Laborbericht - NVS - 5CHIF

Name: Juri Schreib	**Datum:** 2017-03-14

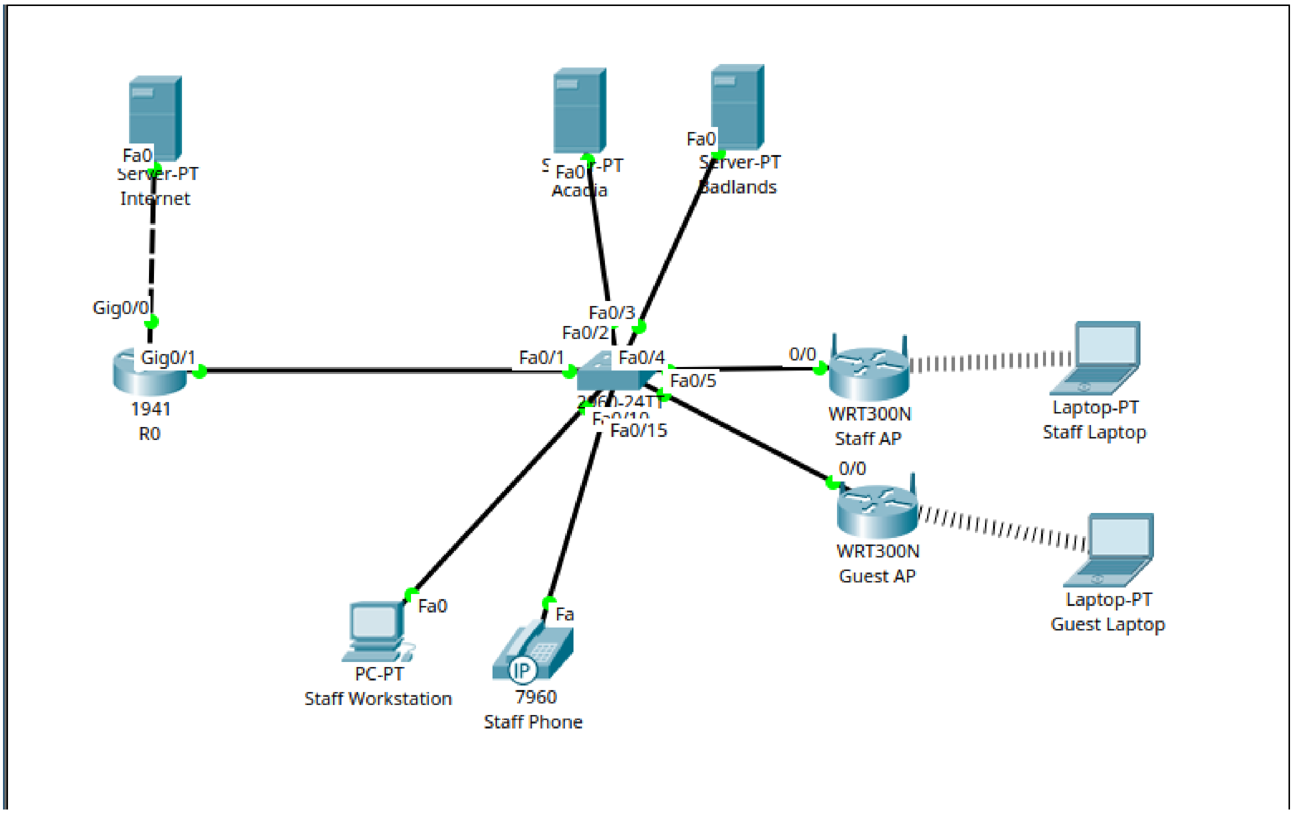
Ziel: Erfüllung der Aufgabenstellung

Vorweg-Information zum ASA Gerät

Da die ASA mit der standard Lizenz nur 2-Vlans forwoarding konfiguriert werden kann, wird ein 2. kleiners Testnetzwerk modeliert, um die funktionsweiße der ASA zu testen und demonstrieren. Da der DHCP Server nach der Dokumentation auf dem Router läuft, wird am Router einfach inter-vlan routing genutzt, um zwischen den verschiedenen VLANs zu kommunizieren.

Das Device hardening wird im ersten Schritt erstmal ausgelassen. Es geht erst mal Darum, eine funktionierendes Netzwerk aufzusetzen.

Netzwerkkonfiguration



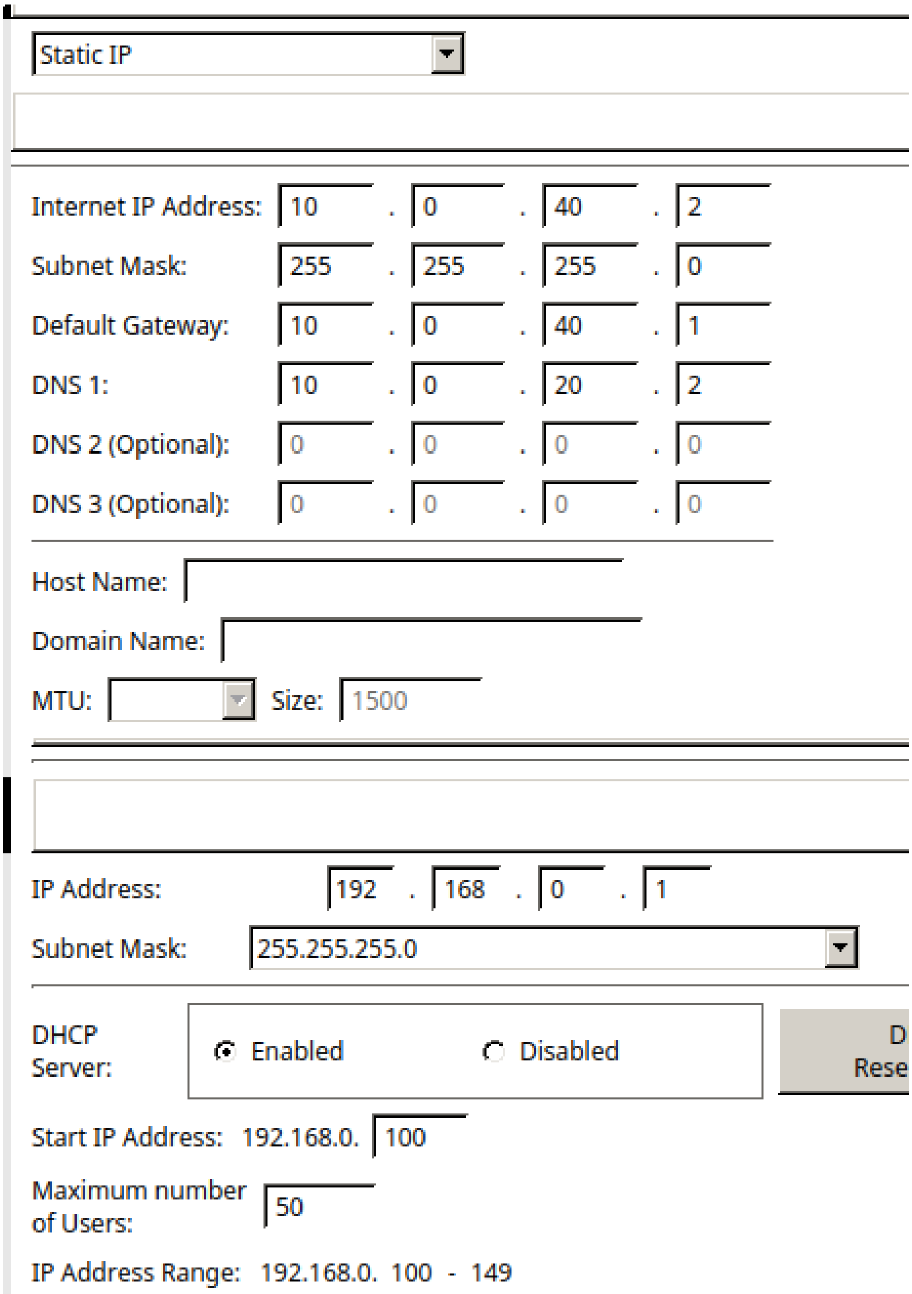
IP Konfiguration

Dem Router wird die öffentliche IP Adresse 1.1.1.2 im Netz 1.1.1.0/24 zur verfügung gestellt. Das Internet wird durch einen Server mit der IP Adresse 1.1.1.1 emuliert.

Alle anderen statischen IP Adressen und Interfaces werden so wie in3 Sofrware & Unternehmenswebsite definiert vergeben.

Da es im Packet Tracer keinen Access Pint gibt, der 802.1Q unterstüzt, wrid dieser durch 2 Acess Points ersetzt, die sich in den jeweiligen vlans (Guest & Staff) befinden und einer sich in dem jewiligen Subnet befindlichen IP Adresse zugewiesen werden. Der einfachheit halber bliebt auf diesen Geräten NAT und DHCP aktiviert.

