

# Multi-Layer Switch mit VLANs und Dual-Stack (IPv4/IPv6)

---

## Lernsituation

### Ausgangssituation

Die Bildungseinrichtung "Campus Network AG" benötigt eine moderne Netzwerkinfrastruktur zur Segmentierung verschiedener Benutzergruppen. Die Einrichtung verfügt über drei Hauptnutzergruppen mit unterschiedlichen Sicherheits- und Netzwerkanforderungen:

- **Staff (Personal)**: Administratives Personal und Lehrer mit erhöhten Sicherheitsanforderungen
- **Students (Studenten)**: Studenten mit standardmäßigem Internetzugang und eingeschränkten Berechtigungen
- **Faculty (Fakultät)**: Professoren und Forscher mit erweiterten Netzwerkrechten

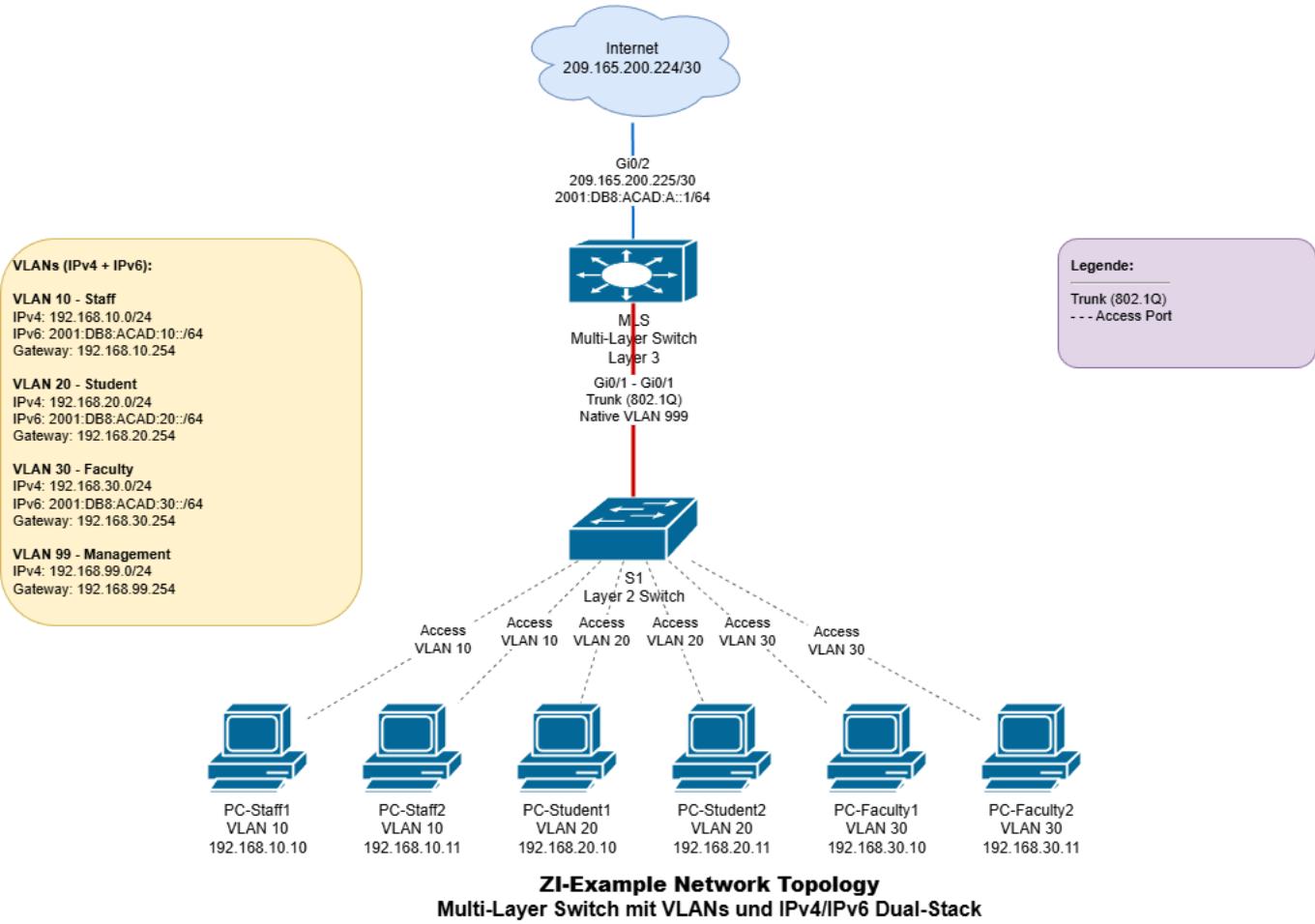
Die IT-Abteilung möchte eine zukunftssichere Lösung implementieren, die sowohl IPv4 als auch IPv6 unterstützt. Zusätzlich soll ein Management-VLAN für die Verwaltung der Netzwerkgeräte eingerichtet werden. Die Lösung verwendet einen Multi-Layer Switch (Layer 3 Switch) für Inter-VLAN Routing und einen Layer 2 Access Switch für die Endgeräteanbindung.

