



Titel: Labor06 – LACP, WPA2-E, Port-Sec.

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 15.12.2020 Abgabe: 12.01.2021

Inhaltsverzeichnis

1	Theorie-Teil	1
1.1	Etherchannel.....	1
1.1.1	Allgemeines Etherchannel	1
1.1.2	Benefits of Etherchannel.....	1
1.2	RADIUS / 802.1x.....	2
1.2.1	Overview	2
1.2.2	Auth-Process	2
2	Etherchannel	4
2.1	Konfigurieren von LACP	4
2.1.1	Am Core-Switch für Port Fa0/1-2 (linker Switch)	4
2.1.2	Konfiguration am Core-Switch für Port Fa0/3-4 (rechter Switch).....	5
2.1.3	Konfigurieren von linkem Switch (D1)	5
2.2	Konfigurieren von rechtem Switch (D2)	6
2.3	Informationen anzeigen	6
2.4	Stellen Sie sicher, dass der Core-Switch die Root-Bridge ist.	7
2.5	DHCP einschalten am Router (192.168.6.0/24).....	8
3	Port-Security.....	9
3.1	Konfigurieren Sie auf den Access Ports Portsecuritydamit sich jeweils nur ein Client (eine MAC Adresse) verbinden darf. Testen Sie die statische und die dynamische Variante.	9
3.1.1	Statische Variante	9
3.1.2	Dynamisch.....	12
3.2	Welche Befehle stehen zur Verfügung um den Zustand der Ports zu überprüfen?	14
3.2.1	Show port-security	14
3.2.2	Show port-sec address.....	15
3.2.3	Show port-sec in x/x	16
3.2.4	Show mac address-table	16
4	WPA2-Enterprise	17
4.1	Aufbau	17
4.2	Router0 einrichten.....	17
4.3	DHCP Server am Router anschalten	17
4.4	RADIUS am Server einrichten	18
4.5	Den Wireless-Router einrichten	19
4.6	Konfiguration der Laptops	19
4.6.1	Laptop0.....	19
4.7	Legen sie am Radiusserver mehrere User an und testen sie die Anmeldung	20
4.7.1	Angepasstes Modell.....	21
4.7.2	Testen des Users niklas2 mit Laptop1.....	21
4.7.3	Testen des Users niklas3 mit Laptop2.....	22

1 Theorie-Teil

<https://en.wikipedia.org/wiki/EtherChannel>

1.1 Etherchannel

1.1.1 Allgemeines Etherchannel

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. An EtherChannel can be created from between two and eight active Fast, Gigabit or 10-Gigabit Ethernet ports, with an additional one to eight inactive (failover) ports which become active as the other active ports fail. EtherChannel is primarily used in the backbone network, but can also be used to connect end user machines.

EtherChannel technology was invented by Kalpana and conceptualized by Kalpana employee Scott Childs in the early 1990s. It was later acquired by Cisco Systems in 1994. In 2000 the IEEE passed 802.3ad which is an open standard version of EtherChannel.

1.1.2 Benefits of Etherchannel

Using an EtherChannel has numerous advantages, and probably the most desirable aspect is the bandwidth. Using the maximum of 8 active ports a total bandwidth of 800 Mbit/s, 8 Gbit/s or 80 Gbit/s is possible depending on port speed. This assumes there is a traffic mixture, as those speeds do not apply to a single application only. It can be used with Ethernet running on twisted pair wiring, single-mode and multimode fiber.

Because EtherChannel takes advantage of existing wiring it makes it very scalable. It can be used at all levels of the network to create higher bandwidth links as the traffic needs of the network increase. All Cisco switches have the ability to support EtherChannel.

When an EtherChannel is configured all adapters that are part of the channel share the same Layer 2 (MAC) address. This makes the EtherChannel transparent to network applications and users because they only see the one logical connection; they have no knowledge of the individual links.

EtherChannel aggregates the traffic across all the available active ports in the channel. The port is selected using a Cisco-proprietary hash algorithm, based on source or destination MAC addresses, IP addresses or TCP and UDP port numbers. The hash function gives a number between 0 and 7, and the following table shows how the 8 numbers are distributed among the 2 to 8 physical ports. In the hypothesis of real random hash algorithm, 2, 4 or 8 ports configurations lead to fair load-balancing, whereas other configurations lead to unfair load-balancing.

Fault-tolerance is another key aspect of EtherChannel. Should a link fail, the EtherChannel technology will automatically redistribute traffic across the remaining links. This automatic recovery takes less than one second and is transparent to network applications and the end user. This makes it very resilient and desirable for mission-critical applications.

Spanning tree protocol (STP) can be used with an EtherChannel. STP treats all the links as a single one and BPDUs are only sent down one of the links. Without the use of an EtherChannel, STP would effectively shutdown any redundant links between switches until one connection goes down. This is where an EtherChannel is most desirable, it allows use of all available links between two devices.

EtherChannels can be also configured as VLAN trunks. If any single link of an EtherChannel is configured as a VLAN trunk, the entire EtherChannel will act as a VLAN trunk. Cisco ISL, VTP and IEEE 802.1Q are compatible with EtherChannel.

1.2 RADIUS / 802.1x

https://en.wikipedia.org/wiki/IEEE_802.1X

1.2.1 Overview

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device which provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the authentication server is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the RADIUS and EAP protocols. In some cases, the authentication server software may be running on the authenticator hardware.

