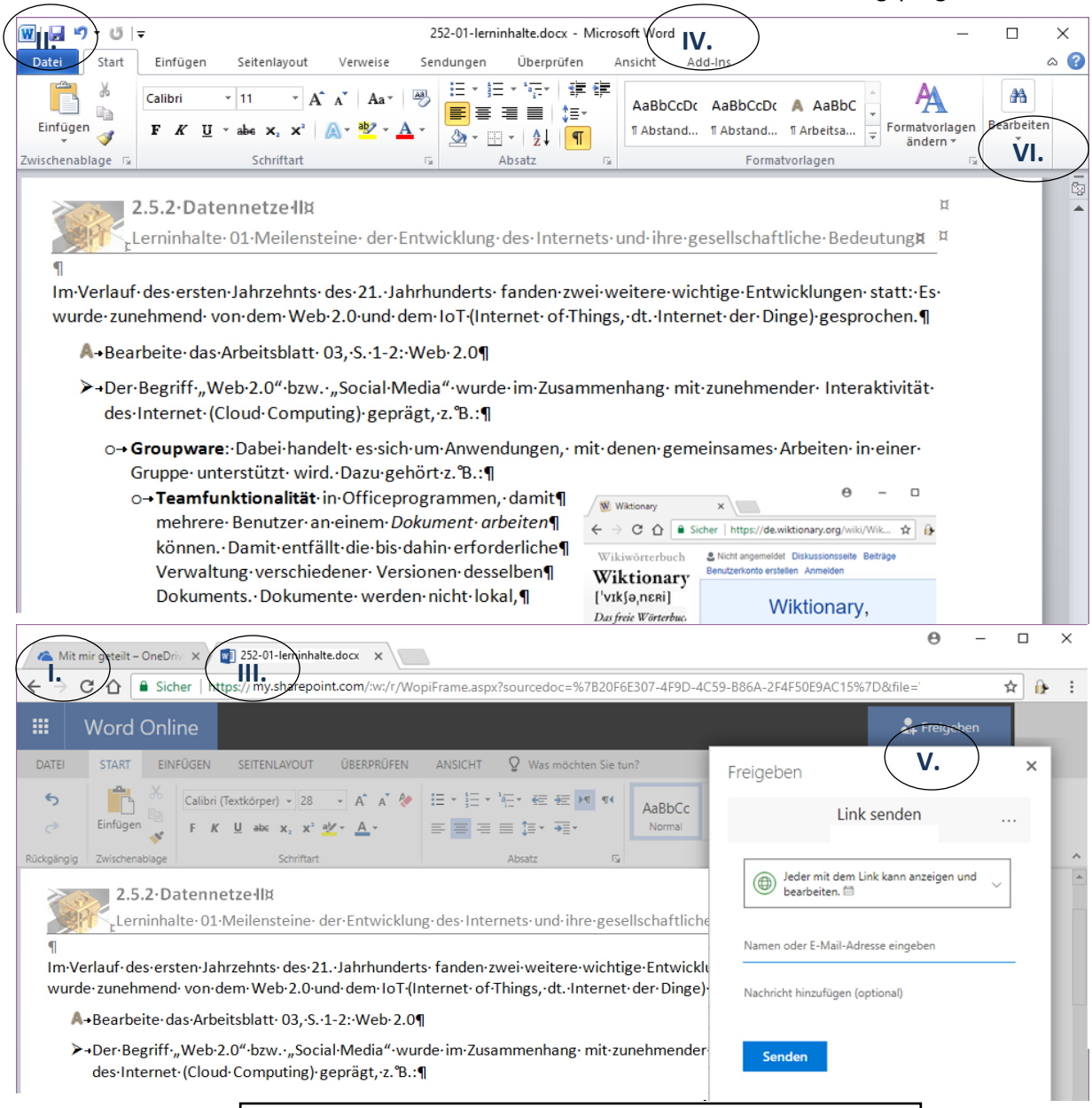
Web 2.0

1. Beschreibe die Unterschiede zwischen den beiden Versionen des Textverarbeitungsprogramms.



I. Die Datei wird _____ gespeichert.

II. Die Datei wird _____ gespeichert.

III. Die Programmoberfläche wird _____ angezeigt,
die Anwendung wird _____ ausgeführt.

IV. Die Anwendung ist _____ installiert.

V. Das Textdokument kann _____ gleichzeitig bearbeitet werden.

VI. Das Textdokument kann _____ bearbeitet werden.

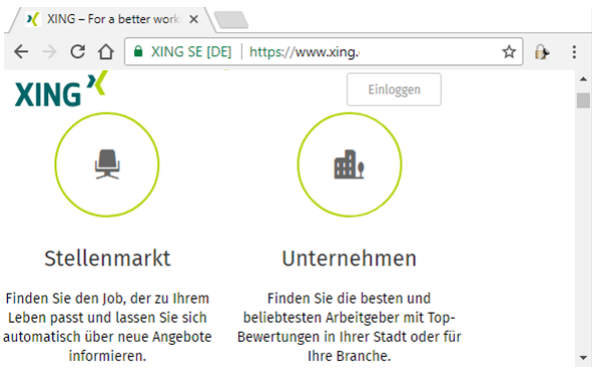
➢ Früher war eine Anwendung immer auf einem lokalen Rechner installiert. Beim **Cloud Computing** wird Speicherplatz und Anwendungssoftware im Internet genutzt. Im „**Web 2.0**“ können Benutzer Daten im Internet zur Verfügung stellen, direkt zusammenarbeiten und kommunizieren.

2. Beschreibe die Merkmale eines Wikis:
(siehe Abbildung rechts)

3. Bei einem **Blog** („Weblog“) handelt es sich um ein öffentlich einsehbares Tagebuch. Die Leser können meist Diskussionsbeiträge ergänzen, so dass im Blog auch Kommunikation möglich ist. Beispielsweise in *Twitter* können Kurznachrichten verfasst werden.
