

Dokumentation
2022 / 2023

VERSUCH SWITCHKONFIGURATION



Bonjov Hima
Bjarne Doench
Marius Starke

Betreut durch: Herr Ransch

Inhalt

1 Projektbeschreibung	1
2 Vorbereitung	2
2.1 Begriffserklärung	2
2.1.1 Switch-Stacking	2
2.1.2 Switchkaskadierung	2
2.1.3 Spanning-Tree-Verfahren	2
2.1.4 Auto-Negotiation	3
2.1.5 AutoUplink(MDI/MDI-X)	3
2.1.6 Link Aggregation/ Port Trunking	3
2.1.7 Vollduplex-Betrieb	3
2.1.8 Mac-Adressenfilter	4
2.2 Netzwerktrennung	4
2.2.1 VLAN	4
2.2.2 Vorteile von VLAN	5
2.2.3 VLAN-fähige Switches sind der Schlüssel	5
2.2.4 Zu welchem VLAN gehört ein Frame?	6
2.2.5 Wie funktioniert ein VLAN-fähiger Switch?	6
2.2.6 VLAN-Tagging	7
2.2.7 Normen und Interoperabilität	7
2.2.8 VLAN-Trunking	8
2.3 Übersicht des NETGEAR-Switches	9
3 Versuchsaufbau	10
3.1 Szenario	10
3.2 Durchführung	10
3.2.1 Funktionsprüfung des Netzwerks	10
3.2.2 Unterteilung in Subnetze	10
3.2.3 Trennung durch VLAN herstellen	12
3.2.4 VLAN übergreifenden Server integrieren	14
3.2.5 Einrichtung Layer2-Switches	16
4 Auswertung	17
4.1 Grundlagen Switchkonfiguration	17
4.2 Vergleich und Beurteilung	18
Literatur	19
Glossar	20
Abbildungsverzeichnis	21
Abkürzungsverzeichnis	22
Eidesstattliche Erklärung	23

1 Projektbeschreibung

In einer Firma „Mustermann GbR“ sollen die Abteilungen durch die Einrichtung von VLANs logisch unterschieden werden, d.h. dass alle PCs einer Abteilung untereinander, aber nicht mit den Rechnern anderer Abteilungen Daten austauschen können.

2 Vorbereitung

2.1 Begriffserklärung

2.1.1 Switch-Stacking

Switch-Stacking ist ein wichtiges Merkmal von Netzwerk-Switches. Diese Switches können miteinander verbunden werden, um als logische Einheit zu fungieren. Durch das Zusammenschalten weiterer Switches, wird die Netzwerkkapazität dank der höheren Anzahl verfügbarer Ports, besserer Ausfallsicherheit und der Möglichkeit Link-Aggregation zu betreiben, erheblich erhöht. Switch-Stacking wird nur von stapelbaren Switches unterstützt.

Switches in einem Stack können mittels DAC-Kabeln, optischen Transceiver oder Stacking-Kabeln verbunden werden. Es gibt einen Stack-Master, der das Zentrum des Stack-Systems ist und die Konfigurationsdaten verwaltet. Die anderen Switches im Stack werden als Stack-Slaves bezeichnet. Der Stack-Master kann von Benutzern verwaltet werden, und falls er ausfällt, wird ein neuer Master-Switch unter den Slaves ausgewählt.

Zusammenfassend lassen sich folgende Vorteile von Switch-Stacking erschließen:

- Verbesserung der Zuverlässigkeit und Flexibilität des Netzwerkes
- Erhöhung der Bandbreite und Vereinfachung der Vernetzung
- hohe Skalierbarkeit des Netzwerkes

2.1.2 Switchkaskadierung

Kaskadierung ist die traditionelle Methode zum Verbinden mehrerer Ethernet-Switches und umfasst verschiedene Methoden für unterschiedliche Netzwerktopologien.

Durch die Verknüpfung mehrerer Switches können Benutzer mehrere Ports haben, die jeden Switch miteinander verbinden, unabhängig voneinander konfiguriert und als Gruppe verwaltet werden können. In einem Kaskaden-Switch-Netzwerk sind Daisy-Chain-Topologie und Sterntopologie zwei gängige Methoden.

2.1.3 Spanning-Tree-Verfahren

Der Spanning-Tree-Algorithmus führt eine Reihe von Schritten aus, um sicherzustellen, dass die Topologie schleifenfrei ist und das Ethernet ordnungsgemäß funktioniert:

1. Root-Bridge-Auswahl – Zuerst wählt STP eine Root-Bridge aus. Dies ist der wichtigste Schalter in der Topologie. Es ist die Wurzel des azyklischen Baums.
2. Schleifentopologie-Erkennung – Sobald die Root-Bridge ausgewählt ist, beginnt sie mit dem Senden von Spanning-Tree-Nachrichten (BPDU's). Der Switch verwendet diese Nachrichten, um den Teil der Topologie zu finden, der die Schleife enthält.
3. Bestimmen der Port-Rollen – Nach dem Bestimmen des Loop-Teils der Topologie platziert jeder Switch so viele Switch-Ports wie nötig, um sicherzustellen, dass die Topologie schleifenfrei ist.

4. Dropout – Switches tauschen weiterhin Nachrichten aus, um die Verfügbarkeit von Links und Nachbarkontakten zu verfolgen. Wenn die Verbindung oder der Switch ausfällt, führt der Switch die Schritte 2 und 3 erneut aus, um sicherzustellen, dass die neue Topologie schleifenfrei ist.

2.1.4 Auto-Negotiation

Auto-Negotiation ist eine Funktion, die es zwei Netzwerken mit unterschiedlichen Geschwindigkeiten ermöglicht, zu kommunizieren und sich an eine Geschwindigkeit anpasst, die für beide Netzwerke geeignet ist. Beispielsweise verfügt ein Switch über einen 1-Gbit/s-Port (Gigabit-Ethernet), der mit einem 100-Mbit/s-Port (Fast Ethernet) an einem anderen Switch verbunden ist. Die Portgeschwindigkeiten an beiden Enden müssen gleich sein, um eine Verbindung herzustellen. Das Autonegotiation-Protokoll teilt Baudrate, Duplexmodusstatus und Flusssteuerungsinformationen zwischen zwei Ports. Sobald der Port die obigen Parameterinformationen empfangen hat, passt er seinen Pegel entsprechend den Fähigkeiten des Peer-Ports an.

2.1.5 AutoUplink(MDI/MDI-X)

Ein Ethernet-Netzwerkport (z. B. an einem Switch) verwendet die automatische Uplink-Funktion, um zu erkennen, an welchen Switch er senden und empfangen (MDI/MDIX) soll. Mit der automatischen Uplink-Funktion können sowohl Crossover-Kabel als auch 1:1-Netzkabel verwendet werden.

2.1.6 Link Aggregation/ Port Trunking

Link Aggregation ist eine Methode zur Zusammenfassung mehrerer Netzwerkverbindungen zu einer logischen Verbindung. Clustering erhöht den Datendurchsatz und reduziert Fehler. Standardisiert ist das Verfahren im IEEE-Standard 802.1AX, der 2008 den älteren Standard 802.3ad ablöste. Neben diesen Standards gibt es auch herstellerspezifische Implementierungen.