Konfiguration Staff AP



Static IP

Internet IP Address: 10 . 0 . 40 . 2

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 0 . 40 . 1

DNS 1: 10 . 0 . 20 . 2

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name:

Domain Name:

MTU: Size: 1500

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

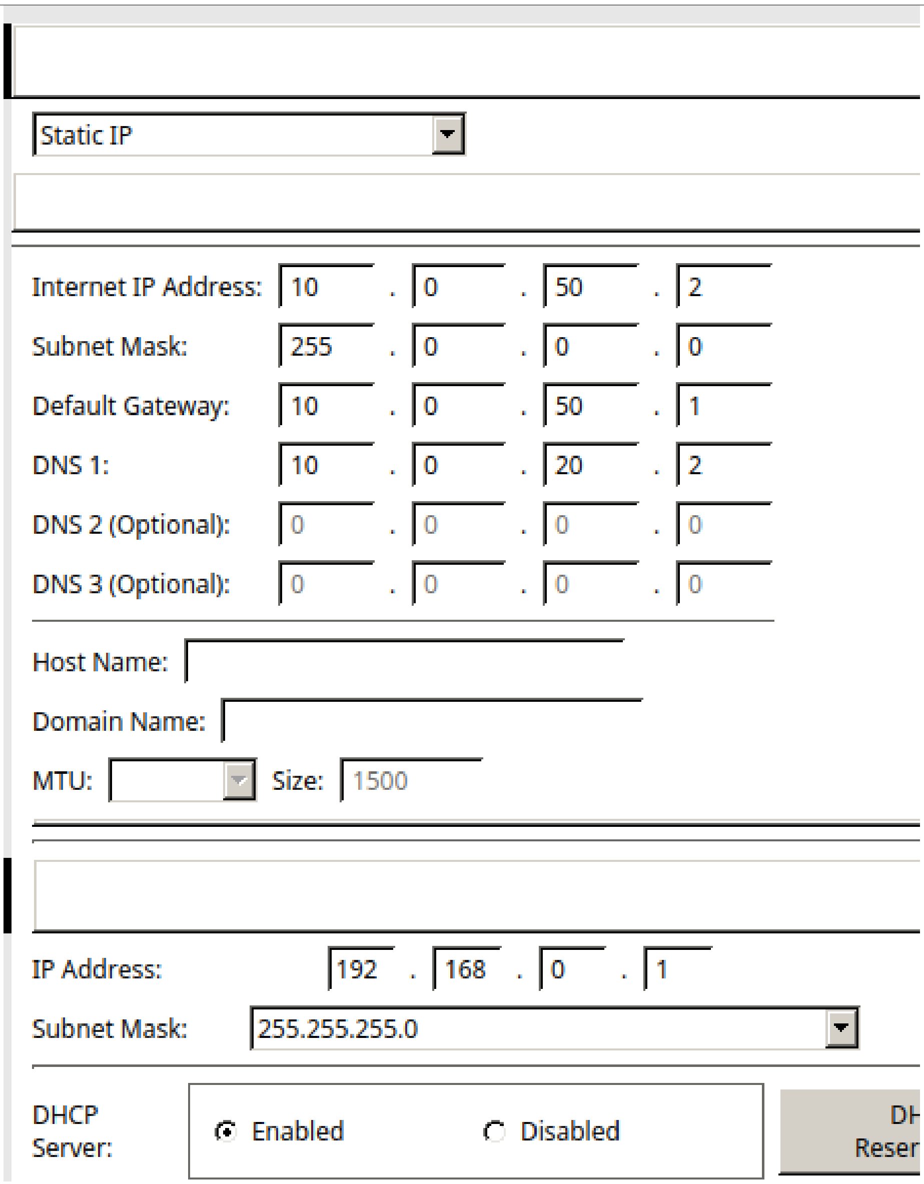
DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Konfiguration Guest AP



Static IP

Internet IP Address: 10 . 0 . 50 . 2

Subnet Mask: 255 . 0 . 0 . 0

Default Gateway: 10 . 0 . 50 . 1

DNS 1: 10 . 0 . 20 . 2

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name:

Domain Name:

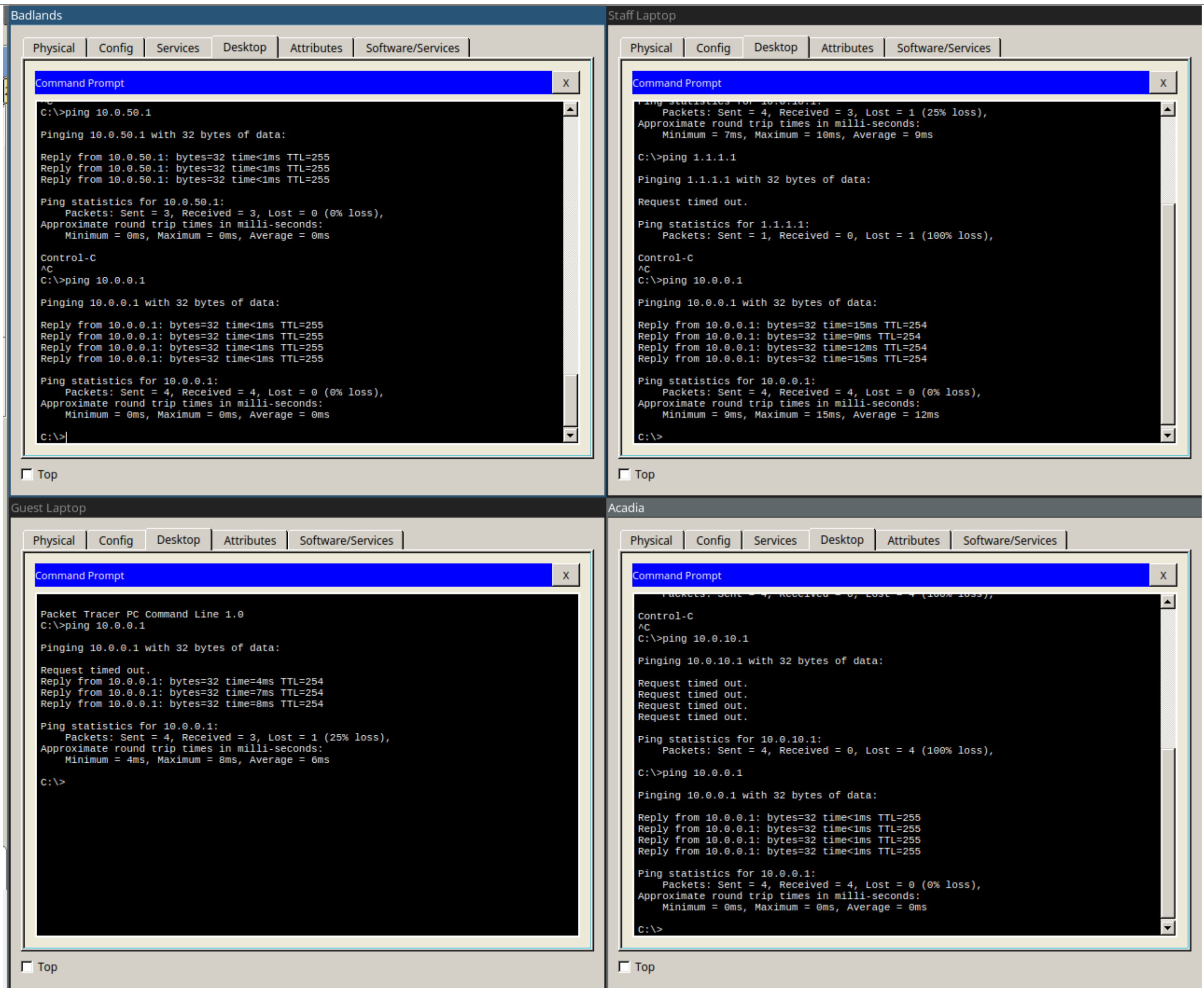
MTU: Size: 1500

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server: ● Enabled ○ Disabled

Testen



```
C:\>ping 10.0.50.1

Pinging 10.0.50.1 with 32 bytes of data:

Reply from 10.0.50.1: bytes=32 time<1ms TTL=255
Reply from 10.0.50.1: bytes=32 time<1ms TTL=255
Reply from 10.0.50.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.50.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Ping statistics for 10.0.10.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 10ms, Average = 9ms

C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Request timed out.

Ping statistics for 1.1.1.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=15ms TTL=254
Reply from 10.0.0.1: bytes=32 time=9ms TTL=254
Reply from 10.0.0.1: bytes=32 time=12ms TTL=254
Reply from 10.0.0.1: bytes=32 time=15ms TTL=254

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 12ms

C:\>
```

