# Networking 2

## I.BA_NETW2.F25 — Spick

**Authors** Hannah, Ivo, Lukas
**Date** 16. Mar. 2026
**Pages** 16

# Inhaltsverzeichnis

# 1. Device Config

## 1.1. Switch Boot Sequence

1. Power-on self-test (POST) wird geladen und checkt Prozessor, DRAM und flash Filesystem
2. Boot Loader Software aus dem ROM wird geladen
3. Boot Loader initialisiert Prozessor Register welche das Physical RAM kontrollieren
4. Boot Loader initialisiert Flash File System
5. Boot Loader ladet das default IOS Betriebssystem ins Memory und übergibt die Rolle ans OS

- Switch versucht mit Information aus BOOT Environment Variable zu booten
  - Funktioniert das nicht, ladet und führt er das erste ausführbare File aus

BOOT environment Variable wird gesetzt mit: `boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin` Auslesen: `Show Boot`

## 1.2. Switch LEDs

| Name | Beschreibung |
|---|---|
| SYST | Bekommt Strom und funktioniert |
| RPS | Redundant Powersuppy Status |
| STAT | Port Status Mode ist aktiviert |
| DUPLEX | Port Duplex Mode ist aktiviert |
| SPEED | Port Speed Mode ist aktiviert |
| PoE | PoE Supportet |

## 1.3. Recover from System Crash

1. PC mit Konsolen Kabel verbinden.
2. Switch austecken
3. Switch einstecken, Mode Button drücken während System LED grün blinkt
4. Mode Button drücken bis SYST kurz orange wird und dann grün bleibt
5. Boot Loader Switch Prompt taucht auf dem PC auf
6. Vergessene Passwörter können recovered werden oder IOS neu installiert

## 1.4. Switch Management Interface konfigurieren

```
S1# configure terminal
S1(config)# interface vlan 99
S1(config-if)# ip address 172.17.99.11
255.255.255.0
S1(config-if)# ipv6 address
2001:db8:acad:99::1/64
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 172.17.99.1
S1(config-if)# end
S1# copy running-config startup-config
```

## 1.5. Switch Port konfigurieren

### 1.5.1. Duplex Konfiguration

**Full Duplex**: Beide Seiten können gleichzeitig senden und empfangen
**Half Duplex**: Performance Issues aufgrund von Collisions

Speed und Duplex können konfiguriert werden: default auto -> kann so belassen werden ausser man kennt das angeschlossene Gerät (Switch, Router, Server,etc)

```
S1(config)# interface FastEtherne 0/1
S1(config-if)# duplex full
S1(config-if)# speed 100
S1(config-if)# end
```

### 1.5.2. Auto MDIX

Dadurch ist es egal ob crossover oder straight-through Kabel Ohne Auto-MDIX

- straight-through für Servers, Workstations, Router
- crossover für Switches und Repeater

=> Funktioniert nur wenn speed und duplex auf auto

### 1.5.3. Network Access Layer Issues

Dabei gibt es zwei Parameter die anzeigen ob eine Verbindung `show interfaces` funktioniert:

- FastEthernet0/18 is up ⟶ Hardware layer, carrier detect signal wird received
- Line protocol is up ⟶ data link layer keepalives werden received
- Interface is up, line protocol is down ⟶ Problem (Hardware, Encapsulation Type mismatch, other end error disabled)
- Beide down ⟶ Kabel ist nicht angeschlossen
- Interface is administratively down ⟶ Shutdown Befehl

### 1.5.4. Errors

| Error Type | Description |
|---|---|
| Input Errors | Total Anzahl Errors in Data Frames die empfangen wurden (Runts, Giants, CRC) |
| Runts | Pakete die zu klein sind für das Medium (z.B. Ethernet Paket kleiner als 64 Bytes) |
| Giants | Pakete die zu groß sind für das Medium (z.B. Ethernet Paket größer als 1518 Bytes) |
| [CRC] | Kalkulierte Checksumme nicht gleich wie erhaltene Checksumme |
| Output Errors | Summe aller Fehler welche das Senden verhindern (Collisions, Late Collisions) |
| Collisions | Anzahl Kollisionen |
| Late Collisions | Anzahl Kollisionen nachdem bereits 512 Bits übertragen wurden |

## 1.6. Router Grundkonfiguration

```
Router# configure terminal
Reouter(config)# hostname R1
R1(config)# enable secret [secret]
R1(config)# line console 0
R1(config-line)# password [password]
R1(config-line)# logn
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password [password]
R1(config-line)# login [password]
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access
Only! $
R1# copy running-config startup-config
```

### 1.7. Router Interface

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1
255.255.255.0
R1(config-if)# ipv6 address
2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
```

Loopback interface:

```
R1(config)# interface loopback
R1(config-if)# ip address 192.168.10.1
255.255.255.0
```

## 2. Switching Concpts

### 2.1. Frame-Forwarding

Aufteilung in **Ingress** und **Egress**. Wird basierend auf **Ingress** und **Ziel-MAC** weitergeleitet.

**Prozess**

1. Speicher der Source-MAC und Ingress-Port oder Timeout-Resetten.
2. Weiterleiten an Egress (falls vorhanden) oder an alle Ports flooden (ekl. Ingress.)

**Vermeiden von Congestions**

- **Fast Port Speed**: Bis zu 100Gbps.
- **Fast Internal Switching**: Schnell interne Busse und shared Memory -> Perfomace
- **Large Frame Buffers**: Temporäres Speicher von Frames während Verarbeitung
- **High Port Density**: Mehr lokaler Traffic.

#### 2.1.1. Store and Forward

**Charakteristika**:

- **Error Checking:** Verwerfen von fehlerhaften Frames
- **Buffering:** Unterstützen von verschiedenen Geschwindigkeiten

#### 2.1.2. Cut Trough

Nach Erhalt von Source-MAC unmittelbare Weiterleitung.

**Charakteristika**

- Angemessen für Low-Latency-Anforderungen ($< 10\mu s$)
- Kein FCS-Check
- Kann zu Bandbreiten-Fehlern führen (Fehler werden propagiert)
- Keine Unterstützung von verschiedenen Geschwindigkeiten

#### 2.1.2.1. Fragment-Free

Sicherstellen, dass Frame min. 64 Byte gross -> vermeiden von Runts

### 2.2. Collision Domain

Switch reduziert Collision-Domain und Congestions (keine zwischen Switch und Client).

- $\leq 1$ Gerät in Half-Duplex -> Collision-Domain zwischen Switch und Client
- Moderne Geräte haben „auto negotiation“ für Duplex-Mode und Speed.

### 2.3. Broadcast-Domain

Layer 1 & 2 (Switches) erhöhen Broadcast-Domain. Nur Layer 3 bricht Broadcast-Domain

## 3. VLANs

### 3.1. Übersicht

- Logische Verbindungen mit anderen, ähnlichen Geräten
- Isolation auf Layer 2
- Segmentation von unterschiedlichen Geräten auf dem *selben* Switch
- Folgen
  - Broadcastst, multicasts und Unicasts sind isoliert
  - Jedes VLAN hat sein eigenes IP-Netz
  - Kleinere Broadcast-Domains

#### 3.1.1. Vorteile

**Kleinere Broadcast-Domain** Weniger Kollisionen

**Bessere Security** Nur geräte im selben VLAN können kommunizieren

**Bessere Effizienz** Geräte mit ähnlichen Anforderungen gruppieren

**Reduzierte Kosten** Ein switch kann mehrere VLANs beherbergen

**bessere Performance** Durch kleinere Broadcast-Domain weniger traffic

**Einfacheres Management** Ähnliche Geräte werden auch zugang zu ähnlicheren Netzwerk-Ressourcen brauchen

#### 3.1.2. Typen

**Native** Nur für trunk-links, alle Frames sind auf einem Trunk-Interface mit 802.1Q getaggt, ausser jene für das native-vlan

**Data** Normaler Datenverkehr, per default `1`

**Management** Zur Administration, kein Enduser-Traffic, für SSH, Telnet und andere Admin-Zwecke, typischerweise auf einem SVI konfiguriert

**Voice** Für VOIP mit QoS Prioritäten, delay < 150 ms, oft vlan `150`, separate Queue auf Switch

### 3.2. Multiswitch Umgebungen

#### 3.2.1. Trunk

- Point-to-Point link zwischen zwei Netzwerk-Geräten
- Mehr als ein VLAN „fliessen“ über solche Ports
- Notwendig für Switchübergreifende VLANs
- Per default werden alle VLANs übertragen
- Wenn ein VLAN ohne Tag auf einem Trunk-Port ankommt, so wird es dem Native-VLAN zugeordnet

#### 3.2.2. VLAN Tags

- Normales Ethernet-Frame hat keine VLAN-Info enthalten
- Neuer, 4 Byte-Header nach IEEE 802.1Q wird bei tagging hinzugefügt
- Wenn der Header hinzugefügt wird → neuberechnen der FCS (Checksum)
- Bestandteile des Headers

  **Type** 2-Byte; tag protocol; Hex-wert; `0x8100`

  **User Priority** 3-Bit, service level implementation

  **Canonical Format Identifier (CFI)** 1-bit, für token-ring frames auf Ethernet

  **VLAN-ID** 12-bit VLAN Identifier, bis zu `4096` VLANs

#### 3.2.3. VOIP Phones

- Es gibt Cisco-VOIP-Phones, welche über einen Link vom Phone zum Switch das Voice- und das Data-VLAN trunken können

- Diese geräte haben einen internen kleinen switch, welche zen Datenverkehr aufsplitten und den „normalen“ traffic an einen PC und den Voice-Traffic ans Phone weiterleiten
- Für einen Switch-port kann deshalb noch ein zusätzliches Voice-VLAN konfiguriert werden

## 3.3. Konfiguration

### 3.3.1. VLAN Ranges

**Normal range** von 1 bis 1005, wobei 1002 - 1005 für legacy technologien reserviert sind, wird im flash gespeichert

**Extended range** 1006 - 4096, in der running-config gespeichert, weniger features wie die normalen vlans

### 3.3.2. Config

