CCNA Zusammenfassung

Cisco Certified Network Associate Zusammenfassung

Emanuel Duss

2016-09-07 20:31

Contents

1 CCNA 1: Network Fundamentals

1.1 ISO/OSI Modell

Nr	Layer	PDU	Protocol Example	Devices
7	Application Layer	Data	HTTP/DNS/SMTP/...	
6	Presentation Layer		ASCII, JPEG	
5	Session Layer		3 Way Handshake	
4	Transport Layer	Segment/Datagram	TCP,UDP	
3	Network Layer	Packet	IPv4,IPv6	Router,L3 Switch
2	Data Link Layer	Frame	802.2,802.3,PPP	Bridge/Switch,Node
1	Physical Layer	Bit		Hub

1.2 Layer 1: Physical Layer

Ethernet Types

Ethernet Typ	Bandbreite	Kabeltyp	Duplex	Maximale Distanz
10Base-5	10 Mbps	Thiknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thiknet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-T	100 Mbps	Cat5 UTP	Half	100 m
100Base-T	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fibber	Half	400 m
100Base-FX	200 Mbps	Multimode Fibber	Full	2 km
1000Base-T	1 Gbps	Cat 5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat 6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	5 km
10GBase-CX4	10 Gbps	Twinaxial	Full	15 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km

- Electrical, optical oder Mikrowellensignale
- Fundamentale Funktionen: Physikalische Komponenten, Encoding und Signalisierung
  - Encoding: 0 und 1
  - Signaling: Wie werden 1 und 0 dargestellt
  - NRZ: Non Return no Zero: Low = 0; High = 1 // Langsam, da ineffizient, Fehlerhaft wenn mehrere 1 nacheinander
  - Manchester: 1 = Steigend; 0 = Fallende Flanke // Auch nicht sooo schnell. 10Mbps ok
- Signal Pattern: Start of Frame; End of Frame; Frame Content
  - Können in Bits umgewandelt werden
- Data (11111) -> Code (101101010) -> Signal $^{vv}v^{vvv}$
- Encoding: Error Detection, Clock synchronisation verbesserung
  - Nicht zu viele 1 oder 0 in Folge
  - Energie sparen (ausgleich zwischen high und low)
  - Data und Control besser unterscheidbar
- Encoding: 4B/5B
- Geschwindigkeit
  - Bandbreite: kbps

  - Throughput: transfer of bits over a given period of time
  - Goodput: Usable transfer ofer a given period of time (most interest to users) // Nutzlast

1.2.1 Fiber Media

- Single-Mode
  - Laser: Ein Laser Lichtstrahl im Zentrum
  - Lange Distanzen; kein Verlust da keine Reflektionen; bis 100 km
  - Kleiner Core: 8-10 microns (Cladding: 125 microns)
  - Teurer
- Multimode
  - LED: Mehrere Winkel über mehrere Reflektionen
  - Kurze Distanzen, da Verlust bei der Reflektion; bis 2 km
  - Grosser Core: 50/62.5 microns (Cladding: 125 microns)
  - Günstiger

1.2.2 Wireless Media

- 802.11 mit CSMA/CA; WLAN
  - a: 5GHz bis 54Mbps; hohe frequenz: schwieriger durch gebäude/mauern; nicht mit b/g kompatibel, da hohe frequenz
  - b: 2.4Ghz 11Mbps; grössere Reichweite
  - g: 2.4Ghz: 54Mbps
  - n: 2.4 oder 5Ghz; 100-210Mbps 70M distanz
- 802.15 WPAN = Bluetooth
- 802.16: WiMAX: Point to Multipoint Breitbandanschluss
- GSM: Telefonie

1.3 Layer 2: Data Link Layer

1.3.1 Begriffe

- Data Link Layer: Verbindung zwischen HW und SW
- Frame
  - Header
  - Data
  - Trailer
  - Ende detektieren / Error Detection
  - FCS Frame Check Sequence mittels CRC (Hash)
  - Plus Padding
- Sublayer
  - LLC Logical Link Control
  - Software Process
  - Network Layer Packet identifizieren und bilden
  - MAC Media Access Control
    - Media Access Control: Frame auf und vom Medium
  - Hardware Process
  - Frame adressieren
  - Beginn und Ende markieren
  - Schaut, ob Medium frei ist.
- Standards
  - Ethernet, PPP, HDLC, Frame Relay, ATM
  - IEEE 802.2 (LLC)

        * IEEE 802.3 (Ethernet)
        * IEEE 802.11 (WLAN)
    - Q.922 (Frame Relay)
        * Q.921 ISDN Data Link Standard)
- Topology
    - Point to Point: Half Duplex
- TCP/IP Netzwerke verwenden Ethernet II Frames
- PPP
    - WAN Protokoll in RFC definiert (Nicht IEEE)
    - Punkt zu Punkt (kein Absende/Empfänger im Frame)
- WLAN
    - CSMA/CA mit Backoff Algorithmus: Warten auf Zugriff
    - Frame: Type: Entweder Control, Data oder Management

1.4 Ethernet

- Ethernet definiert Layer 1 und Layer 2
    - Layer 2 LLC: IEEE 802.2
    - Layer 2 MAC und Layer 1: IEEE 802.3
- Früher: Bus: Thicknet 10Base5 und Thinnet 10Base2
    - Multi Access: Logical Topology: Bus
- Collision
    - Hub: Half-Duplex
    - Switch: Full-Duplex
- Frame
    - DIX = Ethernet II = Ethernet: Preamble + Start of Frame delimiter, Type
    - IEEE 80.23: Preamble 8, Length
    - Zwischen 64 und 1518 Bytes
- Multicast
    - IP: 224.0.0.0 - 239.255.255.255
    - MAC: 01:00:5E: + Lower 23 Bits der IP Adresse
- CSMA/CD: Clients erkennen Kollisionen aufgrund ansteigender Amplitude
    - JAM Signal wird gesendet
    - Backoff warten
- Collision Domain = Netzwerksegment
- Timing
    - Bit Time / Slot Time
- 10Base-T: Manchester
    - 100Base-TX: 4b/5b
    - 100Base-Fx: Fiber
    - 1000Base-T: Braucht alle 8 Adern mit 125Mbps = 1Gbps
- Switching
    - Store and Forward: FCS wird geprüft

1.5 Planning and Cabling Networks

- Router: Zwischen Netzwerken "routen"
- Switch: Point to Point logical Topology zwischen 2 Hosts
- MDI (Media Dependent Interface) 1,3 TX; 3,6 RX
    - MDIX (crossover)
- WAN: Stecker = Winchester (60 Pin Serial) oder RJ11 (Telefon)
    - DCE: Gibt Clock an; Provider (Female)
    - DTE: Empfängt Clock; Customer (Male)
- Cabeling

