

**Versuch 3:  
Packet Tracer –  
Betrachtung weiterer  
Netzwerktechnologien**



**Studiengänge**

**Ausbildungsziel**

**Ausbildungsinhalte**

**Hardware / Software**

**Vorkenntnisse**

- Medientechnik
- Kennenlernen weiterführender Netzwerktechnologien
- Verstehen grundlegender Funktionsweisen von verschiedenen Technologien
- Einrichtung, Test und Betrachtung von:
  - MAN
  - VLAN
  - Firewalls
  - NAT
- IPv6
- Visualisierung der Paketübertragungswege
- Einführung in die Konsolenkonfiguration von Cisco Geräten
- 1 PC mit Virtual Box inklusive vorinstallierter Packet Tracer Software
- Versuch 1, Versuch 2
- Theoretische Grundlagen der Vorlesungsunterlagen Netzwerktechnik und Administration I & II

In diesem dritten Versuch soll zu Beginn ein einfaches MAN simuliert werden, um die Funktionsweise der Technologie von Netzwerken über einen geografisch ausgedehnten Raum näher zu betrachten und zu verstehen. Weiterhin sollen mit VLANs eine weitverbreitete und nützliche Technologie simuliert und untersucht werden. Daran anschließend wirft dieser Versuch einen Blick auf den Einsatz und die grundlegenden Funktionsweisen von Firewalls. Aus aktuellem Anlass behandelt dieser Versuch ebenfalls die in der Vorlesung besprochene IPv6 Adressierung. Abschließend soll auf die in der Vorlesung behandelte NAT / NATPT Technologie eingegangen werden, um den theoretischen Grundlagen aus den vorangegangenen Versuchen einen praxisnahen Bezug zu vermitteln. Fortführend wird in diesem Praktikum erstmals die IOS – Konsole Anwendung finden, welche in der Praxis zur Konfiguration von Cisco – Routern verwendet wird. Dieser Versuch setzt den Abschluss des ersten und zweiten Versuches voraus, grundlegende Schritte und bekannte theoretische Grundlagen werden in diesem Praktikum nicht mehr Schritt für Schritt erläutert.

---

### **Aufgabe 1: Einrichten eines Metropolitan Area Network (MAN) inkl. DHCP**

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)



2950 – 24 Switch (Standard 24 – Port Switch)



Generic – Router (zuständig für Routing und DHCP)



Serial – DCE (Seriellles Kabel zur Verbindung der Standorte)



In diesem Schritt soll unter Verwendung des Packet Tracer ein einfaches *MAN*<sup>1</sup> simuliert werden. Die Aufgabe basiert auf 3 Standorten, deren unterschiedliche Netzwerke über Router miteinander kommunizieren. Diese Technologie wird beispielsweise verwendet, um einzelne Gebäude einer Hochschule miteinander zu vernetzen. In diesem Beispiel sollen pro Standort zwei Klienten in Form handelsüblicher Computer ans Netz angeschlossen werden. Die Klienten sind

---

<sup>1</sup> MAN (Metropolitan Area Network) ist eine Sonderform des WAN (Wide Area Network). Hierbei werden üblicherweise viele LANs verbunden. Dazu wird meistens eine Glasfasertechnik verwendet.

miteinander über einen Switch verbunden, welcher wiederum am zugehörigen Router angeschlossen wird. Dieser Router übernimmt ebenfalls die IP – Vergabe via DHCP für den betreffenden Standort.

Zu Beginn platzieren Sie zunächst für jeden der 3 Standorte die Klienten auf der Arbeitsfläche. Setzen Sie ebenfalls zu jeder Zweiergruppe PCs einen Standard 2950 – 24 Switch dazu (Abbildung 1).

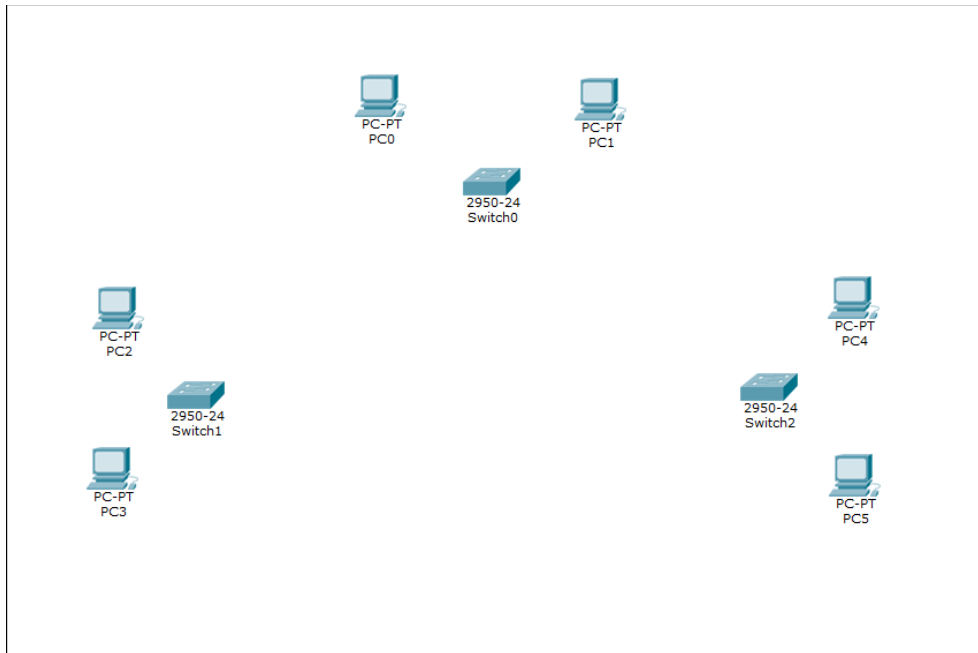



Abbildung 1

Verbinden Sie diese Komponenten nun wie gewohnt. Lassen Sie jedoch den Anschluss *FastEthernet0/24* am Switch unbelegt, da dieser für die Verbindung zum Router genutzt werden soll. Im nächsten Schritt wählen Sie die Router aus. Benutzen Sie für diese Konstellation 3  Generic – Router. Achten Sie dabei darauf, dass Sie im Geräte – Manager *Router-PT* und nicht *Router-PT-Empty* wählen (Abbildung 2).

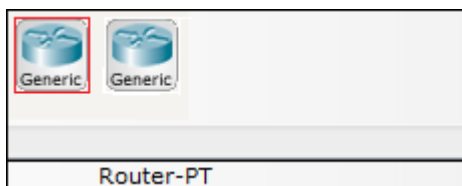


Abbildung 2

Fügen Sie anschließend jeweils einen *Generic – Router* zu jedem Netz hinzu (Abbildung 3).

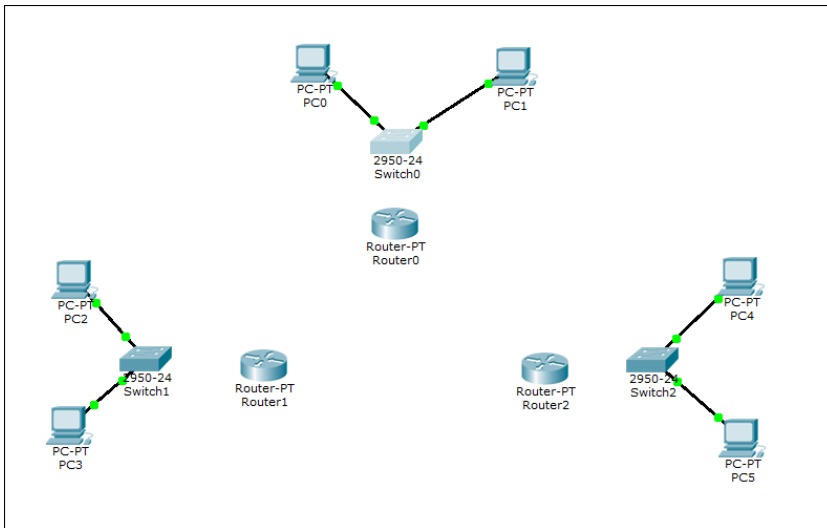


Abbildung 3

Dieser Router verfügt im Vergleich zu den bisherig benutzten Routern über serielle Anschlüsse, welche für die Verbindung der einzelnen Standorte notwendig sind. Verbinden Sie nun jeden Switch mit dem dazugehörigen Router. Zur besseren Übersichtlichkeit, verwenden Sie an den Routern jeweils den *FastEthernet0/0* – Port. An den Switches nutzen Sie dazu den zuvor freigehaltenen Port *FastEthernet0/24* (Abbildung 4).

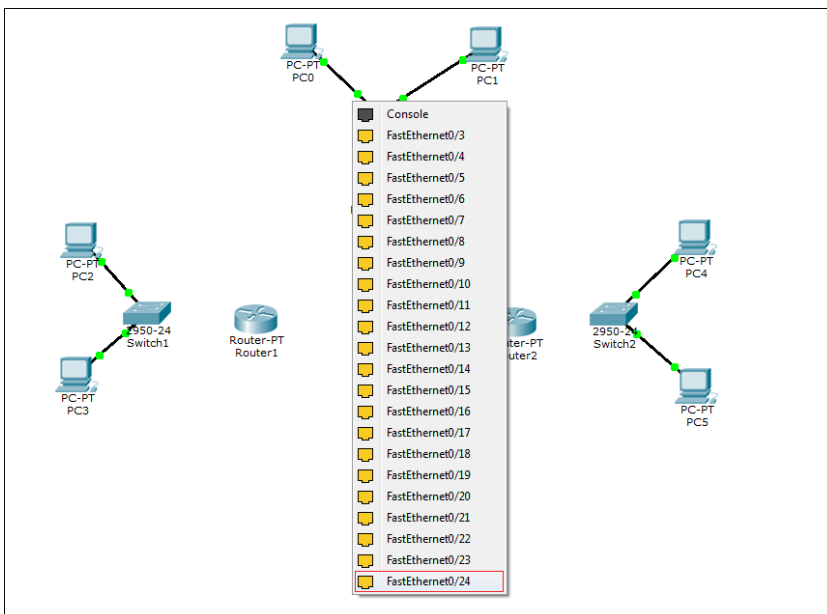



Abbildung 4

Abschließend wählen Sie im Gerätemanager  *Serial DCE*. Hierbei handelt es sich um ein serielles Kabel, welches besonders zur Datenübertragungen über große Entfernungen und somit zur Verbindung der 3 Standorte in diesem Versuch geeignet ist. Verbinden Sie nun die Router über die Serial - Ports (Abbildung 5).

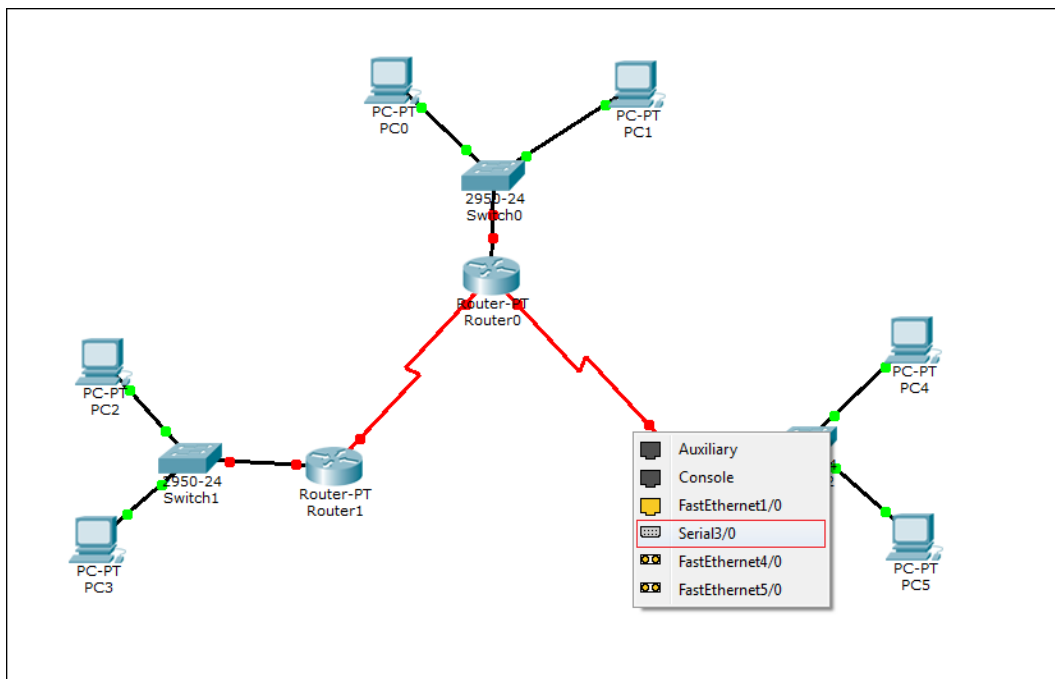


Abbildung 5

Das Grundgerüst des Netzwerkes ist nun fertiggestellt. In den nächsten Schritten wird die Konfiguration des Netzwerkes näher betrachtet. Folgende Netze sollen für die Klienten verwendet werden:

|                     |  |
|---------------------|--|
| <i>Erstes Netz</i>  | <i>Netz-IP: 192.168.1.0 SNM: 255.255.255.0</i> |
| <i>Zweites Netz</i> | <i>Netz-IP: 192.168.2.0 SNM: 255.255.255.0</i> |
| <i>Drittes Netz</i> | <i>Netz-IP: 192.168.3.0 SNM: 255.255.255.0</i> |

Da eine statische IP – Vergabe an die Klienten eines Netzwerkes in der Praxis unüblich ist, soll diese hier dynamisch stattfinden. Damit die Router diese Aufgabe übernehmen können, müssen diese per Konsole auf diesen Dienst programmiert werden. Bevor jedoch auf diese Konfiguration näher eingegangen wird, bedarf es noch einiger Einstellungen. Zunächst müssen die Router als Gateway definiert werden, damit eine Kommunikation der Netze untereinander gewährleistet ist. Hier

soll gelten, dass jeder Router eines Netzes jeweils die letzte Host-IP – Adresse in diesem Netz erhält (Beispiel: Netz 1, Gateway 192.168.1.254). Setzen Sie nun für die verwendeten FastEthernet – Ports der Router diese Gateways. Orientieren Sie sich an der Bezeichnung der Geräte, um eine geordnete Reihenfolge zu erhalten (Abbildung 6).

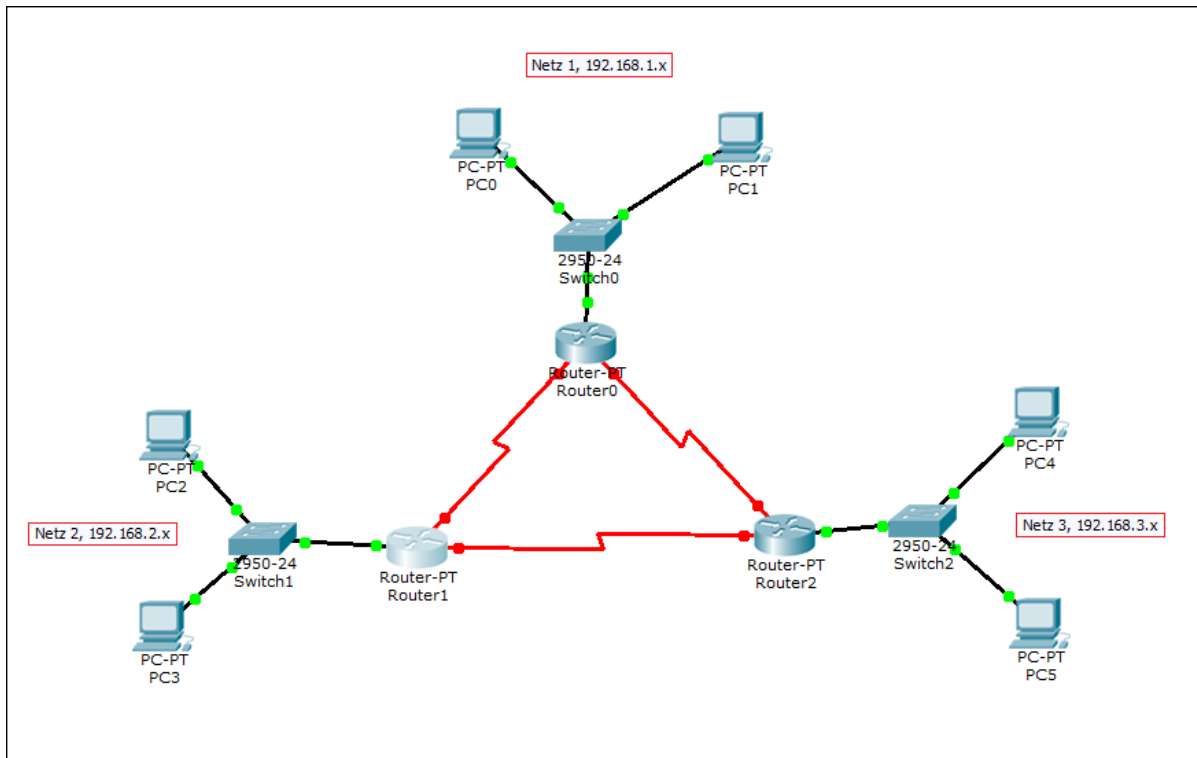


Abbildung 6

Achten Sie darauf, nach der Zuweisung der IPs den Port – Status des betreffenden Anschlusses auf *On* zu schalten. Bei Problemen mit dieser Konfiguration, orientieren Sie sich an *Versuch 2, Aufgabe 4: Einrichten eines Netzwerks mit verschiedenen Netzen*. Damit sind die Gateways klientseitig konfiguriert. In einem nächsten Schritt soll die IP – Vergabe an die Klienten per DHCP auf den Routern eingerichtet werden. Dies findet in der IOS – Konsole (*IOS Command Line Interface, CLI*) statt. Rufen Sie diese über den Reiter *CLI* im Konfigurationsfenster *Router0* auf (Abbildung 7).