### Lernziele

Nach Abschluss dieser Übung können Sie:

- VLANs auf Cisco Switches erstellen und konfigurieren
- Layer 3 Funktionalität auf Multi-Layer Switches aktivieren (IP Routing)
- Dual-Stack Konfiguration (IPv4 und IPv6) implementieren
- SVIs (Switched Virtual Interfaces) für Inter-VLAN Routing konfigurieren
- Trunk-Ports mit 802.1Q Encapsulation einrichten
- Native VLAN für zusätzliche Sicherheit konfigurieren
- Access-Ports einzelnen VLANs zuweisen
- IPv6 Unicast-Routing aktivieren und konfigurieren
- Netzwerk-Konnektivität in Dual-Stack Umgebungen testen
- Best Practices für Enterprise Netzwerke anwenden

## Topologie



## Netzwerkgeräte

- **1x Multi-Layer Switch (MLS):** Cisco Catalyst 3650/3850 oder ähnlich mit Layer 3 Funktionalität
- **1x Layer 2 Switch (S1):** Cisco Catalyst 2960 oder ähnlich
- **6x PCs:** Endgeräte in verschiedenen VLANs
  - 2x PCs in VLAN 10 (Staff)
  - 2x PCs in VLAN 20 (Student)
  - 2x PCs in VLAN 30 (Faculty)

## Externe Verbindung

- **Internet-Anbindung:** Über MLS GigabitEthernet0/2
- **IPv4:** 209.165.200.225/30
- **IPv6:** 2001:DB8:ACAD:A::1/64

## VLAN- und IP-Adressplan

### IPv4 Adressen

| VLAN | Name    | Zweck                | Netz            | Maske         | Gateway (MLS SVI) |
|------|---------|----------------------|-----------------|---------------|-------------------|
| 10   | Staff   | Personal/Lehrer      | 192.168.10.0/24 | 255.255.255.0 | 192.168.10.254    |
| 20   | Student | Studenten            | 192.168.20.0/24 | 255.255.255.0 | 192.168.20.254    |
| 30   | Faculty | Professoren/Forscher | 192.168.30.0/24 | 255.255.255.0 | 192.168.30.254    |

| VLAN | Name       | Zweck             | Netz            | Maske         | Gateway (MLS SVI) |
|------|------------|-------------------|-----------------|---------------|-------------------|
| 99   | Management | Switch-Verwaltung | 192.168.99.0/24 | 255.255.255.0 | 192.168.99.254    |

IPv6 Adressen

| VLAN | IPv6 Netz             | Gateway (MLS SVI)   |
|------|-----------------------|---------------------|
| 10   | 2001:DB8:ACAD:10::/64 | 2001:DB8:ACAD:10::1 |
| 20   | 2001:DB8:ACAD:20::/64 | 2001:DB8:ACAD:20::1 |
| 30   | 2001:DB8:ACAD:30::/64 | 2001:DB8:ACAD:30::1 |

Beispiel PC-Konfigurationen

| PC          | VLAN | IPv4          | Subnet Mask   | Gateway        | IPv6                    |
|-------------|------|---------------|---------------|----------------|-------------------------|
| PC-Staff1   | 10   | 192.168.10.10 | 255.255.255.0 | 192.168.10.254 | 2001:DB8:ACAD:10::10/64 |
| PC-Staff2   | 10   | 192.168.10.11 | 255.255.255.0 | 192.168.10.254 | 2001:DB8:ACAD:10::11/64 |
| PC-Student1 | 20   | 192.168.20.10 | 255.255.255.0 | 192.168.20.254 | 2001:DB8:ACAD:20::10/64 |
| PC-Student2 | 20   | 192.168.20.11 | 255.255.255.0 | 192.168.20.254 | 2001:DB8:ACAD:20::11/64 |
| PC-Faculty1 | 30   | 192.168.30.10 | 255.255.255.0 | 192.168.30.254 | 2001:DB8:ACAD:30::10/64 |
| PC-Faculty2 | 30   | 192.168.30.11 | 255.255.255.0 | 192.168.30.254 | 2001:DB8:ACAD:30::11/64 |

