



Modul 4

Internetanbindung





Inhaltsvorschau

Was Sie in den nächsten
24 LE erwartet:



- Internetanbindung
 - Verfügbare Technologien
 - Auswahl einer Internetanbindung
 - Routing und NAT
- Internet-Sicherheit
 - Arten der Bedrohungen
 - Gegenmaßnahmen
 - Firewall-Technologien
 - Browser
- Remote Access
 - Verfügbare Technologien
 - Einrichtung eines VPN-Zugangs
 - Remoteunterstützung



Netzwerkadministrator

Internetanbindung



Verfügbare Technologien



Verfügbare Technologien

- Festnetzbasierte Technologien
DSL (ADSL, SDSL, VDSL...), Powerline Internet, „Fiber“
- Mobilfunkbasierte Technologien
2G (GPRS, EDGE), **3G** (HSPA/HSPA+), **4G** (LTE, WIMAX)
- Dedizierte Anbindungen
z.B. MPLS, LWL-Verbindungen



Festnetzbasierte Technologien

DSL – Digital Subscriber Line

- Hohe Bandbreiten (theoretisch 500-1000 MBit/s)
- Aufgebaut zwischen DSL-Modem und DSLAM (DSL Access Multiplexer)
- Stand der Technik, wird beständig weiterentwickelt



Festnetzbasierende Technologien

Powerline Internet

- Datenübertragung über das Stromnetz
- DSL-Protokolle auf Stromleitungen moduliert
- Randerscheinung (eher für einfaches Home-LAN und Babyphon)



Festnetzbasierte Technologien

„Fiber“ Internet

- Nur in vorab erschlossenen Gebieten oder Gebäuden
- Meist normales DSL („*fiber to the node*“ oder „*fiber to the basement*“)
- Keine reine LWL-Anbindung („*fiber to the home*“ oder „*fiber to the desk*“)



Festnetzbasierte Technologien – Zusammenfassung

- DSL
Telefon-Verkabelung, aktuell und weit verbreitet
- Powerline
DSL über das Stromnetz, exotische Randerscheinung
- Fiber
An vorbereiteten Standorten, als DSL mit höheren Bandbreiten



Mobilfunkbasierte Technologien

2G – Second Generation (GSM)

- **GPRS** (General Packet Radio Service), bis zu 171 KBit/s
- **EDGE** (Enhanced Data Rates for GSM Evolution), bis zu 473 KBit/s





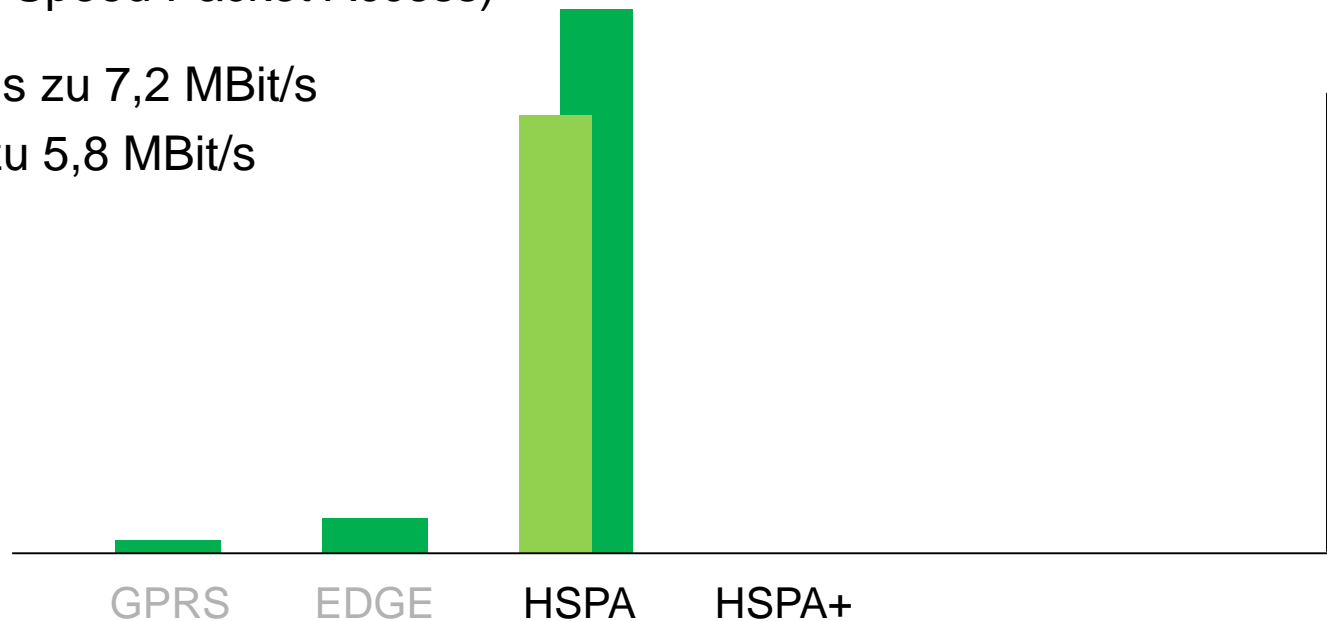
Mobilfunkbasierte Technologien

3G – Third Generation (UMTS)

- **HSPA** (High Speed Packet Access)

Download bis zu 7,2 MBit/s

Upload bis zu 5,8 MBit/s





Mobilfunkbasierte Technologien

3G – Third Generation (UMTS)

- **HSPA** (High Speed Packet Access)

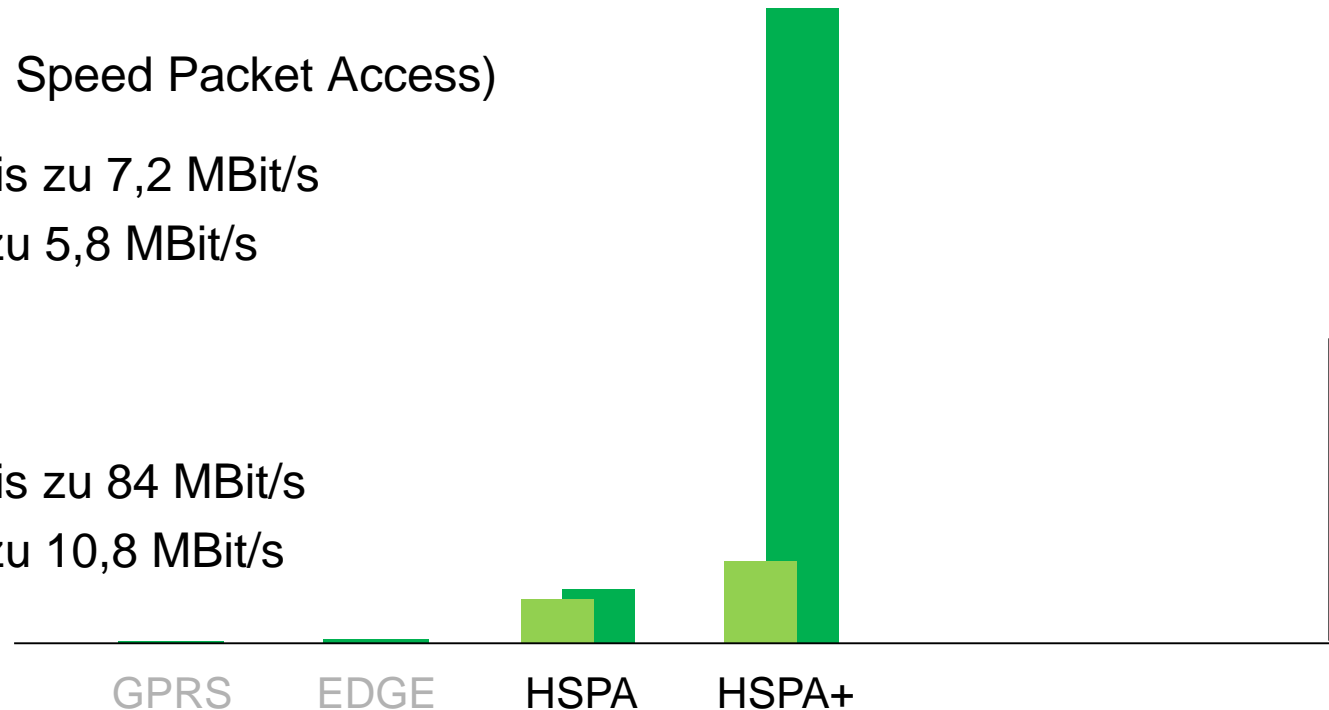
Download bis zu 7,2 MBit/s

Upload bis zu 5,8 MBit/s

- **HSPA+**

Download bis zu 84 MBit/s

Upload bis zu 10,8 MBit/s

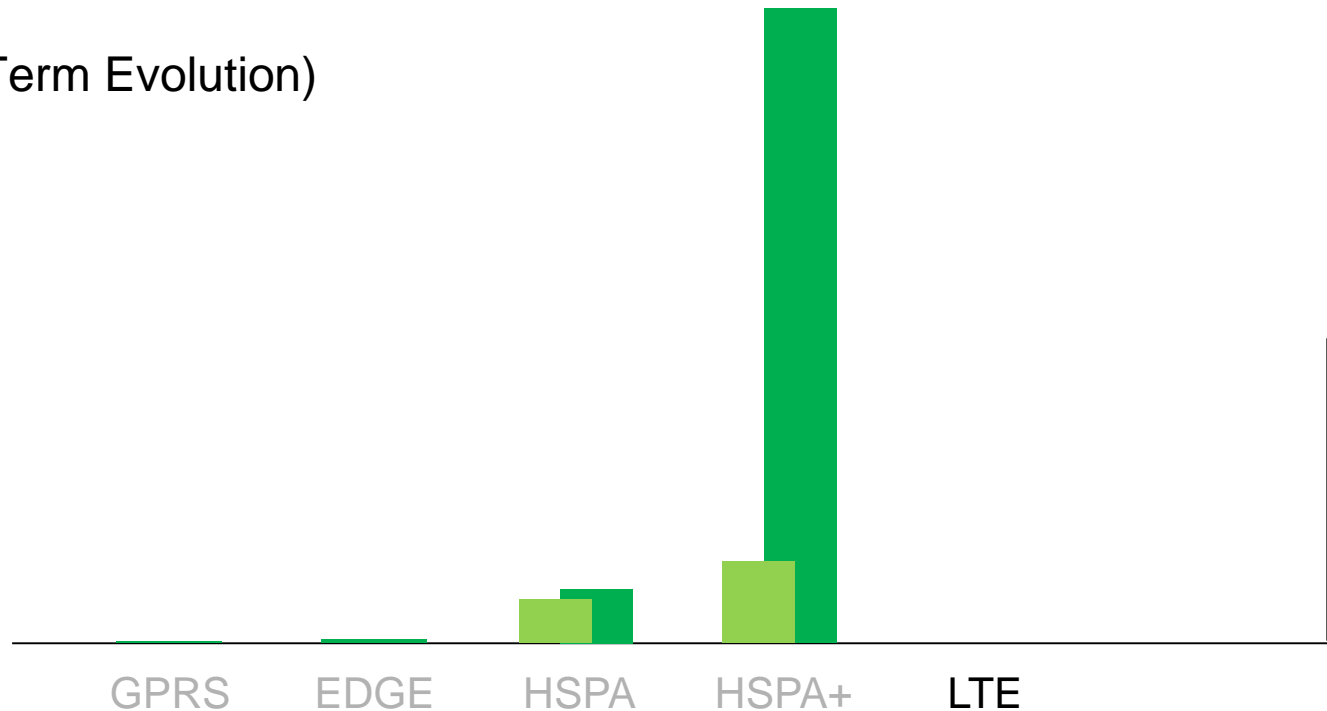




Mobilfunkbasierte Technologien

4G – Fourth Generation

- **LTE** (Long Term Evolution)

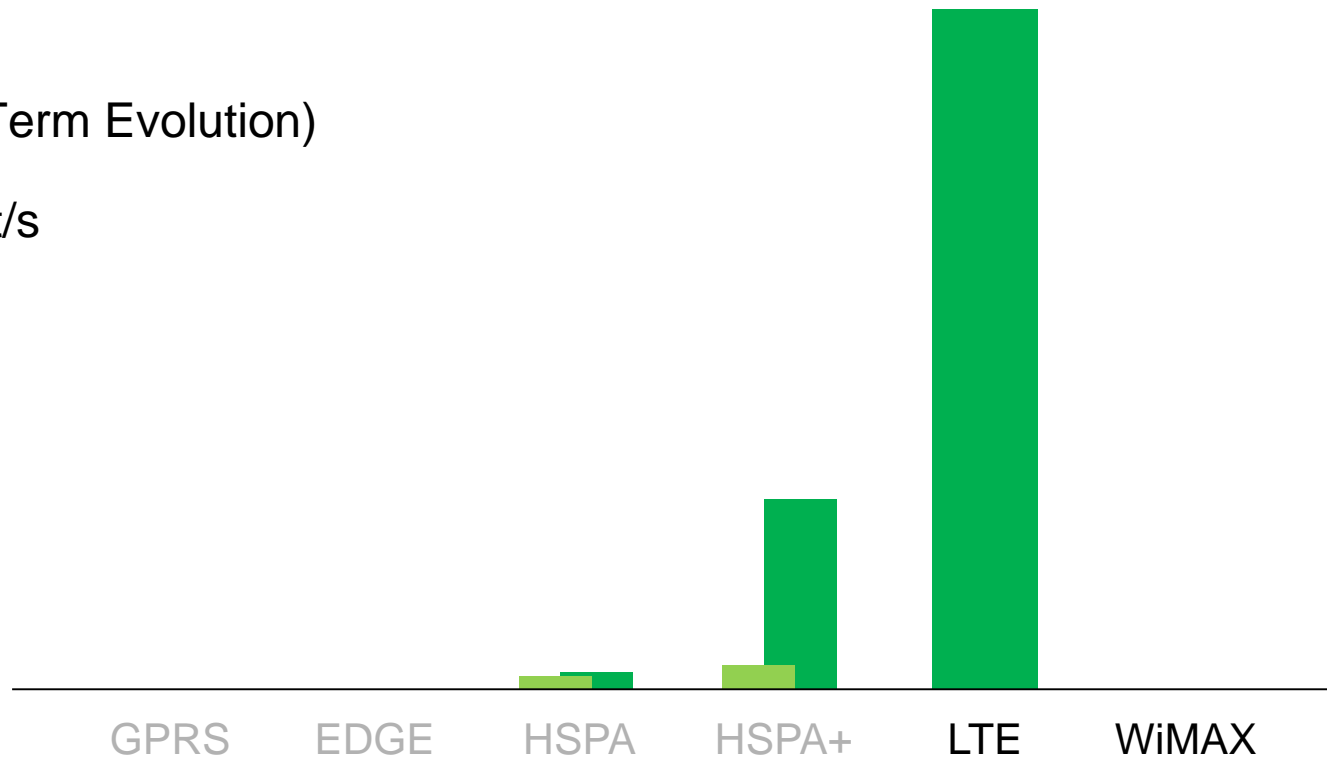




Mobilfunkbasierte Technologien

4G – Fourth Generation

- **LTE** (Long Term Evolution)
bis 300 MBit/s

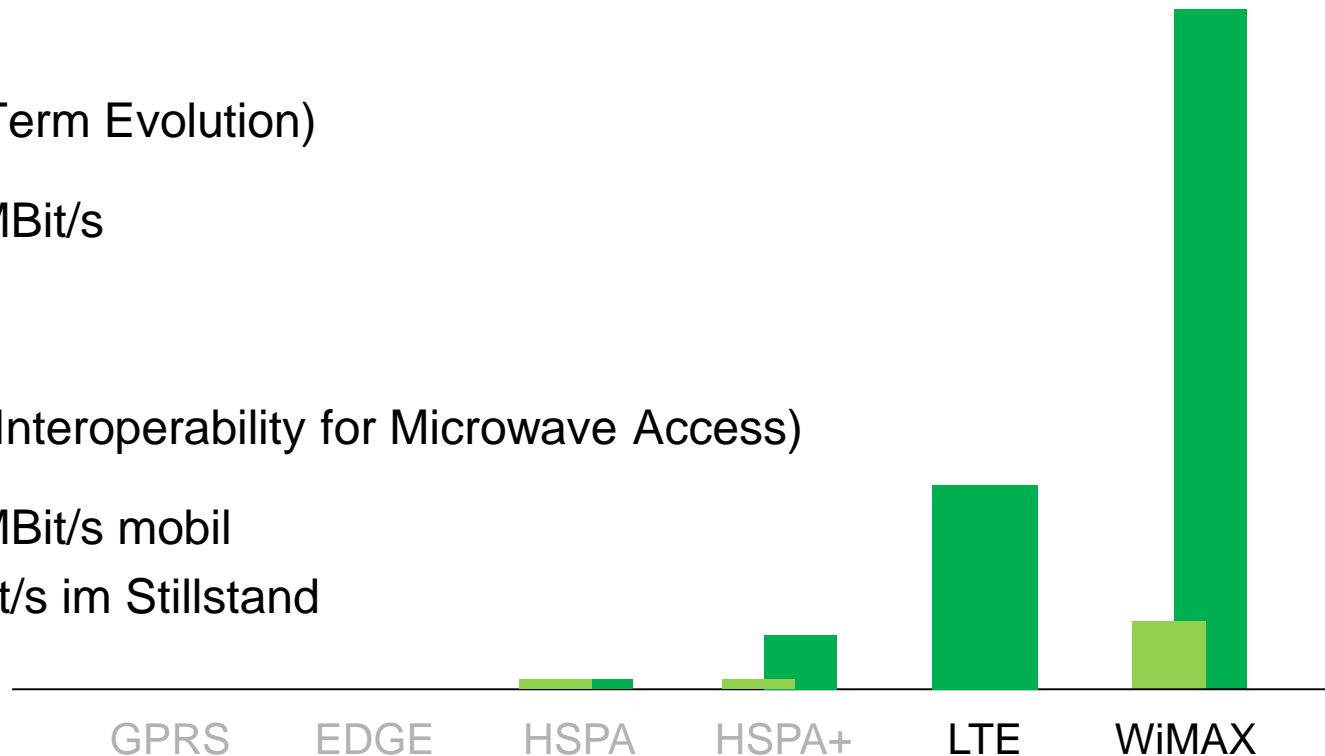




Mobilfunkbasierte Technologien

4G – Fourth Generation

- **LTE** (Long Term Evolution)
bis zu 300 MBit/s
- **WiMAX**
(Worldwide Interoperability for Microwave Access)
bis zu 100 MBit/s mobil
bis zu 1 GBit/s im Stillstand





Mobilfunkbasierte Technologien – Zusammenfassung

- **2G**

GPRS und **EDGE**
Abgelöster Standard (bzw. als fall-back-Lösung in schlecht versorgten Gebieten)

- **3G**

HSPA und **HSPA+**
Verbreiteter Standard

- **4G**

LTE und **WiMAX**
LTE in Ballungsräumen weit verbreitet, WiMAX hierzulande unüblich



Dedizierte Anbindungen

MPLS - Multiprotocol Label Switching

- Switching der Pakete anhand zusätzlicher Header (IP-Pakete) oder bestehender Header (ATM, Frame Relay)
- keine Paketzerlegung, sondern nur „Etikettierung“
- Verbindungsorientiert, zusätzliche Features möglich (VPN, Traffic Engineering)



Dedizierte Anbindungen

gemietete LWL-Direktverbindung

- Meistens IP-Verbindung ins Netz des Providers
- auch „providerfreier“ Betrieb mittels BGP-Router möglich
- Bandbreite meist nur rein vertraglich beschränkt



Dedizierte Anbindungen – Zusammenfassung

- MPLS
Hochperformantes Switching-Protokoll zur Bildung von Transportnetzen und verteilten Netzwerken
- LWL-Direktverbindung
Direkte, einzeln genutzte IP-Verbindung, entweder zum Provider oder direkt ins Carrier-Netzwerk



Fokus – DSL und Mobiles Internet

Im Folgenden näher betrachtet:

- DSL
 - Häufigst angetroffene Anbindung
 - Für die meisten Zwecke passende Varianten
- Mobiles Internet
 - Zunehmend höhere Bandbreiten
 - Fallweise auch als stationäre Anbindung