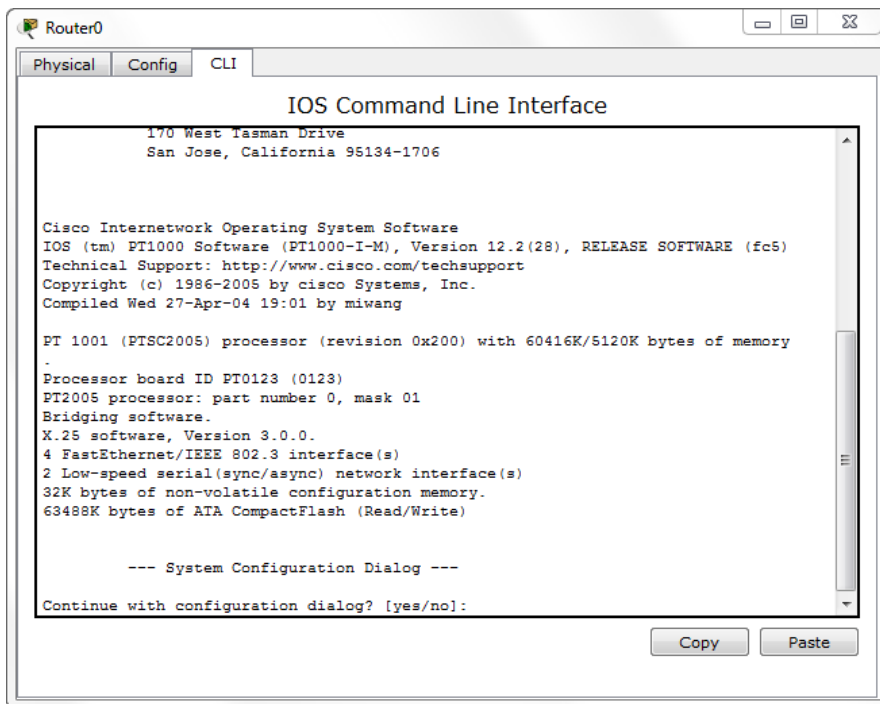


Abbildung 7

*Continue with configuration dialog?* gibt Ihnen die Möglichkeit, den Router per Kommandozeile in einem Basic Setup zu konfigurieren (IP – Adresse, Subnetzmaske usw.). Dies soll an dieser Stelle ohne Bedeutung sein. Tippen Sie ein *no* in die Kommandozeile und bestätigen Sie dies mit *Enter* (Abbildung 8).

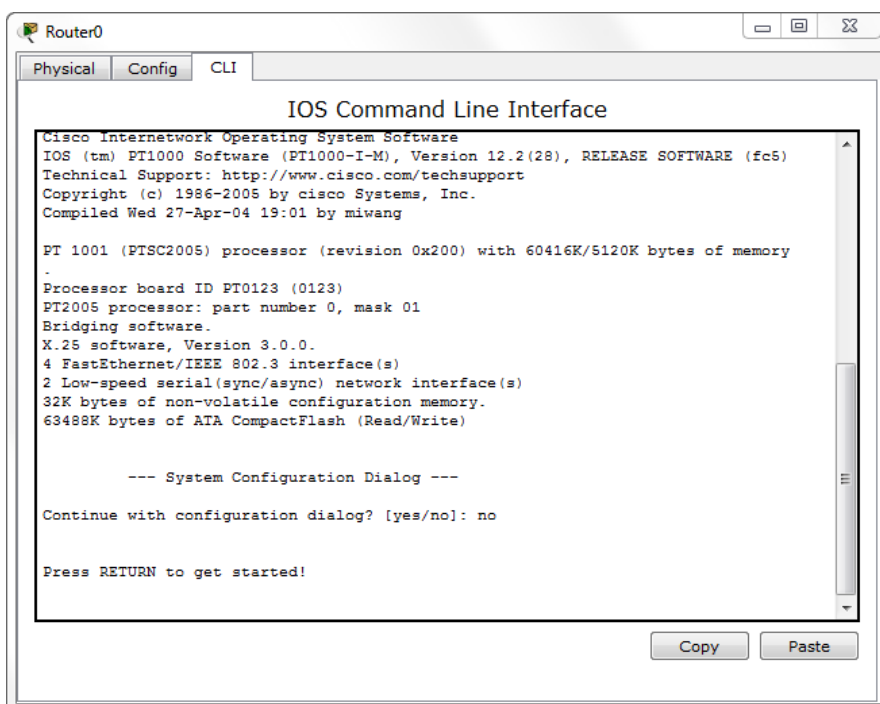


Abbildung 8

Durch erneutes Betätigen der *Enter* – Taste starten Sie die manuelle Konfiguration (Abbildung 9). Sollte der in Abbildung 8 dargestellte Inhalt bei Ihnen nicht erscheinen, dann geben Sie bitte „exit“ in die Kommandozeile ein. Wiederholen Sie diesen Befehl, bis „Router>“ angezeigt wird (Abbildung 9).

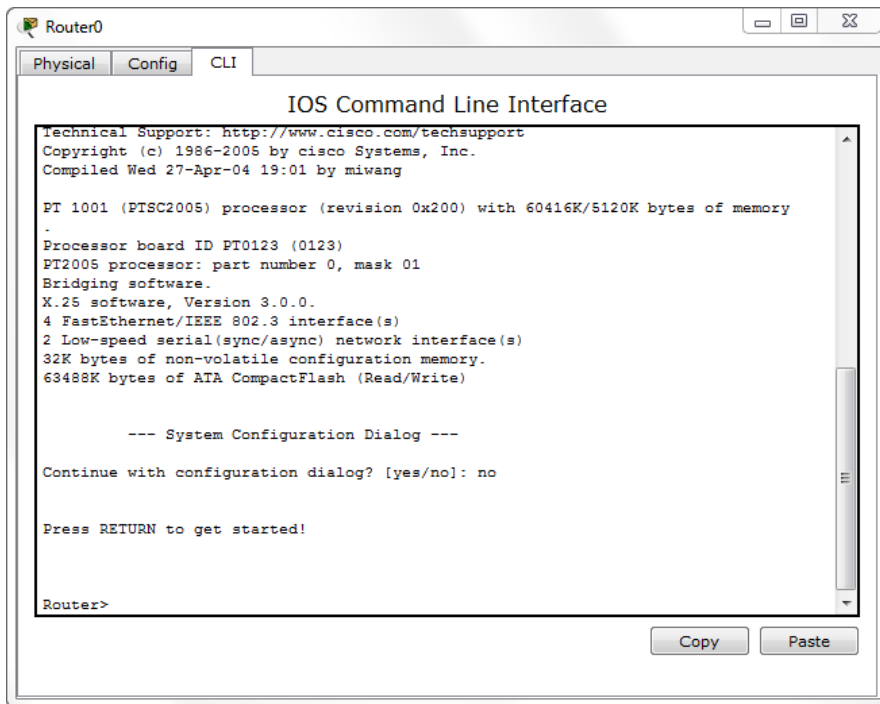


Abbildung 9

Den Router bereiten Sie mit dem Befehl

*enable*

auf die Konfiguration vor. Senden Sie den Befehl mit *Enter* ab. Mit einer nächsten Eingabe

*configure terminal*

verschaffen Sie sich Zugang zum globalen Konfigurationsmodus. Da der Router bereits eine statische IP zugewiesen bekommen hat, müssen Sie diese zunächst von der IP – Vergabe ausschließen. Geben Sie den folgenden Befehl

*ip dhcp excluded-address 192.168.1.254*

in die Konsole ein und bestätigen Sie erneut mit *Enter*. Damit ist das Gerät darauf programmiert, diese IP bei der Zuweisung nicht zu berücksichtigen. Durch die Eingabe



*ip dhcp pool [beliebiger Name Ihres Netzes]*<sup>2</sup>

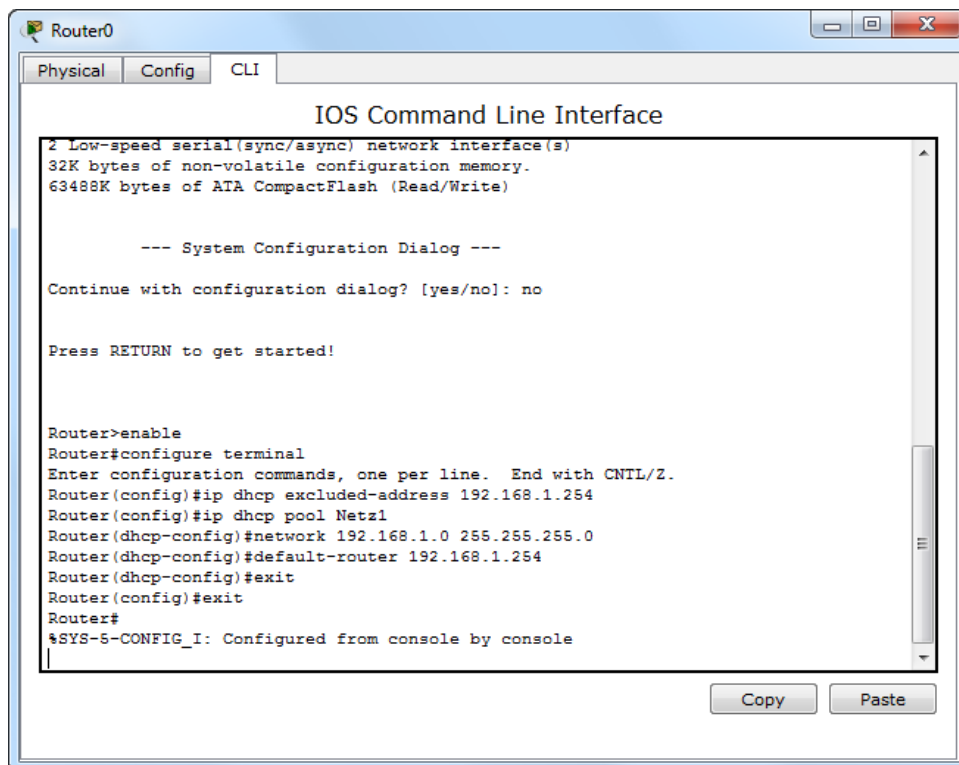
begeben Sie sich in die DHCP Konfiguration des Routers. An der aktuellen Pfadangabe der Konsole *Router (dhcp-config)* ist erkennbar, dass man sich nun in der DHCP – Konfiguration befindet. Durch den Befehl

*network 192.168.1.0 255.255.255.0*

teilen Sie dem Router mit, dass dieser an alle an diesen Router angeschlossenen Geräte, die einen DHCP – Request senden, eine IP Adresse aus dem *192.168.1.0* – Netz vergibt. Damit nun alle Pakete, welche in die anderen Netze gesendet werden sollen, erfolgreich über diesen Router vermittelt werden können, muss die eigene IP-Adresse des Routers als *Default Gateway* konfiguriert werden. Dies wird durch die Eingabe des Befehls