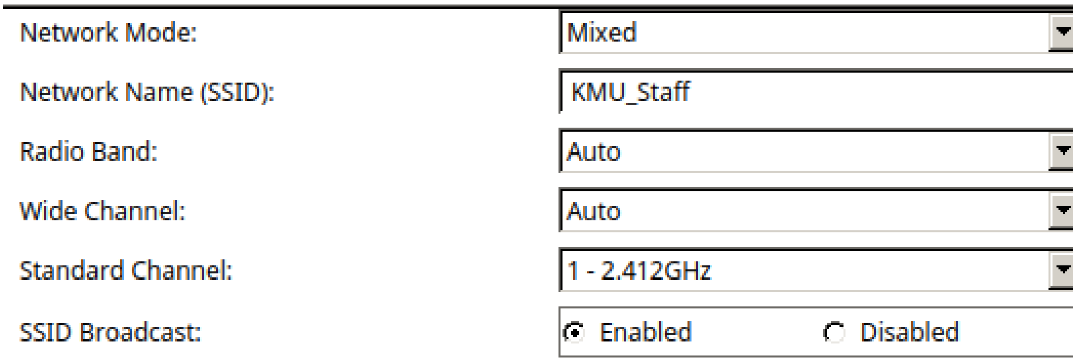
```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.1: bytes=32 time=4ms TTL=254
Reply from 10.0.0.1: bytes=32 time=7ms TTL=254
Reply from 10.0.0.1: bytes=32 time=8ms TTL=254

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 6ms

C:\>
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Control-C
^C
C:\>ping 10.0.10.1

Pinging 10.0.10.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

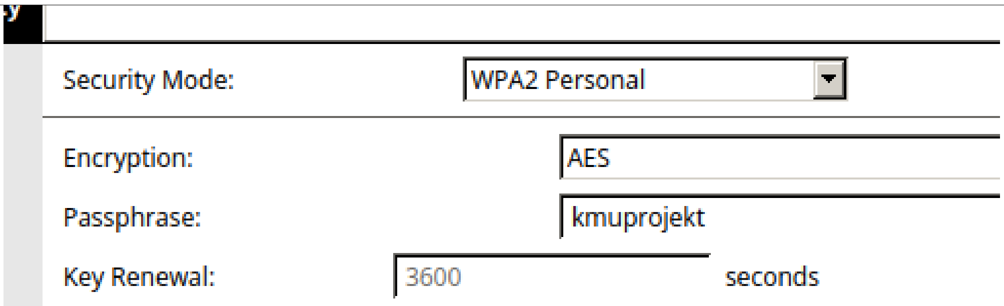
Wireless Configuration

SSID	Verschlüsselungsmethode	Password
KMU_Guest	-	-
KMU_Staff	kmuprojekt	WPA2/PSK (AES)

Konfiguration Staff AP



Network Mode:	Mixed
Network Name (SSID):	KMU_Staff
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	● Enabled ○ Disabled



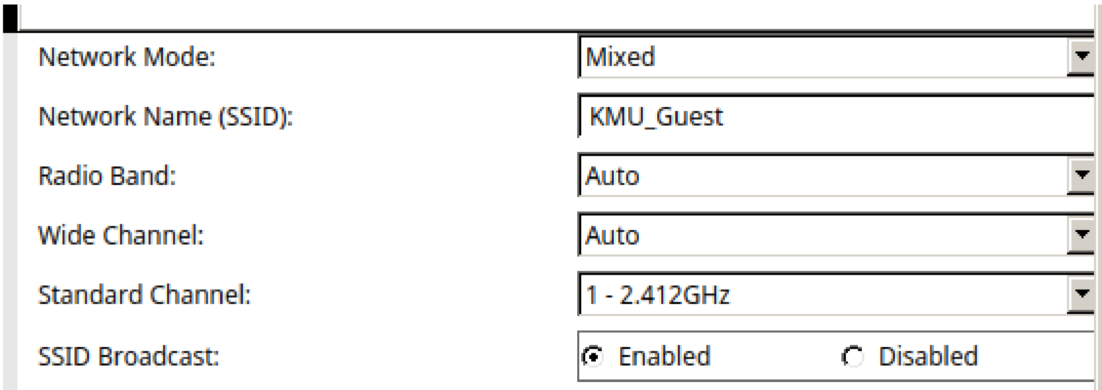
Security Mode: WPA2 Personal

Encryption: AES

Passphrase: kmuprojekt

Key Renewal: 3600 seconds

Konfiguration Guest AP



Network Mode: Mixed

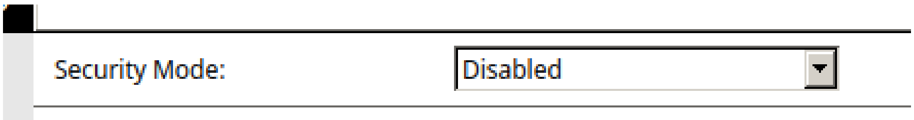
Network Name (SSID): KMU_Guest

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ● Enabled ○ Disabled



Security Mode: Disabled

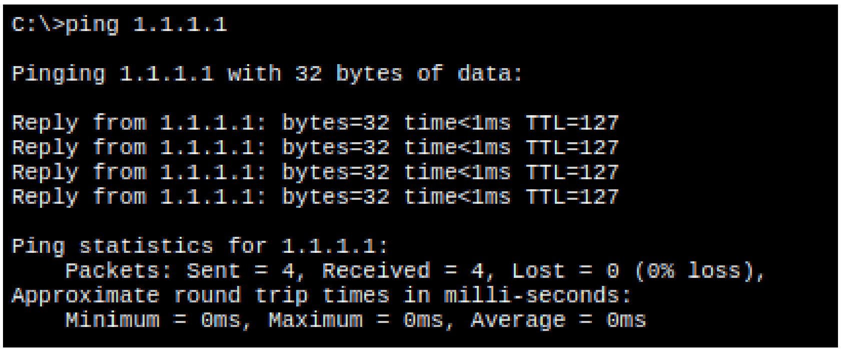
Nat Konfiguration am Router

Im echten Netzwerk muss die öffentliche Ip Adresse, mit der des ISPs ersetzt werden.

Das Interface g0/0 wird als outside interface definiert. Alle subinterface von g0/1 als inside.

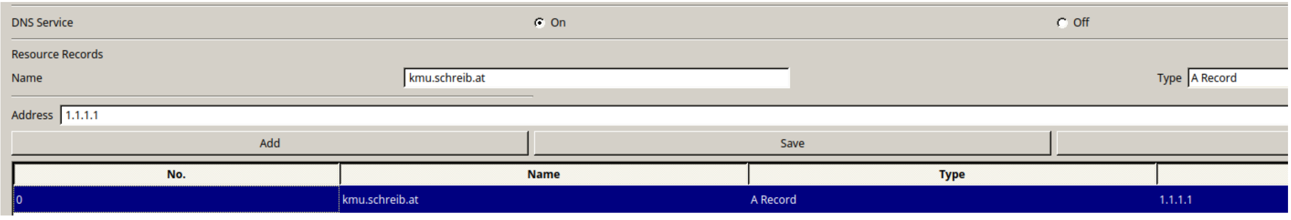
```
ip nat pool NAT 10.0.0.1 10.0.50.255 netmask 255.255.0.0
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.255.255
```

Testen



```
C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time<1ms TTL=127
Reply from 1.1.1.1: bytes=32 time<1ms TTL=127
Reply from 1.1.1.1: bytes=32 time<1ms TTL=127
Reply from 1.1.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Es wird der DNS Server auf Badlands, und der Webserver auf dem Internet Server aktiviert