```
!!! Vlan erstellen !!!
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
!!! port einem vlan zuweisen !!!
Switch(config)# interface fa0/6
Switch(config-if)# switchport mode access
Switch(config-if)# switchportswitchport access
vlan 20
!!! Voice VLAN konfigurieren !!!
Switch(config)# interface fa0/6
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
!!! Übersicht anzeigen !!!
S1# show vlan [ summary | brief ]
show interfaces fa0/18 switchport
!!! Ein VLAN entfernen !!!
Switch(config)# no vlan vlan-id
!!! Alle vlans löschen !!!
delete flash:vlan.dat
!!! Interface in Trunkmode setzen !!!
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan
10,20,30,99
!!! Trunk etnfernenEntfernen !!!
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
```

## 3.4. Dynamic Trunking Protocol (DTP)

- Properitäres Cisco-Protokoll
- Trunking mit nachbar-Switch automatisch verhandeln
- Per default aktiviert

### 3.4.1. Modes

```
 Switch(config-if)# switchport mode {  access |
dynamic {  auto | desirable } |  trunk }
```

**`access`** Permanent non-trunking

**`dynamic auto`** Kann sich zu trunk verwandeln, wenn nachbar auf `trunk` oder `desirable` steht

**`dynamic desirable`** Interface versucht aktiv, einen Trunklink aufzubauen, interface wird zu trunk, wenn nachbar auf `trunk`, `desirable` oder `dynamic auto` steht

**`trunk`** Interface ist in jedem Fall ein Trunk, verhandelt mit dem Nachbar, dass er auch trunk wird

| | **Dynamic Auto** | **Dynamic Desirable** | **Trunk** | **Access** |
|---|---|---|---|---|
| **Dynamic Auto** | Access | Trunk | Trunk | Access |
| **Dynamic Desirable** | Trunk | Trunk | Trunk | Access |
| **Trunk** | Trunk | Trunk | Trunk | Limited connectivity |
| **Access** | Access | Access | Limited connectivity | Access |

```
! DTP Disable Negotiation
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
! DTP Re-Enable
S1(config-if)# switchport mode dynamic auto
! DTP auf Interface anzeigen
show dtp interface fa0/1
```

# 4. Inter-VLAN Routing

Hosts in verschiedenen VLANs können nicht miteinander kommunizieren ohne einen Router oder Layer 3 Switch.

## 4.1. Legacy Inter-VLAN routing

Router mit mehreren Etherent Interfaces. Jedes Interface ist verbunden mit einem Switch Port in einem anderen VLAN. Nicht wirklich skalierbar und wird so nicht mehr implementiert.

## 4.2. Router-on-a-Stick Inter-VLAN Routing

Nur eine physisches Ethernet Interface wird benötigt. Ein Interface wird als 802.1Q trunk konfiguriert. Darauf können dann verschiedenen Subinterfaces konfiguriert werden.

- Das sind sogenannte Software Based Virtual Interfaces.
- Pro VLAN gibt es ein Subinterface mit einem eigenen Subnetz

Ablauf:

1. VLAN tagged traffic kommt im Router Interface an
2. Er wird zum passenden Subinterface weitergeleitet
3. Router determiniert exit Interface
4. Wenn das Interface ein 802.1q Subinterface ist, wird das Paket neu getaggt und gesendet

=> Router on-a-stick skaliert nicht bei mehr als 50 VLANs.

### 4.2.1. Konfiguration

```
R1(config)#interface G0/0/1.10
R1(config-subif)#Description Default Gateway for
VLAN 10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add 192.168.10.1
255.255.255.0
R1(config-subif)#exit
R1(config)#interface G0/0/1.20
R1(config-subif)#Description Default Gateway for
VLAN 20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip add 192.168.20.1
255.255.255.0
R1(config-subif)#exit
R1(config)#interface G0/0/1
R1(config-if)#Description Trunk link to S1
R1(config-if)#no shut
```

#### 4.2.2. Layer 3 Switch

Routing auf Layer 3 Switchen funktioniert mit switched virtual interfaces. ⟶ SVI werden auf die gleiche Art und Weise konfiguriert wie das Management Interface

Vorteile:
- Schneller als Router on a Stick
- Keine externen Links werden benötigt
- Etherchannel kann benutzt werden
- Niedrigere Latenz weil alles auf dem Switch gemacht werden kann

Konfiguration von SVI

```
interface vlan 2
```

Ablauf:
1. VLANs erstellen
2. SVI VLAN konfigurieren, die konfigurierte IP Adresse ist der Default Gateway
3. Access Ports konfigurieren
4. IP Routing anschalten `ip routing`

Wenn die VLANs erreichbar sein sollen von anderen Layer 3 Geräten muss ein routed port konfiguriert werden:
1. `no switchport` ⟶ Dadurch wird der Port zum routed Port
2. `ip routing` ⟶ Enabled Routing
3. Routing konfigurieren
4. Routing verifizieren mit `show ip route`
5. Konnektivität verifizieren mit `ping`

### 4.3. Common Issues

Missing VLAN:

```
show vlan [brief]
show interfaces switchport
ping
```

Switch Trunk Port Issues:

```
show interface trunk
show running-config
```

Switch Access Port Issues:

```
show interfaces switchport
show running-config interface
ipconfig
```

Router Configuration Issues:

```
show ip interface brief
show interfaces
```

## 5. STP-Concepts

- Spanning Tree Protocols verhindern Layer 2 Loops.
- Layer 2 Loop führt zu: MAC instability, Link saturation, hohe CPU Auslastung, Broadcast-Strom (Netz in s down)
- Alternative: Layer3 everywhere

### 5.1. Alorithmus

1. **Rootbridge Election**: Root-Bridge-Prio: 0 - 61440 (32768 Standard, tiefer = besser, 4096-Schritte), **Extended-Sys-Id:** VLAN-ID wird zur Prio addiert. In extremfall: tiefere MAC
2. **Root-Ports selektieren:** Root-Port ist Port mit tiefster Cost zur Rootbridge

| Link Speed | STP Cost | RSTP Cost |
|---|---|---|
| 10 Gbps | 2 | 2′000 |
| 1 Gbps | 4 | 20′000 |
| 100 Mbps | 19 | 200′000 |
| 10 Mbps | 100 | 2′000′000 |

   **Tiebreaker**:
   1. (R)STP-Cost
   2. BID (Bridge Priorität)
   3. Port Priorität (Konfigurierbar auf Switch)
   4. Port-Nummer
3. **Bestimmen von Designated Ports**
   - Jeder Port zu Endgerät = Designated
   - Jeder Port gegenüber Root-Port = Designated
   - Jeder Port-Zwischen 2 Switches bei dem Switch, mit der tieferen Root-Path-Cost
4. **Blocked-Ports**: Alle nicht Root- und Designated-Ports sind blocked or alternate Ports

Die gesmate Kommunikation läuft über Bridge-Protocol-Data-Units (BPDU, enthalten Root-Cost, BID usw.). Werden alle 2s versendet.

Spanning-Trees können auch per VLAN gemacht werden (PVST).

### 5.2. Unterschiedliche Versionen

- **PVST+**: Proprietäres per VLAN Impl. von 802.1w inkl. loadsharing
- **RSTP**: Cisco Impl. von 802.1D
- **MSTP**: Fast converging verbesserung von 802.1D
- **MST**: IEEE Standard, reduziert STP Instanzen.

Laut IEEE ist RSTP Standard. Cisco nutzt standardmässig PVST+.

**Unterschied RSTP und STP**

| State | | Port | |
|---|---|---|---|
| STP | RSTP | RSTP | STP |
| Disabled | Discarding | Root P | Root P |
| Blocking | | Designated P | Designated P |
| Listening | | Backup (to Hub) | Blocked |
| Learning | Learning | Alternate P | |
| Forwarding | Forwarding | | |

### 5.3. PortFast & BPDU-Guard

Mit STP kann es zu DHCP-Timouts kommen (Wartezeit bis STP durch).

**PortFast** Unmittelbare Transition von Blocking zu Forwarding-> Unmittelbares Forwarding (nur für Acces-Ports)

**BPDU-Guard** PortFast-Port darf nie ein BPDU erhalten -> Spanning-Tree Loop, BPDU-Guard setzt Port in err-state, wenn BPDU ankommt.

```
# Portfast globall für alle access-ports
S1(config)# spanning-tree portfast default
```

```
# auf Interface
S1(config-if)# spanning-tree portfast
# BPDU globall für alle access-ports
S1(config)# spanning-tree portfast bpduguard
default
# auf Interface
S1(config-if)# spanning-tree bpduguard enable
```

# 6. EtherChannel

- Für mehr Bandbreite oder Redundanz zwischen 2 Geräten verwendet
- STP blockiert redundante Links per default
- Ether-Channel erlaubt durch Link-Aggregation parallele verbindungen
- fault-tolerance, load sharing, increased bandwidth, and redundancy between switches, routers, and servers.

## 6.1. Operation

### 6.1.1. Vorteile

- Viele configs können direkt auf EtherChannel gemacht werden, anstatt auf den einzelnen Ports → Konsistenz
- LoadBalancing möglichkeiten auf MAC und IP Ebene
- Jeder EtherChannel wird als 1 Link betrachtet, existieren mehrere zwischen 2 Geräten, so greift STP wieder ein
- Das ausfallen eines EtherChannel links hat keiner weiteren folgen, abgesehen von weniger Bandbreite, die Netzwerk-Topologie ändert sich dadurch nicht

### 6.1.2. Einschränkungen

- Interface-Typen können innerhalb eines EtherChannels nicht gemicht werden, also nicht 1 FastEthernet und ein GigabitEthernet
- Bis zu 8 Ports pro EtherChannel
- Die beiden EtherChannel configs müssen auf den beteiligten Geräten identisch sein, wenn die eine Seite als Trunk konfiguriert ist, dann muss das die andere auch sein
- Jeder EtherChannel hat ein PortChannel interface, configs welche darauf gemacht werden haben einfluss auf alle Interfaces, welche teil davon sind

### 6.1.3. Auto Negotiation

- Automatisches aufbauen eines EtherChannels entweder über **Port Aggregation Protocol** (PAgP) oder **Link Aggregation Control Protocol** (LACP).

#### 6.1.3.1. PAgP

- Cisco Properitär
- Packages alle 30 Sec
- States sind

**`On`** Interface wird zu EtherChannel forciert, ohne Verwendung von PAgP

**`PAgP desirable`** Aktive Verhandlung des Interfaces, initiiert die EtherChannel bildung

**`PAgP auto`** Passive Verhandlung, antwort auf PAgP Packages, jedoch keine eigene Inittierung

| | On | Desirable | Auto |
|---|---|---|---|
| **On** | ✅ | 🚫 | 🚫 |
| **Desirable** | 🚫 | ✅ | ✅ |
| **Auto** | 🚫 | ✅ | 🚫 |

#### 6.1.3.2. LACP

- Offener standard (ursprünglich `IEEE 802.3ad`, neu `IEEE 802.1AX`)
- Gleiche benefits wie PAgP
- Erlaubt 8 aktive und 8 standby links (standby wird aktiv, wenn ein aktiver ausfällt)
- Folgende States

**`On`** Interface wird zu EtherChannel forciert, ohne LACP

**`LACP Active`** Aktive Verhandlung, initiiert EtherChannel bildung

**`LACP passive`** passiv, Antwrot auf LACP Packages, keine eigene inittierung

| | On | Active | Passive |
|---|---|---|---|
| **On** | ✅ | 🚫 | 🚫 |
| **Active** | 🚫 | ✅ | ✅ |
| **Passive** | 🚫 | ✅ | 🚫 |

## 6.2. Configureation

Anforderungen

**EC Support** Alle interfaces müssen EtherChannel unterstützen

**Speed + Duplex** Alle Interfaces, welche teil eines EC sind, müssen selben Speed und Duplex haben

**VLAN** Alle Interfaces im EC müssen dem selben VLAN angehören oder als Trunk konfiguriert sein

**VLAN Range** Wenn es sich um Trunk-Interfaces handelt, so müssen die allowed-vlans die selben sein bei beiden enden, sonst bildet sich kein EC

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan
1,2,20
```

## 6.3. Troubleshooting

Common issues

- Ports im PC nicht im selben VLAN, nicht beide Trunk, Trunk mit unterschiedlichen NativeVLANs
- Nur ein paar Ports welche teil des ECs sind haben Trunking konfiguriert → truk immer auf EC konfigurieren
- Allowed-VLANs sind unterschiedlich auf den beiden PortChannels
- DynamicConfig modes sind nicht kompatibel

```
! Port channel anzeigen
show interfaces port-channel 1
! EC übersicht
S1# show etherchannel summary
! Info über spezifischen PortChannel
S1# show etherchannel
! Interface config anzeigen
S1# show interfaces f0/1 etherchannel
```

# 7. DHCPv4

DHCPv4 (Dynamic Host Configuration Protocol) weist einem Interface dynamisch eine Netzwerkkonfiguration zu.

- Ein Cisco Router kann als DHCP Server konfiguriert werden.
- Ein Server leased Adressen zu Clients, diese sind dann für einen festgelegten Zeitpunkt gültig. Ist der Lease abgelaufen muss der Client erneut nachfragen
  - Dadurch kann verhindert werden das inaktive Clients Adressen blockieren

## 7.1. Ablauf

Bei einer neuen Adresse:

1. DHCP Discover C ⟶ S
2. DHCP Offer C ⟵ S
3. DHCP Request C ⟶ S
4. DHCP Acknowledgement C ⟵ S

Bei einem abgelaufenen Lease:

1. DHCP Request C ⟶ S
2. DHCP Acknowledgement C ⟵ S

## 7.2. Konfiguration

Bevor man den DHCP Server Konfiguriert kann man Adressen ausschliessen, in dem man die erste und die Letzte Adresse der excluded Range spezifiziert.

```
R1(config)# ip dhcp excluded-address
192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address
192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0
255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.4
R1(dhcp-config)# domain-name example.com
```

Zusätzliche Parameter sind:

```
lease {days [hours [ minutes]] | infinite}
netbios-name-server address [ address2…ad
```

## 7.3. Verifizieren

```
show running-config | section dhcp
show ip dhcp binding
show ip dhcp server statistics
```

## 7.4. Enable/Disable

Per default is DHCP enabled.

```
R1(config)# no service dhcp
R1(config)# service dhcp
```

Wenn man den DHCP Service restarted kann es temporär dazukommen das IP Adressen doppelt vergeben werden

## 7.5. DHCP Relay

Ein DHCP Relay wird dazu verwendet DNS Anfragen an den zuständigen Server in einem anderen Subnetz weiterzuleiten.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
```

Die IP Helper Adresse leitet auch die folgenden Dienste weiter:

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP server
- Port 68: DHCP/BOOTP client
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

## 7.6. Client Konfiguration

Um einen Router als DHCP Client zu konfigurieren:

```
R1(config)# interface g0/0/1
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown
```

# 8. SLAAC & DHCPv6

Jedes IPv6 fähige gerät generiert Link-Local Adresse beim Bootup. Die GUA Adresse wird über Router-Advertisment (RA) Nachrichten generiert.

**3 Arten:** SLAAC /SLAAC & statless DHCP/ statefull DHCP
**Verwendung** wird über Flags bestimmt:

- **A-Flag:** Sinalisiert benutzung von SLAAC
- **O-Flag:** Zusätzliche Verwendung von DHCP
- **M-Flag:** Signalisiert stateful DHCP

| | |
|---|---|
| A=1,O=0,M=0 | Slaac only |
| A=1,O=1,M=0 | Slaac & stateles DHCP |
| A=0,O=0,M=1 | stateful DHCP |

## 8.1. Stateless Address Autoconfiguration

SLAAC ermöglicht die statels generierung einer Global-Unique-Address. SLAAC nutzt dabei die Informationen von RA-Packages.
**Prozess:**

1. 64-bit Subnet info von RA (von router oder DHCP)
2. 64-bit Interface ID
   - **Random-Generated**: Zufällig nich von MAC-Abhängig -> ändert regelmässig
   - **EUI-64**: 48-bit MAC wird auf 64-bit ergänzt (`FF-FE` in Mitte) -> rückverfolgbar
   - **Stable privacy addresses**: Ändert pro Netzwerk. Meist Hash von verschiedenen Parameter. Nich überall gelich implementiert

Ein SLAAC Konfigurierter Router sendet alle 200s ein RA. Ebenfalls antwortet er auf RS Nachrichten mit RAs. RS (Router Solicitation) Nachrichten werden an `FF02::2` multicasted.

**Duplicate Address Detection (DAD)** Da die durch SLAAC generiert IPv6 nicht immer eindeutig ist, wird DAD verwendet.

- Host sendet ICMPv6 Neighbor Solicitation (NS) Nachricht mit dem letzten Teil seiner IP.
- Wenn er keine Antwort bekommt => i.O, ansonsten neu wird Adresse neu generiert.

=> DAD nicht wirklich notwendig da IPv6 sehr kollisionsresistent ist.

## 8.2. DHCPv6

Kommunikationsablauf wenn DHCP werdendet wird:

1. Host sendet RS message
2. Router antwortet mit RA
3. Host sendet DHCPv6 SOLICIT message (an alle DHCPv6 Server)
4. DHCPv6 antwortet mit ADVERTISE message (Unicast)
5. Antwort von Host zu DHCP (REQUEST / INFORMATION-REQUEST; Unicast)
6. DHCP sendet Reply (Unicast)

=> Client zu DHCP = UDP 547, DHCP zu Client = UDP 546

Bei Stateless wird „nur“ Zusatinformation beim DHCP angefragt.

## 8.3. Konfiguration

