**Netzwerk- & Kommunikationstechnik**

[Netzwerke 3](#_Toc499023030)

[IP-Adresse 3](#_Toc499023031)

[Domain 3](#_Toc499023032)

[Subnetmask: 3](#_Toc499023033)

[MAC-Adresse: 3](#_Toc499023034)

[DHCP 4](#_Toc499023035)

[Firewall 4](#_Toc499023036)

[Domain Name System (DNS): 4](#_Toc499023037)

[Proxy 4](#_Toc499023038)

[Switch 4](#_Toc499023039)

[Router 5](#_Toc499023040)

[Hub: 5](#_Toc499023041)

[Network Address Translation (NAT) 5](#_Toc499023042)

[Netzklassen: 5](#_Toc499023043)

[Datenpaket 5](#_Toc499023044)

[Transmission Control Protocol (TCP): 5](#_Toc499023045)

[User Datagram Protocol (UDP): 6](#_Toc499023046)

[Port 6](#_Toc499023047)

[OSI-Modell: 6](#_Toc499023048)

[Fernzugriff 7](#_Toc499023049)

[Was ist ein Fernzugriffsprogramm? 7](#_Toc499023050)

[RemoteDesktop 7](#_Toc499023051)

[TeamViewer 7](#_Toc499023052)

[Wake on LAN (WoL): 7](#_Toc499023053)

[WoL + RemoteDesktop: 8](#_Toc499023054)

[TeamViewer-Screenshots: 9](#_Toc499023055)

[RemoteDesktop-Screenshots: 10](#_Toc499023056)

[WoL-Screenshots: 11](#_Toc499023057)

[Android Apps erstellen mit dem MIT App Inventor 12](#_Toc499023058)

[Was ist der MIT App Inventor? 12](#_Toc499023059)

[Beispiel: Sprachgesteuerter Musik-Player 12](#_Toc499023060)

[12](#_Toc499023061)

[Arduino Bluetooth apps 13](#_Toc499023062)

[Bluetooth Module 13](#_Toc499023063)

[Software Serial 13](#_Toc499023064)

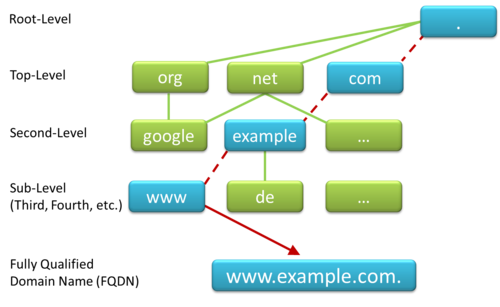
[Quellen 14](#_Toc499023065)

**Netzwerke**

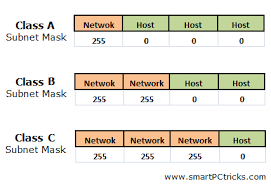
IP-Adresse**:**

* Wird in jeglichen Computernetzen (mit IP Protokoll) als Adresse für Netzgeräte verwendet
* Ist global einzigartig, wobei 32-stellige IPv4, 128-stellige IPv6 Adressen existieren
* Lokal kann eine IP-Adresse je nach Subnetmask spezifiziert werden. Dank des NAT müssen lokale IP-Adressen nicht global einzigartig sein
* Alle Datenpakete werden mit einer IP-Adresse versehen, die den Empfänger identifiziert

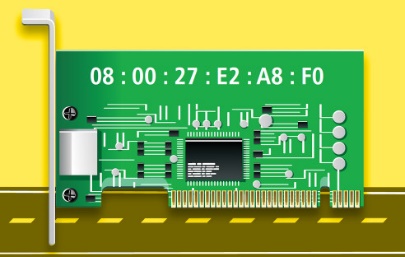
Domain**:**

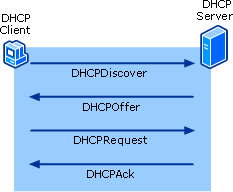
* Meist die lesbare Adresse eines Webservers
* Wie die IP-Adresse ist auch jede Domain weltweit einmalig
* Sie besteht aus unterschiedlichen Teilen:
  + Top-Level-Domain:
    - Die letzte Stelle in der Domain, meist international „.com“ oder „.org“ oder landesspezifisch „.at“ oder „.en“.
  + Second-Level / Hostnamen:
    - Hier wird die Second-Level Domain wie „.co“ spezifiziert
    - Viele Domains haben auch hier schon ihren Hostnamen (zB. „google“)
  + Third-Level:
    - Labels wie „www.“ bzw. Subdomains

Subnetmask:

* Wird auch Netzmaske genannt
* In Verbindung mit der IP-Adresse eines Gerätes legt die Subnetmask fest, welche IP-Adressen dieses Gerät im eigenen Netz ohne die Zuhilfenahme eines Routers erreichen kann und für welche Ziel-Netze das Gerät Pakete an einen Router zwecks weiterer Vermittlung in andere Netze zustellen muss.
* Der Netzwerkteil ist bei allen Geräten des jeweiligen Netzes gleich
* Alle Kommunikationsteilnehmer dieses IP-Netzes verwenden dieselbe Subnetzmaske
* Der Geräteteil der IP-Adresse wird für jedes Gerät innerhalb des Netzes individuell vergeben

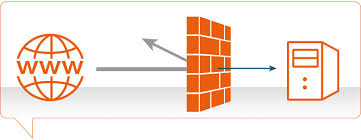
MAC-Adresse:

* Media-Access-Control-Adresse
* Hardware-Adresse eines Netzwerkadapters
* Bei IPv4 (Ethernet-Netze) besteht die MAC-Adresse aus 48 Bit (sechs Bytes). Die Adressen werden hexadezimal geschrieben.
* Eine MAC-Adresse kann global oder lokal registriert ist (0 = Universal, 1 = Lokal)
* Obwohl eine MAC-Adresse in erster Linie zur Identifikation und damit zur Sicherheit dient, kann sie recht einfach vorgetäuscht (Spoofing) werden.

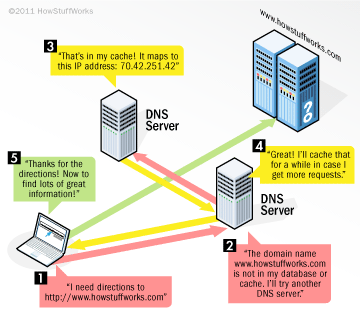
DHCP**:**

* Kommunikationsprotokoll (Hintergrunddienst)
* Zur Einbindung noch nicht identifizierter Clients ins Netzwerk
* Wenn mit Netzwerk verbunden, „fragt“ der Client nach dem DHCP Server. Dieser Identifiziert den Client mit dessen MAC-Adresse und weist ihm eine IP zu.
* Es gibt die automatische, manuelle (statische) und dynamische Zuordnung in einem vordefinierten IP-Bereich

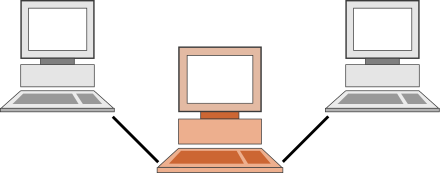
Firewall**:**

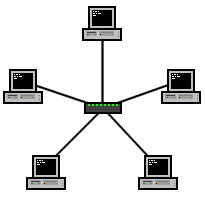
* Sicherungssystem
* Schützt vor unerwünschten Netzwerkzugriffen
* Anhand festgelegter Regeln wird der Datenverkehr überwacht und beschränkt
* Bestimmte Ports werden in verschiedene Richtungen eingeschränkt
* „Intelligente“ Firewalls beschränken den Internetzugriff auch je nach Programm bzw. dessen Signatur

Domain Name System (DNS):

* Das DNS liefert dem Client die IP-Adressen der angefragten Domains
* Ein DNS kann sowohl im lokalen Netz als auch extern sein, viele Firmen und Internetanbieter verwenden interne DNS, um bestimmte Websites zu sperren
* IP-Adressen und Domains von Webservern können relativ einfach und unkompliziert geändert werden

Proxy**:**

* Ein „Vermittler“ in Netzwerken
* Ein Proxy befindet sich zwischen zwei Netzgeräten, um die jeweiligen Anfragen über seine eigene Adresse weiterzuleiten.
* Mithilfe eines Proxys kann man unter anderem oft heruntergeladene Dateien speichern, was in großen Netzwerken zu einer erheblichen Entlastung der Bandbreite führen kann.
* Auch Internetanbieter verwenden Proxys um Bandbreite zu sparen

Switch**:**

* Verbindet Netzwerksegmente
* Leitet Datenpakete weiter
* Im Gegensatz zum Repeater-Hub kommen die Datenpakete tatsächlich nur am Ziel an und werden nicht an jeden Netzwerkteilnehmer gesendet

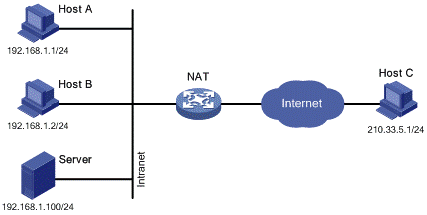
Router**:**

* Netzwerkgeräte, die Datenpakete zwischen Rechnernetzen weiterleiten
* Oft dienen sie zur Internetanbindung oder Kopplung diverser Netzwerke
* Da viele Heimrouter (portable) Netzwerk-Alleskönner sind, also Switches, Umwandler bzw. SIM-Card-Slots, USB, WLAN usw. integriert sind, können sie für das schnelle Set-Up von (drahtlosen) lokalen Netzwerken, FTP bzw. Samba Servern usw. genutzt werden.

