Abteilung für INFORMATIK

HTL ST. PÖLTEN

Titel: Labor Unternehmensnetzwerk

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 02.03.2021 Abgabe: 23.03.2021

Inhaltsverzeichnis

1 Theorie-Teil

1.1 NAT

https://de.wikipedia.org/wiki/Netzwerkadress%C3%BCbersetzung

https://www.elektronik-kompendium.de/sites/net/0812111.htm

1.1.1 Warum NAT?

Die ersten IPv4-Netze waren anfangs eigenständige Netz ohne Verbindung nach außen. Hier begnügte man sich mit IPv4-Adressen aus den privaten Adressbereichen. Parallel dazu kam es bereits Ende der 1990er Jahre zu Engpässen bei öffentlichen IPv4-Adressen. Die steigende Anzahl der Einwahlzugänge über das Telefonnetz mussten mit IPv4-Adressen versorgt werden.
Bis heute bekommt ein Internet-Anschluss nur eine IPv4-Adresse für ein Gerät. Damals war es undenkbar, dass an einem Internet-Anschluss ein ganzes Heimnetzwerk betrieben wird. Wenn ein Haushalt einen PC per Modem an das Telefonnetz angeschlossen und sich ins Internet eingewählt hat, dann war das schon etwas besonderes.

Heute betreibt jeder Haushalt mit Internet-Zugang sein eigenes lokales Netzwerk, in dem jedes Endgerät eine IPv4-Adresse braucht. In solchen Fällen bekommen die Geräte IPv4-Adressen aus den privaten Adressräumen 10.0.0.0/8, 192.168.0.0/16 oder 172.16.0.0/12 zugeteilt, um die wenige öffentlichen IPv4-Adressen einzusparen.
Allerdings sind private IPv4-Adressen nicht routbar. Das heißt, mit ihnen kann man keine Verbindung ins Internet aufbauen. Deshalb wurde mit NAT ein Verfahren eingeführt, bei dem in ausgehenden Datenpaketen die private IP-Adresse gegen eine öffentliche IP-Adresse ausgetauscht wird.

1.1.2 Vorteile

- NAT hilft die Verknappung der IPv4 Adressen zu entschleunigen. Dies geschieht durch die Ersetzung mehrerer Adressen für mehrere Endsysteme durch eine einzige IP-Adresse.[4]
- IP-Adressen eines Netzes können vor einem anderen Netz verborgen werden. Somit kann NAT zur Verbesserung der Privatsphäre eingesetzt werden.
- Dieselben IP-Adressbereiche können von mehreren abgeschlossenen privaten Netzwerken verwendet werden, ohne dass es zu Adresskollisionen kommt, da nach außen nur die IP-Adresse des NAT-Routers sichtbar ist.

1.1.3 Nachteile

- Ein Problem an NAT ist, dass die saubere Zuordnung „1 Host mit eindeutiger IP-Adresse“ nicht eingehalten wird.Durch die Umschreibung von Protokoll-Headern, die einem Man-in-the-middle-Angriff ähnelt, haben so insbesondere ältere Protokolle und Verschlüsselungsverfahren auf Netzwerk- und Transportebene durch diesen Designbruch Probleme (zum Beispiel. IPsec-AH). Protokollkomplikationen durch NAT werden in RFC 3027 beschrieben.
- Ebenso leiden insbesondere Netzwerkdienste, die Out-of-Band-Signalisierung und Rückkanäle einsetzen, etwa IP-Telefonie-Protokolle, unter Komplikationen durch NAT-Gateways.
- Das Ende-zu-Ende Prinzip wird verletzt, indem der NAT-Router das IP-Paket bzw. TCP-Segment verändert, ohne dass er selbst der verschickende Host ist.

1.2 ACL

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

1.2.1 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.

1.2.2 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.

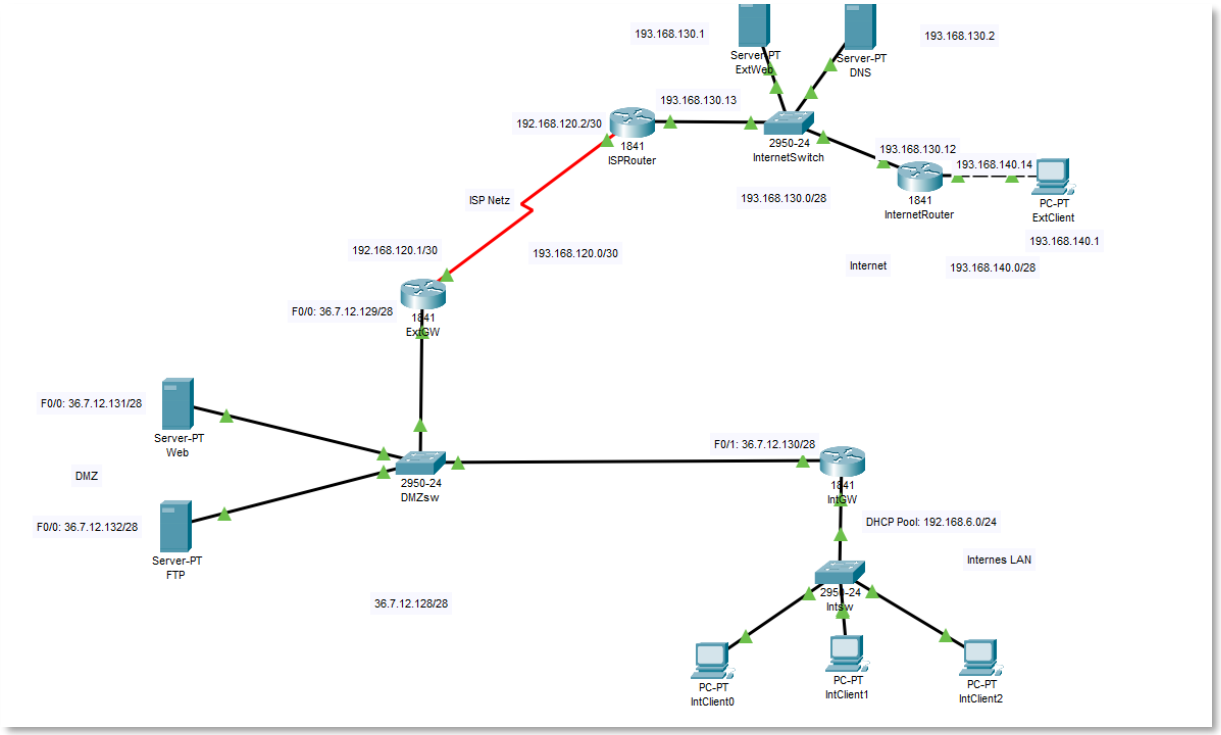
Source or Destination:
Define the Source or Destination target as a Single IP, a Address Range (CIDR), or all Addresses.

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 Konfigurieren von IntGW als DHCP Server

2.2.1 Einstellen des Ethernet Interfaces welches zum Switch geht

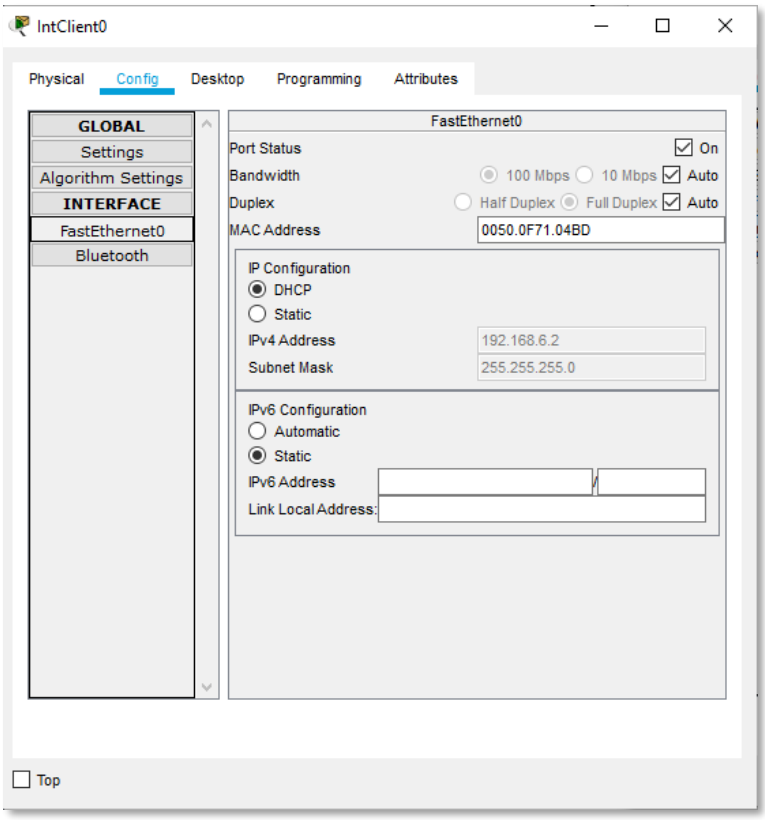
```
IntGw(config)#int f0/0
IntGw(config-if)#ip address 192.168.6.1 255.255.255.0
IntGw(config-if)#no shut
```