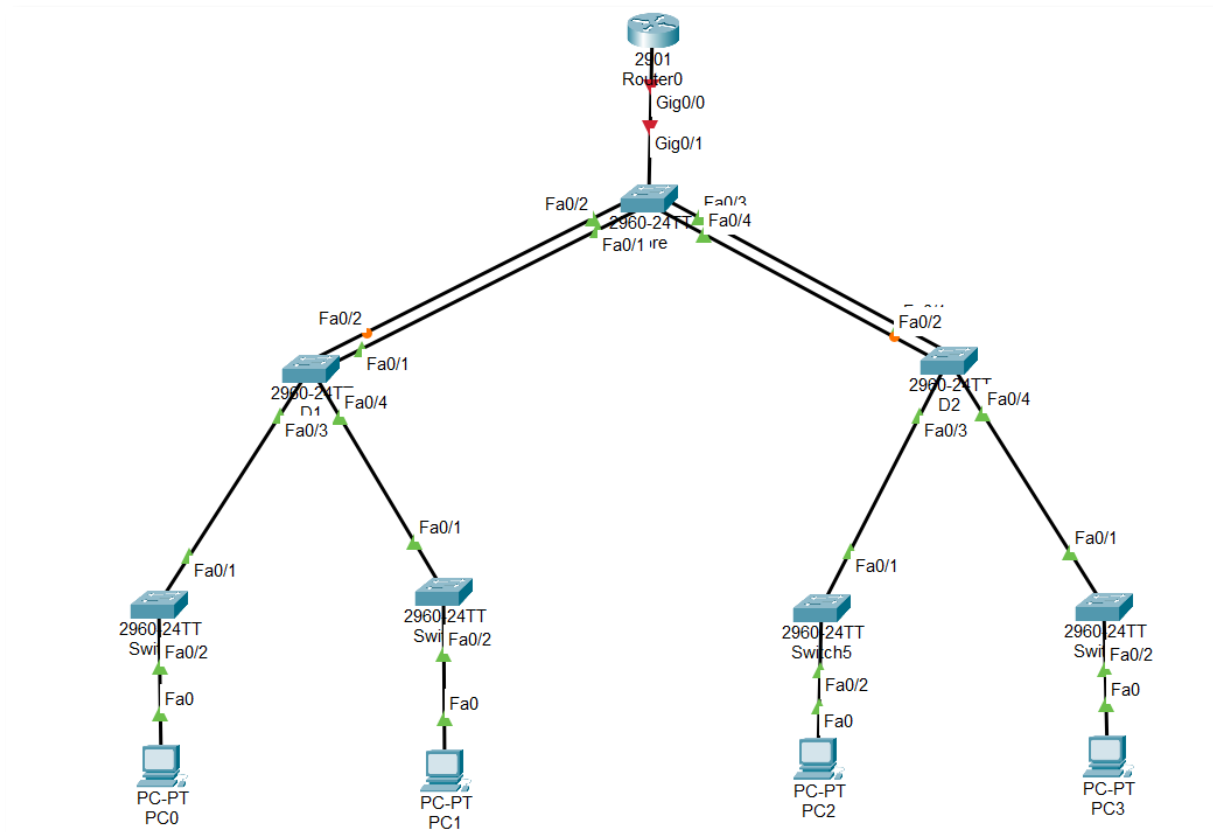
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant must initially provide the required credentials to the authenticator - these will have been specified in advance by the network administrator, and could include a user name/password or a permitted digital certificate. The authenticator forwards these credentials to the authentication server to decide whether access is to be granted. If the authentication server determines the credentials are valid, it informs the authenticator, which in turn allows the supplicant (client device) to access resources located on the protected side of the network.

1.2.2 Auth-Process

1. Initialization On detection of a new supplicant, the port on the switch (authenticator) is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as the Internet Protocol (and with that TCP and UDP), is dropped.

2. **Initiation** To initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address (01:80:C2:00:00:03) on the local network segment. The supplicant listens on this address, and on receipt of the EAP-Request Identity frame it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as a User ID. The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server. The supplicant may also initiate or restart authentication by sending an EAPOL-Start frame to the authenticator, which will then reply with an EAP-Request Identity frame.
3. **Negotiation (Technically EAP negotiation)** The authentication server sends a reply (encapsulated in a RADIUS Access-Challenge packet) to the authenticator, containing an EAP Request specifying the EAP Method (The type of EAP based authentication it wishes the supplicant to perform). The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant. At this point the supplicant can start using the requested EAP Method, or do an NAK ("Negative Acknowledgement") and respond with the EAP Methods it is willing to perform.
4. **Authentication** If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet), or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

2 Etherchannel



2.1 Konfigurieren von LACP

2.1.1 Am Core-Switch für Port Fa0/1-2 (linker Switch)

```
Core_SWITCH(config)#int r fa0/1-2
Core_SWITCH(config-if-range)#channel-protocol lacp
Core_SWITCH(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
```

2.1.2 Konfiguration am Core-Switch für Port Fa0/3-4 (rechter Switch)

```
Core_SWITCH(config)#int r fa0/3-4
Core_SWITCH(config-if-range)#channel-protocol lacp
Core_SWITCH(config-if-range)#channel-group 2 mode active
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up
```

2.1.3 Konfigurieren von linkem Switch (D1)

```
D1(config)#interface range fa0/1-2
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
```

2.2 Konfigurieren von rechtem Switch (D2)

```
D2(config)#interface range fa0/1-2
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
```

2.3 Informationen anzeigen

Mit `show etherchannel` kann man sich alle Informationen anzeigen lassen.

```
Core_SWITCH#show etherchannel
Channel-group listing:
-----
Group: 1
-----
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
Group: 2
-----
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
```


Mit show etherchannel summary kann man sich anzeigen lassen, welche Ports zu welchem Channel gehören.

```
Core_SWITCH#show etherchannel summary
```

```
Number of channel-groups in use: 2
```

```
Number of aggregators: 2
```

```
Group Port-channel Protocol Ports
```

```
-----+-----+-----+-----
-----
```

```
1 Po1(SU) LACP Fa0/1(P) Fa0/2(P)
```

```
2 Po2(SU) LACP Fa0/3(P) Fa0/4(P)
```

2.4 Stellen Sie sicher, dass der Core-Switch die Root-Bridge ist.

```
Core_SWITCH(config)#spanning-tree vlan 1 priority 0
```

```
Core_SWITCH#show sp
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID Priority 1
```

```
Address 0001.C730.8002
```

```
This bridge is the root
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 1 (priority 0 sys-id-ext 1)
```

```
Address 0001.C730.8002
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 20
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
-----
```

```
Fa0/3 Altn BLK 19 128.3 P2p
```

```
Fa0/2 Desg FWD 19 128.2 P2p
```

```
Fa0/4 Desg LSN 19 128.4 P2p
```

```
Fa0/1 Desg FWD 19 128.1 P2p
```

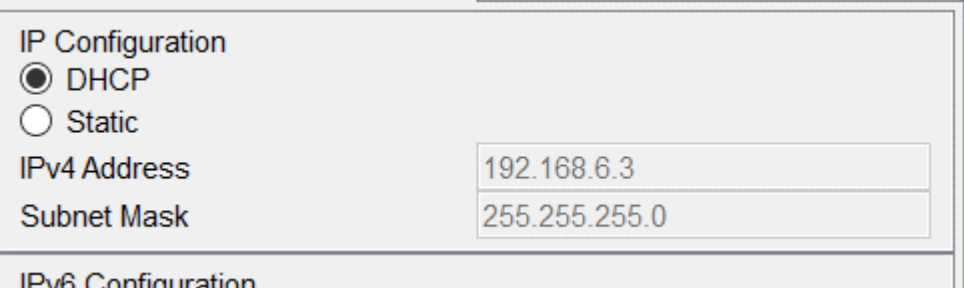
2.5 DHCP einschalten am Router (192.168.6.0/24)

```
Router(config)#int gig0/0
Router(config-if)#ip helper-address 192.168.6.1
Router(config-if)#exit
Router(config)#ip dhcp pool niklas
Router(dhcp-config)#network 192.168.6.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.6.1
Router(dhcp-config)#domain-name niklas.local
Router(dhcp-config)#exit
```