Hub:

* Schneller als ein Switch, da die Datenpakete nicht eingelesen werden müssen
* Unsicher, da alle Datenpakete an alle Clients gesendet werden

Network Address Translation (NAT)**:**

* Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden
* Kommt auf Routern zum Einsatz
* Mithilfe eines NAT kann man lokale IPv4-Adressen erstellen, die nur für das jeweilige Netzwerk gelten
* NAT entstand als Lösung für die Knappheit öffentlicher IPv4-Adressen

Netzklassen:

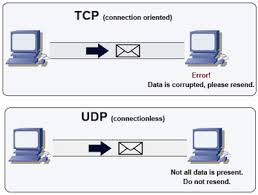
* Netzklassen sind eine Unterteilung des IPv4-Adressbereichs in Teilnetze.
* Sie wurden von 1981 bis 1993 verwendet.
* Es gibt 5 verschiedene Netzklassen (A … E), die mithilfe der Subnetmask zu bestimmen sind

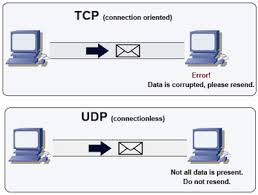


Datenpaket**:**

* ****Beinhaltet Information, die von einem Netzwerkgerät zum Nächsten geschickt wird
* Normalerweise ist jedes Datenpaket mit einer eindeutigen (IP-)Adresse versehen, an die es vom Switch gesendet wird.

Transmission Control Protocol **(TCP):**

* Definiert, wie Daten ausgetauscht werden sollen
* [Verbindungsorientiert](https://de.wikipedia.org/wiki/Nachrichtenverbindung) und [paketvermittelnd](https://de.wikipedia.org/wiki/Paketvermittlung)
* Erste Standardisierung 1981
* Verbindung zwischen zwei Endpunkten eines Sockets in beide Richtungen
* Automatische Erkennung/Behebung von Datenverlusten

**User Datagram Protocol (UDP):**

* Definiert, wie Daten ausgetauscht werden sollen
* Minimal und verbindungslos
* Entwicklung 1977
* Auf Schnelligkeit ausgelegt; Keine Sicherung bei der Datenübertragung; ungeschützt
* Paket kann mehrmals, in falscher Reihenfolge oder gar nicht ankommen, aber die Übertragungsgeschwindigkeit ist höher
* Variation: UDP Lite

Port**:**

* Teil einer Netzwerk-Adresse
* Kann nicht zwei Mal gleichzeitig benutzt werden
* Es gibt well-known und freie Ports, die von Entwicklern für ihre Software genutzt werden kann
* Auf der Website <https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports> findet man eine detaillierte Zuordnung von TCP/UDP-Ports zu Protokollen

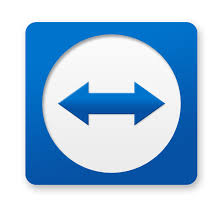
OSI-Modell:

* Netzwerkmodell
* Basis für viele Netzprotokolle
* Ermöglicht Kommunikation über unterschiedliche Systeme hinweg
* Besteht aus sieben Schichten
  + **7. Schicht / Anwendung:**   
    Funktionen für Anwendungen, sowie die Dateneingabe und -ausgabe.
  + **6. Schicht / Darstellung:**   
    Umwandlung der systemabhängigen Daten in ein unabhängiges Format.
  + **5. Schicht / Sitzung:**   
    Steuerung der Verbindungen und des Datenaustauschs.
  + **4. Schicht / Transport:**   
    Zuordnung der Datenpakete zu einer Anwendung.
  + **3. Schicht / Vermittlung:**   
    Routing der Datenpakete zum nächsten Knoten.
  + **2. Schicht / Sicherung:**   
    Segmentierung der Pakete in Frames und Hinzufügen von Prüfsummen.
  + **1. Schicht / Bitübertragung:**   
    Umwandlung der Bits in ein zum Medium passendes Signal und physikalische Übertragung.

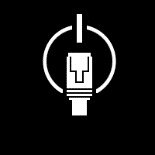
Fernzugriff

Was ist ein Fernzugriffsprogramm?  
Fernzugriffsprogramme sind Anwendungen, die es dem User erlauben, auf andere Computer zuzugreifen.  
Solange das Fernzugriffsprogramm auf dem Computer eingerichtet ist, muss der User keinen physischen Zugang zu dem Gerät haben. Auch muss kein Bildschirm oder jegliche Peripherie angeschlossen sein.  
  
Diese Möglichkeiten machen Fernzugriffsprogramme zu einem sehr wichtigen Werkzeug für Admins und Entwickler zur Lösung von Problemen (Fernwartung).  
Sobald eine Remote-Verbindung initialisiert wurde, überträgt das Programm, auf beiden PCs aktiviert sein muss, Tastatureingaben und Mausevents (Koordinaten des Cursors, Clicks) zwischen den Geräten.  
  
Der aktuelle Bildschirm wird, um jegliche Latenz zu minimieren, stark komprimiert, auf den zugreifenden PC gestreamt. Die Auflösung spielt hierbei eine wesentliche Rolle.  
Oft laufen Fernzugriffsprogramme als Dienste im Hintergrund, um so ohne Anmeldung sofort auf Zugriffsanfragen reagieren zu können. In Verbindung mit Wake on LAN kann dies zu einer effizienten Wartung ganzer Computernetzwerke dienen.

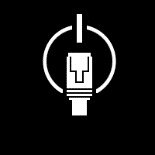
RemoteDesktop**:**RemoteDesktop ist ein simples, in Windows integriertes Programm für Fernzugriff auf den PC. Da das Programm ein fixer Bestandteil des Betriebssystems ist, läuft es sehr stabil und kann ohne Einrichtung sofort verwendet werden.

