Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Communication Networks
Einleitung Praktikum 1: Hardware, OSI Schichten 2,3

Willkommen zum ersten Praktikum der Vorlesung 'Communication Networks'. Wir werden uns an diesem Praktikumsnachmittag hauptsächlich der Hardware und den Schichten 2 und 3 des OSI Modells widmen.

Ziel:

Ziel des Nachmittages ist es, die vorhandene Hardware richtig einzusetzen um ein Netzwerk aufzubauen. Weiter soll das theoretische Wissen über das Address Resolution Protocol (ARP), das Internet Protocol (IP) und das Transport Control Protocol (TCP) anhand von praktischen Beispielen illustriert und erweitert werden. Zusätzlich geht es darum, die Versuchsumgebung und einige Tools (Software) kennenzulernen, die zur Problemerkennung und -behebung eines Rechnernetzes eingesetzt werden.

Diese Einleitung sollte Ihnen die vorhandene Hard- und Software näherbringen. Falls Ihnen einige Geräte oder deren Funktionalität noch unbekannt sind - keine Angst - im Verlauf der Anleitung wird detailliert auf alle Geräte und Tools eingegangen.

Vorhandene Hard- & Software

Hier eine Übersicht über Geräte, die jeder Gruppe zur Verfügung stehen.

- 1 500 MHz PIII PC mit zwei Netzwerkkarten
- MS Windows 98 und Debian Linux DualBoot Betriebssystem
- 1 8 Port Hub
- 1 Port am Cisco Router
- 2 * 2m und 1 * 6m Netzwerkkabel

Eigens für das Praktikum wurde ein Lokales Netz (LAN) aufgebaut. Die Topologie des Netzwerkes wird in Abb. 1 dargestellt.

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

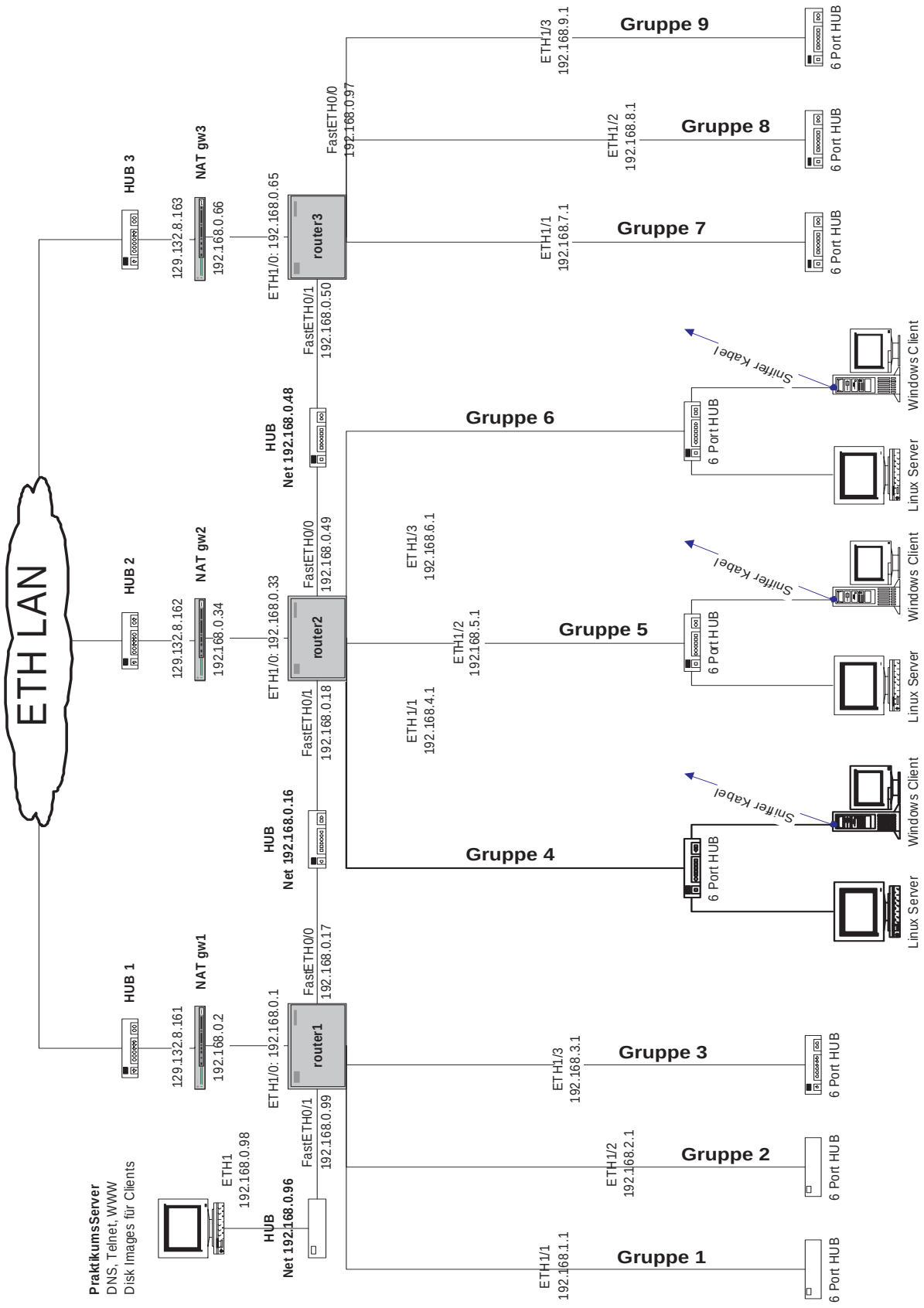


Abb. 1: Aufbau des Praktikumsnetzwerk

Erklärung zu den einzelnen Geräten:

Personalcomputer

Die beiden Computer sind handelsübliche Geräte. Die Betriebsysteminstallation ist ebenfalls standard. Beide PC's haben zwei Netzwerkkarten eingebaut, die mit *ETH0* und *ETH1* beschriftet sind. *ETH0* steht für das primäre Ethernet Interface, jenes also, welches das Betriebsystem normalerweise braucht. Die beiden PC's werden über *Ethernet* miteinander verbunden. Ethernet hat sich als Name für die Vernetzung mittels dem IEEE 802.3 Standard eingebürgert.

