

B.Sc. Max Pfeiffer
B.Sc. Martin Grabe
B.Sc. Björn Wolfahrt
B.Sc. Dirk Hoffstadt
Dipl.-Wirt.-Inf. Jobin Pulinthanath

Institut für Experimentelle Mathematik
Lehrstuhl Technik der Rechnernetze
Ellernstr. 29
D 45326 Essen

WS 07 / 08
Praxisübung 1 für "Kommunikationsnetze 1"



Thema: Grundlegende Internetprotokolle / Subnetting

1. Das LAN ist über ein Gateway (IP-Adresse: **132.252.152.1**) mit dem öffentlichen Internet verbunden. Die Subnetzmaske ist 255.255.255.128 (Tip: Hexadezimal FF.FF.FF.80). Wie viele Rechner (bzw. IP-Adressen) kann man in dem LAN betreiben? Welche IP-Adressen können diese nutzen?

2. Wie heißt die Broadcast-Adresse ?

3. Kann ein Computer in diesem LAN einen weiteren mit der Adresse 132.252.152.200 ohne Hilfsmittel erreichen? Begründen Sie Ihre Antwort!

4. Um Subnetze der obigen Art zu beschreiben, verwendet man auch die Notation **132.252.152.0/25**, wobei der Wert hinter dem „/“ die Anzahl der gesetzten Bits in der Subnetzmaske angibt. Welche Subnetzmaske hat ein Rechner mit der Adresse 192.168.34.45/29?

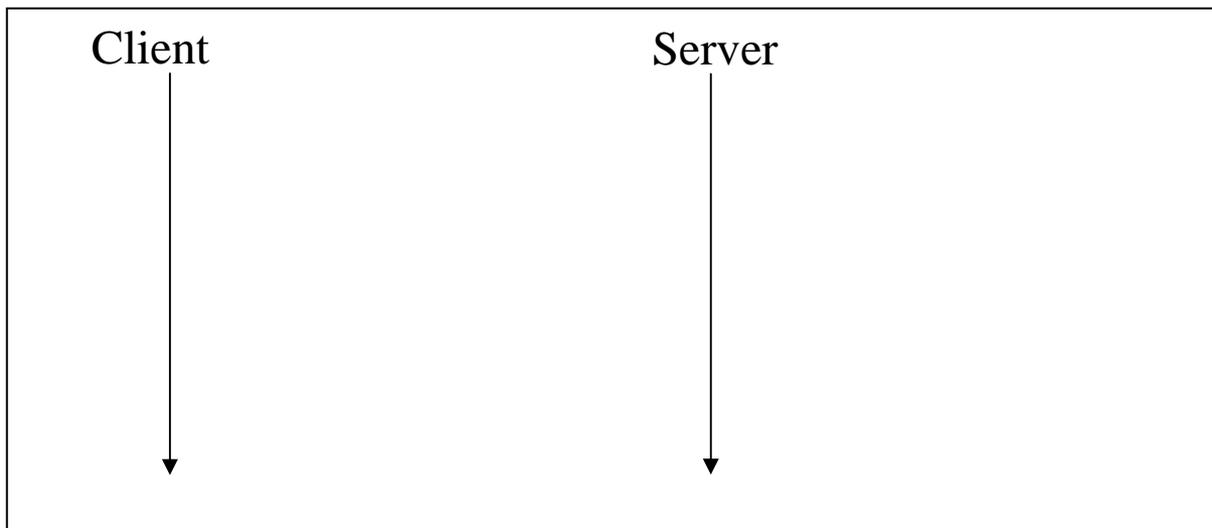
5. Wie heißen Netzwerk- und Broadcast-Adresse für das oben genannte Netz?

