

Titel: Labor Netzwerk – Ipv6

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 13.04.2021 Abgabe: 27.04.2021

# Inhaltsverzeichnis

1	Theorie-Teil.....	1
1.1	DMZ .....	1
1.1.1	Quellen .....	1
1.1.2	Definition .....	1
1.1.3	Allgemeines .....	1
1.1.4	DMZ 3 Port Lösung .....	1
1.1.5	DMZ mit exposed Host .....	1
1.1.6	Zero Trust .....	2
1.2	ACL.....	3
1.2.1	Quellen .....	3
1.2.2	What is an ACL? .....	3
1.2.3	What Are The Components of An ACL?.....	3
2	Praxisteil .....	5
2.1	Netzwerkskizze .....	5
2.2	Netzwerke aufteilen .....	5
2.3	Konfiguration der statischen IP Adressen .....	5
2.3.1	IntGW – F0/0 Internes Netz.....	5
2.3.2	Konfiguration interne Clients .....	6
2.3.3	Konfiguration IntGW F0/1 zu ExtGW und Servern .....	7
2.3.4	Konfiguration ExtGW F0/0.....	8
2.3.5	Konfiguration interner Server .....	8
2.4	Konfigurieren der Routen.....	9
2.4.1	ExtGW:.....	9
2.4.2	IntGW .....	9
2.4.3	Ping Test aus internem Netz zu DMZ Rechner: .....	9
2.4.4	Ping Test aus internem Netz zu DNS Server im Internet, über ISP Routing: .....	10
2.5	DNS-Einträge .....	10
2.6	Test ohne ACLs .....	11
2.6.1	FTP Intern .....	11
2.6.2	Interner Webserver .....	11
2.6.3	Externer Webserver .....	12
2.7	ACLs .....	12
2.7.1	IntGW .....	12
2.7.2	ExtGW .....	14
2.8	Einrichten von SSH auf dem externen Gateway.....	14

2.9	Testen der Verbindungen mit ACLs .....	15
2.9.1	SSH Verbindung zu ExtGW .....	15
2.9.2	Interner Webserver .....	15
2.9.3	Externer Webserver .....	16
2.9.4	FTP .....	16
3	Configs .....	17
3.1	IntGW Running Config .....	17
3.2	ExtGW Running Config .....	20

# 1 Theorie-Teil

## 1.1 DMZ

### 1.1.1 Quellen

<https://www.security-insider.de/was-ist-eine-dmz-demilitarized-zone-a-677267/>

<https://www.elektronik-kompodium.de/sites/net/0907241.htm>

### 1.1.2 Definition

Bei der Demilitarized Zone (DMZ) handelt es sich um ein eigenständiges Netzwerk, das als Pufferzone zwischen einem externen Netz und dem internen Netzwerk agiert. In dem Puffernetzwerk befinden sich beispielsweise Webserver oder Mailserver, deren Kommunikation durch Firewalls überwacht ist.

### 1.1.3 Allgemeines

Die Abkürzung DMZ steht für Demilitarized Zone und bezeichnet ein speziell kontrolliertes Netzwerk, das sich zwischen dem externen Netzwerk (Internet) und dem internen Netz befindet. Es stellt eine Art Pufferzone dar, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt.

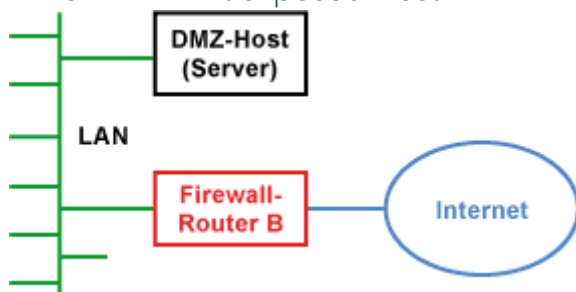
In der Demilitarized Zone befinden sich Server wie Webserver, Mailserver, Authentication-Server oder Anwendungs-Gateways. Nur diese sind für User aus dem Internet erreichbar. Durch die Trennung der DMZ vom internen Netz ist kein Zugriff für externe Anwender auf interne Ressourcen möglich. Das private Netzwerk bleibt vor Angriffen aus dem Internet oder vor Überlastung durch Internetanfragen geschützt. Die Demilitarized Zone kann durch eine oder mehrere Firewalls von den angrenzenden Netzwerken separiert sein.

### 1.1.4 DMZ 3 Port Lösung



Eine Alternative zur Zwei-Router-Lösung ist der Drei-Port-Router. In diesem Router wird eine WAN-Seite und zwei LAN-Ports konfiguriert. Ein LAN-Port wird genattet und stellt den eigentlichen LAN-Port dar. Der zweite LAN-Port wird als DMZ konfiguriert. Dahinter befindet sich der Teil des lokalen Netzwerks, der von außen erreichbar sein soll.

### 1.1.5 DMZ mit exposed Host



Der Konfigurationsaufwand für eine DMZ kann nicht unerheblich sein. Eine Alternative kann ein spezieller DMZ-Host im LAN sein. In vielen einfachen Routern wird das als DMZ bezeichnet. Es handelt sich aber um keine echte Demilitarisierte Zone, sondern um einen "Exposed Host" der alle eingehenden Datenpakete erhält, für die keine ausgehende Verbindung bekannt ist.

Die Konfiguration sieht einen Standard-Empfänger im Router vor. Dabei gibt es zwei Ansätze. Die gute Lösung leitet alle Pakete nur dann zum DMZ-Host (Exposed Host) weiter, wenn eine feste NAT-Vorgabe (Port-Forwarding bzw. DNAT) konfiguriert ist. Falls nicht, wird das Datenpaket verworfen.

Die schlechte Lösung leitet alle von außen initiierte Verbindungen an den DMZ-Host weiter. Dadurch kann der DMZ-Host mit Datenpaketen überschwemmt und ein Ausfall oder sogar das Eindringen in das betreffende System provoziert werden.

