Schnellstraße in die Cloud

Ist ihre Netzwerk-Infrastruktur bereit?

Frank Carius

IT vNext
Technologien richtig nutzen!

Net at Work
Building IT-Excellence.

Über mich

IT vNext
Technologien richtig nutzen!

- Net at Work
  - Standort Paderborn
  - Gegründet 1995
  - 45 Mitarbeiter
  - IT-Systemintegration und Software Development
- Frank Carius
  - Microsoft MVP für Skype for Business
  - Microsoft Certified Master Lync 2010
  - Betreiber von www.msxfaq.de
- Schwerpunkte
  - Exchange
  - Skype for Business
  - Office 365
  - Infrastruktur: AD, ADFS, DirSync, Netzwerk
  - Mail Encryption und Signierung, NoSpamProxy

Net at Work
Building IT-Excellence.

Microsoft Partner
Gold Messaging
Gold Communications
Gold Collaboration and Content
Gold Application Development

Microsoft CERTIFIED Master

MVP Microsoft Most Valuable Professional

www.msxfaq.de

noSpam proxy

Wer ist denn schon in der Cloud ?

Cloud ist neu

Macht doch noch keiner ernsthaft

Randbedingungen

IT vNext
Technologien richtig nutzen!

- Cloud ist nicht neu
  - Telefonanschluss ist eine „Hosted TK-Anlage
  - Private Webseiten und Postfächer (1998: GMX/WEB.DE, MSXFAQ seit 1999)
  - Brief- und Pakettransport (Post)
  - Banken, Steuerberatung (Datev-Hosting), Buchhaltung (SAP-Hosting)
- Geräte, Bandbreiten, Kosten
  - Mobile Nutzer, mehrere Geräte
  - Sehr gute Verfügbarkeit des „Internet“
  - Deutlich gefallene Kosten
  - Mieten statt kaufen
- Der Betreiber
  - Welches Land, welches Rechtssystem ?
  - Welche Firma, welche Personen ?
  - Welche politischen Einstellungen ?
  - Stabilität, Erreichbarkeit, Kontinuität der Produkte
- Ist ihre „OnPremise-Umgebung“ sicherer ?
  - Physikalischer Zugangsschutz zum Server
  - „Vertrauenswürdige Administratoren
  - Wasserdichtes Auditing/Monitoring

Bandbreitenklasse	Ende 2010	Ende 2011	Ende 2012	Ende 2013
≥ 1 Mbit/s	98,3%	99,1%	99,7%	99,9%
≥ 2 Mbit/s	93,3%	95,7%	97,3%	99,4%
≥ 6 Mbit/s	81,7%	87%	90,2%	94,6%
≥ 16 Mbit/s	67,9%	71,4%	75,9%	77,8%
≥ 50 Mbit/s	39,5%	48,2%	55%	59,7%

Wer ist schon in der Cloud ?

IT vNext
Technologien richtig nutzen!

- UPN-Domain prüfen
  - `Nslookup -querytype=TXT <domain.tld>`
  - Gibt es einen „ms=*“ Eintrag?
- ADFS-Test
  - https://login.onmicrosoft.com ansurfen
  - Benutzername aus der Domäne angeben und OK klicken
  - ADFS-Umleitung abwarten
- Mailrouting
  - `nslookup -querytype=MX <domain.tld>`
    Zieladresse <tenantname>.mail.protection.outlook.com ?
  - `nslookup -querytype=A autodiscover.<domain.tld>`
- Skype for Business Online
  - `nslookup -querytype=A lyncdiscover.<domain>`
  - `nslookup -querytype=SRV _sip._tcp.<domain>`
  - `nslookup -querytype=SRV _sipfederationtls._tcp.<domain>`
- SharePoint
  - `http://<tenantname>.sharepoint.com`
  - Meldet sich ein SharePoint Server ?

Stichprobe:

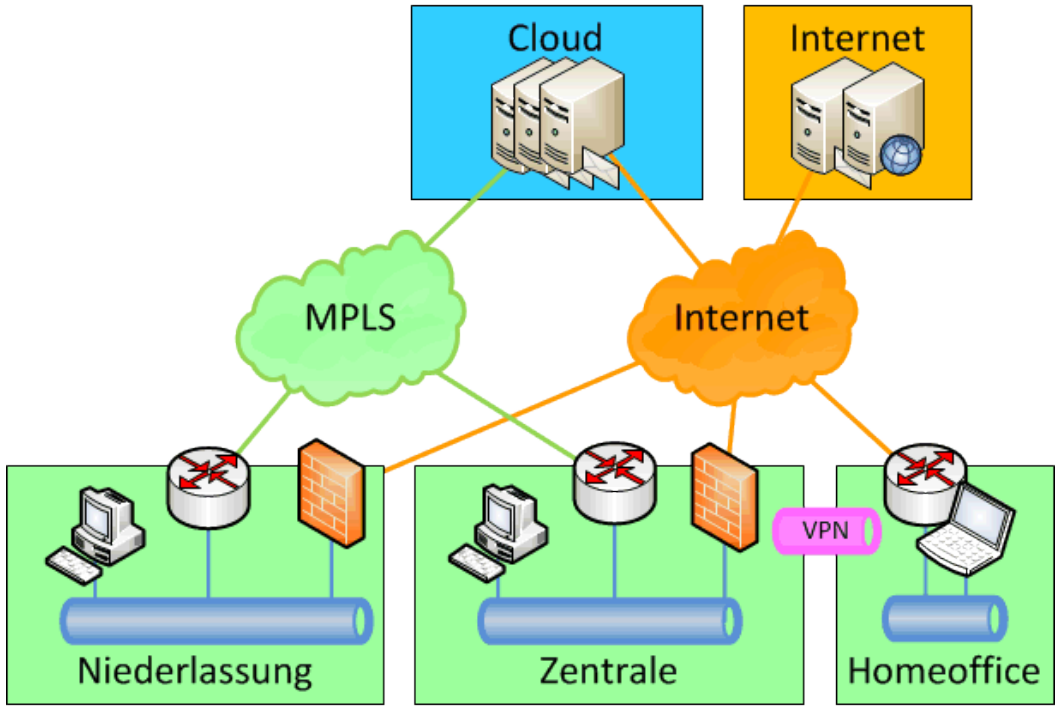
basf.com
siemens.com
rwe.com
welt.de
eon.com
bayer.com
thyssenkrupp.com
spiegel.de
bild.de
sueddeutsche.de
faz.de
carlsberg.de
netatwork.de

Bestandsaufnahme Ihre eigenes WAN

Zentrale, Niederlassung, Homeoffice, Cloud, Internet

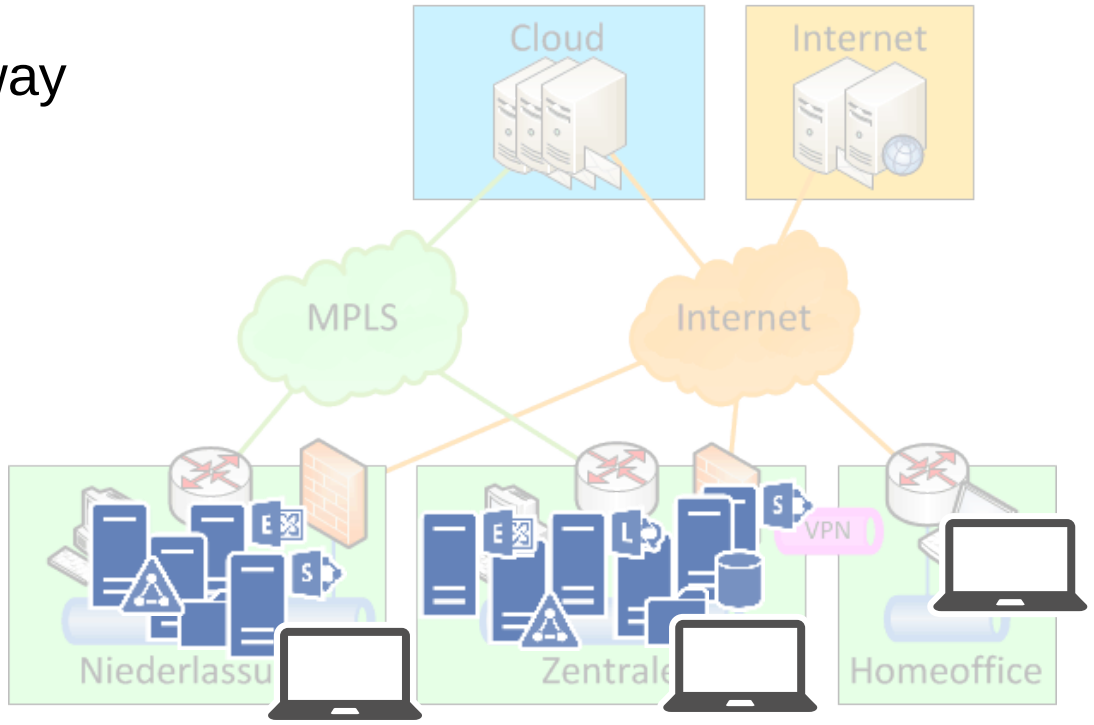
Die Umgebung

- Externe Dienste
  - Cloud
  - Internet
- WAN
  - Internet
  - MPLS/VPN
- Firmennetzwerk
- Zentrale
- Niederlassung
- Homeoffice



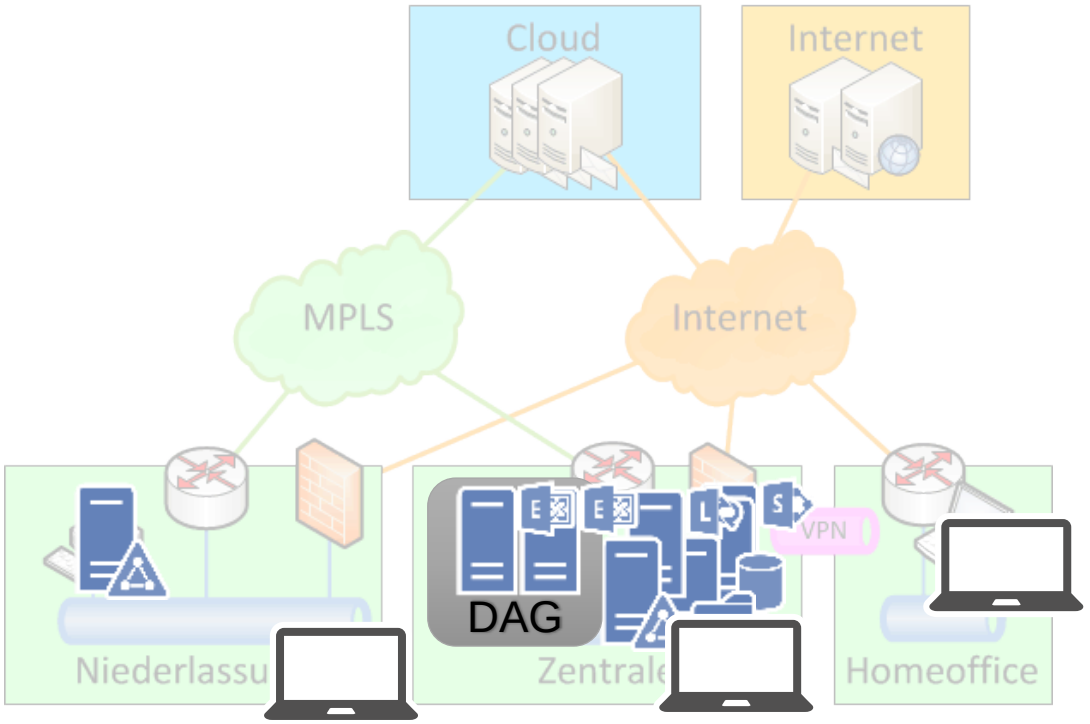
Die „dezentrale “ Firma

- Lokale Server
- Begrenzte Bandbreite
- Zentrales Internetgateway
- VPN für Clients
- Relativ geschlossen
- „Surfen und Mail“



Die „zentralisierte“ Firma

- Zentrale Dienste
- Mehr Bandbreite
- Hochverfügbarkeit
- Virtualisierung
- Client
- OST-Datei
- Branch Cache
- Remotezugriff
  Outlook Anywhere



Der ideale Office 365 Kunde

Services

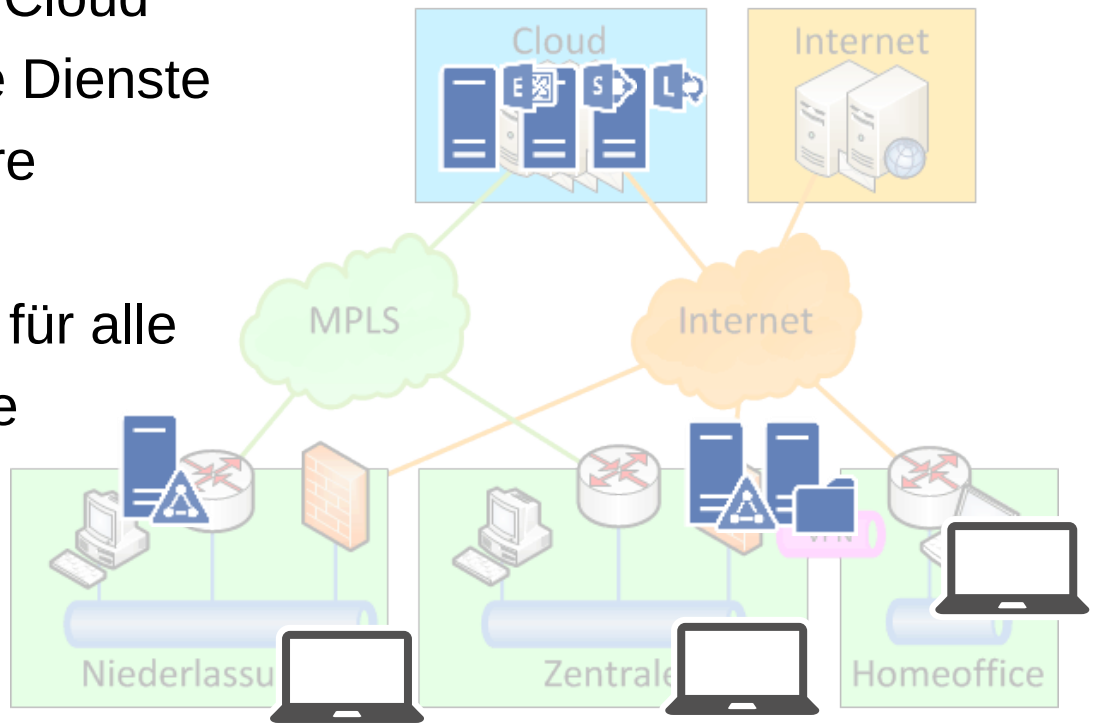
- Zentrale Dienste in der Cloud
- Lokales AD und wenige Dienste
- Weitere Dienste in Azure

