Aufbau und Funktionsweise von Datennetzen (Best. Nr. 4502)

Diese Einheit behandelt grundlegende Themen zum Aufbau von Computernetzwerken. Vermittelt werden u. a. Kenntnisse über das OSI-Modell, Netzwerkarchitekturen, Topologien, Netzwerkkomponenten, wichtige Protokolle und Dienste.
Dabei werden neben der Erarbeitung der theoretischen Kenntnisse immer wieder Experimente angeregt, um die verschiedenen Funktionen 'begreifbar' zu machen.
Jeder Abschnitt umfasst eine ausführliche Hinführung, ein Arbeitsblatt, eine Folie zur Vertiefung, weiterführende Internetlinks sowie eine Lernzielkontrolle.
Autor und Verlag wünschen Ihnen viel Erfolg beim Einsatz dieser Unterrichtseinheit.

Gesamtdatei	
091_Netzw.ges	Alle Dateien in obiger Reihenfolge

Die Einzeldateien	
1. Didaktische Hinweise	
001_Vorwort.did	Einführung zu dieser Einheit
2. Leben in der Informationsgesellschaft	
002_Netzw1.arb	Arbeitsblatt - Informationsgesellschaft
003_Netzw1.loe	Lösungsblatt - Informationsgesellschaft
3. Was ist ein Netzwerk?	
004_Netzw2.hin	Hinführung - Was ist ein Netzwerk
005_Netzw2.arb	Arbeitsblatt - Definitionen Netzwerk
006_Netzw2.loe	Lösungsblatt - Definitionen Netzwerk
007_Netzw2.fol	Folie - Beispiel für ein Netzwerk
008_Netzw2.lzk	Lernzielkontrolle - Was ist ein Netzwerk
009_Netzw2.lzl	Lösung zur Lernzielkontrolle
010_Netzw2.int	Vertiefende Internetlinks

4. Clients, Server, Dienste	
011_Netzw3.hin	Hinführung - Clients, Server, Dienste
012_Netzw3.arb	Arbeitsblatt - Clients, Server, Dienste
013_Netzw3.loe	Lösungsblatt - Clients, Server, Dienste
014_Netzw3.fol	Folie - Peer-to-Peer und Client-Server
015_Netzw3.lzk	Lernzielkontrolle - Clients, Server, Dienste
016_Netzw3.lzl	Lösung zur Lernzielkontrolle
017_Netzw3.int	Vertiefende Internetlinks

5. Wie werden Daten in Netzwerken gesendet?	
018_Netzw4.hin	Hinführung - Paketvermittlung
019_Netzw4.arb	Arbeitsblatt - Paketvermittlung
020_Netzw4.loe	Lösungsblatt - Paketvermittlung
021_Netzw4.fol	Folie - Paketvermittlung
022_Netzw4.lzk	Lernzielkontrolle - Paketvermittlung
023_Netzw4.lzl	Lösung zur Lernzielkontrolle
024_Netzw4.int	Vertiefende Internetlinks

6. Netzwerktopologien: Bus, Stern, Ring, Netz	
025_Netzw5.hin	Hinführung - Netzwerktopologien
026_Netzw5.arb	Arbeitsblatt - Netzwerktopologien
027_Netzw5.loe	Lösungsblatt - Netzwerktopologien
028_Netzw5.fol	Folie - Netzwerk einer Universität
029_Netzw5a.loe	Lösungsblatt zur Folie
030_Netzw5.lzk	Lernzielkontrolle - Netzwerktopologien
031_Netzw5.lzl	Lösung zur Lernzielkontrolle
032_Netzw5.int	Vertiefende Internetlinks

7. Netzwerke im Modell: OSI	
033_Netzw6.hin	Hinführung - Netzwerke im Modell
034_Netzw6.arb	Arbeitsblatt - Das OSI-Modell

035_Netzw6a.arb	Arbeitsblatt - Analogie zum OSI-Modell
036_Netzw6.loe	Lösungsblatt - Das OSI-Modell
037_Netzw6.fol	Folie - Das OSI-Modell
038_Netzw6.lzk	Lernzielkontrolle - Das OSI-Modell
039_Netzw6.lzl	Lösung zur Lernzielkontrolle
040_Netzw6.int	Vertiefende Internetlinks

8. Netzwerkkomponenten I	
041_Netzw7.hin	Hinführung - Netzwerkkomponenten I
042_Netzw7.arb	Arbeitsblatt - Experiment MAC-Adressen
043_Netzw7a.arb	Arbeitsblatt - Netzwerkkomponenten I
044_Netzw7.loe	Lösungsblatt - Netzwerkkomponenten I
045_Netzw7.fol	Folie - Netzwerkkomponenten I
046_Netzw7.lzk	Lernzielkontrolle - Netzwerkkomponenten I
047_Netzw7.lzl	Lösung zur Lernzielkontrolle
048_Netzw7.int	Vertiefende Internetlinks

9. Die Sprachen des Netzwerks: Protokolle	
049_Netzw8.hin	Hinführung - Die Sprachen des Netzwerks
050_Netzw8.arb	Arbeitsblatt - Experiment POP3
051_Netzw8.did	Hinweise zum Experiment FTP
052_Netzw8a.arb	Arbeitsblatt - Experiment FTP
053_Netzw8.fol	Folie - Aufgaben von Protokollen
054_Netzw8.lzk	Lernzielkontrolle - Protokolle
055_Netzw8.lzl	Lösung zur Lernzielkontrolle
056_Netzw8.int	Vertiefende Internetlinks

10. TCP/IP: IP-Adressierung – Teil 1	
057_Netzw9.hin	Hinführung - IP-Adressierung
058_Netzw9.arb	Arbeitsblatt - IP-Adressierung
059_Netzw9.loe	Lösungsblatt - IP-Adressierung
060_Netzw9.fol	Folie - Umwandlung von IP-Adressen

11. TCP/IP: IP-Adressierung – Teil 2

061_Netzw10.hin	Hinführung - Klassenlose Adressierung
062_Netzw10.arb	Arbeitsblatt - Klassenlose Adressierung
063_Netzw10.loe	Lösungsblatt - Klassenlose Adressierung
064_Netzw10.lzk	Lernzielkontrolle - IP-Adressierung
065_Netzw10.lzl	Lösung zur Lernzielkontrolle
066_Netzw10.int	Vertiefende Internetlinks