*default-router 192.168.1.254*

erreicht. Die Konfiguration ist nun abgeschlossen und Sie können die DHCP – Konfiguration durch Eingabe von *exit* verlassen. Die vollständige Konfiguration von *Router0* in *Netz 1* über die Konsole sollte wie folgt aussehen (Abbildung 10):



```
Router0
Physical Config CLI
IOS Command Line Interface
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.1.254
Router(config)#ip dhcp pool Netz1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.254
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Abbildung 10

<sup>2</sup> Angabe ohne [ ]

Sie können das Konsolenfenster nun schließen. Um die einwandfreie Funktion der eben konfigurierten DHCP – Zuweisung zu überprüfen, öffnen Sie das Einstellungsfenster von *PC0* und wählen im Reiter Desktop das Menü *IP Configuration*. Aktivieren Sie den DHCP – Modus. Sind alle Schritte korrekt ausgeführt worden, erhält der PC nun die erste freie IP aus dem von Ihnen festgelegten IP – Pool (Abbildung 11).

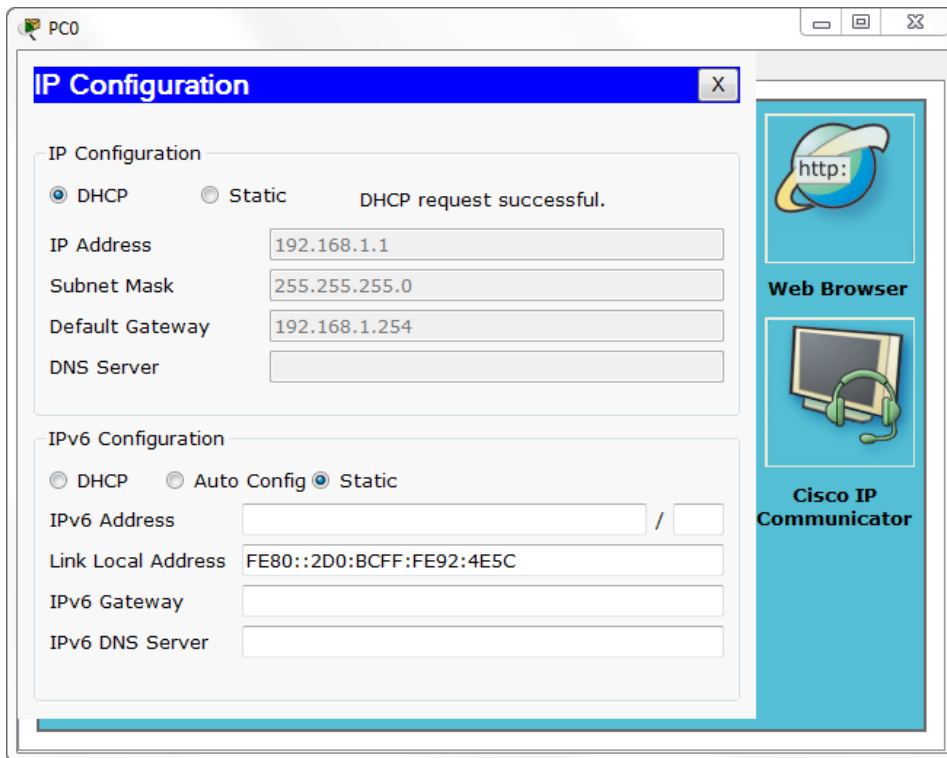


Abbildung 11

Wiederholen Sie nun diese Schritte zur Konfiguration der anderen beiden Router, um diese für die IP – Vergabe in den zugehörigen Netzen zu programmieren. Ist dies abgeschlossen, müssen Sie abschließend bei sämtlichen beteiligten PCs die IP – Bezugsmethode auf DHCP stellen, damit jedes Gerät eine IP erhält. Vergewissern Sie sich, dass alle Komponenten eine IP erhalten, um Fehler bei der Konfiguration auszuschließen.

Im nächsten Schritt muss nun auch eine Kommunikation zwischen den Router gewährleistet werden. Dazu müssen die seriellen Anschlüsse ebenfalls noch konfiguriert werden. Rufen Sie dazu das Konfigurationsfenster von *Router0* auf und begeben Sie sich unter *Config / Interface* ins Untermenü des Anschlusses, welcher zur Verbindung mit *Router1* verbunden ist. Sollten Sie sich nicht erinnern, über

welche Anschlüsse die Router verbunden sind, schließen Sie das Konfigurationsfenster und berühren Sie mit dem Cursor den betreffenden Anschluss, um sich die Bezeichnung des Ports anzeigen zu lassen (siehe auch *Abbildung 24, Versuch 2*). Zurück im Menü tragen Sie folgende Daten ein:

|                    |                      |
|--------------------|----------------------|
| <i>IP Address</i>  | <i>10.30.101.1</i>   |
| <i>Subnet Mask</i> | <i>255.255.255.0</i> |

Vergewissern Sie sich auch, dass der Port Status auf *On* geschaltet ist. Dieser erste Port ist nun konfiguriert und Sie können das Fenster schließen. Begeben Sie sich nun in das Einstellungsmenü des zugehörigen Ports in *Router1*. Hier fügen Sie folgende Parameter ein:

|                    |                      |
|--------------------|----------------------|
| <i>IP Address</i>  | <i>10.30.101.2</i>   |
| <i>Subnet Mask</i> | <i>255.255.255.0</i> |

Verfahren Sie nun mit allen noch übrigen seriellen Anschlüssen der Router genauso. Nehmen Sie dazu folgende Tabelle zur Hilfe:

|  |              |                      |
|--|--------------|----------------------|
| Router1, Interface verbunden mit Router2 | IP Adresse   | <i>10.30.102.1</i>   |
|  | Subnetzmaske | <i>255.255.255.0</i> |
| Router2, Interface verbunden mit Router1 | IP Adresse   | <i>10.30.102.2</i>   |
|  | Subnetzmaske | <i>255.255.255.0</i> |
| Router2, Interface verbunden mit Router0 | IP Adresse   | <i>10.30.103.1</i>   |
|  | Subnetzmaske | <i>255.255.255.0</i> |
| Router0, Interface verbunden mit Router2 | IP Adresse   | <i>10.30.103.2</i>   |
|  | Subnetzmaske | <i>255.255.255.0</i> |

Nach Abschluss dieser Einstellungen wählen Sie bitte eine *Simple PDU* und schicken Sie diese von *PC0* an einen PC Ihrer Wahl in einem der beiden anderen Netze. Wie Sie sehen, schlägt diese Übertragung fehl. Dies liegt daran, dass die Router zwar nun eine Adresse besitzen, aber noch nicht zwischen diesen kommunizieren können. Dazu muss den Routern noch mitgeteilt werden, welche Netzwerke über welche

Ports erreichbar sind (*Routing*). Um die erste Verbindung zwischen Netz 1 und Netz 2 zu vervollständigen, rufen Sie das Menü *Static* über den Reiter *Config* im Konfigurationsfenster von Router0 auf (Abbildung 12).

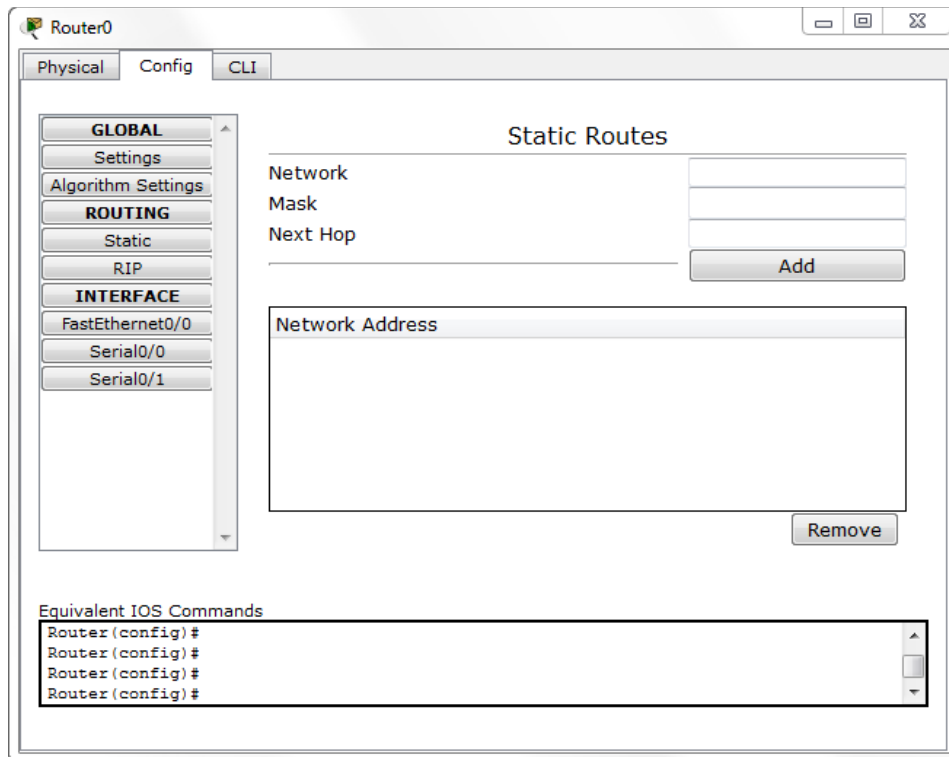


Abbildung 12

In jedem Router müssen hier nun jeweils zwei IP – Routen definiert werden, da jedes Gerät in diesem Beispiel an zwei Netze angeschlossen ist. Widmen Sie sich zuerst der Verbindung zu Netz 2 (192.168.2.0). Tragen Sie folgende Parameter in die dafür vorgesehenen Felder ein:

|                              |                      |
|------------------------------|----------------------|
| <i>Network</i>               | <i>192.168.2.0</i>   |
| <i>Mask</i>                  | <i>255.255.255.0</i> |
| <i>Next Hop</i> <sup>3</sup> | <i>10.30.101.2</i>   |

Fügen Sie den Eintrag per Einfachklick auf *Add* zur Routingliste hinzu. Wie an diesen Parametern erkennbar ist, sind als Route jeweils die Daten des zu kontaktierenden Netzes einzutragen. Wechseln Sie nun in das *Static* – Menü von *Router1* und

---

<sup>3</sup> Next Hop definiert den nächsten Netzknoten, zu welchem das zu vermittelnde Paket übertragen werden muss. Hier ist der jeweilige serielle Port gemeint, über welchem die Router miteinander verbunden sind.

schließen Sie die Verbindungskonfiguration zu Netz 1 ab. Fügen Sie hier die Route hinzu, welche Netz 1 kontaktiert:

|                 |               |
|-----------------|---------------|
| <i>Network</i>  | 192.168.1.0   |
| <i>Mask</i>     | 255.255.255.0 |
| <i>Next Hop</i> | 10.30.101.1   |

Führen Sie diese Schritte nun angepasst an allen Routern aus und führen Sie somit die Konfiguration Ihres MANs zum Abschluss. Das nun aufgebaute und eingerichtete MAN könnte so beispielsweise zur Vernetzung verschiedener Firmengebäude oder der zahlreichen Häuser einer Hochschule innerhalb einer Stadt verwendet werden (Abbildung 13).

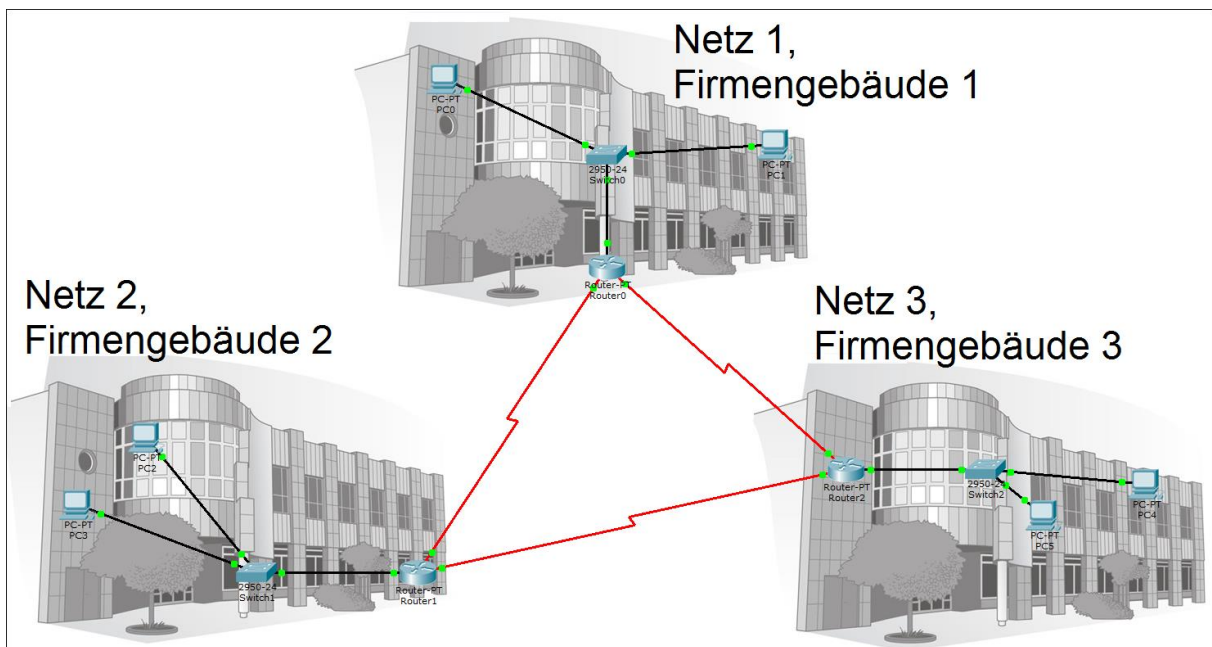


Abbildung 13

Testen Sie nun die Kommunikation der angeschlossenen Netzwerkkomponenten untereinander. Denken Sie auch hier daran, dass die jeweils erste Übertragung einer PDU zwischen zwei Komponenten durch den ARP – Request fehlschlagen kann. Sollte dies bei Ihnen auftreten, starten Sie erneut eine Übertragung zwischen diesen beiden Komponenten. Leeren Sie vorher bei Bedarf die Eventliste.

## Aufgabe 2: Einrichten eines VLANs mit statischer IP – Vergabe

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)



2950 – 24 Switch (Standard 24 – Port Switch)



In dieser nächsten Aufgabe soll ein funktionsfähiges VLAN<sup>4</sup> eingerichtet und die grundlegende Funktion mit Hilfe der Packet Tracer Simulation verstanden werden. VLANs kommen beispielsweise in größeren Unternehmen zum Einsatz, welche ein physikalisches Netz besitzen, in diesem jedoch Abteilungen untereinander in virtuelle Teilnetze aufgeteilt sind. Dadurch ist eine Kommunikation der Fachbereiche ausschließlich untereinander gewährleistet. Man unterscheidet zwischen *statischen*, *dynamischen* und *tagged* VLANS. Diese Aufgabe basiert auf dem Prinzip des statischen VLANS, in welchem bestimmte Ports des Switches einem, vom Administrator festgelegten VLAN angehören. In diesem Beispiel sollen 3 VLANs eingerichtet werden, welche über einen Switch gesteuert werden (vgl. beispielsweise 3 Fachbereiche einer Firma auf einer Etage des Firmengebäudes). Darauf aufbauend soll noch ein weiterer Switch installiert werden, welcher über einen *Trunk*<sup>5</sup> mit dem Ausgangsswitch verbunden ist (vgl. zum Beispiel die genannten Fachbereiche auf unterschiedlichen Etagen des Firmengebäudes). Zum Aufbau des ersten einfachen VLANs platzieren Sie zunächst einen handelsüblichen 24 – Port Switch mittig auf der Arbeitsfläche. Um den eben platzierten Switch setzen Sie nun insgesamt 12 PCs, jeweils in Zweiergruppen zusammengefasst. Verbinden Sie die Computer nun mit dem Switch. Die Konstellation sollte etwa wie folgt aussehen (Abbildung 14):

---

<sup>4</sup> Als VLANs (Virtual Local Area Network) werden virtuelle Teilnetze eines physikalischen Netzes bezeichnet.

