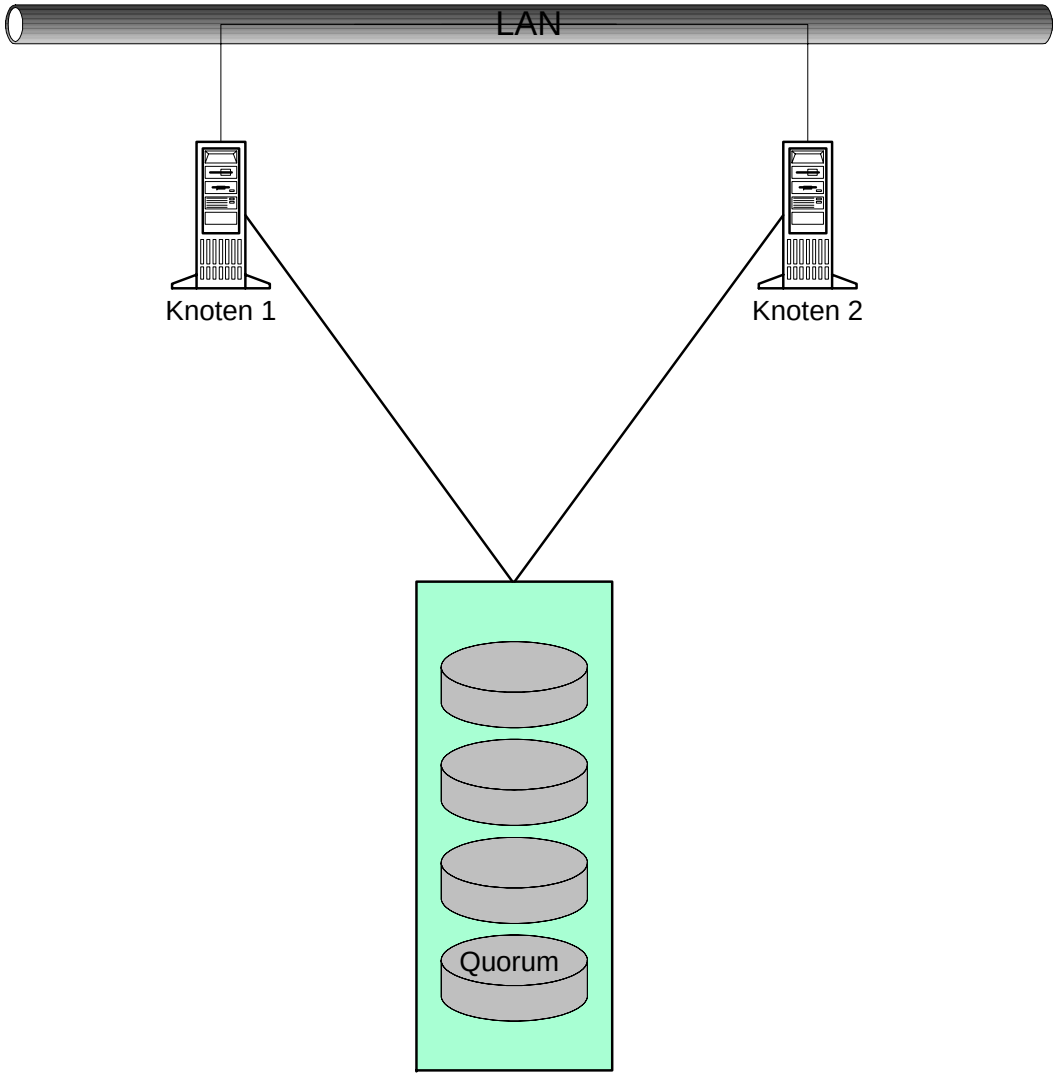
- **Plattenspeichersysteme**
  RAID+ Hot Spare
  Redundante Stromversorgung
  Redundante Controller mit gespiegelten Caches
  Redundante Datenpfade
  Konfigurationsänderungen im „Online-Betrieb“
  Erweiterungen bzw. Austausch von Komponenten im „Online-Betrieb“
  Unterbrechungsfreie Firmware Updates (mit Rollback-Möglichkeit)

HA-Cluster
Einordnung aus der Sicht der Server-Infrastruktur (BMW-IT)

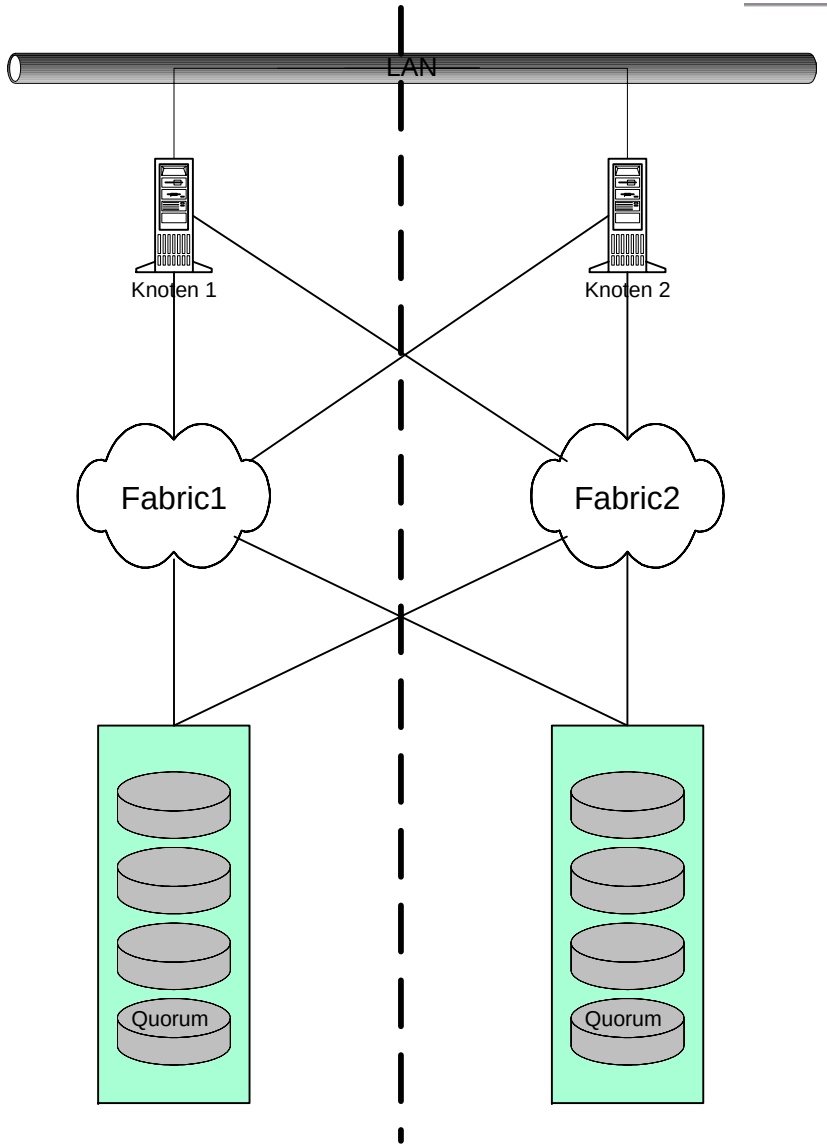
CoC ITA



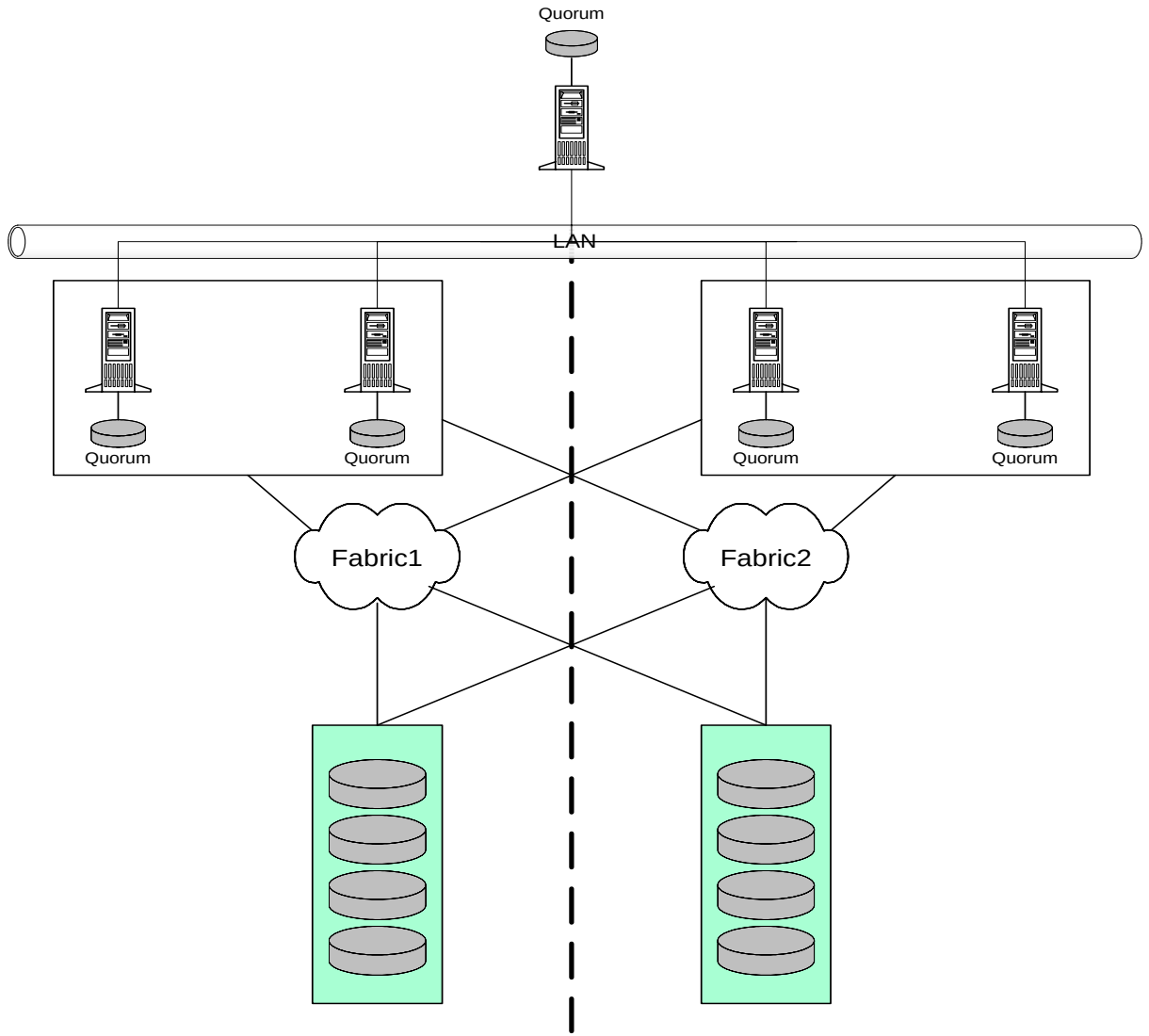
Prinzip des HA-Clusters mit gemeinsamer Quorum



Katastrophensicherer HA-Cluster ohne SPOF



Katastrophensicherer HA-Cluster mit „Majority Node Set Quorum“



Fragen, die beim Einsatz von HA-Clustern geklärt werden sollten (1)

CoC ITA

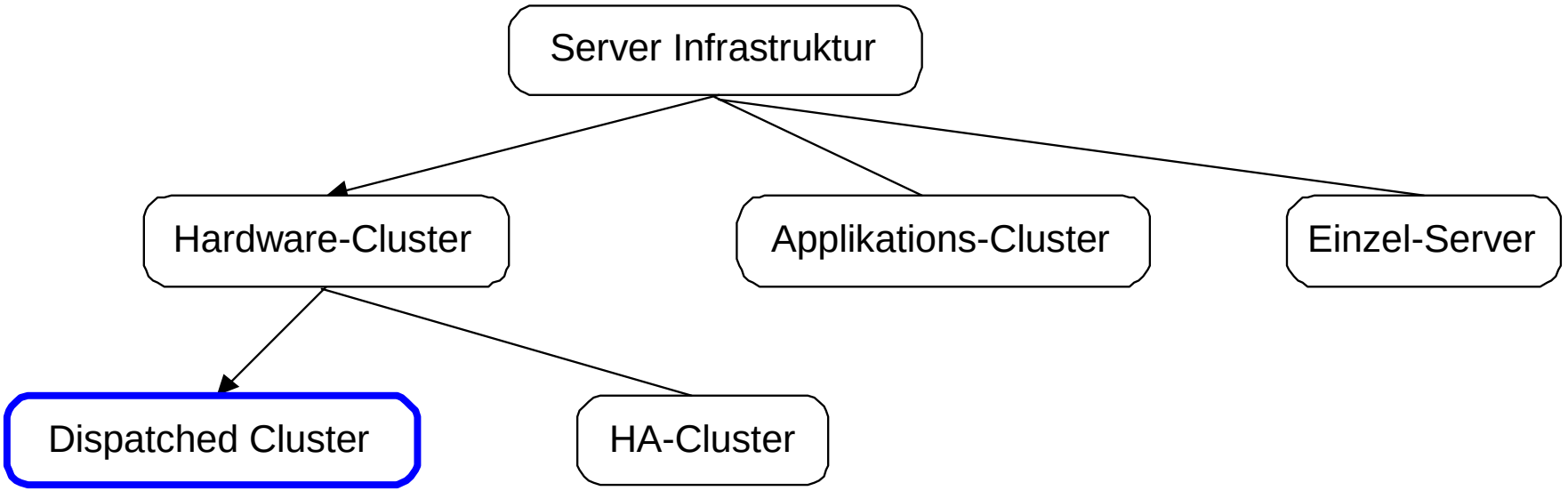
- Sind die Applikationen Cluster tauglich?
  - falls ja, sind spezielle Anpassungen nötig?
- Sind alle wichtigen Fehlerszenarien getestet?
- Können die Administratoren damit umgehen?
  - Gibt es Durchführungsanweisungen?
  - Haben die Administratoren diese Operationen am realen System (Testumgebung) eingeübt?
- Welche Konsequenzen hat ein Failover für die Anwender?
- Sind die Kapazitäten im Fehlerfall ausreichend?

