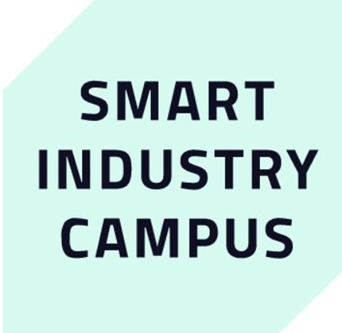
****



|  |  |  |
| --- | --- | --- |
| **Abschlussarbeit** |  |  |

**ARPAD MARIUS AZILAGYI**

**BÜRO NETZWERK + KOMPLEX**

# THEMA: BÜRO NETZWERK + KOMPLEX

Autor: MARIUS ARPAD SZILAGYI

Studiengang: IT-Fachkraft für Industrie 4.0

Seminargruppe:

Erstprüfer: Enrico Rühle

Zweitprüfer: Jens Riedel

Einreichung:17.08.2023

BIBLIOGRAFISCHE BESCHREIBUNG:

Name, Vorname: Szlagyi Marius Arpad

Thema der Graduierungsarbeit: Büro Netzwerk + Komplex

Jahr: 2023

Seitenzahlverzeichnisse:11

Seitenzahl des Inhalts:33

S.München, Smart Industry Campus.

**In diesem Projekt möchte ich Ihnen meine Arbeit und Erfahrungen zur Einrichtung und Konfiguration eines Bürokomplex-Netzwerks mit mehreren Etagen präsentieren.**

**Dieses Projekt umfasst verschiedene Elemente und Topologien, von der Einrichtung einer Stern-Topologie auf der ersten Etage bis hin zur Verwendung von VLANs auf der dritten Etage. Dabei wird besonderer Wert auf Sicherheit, Flexibilität und Skalierbarkeit gelegt.**

**Ich habe viel Zeit und Mühe investiert, um dieses Projekt so informativ und unterhaltsam wie möglich zu gestalten. Ich hoffe, dass es Ihnen gefallen wird und dass Sie genauso viel Freude haben werden wie ich bei der Erstellung.**

## REFERAT

KURZBESCHREIBUNG

In Projekt dreht sich alles um die Einrichtung und Konfiguration eines Bürokomplex-Netzwerks mit mehreren Etagen, das aus verschiedenen Elementen und Topologien besteht.

Die erste Etage wird mit einer Topologie eingerichtet, die einen PC, einen Laptop, einen Hub, einen Server und einen Sniffer beinhaltet. Alle Geräte sind über den Hub verbunden, was auf eine Stern-Topologie hindeutet. Die IP-Adressen werden festgelegt und ein Sniffer wird konfiguriert, um den Netzwerkverkehr zu überwachen. Es wird ein DHCP-Server implementiert, um IP-Adressen dynamisch zuzuweisen, und der Server wird als DNS-Server konfiguriert, um die Namensauflösung zu erleichtern. Weitere Server werden auf beiden Seiten des Routers hinzugefügt, um den Zugriff auf sie über ihre Namen zu ermöglichen.

Die zweite Etage verwendet eine 1-zu-1-Topologie für Punkt-zu-Punkt-Verbindungen. Die Router werden so konfiguriert, dass sie statische Routen verwenden und das Routing Information Protocol Version 2 (RIP v2) ermöglicht die Kommunikation zwischen den PCs und Laptops.

Auf der dritten Etage wird die Netzwerkstruktur weiter differenziert durch die Einrichtung von VLANs auf den Switches. Diese VLANs werden so konfiguriert, dass sie untereinander routen können und spezifische IP-Adressen sowie Subnetzmasken erhalten.

Die Computer auf dieser Etage sind so eingestellt, dass sie die VLAN-Schnittstelle ihres jeweiligen Netzwerks als Standardgateway verwenden.

Insgesamt handelt es sich um ein anspruchsvolles Projekt zur Vernetzung eines mehrstöckigen Bürokomplexes, bei dem verschiedene Netzwerktopologien und -technologien kombiniert werden. Dabei wird besonderer Wert auf Sicherheit, Flexibilität und Skalierbarkeit gelegt.

**Inhaltsverzeichnis**

[1 THEMA: BÜRO NETZWERK + KOMPLEX 2](#_Toc142902135)

[1.1 REFERAT 2](#_Toc142902136)

[2 Projekt Kurzbeschreibung 5](#_Toc142902137)

[3 Einführung 8](#_Toc142902138)

[3.1 Einleitung. 8](#_Toc142902139)

[3.2 Ziel und Zweck der Dokumentation. 8](#_Toc142902140)

[3.3 Überblick über das Netzwerkprojekt. 9](#_Toc142902141)

[4 Erste Etage: Netzwerktopologie und Konfiguration 9](#_Toc142902142)

[4.1 Erstellung der Topologie 9](#_Toc142902143)

[4.2 Konfiguration des Sniffers und des Servers 10](#_Toc142902144)

[4.2.1 Sniffer-Konfiguration 10](#_Toc142902145)

[4.2.2 Server-PT-Konfiguration. 10](#_Toc142902146)

[4.3 Einbau und Konfiguration des Routers, Switches und der drahtlosen Geräte 11](#_Toc142902147)

[4.3.1 Router-Konfiguration 11](#_Toc142902148)

[4.3.2 Switch-Konfiguration 11](#_Toc142902149)

[4.3.3 Einbindung und Konfiguration der drahtlosen Geräte 11](#_Toc142902150)

[5 Erste Etage: Netzwerktopologie und Konfiguration 12](#_Toc142902151)

[5.1 Erstellung der Topologie 12](#_Toc142902152)

[5.2 Konfiguration des Sniffers und des Servers 12](#_Toc142902153)

[5.2.1 Sniffer-Konfiguration 12](#_Toc142902154)

[5.2.2 Server-PT-Konfiguration 13](#_Toc142902155)

[5.3 Einbau und Konfiguration des Routers, Switches und der drahtlosen Geräte 13](#_Toc142902156)

[5.3.1 Router-Konfiguration 13](#_Toc142902157)

[5.3.2 Switch-Konfiguration 14](#_Toc142902158)

[5.3.3 Einbindung und Konfiguration der drahtlosen Geräte 14](#_Toc142902159)

[5.4 Implementierung und Konfiguration des DHCP-Servers 14](#_Toc142902160)

[5.4.1 Übersicht 14](#_Toc142902161)

[5.4.2 Einrichtung des DHCP-Servers 14](#_Toc142902162)

[5.4.3 DHCP-Bereichskonfiguration 15](#_Toc142902163)

[5.4.4 Verifikation der DHCP-Funktion 15](#_Toc142902164)

[5.4.5 Weitere Konfigurationen 15](#_Toc142902165)

[5.5 Netzwerkanalyse und Verwendung des Sniffers 15](#_Toc142902166)

[5.5.1 Einführung in den Sniffer 15](#_Toc142902167)

[5.5.2 Einrichtung des Sniffers 15](#_Toc142902168)

[5.5.3 Analyse des Netzwerkverkehrs 16](#_Toc142902169)

[5.5.4 Sicherheitsbedenken 16](#_Toc142902170)

[5.5.5 Fazit 16](#_Toc142902171)

[5.6 Router und drahtlose Konfiguration 16](#_Toc142902172)

[5.6.1 Einführung in Router und drahtlose Netzwerke 16](#_Toc142902173)

[5.6.2 Router-Konfiguration 16](#_Toc142902174)

[5.6.3 Drahtlose Konfiguration 16](#_Toc142902175)

[5.6.4 Vorteile der Dual IP-Konfiguration 17](#_Toc142902176)

[5.6.5 Fazit 17](#_Toc142902177)

[5.7 DHCP-Konfiguration und Bereichsanpassung 17](#_Toc142902178)

[5.7.1 Einführung in DHCP 17](#_Toc142902179)

[5.7.2 Ersteinrichtung des DHCP-Servers 17](#_Toc142902180)

[5.7.3 DHCP-Bereichsanpassung und Erweiterung 17](#_Toc142902181)

[5.7.4 Verifizierung der DHCP-Funktionalität 18](#_Toc142902182)

[5.7.5 Vorteile der DHCP-Nutzung 18](#_Toc142902183)

[5.7.6 Fazit 18](#_Toc142902184)

[5.8 Transformation des Servers in einen DNS-Server 18](#_Toc142902185)

[5.8.1 Einführung in DNS 18](#_Toc142902186)

[5.8.2 Implementierung des DNS-Servers 18](#_Toc142902187)

[5.8.3 Vorteile des DNS-Systems 18](#_Toc142902188)

[5.8.4 Verifizierung der DNS-Funktionalität 19](#_Toc142902189)

[5.8.5 Fazit 19](#_Toc142902190)

[5.9 Hinzufügung weiterer Server auf beiden Seiten des Routers 19](#_Toc142902191)

[5.9.1 Zielsetzung 19](#_Toc142902192)

[5.9.2 Implementierungsschritte 19](#_Toc142902193)

[5.9.3 Verifizierung der Serverfunktionalität 19](#_Toc142902194)

[5.9.4 Vorteile der erweiterten Serverarchitektur 19](#_Toc142902195)

[5.9.5 Fazit 20](#_Toc142902196)

[5.10 IP-Konfiguration und Netzwerktopologie der zweiten Etage 20](#_Toc142902197)

[5.10.1 IP-Konfiguration 20](#_Toc142902198)

[5.10.2 Netzwerktopologie und Konfiguration 20](#_Toc142902199)

[5.10.3 Fazit 20](#_Toc142902200)

[5.11 Netzwerktopologie und Konfiguration der dritten Etage 20](#_Toc142902201)

[5.11.1 VLAN-Konfiguration 20](#_Toc142902202)

[5.11.2 Inter-VLAN-Routing 21](#_Toc142902203)

[5.11.3 PC-Konfiguration 21](#_Toc142902204)

[5.11.4 Fazit 21](#_Toc142902205)

[6 Abbildungsverzeichnis 22](#_Toc142902206)

[7 Abkürzungsverzeichnis 31](#_Toc142902207)

[8 QUELLVERZEICHNISS 32](#_Toc142902208)

# Projekt Kurzbeschreibung

Technischer Bericht: Analyse der Netzwerktopologie

In diesem technischen Bericht wird die Netzwerktopologie eines dreistöckigen Aufbaus beschrieben. Das Netzwerk besteht aus verschiedenen miteinander verbundenen Geräten und Subnetzwerken, die die Kommunikation innerhalb der Organisation erleichtern. Die Topologie ist so konzipiert, dass sie einen effizienten Datenfluss und Konnektivität zwischen verschiedenen Etagen und Geräten ermöglicht. Netzwerkkomponenten

Die Netzwerktopologie ist in drei Stockwerke unterteilt: Ebene 1, Etage 2 und Etage 3. In diesem Bericht konzentrieren wir uns auf die Netzwerkkomponenten von Floor 1 und deren Konnektivität.

**Etage 1 Komponenten**

**Router RTR-1**: Der Router RTR-1 ist ein zentrales Netzwerkgerät, das als Gateway zwischen dem lokalen Netzwerk und externen Netzwerken dient. Er ist der Hauptein- und Ausstiegspunkt für den Datenverkehr. Der Router verfügt über zwei Ports: Fa0/1 und Fa1/0.

HUB-Switch Der HUB-Switch wird an Port Fa0/1 des RTR-1 angeschlossen. Dieser Schalter fungiert als zentraler Punkt für den Anschluss verschiedener Geräte innerhalb von Etage 1. Es ermöglicht Geräten, miteinander zu kommunizieren, indem Datenrahmen zwischen ihnen weitergeleitet werden.

**Geräte, die mit dem HUB-Switch verbunden sind:**

PC: PCs sind mit dem HUB-Switch verbunden. Diese Geräte sind Teil des lokalen Netzwerks und können mit anderen Geräten innerhalb desselben Subnetzes kommunizieren.

**Sniffer:** Ein Netzwerk-Sniffer-Tool ist mit dem HUB-Switch verbunden. Es wird zur Überwachung und Analyse des Netzwerkverkehrs zur Fehlerbehebung und zu Sicherheitszwecken verwendet.

**WEB-Server:** Ein Webserver ist mit dem HUB-Switch verbunden. Es hostet Webanwendungen oder Websites und reagiert auf Kundenanfragen.

**DHCP-Server: (fungiert auch als DNS):** Der DHCP-Server ist für die dynamische Zuweisung von IP-Adressen zu Geräten im Netzwerk verantwortlich. Es dient auch als DNS-Server und löst Domainnamen in IP-Adressen auf.

Ein DHCP-Server ist eine Software, die es ermöglicht, Clients automatisch in ein Netzwerk einzubinden. Die Abkürzung DHCP steht für **Dynamic Host Configuration Protocol**. Es ist ein Kommunikationsprotokoll für Computernetzwerke, das 1997 im RFC 2131 definiert wurde. Nach dem Client-Server-Prinzip sorgt es dafür, dass verbindungssuchende Geräte automatisch eine wiederverwendbare Netzwerkadresse und alle weiteren relevanten Parameter beziehen2.

DHCP wurde als Lösung für größere Netzwerke und tragbare Computer entwickelt und ergänzt das Bootstrap Protocol (BOOTP) unter anderem durch die Fähigkeit der automatischen Zuweisung von wiederverwendbaren Netzwerkadressen sowie durch zusätzliche Konfigurationsmöglichkeiten. Die Internet Assigned Numbers Authority (IANA) hat DHCP zu diesem Zweck die UDP-Ports 67 und 68 zugewiesen2.

Die Adresszuordnung mit DHCP funktioniert nach dem Client-Server-Prinzip: Die verbindungssuchenden Geräte fordern die IP-Adresskonfiguration von einem DHCP-Server an, der seinerseits auf eine Datenbank zurückgreift, in der die einzustellenden Netzwerkparameter vorgegeben sind2. Unter anderem kann dieser Server dem Client mithilfe seiner Datenbankinformationen folgende Einstellungen zuweisen: eindeutige IP-Adresse, Subnetzmaske, Standard-Gateway, DNS-Server und Proxy-Konfiguration via WPAD (Web Proxy Auto-Discovery Protocol

**Subnetze und IP-Adressen:**

Netzwerk 192.168.1.1/24:

Dieses Netzwerk wird für Geräte verwendet, die mit dem HUB-Switch verbunden sind. Es verfügt über eine Subnetzmaske von 255.255.255.0, sodass bis zu 254 Geräte angeschlossen werden können. Geräte innerhalb dieses Netzwerks können direkt miteinander kommunizieren.

Die IP-Adresse 192.168.1.1/24 ist eine IP-Adresse im CIDR-Format (Classless Inter-Domain Routing). Die Zahl nach dem Schrägstrich gibt die Anzahl der Bits an, die für die Netzwerkadresse verwendet werden. In diesem Fall bedeutet dies, dass die ersten 24 Bits für die Netzwerkadresse verwendet werden und die restlichen 8 Bits für die Hostadresse. Dies entspricht einer Subnetzmaske von 255.255.255.01.

Die IP-Adresse 192.168.1.1/24 gibt an, dass das Netzwerk die IP-Adressen von 192.168.1.0 bis 192.168.1.255 umfasst. Die erste Adresse (192.168.1.0) wird normalerweise als Netzwerkadresse verwendet und die letzte Adresse (192.168.1.255) als Broadcast-Adresse, sodass die tatsächlich nutzbaren Adressen für Hosts im Bereich von 192.168.1.1 bis 192.168.1.254 liegen.

**Switch2:**

Switch2 ist mit Port Fa1/0 von RTR-1 verbunden. Es bietet Konnektivität für Geräte, die sich auf Ebene 1 befinden, und dient als Erweiterung des Netzwerks.