Netzwerkadresse: _____
Broadcastadresse: _____

6. Wie notiert man das Netzwerk 172.19.32.128 mit der Subnetzmaske 255.255.255.240 nach der neuen „/“-Notation?

7. Wie viele nutzbare IP-Adressen gibt es in diesem Netz?

8. Starten Sie das Programm "**wireshark**". Schalten Sie in den Trace-Modus (unter „Capture“ → „Start“) und schicken Sie mit dem Befehl "**ping -c 1 132.252.152.<Rechnernr.>**" ein ICMP-Paket an einen Rechner, der **nicht** im ARP-Cache aufgelistet ist! (<Rechnernr.> kann dabei Werte von 70-79 annehmen!). Schauen Sie sich den Output im „**wireshark**“ an und versuchen Sie ARP- und ICMP-Pakete von und zu Ihrem Rechner auszumachen. Wenn Sie die Pakete mit der Maus markieren, können Sie im unteren Bereich von „**wireshark**“ die Details zu diesem Datenpaket ansehen. Skizzieren Sie den Nachrichtenfluss von ARP- und ICMP-Paketen! Markieren Sie dabei Broadcasts!



9. Ein ARP-Request fordert generell die Abbildung einer Hardware-Adresse (zunächst nicht auf Ethernet beschränkt) auf eine Protokoll-Adresse an – betrachten Sie den ARP-Request in der Detail-Ansicht von „**wireshark**“:

Wie lautet die Codierung für den Hardware-Typen Ethernet?

10. Wie lautet die Codierung für den Protokoll-Typen IP (Internet-Protokoll)?

11. Welche anderen Hardware-Typen/Protokoll-Typen könnten Sie sich vorstellen?

12. Wie lang sind die Hardware-Adressen (MAC-Adresse)?

13. Wie lang sind die Protokoll-Adressen (IP-Adressen)?

14. Wie lauten die Hardware/Protokoll-Adressen des Empfängers (Targets) des ARP-Requests? Notieren Sie bei der HW-Adresse sowohl die Zieladresse des ARP-Paketes selbst als auch die *im* ARP-Paket angegebene Zieladresse!

15. Wodurch unterscheiden sich ARP-Request und ARP-Reply ?

16. Skizzieren Sie den Aufbau eines ICMP-Echo-Request Paketes (Längen in Bytes, inkl. MAC und IP-Header, nur Header, nicht jedes einzelne Feld im Header)!

--	--	--	--

17. Welche Protokoll-ID wird im IP-Header für ICMP benutzt?

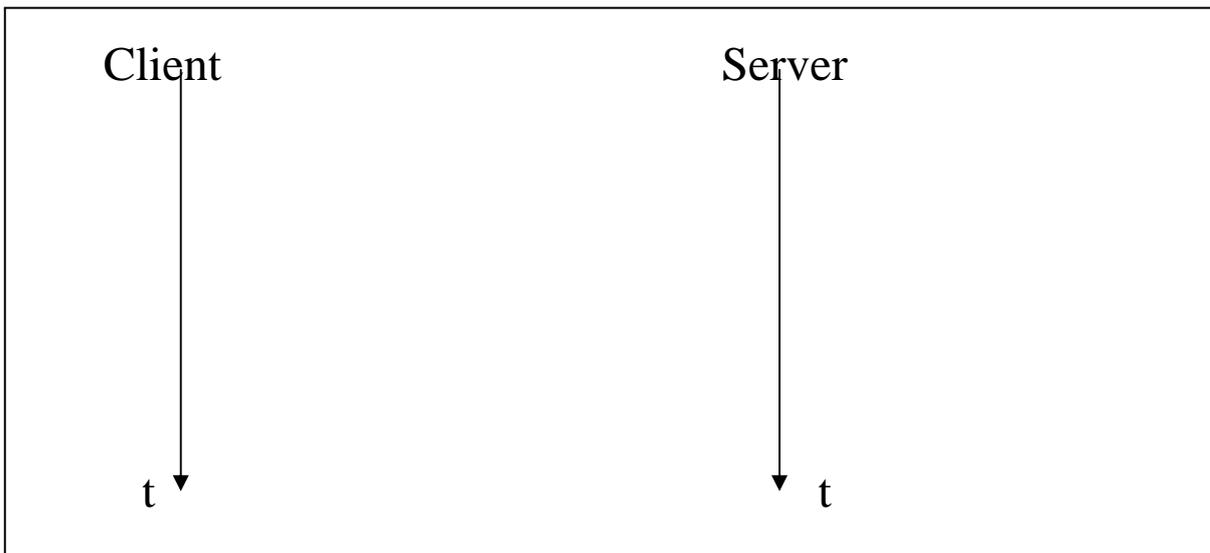
18. Welchen ICMP-Typ-Code haben Echo-Request bzw. Echo-Reply?