WAN

- Lokaler Internetzugang für alle
- Ausreichend Bandbreite

Clients

- OST-Datei
- Branch Cache

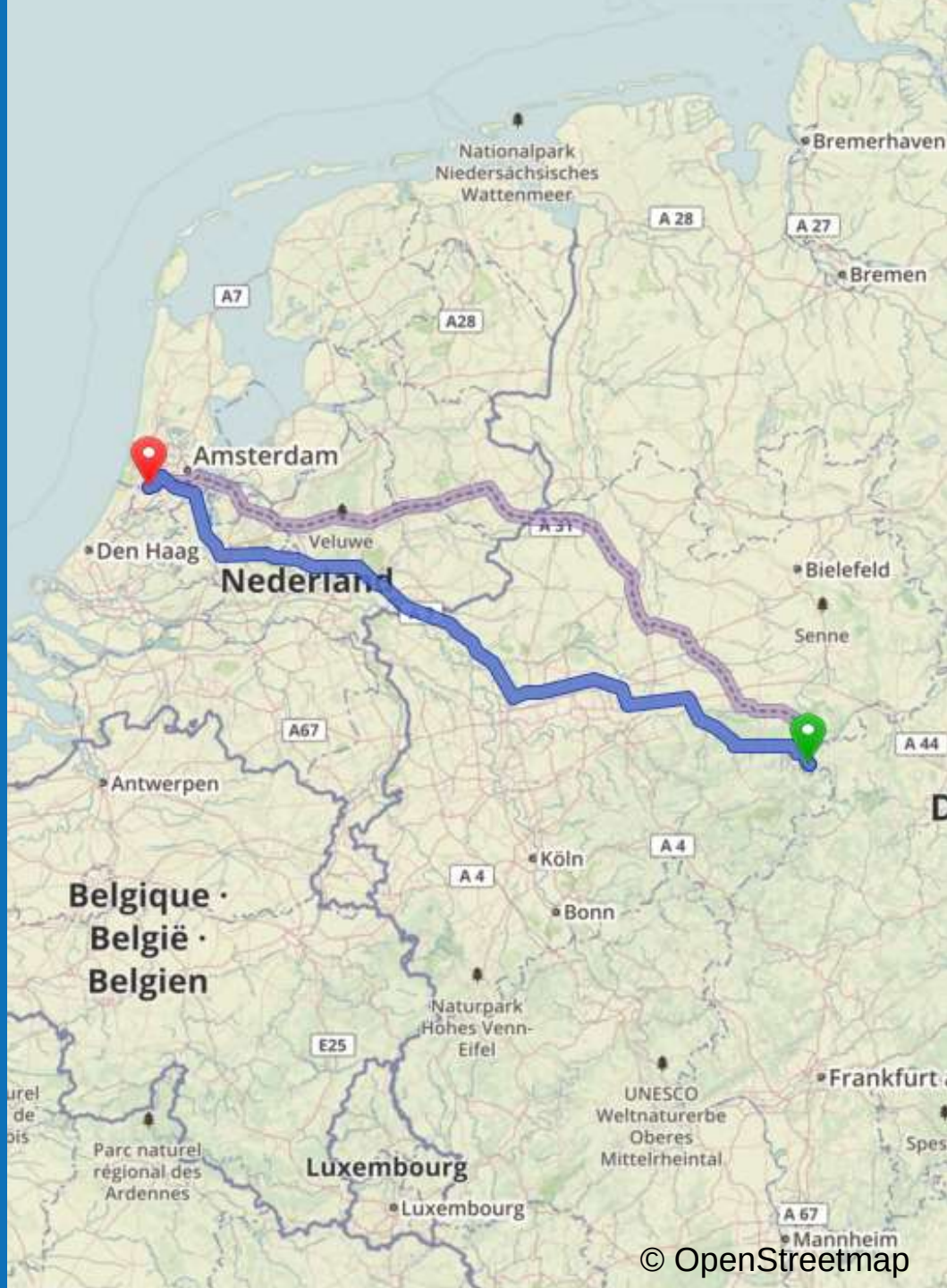


WAN-Strecken

MPLS

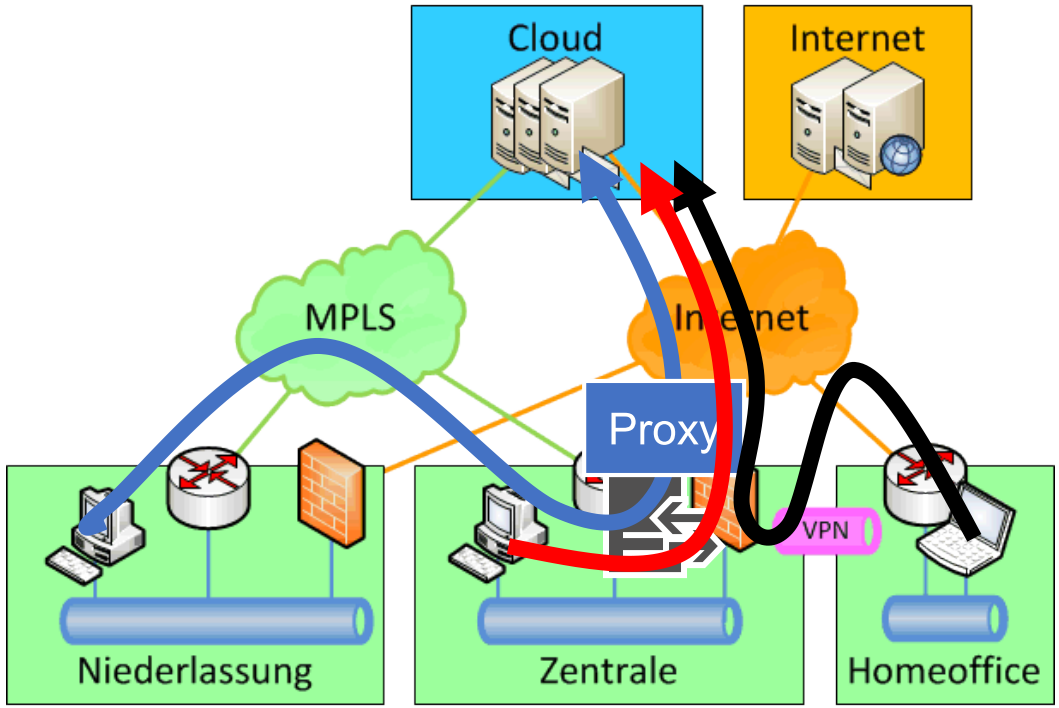
VPN

Express Route



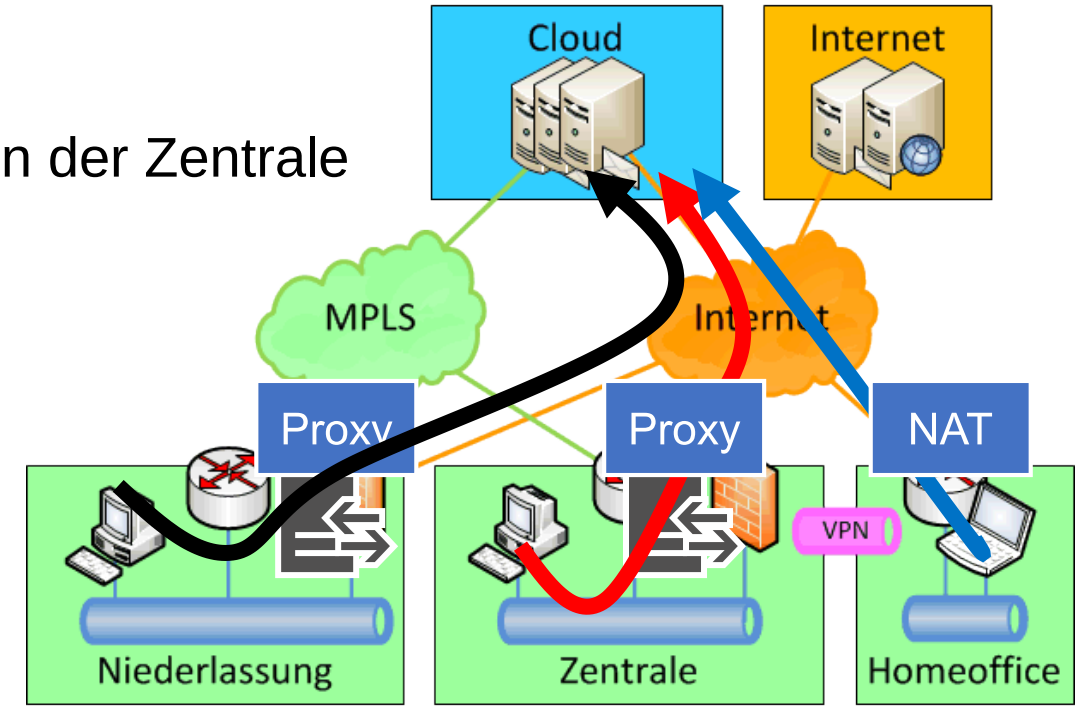
Zentralproxy der Firma

- Klassisch für „sicherere Firmen“
- Wenige Firewalls
- Ineffektiv für Office 365
- Viel Bandbreite
- Lange Wege



Lokale Breakouts

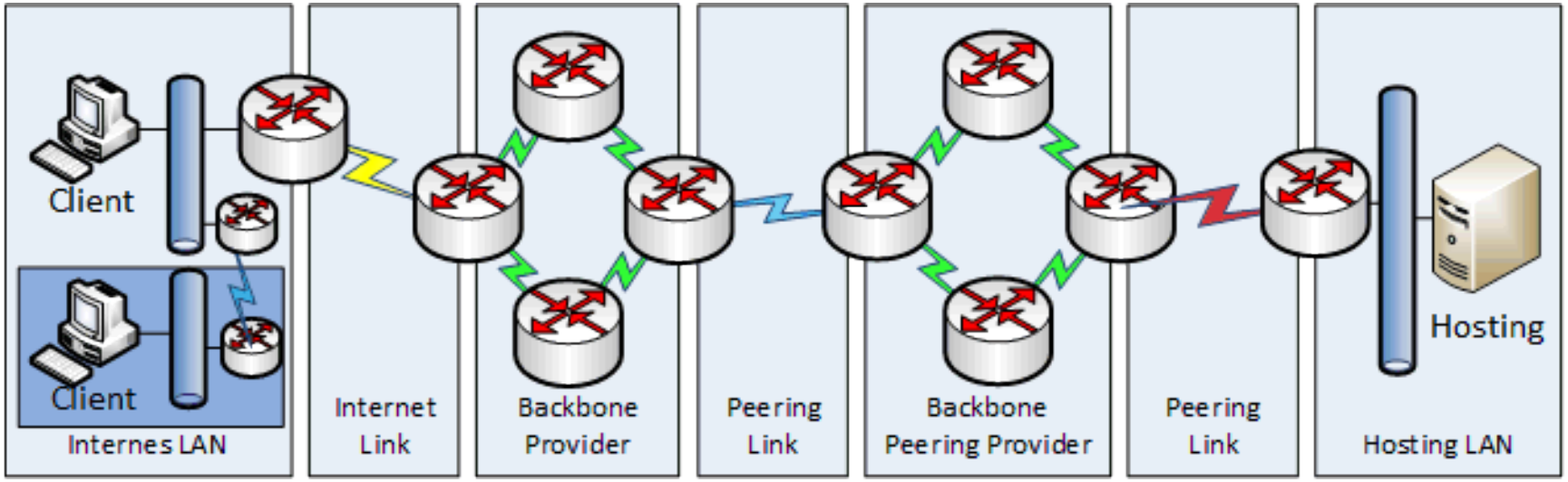
- Zusätzliche Übergänge ins Internet
- Zusätzliche Proxyserver
- Kurze Weg
- Weniger Abhängigkeit von der Zentrale
- Oft günstigere Bandbreite



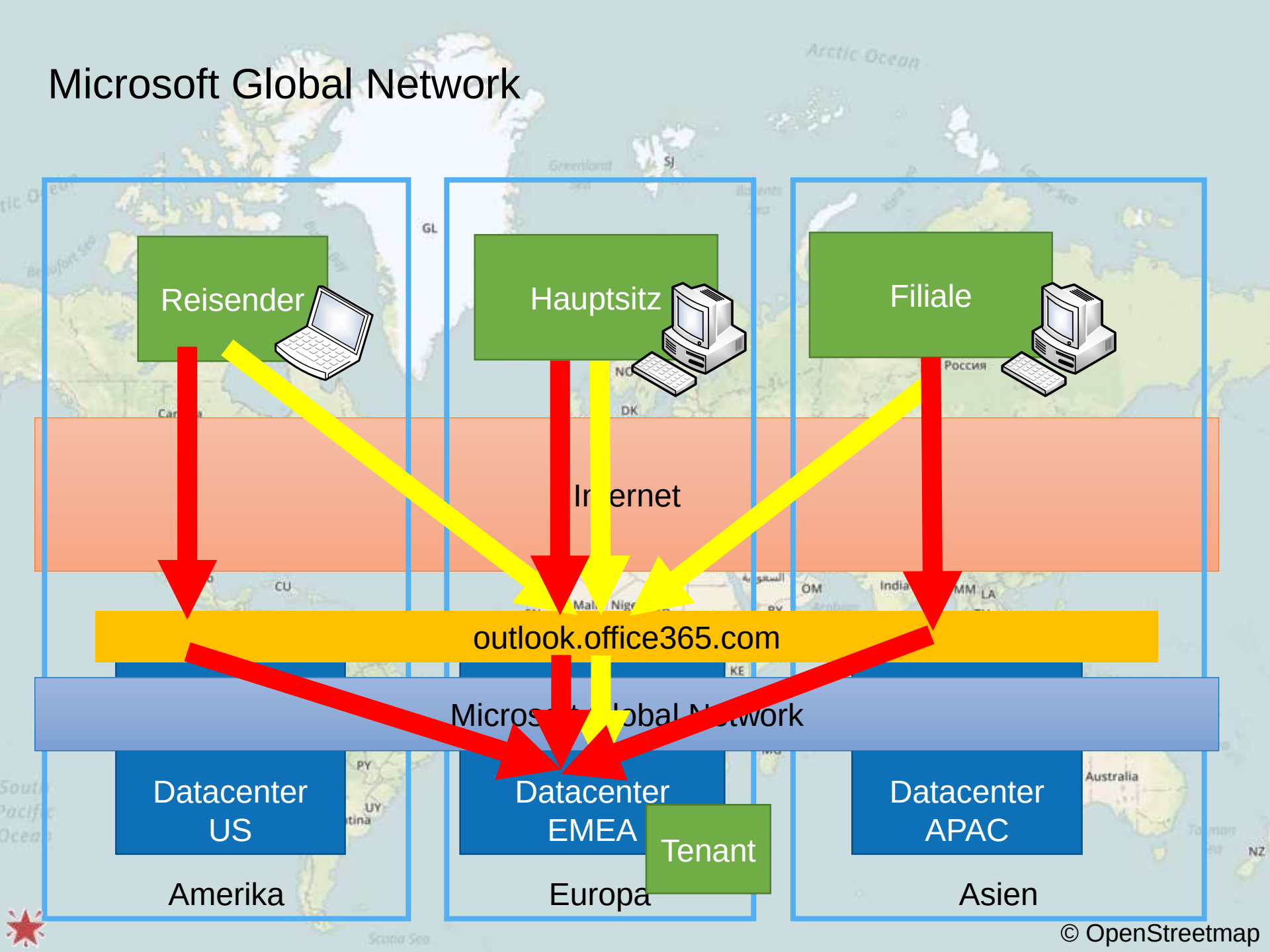
Cloud über Internet

IT vNext
Technologien richtig nutzen!

- Nutzung der normalen Internet Verbindung
  - Kein SLA zur Verfügbarkeit
  - Keine Bandbreitengarantie
  - Keine Laufzeitgarantie
- Wettbewerb mit YouTube, Netflix und Co.
- Unklare Peerings



Microsoft Global Network



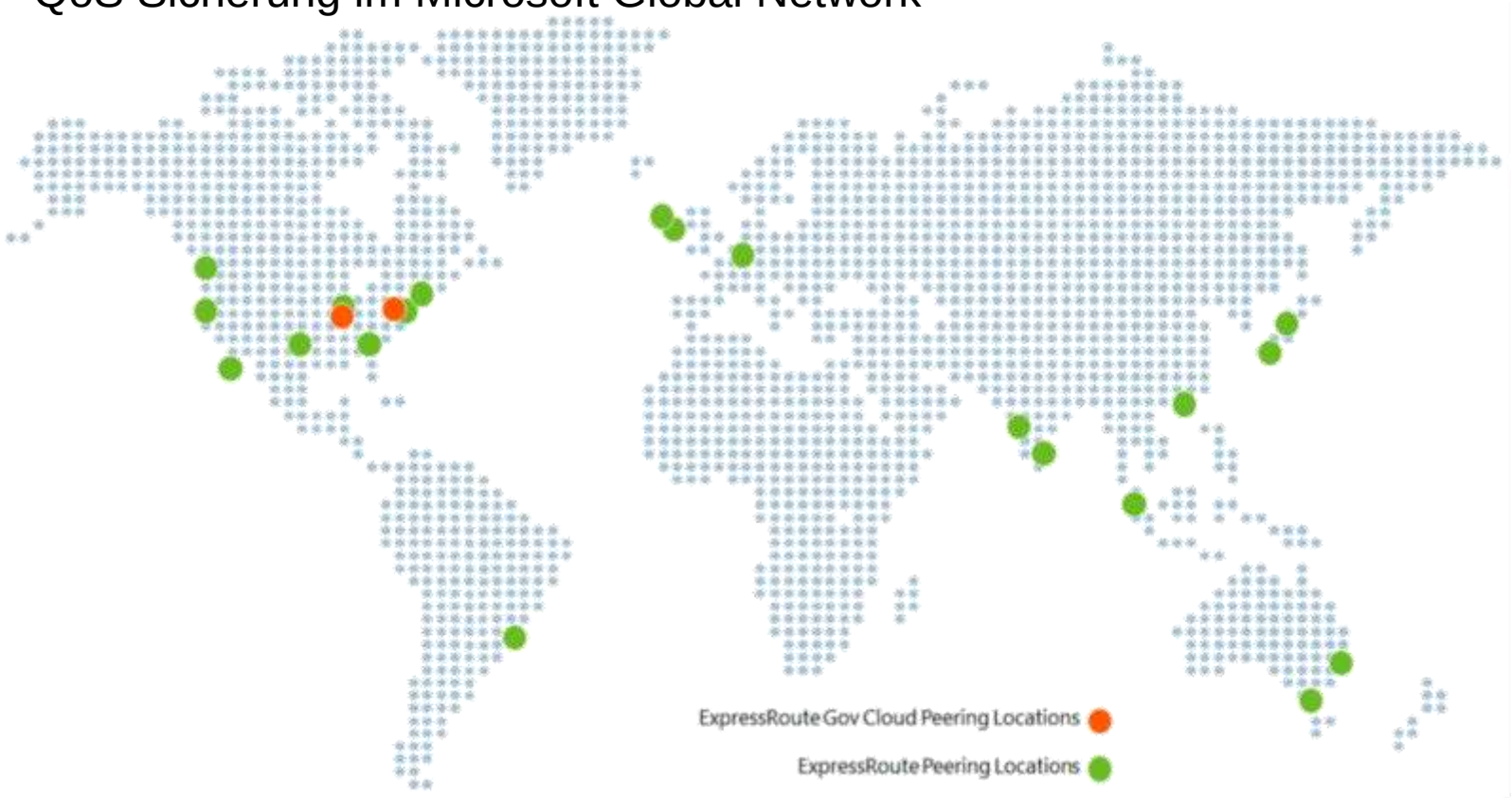
GeoDNS

- `NSLOOKUP outlook.office365.com <ip DNS-Server>`
  - z.B. von http://www.ungefiltert-surfen.de/
- DNS-Abfragen in der Welt: (Stand 18. Feb 2016, ohne IPv6 Adressen)

Region	BR	UK	DE	TW
DNS-Server	152.250.250.178	109.204.97.30	Telekom	118.143.233.5
Name	outlook-namsouth2.office365.com	outlook-emeawest2.office365.com	outlook-emeaeast2.office365.com	outlook-apaccentral.office365.com
IPv4	40.96.0.98 132.245.245.178 132.245.16.242 132.245.15.210 132.245.68.130 132.245.53.2 132.245.245.194 132.245.58.146	40.101.1.82 132.245.212.98 132.245.27.34 132.245.77.18 132.245.195.162 132.245.226.50 132.245.226.34 132.245.228.2 132.245.176.66 132.245.55.178	40.101.0.2 132.245.67.82 134.170.68.82 132.245.34.34 132.245.61.226 132.245.35.98 132.245.51.50 132.245.74.114 132.245.229.178 132.245.76.226	40.96.1.210 40.96.2.114 40.96.13.146 40.100.0.210 132.245.69.50 132.245.41.114 132.245.43.98 132.245.254.242

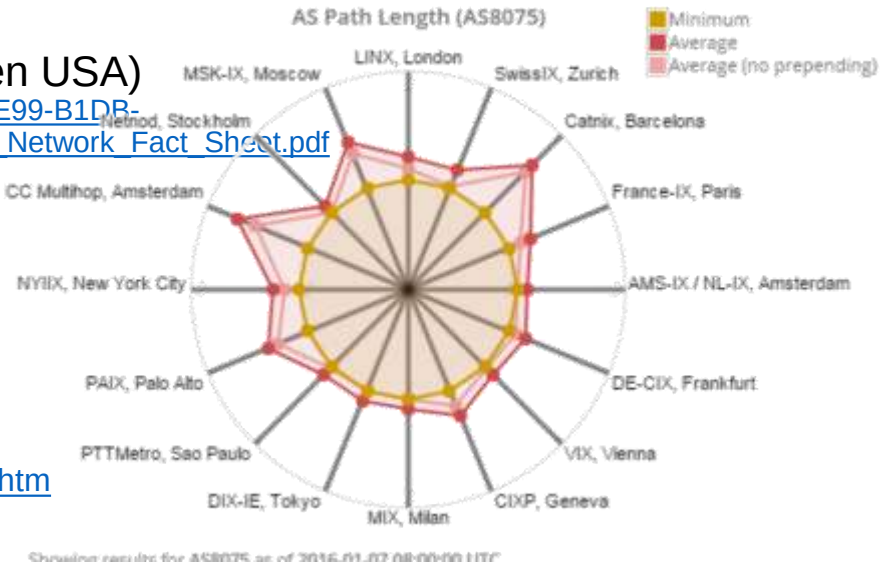
Microsoft Global POPs

- Weltweite Übergänge
  - https://azure.microsoft.com/en-us/documentation/articles/expressroute-locations/
  - DNS leitet den Client zum nächsten Zugang
  - „Kurze Wege“ über das Internet
  - QoS Sicherung im Microsoft Global Network



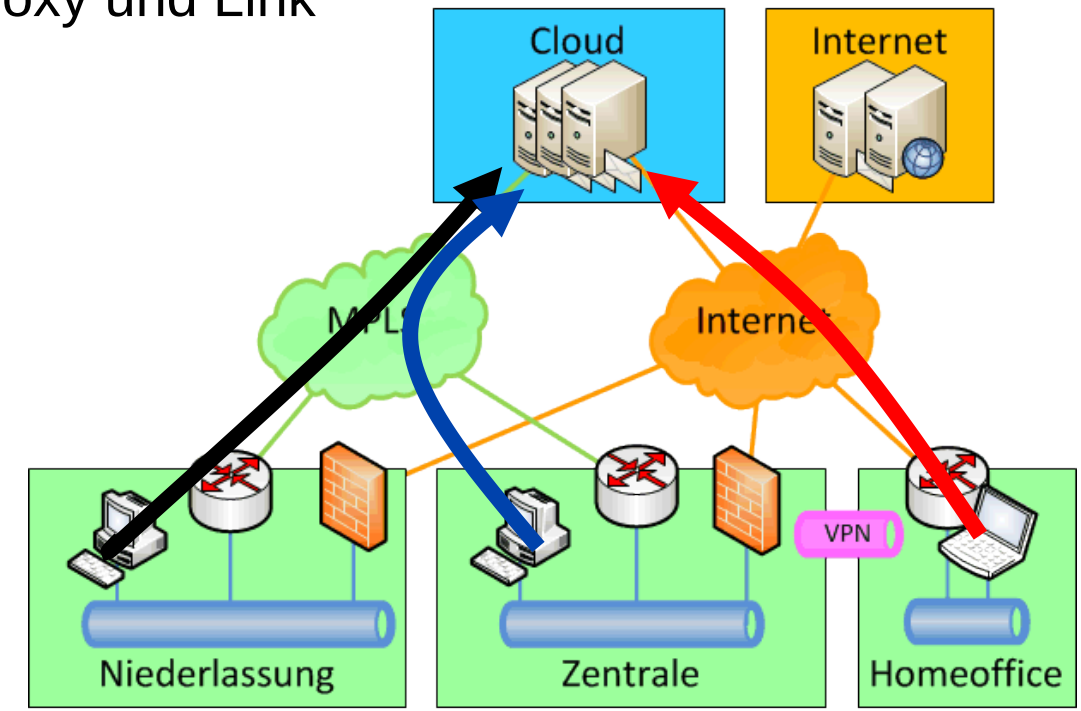
Microsoft Global Network

- Microsoft betreibt ein sehr großes WAN
  - über 100 Sites, über 1800 ISP Partner
  - Mehrere Terabit Peering (10% Utilization)
  - Eigene Glasfaser (angeblich 800.000km in den USA)
    http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf
  - Komplett QoS -Managed
- BGP: Microsoft ASN= 8075
  - https://stat.ripe.net/AS8075#tabId=at-a-glance
  - IPv4 prefixes: 149: insgesamt 20.184.320 IPs
  - IPv6 prefixes: 10: insgesamt 8.589.324 /48s
  - http://www.msxfaq.de/cloud/verbindung/o365_netzwerkziele.htm
- www.peeringdb.com
  - https://www.peeringdb.com/private/participant_view.php?id=694
  - Deutlich mehr Links als z.B. große Carrier



