

Verfügbarkeit

Für jeden Einsatzzweck der richtige Ansatz

Frank Carius

Net at Work GmbH



Steckbrief



- Frank Carius
(www.msxfaq.de)



- Schwerpunkte
 - Lync, Exchange
 - Infrastruktur
 - Mailverschlüsselung und Signierung, DE-Mail
- Was treibt mich an
 - Wissen zu mehrern
 - Lösungen zu entwickeln
 - Andere vor Fehlern bewahren

- Net at Work
(www.netatwork.de)

- Standort Paderborn, Gegründet 1995, 43 Mitarbeiter
- IT-Systemintegration und Softwarehaus
- Kunden: klassischer Mittelstand bis Enterprise
- NoSpamProxy und enQsig

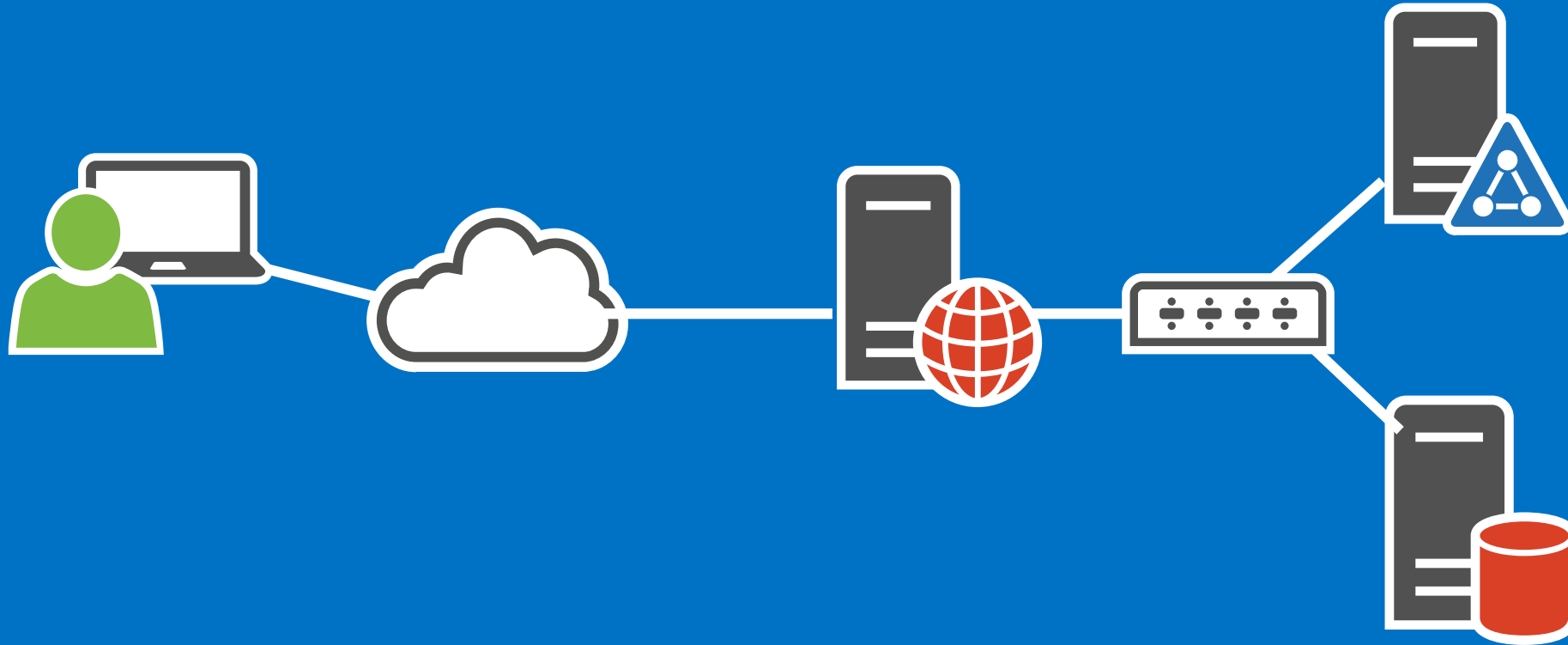


Verfügbarkeit ist ...

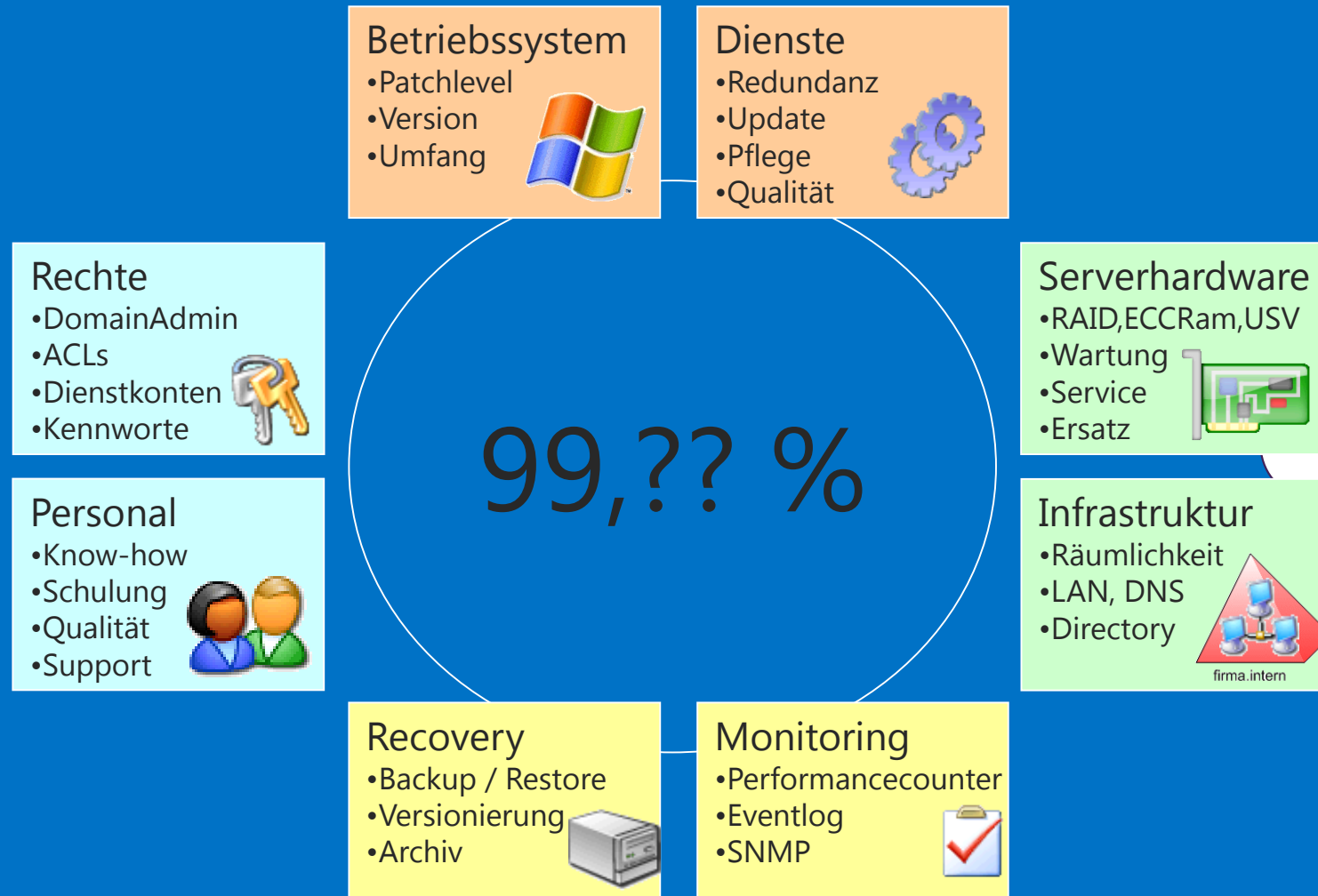
... wenn der Anwender eine
Störung nicht merkt.

Ein Ausfall ist nur dann ein
Ausfall, wenn es aufgefallen ist.