19. Wie könnten sich die Daten zusammensetzen, die am Ende des ICMP-Pakets mitgeschickt werden (dazu am Terminal "**man ping**" eingeben!)? Evtl. auch mehrere ICMP-Pakete, auch unterschiedlicher Länge, betrachten und vergleichen)

20. Laden Sie mit dem Terminal-Programm "wget" ("wget --help") die Datei mit dem URL „http://132.252.152.100/test.data“ herunter! Verfolgen Sie die Übertragung mit dem Programm "wireshark"!

An welche MAC-Adresse werden die TCP/IP-Pakete gesendet? Welcher Rechner ist das?

21. Skizzieren Sie den Nachrichtenfluss des TCP-Verbindungsaufbaus, so wie er mit "wireshark" betrachtet wurde! Tragen Sie auch die gesetzten Flags des TCP-Protokollkopfes ein!



22. Welchen Port nutzt der Client, welchen der Server?

23. Wie groß ist die maximale Segmentlänge des IP-Paketes (Tip: TCP-Header beim Verbindungsaufbau betrachten)?

24. Wie lang ist das längste IP-Paket (Begründung!)?

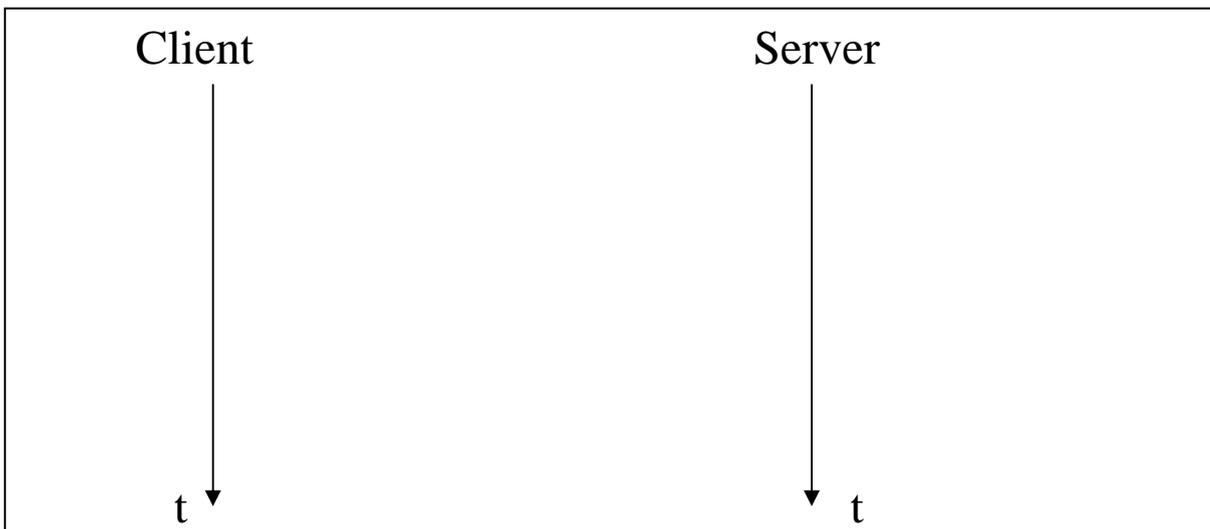
25. Wie lang ist dann der längste MAC-Rahmen?

26. Welche Fenstergröße (= „*window size*“, entspricht dem „*Receiver-Window*“) wird beim Verbindungsaufbau zwischen den beiden TCP-Instanzen ausgehandelt?