WAN-Kopplung

- „Privates“ Internet mit QoS-Option
- Entlasten des Internet Proxy und Link
- Azure Express Route



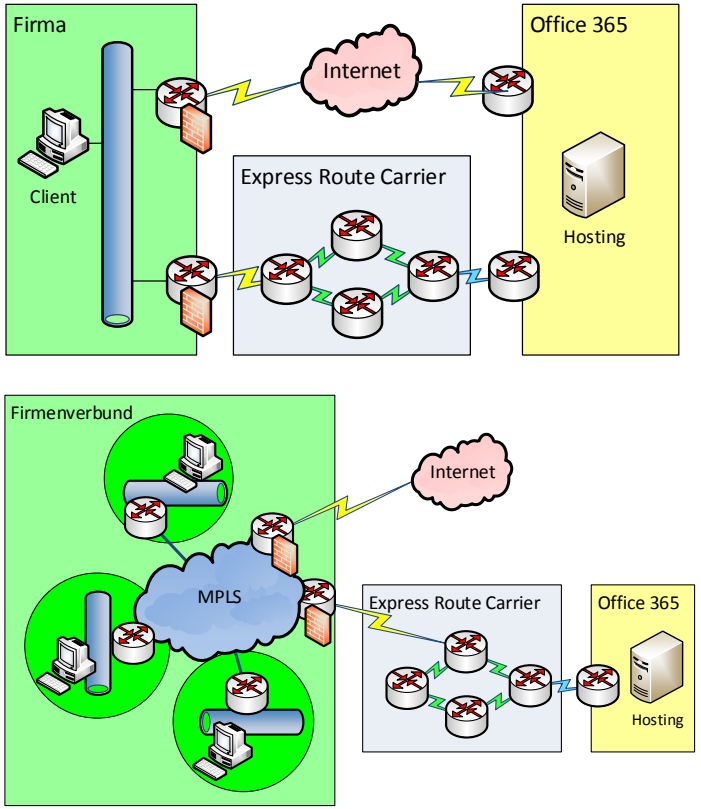
Express Route

IT vNext
Technologien richtig nutzen!

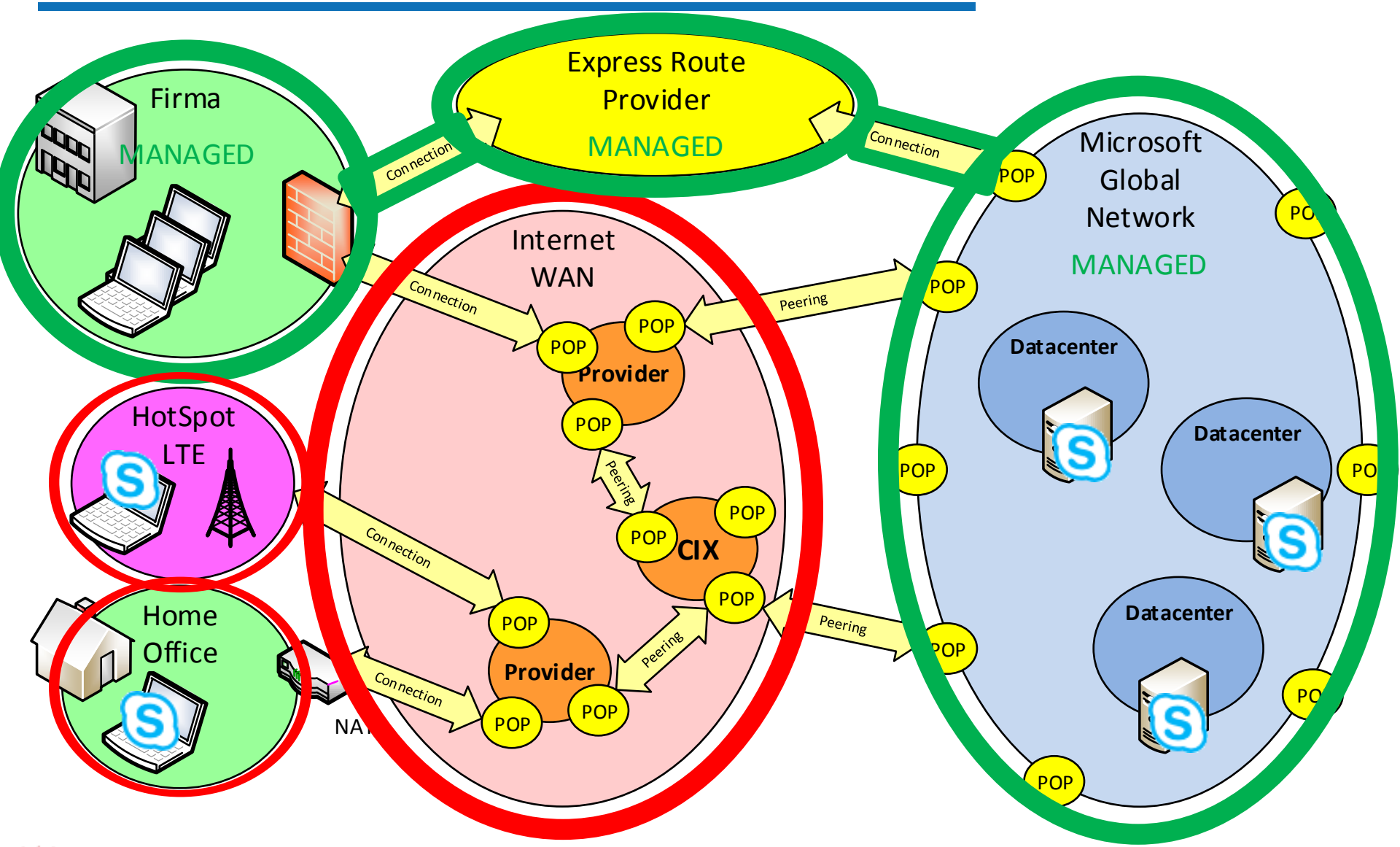
- Verträge und Kosten
  - Sie kaufen bei Microsoft einen Port
    - mind. 50 Megabit, max. 10 Gigabit
    - https://azure.microsoft.com/de-de/pricing/details/expressroute/
  - Sie kaufen die Verbindung bei einem teilnehmenden Provider
    - https://azure.microsoft.com/de-de/partners/directory/
- SLA, Bandbreite und QoS
  - Express Route kann SLAs garantieren
  - Express Route garantiert eine nutzbare Bandbreite bis zu Office 365
  - Achtung: Nicht alle Provider unterstützen QoS innerhalb der ER Bandbreite
- Technik
  - Es ist kein VPN oder eine private Verbindung
  - Zieladressen bleiben die „öffentlichen“ Office 365-Adressen
  - Über Routing (BGP) werden die Pakete über den neuen Weg geroutet
    Achtung: bei Azure Netzwerkverbindungen mit privaten Adressen
  - Proxy/NAT erforderlich mit privaten internen Adressen

Express Route Anbindung

- Single Link
  - Eine 1:1 Verbindung
  - Gut bei zentralem Standort
  - Keine Entlastung des eigenen WAN
- Firmen-Link
  - Verbindung aller Standorte
  - WAN-Provider addiert Office 365 wie einen weiteren Standort
- Weitere denkbar
  - Multisite-Links
  - IP VPN



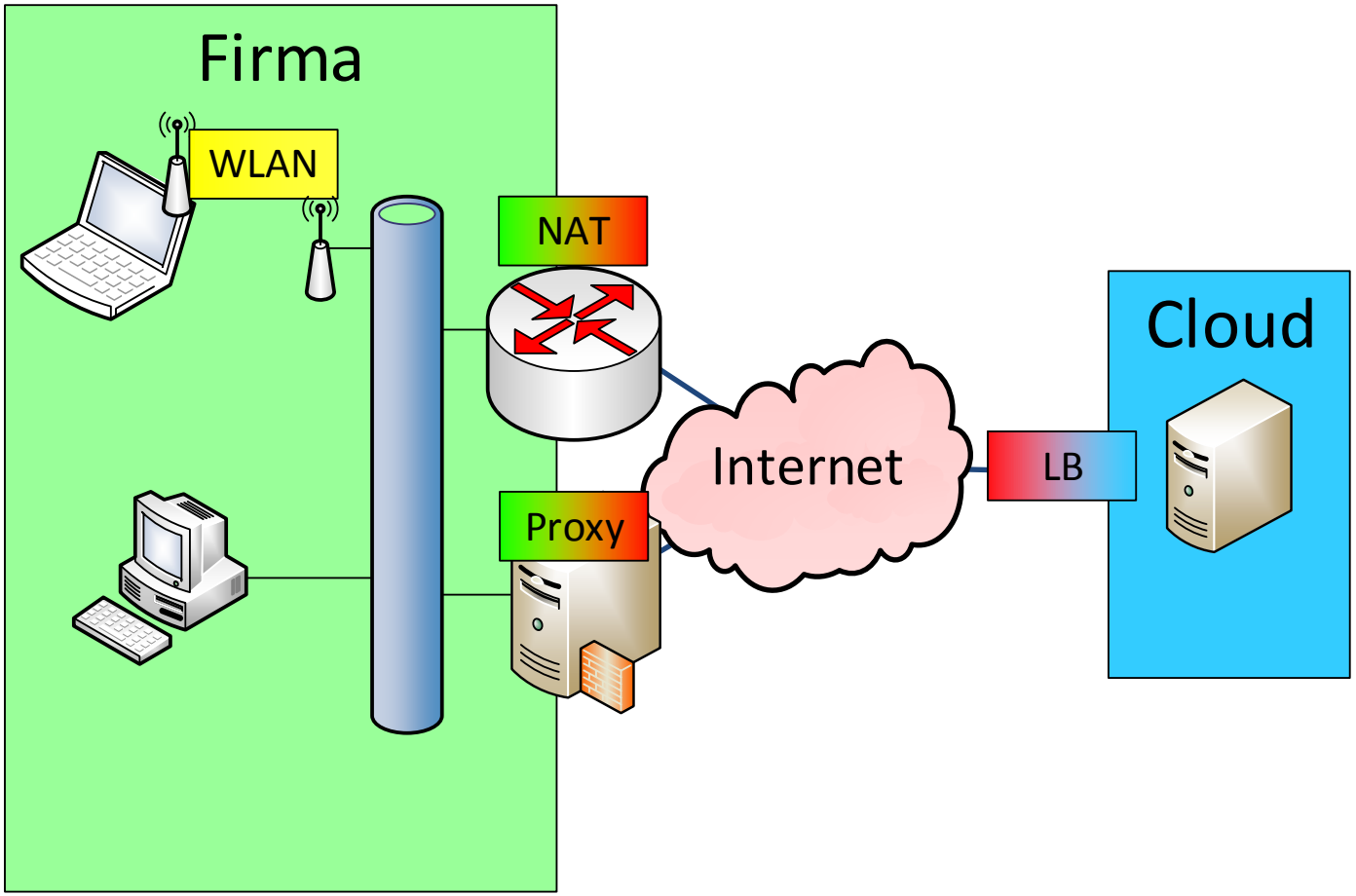
Managed vs. Unmanaged



Zwischenstationen

Proxy, Router, Firewall, Loadbalancer

Besonderheiten der Anbindung

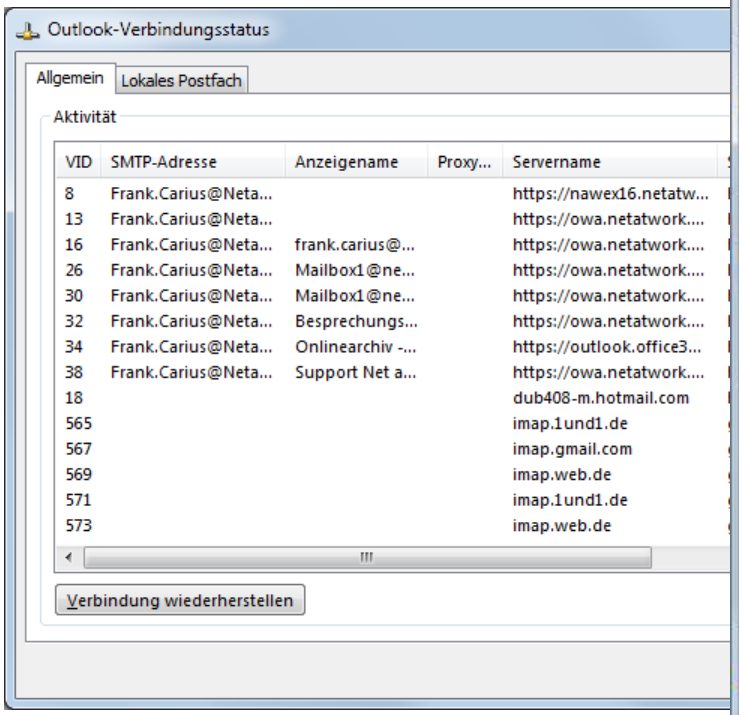


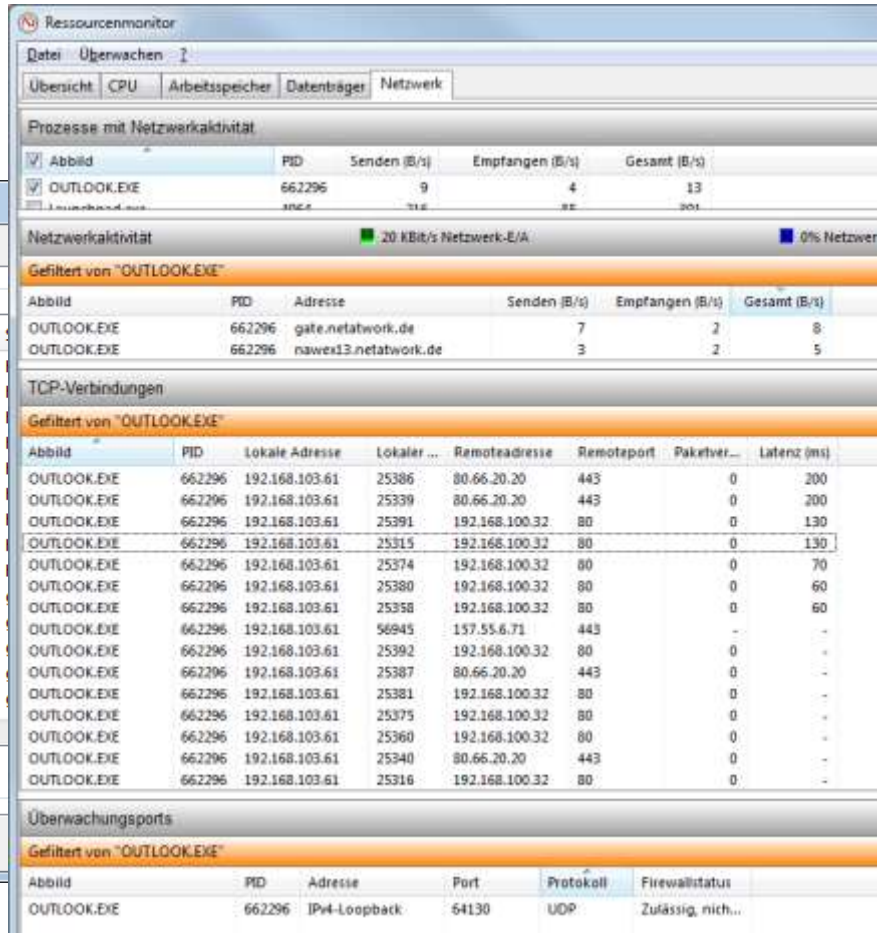
Outlook: Ports und Connections

IT vNext
Technologien richtig nutzen!

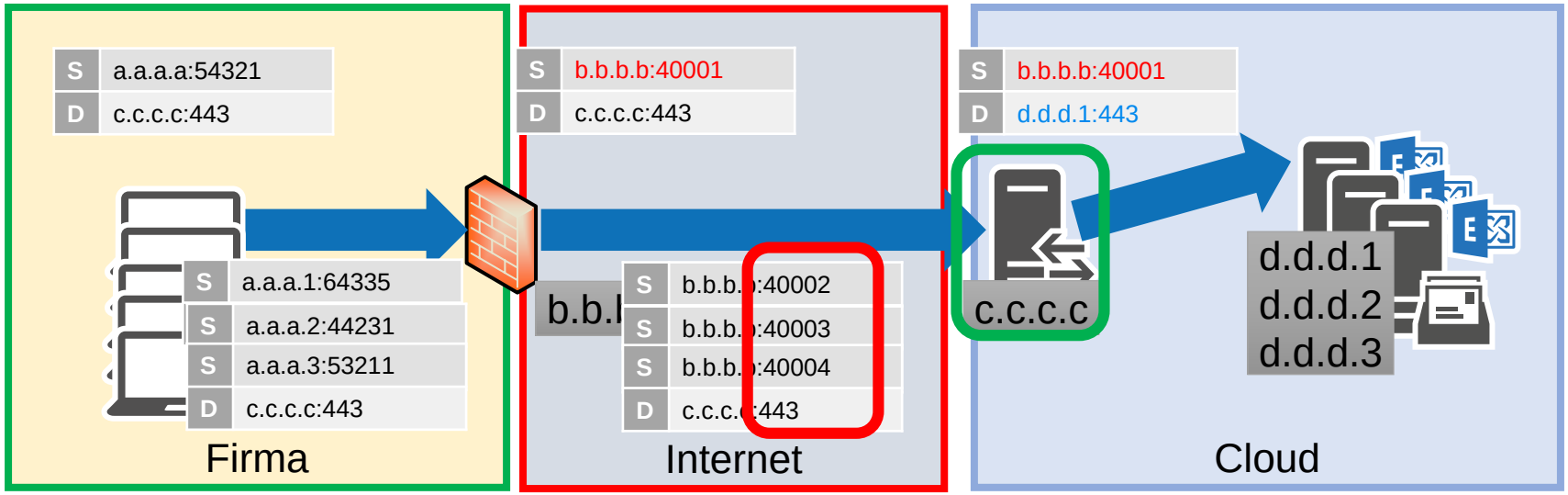
Mehrere Verbindungen

- Eigenes Postfach, Stellvertreter
- Public Folder, Adressbuch
- EWS-Abfragen
- POP/IMAP Konten





NAT und Proxy und die 65535 Ports



- Max 65535 ausgehende Ports
- „langlaufende“ HTTP-Sessions

- Loadbalancer
- Affinität nach Source-IP

Port-Mathematik

IT vNext
Technologien richtig nutzen!