Ein ganz einfacher Service

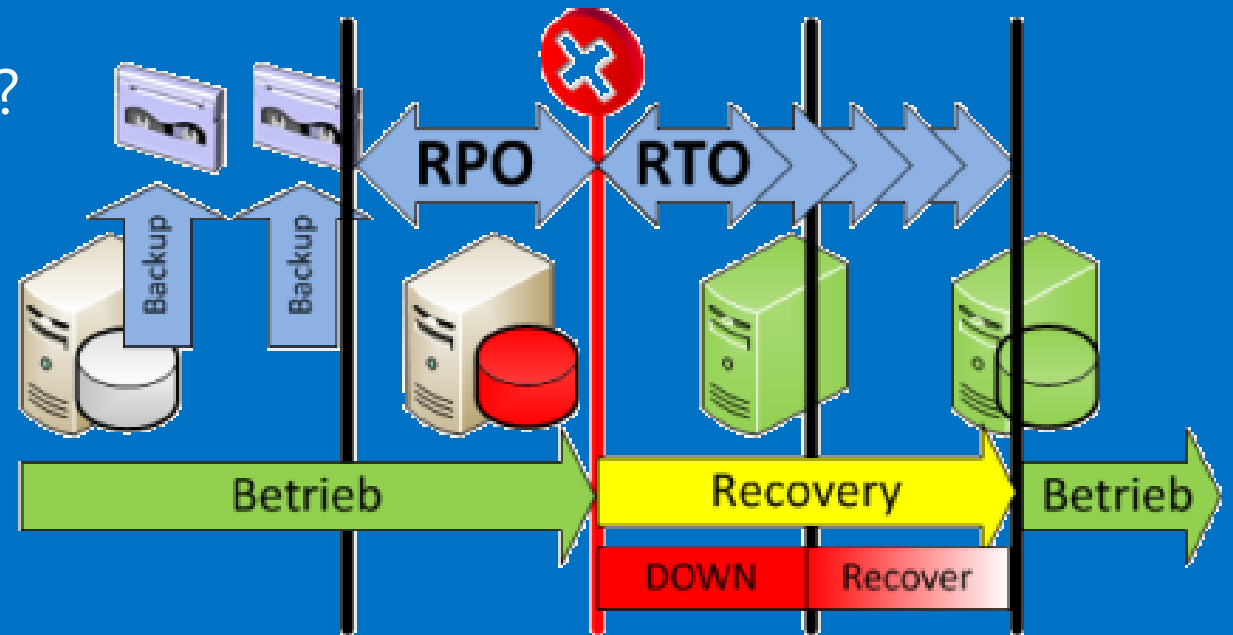


Da kann einiges schief gehen ...

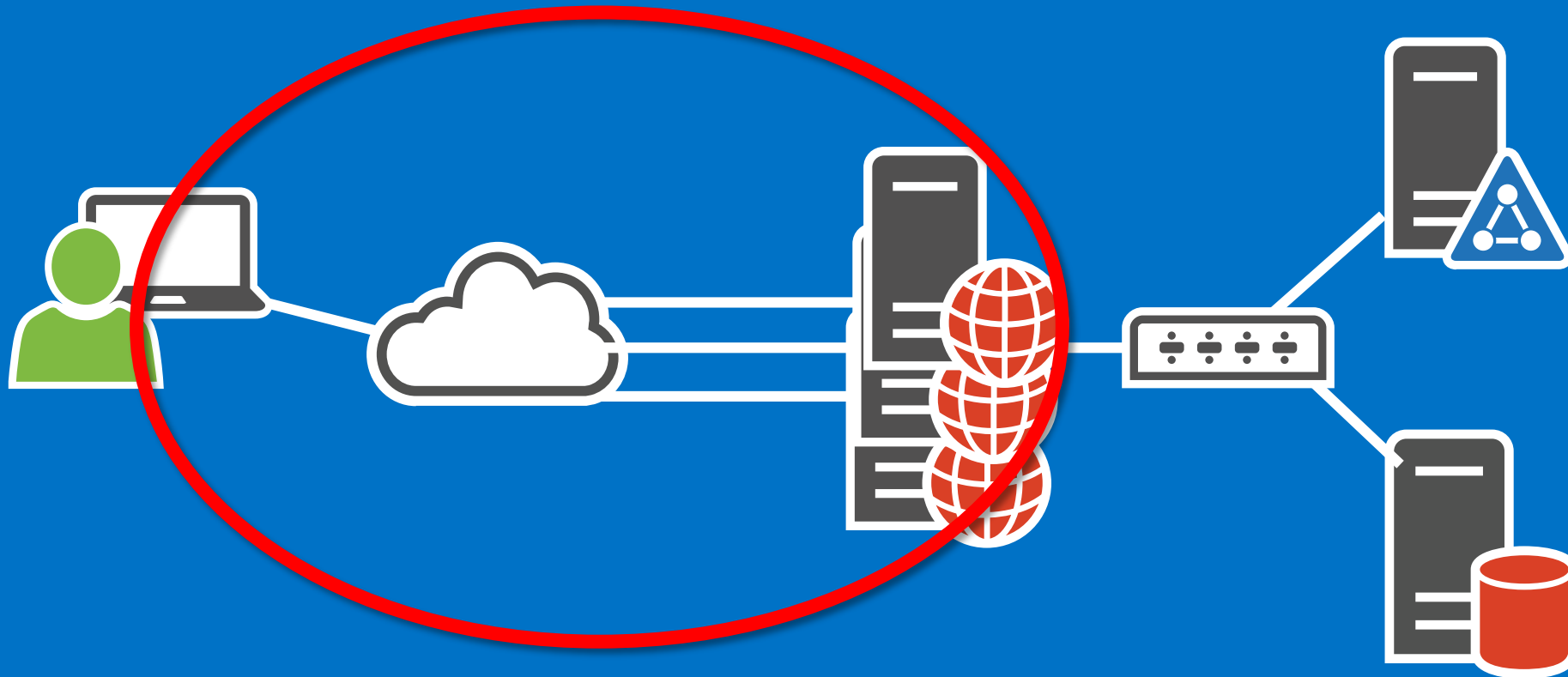


... und Wiederherstellung dauern

- RPO: Recovery Point Objective
 - Bis zu welchem Zeitpunkt komme ich heran
 - D.h. wie groß ist der Verlust
- RTO: Recovery Time Objective
 - Wie lange dauert die Wiederherstellung ?
- Monitoring?
 - Erkennen, dass es einen Ausfall gibt
- Redundanz
 - Ausfälle überbrücken



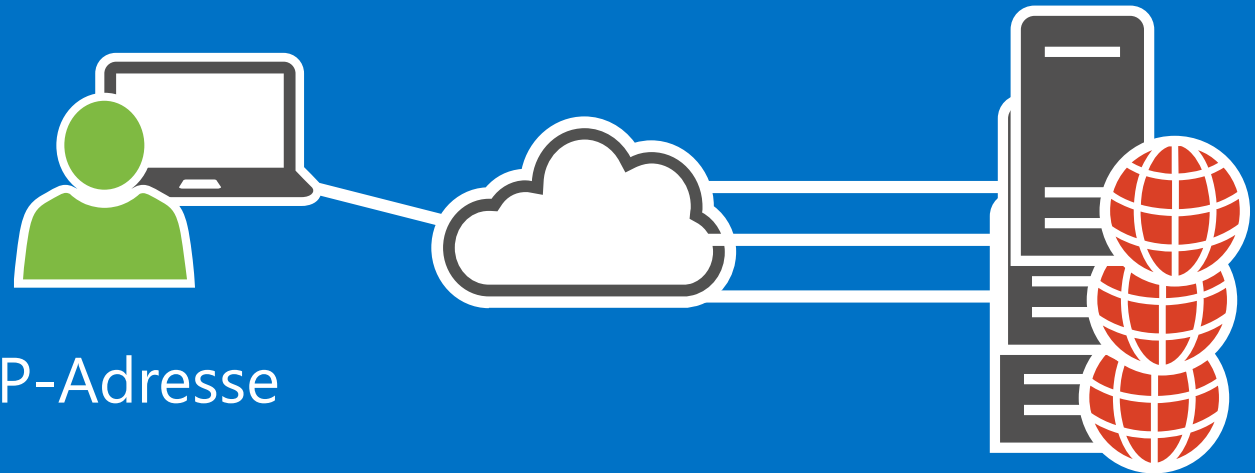
Unser Thema: Clientzugriff



Clientzugriffe verteilen

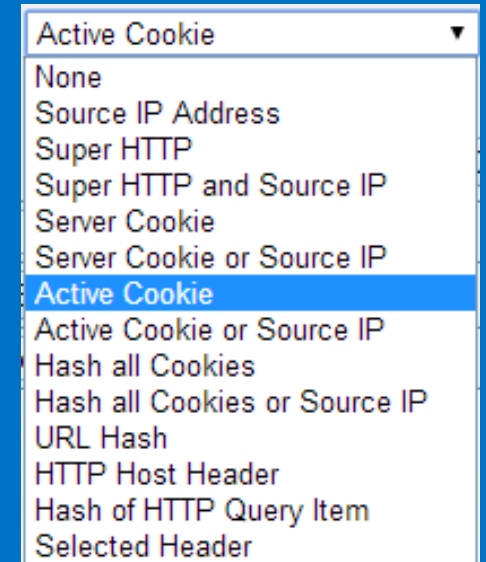
Ein Client – viele Server

- IP-Failover
 - Klassischer Microsoft Cluster Services
 - IP-Adresse schwenkt auf anderes System
- DNS Round Robin
 - Einfach nutzbar
 - Verteilung auf HA-IPs
- IP Sharing mit NLB
 - Mehrere Server haben die gleiche IP-Adresse
- Loadbalancer
 - Aktive Spezialisten zum Verteilen
 - Oft mit Zusatzfunktionen



Affinität

- Anforderung
 - Ein Client muss/soll beim „gleichen“ Backend-Server bleiben
- Warum ?
 - Authentifizierung und Session beibehalten
 - Caching und Speicher auf dem Backend
 - Einfachere Fehlersuche
 - Client unterstützt keine Failover-Funktionen
- Wie ?