Fragen, die vor dem Einsatz von HA-Clustern geklärt werden sollten (2)

CoC ITA

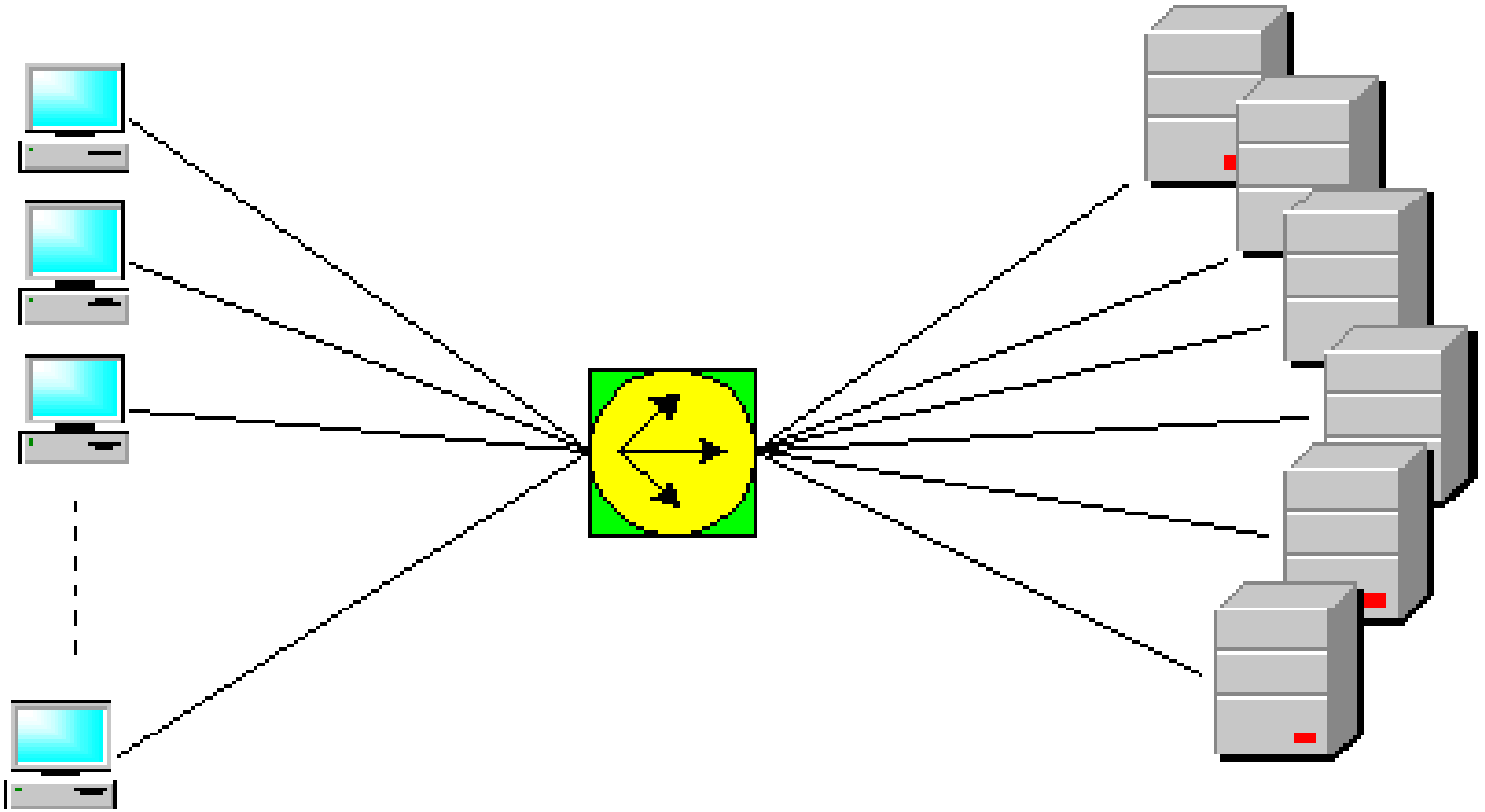
- Sind die ermittelten Failover-Zeiten für die Anwender akzeptabel?
- Gibt es noch SPOFs?
- Sind „Rolling Upgrades“ möglich?
- Wie können weitere Knoten hinzugefügt werden?
- Inwieweit unterstützen die Hersteller die Kombination der eingesetzten Produkte?

Dispatched Cluster
Einordnung aus der Sicht der Server-Infrastruktur (BMW-IT)



Dispatched Cluster

Grundprinzip



Dispatched Cluster

CoC ITA

Funktionsprüfung (Health Check)

- Einfacher PING
- Erreichbarkeit bestimmter Ports
- Gründliche Prüfung der Applikation per Skript

Dispatched Cluster

CoC ITA

Lastprüfung

- Anzahl der Sitzungen
- Anzahl der Sitzungen mit Gewichtung
- Schnellste Antwort
- Agenten auf Cluster-Server
- Kombination aus obigen Verfahren

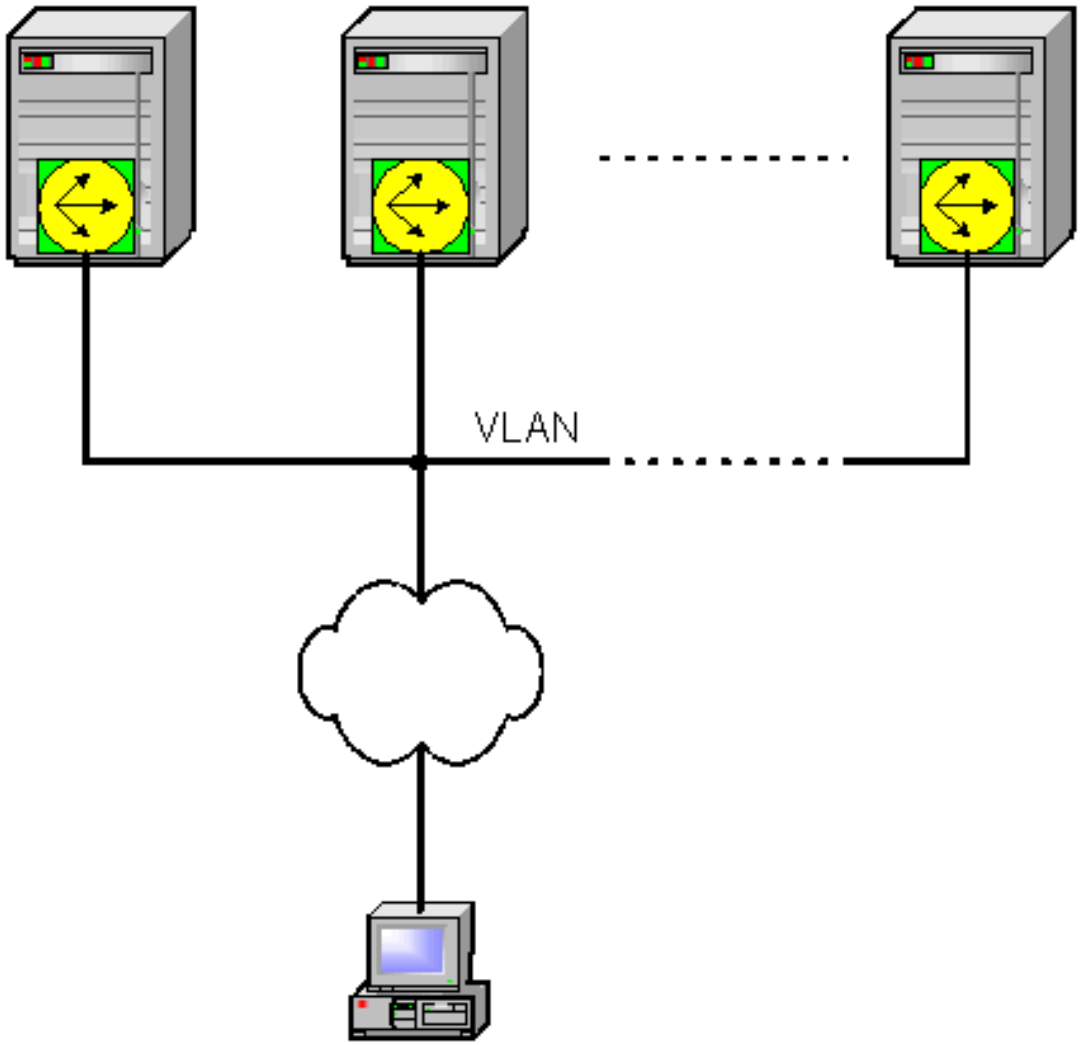
Dispatched Cluster

CoC ITA

Persistenz (Affinität, Persistancy, Stickiness)

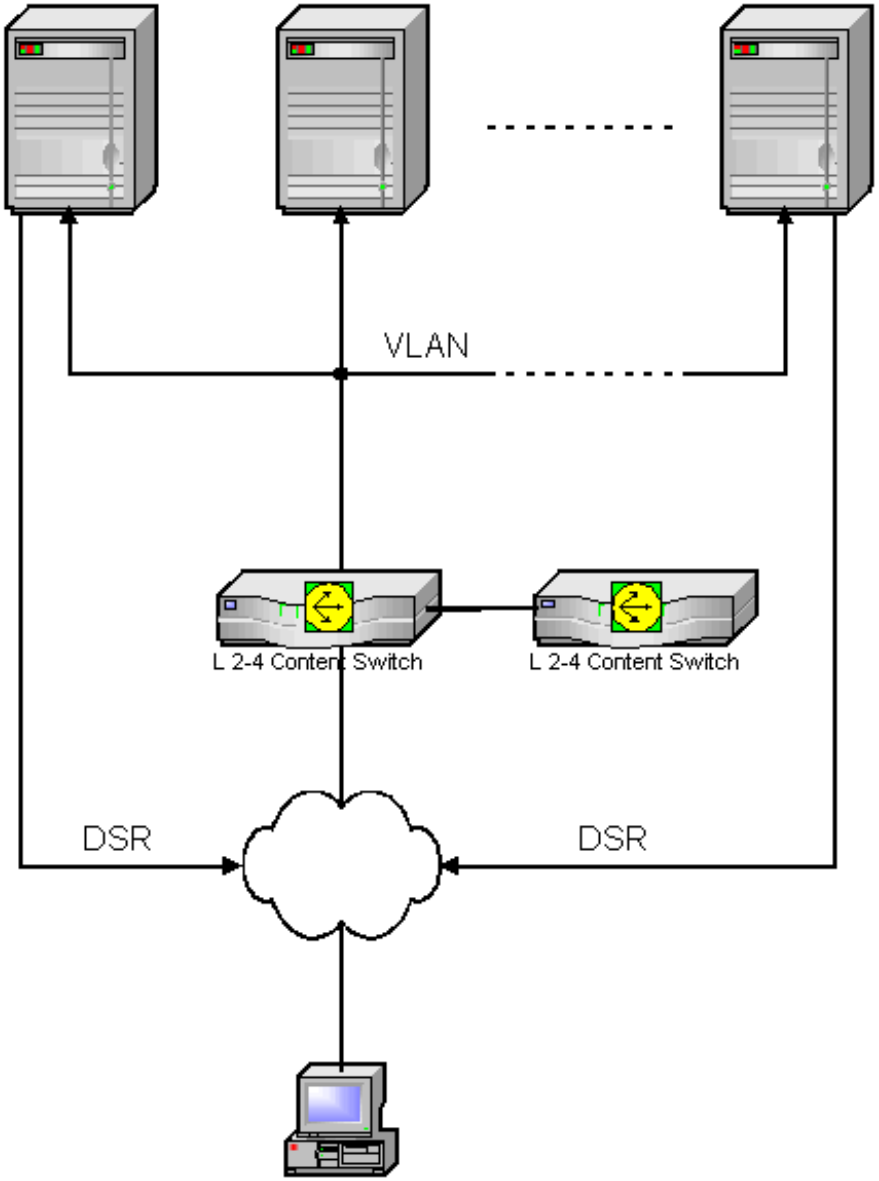
- Layer-3-Persistenz
- URL-Variablen-Persistenz
- Cookie-Persistenz
- SSL-Sitzungspersistenz