Verkabelung

Als physikalischen Träger verwenden wir *10 Base T Ethernet*. Die Zahl 10 steht dabei für die Geschwindigkeit, also *10 MBit / sec*. Das T steht für den Begriff *UTP* - Unshielded Twisted Pair - Kabel. Die Kabeladern sind paarweise verdrillt. Das Kabel selbst hat keine Abschirmung (=shielding), wie dies bei Koax-Kabel der Fall ist. Bei allen XXX BaseT Kabel sind die Kontakte direkt durchverbunden. Das heisst, dass Pin 1 am Stecker der einen Seite mit demselben Pin 1 auf der anderen Seite verbunden ist.

Die Netzwerktopologie bei allen XXXBaseT Verkabelungen ist immer sternförmig. In der Mitte des Sternes muss ein Gerät sein, das die Kabel, analog zu einem Vielfachstecker, zusammenfasst.

Neben *10BaseT* oder *100BaseT* ist *10Base2* relativ weit verbreitet. Diese Verkabelungsart ist als Bus über koaxial Kabel aufgebaut. Einige Netzwerkkarten haben aus diesem Grund neben einer *RJ45* Buchse - Die Steckerart für XXXBaseT Verbindungen - noch eine Buchse für Koaxialstecker.

HUB

Der sogenannte Vielfachstecker im Zentrum des Netzwerksternes heisst HUB. Ein HUB ist ein Gerät, das die verschiedenen Netzwerkkabel elektrisch miteinander verbindet. Die Leitungen müssen vom HUB so gekoppelt werden, dass die Sendeleitung **jeder** Station mit der Empfangsleitung **aller anderen** Station verbunden ist. Als Nebeneffekt kreuzt ein Hub also Sende- und Empfangsleitung der Kabel.

Der Fachbegriff für die Buchsen eines Gerätes im Netzwerkumfeld heisst *Port*. Ein HUB hat normalerweise 4,8 oder 16 Ports. Sobald mehrere Computer mit Netzwerkkabel an ein HUB angeschlossen sind, können diese miteinander kommunizieren.

Möchte man nur zwei PC's miteinander mit UTP Kabel verbinden, gibt es einen Trick, der ohne weitere Hardwareanschaffungen einsetzbar ist. Mittels einem Spezialkabel, einem sogenannten *CrossOver Cabel*, ist dies auch ohne Hub möglich. Wie der Name sagt, ist im Kabel die Verdrahtung so ausgelegt, dass Sende und Empfangsleitung gekreuzt sind.

CrossOver Kabel haben noch eine weitere Einsatzmöglichkeit. Die XXXBaseT Topologie erlaubt die Kaskadierung von Hubs zu einem Baum. So kann man beispielsweise in zwei verschiedenen Räumen je ein Hub haben, die miteinander Verbunden sind. Werden die Ausgänge von zwei Hubs zusammengehängt, muss aus obengenannten Gründen wiederum ein Cross-Over Kabel eingesetzt werden.

Der Einfachheit halber haben HUB's normalerweise sogenannte *Uplink Ports*. Diese Ports sind entweder fest verdrahtet oder können mittels einem Schalter auf Uplink Verdrahtung eingestellt werden. In diesem Fall ist keine Verbindung mittels Cross-Over Kabel nötig, um zwei HUB's zu kaskadieren. Die im Praktikum eingesetzten Geräte haben einen Port, der mittels einem neben der Buchse angeordneten Schalter auf Uplinkverdrahtung engestellt werden kann.

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Im allgemeinen haben die Buchsen - Ports - von den Geräten und Netzwerkkarten eine LED, die als *Link Control* eingesetzt wird. Die Link Control LED leuchtet, sobald eine Verbindung - ein Link - physikalisch steht. Die LED zeigt also nur die 'korrekte' Verkabelung an, sagt jedoch noch nichts über die Netzwerkkonfiguration aus.

Je nach Bauart des Gerät, ist noch eine zweite LED vorhanden, die den Netzverkehr durch Blinken anzeigt. In einigen Geräten ist diese Funktionalität in einer einizigen LED Anzeige eingebaut. Die Anzeige leuchtet im Normalfall rot, wechselt auf grün, sobald ein Kabel eingesteckt wird und die Verbindung steht. Netzverkehr wird sodann durch Blinken der grünen Anzeige symbolisiert.

Tip: Die *Link Control* Anzeige, ist sehr hilfreich beim 'debuggen' von Netzwerkverbindungen. Kontrolieren Sie bei jeder Verbindung, die Sie machen, ob die LED Anzeige eine korrekte Verkabelung anzeigt.

Die im Praktikum eingesetzten HUB's sind normale 8 Port Geräte, die im Handel etwa 25.- kosten. Ein Ausgang kann mittels eingebautem Schalter auf Uplink Modus, also auf gekreutzte Verkabelung geschaltet werden.

Switches

In neu eingerichteten Umgebungen werden normalerweise Switches anstatt HUB's eingesetzt. Ein Switch ist ein Gerät, das auf OSI Schicht 2 Verbindungen herstellt. Anhand der bekannten MAC Adressen werden bei der Kommunikation zweier Geräte die beiden betroffenen Ports 'virtuell' kurzgeschlossen. Der Einsatz eines Switch gleicht dem eines HUB's. Pro Port kommt normalerweise ein Endgerät. Switches verkleinern die sogenannte Kollisionsdomäne - Pakete von Rechner A zu Rechner B können nicht mehr Kollisionen verursachen bei der Kommunikation von Rechner C zu Rechner D.

Router

Ein Router arbeitet - wie aus der Vorlesung bekannt ist - auf OSI Schicht 3. Anhand der IP Adresse betreibt ein Router Leitweglenkung für die Datenpakete.

IP Adressen für das Praktikum

Für die Vernetzung der Computer unter TCP/IP muss jedem Gerät eine eigene IP Adresse zugewiesen werden. Zudem müssen die Geräte dem Adressierungsschema der ETH folgen, um vollständig ins Netz eingebunden zu werden. Um diese Einschränkung zu umgehen, wird im Praktikumsnetzwerk ein spezielles Verfahren - Network Address Translation *NAT* - angewendet. Die Router bilden eine Schnittstelle zum ETH Netzwerk. An der Schnittstelle werden alle IP Pakete umgeschrieben. Die IP Adressen werden 'übersetzt' (=translation). Mittels *NAT* können wir hinter einem Router eine beliebige Adressierungsschema verwenden, ohne das ETH Netzwerk zu tangieren. Das Interface des Routers, agiert als Übersetzer zwischen den beiden 'Welten'.