12. Das Protokoll TCP

067_Netzw11.hin	Hinführung - Das Protokoll TCP
068_Netzw11.arb	Arbeitsblatt - Experiment Firewall
069_Netzw11.loe	Lösungsblatt - Experiment Firewall
070_Netzw11.fol	Folie - Portfilterung an einer Firewall
071_Netzw11.lzk	Lernzielkontrolle - Das Protokoll TCP
072_Netzw11.lzl	Lösung zur Lernzielkontrolle
073_Netzw11.int	Vertiefende Internetlinks

13. Netzwerkkomponenten II

074_Netzw12.hin	Hinführung - Router
075_Netzw12.arb	Arbeitsblatt - Router
076_Netzw12.loe	Lösungsblatt - Router
077_Netzw12.fol	Folie - Ein geroutetes Netzwerk
078_Netzw12.lzk	Lernzielkontrolle - Router
079_Netzw12.lzl	Lösung zur Lernzielkontrolle
080_Netzw12.int	Vertiefende Internetlinks

14. DHCP und DNS

081_Netzw13.hin	Hinführung - DHCP und DNS
082_Netzw13.arb	Arbeitsblatt - Experiment DNS
083_Netzw13.loe	Lösungsblatt - Experiment DNS
084_Netzw13.fol	Folie - DNS-Auflösung
085_Netzw13.lzk	Lernzielkontrolle - Netzwerkdienste

086_Netzw13.lzl	Lösung zur Lernzielkontrolle
087_Netzw13.int	Vertiefende Internetlinks

15. Das Internet	
088_Netzw14.hin	Hinführung - Das Internet
089_Netzw14.fol	Folie - Internetinfrastruktur Deutschland
090_Netzw14.int	Vertiefende Internetlinks

Die dreistelligen Buchstabenkombinationen am Ende der Kurz-Dateinamen bedeuten:

*.hin	Hinführung zum Thema	*.arb	Arbeitsblatt
*.loe	Lösungsblatt	*.did	Hinweise für Lehrer
*.fol	Folie	*.lzk	Lernzielkontrolle
*.lzl	Lösung zur Lernzielkontrolle	*.int	Weiterführende Internetlinks
*.ges	Gesamtdatei		

Hinweise zu dieser Einheit

Diese Einheit behandelt grundlegende Themen zum Aufbau von Netzwerken. Dabei wird immer wieder angeregt, mit bestimmten Funktionen auch praktische Experimente durchzuführen. Da aber in Schulen meist keine Möglichkeit besteht, auf administrativer Ebene Änderungen an Schüler-Computern durchzuführen bzw. wirklich mit verschiedenen Einstellungen zu testen, sind die Experimente so ausgelegt, dass sie keine Änderungen am Clientcomputer erfordern. Stattdessen werden Experimente mit dem Internet angeboten. Dies setzt allerdings voraus, dass der dafür nötige Verkehr nicht durch eine Firewall geblockt wird. Sollte es keine Möglichkeit geben, dies zu realisieren, können die Experimente oft auch als Hausarbeit am privaten Computer durchgeführt werden. Daneben ist es natürlich möglich, Entsprechendes auch mit einem passend konfigurierten Test-/Servercomputer im Klassenraum darzustellen.

Screenshots und Anweisungen basieren in dieser Einheit auf Windows XP. Alle Experimente lassen sich jedoch auch in Windows Vista und Windows 7 realisieren, wobei evtl. andere Wege zum Ziel führen oder auch Komponenten nachinstalliert werden müssen (z. B. Telnet).

Selbstverständlich sind dieselben Versuche auch mit Linux-Rechnern jederzeit möglich, wenn die Befehle entsprechend angepasst werden.

Leben in der Informationsgesellschaft

Partnerarbeit:

Denkt einmal über einen typischen Tag nach und listet in der Tabelle unten auf, wo ihr an diesem Tag technische Hilfsmittel zur Kommunikation verwendet. Notiere, welche Tätigkeiten zu eurem Tagesablauf gehören und welche Geräte/Systeme zum Einsatz kommen.

Uhrzeit	Tätigkeiten	Geräte/Systeme
Beispiel: 7:30	Noch kurz vor der Schule SMS an Freunde, um Treff zu verabreden	Handy, Mobilfunknetz

Fragen zum Weiterdenken und Diskutieren:

Bestimmt, auf wie viele Punkte ihr gekommen seid. Diskutiert, wie wichtig diese Dinge für euren Alltag sind. Beschreibt, wie ein Leben ohne diese Technik aussähe.

Ein Großteil dieser Technologien basiert auf Netzwerken. Definiere den Begriff Netzwerk.

Leben in der Informationsgesellschaft

Partnerarbeit:

Denkt einmal über einen typischen Tag nach und listet in der Tabelle unten auf, wo ihr an diesem Tag technische Hilfsmittel zur Kommunikation verwendet. Notiere, welche Tätigkeiten zu eurem Tagesablauf gehören und welche Geräte/Systeme zum Einsatz kommen.

Beispiel-Lösung:

Uhrzeit	Tätigkeiten	Geräte/Systeme
Beispiel: 7:30	Noch kurz vor der Schule SMS an Freunde, um Treff zu verabreden	Handy, Mobilfunknetz
10:00	Als Teil einer Schulaufgabe Recherche im Internet	Computer, DSL-Leitung, Internet
12:00	E-Mail an Freundin	Computer, DSL-Leitung, Internet
13:00	Freund anrufen mit dem Handy	Handy, Mobilfunknetz
15:00	Festnetztelefonat mit Freundin (der Handyakku ist leer...)	Mobiles Gesprächsteil, Basisstation, Telefonleitung, Telefonnetzwerk
17:00	Treff mit Clan zum Gamen im Internet	Computer, DSL-Leitung, Internet
20:00	Fernsehen	Fernseher, Fernbedienung, Satellit- oder Kabelnetzwerk

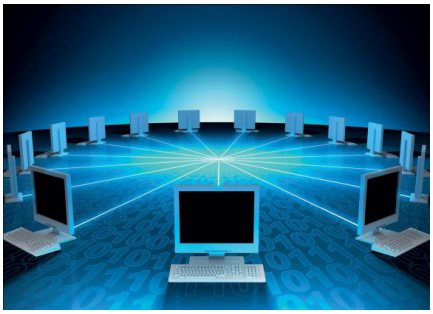
Fragen zum Weiterdenken und Diskutieren:

Bestimmt, auf wie viele Punkte ihr gekommen seid. Diskutiert, wie wichtig diese Dinge für euren Alltag sind. Beschreibt, wie ein Leben ohne diese Technik aussähe.

Ein Großteil dieser Technologien basiert auf Netzwerken. Definiere den Begriff Netzwerk.

Abbildung: http://www.gea.de/fastmedia/38/handy_telefonieren_dpa.jpg, 26.04.10

Was ist ein Netzwerk?