Dispatched Cluster mit Software Load Balancing



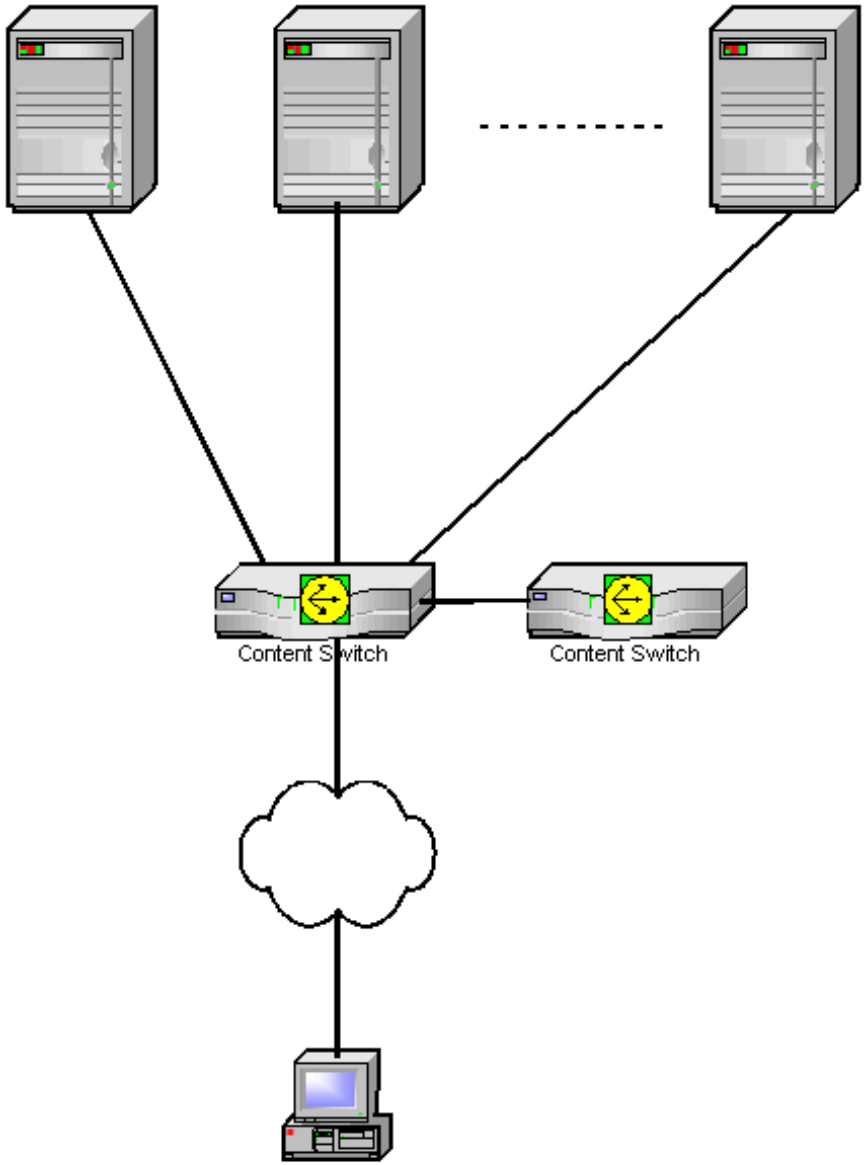
Dispatched Cluster mit HW-LV und „Direct Server Return“ (DSR)

CoC ITA



Dispatched Cluster mit NAT

CoC ITA



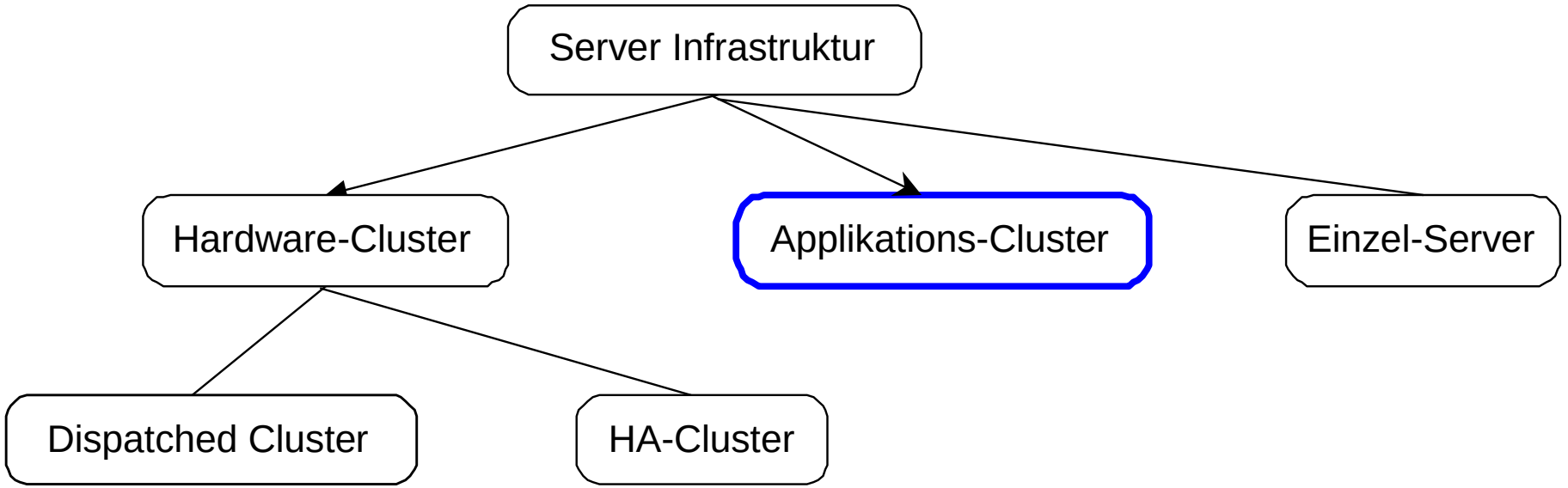
Gegenüberstellung
HA-Cluster / Dispatched Cluster

CoC ITA

HA-Cluster	Dispatched Cluster
Nur jeweils 1 Instanz (Ressource) aktiv, z.B. Datenbank-System, eMail-System	Mehrere Instanzen gleichzeitig aktiv, z.B. Frontend-Server für Web
Failover beansprucht Zeit für kontrolliertes Beenden u. Hochfahren von Ressourcen	Schneller Wechsel durch Umleitung
I.d.R. gemeinsamer Speicher mit SCSI- bzw. iSCSI-Schnittstelle erforderlich	I.d.R. genügt lokaler Speicher (aber Persistenz von Sitzungen nötig)
Wenig flexibel, starke Abhängigkeit der Komponenten	Sehr flexibel, leichte Austauschbarkeit der Komponenten
Relativ kompliziert (Split Brain Problematik, Abhängigkeit von Ressourcen etc.)	Einfacher zu implementieren, leichter erweiterbar, aber mehr Netzwerk Know-how erforderlich

Applikations-Cluster
Einordnung aus der Sicht der Server-Infrastruktur (BMW-IT)

CoC ITA



Applikations-Cluster

Beispiele

CoC ITA

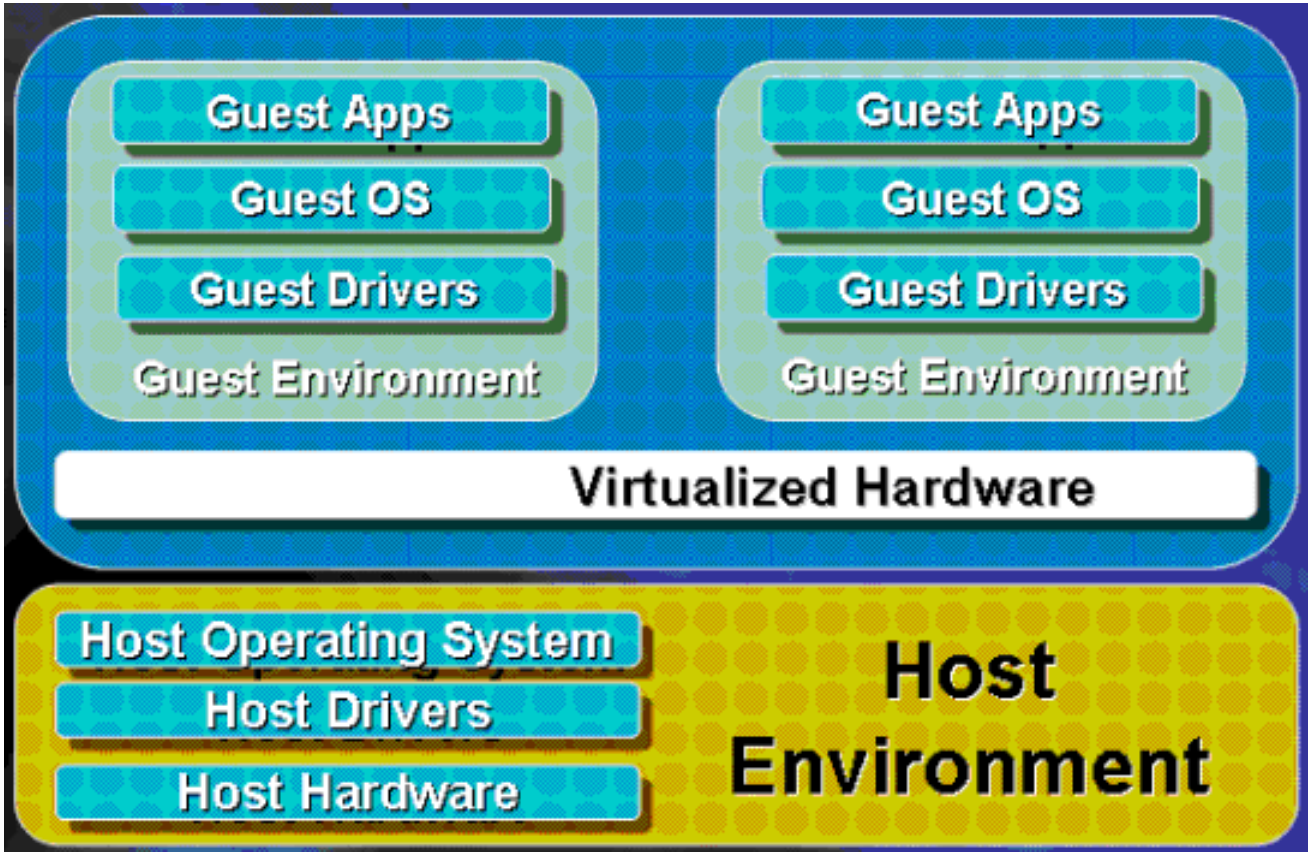
Beim Applikations-Cluster sorgt die Applikations selbst für die Hochverfügbarkeit der Server.

1. Beispiel: „Citrix Terminal Service“

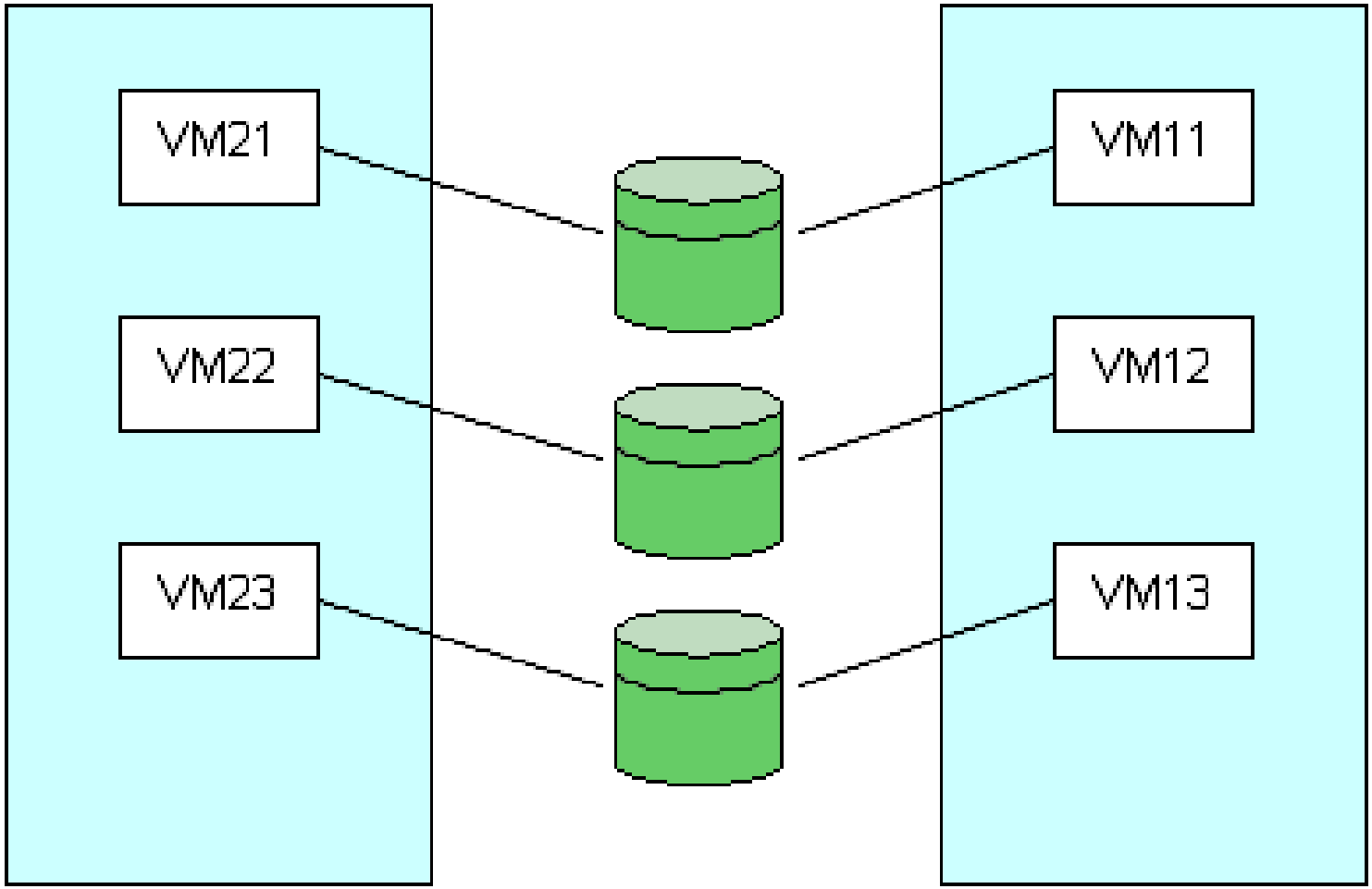
2. Beispiel: „Microsoft Active Directory“

Nicht selten gibt es bei Applikations-Clustern „Single Master Rollen“, die mit klassischen HV-Technologien hochverfügbar gemacht werden müssen.