Netzwerkadministrator

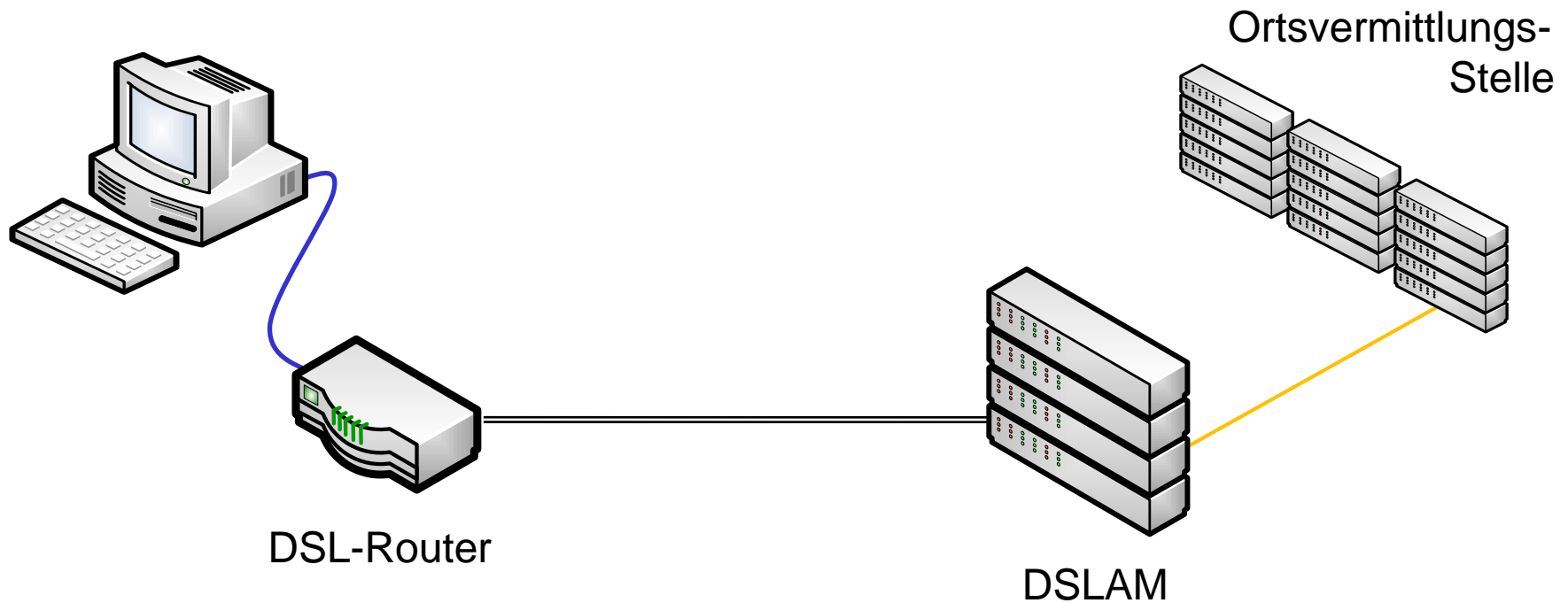
Internetanbindung



DSL – Digital Subscriber Line

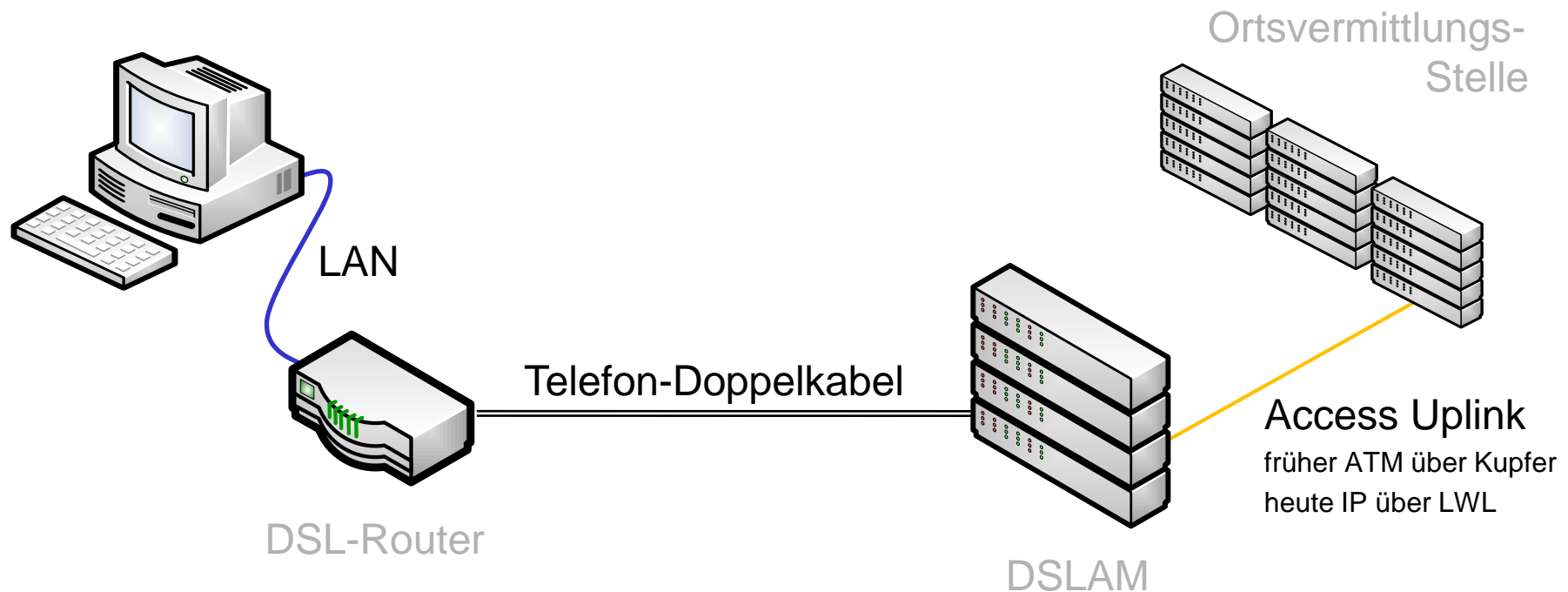


DSL: Geräte



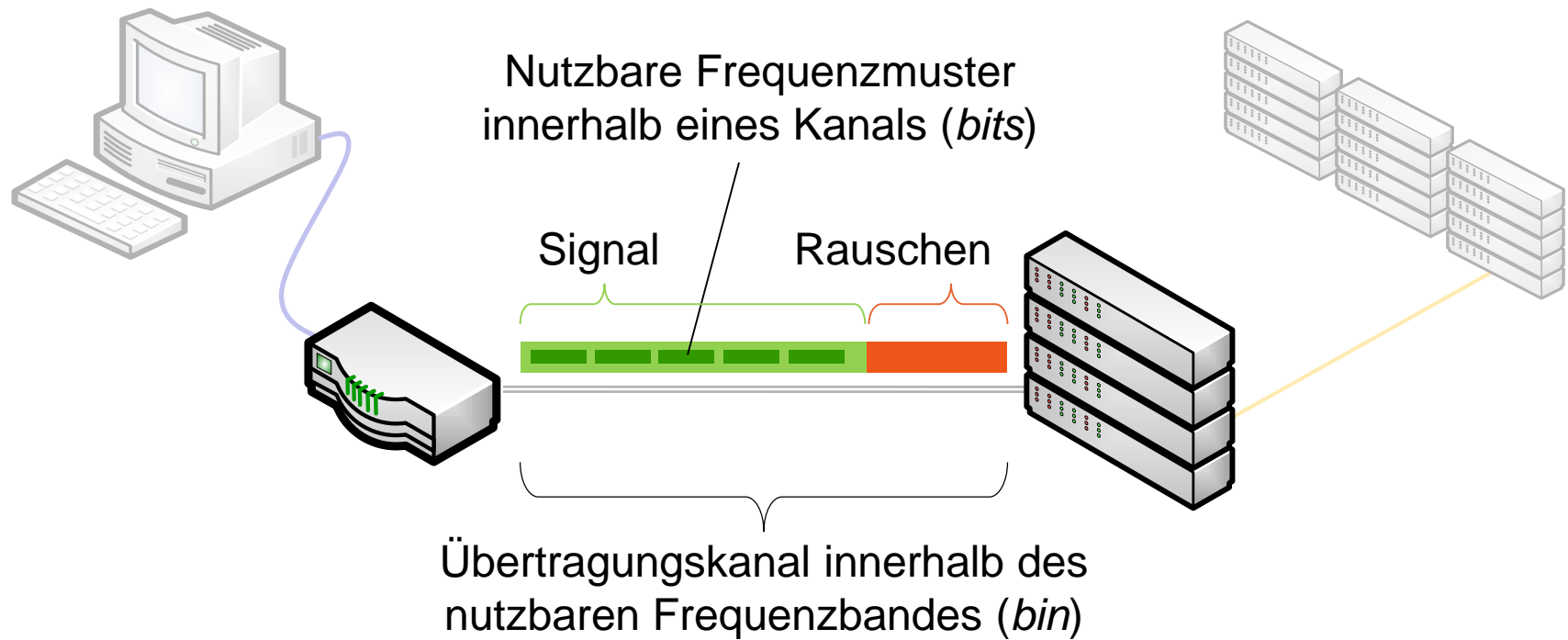


DSL: Verbindungen



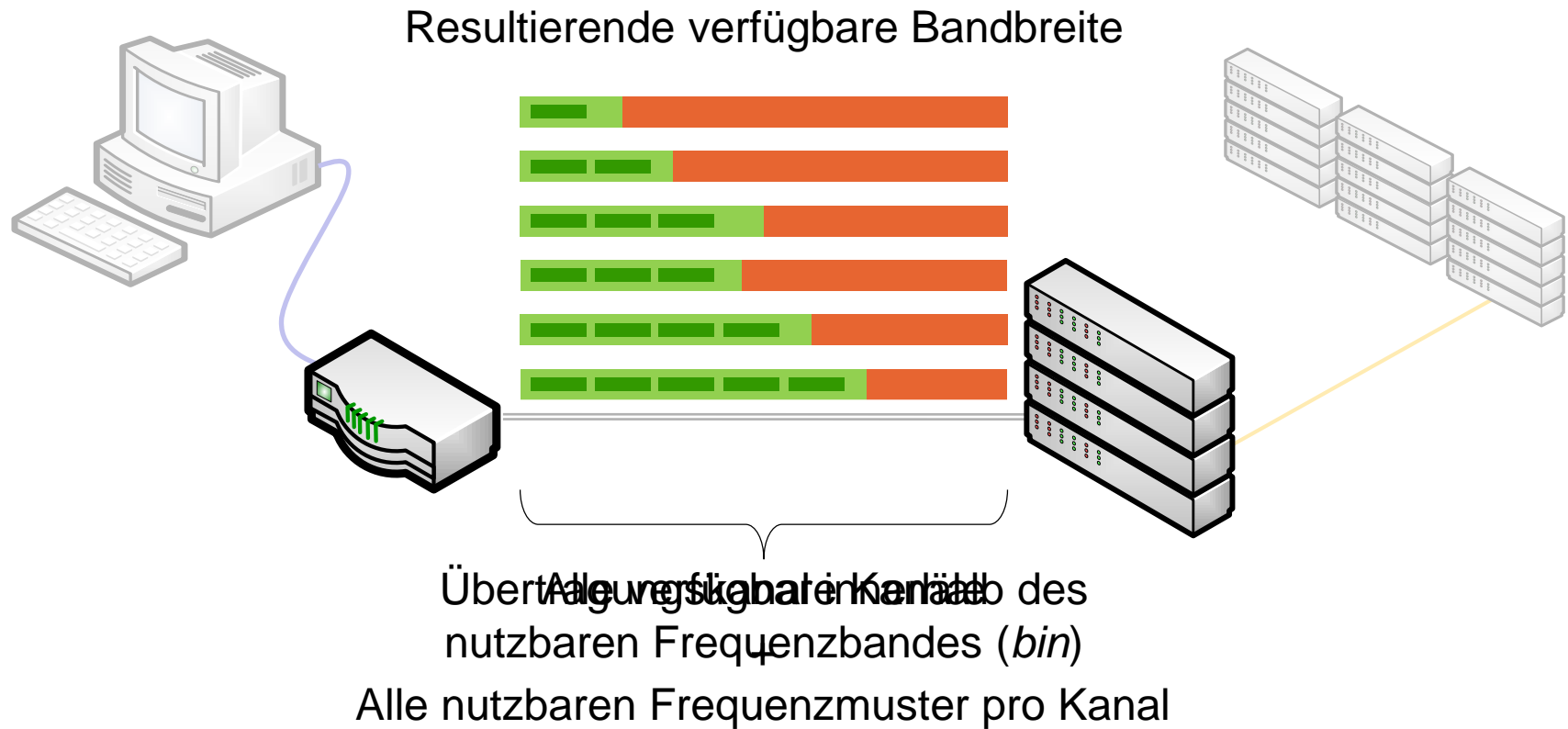


DSL: Synchronisierung





DSL: Synchronisierung

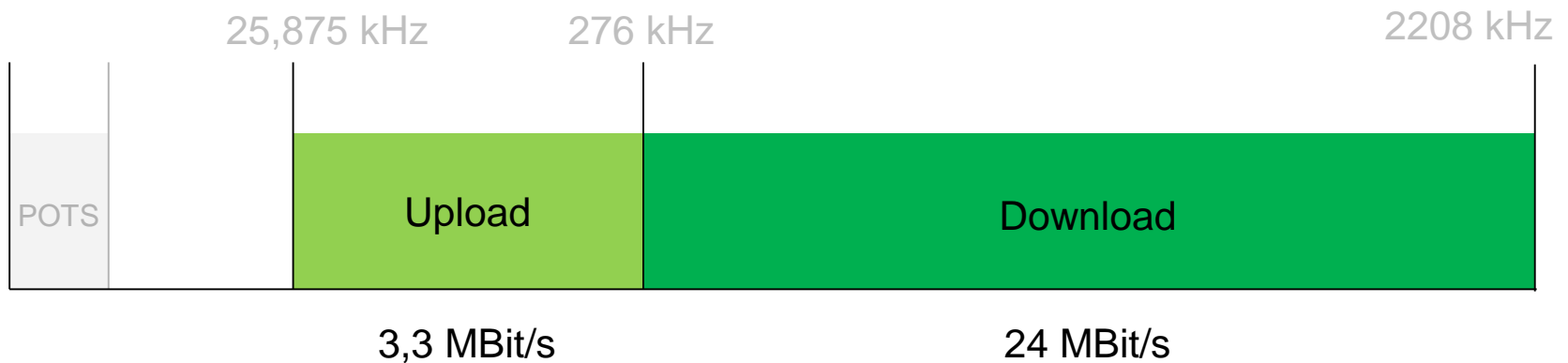




DSL: Symmetrie

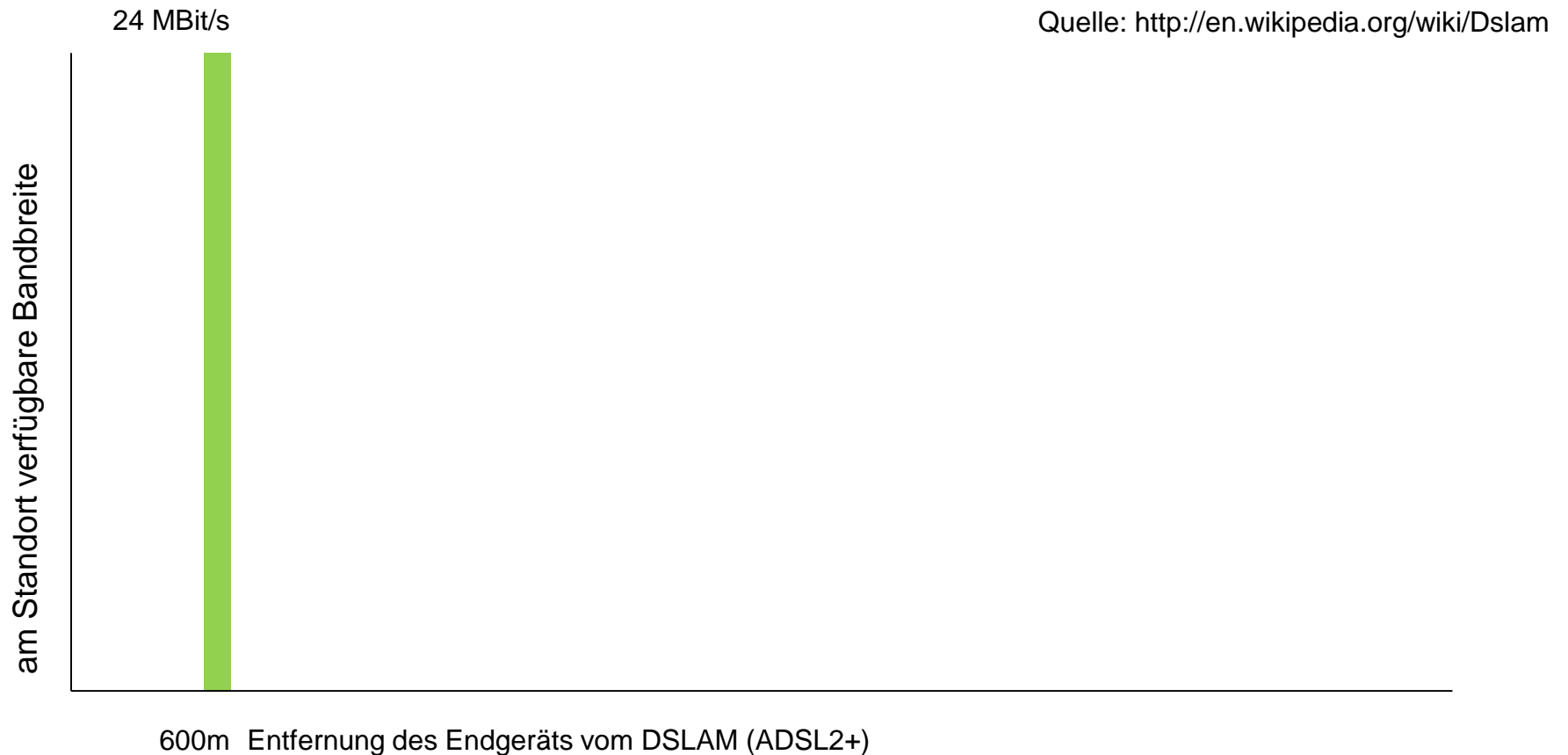
ADSL (Asymmetric Digital Subscriber Line)

Nach dem ADSL2+ Standard:



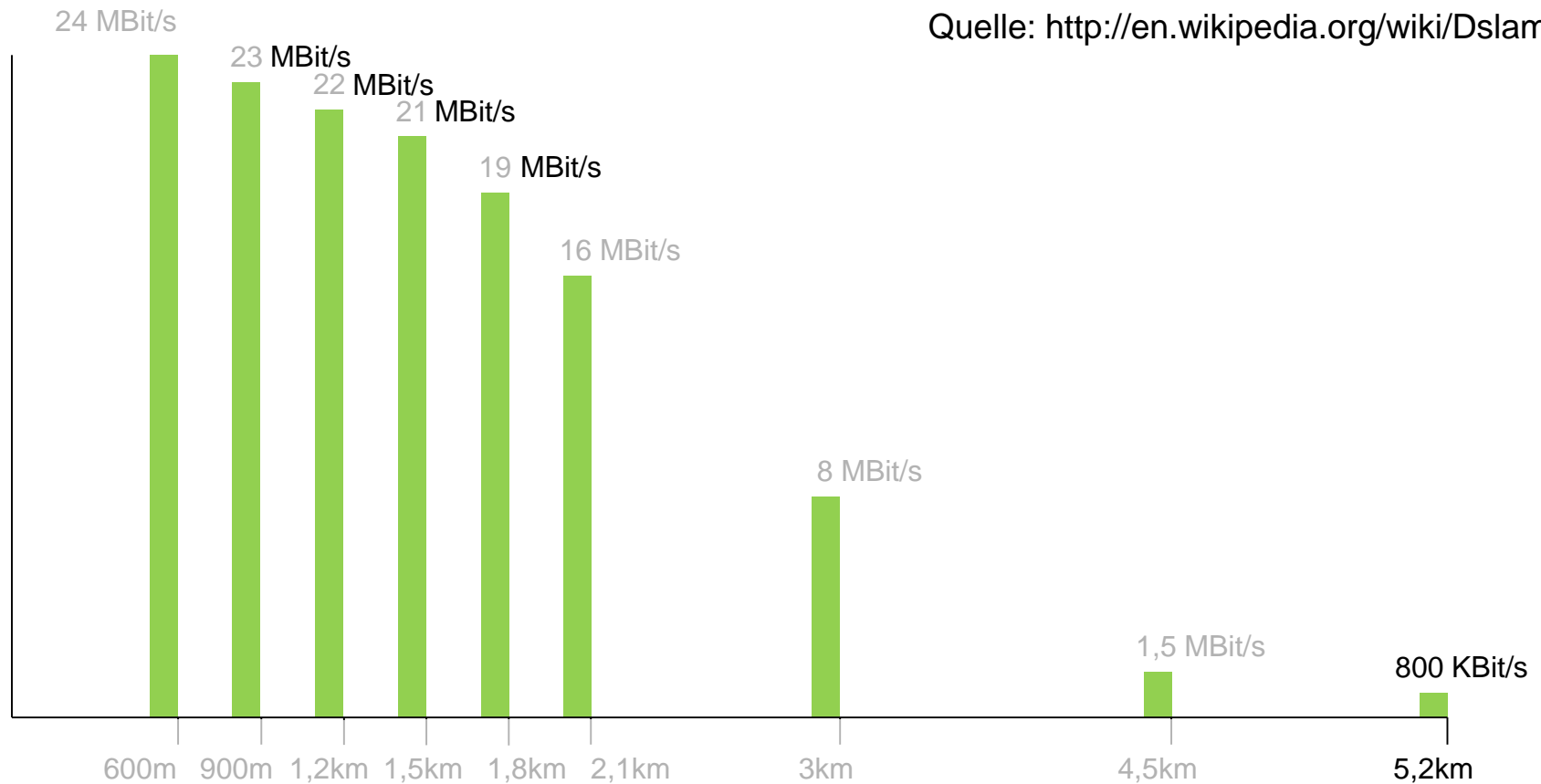


DSL: Leitungsdämpfung





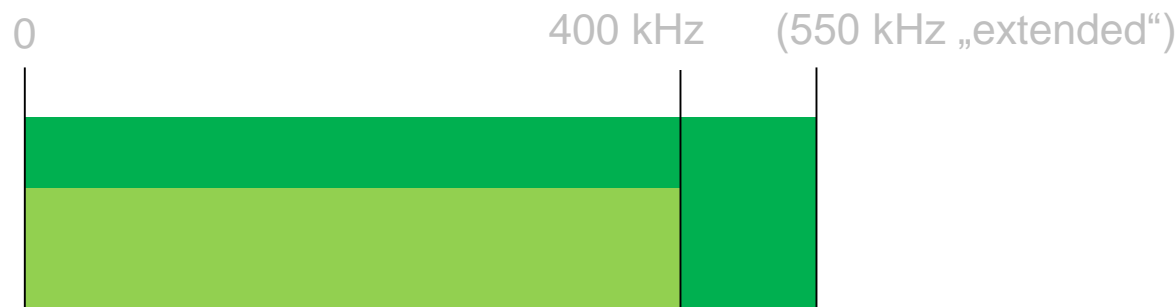
DSL: Leitungsdämpfung





DSL: SDSL

SDSL Symmetric Digital Subscriber Line (G.SHDSL Standard)



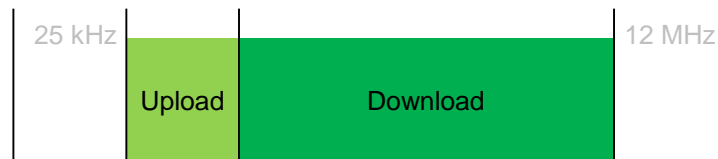
- bis zu 2,3 MBit/s pro Doppelkabel, „extended“ Mode bis zu 5,6 MBit/s
- Bündelung von bis zu vier Doppelkabeln
- Up- und Download auf denselben Frequenzen (Zeit-Multiplexing)
- Reichweite ca. 3km, keine parallele Sprachübertragung



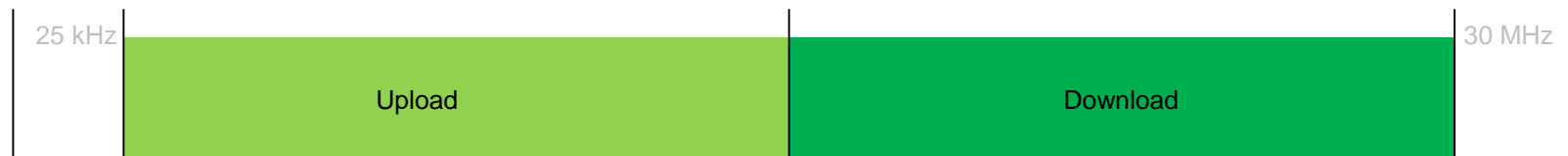
DSL: VDSL

VDSL Very-high-bit-rate Digital Subscriber Line (auch VHDSL)

- bis zu 3 MBit/s upstream und 55 MBit/s downstream



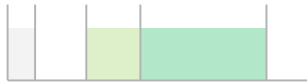
- VDSL2 bis zu 100MBit/s up- und downstream



- max. 300m Leitungslänge

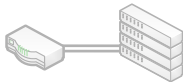
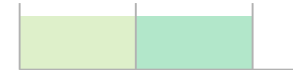


Zusammenfassung – DSL



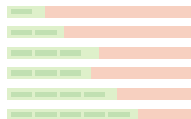
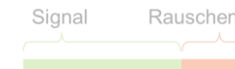
Asymmetrisch
als ADSL (ADSL2/2+)
oder VDSL

Symmetrisch
als SDSL
oder VDSL



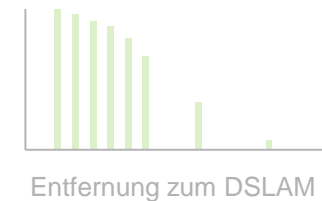
Aufgebaut
zwischen DSL-Router
und DLSAM

Bandbreite
wird bei der
Synchronisierung
ermittelt



Rechnerisch
hängt die Bandbreite
von *bits* und *bins* ab

Praktisch
sehr stark von der
Leitungsdämpfung





Netzwerkadministrator

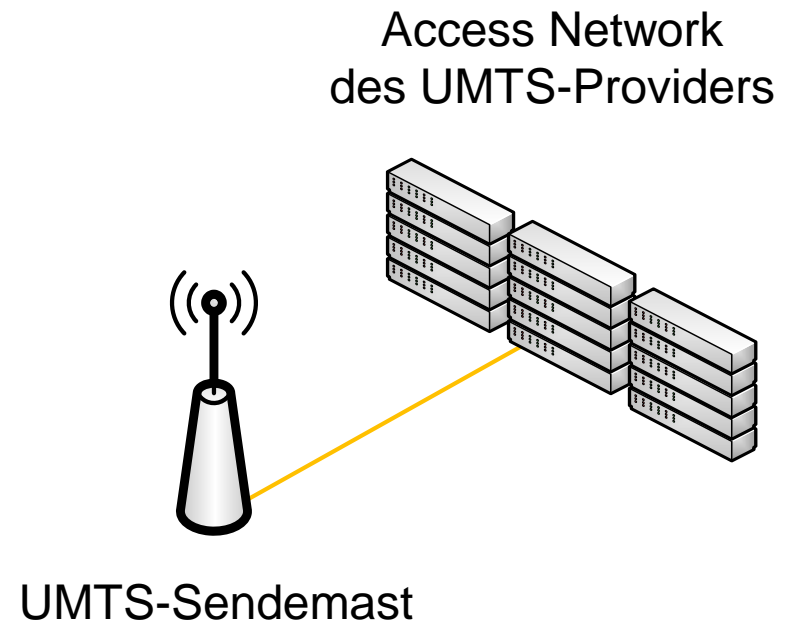
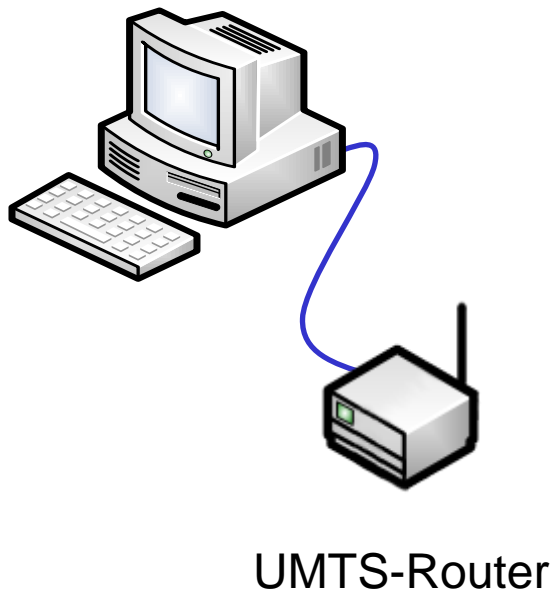
Internetanbindung