2.1.6 An Switch2 angeschlossene Geräte PC5:

Ähnlich wie andere PCs ist PC5 ein Gerät für allgemeine Computer.

WEB-Server: Eine weitere Instanz eines Webservers ist mit Switch2 verbunden und bietet Redundanz oder Lastenausgleich für Webdienste.

**DHCP-Server (fungiert auch als DNS):** Ähnlich wie der DHCP-Server auf dem HUB-Switch weist dieser Server dynamisch IP-Adressen zu und führt die DNS-Auflösung für Geräte durch, die mit Switch2 verbunden sind.

**DNS-Server:**

Ein DNS-Server ist ein Server, der das **Domain Name System (DNS)** implementiert. DNS ist ein hierarchisch unterteiltes Bezeichnungssystem in einem meist IP-basierten Netz zur Beantwortung von Anfragen zu Domain-Namen (Namensauflösung). Es funktioniert ähnlich wie eine Telefonauskunft.

Computer und andere Netzwerkgeräte im Internet verwenden eine IP-Adresse. Möchten Sie nun eine Website im Internet aufrufen, wird die IP-Adresse abgefragt. Der Prozess gleicht in etwa dem Wählen einer Telefonnummer, um eine Verbindung mit einer Person herzustellen, die Sie erreichen möchten2. Mithilfe von DNS müssen Sie sich nicht jede numerische Kombination von IP-Adressen merken. Stattdessen stellen Sie einfach eine Verbindung mit dem DNS-Server her, der eine riesige Datenbank verwaltet und die Websitenamen auf IP-Adressen abbildet. Das DNS funktioniert also ähnlich einem Telefonbuch.

„Es gibt übrigens nicht nur den einen DNS-Server. Weltweit gibt es insgesamt dreizehn Root-Server. Es kann also vorkommen, dass ein DNS-Server der angefragten URL keine IP-Adresse zuordnen kann. Dann wird die Anfrage ganz einfach an den nächsten Server weitergegeben. Kann keiner der Server die Eingabe beantworten, erhalten Sie im Browser eine Fehlermeldung. Im Regelfall liegt das Problem dann an der eingegebenen Adresse. Vielleicht ist ein Tippfehler oder Zahlendreher schuld“.

**Access Point:** Der Access Point ermöglicht die drahtlose Konnektivität für Geräte wie Laptops und Smartphones.

Drucker1: An Switch2 ist ein Netzwerkdrucker angeschlossen, der das Drucken von verschiedenen Geräten aus ermöglicht. PC6: Ein zusätzlicher PC, der mit Switch2 verbunden ist.

**Subnetze und IP-Adressen:**

Netzwerk 172.10.1.0/24: Geräte, die mit Switch2 verbunden sind, sind Teil dieses Netzwerks. Es verwendet auch eine Subnetzmaske von 255.255.255.0 und bietet Platz für bis zu 254 Geräte.

In Fortsetzung des vorherigen Abschnitts konzentriert sich dieser technische Bericht auf Ebene 2 der Netzwerktopologie. Etage 2 besteht aus vier Routern (RTR-2, RTR-3, RTR-4 und RTR-5) und ihren jeweiligen Verbindungen. Das Ziel dieses Berichts ist es, die Konnektivität und die Kommunikationswege zu analysieren, die auf dieser Etage eingerichtet wurden.

**Netzwerkkomponenten auf Ebene 2:**

In Etage 2 befinden sich vier Router mit jeweils spezifischen Verbindungen, die den Datenfluss über das Netzwerk erleichtern. Nachfolgend finden Sie eine Übersicht über die Router und ihre Verbindungen:

**Router RTR-2**:

RTR-2 spielt eine Schlüsselrolle bei der Verbindung von Floor 1 mit den Geräten und Routern auf Etage 2

Port. Fa0/0 (192.168.4.0/24): Dieser Port verbindet RTR-2 mit RTR-1 auf Ebene 1 über das Netzwerk 192.168.4.0/24. Es stellt eine Verbindung zwischen den beiden Etagen her und ermöglicht die Kommunikation zwischen ihnen.

Port Fa0/1 (192.168.5.0/24): Dieser Port verbindet RTR-2 mit RTR-3 auf Ebene 1 über das Netzwerk 192.168.5.0/24. Ähnlich wie bei der vorherigen Verbindung erleichtert diese Verbindung den Datenaustausch zwischen den beiden Routern.

**Router RTR-3:**

RTR-3 dient als zentraler Router auf Ebene 2 und verbindet sich mit anderen Routern und Geräten.

Port Fa1/0 (172.16.2.0/24): Dieser Port verbindet RTR-3 mit RTR-4 über das Netzwerk 172.16.2.0/24. Diese Verbindung stellt einen Kommunikationspfad zwischen den beiden Routern her, über den sie Daten austauschen können.

Port Fa0/1 (192.168.2.0/24): Dieser Port verbindet RTR-3 mit RTR-5 über das Netzwerk 192.168.2.0/24. Ähnlich wie bei der vorherigen Verbindung ermöglicht diese Verbindung die Datenübertragung zwischen den Routern.

Port Fa0/0 (192.168.3.0/24): Dieser Port verbindet RTR-3 mit Switch4 auf Ebene 2 über das Netzwerk 192.168.3.0/24. Es stellt die Konnektivität zwischen dem Router und den lokalen Netzwerkgeräten her, die mit Switch4 verbunden sind.

**Router RTR-4:**

RTR-4 ist mit RTR-3 auf Ebene 2 verbunden.

Port Fa1/0 (172.16.2.0/24): Dieser Port verbindet RTR-4 mit RTR-3 über das Netzwerk 172.16.2.0/24. Die Verbindung ermöglicht den Datenaustausch zwischen den beiden Routern.

**Router RTR-5:**

RTR-5 ist auch mit RTR-3 auf Ebene 2 verbunden.

Port Fa0/1 (192.168.2.0/24): Dieser Port verbindet RTR-5 mit RTR-3 über das Netzwerk 192.168.2.0/24. Die Verbindung erleichtert die Kommunikation zwischen den Routern.

**Netzwerkkomponenten auf Ebene 3:**

Etage 3 ist mit einer Kombination aus Switches und Geräten ausgestattet, die jeweils zur Funktionalität des Netzwerks beitragen. Nachfolgend finden Sie eine Aufschlüsselung der wichtigsten Komponenten auf Ebene 3:

**Multilayer-Switch 3650:**

Der Multilayer Switch 3650 dient als zentrales Netzwerkgerät, das sowohl Layer-2- als auch Layer-3-Funktionen verarbeiten kann.

Switch 6 (VLAN 2, Subnetz: 192.168.20.0/24)

Switch 6 ist mit VLAN 2 konfiguriert und dem Subnetz 192.168.20.0/24 zugeordnet.

**VLAN:** VLANs werden verwendet, um das Netzwerk in logische Gruppen zu segmentieren. In diesem Fall trennt VLAN 2 bestimmte Geräte oder Gerätegruppen vom Rest des Netzwerks.

Subnetz: Das Subnetz 192.168.20.0/24 stellt IP-Adressen für Geräte innerhalb von VLAN 2 bereit. Dieses Subnetz kann bis zu 254 Geräte aufnehmen.

**Switch 8:** (VLAN 30, Subnetz: 192.168.30.0/24)

Switch 8 ist VLAN 30 zugeordnet und verwendet das Subnetz 192.168.30.0/24. Dieser Switch verbindet einen Access Point, einen Drucker und zwei PCs.

**Access Point:** Der Access Point ermöglicht die drahtlose Verbindung von Geräten auf Ebene 3.

**Drucker:** Ein Netzwerkdrucker ist mit Switch 8 verbunden, sodass Geräte Druckaufträge an ihn senden können.

**PCs:** Zwei PCs sind mit Switch 8 verbunden und bieten allgemeine Rechenfunktionen.

**VLAN-Konfiguration:**

VLANs spielen eine entscheidende Rolle bei der Segmentierung des Netzwerks, der Isolierung des Datenverkehrs und der Optimierung des Netzwerkmanagements. In dieser Konfiguration werden VLAN 2 und VLAN 30 verwendet, um Geräte mit ähnlichen Anforderungen zu gruppieren und so einen effizienten Datenfluss und Sicherheit zu gewährleisten.

**Konfiguration des Subnetzes:**

Subnetze werden verwendet, um den IP-Adressraum in überschaubare Segmente zu unterteilen. Die Subnetzkonfiguration auf Ebene 3 stellt sicher, dass Geräte innerhalb desselben VLANs Teil desselben IP-Adressbereichs sind. Hier ist eine kombinierte Tabelle, die das IP-Adressierungsschema für jede Etage und jedes VLAN darstellt, einschließlich der ersten IP-Adresse als Standard-Gateway:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Etage / VLAN** | **Subnet** | **IP Range** | **Subnet Mask** | **Default Gateway** |
| Etage 1 | 192.168.1.0/24 | 192.168.1.1-254 | 255.255.255.0 | 192.168.1.1 |
|  | 172.16.1.0/24 | 172.16.1.1-254 | 255.255.255.0 | 172.16.1.1 |
| Etage 2 | 172.16.2.0/24 | 172.16.2.1-254 | 255.255.255.0 | 172.16.2.1 |
|  | 192.168.3.0/24 | 192.168.3.1-254 | 255.255.255.0 | 192.168.3.1 |
|  | 192.168.2.0/24 | 192.168.2.1-254 | 255.255.255.0 | 192.168.2.1 |
|  | 192.168.7.0/24 | 192.168.7.1-254 | 255.255.255.0 | 192.168.7.1 |
|  | 192.168.6.0/24 | 192.168.6.1-254 | 255.255.255.0 | 192.168.6.1 |
|  | 192.168.5.0/24 | 192.168.5.1-254 | 255.255.255.0 | 192.168.5.1 |
| Etage 3 VLAN 2 | 192.168.20.0/24 | 192.168.20.1-254 | 255.255.255.0 | 192.168.20.1 |
| Etage 3 VLAN 3 | 192.168.30.0/24 | 192.168.30.1-254 | 255.255.255.0 | 192.168.30.1 |

**7. Fazit:**

Die Netzwerktopologie auf Ebene 1 ist so konzipiert, dass sie die Konnektivität und den Datenaustausch zwischen verschiedenen Geräten unterstützt. Das Vorhandensein von Routern, Switches, Servern und Clients sorgt für eine effiziente Kommunikation innerhalb des lokalen Netzwerks. Die Verwendung verschiedener Subnetze ermöglicht eine effektive Verwaltung von IP-Adressen und die Segmentierung des Netzwerkverkehrs. Diese Netzwerktopologie bildet die Grundlage für eine funktionierende und vernetzte IT-Infrastruktur im 1. Stock. Etage 2 der Netzwerktopologie besteht aus einer komplexen Anordnung von Routern und Verbindungen, die eine effiziente Datenübertragung und Kommunikation zwischen Geräten ermöglichen. Die miteinander verbundenen Router (RTR-2, RTR-3, RTR-4 und RTR-5) bilden Wege, die Etage 2 mit Etage 1 verbinden und den Datenaustausch innerhalb des lokalen Netzwerks erleichtern. Diese Verbindungen sind ein wichtiger Bestandteil der gesamten Netzwerkinfrastruktur und tragen zum reibungslosen Funktionieren der Kommunikationssysteme des Unternehmens bei.

Die Netzwerktopologie von Etage3 demonstriert die Verwendung von VLANs und Subnetzen zur Organisation von Geräten und zur effektiven Verwaltung des Netzwerkverkehrs.

Der Multilayer Switch 3650 dient als zentraler Hub für Konnektivität- und Routing-Funktionen, während Switch 6 und Switch 8 spezifische Konnektivität für Geräte innerhalb der VLANs 2 bzw. 30 bieten. Diese Konfiguration sorgt für einen reibungslosen Datenfluss innerhalb der 3. Etage und trägt zu einer gut strukturierten und effizienten Netzwerkumgebung bei.

# Einführung

## Einleitung.

Die fortschreitende Digitalisierung und die wachsenden Anforderungen an IT-Netzwerke erfordern eine klare Planung und Dokumentation von Netzwerktopologien und Konfigurationsprozessen. In einer Welt, in der Daten den Kern vieler Geschäftsabläufe bilden, hat die Sicherheit und Effizienz von Netzwerkinfrastrukturen oberste Priorität.

## Ziel und Zweck der Dokumentation.

Das Hauptziel dieser Dokumentation ist es, eine klare und detaillierte Beschreibung der Implementierung und Konfiguration eines mehrstöckigen Bürokomplex-Netzwerks bereitzustellen. Sie dient als Referenzhandbuch für Netzwerkadministratoren, Techniker und alle Beteiligten, die an der Wartung, Überwachung oder Erweiterung des Netzwerks beteiligt sind. Durch diese Dokumentation soll sichergestellt werden, dass alle Konfigurationen transparent, nachvollziehbar und für zukünftige Anpassungen oder Fehlerbehebungen leicht verständlich sind.

Es kann auch als Benchmark für zukünftige Netzwerkprojekte oder für die Überprüfung und Optimierung der aktuellen Infrastruktur verwendet werden.

## Überblick über das Netzwerkprojekt.

-Das Netzwerkprojekt im Büro-Komplex erstreckt sich über drei Etagen, wobei jede Etage spezifische Anforderungen und Konfigurationen aufweist. Die erste Etage konzentriert sich auf die grundlegende Netzwerktopologie, einschließlich der Einrichtung von PCs, Laptops, einem Hub, einem Server und spezifischen Netzwerkdiensten wie DHCP und DNS. Es wird auch ein Sniffer implementiert, um den Datenverkehr zu überwachen und wertvolle Einblicke in das Netzwerkverhalten zu gewinnen.

-Die zweite Etage fokussiert auf erweiterte Netzwerkrouting-Techniken, darunter statisches Routing und die Implementierung des Routing Information Protocol (RIP) v2. Es wird auch eine spezielle Topologie eingeführt, die in "Abbildung 1" detailliert dargestellt ist.

-Die dritte und letzte Etage widmet sich der Implementierung und Konfiguration von Virtual Lokal Area Networks (VLANs). Diese Etage beinhaltet die Segmentierung des Netzwerkverkehrs, um Effizienz und Sicherheit zu gewährleisten. Es werden Techniken wie Inter-VLAN-Routing und spezifische VLAN-Schnittstellenkonfigurationen verwendet.

Insgesamt bildet dieses Netzwerkprojekt eine umfassende, mehrschichtige Architektur, die sowohl grundlegende als auch fortgeschrittene Netzwerktechniken integriert, um einen reibungslosen, effizienten und sicheren Datenverkehr im gesamten Büro-Komplex zu gewährleisten.

# Erste Etage: Netzwerktopologie und Konfiguration

## Erstellung der Topologie

-Die Erstellung der Topologie für die erste Etage bildet die Grundlage des gesamten Netzwerkprojekts. Es ist unerlässlich, eine solide Basis zu schaffen, auf der weitere Netzwerkkomponenten und -dienste implementiert werden können. Hier sind die Schritte und Entscheidungen, die bei der Erstellung dieser Topologie berücksichtigt wurden:

**PC und Laptop:** Zwei primäre Endbenutzergeräte wurden in die Topologie eingefügt. Diese Geräte sind typisch für Bürokomplexe, wo Mitarbeiter auf zentralisierte Dienste und Ressourcen zugreifen müssen. Die Auswahl von sowohl festen PCs als auch mobilen Laptops ermöglicht eine flexible Arbeitsumgebung.