   - Rufe einen Blog auf. Wähle z. B. eine prominente Person aus der Politik, aus dem Showgeschäft oder aus dem Sport. Lies und bewerte einige Beiträge.

4. Nenne Vorteile von **Instant-Messaging**-Diensten wie *Skype* oder *WhatsApp* gegenüber *SMS* oder *E-Mail*.

5. Über **Soziale Netzwerke** wie *Facebook*, *XING* oder *LinkedIn* können sich Benutzer vernetzen. Nenne Gründe für die Nutzung der unterschiedlichen Sozialen Netzwerke.



➢ Der Begriff „**Social Media**“ beinhaltet, dass sich Benutzer im Internet vernetzen können.
   - Das beinhaltet, Inhalte einfach veröffentlichen und gemeinsam bearbeiten können.
   - Damit kann das gemeinsame Wissen von Nutzern zusammengefasst und vernetzt werden.
   - Wissen, Meinungen und andere Informationen werden schnell verbreitet.

„Dinge“ in Netzwerken

In privaten Privathaushalt werden immer häufiger unterschiedliche Geräte mit einem WLAN vernetzt. Oft funktioniert das Lokale Netz ohne weitere Anpassungen. Fraglich ist nur, ob die Standardeinstellungen des WLAN-Routers sinnvoll sind und was zu tun ist, wenn doch nicht alles wie gewünscht funktioniert.