2.2.2 DHCP Pool erstellen

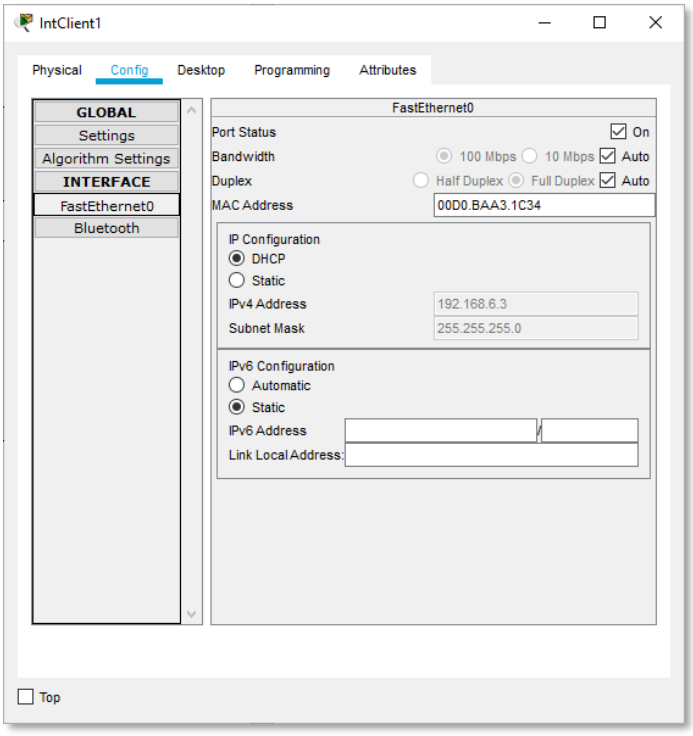
```
IntGw(config)#ip dhcp pool intlan
IntGw(dhcp-config)#network 192.168.6.0 255.255.255.0
IntGw(config)#exit
IntGw(dhcp-config)#ip dhcp pool intlan
IntGw(dhcp-config)#default-router 192.168.6.1
IntGw(dhcp-config)#dns-server 193.168.130.2
IntGw(dhcp-config)#ip dhcp excluded-address 192.168.6.1
```

2.2.3 Testen ob interne Clients IPs bekommen

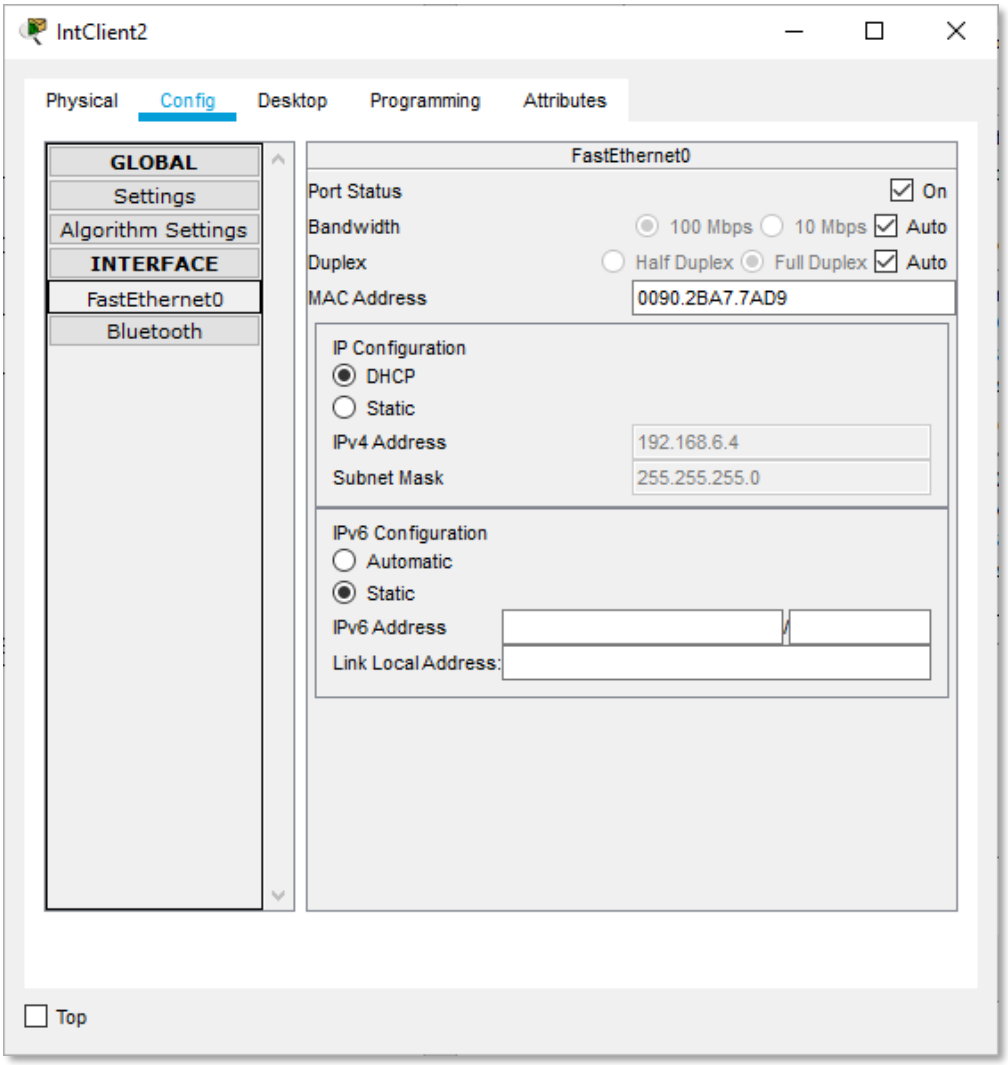
2.2.3.1 Client 1



2.2.3.2 Client 2



2.2.3.3 Client 3:



2.3 Vergeben der IPs aus dem Netzwerk 36.7.12.128/28

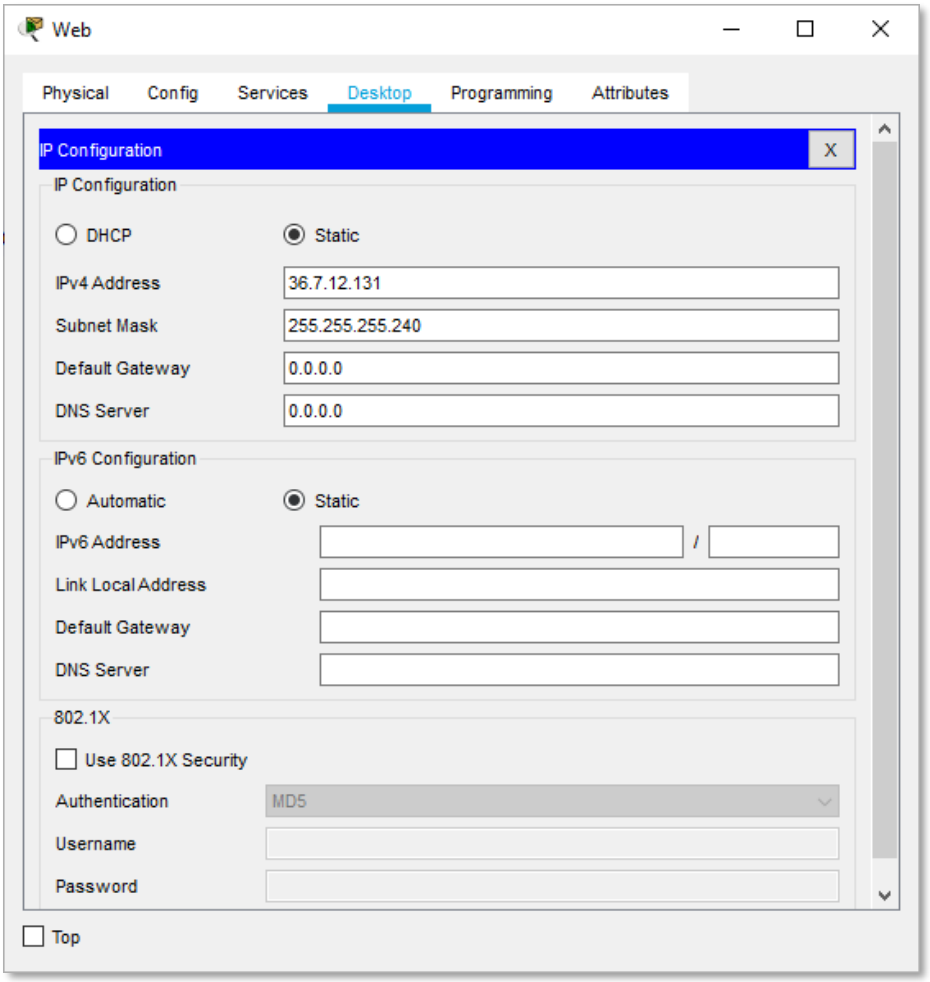
2.3.1 Externer Gateway

```
ExtGW(config)#int f0/0

ExtGW(config-if)#ip address 36.7.12.129 255.255.255.240

ExtGW(config-if)#no shut
```