Mobiles Internet

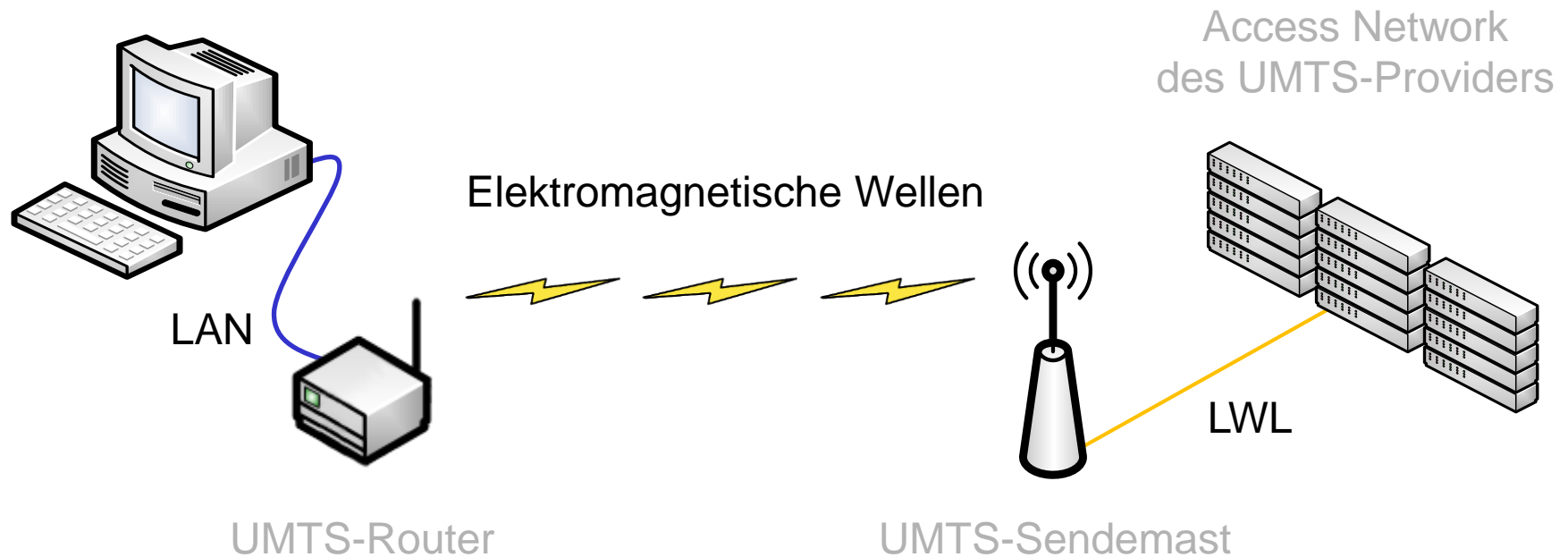


Mobiles Internet: Geräte



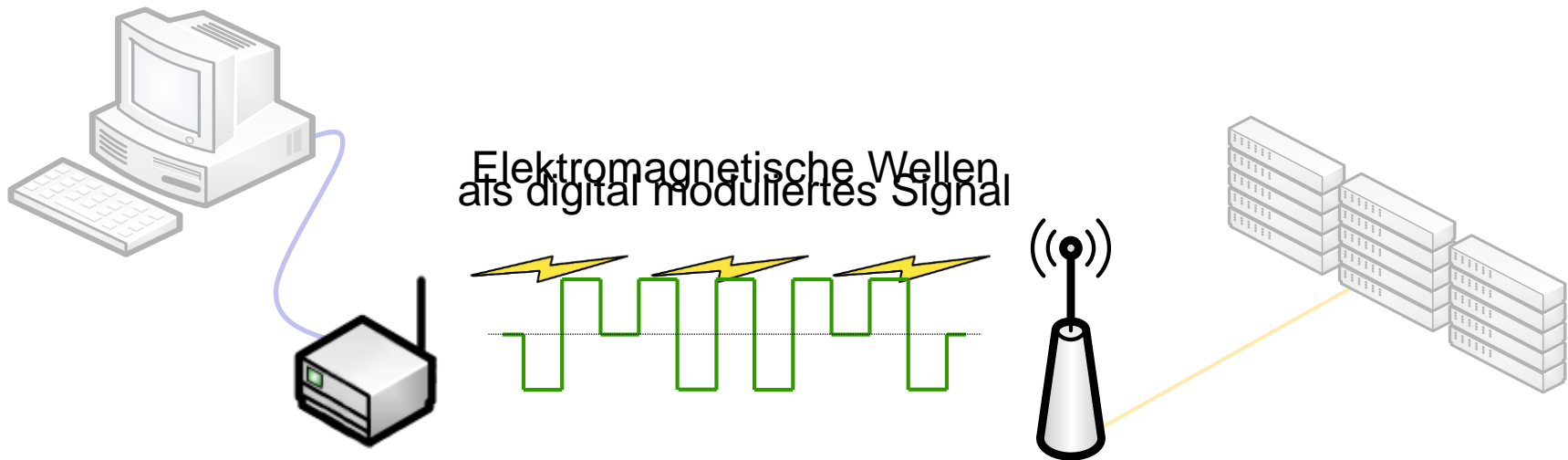


Mobiles Internet: Verbindungen



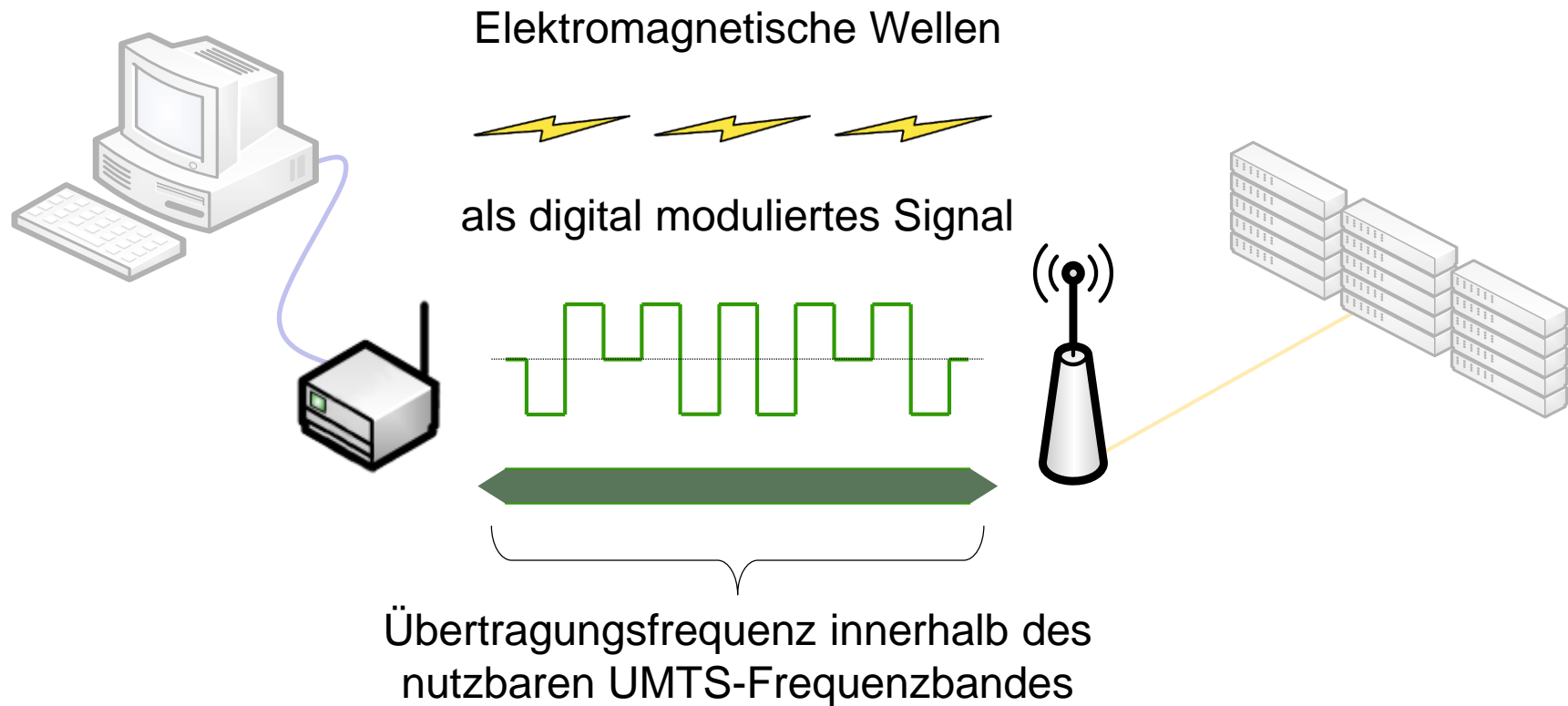


Mobiles Internet: Multiplexing



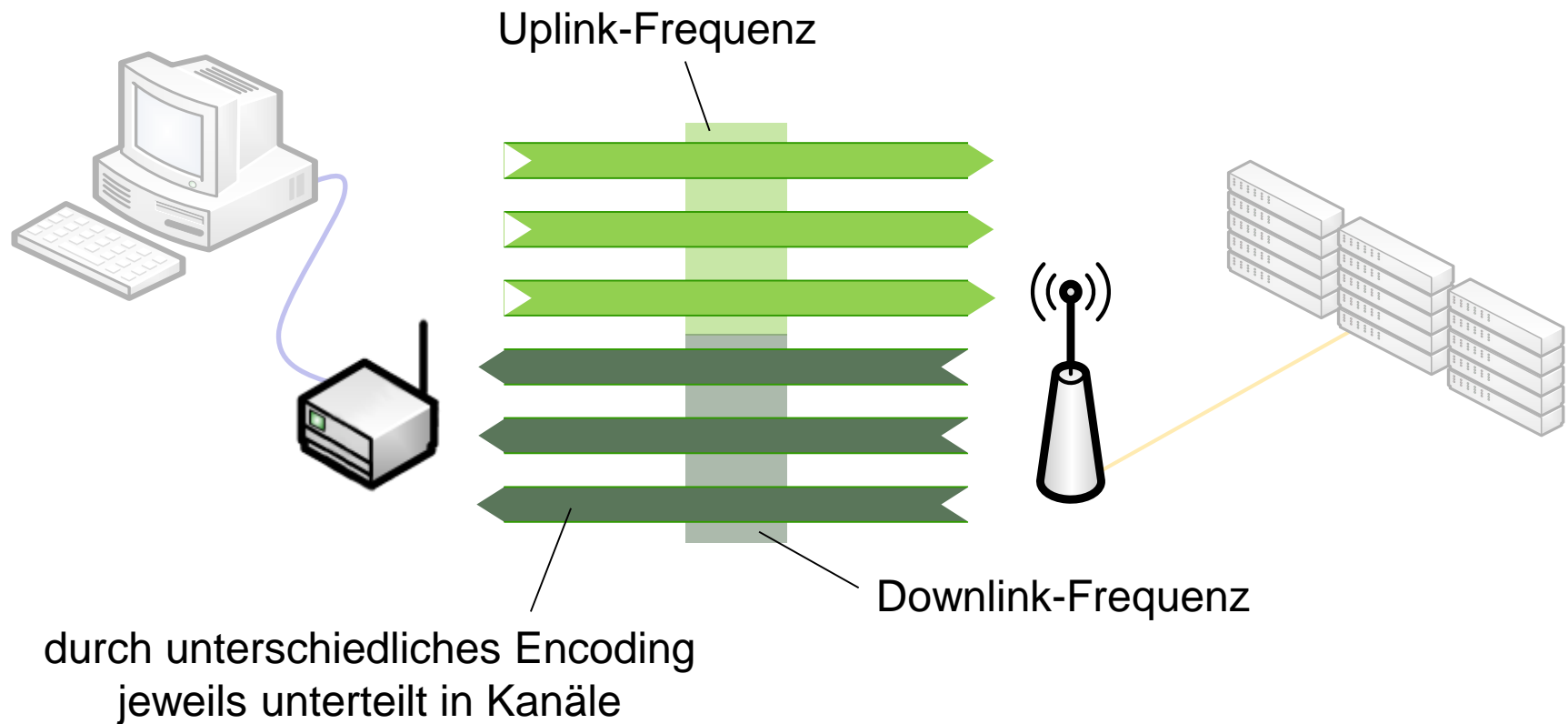


Mobiles Internet: Multiplexing



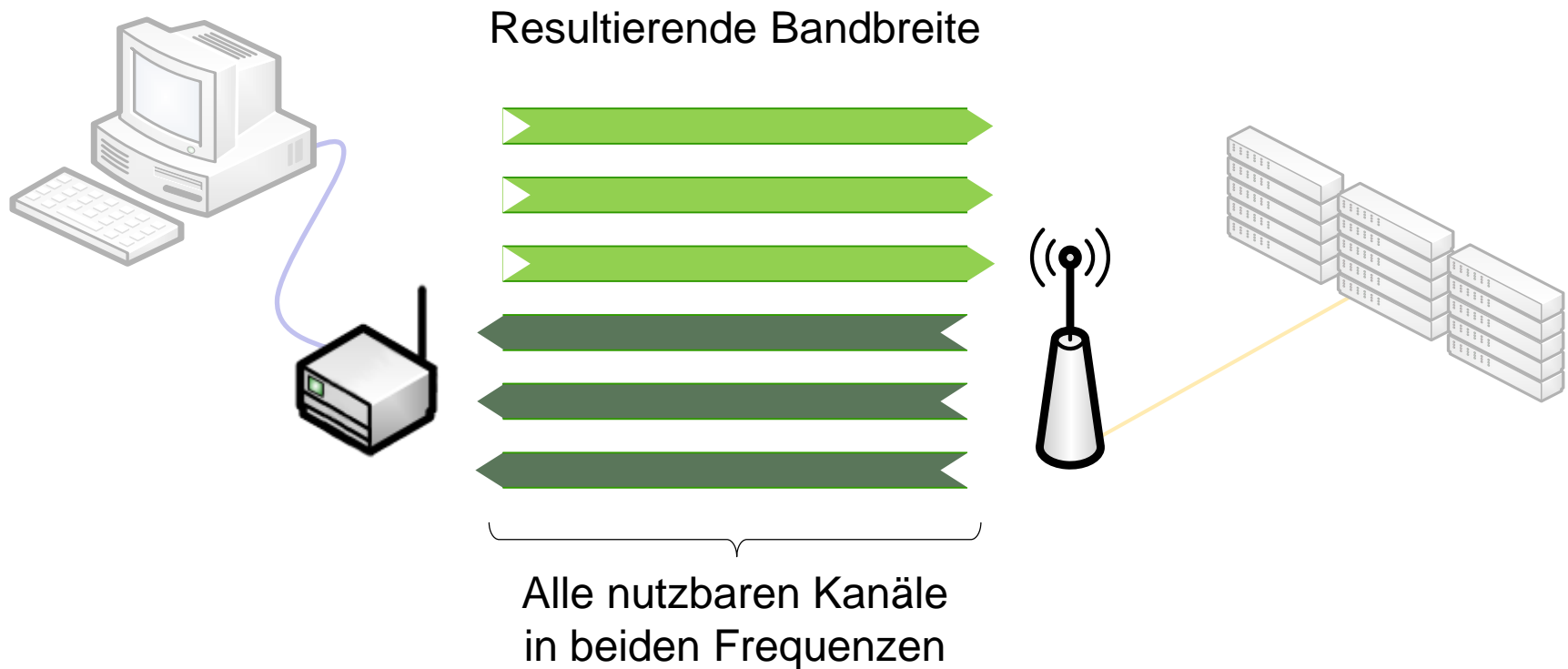


Mobiles Internet: Code Division Multiplexing



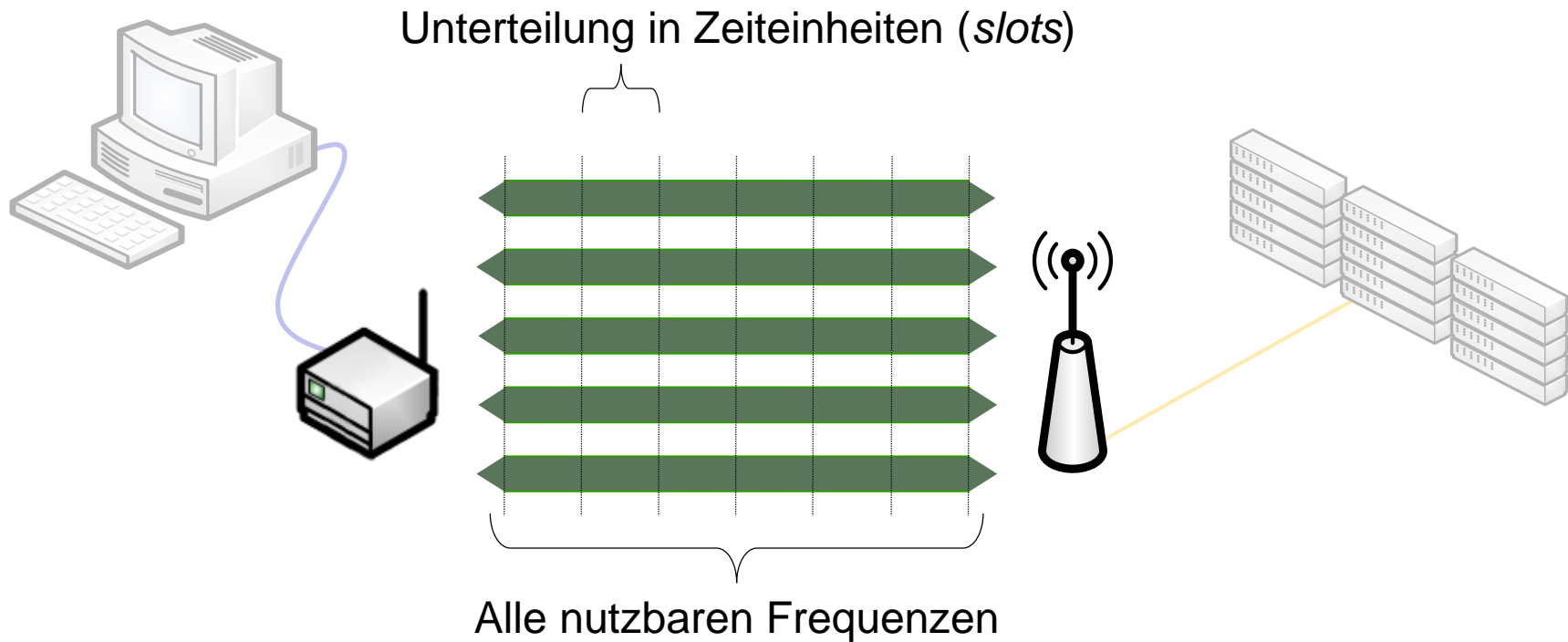


Mobiles Internet: Code Division Multiplexing



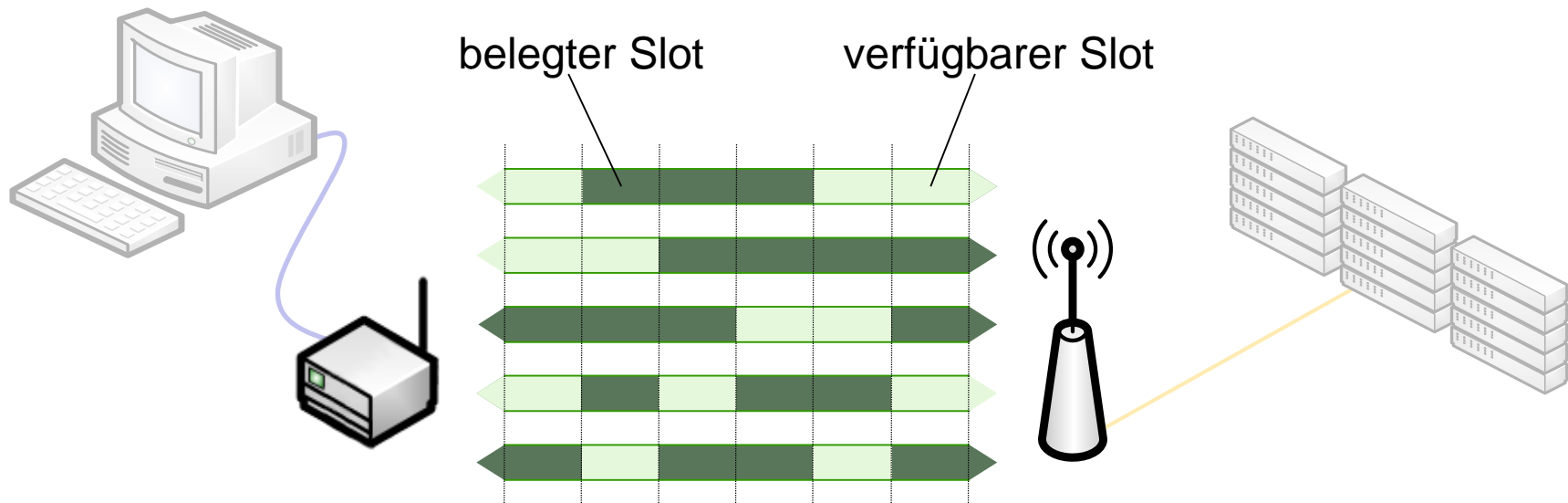


Mobiles Internet: Time Division Multiplexing



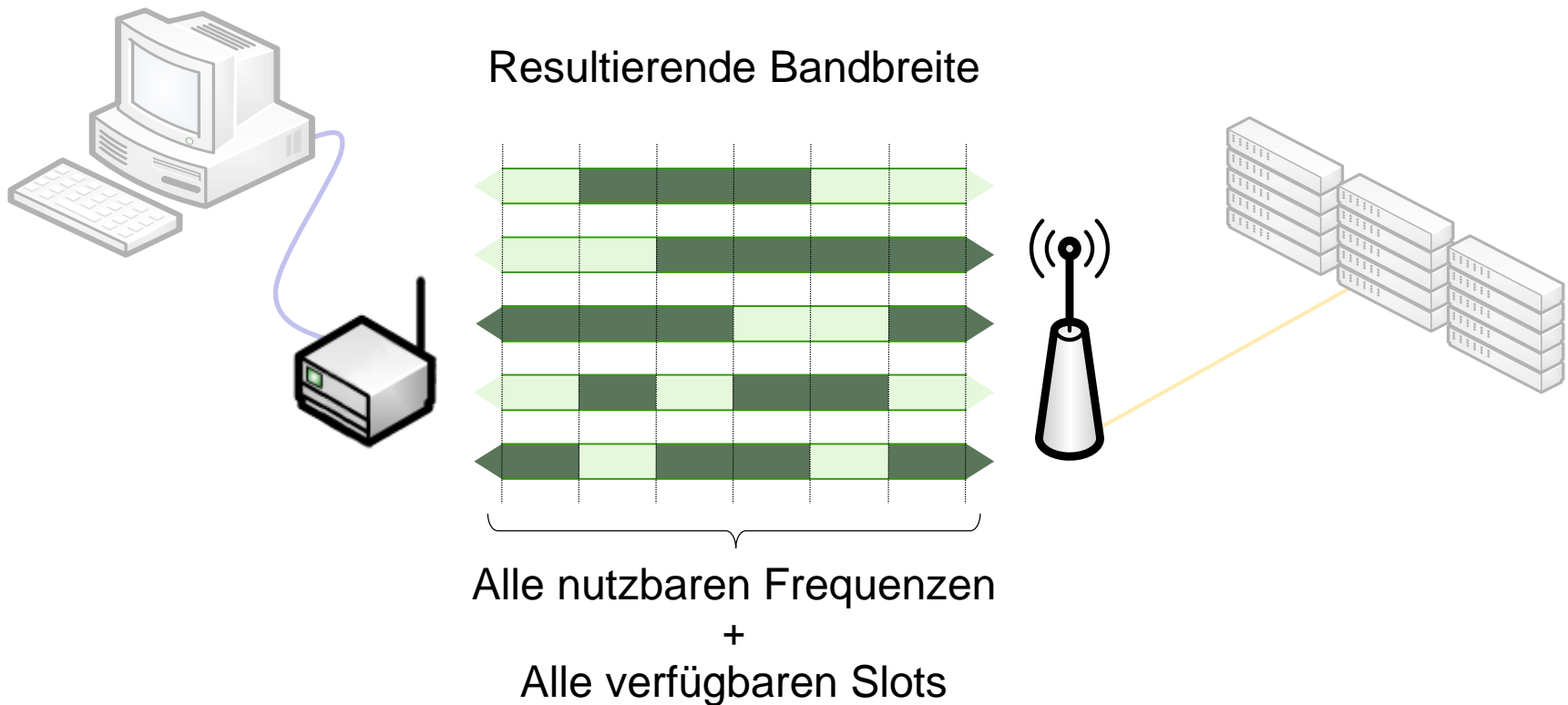


Mobiles Internet: Time Division Multiplexing



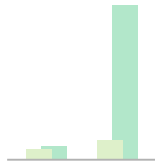


Mobiles Internet: Multiplexing



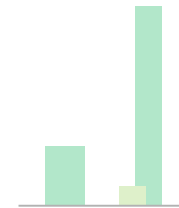


Zusammenfassung – Mobiles Internet



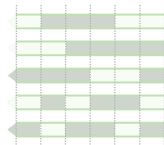
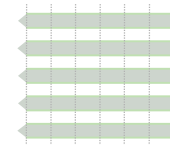
3G
HSPA und
HSPA+

4G
LTE und
WiMAX



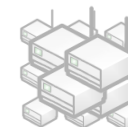
Aufgebaut
zwischen Endgerät
und Sendemast

Bandbreite
ist das Ergebnis
von Multiplexing



Rechnerisch
hängt die Bandbreite
von Kanälen
oder Zeitslots ab

Praktisch
auch von Abdeckung
und Zahl der Nutzer
und ist unvorhersehbar





Netzwerkadministrator

Internetanbindung



Auswahl einer Internetanbindung



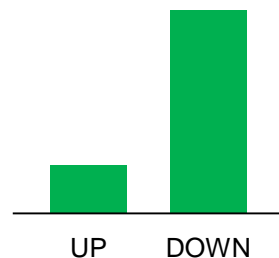
Auswahl einer Internetanbindung – Bandbreite

Anforderungsprofil eines Clients:



unternehmens-interner Client

Benötigte Bandbreite



berufliche Verwendung des Internet

- Websiteaufrufe / Recherche
- externe Webanwendungen
- Download / Streaming
- off-site Backup
- ...

private Verwendung des Internet (so erlaubt)

- Websiteaufrufe / social media
- Download / Streaming



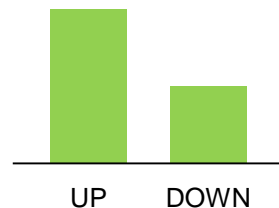
Auswahl einer Internetanbindung – Bandbreite und Symmetrie

Anforderungsprofil eines Clients:



unternehmens-externer Client

Benötigte Bandbreite



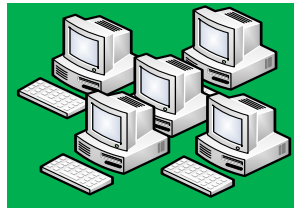
Nutzung des Unternehmensnetzwerks

- VPN
- Remote Desktop
- Support / Download
- on-site Hosting (Web, Mail etc.)
- zentrale Datensicherung
- zentrale Virenschutzlösung
- ...



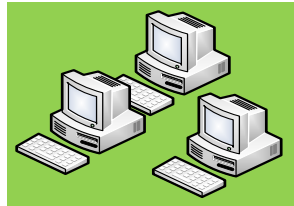
Auswahl einer Internetanbindung – Bandbreite und Symmetrie

Interne Clients



+

Externe Clients

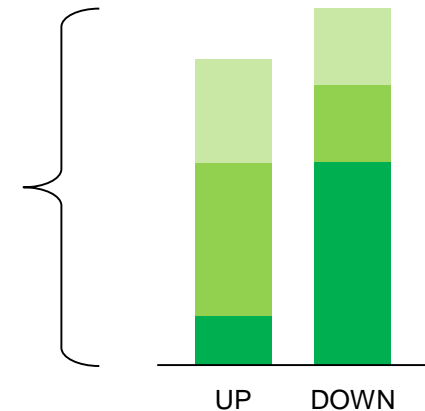


+

Sonstiges

- Fernwartung
- Außenstellen
- etc.

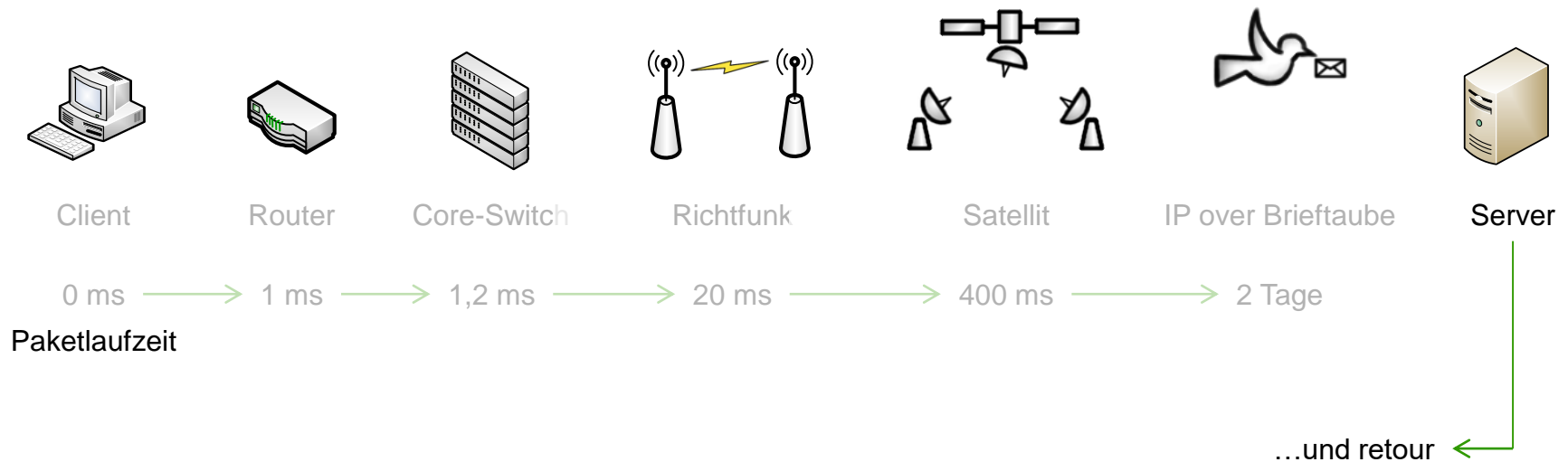
Erforderliche
Bandbreite



Benötigte Symmetrie

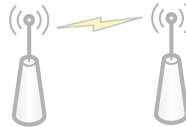
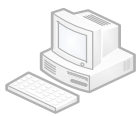


Auswahl einer Internetanbindung – Round-Trip-Time





Auswahl einer Internetanbindung – Round-Trip-Time



Kurze RTT benötigen z.B.:

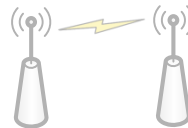
- IP-Telefonie
- Web-Conferencing
- Remote-Desktop
- Virtual Desktop

Unempfindlich bezüglich RTT:

- Download
- Streaming
- Datenversand (FTP, SCP, Torrent...)
- Mail-Verkehr



Auswahl einer Internetanbindung – Round-Trip-Time



Kurze RTT bieten z.B.:

- LWL
- MPLS
- DSL (oft insbesondere SDSL)

Lange RTT tritt meist auf bei:

- Satellitenverbindungen
- Richtfunk (teilweise WLAN)
- Mobilem Internet



Auswahl einer Internetanbindung – Transfervolumen

Hohes Transfervolumen verursachen z.B.:

- Download / Streaming / Datenversand
- on-site Hosting
- off-site Backup
- Desktopvirtualisierung
- Massenmailing

Geringes Transfervolumen reicht z.B. für:

- IP-Telefonie
- textbasierte eMails
- Web-Recherche (textintensive Seiten)



Auswahl einer Internetanbindung – Transfervolumen

Hohes Transfervolumen bieten:

- DSL
- LWL (*light fiber*)
- mobile *flat-rate*

Oft nach Transfervolumen abgerechnet:

- LWL (*dark fiber*)
- Satellitenverbindungen
- die meisten Mobilfunkverträge



Auswahl einer Internetanbindung – Verfügbarkeit

98,5% garantierte Verfügbarkeit!

...gut?

...schlecht?



Auswahl einer Internetanbindung – Verfügbarkeit

98,5% Verfügbarkeit im Detail:

Eine Kalenderwoche hat 10080 Minuten.

98,5% davon sind 9928,8 Minuten.

Das ergibt eine Differenz von 151,2 Minuten.

Die Leitung darf also jede Woche zweieinhalb Stunden lang ausfallen.

...schlecht!



Auswahl einer Internetanbindung – Verfügbarkeit

Hohe Verfügbarkeit benötigen z.B. Unternehmen, die:

- bei Stillstand Geld verlieren
 - Webshop-Betreiber
 - online-Wertpapierhändler
 - ...
- selbst Leitungsprodukte anbieten
 - Server-Housing
 - Webhosting
 - ...
- nicht produzieren können
 - Web-Designer
 - Nachrichtenagenturen
 - ...
- eventuell Fristen versäumen
 - Anwälte und Notare
 - Planungsbüros
 - ...



Auswahl einer Internetanbindung – Verfügbarkeit

Auch 99,9% sind nicht gleich 99,9%

Beurteilungszeitraum: 1 Woche

$$7 \times 24 \times 60 = 10080$$

$$10080 \times 0,999 = 10069,92$$

$$10069,92 - 10080 = -10,08$$

Maximale Ausfallsdauer: 10 Minuten

Beurteilungszeitraum: 3 Monate

$$91 \times 24 \times 60 = 131040$$

$$131040 \times 0,999 = 130908,96$$

$$131040 - 130908,96 = 131,04$$

Maximale Ausfallsdauer: über 2 Stunden



Auswahl einer Internetanbindung – Verfügbarkeit

Oft billiger als 99,999%: Redundante Anbindung

Echte redundante Anbindung

- nutzt nicht dieselbe Technologie
- ist nicht vom selben Anbieter

Idealerweise

- zahlt man erst bei Nutzung
- ist die Umschaltzeit gering



Auswahl einer Internetanbindung – SLA

SLA – Service Level Agreement

Ein SLA definiert

- die Verfügbarkeit des Produktes
- einen Beurteilungszeitraum für diese
- mindestens den Beginn der Störungsbehebung
- idealerweise einen Behebungszeitraum
- die Rechte des Kunden bei Nichterfüllung



Auswahl einer Internetanbindung – Adressierung

Statische IP-Adresse

Die IP-Adresse bleibt bei jedem Verbindungsaufbau die selbe.

- LWL
- meist SDSL
- generell Business-Produkte

Dynamische IP-Adresse

Die IP-Adresse kann sich mit jedem Aufbau der Verbindung ändern.

