5.4 VLANs und Broadcast-Domänen

VLANs gehören zu OSI-Schicht 2.

VLAN steht für:

```
Virtual Local Area Network
```

Auf Deutsch sinngemäß:

```
virtuelles lokales Netzwerk
```

Mit VLANs kann man ein physisches Switch-Netz in mehrere logisch getrennte Netzbereiche aufteilen.

Merksatz:

```
VLAN = logische Netztrennung auf Schicht 2.
```

Grundidee eines VLANs

Ohne VLAN befinden sich viele Geräte im gleichen lokalen Netzwerkbereich.

Das bedeutet:

```
Sie befinden sich in derselben Broadcast-Domäne.
```

Mit VLANs kann ein Switch mehrere getrennte logische Netze bereitstellen.

Beispiel:

```
ein Switch
aber mehrere getrennte Netze
```

Typische VLANs:

```
- Mitarbeiter
- Gäste
```

```
- Server
- VoIP
- Drucker
- Management
- IoT
```

Merksatz:

```
Ein physischer Switch kann mehrere logische Netze enthalten.
```

Warum nutzt man VLANs?

VLANs helfen dabei, Netzwerke sauber zu strukturieren.

Vorteile:

```
- logische Trennung von Geräten
- bessere Übersicht
- weniger Broadcast-Verkehr pro Netz
- mehr Sicherheit
- einfachere Verwaltung
- Trennung von Abteilungen oder Gerätetypen
- bessere Netzplanung
- Grundlage für Firewall-Regeln
```

Beispiel:

```
Gäste sollen ins Internet,
aber nicht auf interne Server.
```

Dafür kann man ein eigenes Gast-VLAN verwenden.

Merksatz:

```
VLANs trennen Geräte logisch,
auch wenn sie am gleichen Switch hängen.
```

VLAN und physische Verkabelung

Ohne VLAN müsste man für getrennte Netze oft getrennte Switches verwenden.

Beispiel ohne VLAN:

```
Switch 1 für Mitarbeiter
Switch 2 für Gäste
Switch 3 für Server
```

Mit VLANs kann ein einzelner Switch mehrere logische Netze bereitstellen.

Beispiel mit VLAN:

```
VLAN 10 = Mitarbeiter
VLAN 20 = Gäste
VLAN 30 = Server
```

Alle VLANs können auf demselben physischen Switch existieren.

Merksatz:

```
VLANs sparen physische Trennung durch logische Trennung.
```

Begriff: Broadcast

Ein Broadcast ist eine Nachricht an alle Geräte im lokalen Netzwerkbereich.

Die Broadcast-MAC-Adresse lautet:

```
FF:FF:FF:FF:FF:FF
```

Broadcasts werden zum Beispiel verwendet bei:

```
- ARP-Anfragen
- DHCP-Anfragen
- bestimmten lokalen Suchdiensten
```

Merksatz:

```
Broadcast = Nachricht an alle Geräte im lokalen Netz.
```

Begriff: Broadcast-Domäne

Eine Broadcast-Domäne ist ein Bereich, in dem Broadcasts verteilt werden.

Alle Geräte innerhalb derselben Broadcast-Domäne erhalten Broadcasts.

Ein VLAN bildet normalerweise eine eigene Broadcast-Domäne.

Beispiel:

```
VLAN 10 = eigene Broadcast-Domäne
VLAN 20 = eigene Broadcast-Domäne
VLAN 30 = eigene Broadcast-Domäne
```

Broadcasts aus VLAN 10 werden nicht automatisch an VLAN 20 weitergegeben.

Merksatz:

```
Ein VLAN = eine Broadcast-Domäne.
```

Warum Broadcast-Domänen begrenzen?

Zu viele Broadcasts können ein Netzwerk belasten.

Broadcasts werden an alle Geräte im gleichen lokalen Netz gesendet.

