



How to build a proper connection to cloud services

Frank Carius frank.carius@netatwork.de



About Me



Frank Carius

Enterprise Architect & Partner

Net at Work GmbH

 @msxfaq

 <https://www.linkedin.com/in/frankcarius>

<https://www.msxfaq.de>



Think about trucks ...

- You are a gatekeeper at a factory exit and....
 - ... you count the truck in/out
 - ... you weight the trucks

Thats SNMP-Monitoring today!

- SNMP means
 - Measure packets/sec in/out
 - Measure 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

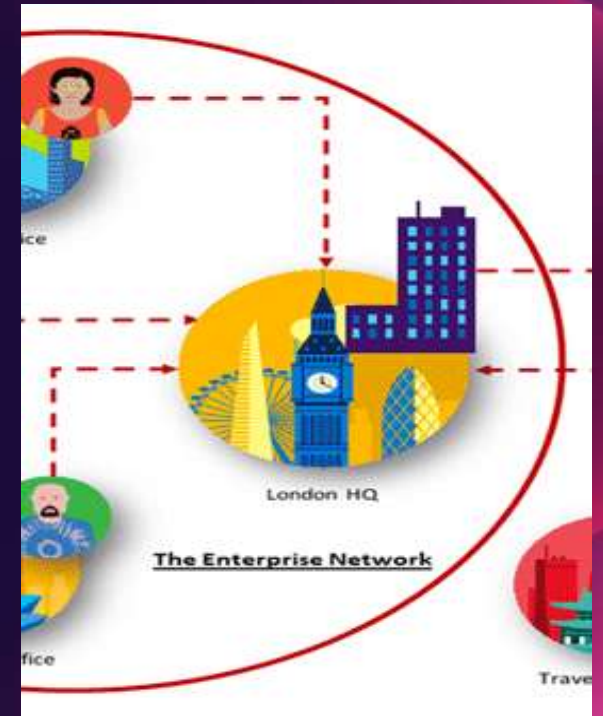


Challenges - Network Evolution

- 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 traffic, vpnbypass)
 - 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



Office 365 Guiding Principles

Identify and differentiate Office 365 traffic using Microsoft published endpoints

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

Office 365 URLs and IP address ranges

Updated: 11/20/2017

Summary - The following endpoints (FQDNs, Ports, URIs, IPV4, and IPv6) published apply to Office 365 plans, including Government Community Cloud (GCC) and are designed to deliver productivity services to organizations using only these plans.

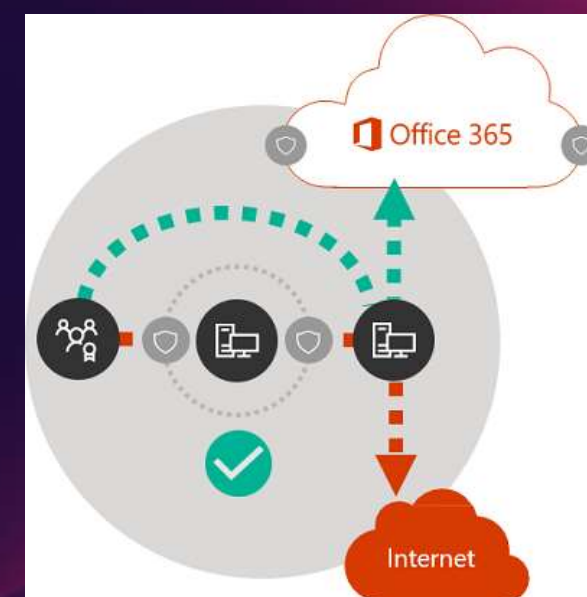
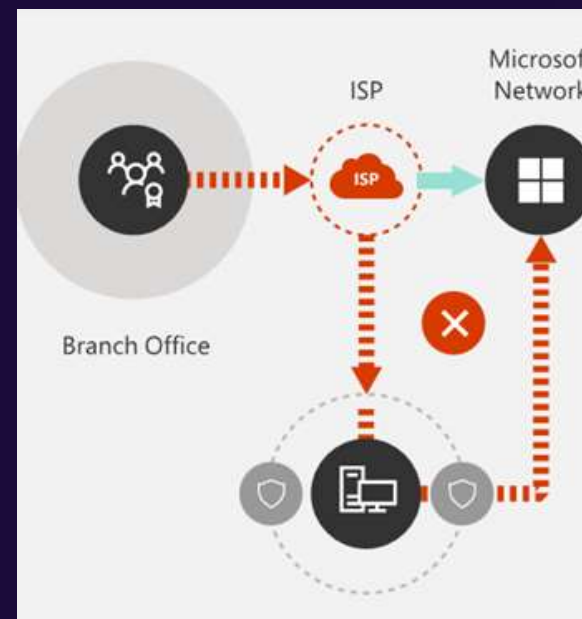
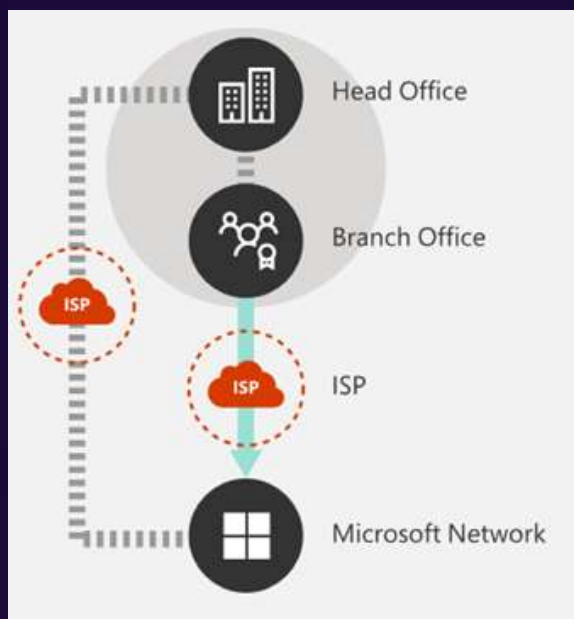
Office 365 endpoints worldwide (including GCC) | Office 365 endpoints by IP range | Office 365 Germany | Office 365 U.S. Government Defense/DoD | Office 365 U.S. Government Defense/Armed |

Last updated: 11/20/2017 [Change log subscription](#) [Download: the full list in CSV format](#)

Office 365 requires **direct connectivity** from every computer connecting to the service. This article serves as a reference for the specific Microsoft and third-party endpoints computers need to be able to reach. Start with our guide [managing Office 365 endpoints](#) to understand how best to use the information here. Google for emergency changes; endpoints are updated at the end of each month.

Important: Endpoints may be listed as an IP address only, FQDN/URI only, or a combination of the two. Some endpoints are shared with Office 365 and some are shared with consumer services. Pay attention to the introduction for each service, specific guidance that applies only to that service will be included there. Office 365 supports on-premise based services such as Microsoft second cloud services with dynamic addressing, Domain Name Services (DNS), Content Delivery Networks (CDN), Certificate Revocation Lists (CRL), and other services.

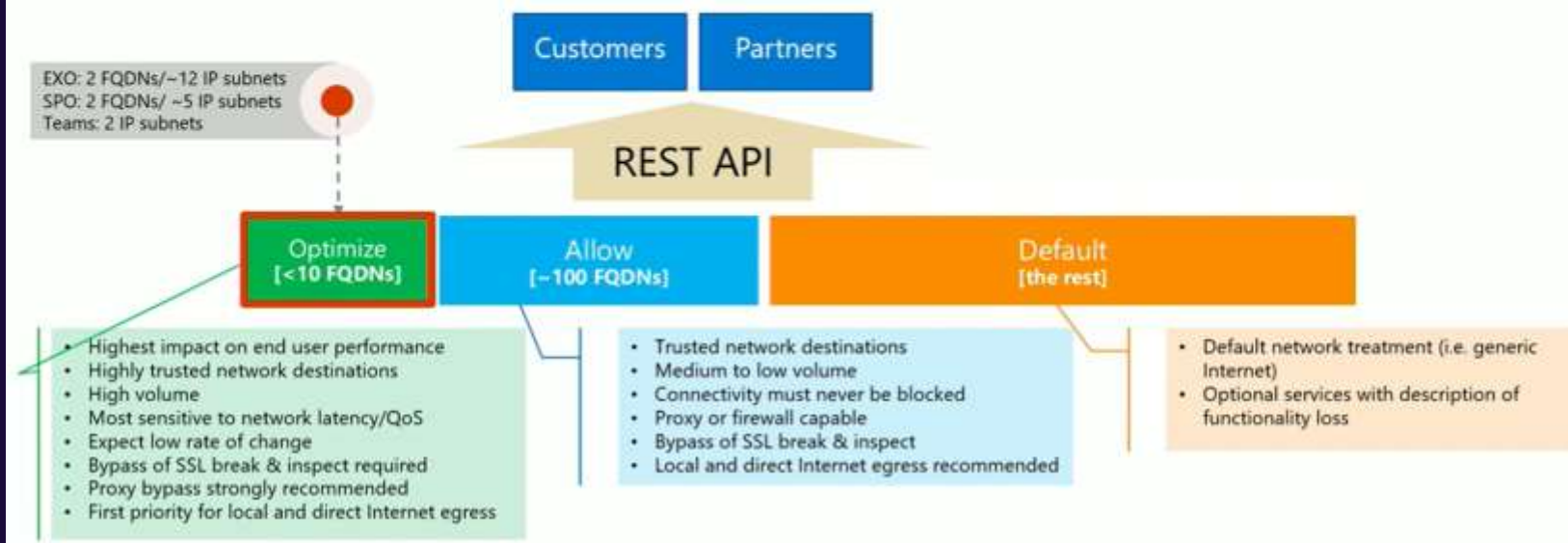
aka.ms/o365ip



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)



More Microsoft Links

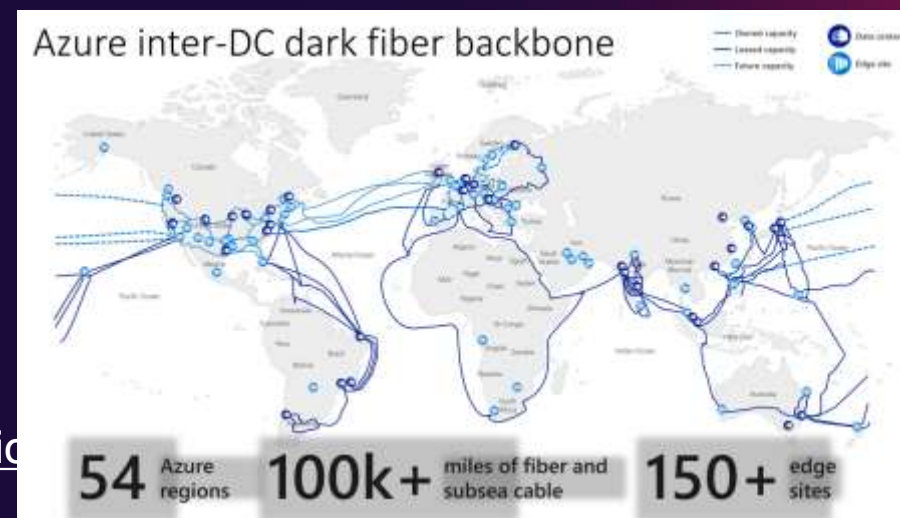
- Office 365 Connectivity Principles in greater detail
<https://aka.ms/PNC>
<https://techcommunity.microsoft.com/t5/Office-365-Blog/Getting-the-best-connectivity-and-performance-in-Office-365/ba-p/124694>
- Office 365 product group videos expanding on the Office 365 connectivity principles:
Strategy: <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 network
<https://techcommunity.microsoft.com/t5/Microsoft-Tech-Summit-Content-17/Understanding-optimizing-amp-securing-enterprise-network/td-p/126371>

