



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen





Überblick

Was Sie in den nächsten
24 Lehreinheiten erwartet:



- Einstiegsdiskussion
- Passive Netzwerkhardware
- Ethernet
- WLAN
- Routingfähigkeit
- TCP/IP Grundlagen
 - Layer 4 Troubleshooting
 - IP-Adressierung und Layer 3 Troubleshooting
 - Switching und Layer 2 Troubleshooting
- Namensauflösung
- DHCP
- IPv6 (optional)
- VLANs



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Diskussion



Diskussion

Was bezeichnet man eigentlich als "LAN"?

Das Computernetzwerk, das im Allgemeinen zu Anschaltung der Rechner innerhalb des Standorts eines Unternehmens oder aber auch zu Hause verwendet wird.

Die Abkürzung LAN steht für Local Area Network



Diskussion

Wie heißt der heute übliche Netzwerk-Standard im kabelgebundenen LAN-Bereich?

Ethernet



Diskussion

Wie alt ist Ethernet eigentlich schon?

Entwickelt in den 1970ern und 1980ern
1985 standardisiert
Seitdem beständig weiterentwickelt



Diskussion

Wie werden Geschwindigkeiten/Bandbreiten/Datenraten von Computernetzwerk-Verbindungen gemessen?

Mbit/s (Megabit pro Sekunde)
Gbit/s (Gigabit pro Sekunde)



Diskussion

Welche Geschwindigkeiten wurden bei Ethernet definiert?

10MBit/s

Veraltet

Keine Neugeräte

100MBit/s

HomeOffice

Industrienetzwerke

1GBit/s

Typischer Client

Kleinere Server

10GBit/s

Netzwerkverteilung

Virtualisierungs-
Server

40GBit/s

Netzwerkverteilung

deprecated



Diskussion

Welche Geschwindigkeiten wurden bei Ethernet definiert?

2.5GBit/s	5GBit/s	25GBit/s	50 GBit/s	100GBit/s
WLAN Access Points	Server Netzwerkverteilung	Server	Netzwerkverteilung Server	Netzwerkverteilung



Diskussion

Welche Datenrate hat Ihr Internetzugang zu Hause im Vergleich?

...



Diskussion

Was bedeutet jetzt eigentlich 1 GBit/s?
Sind wir nicht eher MB/s gewohnt?

1 Byte = 8 Bit
Also MBit/s / 8 = MB/s
1000 MBit/s / 8 = 125 MB/s



Übung - Datenraten

- Ihr Trainer kopiert eine größere Datei von einem Rechner im Netz auf den Desktop seines lokalen Rechners
- Was können Sie über die Netzwerkanbindung beider Rechner sagen?
- Kopieren Sie nun alle gleichzeitig die Datei auf Ihren Desktop
- Was fällt Ihnen auf?



Diskussion

Betrachten Sie nochmals die erreichte Datenrate aus dem ersten Übungsbeispiel. Wieso wurde die theoretische Maximal-Datenrate nicht erreicht?

Management-Information zählt nicht zu den Nutzdaten

Kann die restliche Hardware der beteiligten Rechner die Daten schnell genug anliefern/schreiben?



Diskussion

Nehmen wir an, Sie möchten eine 4 GB große Datei über das Netzwerk kopieren.

In welcher Form werden die Daten übertragen?

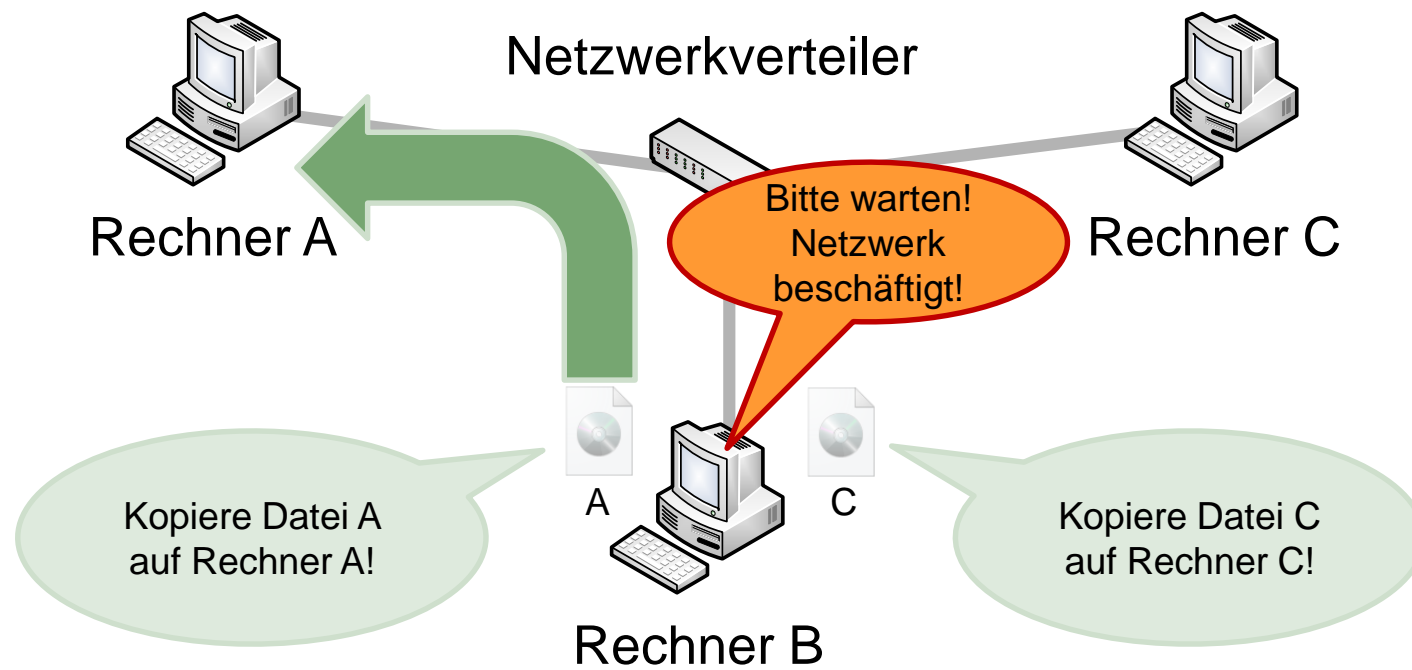
In Paketen

Auf Ethernet ist ein Paket ca. 1500 Bytes groß und wird als "Frame" bezeichnet



Warum eigentlich Pakete?

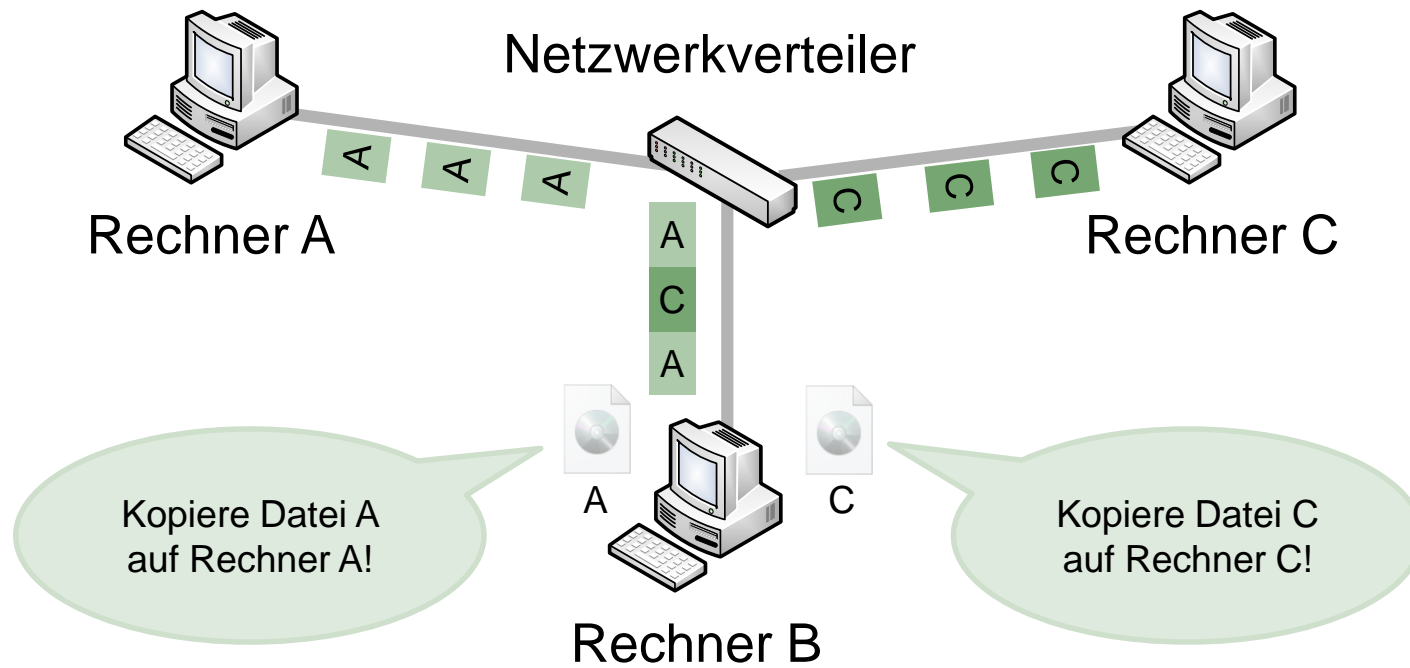
- Wenn alles auf einmal übertragen würde....





Warum eigentlich Pakete?

- Und jetzt mit Paketen....





Diskussion

Damit die Pakete ihren Weg finden, welche Information muss jedes Paket zusätzlich zu den Nutzdaten tragen?

Irgendeine Form von Adressen auf jedem Paket

Diese Adressen zählen unter anderem zu den zuvor erwähnten Management-Informationen, welche die Nutzdatenrate reduzieren



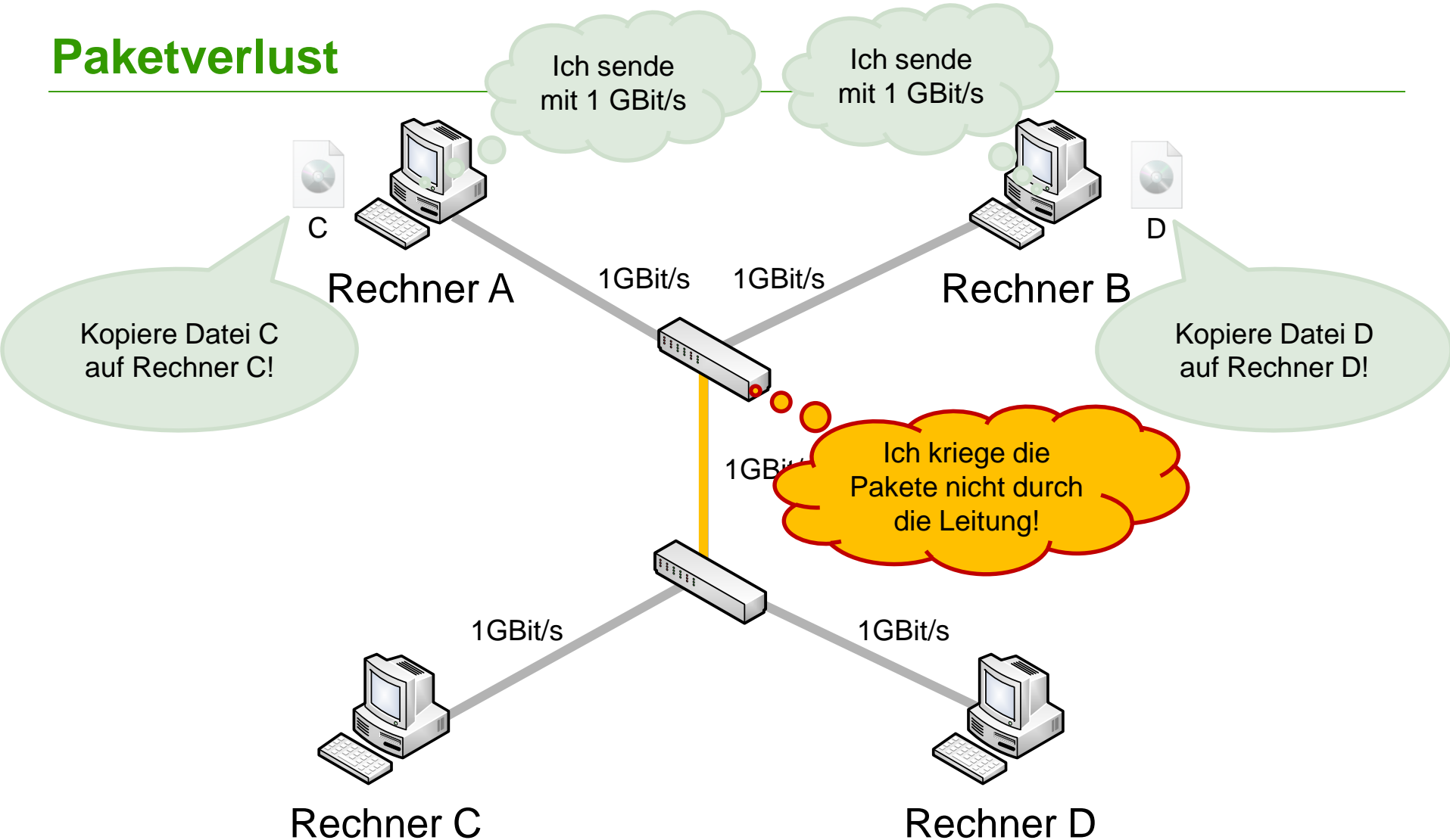
Diskussion

Kann es sein, dass Pakete während der Übertragung verloren gehen?

Versuchen Sie ein Szenario zu entwickeln, in dem es zu Paketverlusten kommt

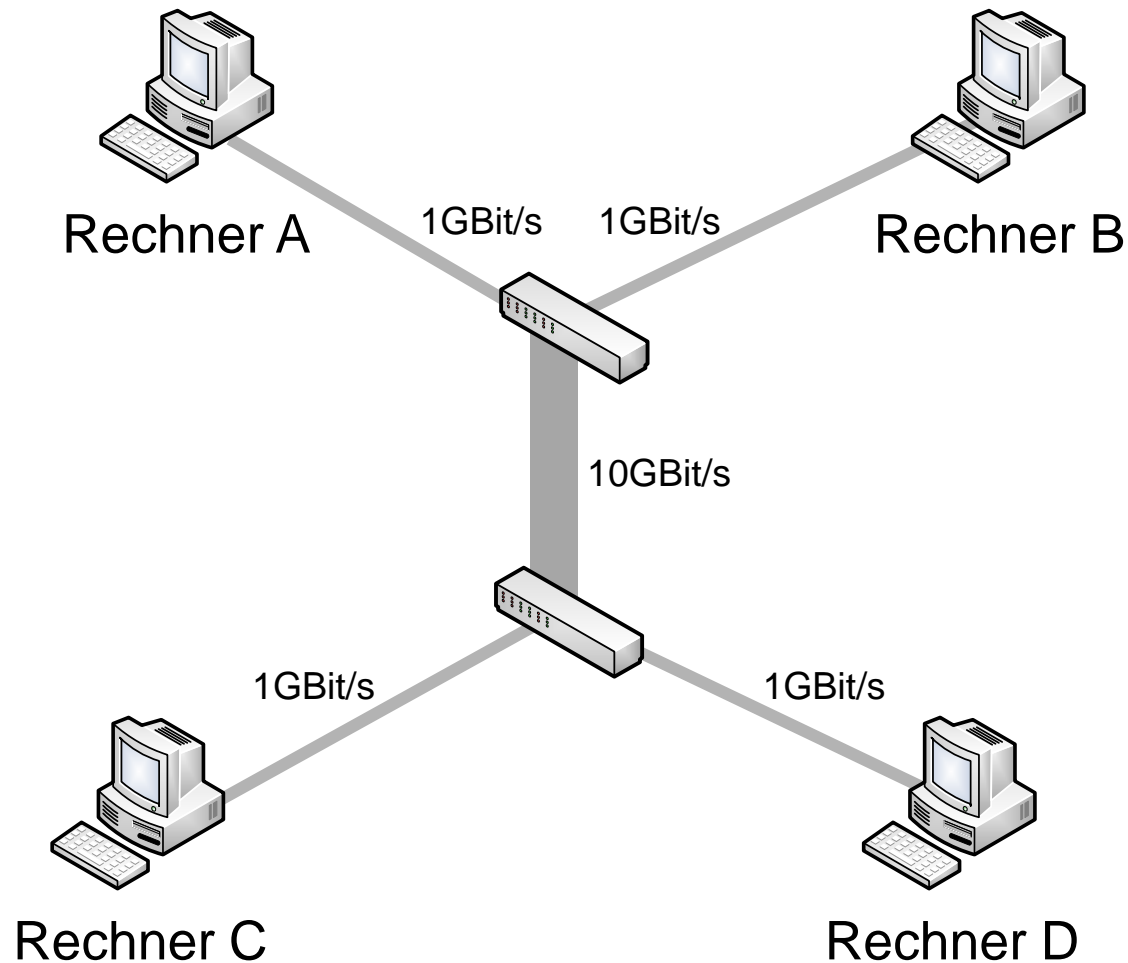


Paketverlust





Ein möglicher Ansatz





Diskussion

Ist Paketverlust in einem LAN etwas 'Normales' oder ein Ausnahmefall?

In Situationen zeitweiser hoher Auslastung ist Paketverlust normal und bei den meisten Anwendungen akzeptabel.

Bei dauerhafter Auslastung und damit einhergehendem Paketverlust besteht Handlungsbedarf.



Diskussion

Die Erfahrung lehrt aber, dass wir riesige Dateien fehlerfrei über ein Netzwerk herunterladen/kopieren können.

Warum funktioniert das trotz möglichem Paketverlust?

Auf den Rechnern ist eine Softwarekomponente – das Netzwerkprotokoll – installiert.

Dieses erkennt - wenn gewünscht - verlorene Pakete, überträgt sie erneut und passt die Senderate so an, dass keine Pakete mehr verloren gehen sollten.

Ein Netzwerkprotokoll hat noch eine Vielzahl anderer Aufgaben



Diskussion

Wie heißt die heute am meisten verwendete Sammlung von Netzwerkprotokollen?

TCP/IP

Doch bevor wir uns mit Software beschäftigen, reden wir über..



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Passive Netzwerkhardware

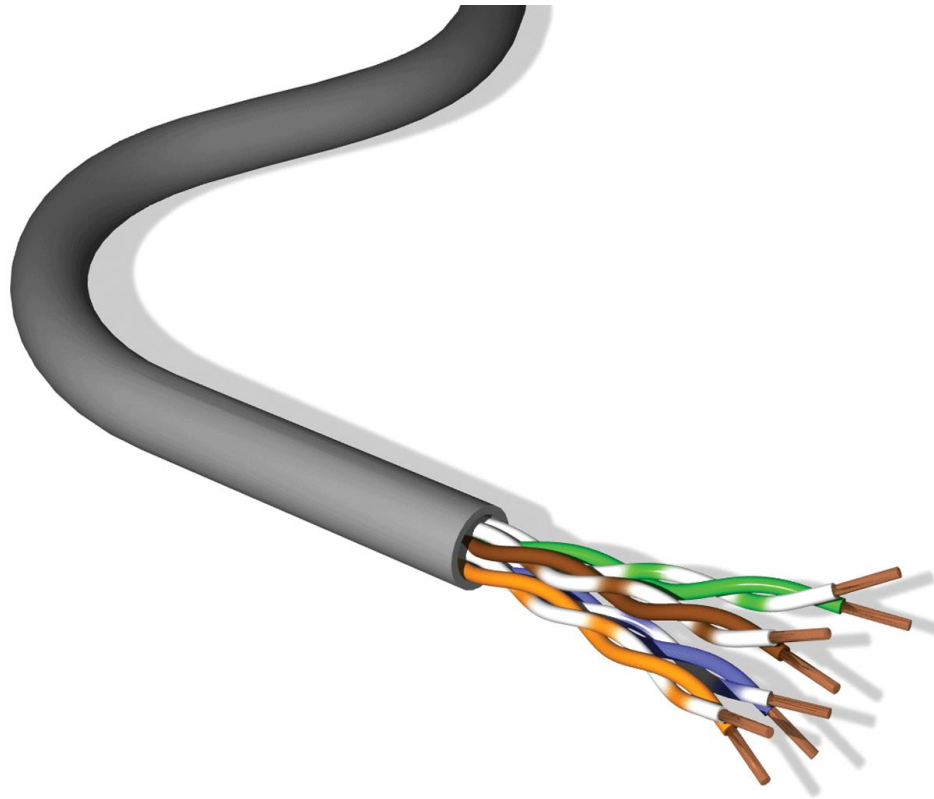


Warum reden wir über Verkabelungen?

- Eine Netzwerkverkabelung kann 20-25 Jahre im Einsatz sein
- Die Kosten für Verkabelungsarbeiten sind auch in kleinen Umgebungen relativ hoch
- Daher müssen Sie in der Lage sein
 - festzustellen, welche Verkabelung Sie mindestens für Ihre Anforderungen benötigen
 - das Angebot eines Installationsunternehmens interpretieren zu können



Twisted-Pair-Kabel





Twisted-Pair Kabel

- 4 Adernpaare
- Maximale Bandbreiten

CAT 3	16MHz	veraltet
CAT 5, CAT5e	100 MHz	Bestandsinstallationen
CAT 6	250 MHz	häufig
CAT 6 _A	500 MHz	häufig, optimiert für 10GbE
CAT 7*	600 MHz	Neuinstallationen*
CAT 7 _A *	1000 MHz	selten*
CAT8	2000 MHz	Rechenzentren

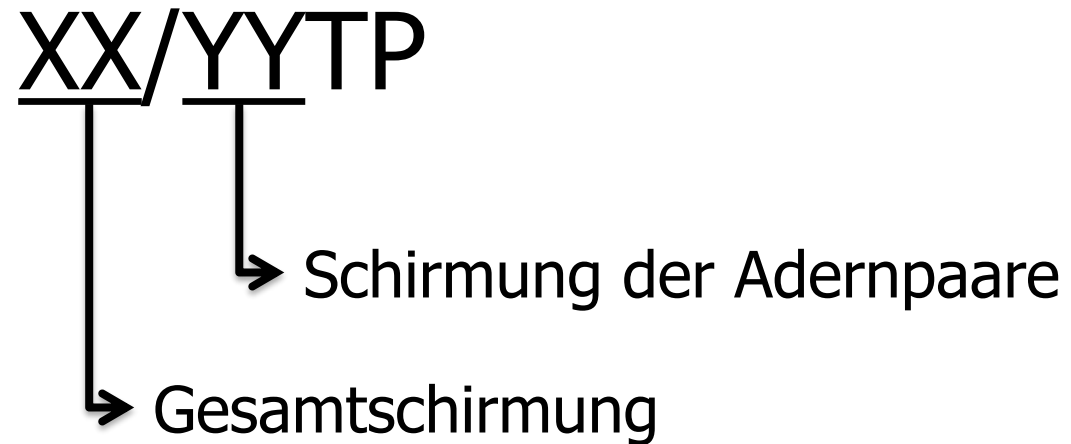
*Kein EIA Standard

- Die Bandbreite bestimmt, ob das Kabel einen bestimmten Ethernet-Standard (z.B. 10Gbit/s) übertragen kann. Später mehr!