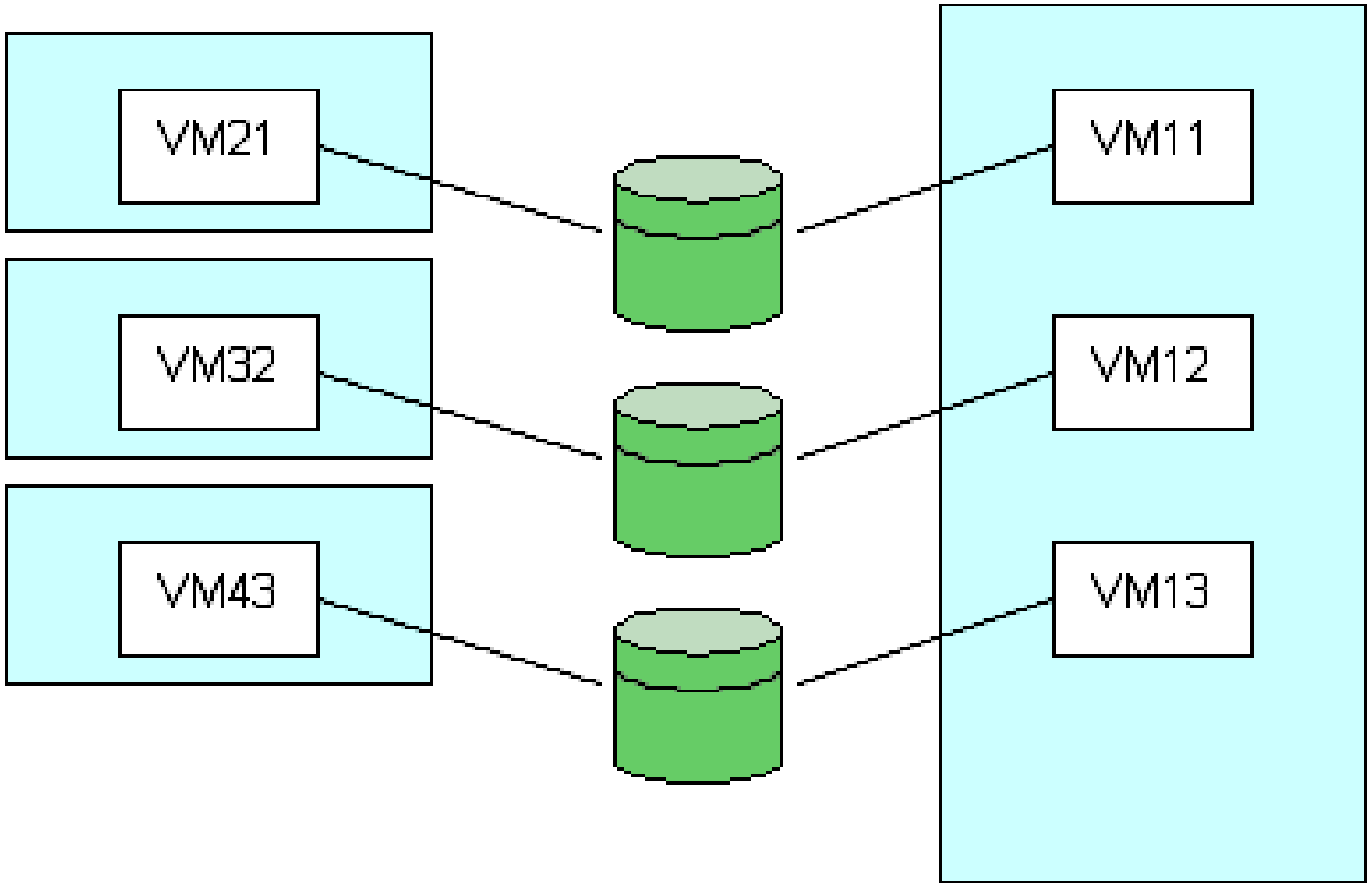
HV mit „virtuellen Maschinen“ (1)



HV mit „virtuellen Maschinen“ (2)



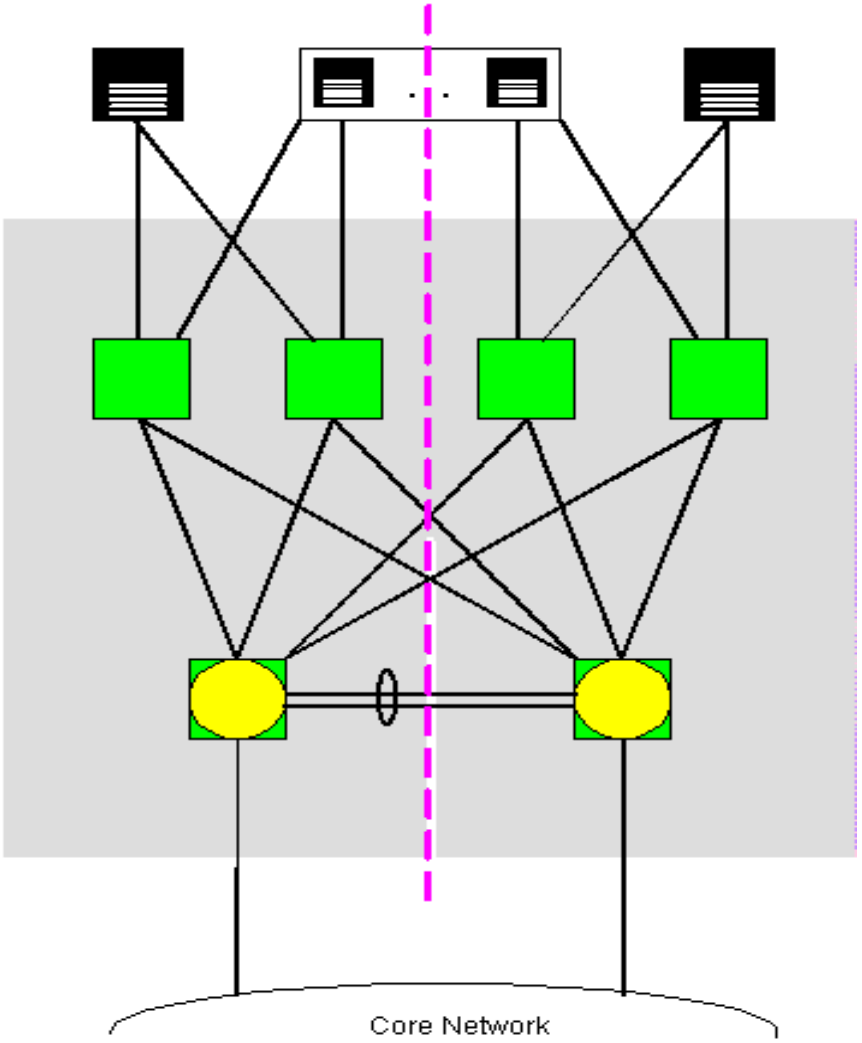
HV mit „virtuellen Maschinen“ (3)