“Port Trunking ist das Zusammenfassung der Verbindungen mehrerer physischer Ports zu einer logischen Verbindung höherer Bandbreite.“ [8]

Eine Trunk-Leitung kombiniert logisch oder physisch mehrere Kommunikationsverbindungen oder -kanäle zu einer einzigen Leitung oder logischen Verbindung. Diese angeschlossenen Leitungen werden in vielen verschiedenen Bereichen der Netzwerk- und Kommunikationstechnik, wie beispielsweise Switches, Telefonanlagen oder anderen Netzwerkkomponenten eingesetzt.

2.1.7 Vollduplex-Betrieb

In der Kommunikationstechnik bezeichnet Duplex (Vollduplex), Halbduplex oder Simplex die Richtwirkung des Kommunikationskanals.

- Simplex (SX) ist ein Richtungsbetrieb. Das bedeutet, dass Informationen nur in eine bestimmte Richtung übertragen werden (nur Nachrichten senden oder empfangen), z.B. Radio, TV oder Pager
- Halbduplex (HX), ist ein Zwei-Wege-Betrieb. Informationen können in beide Richtungen fließen, aber nicht gleichzeitig, z.B. Funkamateure
- Vollduplex (DX, manchmal FDX) ist ein synchroner Betrieb. Dadurch können Informationen gleichzeitig in beide Richtungen übertragen werden, z.B. Telefon

2.1.8 Mac-Adressenfilter

Ein MAC-Filter (MAC-Adressfilter) ist ein Netzwerkzugriffsschutz, der nur Geräten mit bestimmten MAC-Adressen den Zugriff auf das Netzwerk ermöglicht. MAC-Filter werden üblicherweise im LAN oder WLAN verwendet und sind als Tabelle im Router (Firewall) hinterlegt. Aus Sicherheitsgründen ist der MAC-Filter jedoch ein schwacher Zugriffsschutz, da er leicht umgangen werden kann.

2.2 Netzwerktrennung

2.2.1 VLAN

Die Virtual LAN (VLAN)-Technologie ermöglicht es Netzwerkadministratoren, die logische Netzwerkkonnektivität von der physischen Konnektivität zu trennen. Dieses Konzept unterscheidet sich von einem herkömmlichen LAN insofern, als ein LAN durch seine physische Konnektivität begrenzt ist. Alle Benutzer in einem LAN gehören zu einer einzigen Broadcast-Domäne und können auf der Datenverbindungsschicht oder SSchicht 2"miteinander kommunizieren. Netzwerkmanager haben VLANs verwendet, um ein komplexes Netzwerk in kleinere Einheiten aufzuteilen, um es besser verwalten zu können und die Leistung und Sicherheit zu verbessern. Zum Beispiel verwenden Netzwerkmanager ein VLAN für jedes IP-Subnetz in ihrem Netzwerk. Die Kommunikation zwischen den Subnetzen wird auf der Netzwerkschicht oder SSchicht 3"durch IP-Router ermöglicht.

Ein VLAN kann man sich als ein einziges physisches Netzwerk vorstellen, das logisch in einzelne LANs unterteilt werden kann, die unabhängig voneinander arbeiten können.

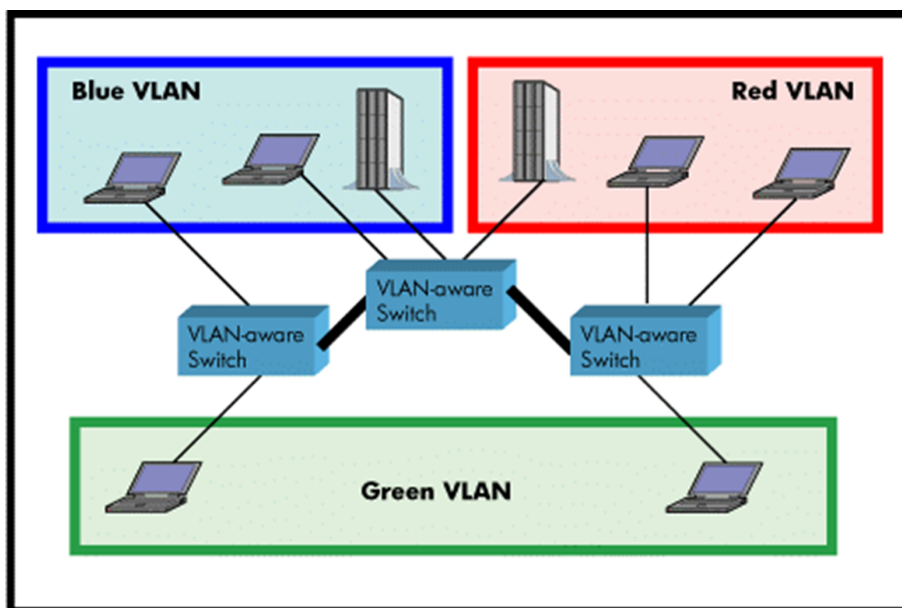


Abbildung 1: Verwenden von VLANs zum Erstellen unabhängiger Broadcast-Domänen über Switches hinweg

Abbildung 1 verdeutlicht einige wesentliche Unterschiede zwischen herkömmlichen LANs und VLANs.

- Alle Switches sind miteinander verbunden. Es gibt jedoch drei verschiedene VLANs oder Broadcast-Domänen im Netz. Eine physische Isolierung ist für die Definition von Broadcast-Domänen nicht erforderlich. Wenn Abbildung 1 ein herkömmliches LAN ohne VLAN-fähige Switches wäre, würden alle Stationen zu einer Broadcast-Domäne gehören.

- Alle Switch-Ports können auf der Datenübertragungsschicht miteinander kommunizieren, wenn sie Mitglieder desselben VLAN werden.
- Der physische Standort einer Endstation definiert nicht ihre LAN-Grenze.
 - Eine Endstation kann physisch von einem Switch-Port zu einem anderen verschoben werden, ohne ihre Sicht auf das Netzwerk zu verlieren. Das heißt, die Menge der Stationen, mit denen sie auf der Datenübertragungsschicht kommunizieren kann, bleibt dieselbe, vorausgesetzt, dass ihre VLAN-Mitgliedschaft ebenfalls von Port zu Port migriert wird.
 - Durch die Neukonfiguration der VLAN-Mitgliedschaft des Switch-Ports, an den eine Endstation angeschlossen ist, können Sie die Netzwerksicht der Endstation einfach ändern, ohne dass ein physischer Wechsel von Port zu Port erforderlich ist.