Twisted-Pair-Kabel

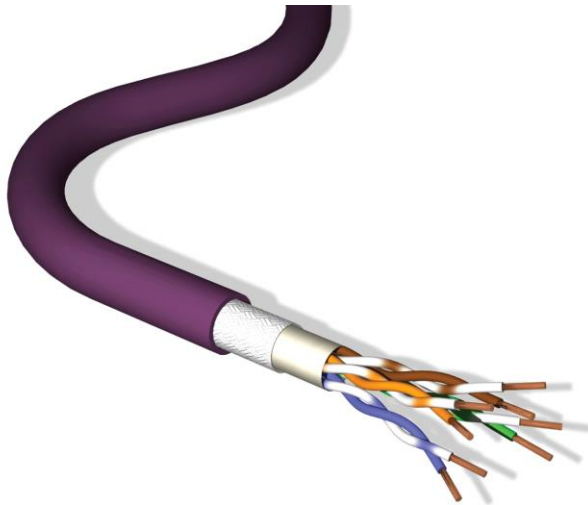
- Abschirmung



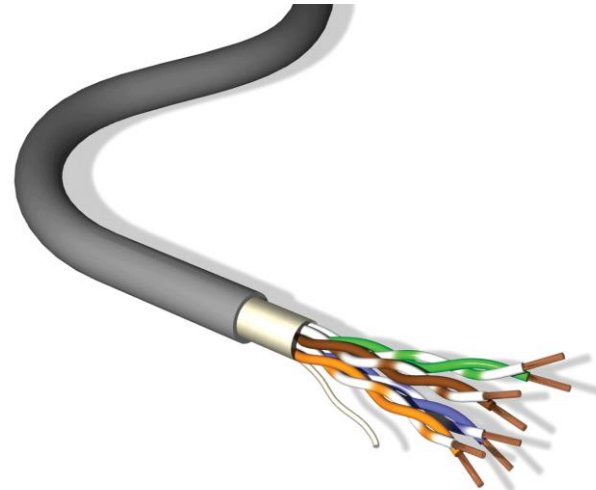


Twisted-Pair-Kabel

- SF/UTP



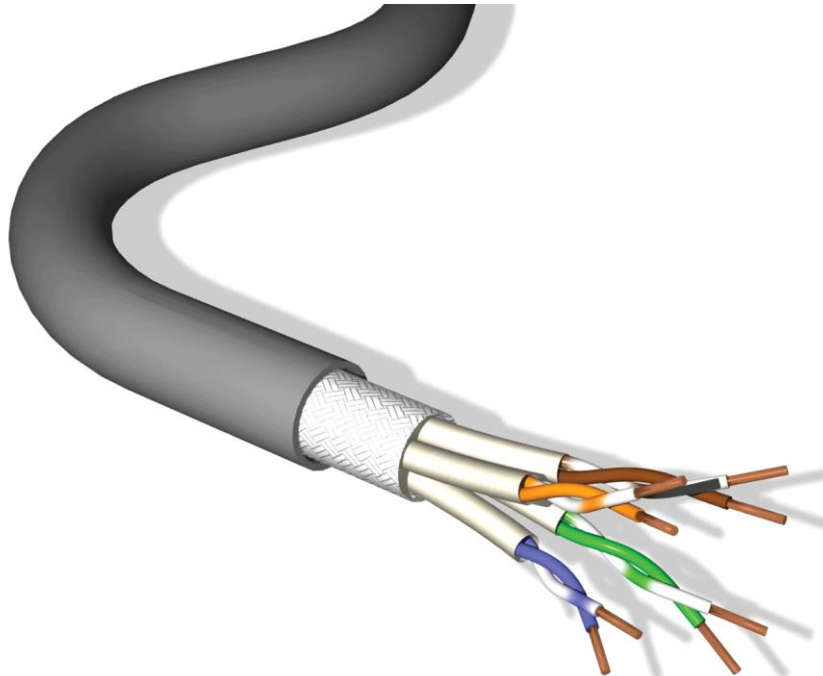
- F/UTP





Twisted-Pair-Kabel

- S/FTP





Noch ein paar Worte zur Abschirmung

Kategorie	Abschirmung
CAT 3	optional
CAT 5, CAT5e	optional
CAT 6	optional
CAT 6 _A	optional
CAT 7*	vorgeschrieben
CAT 7 _A *	vorgeschrieben
CAT8	vorgeschrieben



Stecker

- Stecker-Norm:
 - 8P8C (umgangssprachlich RJ45)





Lichtwellenleiter

- Im LAN-Bereich:
 - Verkabelungen zwischen Gebäudeteilen
 - Verkabelungen durch Produktionshallen (EMI)
 - Zur direkten Rechner-Anbindung unüblich (außer im Storage-Bereich)

Zwischen Gebäuden immer LWL

Vertikal LWL – horizontal Kupfer
(wenn das ihre finanzielle Situation erlaubt)



Lichtwellenleiter

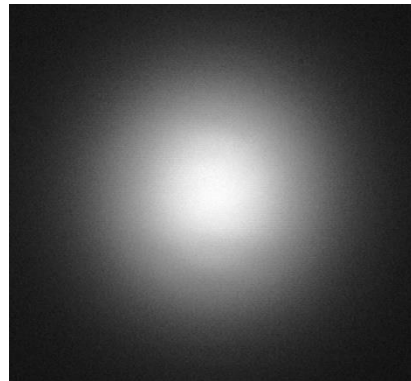
- MultiMode-Fasern
 - kürzere Längen überbrückbar
 - Transceiver billiger
 - 50/125µm (häufig) 62,5/125µm (selten)
 - Stecker von Patchkabeln: grau
 - „Kategorien“: OM1 (oranges Kabel), OM2 (oranges Kabel), OM3 (türkises Kabel), OM4

- MonoMode oder SingleMode -Fasern
 - größere Längen überbrückbar
 - Tranceiver teurer
 - 9/125µm (häufig)
 - Stecker von Patchkabeln: blau
 - „Kategorien“: OS1 (gelbes Kabel), OS2 (gelbes Kabel)

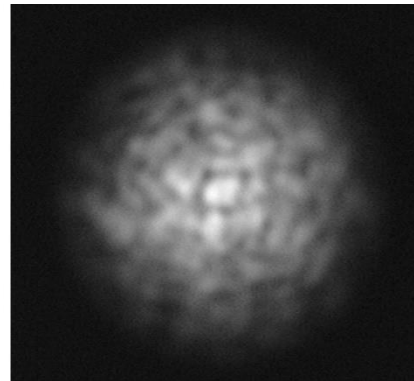


Lichtwellenleiter

- Wieso reichen Monomode-Fasern eigentlich weiter?



Monomode



Multimode

Quelle: Wikipedia

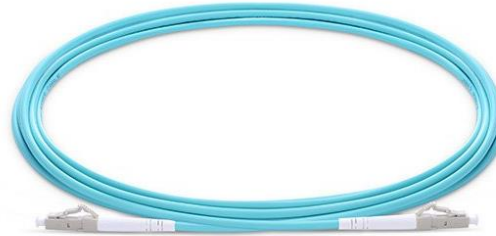
Von Kirnehkrib - Eigenes Werk, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=17511799>



LWL Patchkabel



OM 1/2



OM 3



OM 4



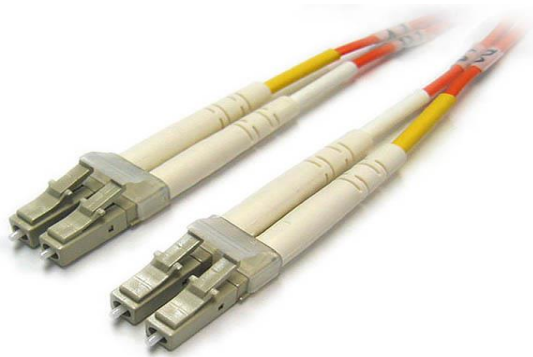
OS 1/2



übliche LWL-Steckernormen



ST-Stecker



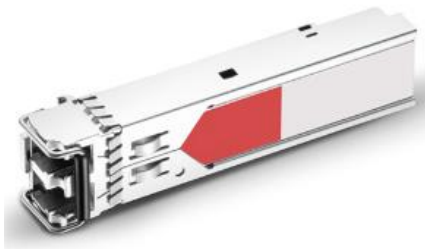
LC Stecker



SC-Stecker



LWL im LAN-Bereich



- SFP Modul
- SFP+ Modul
- auch als GBIC bezeichnet
- Bis maximal 10GBit/s



SFP- Einschübe auf einem Switch
Teilweise gemeinsam mit Kupferports genutzt,
wie im Bild ersichtlich

Achtung: Die meisten Switches akzeptieren nur SFPs vom selben Hersteller



LWL im LAN-Bereich



- QSFP Modul
- QSFP+ Modul
- 10GBit/s bis 100GBit/s



Direct Attach Cable

- Kupfer-Ports für 10Gbit/s und höher sind verhältnismäßig teuer
- Die volle Übertragungslänge wird in Serverräumen meist nicht benötigt
- LWL-Transceiver sind auch teuer
- LWL-Übertragungslängen werden in Serverräumen schon gar nicht benötigt
- DAC:
 - Kabel mit zwei SFP+/QSFP-Enden
 - Vorkonfektionierte Längen (50 cm bis 10m)
 - Verhältnismäßig billig (50-200 EUR)
 - Fanouts möglich (Eine Seite 100Gbit/s, vier 25Gbit/s Seiten)
 - Optimal zur Serveranbindung
- Vorsicht bei Geräten verschiedener Hersteller, da viele Geräte nur herstellereigene SFP+/QSFPs akzeptieren



DAC



QSFP DAC



QSFP/SFP+ DAC
1x 40GbE auf 4x 10 GbE



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Power over Ethernet (PoE)



PoE – Power over Ethernet

- Stromversorgung von Geräten über das Netzkabel
 - über PoE-Switch
 - oder über Power Injector
- Nicht PoE-fähige Geräte an PoE Ports nehmen keinen Schaden (Verhandlung vor Stromversorgung)
- Üblich für
 - WLAN Access Points
 - Telefone
- 5 Klassen, Klasse gibt max. Leistungsbedarf an
- Bis zu 25W (Klasse 4) - Spannung bis zu 57V!

Achtung: Switches haben meist eine Gesamtleistung, die überschritten werden kann, wenn auf zu vielen Ports die volle Leistung benötigt wird.



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Ethernet



Ethernet

- Entwickelt in den 70igern und 80igern
- 1985 standardisiert
- Definiert in IEEE 802.3
 - Physikalische Topologie: Bus oder Stern (heute üblich)
 - Logische Topologie: Bus
 - physikalische Medien: Koaxkabel, TwistedPair-Kabel, LWL



Ethernet 100MBit/s

Name	Kabel	Max. Länge	Top.	
100BASE-TX	>CAT5*	100m	Stern	häufig
100BASE-FX	2xLWL MultiMode	400m (HalfDuplex) 2km (FullDuplex)	Stern	
100BASE-SX	2xLWL MultiMode	550m	Stern	häufig

* Nur zwei Adernpaare verwendet



Ethernet 1GBit/s

Name	Kabel	Max. Länge	Top.	
1000BASE-T	> CAT5*	100m	Stern	DER STANDARD 4 Adernpaare
1000BASE-SX	2xLWL MultiMode	550m	Stern	häufig
1000BASE-LX	2xLWL MonoMode	5000m	Stern	häufig

* CAT5e empfohlen



Ethernet 10GBit/s (10GbE)

Name	Kabel	Max. Länge	Top.	
10GBASE-T	CAT5e CAT6 $\geq \text{CAT6}_A$	45m 55m 100m	Stern	
10GBASE-SR	2xMultimode-LWL OM2 OM3 OM4	82m 300m 400m	Stern	SAN
10GBASE-LR	2xMonoMode-LWL	10.000m	Stern	SAN



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Power over Ethernet (PoE)



PoE – Power over Ethernet

- Stromversorgung von Geräten über das Netzkabel
 - über PoE-Switch
 - oder über Power Injector
- Nicht PoE-fähige Geräte an PoE Ports nehmen keinen Schaden (Verhandlung vor Stromversorgung)
- Üblich für
 - WLAN Access Points
 - Telefone
- 5 Klassen, Klasse gibt max. Leistungsbedarf an
- Bis zu 25W (Klasse 4) - Spannung bis zu 57V!

Achtung: Switches haben meist eine Gesamtleistung, die überschritten werden kann, wenn auf zu vielen Ports die volle Leistung benötigt wird.



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Duplexmodus



Vollduplex - Halbduplex

- nur bei 10/100MBit/s Ethernet
- Halbduplex:
 - 1 Adernpaar für Datenübertragung
 - 1 Adernpaar für Kollisionserkennung
- Vollduplex:
 - 1 Adernpaar zum Senden
 - 1 Adernpaar zum Empfangen
 - Keine Kollisionen
- AutoNegotiation sorgt für häufige Probleme, besonders bei
 - Internetmodems
 - VoIP-Telefonen
 - SPS



Übung - Duplexmodus

- Konfigurieren Sie Ihre Netzwerkkarte für Vollduplex-Betrieb!
- Konfigurieren Sie Ihr Switchport für Vollduplex-Betrieb!

```
ProCurve Switch 5406zl                               10-Jan-2013  12:52:38
===== TELNET - MANAGER MODE =====
Switch Configuration - Port/Trunk Settings

  Port      Type      Enabled      Mode      Flow Ctrl  Group  Type
  ----      -
B18    1000T      | Yes      Auto      Disable
B19    1000T      | Yes      10FDx     Disable
B20    1000T      | Yes      Auto-1000 Disable
B21    1000SX     | Yes      Auto      Disable
B22    1000SX     | Yes      Auto      Disable
B23    1000SX     | Yes      Auto      Disable
B24    1000SX     | Yes      Auto      Disable
C1     1000T      | Yes      Auto      Disable
Actions->  Cancel    Edit      Save      Help
```



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



WLAN / WiFi



Wireless LANs

- lokales Funknetz
- auch WiFi
- geteilte Bandbreite
- Betriebsmodi
 - Ad-Hoc Betrieb (Rechner zu Rechner)
 - Infrastrukturmodus (Betrieb über Access Points)
- Entwickelt in den 90igern
- Standards in der IEEE 802.11-Familie

- Beachten Sie, dass im Einzelhandel kaum mehr Access-Points, sondern nur mehr Router verkauft werden! Wenn Sie nur Ihr LAN auf WLAN 'verlängern' wollen, ist das nicht das richtige Gerät!



WiFi Standards

Name	Geschwindigkeit (theoretisch)	Geschwindigkeit (realistisch)	Frequenz	
802.11a	54Mbit/s	ca. 20MBit/s	5GHz	selten
802.11b	11MBit/s	ca. 5MBit/s	2,4GHz	selten
802.11g	11/54Mbit/s parallel	ca. 20MBit/s	2,4GHz	häufig
802.11n	600MBit/s	ca. 100MBit/s	2,4 bzw. 5GHz umschaltbar	häufig
802.11ac	1.3Gbit/s	ca. 230MBit/s	5GHz	'emerging'



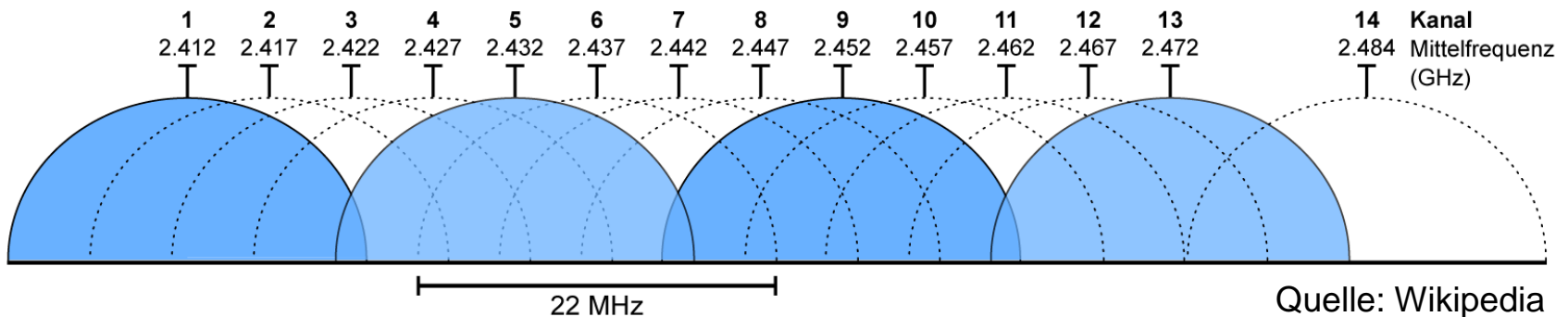
Kanäle und Frequenzen bei 802.11n

- 802.11n unterstützt 2 Frequenzbänder
 - 2.4 GHz, 14 Kanäle
 - 5GHz, 19 bzw. 9 Kanäle
- Endgeräte können
 - in manchen Fällen nur 2.4 GHz
 - oder 2.4 oder 5GHz alternativ



802.11n - 2.4 GHz

- Ein Kanal benötigt für optimale Leistung 20MHz Bandbreite
- Die 14 Kanäle befinden sich zwischen 2.412 und 2.484 GHz
- Im 2.4 GHz Bereich kann es zu Interferenzen durch Mikrowellenherde kommen!
- Kanäle erlauben Überlappungen, die den Durchsatz reduzieren
 - Nur Kanäle 1,5,9,13 sind nahezu überlappungsfrei nutzbar



- Beispiel zur Kanalbelegung:
Graz, Innenstadt, dicht bebautes Wohngebiet:

41 WiFi Netze!



Mehrere WiFi-Netzwerke auf einem Kanal

- Es wird für den Empfänger schwerer, das gewünschte Signal zu extrahieren
- Dadurch sinkt die Reichweite
- Stellen Sie sich vor, Sie möchten sich in einem lauten Lokal mit einem Freund unterhalten



Was tun?

- Setzen Sie die Kanalwahl Ihres APs auf "Automatisch"
- Verwenden Sie 802.11n mit 5GHz!
 - Stellen Sie sicher, dass alle Geräte auch wirklich 5GHz unterstützen!
 - Wenn nicht verwenden Sie Dual-Radio Access-Points!
 - 20 MHz Bandbreite: 19 überlappungsfreie Kanäle
 - 40 MHz Bandbreite: 9 überlappungsfreie Kanäle (besserer Durchsatz)
 - Die Kanalbandbreite ist bei guten APs konfigurierbar!
- Teilweise Probleme mit Wetterradaren
- Weniger Probleme im Ballungsgebieten
 - Weniger 5GHz Installationen
 - Mehr Kanäle



Ein paar Worte zu 802.11ac

- Ausschließlich 5GHz
- Bandbreiten:
 - 20MHz: 19 Kanäle
 - 40MHz: 9 Kanäle
 - 80MHz: 4 Kanäle
 - 160MHz: Zwei Kanäle
- "Datenblattleistung" nur bei 160 MHz und MIMO Installationen
- AC wird daher noch zögerlich eingesetzt



WLAN-Herausforderungen

Wer kann mein Signal empfangen?

Verschlüsselung

Wer darf mein WLAN verwenden?

Authentifizierung

Wie weit muss mein Signal reichen?

Sendeleistung, Antennen, Roaming



Sicherheitstypen

Typ	Authentifizierung	Verschlüsselung	Sicherheit	Kompatibilität
offen	keine	keine	keine	hoch
WEP	PreSharedKey	WEP (RC4) 64/128 Bit	niedrig	hoch
WPA Personal	PreSharedKey	TKIP (RC4)	hinreichend	hoch
WPA Enterprise	Zentrale Authentifizierung	TKIP (RC4)	hinreichend	hoch
WPA2 Personal	PreSharedKey	AES	hoch	Gut
WPA2 Enterprise	Zentrale Authentifizierung	AES	hoch	Gut



WLAN Planung um wenig Geld

- VisiStumbler (<https://www.vistumbler.net/>)
 - Welche WiFis gibt es in der Umgebung?
 - Welche Kanäle verwenden diese?
 - Wie stark kann ich diese empfangen?
- Ein paar Worte zur Signalstärke
 - alles bis -67dBm: OK
 - bis -72dBm: Brauchbar
 - darunter: unbrauchbar
- Wirelessmon (www.passmark.com)
 - Messung der Empfangsstärke+ Interpolation auf Gebäudeplan
- Und wenn Geld keine Rolle spielt: Airmagnet, Ekahau



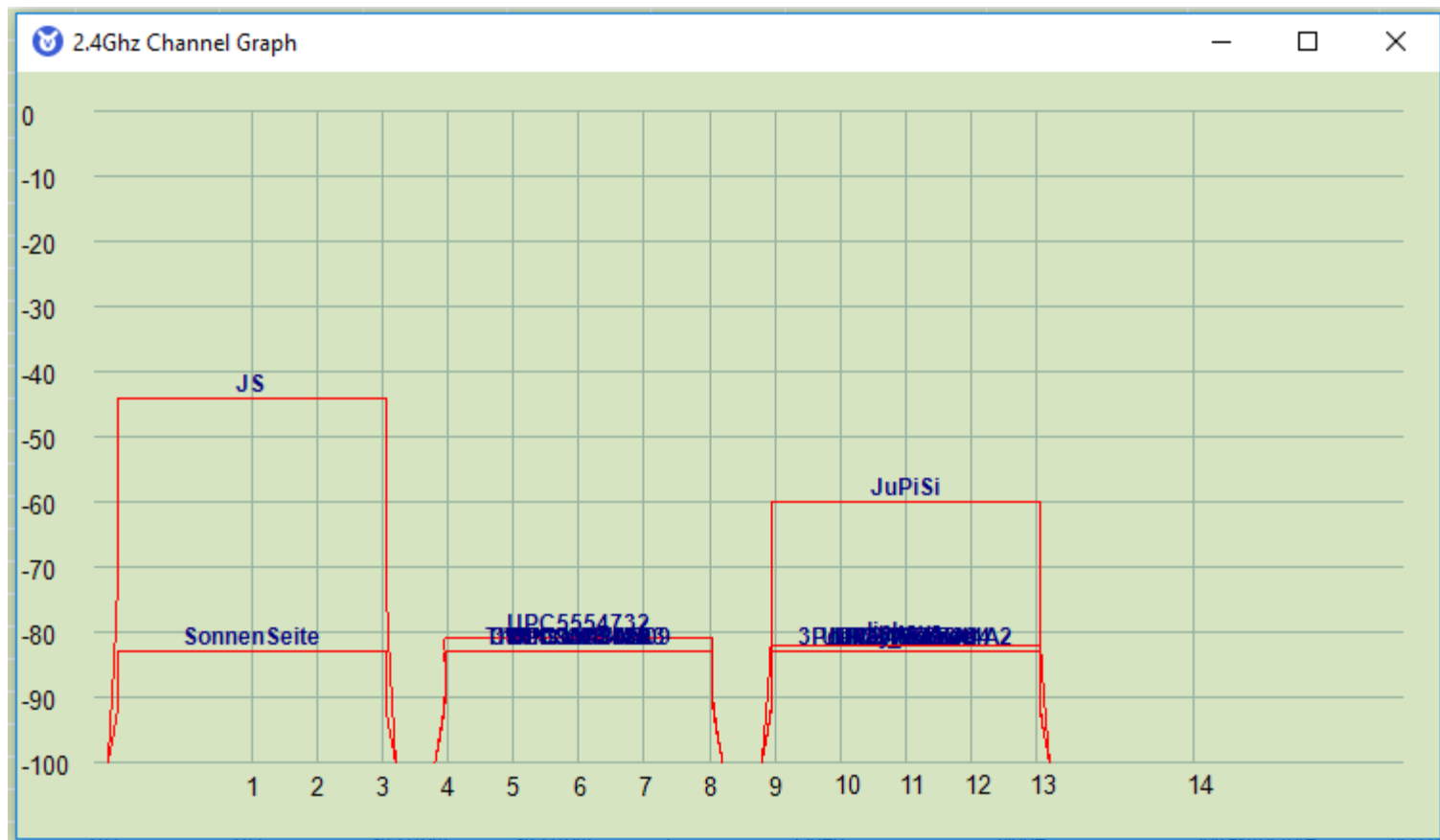
Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



VisiStumbler

- Viel Spaß mit 2.4 GHz an dem Standort ;-)





Verbinden mit einem WLAN

- Was muss bekannt sein?
 - Netzwerkname (SSID)
 - Verschlüsselungsstandard
 - Authentifizierung

- Bedingt sinnvolle Schutzmechanismen
 - Abschalten des SSID-Broadcasts
 - Einrichten von MAC-Filtern



WLAN-Übung

- Ermitteln Sie die Kanalbelegung im 2,4GHz-Bereich mit Hilfe von VisiStumbler
- Errichten Sie ein WLAN und verwenden Sie folgende Einstellungen:
 - 802.11n, 5GHz, 40MHz Kanalbandbreite
 - SSID: NA
 - Verschlüsselung: WPA mit AES
 - Authentifizierung: Preshared Key: 602adgl363
- Überprüfen Sie die Funktionalität
- Installieren Sie die Eval-Version von Wirelessmon auf einem Notebook
- Laden Sie den Gebäudeplan des WIFIs
- Machen Sie eine Messung!