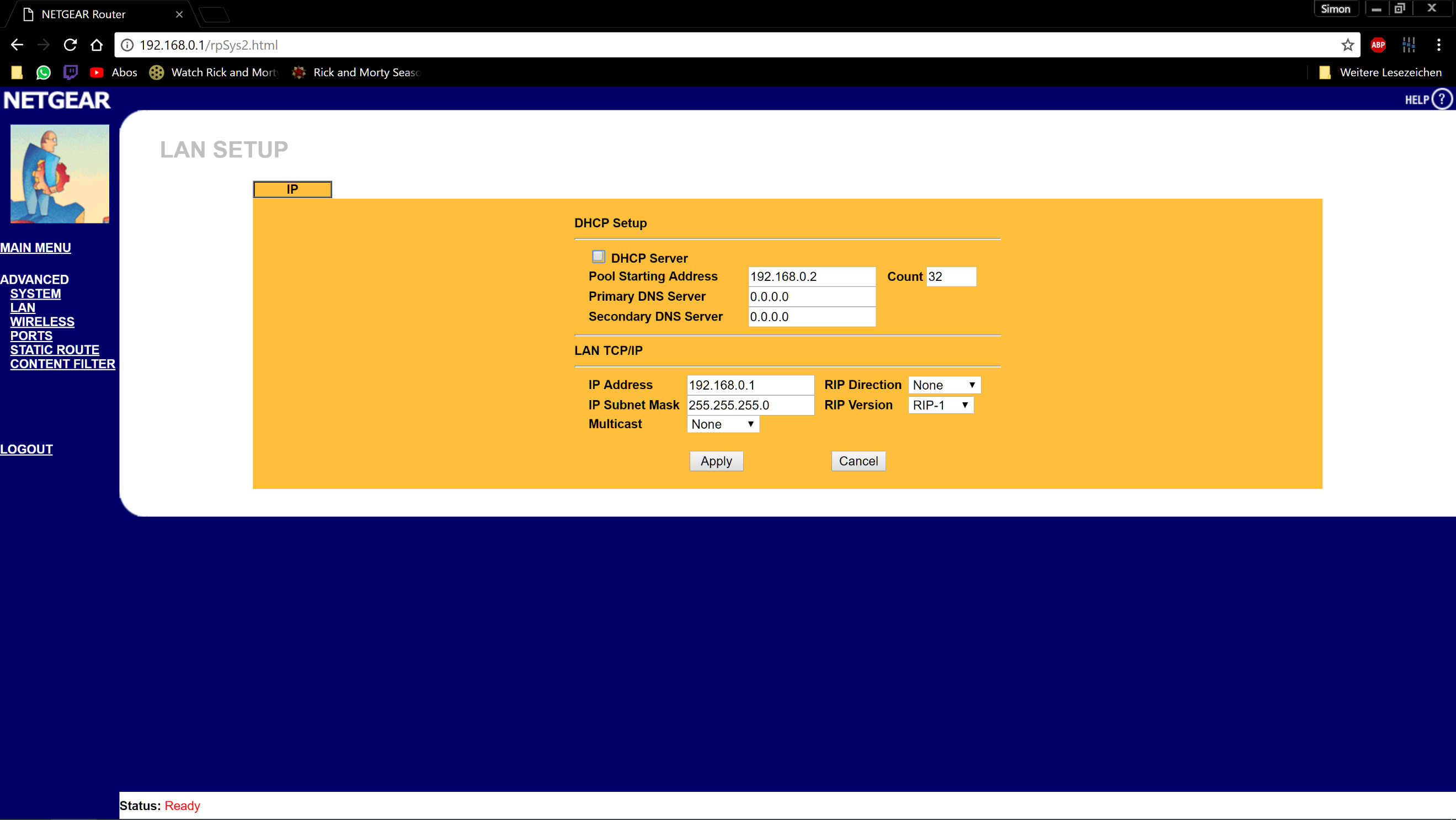
TeamViewer**:**Im Gegensatz zu RemoteDesktop ist TeamViewer ein sogenannte „3rd Party“-Programm, d.h. es muss zuerst installiert und eingerichtet werden.  
TeamViewer ergänzt das Prinzip von RemoteDesktop um viele nützliche Features wie das automatische Verbinden der PCs, einen Whiteboard-Modus, Video- und Audioanrufe und vieles mehr. Außerdem funktionieren Zugriffe unabhängig vom Betriebssystem, was unter anderem die Übertragung auf/von ein/einem Smartphone ermöglicht.  
Auch Bildschirmaufzeichnungen, die, in verschiedenen Formaten und Kompressionsraten, zum späteren erneuten Ansehen der Session gespeichert werden können, sind möglich. Dabei ist die Ausgangsdatei üblicherweise sehr klein.  
Insbesondere im unbeaufsichtigten Modus, in dem das System ohne Bestätigung seitens des PCs, auf den zugegriffen wird, uneingeschränkt kontrolliert werden kann, muss besonderer Wert auf Sicherheit gelegt werden.  
TeamViewer verwendet daher ein ID und Passwort-System, wobei sich das Passwort, sofern nicht anders festgelegt, nach jeder Session ändert, die User-ID aber gleich bleibt. Zudem wird das Hintergrundbild des Users aus Datenschutzgründen temporär ausgeblendet.

Wake on LAN (WoL):

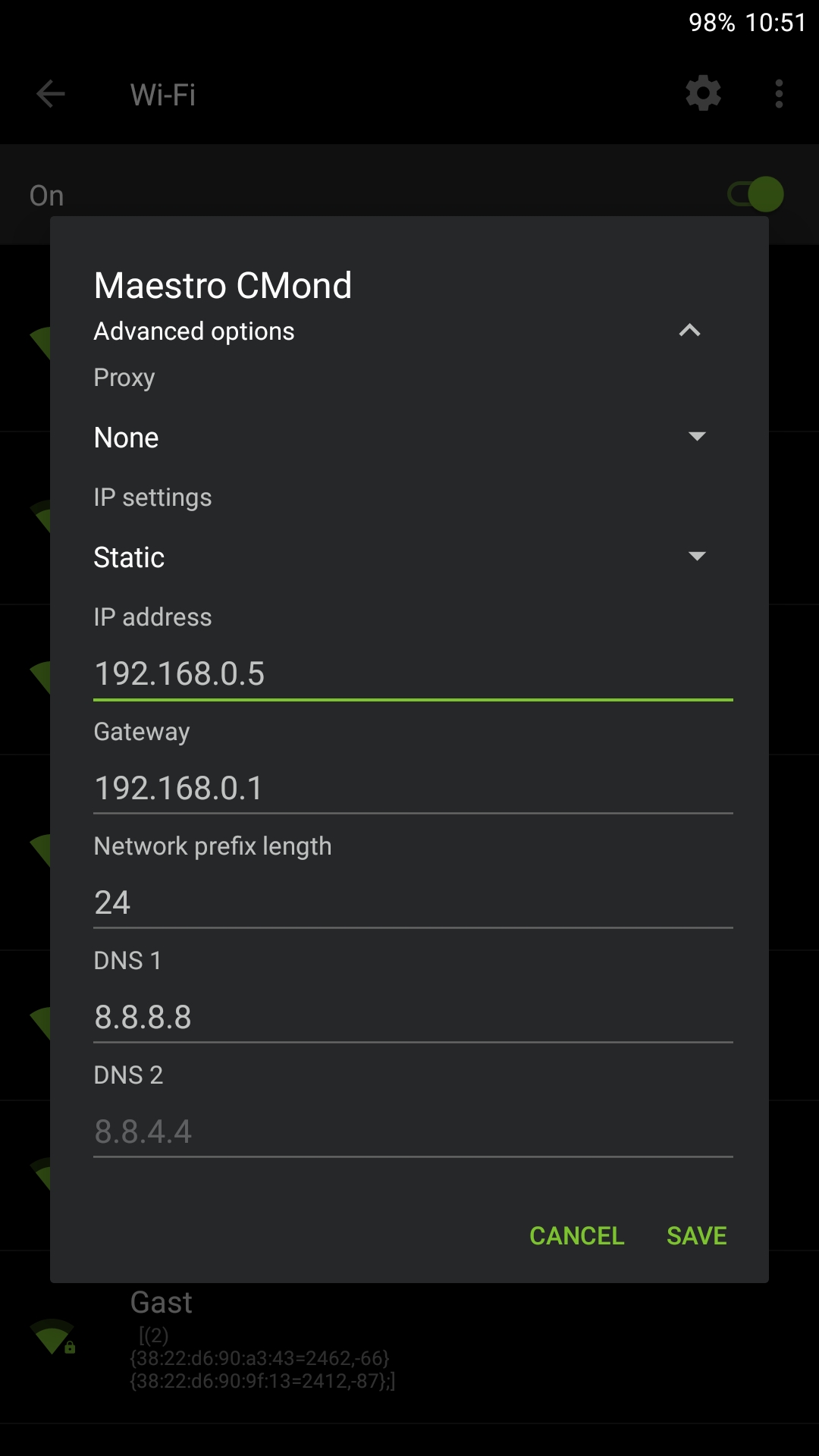
Wake on LAN ist ein 1995 von AMD und HP entwickelter Standard, um Computer per Netzwerkschnittstelle hochzufahren bzw. aus dem Ruhezustand zu holen, indem ein sogenanntes „Magic Packet“ an den PC gesendet wird. Die Ansteuerung des PCs erfolgt hierbei über dessen MAC-Adresse.  
  
Um WoL benutzen zu können, muss es auf den meisten Geräten zuerst im BIOS und auch im Betriebssystem (Netzwerkeinstellungen) aktiviert werden.

WoL + RemoteDesktop:

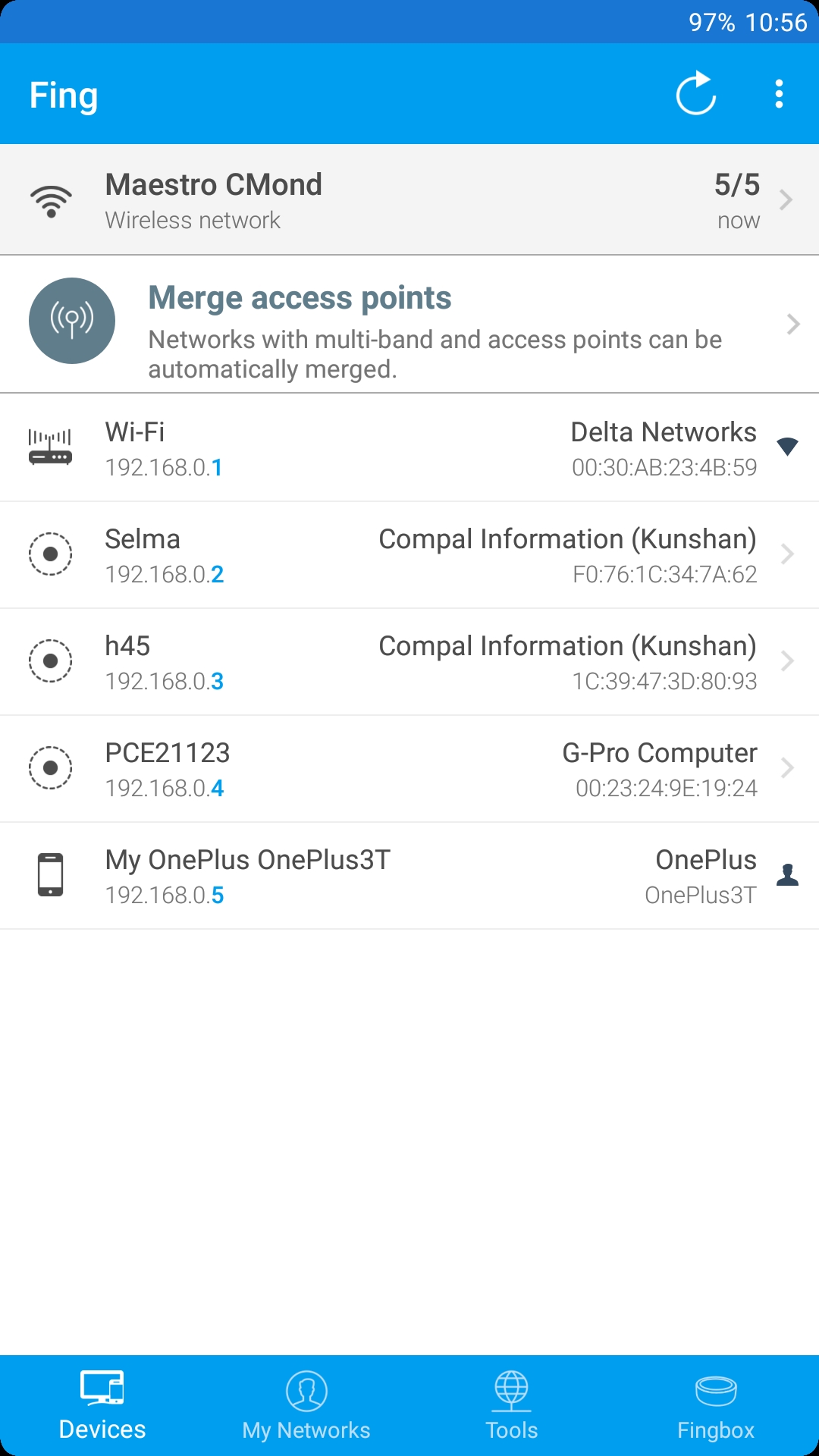
Eine Kombination mit Wake on LAN und RemoteDesktop kann eine einfache Kontrolle eines ausgeschalteten PCs ermöglichen. Zuerst wird das Gerät mit WoL hochgefaren, anschließend kann man sich per RemoteDesktop einloggen und auf das System zugreifen.  
Ein Router, der als kabelloser Access-Point dient, wird für den unkomplizierten Fernzugriff mit Geräten wie einem Smartphone empfohlen.  
Es folgen Screenshots vom Setup des Zugangs zum PC, ohne mit diesem PC physisch zu interagieren:



Einstellung / Setup Router  
DHCP wird deaktiviert



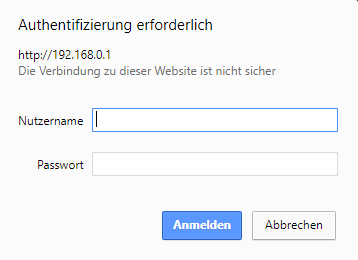
Verbindung zum WLAN  
Auswahl der IP-Adresse