#### 1.1.6 Zero Trust

Zero Trust ist ein Sicherheitskonzept, bei dem generell jedem Netzwerkverkehr, unabhängig von seiner Herkunft, misstraut wird. Teil des Konzepts ist, dass jeder Zugriff einer Zugangskontrolle und jede Verbindung einer Verschlüsselung unterliegt.

## 1.2 ACL

### 1.2.1 Quellen

<https://www.ittsystems.com/access-control-list-acl/#:~:text=ACLs%20work%20on%20a%20set,flowing%20from%20source%20to%20destination.>

### 1.2.2 What is an ACL?

Access Control Lists “ACLs” are network traffic filters that can control incoming or outgoing traffic.

ACLs work on a set of rules that define how to forward or block a packet at the router’s interface.

An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination.

When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it.

The criteria for defining the ACL rules could be the source, the destination, a specific protocol, or more information.

ACLs are common in routers or firewalls, but they can also configure them in any device that runs in the network, from hosts, network devices, servers, etc.

### 1.2.3 What Are The Components of An ACL?

The implementation for ACLs is pretty similar in most routing platforms, all of which have general guidelines for configuring them.

Remember that an ACL is a set of rules or entries. You can have an ACL with single or multiple entries, where each one is supposed to do something, it can be to permit everything or block nothing.

When you define an ACL entry, you’ll need necessary information.

**Sequence Number:**

Identify an ACL entry using a number.

**ACL Name:**

Define an ACL entry using a name. Instead of using a sequence of numbers, some routers allow a combination of letters and numbers.

**Remark:**

Some Routers allow you to add comments into an ACL, which can help you to add detailed descriptions.

**Statement:**

Deny or permit a specific source based on address and wildcard mask. Some routing devices, such as Cisco, configure an implicit deny statement at the end of each ACL by default.

**Network Protocol:**

Specify whether deny/permit IP, IPX, ICMP, TCP, UDP, NetBIOS, and more.

**Source or Destination:**

Define the Source or Destination target as a Single IP, a Address Range (CIDR), or all Addresses.

**Log:**

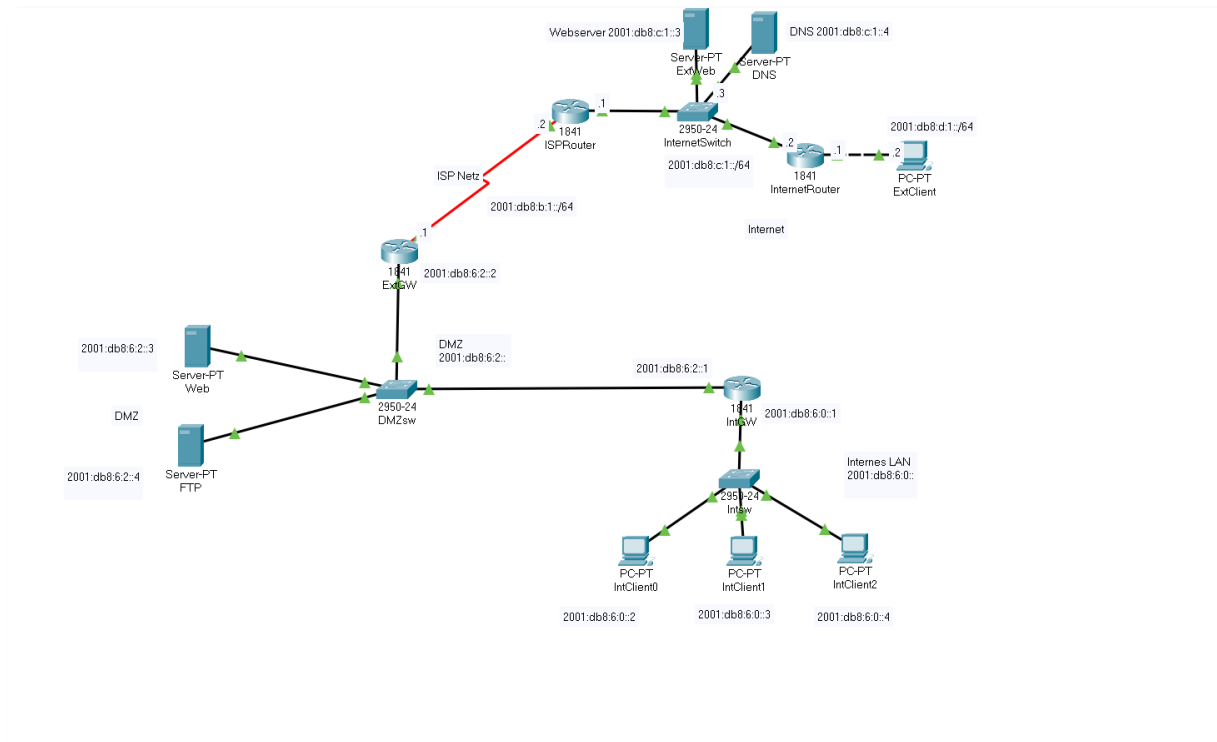
Some devices are capable of keeping logs when ACL matches are found.

**Other Criteria:**

Advanced ACLs allow you to use control traffic through the Type of Service (ToS), IP precedence, and differentiated services codepoint (DSCP) priority.