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



TCP/IP - Grundlagen



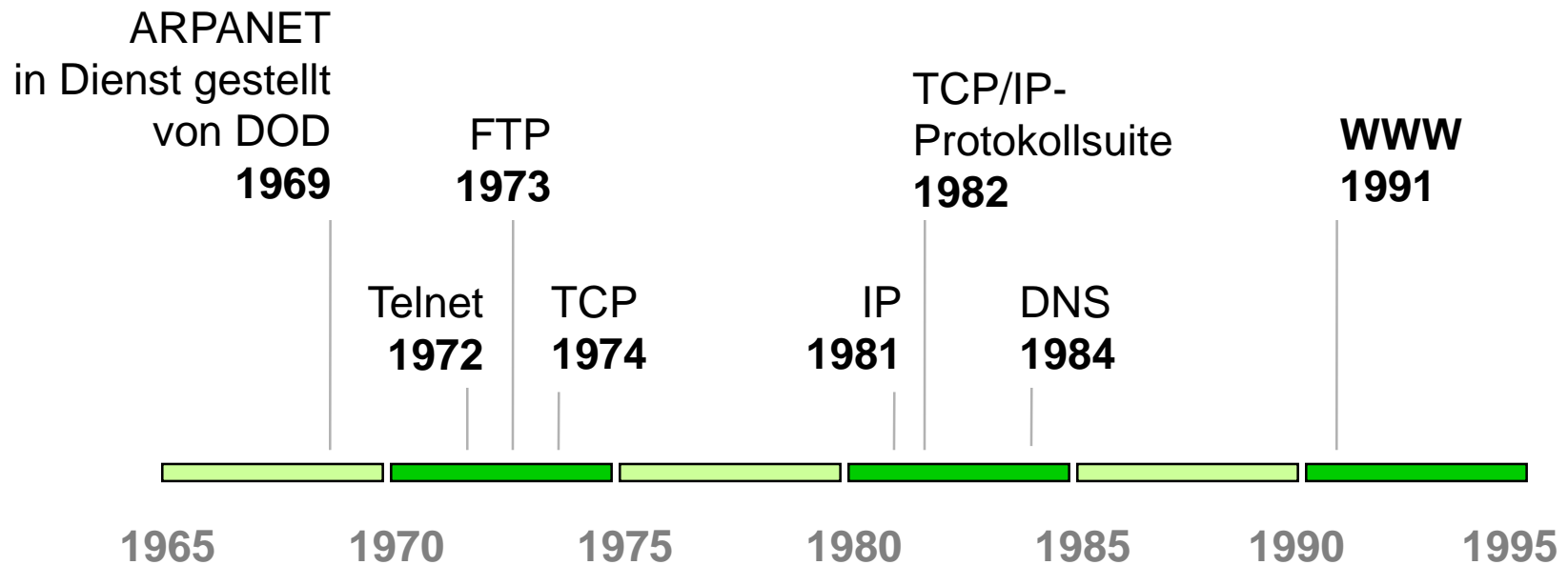
Diskussion

Es gab früher zig verschiedene Netzwerkprotokolle...
Wieso hat nur TCP/IP 'überlebt'?

TCP/IP ist das Standardprotokoll des Internets.
Deswegen wird es auch intern in LANs verwendet.



TCP/IP und das Internet



<https://www.internetsociety.org/internet/history-internet/brief-history-internet/>



Diskussion

Eine der Eigenschaften, die TCP/IP als Protokoll des Internets braucht, ist dessen Routingfähigkeit.

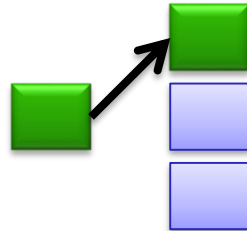
Was heißt eigentlich routingfähig?

Da müssen wir jetzt etwas ausholen ;-)

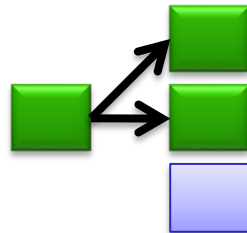


Kommunikation im Netzwerk

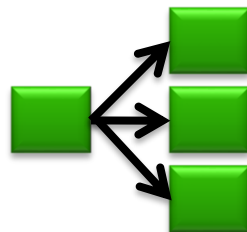
■ Unicast



■ Multicast



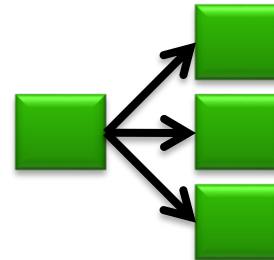
■ Broadcast





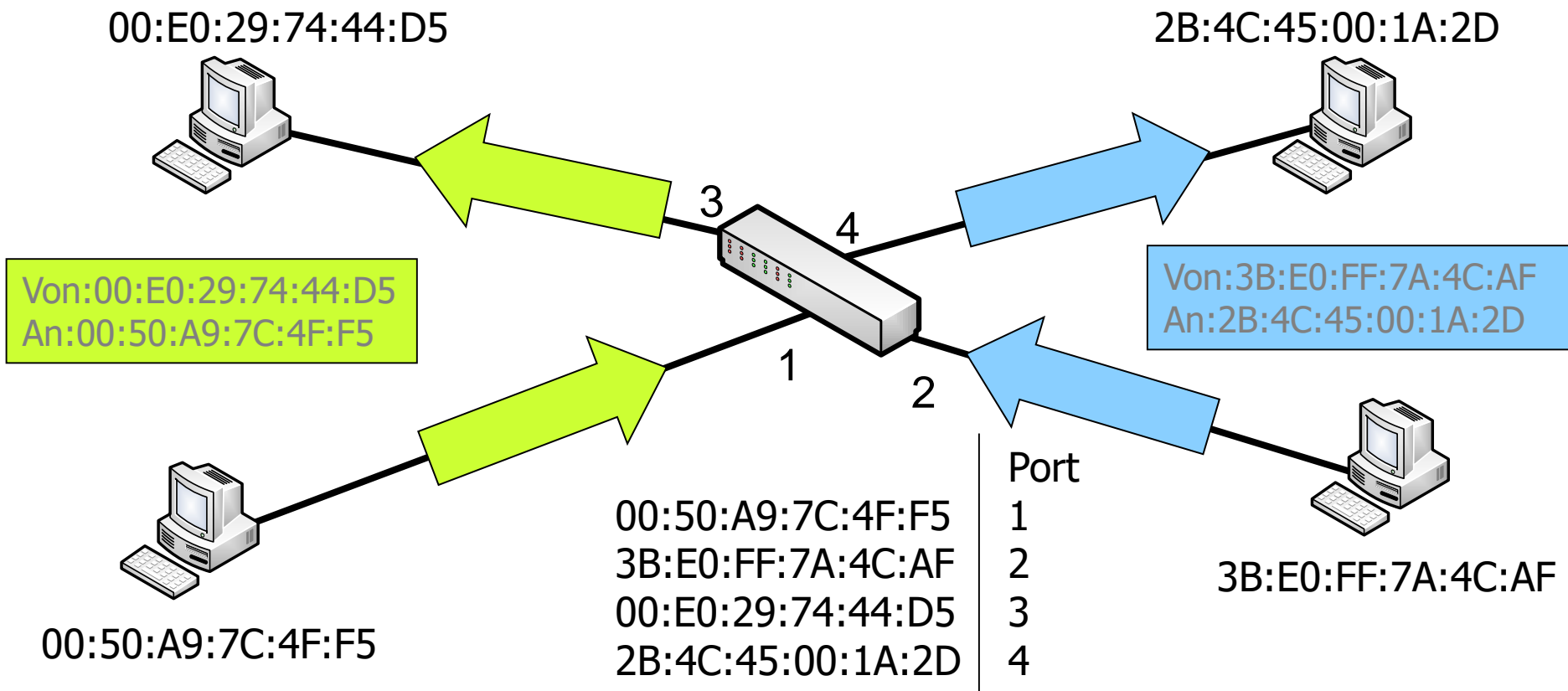
Was sind die Nachteile von Broadcasts?

- Broadcast



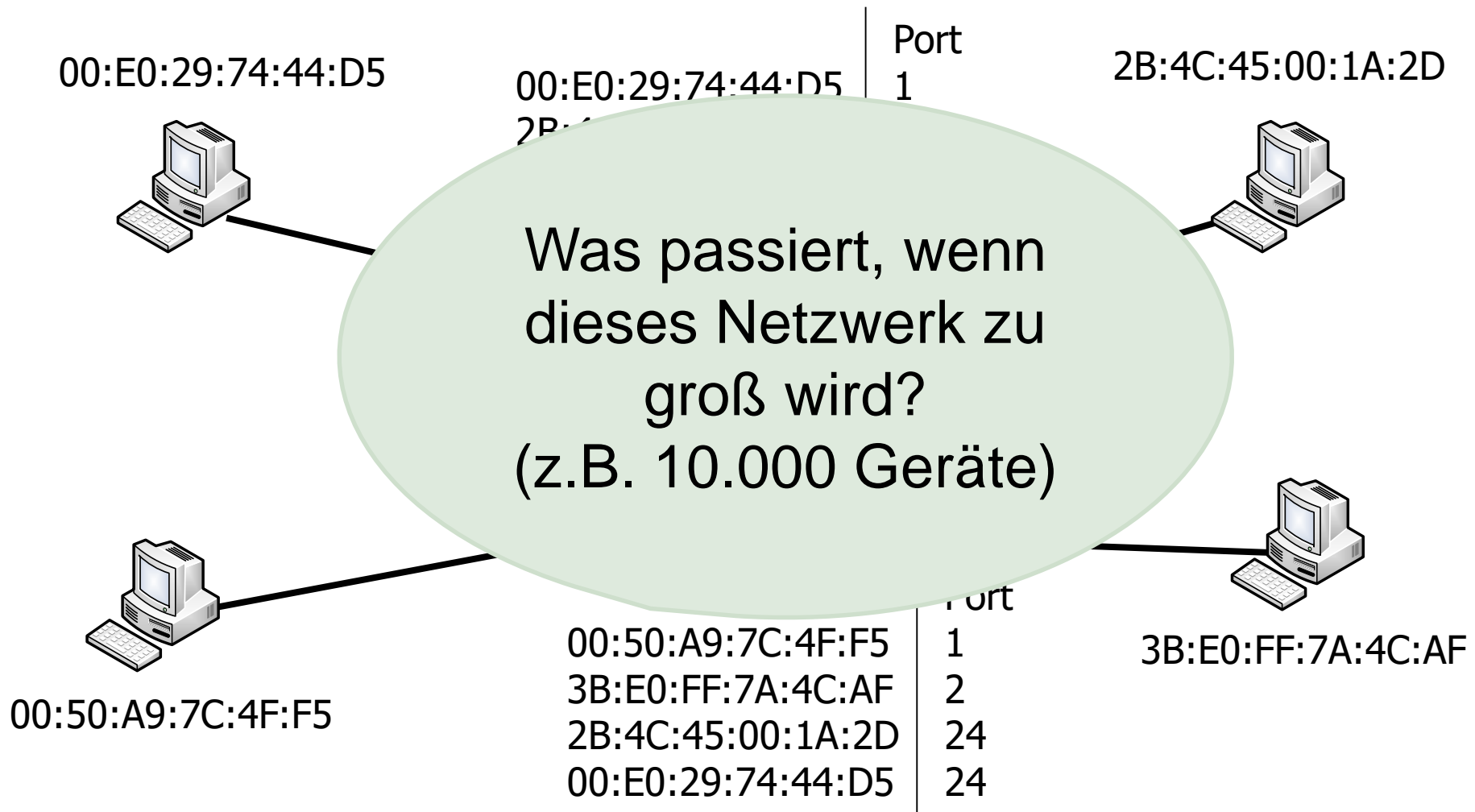


Was tut eigentlich ein Switch?



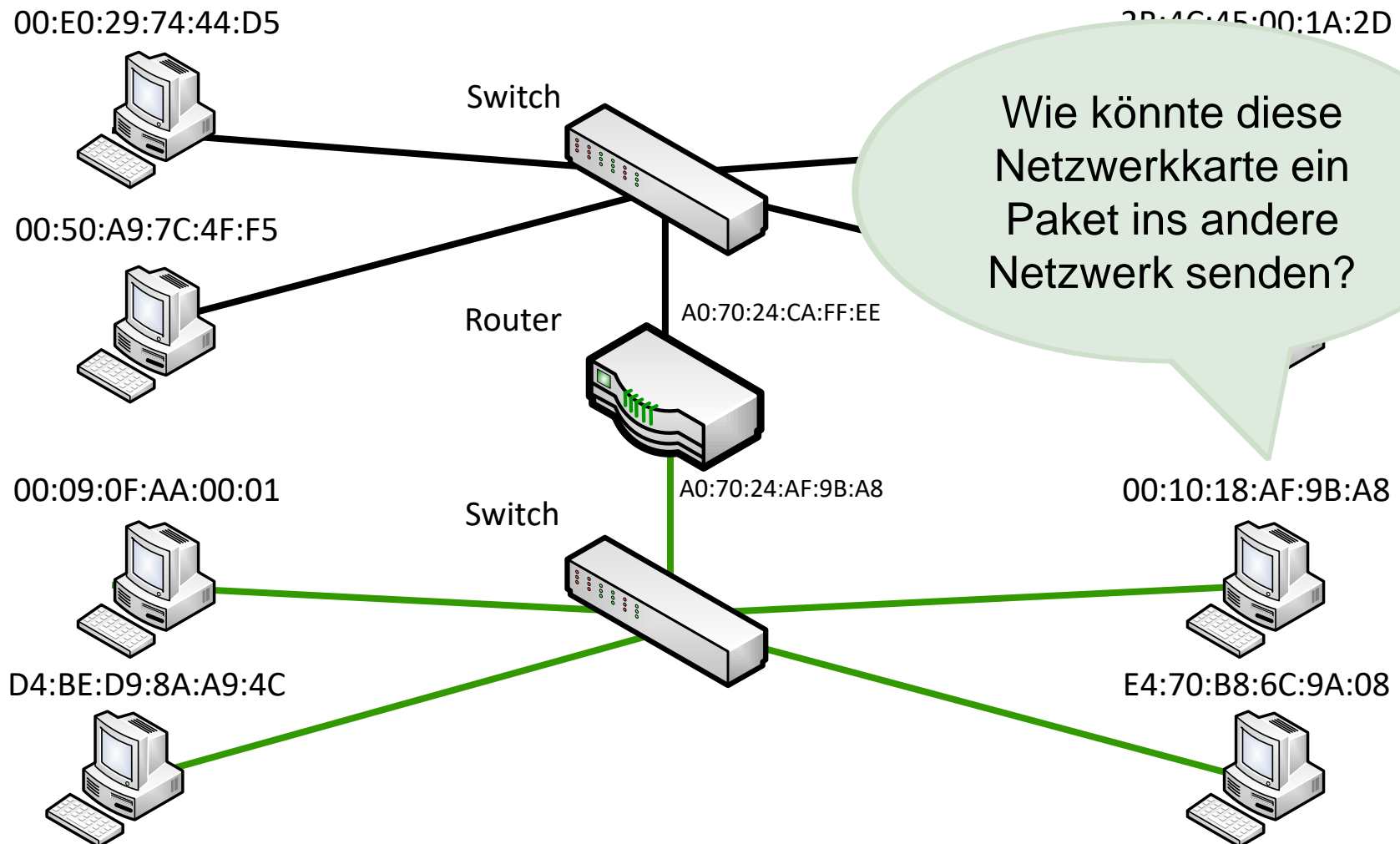


Und wenn man mehrere Switches hat?



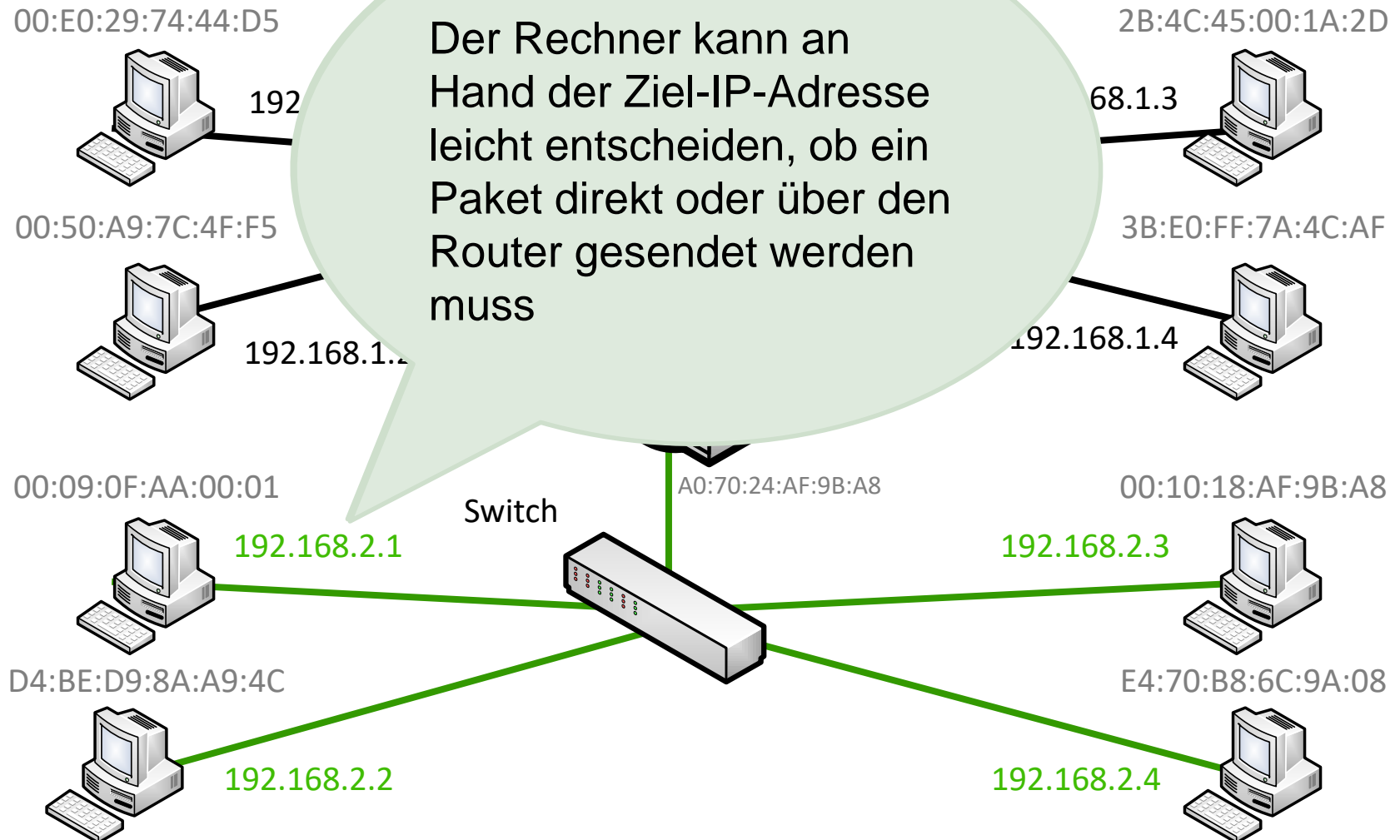


Auftrennen von Netzen





Auftritt IP-Adressen





Pakete tragen MAC und IP-Adressen

Quell-MAC: 00:E0:29:74:44:D5

Ziel-MAC: 3B:E0:FF:7A:4C:AF

Quell-IP: 192.168.1.1

Ziel-IP: 192.168.1.4

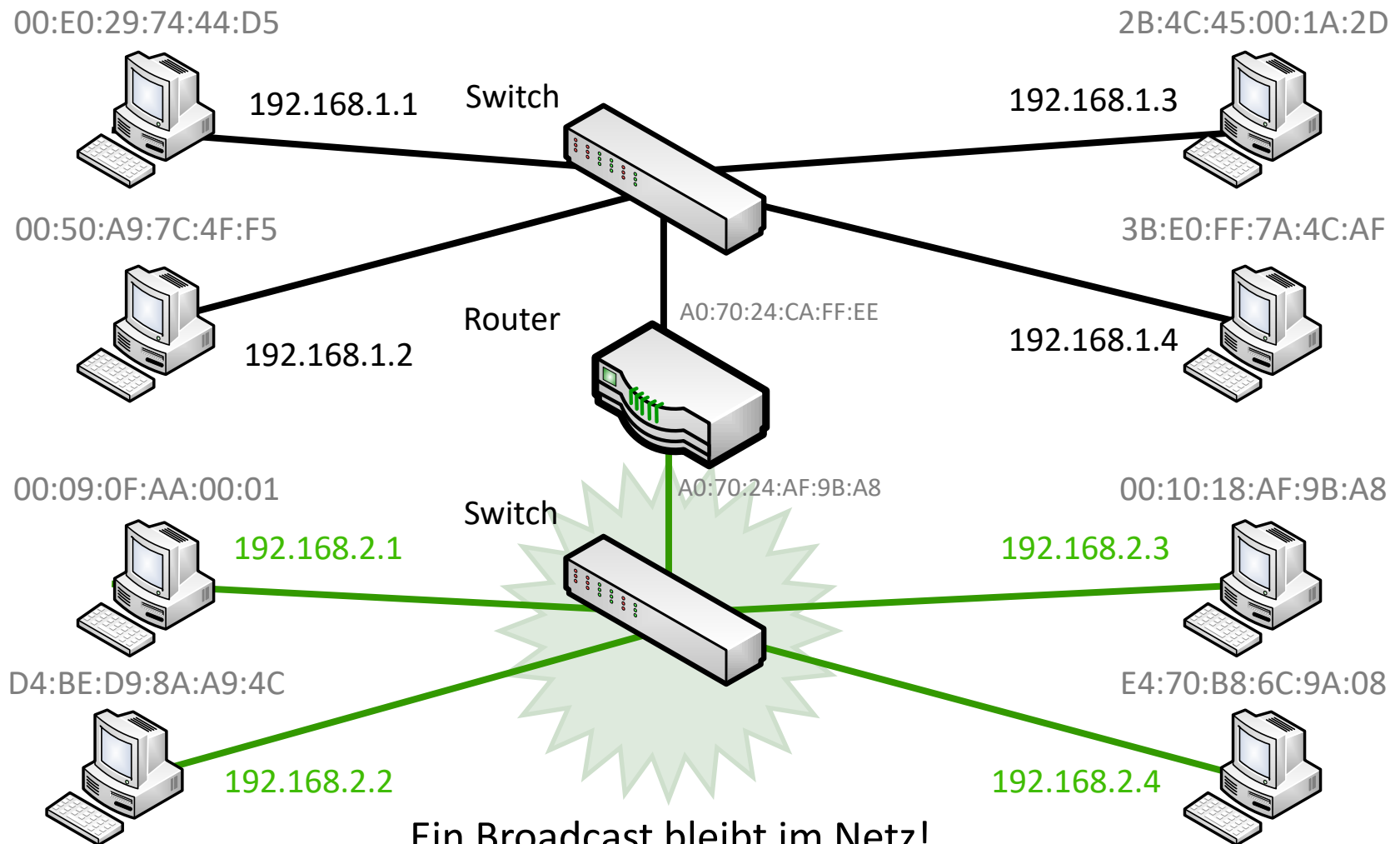
Eigentlicher Paketinhalt

Wichtig im LAN (Switches)

Wichtig, um von Routern
zwischen Netzen vermittelt
zu werden.