  - Horizontal Cabling / Distribution Cabling = Patchdose - Patchpanel
  - Vertical: Backbone
  - Router WAN
  - Smart Serial (Cisco) - Winchester -> Winchester - Smart Serial
- Console Cabel: DB-9 - RJ45
  - Configuration Cisco Devices via Rollover Cable
  - Bps: 9600 bps
  - Data Bits: 8
  - Parity: None
  - Stop Bits: 1
  - Flow Control: None

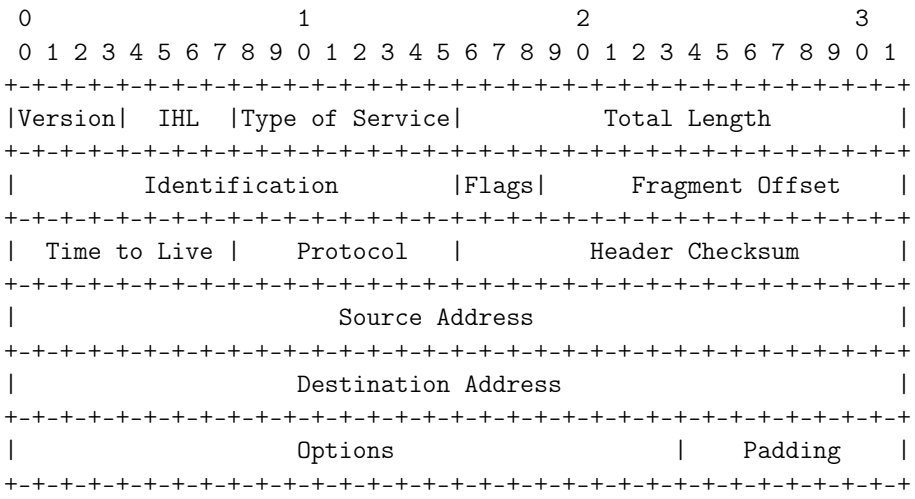
1.6 Layer 3: Network Layer

1.6.1 IP

Definiert im RFC 791.

- Effizient: Best Effort = Unreliable
- Medienunabhängig
- Fragmentierung möglich (MTU: Maximale Framegrösse; Flags: DF/MF)

Header:



- TOS = QOS
- Protocol: 1 ICMP, 6 TCP, 17 UDP

1.7 Layer 4: Transport Layer

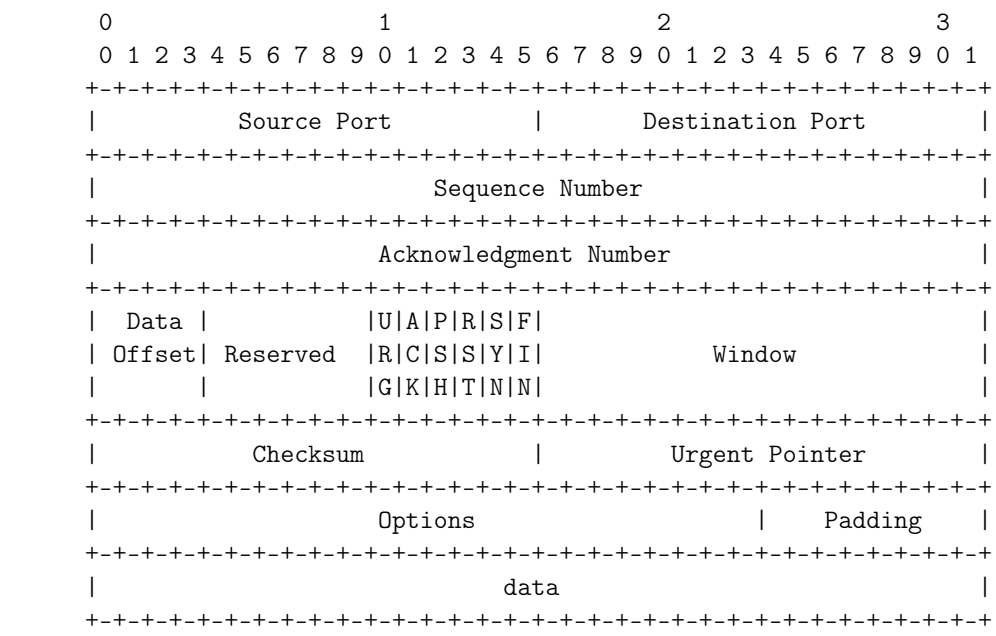
1.7.1 Port Nummern

Port Nummern	Anwendungsbereich
0-1023	Well Known Ports
1024-49151	Registred Ports
49152-65535	Private/Dynamic Ports / Ephemeral Ports

- http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

1.7.2 Transmission Control Protocol (TCP)

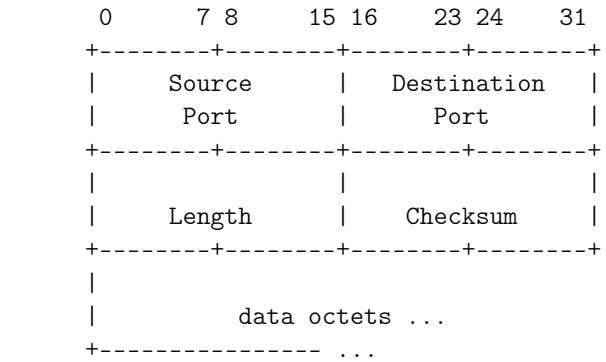
RFC 793



- Sequence Number: Wieviele Bytes schon übertragen wurden
- Acknowledge Number: Welches Byte als nächstes erwartet wird (expectional acknowledge)
- Nicht vergessen: Verbindung sind zwei One-Way Sessions
- Window Size: Wieviele unbestätigte ACKs vorhanden sein dürfen

1.7.3 UDP

RFC 768



- *Length* is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)
- *Checksum* is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

1.8 Layer 7: Application Layer

1.8.1 Dynamic Host Control Protocol (DHCP)

- Discover, Offer, Request, Acknowledge

- Request nachträglich ablehnen (NACK)

1.9 Kapitel 11: Configuring and Testing Your Network

- CLI: virtual teletype interface (vty)
- Configuration Files
  - Startup Config in NVRAM (Nonvolatile RAM)
  - Running Config: Startup Config wird vom NVRAM beim Startup ins RAM kopiert
  - `Router# copy running-config startup-config`
- IOS Modes
  - User EXEC mode, Privileged EXEX mode, Global configuration mode und Other configuration modes
  - `Router#show privilege`
- IOS Helping
  - Context-sensitive help
  - Command syntax check
  - Hot keys and shortcuts

2 CCNA 2: Routing Protocols and Concepts

2.1 Ein Router

- Stub Network: Network accessed by a single router
- Startsequenz
  - POST (Power On Self Test)
  - Bootstrap Code ausführen
  - Configuration Register überprüfen (in NVRAM; setzen mit Command `config-register command <NR>`)
  - Startup Config
  - Keine Startup Config: IOS von Flash, TFTP oder ROM booten
- IOS Laden: Flash oder TFTP
- Serielles Kabel
  - DTE: Male
  - DCE: Female; Clock angeben

