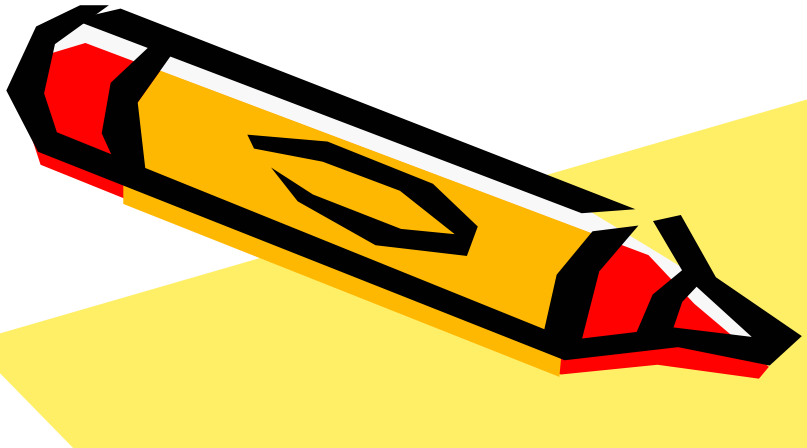


Ch. 8 – VLAN (Virtual LAN)

CCNA 3 version 3.0

Wolfgang Riggert, FH Flensburg, auf der Grundlage von
Rick Graziani, Cabrillo College

Vorbemerkung

Die englische Originalversion finden Sie unter :
http://www.cabrillo.cc.ca.us/~rgraziani/

Der username ist *cisco* und das Password *perlman*

- Viele der Informationen ergänzen das Online-Curriculum
- Die Zusatzinformation ist zur Verdeutlichung und weiteren Erklärung der Themen eingefügt.
- Die Originalversion ist um eigene Folien erweitert, um das Verständnis zu fördern

Überblick

Die Folien sollen folgende Lernziele unterstützen:

- Definition von VLANs
- Nutzen von VLANs
- VLANs und ihr Verhältnis zu Broadcastdomänen
- Einsatz von Routern in VLAN-Umgebungen
- VLAN Typen
- Definition von ISL und 802.1Q
- Konfiguration und Verifikation von VLANs

VLAN Definition

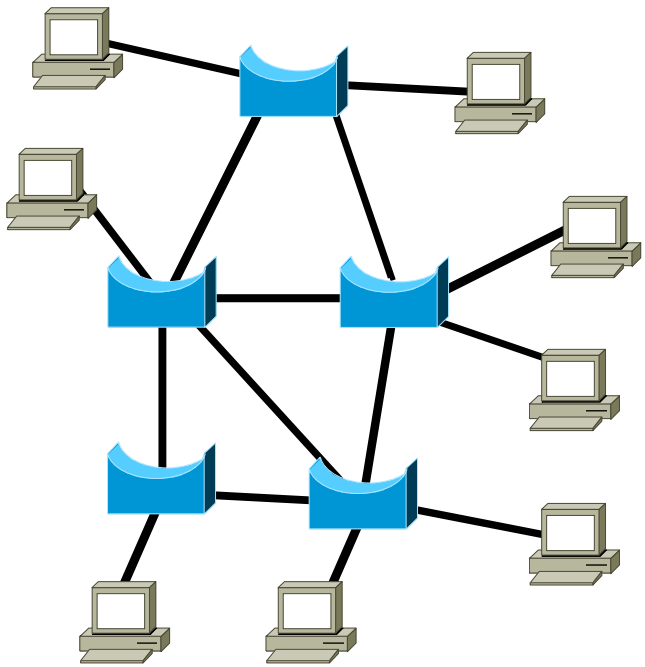
- VLANs segmentieren ein Netz durch die Bildung von Broadcastdomänen. Ein VLAN ist eine Gruppe von Endstationen, die sich auf unterschiedlichen LAN-Segmenten befinden können, aber logisch zusammengehören. Damit wird das VLAN zu einer auf Layer-2 definierten Broadcastdomäne

VLAN Eigenschaften

- VLANs richten sich an die Skalierbarkeit, die Sicherheit und das Netzwerkmanagement.
- Switches können keinen Datenverkehr zwischen unterschiedlichen VLANs vermitteln
- Zur Kommunikation zwischen unterschiedlichen VLANs ist ein Router erforderlich

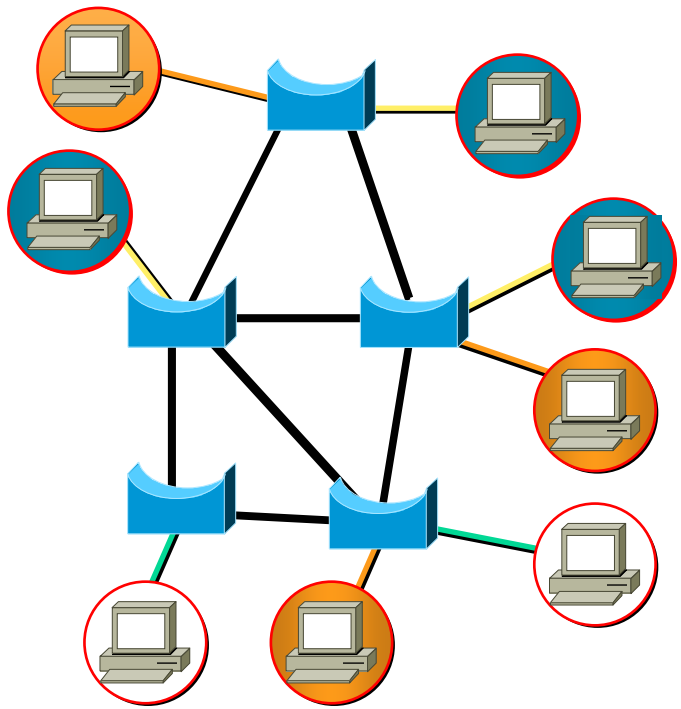
VLAN-Aufbau

Ausgangssituation



Jede Station kann mit jeder kommunizieren

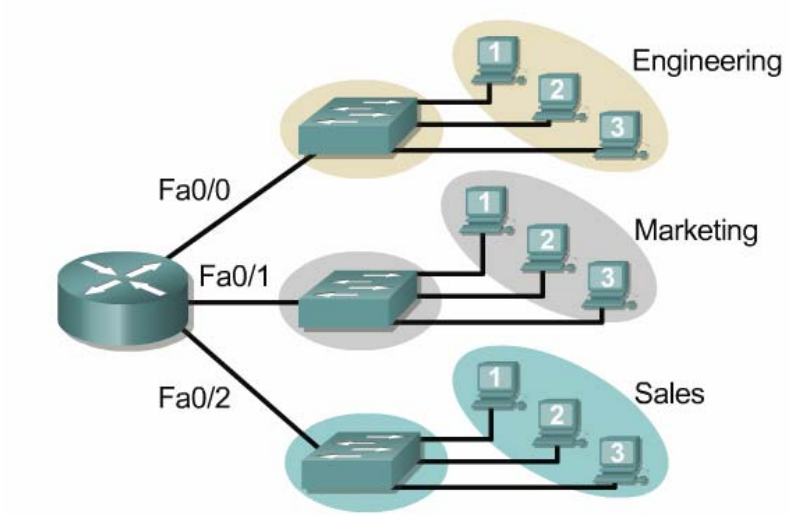
VLAN-Lösung



Nur Stationen gleicher Schattierung können miteinander kommunizieren

Broadcastdomänen mit VLANs und Routern

drei Vlans =
drei Broadcastdomänen
mit je einem Switch
und einem Router zur
Vermittlung