**Hub-PT:** Ein Hub ist ein grundlegendes Netzwerkgerät, das Datenpakete zwischen Netzwerkgeräten überträgt. In dieser Topologie dient der Hub als zentrale Verbindungseinheit, die den Datenverkehr von und zu allen Geräten im Netzwerk weiterleitet. Es ist wichtig zu beachten, dass ein Hub alle Daten an alle angeschlossenen Geräte sendet, was potenziell zu Netzwerkstaus führen kann. Trotzdem wurde er hier aufgrund seiner Einfachheit und Unkompliziertheit gewählt.

**Server-PT:** Ein zentraler Server wurde hinzugefügt, um Netzwerkdienste wie Datei- und Druckerfreigabe, DNS und DHCP bereitzustellen. Seine primäre Aufgabe ist es, zentrale Dienste für alle Endbenutzergeräte bereitzustellen. Eine feste IP-Adresse (192.168.1.2/24) wurde ihm zugewiesen, um eine konsistente Kommunikation und Erreichbarkeit zu gewährleisten.

**Sniffer:** Dieses Werkzeug wurde in die Topologie integriert, um den Netzwerkverkehr zu überwachen und zu analysieren. Ein Sniffer ermöglicht es Netzwerkadministratoren, den Datenverkehr in Echtzeit zu überwachen, potenzielle Probleme zu identifizieren und Einblicke in die Netzwerkleistung zu erhalten.

-Die Gesamtkonfiguration dieser Geräte auf der ersten Etage ermöglicht eine einfache, aber effiziente Kommunikationsstruktur. Es wurde darauf geachtet, dass die Grundbedürfnisse eines Büronetzwerks abgedeckt sind, während gleichzeitig Raum für Erweiterungen und Modifikationen in den folgenden Etagen des Projekts bleibt.

## Konfiguration des Sniffers und des Servers

### Sniffer-Konfiguration

-Ein Sniffer, auch bekannt als Netzwerkanalysator oder Packet Capture Tool, ermöglicht es, den Netzwerkverkehr in Echtzeit zu überwachen und Datenpakete, die durch das Netzwerk fließen, zu inspizieren. Dies ist besonders nützlich, um Netzwerkleistung, Sicherheitsbedrohungen und allgemeines Netzwerkverhalten zu überwachen.

*Schritte zur Konfiguration des Sniffers:*

**1.Standortwahl:** Der Sniffer wurde so positioniert, dass er alle Datenpakete, die durch den Hub fließen, abfangen kann, um einen vollständigen Überblick über den Netzwerkverkehr zu erhalten.

**2.Interface-Auswahl:** Das richtige Interface des Sniffers wurde ausgewählt, um den Datenverkehr auf dem gesamten Netzwerk zu überwachen.

**3.Filtereinstellungen** (optional): Je nach Bedarf können spezifische Filter angewendet werden, um nur bestimmte Typen von Datenpaketen anzuzeigen. Dies kann nützlich sein, um spezifische Netzwerkaktivitäten oder -probleme zu isolieren.

### Server-PT-Konfiguration.

Der Server in unserer Topologie erfüllt eine zentrale Rolle und bietet verschiedene Dienste für das gesamte Netzwerk.

*Schritte zur Konfiguration des Server-PT:*

**1.Feste IP-Adresse zuweisen:**

- Gemäß den Projektanforderungen wurde dem Server die IP-Adresse 192.168.1.2 mit einer Subnetzmaske von /24 zugewiesen. Dies stellt sicher, dass der Server konsequent erreichbar ist und als stabile Ressource im Netzwerk dient.

**2. DHCP-Konfiguration:**

- Aktivierung den DHCP-Dienst auf dem Server.

- Definieren Sie den IP-Adressbereich, den der DHCP-Server den Endgeräten zuweisen kann. In diesem Fall startet der Bereich bei 192.168.1.3 (da 192.168.1.1 und 192.168.1.2 bereits zugewiesen sind) und könnte bis 192.168.1.254 gehen, je nach Anzahl der Geräte im Netzwerk.

- Lease-Zeit und andere DHCP-Einstellungen können je nach den spezifischen Anforderungen des Netzwerks angepasst werden.

**3. Überprüfung der DHCP-Funktionalität:** Nach der Konfiguration des DHCP-Servers wurde überprüft, ob das PC und das Laptop automatische IP-Adressen vom DHCP-Server erhalten haben. Dies stellt sicher, dass der DHCP-Server ordnungsgemäß funktioniert und die Endgeräte korrekt konfiguriert sind.

Der Server und der Sniffer sind jetzt einsatzbereit und bieten sowohl Netzwerkdienste als auch Überwachungsfunktionen für die erste Etage des Bürokomplexes.

## Einbau und Konfiguration des Routers, Switches und der drahtlosen Geräte

### Router-Konfiguration

-Die Integration eines Routers in die Topologie ermöglicht eine Segmentierung des Netzwerks und bietet die Möglichkeit zur Kommunikation zwischen diesen Segmenten. Er spielt eine entscheidende Rolle in unserer Netzwerktopologie, insbesondere bei der Verbindung zu anderen Etagen oder Segmenten.

*Schritte zur Konfiguration des Routers:*

**1.IP-Adressierung:** Gemäß den Projektanforderungen wurde die erste IP-Adresse des Routers auf 192.168.1.1/24 und die zweite IP-Adresse auf 172.16.1.1/24 festgelegt. Dies stellt sicher, dass der Router sowohl im 192.168.1.0/24-Netzwerksegment als auch im 172.16.1.0/24-Segment ordnungsgemäß kommunizieren kann.

**2. Routing:** Standard-Routing-Einträge wurden hinzugefügt, um die Kommunikation zwischen den verschiedenen Subnetzen zu ermöglichen.

### Switch-Konfiguration

-Ein Switch wurde eingefügt, um eine effizientere Netzwerkkommunikation im Vergleich zu einem Hub zu ermöglichen. Im Gegensatz zu einem Hub sendet ein Switch Datenpakete nur an das spezifische Zielgerät, was den Netzwerkverkehr reduziert und die Leistung verbessert.

*Grundlegende Schritte zur Konfiguration des Switches:*

**1.Port-Konfiguration:** Die Ports des Switches wurden entsprechend den angeschlossenen Geräten konfiguriert. Dies kann VLAN-Zuweisungen, Port-Geschwindigkeiten und andere spezifische Einstellungen umfassen.

### Einbindung und Konfiguration der drahtlosen Geräte

-Drahtlose Kommunikation ist in modernen Büroumgebungen unerlässlich und bietet Flexibilität und Mobilität für die Benutzer.

*Schritte zur Einbindung drahtloser Geräte:*

**1.Access Point (AP) hinzufügen:** Ein Access Point wurde in die Topologie integriert, um drahtlose Geräte wie Laptops und mobile Geräte mit dem Netzwerk zu verbinden.

**2.Drahtlose Endgeräte:** Ein PC und ein Drucker wurden drahtlos über den Access Point hinzugefügt. Dies ermöglicht diesen Geräten, ohne physische Verkabelung mit dem Netzwerk zu kommunizieren.

**3.Access Point-Konfiguration:**

-Hier können wir Sicherheitsprotokolle wie WPA2 wurden aktiviert, um die drahtlose Kommunikation zu sichern.

- Es kann auch ein SSID (Service Set Identifier) festlegen, um das drahtlose Netzwerk zu identifizieren.

-Die drahtlosen Kanaleinstellungen wurden so konfiguriert, dass sie minimale Interferenzen mit anderen drahtlosen Netzwerken oder Geräten aufweisen.

Mit der Integration und Konfiguration dieser Netzwerkelemente auf der ersten Etage wird eine robuste und flexible Netzwerktopologie geschaffen, die den Anforderungen eines modernen Bürokomplexes gerecht wird.

# Erste Etage: Netzwerktopologie und Konfiguration

## Erstellung der Topologie

-Die Erstellung der Topologie für die erste Etage bildet die Grundlage des gesamten Netzwerkprojekts. Es ist unerlässlich, eine solide Basis zu schaffen, auf der weitere Netzwerkkomponenten und -dienste implementiert werden können. Hier sind die Schritte und Entscheidungen, die bei der Erstellung dieser Topologie berücksichtigt wurden:

**PC und Laptop:** Zwei primäre Endbenutzergeräte wurden in die Topologie eingefügt. Diese Geräte sind typisch für Bürokomplexe, wo Mitarbeiter auf zentralisierte Dienste und Ressourcen zugreifen müssen. Die Auswahl von sowohl festen PCs als auch mobilen Laptops ermöglicht eine flexible Arbeitsumgebung.

**Hub-PT:** Ein Hub ist ein grundlegendes Netzwerkgerät, das Datenpakete zwischen Netzwerkgeräten überträgt. In dieser Topologie dient der Hub als zentrale Verbindungseinheit, die den Datenverkehr von und zu allen Geräten im Netzwerk weiterleitet. Es ist wichtig zu beachten, dass ein Hub alle Daten an alle angeschlossenen Geräte sendet, was potenziell zu Netzwerkstaus führen kann. Trotzdem wurde er hier aufgrund seiner Einfachheit und Unkompliziertheit gewählt.

**Server-PT:** Ein zentraler Server wurde hinzugefügt, um Netzwerkdienste wie Datei- und Druckerfreigabe, DNS und DHCP bereitzustellen. Seine primäre Aufgabe ist es, zentrale Dienste für alle Endbenutzergeräte bereitzustellen. Eine feste IP-Adresse (192.168.1.2/24) wurde ihm zugewiesen, um eine konsistente Kommunikation und Erreichbarkeit zu gewährleisten

**Sniffer:** Dieses Werkzeug wurde in die Topologie integriert, um den Netzwerkverkehr zu überwachen und zu analysieren. Ein Sniffer ermöglicht es Netzwerkadministratoren, den Datenverkehr in Echtzeit zu überwachen, potenzielle Probleme zu identifizieren und Einblicke in die Netzwerkleistung zu erhalten.

Die Gesamtkonfiguration dieser Geräte auf der ersten Etage ermöglicht eine einfache, aber effiziente Kommunikationsstruktur. Es wurde darauf geachtet, dass die Grundbedürfnisse eines Büronetzwerks abgedeckt sind, während gleichzeitig Raum für Erweiterungen und Modifikationen in den folgenden Etagen des Projekts bleibt.

## Konfiguration des Sniffers und des Servers

### Sniffer-Konfiguration

Ein Sniffer, auch bekannt als Netzwerkanalysator oder Packet Capture Tool, ermöglicht es, den Netzwerkverkehr in Echtzeit zu überwachen und Datenpakete, die durch das Netzwerk fließen, zu inspizieren. Dies ist besonders nützlich, um Netzwerkleistung, Sicherheitsbedrohungen und allgemeines Netzwerkverhalten zu überwachen.

*Schritte zur Konfiguration des Sniffers:*

**1.Standortwahl:** Der Sniffer wurde so positioniert, dass er alle Datenpakete, die durch den Hub fließen, abfangen kann, um einen vollständigen Überblick über den Netzwerkverkehr zu erhalten.

**2.Interface-Auswahl:** Das richtige Interface des Sniffers wurde ausgewählt, um den Datenverkehr auf dem gesamten Netzwerk zu überwachen.

**3.Filtereinstellungen (optional):** Je nach Bedarf können spezifische Filter angewendet werden, um nur bestimmte Typen von Datenpaketen anzuzeigen. Dies kann nützlich sein, um spezifische Netzwerkaktivitäten oder -probleme zu isolieren.

### Server-PT-Konfiguration

Der Server in unserer Topologie erfüllt eine zentrale Rolle und bietet verschiedene Dienste für das gesamte Netzwerk.

*Schritte zur Konfiguration des Server-PT:*

**1.Feste IP-Adresse zuweisen:** Gemäß den Projektanforderungen wurde dem Server die IP-Adresse 192.168.1.2 mit einer Subnetzmaske von /24 zugewiesen. Dies stellt sicher, dass der Server konsequent erreichbar ist und als stabile Ressource im Netzwerk dient.

**2.DHCP-Konfiguration:**

-Aktivierung den DHCP-Dienst auf dem Server.

-Definierung den IP-Adressbereich, den der DHCP-Server den Endgeräten zuweisen kann. In diesem Fall startet der Bereich bei 192.168.1.3 (da 192.168.1.1 und 192.168.1.2 bereits zugewiesen sind) und könnte bis 192.168.1.254 gehen, je nach Anzahl der Geräte im Netzwerk.

-Lease-Zeit und andere DHCP-Einstellungen können je nach den spezifischen Anforderungen des Netzwerks angepasst werden.

**3.Überprüfung der DHCP-Funktionalität:** Nach der Konfiguration des DHCP-Servers wurde überprüft, ob das PC und das Laptop automatische IP-Adressen vom DHCP-Server erhalten haben. Dies stellt sicher, dass der DHCP-Server ordnungsgemäß funktioniert und die Endgeräte korrekt konfiguriert sind.

Der Server und der Sniffer sind jetzt einsatzbereit und bieten sowohl Netzwerkdienste als auch Überwachungsfunktionen für die erste Etage des Bürokomplexes.

## Einbau und Konfiguration des Routers, Switches und der drahtlosen Geräte

### Router-Konfiguration

-Die Integration eines Routers in die Topologie ermöglicht eine Segmentierung des Netzwerks und bietet die Möglichkeit zur Kommunikation zwischen diesen Segmenten. Er spielt eine entscheidende Rolle in unserer Netzwerktopologie, insbesondere bei der Verbindung zu anderen Etagen oder Segmenten.

*Schritte zur Konfiguration des Routers:*

**IP-Adressierung:** Gemäß den Projektanforderungen wurde die erste IP-Adresse des Routers auf 192.168.1.1/24 und die zweite IP-Adresse auf 172.16.1.1/24 festgelegt. Dies stellt sicher, dass der Router sowohl im 192.168.1.0/24-Netzwerksegment als auch im 172.16.1.0/24-Segment ordnungsgemäß kommunizieren kann.

**Routing:** Standard-Routing-Einträge wurden hinzugefügt, um die Kommunikation zwischen den verschiedenen Subnetzen zu ermöglichen.

### Switch-Konfiguration

Ein Switch wurde eingefügt, um eine effizientere Netzwerkkommunikation im Vergleich zu einem Hub zu ermöglichen. Im Gegensatz zu einem Hub sendet ein Switch Datenpakete nur an das spezifische Zielgerät, was den Netzwerkverkehr reduziert und die Leistung verbessert.

Grundlegende Schritte zur Konfiguration des Switches:

Port-Konfiguration: Die Ports des Switches wurden entsprechend den angeschlossenen Geräten konfiguriert. Dies kann VLAN-Zuweisungen, Port-Geschwindigkeiten und andere spezifische Einstellungen umfassen.

### Einbindung und Konfiguration der drahtlosen Geräte

Drahtlose Kommunikation ist in modernen Büroumgebungen unerlässlich und bietet Flexibilität und Mobilität für die Benutzer.

*Schritte zur Einbindung drahtloser Geräte:*

**1.Access Point (AP) hinzufügen:** Ein Access Point wurde in die Topologie integriert, um drahtlose Geräte wie Laptops und mobile Geräte mit dem Netzwerk zu verbinden.

**2.Drahtlose Endgeräte:** Ein PC und ein Drucker wurden drahtlos über den Access Point hinzugefügt. Dies ermöglicht diesen Geräten, ohne physische Verkabelung mit dem Netzwerk zu kommunizieren.

**3.AP-Konfiguration:**

Sicherheitsprotokolle wie WPA2 kann hier aktiviert werden, um die drahtlose Kommunikation zu sichern.

