

## **WLAN Konfiguration**

In diesem Kapitel erfahren Sie

- wie Autonomous APs generell konfiguriert werden
- wie Lightweight APs ihre Konfigurationen automatisch beziehen
- wie WLCs konfiguriert werden
- welche planerischen Überlegungen einer WLAN Implementierung vorausgehen sollten
- wie eine Split-MAC Architecture mit Cisco WLC und Lightweight APs realisiert wird, bzw. wie ein Cisco WLC über GUI (und Kommandozeile) eingestellt werden kann

## Autonomous AP Konfiguration

Die Konfiguration von Autonomous APs kann durch 3 unterschiedliche Methoden erfolgen:

- **IOS CLI** (console, telnet/SSH)
- **WebBrowser** (GUI)
- **Management Software**

Autonomous APs (1100, 1200, 1300) können unterschiedliche Funktionen bereitstellen

- Wireless AP
- Wireless Bridge (root oder non-root), mit oder ohne zusätzlichen Client Access
- Wireless Repeater
- Workgroup Bridge (WDS)
- Scanner

Ein **Autonomous AP** kann jederzeit auf einen **Leightweight AP** umgestellt werden ..  
.. ABER i.d.R. NICHT mehr zurück in den autonomous mode.

Bei der Umstellung eines autonomous AP in den lightweight mode ist weiterhin folgendes zu beachten:

- der umgestellte AP muss eine IP Address erhalten und den WLC ermitteln
- der umgestellte AP unterstützt kein Layer 2 LWAPP
- der umgestellte AP stellt nur noch einen "read-only consolen port" zur Verfügung
- der umgestellte AP kann nur noch mit dem WLC kommunizieren
- die meisten Modelle (ausser 1000 series) stellen nur noch 8 BSSIDs zur Verfügung, d.h. sie unterstützen nur noch 8 WLANs. Nur die WLANs 1 bis 8 werden übernommen.

## Lightweight AP Konfiguration

Ein LAP wird ausschließlich **via WLC administriert**.

Nach erfolgreichem Tunnelaufbau zum WLC ..

.. werden alle notwendigen Einstellungen vom WLC an den LAP via CAPWAP Tunnel übertragen.

Dazu muss der LAP zwingend

- eine **Management IP Adresse** besitzen
- die **IP Adresse des WLC kennen und erreichen können**

Diese Informationen bezieht der LAP i.d.R **via DHCP**, wobei die Anforderungen an den DHCP Server in Abhängigkeit zum Standort des WLC unterschiedlich sind:

- LAP und WLC in der gleichen Broadcast Domain:
  - LAP entdeckt WLC – nach Bezug der IP vom DHCP - über L2 Discovery automatisch
- LAP und WLC in unterschiedlichen Broadcast Domains:
 

Damit der LAP den WLC erreichen kann, muss der DHCP Server

  - mit **Option 43** die IP des des WLCs an die LAPs vergeben
  - mit **Option 60** die VCI – Vendor Class ID des APs angeben (insbesondere für 3700 Series APs) .. NUR wenn APs mit der VCI anfragen, wird die Option 43 verteilt.

Syntax für Option 43:

**option 43 hex** *hex-string*

*hex-string* = Type → "**F1**", Length → **WLC IPs \* 4 in hex**, Value → **IP(s) in hex**

Beispiel:

Parameter für 3702i LAP(s) :

- Mgmt IP aus 10.1.1.0/24 mit Default GW 10.1.1.1
- DNS IP 10.1.1.254
- Ein WLC mit IP 192.168.11.1

DHCP ServerKonfig auf Cisco L3 Switch für LAP 3702i

- Option 60 = **Cisco AP c3700**
- Option 43 = **F104C0A80B0B**  
(Type → **F1**, eine (1) WLC IP → **04**, die WLC IP: 192.168.11.11 → **COA80B0B**)

!

```
ip dhcp pool LAPs
network 10.1.1.0 255.255.255.0
default-router 10.1.1.1
dns-server 10.1.1.254
option 60 ascii "Cisco AP c3700"
option 43 hex F104C0A80B0B
```

!

## LAP Modi

Ein LAP kann über den WLC gesteuert unterschiedliche Funktionen übernehmen.

Dabei kann immer nur eine Funktion ausgeführt werden, multiple Funktionen sind nicht möglich.

Übersicht LAB Modi/Funktionen

(Einstellbarer) Modus	Beschreibung
<b>Modus mit Bereitstellung von BSSs für die Client Anbindung</b>	
<b>Local</b> (default)	Normaler Modus. ACHTUNG: einziger Modus der den Anschluss von Clients ermöglicht.  Transmitting Funktion: → Senden/Empfangen von WLAN Traffic für ein oder multiple BSS (SSIDs) Scanning/Monitoring Funktion: → Messungen von Rauschen und Störungen (noise/interference), Ermittlung anderer SSIDs/APs (rougue devices)
<b>Modi ohne Bereitstellung von BSSs – KEINE Clientanbindung möglich</b>	
<b>Monitor</b>	NUR Scanning/Monitoring – kein Transmitting
<b>FlexConnect</b>	Der LAP übernimmt die die Kommuniation zwischen WLAN und wired LAN – NUR im Falle eines WLC Ausfalls und entsprechender Konfiguration – selbst.
<b>Sniffer</b>	Scanning/Monitoring Funktion optimiert auf Informationsermittlung zu anderen Quellen.  Die Infomationen werden dann an einen PC weitergeleitet, auf dem entsprechende Analysesoftware zur Verfügung steht.
<b>Rougue detector</b>	Scanning/Monitoring Funktion optimiert auf die Erkennung von Rougue Devices.  Rougue Devices sind Geräte der MAC Adresse sowohl im LAN als auch im WLAN auftaucht.
<b>Bridge</b>	Für P2p "Verbindungs"-WLANs (Bridge Mode)  2 LAPs im Bridge Mode → bieten eine P2p "long distance" WLAN Verbindung Multiple LAPs im Bridge Mode → bieten indoor oder outdoor meshed WLAN networks
<b>Flex+Bridge</b>	FlexConnect Mode für LAPs im Bridge Mode
<b>SE-Connect</b>	Scanning/Monitoring Funktion, die Spektralanalysen durchführt.  Diese werden dann auf einem PC mit Tools wie "MetaGeek Channelizer" oder "Cisco Spectrum Expert" gesammelt und stehen für die Ermittlung von Störungen, etc. zur Verfügung