2.2 Theorie

Überblick Routing Protokolle

Eigenschaft	RIP	RIPv2	IGRP	EIGRP	OSPF	RIPng	EIGRP for IPv6	OSPFv3
IGP	x	x	x	x	x	x	x	x
EGP								
Distance Vector	x	x	x	x		x	x	
Link State					x			x
Classful	x		x					
Classless		x		x	x	x	x	x
IPv4	x	x	x	x	x			
IPv6						x	x	x

- IGP: Interior Gateway Protocol
- EGP: Exterior Gateway Protocol (z. B. BGP)
- LinkState: Informationen werden unverändert an alle weitergeleitet

- RIP (Routing Information Protocol): Hop-Count based
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First): Bandwith based
- IS-IS (Intermediate System–to–Intermediate System)
- BGP (Border Gateway Protocol)

Administrative Distanzen

Route Source	Administrative Distanz
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200
Ungültig	255

Subnetting (Beispiel `255.255.255.0`)

Zusätzliche Bits	Oktett	Adressen pro Subnetz
0	.0	255
1	.128	128
2	.192	64
3	.224	32
4	.240	16
5	.248	8
6	.252	4
7	.254	2
8	.255	1

- Anzahl Subnetze = 2^n (n = geborgte Bits)
- Anzahl Hosts: 2^n-2 (n = 0 in Netzmaske)

ICMP Codes

Type	Code	Description
0	0	echo reply
3		destination unreachable
	0	network unreachable
	1	host unreachable
	2	protocol unreachable
	3	port unreachable
	4	fragmentation needed
	5	source route failed
	6	destination network unknown
	7	destination host unknown
	8	source host isolated
	9	destination network administratively prohibited
	10	destination host administratively prohibited

Type	Code	Description
	11	network unreachable for ToS
	12	host unreachable for ToS
	13	communication administratively prohibited by filtering
	14	host precedence violation
	15	precedence cutoff in effect
4	0	source quench
5		redirect
	0	redirect for network
	1	redirect for host
	2	redirect for type of service and network
	3	redirect for type of service and host
8	0	echo request
9	0	router advertisement
10	0	router solicitation
11		time exceeded
	0	time-to-live equals 0 during transmit
	1	time-to-live equals 0 during reassembly
12		parameter problem
	0	IP header bad
	1	required option missing
13	0	timestamp request
14	0	timestamp reply
15	0	information request
16	0	information reply
17	0	address mask request
18	0	address mask reply

2.3 Grundkonfiguration

Privileged EXEC Mode

```
Router> enable
```

Konfiguration löschen

```
Router# erase startup-config
Router# reload
```

Konfigurieren

```
Router# configure terminal
```

Logging Meldungen sollen Eingabezeile nicht überschreiben

```
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#logging synchronous
```

Timeout setzen

```
Router(config-line)#exec-timeout minutes [seconds]

R1(config)#line console 0
R1(config-line)#exec-timeout 0 0

R1(config-line)#line vty 0 4
R1(config-line)#exec-timeout 0 0
```

Hostname setzen

```
Router(config)#hostname R5
```

Disable DNS Lookup

```
R(config)# no ip domain-lookup
```

EXEC Mode Passwort setzen

```
R(config)#enable password foobar // Klartext
R(config)#enable secret foobar // leicht verschlüsselt
```

EXEC Mode Passwort entfernen

```
R1(config)#no enable password
```

Konsolenpasswort setzen

```
R(config)#line console 0
R(config-line)#password cisco
R(config-line)#login
```

Telnet Passwort

```
R(config)#line vty 0 4
R(config-line)#password cisco
R(config-line)#login
```

Sessions anzeigen (Z. B. Telnet-Sessions)

```
R(config)#show session
```

MOTD-Banenr setzen

```
R(config)#banner motd #
AUTHORIZED ACCESS ONLY!
#
```

Ethernet Interface Konfigurieren

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#description R1 LAN
R1(config-if)#no shutdown
```

Interface ohne Verbindungn pingen

```
R1(config-if)#no keepalive
```

Serial Interface Konfigurieren

```
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#end
```

Konfiguration speichern

```
R2#copy running-config startup-config
```

Konfiguration anzeigen

```
R1#show running-config
R1#show startup-config
```

Version anzeigen

```
R1#show version
```

Interfaces anzeigen

```
Router# show ip interface brief
```

Stack testen

```
R#ping 127.0.0.1
R#traceroute 127.0.0.1
```

- `!` ICMP Reply
- `.` Timeout
- `U` ICMP Unreachable

Ping / traceroute

```
R1#ping 192.168.1.10
R1#traceroute 192.168.1.10
```

2.4 Statisches Routing

Route anzeigen

```
R# show ip route
```

Debugging aktivieren / deaktivieren

```
R1#debug ip routing
R1#no debug ip routing
```

Statische Route hinzufügen

```
Router(config)# ip route network-address subnet-mask ip-address
R3(config)# ip route 172.16.2.0 255.255.255.0 Serial0/0/1
```

Default-Route (Wirt mit einem * markiert)

```
Router(config)#ip route 0.0.0.0 0.0.0.0 { ip-address | interface }
```

2.5 RIPv1 - Classful

2.5.1 Theorie

- Distance Vector
- Classful
  - Subnetzmaske wird nicht weitergeleitet
- Hop Count Max = 15
- Broadcast Routing Information
- UDP Port 520

Timers

- Update-Timer: Alle 30 Sekunden
- Invalid-Timer: Nach 180 Sekunden wird die Route auf `invalid` gesetzt (mit Metrik = 16).
- Flush-Timer: Nach 240 Sekunden wird die Route gelöscht.
- Hold-down-Timer: Für Loop-Verhinderung: Nachdem eine Route als unerreichbar (Metrik = 16) markiert wurde, wird der Hold-Down-Timer auf 180 Sekunden gesetzt und während dieser Zeit keine neuen Updates mehr erhalten

2.5.2 Konfiguration

RIP aktivieren

```
R1(config)#router rip
```

RIP Protokoll auf Netzwerk aktivieren und Netzwerk ankündigen

```
R1(config-router)#network 192.168.1.0
R1(config-router)#no auto summary # nicht summarisieren! Nicht automatisch zusammenfassen
```

RIP-Messages auf einem Interface nicht senden und nicht empfangen:

```
R1(config-router)#passive-interface Fastethernet 0/0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface Fastethernet 0/0
```

Default-Route miteinbeziehen

```
R2(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
R2(config)#router rip
R2(config-router)#default-information originate
```

Route Anzeigen [Administrative Distanz / Anzahl Hops (Metrik)]

```
R3#show ip route
R    192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:22, Serial0/0/0
```

Anzeigen von Version, Update-Interval, Next Update, Sent, Recvd, Routing for Networks, Routing Sources

```
R3#show ip protocols
```

Routing Tabelle löschen R# clear ip route *

Debugging

