

Default Port befehle Cisco CLI im: conf t

TIPP: bei zweifel tabulator drücken

```
interface gi0/1
encapsulation dot1q (Für router )
description xxxx
```

```
switchport mode access / trunk
switchport access vlan 5
switchport trunk allowed vlan
switchport native vlan
```

```
sh ip int brief
sh vlan br
```

Begriffe:

Uplink: Nächster schritt nach oben
Endgeräte > Access-Switches > Core-Switches

Accessport: zu Endgerät (PC)

Trunkport: zu Switch oder Router

Tagged Frames: Dot1Q-Frames mit VLAN-ID.

Untagged Frames: Frames ohne VLAN-ID, verwendet an Access-Ports.

Kupferports (RJ45)

SFP- Ports (**S**mall **F**orm-factor **P**luggable)

WEP: Wired Equivalent Privacy

WPA : Wi-Fi Protected Access

MIB: Management Information Base

OID: Object identifier (MIB Zahl)

GRE : Generic Routing Encapsulation

MPLS: Multiprotocol Labelswitching

MTU : Maximum Transmission Unit

SSID : Service Set Identifier

SNMP-Agent: Software auf einem Netzwerkgerät (Router, Switch) läuft.

SNMP-Trap: Alarmmeldung, die vom SNMP-Agenten an den SNMP-Manager

SNMP-Community: einfacher Klartext-String, der als Passwort dient

- **public** für lesenden (GET).
- **private** für schreibenden (SET).

nano /etc/snmpd.conf

SNMP im FCAPS Modell

ein älteres Modell das den Betrieb eines Netzwerks anhand von fünf Bereichen beschreibt:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

Fault Management ist das Erkennen, Isolieren, Beheben und Protokollieren von im Netz aufgetretenen Fehlern. **Performance** Management sammelt und analysiert Leistungsdaten und will das Netz für die Zukunft vorzubereiten

Wi-Fi Gen	IEEE Standard	Release Date	2.4 GHz	5 GHz	Max Data Rate
Wi-Fi	802.11	1997	Yes	No	2 Mbps
Wi-Fi 1	802.11b	1999	Yes	No	11 Mbps
Wi-Fi 2	802.11a	1999	No	Yes	54 Mbps
Wi-Fi 3	802.11g	2003	Yes	No	54 Mbps
Wi-Fi 4	802.11n	2009	Yes	Yes	600 Mbps
Wi-Fi 5	802.11ac	2013	No	Yes	6.93 Gbps
Wi-Fi 6	802.11ax	2019	Yes	Yes	14 Gbps

1. WPA3 + AES-CCMP/AES-GCMP

2. WPA2 + AES

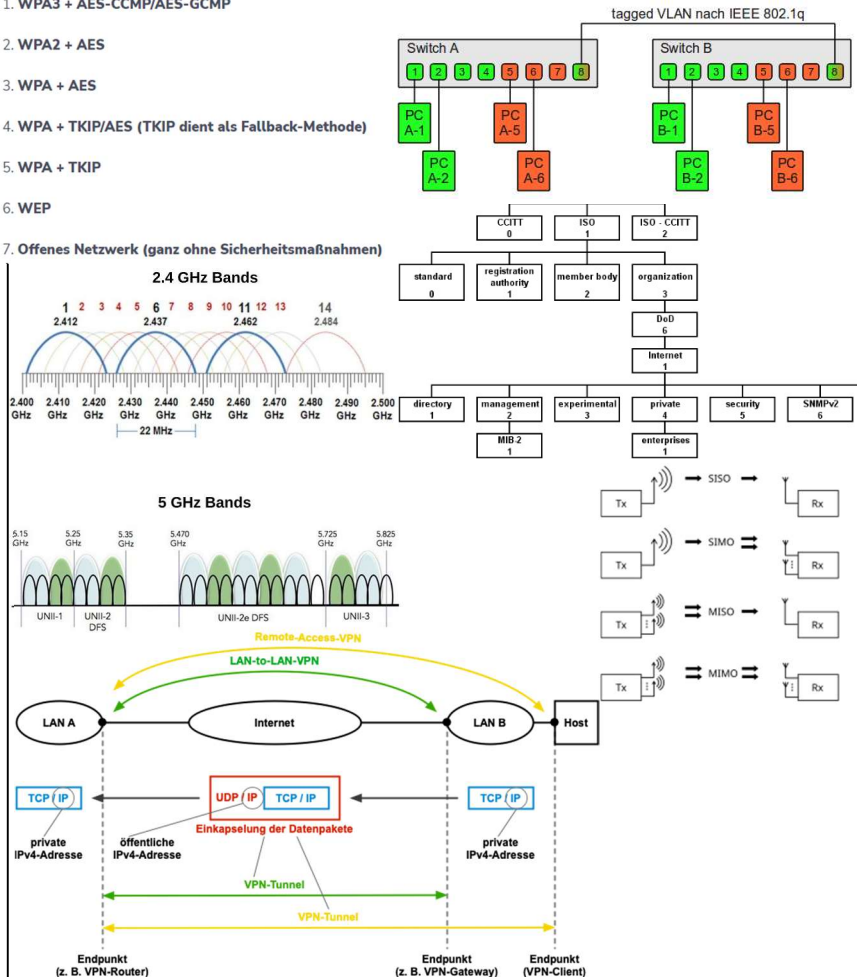
3. WPA + AES

4. WPA + TKIP/AES (TKIP dient als Fallback-Methode)

5. WPA + TKIP

6. WEP

7. Offenes Netzwerk (ganz ohne Sicherheitsmaßnahmen)



5 GHz

Mit rund 380 MHz verfügbarer Bandbreite bietet es erheblich mehr Raum für Übertragungen. Die Kanäle sind überlappungsfrei.

2.4 GHz

Die Bandbreite ist ca. 80 MHz. Die Kanäle überschneiden sind.

VPN-Protokoll	IPsec	L2TP	PPTP	MPLS
OSI-Schicht	3	2	2	2
Standard	Ja	Ja	Nein	Ja
Paketauthentisierung	Ja	Nein	Nein	Nein
Datenverschlüsselung	Ja	Nein	Ja	Nein
IP-Tunneling	Ja	Ja	Ja	Ja
Hauptanwendung	End-to-End	Provider	End-to-End	Netzbetreiber

Feature	SNMPv1	SNMPv2c	SNMPv3
Introduction Year	1988	1993	2002
Authentication	Community strings (plaintext)	Community strings (plaintext)	User-based authentication (USM)
Security	Minimal, vulnerable to attacks	Minimal, vulnerable to attacks	Strong security with encryption
Operations	GET, SET, TRAP	GET, SET, TRAP, GETBULK, INFORM	GET, SET, TRAP, GETBULK, INFORM
Performance	Basic	Improved with GETBULK operation	Improved with GETBULK operation
Access Control	Community strings	Community strings	View-based access control (VACM)
Encryption	None	None	Supports message encryption
Compatibility	Older devices, legacy systems	Commonly supported, better performance	Newer devices, modern networks
Use Case	Small/legacy networks	Networks needing better performance without security needs	Networks requiring strong security
Primary Limitation	Weak security	Weak security	More complex to configure initially

