

## Datennetze 2 Teil1: Switching

Dieser Zusammenfassung für den ersten Teils des Kurses Datennetz 2 liegt das CCNA Curriculum mit dem letzten Teil von „Routing and Switching Essentials“ zugrunde. Die Figuren stammen grössten Teils aus dem CCNA Curriculum.

Damit der Rahmen eines Drei-ECTS-Moduls nicht gesprengt wird, handelt es sich um eine unvollständige Zusammenfassung des CCNA Curriculums. Nötigenfalls müssen Studierende auf das Bücher zurückgreifen, um alle Zusammenhänge richtig zu verstehen. Es stehen folgende Bücher von Cisco zur Verfügung:

- Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, ISBN-10: 0-13-336788-6.  
Dieses Buch deckt die Kurse „Introduction to Networks“ und „Routing and Switching Essentials“ ab.
- Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide. ISBN-10: 0-13-336771-1. Dieses Buch deckt die Kurse „Scaling Networks“ und „Connecting Networks“ ab.

Für den Unterricht wird versucht, allgemeine Konzepte zu Datenkommunikation möglichst herstellerunabhängig beizubringen. Geübt wird an Hand von Cisco Equipment. Es sollte aber möglich sein, das Gelernte ohne grossen Aufwand ebenso auf Equipment anderer Hersteller anwenden zu können.

Zu diesem Kurs gehören die folgenden Werkzeuge:

- Netzwerksimulator: PacketTracer von Cisco.
- Protokoll-Analysator: Wireshark

Es wird empfohlen, diesen Text auf Papier auszudrucken und sich im Unterricht Notizen und erläuternde Beispiele dazu zu notieren.

Autor: Peter Gysel, Institut für Mobile und Verteilte Systeme

## Inhaltsverzeichnis

1 LAN Infrastrukturen.....	4
1.1 Konvergierte Netze.....	5
1.2 Hierarchischer Netzansatz.....	6
1.3 Switch Basis Konfiguration.....	8
1.3.1 Initial-Konfiguration.....	8
1.3.2 Port-Konfigurationen.....	10
1.4 Sicherheitsfunktionen.....	11
1.4.1 Angriffe.....	11
1.4.2 Sicherer remote access.....	12
1.4.3 Port-Security.....	12
2 Virtuelle LANs (VLANs).....	15
2.1 Segmentierung mit VLANs.....	16
2.1.1 Übersicht über VLANs.....	16
2.1.2 Kennung von VLANs.....	18
2.2 Implementation von VLANs.....	22
2.2.1 VLAN Zuweisung.....	22
2.2.2 VLAN Trunks.....	23
2.2.3 Dynamic Trunking Protocol.....	23
Troubleshooting für VLANs und Trunks.....	25
2.3 Inter-VLAN Routing.....	25
2.3.1 Funktionsweise von Inter-VLAN Routing.....	25
2.3.2 Konfiguration Router-on-a-Stick für Inter-VLAN Routing .....	26
3 Redundanz im LAN .....	28
3.1 Konzepte des Spanning Tree Protocols (STP).....	29
3.1.1 Der Zweck von STP.....	29
3.1.2 Der STP Algorithmus gemäss IEEE 802.1D.....	30
3.2 Verschiedene Varianten des Spanning Tree Protokolls.....	36
3.2.1 Übersicht.....	36
3.2.2 Per VLAN Spanning Tree Plus (PVST+).....	36
3.2.3 Rapid Per VLAN Spanning Tree Plus (Rapid PVST+).....	37
3.3 Konfigurationen zu Spanning Tree.....	38
3.3.1 Konfiguration PVST+, Rapid PVST+ .....	38
3.4 Redundanz beim Default Gateway.....	40
3.4.1 Konzepte für First Hop Redundancy Protocols (FHRP).....	40
3.4.2 Verschiedene Ausführungen von First Hop Redundancy Protokollen.....	41
3.4.3 Konfiguration und Statusabfragen bei First Hop Redundancy Protokollen.....	42
4 Weiterführende Konzepte im LAN.....	44
4.1 VLAN Trunking Protocol VTP.....	45
4.1.1 Wozu VTP?.....	45
4.1.2 VTP Begriffe.....	46
4.1.3 VTP Advertisements.....	46
4.1.4 Die Default VTP Konfiguration eines Switch.....	47
4.1.5 VTP Sicherheitswarnung.....	47
4.1.6 VTP Pruning.....	48
4.1.7 Konfiguration von VTP.....	49
4.2 Link Aggregation .....	50
4.2.1 Konzepte.....	50
4.2.2 Funktionsweise Etherchannel.....	51
4.2.3 Konfiguration von Etherchannel.....	52
4.2.4 Status-Abfragen und Troubleshooting Etherchannel.....	53
4.3 Layer 3 Switching.....	54

4.3.1 Routed Port.....	55
4.3.2 Switched Virtual IF (SVI).....	55
5 Wireless LAN.....	56
5.1 Konzepte Drahtloser Kommunikation.....	57
5.1.1 Übersicht drahtlose Kommunikation.....	57
5.1.2 Komponenten von WLANs.....	59
5.1.3 802.11 WLAN Topologien.....	61
5.2 Funktionsweise Wireless LAN.....	63
5.2.1 Kanalzugriffsverfahren.....	63
5.2.2 Anmeldung am Access Point.....	67
5.2.3 Kanalzuteilung.....	68
5.2.4 802.11 Rahmen.....	71
5.3 Sicherheit in Wireless LAN.....	74
5.3.1 WLAN Angriffspunkte.....	74
5.3.2 Sicherung von WLANs.....	75
5.4 Konfiguration von Access Points.....	78

## 1 LAN Infrastrukturen

- 1.1 Konvergierte Netze
- 1.2 Hierarchischer Netzansatz
- 1.3 Switch Basis Konfiguration
- 1.4 Sicherheitsfunktionen

Lernziele:

- Sie kennen die Ansprüche, die man heute an konvergierte Netze im Switching Umfeld stellt
- Sie verstehen den Ansatz hierarchischer Netze
- Sie wissen, wie ein Switch aufstartet
- Sie kennen die möglichen Einstellungen der Switch-Ports
- Sie kennen die wichtigsten Angriffe auf Switch
- Sie können einen sicheren Remote-Zugang zum Switch erstellen
- Sie können die grundlegenden Sicherheitseinstellungen auf einem Switch vornehmen

## 1.1 Konvergierte Netze

Aus Datennetzen sind im LAN-Bereich konvergierte Netze geworden. Sie unterstützen

- Datentransfer, z.B. Dateien, e-Mails u.a.. D.h. Sie stellen grosse Bandbreiten zur Verfügung.
- Telefonie: Voice over IP (VoIP). D.h. Es kann für Quality of Service (QoS) gesorgt werden.
- Video-Verteilung und Video-Konferenzen. D.h. Datenstöße können per Multicast verteilt werden.
- Mobilität: Teilnehmer können sich drahtlos verbinden und sich bewegen.
- Sicherheit

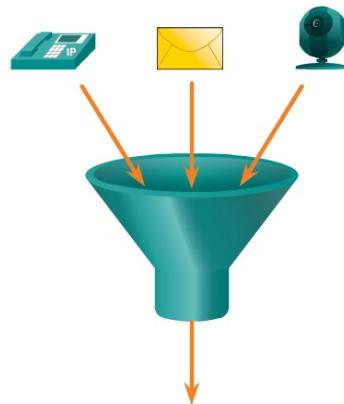


Abbildung 1.1: Verschiedene Arten von Verkehr in einem Netz

Dies ergibt neue Anforderungen an die Netze, insbesondere bezüglich Verfügbarkeit. Der Vorteil konvergierter Netze: Es muss nur noch ein Netz unterhalten werden. Dieses Netz ist aber komplizierter geworden.

Anforderungen an ein LAN:

- Hoher Datendurchsatz
- geringe Verzögerung für Sprachpakete für die Unterstützung von Voice over IP (VoIP)
- Hohe Verfügbarkeit
- Skalierbarkeit
- Einfache Integration neuer Dienste
- Einfache Wartung und Betrieb
- Sichtbarkeit des aktuellen Zustandes
- Schutz vor bekannten Angriffen

Wie muss man LANs entwerfen, um diesen Anforderungen gerecht werden zu können?

Konzept:

- LAN Infrastrukturen werden in Schichten entworfen (Abb. 1.2).
- Switch werden 'vertikal' verbunden (keine 'waagrechten' Vergindungen innerhalb der Schichten Access bzw. Distribution).
- Ende bis Ende: Maximal sechs Hops (sieben Leitungen).

## 1.2 Hierarchischer Netzansatz

Das „Hierarchische Netzmodell“ sieht drei Schichten vor: Core, Distribution und Access

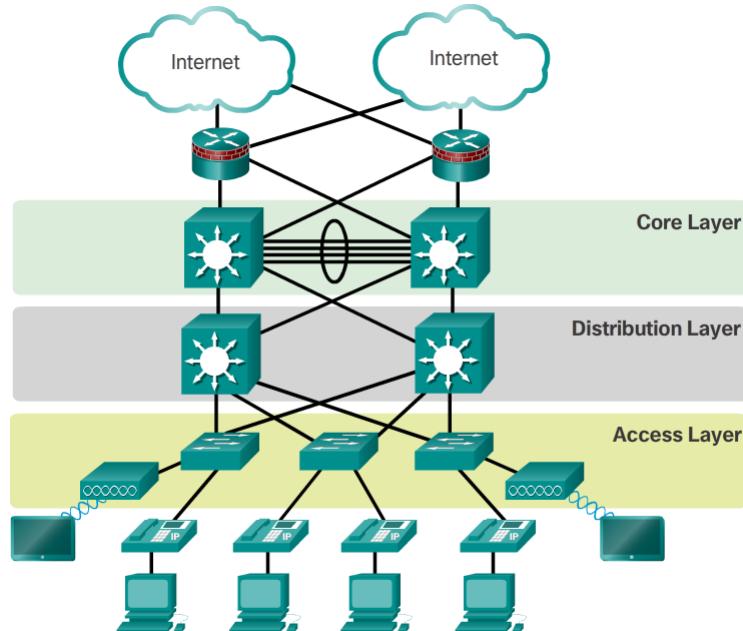


Abbildung 1.2: Hierarchisches Netzmodell

Um eine hohe Verfügbarkeit zu erreichen und gegen Ausfälle besser geschützt zu sein, werden Distribution und Core Switch redundant ausgelegt. Im komfortabelsten Fall wird sogar das Default-Gateway redundant ausgeführt. Fällt ein Switch, ein Router oder eine Leitung aus, so soll ein neuer Weg genommen werden können. Endgeräte können allerdings nur an *einen* Switch angehängt werden.

In kleineren bis mittleren Netzen werden die Schichten Distribution und Core manchmal zusammengefasst und man redet von einem „collapsed core“, Abb. 1.3.

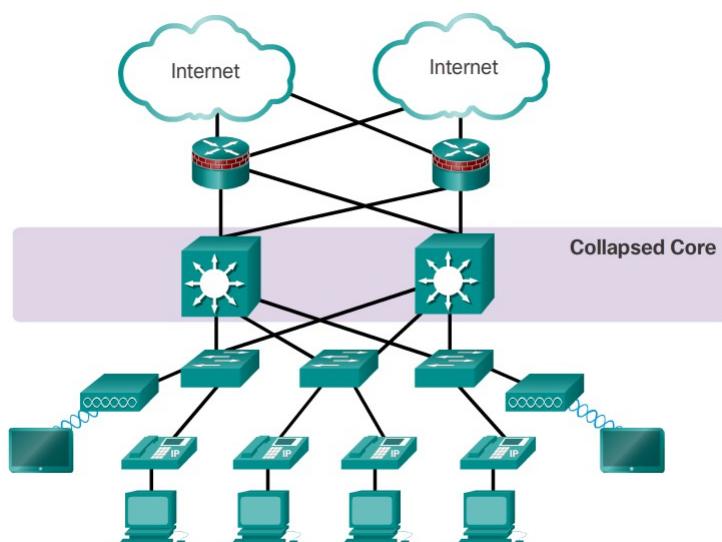


Abbildung 1.3: Netzentwurf für kleinere Netze mit zwei Schichten.

### Vorteile eines hierarchischen Netzaufbaus:

- **Skalierbarkeit:** Das Netz kann wachsen, ohne dass die Struktur neu aufgebaut werden muss.
- **Hohe Verfügbarkeit:** Jeder ALS wird mit zwei DLS verbunden. Ein Distribution Layer Switch, DLS, wird mit zwei Core Switches verbunden, so dass beim Ausfall einer Leitung oder eines Switch ein neuer Pfad durch das Netz geöffnet wird. Einziger "Single Point of failure": Der Access Layer Switch, ALS. Beim Ausfall eines ALS werden die direkt angeschlossenen Endgeräte vom Netz getrennt.
- **Hoher Durchsatz:** Wenn zwischen Distribution Layer Switches und Core Switch genügend Bandbreite geplant wird, so können die Endgeräte mit voller Geschwindigkeit kommunizieren ("near wire speed"). Dazu können mehrere Leitungen zu einem sogenannten "Etherchannel" aggregiert werden. Zwischen Core-Switches werden gewöhnlich Gigabit-Ethernet oder 10 Gigabit-Ethernet-Leitungen eingesetzt. Wichtig ist, dass ein LAN den Bedürfnissen verschiedener Anwendungen gerecht wird: Der einen Anwendung einen hohen Durchsatz, der anderen eine minimale Verzögerung der (kleinen) Pakete.
- **Sicherheit:** Die Sicherheit kann einfach und übersichtlich implementiert werden. In einem ALS wird der Zutritt zum Netz geregelt. Im Distribution Layer können Access-Listen (siehe Teil 2 dieses Kurses) konfiguriert werden, die bestimmten Verkehr zulassen oder verhindern können.
- **Einfache Wartbarkeit:** Wenn bestimmte Aufgaben bestimmten Schichten zugeordnet sind, so wird der Unterhalt einfacher und schneller.
- **Einschränkung** der betroffenen Gebiete im Fehlerfall („limiting failure domains“): Wenn eine Netzkomponente aussteigt, so sollen möglichst wenige Benutzer betroffen sein.

Abb. 1.4 zeigt, wie die Switch der verschiedenen Schichten typischerweise auf verschiedene Gebäude verteilt sein können.

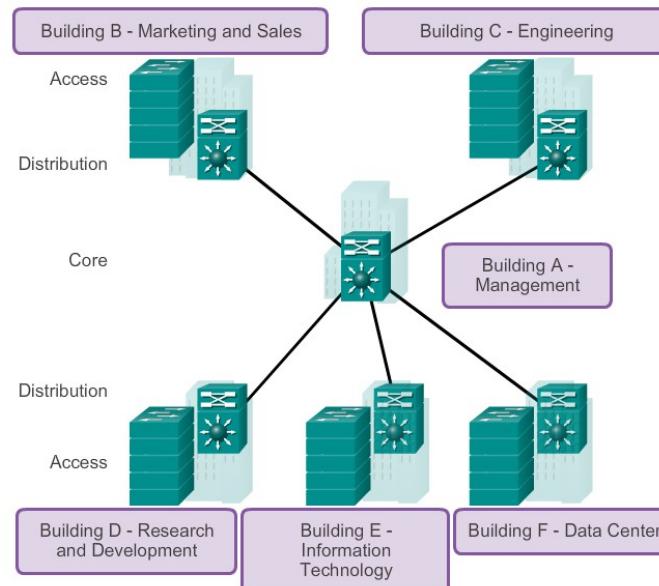


Abbildung 1.4: Beispiel eines hierarchischen Netzen verteilt über mehrere Gebäude

## 1.3 Switch Basis Konfiguration

### 1.3.1 Initial-Konfiguration

#### Boot-Sequenz

Moderne Switches besitzen ein Betriebssystem und ein oder mehrere Benutzer-IFs. Cisco Switch führen beim Start eine Bootsequenz durch. Diese Bootsequenz besteht aus den folgenden Schritten:

1. Durchführen POST(Power On Self Test)
2. Starten Boot Loader Software
3. Der Boot Loader führt eine CPU Diagnose Software aus
4. Der Boot Loader initialisiert das Filesystem für den Start des Betriebssystems (IOS)
5. Der Boot Loader startet das Betriebssystem von der angegebenen Lokation (Flash). Beim Start wird das Betriebssystem komplett ins RAM des Switches geladen.

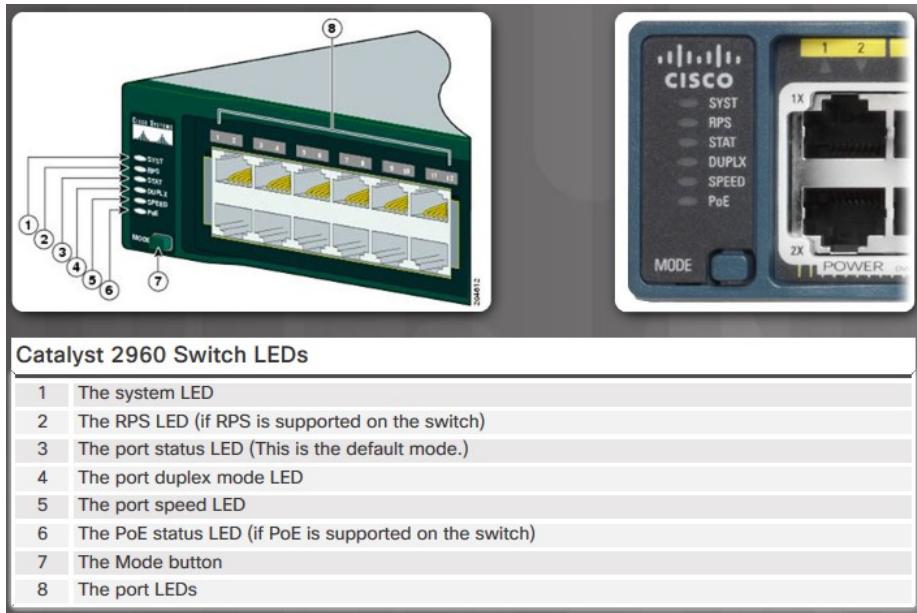
Es ist möglich auf dem Gerät mehrere Versionen des Betriebssystems installiert zu haben. Mit dem Befehl

```
Switch(config)#boot system flash:c2960-lanbase-mz.122-25.FX.bin
```

kann über Boot Variablen angegeben, welches Betriebssystem gestartet werden soll. Das Betriebssystem wird manchmal in einen Ordner mit dem gleichen Namen wie die IOS-Datei (aber ohne Extension .bin) gelegt. Den Inhalt des Flash-Speichers und eine allfällige Ordnerstruktur findet man mit:

```
Switch#show flash:
```

#### Switching Hardware und LEDs



*Abbildung 1.5: LEDs eines Cisco-Switch und ihre Bedeutung. RPS: Redundant Power System.*

Switches besitzen keinen Einschaltknopf. Sobald der Switch an die Stromversorgung angeschlossen wird, wird dieser eingeschaltet. Will man einen Switch ausschalten, so muss der

Stecker gezogen werden. Anhand der Status LED's kann der Betriebsstatus kontrolliert werden, ohne sich extra auf den Switch verbinden zu müssen.

Wenn man einen Rechner an einen Switch anschliesst und die LED oberhalb des zugehörigen Ports nicht leuchtet, so weiss man sofort, dass die Kommunikation nicht funktionieren kann. Die LEDs geben wertvolle Informationen zum Zustand des Switch.

### Switch Remote Management

Moderne Netzwerkkomponenten können alle von ferne („remote“) verwaltet werden. Um ein Switch über Telnet zu konfigurieren und zu verwalten, müssen zuerst über die Konsole Voraussetzungen geschaffen werden. Diese Basiskonfiguration beinhaltet die folgenden Schritte:

- Kontrolle des Zugangs
  - Konfiguration eines Consolen-Passworts.
  - Falls Konfiguration per Telnet zugelassen ist: Konfiguration eines vty-Passworts.
- Kontrolle des Übergangs in den privileged mode: Konfiguration eines enable-Passworts.  
Der Privilidged Mode erlaubt die Konfiguration des Gerätes.
- Konfiguration einer IPv4 Adresse auf das virtuelle IF zum Mgmt-VLAN und Einschalten des IFs.
- Konfiguration Default Gateway (häufige Fehlerquelle bei einer Remote Konfiguration)

### BEISPIEL

```
hostname S2
!
enable password class
!
interface FastEthernet0/1
!
...
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan30
  ip address 172.17.30.3 255.255.255.0
  no shutdown
!
ip default-gateway 172.17.30.1
!
line con 0
!
line vty 0 4
  password cisco
  login
!
end
```

Der IPv6-Stack ist auf einem Switch defaultmäßig nicht eingeschaltet. Gewöhnlich reicht eine IPv4-Adresse für die Konfiguration eines Switch.

### 1.3.2 Port-Konfigurationen

Ein Switch-Port hat beim Aufstarten des Schicht-2-Protokolls zwei Freiheitsgrade:

- den Duplex Mode
- die Datenrate

Das Konzept ist, dass die zwei Seiten einer Ethernet-Leitung beide Parameter automatisch aushandeln.

#### Full- und Halb-Duplex

Ethernet unterstützt die Übertragung von Rahmen im Halb- und im Voll-Duplex Übertragungsmodus. Das ursprüngliche Ethernet läuft im Halb-Duplex Modus. Es benutzt einen Bus, auf den mehrere Stationen zugreifen können ('shared medium'). Das bedeutet: Nur eine Station kann gleichzeitig senden. Auf einem Ethernet-Port kann zu einem gegebenen Zeitpunkt nur entweder gesendet oder nur empfangen werden falls der Bus belegt ist. Aber nicht beides gleichzeitig. Ist am gegenüberliegenden Ende eines Switch-Ports ein Gerät angeschlossen, dass nur Half-Duplex beherrscht, z.B. ein Hub, so wird sich das IF automatisch in den Halb-Duplex Mode umschalten. Ausnahme: Es wurde von Hand ein Mode hart konfiguriert.

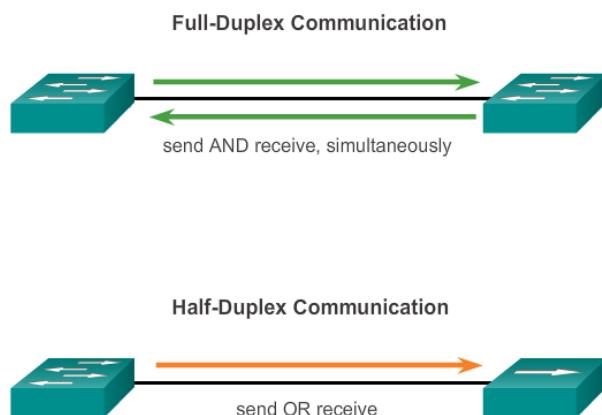


Abbildung 1.6: Halb-Duplex und Voll-Duplex Mode

Um Full Duplex Modus in einem Ethernet zu ermöglichen, wurde das Konzept der Mikrosegmentierung eingeführt. Im Gegensatz zu einem Hub, zwischenspeichert ein Switch einen Rahmen und teilt die Kollisionsdomäne auf. Ferner trennt ein Switch Sende- und Empfangsrichtung auf zwei Adresspaare auf. Das Gegenüber auf einem Switchport kann dann gleichzeitig senden und empfangen. Der Full Duplex Modus ermöglicht zudem eine kollisionsfreie Datenübertragung im Netzwerk. In einem 'geswitchten' Netzwerk sorgt die automatische Aushandlung des Duplex-Modes gewöhnlich dafür, dass alle Ports im Full-Duplex Mode laufen.

Unterstützt ein Ende einer Ethernet-Leitung Gbps und das andere nur 100Mbps, so stellen sich beide Enden – falls die IFs sich im Default-Zustand befinden - automatisch auf 100Mbps ein.

Mit Hilfe den folgenden Befehlen kann ein Switchport fix in den Full Duplex Modus und die Geschwindigkeit auf 100 Mbps konfiguriert werden:

```
Switch(config)#interface f0/1
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

Die Duplex und Speed Einstellungen müssen in diesem Fall auf beiden Ports, die miteinander verbunden werden, konsistent konfiguriert sein. Entsteht eine Inkonsistenz, so kommt die Verbindung nicht zu Stande.

### **MDIX AutoConfig**

Moderne Switches besitzen heute die MDIX Funktion. Diese Funktion ermöglicht, dass ein Switch automatisch erkennt, auf welchem Aderpaar das Gegenüber sendet (Tx) und auf welchem empfängt (Rx). Werden zwei Switches mit einem geraden Kabel miteinander verbunden, werden die TX/RX Übertragungsrichtungen automatisch ausgetauscht. Dank dieser Funktion müssen keine gekreuzten Twisted-Pair Kabel mehr verwendet werden. Die MDIX Funktion ist heute standardmäßig auf neuen Switch aktiviert. Allerdings kann es immer vorkommen, dass noch ältere Switch ohne die MDIX Funktion im Netz sind. Zudem sind alle Switchports defaultmäßig so konfiguriert, dass die Duplex Settings und die Übertragungsgeschwindigkeit (Speed) zwischen zwei Ports automatisch ausgehandelt werden:

```
Switch(config)#interface f0/1
Switch(config-if)#duplex auto
Switch(config-if)#speed auto
Switch(config-if)#mdix auto
```

### **Statusabfragen**

```
S1#show interfaces [if-id]
S1#show startup-config
S1#show flash
S1#show version
S1#show history
S1#show ip interface brief
S1#show mac-address-table
```

## **1.4 Sicherheitsfunktionen**

### **1.4.1 Angriffe**

Die wichtigsten Hacker Angriffe In Ethernet Umgebungen heute:

- Passwort Angriffe (Brute force, Abhören des PW beim Einloggen per Telnet)
- MAC Address Flooding: Ein Switch-Port wird mit MAC-Adressen überhäuft, so dass ihm die Ressourcen ausgehen. Folge: Alle Rahmen werden auf alle Ausgangsports gegeben. Damit kann ein Angreifer andere Verbindungen abhören.
- Spoofing Attacks:
  - DHCP spoofing: Vortäuschen eines DHCP Servers. Dies kann unbeabsichtigt durch falsches Anschliessen eines WLAN Access-Points passieren. Folge: Teilnehmer, die sich neu anschliessen, können nicht mehr Kommunizieren.
  - ARP spoofing: Vortäuschen einer falschen IP-Adresse. Damit kann im ARP Protocol eine Man in the Middle Attacke gemacht werden.
- CDP Attacks. CDP: Cisco Discovery Protokoll. Cisco-Geräte senden spontan Angaben über das verwendete Betriebssystem und die unterstützten Features. Dies ermöglicht benutzerfreundliche Features. Es stellt heute aber ein Sicherheitsrisiko dar. Deshalb wird in einem gut geschützten Netz CDP ausgeschaltet.

- DoS und DDoS: (Distributed) Denial of Service Attacken z.B. mittels Login-Anfragen.

#### **1.4.2 Sicherer remote access**

Damit das PW nicht in Klartext über das Ethernet übertragen wird, sollte man heute nur noch Zugang per SSH konfigurieren.