2.2.2 Vorteile von VLAN

Zu den wichtigsten Vorteilen der Verwendung von VLANs gehören die folgenden:

- **Bandbreitenerhalt:** Ein gut konzipiertes VLAN trägt dazu bei, den Broadcast- und Multicast-Verkehr auf die Stationen zu beschränken, die den mit diesem VLAN verbundenen Verkehr hören und darauf reagieren. Die Netzwerk- und Computerressourcen von nicht teilnehmenden Stationen werden nicht beeinträchtigt, wodurch die Leistung verbessert wird.
- **Verwaltbarkeit:** Umzüge, Hinzufügungen und Änderungen der Netzwerktopologie erfordern keine physischen Änderungen der Netzwerktopologie. Die Mobilität der Benutzer ist aufgrund der dynamischen Natur von VLANs viel einfacher. Physikalisch verteilte Arbeitsgruppen können logisch innerhalb derselben Broadcast-Domäne verbunden werden, so dass es so aussieht, als befänden sie sich im selben physischen LAN. Eine einzige physische Verbindung kann gleichzeitig mehrere IP-Subnetze bedienen, wenn subnetzbasierte VLANs auf dieser Verbindung konfiguriert sind. Endstationen, die VLANs verwenden, können lokal rudimentäre Class of Service (CoS) anbieten, indem sie dem Datenverkehr für bestimmte Aktivitäten Priorität einräumen.
- **Verbesserte Sicherheit:** Sie können verschiedene Sicherheitsdomänen einrichten, um verschiedene Sicherheitsstufen im Netzwerk bereitzustellen, da das Netzwerkdesign flexibler ist als das von herkömmlichen LANs. Da Frames nur dann an einen Zielport weitergeleitet werden, wenn der Port zum selben VLAN wie der Frame gehört, tragen VLANs dazu bei, die Isolierung des Datenverkehrs zu erzwingen, und bieten so eine zusätzliche Sicherheitsebene im Netzwerk.

2.2.3 VLAN-fähige Switches sind der Schlüssel

Um ein VLAN in Ihrem Netzwerk zu implementieren, müssen Sie VLAN-fähige Switches verwenden. In diesem Abschnitt wird beschrieben, wie sich VLAN-fähige Switches von herkömmlichen Switches unterscheiden. Um zu verstehen, wie die logische Partitionierung einer LAN-Infrastruktur mit Hilfe von VLAN erfolgt, ist es hilfreich, sich an die grundlegende Funktionsweise eines herkömmlichen Switch-LANs zu erinnern. Ohne auf die Details des Switch-Designs einzugehen, sollten Sie sich die folgenden zwei Regeln für die Funktionsweise eines herkömmlichen LAN-Switches merken:

1. Wenn der Switch einen Broadcast- oder Multicast-Frame von einem Anschluss empfängt, sendet er den Frame an alle anderen Anschlüsse des Switches.
2. Wenn der Switch einen Unicast-Frame empfängt, leitet er ihn nur an den Port weiter, an den er adressiert ist.

Ein VLAN-fähiger Switch ändert die beiden oben genannten Regeln wie folgt:

1. Wenn der Switch einen Broadcast- oder Multicast-Frame von einem Port empfängt, leitet er den Frame nur an die Ports weiter, die demselben VLAN angehören wie der Frame.
2. Wenn ein Switch einen Unicast-Frame empfängt, leitet er ihn nur dann an den Port weiter, an den er adressiert ist, wenn dieser Port zum selben VLAN gehört wie der Frame.
3. Eine eindeutige Nummer, die VLAN-ID, identifiziert jedes VLAN². Es handelt sich um ein 12-Bit-Feld im VLAN-Tag. Sie können theoretisch bis zu 4095 diskrete VLANs in Ihrem Netzwerk haben.

2.2.4 Zu welchem VLAN gehört ein Frame?

Im vorigen Abschnitt wurde festgestellt, dass ein Frame zu einem VLAN gehören kann. Die nächste Frage lautet: Wie wird diese Zuordnung vorgenommen?

- Ein VLAN-fähiger Switch kann die Zuordnung auf der Grundlage verschiedener Attribute des Rahmens (wie Ethernet- und IP-Header-Inhalt) vornehmen. Zu den Attributen gehören beispielsweise die MAC-Zieladresse, die IP-Adresse, der TCP-Port, das Protokoll der Netzwerkschicht usw.
- Attribute wie "der Switch-Port, an dem der Frame angekommen ist" können ebenfalls verwendet werden. In diesem Fall ordnet der Switch allen Frames, die an einem bestimmten Port ankommen, implizit eine VLAN-ID zu.
- Ein Frame kann explizite VLAN-Informationen in einem Tag enthalten, das dem Ethernet-Header hinzugefügt wird (explizites VLAN-Tagging).

2.2.5 Wie funktioniert ein VLAN-fähiger Switch?

Sie können VLAN-fähige Switches so konfigurieren, dass sie Ports zu einer VLAN-Gruppe oder zu Gruppen hinzufügen. Diese Switches führen zwei einfache, zusammenhängende Tabellen:

- eine Liste der Ports, die zu jedem auf dem Switch aktivierten VLAN gehören
- die Menge der VLANs, die an jedem Port aktiviert sind

Es gibt mehrere Varianten von VLAN-fähigen Switches:

- Die einfachsten dieser Switches unterstützen portbasierte VLANs. In einem portbasierten VLAN bestimmt der Switch-Port, an dem der Frame angekommen ist, die VLAN-Mitgliedschaft des Frames. Diese Switches können nicht mehr als ein VLAN pro Switch-Port unterstützen, es sei denn, sie unterstützen VLAN-Tagging, das in den folgenden Abschnitten erläutert wird. Ein einfaches portbasiertes VLAN, das VLAN-Tagging unterstützt, ist alles, was Sie zur Implementierung eines VLANs in einer HP-UX-Umgebung benötigen.

- Anspruchsvollere Switch-Angebote ermöglichen die Konfiguration von VLAN- Zugehörigkeitsregeln auf der Grundlage des Frame-Inhalts, wie MAC-Adresse, TCP/UDP-Port, IP- Adresse und so weiter. Dies kann die Switch-Leistung beeinträchtigen.
- VLAN-fähige Layer-3-Switches (oder Routing-Switches) übernehmen zusätzlich zur VLAN-Klassifizierung die Funktion der Schicht 3 (z. B. IP-Routing).

Im Hinblick auf andere Netzwerkgeräte ist Folgendes zu beachten:

- Sie können eine Endstation so konfigurieren, dass sie zu mehr als einem VLAN gehört.
- Geräte mit gemeinsam genutzter Bandbreite, wie z. B. Hubs, können nicht VLAN-kompatibel sein, obwohl sie in eine VLAN-Umgebung eingebunden werden können. Wenn ein Hub in einer VLAN-Umgebung verwendet wird, müssen alle Knoten an diesem Hub zum selben VLAN oder Satz von VLANs gehören, wodurch die Vorteile von VLANs eingeschränkt werden.
- Ein weit verbreiteter Irrglaube ist, dass Switching das Routing im Netzwerk ersetzen kann, weil sich mehrere IP-Subnetze eine einzige Switching-Infrastruktur mit VLANs teilen können. Denken Sie daran, dass VLAN eine reine Data Link Layer (Layer 2) Technologie ist. Sie müssen Router für die Kommunikation zwischen IP-Subnetzen verwenden, auch in einem VLAN. [Wenn Sie einen VLAN-fähigen Layer-3-Switch (Routing-Switch) verwenden (der bereits als eine der verfügbaren Arten von VLAN-fähigen Switches erwähnt wurde), benötigen Sie keinen separaten Router, da die VLAN-fähigen Routing-Switches sowohl die Layer-2- als auch die Layer-3-Funktionen beinhalten.]