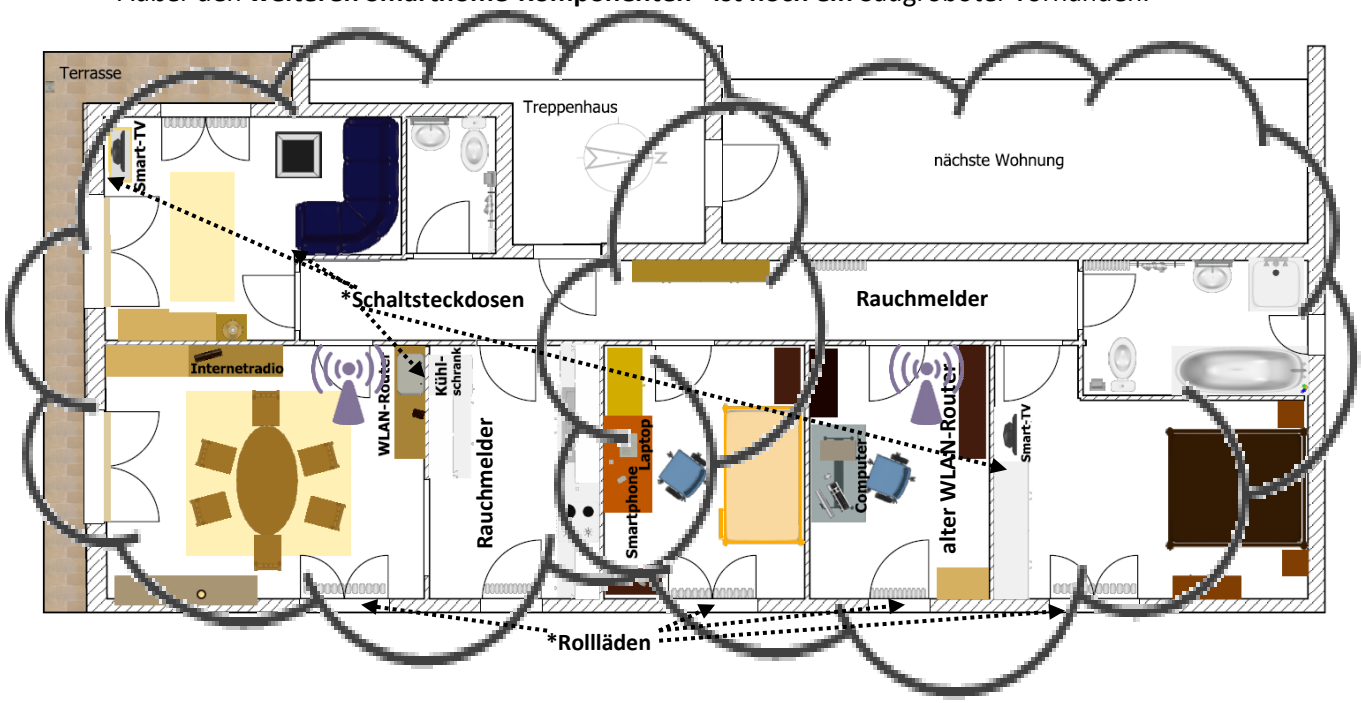
- Im Beispiel (vgl. Arbeitsblatt 2.5.1–07, S. 2-3) wurde ein Twisted-Pair- Kabel in das Arbeitszimmer gelegt und dort eine Ethernet-Anschlussdose installiert.
  * Erstellt mit Sweet Home 3D.
    Das Programm ist veröffentlicht unter der GNU General Public License.
    Weitere Informationen und Download: http://www.sweethome3d.com/

    Hinweise (Wiederholung):
    - Da der WLAN-Router der Ausgangspunkt möglicher Maßnahmen ist, wird dieser vergrößert dargestellt.
    - Durch Hindernisse wird das Funksignal gedämpft. Eine Mauer reduziert die Signalstärke je nach Dicke der Wand etwa um ein Viertel. Feuchtigkeit und Metall dämpfen besonders stark. Das gilt z. B. für mit Metallträgern gebaute Rigipswände, Fußbodenheizungen, Waschmaschinen oder Kühlschränke.
    - Die Signalstärke ist im Bereich von 2-3 Wänden normalerweise hinreichend, wobei die Datenübertragungsrate mit jeder Wand immer weiter abnimmt.
    - Der WLAN-Router steht auf der anderen Seite der Wand direkt hinter dem Kühlschrank. Allgemein gilt: Je höher der Router steht, desto besser. In diesem Fall sollte er auf jeden Fall über dem Kühlschrank montiert werden, wofür man ein Wandregal anbringen könnte.