LAN / MAN / WAN / GAN

Wenn man mit Computern oder Technik im Allgemeinen zu tun hat, begegnen einem leider oft eine Menge Abkürzungen.

Aufgabe:

LAN / MAN / WAN und GAN bezeichnen Netzwerke unterschiedlicher Größe.

Recherchiere im Internet und ergänze unten die Definitionen.

LAN = _____

MAN = _____

WAN = _____

GAN = _____

Abbildung: http://res.magnus.de/res/_2/3/2/1/45303.jpg, 26.04.10

Clients, Server, Dienste

Netzwerke dienen dazu, Ressourcen gemeinsam zu nutzen. Solche Ressourcen können Daten sein, die für alle gemeinsam zur Verfügung stehen müssen, ein Drucker, der von allen im Büro genutzt wird, externer Festplattenspeicher, eine Datenbank oder die Verbindung zum Internet. Bei der Erstellung eines Netzwerks stellt sich daher rasch die Frage, wer die gemeinsamen Ressourcen zur Verfügung stellt und verwaltet.

Es gibt zwei grundsätzliche Arten von Netzwerken:

1. Peer-to-Peer-Netzwerke

In einem Peer-to-Peer-Netzwerk sind alle Rechner gleichberechtigt. Jeder Rechner kann Dienste und Ressourcen für andere Rechner zur Verfügung stellen und Dienste und Ressourcen von anderen Rechnern nutzen. So können zum Beispiel wichtige Dateien für die Arbeit in einem Büro auf verschiedenen Rechnern liegen, je nachdem, wer sie erstellt hat. Die anderen können dann auf die verschiedenen Rechner zugreifen, um die Dateien ebenfalls zu nutzen. Auf einem der Rechner ist vielleicht ein Drucker lokal angeschlossen, auf den die anderen zugreifen etc.

Diese Art, ein Netzwerk zu betreiben, ist leider ziemlich schwer zu verwalten und wird bald ziemlich unübersichtlich. Es kommen leicht Fragen auf: Wo lag noch mal die Datei? Wie hieß noch mal der Rechner, wo der Drucker dranhängt? Und so weiter. Deshalb verwendet man solche Peer-to-Peer-Netzwerke nur bei kleinen Netzwerken mit nicht mehr als 10 Rechnern.

2. Client-Server-Netzwerke

In einem Client-Server-Netzwerk werden Dienste und Ressourcen zentral verwaltet und auf Servern (von englisch „to serve“: dienen) zur Verfügung gestellt. So lassen sich zum Beispiel wichtige Dateien dort leicht wiederfinden und auch leicht gemeinsam sichern. Ein Client ist ein Rechner, der Ressourcen eines Servers nutzt.

Ein Server kann mehrere Dienste und Ressourcen gleichzeitig zur Verfügung stellen oder auch nur exklusiv eine Aufgabe erfüllen. Wichtige Arten von Servern, die in einem Netzwerk häufig zum Einsatz kommen, sind zum Beispiel:

* Datei- und Druckserver
* Datenbankserver
* E-Mail-Server
* Webserver

Daneben gibt es verschiedene Server, die administrative Dienste im Netzwerk übernehmen. Zwei davon sehen wir uns in einem späteren Kapitel genauer an.

Abbildung: https://portfolio.du.edu/pc/port?page=4&uid=15501, 26.04.10

Clients, Server, Dienste

Aufgabe 1:

Ergänze die Tabelle, die wichtige Eigenschaften von Client-Server- bzw. Peer-to-Peer-Netzwerken gegenüberstellt.

Eigenschaft	Peer-to-Peer-Netzwerk	Client-Server-Netzwerk
Wie groß ist das Netzwerk normalerweise?		
Wie wird das Netzwerk verwaltet?		
Wer bietet Dienste an?		
Wo liegen die Daten?		
Wer ist verantwortlich für die Sicherheit von Daten?		
Wo werden Daten gesichert?		
Welche Probleme können auftreten?		

Aufgabe 2:

Die Darstellung von Peer-to-Peer-Netzwerken in der Hinführung zu diesem Kapitel beschränkt sich auf die klassische Form eines Peer-to-Peer-Netzwerkes im Rahmen eines LANs. Darauf beziehen sich auch die oben dargestellten Eigenschaften. Es gibt aber auch noch eine weitere Variante von Peer-to-Peer-Netzwerken, die im Internet mittlerweile eine große Verbreitung haben. Die großen Filesharing-Netze und Musiktauschbörsen arbeiten zum Beispiel auf dieser Grundlage. Wahrscheinlich hast du auch schon Erfahrungen damit gesammelt.

Beschreibe die Funktionsweise dieser Art von Peer-to-Peer-Netzwerken am Beispiel eines bekannten Netzwerkes (zum Beispiel Gnutella, Emule-Kademlia, FastTrack/KaZaA). (Je nach Netzwerk und verwendetem Client gibt es leicht unterschiedliche Funktionen.) Recherchiere, wenn nötig, im Internet.

Abbildung: http://www.myprimeyears.com/lilypad/uploaded_images/communication.jpg, 26.04.10

In der Vergangenheit mussten viele solcher Tauschbörsen bereits den Betrieb einstellen. Nenne einen Grund dafür.