2.2.6 VLAN-Tagging

Wie bereits erwähnt, können Sie die VLAN-Funktionalität durch explizites Frame-Tagging durch Switches und Endstationen implementieren. Netzwerk-Switches und -Endstationen, die über VLANs Bescheid wissen, werden als VLAN-bewusst bezeichnet. Netzwerk-Switches und -Endstationen, die VLAN-Tags interpretieren können, werden als VLAN-Tag-fähig bezeichnet. VLAN-Tag-fähige Switches und Endstationen fügen VLAN-Tags zu Standard-Ethernet-Frames hinzu - ein Prozess, der explizites Tagging genannt wird. Beim expliziten Tagging bestimmt die Endstation oder der Switch die VLAN-Zugehörigkeit eines Frames und fügt ein VLAN-Tag in den Frame-Header ein (siehe Abbildung 2), so dass nachgelagerte Link-Partner nur das Tag untersuchen können, um die VLAN-Zugehörigkeit zu bestimmen. Das Tagging hat mehrere Vorteile: Die VLAN-Zuordnung muss nur einmal an einer Endstation oder an einem Edge-Switch vorgenommen werden, so dass die nachgeschalteten Switches auf dem gesamten Weg zum Ziel von der Klassifizierung der Frames entlastet werden. Das Tagging an Endstationen ist besonders vorteilhaft, da der Overhead der Rahmenklassifizierung verteilt wird.

2.2.7 Normen und Interoperabilität

IEEE 802.1Q spezifiziert die Architektur für VLAN-Tagging - Tag-Format, Tag-Einfügung und Tag-Stripping. Das IEEE 802.1Q-Tag (in Abbildung 2 für einen Ethernet-Frame dargestellt) enthält auch eine Bestimmung für die Prioritätskodierung. Das 3-Bit-Prioritätsfeld im getaggten Frame enthält Prioritätsinformationen. IEEE 802.1p (später in IEEE 802.1D aufgenommen) hat diese Prioritätskodierung standardisiert.

2.2.8 VLAN-Trunking

Switches, die nur portbasiertes VLAN implementieren, können nur ein VLAN pro Port unterstützen. Wenn sie jedoch Tag-fähig sind (auch Q-kompatibel genannt), können sie mehrere VLANs pro Port unterstützen - ein nicht getaggttes VLAN und mehrere getaggte VLANs. Wenn ein Frame kein explizites VLAN-Tag hat, wird ihm automatisch die üntaggted VLAN IDöder die "default VLAN ID-ßugewiesen. Ein eingehender Frame, der getaggt ist, hat seine VLAN-ID im Frame-Header. Einige Switch-Anbieter bezeichnen die Möglichkeit, mehrere getaggtte Frames pro Anschluss zu verarbeiten, als VLAN-Trunking.

2.3 Übersicht des NETGEAR-Switches

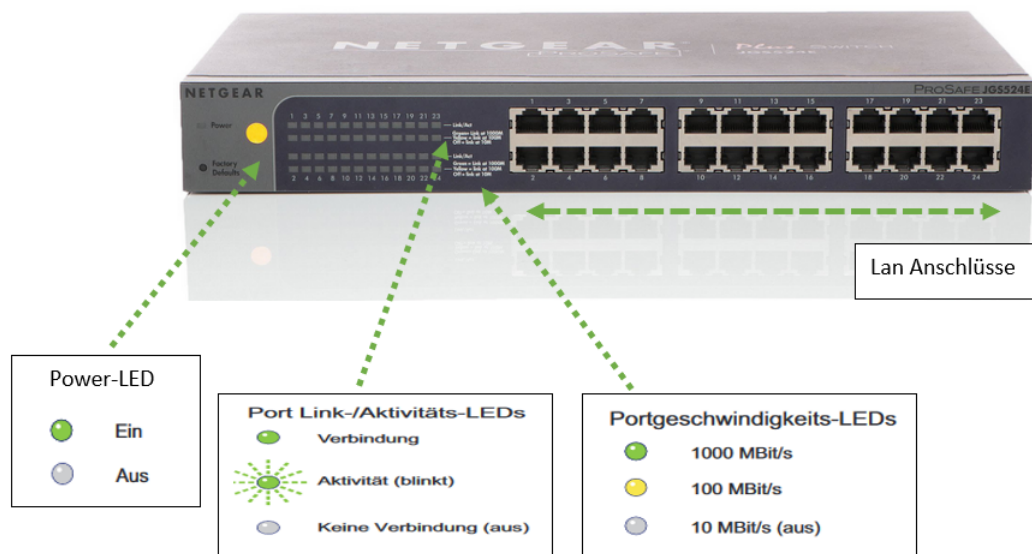


Abbildung 2: NETGEAR-Switch Vorderansicht



Abbildung 3: NETGEAR-Switch Rückansicht

3 Versuchsaufbau

3.1 Szenario

Im ersten Schritt wurde das Netzwerk mithilfe von Subnetting getrennt und anschließend unter Verwendung von managebaren NETGEAR-Switches in unterschiedliche VLANs unterteilt.

3.2 Durchführung

3.2.1 Funktionsprüfung des Netzwerks

	PC1	PC2	PC3	PC4
PC1		X		
PC2	X			
PC3				X
PC4			X	

Tabelle 1: Ergebnistabelle
(Erreichbarkeit der einzelnen PCs untereinander) mittels „ping“-command

3.2.2 Unterteilung in Subnetze

Im folgenden Screenshot ist unser Netzwerkplan dokumentiert, welcher als Grundlage für den Versuchsaufbau fungiert.

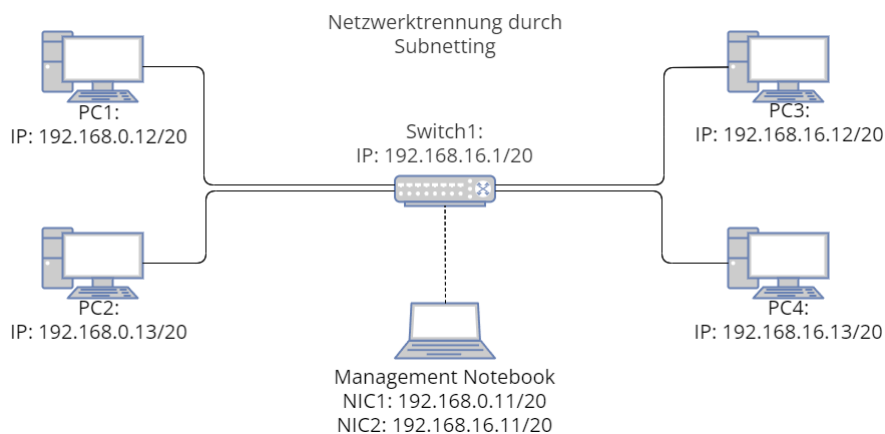


Abbildung 4: Netzwerkplan Subnetting

Die beiden folgenden Screenshots zeigen, dass im Netzwerk zwei PCs erreichbar sind. Im ersten Netzwerk (192.168.0.0) sind die Clients 1 und 2 mit den IP-Adressen 192.168.0.12 und 192.168.0.13 zu finden, während sich im zweiten Netzwerk (192.168.16.0) die Clients 3 und 4 mit den IP-Adressen 192.168.16.12 und 192.168.16.13 befinden. Der Switch(192.168.16.1) befindet sich im zweiten Netzwerk(192.168.16.0).