Dem Router eine IP geben:

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.6.1 255.255.255.0
Router(config-if)#no shut
```

PCs bekommen erfolgreich eine IP zugewiesen (PC0):



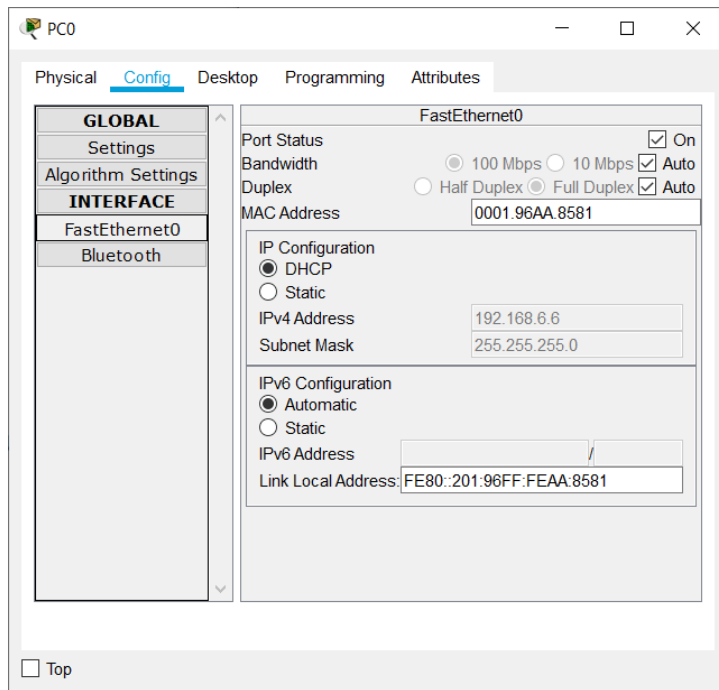
The screenshot shows a configuration window titled "IP Configuration". Under the "IP Configuration" section, the "DHCP" radio button is selected, and the "Static" radio button is unselected. Below this, the "IPv4 Address" field contains the value "192.168.6.3" and the "Subnet Mask" field contains the value "255.255.255.0". At the bottom of the window, the "IPv6 Configuration" section is visible but not expanded.

3 Port-Security

3.1 Konfigurieren Sie auf den Access Ports Portsecuritydamit sich jeweils nur ein Client (eine MAC Adresse) verbinden darf. Testen Sie die statische und die dynamische Variante.

3.1.1 Statische Variante

PC0 welcher an den ganz rechten Switch angeschlossen ist, hat folgende Netzwerkdaten (IP per DHCP):



```
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-sec
Switch(config-if)#switchport port-security mac-address
0001.96AA.8581
Switch(config-if)#switchport port-security violation protect
```

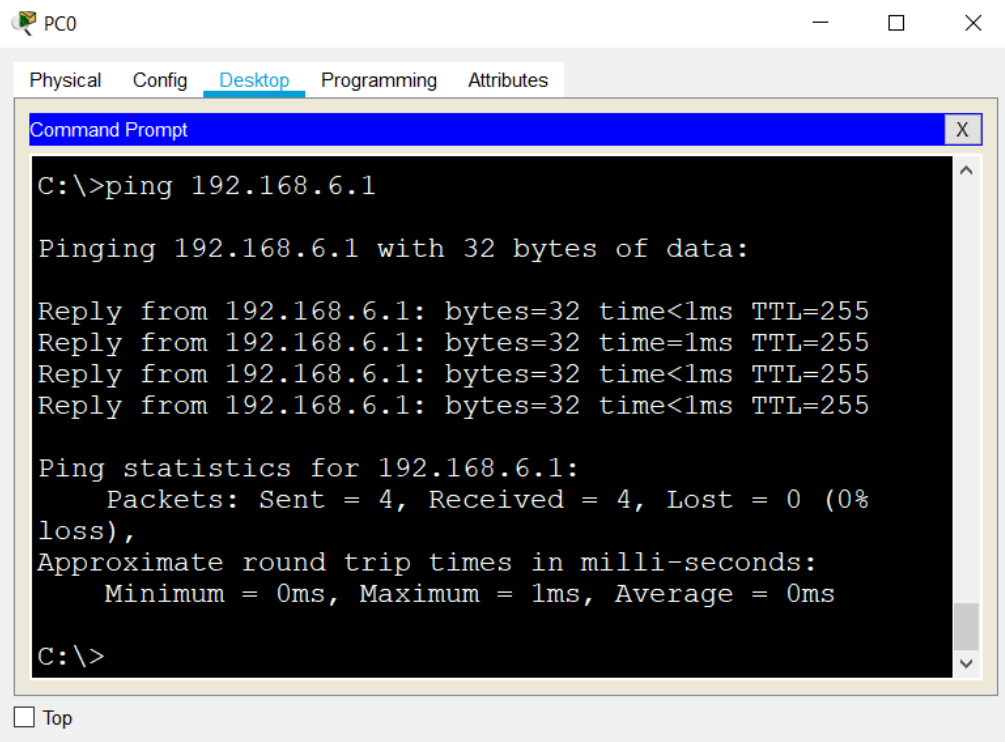
Sicherstellen, dass die Regeln eingerichtet wurden per show port-security:

```
Switch#show port-sec

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security
Action
(Count) (Count) (Count)
-----
Fa0/2 1 1 0 Protect
```

3.1.1.1 Kann der PC noch pingen? (PC0)

Ja, PC kann immer noch pingen, da seine Mac-Adresse der richtigen in der Table des Switches entspricht.



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of the command "C:\>ping 192.168.6.1". The output indicates a successful ping with 32 bytes of data, showing four replies from 192.168.6.1 with times less than 1ms and TTL=255. The ping statistics show 4 packets sent, 4 received, and 0% loss. The approximate round trip times are 0ms minimum, 1ms maximum, and 0ms average. The command prompt ends with "C:\>".