```
R1#debug ip rip
R1#undebug all
R1#show ip rip database
```

Rip deaktivieren

```
R1(config)#no router rip
```

2.6 RIPv2 - Classless

2.6.1 Theorie

- Multicast Address: 224.0.0.10 bzw. ff02::9

2.6.2 Konfiguration

RIPv2 aktivieren

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R1(config-router)#default-information originate
```

- `no auto-summary`: Nicht an Klassengrenzen zusammenfassen beim verschicken von Updates

2.7 Routingtabelle interpretieren

- Lowest Administrative Distance gewinnt
- Level 1 Route: A level 1 route is a route with a subnet mask equal to or less than the classful mask of the network address.
- Level 2 Route: A level 2 route is a route that is a subnet of a classful network address.
- Routing Table Prinzipien
  - Asymmetric Routing: Anderer Weg zurück
  - Best Path and Metrics
  - Equal-cost-metric: Equal-cost load balancing
  - unequal-cost load balancing: EIGRP und IGRP
- Pfadbestimmung
  - Directly connected: Directly forwarded
  - Remote Network: Forwarding to next hop at exit interface
  - No route: ICMP Unreachable
- Route Types
  - Parent Route: 172.16.0.0/16 # Klassful
  - Child Route: 172.16.1.0/16 # Unterteilte Klasse

Routingverhalten Clasful

```
no ip classless
```

Routingverhalten Classless

```
ip classless
```

2.8 EIGRP

2.8.1 Theorie

- Feasible distance (FD) is the lowest calculated metric to reach the destination network.
- Feasible Successor: (FS) is a neighbor who has a loop-free backup path to the same net- work as the successor by satisfying the feasibility condition
- Metric Calculation: Bandbreite, Load, Delay, Reliability
  - Default Composite Formula: metric = [K1*bandwidth + K3*delay]
  - Complete Composite Formula: metric = [K1*bandwidth + (K2*bandwidth)/(256 – load)
    - K3*delay]* [K5/(reliability + K4)] (Not used if "K" values are 0)
    - K1 (bandwidth) = 1
    - K2 (load) = 0
    - K3 (delay) = 1
    - K4 (reliability) = 0
    - K5 (reliability) = 0
  - Router(config-router)#metric weights tos k1 k2 k3 k4 k5
- K-Values müssen auf allen Routern übereinstimmen
  - Delay (Additiv)
  - Bandwith (Bottlenek, kleinste Bandbreite)

Delay

Media	Delay (in us)
Fast Ethernet	100
Ethernet	1,000
T1 (Serial Default)	20,000
56K	20,000

Null0 Summary Route

- Route ins Nirvana

2.8.2 Konfiguration

EIGPR

```
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
```

- 1 = Prozess-ID (muss überall gleich sein)

Netzwerk hinzufügen (Achtung: Wildcard Subnet Mask!)

```
R1(config-router)# network 192.168.10.4 0.0.0.3
```

Wird keine Wildcard Maske angegeben, wird die Klasse genommen.

Routen werden in der Routingtabelle mit einem D für DUAL (Diffusing Update Algorithm) angezeigt (Algorithmus von EIGRP).

Nachbarn anzeigen

```
R# show ip eigrp neighbors
```

Topologie anzeigen

```
R2#show ip eigrp topology
R2#show ip eigrp topology 192.168.1.0 // Mehr Details zu diesem Netz
```

Manuell Summarisieren

```
R3(config)#interface serial0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

Default-Route verteilen

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R2(config)#router eigrp 1
R2(config-router)#redistribute static
```

2.9 OSPF

2.9.1 Theorie

- Multicast Adressen
  - 224.0.0.5 bzw. FF02::5 (AllSPFRouters: Router)
  - 224.0.0.6 bzw. FF02::6 (AllDRouters: Designated Router)
- Timer (müssen überall gleich sein)
  - Hello-Timer: 10 Sekunden
  - Dead-Timer: 40 Sekunden
- Topology DB: Wer gibt es und wer ist mit wem verbunden?
- Jede Area hat einen Designated Router am Rand zu anderen Areas
- Area 0 vermittelt zwischen verschiedenen Areas
- OSPF Packet Types
  - 1) Hello: Adjacency mit anderen OSPF Routern erstellen und beibehalten
  - 2) DBD (Database Description): Abgekürzte Liste der Link State Database senden. Wird zum überprüfen der lokalen Link State Database gebraucht.
  - 3) LSR (Link State Request): Mit LSRs werden mehr Infos der DBD angefragt.
  - 4) LSU (Link State Updates): Reply auf LSRs und neue Informationen ankündigen
  - 5) LSAck: Bestätigung wenn LSU enrhalten

- Jeder Router hat eine Router ID
  - 32 Bit Zahl dotted dezimal (wie eine IP-Adresse, hat aber gar nichts damit zutun!)
  - Router ID = `router-id` Command, höchste Loopback Addresse, kein Loopback: Höchste IP Adresse; sont 0.0.0.0
  - Bei IPv6 Only Router, muss ein Loopback Interface mit IPv4 konfiguriert werden
- Netzwerk Änderungen mittels Link State Advertisement (LSA) mitteilen
  - Default: Alle 30 Minuten; MaxAge 60 Min
- Auswahl Designated Router: Distribution Point von LSAs um Flooding zu vermeiden
  - Priorität im Hello (kann manuell 8 Bit Zahl gesetzt werden)
  - Falls Priorität gleich; Router ID zählt
- Bis zu 4 Routen mit gleichen Kosten können in der Routingtabelle sein
- Aus Topology Database (auf allen Routern gleich) wird die Routing-Tabelle berechnet
- Link State Packets für alle directly connected Networks generieren
  - Andere Router tragen das in der Topology Database ein und leiten es weiter
- Alle LSPs erhalten? –> Dijkstra berecnen
- Vorteil: Router findet schnell eine alternative Route, da er die gesamte Topologie kennt (innerhalb der eigenen Area)
  - Die Topology Database kann nicht summarisiert werden, da das vorenthalten von Informationen ist
  - Zwischen den Areas kann summarisiert werden
  - Maximal 50 Router pro Area, wegen der Rechenleistung und RAM des Routers

Eigenschaften für Neighbor Relationship

- Area ID muss übereinstimmen
- Hello- und Failure-Time Interval Timer müssen übereinstimmen
- OSPF Passwort muss übereinstimmen (optional)

Kosten

Interface Type	10^8 / bps	Cost
Fast Ethernet and faster	108/100,000,000 bps	1
Ethernet	108/10,000,000 bps	10
E1	108/2,048,000 bps	48
T1	108/1,544,000 bps	64
128 Kbps	108/128,000 bps	781
64 Kbps	108/64,000 bps	1562
56 Kbps	108/56,000 bps	1785

Router ID feststellen

1) Wert von `router-id`
2) Höchste IP-Adresse eines Loopback-Interfaces
3) Höchste IP-Adresse eines aktiven Interfaces

2.9.2 Konfiguration

OSPF aktivieren

```
R1(config)#router ospf 1
```

Netzwerk hinzufügen

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
```

OSPF-Nachrichten nicht Senden/Empfangen auf Interface