Microsoft Global Network

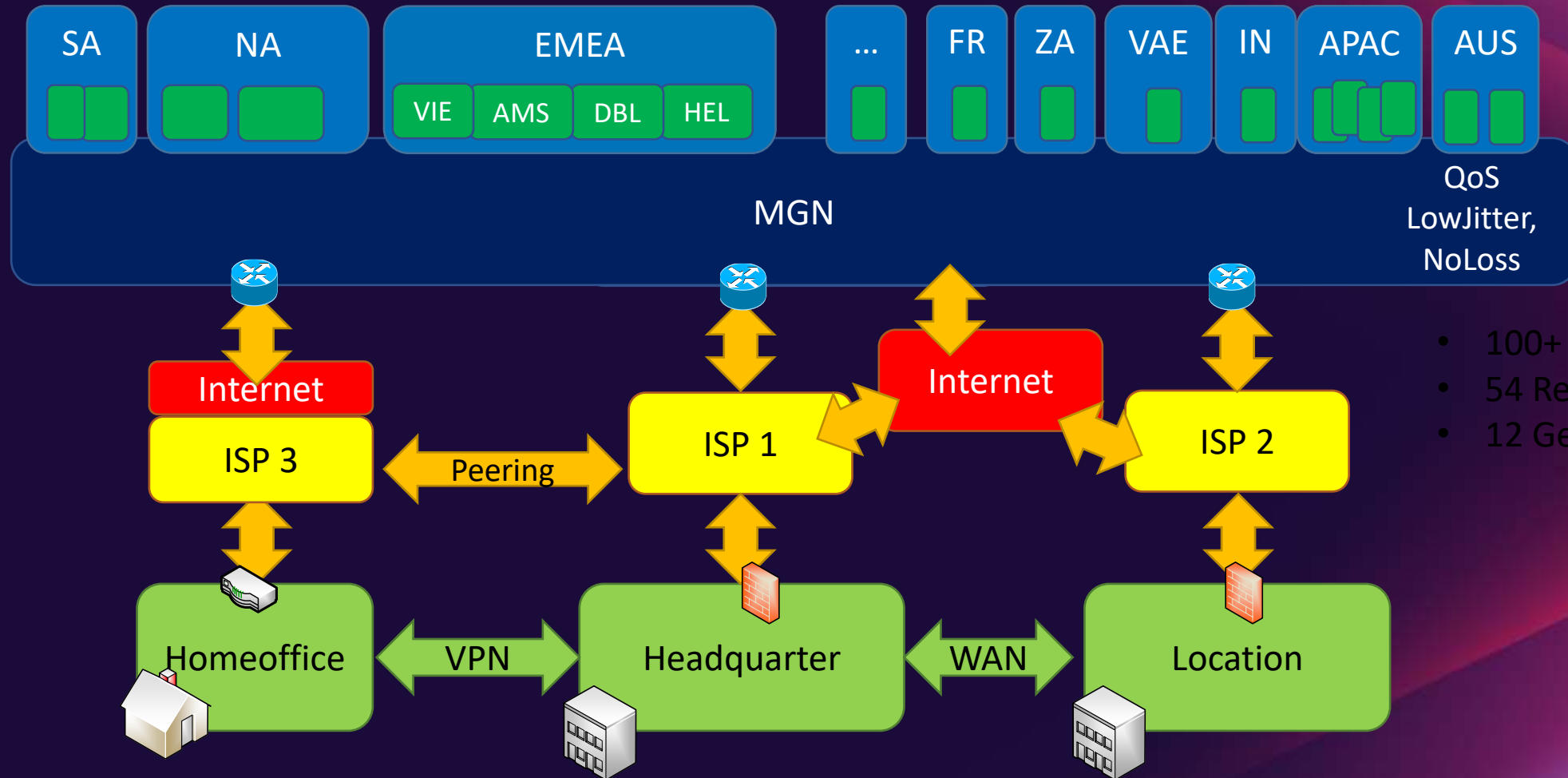


Microsoft Global Network

- Microsofts own world wide network
 - 200+ Peering Locations, 4000+ Networkpartners, 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](http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft%20Cloud%20Infrastructure%20Datacenter%20and%20Network%20Fact%20Sheet.pdf)
 - QoS managed, no loss, no jitter
 - Multiple Terabit Peerings
- BGP: Microsoft ASN= 8075
 - <https://www.peeringdb.com/asn/8075>
 - <https://stat.ripe.net/AS8075#tabId=at-a-glance>
 - #IPv4 Prefix:243 about 44.816.640 IPs
 - #IPv6 Prefix:19 about 8.523.790/48 nets
- Peering List for Azure
 - <https://docs.microsoft.com/en-us/rest/api/peering/peeringlocation>

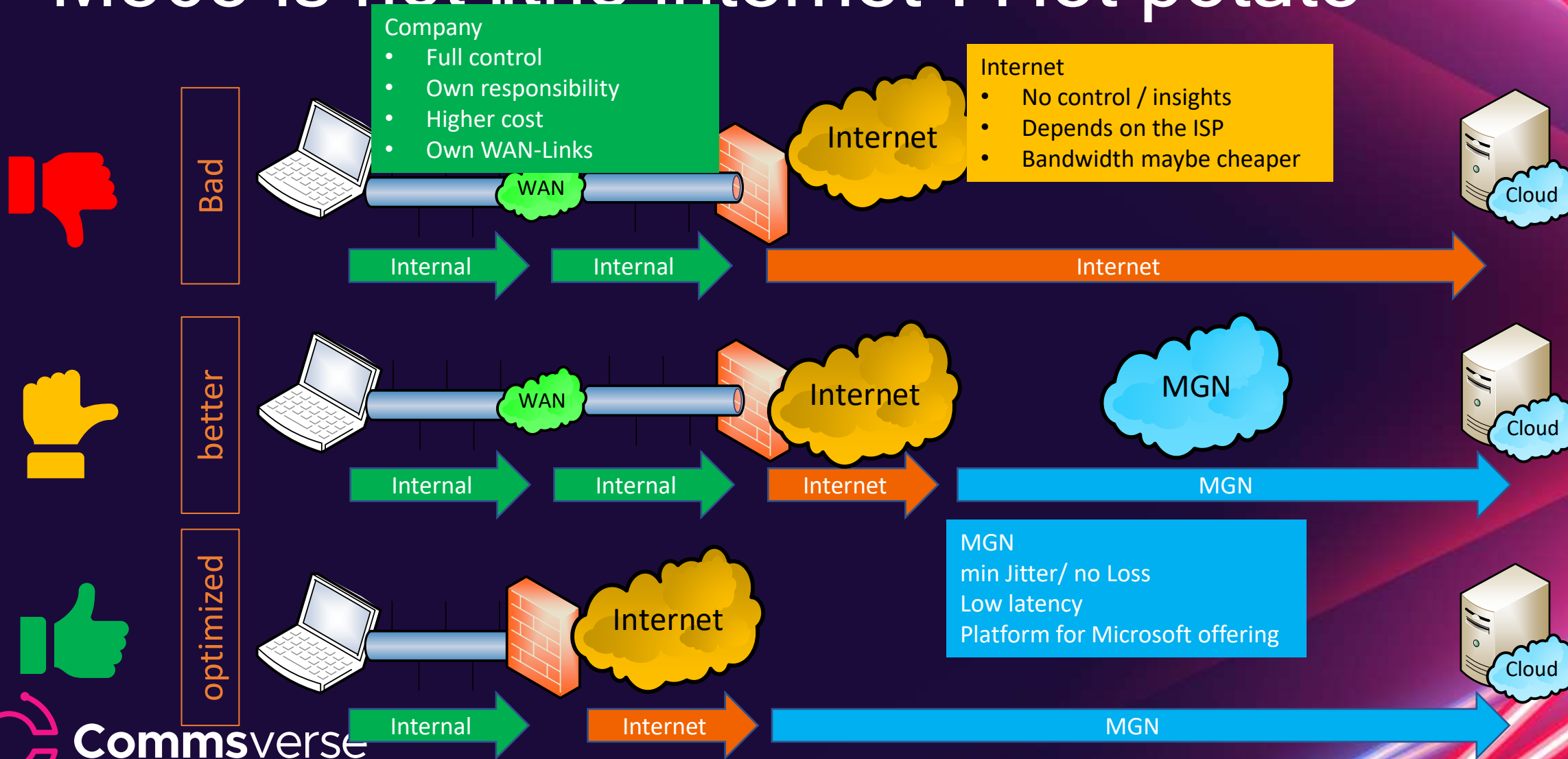


Connect your client to the service



- 100+ Azure RZs
- 54 Regions
- 12 Geos

M365 is not „the internet“. Hot potato



Company

- Full control
- Own responsibility
- Higher cost
- Own WAN-Links

Internet

- No control / insights
- Depends on the ISP
- Bandwidth maybe cheaper

MGN

- min Jitter/ no Loss
- Low latency
- Platform for Microsoft offering

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

The screenshot shows the Microsoft Peering website. The browser address bar displays peering.azurewebsites.net/peering/. The page features the Microsoft logo and a banner for PeeringDB. A navigation menu includes 'Peering' and 'Caching'. The main content area is titled 'Peering' and contains a list of requirements. Three callout boxes highlight specific details: the first lists general network capabilities and NOC support; the second lists prerequisites for peering; the third details requirements for private interconnections, with '10Gbps or 100Gbps optics' and 'upgrade their ports when peak utilization exceeds 50%' highlighted in red boxes.

Microsoft

Proud Sponsor of PeeringDB DIAMOND

Peering

Peering Caching

Peering

Peering is the direct interconnection of network for the purpose of exchanging traffic between networks.

Microsoft peers at the Internet Service Provider (ISP) level.

- A fully redundant network with sufficient capacity to exchange traffic without congestion.
- A knowledgeable and fully staffed 24x7x365 Network Operations Center (NOC), capable of assisting in the resolution of:
 - All technical and performance issues.
 - All security violations, denial of service attacks, or any other abuse originating within the peer or their customers.
- Microsoft will only establish private interconnection points with ISP or Network Service providers.

Additional Requirements for Private Interconnections

- Interconnection must be over single-mode fiber using the appropriate 10Gbps or 100Gbps optics.
- Peers are expected to upgrade their ports when peak utilization exceeds 50% and maintain diverse capacity in each metro, either within a single location or across several locations in a metro.

- A publicly routable IP address.
- At least one public IP address.
- Current and complete account and phone records.
- Neither party shall be held liable for the other's actions.



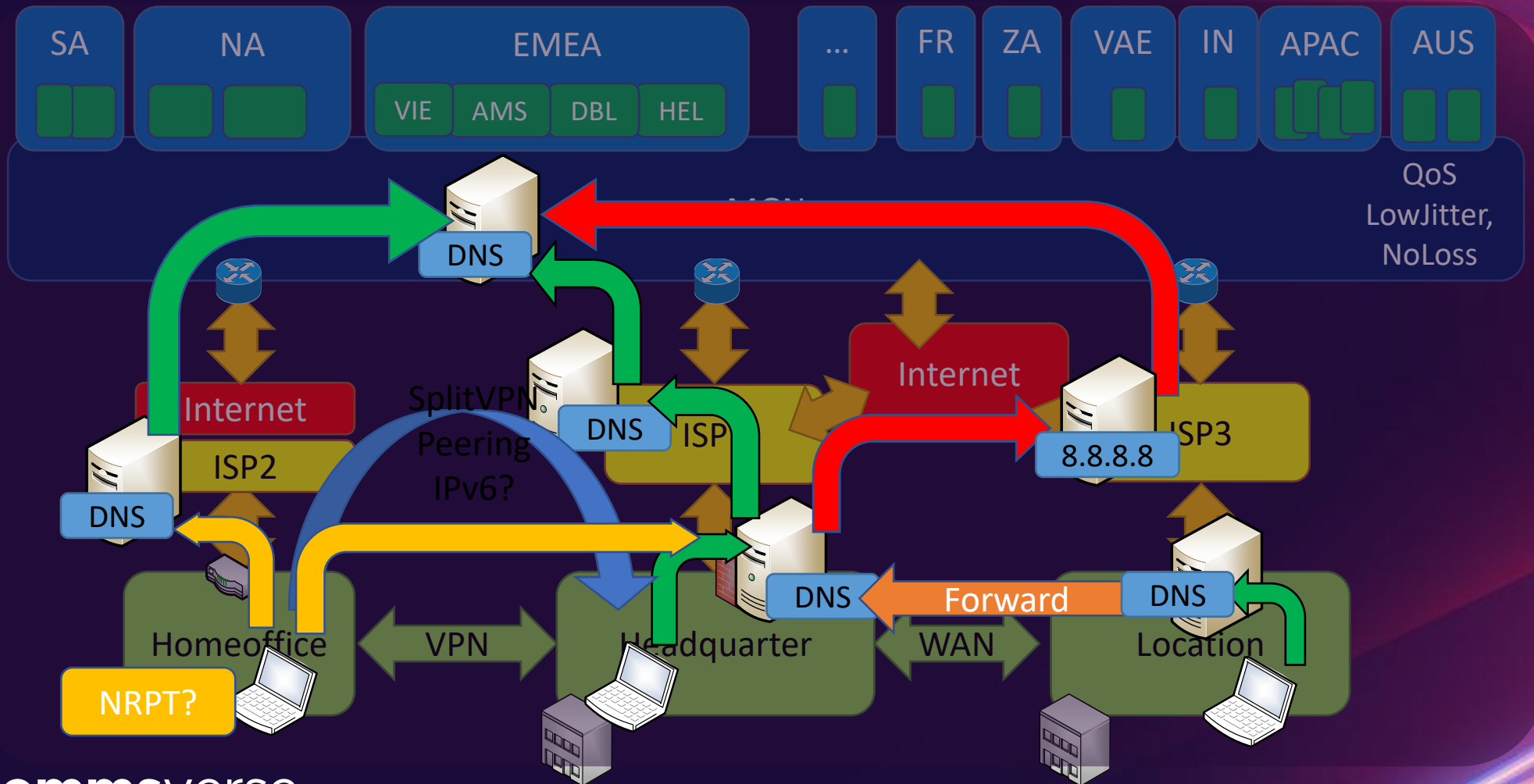
Commiverse

<https://www.microsoft.com/peering> -> <https://peering.azurewebsites.net/peering/>