<sup>5</sup> Als Trunk wird eine physikalische Leitung bezeichnet, welche mehrere Übertragungskanäle (hier VLANs) zu einer logischen Verbindung zusammenführt.

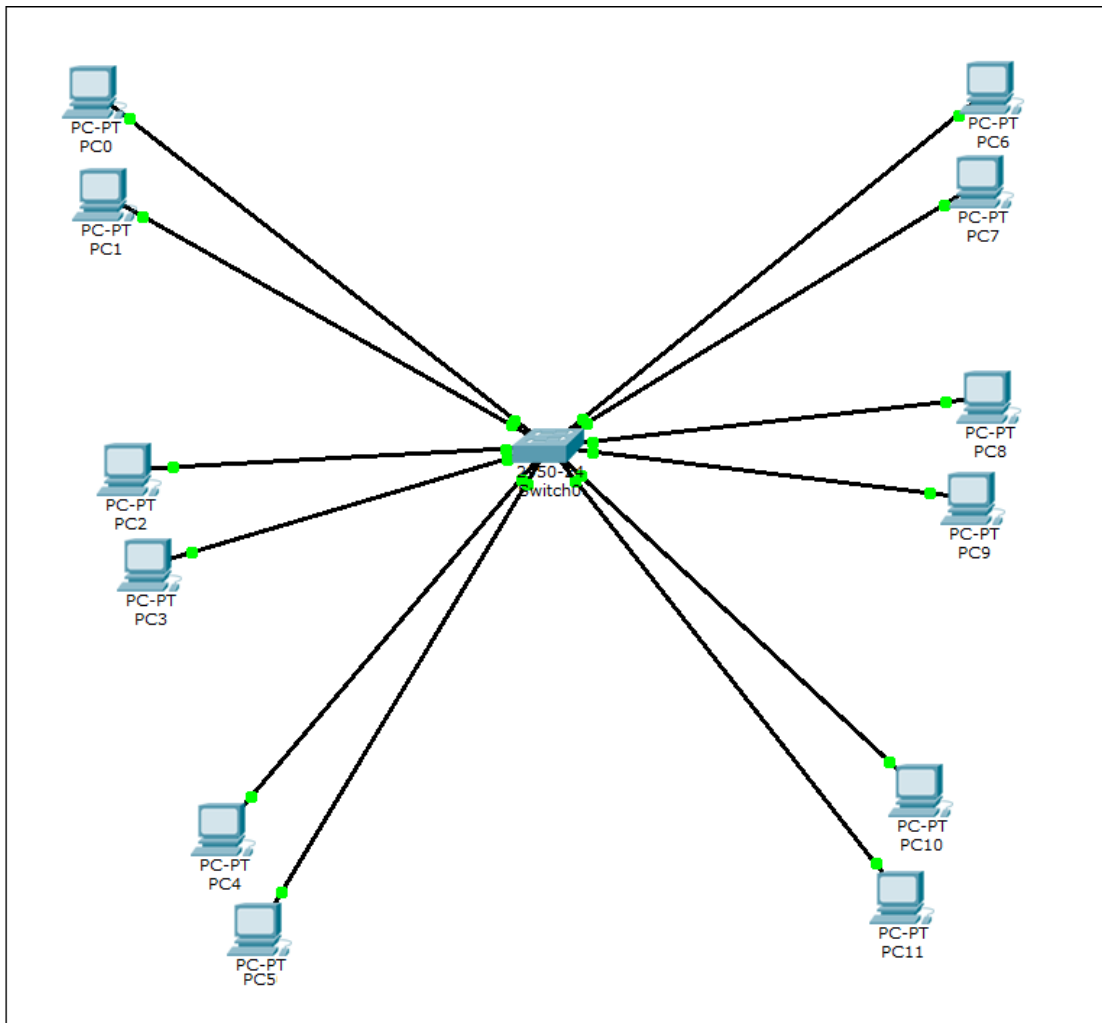


Abbildung 14

Konfigurieren Sie für jeden PC die IP Einstellungen. Achten Sie darauf, dass sich sämtliche Computer im gleichen Netz befinden sollen, da auf Routing an dieser Stelle verzichtet werden soll. Im nächsten Schritt soll sich der VLAN – Konfiguration zugewandt werden. Öffnen Sie dazu die Konfigurationsübersicht des Switches und navigieren Sie über Config nach VLAN Database (Abbildung 15).

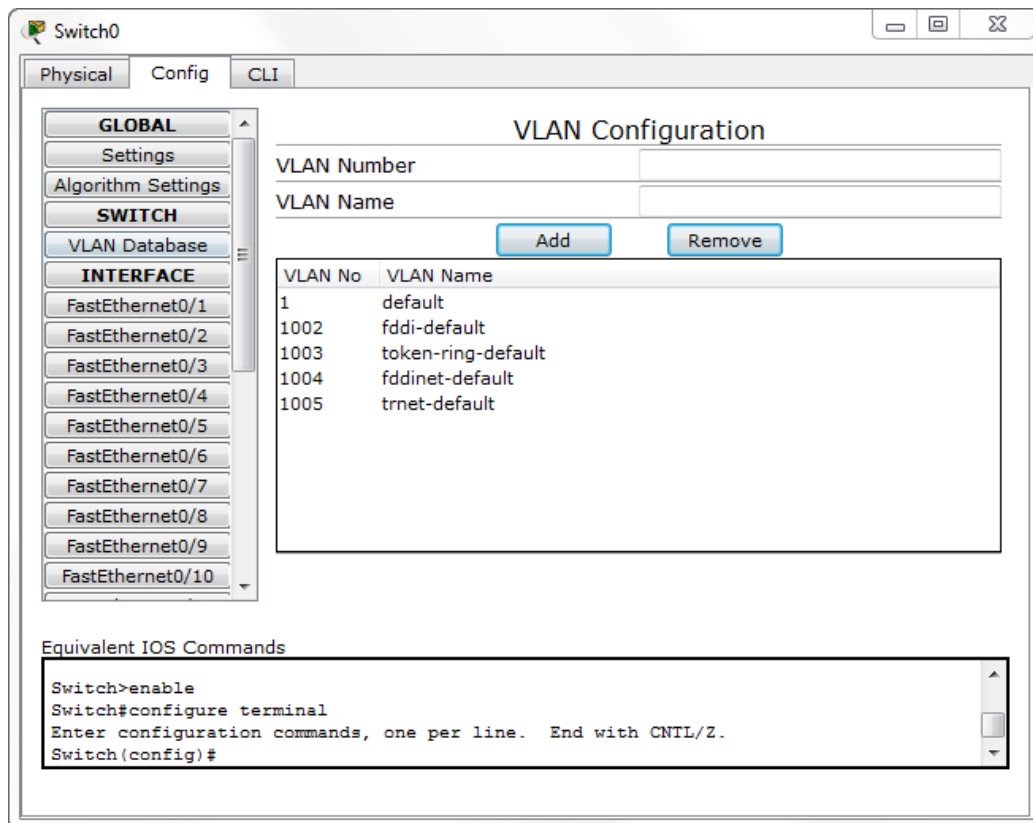


Abbildung 15

Die vorkonfigurierten Einträge können Sie an dieser Stelle ignorieren. Tragen Sie nun 3 VLAN – Netze in die Liste ein. Nutzen Sie dazu der Übersichtlichkeit wegen die Nummerierungen 10, 20 und 30. Die Namen der VLANs können sie selbst wählen. Den Eintrag fügen Sie mit einem Einfachklick auf *Add* hinzu. Begeben Sie sich nun in das Menü des Anschlusses *FastEthernet0* (dieser sollte mit *PC0* verbunden sein). Setzen Sie nun den VLAN – Modus auf *Access* und wählen Sie in der nebenstehenden Liste Ihr erstes angelegtes VLAN (10). Heben Sie sämtliche Auswahlen der anderen VLANS auf (Abbildung 16).



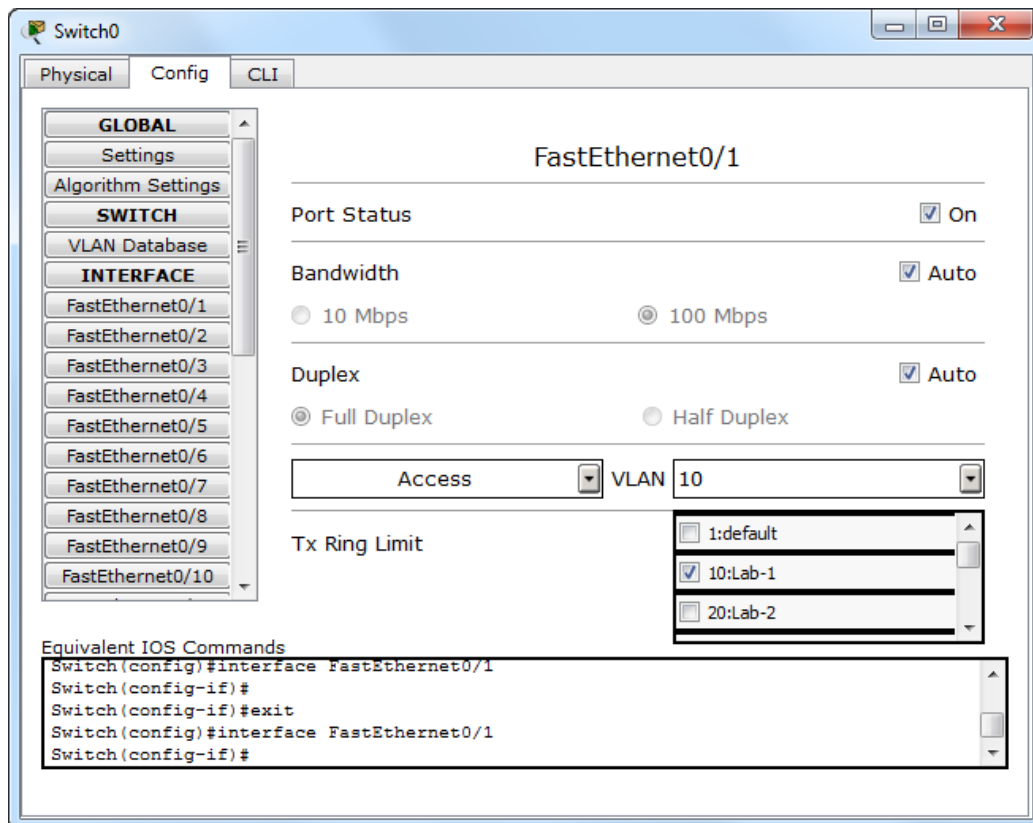


Abbildung 16

Wiederholen Sie diese Schritte nun für PC1 und das jeweils andere Computerpaar, welches Sie im gleichen VLAN geplant haben (nach Abbildung 14 PC6 und PC7). Im Anschluss daran konfigurieren Sie für die zwei anderen Computerpaare nun die zwei anderen angelegten VLANs (nach Abbildung 14 PC2 / PC3 – PC8 / PC9 VLAN 2, PC4 / PC5 – PC10 / PC11 VLAN 3). Nach diesem Schritt ist Ihr einfaches VLAN nun konfiguriert und kann getestet werden. Wechseln Sie dazu in den Simulationsmodus und stellen Sie den Protokollfilter auf ICMP. Um die Funktionsweise des VLANS zu verstehen, senden Sie nun einige Simple PDUs zwischen den einzelnen VLANS hin und her. Verfolgen Sie dazu die einzelnen Pakete und machen Sie sich ein Bild von dem stattfindenden Datenverkehr. Wie sie sehen, ist eine Übertragung nur zwischen Geräten innerhalb eines VLANS möglich, was den Verwendungszweck dieser Technologie demonstriert. Um nun *Trunking* mit in die Umgebung einzubeziehen, löschen Sie zunächst sämtliche Szenarien und wechseln zurück in den Echtzeitmodus. Platzieren Sie nun einen weiteren Switch neben dem ersten und verbinden Sie die Geräte untereinander. Trennen Sie ebenfalls jeweils ein Computerpaar vom ersten Switch und schließen Sie die insgesamt 3 Gerätepaare an den neu platzierten Switch an (Abbildung 17).

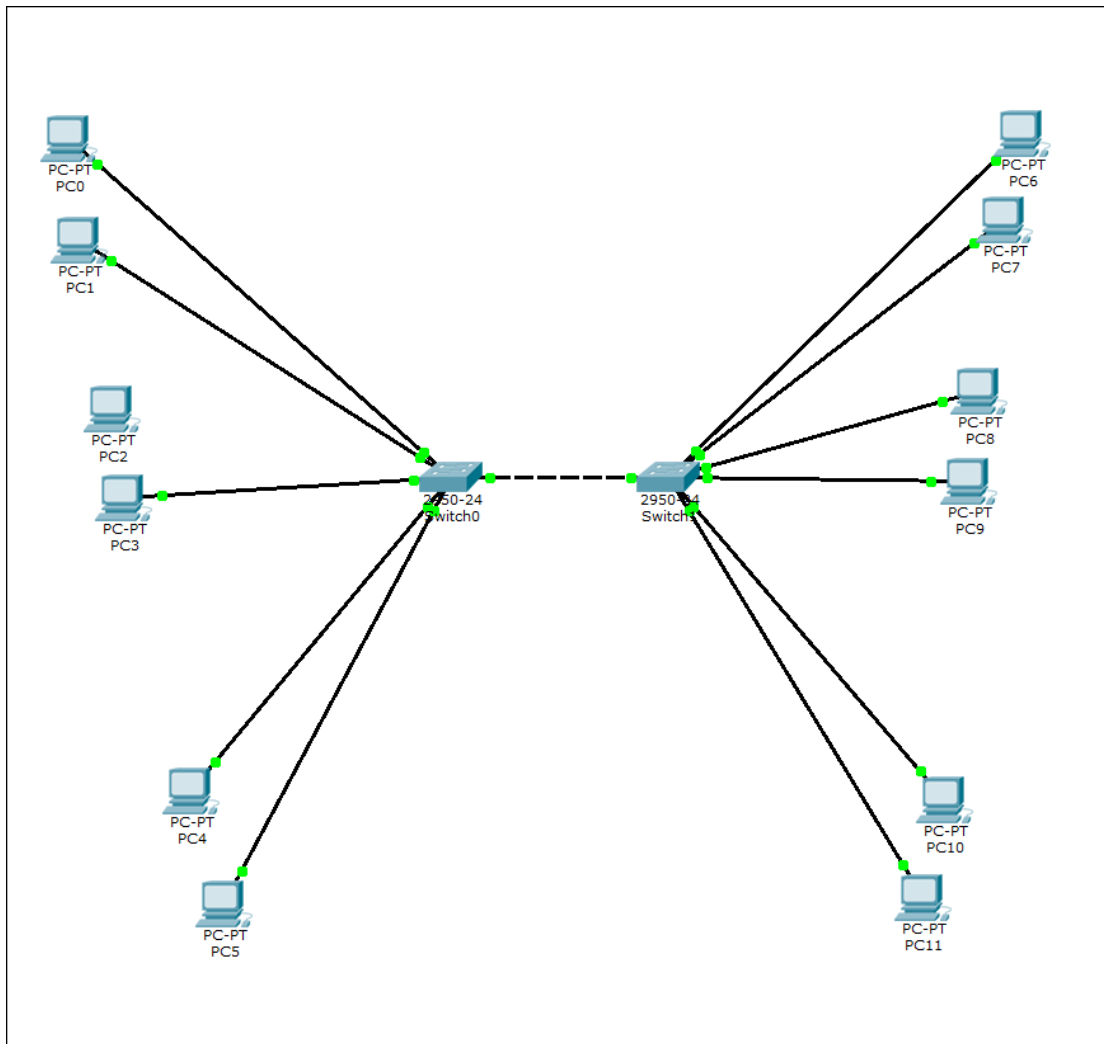


Abbildung 17

Richten Sie *Switch1* nun mit der Konfiguration von *Switch0* ein. Achten Sie dabei darauf, dass VLAN – Nummern und – Namen übereinstimmen. Begeben Sie sich nun nacheinander in die Konfigurationsterminals der beiden Switches und rufen Sie jeweils die Ports auf, über welche die Geräte miteinander verbunden sind. Wechseln Sie in den VLAN – Modus auf *Trunk* und setzen Sie die Häkchen in der nebenstehenden Liste bei allen 3 angelegten VLANs (Abbildung 18).

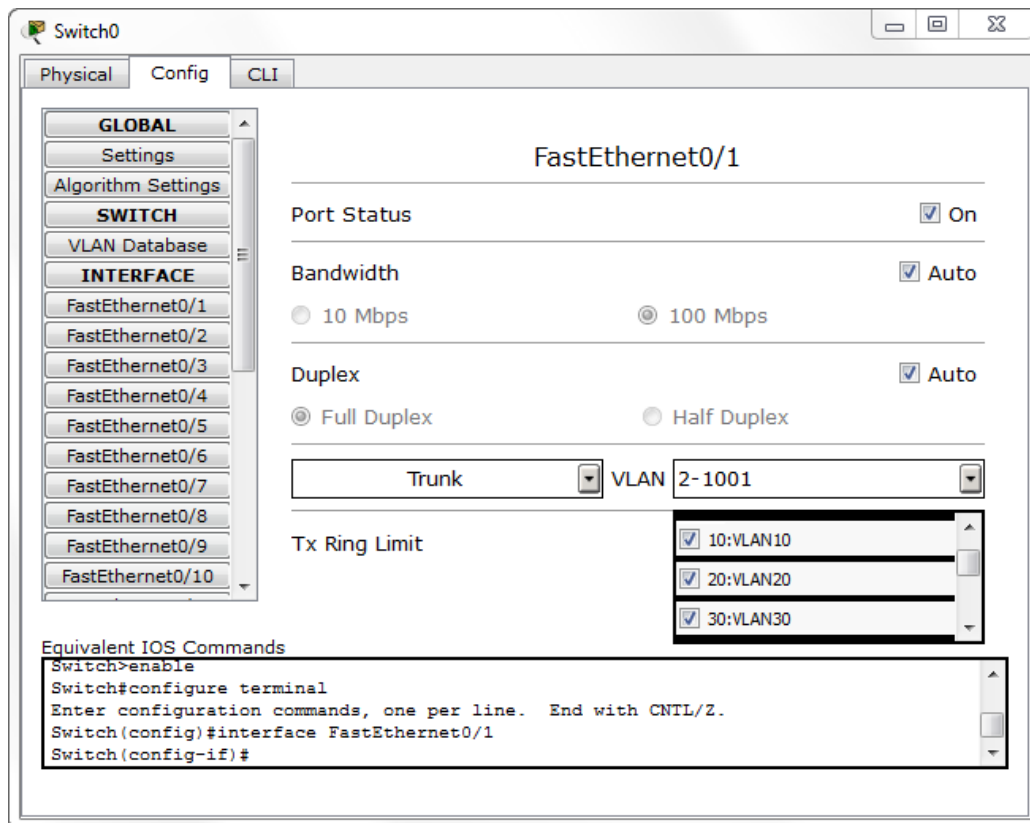


Abbildung 18

Dies bedeutet, dass der Trunk alle verwendeten VLANs verbindet und den Switches zugänglich macht. Richten Sie nun noch die Access – Ports am neuen Switch für alle PCs ein, welche an diesen angeschlossen sind (nach Abbildung 17 *PC6*, *PC7*, *PC8*, *PC9*, *PC10*, *PC11*) und weisen Sie diesen wieder die entsprechenden VLANs zu. Um die VLANs inklusive *Trunking* nun zu analysieren, wechseln Sie wieder in den Simulationsmodus und senden Sie eine einfache PDU von *PC0* an *PC6* (*VLAN10*). Verfolgen Sie den Transportweg des Pakets nun via *Capture / Forward*, bis dieses am ersten Switch eintrifft. Führen Sie einen Einfachklick auf das Briefsymbol aus, um die Detailansicht der Übermittlung aufzurufen. Wechseln Sie in *Layer 2* der *Out Layers* – Spalte (Abbildung 19).

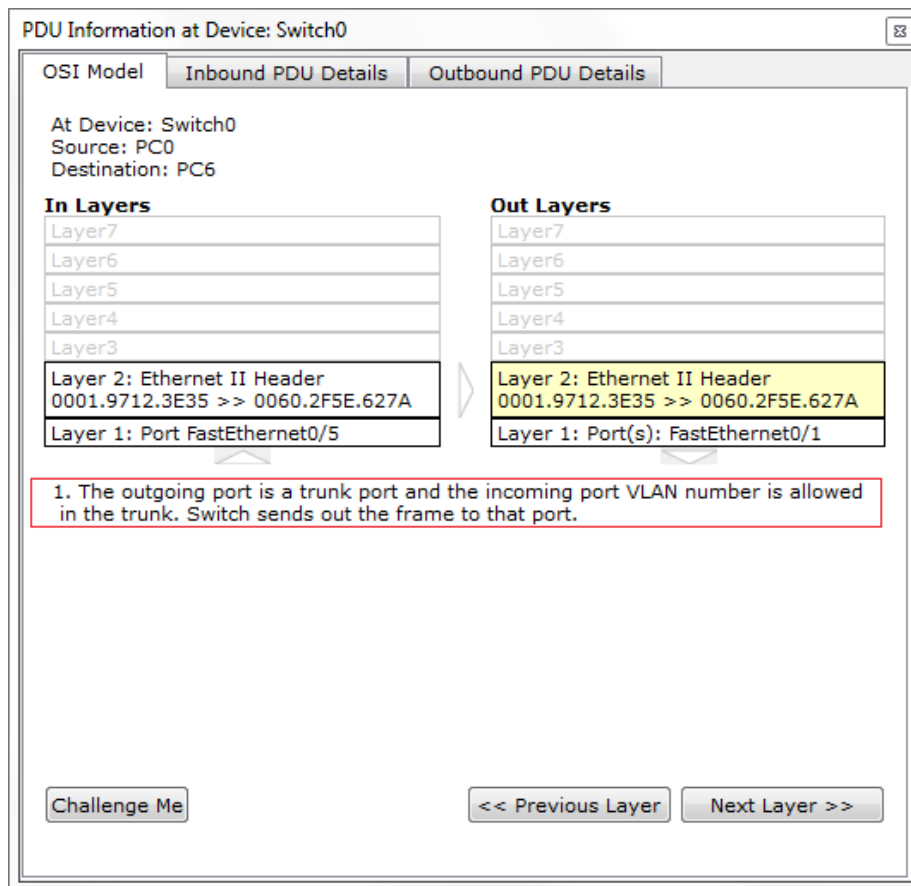


Abbildung 19

Hier sehen Sie nun, dass der Switch das Paket über den Trunk an den anderen Switch weiterleitet (vgl. Kommunikation über VLANs innerhalb eines Gebäudes auf mehreren Etagen). Durch die vorangegangenen Einstellungen erkennt der Switch, dass das eingehende Paket innerhalb eines VLANs versendet wird, welches auf dem Trunk zugelassen ist. Die Kommunikation kann fehlerfrei stattfinden.

### Aufgabe 3: Einrichten und Konfiguration einer serverseitigen Firewall

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)



2950 – 24 Switch (Standard 24 – Port Switch)



1841 – Router (Standard Router)



Generic Server (Standard Server, Dienste: HTTP, DNS, FTP)



Ziel dieser Aufgabe ist es, eine, auf Seite des Servers installierte Firewall in ein überschaubares Netzwerk zu implementieren, um so die Arbeitsweise dieser Technologie zu analysieren. Die Kriterien der Firewall soll sich an den Protokollen ICMP, TCP und UDP orientieren. Dazu werden verschiedene Dienste im Netzwerk zuerst implementiert, um anschließend die Firewall zu konfigurieren und zu testen. Ebenfalls soll der Zusammenhang zwischen verschiedenen Protokollen und Diensten in der Netzwerktechnik mit dieser Aufgabe verdeutlicht werden. Platzieren Sie zu Beginn zwei PCs, den Switch, den Router und den Server auf der Arbeitsfläche. Verbinden Sie die PCs mit dem Switch und schließen Sie diesen an den Router an. Den zweiten Ethernet – Anschluss des Routers benutzen Sie zur Verbindung mit dem Server. Rufen Sie nun die IP Konfiguration des Servers auf. Vergeben Sie die IP Adresse *10.10.10.1* an den Server und nutzen Sie die vorgeschlagene Subnetzmaske. Schließen Sie vorerst das Konfigurationsfenster des Servers und begeben Sie sich in das IP Einstellungsfenster der PCs. Nutzen Sie für die IP Konfiguration *192.x.x.x* Adressen. Tragen Sie im Feld DNS Server die IP Adresse des Servers ein, da dieser später als DNS – Server fungieren wird. Schließen Sie die Konfigurationsfenster wieder. Wenden Sie sich nun dem Routing zu und ermöglichen Sie eine Kommunikation zwischen Klienten (PCs) und Server (siehe auch *Versuch 2, Aufgabe 4*). Nach Abschluss der Konfiguration testen Sie die Kommunikation zwischen PCs und Server mittels *Simple PDU*. Funktioniert diese einwandfrei, wenden Sie sich erneut dem Server zu. Legen Sie im DNS – Menü des Servers zu Testzwecken einen Eintrag fest und schalten Sie den DNS Service auf *On* (Abbildung 20).

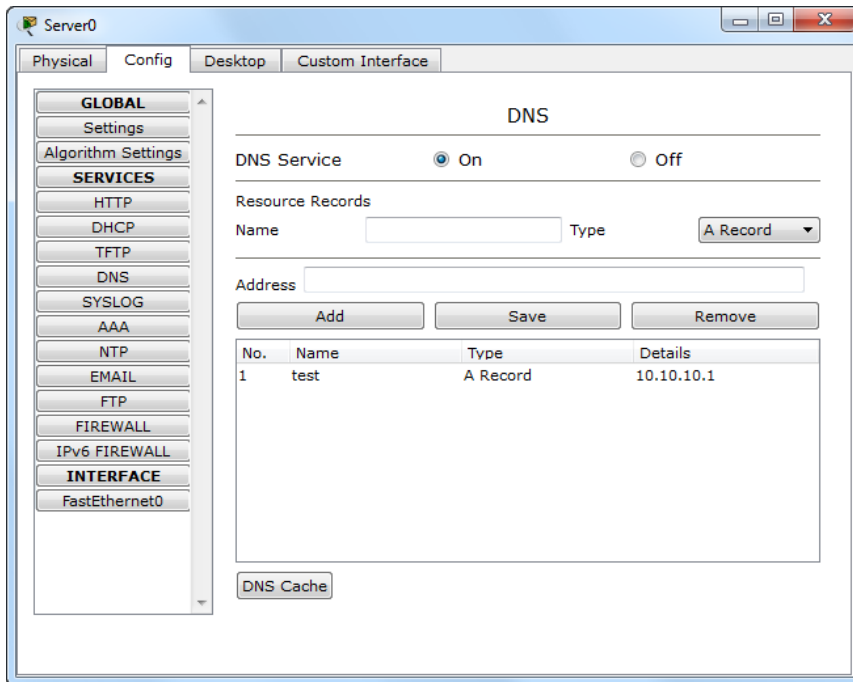


Abbildung 20

Vergewissern Sie sich, dass die Dienste HTTP und FTP aktiviert sind. Sind diese Einstellungen vollständig, kann mit der Konfiguration der Firewall begonnen werden. Navigieren Sie dazu in das entsprechende Menü über die Schaltfläche *FIREWALL* (Abbildung 21).

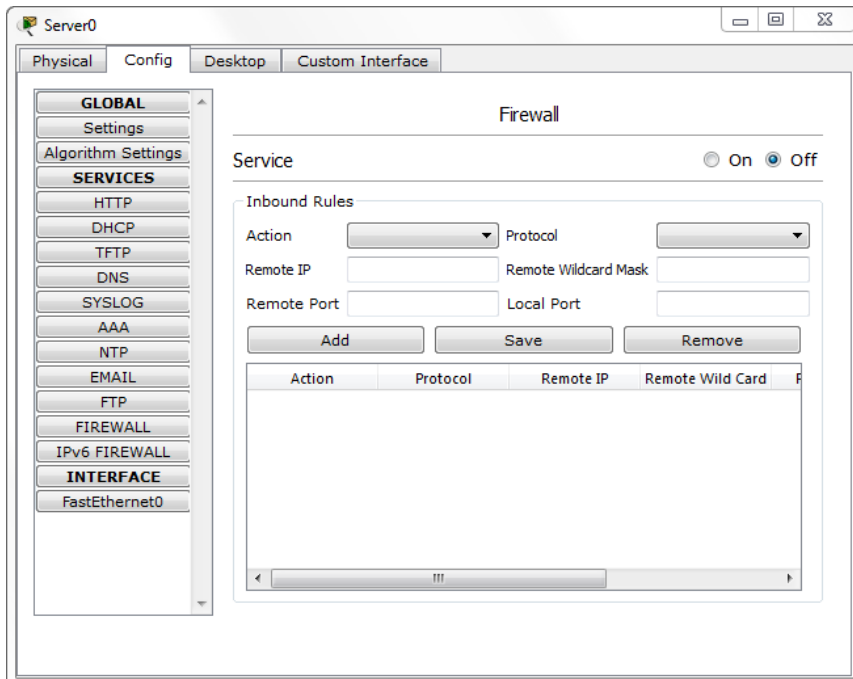


Abbildung 21

Zuerst soll eine Richtlinie für ICMP festgelegt werden. Es soll erreicht werden, dass eben jene Anfragen von der Firewall blockiert werden und somit keine Kommunikation über dieses Protokoll stattfinden kann. Wählen Sie entsprechend unter *Action* die Option *Deny*. Stellen Sie die *Protocol* – Schaltfläche auf *ICMP*. Im Feld *Remote IP* tragen Sie *192.0.0.0* ein, da sämtliche Anfragen aus diesem Netz geblockt werden sollen. Die zugehörige *Remote Wildcard Mask* lautet hier *0.255.255.255*. Für *Remote Port* und *Local Port* müssen Sie hier keine Einstellungen vornehmen. Fügen Sie den Eintrag mit einem Einfachklick auf *Add* hinzu. Die Richtlinie für ICMP Anfragen ist damit abgeschlossen. Weiterhin sollen noch 3 weitere Einträge hinzugefügt werden, welche die Protokolle TCP und UDP betreffen. Nehmen Sie diese Einstellungen mit Hilfe der nachfolgenden Tabellen vor.

#### Richtlinie für FTP

|             |                  |                      |                       |
|-------------|------------------|----------------------|-----------------------|
| Action      | <i>Deny</i>      | Protocol             | <i>TCP</i>            |
| Remote IP   | <i>192.0.0.0</i> | Remote Wildcard Mask | <i>0.255.255.255</i>  |