NAT

Diese Möglichkeit der Adressübersetzung wird oft in Firewalls eingesetzt. NAT bietet hohe Sicherheit, da die Übersetzung nur in einer Richtung aktiviert wird. Vom Internet her ist nur eine einzige IP Adresse - diejenige des Router Interface - sichtbar. Dahinter können sich hunderte von Rechnern verbergen. Mehr Information zu NAT kann in RFC 2663, 'IP Network Address Translator (NAT) Terminology and Considerations' nachgeschlagen werden.

IP Adressen

Die Frage der Abkopplung zum ETH Netzwerk ist mittels NAT gelöst. Es bleibt nun noch die Frage, welche *IP Adressen* verwendet werden soll. Durch den Einsatz von NAT haben wir die Möglichkeit, irgendwelche IP Adressen zu verwenden. Wir könnten hinter unseren Router beispielsweise die IP Adressen einer anderen Firma, bspw. General Motors, verwenden.

Für unseren Fall wurde speziell vorgesorgt. RFC 1918 'Address Allocation for Private Internets' sieht spezielle Adressbereich für genau diesen Einsatz vor. Das A-Klasse Netz 10.x.x.x, die B-Klassen Netze 172.16.x.x bis 172.31.x.x und die C-Klassen Netze 192.168.x.x sind sogenannte private IP Adressen. Diese Netze werden auf dem Internet nicht geroutet. Das heisst: Ein Router wird ein Paket an den Empfänger 10.1.2.4 nie weiterleiten.

Im lokalen Netz, wo die Router selbst konfiguriert werden, können diese Adressen eingesetzt werden. Im LAN können die eigenen Router angewiesen werden, diese Adressebereiche trotzdem weiterzuleiten.

Adressbereich

Für das Praktikum verwenden wir Adressen aus dem 192.168.x.x Bereich. Jeder Gruppe ist ein eigenes *C-Klasse Netz* zugeordnet. Es stehen somit 253 IP Adressen zur Verfügung. Gruppe 1 steht zum Beispiel IP Adressen 192.168.1.1 bis 192.168.1.254 zu, der Gruppe 8 der Bereich 192.168.8.1 bis 192.168.8.253.

Sie fragen sich vielleicht, wieso Ihnen nicht 255 Adressen zustehen. Die 'Zahlen' in der Adresse gehen bekanntlich von 0 bis 255. Dies hat einen einfachen Grund:

192.168.x.0 wird von den Routern als Adresse für ein ganzes Netzwerk gebraucht. Sieht ein Router eine Empfängeradresse wie 192.168.5.3 weiss er, dass er dieses Paket an den Router weiterleiten muss, der das Netz 192.168.5.0 bedient.

192.168.x.255 hat ebenfalls eine spezielle Bedeutung. Diese Adresse ist die sogennante Broadcast

Adresse, mit welcher jeder Host innerhalb eines Netzes angesprochen werden kann.

Wir werden die Thematik der IP Adressen in Praktikum 2 näher betrachten. Kapitel 4.1.3 im Buch zur Vorlesung, 'Computer Networks' gibt Ihnen zudem eine kleine Ubersicht.

Adressvergabe

An dieser Stelle seien noch einige weitere Gegebenheiten beschrieben. Es hat sich so eingebürgert, dass die jeweilige Adresse .1, also bspw. 192.168.6.1, als *DefaultGateway* eingerichtet ist. Der *DefaultGateway* eines Netzes ist ein Rechner oder Router, der über die weitere Netzwerktopologie Bescheid weiss.

Möchte eine Station A ein Paket an eine entfernte Station B senden, vergleicht sie zuerst die IP Adresse von B mit der eigenen Adresse. Ist das Netz dasselbe - in unserem Beispiel wären die 3 ersten Tupel der IP Adresse gleich - so versendet A das Paket direkt an B. Ist dies nicht der Fall - A hat bspw. die Adresse 192.168.3.4 und B die Adresse 192.168.6.7 - so wird das Paket von A an den DefaultGateway weitergegeben. Der DefaultGateway muss sodann das Paket an eine geeignete Adresse weiterleiten. Dies ist entweder ein Netz, das an einer zweiten Netzwerkkarte angeschlossen ist, oder ein weiterer Router.

Mehr zum Thema Routing erfahren Sie in Praktikum 2.

In unserem Praktikum hat jeweils der Router, der die einzelnen Gruppennetzwerke verbindet, die Adresse 192.168.x.1

Beispiel

Um die Adressierung nochmals zu klären, wurde Ihnen noch ein Beispiel zusammengestellt:

Angenommen, Sie wären in Gruppe 9 eingeteilt. In diesem Fall steht Ihnen das C-Klasse Netz 192.168.9.0 zur Verfügung. Der Ihnen zugewiesene Port am Router hat laut oben genannter Konvention die IP Adresse 192.168.9.1. Für die Geräte in Ihrem LAN können Sie nun eine beliebige IP Adresse wählen.

Fragen?

Für Fragen ausserhalb des Praktikums wurde eine spezielle eMailadresse eingerichtet.

Unter **cn@tik.ee.ethz.ch** erreichen Sie den für die Praktikas verantwortlichen Assistenten.

Nun, genug Theorie... Mehr werden Sie in Praktikum 1 erfahren.

Wir wünschen Ihnen dabei viel Spass!

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Communication Networks
Anleitung Praktikum 1: Hardware, OSI Schichten 2,3

Willkommen zum ersten Praktikum der Vorlesung “Communication Networks”. Wir werden uns an diesem Praktikumsnachmittag hauptsächlich der Hardware und den Schichten 2 und 3 des OSI Modells widmen. Das heutige Praktikum gliedert sich in 5 Teilgebiete:

1. Netzwerk Hardware
2. Address Resolution Protocol ARP
3. Internet Control Message Protocol ICMP
4. Dynamic Host Configuration Protocol DHCP
5. TCP / IP

Für die Bearbeitung der Kapitel 1,3 und 4 sind je 1/2 Stunden vorgesehen. Für die restlichen zwei Gebiete sollten je eine Stunde reichen.