```
S1(config)#ip domain-name beispiel.ch
S1(config)#crypto key generate rsa          //Erzeugen von Schlüsseln nach dem RSA-Alg.
...                                         //Eine bit-Länge von 1024 wird empfohlen
S1(config)#username admin1 password Xxgeheim
S1(config)#username ... password ...
S1(config)#line vty 0
S1(config-line)# transport input ssh
S1(config-line)#login local
S1(config)#ip ssh version 2
```

Die Konfiguration hat zur Folge, dass die „credentials“ (username-passwort-Paare) auf dem lokalen Router/Switch gesucht werden. Die Alternative wäre ein LDAP/Active Directory Server.

Um sich über SSH auf einem Router / Switch einzuloggen benutzt man auf einem Windows-Rechner ein Terminal-Programm wie Putty. Im Simulator PacketTracer wählt man auf dem Desktop den Command Prompt und gibt folgenden Befehl ein:

```
ssh -l username target
```

Sollen die PW in der Konfigurationsausgabe verschlüsselt dargestellt werden, so wird am besten folgender Dienst benutzt:

```
S1(config)#service password-encryption
```

#### **1.4.3 Port-Security**

Die Port-Security Funktion bietet eine einfache Möglichkeit die Netzwerkinfrastruktur vor MAC Address Flooding Attacken zu schützen. Es gibt drei Möglichkeiten, um Gruppen von zulässigen MAC-Adressen zu definieren.

**Voraussetzung:**

```
S1(config-if)#switchport mode access // Port security funktioniert nur auf Access-Ports!
S1(config-if)#switchport port-security // Port security muss eingeschaltet werden
```

Der Default-Zustand für Port-Security bedeutet, dass nur eine MAC-Adresse akzeptiert wird und bei Zuwiederhandlung der Port ausgeschaltet wird.

**Statisch**

```
s1(config)#switchport port-security mac-address AB.CD.EF
```

Nur die MAC-Adresse AB.CD.EF kann sich an diesem Port anmelden. Dieses Vorgehen ist für einzelne Ports in Ordnung, skaliert aber nicht.

**Dynamisch**

```
S1(config-if)#switchport port-security maximum n
```

Es können sich maximal  $n$  MAC-Adressen an diesem Port anmelden.

**Sticky MAC:**

```
S1(config-if)#switchport port-security mac-address sticky
```

„Sticky“ bedeutet „klebrig“: Die ersten  $n$  MAC-Adressen wird an den Port „geklebt“. Rechner mit anderen Adressen werden nicht mehr akzeptiert. Die MAC-Adresse wird in die Konfiguration geschrieben und kann gespeichert werden.

Es kann konfiguriert werden, wie ihm Fehlerfall reagiert werden soll. Es gibt drei „Violation modes“. Im Modus „shutdown“ wird der ganze Port deaktiviert, wenn die Anzahl erlaubter MAC Adressen überschritten. In den Modi „Restrict“ und „Protect“ werden diejenigen Rahmen abgelehnt, welche die erlaubte Anzahl MAC Adressen überschreiten.

**Violation Modes:**

Die Port-Security Funktion unterstützt die folgenden Violations:

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	Yes	No	Yes	Yes

**Statusabfrage:**

```
S1# show port-security interface FastEthernet 0/1
```

**Beispiel Konfiguration:**

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation protect
```

**Nicht benutzte Switchports**

Auf Switches sind alle Ports defaultmäßig aktiviert und dem VLAN 1 zugewiesen. Sobald ein Endgerät an einem Port angeschlossen wird, wird die Verbindung zwischen dem Endgerät und dem Switch aktiviert. Unter gewissen Umständen stellt dies ein Sicherheitsproblem dar.

Es gibt verschiedene mögliche Massnahmen:

- nicht benutzte Switchports durch die Eingabe des Befehls „shutdown“ deaktivieren. In einer Bank eine geeignete Massnahme, in einer Schule nicht.
- nicht benutzte Switchports auf `mode access` stellen (siehe Kapitel VLANs) und in ein „black hole“ VLAN legen.
- Authentisierung gemäss IEEE 802.1X. Dies ist sicher eine gute Lösung für viele Umgebungen, verlangt aber tieferes Know How in Sicherheit und gibt einen umständlichen Betrieb. Meistens müssen für Geräte, die nicht gewöhnliche Clients sind, Ausnahmen gemacht werden.

Um nicht jeden Port einzeln konfigurieren zu müssen, gibt es den `interface range` Befehl:

```
Switch(config)# interface range type module/first-number - last-number
```

Bsp.:

```
AS11(config)#interface range fastEthernet 0/2 - 8
AS11(config-if-range)#shutdown
AS11(config-if-range)#exit
AS11(config)#+
```

Mögliche Statusabfragen:

```
AS11#show interface fa0/18 status
AS11#show port-security interface fastEthernet 0/18
```

```
Port Security          : Disabled
Port Status            : Secure-down
Violation Mode        : Protect
Aging Time            : 0 mins
Aging Type            : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses   : 0
Configured MAC Addresses : 0
Sticky MAC Addresses  : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

## 2 Virtuelle LANs (VLANs)

### Kapitelaufbau

2.1 Segmentierung mit VLANs

2.2 Implementation von VLANs

2.3 Inter-VLAN Routing

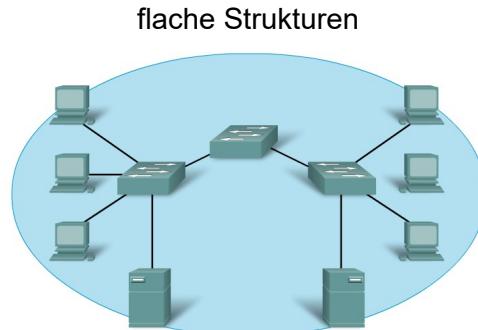
### Lernziele

- Sie können erklären, weshalb und wozu man VLANs macht
- Sie verstehen, wie ein Switch Rahmen von verschiedenen VLANs weiterleitet
- Sie können VLANs, Trunkports und Accessports konfigurieren
- Sie können Fehler in der VLAN-Konfiguration finden und beheben
- Sie verstehen die verschiedenen Ansätze, VLANs über einen Router miteinander zu verbinden.
- Sie verstehen, was man machen muss, damit ein Router mit dem VLAN-Tagging der Rahmen umgehen kann.
- Sie können Inter-VLAN richtig konfigurieren.
- Sie verstehen es, Fehler zu finden und kennen die geeigneten Statusabfragen dazu.

## 2.1 Segmentierung mit VLANs

### 2.1.1 Übersicht über VLANs

Wozu VLANs? Was ist günstiger, flache Netzstrukturen oder hierarchische Netzstrukturen?



oder

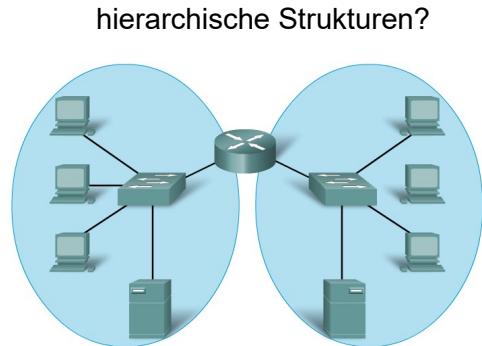


Abbildung 2.1: Flache oder ...

Abbildung 2.2: ...hierarchische Strukturen

Was ist besser: Ein einziges IP-Netz und nur Switching oder mehrere IP-Netze und Routing?  
In einem hierarchischen Netz kann man besser Ordnung bewahren. Insbesondere, wenn ein Netz wächst. Wünschenswert wäre aus Sicherheitsgründen, wenn man die Broadcast-Domäne auf einzelne Benutzergruppen einschränken könnte. Und zwar unabhängig davon, wo die einzelnen Mitglieder einer Benutzergruppe sitzen. Dies spricht für einen hierarchischen Ansatz. Aus Kostengründen möchte man aber nicht für jede Benutzergruppe einen Switch. Wie kann man das bewerkstelligen?

Lösung: Jede Benutzergruppe erhält ein eigenes IP-Netz oder anders ausgedrückt ein virtuelles LAN (VLAN). D.h.: Die verschiedenen Benutzergruppen sollen durch einen Router getrennt sein, obwohl sie sich in der gleichen LAN-Infrastruktur befinden. Damit werden Broadcasts auf Benutzergruppen eingeschränkt.

Bsp.1:

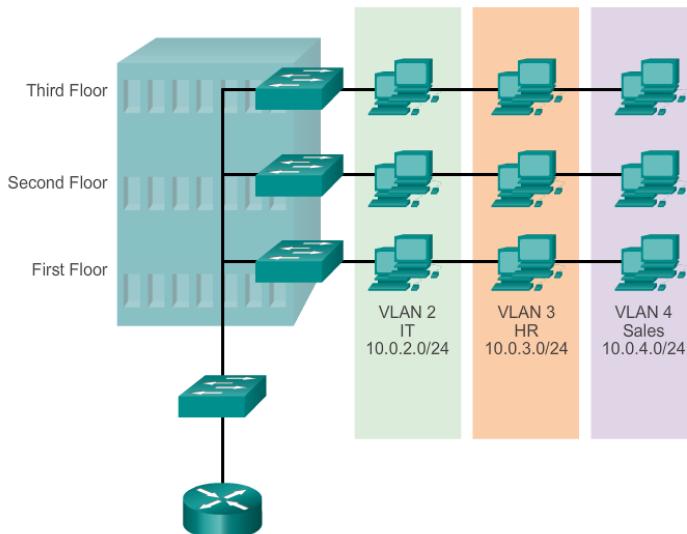


Abbildung 2.3: Verschiedene Benutzergruppen werden in verschiedene VLANs zusammengefasst

Benutzergruppen und die räumliche Aufteilung der Arbeitsplätze sind im Allgemeinen nicht gleich. Man möchte aber alle Mitarbeiter der IT in *ein* IP-Netz nehmen, auch wenn sie z.B. nicht im gleichen Stockwerk ihren Arbeitsplatz haben. Dasselbe für alle Mitarbeiter der Human Resources und alle des Verkaufs. Deshalb macht man für jede Benutzergruppe ein VLAN.

## Vergleich

Virtualisierung bei Rechnern: Auf *einem* Rechner laufen verschiedene virtuelle Maschinen.

Virtualisierung bei LANs: Auf *einem* Switch laufen verschiedene Switching-Instanzen. Für jedes virtuelle LAN läuft eine Switching-Instanz.

## Vorteile von VLANs:

- Die Broadcast-Domänen werden eingeschränkt. Es gibt übers ganze weniger Broadcastverkehr und damit mehr Kapazität für den Datenverkehr.
- Mehr Vertraulichkeit und Sicherheit.
- Bekämpfung von Broadcaststorms: Falls durch Fehlmanipulation ein Broadcaststorm auftritt, so bleiben die Folgen auf das betroffene VLAN beschränkt. Broadcaststorms werden im Kapitel 3 erklärt.
- Effizienter Betrieb des Netzes.

Das alles, ohne dass mehr Hardware benötigt wird und die Hardware-Kosten steigen.

## Typen von VLANs:

- Daten VLANs (Normalfall). Daten-VLANs werden beispielsweise für jede Abteilung einer Firma oder für jedes Stockwerk angelegt.
- Das Default-VLAN: VLAN1. Dieses VLAN kann nicht gelöscht werden. Das Cisco Discovery Protocol, CDP, und das Spanning Tree Protocol, STP, laufen über VLAN1.
- Das "Black hole VLAN": Aus Sicherheitsüberlegungen konfigurieren Administratoren manchmal ein VLAN, dem alle nicht benutzten Ports zugeordnet werden. Wenn es einem Eindringling gelingt, sich an einen offenen Port anzuschliessen, so kommt er nicht aus diesem schwarzen Loch hinaus.
- "Native VLAN". Ein Trunk-Port gemäss IEEE 802.1Q unterstützt neben Rahmen mit einem VLAN-Tag auch Rahmen ohne VLAN-Tag. Also Rahmen, die einem VLAN zugeordnet sind, das keine ID hat. Dieses VLAN wird "native VLAN" genannt. Der Grund für dieses „native VLAN“: Kompatibilität zu älteren Systemen ("Legacy systems").
- Management VLAN. Für das Management der Netzelemente wird gewöhnlich ein Extra-VLAN verwendet. Im Labor wird z.B. die ID 99 benutzt. Man vergibt dem Management VLAN einen Adressraum (ein eigenes Subnet) und konfiguriert auf einem Switch eine IP-Adresse und ein Default-Gateway für dieses VLAN. Ein Switch kann dann von einer entfernten Station über diese IP-Adresse angesprochen und über Telnet, SSH, HTTP oder SNMP verwaltet werden.
- Voice VLANs: Es ist wünschenswert, den Sprachverkehr in ein eigenes VLAN zu nehmen, falls das möglich ist. Hinweis: Hardware IP-Phones unterscheiden sich von Softphones.

## 2.1.2 Kennung von VLANs

Gibt es in einem LAN nur ein einziges VLAN, nämlich das Default-VLAN 1, so wird jeder Broadcast an jedes Endgerät ausgeliefert. Eine Statusabfrage auf dem Switch ergibt folgende Ausgabe:

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
...			

Alle Switch Ports sind dem VLAN 1 zugeordnet. Es gäbe sehr viel Broadcast-Verkehr.

## Trunk- und Access-Leitungen

In Abb. 2.4 gibt es jetzt vier verschiedene VLANs:

- eines für die Fakultät und die Mitarbeiter
- eines für Studierende
- eines für Gäste
- eines für das Netzmanagement

Die Leitungen zu den Endgeräten sind im **Access-Mode**. Alle Rahmen, die auf einer Access-Leitung zum Switch gelangen, werden einem einzigen VLAN zugeordnet.

Ein „**Trunk**“ ist eine Ethernet-Leitung über die Rahmen, die zu verschiedenen VLANs gehören, transportiert werden. Wie die VLAN-Zugehörigkeit eines Rahmens auf einem Trunk gekennzeichnet wird, ist in der IEEE Norm 802.1Q standardisiert („dot1Q“). In Abb. 2.4 sind die Leitungen zwischen den Switch Trunk-Leitungen.

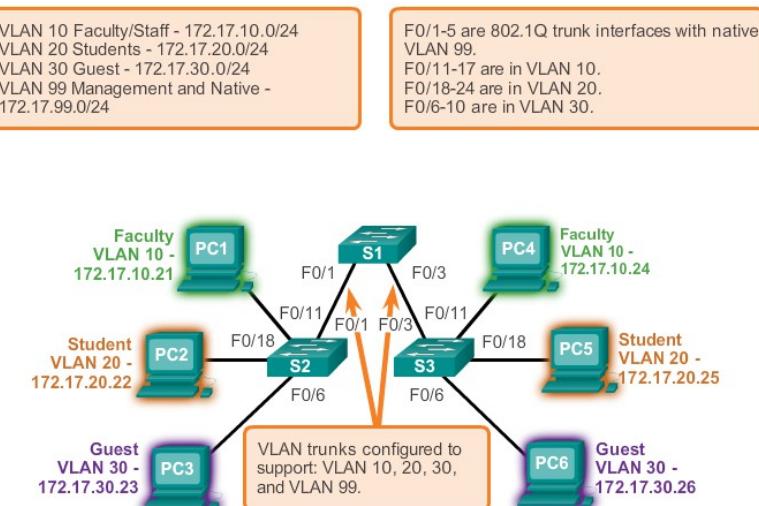


Abbildung 2.4: Vier VLANs in einem LAN

Dank der VLANs wird jetzt beispielsweise ein Broadcast von PC2 nur an PC5 weitergeleitet. D.h. es gibt weniger Broadcast-Verkehr.

Der Switch-Port FastEthernet0/1 auf Switch 2 ist jetzt im Trunk-Mode:

```
S2#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-1005

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30

Die Zugehörigkeit eines Rahmens zu einem VLAN wird auf einer Trunk-Leitung mit einem neuen Feld im Ethernet-Header festgelegt. Dieses neue Feld wird 802.1Q-Tag genannt.

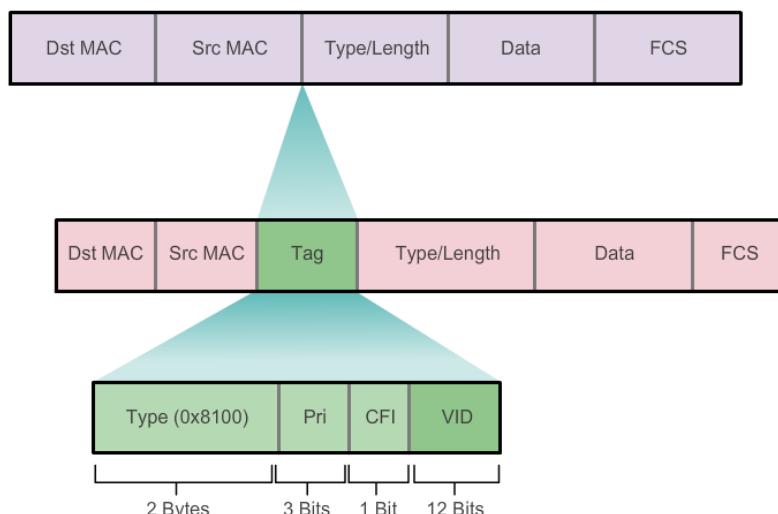


Abbildung 2.5: IEEE 802.1Q-Tag im Ethernet-Rahmen zur Identifikation des VLANs

Ein 802.1Q-Tag besteht aus vier Byte. Die ersten zwei entsprechen dem Feld „Type“ des gewöhnlichen Ethernet-Rahmens. Der Protokoll-Code 0x8100 besagt, dass die nächsten zwei Byte als VLAN-Tag interpretiert werden sollen. Sie sind wie folgt aufgeteilt:

- *Priority Code Point (PCP, im Bild Pri)*: Ein 3-bit Feld, welches die Priorität des Frames gemäss IEEE 802.1p beschreibt. 0 ist die tiefste, 7 ist der höchste Priorität. Es werden acht verschiedene Classes of Service definiert. Damit wird eine differenzierte Behandlung von Rahmen im Switchingbereich ermöglicht.
- *Canonical Format Indicator (CFI)*: Ein 1-bit Feld, welches die Reihenfolge der Bits der MAC-Adresse bei der Übertragung angibt. Ist bei Ethernet auf 1 gesetzt (tiefstwertiges Bit zuerst), bei Token Ring wäre es auf Null (höchstwertiges Bit zuerst).
- *VLAN Identifier (VID)*: Ein 12-bit Feld. Die Werte 0x000 und 0xffff sind reserviert, somit sind 4094 Werte möglich.

Diese Kapselung wird bei Cisco „dot1q“ genannt.

Bemerkung: Cisco verwendete früher eine andere Kapselung: Inter Switch Link, ISL. Heute wird aber meist nur noch IEEE 802.1Q verwendet.

Die Switches der Reihe 2950 können nur „dot1q“, die Kapselung wird nicht spezifiziert. Andere Switch-Modelle unterstützen beide Kapselungsmethoden. Bei diesen Switchmodellen muss zuerst die die Kapselungsmethode explizit konfiguriert werden. Erst dann kann der Mode auf „trunk“ gesetzt werden.

### Kompatibilität zu älteren Geräten

Um die Kompatibilität zu älteren Systemen, die keine VLANs unterstützen, zu gewährleisten, musste das Konzept des „native VLAN“ eingeführt werden. In jeder Multi-VLAN-Umgebung gibt es ein VLAN, dessen Rahmen auf einer Trunk-Leitung keinen Tag erhalten. Welche ID das native VLAN erhalten soll, wird durch die Port VLAN ID, PVID, festgelegt. Per Default ist das VLAN 1 das native VLAN. D.h.: Rahmen des VLANs 1 werden auf einer Trunkleitung nicht mit einem Tag versehen. Abb. 2.6 zeigt ein Anwendungs-Beispiel. Der Hub beherrscht die Unterscheidung Access-Ports – Trunk-Ports nicht und leitet alle Rahmen transparent weiter. Rahmen vom PC1 landen deshalb im native VLAN, d.h. im VLAN 1 (falls nichts anderes konfiguriert wurde).

Aller „ungetagte“ Verkehr, der auf einem Trunkport ankommt, wird dem native VLAN zugeordnet. Umgekehrt wird ein Switch, der einen Rahmen, der dem native VLAN zugeordnet ist und auf die Trunkleitung weitergeleitet wird, ohne VLAN-Tag absenden.

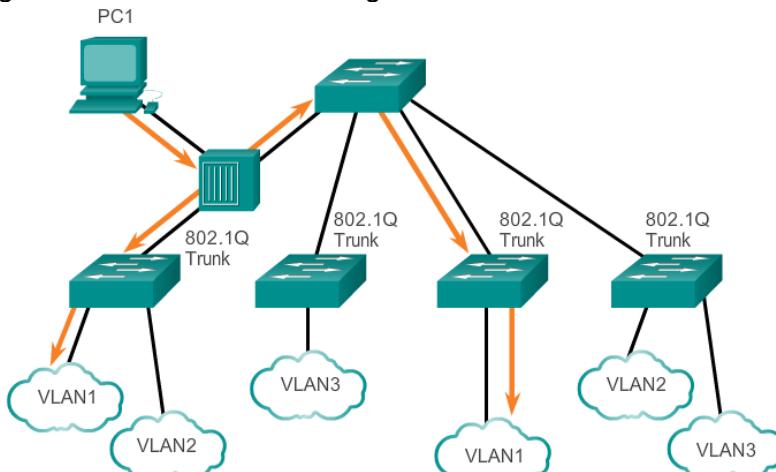


Abbildung 2.6: Für ältere Geräte wurde das "native VLAN" ohne Tagging eingeführt.

### Voice-VLANS

Damit man bei der Einführung von Voice over IP, VoIP, bestehende Verkabelungen nicht auszutauschen braucht, wird ein Arbeitsplatz mit einem HW-Telefon und einem Rechner weiterhin mit *einem* Kabel angeschlossen. Dies ist in Abb. 2.7.

Ein Hardware-IP-Phone hat üblicherweise zwei Ethernet-Buchsen: Eine zum Switch und eine zur Arbeitsstation. Im Telefon ist ein kleiner Drei-Port-Switch integriert (Abb. 2.8). Der Datenverkehr vom PC5 geht „ungetagt“, d.h. ohne VLAN-Kennung, durch den Drei-Port-Switch des Telefons bis zum Switch S3 (interne Ports 3 und 1). Der Voice-Verkehr wird einem separaten VLAN, z.B. 150 zugeordnet. Der Switch S3 wird die „ungetagten“ Rahmen dem VLAN 20 zuordnen. Das IP-Telefon wird seine Rahmen mit einer hohen Priorität kennzeichnen. Prinzipiell wird ein Switch auf einem Access Port die Priorität eines ankommenden Paketes zurück auf Null setzen. Sonst könnte nämlich jede Anwendung ihren Verkehr priorisieren. Mit einer Konfiguration wird dem Switch Port mitgeteilt, dass er das Class of Service Feld (CoS) der Rahmen vom Cisco-Phone akzeptieren soll („trust“). Verzögerung von Sprache stört die Wahrnehmung. Die Einweg-Verzögerung von Sprachpaketen sollte für eine gute Sprachqualität 50ms nicht überschreiten, für eine akzeptable Qualität 100ms. Deshalb gibt man dem Sprachverkehr eine Spezialbehandlung und ein eigenes VLAN.