_____

_____

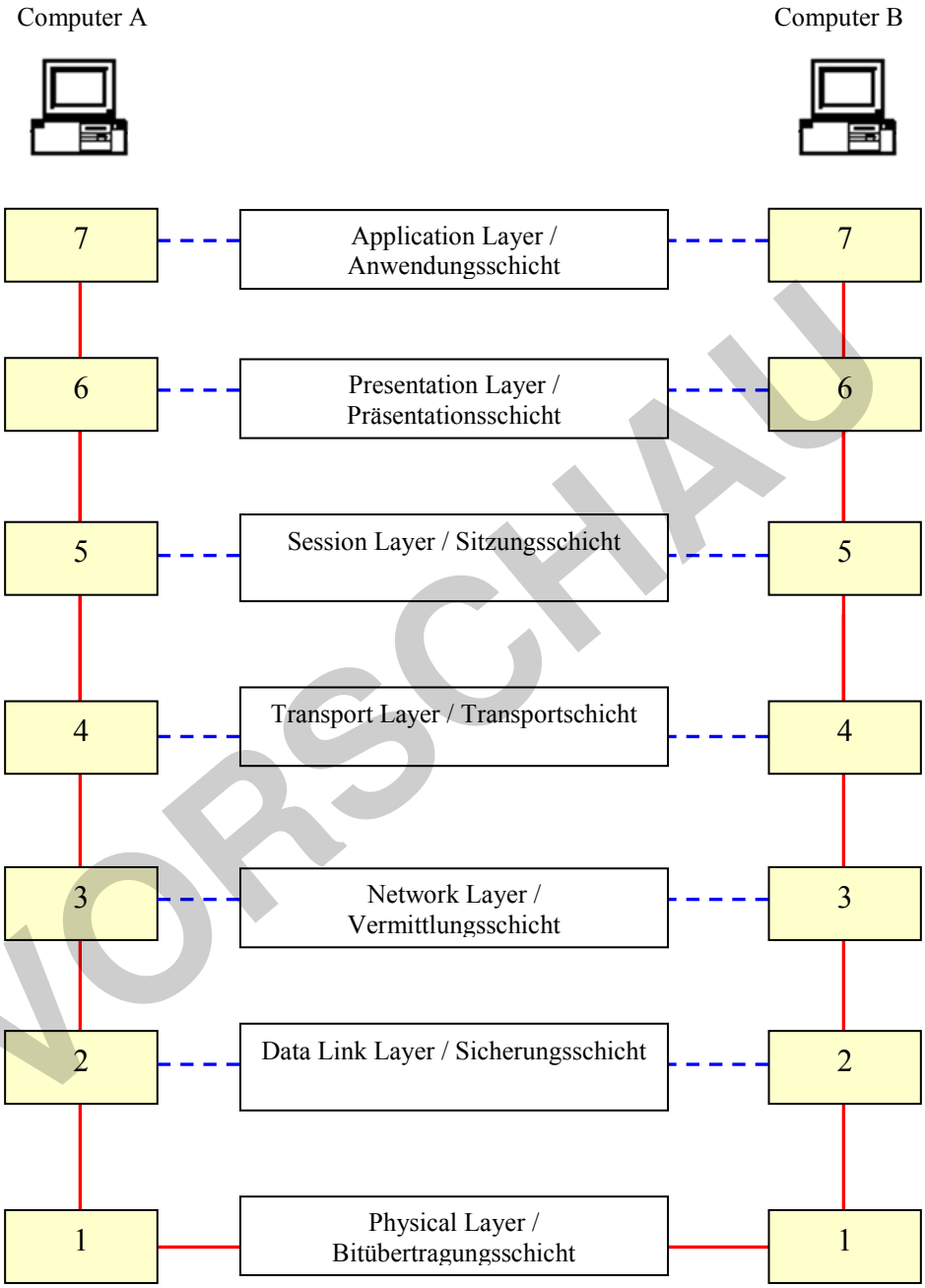
_____

Aufgabe 3:

Häufig sind Downloads über P2P-Tauschbörsen illegal. Diskutiert darüber, wie ihr damit umgeht.

Netzwerke im Modell: OSI

Um besser zu verstehen, wie die einzelnen Komponenten eines Netzwerkes zusammenarbeiten, wurden verschiedene Modelle entwickelt. Diese Modelle erscheinen auf den ersten Blick manchmal etwas kompliziert, sie erleichtern aber das Verständnis des Netzwerkverkehrs. In diesem Abschnitt betrachten wir eines der wichtigsten Modelle: das OSI-Modell. OSI steht für „Open Systems Interconnection“. Das Modell stellt den Netzwerkverkehr in verschiedenen Schichten dar.



Der **tatsächliche Weg** einer Nachricht verläuft in diesem Modell entlang der roten Linie: Ein Anwendungsprogramm, zum Beispiel ein E-Mail-Programm, erstellt eine Nachricht auf Rechner A. Diese Nachricht wird an Funktionen übergeben, die auf der Anwendungsschicht (Schicht 7) des OSI-Modells definiert sind. Von dort durchläuft sie die verschiedenen Ebenen, wobei sie auf jeder Ebene in bestimmter Weise verarbeitet und für den weiteren Transport aufbereitet wird. Dies geschieht innerhalb des Computers. Erst auf Schicht 1 findet dann die eigentliche Übertragung über

das Netzwerkmedium statt. Auf dem Zielcomputer werden alle Schichten in umgekehrter Reihenfolge durchlaufen, bis die Nachricht im Anwendungsprogramm des Nutzers dort dargestellt wird.

Die eigentliche **logische Kommunikation** findet entlang der blauen Linien statt: Logisch betrachtet kann man sich das so vorstellen, dass das Mailprogramm des Senders und des Empfängers miteinander kommunizieren, obwohl das nicht direkt der Fall ist, denn tatsächlich liegen viele Schritte dazwischen. Ebenso könnte man sagen, dass die Netzwerkkarte des Senders und des Empfängers miteinander kommunizieren. Aber auch hier liegen tatsächlich noch einige Schritte dazwischen.

Bei der Betrachtung der Ebenen ist keine Schicht sehr interessiert an den Einzelheiten der anderen Ebenen. Wichtig ist nur, dass jede Schicht die vorgegebenen Funktionen erfüllt.

Die Schichten und ihre speziellen Aufgaben werden im Folgenden kurz beschrieben:

Schicht 7: die Anwendungsschicht

Diese Schicht ermöglicht den eigentlichen Anwendungen den Zugriff auf eine Netzwerkkommunikation. Die Anwendung selbst ist aber nicht Teil des Modells. Beispiel: Der Internetbrowser soll auf das Internet zugreifen. Dazu benötigt er das HTTP-Protokoll oder zum Downloaden von Daten das FTP-Protokoll. Diese befinden sich auf dieser Schicht (zu Protokollen allgemein vgl. das entsprechende Kapitel).

Schicht 6: die Präsentationsschicht

Diese Schicht übersetzt die systemabhängige Darstellung von Daten in ein systemunabhängiges Format. Auch Verschlüsselung und Komprimierung von Daten finden hier statt.

Schicht 5: die Sitzungsschicht

Die Sitzungsschicht ist verantwortlich für die Aufrechterhaltung einer Session (Sitzung). Eine Session ist eine stehende Verbindung zwischen zwei Computern. Sie beginnt normalerweise mit einem Login und endet mit einem Logout. Diese Schicht sorgt dafür, dass die Session nicht abbricht, wenn es beim Transport der Daten zu Unregelmäßigkeiten kommt.

Schicht 4: die Transportschicht

Die Transportschicht kontrolliert unter anderem, ob die einzelnen Datenpakete, die über das Netz gesendet wurden, vollständig sind und nichts verloren ging. Fehlen Datenpakete, dann werden sie beim Sender erneut angefordert. Außerdem gibt es hier Funktionen, um Datenstau zu vermeiden.