## WLC Konfiguration

Unterschiedliche **Konfigurationsarten** möglich

- **CLI** → via Console Port oder Fernwartung über Management IF (Telnet/SSH)
- **GUI** → via HTTPS und/oder HTTP über Service Port oder Management IF
- **SNMPv1, v2c, v3**
- **Cisco Prime Infrastructure Tools**

WICHTIG:

Ein **WLC** kann, je nach Hardware-Plattform, **maximal 512 WLANs** verwalten.

Ein **LAP** kann **maximal 16 WLANs** verwalten.

Die Anzahl der LAPs pro WLC ist ebenfalls beschränkt und kann z.B. auf der Kommandozeile mit folgendem Kommando ermittelt – und in Abhängigkeit zur Lizenz – auch verändert werden. Informationen zur maximalen Anzahl von APs

> **show ap maximum**

Ein WLC verfügt über eine Reihe von physikalischen Ports und logischen (virtuellen) Interfaces für die Verarbeitung von Management und WLAN Traffic.

## WLC Ports (physikalisch)

- **Console Port**
  - CLI Konfigurationszugang
- **Distribution System Ports**
  - Physikalische Verbindung i.d.R. (gebündelte) dot1q Trunk Verbindung zum Switch
  - die Ports können mit statischer Link Aggregation zu einem logischen Port gebündelt werden (**LAG**)
  - führen intern zu folgenden logischen Interfaces
    - **dynamic interfaces** für WLAN Traffic
    - **management interface** für Management Zugriff und LAP Kommunikation
    - **ap-manager interface** (auf einigen Modellen) für LAP Kommunikation
- **Service Port** .. und zugleich logisches Interface
  - .. nur auf bestimmten Modellen (nicht 2504, 5508)
  - out-of-band management, system recovery
  - unterstützt kein VLAN tagging, daher immer an einen Access Port auf dem Switch anschließen .. oder nur im Bedarfsfall direkt einen Host anschließen
  - der Service Port sollte immer in ein VLAN führen, auf das nur Administratoren zugreifen können
  - der Service Port sollte niemals in ein VLAN führen, das für ein WLAN verwendet wird
  - Default IP: 192.168.1.1/24
  - Zugriff via HTTPS (default)
- **Redundancy Port** .. und zugleich logisches Interface
  - .. nur auf bestimmten Modellen (nicht 2504, 5508)
  - für High-Availability (HA) Umgebungen mit 2 redundanten WLCs
  - verbindet die WLCs physikalisch
  - testet Erreichbarkeit alle 100 ms
  - IP Adresse des Ports immer aus 169.254.0.0/16

## Interfaces (logisch)

- **Dynamic Interfaces**
  - physikalische Anbindung über **distribution port** (i.d.R. Trunk)
  - Multiple IFs möglich – pro WLAN/VLAN eines
  - WLAN ↔ LAN Client Kommunikation
  - Jedes dynamic IF mapped auf ein bestimmtes VLAN ..  
.. jede WLAN SSID mapped dann auf ein bestimmtes dynamic IF
- **Management Interface**
  - physikalische Anbindung über **distribution port** (i.d.R. Trunk)
  - default IF für Remote Administration (CLI oder GUI)
  - ebenfalls verwendet für L3 Kommunikation mit den LAPs (Tunnelendpunkt)  
.. mit "enable dynamic AP Management" (Dynamic AP-Management Option) auch für CAPWAP verwendbar, fall kein AP-Manager IF verfügbar ist
  - einziges IF das "ping-bar" ist
- **AP-Manager Interface**
  - .. nur auf bestimmten Modellen (nicht 2504, 5508)
  - physikalische Anbindung über **distribution ports** (i.d.R. Trunk)
  - Multiple IFs möglich – pro physikalischem Distribution Port einer
  - für differenzierte L3 Kommunikation mit den LAPs (differenzierte Tunnelendpunkte) .. der Tunnelendpunkt wird über eine eigenes AP-Manager IF bereitgestellt anstelle über das gemeinsame Management IF.
  - CAPWAP aktiv
- **Virtual Interface**
  - internes Interface für WLAN Client Support
  - keine physikalische Anbindung
  - .. agiert als DHCP Platzhalter für WLAN Clients, die ihre IP via DHCP beziehen
  - .. redirect address für die Web Authentication Login Page
  - Vergabe einer unbenutzten IP (z.B. aus 192.0.2.0/24 RFC "TEST-NET1") nur für interne Zwecke (nicht ping-bar)
  - Identische IP auf mutliplen WLCs innerhalb einer gleichen mobility group für roaming notwendig

## Übersicht WLC Ports und Interfaces

Port	Interface *obligatorisch	IP Adressierung	Bedeutung
<b>Console</b>	-	-	serieller CLI Zugang
<b>Redundancy</b>		aus 169.254.0.0/16	Optional: Verbindet redundante WLCs
<b>Service</b>		separates "Service" VLAN	Optional: Out-of-band Management via IP
<b>Distribution System</b>	<b>Management*</b>	separates "MGMT" VLAN	Remote Login und CAPWAP Tunnelendpunkt
	<b>AP-Manager</b>	aus MGMT VLAN multiple IPs .. eine pro physik. Port	Optional: differenzierte CAPWAP Tunnelendpunkte
	<b>Dynamic*</b>	multiple separate "WLAN" VLANs mit jeweils einer IP .. pro SSID/WLAN	WLAN ↔ LAN Kommunikation
-	<b>Virtual*</b>	aus 192.0.2.0/24	Interne Funktionen