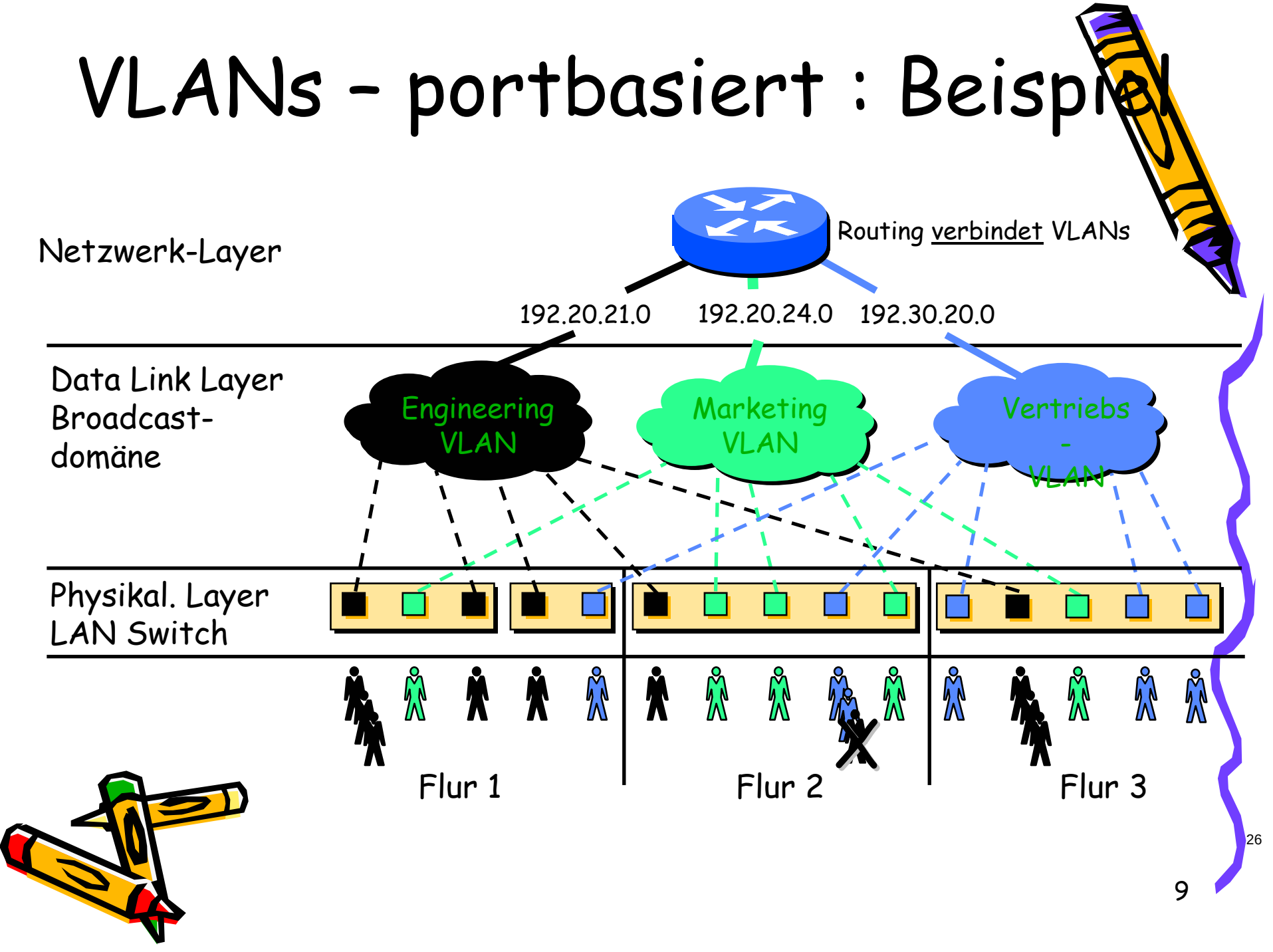


- Ein VLAN ist eine Broadcastdomäne, die einen oder mehrere Switches umfassen kann

VLAN – statische Zuordnung: portbasiert

- Jeder Port eines Switches wird einem VLAN zugeordnet. Eine Endstation, die an diesem Port angeschlossen wird, ist automatisch Teil dieses VLANs. Eine explizite Zuweisung eines Hosts zu einem VLAN ist damit überflüssig.
- Ports, die dem gleichen VLAN zugewiesen sind, gehören der gleichen Broadcastdomäne an
- Ports können nur Mitglied eines VLANs sein
- Das Default-VLAN (VID 1) ist in jeder Standardkonfiguration portbasiert definiert und kann nicht gelöscht werden

VLANs – portbasiert : Beispiel



VLAN – dynamische Zuordnung

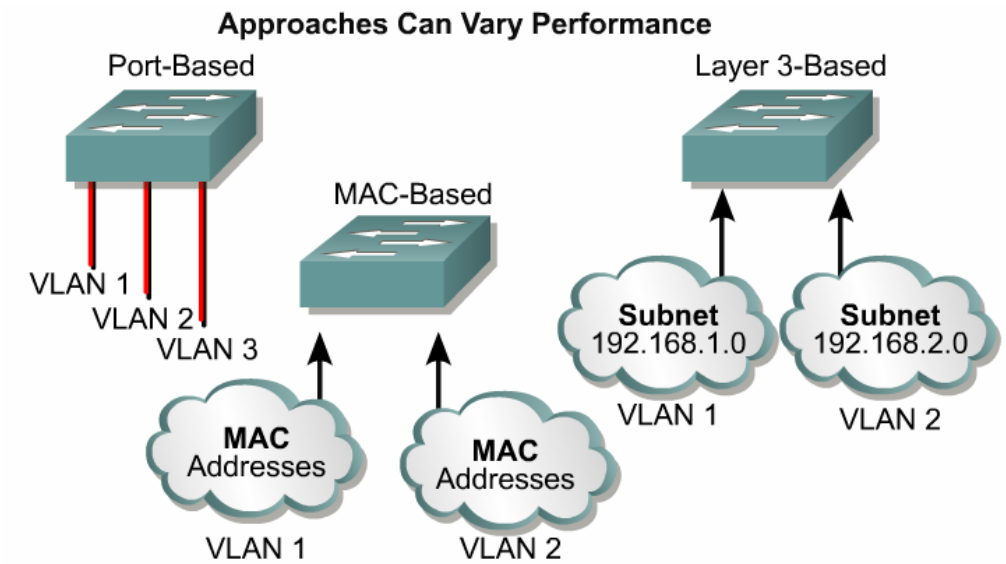
- Die dynamische Mitgliedschaft zu einem VLAN wird durch Management Software hergestellt.
- Dynamische VLANs ordnen die Hosts z.B. auf Basis der MAC-Adresse einem VLAN zu.
- Dieses Konzept verlangt die Existenz einer Datenbank für jeden Switch, die Auskunft über die VLAN-Mitgliedschaft gibt.