Wenn sehr viele Geräte in einer Broadcast-Domäne sind, kann unnötiger Datenverkehr entstehen.

VLANs helfen dabei, Broadcast-Verkehr zu begrenzen.

Beispiel:

```
ARP-Broadcast aus dem Gäste-Netz
erreicht nicht automatisch das Server-Netz.
```

Merksatz:

```
VLANs begrenzen Broadcasts auf einen logischen Bereich.
```

VLAN-ID

Ein VLAN wird durch eine Nummer gekennzeichnet.

Diese Nummer heißt:

```
VLAN-ID
```

Beispiele:

VLAN-ID	Zweck
10	Mitarbeiter
20	Gäste
30	Server
40	VoIP
99	Management

Die VLAN-ID dient zur eindeutigen Zuordnung eines Frames zu einem VLAN.

Merksatz:

```
VLAN-ID = Nummer eines VLANs.
```

VLAN und Name

Neben der VLAN-ID kann ein VLAN auch einen Namen haben.

Beispiel:

VLAN-ID	VLAN-Name
10	Mitarbeiter
20	Gast
30	Server
40	VoIP
99	Management

Der Name dient der Übersicht.

Technisch entscheidend ist aber die VLAN-ID.

Merksatz:

```
VLAN-Name hilft Menschen.
VLAN-ID ist technisch entscheidend.
```

VLAN und IP-Subnetz

Ein VLAN ist nicht dasselbe wie ein IP-Subnetz.

VLAN gehört zu:

```
OSI-Schicht 2
```

IP-Subnetz gehört zu:

```
OSI-Schicht 3
```

In der Praxis wird aber häufig jedem VLAN ein eigenes IP-Subnetz zugeordnet.

Beispiel:

VLAN	Zweck	IP-Subnetz
VLAN 10	Mitarbeiter	192.168.10.0/24
VLAN 20	Gäste	192.168.20.0/24
VLAN 30	Server	192.168.30.0/24

Merksatz:

```
VLAN = Schicht 2.
IP-Subnetz = Schicht 3.
```

Warum VLAN und Subnetz oft zusammengehören

Wenn zwei VLANs getrennte Broadcast-Domänen sind, können Geräte darin nicht einfach direkt auf Schicht 2 miteinander kommunizieren.

Damit Kommunikation zwischen VLANs möglich ist, braucht man Routing.

Routing arbeitet auf Schicht 3.

Deshalb plant man meistens:

```
ein VLAN
=
ein eigenes IP-Subnetz
```

Beispiel:

```
VLAN 10 → 192.168.10.0/24
VLAN 20 → 192.168.20.0/24
```

Merksatz:

```
Pro VLAN häufig ein eigenes IP-Subnetz.
```

Access-Port

Ein Access-Port ist ein Switch-Port, der normalerweise zu genau einem VLAN gehört.

Typischer Einsatz:

```
- PC
- Drucker
- IP-Kamera
- einzelnes Endgerät
- einfacher Access Point
- VoIP-Telefon mit bestimmter Konfiguration
```

Beispiel:

```
Port 1 ist Access-Port in VLAN 10.
```

Ein Gerät an Port 1 gehört dann logisch zu VLAN 10.

Merksatz:

```
Access-Port = ein VLAN für ein Endgerät.
```

Access-Port-Beispiel

Beispiel-Switch:

Port	Modus	VLAN	Gerät
1	Access	10	Mitarbeiter-PC
2	Access	10	Mitarbeiter-PC
3	Access	20	Gäste-PC
4	Access	30	Server

Wichtig:

> Geräte an Access-Ports müssen normalerweise nichts von VLANs wissen.

Der Switch ordnet den Port intern dem VLAN zu.

Merksatz:

> Beim Access-Port übernimmt der Switch die VLAN-Zuordnung.

Trunk-Port

Ein Trunk-Port kann mehrere VLANs über eine einzige Verbindung transportieren.