```
C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:


Reply from 192.168.6.1: bytes=32 time<1ms TTL=255
Reply from 192.168.6.1: bytes=32 time=1ms TTL=255
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

3.1.1.2 Verhalten bei Änderung der MAC-Adresse

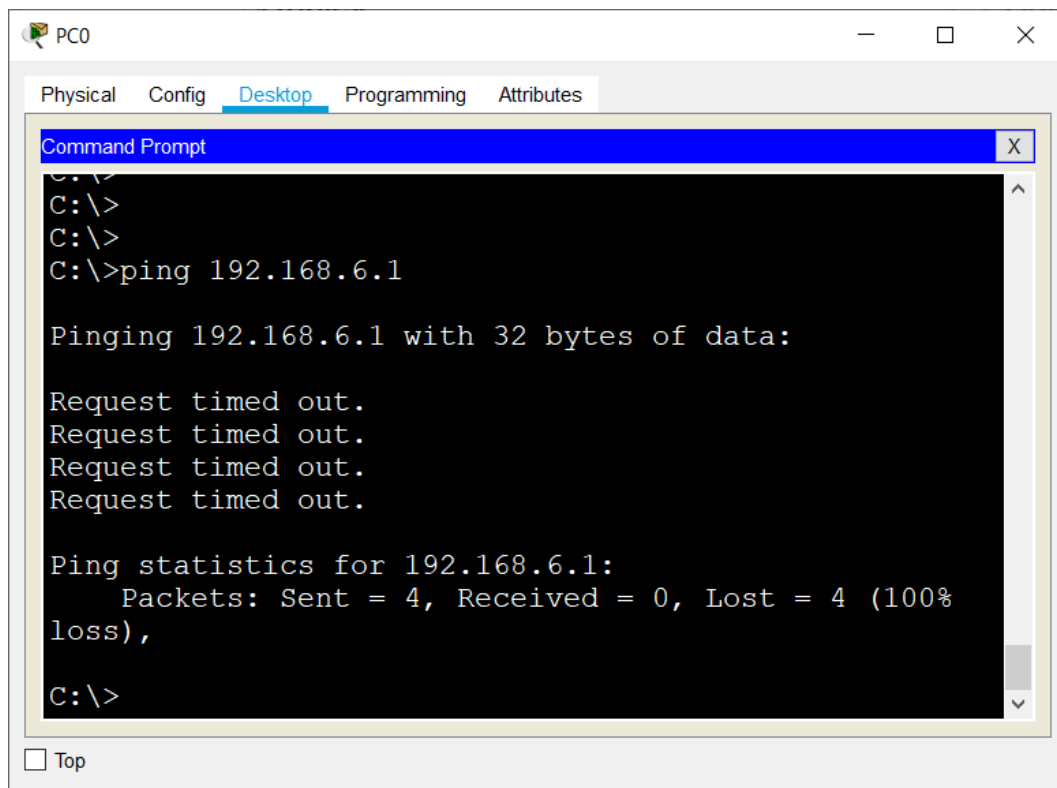
Neue MAC-Adresse



FastEthernet0

Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0001.96AA.8582

Der PC kann nicht mehr pingen:



3.1.2 Dynamisch

Zuerst muss die statisch eingetragene MAC-Adresse entfernt werden:

```
Switch(config-if)#no switchport port-security mac-address
0001.96AA.8581
```

3.1.2.1 Einschalten

Zuerst ins Interface wechseln, und dann den Port auf sticky umschalten. So wird der erste PC, der angeschlossen wird, dem seine MAC Adresse eingetragen und dann kann nur dieser auf das Netzwerk zugreifen.

```
Switch(config)#int fa0/2
Switch(config-if)#switchport port-sec mac-a sticky
```

Wir geben dem Test-PC (PC0) dieselbe MAC, die wir ihm beim letzten Test gegeben haben:

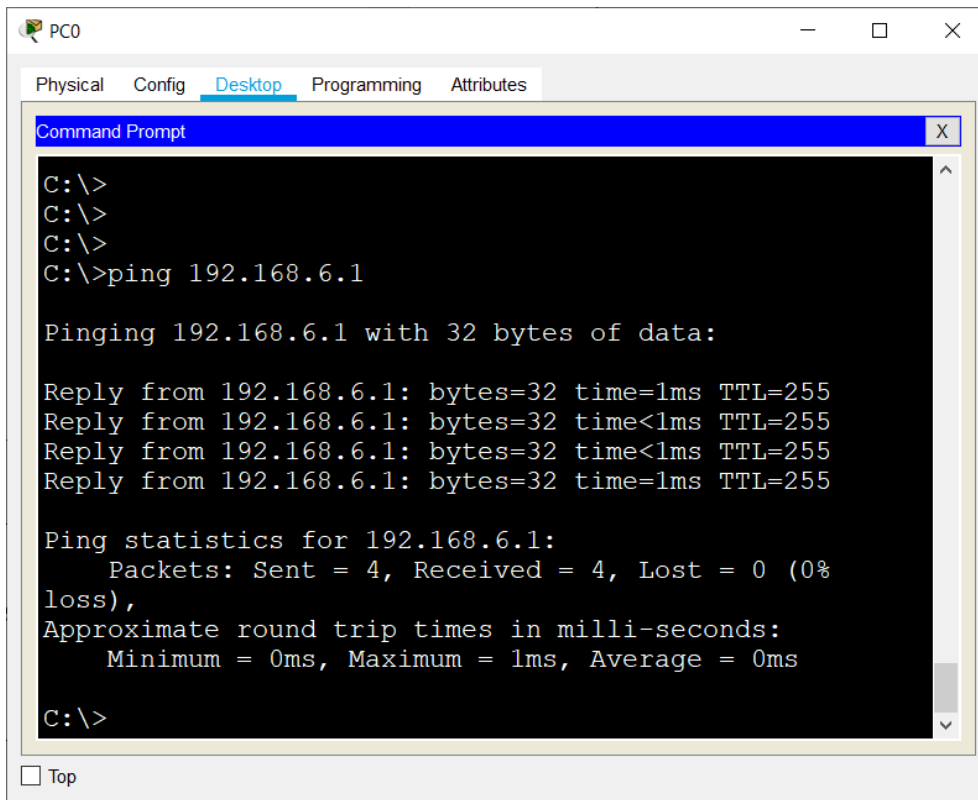
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	<input type="text" value="0001.96AA.8582"/>

Sicherstellen, dass die Sticky MAC in der Table steht:

```
Switch#show port-sec a
Secure Mac Address Table
-----
Vlan Mac Address Type Ports Remaining Age
(mins)
----
1 0001.96AA.8582 SecureSticky FastEthernet0/2 -
1 0001.96AA.8581 DynamicConfigured FastEthernet0/2 -
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
```

3.1.2.2 Testen mit PC0

Da PC0 die richtige, vom Switch gelernte MAC besitzt, kann er den Router pingen.