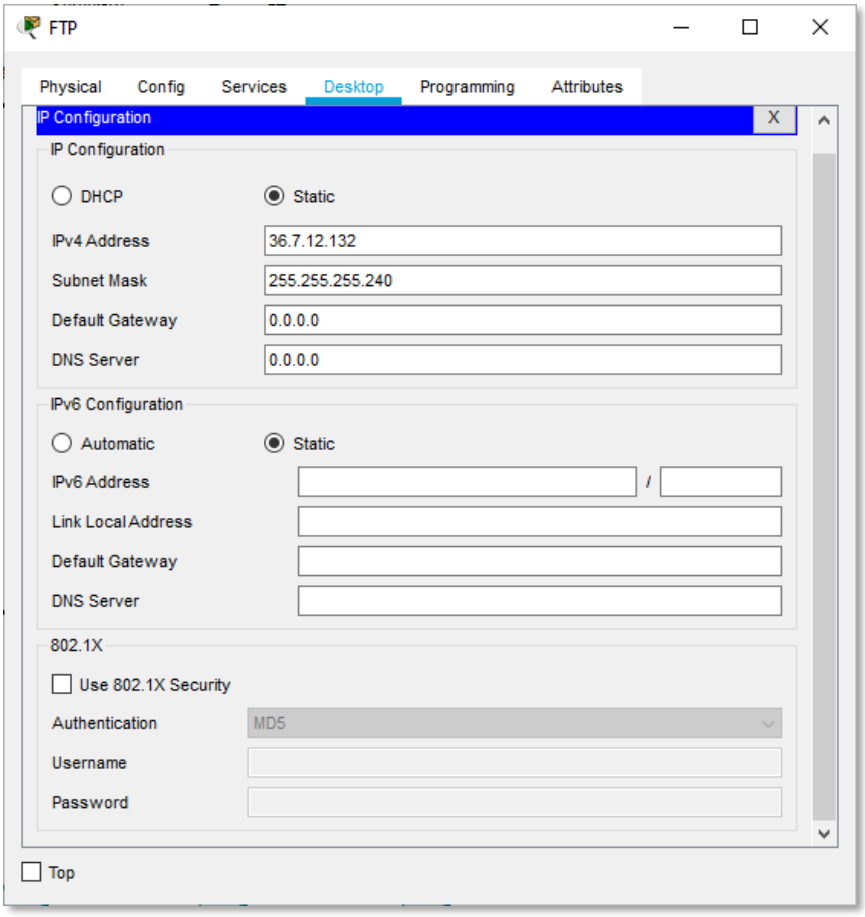
2.3.2 Interner Gateway

```
IntGw(config)#int f0/1

IntGw(config-if)#ip address 36.7.12.130 255.255.255.240

IntGw(config-if)#no shut
```