Nutzen von VLANs

- Der Kernnutzen entsteht durch die Möglichkeit, das LAN nach organisatorischen Gesichtspunkten und nicht nach physikalischen zu strukturieren.

- Dies erlaubt dem Administrator:
  - einen problemlosen Umzug von Hosts
  - ein leichtes hinzufügen neuer Stationen
  - einen einfacheren Wechsel der LAN-Konfiguration
  - gesteigerte Kontrolle des Netzverkehrs
  - verbesserte Sicherheit

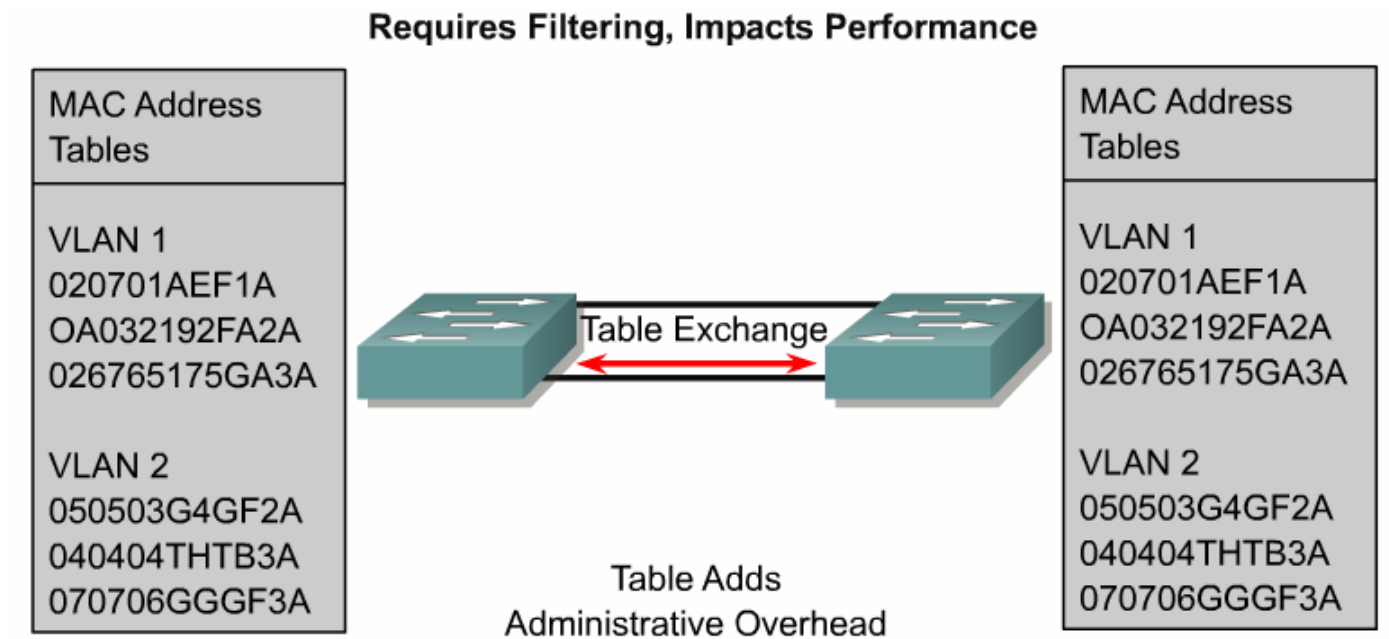
VLAN Types



Üblich sind drei VLAN-Typen:

- portbasiert
- MAC-Adressen basiert – selten implementiert
- protokollbasiert

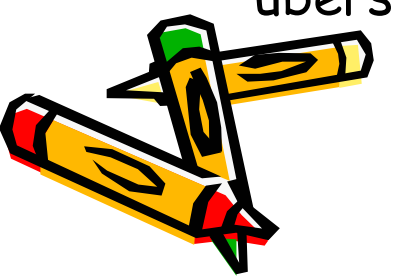
MAC Adressenbasierte VLANs



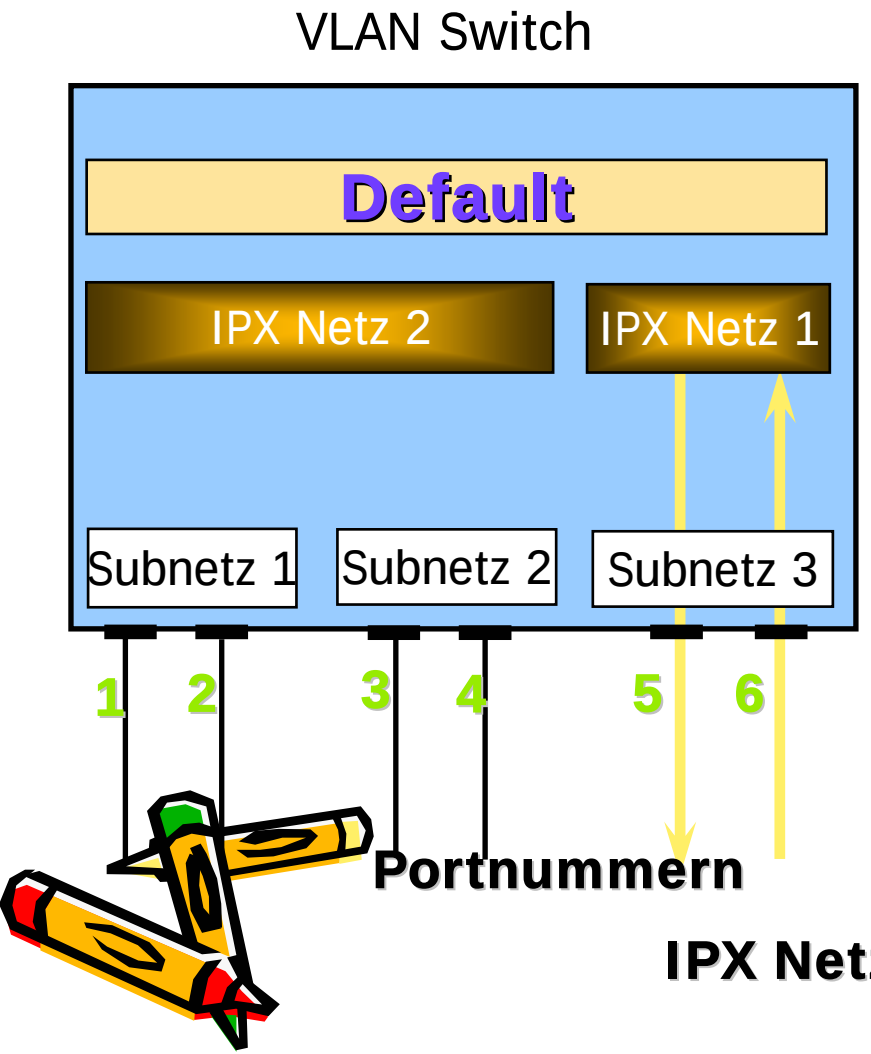
- User assigned based on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability, and administration
- Offers similar process for higher layers