```
router ospf 1
passive-interface FastEthernet0/0
```

Router ID anzeigen

```
R3#show ip protocols
R3#show ip ospf
R3#show ip ospf interface
```

Router ID konfigurieren

```
R1(config)#interface loopback 0
R1(config-if)#ip address 10.1.1.1 255.255.255.255
```

Um Änderungen zu übernehmen, Router neustarten (`copy run start` nicht vergessen).

Oder Router ID so konfigurieren

```
R1(config-router)#router-id 10.4.4.4
```

OSPF Prozess neustarten

```
R1# clear ip ospf process
```

Nachbarn anzeigen

```
R1#show ip ospf neighbor
```

OSPF Bandbreite konfigurieren

```
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64 // In 1k
```

Kosten berechnen

```
10^8 / Bandbreite
```

OSPF Kosten konfigurieren

```
R3(config)#interface serial0/0/0
R3(config-if)#ip ospf cost 1562
```

Default Route verteilen

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback1
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

Referenzbandbreite ändern (Default: 1000) auf 10 Gbps

```
R1(config-router)#auto-cost reference-bandwidth 10000
```

Hallo- und Deaed-Interval ändern (Muss auf allen Routern gleich sein!)

```
R1(config)#interface serial0/0/0
R1(config-if)#ip ospf hello-interval 5
R1(config-if)#ip ospf dead-interval 20
```

Priorität ändern zum Bestimmen des DR und BDR

```
R1(config)#interface fastEthernet0/0
R1(config-if)#ip ospf priority 255
```

2.10 Cisco Discovery Protocol (CDP)

- Geräte senden periodisch alle 60 Sekunden ein CDP advertisement
- L3 Neighbors: Router
- L2 Neighbors: Router, Switches
- Informationen
  - Neighbor device ID

  - Local interface
  - Holdtime value, in seconds
  - Neighbor device capability code
  - Neighbor hardware platform
  - Neighbor remote port ID

Neighbors anzeigen

```
R3# show cdp neighbors
R3# show cdp neighbors detail
```

Aus sicherheitsgründen deaktivierbar

```
Router(config)# no cdp run # Global
Router(config-if)# no cdp enable # Interface
```

3 CCNA 3: LAN Switching and Wireless

3.1 Grundlagen Switchkonfiguration

3.1.1 Theorie

Forwarding Modes

- Fast Forward: Nach 6 Bytes (nach DA)
- Fragment Free: Mindestens 64 Bytes wegen der Minimallänge eines Frames
- Store-and-Forward: Komplett speichern und dann weiterleiten; mit CRC
- Asymmetrisches Switching: Verschiedene Bandbreiten pro Switchport

3.1.2 Konfiguration

Privileged Exec Mode

```
Router>enable
```

IOS Version anzeigen

```
Switch#show version
```

Konfigurationsmodus

```
S1#configure terminal
```

Hostnamen setzen

```
Router(config)#hostname Router1
```

DNS-Lookup verhindern

```
Switch#no ip domain-lookup
```

Privileged Exec Mode verschlüsseltes Passwort setzen

```
S1(config)#enable secret class
```

Konsolenpasswort setzen

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
```

Telnet Passwort setzen

```
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

SSH aktivieren

```
S1(config)# ip domain-name foobar.net
S1(config)# crypto key generate rsa
S1(config)# ip ssh version 2
S1(config)# line vty 0 15
S1(config)# transport input SSH
```

SSH RSA Key löschen und SSH-Service stoppen

```
S1(config)#crypto key zeroize rsa
```

Passwort wiederherstellen

- MODE Button drücken und Gerät einschalten
- Warten bis SYST LED nicht mehr blinkt

  switch:flash_init switch:load_helper switch:dir flash: switch:rename flash:config.text flash:config.old boot ... Switch#copy flash:config.text system:running-config ALSwitch#configure terminal ALSwitch(config)#no enable secret

Interface konfigurieren

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

Default Gateway setzen

```
S1(config)#ip default-gateway 172.17.99.1
```

Speed und Duplex-Settings

```
S1(config-if)#speed 100
S1(config-if)#duplex full
```

Mehrere Interfaces konfigurieren

```
S(config)# interface range fastethernet 0/1 - 12
S(config)# interface range fastethernet 0/1 , fastethernet 0/13
```

Konfiguration anzeigen

```
Switch#show running-config
Switch#show startup-config
```

IOS Software vom Server auf Switch laden (Auf server Image `c2960-lanbase-mz.122-25.FX.bin` bereitstellen)

```
ALSwitch#copy tftp flash
```

IOS Software von TFTP Server herunterladen

```
S1#copy tftp flash
```

Konfiguration auf TFTP Server speichern

```
LSwitch#copy running-config startup-config
AlSwitch#copy startup-config tftp
```

Konfiguration von TFTP Server herunterladen

```
Switch#copy tftp startup-config
```

Konfiguration löschen

```
Switch#erase startup-config
```

Switch neustarten

```
Switch(config)#reload
```

Interfacekonfiguration anzeigen

```
Switch#show interface vlan1
Switch#show ip interface vlan1
```

3.1.3 Debugging

```
ALSwitch#ping 172.17.99.21
```

3.1.4 MAC-Adresstabelle

MAC-Adresstabelle anzeigen

```
S1#show mac address-table
S1#show mac address-table address dynamic
S1#show mac address-table address <PC1 MAC here>
```

MAC-Adresstabelle leeren

```
S1#clear mac address-table dynamic
```

MAC-Adresse statisch in MAC-Adresstabelle hinzufügen

```
S1(config)#mac-address-table static 00e0.2917.1884 vlan 99 interface fastethernet 0/18
```

Statische eingetragene MAC-Adresse aus MAC-Adresstabelle löschen

```
S1(config)#no mac-address-table static 00e0.2917.1884 vlan 99 interface fastethernet 0/18
```

VLAN Informationen anzeigen

```
Switch#show vlan
```

Flash Inhalt anzeigen

```
Switch#dir flash:
Switch#show flash
```

Konfiguration speichern

```
S(config)# switchport mode access
```

History

```
terminal history
terminal history size 50
terminal no history size
terminal no history
```

Show command

```
show interfaces [id]
show ip interface
show ip http
show ip arp
show mac-address-table
```

```
Switch#show interface status
```

Telent line vty 0 15 transport input telnet

SSH ip domain-name mydomain.com c ytbd

3.1.5 Port Security

Port Security defaults

```
switchport mode access ! Port muss im Access Mode sein
switchport port-security
switchport port-security maximum 50
switchport port-security mac-address sticky
```

Port Security einstellen

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation protect
S1(config-if)#switchport port-security violation shutdown
```

Port Security anzeigen

```
S1#show port-security
S1#show port-security interface FastEthernet 0/23
```