2.3.3 Web Server Konfiguration



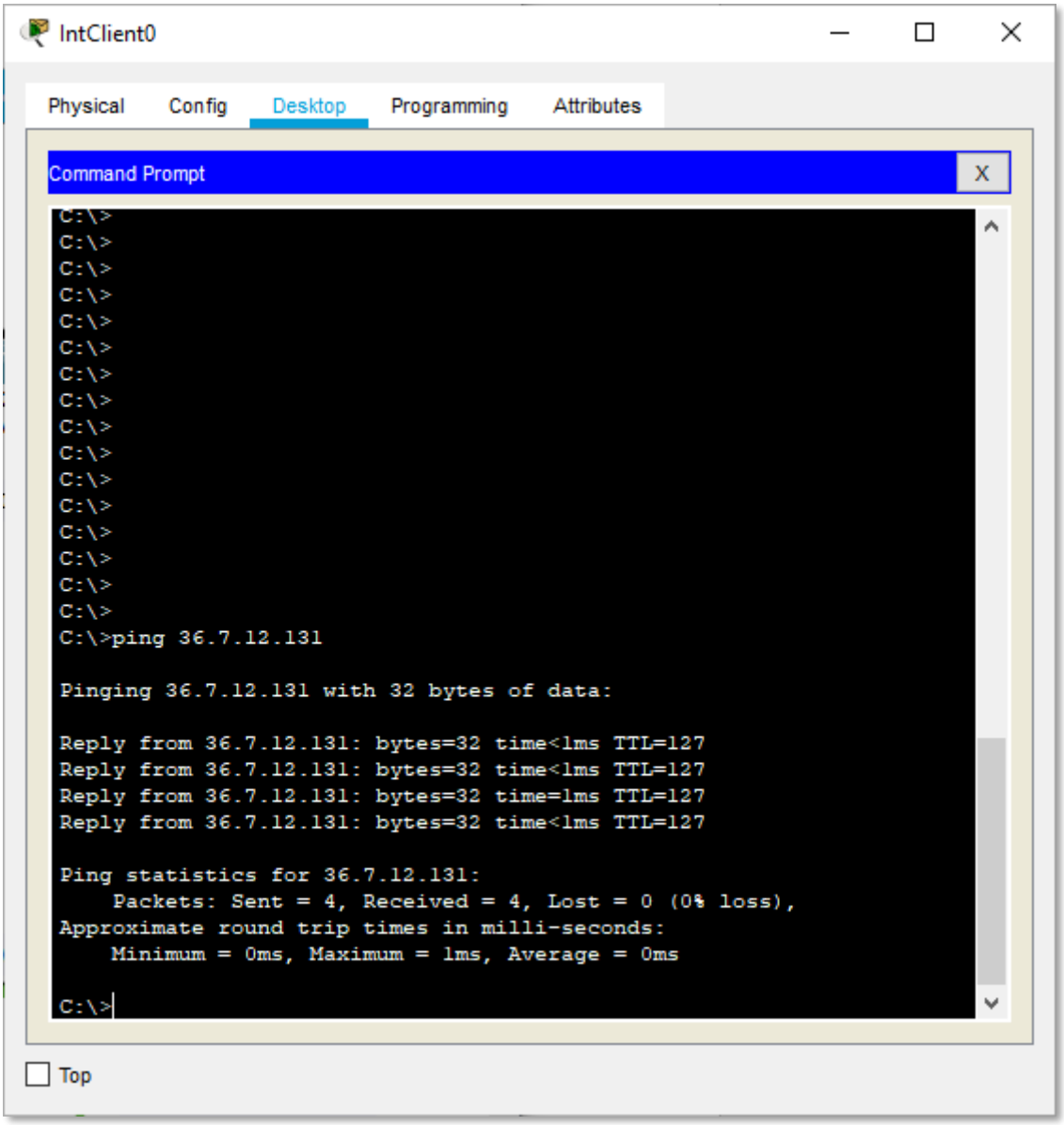
2.3.4 FTP Server Konfiguration



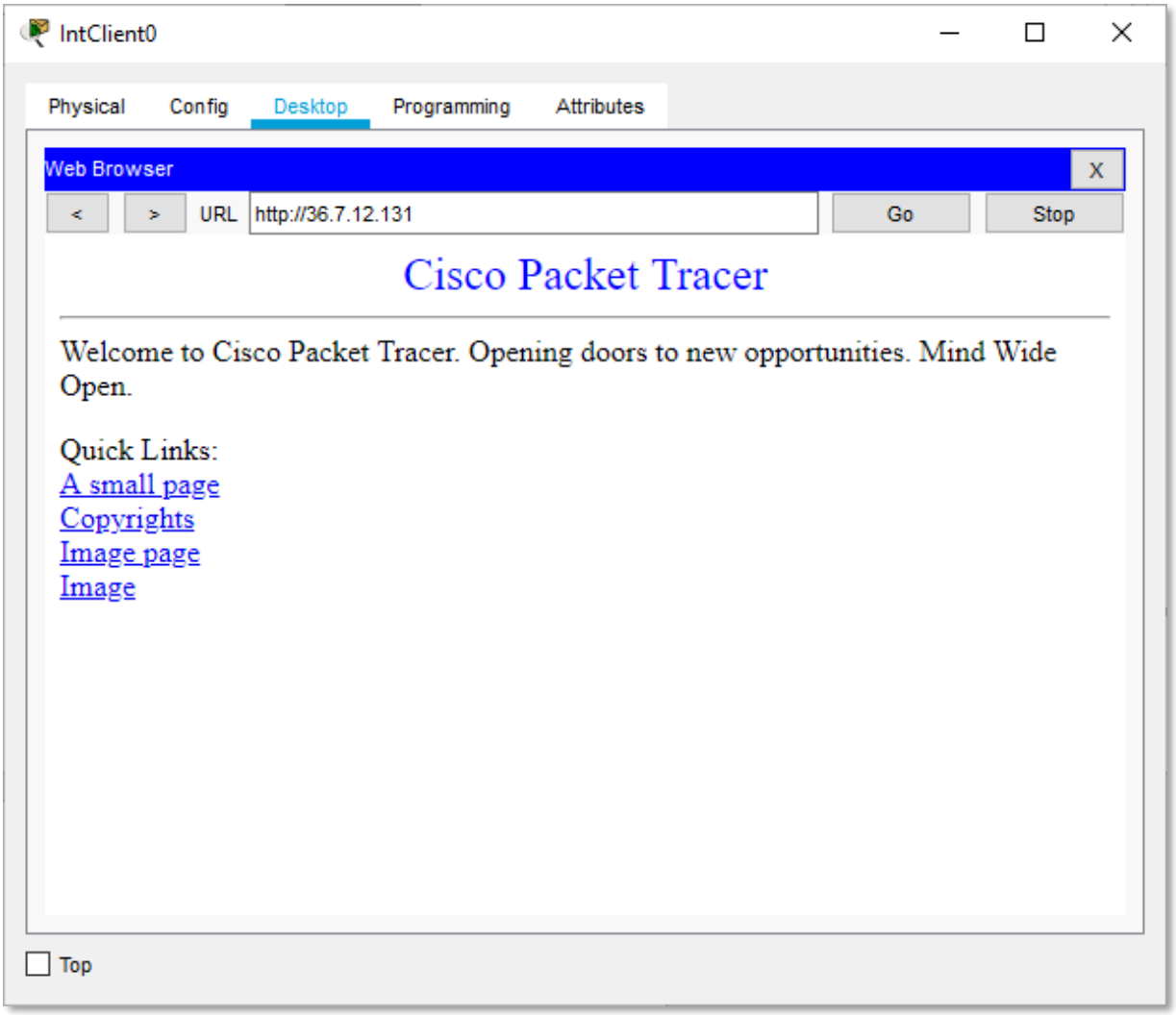
2.4 Konfigurieren des internen Gateways

```
IntGw(config)#access-list 1 permit 192.168.6.0 0.0.0.255

IntGw(config)#ip nat inside source list 1 interface f0/1

IntGw(config)#int f0/0

IntGw(config-if)#ip nat inside

IntGw(config-if)#exit

IntGw(config)#int f0/1

IntGw(config-if)#ip nat outside

IntGw(config-if)#exit
```

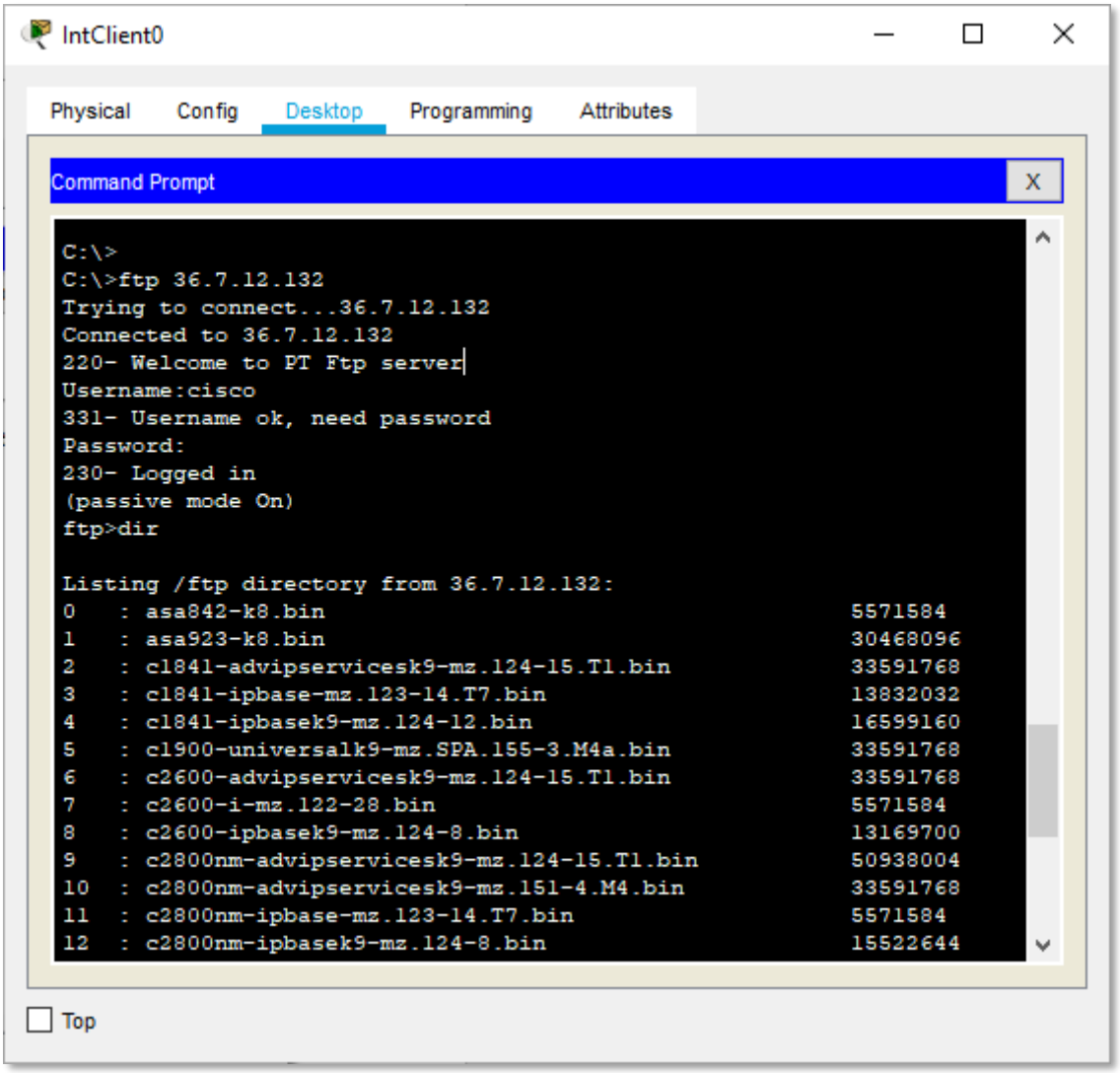
2.4.2 Testen ob ping auf einen Server funktioniert über internen Client