Ein SSID (Service Set Identifier) können wir festlegen, um das drahtlose Netzwerk zu identifizieren.

Die drahtlosen Kanaleinstellungen wurden so konfiguriert, dass sie minimale Interferenzen mit anderen drahtlosen Netzwerken oder Geräten aufweisen.

Mit der Integration und Konfiguration dieser Netzwerkelemente auf der ersten Etage wird eine robuste und flexible Netzwerktopologie geschaffen, die den Anforderungen eines modernen Bürokomplexes gerecht wird.

## Implementierung und Konfiguration des DHCP-Servers

### Übersicht

-Das Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkprotokoll, das es Netzwerkgeräten ermöglicht, automatisch IP-Adressen und andere Netzwerkkonfigurationsinformationen von einem DHCP-Server zu erhalten. In diesem Projektsegment wird ein DHCP-Server eingerichtet, um automatisch IP-Adressen an Netzwerkgeräte auf der ersten Etage zu verteilen.

### Einrichtung des DHCP-Servers

**1.Server-Installation:** Ein dedizierter DHCP-Server wurde dem Netzwerk hinzugefügt und mit dem Switch verbunden, um eine optimale Erreichbarkeit für alle Geräte zu gewährleisten.

**2.IP-Adressierung:** Gemäß den Projektanforderungen wurde dem Server die statische IP-Adresse 192.168.1.2/24 zugewiesen, um Konflikte mit dynamisch zugewiesenen Adressen zu vermeiden.

### DHCP-Bereichskonfiguration

-Es wurden zwei DHCP-Bereiche eingerichtet, um den Anforderungen des Büronetzwerks gerecht zu werden:

**1. Erster Bereich:** Dieser Bereich deckt das 192.168.1.0/24-Netzwerksegment ab und ist für Geräte in diesem Segment vorgesehen. Der Bereich stellt sicher, dass Geräte automatisch IP-Adressen aus diesem Segment erhalten.

**2.Zweiter Bereich:** Ein zusätzlicher Bereich wurde eingerichtet, um das 172.16.1.0/24-Netzwerksegment abzudecken. Dieser Bereich ist hauptsächlich für den drahtlosen Bereich vorgesehen und der Startpunkt wurde auf 172.16.1.100/24 festgelegt.

### Verifikation der DHCP-Funktion

**1.Automatische IP-Adresszuweisung:** Es wurde überprüft, ob der PC und das Laptop, die mit dem Netzwerk verbunden sind, automatisch IP-Adressen aus den konfigurierten DHCP-Bereichen erhalten haben.

**2.DHCP-Lease:** Über das DHCP-Management-Tool wurde bestätigt, dass die Geräte die IP-Adressen korrekt von unserem DHCP-Server bezogen haben.

### Weitere Konfigurationen

**1.DNS-Integration:** Der DHCP-Server wurde ebenfalls als DNS-Server konfiguriert. Dadurch können Client-Geräte nicht nur IP-Adressen, sondern auch DNS-Informationen automatisch erhalten, was die Namensauflösung im Netzwerk erleichtert.

**2. Anpassung der DHCP-Bereiche:** Je nach den Bedürfnissen des Netzwerks können Bereiche erweitert oder verkleinert werden. In diesem Szenario wurde keine Änderung an den Bereichen vorgenommen, aber die Möglichkeit besteht.

**3.Erweiterung des Server-Pools:** Zusätzliche Server wurden beidseitig des Routers hinzugefügt, um sicherzustellen, dass Clients sie über ihren Namen und nicht nur über ihre IP-Adresse lokalisieren können.

Durch die Implementierung des DHCP-Servers auf der ersten Etage wird sichergestellt, dass Netzwerkgeräte automatisch die benötigten IP-Konfigurationsinformationen erhalten, was die Netzwerkverwaltung vereinfacht und die Effizienz erhöht.

## Netzwerkanalyse und Verwendung des Sniffers

### Einführung in den Sniffer

Ein Sniffer, oft auch als Netzwerkanalysator bezeichnet, ist ein Werkzeug, das den Datenverkehr in einem Netzwerk abfangen und analysieren kann. Er ermöglicht es Administratoren und Sicherheitsexperten, den Netzwerkverkehr zu überwachen und Unregelmäßigkeiten oder Sicherheitsbedrohungen zu erkennen.

### Einrichtung des Sniffers

**1.Positionierung:** Der Sniffer wurde strategisch im Netzwerk platziert, indem er direkt mit dem Hub verbunden wurde. Da Hubs den Datenverkehr an alle angeschlossenen Geräte senden, ist er der ideale Ort, um den gesamten durchgehenden Verkehr abzufangen.

**2.Konfiguration:** Für die Basiskonfiguration wurde der Sniffer so eingestellt, dass er den gesamten Datenverkehr abfängt, der durch den Hub fließt. Besondere Filter oder Einstellungen wurden zunächst nicht angewendet, um einen allgemeinen Überblick über den Netzwerkverkehr zu erhalten.

### Analyse des Netzwerkverkehrs

*Mit dem Sniffer konnten verschiedene Aspekte des Netzwerkverkehrs analysiert werden:*

**1.DHCP-Verkehr:** Es wurde beobachtet, wie Geräte DHCP-Anfragen senden und der DHCP-Server entsprechend Antworten liefert. Dies half, den Prozess der automatischen IP-Zuweisung zu bestätigen.

**2.ARP-Verkehr:** Address Resolution Protocol (ARP) Anfragen und Antworten wurden beobachtet, was bei der Zuordnung von IP-Adressen zu MAC-Adressen hilfreich ist.

**3.Ping-Tests:** Die erfolgreichen ICMP-Echo-Anfragen und -Antworten (Pings) zwischen den Geräten zeigten, dass die Kommunikation im Netzwerk ordnungsgemäß funktioniert.

### Sicherheitsbedenken

-Obwohl Sniffer wertvolle Werkzeuge für Netzwerktechniker sind, können sie auch von Angreifern verwendet werden, um Datenverkehr abzufangen und möglicherweise sensible Informationen zu stehlen. Es ist daher von entscheidender Bedeutung, sicherzustellen, dass nur autorisierte Benutzer Zugriff auf den Sniffer haben und dass alle gesammelten Daten sicher aufbewahrt und nach der Analyse ordnungsgemäß entsorgt werden.

### Fazit

Die Einführung eines Sniffers in das Büronetzwerk ermöglichte eine tiefe Einsicht in den Datenverkehr und die Funktionsweise des Netzwerks. Es wurde sichergestellt, dass die Konfigurationen, wie sie in den vorherigen Punkten beschrieben wurden, korrekt implementiert wurden und dass das Netzwerk effizient arbeitet.

## Router und drahtlose Konfiguration

### Einführung in Router und drahtlose Netzwerke

Router sind entscheidende Netzwerkgeräte, die Datenverkehr zwischen verschiedenen Netzwerken leiten, während drahtlose Netzwerke es Geräten ermöglichen, ohne physische Verbindungen miteinander zu kommunizieren.

### Router-Konfiguration

**1.Dual IP-Konfiguration:** Der Router wurde so konfiguriert, dass er zwei verschiedene IP-Adressen in unterschiedlichen Netzwerken verwendet:

-Die erste IP-Adresse ist 192.168.1.1/24. Dies ermöglicht die Kommunikation mit dem Hauptnetzwerk.

-Die zweite IP-Adresse ist 172.16.1.1/24. Dies dient der Kommunikation mit einem sekundären Netzwerkbereich.

**2.Schnittstellenkonfiguration:** Jede IP-Adresse wurde einer spezifischen Schnittstelle auf dem Router zugewiesen, um den Datenverkehr korrekt zu leiten.

### Drahtlose Konfiguration

**1.Access Point (AP) Einrichtung:** Ein Access Point wurde hinzugefügt, um drahtlose Kommunikation zu ermöglichen. Der AP wurde so konfiguriert, dass er sich nahtlos in das bestehende Netzwerk einfügt und die nötige Sicherheit gewährleistet.

**2.Drahtlose Geräte:** Ein PC und ein Drucker wurden drahtlos mit dem Access Point verbunden. Sie wurden so eingerichtet, dass sie sich automatisch mit dem bestehenden Netzwerk verbinden und die entsprechenden Ressourcen nutzen können.

**3.Sicherheitsstandards:** WPA3-Sicherheitsstandards wurden implementiert, um sicherzustellen, dass die drahtlose Kommunikation sicher und frei von Eindringlingen ist.

### Vorteile der Dual IP-Konfiguration

*Durch die Verwendung von zwei IP-Adressen auf dem Router können:*

1.Effizientere Datenroutingszenarien geschaffen werden.

2.Getrennte Netzwerkbereiche eingerichtet werden, die dennoch miteinander kommunizieren können.

3.Bestimmte Dienste oder Anwendungen können in einem bestimmten IP-Bereich isoliert werden, was die Sicherheit und Performance erhöhten.

### Fazit

Mit der Einrichtung eines Routers mit Dual IP-Konfiguration und der Implementierung eines drahtlosen Netzwerks wurde die Flexibilität und Skalierbarkeit des Büronetzwerks erheblich verbessert. Diese Konfiguration ermöglicht es, dass verschiedene Abteilungen oder Teams in separaten Netzwerken arbeiten können, während sie noch miteinander und mit zentralen Ressourcen kommunizieren können.

## DHCP-Konfiguration und Bereichsanpassung

### Einführung in DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Netzwerkprotokoll, das es ermöglicht, IP-Adressen und andere Netzwerkkonfigurationen automatisch an Netzwerkgeräte zu verteilen. Es reduziert die manuelle Konfigurationsarbeit und hilft, IP-Konflikte zu vermeiden.

### Ersteinrichtung des DHCP-Servers

**1.Server-Konfiguration:** Ein DHCP-Server wurde im Netzwerk eingerichtet. Die primäre IP-Adresse des Servers wurde auf 192.168.1.2/24 gesetzt.

**2.Erster DHCP-Bereich:** Ein Bereich von IP-Adressen wurde erstellt, um an die Geräte im Netzwerk verteilt zu werden. Dies stellt sicher, dass jedes Gerät eine einzigartige IP-Adresse erhält.

### DHCP-Bereichsanpassung und Erweiterung

**1.Zweiter DHCP-Bereich:** Ein zusätzlicher DHCP-Bereich wurde hinzugefügt, um die Geräte im Netzwerksegment 172.16.1.x/24 zu bedienen. Die Start-IP-Adresse dieses Bereichs wurde auf 172.16.1.100/24 festgelegt.

**2. Reservierungen:** Für kritische Geräte wie Server wurden feste IP-Reservierungen im DHCP eingerichtet. Dies stellt sicher, dass diese Geräte immer dieselbe IP-Adresse erhalten, unabhängig von Netzwerkausfällen oder Neustarts.

**3.Lease-Zeit:** Die Lease-Zeit (die Dauer, für die eine IP-Adresse an ein Gerät vergeben wird) wurde entsprechend den Netzwerkanforderungen festgelegt. Dies ermöglicht eine flexible und dynamische IP-Adressverwaltung.

### Verifizierung der DHCP-Funktionalität

**1.Automatische IP-Zuweisung:** Es wurde überprüft, ob PC und Laptop automatisch IP-Adressen vom DHCP-Server erhalten. Dies bestätigt die ordnungsgemäße Funktion des DHCP-Servers.

**2.Server-Bereiche:** Durch Überprüfung der Serverkonfiguration wurde sichergestellt, dass beide IP-Bereiche korrekt eingerichtet und aktiv sind.

### Vorteile der DHCP-Nutzung

*Die Implementierung von DHCP bietet verschiedene Vorteile:*

**1.Zeitersparnis:** Manuelle IP-Adresszuweisung ist zeitaufwendig und fehleranfällig. DHCP automatisiert diesen Prozess.

**2.Flexibilität:** Bei Änderungen im Netzwerklayout oder der Erweiterung des Netzwerks ermöglicht DHCP eine einfache Skalierung ohne umfangreiche manuelle Konfigurationen.

**3.Reduzierung von IP-Konflikten:** Durch die automatische Zuweisung von IP-Adressen werden Konflikte, die durch die doppelte Verwendung derselben IP-Adresse entstehen könnten, vermieden.

### Fazit

Durch die Einrichtung und Anpassung des DHCP-Servers wurde die Netzwerkkonfiguration vereinfacht und die Effizienz erhöht. Der Server stellt nun sicher, dass alle Geräte im Netzwerk ordnungsgemäß konfiguriert sind und nahtlos miteinander kommunizieren können.

## Transformation des Servers in einen DNS-Server

### Einführung in DNS

-DNS (Domain Name System) ist ein hierarchisches und dezentrales Namenssystem für Computer, Dienste oder andere Ressourcen, die mit dem Internet oder einem privaten Netzwerk verbunden sind. Es übersetzt besser merkbare Domain-Namen in die mit ihnen assoziierten IP-Adressen, die zum Lokalisieren und Identifizieren von Computerdiensten und -geräten mit den zugrunde liegenden Netzwerkprotokollen benötigt werden.

### Implementierung des DNS-Servers

**1.Server-Konfiguration:** Der bisherige Server mit der IP-Adresse 192.168.1.2/24 wurde in einen DNS-Server umgewandelt. Dies ermöglicht dem Netzwerk, Domain-Anfragen zu verarbeiten und aufzulösen.

**2.Domain-Zuweisung:** Domains wurden dem DNS-Server hinzugefügt, die jeweils mit bestimmten IP-Adressen im Netzwerk korrespondieren. Dies erleichtert die Netzwerkkommunikation, da Geräte nun über Domain-Namen anstelle von IP-Adressen kommunizieren können.

### Vorteile des DNS-Systems

**1.Benutzerfreundlichkeit:** Anstelle der Erinnerung an IP-Adressen können Benutzer einfach Domain-Namen eingeben, um auf Ressourcen zuzugreifen.

**2.Skalierbarkeit:** Mit DNS können Tausende von Domain-Namen und ihre entsprechenden IP-Adressen verwaltet werden, was besonders nützlich für große Netzwerke ist.

**3.Effiziente Netzwerkauflösung:** Das DNS-System beschleunigt die Netzwerkkommunikation, indem es Anfragen schnell auflöst.

### Verifizierung der DNS-Funktionalität

**1.Namensauflösung:** Es wurde überprüft, ob PCs und andere Netzwerkgeräte die Domain-Namen korrekt in IP-Adressen auflösen können.

**2.Server-Reaktionszeit:** Die Antwortzeiten des DNS-Servers wurden überwacht, um sicherzustellen, dass er Anfragen in einer akzeptablen Zeit bearbeitet.

### Fazit

Durch die Umwandlung des vorhandenen Servers in einen DNS-Server wurde die Netzwerkkommunikation erheblich verbessert. Die Benutzer können jetzt leichter auf Netzwerkressourcen zugreifen und der gesamte Kommunikationsprozess ist effizienter und benutzerfreundlicher.

## Hinzufügung weiterer Server auf beiden Seiten des Routers

### Zielsetzung

-Um die Leistungsfähigkeit und Redundanz des Netzwerks zu erhöhen und gleichzeitig sicherzustellen, dass die Clients effizient mit den Servern interagieren können, werden weitere Server auf beiden Seiten des Routers hinzugefügt. Dies ermöglicht es, dass die Clients die Server über deren Namen lokalisieren und mit ihnen kommunizieren können.

### Implementierungsschritte

**1.Serverplatzierung:** Weitere Server wurden strategisch auf beiden Seiten des Routers platziert, um die optimale Verteilung von Netzwerklast und Redundanz sicherzustellen.