    ➔ An dem Computer im Arbeitszimmer kann man das WLAN-Signal evtl. noch empfangen, an dem Smart-TV im Schlafzimmer aber auf keinen Fall mehr.

  Da ein alter WLAN-Router übrig war, musste kein WLAN Access Point gekauft werden. Die beiden WLAN-Router lassen sich einfach über die Ports ihrer Switches verbinden.

  Außer den **weiteren Smarthome-Komponenten* ist noch ein** Saugroboter vorhanden.



Sicherheitslücken

„**Massiver DDoS auf weite Teile des Internets**“ – Dienste wie Twitter, Netflix, Spotify und PayPal waren teilweise nicht erreichbar. Grund war ein Distributed-Denial-of-Service-Angriff mit Hilfe des Mirai-Botnetzes, „das zum großen Teil aus gehackten Geräten aus dem Internet der Dinge (IoT) wie Kameras und smarten Haushaltsgeräten besteht.“ (c’t 2016, Heft 23, S. 39)

6. Mit Hilfe gekaperter Geräte werden **Botnetze** aufgebaut. Diese können für **DDoS-Angriffe** genutzt werden („Distributed Denial of Service“; dt. „Verbreitete Verweigerung des Dienstes“).
   Dabei werden Datennetze durch Überlastung lahmgelegt. Die arglosen Nutzer, deren Geräte für das Botnetz missbraucht werden, ahnen nichts davon, dass sie an einer kriminellen Aktion beteiligt sind. Auch zurückverfolgen lassen sich die Angriffe praktisch nicht.
   Oft entsteht der Schaden schon durch den Ausfall des Netzes. Ein DDoS-Angriff kann aber auch als Ablenkungsmanöver genutzt werden, um über einen anderen Weg in fremde Netze einzudringen.

   Welches Interesse könnte an DDoS-Angriffen bestehen?

   - Terroristen:
   - Staaten:
   - Kriminelle:

➢ **Wir sind auch für das verantwortlich, was wir nicht tun!** Wer sich nicht um die Sicherheit seiner IT-Ausstattung kümmert, schadet potentiell nicht nur sich selbst, sondern auch der Allgemeinheit. Deshalb wurden im IT-Unterricht bereits Maßnahmen in Bezug auf Datenschutz und Datensicherheit besprochen (vgl. Lerninhalte 1.4–05 *Risiken bei der Nutzung digitaler Kommunikationsformen* sowie 1.8–04 *Datensicherheit*).
Hier lernst du zunächst weitere Beispiele für Risiken beim Umgang mit Datennetzen kennen.
Später werden Maßnahmen zur Konfiguration von Datennetzen besprochen, mit denen die Risiken vermindert werden können.

7. Das Internet der Dinge umfasst keineswegs nur Geräte in Privathaushalten. Durch Fernzugriff lässt sich viel Geld und Energie sparen sowie auch die Lebensumstände von Menschen verbessern, z. B. in der Gesundheitsversorgung. Das betrifft beispielsweise:

   - Industrieanlagen
   - Energieversorgungsnetze und auch einzelne Kraftwerke
   - Heizungsanlagen
   - Beleuchtungssteuerung
   - Medizinische Geräte

   „Kirchenglocken kann jedermann per Mausklick läuten. Einbrecher kapern Autos, sie knacken Safes mit USB-Sticks; der DSL-Router mutiert zur Angriffswaffe und der Fernseher spioniert bereits ab Werk. Dystopie? Keineswegs! Von der Webcam bis zur Infusionspumpe: Ohne Firmware geht nichts mehr. Mit zunehmender Vernetzung steigen Risiko und Verantwortung.“ (c’t 2015, Heft 21, S. 80)

   - Beschreibe das grundsätzliche Problem bei der Verwendung vernetzter Geräte.