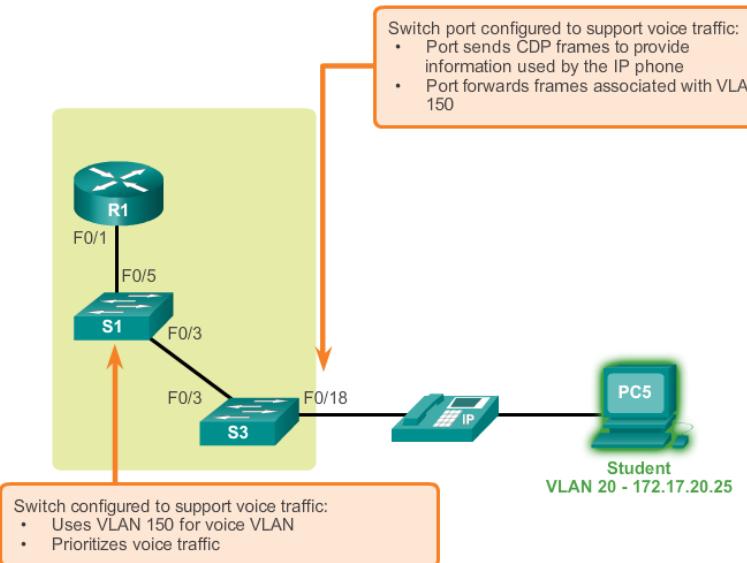


Abbildung 2.7: VLAN 20 für die Studierenden, VLAN 150 für die Telefonie

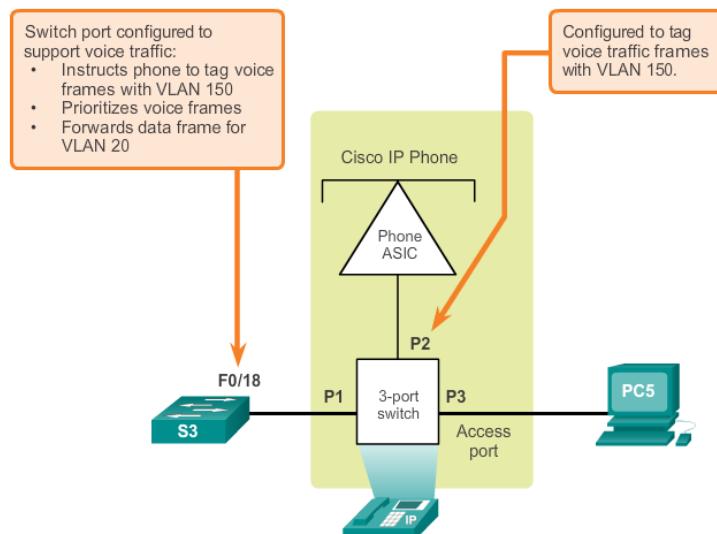


Abbildung 2.8: Ein HW-Phone mit einem internen 3-Port-Switch

## 2.2 Implementation von VLANs

### 2.2.1 VLAN Zuweisung

#### VLAN Nummerierung:

- “Normal range”: VLAN ID 1 bis 1005. VLAN 1 und die VLANs 1002 bis 1005 (Token Ring, FDDI) sind auf einem Cisco-Switch standardmäßig vorhanden.
- “Extended range”: VLAN IDs von 1006 bis 4094. Die 802.1Q-Norm lässt 4000 VLANs zu (12 bit). Dies ist aber eher theoretischer Natur.

Praxis: Auf einem Cisco 2960-Switch können maximal 255 VLANs konfiguriert werden. Wo werden diese VLANs gespeichert?

Antwort: Bei den 29x0-Switch, die wir verwenden, wird die VLAN-Information im Flash in der Datei `vlan.dat` und *nicht* in der Konfigurationsdatei `running-config` gespeichert. Bei den grösseren 4000er-Switch kann es anders sein.

Folge: Das Löschen unserer Access-Switch ist etwas komplizierter als das Löschen eines Routers, da die beiden Dateien `flash:vlan.dat` und die `startup-config` in separaten Schritten gelöscht werden müssen.

#### Erstellen eines VLANs:

```
S2(config)#vlan 10
```

```
S2(config-vlan)#name Faculty
```

#### Ein Access-Port wird durch Konfiguration einem VLAN zugewiesen:

```
S2(config)#interface FastEthernet0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

Häufig werden eine ganze Reihe Ports einem VLAN zugeordnet. Dazu ist der Befehl

```
S2(config)#interface range FastEthernet0/11 - 17
```

```
S2(config-if)#switchport mode access
```

```
S2(config-if)#switchport access vlan 10
```

geeignet.

#### Statusabfragen allgemein:

```
S2#show vlan [brief | id vlan-id | name vlan-name | summary]
```

Bsp.:

```
S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Verkauf	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Die VLANs 1, 1002 -1005 sind auf Cisco-Switches immer vorhanden.

```
S2#show vlan id 10
VLAN Name          Status    Ports
---- -----
10  Verkauf        active    Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15
                               Fa0/16, Fa0/17

VLAN Type   SAID      MTU     Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- -----  -----  -----  -----  -----  -----  -----  -----  -----  -----
10  enet     100010   1500    -       -       -       -       -       0       0
```

## 2.2.2 VLAN Trunks

Ein Port wird als Trunk konfiguriert:

```
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
```

Kontrolle:

```
S2#show interface trunk
Port      Mode   Encapsulation      Status      Native vlan
Fa0/1     on     802.1q            trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10
```

Zusätzlich sollt man aus Sicherheitsgründen ein alternatives VLAN als native VLAN definieren:

```
S1(config-if)#switchport trunk native vlan 99
```

Es ist möglich, die VLANs, die über einen Trunk transportiert werden, einzuschränken:

```
S1(config-if)#switchport trunk allowed vlan 10,99
```

Werden nun zwei weitere VLANs 20 und 30 hinzugefügt, so würden Rahmen für diese VLANs nicht über den Trunkport weitergeleitet. Der Autor hält diese Konfiguration eher für gefährlich und eine mögliche Fehlerquelle.

## 2.2.3 Dynamic Trunking Protocol

Ein Switch weiss a priori nicht, was für ein Gerät auf der anderen Seite einer Leitung angeschlossen ist. Ist da ein Switch, der ebenfalls VLANs unterstützt? Um Inkonsistenzen zu vermeiden, wird zwischen Switch-Ports das Dynamic Trunking Protocol, DTP, ausgeführt. Es dient dazu, dynamisch festzustellen, ob beide Enden einer Leitung VLANs unterstützen, welche VLANs und ob ein Trunk aufgebaut werden kann oder nicht.

Für einen Switch-Port gibt es vier verschiedene mögliche Modi:

- Dynamic Auto
- Dynamic Desirable
- Trunk

- Access

Konfiguration:

```
Switch(config-if)#switchport mode ?
access      Set trunking mode to ACCESS unconditionally
dynamic     Set trunking mode to dynamically negotiate access or trunk mode
trunk       Set trunking mode to TRUNK unconditionally
```

und

```
S1(config-if)#switchport mode dynamic ?
auto        Set trunking mode dynamic negotiation parameter to AUTO
desirable   Set trunking mode dynamic negotiation parameter to DESIRABLE
```

Je nach dem, welche Kombination an den beiden Enden auftritt, wird ein Trunk aufgebaut oder nicht. Wahrheitstabelle:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	-
Access	Access	Access	-	Access

In älteren Cisco-Switch (2950) ist der Default Dynamic Desirable. In neueren Switch (2960) ist der Default Dynamic Auto. Werden zwei neue Switch ohne Konfiguration miteinander verbunden, so bleibt die Leitung eine Access Leitung. Werden zwei alte oder ein alter und ein neuer miteinander verbunden, so geht die Leitung *ohne* Konfiguration in den Trunk-Modus. Dies ist zwar praktisch, stellt aber ein gewisses Sicherheitsrisiko dar.

In welchen Mode befindet sich eine Leitung?

Statusabfrage:

```
Core1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
```

Beachten Sie den Unterschied zwischen dem Administrative Mode und dem Operational Mode. Der Port FastEthernet0/1 ist administrativ im Mode dynamic auto. Operationell ist er im Mode Trunk, da auf der Gegenseite dieser Mode konfiguriert wurde.

### Troubleshooting für VLANs und Trunks

Wie kann vorgegangen werden, wenn in einem Switching-Netz mit verschiedenen VLANs etwas nicht funktioniert?

- Sind die Endgeräte richtig adressiert? D.h.: Entsprechen die IP-Adressen der Rechner den VLANs, denen die Rechner zugeordnet sind?
- Sind die Ports, an denen die Endgeräte angeschlossen sind, den richtigen VLANs zugeordnet?
- Laufen die Leitungen zwischen den Switch im Trunk Mode?
- Sind alle VLANs auf jedem Switch erstellt worden?
- Werden alle VLANs auf einer Trunk-Leitung unterstützt?
- Ist auf beiden Seiten einer Trunkleitung das „native VLAN“ dasselbe?

## 2.3 Inter-VLAN Routing

### 2.3.1 Funktionsweise von Inter-VLAN Routing

In Abb. 2.4 ist ein Netz mit vier VLANs „Students“, „Faculty“, „Guests“ und „Management“ dargestellt. Die vier Netze sind vollständig voneinander getrennt. Die Studierenden können nicht ins Netz der Fakultät gelangen. Und umgekehrt ebenso.

Manchmal wäre man aber froh, wenn beispielsweise Administratoren in andere Netze gelangen. Wenn man diese virtuellen Netze wieder miteinander verbindet, so gibt man nicht alle erlangten Vorteile wieder preis. Der Broadcast-Verkehr bleibt eingeschränkt auf die VLANs. Und Sicherheit kann mittels Access-Control-Listen implementiert werden (siehe zweiter Teil von Datennetze 2).

Wie kann man vorgehen, damit man von einem VLAN in ein anderes kommunizieren kann? Man benötigt einen Router!

1. Ansatz: *Ein VLAN pro Leitung zum Router*

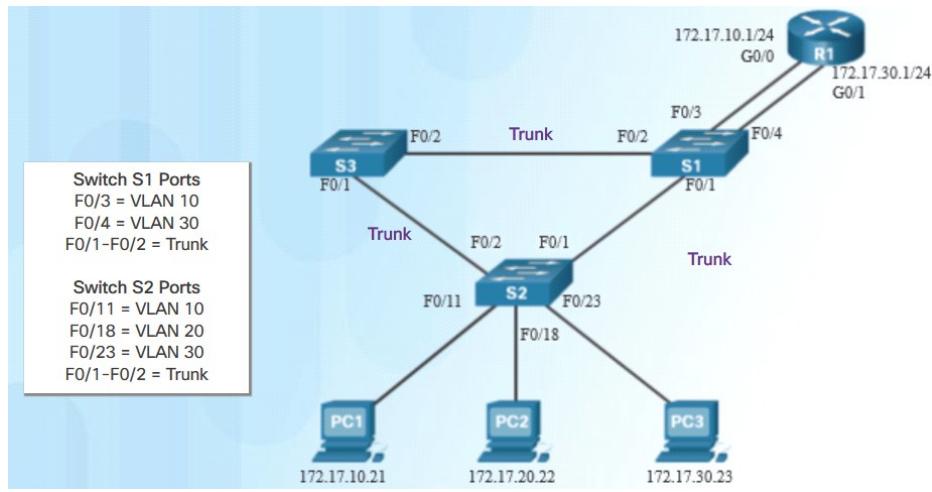


Abbildung 2.9: Verbindung zwischen VLANs mit „legacy“ Routing

In Abb. 2.9 werden die Ports FastEthernet0/3 und 0/4 von S1 als Access Ports konfiguriert und in die VLANs 10 und 30 gelegt.

Die IFs G0/0 und 0/1 des Routers erhalten eine Hostadresse in den Netzen 172.17.10.0/24 und

172.17.30.0/24.

Ergebnis: PC1 erreicht PC3.

Dieser Ansatz hat den Nachteil, dass man meistens nur zwei VLANs miteinander verbinden kann, da Router standardmäßig nur zwei Ethernet-IFs haben. Will man weitere Ethernet-IFs, so müssen diese extra gekauft und in leere Slots eingesetzt werden.

Von den Switch kennen wir VLAN-Trunking mit IEEE 802.1Q. Gibt es etwas ähnliches für Router?

2. Ansatz: Alle VLANs gemultiplext über eine Trunk-Leitung zum Router führen

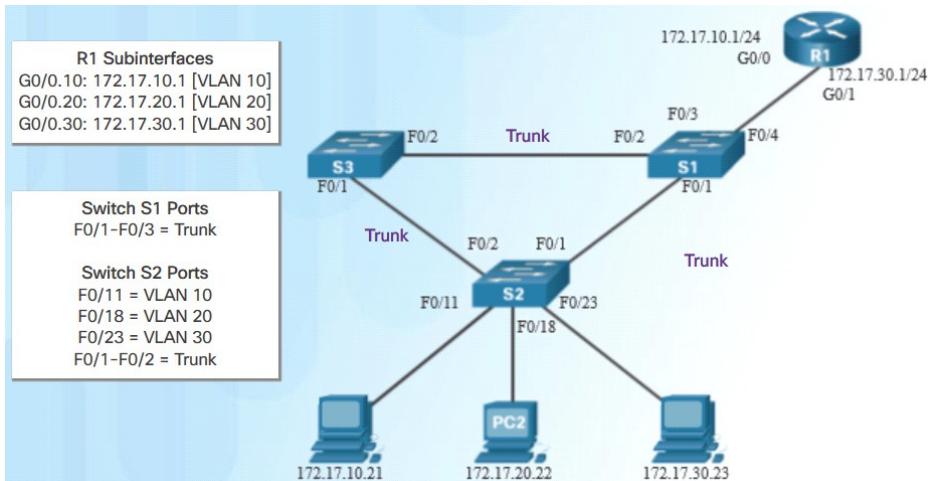


Abbildung 2.10: Inter-VLAN Routing mit einem Trunk-Link zum Router („Router-on-a-Stick“)

Diese Methode hätte grosse Vorteile. Man belegt nur ein physikalisches IF beim Router. Bisher haben aber keine Mittel kennen gelernt, wie ein Router mit VLANs umgehen kann.

**Abhilfe:** Auf einem Router wird ein Port mit demselben Trunking IEEE 802.1Q, wie zwischen zwei Switches eingerichtet. Zusätzlich werden noch *logische* Interfaces für jedes VLAN eingerichtet. Diese logischen IFs heissen auf einem Router Sub-IFs und werden beispielsweise GigabitEthernet0/0.10 und GigabitEthernet0/0.30 bezeichnet. Für den Identifier nach dem Punkt wird am besten die VLAN-ID genommen.

### 2.3.2 Konfiguration Router-on-a-Stick für Inter-VLAN Routing

Der Router muss einerseits wissen, dass aus seinem IF G0/0 Ethernethrahmen mit einem 802.1Q-Tag transportiert werden. D.h. Sie müssen dem IF mitteilen, dass die Rahmen inkapsuliert werden. Andererseits muss für jedes VLAN ein logisches IF da sein. Man erreicht das, indem auf dem physikalischen IF für jedes VLAN ein Sub-IF erstellt wird.

Dem Switch muss die Leitung zum Router als Trunk konfiguriert werden, s. Abb. 2.10.

Konfiguration Switch S1:

```
S1(config)#interface Fa0/1, Fa0/2, Fa0/4
S1(config-if)#switchport mode trunk
```

Konfiguration Router:

```
R1(config)#interface G0/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config)#interface G0/0.10
R1(config-if)#encapsulation dot1Q 10 //Sub-IF für VLAN 10
R1(config-if)#ip address 172.17.10.1 255.255.255.0
```

```
R1(config-if)#interface G0/0.20                                //Sub-IF für VLAN 20
R1(config-if)#encapsulation dot1Q 20
R1(config-if)#ip address 172.17.20.1 255.255.255.0
R1(config-if)#interface G0/0.30                                //Sub-IF für VLAN 30
R1(config-if)#encapsulation dot1Q 30
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#end
```

Obige Konfiguration bewirkt, dass auf dem physikalischen IF GigabitEthernet0/0 drei logische IFs erstellt werden. Eingehende Pakete mit VLAN-ID 10 werden dem Sub-IF 0/0.10 zugeordnet, Pakete mit VLAN-ID 30 dem Sub-IF 0/0.30. Damit diese Konfigurationen möglich sind, muss das IOS des Routers IEEE 802.1Q-Tagging unterstützen. Ausgehende Pakete für das 10er-Netz werden mit der VLAN-ID 10 „getag“ und dem Sub-IF G0/0.10 zugeordnet.

Frage: Bemerkt der Switch S1, dass am anderen Ende nicht ein Switch, sondern ein Router steht? Funktioniert das Dynamic Trunking Protocol immer noch?