Hochverfügbare Netze

CoC ITA

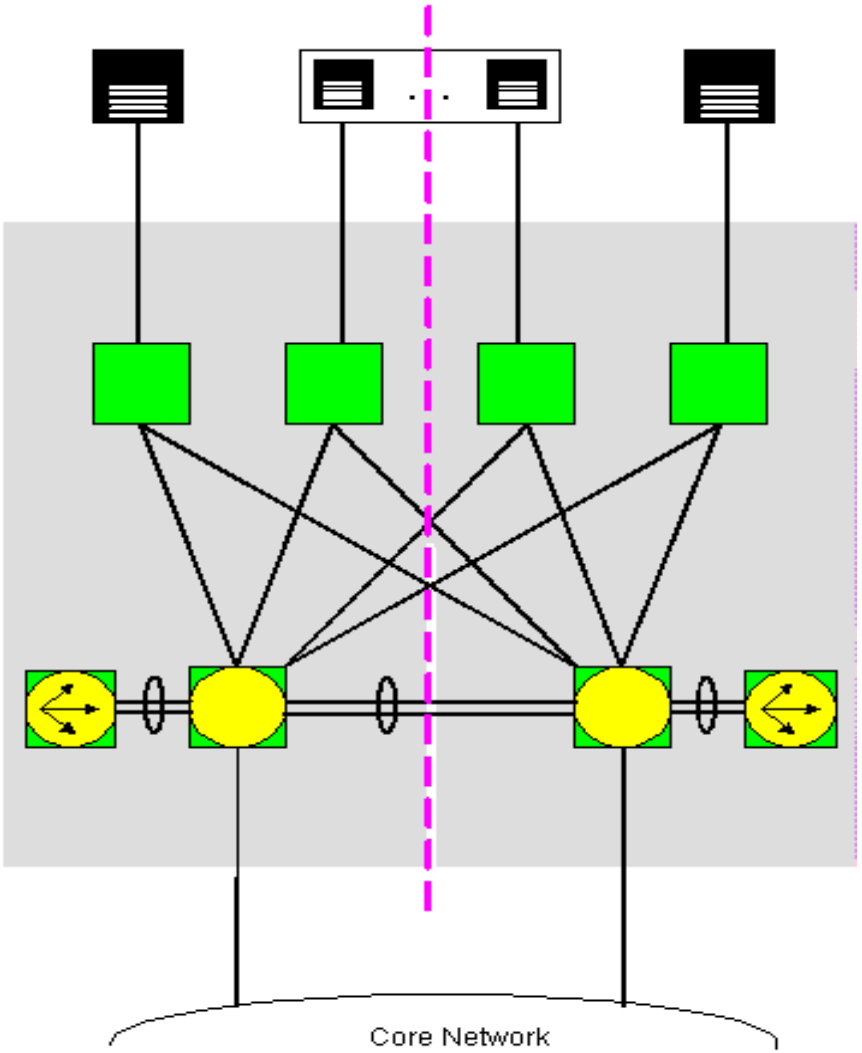
Struktur B ohne Lastverteiler



Hochverfügbare Netze

CoC ITA

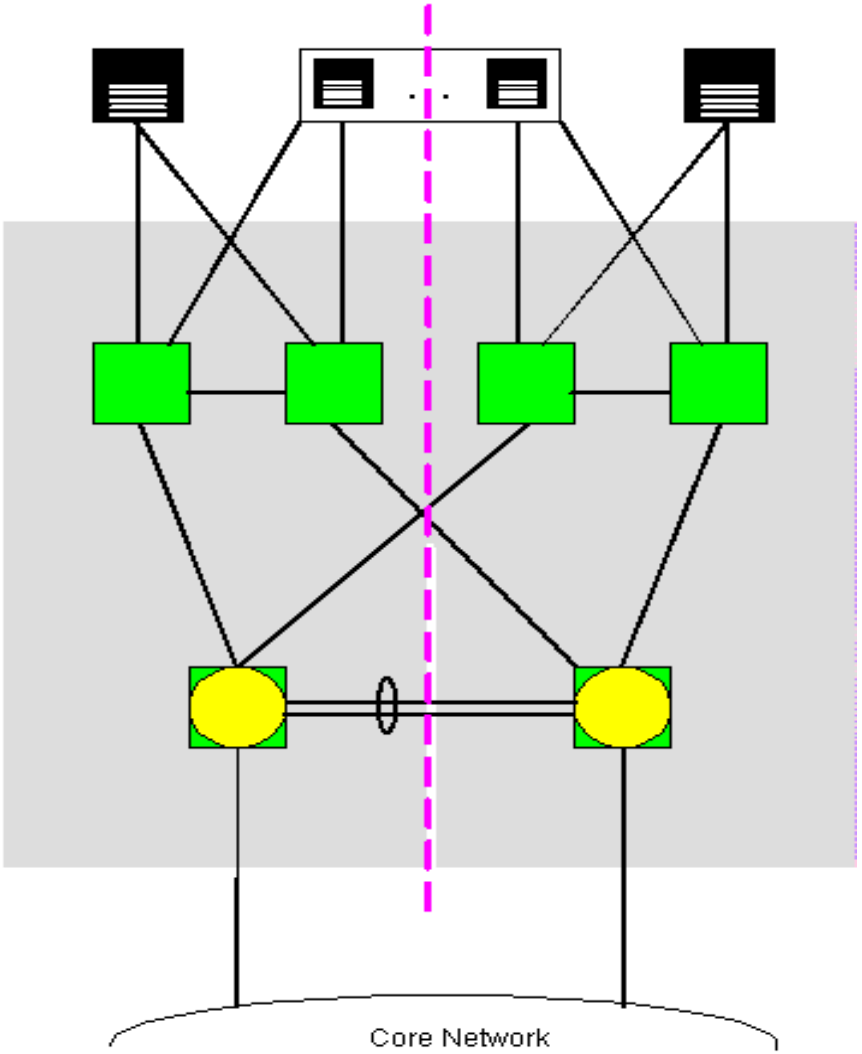
Struktur B mit Lastverteiler



Hochverfügbare Netze

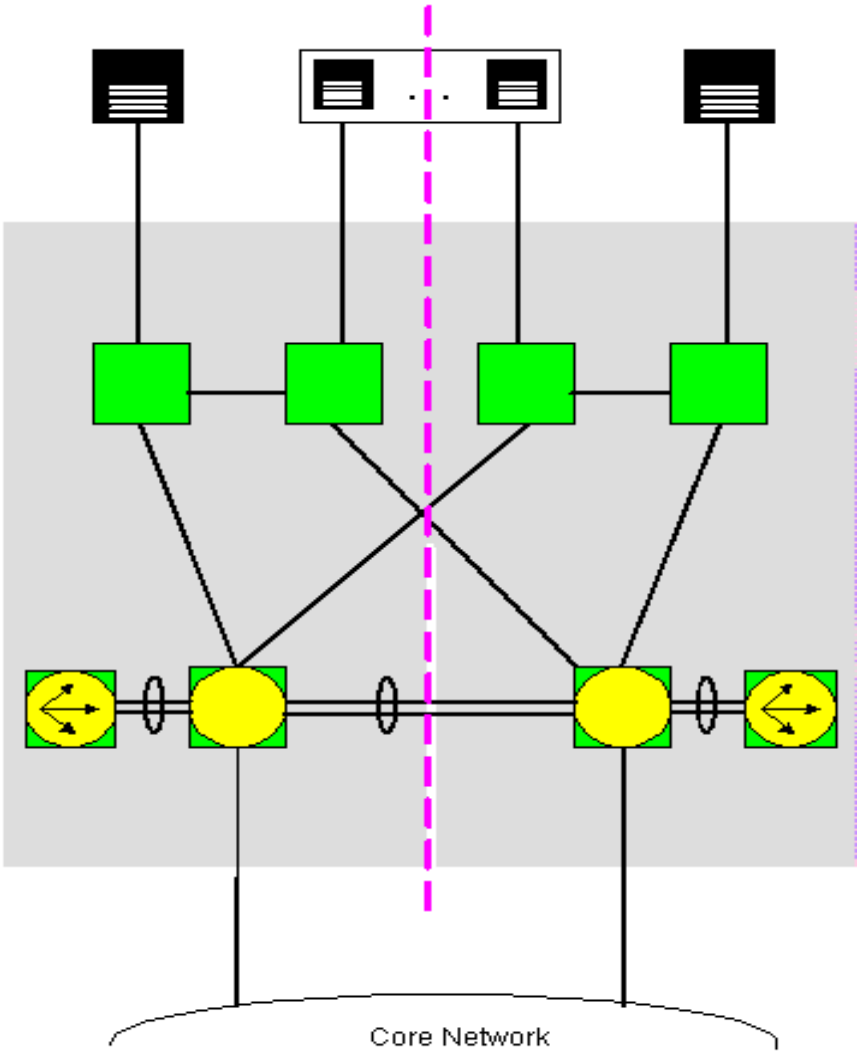
CoC ITA

Struktur C ohne Lastverteiler



Hochverfügbare Netze

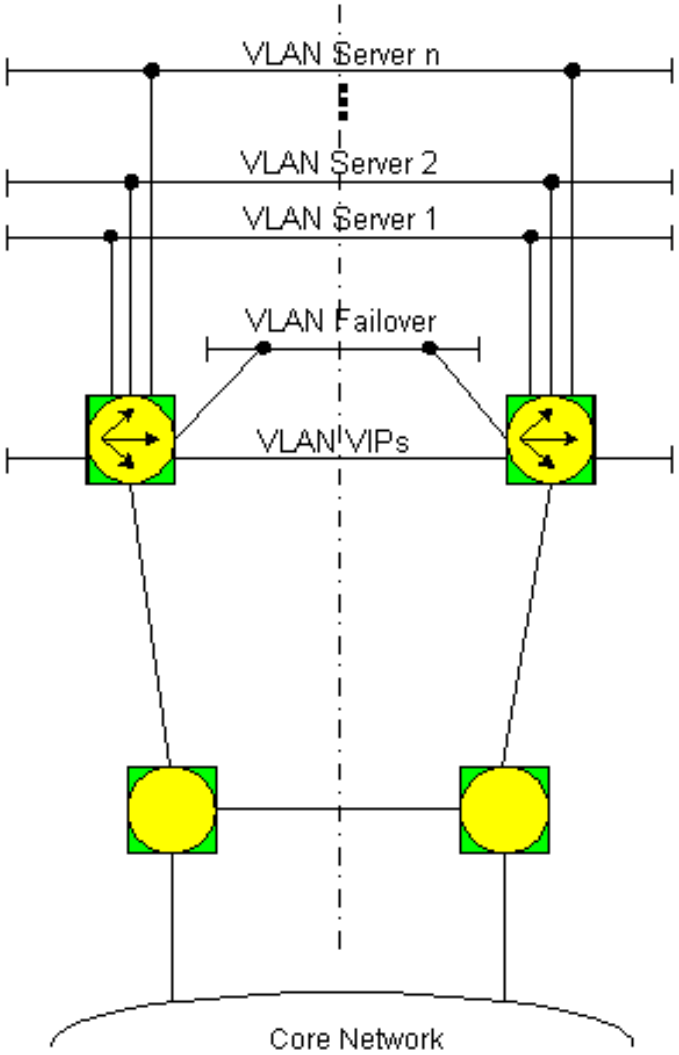
Struktur C mit Lastverteiler



Hochverfügbare Netze

CoC ITA

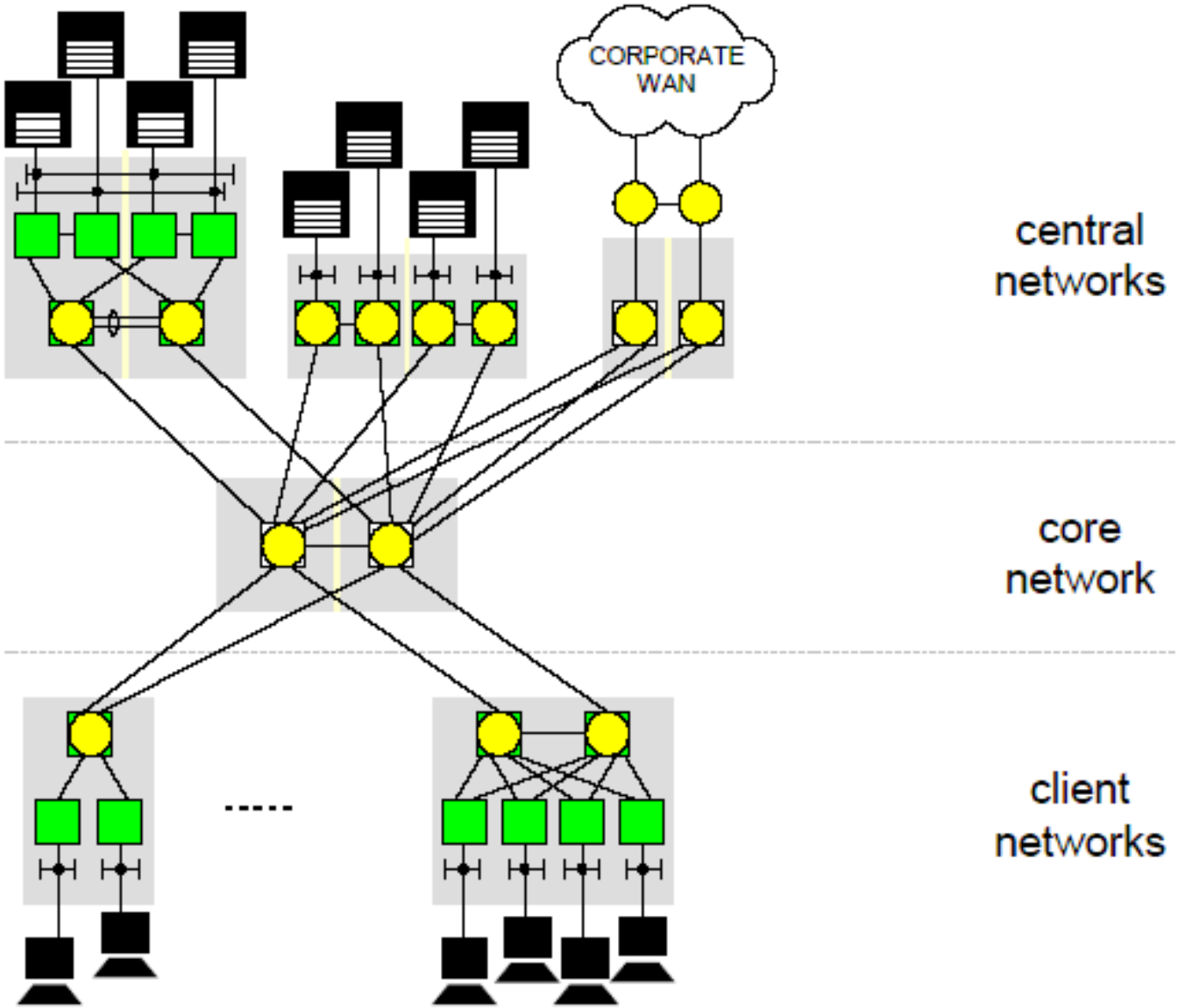
Logische Sicht der Strukturen B und C



Hochverfügbare Netze

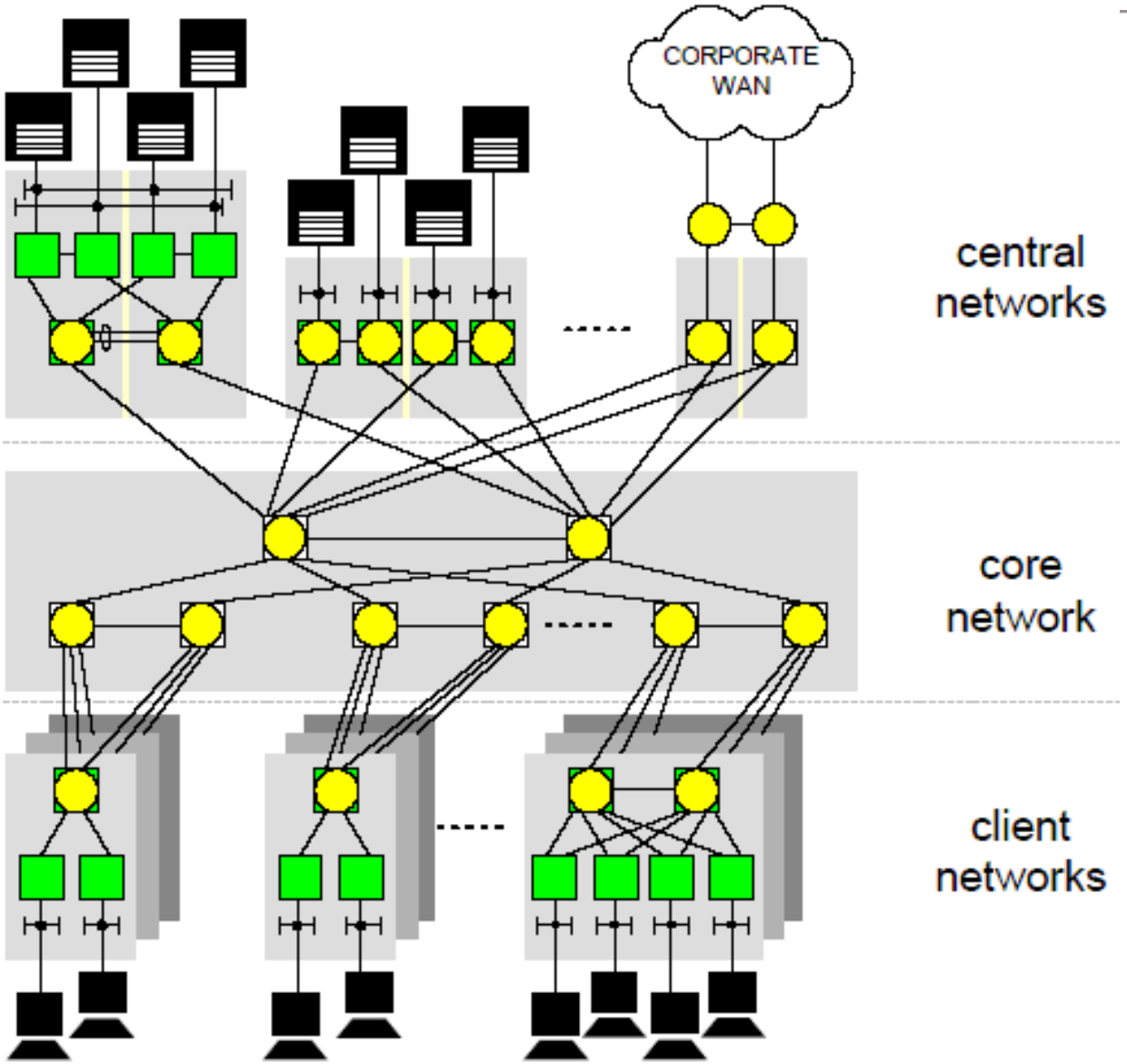
CoC ITA

Gesamtstruktur (1)