Schicht 3: die Netzwerkschicht

Auf dieser Ebene findet die logische Adressierung statt. Hier wird auf der Basis von Start- und Zieladresse entschieden, wie ein Paket sein Ziel erreicht.

Schicht 2: die Sicherungsschicht

Hier wird der Datenstrom in Blöcke aufgeteilt, es werden Folgenummern und Prüfsummen hinzugefügt.

Schicht 1: die Bitübertragungsschicht

Auf dieser Schicht findet schließlich die eigentliche Datenübertragung statt. Die Daten werden als Folge von 0 und 1 über das Netzwerk gesendet. Auch werden hier zum Beispiel die Spezifikationen von Kabeln und verschiedenen Netzwerkgeräten festgelegt, Besonderheiten der Kommunikation über Funk usw.

Das OSI-Modell

Um das OSI-Modell leichter verständlich zu machen, wird es oft anhand einer Analogie dargestellt: Der Manager einer großen deutschen Firma möchte einem Kollegen in Japan, der nur Japanisch spricht, einen Brief senden. Der Manager diktiert oder schreibt also den Brief. Er trägt ihn jedoch nicht gleich selbst zur Post. Da sich beide Manager nicht verstehen, muss der Brief zunächst übersetzt werden. Ein Japanisch-Übersetzer steht aber nicht zur Verfügung. Der Assistent des Managers übersetzt den Brief daher in Englisch. Der Assistent des japanischen Managers kann dann den englischen Brief am Ziel in Japanisch übersetzen. Auch der Assistent läuft aber nicht selbst zur Post. Der Brief geht zunächst an die Sekretärin, diese adressiert ihn und gibt ihn dem Fahrer der Firma, der ihn schließlich zur Post bringt ...

Der Brief durchläuft also verschiedene „Funktionsebenen“ sowohl beim Sender als auch beim Empfänger, bevor er sein Ziel erreicht. Diese Funktionsebenen haben ganz ähnliche Aufgaben wie die verschiedenen Schichten im OSI-Modell.

Aufgabe

Arbeite gemeinsam mit deinem Nachbarn. Schneidet zuerst die Piktogramme auf dem zusätzlichen Arbeitsblatt aus und sortiert sie so, dass sie den Weg des Briefs beim Sender und beim Empfänger in der richtigen Reihenfolge darstellen. Klebt die Piktogramme in der richtigen Reihenfolge auf der nächsten Seite untereinander auf: links von oben nach unten den Weg vom Manager bis zum Versand mit der Post, rechts von unten nach oben den Weg vom Postversand bis zum Manager (gleiche Funktionen also auf derselben Ebene).

Tragt nun in der Mitte die Namen der entsprechenden Schichten des OSI-Modells ein und überlegt, welche Tätigkeiten auf der jeweiligen Ebene bei Sender und Empfänger erfüllt werden, die dem OSI-Modell in etwa entsprechen. Vergleicht dazu die Funktionen mit den in der Hinführung beschriebenen Funktionen der einzelnen OSI-Ebenen. Die Begriffe im Kasten helfen euch dabei.

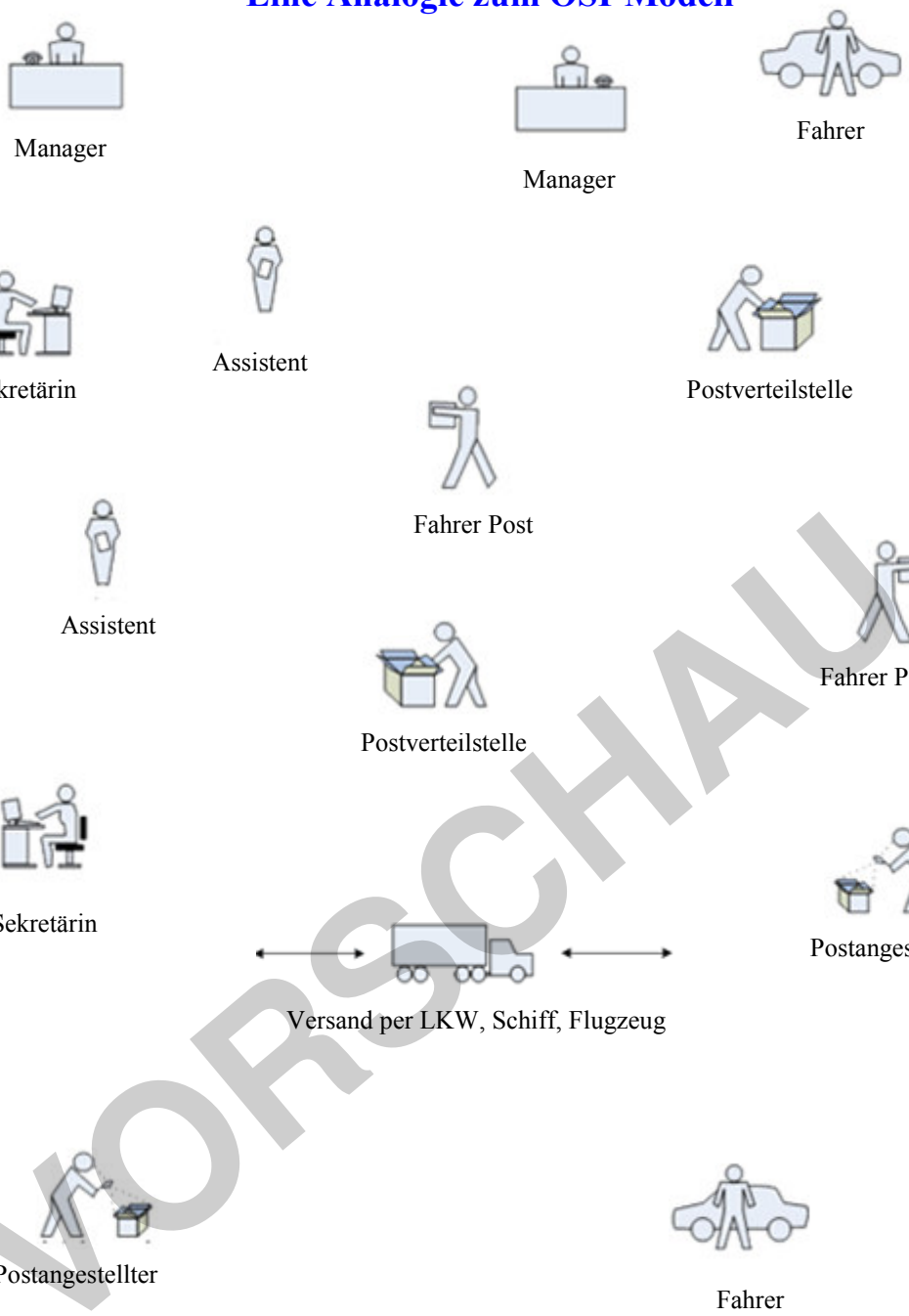
Nachricht abholen und auf Beschädigung überprüfen, Nachricht öffnen und korrekt weiterleiten, über Versandweg entscheiden, Nachrichten aus verschiedenen Richtungen in Empfang nehmen und überprüfen, Nachricht übersetzen, Nachricht auf den Weg bringen, für den richtigen Versand korrekt zuordnen und verpacken, versenden, Nachricht dem richtigen Empfänger zuordnen und diesem übergeben, Nachricht übersetzen, Verwaltung abwickeln

Anmerkung: Manchmal ist die richtige Zuordnung nicht ganz eindeutig. Schließlich handelt es sich hier nur um eine Analogie. Wichtig ist, dass das Prinzip deutlich wird.