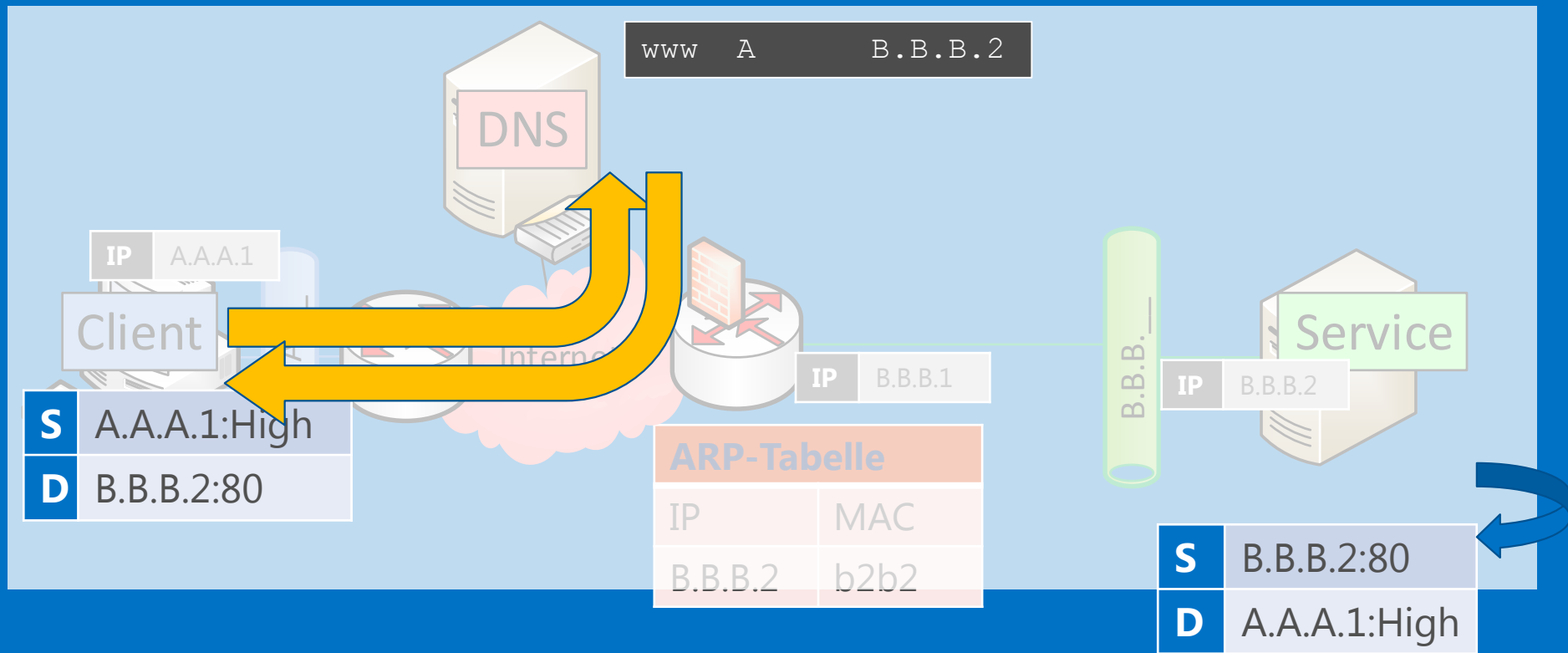


Affinity	Beschreibung
Keine	<ul style="list-style-type: none">• Jeder HTTP-Request oder jede TCP-Connection wird neu verteilt
Source IP	<ul style="list-style-type: none">• Alle Anfragen von einer Source-IP landen beim gleichen Ziel• Probleme bei vielen Clients hinter NAT/Proxies (z.B. Office 365), auf Terminal Server
HTTP Header	<ul style="list-style-type: none">• Nur für HTTP oder mit SSL-Offloading nutzbar• Passender Header muss gesucht werden, (z.B. Authentication)
Cookie	<ul style="list-style-type: none">• Nur für HTTP oder mit SSL-Offloading nutzbar.• Bestehender Cookie suchen oder Cookie einfügen lassen

Erhöhte Anforderungen

- Single TCP-Connection
 - Telnet, RDP, POP, IMAP, SMTP
- Parallele Verbindungen
 - HTTP-Zugriffe (Hauptseite, CSS, Images)
 - Downloads, ggfls. Media Streaming
- Protokolle mit Rückkanal
 - FTP: Port 21 = Steuerung, Port 20 = Data
- Protokolle mit „sekundären Ports“
 - RPC Start mit 135 Portmapper, Info über Service-Port z.B. Exchange-MAPI, DCOM, Windows-RPC
- Verschlüsselte Verbindungen
 - Ein Einblick über die Identität
 - Source-IP und Port ist nicht immer genug
 - SSL Decodierung / SSL-Offloading

Die erste Animation

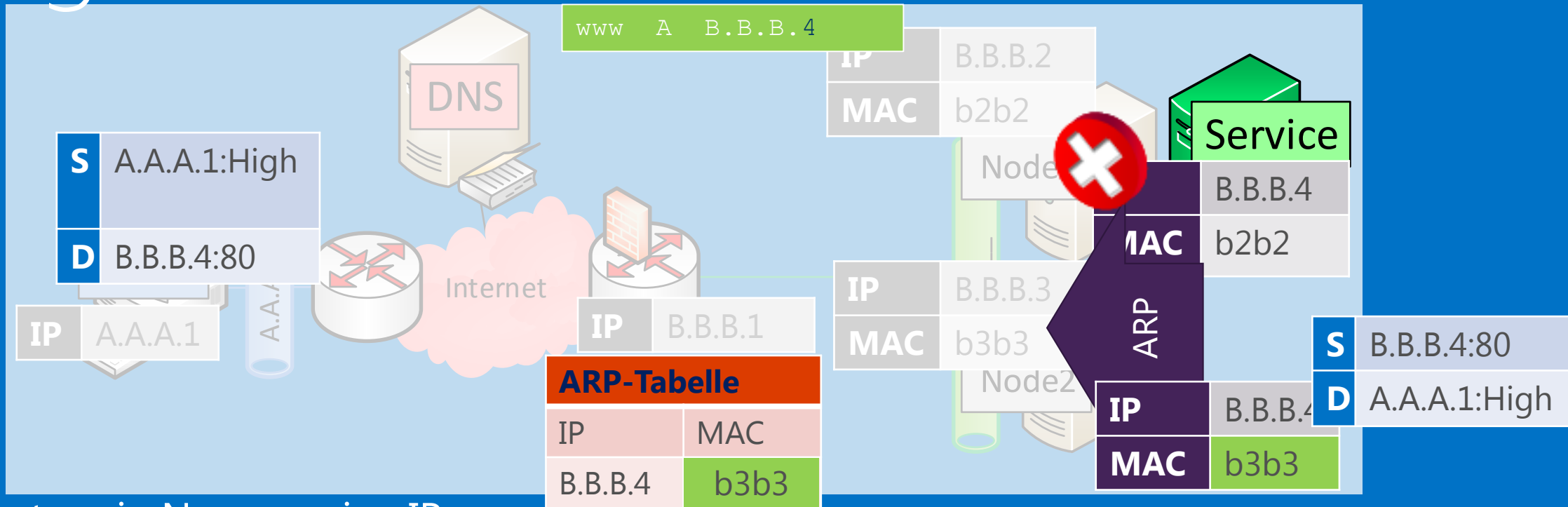


- A.A.A.1/B.B.B.2 sind IP-Adressen
- a1a1 und b1b1 sind MAC-Adressen
- Keine Hochverfügbarkeit
- Keine Lastverteilung



IP Failover

Verfügbarkeit durch IP-Failover



- Ein Dienst = ein Name = eine IP
- Microsoft Cluster
 - 1-n Server sind als Cluster verschaltet
 - Eine Service ist auf genau einem Knoten mit IP-Adresse aktiv
 - Failover: Ressourcen umhängen, Dienste starten, ARP-Paket senden
- Manuelles Failover-Skript
 - Server 2 „prüft“ Erreichbarkeit des Servers 1 und bindet im Fehlerfall die IP
 - <http://www.msxfaq.de/cluster/minisft.htm>



IP/Service-Failover und Clients

Client	Status	Beschreibung
PING (ICMP)	Green	Ganz kurze Ausfallzeit, eher Sekunden
TELNET	Yellow	Reconnect erforderlich, sehr schnell möglich
FTP.EXE	Yellow	Reconnect erforderlich, sehr schnell möglich
FTP (FileZilla)	Yellow	Reconnect erforderlich, sehr schnell möglich
IMAP4 (Outlook)	Green	Reconnect erforderlich aber für den Anwender transparenter Wechsel.
SMTP	Green	Bestehende Connection geht verloren. Neue Verbindungen erreichen zuverlässig „ihren“ Service
HTTP	Yellow	HTTP-Reconnect sofort möglich. Problemlos für „Anonym“ Session muss ggfls. neu aufgebaut werden.
SMB	Green	Bevorzugte Lösung für Fileserver
SQL	Green	Seit jeher die SQL-Lösung eher SQL-Mirroring