VLAN - protokollbasiert

- Ein protokollbasiertes VLAN besteht aus einer Gruppe von Switchports, für die jeweils ein oder mehrere Protokolltypen definiert werden.
- Folgende Protokolle sind möglich:
  - IP
  - IPX
  - DECnet
  - AppleTalk
  - SNA – VINES – X.25 - NetBIOS
- Ein protokollbasiertes VLAN schließt jeden Frame aus, der nicht der Protokolltypdefinition entspricht.
- Protokollbasierte VLANs des gleichen Typs können sich nicht überschneiden.



VLAN – protokollbasiert : Beispiel



Default VLAN

IPX VLANs

IP VLANs

VLANs	Port nummer
Default	1 – 6
IPX Netz 1	5 – 6
IPX Netz 2	1 – 4
IP Subnetz 1	1 – 2
IP Subnetz 2	3 – 4
IP Subnetz 3	5 – 6

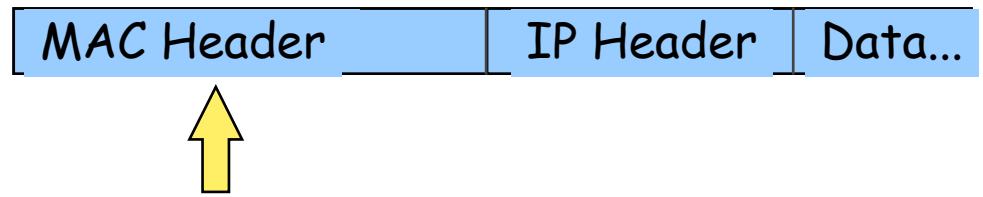
IPX Netz 1 – Broadcast

Quelle : 3Com University

VLAN Tagging

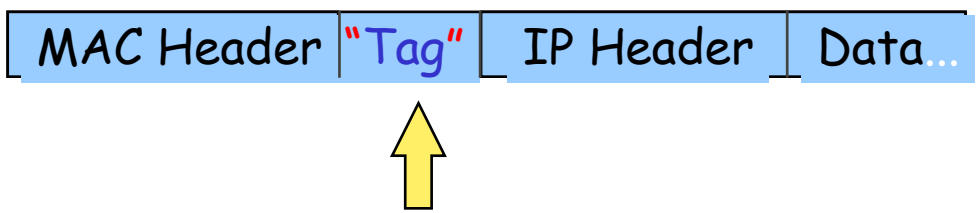
- VLAN Tagging wird notwendig, wenn eine Verbindung mehr als den Verkehr eines VLANs transportieren muss. Ein Beispiel hierfür sind Trunks.
- Eine Marke = Tag wird dem Header hinzugefügt, um die VLAN-Zugehörigkeit zu erkennen
- Das Paket wird dann dem entsprechenden Switch oder Router auf der Basis des VLAN-Identifiers und der MAC-Adresse zugestellt.
- Der zum Empfänger nächstgelegenen Switch entfernt die VLAN-ID und stellt das Originalpaket zu

VLAN-Komponenten - Frameidentifikation



Beispiel : Protokolltyp

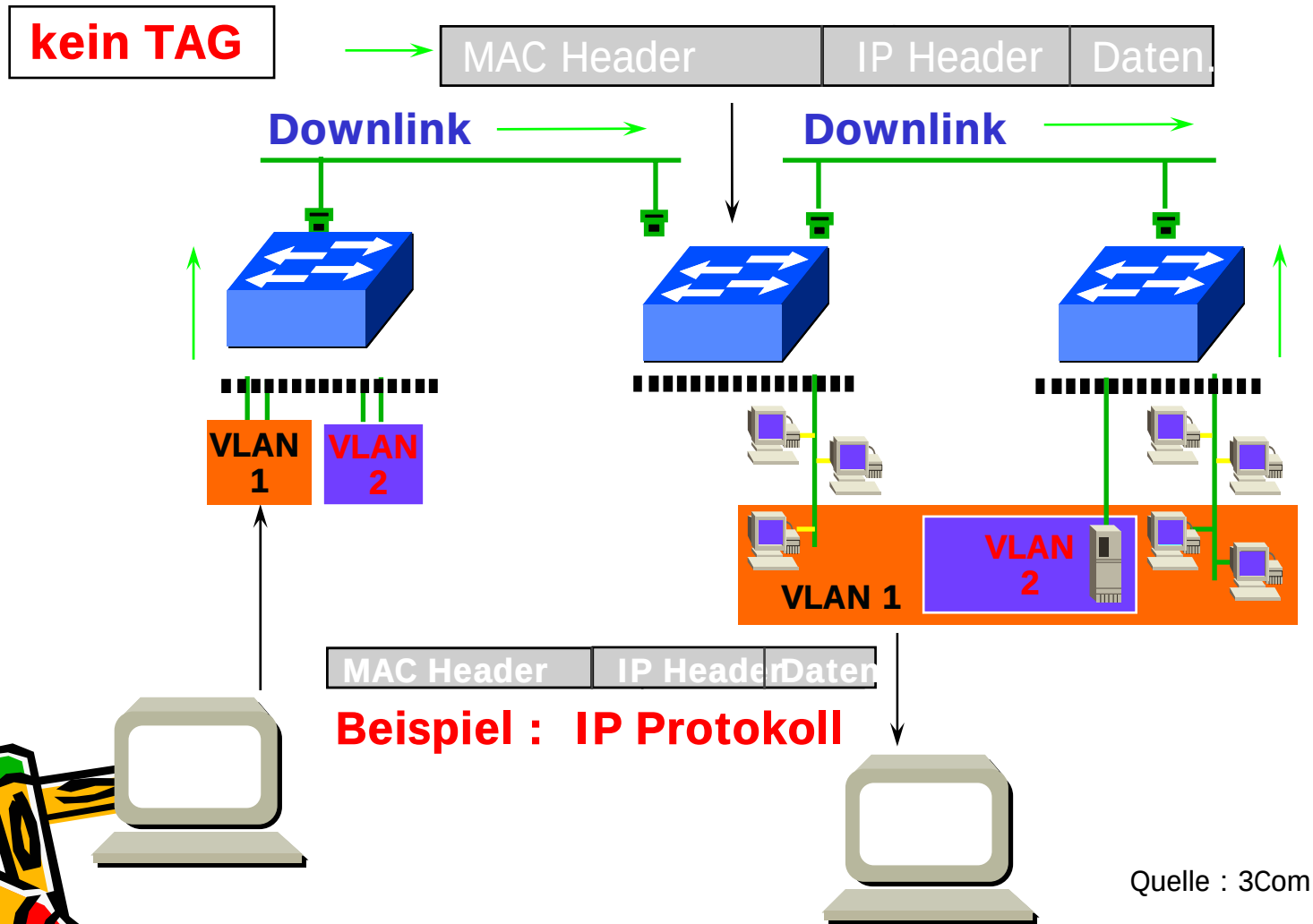
Implizite Identifikation : Information im Frame eingefügt