Testatpflicht für das Praktikum 1 ist eine sinnvolle Bearbeitung dieser Anleitung. Das Testat wird Ihnen am Schluss des Praktikumsnachmittages ausgehändigt.

Das Praktikum wird in den eingeschriebenen Gruppen durchgeführt. Jeder Arbeitsplatz ist mit einer Gruppennummer ausgestattet. Benutzen Sie für die Bearbeitung den Ihrer Gruppe zugewiesenen Arbeitsplatz. Sie werden über alle Praktikumsnachmittage denselben Arbeitsplatz haben.

Ziel:

Ziel des Nachmittages ist es, ein Netzwerk mit der vorhandenen Hardware aufzubauen und zu konfigurieren. Weiter soll das theoretische Wissen über das Address Resolution Protocol (ARP), das Internet Protocol (IP) und das Transport Control Protocol (TCP) anhand von praktischen Beispielen illustriert und erweitert werden. Zusätzlich geht es darum, die Versuchsumgebung und einige Tools (Software) kennenzulernen, die zur Problemerkennung und -behebung eines Rechnernetzes eingesetzt werden.

1 Aufbau und Konfiguration der Versuchsanordnung

Zuerst gilt es, die Hardware zu verkabeln und die beiden PC’s für den Praktikumseinsatz zu konfigurieren. Diese Aufgabe muss in der Praxis für jeden Rechner durchgeführt werden, der an ein Netzwerk angehängt wird.

Noch ein Wort zur Nomenklatur: Fortan wird in der Anleitung vom “Server” oder “Linux Server” gesprochen. Dabei wird immer die Arbeitsstation mit dem Linux Betriebssystem gemeint. Der zweite PC mit Windows Betriebssystem wird als “Windows Arbeitsstation” oder “Windows Workstation” angesprochen.

Die Netzwerkkarten aller Geräte folgen ebenfalls einer festgelegten Nomenklatur. Das erste Ethernet Interface wird als ETH0 bezeichnet, das zweite mit ETH1 etc. Dies gilt für die PC’s wie auch bei den Routern.

1.1 Netzwerk Hardware

- Verbinden Sie die Netzwerkkarten ETH0 der beiden PC's mit dem HUB mittels UTP Kabel.
- Verbinden Sie den HUB mit dem Router Port der Ihrer Gruppe zugewiesenen wurde. Tip: Lesen sie die Beschreibung des HUB's in der Einleitung nochmals durch. Welcher Ausgang des HUBs muss gewählt werden? (Uplink oder normal?)
  In Abb. 1 der Einleitung ist der schematische Aufbau des Netzwerks mit den zugewiesenen Adressen und Ports genau dargestellt.
- Schalten Sie nun HUB und beide PC's ein.
- Wählen Sie beim Bootmenu bei einem Rechner das Windows 98 Betriebssystem aus, beim anderen Rechner Linux
- Verifizieren Sie anhand der Kontrollanzeigen des HUB's, ob die Verkabelung richtig funktioniert. Die LED's müssen in der richtigen Farbe leuchten!

1.2 Konfiguration des Servers

Der PC, der mit dem Linux Betriebssystem aufgestartet wurde, wird als Server für die drei Praktikumsnachmittage genutzt. Aus diesem Grund ist darauf ein gängiges Server Betriebssystem - Linux - installiert. Obschon es auch für Linux graphische Konfigurationsprogramme gibt, benutzen wir hier bewusst die Command-Line. Auf der Windows Arbeitsstation benutzen wir konsequenterweise die zur Verfügung gestellten graphischen Tools.

Loggen Sie sich für die Konfiguration mit dem Login

root

und Passwort

root

in das System ein. Öffnen sie danach im Start-Menü des Window Managers eine neue Shell.

- In der Shell muss der Rechnername mit folgendem Befehl gesetzt werden:

  hostname server-gX (X mit der Gruppennummer ersetzen!)

- Setzen Sie die IP Adresse des Servers mit

  ifconfig eth0 IPADDR

  Wobei IPADDR eine gültige IP Adresse in dem ihrer Gruppe zugewiesenen Netz ist. *ifconfig* ist ein Programm zum Setzen und Abfragen der TCP/IP Konfiguration.
  Tip: In der Praktikumsanleitung sind einige Hinweise zu der Vergabe von IP Adressen gegeben
- Setzen Sie die Netz Maske mit dem Befehl:

  ifconfig eth0 netmask 255.255.255.0

  Der Sinn der Netmask wird in Praktikum 2 besprochen.
- Zuletzt muss das Netzwerk Interface, die Netzwerk Karte also, noch aktiviert werden.

  ifconfig eth0 up

- Um den Rechner ins Praktikumsnetzwerk einzubinden, sind noch einige weitere Befehle notwendig. Geben Sie folgende Eingaben nacheinander in der Kommandozeile ein:

route add default gw 192.168.X.1

Achtung: X steht wiederum für Ihre Gruppennummer.
Mit diesem Befehl verwenden wir den Router als Default-Gateway
Die Bedeutung des *route* Befehls werden wir auch in Praktikum 2 betrachten.

Nun sollte der Server korrekt für den Einsatz im Praktikum 1 konfiguriert sein.