| Remote Port | <i>any</i>       | Local Port           | <i>21<sup>6</sup></i> |

#### Richtlinie für HTTP

|             |                  |                      |                       |
|-------------|------------------|----------------------|-----------------------|
| Action      | <i>Allow</i>     | Protocol             | <i>TCP</i>            |
| Remote IP   | <i>192.0.0.0</i> | Remote Wildcard Mask | <i>0.255.255.255</i>  |
| Remote Port | <i>any</i>       | Local Port           | <i>80<sup>7</sup></i> |

#### Richtlinie für DNS

|             |                  |                      |                       |
|-------------|------------------|----------------------|-----------------------|
| Action      | <i>Allow</i>     | Protocol             | <i>UDP</i>            |
| Remote IP   | <i>192.0.0.0</i> | Remote Wildcard Mask | <i>0.255.255.255</i>  |
| Remote Port | <i>any</i>       | Local Port           | <i>53<sup>8</sup></i> |

Aktivieren Sie nun den Dienst, indem Sie die Schaltfläche *On* aktivieren. Mit diesen Einstellungen werden nun Anfragen aus dem 192.0.0.0 - Netz blockiert, welche ICMP

<sup>6</sup> Port 21 – Standardisierter Port für FTP – Kontrollen

<sup>7</sup> Port 80 – Standardisierter Port für HTTP – Requests

<sup>8</sup> Port 53 – Standardisierter Port für DNS

nutzen. Ebenfalls abgelehnt werden TCP – Anfragen auf Port 21, also FTP – Verbindungen. Zugelassen hingegen sind HTTP – Requests und Anfragen, die DNS benutzen. In den nächsten Schritten soll ein genauerer Blick auf diese Funktionsweise geworfen werden. Wechseln Sie in den *Simulationsmodus* und ändern sie den *Event List Filter* auf *ICMP*. Senden Sie nun eine *Simple PDU* von einem der beiden PCs an den Server und verfolgen Sie mit *Capture / Forward* den Übertragungsweg des Pakets. Sobald dieses den Server erreicht, wird es verworfen (Abbildung 22).

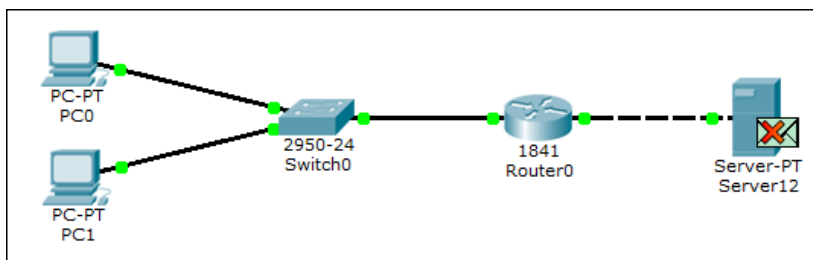


Abbildung 22

Führen Sie nun einen Einfachklick auf das Briefsymbol aus, um einen detaillierteren Einblick über die Übertragung zu erhalten. Schicht 1 und Schicht 2 arbeitet hier normal (Abbildung 23 und 24).

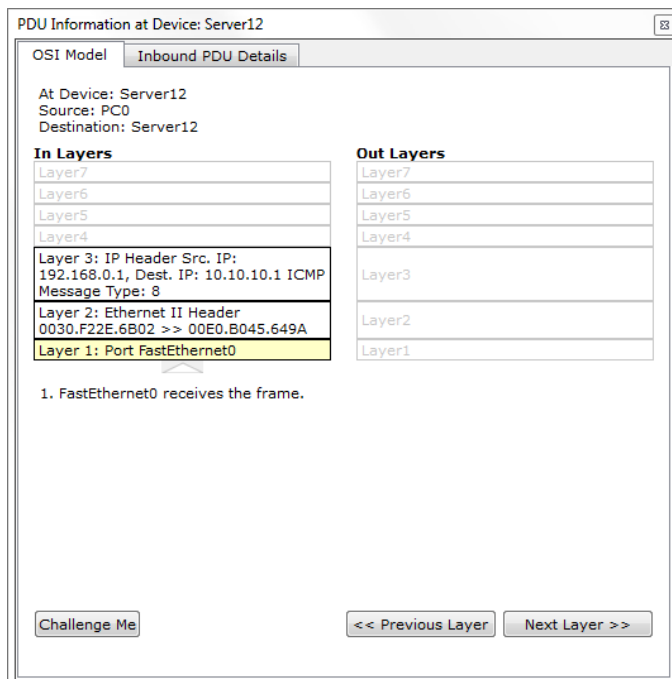


Abbildung 23



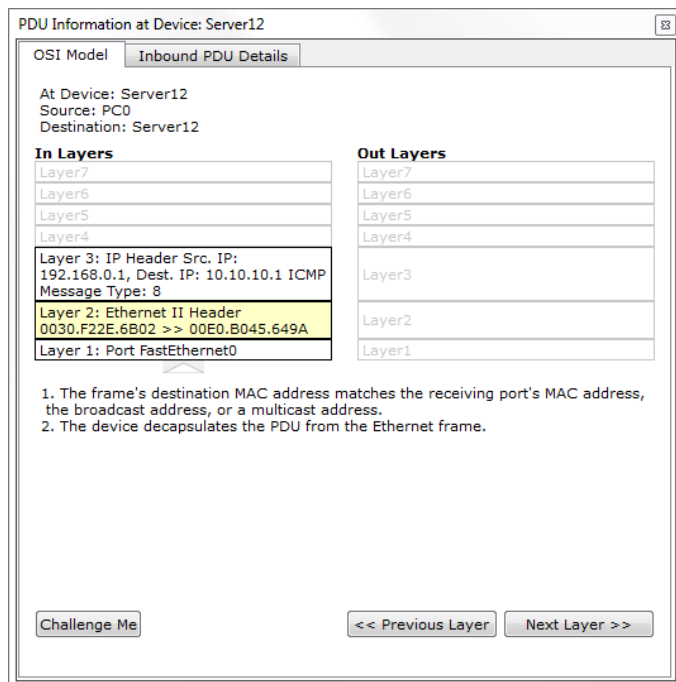


Abbildung 24

Da sich die konfigurierte Richtlinie auf ICMP Pakete beschränkt und keine Portbeschränkungen nennt, arbeitet diese als Paketfilter auf Schicht 3 des OSI – Referenzmodells. Per Einfachklick auf *Layer 3* rufen Sie die Informationen zur Paketübermittlung auf, welche auf Schicht 3 stattfinden. Sie erkennen, dass die Firewall des empfangenden Gerätes (hier: Server) das übertragene Paket mit der festgelegten Konfiguration abgleicht und daraufhin das Datenpaket ablehnt. Das Paket weist Übereinstimmungen mit den Ablehnungskriterien der Firewall auf und wird damit verworfen (Abbildung 25).

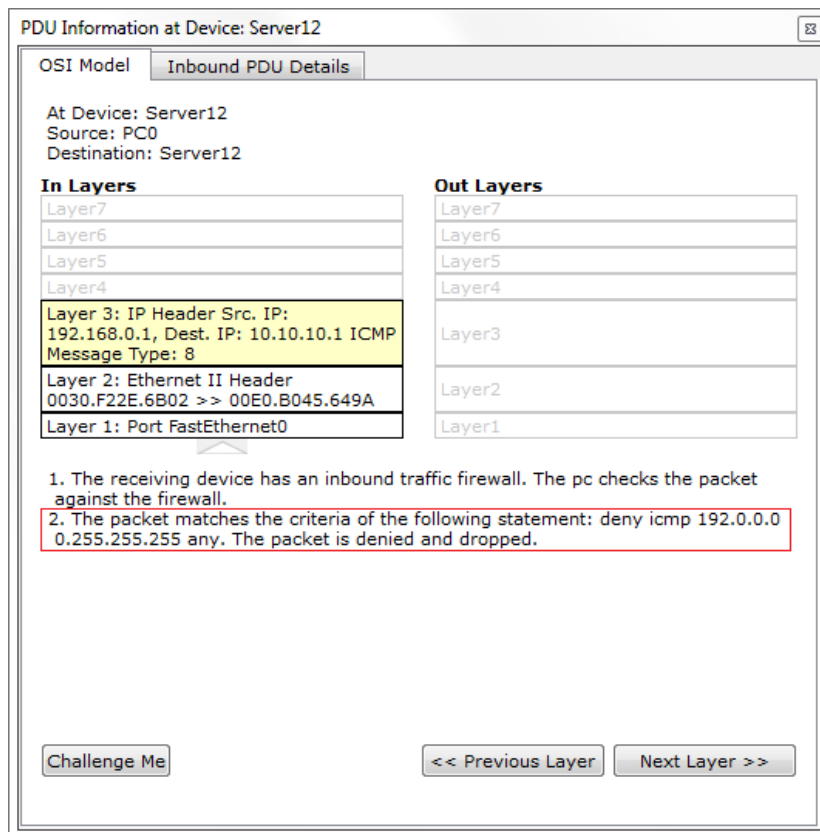


Abbildung 25

Um eine nächste Übertragung zu verfolgen, löschen Sie zunächst die zuletzt durchgeführte Übermittlung mit einem Einfachklick auf *Delete* im Szenario – Manager. Bei der nächsten Sendung soll es sich um eine FTP – Anfrage handeln. Stellen Sie also den Event Filter auf TCP, da für den Transport von FTP – Paketen dieses Protokoll verwendet wird. Öffnen Sie nun die Kommandozeile eines PCs via *Desktop / Command Prompt*. Geben Sie

*ftp 10.10.10.1*

in diese ein und schicken Sie den Befehl durch Betätigen der Enter – Taste ab. Es erscheint nun ein Briefsymbol am sendenden PC auf der Arbeitsfläche (Abbildung 26).

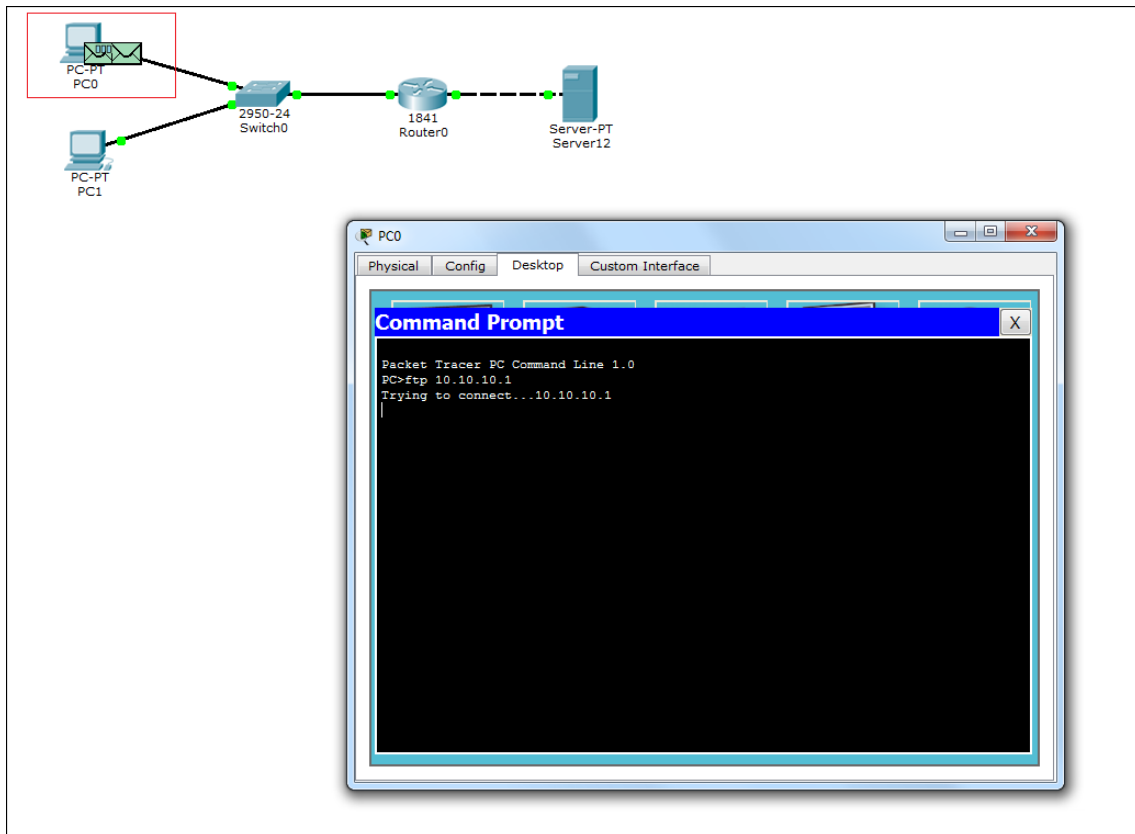


Abbildung 26

Per wiederholtem Klick auf *Capture / Forward* können Sie den Weg des Pakets erneut verfolgen. Sobald das Paket den Server erreicht hat, führen Sie einen Einfachklick auf das Briefsymbol aus. Unter Layer 3 wird Ihnen, wie schon bei der vorherigen Paketübertragung, angezeigt, dass dieses Paket ebenfalls die Ausschlusskriterien der Firewall erfüllt und somit verworfen wird. Im nächsten Schritt soll demonstriert werden, wie die Firewall zugelassene Pakete passieren lässt und eine Übertragung ermöglicht. Schließen Sie zuerst die Kommandozeile und entfernen Sie das eben durchgeführte Szenario wieder. Fügen Sie *DNS* dem *Event List Filter* hinzu. Begeben Sie sich anschließend zurück in die Desktopumgebung eines PCs und rufen Sie den Web Browser auf. In die Adresszeile geben Sie nun den Namen ein, welchen Sie in der DNS Konfiguration am Server festgelegt haben. Mit einem Einfachklick auf Go schicken Sie die Anfrage ab. Wieder erscheint das Briefsymbol am verwendeten PC. Per *Capture / Forward* können Sie den Weg des Pakets beobachten. Rufen Sie die Detailansicht erneut auf, sobald das Paket den Server erreicht. Layer 3 gibt Ihnen erneut Auskunft, wie die gesendete Einheit behandelt wird. In diesem Fall erfüllt dieses die Zulassungskriterien der Firewall und wird weiter bearbeitet (Abbildung 27).

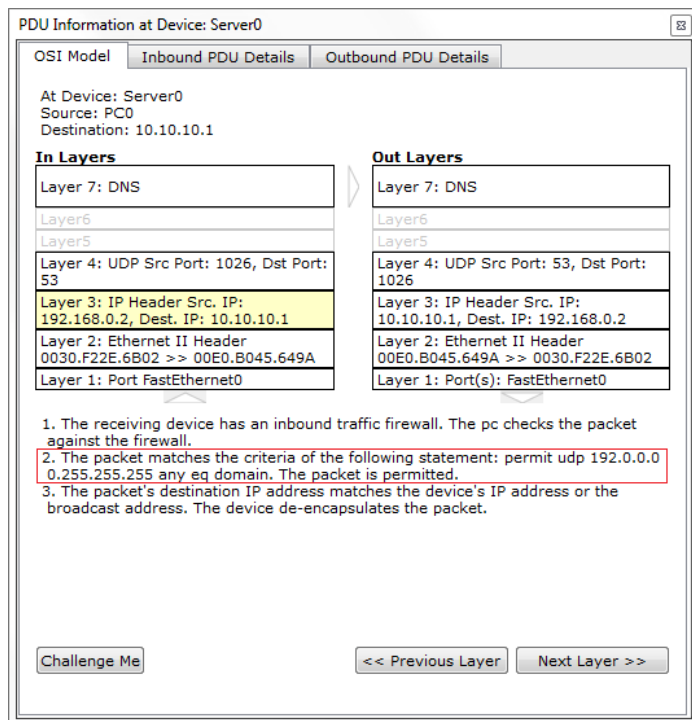


Abbildung 27

Diese Ansicht ermöglicht ebenfalls einen sehr guten Einblick in die Arbeitsweisen des DNS – Dienstes, in Hinblick auf das OSI – Modell. Mit einem Einfachklick auf *Auto Capture / Play* setzen Sie die komplette Kommunikation, ausgelöst durch den DNS – Request im Browser, fort und können diese verfolgen. Hier kann beispielsweise die Übersetzung des DNS – Namen in die zugehörige IP – Adresse eingesehen und beobachtet werden, welche Übertragungen hier stattfinden, bis letztendlich ein Ergebnis beim Klienten ankommt. Abschließend können Sie nun die Firewall nach Ihren Wünschen konfigurieren und verschiedene Szenarien testen.

#### Aufgabe 4: Simulation der IP – Übersetzung via NAT

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)



2950 – 24 Switch (Standard 24 – Port Switch)




Generic Router (Standard Router)



Generic Server (Standard Server)



In der Praxis ist die eigentliche IP Adresse eines Gerätes heutzutage nur noch selten die direkte Kontaktadresse für Kommunikationsanfragen von außen (Beispiel Webserver). Stattdessen werden sämtliche privat nutzbare Adressen in eine öffentliche IP – Adresse übersetzt, über welche sämtliche Anfragen dann erfolgen. Dies führt dazu, dass IP – Adressen von verschiedenen Klienten mehrfach verwendet werden können (da sie logisch nur über eine öffentliche IP – Adresse kommunizieren) und somit die Verteilung der IPv4 – Adressen verlangsamt wird. Die grundlegende Funktionsweise dieser Technologie soll in dieser Aufgabe mit einem Packet Tracer Szenario demonstriert werden. Platzieren Sie zuerst zwei handelsübliche Computer, welche über einen Switch mit dem Generic Router verbunden sind, auf der Arbeitsfläche. Zusätzlich setzen Sie einen Server und verbinden Sie ihn mit einem weiteren Generic Router. Verbinden Sie beide Router mit einem  Serial DCE – Kabel. Das Netzwerk kann nun konfiguriert werden (Abbildung 28).

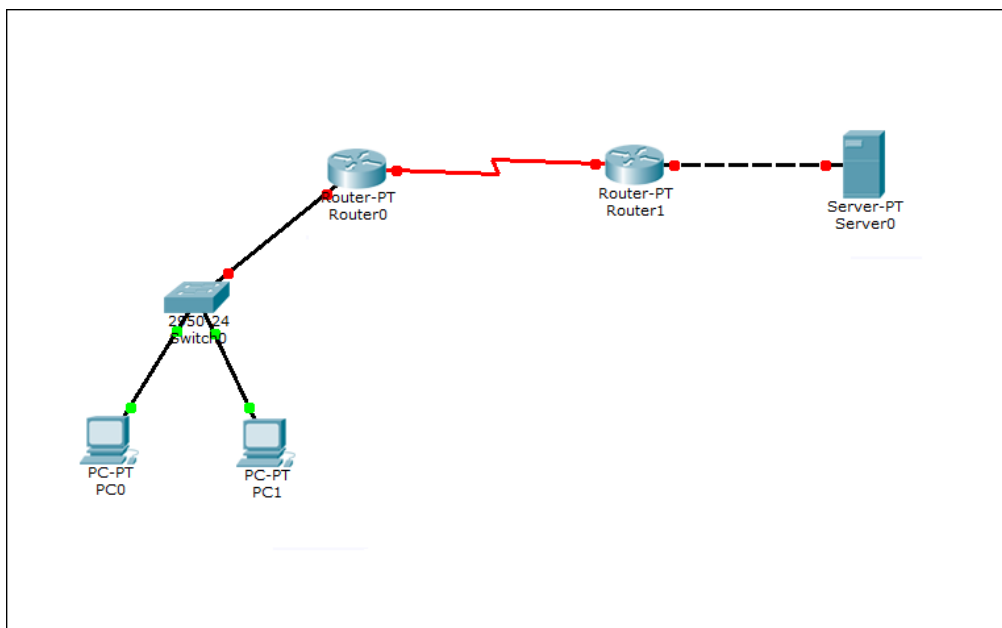


Abbildung 28

Zuerst vergeben Sie statische IP – Adressen an die Endgeräte. Nutzen Sie für die PCs 192.168.1.x – Adressen. Konfigurieren Sie dementsprechend am *FastEthernet* – Port von *Router0* eine Adresse als Gateway für dieses Netz und aktivieren Sie den Port. Tragen Sie die Gateway – Einstellungen in die IP – Konfigurationen der

Computer ein. In einem nächsten Schritt konfigurieren Sie den Server und den dazugehörigen Router1. Nutzen Sie für den Server die IP 10.0.0.254. Dem dazugehörigen Routeranschluss geben Sie die IP 10.0.0.1. Tragen Sie diese ebenfalls als Gateway am Server ein. Abschließend vergeben Sie noch die öffentliche IPs an die seriellen Ports der Router:

Router0     200.10.0.1

Router1     200.10.0.2

Die IP – Konfigurationen der Geräte ist nun abgeschlossen. Um eine Kommunikation zwischen Server und Klienten zu ermöglichen, müssen Sie nun eine IP Route festlegen, die den Transport ermöglicht. Dies soll hier über eine Default Route 0.0.0.0 0.0.0.0 erfolgen. Öffnen Sie dazu die Konsole von Router0 und begeben Sie sich in den globalen Konfigurationsmodus. Setzen Sie die Route und definieren Sie diese über den seriellen Anschluss mit dem Befehl