**2.Serverkonfiguration:** Jeder neue Server wurde konfiguriert, um spezifische Dienste im Netzwerk bereitzustellen. Dies könnte Dienste wie Datenbanken, Webhosting oder Dateispeicherung umfassen.

**3.DNS-Einträge:** Neue Domain-Namen und die zugehörigen IP-Adressen wurden zum DNS-Server hinzugefügt. Dies erleichtert den Clients das Auffinden und Kommunizieren mit den neuen Servern über deren Domain-Namen.

### Verifizierung der Serverfunktionalität

**1.Ping-Tests:** Nach der Einrichtung der Server wurde von verschiedenen Clients aus ein Ping-Test durchgeführt, um sicherzustellen, dass die Kommunikation korrekt funktioniert.

**2.Dienstverfügbarkeit:** Die auf den Servern bereitgestellten Dienste wurden überprüft, um sicherzustellen, dass sie wie erwartet funktionieren und für die Clients zugänglich sind.

### Vorteile der erweiterten Serverarchitektur

**1.Erhöhte Kapazität:** Mit mehr Servern kann das Netzwerk mehr gleichzeitige Benutzeranfragen verarbeiten, was zu einer insgesamt besseren Performance führt.

**2.Redundanz:** Durch das Hinzufügen zusätzlicher Server wird das Risiko von Ausfällen minimiert, da der Datenverkehr bei Ausfall eines Servers zu einem anderen umgeleitet werden kann.

**3.Flexibilität:** Das Netzwerk kann leicht skaliert werden, indem bei Bedarf zusätzliche Server hinzugefügt werden.

### Fazit

Die Integration weiterer Server auf beiden Seiten des Routers hat nicht nur die Kapazität und Leistungsfähigkeit des Netzwerks erhöht, sondern auch die Flexibilität und Redundanz verbessert. Dies stellt sicher, dass die Benutzererfahrung optimiert wird und das Netzwerk selbst bei hohem Datenverkehr oder Serverausfällen stabil bleibt.

## IP-Konfiguration und Netzwerktopologie der zweiten Etage

In der zweiten Etage wurde eine differenzierte Netzwerkstruktur implementiert, um die verschiedenen Anforderungen und Services optimal zu unterstützen.

### IP-Konfiguration

Die verschiedenen IP-Subnetze in der zweiten Etage dienen dazu, die verschiedenen Abteilungen und Dienste zu segmentieren und zu organisieren:

Subnetz IP-Bereich Subnetzmaske Standard-Gateway

172.16.2.0/24 172.16.2.1-254 255.255.255.0 172.16.2.1

192.168.3.0/24 192.168.3.1-254 255.255.255.0 192.168.3.1

192.168.2.0/24 192.168.2.1-254 255.255.255.0 192.168.2.1

192.168.7.0/24 192.168.7.1-254 255.255.255.0 192.168.7.1

192.168.6.0/24 192.168.6.1-254 255.255.255.0 192.168.6.1

192.168.5.0/24 192.168.5.1-254 255.255.255.0 192.168.5.1

### Netzwerktopologie und Konfiguration

**Statische Routen:** Zur Gewährleistung einer kontinuierlichen Kommunikation zwischen den unterschiedlichen IP-Subnetzen wurden statische Routen in den Routern eingerichtet.

**RIP v2 Konfiguration:** Für ein dynamisches Routing und um eine effiziente Datenübertragung sicherzustellen, wurde RIP v2 auf allen Routern konfiguriert.

**1 zu 1 Topologie:** Diese Topologie wurde implementiert, um die Netzwerkkommunikation zu optimieren und die Abteilungen effektiv miteinander zu verbinden.

### Fazit

Die IP-Konfiguration und Netzwerktopologie der zweiten Etage gewährleisten eine effiziente und robuste Kommunikation, die auf die spezifischen Anforderungen der einzelnen Abteilungen und Dienste zugeschnitten ist.

## Netzwerktopologie und Konfiguration der dritten Etage

-Die dritte Etage stellt zusätzliche Netzwerkanforderungen, einschließlich der Implementierung von VLANs und inter-VLAN-Routing. Diese Ebene hat eine spezifische Konfiguration, die nicht nur die physische Struktur, sondern auch die logische Segmentierung des Netzwerks betrifft.

### VLAN-Konfiguration

-Virtual Local Area Networks (VLANs) sind in der dritten Etage eingeführt worden, um den Datenverkehr effektiv zu segmentieren und das Netzwerkmanagement zu vereinfachen.

**VLAN 2:** Dieses VLAN ist dem Subnetz 192.168.20.0/24 zugeordnet, mit einem IP-Bereich von 192.168.20.1-254. Das Standard-Gateway für dieses VLAN ist 192.168.20.1.

**VLAN 3:** Dieses VLAN ist dem Subnetz 192.168.30.0/24 zugeordnet, mit einem IP-Bereich von 192.168.30.1-254. Das Standard-Gateway für dieses VLAN ist 192.168.30.1.

### Inter-VLAN-Routing

-Da VLANs den Datenverkehr innerhalb ihrer eigenen Grenzen isolieren, wurde eine Lösung für das Inter-VLAN-Routing benötigt, um die Kommunikation zwischen VLAN 2 und VLAN 3 zu ermöglichen.

Router-on-a-Stick: Ein Multilayer-Switch wurde konfiguriert, um das Routing zwischen den VLANs zu ermöglichen. Die VLAN-Schnittstellen wurden mit IP-Adressen und Subnetz-Masken konfiguriert, wobei die erste Adresse ihres jeweiligen Subnetzes als IP-Adresse der Schnittstelle festgelegt wurde.

### PC-Konfiguration

-Alle PCs in der dritten Etage, die an beiden Access-Switches angeschlossen sind, wurden so konfiguriert, dass sie ihre jeweilige VLAN-Schnittstelle als Standard-Gateway verwenden.

### Fazit

-Die dritte Etage verfügt über eine erweiterte Netzwerkkonfiguration, die sowohl physische als auch logische Segmentierung bietet, um eine effiziente Kommunikation und Datenverkehrsteuerung innerhalb der Büroetage zu gewährleisten.

**Note:**

**Studie über Netzwerktopologien im Projekt**

**Gesamtes Projekt:**

Das gesamte Netzwerk in diesem Projekt stellt eine hierarchische Topologie dar, wobei jede Etage spezifische Netzwerkelemente und -strukturen aufweist. Die hierarchische Topologie ermöglicht die Skalierbarkeit des Netzwerks und erleichtert das Management durch die Segmentierung in verschiedene Ebenen.

Erste Etage:

Topologie: Auf dieser Etage wird eine Stern-Topologie verwendet, wobei das zentrale Verbindungselement ein Hub ist. Die Geräte, einschließlich PC, Laptop und Server, sind alle direkt mit dem Hub verbunden.

Verbindungstypen:

1.Kabelgebunden: PC, Laptop, Server und Sniffer sind über kabelgebundene Verbindungen an den Hub angeschlossen.

2.Drahtlos: Ein PC und ein Drucker sind drahtlos über einen Access Point verbunden.

Zweite Etage:

Topologie: In dieser Etage wird eine 1:1-Topologie (auch Punkt-zu-Punkt-Topologie genannt) verwendet, wobei jedes Gerät genau mit einem anderen Gerät verbunden ist.

Verbindungstypen:

1.RIP v2: Hier wurde RIP v2 verwendet, um den Routing-Prozess zu konfigurieren und die Konnektivität zwischen den PCs und Laptops zu gewährleisten.

Dritte Etage:

Topologie: Die dritte Etage verwendet eine VLAN-basierte Topologie, wobei VLAN 2 und VLAN 3 eingerichtet sind. Das gesamte VLAN-Netzwerk könnte als virtuelle Stern-Topologie betrachtet werden, wobei der zentrale Punkt (z.B. der Switch oder der Router) als Verbindungspunkt für verschiedene VLANs dient.

Verbindungstypen:

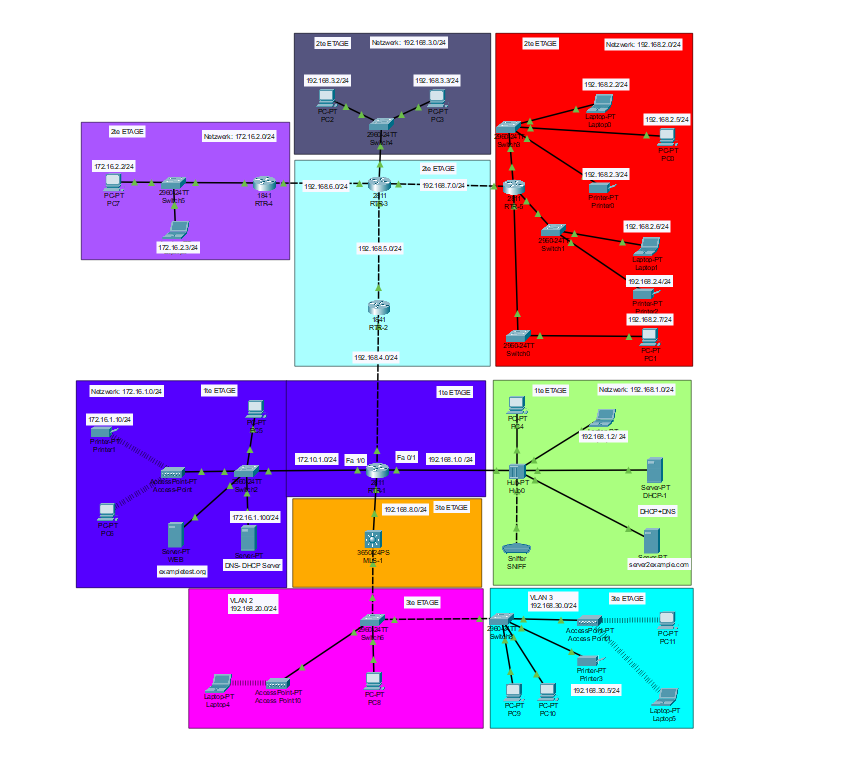
1.Router-on-a-Stick: Dies ermöglicht das Routing zwischen verschiedenen VLANs, die über denselben physischen Switch laufen.

-Insgesamt wird eine Mischung aus physischen und logischen Topologien verwendet, um das Netzwerk zu organisieren und die Kommunikation zwischen den Geräten zu ermöglichen.

Zusammenfassend basiert das Netzwerkdesign dieses Projekts auf einer Kombination verschiedener Topologien, um die Anforderungen und Ziele jeder Etage zu erfüllen. Das Ergebnis ist ein gut strukturiertes, skalierbares und effizientes Netzwerk.

# Abbildungsverzeichnis

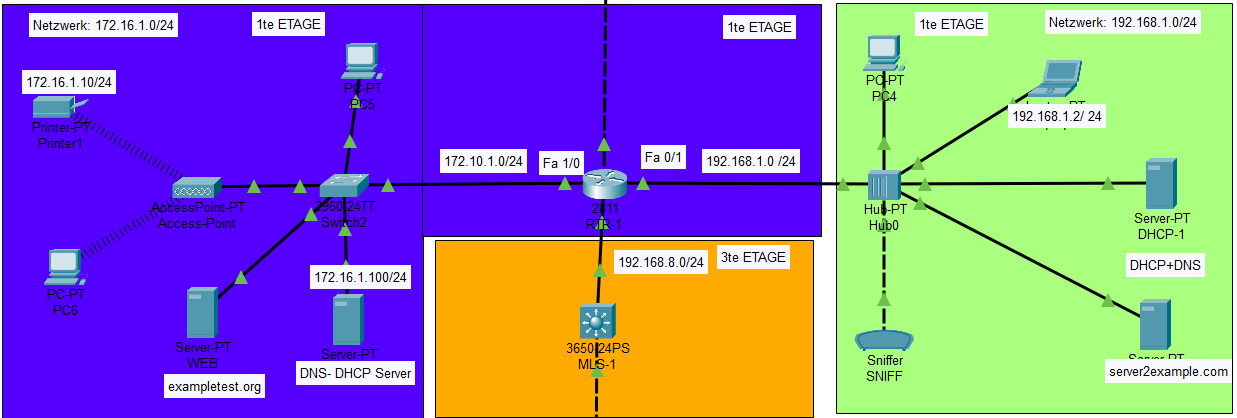
**Abbildung Gesamt Netzwerk Projekt:**

****

Gesamt Netzwerk-Projekt

**Erste Etage:**

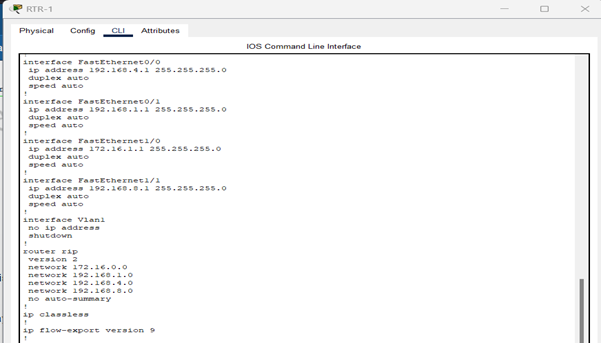
**Abbildung Gesamt Erste Etage:**

****

Erste Etage Gesamt-Abbildung

Abbildung 1.1: Router RTR 1

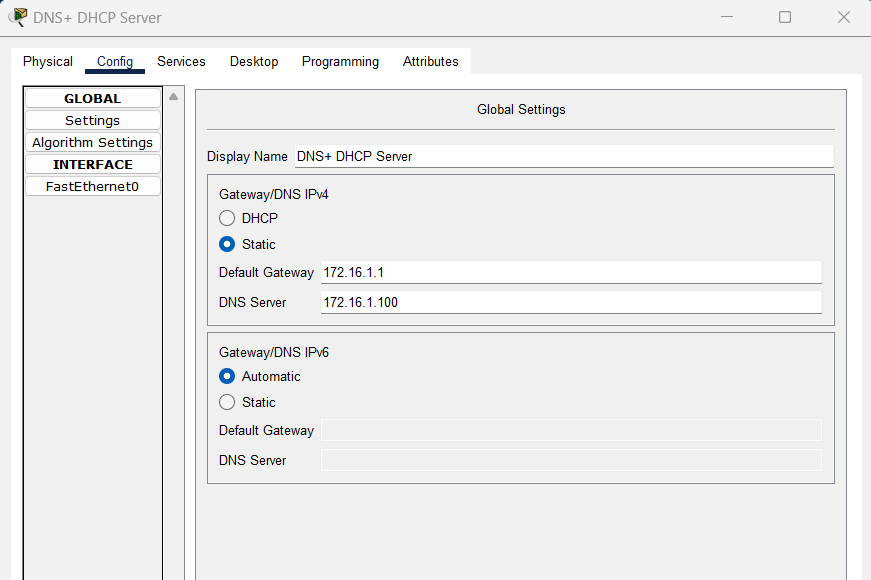
Zentraler Router, der die erste Etage mit dem Internet und den anderen Etagen verbindet.