Das Ergebnis der Konfigurationen auf dem Router ist folgendes:

```
R1#show ip route
  172.17.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L      172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C      172.17.20.0/24 is directly connected, GigabitEthernet0/0.20
L      172.17.20.1/32 is directly connected, GigabitEthernet0/0.20
C      172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L      172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

Test: Kann PC1 den PC3 anpingen?

### 3 Redundanz im LAN

Kapitelaufbau:

- 3.1 Konzepte des Spanning Tree Protocols (STP)
- 3.2 Verschiedene Varianten des Spanning Tree Protokolls
- 3.3 Konfigurationen zu Spanning Tree
- 3.4 Redundanz beim Default Gateway

Lernziele:

- Sie verstehen, wann und wieso ein LAN das STP braucht
- Sie verstehen, *wie* der Spanning Tree aufgebaut wird
- Sie kennen und verstehen die verschiedenen Rollen der Ports im STP
- Sie können die Bedeutung und den Ablauf der BPDUs erklären
- Sie kennen die verschiedenen Zustände bei der Konvergenz des STP und deren Timer
- Sie kennen die wichtigsten Varianten des STP
- Sie kennen die Weiterentwicklungen von STP: PVST+, Rapid PVST+
- Sie können die beiden Varianten PVST+ und Rapid PVST+ konfigurieren
- Sie können das STP für eine gegebene Topologie so anpassen, dass der Verkehr Ihren Wünschen entsprechend läuft
- Sie kennen die wichtigen Statusabfragen und können sie richtig einsetzen
- Sie können Fehler im Zusammenhang mit STP finden
- Sie wissen, was benötigt wird, um Redundanz auf der Schicht 3 (d.h. im Default-Gateway) zu erhalten
- Sie kennen die verschiedenen Varianten von First Hop Redundancy Protokollen und können sie konfigurieren

### 3.1 Konzepte des Spanning Tree Protocols (STP)

#### 3.1.1 Der Zweck von STP

Redundanz auf Schicht 1 soll ermöglichen, dass, wenn Netzgeräte oder Leitungen ausfallen, möglichst viele Mitarbeiter trotzdem weiterarbeiten können. Man versucht „Single Points of Failure“ zu eliminieren.

Redundanz im LAN kreiert neue Herausforderungen.

Ohne besondere Massnahmen führen Redundanzen zu Schleifen. Broadcast-Rahmen, die sich bei jedem Switch vervielfältigen, würden in einer Schicht-2-Schleife unendlich lang kreisen, da der Ethernet-Rahmen kein TTL-Feld hat, das heruntergezählt wird. Folge: Es treten sogenannte „Broadcast Storms“ auf. Broadcast-Pakete kreisen in Schleifen und stopfen das ganze Netz zu.

Man kann zwei Fälle von Schleifen unterscheiden:

- Schleifen im LAN :

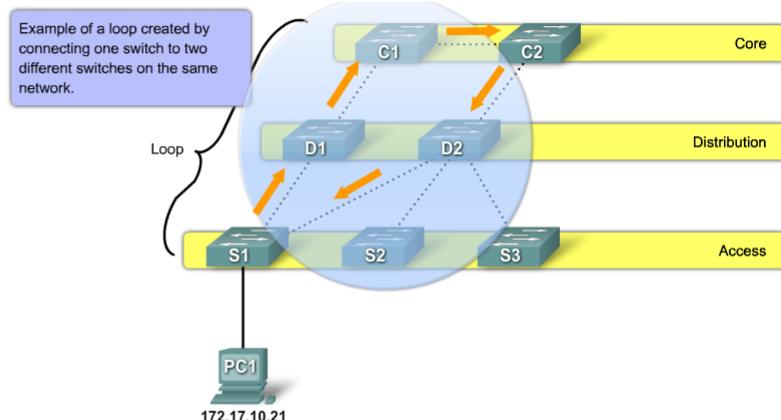


Abbildung 3.1: Schleifenbildung im LAN

- Schleifen an redundanten Leitungen

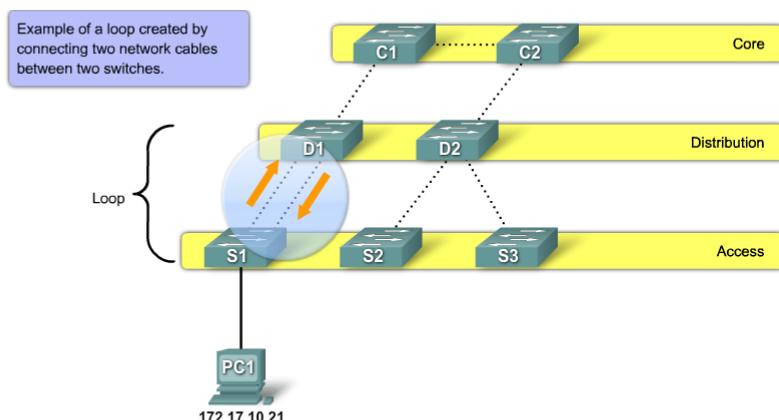
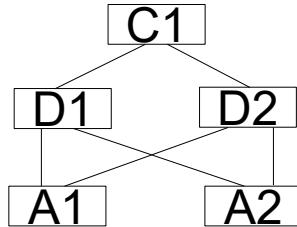


Abbildung 3.2: Schleifen im Verteilerraum

Es ist auch möglich, dass in einem Netz mit Redundanzen ein Unicast-Rahmen mehrfach ausgeliefert wird falls keine Schutzmassnahmen getroffen werden.

### Wie kann der Schleifenbildung begegnet werden?

Idee: Bildung eines Spannbaums. Eine logische, schleifenfreie Baum-Struktur wird auf der Schicht 2 (L2) über eine vermaschte physikalische Struktur (L1) gelegt. Wie würden Sie einen Spannbaum über die untenstehende Struktur legen? Welche Überlegungen machen Sie dabei?



- Wie könnte ein Algorithmus aussehen, der uns für eine beliebige Struktur einen Spannbaum aufbaut?
- Was für Überraschungen kann es geben, wenn ein Algorithmus den Spannbaum macht?

Gleich wie Router für Routing Protokolle Routing-Updates austauschen, tauschen Switch (oder „Bridges“) Informationsrahmen untereinander aus. Switches, die an einem STP teilnehmen, senden und empfangen 'Bridge Protocol Data Unit' Rahmen, BPDUs. Es sind Rahmen mit einem IEEE Header (Ethernet und LLC) und keinen weiteren Headern mehr. Es handelt sich also um ein Schicht-2 Protokoll. Die Destination MAC-Adresse lautet 01-80-C2-00-00-00. Dies ist eine Multicast-Adresse. Jeder Switch, der das STP ausführt, liest diese Rahmen. Der Inhalt des LLC-Feldes zeigt auf den „Service Access Point“ 0x42, d.h. auf das Spanning Tree Protocol.

#### 3.1.2 Der STP Algorithmus gemäss IEEE 802.1D

Der Spanning Tree Algorithmus, STA, sorgt dafür, dass zwischen zwei Switch nur *ein* logischer Pfad existiert. Nicht benötigte Leitungen werden gezielt in einen blockierenden Zustand versetzt. So werden Schleifen unterbunden. Wenn der Algorithmus konvergiert hat, werden gewisse Ports blockiert. Die STP Protokoll-Rahmen, die BPDUs, werden aber weiterhin durchgelassen. Wird eine Leitung unterbrochen oder kehrt eine Leitung zurück in Betrieb, so kann das STP den Spanning Tree über die BPDUs neu aufbauen.

Das STP ordnet jedem Switch Port eine **Rolle** zu.

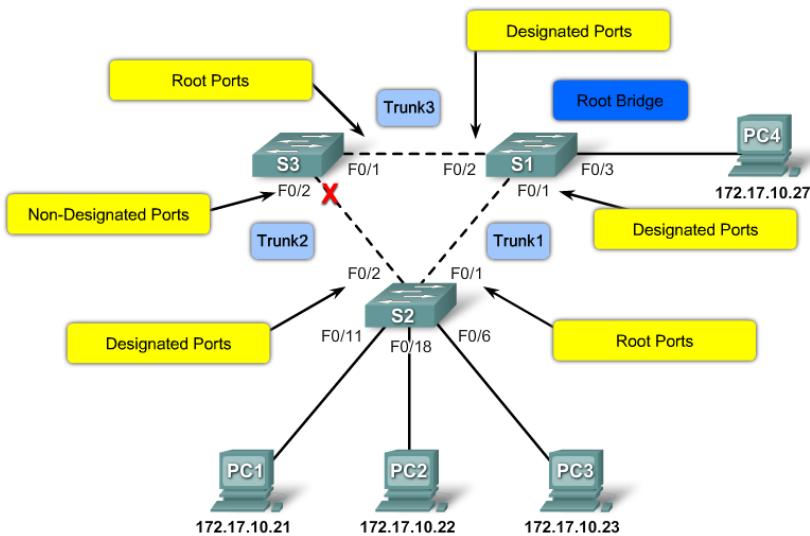


Abbildung 3.3: Referenz-Topologie mit den verschiedenen STP Rollen der Switch-Ports.

### Protokollablauf:

1. Bestimmung der root bridge: Wahl des Switch mit der tiefsten Bridge ID (BID, siehe unten). Er wird Root.
2. Bestimmung der Root Ports. Jeder Switch bestimmt den Port mit dem kürzesten Weg zur Root. Dazu wird eine Metrik für die Links benötigt. Sie wird weiter unten beschrieben. Ein Root-Port wird nie blockiert.
3. Auf jedem LAN-Segment: Bestimmung des „designated ports“ (der Switch-Port, der am nächsten zur root ist).

„Alternate ports“ oder „non-designated“ Ports (Ports die weder „designated“ Ports noch Root Ports sind) werden blockiert. In der ursprünglichen Protokoll Version IEEE802.1D wurden die betreffenden Ports „non-designated“ genannt. In der neueren Protokoll Version IEEE802.1w werden sie „Alternate ports“ genannt.

Der STA hadelt zuerst eine Wurzel für den aufzuspannenden Baum aus. Jeder Switch gibt in seinen BPDU-Rahmen seine BID bekannt. Der Switch mit der **niedrigsten** BID wird Wurzel („Root Bridge“).

### Die Bridge-ID

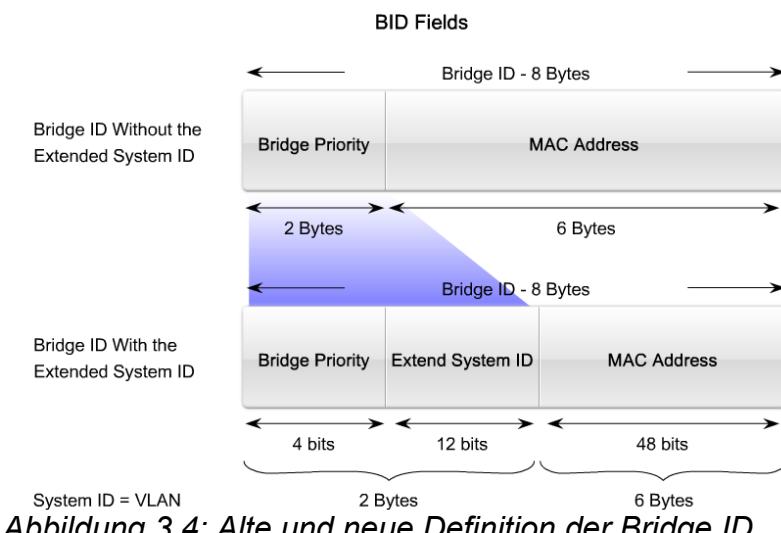


Abbildung 3.4: Alte und neue Definition der Bridge ID

Die Bridge-ID, 8 Byte, besteht aus der Bridge Priority, der extended System ID und der MAC-Adresse des Switch (MAC-Adr. Zu VLAN 1). Die **bridge priority** umfasst gemäss neuer Definition die vier höherwertigen bit des höchstwertigen Bytes. Sie kann damit nur in Schritten von 4096 verändert werden. Die **Extended System ID** gibt an, zu welchem VLAN der Rahmen gehört.

Default Priority + ext. Sys.ID:	1000 0000 0000 0001	32'769
Priority ein Mal dekrementiert:	0111 0000 0000 0001	28'673
Priority zwei Mal dekrementiert:	0110 0000 0000 0001	24577

Ein Switch hat mehrere Bridge-IDs, nämlich so viele wie VLANs. Im folgenden betrachten wir jeweils einfach die BID zu VLAN 1.

Bei der STP Variante PVST+ (Default bei Cisco) wird der STA für jedes VLAN ausgeführt. In dem man verschiedenen VLANs verschiedene Priorities konfiguriert, wird es möglich, dass verschiedene VLANs verschiedene Wurzeln haben.

### Bestimmung der Root-Bridge

Welcher Switch wird zur Root Bridge? Regel: Der Switch mit der tiefsten Bridge ID. Jeder Switch sendet auf allen aktiven Ports alle zwei Sekunden eine BPDU und liest die eingehenden. Was soll er in das Feld 'Root ID' einer BPDU (siehe Abb. 3.7) hineinschreiben, wenn er sie noch nicht kennt? Zu Beginn schreibt er seine eigene ID in dieses Feld und geht davon aus, er sei die Root. Sobald er eine BPDU erhält, die eine tiefere Root ID angibt, so übernimmt er diese und weiss, dass nicht er Root ist.

Was entscheidet darüber, welcher Switch Root wird, wenn alle Switch im Default-Zustand sind? Der Zufall entscheidet. Die MAC-Adresse des Switch macht es aus, da standardmäßig die Bridge Priority für alle Switches 32'768 beträgt. In der Praxis ist es wichtig, dass nicht der Zufall, sondern der Netzadministrator entscheidet, wo die Root zu liegen kommt. Dazu kann der Netzadministrator die Bridge-ID der gewünschten Root gezielt erniedrigen.

### Bestimmung der Port-Rollen

Wir unterscheiden folgende Rollen: Root port, designated port, non-designated port (alternate port).

Jeder Switch ermittelt **einen root port**. Es ist der Port mit den geringsten Pfadkosten zur Root. Jede Bridge bestimmt für jeden Port im Zustand „up“ die Pfadkosten zur Root (Summe der Kosten der einzelnen Links bis zur Root). Dazu wird folgende Metrik verwendet:

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Abbildung 3.5: Kosten eines Ports im Spanning Tree Protocol

Dies wird in Abb. 3.6 für Switch S2 verdeutlicht.

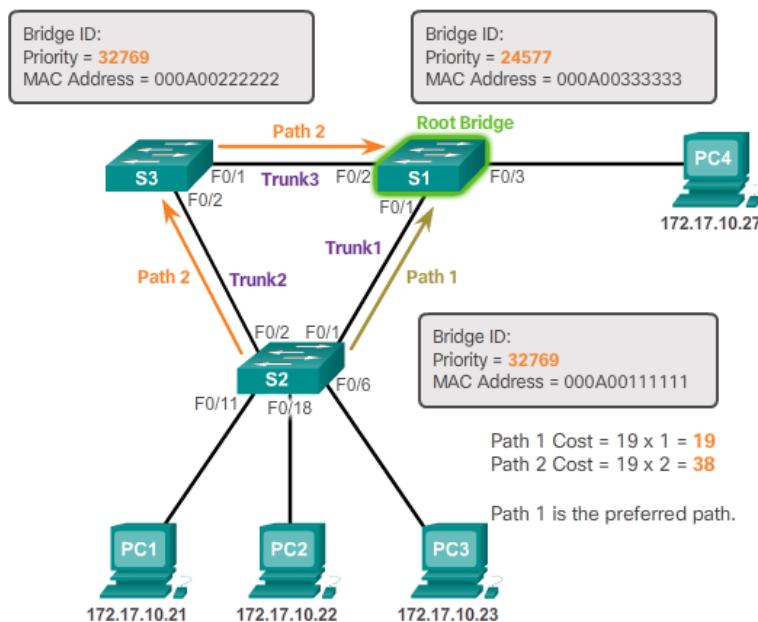


Abbildung 3.6: Berechnung der Pfadkosten zur Root

Falls zwei Wege die gleichen Kosten zur Root ergeben, so entscheidet der Switch nach folgenden Kriterien:

- tiefere Sender BID
- tiefere Port Priorität
- tiefere Port-Nummer

Falls der Weg, der gewählt wird, aus Sicht des Admins ungünstig liegt, so hat er folgende drei Möglichkeiten, die Ausgestaltung des spanning trees zu beeinflussen:

- Veränderung der BID
- Veränderung von Link-Kosten
- Veränderung einer Port-Priorität.

#### **Bestimmung der „designated port“:**

Auf jedem *Link* wird ein designated Port ermittelt. Es ist der „nächste“ Port zur Root: Der Port mit den geringeren Path-Kosten zur Wurzel.

Die Root Bridge ordnet jedem aktiven Port automatisch die Rolle „designated“ zu.

Alle anderen Switch:

Für jeden laufenden Port macht der Switch einen Vergleich der Kosten bis zur Root. Die Kosten, um über den eigenen Switch zur Root zu gelangen, kennt er. Die Kosten für den gegenüberliegenden Port um zur Root zu gelangen entnimmt er dem BPDU, das auf dem entsprechenden Port empfangen wird. Ist der Weg über den eigenen Switch kürzer, so wird er als designated konfiguriert. Es kann vorkommen, dass beide Ports eines Links, die gleichen Pfadkosten zur Wurzel aufweisen. Bsp.: Port Fa0/2 von S2 und Port Fa0/2 von S3 haben beide Kosten 38 bis zur Wurzel (neue Metrik). In diesem Fall entscheidet die tiefere BID für den designated Port.

#### **Austausch der BPDUs**

Um die Mechanik des Protokolls zu verstehen, betrachten wir zuerst den BPDU-Rahmen.

Field Number	Bytes	Field
1-4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
5-8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

*Abbildung 3.7: Format eines BPDU-Rahmens*

Ein BPDU-Rahmen hat 12 Felder. Die ersten vier Felder enthalten die Information über die Protokoll-ID, die Protokoll-Version, den Nachrichten Typ und die Flags (z.B. Flag für Topology Change). Mit den nächsten vier Feldern kann man die Mechanik des STP verstehen. Sie enthalten folgende Information:

- die Root ID (RID)
- die Kosten des Pfades bis zur Root Bridge
- die eigene BID
- die Port ID

Die letzten vier Felder enthalten Timer Informationen.

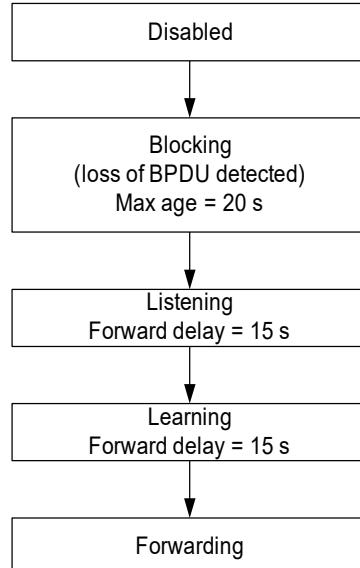
Wir gehen vom Beispiel in Abb. 3.6 aus. Dem Switch S1 ist eine Priorität von 24576 konfiguriert worden, damit er zur Root wird. Jeder Switch nimmt zu Beginn an, er sei Root. Bis er über ein BPDU erfährt, dass ein anderer Switch eine tiefere BID hat.

Beispielablauf: Füllen Sie in der Tabelle folgende Parameter für jede BPDU ein: Root ID, Path cost to root, Bridge ID.

#	Abs.	Parameter	Empf.	Parameter	Entscheidungen
1	S2	RID Cost BID	S1	RID Cost BID	
			S3	RID Cost BID	
2	S3	RID Cost BID	S1	RID Cost BID	
			S2	RID Cost BID	
3	S1	RID Cost BID	S2	RID Cost BID	
			S3	RID Cost BID	

### STP-Zustände

Startet ein Switch auf, beginnt er sofort, das Spanning Tree Protocol auszuführen bevor er Rahmen weiterleitet. Ein Switch benötigt eine gewisse Zeit, um seinen Ports die richtigen Rollen zuzuweisen. Das STP unterscheidet folgende Zustände:



*Abbildung 3.8: Spanning Tree Zustände*

Was macht ein Port in den verschiedenen Zuständen?

Processes	Blocking	Listening	Learning	Forwarding	Disable
Receives and process BPDUs	✓	✓ <sup>1</sup>	✓	✓	✗
Forward data frames received on interface	✗	✗	✗	✓	✗
Forward data frames switched from another interface	✗	✗	✗	✓	✗
Learn MAC addresses	✗	✗	✓	✓	✗

<sup>1</sup>Return to blocking if not lowest cost path to root bridge

Unterschied Blocking – Listening: Im Listening Modus werden BPDUs nicht nur gelesen, sondern es werden auch die eigenen BPDUs gesendet.

Eine wichtige Rolle im STP spielen die Timer (Abb. 3.8):

- Hello time
- Forward delay
- Maximum age

Die Timers sind auf die Annahme 'network diameter'=7 optimiert (maximal 7 Leitungen von Ende zu Ende). Es wird empfohlen, nie die einzelnen Timer zu ändern.

Access Ports müssen den STP Algorithmus nicht mitmachen und können als PortFast konfiguriert werden. Wird ein Kabel eingesteckt, so geht der Port sofort in den Zustand Forwarding.

ACHTUNG: Es dürfen dort keine Switches angeschlossen werden, da sonst Schleifen entstehen können! Cisco offeriert ein Feature, das eine automatische Kontrolle macht: BPDU guard. Ist auf einem Port PortFast konfiguriert, bpdu guard eingeschaltet und er erhält BPDUs auf diesem Port weil ein Switch angeschlossen wurde, so wird der Port ausgeschaltet.

### 3.2 Verschiedene Varianten des Spanning Tree Protokolls

#### 3.2.1 Übersicht

- IEEE802.1D-1998: Ursprüngliche Version, die annimmt, dass es einen Spanning Tree für das ganze LAN gibt, unabhängig von der Anzahl VLANs.
- PVST+, Zusatz von Cisco zum obigen Standard: Jedes VLAN kann seinen eigenen Spanning Tree aufbauen.
- IEEE802.1D-2004: Update des 98er-Standards
- IEEE802.1w (Rapid STP): Schnellere Konvergenz dank neuen Port-Rollen
- Rapid PVST+: Cisco-Variante von RSTP aufbauend auf PVST+
- IEEE802.1s (MSTP): Mehrere VLANs können in eine STP-Instanz abgebildet werden.

Eigenschaften der verschiedenen Varianten:

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s, Cisco	Medium or high	Fast	Per Instance

Abbildung 3.9: Übersicht über die wichtigsten Eigenschaften der verschiedenen Varianten

#### 3.2.2 Per VLAN Spanning Tree Plus (PVST+)

PVST+ macht für jedes VLAN einen Spanning Tree.

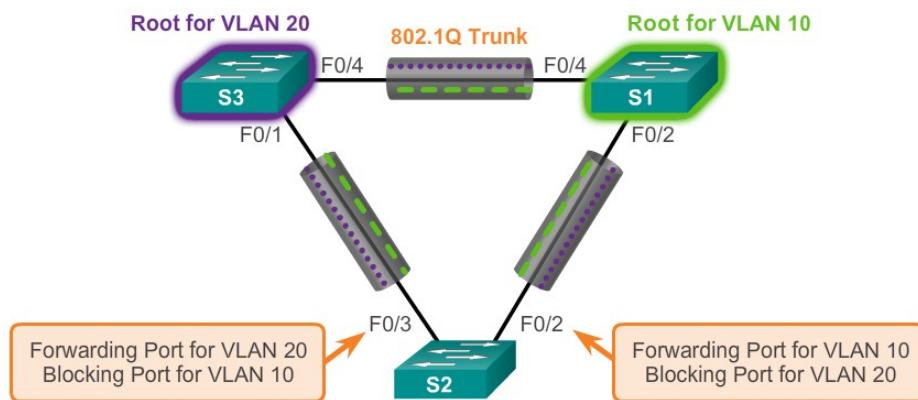


Abbildung 3.10: Verschiedene Spanning Trees für verschiedene VLANs

Die Root kann wahlweise auf verschiedene Switch gelegt werden. Damit kann ein gewisses load balancing auf die verschiedenen Leitungen erreicht werden.

### 3.2.3 Rapid Per VLAN Spanning Tree Plus (Rapid PVST+)

IEEE 802.1w, RSTP:

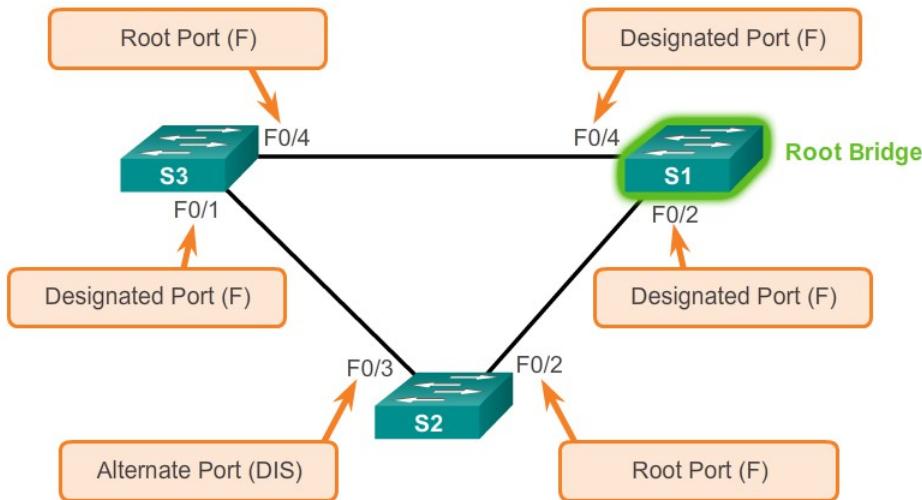


Abbildung 3.11: RSTP: Neue Port-Rolle Alternate Port

Der Hauptvorteil von RSTP besteht darin, dass die automatische Rekonfiguration des Spanning Trees bei einem Unterbruch sehr rasch geht.

RSTP ist rückwärts kompatibel zu 802.D. Kann ein Switch kein RSTP, so kann auf einem Link von Port zu Port auf 802.D zurück gewechselt werden. Wenn ein Admin gewohnt ist in der Konfiguration von 802.1D, so kann er mit wenig Aufwand zu RSTP übergehen. Der Prozess für die Bestimmung der Root und die meisten Bezeichnungen bleiben gleich. Aber es gibt einen neuen Port Typ: „Alternate Port“. Er ist im „discarding state“. Bei RSTP gibt es keine blockierenden Ports mehr. Allgemein werden nur noch drei Status unterschieden: discarding, learning, forwarding.

Der Vorteil von RSTP kommt dadurch zu Stande, dass das Protokoll aktiv einem Port mitteilen kann, dass er in den forwarding state übergehen kann und so nicht auf den Ablauf von Timern warten muss.

Rapid PVST+ ist die Cisco-Variante von RSTP, die für jedes VLAN einen Spanning Tree aufbaut.

Unterschiede PVST+ zu Rapid PVST+:

- In RSTP werden die BPDUs leicht anders genutzt (Abb. 3.12). RSTP versendet Version 2 und Type 2 BPDUs. Das Flag enthält jetzt andere Infos. Ein RSTP Switch kann aber BPDUs mit einem 802.1D Switch austauschen.
- Eine RSTP Bridge sendet immer BPDUs im Abstand des Hello-Intervalls (2 s per Default). Auch wenn sie selbst keine BPDU von der Bridge mehr erhält.
- Bei RSTP gibt es eine Unterscheidung von zwei Link Types: „Shared“ (half duplex) und „Point-to-Point“ (full duplex). Designated ports können rasch Übergänge machen sofern der Port Type Point-to-Point ist.

Auch bei RSTP können Access-Ports als solche gekennzeichnet werden. Sie gehen dann sofort in den forwarding state über. Bei RSTP werden sie „Edge Ports“ genannt.

The diagram illustrates the RSTP Version 2 BPDU structure and the mapping of its flags to specific bits.

RSTP Version 2 BPDU	
Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID=0x02	1
BPDU Type=0X02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

Flag Field	
Field Bit	Bit
Topology Change	0
Proposal	1
Port Role	2-3
Unknown Port	00
Alternate or Backup	01
Port	
Root Port	10
Designated Port	11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

Abbildung 3.12: Das BPDU-Format bei RSTP.

### 3.3 Konfigurationen zu Spanning Tree

#### 3.3.1 Konfiguration PVST+, Rapid PVST+

Defaultwerte

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

**Tabelle 3.1: Defaultwerte für Cisco Switch****Festlegung der Root in einem LAN:**

```
S1(config)#spanning-tree vlan 1 priority 24576
S1(config)#spanning-tree vlan 1 root primary
S1(config)#spanning-tree vlan 1 root secondary
```

//Oder:  
 //Dieser Switch wird root  
 //Dieser Switch wird Backup root

**Änderung der Kosten eines Links:**

```
S1(config-if)#spanning-tree cost 25
```

**Änderung der Port Priority:**

```
S1(config)#interface FastEthernet 0/1
S1(config-if)#spanning-tree port-priority 112
```

**Konfiguration von Portfast bzw. Edge Port**

```
interface FastEthernet0/3
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
```

**oder im globalen Konfigurationsmodus:**

```
spanning-tree portfast default
spanning-tree portfast bpduguard default
```

D.h.: Alle Ports, die nicht im Trunk Mode sind, werden in den Port-Fast Mode gesetzt.

**Rapid PVST: Im globalen Config Mode**

```
spanning-tree mode rapid-pvst
```

Staatsabfragen:

Die wichtigste Status-Abfrage für das STP lautet

S1#show spanning-tree

```
S2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority 27577
              Address   000A.0033.3333
              Cost      19
              Port      1
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority   32769  (priority 32768 sys-id-ext 1)
              Address   000A.0011.1111
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

  Interface   Role Sts Cost      Prio.Nbr Type
  -----  -----
  F0/1        Root FWD 19       128.1    Edge P2p
  F0/2        Desg FWD 19       128.2    Edge P2p
```

Tabelle 3.2: Alle Angaben über den STP-Zustand eines Switch

### 3.4 Redundanz beim Default Gateway

#### 3.4.1 Konzepte für First Hop Redundancy Protocols (FHRP)

Problematik: Jedem Endgerät wird genau *ein* Default Gateway, DGW, konfiguriert. Was passiert, wenn das DGW nicht mehr erreichbar ist? Die Endgeräte holen sich *nicht* eine neue Adresse für das DGW.

Benötigt wird ein Mechanismus für ein zweites DGW. Ein zweiter Router muss ans gleiche VLAN angeschlossen sein.

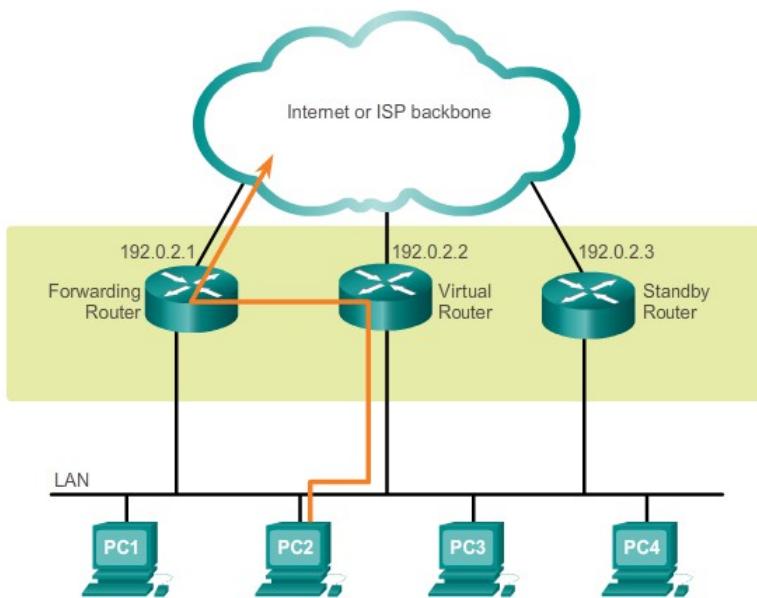


Abbildung 3.13: Konzept für ein "First Hop Redundancy Protocol".

Idee: Physikalisch sind zwei Router da. Die Endgeräte „sehen“ nur einen virtuellen Router. Als DGW wird den Endgeräten die Adresse des virtuellen Routers konfiguriert.

Beispiel (siehe Abb. 3.13):

Zwei physikalische Router mit den Adressen 192.0.2.1 (aktiver Router) und 192.0.2.3 (standby Router) stehen bereit. Die Endgeräte sehen einen virtuellen Router mit IP-Adresse 192.0.2.2.

Ein First Hop Redundancy Protocol, FHRP, muss einen Mechanismus definieren, welcher der beiden physikalischen Router die aktive Rolle übernimmt. Wenn der aktive Router (oder der Link zum Internet) ausfällt und der Standby-Router übernimmt, so soll das für das Endgerät transparent sein.

Wenn ein Endgerät einen Ethernet-Rahmen ans DGW senden will, so ermittelt es mit dem ARP-Protokoll die MAC-Adresse des DGW. Es erhält die MAC-Adresse des virtuellen Routers. Der aktive Router wird den Rahmen mit der Ziel-MAC-Adresse des virtuellen Routers verarbeiten.

Der aktive Router

- antwortet auf ARP-Anfragen mit der MAC-Adresse des virtuellen Routers
- leitet die Pakete für den virtuellen Router weiter
- sendet periodisch Hello Pakete

Ein Router im Standby Zustand

- hört auf die Hello Pakete des aktiven Routers und überwacht die Funktion
- übernimmt die Aufgaben des aktiven Routers, wenn er keine Hello Pakete mehr erhält.

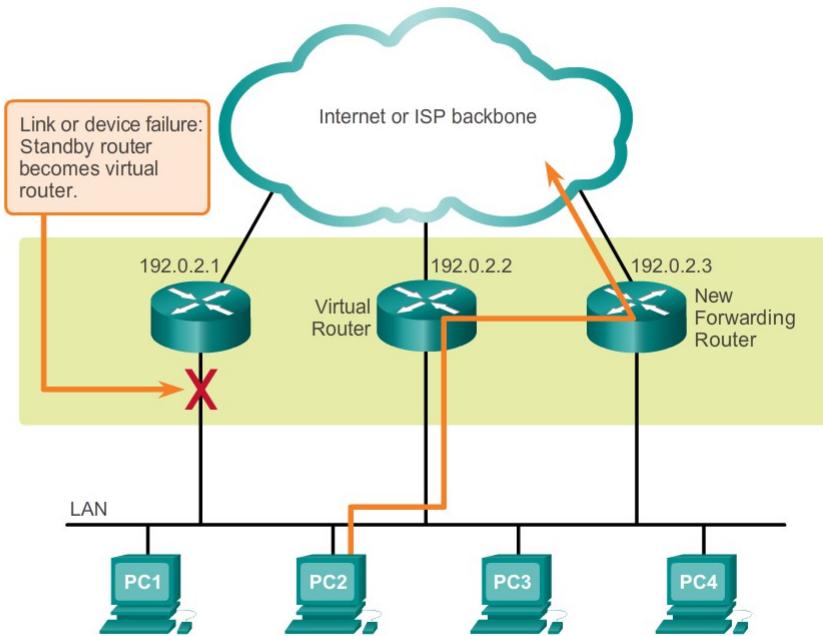


Abbildung 3.14: Ausfall des aktiven Default Gateways

### 3.4.2 Verschiedene Ausführungen von First Hop Redundancy Protokollen

- **Hot Standby Router Protocol (HSRP)**

Es handelt sich um ein Cisco-proprietäres Protokoll für IPv4. Der Standby Router überwacht die Funktion des aktiven Routers. Der Verkehr läuft im Normalfall nur über *eine* Leitung. Die zweite Leitung liegt brach. Es können mehrere Standby Gruppen konfiguriert werden.

- **HSRP for IPv6**

Separates, Cisco-proprietäres Protokoll für IPv6 mit der gleichen Funktion wie HSRP. Eine HSPRv6 Gruppe bildet aus der Gruppennummer eine virtuelle MAC-Adresse und eine virtuelle link-lokale IPv6-Adresse. In den Router Advertisements, RA, steht die virtuelle link-lokale Adresse.

- **Virtual Router Redundancy Protocol version 2**, VRRPv2. Offenes FHRP.

- **VRRPv3**. Verbesserung von VRRPv2, das besser skaliert und IPv6 unterstützt.

- **Gateway Load Balancing Protocol**, GLBP, siehe Abb. 3.2. Cisco proprietäres FHRP, das ein load balancing über die beteiligten Router möglich macht.

- **Gateway Load Balancing Protocol for IPv6**.

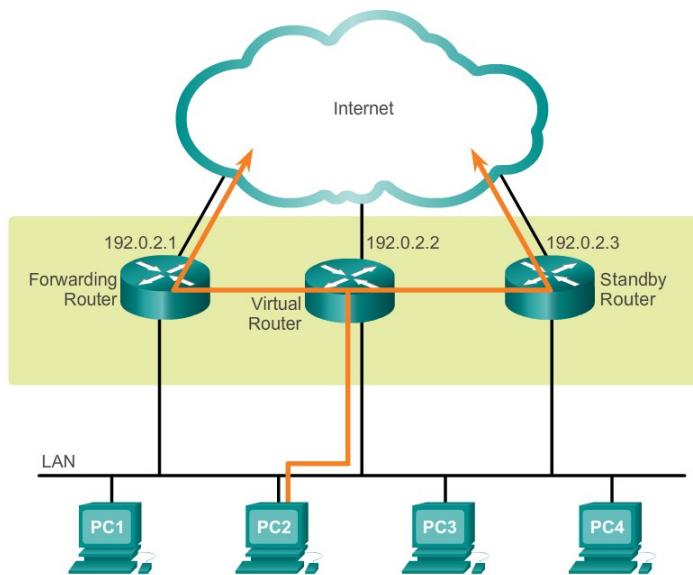


Abbildung 3.15: Gateway Load Balancing Protocol

### 3.4.3 Konfiguration und Statusabfragen bei First Hop Redundancy Protokollen

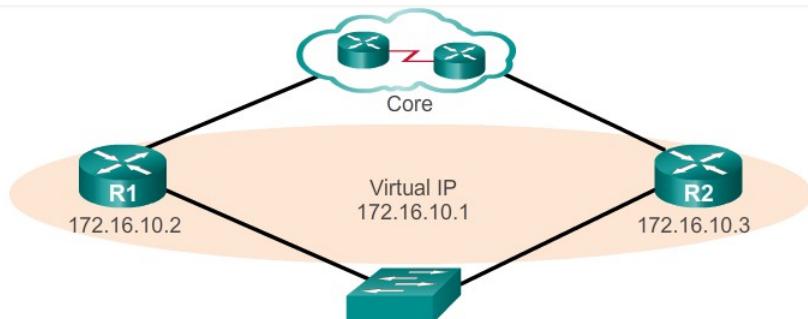


Abbildung 3.16: Konfigurationsbeispiel-Topologie

#### Konfiguration HSRP auf R1:

```

interface GigabitEthernet0/1
  ip address 172.16.10.2 255.255.255.0          //IP-Adresse des phys. Router-IFs
  standby 10 ip 172.16.10.1                      //Gruppe und IP-Adresse des virt. Router-IFs
  standby 10 priority 150                         //Optional: Priorität für den Router
  standby 10 track s0/0/0                          //Verfolge den Zustand des IFs s0/0/0
  standby 10 preempt                               //Opt.: Nach einem Ausfall soll er wieder Master
                                                //werden.
  
```

Der Router R2 wird analog konfiguriert. Mit der Konfiguration der `priority` kann gewählt werden, welcher Router aktiv sein wird. Die höhere `priority` gewinnt. Wenn der aktive Router ausfällt, der Standby hat übernommen und der ehemals aktive wird wieder hergestellt, so wird er ohne weitere Massnahme die Standby Funktion übernehmen. Will man, dass er wieder aktiv wird, so geschieht das mit dem `preempt`-Befehl. Um ein load balancing zu erreichen, können für verschiedene VLANs verschiedene Gruppen definiert werden. Einmal wird der Router R1 priorisiert, einmal der

Router R2.

### **Statusabfragen:**

```
R1#show standby brief
```

```
P indicates configured to preempt.  
|  
Interface  Grp   Pri  P State      Active          Standby        Virtual IP  
Gig0/1      10    150  P Active     local           172.16.10.3    172.16.10.1  
und
```

```
R2#show standby brief
```

```
P indicates configured to preempt.  
|  
Interface  Grp   Pri  P State      Active          Standby        Virtual IP  
Gig0/1      10    140  S Standby    172.16.10.2    local          172.16.10.1
```

```
R1#show standby
```

```
GigabitEthernet0/1 - Group 10 (version 2)  
State is Active  
  6 state changes, last state change 00:00:32  
Virtual IP address is 172.16.10.1  
Active virtual MAC address is 0000.0C9F.0000  
Local virtual MAC address is 0000.0C9F.F00A (v2 default)  
Hello time 3 sec, hold time 10 sec  
  Next hello sent in 0.947 secs  
Preemption enabled  
Active router is local  
Standby router is 172.16.10.3, priority 150 (expires in 8 sec)  
Priority 150 (configured 150)  
Group name is hsrp-Gig0/1-10 (default)
```

HSRP macht von sich aus kein Load Balancing. Dieser Nachteil kann teilweise behoben werden indem man für verschiedene VLANs verschiedene Standby-Gruppen definiert. Die Rolle des aktiven Routers wird dann auf die verschiedenen Gruppen verteilt. Das „Gateway Load Balancing Protocol“ hingegen realisiert von sich aus ein Load Balancing und benutzt beide Leitungen.

### **Konfiguration GLBP auf R1:**

```
interface GigabitEthernet0/1  
ip address 172.16.10.2 255.255.255.0  
glbp 10 ip 172.16.10.1  
glbp 10 priority 150
```

### **Statusabfrage:**

```
R1#show glbp
```

## 4 Weiterführende Konzepte im LAN

Angenommen, Sie haben ein hierarchisches LAN nach den Regeln der Kunst mit zwei Core-Switch, vier Distribution-Swtich und 6 Access-Switch. Die VLANs 10, 20 und 99 seien ordnungsgemäss konfiguriert. Nun muss ein neues VLAN 30 hinzugefügt werden. Mit den bisher bekannten Mitteln bedeutet das, dass sich der Administrator von seinem Büro aus, auf zwölf Switch einloggen und das VLAN erstellen muss. Das gibt erstens viel Arbeit und ist fehleranfällig. Wir benötigen deshalb ein Werkzeug, das es uns möglich macht, die VLANs auf einem Switch zu installieren und das Werkzeug verteilt die VLAN auf alle Switch.

Inhalt:

4.1 VLAN Trunking Protocol VTP

4.2 Link Aggregation

4.3 Layer 3 Switching

Lernziele:

- Sie verstehen den Zweck des VLAN Trunking Protocols VTP.
- Sie verstehen die Konzepte hinter VTP.
- Sie können die Funktionsweise von VTP erklären (domains, modes, advertisements, pruning).
- Sie können VTP konfigurieren.
- Sie wissen, wie Sie im Fehlerfall suchen müssen.
- Sie verstehen die Gefahren, die mit VTP verbunden sind.
- Sie haben verstanden, weshalb es sinnvoll ist, parallele Leitungen zwischen zwei Switch zu einer logischen Verbindung zu bündeln („port-channel“).
- Sie verstehen die Funktion der Link-Aggregations-Protokolle (PAgP, LACP) .
- Sie kennen die verschiedenen Modi der beiden Protokolle PAgP und LACP und wissen, bei welchen Kombinationen der Modi ein Port-Channel zu Stande kommt und wann nicht.
- Sie können ein Firmennetz mit port-channels verkabeln und betreiben.
- Sie kennen die wichtigen Statusabfragen und können Fehler finden.
- Sie verstehen, was man mit Layer 3 Switching gewinnen kann.
- Sie können routed Ports und switched virtual IFs richtig einsetzen und konfigurieren.
- Sie können ein Enterprise LAN mit Layer 3 Switching geeignet planen.
- Sie wissen, was benötigt wird, um Redundanz auf der Schicht 3 (d.h. im Default-Gateway) zu erhalten
- Sie kennen die verschiedenen Varianten von First Hop Redundancy Protokollen und können sie konfigurieren

## 4.1 VLAN Trunking Protocol VTP

### 4.1.1 Wozu VTP?

*Problematik:* Im Netz von Abb. 4.1 sind die VLANs 10, 20 und 99 bekannt. Nun wird ein neues VLAN eingeführt: VLAN 30. Der Netz-Administrator muss auf allen Switches die nötigen Konfigurationen von Hand vornehmen!

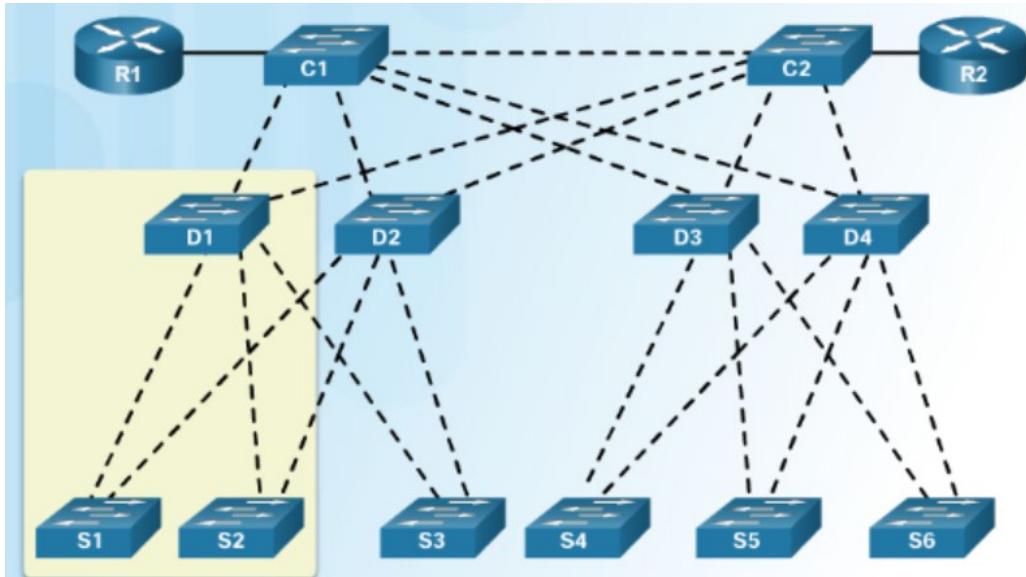


Abbildung 4.1: Ein neues VLAN verursacht Konfigurationsarbeit auf jedem Switch.

Bei grossen Netzen wäre es ein Riesenaufwand, auf jedem Switch von Hand eine und dieselbe VLAN-Konfiguration einzugeben. Änderungen sind ferner sehr fehleranfällig.

*Lösung:* **Zentrales Management** der VLANs. Dazu hat Cisco das VLAN Trunking Protocol, VTP, entwickelt. VTP erlaubt einem Administrator die VLANs auf *einem* Switch, der als VTP Server konfiguriert ist, zu verwalten. Der VTP Server verteilt und synchronisiert die VLAN Informationen über die Trunk-Leitungen zwischen den Switch. Dies minimiert die Probleme, die bei inkonsistenten VLAN-Konfigurationen entstehen können.

Vorteile von VTP:

- man hat eine konsistente VLAN-Konfigurationen über das ganze Netz
- es resultiert eine rasche Verteilung von Änderungen an alle Switch

*Gefahren:* Die automatische Verteilung der VLANs aus der VLAN-DB eines VTP-Servers kann zu Effekten führen, die der Administrator gar nicht beabsichtigte. Er muss genau verstehen, wie VTP abläuft.

**ACHTUNG:** Die VTP Konfigurationen werden nicht in der Datei `running-config` abgespeichert, sondern in der VLAN-Datenbank (`flash:vlan.dat`). Mit der Abfrage `show running-config` findet man keine Angaben zu VTP.

#### 4.1.2 VTP Begriffe

VTP Komponente	Definition
VTP Domain	Nur Switches in der gleichen VTP Domain tauschen Infos aus. Wird auf einem VTP Server ein Domain Name konfiguriert, so wird dieser Domain Name allen Nachbarn mitgeteilt. Voraussetzung ist, dass die Leitung zum Nachbarn als Trunk funktioniert. Die Nachbarn übernehmen den Domainnamen und machen nun beim VTP mit. Die VTP-Advertisements laufen über VLAN 1.
VTP Advertisements	-Jeder Switch in der Domain sendet periodisch advertisements auf jeden Trunk an eine reservierte Multicast Adresse. -Nachbar-Switch nehmen die advertisements entgegen und aktualisieren ihre VLAN Konfigurationen falls nötig.
VTP Passwort	VTP sollte mit einem Passwort geschützt werden
VTP Modi	Es gibt drei mögliche VTP Modi: Server, Client oder Transparent
VTP Server	Nur auf einem VTP Server können VLANs instanziert werden. Sie speichern die VLAN Informationen für die ganze Domain dauerhaft. Sie tauschen alle VLAN Information mit allen Switch der Domäne aus. Der VTP Mode Server ist default.
VTP Client	Auf VTP Clients können keine VLANs mehr instanziert werden. Sie speichern die VLAN Information nur im RAM. Sie tauschen aber ihre VLAN Information mit allen Nachbarn der Domäne aus.
VTP Transparent	Der Mode VTP Transparent bedeutet, dass ein Switch die VTP Information zwar weitergibt, aber nicht liest und anwendet.

#### 4.1.3 VTP Advertisements

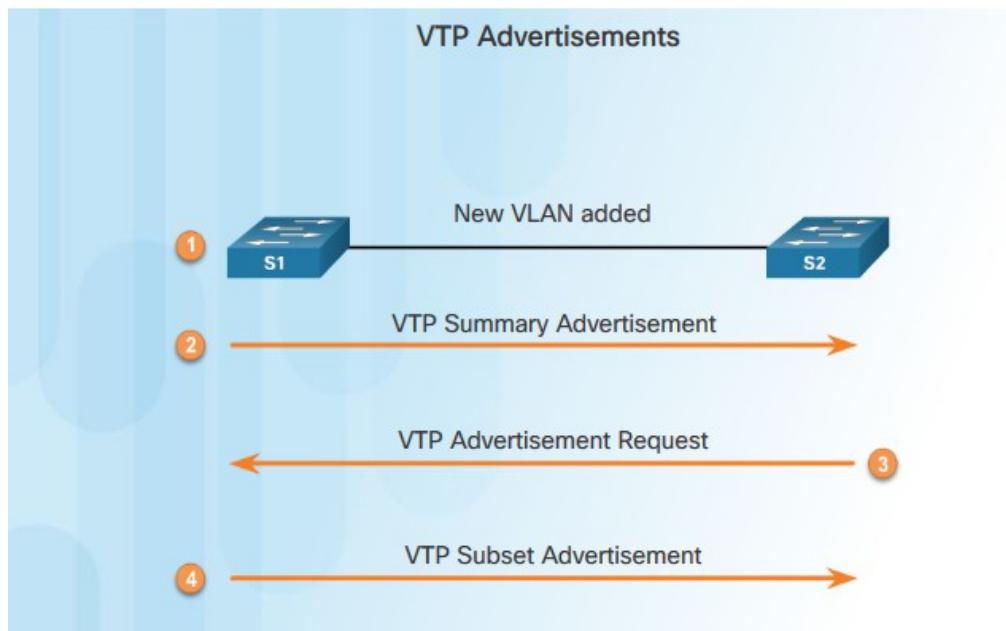


Illustration 4.2: Ablauf des Informationsaustauschs

**Summary Advertisement:** Informiert benachbarte Switch über VTP Domain Namen und die *configuration revision number*. Cisco Switch senden per defalut alle fünf Minuten ein summary advertisement. Die configuration revision number wird dazu benutzt, um festzustellen, ob ein Switch eine aktuelle oder eine veraltete VLAN-Konfiguration hat. Wenn ein Switch ein VTP Advertisement erhält, so vergleicht er dessen configuration revision number mit seiner eigenen. Ist seine configuration revision number gleich oder grösser als diejenige des Advertisements, so verwirft er es.

Ist sie kleiner, so versendet er ein **Advertisement Request**. Dieses verlangt ein **Subset Advertisement**, das die Infos über die Veränderungen enthält. Wenn auf einem VTP Server eine Veränderung der VLANs gemacht wird, so wird die configuration revision number inkrementiert und ein (oder mehrere) Subset Advertisement mit den Veränderungen verschickt.

VTP Advertisements werden an die Multicast MAC-Adresse 01-00-0C-CC-CC-CC gesandt. Es sind IEEE-Rahmen mit einem 802.1Q Tag.

#### 4.1.4 Die Default VTP Konfiguration eines Switch

Die VTP Parameter erhält man mit der Statusabfrage

```
Switch#show vtp status
```

Feld	Standardeinstellung	Bemerkung
VTP Version capable	1 – 3	Je nach IOS Version
VTP Version running	1	
VTP Domain Name	NULL	Muss gesetzt werden
VTP Pruning mode	disabled	
VTP Traps generation	disabled	
VTP Operating mode	Server	
Maximum VLANs supported locally	Hängt von der Switch Plattform ab	
Number of existing VLANs	5	VLANs 1, 1002-1005
Configuration Revision Nr. (32 bit Zahl)	0	Wird bei jeder Änderung der Konfiguration bezüglich VLANs inkrementiert. Synchronisiert den Zustand in der Domäne.
MD5 digest	16 byte	Authentifikation: checksum of the VTP configuration

Beachte: Der Default-Mode ist VTP-Server!

#### 4.1.5 VTP Sicherheitswarnung

Beim Einbau eines „neuen“ Switch in ein bestehendes LAN muss genau darauf geachtet werden, dass die VLAN- und die VTP-Konfiguration im Default-Zustand ist. Sonst können von diesem neuen Switch unter Umständen Falsch-Informationen verbreitet werden (Abb. 4.3).

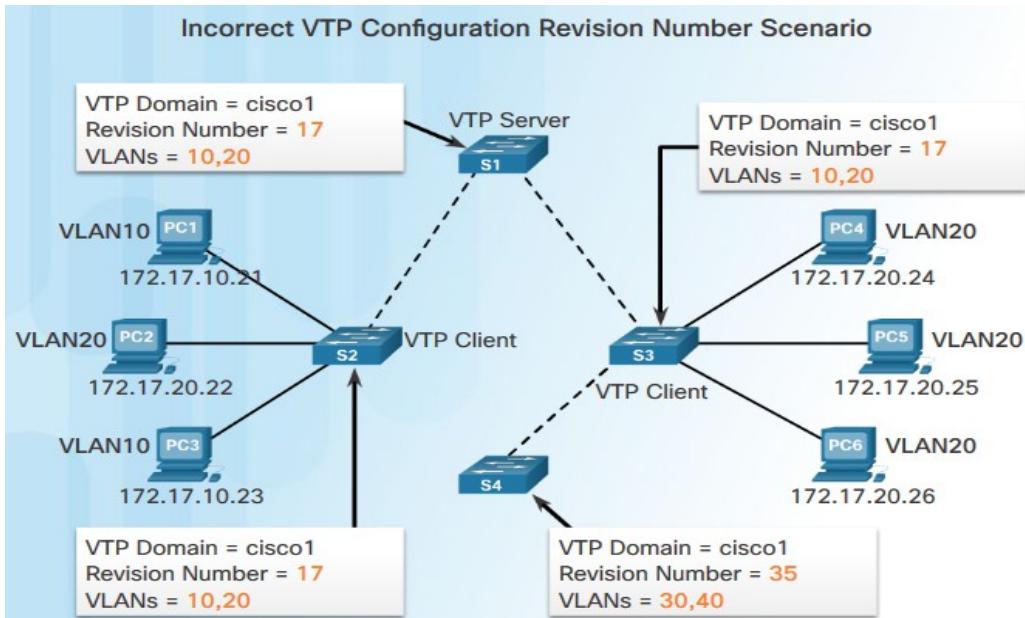


Illustration 4.3: Vorsicht beim Einfügen 'neuer' Switch

Wenn ein gebrauchter Switch mit einer höheren configuration revision number (Switch S4 in der Abbildung) in ein bestehendes Netz eingefügt wird, so überschreibt dessen VLAN Konfiguration alles bestehenden (S1 bis S3). Die Konfiguration *und* die VLAN Datenbank des Switch S4 müssen unbedingt vor dem Einfügen gelöscht werden.

#### 4.1.6 VTP Pruning

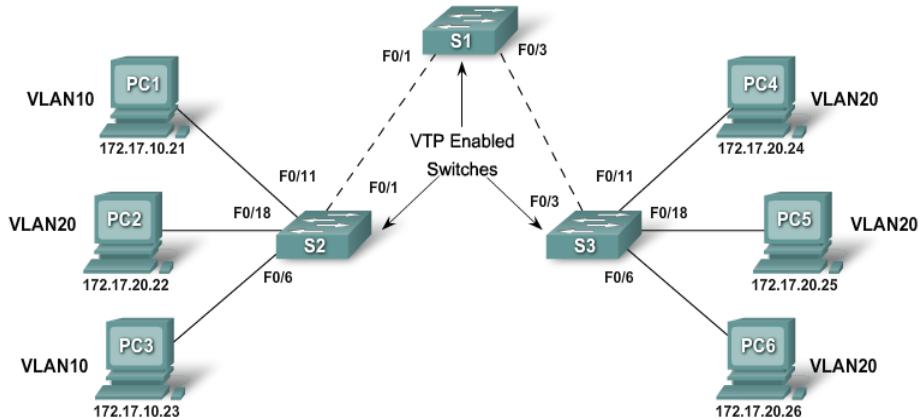


Abbildung 4.4: VTP Pruning: Switch S3 teilt S1 mit, dass er nur das VLAN 20 bedient.

Muss Switch S2 einen Broadcast von PC1 auf die Trunkleitung weiterleiten? Wenn S2 die Information hat, welche VLANs auf S3 vorkommen, dann ist das unnötig. Dazu benötigt man eine Kommunikation zwischen den Switches, welche VLANs an den Accessports tatsächlich konfiguriert sind. Broadcasts für VLANs, die am anderen Ende nicht vorkommen, können eingespart werden. Dies kann auch einen Sicherheitsvorteil bringen.

Pruning muss auf mindestens einem Server pro Domain eingeschaltet werden:

S1(config)#vtp pruning

#### 4.1.7 Konfiguration von VTP

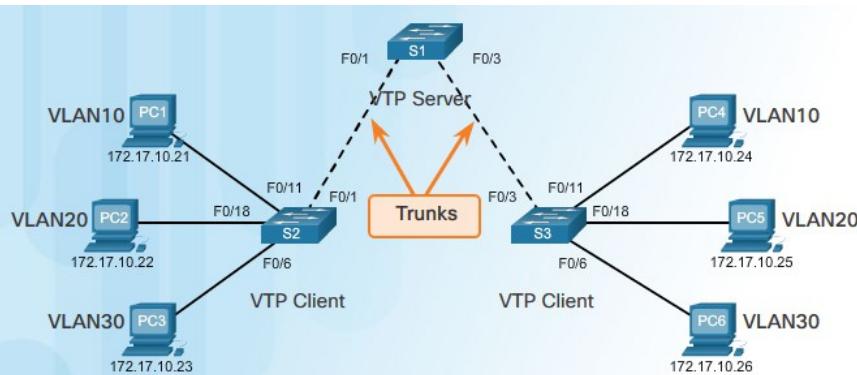


Illustration 4.5: Beispiel LAN für VTP Konfiguration

Voraussetzung: Die VLAN-DB wurde auf allen Switch gelöscht. Die Leitungen zwischen den Switch sind im Trunk Mode.

Vorgehen:

- (1) VTP-Konfigurationen auf dem beabsichtigten Server erstellen
- (2) Konfiguration der beabsichtigten Clients
- (3) Konfiguration der VLANs auf dem Server
- (4) Kontrolle, ob die VLANs verteilt wurden

Konfigurationen:

Die Konfiguration wird am Beispiel der Abb. 4.5 illustriert.

Zuerst ist zu kontrollieren, ob alle Switch im VTP Defaultzustand sind:

Switch#show vtp status

##### (1) Abfolge VTP server (Switch S1)

- domain name auf Server S1 konfigurieren.  
S1 (config) #vtp domain MyDomain
- Gewünschte VTP version wählen (version 1 ist default).  
S1 (config) #vtp version 2
- Authentifikation: Ein PW konfigurieren.  
S1 (config) #vtp password myPW

##### (2) Abfolge VTP client (Switch S2 und S3)

- client mode konfigurieren. Es können keine VLANs mehr konfiguriert werden.  
S2 (config) #vtp mode client
- VTP Domain Name, VTP version und VTP PW konfigurieren (wie auf dem Server).
- Kontrolliere VTP status: show vtp status

##### (3) Auf dem Server die VLANs konfigurieren

##### (4) Auf den Clients:

- Kontrolle: Haben alle VTP Client Switch die VLANs erhalten?
- Konfiguriere Access Ports und ordne Access Ports (erhaltenen) VLANs zu.

Achtung:

- VTP verteilt VLANs. VTP konfiguriert aber keine Ports! Dies muss immer noch von Hand gemacht werden.
- Am besten ist, man konfiguriert zwei Switch als Server. Geht ausgerechnet der Switch, auf dem man die VLANs konfiguriert kaputt, so ist die VLAN Konfiguration auf dem zweiten Server noch gespeichert.

## 4.2 Link Aggregation

### 4.2.1 Konzepte

Access-Layer Switch konzentrieren den Verkehr von  $N$  Teilnehmern und senden ihn an den Distribution Layer Switch. Damit mehrere Teilnehmer gleichzeitig die volle Access-Bandbreite zur Verfügung haben, müssen Massnahmen ergriffen werden. Dazu bestehen verschiedene Möglichkeiten:

- Die Leitungen zwischen den Switch wird mit einer höheren Bandbreite ausgestattet. Bsp.: Die Access-Leitung habe eine Bandbreite von 100 Mbps. Nimmt man eine Gbps-Leitung zwischen Access- und Distribution Layer, so kann man damit rechnen, dass etwa 8-9 Teilnehmer die volle Access-Bandbreite zur Verfügung haben werden. Schnellere IFs sind aber teuer und nicht immer vorhanden.
- Man legt mehrere Leitungen parallel zwischen zwei Switch. Allerdings wird das Spanning Tree Protocol redundante Leitungen blockieren (Abb. 4.6). Es ist nötig, redundante Leitungen logisch zu einem Bündel zusammenzufassen. Das Spanning Tree Protocol wird das Bündel als eine einzige Leitung behandeln, so dass alle Leitungen für die Übertragung benutzt werden können. Bei Cisco heisst so ein Bündel „EtherChannel“. Das virtuelle IF, das entsteht, wird „port channel“ genannt.

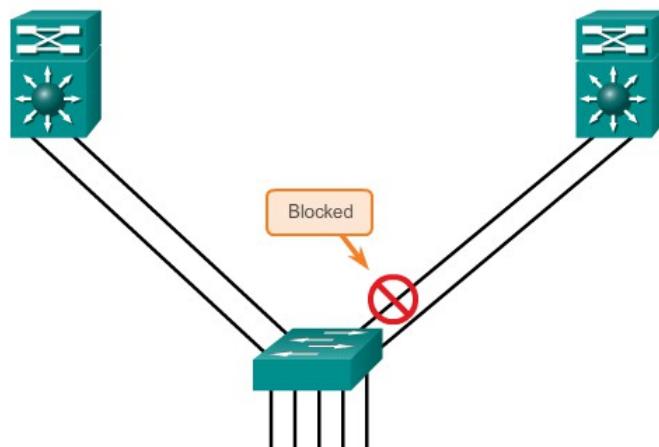


Abbildung 4.6: Das Spanning Tree Protocol sperrt redundante Leitungen und Schleifen zu vermeiden.

Ein EtherChannel ermöglicht eine bessere Ausnutzung der Bandbreite, in dem ein Load Balancing für verschiedene TCP-Verbindungen gemacht wird. Wird eine Leitung unterbrochen, so funktioniert

der Channel weiter – wenn auch mit geringerer Bandbreite – solange mindestens eine Leitung vorhanden ist.

Abb. 4.7 zeigt einen Switch mit zwei EtherChannels. Auf einem Switch können bis zu acht Leitungen zu einem EtherChannel zusammengefasst werden. Und unsere Switch unterstützen bis zu sechs PortChannels.

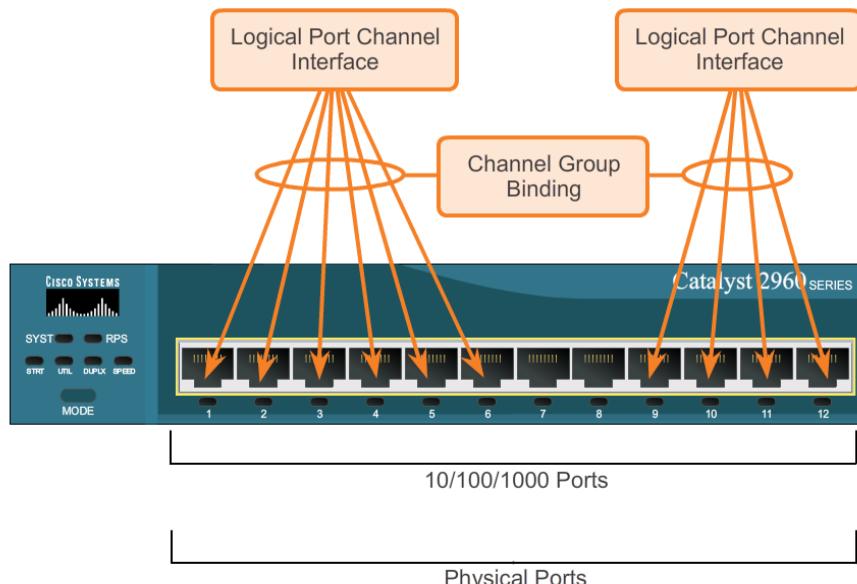


Abbildung 4.7: Beispiel: Zwei EtherChannel auf einem Switch

#### 4.2.2 Funktionsweise Etherchannel

Ein EtherChannel kann zwischen einem Switch und einem anderen Switch aufgebaut werden oder neuerdings auch zwischen einem Switch und einem Server, der EtherChannel unterstützt. Aber ein EtherChannel läuft immer nur zwischen **zwei** Geräten. Auf beiden Seiten müssen die Ports eines EtherChannels konsistent konfiguriert sein. Und die Kabel müssen die konfigurierten Ports richtig miteinander verbinden.

Zwischen den beiden Geräten muss ein Protokoll kontrollieren, ob die Ports konsistent konfiguriert und richtig miteinander verbunden sind. Dazu gibt es zwei Protokolle:

- PAgP: Port Aggregation Protocol, Cisco proprietär.
- LACP: Link Aggregation Control Protocol