- Port für einen „typischen Client“
  - Outlook : 10 - 20 Connections
  - Skype for Business: 5 - 10 Connections
  - Browser: 5 - 50 Connections
  - Annahme: 40 relevante Verbindungen Richtung Office 365
- Firma mit 5.000 Anwendern
  - 200.000 gleichzeitige TCP-Sessions !
  - „Single External IP“ reicht nicht mehr
  - Optimierung des Client möglich

Nachschauen !
- Ressourcen Monitor
- Netstat
- Perfmon
  IPv4: Hergestellte Verbindungen
- SNMP

Microsoft: max. 6000 Clients hinter einer IP-Adresse.
Network Address Translation (NAT) support with Office 365
http://msdn.microsoft.com/en-us/library/dn850366.aspx

TCP Sessions und Keep-Alive

IT vNext
Technologien richtig nutzen!

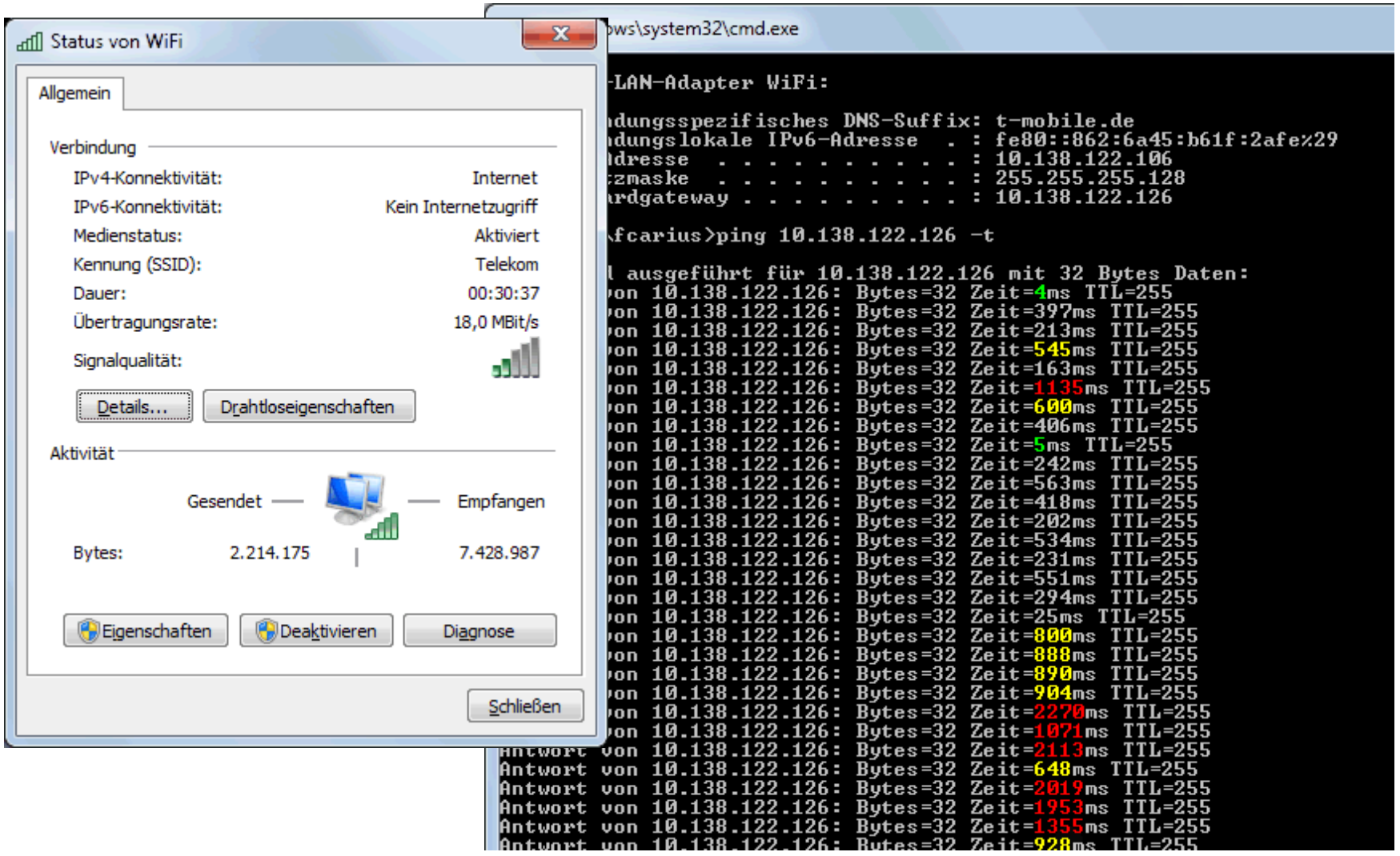
- TCP-Ports sind „kostbar“
  - Aber wann kann ein NAT-Router die Assoziation wieder aufheben ?
- Problem: Nicht alle sagen dem Client Bescheid
  - Client verliert Zeit durch „Retry“
  - Anpassung der „Keep-Alive Timeout für TCP-Verbindungen
- Keep-Alive: 2h Default aber…
  - Default 2h für aktive Verbindungen
  - Fritzbox: 900 Sek(TCP), ca. 7000 Sessions
  - Squid: 120 Sekunden (HTTP)
  - Kemp Loadbalancer: 660Sek (Session)
- Problem „bekannt“ seit ActiveSync

RFC1122 - Requirements for Internet Hosts
https://tools.ietf.org/html/rfc1122
4.2.3.6 TCP Keep-Alives
Keep-alive packets MUST only be sent when no data or acknowledgement packets have been received for the connection within an interval. This interval MUST be configurable and MUST default to no less than two hours.

Network Perimeters & TCP Idle session settings for Outlook on Office 365
http://blogs.technet.com/b/onthewire/archive/2014/03/04/network-perimeter-tcp-idle-session-settings-for-office-365.aspx
2535656 Troubleshooting long running MAPI connections to Exchange Server 2010 through Network Load Balancers

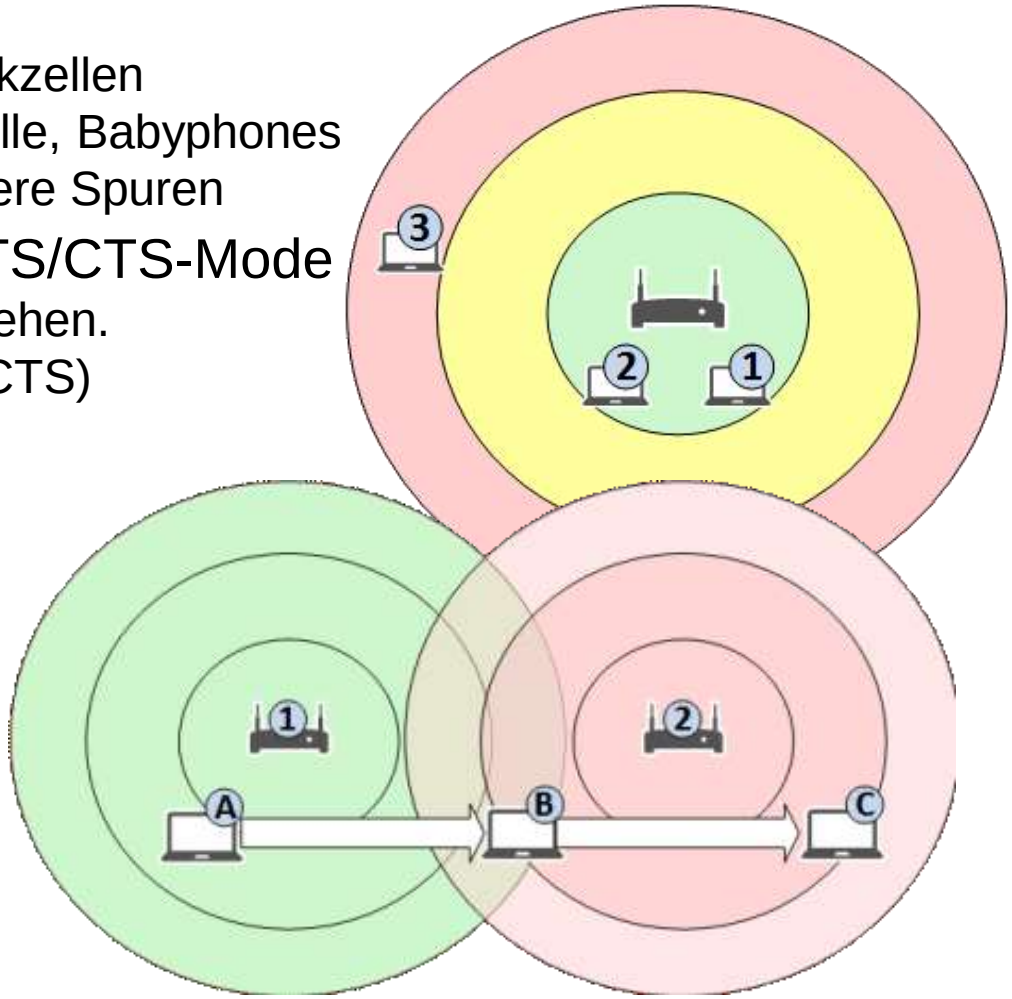
WLAN – ist ein Problem

IT vNext
Technologien richtig nutzen!



Besonderheiten WiFi

- WiFi ist ein „Shared Medium“
  - Andere Teilnehmer, andere Funkzellen
  - 2,4GHz und Bluetooth, Mikrowelle, Babyphones
  - Mehrere Bänder schaffen mehrere Spuren
- Sichtbarkeit CSMA/CA und RTS/CTS-Mode
  - Teilnehmer müssen sich nicht sehen.
  - Access-Point koordiniert (RTS/CTS)
- „Airtime“ und Durchsatz
  - Entfernung = Langsamer
  - Gleiche Paketgröße
  - längere Belegung
- Hand-Over
  - Wann wechselt ein Client?
- Qualitätssicherung
  - WMM PowerSave
  - WMM Admission Control
  - WMM QoS (802.11e)



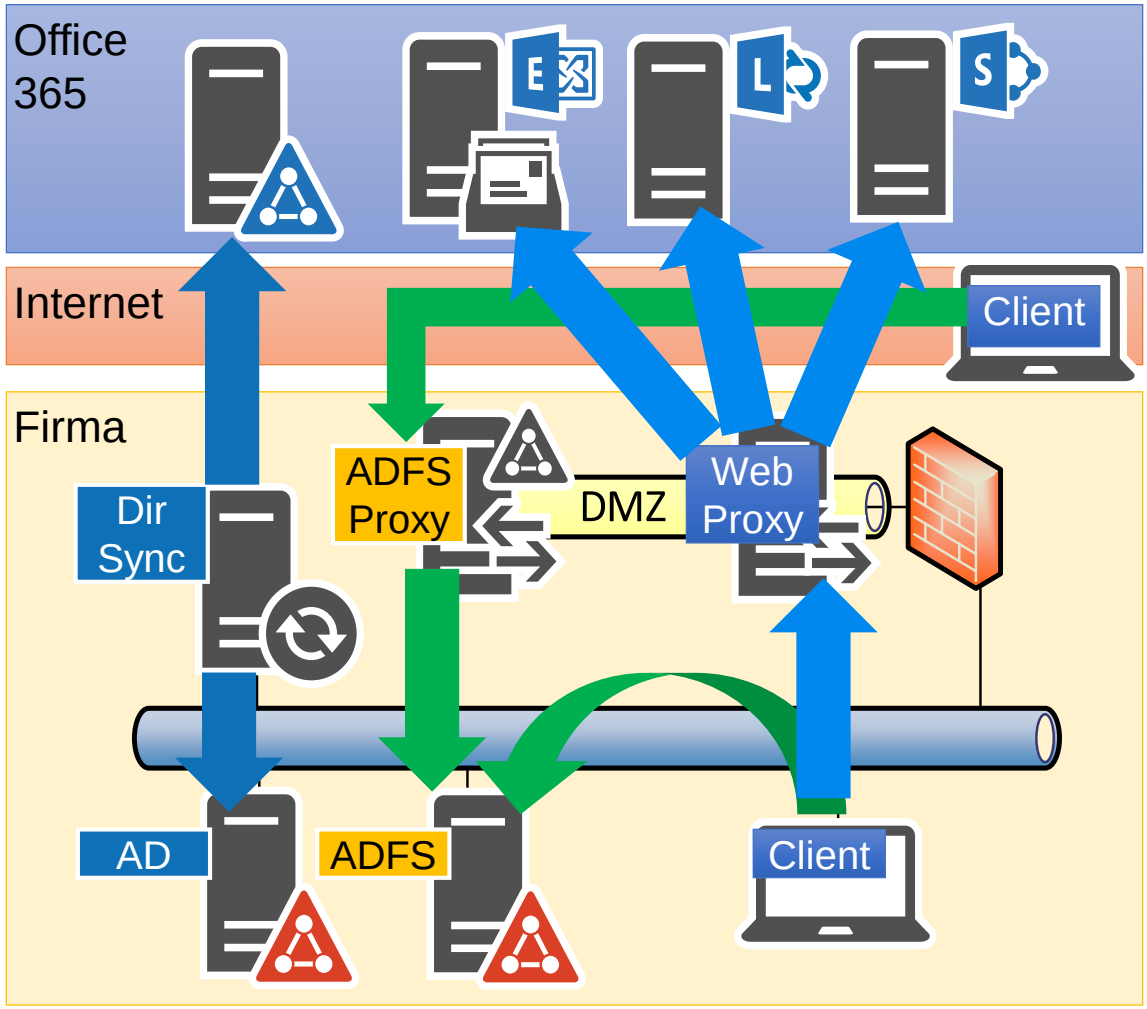
Dienste und ihr Verkehrsverhalten

DirSync, ADFS, Mail, RTC, HTTP, …

Die Office 365 Dienste im Überblick

IT vNext
Technologien richtig nutzen!

- DirSync
  - HTTPS zur Cloud
- ADFS
  - HTTPS vom Client
- Exchange
  - Clientzugriff
  - Mail-Routing
  - Migration
- Skype for Business
  - SIP-Protokoll
  - RTP (A/V)
- SharePoint/OneDrive
  - HTTPS
- Office Software
  - Internet: HTTP
  - Lokal: SMB/HTTP



DirSync

DirSync

Workload

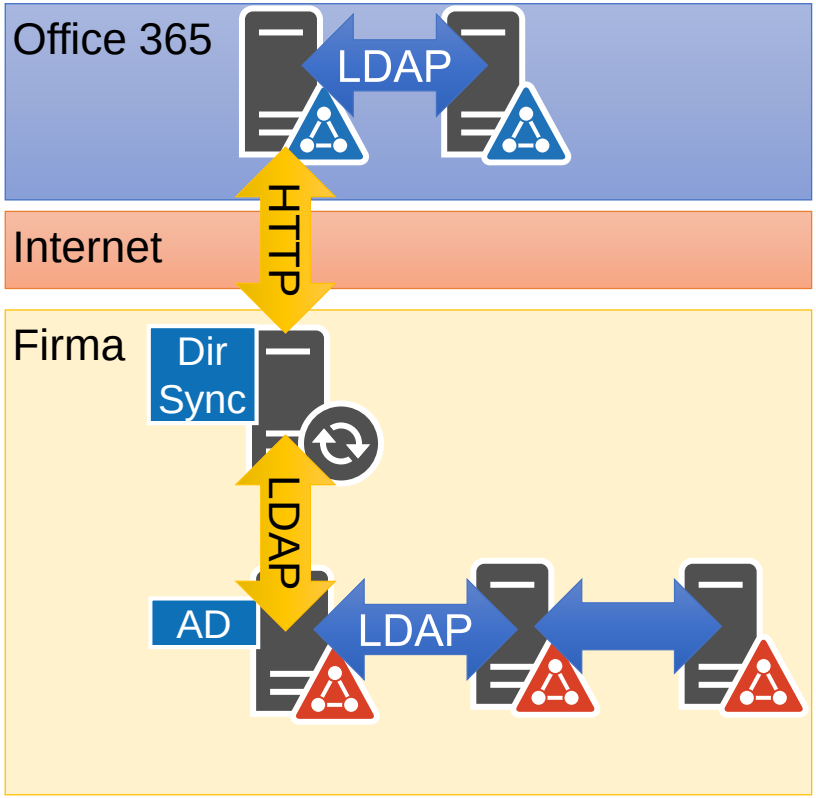
- Repliziert Änderungen zwischen OnPremise-AD und Cloud
- Alle 3 Stunden
  Ausnahme „Password-Sync“
- Delta-Replikation

Protokoll

- HTTPS ausgehend

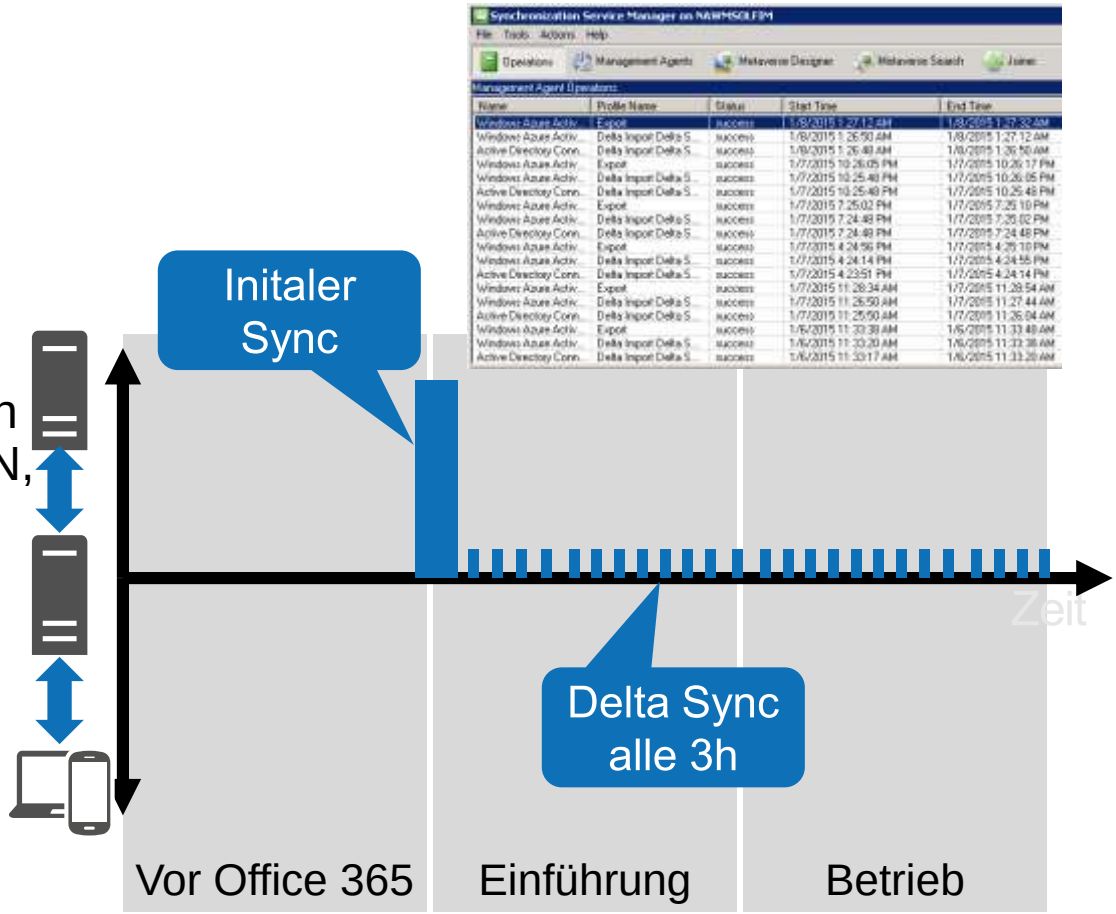
Verfügbarkeit

- Weniger kritisch
- Ausnahme: Kennwort-Sync



DirSync Volumen

- Full Sync/Delta Sync
  - Alle 3 Stunden
- Uni/Bidirektional
- Kennwort Sync
- Achtung
  - Umfangreiche Änderungen z.B. ProxyAddressen, UPN, Firmenname, Straße



Dirsync - Volumen

IT vNext
Technologien richtig nutzen!