3.2 VLANS

3.2.1 Theorie

- Trunk: Mehrere VLANs werden übertragen
- 802.1Q: VLAN-Tag wird Ethernet-Frame hinzugefügt
- Statisch und dynamisches VLAN
  - Statisch: Port in ein VLAN
  - Dynamisch: 802.1x mit Authentifizierung an Radius-Server oder MAC-Adresse in einer Tabelle zuordnen
- Default VLAN: VLAN 1
- Native VLAN
  - Untagged Verkehr wird mit Native VLAN getagt
  - Tagged Verkehr vom Native VLAN wird enttagt
- Management VLAN

VLAN IDs

- Normal Range
  - 1-1005
  - 1002-1005 reserved for Token Ring and FDDI VLAN‘s
  - 1 and 1002 to 1005 are automatically created and cannot be removed.
  - Stored in the vlan.dat file in flash memory
- Extended Range
  - 1006-4094
  - Designed for service providers
  - Stored in the running-configuration file

Trunking Modes: Trunk Negotiation Combinations

Combination	Dynamic Auto	Dynamic Desireable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

3.2.2 VLANs

VLAN Datenbank löschen

```
Switch#delete flash:vlan.dat
```

Alle Interfaces deaktivieren

```
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
```

User Ports aktivieren (In Access Mode setzen)

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

VLANs konfigurieren

```
S1(config)#vlan 10
S1(config-vlan)#name Students
```

VLANs anzeigen

```
S1#show vlan
S1#show vlan brief
```

Ports zu einem VLAN hinzufügen (Existiert das VLAN nicht, wird es automatisch erzeugt!)

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 10
```

Schauen, welche Ports zu einem VLAN (10) gehören

```
S1#show vlan 10
S1#show vlan Students
```

Management VLAN mit IP-Adresse konfigurieren

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

Trunk konfigurieren

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

Trunks anzeigen

```
S1#show interface trunk
```

Assign Ports to a vlan

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport mode access // Ausgabe: ungetagt
Switch(config-if)#switchport access vlan vlan_number
```

Native VLAN

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
```

3.3 VLAN Trunking Protokoll VTP

3.3.1 Theorie

- Server sagt den Clients, welche VLANs existieren
- VTP Domain: Greäte mit gemeinsamer VLAN DB
- VTP Modes: Was kann der Switch?
  - Server: Hinzufügen, ändern, löscheb über vlan advertisements (default)
  - Client: Empfange
  - Transparent: Nur Weiterleiten
- VTP Modes
- VTP Advertisement
- VTP synchronisiert zu der neusten Revision Number
- VTP Pruning: Broadcast wird nur dorthin verschickt, wo es Clients hat. Clients hat es in den VLANs wo auf einem Port eine MAC-Adresse aktiv ist.
- Unbedingt VTP Domainnamen und Passwort konfigurieren, damit keine Unfälle passieren

3.3.2 Konfiguration

VTP Revision nummer zurücksetzen

```
Switch(config)#vtp mode transparent
```

VTP Server bestimmen (Schickt VLANs raus)

```
Switch(config)#vtp mode server
Switch(config)#vtp domain foobar
Switch(config)#vtp password barfoo
```

VTP Client bestimmen (trägt empfangene VLANs ein)

```
Switch(config)#vtp mode client
Switch(config)#vtp domain foobar
Switch(config)#vtp password barfoo
```

VTP-Advertisement nur weiterleiten und nicht eintragen

```
Switch(config)#vtp mode transparent
```

VTP Pruning aktivieren (nur auf Server aktivieren)

```
Switch(config)#vtp pruning
```

VTP Status anzeigen

```
Switch#show vtp status
Switch#show vtp counters
```

3.4 STP Spanning Tree Protocol

3.4.1 Theorie

- Loops können verhindert werden
- Legacy STP: IEEE 802.1D
- Root-Switch alle Ports im Forwarding
- Tiefste Bridge ID wird Root-Bridge
- Root-Port zeigen zur Root-Switch
- BPDU's (Bridge Protocol Data Unit) periodisch versendet
- Zuerst blocking Mode, nur BPDUs werden ausgetauscht
- Pro Segment nur 1 Designated Port: Tiefste Kosten; falls Kosten gleich: Bridge ID zählt auch mit
- RSTP: Schnellere Konvergenz
- Edge Ports: Endgerät

3.4.2 Konfiguration

STP Infos anzeigen

```
S1#show spanning-tree
```

STP debuggen

```
S1#debug spanning-tree events
```

Portfast (keine STP Devices hinter diesem Port; verbessert Konvergenzzeit)

```
S2(config)#interface fastEthernet 0/11
S2(config-if)#spanning-tree portfast
```

Maximaler Duchrmesser Access-Switch zu Access-Switch

```
S1(config)#spanning-tree vlan 1 root primary diameter 5
```

STP optimieren: Priorität setzen, da Bridge für jedes VLAN Root wird

```
S3(config)#spanning-tree vlan 99 priority 4096
```

S3 wird auf dem VLAN99 nicht Root-Bridge, da höhere ID als die andern.

Priorität einstellen: Fester Wert (default 32768)

```
S3(config)#spanning-tree vlan 20 priority 4096
```

Priorität einstellen: Wert für Root selber suchen und einstellen

```
spanning-tree vlan 1 root primary
```

Priorität einstellen: Wert für secondary Root selber suchen und einstellen

```
spanning-tree vlan 1 root secondary
```

RSTP-PVST Rapid Spanning Tree Protocol

```
S1(config)#spanning-tree mode rapid-pvst
```

Point-to-Point Links konfigurieren

```
S3(config)#interface FastEthernet 0/1
S3(config-if)#spanning-tree link-type point-to-point
```

3.5 Inter-VLAN Routing

3.5.1 Via Switch Virtual Interface (SVI)

Interface id = VLAN number

```
Switch(config)#ip routing
Switch(config)#interface vlan 120
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
Switch(config-if)#no shutdown
Via routed port
```

3.5.2 Via Routed Port

Turn a switchport into a routed port

```
Switch(config)#ip routing
Switch(config)#interface fastethernet 0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.10.10.1 255.255.255.0
Switch(config-if)#no shutdown
```

3.5.3 Via externer Router

Router on a Stick (Externer Router)

```
Router(config)#interface fastethernet 0/0
Router(config-if)#no ip address
```

Router: VLAN 1

```
Router(config)#interface fastethernet 0/0.1
Router(config-subif)#description Control Traffic VLAN1
Router(config-subif)#encapsulation dot1q 1 ! [native]
Router(config-subif)#ip address 10.10.1.1 255.255.255.0
```

Router: VLAN 10

```
Router(config)#interface fastethernet 0/0.10
Router(config-subif)#description Management VLAN 10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 10.10.10.1 255.255.255.0
```

Router: VLAN 20

```
Router(config)#interface fastethernet 0/0.20
Router(config-subif)#description Engineering VLAN 20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 10.10.20.1 255.255.255.0
```

Switch

```
Switch(config)#interface vlan 10
Switch(config-if)#description Management VLAN 10
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown

Switch(config)#interface fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 1
```

Überprüfen