```
AS01(config)#int range fa0/1 - 3
AS01(config-if-range)#channel-protocol ?
    lacp      Prepare interface for LACP protocol
    pagp      Prepare interface for PAgP protocol
```

PagP ist das Default Protokoll bei Cisco Switch. Achtung: Der PacketTracer Simulator unterstützt bis zur Version 6.2 nur PAgP. Es werden alle 30 Sekunden Pakete ausgetauscht, um zu kontrollieren ob ein Etherchannel aufgebaut werden soll / kann. Das Protokoll kontrolliert

- sind die gegenüberliegenden Enden auf einem und demselben Gerät?
- Sind die Bandbreite und der Duplex Mode auf beiden Seiten gleich?

- Werden dieselben VLANs unterstützt?

Wenn alle Konfigurationen übereinstimmen, so wird ein port channel aufgefaut und dem Spanning Tree Protocol als *eine* logische Leitung hinzugefügt.

Die Enden eines PortChannels auf einem Switch können in verschiedenen Modi konfiguriert werden:

- On,
- Desirable,
- Auto.

Je nach Kombination wird ein EtherChannel aufgebaut oder nicht.

Wahrheitstabelle:

S1	S2	Channel wird aufgebaut
On	On	Ja
Auto/Desirable	Desirable	Ja
On/Auto/Desirable	Keine Konfiguration	Nein
On	Desirable	Nein
Auto/On	Auto	Nein

LACP ist ein IEEE-Standard: 802.1AX. Es übernimmt dieselbe Funktion wie PAgP, jedoch unterscheidet es andere Port Modi:

- On
- Active
- Passive

S1	S2	Channel wird aufgebaut
On	On	Ja
Active/Passive	Active	Ja
On/Active/Passive	Keine Konfiguration	Nein
On	Active	Nein
Passive/On	Passive	Nein

Die Protokolle PAgP und LACP sollten nicht mit dem Dynamic Trunking Protocol, DTP, verwechselt werden. Bei den ersten beiden geht es darum zu kontrollieren, ob Ports gebündelt werden können. Bei DTP geht es darum, dass ein Link gegebenenfalls automatisch in den (VLAN-)trunk mode übergeht oder nicht.

#### 4.2.3 Konfiguration von Etherchannel

Wenn sich eine Port-Konfiguration (Duplex mode, Geschwindigkeit, VLAN) unterscheidet, so muss durch Konfiguration der Ports Übereinstimmung erzielt werden. Dies ist Voraussetzung.

Konfiguration mit PAgP:

Schritt 1: Wahl des Protokolls (optional) und Erstellen der channel group:

```
S2 (config) #interface range Fa0/3 - 4
```

```
S2(config-if-range) #channel-protocol pagp          //ist Defaultwert
                    #channel-group 1 mode {desirable | on | auto}
                    #exit
```

### Schritt 2: Konfiguration des Trunk-Mode

```
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk
```

## LACP

### Schritt 1:

```
S2(config)#interface range Fa0/3 - 4
S2(config-if-range) #channel-protocol lacp
                    #channel-group 1 mode {active | on | passive}
                    #exit
```

### Schritt 2:

```
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk
```

Der Schritt 1, die channel-group Konfiguration, muss auf beiden Switch vorgenommen werden.

Wie das load balancing dann tatsächlich gemacht wird, ist nicht ganz einfach. Rahmen einer TCP-Verbindung werden immer über das gleiche Kabel gesendet. Für jede Verbindung wird mit einer mathematischen Operation entschieden, über welches Kabel die Rahmen laufen. Als Kriterien können MAC-Adressen, IP-Adressen (Quelle oder Ziel) oder beides herangezogen werden:

```
AS01(config)#port-channel load-balance ?
dst-ip           Dst IP Addr
dst-mac          Mac Addr
src-dst-ip       Src XOR Dst IP Addr
src-dst-mac     Src XOR Dst Mac Addr
src-ip           Src IP Addr
src-mac          Src Mac Addr
```

Diese Konfiguration ist optional.

### **4.2.4 Status-Abfragen und Troubleshooting Etherchannel**

Statusabfragen:

```
show ip interface brief
show etherchannel
show etherchannel summary
show etherchannel port-channel
show interfaces etherchannel
```

### 4.3 Layer 3 Switching

Bisher wurde das Inter-VLAN-Routing mit 'Router-on-a-Stick' bewerkstelligt. Das funktioniert soweit gut. Im Sinne der Optimierung des LANs kommt nun die Frage, ob man das Inter-VLAN-Routing nicht gerade auf einem Distribution oder Core Switch erledigen könnte. Dieser Sachverhalt ist es in Abb. 4.8 dargestellt. Die Switch D1 und D2 erledigen das Routing zwischen den VLANs. Die Leitung zum Router R2 und der Router R2 selber werden dann nicht mehr beansprucht, um von einem VLAN in ein anderes zu gelangen. Dazu braucht es allerdings fortgeschrittene Switch mit einer integrierten Routing Funktionalität, z.B. C3560 oder C3650.

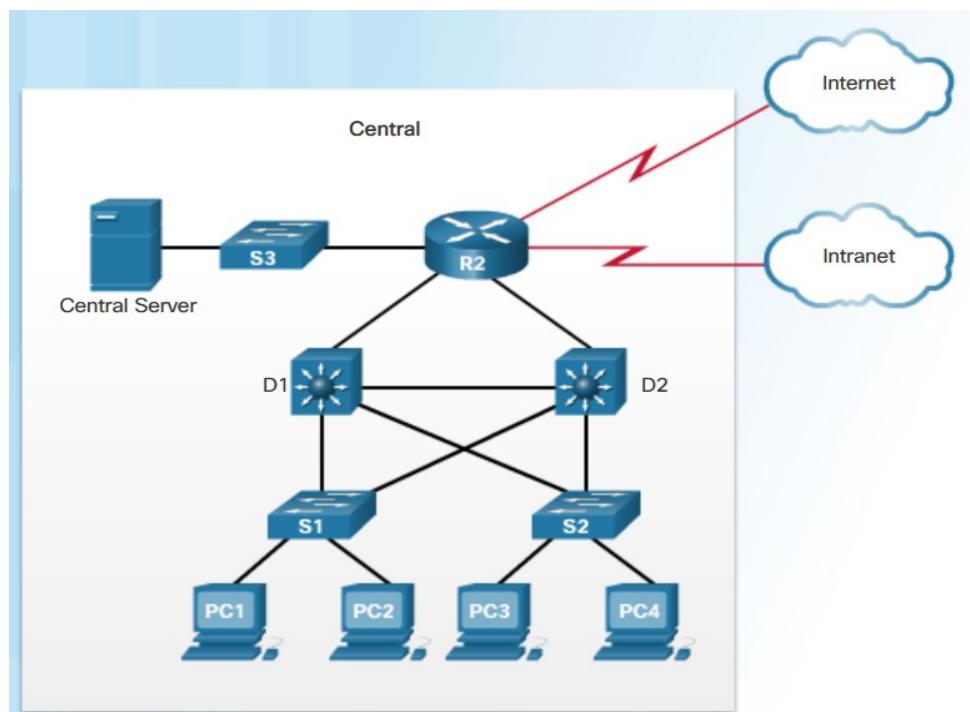


Abbildung 4.8: Layer 3 Switch in einem LAN

Es gibt zwei Arten von Schicht-3-IFs auf einem Layer 3 Switch:

- Routed Ports (wie Ports an einem gewöhnlichen Router) und
- switched virtual Interfaces (SVI).

Die Abb. 4.9 veranschaulicht 'routed ports' (in der Abb. 'Layer 3 Port' genannt) und SVI.

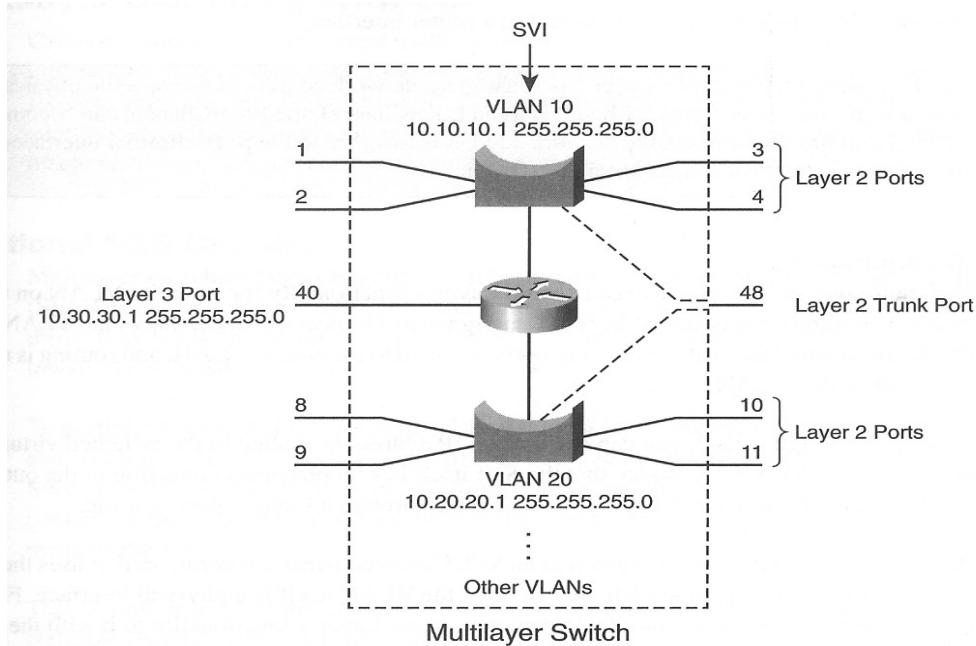


Abbildung 4.9: Funktionsschema eines Layer 3 Switch

#### 4.3.1 Routed Port

Zuerst muss auf einem Switch-3-Switch die Routingfunktionalität eingeschaltet werden:

```
S1(config)#ip routing
```

Ein *physikalischer* Port wird von der Switching Fabric getrennt und an den 'Route Processor' angeschlossen:

```
S1(config)#interface Fa0/40
S1(config-if)#no switchport
S1(config-if)#ip address 10.30.30.1 255.255.255.0
S1(config-if)#no shutdown
```

#### 4.3.2 Switched Virtual IF (SVI)

Ein *logisches* VLAN-IF wird mit der Routing-Funktion verbunden.