Datenblatt: IP-Failover

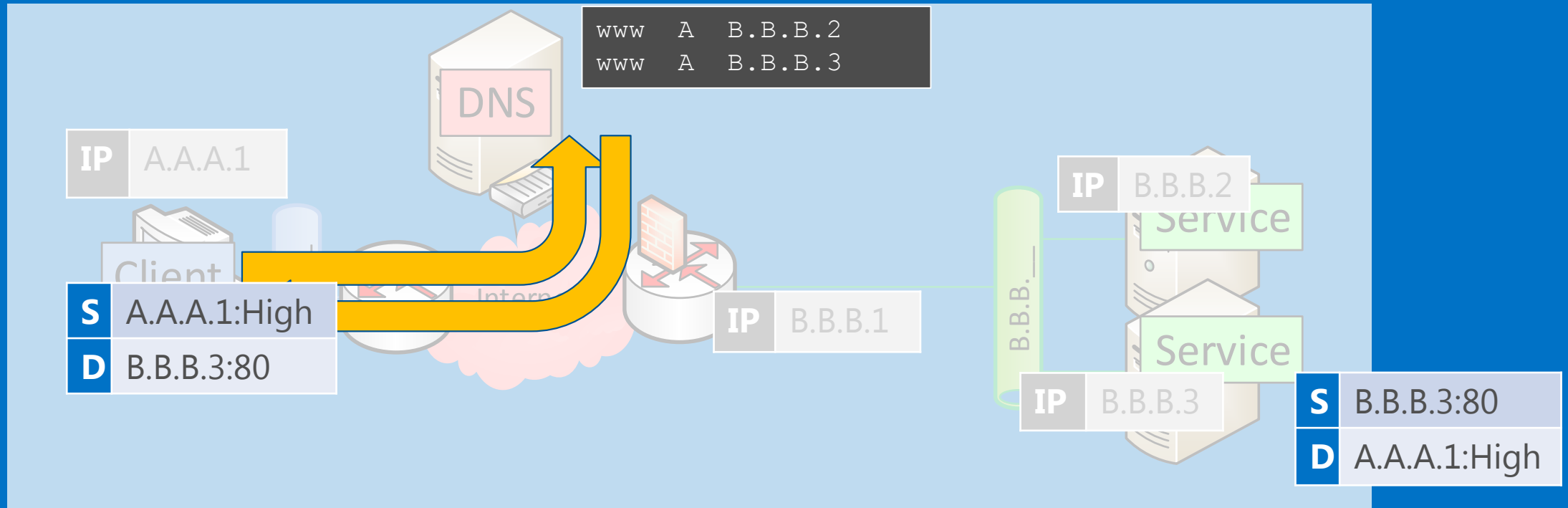


Merkmale	Beschreibung
Funktionsweise	Ein Name verweist auf mehrere IP-Adressen
Umsetzung	<ul style="list-style-type: none">• Microsoft Cluster (Lizenzen) oder Skripte• Integrierte Überwachung
Verfügbarkeit	<ul style="list-style-type: none">• Sehr hoch• Kurze Failover-Zeiten mit Client Reconnect• Dienste und Ressourcen können mit geschwenkt werden• Geplante Wartung und Updates möglich.
Lastverteilung	<ul style="list-style-type: none">• Nur Aktiv/Passiv pro Service möglich• Dimensionierung: Anzahl der Knoten -1
Affinität	<ul style="list-style-type: none">• Entfällt da nur ein aktiver Service
SSL Offloading	<ul style="list-style-type: none">• Nicht vorhanden
Client	<ul style="list-style-type: none">• Client muss beim Schwenk einen „Reconnect“ machen

IP-Failover-Lösungen sind eine einfache HA-Option, wenn die Dienste sowieso nicht auf mehrere Server verteilt werden können. (z.B. Dateiserver)

DNS Round Robin

DNS-Round Robin



- DNS liefert bis zu 16 IP-Adressen in variabler Reihenfolge
- Einige DNS-Server liefert „Routing-optimierte“ Adressen
Windows DNS macht das, wenn Client und Server im gleichen Subnetz
- Client verbindet sich zur IP-Adresse
- Einige Clients sind für DNS-RR „optimiert“



DNS RR und fehlende Server

- DNS-Server kennen nicht den Betriebsstatus
 - DNS liefert weiterhin auch IPs die nicht funktionieren
- Clients versuchen diesen Server
 - TCP-Handshake dauert Zeit



Demo

Wir schauen mit NETMON nach

DNS-RR und Clients

Client	Status	Beschreibung
PING (ICMP)	Red	Spricht nur eine IP-Adresse an. Geht/Geht nicht-Effekt pro Aufruf
TELNET	Yellow	nach 21 Sekunden Retry zur anderer IP, 4 mal, Verzögerung !
FTP.EXE	Yellow	Versucht sequenziell die Adressen. (21 Sek. Verzögerung)
FTP (FileZilla)	Red	Bleibt an der ersten IP-Adresse hängen
IMAP4 (Outlook)	Green	Sequenziell aber für den Anwender transparenter Wechsel.
IE9	Yellow	Versucht sequenziell die Server zu erreichen. 21 Sek Verzögerung
Chrome 27	Yellow	Sequentielles DNS mit drei parallelen Verbindungen zur ersten IP-Adresse und dann mit drei Verbindungen zur nächsten IP-Adresse
Firefox	Green	Firefox macht wie Opera parallel Verbindungen zu den IP-Adressen auf und versucht es sehr hartnäckig:
SMB	Red	Nicht sinnvoll über mehrere Server möglich
Lync Client	Green	Offizieller Weg einen Pool erreichbar zu machen. Clients geht nicht nur damit um, sondern cached sogar Einträge

Weitere Details auf <http://www.msxfaq.de/cluster/dnsroundrobin.htm>



Datenblatt: DNS Round Robin



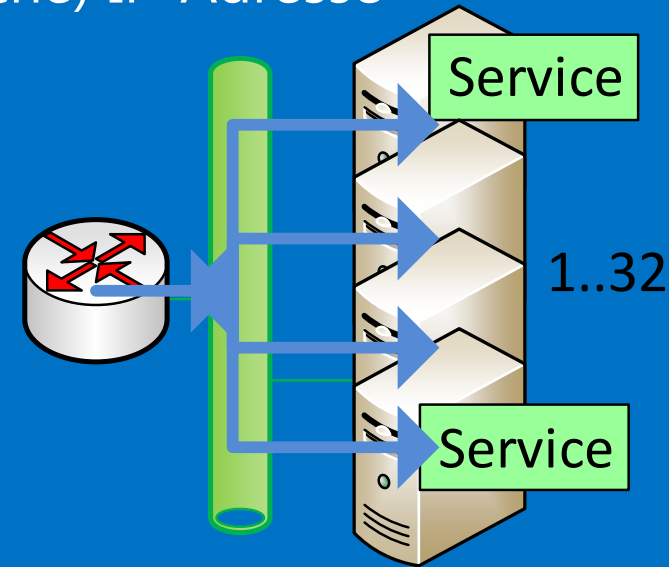
Merkmale	Beschreibung
Funktionsweise	Ein Name verweist auf mehrere IP-Adressen
Umsetzung	<ul style="list-style-type: none">• Sehr einfach• Keine Investitionen
Verfügbarkeit	<ul style="list-style-type: none">• Client muss herausfinden, wenn ein Server nicht antwortet• Ggfls. TCP-Session Timeout (ca. 48 Sek)• Keine Bindung an die Serververfügbarkeit DNS Cache erschwert aktive Steuerungen• „Geplante Wartung“ nur mit viel Vor- und Nachlauf
Lastverteilung	<ul style="list-style-type: none">• Gleichverteilung nach Clientanfragen• Keine Berücksichtigung von Serverlast und Antwortzeiten
Affinität	<ul style="list-style-type: none">• Abhängig vom Client• Nicht garantiert
SSL Offloading	<ul style="list-style-type: none">• Nicht verfügbar
Client	<ul style="list-style-type: none">• Muss aktiv einen „Failover“ machen• Einige Clients machen das !!

DNS-RR ist eine einfache, günstige Möglichkeit, mehrere Server erreichbar zu machen. Die Verfügbarkeit wird nur besser, wenn die Clients mitspielen.