Und warum nochmals der ganze Spaß?





Diskussion

Wer kommuniziert eigentlich mit wem über ein Netzwerk?
Oder anders gefragt: Wer generiert die Daten, die übertragen werden?

Anwendungen kommunizieren über ein Netzwerk miteinander!
Diese generieren auch die Daten, die übertragen werden sollen.



Diskussion

Glauben Sie, dass jede Anwendung weiß, wie Daten in Pakete zerlegt werden müssen?

Nein, die Anwendung sieht nur eine Verbindung. Sie weiß im Allgemeinen nichts von Paketen!



Diskussion

Ist es einer Anwendung wichtig, ob die Daten, die sie übertragen möchte letztendlich über 3G oder Ethernet übertragen werden?

Nein, einmal geht es eben langsamer, einmal schneller!



Diskussion

Was versteckt eigentlich diese gesamte Komplexität vor der Anwendung?

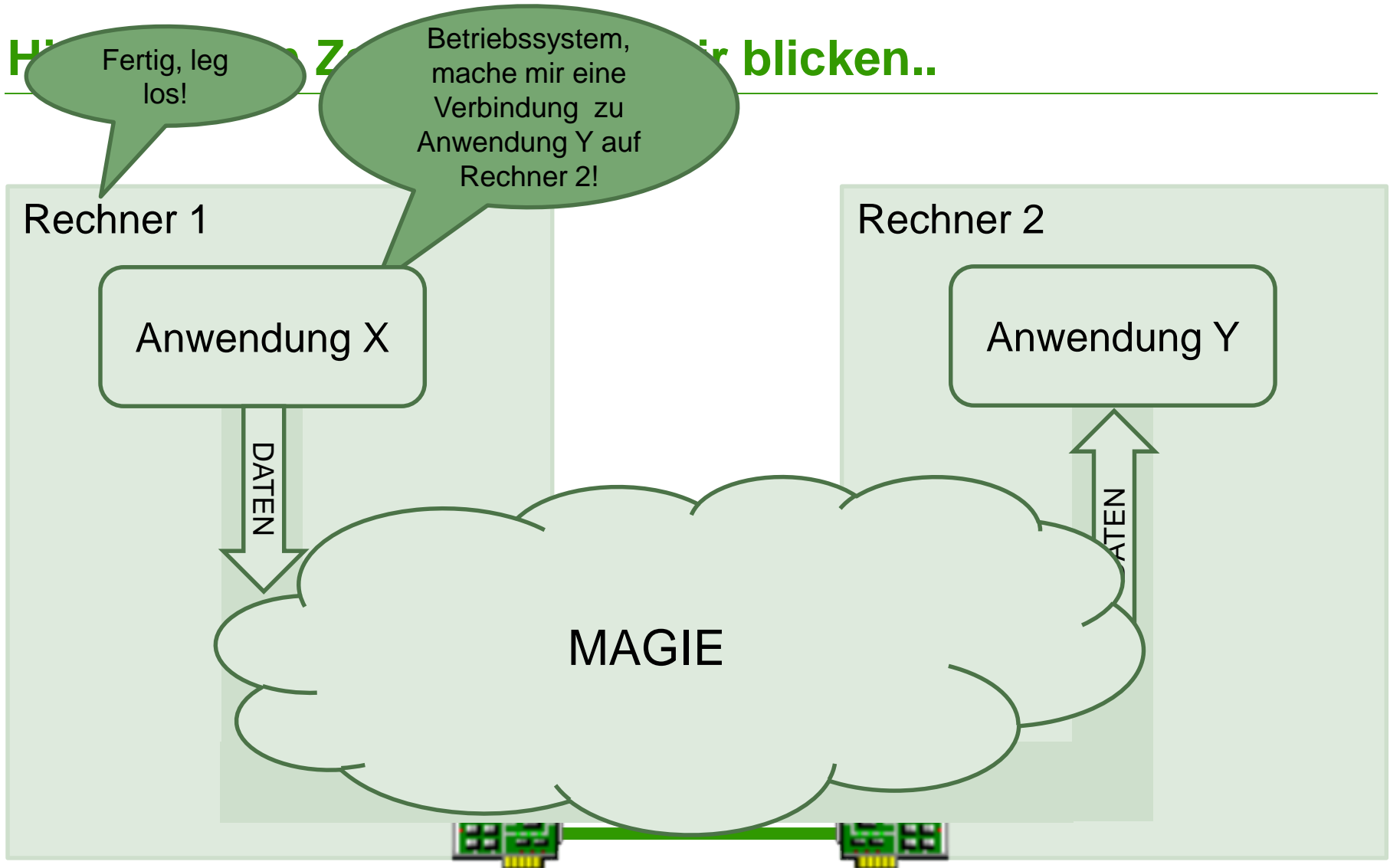
TCP/IP mit Hilfe einer Reihe von Protokollen, die sich um verschiedene Aufgaben kümmern!

Als Anwendung könnte man das auch so betrachten...



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen

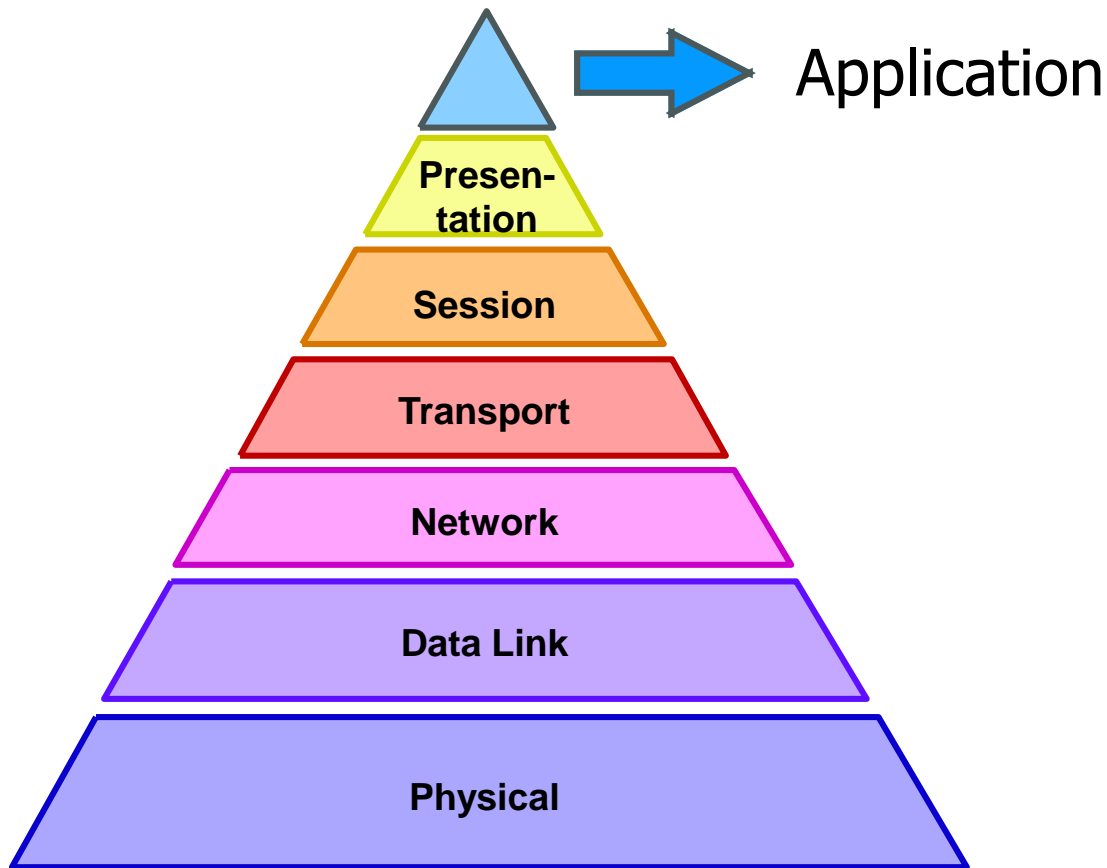




TCP/IP im Kontext des OSI sieben-Schichten-Modells



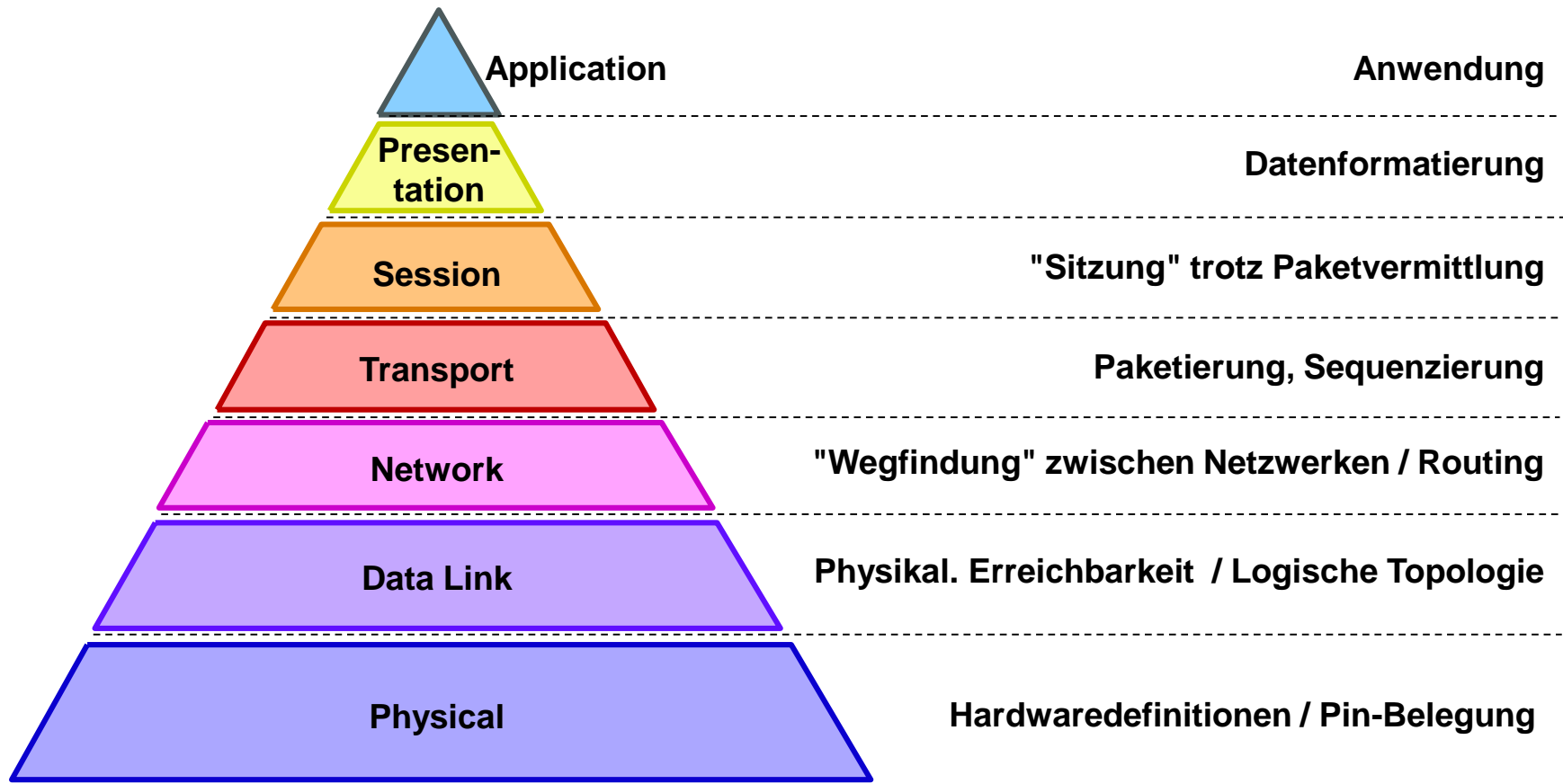
Das OSI 7-Schichten Modell



All
People
Seem
To
Need
Data
Processing



Aufgaben der Schichten





OSI vs. TCP/IP

Application	Application	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, SSH, TELNET, DNS,...
Presentation		
Session		
Transport	Transport	TCP UDP
Network	Internet	ICMP IP ARP
Data Link		
Physical	Network Interface	Ethernet, DSL, 3G/4G, ...

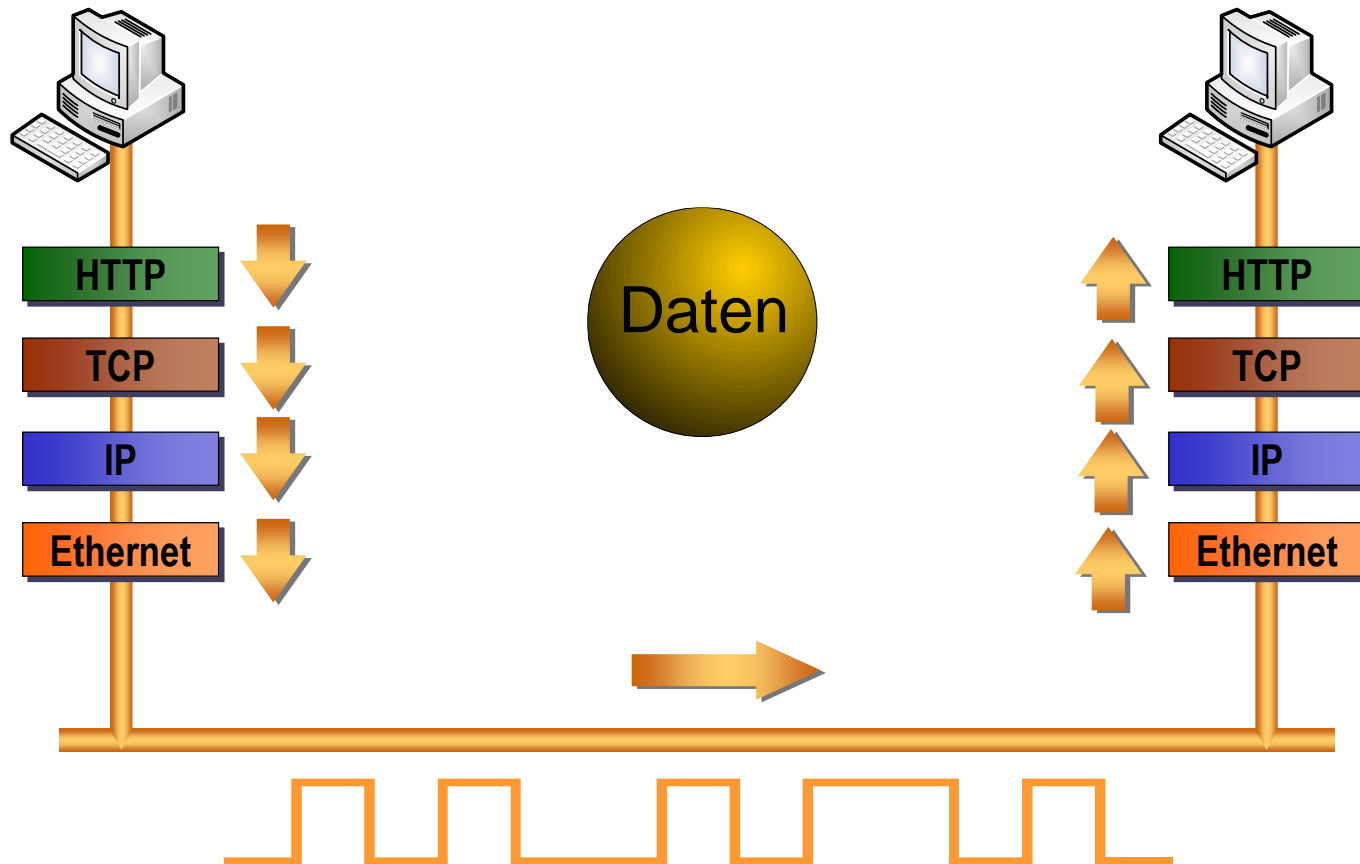


TCP/IP Einzelprotokolle

- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- IP: Internet Protocol
- ICMP: Internet Control Message Protocol
- ARP: Address Resolution Protocol



Daten





Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Layer 4 – Details und Troubleshooting

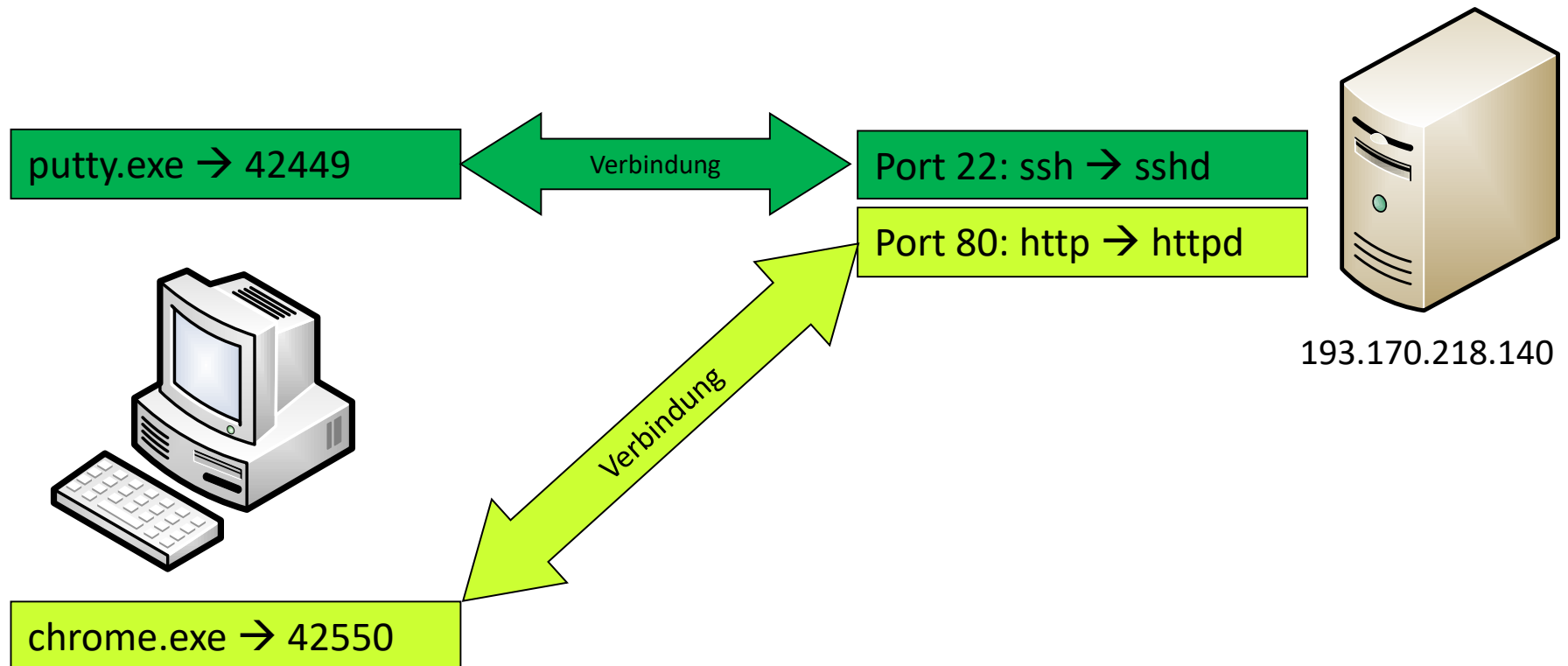


Ports

- Adresse einer Anwendung auf einem TCP/IP-Host ('Layer-4 Adresse')
- Bereich: 0-65535
- Well-Known-Ports: 0-1024
 - Windows:
 - %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC\SERVICES
 - UNIX/Linux:
 - /etc/services



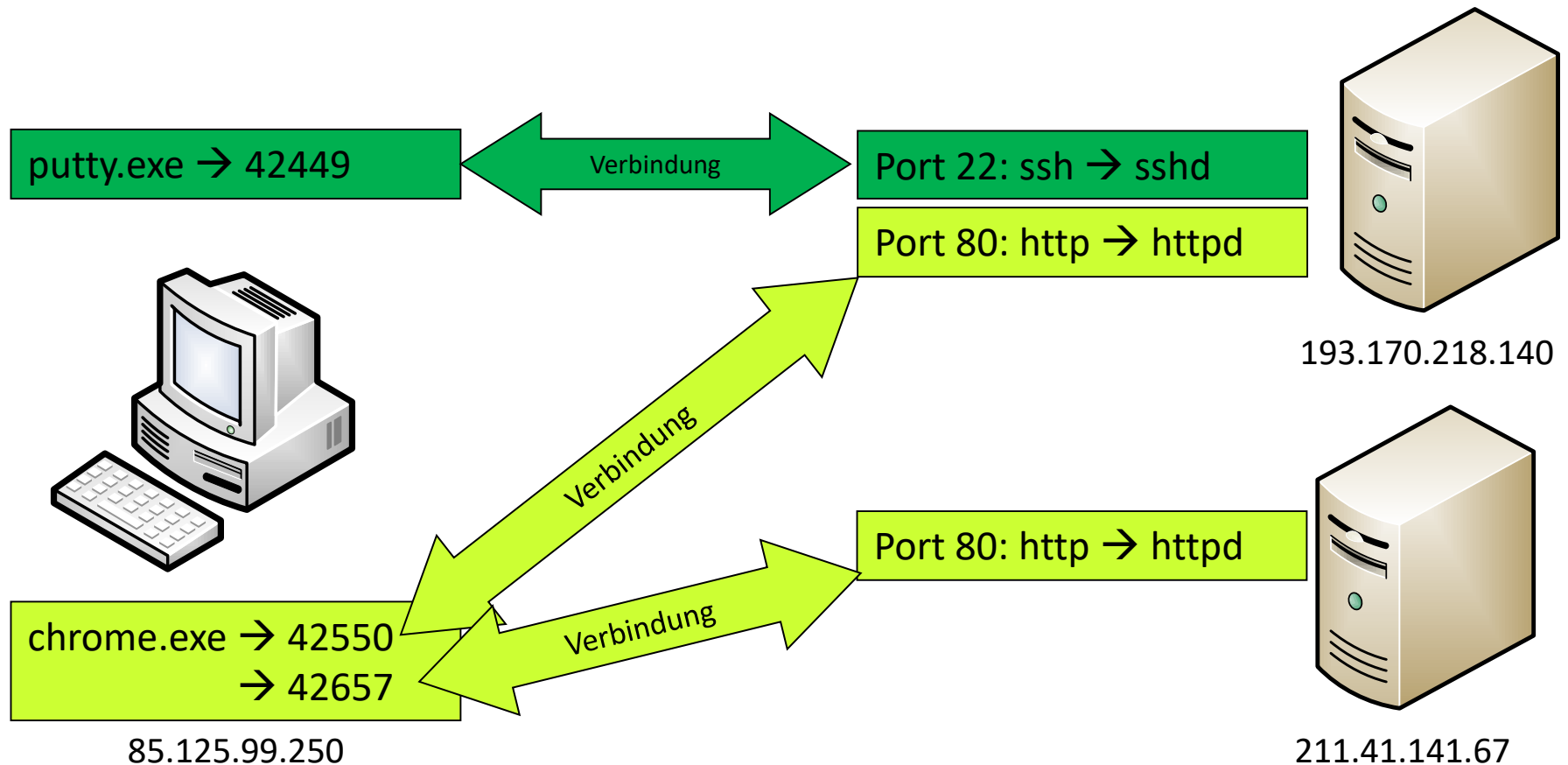
Ports und Anwendungen



Socket = IP-Adresse, Port, Layer-4 Protokoll
193.170.218.140:80,tcp



Ports und Anwendungen





Netzwerkadministrator

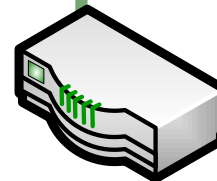
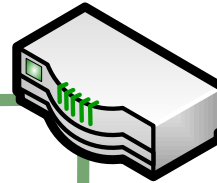
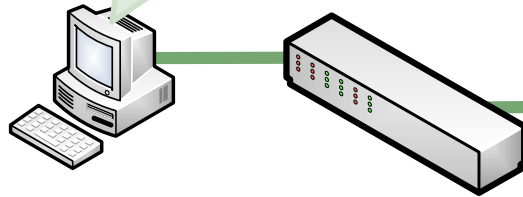
Modul 1 – Netzwerk Grundlagen



