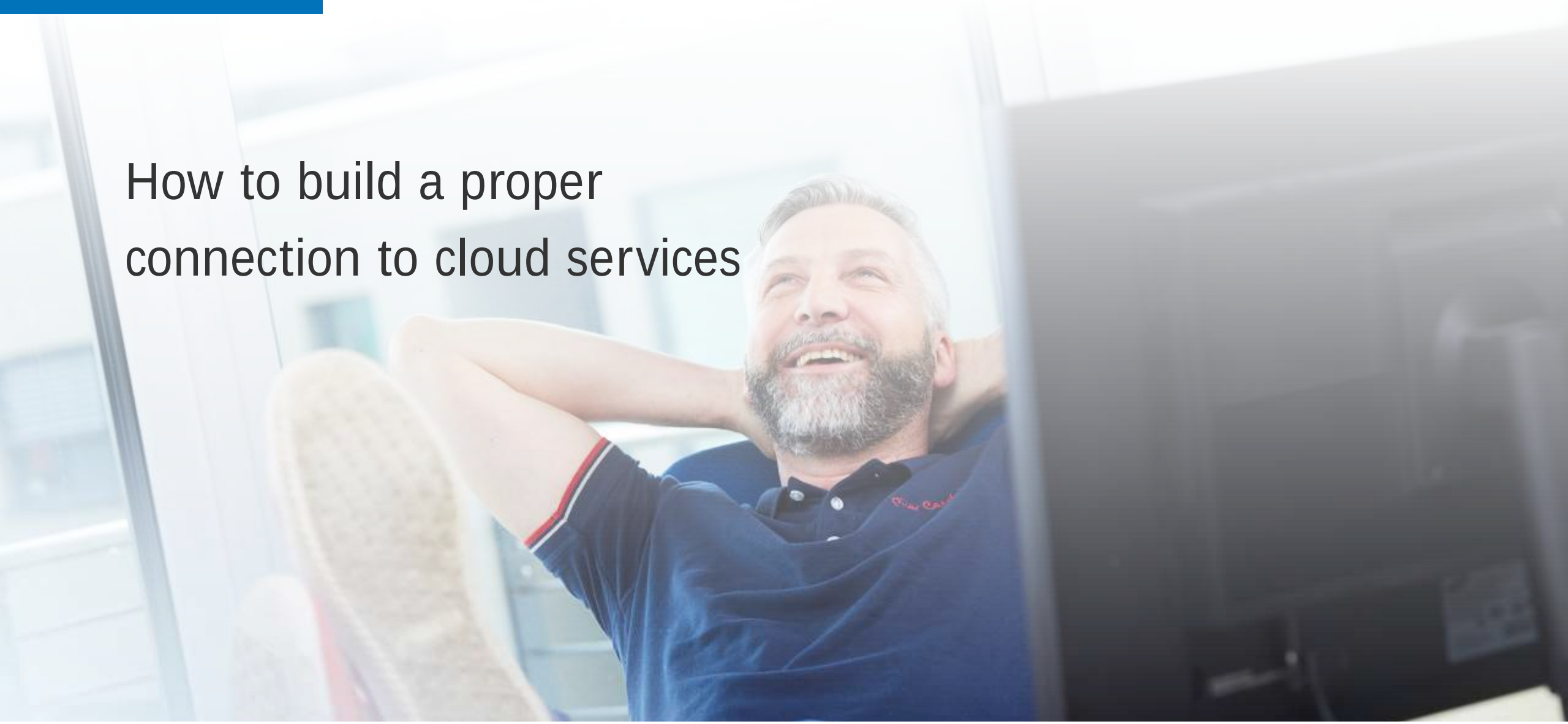
How to build a proper connection to cloud services



Net at Work
Building IT-Excellence.

My company and me

Frank Carius

Consultant and partner
MVP (20+ years)
MCM Lync 2010
https://www.msxfaq.de

My mission for today

- Lessons learned from many past “network assessment”
- Give you a “fresh up” about well known topics
- Show you additional options to monitor your network

Net at Work

130+ Employees
Founded: 1995
Head Office: Paderborn

Gold
Microsoft Partner
Cloud Productivity
Microsoft

System integrator with solutions and tools for your digital communication and collaboration

Think about trucks …

You are a gatekeeper at a factory exit and….

… you count the truck in/out

… you weight the trucks

That‘s SNMP-Monitoring today!

SNMP means

- Measures packets/sec In/Out
- Measures bytes/sec In/Out
- Shows bandwidth utilization

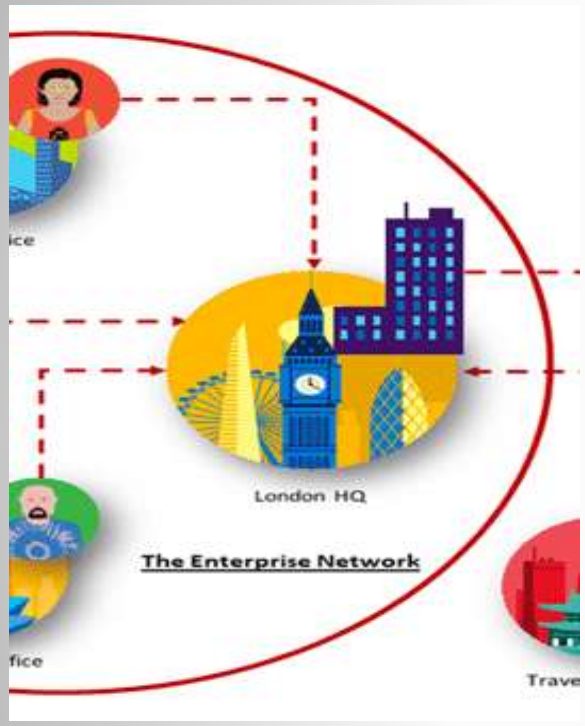
Is this valid to measure cloud performance?

- Low utilization = no problem ?
- Far network congestion = empty gate
- Providers are not delivering „Live traffic maps“

We have to change our current monitoring?

Challenges – Network Evolution

- Prior cloud adoption
  - Structured progress, data collection and forecast (hopefully)
  - How much bandwidth do we need?
  - Do we really have to buy more bandwidth? ($$$)
  - Can we have some estimations, can we measure our current system ?
  - Can we make sure that … everything is working. Can you certify that?
- Spring 2020 (Covid, Homeoffice, inbound, offload)
  - bandwidth overload, SfB OnPremises, high load on VPN-Servers, …
  - Quick Migration to Cloud Services (primarily Teams, Zoom, …)
  - Companies have increased bandwidth and VPN-Servers
- 2021 Back to office – outgoing traffic
  - People were coming back to the office
  - But they will not stop using teams and other cloud service



What Microsoft tells us

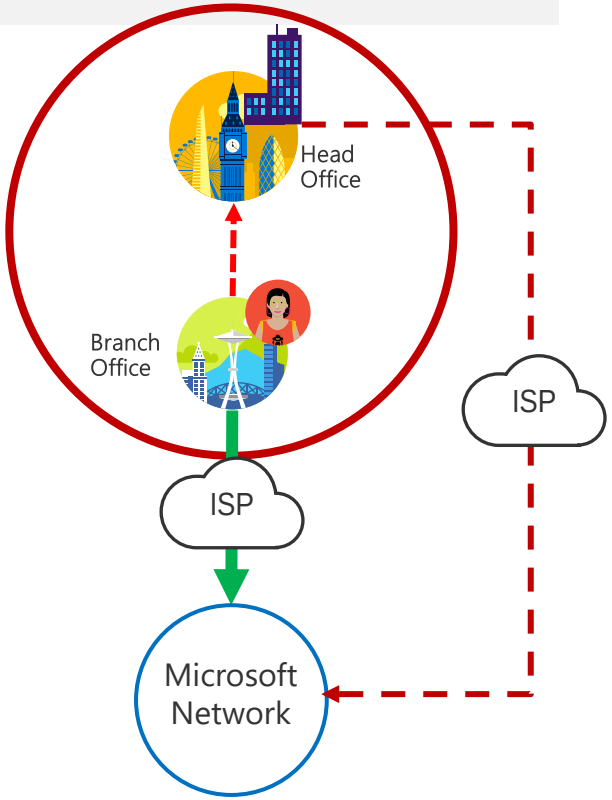
(Slide 1-3)

Office 365 Guiding Principles

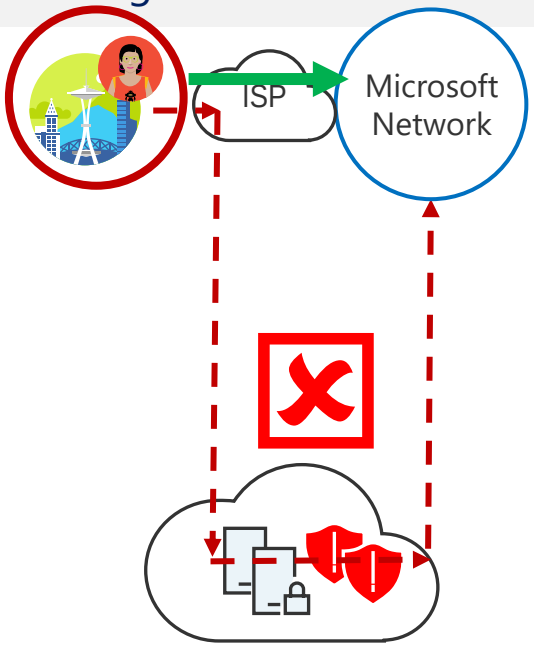
Identify and differentiate Office 365 traffic using Microsoft published endpoints

aka.ms/o365ip

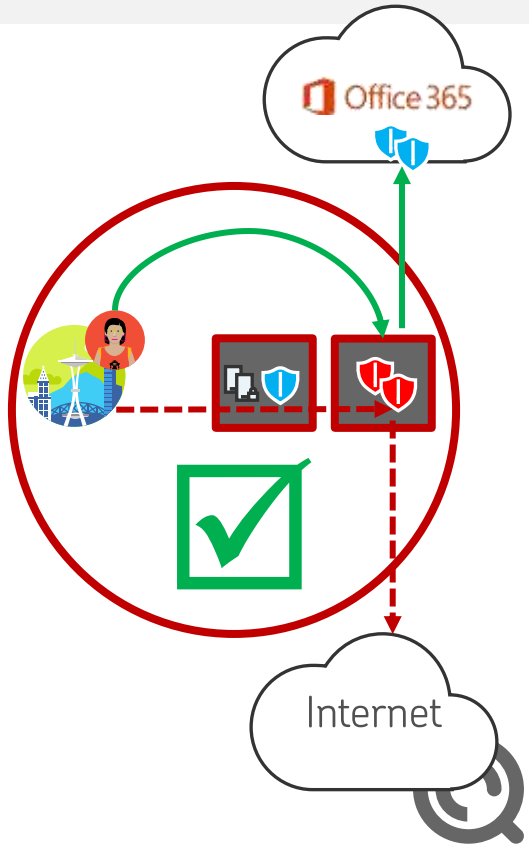
Egress Office 365 data connections as close to the user as practical with matching DNS resolution



Avoid network hairpins and optimize connectivity directly into the nearest entry point into Microsoft's global network



Assess bypassing proxies, traffic inspection devices and duplicate security which is available in Office 365

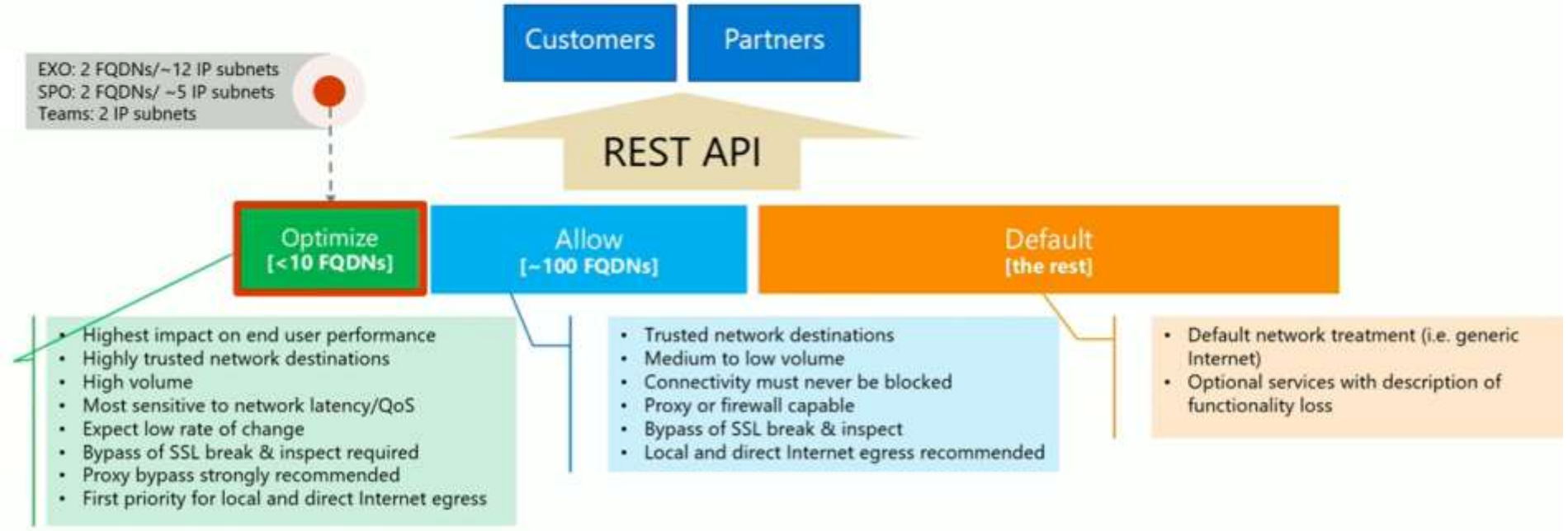


Source: BRK3030 - Office 365 Network - Guiding Principles
https://techcommunity.microsoft.com/t5/Microsoft-Tech-Summit-Content-17/Understanding-optimizing-amp-securing-enterprise-network/td-p/126371

Target: Optimize, Allow and Default

Office 365 endpoints (FQDNs, IPs, ports, protocols)

- Office 365 REST API (http://aka.ms/ipurlws) for automating customer Office 365 network settings
- Priority driven endpoint taxonomy (http://aka.ms/ipurlblog) for easier customer network optimizations
- Growing support for native integration across partner community
- **Key point: Focus your network optimization on key Office 365 experiences first (Optimize set)**



Optimal network connectivity for Office 365 performance: What is it and how to get | BRK3040
Source: https://youtu.be/XiQwR12rkO8?t=1564

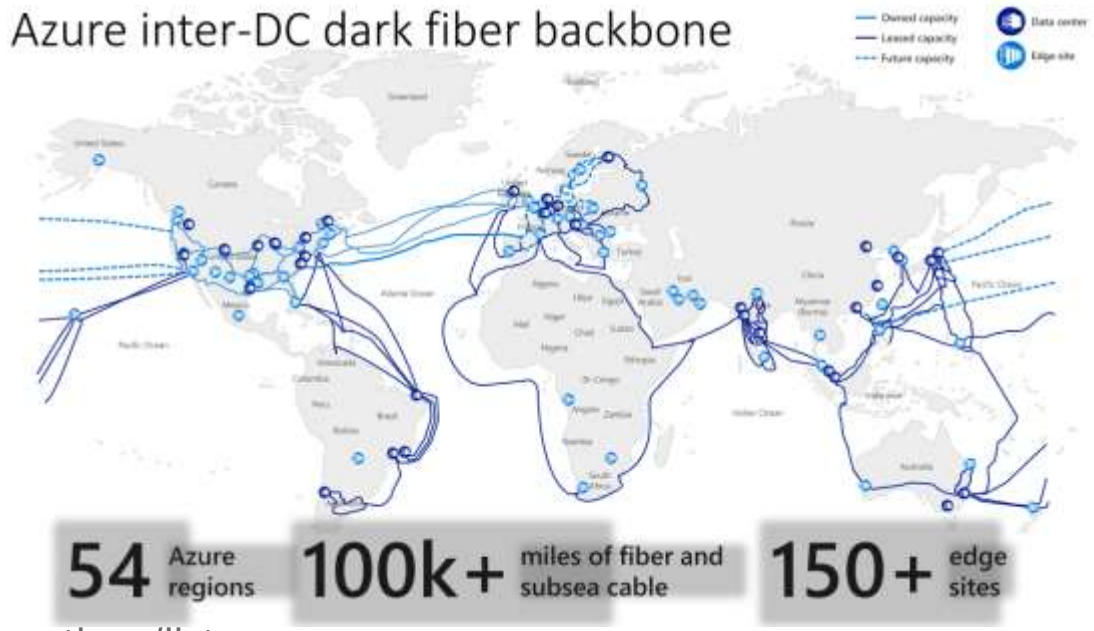
More Microsoft Links

- Office 365 Connectivity Principles in greater detail
  https://aka.ms/PNC
  https://techcommunity.microsoft.com/t5/Office-365-Blog/Getting-the-best-connectivity-and-performance-in-Office-365/ba-p/124694
- Office 365 product group videos expanding on the Office 365 connectivity principles:
  Strategy: https://youtu.be/19a8s90HboQ
  Planning: https://youtu.be/cJDpB59gk3M
  Implementation: https://youtu.be/lZwvitkvg6A
- Optimal network connectivity for Office 365 performance: What is it and how to get | BRK3040
  https://aka.ms/brk3000 ->
  https://www.youtube.com/watch?v=XiQwR12rkO8
- Guidance on network planning and perf tuning in Office 365
  https://aka.ms/tune
- Office 365 URLs and IP addresses:
  https://aka.ms/O365IP
- Managing bandwidth requirements for Office 365
  https://aka.ms/O365networkconnectivity
- Getting the best connectivity and performance in Office 365
  https://techcommunity.microsoft.com/t5/office-365-blog/getting-the-best-connectivity-and-performance-in-office-365/ba-p/124694
- Announcing: Office 365 endpoint categories and Office 365 IP Address and URL web service
  https://techcommunity.microsoft.com/t5/office-365-blog/announcing-office-365-endpoint-categories-and-office-365-ip/ba-p/177638
- Understanding optimizing&securing enterprise networkhttps://techcommunity.microsoft.com/t5/Microsoft-Tech-Summit-Content-17/Understanding-optimizing-amp-securing-enterprise-network/td-p/126371