### Beispiel IP Address Planung WLC 2504

.. nur Consolen Port und Distribution System Ports verfügbar

.. AP-Manager Interface nicht verfügbar

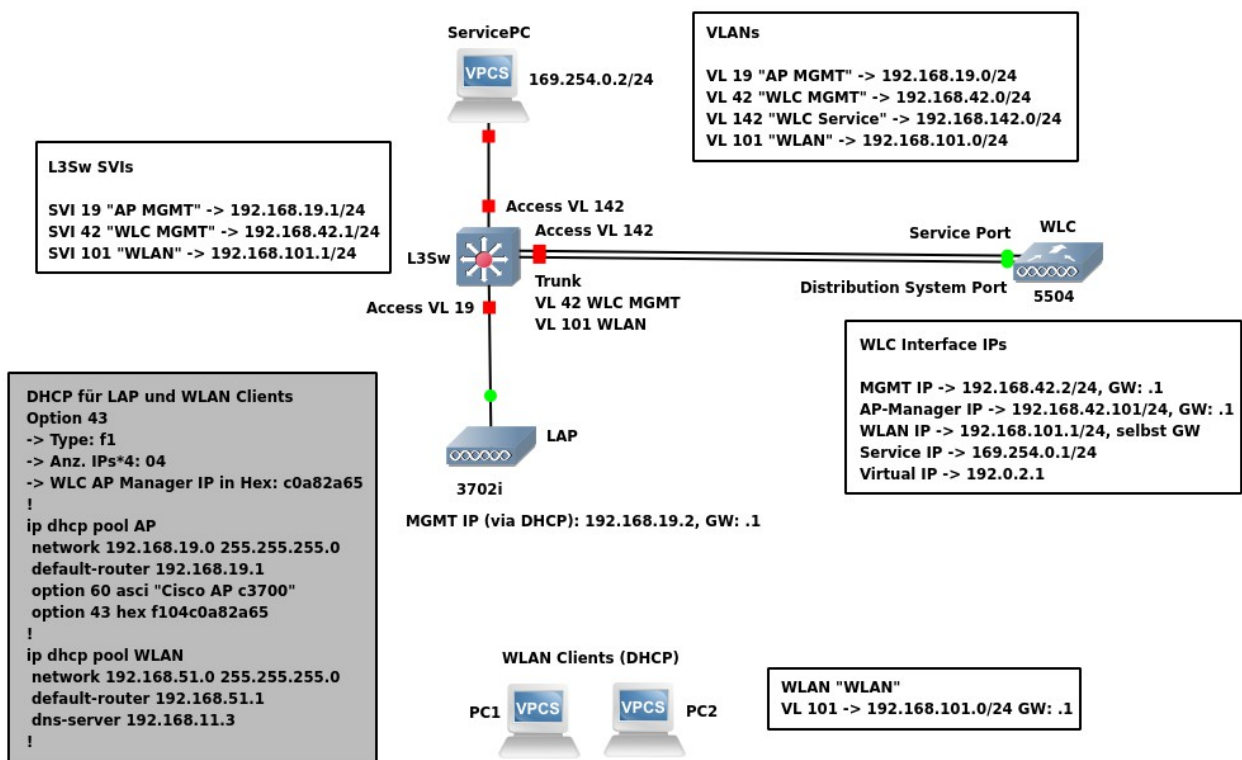
- Obligatorisch
  - **Management Interface** .. via Distribution System Port  
VLAN 42 "WLC MGMT" → 192.168.42.2/24
  - **Dynamic Interface** .. via Distribution System Port  
VLAN 101 "WLAN 1" → 192.168.101.1/24 (GW)
  - **Virtual Interface**  
→ 192.0.2.1/24

## Beispiel IP Address Planung WLC 5504

.. alle Ports und Interfaces verfügbar

- Obligatorisch
  - **Management Interface** .. via Distribution System Port  
VLAN 42 "WLC MGMT" → 192.168.42.2/24
  - **Dynamic Interface** .. via Distribution System Port  
VLAN 101 "WLAN" → 192.168.101.1/24 (GW)
  - **Virtual Interface**  
→ 192.0.2.1/24
- Optional
  - **AP-Manager Interface** .. via Distribution System Port  
→ VLAN 42 "WLC MGMT" → 192.168.42.101/24
  - **Service Interface** .. via Service Port  
→ VLAN 142 "WLC Service" → 192.168.142.42/24
  - **Redundancy Interface** .. zweiter WLC via Redundancy Port  
→ 169.254.0.1/24

.. Topologie – ohne Redundancy Interface





## Praktisches Beispiel – Planung

Praktisches Beispiel für die Konfiguration einer WLAN Split-MAC Architecture mit WLC und LAP.

Notwendige Planung für ..

- benötigte Geräte und Schnittstellen, generell benötigte Dienste (DHCP, NTP)
- benötigte Topologie für LAN/WLAN
- benötigte VLANs und IP Adressplanung: VLANs für WLANs, MGMT VLANs, ..
- mgl. weitere Serverdienste: z.B. Radius (hier nicht vorgesehen)

## Geräte inkl. Interfaces und Funktionen

### WLC 2504

.. mit einem Consolen Port und 4 Distribution System Ports (Service Port und Redundancy Port sind nicht verfügbar).

Es wird nur ein Distribution System Port für den physikalischen Anschluss an den L3 Switch verwendet - kein **LAG**.

Zu konfigurierende L3 Interfaces

- **Managment Interface** (Administrativer Zugriff via SSH, Telnet und HTTP; CAPWAP)
- **Dynamic Interface** (ein WLAN Interface für SSID "moinsen": Übergang WLAN ↔ LAN)
- **Virtual Interface** (obligatorisch – aber NUR interne Bedeutung)

### LAP 3702i

Dynamisches L3 Interface

- **Management Interface** (Kommunikation mit WLC) ..  
.. IP Adressbezug via – bereitzustellendem – DHCP Server mit Option 43 und 60, da LAP und WLC in unterschiedlichen BC Domains geplant

HINWEIS: der LAP wird nicht konfiguriert, sondern nur korrekt ans Netzwerk angeschlossen. Nach Boot holt sich der LAP eine IP und notwendige IP Informationen wie die IP des WLC vom DHCP Server. Anschließend wird der WLC kontaktiert und alle notwendigen Softwarekomponenten (z.B. aktuelles Image, Einstellungen) automatisch vom WLC bezogen.