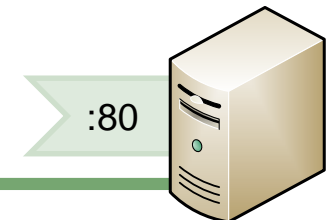
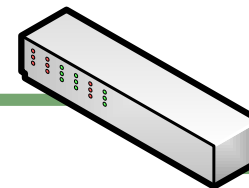
Übung – Füllen Sie die fehlenden Daten aus

http://191.217.6.200

IP: 83.64.18.254
MAC: 00:af:cb:92:2c:db



IP: 191.217.6.1
MAC: 00:22:65:17:dd:e3



IP: 191.217.6.200
MAC: f2:37:18:22:8c:d3

Ethernet:
Quell-MAC: _____
Ziel-MAC: _____

IP:
Quell-IP: _____
Ziel-IP: _____

TCP:
Quellport: _____
Zielport: _____

HTTP:
200 OK
Content-Type: HTML

IP: 83.64.18.11
MAC: 00:c3:b4:28:75:ff

Ethernet:
Quell-MAC: _____
Ziel-MAC: _____

IP:
Quell-IP: _____
Ziel-IP: _____

TCP:
Quellport: _____
Zielport: _____

HTTP:
GET / HTTP/1.0



Sockets-Übungen

- Öffnen Sie eine Website in einem Browser
- Überprüfen Sie die aufgebauten Verbindungen mit Hilfe von
`netstat -ano`
- Überprüfen Sie die Verbindung zu einem TCP-Service mit Hilfe von
`telnet ip-adresse port`
`telnet 87.230.34.122 143`



Auf welchem Server laufen welche Dienste?

Serverdienst	Server-Port	85.125.99.250	87.230.34.122
ssh			
http			
https			
imap			



Auf welchem Server laufen welche Dienste?

Serverdienst	Server-Port	85.125.99.250	87.230.34.122
ssh	22	ja	ja
http	80	ja	ja
https	443	nein	nein
imap	143	nein	ja



Netzwerkanalyse - Übung

- Verwenden Sie Wireshark (<http://www.wireshark.org>), um die Encapsulierung von Daten zu betrachten
- Öffnen Sie eine HTTP-basierte Website
- Setzen Sie die Pakete mit Hilfe von Wireshark wieder zusammen
- Versuchen Sie dasselbe mit einer HTTPS-basierenden Website
- Starten Sie einen Capture und öffnen Sie in einem Browser <http://85.125.99.250/geheim>
- Sie werden nach Credentials gefragt – Ihr Trainer gibt diese ein
- Stoppen Sie den Capture
- Können Sie mit Hilfe des Paket-Dumps das Passwort herausfinden?



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Layer 3 – Details und Troubleshooting



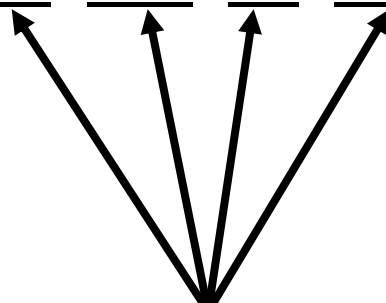
IP-Adressdaten

- IP-Adresse
 - Subnetzmaske
 - Gateway
-
- 192.168.1.1
 - 255.255.255.0
 - 192.168.1.254



Dotted Quad Notation

119 . 221 . 17 . 147



Namen: Oktett, Byte, Quad
Bereich: 0-255



Netz- und Hostanteil

172.231	.	1.2
255.255	.	0.0

Netzanteil oder Netz-ID: 172.231.0.0

Hostanteil oder Host-ID: 0.0.1.2

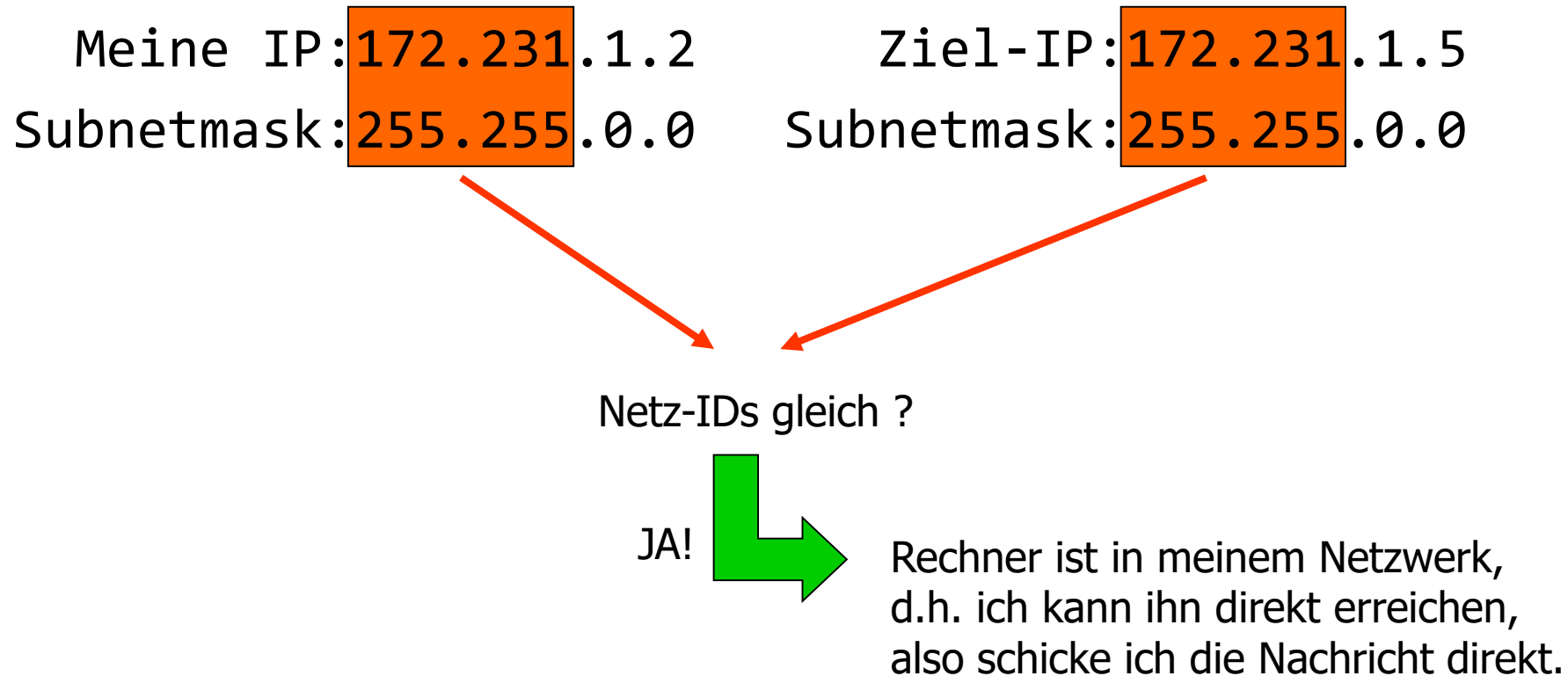
Netzanteil darf nicht ,durchgehend` 0 oder 255 sein

Hostanteil darf nicht ,durchgehend` 0 (Gesamtes Netz)

Hostanteil darf nicht ,durchgehend` 255 (Layer 3 Broadcast)

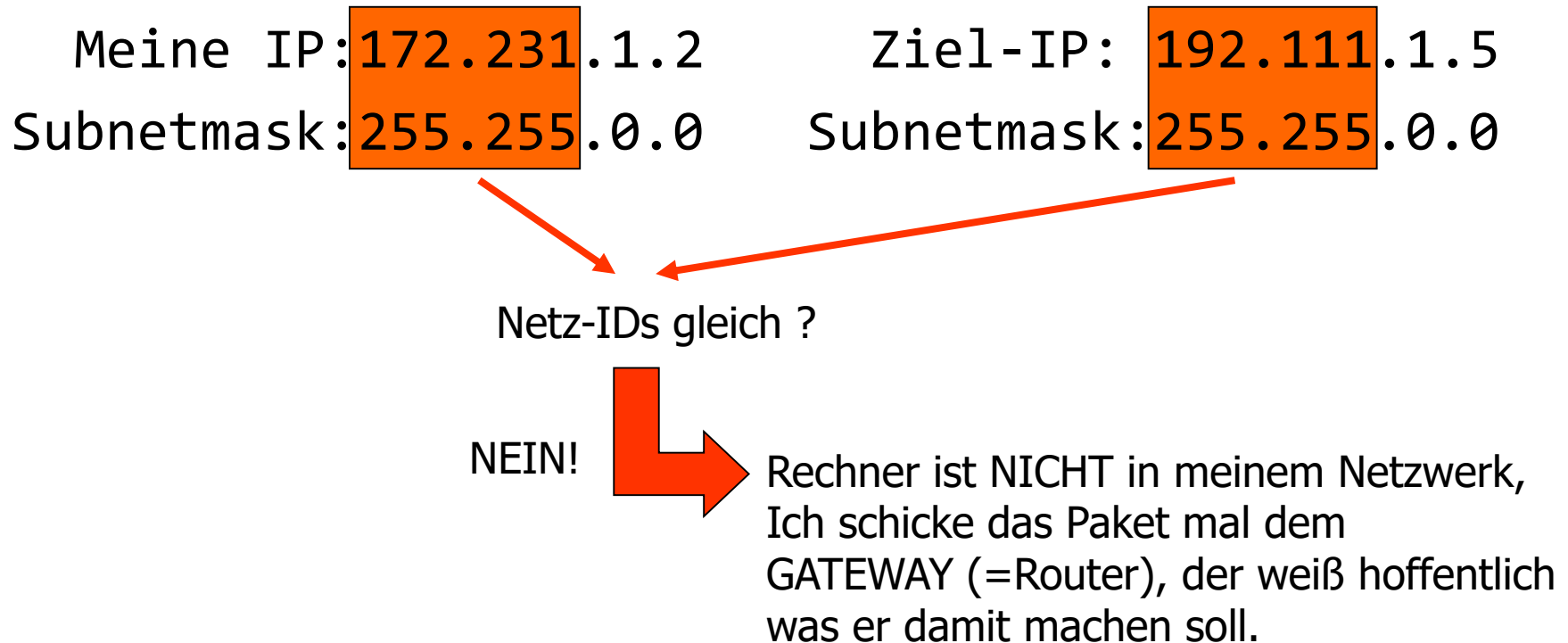


Die Entscheidung des Hosts





Die Entscheidung des Hosts





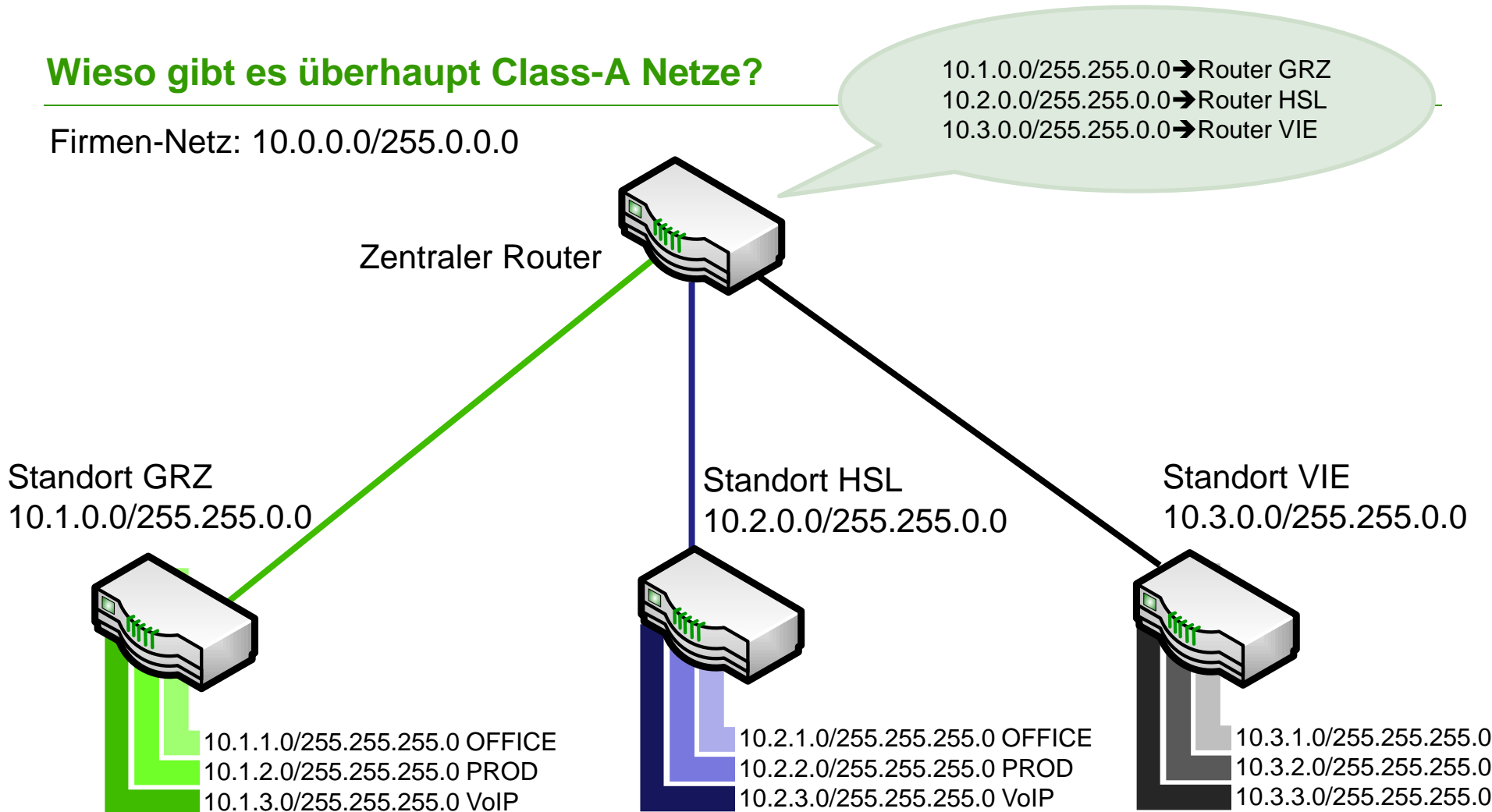
IP-Adressklassen

Klasse	Netzmaske	Hosts pro Netz
A	255.0.0.0 (/8)	~16,7 Mio
B	255.255.0.0 (/16)	65.534
C	255.255.255.0 (/24)	254



Wieso gibt es überhaupt Class-A Netze?

Firmen-Netz: 10.0.0.0/255.0.0.0





Gefühl Für IP-Adressen – Teil 1

- Netzadresse: **172.48.0.0**
- Subnetzmaske: **255.255.0.0**
- Erste verwendbare IP-Adresse: 172.48.0.1
- Letzte verwendbare IP-Adresse: 172.48.255.254
- Broadcast-Adresse: 172.48.255.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: **102.0.0.0**
- Subnetzmaske: **255.0.0.0**
- Erste verwendbare IP-Adresse: 102.0.0.1
- Letzte verwendbare IP-Adresse: 102.255.255.254
- Broadcast-Adresse: 102.255.255.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 131.0.0.0
- Subnetzmaske: **255.255.0.0**
- Erste verwendbare IP-Adresse: 131.0.0.1
- IP-Adresse eines Rechners: **131.0.212.148**
- Letzte verwendbare IP-Adresse: 131.0.255.254
- Broadcast-Adresse: 131.0.255.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 193.0.0.0
- Subnetzmaske: **255.255.255.0**
- Erste verwendbare IP-Adresse: 193.0.0.1
- IP-Adresse eines Rechners: **193.0.0.47**
- Letzte verwendbare IP-Adresse: 193.0.0.254
- Broadcast-Adresse: 193.0.0.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 161.255.255.0
- Subnetzmaske: **255.255.255.0**
- Erste verwendbare IP-Adresse: 161.255.255.1
- IP-Adresse eines Rechners:
- Letzte verwendbare IP-Adresse: 161.255.255.254
- Broadcast-Adresse: **161.255.255.255**



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 193.218.150.0
- Subnetzmaske: **255.255.255.0**
- Erste verwendbare IP-Adresse: **193.218.150.1**
- IP-Adresse eines Rechners:
- Letzte verwendbare IP-Adresse: 193.218.150.254
- Broadcast-Adresse: 193.218.150.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 147.0.0.0
- Subnetzmaske: **255.255.0.0**
- Erste verwendbare IP-Adresse: 147.0.0.1
- IP-Adresse eines Rechners: **147.0.0.3**
- Letzte verwendbare IP-Adresse: 147.0.255.254
- Broadcast-Adresse: 147.0.255.255



Gefühl Für IP-Adressen – Teil 1

- Netzadresse: 147.0.0.0
- Subnetzmaske: **255.255.0.0**
- Erste verwendbare IP-Adresse: 147.0.0.1
- IP-Adresse eines Rechners: **147.0.0.3**
- Letzte verwendbare IP-Adresse: 147.0.255.254
- Broadcast-Adresse: 147.0.255.255

Sobald Sie eine IP-Adresse und die Netzmaske wissen, können Sie die Größe des Netzes bestimmen!



Weitere IP-Adressbereiche

- 127.0.0.0/255.0.0.0 – Netz:
 - Loopback
- Erstes Oktett: 224 – 239
 - MultiCast
- Erstes Oktett: 240 – 255
 - Experimental



Gefühl für IP-Adressen – Teil 2

- Welche IP-Adressen könnten unter der Annahme der von der Klasse vorgegebenen Standard-Subnetzmaske auf einem Rechner konfiguriert werden?
 - 131.107.256.80/255.255.0.0
 - 22.22.255.222/255.0.0.0
 - 231.200.1.1/255.255.255.0
 - 126.1.0.0/255.0.0.0
 - 0.127.4.100/255.0.0.0
 - 190.7.2.0/255.255.0.0
 - 127.1.1.1/255.0.0.0
 - 198.121.254.255/255.255.255.0

- Begründen Sie Ihre Entscheidungen!



Private Adressbereiche

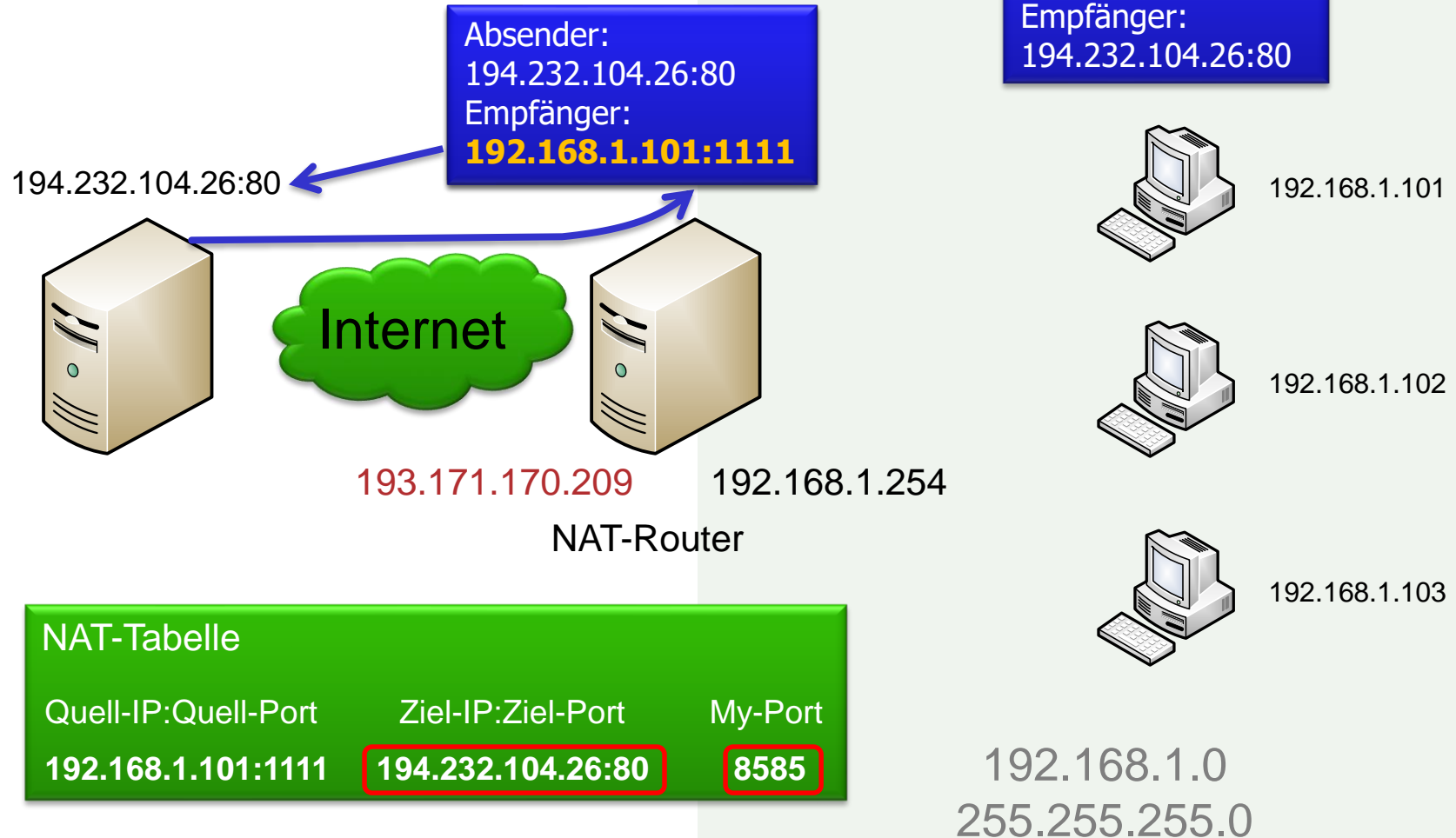
- Class A:
 - 10.0.0.0 / 255.0.0.0, 1 Netz

- Class B:
 - 172.16.0.0 / 255.255.0.0 bis
172.31.0.0 / 255.255.0.0, 16 Netze

- Class C:
 - 192.168.0.0 / 255.255.255.0 bis
192.168.255.0 / 255.255.255.0, 256 Netze



Was macht eigentlich ein NAT-Router?