Beispiel : Standard 802.1 Q tag

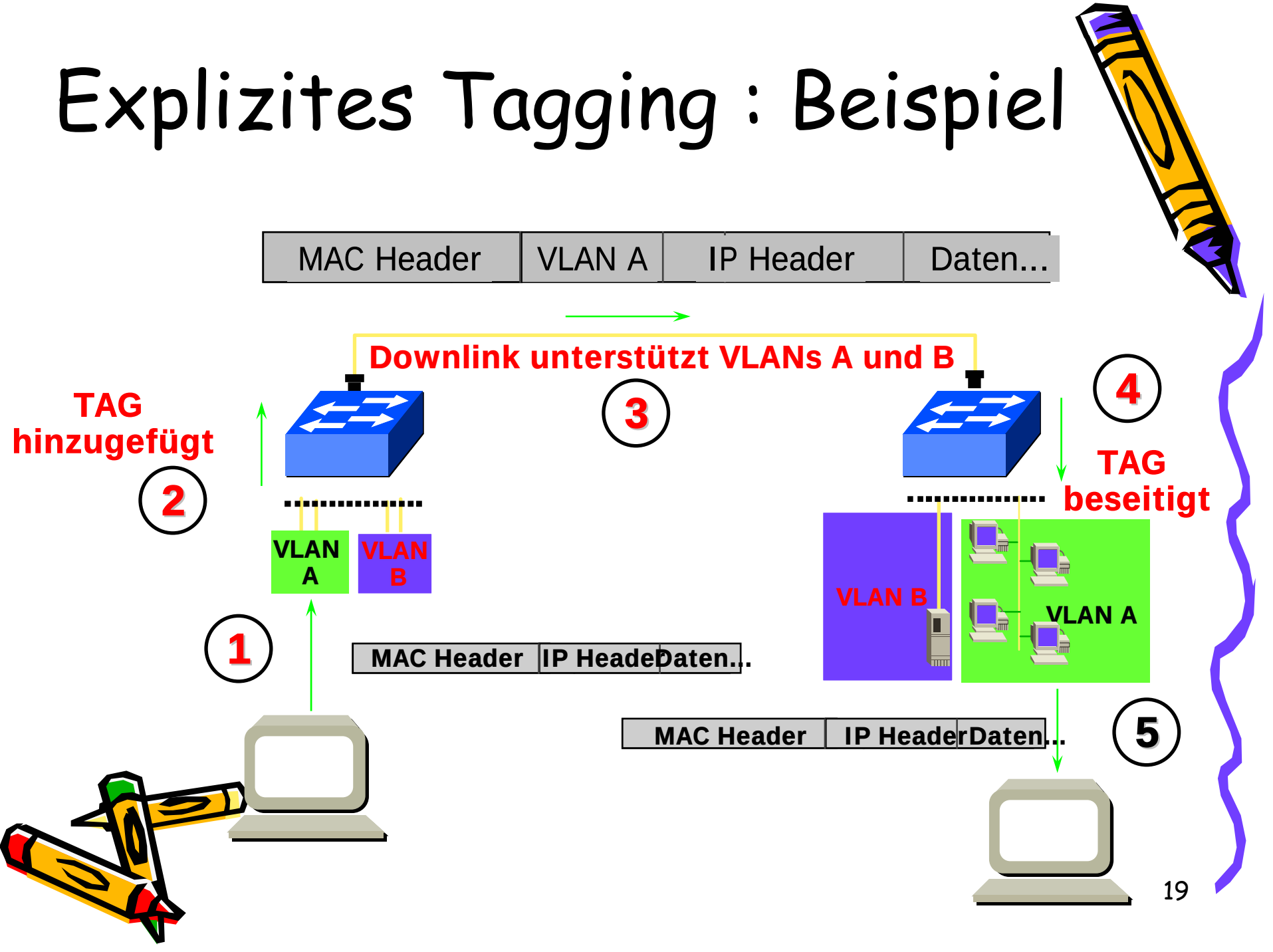
Explizite Identifikation : Information dem Frame hinzugefügt

Implizites Tagging



Quelle : 3Com University

Explizites Tagging : Beispiel



Explizites Tagging : Ablauf

- 1. Ein Frame wird durch ein Device übertragen, das Mitglied von VLAN A ist.
- 2. Dieser Frame wird vom Switch identifiziert und um einen 802.1Q Tag ergänzt, der VLAN A kennzeichnet.
- 3. Der Frame wird auf einem Interswitch-Link übertragen (Downlink).
- 4. Der getagged Frame erreicht den entfernten Switch, der ihn als zu VLAN a zugehörig erkennt und ihn an den entsprechenden Port weiterleitet.
- 5. Da der Port untagged für VLAN A ist, entfernt der Switch den Tag.

Explizites Tagging : Merkmale

- **Explicit Tagging** ist die am häufigsten verwendete Methode zur Bestimmung der VLAN-Zugehörigkeit
  - Unter 802.1Q werden bestimmte Tagginginformationen, die die VLAN-Identifikation gewährleisten hinzugefügt.
  - Ein einfacher Downlink kann Verkehr für mehrere VLANs zwischen den Switches transportieren.
  - Wird Tagging über einen Downlink verwendet, müssen beide Endstationen VLAN-fähig sein.