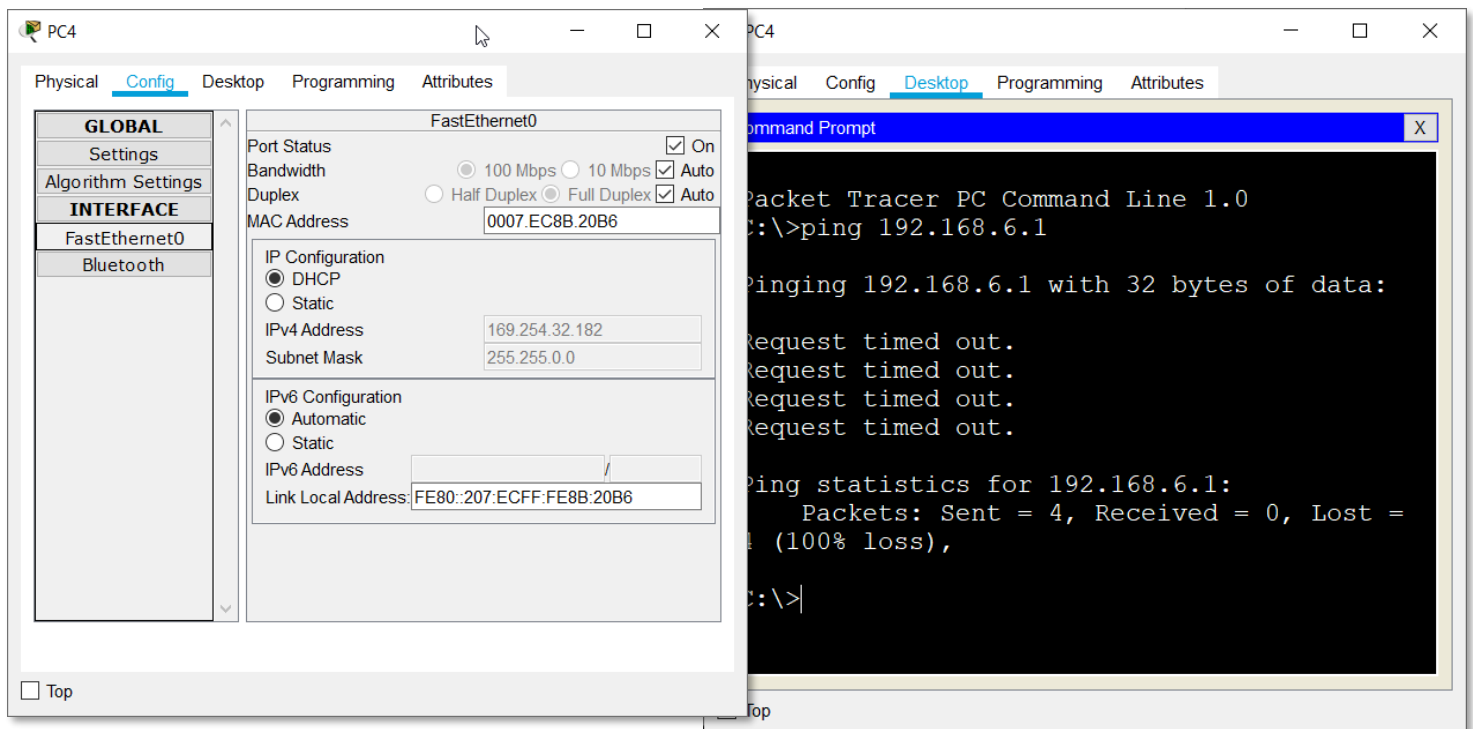
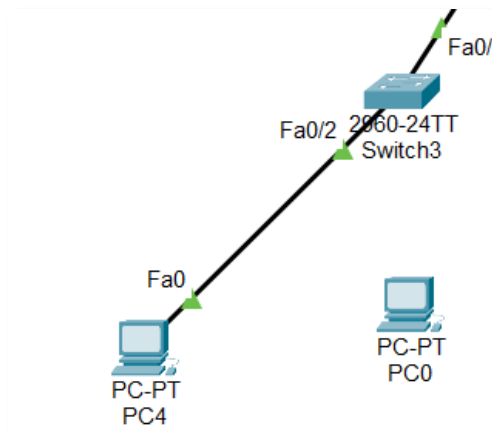


The screenshot shows a window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following text:

```
C:\>  
C:\>  
C:\>  
C:\>ping 192.168.6.1  
  
Pinging 192.168.6.1 with 32 bytes of data:  
  
Reply from 192.168.6.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.6.1: bytes=32 time=1ms TTL=255  
  
Ping statistics for 192.168.6.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0%  
loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>
```

At the bottom left of the PC0 window, there is a checkbox labeled 'Top' which is currently unchecked.

Schließt man jetzt allerdings einen anderen, zweiten PC an das selbe Interface wie PC0 an, so bekommt dieser keine IP vom DHCP Server zugesendet, da der Switch die Weitergabe der Angesch- Pakete des neuen PCs verweigert.



So schlägt der versuch, den Router zu pingn, auch fehl, da sich der Switch weigert, die ICMP Pakete weiter zu reichen.

3.2 Welche Befehle stehen zur Verfügung um den Zustand der Ports zu überprüfen?

3.2.1 Show port-security

Es ist der einfachste Befehl, zeigt allerdings auch nur den Port an und liefert wenig Information.

```
Switch#show port-security
```



```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security
Action
(Count) (Count) (Count)
-----
Fa0/2 1 1 0 Protect
-----
Switch#
```

3.2.2 Show port-sec address

Mit diesem Befehl kann man sich das VLAN, die Mac, den Port und das Remaining Age der Port-Security anzeigen lassen. Dieser Befehl liefert wesentlich mehr Informationen.

```
Switch#show port-sec a
Secure Mac Address Table
-----
-----
Vlan Mac Address Type Ports Remaining Age
(mins)
-----
1 0001.96AA.8582 SecureSticky FastEthernet0/2 -
1 0001.96AA.8581 DynamicConfigured FastEthernet0/2 -
-----
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 1024
```

3.2.3 Show port-sec in x/x

Möchte man sich detaillierte Informationen zu einem Interface anzeigen lassen, so kann man diesen Befehl nutzen. Ein Beispiel:

```
Switch#show port-sec in fa0/2
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0007.EC8B.20B6:1
Security Violation Count : 0
```