**Hinweis:** Native VLAN 999 wird für zusätzliche Sicherheit verwendet (Best Practice).

Netzwerkarchitektur

### Physische Verbindungen:

- **MLS (Multi-Layer Switch)**
  - Gi0/1 → S1 Gi0/1 (Trunk mit 802.1Q, Native VLAN 999)
  - Gi0/2 → Internet (Routed Port)
- **S1 (Layer 2 Access Switch)**
  - Gi0/1 → MLS Gi0/1 (Trunk, Native VLAN 99)
  - Access Ports für Endgeräte in verschiedenen VLANs

## Arbeitsauftrag

### Aufgabe 1: Verkabelung

#### 1.1 Physische Verbindungen herstellen

Verkabeln Sie die Geräte gemäß der Topologie:

- MLS Gi0/2 ↔ Internet Router (Copper Straight-Through)
- MLS Gi0/1 ↔ S1 Gi0/1 (Copper Straight-Through - Trunk)
- S1 mit PCs verbinden (6 PCs auf verschiedenen Ports)

## Aufgabe 2: Multi-Layer Switch (MLS) Konfiguration

### 2.1 Grundkonfiguration und Layer 3 aktivieren

```
enable
configure terminal
hostname MLS
no ip domain-lookup

! Layer 3 Routing aktivieren
ip routing
ipv6 unicast-routing
```

#### Erklärung:

- **ip routing**: Aktiviert IP-Routing auf dem Multi-Layer Switch
- **ipv6 unicast-routing**: Aktiviert IPv6-Routing Funktionalität

### 2.2 Trunk-Port zum Access Switch konfigurieren

```
! Trunk-Port zu S1
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
no shutdown
```

#### Erklärung:

- **switchport trunk encapsulation dot1q**: Setzt 802.1Q VLAN-Tagging
- **switchport trunk native vlan 999**: Definiert natives VLAN für ungetaggtten Traffic (Sicherheits-Best-Practice)
- **switchport mode trunk**: Konfiguriert Port als Trunk

### 2.3 Routed Port für Internet-Verbindung

```
! Routed Port zu Internet (Layer 3 Port)
interface GigabitEthernet0/2
no switchport
ip address 209.165.200.225 255.255.255.252
ipv6 address 2001:DB8:ACAD:A::1/64
no shutdown
```

## Erklärung:

- `no switchport`: Konvertiert Switchport zu einem Routed Port (Layer 3)
- Dual-Stack Konfiguration mit IPv4 und IPv6 Adressen

## 2.4 VLANs erstellen

```
! VLANs anlegen
vlan 10
  name Staff
vlan 20
  name Student
vlan 30
  name Faculty
vlan 99
  name Management
vlan 999
  name Native
```

## 2.5 SVIs (Switched Virtual Interfaces) für Inter-VLAN Routing

```
! VLAN 10 - Staff
interface Vlan10
  ip address 192.168.10.254 255.255.255.0
  ipv6 address 2001:DB8:ACAD:10::1/64
  no shutdown

! VLAN 20 - Student
interface Vlan20
  ip address 192.168.20.254 255.255.255.0
  ipv6 address 2001:DB8:ACAD:20::1/64
  no shutdown

! VLAN 30 - Faculty
interface Vlan30
  ip address 192.168.30.254 255.255.255.0
  ipv6 address 2001:DB8:ACAD:30::1/64
  no shutdown

! VLAN 99 - Management
interface Vlan99
  ip address 192.168.99.254 255.255.255.0
  no shutdown

end
write memory
```

**Erklärung:**

- SVIs (Switched Virtual Interfaces) fungieren als Default-Gateways für die VLANs
- Jedes SVI erhält IPv4 und IPv6 Adressen (außer Management VLAN)
- `no shutdown` aktiviert die virtuellen Interfaces

Aufgabe 3: Switch S1 Konfiguration (Layer 2 Access Switch)

**3.1 Grundkonfiguration**

```
enable
configure terminal
hostname S1
no ip domain-lookup
```

**3.2 VLANs erstellen**

```
! VLANs anlegen (müssen auch auf S1 definiert werden)
vlan 10
 name Staff
vlan 20
 name Student
vlan 30
 name Faculty
vlan 99
 name Management
vlan 999
 name Native
```