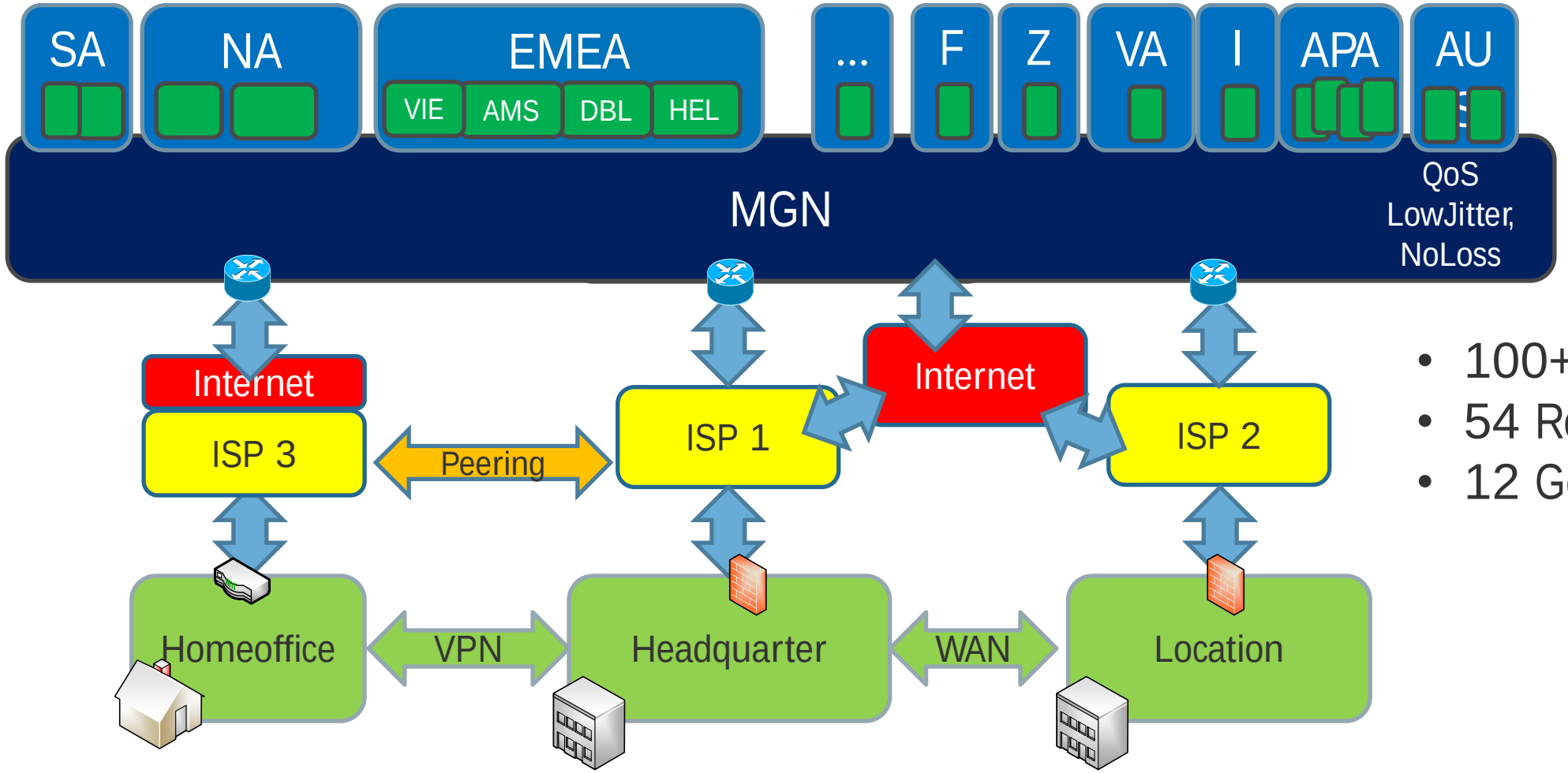
Microsoft Global Network

Microsoft Global Network

- Microsofts own world wide network
  - 200+ Peering Locations, 4000+ Network, 100+ Frontdoor-Locations, 50 Datacenter Regions
  - Owned fiber (>800.000km in USA) (document from 2015) http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf
  - QoS managed, no loss, no jitter
  - Multiple Terabit Peerings
  - See BRK3000 - Strategies for building effective, optimal and future proof connectivity to Office 365 that will delight your users
- BGP: Microsoft ASN= 8075
  - https://www.peeringdb.com/asn/8075
  - https://stat.ripe.net/AS8075#tabId=at-a-glance
  - #IPv4 Prefix:149 about 20.184.320 IPs
  - #IPv6 Prefix:10 about 8.589.324 /48s
- Peering List for Azure
  - https://docs.microsoft.com/en-us/rest/api/peering/peeringlocations/list

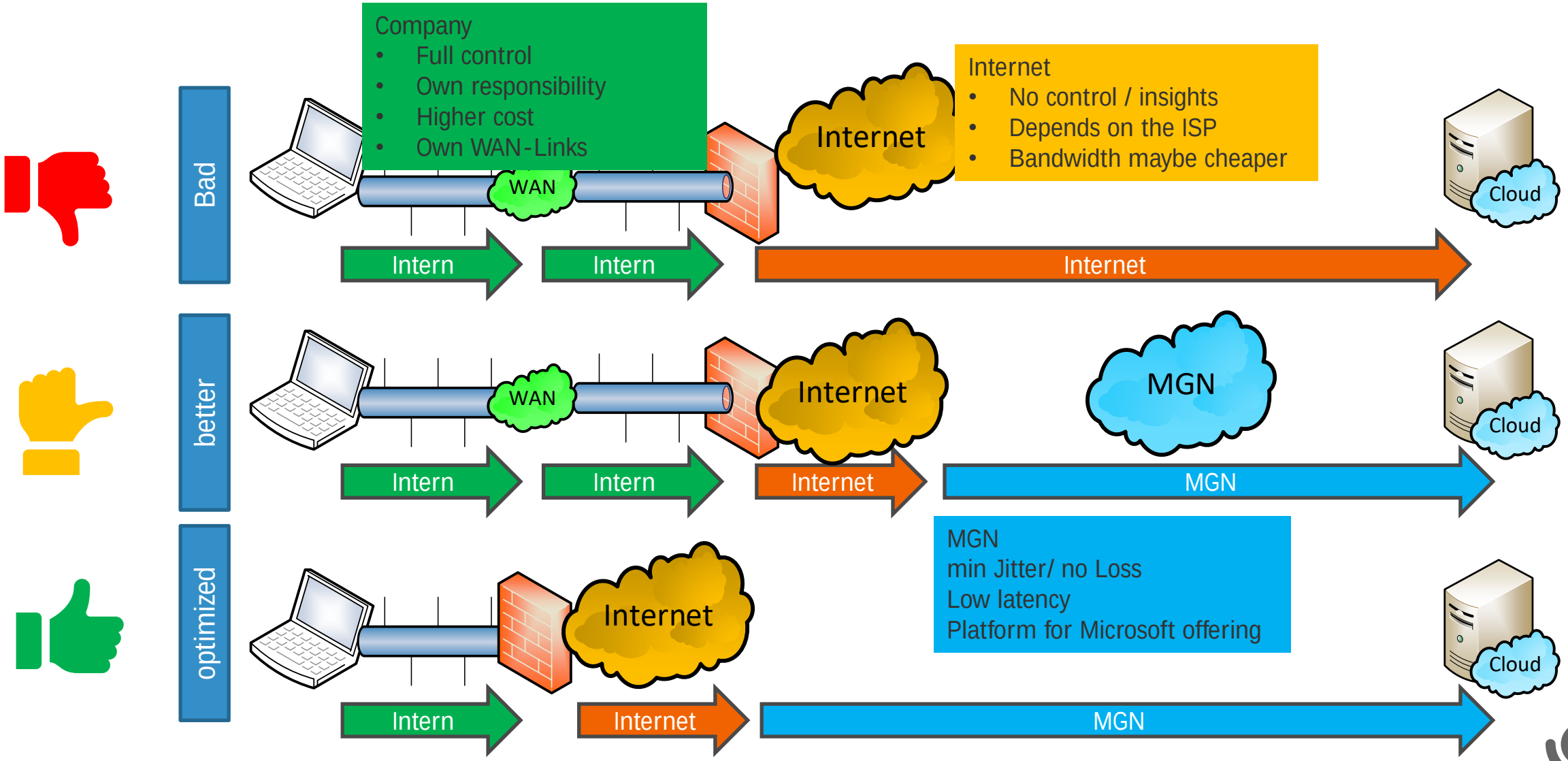


Connect your client to the service



- 100+ Azure RZs
- 54 Regions
- 12 Geos

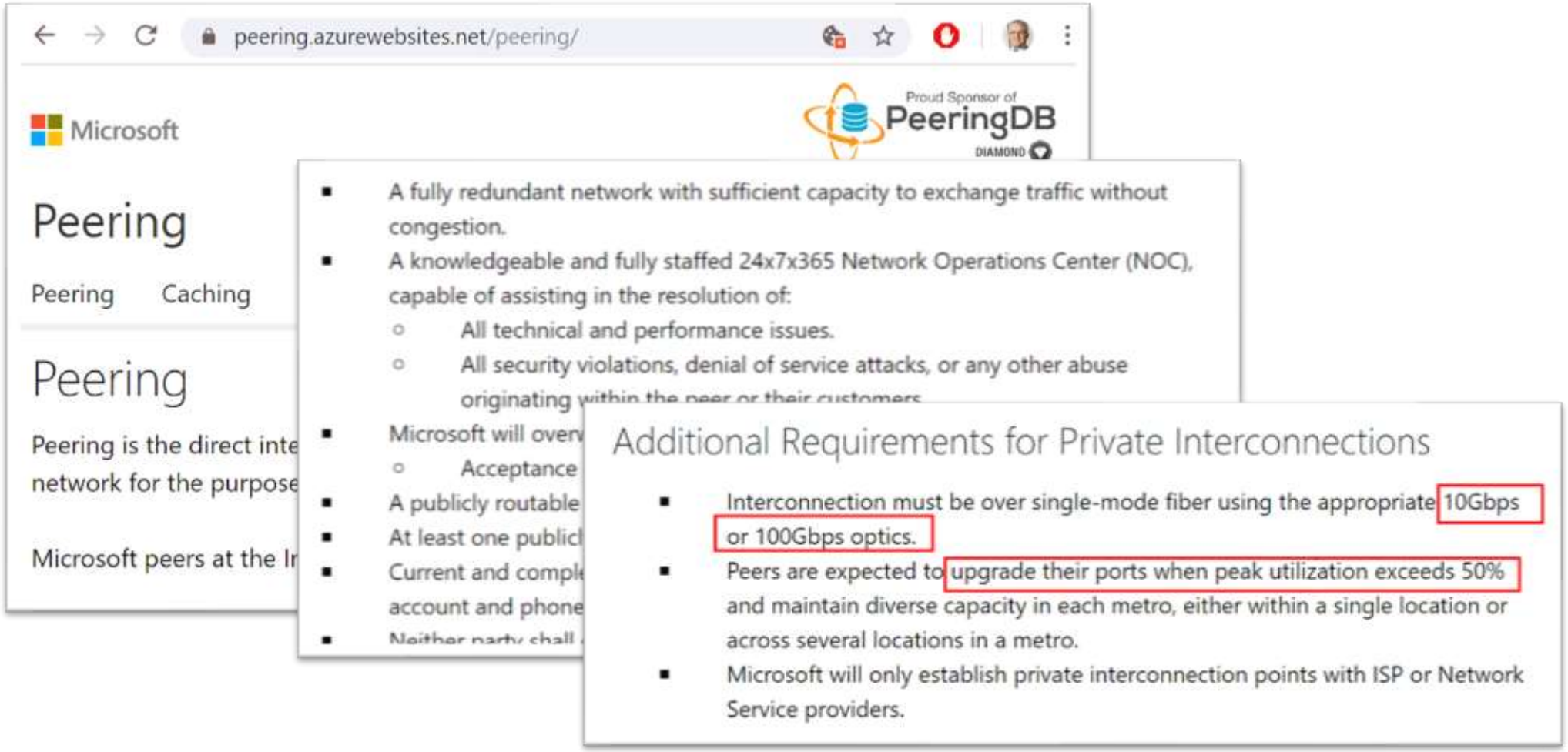
M365 is not „the internet“. Hot potato



Peerings

- Public Peering
  - AMS-IX, DECIX, u.a.
  - Check your routing, ask your upstream provider, do a traceroute
  - https://peeringdb.com
- Expressroute
  - Bring your own Eigene Leitung zu Azure
  - BGP-Routing
  - POP in Amsterdam und Rotterdam
- Option: Provider with Peerings (Auszug)
  - Peering Service Preview Partners
    https://docs.microsoft.com/en-us/azure/peering-service/location-partners
  - DeCIX Azure Peering Services
    https://www.de-cix.net/en/de-cix-service-world/closed-user-groups/microsoft-azure-peering-service
  - Colt
    https://www.colt.net/why-colt/strategic-alliances/microsoft-partnership/
  - InterCloud
    https://intercloud.com/partners/microsoft-saas-applications/
  - interxion
    https://www.interxion.com/why-interxion/colocate-with-the-clouds/Microsoft-Azure/

Microsoft Peering



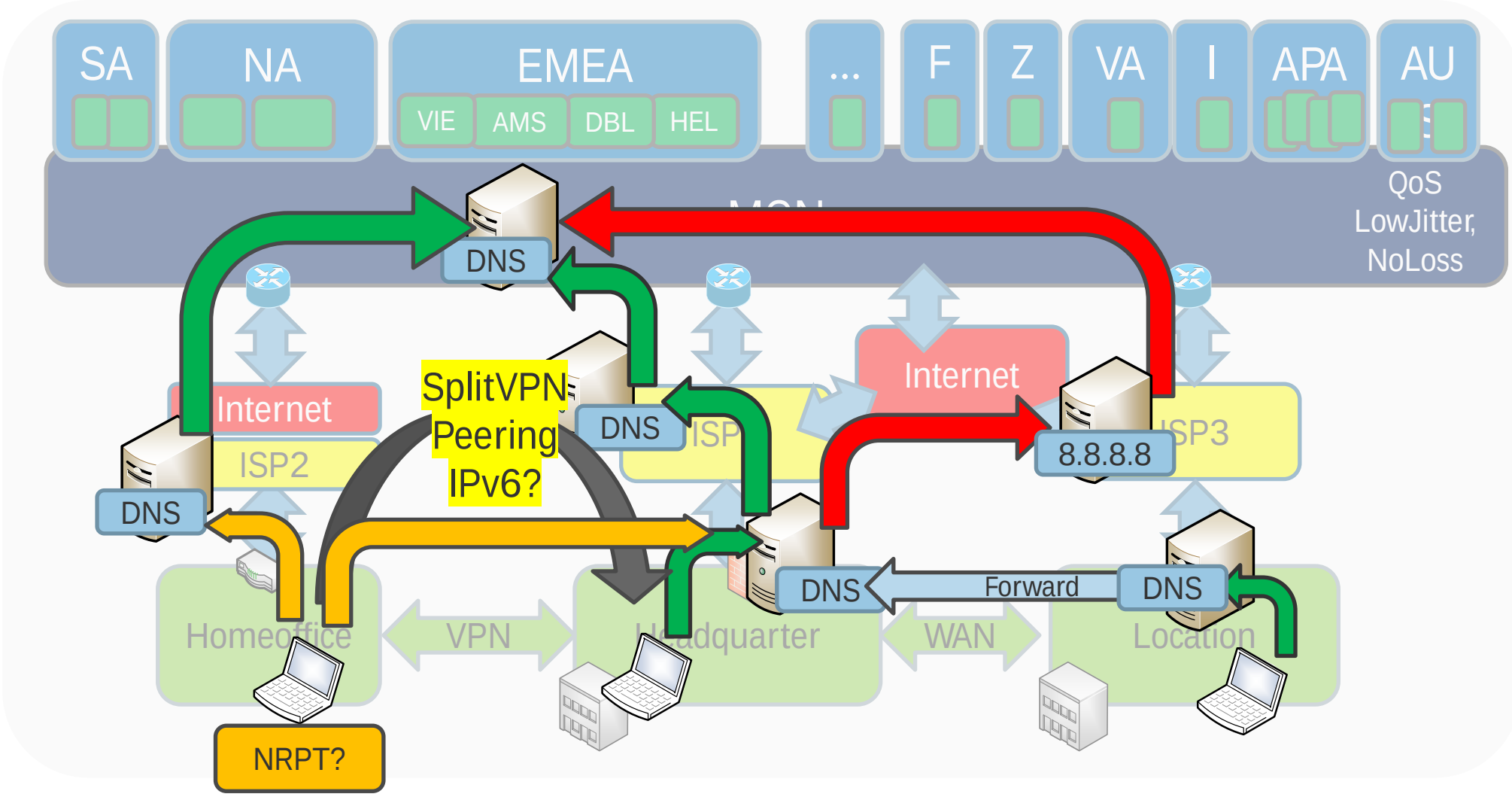
Microsoft Peering Policy
https://www.microsoft.com/peering -> https://peering.azurewebsites.net/peering/

```
Eingabeaufforderung - pwsh
PS C:\Users\fcarius> tracert outlook.office365.com

Routenverfolgung zu FRA-efz.ms-acdc.office.com [52.97.223.82]
über maximal 30 Hops:

  1     1 ms     2 ms     1 ms  10.42.0.1
  2     1 ms     1 ms     1 ms  port-195-158-157-129.static.isionline-dialin.de [195.158.157.129]
  3     2 ms     1 ms    15 ms  ipservice-092-214-080-105.092.214.pools.vodafone-ip.de [92.214.80.105]
  4     3 ms     2 ms     2 ms  88.79.20.28
  5     4 ms     4 ms     3 ms  188.111.129.22
  6     3 ms     3 ms     3 ms  145.254.2.183
  7     4 ms     3 ms     4 ms  ae60-0.ier01.dus30.ntwk.msn.net [104.44.36.177]
  8    14 ms    21 ms     7 ms  ae27-0.icr01.ams30.ntwk.msn.net [104.44.42.95]
  9     9 ms     9 ms     9 ms  be-100-0.ibr01.ams30.ntwk.msn.net [104.44.22.215]
 10     9 ms     8 ms     9 ms  be-9-0.ibr03.ams06.ntwk.msn.net [104.44.29.249]
 11    13 ms     8 ms     8 ms  ae142-0.icr02.ams06.ntwk.msn.net [104.44.21.174]
 12     *        *        *     Zeitüberschreitung der Anforderung.
 13     *        *        *     Zeitüberschreitung der Anforderung.
 14     *        *        *     Zeitüberschreitung der Anforderung.
 15     *        *        *     Zeitüberschreitung der Anforderung.
 16     *        *        *     Zeitüberschreitung der Anforderung.
 17     8 ms     8 ms     7 ms  52.97.223.82

Ablaufverfolgung beendet.
```