2.4.3 Testen des externen Webservers



2.4.4 FTP Server Test

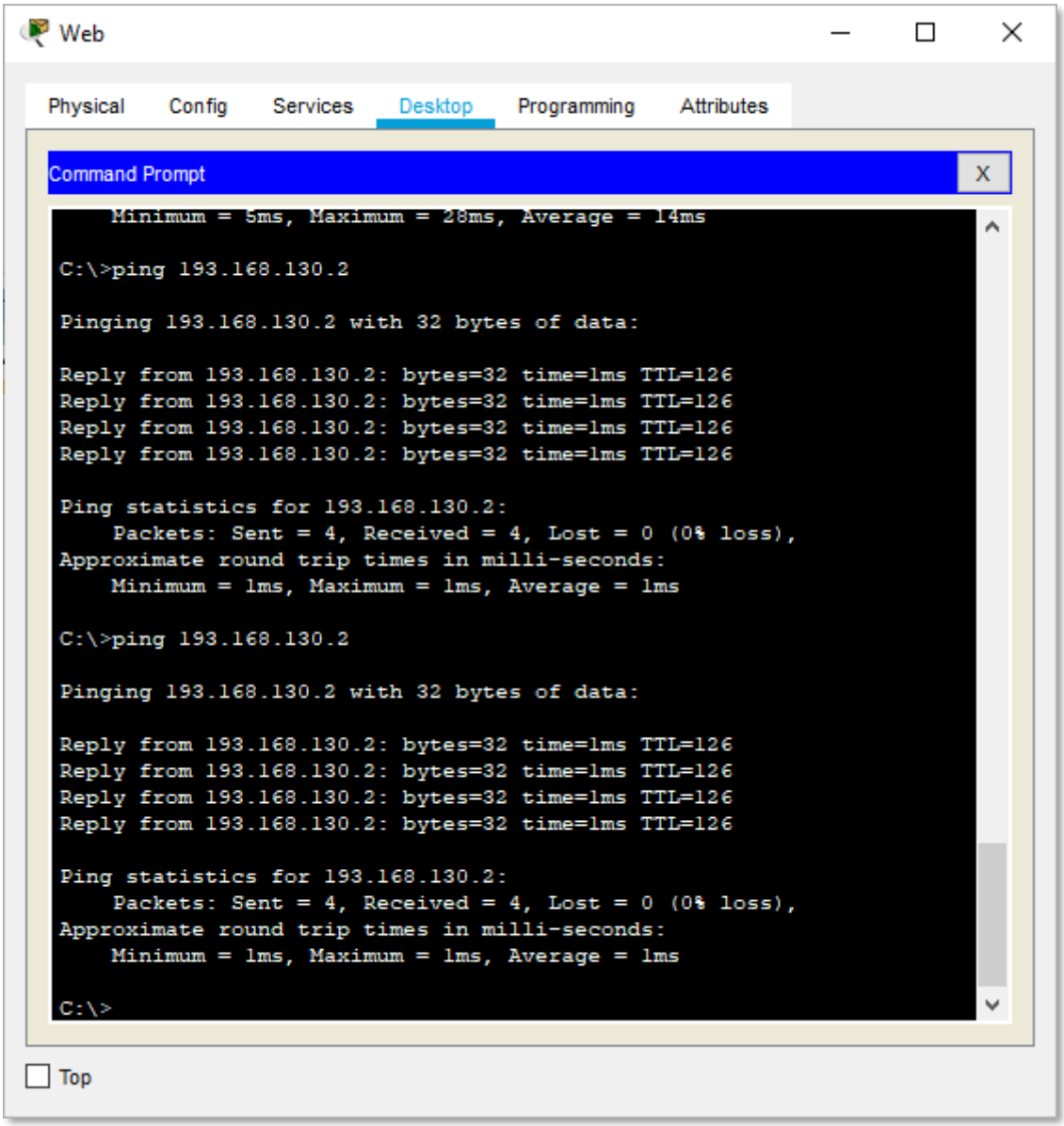


2.5 Konfigurieren des externen Gateways

```
ExtGW(config)#access-list 1 permit 36.7.12.128 0.0.0.255
ExtGW(config)#ip nat inside source list 1 s0/0/0
^
% Invalid input detected at '^' marker.
ExtGW(config)#ip nat inside source list 1 interface s0/0/0
ExtGW(config)#int f0/0
ExtGW(config-if)#ip nat inside
ExtGW(config-if)#exit
ExtGW(config)#int s0/08?
/ .
ExtGW(config)#int s0/0/0
```

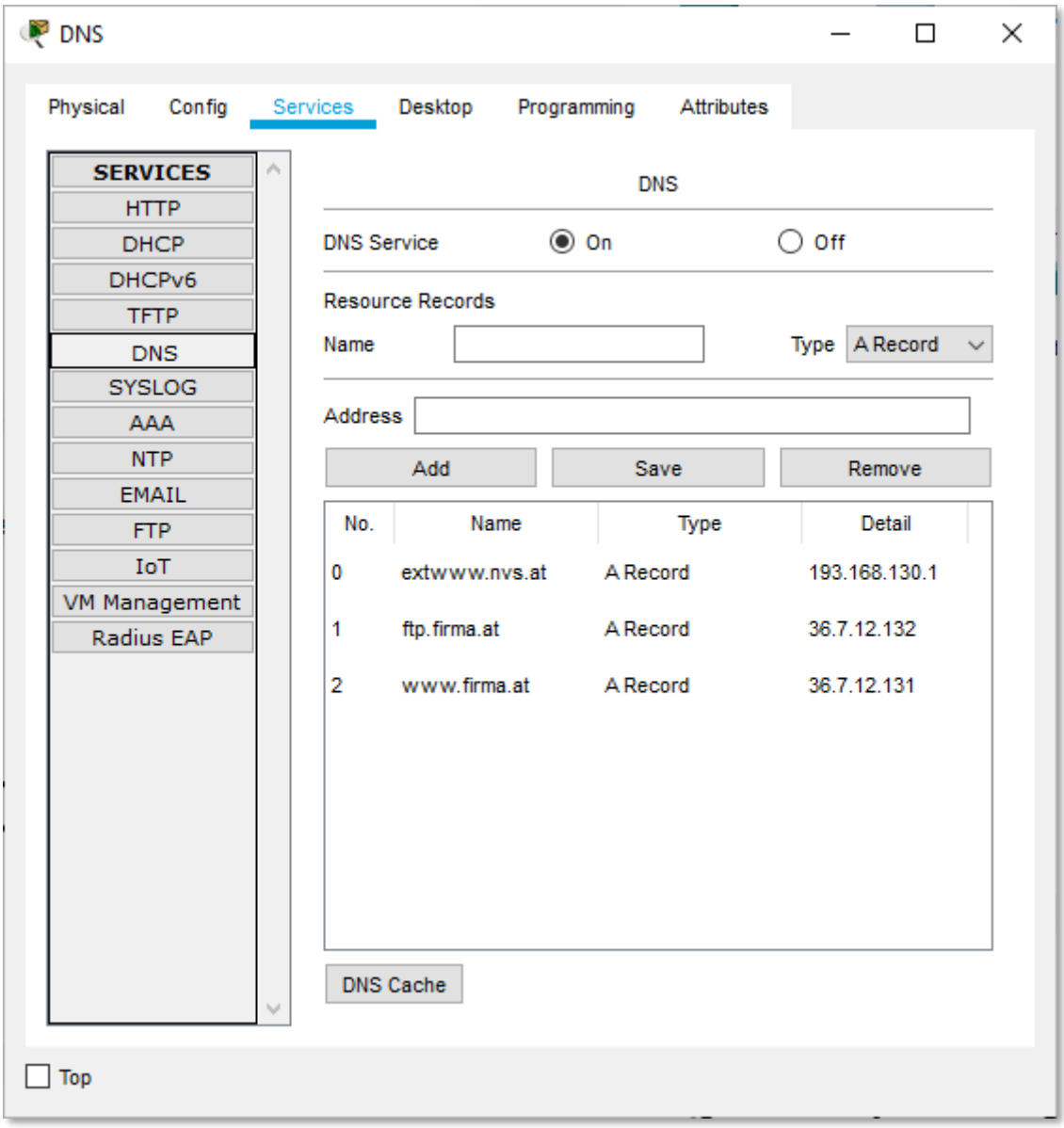
```
ExtGW(config-if)#ip nat outside

ExtGW(config-if)#exit

ExtGW(config)#copy run start
```

2.5.1 Ping Test von Webserver auf ext. DNS Server



2.6 Die Web und FTP Server sollen über ihren Namen erreichbar sein.

Dafür macht man im externen Webserver ein paar A-Records, die mit einem Namen auf die IP Adresse zeigen.