Typischer Einsatz:

> - Switch zu Switch
> - Switch zu Router
> - Switch zu Firewall
> - Switch zu Access Point mit mehreren SSIDs
> - Switch zu Virtualisierungshost

Beispiel:

> VLAN 10
> VLAN 20
> VLAN 30

laufen gemeinsam über einen Trunk-Port.

Merksatz:

```
Trunk-Port = mehrere VLANs über eine Verbindung.
```

Warum braucht man Trunk-Ports?

Trunk-Ports werden benötigt, wenn mehrere VLANs über eine gemeinsame Verbindung transportiert werden sollen.

Beispiel:

```
Switch A hat VLAN 10, 20 und 30.
Switch B soll diese VLANs ebenfalls nutzen.
```

Dann braucht die Verbindung zwischen beiden Switches einen Trunk.

Ohne Trunk müsste man für jedes VLAN eine eigene physische Verbindung verwenden.

Merksatz:

```
Trunk spart Kabel,
indem mehrere VLANs über eine Verbindung laufen.
```

VLAN-Tagging

Damit ein Trunk mehrere VLANs unterscheiden kann, müssen Frames markiert werden.

Diese Markierung nennt man:

```
VLAN-Tag
```

Der VLAN-Tag enthält die VLAN-ID.

Dadurch weiß die Gegenstelle:

```
Dieser Frame gehört zu VLAN 10.
Dieser Frame gehört zu VLAN 20.
Dieser Frame gehört zu VLAN 30.
```

Merksatz:

```
VLAN-Tag = Markierung eines Frames mit der VLAN-ID.
```

IEEE 802.1Q

IEEE 802.1Q ist der Standard für VLAN-Tagging bei Ethernet.

802.1Q fügt einem Ethernet-Frame eine VLAN-Information hinzu.

Diese Information enthält unter anderem:

```
- VLAN-ID
- Prioritätsinformationen
```

Für AP1/AP2 ist besonders wichtig:

```
802.1Q = VLAN-Tagging bei Ethernet
```

Merksatz:

```
IEEE 802.1Q = VLAN-Tagging-Standard.
```

Tagged und Untagged

Bei VLANs unterscheidet man häufig:

```
tagged
untagged
```

Tagged bedeutet:

```
Der Ethernet-Frame enthält einen VLAN-Tag.
```

Untagged bedeutet:

```
Der Ethernet-Frame enthält keinen VLAN-Tag.
```

Typisch:

```
Access-Port:
meist untagged zum Endgerät

Trunk-Port:
mehrere VLANs tagged
```

Merksatz:

```
tagged = mit VLAN-Markierung.
untagged = ohne VLAN-Markierung.
```

Access-Port und untagged Frames

Ein normales Endgerät an einem Access-Port sendet meist untagged Frames.

Das bedeutet:

```
Der PC sendet normale Ethernet-Frames ohne VLAN-Tag.
```

Der Switch weiß aber:

```
Dieser Port gehört zu VLAN 10.
```

Also ordnet der Switch die Frames intern VLAN 10 zu.

Merksatz:

```
Access-Port: Endgerät sendet meist untagged,
Switch ordnet VLAN zu.
```

Trunk-Port und tagged Frames

Auf einem Trunk-Port laufen mehrere VLANs.

Damit die Gegenstelle die VLANs unterscheiden kann, werden Frames meistens tagged übertragen.

Beispiel:

```
Frame mit Tag VLAN 10
Frame mit Tag VLAN 20
Frame mit Tag VLAN 30
```

Die Gegenstelle liest den VLAN-Tag und ordnet den Frame dem richtigen VLAN zu.

Merksatz:

```
Trunk-Port: mehrere VLANs werden durch Tags unterschieden.
```

Native VLAN

Bei manchen Switch-Konzepten gibt es auf Trunk-Ports ein sogenanntes Native VLAN.

Das Native VLAN ist das VLAN, dessen Frames auf einem Trunk untagged übertragen werden können.