```
S1(config)#interface vlan 10
S1(config-if)#ip address 10.10.10.1 255.255.255.0
S1(config-if)#no shutdown
S1(config)#interface vlan 20
S1(config-if)#ip address 10.20.20.1 255.255.255.0
S1(config-if)#no shutdown
```

Damit wird ohne weitere Konfiguration zwischen SVIs und „routed Ports“ geroutet. Voraussetzung ist lediglich, dass mit `ip routing` eine Routerinstanz eingeschaltet wurde.

## 5 Wireless LAN

### Lernziele

- Sie kennen und verstehen die Unterschiede zwischen drahtgebundenen und drahtlosen LANs
- Sie kennen die wichtigsten Charakteristika der verschiedenen IEEE802.11x-Standards
- Sie kennen die Komponenten eines WLANs und können die Funktionsweise erklären
- Sie kennen die verschiedenen Service Sets bei WLAN
- Sie kennen die verschiedenen Schritte bei der Anmeldung eines Clients an einem WLAN gemäss IEEE 802.11 Standard
- Sie können die Einführung von WLAN-Anschluss in ein Firmennetz sinnvoll planen
- Sie kennen Vor- und Nachteile von drahtlosem Netzzugang
- Sie verstehen die Sicherheitsmaßnahmen in WLANs
- Sie kennen die Sicherheitsprotokolle für Firmennetze und für kleinere private Netze
- Sie können drahtlosen Netzzugang konfigurieren
- Sie können bei Fehlerzuständen die Ursachen identifizieren und beheben

### Kapitelaufbau

5.1 Konzepte Drahtloser Kommunikation

5.2 Funktionsweise Wireless LAN

5.3 Sicherheit in Wireless LAN

## 5.1 Konzepte Drahtloser Kommunikation

### 5.1.1 Übersicht drahtlose Kommunikation

Der Vorteil von drahtloser Kommunikation liegt in der Mobilität: Da auf Kabel verzichtet werden kann, kann sich ein Client frei bewegen. In einem Wohnhaus beispielsweise müssen keine Kabel mehr verlegt werden.

Dieses Mobilität hat aber auch einen Preis.

- Wir sind heute dauernd elektromagnetischer Strahlung ausgesetzt. Besonders in Räumen mit vielen Leuten, z.B. In Schulzimmern, wird die Leistung elektromagnetischer Strahlung wegen der vielen Clients auf engem Raum doch erheblich und man sollte mögliche Folgen für die Gesundheit nicht ganz ausser Acht lassen.
- Der Kommunikationskanal „Luft“ wird mit jedermann geteilt. Die Bandbreite wird geteilt. Jedermann kann mithören. Jedermann kann (in den WLAN-Frequenzbändern) stören.

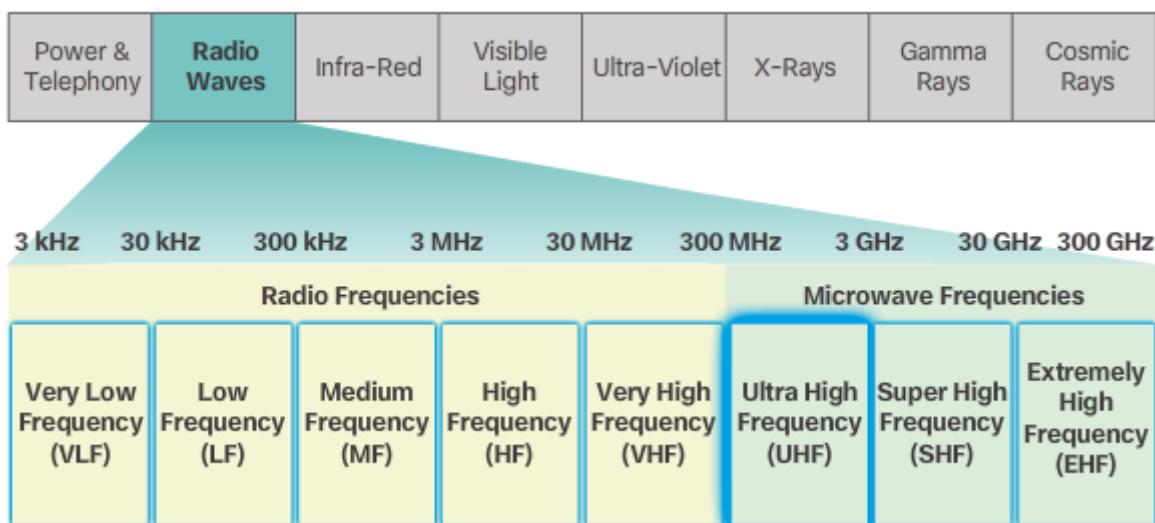


Abbildung 5.1: Frequenzbänder

Abb. 5.3 Gibt eine Übersicht über Frequenzbänder.

	UHF	SHF	EHF
Wellenlängen			
Anwendungen	WLAN (2.4 GHz) Bluetooth Mobilfunk Fernsehen Mikrowellenofen GPS	WLAN (5 GHz) Mikrowellenverbindungen Satelliten Kommunikation Radio Astronomie	WiGig WLANs (60 GHz) Radar Systeme

Tabelle 5.1: Anwendungen in Frequenzbändern

Übersicht über verschiedene Einsatzbereiche nach Übertragungsstrecken:

- Wireless Personal Area Network, WPAN. Distanzen: Ein bis zwei Meter. Standard: Bluetooth IEEE 802.15.
- Wireless LANs, WLAN. Distanzen: Bis ca. hundert Meter. Standard: IEEE802.11 WLAN, bekannt unter dem Namen WiFi.
- Mobilfunk für Telefonie. 2. Generation (GSM, 1991), 3. Generation (UMTS, 2001), 4. Generation (LTE)
- Worldwide Interoperability for Microwave Access, WiMAX. Distanzen: bis 50 km. Standards: IEEE802.16. Netz-Zugangstechnologie.
- Satelliten Kommunikation.

In unserem Kurs beschränken wir uns auf WLAN.

Tabelle 5.2 gibt eine Übersicht über die aktuellen WLAN-Standards, welche Frequenzräume sie belegen und wie es um die Kompatibilität mit älteren Standards steht. Der Standard 802.11 wurde von IEEE im Jahr 1997 herausgegeben und ist heute obsolet. Mit dem Standard 802.11ac (auch Wi-Fi 5 genannt) kam 2016 zum ersten Mal das Feature MU-MIMO (Multi User MIMO). Im downstream kann der Access Point Daten an zwei Benutzer gleichzeitig senden. Der neue Standard 802.11ax (Wi-Fi6) war für Februar 2021 angekündigt.

Standard	Max. Datenrate Mbps	Frequenzband GHz	Modulation	Rückwärts-Kompatibilität
IEEE802.11g	54	2.4	OFDM	
IEEE802.11n	600	2.4 / 5	OFDM, MIMO	802.11g
IEEE802.11ac Wi-Fi5	1300	5	OFDM, MIMO	802.11n
IEEE802.11ax WiFi6	4000	2.4 / 5 / 6	OFDM, MIMO	802.11ac/n

*Tabelle 5.2: Standards für drahtlose LAN. OFDM: Orthogonal Frequency Division Multiplexing, MIMO: Multiple Input Multiple Output.*

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

*Abbildung 5.2: Vergleich von WLAN und LAN Technologie*

Drei Organisationen sind für die Standardisierung der Kommunikation und für die Interoperabilität von Geräten zuständig.

- Die **ITU-R** regelt die Belegung der Frequenzbänder. Dabei werden den nationalen Verbänden gewisse Freiheiten eingeräumt.

- Der **IEEE** hat Modulation standardisiert, hat aber keine Herstellungsstandards festgelegt, was zu Interoperabilitätsproblemen führen kann.
- Die **WiFi Alliance** ist eine von Industrien getragene Organisation, die die Interoperabilität prüft und zertifiziert.

WLAN hat keine klaren Grenzen. Alle Teilnehmer teilen sich den Kanal. Ein Teilnehmer hat keinen Schutz gegen andere Teilnehmer. Weder bezüglich Abhören noch bezüglich Stören. Die Frequenzbänder werden national geregelt. Es gibt keine international gültigen Standards.

Die MAC-Schicht (Medium Access Control) ist bei WLAN anders als bei LAN. Deshalb werden auch verschiedene Rahmen benötigt.

### 5.1.2 Komponenten von WLANs

Typische Komponenten in einem Heimnetz:

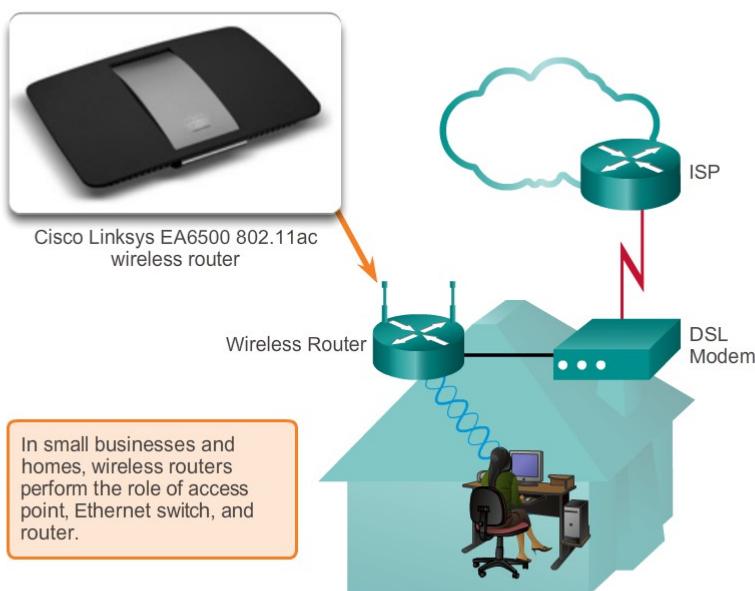
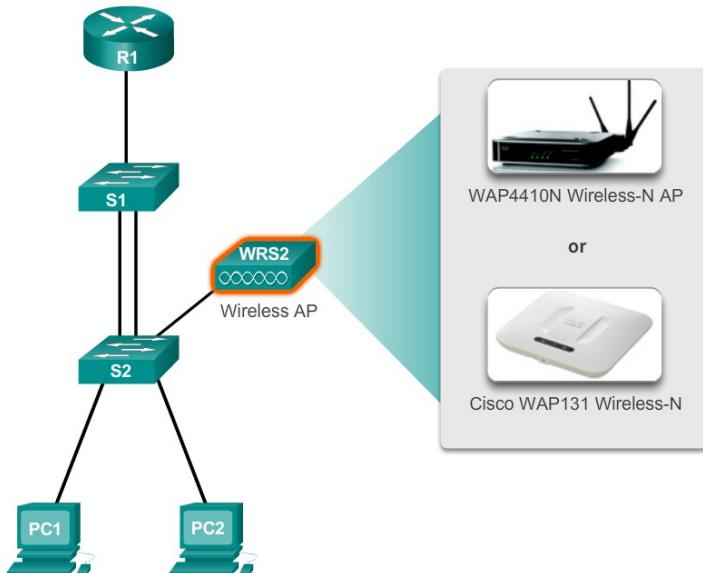


Abbildung 5.3: Typischer Aufbau eines WLANs in einem Heimnetz

Entweder sind Wireless Router und das Modem zwei separate Geräte (im Falle von Cable Modems) oder beide Funktionen sind in einem Gerät untergebracht (DSL Anschlüsse). Während WLAN Adapter für Rechner früher eigene Komponenten waren, sind sie heute meist im Rechner integriert.

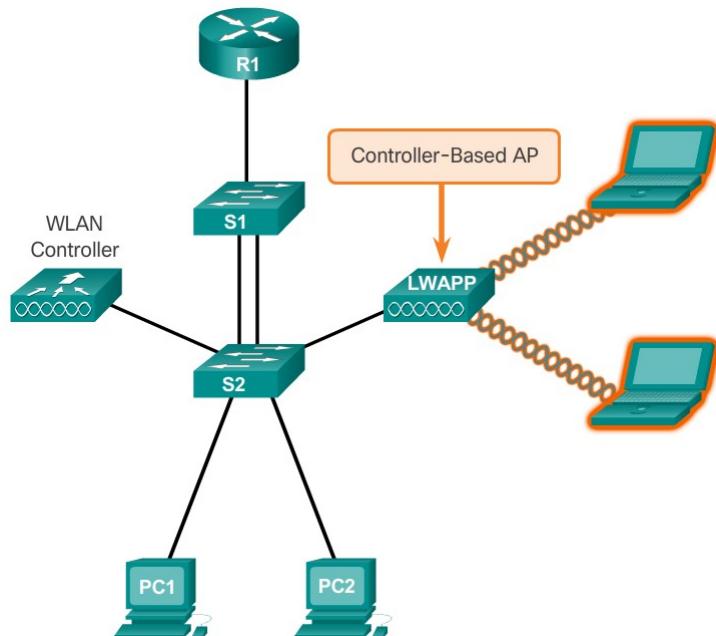
Kleinere und mittlere Betriebe:



*Abbildung 5.4: WLAN Komponenten in einem mittleren Betrieb mit autonomen Access Points.*

Das Netz hat eine Switching Infrastruktur mit einem oder mehreren Wireless Access-Points (APs). Jeder AP wird einzeln konfiguriert über ein User Interface, meistens ein Web-IF.

Grosse Betriebe: Ein WLAN hat soviele APs, dass der Betreiber es vorzieht, die APs zentral von einem WLAN-Controller aus zu konfigurieren.



*Abbildung 5.5: Grosse Netze mit Light Weight Access Points, die von einem WLAN Controller konfiguriert werden.*

Der WLAN-Controller kann sowohl eine Hardware in der Switching Infrastruktur als auch eine Software irgendwo in einer „Cloud“ sein (Cisco: Meraki cloud).

Bei den Antennen für WLAN unterscheidet man

- Omnidirectional Wi-Fi Antennas: Dipol-Antennen strahlen punktsymmetrisch in 360° ab. Es ist die häufigste Antennenform und wird typischerweise in Büros eingesetzt.
- Directional Wi-Fi Antennas: Sie bündeln die Strahlung in eine Richtung. Sie werden gebraucht, um Ecken „auszuleuchten“, die sonst zu wenig Signal erhalten.
- Yagi antennas: Diese Art von gerichteten Antennen kann WLAN-Verbindungen über lange Distanzen benutzt werden. Beispielsweise können schwer zugängliche, abgesetzte Standorte mit Yagi Antennen erschlossen werden.



Abbildung 5.6: Verschiedene Arten von Antennen.

### 5.1.3 802.11 WLAN Topologien

Es werden zwei Topologien unterschieden:

- Ad Hoc Mode: Die Clients kommunizieren direkt, ohne AP. Man nennt diese Topologie Independent Basic Service Set, IBSS.

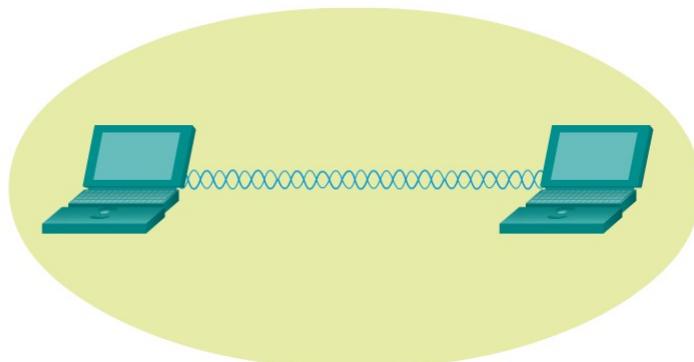
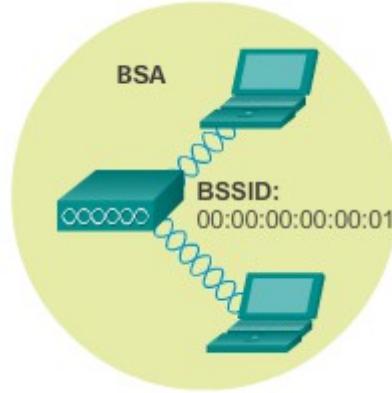
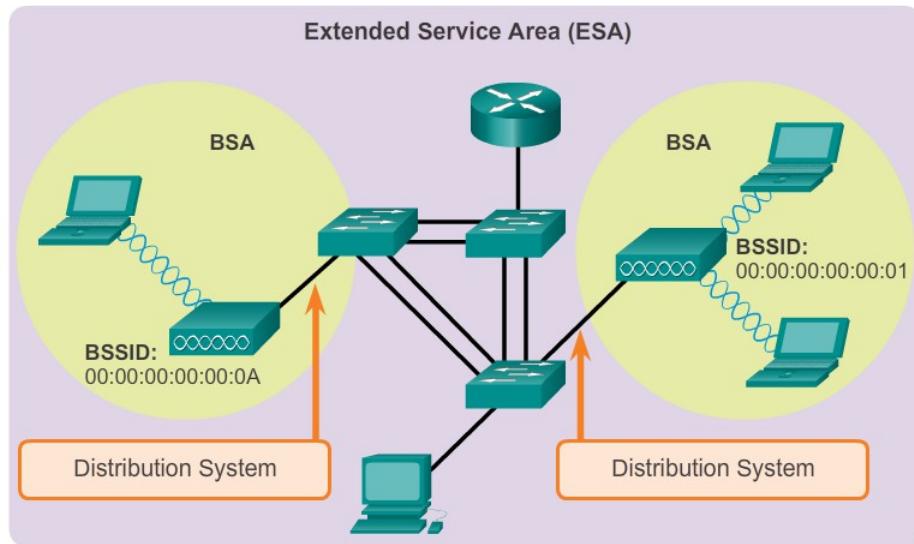


Abbildung 5.7: Ad Hoc Mode

- Infratruktur Mode: Die Clients kommunizieren über einen AP. Man unterscheidet zwei Fälle.



*Abbildung 5.8: **Basic Service Set**, BSS: Ein AP bedient alle Clients in einer Basic Service Area, BSA.*



*Abbildung 5.9: **Extended Service Set**, ESS.*

Im Extended Service Set kann ein Client andere mobile Clients in der ganzen extended service area, ESA, erreichen, d.h. Clients in verschiedenen basic service areas (BSA). Ein Client kann sich aus einer BSA in eine andere bewegen und behält dabei die Verbindung (roaming).

## 5.2 Funktionsweise Wireless LAN

Access Points (AP) arbeiten wie ein Hub: Der Kommunikationskanal (die Luft) ist ein „Shared Medium“. Das Kanalzugriffsverfahren lautet CSMA/CA. CA: Collision Avoidance. Hier ist also ein Unterschied zum Zugriffsverfahren bei Ethernet mit Collision Detection (CD). Bei drahtlosem Zugang müssen Kollisionen im Voraus vermieden werden.

Hidden node problem: PC1 und 2 hören einander nicht. Beide hören aber den AP.

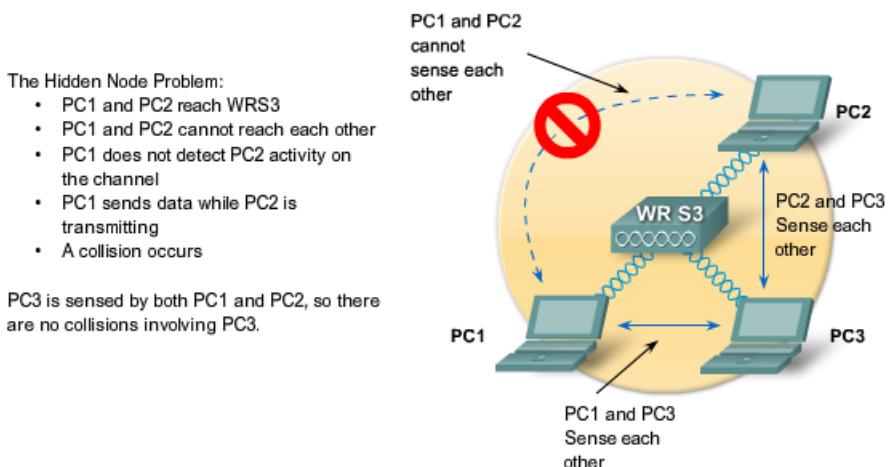


Abbildung 5.10: Das hidden node Problem

Damit keine Kollisionen auftreten, muss der Kanal Zugriff geregelt werden. Eine mögliche Art und Weise: Request to send (RTS), clear to send (CTS). Dabei ordnet eine zentrale Stelle (der AP) den Kanal *einem* Sender zu.

### 5.2.1 Kanalzugriffsverfahren

#### Kanalzugriffsverfahren:

Wegen der hidden node Problematik definierte der IEEE ein zweites Kanalzugriffsverfahren, CSMA/CA, Collision Avoidance. Es stellt sich hier die Frage, ob Kollisionen überhaupt vermieden werden können und wenn Ja, wie?

Kollisionen lassen sich nicht ganz, aber weitgehend ausschliessen. Deshalb muss bei WLAN jeder Datenrahmen, der richtig empfangen wurde, bestätigt werden (ACK, Steuernachricht). Wird ein Rahmen nicht bestätigt, so muss der Sender ihn nochmals senden.

IEEE 802.11 sieht für die *Distributed Foundation Wireless Medium Access Control (DFWMAC)* drei Ansätze vor, Kollisionen zu verhindern:

- (1) Einfaches DFWMAC mit CSMA/CA (notwendig)
- (2) DFWMAC mit RTS/CTS Erweiterung (Anwendung optional)
- (3) DFWMAC mit Polling (Unterstützung optional)

Die Ansätze (1) und (2) bilden zusammen die ‚distributed coordination function‘ (DCF). Der dritte Ansatz wird ‚point coordination function‘ genannt (PCF). Er wird heute in der Praxis kaum angewandt und wird der Vollständigkeit halber erwähnt.

Zuerst benötigen wir die Klärung einiger Begriffe.

**Inter-Frame Spacing (IFS):** Das IFS ist der mindeste Abstand zwischen zwei Rahmen.

Es gibt drei verschiedene IFS:

- Short IFS (SIFS): Für Rahmen mit höchster Priorität (z.B. Bestätigungen); 10 ms für Direct Sequence Spread Spectrum Übertragung (DSSS).
- PCF IFS (PIFS): Stellt die IFS für PCF (3) dar.
- DCF IFS (DIFS): Für gewöhnliche Rahmen (niedrige Priorität) in der DCF (1) und (2).

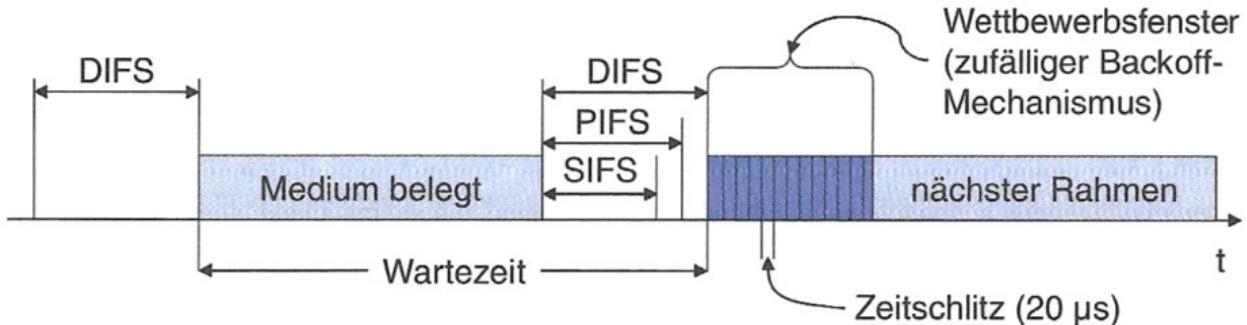


Abbildung 5.11: Erklärung der verschiedenen Inter Frame Spacings (IFS).

**CCA Signal:** Die physikalische Schicht stellt der Schicht 2 das Clear Channel Assessment Signal, CCA, zur Verfügung. Es besagt, ob der Kanal frei ist oder nicht.

**Zeitschlitz Ts (Slot Time):** die maximale Zeit, die von Beginn des Sendens eines Rahmens verstreichen kann, bis das CCA Signal jedes Empfängers anzeigen, dass der Kanal belegt ist (Signal-Ausbreitungszeit + Verarbeitungszeit im Empfänger).

### (1) Einfaches DFWMAC mit CSMA/CA

Jede Implementation des IEEE-802.11-Standards muss das CSMA/CA Verfahren unterstützen.

- Falls geringe Last vorliegt (der Kanal war für  $t > \text{DIFS}$  frei): Eine Station darf unmittelbar nach Ablauf der DIFS senden. Kein Wettbewerb.
- Falls mehrere Stationen im Wettbewerb sind: Jede Station, die Senden möchte, „würfelt“ eine Zahl  $n$  ( $0 < n < N$ ) und wartet nachdem der Kanal frei geworden ist während einer zufälligen Backoff-Zeit  $\text{DIFS} + n * \text{Ts}$  bevor er sendet. Falls bis dahin ein anderer zu senden begonnen hat, so muss er warten.

In dieser Ausführung wäre das CSMA-CA Verfahren nicht fair. Es könnte vorkommen, dass eine Station nie dran kommt. Fairness: Falls eine Station den Wettbewerb um den Kanalzugang verloren, so hält sie den Zähler an und bestimmt keine neue Zufallszahl  $n$ . Wenn wieder ein Wettbewerbsfenster kommt, so zählt sie weiter herunter.

Eine Kollision zerstört i.A. den Empfang der Daten. Übertragungswiederholungen werden nicht bevorzugt: Die Stationen müssen eine neue Zahl  $n$  würfeln.

WLAN-IFs müssen sich automatisch an die aktuellen Lastverhältnisse anpassen. Grosse Last: Grosses  $N$ ; kleine Last: kleines  $N$  (exponential backoff).

Bestätigung: Wurde ein Datenrahmen richtig übertragen, so muss er bestätigt werden. Der Empfänger muss nur die Zeitspanne SIFS abwarten.

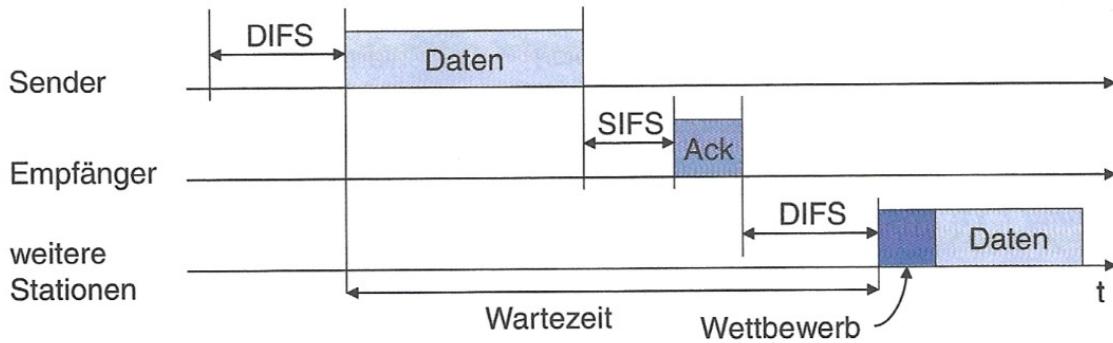


Abbildung 5.12: Priorisierung von Bestätigungsrahmen

**Beispiel:** CSMA-CA mit fünf Stationen und einer Kollision

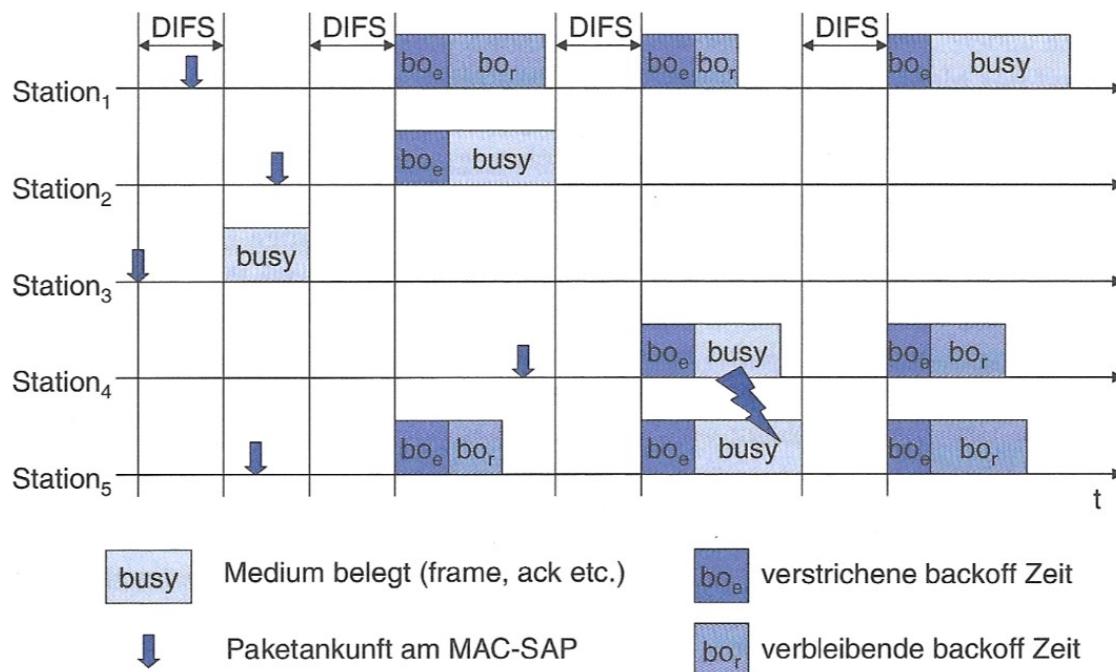


Abbildung 5.13: Beispiel von CSMA-CA mit einer Kollision.

$bo_e$ : elapsed backoff time;  $bo_r$ : residual backoff time

Nachdem die Station 3 den Kanal belegt hat möchten sowohl die Stationen 1, 2 als auch 5 senden. Die Station 2 kommt aufgrund ihres Zählers als erste dran und darf den Kanal belegen. Während dieser Sendezeit möchte die Station 4 auch mit Senden beginnen und würfelt eine Wartezeit. Diese ist zufälligerweise genau so gross wie die verbleibende Wartezeit für die Station 5. Nach Abschluss des Sendens der Station 2 wird eine Zeit DIFS + verbleibende Wartezeit gewartet. Die Stationen 4 und 5 beginnen zufälligerweise gleichzeitig zu senden und produzieren eine Kollision. Darauf hin muss wieder eine Zeit DIFS gewartet werden. Die Stationen 4 und 5 müssen neu würfeln. Bei Station 1 wird der Timer als erster ablaufen und sie darf senden.

## (2) DFWMAC mit RTS / CTS

RTS: Request to Send; CTS: Clear to Send.

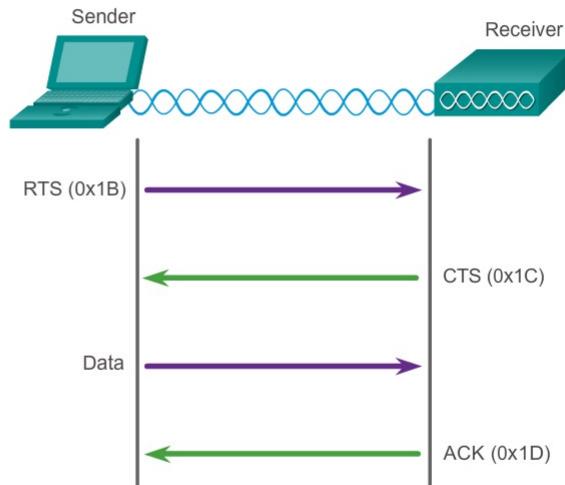


Abbildung 5.14: Zwei-Weg Hand Shake bei WLAN

Das Verfahren RTS/CTS löst das Problem versteckter Knoten. Die Anwendung dieses Verfahrens ist optional; aber jeder Knoten muss richtig auf RTS-/CTS-Rahmen reagieren können. Es müssen also alle Knoten das Verfahren unterstützen.