```
ip route 0.0.0.0 0.0.0.0 s2/0
```

Schließen Sie das Konfigurationsfenster von Router0 und wiederholen Sie diesen Schritt bei Router1. Nun kann eine Kommunikation zwischen Server und PCs stattfinden. Testen Sie dies, indem Sie eine Simple PDU von einem der beiden PCs an den Server senden (Echtzeitmodus). Öffnen Sie nun zu Demonstrationszwecken den Webbrowser von PC0 und geben Sie die IP des Servers in die Adresszeile ein (vergewissern Sie sich, dass der http Dienst am Server aktiviert ist). Es wird Ihnen die konfigurierte Website angezeigt. In der Praxis ist die direkte IP des Webservers jedoch nicht immer bekannt. Der Request wird dann häufig an ein Gerät (hier Router1) mit einer öffentlichen IP gesendet, welche diesen dann an den Server weiterleitet und die Antwort zurückleitet. Dabei wird dessen IP via NAT übersetzt, womit als Source – IP hier die öffentliche IP des Routers im IP Header des Pakets auftaucht. Dies soll nun demonstriert werden. Um eine Detailüberblick auf die Übertragung ohne NAT zu werfen, begeben Sie sich in den Simulationsmodus und stellen Sie den Event Filter auf ICMP. Schicken Sie nun erneut eine Simple PDU von PC0 an den Server und verfolgen Sie die Übertragung mittels Capture / Forward bis das Paket Router1 erreicht. Öffnen Sie nun die Detailansicht per Einfachklick auf das Briefsymbol und rufen Sie die Inbound PDU Details auf (Abbildung 29).

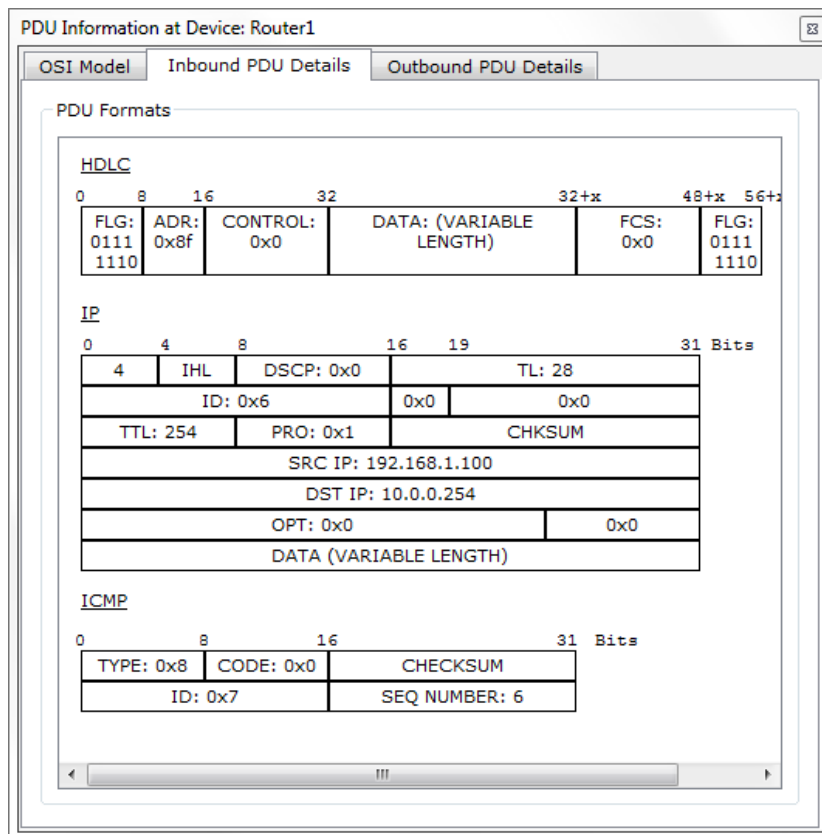


Abbildung 29

Wie zu erkennen, ist als Ziel – IP die direkte IP des Servers im Paket enthalten. Ebenso findet sich als Source IP die Adresse des sendenden Rechners. Löschen Sie das aktuelle Szenario und begeben Sie sich zurück in den Echtzeitmodus. Um Nat nun zu konfigurieren, begeben Sie sich in die Konsole des Serverrouters und rufen den globalen Konfigurationsmodus auf. Zunächst sollen alle Pakete, welche vom Server kommen, auf die öffentliche IP Adresse des Routers übersetzt werden. Dabei wird die Adresse des Servers auf die öffentliche Adresse des Routers gemappt. Dies geschieht über den Befehl

*ip nat inside source static 10.0.0.254 200.10.0.2*

Im nächsten Schritt muss dem Router mitgeteilt werden, welcher Port als Ein- bzw. als Ausgang für die NAT – Übersetzung verwendet werden soll. Begeben Sie sich per

*interface fa0/0*

in die Konfiguration des Ethernet – Ports, an den der Server angeschlossen ist und definieren Sie ihn via