```
# IPv6 Enable
R1(config)# ipv6 unicast-routing
# O-Flag
R1(config-if)# ipv6 nd other-config-flag
# M-Flag
R1(config-if)# ipv6 nd managed-config-flag
# Stateless DHCP
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool POOL-NAME
R1(dhcp-config)# network NETWORK
R1(dhcp-config)# default-router ROUTER
R1(dhcp-config)# dns-server DNS
R1(dhcp-config)# (Statefull-Options here)
R1(config-if)# ipv6 dhcp server POOL-NAME
# DHCP Client
R1(config)# ipv6 unicast-routing
R1(config-if)# ipv6 enable
# Stateful DHCP Client
R1(config-if)# ipv6 address dhcp
# autoconfig heisst SLAAC
R1(config-if)# ipv6 address autoconfig/dhcp
# Relay Agent
R1(config-if)# ipv6 dhcp relay destiatnion IPV6
EGRESS-INT
# Verification Commands
R1# show ipv6 dhcp pool
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp interface
R1# show ipv6 dhcp pool
```

# 9. FHRP

- First Hop Redundancy Protocols
- Wenn ein Router, welcher für ein bestimmtes Netzwerk den Default-Gateway stellt ausfällt, ist dieses Netz isoliert
- FHRP ermöglicht, in diesen Fällen einen alternativen Default-Gateway zur Verfügung zu stellen, sofern es weitere Router in diesem Netzwerk gibt
- Es wird ein virtueller Router eingesetzt, welcher eine eigene Mac und IP hat, welcher dann jeweils von einem physischen Router zur Verfügung gestellt wird
- Wenn ein aktiver router ausfällt, dann wird ein standby router aktiv und übernimmt den Job des ehemaligen Haupt-Routers
- Virtueller Router „Floatet“ dann auf den anderen Router

## 9.1. Protokolle

**HSRP** Hot Standby Router Protocol
- Cisco Properitär
- Transparenter failover
- Wird verwendet, um aktiv- und Standby Device zu wählen

**HSRP IPv6** Gleich wie HSRP, einfach für IPv6
- Virtuelle MAC von der HSRP Gruppennummer
- virtuele IPv6 Link-Local Adresse
- Router Advertisements werden auf die Link-Local Adresse gechickt, um zu signalisieren, dass der Router noch aktiv ist

**VRRPv2** Virtual Router Redundancy Protocol (Version 2)
- Offenes Protokoll
- Verantwortungsverteilung für virtuelle Router in IPv4 LAN
- Ein „Master“, mehrere Backups, master wird geählt von allen

**VRRPv3** Ähnlich zu VRRPv2, einfach mit IPv6 Support, zudem bessere Skalierbarkeit

**GLBP** Gateway Load Balancing Protocol
- Cisco Properitär FHRP
- Wie HSRP und VRRP aber mit zusätzlicher Möglichkeit für LoadBalancing / Load Sharding über mehrere Router

**GLBPv6** GLBP mit IPv6 Support

**IRDP** ICMP Router Discovery Protocol
- RFC 1256, legacy
- Wurde von Hosts verwendet, um router zu finden, welche non-local IP netzwerke ihnen zugänglich machen

## 9.2. HSRP im Detail

- Rollen werden bei HSPR Election festgelegt
- Defaultmässig wird der Router mit der numerisch höchsten IPv4 adresse zum aktiven Router gewählt
- Beeinflussung davon über die Priorität möglich und Empfohlen
  - Standardmässig bei 100
  - Wenn Router selbe Prio haben, dann gewinnt der mit der höheren IP
  - Prios in Range von 0 bis 255
  - Kann mit `standby piority` auf einem Interface gesetzt werden
- Preemption
  - Wenn ein Router aktiv ist und ein anderer mit höherer Prio aktiv wird, so bleibt der Ursprungsrouter aktiv
  - Wenn in jedem Fall neu gewählt werden soll, sobald eine höhere Prio dazukommt, muss das mit `standby preempt` auf dem Interface aktiviert werden
  - `standby preempt` erlaubt dem entsprechenden Router, eine re-election zu forcieren
  - Eine Re-Election findet nur statt, wenn der Router eine höhere Prio hat, wenn er die gleiche prio, aber eine höhere IP hat, dann wird er auch durch preemtion nicht aktiv
  - Wenn Preemption disabled ist, dann wird der Router, welcher zuerst booted active, sofern während seines election-prozesses keine anderen Router mit höherer Prio online sind

### 9.2.1. HSRP States

**Initial** Durch config-change oder wenn das Interface zum ersten mal verfügbar wird

**Learn** router kennt die V-IP noch nicht und hat auch noch keine `hello` message vom aktiven router gesehen, er wartet vom Aktiven router zu hören

**Listen** Router kennt die virtuelle ip, hat aber noch nicht vom aktiven gehört und ist deshalb weder aktiv noch standby und wartet auf ein `hello`

**Speak** Router sendet periodische `hello`-Messages und partizipiert aktiv an der leader election

**Standby** Router ist kandidat, aktiv zu werden und sendet periodische `hello` requests

**Active** Router welcher die Election gewonnen hat

- Active und Standby Router senden alle 3 Sekunden ein `hello`-Packages auf die HSRP-Multicast-Adresse.
- Standby wird aktiv, wenn er innert 10 Sekunden keine `hello` vom Aktiven Router bekommt
- Kann beides konfiguriert werden
- hello-timer sollte nicht unter 1 Sec., hold timer nicht unter 4 Sec. sein → CPU-Last gering halten

# 10. Lan Security

## 10.1. Attacken

- DDoS
- Data Breach
- Malware

## 10.2. Netzwerk Security Devices

- VPN enabled Router
- NGFW (Next Generation Firewall)
  - Stateful Paket Inspection, Application Visibility, Intrusion Prevention System, URL Filtering, Advanced Malware Inspection
- Network Access Control (NAC)
  - Authentication, Authorization und Accounting. Z.B. Cisco Identity Services Engine

## 10.3. Endpoint Protection

- Endpoints: Laptops, Desktops, Servers, Mobilgeräte
  - Anfällig für Malware durch Email oder Webbrowsing
  - Typischerweise Antivirus Software, Host-based Firewalls und Host-based intrusion prevention System
  - Bester Schutz mit: **NAC, AMP, Email Security Appliance (ESA), Web Security Appliance (WSA)**

### 10.3.1. Email Security Appliance (ESA)

- Überwacht SMTP
- Wird updated mit Daten von Cisco Talos (Weltweite Datenbank von Threats) alle 3 bis 5 Minuten
- Funktionen
  - Bekannte Threats blockieren
  - Beseitigen von Malware
  - Emails mit Bad Links verwerfen
  - Zugriff auf infizierte Webseiten blockieren
  - Verschlüsseln von outgoing Emails

### 10.3.2. Cisco Web Security Appliance (WSA)

- Sichert und kontrolliert Web Traffic
- Verbindet Advanced Malware Protection, Application visibility und control, use policy controls und reporting
- Funktionen und Applikationen (chat, video und audio) können erlaubt, eingeschränkt oder geblockt werden
  - Zeit-, Bandbreite Limit
- URL Blacklisting, URL Filtering, Malware Scanning, URL Categorization, Web application filtering, encryption und decryption von Web Traffic

## 10.4. Access Control

- Local Authentication
  - Lokales Login und SSH (sicherer)
  - Problem: Nicht Skalierbar auf mehrere Geräte
- AAA (Authentication, Authorization, Accounting) → Framework für Access Control auf Netzwerk Geräten
  - Wer (Authentication) darf was (Authorization) und wie wird es geloggt (Accounting)

### 10.4.1. Authentication

- Local AAA
  - Username und Passwort werden auf Gerät gepsiecher
  - User authentifiziert sich am Gerät
  - Ideal für kleine Netzwerke
- Server-Based AAA
  - Zentraler AAA Server mit Usernamen und Passwörter für alle User
  - Protokolle: RADIUS (Remote Authentication Dial-In User Service), TACACS+ (Terminal Access Controller Access Control System)
  - Bei mehreren Usern und Switches ideal

### 10.4.2. Authorization

- Automatisch
- Attribute welcher der Sever nutzt um zu bestimmen ob ein User Zugriff auf bestimmte Komponenten hat

### 10.4.3. Accounting

- AAA Server speichert detailiertes Log (alle EXEC und Configuration Commands werden gespeichert)
- Log enthält username, datum und zeit + command

### 10.4.4. 802.1X

Port basiertes access control und Authentifizierungsprotokoll.

- Nichtautorisierte Workstations werden daran gehindert sich mit dem LAN zu verbinden

Rollen:

- Client (Supplicant)
- Switch (Authenticator), verbindet Client und Server
  - leitet Authentifizierungsinformationen weiter
  - blockiert access für nicht authentifizierte Geräte
- Authentication Server
  - Validiert Client Credentials und leitet Ergebnis an Switch weiter

## 10.5. Layer 2 Vulnerabilities

Wird Layer 2 kompromittiert sind alle nachfolgenden Layers ebenfalls kompromittiert.

### 10.5.1. Mac Address Table Attacks

- Mac Address Tabellen haben eine fixe Grösse → Ressourcen können ausgehen
- **Mac Address Flodding**: MAC Adressen Tabellen mit falschen Einträgen füllen
  - Konsequenz: Switch verschickt alle Frames durch sämtliche Ports, Angreifer kann so traffic abfangen
  - macof: Programm um sehr schnell Mac Address Flodding zu betreiben
  - Massnahme: Port Security

### 10.5.2. VLAN Attacks

- VLAN Hopping
  - Angreifer konfiguriert 801.1Q als unauthorised Trunk und kann so Traffic auf allen VLANS senden und empfangen ⟶ DTP Dynamic Trunking Protocol von Cisco wird ausgenutzt
- VLAN Double-Tagging
  - Einfügen von einem 802.1Q Tag in eine Frame das bereits ein 802.1Q Tag hat
    - Äusserer Tag ist das Native VLAN, innerer Tag das tatsächliche VLAN
    - Weil es das Native VLAN ist wird das Frame nicht retagged
    - Das erlaubt dem Angreifer Frames in ein VLAN zu senden zu dem er sonst kein Access gehabt hätte
- Massnahmen: Trunking on Access Ports deaktivieren, DTP deaktivieren, Native VLAN nur für Trunk Links benutzen

### 10.5.3. DHCP Attacks

- DHCP Starvation
  - Gobbler versucht sämtliche DHCP Adressen mit falschen MAC Adressen zu leasen
- DHCP Spoofing
  - Falscher DHCP Server welche falsche Konfigurationen verteilt

### 10.5.4. ARP Attacks

- Man-in-the-middle Attack: Angreifender sendet unsolicited ARP Reply mit Info das seine Mac Adresse zur IP des Default GW gehört
- Massnahme: Dynamic ARP Inspection

### 10.5.5. Address Spoofing

- IP Spoofing und MAC Spoofing sind schwer zu umgehen
- Massnahme: IP Source Guard

### 10.5.6. STP Attacks

- Manipulation vom STP in dem Root Bridge gespoofed wird und die Netzwerk Topologie geändert wird
- BPDU (Bridge Protocol Data Units) werden gesendet mit lower bridge priority um als Root Bridge gewählt zu werden
- Massnahme: BPDU Guard

### 10.5.7. CDP Reconnaissance

- Manipulation vom Cisco Discovery Protocol (Broadcasted IP, IOS Version, Platform, Capabilities und Native VLAN)
- Per Default enabled: Disable mit global `no cdp run` oder auf einem Port mit `no cdp enable`
- Dasselbe gilt für lldp

### 10.5.8. Abwehrtechniken

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)

⟶ Diese Techniken bringen nur etwas wenn der Zugriff auf das Switch Management sicher ist:

- sichere Protokolle verwenden (SSH, SFTP)
- eigenes Management Netzwerk und VLAN
- ACLs

# 11. Switch Security

- Unused Ports mit `S1(config-if)# shutdown` deaktivieren.

## 11.1. Switch-Port Security

Portsecurity limitiert die Anzahl der gültigen MACs pro Port. Erlaubte MACS können **statisch** konfiguriert oder **erlernt** werden. Wenn eine Regeln verletzt wird geht der Port in einen err-disabled state.

Wenn max. von MACs noch nicht erreicht, werden Adressen **automatisch erlernt**. Erlernte Adressen gehen nach Reboot verloren ausser der `sticky`-Mode is ein.

**Aging** Mit dem Aging werden gelernte MACs nach einer Zeit wieder entfernt.

**Modi**

**absolute** Löschen der MAC nach Ablauf der Zeit
**inactivity** Löschen der MAC nach spez. Inaktivität

**Port Disabled State** Wenn eine MAC eine Port anspricht und eine Regel bricht kommt der Port in err-disabled-state.

**shutdown (default)** Syslog-Msg, Security-Counter++, Port muss manuell enabled werden (`shutdown` und `no shutdown`)

**restrict** Syslog-Msg, Drop von Paketen von Unbekannten MAC, Security-Counter++
**protect** Drop von Paketen von Unbekannten MAC

Bei `restrict` und `protect` kommen die Ports wieder „online“ wenn neue Adressen erlernt werden können.

**Konfiguration** im Interface-Config-Mode

```
# Einschalten
switchport port-security
# Max Anzahl an MACs setzen
switchport port-secuirty maximum <value>
# statische MAC hinzufügen
switchport port-secuirty mac-adress <mac>
# MAC sticky erlenen
switchport port-secuirty mac-adress sticky
# Aging time
switchport port-secuirty aging time <time>
switchport port-secuirty aging type <mode>
# violation Mode
switchport port-security violation <mode>
# verify
show port-security <interface>
show port-security address
```

## 11.2. Vermeiden von VLAN Hopping

3 Arten für Vlan Hopping: DTP Spoofing, Rouge Switch, double tagging

**Schritte:**

- `swtichport mode access|trunk` explizit setzen
- unused ports disalbed und in leeres vlan
- Bei trunks `switchport nonegotiate` setzen
- Native VLAN setzen `switchport trunk native vlan ID`

## 11.3. Vermeiden von DHCP-Attacks

1. Portsecurity nuten.
2. DHCP snooping (ratelimits) einschalten, Erstellt ‚DHCP-Binding-Table‘ mit IP und MAC