**3.3 Trunk-Port zum MLS konfigurieren**

```
! Uplink-Trunk zu MLS
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk native vlan 99
 no shutdown
```

**Erklärung:**

- Native VLAN muss auf beiden Seiten des Trunks übereinstimmen
- Bei 2960 Switches ist `switchport trunk encapsulation` nicht notwendig (nur dot1q unterstützt)

**3.4 Access-Ports für Endgeräte konfigurieren**

```
! Access-Ports für Staff (VLAN 10)
interface range FastEthernet0/1-2
switchport mode access
switchport access vlan 10
spanning-tree portfast
no shutdown

! Access-Ports für Students (VLAN 20)
interface range FastEthernet0/3-4
switchport mode access
switchport access vlan 20
spanning-tree portfast
no shutdown

! Access-Ports für Faculty (VLAN 30)
interface range FastEthernet0/5-6
switchport mode access
switchport access vlan 30
spanning-tree portfast
no shutdown

end
write memory
```

## Erklärung:

- `switchport mode access`: Konfiguriert Port als Access-Port
- `switchport access vlan X`: Weist Port einem VLAN zu
- `spanning-tree portfast`: Beschleunigt Port-Aktivierung für Endgeräte

## Aufgabe 4: PC-Konfiguration

### 4.1 PC-Staff1 (VLAN 10)

```
IPv4 Address: 192.168.10.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
IPv6 Address: 2001:DB8:ACAD:10::10/64
IPv6 Gateway: 2001:DB8:ACAD:10::1
```

### 4.2 PC-Staff2 (VLAN 10)

```
IPv4 Address: 192.168.10.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
IPv6 Address: 2001:DB8:ACAD:10::11/64
IPv6 Gateway: 2001:DB8:ACAD:10::1
```

#### 4.3 PC-Student1 (VLAN 20)

```
IPv4 Address: 192.168.20.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.254
IPv6 Address: 2001:DB8:ACAD:20::10/64
IPv6 Gateway: 2001:DB8:ACAD:20::1
```

#### 4.4 PC-Student2 (VLAN 20)

```
IPv4 Address: 192.168.20.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.20.254
IPv6 Address: 2001:DB8:ACAD:20::11/64
IPv6 Gateway: 2001:DB8:ACAD:20::1
```

#### 4.5 PC-Faculty1 (VLAN 30)

```
IPv4 Address: 192.168.30.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.30.254
IPv6 Address: 2001:DB8:ACAD:30::10/64
IPv6 Gateway: 2001:DB8:ACAD:30::1
```

#### 4.6 PC-Faculty2 (VLAN 30)

```
IPv4 Address: 192.168.30.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.30.254
IPv6 Address: 2001:DB8:ACAD:30::11/64
IPv6 Gateway: 2001:DB8:ACAD:30::1
```

### Verifizierung und Tests

Test 1: VLAN-Konfiguration überprüfen

**Auf MLS:**

```
show vlan brief
show ip interface brief
show ipv6 interface brief
```

**Erwartete Ausgabe:**

- Alle VLANs (10, 20, 30, 99, 999) sollten vorhanden sein
- SVIs sollten Status "up/up" haben
- IPv4 und IPv6 Adressen sollten korrekt sein

**Auf S1:**

```
show vlan brief  
show interfaces trunk
```

**Erwartete Ausgabe:**

- Alle VLANs sollten vorhanden sein
- Gi0/1 sollte als Trunk konfiguriert sein
- Native VLAN sollte 99 sein

Test 2: Trunk-Verbindung verifizieren

**Auf S1:**

```
show interfaces GigabitEthernet0/1 switchport  
show interfaces GigabitEthernet0/1 trunk
```

**Erwartete Ausgabe:**

- Administrative Mode: trunk
- Operational Mode: trunk
- Native VLAN: 99

**Auf MLS:**

```
show interfaces GigabitEthernet0/1 switchport  
show interfaces GigabitEthernet0/1 trunk
```

**Erwartete Ausgabe:**

- Administrative Mode: trunk
- Operational Mode: trunk
- Native VLAN: 999
- Encapsulation: 802.1Q

Test 3: IP-Routing Funktionalität

**Auf MLS:**

```
show ip route  
show ipv6 route
```

**Erwartete Ausgabe:**

- Connected Routes für alle VLANs (192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24)
- IPv6 Connected Routes für alle VLANs
- Route zum Internet-Gateway