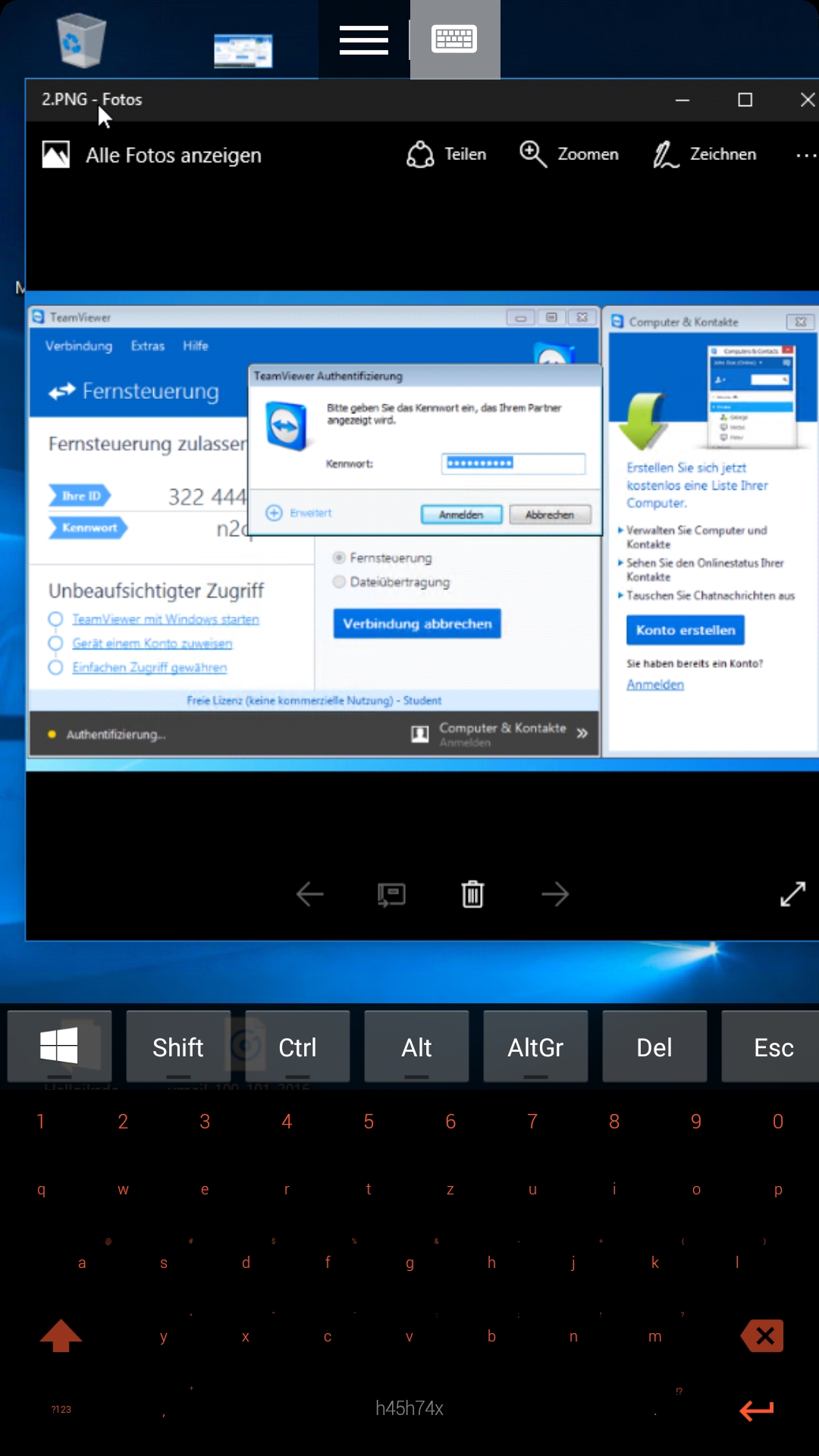
Netzwerkscan im WLAN



WoL-App

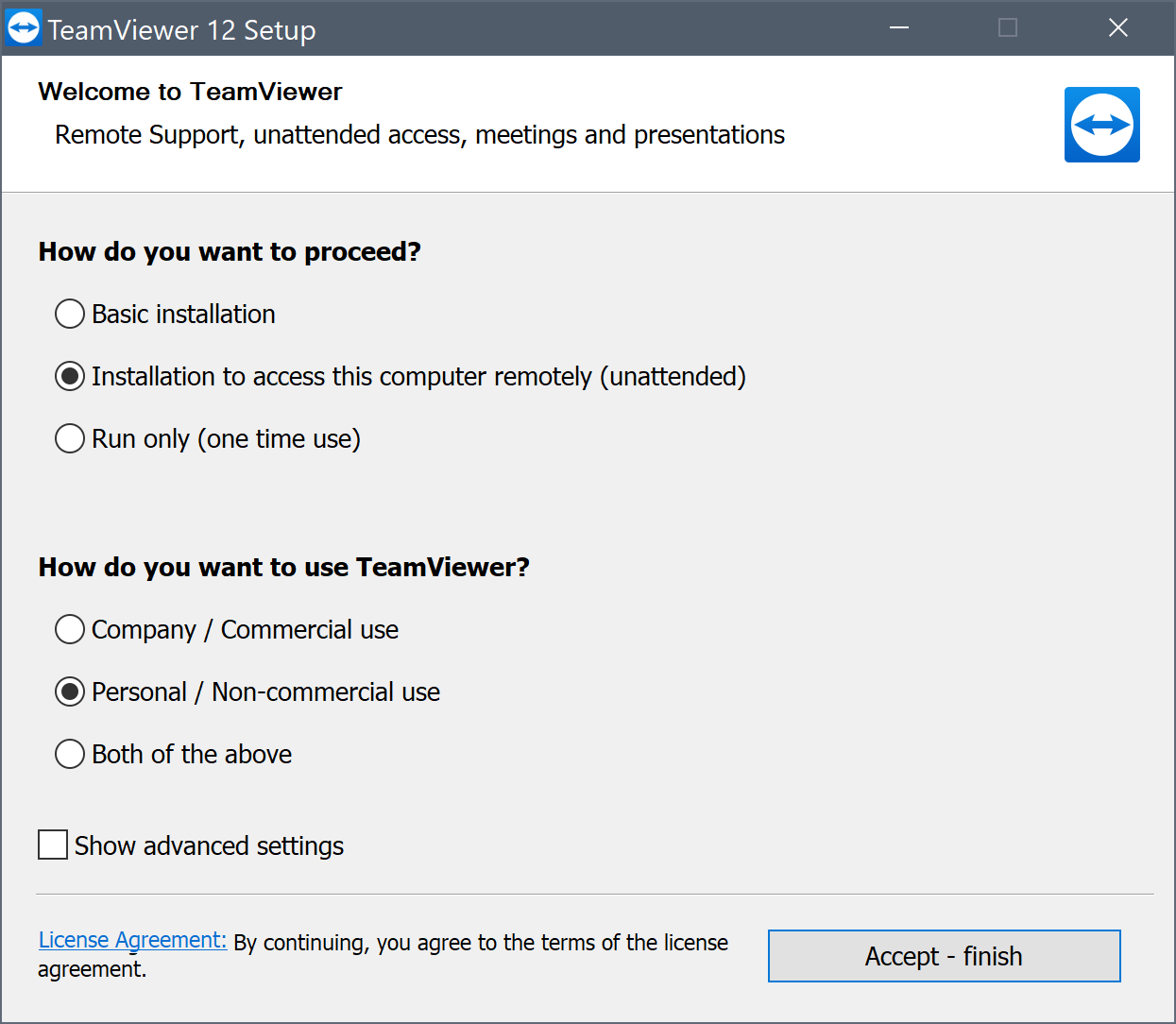


Anmeldung im Webinterface  
auf der Standard-IP des Routers

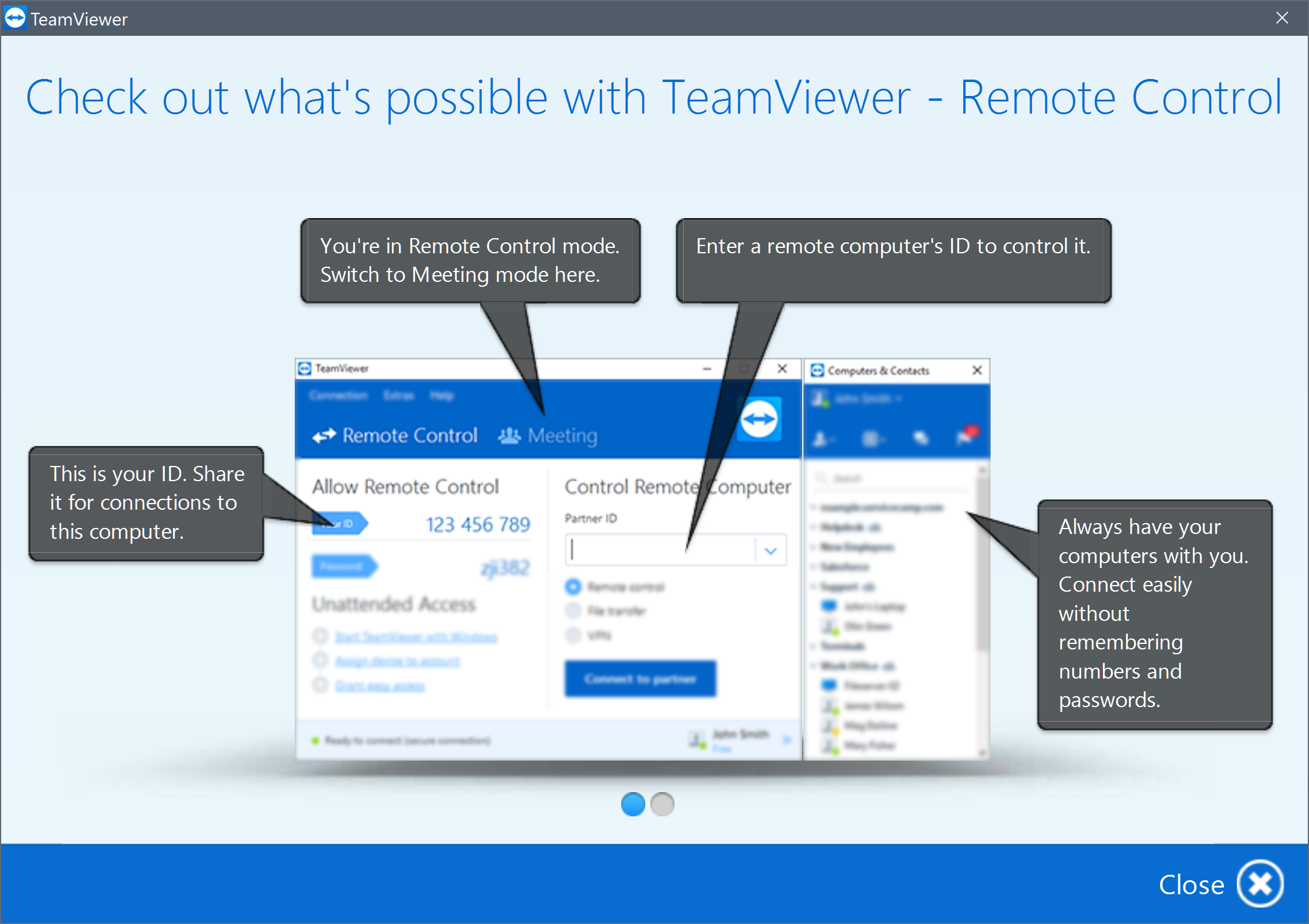


RemoteDesktop-Sitzung am durch WoL hochgefahrenen PC

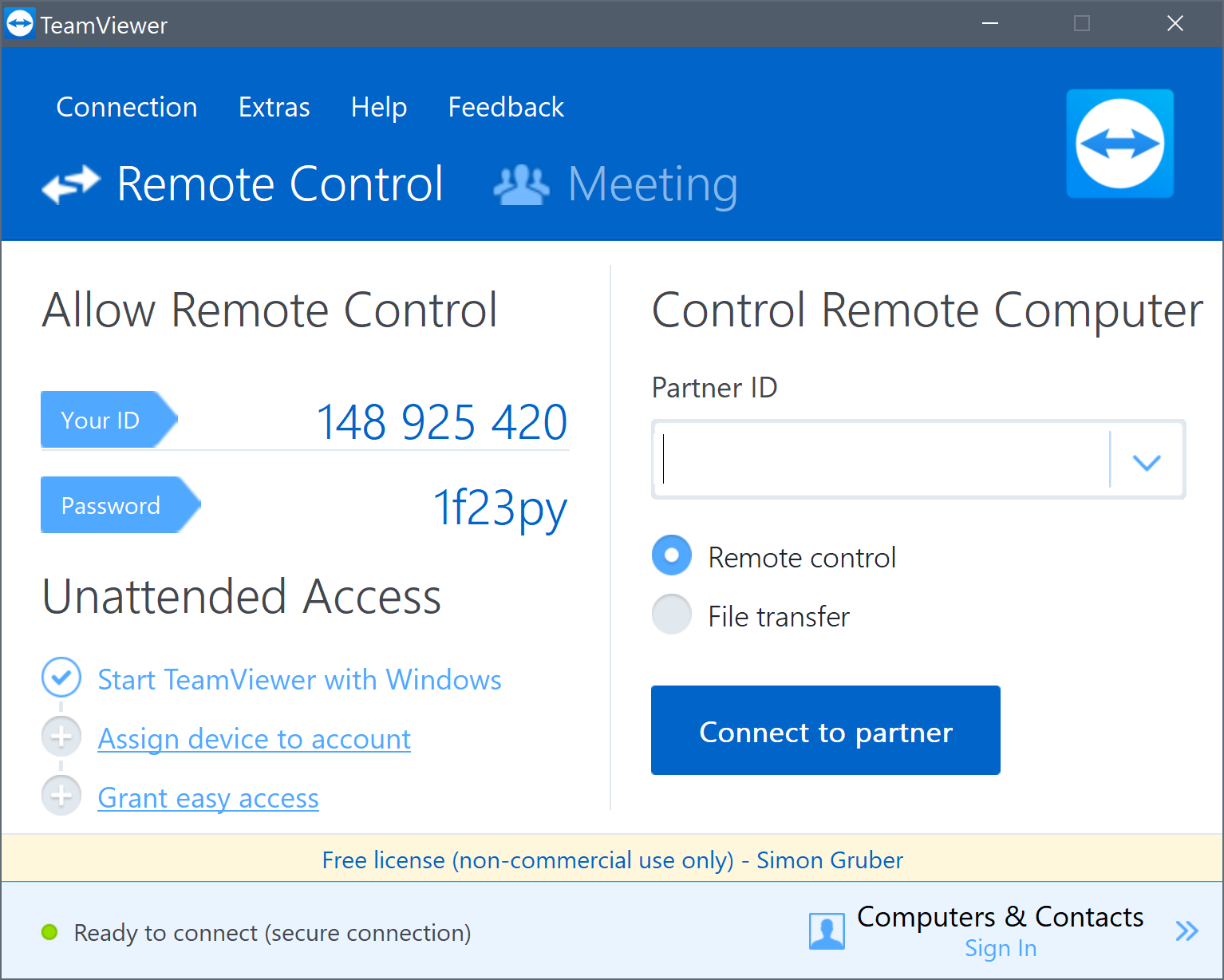
TeamViewer-Screenshots:



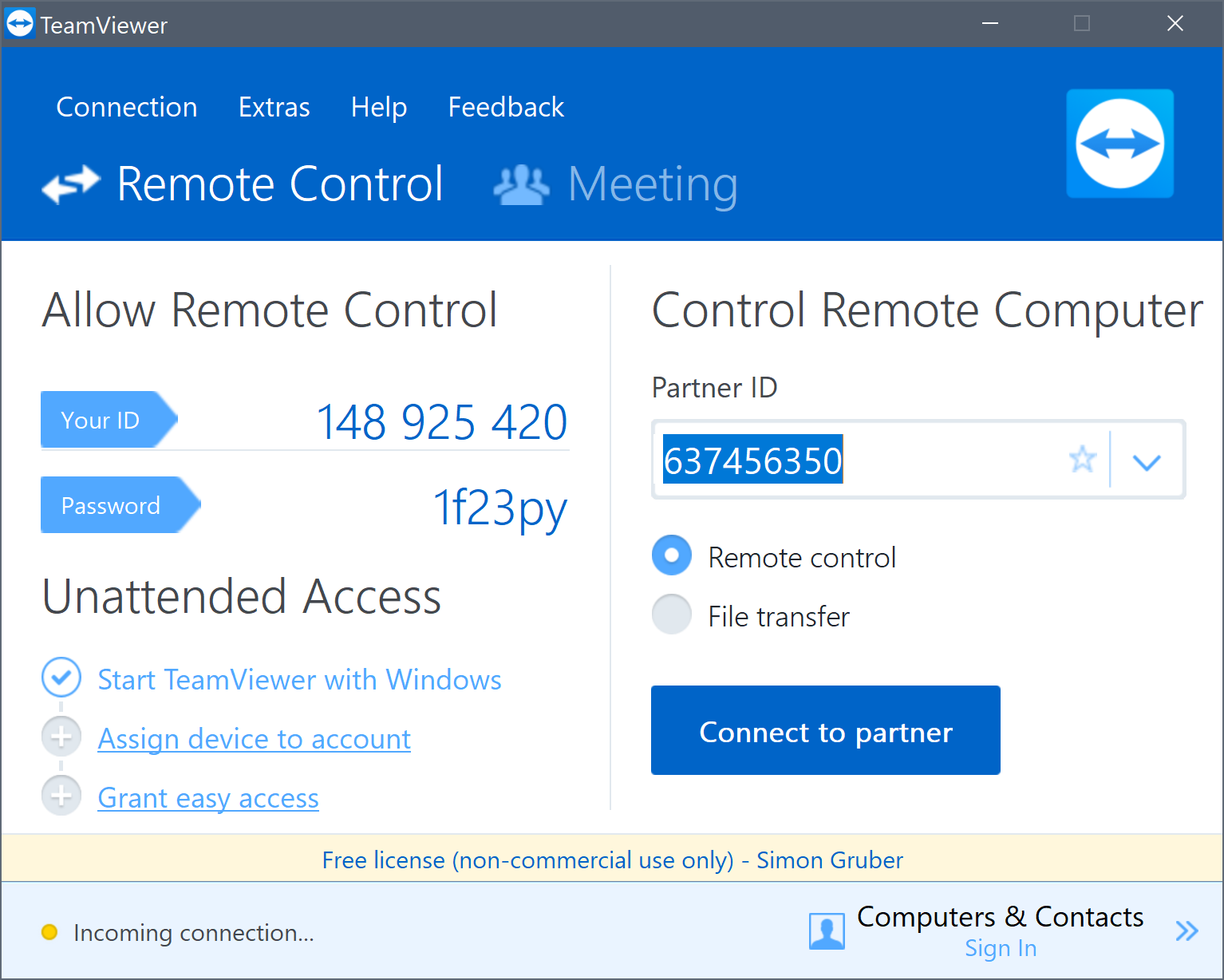
Einstellung / Setup



Erklärungsbildschirm während der Installation



Hauptbildschirm



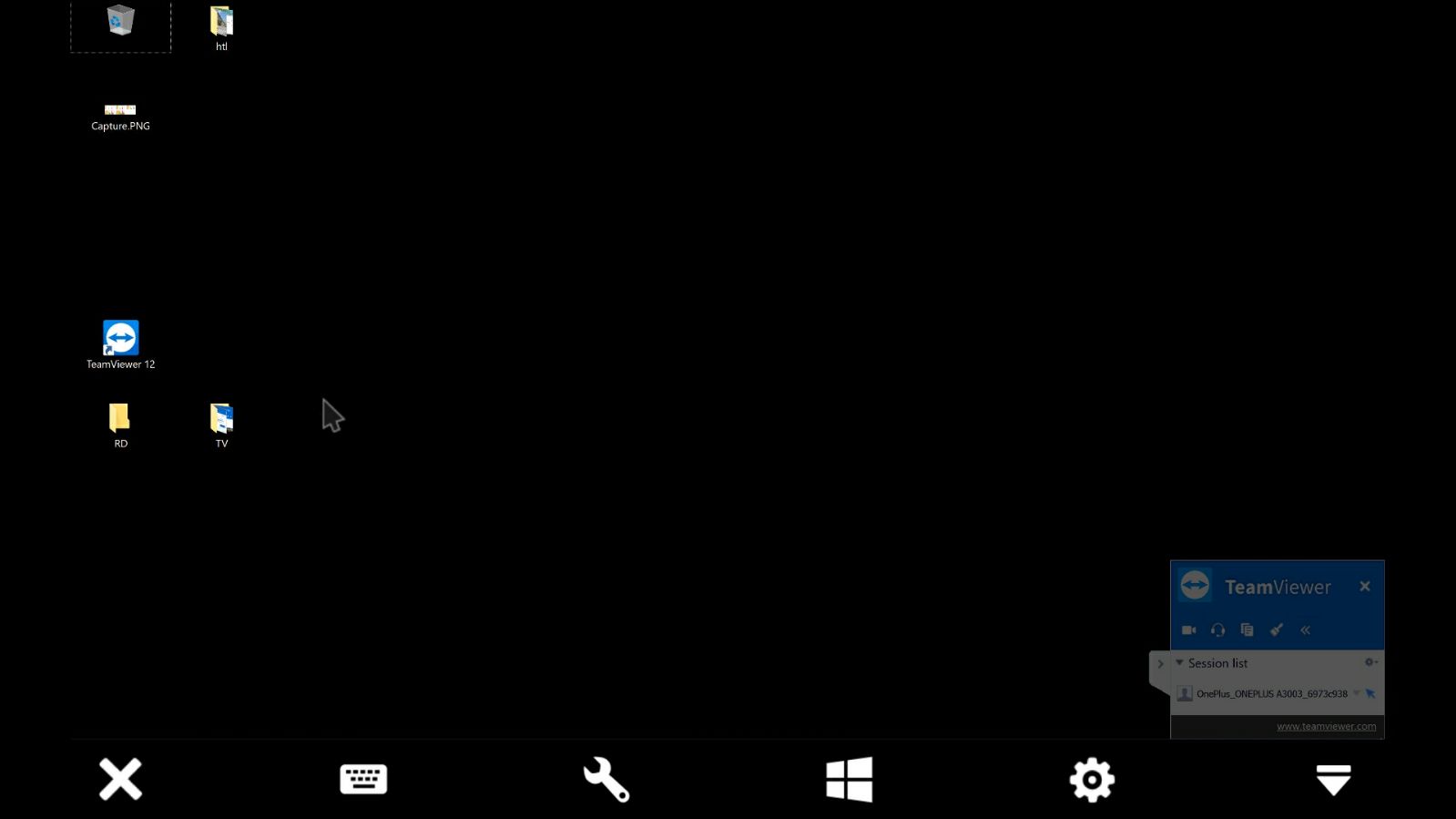
Verbindungsaufbau zu einem   
anderen PC