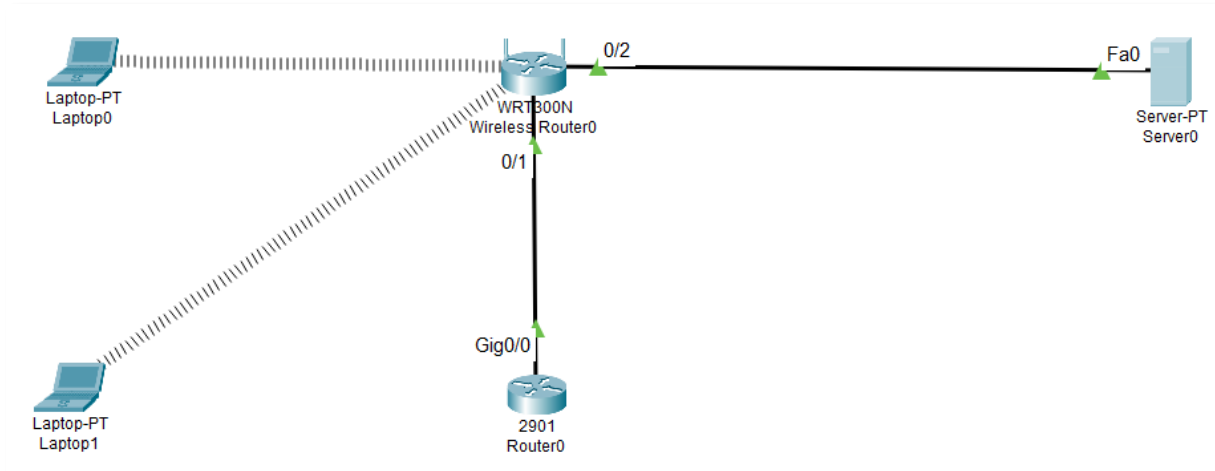
3.2.4 Show mac address-table

Mit diesem Befehl kann man sich anzeigen lassen, welche Mac-Adresse zu welchem Port sie gehört und welcher Typ sie ist, entweder statisch oder dynamisch.

```
Switch#show mac address-table
Mac Address Table
-----
Vlan Mac Address Type Ports
----
1 0001.43dc.de03 DYNAMIC Fa0/1
1 0001.96aa.8582 STATIC Fa0/2
```

4 WPA2-Enterprise

4.1 Aufbau



4.2 Router0 einrichten

Ich weise dem Router0 die IP 192.168.10.254 zu, wie in der Angabe angegeben.

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
Router(config-if)#ip address 192.168.10.254 255.255.255.0
```

4.3 DHCP Server am Router anschalten

Es wird ein DHCP Server auf dem Router konfiguriert, damit sich die Laptop-Clients später automatisch eine IP holen können.