Beispielfirma (10.000 User)

- Initial Load: 18 Stunden
- Delta update 2-10 Min
- Datenmenge nicht „auffällig“

Beispielfirma (50 User)

- Initial Load: 5 Minuten
- Delta Update: <1 Min
- Datenmenge nicht messbar

Einschätzung

- Initial Load und Full Sync dauert einfach Zeit -> Geduld
- SQL-Performance lokal beachten
- Bandbreite ist im Vergleich zu den Diensten vernachlässigbar
- Monitoring ist wichtig ! (DirSync, korrupte Objekte, USNChange)

Wenn ein Anwender 1x eine PowerPoint aus der Cloud lädt, sind das viel mehr Daten als die Aktualisierung dieses Benutzers über Jahre.

ADFS

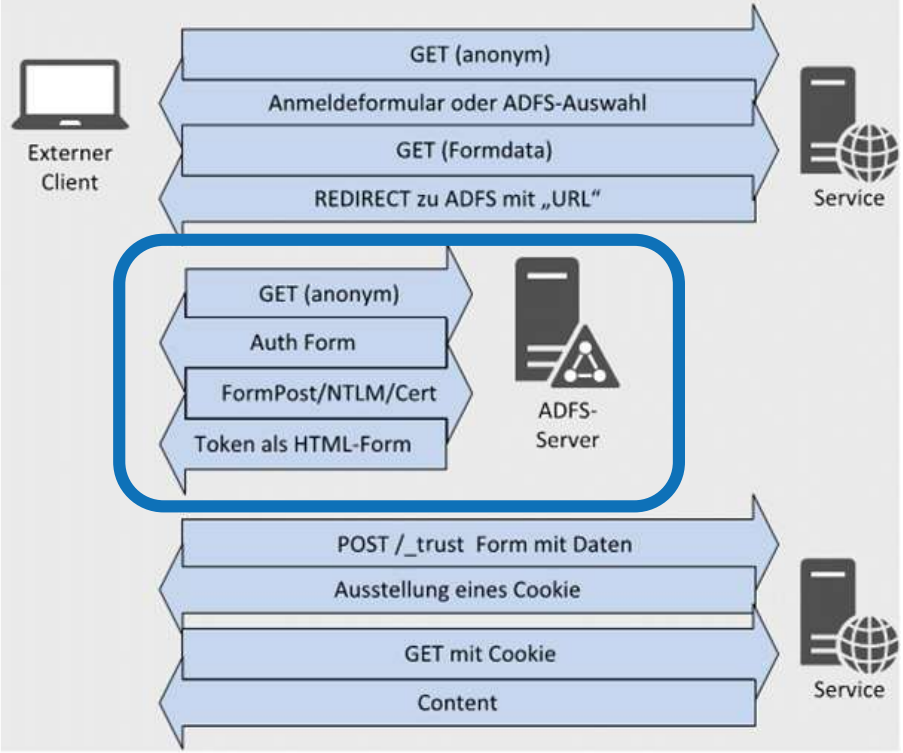
ADFS

Workload

- Stellt Tickets für Anwender aus
- Jede Anmeldung erfordert ein Ticket
- Auch mit OnPremise-Apps nutzbar

Protokoll

- Externe Anwender: HTTPS eingehend über ADFS Proxy
- Interne Anwender HTTPS eingehend auf ADFS-Server
- Verfügbarkeit KRITISCH ! Loadbalancer



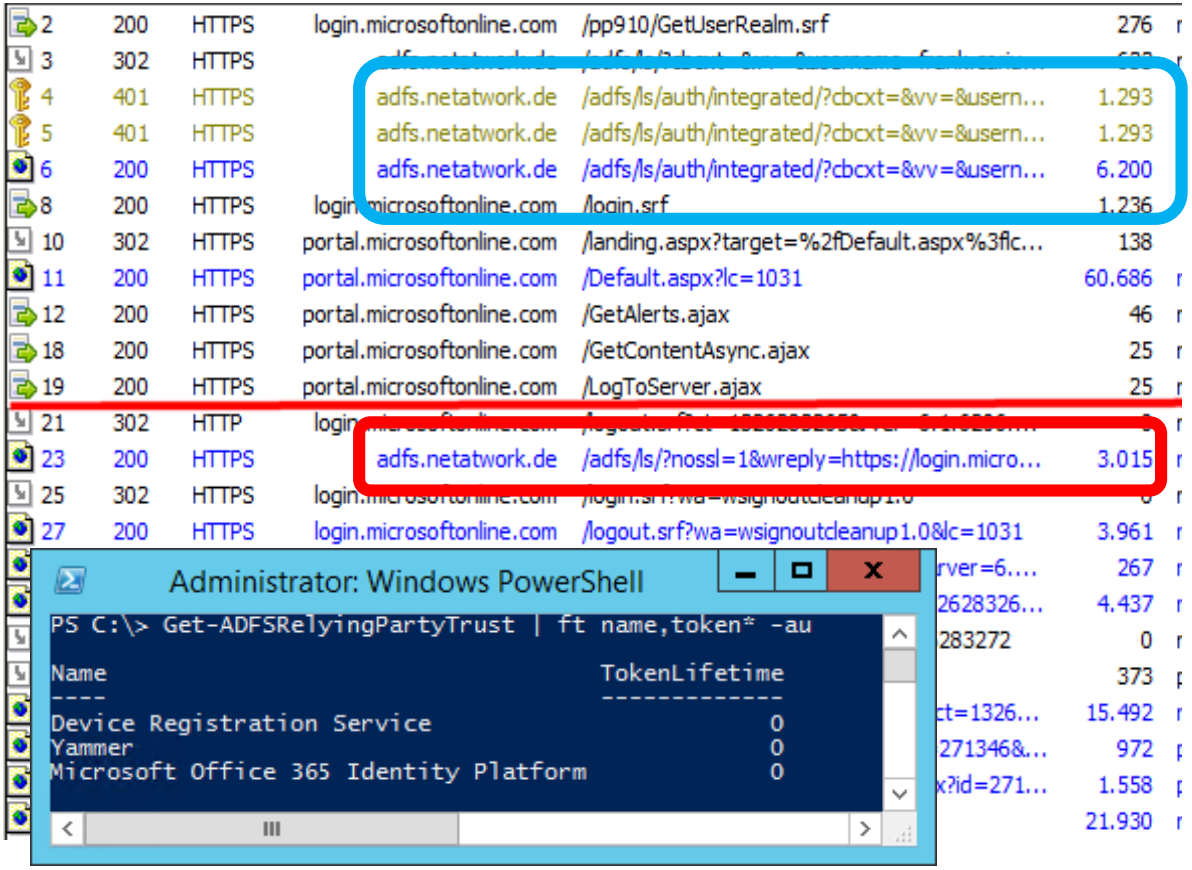
ADFS - Volumen

Erfassen

- IIS-Logs (Server)
- Fiddler (Client)
- NetFlow, Sniffer

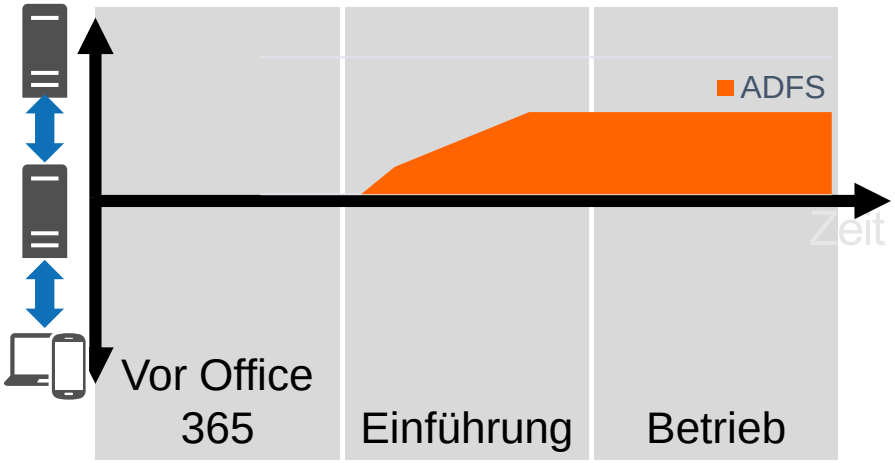
Volumen

- Login: 9kByte
- Logoff: 3kByte
- TokenLifeTime:
  60Min,
  bis 240 Min möglich



ADFS Sizing

- Beispielkunde
  - 50.000 User, 24x7 Betrieb
  - Exchange + Skype for Business
  - 8h Arbeitstag
  - Annahme: 30 Ticketanforderungen/ Tag/User a 10kB
  - Ergebnis:
    500 Mbyte/Tag = 60kbit/Sek
  - Server: 0,3 Server
    (8 Core, 16GB Ram)

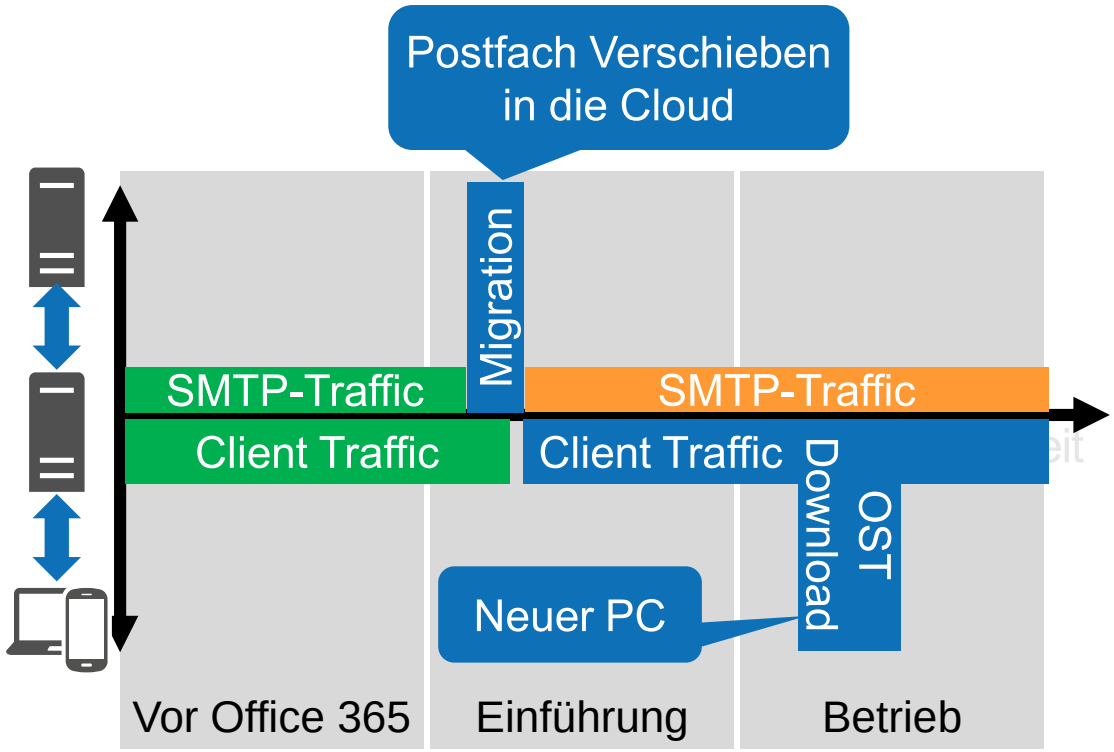


- Einschätzung
  - Verfügbarkeit des Service ist wichtiger
  - Bandbreite ist im Vergleich zu den Diensten vernachlässigbar
- Sizing des ADFS-Servers
  - AD FS 2.0 Capacity Planning Spreadsheet
    http://www.microsoft.com/en-us/download/details.aspx?id=2278

Exchange / Outlook

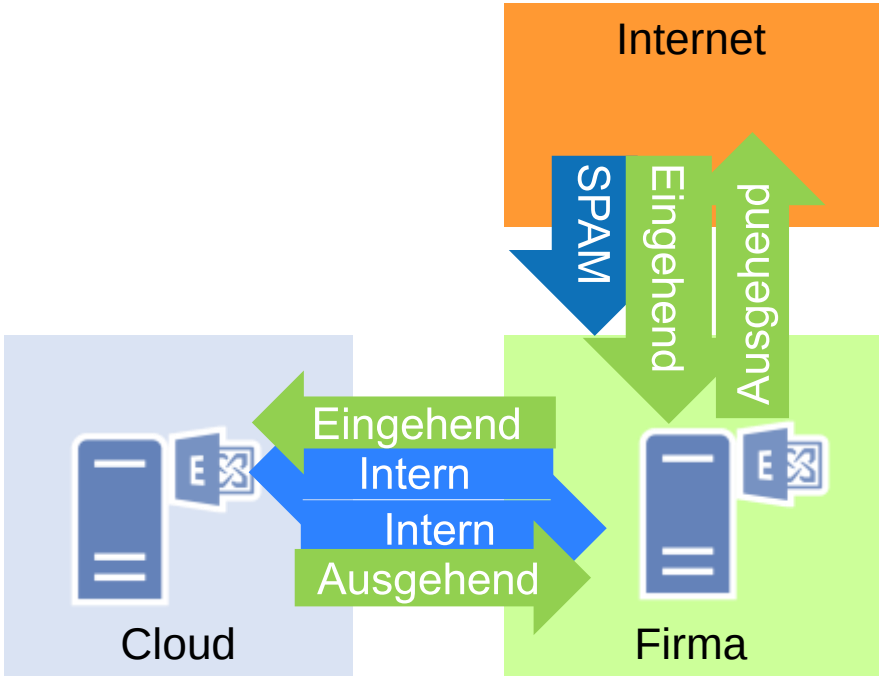
Der Outlook Lebenslauf

- Start
  - Autodiscover
  - OST Replikation
  - OAB Download
- Betrieb
  - Mail In/Out,
  - Termine, Kontakte
  - Aufgaben
  - Stellvertreter
  - Öffentliche Ordner
  - FreeBusy, OOF, UM



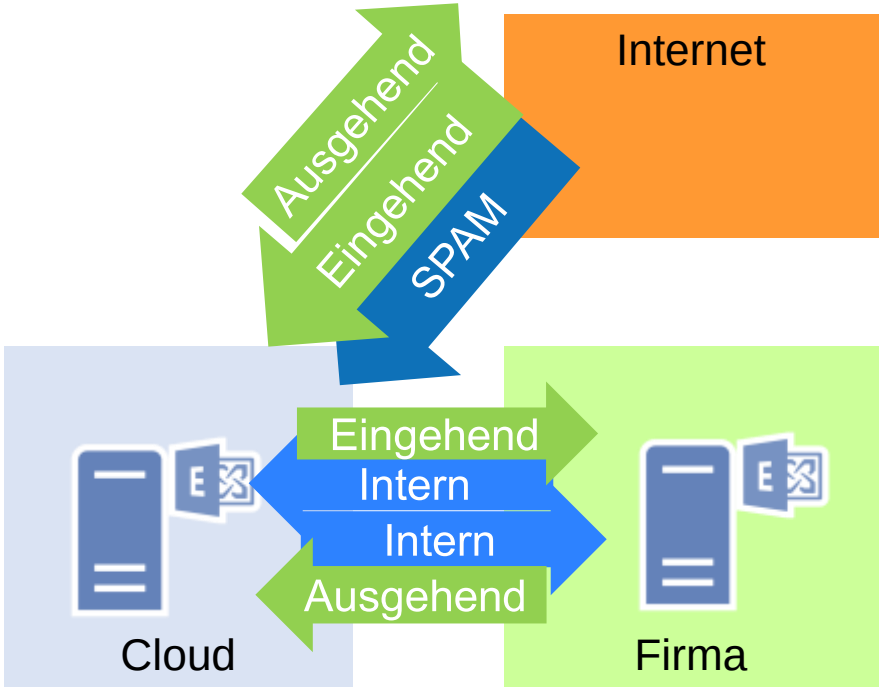
Mailrouting über onPremise

- Einsatz
  - Wenig Postfächer in der Cloud
  - Besondere lokale Gateways
- MX-Record auf Firma
  - Eigene Spamfilter
  - Eigene Verschlüsselungen
  - Eigene Partner-Verbindungen (TLS/VPN)
- Ausgehend
  - Disclaimer, Rewriting
- Netzwerk
  - Spam belastet Internetlink
  - Cloud-Traffic geht zweimal über Internet



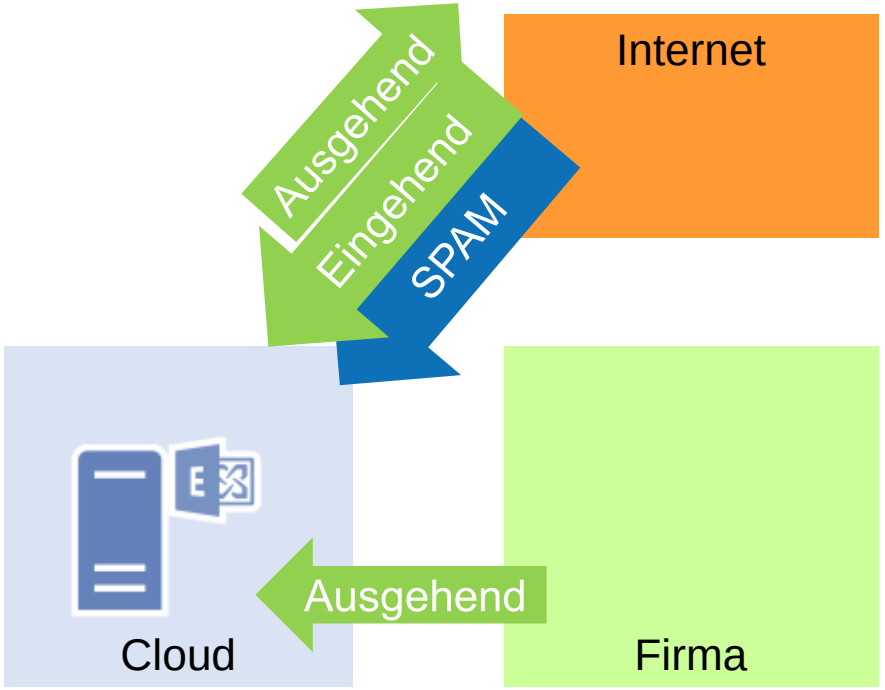
Mailrouting über Office 365

- Einsatz
  - Viele Postfächer in der Cloud
  - Nutzung der Microsoft Spamfilter
- MX-Record auf Office 365
  - Exchange Online Protection
- Ausgehend
  - Disclaimer, Rewriting
- Netzwerk
  - Spam landet bei Office 365
  - Nur erwünschter Mailverkehr auf Internet Links