Geben Sie nun den Befehl

ifconfig -a

ein und vergleichen Sie die Ausgabe mit:

```
...
eth0  Link encap:Ethernet  HWaddr 00:50:DA:DE:96:C2
      inet addr:192.168.X.Y  Bcast:192.168.X.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:xyz errors:0 dropped:0 overruns:0 frame:0
      TX packets:xyz errors:0 dropped:0 overruns:0 carrier:6
      Collisions:xy
      Interrupt:10 Base address:0xd800
   ...
```

Stimmen die Ausgaben nicht überein, so müssen die obigen Schritte nochmals ausgeführt werden. Wichtig sind v. A. die Felder *inet addr, Bcast, Mask.*

Um die Erreichbarkeit von anderen Rechnern zu prüfen, gibt es unter unix und Windows spezielle Tools. Probieren Sie mit dem Befehl

ping www.ethz.ch

ob der WebServer der ETH Erreichbar ist. Ist alles IO, müsste die Ausgabe des ping Befehls wie folgt aussehen:

```
PraktikumServer:~# ping www.ethz.ch
PING w3.ethz.ch (129.132.200.35): 56 data bytes
64 bytes from 129.132.200.35: icmp_seq=0 ttl=245 time=23.5 ms
64 bytes from 129.132.200.35: icmp_seq=1 ttl=245 time=20.6 ms
64 bytes from 129.132.200.35: icmp_seq=2 ttl=245 time=21.7 ms

--- w3.ethz.ch ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 20.6/21.9/23.5 ms
```

Das *ping* Programm schickt sogenannte ICMP Echo Pakete an den angegebenen Rechner. Dieser sendet eine Echo zurück. So kann die Erreichbarkeit eines Rechners festgestellt werden. Je nach Implementation, sendet *ping* eine oder mehrere Nachrichten an den Rechner. Mit der Eingabe von *ctrl-c* kann das Programmm abgebrochen werden.

1.3 Konfiguration der Windows Arbeitsstation

Der PC mit Beschriftung pc-gX (X steht für Ihre Gruppennummer) soll eine typische Arbeitsstation darstellen. Daher wurde MS Windows 98 als ein Beispiel für die 32-Bit Betriebssysteme von Microsoft installiert[1]. Für die Konfiguration der Arbeitsstation sind ähnliche Schritte nötig, wie sie oben für den Server beschrieben wurden. Die Konfiguration geschieht allerdings graphisch über

Start Menu->Einstellungen->Systemsteuerung.

Im darauf geöffneten Fenster findet sich das Tool *Netzwerk*, das mit Doppel-Klick gestartet werden kann. Die Parameter für das Netzwerk können durch anwählen von TCP/IP in der Auswahl und klicken auf *Einstellungen* verändert werden.

- Eine Arbeitsstation erhält typischerweise keine feste IP-Adresse. Unter der Schaltfläche *IP-Adresse* muss demnach *IP-Adresse automatisch beziehen* angewählt sein. Beim Systemstart wird nun der Arbeitsstation vom Praktikumsserver eine IP Adresse zugewiesen.
- Unter der Schaltfläche *Gateway* muss noch die Adresse des Routers eingetragen werden. Geben Sie die IP Adresse des Routers, also 192.168.X.1, ein und klicken Sie auf *hinzufügen*

Die Konfiguration wird durch zweimaliges betätigen der *OK* Taste übernommen. An dieser Stelle ist allenfalls einen Neustart fällig.

Nun ist auch die Windows Arbeitsstation konfiguriert. Um die Funktionalität zu testen, gibt es für Windows ebenfalls ein *ping* Tool. Öffnen Sie unter *Start Menu->Programme* eine “MS Dos Eingabeaufforderung”. Auf der DOS Kommandozeile kann wie bei unix mit

ping IPADDR

einen Rechner angepingt werden. Versuchen Sie www.ethz.ch und die IP Adresse des Linux servers anzupingen. Gelingt dies, so sind Server und Arbeitsstation richtig konfiguriert. Andernfalls sind obengenannte Schritte nochmals zu verifizieren.

[1] Die Konfiguration der moderneren Versionen Windows 2000 und Windows XP geschieht auf ähnliche Weise - es gibt keine grundsätzlichen Unterschiede.

2 Address Resolution Protocol ARP

2.1 Grundsätzliches

Wie Ihnen sicherlich aus der Vorlesung bekannt ist, werden auf OSI Schicht 2 andere Computer über ihre MAC Adresse angesprochen. Mittels dem Address Resolution Protocoll ARP werden IP Adressen auf physikalische MAC Adressen abgebildet. In diesem Kapitel wird das Handling von MAC Adressen näher betrachtet.

Aufgabe:

Lesen Sie auf dem Linux Server die Manualpage zum Befehl *arp*. Die Hilfeseite wird nach Eingabe von

man arp

in der Linux Kommandozeile angezeigt.
Dasselbe existiert auch auf Windows unter

arp

Frage:

Wie muss der *arp* Befehl aufgerufen werden, um Einträge in der ARP Tabelle anzuzeigen oder zu löschen?

Die MAC Adressen von anderen Rechnern werden lokal in einem Cache Speicher abgelegt. Wir füllen den Cache Speicher, indem wir den Router und den Server mit einem *ping* kontaktieren.

Aufgabe:

Schicken Sie von Ihrem Windows-Rechner dem Server und Router auf die jeweilige IP Adresse ein *ping*. Betrachten Sie danach die Einträge in die ARP Tabelle.

Fragen:

- Welche MAC Adressen sind gespeichert?
- Welcher Rechner korrespondiert mit welcher IP und MAC Adresse
- Was sind die Vor- und Nachteile eines Speicherns von MAC Adressen in einem Cache?
- Wie lange sind solche Einträge sinnvollerweise vorhanden? Weshalb?

Aufgabe:

Schicken Sie nochmals ein *ping* Paket zum Router und betrachten Sie danach die Einträge in der ARP Tabelle. Nun schicken Sie ein *ping* Paket an die IP Adresse von www.ethz.ch (129.132.200.35) und betrachten wiederum die ARP Tabelle.

Frage:

Was hat sich geändert? Wieso gibt es keinen ARP Eintrag für den WebServer der ETH?

2.2 ARP Protokoll

Nun möchten wir das ARP Protokoll einmal näher betrachten. Wir benötigen dafür ein Tool, das uns aufzeigt, was genau auf Netzwerkebene abgeht. Ein solches Tool, Netzwerk Sniffer genannt, ist der Surveyor von Finisar Systems (früher "Shomiti Surveyor"[2], aktuell siehe http://www.finisar.com/product/product.php?product_id=104&product_category_id=96), das auf der Windows Arbeitsstation installiert ist.