The magic of DNS



DNS-Resolution



DNS Round Robin / TTL

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



Sample: wrong DNS-Server

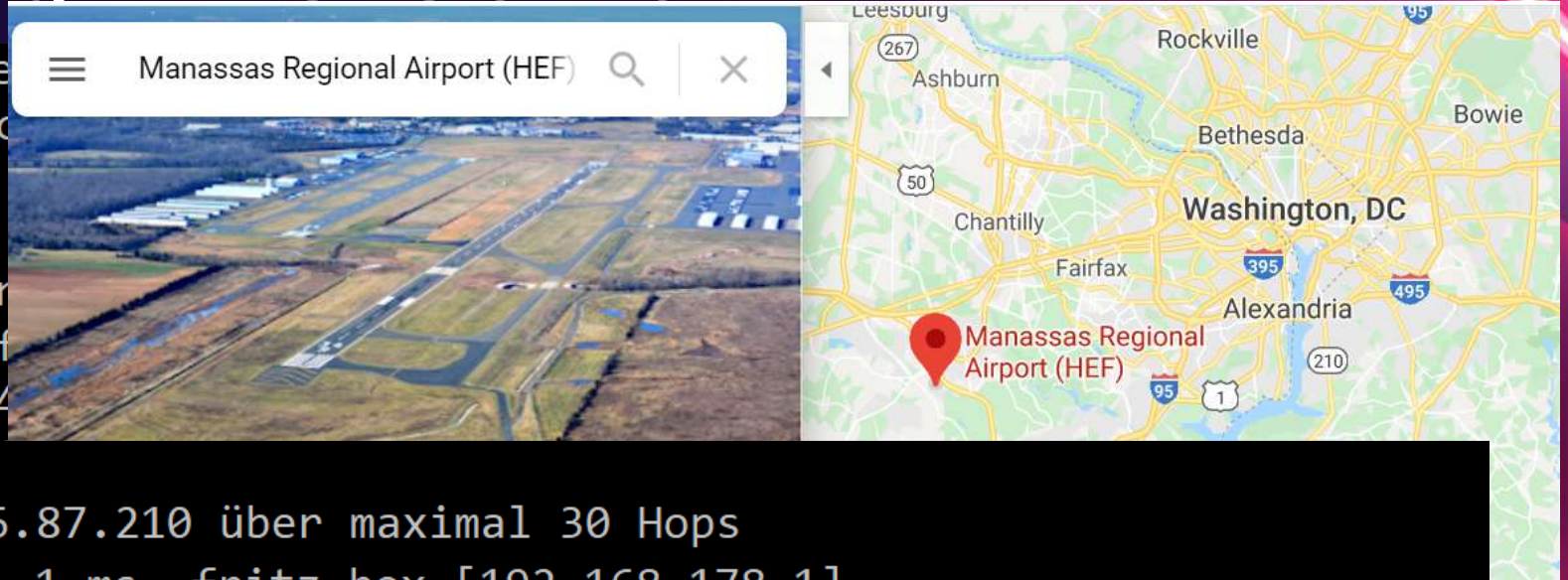
```
C:\>nslookup outlook.office
Server: home1.bellatlantic
Address: 199.45.32.43
```

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

```
C:\>tracert 52.96.87.210
```

```
Routenverfolgung zu 52.96.87.210 über maximal 30 Hops
```

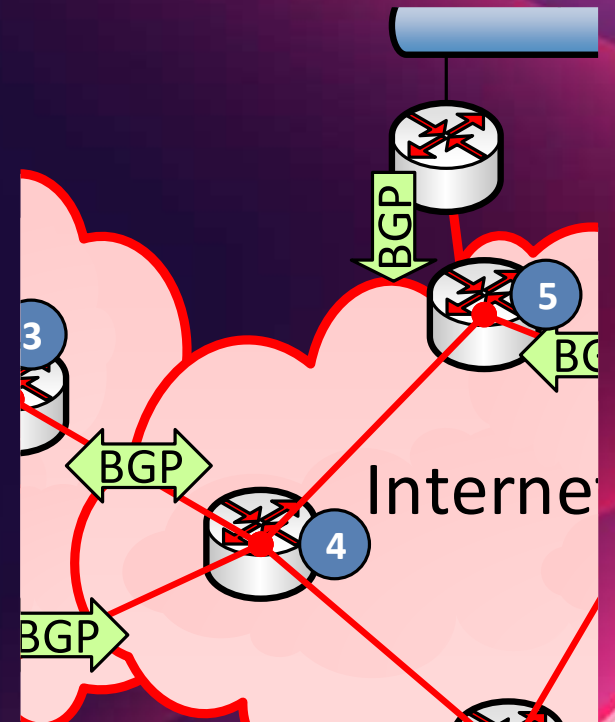
1	2 ms	1 ms	1 ms	fritz.box [192.168.178.1]
2	5 ms	4 ms	5 ms	p3e9bf2dc.dip0.t-ipconnect.de [62.155.242.220]
3	12 ms	11 ms	12 ms	d-ed5-i.D.DE.NET.DTAG.DE [62.154.5.213]
4	12 ms	12 ms	12 ms	80.157.204.58
5	16 ms	15 ms	16 ms	ae18.cr3-ams1.ip4.gtt.net [213.200.117.218]
6	16 ms	16 ms	16 ms	ip4.gtt.net [154.14.37.246]
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.sx171.ntwk.msn.net [104.44.16.116]



Validation

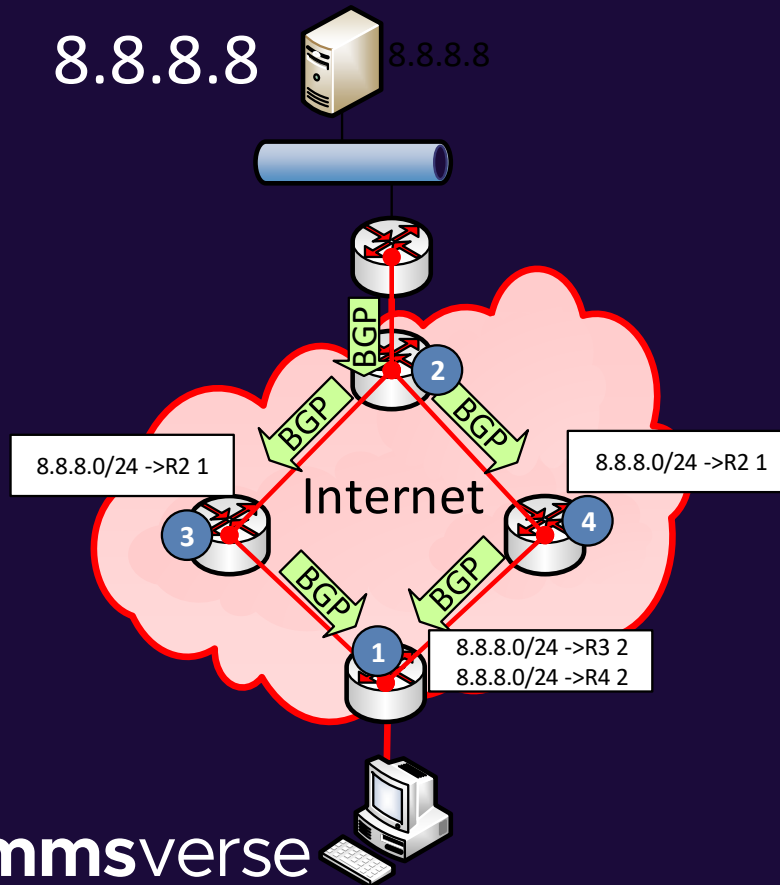
- Make sure that the clients use the „right DNS-Server“
- Watch for
 - DNS-Servers in the wrong region
 - DNS-Forwarding from location to headquarter
 - „optimizing“ servers (PiHole etc)
 - „Hosted“ Filter-Services
 - Cloud Proxy
 - IPv6 and VPN
- DNS and VPN: Name Resolution Policy Table?
- DNS Resolution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