```
Router(config-if)#ip helper-address 192.168.10.254
Router(config)#ip dhcp pool niklas
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.254
```

4.4 RADIUS am Server einrichten

Für Radius auf einem Server geht man in den Services Tab und dort auf ‚AAA‘. Dort kann man Radius einschalten und Clients / Benutzer hinzufügen.

The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. The 'AAA' service is highlighted in the left sidebar. The main configuration area for AAA is shown, including a 'Service' toggle set to 'On' and a 'Radius Port' of 1645. Below this, the 'Network Configuration' section contains a table with one entry: '1 WPA2' with 'Client IP' 192.168.0.1, 'Server Type' Radius, and 'Key' nvs. The 'User Setup' section contains a table with one entry: '1 nvsuser' with 'Username' nvsuser and 'Password' nvs. Both sections have 'Add', 'Save', and 'Remove' buttons.

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key	
1	WPA2	192.168.0.1	Radius	nvs	<div>Add</div>
					<div>Save</div>
					<div>Remove</div>

User Setup

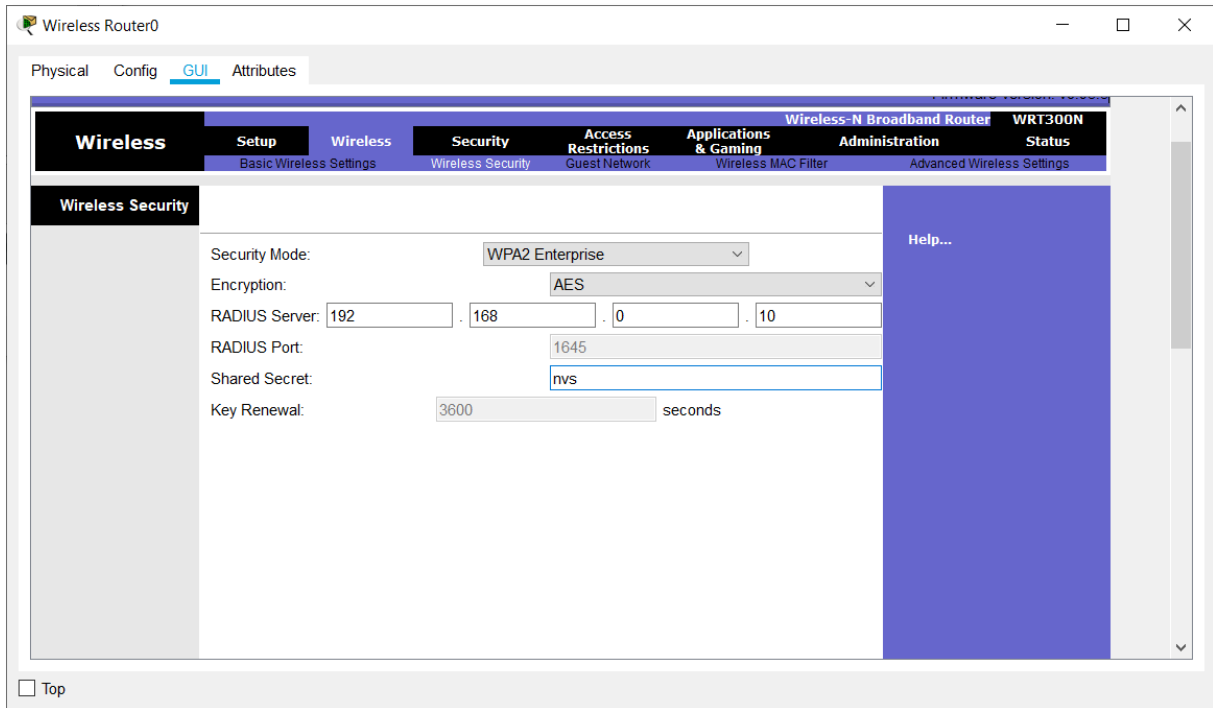
Username Password

	Username	Password	
1	nvsuser	nvs	<div>Add</div>
			<div>Save</div>
			<div>Remove</div>

☐ Top

4.5 Den Wireless-Router einrichten

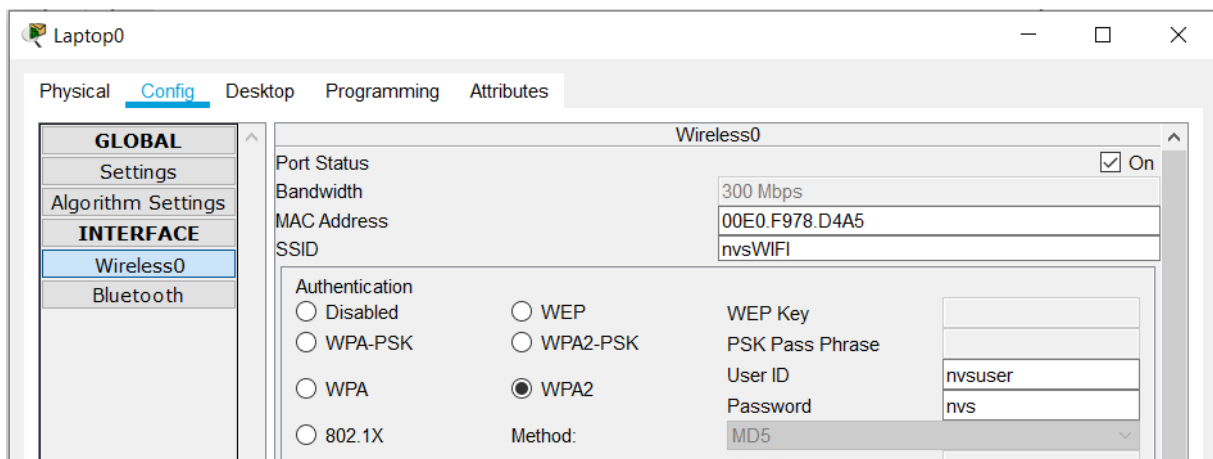
Unter Wireless->Wireless Security kann man den Wireless Mode einrichten. Dort wählt man WPA2 Enterprise aus, legt den RADIUS Server und das Secret fest.



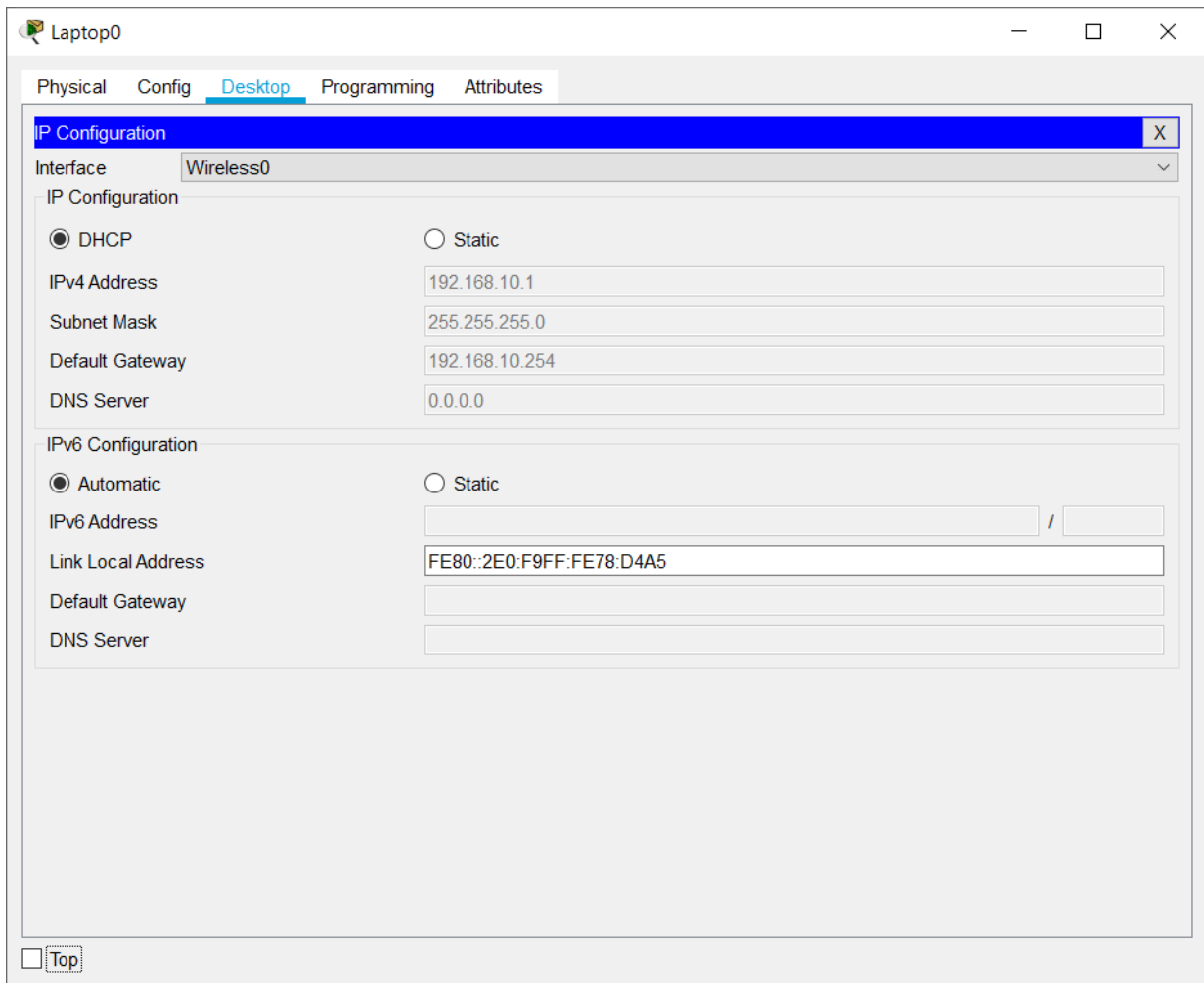