Diskussion

Wenn ein NAT-Router ohnehin die internen IP-Adressen quasi hinter der NAT-Breakout-Adresse versteckt, wieso muss ich dann intern private IP-Adressen verwenden?

Schauen wir mal folgendes Beispiel an....

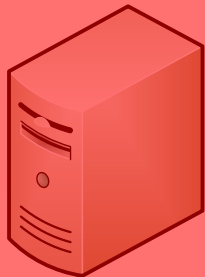


Muss man intern private IPs verwenden?

Absender:
29.3.77.101:1111
Empfänger:
29.3.77.191:80

Der ist ja im
selben Netz wie
ich!

29.3.77.191:80



Internet

193.171.170.209

29.3.77.254

KEINE GUTE IDEE

29.3.77.101



29.3.77.102



29.3.77.103



29.3.77.0
255.255.255.0



NAT-Übung

- Finden Sie die IP mit der Sie im Internet auftreten mit Hilfe der Website <https://www.whatismyip.net/> heraus



APIPA

- Automatic Private IP Addressing
 - Zur automatischen "Adressbeschaffung" ohne DHCP-Server
 - Adressbereich: 169.254.0.0 / 255.255.0.0



IP-Adressierung - Übung

- Konfigurieren Sie die IP-Adresse Ihres Rechners gemäß der Vorgabe Ihres Trainers



Überprüfung der IP-Konfiguration

- ping
 - ping <IP-Adresse>
 - ping -t <IP-Adresse> ('Dauerping')
 - Beispiel: ping 8.8.8.8
- ipconfig
 - ipconfig /all

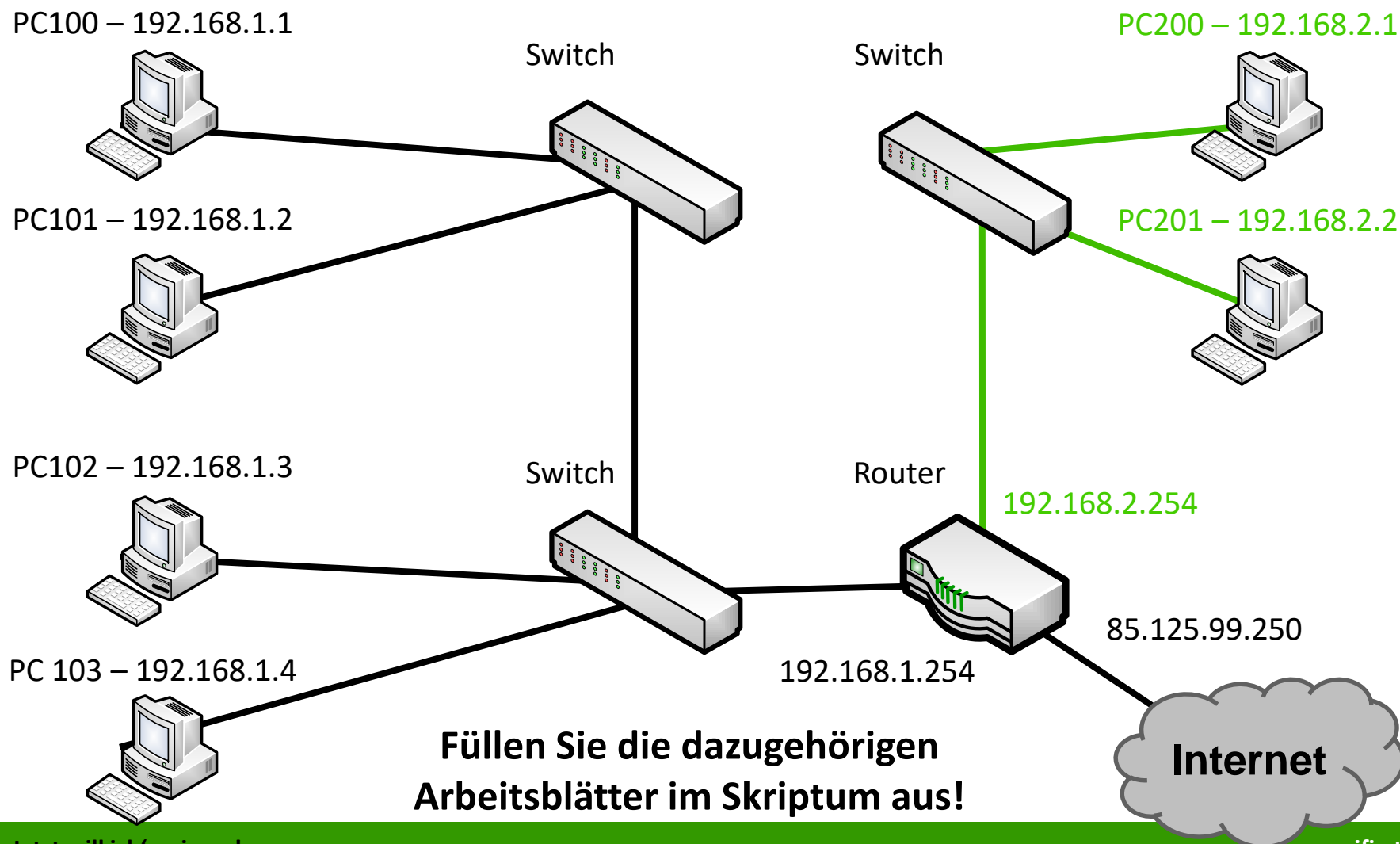


IP-Adressierung - Übung

- Konfigurieren Sie die IP-Adresse Ihres Rechners gemäß der Vorgabe Ihres Trainers
- Testen Sie die Erreichbarkeit anderer Rechner und von Rechnern im Internet mit Hilfe von ping



Richtiges Pingen – Ein Gedankenexperiment



Füllen Sie die dazugehörigen
Arbeitsblätter im Skriptum aus!



Eine Horrorgeschichte

- Kundenanruf
 - Ich habe einen Server neu aufgesetzt und eine statische IP-Adresse konfiguriert. Diese ist 192.168.1.5
 - Ich komme von dem Server aus ins Internet
 - Ich kann von diesem Server aus nur einen bestimmten Server im Internet nicht erreichen. Genau den muss ich aber erreichen können!
 - Probiere ich den Server im Internet von einem beliebigen anderen Rechner in meinem Netzwerk zu erreichen, so gelingt mir das.
- Aktion des Supports
 - Ping des Servers im Internet vom lokalen Arbeitsplatz : Antwort 192.221.37.20
- Antwort des Support
 - "Ich glaube, ich weiß, was Ihr Problem ist"

Was glaubt der Support ist das Problem?



Diskussion

Kann eine Netzwerkkarte ein Paket an eine IP-Adresse senden?

Nein, nur an eine MAC-Adresse!

Also wie findet das System die zu einer IP passende MAC-Adresse?



Layer 2 –Details und Troubleshooting



ARP

- Auflösung IP → MAC
- Auflösung über Layer 2 Broadcast
- Zwischenspeicherung in einem Cache
- Statische Zuordnungen möglich
(z.B.: Erstkonfiguration eines Printservers)
- RFC 826



ARP-Auflösung I

Gerät 192.168.1.1 möchte Gerät 192.168.1.2 erreichen:

Was passiert auf Rechner 192.168.1.1?

- Habe ich die MAC-Adresse von 192.168.1.2 im Cache?
- NEIN → ARP-REQUEST (Broadcast)

Sender IP	192.168.1.1
Sender MAC	00:E0:27:74:44:D5
Empf. IP	192.168.1.2
Empf. MAC	Bitte ausfüllen!



ARP-Auflösung II

Was passiert auf Rechner 192.168.1.2?

- fängt Anfrage auf
- trägt Daten von A in ARP-Cache ein
- Gerichtete Antwort: ARP-REPLY

Sender IP	192.168.1.2
Sender MAC	00:04:76:A2:7B:EA
Empf. IP	192.168.1.1
Empf. MAC	00:E0:27:74:44:D5



ARP

- Cache auslesen

```
C:\>arp -a
```

- Cache löschen

```
C:\>arp -d
```



ARP-Übungen

- Löschen Sie den ARP-Cache Ihres Rechners!
- Vergewissern Sie sich, dass der ARP-Cache des Nachbarrechners ebenfalls gelöscht wurde!
- Pingen Sie die IP-Adresse Ihres Nachbarrechners!
- Welche Einträge befinden sich in Ihrem ARP-Cache?
- Welche Einträge befinden sich im ARP-Cache Ihres Nachbarn?
- Hat sich der ARP-Cache Ihrer Kollegen verändert?



ARP-Übungen

- Pingen Sie zwei IP-Adressen im Internet!
8.8.8.8, 85.125.99.250
 - Wie viele Einträge wurden in Ihrem ARP-Cache hinzugefügt?
 - Was bedeuten diese?

- Pingen Sie einen Namen im Internet!
z.B. www.iic.wifi.at
 - Hat sich Ihr ARP-Cache verändert?
 - Warum (nicht)?



Diskussion

Nehmen wir an, Sie pingen einen PC, um dessen Erreichbarkeit zu prüfen. Gib es einen Weg festzustellen, ob der PC wirklich nicht erreichbar ist, oder nur dessen Firewall die ICMP-Echo Request Pakete verwirft?

Auf ARP-Requests muss ein PC immer antworten.
Sehen Sie also eine Zuordnung MAC → IP läuft der Rechner, lässt sich aber nicht pingen!

Unter welchen Bedingungen können Sie diesen Trick nur anwenden?



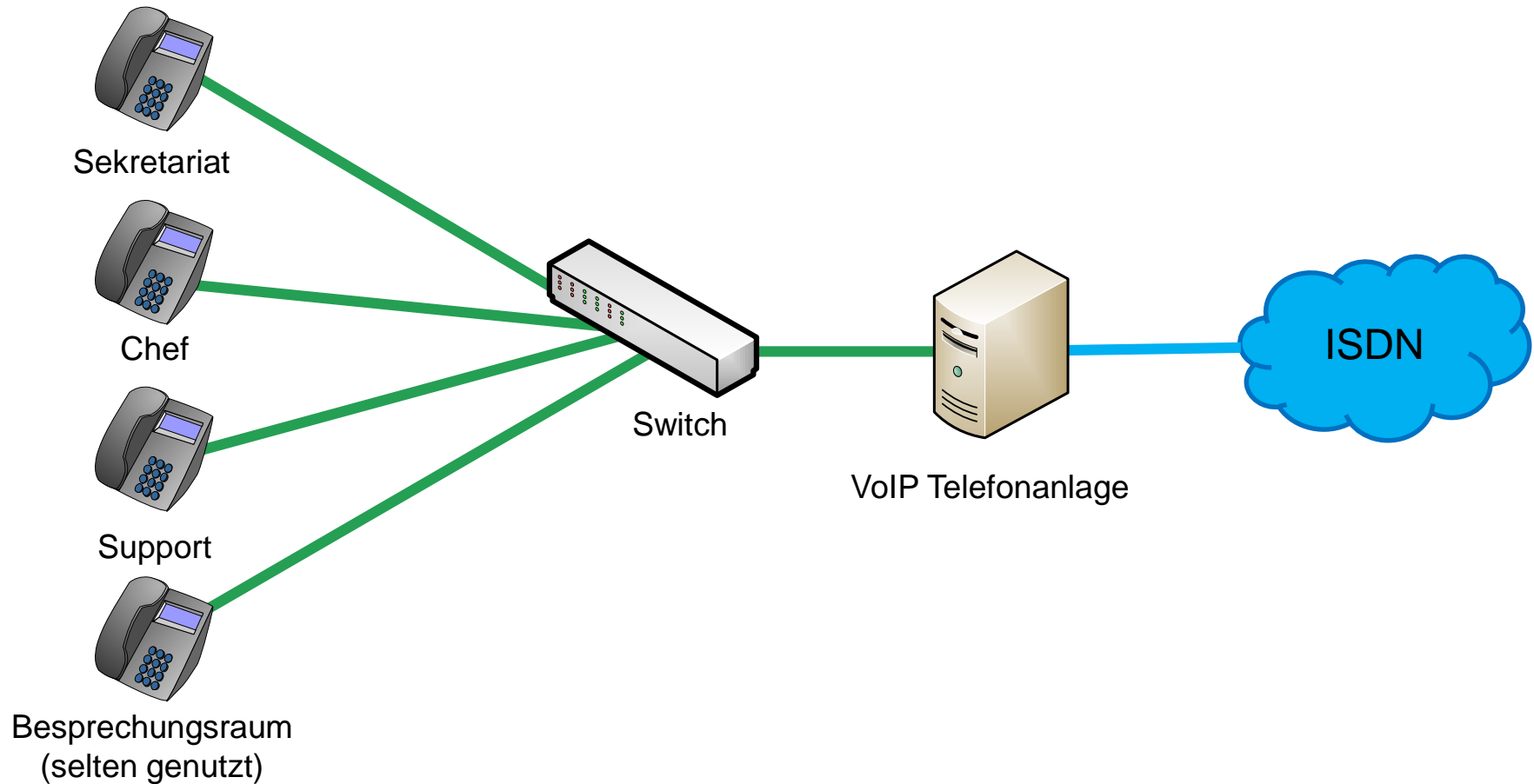
ARP-Übungen

- Versuchen Sie das Verfahren aus der letzten Folie unter Anleitung Ihres Trainers nachzustellen!



Eine VoIP-Horrorgeschichte

■ Ausgangssituation





Eine VoIP-Horrorgeschichte

- Sekretariat meldet:
 - Wenn ich telefoniere höre ich nach spätestens 10 Minuten meinen Gesprächspartner nicht mehr
 - Er hört mich sehr wohl noch
 - Versuche ich es einige Minuten später nochmals, funktioniert alles
 - Aber nach spätestens 10 Minuten Gespräch, tritt das Problem wieder auf!

Woran könnte das Problem liegen?

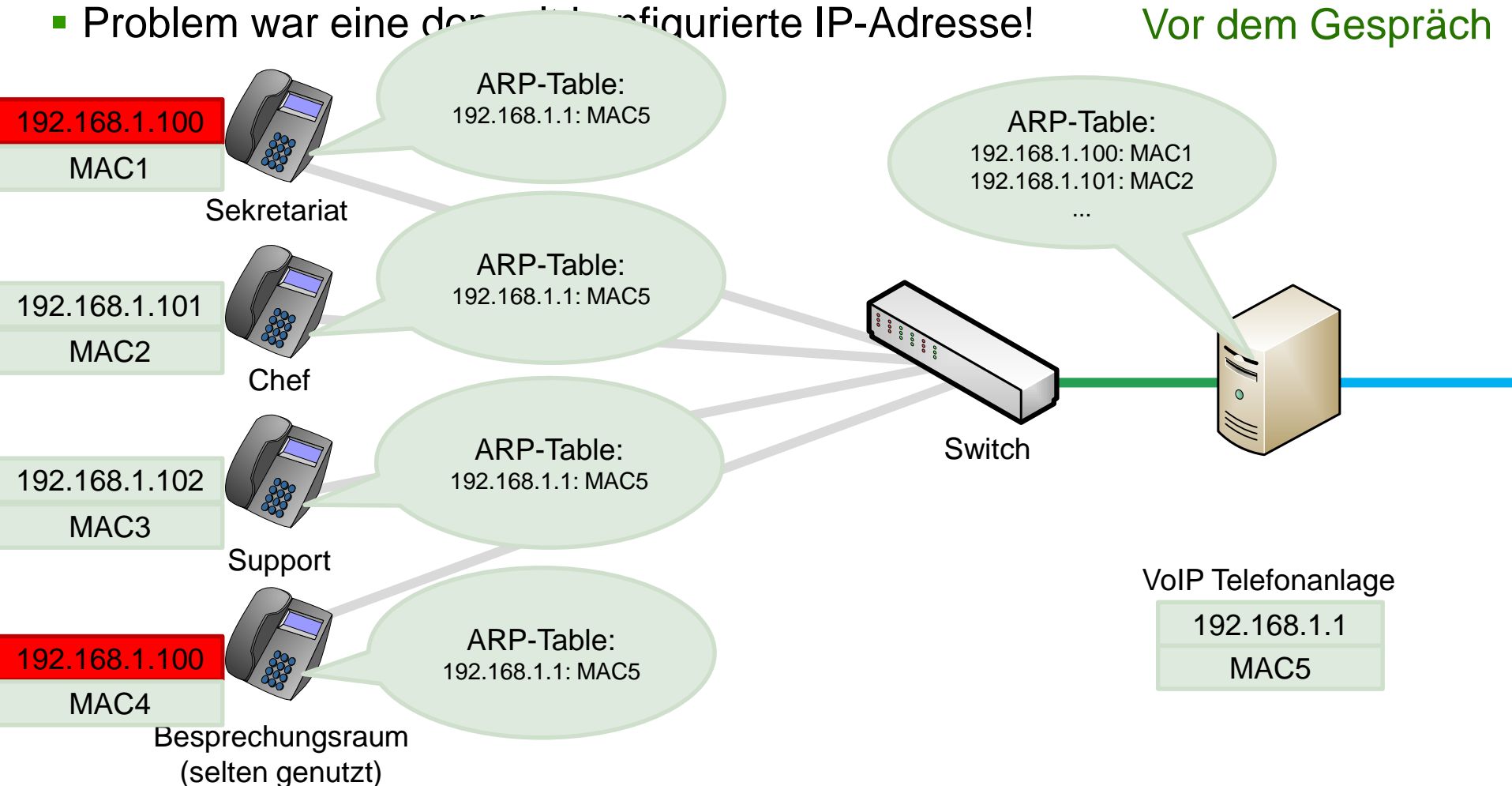
Denken Sie daran, dass der eigentliche Voice-Stream eines VoIP-Anrufs rein über UDP, also ohne Empfangsbestätigungen läuft!



Eine VoIP-Horrorgeschichte

- Problem war eine doppelt konfigurierte IP-Adresse!

Vor dem Gespräch

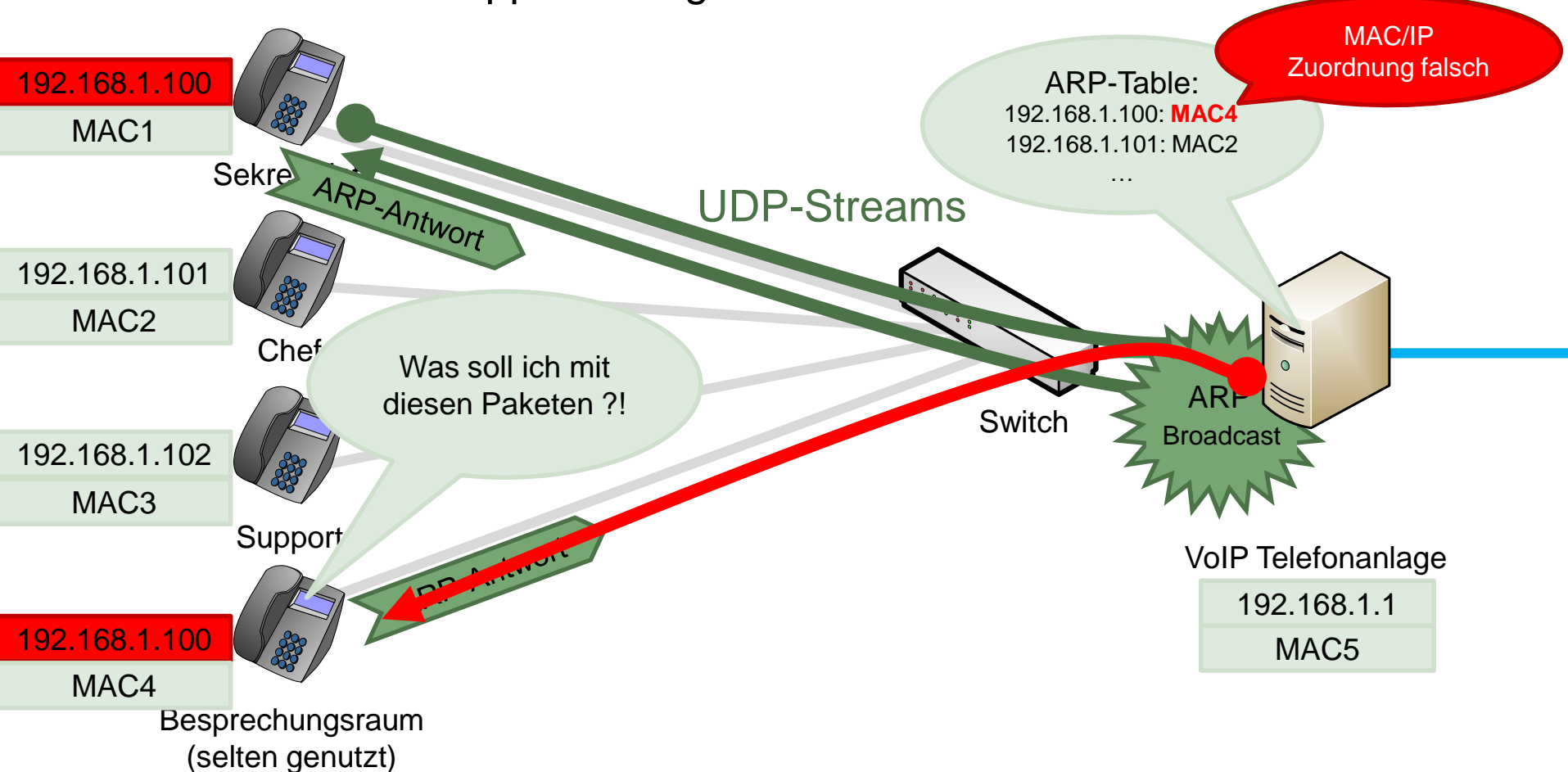




Eine VoIP-Horrorgeschichte

- Problem war eine doppelt konfigurierte IP-Adresse!

Problem beginnt





Eine VoIP-Hororgeschichte

- Ergebnis eines kleinen Konfigurationsfehlers
 - 1,5 Manntage Problemsuche!
- Wieso war das Problem überhaupt nachvollziehbar?
 - Das Besprechungsraumtelefon wurde kaum genutzt.
Deswegen war die Wahrscheinlichkeit hoch, dass der ARP-Table der Anlage die Zuordnung fürs Sekretariat beinhaltet!
 - Die ARP-Antwort des ungenutzten Telefons kommt mit sehr hoher Wahrscheinlichkeit früher an als die des Telefons, von dem gerade telefoniert wurde, da dieses die ARP-Antwort zwischen die zu sendenden VoIP-Pakete zwängen musste!



Wenn wir schon über MAC-Adressen reden...