Anycast IP Routing

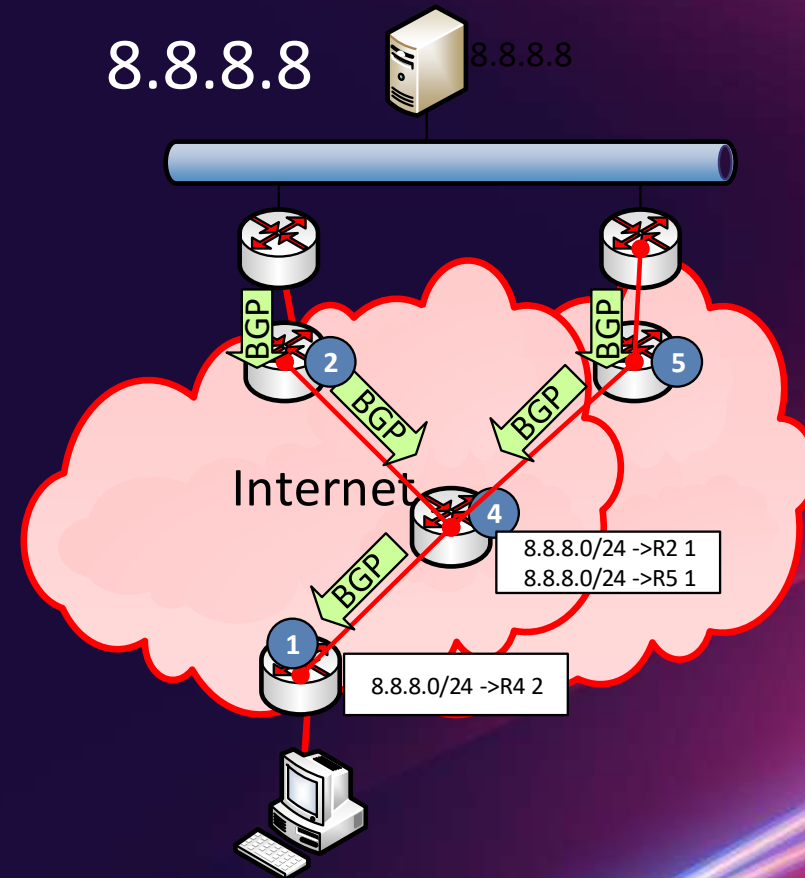


Redundancy with IP-Routing

Redundant routing

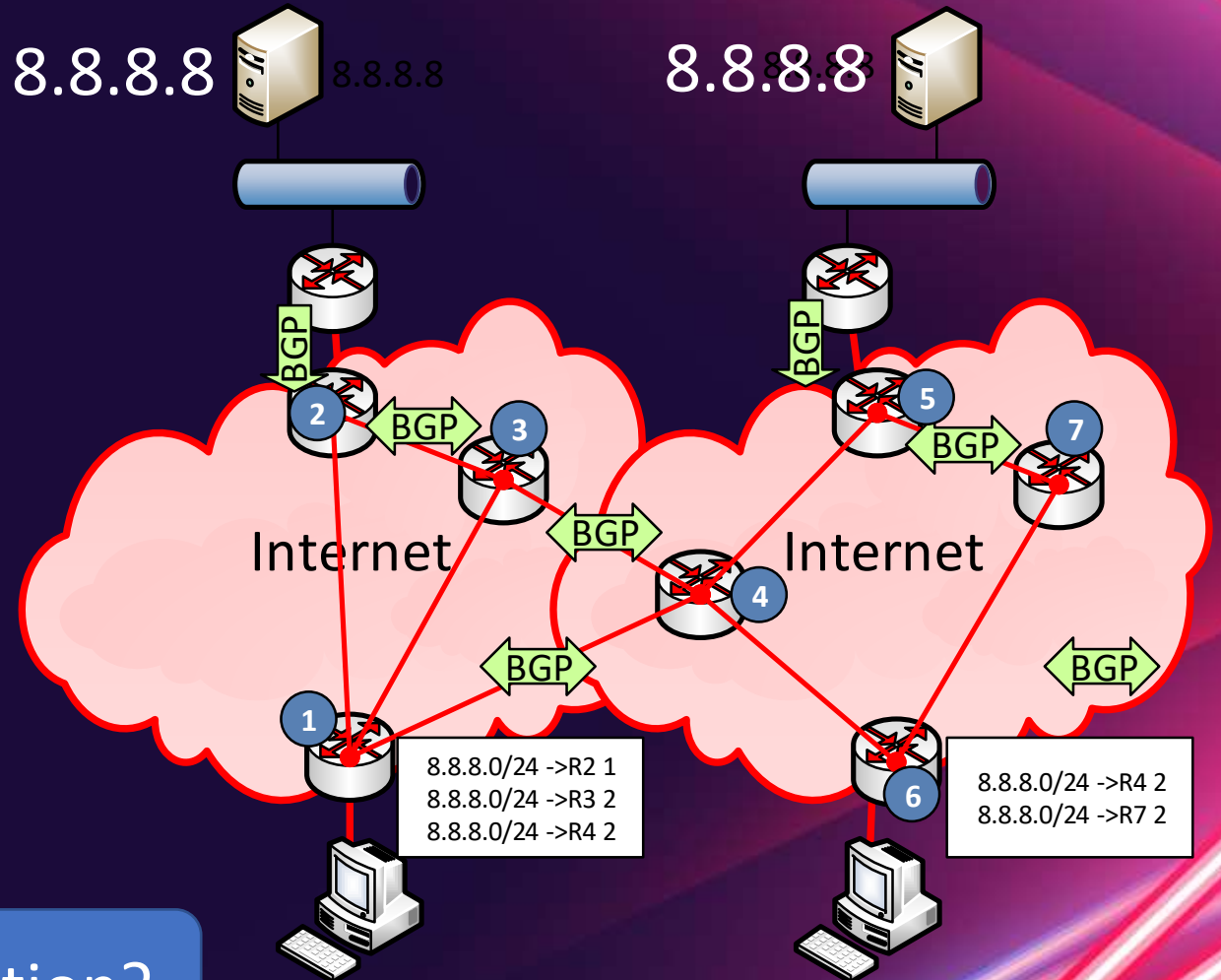


Redundant provider



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
ExchangeOnline	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 AnycastDNS eu.turn.teams.microsoft.com (Protocol uses Redirect to RealIP)	To much and very short TTL EU-Tenants	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	3PIP-Phones



- TCP Level 400
 - Windows Size
 - Port-Limits
 - TCP-Chimney
 - Window size / RSS
 - SACK

You all should know this already! – Part 1



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



$50 \text{ packets} * 1514 \text{ bytes} = 75\text{kByte/sec}$

Windows Scaling and latency

- Send multiple packets as block and accept later ACK-packets
 - Sender and receiver must maintain a buffer to resend lost packet and reassemble reordered packets
 - Negotiation of buffer size 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://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc162519(v=msdn.10))

https://www.msxfaq.de/netzwerk/grundlagen/tcp_retransmit_und_sack.htm

```
> Frame 885: 271 bytes on wire (2168 bits), 271 bytes captured
> Ethernet II, Src: Portwell_49:4f:68 (00:90:fb:49:4f:68), Dst:
> Internet Protocol Version 4, Src: 40.97.134.18, Dst: 192.168.1.1
v Transmission Control Protocol, Src Port: 443, Dst Port: 49870
  Source Port: 443
  Destination Port: 49870
  [Stream index: 28]
  [TCP Segment Len: 217]
  Sequence number: 5544 (relative sequence number)
  [Next sequence number: 5761 (relative sequence number)]
  Acknowledgment number: 2783 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 65535
  [Calculated window size: 1048560]
  [Window size scaling factor: 16]
  Checksum: 0x01a4 [unverified]
  [Checksum Status: Unverified]
```

Window size and Latency = Throughput

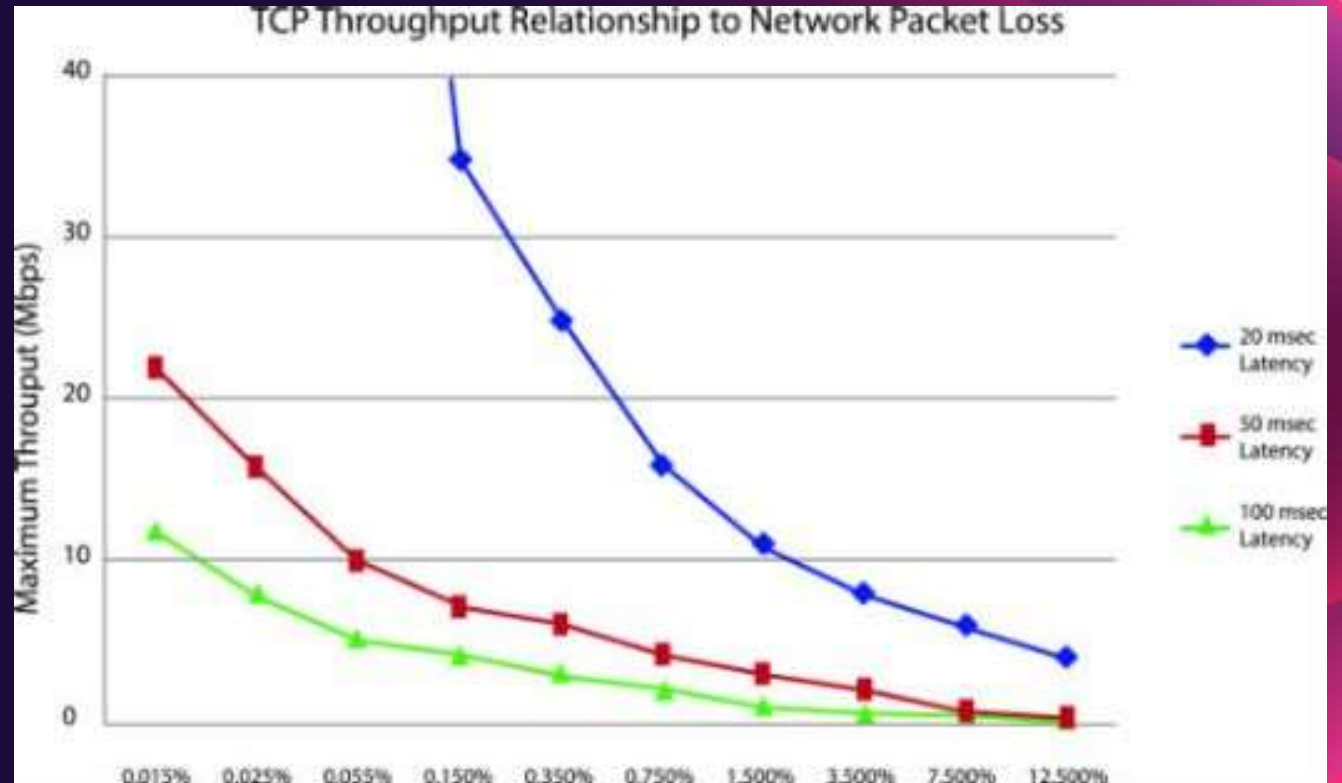
Applikation	Window size	1ms	20ms	50ms	100ms	200ms
Exchange Webservices (EWS)	1.048.560	na	50MB/s	20MB/s	10MB/s	5MB/s
OneDrive 10MB Upload	1.059.840	na	50MB/s	20MB/s	10MB/s	5MB/s
SharePoint 12MB Download	4.273.920	na	208MB/s	84MB/s	42MB/s	21MB/s
End2end-http Outlook	1.588.480	na	75MB/s	30MB/s	15MB/s	7,5MB/s
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

Packet 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/>

Latency per connection -> more connections

- Outlook
- Teams
- others

Outlook-Verbindungsstatus

Allgemein Lokales Postfach

Aktivität

VID	SMTP-Adresse	Servername	Status	Proto...	Authn	Verschl...	Typ	Anfr/Fehle
6	Frank.Carius@Netat...	https://outlook.office365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-Verzei...	60/3
10	admin@carius.onmi...	https://outlook.office365.com/...	hergestellt	HTTP	Klartext*	SSL	Exchange-Verzei...	58/2
17	Frank.Carius@Netat...	https://outlook.office365.com/...	hergestellt	HTTP	Träger*	SSL	Exchange-Verzei...	376/4

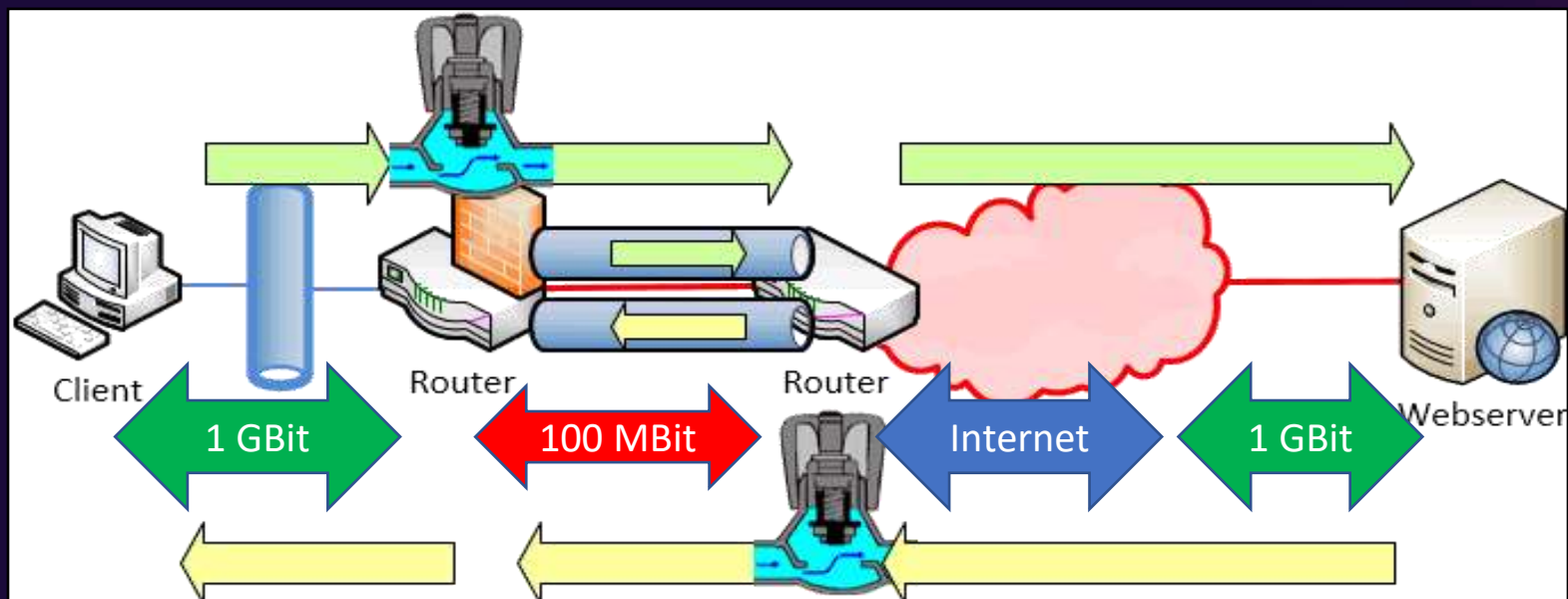
TCP-Verbindungen

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	llt	HTTP Träger* SSL Exchange-E-Mail 14711/6
Teams.exe	14412	172.18.241.38	58439	52.114.88.46	443	0	76	llt	HTTP Klartext* SSL Exchange-E-Mail 169/5
Teams.exe	13952	172.18.241.38	58447	52.114.74.39	443	0	74	llt	HTTP Klartext* SSL Exchange-E-Mail 783/4
Teams.exe	14412	172.18.241.38	58457	52.178.94.2	443	-	-	llt	HTTP Träger* SSL Exchange-E-Mail 173/2
Teams.exe	13952	172.18.241.38	58448	52.113.194.131	443	-	-	llt	HTTP Nego* SSL Exchange-E-Mail 113/13
Teams.exe	14412	172.18.241.38	58435	52.113.194.131	443	-	-	llt	HTTP Träger* SSL Exchange-E-Mail 64/6
Teams.exe	13952	172.18.241.38	58417	52.114.76.35	443	-	-	llt	HTTP Klartext* SSL Exchange-E-Mail 64/6
OUTLOOK.EXE	22632	172.18.241.38	58520	40.101.12.18	443	0	1.190	llt	HTTP Träger* SSL Exchange-E-Mail 72/3
OUTLOOK.EXE	22632	172.18.241.38	58519	40.101.12.18	443	0	567	llt	HTTP Träger* SSL Exchange-E-Mail 97/4
OUTLOOK.EXE	22632	172.18.241.38	58507	40.101.12.18	443	0	553	llt	HTTP Klartext* SSL Exchange-E-Mail 2470/6
OUTLOOK.EXE	22632	172.18.241.38	58499	40.101.12.18	443	0	523	llt	HTTP Träger* SSL Exchange-E-Mail 12/0
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		

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?