TRACEROUTE, PEERINGDB

The magic of DNS

DNS-Resolution



DEMO: DNS WITH EXCHANGE ONLINE

DNS Round Robin / TTL

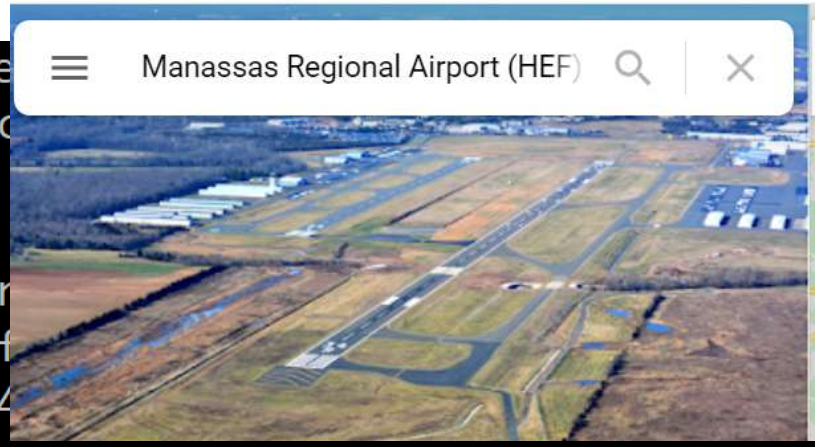
PowerShell 7 (x64)

```
PS C:\> Get-DnsClientCache outlook.office365.com | ft -AutoSize

Entry                RecordName                RecordType Status  Section TimeToLive Data
-----                ----------                ---------- ------  ------- ---------- ----
outlook.office365.com outlook.office365.com      CNAME      Success Answer          2 outlook.ms-acdc.office.com
outlook.office365.com outlook.ms-acdc.office.com CNAME      Success Answer          2 FRA-efz.ms-acdc.office.com
outlook.office365.com FRA-efz.ms-acdc.office.com AAAA       Success Answer          2 2603:1026:200:63::2
outlook.office365.com FRA-efz.ms-acdc.office.com AAAA       Success Answer          2 2603:1026:207:131::2
outlook.office365.com FRA-efz.ms-acdc.office.com AAAA       Success Answer          2 2603:1026:207:cd::2
outlook.office365.com outlook.office365.com      CNAME      Success Answer          8 outlook.ms-acdc.office.com
outlook.office365.com outlook.ms-acdc.office.com CNAME      Success Answer          8 FRA-efz.ms-acdc.office.com
outlook.office365.com FRA-efz.ms-acdc.office.com A          Success Answer          8 40.101.19.162
outlook.office365.com FRA-efz.ms-acdc.office.com A          Success Answer          8 40.101.121.34
outlook.office365.com FRA-efz.ms-acdc.office.com A          Success Answer          8 40.101.80.2
```

- outlook.office365.com is CNAME to outlook.ms-acdc.office.om
- outlook.ms-acdc.officec.om is CNAME to <region>.ms-acdc.office.com
- <region>.ms-acdc.office.com has multiple A-Records
- All entries have a very short TTL!

Sample: wrong DNS-Server

```
C:\>nslookup outlook.office
Server:  home1.bellatlantic
Address:  199.45.32.43

Nicht autorisierende Antwor
Name:    MNZ-efz.ms-acdc.of
Addresses:  2603:1036:302:4
```

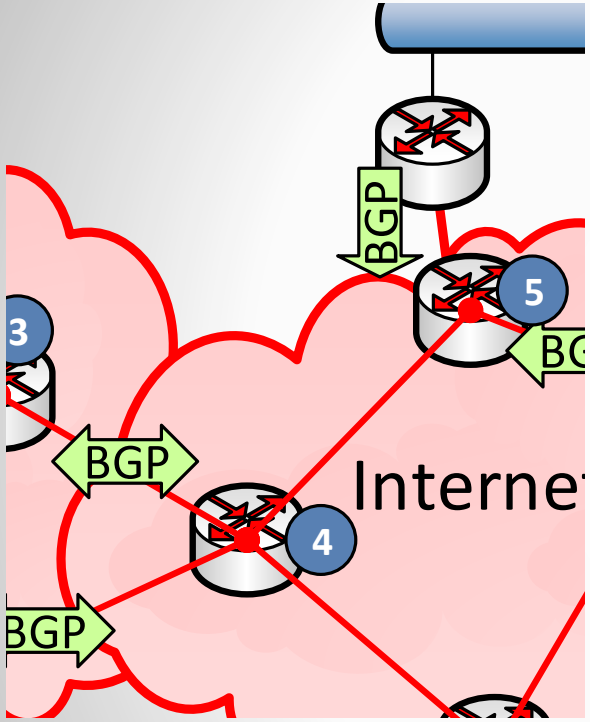



```
C:\>tracert 52.96.87.210

Routenverfolgung zu 52.96.87.210 über maximal 30 Hops

  1     2 ms     1 ms     1 ms  fritz.box [192.168.178.1]
  2     5 ms     4 ms     5 ms  p3e9bf2dc.dip0.t-ipconnect.de [62.155.242.220]
  3    12 ms    11 ms    12 ms  d-ed5-i.D.DE.NET.DTAG.DE [62.154.5.213]
  4    12 ms    12 ms    12 ms  80.157.204.58
  5    16 ms    15 ms    16 ms  ae18.cr3-ams1.ip4.gtt.net [213.200.117.218]
  6    16 ms    16 ms    16 ms  ip4.gtt.net [154.14.37.246]
  7    16 ms    16 ms    16 ms  ae25-0.icr01.ams21.ntwk.msn.net [104.44.239.75]
  8    97 ms    96 ms    96 ms  be-100-0.ibr01.ams21.ntwk.msn.net [104.44.22.235]
  9    97 ms    96 ms    96 ms  be-8-0.ibr01.dub08.ntwk.msn.net [104.44.19.212]
 10    97 ms    96 ms    96 ms  be-7-0.ibr01.sxl71.ntwk.msn.net [104.44.16.116]
```

Validation

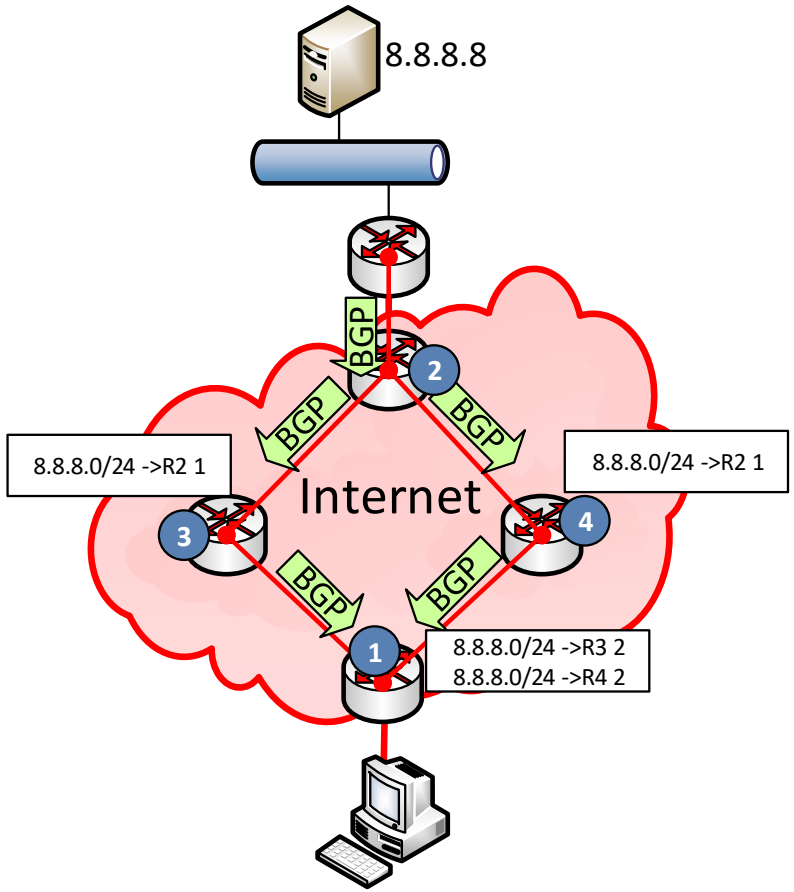
- Make sure that the clients use the „right DNS-Server“
- Watch for
  - DNS-Servers in the wrong region
  - DNS-Forwarding from location to headquarter
  - „optimizing“ servers (PiHole etc)
  - „Hosted“ Filter-Services
  - Cloud Proxy
  - IPv6 and VPN
- DNS and VPN: Name Resolution Policy Table?
- DNS Resolution should follow packet routing

Anycast IP Routing

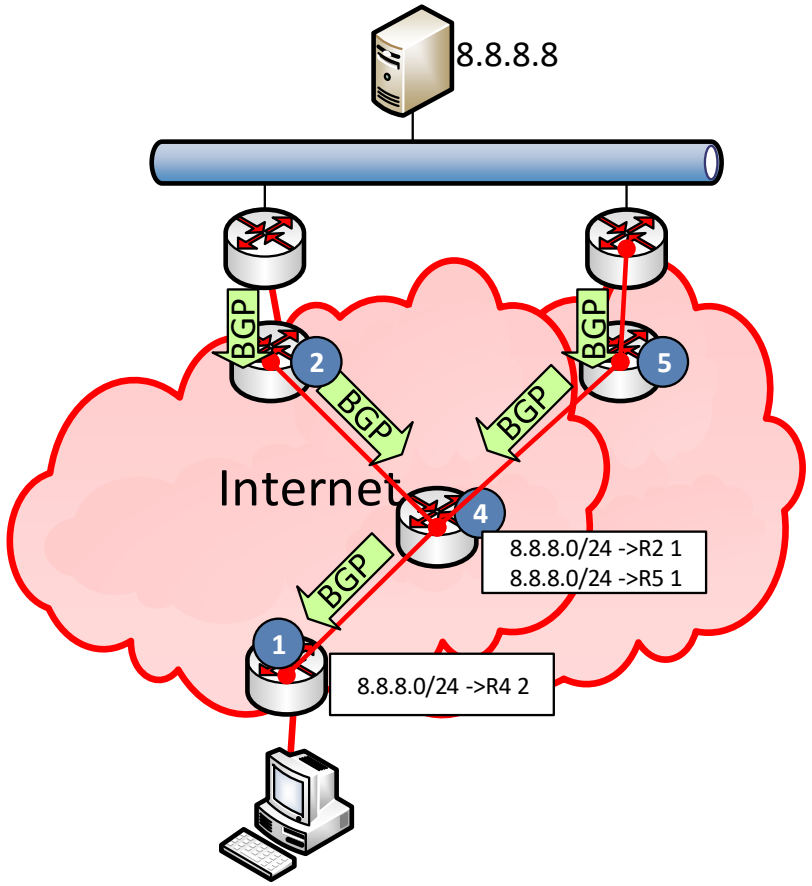


Redundant IP-Routing

Redundant routing

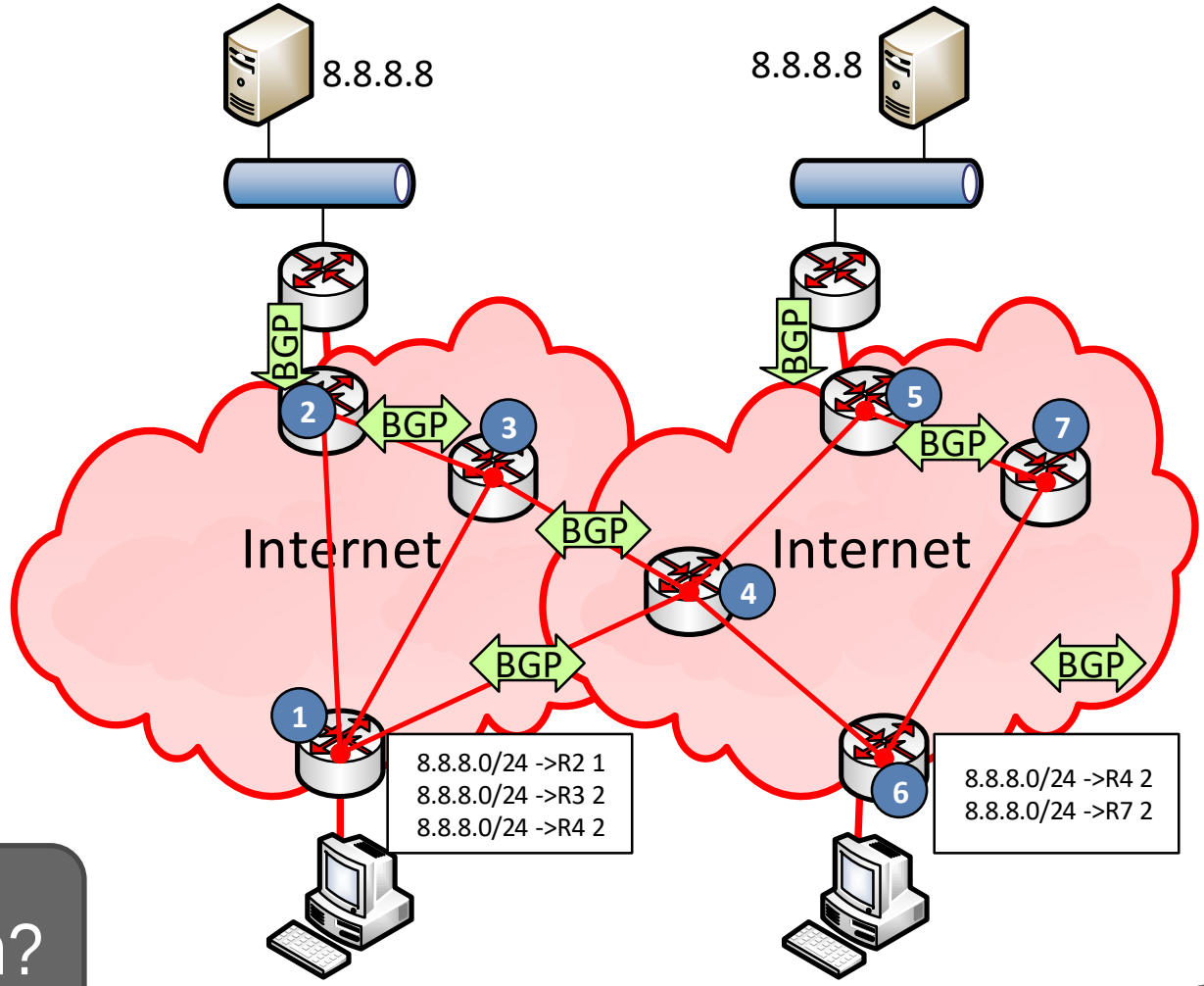


Redundant provider



Anycast IP

- Multiple servers
- Identical services
- Distributed locations
- Announced by BGP etc.
- Is not „Geo-DNS“
- High available
- High scalability
- „Nearest Server“



„fixing“ a wrong DNS configuration?