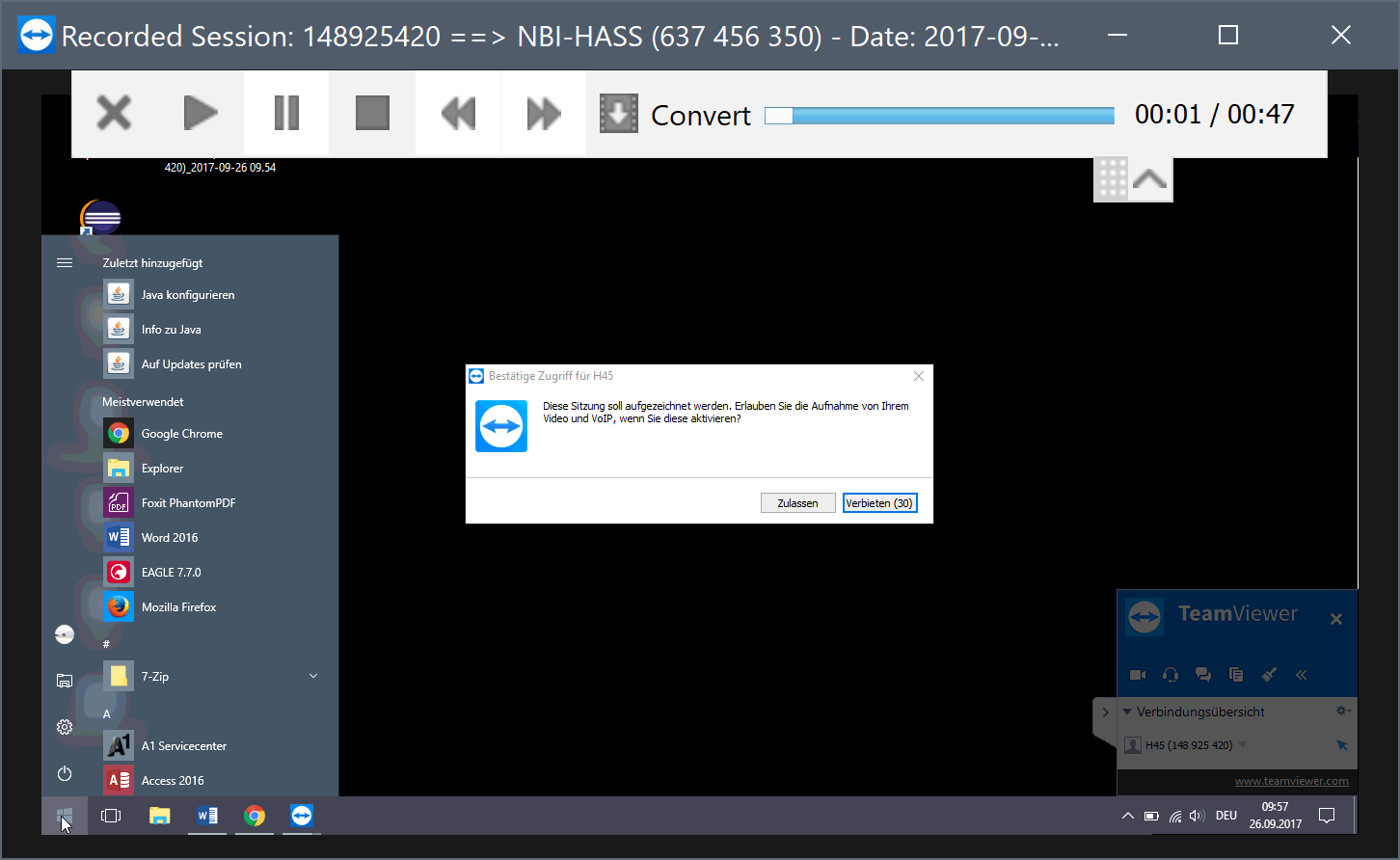
Erzwungener Passwort-Refresh



Remote-Control Session

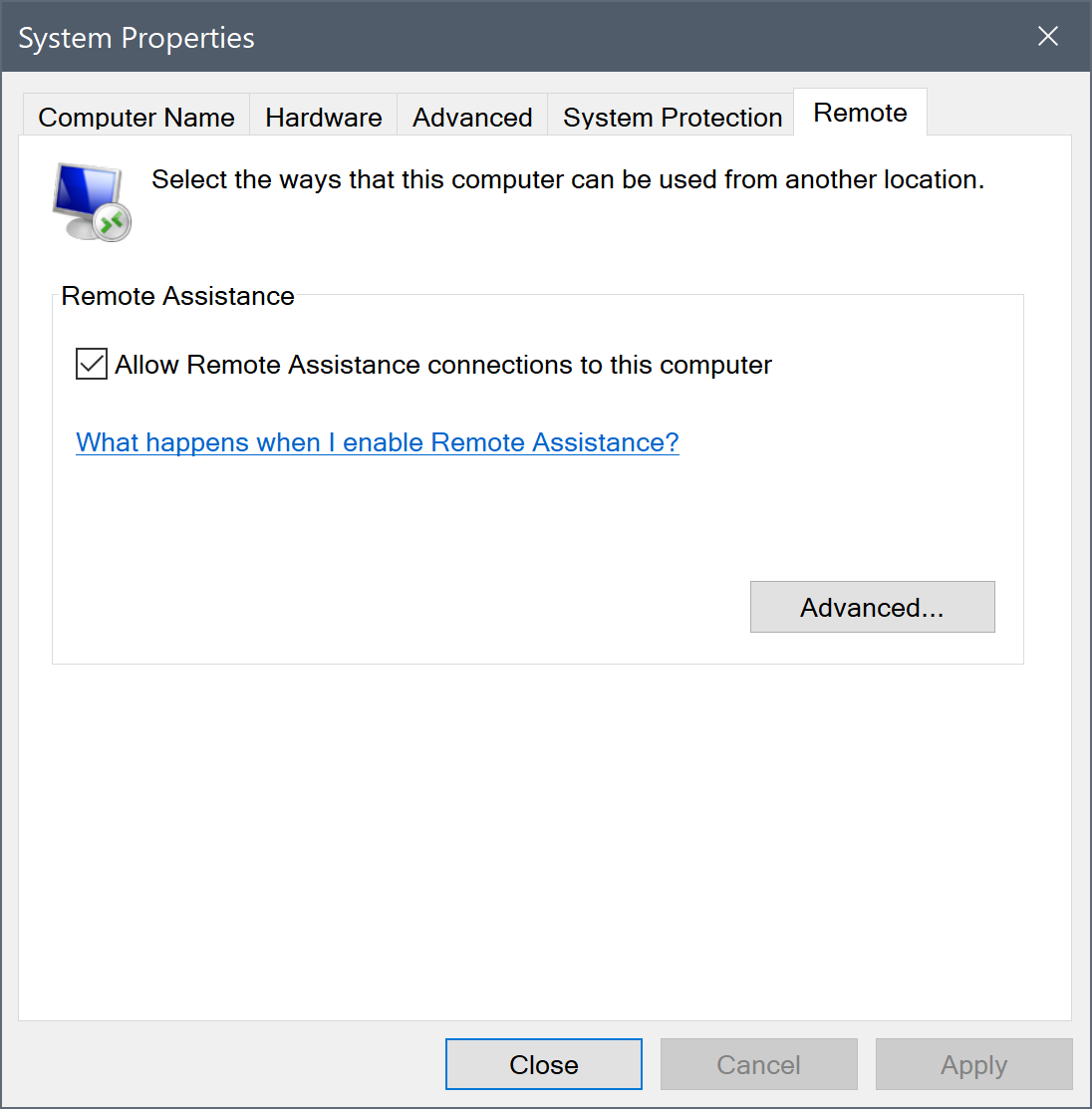


Zugriff per Android-App

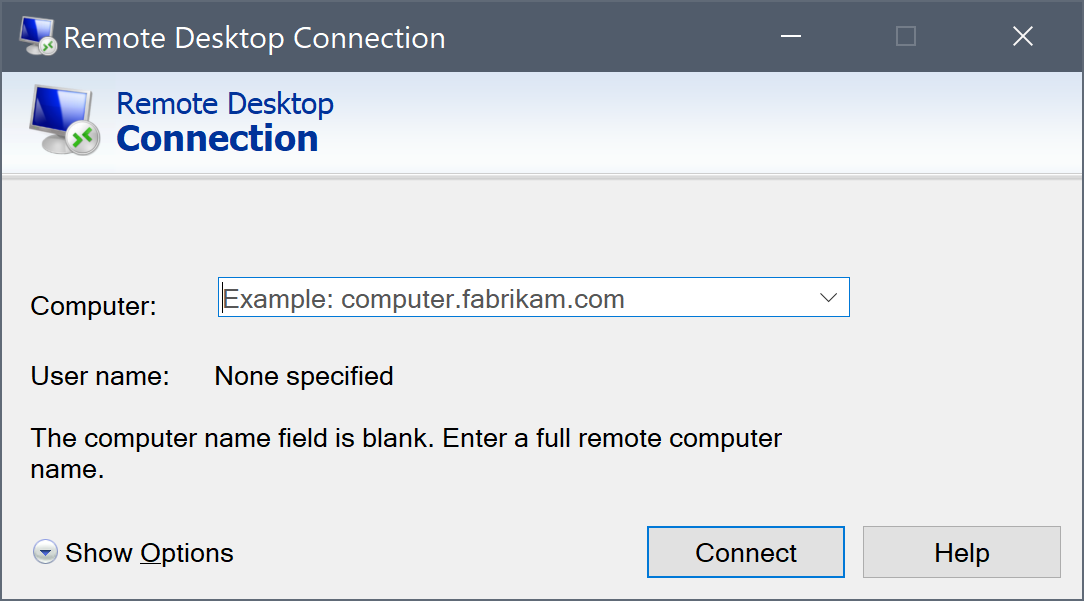


Eingebauter Video-Player zum Ansehen und Konvertieren der aufgezeichneten Sessions