- Mobiles Internet
- häufig ADSL
- generell Privat-Produkte



Auswahl einer Internetanbindung – Adressierung

Statische öffentliche IP-Adressen benötigen z.B. Unternehmen, die

- Server hosten
- Anwendungen veröffentlichen
- VPN betreiben
- Remote Desktops verwenden
- auf Firewalls ihrer Kunden und Anbieter freigeschaltet werden müssen



Auswahl einer Internetanbindung – Adressierung

Wie viele Adressen werden benötigt?

Den Betrieb mehrerer Dienste an einer IP ermöglichen

- Firewalls, Proxy Server und Load Balancer
- Dienste auf unterschiedlichen Sockets (HTTP, SMTP, VPN...)



Auswahl einer Internetanbindung – Adressierung

Eigene, separate öffentliche IP-Adressen benötigen

- Dienste auf denselben Sockets (SSTP, HTTPS)
- Dienste auf unterschiedlichen Plattformen (IIS und Apache...)
- erforderliche Reverse-DNS-Einträge



Auswahl einer Internetanbindung – Routing oder NAT

Routing

Die öffentlichen IP-Adressen werden an die Geräte des Leitungskunden durchgereicht .

- eigene Firewall erforderlich
- größere Flexibilität
- üblich bei Business-Produkten

NAT

Die öffentliche IP-Adresse liegt am Router des Providers an, die Geräte des Leitungskunden bekommen nur private IP-Adressen.

- Firewall meist integriert
- weniger Konfigurationsaufwand
- generell bei Privat-Produkten und mobilem Internet



Zusammenfassung – Auswahl einer Internetanbindung



Dimensionieren
der Bandbreite
und Symmetrie

Feststellen
der zulässigen
Round-Trip-Time



Erfassen
des benötigten
Transfervolumens

Festlegen
der benötigten
Verfügbarkeit

99
99,9
99,99
99,999

/28
/29
/30
/32

Ermitteln
der erforderlichen
Anzahl an IP-Adressen

Auswählen
von Routing
oder NAT

0
1



Netzwerkadministrator

Internetanbindung



Umsetzung der Anbindung

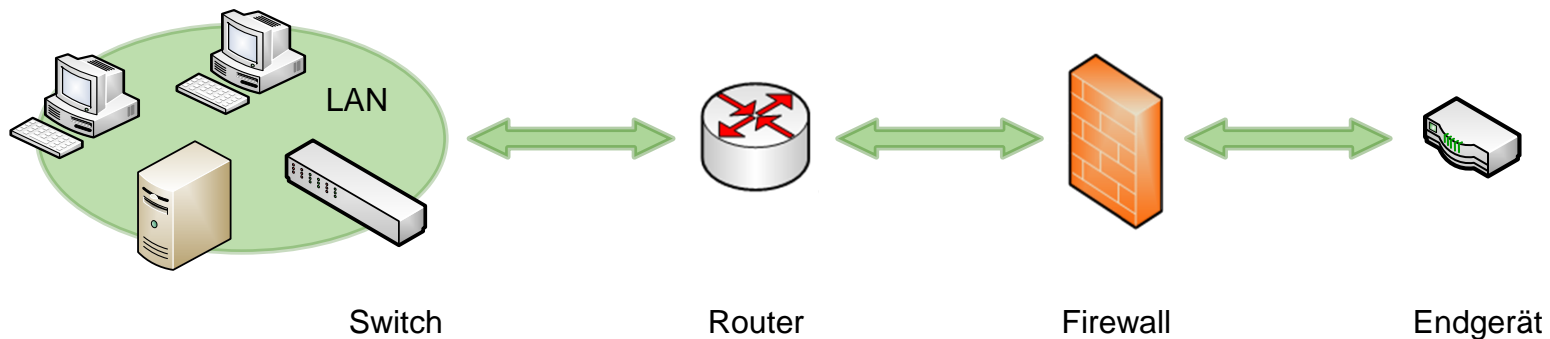


Umsetzung der Anbindung – Herstellungsvoraussetzungen

Anbindungsart	Schlüsselkriterium
DSL	Leitungs-Verfügbarkeit
mobiles Internet	Netz-Abdeckung
Dedizierte Anbindung	Kosten



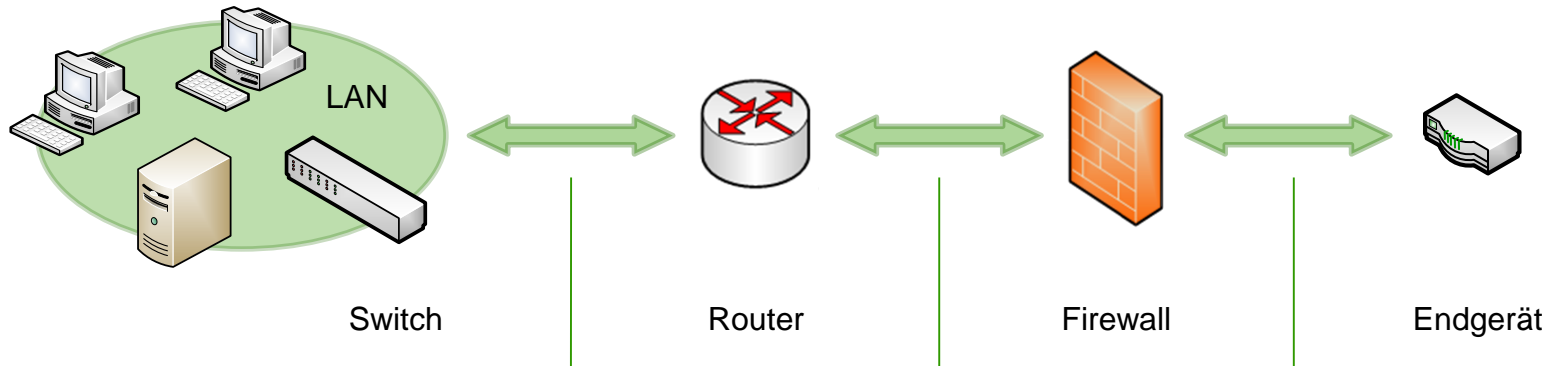
Umsetzung der Anbindung – Lokale Infrastruktur



- Welche Geräte sind vorhanden?
- Welche Geräte stellt der Provider?
- Welche Geräte werden benötigt?



Umsetzung der Anbindung – Lokale Infrastruktur



Home Office

Ein Gerät

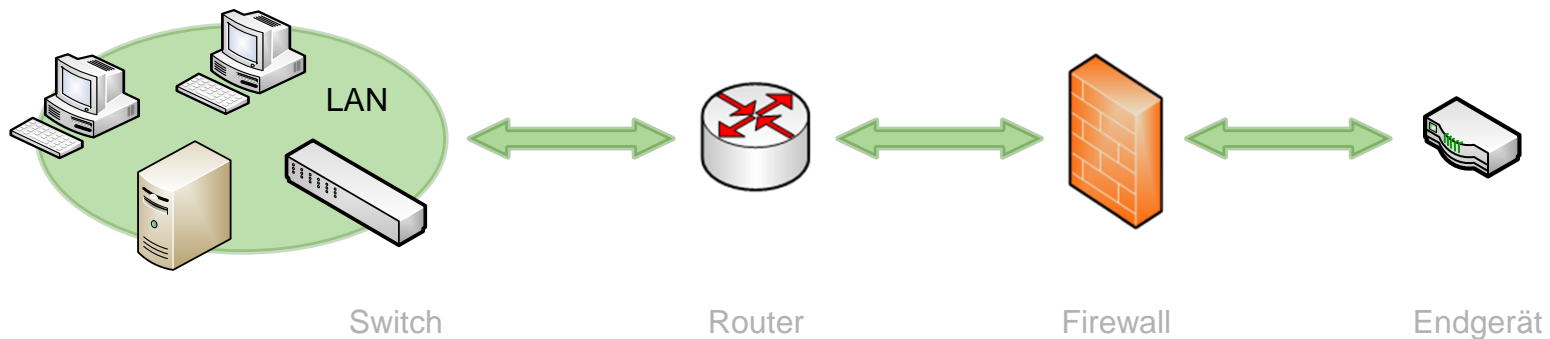
Kleinunternehmen

Mittleres Unternehmen

Mehrere Gebäude,
Stockwerke, Standorte



Umsetzung der Anbindung – Lokale Infrastruktur

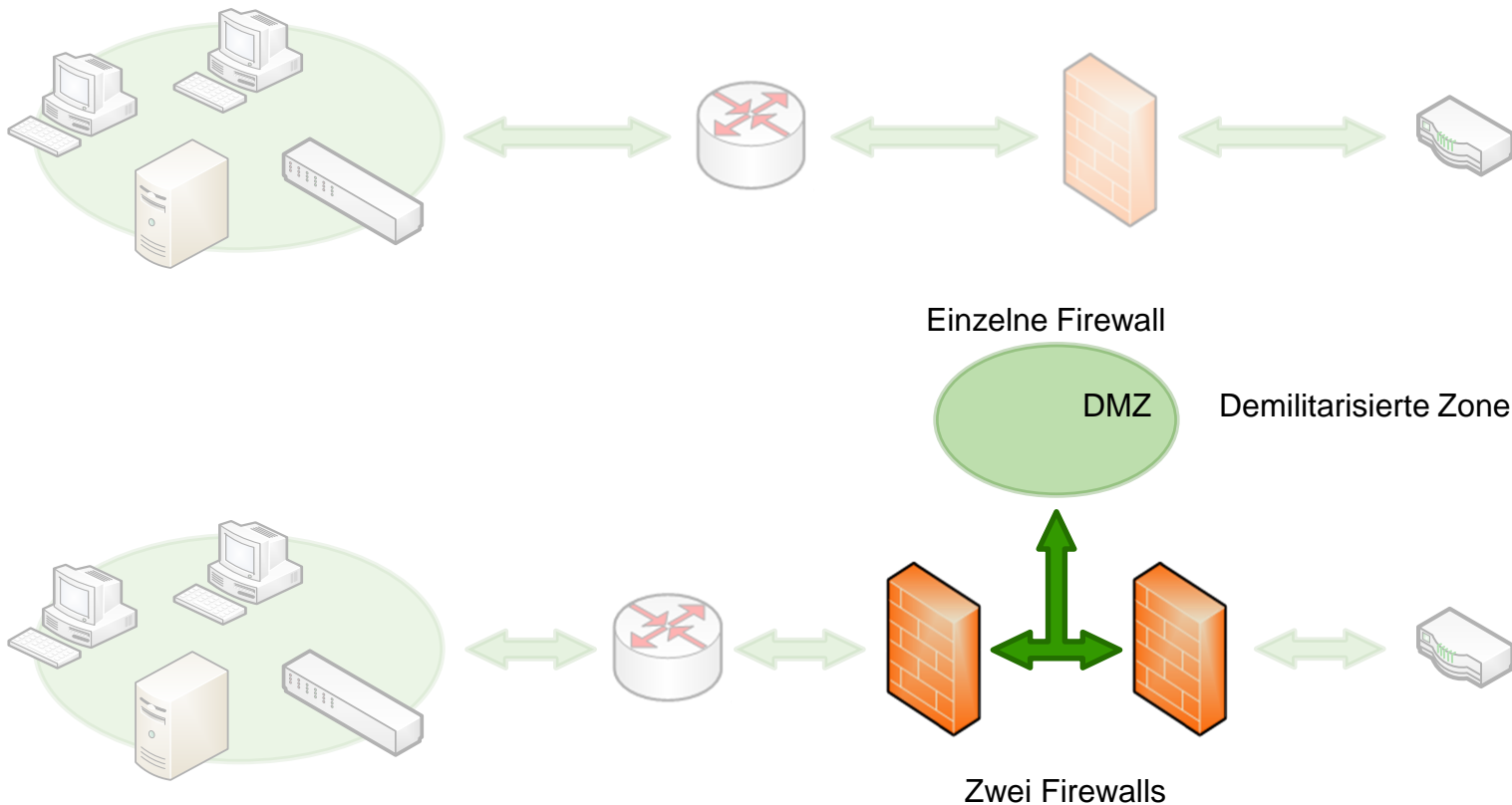


Ergänzende Fragen, wie z.B:

- Wo stehen die Geräte?
- Wie wird verkabelt?
- Was muss an die USV?



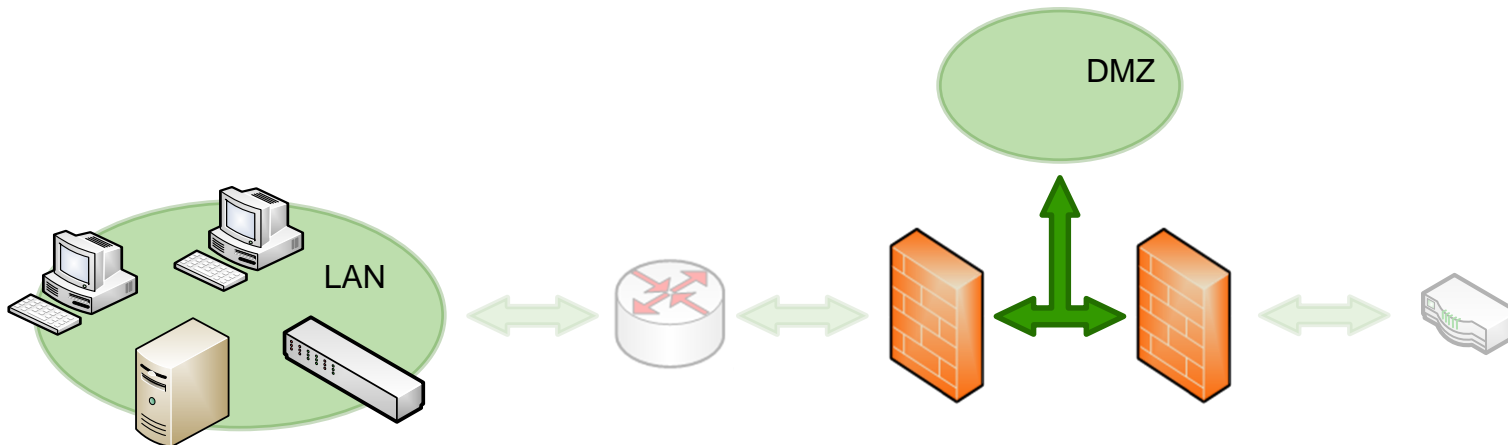
Umsetzung der Anbindung – DMZ





Umsetzung der Anbindung – DMZ

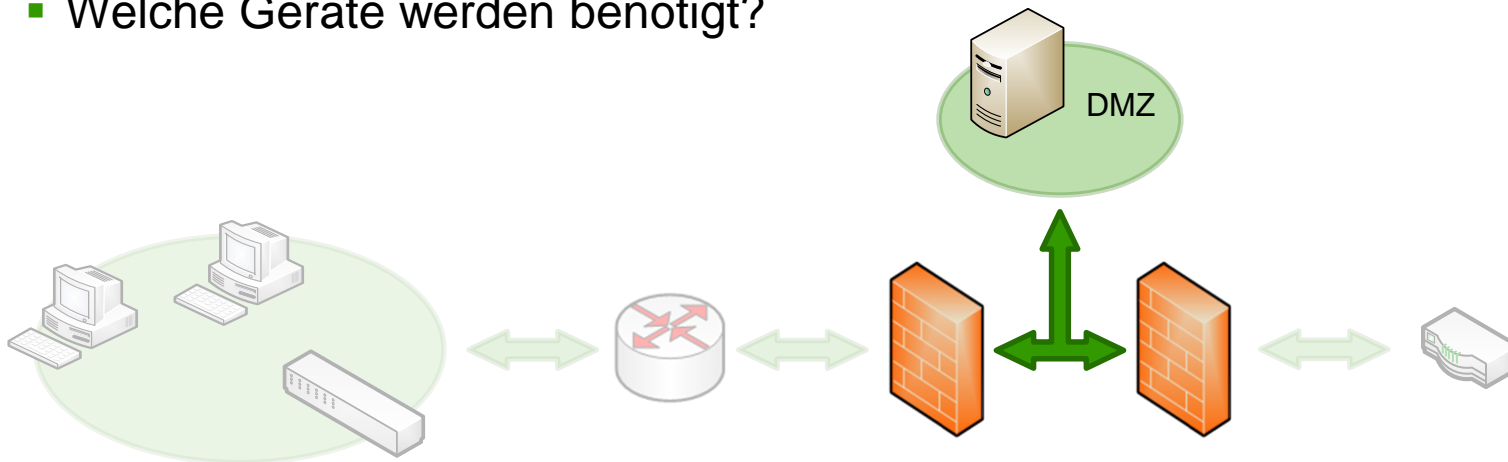
geschützt von innen → ← geschützt von außen





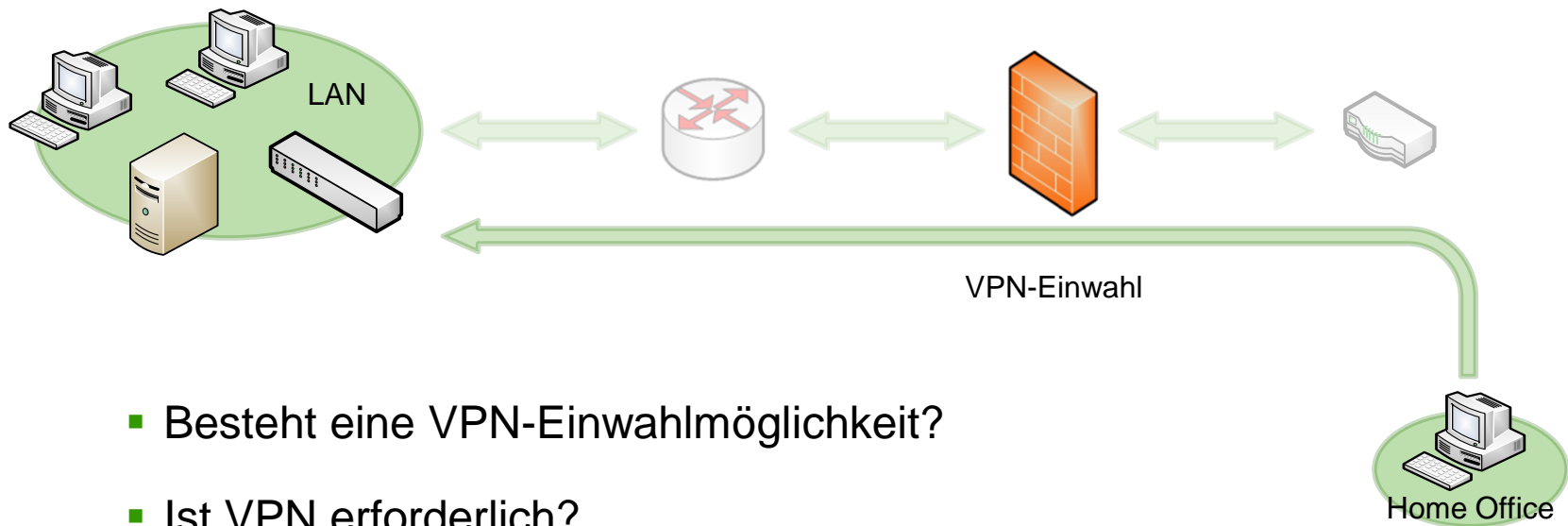
Umsetzung der Anbindung – DMZ

- Gibt es eine DMZ?
- Ist eine DMZ angebracht?
- Welche Geräte werden benötigt?





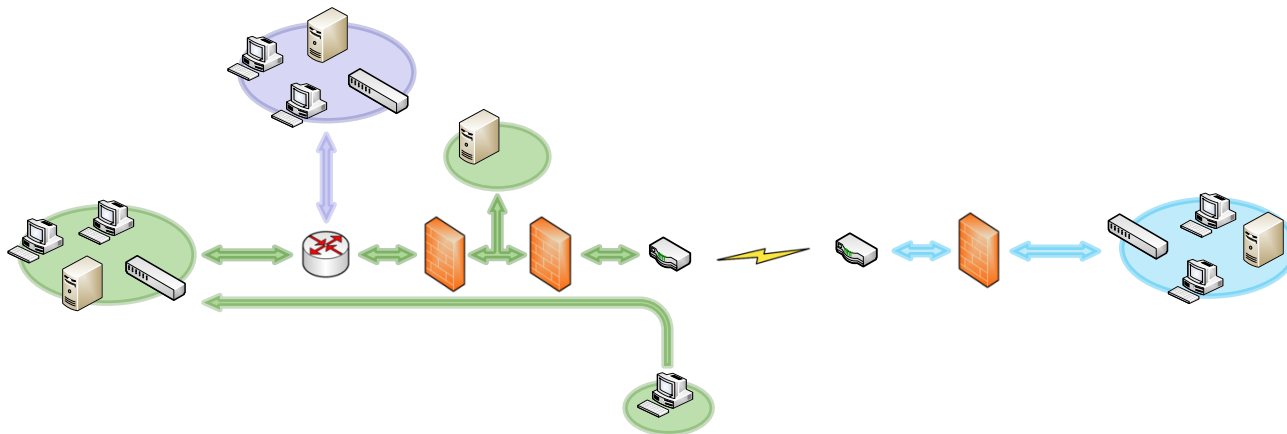
Umsetzung der Anbindung – VPN



- Besteht eine VPN-Einwahlmöglichkeit?
- Ist VPN erforderlich?
- Welche Technologie kommt zum Einsatz?
- Welche Geräte werden benötigt?



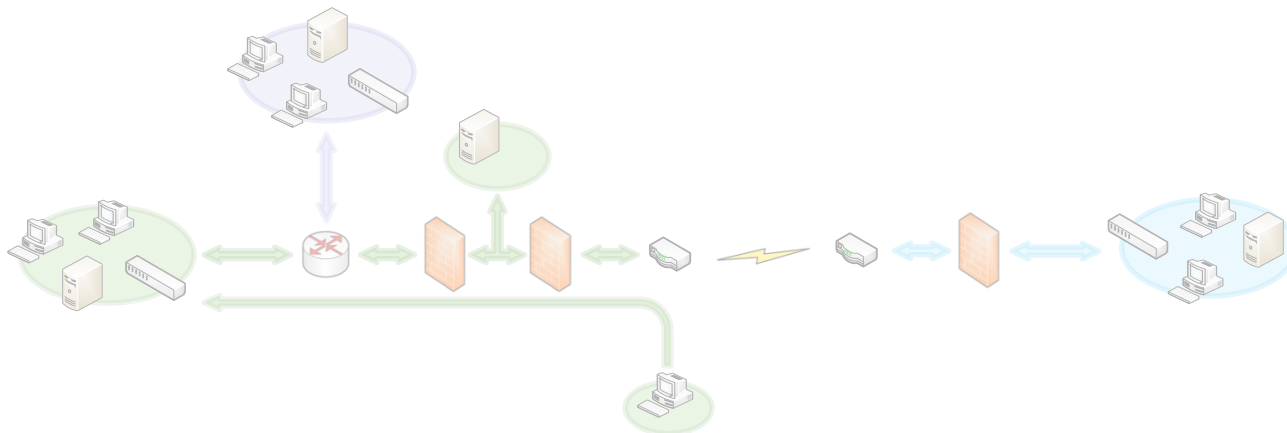
Umsetzung der Anbindung - Netzwerkskizze



Egal, wie einfach oder kompliziert das Netzwerk wird:
Netzwerkskizzen helfen, Fehler zu vermeiden.



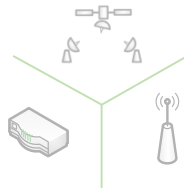
Umsetzung der Anbindung - Netzwerkskizze



- Es herrscht Formfreiheit – verständlich muss sie sein.
- Schlüsselfrage: Sie haben noch nie von dem Projekt gehört und müssen es morgen übernehmen!
Was wollen Sie darüber wissen?

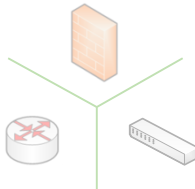


Zusammenfassung – Umsetzung der Anbindung



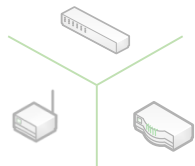
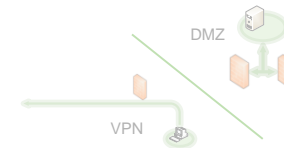
Dimensionieren
der Anbindung

Kontrollieren
der Herstellungs-
Voraussetzungen



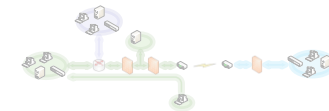
Feststellen
der Infrastruktur

Abklären
der Features



Erfassen
der erforderlichen
Hardware

Visualisieren
der Geräte und
Funktionen





Netzwerkadministrator

Internetanbindung



Übung: Auswahl einer Internetanbindung



Netzwerkadministrator

Internetanbindung



Routing und NAT



Wiederholung: IP-Adressen

	Netzanteil	Hostanteil
IP-Adresse	192 . 168 . 100	12
Subnetzmaske	255 . 255 . 255	0
Gateway-Adresse	192 . 168 . 100	254



Wiederholung: IP-Adressen

Klasse	Erste Oktett von bis	Netzmaske	Netze	Hosts pro Netz
A	1-127	255.0.0.0	127	~16,7 Mio
B	128-191	255.255.0.0	$64 \cdot 256$ = 16384	65.534
C	191-223	255.255.255.0	$32 \cdot 256 \cdot 256$ = ~2 Mio	254



Wiederholung: IP-Adressen

Private Adressbereiche

Klasse A:	10.0.0.0 / 255.0.0.0	1 Netz
Klasse B:	172.16.0.0 / 255.255.0.0 bis 172.31.0.0 / 255.255.0.0	16 Netze
Klasse C:	192.168.0.0 / 255.255.255.0 bis 192.168.255.0 / 255.255.255.0	256 Netze



Wiederholung: IP-Adressen

Besondere Adressbereiche

Loopback	127.0.0.0 / 255.0.0.0
APIPA	169.254.0.0 / 255.255.0.0
Multicast	224.0.0.0 bis 239.255.255.255
Experimental	240.0.0.0 bis 255.255.255.254



Wiederholung: IP-Adressen

Subnetzmaske in Dotted-Quad-Schreibweise

255 . 255 . 255 . 0

Subnetzmaske in Binär-Schreibweise

11111111 . 11111111 . 11111111 . 00000000



Von links gelesen: 24 „Einser“

Subnetzmaske in CIDR-Schreibweise

(Classless Inter-Domain Routing)

/24



Wiederholung: IP-Adressen

Angabe des Providers:

Nutzbarer Adressbereich: 81.223.57.96 / 29

11111111 . 11111111 . 11111111 . 11111000

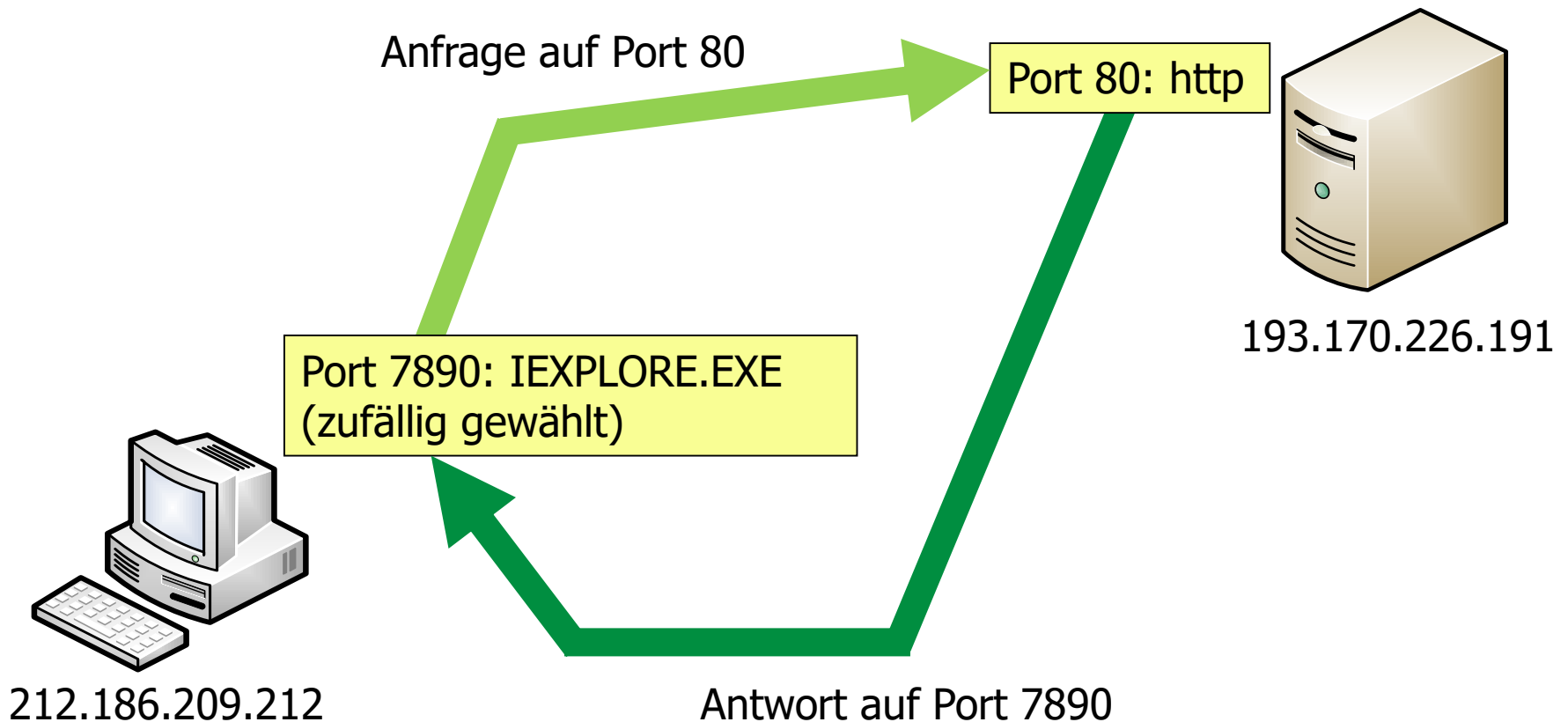


Von links gelesen: 29 „Einser“

Hostanteil



Wiederholung: Client-Server-Modell





Netzwerkadministrator

Internetanbindung



Routing



Routing

- Verbindet getrennte Netze
- Layer-3 Operation (IP-Adressen)
- Subnetzmaske als Entscheidungsgrundlage



Die Routing-Entscheidung

Quell-IP-Adresse:

192 . 168 . 200 . 10

Quell-Subnetzmaske:

255 . 255 . 255 . 0

Netzanteil

Hostanteil

Ziel-IP-Adresse:

192 . 168 . 200 . 20

Quell-Subnetzmaske:

255 . 255 . 255 . 0



Die Routing-Entscheidung

Quell-IP-Adresse:

192 . 168 . 200 . 10

Quell-Subnetzmaske:

255 . 255 . 255 . 0

Sind die Netzanteile gleich?

