Netzwerk - VLAN (Virtual Local Area Network)

Was ist ein VLAN?

- Ein VLAN ist eine logische Unterteilung eines physischen Netzwerks in mehrere isolated Broadcast-Domains.

- Geräte in verschiedenen VLANs sehen einander standardmäßig nicht direkt, auch wenn sie sich im gleichen physischen Netzwerk befinden.

- Ein VLAN wird durch eine VLAN-ID (802.1Q-Tagging) markiert, damit Switches wissen, zu welchem logischen Segment ein Frame gehört.

<u>Wichtige Konzepte</u>

- Access-Ports vs. Trunk-Ports:

  - Access-Port: Ein einzelnes VLAN direkt für Endgeräte (PC, Drucker). Frames tragen kein Tag, der Switch ordnet sie dem richtigen VLAN zu.

  - Trunk-Port: Verbindet Switches oder Switch zu Routern/Firewalls. Trägt mehrere VLANs über Tags (802.1Q).

- Inter-VLAN-Routing:

  - Standardweg: Ein Layer-3-Gerät (Managed Switch oder Router) routet zwischen VLANs. Ohne dieses Routing bleiben VLANs voneinander isoliert.

- DHCP und DNS pro VLAN:

  - Jedes VLAN braucht idealerweise einen DHCP-Server oder-relay, damit Clients IPs erhalten.

  - DNS-Auflösung funktioniert meist transparent, aber Hosts können je VLAN unterschiedliche DNS-Server nutzen.

- Sicherheit:

  - VLANs erhöhen die Sicherheit durch Segmentierung, aber erfordern zusätzliche Schutzmaßnahmen gegen falsches Tagging (VLAN Hopping) und Fehlkonfigurationen.

Typische VLAN-BN-Beispiele (was sinnvoll ist)

- Management: Nur Geräte wie Switch- und Router-Management, Server-Admin-PCs

- Nutzer/Arbeitsplätze: Büroarbeitsplätze

- Server: Hypervisor, Datenbank-, App-Servern

- Voice: VoIP-Telefone mit dediziertem VLAN

- Guest: Gäste-WLAN, eingeschränkter Zugriff

- IoT: Drucker, Sensoren, Kameras (oft restriktiv)

- Backup/Storage: Speicher-Netzwerk-Komponenten (vorgeschriebene Pfade)

Was ist zu beachten (Best Practices)

- Klare VLAN-Planung:

  - Erstelle eine, sinnvoll logische VLAN-Struktur, vermeide unnötig feine Unterteilung.

  - Dokumentiere: VLAN-ID, Zweck, Zugehörige Subnetze, Router-Interfaces.

- Konsistente Adressierung:

  - Weisen Sie jedem VLAN ein eigenes Subnetz zu (z. B. 10.0.10.0/24 für VLAN 10).

  - Vermeide Überlappungen; halte Subnetze klein genug für Broadcast-Domänen, aber groß genug für Wachstum.

- Inter-VLAN-Routing:

  - Nutze zentrale Router/Switches für Routing (Layer-3-Switch). Vermeide unübersichtliche „double-hop“-Konfiguration.

- Sicherheit und Zugriffskontrollen:

  - Beschränke Routing zwischen sensiblen VLANs (Zugriffslisten, Firewall-Policies).

  - Nutze Private VLANs, Falls nötig, um Host-Kommunikation weiter zu isolieren.

  - DHCP-Snooping, ARP-Inspektion, Port-Security, und Spanning Tree (RSTP/MSTP) korrekt konfigurieren.

- Trunk-Verbindungen sinnvoll nutzen:

  - Nur notwendige VLANs über Trunks, Trunk-Pruning und Allowed-VLANs verwenden.

- QoS:

  - Priorisiere Voice- und Video-Traffic, besonders in VLANs mit Telefonie/Video-Konferenz.

- Monitoring und Troubleshooting:

  - VLAN- und Port-basierte Logs, Network-Flow-Mm, CLI-Skripte, regelmäßig überprüfen.

- DHCP- und DNS-Plan:

  - DHCP-Scopes sinnvoll pro VLAN anlegen; Relay-Agents auf dem Router/Switch.

  - Falls nötig, Trennung von DNS-Resolvern pro VLAN oder zentrale DNS-Dienste nutzen.

- Skalierbarkeit:

- Vermeide Explosion von VLANs auf einzelnen Trunk-Links; plane ausreichend Port- und Bandbreitenkapazität.

- Dokumentiere Änderungen versioniert.

Typische Optimierungstipps

- Nutze Aggregation/Trunks statt Einzelverbindungen, wo sinnvoll, aber beschränke die Anzahl der VLANs pro Trunk (Allowed-VLANs).

- Verwende Layer-3-Switching dort, wo viele VLANs viel Routing benötigen; reduziert Broadcast-Storms und verbessert Performance.

- Segmentiere Broadcast-Domänen sinnvoll, verringere unnötiges Broadcast-Verkehr, besonders in großen Netzwerken.

- Reserve Separate VLANs für Management, um den Zugriff auf Switch-Konfiguration abzuschirmen.

- Setze Access-Listen (ACLs) auf dem Router/Switch ein, um nur notwendige Verkehrsmuster zwischen VLANs zu erlauben.

- Nutze Port-Based- oder 802.1X-Authentifizierung, um unerlaubte Geräte im VLAN zu verhindern.

- Beachte MTU-Größe auf Trunks (802.1Q overhead) – sicherstellen, dass Frames nicht fragmentiert werden.

- Halte Firmware/Software der Switches aktuell; implementiere Sicherheits- und Stabilitäts-Patches zeitnah.

Ein einfaches Beispiel für ein VLAN-Layout

- VLAN 10: Management (Subnetz 10.0.10.0/24)

- VLAN 20: Büro-Arbeitsplätze (Subnetz 10.0.20.0/24)

- VLAN 30: Server (Subnetz 10.0.30.0/24)

- VLAN 40: VoIP (Subnetz 10.0.40.0/24)

- VLAN 50: Gäste (Subnetz 10.0.50.0/24)

- VLAN 60: IoT (Subnetz 10.0.60.0/24)

Typische Fehlerquellen

- Falsche Tagging-Einstellungen am Trunk (z. B. unbeabsichtigtes Tagging auf Access-Ports).

- Inter-VLAN-Routing fehlt oder falsch konfiguriert (Clients können sich nicht erreichen oder VLANs sehen sich gegenseitig ungefiltert).

- DHCP-Konflikte (gleiche IP-Bereiche in mehreren VLANs) oder fehlende DHCP-Relays.

- Sicherheitslücken durch ungetrennte Verwaltungs- und Benutzerschnittstellen.

Zusammenfassung

- VLANs sind sinnvoll, um Netzwerke logisch zu segmentieren, Sicherheit zu erhöhen und Broadcast-Verkehr zu reduzieren.

- Planung, klare Subnetze, gezieltes Routing, gemeinsame Sicherheitsrichtlinien und regelmäßige Wartung sind der Schlüssel.

- Durch gezielte Trennung (Management, Nutzer, Server, VoIP, Gäste, IoT) lassen sich Performance, Sicherheit und Übersicht deutlich verbessern.