### c3650 L3 Switch

Gateway und DHCP Server

Zu konfigurierende L3 Interfaces

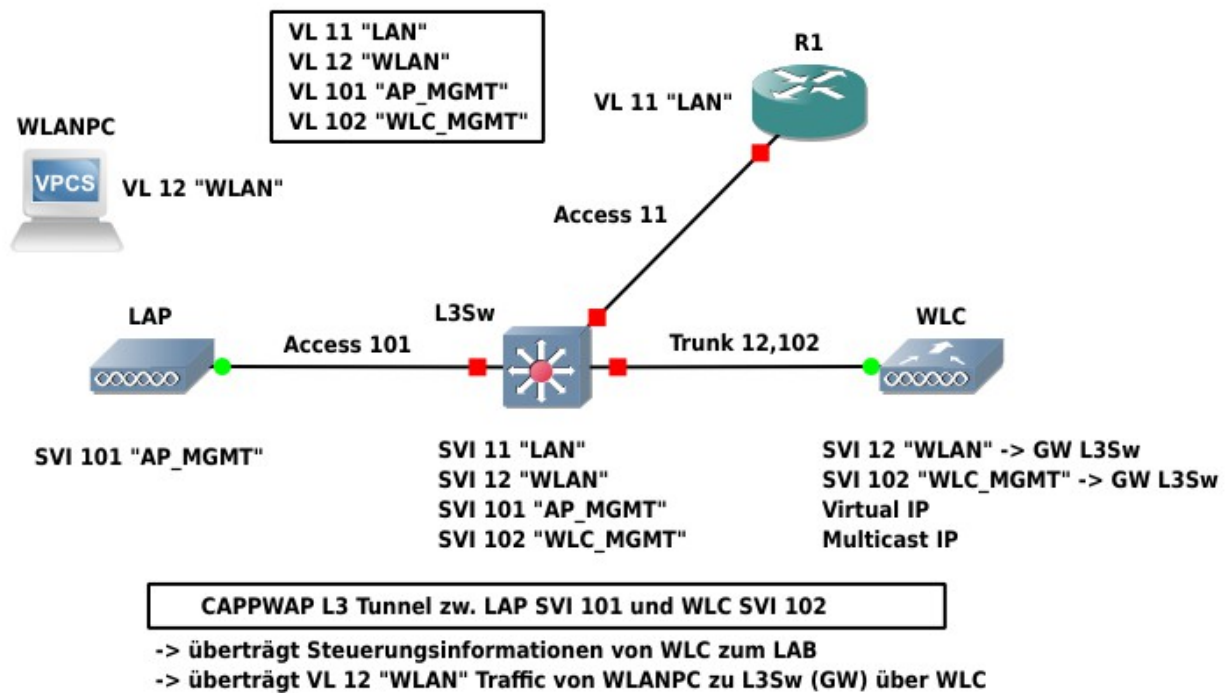
- **Gateway für WLC Management Interface**
- **Gateway für LAP Management Interface**
- **Gateway für WLAN → Übergang ins "wired" LAN**
- **Gateway für LAN → Übergang ins WLAN**

Zu konfigurierende Dienste:

- DHCP für LAP (inkl. Option 43 und Option 60)
- DHCP für WLAN Client-PCs
- Optional: NTP Serverdienst

## Topologie

BSS (auf ESS mit Distribution System erweiterbar) mit Split-MAC Architektur



## IP Adressierung

**VL 11 "LAN" → 192.168.11.0/24**

- L3Sw → .1
- Router → .254

**VL 12 "WLAN" → 192.168.12.0/24**

- L3Sw → .1
- WLC → .2
- WLANPC → via DHCP

**VL 101 "AP\_MGMT" → 10.1.1.0/30**

- L3Sw → .1
- AP → .2 (CAPWAP Tunnelendpunkt)

**VL 102 "WLC\_MGMT" → 10.1.1.4/30**

- L3Sw → .5
- WLC → .6 .. via DHCP (CAPWAP Tunnelendpunkt)

## Praktisches Beispiel – L3 Switch Konfiguration

### VLANs, Trunks, Access Ports

```
!  
vlan 11  
  name LAN  
vlan 12  
  name WLAN  
vlan 101  
  name AP_MGMT  
vlan 102  
  name WLC_MGMT  
!  
interface gi 0/1  
  description ROUTER  
  switchport mode access  
  switchport access vlan 11  
!  
interface gi 0/2  
  description WLC  
  switchport mode trunk  
  switchport trunk allowed vlan 12,102  
!  
interface gi 0/3  
  description AP  
  switchport mode access  
  switchport access svlan 101  
!
```

### Routing und SVI IP Adressierung

```
!  
ip routing  
!  
interface vlan 11  
  description LAN  
  ip address 192.168.11.1 255.255.255.0  
!  
interface vlan 12  
  description WLAN (GW)  
  ip address 192.168.12.1 255.255.255.0  
!  
interface vlan 101  
  description AP (GW)  
  ip address 10.1.1.1 255.255.255.252  
!  
interface vlan 102  
  description WLC (GW)  
  ip address 10.1.1.5 255.255.255.252  
!
```

**DHCP für WLAN und AP\_MGMT**

Option 43 und 60 notwendig für LAP.