Ja!

Das Ziel ist lokal –
Es muss nicht geroutet werden

Ziel-IP-Adresse:

192 . 168 . 200 . 20

Quell-Subnetzmaske:

255 . 255 . 255 . 0



Die Routing-Entscheidung

Quell-IP-Adresse: 192 . 168 . 200 . 10

Quell-Subnetzmaske: 255 . 255 . 255 . 0

Ziel-IP-Adresse: 192 . 168 . 150 . 200

Quell-Subnetzmaske: 255 . 255 . 255 . 0



Die Routing-Entscheidung

Quell-IP-Adresse:

192 . 168 . 200 . 10

Quell-Subnetzmaske:

255 . 255 . 255 . 0

Sind die Netzanteile gleich?

Nein!

Das Ziel ist **nicht** lokal –
Es muss geroutet werden

Ziel-IP-Adresse:

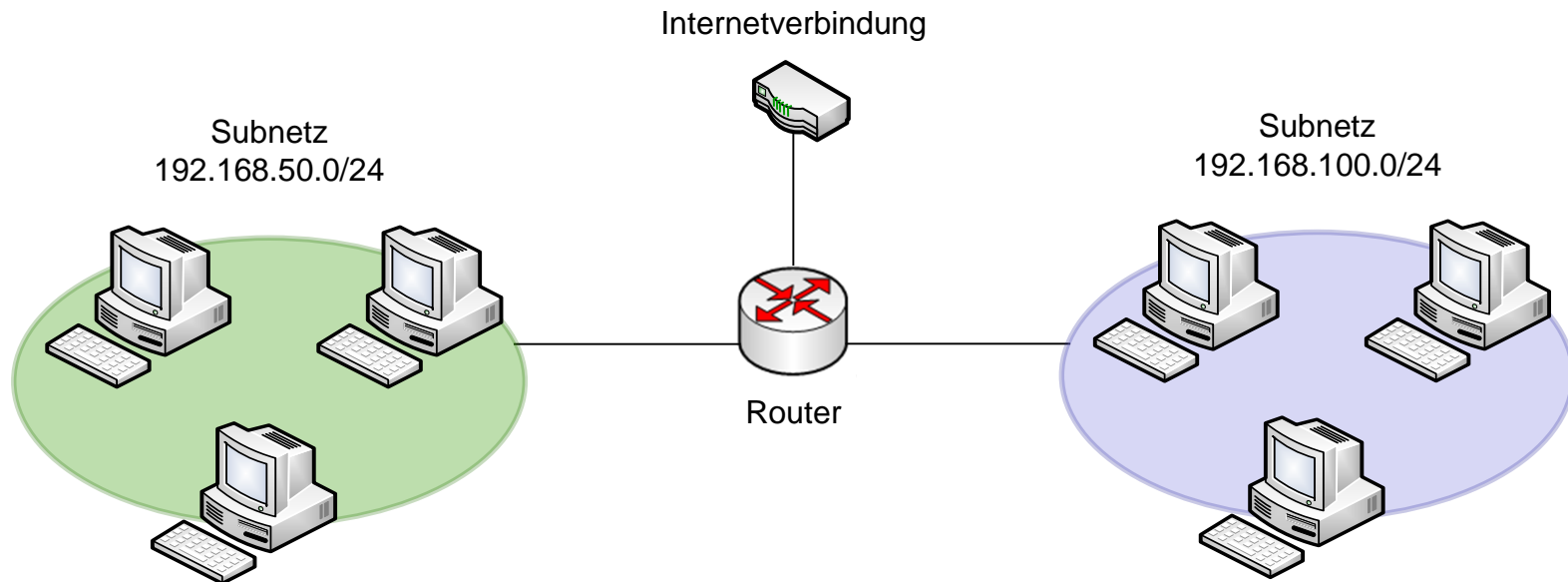
192 . 168 . 150 . 200

Quell-Subnetzmaske:

255 . 255 . 255 . 0

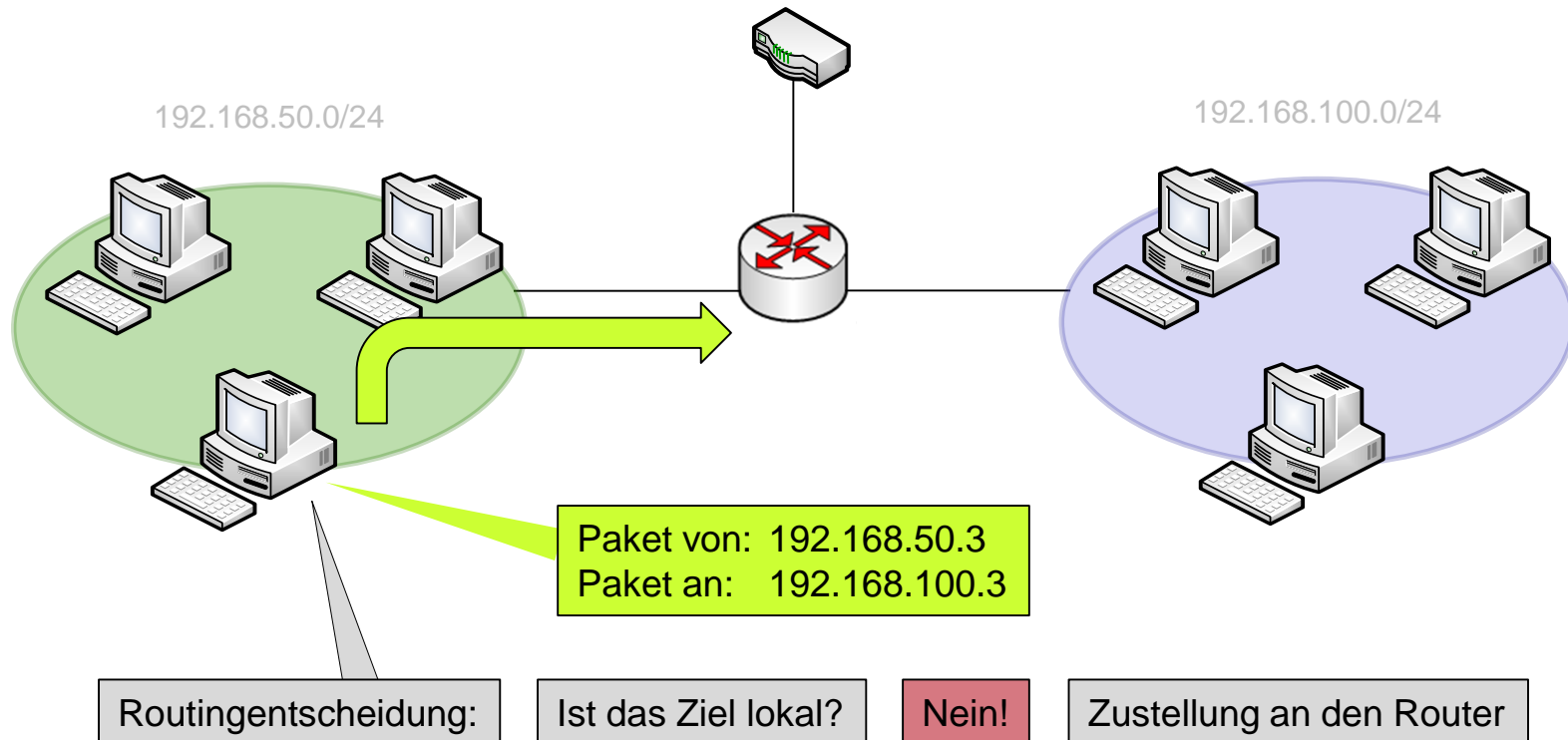


Routing



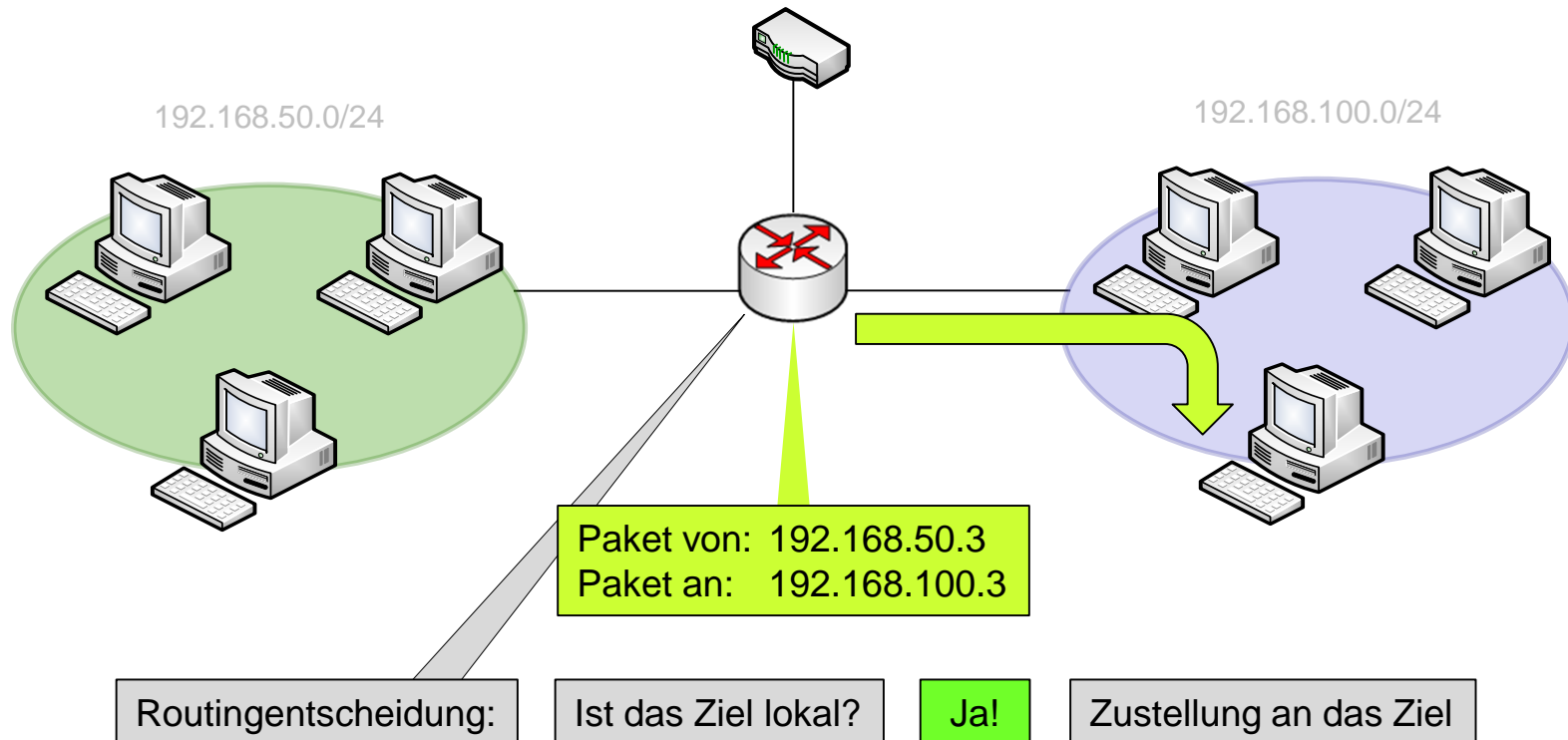


Routing



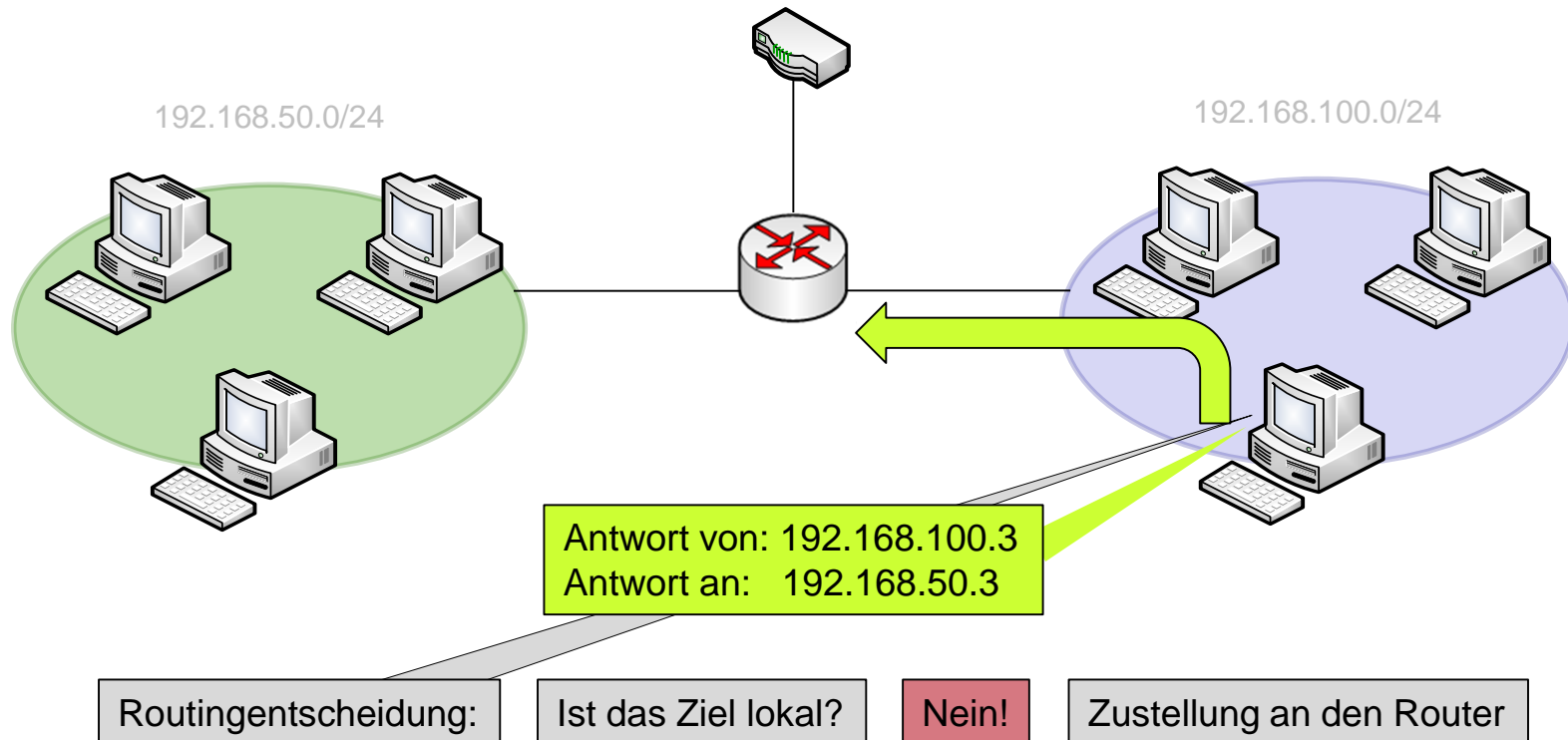


Routing



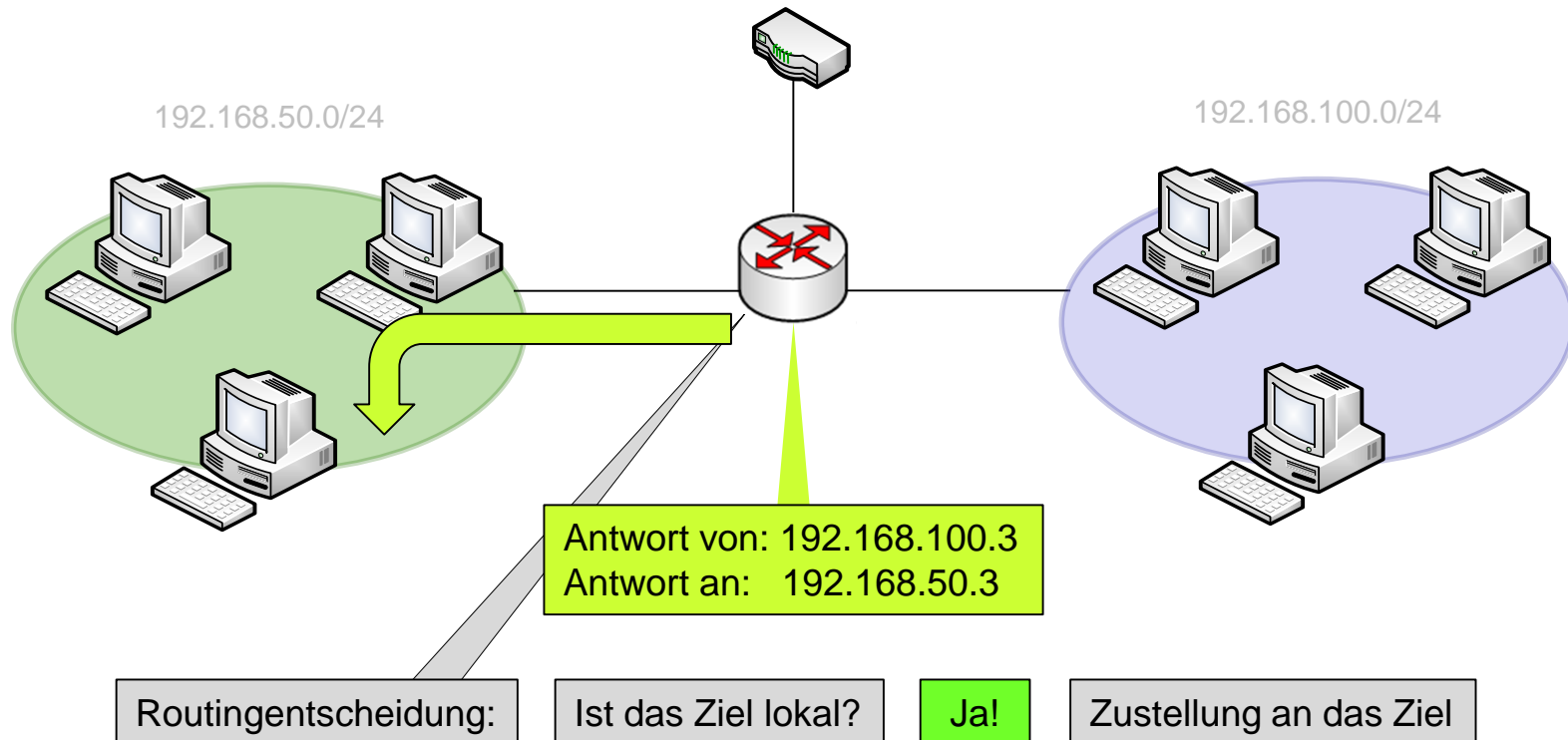


Routing



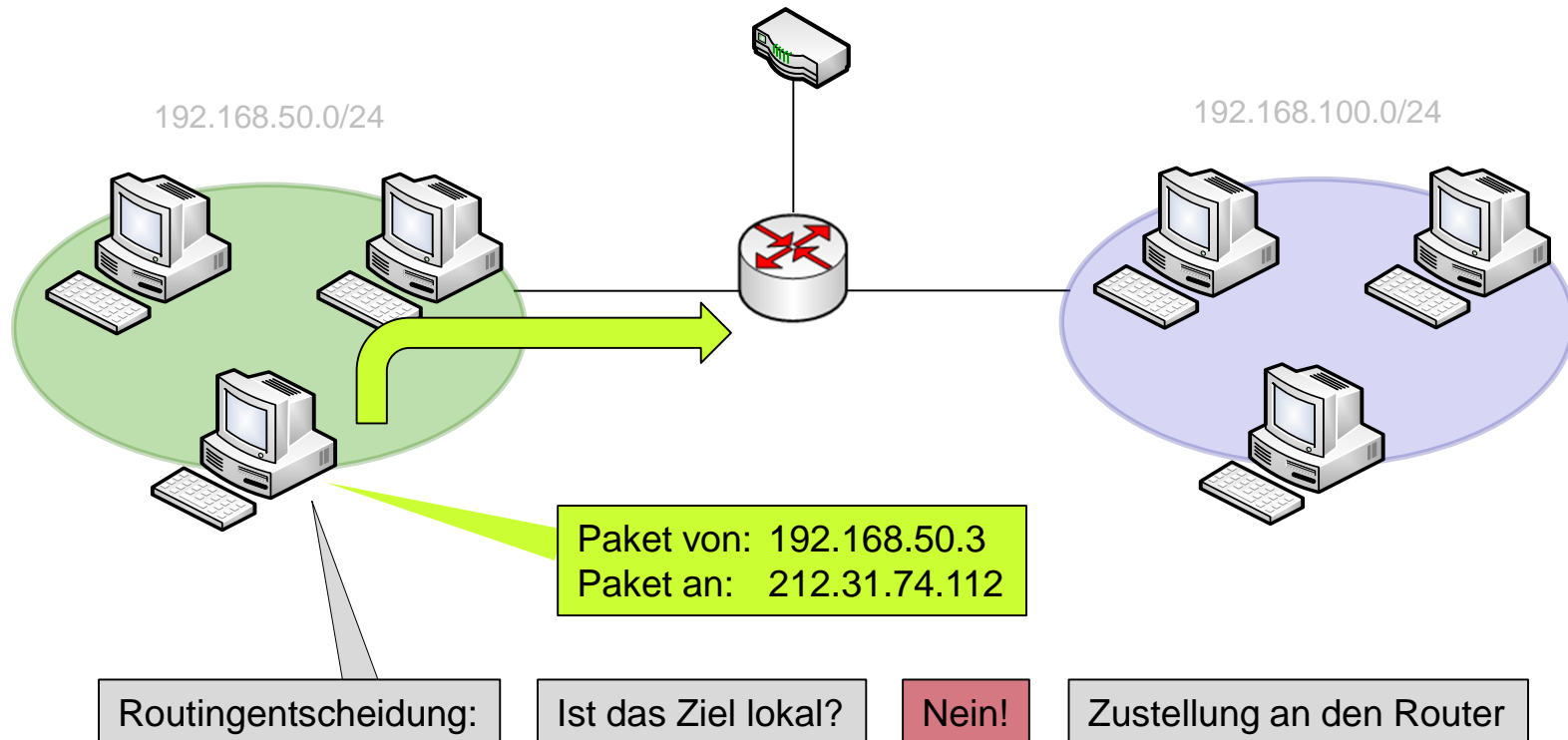


Routing



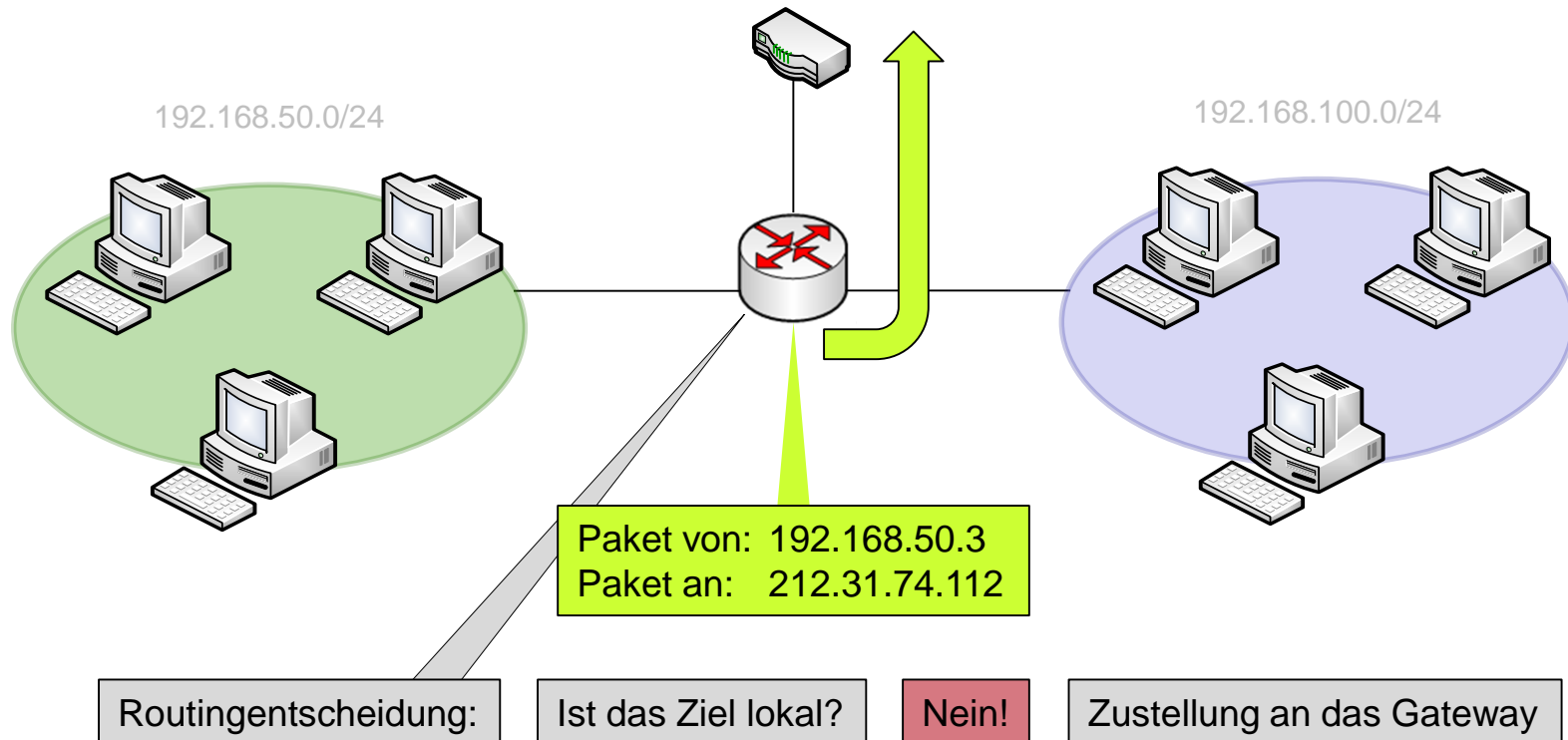


Routing





Routing





Routingtabelle

- Entscheidungsgrundlage
- automatisch generiert nach IP-Adressen
- manuelle Definition möglich

route delete <Ziel-IP>

route change <Ziel-IP> <Änderungen>

route add [-p] <Ziel-IP> mask <Subnetz-Maske> <Gateway-IP> metric <Metrik> if <Schnittstelle>

```
Administrator: Eingabeaufforderung

IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel    Netzwerkmaske    Gateway    Schnittstelle    Metrik
  0.0.0.0         0.0.0.0         81.223.57.97    81.223.57.100    281
  81.223.57.96    255.255.255.248  Auf Verbindung  81.223.57.100    281
  81.223.57.100   255.255.255.255  Auf Verbindung  81.223.57.100    281
  81.223.57.103   255.255.255.255  Auf Verbindung  81.223.57.100    281
  127.0.0.0       255.0.0.0       Auf Verbindung  127.0.0.1        331
  127.0.0.1       255.255.255.255  Auf Verbindung  127.0.0.1        331
  127.255.255.255 255.255.255.255  Auf Verbindung  127.0.0.1        331
  192.168.50.0    255.255.255.0    Auf Verbindung  192.168.50.254    281
  192.168.50.254  255.255.255.255  Auf Verbindung  192.168.50.254    281
  192.168.50.255  255.255.255.255  Auf Verbindung  192.168.50.254    281
  224.0.0.0       240.0.0.0       Auf Verbindung  127.0.0.1        331
  224.0.0.0       240.0.0.0       Auf Verbindung  81.223.57.100     281
  224.0.0.0       240.0.0.0       Auf Verbindung  192.168.50.254    281
  255.255.255.255 255.255.255.255  Auf Verbindung  127.0.0.1        331
  255.255.255.255 255.255.255.255  Auf Verbindung  81.223.57.100     281
  255.255.255.255 255.255.255.255  Auf Verbindung  192.168.50.254    281
=====
Ständige Routen:
  Netzwerkadresse    Netzmaske    Gatewayadresse    Metrik
  0.0.0.0            0.0.0.0      81.223.57.97      Standard
=====
```