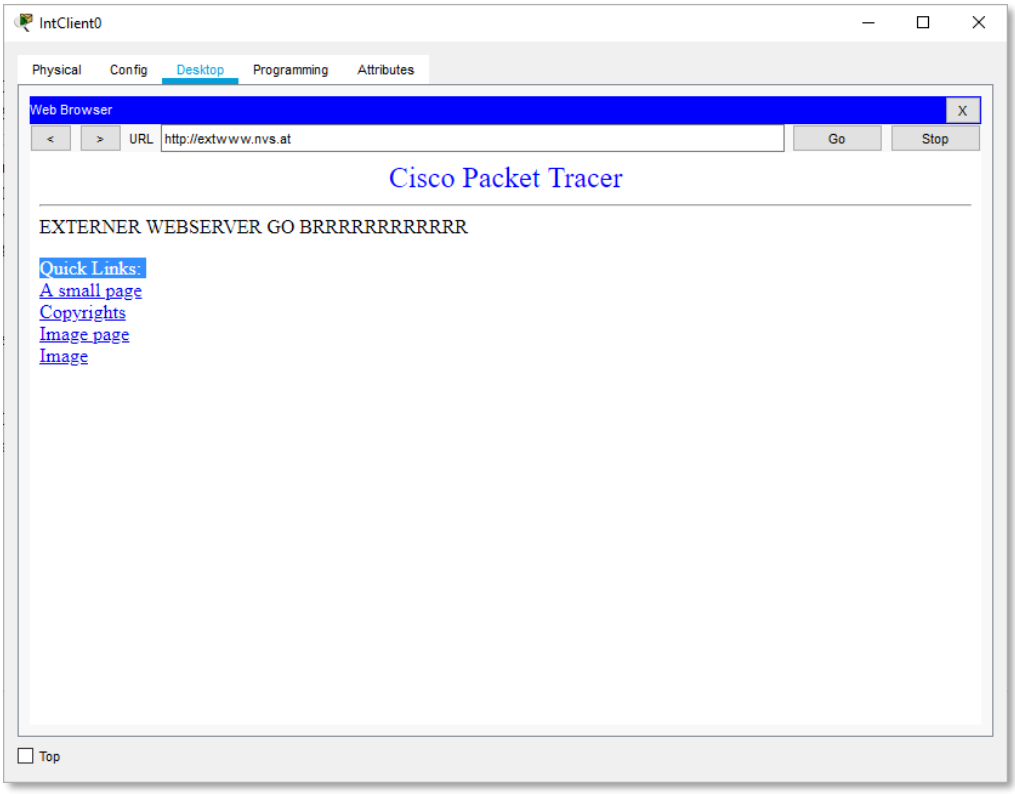
2.7 Der Web und FTP Server soll vom Internet und vom LAN erreichbar sein.

Wir haben noch ein Problem. Aus dem internen LAN (192.168.6.0/24) sind der externe Webserver 193.168.130.1 oder 193.168.130.2, der externe DNS Server, sind nicht zu erreichen. Das kommt daher, dass der Interne Router nicht weiß, woher er das Paket routen soll. Das lässt sich mit einer einfachen default Route fixen.

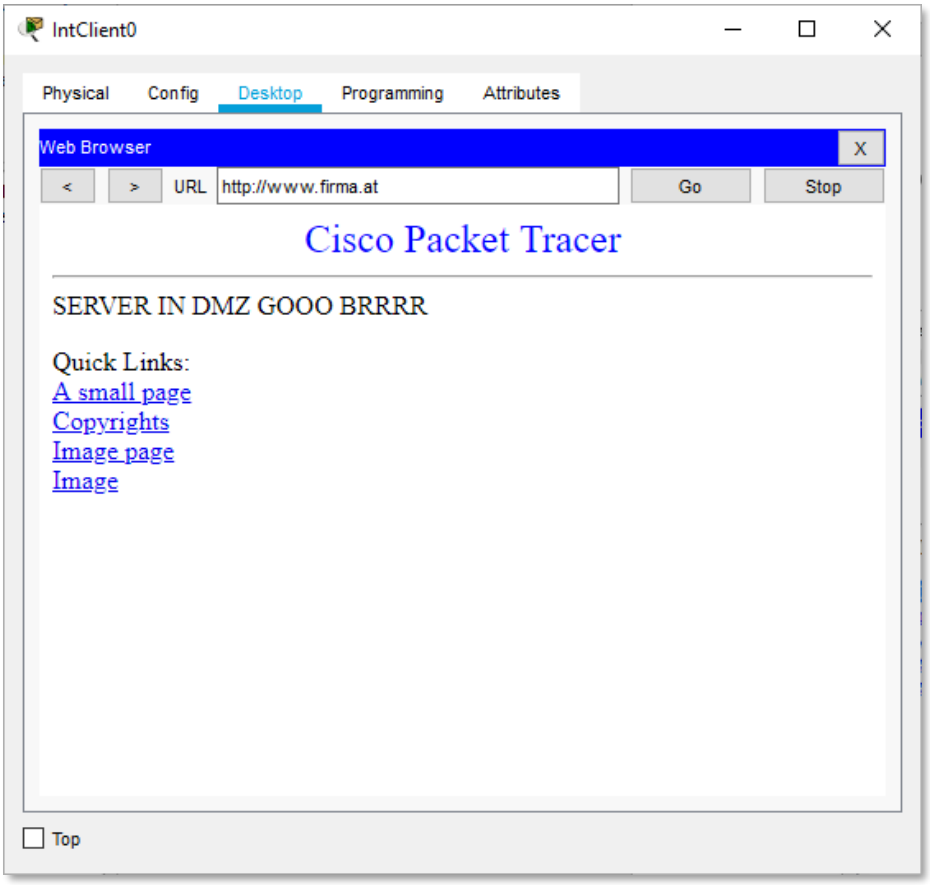
```
IntGw(config)#ip route 0.0.0.0 0.0.0.0 36.7.12.129
```

Sie nimmt die Requests von beliebigen IPs die an den internen Router angeschlossen sind und schickt sie an beliebige IPs in das Internet bzw. andere Netzwerke weiter. Die letzte Adresse ist das Gateway, der das externe 193.168.xxx Netz mit dem 36.xxx Netz verbindet. Danach sind der externe DNS-Server und der externe Web Server erreichbar (www.firma.at ist der externe Webserver).

2.7.1 Testen der Erreichbarkeit vom externen Webserver



2.7.2 Testen der Erreichbarkeit vom Webserver in der DMZ per DNS-Name



2.8 ACLs für Ports konfigurieren

Die internen Clients sollen auf interne und externe Webserver (Port 80 und 443) zugreifen können. Weiters sollen sie Zugriff auf den Firmen FTP-Server haben. Andere Ports sind zu sperren.

Mit der Hilfe von Access Control Lists kann man den Traffic so einschränken, dass Geräte bzw. Nutzer nur auf bestimmte Dienste, die der Administrator vorgibt, zugreifen können. Bei ACLs kann man Port, Quelle, Ziel, Typ der Verbindung, d.h. TCP bzw. UDP festlegen.

Im folgenden Beispiel sollen Nutzer nur den Zugriff auf http(s) Server erhalten und auf den bestimmten FTP Server, der in der DMZ hängt.

ACLs lassen sich mit

```
no access-list <ACL_NUM>
```

rückgängig machen.

2.8.1 ACL einschalten

Damit der Router auf eine Access Control List zurückgreift, muss er darauf aufmerksam gemacht werden.

Dies funktioniert mit dem Kommando `ip access-group <NR> <IN/OUT>`

```
IntGw(config-if)#ip access-group 101 in
```

2.8.2 Notwenige ACLs konfigurieren

Der Router blockt standardmäßig alles, welche keine Ausnahme beinhaltet, d.h. keine ACL für den bestimmten Port / Dienst konfiguriert ist. Damit Dinge wie Namensauflösung durch einen DNS Server funktionieren, muss dieser auch freigegeben werden.

DNS schickt seine Anfragen standardmäßig über Port 53/udp. D.h. wir müssen eine ACL erstellen, die eine Übertragung dieser DNS Pakete über Port 53 und das UDP Protokoll erlaubt.

```
access-list 101 permit udp 192.168.6.0 0.0.0.255 193.168.130.2 eq 53
```