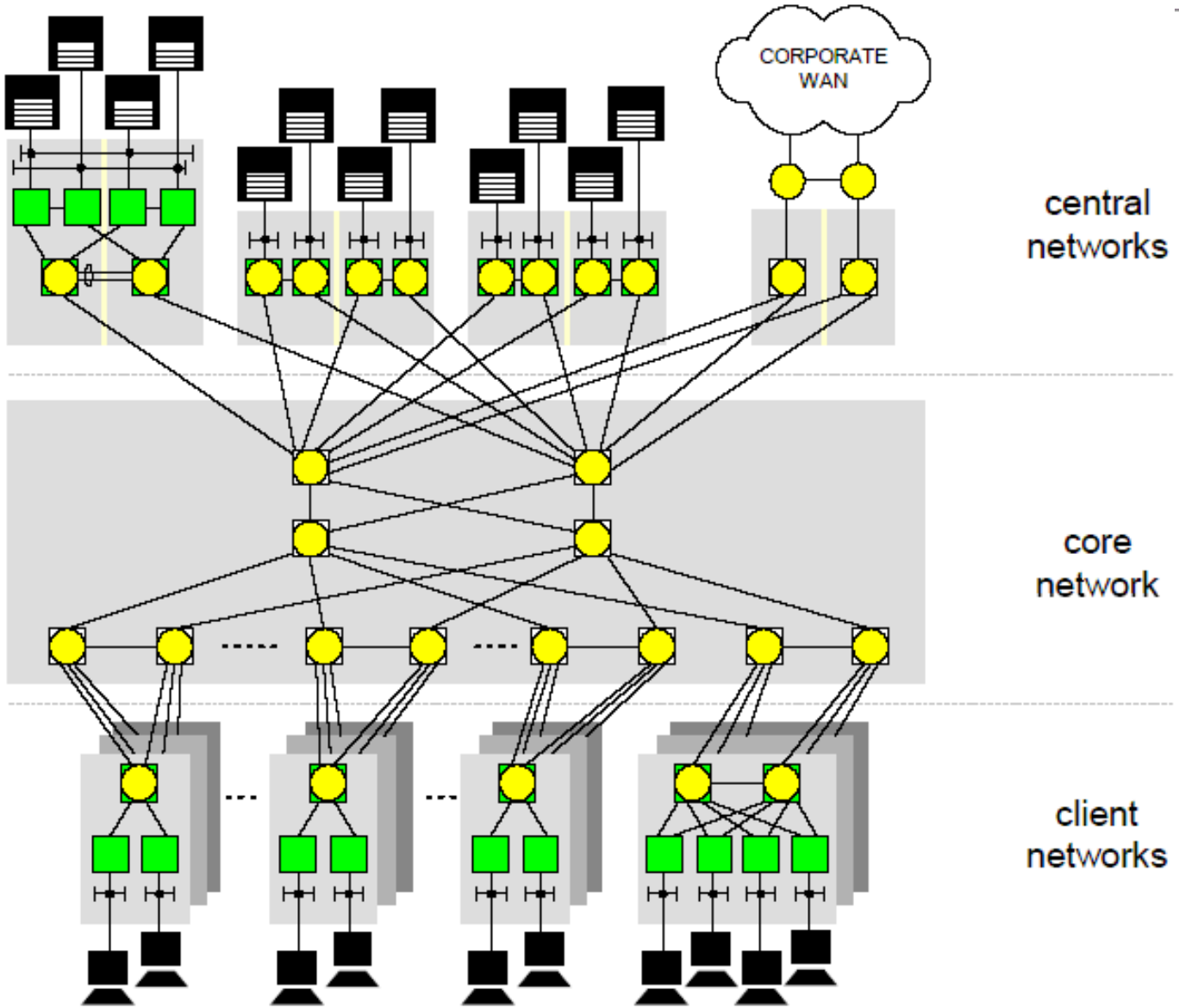
Hochverfügbare Netze

Gesamtstruktur (2)



Hochverfügbare Netze

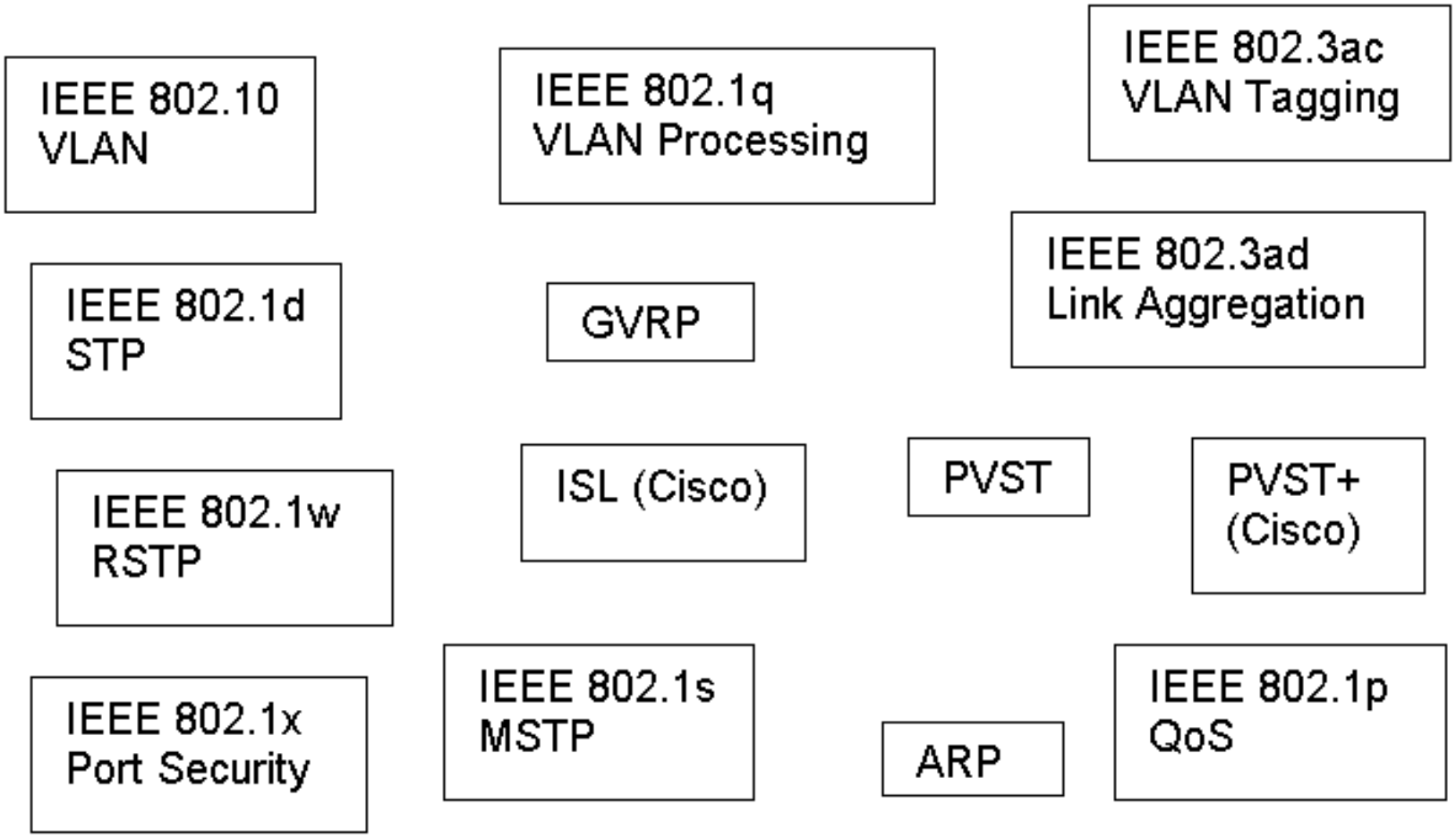
Gesamtstruktur (3)



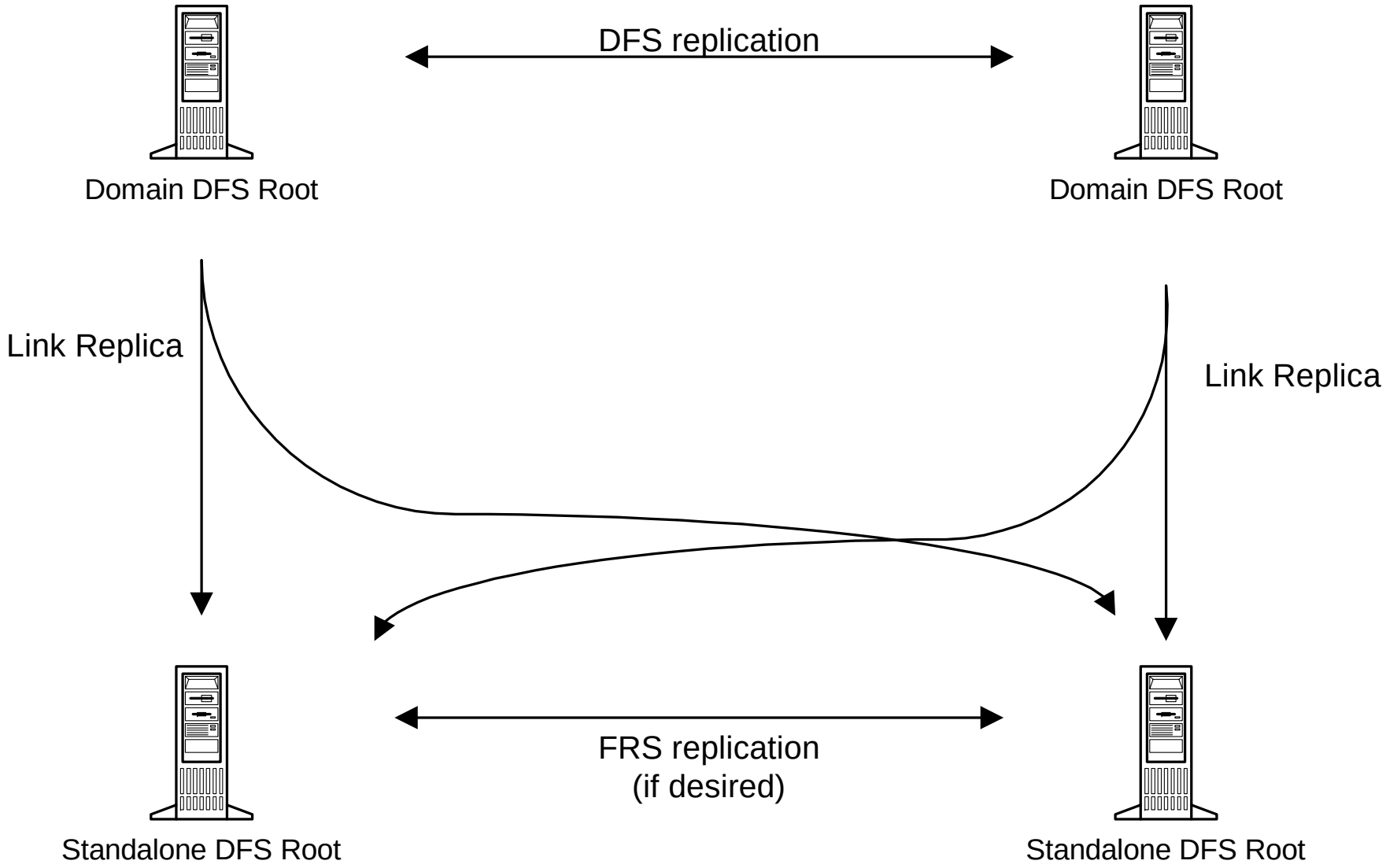
Hochverfügbare Netze

CoC ITA

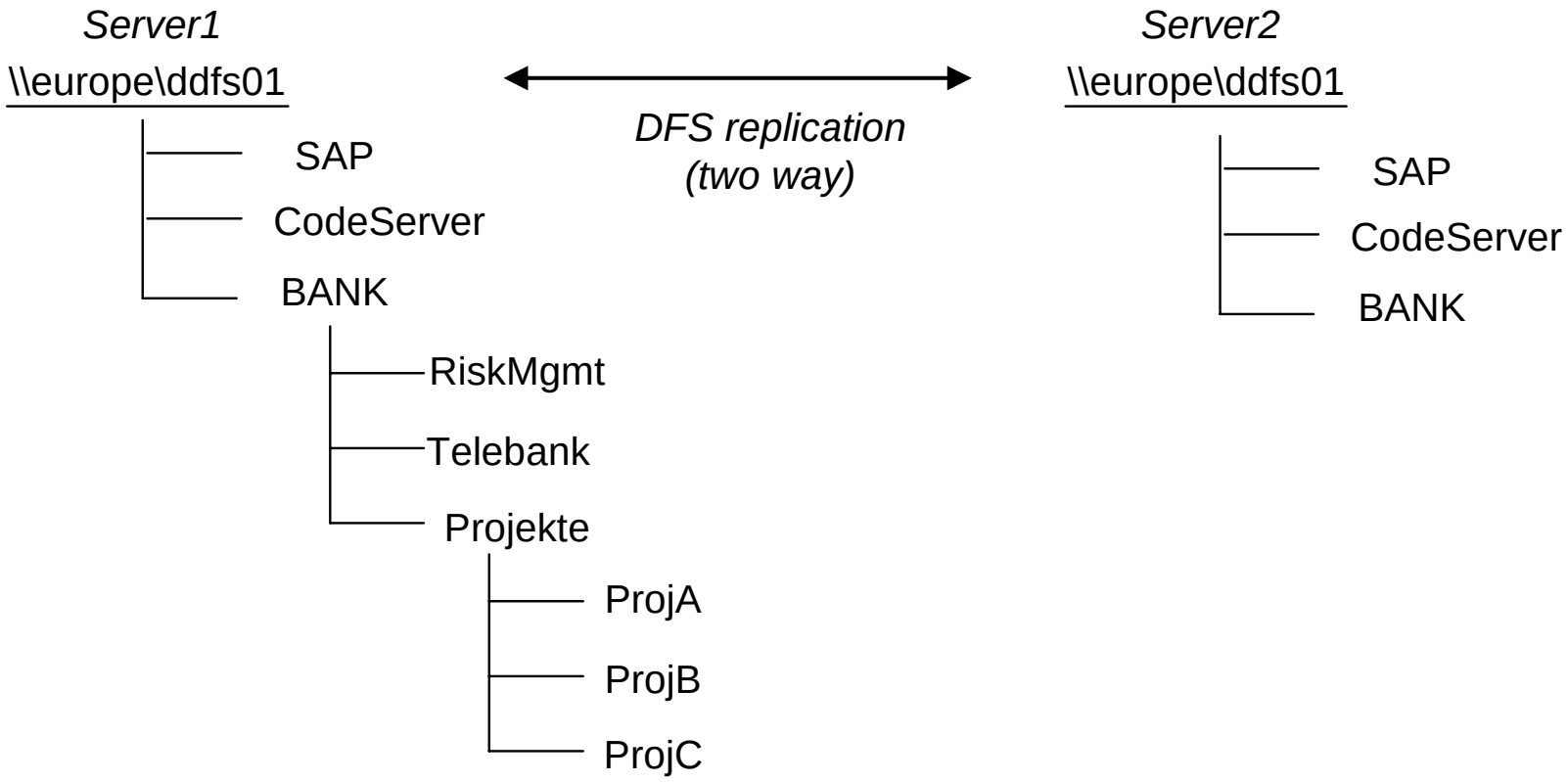
Layer 2 Protokolle und Standards (Auszug)