Netzwerkadministrator

Internetanbindung



NAT



NAT – Network Address Translation

- Erfolgt üblicherweise am Router
- anhand vorher definierter Tabellen
- Layer-3 Operation

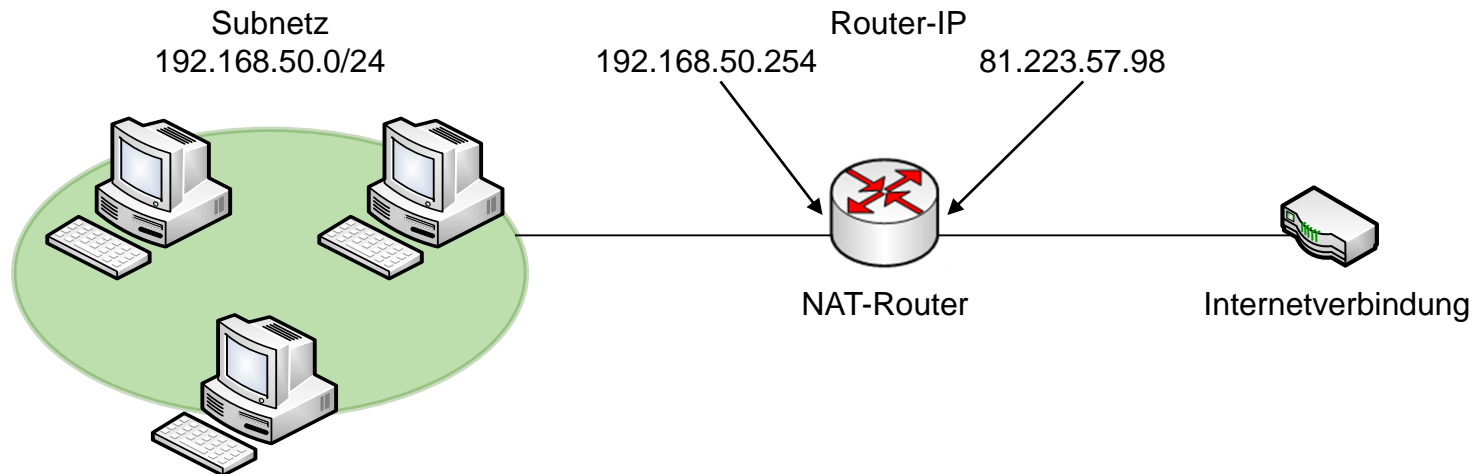


Variante 1: Source NAT

- Das Austauschen der Absender-IP
- erfolgt beim Verlassen des Subnetzes
- nach der Routingentscheidung
- zum Maskieren interner (privater) Adressen

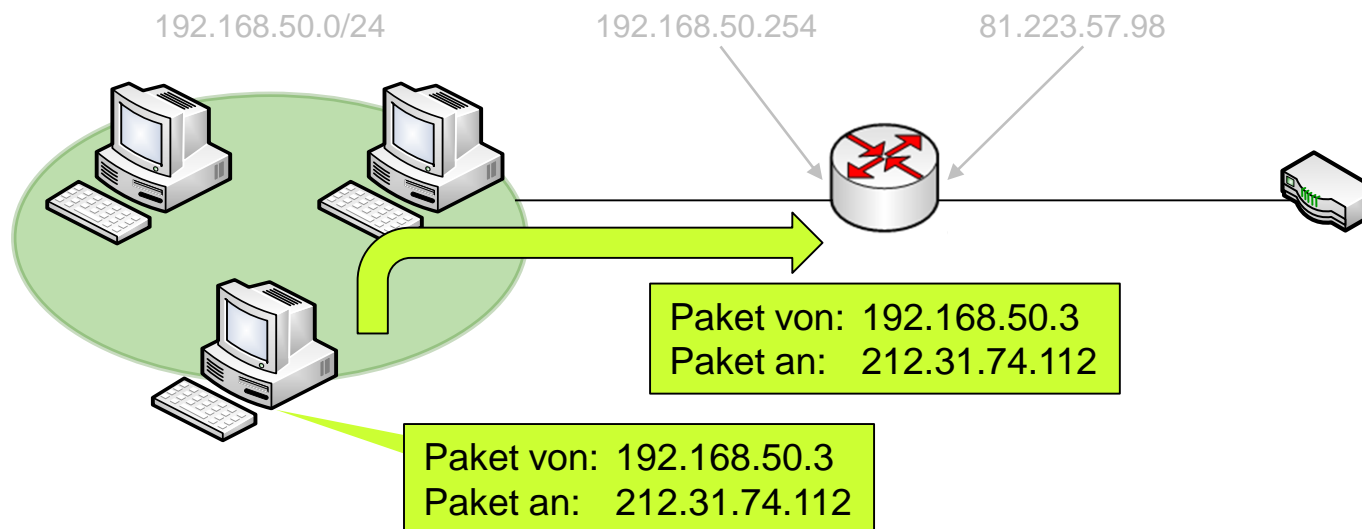


Source NAT



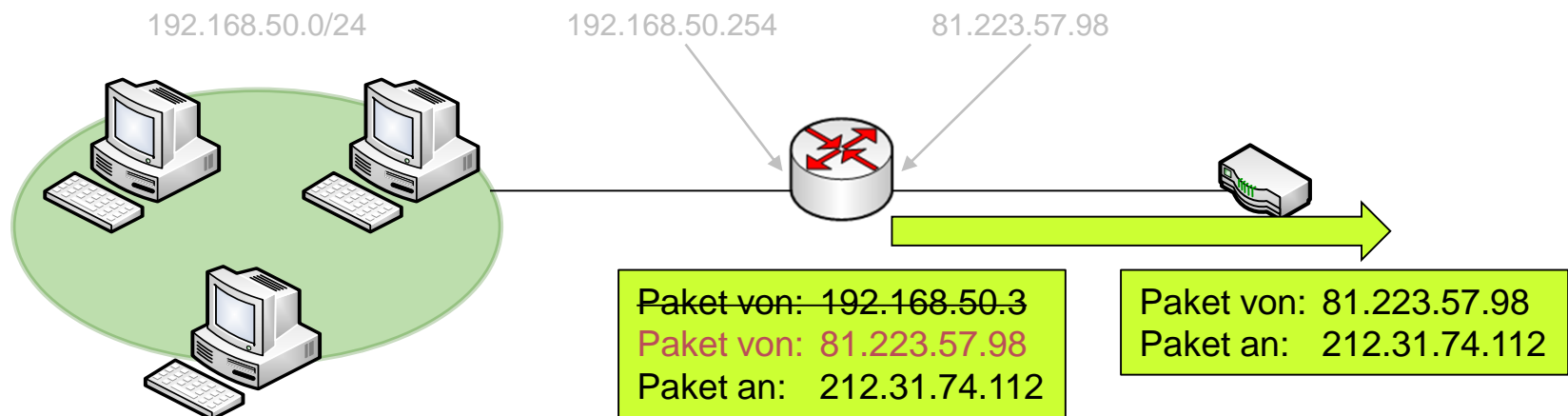


Source NAT



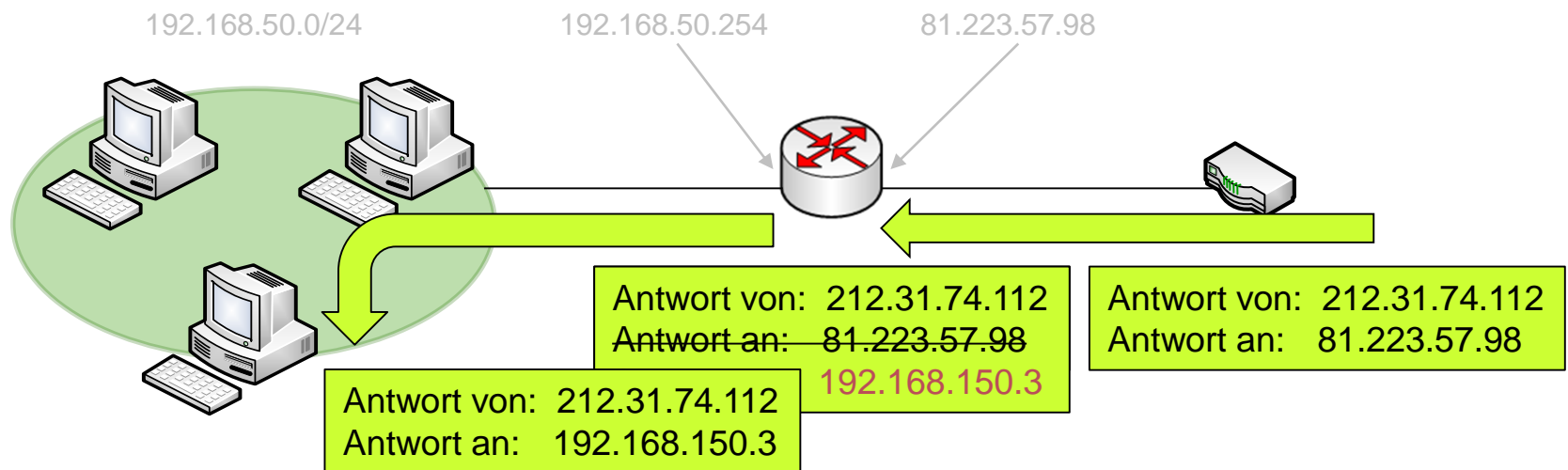


Source NAT





Source NAT



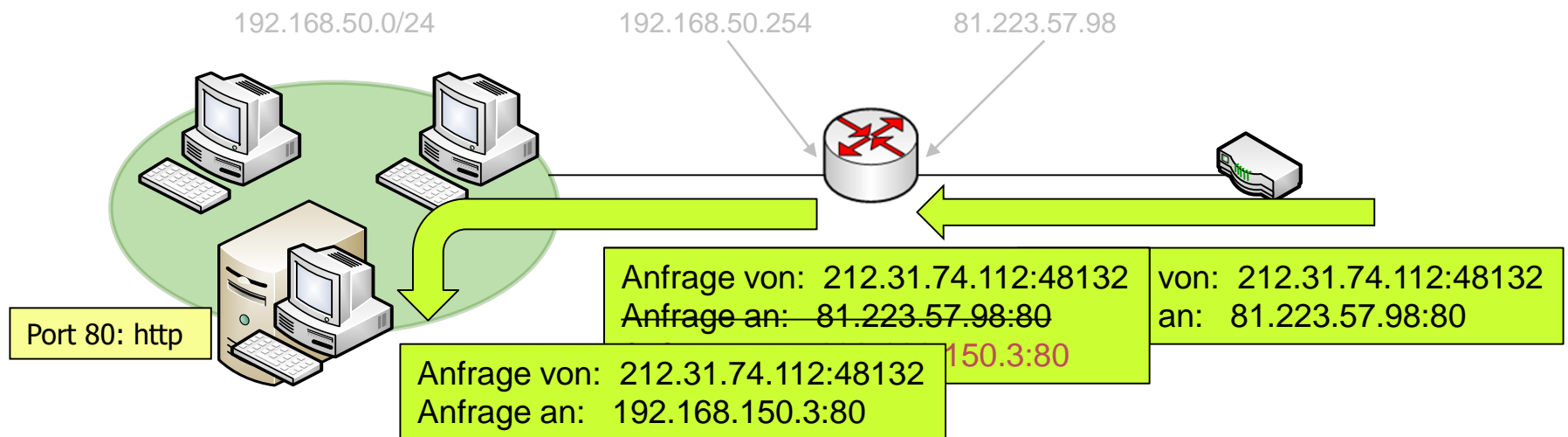


Variante 2: Destination NAT

- Das Austauschen der Ziel-IP
- erfolgt beim Eintreffen der Pakete an der Netzwerkgrenze
- vor der Routingentscheidung
- zum Veröffentlichen interner Dienste (*port-forwarding*)

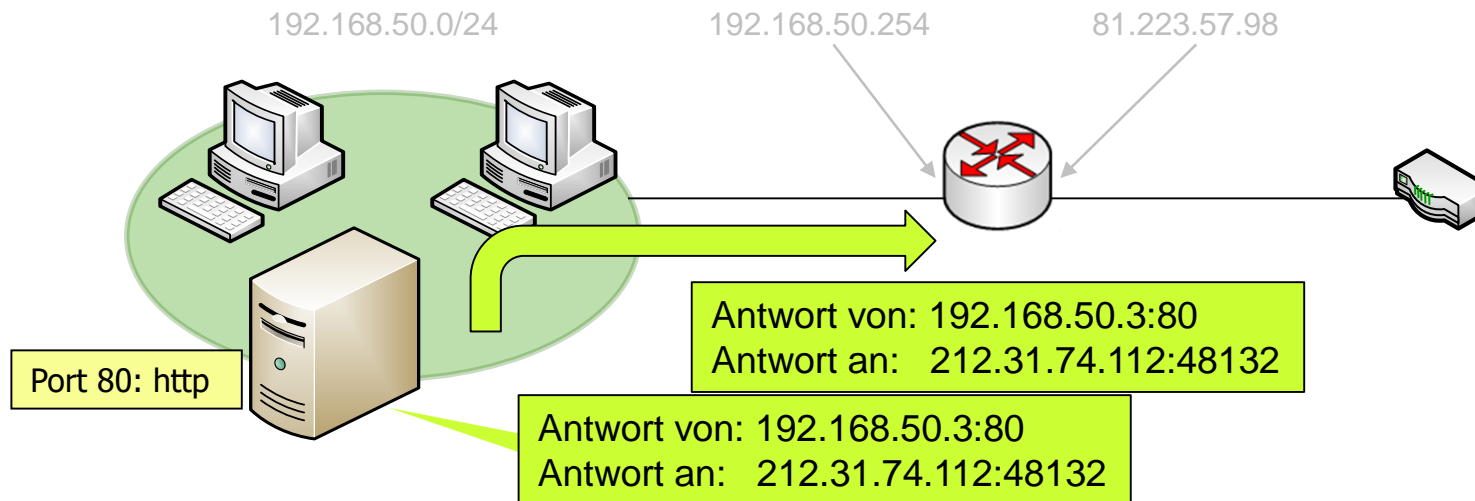


Destination NAT



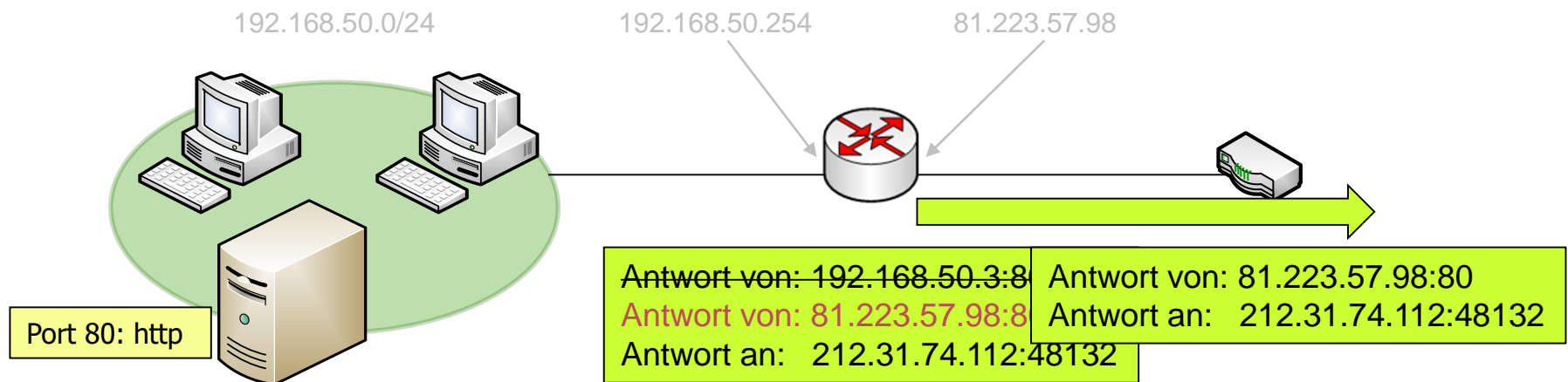


Destination NAT





Destination NAT

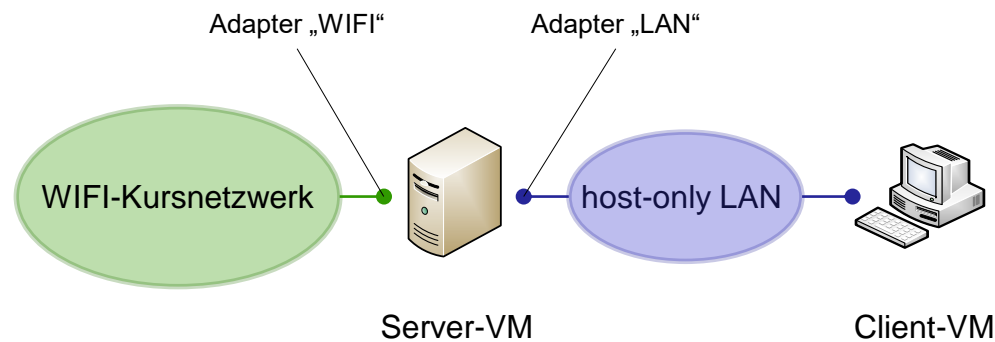




Übung: Routing und NAT

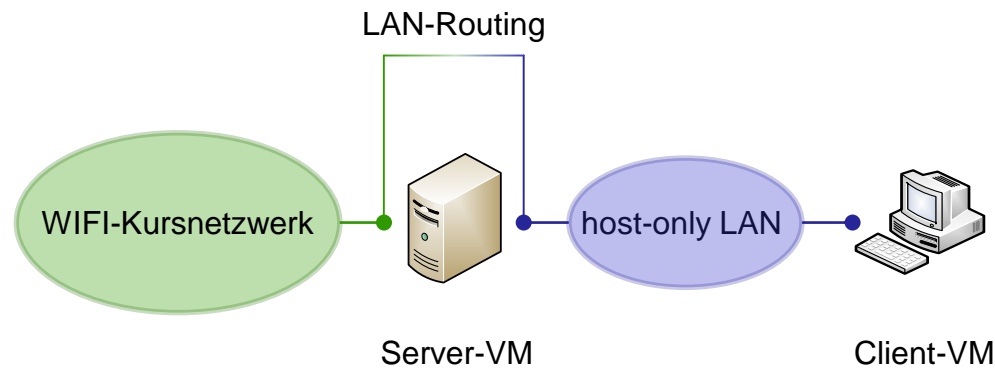


Übung: Routing – Skizze der Umgebung



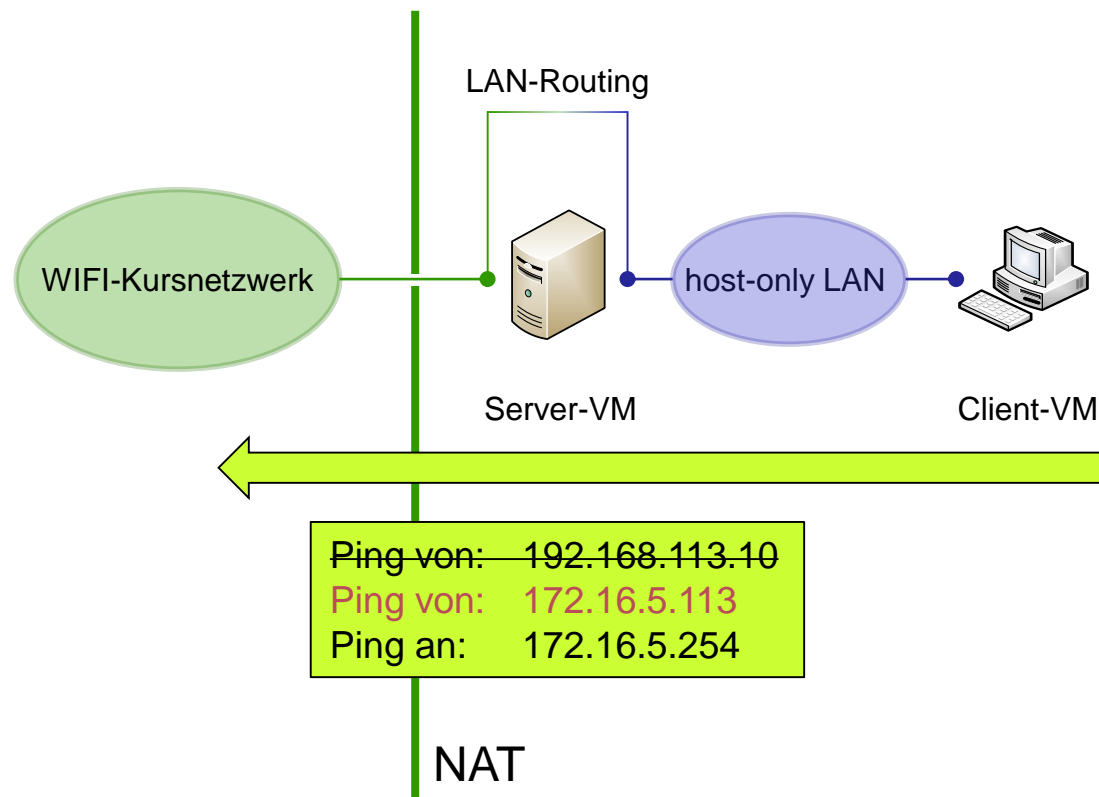


Übung: Routing – Skizze der Umgebung mit LAN-Routing





Übung: Routing – Skizze der Umgebung mit LAN-Routing und NAT





Netzwerkadministrator

Internetanbindung



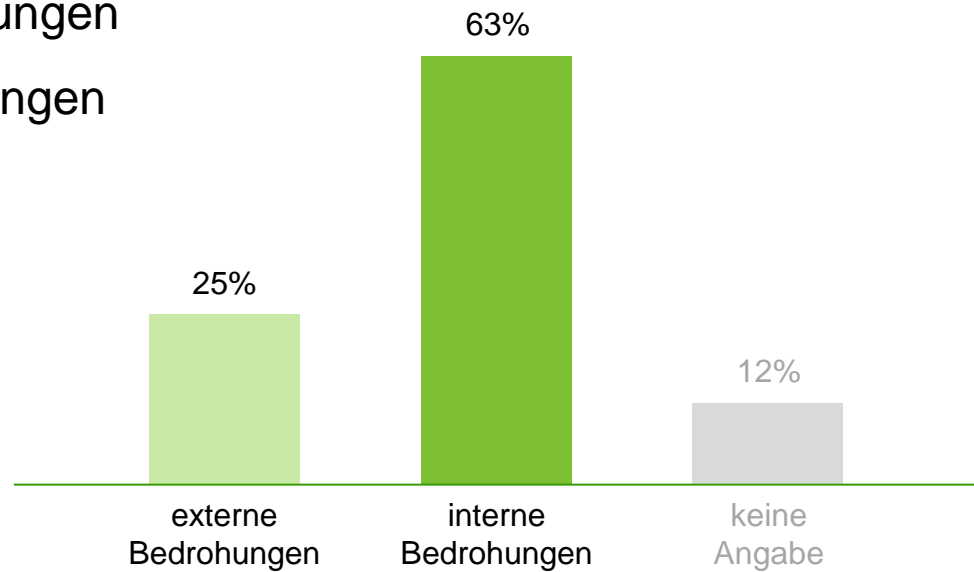
Sicherheits-Bedrohungen



Sicherheits-Bedrohungen

Bedrohungen werden ihrer Herkunft nach unterschieden in

- externe Bedrohungen
- interne Bedrohungen



Quelle: Forrester Research, 2012



Bedrohungen

Die Klassiker: „Wares“

- **Malware**
(Viren, Würmer, Trojaner...) Direkt schädliche Software
- **Spyware**
Spioniert Benutzer- und Systemdaten aus
- **Adware**
Blendet unaufgefordert Werbung ein
- **Scareware, Ransomware**
Verunsichert den Benutzer und verleitet zu Fehlverhalten



Malware

Computervirus

- infiziert fremde Dateien mit seinem Code
- verbreitet sich bei lokalem Aufruf einer infizierten Datei auf weitere Dateien
- meist auf einen bestimmten Dateityp beschränkt (Executables, Archive, etc.)

Computerwurm

- infiziert keine fremden Dateien, liegt als separates Programm vor
- verbreitet sich selbst über eine oder mehrere Methoden (eMail, Messaging etc.)
- meist auf eine bestimmte Verbreitungsart (z.B. eMail, Instant Messaging) oder
- eine konkrete Sicherheitslücke beschränkt (z.B. der „Slammer“-Wurm für MSSQL2000)



Malware

Trojaner

- Täuscht eine Anwendung vor (z.B. Computerspiel, Key-Generator)
- betreibt zusätzlich zur „Tarn“-Funktion eine Schadfunktion
- überwiegend für Backdoors benutzt

Backdoor

- stellt einen unerwünschten Fernzugriff bereit
- dient oft dem unberechtigten Erwerb von Benutzerdaten oder
- der Bildung von Bot-Nets



„Grayware“

Spyware

- Sammelt unbemerkt Benutzerdaten (z.B. Zahlungsinformationen)
- oder Informationen zum Benutzerverhalten (z.B. besuchte Internetseiten, online erworbene Waren, Verwendung bestimmter Software)

Adware

- zeigt unerwünscht Werbung an
- oder lenkt den Benutzer unerwünscht z.B. auf bestimmte kommerzielle Suchmaschinen (häufig bei Browser-Toolbars) oder Angebote
- und sammelt dabei eventuell auch noch Daten zum Benutzerverhalten



„Grayware“

Scareware

- verunsichert den Benutzer (z.B. durch Vortäuschen von Virenbefall oder Systemfehlern)
- verleitet zur Installation von Schadsoftware oder dem Kauf unnötiger „Reparaturprogramme“

Ransomware

- bewirkt Störungen des Systembetriebs (oder täuscht diese vor)
- und fordert zur Bezahlung auf, um diese zu beheben (z.B. „Polizei-Trojaner“)



Netzwerkadministrator Internetanbindung



Phishing

Verleitet z.B. durch gefälschte eMails

Warning:Your PayPal Account has been limited
service@paypal.com <team.paypal@intl.service.com>
Gesendet: Di 12.06.2012 00:28
An: petey@petey.at

und manipulierte Links

[http://paypal.com.cgi.bin.webscr.cmd.
login.submit.dispatch.
5885d80a1311f8e263taee8d4026841ac68a4j
k9dadj5652b2alm.profootacademie.be/
webscr_cmd_home/
Klicken, um Link zu folgen](http://paypal.com.cgi.bin.webscr.cmd.login.submit.dispatch.5885d80a1311f8e263taee8d4026841ac68a4jk9dadj5652b2alm.profootacademie.be/webscr_cmd_home/)

zur Preisgabe von Benutzerinformationen

Warning:Your PayPal Account has been limited
service@paypal.com <team.paypal@intl.service.com>
Gesendet: Di 12.06.2012 00:28
An: petey@petey.at



Information Regarding Your account:
Dear PayPal Member:

Attention! Your PayPal account has been limited!