Starten Sie das Programm mit

Start Menu -> Programme -> Shomiti Surveyor -> Surveyor

Uns interessiert nun die Detailansicht, die sich mittels dem Menueintrag *Detail View* unter dem Menu *Module* befindet. (Alternativ kann die Detailansicht auch mit *F9* aufgerufen werden)

Öffnen Sie nun die Paketübersicht über den Eintrag *Packet Summary* im Menu *Monitor View*, das

[2] In diesen Unterlagen wird das Werkzeug jeweils mit "Shomiti Surveyor" bezeichnet.

sich im eben geöffneten Fenster *Detail View* befindet.

Der Netzwerk Sniffer kann nun den vollständigen Verkehr auf dem Netzwerk analysieren. Starten Sie hierzu den Sniffer unter dem Menu *Module->Start* (Alternativ kann *ctrl-t* oder der Knopf mit grünem Dreieck in der Shortcut Leiste benutzt werden.)

Versuchen Sie nun aus einem DOS Kommandozeilenfenster oder vom Linux Server einen anderen Rechner anzupingen. Falls alles richtig läuft, sollte im Fenster *Packet Summary* im Surveyor Einträge, der auf dem Netzwerk gesnifften Pakete erscheinen.

Stoppen Sie nun den Sniffer mit *Module->Stop*. (Alternativ *ctrl-p* oder Knopf mit rotem Quadrat in der Shortcut Leiste)

Mittels einem Doppelklick auf einen Eintrag im Fenster *Packet Summary* erscheint ein neues Fenster, das jedes aufgefangene Paket in allen Details auflistet. Diese zweigeteilte Fenster listet oben die Pakete auf, unten sind für alle Protokollebenen die Informationen eingeblendet.

Schliessen Sie nun das Fenster *Shomiti Surveyor Capture View*.

Aufgabe:

- Wir möchten nun einen ARP Vorgang im Detail betrachten. Hierzu muss die ARP Tabelle zuerst gelöscht werden.
  Zeigen sie die ARP Tabelle in einer DOS Kommandozeile an.
- Jeder vorhandene Eintrag muss gelöscht werden.
  Wiederholen Sie dies solange, bis die ARP Tabelle keine Einträge mehr zeigt.
- Starten sie nun den Paketsniffer wiederum mit dem Menueintrag “Module->Start”.
- In der DOS Kommandozeile führen Sie nun ein ping an die Adresse 129.132.200.35 (www.ethz.ch) aus.
- Der Sniffer kann nun gestoppt werden und mittels Doppelklick im *Packet Summary* Fenster die *Surveyor Capture View* aktiviert werden. Sie sollten nun mindestens zwei grüne Einträge vorfinden, die im Feld *Summary* mit ARP beginnen. Wählen sie das Paket mit Summary “ARP Q .....” an und betrachten Sie in der zweiten Fensterhälfte den Paketinhalt.

Fragen:

- Was für ein Typ von ARP Paket ist das zu betrachtende Paket? (Tip: Feld "Operation")

- Welche Station schickt das Paket ab? An wen ist es gerichtet? (Tip: Data Link Control Einträge)

Aufgabe:

Betrachten Sie nun das Paket mit Summary "ARP R HA=....."

Fragen:

- Welche Station schickt das Paket ab? An wen ist es gerichtet?

- Welche Information trägt das Paket? Was weiss die Windows Station nun mehr?

- Surveyor erkennt den Hardware Hersteller der Ethernet Karte / Computers etc. Können Sie sich vorstellen wieso?

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

3 Internet Control Message Protocol ICMP

In der letzten Aufgabe haben wir das ARP Protokoll anhand eines ping Paketes angeschaut. Neben den ARP Paketen, die der Surveyor auf dem Netzwerk registriert hat, sind noch Pakete durch ping aufgezeichnet worden. Ping funktioniert über das ICMP Protokoll.

Fragen:

Beschreiben Sie den Ablauf eines pings an die IP Adresse 129.132.200.35. Welche Pakete werden verschickt? (Sowohl ICMP wie ARP) Wer schickt wem was?

Ein ping wird oft zur Messung der Verzögerung, die ein Netzwerk aufweisst, eingesetzt. Wie lange dauert es nach Absenden des Pakets, bis eine Antwort registriert wird? Kommentieren Sie die Verzögerung.

4 Dynamic Host Configuration Protocol DHCP

Beim Konfigurieren des Windows Rechners, haben wir in den Netzwerkeinstellungen angegeben, dass die IP-Adresse automatisch bezogen wird. Das automatische Konfigurieren der Netzwerkparameter geschieht über das DHCP Protokoll. In dieser Aufgabe werden wir vom Linux Server aus betrachten, wie DHCP funktioniert.

Linux kommt standardmässig mit einem Netzwerksniffer Programm. Das Tool *ethereal* hat gleichartige Funktionalität wie Shomiti Surveyor.

Aufgabe:

Beenden Sie Windows und fahren Sie den Rechner hinunter. Auf dem Linux PC starten Sie eine neue Shell und geben darin den Befehl

ethereal

ein. Starten Sie den Sniffer mit

Capture -> Start -> OK

Starten Sie nun den Windows PC neu.

Frage:

Erklären Sie anhand der Ausgabe von *ethereal* wie das DHCP Protokoll funktioniert. Was ist der Vorteil eines Einsatzes von DHCP?
Wie stellt der DHCP Server sicher, dass die ausgegebene Adresse nicht schon besetzt ist?

Extra Credit Aufgabe:

Diese Aufgabe ist freiwillig zu lösen.

Shomiti Surveyor schlüsselt das DHCP Protokoll weiter auf. Zudem muss der PC keine gültige Netzwerkkonfiguration haben um mit Surveyor zu arbeiten.

Mit dem Programm *winipcfg* (aus der DOS Kommandozeile starten) können ausgefasste DHCP Adressen freigegeben und neu bezogen werden (Ohne Reboot).

Betrachte nun den sogenannten DHCP release und das neue Ausfassen einer IP Adresse mit Surveyor.

5 Kommunikation mit TCP / IP

Wir möchten uns nun höheren Protokollschichten zuwenden. Wir betrachten eine einfache verbindungsorientierte Kommunikation, wie es beispielsweise *telnet* macht.

Bei einer Telnet Verbindung zwischen Client und Server kommen mehrere Protokolle zum Einsatz. Die rohen Pakete werden mittels dem Internet Protokoll IP zwischen den beiden Maschinen hin und her geleitet.