- Schreibweise

D4-BE-D9-8A-A9-4C
Windows

d4:be:d9:8a:a9:4c
Linux/macOS

d4bed9-8aa94c
HP-Switch

d4bed9.8aa94c
Cisco Switch

- Die ersten 6 Stellen kennzeichnen den Hersteller

d4:be:d9:8a:a9:4c
 Dell

OUI Lookup-Tool:

<https://www.wireshark.org/tools/oui-lookup.html>

- Broadcast-Adresse: FF:FF:FF:FF:FF:FF



Der Bridging-Table auf eines Switches

```
ProCurve Switch 5406zl                               13-Feb-2013  16:44:16
===== TELNET - MANAGER MODE =====
Status and Counters - Address Table - UNTERRICHT

  MAC Address      Located on Port
  -----
000085-dc94d8      C13
000f61-092a20      C19
000ffe-96a741      C21
001018-f7446c      Trk1
001018-f7446d      Trk1
001517-4565d4      B19
001517-cf9508      D9
00155d-7eca01      Trk1
00155d-7eca03      Trk1
Actions->  Back    Search    Next page    Prev page    Help
```



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Troubleshooting am Switch

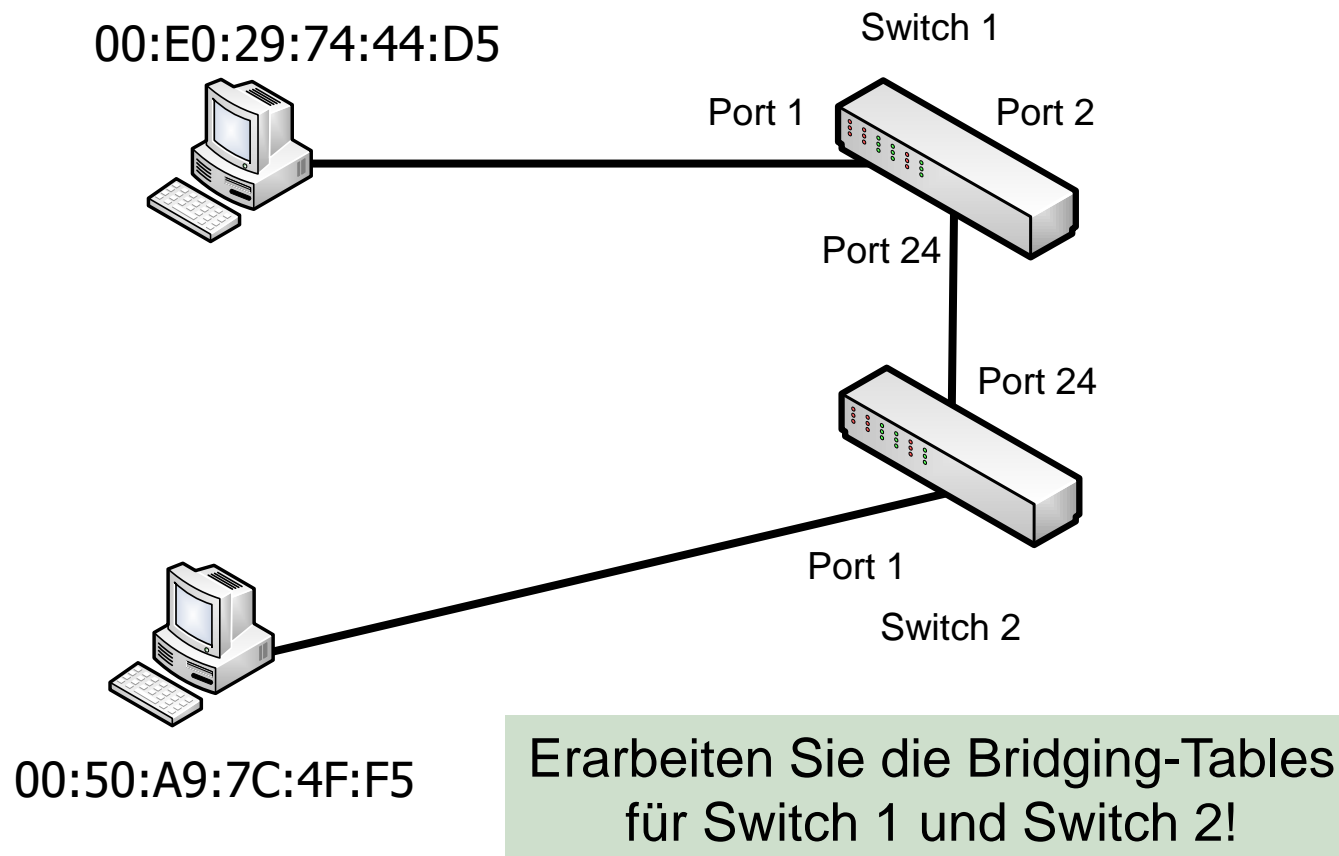
```
switch.schwarz.local - PuTTY
SWITCH-GS 3-Apr-2020 16:20:33
===== TELNET - MANAGER MODE =====
Status and Counters - Port Counters - Port 7

Name :
Link Status : Up
Totals (Since boot or last clear) :
  Bytes Rx      : 454,324,155      Bytes Tx      : 2,299,976,447
  Unicast Rx    : 1,759,938        Unicast Tx    : 1,722,886
  Bcast/Mcast Rx : 37,677          Bcast/Mcast Tx : 13,089,655
Errors (Since boot or last clear) :
  FCS Rx        : 264              Drops Rx      : 0
  Alignment Rx  : 12              Collisions Tx : 0
  Runts Rx      : 0               Late Colln Tx : 0
  Giants Rx     : 0               Excessive Colln : 0
  Total Rx Errors : 269            Deferred Tx   : 0

Actions->  Back  Reset  Help
Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

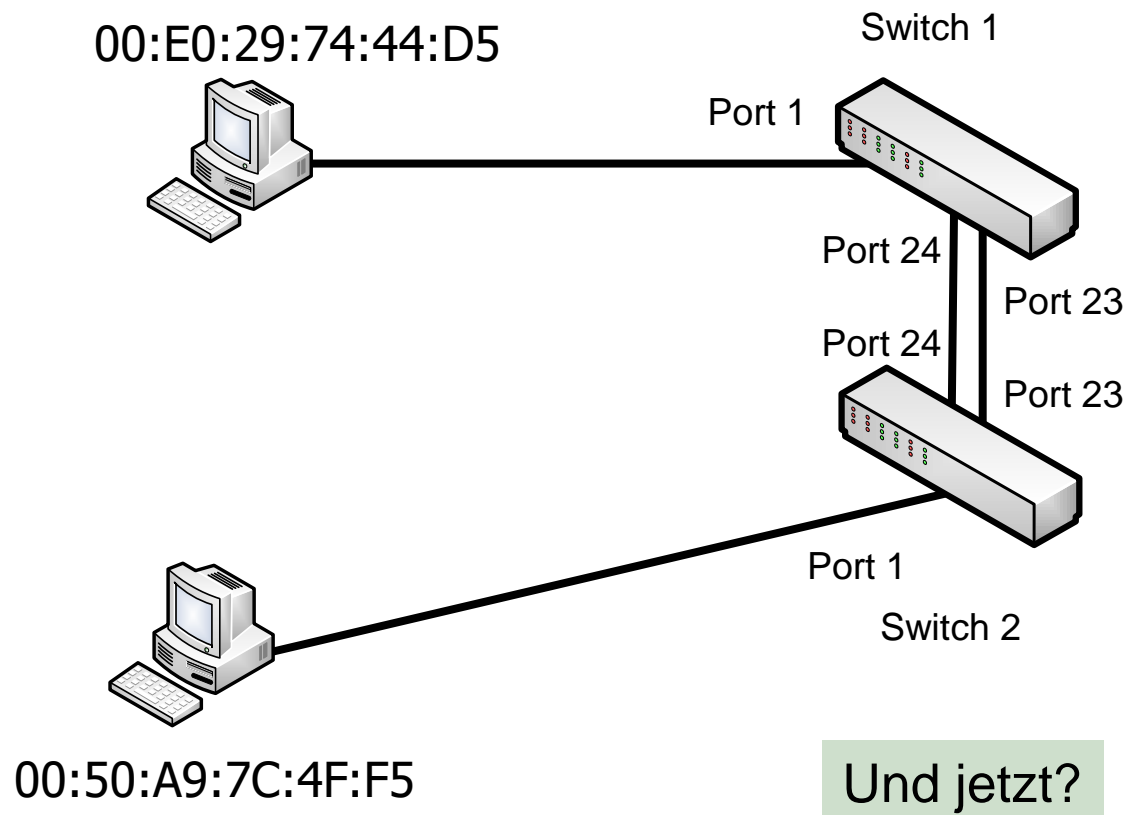


Was ist eigentlich ein Bridging Loop?





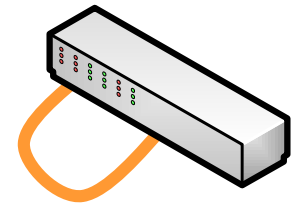
Was ist eigentlich ein Bridging Loop?





Bridging Loops

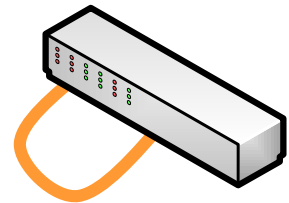
- Bridging Loops treten auf, sobald irgendwo im Netzwerk eine "Schleife" gesteckt ist und keine Schutzmaßnahmen konfiguriert sind
- Diese Schleife kann auch auf einem Switch auftreten
- Durch den Loop fangen Pakete zu kreisen an – Broadcasts vervielfältigen sich. Das gesamte Netzwerk wird innerhalb weniger Sekunden überlastet!
- Ein Bridging Loop im Randbereich eines Netzwerks kann trotzdem das gesamte Netzwerk lahmlegen!
- Ein Bridging Loop kann sogar andere Funktionen von Geräten, die mit dem Netzwerk verbunden sind lahmlegen, da die Interrupts ankommender Pakete die CPU sättigen.





Bridging Loops

- Schutzmaßnahmen:
 - Spanning Tree
 - Loop Protection
- Übung
 - Verbinden Sie drei weitere Rechner Ihrer Kollegen mit dem Testswitch
 - Pingen Sie alle Rechner
 - Trennen Sie die Verbindung des Test-Switches mit dem WIFI-Netz
 - Schalten Sie gemäß den Anweisungen Ihres Trainers Spanning Tree ab, falls es standardmäßig auf dem Testswitch aktiviert ist.
 - Stecken Sie einen Loop und beobachten Sie den Ping!





Bridging-Loops - Eine Horrorgeschichte

- Kundenanruf
 - Bei mir steht das ganze Netzwerk
 - Intern geht nichts, das Internet funktioniert auch nicht
 - Nicht einmal meine ISDN-Telefonanlage funktioniert
- Reaktion des Supports
 - Checken Sie mal Ihre Stromversorgung, die Telefonanlage ist doch bis auf das Management-Interface vollkommen unabhängig vom Netzwerk

Das Problem war letztendlich ein Loop

Warum hat der Loop die Telefonanlage mit in den Untergang gerissen?



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



Namensauflösung



Gängige Namenstypen

- Hostnamen
 - Verwendet:
 - Im Internet
 - In Unix/Linux Netzwerken
 - Zur internen Namensauflösung in Windows Domänen
- NetBIOS-Namen
 - verwendet als:
 - „Legacy“-Namenssystem unter Windows
 - Standardnamens-System von NT4 und früher
 - Max 15 Zeichen

Ein Windows-Rechner verwendet denselben Namen in beiden Welten!



Gängige Namenstypen

- Windows-Rechner verwenden Hostnamen und NetBIOS-Namen zur Namensauflösung
- Jedes Mal, wenn ein Rechnername eingegeben wird, versucht das Betriebssystem diesen Namen für die Anwendung zu einer IP-Adresse aufzulösen
- Bei der Eingabe von z.B.: `http://server1` können Sie nicht mit Sicherheit sagen, über welche Technologie der Name aufgelöst wurde



Reihenfolge der Namensauflösung

„Namenswelt“: Hostnamen

1.) HOSTS-Datei

2.) DNS-Anfrage

3.) LLMNR+Cache

„Namenswelt“: NetBIOS-Namen

4.) NetBIOS Cache

5.) WINS-Server

6.) Broadcast

7.) LMHOSTS-Datei



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



DNS (Domain Name System)



Arten der Auflösung

- Forward-Lookup
 - Name → IP
- Reverse-Lookup
 - IP → Name



Wie arbeitet DNS?

- Clients fragen einen Server, der sich um die Auflösung der Namen kümmert.
- Server haben sogenannte ZONEN geladen (Namens/IP – Tabellen) und können über deren Inhalte Auskunft geben.
- Zonen werden zu einem "Namensraum" verbunden.



Begriffserklärungen

- FQDN
(Fully qualified Domain Name)

Kombination aus Hostname und Domäne:

www.iic.wifi.at

↓ ↓

Hostname Domäne



Begriffserklärungen

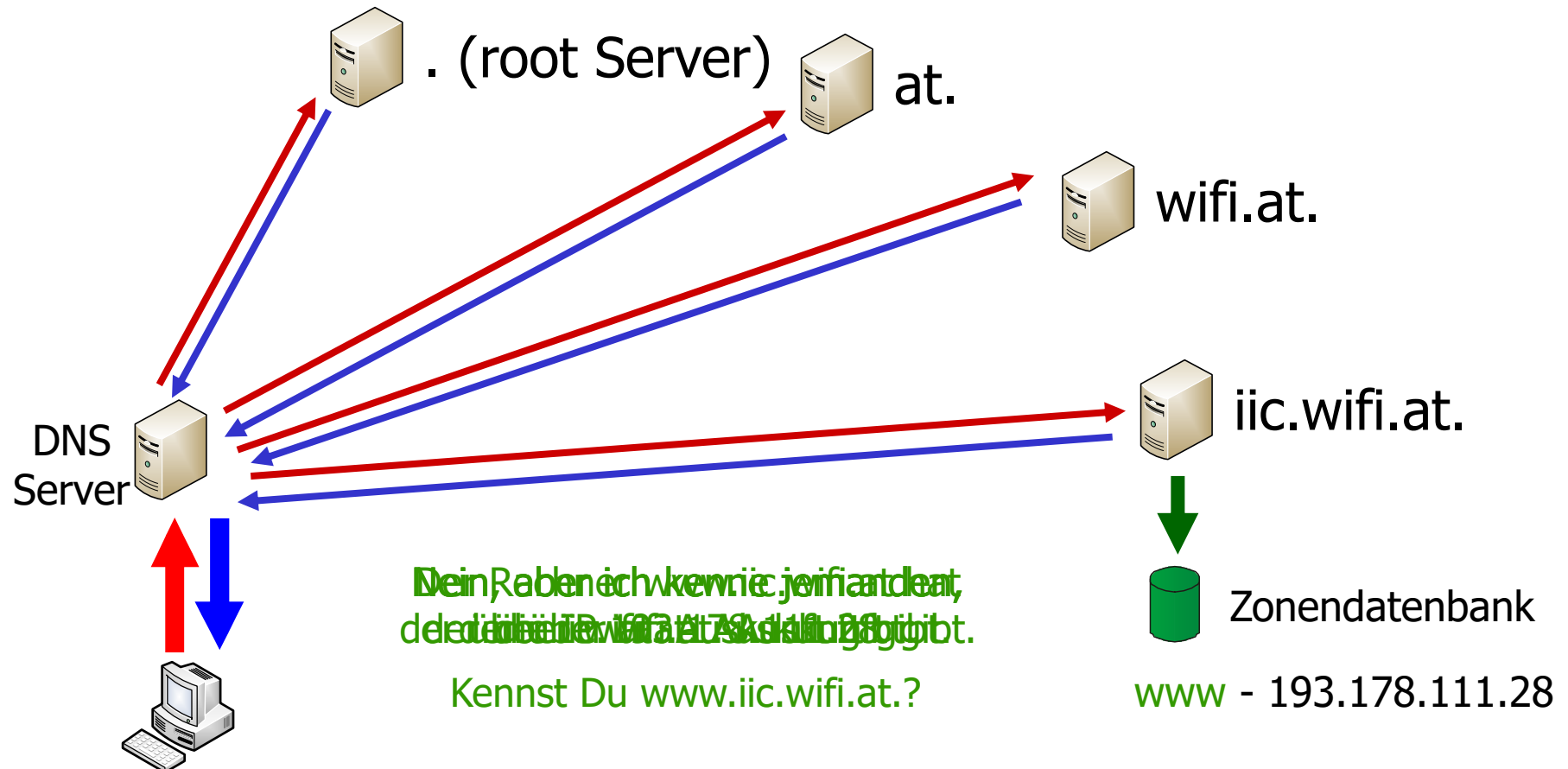
- Domäne:
Pfad durch den Namensraum; beinhaltet alle Zonen, die befragt werden müssen.

iic.wifi.at.





DNS-Namensauflösungsprozess





Was ist das Domänensuffix eines Rechners?

- Wird im Rahmen eines Namensauflösungs-prozesses nur der Hostname angegeben, wird das Suffix des Rechners angehängt, um einen FQDN zu formen
- Dieser FQDN wird dem DNS-Server zur Auflösung übergeben



Übung-DNS

- Konfigurieren Sie Ihren Rechner so, dass er die vom Trainer angegebenen DNS-Server verwendet!
- Setzen Sie das DNS-Suffix Ihres Rechners auf den vom Trainer vorgegebenen Wert!



Überprüfung der DNS-Funktion

- nslookup <FQDN>

Beispiel:

```
C:\>nslookup www.iic.wifi.at
Server:    dns1.firma.intern
Address:   192.168.2.254
```