DNS by Microsoft 365 Service

	Name	IP	Target
Exchange Online	GeoDNS outlook.office365.com AnyCast-DNS (partial) outlook.office.com	AMS-efz.ms-acdc.office.com FRA-efz.ms-acdc.office.com LHR-efz.ms-acdc.office.com SFX-efz.ms-acdc.office.com SJC-efz.ms-acdc.office.com CPQ-efz.ms-acdc.office.com	Different entry points
SharePoint/OneDrive	Anycast DNS <tenant>.sharepoint.com <tenant>-my.sharepoint.com	spo-0004.spo-msedge.net	13.107.136.9
Teams HTTP	Anycast DNS teams.microsoft.com	s-0005.s-msedge.net o.a.	52.113.194.132 2620:1ec:42::132
Teams RTP	GeoDNS worldaz.tr.teams.microsoft.com	To much and very short TTL	13.107.64.0/18 52.112.0.0/14 52.120.0.0/14
SfB Online Edge	IP-Adresses as part of the SDP	No DNS, Inband	obsolet

Windows Size

Port-Limits

TCP-Chimney

Windowsize / RSS

SACK

You all should know this already – but it is not present

TCP Level 400

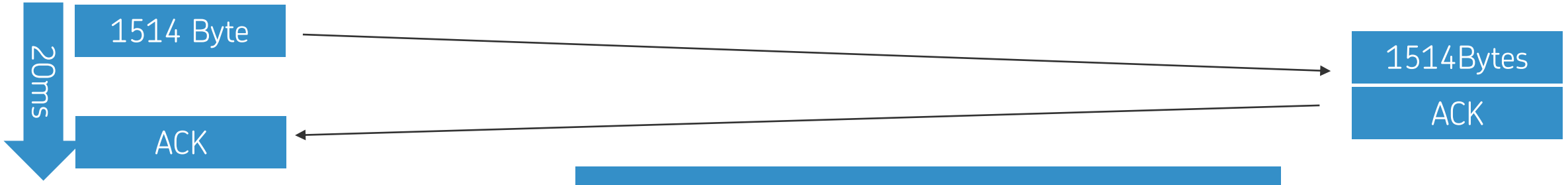
LATENCY AND THROUGHPUT

Big-Fat-Pipe problem and latency

- 1x PC + 1x Server
  - CPU unlimited
  - Disk unlimited
  - LAN Unlimited
- 1x WAN-Link
  - „Unlimited“ Bandwidth
  - 20ms Roundtrip Time

Quiz: Maximum throughput with single FTP transfer

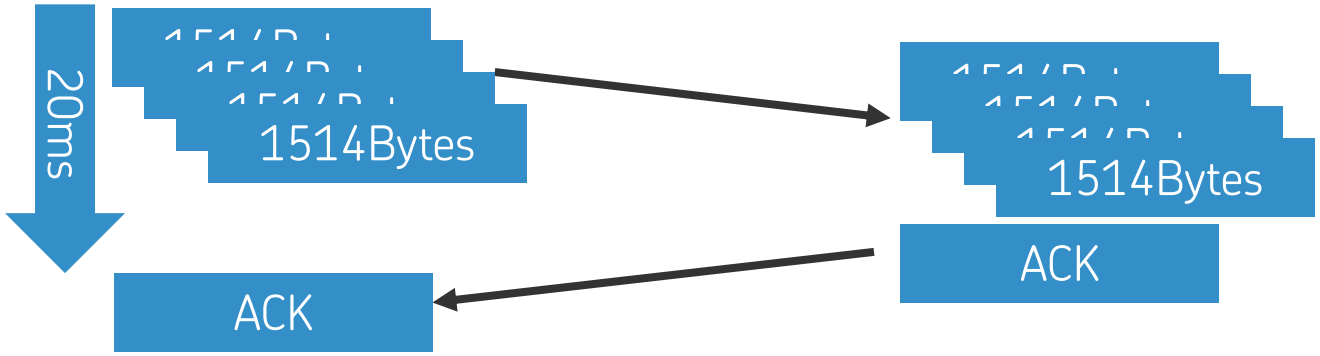
- <=1 MBit
- 1-10 MBit
- 10-100 MBit
- >100 MBit



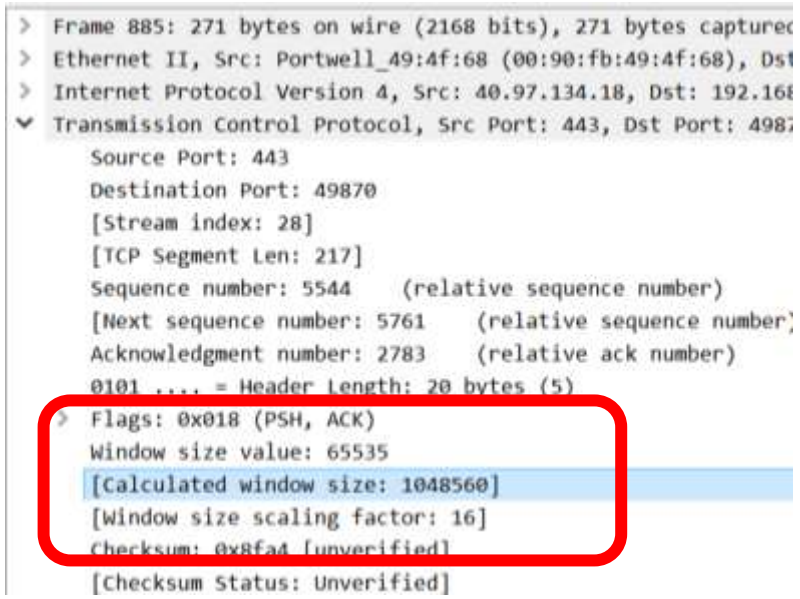
50 packets * 1514 bytes = 75kByte/sec

Windows Scaling and latency

- Send multiple packets as block and accept later ACK-packes
  - Sender and receiver must maintain a buffer to resend lost packet and reassemble reordered packes
  - Negotiation of buffersize required: (max. 1 GB, Win2008: 16MB)
  - „RFC1323 TCP Extensions for High Performance"
  - Selective Ack (SACK)



https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc162519(v=msdn.10)
https://www.msxfaq.de/netzwerk/grundlagen/tcp_retransmit_und_sack.htm



Windowsize and Latenz = Throughput

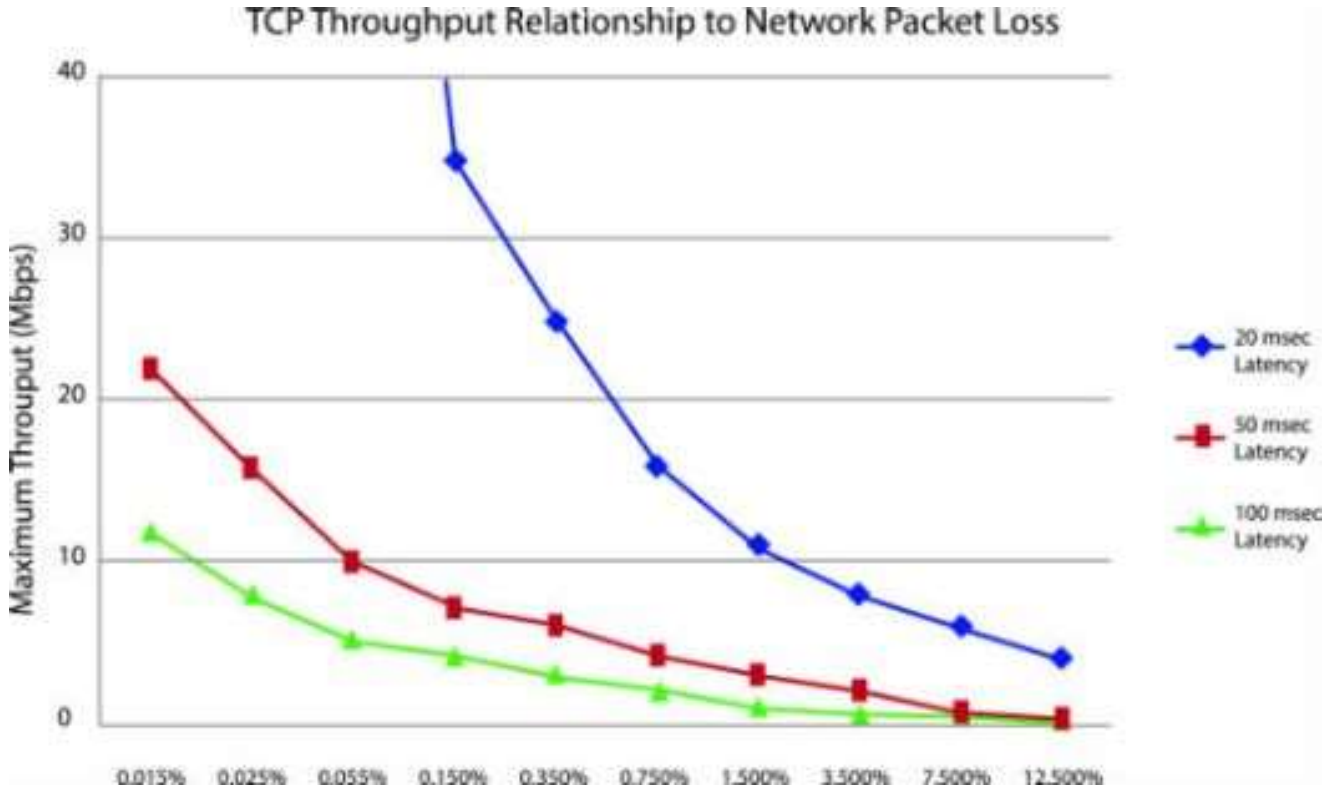
Applikation	Windowsize	1ms	20ms	50ms	100ms	200ms
Exchange Webservices (EWS)	1.048.560	na	50MB/s	20MB/s	10MB/s	5MB/s
OneDrive 10MB Upload	1.059.840	na	50MB/s	20MB/s	10MB/s	5MB/s
SharePoint 12MB Download	4.273.920	na	208MB/s	84MB/s	42MB/s	21MB/s
End2end-http Outlook	1.588.480	na	75MB/s	30MB/s	15MB/s	7,5MB/s
Outlook Client	525.568	na	25MB/s	10MB/s	5MB/s	2,5MB/s
SFTP using SSH 1and1	131584	na	6MB/s	2,4MB/s	1,2MB/s	660kB/s
SMB im LAN	2.102.272	GB+	na	na	na	na

These are „real world“ values, measured with WireShark.
Have you checked your values? Some firewalls are „adjusting“ them

PACKETLOSS AND THOUGHPUT

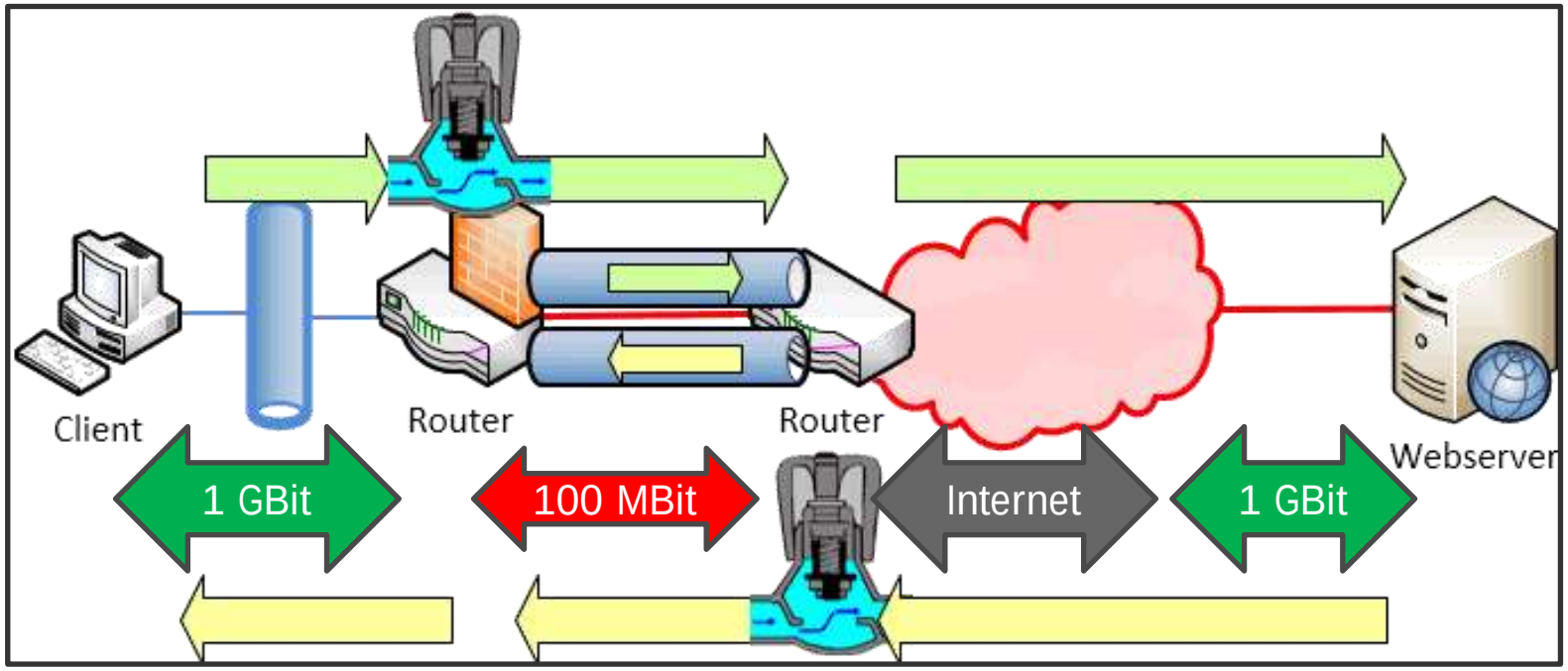
Paket Loss affects throughput

- Why Packetloss
  - Link-Congestion
  - Queue-overflow
  - Rare: electrical issues
- TCP-Stack: Recipient
  - Stop delivery
  - Request retransmit
- TCP-Stack: Sender
  - Retransmit lost packet
  - Throttle down send rate
- VoIP ?
  - UDP preferred – no retransmit
  - RTCP-Message to sender
  - Adapt Bitrate (less fps)
  - Change codec (wideband to narrowband)



Source: https://telnetnetworks.wordpress.com/tag/packet-loss/

Quiz: Bandwidth policies and firewall



Given situation: limited bandwidth. Can i control „downstream?

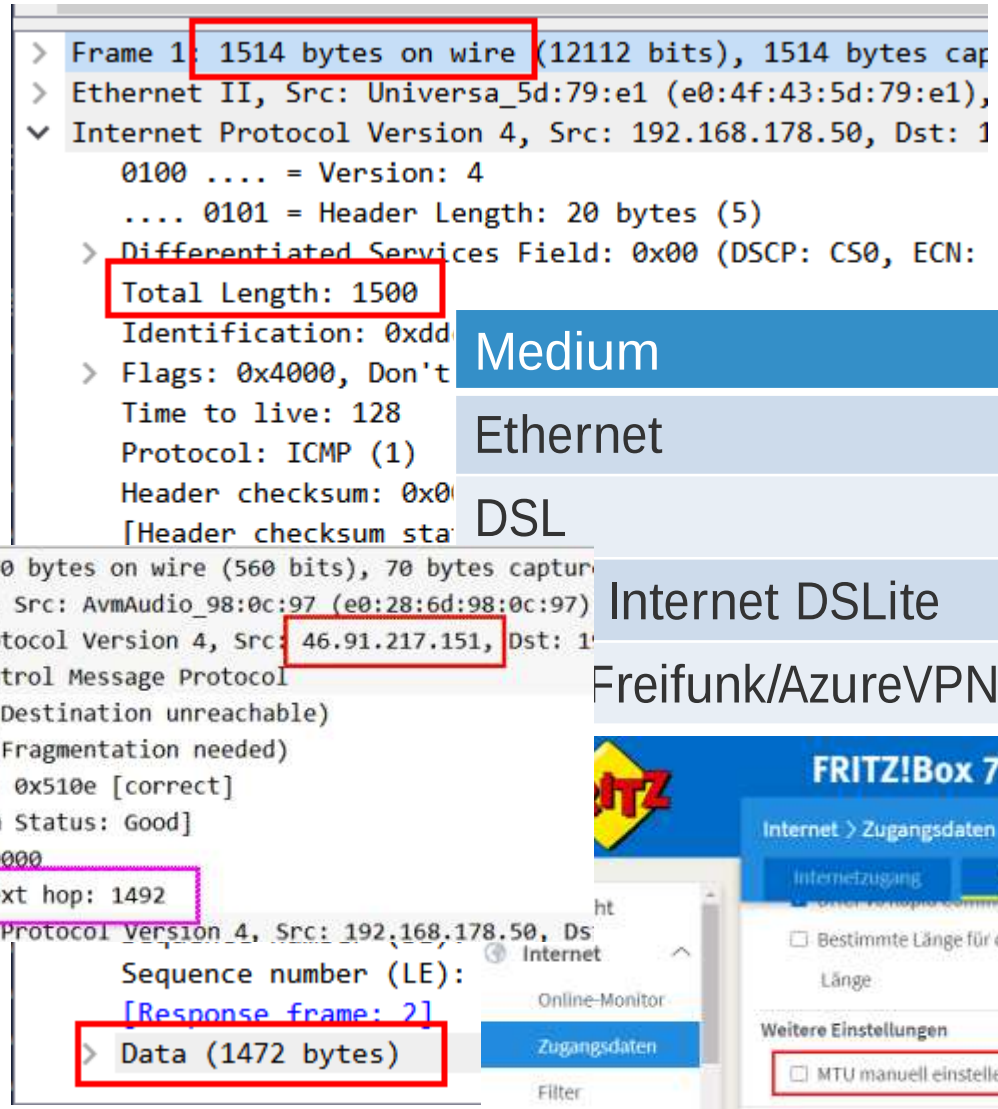
- I can control and prioritize outbound traffic
- But do i need my ISP to optimize inbound traffic?

A Firewall can throttle TCP-ACK to limit inbound rate.