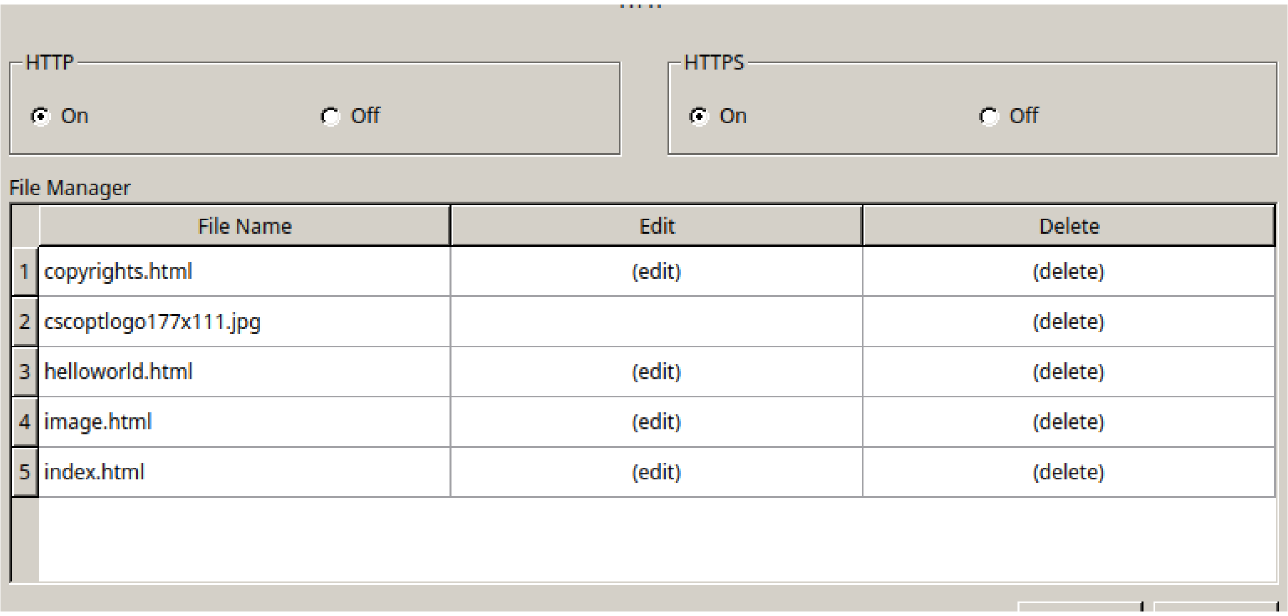
DNS Service ● On ○ Off

Resource Records

Name kmu.schreib.at Type A Record

Address 1.1.1.1

No.	Name	Type	
0	kmu.schreib.at	A Record	1.1.1.1



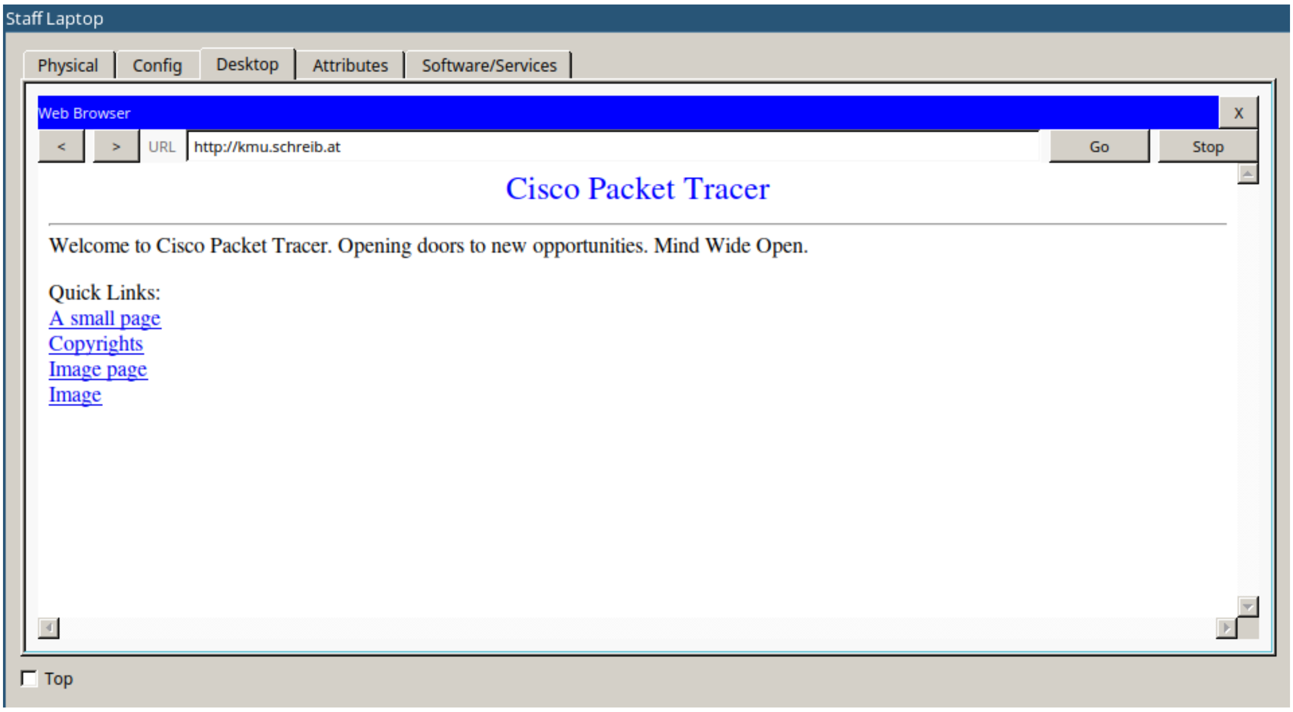
HTTP ● On ○ Off

HTTPS ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Es wird getestet ob alle Endgeräte (bis auf Staff Workstation, da hier noch DHCP konfiguriert werden musss) auf die öffentliche Website kommen