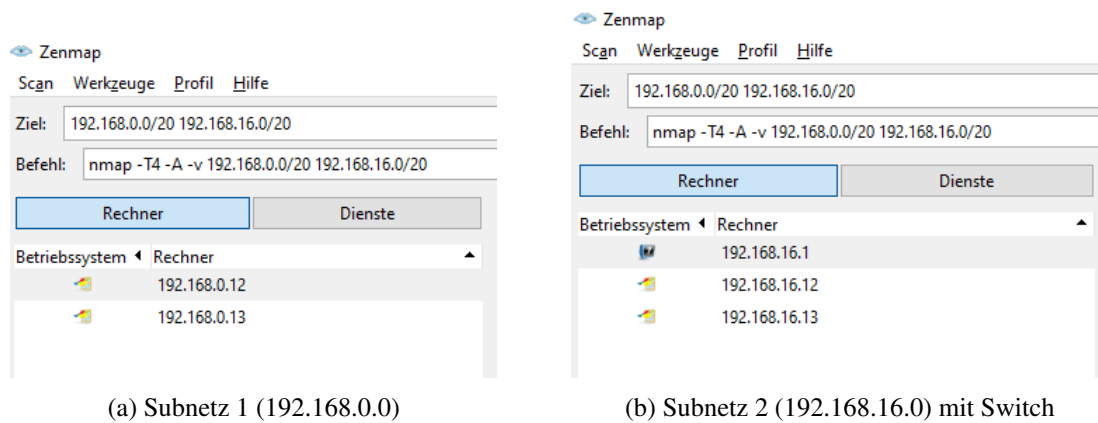


Abbildung 5: Zenmap-Scan Subnetze

Es ist ersichtlich, dass die Clients der beiden Netzwerke nicht miteinander kommunizieren können, wodurch eine abteilungsübergreifende Erreichbarkeit der PCs nicht mehr möglich ist. Dies ist auch in den beiden folgenden Screenshots deutlich erkennbar, in denen der Befehl „ipconfig“ und „ping“ in der Befehlszeile des jeweiligen Clients ausgeführt wurde.

```

Eingabeaufforderung
IPv4-Adresse (Auto. Konfiguration): 169.254.211.9
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway . . . . . :

C:\Users\schueler>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet:

    Verbindungsspezifisches DNS-Suffix: laba304.bsz-et.lan.dd-schulen.de
    Verbindungslokale IPv6-Adresse . . : fe80::9dd7:756e:2b86:d309%11
    IPv4-Adresse . . . . . : 192.168.0.12
    Subnetzmaske . . . . . : 255.255.240.0
    Standardgateway . . . . . :

C:\Users\schueler>ping 192.168.16.12

Ping wird ausgeführt für 192.168.16.12 mit 32 Bytes Daten:
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.

Ping-Statistik für 192.168.16.12:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
            (100% Verlust),

C:\Users\schueler>

```

(a) ping PC1 zu PC3

```

Eingabeaufforderung
Microsoft Windows [Version 10.0.19044.1469]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\schueler>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet:

    Verbindungsspezifisches DNS-Suffix: laba304.bsz-et.lan.dd-schulen.de
    Verbindungslokale IPv6-Adresse . . : fe80::b839:6caa:3c48:4bd6%12
    IPv4-Adresse . . . . . : 192.168.16.12
    Subnetzmaske . . . . . : 255.255.240.0
    Standardgateway . . . . . :

C:\Users\schueler>ping 192.168.0.12

Ping wird ausgeführt für 192.168.0.12 mit 32 Bytes Daten:
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.

Ping-Statistik für 192.168.0.12:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
            (100% Verlust),

C:\Users\schueler>

```

(b) ping PC3 zu PC1

Abbildung 6: Erreichbarkeit Netzwerke Subnetting

3.2.3 Trennung durch VLAN herstellen

Im folgenden Screenshot ist unser Netzwerkplan dokumentiert, welcher als Grundlage für den Versuchsaufbau der Netzwerktrennung durch VLANs fungiert.

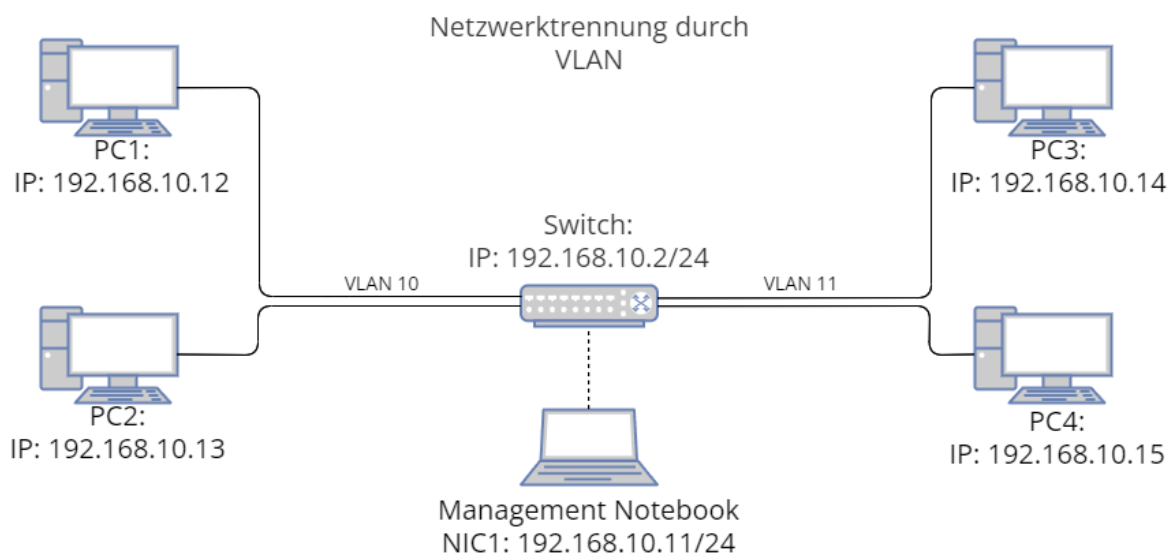
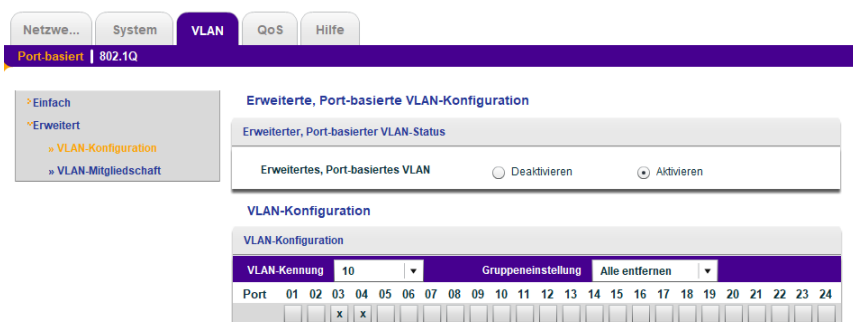
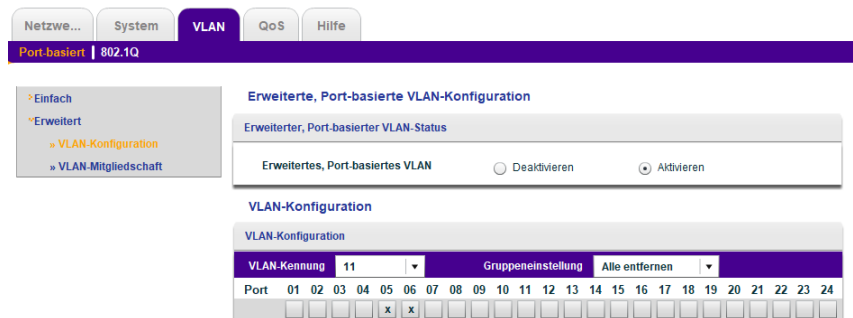