```
Switch#show ip route
Switch#show ip interface interface
Switch#show ip interface brief
Switch#show interface status
```

3.6 Wireless LAN

- CSMA/CD nicht möglich wegen hidden Stations
  - Deshalb CSMA/CA (Verhindern statt bemerken)

4 CCNA 4: Accessing the WAN

4.1 PPP

4.1.1 Theorie

- Link Control Protocol (LCP): Im Data Link Layer: Herstellen, konfigurieren und Testen der Verbindung
- Network Control Protocols (NCP)
- Loadbalancing mittels Multilink Verbindungen
- Authentication: Checks if the caller has the permission for a connection
- Compression: Increases the effective throughput on PPP connection
- Error detection: Fault condition can be identified
- Callback: Calls the client back based on routers configuration statement

4.1.2 Konfiguration

Debugging

```
R1#debug ppp negotiation
PPP protocol negotiation debugging is on
R1#debug ppp packet
```

PPP auf einem Interface aktivieren

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
```

PPP Authentication PAP

```
R1(config)#username R1 password cisco
R1(config)#int Serial0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R2 password cisco

R2(config)#username R2 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R1 password cisco
```

PPP Authentication CHAP

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
```

```
R3(config)#username R2 password cisco
R3(config)#int Serial/0/1
R3(config-if)#ppp authentication chap
```

Komprimierung aktivieren (auf beiden Seiten)

```
Router(config-if)#compress predictor
! oder
Router(config-if)#compress stac
```

Zurück zu HDLC

```
Router(config-if)#encapsulation hdlc
```

4.2 Frame Relay

4.2.1 Theorie

- Default-Encapsulation Type: Cisco; Alternativ IETF für Nicht-Cisco Geräte
- LMI: Logical Management Interface
  - Keepalive-Mechanismus welcher Statusinformationen über die Frame Relay Verbindungen zwischen Router (DTE) und Frame Relay Switch (DCE) austauscht
  - Types: Cisco, ANSI oder q933a
- Virtual Circuit (VC)
  - VCIs sind durch DLCI identifizieret
  - Switched VC (SVC): Dynamische Verbindung: Aufbau, übertragung und wieder schliessen.
  - Permanent VC (PVC): Für konstanten Datentransfer
- Default physikalisches Netzwerk: Nonbroadcast multi-access (NBMA)
- Congestion Notification Mechanism
  - BECN: Backward Explicit Congestion Notification: Frame Relay Switch warnt die upstream Devices über eine Queue
  - FECN: Forward Explicit Congestion Notification: Frame Relay Switch warnt die downstream Devices über eine Queue

4.2.2 Frame Relay Switch

Switch als Frame Relay Switch und zwei PVC zwischen R1 und R2 definieren

```
FR-Switch(config)#frame-relay switching
```

Encapsulation Type auf Frame Relay setzen

```
FR-Switch(config)#interface serial 0/0/0
FR-Switch(config-if)#clock rate 64000
FR-Switch(config-if)#encapsulation frame-relay
```

Oder anderer Frame Relay Type:

```
FR-Switch(config-if)#encapsulation frame-relay ietf
```

Interface Typ auf DCE setzen

```
FR-Switch(config-if)#frame-relay intf-type dce
```

Traffic routen (PVC erstellen)

```
FR-Switch(config-if)#frame-relay route 102 interface serial 0/0/1 201
FR-Switch(config-if)#no shutdown
```

Konfiguration überprüfen

```
FR-Switch#show frame-relay pvc
FR-Switch#show frame-relay route
```

Selbiges für anderes Interface

```
FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config)#clock rate 64000
FR-Switch(config-if)#encapsulation frame-relay
FR-Switch(config-if)#frame-relay intf-type dce
FR-Switch(config-if)#frame-relay route 201 interface serial 0/0/0 102
FR-Switch(config-if)#no shutdown
```

4.2.3 Router R1 für Frame Relay konfigurieren

Konfigurieren

```
R1(config)#interface serial 0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay inverse-arp

R1(config-if)#frame-relay map ip 10.1.1.2 102 broadcast

R1(config-if)#frame-relay map ip 10.1.1.1 102

R1(config-if)#no shutdown
```

Überprüfen

```
R1#show frame-relay map
```

Debugging

```
R1#debug frame-relay lmi
```

LMI Type ändern

```
R2(config)#interface serial 0/0/1
R2(config-if)#encapsulation frame-relay
R2(config-if)#frame-relay lmi-type ansi
! Zurück auf Cisco
R2(config-if)#frame-relay lmi-type cisco

R2#show frame-relay lmi

R2#debug frame-relay lmi
```

R2(config-if)#frame-relay lmi-type cisco

Frame Relay Subinterface

```
FR-Switch(config)#interface serial 0/0/0
FR-Switch(config-if)#frame-relay route 112 interface serial 0/0/1 212
FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config-if)#frame-relay route 212 interface serial 0/0/0 112

R1(config)#interface serial 0/0/1.112 point-to-point
R1(config-subif)#ip address 10.1.1.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 112
```

- Multipoint: Alle Router im selben Subnetz
- Point-to-Point: Jedes Router-Paar hat sein eigenes Subnetz

4.3 Network Security

4.3.1 User management

Neuen User anlegen

```
R1(config)#username ccna password ciscoccna
```

AAA global aktivieren (authentication, authorization, and accounting) aktivieren)

```
R1(config)#aaa new-model
```

Login per Console erlauben

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

4.3.2 RIP Routing Update Propagation und RIP Authentication

Routen nur auf bestimmten Interfaces propagieren

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

Routen nur von authorisierten Routern akzeptieren (auf allen ausführen)

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco

R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

4.3.3 EIGRP Authentication

```
R1(config)# key chain EIGRP-KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco

R1(config)# interface s0/0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEY
```

4.3.4 OSPF Authentication

- Null Authentication: Type 0: No Authentication (Default)
- Plain Text Authentication: Type 1: Clear-Text
- MD5 Authentication: Type 2: MD5

Routen nur auf bestimmten Interfaces propagieren

```
R1(config)#router ospf
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

Routen nur von authorisierten Routern akzeptieren (auf allen ausführen)

```
R1(config-if)# ip ospf message-digest-key 1 md5 cisco
R1(config-if)# ip ospf authentication message-digest

R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
```

4.3.5 SNMP logging

SNMP Messages an 192.168.10.10 schicken

```
R1(config)#logging 192.168.10.10
```

Level setzen, folgende Typen sind möglich: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, `debugging`.

```
R1(config)#logging trap warnings
```

4.3.6 Hardening

Unbenötigte globale Services ausschalten

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

Unbenötigte Interface Services ausschalten

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachables
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

Router mit AutoSecure absichern

```
R3#auto secure
```

4.4 Access Control Lists (ACL)

4.4.1 Theorie

- Gibt es keinen Match in der ACL, wird das Paket verworfen ("implicit deny any")
- Pro Interface kann pro Richtung (`in`/`out`) nur eine ACL angewendet werden