NLB

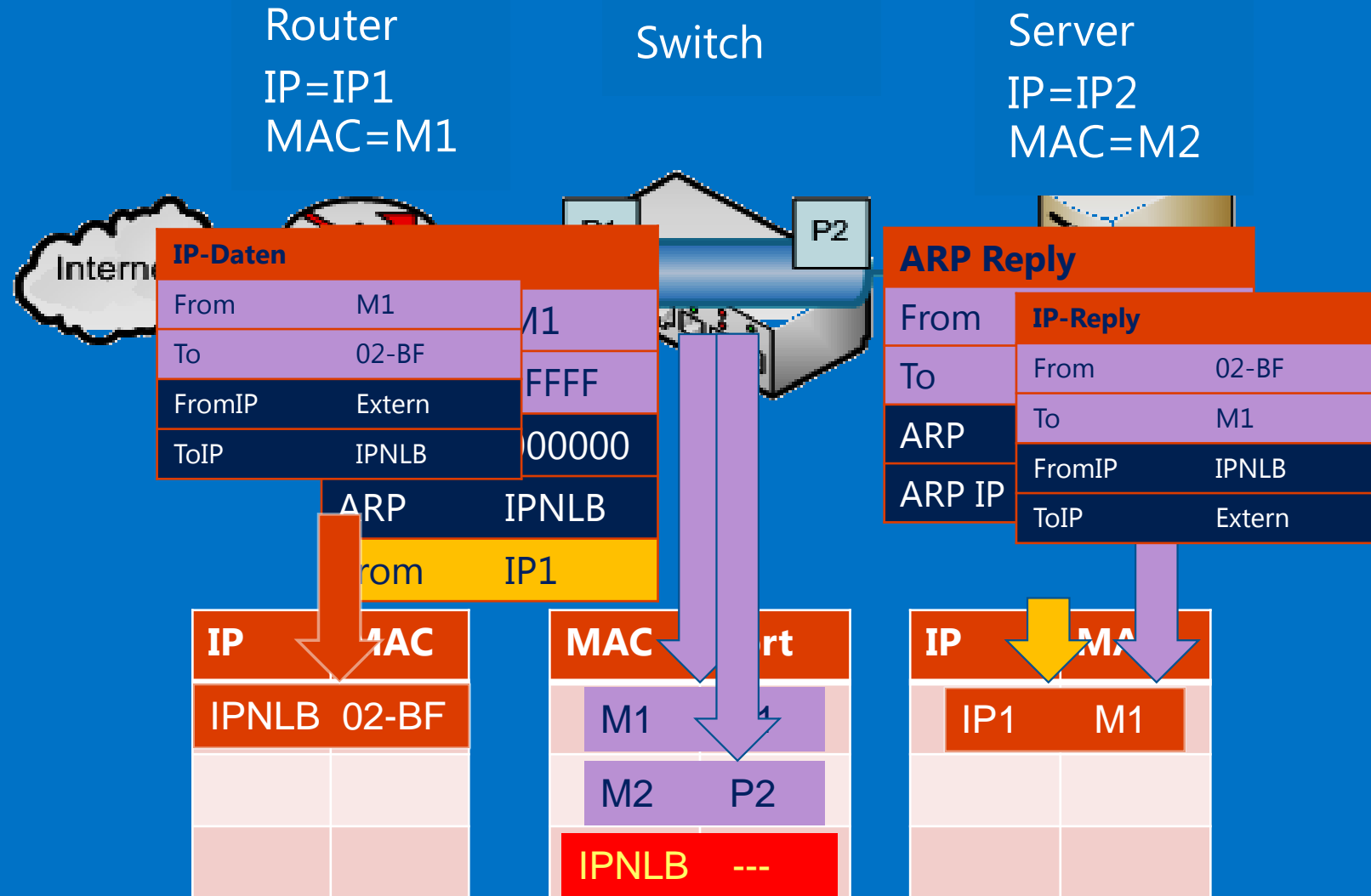
Verteilen mit NLB

- Funktionsweise:
 - Bis zu 32 Server haben eine gemeinsame (zusätzliche) IP-Adresse
 - Zustellung aller Pakete erfolgt an "alle Server"
 - Unicast, Multicast, IP Multicast
 - Jeder Server pickt sich "seine" Pakete heraus
 - Alle Server können alle Daten liefern
 - Nicht mit Windows Failover Cluster kombinierbar
- Verteilung ?
 - Statisch anhand Source-IP (Hash)
 - Affinity nach Client IP oder „Keine“
- Einschränkungen
 - Keine Rücksicht, ob Server überlastet
 - Keine Überwachung, wenn Dienst funktionsfähig ist
 - Viele Clients hinter NAT
 - Kleine Umgebungen mit wenig Clients und Subnetzen

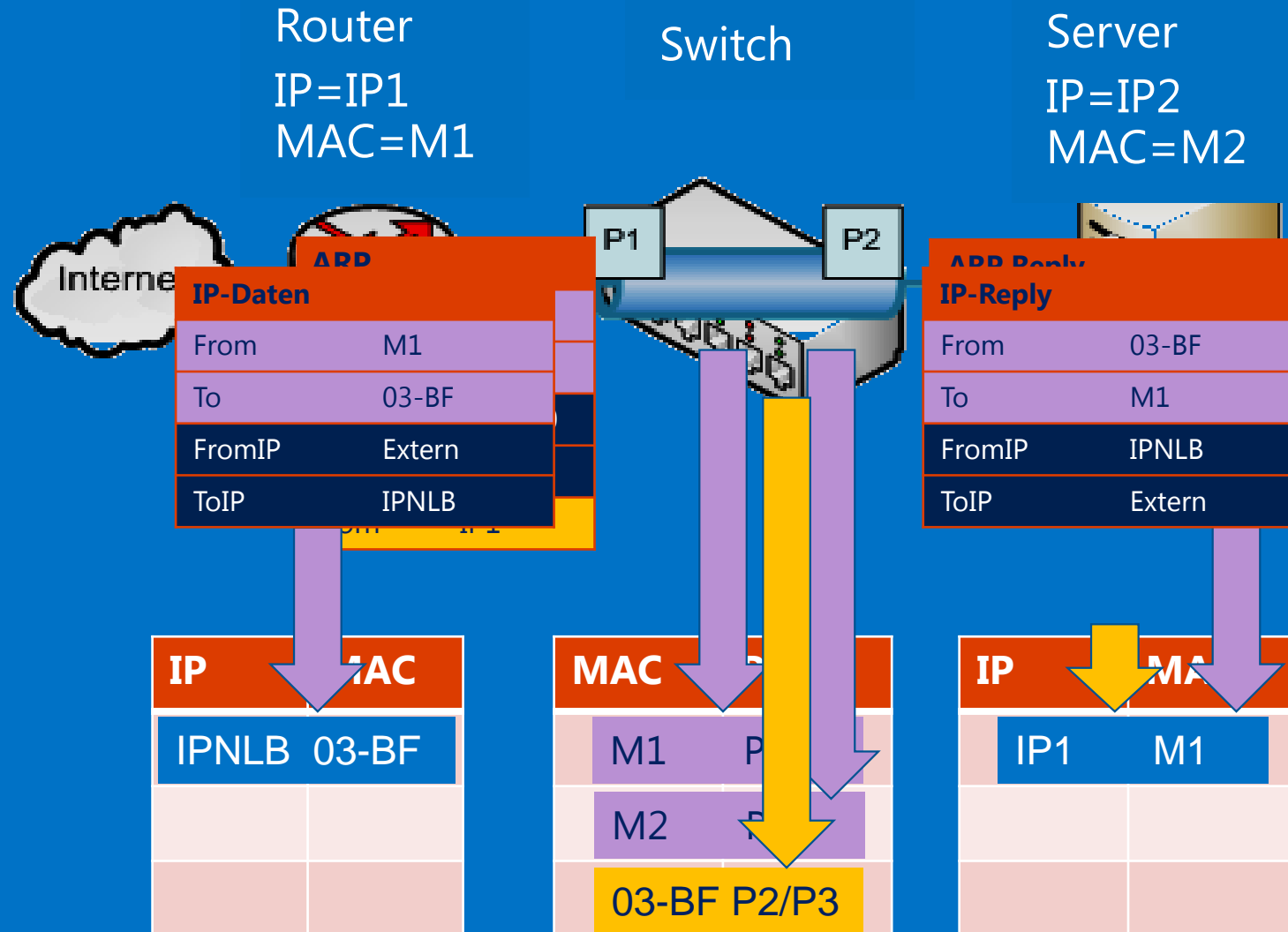


Wie schafft NLB es, dass ein Paket an eine IP-Adresse zu vielen Servern geht ?

NLB mit Unicast



NLB mit Multicast



NLB - Verteilvarianten

- Lösung 1: NLB im UNICAST (02-BF-xx-xx-xx-xx)
 - NLB nutzt besondere MAC-Adresse, mit der niemand antwortet
 - Switch kann die Adresse nicht lernen, Pakete an die MAC-Adresse werden auf allen Ports geflutet
 - Problem: Fluten des V-LANs, Sichtbarkeit an anderen Systemen
 - Ratsam: eigenes VLAN
- Lösung 2: NLB Multicast (03-BF-xx-xx-xx-xx)
 - NLB nutzt besondere MAC-Adresse
 - Switch „versteht“ 03-bf als MAC-Level Multicast
 - MAC-Adresse ist auf mehreren Ports „legitim“
 - Switch muss MAC-Multicast verstehen und an alle Ports senden
- Lösung 3: NLB mit IP-Multicast (224.0.0.0 - 239.255.255.255)
 - NLB nutzt besondere IP und MAC-Adresse (Class-D-Netz)
 - Problem: IGMP muss firmenweit/weltweit funktionieren

Datenblatt: NLB



Merkmale	Beschreibung
Funktionsweise	<ul style="list-style-type: none">• Mehrere Server haben die gleiche IP-Adresse• Connection Picking, Nicht mit MS-Cluster kombinierbar
Umsetzung	<ul style="list-style-type: none">• Kostenfrei in Windows Server enthalten• Kniffliges Setup im LAN, Router, Switches, virtuell
Verfügbarkeit	<ul style="list-style-type: none">• Überwacht keine Dienste• „Geplante Wartung“ möglich (DrainStop)
Lastverteilung	<ul style="list-style-type: none">• Verteilung nach festem Schlüssel mit Source-IP• Keine Berücksichtigung von Serverlast und Antwortzeiten
Affinität	<ul style="list-style-type: none">• Nach Source-IP, Subnetz oder keine.• Keine Cookies o.ä.
SSL Offloading	<ul style="list-style-type: none">• Nicht verfügbar
Client	<ul style="list-style-type: none">• Keine Besonderheit zu berücksichtigen• TCP-Reconnect erforderlich, wenn Knoten ausgefallen ist.

Mit NLB können bis zu 16 Server die gleiche IP nutzen und die Anfragen untereinander aufteilen. Allerdings sind Einschränkungen zu beachten.