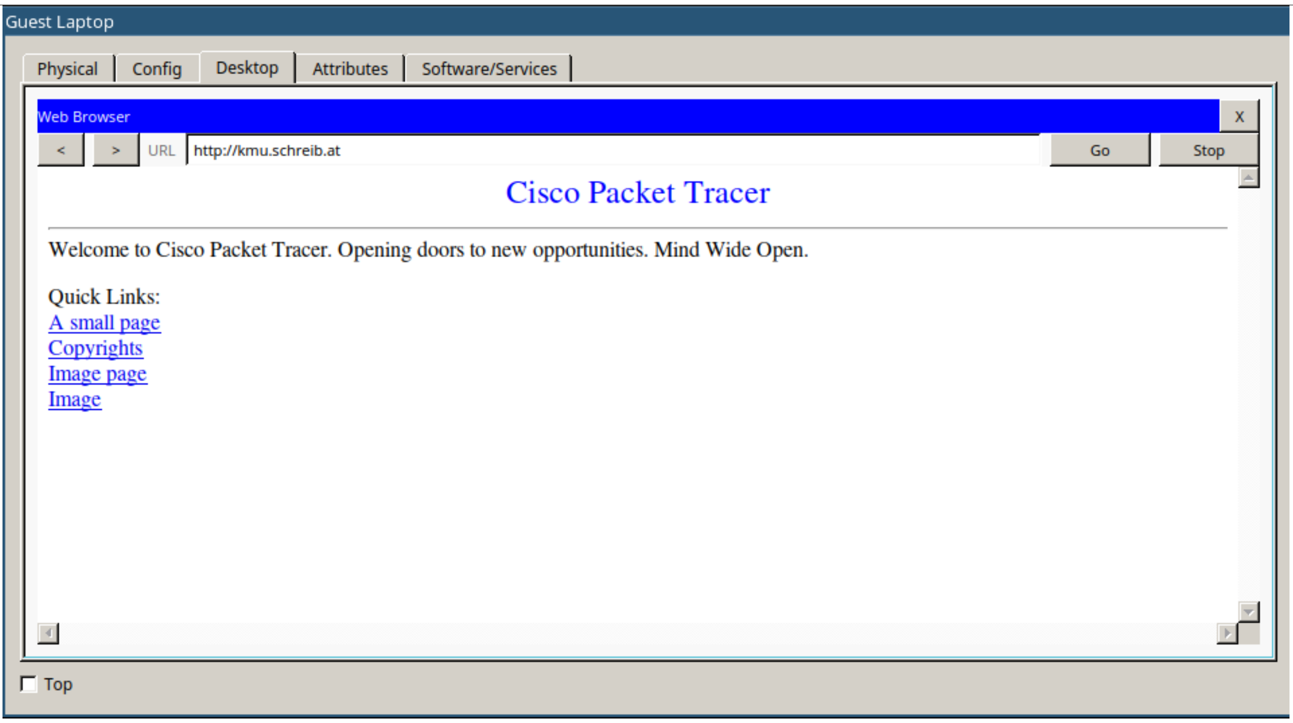


URL http://kmu.schreib.at

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



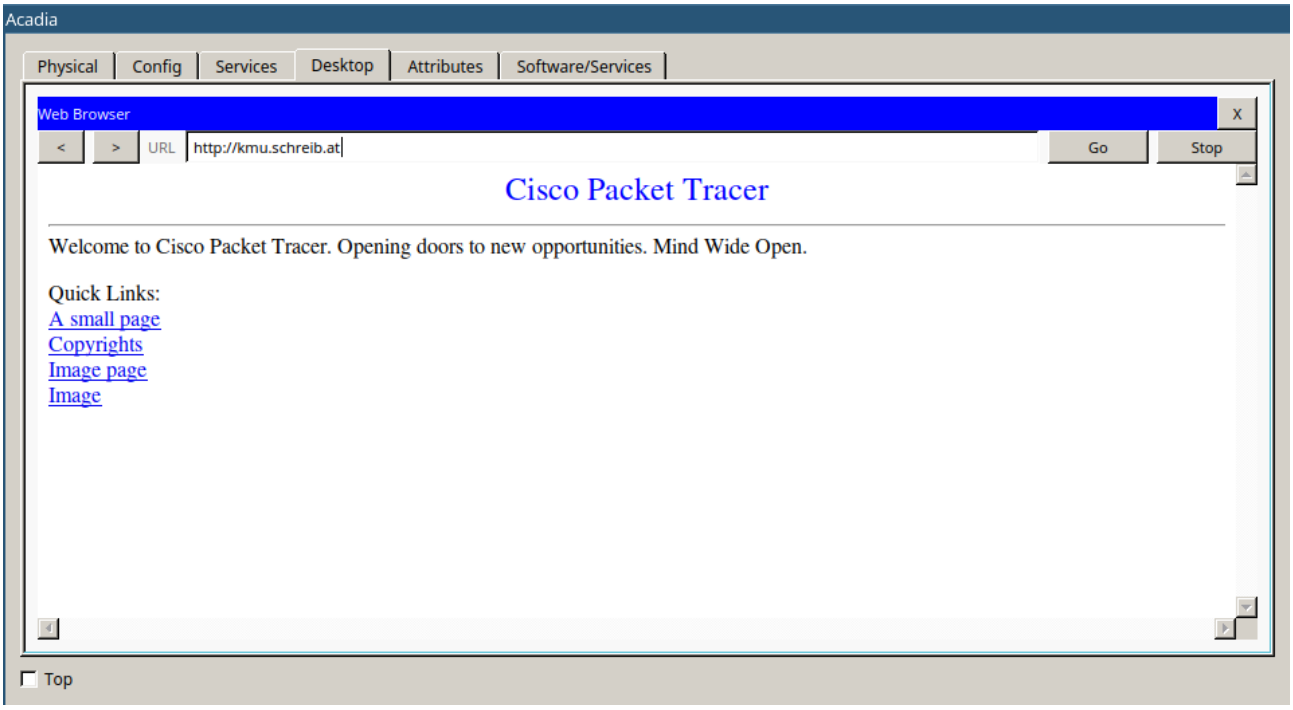
http://kmu.schreib.at

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

□ Top



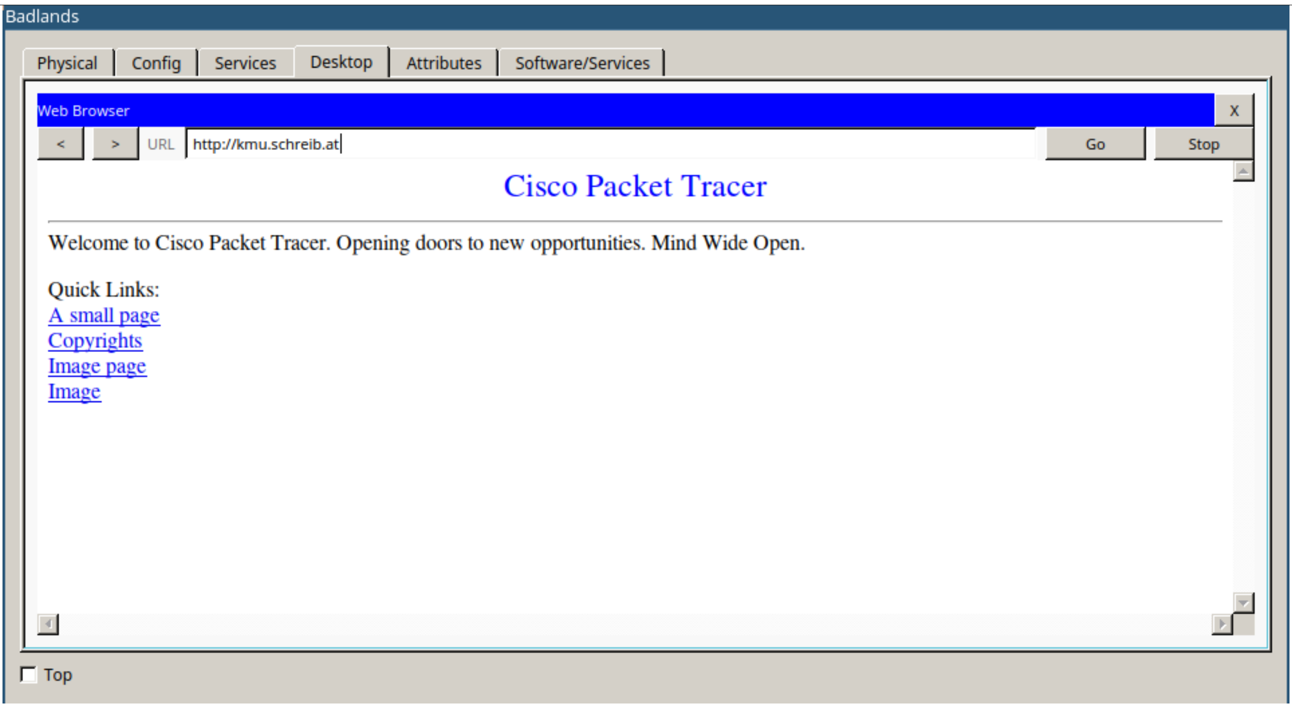
http://kmu.schreib.at

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

□ Top



http://kmu.schreib.at

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

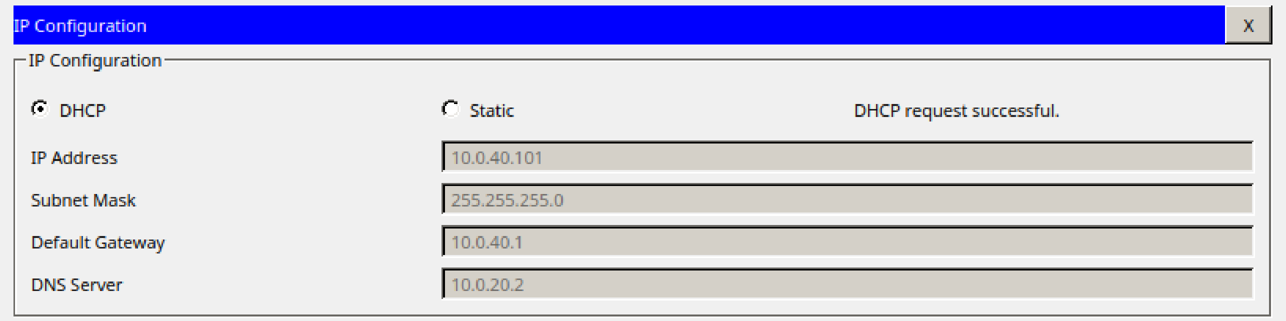
Quick Links:
A small page
Copyrights
Image page
Image

DHCP Konfiguration am Router

Da DHCP im Guest Vlan in diesem Modell vom Access-Point übernommen wird, muss nur ein DHCP pool im Staff VLAN aktiviert werden.

```
ip dhcp pool Staff
network 10.0.40.0 255.255.255.0
default-router 10.0.40.1
dns-server 10.0.20.2
ip dhcp excluded-address 10.0.40.1 10.0.40.100
```

Testen



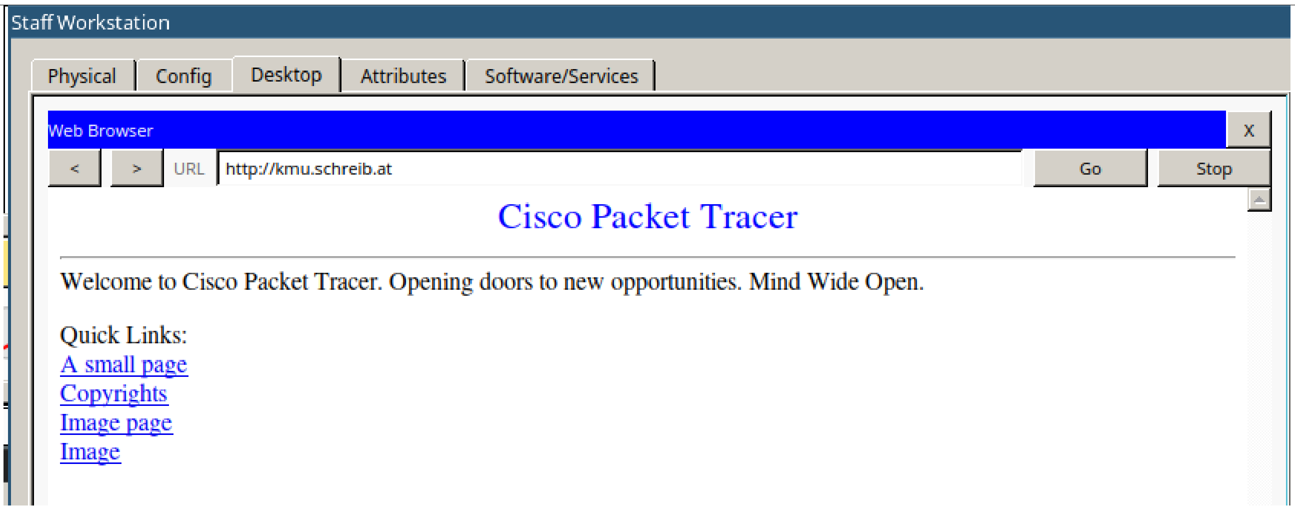
● DHCP ○ Static DHCP request successful.

IP Address 10.0.40.101

Subnet Mask 255.255.255.0

Default Gateway 10.0.40.1

DNS Server 10.0.20.2



http://kmu.schreib.at

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Authentication & Router hardening

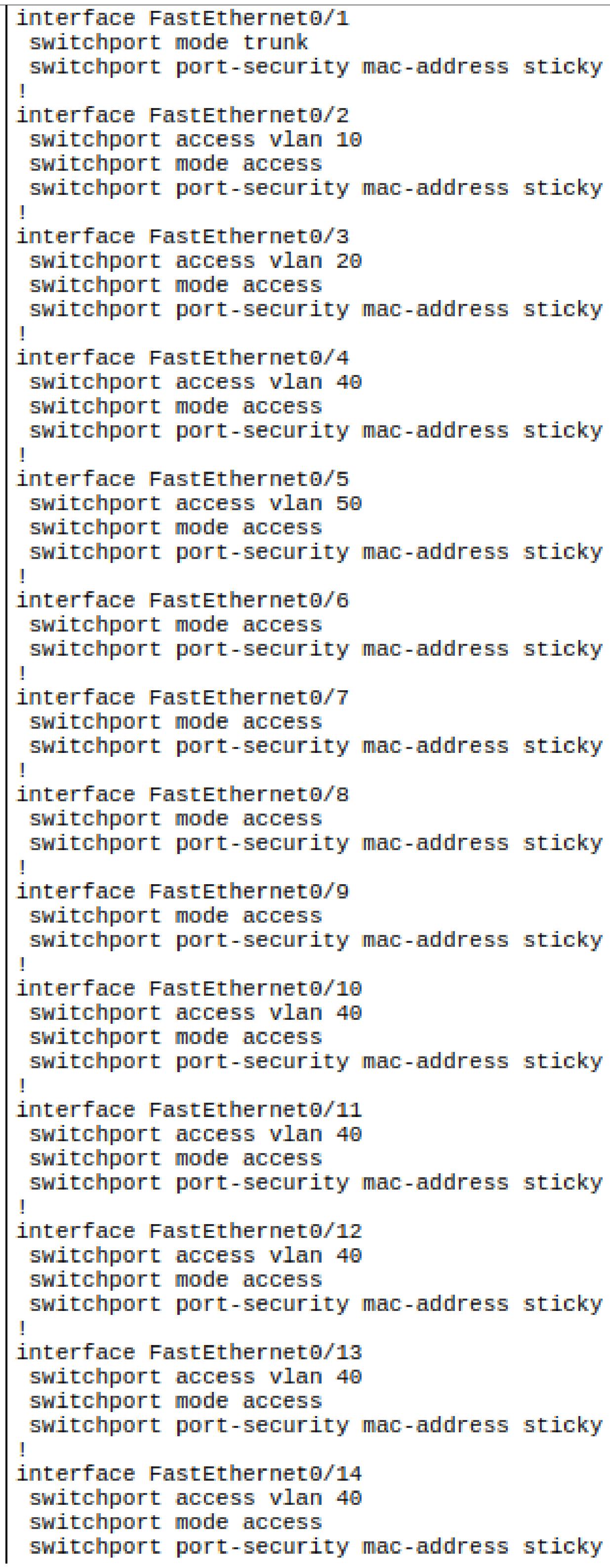
Gleichzeitig mit dem Router hardening wird auf den Geräten SSH aktiviert.