```
ip nat inside
```

als Eingangsport. Verlassen Sie mit *exit* diesen Port und wechseln Sie mit

```
interface s2/0
```

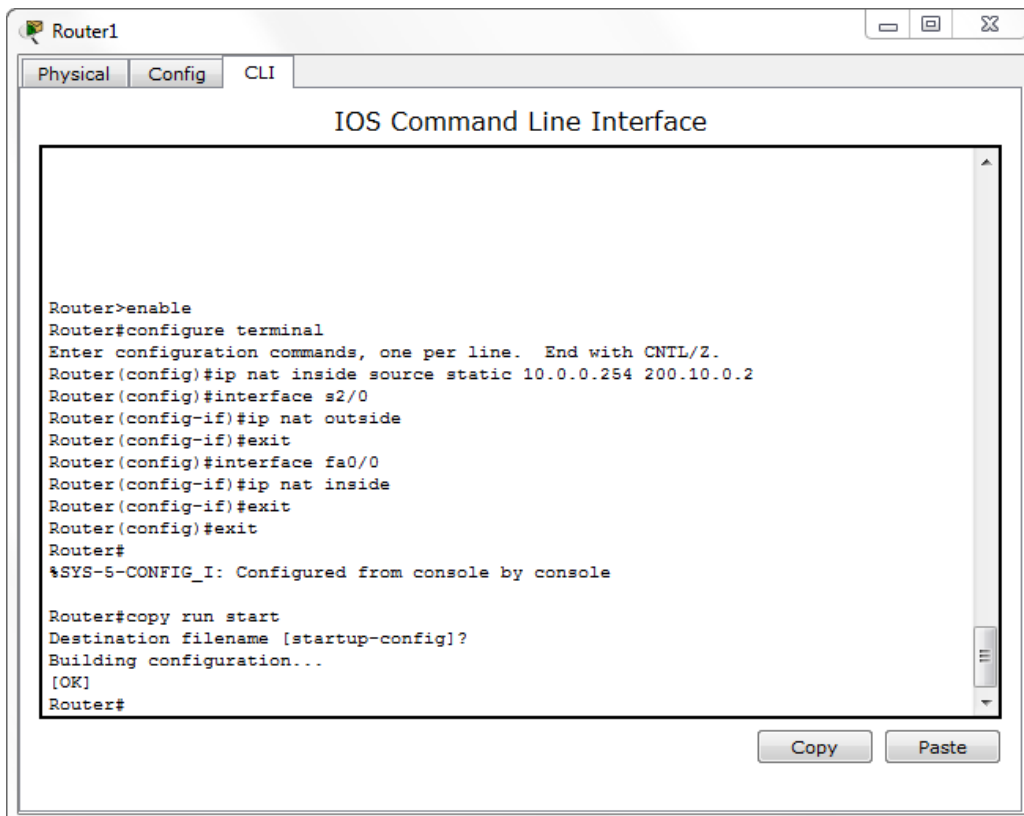
zum seriellen Port. Legen Sie nun mit dem Befehl

```
ip nat outside
```

diesen Port als Ausgangsport für die Adressübersetzung fest. Durch zweimaliges Absenden des *exit* – Befehls und einmaliges Betätigen der Enter – Taste gelangen Sie zurück in den Standard Konfigurationsmodus des Routers. Speichern Sie Ihre Einstellungen mit dem Befehl

```
copy run start
```

und bestätigen Sie die nachfolgende Frage mit Enter (Abbildung 30).



The screenshot shows a terminal window titled "Router1" with tabs for "Physical", "Config", and "CLI". The main window is titled "IOS Command Line Interface" and displays the following commands and their outputs:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 10.0.0.254 200.10.0.2
Router(config)#interface s2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

Abbildung 30



Schließen Sie die Konsole. Serverseitig ist die NAT Technologie nun implementiert. Dies können Sie überprüfen, indem Sie erneut den Webbrowser eines PCs aufrufen. Geben Sie nun die IP – Adresse des Servers ein, werden Sie kein Ergebnis erhalten. Benutzen Sie hierfür allerdings die Öffentliche IP – Adresse des Serverrouters, wird Ihnen die Website angezeigt. Im nächsten Schritt wird NAT nun auch in Router0 eingebunden. Öffnen Sie dazu die Konsole von Router0 und arbeiten Sie sich in den globalen Konfigurationsmodus vor. Zuerst wird hier nun eine Zugangsliste angelegt, welche es erlaubt, sämtliche Geräte des Netzes 192.168.1.x an diesem Router zu betreiben. So muss nicht jedes einzelne Gerät manuell am Router auf NAT konfiguriert werden. Diese Liste legen Sie mit dem Befehl

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

an. Die verwendete Wildcard Maske steht hier für die umgekehrte Subnetzmaske. Mit dem nächsten Befehl

```
ip nat inside source list 1 interface s2/0 overload
```

kommt NAT zum Einsatz, denn alle Geräte, welche zu List1 gehören, sollen auf die öffentliche Adresse des seriellen Ports am Router übersetzt werden. Abschließend müssen nun noch Ein- und Ausgangsport definiert und die Einstellungen gespeichert werden. Gehen Sie dabei wie bei der Konfiguration des Serverrouters vor (achten Sie auf die korrekten Portbezeichnungen, an denen Sie die Geräte angeschlossen haben). Ist dies abgeschlossen können Sie das Konsolenfenster schließen und die NAT Konfiguration testen. Rufen Sie die Kommandozeile eines PCs auf und versuchen Sie, mittels *ping 10.0.0.254* den Server direkt zu erreichen. Da nun auf Grund der NAT – Übersetzung der Server so nicht mehr antwortet, wird keines der gesendeten Datenpakete erfolgreich übermittelt (Abbildung 31).

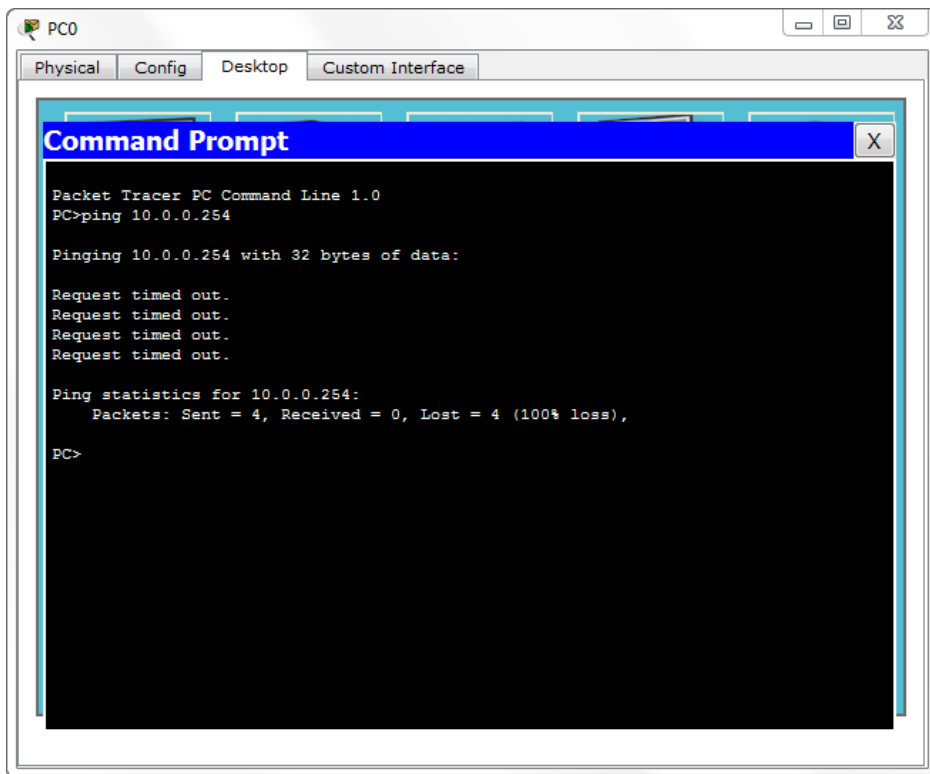


Abbildung 31

Wechseln Sie nun in den Simulationsmodus und starten Sie eine Übertragung mittels Simple PDU von PC0 an den Serverrouter. Verfolgen Sie das Paket, bis dieses bei Router0 angekommen ist und öffnen Sie die Detailansicht der Übertragung. Rufen Sie nun nacheinander die Inbound PDU Details und die Outbound PDU Details auf (Abbildung 32 und 33).

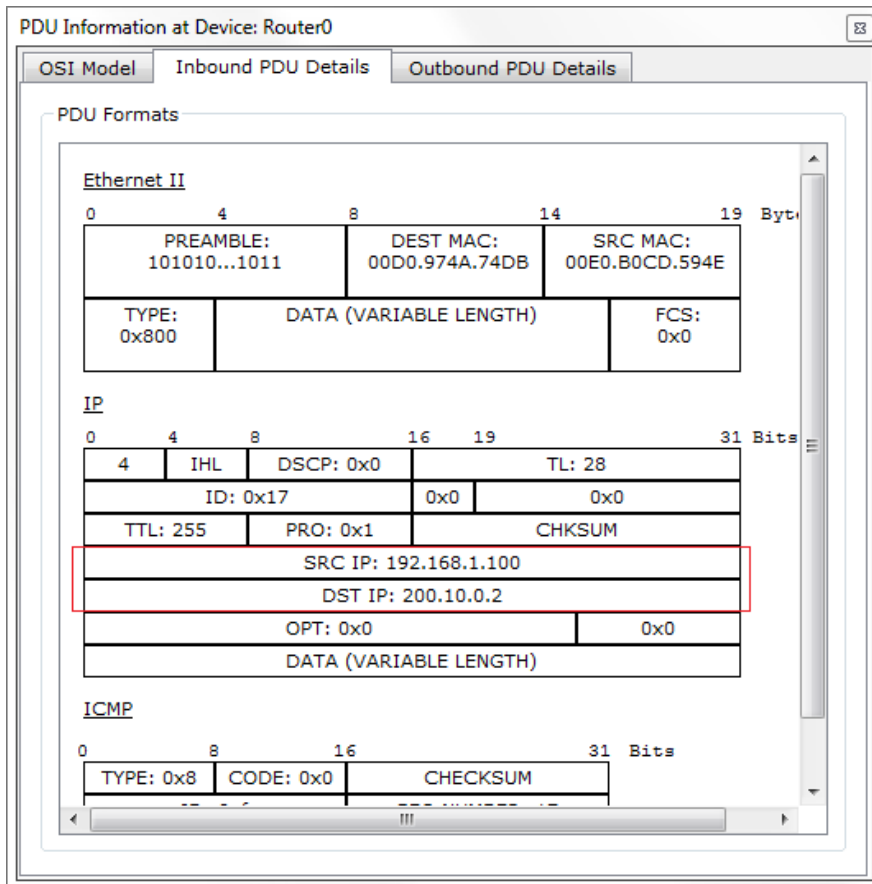


Abbildung 32

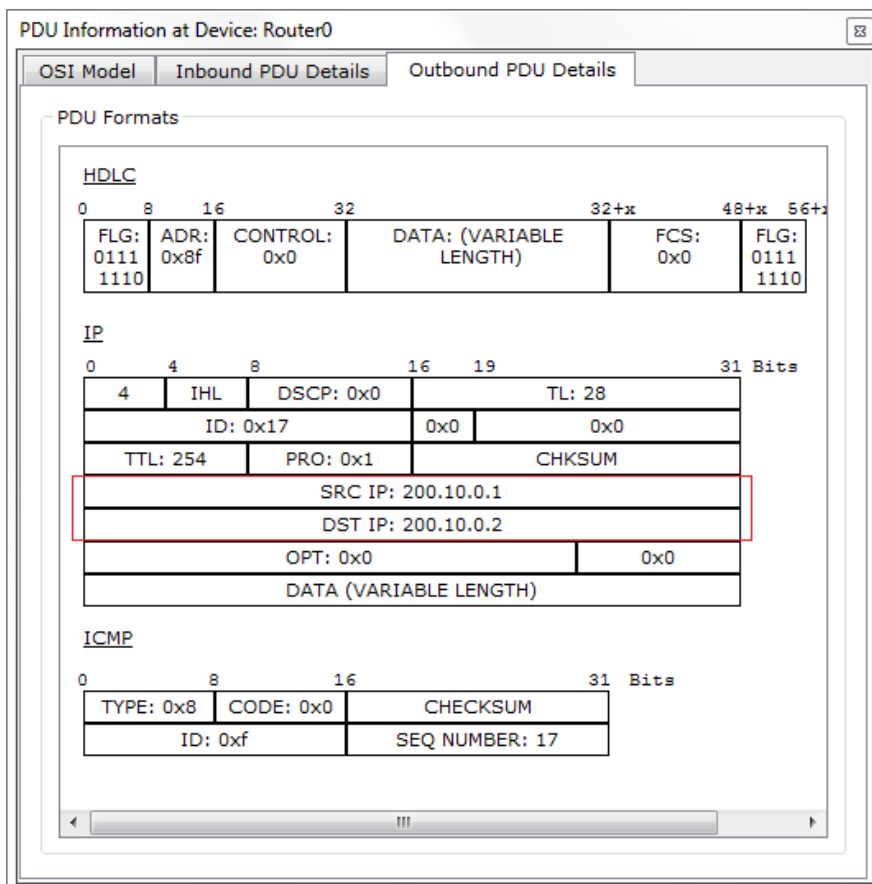


Abbildung 33

Hier wird deutlich, dass die Source IP des Rechners nur im IP Header des Pakets vorhanden ist, bis dieses den Router erreicht. Dieser übersetzt diese Adresse via NAT nun, wie in den Outbound PDU Details erkennbar ist. Beobachten Sie nun den weiteren Verlauf des Pakets. Obwohl Sie die PDU an Router1 geschickt haben, wird das Paket an den Server weitergeleitet. Rufen Sie die Detailansicht der Übertragung auf, wenn diese den Server erreicht hat und navigieren Sie die in die Outbound Details (Abbildung 34).

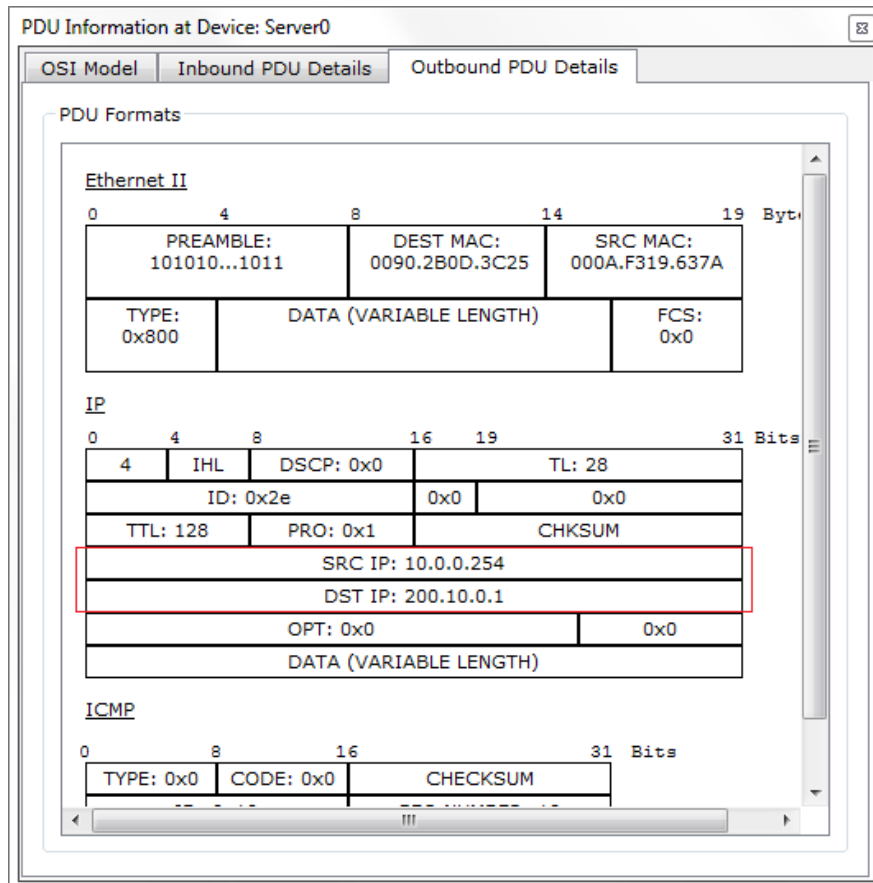


Abbildung 34

Der Server schickt dieses Paket an die öffentliche IP des Routers, da ihm durch die NAT – Übersetzung die ursprüngliche Herkunft des Paketes nicht bekannt ist. Das Paket wird in den nächsten Schritten über Router1 zurück an Router0 übermittelt, wo es die Ziel IP des sendenden PCs zurückerhält, damit dieser die Antwort entgegennehmen kann.

## Aufgabe 5: Simulation eines IPv6 – basierenden Netzwerkes

Zum Einsatz kommende Hardware:

Generic PC (Standard PC)



2950 – 24 Switch (Standard 24 – Port Switch)



1841 – Router (Standard Router)



Durch die NAT – Technologie kann die Verteilung und das damit verbundene Zuneigehen der IPv4 Adressen deutlich gebremst werden. Jedoch bringt NAT auch Probleme mit sich (siehe auch Seite 58, Vorlesungsskript Administration und Netzwerktechnik II), weshalb IPv6 als Nachfolge für IPv4 entwickelt wurde. Diese Aufgabe widmet sich der Simulierung eines einfachen privaten Netzwerkes, welches auf IPv6 – Adressierungen basiert (siehe auch Seite 68f., Vorlesungsskript Netzwerktechnik und Administration II). Mittels der Packet Tracer Software soll dieses Netzwerk aufgebaut werden und einige, in der Vorlesung behandelte Elemente simulieren. Arrangieren Sie zunächst alle benötigten Geräte auf der Arbeitsfläche. Es sollen insgesamt 3 PCs, ein Router, sowie zwei Switches zum Einsatz kommen. Der erste und zweite Computer sind über einen Switch an den Anschluss *FastEthernet0/0* des Routers angeschlossen. Über das weitere Interface *FastEthernet0/1* des Routers ist der dritte Computer über einen zweiten Switch verbunden (Abbildung 35).

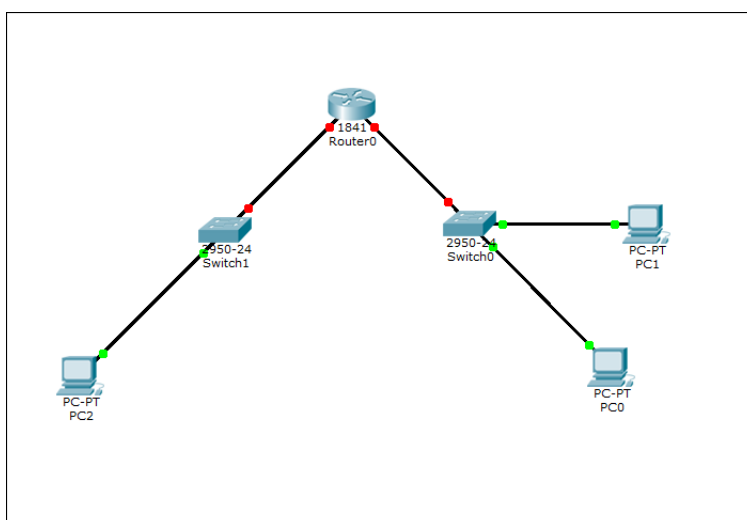


Abbildung 35

In einem nächsten Schritt soll der Router für die Arbeit mit IPv6 vorbereitet und die Link – Local Adressen der beiden verbundenen Routerinterfaces konfiguriert werden. Normalerweise werden diese Adressen zwar beim Start eines Gerätes automatisch erzeugt, jedoch ist es zu Administrationszwecken von Vorteil, diese Einstellung (zumindest in diesem Größenumfang) manuell vorzunehmen. Begeben Sie sich dazu in die Konsole von Router0. Verschaffen Sie sich nun Zugang zum globalen Konfigurationsmodus. Aktivieren Sie das IPv6 – Routing mittels des Befehls