## Option 43

- Type → f1
- Anz. IPs\*4 → 04
- WLC IP: 10.1.1.6 → 0a010106

## Option 60

- Vendor ID

```
!
ip dhcp excluded-address 10.1.1.1
ip dhcp excluded-address 192.168.12.1 192.168.21.99
!
ip dhcp pool AP
 network 10.1.1.0 255.255.255.252
 default-router 10.1.1.1
 option 60 ascii "Cisco AP c3700"
 option 43 hex f104.0a01.01026
!
ip dhcp pool WLAN
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 192.168.11.254
!
```

**NTP**

Im Beispiel ist der Switch daselbst der Server .. alternativ kann ein beliebiger NTP Server verwendet werden.

```
!
ntp master
!
clock timezone CET 1
clock summer-time CEST recurring last sunday march 02:00 last sunday october 03:00
service timestamps log datetime localtime msec
service timestamps debug datetime localtime msec
!
```

## Praktisches Beispiel – WLC Konfiguration

### Überblick Allgemeine Arbeitsschritte

1. **Zurücksetzen des Gerätes** bei ersten Boot ..  
.. durch Eingabe von **Recover-Config** am User Prompt
2. Verwendung des **Configuration Wizard** zur initialen Konfiguration (empfohlen)  
Dabei werden folgende Konfigurationen – nach Planung - vorgenommen:
  - **Hostname** → WLC
  - **Login User / Passwort** → admin / cisco
  - Optional: **LAG** → .. Link Aggregation hier nicht geplant
  - **Management IF** → IP 10.1.1.6, GW L3Sw 10.1.1.5, VLAN ID 102, ..
  - **Virtual IF IP** → 192.0.2.1 (reservierte IPv4 Unicast - empfohlen)
  - **Multicast IP** → 239.1.1.1 (private IPv4 Multicast – empfohlen)
  - **Mobility** → Mobility Group Name (beliebig wählbar)
  - **WLAN** → SSID "moinsen", Distribution Port, CountryCode "DE"
  - Optional: **Radius** → .. hier nicht geplant
  - **802.11 Standards** → alle aktivieren
  - **NTP** → Server: L3Sw 10.1.1.5
  - Optional: **IPv6** → .. hier nicht geplant
3. Weitere notwendige Einstellungen werden via Kommandozeile (Console oder SSH) oder GUI (HTTP oder HTTPS) vorgenommen:
  - **Dynamic Interface**  
.. hier: Anbindung des WLANs über Distribution Port mit L3Sw als GW
  - **WLAN Security**  
.. hier: WPA2 PSK "personal"  
.. alternativ: **Radius EAP und** WPA2 "enterprise"
  - Optional (sinnvoll): **QoS**

## Zurücksetzen des Geräts

.. beim ersten Boot, durch Eingabe von Recover-Config am User: Prompt.

```
Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)
```

```
User: Recover-Config
```

```
Initiating system recovery process... please wait
```

```
Writing to flash ...done
```

```
Rebooting system
```