2.8.3 ACLs für IntGW (internen Gateway)

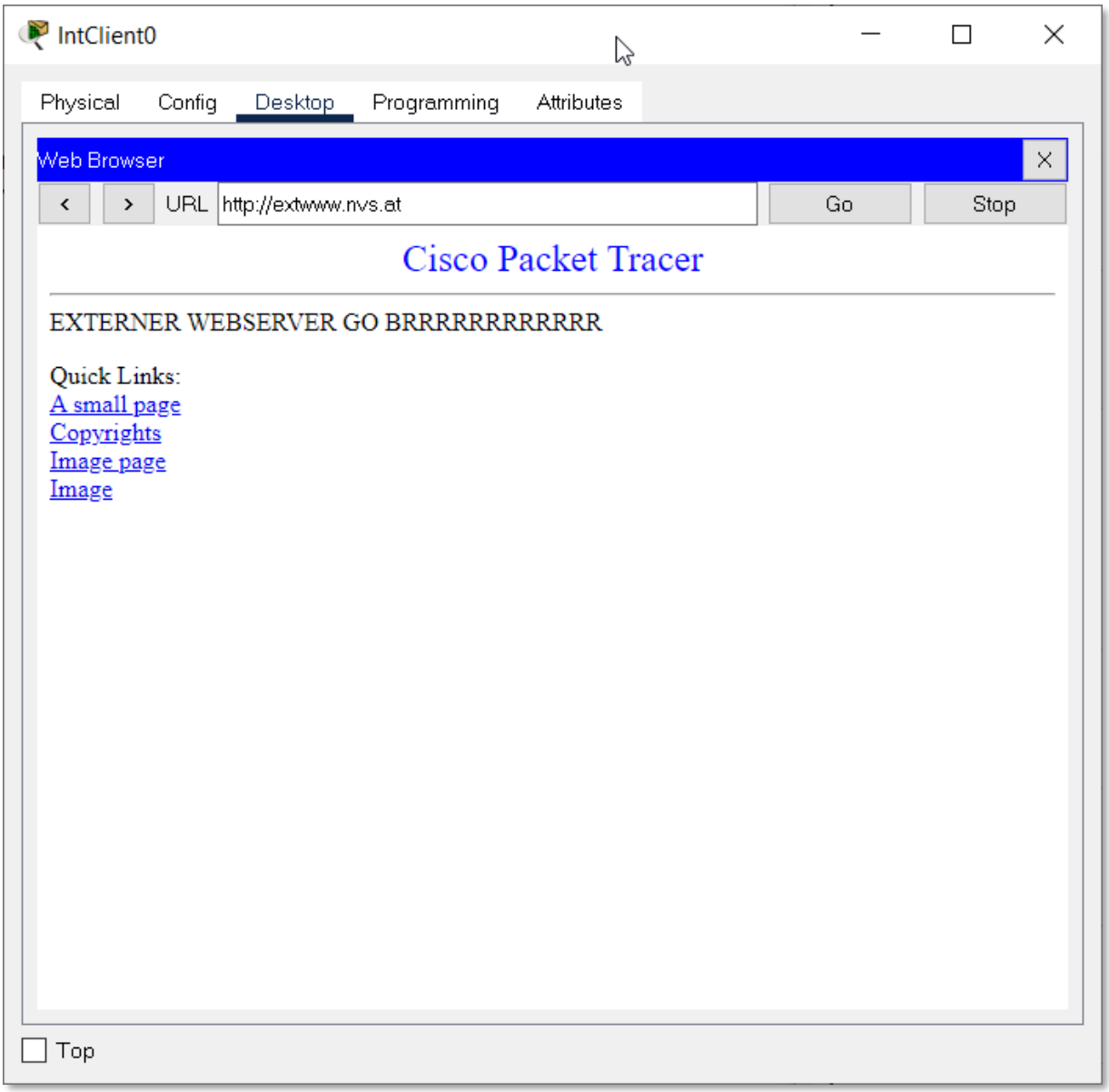
Diese Regeln werden am Interface F0/0 des internen Gateways angelegt, da dort der Traffic von den Clients reinkommt.

```
no access-list 101

access-list 101 remark "Erlaube das Verbinden aus dem internen LAN
zu unserem DNS Server, um Namensabfragen machen zu können"

access-list 101 permit tcp 192.168.6.0 0.0.0.255 host 193.168.130.2
eq 53

access-list 101 permit udp 192.168.6.0 0.0.0.255 host 193.168.130.2
eq 53

access-list 101 remark "Erlaube das Verbinden aus dem internen LAN
auf den Firmen FTP-Server"

access-list 101 permit tcp 192.168.6.0 0.0.0.255 host 36.7.12.132 eq
21
```

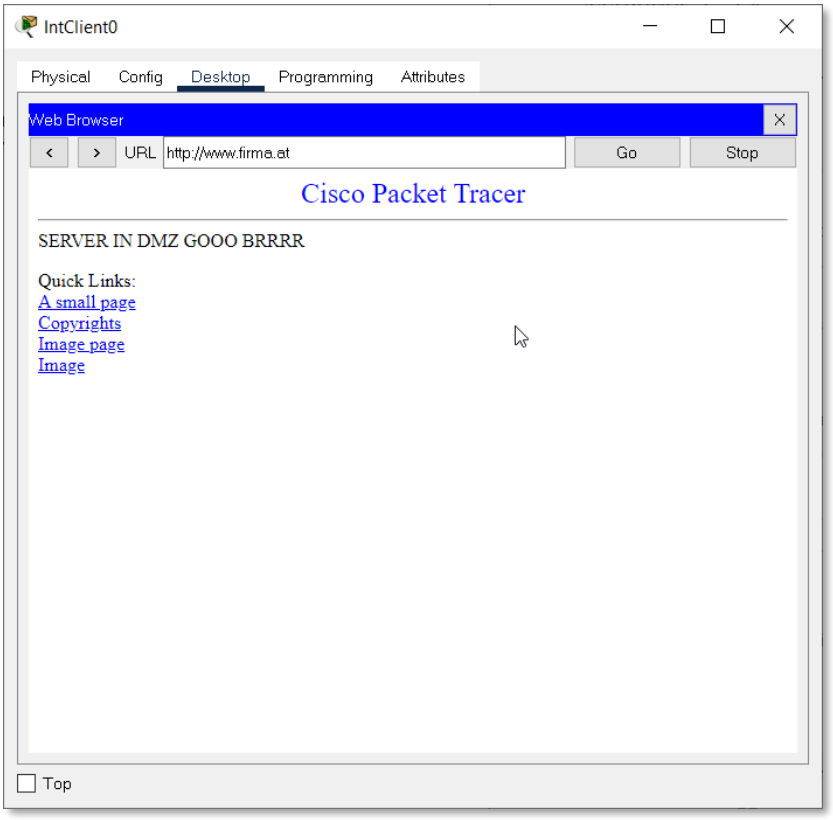
```
access-list 101 remark "Erlaube das Verbinden aus dem internen LAN auf jeden beliebigen Webserver über HTTP mit Port 80 oder HTTPS mit Port 443"
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any eq  80
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any eq  443
access-list 101 remark "Lässt alle Pakete durch, die zu einer bestehenden Verbindung gehoeren - funktioniert nur auf TCP."
access-list 101 permit tcp any any established #erlaubt alle aufgebauten Verbindungen durch die Firewall
```