## 2 Praxisteil

### 2.1 Netzwerkskizze



### 2.2 Netzwerke aufteilen

#### POSSIBLE NETWORKS

First Network: 2001:db8:6::/49

Last Network: 2001:db8:6:8000::/49

### 2.3 Konfiguration der statischen IP Adressen

#### 2.3.1 IntGW - F0/0 Internes Netz

IntGW zu Internem Netzwerk: F0/0: 2001:db8:6:0::1/64

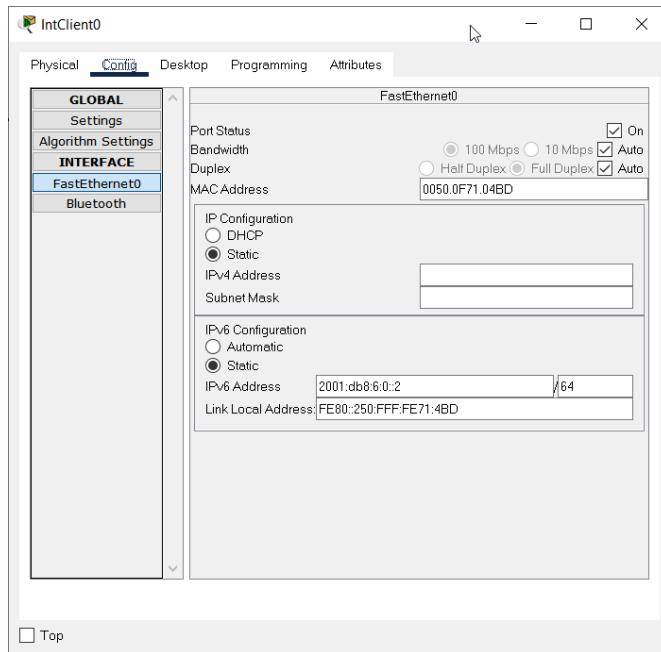
```
IntGw(config)#int f0/0
IntGw(config-if)#ipv6 unicast-routing
IntGw(config)#int f0/0
IntGw(config-if)#ipv6 add 2001:db8:6:0::1/64
IntGw(config-if)#no shut
```



## 2.3.2 Konfiguration interne Clients

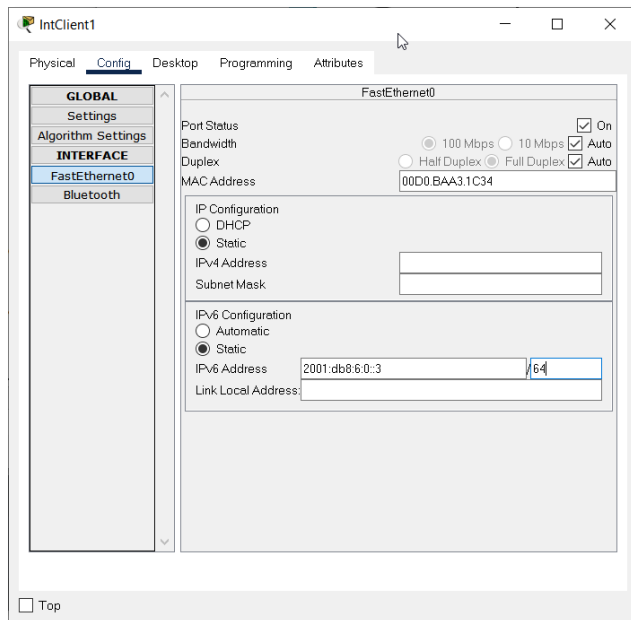
### 2.3.2.1 IntClient0

IntClient0: 2001:db8:6:0::2/64



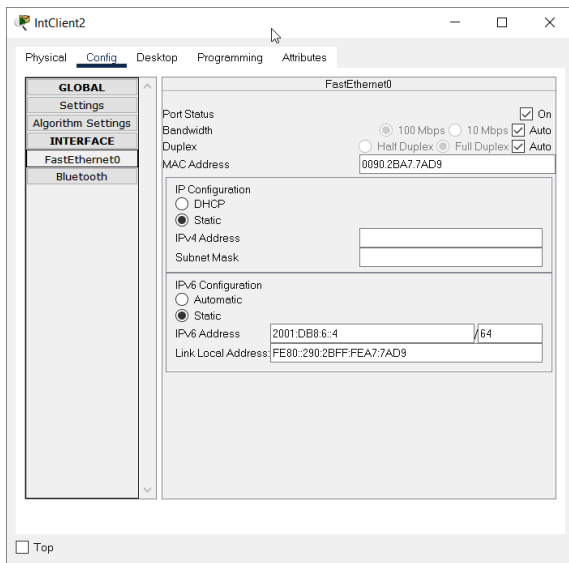
### 2.3.2.2 IntClient1

IntClient1: 2001:db8:6:0::3/64



### 2.3.2.3 IntClient2

IntClient 2: 2001:db8:6:0::4/64



### 2.3.2.4 Ping Test IntGW

```
C:\>ping 2001:db8:6:0::1

Pinging 2001:db8:6:0::1 with 32 bytes of data:

Reply from 2001:DB8:6::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:6::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:6::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:6::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:6::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

### 2.3.3 Konfiguration IntGW F0/1 zu ExtGW und Servern

IP: 2001:db8:6:2::1/64

```
IntGw(config)#int f0/1
IntGw(config-if)#ipv6 unicast-routing
IntGw(config)#int f0/1
IntGw(config-if)#ipv6 add 2001:db8:6:2::1/64
IntGw(config-if)#no shut
```

### 2.3.4 Konfiguration ExtGW F0/0

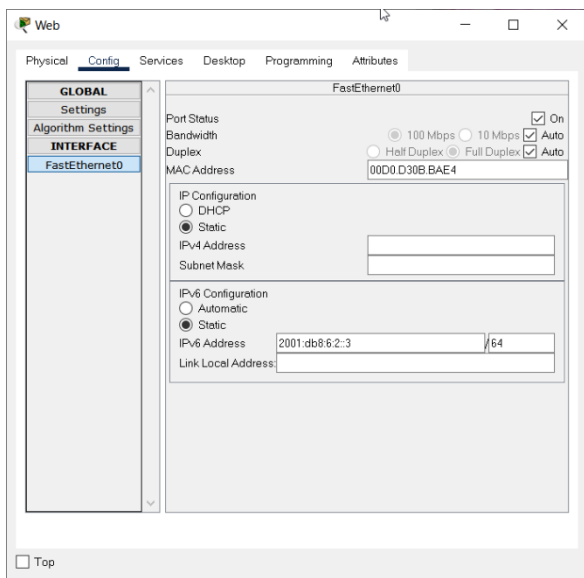
IP: 2001:db8:6:2::2/64