As part of our security measures, we regularly screen activity in the PayPal system. We recently contacted you after noticing an issue on your account. We requested information from you for the following reason:

Our system detected unusual charges to a credit card linked to your PayPal account.

Reference Number: PP-259-187-991

This is the Last reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access.


Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

[Click here to activate your account](#)

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologise for any inconvenience..

Sincerely,
PayPal Account Review Department

Copyright © 1999-2012 PayPal. All rights reserved. PayPal Ltd. PayPal FSA Register Number: 226056.

 service@paypal.com

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (<http://paypal.com/>) to be sure you are on the real PayPal site.

For more information on protecting yourself from fraud, please review our Security Tips at <https://www.paypal.com/us/securitytips>

Protect Your Password

You should never give your PayPal password to anyone.



Netzwerkadministrator Internetanbindung



Phishing

Angst machen

Attention! Your PayPal account

unusual charges to a credit card

und Druck erzeugen

This is the Last reminder

as soon as possible.

wirken leider immer noch zu oft.

Warning: Your PayPal Account has been limited

service@paypal.com <team.paypal@intl.service.com>

Gesendet: Di 12.06.2012 00:28

An: petey@petey.at



Information Regarding Your account:

Dear PayPal Member:

Attention! Your PayPal account has been limited!

As part of our security measures, we regularly screen activity in the PayPal system. We recently contacted you after noticing an issue on your account. We requested information from you for the following reason:

Our system detected unusual charges to a credit card linked to your PayPal account.

Reference Number: PP-259-187-991

This is the Last reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access.

Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

[Click here to activate your account](#)

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologise for any inconvenience..

Sincerely,
PayPal Account Review Department

Copyright © 1999-2012 PayPal. All rights reserved. PayPal Ltd. PayPal FSA Register Number: 226056.

service@paypal.com

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (<http://paypal.com/>) to be sure you are on the real PayPal site.

For more information on protecting yourself from fraud, please review our Security Tips at <https://www.paypal.com/us/securitytips>

Protect Your Password

You should never give your PayPal password to anyone.



Pharming

Diese Variante des Phishing

- verwendet manipulierte DNS-Einträge
(DNS cache poisoning)
 - oder manipuliert den Resolver des Clients
(hosts-Datei, Verstellen der DNS-Server)
- und ist dadurch viel schwieriger zu entdecken.



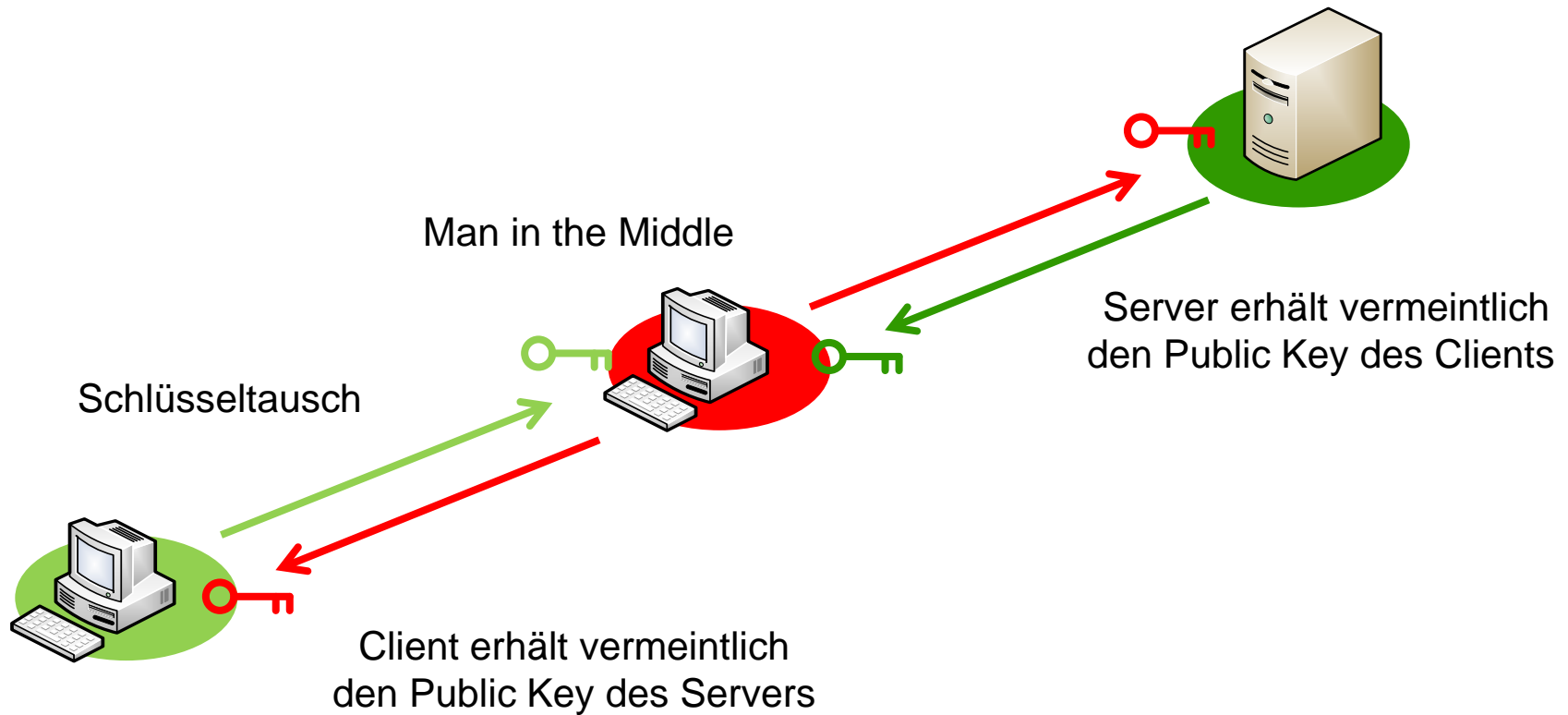
Port 443: https

Server und Client tauschen Public Keys

Verschlüsselung erfolgt mit dem Public Key des Anderen

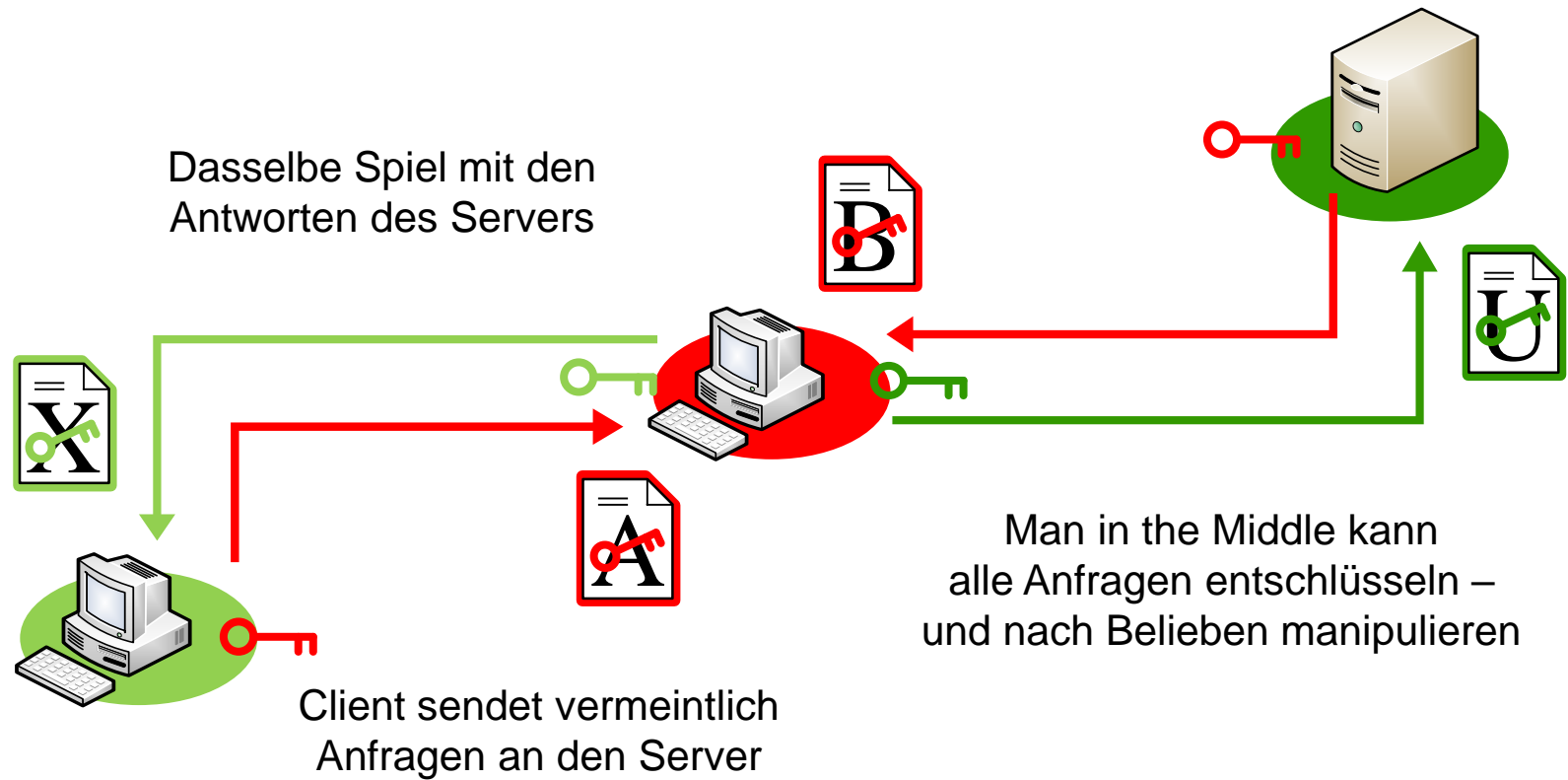


Man in the Middle



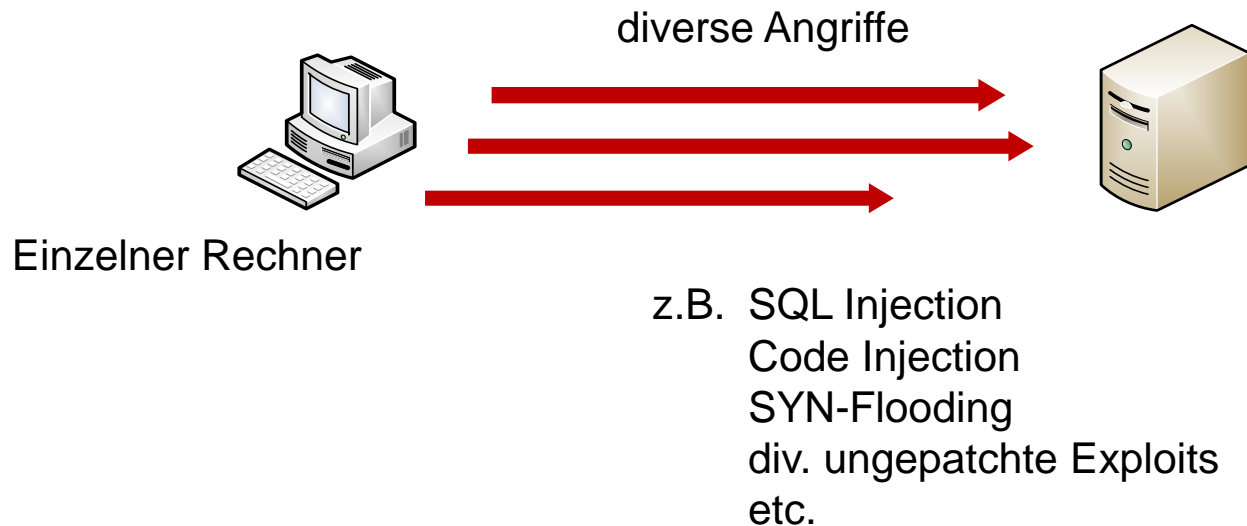


Man in the Middle



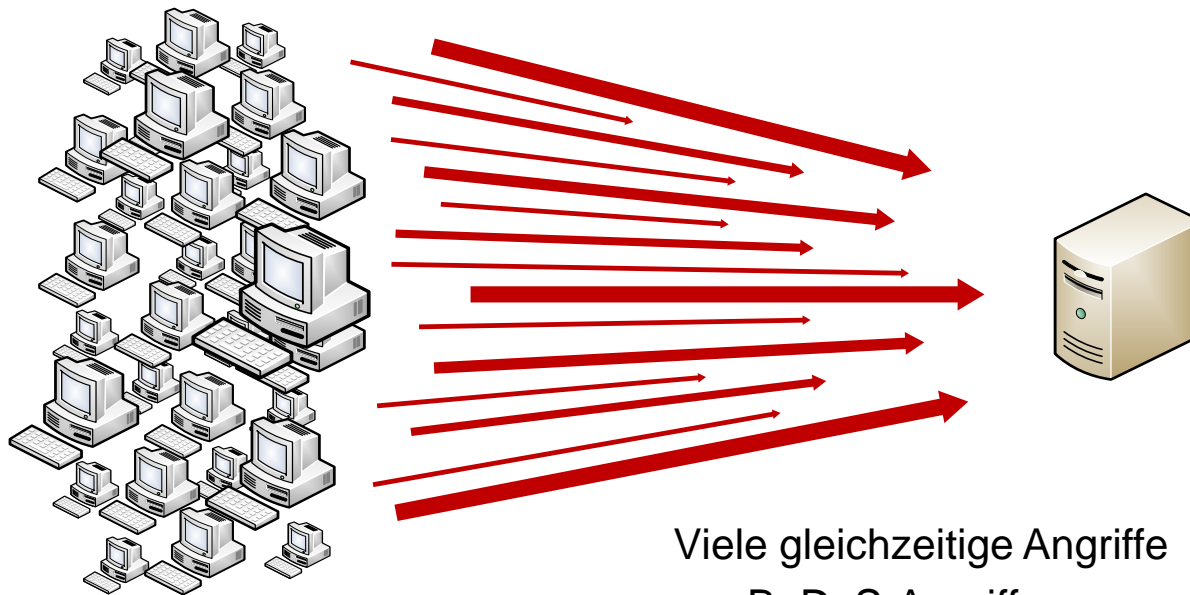


DoS – Denial of Service





DDoS – Distributed Denial of Service



Viele Rechner
z.B. Bot-Net,
Hackergruppe etc.

Viele gleichzeitige Angriffe

- z.B. DoS-Angriffe
- oder zu große Menge „normaler“ Aufrufe



Sicherheits-Bedrohungen

Fehlleistung

z.B.:

- mangelhaft geschriebene Anwendungen
- ungenügend dimensionierte Lösungen
- fehlerhafte Implementationen



Sicherheits-Bedrohungen

Fehlbedienung

z.B.:

- Löschen von Daten oder Konfigurationen
- Upload oder Verarbeitung korrupter Dateien
- Eingabe falscher Formate in unvalidierte Felder



Sicherheits-Bedrohungen

Diebstahl und Verlust

z.B.:

- Smartphone mit gespeicherten Passwörtern
- Laptop mit offline-synchronisierten Mails und Dateien
- USB-Stick mit Buchhaltungs- oder Forschungsdaten



Zusammenfassung: Sicherheits-Bedrohungen

Malware

Viren,
Würmer,
Trojaner,
Backdoors

Phishing und Pharming

Erschleichen von Benutzerdaten

Man in the Middle

Mithören – schlimmstenfalls
sogar Manipulieren – des
Netzwerkverkehrs

Grayware

Spyware,
Adware,
Scareware,
Ransomware

DoS und DDoS

Sabotieren oder Überlasten von Servern

Fehlleistung und Fehlbedienung

Ungewollt Fehler schaffen oder finden

Diebstahl und Verlust

Außerplanmäßige Abschreibung
von Geräten und Daten



Netzwerkadministrator









Internetanbindung



Gegenmaßnahmen











Gegenmaßnahmen: Malware

	Virens Scanner (evtl. dediziert)	Firewall (evtl. Entfernungstool)
Viren		
Würmer		
Trojaner		
Backdoors		

keine Verbindung nach draußen
=
relativ unschädlich







Gegenmaßnahmen: Grayware

	Virens Scanner	Benutzer schulen
Adware		
Spyware		
Scareware		
Ransomware		



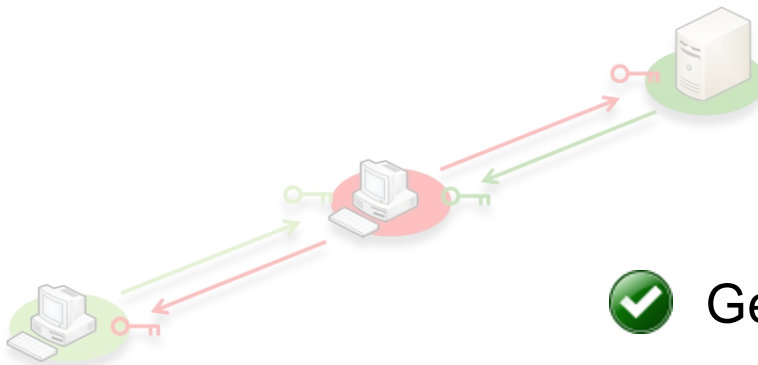
Gegenmaßnahmen: Phishing und Pharming

	Site Inspection (z.B. Benutzerwarnungen)	Benutzerschulung
Phishing		
Pharming		

Wenn die DNS-Manipulation bereits geglückt ist,
ist Pharming potentiell sehr schwer zu erkennen.



Gegenmaßnahmen: Man in the Middle



- ✓ Gegenseitige Authentifizierung
- ✓ Geheime Schlüssel
- ✓ One-Time-Pads



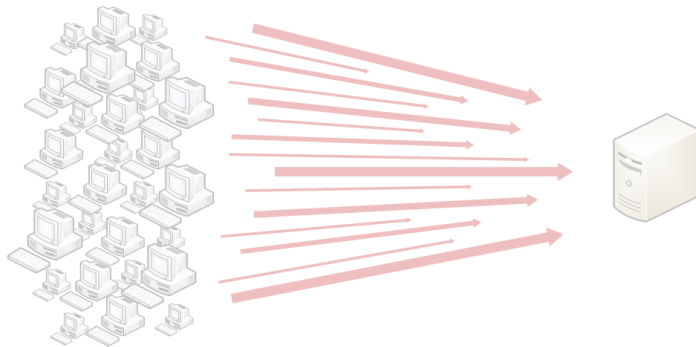
Gegenmaßnahmen: DoS



- ✓ Firewalls
- ✓ Updates und Patches
- ✓ Penetration Tests
- ✓ Lasttests



Gegenmaßnahmen: DDoS



✓ Firewalls

✓ Lasttests

Bei einer ausreichend hohen Anzahl an Angreifern hilft gegen DDoS gar nichts.



Gegenmaßnahmen: Fehlleistung

Fehlleistungen wie z.B.

- mangelhaft geschriebene Anwendungen
- ungenügend dimensionierte Lösungen
- fehlerhafte Implementationen

- ✓ Penetration Tests
(„White Hacking“)
- ✓ Lasttests
- ✓ unabhängige Qualitätskontrolle



Gegenmaßnahmen: Fehlbedienung

Fehlbedienung wie z.B.

- Löschen von Daten oder Konfigurationen
- Upload oder Verarbeitung korrupter Dateien
- Eingabe falscher Formate in unvalidierte Felder

- ✓ Berechtigungen einschränken
- ✓ Eingabedaten validieren
- ✓ Benutzer schulen



Gegenmaßnahmen: Diebstahl und Verlust

Wie z.B. Verlust oder Diebstahl von:

- Smartphone mit gespeicherten Passwörtern
- Laptop mit offline-synchronisierten Mails und Dateien
- USB-Stick mit Buchhaltungs- oder Forschungsdaten

- ✓ Hardware-Sicherungen (z.B. Intel vPro)
- ✓ Daten-Verschlüsselung
- ✓ Benutzer schulen



Zusammenfassung: Gegenmaßnahmen

Die einfachsten Maßnahmen:

Firewall und Virens Scanner

Helfen bei Malware und Grayware, machen DoS schwieriger, können die Auswirkungen von Fehlleistung mindern

Patches und Updates

Vermindern die Angriffsfläche für DoS und Malware, teilweise für Fehlleistung und Fehlbedienung

Sparsamer Umgang mit Benutzerrechten

Vermindert das Schadpotential von Malware und Grayware, erschwert DoS von innen, kann vor Fehlbedienung schützen



Zusammenfassung: Gegenmaßnahmen

Viel zu selten umgesetzt:

Benutzer schulen

Vermindert das Auftreten bzw. die Auswirkungen von Malware, Grayware, Phishing und Pharming, Fehlbedienung und Verlust

Lasttests bzw. unabhängige Qualitätskontrolle

Vermindert die Angriffsfläche für DoS und DDoS, verringert das Auftreten von Fehlleistung und die Häufigkeit von Fehlbedienung

Penetration Testing

Hilft Fehlleistung und Angriffspunkte von Malware aufzudecken, erschwert DoS und teilweise DDoS, lindert Angst und Schuldgefühle



Netzwerkadministrator

Internetanbindung

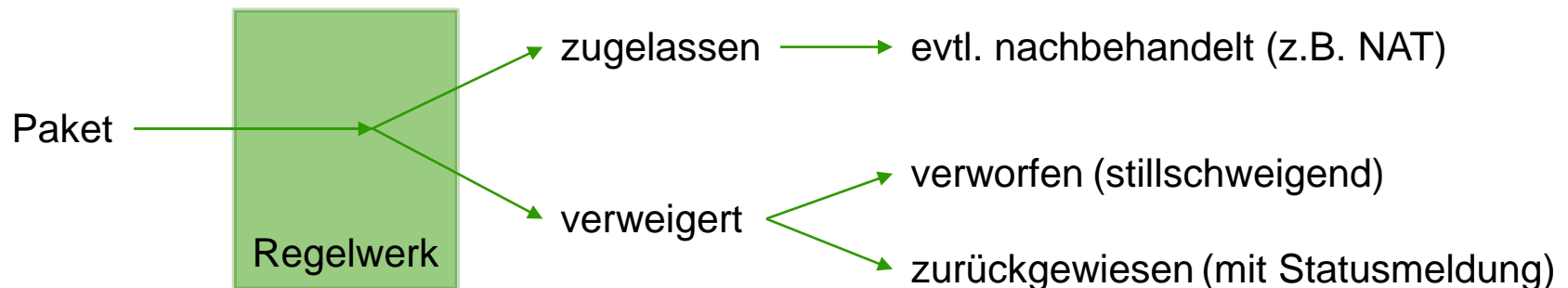


Firewalls



Funktionsprinzip

- Von der Grundfunktion her ein Paketfilter
- Pakete werden inspiziert und danach zugelassen oder verweigert
- Entscheidung erfolgt aufgrund vorher definierter Regeln



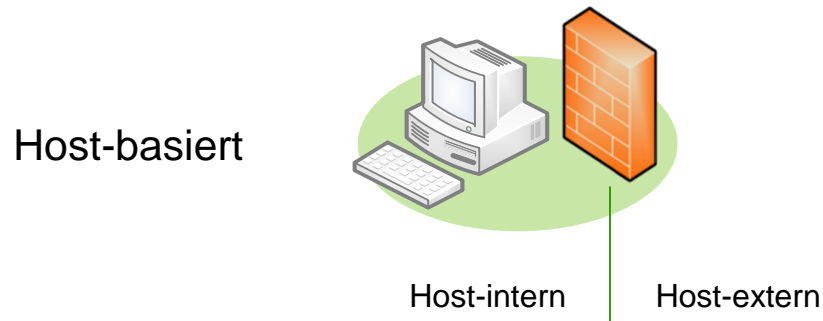


Entscheidungsgrundlagen

	OSI-Layer
<ul style="list-style-type: none">■ Verbindungsstatus (Stateful Inspection)<ul style="list-style-type: none">■ z.B. neu (SYN) oder■ bestehend (SYN/ACK, ACK)	
<ul style="list-style-type: none">■ Paket-Herkunft und -Ziel<ul style="list-style-type: none">■ innere /äußere Netzwerkschnittstelle■ Quell- und Ziel-IP-Adresse■ Quell- und Ziel-Port	
<ul style="list-style-type: none">■ verwendetes Protokoll	
<ul style="list-style-type: none">■ sendende oder empfangende Anwendung	
<ul style="list-style-type: none">■ Inhalt des Pakets	



host-basierte Firewalls: Zonen

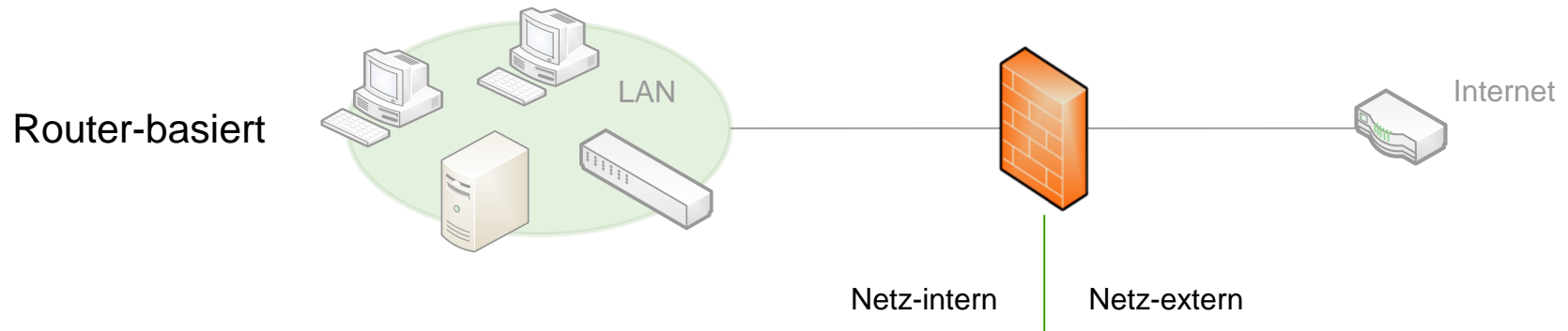


Mögliche Richtungen für Netzwerk-Pakete:

- Ausgehend
- Eingehend
- Intern (z.B. Loopback)



router-basierte Firewalls: Zonen



Mögliche Richtungen:

- Ausgehend
- Eingehend
- Intern
- Weiterleitung ausgehend (Netz-intern nach Netz-extern)
- Weiterleitung eingehend (Netz-extern nach Netz-intern)



Hardware-Firewall

- Gerät, das nur der Firewall-Applikation dient
- meist eigenes, streng angepasstes OS (Firmware)
- meist extern verwaltet (Weboberfläche, SSH, ext. Software)
- z.B. Cisco, Sonicwall, Juniper, FortiNet...

Vorteile: z.B. weniger Angriffsfläche, spezialisiert und effizient

Nachteile: z.B. Anschaffungskosten, separat zu verwalten



Software-Firewall

- Anwendung, die zusätzlich auf einem bestehenden OS läuft
- setzt auf vom OS genutzte Hardware und Treiber auf
- meist über GUI verwaltet
- z.B. Windows-Firewall, Norton Internet Security, Zone Alarm...