MTU AND ICMP BLOCKING

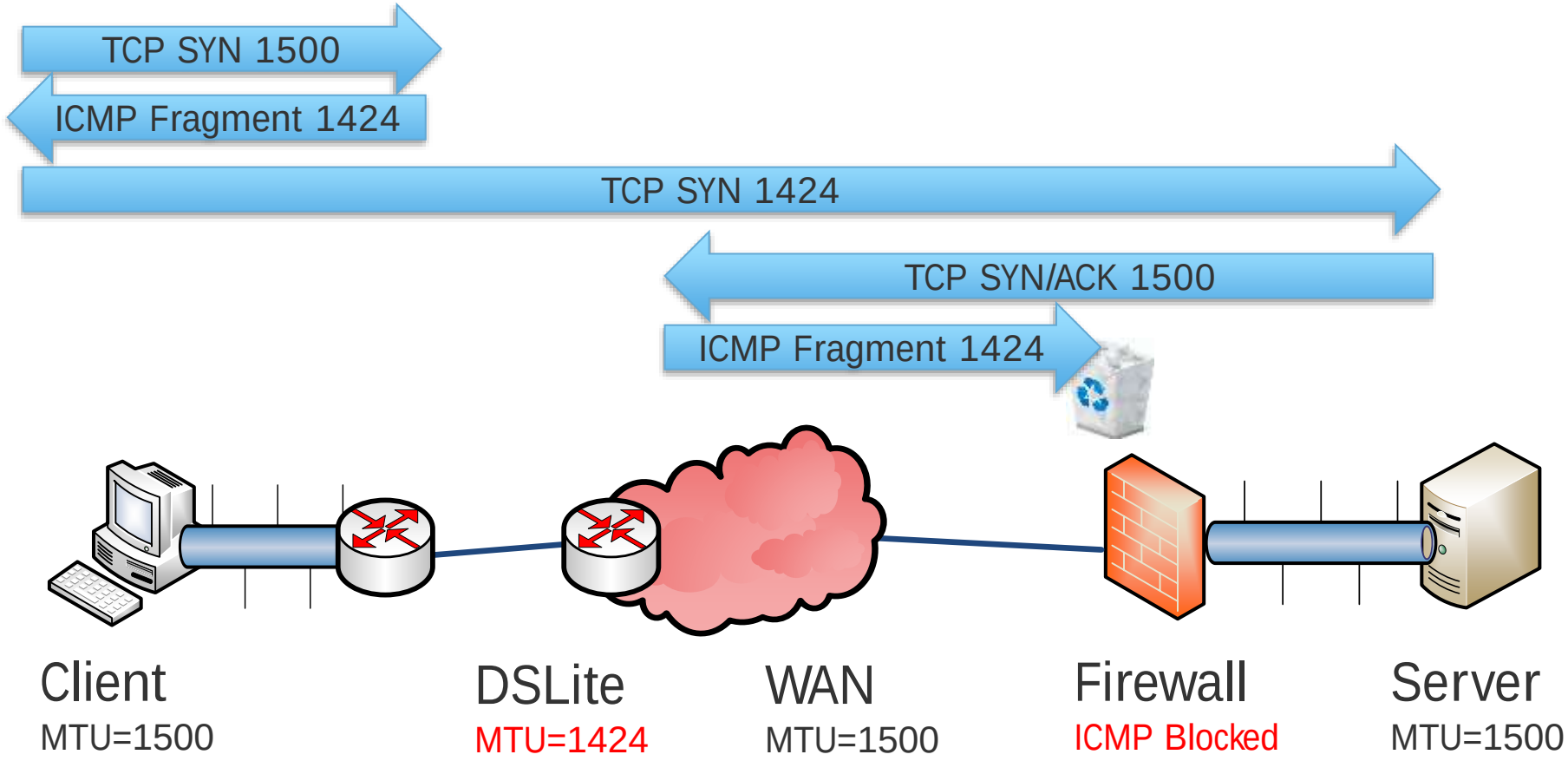
MTU and ICMP

- Maximum and Minimum Packetsize
  - Attn. DSlite
  - Attn. Azure VPN
    https://www.msxfaq.de/cloud/azure/azure_vpn_und_mtu.htm
- Fragmentation
  - Ineffective, should not happen
  - IPv6 no fragmentation!
  - ICMP „Exceeded“ Meldung
- Best Practice
  - Let endpoint negotiate the maximum p
  - ICMP (Typ=3, Code=4) required



Medium	Typ
Ethernet	1492
DSL	1464
Internet DSLite	1472
Freifunk/AzureVPN	1372

MTU – Real customer case

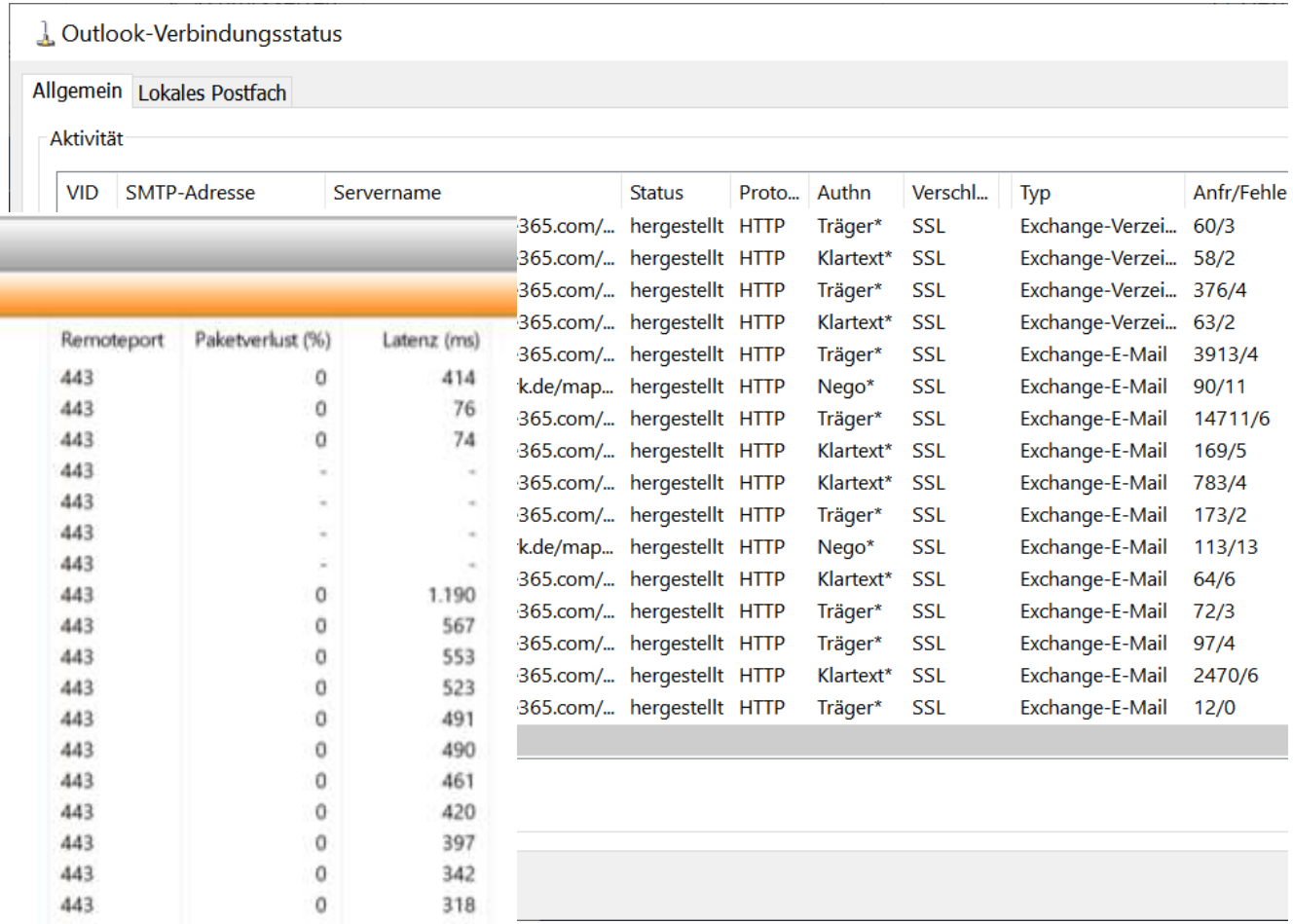


TCP/IP and Ports

You all should know this already – but it is not present, Part 2

Latenz per Connection -> more connections

- Sample Outlook
- Sample Teams



VID	SMTP-Adresse	Servername	Status	Proto...	Authn	Verschl...	Typ	Anfr/Fehle
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-Verzei...	60/3
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-Verzei...	58/2
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-Verzei...	376/4
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-Verzei...	63/2
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	3913/4
		k.de/map...	hergestellt	HTTP	Nego*	SSL	Exchange-E-Mail	90/11
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	14711/6
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-E-Mail	169/5
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-E-Mail	783/4
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	173/2
		k.de/map...	hergestellt	HTTP	Nego*	SSL	Exchange-E-Mail	113/13
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-E-Mail	64/6
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	72/3
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	97/4
		365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-E-Mail	2470/6
		365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-E-Mail	12/0

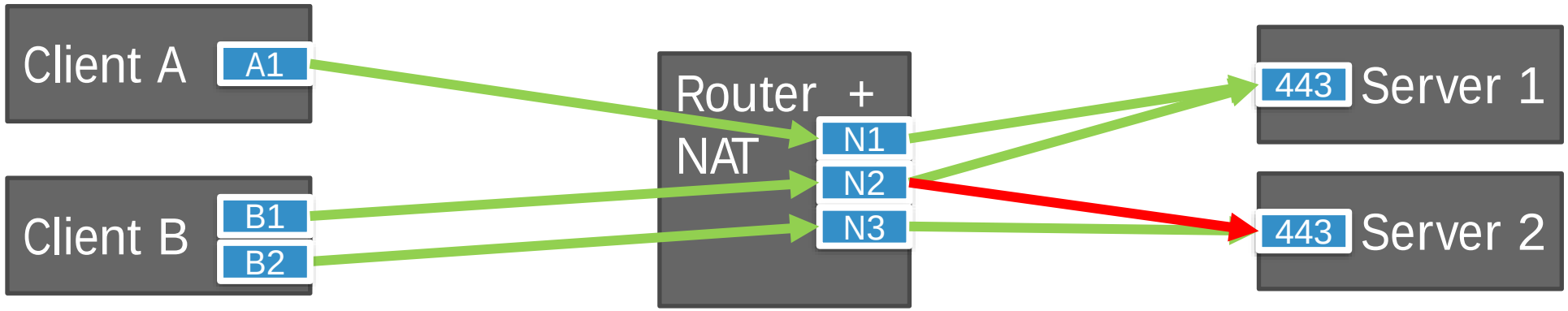
TCP-Verbindungen

Gefiltert von "OUTLOOK.EXE, Teams.exe, Teams.exe"

Prozess	PID	Lokale Adresse	Lokale...	Remoteadresse	Remoteport	Paketverlust (%)	Latenz (ms)
Teams.exe	14412	172.18.241.38	58440	52.114.128.13	443	0	414
Teams.exe	14412	172.18.241.38	58439	52.114.88.46	443	0	76
Teams.exe	13952	172.18.241.38	58447	52.114.74.39	443	0	74
Teams.exe	14412	172.18.241.38	58457	52.178.94.2	443	-	-
Teams.exe	13952	172.18.241.38	58448	52.113.194.131	443	-	-
Teams.exe	14412	172.18.241.38	58435	52.113.194.131	443	-	-
Teams.exe	13952	172.18.241.38	58417	52.114.76.35	443	-	-
OUTLOOK.EXE	22632	172.18.241.38	58520	40.101.12.18	443	0	1.190
OUTLOOK.EXE	22632	172.18.241.38	58519	40.101.12.18	443	0	567
OUTLOOK.EXE	22632	172.18.241.38	58507	40.101.12.18	443	0	553
OUTLOOK.EXE	22632	172.18.241.38	58499	40.101.12.18	443	0	523
OUTLOOK.EXE	22632	172.18.241.38	58517	40.101.12.18	443	0	491
OUTLOOK.EXE	22632	172.18.241.38	58497	40.101.12.18	443	0	490
OUTLOOK.EXE	22632	172.18.241.38	58493	40.101.12.18	443	0	461
OUTLOOK.EXE	22632	172.18.241.38	58506	52.114.76.35	443	0	420
OUTLOOK.EXE	22632	172.18.241.38	58487	40.101.12.18	443	0	397
OUTLOOK.EXE	22632	172.18.241.38	58490	40.101.12.18	443	0	342
OUTLOOK.EXE	22632	172.18.241.38	58485	40.101.12.18	443	0	318
OUTLOOK.EXE	22632	172.18.241.38	58521	40.101.12.18	443	0	301
OUTLOOK.EXE	22632	172.18.241.38	58510	40.101.12.18	443	0	272
OUTLOOK.EXE	22632	172.18.241.38	58503	40.101.12.18	443	0	188
OUTLOOK.EXE	22632	172.18.241.38	58486	40.101.12.18	443	0	186
OUTLOOK.EXE	22632	172.18.241.38	58501	40.101.12.18	443	0	182

Private adresses and public ports

- We need a translation from private IP to internet services
  - NAT-Device or HTTP-Proxy

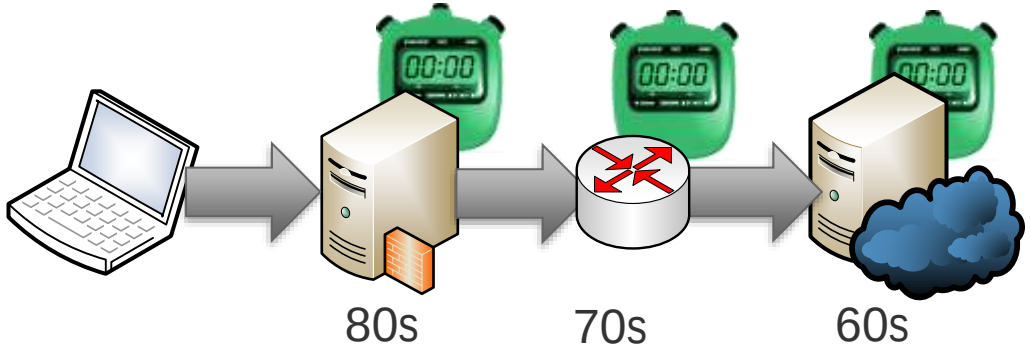


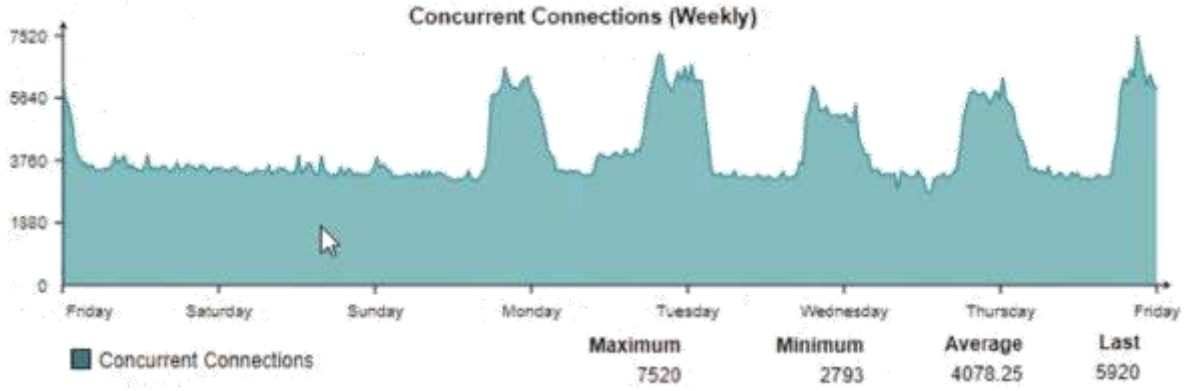
- Questions
  - How many outgoing connections per IP-Address?
  - How many connections are „typical“ per client ?
- Microsoft estimation
  - 6 ports/client + 4 ports „peak“ = 10 ports/client
  - 64000 Ports per NAT-Device – 4000 reserved = 60.000 Ports for Clients

NAT support with Office 365 https://docs.microsoft.com/en-us/microsoft-365/enterprise/nat-support-with-microsoft-365

Session Timeout / Keepalive

- Clients are not friendly
  - Client looses WLAN-Connection
  - Client removed from the docking unit
  - NAT-Session stays active for how long ?
- TCP Session Timeout
  - Min 120 Seconds. Not shorter
  - „Long running connections“
  - HTTP-Chunked-connections
- Action: Monitor connections





TCP keep-alives can be sent once every KeepAliveTime (defaults to 7,200,000 milliseconds or two hours) if no other data or higher-level keep-alives have been carried over the TCP connection.
https://blogs.technet.microsoft.com/nettracer/2010/06/03/things-that-you-may-want-to-know-about-tcp-keepalives/
https://www.msxfaq.de/netzwerk/grundlagen/tcp_session_timeout.htm
https://blogs.technet.microsoft.com/onthewire/2014/03/04/network-perimeters-tcp-idle-session-settings-for-outlook-on-office-365/

Teams realtime traffic protocol (RTP)

Audio and Video with Teams

- Audiostream
  - 20ms „audio“ per packet (2st hop Latency!)
  - 50 packets/sec
  - About 160Byte payload (64kbit)
  - 100kbit/Sec continuous stream
- Preferred protocol: UDP!
  - Ask your firewall guys!
- Max Latency: 100ms
- Packetloss and RTP

Firewall and proxy requirements

Microsoft Teams connects to Microsoft Online Services and needs internet connectivity for this. For Teams to function correctly, you must open TCP ports 80 and 443 from the clients to the internet, and UDP ports 3478 through 3481 from the clients to the internet. The TCP ports are used to connect to web-based content such as SharePoint Online, Exchange Online, and the Teams Chat services. Plug-ins and connectors also connect over these TCP ports. The four UDP ports are used for media such as audio and video, to ensure they flow correctly.

Opening these ports is essential for a reliable Teams deployment. Blocking these ports is unsupported and will have an effect on media quality.