```
ExtGW(config)#int f0/0
ExtGW(config-if)#ipv6 unicast-routing
ExtGW(config)#int f0/0
ExtGW(config-if)#ipv6 add 2001:db8:6:2::2/64
ExtGW(config-if)#no shut
```

### 2.3.5 Konfiguration interner Server

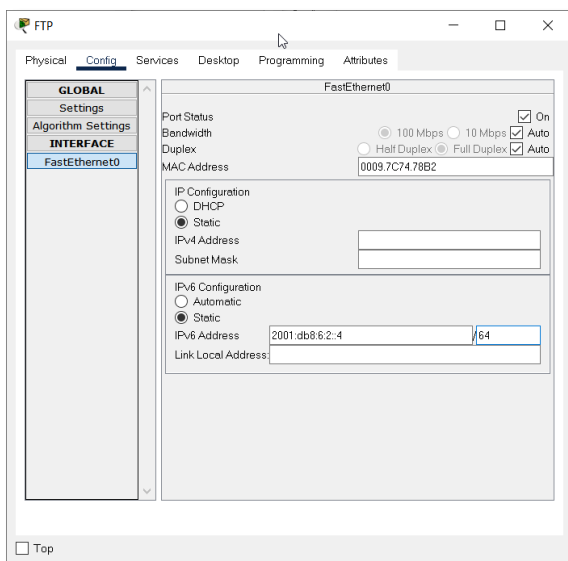
#### 2.3.5.1 Webserver

IP: 2001:db8:6:2::3/64



#### 2.3.5.2 FTP Server

IP: 2001:db8:6:2::4/64



## 2.4 Konfigurieren der Routen

### 2.4.1 ExtGW:

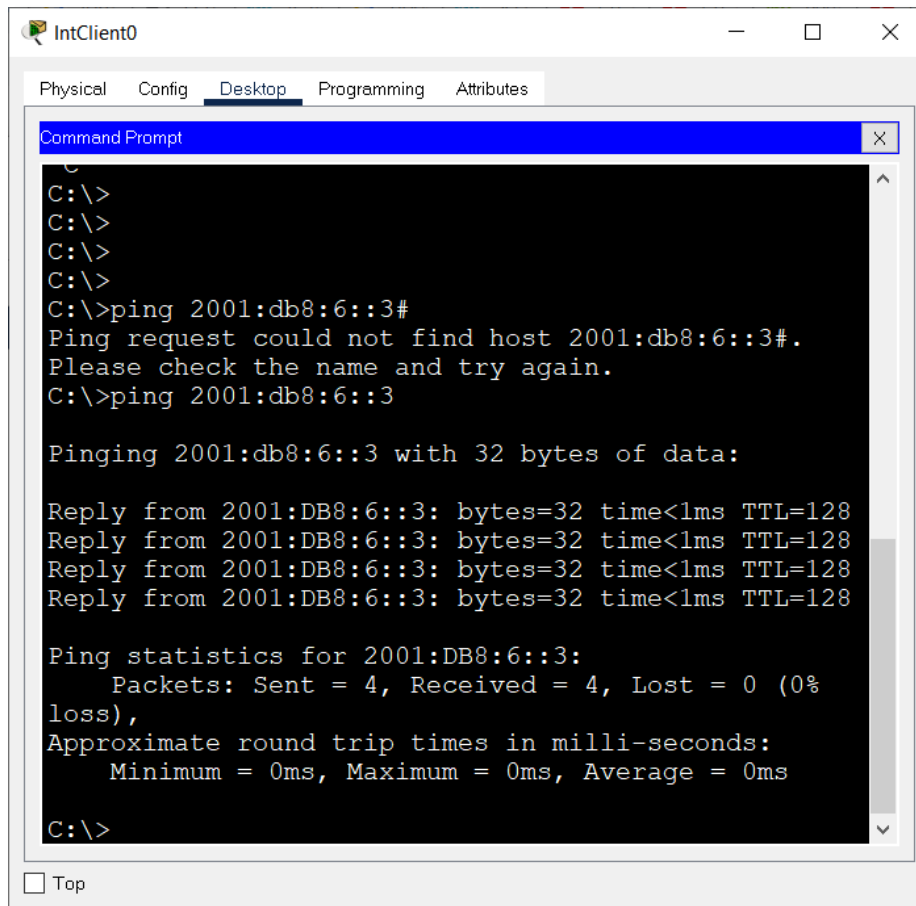
```
ipv6 route <SUBNET> <NEXT HOP>
```

```
ExtGW(config)#ipv6 route 2001:db8:6:0::/64 2001:db8:6:2::1
```

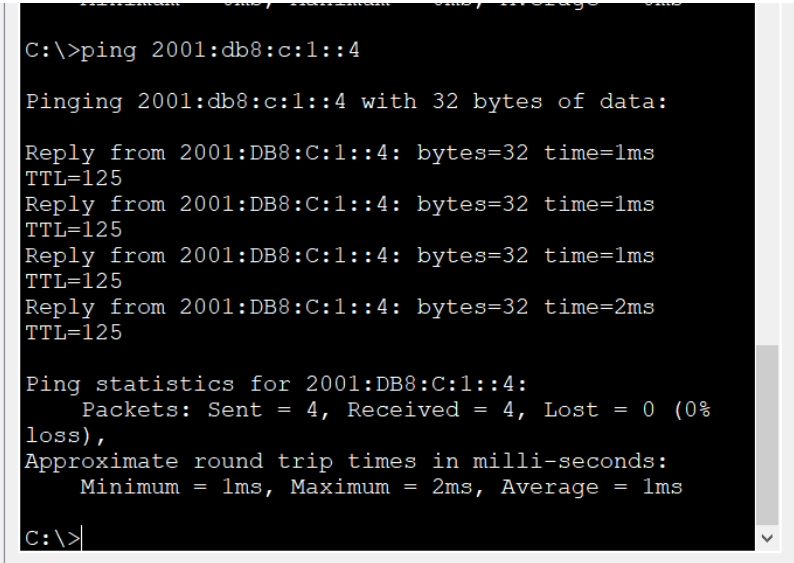
### 2.4.2 IntGW