Abbildung 7: Netzwerkplan portbasiertes VLAN

Um die Trennung durch VLANs zu realisieren haben wir als erstes ein portbasiertes VLAN eingerichtet, welches wir in den weiteren Aufgaben auf PVID erweitert haben.



(a) VLAN10 Konfiguration



(b) VLAN11 Konfiguration

Abbildung 8: Konfiguration des portbasierten VLANs

Die Clients sind hierbei in zwei VLANs getrennt, 10 und 11. In den folgenden Screenshots sind Erreichbarkeiten der anderen Clients an dem jeweiligen Client dokumentiert.

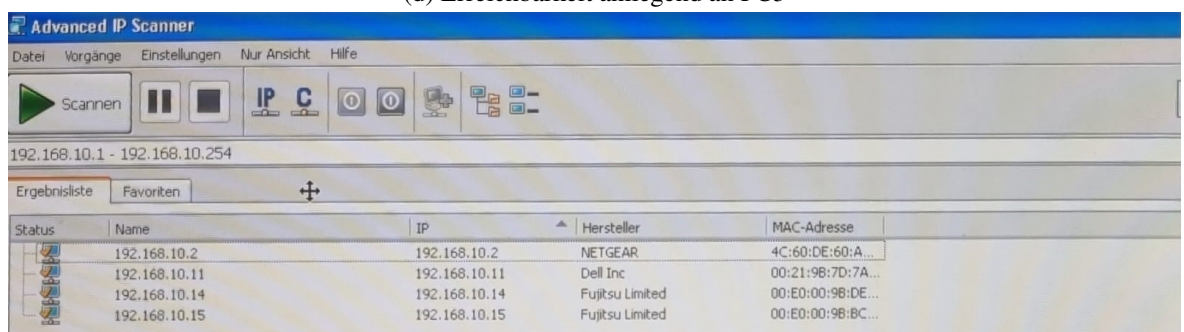
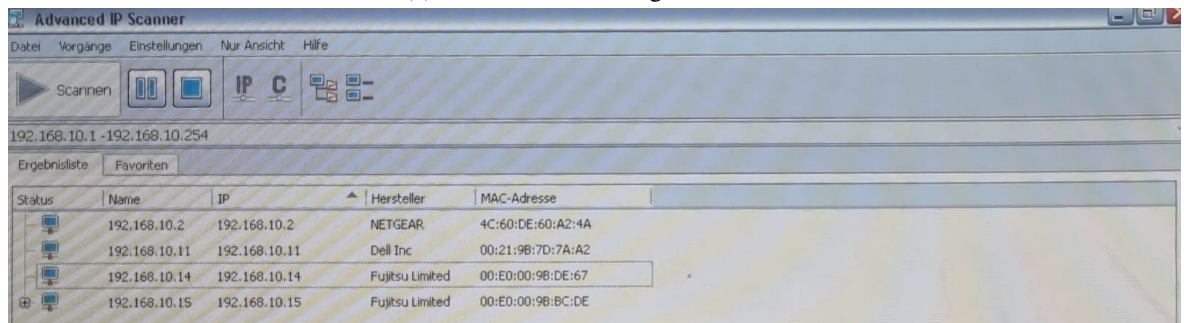
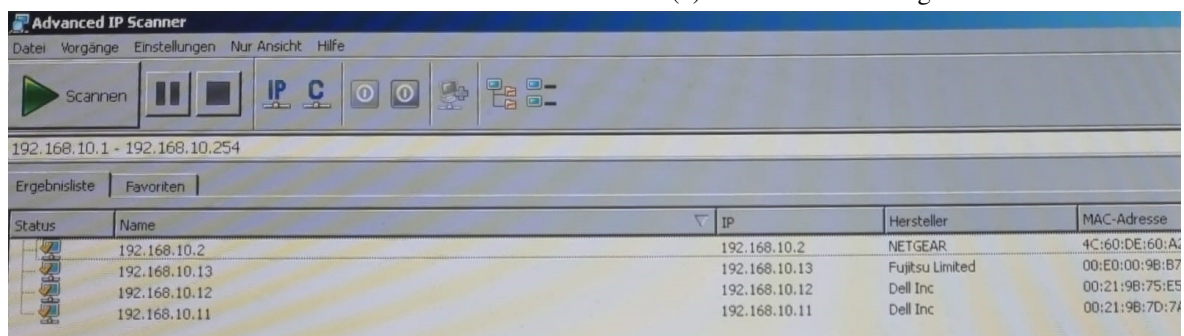
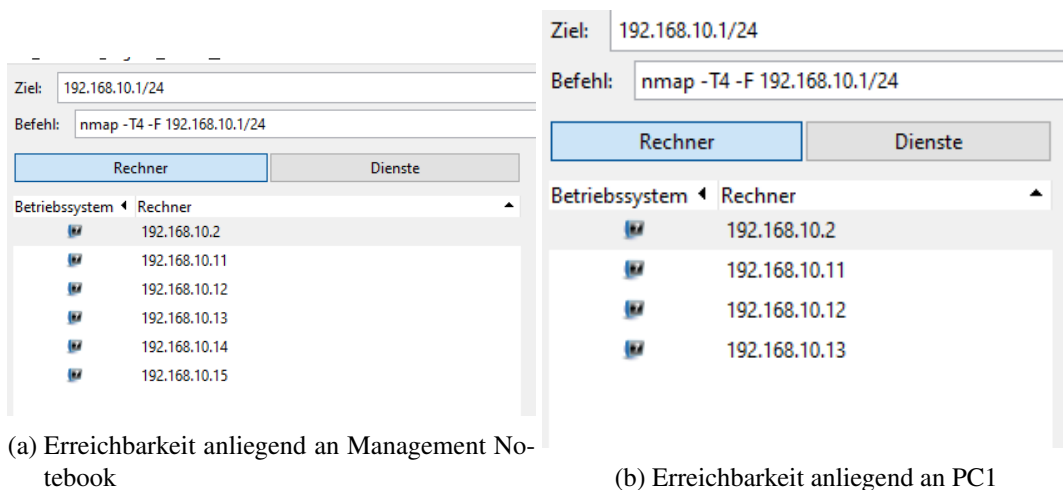


Abbildung 9: Erreichbarkeiten im portbasierten VLAN

Aus den oben aufgezeigten Screenshots lässt sich erkennen, dass ausschließlich die Clients der zugehörigen VLANs miteinander kommunizieren können.