4.6 Konfiguration der Laptops

Damit die Laptops WLAN empfangen können, muss ihnen vorher noch die WLAN Karte eingebaut werden. Ist das geschafft, geht man in den Config Tab, Wireless0, und trägt dort die SSID ein. Dann als Methode WPA2 wählen und dort die Daten wie Benutzername, Passwort eintragen.

4.6.1 Laptop0



Nachdem der Laptop mit den richtigen Daten versehen ist, bekommt er eine IP vom DHCP Server zugewiesen:



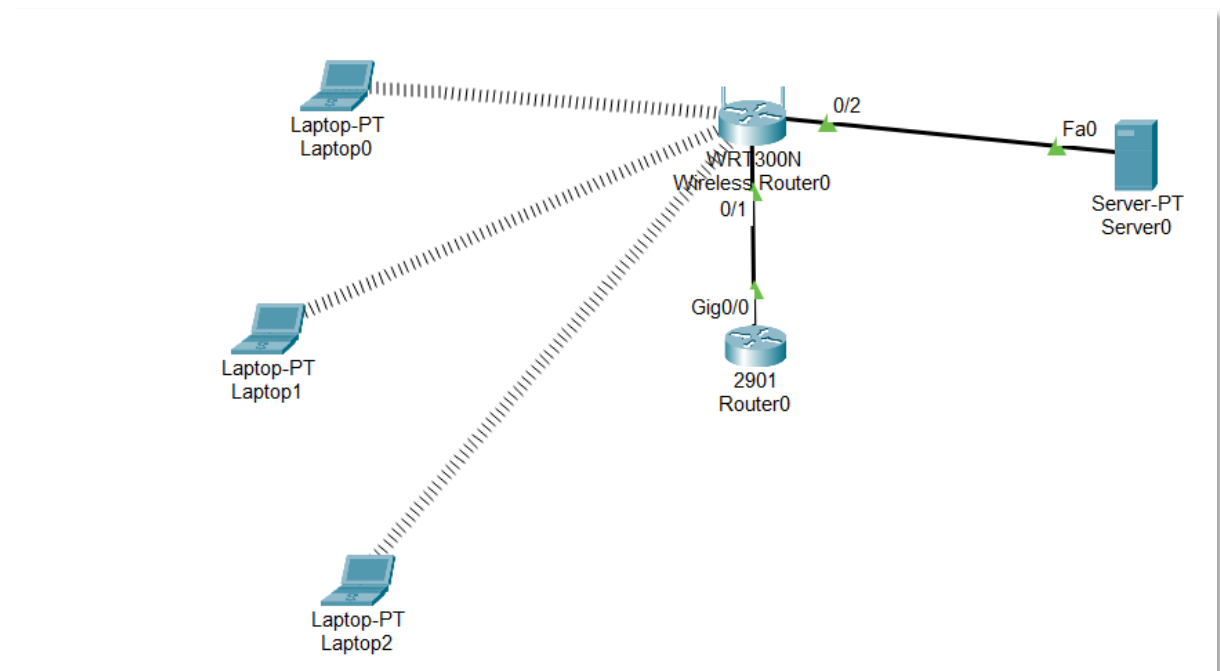
4.7 Legen sie am Radiusserver mehrere User an und testen sie die Anmeldung

User Setup

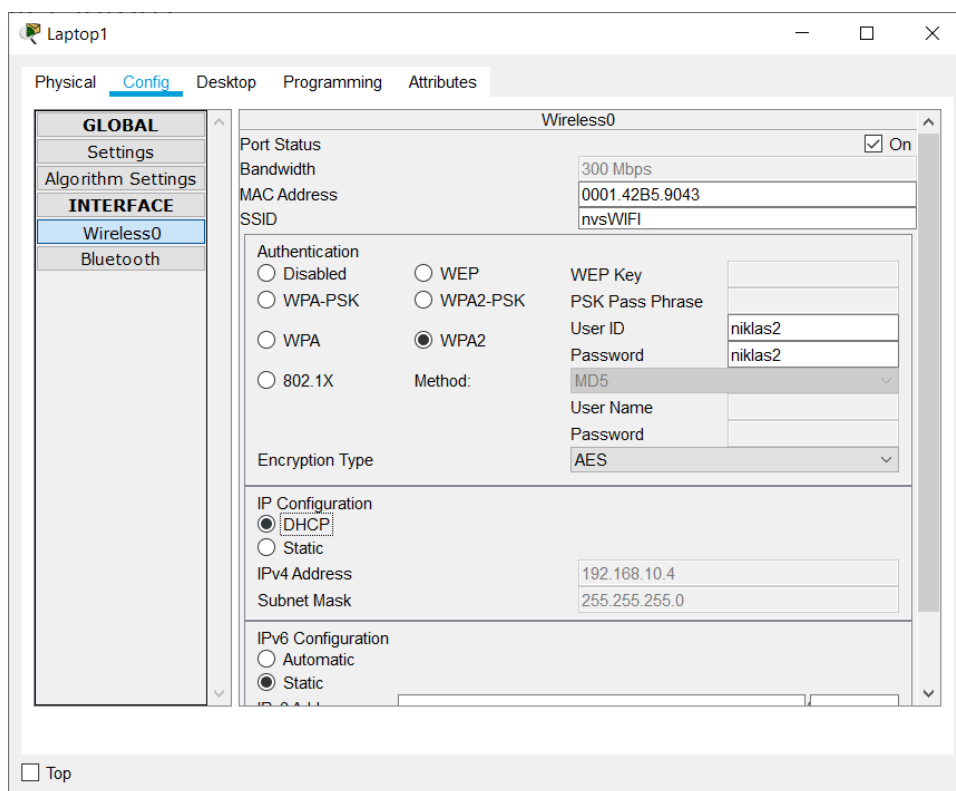
Username Password

	Username	Password
1	nvsuser	nvs
2	niklas2	niklas2
3	niklas3	niklas3

4.7.1 Angepasstes Modell



4.7.2 Testen des Users niklas2 mit Laptop1



4.7.3 Testen des Users niklas3 mit Laptop2

Laptop2

Physical **Config** Desktop Programming Attributes

GLOBAL

- Settings
- Algorithm Settings

INTERFACE

- Wireless0**
- Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 11 Mbps

MAC Address 0000.0C06.0307

SSID nvsWIFI

Authentication

- ☐ Disabled
- ☐ WEP
- ☐ WPA-PSK
- ☐ WPA2-PSK
- ☐ WPA
- ☒ WPA2
- ☐ 802.1X

Method: WPA2

WEP Key

PSK Pass Phrase

User ID niklas3

Password niklas3

MD5

User Name

Password

Encryption Type AES

IP Configuration

- ☒ DHCP
- ☐ Static

IPv4 Address 192.168.10.5

Subnet Mask 255.255.255.0

IPv6 Configuration

- ☐ Automatic
- ☒ Static

IPv6 Address

Link Local Address: FE80::200:CFF:FE06:307

☐ Top