```
IntGw(config)#ipv6 route ::/0 2001:db8:6:2::2
```

### 2.4.3 Ping Test aus internem Netz zu DMZ Rechner:



#### 2.4.4 Ping Test aus internem Netz zu DNS Server im Internet, über ISP Routing:



```
C:\>ping 2001:db8:c:1::4

Pinging 2001:db8:c:1::4 with 32 bytes of data:

Reply from 2001:DB8:C:1::4: bytes=32 time=1ms
TTL=125
Reply from 2001:DB8:C:1::4: bytes=32 time=1ms
TTL=125
Reply from 2001:DB8:C:1::4: bytes=32 time=1ms
TTL=125
Reply from 2001:DB8:C:1::4: bytes=32 time=2ms
TTL=125

Ping statistics for 2001:DB8:C:1::4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

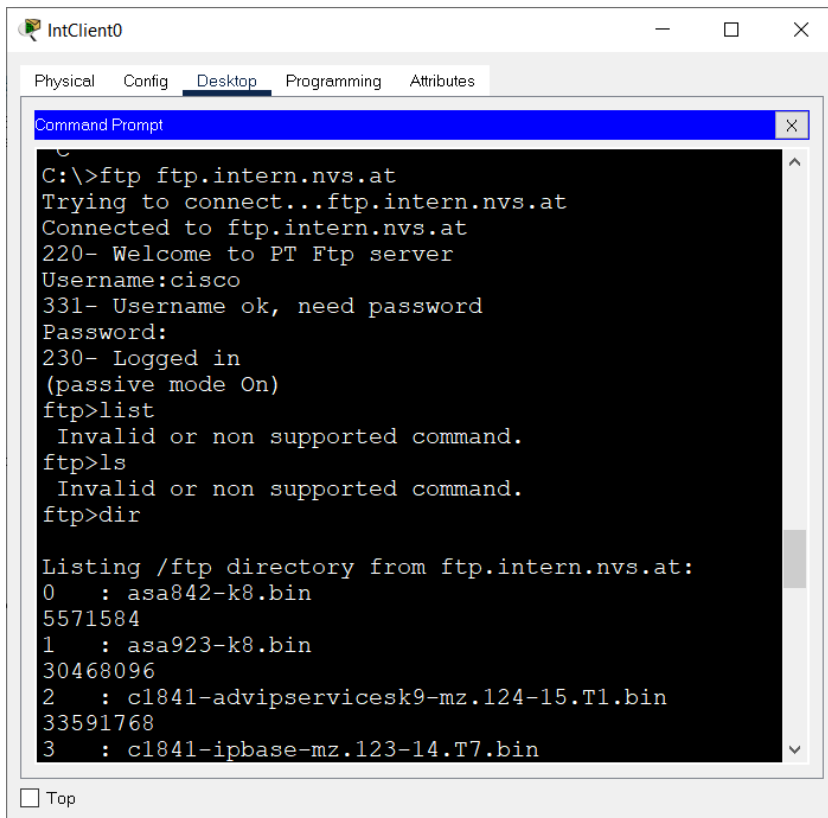
☐ Top

#### 2.5 DNS-Einträge

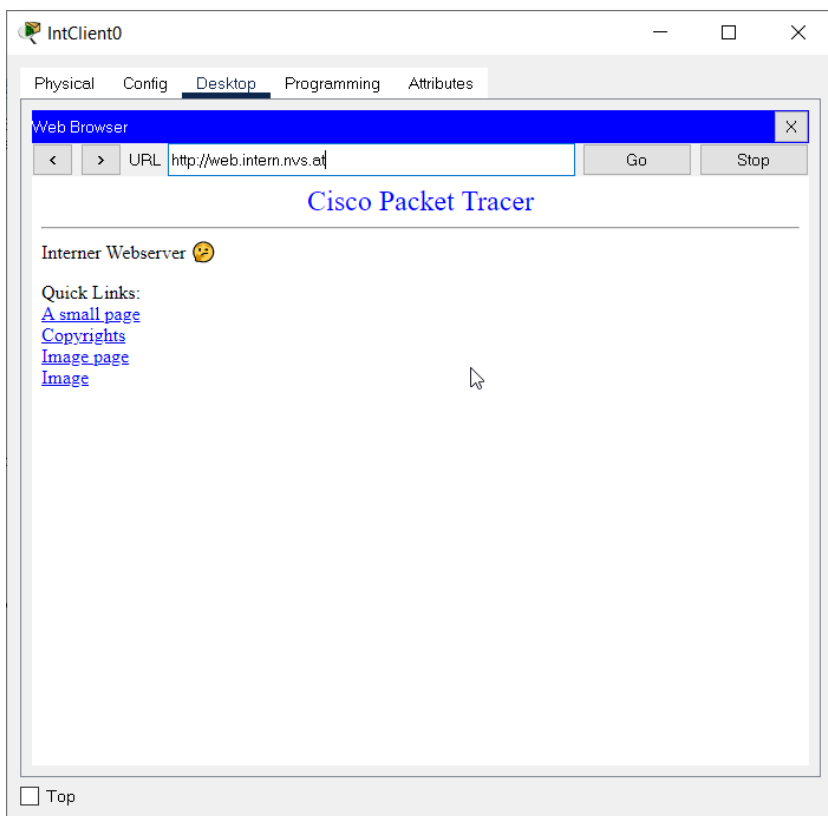
No.	Name	Type	Detail
0	ftp.intern.nvs.at	A Record	2001:DB8:6:2::4
1	web.intern.nvs.at	A Record	2001:DB8:6:2::3
2	www.nvs.at	A Record	2001:DB8:C:1::3