3.2.4 VLAN übergreifenden Server integrieren

Um einen VLAN-übergreifenden Server zu integrieren, ist es erforderlich, ein zusätzliches VLAN einzubeziehen, das die Verbindung zwischen den VLANs herstellt, jedoch keine direkte Kommunikation ermöglicht. Im folgenden Netzwerkplan wird mithilfe des Management-Notebooks die Realisierung eines neuen VLANs 12 erreicht, wobei die Mitglieder von VLAN 10 und 11 ebenfalls Teil von VLAN 12 sind.

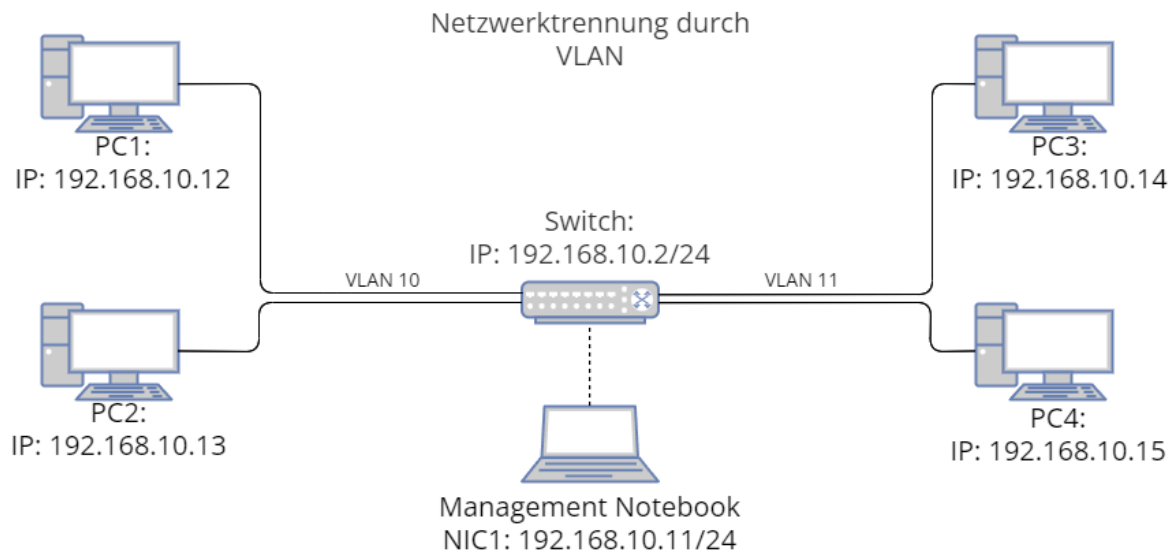
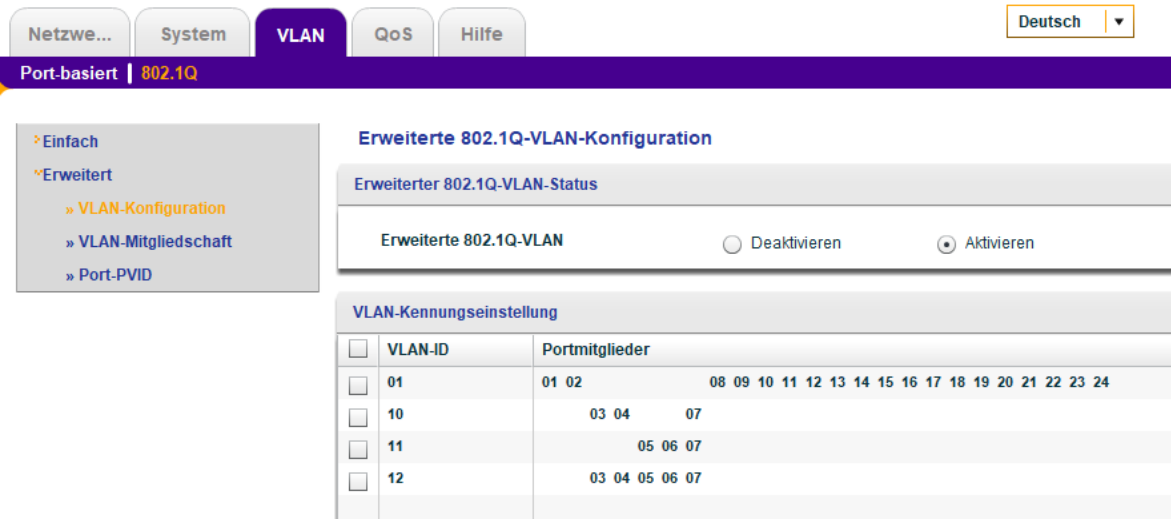


Abbildung 10: Netzwerkplan - Integration eines Servers

Der nächste Screenshot dokumentiert die Konfiguration des Switches zur Einrichtung des VLAN 12. Hierbei haben wir von portbasiertem VLAN auf die erweiterte 802.1Q-VLAN-Konfiguration umgestellt.

VLAN-ID	Portmitglieder
01	01 02 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
10	03 04 07
11	05 06 07
12	03 04 05 06 07