Explizites Tagging : Information

Normaler Ethernet Frame

Präambel: 7	SFD: 1	DA: 6	SA: 6	Typ / Länge: 2	Daten: 48 bis 1500	CRC: 4

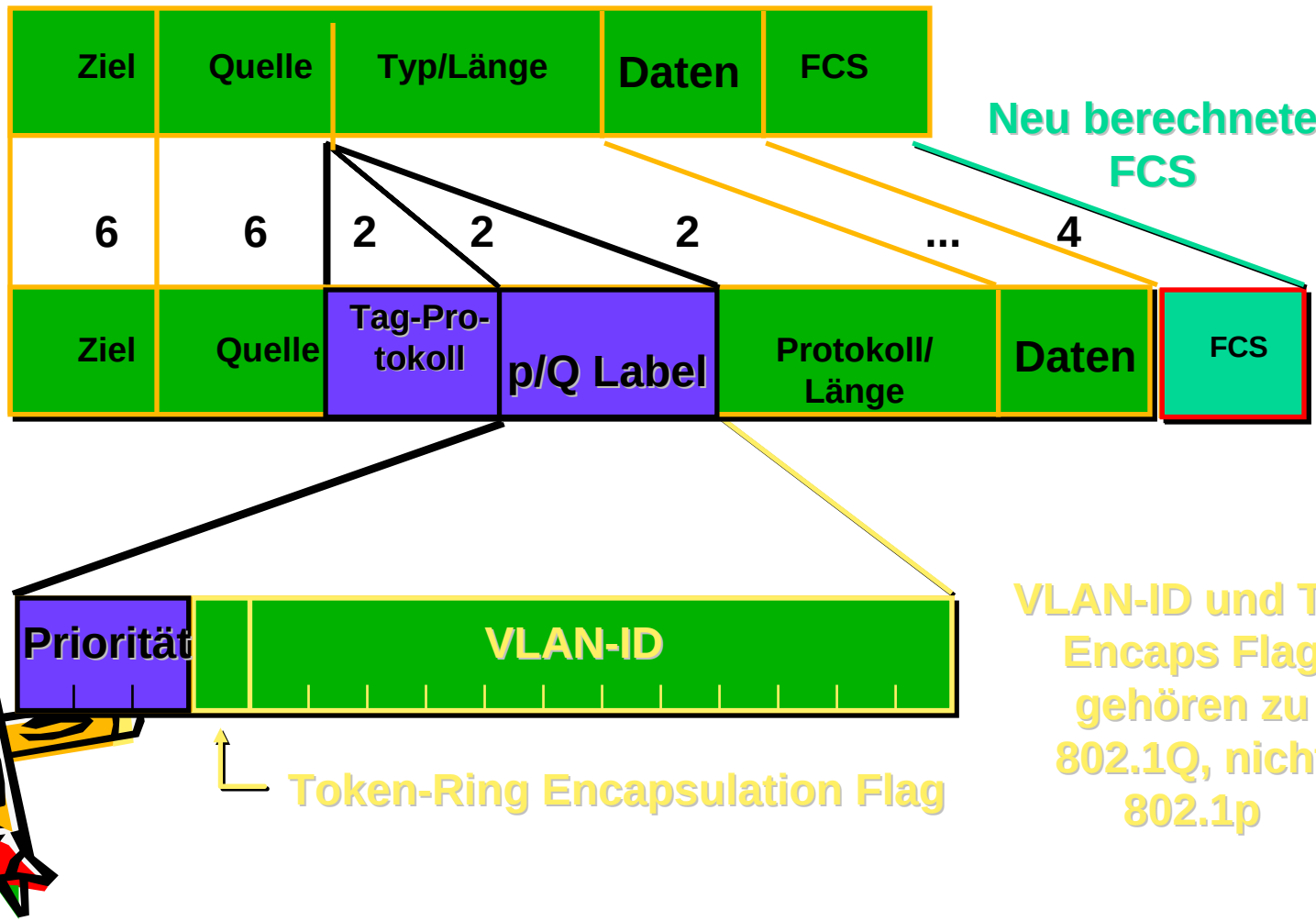
Eingefügte Felder

802.1Q Tagged Frame

Präambel: 7	SFD: 1	DA: 6	SA: 6	2 TPI	2 TAG	Typ / Länge: 2	Daten: 48 bis 1500	CRC: 4

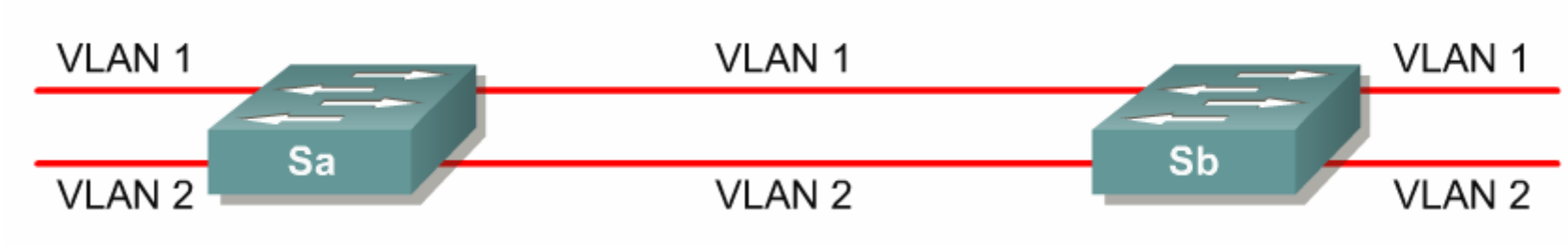
User Priorität	CFI	Bits der VLAN ID (VID) zur Identifikation 4,096 möglicher VLANs
3 bits	1 bit	12 bits