```
ipv6 unicast-routing
```

Der Router kann nun damit arbeiten. Nachfolgend soll die Link – Local Adresse von Interface *FastEthernet0/0* festgelegt werden. Diese soll *FE80::1* lauten (verkürzte Schreibweise). Begeben Sie sich per

```
interface fa0/0
```

in die Konfigurationsumgebung für diesen Anschluss. Mit Hilfe des Befehls

```
ipv6 address FE80::1 link-local
```

weisen Sie diese Adresse dem Port zu und definieren Sie gleichzeitig als Link – Local Adresse. Speichern Sie diese Konfiguration mit Hilfe der Eingabe

```
no shutdown
```

und betätigen nach der Bestätigung dieses Befehls erneut die Enter – Taste, um zurück in den Konfigurationsmodus zu gelangen.

Verlassen Sie per *exit* nun die Konfiguration dieses Anschlusses und wenden Sie sich via

```
interface fa0/1
```

dem anderen Port zu. Auf Grund der Funktionsweise von IPv6 und der rein lokalen Signifikanz der Link – Local Adresse kann der Port *FastEthernet0/1* ebenfalls die Adresse *FE80::1* erhalten. Weisen Sie diesem Anschluss nun ebenfalls diese Adresse zu und speichern Sie diese Konfiguration. Beide Anschlussknoten des Routers sollten nun grün gekennzeichnet sein. Jedoch kann noch keine Kommunikation zwischen den beiden Netzen stattfinden, da der Router, sowie die Endgeräte noch keine routingfähigen globalen Unicast – Adressen besitzen. Für die

Konfiguration soll eine IPv6 Adresse verwendet werden, welche ein 64bit – Netzwerkpräfix besitzt. Für Netz 1 (Anschluss *FastEthernet0/0*) soll folgende Adresse verwendet werden:

*2015:00A1:AAAA:000A:0000:0000:0000:0001* (volle Schreibweise)

(Netzpräfix *2015:00A1:AAAA:000A*)

*2015:A1:AAAA:A::1* (verkürzte Schreibweise)

Hierbei handelt es sich bei *2015:A1:AAAA:A* um den Netzwerkpräfix von Subnetz A. Äquivalent dazu, jedoch im Subnetz B, soll Port *FastEthernet0/1* folgende Adresse erhalten:

*2015:00A1:AAAA:000B:0000:0000:0000:0001* (volle Schreibweise)

(Netzpräfix *2015:00A1:AAAA:000B*)

*2015:A1:AAAA:B::1* (verkürzte Schreibweise)

Begeben Sie sich zurück in die Konsole des Routers. Rufen Sie den Konfigurationsmodus von Anschluss *FastEthernet0/0* auf und weisen Sie diesem mittels des Befehls

*ipv6 address 2015:A1:AAAA:A::1/64*

diese Adresse zu (mittels */64* wird mitgeteilt, dass 64 Bits der Adresse zum Netzpräfix zugehörig sind). Verlassen Sie mit *exit* das Interface *FastEthernet0/0* und vergeben Sie an Netz 2 (Anschluss *FastEthernet0/1*) die Adresse des B – Subnetzes. Der Router ist nun konfiguriert und das Konsolenfenster kann geschlossen werden. Um nun zu überprüfen, ob die Endgeräte ihre eigenen IPv6 – Adressen beziehen, öffnen Sie die IP – Konfiguration eines PCs und schalten Sie in den IPv6 – Einstellungen von *Static* auf *Auto Config*. Sind alle Konfigurationsschritte erfolgreich durchgeführt worden, erzeugt das Gerät nun eine IPv6 – Adresse, basierend auf der MAC – Adresse des Netzwerkadapters. Ebenfalls wird das IPv6 – Gateway erkannt (Link – Local Adresse des Routerinterfaces) (Abbildung 36).

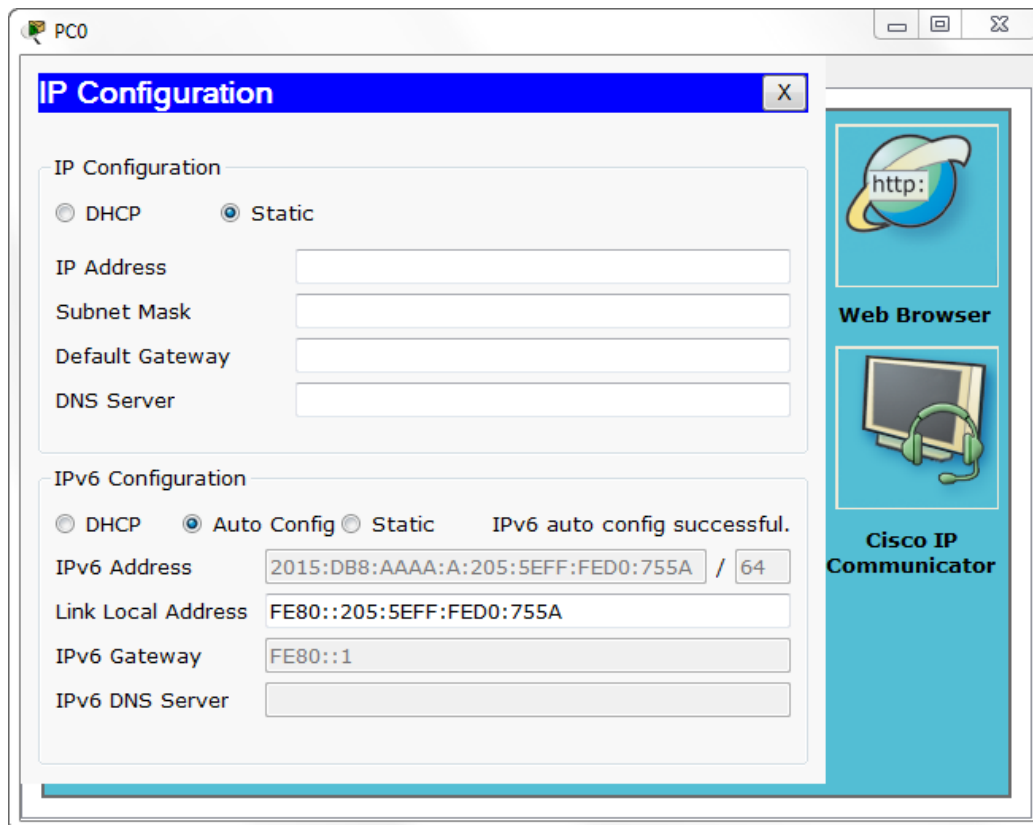


Abbildung 36

An diesem Beispiel sieht man, dass die Adresse im Subnetz A generiert. Wiederholen Sie nun diese Schritte bei den anderen PCs und achten Sie darauf, welche Adresse jener PC in Subnetz B generiert. Nun können Sie die Kommunikation zwischen den PCs untereinander analysieren. Senden Sie dazu zunächst im Echtzeitmodus mehrere einfache PDUs zwischen den Computern hin und her, um die Mac – Adressenermittlung in der Detailansicht zu umgehen. Wechseln Sie nun in den Simulationsmodus und stellen Sie den Event Filter auf ICMPv6. Senden Sie nun eine Simple PDU von *PC0* an *PC2* und verfolgen Sie die Paketübermittlung schrittweise mittels *Capture / Forward*. Öffnen Sie die Detailansicht des Pakets, sobald dieses den Router erreicht und werfen Sie einen Blick auf die *Inbound Details* (also die am Router ankommenden Paketdetails) (Abbildung 37).



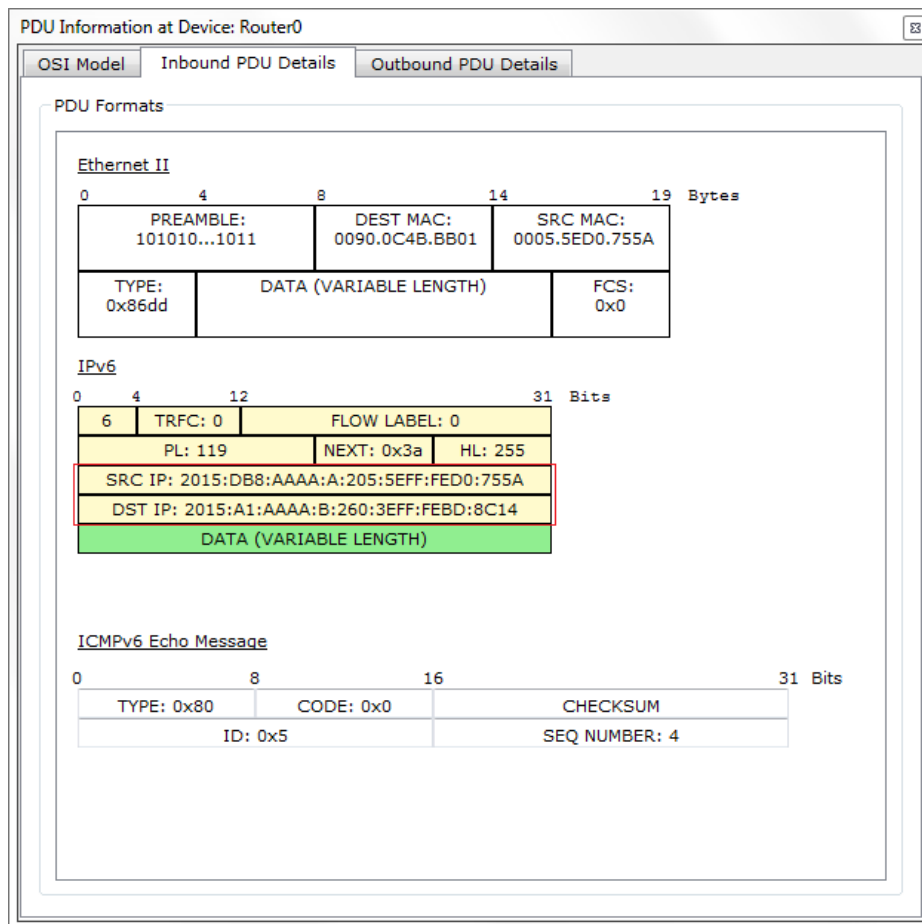


Abbildung 37

Hier deutlich zu erkennen, die für Source – und Destination IP aufgelisteten IPv6 – Adressen. Die erfolgreiche Übertragung des Pakets findet also komplett über IPv6 – Mechanismen statt und ohne die herkömmlichen IPv4 – Konfigurationen, wie Adresse oder Subnetzmaske.

### Aufgaben zum Versuch

1. Von welcher Technologie stellt MAN eine Sonderform dar?
2. Was bedeutet VLAN und wozu dient es?
3. Auf welcher Schicht des OSI – Modells arbeiten paketfilterbasierende Firewalls?
4. Wie funktioniert NAT und wozu wird es verwendet? Welche Nachteile hat es?
5. Wo liegt der Unterschied zwischen IPv4 und IPv6 Adressierungen?