Darüber läuft das Transport Control Protocol TCP, das eine verbindunsgorientierte Kommunikation sicherstellt. Als letztes Protokoll kommt zuoberst des Telnet Protokoll. Dieses besteht einerseits aus rohen Datenpakete und Kontrollinformationen. Surveyor nimmt einem die Arbeit ab, die Protokollschichten zu separieren. Die einzelnen Schichten werden in verschiedenen Farben dargestellt:

Grüne Farbe - IP

Rote Farbe - TCP

Blaue Farbe - Telnet Protokoll

Datenpakete sind im *Summary* als *Data* angeschrieben werden. Wir betrachten in den nächsten Aufgaben jede Schicht einzeln.

5.1 Internet Protokoll

Aufgabe:

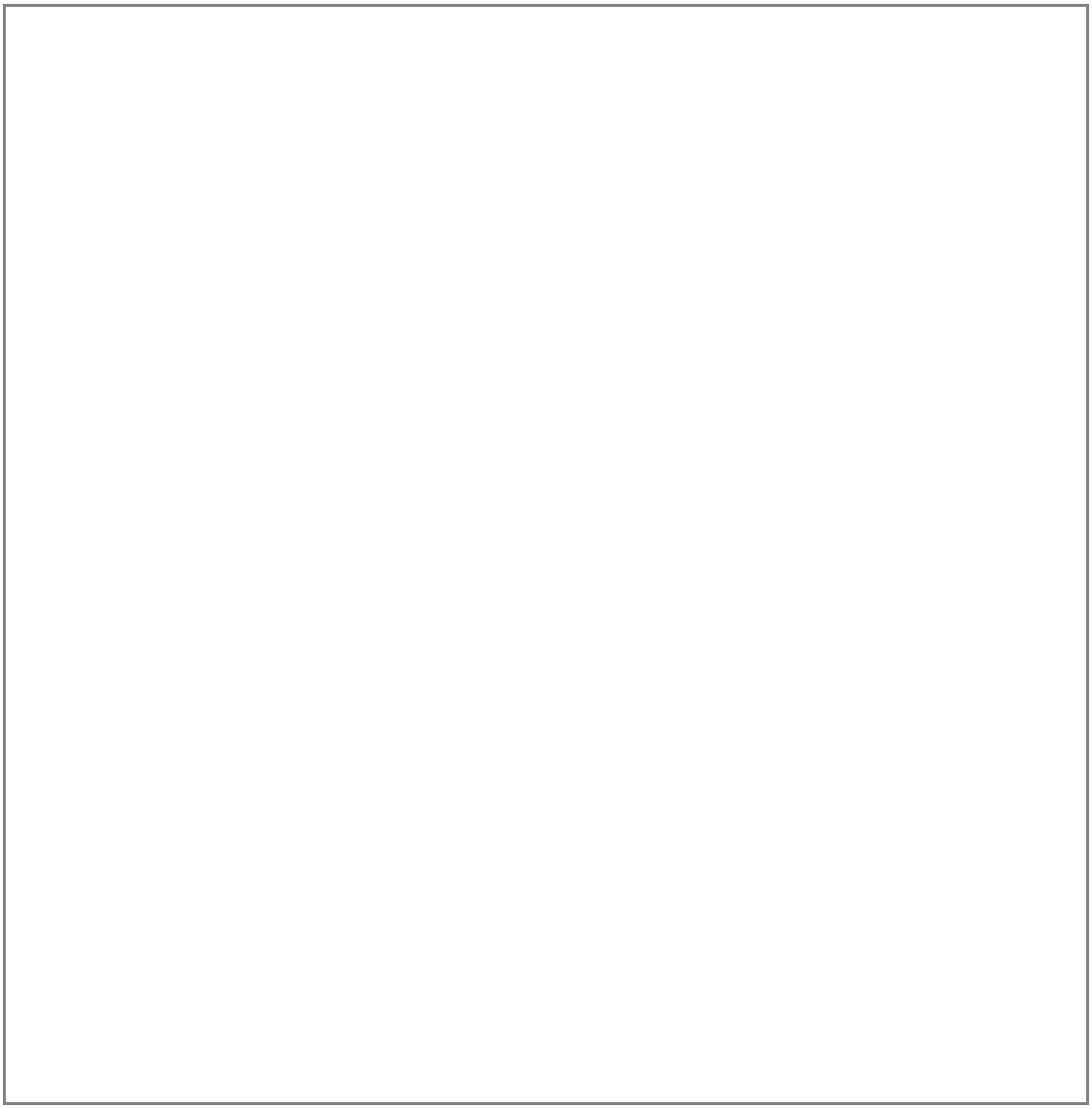
- Starten Sie den Surveyor und öffnen Sie eine telnet Verbindung zum Praktikumsserver mit dem Befehl

  telnet 192.168.0.98

  den Sie von der DOS oder Linux Kommandozeile abgeben.
  Der Login lautet *praktikum*, das Passwort ebenso.
- Loggen Sie sich nun mit dem Befehl *exit* wieder aus, und betrachten Sie im Surveyor die aufgefangenen Pakete. Stoppen Sie hierzu die Aufnahme des Surveyors und öffnen das *Capture View* Fenster. (Anmerkung: Der Vorgang ist derselbe, wie in den Aufgaben zu ARP bereits beschrieben wurde)
- Betrachten Sie das erste rote (TCP) Paket, mit welchem die Telnet Verbindung beginnt. Machen Sie sich nun als erstes mit den grünen Einträge zum Internet Protokoll IP vertraut.

Fragen:

- Welche Information ist im IP Protokoll enthalten?
- Ist das Paket gültig, oder wurde es fehlerhaft übertragen?
- Wieviele Bytes Daten enthält das Paket? Was sind das für Daten?
- In Protokoll gibt es ein Feld “Time to live”. Was ist wohl der Sinn eines solchen Feldes im Protokollheader?



5.2 Transport Control Protocol

Wir möchten nun die Funktionalität des TCP Protokolls betrachten.