   Auf den folgenden Seiten lernst du ein paar Beispiele dazu genauer kennen.

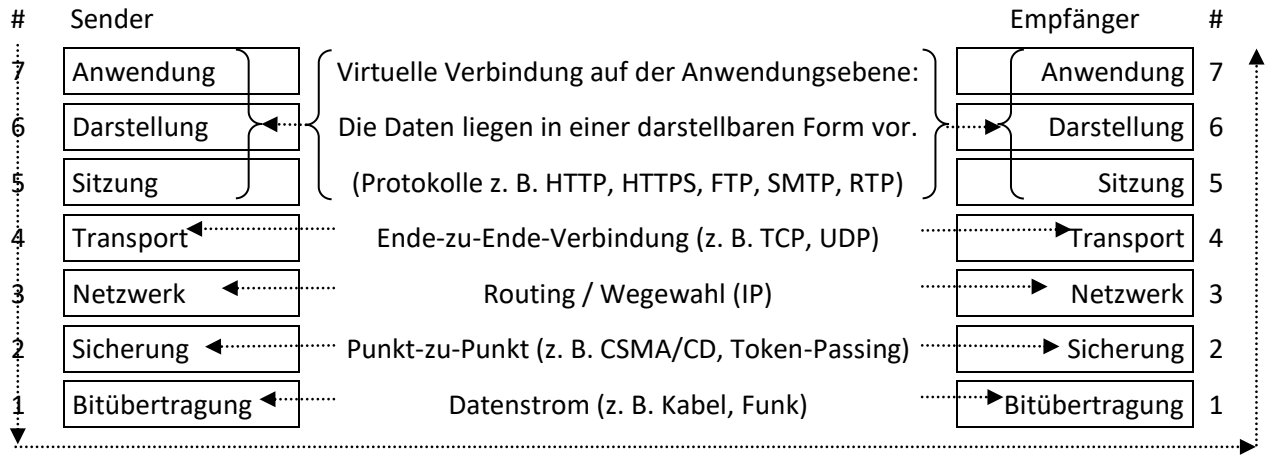
Ports

8. Angriffsziel Router von Kunden der Telekom:

> Ende November 2016 fiel für etwa 900.000 Bundesbürger der Internetzugang und das Telefonnetz aus. Grund war ein Mirai-ähnlicher Wurm, der verschiedene WLAN-Router der Telekom über eine Sicherheitslücke lahmlegte. Die Lücke war der TCP-Port 7547, der es ermöglichte, bei den Routern anzuklopfen, um z. B. ein Softwareupdate zu veranlassen.

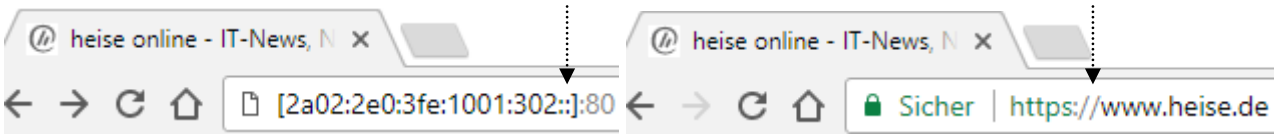
Du kennst die Darstellung des OSI-Modells bereits aus dem vorigen Arbeitsblatt:

- Auf der OSI-Schicht 4 wird der Transport von Daten gewährleistet.
- Für die Anwendungsebene muss aber darüber hinaus bekanntgegeben werden, wie mit diesen Daten umzugehen ist – also welches Protokoll verwendet wird.