Source: https://docs.microsoft.com/en-us/microsoftteams/3-envision-evaluate-my-environment#firewall-and-proxy-requirements

Teams RTP requirements

- Latency, Loss

Metric	Edge	Client
Latency (one way)	< 30ms	< 50ms
Latency (RTT)	< 60ms	< 100ms
Burst packet loss	<1% during any 200 ms interval	<10% during any 200ms interval
Packet loss	<0.1% during any 15s interval	<1% during any 15s interval
Packet inter-arrival Jitter	<15ms during any 15s interval	<30ms during any 15s interval
Packet reorder	<0.01% out-of-order packets	<0.05% out-of-order packets

https://docs.microsoft.com/de-de/skypeforbusiness/optimizing-your-network/media-quality-and-network-connectivity-performance#network-performance-requirements-from-your-network-edge-to-microsoft-network-edge

- Run the network latency analytics tool .
- Ping the Google Meet media front-end server for at least

```
> ping lens.l.google.com
PING lens.l.google.com (74.125.143.127): 56 dat
64 bytes from 74.125.143.127: icmp_seq=0 ttl=47
64 bytes from 74.125.143.127: icmp_seq=1 ttl=47
64 bytes from 74.125.143.127: icmp_seq=2 ttl=47
64 bytes from 74.125.143.127: icmp_seq=3 ttl=47
64 bytes from 74.125.143.127: icmp_seq=4 ttl=47
```

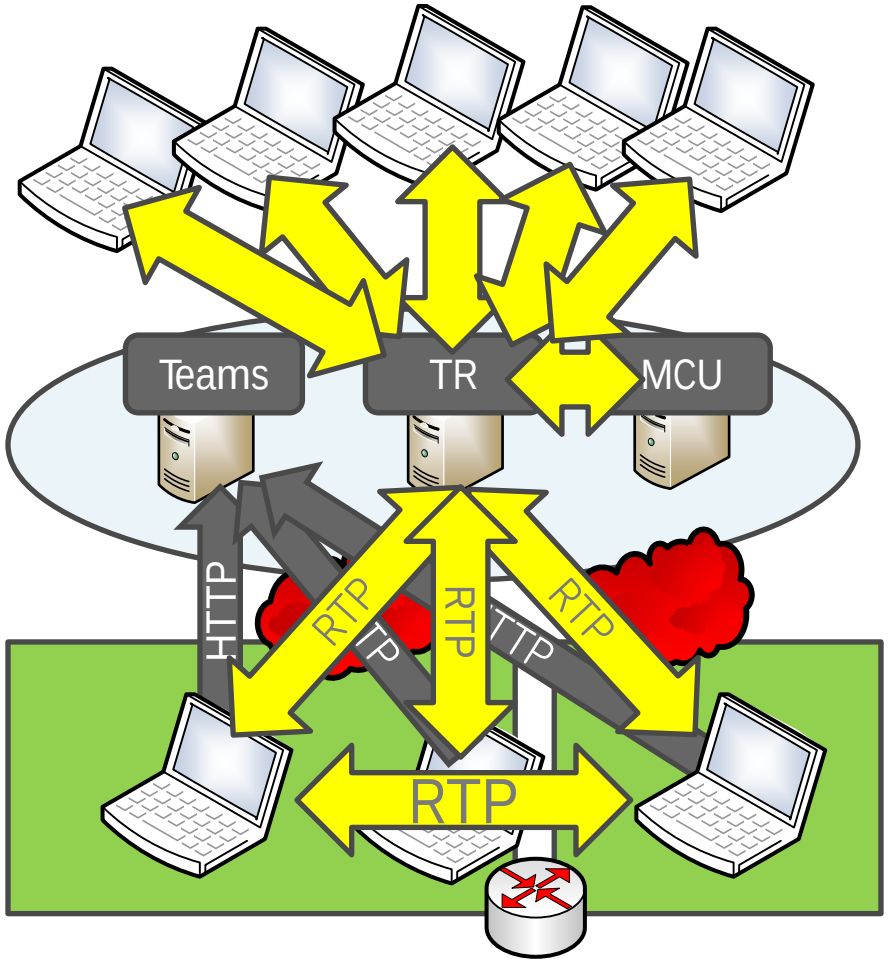
Make sure your latency is consistent at 100 ms or less. Don't average the values because it can hide spikes and intermediate latency problems.

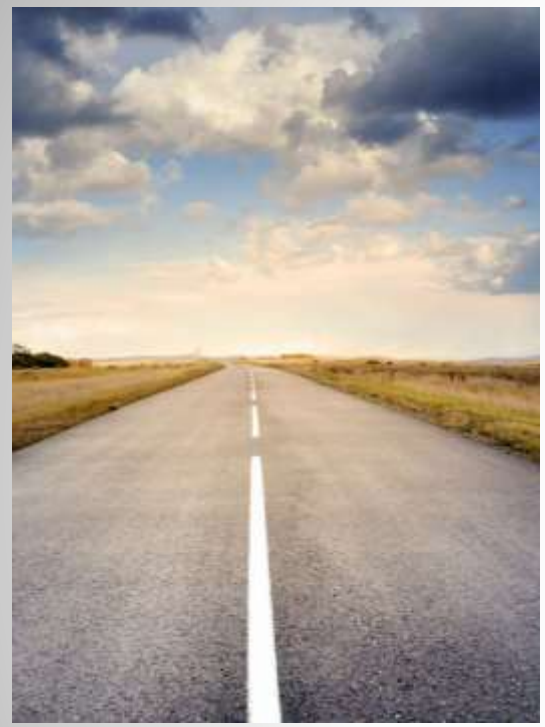
If your latency is not 100 ms or less, use the traceroute utility to print out the network path from your current machine to the Meet media front-end. This path should be as short as possible, for example:

Source:https://support.google.com/a/answer/7582554?hl=en#zippy=%2Cmeasure-latency

Teams and Media

- 1:1 is easy
  - Direct UDP
  - Transport Relay
- Meeting uses MCU
  - Always using the transport Relay
  - „central Mixer“ is online
- Homeschooling
  - 1 teacher talking
  - nn students listening



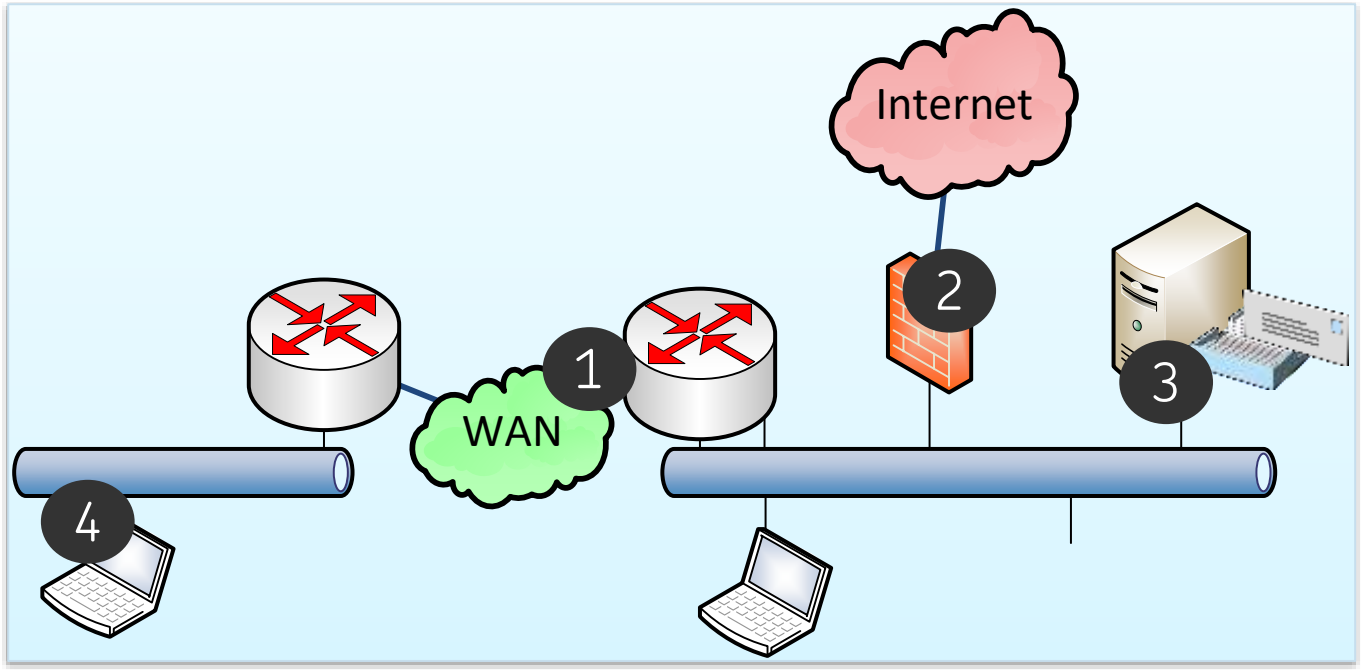


From my firewall to Microsoft 365

https://pixabay.com/photos/road-pavement-landscape-roadway-220058/

Local monitoring

1. **Own WAN network**
   - Bandwidth via SNMP
   - NetFlow for details
2. **Internet**
   - Bandwidth via SNMP
   - Proxylogs/URL-Logs
3. **Server**
   - Perfmon
   - IIS-Logs
   - Eventlog
4. **Client Performance**
   - Rare, most not used

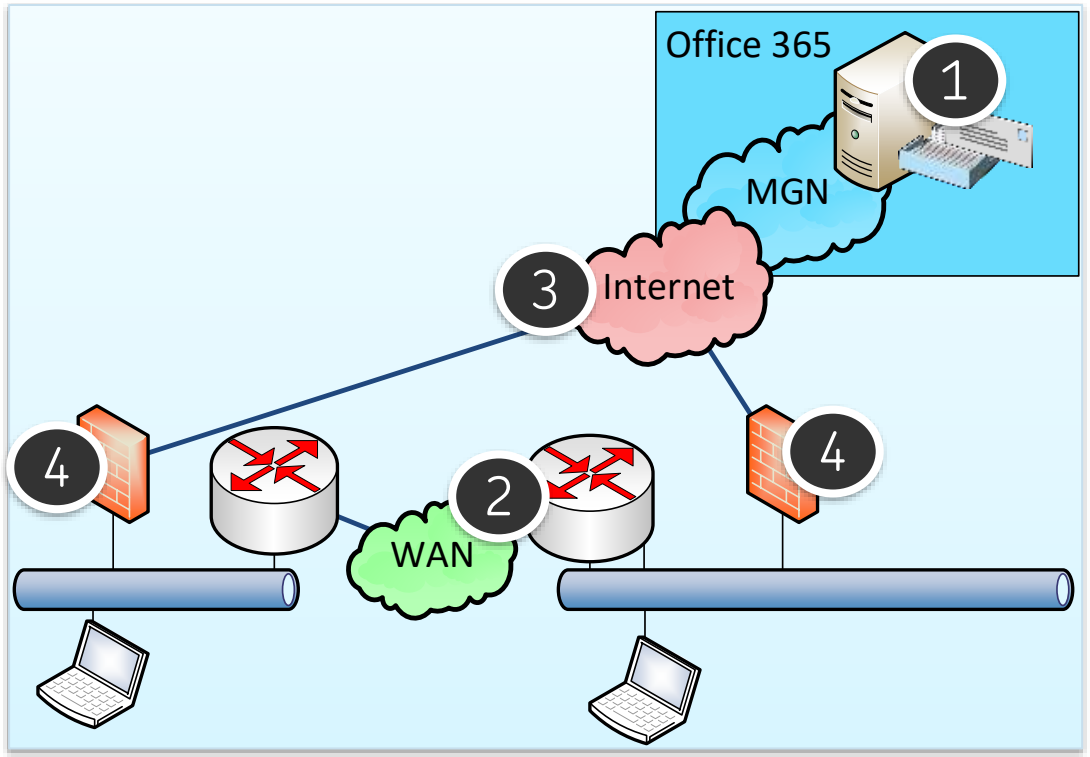


Everything under control?

Performance Monitoring with Cloud services

1. Service are „outside“
   - Managed by Microsoft
2. No relevant local traffic
   - Local breakout
   - bypass own WAN
3. No details from ISP
4. More „Internet Traffic“

Adjust your existing monitoring!



Measure cloud performance, latency etc.

Common mistakes

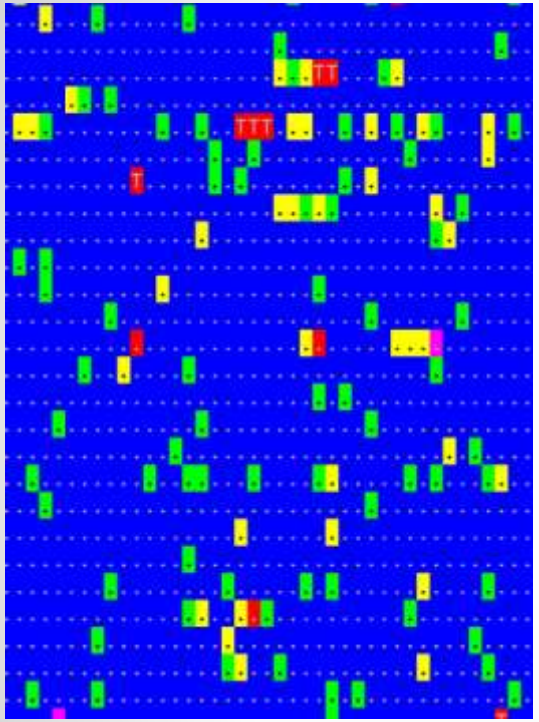
- Latency vs. Bandwidth
  - 80% saturated line is not bad
  - If the latency is still low
  - High latency = not enough bandwidth „somewhere“
- Interval Seconds vs. Minutes
  - Don‘t measure a line every minute
  - You cannot „see“ RTP-Problems
- Average vs. Percentil
  - Do not measure averages
  - You cannot see spikes or high jitter
  - Think about percentil

What is Percentil?

- Think about a pizza service
  - „Expected average delivery Time is 10 minutes“
  - 50% withing 5 minutes and hot
  - 50% withing 15 minutes and cold
  - -> 50% unhappy customers
- „Average“ is the wrong approach
  - No distribution, no bursts
- Better
  - 95% of the pizzas are „hot enough“
  - max. 5% unsatisfied customers
- „Percentil“
  - Based on the requirements

Google: “Make sure your latency is consistent at 100ms or less. Don't average the values because it can hide spikes and intermediate latency problems.”
Quelle:
https://support.google.com/a/answer/7582554

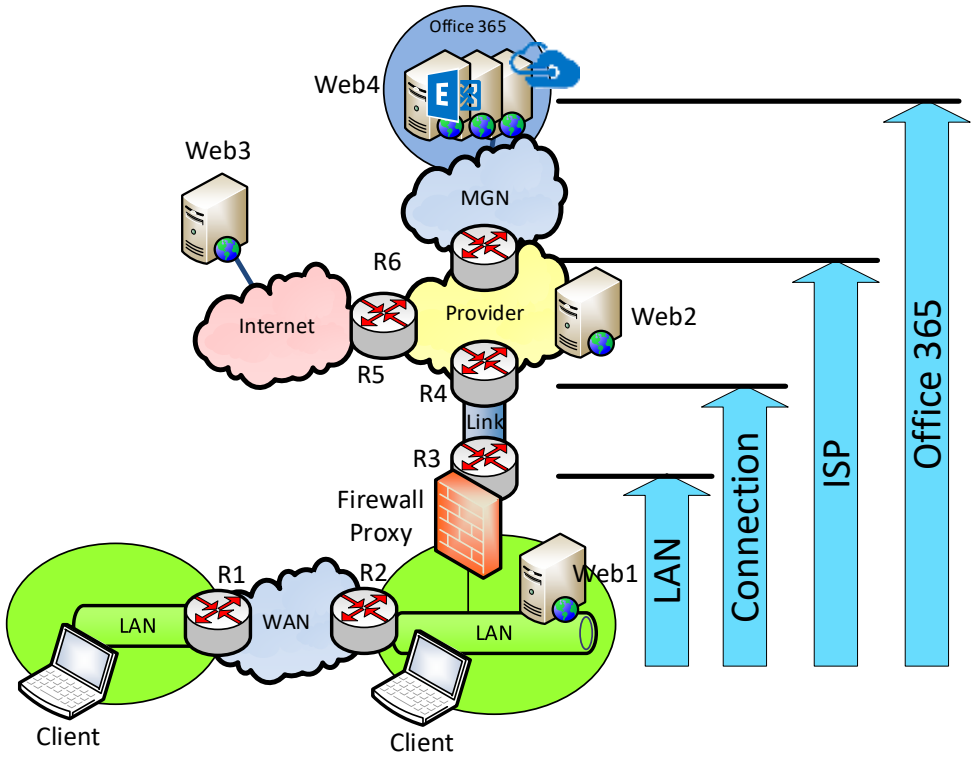
Bild: https://pixabay.com/vectors/cook-boy-kid-pizza-holding-1773658/



End2End-Scripts and Samples

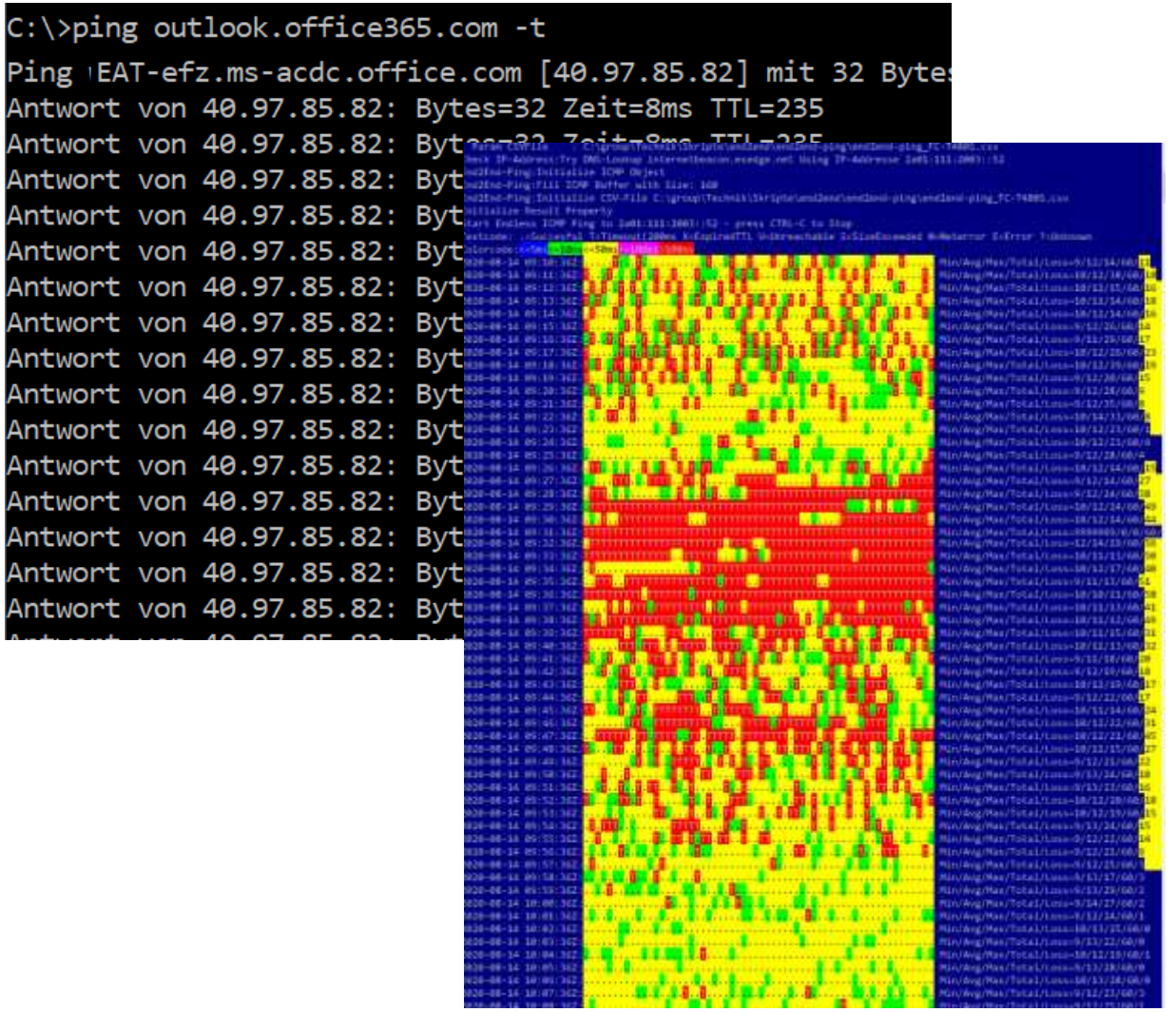
Remote endpoints

- Intermediate Systems
  - Routers
- Microsoft 365 –Services
  - Exchange Online
  - Teams Transport Relay
  - SharePoint
  - …
- Other Cloud Dienste
  - Facebook, Twitter, Google, ….
- Own Services
  - Default Gateway, VPN-Server, RDP-Gateway, Company Portal,…