## Wizard

```
Welcome to the Cisco Wizard Configuration Tool
```

```
Use the '-' character to backup
```

```
Would you like to terminate autoinstall? [yes]:
```

```
System Name [Cisco_b3:0b:65] (31 characters max): WLC
```

```
Enter Administrative User Name (24 characters max): admin
```

```
Enter Administrative Password (3 to 24 characters): cisco
```

```
Re-enter Administrative Password : cisco
```

```
Enable Link Aggregation (LAG) [yes][NO]: no
```

```
Management Interface IP Address: 10.1.1.6
```

```
Management Interface Netmask: 255.255.255.252
```

```
Management Interface Default Router: 10.1.1.5
```

```
Cleaning up Provisioning SSID
```

```
Management Interface VLAN Identifier (0 = untagged): 102
```

```
Management Interface Port Num [1 to 4]: 1
```

```
Management Interface DHCP Server IP Address: 10.1.1.5
```

```
Virtual Gateway IP Address: 192.0.2.1
```

```
Multicast IP Address: 239.1.1.1
```

```
Mobility/RF Group Name: myRF
```

```
Network Name (SSID): moinsen
```

```
Configure DHCP Bridging Mode [yes][NO]: no
```

```
Allow Static IP Addresses [YES][no]: no
```

```
Configure a RADIUS Server now? [YES][no]: no
```

```
Warning! The default WLAN security policy requires a RADIUS server.
```

```
Please see documentation for more details.
```

```
Enter Country Code list (enter 'help' for a list of countries) [US]: DE
```

```
Enable 802.11b Network [YES][no]: yes
```

```
Enable 802.11a Network [YES][no]: yes
```

```
Enable 802.11g Network [YES][no]: yes
```

```
Enable Auto-RF [YES][no]: yes
```

```
Configure a NTP server now? [YES][no]: yes
```

```
Enter the NTP server's IP address: 10.1.1.5
```

```
Enter a polling interval between 3600 and 604800 secs: 36000
```

```
Would you like to configure IPv6 parameters[YES][no]: no
```

```
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

## GUI - Weitere Einstellungen

.. CCNA relevant

Nachdem mit dem Configuration Wizard die elementaren Einstellungen für den WLC vorgenommen wurden, können jetzt weitere notwendige Einstellungen über die GUI vorgenommen werden:

- Optional: **RADIUS**
- **WLAN Security**
- **WLAN Qos**
- **Dynamic Interface** .. einem WLAN zuordnen

Der WLC GUI ist über die Management Interface IP Adresse via HTTP bzw. HTTPS erreichbar, was natürlich auch über die GUI angepasst werden kann:

- <http://WLC-IP>
- <https://WLC-IP>

Nach erfolgreichem Login mit Username und Passwort wird das Dashboard angezeigt.

The screenshot displays the Cisco 2500 Series Wireless Controller GUI. The browser address bar shows the URL `192.168.21.2/screens/dashboard.html#/MainDashboard`. The dashboard features a left-hand navigation menu with options like 'Monitoring', 'Network Summary', 'Access Points', 'Clients', 'Wireless Dashboard', 'AP Performance', 'Client Performance', and 'Best Practices'. The main content area is titled 'NETWORK SUMMARY' and contains several key performance indicators (KPIs):

Wireless Networks	Access Points	Active Clients	Rogues	Interferers
1	1	0	50 APs 0 Clients	0

Below the KPIs, there are two main sections: 'ACCESS POINTS BY USAGE' which shows a donut chart for a specific AP (AP00fe.c8fd.6db4), and 'OPERATING SYSTEMS' which currently shows a warning icon.

Über den Link "advanced" oben rechts gelangt man vom Dashboard auf die Oberfläche zur Administration des WLC.

Zum Dashboard zurück gelangt man von der "advanced" Oberfläche wieder über den Link "Home" oben rechts.

## Advanced

6 Access Points Supported

Controller Summary

Management IP Address	192.168.21.2, ::/128
Software Version	8.3.111.0
Field Recovery Image Version	1.0.0
System Name	WLC
Up Time	0 days, 1 hours, 11 minutes
System Time	Sat Jun 27 10:14:45 2020
Redundancy Mode	N/A
Internal Temperature	+32 C
802.11a Network State	Enabled

Rogue Summary

Active Rogue APs	50	<a href="#">Detail</a>
Active Rogue Clients	0	<a href="#">Detail</a>
Adhoc Rogues	0	<a href="#">Detail</a>
Rogues on Wired Network	0	

Session Timeout

Top WLANs

Profile Name	# of Clients

Most Recent Traps

Rogue AP : 74:6f:f7:96:1b:31 removed from Base Radio MAC : 00:f2:8b:40:ac:c0 Interface no:0(802.11n(2.4 GHz))

Startseite der "advanced" Oberfläche ist das Monitoring (MONITOR Reiter orange unterlegt). Über die Navigation links können detaillierte Informationen abgerufen werden.

Über die weiteren Reiter WLANs, CONTROLLER, etc. können Einstellungen für den WLC vorgenommen werden. So können über den Reiter MANAGEMENT u.a. Einstellungen für Telnet, SSH, HTTP/HTTPS Zugang auf den WLC angepasst werden.

Management Summary

SNMP Protocols	v1:Disabled v2c:Enabled v3:Enabled
Syslog	Disabled
HTTP Mode	Enabled
HTTPS Mode	Enabled
New Telnet Sessions Allowed	No
New SSH Sessions Allowed	Yes
Management via Wireless	Enabled



## GUI - RADIUS

Über den Reiter SECURITY und die linke Navigation RADIUS → Authentication gelangt man auf die folgende Seite.

The screenshot shows the Cisco WLC GUI interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY' (highlighted), 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows a tree view under 'Security' with 'RADIUS' expanded to 'Authentication'. The main content area is titled 'RADIUS Authentication Servers' and contains the following configuration options:

- Auth Called Station ID Type: AP MAC Address:SSID
- Use AES Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- MAC Delimiter: Hyphen
- Framed MTU: 1300

Below these options is a table with columns: Network User, Management, Server Index, Server Address(Ipv4/Ipv6), Port, IPsec, and Admin Status. The table is currently empty. At the top right of the configuration area are 'Apply' and 'New...' buttons.

Über den Button "New" rechts oben kann man einen neuen Radius Server einrichten.

The screenshot shows the 'New' configuration page for a RADIUS Authentication Server. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration options:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 10.10.10.10
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Disabled
- Server Timeout: 2 seconds
- Network User Management:  Enable
- Management:  Enable
- Management Retransmit Timeout: 2 seconds
- IPsec:  Enable

At the top right of the configuration area are '< Back' and 'Apply' buttons.

## GUI - WLAN inkl. Security und QoS

Bei der elementaren Konfiguration des WLC ist bereits ein WLAN eingerichtet worden. Über die GUI können zusätzliche Einstellungen für das WLAN festgelegt werden, aber ebenfalls neue WLANs definiert oder alte gelöscht werden. Über den Reiter WLAN gelangt man auf die entsprechende Seite.