## 2.6 Test ohne ACLs

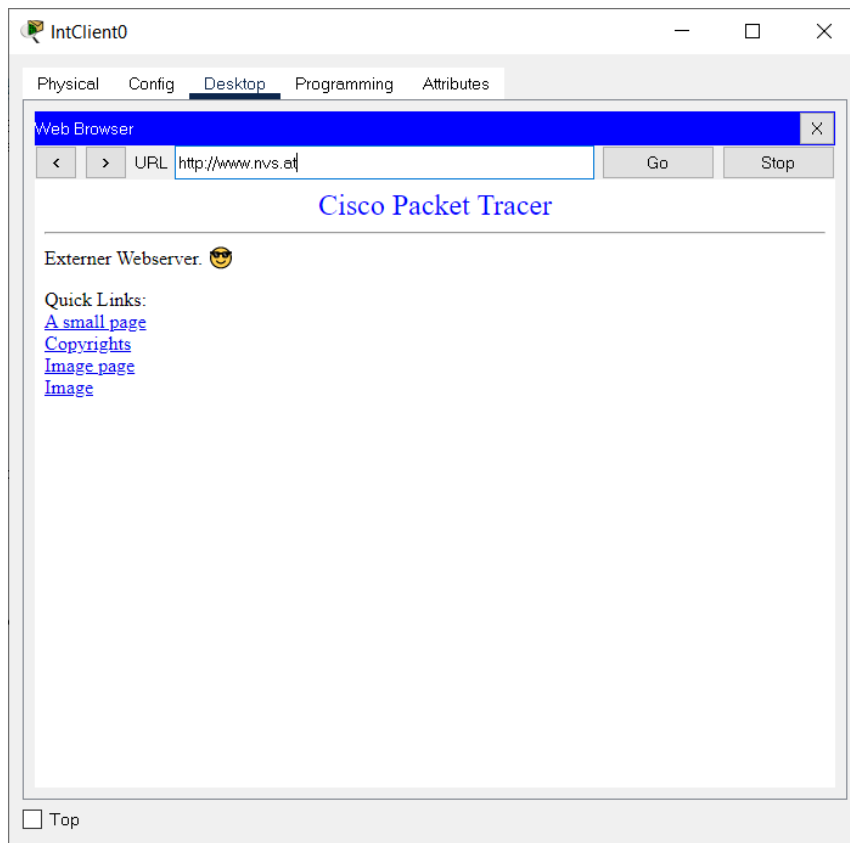
### 2.6.1 FTP Intern



### 2.6.2 Interner Webserver



## 2.6.3 Externer Webserver



## 2.7 ACLs

### 2.7.1 IntGW

```
no ipv6 access - list LAN_INT_OUT
ipv6 access - list LAN_INT_OUT

remark IntGW
remark for Interface f0/0 aka Internal Network

remark Erlaube HTTP Zugriff
permit tcp 2001:db8:6:0::/64 any eq 80

remark Erlaube HTTPS Zugriff
permit tcp 2001:db8:6:0::/64 any eq 443

remark Erlaube FTP Zugriff auf internen Server
permit tcp 2001:db8:6:0::/64 host 2001:db8:6:2::4 eq 21
```

```
remark Erlaube nur von IntClient0 SSH Zugriff
permit tcp 2001:db8:6:0::1 any eq 22

remark Erlaube DNS Zugriff
permit tcp 2001:db8:6:0::/64 host 2001:db8:c:1::4 eq 53
permit udp 2001:db8:6:0::/64 host 2001:db8:c:1::4 eq 53

remark Erlaube Ping ICMP Tests
permit udp tcp 2001:db8:6:0::/64 any

no ipv6 access-list LAN_INT_IN
ipv6 access-list LAN_INT_IN

remark IntGW
remark Workaround, da Packettracer mit any any alles durchlaesst,
also effektiv die Firewall nutzlos macht

remark for interface f0/1

remark HTTP & HTTPS
permit tcp any eq 80 any
permit tcp any eq 443 any

remark FTP
permit tcp any eq 21 any

remark DNS
permit tcp any eq 53 any
permit udp any eq 53 any

remark SSH Zugriff
permit tcp host 2001:db8:6:0::2 eq 22 host 2001:db8:6:0::1
```



### 2.7.2 ExtGW

```
no ipv6 access - list LAN_EXT_IN
ipv6 access - list LAN_EXT_IN
remark ExtGW
remark for interface se0/0/0
remark HTTP(S)
permit tcp any host 2001:db8:6:2::3 eq 80
permit tcp any host 2001:db8:6:2::3 443
remark FTP
permit tcp any host 2001:db8:6:2::4 eq 21
remark DNS
permit tcp host 2001:db8:c:1::4 eq 53 any
permit udp host 2001:db8:c:1::4 eq 53 any

remark Erlaube jeglichen HTTP(S) Traffic ins Internet ueber ExtGW
permit tcp any eq 80 any
permit tcp any eq 443 any
```