802.1p/Q Struktur

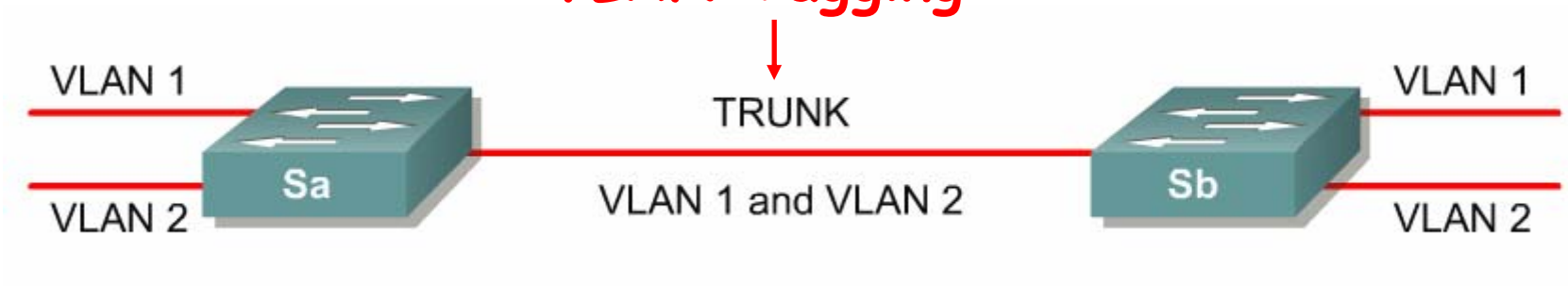


VLAN Tagging

kein VLAN Tagging



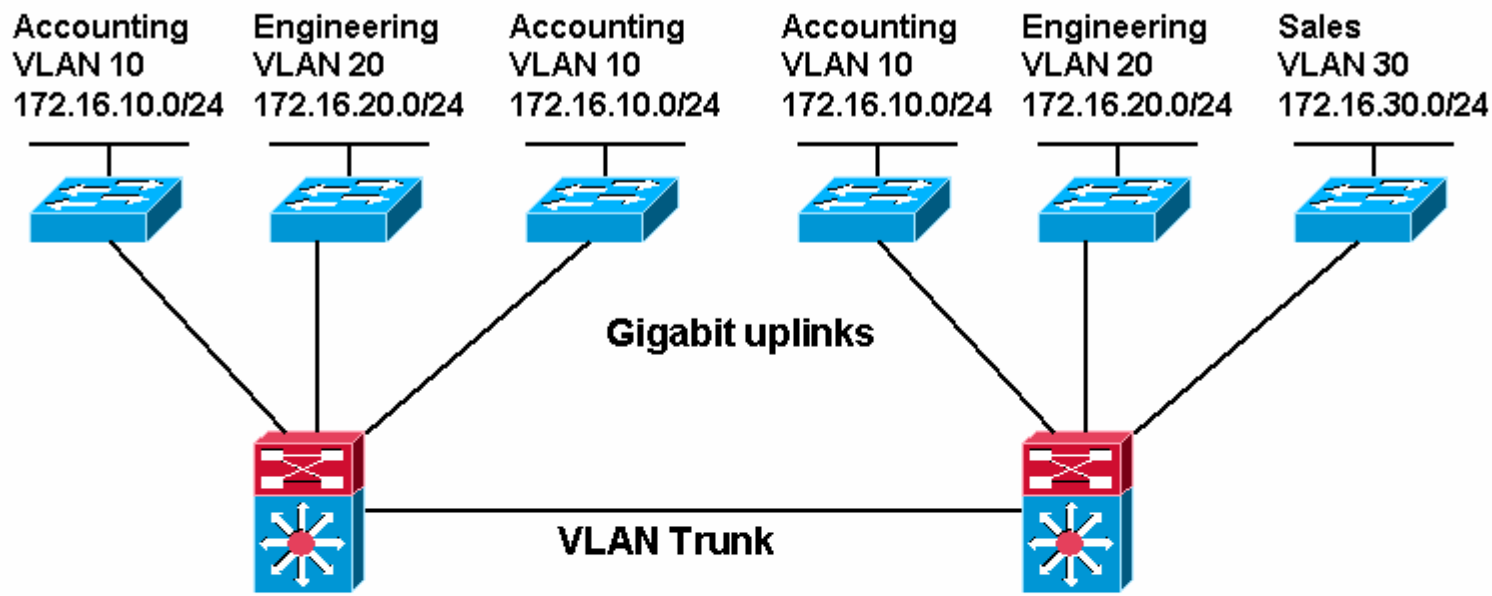
VLAN Tagging



VLAN Taggingmethoden

- Es gibt zwei Methoden des Taggings:
  - Ciscos herstellerspezifisches **Inter-Switch Link (ISL)**
  - **IEEE 802.1Q**.
- ISL wird durch 802.1Q ersetzt, da es einen Quasi-Standard darstellt.

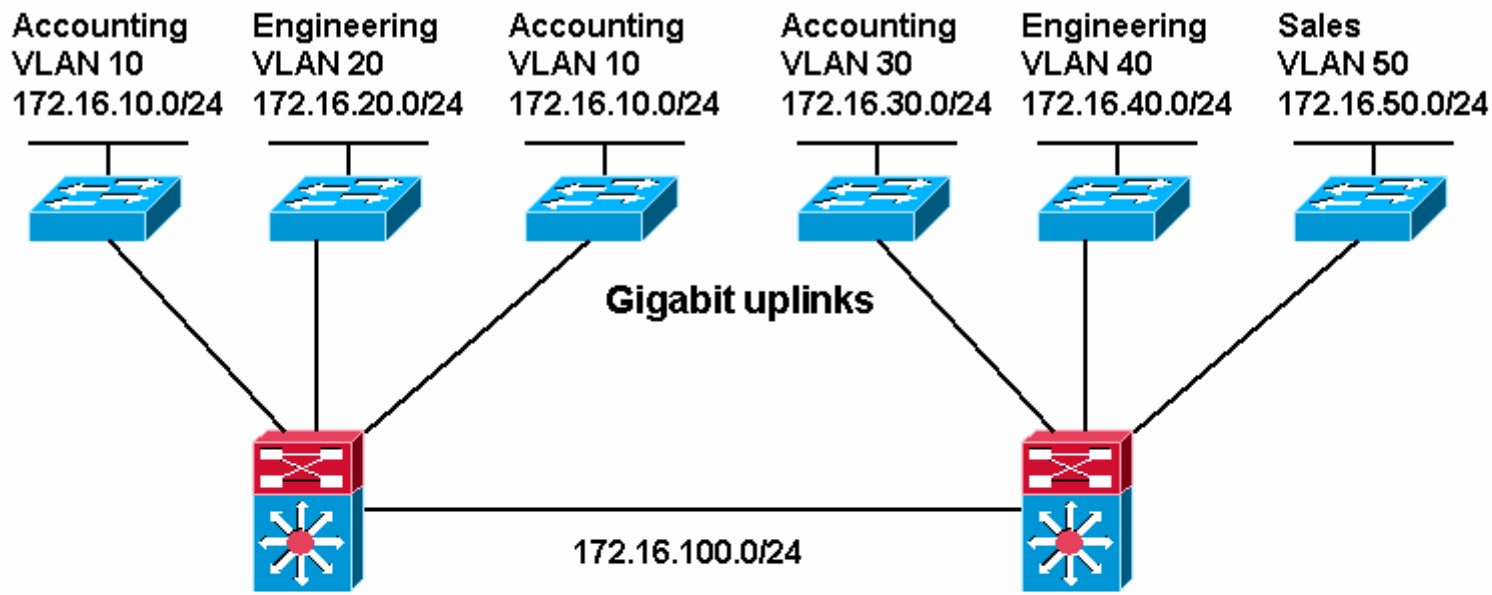
Ende-zu-Ende oder Campus-VLANs



Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

Geographische oder Lokale VLANs



Local or Geographic VLAN Model

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

Ende-zu-Ende oder Campus-VLANs

- einige VLAN/Subnetze unabhängig von der Positionierung im Netz
- Trunking und Routing zwischen den VLANs durch Kernrouter
- Von den Herstellern nicht empfohlen
- Fügt dem Netz Komplexität im Management hinzu
- Löst keine Spanning-Tree Probleme
- Richtet sich an alte 80/20-Regel – daher obsolet

Geographische oder lokale VLANs

- Weit verbreitet
- Routing im Kern
- Unterschiedliche VLAN/Subnetze abhängig von der Lokation
- Nutzer benötigen Ressourcen außerhalb ihres VLANs
- Die Zentralisierung von Ressourcen erzeugt Schwierigkeiten im Ende-zu-Ende-Design
- Eine neue 80/20-Regel besagt, dass 80% des Datenverkehrs remote verläuft und nur 20% lokal, d.h. der Nutzer muss in 80% der Fälle ein Layer-3-Device überqueren

Konfigurieren statischer VLANs

- Die maximale Anzahl VLANs ist switchabhängig:
  - 29xx Switches erlauben 4,095 VLANs
- VLAN 1 ist das Default-VLAN
- Cisco Discovery Protocol (CDP) und VLAN Trunking Protocol (VTP) Advertisements werden auf VLAN 1 gesendet
- Die Catalyst 29xx IP-Adresse gehört zur VLAN 1 Broadcastdomäne