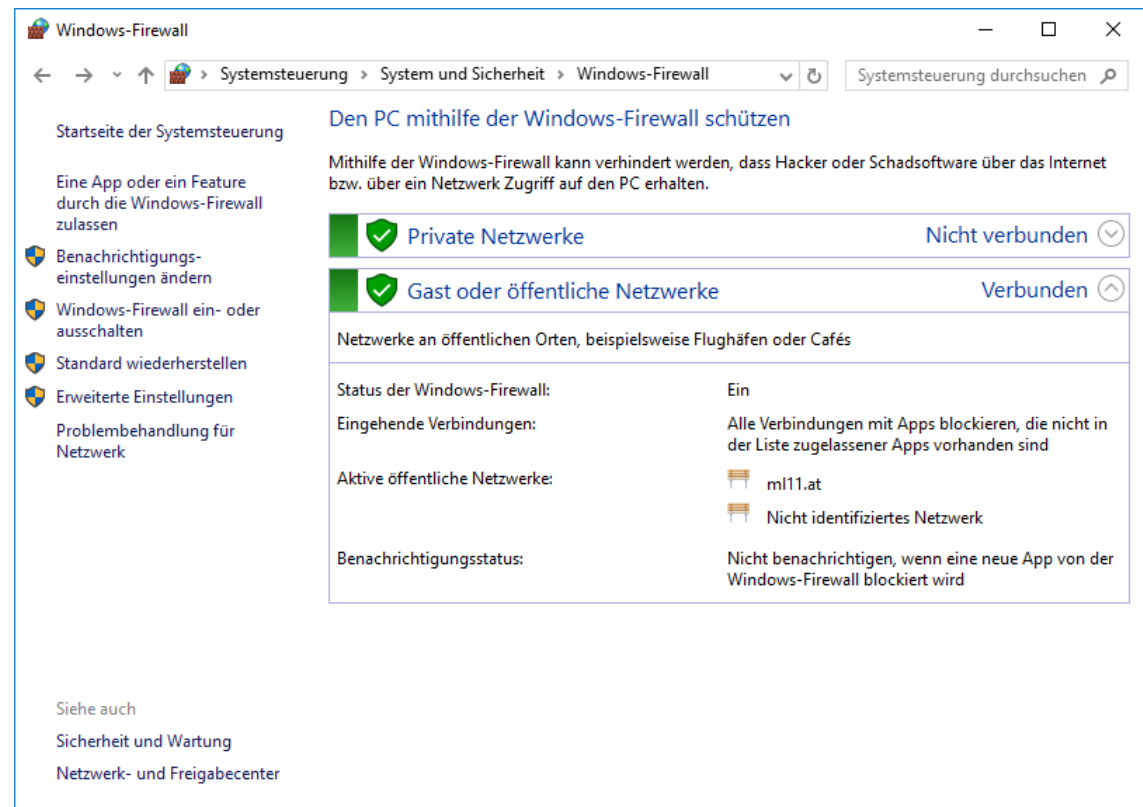
Vorteile: z.B. Kostenersparnis, Verwaltbarkeit

Nachteile: z.B. Abhängigkeit von OS-Sicherheit und -Integrität



Windows-Firewall

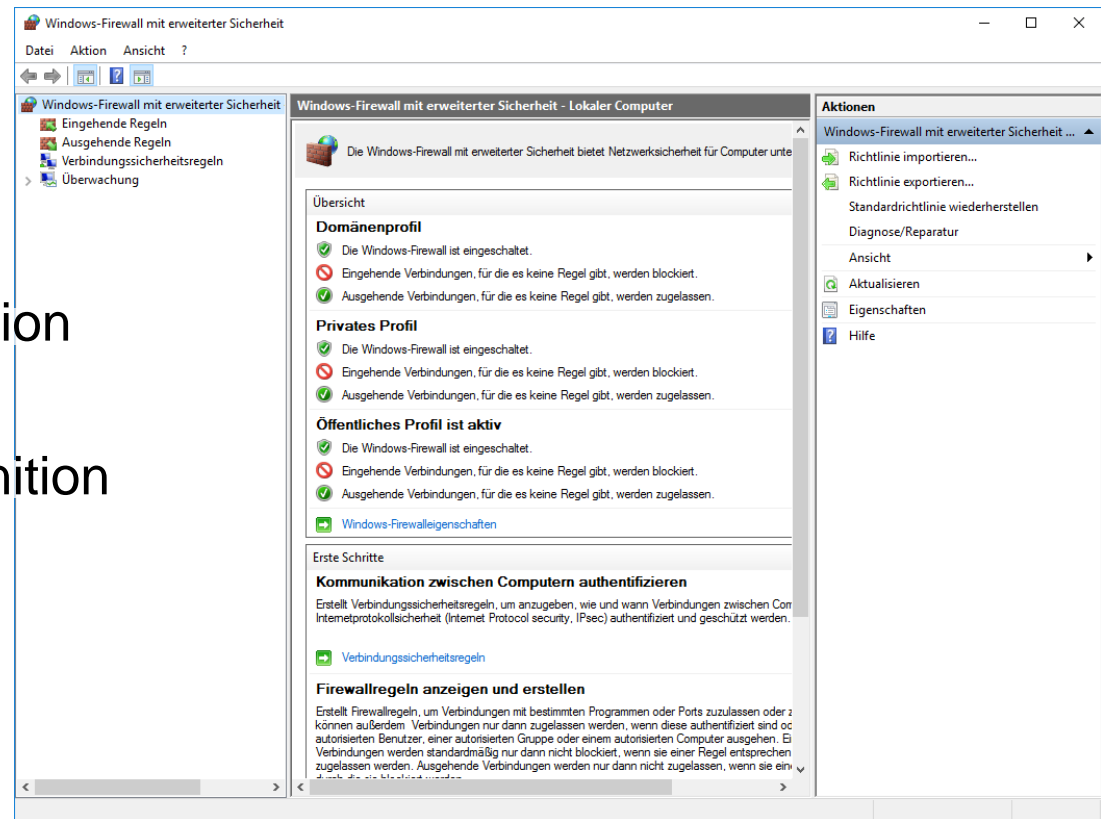
- host-basiert
 - eingehende und
 - ausgehende Regeln
- Software-Firewall
 - auf Basis der Windows Filtering Platform
- Konfiguration in Zonen





Windows-Firewall: erweiterte Einstellungen

- manuelle Konfiguration
- manuelle Regeldefinition

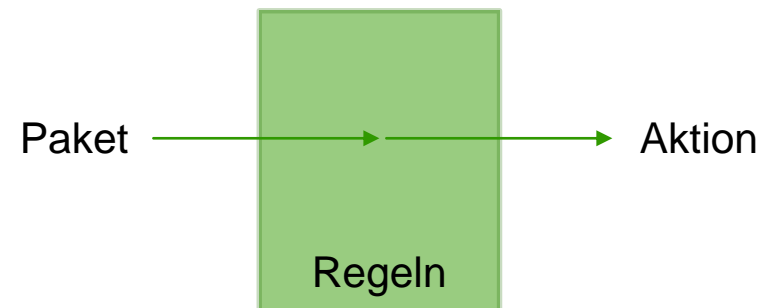
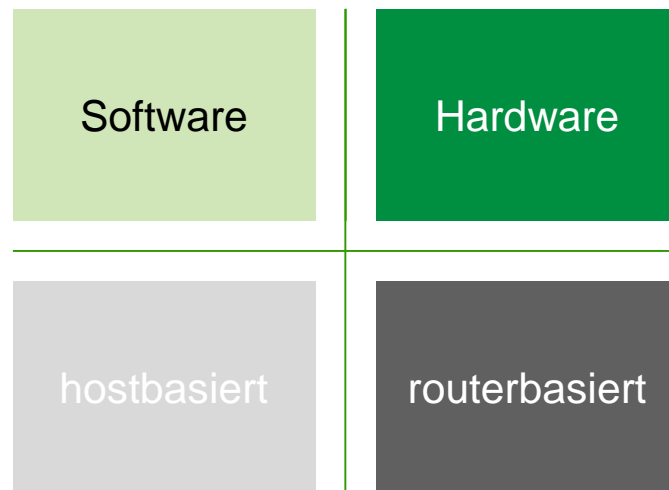




Übung: Windows-Firewall



Zusammenfassung: Firewalls





Netzwerkadministrator

Internetanbindung



Browser



Microsoft Edge

- Kein Support für „Legacy-Technologien“ wie ActiveX und VBscript
- Sicherheitseinstellungen wenig konfigurierbar (ein/aus)
- Gruppenrichtlinienfähig
- Enterprise Mode für den Wechsel zu IE
 - Enterprise Mode Site List Manager + Gruppenrichtlinien für zentrale Config



Internet Explorer: Sicherheitszonen

- Vier Sicherheitszonen



Internet



Lokales Intranet



Vertrauenswürdige
Sites













Eingeschränkte Sites

- URL-basierte Zuteilung
- Separate Sicherheitseinstellungen für jede Zone
- Steuerung der Anzeige von bzw. des Umgangs mit
 - Web-Inhalten (HTML, Grafiken...)
 - Datei-Downloads
 - Benutzer-Authentifizierung
 - .NET Framework-Objekten
 - ActiveX-Steuerelementen
 - Skripts und Erweiterungen



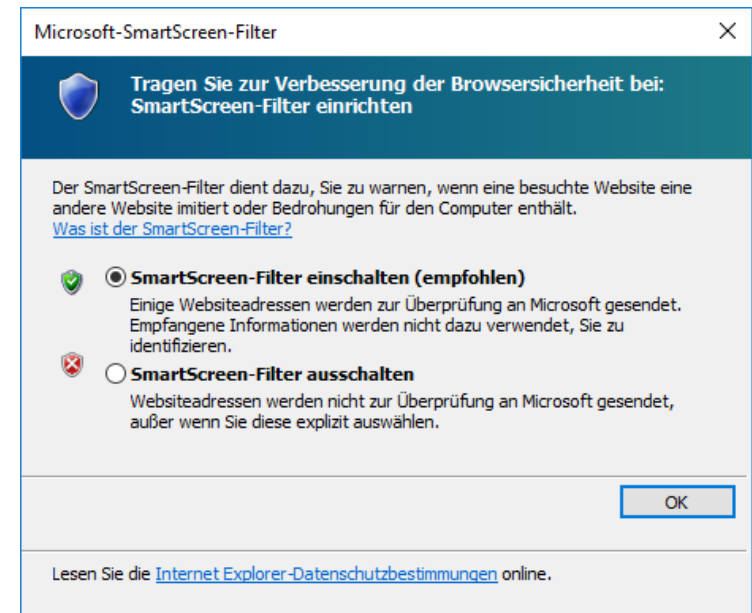
Internet Explorer: Sicherheitszonen

	 Internet	 Lokales Intranet	 Vertrauenswürdige Sites	 Eingeschränkte Sites
Smartscreen-Filterung				
Geschützter Modus				



Smartscreen Filterung

- verwendet eine online gehostete Microsoft Reputations-Datenbank
- hilft, Phishingversuche zu entdecken
- schränkt Download bekannt fragwürdiger Anwendungen ein (unabhängig von der Quelle)
- warnt bei Zugriff auf bekannt fragwürdige Seiten



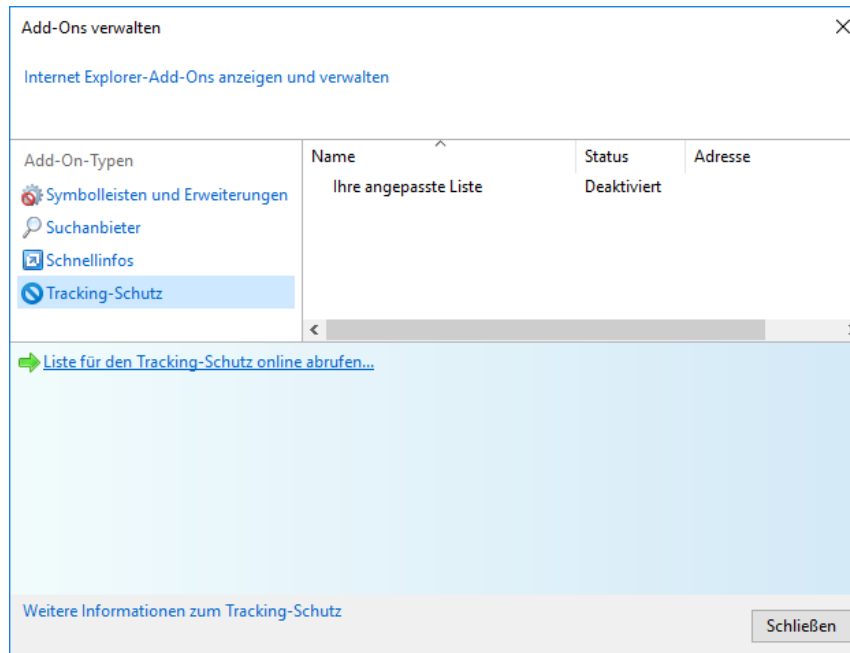


Geschützter Modus

- Anbindung an UAC (User Account Control)
- Ausführung mit verringerten Berechtigungen
- Hilft, Auftreten und Auswirkungen von Malware zu mindern
- Kann vor Ausnutzung von Sicherheitslücken schützen



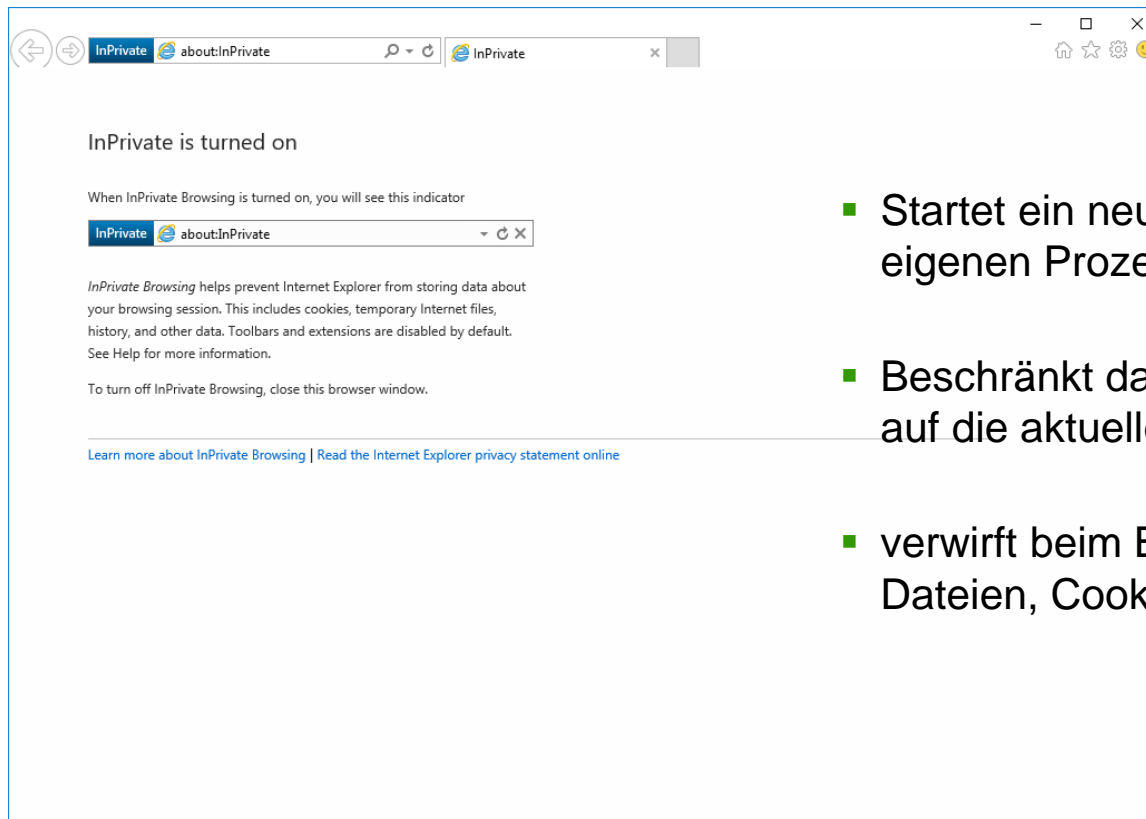
Tracking Protection



- als Browser-AddOn ausgeführt
- verwendet downloadbare Listen
- verhindert Aufruf von bekannten, zum Tracking verwendeten Inhalten



inPrivate



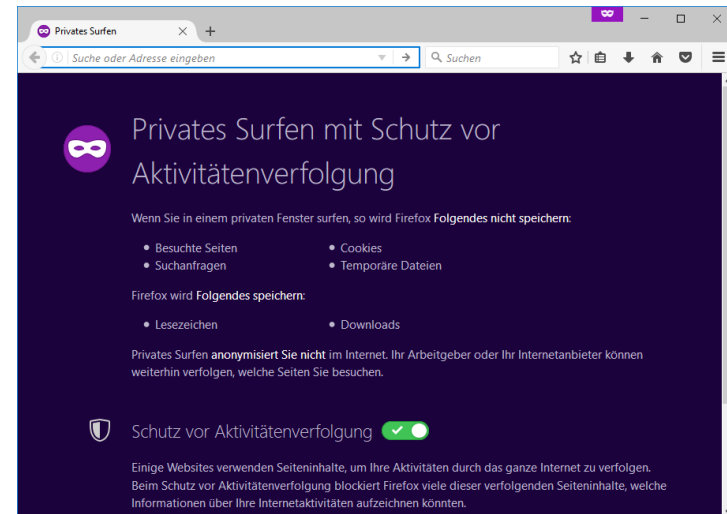
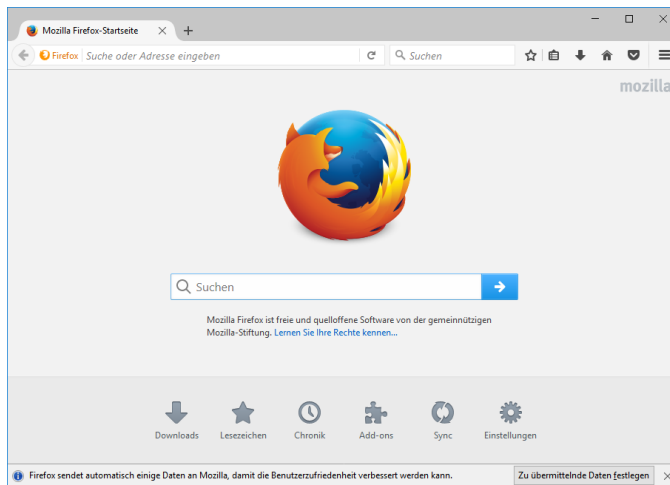
- Startet ein neues Browserfenster in einem eigenen Prozess
- Beschränkt das Anlegen eines Browserverlaufs auf die aktuelle Sitzung
- verwirft beim Beenden sämtliche temporären Dateien, Cookies und gespeicherten Daten



Third-Party Browser

Bieten ebenfalls Betriebsmodi zum Vermeiden eines Verlaufs

z.B. Mozilla Firefox

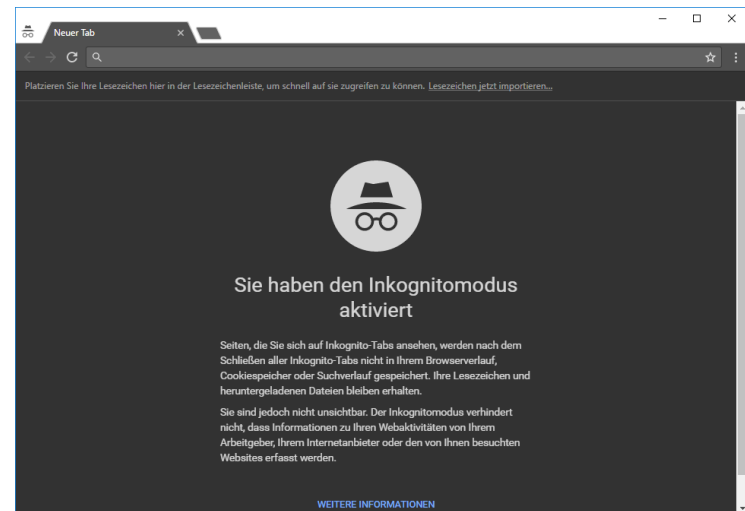
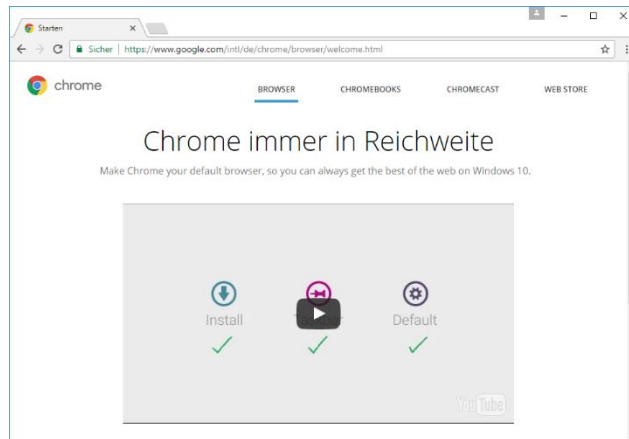




Third-Party Browser

Bieten ebenfalls Betriebsmodi zum Vermeiden eines Verlaufs

z.B. Google Chrome





Third-Party Browser

Bei geplanter bzw. geduldeter Verwendung zu beachten:

- benutzen meist eigene Zertifikatsspeicher
- ActiveX und .NET Framework Unterstützung oft über AddOns
- geringfügige bis ausgeprägte Unterschiede in der Darstellung



Third-Party Browser

Bei geplanter bzw. geduldeter Verwendung zu beachten:

- sind separat zu patchen (kann Administrator-Rechte erfordern)
- kein Automatisches Anmelden möglich (z.B. Intranet-Anwendungen)
- nicht gruppenrichtlinienfähig – keine zentrale Steuerung z.B. der Sicherheitseinstellungen möglich



Netzwerkadministrator

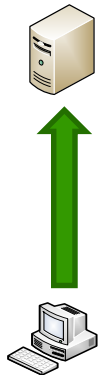
Internetanbindung



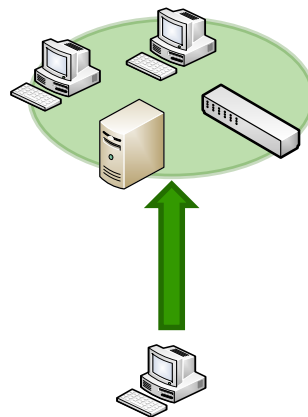
Remote Access



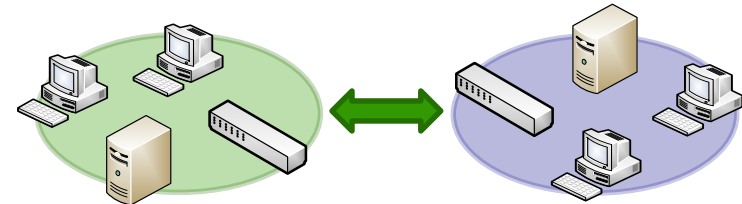
Remote Access



host to host



host to network



network to network

oder

site to site



PPTP – Point-to-Point Tunneling Protocol

- Aufbau durch TCP-Kontrollverbindung (Port 1723)
- PPP-Pakete (meistens verschlüsselt) werden in GRE getunnelt
- Einfach zu implementieren (z.B. host to host, host to site)
- anfällig gegen diverse Brute-Force Methoden
- seit Oktober 2012 offiziell als unsicher eingestuft



SSTP – Secure Socket Tunneling Protocol

- Aufbau durch SSL-Verbindung (Port 443)
- PPP-Pakete werden in HTTPS-Sitzung verschlüsselt
- nutzbar für host to host und host to site
- unterstützt beiderseitige Zertifikats-Authentifizierung
- Implementation erfordert PKI



IPSec

- Authentication Header (AH) und Encapsulated Secure Payload (ESP) bieten Authentifizierung und Schutz vor Manipulation
- unterstützt unterschiedliche Methoden zur Authentifizierung und Verschlüsselungs-Algorithmen
- verschlüsselt nur die Nutzdaten (Transport Mode) oder das ganze IP-Paket (Tunnel Mode)
- Transport Mode meist für host to host, Tunnel Mode für site to site



Proprietäre Implementationen

- auf Hardware-Firewalls namhafter Hersteller vorinstalliert (z.B. Cisco, Sonicwall, Juniper, etc.)
- meist eigener Client erforderlich (mitgeliefert)
- Authentifizierungs- und Verschlüsselungsmethoden wählbar
- geringer Konfigurationsaufwand
- oft nach User lizenziert



Netzwerkadministrator

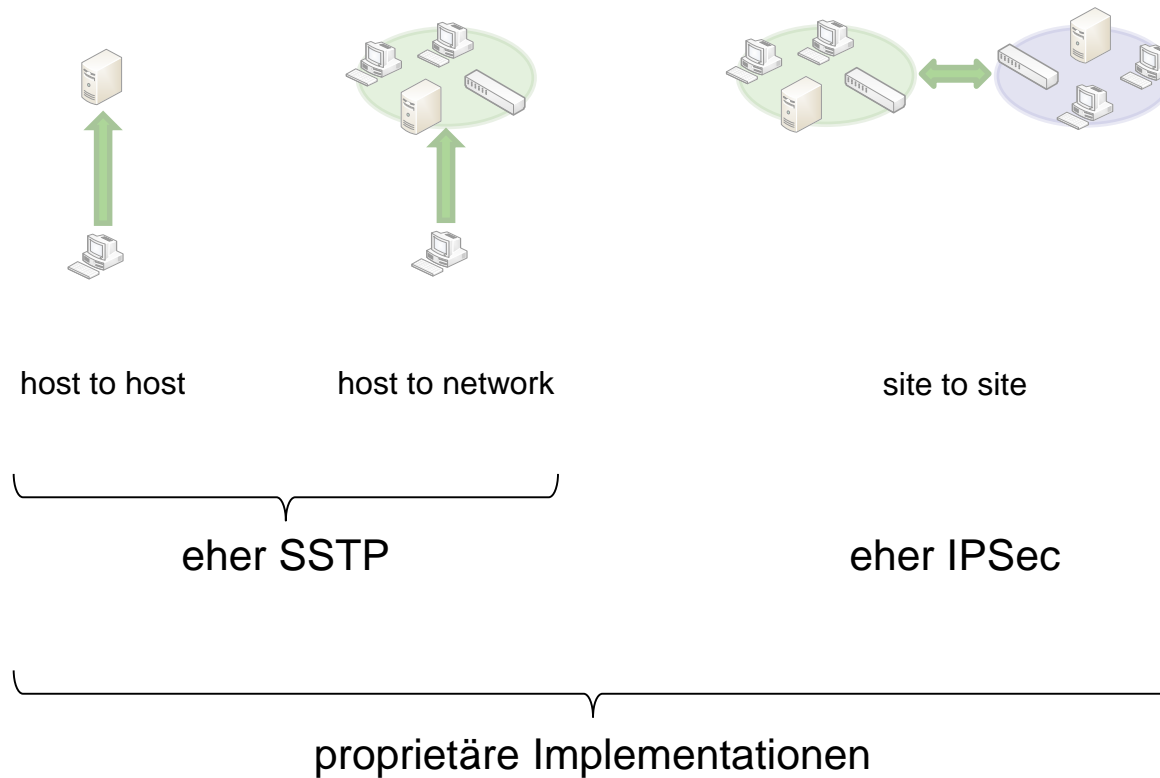
Internetanbindung



Übung: VPN



Zusammenfassung: Remote Access





Netzwerkadministrator

Internetanbindung



Remoteunterstützung



Remoteunterstützung

- MSRA.exe - Bordmittel seit Windows Vista
- EasyConnect benötigt IPv6 (direkt oder getunnelt)
- Einladung (User zu Helfer) über diverse Medien (Datei, eMail, Messenger)
- Ohne Einladung (Helfer zu User) über AD Domain Policy
- User muss immer bestätigen



Netzwerkadministrator

Internetanbindung



Übung: Remoteunterstützung