Wichtig:

```
Falsch konfigurierte Native VLANs können Sicherheits- oder Verbindungsprobleme verursachen.
```

Für die Prüfung reicht meistens:

```
Native VLAN = untagged VLAN auf einem Trunk
```

Merksatz:

```
Native VLAN auf beiden Seiten eines Trunks korrekt konfigurieren.
```

Allowed VLANs

Auf einem Trunk kann festgelegt werden, welche VLANs erlaubt sind.

Beispiel:

```
erlaubt:
VLAN 10
VLAN 20
```

VLAN 30

nicht erlaubt:
VLAN 40

Wenn ein VLAN auf dem Trunk nicht erlaubt ist, wird es darüber nicht transportiert.

Merksatz:

Allowed VLANs bestimmen,
welche VLANs über einen Trunk laufen dürfen.

VLANs und WLAN

Access Points können mehrere WLAN-Namen bereitstellen.

Diese WLAN-Namen heißen:

SSIDs

Jede SSID kann einem eigenen VLAN zugeordnet werden.

Beispiel:

SSID	VLAN	Zweck
Firma-Mitarbeiter	VLAN 10	internes Netzwerk
Firma-Gast	VLAN 20	Gastzugang
Firma-IoT	VLAN 30	Geräte-Netz

Der Switch-Port zum Access Point ist dann oft ein Trunk-Port.

Merksatz:

Mehrere SSIDs nutzen häufig VLANs über einen Trunk.

VLANs und VoIP

VoIP steht für:

Voice over IP

In Unternehmen gibt es häufig ein eigenes VLAN für Telefone.

Beispiel:

VLAN 10 = PCs
VLAN 40 = VoIP-Telefone

Warum?

- Sprachverkehr kann getrennt behandelt werden
- Priorisierung ist einfacher
- Sicherheit und Übersicht werden besser
- eigene DHCP-Optionen können genutzt werden

Merksatz:

VoIP wird oft in einem eigenen VLAN betrieben.

Management-VLAN

Ein Management-VLAN wird zur Verwaltung von Netzwerkgeräten verwendet.

Darin befinden sich zum Beispiel:

- Switch-Management
- Access-Point-Management
- Controller
- Monitoring-Systeme
- Administrationszugänge

Ziel:

Management-Zugriffe sollen vom normalen Benutzerverkehr getrennt werden.

Merksatz:

```
Management-VLAN = separates Netz für Verwaltung.
```

Gast-VLAN

Ein Gast-VLAN ist ein separates Netz für Besucher oder private Geräte.

Ziel:

```
Gäste sollen Internetzugang haben,
aber keinen Zugriff auf interne Systeme.
```

Typische Regeln:

```
Gast-VLAN → Internet erlaubt
Gast-VLAN → interne Server blockiert
Gast-VLAN → andere Gäste eventuell blockiert
```

Merksatz:

```
Gast-VLAN vom internen Netzwerk trennen.
```

IoT-VLAN

IoT steht für:

```
Internet of Things
```

In einem IoT-VLAN können Geräte gesammelt werden wie:

```
- Kameras
- Sensoren
- Smart-TVs
- Drucker
- Steuergeräte
- andere eingebettete Geräte
```

Warum?

IoT-Geräte sind oft schlechter wartbar oder unsicherer als normale Clients.

Ein eigenes VLAN erleichtert Kontrolle und Firewall-Regeln.

Merksatz:

IoT-Geräte sinnvoll vom normalen Client-Netz trennen.

Inter-VLAN-Routing

Geräte in unterschiedlichen VLANs können nicht direkt nur über Schicht 2 miteinander kommunizieren.

Wenn VLAN 10 mit VLAN 20 kommunizieren soll, braucht man Routing.

Das nennt man:

Inter-VLAN-Routing

Dafür nutzt man zum Beispiel:

- Router
- Layer-3-Switch
- Firewall

Merksatz:

Kommunikation zwischen VLANs braucht Schicht-3-Routing.