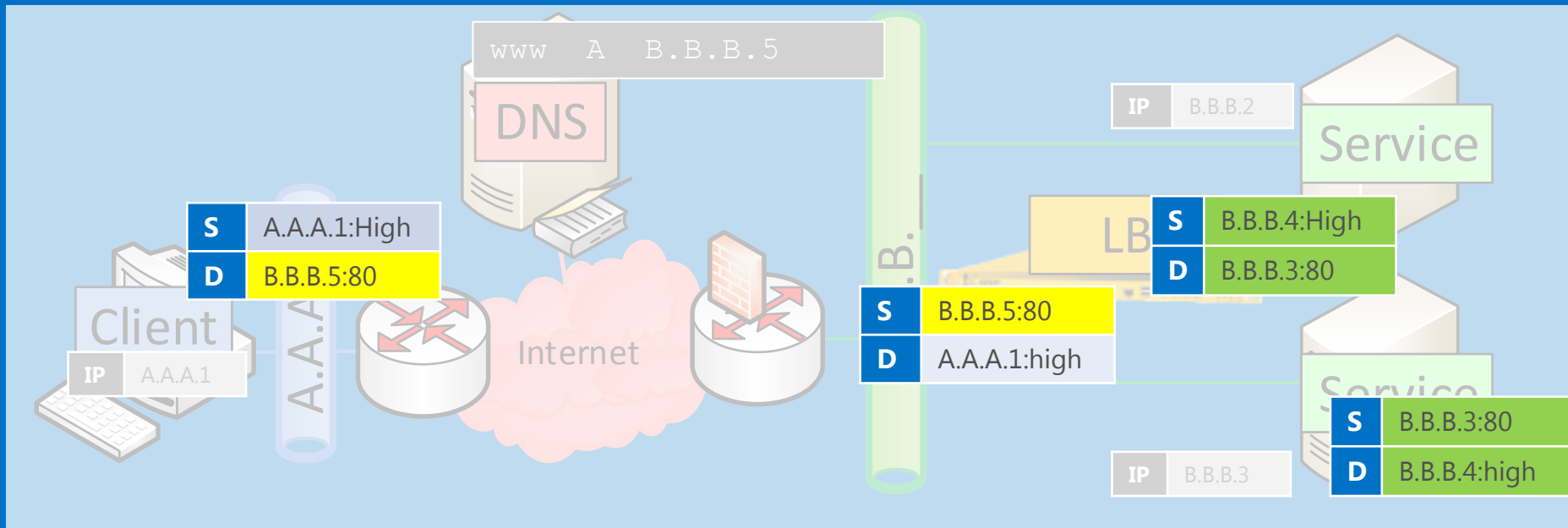
Loadbalancer

Verteilen mit Load Balancer

- Funktionsweise
 - Loadbalancer hat eine „physikalische IP“
 - Dienste werden über „virtuelle IP“ bereit gestellt
 - Rückantwort des Backend „sollte“ über LB zurück
 - Auch der Loadbalancer muss „HA“ anbieten
 - Z.B. Aktiv-Passiv mit IP/MAC-Failover
- Aktive Komponente im Netzwerk
 - Hardware oder Virtuell
 - Single Leg oder Two Leg
- Affinity
 - Layer 4 (IP-Adresse:Port)
 - Layer 7 („etwas“ im Datenstrom, z.B. Cookie)

Auf den nächsten zwei Seiten zeige ich die Funktion von zwei Varianten. Es gibt natürlich noch weitere Möglichkeiten, Dienste über einen LB bereitzustellen.

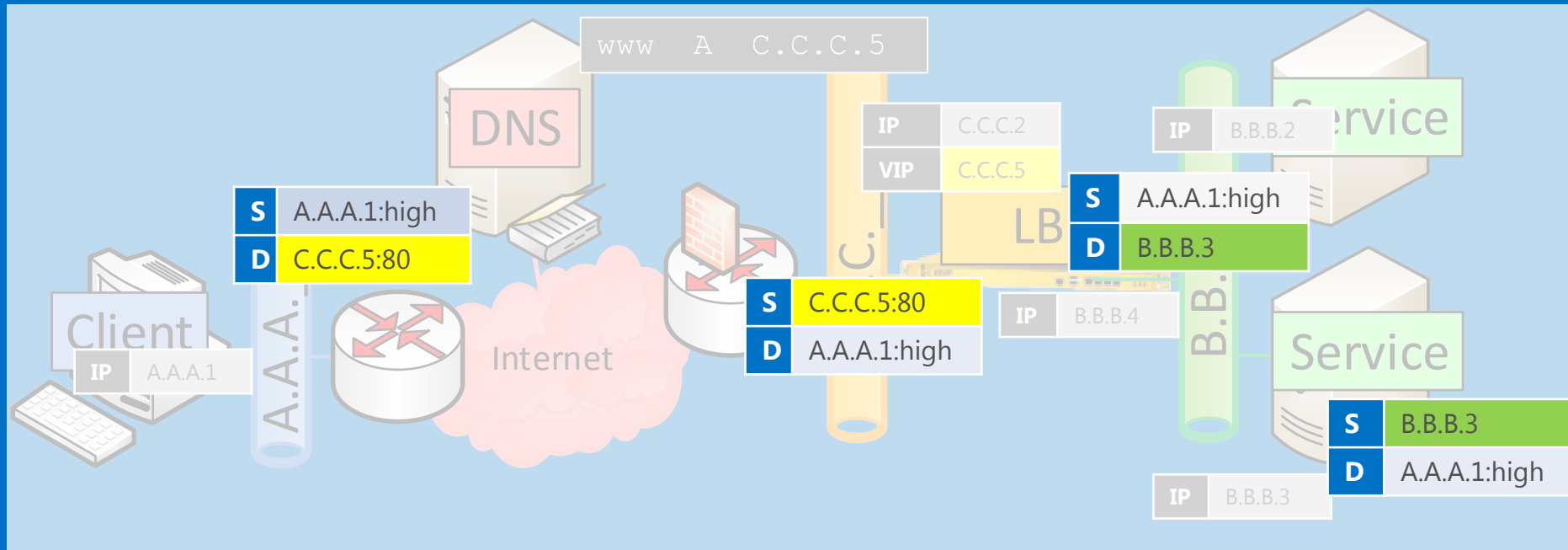
HLB als „Single Leg“



- Doppelt NAT (Source und Destination)
- Doppelter Weg auf dem LAN
- Problem: 65535 Source-Ports
- Problem: Backend sieht nur HLB-IP -> Logging, Restriktionen



HLB als „Two Leg“

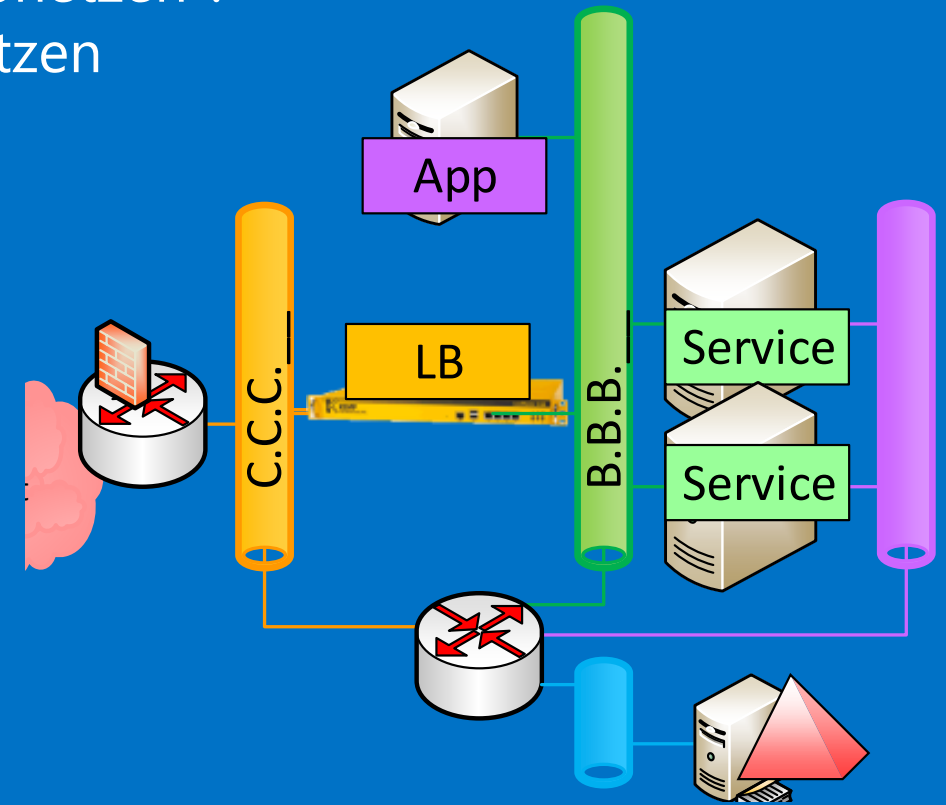


- Weiteres Subnetz erforderlich
- Default Gateway ist der Loadbalancer
- Kein Source NAT
 - Backend sieht Client-IP
 - Kein 65535 Port Problem



Load Balancer Herausforderungen

- Default Gateway des Backend ist der Load Balancer
 - Routing zu anderen „RZ-Netzen“
 - Verbindung zum Domaincontroller in anderen Subnetzen ?
 - Verbindung zum Backup Server in anderen Subnetzen
- Direct Server Return
 - Load Balancer Bypass für Rückpaket
 - Real-IP statt Virtual-IP
- „Clients“ im Transfernetz oder RZ-Netz
 - Applikation die Exchange nutzen
 - Monitoring Server (SCOM)
 - Backup Server
- Loadbalancer als aktiver Router
 - Abstimmung mit Netzwerkkern
- HA für Loadbalancer selbst !