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 packet size
 - ICMP (Typ=3, Code=4) required

```

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured on interface 0
> Ethernet II, Src: Universa_5d:79:e1 (e0:4f:43:5d:79:e1), Dst: 08:00:27:00:00:00
  > Internet Protocol Version 4, Src: 192.168.178.50, Dst: 192.168.178.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 1500
      Identification: 0xdd86
    > Flags: 0x4000, Don't Fragment
      Time to live: 128
      Protocol: ICMP (1)
      Header checksum: 0x0000 [Header checksum status: Bad]
      Source: 192.168.178.50
    
```

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

```

> Frame 422: 70 bytes on wire (560 bits), 70 bytes captured on interface 0
> Ethernet II, Src: AvmAudio_98:0c:97 (e0:28:6d:98:0c:97), Dst: 08:00:27:00:00:00
  > Internet Protocol Version 4, Src: 192.168.178.50, Dst: 192.168.178.1
    > Internet Control Message Protocol
      Type: 3 (Destination unreachable)
      Code: 4 (Fragmentation needed)
      Checksum: 0x510e [correct]
      [Checksum Status: Good]
      Unused: 0000
      MTU of next hop: 1492
    > Internet Protocol Version 4, Src: 192.168.178.50, Dst: 192.168.178.1
      [Response frame: 2]
    
```

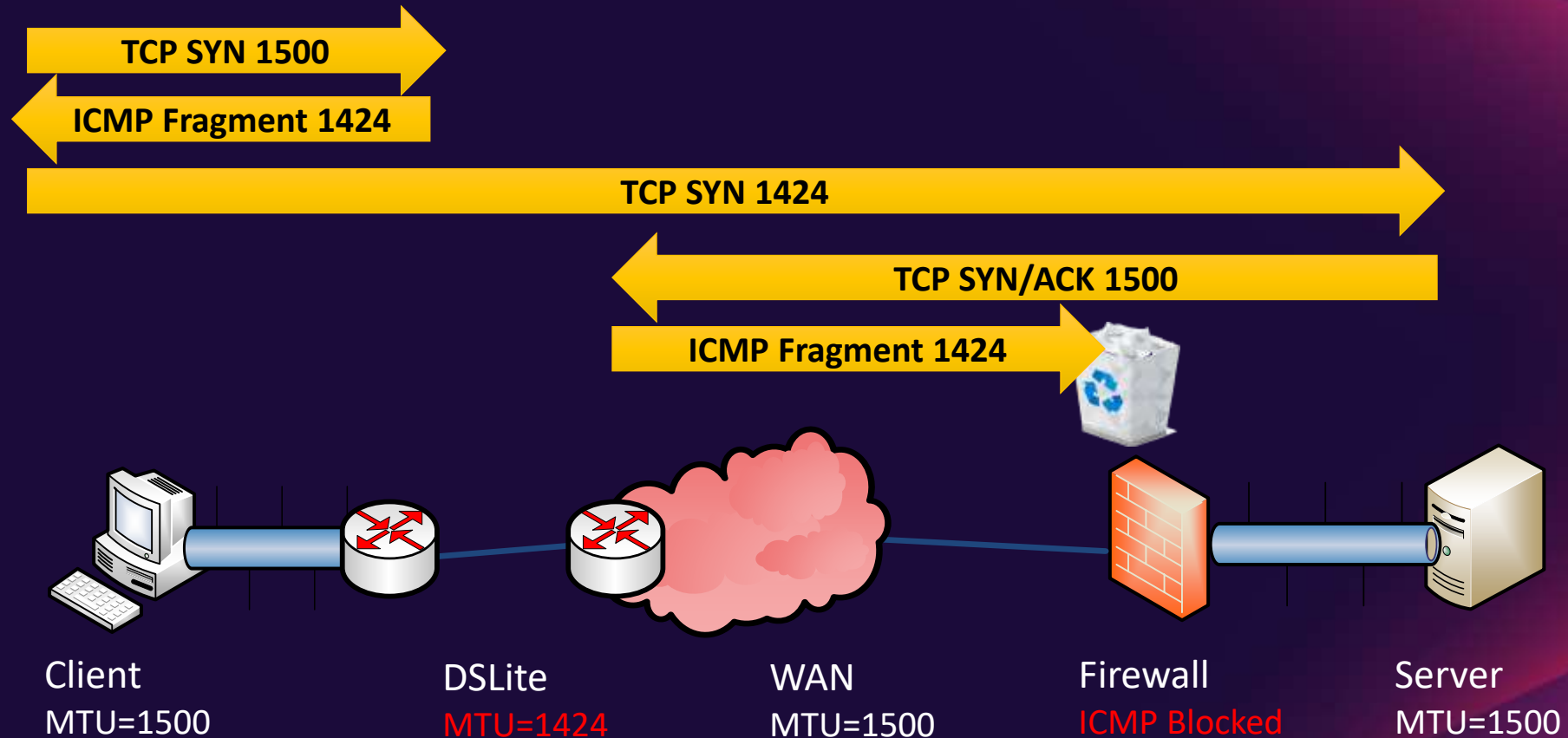
```

> Data (1472 bytes)

```



MTU - Real customer case



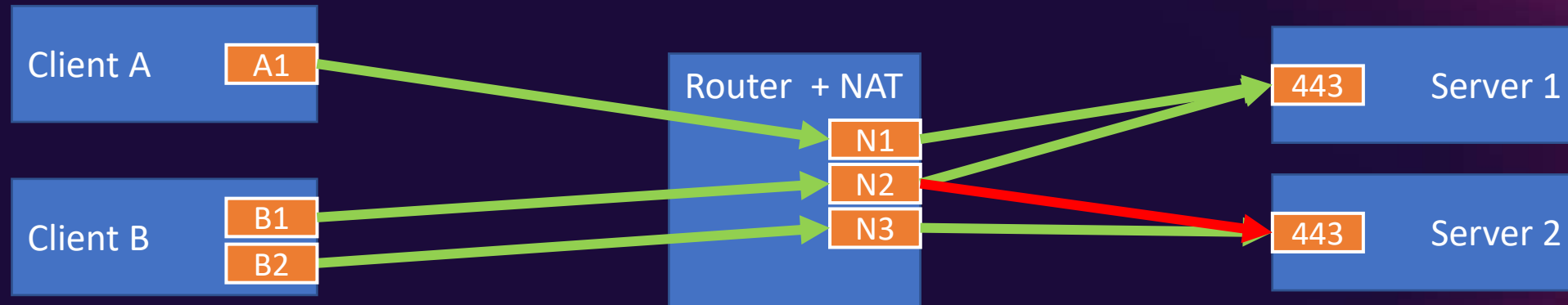
- TCP/IP and Ports

You all should know this already - Part 2



Private addresses and public ports

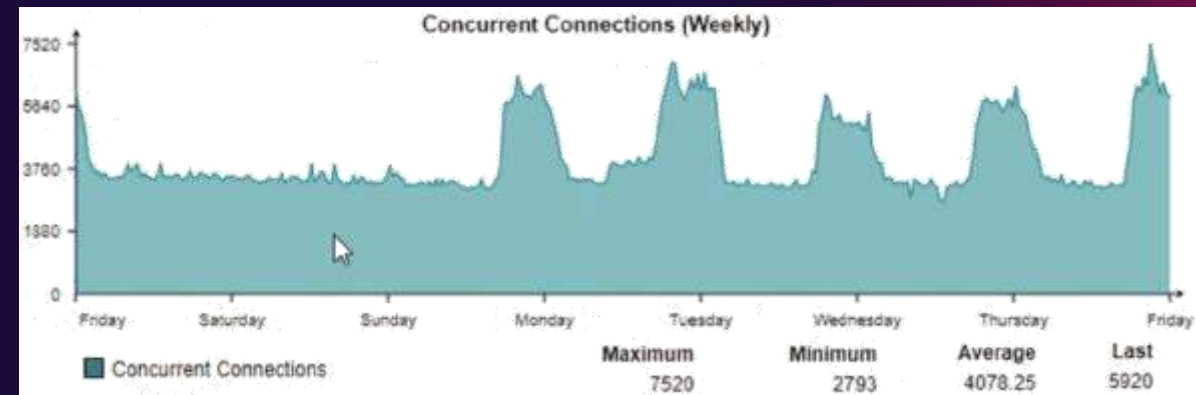
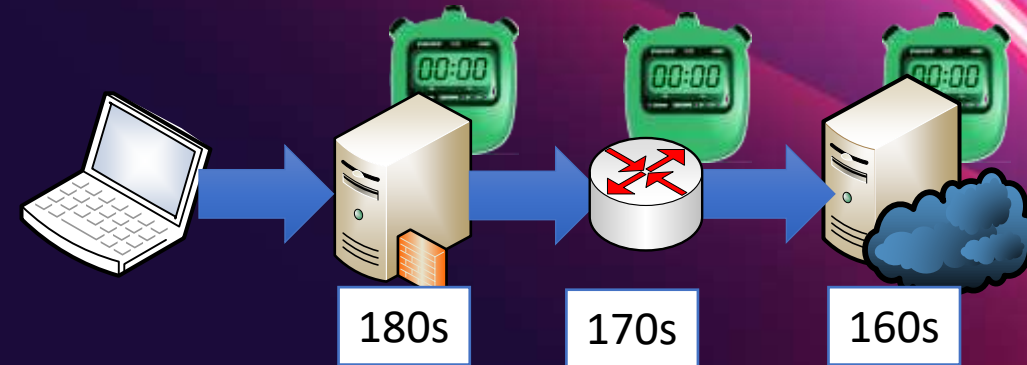
- We need a translation from private IP to internet services
 - NAT-Device or HTTP-Proxy



- 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-IP - 4000 reserved = 60.000 available ports for clients

Session Timeout / Keepalive

- Clients are not friendly
 - Client loses 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.msxfag.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 Audio/Video (RTP)

Teams is the canary in your network
like the canary in a coal mine or winery
If there is a problem, team will expose it



• Teams Workloads

Workload	Service
Login/Logoff/Presence	https:\\teams.microsoft.com
Chat (1:1, Groups, Channel, Federation)	https:\\teams.microsoft.com
Channel-Files	https:\\<tenant>.sharepoint.com
1:1 Files	https:\\<tenant>-my.sharepoint.com
Apps	https:\\<Application-URL>
1:1 Audio/Video/Sharing	UDP: RTP Client<->Client
Conference	UDP: RTP Client <-> MCU
Phone	UDP: RTP Client <-> SBC / Mediarelay

• Why UDP preferred ? - Audio is not „Data“

- Files, Mails, Databases,
 - Larger bursts of packets
 - Fast but not „realtime“
 - TCP to solve reordering and packet loss
 - Large packets (max. MTU-size)
- VoIP Audio/Video
 - Many small packets (20ms, 160 Bytes (=64kbit))
 - Realtime, low latency
 - No need to resend slow/lost packets
 - Application should „see“ latency, jitter loss
 - Application can change Codec, Bitrate, resolution
 - UDP is preferred protocol for audio/video
- Issues with TCP or HTTPS
 - Packet Loss: Streams stops until missing data arrives
 - Audio and video stops

Kriterium	Files etc	Audio/Video
Packetsize	1500 kBytes	160 Bytes
Protocol	TCP	UDP
Usage profile	Larger bursts	Contiuous small packets
Packet loss	TCP resend	Do not resend
Ordering	TCP ordering	Jitter buffer
Adaption	None	Codec, Resolution wide/narrowband
Security	HTTPS/	SRTP