Router RTR 1 #show-running-config

Abbildung 1.2: DHCP + DNS-Server

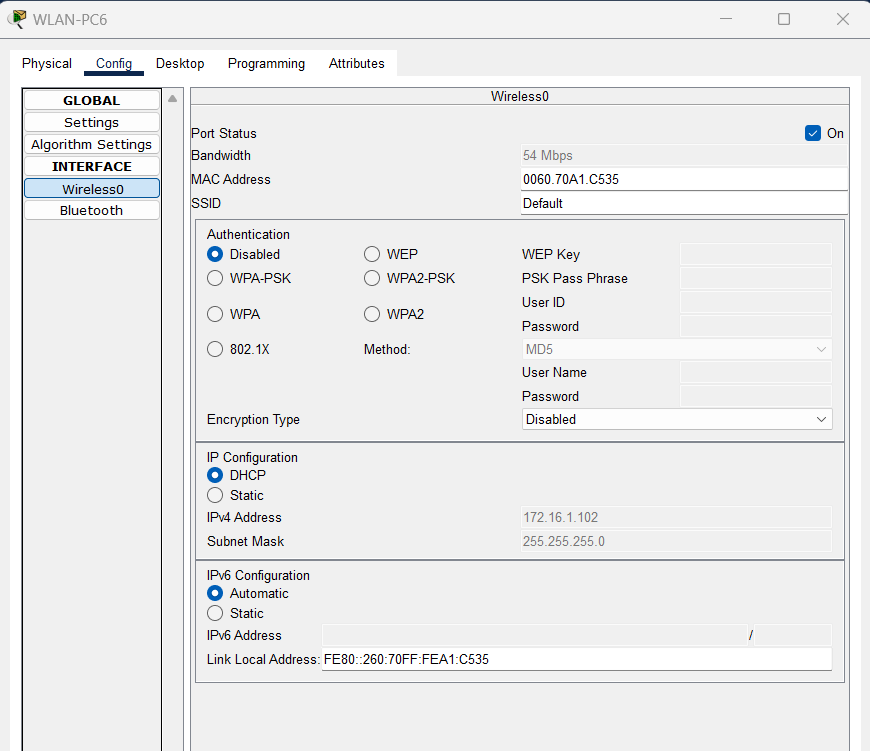
Hauptserver, der IP-Adressen verteilt und Domain-Namensanfragen auflöst.



DNS + DHCP-Server

Abbildung 1.3: WLAN PC

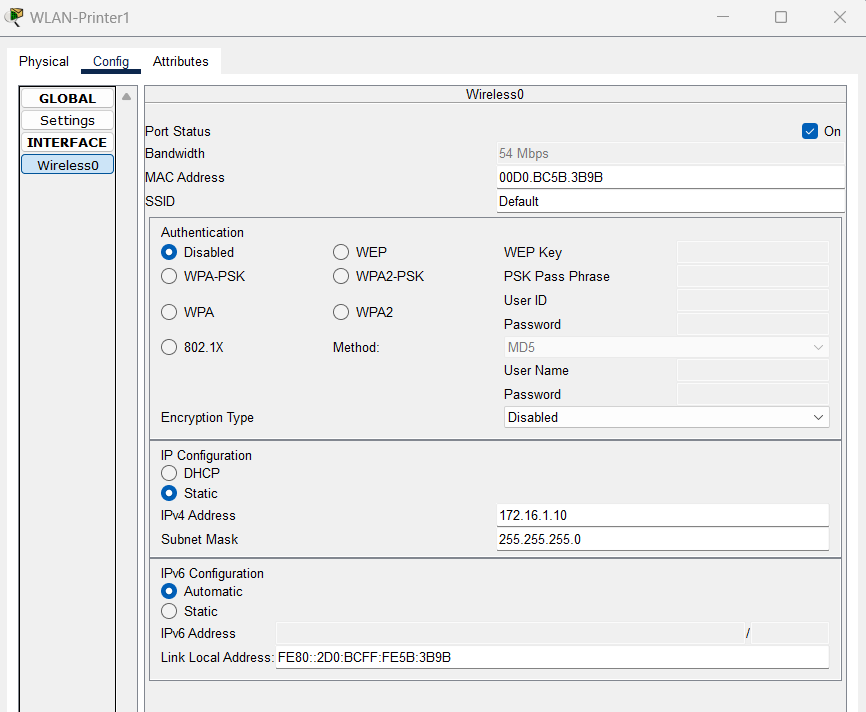
Ein drahtlos verbundener Arbeitsplatzrechner.



WLAN-Verbunden-Desktop Rechner

Abbildung 1.4: WLAN-Printer

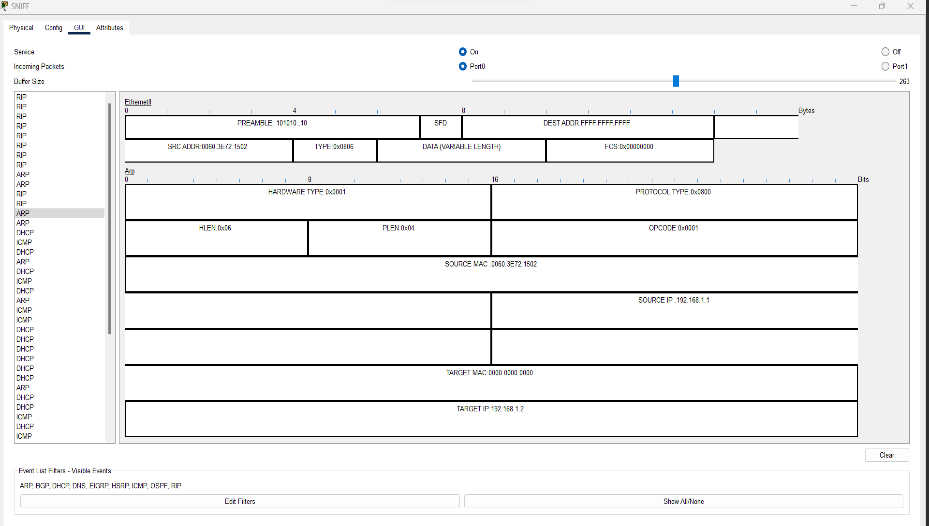
Drahtloser Drucker, der Druckaufträge aus dem Netzwerk entgegennimmt.



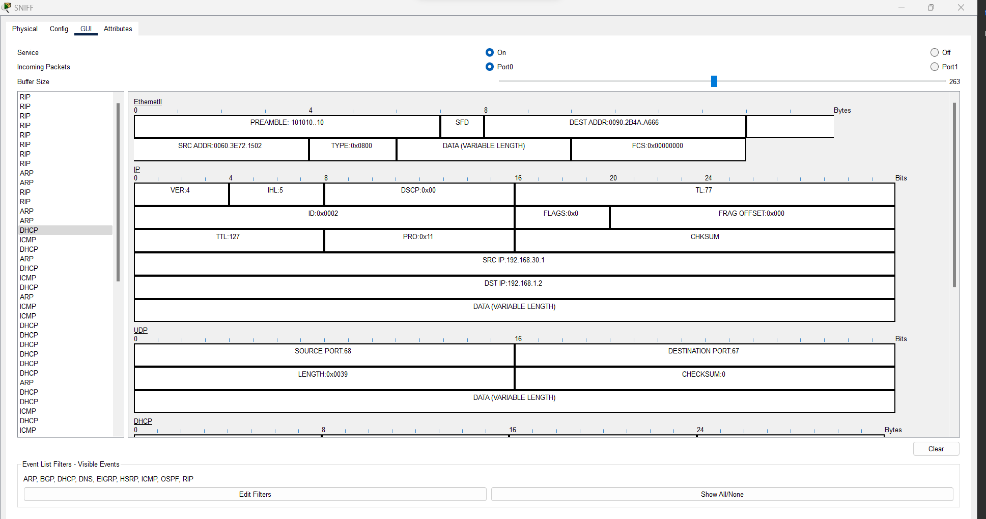
WLAN-Printer 1

Abbildung 1.5: Sniffer

Netzwerkanalysegerät zum Überwachen und Erfassen von Netzwerkverkehr.



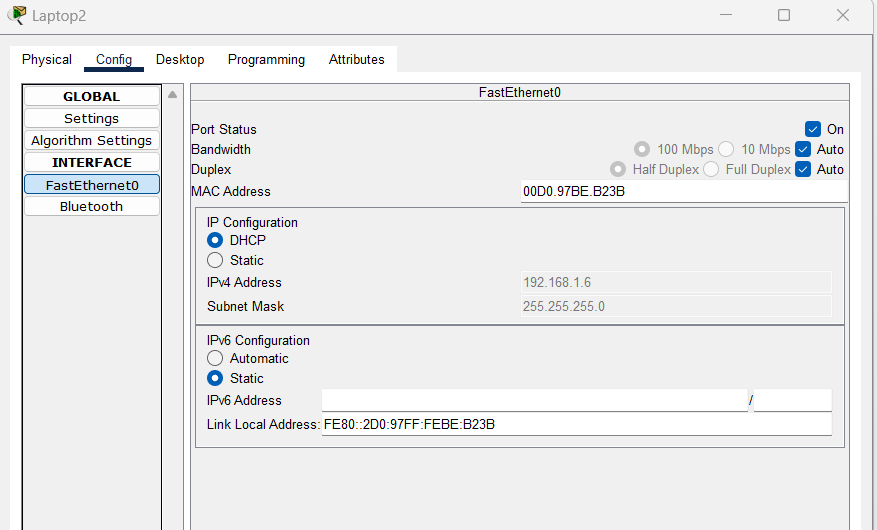
Sniffer ARP-Spoofing



DHCP Snooping and Spoofing

Abbildung 1.6: Laptop

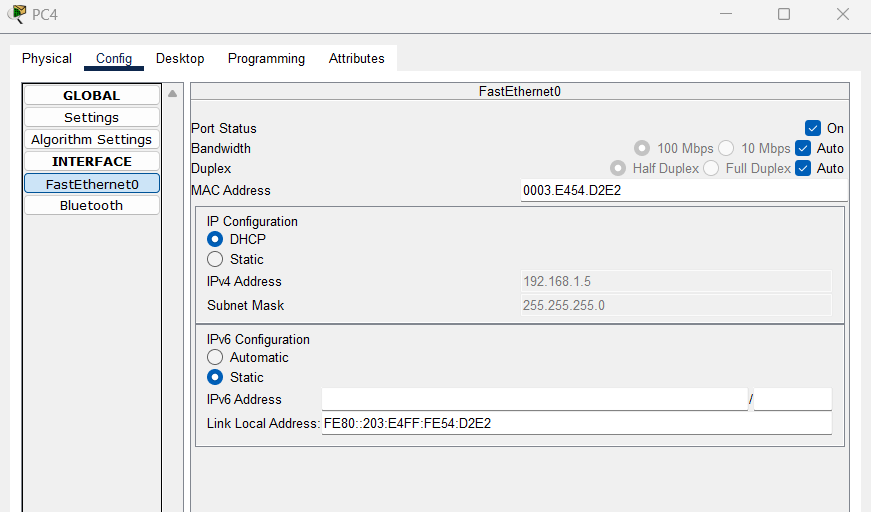
Mobiler Computer, der direkt über den Hub verbunden ist.



Laptop Konfiguration

Abbildung 1.7: PC

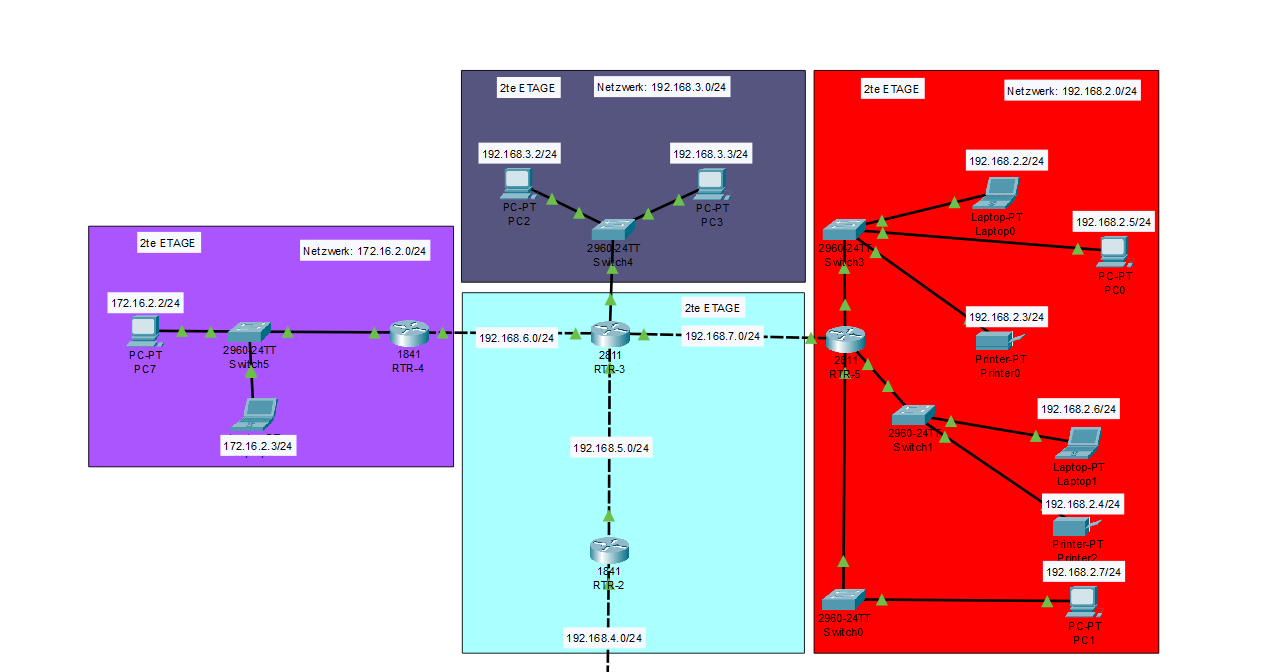
Arbeitsplatzrechner für tägliche Büroaufgaben.



Desktop PC-Konfiguration

**Zweite Etage:**

**Abbildung Gesamt Zweite Etage:**

****

2-te Etage gesamt Abbildung

Abbildung 2.1: RTR3-Router

Set von Routern, die den Datenverkehr zwischen den verschiedenen Segmenten der zweiten Etage steuern.