Die einzelnen Funktionsebenen arbeiten in dieser Analogie wie im OSI-Modell unabhängig voneinander. Es ist dem Manager ziemlich egal, ob der Fahrer der Firma im Stau steht oder wegen einer Baustelle eine Umleitung fährt, wenn er den Brief zur Post bringt. Wichtig ist nur, dass der Brief zeitnah dort ankommt und verschickt wird. Auch die Sekretärin interessiert sich nicht für die internen Abläufe der Post. Ihr ist nur wichtig, dass die Sekretärin des japanischen Managers möglichst bald den Brief bekommt und ihr keinen Stress macht.

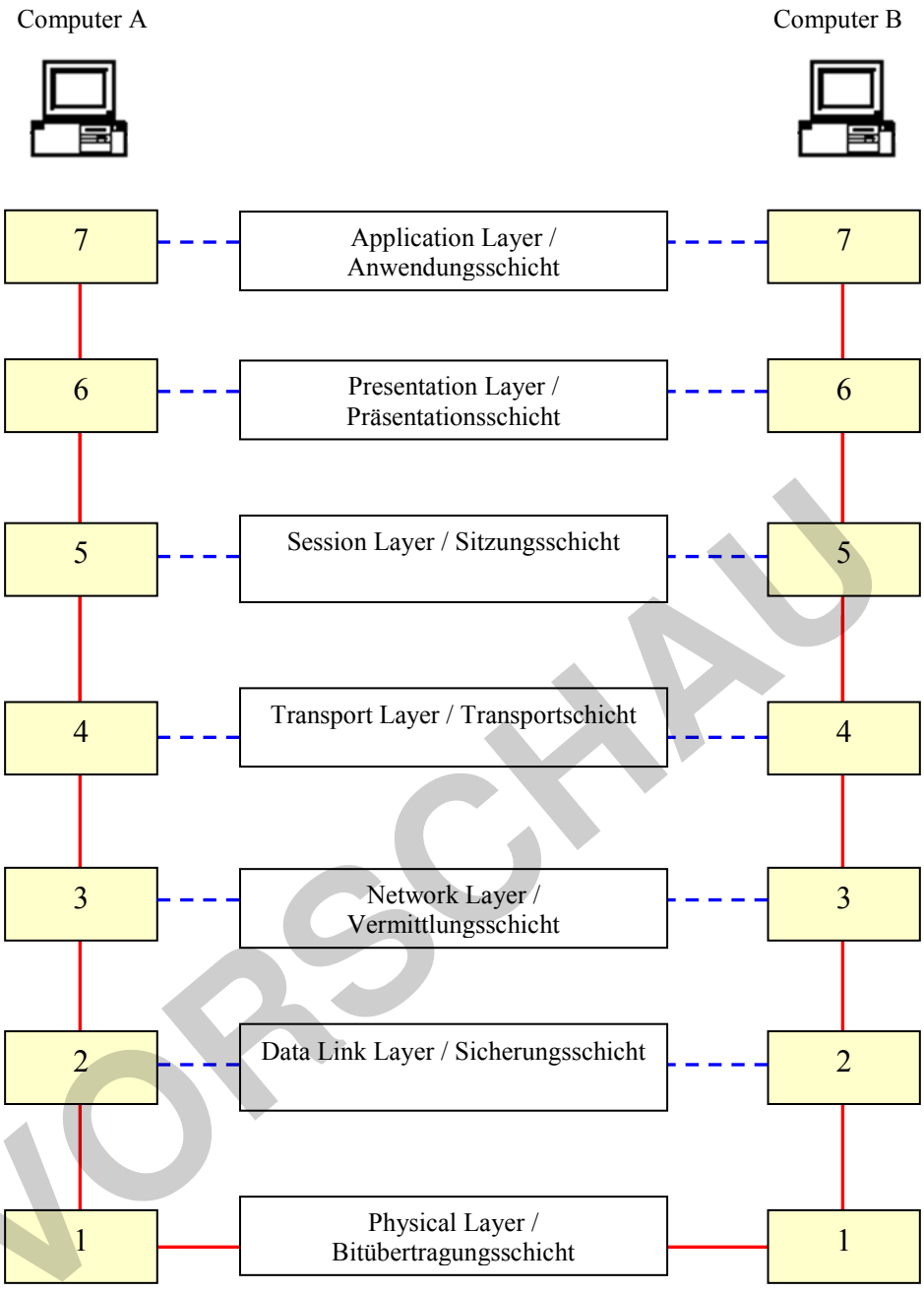
Abbildung: http://ich-leih-dir-mein-ohr.com/resources/Fotolia_Schreibhand_M.jpg, 26.04.10

Eine Analogie zum OSI-Modell



Piktogramme von: http://www.thered.co.uk/nplus/nplus_images/osi-mail.gif, 11.03.10

Das OSI-Modell



TCP/IP: Das Protokoll TCP

Wie wir bereits zuvor gesehen haben, implementiert das Protokoll TCP Schicht 4 von OSI. Wir werden in diesem Kapitel nicht die Feinheiten von TCP betrachten, gehen aber auf einige wichtige Punkte ein.

Während mithilfe der IP-Adresse ein Zielrechner adressiert wird, wird über TCP der **Prozess auf dem Zielrechner** adressiert, der die Nachricht erhalten soll.

Man kann sich dies wieder anhand einer Hausadresse zum Beispiel einer Firma vorstellen. Während die Netzwerkadresse der Straße und die Hostadresse einer Hausnummer entspricht, wird über den Prozess die Abteilung innerhalb des Hauses angegeben. Nur wenn diese Abteilung die Nachricht akzeptiert, wird sie auch angenommen.