Die RTS-Rahmen sind kurz und enthalten ein Feld mit der Dauer der gesamten Übertragung (Senden plus Bestätigung). Jede Station, welche einen RTS-Rahmen empfängt, muss die Dauer der Kanalbelegung in ihrem **Net Allocation Vector** (NAV) speichern. Der NAV gibt den frühestmöglichen Zeitpunkt an, zudem eine dritte Station wieder versuchen darf, auf den Kanal zuzugreifen.

Der Empfänger eines RTS-Rahmens antwortet nach der Zeit SIFS mit einem CTS-Rahmen (priorisierte Rahmen), der die Dauer der Belegung enthält. Alle Stationen, die diesen Rahmen empfangen, müssen ihren NAV entsprechend anpassen. Auch ein „versteckter Knoten“. Ein „shared medium“ wird durch RTS/CTS virtuell für eine bestimmte Dauer für zwei Stationen reserviert.

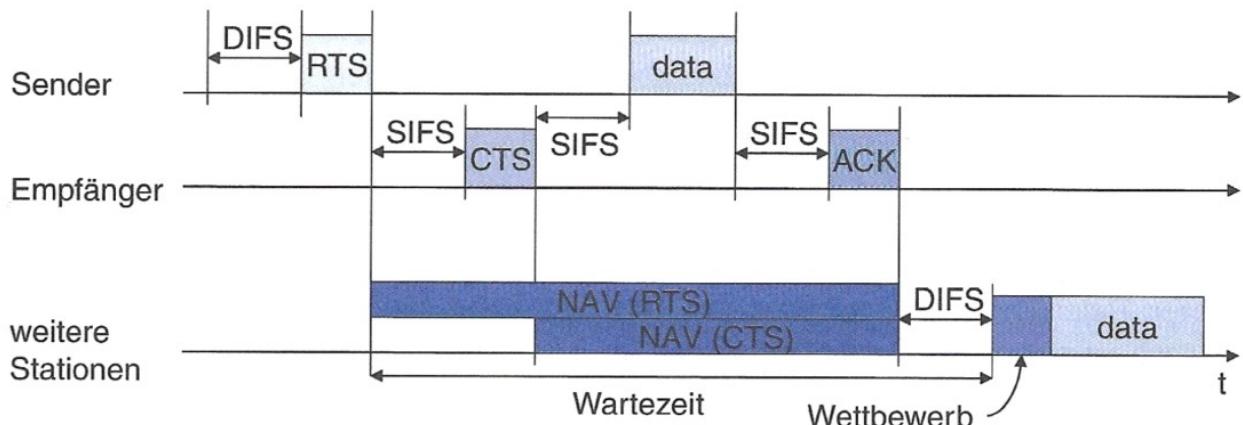


Abbildung 5.15: Reservierung des Kanals für zwei Knoten mittels RTS/CTS.

Vorteile und Nachteile von RTS/CTS:

- Kollisionen mit einem „hidden node“ können nur noch zu Beginn, nämlich beim Senden des

RTS, auftreten. Die RTS-Rahmen sind sehr kurz (siehe Abschnitt 802.11 Rahmen).

- Der RTS/CTS-Mechanismus bedeutet einen zusätzlichen Overhead. Er vermindert den Durchsatz und erhöht die Zugriffsverzögerung.
- Er bringt Vorteile, wenn zwei Endgeräte, die sich gegenseitig nicht sehen, etwa gleichzeitig längere Rahmen senden möchten.
- Oft wird ein RTS-Schwellwert eingesetzt, der bestimmt, ab welcher Rahmengröße der Mechanismus eingesetzt wird.

### 5.2.2 Anmeldung am Access Point

Anders als bei Ethernet muss sich ein wireless client bei einem AP zuerst anmelden. Dies geschieht in drei Schritten:

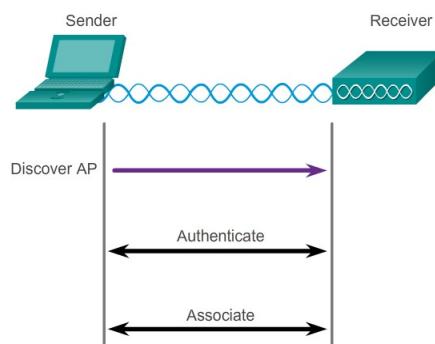


Abbildung 5.16: Anmeldung eines Clients am AP

Angenommen es gebe mehrere wireless networks in einer Umgebung, so muss man diese unterscheiden können. Dies geschieht mit der SSID. Die SSID ist der Name eines wireless networks. Discover:

Es gibt zwei mögliche Verhalten eines APs:

- Passive Mode: Der AP gibt seine SSID in regelmässigen Abständen mit einem Beacon Frame (Management Frame mit Frame Subtype 0x08) allen bekannt (passive mode: Der Client muss a priori nichts wissen). Im Beacon stehen: SSID, supported standards, security settings.

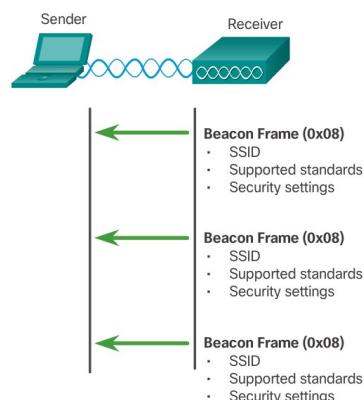


Abbildung 5.17: Passive Erkennung eines WLANs mittels Beacon Rahmen

- Active Mode: Die Clients müssen die SSID a priori kennen und initiieren die Anmeldung.

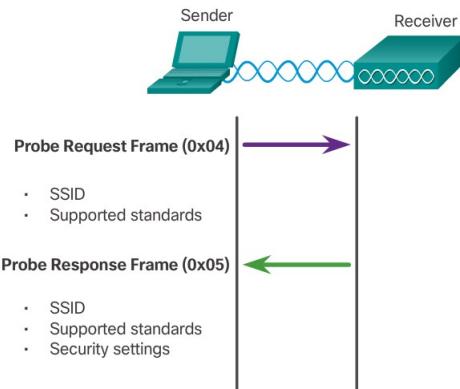


Abbildung 5.18: Aktive Erkennung eines WLANs

Der Client sendet einen Probe Request (frame subtype 0x04), der AP antwortet mit einer Probe Response (subtype 0x05).

### Authentisierung

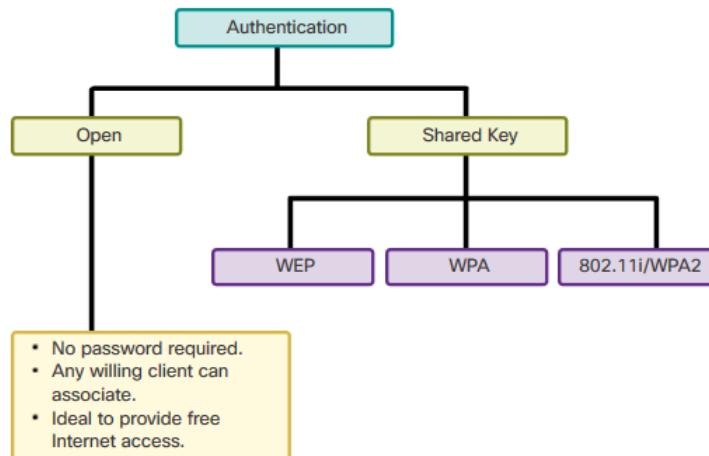


Abbildung 5.19: Authentisierungsvarianten

WEP: Wired Equivalence Privacy. Gilt nicht mehr als sicher.

WPA: WiFi Protected Access. Zwischenlösung mit besserer Sicherheit.

802.11i/WPA2: Die heute übliche Lösung von drahtgebundenen Systemen. Hohe Sicherheit.

### Association

- Der Client sendet einen Association Request (frame subtype 0x00) mit seiner MAC-Adresse
- Der AP antwortet mit einer Association Response (subtype 0x01) mit seiner MAC-Adresse. Der AP erstellt eine Association ID, AID für diesen Client. Eine AID ist ein logischer Port für diesen Client.

#### 5.2.3 Kanalzuteilung

Bei den verschiedenen 802.11-Standards kommen folgende Modulationsarten zum Zug:

- DSSS: Direct Sequence Spread Spectrum
- OFDM: Orthogonal Frequency Division Multiplexing
- MIMO: Multiple Input, Multiple Output. Über mehrere Sende- und Empfangsantennen werden zur gleichen Zeit auf der gleichen Frequenz Signale übermittelt. Dank

unterschiedlichen Wegen (spatial multiplexing) können diese Ströme herausgerechnet und kombiniert werden.

Diese Modulationsarten belegen verschiedenartige Spektralbereiche.

Frequenzbänder:

- UHF: 2.4 GHz ISM (Industrial, Scientific, Medical) Band. Es handelt sich um ein freies Band, welches ohne Lizenz genutzt werden darf. Es gibt also keine Garantien, dass WLAN ungestört funktioniert.
- SHF: 5 GHz Band.
- Neu: EHF 60 GHz. Diese Strahlen durchdringen keine Wände und benötigen Sichtverbindung.

Microwave Frequencies		
Ultra High Frequency (UHF)	Super High Frequency (SHF)	Extremely High Frequency (EHF)
2.4 GHz WLANs	5 GHz WLANs	60 GHz WLANs
✓ 802.11b	✓ 802.11a	✓ 802.11ad
✓ 802.11g	✓ 802.11n	
✓ 802.11n	✓ 802.11ac	
✓ 802.11ac	✓ 802.11ad	

Abbildung 5.20: Belegung der Frequenzbänder durch die verschiedenen Versionen

	802.11a	802.11b	802.11g	802.11n
<b>Frequenzband</b>	5.7 GHz	2.4 GHz	2.4 GHz	2.4 GHz / 5.7 GHz
<b>Modulation</b>	OFDM	DSSS	OFDM	OFDM-MIMO
<b>Bruttodatenrate</b>	bis zu 54 Mb/s	bis zu 11 Mb/s	bis zu 54 Mb/s	bis zu 150 Mb/s pro Stream bei 40 MHz Kanalbandbreite, maximal 4 Streams.
<b>Kanalbandbreite</b>	20 MHz	22 MHz	20 MHz	20 / 40 MHz
<b>Anzahl Interferenzfreie Kanäle</b>	bis zu 23, je nach Land	3 (Kanäle 1, 6, 11)	4 (Kanäle 1, 5, 9, 13)	2 im 2.4 GHz Band, bis zu ca. 12 im 5.7 GHz Band, je nach Land
<b>Reichweite</b>	ca. 35m, je nach Abstrahlleistung	ca. 35 m	ca. 35m	ca. 70 m
<b>Bemerkungen</b>	Kürzere Antennen, weniger Interferenzen durch Consumer Electronics.	Interferenzen durch Bluetooth, Mikrowellenöfen, etc.	Interferenzen durch Bluetooth, Mikrowellenöfen, etc.	

	Reichweite je nach Kanal schlechter als oder vergleichbar mit 802.11b, dank höherer Abstrahlung.		
--	--	--	--

## Beispiel 2.4 Ghz-Band

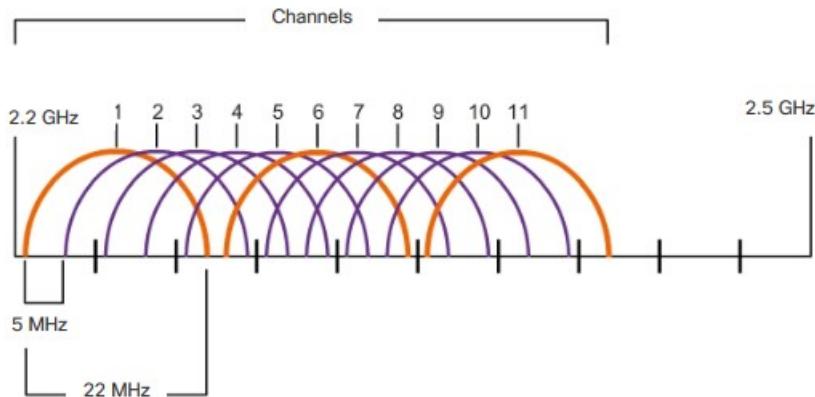


Abbildung 5.21: Alle Kanäle und nicht überlappende Kanäle im Frequenzband IMS

Best Practise: Konfiguriere Access Points so, dass sie nicht überlagernde Kanäle belegen. Viele APs wählen den Kanal automatisch, manche sogar dynamisch.

Alternative mögliche Wahl der Kanäle:

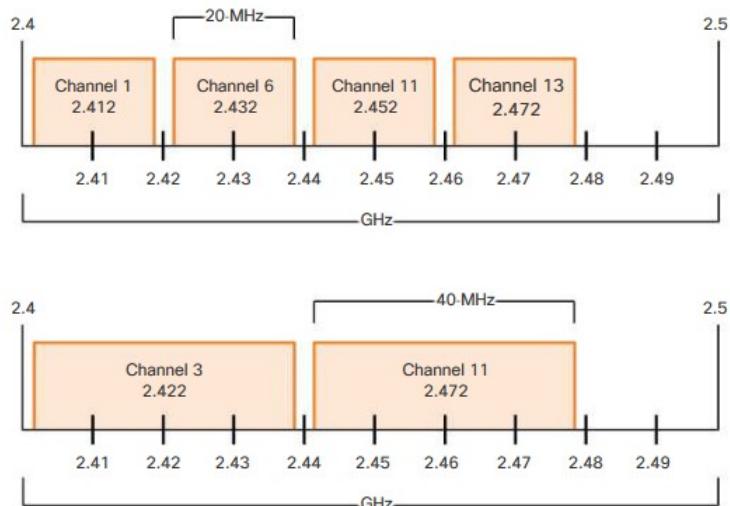


Abbildung 5.22: a) Vier Kanäle für 802.11g/n mit OFDM und b) zwei Kanäle mit 40 MHz Bandbreite bei 802.11n mit OFDM. Mit b) lassen sich höhere Datenraten erzielen.

### 5.2.4 802.11 Rahmen

Da bei WLAN ein anderes MAC-Protokoll benötigt wird als bei Ethernet, sieht auch der WLAN-Rahmen anders aus.

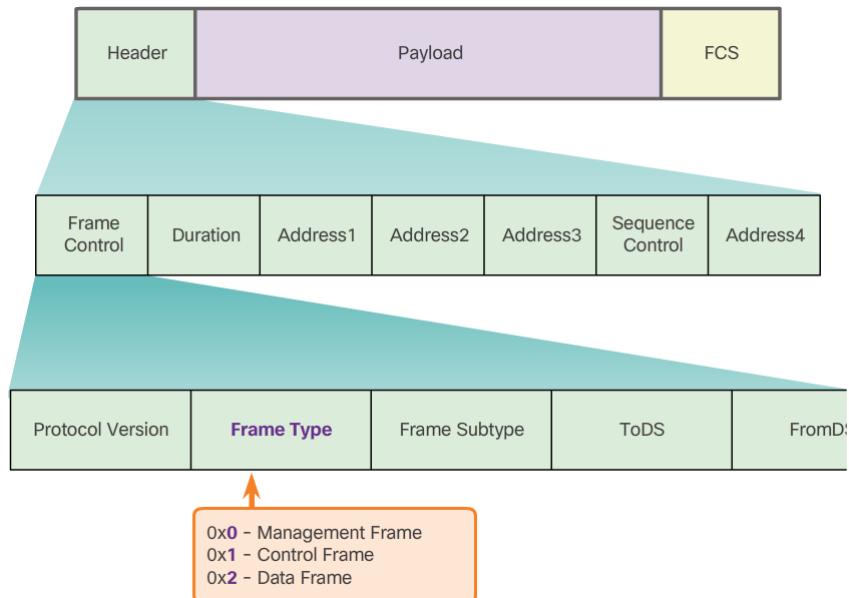


Abbildung 5.23: Die verschiedenen Typen von WLAN Rahmen

Die wichtigsten Parameter:

- Frame Control: Enthält Sub-Felder für die Protokoll-Version, die Identifizierung des Typs des Rahmens, Leistungskontrolle und Sicherheitseinstellungen u.a.
- Duration: Gibt die geschätzte Zeit an, die verbleibt, um den nächsten Datenrahmen zu erhalten (AP an Client)
- Address 1: Empfänger MAC-Adresse
- Address 2: Sender MAC-Adresse
- Address 3: MAC Adresse des Default Gateways
- Sequence Control: Enthält die Sequenznummer des Rahmens und Subfelder für allfällige Fragmentierung
- Address 4: Fehlt meist, wird nur im ad hoc mode beschrieben.

#### Rahmen Typen

Im Feld Frame Type von Frame Control werden folgende Typen von Rahmen unterschieden:

- Management-Rahmen: Zum Finden eines APs, zur Authentifikation und zum Verbindungsauflauf mit einem AP
- Kontroll-Rahmen: Kontrolle des Datenflusses in einer bestehenden Verbindung und helfen, Kollisionen zu verhindern
- Daten-Rahmen

Die Abb. 5.4 zeigt die möglichen Subtypes für **Management Rahmen**. Mit solchen Rahmen kann sich ein Client an einem WLAN anmelden.

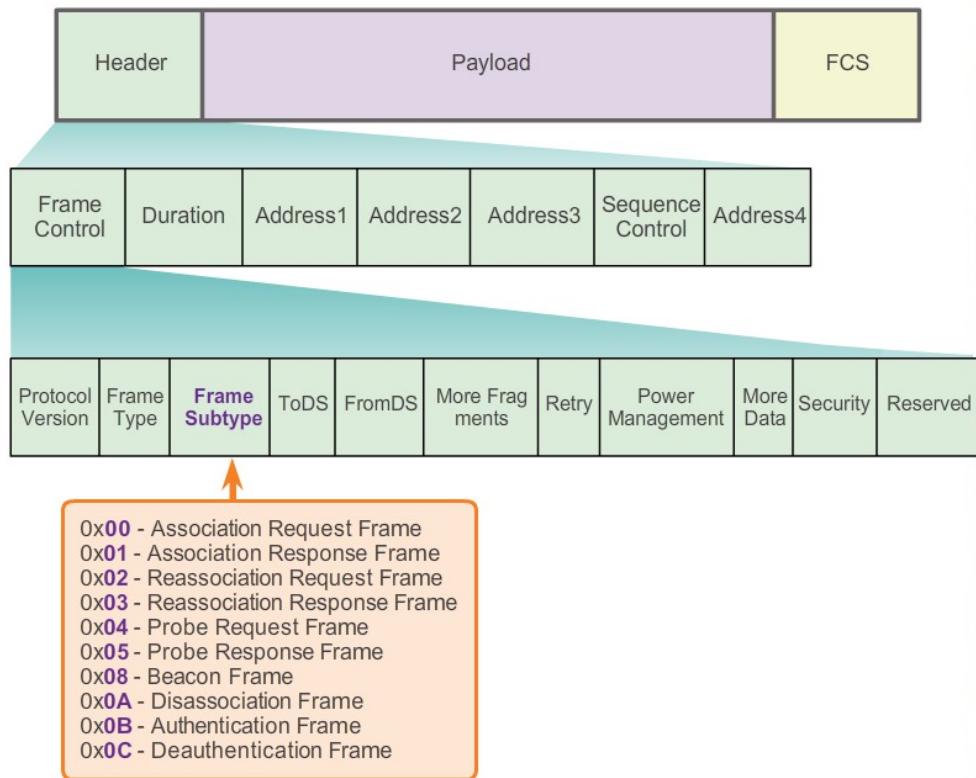
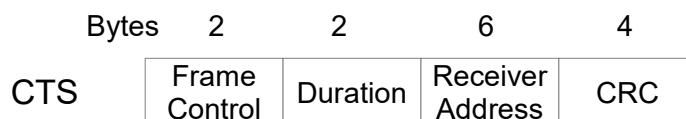
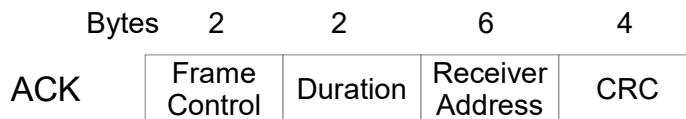


Abbildung 5.24: Ein WLAN Rahmen des Frame Types Management

Kontroll-Rahmen mit einfacherer Form:



### Adressen-Problematik:

Der Weg eines Rahmens eines Clients an das Default Gateway (L3 Gerät, der Router) geht über zwei Abschnitte:

- Drahtloser Abschnitt zum AP (AP: Physikalischer Empfänger des Wireless Rahmens)

- Drahtgebundener Abschnitt durchs Distribution System, DS, bis zum Router (logischer Empfänger des Rahmens)

Der AP bildet die logische Ziel-Adresse des Wireless Rahmens auf die Zieladresse des abgehenden Ethernet Rahmens ab. Ein Wireless Rahmen, der vom AP weitergeleitet werden soll, benötigt drei Adressen: Zwei physikalische Adressen und eine logische.

Bedeutung der verschiedenen Adressen:

Zwei bit im Feld Frame Control:

- To DS: Vom Client zum Router
- From DS: Vom Router zum Client

Management – und Control Rahmen haben beide bit auf 0 gesetzt.

Address 1: Physikalischer Empfänger des Wireless Rahmens

Address 2: Physikalischer Sender des Wireless Rahmens

Adresse 3: Logischer Empfänger / Sender

To DS	From DS	Address 1	Address 2	Address 3
0	1	Client Addr.	AP Addr.	Def. GW Addr.
1	0	AP Addr.	Client Addr.	Def. GW Addr.
0	0	Sender	Empfänger	bedeutungslos

### 5.3 Sicherheit in Wireless LAN

#### 5.3.1 WLAN Angriffspunkte

Vier Hauptgefahren:

- Rogue APs: Ungebetene APs können bewusst eingeschleust werden oder treten durch falsche Handhabung unabsichtlich auf. Rogue APs können mit wireless management SW detektiert werden.
- Wireless Intruders: Ungebetene Gäste versuchen Zutritt zum Netz zu bekommen. Abhilfe kann mit Authentifikation geschaffen werden.
- Interception of data: Wireless Netze können abgehört werden. Gegenmittel: Verschlüsselung. Spezialform: Man in the middle.

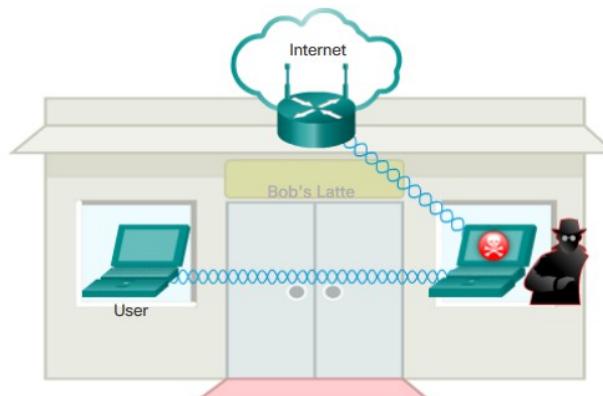


Abbildung 5.25: Die "Man in the Middle" Attacke

- Denial of Service Attacks.
  - (Un-)beabsichtigte Interferenzen
  - CTS flooding
  - spoofed disconnect attack

### 5.3.2 Sicherung von WLANs

Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
<ul style="list-style-type: none"> <li>No encryption</li> <li>Basic authentication</li> <li>Not a security handle</li> </ul>	<ul style="list-style-type: none"> <li>No strong authentication</li> <li>Static, breakable keys</li> <li>Not scalable</li> </ul>	<ul style="list-style-type: none"> <li>Standardized improved encryption</li> <li>Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)</li> </ul>	<ul style="list-style-type: none"> <li>AES Encryption</li> <li>Authentication: 802.1X</li> <li>Dynamic key management</li> <li>WPA2 is the Wi-Fi Alliance implementation of 802.11i</li> </ul>

Abbildung 5.26: Entwicklung der Sicherheits-Massnahmen:

Übersicht über Authentisierungsmethoden:

	WEP	WPA	802.11i/WPA2
Authentication Method	Pre-shared key	PSK or 802.1x	PSK or 802.1x
Encryption	RC4	TKIP	AES
Message Integrity	CRC-32	MIC	CCMP
Security	Weak	Strong	Stronger

Abbildung 5.27: Übersicht über Authentifizierungsmethoden. TKIP:Temporal Key Integrity Protocol. AES: Advanced Encryption Standard.



Abbildung 5.28: Wahl des Authentisierungsverfahrens

Bei WPA und WPA2 gibt zwei Möglichkeiten

- Personal (Pre-shared key, PSK)
- Enterprise (802.1X mit RADIUS server)

#### Personal:

Pre-Shared key authentication:

1. Der Client sendet einen authentication frame an den AP
2. Der AP antwortet mit einem challenge string
3. Der Client verschlüsselt den String mit seinem shared key und sendet die Antwort an den AP.
4. Der AP macht dieselbe Operation und vergleicht die beiden Ergebnisse. Entweder er authentifiziert den Client oder eben nicht.

### Enterprise:

Es steht ein RADIUS Server (Remote Authentication Dial-In User Service) zur Verfügung, der alle [Benutzername, Passwort]-Paare verwaltet. Der Vorteil ist, dass man nachvollziehen kann, wer sich angemeldet hat. Wird ein Windows Server oder ein TACACS Server (Cisco Pendant) verwendet, so kann Autorisierung gemacht werden und der Client dem zugehörigen VLAN zugeteilt werden.

Benutzer melden sich nach dem IEEE802.1X Standard mit dem Extensible Authentication Protocol, EAP, an. Der Access Point wird zum Client des Radius Servers. Er authentifiziert sich mit einem Passwort (Shared Secret) beim Server.

Die Konfiguration auf einem AP kann z.B. wie in Abb. 5.29 aussehen.



Abbildung 5.29: Konfiguration der Authentisierung und Verschlüsselung auf einem AP.

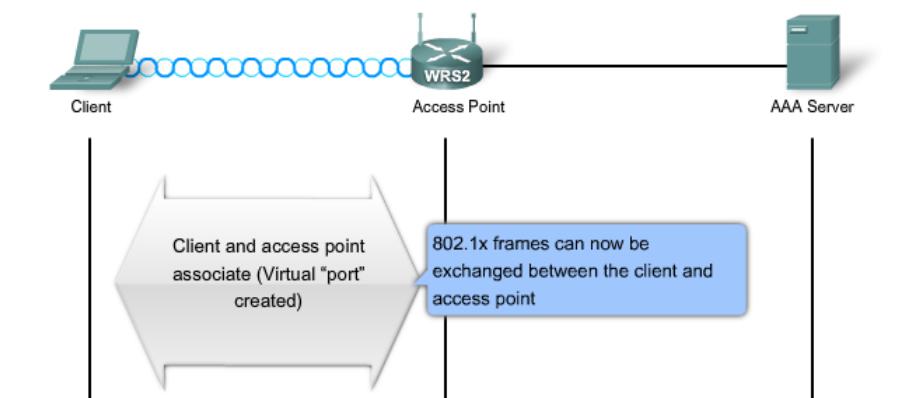


Abbildung 5.30: Komponenten bei WPA2 und 802.1X

- Association: Der AP bildet einen virtuellen Port für jeden Client.
- Aller Verkehr ausser IEEE802.1x Rahmen werden blockiert.
- Die IEEE802.1x Rahmen tragen die EAP-Pakete hin und her
- Ein AAA server (Authentication, Autorization and Accounting, z.B. OpenLDAP, MS Active Directory) kennt die Benutzer und die Credentials. Das RADIUS Protokoll transportiert die IEEE Rahmen zwischen AP und Server.
- Falls eine erfolgreiche Authentifikation stattfindet: Etablierung von Verschlüsselung zwischen Client und AP und Öffnen des virtuellen Ports für Datenrahmen.

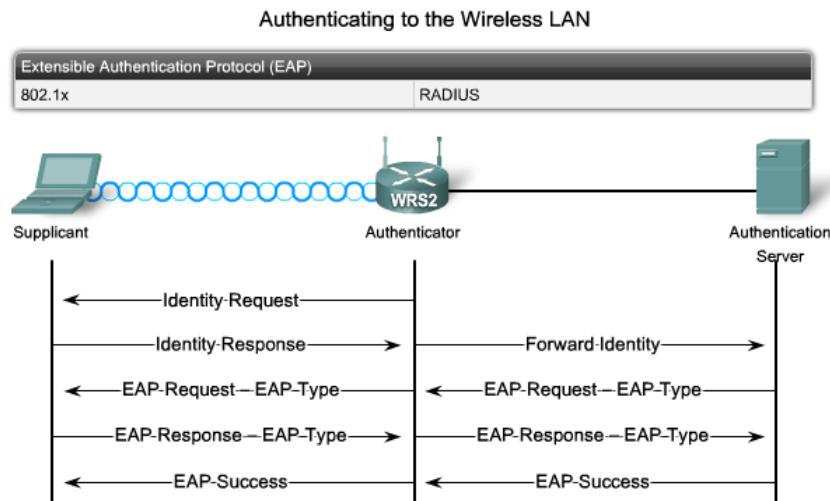


Abbildung 5.31: Ablauf des EAP Protokolls

Die alten Methoden für Authentifizierung (MAC filtering, SSID broadcast ausschalten) sind nicht sicher. Sie können weiterhin verwendet werden. Sie sind aber nicht hinreichend.

### Verschachtelung mehrerer Sicherheits-Hürden in WLANs

“Security in Depth”: Es wird empfohlen, mehrere Sicherheiten hintereinander zu schalten.

- SSID cloaking - SSID broadcasts beim AP ausschalten
- MAC address filtering – MAC-Tabellen erlaubter Clients (von Hand) auf dem AP konfigurieren
- WLAN security implementation - WPA or WPA2

## 5.4 Konfiguration von Access Points

Setup: Adressierung

- IP-Adresse gegen das Internet: Es gibt drei Möglichkeiten für die Vergabe
  - per DHCP des ISP
  - Manuelle Vergabe
  - PPPoE
- IP-Adresse, unter welcher der Router von innen erreichbar sein soll
- DHCP für die eigenen Clients

Wireless Settings

Basic settings

- Netzwerk Mode
- SSID Name
- Kanalwahl

Wireless security

- Wahl der Sicherheits-Methode

Management Zugang setzen (nicht im Defaultzustand belassen!)

Verkabelung



Abbildung 5.32: Verkabelung gegen das drahtgebundene Netz (Internet)