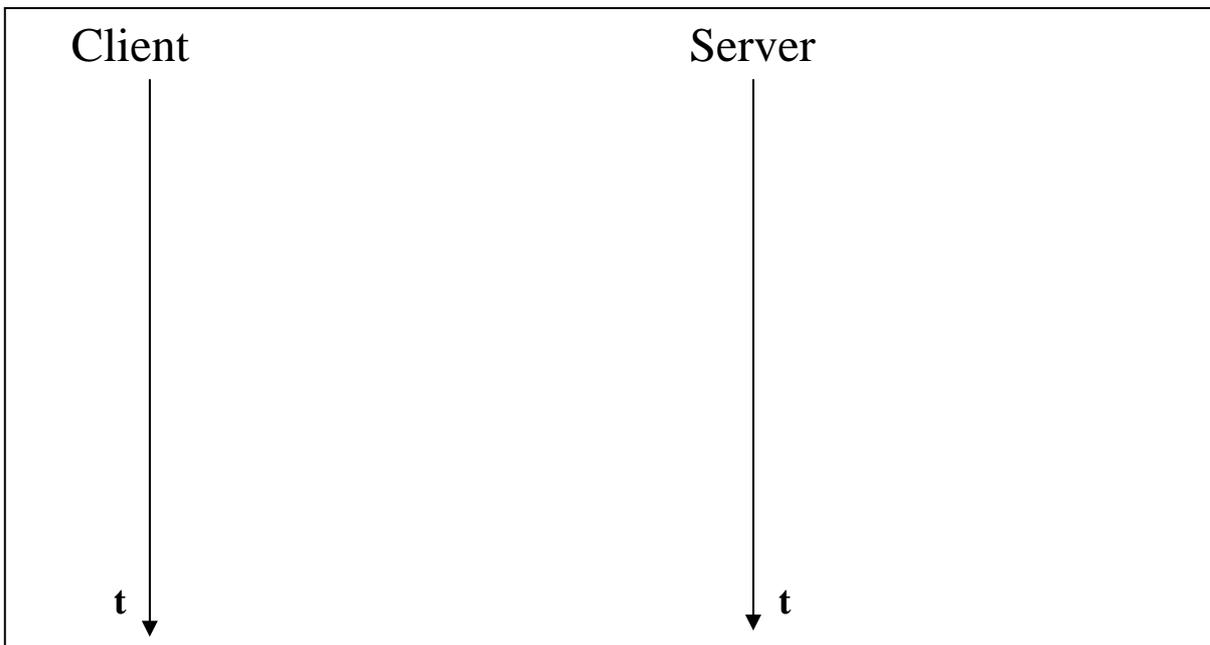
27. Welche Daten überträgt der Client beim HTTP-Request? (mit „**wireshark**“ das HTTP-Feld betrachten!)

28. Welche Daten überträgt der Server bei seiner Antwort? („**wireshark**“: die Antwort des Servers anschauen!)

29. Skizzieren Sie den Nachrichtenfluss des TCP-Verbindungs**abbaus**, so wie er mit "**wireshark**" betrachtet wurde! Tragen Sie auch die gesetzten Flags des TCP-Protokollkopfes ein!



30. Skizzieren Sie den gesamten Datenaustausch zwischen Client und Server!



31. Wie viele Daten (Bytes) werden insgesamt auf dem Layer 2 gesendet (incl. MAC-Header, CRC)?

32. Wie viele Bytes erhält die Client-Anwendung?

33. Wie hoch ist die Effizienz (Anteil erhaltener Daten an insgesamt gesendeten Daten)?

Abschließender Hinweis: Alle in dieser Übung gelernten Mechanismen über Verbindungsverhalten im TCP/IP sind relevant für die Klausur. Sollten Sie also Bedarf an weiterer Übung haben, so sollten Sie sich die Software „wireshark“ selbst auf Ihrem Heimrechner (soweit vorhanden) installieren.

„Wireshark“ gibt es kostenlos bei (sowohl für Linux als auch für Windows!):

<http://www.wireshark.org/>