The screenshot shows the Cisco WLC GUI with the 'WLANs' tab selected. The page title is 'WLANs' and it shows 'Entries 1 - 1 of 1'. A table lists the existing WLAN configuration:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	tachauch-II	tachauch-II	Enabled	[WPA2][Auth(PSK)]

Das bereits angelegte WLAN wird angezeigt und kann mit einem Klick auf den WLAN ID editiert werden. Der Punkt Interface/Interface Group(G) ist auf die VLAN ID des WLAN einzustellen.

The screenshot shows the Cisco WLC GUI with the 'WLANs > Edit 'tachauch-II'' configuration page. The 'General' tab is selected, and the following configuration options are visible:

- Profile Name: tachauch-II
- Type: WLAN
- SSID: tachauch-II
- Status:  Enabled
- Security Policies: [WPA2][Auth(PSK)]  
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): management
- Multicast Vlan Feature:  Enabled
- Broadcast SSID:  Enabled
- NAS-ID: none

**Foot Notes**

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
- 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

Innerhalb des "WLAN edit" Fenster kann man über die Reiter Security die Entsprechenden Einstellung für die WLAN Sicherheit vornehmen.

In diesem Beispiel wurde WPA2 mit PSK und AES Verschlüsselung als Layer 2 Security eingestellt.

Mit einem Klick auf "Apply" oben rechts werden die Einstellungen übernommen.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'tachauch-II'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' is set to 'WPA+WPA2'. The 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. The 'PSK Format' is set to 'ASCII'. The 'Apply' button is visible in the top right corner.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'tachauch-II'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' is set to 'WPA+WPA2'. The 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. The 'PSK Format' is set to 'ASCII'. The 'Apply' button is visible in the top right corner.

Über den Reiter "AAA Servers" können – falls anstelle einer PSK Authentifizierung eine Authentifizierung über dot1x eingestellt wurde – Einstellungen zum zu verwendenden Radius Server vorgenommen werden.

WLANs > Edit 'tachauch-II'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**

RADIUS Server Overwrite interface  Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

**RADIUS Server Accounting**

**Foot Notes**

1 Web Policy cannot be used in combination with IPsec  
 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

Über den Reiter "QoS" sind Einstellungen für Quality of Service möglich. Platinum = voice, Gold = video, Silver = best effort, Bronze = backgrounds

WLANs > Edit 'tachauch-II'

General Security QoS Policy-Mapping Advanced

Quality of Service (QoS) Silver (best effort)

Application Visibility  Enabled

AVC Profile none

Netflow Monitor none

Fastlane Disable

**WMM**

WMM Policy Allowed

7920 AP CAC  Enabled

7920 Client CAC  Enabled

**Foot Notes**

1 Web Policy cannot be used in combination with IPsec  
 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs  
 2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS

## GUI - Dynamic Interface(s)

Neben den weiteren Einstellungen für das WLAN ist noch die Konfiguration von mindestens einem dynamic Interface für die Funktionalität eines WLAN erforderlich. Über den Reiter "CONTROLLER" gelangt man auf die dafür vorgesehen Seiten der GUI.

The screenshot shows the Cisco WLC GUI configuration page for the 'CONTROLLER' section. The 'General' tab is selected, and the configuration is for a device named 'WLC'. The left sidebar shows a navigation menu with 'Interfaces' highlighted. The main content area shows various configuration options for the controller, including Name, 802.3x Flow Control Mode, LAG Mode, Broadcast Forwarding, AP Multicast Mode, AP IPv6 Multicast Mode, AP Fallback, CAPWAP Preferred Mode, Fast SSID change, Link Local Bridging, Default Mobility Domain Name, RF Group Name, User Idle Timeout, ARP Timeout, Web Radius Authentication, Operating Environment, Internal Temp Alarm Limits, and WebAuth Proxy Redirection Mode.

Im linken Navigationsmenü wird dann "Interfaces" gewählt. Dieser Link zeigt alle bereits konfigurierten Interfaces .. im Beispiel existiert neben management und virtual IF bereits ein dynamic IF mit der Bezeichnung "wlan51". Ein neues IF wird mit "New" rechts oben angelegt.

The screenshot shows the Cisco WLC GUI configuration page for the 'CONTROLLER' section, specifically the 'Interfaces' tab. The left sidebar shows a navigation menu with 'Interfaces' highlighted. The main content area displays a table of configured interfaces. The table has the following columns: Interface Name, VLAN Identifier, IP Address, Interface Type, Dynamic AP Management, and IPv6 Address. The table lists three interfaces: 'management', 'virtual', and 'wlan51'.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
<a href="#">management</a>	21	192.168.21.2	Static	Enabled	::/128
<a href="#">virtual</a>	N/A	192.0.2.1	Static	Not Supported	
<a href="#">wlan51</a>	51	192.168.51.2	Dynamic	Disabled	

Mit Klick auf den Interfaces Namen oder nach Klick auf "New" wird die Seite mit den Interface Einstellungen angezeigt .. Hier werden die bereits gesetzten Parameter für das bereits existente dynamic IF "wlan51" angezeigt.

Wichtigste, notwendig Parameter, die bei einem neuen IF zu setzen sind:  
VLAN ID, IP Adresse, Netzmaske, Default GW und DHCP Server IP.

Controller Interfaces > Edit

**General Information**

Interface Name wlan51  
MAC Address 84:78:ac:b3:0b:64

**Configuration**

Guest Lan   
Quarantine   
Quarantine Vlan Id 0  
NAS-ID none

**Physical Information**

Port Number 1  
Backup Port 0  
Active Port 1  
Enable Dynamic AP Management

**Interface Address**

VLAN Identifier 51  
IP Address 192.168.51.2

Controller

VLAN Identifier 51  
IP Address 192.168.51.2  
Netmask 255.255.255.0  
Gateway 192.168.51.1

**DHCP Information**

Primary DHCP Server 192.168.51.1  
Secondary DHCP Server  
DHCP Proxy Mode Global  
Enable DHCP Option 82

**Access Control List**

ACL Name none  
URL ACL none

**mDNS**

mDNS Profile none

**External Module**

3G VLAN

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Nach Konfiguration des dynamic IF ist das WLAN funktional.  
Die Konfiguration des WLC kann jetzt mit "Save Configuration" ganz oben rechts gesichert werden.

## Selbstkontrolle – Aufgaben und Übungen

1. Welche der folgenden Aussagen zum Anschluss der angeführten Geräte an das wired LAN (via L2/L3) Switch sind korrekt?

- Ein Autonomous AP wird an einen access port angeschlossen