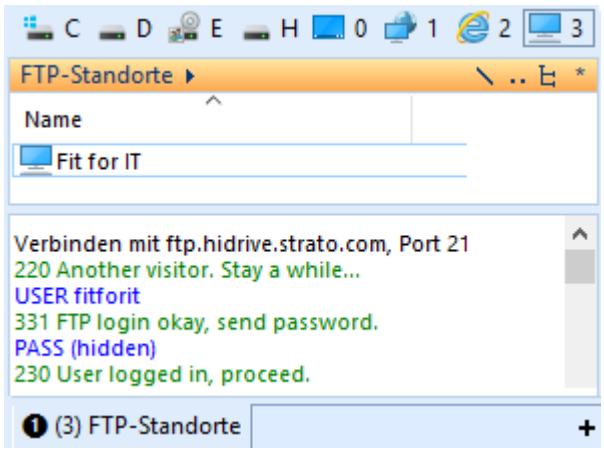


- Die Information, welches Protokoll auf der Anwendungsebene zu verwenden ist, wird mit einer **Portnummer** im Zusammenhang mit der IP-Adresse übermittelt:

Der **Port** ist dem TCP-Protokoll zuzuordnen, also der Schicht 4 des OSI-Modells. Die Portnummer wird mit einem Doppelpunkt abgetrennt an die IP-Adresse angehängt.
Eine IP-Adresse (IPv6) könnte vollständig z. B. so aussehen und zu dem Internetauftritt rechts führen:



Es gibt Standardports für unterschiedliche Protokolle, z. B. für **FTP** ist der Standardport **21**.
Die meisten FTP-Zugriffe sind passwortgeschützt.
Für diese Anwendung ist ein FTP-Client erforderlich.
Die Oberfläche sieht ähnlich aus wie im lokalen Dateisystem – mit dem Unterschied, dass die Dateien hier auf einem entfernten Rechner liegen und über das Internet zugegriffen wird.



Weiter Beispiele für Standardports:
25: **SMTP** (E-Mail-Versand)
80: **HTTP** (Webserver)
110: POP3 (Client-Zugriff auf E-Mail-Server)
443 HTTPS (sicherer Webserver)

- Ein Angriffsziel ist das Port-Forwarding: Für Geräte, die von außen erreichbar sein müssen, werden am Router Port-Weiterleitungen eingerichtet. Dabei leitet der Router Datenpakete, die über einen bestimmten Port eintreffen, an ein zuvor festgelegtes Gerät im Lokalen Netz weiter.

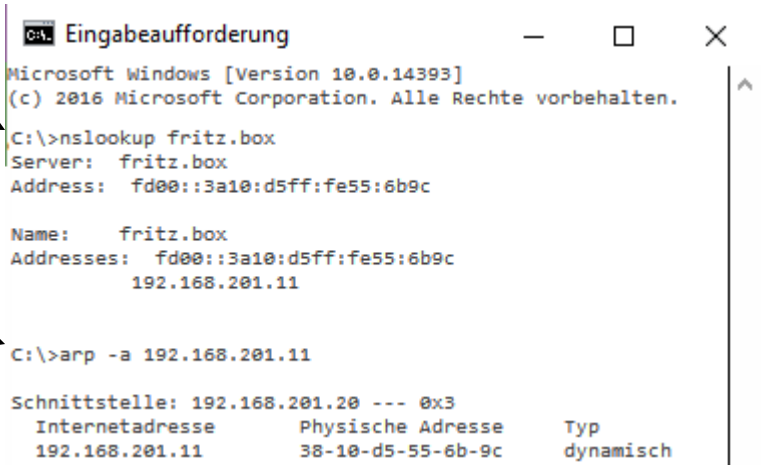
WLAN-Router

9. WLAN-Router lassen sich teilweise mit einfachen Mitteln attackieren. Das kann hier anhand eines Beispiel wird nachvollzogen werden. Eventuell ist an der Schule auch ein „Spielrouter“ verfügbar:

   - Wenn man, wie auch von Servicetechnikern empfohlen, den WPA2-Schlüssel nicht ändert, kann der ab Werk eingestellte Schlüssel oft berechnet werden, weil die Algorithmen dafür bekannt sind oder sich herausfinden lassen. Man benötigt lediglich die MAC-Adresse.