Zur Bezeichnung des Prozesses werden sogenannte **Ports** verwendet. Serverprozesse verwenden dabei in der Regel bekannte Standardports, auf denen sie auf eine Verbindungsaufnahme durch ein bestimmtes Protokoll „lauschen“. Die Tabelle zeigt die Protokolle, die wir betrachtet haben, und die Ports, über die im Allgemeinen kommuniziert wird.

Protokoll	Port
HTTP	80
FTP	20/21
SMTP	25
POP3	110
Telnet	23

Daneben gibt es sehr viele weitere Ports und Protokolle, die wir hier jedoch nicht näher betrachten. Auf dieser (englischen) Wikipedia-Seite gibt es eine ausführliche Liste: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

Wenn man einen bestimmten Port ansprechen möchte, um eine Verbindung aufzunehmen, verwendet man eine Kombination aus IP-Adresse und Port, durch einen Doppelpunkt getrennt. Eine solche Kombination aus IP-Adresse und Port wird **Socket** genannt.

Beispiel: Mit 81.20.93.114:80 wird der Webserver unter dieser Adresse angesprochen und man könnte zum Beispiel eine Webseite herunterladen. Um demselben Server eine Mail zu senden, müsste man 81.20.93.114:25 adressieren.

Ports als Einfallstor

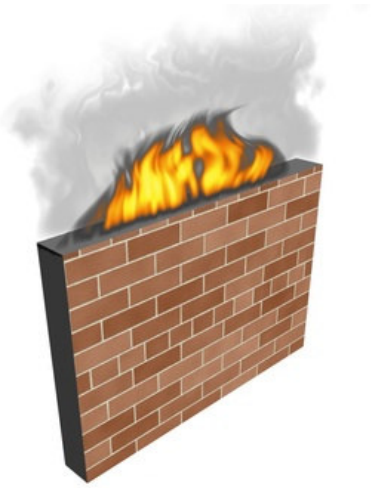
Ports spielen eine wichtige Rolle beim Schutz eines Computers. Der Port ist sozusagen die Tür, durch die eine Verbindung stattfinden kann, die aber auch von Angreifern zum Eindringen verwendet wird. Insgesamt gibt es 65535 Ports, die für Verbindungen verwendet werden können. Gefährdet sind die Ports, die tatsächlich einen Dienst nach außen anbieten und damit offen sind.

Eine Hauptfunktion einer **Firewall** ist es daher, unerwünschte Verbindungsanfragen auf die Ports eines Rechners zu verhindern bzw. bereits vor dem Eintritt in das Netzwerksegment abzufangen. Dies geschieht über einen **Paketfilter**. Mit dessen Hilfe werden ein- und ausgehende Pakete auf ihre Zulässigkeit überprüft und evtl. verworfen. Gefiltert werden kann hierbei in der Regel nach Quell- und Zieladresse, Quell- und Zielport und Protokoll.

Aufgrund der Vielzahl der Kombinationen aus Protokollen, Adressen, Ports, ein- und ausgehendem Verkehr und den weiteren Funktionen einer Firewall ist die manuelle Konfiguration sehr kompliziert und aufwendig. Dies ist normalerweise Experten vorbehalten.

TCP/IP: Das Protokoll TCP

Experiment[4]



Verwende einen Rechner, der möglichst direkt mit dem Internet verbunden sein sollte, gehe auf die Seite https://www.grc.com/x/ne.dll?bh0bkyd2 und lasse den Rechner auf offene Ports scannen. Die Seite ist englisch, ein Klick auf „Proceed“ bringt dich weiter. Ein Scan über die „Common Ports“ ist hier ausreichend, da er sonst sehr lange dauert.

Führe diesen Test einmal mit und einmal ohne aktivierte Windows-Firewall durch. Die Windows-Firewall kann über das Sicherheitscenter in der Systemsteuerung deaktiviert werden.

Beschreibe, welches Ergebnis du erhältst.

Untersuche, ob dein Rechner so konfiguriert ist, dass er bei aktivierter Firewall als sicher eingestuft wird. (Hinweis: Dies ist nicht immer der Fall, denn viele Programme, die wir selbstverständlich freischalten, halten Ports offen und sind evtl. ein Sicherheitsrisiko.)

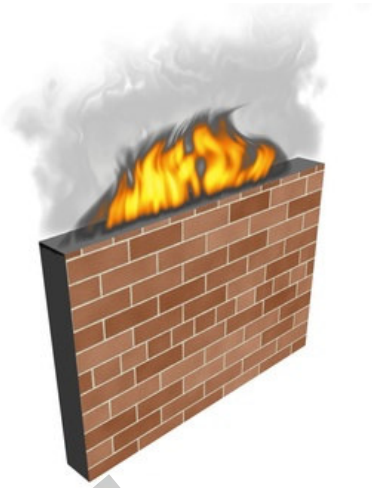
Prüfe, welche Ports bei deaktivierter Firewall geöffnet sind. Lies die Kommentare zu den offenen Ports, in denen erläutert wird, warum der geöffnete Port eine potentielle Gefahr darstellt.

Abbildung: http://www.pc-service-wiesbaden.de/images/firewall.jpg, 05.12.09

[4] Dieses Experiment findet sich in ähnlicher Weise auch in Einheit 4501 zu Datenschutz und Datensicherheit.

TCP/IP: Das Protokoll TCP

Experiment



Verwende einen Rechner, der möglichst direkt mit dem Internet verbunden sein sollte, gehe auf die Seite https://www.grc.com/x/ne.dll?bh0bkyd2 und lasse den Rechner auf offene Ports scannen. Die Seite ist Englisch, ein Klick auf „Proceed“ bringt dich weiter. Ein Scan über die „Common Ports“ ist hier ausreichend, da der Scan sonst sehr lange dauert.

Führe diesen Test einmal mit und einmal ohne aktivierte Windows-Firewall durch. Die Windows-Firewall kann über das Sicherheitscenter in der Systemsteuerung deaktiviert werden.

Beschreibe, welches Ergebnis du erhältst.

Untersuche, ob dein Rechner so konfiguriert ist, dass er bei aktivierter Firewall als sicher eingestuft wird. (Hinweis: Dies ist nicht immer der Fall, denn viele Programme, die wir selbstverständlich freischalten, halten Ports offen und sind evtl. ein Sicherheitsrisiko.)

Prüfe, welche Ports bei deaktivierter Firewall geöffnet sind. Lies die Kommentare zu den offenen Ports, in denen erläutert wird, warum der geöffnete Port eine potentielle Gefahr darstellt.

Beispiel mit aktivierter Firewall:

Your computer at IP:

62.180.176.42

Is being profiled. Please stand by. . .