Konfiguration die über alle Geräte hinweg gleich ist:

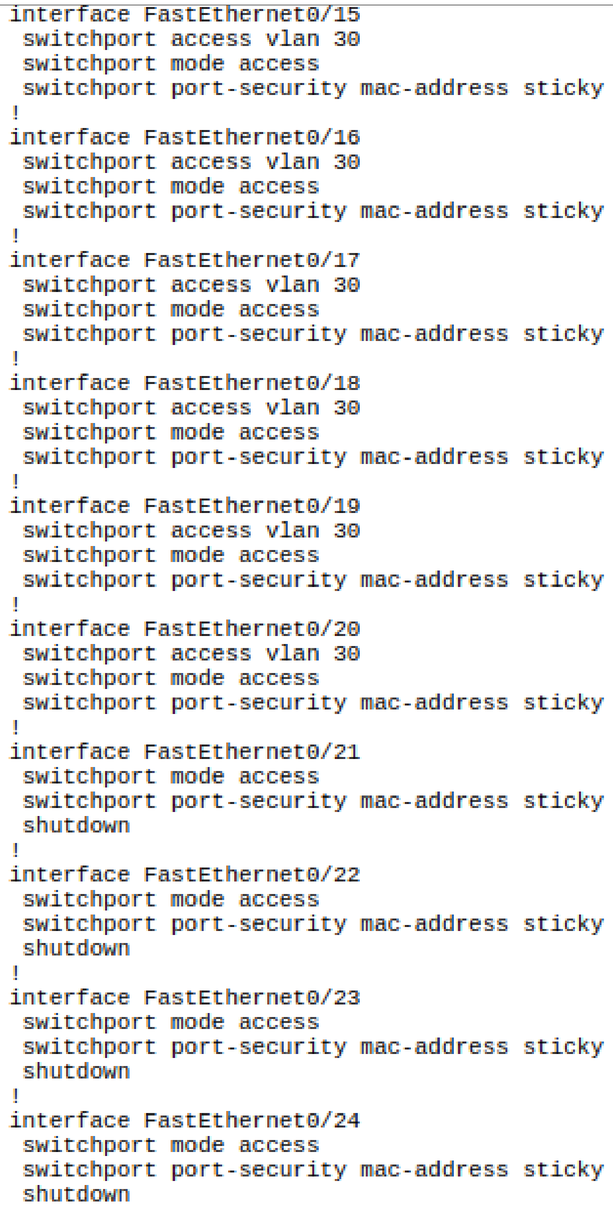
```
banner motd #unauthorized access prohibited#
security passwords min-length 10
service password-encryption
enable secret ciscoclass
username cisco privilege 15 secret ciscoclass
ip domain-name schreib.at
crypto key generate rsa
2048
ip ssh version 2
ip ssh time-out 90
ip ssh authentication-retries 2
line vty 0 15
login local
transport input ssh
transport output ssh
exec-timeout 20
line con 0
login local
transport output ssh
exec-timeout 20
```

Port Security Konfiguration am Switch

Die Port Security wird bei allen Ports auf sticky gestellt. Nicht benutzer Ports werden administrativ deaktiviert

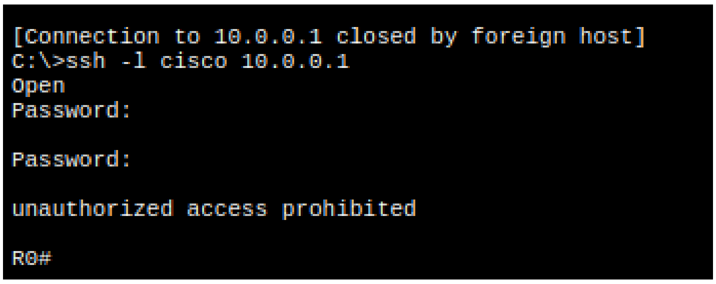


```
interface FastEthernet0/1
 switchport mode trunk
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
```



```
interface FastEthernet0/15
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
```

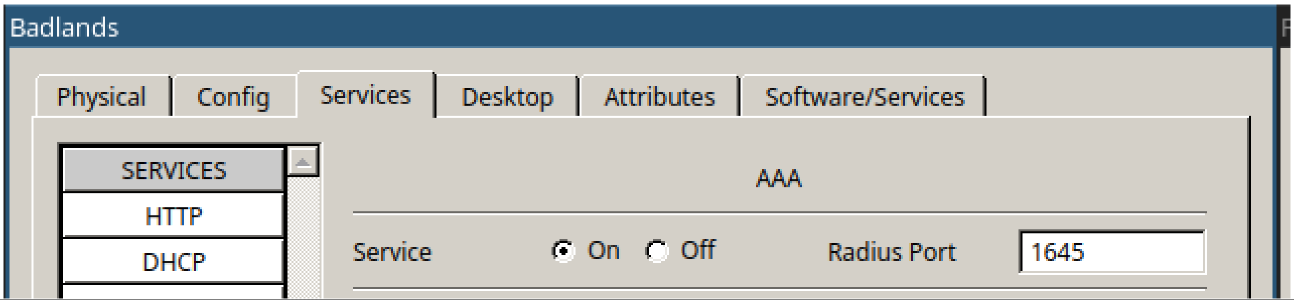
Die SSH verbindung wird getestet



```
[Connection to 10.0.0.1 closed by foreign host]
C:\>ssh -l cisco 10.0.0.1
Open
Password:

Password:

unauthorized access prohibited

R0#
```