Weitere LB Funktionen

- Aktive Überwachung der Backend Server
 - Application Awareness
- Lastverteilung nach unterschiedlichen Kriterien
 - Round Robin, Least Connection, Least Load etc.
- Preauthentication
 - Vorgelagerte Anmeldung, Soft-Lockout
 - Active Directory-Integration oder RADIUS
 - Single Sign On über Virtual Services
 - Zugriffsrechte über Gruppenmitgliedschaften
 - Anmeldeformulare
 - Dual-Faktor-Auth w / RSA SecurID
- URL-Filterung und Parameter-Validierung
- Protokollierung und Berichterstellung
- ...

Domain MSXFAO.NET

Authentication protocol	LDAP-Unencrypt LDAP-StartTLS LDAP-LDAPS RADIUS RSA-SecurID	<input type="text"/>	<input type="button" value="Set LDAP Server(s)"/>	
LDAP Server(s)				
Logon format	Principalname ▾	<input type="text"/>	<input type="button" value="Set Login Domain"/>	
Failed Login Attempts	0	<input type="text"/>	<input type="button" value="Set Failed Login Attempts"/>	
Session Timeout	Public - Untrusted Environment		Private - Trusted Environment	
	900	<input type="button" value="Set Idle Time"/>	900	<input type="button" value="Set Idle Time"/>
	1800	<input type="button" value="Set Max Duration"/>	28800	<input type="button" value="Set Max Duration"/>
	Use for Session Timeout: idle time ▾			
Test User	<input type="text"/>	<input type="button" value="Set Test User"/>		
Test User Password	<input type="text"/>	<input type="button" value="Set Test User Password"/>		

ICMP Ping
HTTP Protocol
HTTPS Protocol
TCP Connection Only
Mail (SMTP) Protocol
Network News (NNTP) Protocol
File Transfer (FTP)
Telnet Protocol
Mailbox (POP3) Pr
Mailbox (IMAP) Pr
None

round robin
weighted round robin
least connection
weighted least connection
resource based (adaptive)
fixed weighting
weighted response time
source IP hash

Zusatznutzen eines LB z.B. bei ...

- SMTP-Versand/Empfang zwischen Servern
 - Mehrere MX-Records
 - Queueing/Retry
- POP3/IMAP
 - Kein „Referral“, Retry fällt auf, Nur ein Hostname in der Konfiguration
 - DNS Round Robin denkbar aber Loadbalancer hat Vorteile
- SMTP-Client
 - LB zur besseren Erreichbarkeit für einfache Mailsender, z.B. Skripte, BLAT u.a. Prozesse ohne Queue oder Retry
- LDAP
 - Adressbuchsuche für Scan2Mail-Systeme, TK-Anlagen etc., die nur einen LDAP-Server unterstützen
- Radius
 - Einige Endgeräte erlauben nur den Eintrag eines Radius-Servers. Da kann ein LB einfach helfen
- LPD
 - Mehrere LPD-Server können elegant die Clients bedienen
- Es gibt sicher noch andere TCP/UDP-Prozesse, die profitieren.

Loadbalancer Schaulauf

- Korrekte Dimensionierung ist wichtig
 - Insbesondere SSL-Leistung, wenn erforderlich
 - Belastung der Server ermitteln oder messen: IISLog, Perfmon, NetFlow
- Besondere Funktionen
 - z.B. Ersatz für TMG Veröffentlichung
 - URL/Header/Content-Rewriting
- Plattform
 - Hardware, Virtuell, Cloud
- Bedienung/GUI
 - Die Standardaufgaben sollte per GUI zu lösen sein.
 - Command Line Interface erforderlich ?
- Applikationssupport
 - Prüfen sie, ob der Hersteller entsprechende Anleitungen bereitstellt
 - Zertifizierung
 - Exchange 2010: <http://technet.microsoft.com/en-us/exchange/gg176682.aspx>
 - Lync: <http://technet.microsoft.com/en-us/lync/gg131938.aspx>

Datenblatt: Loadbalancer



Merkmale	Beschreibung
Funktionsweise	<ul style="list-style-type: none">• Loadbalancer ist der Endpunkt für den Clients• Loadbalancer setzt Anfragen Um (DNAT, SNAT, HTTP-Proxy)• Loadbalancer ist selbst hochverfügbar
Umsetzung	<ul style="list-style-type: none">• Hardware oder virtuelle Maschine• „Single Leg“ im gleichen LAN oder „Dual Leg“ mit zwei Netzwerken
Verfügbarkeit	<ul style="list-style-type: none">• Kann aktiv Dienste überwachen• „Geplante Wartung“ möglich
Lastverteilung	<ul style="list-style-type: none">• Variable Verteilung der Verbindungen• Berücksichtigung von Serverlast und Antwortzeiten
Affinität	<ul style="list-style-type: none">• Umfangreiche Regeln.
SSL Offloading	<ul style="list-style-type: none">• Möglich zur Entlastung des Backen• Erforderlich um Affinität bei https mit Cookies/Header zu erlauben
Client	<ul style="list-style-type: none">• Keine Besonderheit zu berücksichtigen• TCP-Reconnect erforderlich, wenn Knoten ausgefallen ist.

Wer einmal einen Loadbalancer genutzt hat, wird NLB nicht mehr anschauen. Vieles wird sehr viel einfacher, leistungsfähiger und stabiler.

Was mit mit....

- TMG 2010
 - Erlaubt Veröffentlichung von HTTP-Dienste per Loadbalancing
 - Kann Webserver „Proben“
 - Kein Loadbalancing für andere Dienste
 - Nutzt NLB für eingehendes Loadbalancing
- IIS Application Request Routing
 - Erlaubt Anfragen auf mehrere Backend Server zu verteilen
 - Muss selbst aber wieder Hochverfügbar gemacht werden (NLB o.ä.)
 - Einsatzzweck ist Application Performance, Caching, etc.
- WAP – Web Application Proxy
 - Einfacher Reverse Proxy mit ADFS Preauthentication
 - Kein Loadbalancing zum Backend
 - Keine Loadbalancing für eingehende Verbindungen

Gegenüberstellung der Verfahren

Merkmale	IP Failover	DNS RR	NLB	Loadbalancer
Überprüfung des Backend	Ja	Keine Prüfung	Keine Prüfung	Aktive Tests
Lastverteilung	Aktiv/Passiv	Round Robin	Hash-Verfahren	Round Robin, Least Connection, Sourcehash, Responsetime. u.a.
Affinität Layer 4	Entfällt	Abhängig vom Client.	Source IP Source Subnet	Source IP
Affinität Layer 7	Entfällt	Nein	Keine	Cookie AuthHeader URLs u.a.
SSL Offloading	Nein	Nein (1)	Nein (1)	Ja

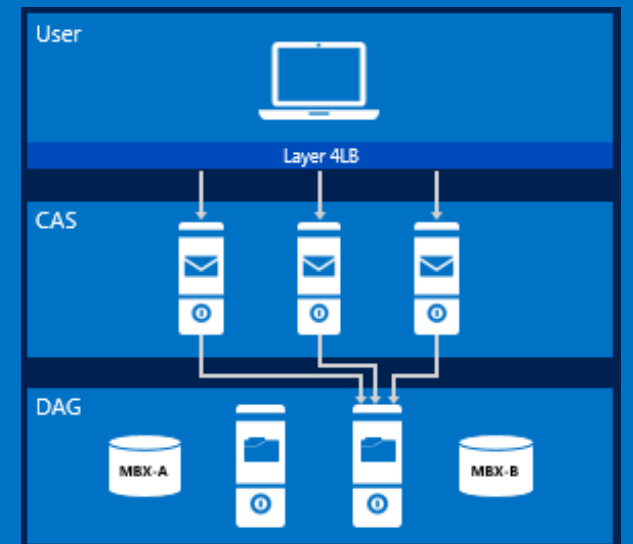
(1) z.B. in Verbindung mit Reverse Proxy (AAR, TMG, WAP o.ä.)