2.8.4 Testen der Regeln für internen Gateway

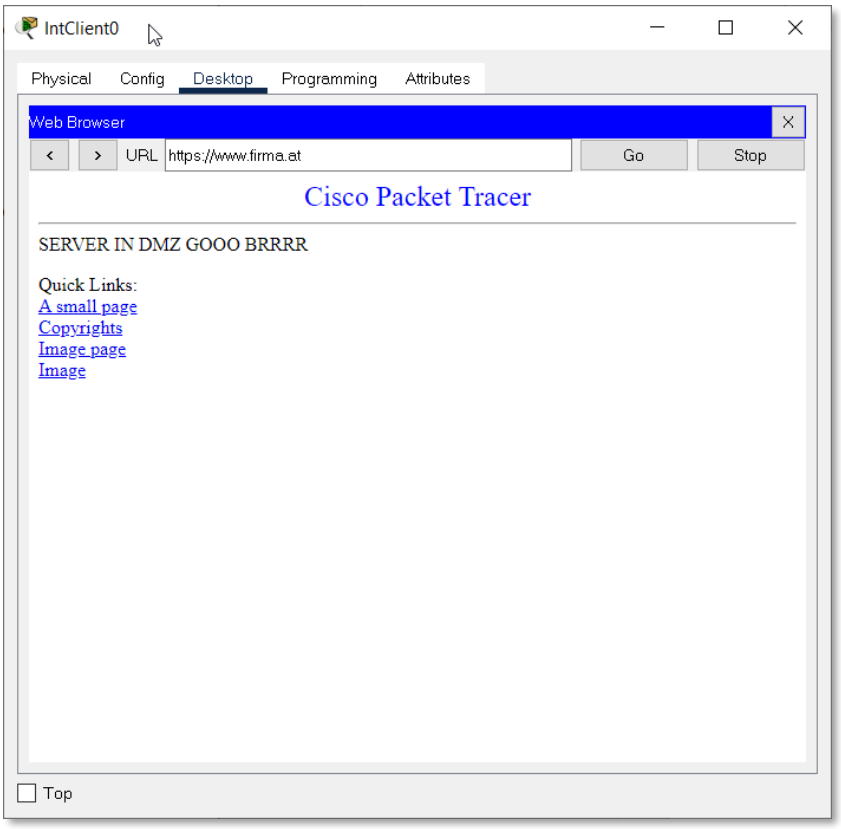
2.8.4.1 Externer Webserver & DNS



2.8.4.2 DMZ Webserver & DNS



2.8.4.3 HTTPS Test



2.8.4.4 FTP Test

ftp.firma.at resolves to 36.7.12.132/28.

```
C:\>ftp ftp.firma.at
Trying to connect...ftp.firma.at
Connected to ftp.firma.at
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

2.8.4.5 Test eines Pings, der nicht erlaubt ist

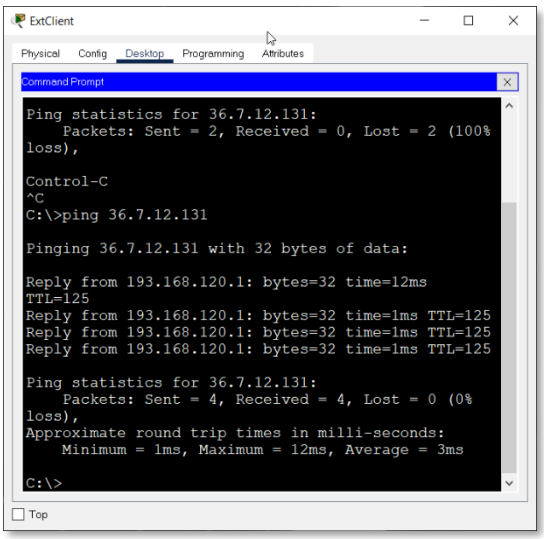
```
C:\>ping ftp.firma.at

Pinging 36.7.12.132 with 32 bytes of data:

Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.

Ping statistics for 36.7.12.132:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

2.8.5 ACLs für externen Gateway

Da das externe Gateway derzeit noch jeden Traffic durchlässt, müssen wir ihn nun auch so konfigurieren, dass er nur das nötigste durchlässt, d.h. FTP, DNS und http/s.

Derzeit haben wir noch das Problem, dass externe Clients den Webserver pingen wollen, was wir nicht wollen, da nur benötigte Protokolle bzw. Ports freigegeben werden.



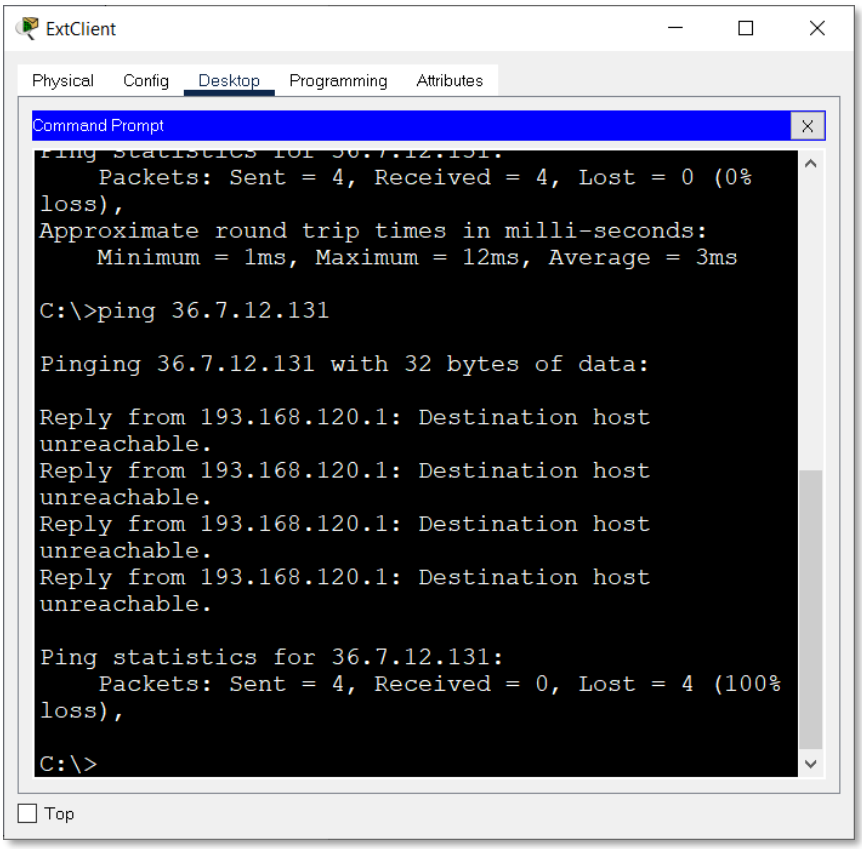
```
no access-list 110
access-list 110 remark "Erlaube Zugriff auf Webserver in DMZ"
access-list 110 permit tcp any host 36.7.12.131 eq 80
access-list 110 permit tcp any host 36.7.12.131 eq 443
access-list 110 remark "Erlaube Zugriff auf FTP-Server in DMZ"
access-list 110 permit tcp any host 36.7.12.132 eq 21
access-list 110 remark "TCP+UDP fuer DNS"
access-list 110 permit tcp host 193.168.130.2 eq 53 any
access-list 110 permit udp host 193.168.130.2 eq 53 an
access-list 110 remark "Erlaube eingehende Verbindungen die von
einem internen Client angefragt wurden"
access-list 110 permit tcp any any established
```

Daher müssen wir am Serial Interface S0/0/0 die ACL aktivieren und dort festlegen, welche Services ein externer Client erreichen darf und welche nicht.

2.8.6 Testen der ACL für externen Gateway

2.8.6.1 Ping Test mit externem Client

Die Pakete werden vom ISPRouter zurückgeworfen, so wie es sein sollte.



3 Router Configs

3.1 IntGW

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

Current configuration : 1413 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname IntGw
!
!
!
!
ip dhcp excluded-address 192.168.6.1
!
ip dhcp pool intlan
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
dns-server 193.168.130.2
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
```

```
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.6.1 255.255.255.0
ip access-group 101 in
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 36.7.12.130 255.255.255.240
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list 1 interface FastEthernet0/1 overload
```

```
ip classless

ip route 0.0.0.0 0.0.0.0 36.7.12.129

!

ip flow-export version 9

!

!

access-list 1 permit 192.168.6.0 0.0.0.255

access-list 101 remark "Erlaube das Verbinden aus dem internen LAN
auf jeden beliebigen Webserver ber HTTP mit Port 80 oder HTTPS mit
Port 443"

access-list 101 permit tcp 192.168.6.0 0.0.0.255 any eq www

access-list 101 permit tcp 192.168.6.0 0.0.0.255 any eq 443

access-list 101 permit udp 192.168.6.0 0.0.0.255 host 193.168.130.2
eq domain

access-list 101 permit tcp 192.168.6.0 0.0.0.255 host 36.7.12.130 eq
ftp

access-list 101 permit tcp 192.168.6.0 0.0.0.255 host 36.7.12.132 eq
ftp

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end
```

3.2 Externer Gateway

```
ExtGW#show run
Building configuration...

Current configuration : 1835 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ExtGW
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
```

```
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 36.7.12.129 255.255.255.240
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 193.168.120.1 255.255.255.252
ip access-group 110 in
ip access-group 111 out
ip nat outside
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
```

```
no ip address
shutdown
!
ip nat inside source list 1 interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
!
access-list 1 permit 36.7.12.0 0.0.0.255
access-list 1 permit 192.168.6.0 0.0.0.255
access-list 1 permit 0.0.0.0 0.0.0.255
access-list 110 remark "Erlaube Zugriff auf Webserver in DMZ"
access-list 110 permit tcp any host 36.7.12.131 eq www
access-list 110 permit tcp any host 36.7.12.131 eq 443
access-list 110 remark "Erlaube Zugriff auf FTP-Server in DMZ"
access-list 110 permit tcp any host 36.7.12.132 eq ftp
access-list 110 remark "TCP+UDP fuer DNS"
access-list 110 permit udp host 193.168.130.2 eq domain any
access-list 110 remark "Erlaube eingehende Verbindungen die von
einem internen Client angefragt wurden"
access-list 110 permit tcp any any established
access-list 111 remark "Erlaube Zugriff auf FTP-Server in DMZ"
access-list 111 permit tcp host 36.7.12.132 any eq ftp
access-list 111 remark "Erlaube Zugriff auf Webserver in DMZ"
access-list 111 permit tcp host 36.7.12.131 any eq www
access-list 111 permit tcp host 36.7.12.131 any eq 443
!
!
!
!
!
```

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