Distributed File System (DFS)



Distributed File System (2)



Gefährdung der Hochverfügbarkeit durch Software-Probleme Gegenmaßnahmen

CoC ITA

- Qualitätssicherung
- Checkpoint-Technologien
- Nutzung der SnapShot-Technologie
- Systems-Management zur Früherkennung von Problemen

Hochverfügbarkeitstechnologien

Zusammenfassung / Ratschläge

CoC ITA

- „Ganzheitliche“ Betrachtung
- Anforderungsanalyse – Vorauswahl – Test - Entscheidung
- Simulation von Ausfallszenarien
- Dokumentation
- Faktor „Mensch“

Hochverfügbarkeitstechnologien

CoC ITA

Fragen?

Zusatzinformationen

CoC ITA

Availability Environment Classification (AEC)

Klassifizierung nach der Harvard Research Group

Conventional (AEC-0):
Funktion kann unterbrochen werden, Datenintegrität ist nicht essentiell;

Highly Reliable (AEC-1):
Funktion kann unterbrochen werden, Datenintegrität muss jedoch gewährleistet sein;

High Availability (AEC-2):
Funktion darf nur minimal unterbrochen werden, das gilt entweder für festgelegte Zeiten oder zu den Hauptbetriebszeiten;

Fault Resilient (AEC-3):
Funktion muss ununterbrochen aufrecht erhalten werden, dito;

Fault Tolerant (AEC-4):
Funktion muss ununterbrochen aufrecht erhalten werden (24x7);

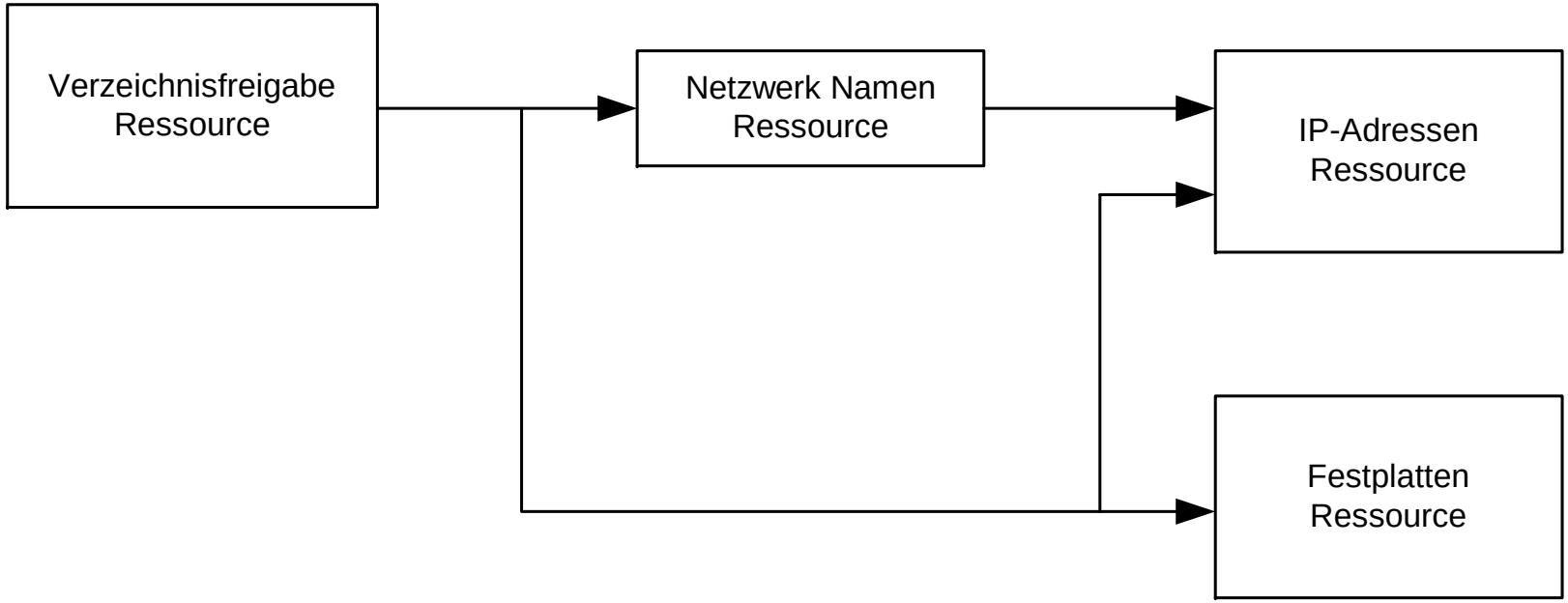
Disaster Tolerant (AEC-5):
Funktion muss unter allen Umständen verfügbar sein