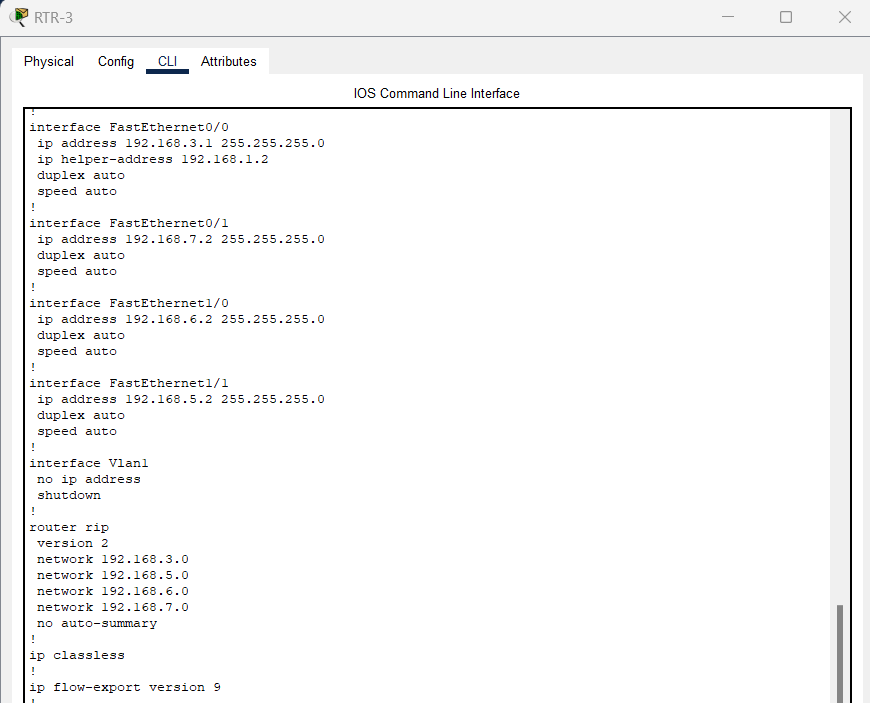
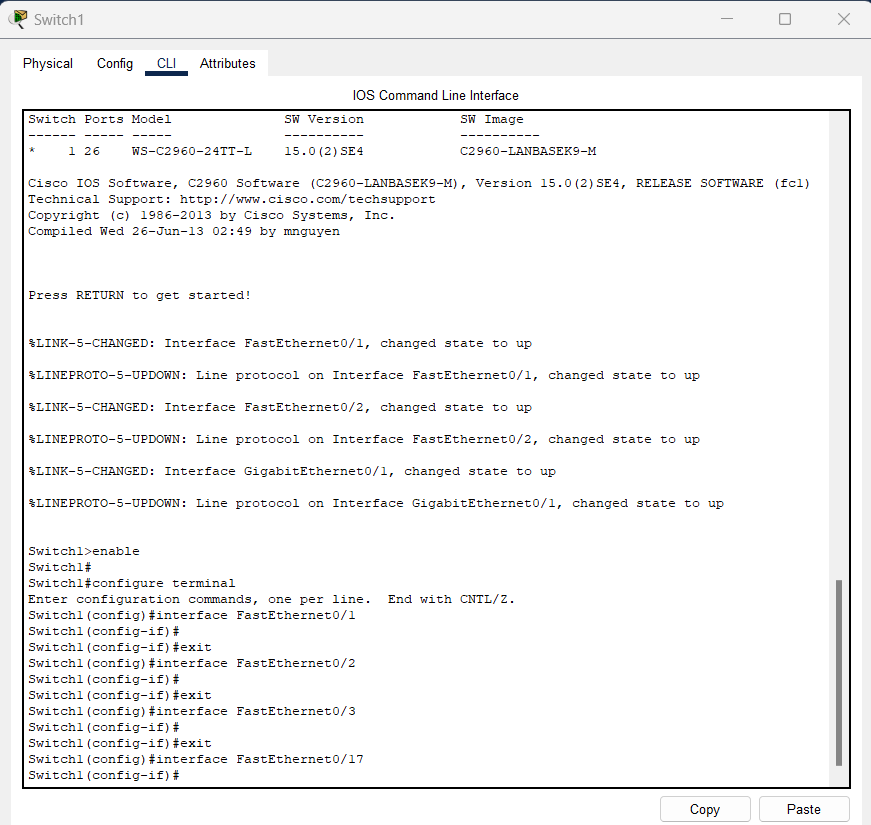


Abbildung Router RTR3 Interface FE-Konfiguration

Abbildung 2.2: Switch1

Gerät zur Verbindung von Netzwerksegmenten und zur Steuerung des Datenverkehrs

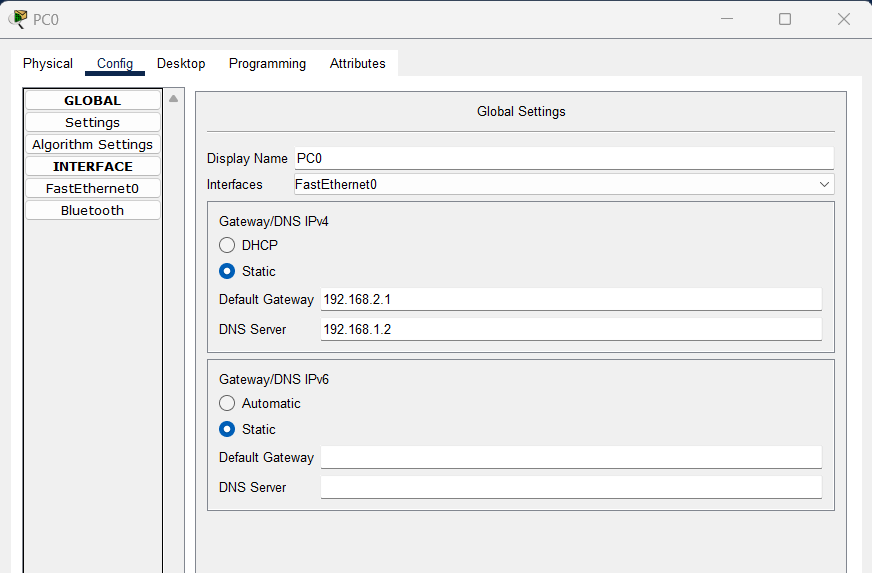
innerhalb des Netzwerks.



Switch 1 -Konfiguration

Abbildung 2.3: PC

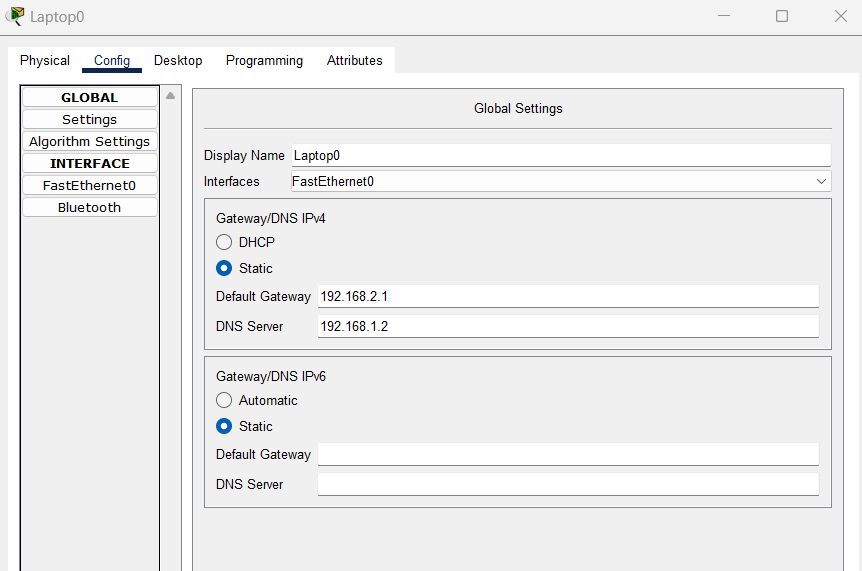
Arbeitsplatzrechner für Büromitarbeiter.



PC0 -Konfiguration

Abbildung 2.4: Laptop

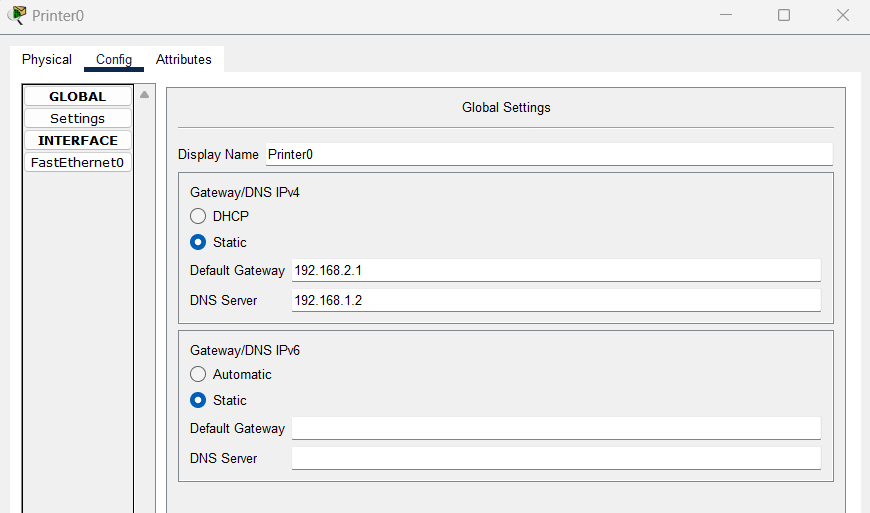
Mobile Arbeitsstation für Mitarbeiter, die Flexibilität benötigen.



Laptop0-Konfiguration

Abbildung 2.5: Printer

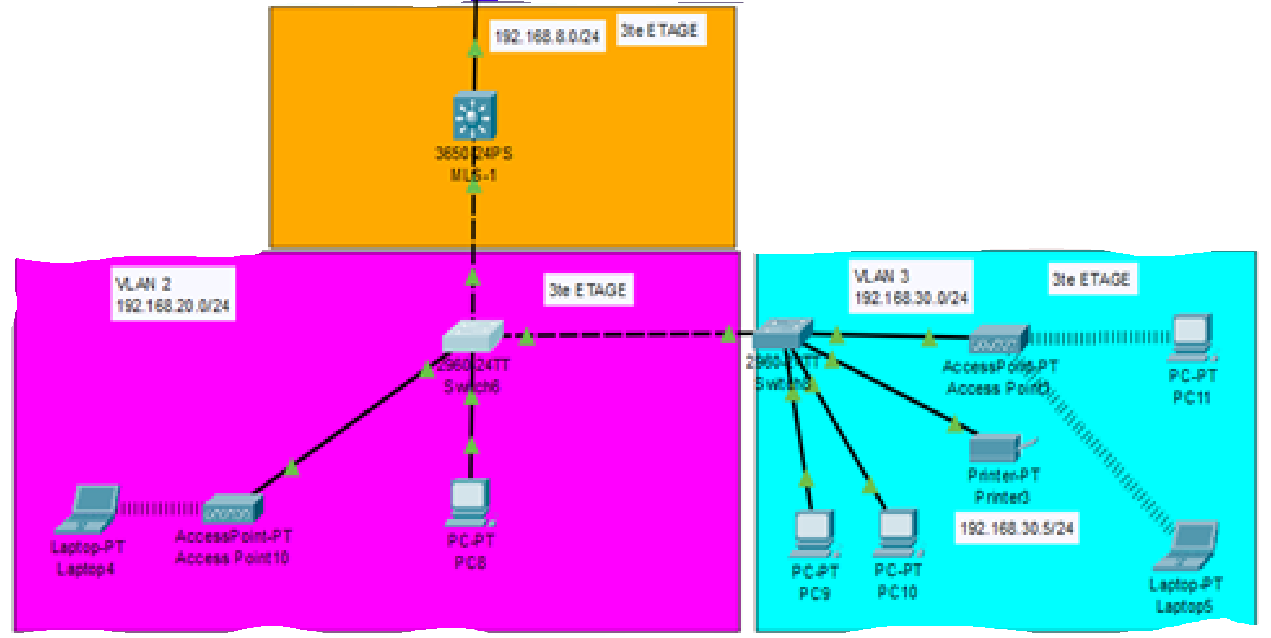
Netzwerkdrucker für alle Mitarbeiter auf der zweiten Etage.



Printer0 Statische-Konfiguration

**Dritte Etage:**

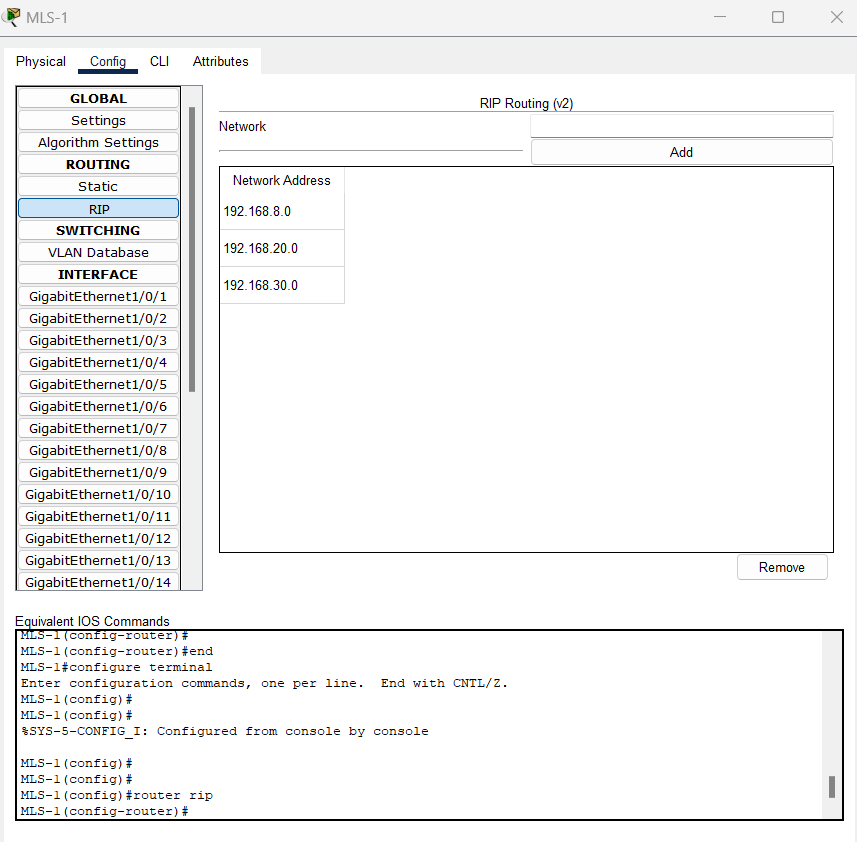
**Abbildung Gesamt Dritte Etage:**

****

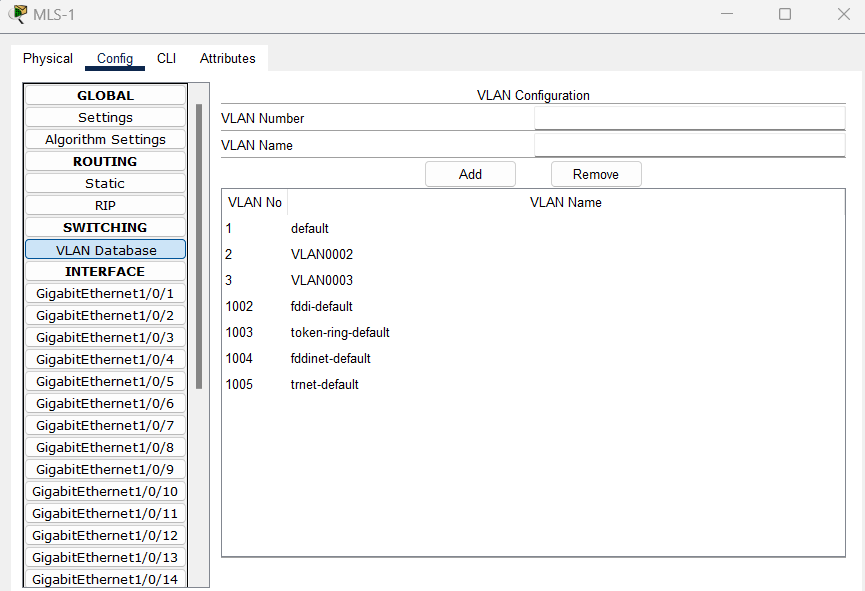
Gesamt Abbildung 3-te Etage

Abbildung 3.1: Multilayer Switch MLS-1

Fortgeschrittener Switch, der sowohl auf der Datenverbindungsebene als auch auf der Netzwerkebene arbeiten kann, um den Datenverkehr effizient zu steuern.