Router-on-a-Stick

Router-on-a-Stick ist eine Methode für Inter-VLAN-Routing.

Dabei verbindet ein einzelner physischer Router-Port mehrere VLANs über einen Trunk.

Der Router besitzt dafür logische Unterinterfaces.

Beispiel:

```
Router-Port
mit VLAN 10
VLAN 20
VLAN 30
```

über eine Trunk-Verbindung zum Switch.

Merksatz:

```
Router-on-a-Stick = Inter-VLAN-Routing über einen Trunk zum Router.
```

Layer-3-Switch

Ein Layer-3-Switch kann Switching und Routing kombinieren.

Er kann:

```
- auf Schicht 2 Frames switchen
- auf Schicht 3 zwischen VLANs routen
```

In größeren Netzwerken ist Inter-VLAN-Routing häufig auf einem Layer-3-Switch umgesetzt.

Merksatz:

```
Layer-3-Switch = Switch mit Routing-Funktion.
```

Firewall zwischen VLANs

In vielen Netzwerken wird die Kommunikation zwischen VLANs über eine Firewall geregelt.

Beispiel:

```
Mitarbeiter-VLAN darf auf Server-VLAN zugreifen.
Gast-VLAN darf nur ins Internet.
IoT-VLAN darf nur bestimmte Dienste erreichen.
```

Vorteil:

Zugriffe können kontrolliert und protokolliert werden.

Merksatz:

VLAN-Trennung wird durch Firewall-Regeln wirksam abgesichert.

VLANs und Sicherheit

VLANs erhöhen die Sicherheit, weil sie Netzbereiche logisch trennen.

Aber:

VLANs allein sind keine vollständige Sicherheitslösung.

Zusätzlich braucht man je nach Umgebung:

- Firewall-Regeln
- Zugriffskontrolle
- sichere Switch-Konfiguration
- 802.1X
- Port Security
- Monitoring
- saubere Dokumentation

Merksatz:

VLAN trennt logisch,
Firewall regelt den Zugriff.

VLANs und DHCP

DHCP stellt IP-Adressen automatisch bereit.

Da VLANs meist eigene IP-Subnetze haben, benötigt jedes VLAN eine passende DHCP-Konfiguration.

Beispiel:

VLAN	Subnetz	DHCP-Bereich
10	192.168.10.0/24	192.168.10.100–192.168.10.200
20	192.168.20.0/24	192.168.20.100–192.168.20.200
30	192.168.30.0/24	192.168.30.100–192.168.30.200

Wenn ein Client im falschen VLAN ist, bekommt er eventuell eine falsche oder keine IP-Adresse.

Merksatz:

```
VLAN und DHCP-Bereich müssen zusammenpassen.
```

DHCP-Relay

Ein DHCP-Server steht nicht immer direkt in jedem VLAN.

Wenn Clients in mehreren VLANs IP-Adressen erhalten sollen, kann ein DHCP-Relay eingesetzt werden.

Aufgabe:

```
DHCP-Anfragen aus einem VLAN an einen zentralen DHCP-Server weiterleiten.
```

DHCP-Relay arbeitet im Zusammenspiel mit Schicht 3.

Merksatz:

```
DHCP-Relay hilft,
DHCP über VLAN-Grenzen hinweg zu nutzen.
```

VLANs und Fehlersuche

Typische VLAN-Fehler:

```
- Port im falschen VLAN
- Access-Port statt Trunk
- Trunk statt Access-Port
- VLAN auf Trunk nicht erlaubt
- falsches Native VLAN
```

- VLAN auf Switch nicht angelegt
- falsche SSID-VLAN-Zuordnung
- falscher DHCP-Bereich
- fehlendes Inter-VLAN-Routing
- Firewall blockiert Kommunikation

Merksatz:

VLAN-Fehler wirken oft wie IP- oder DHCP-Probleme.