## 2.8 Einrichten von SSH auf dem externen Gateway

```
ExtGW(config)#ip domain-name niklas.lan
ExtGW(config)#crypto key generate rsa
The name for the keys will be: ExtGW.niklas.lan
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.

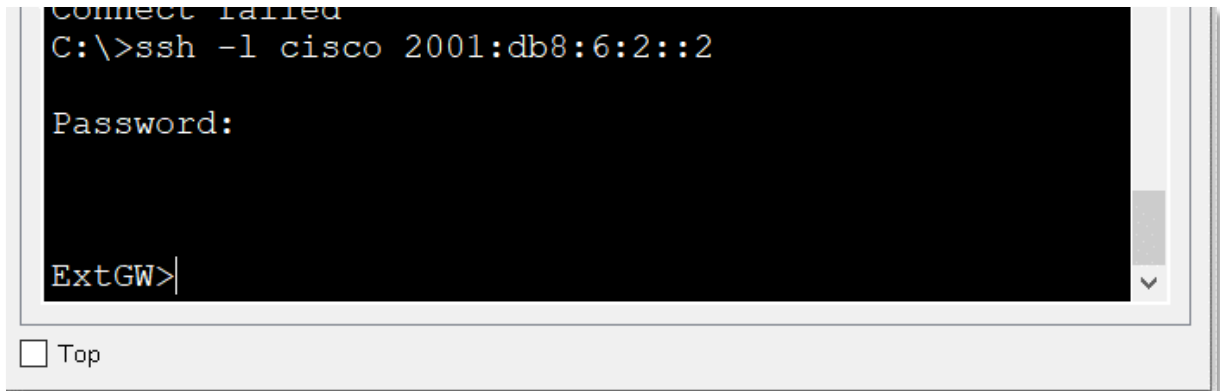
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

ExtGW(config)#
*Mar 2 1:51:16.96: RSA key size needs to be at least 768 bits for
ssh version 2
*Mar 2 1:51:16.96: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

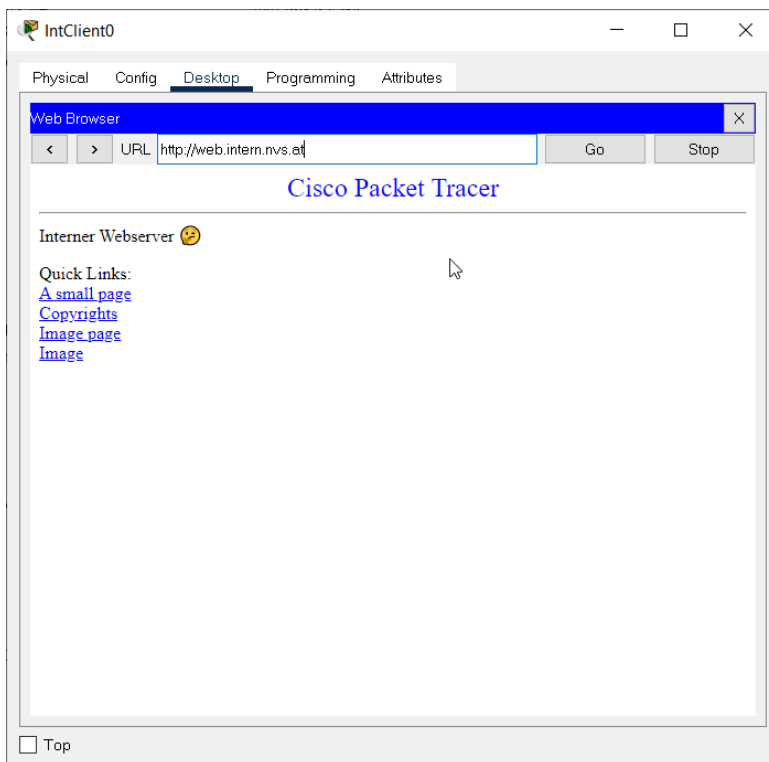
```
ExtGW(config)#line vty 0 4
ExtGW(config-line)#transport input ssh
ExtGW(config-line)#login local
ExtGW(config-line)#exit
ExtGW(config)#username cisco password cisco
```

## 2.9 Testen der Verbindungen mit ACLs

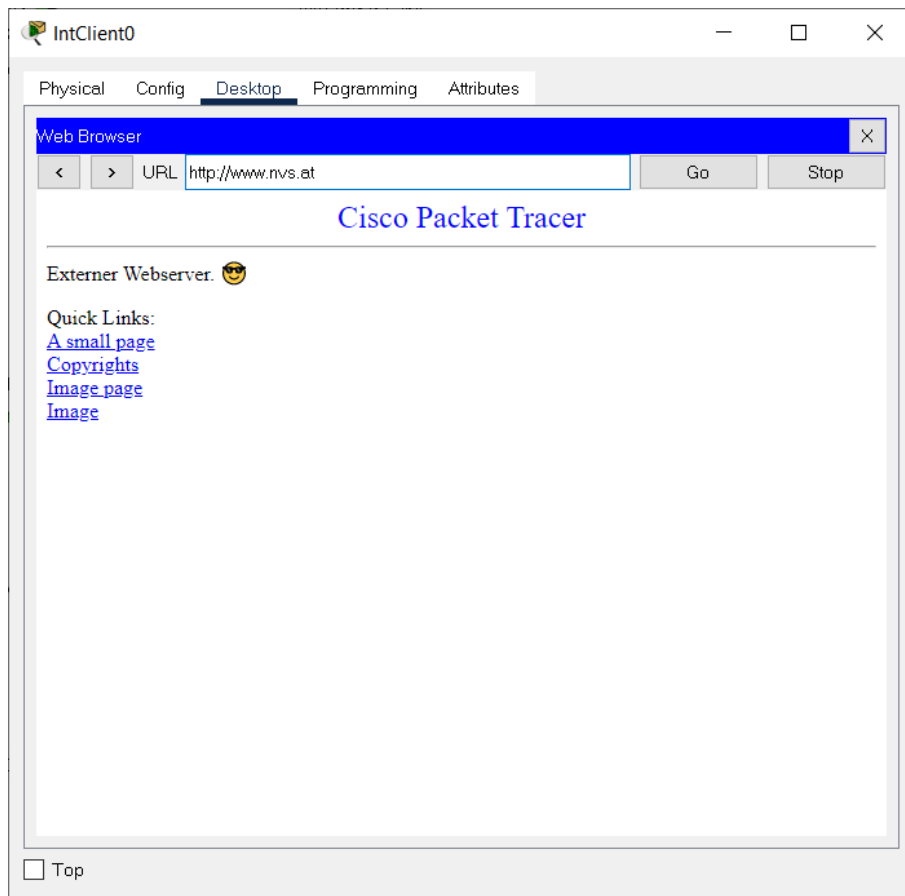
### 2.9.1 SSH Verbindung zu ExtGW



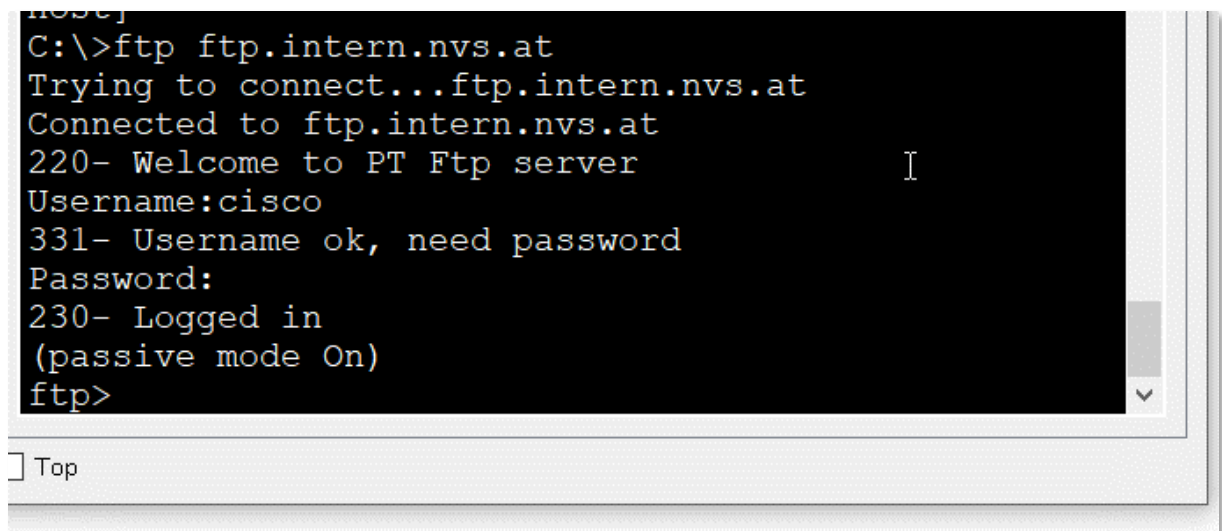
### 2.9.2 Interner Webserver



### 2.9.3 Externer Webserver



### 2.9.4 FTP



## 3 Configs

### 3.1 IntGW Running Config