Verfügbarkeit
nach Diensten

Exchange

- Exchange 2010
 - Viele Dienste benötigen eine Affinität
 - NLB mit SourceIP oder HLB mit Layer 7
 - SessionID /Cookie / SSL
 - MAPI/RPC bitte Ports fixieren.
- Exchange 2013
 - CAS-Rolle ist „Reverse Proxy“. DNS-RR möglich
 - LB ratsam um CAS-Rolle selbst erreichbar zu machen
 - Office 365 als Innovationstreiber, 2000er Client Limit
 - NLB supportet ABER nicht auf MSCluster möglich
- Mailbox Storage
 - Ohne Zweifel: Database Availability Group

Affinity 2010	Muss	Ratsam	Nein
	OWA	RPC/HTTP	OAB
	ECP	EAS	Autodiscover
	EWS	Addressbook	POP3
	RPC	PowerShell	IMAP4



Lync

- SIP-Services
 - präferieren DNS RR
 - Lync Server untereinander machen DNS RR
 - Lync 2010/2013 Client unterstützen DNS RR
 - Edge unterstützt DNSRR
- Einschränkungen
 - OCS2007R2 Clients
 - Public Federation
- Lync Web Services
 - HTTP-Zugriff von Clients - Loadbalancer erforderlich

Lync SIP-Verfügbarkeit

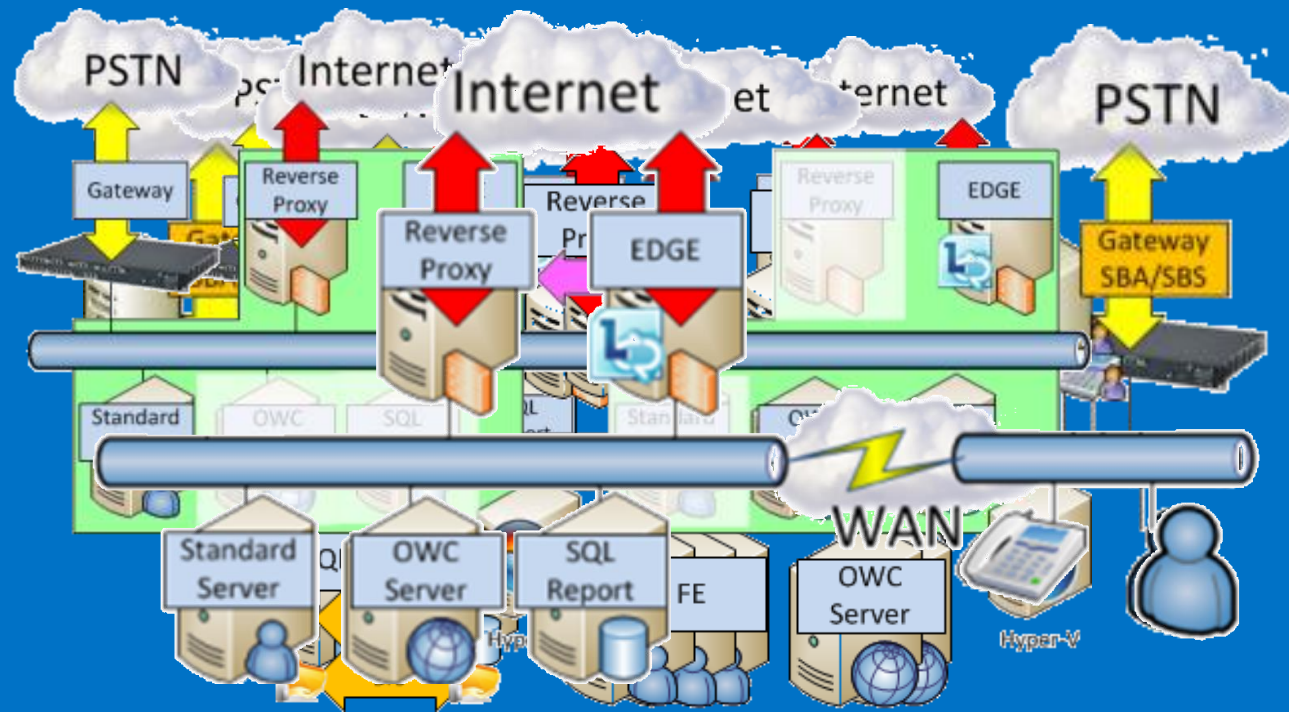
- Failover zu alternative Gegenstelle.

Timeout	Von	Zu	Beschreibung
1,5 Sek	Mediation	Gateway	Auf ein INVITE muss ein 100 Trying kommen
4 Sek	Mediation	Gateway	TLS-Socket Fehler (nur zwei SYN !)
10 Sek	Mediation	Gateway	Auf ein INVITE muss ein RINGING kommen Oder „183 Session Progress“
10 Sek	Lync	Exchange UM	Zeitspanne, die ein Exchange UM Server den Ruf annehmen muss

- Ansonsten zieht Lync den Call mit einem CANCEL zurück und geht einen alternativen Weg
- DNS-RR und logische Failover perfektioniert
- Siehe auch <http://www.msxfaq.de/lync/technik/lynctimeouts.htm>

Lync Server Verfügbarkeit

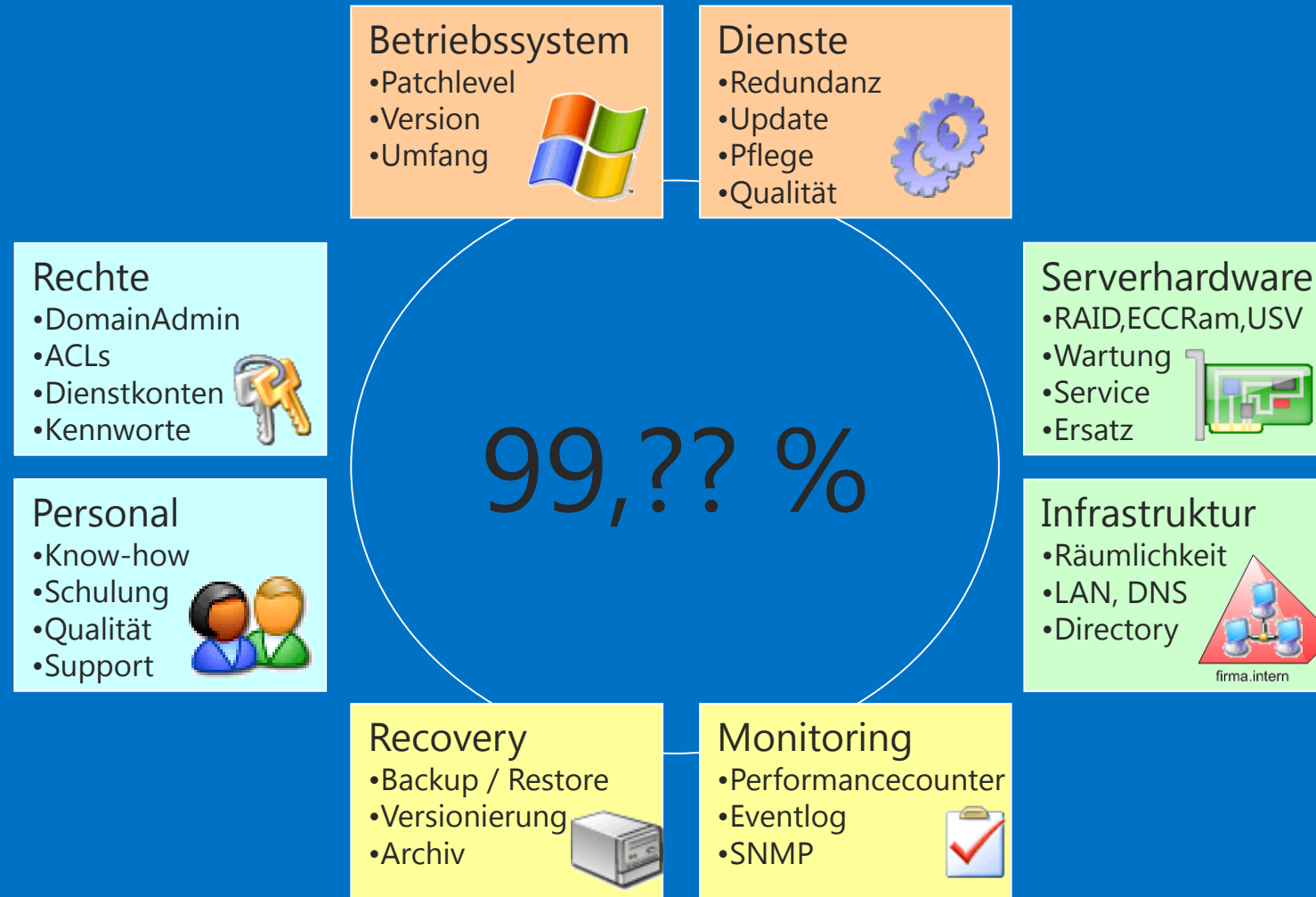
- SBA
- Cluster
- HyperV
- Backup Pool



Verfügbarkeit „eingebaut“...

- IP-Adressvergabe DHCP
 - mehrere DHCP-Server korrekt konfiguriert
 - Überlappende Bereiche mit Prüfung, Achtung vor NACK
 - Splitt-Bereiche (50% Abdeckung)
- IP-Routing
 - Mehrere Router und Leitwege mit Dead Gateway Detection
 - „virtuelle“ Router
- Namensauflösung DNS
 - Mehrere DNS-Server, bitte alle mit dem „gleichen“ Kenntnisstand
- Mailversand zwischen SMTP-Servern
 - MX-Records und Failover
- Anmeldedienste
 - Windows Client kann mit mehreren Domain Controllern umgehen
 - Aber andere LDAP-Anfragen vielleicht nicht
- Storage Replikation
 - SAN, DFS, RAID, DAG

Verfügbarkeit



Weitere Links

- DNS Round Robin
<http://www.msxfaq.de/cluster/dnsroundrobin.htm>
- NLB Loadbalancing
<http://www.msxfaq.de/cluster/nlb.htm>
- MiniSFT
<http://www.msxfaq.de/cluster/minisft.htm>
- NLB vs. HLB
<http://www.msxfaq.de/cluster/nlbvshlb.htm>
- DAG vs. VM
<http://www.msxfaq.de/cluster/dagvsvmha.htm>
- Exchange 2013: Load balancing
[http://technet.microsoft.com/en-us/library/jj898588\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/jj898588(v=exchg.150).aspx)