Aufgabe:

Unter TCP / IP hat jeder angebotene Dienst (Telnet, Web, Mail...) eine sogenannte Port Nummer. Diese Portnummern sind im Internet standardisiert (Siehe RFC 1700 oder / etc/services). So ‘horcht’ ein Webserver immer auf Port 80. Eine Portnummer und IP Adresse bilden zusammen einen eindeutig bestimmten Endpunkt einer Kommunikation über TCP / IP. Man spricht hiervon auch von einem ‘Socket’. Jede Punkt-Zu-Punkt Kommunikation besitzt somit zwei solche Sockets.

Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

Frage:

- Auf welcher Portnummer 'horcht' der Telnet Server?
- Wie lauten die IP Adresse und Portnummer des anderen Kommunikationsendpunktes?

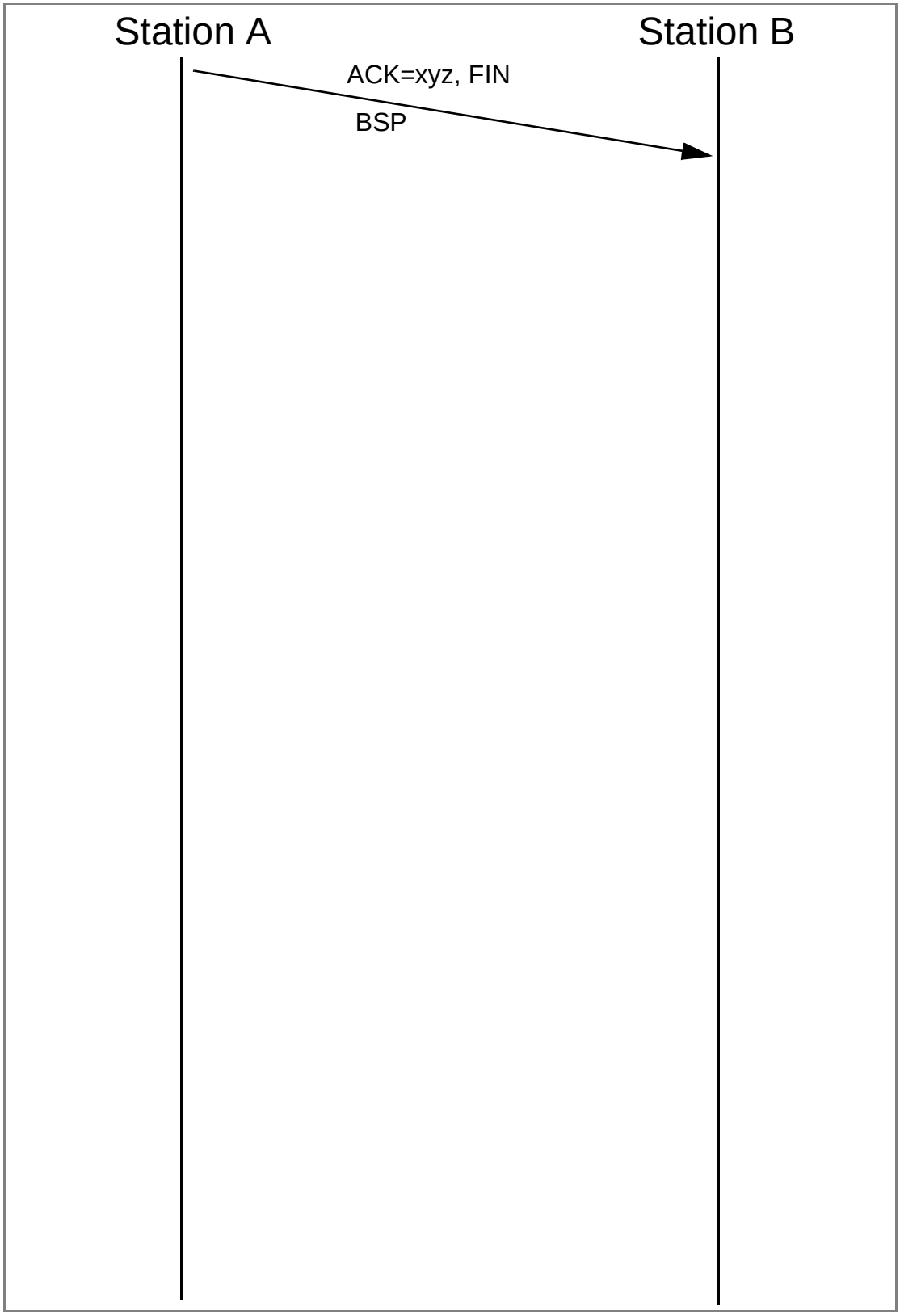
Aufgabe:

Aus der Vorlesung wissen Sie, dass TCP verbindungsorientiert arbeitet. Bei der Kommunikation wird überwacht, dass keine Paketverluste und Vertauschungen auftreten.
Betrachten Sie dazu die roten (=TCP) Pakete.

Fragen:

- TCP Protokoll kennt spezielle Flags zum Aufbau und Abbruch einer Verbindung. Welche Pakete signalisieren einen Verbindungsaufbau?
- Wie wird das signalisiert?
- Welches Paket bestätigt den Verbindungsaufbau?
- Wie sieht das beim Verbindungsabbau aus?

- Zeichnen Sie Verbindungsaufbau und -abbau mittels den versendeten Pakete auf. Für jedes Paket sollen spezielle Flags, die Sequenznummer, die Acknowledgement Nummer notiert werden. Kommentieren Sie zusätzlich die Wirkung jedes einzelnen Pakets.



Prof. Dr. B. Plattner, ETZ G88, Gloriastrasse 35, CH-8092 Zürich, Tel. +41-1-6327000, Fax +41-1-6321035

6. Abschluss, Testatausgabe

Zum erfolgreichen Abschliessen des Praktikums fällt noch eine letzte Aufgabe an. Fahren Sie beide Rechner hinunter und schalten Sie sie aus. Ihre Nachfolger werden Ihnen dankbar sein, wenn sie beide Betriebssysteme korrekt hinunterfahren - die PC's also nicht einfach vom Strom trennen. Nehmen Sie nun die HUB's vom Netz und rollen die Kabel zusammen.

Sobald Ihr Arbeitsplatz wieder so im gleichen Zustand ist, wie Sie ihn angetroffen haben, können Sie sich beim Betreuer melden und das Testat verlangen