Abbildung 11: Switch Konfiguration - Integration eines Servers



(a) Übersicht der VLAN-Mitgliedschaften

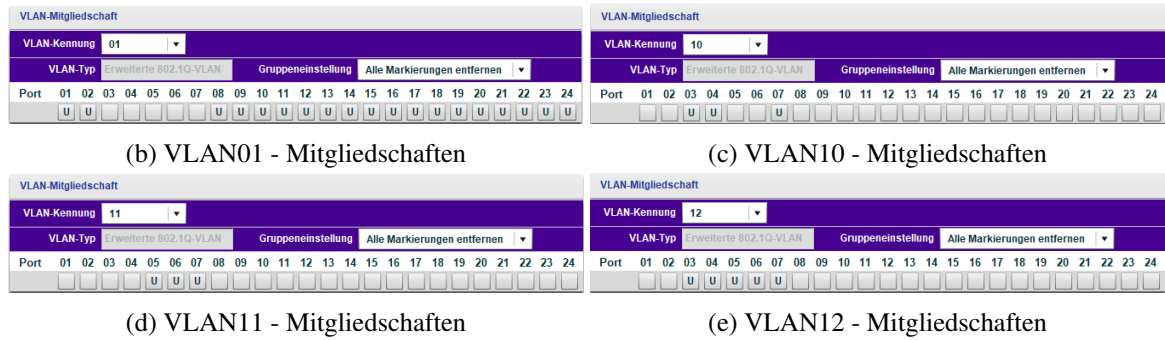


Abbildung 12: Switch Konfiguration - Integration eines Servers

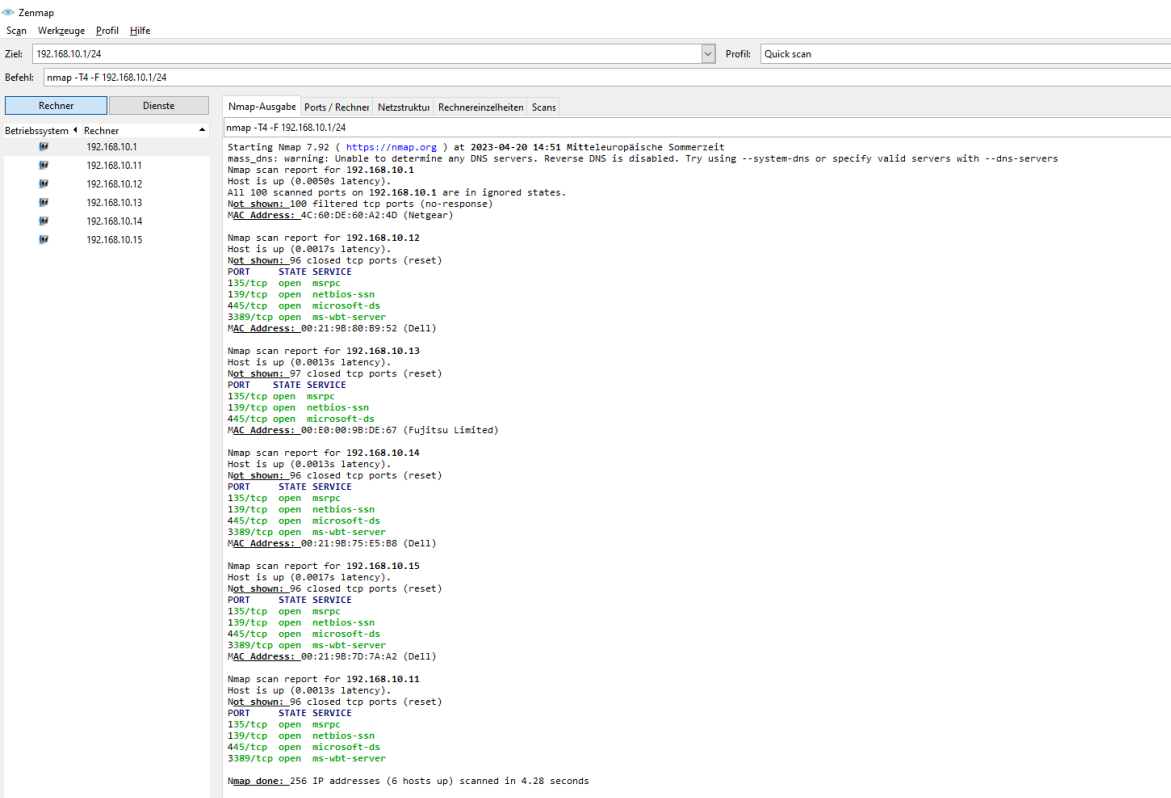


Abbildung 13: Zenmap-Scan Server - Integration eines Servers

3.2.5 Einrichtung Layer2-Switche

Um eine

4 Auswertung

4.1 Grundlagen Switchkonfiguration

4.2 Vergleich und Beurteilung

Literatur

- [1] Academic. *Vollduplex-Betrieb*. Februar 1987. URL: <https://de-academic.com/dic.nsf/dewiki/1473113>. abgerufen am 08.02.2023.
- [2] BS-IT BSZ ET DD. *VLAN*. 6.12.2008. URL: <http://docs.hp.com/en/5992-0538/ar01s01.html>. abgerufen am 08.02.2023.
- [3] CBIC. *Wozu dient die Auto-Negotiation in einem SFP-Transceiver?* November 11, 2019. URL: <https://www.gbic-shop.de/blog/de/96-transceiver/318-wozu-dient-die-auto-negotiation-in-einem-sfp-transceiver.html>. abgerufen am 02.02.2023.
- [4] Charlene. *Verbindung mehrerer Ethernet-Switches*. August 20, 2020. URL: <https://community.fs.com/de/blog/how-to-connect-multiple-ethernet-switches.html>. abgerufen am 02.02.2023.
- [5] Dipl.-Ing. (FH) Stefan Luber und Dipl.-Ing. (FH) Andreas Donner. *Was ist eine Trunk-Leitung?* 23.06.2020. URL: <https://www.ip-insider.de/was-ist-eine-trunk-leitung-a-941266/>. abgerufen am 08.02.2023.
- [6] Dipl.-Ing. (FH) Stefan Luber und Dipl.-Ing. (FH) Andreas Donner. *Was ist Link Aggregation (802.1AX; früher 802.3ad)?* 6.12.2019. URL: <https://www.ip-insider.de/was-ist-link-aggregation-8021ax-frueher-8023ad-a-886319/>. abgerufen am 08.02.2023.
- [7] Howard. *Switch Stacking: Grundlage, Konfiguration und FAQs*. April 01, 2022. URL: <https://community.fs.com/de/blog/switch-stacking-explained-basis-configuration-and-fa-qs.html>. abgerufen am 02.02.2023.
- [8] IT-Administrator. *Port Trunking*. n.A. URL: https://www.it-administrator.de/lexikon/port_trunking.html. abgerufen am 08.02.2023.
- [9] NetworkAcademy.io. *Verbindung mehrerer Ethernet-Switches*. 2021. URL: <https://community.fs.com/de/blog/how-to-connect-multiple-ethernet-switches.html>. abgerufen am 02.02.2023.
- [10] Telefonbau Schneider. *Begriffe aus der ITK-Technik kurz erklärt*. n.A. URL: <https://www.telefonbau-schneider.de/de/glossar/A/auto-uplink/?cHash=f74ae4c0659ddd0076bb73d1ab9b5d03>. abgerufen am 02.02.2023.
- [11] Wikipedia. *Atomic force microscopy*. [Online; accessed April 27, 2013]. 2013. URL: <https://test.de>.
- [12] Wikipedia. *MAC-Filter*. 23.09.2022. URL: <https://de.wikipedia.org/wiki/MAC-Filter>. abgerufen am 08.02.2023.

Glossar

Abbildungsverzeichnis

1	Verwenden von VLANs zum Erstellen unabhängiger Broadcast-Domänen über Swit- ches hinweg	4
2	NETGEAR-Switch Vorderansicht	9
3	NETGEAR-Switch Rückansicht	9
4	Netzwerkplan Subnetting	10
5	Zenmap-Scan Subnetze	11
6	Erreichbarkeit Netzwerke Subnetting	11
7	Netzwerkplan portbasiertes VLAN	12
8	Konfiguration des portbasierten VLANs	12
9	Erreichbarkeiten im portbasierten VLAN	13
10	Netzwerkplan - Integration eines Servers	14
11	Switch Konfiguration - Integration eines Servers	14
12	Switch Konfiguration - Integration eines Servers	15
13	Zenmap-Scan Server - Integration eines Servers	15

Abkürzungsverzeichnis

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Abschlussarbeit selbstständig und nur unter Verwendung der von mir angegebenen Quellen und Hilfsmittel verfasst zu haben. Sowohl inhaltlich als auch wörtlich entnommene Inhalte wurden als solche kenntlich gemacht. Die Arbeit hat in dieser oder vergleichbarer Form noch keinem anderem Prüfungsgremium vorgelegen.

Datum: _____ Unterschrift: _____

Datum: _____ Unterschrift: _____

Datum: _____ Unterschrift: _____