Zusatzinformationen

CoC ITA

Abhängigkeit von Cluster-Ressourcen

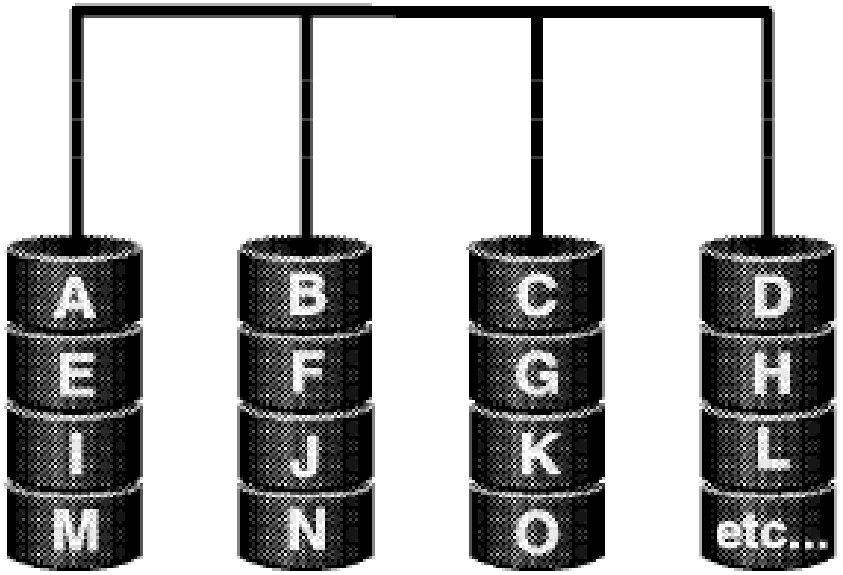
Beispiel Verzeichnisfreigabe



Zusatzinformationen

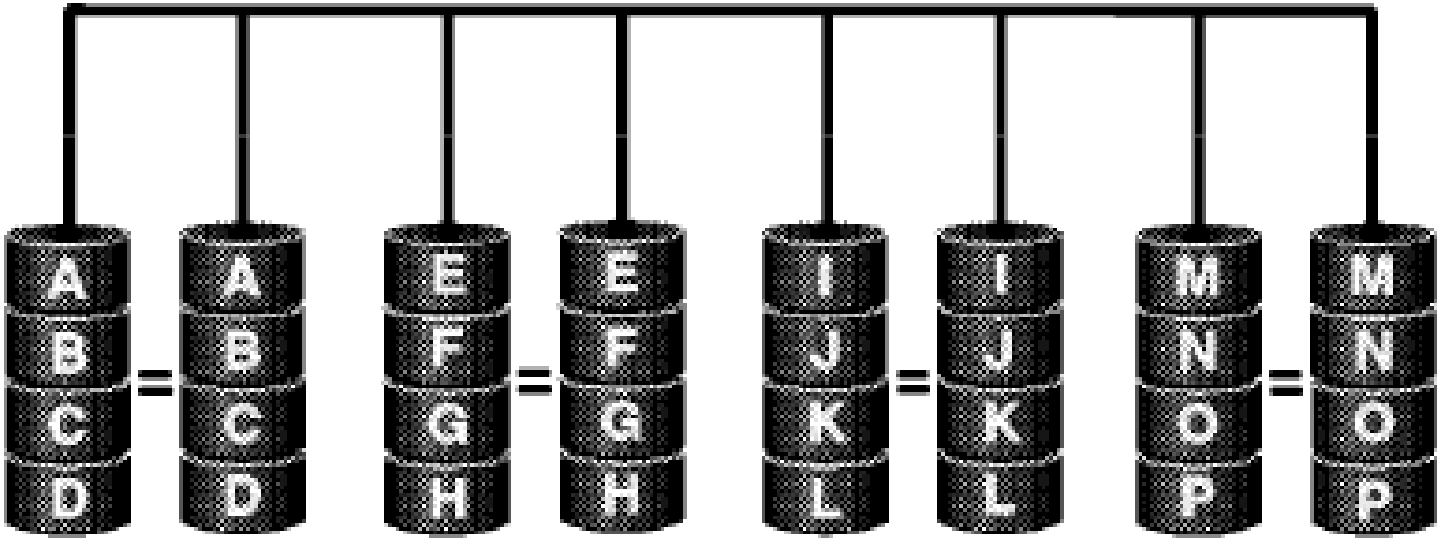
CoC ITA

Raid 0



Zusatzinformationen

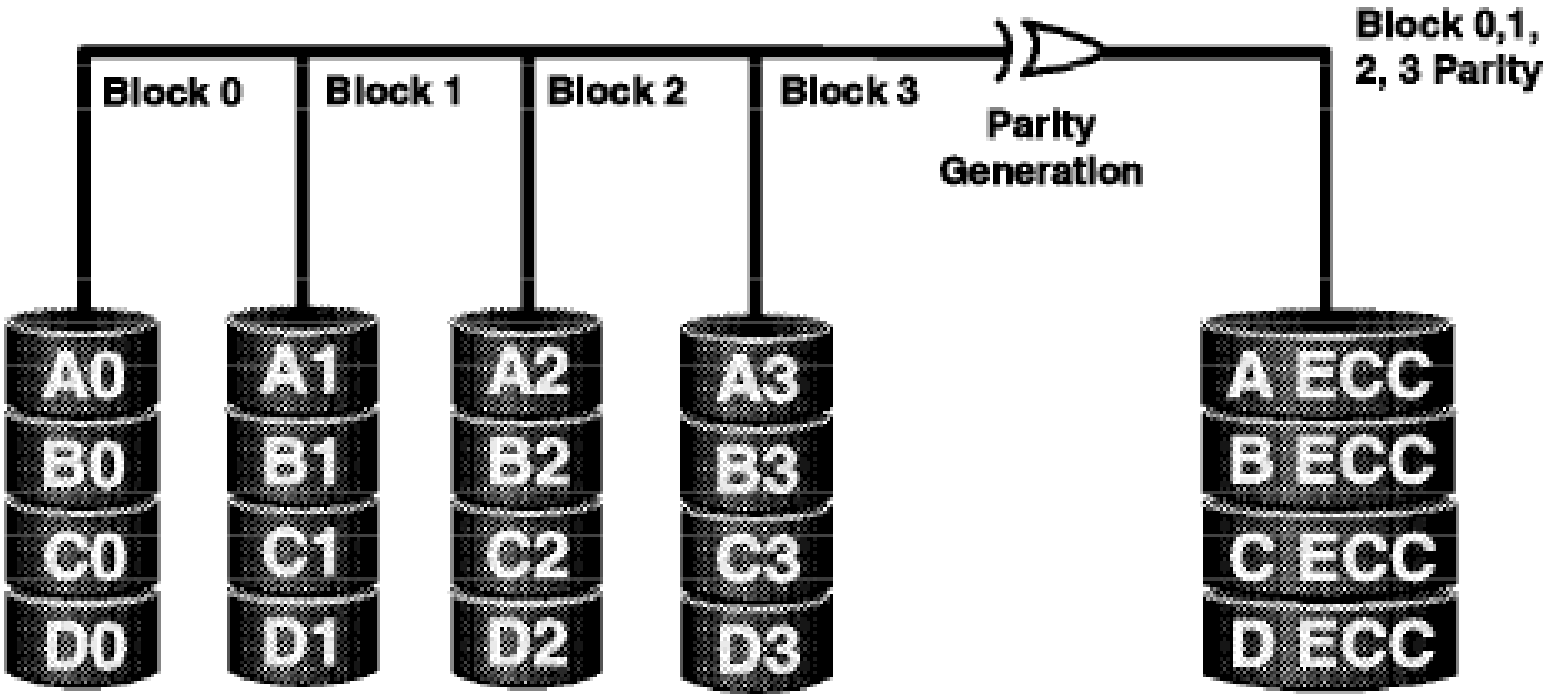
Raid 1



Zusatzinformationen

CoC ITA

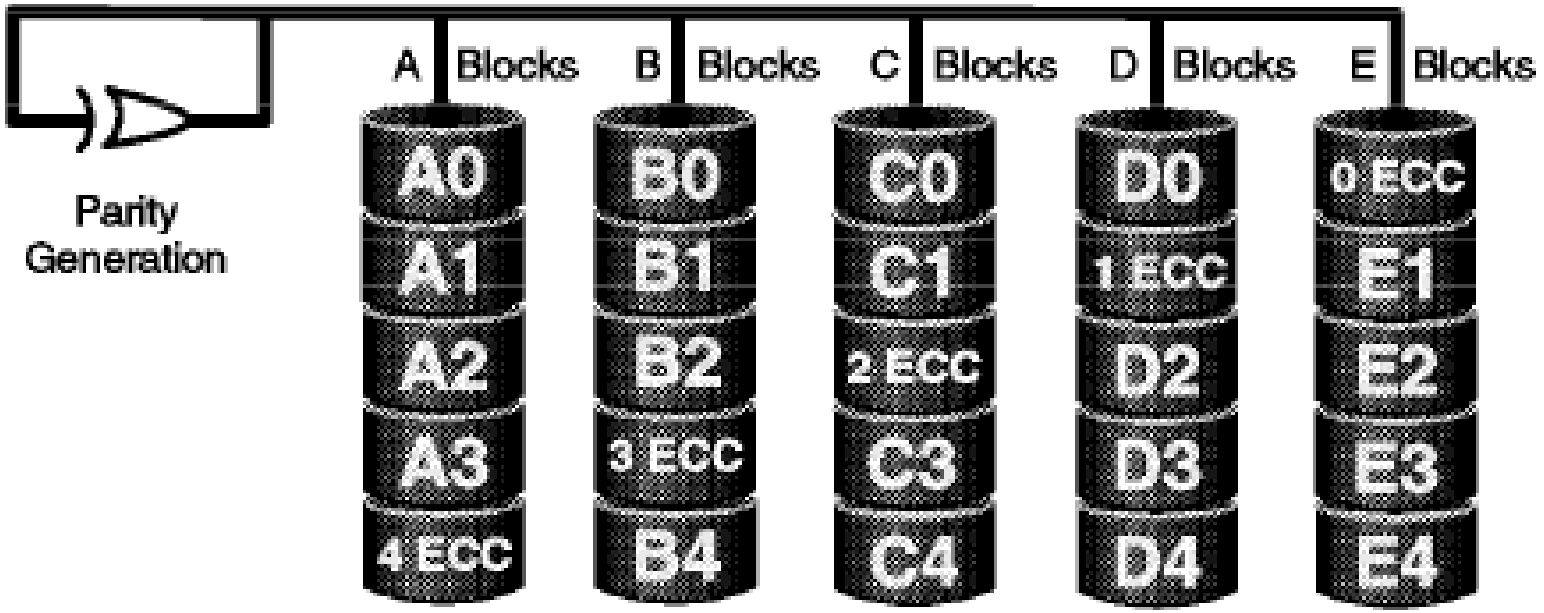
Raid 4



Zusatzinformationen

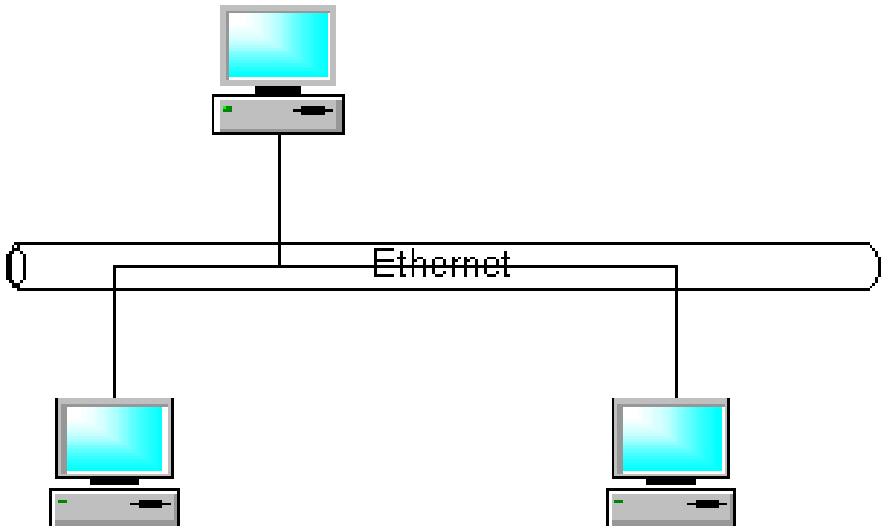
CoC ITA

Raid 5



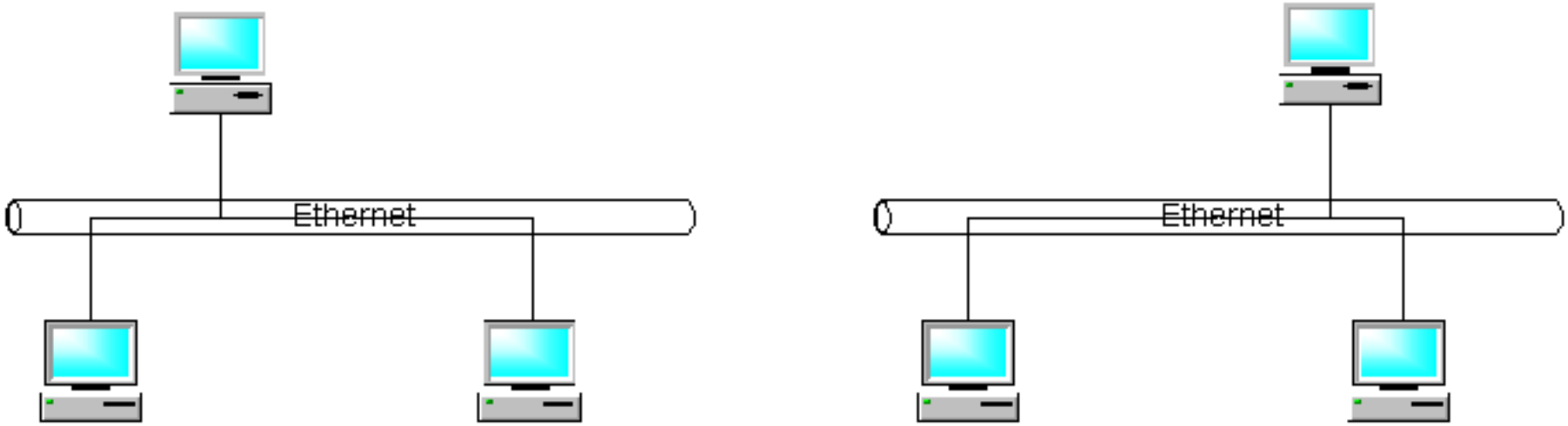
Zusatzinformationen

VLAN (IEEE 802.10)



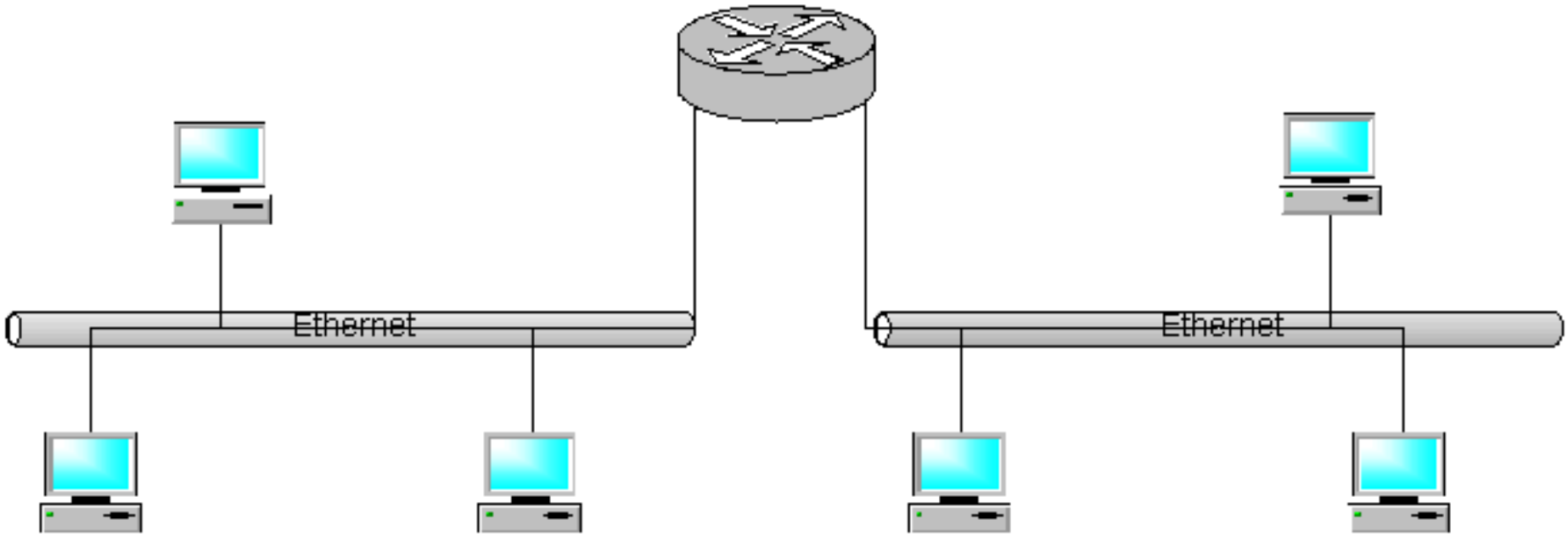
Zusatzinformationen

VLAN (2)



Zusatzinformationen

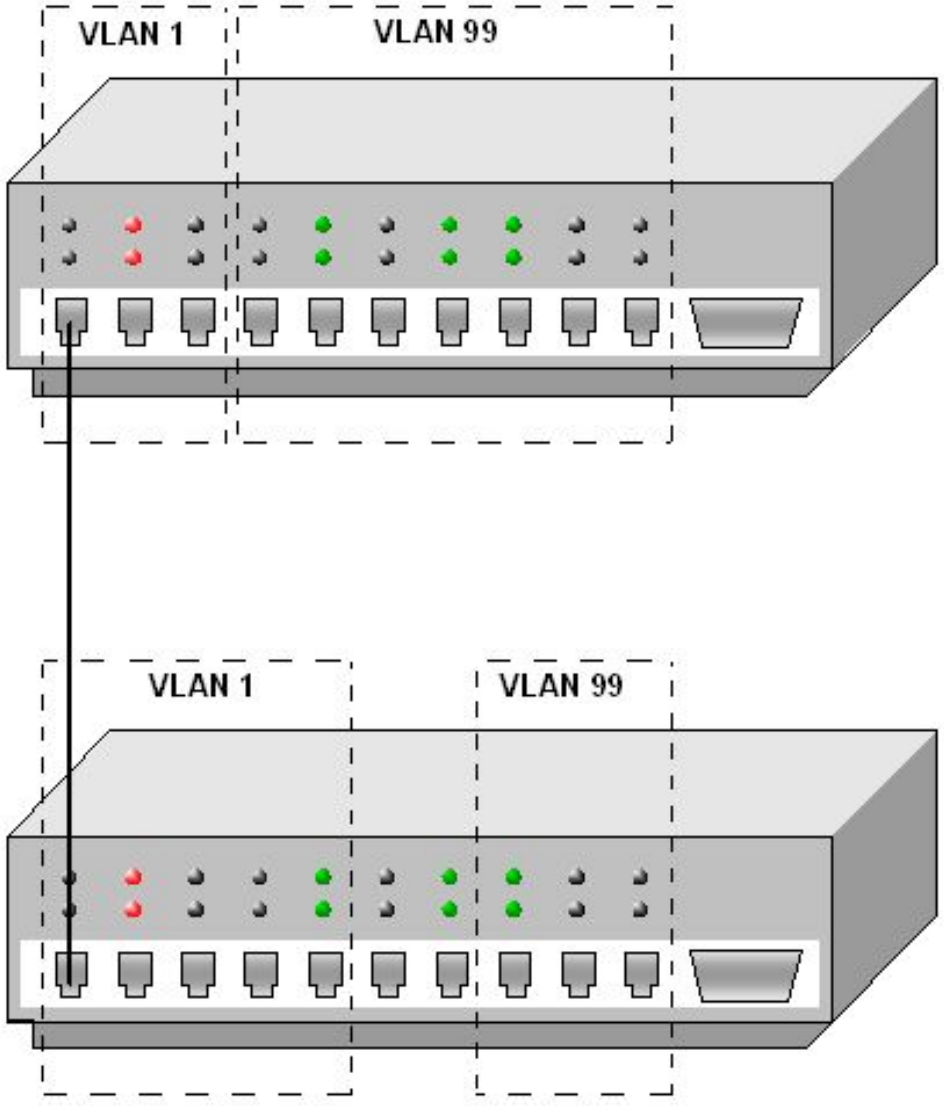
VLAN (3)



Zusatzinformationen

CoC ITA

VLAN (4)



Zusatzinformationen

VLAN (5)