Support statement UDP 3478-3481 /TCP443

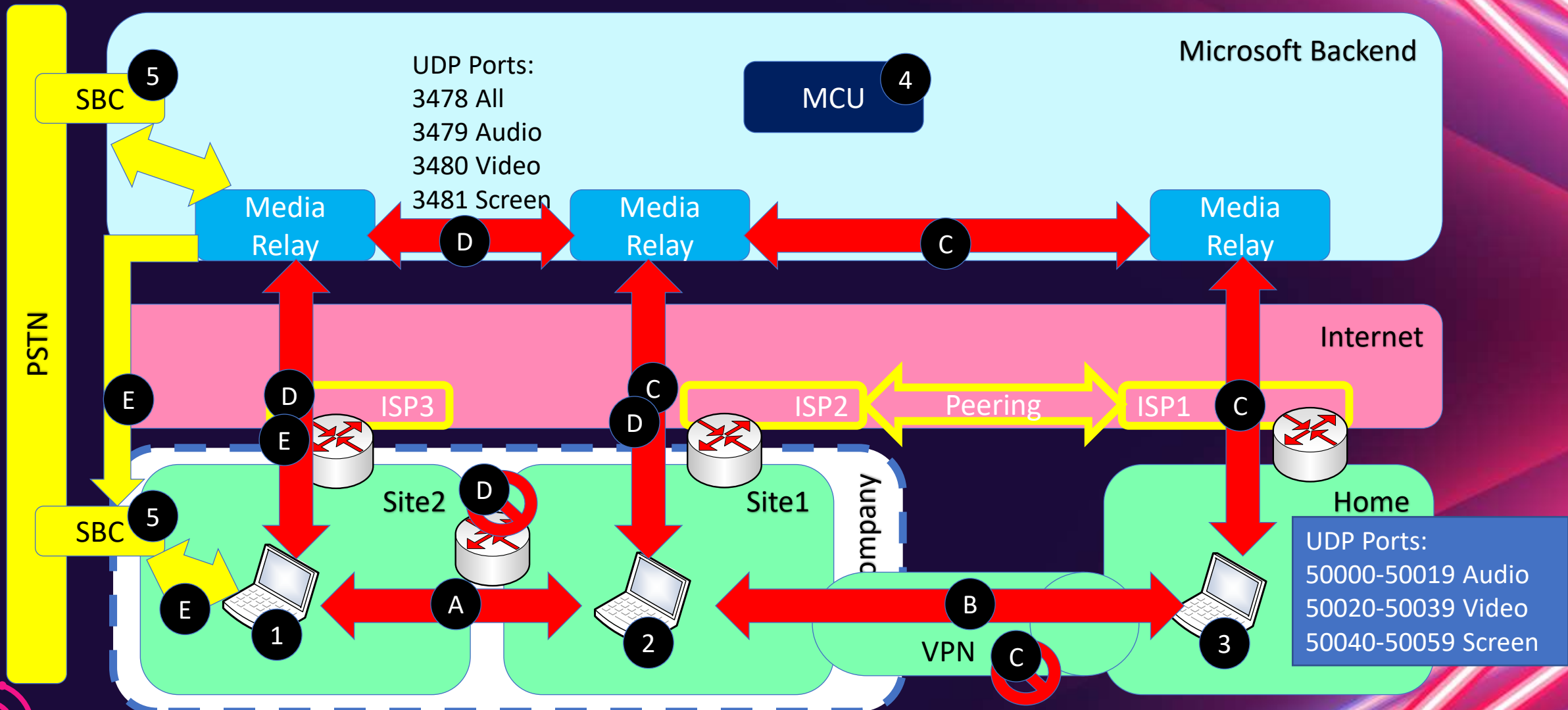
Firewall and proxy requirements

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.

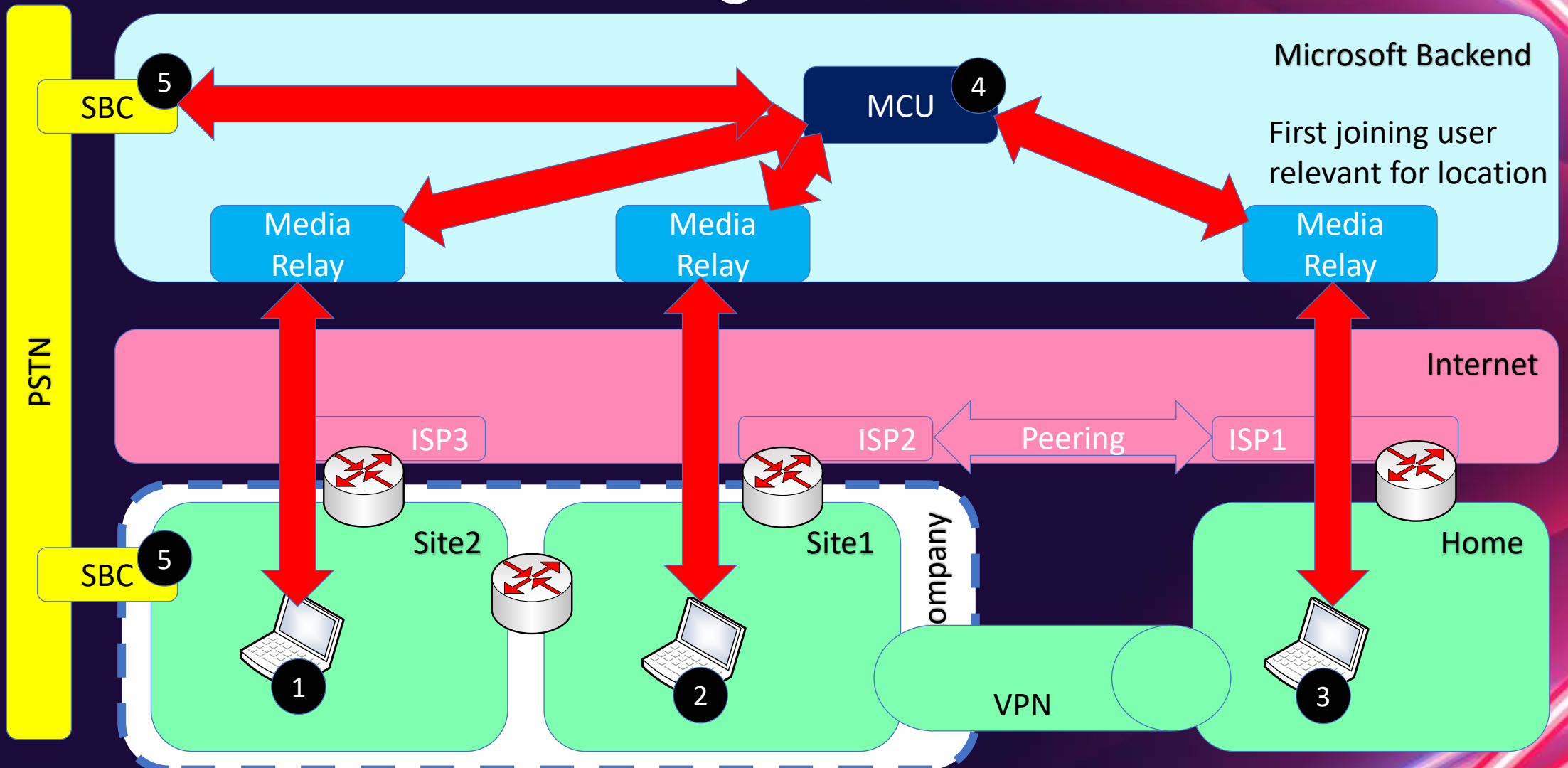
Opening these ports is essential for a reliable Teams deployment. Blocking these ports is unsupported and will have an effect on media quality.

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

Teams RTP 1:1 Teams Call / PSTN Call



Teams RTP Meeting



• Network Ready für VoIP

- Signalling (https)
 - Port 443 (not SIP 5061/TCP)
 - 5-10 kbit/User/sec
 - Neartime but not realtime
- RTP Requirements
 - Client to Transport Relay
 - <https://aka.ms/sof-media-quality>
 - Audio: 100kbit/sec
 - Video 1-2 Mbit/sec
- Protocoll: UDP preferred
 - Fallback: TCP or https
 - Sourceport 50.000-50059
 - Destinationport 3478-3481/UDP
- Network Assessment
 - https://www.msxfaq.de/skype_for_business/tools/microsoft/skype_for_business_online_network_assessment_tool.htm

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>

• Teams Network Assessment Tool

- Free
- CMDLine
- No GUI
- Once
- Not continuous
- 32 RTP Tests
- Output:CSV

```
Eingabeaufforderung - NetworkAssessmentTool.exe
C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe
Microsoft Teams - Network Assessment Tool

Starting Relay Connectivity Check:
UDP, PseudoTLS, FullTLS, HTTPS connectivity will be checked to this relay (VIP) FQDN: worldaz.tr.teams.microsoft.com
If user wants to check connectivity to a particular relay (VIP) IP, please specify in NetworkAssessment.exe.config.

Connectivity check source port range: 50000 - 50019

Relay : 52.114.253.254 is the relay load balancer (VIP)
Relay : 52.114.253.254 is reachable using Protocol UDP and Port 3478
Relay : 52.114.253.254 is QOS (Media Priority) enabled
Relay : 52.114.253.254 is the relay load balancer (VIP)

Starting Service Connectivity Check:
Relay : 52.114.253.254 is reachable using Protocol PseudoTLS and Port 443
Relay : 52.114.253.254 is the relay load balancer (VIP)
Relay : 52.114.253.254 is reachable using Protocol FullTLS and Port 443
Relay : 52.114.253.254 is the relay load balancer (VIP)
Relay : 52.114.253.254 is reachable using Protocol HTTPS and Port 443
Relay : 52.114.254.5 is the actual relay instance (DIP)
Relay : 52.114.254.5 is reachable using Protocol UDP and Port 3478
Relay : 52.114.254.5 is the actual relay instance (DIP)
Relay : 52.114.254.5 is reachable using Protocol UDP and Port 3479
Relay : 52.114.254.5 is the actual relay instance (DIP)
Relay : 52.114.254.5 is reachable using Protocol UDP and Port 3480
Relay : 52.114.254.5 is the actual relay instance (DIP)
Relay : 52.114.254.5 is reachable using Protocol UDP and Port 3481
```

<https://www.microsoft.com/en-us/download/details.aspx?id=103017>

Google Meet Readiness

- Google Meet
 - Destination Port: 19302-19309/UDP 443/TCP
 - <https://support.google.com/a/answer/1279090>
- Test with ICMP
 - 4hours continuous ICMP-Ping
 - Remote Host: lens.l.google.com
 - Always <100ms, no averages
- TraceRoute
 - Optimize for short path
- Bandwidth measurement: 3rd Party tools
- WebRTC Troubleshooter
<https://test.webrtc.org/>

Troubleshoot audio and video quality

Measure latency

If you're having a problem with video quality, make sure your network latency is low and consistent. Video quality is optimal when Meet traffic takes the shortest path between the client and Google. For example, it's best to have round-trip latency (RTT) between the client and Google lower than 100 ms. Meet media quality is reduced if latency is too high, such as 300 ms or more.

To measure latency, you can:

Ping the Google Meet media front-end server for at least 4 hours.

```
> ping lens.l.google.com
```

```
PING lens.l.google.com (74.125.143.127): 56 data bytes
```

```
64 bytes from 74.125.143.127: icmp_seq=0 ttl=47 time=25.424 ms
```

```
64 bytes from 74.125.143.127: icmp_seq=1 ttl=47 time=25.271 ms
```

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:

```
> traceroute lens.l.google.com
```

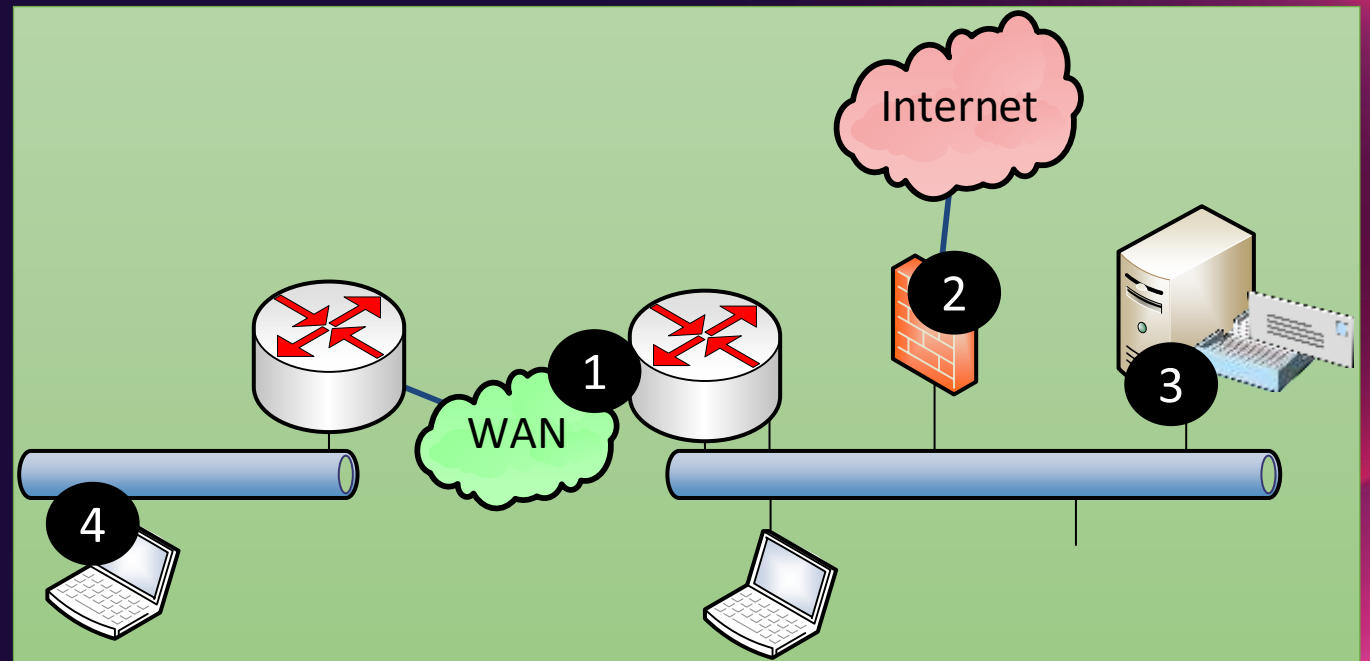
<https://support.google.com/a/answer/7582554#zippy=%2Cbandbreite-messen-und-optimieren%2Clatenz-messen>