Fehlerbild: Client bekommt falsche IP-Adresse

Mögliche Ursache:

Der Switch-Port ist im falschen VLAN.

Beispiel:

Client soll in VLAN 10 sein.
Port ist aber in VLAN 20.

Folge:

Client erhält eine IP-Adresse aus dem falschen Subnetz
oder erreicht nicht die erwarteten Dienste.

Merksatz:

Falsches VLAN kann falsche IP-Adresse verursachen.

Fehlerbild: Access Point mit mehreren SSIDs funktioniert nicht richtig

Mögliche Ursachen:

- Switch-Port ist kein Trunk
- VLANs sind auf dem Trunk nicht erlaubt
- SSID ist falschem VLAN zugeordnet

- Native VLAN falsch
- DHCP fehlt für ein VLAN
- Firewall blockiert Gastnetz
- Access Point unterstützt Konfiguration nicht

Merksatz:

Mehrere SSIDs brauchen meist korrektes VLAN-Tagging.

Fehlerbild: Zwei VLANs erreichen sich nicht

Mögliche Ursachen:

- kein Inter-VLAN-Routing
- falsches Gateway
- Firewall blockiert
- falsche Subnetzmaske
- VLAN nicht korrekt angelegt
- Trunk transportiert VLAN nicht
- Routing-Schnittstelle fehlt

Wichtig:

Wenn zwei VLANs kommunizieren sollen,
braucht man eine Schicht-3-Komponente.

Merksatz:

VLAN zu VLAN braucht Routing.

Einordnung in das OSI-Modell

Thema	Schicht
VLAN	Schicht 2
VLAN-Tag	Schicht 2
Access-Port	Schicht 2
Trunk-Port	Schicht 2

Thema	Schicht
MAC-Adresse	Schicht 2
Broadcast-Domäne	Schicht 2
IP-Subnetz	Schicht 3
Inter-VLAN-Routing	Schicht 3
DHCP	Anwendungsschicht mit Netzwerkbezug
Firewall-Regeln nach IP/Port	Schicht 3 / 4

Merksatz:

> VLAN ist Schicht 2.
> Routing zwischen VLANs ist Schicht 3.

VLAN und Subnetz nicht verwechseln

Begriff	Schicht	Aufgabe
VLAN	2	logische Trennung im LAN
Subnetz	3	logischer IP-Adressbereich
Router / Layer-3-Switch	3	Verbindung zwischen Netzen
Firewall	3 / 4 / 7	Zugriff kontrollieren

Wichtig:

> In der Praxis werden VLAN und Subnetz oft gemeinsam geplant,
> bleiben aber unterschiedliche Konzepte.

Merksatz:

> VLAN trennt Frames.
> Subnetz trennt IP-Bereiche.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist ein VLAN?
- Auf welcher OSI-Schicht arbeitet ein VLAN?
- Was ist eine Broadcast-Domäne?
- Warum nutzt man VLANs?
- Was ist eine VLAN-ID?
- Was ist der Unterschied zwischen Access-Port und Trunk-Port?
- Was bedeutet VLAN-Tagging?
- Was ist IEEE 802.1Q?
- Was bedeutet tagged und untagged?
- Warum braucht man Inter-VLAN-Routing?
- Was ist Router-on-a-Stick?
- Warum ist ein VLAN nicht dasselbe wie ein IP-Subnetz?
- Warum kann ein falsches VLAN zu DHCP-Problemen führen?
- Warum reichen VLANs allein nicht als vollständige Sicherheitslösung?

Typische Prüfungsfallen

VLANs gehören zu Schicht 2.

IP-Subnetze gehören zu Schicht 3.

VLAN und Subnetz sind nicht dasselbe.

Ein VLAN bildet normalerweise eine Broadcast-Domäne.

Access-Port = normalerweise ein VLAN.