```
S1(config)# ip dhcp snooping
# Trusted Ports markieren
S1(config-if) ip dhcp snooping trust
# Untrusted ports ratelimit pro s sezten
```

```
S1(config-if) ip dhcp snooping limit rate
# für VLans aktivieren
S1(config)# ip dhcp snooping vlan v,l,a,n,s
```

### 11.4. ARP-Attacken

ARP-Spoofing und ARP-Poisoning wird mittels DHCP-Spoofing **Dynamic ARP Inspection (DAI)** verhindert. → Keine Progpagieren von schädlichen ARP-Nachrichten. Es gibt folgende Modi:

**dst-mac** Überprüft dest MAC. in Ethernet Header mit Target MAC in ARP-Body.

**src-mac** Überprüft src. MAC in Ethernet Header mit sender MAC in ARP-Body

**ip** Überprüft ARP-Body auf ungültige IP (0.0.0.0, 255.255.255.255, multicasts)

```
S1(config)# ip arp inspection vlan <id>
# trusted Ports konfigurieren, z. B. Uplink
S1(config-if)# ip arp inspection trust
# Modi Komma-Separiert angeben
S1(config)# ip arp inspection validate <modi>
```

### 11.5. Spanning Tree Attacken

Auch ein Spanning-Tree kann angegriffen werden, indem z.B. die Root-Bridge gespooft wird.

**Lösung**: Port-Fast und BPDU-Guard (siehe Abschnitt 5.3).

## 12. WLAN Concepts

### 12.1. Wireless Typen

**WPAN** Wireless personal-Area Network
- 6 - 9 Meter
- Bluetooth und Zigbee
- IEEE 802.15, 2.4 GHz Frequenz

**WLAN** Wireless LAN
- Heimanwendung, Office, Campus
- IEEE 802.11
- 2.4 GHz oder 5 GHz Band

**WMAN** Wireless Metropolitian Area Network
- Grosse geographische Region
- Kabellose Verbindungen für Stadt-teile
- Speziell lizenzierte Frequenzbänder

**WWAN** Wireless Wide-Area Networks
- Abdeckung einer grösseren Geografischen Region
- Globale Kommunikationsnetze
- Speziell lizenzierte Frequenzbänder

### 12.2. Wireless Technologien

**Bluetooth**
- IEEE 802.15
- WPAN Standard, range bis zu 100m

**BLE** Bluetooth Low Energy, meshing und grössere Netzwerktopologien

**BR/EDR** Bluetooth Basic Rate / Enhanced Rate, point-to-point topologie für Audio Streaming

**WiMAX** Wolrdwide Interoperability for Microwave Access
- Alternative zum Kabelgestützten Breitbandinternet
- Wird vor allem dort eingesetze, wo es noch kein Kabelanschluss gibt
- IEEE 802.16
- Bis zu 50 Km range

**Cellular Broadband**
- Voice- und Datenverkehr
- Global System of Mobile (GSM) als intenrnational annerkannter Standard
- Code Division Multiple Access (CDMA) als Standard, welcher vor Allem in den USA verwendet wird
- Abdeckung von ca. 120 Grad pro Antenne

**Satellite Broadband**
- Geostationäre Sateliten mit direktem Alignment
- In Gegenden verwendet, wo es keine Kabelanbindung gibt

### 12.3. 802.11 Standards

| IEEE Standard | Radio Freq. (GHz) | Description |
|---|---|---|
| 802.11 | 2.4 | Bis zu 2 Mb/s |
| 802.11a | 5 | Bis zu 54 Mb/s, nicht kompatibel mit 802.11b / 802.11g, vor Allem in USA |
| 802.11b | 2.4 | Bis zu 11 Mb/s, grössere Rechweite als 802.11a, bessere eindringtiefe |
| 802.11g | 2.4 | bis zu 54 Mb/s, Rückwärtzkompatibel zu 802.11b, gute Akzeptanz in EU |
| 802.11n | 2.4 / 5 | 150 - 600 Mb/s, Mehrere Antennen mit MIMO notwendig |
| 802.11ac | 5 | 450 Mb / s - 1.3 Gb/s, bis zu 8 Antennen, lange ausreichend |
| 802.11ax | 2.4 / 5 | High-Efficiency Wireless (HEW), 1 GHz und 7 GHz, aktueller Standard |

WiFi -> Weltweites Konsortium welches nicht standartisierte Releases raus brachte.

### 12.4. Standardisierungsorganisationen

**ITU** International Telecomunication Union: Allokation von Frequenzbändern und Satelitenbahnen

**IEEE** Herausgabe von Standards für LAN, MAN, WAN in der 802 Familie

**WiFi Alliance** Non-Profit, industriehandelsorganisation um Einsatz von Kabelloser Kommunikation zu fördern, Zertifizierung von Geräten welche nach 802.11 funktionieren

### 12.5. AP Kategorien

**Autonomous** Standalone, eigenständige Konfiguration, verhält sich unabhängig, manuelle Verwaltung

**Controller Based** aka Lightweight APs (LAPs), Lightweight Access Point Protocol (LWAPP) zur Kommunikation mit LWAN controller (LWC). Zentrale konifguration durch LWC.

### 12.6. Antennentypen

**Omnidirectional** 360 Grad Abdeckung, in House oder Office

**Directional** Gerichtetes Signal, Parabolic-Dish

**MIMO** Multiple Input, Multiple Output, bis zu 8 Antennen, höhere Bandbreite

## 12.7. Wireless Topologien

**Ad hoc mode** Zwei Clients verbinden sich Peer-to-Peer ohne teilnahme eines Access-Points

**Infrastructure mode** Clients sind über einen Access-Point kabellos mit dem Netzwerk verbunden

- **BSS** Basic Service Set, verbindet alle Clients, Layer 2 MAC des APs wird für die Identifikation eines BSS über die BSSID verwendet
- **ESS** Extended Service Set, zwei oder mehr BSS, wessen Clients miteinander kommunizeren können, zusammengeschlossen über ein ESS, voraussetzung für fehlerfreies roaming von Wireless-Clients

**Tethering** Persönlicher Hostpot eines Mobilgeräts

## 12.8. 802.11 Frame-Struktur

Ähnlich des Ethernet-Frame-Formates, hat aber mehr Felder

**Frame Control** Typ des Wireless=Frames

**Duration** Verbleibende Zeit, die benötigt wird, um das empfangen des nächsten Frames abzuschliessen

**Address 1** Receiver Address
- Bei Client: MAC des APs
- Bei AP: MAC des Absenders

**Address 2** Transmitter Address
- Bei Client: MAC des Absenders
- Bei AP: MAC des APs

**Address 3** SD/DA/BSSID, Ziel MAC, Wireless oder Kabelgebunden

**Sequence Control** Sequenzkontrolle und Frame-Fragmentierung

**Address 4** Fehlt normalerweise, nur im Ad-hoc-Mode

**Payload** Daten

**FCS** Layer2 Checksumme

## 12.9. CSMA/CA

- WLAN ist halb-duplex, client kann nicht hören währenddem er sendet
- Kollisionen nicht feststellbar
- Es wird CSMA/CA (Carrier Sense multiple access with collision avoidance)

Folgender Ablauf beim Client zum senden:

1. Auf kanal hören und feststellen, ob frei
2. Senden der RTS (ready to send)-Nachricht, Fragt um exklusiven Kanalzugang
3. Empfangen des CTS (Clear to Send) vom AP (Sendeerlaubniss)
   - Wenn keine CTS gekommen ist → Zufällige Zeit warten und nochmal von vorne
4. Daten übertragen
5. Acknowledgen aller übertragungen, wenn kein Ack' kommt geht client von Kollision aus und beginnt wieder von Vorne

## 12.10. Passive und Active Discovery

**Passive** AP broadcastet seine SSID inkl. Stnadards und Security-Settings periodisch

**Active** Clients müssen SSID kennen, um Verbindung aufzubauen

## 12.11. CAPWAP

- IEEE Standard
- Möglichkeit, dass ein Wireless Controller (WLC) mehrere APs aund WLANs verwaltet
- Basiert auf LWAPP, hat aber noch einen Security-Layer, welcher WLAN-Clienttraffic zwischen AP und WLC Tunneled DTLS (UDP, port 5246 / 5274)
- Split-MAC-Architektur führt zum aufteilen von MAC Funktionen auf AP und WLC
  - **AP** Beacons, Probe Responses, Packet Acknowledgment, Retransmission, Frame Queueing and Prioritization, MAC-layer encryption / decryption
  - **WLC** Authentication, (Re-)Association von Roaming-Clients, Frame-Translation in andere protokolle, Terminierung von 802.11 Verkehr auf einem Kabelgebundene Interface
- DTLS ist Enryption zwischen AP und WLC, zwei tunnels, ein mal für Daten (not enabled by default, braucht Lizenz) und Control (encrypted by default)

## 12.12. Wireless Channels

- Wenn zu viele Clients auf einem Kanal unterwegs sind, nimmt die Leistung ab
- Es gibt techniken, um Die Kanäle besser nutzne zu können

**DSSS** Direct-Sequence Spread Spectrum, signal wird über ein breiteres Frequenzband verteilt, von 802.11b verwendet, um Inteferenzen zu vermeiden

**FHSS** Frequency-Hopping Spead Spectrum, schnelles wechseln der Kanäle, Sender und Empfänger müssen synchronisiert sein und wissen, auf welchen Kanal als nächstes gesprungen wird, bei ursprünglichem 802.11 Standard verwendet

**OFDM** Orthogonal Frequency-Division Multiplexing, ein channel nutzt mehrere sub-channels, wird von mehreren Standards wie z. B. 802.11a/g/n/ac verwendet, 802.11ax verwendet variation davon (OFDMA) mit mutliaccess

## 12.13. Channelwahl

- Channels sollten sich nicht überscheiden
- 2.4GHz band ist in unterkanäle mit einer Breite von 22 MHz unterteilt, welche einen 5MHz Abstand voneinben
- In Europa 13 Sub-Channels
- Best practive für `802.11b/g/n` mit mehreren APs ist, dass die Channels nicht überlappen, man also z. B. 1, 6 und 11 verwendet
- Bei 5 GHz gibt es 24 CHannels, welche einen Abstand von 20 MHz haben

## 12.14. Threats

**DoS** Einschränken der Verfügbarkeit durch absichtliches stören des Frequenzbereichs

**Rogue Access Point** AP welcher eigentlich nicht zugelassen ist, kann zum aufspüren von MACs oder zum abhören von Daten verwendet werden, Monitoring kann dagegen helfen

**MITM** Angreiffer positioniert sich zwischen zwei Parteien, gefälschter AP mit selber SSID wird broadcasted um Logindaten abzufangen

## 12.15. Sicherheitsmassnahmen

**SSID Cloaking** SSID-Broadcast wird disabled

**MAC-Address-Filtering** Nur erlaubte MACs können sich verbinden

## 12.16. Authentication Methoden

**Open System** Verbindung ohne Passwort möglich

**Shared Key** Credenitals benötigt

**WEP** Ursprünglicher Standard für 802.11, mit RC4, unsicher

**WPA** Verwendet WEP, aber mit TKIP Encryption, key für jedes Package geändert, WiFi-Alliance Standard

**WPA2** AES Encryption, Braucht *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* (CCMP) um zu prüfen, ob non-encrypted-bits verändert wurden

**WPA3** Neuster standard, braucht noch PMF (Protected Management Frames)

Es gibt WPA-Enterprise, welches RADIUS verwendet um geräte zu authentifizieren.