```
Name:      www.iic.wifi.at
Address:   81.189.214.132
```



DHCP (Dynamic Host Configuration Protocol)



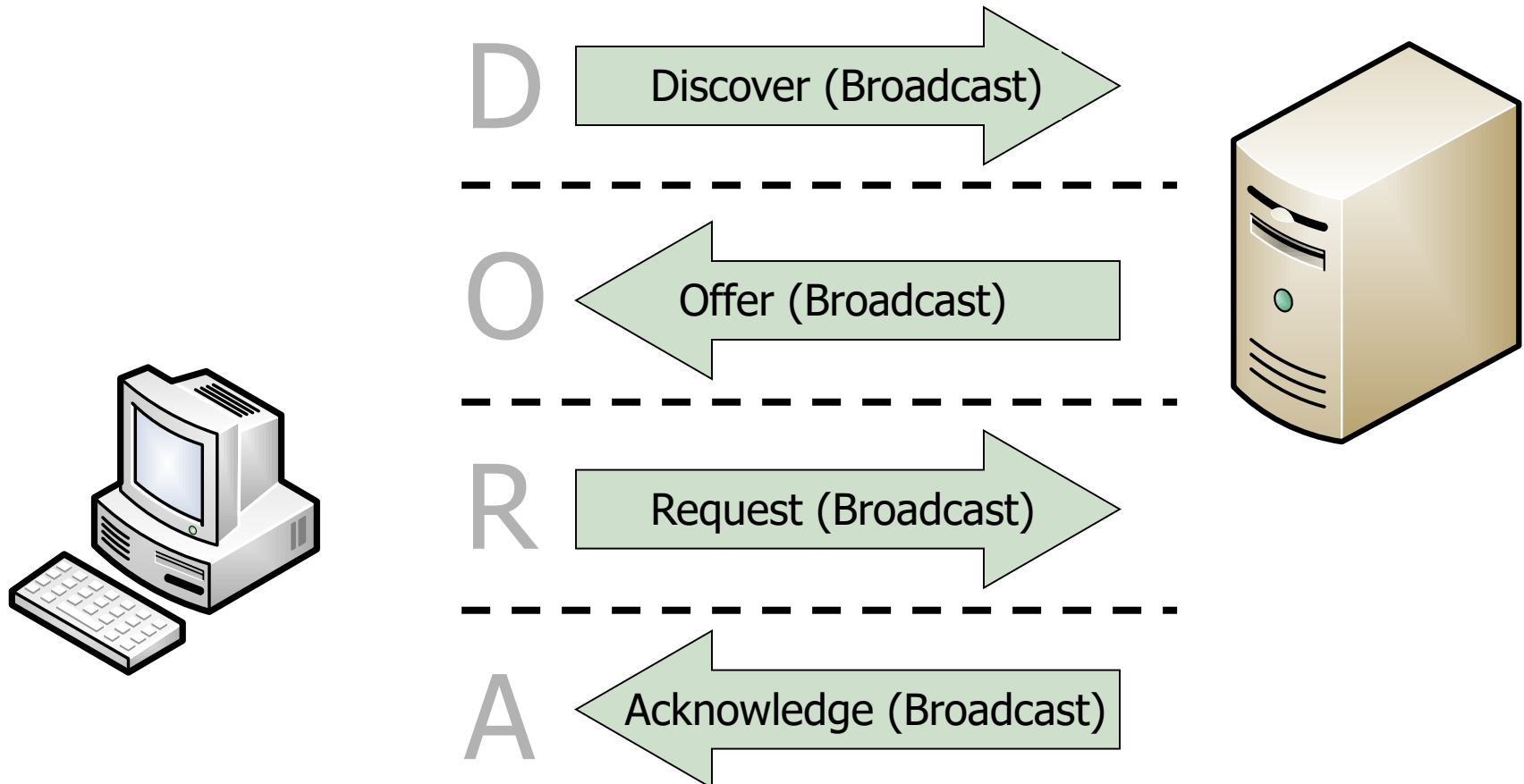
DHCP-Server und Clients

- DHCP-Server Anforderungen
 - DHCP-Dienst
 - Statische IP-Adresse
 - Gültiger Bereich

- Gängige DHCP-Optionen
 - IP-Adresse
 - Subnetz
 - Gateway
 - DNS
 - Domänenname

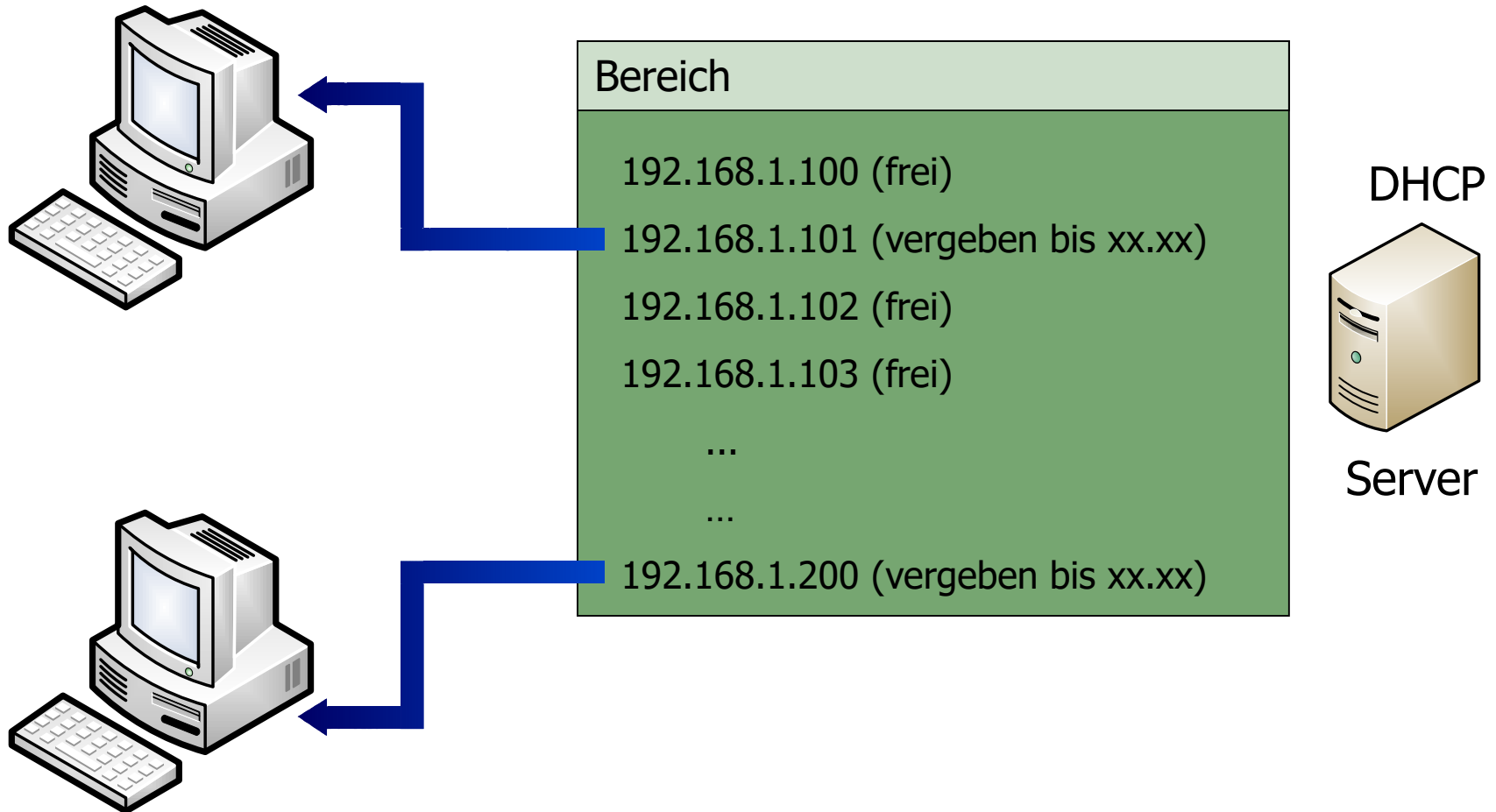


DHCP-Lease Vorgang





DHCP-Bereiche





Was man noch wissen sollte...

- Ein DHCP Server prüft nicht, ob die IP-Adresse, die er gerade ausgibt, bereits im Netzwerk verwendet wird
- Konfigurieren Sie also NIE statische Adressen im Adressbereich des DHCP-Servers!



Übung - DHCP

- Konfigurieren Sie Ihren Rechner als DHCP-Client
- Überprüfen Sie die Konfiguration mit `ipconfig`
- Geben Sie die IP-Adresse wieder frei: `ipconfig /release`
- Beziehen Sie erneut eine IP-Adresse: `ipconfig /renew`



Diskussion

Nehmen wir an, Sie haben einen Rogue-DHCP Server im Netzwerk. Also ein System, das unpassende IP-Konfigurationen über DHCP verteilt und das Sie nicht konfiguriert haben.

Wie finden Sie dieses System und können es vom Netzwerk trennen? Nehmen wir an, sie verwenden verwaltbare Switches in Ihrem Netzwerk.



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



IPv6



IPv6

- Nachfolger von IPv4
- 1998 standardisiert (Arbeiten seit 1995)
- Adressraum: 2^{128} statt 2^{32} Adressen
- Weitgehende Vermeidung von Broadcasts ; vermehrte Abstützung auf Multicasts
- Autokonfiguration (Rechner kann IP-Adresse selbst erstellen)
- IPv6 Internet im Aufbau, Websites von Unternehmen wie Amazon, Google bereits erreichbar



IPv6 - Adressen

- Notation: Hexadezimal: Ziffern von 0 bis 9 und Buchstaben von A-F
- Trennzeichen zwischen Blöcken: :
- 8 Blöcke zu vier Stellen:
`2a00:0000:0000:0c01:0000:0000:0000:0069`
- Vereinfachungsregeln:
 - Aufeinanderfolgende Nullen dürfen durch eine 0 ersetzt werden:
`2a00:0:0:0c01:0:0:0:0069`
 - Führende Nullen im Block dürfen weggelassen werden
`2a00:0:0:c01:0:0:0:69`
 - Aufeinanderfolgende Blöcke von Nullen dürfen einmal in der Adresse durch :: zusammengefasst werden:
`2a00:0:0:c01::69`



Netz- und Hostanteil

- Auf einem Host 64b Netzanteil, 64b Hostanteil ('Trennung in der Mitte')

2a00:0000:0000:0c01:0000:0000:0000:0069

Netzanteil

Hostanteil

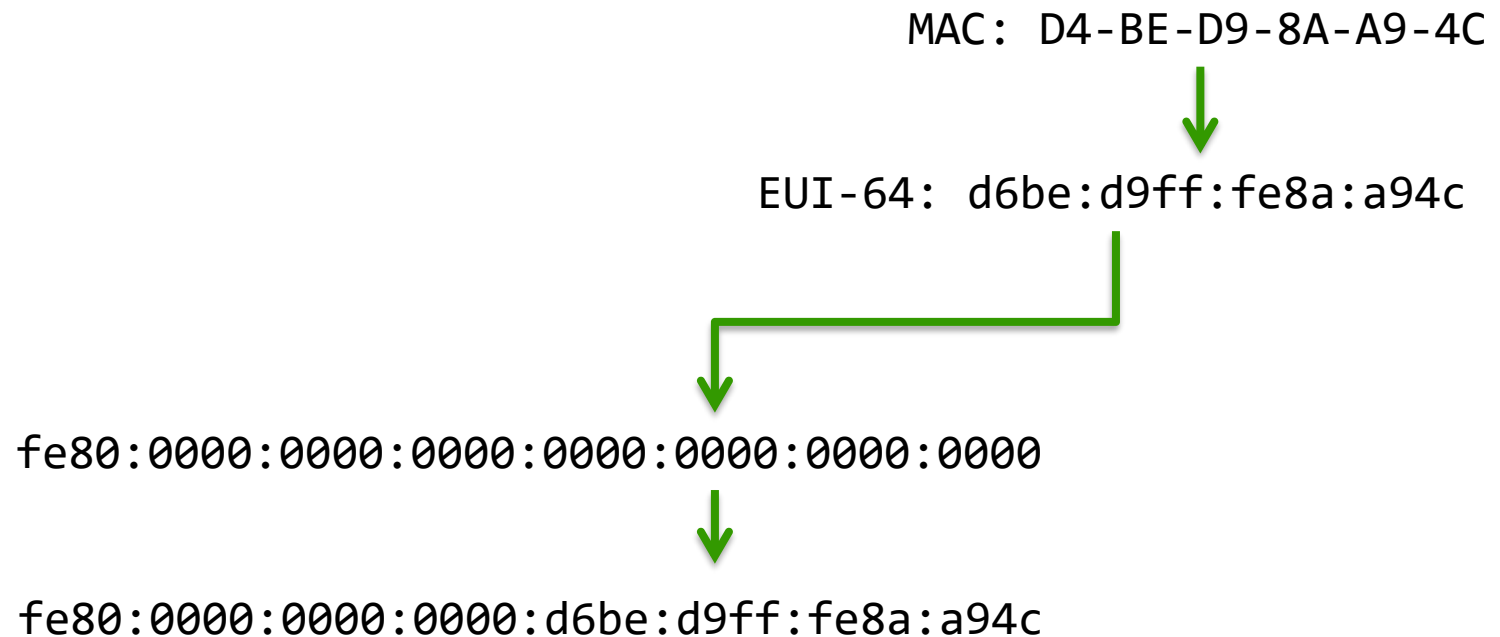


LinkLocal-Adressen

- Werden automatisch generiert
- Zur Kommunikation mit anderen Stationen im selben Netz
- Prefix (=Netzanteil) immer fe80::
- Hostanteil wird aus MAC-Adresse generiert
- **Der Host hat also sofort eine IP-Adresse mit der er zumindest mit Rechnern im selben Netz kommunizieren kann**
- Link-Local-Adressprefix fe80: kommt auf jeder IPv6 aktivierten Netzwerkkarte vor



Generierung von LinkLocal-Adressen





Interface-Index

- Da jede Netzwerkkarte eine LinkLocal-Adresse besitzt, muss angegeben werden können von welcher Karte ein Paket gesendet wird
- Angabe durch % nach der IP-Adresse

```
Ethernet-Adapter LAN:
  Verbindungslokale IPv6-Adresse . : fe80::bd47:224d:a0c8:de6%13
  IPv4-Adresse . . . . . : 192.168.10.119
  Subnetzmaske . . . . . : 255.255.255.0
  Standardgateway . . . . . : 192.168.10.254
Ethernet-Adapter VOIP:
  Verbindungsspezifisches DNS-Suffix:
  Verbindungslokale IPv6-Adresse . : fe80::e434:6db7:77e1:f6df%11
  IPv4-Adresse . . . . . : 10.50.2.181
  Subnetzmaske . . . . . : 255.255.0.0
```

- ping fe80::4c1d:f859:d49d:72c9%11 pingt fe80::4c1d:f859:d49d:72c9 von der Netzwerkkarte VOIP aus



Adress-Präfixe

- Link Local (nur auf dem LAN-Segment gültig):
fe80::
- Global Unicast (~offizielle IP-Adressen)
2000:: bis 3fff::
- Unique Local Unicast (~privaten IP-Adressen)
FC00:: bis FDFF::
- Multicast
FF00:: bis FFFF::

Beispiele:

- **FF02**: Im LAN-Segment, **FF05**: Im Standort, **FF08**: Des Unternehmens
- **FF02::2** Alle Router im LAN
- **FF05::1:3** Alle DHCP-Server im Standort



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



VLANs (Virtual LANs)



Was sind VLANs?

- Vereinfacht gesagt, erlauben VLANs einen Switch in mehrere einzelne virtuelle Switches aufzuteilen
- Die Aufteilung erfolgt mit Hilfe einer Nummer, die jedem VLAN zugewiesen wird
- Diese Nummer wird als VLAN-Tag bezeichnet und bewegt sich im Bereich von 0-4095



Was sind VLANs?

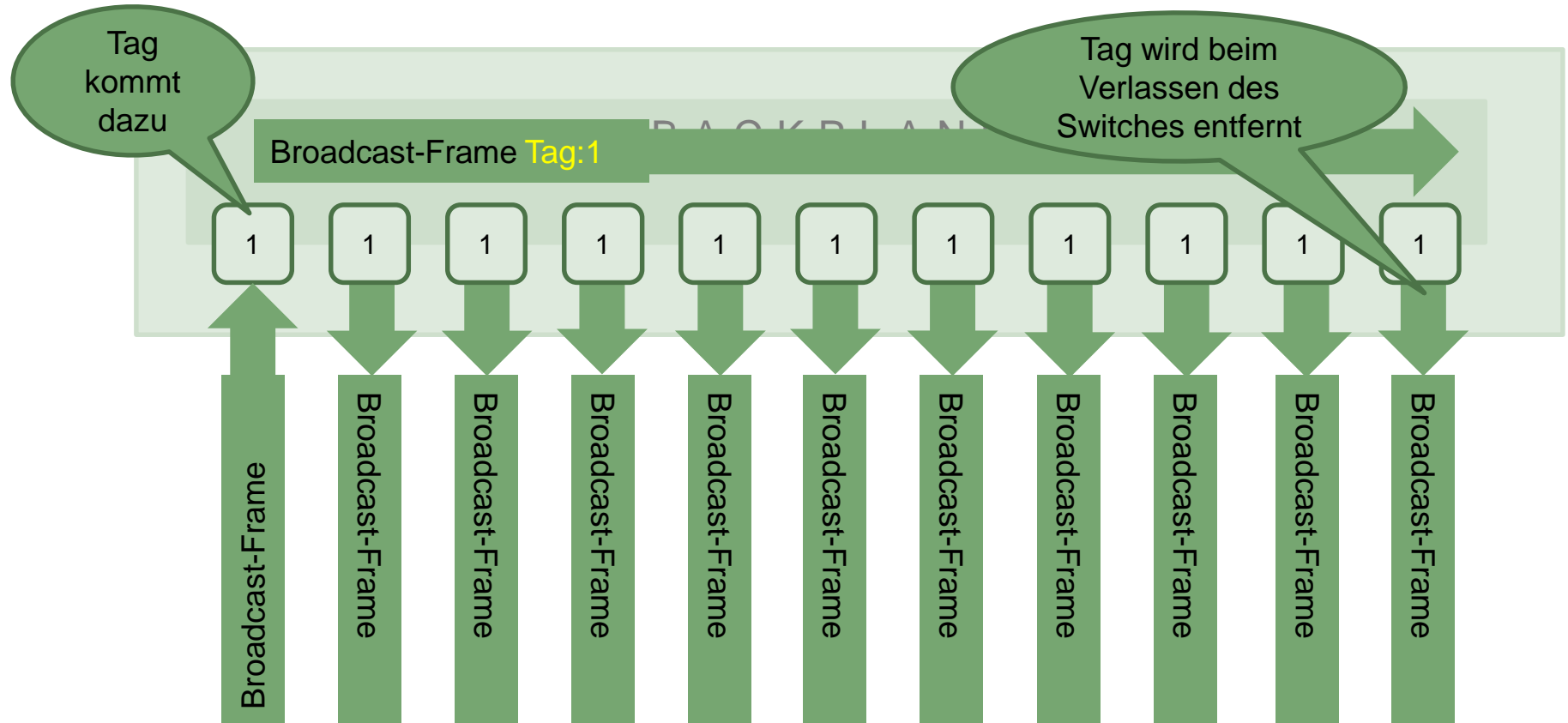
- Jeder Switchport wird einem VLAN zugeordnet
- Beim Ingress wird jedem Frame ein VLAN-Tag hinzugefügt
- Das Paket verlässt den Switch nur auf Ports, die dem VLAN zugeordnet sind
- Vor dem Egress wird der VLAN-Tag entfernt
- Daher arbeitet ein VLAN-fähiger Switch intern immer mit getaggten Paketen

- Durch die Tagging-Information wird ein Frame ein wenig größer und wird von normalen Endgeräten ohne spezielle Treiber nicht 'verstanden'

- Standardisiert in 802.1q
- Neben dem VLAN-Tag werden auch noch Prioritäts-Informationen übertragen



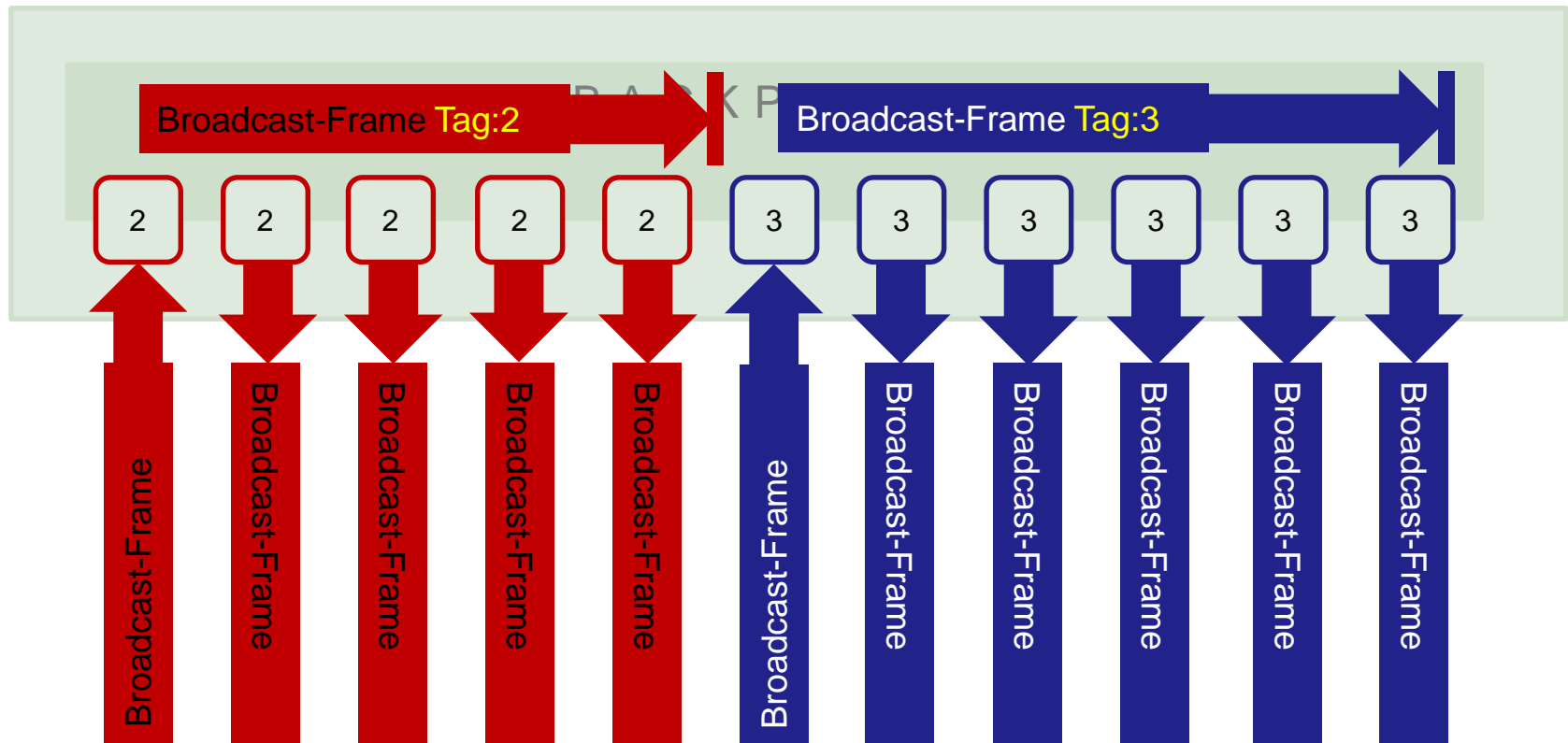
Ein VLAN-fähiger Switch in Standard-Konfiguration



1: Default VLAN



Mehrere VLANs



2: VLAN rot 3: VLAN blau



Porteinstellungen

- Ein Port kann einem VLAN untagged oder tagged angehören
- Untagged
 - Beim Ingress wird der Tag hinzugefügt
 - Beim Egress wird der Tag entfernt
 - Ein Switchport kann nur ein VLAN untagged haben
- Tagged
 - Beim Ingress wird der Tag nicht verändert
 - Beim Egress werden Tags auf dem Frame belassen



Diskussion

Wenn ein Endgerät ohnehin keine getaggten Pakete versteht, wieso gibt es dann den 'Tagged'-Modus?

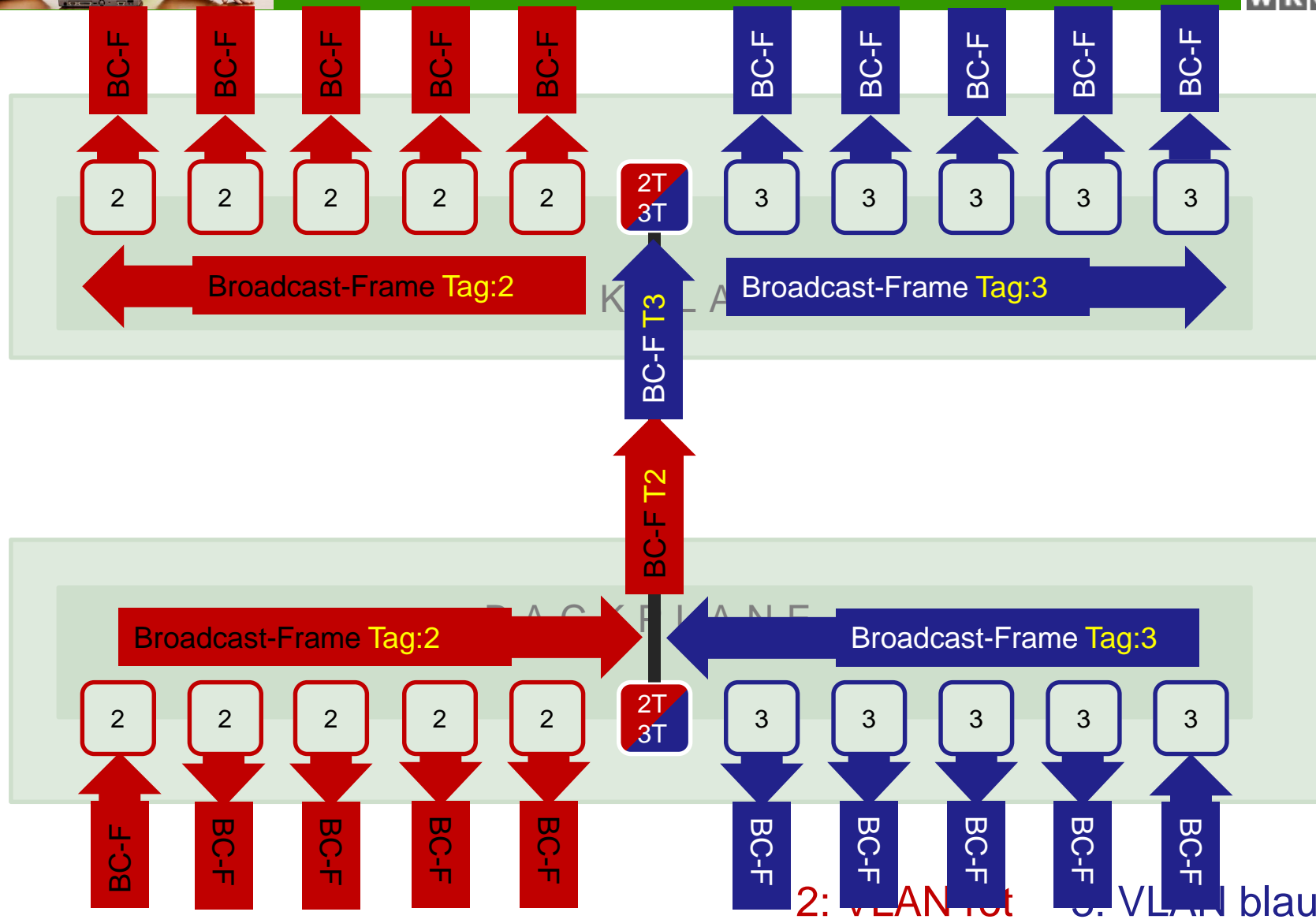
Transport von VLANs über mehrere Switches

Betrieb von Geräten, die mit Hilfe spezieller Treiber VLANs kennen



Netzwerkadministrator

Modul 1 – Netzwerk Grundlagen



2: VLAN rot 3: VLAN blau



VLAN-Übungen

- Vierer-Übung
- Verbinden Sie 4 PCs mit Ihrem Testswitch
- Konfigurieren Sie die PCs mit statischen IP-Adressen in einem privaten Netzwerk
- Pingen Sie auf jedem PC alle anderen PCs mit ping -t
- Konfigurieren Sie auf Ihrem Testswitch nun zwei VLANs
- Schalten Sie jeweils zwei PCs in ein VLAN
- Was fällt Ihnen auf?
- Konfigurieren Sie die PCs in jedem VLAN mit einem eigenen privaten IP-Netzwerk



VLAN-Übungen

- Verwenden Sie nun einen zweiten Testswitch
- Richten Sie auch auf dem zweiten Testswitch die VLANs ein
- Konfigurieren Sie nun eine Verbindung zwischen beiden Switches, und übertragen Sie Pakete beider VLANs tagged über den Uplink
- Verbinden Sie die PCs der beiden VLANs mit jeweils einem der beiden Switches
- Können sich die PCs im jeweiligen VLAN noch pingen?



Diskussion

Wie könnten Sie die VLANs nun wieder miteinander verbinden?

Über einen Router



Diskussion

Wieso tut man sich das dann überhaupt an?

Aus demselben Grund, wieso man sonst Netzwerke trennen würde
(Verschiedene Bereiche, Trennen von Broadcast-Domains, ...)



Diskussion

Kann ein Switchport gleichzeitig ein tagged VLAN und ein untagged VLAN tragen?

Bei welchen Geräten ist diese Konfigurationen üblich?

VoIP-Telefonen mit PC am Telefon
(Meist verwendet, wenn nicht genügend Netzwerkports vorhanden sind)