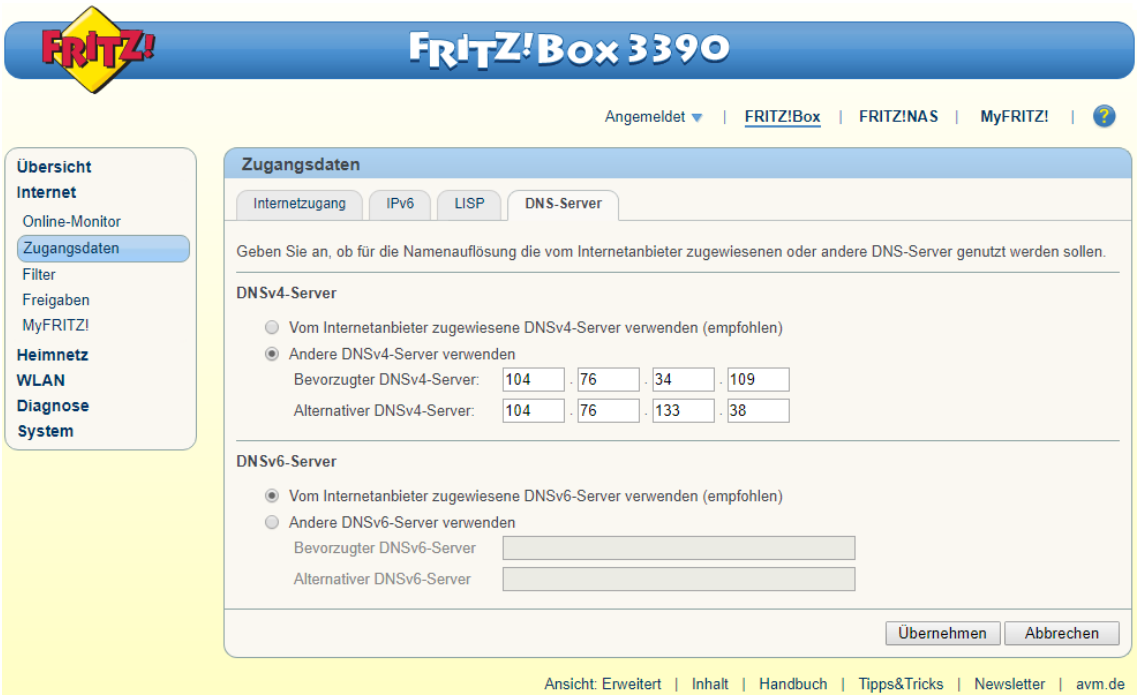
     Erster Schritt: Die IP-Adresse des Routers ermitteln. Wenn man die IP-Adresse schon kennt, weil sie auf der Einstellung ab Werk belassen wurde, kann man sich diesen Schritt sparen.

     Zweiter Schritt: Die MAC-Adesse wird mit dem Kommando `arp` zurückgegeben.



   - WLAN-Router werden tatsächlich manchmal mit der Kombination Benutzername „admin“ und Kennwort „admin“ ausgeliefert! Wenn hier der Benutzer nichts geändert hat, kann der Router leicht übernommen werden. Ansonsten gibt es Tools zu kaufen, die das Kennwort knacken. Man kann beispielsweise den Datenverkehr in einem lokalen Netz belauschen und Datenpakete gezielt abfangen – auch verschlüsselte HTTPS-Verbindungen. Damit lassen sich Benutzernamen und Passwörter ermitteln, aber auch VoIP-Gespräche belauschen.

   - Was dann? – Beispielsweise kann ein Krimineller einen anderen DNS-Server eintragen:



Danach hat der Angreifer leichtes Spiel: Nach Eingabe einer Internetadresse wird die IP-Adresse eines gefälschten Internetauftritts auf einem anderen Server aufgerufen. Der Benutzer bemerkt davon nichts.