Bei WPA3 gibt es bei öffentlichen Netzwerken Opertunistic Wireless Encryption (OWE), wodurch aller Datenverkehr verschlüsselt wird.

- Bei WPA2 konnte ein Angreifer den Handshake abhören und versuchen, den PSK zu brute-forcen
- Bei WPA3 geht das wegen Simultaneous Authentication of Equals nicht mehr, da der PSK nie exposed wird

# 13. WLAN Config

## 13.1. Home Router

Home Router stellen folgende Dienste zur Verfügung: WLAN Security, DHCP, NAT, QoS, etc. Default Information (IP, User, Passwort) kann einfach gefunden werden: **Ändern so früh wie möglich**

Basic Setup:

- Log in im Web Browser
- Default Passwort ändern
- Mit neuem Passwort einloggen
- Default DHCPv4 Adresse ändern
- IP Adressen erneuern
- Mit neuer IP einloggen

Basic Wireless Setup:

- WLAN Defaults anschauen
- Netzwerk Modus ändern → Entscheiden welcher 802.11 Standard
- SSID konfigurieren
- Channels konfigurieren
- Security konfigurieren (Open, WPA, WPA2, etc.)
- Passphrase konfigurieren

Mesh:

- Access Points mit den gleichen Settings hinzufügen, aber anderen Channels

NAT → Lokale Clients können nach aussen kommunizieren

QoS → Traffic Types werden bevorzugt (Video, Voice)

- kann auch auf spezfischen Ports freigeschalten werden

Port Forwarding → Öffnen von bestimmten Ports nach aussen

## 13.2. WLC (WLAN Controller)

- Access Points werden über CDP erkannt
- Meistens über Advanced Settings konfigurieren
- Ports am WLC sind Trunk Ports und supporten viele APs und WLANs
  - Jeder AP kann mehrere WLANs supporten

WLAN konfiguration:

1. WLAN erstellen
2. WLAN aktivieren
3. Interface auswählen
4. WLAN sichern
5. Verifizieren dass das WLAN funktioniert
6. WLAN überwachen
7. Wireless Client Informationen anschauen

### 13.2.1. SNMP und RADIUS

- WLC soll alle SNMP Traps an den SNMP Server weiterleiten
- RADIUS Server für AAA von Services

SNMP enables:

- Manangement → SNMP → Trap Receivers → New…
- Community Name und IP Adresse eingeben
- WLC forwarded nun die Messages

RADIUS konfigurieren:

- Security → RADIUS → Authentication → New…
- IP Adresse und Shared Secret von Radius Server eingeben → Apply

### 13.2.2. VLAN

- Jedes WLAN auf dem WLC braucht ein eigenes virtuelles Interface
- Konfiguration
  1. Neues Interface erstellen
  2. VLAN Name und ID konfigurieren
  3. Port und Interface Adresse konfigurieren
  4. DHCP Server Adresse konfigurieren
  5. Apply und Confirm

### 13.2.3. DHCP Scope

1. Neue DHCP scope erstellen
2. Name vergeben
3. Konfigurieren und einschalten der neuen DHCP Scope

### 13.2.4. WPA2

Per Standard benutzen alle WLANs auf dem WLC WPA2 mit AES

Neues WLAN konfigurieren:

1. Neues WLAN erstellen
2. Name und SSID festlegen
3. WLAN für VLAN enablen
4. AES und 802.1X Defaults überprüfen
5. WLAN Security so konfigurieren dass der Radius Server genutzt wird
6. Überprüfen ob WLAN verfügbar ist

## 13.3. Troubleshooting

1. Problem identifizieren
2. Mögliche Ursachen bestimmen
3. Test ob Ursache stimmt
4. Lösung planen und implementieren
5. Testen und präventive Massnahmen ergreifen
6. Dokumentieren

No Connection:

- Netzwerkkonfiguration vom PC überprüfen

- Bestimmen ob sich der PC mit dem Kabelgebundenen Netzwerk verbinden kann
- Treiber neu laden
- Security Modus und Encryption Settings prüfen
- Geräte und Kabel prüfen

Poor Connection:

- PC ausserhalb der coverage
- Channels prüfen
- 2.4GHz Interference prüfen
- Wireless Clients upgraden von alten WLAN Standards
- Traffic zwischen 2.4 GHz und 5GHz splitten/segmentieren
  - Verschiedene SSIDs vergeben bei Dual Band Router
- Physische Hindernisse entfernen

#### 13.3.1. Firmware Upgrade

WIRELESS ⟶ Access Points ⟶ Global Configuration ⟶ AP Image Pre-Download

# 14. Routing Concepts

Router nutzt Routing-Tabelle um Egress-Interface zu bestimmt. **Best Path = Longest Match.**

**Longest Match**

1. meisten Bits von Links welche zwischen Tabellen-Eintrag und Dst-IP übereinstimmen.
2. Prefix-Länge (Länger = besser)

| Dets. IP | Binär |
|---|---|
| 172.16.0.10 | 10101100.00010000.00000000.00001010 |
| Routing Tabelle | |
| 172.16.0.0/12 | **10101100.0001** 0000.00000000.00001010 |
| 172.16.0.0/18 | **10101100.00010000.00** 000000.00001010 |
| 172.16.0.0/24 | **10101100.00010000.00000000.00** 001010 |

Der Longes Match ist der letze Eintrag.

**Packet Forwarding**

1. Pakett kommt auf Ingress-Interface an
2. Router findet Longest Match
3. Routerverpackt IP-Paket in Layer-2 Paket.
4. Senden zu Next-Hop oder Destination.

- **Directy Connected**: Router findet Dst-MAC über ARP oder Neighbor Discovery und versendet direkt an Ziel
- **Next Hop:** Router bestimmt „Next Hop“, bestimmt dessen MAC und sendet.
- **No Match**: Paket wird verworfen.

**Primäre Ziel:** Pakt in richtigen DataLink-Frame zu verpacken (z.B. Point-to-Point, HDLC, etc.)

**Packet Forwarding Mechanismen**

**Process Switching** Sehr Alt. Jedes Paketet wird an Control-Pane weitergeleitet und Destination gesucht.

**Fast Switching** Alt. Aufbau von Cache. Control-Pane wird entlastet, da gleiche Dest.-IPs aus dem cache genommen werden.

**Cisco Express Forwarding (CEF)** Neu, Aufbau von Forwarding Information Base (FIB) und Adjazenz-Tabellen, Cleveres Cache Handling, Cisco Default

## 14.1. IP Routing Tabelle

| Code | Prefix/ Length | Trust/ Metrik | via IP | TimeStamp | Interface |
|---|---|---|---|---|---|
| C | 10.0.4.0/24 | [110\|60] | 10.0.03.2 | 00:24:22 | S0/1/1 |

**Code** Anschluschart (wie wurde die Route erlenrt):

- **L** Adresse welche direkt dem Router-Intrface assigned ist.
- **C** Directly Connected
- **S** Statisch erstellt
- **Anderes** Dynamisch erlent. (z.B. O -> OSPF)

**Prefix/Maske** Ziel-Netz und Subnetzmaske

**Administrative Distanz** Vertrauenswürdigkeit. Tiefer = besser

**Metrik** Kosten/ Entfernung Tiefer = besser

**TimeStamp** Timestamp seit erlernen der Route.

**Interface** Ausgangsport

**Routing-Table-Prinzipien**

- Jeder Router trifft Entscheidung alleine
- Routing-Tabels können sich unterscheiden pro Router
- Wenn Hinweg gefunden wird, kann Rückweg trotzdem unbekannt sein

#### 14.1.1. Verbindungstypen

**Directly-Connected** wenn das Interfact aktiv ist und eine IP konfiguriert hat. Zu jedem C existiert ein L. Packet welche für ein lokales Interface bestimmt haben einen Prefix von 32 / 64 Bit. (Erkenunnung, damit sie nicht weiter geroutet werden.)

**Static-Route** für: Default route zu provider, Routes ausserhalb der Routing-Domain, Expliziter Pfad notwendig, Routing zwischen Staub-Netzwerke

**Statisch vs Dynamisch**

| Feature | Dynamic | Static |
|---|---|---|
| **Configuration Komplexity** | Unabhänign von Netz-Grösse | Wächst mit Netzgrösse |
| **Topology Changes** | automatische Anpassung | manuelle Anpassung |
| **Scalability** | Für komplexe Netzwerke | einfaceh Topologien |
| **Security** | muss konfiguriert werden | inherent |
| **Resource Usage** | Braucht CPU, Bandbreite, speicher link | keine |
| **Path predicability** | dynamisch | explizit |

**Default-Route** Matcht alles, kommt am Schluss (`0.0.0.0/0, ::/0`)

**Administrative Distanz** Wenn zwei Einträge den selben Longest Match haben, wird die AD verwendet, tiefer = besser

| Source | AD |
|---|---|
| Directly Connected | 0 |
| Static | 1 |
| EIGRP Summary Route | 5 |
| External BGP | 20 |
| Internal EIGRP | 90 |

| Source | AD |
|---|---|
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| External EIGRP | 170 |
| Internal BGP | 200 |

**Routing Protokolle**

**Interior Gateway** Innerhalb einer Organisation
**Exterior Gateway** Zwischen Providern

**Metriken**

**RIP** Hop Distance
**OSPF** cost, Kumulative Bandbreite
**EIGRP** langsamte Bandbreite und delay

**Loadbalancing** Aufteilen von Paketen auf verschieden Routes, welche gleiche cost haben (automatisch bei dynamic routing protocols)

| | Interior Gatewy P. | | | | Exteriro Gateway P. |
|---|---|---|---|---|---|
| | Distance Vektor | | LinkState | | PathVektor |
| IPv4 | RIPv2 | EIGRP | OSPFv2 | IS-IS | BGP-4 |
| IPv6 | RIPng | EIGRP for IPv6 | OSPFv3 | IS-IS for IPv6 | BGP-MP |

# 15. IP Static Routing

## 15.1. Next Hop

Der Next Hop kann wie folgt angegeben werden

**Next-hop Route** Angeben der next-hop-IP
**Direcly Connected** Angabe des Exit-Interfaces des Routers
**Fully Specified** Angabe der Next-Hop-IP und des Exit-Interfaces

## 15.2. Default Static Route

- Gleich wie eine andere statische route, einfach `0.0.0.0` als mask und Network Address bzw. `::/0` bei IPv6

## 15.3. Floating static routes

- Bieten die Möglichkeit, Alternativrouten zu konfigureren, falls eine Hauptroute ausfällt
- Wird über die Administrative Distance gesteuert
  - Per default auf 1 (Somit prioritär im verhältnis zu allen dynamich gelernten Routen)
  - EIGRP = 90, OSPF = 110, IS-IS = 115
  -

## 15.4. Host Routes

- Routen mit einer 32 (IPv4) oder 128 (IPv6) bitmaske
- Direkte route zu einem Host, nicht zu einem Subnetz
- Werden für auf router konfigurierte Adressen automatisch hinzugefügt

## 15.5. IOS Commands