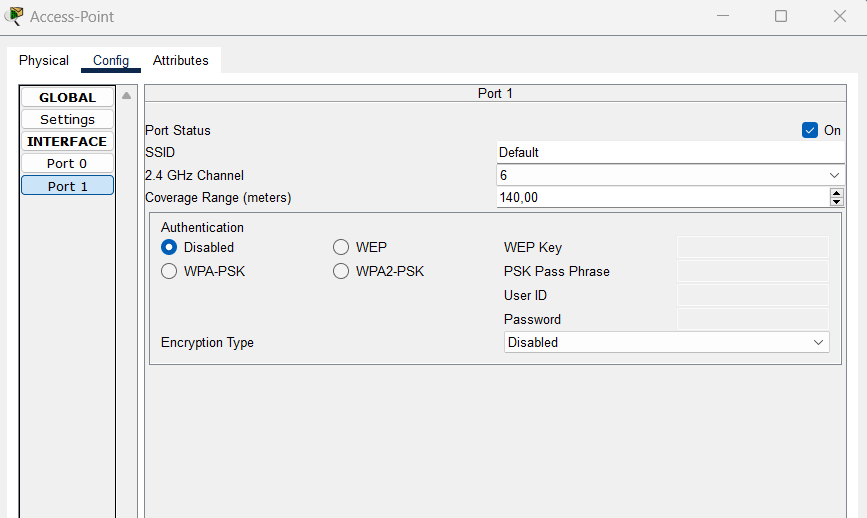
Multilayerswitch RIP-Konfiguration



Multilayerswitch -VLAN Database

Abbildung 3.2: Access Point

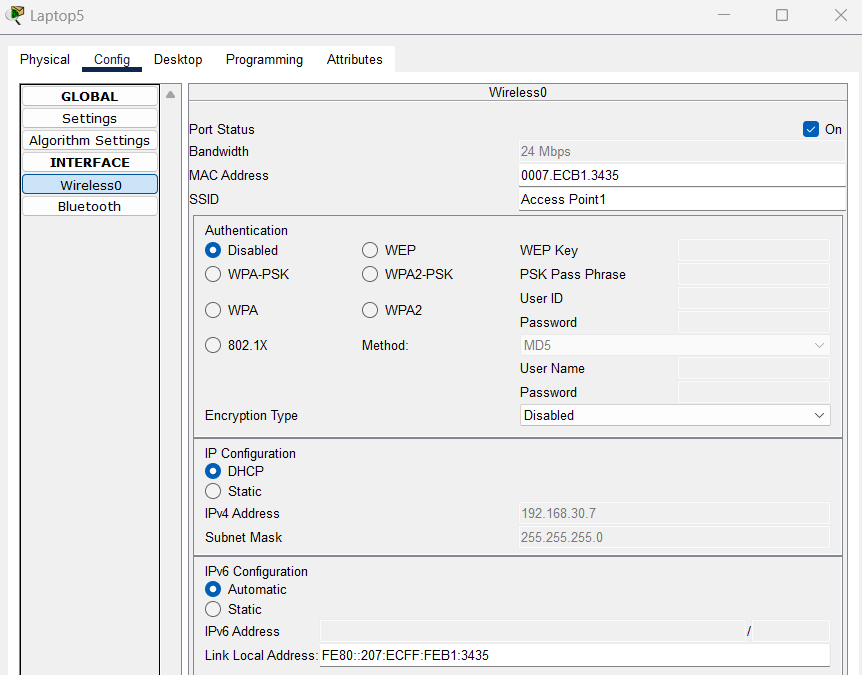
Gerät, das drahtlose Netzwerkkonnektivität für die Geräte auf dieser Etage bietet.



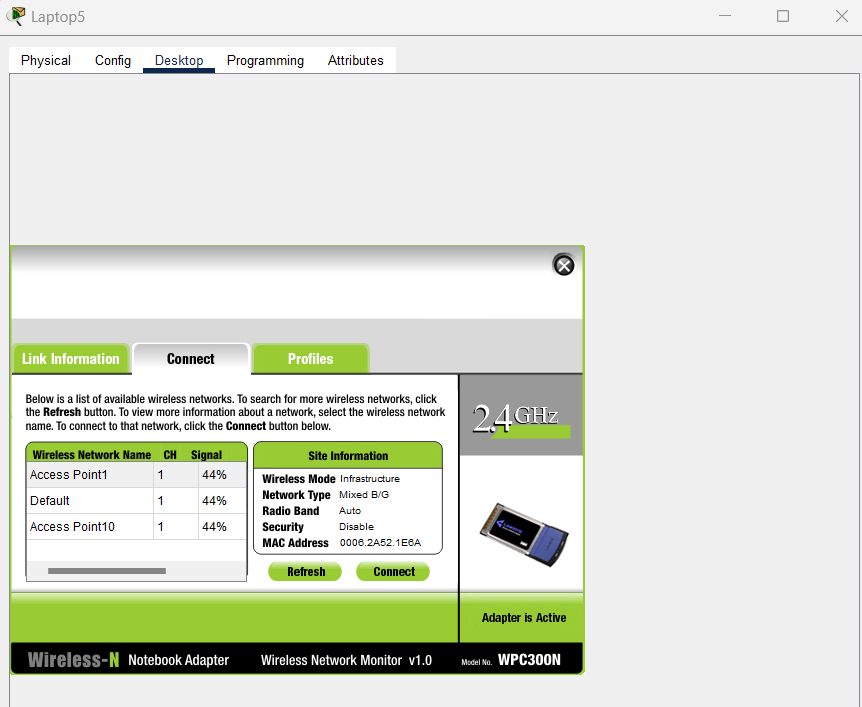
Access-Point Standard-Konfiguration

Abbildung 3.3: WLAN-Laptop

Laptop für Mitarbeiter, der drahtlos mit dem Netzwerk verbunden ist.



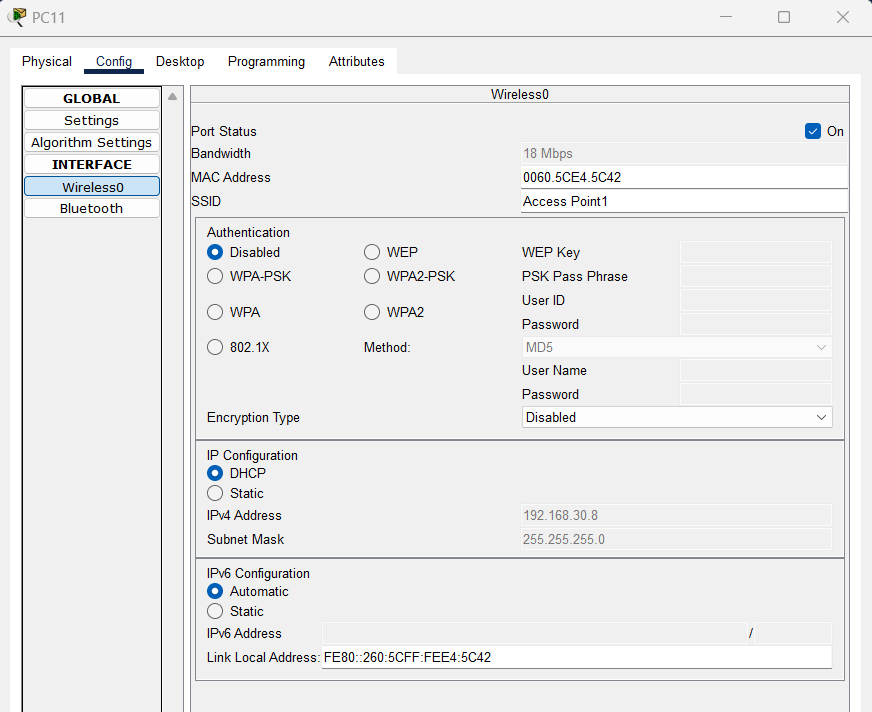
WLAN-Laptop Wireless0-Konfiguration



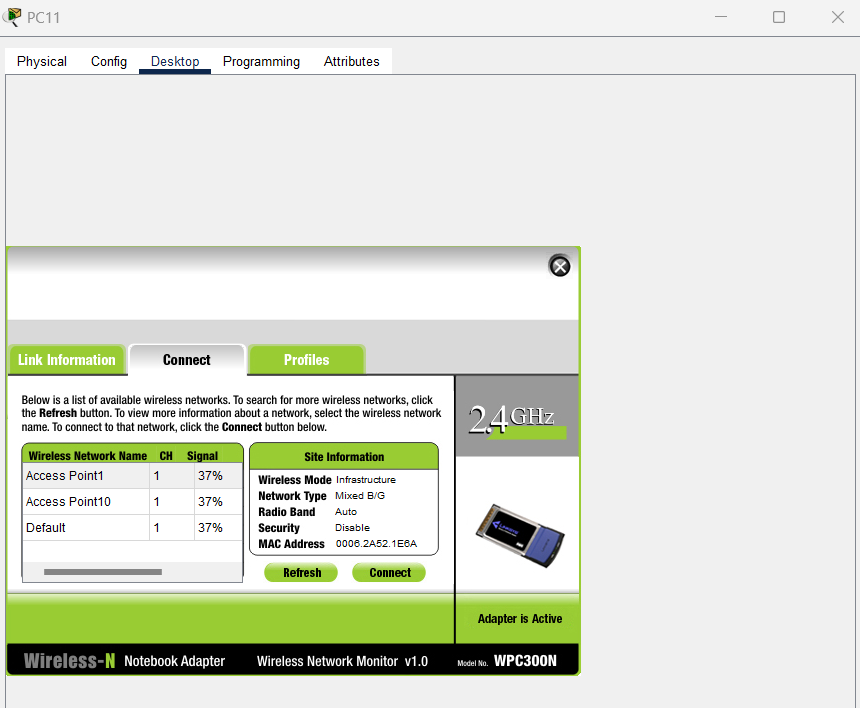
WLAN-Laptop Wireless Data-Connection

Abbildung 3.4: WLAN PC

Arbeitsplatzrechner mit drahtloser Netzwerkkonnektivität.



PC Wireless0-Konfiguration



Wireless PC- Connection

# Abkürzungsverzeichnis

DHCP - Dynamic Host Configuration Protocol: Ein Netzwerkprotokoll, das es Netzwerkgeräten ermöglicht, IP-Adressen und andere Netzwerkkonfigurationsinformationen automatisch von einem Server zu beziehen.

DNS - Domain Name System: Ein System zur Umwandlung von alphanumerischen Domain-Namen in IP-Adressen und umgekehrt.

IP - Internet Protocol: Das Hauptprotokoll in der Internet-Protokollsuite, das die Adressierung und Fragmentierung von Datenpaketen für die Übertragung ermöglicht.

VLAN - Virtual Local Area Network: Ein Netzwerkprotokoll, das es erlaubt, ein physisches Netzwerk in mehrere logischen Netzwerke zu unterteilen.

RIP - Routing Information Protocol: Ein Distanzvektor-Routing-Protokoll, das in lokalen und Weitverkehrsnetzwerken verwendet wird.

PC - Personal Computer: Ein Computer für individuelle Nutzung.

Router - Ein Gerät, das Daten zwischen verschiedenen Netzwerken weiterleitet.

Hub - Ein Netzwerkgerät, das Datenpakete von einem Port an alle anderen Ports weiterleitet.

Switch - Ein Netzwerkgerät, das Datenpakete basierend auf MAC-Adressen weiterleitet.

Sniffer - Ein Diagnose-Tool, das Netzwerkdatenpakete überwacht und analysiert.

Snooping – Erklärung

- "Snooping" bezeichnet im Allgemeinen das Überwachen, Überprüfen oder Abhören von Daten, die in einem Netzwerk übertragen werden. Es kann jedoch in unterschiedlichen Kontexten unterschiedliche spezifische Bedeutungen haben:

Allgemeines Netzwerk-Snooping: Dies bezieht sich auf den Prozess des Abhörens des Netzwerkverkehrs, oft mit dem Ziel, Daten oder Informationen zu erfassen, die zwischen Geräten übertragen werden. Ein Beispiel dafür wäre ein Netzwerkadministrator, der einen Netzwerk Sniffer verwendet, um den Datenverkehr in einem Netzwerk zu überwachen und mögliche Probleme zu diagnostizieren.

1.IGMP Snooping: Das steht für "Internet Group Management Protocol Snooping". Dies ist eine fortgeschrittene Funktion auf vielen Switches, die dazu dient, den Multicast-Verkehr effizienter zu gestalten. Ein Switch mit IGMP Snooping kann Multicast-Datenverkehr nur an die Ports weiterleiten, an denen ein Gerät den Empfang dieser Daten explizit angefordert hat

2.DHCP Snooping: Dies ist eine Sicherheitsfunktion auf vielen modernen Switches. Sie überwacht DHCP-Nachrichten auf dem Netzwerk, um DHCP-basierte Angriffe zu verhindern, wie zum Beispiel das Bereitstellen eines schädlichen DHCP-Servers durch einen Angreifer.

3.ARP Snooping: Dabei handelt es sich um eine Methode zur Überwachung von ARP (Address Resolution Protocol) auf einem Netzwerk, um bestimmte Arten von Angriffen, wie ARP Spoofing oder ARP Poisoning, zu verhindern.

Spoofing- Erklärung und Definition

"Spoofing" bezeichnet eine Kategorie von Cyberangriffen, bei denen eine Person oder ein Programm sich als eine andere Entität ausgibt, um bestimmte Informationen zu erlangen, Zugriff auf Systeme zu erhalten oder Vertrauensbeziehungen innerhalb von Netzwerken auszunutzen. Es gibt verschiedene Arten von Spoofing-Angriffen, abhängig vom spezifischen Kontext und Ziel:

1.IP-Spoofing: Hierbei sendet der Angreifer IP-Pakete mit einer gefälschten Absender-IP-Adresse. Das Ziel kann dazu verleitet werden, zu denken, dass die Pakete von einem vertrauenswürdigen Host stammen.

2.ARP-Spoofing (oder ARP-Poisoning): Der Angreifer sendet gefälschte ARP-Nachrichten in ein lokales Netzwerk, um die MAC-Adresse eines bestimmten Hosts durch die MAC-Adresse des Angreifers zu ersetzen. Dadurch kann der Angreifer den Datenverkehr umleiten und zwischen zwei Parteien im Netzwerk "sitzen", um Daten abzuhören oder zu manipulieren.

3.DNS-Spoofing: Bei diesem Angriff werden DNS-Abfragen manipuliert, um den Benutzer zu einer gefälschten Website zu leiten, die wie die echte Website aussieht. Dies wird oft in Phishing-Angriffen verwendet.

4.E-Mail-Adresse-Spoofing: Hier gibt sich der Angreifer in einer E-Mail als jemand anderes aus, oft mit der Absicht, den Empfänger zu täuschen oder Malware zu verbreiten.

5.Caller-ID-Spoofing: Bei diesem Angriff wird die Anrufer-ID gefälscht, um dem Empfänger eines Anrufs vorzutäuschen, dass der Anruf von einer anderen Nummer oder Person stammt.

6.Website-Spoofing: Bei diesem Angriff wird eine gefälschte Website erstellt, die wie eine legitime aussieht, mit dem Ziel, Benutzerinformationen zu stehlen oder Malware zu verbreiten.

Spoofing-Angriffe zielen darauf ab, Vertrauen zu missbrauchen und können oft schwer zu erkennen sein. Deshalb sind in vielen Systemen und Netzwerken verschiedene Schutzmaßnahmen implementiert, um solche Angriffe zu verhindern oder zu erkennen.

# QUELLVERZEICHNISS

1.YouTube. https://www.youtube.com/. Datum des Zugriffs: 17. Juli 2023.

2.Cisco Systems, Inc. https://www.cisco.com/. Datum des Zugriffs: 20. Juli 2023.

3.Google. https://www.google.com/. Datum des Zugriffs: 25. Juli 2023.

4.Wikipedia, Die freie Enzyklopädie. https://de.wikipedia.org/. Datum des Zugriffs: 2. August 2023.

5.ChatGPT by OpenAI. Formulierung und Informationen bereitgestellt durch ChatGPT. Datum des Gesprächs: 10. August 2023.