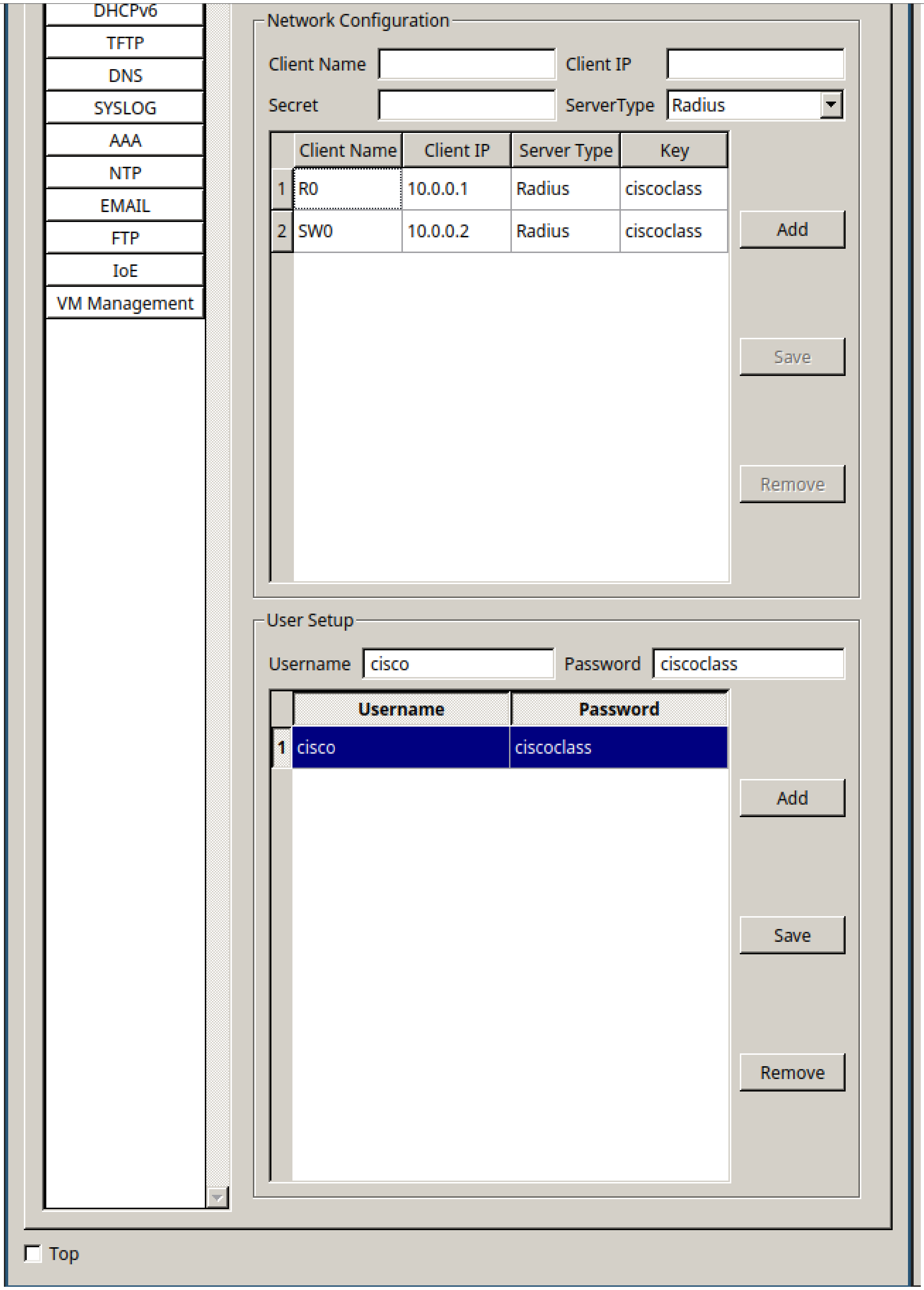
Radius

Als erstes wird der Radius service am Badlands Server aktiviert



AAA

Service ● On ○ Off Radius Port 1645



Network Configuration

Client Name:

Client IP:

Secret:

ServerType: Radius

	Client Name	Client IP	Server Type	Key
1	R0	10.0.0.1	Radius	ciscoclass
2	SW0	10.0.0.2	Radius	ciscoclass

User Setup

Username: cisco

Password: ciscoclass

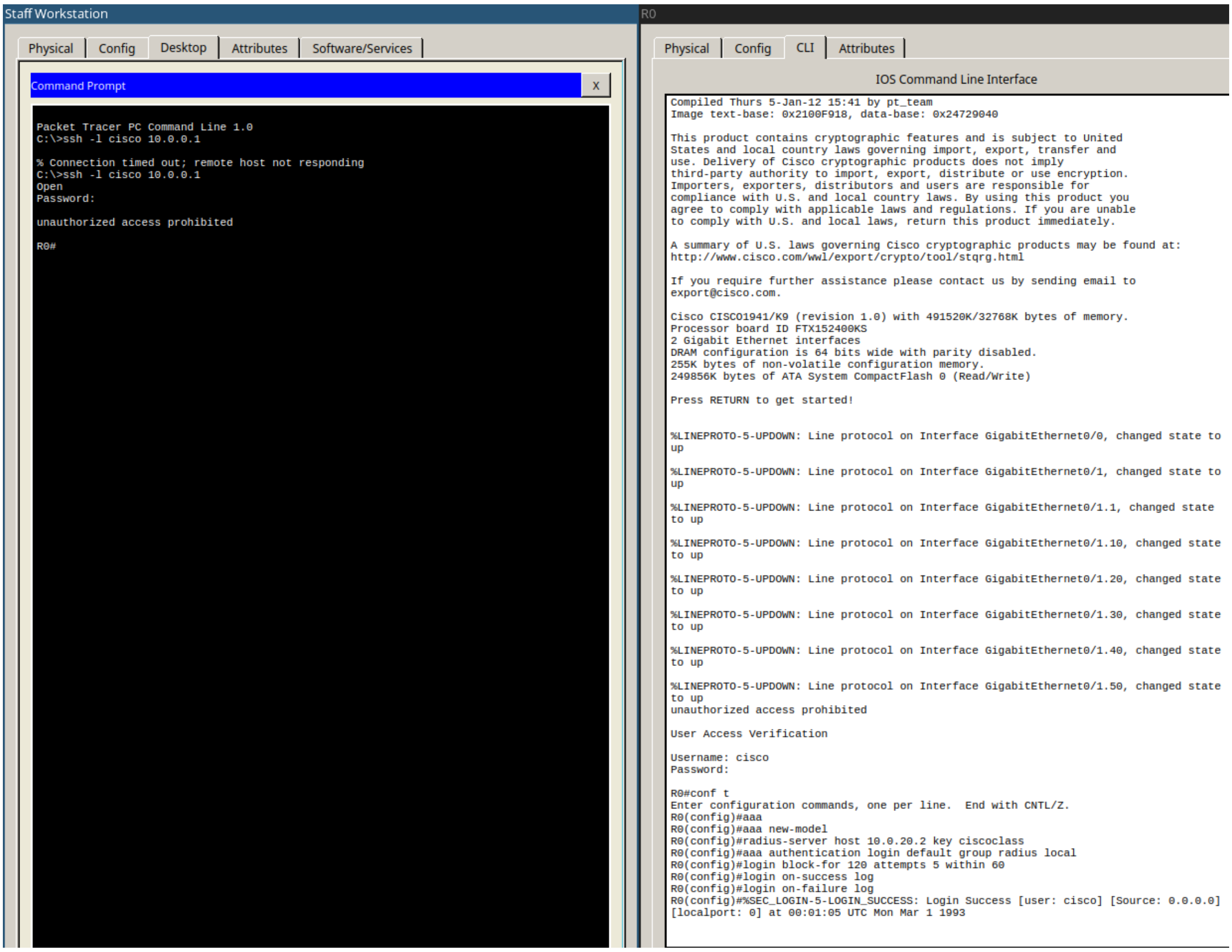
	Username	Password
1	cisco	ciscoclass

Danach wird AAA auf den Intermediate Devices aktiviert

```
aaa new-model
radius-server host 10.0.20.2 key ciscoclass
aaa authentication login default group radius local
login block-for 120 attempts 5 within 60
login on-success log
login on-failure log
```

Der Switch unterstützt im Packet Tracer kein AAA, daher wird diese Konfiguration am Switch in der Testumgebung ausgelassen. Die Obere Konfiguration kann allerdings 1 zu 1 für den Switch übernommen werden, um AAA zu aktivieren.

Testen



```
Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 10.0.0.1

% Connection timed out; remote host not responding
C:\>ssh -l cisco 10.0.0.1
Open
Password:

unauthorized access prohibited

R0#
```

```
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.40, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.50, changed state
to up
unauthorized access prohibited

User Access Verification

Username: cisco
Password:

R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#aaa
R0(config)#aaa new-model
R0(config)#radius-server host 10.0.20.2 key ciscoclass
R0(config)#aaa authentication login default group radius local
R0(config)#login block-for 120 attempts 5 within 60
R0(config)#login on-success log
R0(config)#login on-failure log
R0(config)#%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: 0.0.0.0]
[localport: 0] at 00:01:05 UTC Mon Mar 1 1993
```

Running-config Files

R0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R0
!
login block-for 120 attempts 5 within 60
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
```