```
! Route anlegen
R1(config)# ip route 172.16.1.0 255.255.255.0
172.16.2.2
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route 2001:db8:acad:1::/64
2001:db8:acad:2::2

! Über Interface anlegen
R1(config)# ip route 172.16.1.0 255.255.255.0
s0/1/0
R1(config)# ipv6 route 2001:db8:acad:1::/64
s0/1/0

! Fully Specified
ip route 172.16.1.0 255.255.255.0
GigabitEthernet 0/0/1 172.16.2.2
ipv6 route 2001:db8:acad:1::/64 fe80::2

! Anzeigen
R1# show ip route static | begin Gateway
R1# show ip route 192.168.2.1
R1# show running-config | section ip route

! Default Static Route
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2

! Floating Static Routes
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2
5
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
R1(config)# ipv6 route ::/0 2001:db8:feed:10::2
5

! Static host routes
Branch(config)# ip route 209.165.200.238
255.255.255.255 198.51.100.2
Branch(config)# ipv6 route
2001:db8:acad:2::238/128 2001:db8:acad:1::2
```

# 16. Troubleshooting

Router bekommt Paket. Wenn die Destination IP:

1. eine statische Route matcht, wird die statische Route benutzt um den nächsten Hop zu identifizieren
2. keine spezifische statische Route matcht, wird die Default Route verwendet
3. keinen Routing Tabellen Eintrag matcht, wird das Paket gedroppt und eine ICMP Message zurückgesendet
4. eine direkt verbundenes Interface → Router sendet ARP Request um Mac Adresse herauszufinden

## 16.1. Commands

| Command | Description |
|---|---|
| `ping` | Layer 3 KonnektivitätZusätzliche Optionen mit Extended Pings |
| `traceroute` | Pfad zum Zielnetzwerk überprüfen |
| `show ip route` | Routing Tabelle anzeigen |
| `show ip interface brief` | Status der Device Interfaces |
| `show cdp neighbors` | Zeigt alle direkt angeschlossenen Cisco Geräte |