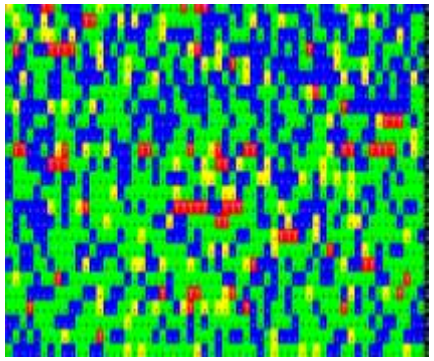
End2End-Ping

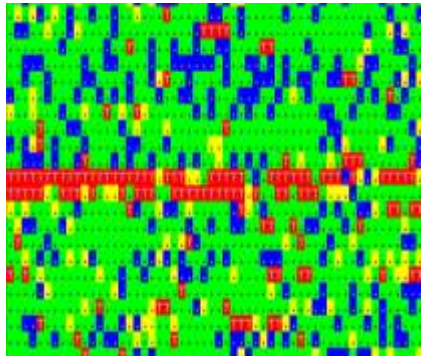
- Send simple ICMP-Ping/sec
  - small 32 Byte Payload
  - Larger packets = higher latency
- Keep in mind
  - No QoS-Tagging
  - ICMP-DoS Protection
  - „Optimized“ by Riverbed etc.
  - Provider may spoof ICMP
- Widely available
- End2end-Ping
  - Simple Powershell Script
  - ASCII-Art works



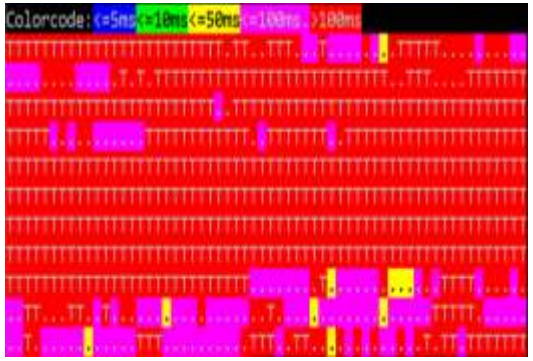
Samples: End2End-Ping

Bellevue Hotel 11:00pm/07:00am

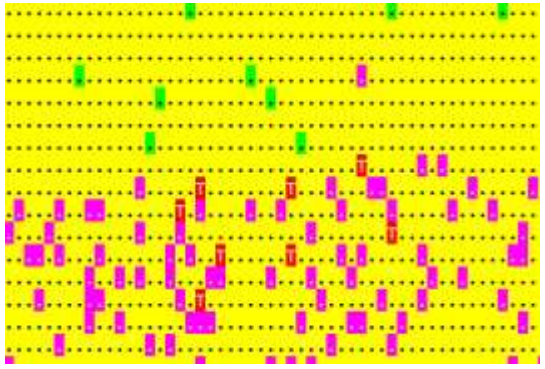




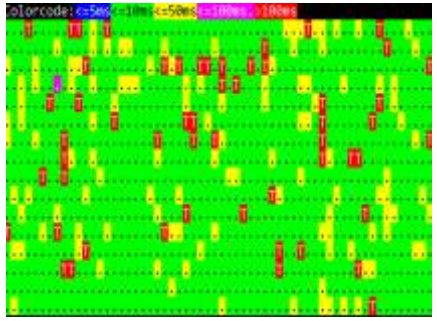
WifiOnICE

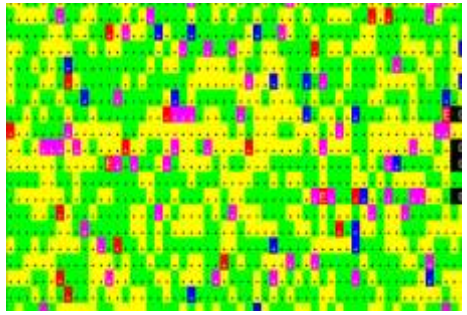


Home DSL 16/1

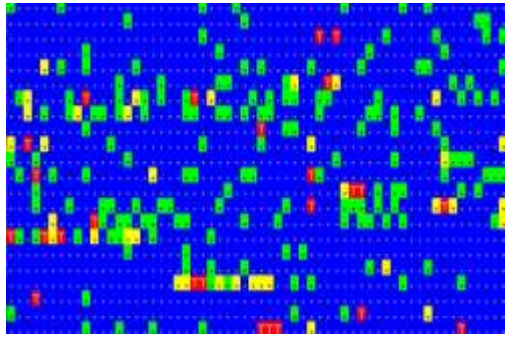


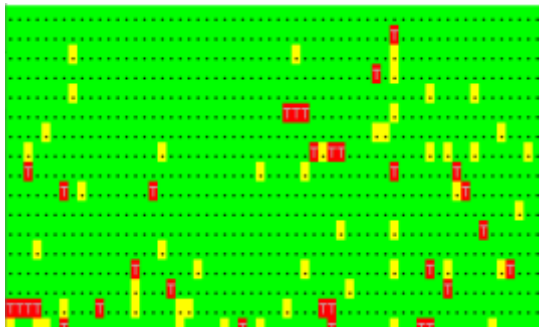
Hotel Frankfurt 01:00am, 07:00





MSTFGuest (Internet / Office365)





Checking HTTP

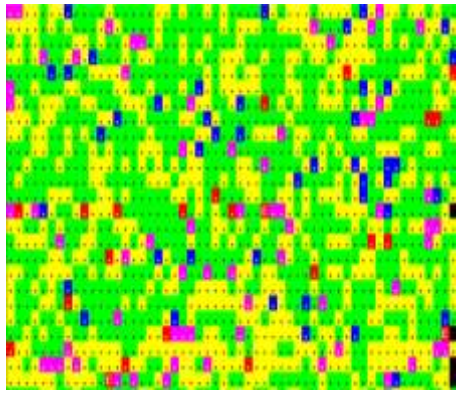
- We need a remote „valid“ endpoint.
  - No authentication
  - No Throttling

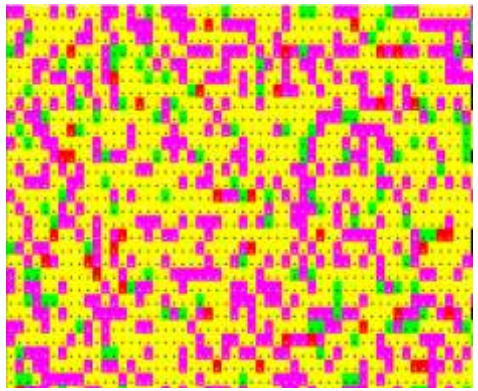
Bereich	URL	Size
Exchange	https://outlook.office365.com/owa/favicon.ico	7886 Bytes
Exchange	https://outlook.office365.com/owa/smime/owasmime.msi	729088 Bytes
OneDrive	https://<tenant>-my.sharepoint.com/	193 Bytes
SharePoint	https://<tenant>.sharepoint.com/	190 Bytes
SharePoint	https://<tenant>.sharepoint.com/_layouts/15/SPAndroidAppManifest.aspx	308 Bytes
EvoSTS	https://login.microsoftonline.com/common/oauth2/authorize	138361 Bytes

- Easy to test (Invoke-WebRequest)
  - Parameter -UseBasicParsing and –MaxRedirects 0
  - Disable processindicator `$ProgressPreference="SilentlyContinue“`
  - Use Method HEAD instead of GET (smaller Paket)

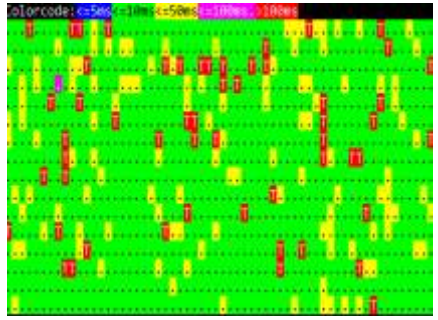
End2End-http: favicon.ico

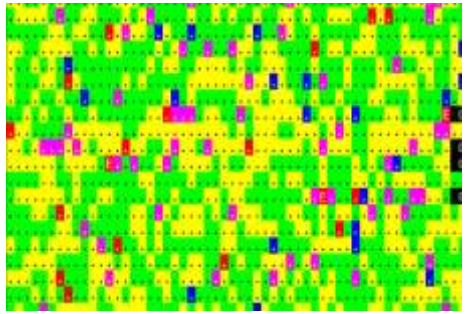
Frankfurt Hotel 01:00am/07:00am



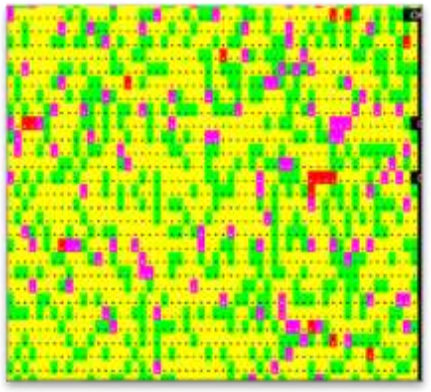


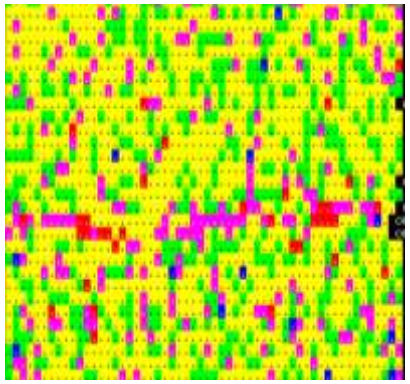
Compare to ICMP



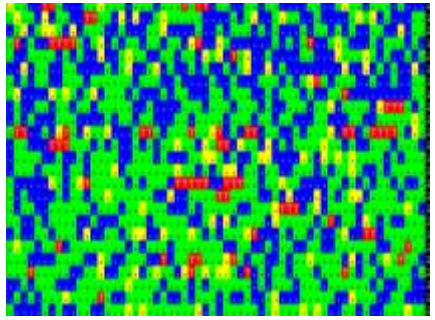


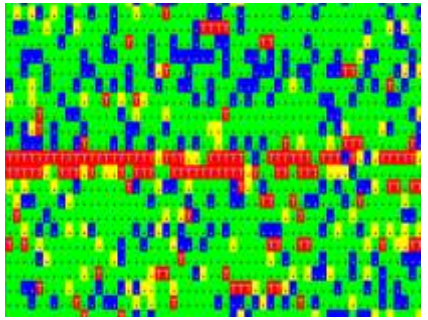
Bellevue Hotel 01:00am / 07:00p





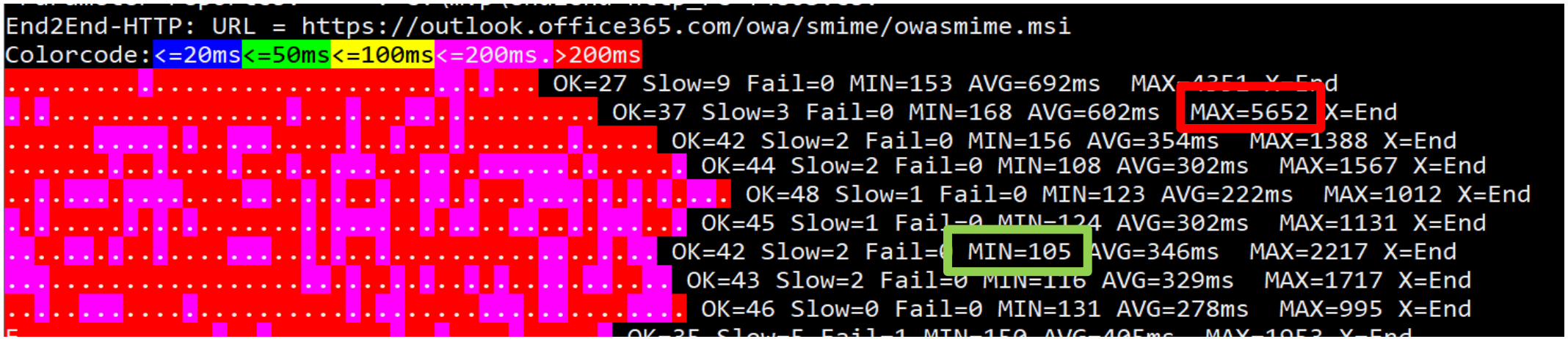
Compare to ICMP





End2end-http with 700k-file

- 700kByte in 105ms = ca. 66 Mbit !
- 700kByte in 5652 sec = ca. 1,3 Mbit
  - Packetloss? Parallel PING?
- Color coding not optimal
- Looks like a DoS



HTTP and Exchange

Response Headers

HTTP/1.1 200 OK

Cache

Cache-Control: private
Date: Mon, 18 Mar 2019 12:22:08 GMT
Vary: Accept-Encoding

Cookies / Login

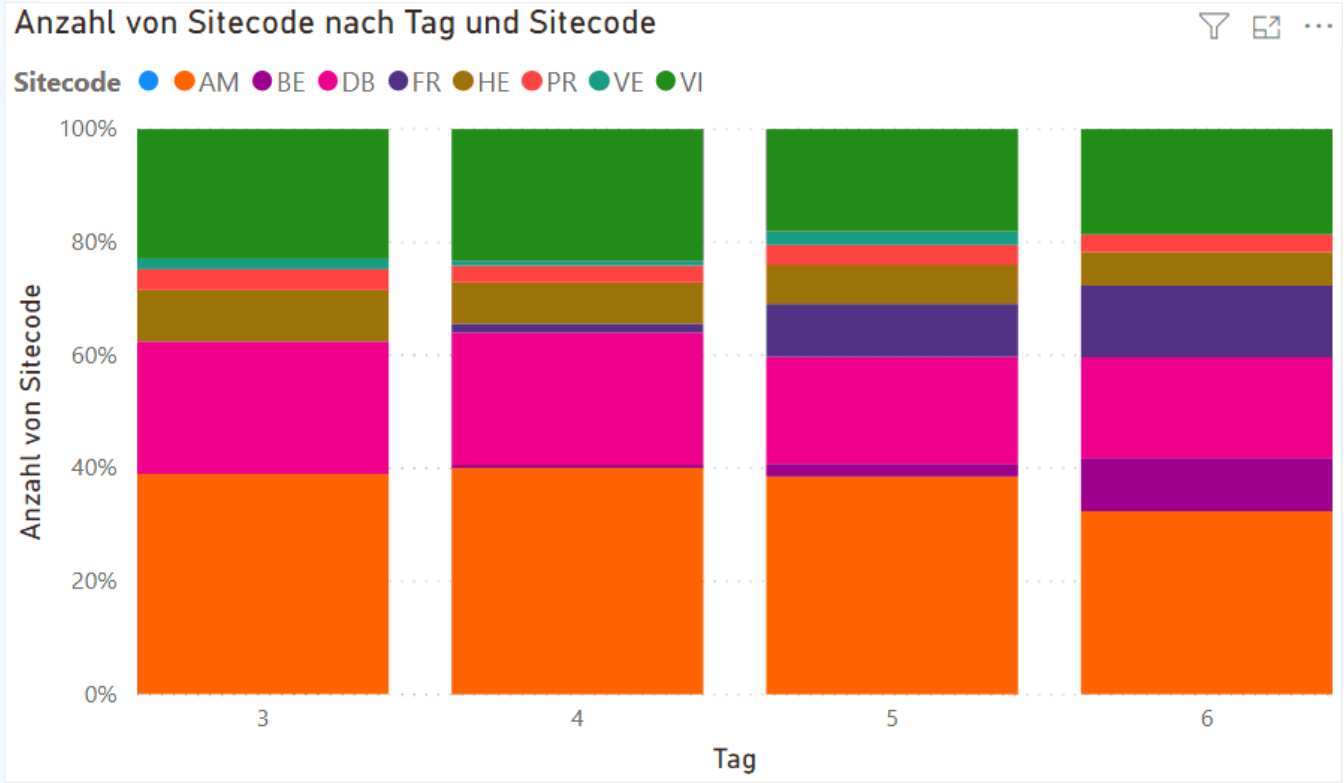
Set-Cookie: exchangecookie=ff2d2bfb560141d3a294a087ecc2b87e; path=/