Typen

- Standard ACL
  - Prüft nur source IP
- Extended ACL

  - Prüft auf destination IP, source und destination TCP/UDP Port, Protokoll-Typ (IP, ICMP, UDP, TCP, oder Protocol Nummer)

Numbering und Naming ACLs

- Numbered ACL
  - 1-99 und 1300-1999: Standard ACL
  - 100-199 und 2000-2699: Extended ACL
  - Einträge können nicht hinzugefügt oder gelöscht werden
- Named ACL
  - Name kann hinzugefügt werden (Grossbuchstaben empfohlen)
  - Einträge können geändert/gelöscht werden
  - ACL kann standard oder extended sein

ACLs positionieren

- Standard ACL: So nahe an der Destination wie möglich
- Extended ACL: So nahe an der Quelle wie möglich

Wildcard Maske

- Bitmaske, welche zeigt, welche Stellen einer IP-Adresse berücksichtigt werden müssen
- Bit mit `0` wird berücksichtigt
- Host-Bitmaske: `0.0.0.0` (Alle Bits müssen matchen)
- Any-Bitmaske: `255.255.255.255` (Adresse kann irgendwas sein)

4.4.2 Standard ACLs konfigurieren

Standard ACL erstellen (Nur Traffic von `192.168.30.0/24` erlauben)

```
R1(config)# access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
R1(config)# access-list 102 deny ip any any
R1(config)# access-list 102 remark Kommentar von mir
```

Standard ACL entfernen

```
R1(config)# no access-list 102
```

Standard ACL auf einem Interface aktivieren

```
R1(config)# interface FastEthernet 0/0
R1(config-if)# ip access-group 1 out

R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
```

Telnet Access mit Named ACLs einschränken

```
R2(config)#ip access-list standard TELNET
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255

R2(config)#line vty 0 4
R2(config-line)#access-class TELNET in
R1(config-line)# login
R1(config-line)# password secret
R2(config-line)#end
```

Standard Named ACL erstellen

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
```

```
R1(config-std-nacl)# permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)# interface Fa0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Standard Named ACL auf einem Interface deaktivieren

```
R3(config-if)#no ip access-group STND-1 in
```

4.4.3 Extended ACLs konfigurieren

Extended Numbered ACL Syntax

```
Router(config)# access-list access-list-number {deny | permit | remark} protocol source
source-wildcard [operator operand] [port port-number or name] destination
destination-wildcard [operator operand] [port port-number or name] [established]
```

Extended Numbered ACL erstellen (192.168.30.0/24 darf auf Port 80 in jedes Netz verbinden)

```
Router(config)# access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
Router(config)# access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
```

Extended Numbered ACL auf einem Interface aktivieren

```
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 104 in
```

Extended Named ACL erstellen

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

```
R1(config)#ip access-list extended EXTEND-1
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
R1(config-ext-nacl)#permit ip any any
```

Extended Named ACL anwenden (Möglichst nahe an der Source)

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out
R1(config-if)#end
```

4.4.4 Debugging

```
R1# show access-lists 101
R1# show access-lists NO_FTP
R1# show ip interface
```

4.4.5 Beispiele Aufgaben

```
access-list 90 permit 192.168.1.0 0.0.0.0.255
access-list 90 deny any
interface fa0/0
ip access-group 90 out
```

```
ip access-list extended 101
deny ip 192.168.1.0 0.0.0.255 10.0.10.100 0.0.0.0
permit ip 192.168.2.0 0.0.0.255 any
```

```
ip access-list 144 tcp 172.16.25.0 0.0.0.255 host 172.16.30.100 eq ssh
ip access-list extendes ssh
permit tcp 172.16.20.0 0.0.0.127 host 172.16.30.100 eq 22

ip access-list standard 95
permit 192.168.18.0 0.0.0.254

ip access-list extended foo
permit tcp host 192.168.1.3 host 172.16.1.23 eq 80
deny tcp any host 172.16.1.23 eq 80
permit ip any any
```

4.4.6 Typische Prüfungsaufgabe

Host 192.168.33.3 darf HTTP auf Host 172.22.242.23 machen, sonst niemand.

```
R(config)# access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
R(config)# access-list 100 deny tcp 192.168.33.0 0.0.0.255 host 172.22.242.23 eq 80
R(config)# access-list 100 permit ip any any

R(config-if)# interface fa0/1
R(config-if)# ip access-group 100 out
```

4.5 DHCP und NAT Konfiguration

4.5.1 DHCP

Theorie

- Bei einem Adresskonflikt wird die IP-Adresse aus dem DHCP-Pool entfernt und ein Admin muss sich um den Konflikt kümmern

DHCP Server

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
R2(config)#ip dhcp pool R1Fa0
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
R2(dhcp-config)#domain-name foo.lan
```

DHCP Relay Agent

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
```

Debugging

```
R1#show ip dhcp binding
R2#show ip dhcp pool
```

4.5.2 NAT Theorie

- Inside local: Host from inside network. Usually RFC 1918..
- Inside global: Public address for the inside host.
- Outside global: A reachable IP address assigned to a host on the Internet.
- Outside local: The local IP address assigned to a host on the outside network.

- Dynamic NAT: Uses a pool of public addresses and assigns them on a first-come, first-served basis.
- Static NAT: Uses a one-to-one mapping of local and global addresses, and these map pings remain constant (Webserver).

4.5.3 Statisches NAT

Statisches NAT

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Inside/Outside Interface definieren

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

4.5.4 PAT / Overloading mit einer Public Adresse

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
!--Defines which addresses are eligible to be translated
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
!--Identifies the outside interface Serial 0/1/0 as the inside global address to
!--be overloaded
R2(config)# interface serial 0/0/0
R2(config-if)# ip nat inside
!--Identifies interface Serial 0/0/0 as an inside NAT interface
R2(config-if)# interface serial s0/1/0
R2(config-if)# ip nat outside
```

4.5.5 Dynamisches NAT mit Adress Pool

Golbaler Adresspool definieren

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
```

Accesslist für die internen Adressen erstellen

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Adresspool verwenden

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

PAT / Overloading

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL overload
```

Inside/Outside Interface definieren

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

4.5.6 Debug

```
R2#show ip nat translations
R2#show ip nat statistics
```

```
R2#debug ip nat
```

NAT-Tabelle löschen

```
R2#clear ip nat translation *
```

4.5.7 NAT Overload

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

4.6 VPN

Warum ein VPN statt ein WAN-Link?

- Tiefere Kosten
- Erhöhte Security (bei Verschlüsselung)
- Besser skalierbar

5 References

Die Informationen stammen mehrheitlich aus folgenden Büchern (Reihe CCNA Exploration Companion Guide von Cisco Press):

Titel	Verlag	ISBN-13
Network Fundamentals	Cisco Press 2008	978-1-58713-208-7
Routing Protocols and Concepts	Cisco Press 2008	978-1-58713-206-3
LAN Switching and Wireless	Cisco Press 2008	978-1-58713-207-0
Accessing the WAN	Cisco Press 2008	978-1-58713-205-6