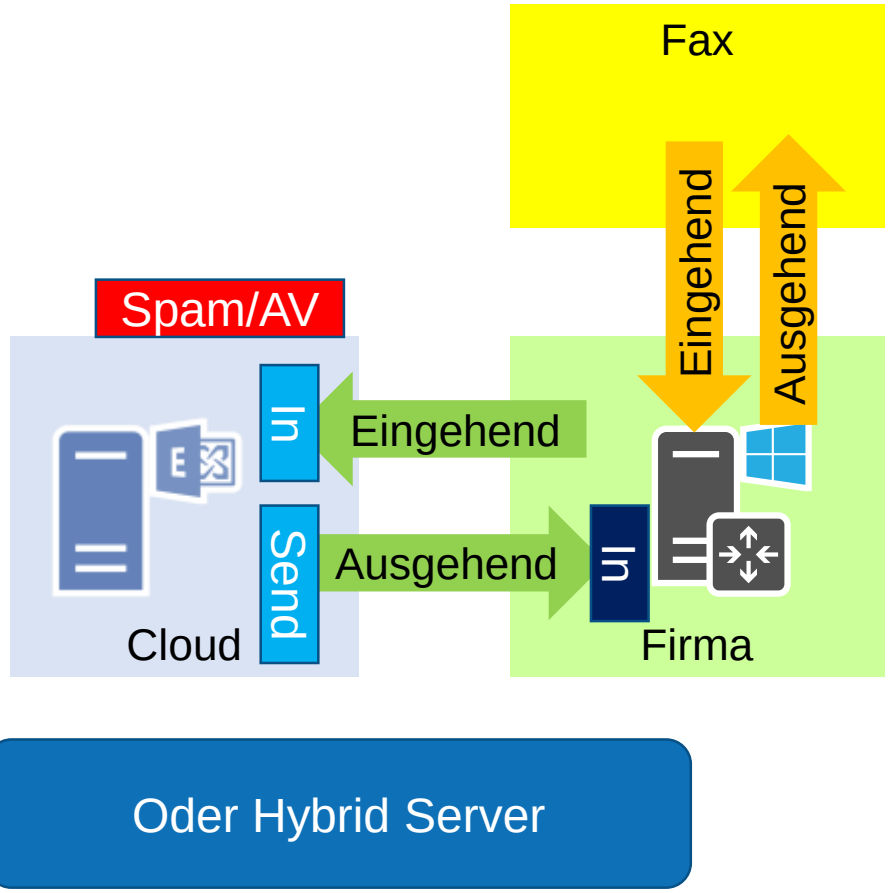
Mailrouting nur Office 365

- Einsatz
  - Alle Postfächer in der Cloud
  - Nutzung der Microsoft Spamfilter
- MX-Record auf Office 365
  - Exchange Online Protection
- Ausgehend
  - Scanner, Faxserver, CRM etc.
- Netzwerk
  - Spam landet bei Office 365
  - Minimaler SMTP-Verkehr
  - Aber natürlich 100% Client Traffic



3rd Party Connector

- Anwendungsfälle
  - Fax, SMS
  - CRM, Kontaktmanagement
- Fax eingehend
  - Connector sendet per SMTP
  - O365 akzeptiert mit Connector
- Fax Ausgehend
  - Outlook sendet an <nummer>@fax.<firma>
  - O365 Routet zum Faxserver
  - Faxserver verifiziert
    - SourceIP TLS, Zertifikat
    - Tenant Header
  - Oder Hybrid Server
- Postfachzugriff
  - EWS
- Bandbreite
  - Heute messen und schätzen



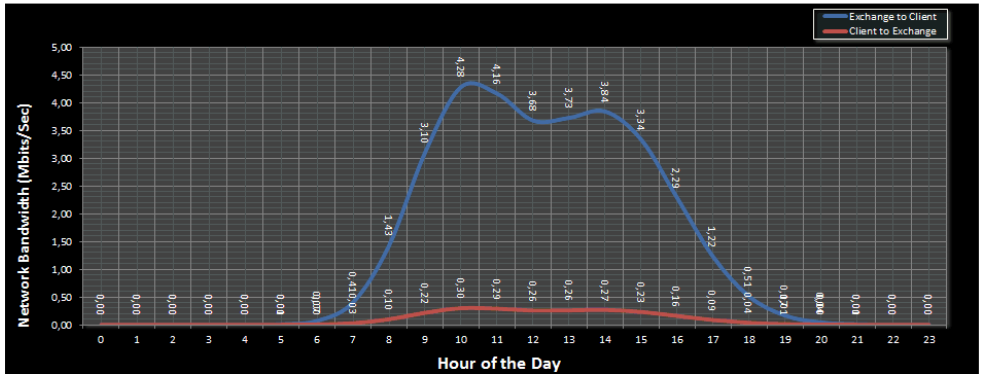
Exchange Bandbreiten Kalkulator

IT vNext
Technologien richtig nutzen!

- Outlook Werte
  - 50*50kB = 2,5MB Change/Tag
  - ca. 1,5-faches Volumen
- Excel Sizer
  - Ähnlich wie Exchange Sizer
  - UserProfiles definieren
- Limits
  - Kein Mailrouting
  - Keine Migration
  - Client immer direkt zur Cloud

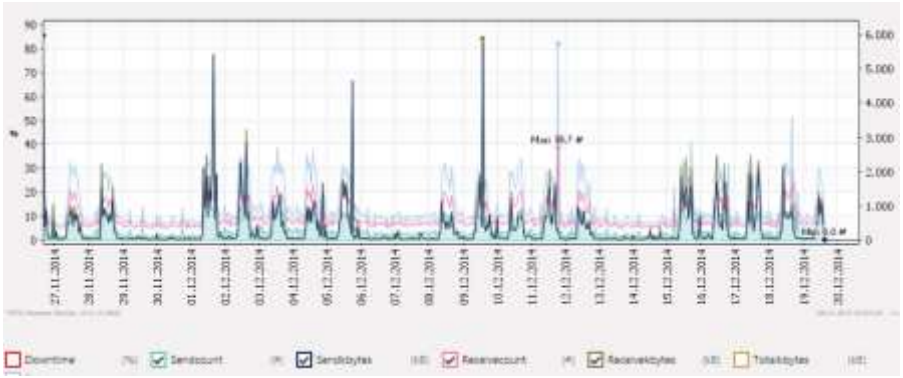
User Profile 2 (Medium) [Sent: 10 Recv: 40 AvgMsg: 50 KB]			
Client	**kB/Day**	**kB/s (Peak)**	**kbps (Peak)**
Outlook 2010 (OA-Cached)	3674,9	0,27	2,17
Outlook 2010 (MAPI-Cached)	3573,3	0,26	2,11

Site Definition				Outlook 2011 MAC (EWS)	Outlook 2010 OA Cached	Outlook 2007 OA Cached	Outlook 2007 MAPI	OWA OWA 2010	Mobile WP7	Network Predictions Total	Network Bandwidth (Exchange to Client)	Network Bandwidth (Client to Exchange)	Recommended Maximum Network Latency	TCP Connections (Aproximation)
Site	Site User Profile	TimeZone	Concurrency											
Zentrale Paderborn	Light	GMT	100%	5	500	500		100	300	1405	2,32 Mbits/sec	0,26 Mbits/sec	320 ms	7686
Niederlassung Berlin	Light	GMT	100%	1	30				10	41	0,62 Mbits/sec	0,01 Mbits/sec	320 ms	229
Niederlassung München	Light	GMT	100%	2	40				25	67	0,64 Mbits/sec	0,01 Mbits/sec	320 ms	320
Niederlassung USA	Light	GMT	100%	1	80				45	126	0,71 Mbits/sec	0,02 Mbits/sec	320 ms	631
				9	650	500	0	100	380	1639	4.28 Mbits/sec	0.30 Mbits/sec	320 ms	8867



Eigene Analyse

- Messagetracking
  - Anzahl der Mails/User
  - Größe der Mail
  - Ziel: (SameSite, SameOrg, Internet)
- Netzwerk (NetFlow u.a.)
  - Client Verbindungen
  - Datenvolumen
  - Firewall Logs
- RCA-Logging (Ex2010)
  - Liefert Outlook Version, User, Client-IP (Netzwerk)
- IISLog, Reverse Proxy
  - Liefert Datenvolumen (OWA, EAS und RPC/HTTP) (Logparser)
  - Tipp: Vorher auf Outlook Anywhere umsteigen.
- PowerShell und PowerBI sind genial
  - Daten per Powershell in CSV-Dateien und mit PowerBI auswerten

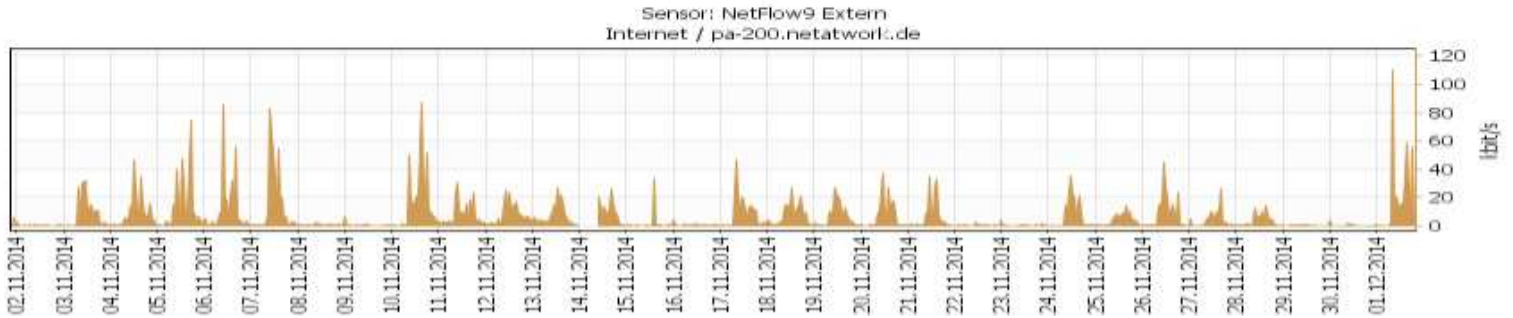


Eigene Analyse

- Net at Work
  - MAPI-Client: 3kbit/User/Sek
  - SMTP-Routing: 2GB/30 Tagen = 6kBit/s
- Kunde (50.000)
  - MAPI-Client: 6kbit/User/Sek !
  - 50.000 User * 6kbit = 292 Mbit Dauerlast !
  - Noch keine Migration oder Mailflow
  - Office 365 nicht möglich mit zentraler Firewall
    -> Diskussion über Netzwerkdesignchange: dezentrale Internet Breakouts

Report for NetFlow9 Extern

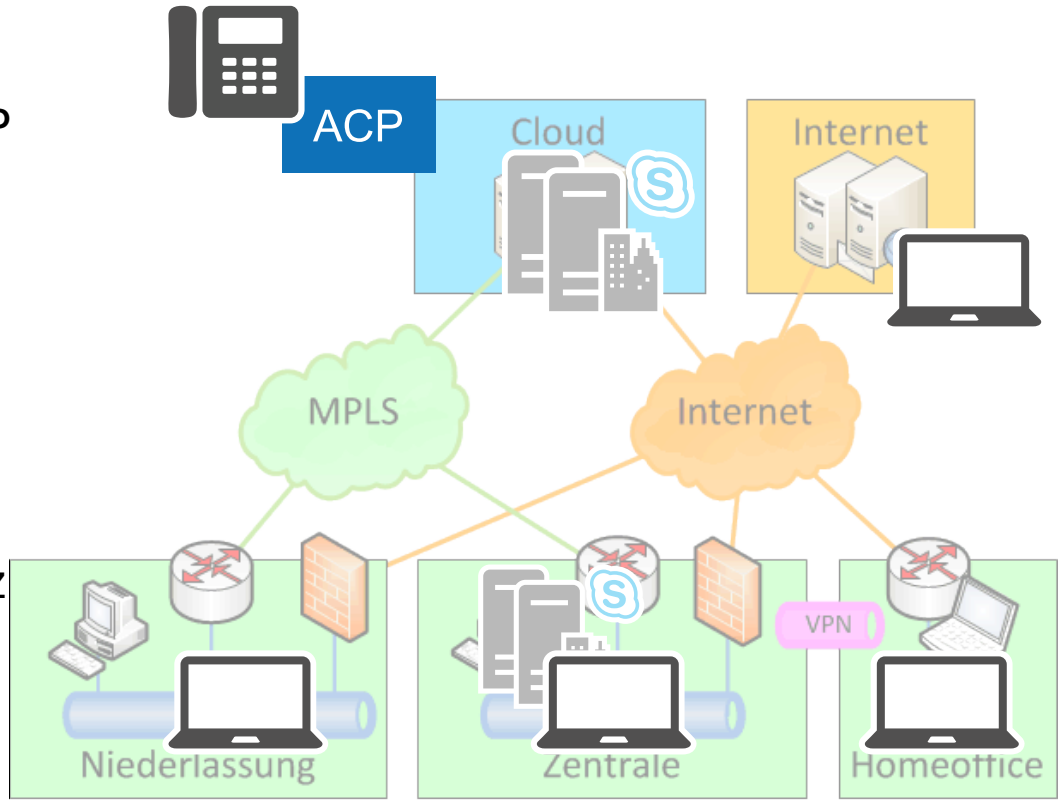
Report Time Span:	01.11.2014 20:34:00 - 01.12.2014 20:34:00					
Sensor Type:	NetFlow V9 (60 s Interval)					
Probe, Group, Device:	Probe NAWPRTG > Internet > pa-200.netatwork.de					
Uptime Stats:	Up:	100 %	[29d12h35m0s]	Down:	0 %	[0s]
Request Stats:	Good:	100 %	[42520]	Failed:	0 %	[0]
Average (Total):	788 kbit/s					
Total (Total):	245.071.780 KByte					



Skype for Business

Skype for Business in der Cloud

- IM/Presence?
  - Client meldet sich per SIP/HTTPS an
  - Client lädt „Kontakte“ per SIP
  - Client lädt Adressbuch per HTTPS
- P2P Audio/Video (1:1)
  - Zwei Clients kommunizieren direkt miteinander
- Konferenz
  - 3+ Clients in einer Konferenz
  - Telefoneinwahl über ACP
- Telefonie
  - Benutzer müssen auf OnPremise Server sein



Skype for Business Protokolle

- Signalisierung (SIP/TCP bzw. SIP/HTTPS)
  - Client verbindet sich mit seinem „Homeserver“
  - Intern per 5061/TLS direkt zum Server
  - Extern per 443/HTTPS über den Edge Server
  - Präsenzstatus, Buddy-Liste und Gesprächssteuerung (INVITE), Textmessages
  - Vergleichbar mit D-Kanal im ISDN oder FTP-Control-Kanal (21/TCP)
- Webservices (HTTPS)
  - Abruf zusätzlicher Informationen
    Adressbuch, Gruppen, Zertifikate, Responsegroup-Steuerung, Meeting-URL, Lyncdiscover,…
  - Intern: direkt gegen den Lync Server bzw. Loadbalancer
  - Extern: über einen Reverse Proxy zum Pool
- Office Web App Server (HTTPS)
  - PowerPoint Präsentation in Meetings
- RTP (UDP/TCP)
  - Audio, Video, Desktop-Sharing, Dateitransfer

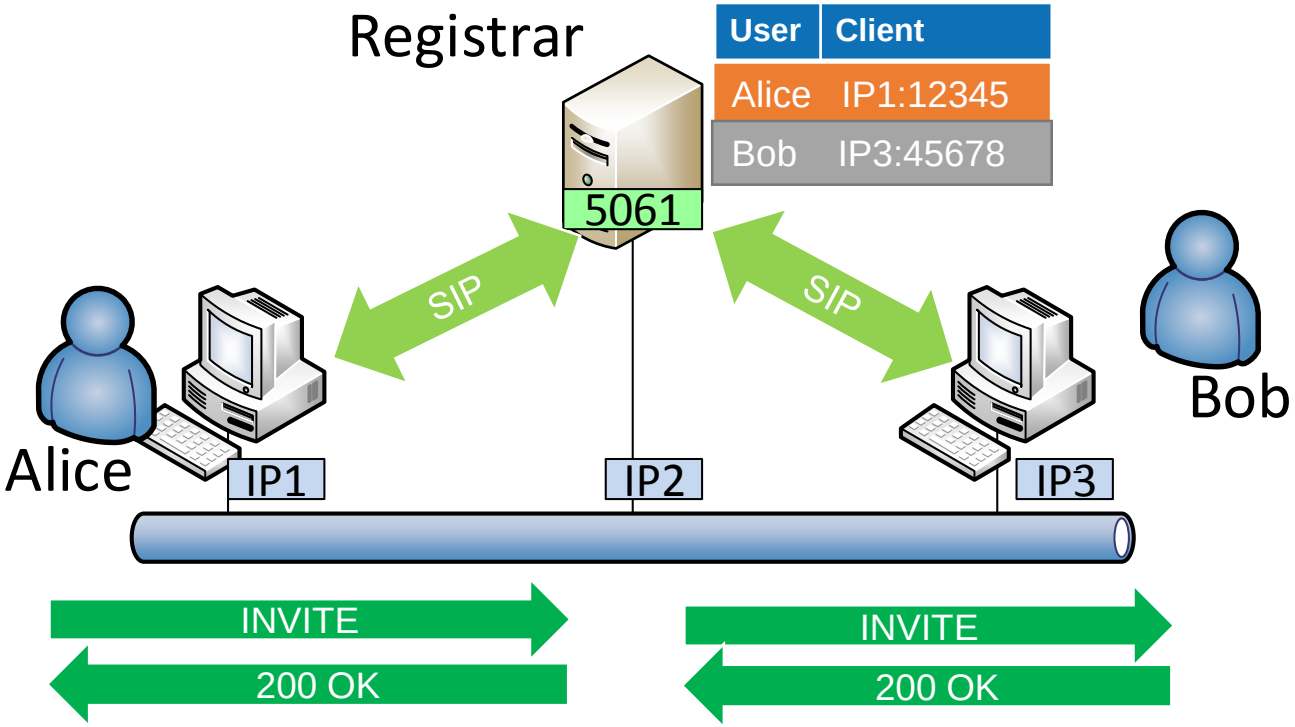
Skype for Business Datenvolumen

Protokoll	kBit/User/Sek	Max Latenz	Bemerkung
SIP	4-8 kbit	Sekunden	Signalisierung
WebService	1-2kbit	Sekunden	
Office Web App	Variabel	Sekunden	PowerPoint Präsentationen
RTP:Audio	40-200	200ms	Je nach Codec
RTP:Video	200-4000	500ms	Je nach Codec und Auflösung
RTP:Desktop Sharing	Variabel	<1 Sek.	Vergleichbar zu RDP

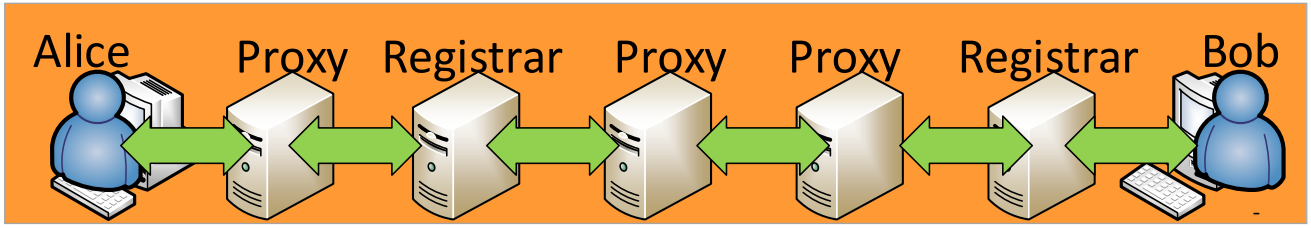
Kritische Komponente ist eindeutig Audio/Video

Network bandwidth requirements for media traffic in Lync Server 2013
http://technet.microsoft.com/en-us/library/jj688118.aspx