- From my firewall to Microsoft 365



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“

2

- Managed by Microsoft

- No relevant local traffic

- Local breakout

- bypass own WAN

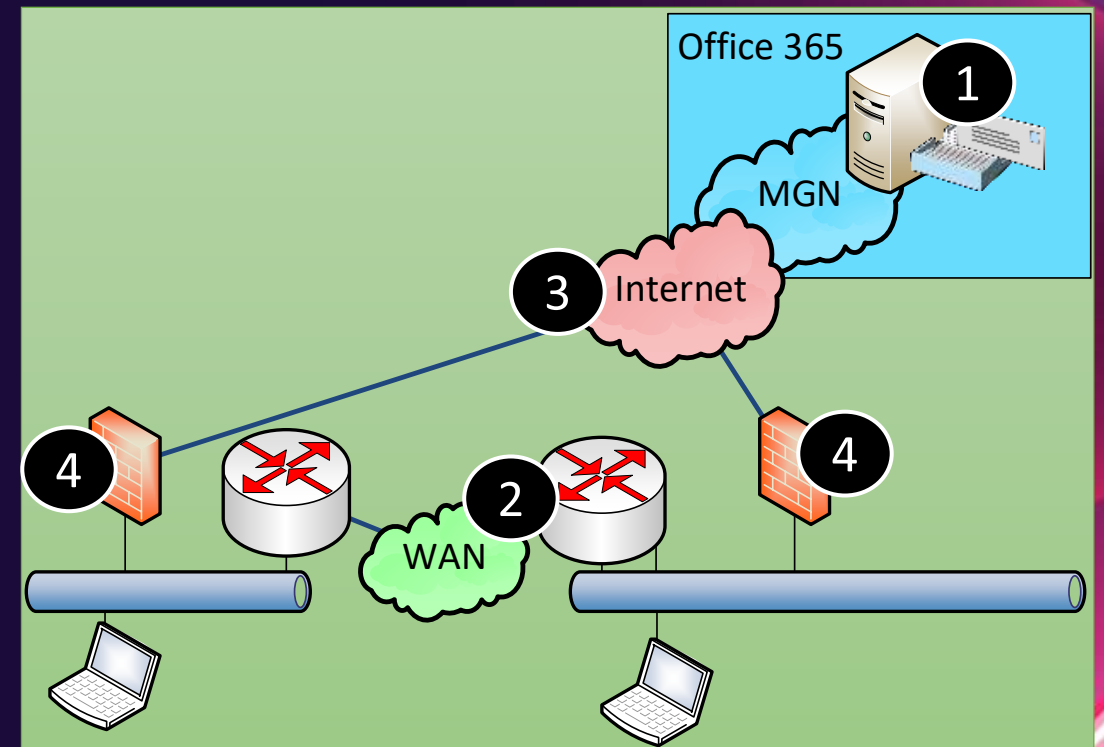
3

- 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



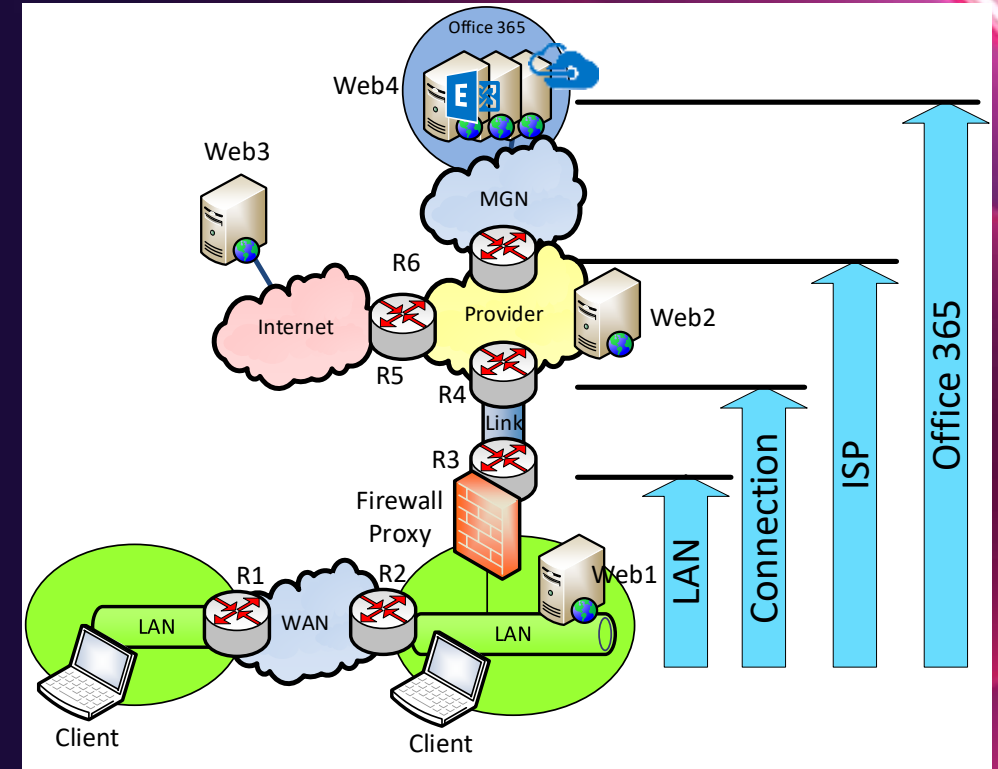
Google: “Make sure your latency is consistent at 100ms or less. Don't average the values because it can hide spikes and intermediate latency problems.”

Quelle:

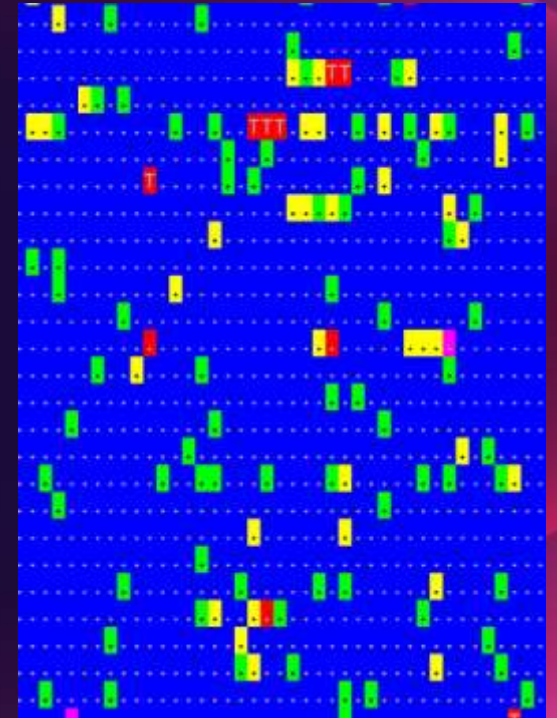
<https://support.google.com/a/answer/7582554>

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,...

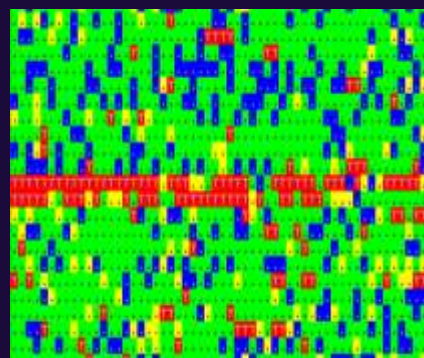
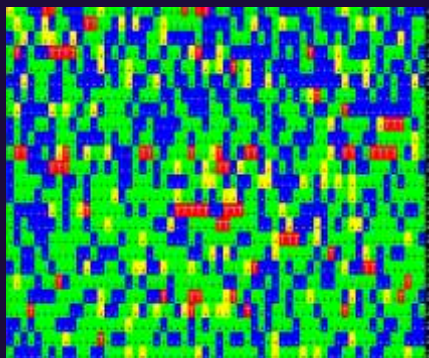


End2End-Scripts and Samples

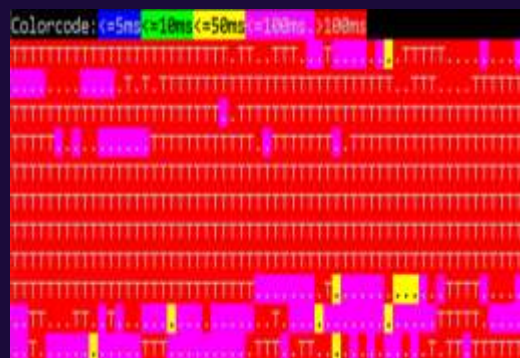


Samples: End2End-Ping

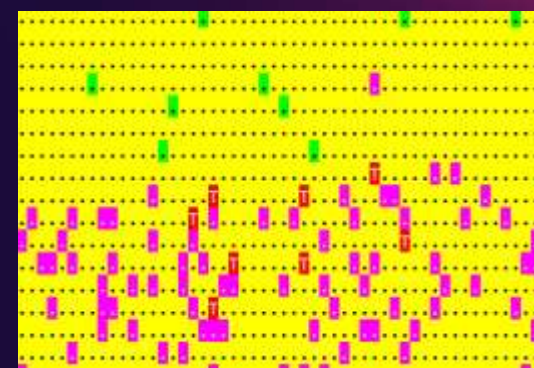
Bellevue Hotel 11:00pm/07:00am



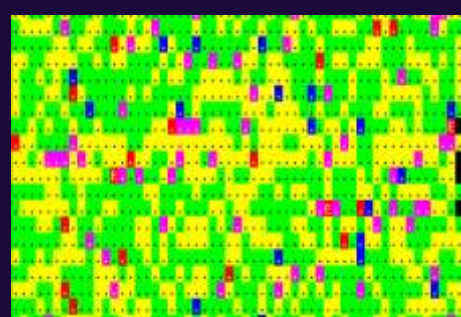
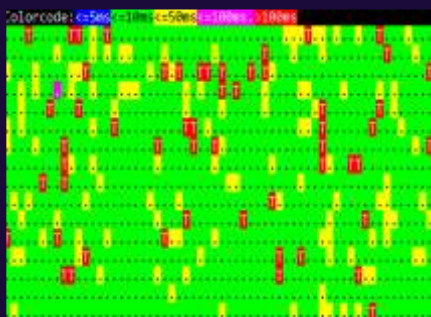
WifiOnICE



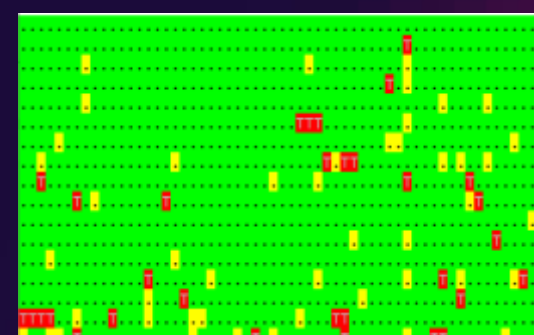
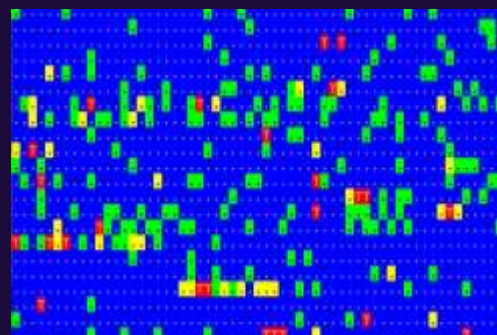
Home DSL 16/1



Hotel Frankfurt 01:00am, 07:00



MSTFGuest (Internet / Office365)