Trunk-Port = mehrere VLANs.

Tagged = mit VLAN-Tag.

Untagged = ohne VLAN-Tag.

IEEE 802.1Q = VLAN-Tagging.

Kommunikation zwischen VLANs braucht Routing.

VLANs allein ersetzen keine Firewall-Regeln.

Falsches VLAN kann wie ein IP- oder DHCP-Problem aussehen.

Mehrere SSIDs auf einem Access Point nutzen häufig VLANs.

Native VLAN muss auf Trunk-Verbindungen korrekt passen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
VLAN	Virtual Local Area Network, logisches LAN
VLAN-ID	Nummer eines VLANs
VLAN-Name	lesbarer Name eines VLANs
Broadcast	Nachricht an alle im lokalen Netz
Broadcast-Domäne	Bereich, in dem Broadcasts verteilt werden
Access-Port	Switch-Port für ein einzelnes VLAN
Trunk-Port	Switch-Port für mehrere VLANs
VLAN-Tag	Markierung eines Frames mit VLAN-ID
IEEE 802.1Q	Standard für VLAN-Tagging
tagged	Frame mit VLAN-Tag
untagged	Frame ohne VLAN-Tag
Native VLAN	untagged VLAN auf einem Trunk
Allowed VLANs	VLANs, die über einen Trunk erlaubt sind
Inter-VLAN-Routing	Routing zwischen VLANs
Router-on-a-Stick	Inter-VLAN-Routing über Router-Trunk
Layer-3-Switch	Switch mit Routing-Funktion
Management-VLAN	VLAN zur Verwaltung von Netzwerkgeräten
Gast-VLAN	separates VLAN für Gäste
IoT-VLAN	separates VLAN für IoT-Geräte
DHCP-Relay	Weiterleitung von DHCP-Anfragen zu zentralem DHCP-Server

---

IHK-sichere Kurzformulierung

Ein VLAN ist ein virtuelles lokales Netzwerk auf OSI-Schicht 2. Mit VLANs können Geräte logisch getrennt werden, auch wenn sie an derselben physischen Switch-Infrastruktur angeschlossen sind. Ein VLAN bildet normalerweise eine eigene Broadcast-Domäne. Access-Ports gehören meist zu genau einem VLAN und werden für Endgeräte verwendet. Trunk-Ports können mehrere VLANs transportieren und nutzen dafür VLAN-Tagging nach IEEE 802.1Q. VLANs sind nicht dasselbe wie IP-Subnetze, werden in der Praxis aber häufig gemeinsam geplant. Kommunikation zwischen VLANs benötigt Routing, zum Beispiel über einen Router, eine Firewall oder einen Layer-3-Switch.

Merksätze

VLAN = Virtual Local Area Network.

VLAN = logische Netztrennung auf Schicht 2.

Ein VLAN bildet eine Broadcast-Domäne.

VLAN-ID = Nummer des VLANs.

VLAN-Name = lesbare Bezeichnung.

VLAN ist nicht IP-Subnetz.

VLAN = Schicht 2.

IP-Subnetz = Schicht 3.

Pro VLAN häufig ein eigenes Subnetz.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

Tagged = mit VLAN-Tag.

Untagged = ohne VLAN-Tag.

IEEE 802.1Q = VLAN-Tagging.

Native VLAN = untagged VLAN auf einem Trunk.

Allowed VLANs bestimmen,
welche VLANs über einen Trunk laufen.

Mehrere SSIDs nutzen häufig VLANs.

Gast-VLAN vom internen Netz trennen.

IoT-VLAN für unsichere Geräte sinnvoll.

VLAN zu VLAN braucht Routing.

Router-on-a-Stick = Inter-VLAN-Routing über Trunk.

Layer-3-Switch kann zwischen VLANs routen.

VLAN trennt logisch,
Firewall regelt den Zugriff.

Falsches VLAN kann DHCP- und IP-Probleme verursachen.