Skype for Business : SIP



Skype for Business – mit mehreren Stationen

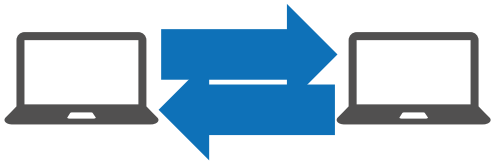



```
INFO   :: Data Received -80.66.20.22:443 (To Local Address: 192.168.10.127:1255) 3807 byt
INFO   :: SIP/2.0 200 OK
ms-user-logon-data: RemoteUser
From: "Carius, Frank"<sip:frank.carius@netatwork.de>;tag=2de808a726;epid=2385f4c267
To: <sip:xxxxxx.xxxxxxe@bertelsmann.de>;tag=2D670080
CSeq: 1 SUBSCRIBE
Via: SIP/2.0/TLS 192.168.10.127:1255;received=84.128.60.79;ms-received-port=1255;ms-rece
Record-Route: <sip:gtlbmllyd0100.bagmail.net:5061;transport=tls;ms-fe=GTLBMLLYD0102.bagm
Record-Route: <sip:csac.bertelsmann.de:5061;transport=tls;lr;ms-key-info=xxxxx>
Record-Route: <sip:nawlyncedge.netatwork.de:5061;transport=tls;lr>
Record-Route: <sip:NAWLYNC001.netatwork.de:5061;transport=tls;opaque=state:F;lr;received
Record-Route: <sip:sip.netatwork.de:443;transport=tls;opaque=state:Ci.R6440f00;lr;ms-rou
ms-edge-proxy-message-trust: ms-source-type=AutoFederation;ms-ep-fqdn=nawlyncedge.netatw
```

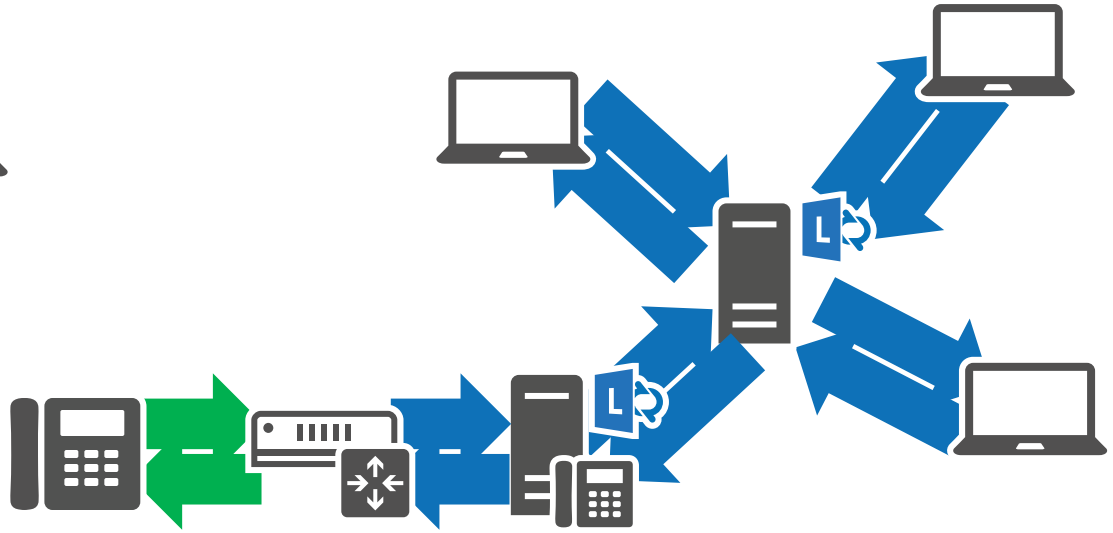
SIP ist SMTP auf Drogen

RTP – Audio, Video und mehr

- RTP sucht den kürzesten Weg
- 1:1 zwischen den Endgeräten
- 1:n Endgerät zur Konferenzeinheit (MCU)

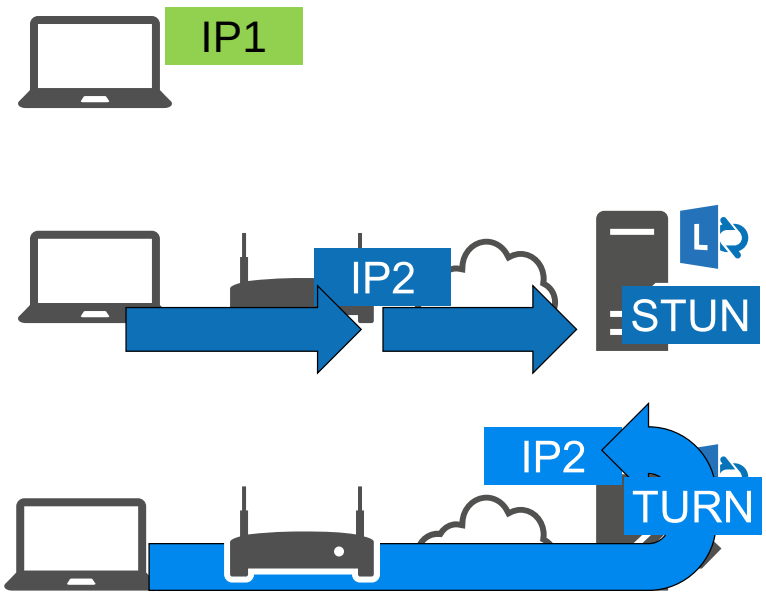


Und wenn NAT oder Firewall eine direkte Verbindung verhindert ?



ICE im Schnelldurchlauf

- Direkt
  - Der Client öffnet auf allen lokalen IP-Adressen Ports zum Empfang
- STUN
  - Session Traversal using NAT
  - Der Client sendet ein Paket an den STUN-Server, der im die IP meldet
  - Pakete an diese IP:Port werden oftmals zum Client geroutet
- TURN (3478/UDP)
  - Der Client baut eine Verbindung zum TURN-Server auf, der im IP-Kandidaten leiht und eingehende Pakete als Relay zum Client sendet



Kandidaten im SDP

IT vNext
Technologien richtig nutzen!

```
a=ice-ufrag:ZMqo
a=ice-pwd:wP8epG6CgHGSrnIPlrHsVr6T
a=candidate:1 1 UDP 2130706431 192.168.102.31 10996 typ host
a=candidate:1 2 UDP 2130705918 192.168.102.31 10997 typ host
a=candidate:2 1 UDP 2130705919 192.168.56.1 22320 typ host
a=candidate:2 2 UDP 2130705406 192.168.56.1 22321 typ host
a=candidate:3 1 UDP 2130705407 192.168.182.1 7622 typ host
a=candidate:3 2 UDP 2130704894 192.168.182.1 7623 typ host
a=candidate:4 1 UDP 2130704895 192.168.23.1 31878 typ host
a=candidate:4 2 UDP 2130704382 192.168.23.1 31879 typ host
a=candidate:5 1 UDP 2130704383 192.168.88.120 29860 typ host
a=candidate:5 2 UDP 2130703870 192.168.88.120 29861 typ host
a=x-candidate-ipv6:6 1 UDP 33551871 2001:0:5ef5:79fb:3876:1945:3f57:99e0 27984 typ host
a=x-candidate-ipv6:6 2 UDP 33551358 2001:0:5ef5:79fb:3876:1945:3f57:99e0 27985 typ host
a=candidate:7 1 TCP-PASS 174453759 80.66.20.21 55789 typ relay raddr 192.168.102.31 rport 13717
a=candidate:7 2 TCP-PASS 174453246 80.66.20.21 55789 typ relay raddr 192.168.102.31 rport 13717
a=candidate:8 1 UDP 184545791 80.66.20.21 59646 typ relay raddr 192.168.102.31 rport 32126
a=candidate:8 2 UDP 184545278 80.66.20.21 51707 typ relay raddr 192.168.102.31 rport 32127
a=candidate:9 1 TCP-ACT 174845951 80.66.20.21 55789 typ relay raddr 192.168.102.31 rport 13717
a=candidate:9 2 TCP-ACT 174845438 80.66.20.21 55789 typ relay raddr 192.168.102.31 rport 13717
a=candidate:10 1 TCP-ACT 1684794879 192.168.102.31 13717 typ srflx raddr 192.168.102.31 rport 13717
a=candidate:10 2 TCP-ACT 1684794366 192.168.102.31 13717 typ srflx raddr 192.168.102.31 rport 13717
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80 inline:JM5R8bFurPPE0BY3hQOx/LB9tJ8BMWyGkrcfpuHs|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:vL9TEWKTPzz/JEGGZY0AzwQvWtSXr8VGpfR20403|2^31|
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:j3bYAZDTVE+YLRB+fOFLxb+HJNzkKnUUwkOyR4HK|2^31
a=maxptime:200
```

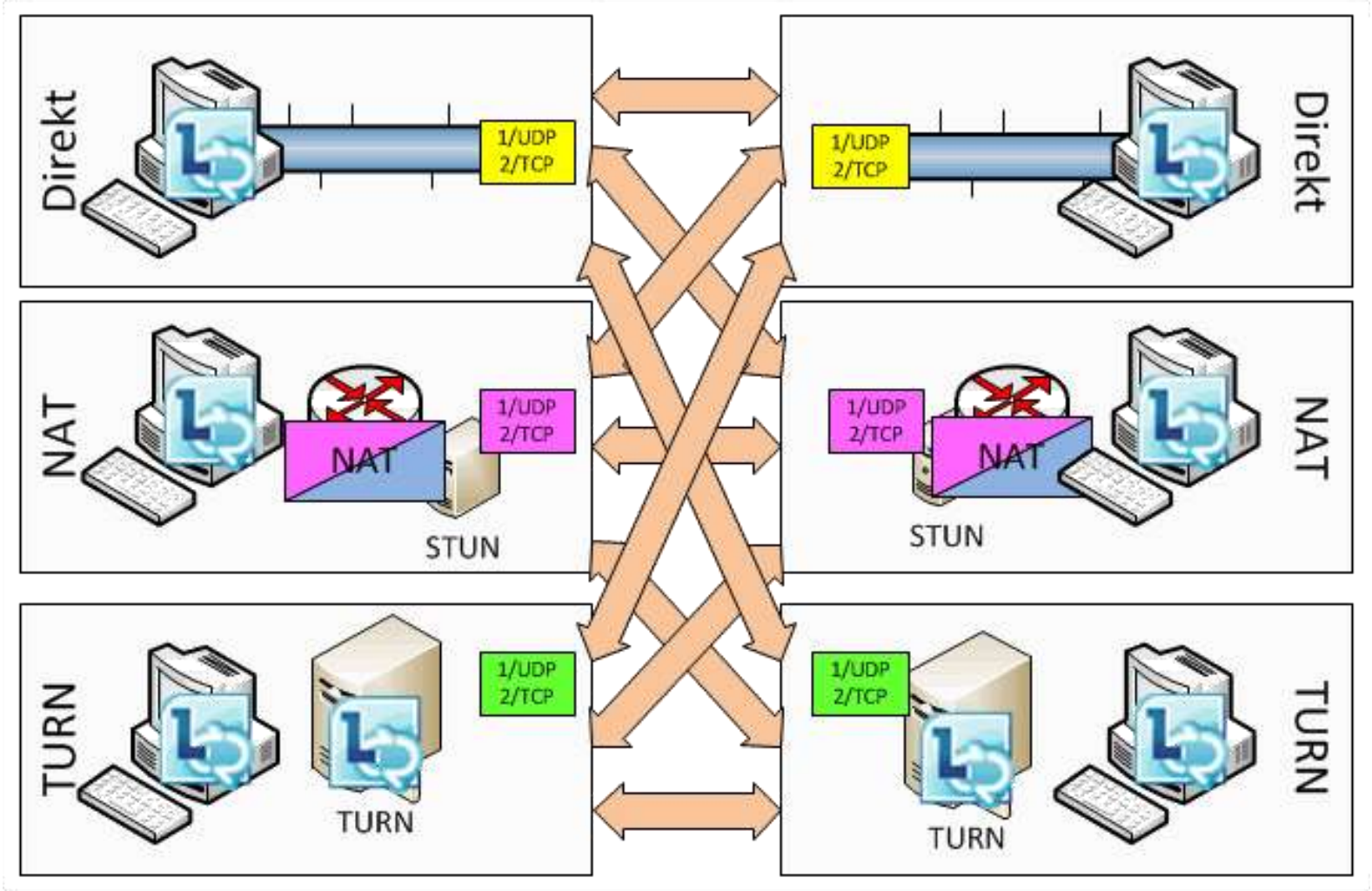
Direkte Kandidaten

TURN

NAT

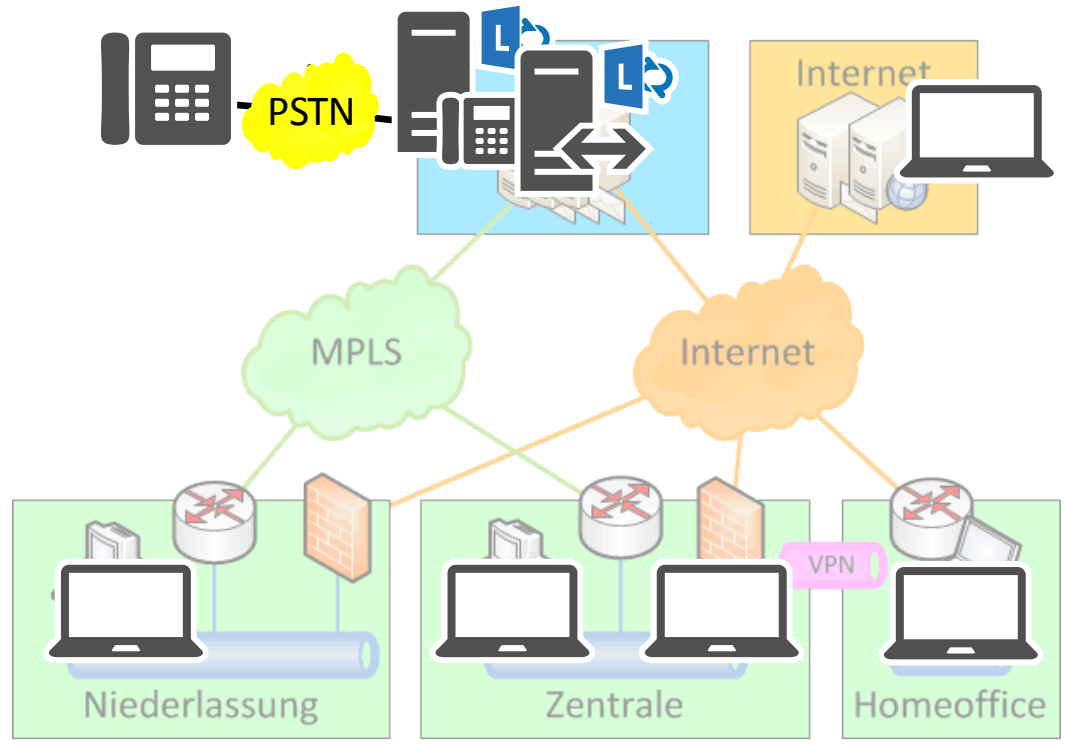
SRTP-Keys

ICE – Speed-Dating



ICE Quiz

- Zentrale <-> Zentrale
- Zentrale <-> Niederlassung
- Zentrale <-> Homeoffice
- 3er Konferenz
- Homeoffice <-> Internet
- Zentrale <-> Telefon

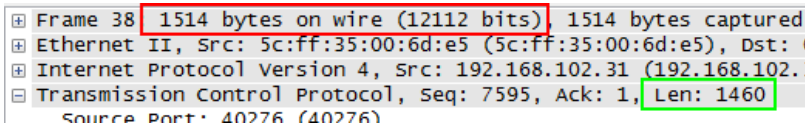


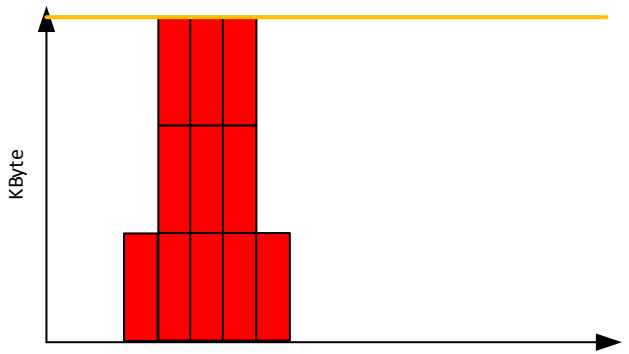
Netzwerkmathematik

Bandbreite, Latenzzeit, Jitter, Packetloss,
SNMP, NetFlow, QoS

Netzwerkmathematik - Daten

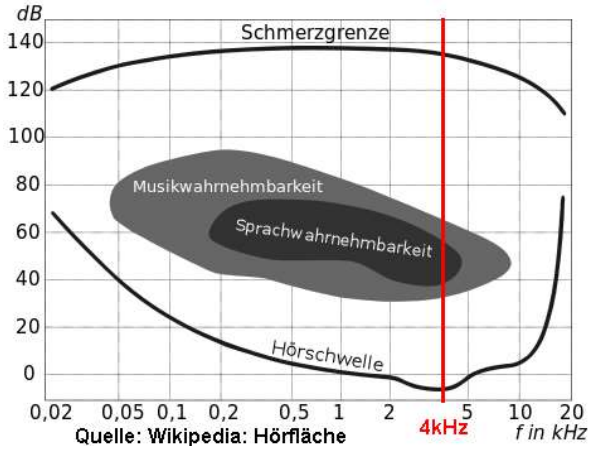
- Ethernet
  - Paketgröße bis zu 1514 Byte
  - CSMA/CD – heute irrelevant
- Beispiel 100 Mbit
  - Bis zu 100.000 Bytes/Sek
  - 65963 Pakete/Sek (a 1514 Byte) (idealisiert)
- Beispiel PowerPoint (10 Mbyte)
  - 100MBit über 100MBit-Link ► 1 Sek Dauer
  - Bei 1.500 Byte/Paket ► 6.666 Pakete/s
- Gigabit ?
  - Hat noch nicht jeder am Desktop
  - Ultraboot/Tablets mit WiFi oder USB-Netzwerk
  - WAN-Strecken
  - Switch Trunks und Uplinks





Netzwerkmathematik - Codec

- VoIP = Sprache
  - Der Mensch hört nicht alles !
    bis ca. 4kHz
  - 8kHz „Abtastung“ erforderlich, z.B. mit 8bit Mono
  - 64KBit = ISDN. (G.711 Codec)
- Analog zu Digitalwandung
  - 1 Sek Sprache mit 64kbit Abtastung
    ► 8 Kilobyte/Sek
  - 1500 Byte/Paket
    ► 6 Pakete mit ca. 160ms/Paket
  - 160ms Verzögerung !!
- Abtastung für VoIP
  - 20ms Abschnitte
    ► 50 Frames/Sek
  - 160 Byte Nutzdaten/Paket
- Andere Codecs
  - Wideband : 16.000 Samples
  - Stereo für Konferenzen
  - Kompression

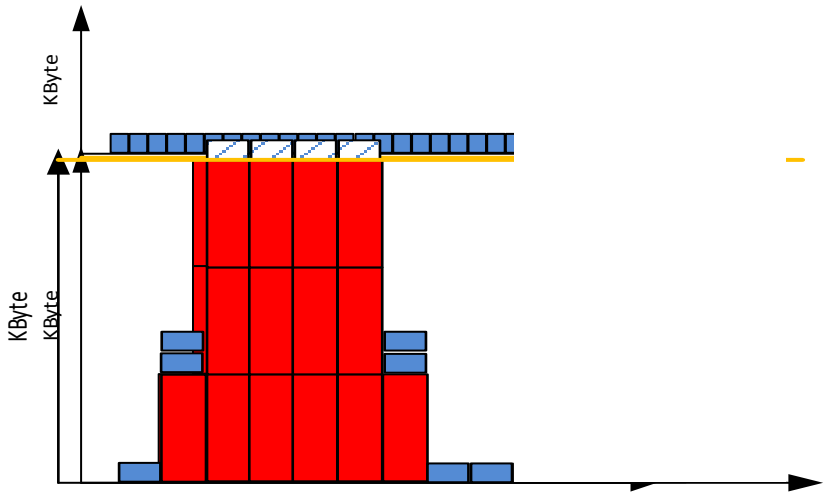


Quelle: Wikipedia: Hörfläche

Die Berechnung ist stark vereinfacht nur
zu Demonstrationszwecken gedacht

Auf dem Kabel – David gegen Goliath

- Große „Peak-Pakete“
  - PPT, Softwareverteilung
- Kleine VoIP-Pakete
  - Dauerläufer
  - Zeitkritisch
- LAN/WAN
  - Bandbreite ist beschränkt
- QoS
  - priorisiert “ den Verkehr
  - verwirft Pakete
  - QoS im Internet (Netflix ?)
- VoIP-Software
  - Wechselt Codec
  - Unterbindet Verbindungen (z.B. CAC)

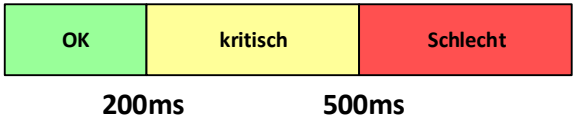


Die wichtige Faktoren

IT vNext
Technologien richtig nutzen!