Entity

Content-Length: 3547
Content-Type: text/xml; charset=utf-8

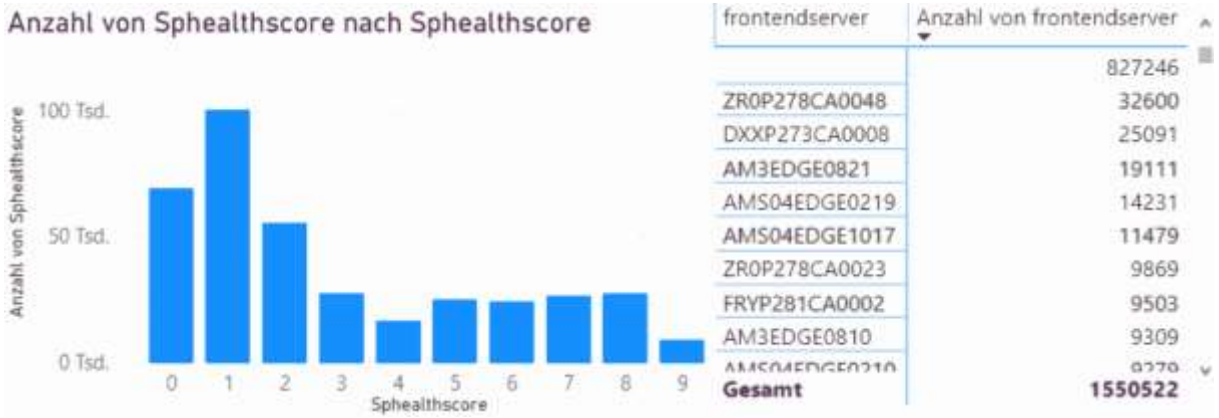
Miscellaneous

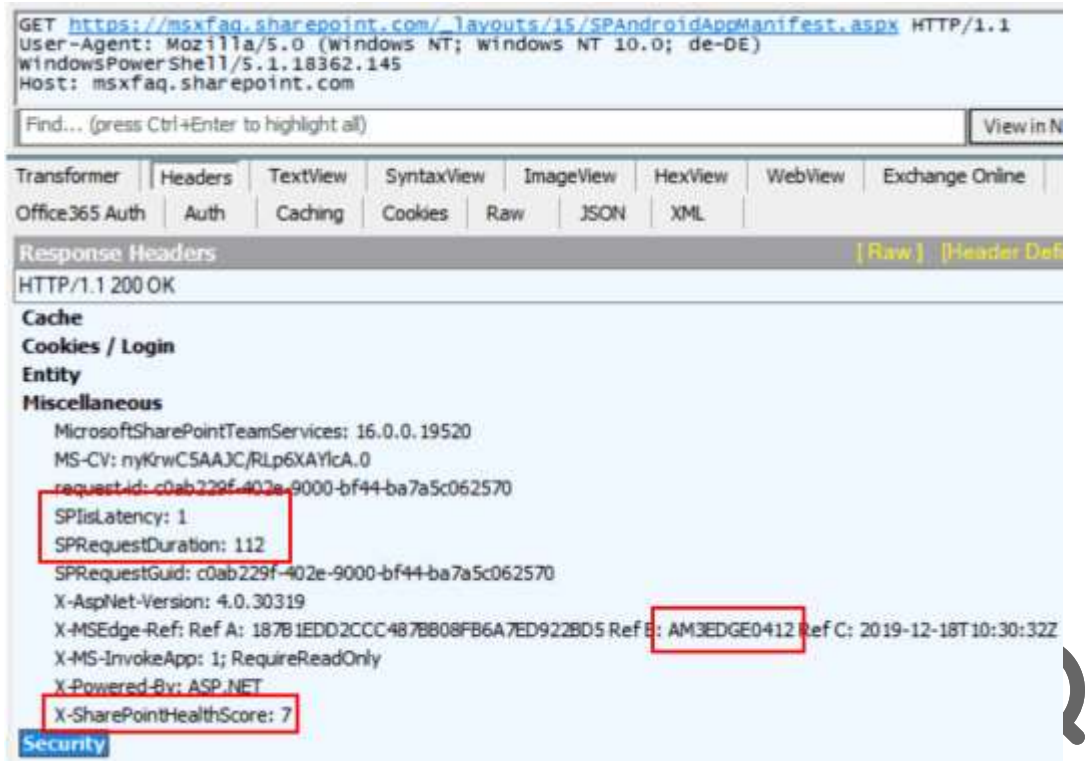
request-id: ab475c60-41d4-44d5-bd68-38c8804ba5e0
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-BackEndHttpStatus: 200
X-BackEndHttpStatus: 200
X-BEServer: AM6PR04MB5013
X-BeSku: WCS5
X-CalculatedBETarget: AM6PR04MB5013.eurprd04.prod.outlook.com
X-CalculatedFETarget: AM6PR0402CU001.internal.outlook.com
X-DiagInfo: AM6PR04MB5013
x-EwsHandler: FindItem
X-FEProxyInfo: AM6PR0402CA0034.EURPRD04.PROD.OUTLOOK.COM
X-FEServer: AM6PR0402CA0034
X-FEServer: MWHPR2201CA0074
X-RUM-Validated: 1



SharePoint Online

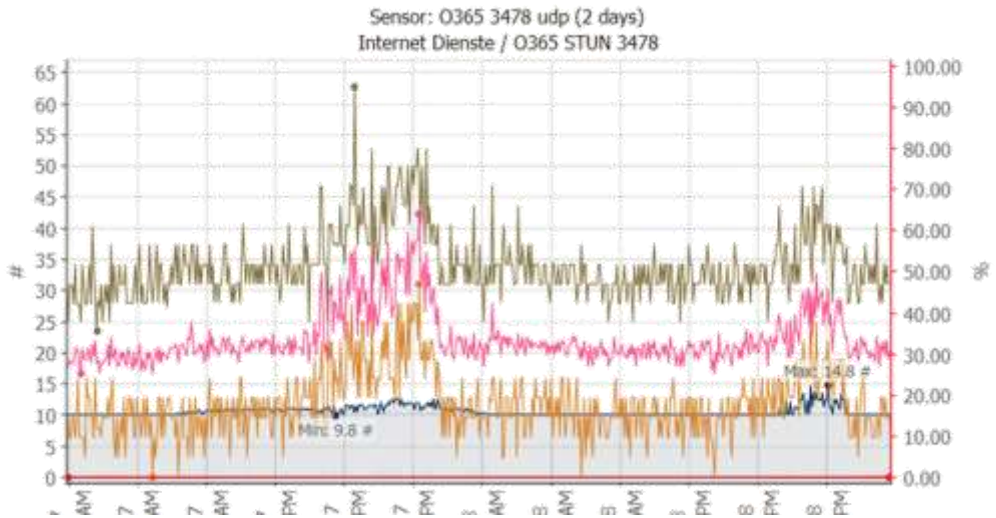
- URL
  - <tenantname>.sharepoint.com
  - <tenantname>-my.sharepoint.com
  - File: /_layouts/15/SPAndroidAppManifest.aspx).headers
- End2End-HTTP
  - Measure frontdoor access
  - Get „HealthScore“





Sample: End2End-UDP3478

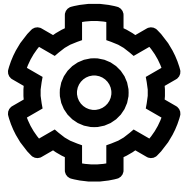
- Connect to UDP-port 3478
- Collect Endpoint name
- Measure Latency
- Measure Hop-Count



Auswählen End2End-UDP3478

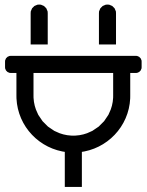
```
PS C:\End2End> .\end2end-udp3478.ps1
End2End-UDP3467:Start
  Mode               : END2END. continuous latency check and no distance check
  MaxTTL             : 128
  MaxRetries         : 0
  AvgIntervalSec     : 60
  InterpacketsleepMS : 20
  Sleeptime          : 0
  prtgpushurl        :
  TURN-Server        : Use Office 365 Microsoft Teams Server: IP=52.113.193.5
End2End-UDP3478:Start UDP-Client on 50019
End2End-UDP3478:Connect UDPClient to 52.113.193.5:3478
Colorcode:<=100ms<=200ms>200ms
Legend: 100 pakets max: . = max<100ms  W= max<200ms  E=max>200ms
End2End-UDP3478:Keyboard: use X=End  P=Pause
2020-10-14 00:10:16Z:RTT:..........(Min/Avg/Max):013/016/039 Total/Fail:1218/000
2020-10-14 00:11:16Z:RTT:..........(Min/Avg/Max):014/016/028 Total/Fail:1215/000
2020-10-14 00:12:16Z:RTT:..........(Min/Avg/Max):013/016/048 Total/Fail:1169/000
2020-10-14 00:13:16Z:RTT:..........(Min/Avg/Max):014/016/055 Total/Fail:1183/000
2020-10-14 00:14:16Z:RTT:..........(Min/Avg/Max):014/016/041 Total/Fail:1184/000
2020-10-14 00:15:16Z:RTT:..........(Min/Avg/Max):014/016/020 Total/Fail:1203/000
2020-10-14 00:16:16Z:RTT:..........E(Min/Avg/Max):013/016/037 Total/Fail:1186/001
2020-10-14 00:17:16Z:RTT:..........(Min/Avg/Max):013/016/049 Total/Fail:1182/000
2020-10-14 00:18:16Z:RTT:..........(Min/Avg/Max):014/016/020 Total/Fail:1211/000
2020-10-14 00:19:16Z:RTT:..........(Min/Avg/Max):013/016/019 Total/Fail:1188/000
2020-10-14 00:20:17Z:RTT:..........(Min/Avg/Max):013/016/019 Total/Fail:1205/000
2020-10-14 00:21:17Z:RTT:..........(Min/Avg/Max):014/016/019 Total/Fail:1202/000
2020-10-14 00:22:17Z:RTT:..........(Min/Avg/Max):013/016/033 Total/Fail:1196/000
2020-10-14 00:23:17Z:RTT:..........(Min/Avg/Max):014/016/020 Total/Fail:1192/000
2020-10-14 00:24:17Z:RTT:..........(Min/Avg/Max):014/016/019 Total/Fail:1189/000
2020-10-14 00:25:17Z:RTT:..........(Min/Avg/Max):013/016/023 Total/Fail:1179/000
2020-10-14 00:26:17Z:RTT:..........(Min/Avg/Max):014/016/026 Total/Fail:1169/000
2020-10-14 00:27:17Z:RTT:..........(Min/Avg/Max):013/016/028 Total/Fail:1206/000
2020-10-14 00:28:17Z:RTT:...E......(Min/Avg/Max):013/017/047 Total/Fail:1179/001
2020-10-14 00:29:17Z:RTT:.....E....(Min/Avg/Max):014/017/054 Total/Fail:1162/001
2020-10-14 00:30:17Z:RTT:..........(Min/Avg/Max):013/017/045 Total/Fail:1179/000
2020-10-14 00:31:17Z:RTT:..........(Min/Avg/Max):014/017/049 Total/Fail:1181/000
```

Missing: Connection advisor on every client



Configuration

- LAN/WLAN, Network boards, Default Gateway, Routing
- DNS-Server, Proxy-Server
- Operating System, Patchlevel, „Teams-Version“, ...



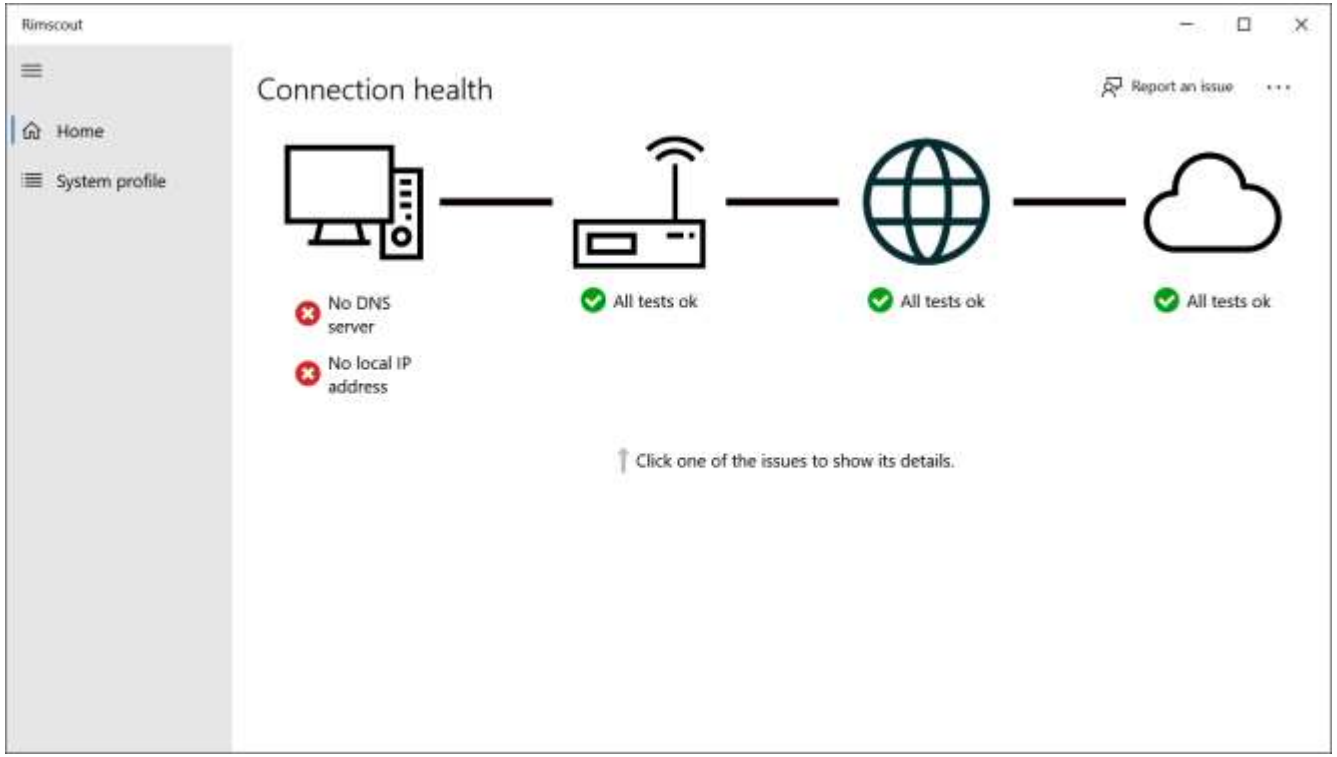
Connectivity

- Are all Services „reachable“ ? (ICMP, DNS, UDP, TCP, HTTP)
- Especially Microsoft 365 services (Exchange, SharePoint, Teams, ...
- Other Cloud Services (Yes, they are also in use)
- Own services like VPN-Servers, Terminal Services gateways, ...

Durability

- Bandbreite vs. Latenzzeit, Packetloss, Jitter, Thoughput
- Whats visible for the end user
- How reliable is that connection

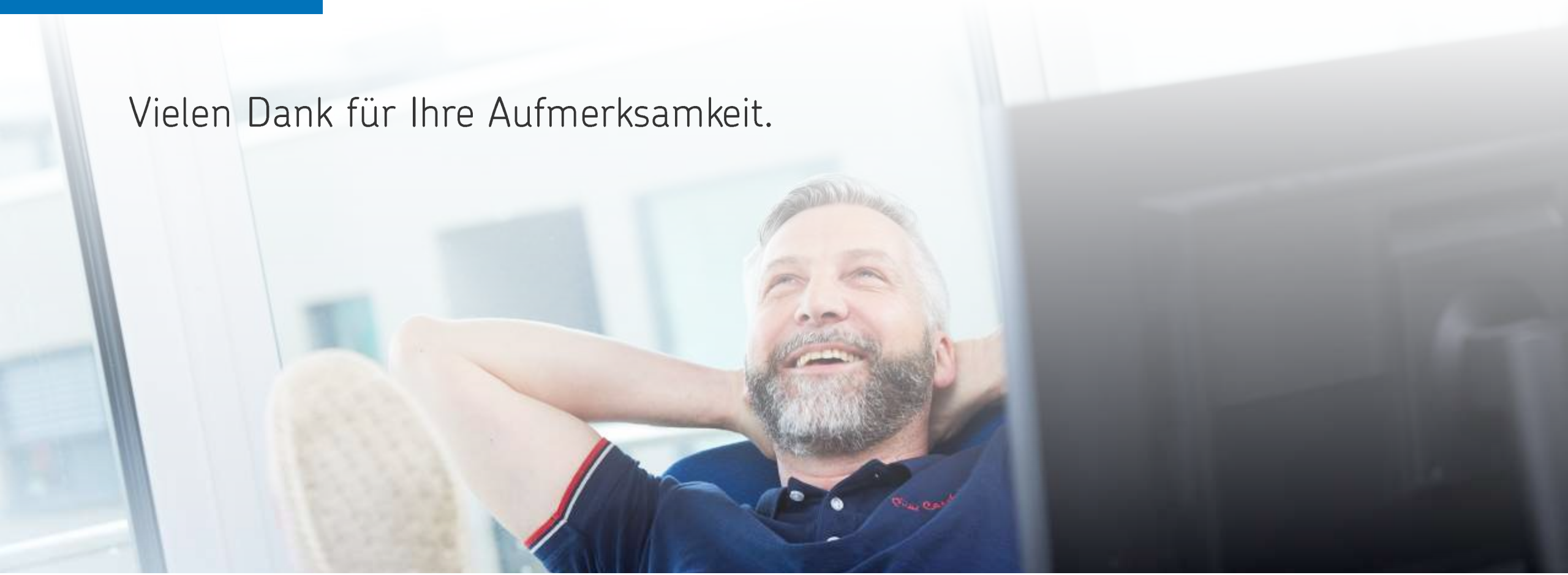
Tools



- PowerShell End2End-Scripts
- Network tools
  - Cisco IP-SLA, HP-NQA, UDP-Mirrors, PRTG
- On every Desktop
  - Configuration Check
  - Connection Check
  - Stability Check

Rimscout: Sample Reports

Vielen Dank für Ihre Aufmerksamkeit.



Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
Frank.carius@netatwork.de

Building IT-Excellence.

www.netatwork.de