- Ein Autonomous AP wird an einen trunk port angeschlossen
- Ein LAP wird an einen access port angeschlossen
- Ein LAP wird an einen trunk port angeschlossen
- Ein WLC wird an einen access port angeschlossen
- Ein WLC wird an einen trunk port angeschlossen

2. Welche der folgenden Methoden bzw. Verbindungsmöglichkeiten stehen zur Administration eines WLC zur Verfügung?

- Console
- VNC
- SSH
- HTTP/HTTPs
- Telnet
- LLDP
- CDP
- SNMP

3. Auf einem WLC ist es möglich, alle physikalischen Distribution System Ports zu einem logischen Port zu bündeln. Wie heißt dieses Feature?

- EtherChannel
- PAgP
- LACP
- LAG

4. In welchem Modus muss ein LAP eingestellt sein, damit er WLAN Konnektivität für Clients bereitstellen kann?

- bridge
- local
- monitor
- sniffer

5. Welche Parameter werden einem LAP durch einen existenten DHCP Server bereitgestellt, wenn sich der WLC in einem anderen Subnetz befindet.

- IP Adresse und Subnetzmaske
- SSID
- IP Adresse des Default Gateways
- IP Adresse des WLC
- BSSID
- IP Adresse des Radius Servers

6. Über welchen der folgenden Ports eines WLC fließt CAPWAP Management Datenverkehr mit dem LAP?

- Console
- Distribution System
- Service
- Redundanc

7. Welcher der folgende Ports eines WLC wird für den ersten Konfigurationszugang genutzt?

- Console
- Distribution System
- Service
- Redundancy

8. Welcher der folgenden Ports eines WLC wird auf dem WLC verwendet, wenn ein Administrator eine SSH Verbindung zum WLC aufgebaut hat?

- Console
- Distribution System
- Service
- Redundancy

9. Welche der folgenden WLC Interfaces müssen IMMER mit einer IP Adresse konfiguriert werden, damit Geräte innerhalb eines WLAN mit dem wired LAN kommunizieren können?

- Dynamic
- Management
- AP Manager
- Virtual
- Service
- Redundancy

10. Welches der folgenden Interfaces auf einem WLC hat keine physikalische Anbindung?

- Dynamic
- Management
- AP-Manager
- Virtual

11. Welche der folgenden Parameter können bzw. werden auf einem WLC durch den Configuration Wizard eingestellt?

- System Name (Hostname)
- Administrator Passwort
- IP Adresse für ein Dynamic Interface
- LAG
- 802.1x Standards
- IP Adresse für das Virtual Interface
- QoS
- 802.11 Standards
- WLAN Security (WPA2/WPA3)
- IP Adresse für das Management Interface



12. Der Administrator eines Netzwerks möchte eine WLAN mit 802.1x EAP Authentication verwenden. Welche der folgenden Einstellungen sind – nach den alle grundlegenden Einstellungen über den Wizard vorgenommen wurden – notwendig, damit Geräte innerhalb eines WLAN kommunizieren können.

- Dynamic Interface
- WLAN Security
- LAG
- SSID

13. Auf welche Art und Weise wird i.d.R. ein LAP konfiguriert?

- CLI
- GUI (eine CLI steht nicht zur Verfügung)
- Ein LAP wird ausschließlich über den WLC gesteuert
- Ein LAP bezieht seine IP Informationen von einem lokalen DHCP und wird dann über den WLC gesteuert

14. Auf welche Art und Weise wird i.d.R. ein Autonomous AP konfiguriert?

- CLI (eine GUI steht nicht zur Verfügung)
- GUI
- Ein Autonomous AP wird ausschließlich über den WLC gesteuert
- Ein Autonomous bezieht seine IP Informationen von einem lokalen DHCP und wird dann über den WLC gesteuert

## Selbstkontrolle – Lösungen

1. Welche der folgenden Aussagen zum Anschluss der angeführten Geräte an das wired LAN (via L2/L3) Switch sind korrekt?

- Ein Autonomous AP wird an einen access port angeschlossen
- Ein Autonomous AP wird an einen trunk port angeschlossen
- Ein LAP wird an einen access port angeschlossen
- Ein LAP wird an einen trunk port angeschlossen
- Ein WLC wird an einen access port angeschlossen
- Ein WLC wird an einen trunk port angeschlossen

2. Welche der folgenden Methoden bzw. Verbindungsmöglichkeiten stehen zur Administration eines WLC zur Verfügung?

- Console
- VNC
- SSH
- HTTP/HTTPs
- Telnet
- LLDP
- CDP
- SNMP

3. Auf einem WLC ist es möglich, alle physikalischen Distribution System Ports zu einem logischen Port zu bündeln. Wie heißt dieses Feature?

- EtherChannel
- PAgP
- LACP
- LAG

4. In welchem Modus muss ein LAP eingestellt sein, damit er WLAN Konnektivität für Clients bereitstellen kann?

- bridge
- local
- monitor
- sniffer

5. Welche Parameter werden einem LAP durch einen existenten DHCP Server bereitgestellt, wenn sich der WLC in einem anderen Subnetz befindet.

- IP Adresse und Subnetzmaske
- SSID
- IP Adresse des Default Gateways
- IP Adresse des WLC
- BSSID
- IP Adresse des Radius Servers

6. Über welchen der folgenden Ports eines WLC fließt CAPWAP Management Datenverkehr mit dem LAP?

- Console
- Distribution System
- Service
- Redundanc

7. Welcher der folgende Ports eines WLC wird für den ersten Konfigurationszugang genutzt?

- Console
- Distribution System
- Service
- Redundancy

8. Welcher der folgenden Ports eines WLC wird auf dem WLC verwendet, wenn ein Administrator eine SSH Verbindung zum WLC aufgebaut hat?

- Console
- Distribution System
- Service
- Redundancy

9. Welche der folgenden WLC Interfaces müssen IMMER mit einer IP Adresse konfiguriert werden, damit Geräte innerhalb eines WLAN mit dem wired LAN kommunizieren können?

- Dynamic
- Management
- AP Manager
- Virtual
- Service
- Redundancy

10. Welches der folgenden Interfaces auf einem WLC hat keine physikalische Anbindung?

- Dynamic
- Management
- AP-Manager
- Virtual

11. Welche der folgenden Parameter können bzw. werden auf einem WLC durch den Configuration Wizard eingestellt?

- System Name (Hostname)
- Administrator Passwort
- IP Adresse für ein Dynamic Interface
- LAG
- 802.1x Standards
- IP Adresse für das Virtual Interface
- QoS
- 802.11 Standards
- WLAN Security (WPA2/WPA3)
- IP Adresse für das Management Interface

12. Der Administrator eines Netzwerks möchte eine WLAN mit 802.1x EAP Authentication verwenden. Welche der folgenden Einstellungen sind – nach den alle grundlegenden Einstellungen über den Wizard vorgenommen wurden – notwendig, damit Geräte innerhalb eines WLAN kommunizieren können.

- Dynamic Interface
- WLAN Security
- LAG
- SSID

13. Auf welche Art und Weise wird i.d.R. ein LAP konfiguriert?

- CLI
- GUI (eine CLI steht nicht zur Verfügung)
- Ein LAP wird ausschließlich über den WLC gesteuert
- Ein LAP bezieht seine IP Informationen von einem lokalen DHCP und wird dann über den WLC gesteuert

14. Auf welche Art und Weise wird i.d.R. ein Autonomous AP konfiguriert?

- CLI (eine GUI steht nicht zur Verfügung)
- GUI
- Ein Autonomous AP wird ausschließlich über den WLC gesteuert
- Ein Autonomous bezieht seine IP Informationen von einem lokalen DHCP und wird dann über den WLC gesteuert