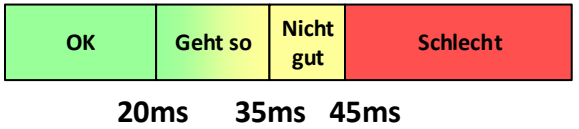
Laufzeit/Roundtrip

- Wie lange sind die Daten „unterwegs“ ?
- Wie schnell ist der Transporter unterwegs ?
- „Network Round Tipp Time (NTT)



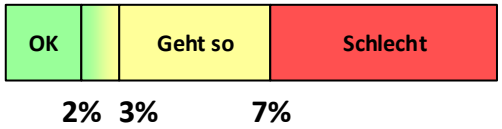
Jitter

- Wie gleichmäßig ist der Transport
- Empfänger muss puffern.
- Einfluss auf Laufzeit



Paket Loss

- Wenige Prozent verlorene Pakete sind tolerierbar
- Ein Paket enthält 20ms „Ton“
- Burst-Loss-Problem.



Bandbreite

- Genug um die anderen drei Werte „grün“ zu halten
- Audio braucht ca. 40-160kBit (je nach Codec)
- Video braucht ca. 150kBit-2MBit (HD) (pro Stream)

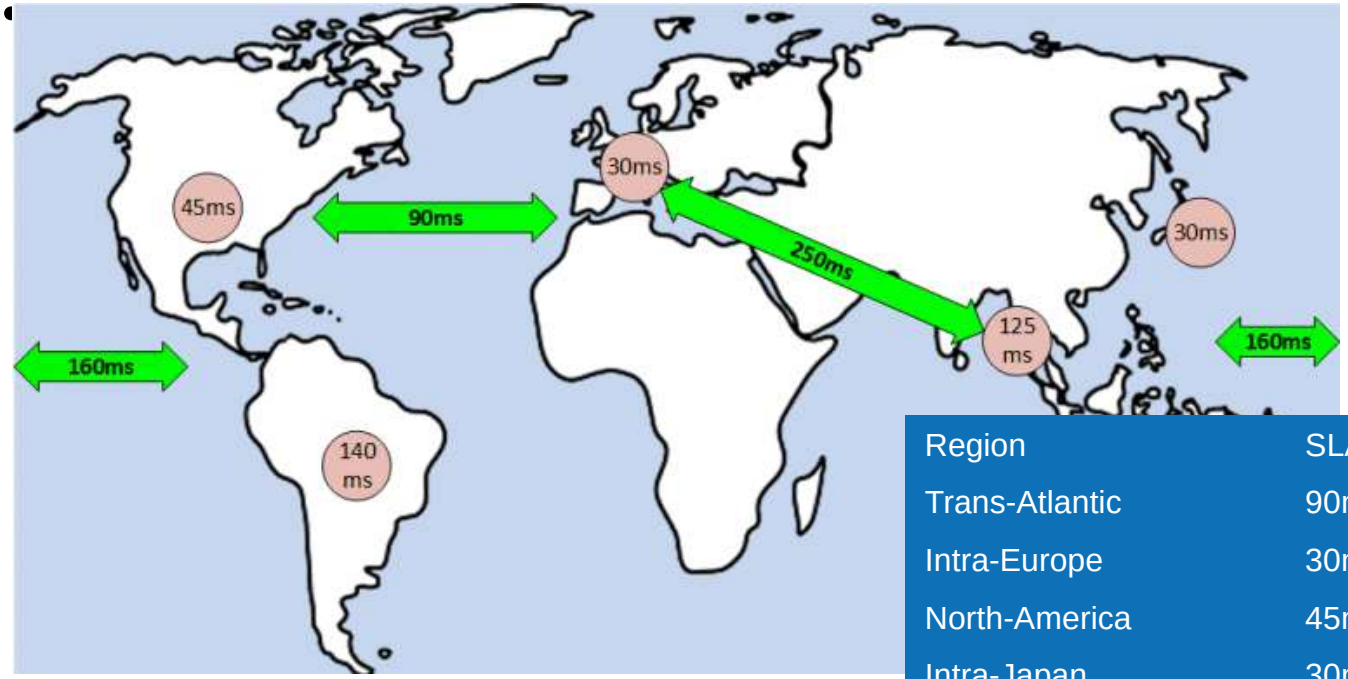
Alle Werte hängen voneinander ab.

Bandbreite

- Bandbreite und Geschwindigkeit
  - Der Weg ist selten mehrspurig
  - Es gibt nur eine Gleis pro Richtung
  - Bit/Sek steht für die Reisegeschwindigkeit
  - Überholverbot auf der Strecke
- HyperV-Netzwerke
  - virtuelle Switches
  - Virtuelle Netzwerke
  - QoS in virtuellen Welten
  - 10 Gigabit und NPAR
- VLAN
  - Getrennte logische Netze
  - Gemeinsame Bandbreite
- VPN
  - Overhead (UDP in HTTPS)

Latenz

- Nichts ist schneller als das Licht – Entfernung ist das Problem
- Store and Forward kostet Zeit – Hop count ist das Problem



Region	SLA	Min/Max
Trans-Atlantic	90ms	70-75
Intra-Europe	30ms	10-12
North-America	45ms	34-36
Intra-Japan	30ms	8-10
Trans-Pacific	160ms	109-111
Intra-APAC	125ms	94-112
Latin-America	140ms	134-142
EMEA-to-APAC	250ms	117-167

http://www.verizonenterprise.com/about/network/latency/

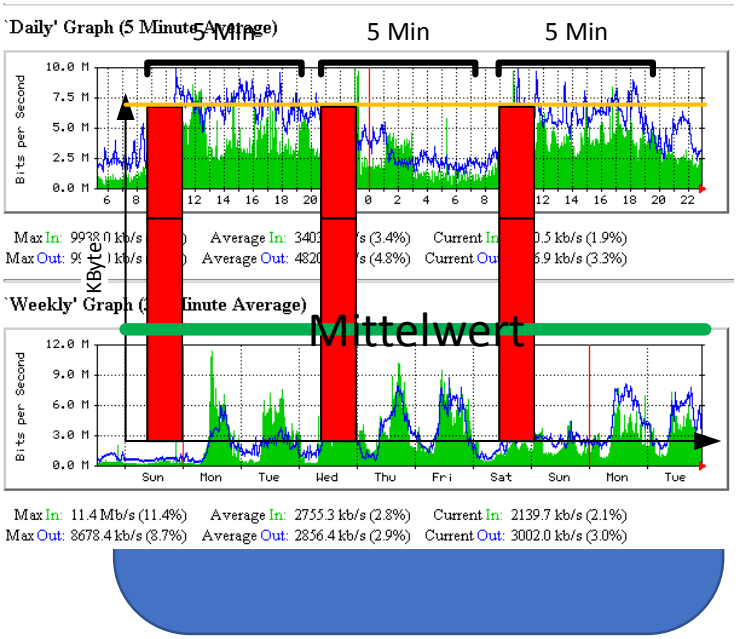
Anforderungen

IT vNext
Technologien richtig nutzen!

Datenprofil	Bandbreite	Latenzzeit	Jitter	Paket Loss
Große Daten • Betriebssysteminstallation • Softwareinstallation • Software Updates • Replikationsdaten • Backup				
Anwenderdaten • Word-Dateien • Excel-Tabellen • PowerPoint • CAD-Daten				
Streaming Daten • YouTube-Videos etc. • „Radio“, WebCast, Training				
Infrastruktur • DNS-Abfragen • AD-Replikation				
VoIP • Audio (100kit/Stream) • Video (150kbit - 2MBit)				

Monitoring

- „Klassisches Monitoring“ (MRTG, Cacti, Nagios, …)
  - Per SNMP all 5 Min die Bytes IN/OUT abfragen
  - Differenz ermitteln
  - Speichern und visualisieren
  - Tage/Woche/Monat
  - Mittelwerte über 5 Min !
- Problemfall
  - Kurzzeitige (>100ms) Peaks
  - Werden nicht erkannt
  - trügerische Sicherheit
- Besseres Monitoring
  - Router Queues (Packet Drop)
  - QoS Reports
  - „Dauerping“-Messung
  - VoIP-Readyness



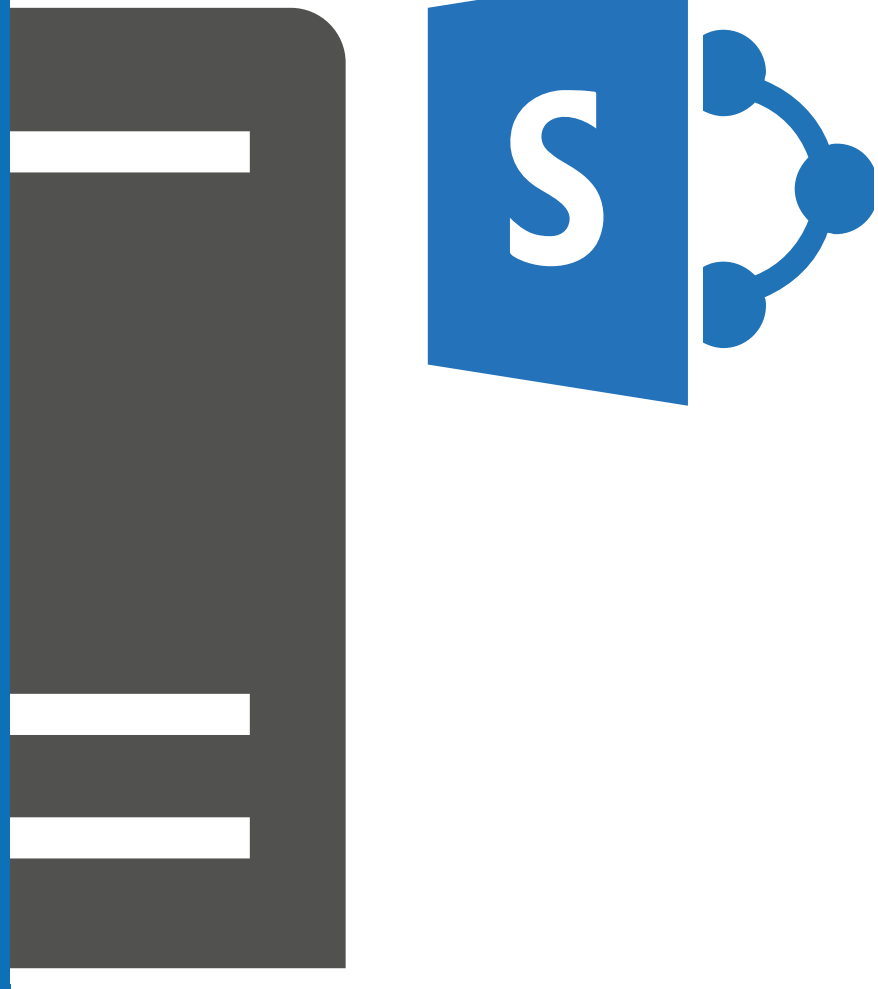
Skype for Business Online

IT vNext
Technologien richtig nutzen!

- Skype for Business in der Cloud ist genial für
  - IM/Presence intern und mit der Welt
  - Konferenzen mit externen Teilnehmern
  - 1:1 Audio/Video innerhalb der Firma
- Seit Dezember 2015
  - Konferenzeinwahl per Telefon in vielen Ländern
  - Broadcast Meetings für bis zu 10.000 User
- Einschränkungen gibt es bei ..
  - Konferenzen mit vielen internen Mitarbeitern
  - Audio in entfernten Niederlassungen

Telefonie/Audio bitte mit Express Route

SharePoint
One Drive



SharePoint / OneDrive Business

IT vNext
Technologien richtig nutzen!

- Online (Browser)
  - Anwender greifen per HTTPS auf Webseiten zu
  - Kurze große Datenmengen
  - Ein/Auschecken
  - Office Applikationen übertragen im Hintergrund
- Offline (OneDrive Business)
  - Client replizieren per HTTPS Verzeichnisse
  - Anwender nutzen lokale Dateien
  - Differenzreplikation
  - Mehrere Geräte erhöhen Bandbreite, Replikation „zu vieler“ Daten

Einschätzung

IT vNext
Technologien richtig nutzen!

- Bandbreite
  - Erforderlich aber nicht „Realtime“
  - Belastung des HTTPS-Proxy
- Volumen
  - Keine verlässliche Aussagen möglich
  - Permanent überwachen und beobachten
  - Lokale SharePoint Server / Dateiserver auswerten
    - z.B. per NetFlow auf dem SwitchPort
    - z.B. IISLogs beim Webserver

Office 365 Pro Plus

Software Office 365 ProPlus

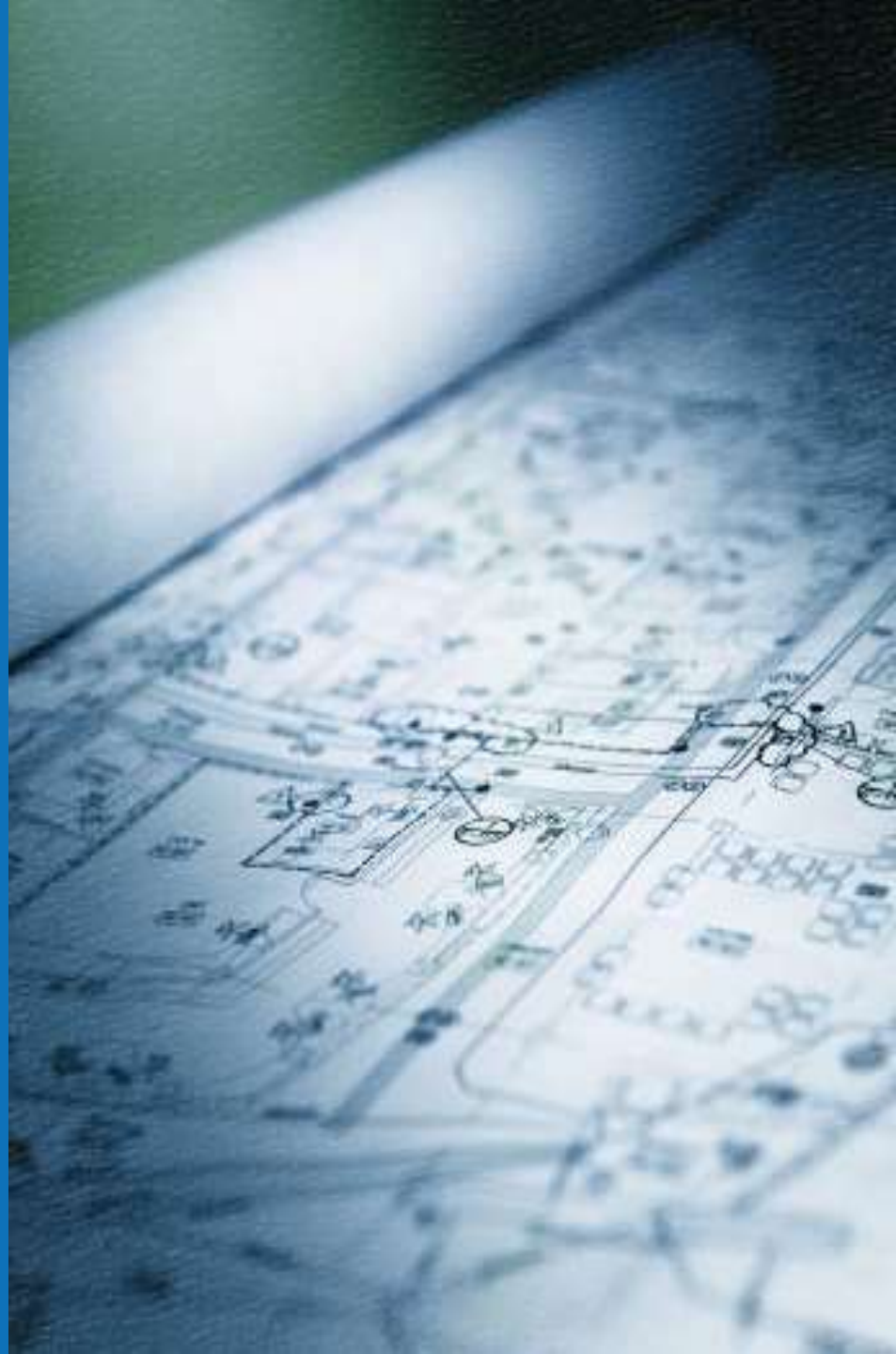
IT vNext
Technologien richtig nutzen!

- Office 365 enthält Software
  - Word, Excel, PowerPoint, Skype for Business
  - Lizenz muss durch den Admin zugewiesen sein
- Installation per „Click to Run“
  - Auch durch den Anwender selbst (Muss lokaler Admin sein)
  - HTTP-Proxy Caching
  - Lokale Verteilung ratsam !!
- Update per Streaming
  - Nicht mehr in WSUS/Windows Update zu sehen !
- Steuerung per XML und GPO
- Bandbreite: 800MB/Monat
- Sonderfall Terminal Server

Choose the Office software that users can install from the Office 365 portal
http://technet.microsoft.com/en-us/library/jj219421(v=office.15).aspx

Aktionsplan

Erfassen, Bewerten, Planen, Umsetzen, Kontrollieren



Aktionsplan

IT vNext
Technologien richtig nutzen!

- Analyse und Bewerten
  - Netzwerk: Verbindungen, Bandbreiten, Auslastung, Verwendung
  - Server/Client: Zugriffsmuster, Datenmengen (Migration), Forecast
- Planen
  - Zieldefinition, Migrationsweg, Kosten
  - Welche Protokolle und Datenmengen fallen wo an ?
- Umsetzen
  - Pilot aufsetzen, Planungen überprüfen, Bandbreiten und Monitoring anpassen.
- Migrieren und Betreiben

Links

- Artikel
  - Plan for Internet bandwidth usage for Office 365
    http://technet.microsoft.com/en-us/library/hh852542.aspx
  - Network bandwidth requirements for media traffic in Lync Server 2013
    http://technet.microsoft.com/en-us/library/jj688118.aspx
  - Plan for bandwidth requirements
    http://technet.microsoft.com/en-us/library/cc262952(v=office.15).aspx
- Kalkulatoren (Excel)
  - Exchange Client Network Bandwidth Calculator
    http://go.microsoft.com/fwlink/?LinkId=321550
  - Lync 2010 and 2013 Bandwidth Calculator
    http://go.microsoft.com/fwlink/?LinkId=321551
  - OneDrive for Business synchronization calculator
    http://go.microsoft.com/fwlink/?LinkId=517364
  - AD FS 2.0 Capacity Planning Spreadsheet
    http://www.microsoft.com/en-us/download/details.aspx?id=2278

Fragen?

Kontakt:
Frank Carius, frank.carius@netatwork.de
Net at Work GmbH, Am Hoppenhof 32 A, Paderborn
Tel:+49(5251)304-600
sip:frank.carius@netatwork.de