Test 4: Konnektivität innerhalb eines VLANs (Layer 2)

**Von PC-Staff1:**

```
ping 192.168.10.11  
ping 2001:DB8:ACAD:10::11
```

**Erwartetes Ergebnis:**

- Erfolgreiche Pings zu PC-Staff2 (gleiches VLAN)
- IPv4 und IPv6 Pings sollten funktionieren

Test 5: Inter-VLAN Routing (Layer 3)

**Von PC-Staff1:**

```
ping 192.168.20.10  
ping 192.168.30.10  
ping 2001:DB8:ACAD:20::10  
ping 2001:DB8:ACAD:30::10
```

**Erwartetes Ergebnis:**

- Erfolgreiche Pings zu PCs in anderen VLANs
- Traffic wird über MLS geroutet
- IPv4 und IPv6 funktionieren

Test 6: Gateway-Erreichbarkeit

**Von jedem PC:**

```
ping 192.168.10.254  
ping 192.168.20.254  
ping 192.168.30.254
```

```
ping 2001:DB8:ACAD:10::1
ping 2001:DB8:ACAD:20::1
ping 2001:DB8:ACAD:30::1
```

**Erwartetes Ergebnis:**

- Alle Gateways sollten erreichbar sein

**Test 7: Traceroute zur Analyse des Routing-Pfads****Von PC-Staff1 zu PC-Student1:**

```
tracert 192.168.20.10
```

**Erwartete Ausgabe:**

```
1 192.168.10.254 (MLS VLAN 10 Gateway)
2 192.168.20.10 (PC-Student1)
```

## Troubleshooting

**Problem 1: Keine Konnektivität zwischen VLANs****Mögliche Ursachen:**

1. IP-Routing nicht aktiviert auf MLS
  - Lösung: `ip routing` und `ipv6 unicast-routing` auf MLS konfigurieren
2. SVI nicht aktiviert
  - Lösung: `no shutdown` auf VLAN-Interfaces
3. Falsche Gateway-Konfiguration auf PCs
  - Lösung: Gateway-Adressen auf PCs überprüfen

**Diagnosebefehle:**

```
show ip route
show ip interface brief
show interfaces status
```

**Problem 2: Trunk-Verbindung funktioniert nicht****Mögliche Ursachen:**

1. Native VLAN Mismatch
  - Lösung: Native VLAN auf beiden Seiten des Trunks angleichen
2. Trunk-Modus nicht aktiv

- Lösung: `switchport mode trunk` auf beiden Seiten konfigurieren

#### **Diagnosebefehle:**

```
show interfaces trunk  
show interfaces switchport  
show spanning-tree
```

Problem 3: IPv6 funktioniert nicht

#### **Mögliche Ursachen:**

1. IPv6 Routing nicht aktiviert
  - Lösung: `ipv6 unicast-routing` auf MLS
2. IPv6 Adressen fehlen auf SVIs
  - Lösung: IPv6 Adressen auf VLAN-Interfaces konfigurieren
3. IPv6 auf PCs nicht konfiguriert
  - Lösung: IPv6 Adressen und Gateway auf PCs setzen

#### **Diagnosebefehle:**

```
show ipv6 interface brief  
show ipv6 route  
ping ipv6 <address>
```

Problem 4: PCs im gleichen VLAN können nicht kommunizieren

#### **Mögliche Ursachen:**

1. Port nicht im richtigen VLAN
  - Lösung: `show vlan brief` prüfen, Port neu zuweisen
2. Port im Shutdown-Status
  - Lösung: `no shutdown` auf Port konfigurieren
3. Spanning Tree blockiert Port
  - Lösung: Spanning Tree Status prüfen mit `show spanning-tree`

#### **Diagnosebefehle:**

```
show vlan brief  
show interfaces status  
show mac address-table
```

## Erweiterte Aufgaben (Optional)

Erweiterte Aufgabe 1: Port Security

Konfigurieren Sie Port Security auf den Access-Ports von S1:

- Maximal 2 MAC-Adressen pro Port
- Sticky MAC-Learning
- Violation Mode: restrict

```
interface range FastEthernet0/1-6
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

Erweiterte Aufgabe 2: DHCP Snooping

Aktivieren Sie DHCP Snooping für zusätzliche Sicherheit:

```
! Auf S1
ip dhcp snooping
ip dhcp snooping vlan 10,20,30

! Trust Port zum MLS
interface GigabitEthernet0/1
ip dhcp snooping trust
```

Erweiterte Aufgabe 3: Management-Zugriff konfigurieren

Konfigurieren Sie den Management-Zugriff auf S1:

```
! Management IP auf S1
interface Vlan99
ip address 192.168.99.10 255.255.255.0
no shutdown

! Default Gateway für Management
ip default-gateway 192.168.99.254

! SSH aktivieren
ip domain-name campus.local
crypto key generate rsa modulus 2048
username admin privilege 15 secret Admin123!
line vty 0 15
login local
transport input ssh
```

Erweiterte Aufgabe 4: Access Control Lists (ACLs)

Erstellen Sie eine ACL, um Studenten den Zugriff auf das Staff-Netzwerk zu verbieten:

```
! Auf MLS
ip access-list extended STUDENT_FILTER
deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
permit ip any any

interface Vlan20
 ip access-group STUDENT_FILTER in
```

## Best Practices

### Sicherheit

1.  Separates Native VLAN verwenden (999)
2.  Management VLAN (99) für Switch-Administration
3.  Port Security auf Access-Ports aktivieren
4.  Ungenutzte Ports in eigenes VLAN verschieben und deaktivieren
5.  SSH statt Telnet für Management-Zugriff

### Design

1.  Strukturierte VLAN-Benennung
2.  Logische IP-Adressierung mit /24 Subnetzen
3.  Dual-Stack (IPv4/IPv6) für Zukunftssicherheit
4.  Dokumentation aller Konfigurationen

### Performance

1.  PortFast auf Access-Ports für schnellere Endgeräte-Verbindung
2.  VLAN-Pruning auf Trunk-Ports
3.  Spanning Tree Optimierung

## Zusammenfassung

In dieser Übung haben Sie gelernt:

- Multi-Layer Switch Konfiguration mit Layer 3 Funktionalität
- Inter-VLAN Routing mit SVIs (Switched Virtual Interfaces)
- Dual-Stack Netzwerk mit IPv4 und IPv6
- 802.1Q Trunk-Konfiguration mit Native VLAN
- VLAN-Segmentierung für verschiedene Benutzergruppen
- Systematische Netzwerk-Verifizierung und Troubleshooting
- Sicherheits-Best-Practices für Enterprise-Netzwerke

Diese Konfiguration bietet eine skalierbare, sichere und zukunftssichere Netzwerklösung für moderne Campus-Umgebungen.

# Konfigurationsübersicht (Quick Reference)

## MLS Komplette Konfiguration

```
enable
configure terminal
hostname MLS
no ip domain-lookup
ip routing
ipv6 unicast-routing

interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
no shutdown

interface GigabitEthernet0/2
no switchport
ip address 209.165.200.225 255.255.255.252
ipv6 address 2001:DB8:ACAD:A::1/64
no shutdown

vlan 10
name Staff
vlan 20
name Student
vlan 30
name Faculty
vlan 99
name Management

interface Vlan10
ip address 192.168.10.254 255.255.255.0
ipv6 address 2001:DB8:ACAD:10::1/64
no shutdown

interface Vlan20
ip address 192.168.20.254 255.255.255.0
ipv6 address 2001:DB8:ACAD:20::1/64
no shutdown

interface Vlan30
ip address 192.168.30.254 255.255.255.0
ipv6 address 2001:DB8:ACAD:30::1/64
no shutdown

interface Vlan99
ip address 192.168.99.254 255.255.255.0
no shutdown
```

```
end  
write memory
```

## S1 Komplette Konfiguration

```
enable  
configure terminal  
hostname S1  
no ip domain-lookup  
  
vlan 10  
  name Staff  
vlan 20  
  name Student  
vlan 30  
  name Faculty  
vlan 99  
  name Management  
  
interface GigabitEthernet0/1  
  switchport mode trunk  
  switchport trunk native vlan 99  
  no shutdown  
  
interface range FastEthernet0/1-2  
  switchport mode access  
  switchport access vlan 10  
  spanning-tree portfast  
  no shutdown  
  
interface range FastEthernet0/3-4  
  switchport mode access  
  switchport access vlan 20  
  spanning-tree portfast  
  no shutdown  
  
interface range FastEthernet0/5-6  
  switchport mode access  
  switchport access vlan 30  
  spanning-tree portfast  
  no shutdown  
  
end  
write memory
```

---

**Viel Erfolg bei der Implementierung! 🎉**