Total elapsed testing time: 6.042 seconds

PASSED **TruStealth Analysis** PASSED

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Service	Status	Security Implications
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
119	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Hier sind alle Ports als „Stealth“ markiert, das heißt, sie sind im Internet nicht sichtbar. Dieser Rechner ist vergleichsweise sicher.

Abbildung: http://www.pc-service-wiesbaden.de/images/firewall.jpg, 05.12.09

Und bei deaktivierter Firewall:

Port	Service	Status	Security Implications
0	<nil>	Closed	Your computer has responded that this port exists but is currently closed to connections.
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
22	SSH	Closed	Your computer has responded that this port exists but is currently closed to connections.
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	OPEN!	The web is so insecure these days that new security "exploits" are being discovered almost daily. There are many known problems with Microsoft's Personal Web Server (PWS) and its Frontpage Extensions that many people run on their personal machines. So having port 80 "open" as it is here causes intruders to wonder how much information you might be willing to give away.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
119	NNTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
135	RPC	OPEN!	(Remote Procedure Call) This impossible-to-close port appears in most Windows systems. Since many insecure Microsoft services use this port, it should never be left "open" to the outside world. This port has been exploited to send "Messenger Spam" pop-ups to Microsoft windows users. Since it is impossible to close, you will need a personal firewall or NAT router to block it from external access. Do it soon!
139	Net BIOS	Closed	Your computer has responded that this port exists but is currently closed to connections.
143	IMAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
389	LDAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
443	HTTPS	OPEN!	The presence of this secure web port in your system implies that this system is establishing secure connections with web browsers. The number one reason for doing this is the transmission of credit card information. This implies that the successful intruder could access the web server's credit card database and score bigtime. This is a VERY bad port to have open unless you are actually conducting secure web commerce!

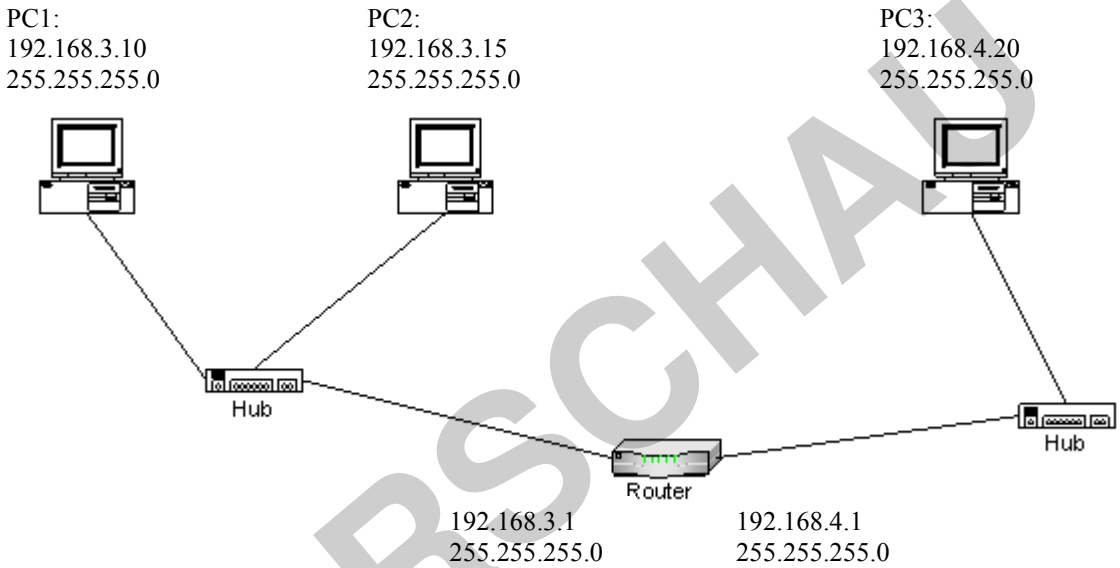
Hier sieht man, dass einige Ports geöffnet sind und damit potentiell Verbindungen aus dem Internet akzeptieren.

Netzwerkkomponenten II: Router

Im Teil I zu den Netzwerkkomponenten haben wir Geräte betrachtet, die auf den OSI-Schichten 1 und 2 arbeiten. In diesem Kapitel schauen wir uns nun den Router an. Dieser arbeitet auf OSI-Schicht 3.

Wie wir gesehen haben, können Rechner nur dann direkt miteinander kommunizieren, wenn sie sich – neben der physischen Verbindung – auch logisch (also im Bezug auf die IP-Adresse) im selben Netzwerksegment befinden. Router sind so konfiguriert, dass sie über mehrere Netzwerkkarten gleichzeitig an mehrere Netzwerksegmente angeschlossen sind. Anhand von sogenannten **Routingtabellen** entscheiden sie, in welches ihrer angeschlossenen Netzwerksegmente eine Nachricht weitergeleitet werden muss, um ihr Ziel zu erreichen. Router sind zudem in der Lage auch unterschiedliche Netzwerkmedien zu verbinden, zum Beispiel die Verbindung zwischen einem WLAN und einem verkabelten LAN herzustellen.

Beispiel:



Hier verbindet ein Router zwei Netzwerksegmente, in denen jeweils einige Rechner stehen. Die Rechner im einen Segment haben alle die Netzwerkadresse 192.168.3.0, die Rechner im anderen Segment haben die Netzwerkadresse 192.168.4.0.

(Anmerkung: Bis jetzt haben wir IP-Adressen nur zur Bezeichnung eines Rechners kennen gelernt. Tatsächlich hat aber auch jedes Netzwerksegment eine Adresse. Dabei ist der Hostanteil der Adresse 0.)

Nur über den Router können die Rechner im einen Segment mit den Rechnern im anderen Segment kommunizieren.

Wenn PC1 eine Nachricht an PC3 senden möchte, überprüft er zunächst die eigene und die fremde IP-Adresse (wie er diese ermittelt, dazu mehr im nächsten Kapitel). Dabei stellt er fest, dass PC3 nicht in seinem Netzwerksegment liegt und er deshalb seine Nachricht nicht direkt dorthin senden kann. Für diesen Fall wird auf jedem Rechner ein **Standard-Gateway** (englisch: **default gateway**) definiert – die Adresse des Routers. Das heißt: jede Nachricht, die der Rechner nicht direkt seinem eigenen Netzwerksegment zuordnen kann, wird automatisch an das Standard-Gateway und damit den Router gesendet. Der Router erkennt, dass er mit dem Segment von PC3 direkt verbunden ist und leitet die Nachricht dorthin weiter.