Checking HTTP

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

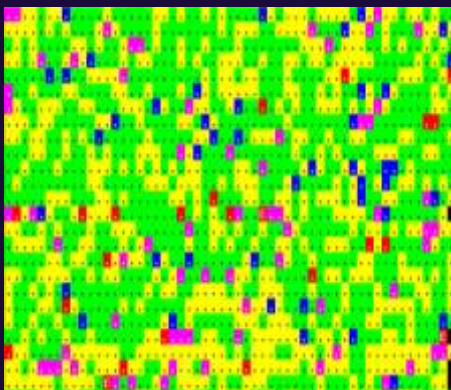
Bereich	URL	Size
Exchange	https://outlook.office365.com/owa/favicon.ico	7886 Bytes
Exchange	https://outlook.office365.com/owa/smime/owasmime.msi	729088 Bytes
OneDrive	<a href="https://<tenant>-my.sharepoint.com/">https://<tenant>-my.sharepoint.com/	193 Bytes
SharePoint	<a href="https://<tenant>.sharepoint.com/">https://<tenant>.sharepoint.com/	190 Bytes
SharePoint	<a href="https://<tenant>.sharepoint.com/_layouts/15/SPAndroidAppManifest.aspx">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)

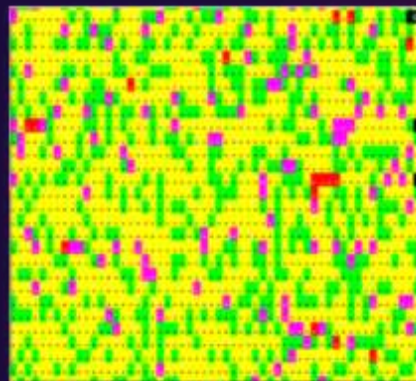
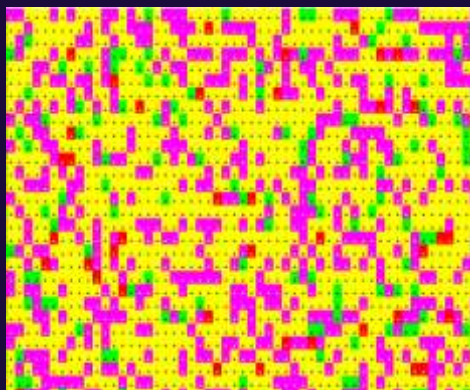
End2End-http: favicon.ico

Frankfurt Hotel 01:00am/07:00am

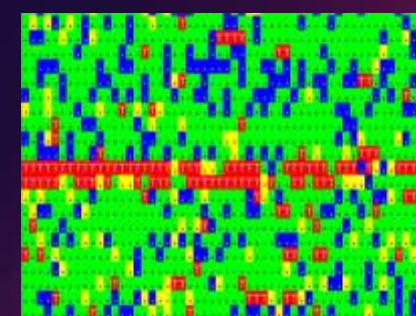
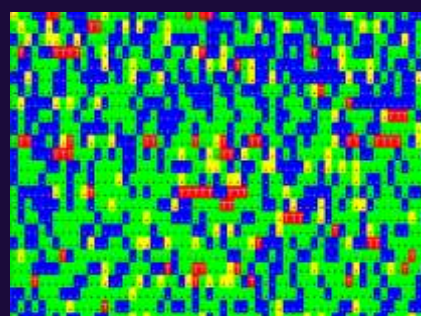
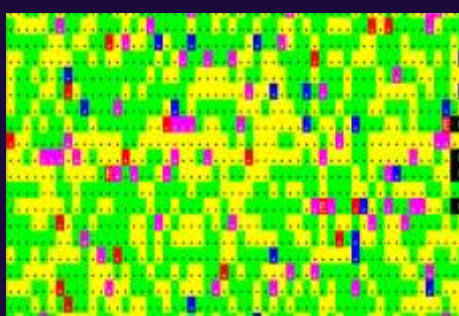
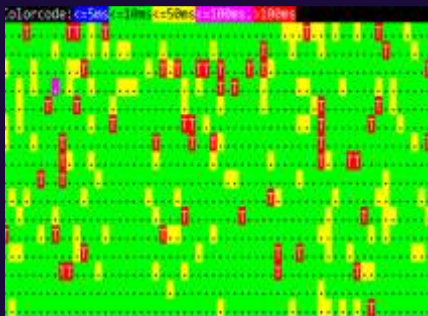
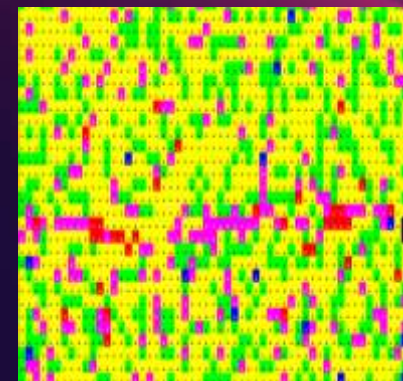
Bellevue Hotel 01:00am / 07:00p



Compare to ICMP



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

```
End2End-HTTP: URL = https://outlook.office365.com/owa/smime/owasmime.msi
Colorcode: <=20ms <=50ms <=100ms <=200ms >200ms
..... OK=27 Slow=9 Fail=0 MIN=153 AVG=692ms MAX=4351 X=End
..... OK=37 Slow=3 Fail=0 MIN=168 AVG=602ms MAX=5652 X=End
..... OK=42 Slow=2 Fail=0 MIN=156 AVG=35ms MAX=138 X=End
..... OK=44 Slow=2 Fail=0 MIN=108 AVG=302ms MAX=1567 X=End
..... OK=48 Slow=1 Fail=0 MIN=123 AVG=222ms MAX=1012 X=End
..... OK=45 Slow=1 Fail=0 MIN=124 AVG=302ms MAX=1131 X=End
..... OK=42 Slow=2 Fail=0 MIN=105 AVG=346ms MAX=2217 X=End
..... OK=43 Slow=2 Fail=0 MIN=116 AVG=329ms MAX=1717 X=End
..... OK=46 Slow=0 Fail=0 MIN=131 AVG=278ms MAX=995 X=End
..... OK=35 Slow=5 Fail=1 MIN=150 AVG=405ms MAX=1052 X=End
```


SharePoint Online

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



```
GET https://msxfaq.sharepoint.com/_layouts/15/SPAndroidAppManifest.aspx
User-Agent: Mozilla/5.0 (Windows NT; windows NT 10.0; de-DE)
WindowsPowerShell/5.1.18362.145
Host: msxfaq.sharepoint.com
```

Find... (press Ctrl+Enter to highlight all)

Transformer | Headers | Text View | Syntax View | Image View | Hex View | Web View

Office365 Auth | Auth | Caching | Cookies | Raw | JSON | XML

Response Headers

HTTP/1.1 200 OK

Cache

Cookies / Login

Entity

Miscellaneous

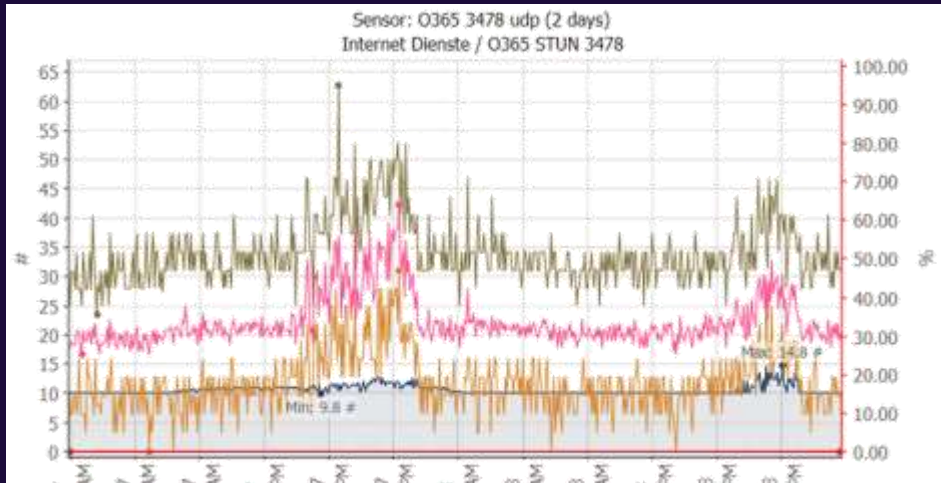
MicrosoftSharePointTeamServices: 16.0.0.19520
MS-CV: nyKrwC5AAJC/RLp6XAYlcA.0
request-id: c0ab229f-402e-9000-bf44-ba7a5c062570
SPisLatency: 1
SPRequestDuration: 112
SPRequestGuid: c0ab229f-402e-9000-bf44-ba7a5c062570
X-AspNet-Version: 4.0.30319
X-MSEdge-Ref: Ref A: 187B1EDD2CCC487B808FB6A7ED922BD5 Ref B: AM3EDGE0412 Ref C: 20
X-MS-InvokeApp: 1; RequireReadOnly
X-Powered-By: ASP.NET
X-SharePointHealthScore: 7

Security



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
```

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, ...

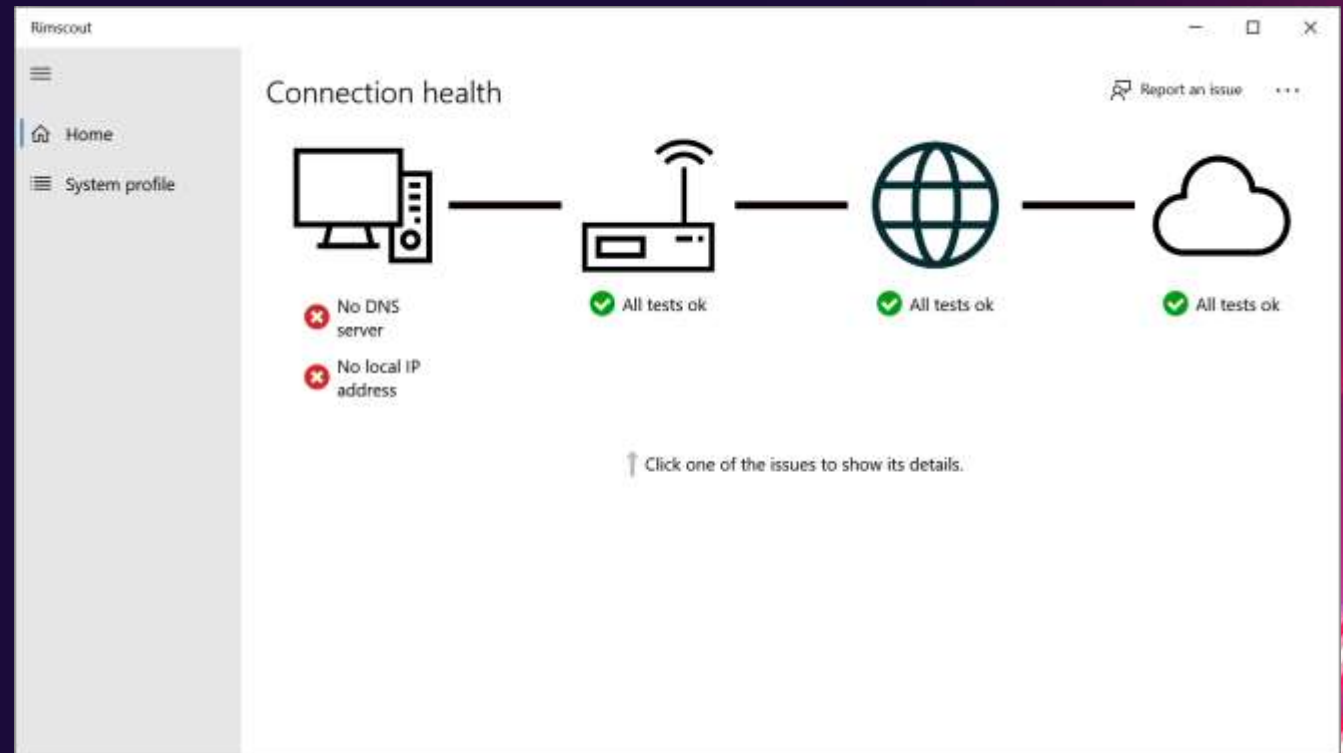


Durability

- Bandwidth vs. Lantency, Packetloss, Jitter, Throughput
- What's 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



Checklist/Summary

- Ensure optimized routing for Microsoft 365 services
 - Local Breakout, HTTP-Proxy-Bypass, skip Deep-Inspection
- Client-VPN
 - Use Split-VPN AND Split-DNS instead of TunnelVPN. Watch for IPv6-Tunnel
- Optimized DNS-Resolution
 - DNS follows IP-Routing, no „Google“-DNS or other Cloud-Filter-DNS
- Open UDP 3478-3481 for optimal Teams/Skype AV-Connection
 - Also think about optimizing WebEx, Zoom, Routers like Fritz!Box-GuestWLAN blocks UDP!
- Allow connection to CRL-Revocation lists
- Check TCP-Details
 - TCP-Connections, NAT-Limit, Session-Timeout, Keepalive
 - MTU/TCP Segment size, QoS-Tagging, Teams Portrange
 - Windows Scaling (MSS), RSS, Offloading, SACK
- Monitor Round Trip Time, not bandwidth