```
!
ip dhcp excluded-address 10.0.40.1 10.0.40.100
!
ip dhcp pool Staff
 network 10.0.40.0 255.255.255.0
 default-router 10.0.40.1
 dns-server 10.0.20.2
!
!
aaa new-model
!
aaa authentication login default group radius local
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username cisco privilege 15 secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
license udi pid CISCO1941/K9 sn FTX1524813R
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
ip domain-name schreib.at
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.0.10.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.0.20.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 10.0.30.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 10.0.40.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 10.0.50.1 255.255.255.0
 ip nat inside
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool NAT 10.0.0.1 10.0.50.255 netmask 255.255.0.0
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.255.255
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
banner motd ^Cunauthorized access prohibited^C
!
radius-server host 10.0.20.2 auth-port 1645 key ciscoclass
```

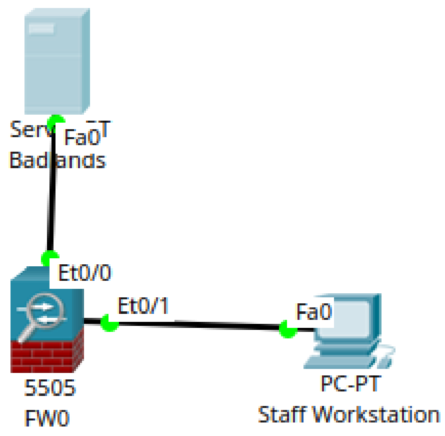
```
!
!
!
line con 0
 transport output ssh
 exec-timeout 20 0
!
line aux 0
!
line vty 0 4
 exec-timeout 20 0
 transport input ssh
 transport output ssh
line vty 5 15
 exec-timeout 20 0
 transport input ssh
 transport output ssh
!
!
!
end
```

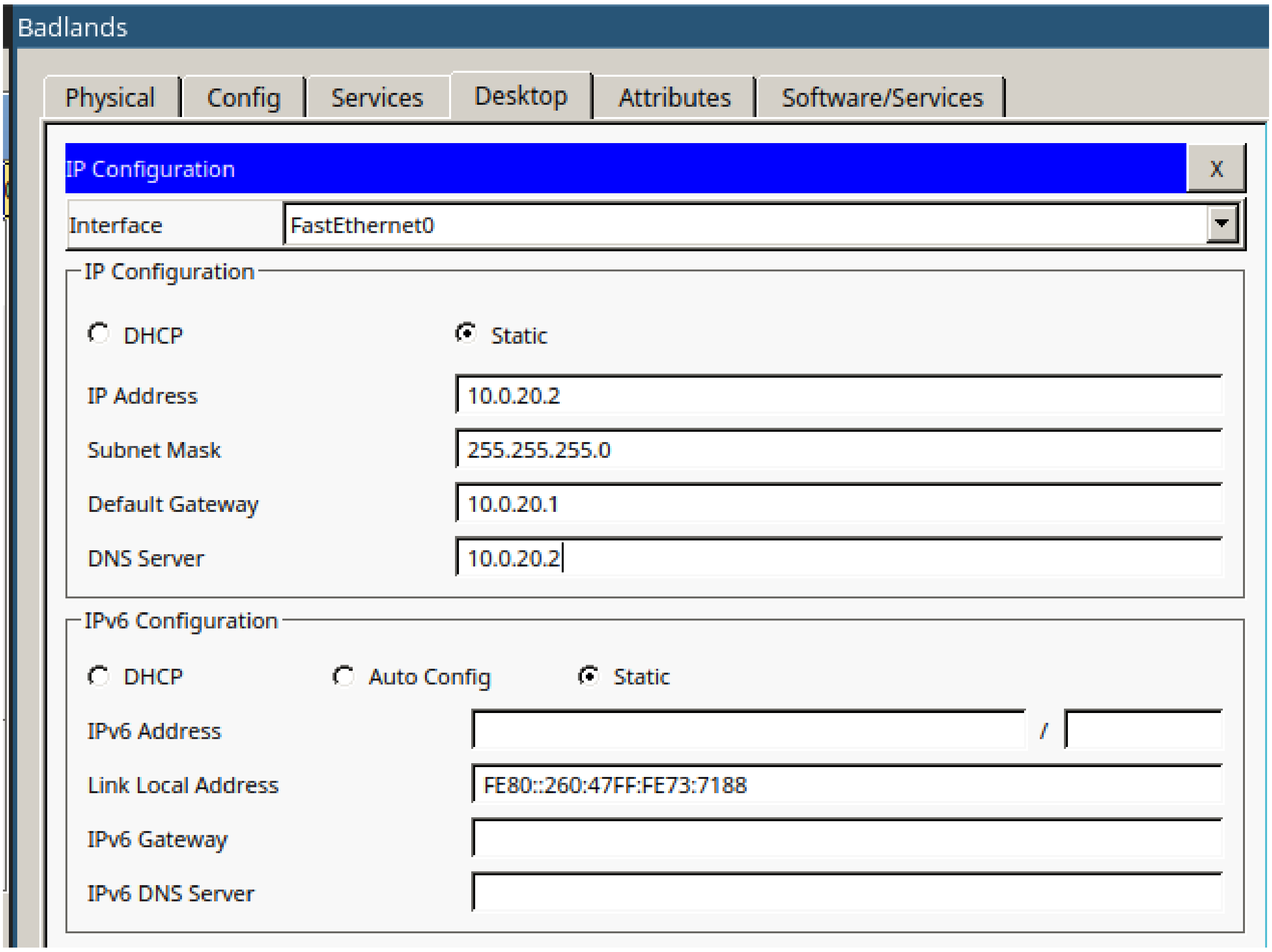
SW0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW0
!
enable secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
ip domain-name schreib.at
!
username cisco secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 switchport port-security mac-address sticky
 shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.0.0.2 255.255.255.0
!
interface Vlan10
 mac-address 00d0.ff1b.ee01
 no ip address
!
interface Vlan20
 mac-address 00d0.ff1b.ee02
 no ip address
!
interface Vlan30
 mac-address 00d0.ff1b.ee03
 no ip address
!
interface Vlan40
 mac-address 00d0.ff1b.ee04
 no ip address
!
interface Vlan50
 mac-address 00d0.ff1b.ee05
 no ip address
!
ip default-gateway 10.0.0.1
!
banner motd ^Cunauthorized access prohibited^C
!
!
!
line con 0
 login local
 exec-timeout 20 0
!
line vty 0 4
 exec-timeout 20 0
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 exec-timeout 20 0
 login local
 transport input ssh
 transport output ssh
!
!
!
end
```

ASA Konfiguration

DA die ASA im Packettracer nicht sonderlich gut simuliert wird, wird ein kleineres Netzwerk aufgebaut, um die Konfiguration der ASA durchzuführen. Indiesem mini-netzwerk werden nur die Geräte FW0, Staff Workstation und Badlands simuliert, da mehr als 2 VLANs nicht unterstützt werden.





Badlands

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 10.0.20.2

Subnet Mask: 255.255.255.0

Default Gateway: 10.0.20.1

DNS Server: 10.0.20.2

IPv6 Configuration

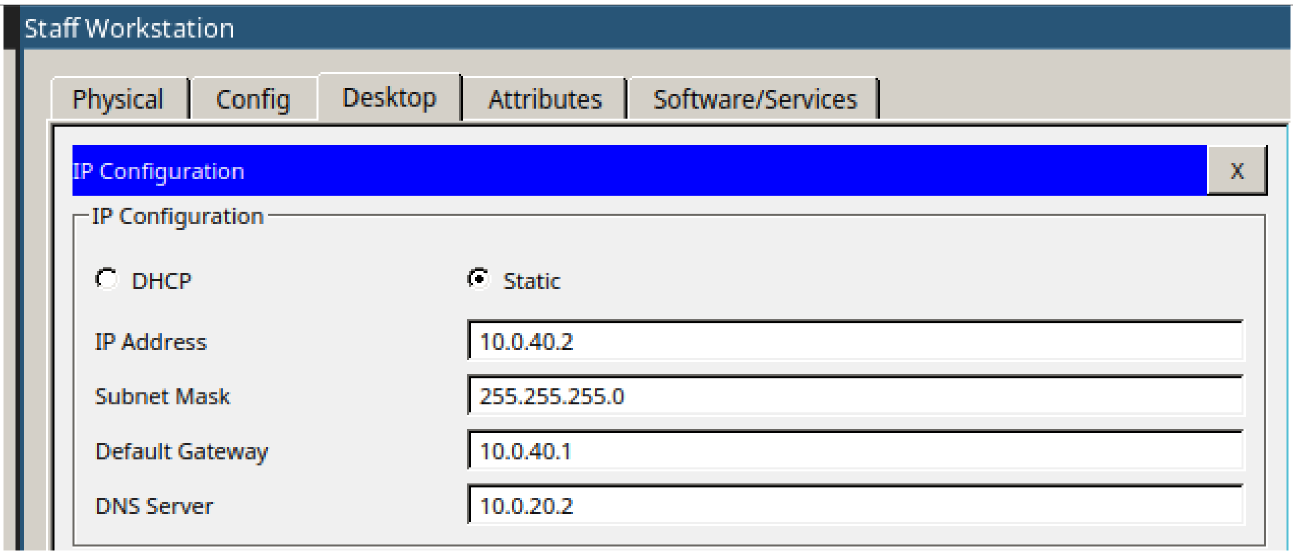
○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::260:47FF:FE73:7188

IPv6 Gateway:

IPv6 DNS Server:


Staff Workstation

IP Configuration

○ DHCP ● Static

IP Address: 10.0.40.2

Subnet Mask: 255.255.255.0

Default Gateway: 10.0.40.1

DNS Server: 10.0.20.2

Die Vlans sollten auf der echten ASA mit folgenden Security levels konfiguriert werden:

ID	Name	Security-Level
1	Management	100
2	Outside	0
10	DMZ	0
20	Intranet	40
30	VOIP	60
40	Staff	80
50	Guest	0

Alle konfigurierten access listen werden als inbound definiert. Die Acess Listen werden auf der konfiguration der ASA noch mit keinem Interface in verbindung gebracht, da diese vom Testnetzwerk und vom realen Netzwerk abweichen.

Um die DMZ nutzen zu könenn muss folgendes Kommando zusätzlich an der ASA ausgeführt werden:

```
route outside 0.0.0.0 0.0.0.0 10.0.20.1
```

Um die Outside Access-List einem Interface zuzuweißen, muss folgendes Kommando angegeben werden:

```
access-group outside in interface outside
```

Da es in der Testumgebung das Outside interface nicht exestiert, ist es nicht möglich, diese Befehle auszuführen.

Running-config der ASA

```
hostname FW0
names
!
interface Ethernet0/0
 switchport access vlan 2
```

```
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif intranet
 security-level 50
 ip address 10.0.20.1 255.255.255.0
!
interface Vlan2
 nameif staff
 security-level 100
 ip address 10.0.40.1 255.255.255.0
!
interface Vlan20
 no nameif
 no security-level
 no ip address
!
object network acadia
 host 10.0.20.1
!
!
access-list outside extended permit tcp any object acadia
access-list outside extended permit tcp any object acadia eq smtp
access-list outside extended permit tcp any object acadia eq pop3
access-list outside extended permit tcp any object acadia eq www
access-list outside extended permit tcp any object acadia eq 22
access-list outside extended permit tcp any object acadia eq 25565
access-list outside extended permit tcp any object acadia eq 1194
access-list outside extended permit tcp any object acadia eq 8001
access-list outside extended permit tcp any object acadia eq 27900
access-list outside extended permit udp any 10.0.30.0 255.255.255.0 eq 5060
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
```

```
dhcpd auto_config outside
```

http://localhost:4000/NVS/5CHIF_20170314_Schreib/