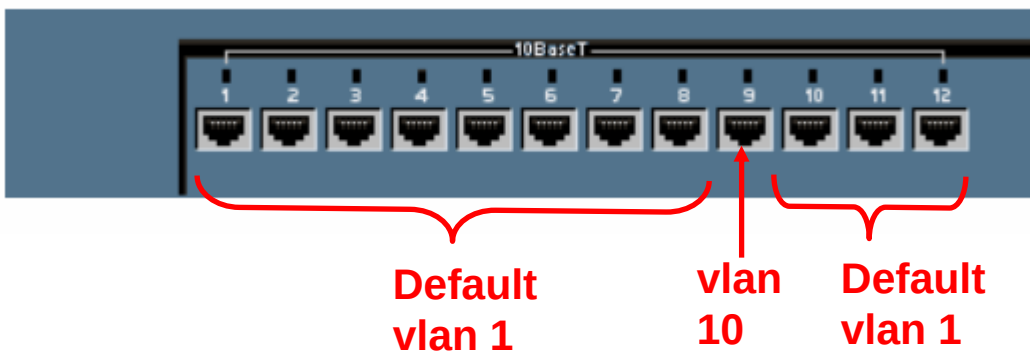
Anlegen von VLANs

- **Einrichten eines VLANs 10**

```
Switch#vlan database
Switch(vlan)#vlan 10
Switch(vlan)#exit
```

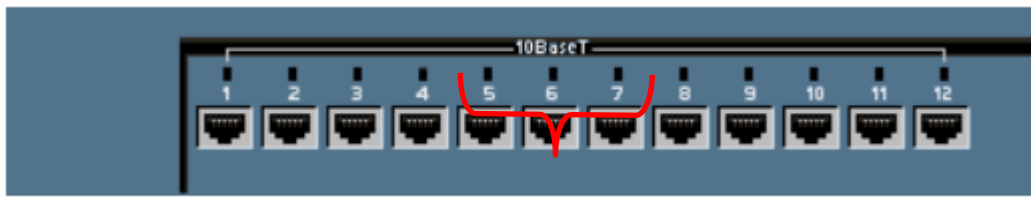
- **Zuweisung eines Accessports zu VLAN 10 (kein Trunkport!!!)**

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
```



VLAN portbasiert

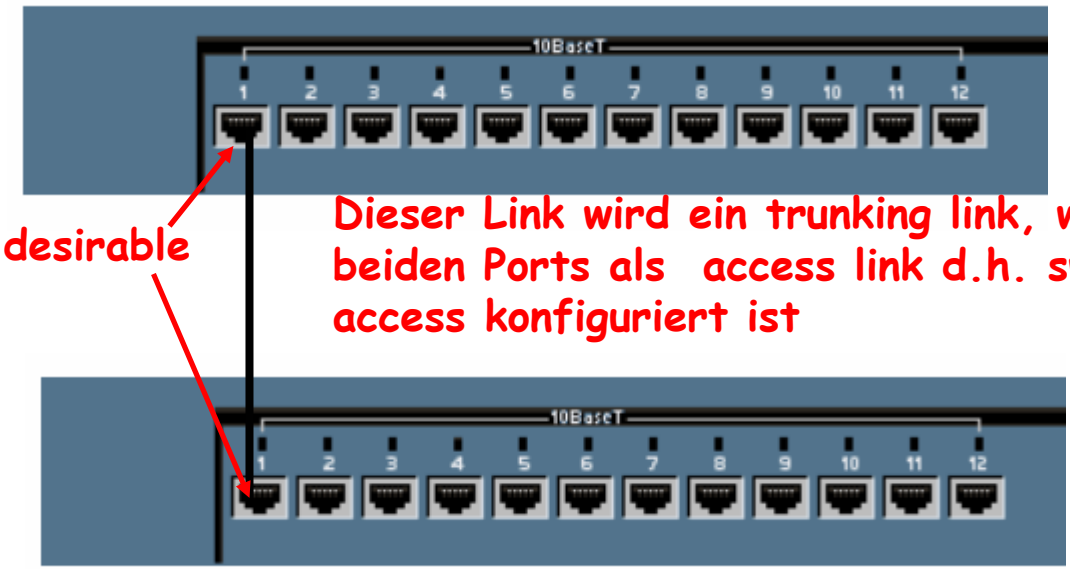
Port 5-7 wird VLAN 2 zugewiesen:



VLAN 2

```
SydneySwitch(config)#interface fastethernet 0/5
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/6
SydneySwitch(config-if)#switchport access vlan 2
SydneySwitch(config-if)#exit
SydneySwitch(config)#interface fastethernet 0/7
SydneySwitch(config-if)#switchport access vlan 2
```

VLAN Trunkports

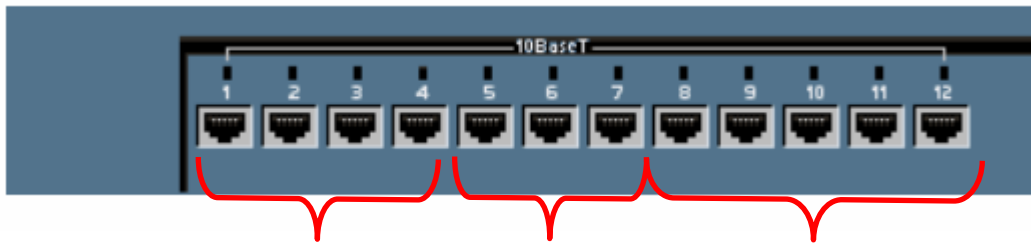


Default: dynamic desirable

Dieser Link wird ein trunking link, wenn keiner der beiden Ports als access link d.h. switchport mode access konfiguriert ist

- Standardmäßig sind alle Ports als **`switchport mode dynamic desirable`** eingestellt. Sobald dieser Port mit einem anderen Switch verbunden wird, wird er als Trunk erkannt

VLANs - show vlan



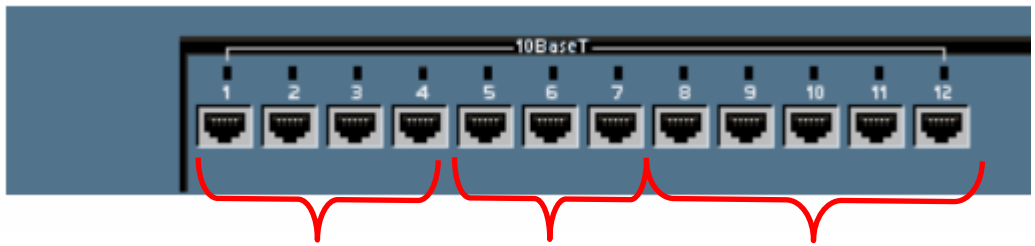

```
SydneySwitch#show vlan

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -   -     1002   1003
2    enet 100002 1500  -      -      -        -   -     0      0
```

VLAN - show vlan brief




```
SydneySwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Löschen von VLANs

```
Switch(config-if)#no switchport access vlan 300
```

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```