```
IntGw#show run
Building configuration...

Current configuration : 1647 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname IntGw
!
!
!
!
!
!
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
!
!
!
!
```

```
!  
!  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
no ip address  
duplex auto  
speed auto  
ipv6 address 2001:DB8:6::1/64  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
ipv6 address 2001:DB8:6:2::1/64  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9  
!  
ipv6 route ::/0 2001:DB8:6:2::2
```

```
!  
  
ipv6 access-list LAN_INT_OUT  
remark IntGW  
remark for Interface f0/0 aka Internal Network  
remark Erlaube HTTP Zugriff  
permit tcp 2001:DB8:6::/64 any eq www  
remark Erlaube HTTPS Zugriff  
permit tcp 2001:DB8:6::/64 any eq 443  
remark Erlaube FTP Zugriff auf internen Server  
permit tcp 2001:DB8:6::/64 host 2001:DB8:6:2::4 eq ftp  
remark Erlaube nur von IntClient0 SSH Zugriff  
remark Erlaube DNS Zugriff  
permit tcp 2001:DB8:6::/64 host 2001:DB8:C:1::4 eq domain  
permit udp 2001:DB8:6::/64 host 2001:DB8:C:1::4 eq domain  
remark Erlaube Ping ICMP Tests  
ipv6 access-list LAN_INT_IN  
remark IntGW  
  
remark Workaround, da Packettracer mit any any alles durchlaesst,  
also effektiv die Firewall nutzlos macht  
remark for interface f0/1  
remark HTTP & HTTPS  
permit tcp any eq www any  
permit tcp any eq 443 any  
remark FTP  
permit tcp any eq ftp any  
remark DNS  
permit tcp any eq domain any  
permit udp any eq domain any  
remark SSH Zugriff  
permit tcp host 2001:DB8:6::2 eq 22 host 2001:DB8:6::1  
  
!  
  
!  
  
!
```

```
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
!  
!  
!  
end
```

### 3.2 ExtGW Running Config

```
ExtGW#show run  
Building configuration...  
  
Current configuration : 1377 bytes  
!  
version 12.4  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname ExtGW  
!  
!  
!  
!  
!  
!  
!  
!
```

```
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username cisco password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name niklas.lan
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:6:2::2/64
```



```
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/0/0  
no ip address  
ipv6 address 2001:DB8:B:1::1/64  
!  
interface Serial0/0/1  
no ip address  
clock rate 2000000  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9  
!  
ipv6 route ::/0 2001:DB8:B:1::2  
ipv6 route 2001:DB8:6::/64 2001:DB8:6:2::1  
!  
ipv6 access-list LAN_EXT_IN  
remark ExtGW  
remark for interface se0/0/0  
remark HTTP(S)  
permit tcp any host 2001:DB8:6:2::3 eq www
```

```
permit tcp any host 2001:DB8:6:2::3 eq 443
remark FTP
permit tcp any host 2001:DB8:6:2::4 eq ftp
remark DNS
permit tcp host 2001:DB8:C:1::4 eq domain any
permit udp host 2001:DB8:C:1::4 eq domain any
remark Erlaube jeglichen HTTP(S) Traffic ins Internet ueber ExtGW
permit tcp any eq www any
permit tcp any eq 443 any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
!
!
end
```