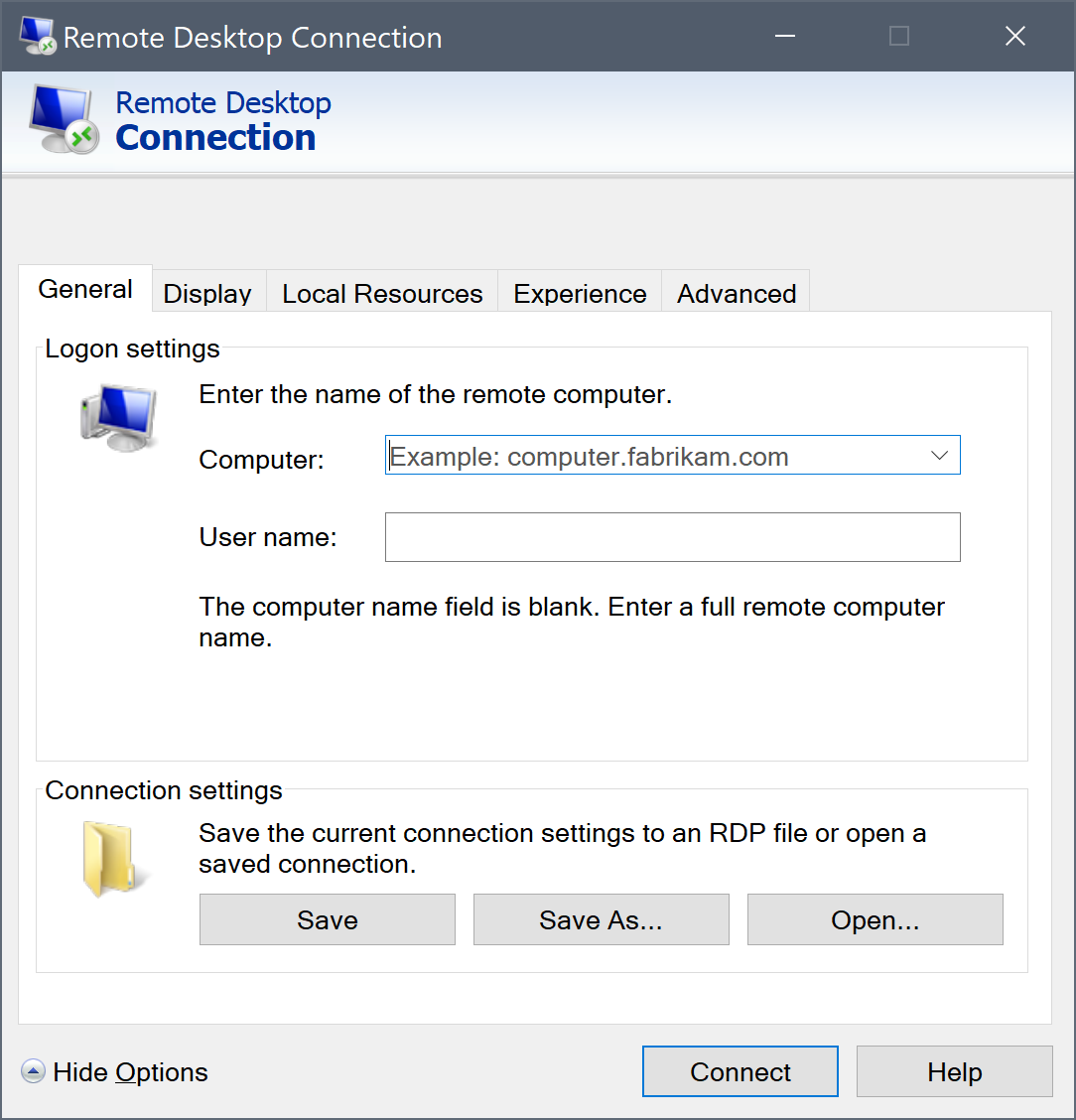
RemoteDesktop-Screenshots:



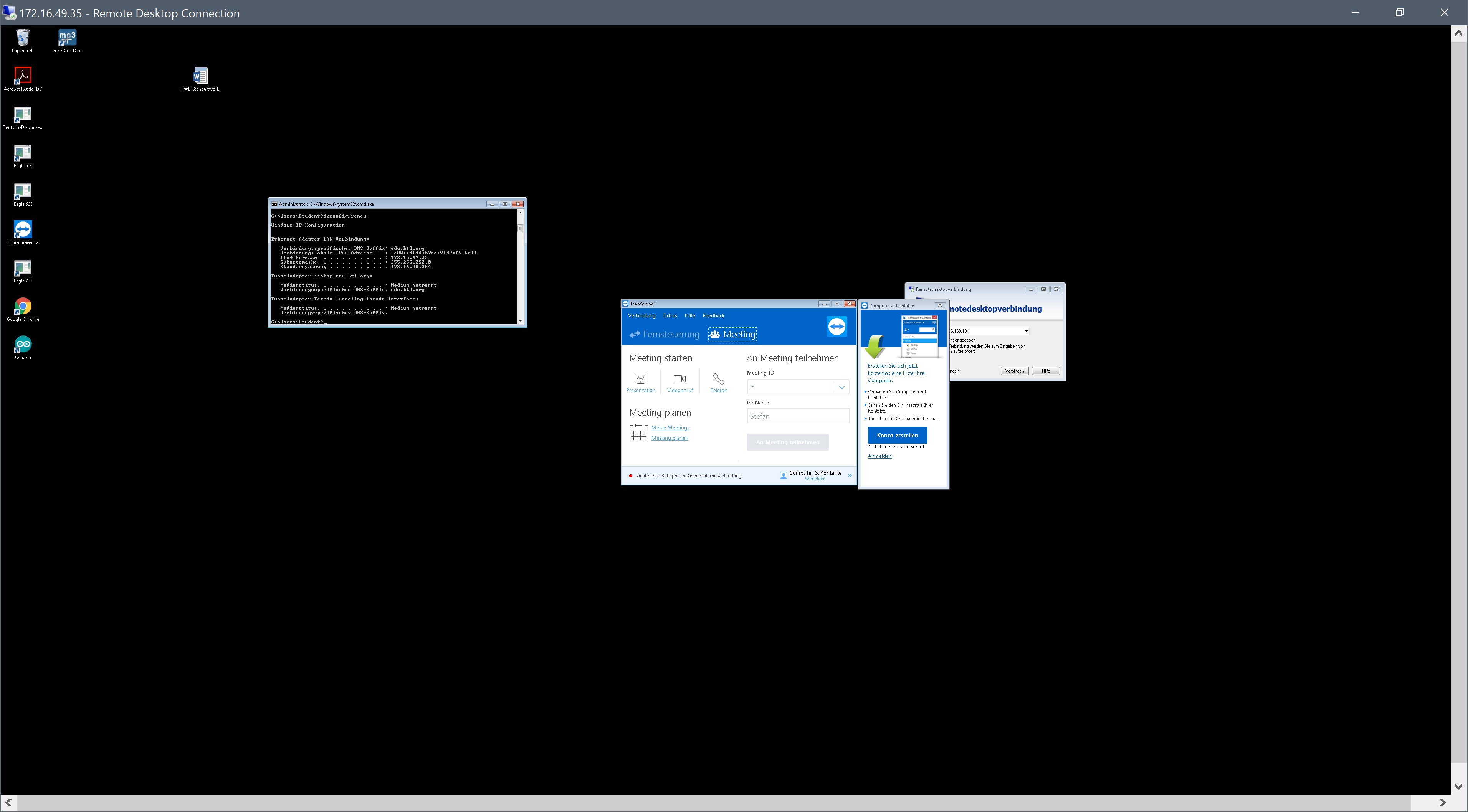
Einstellung / Setup



Hauptbildschirm für schnelle Verbindung

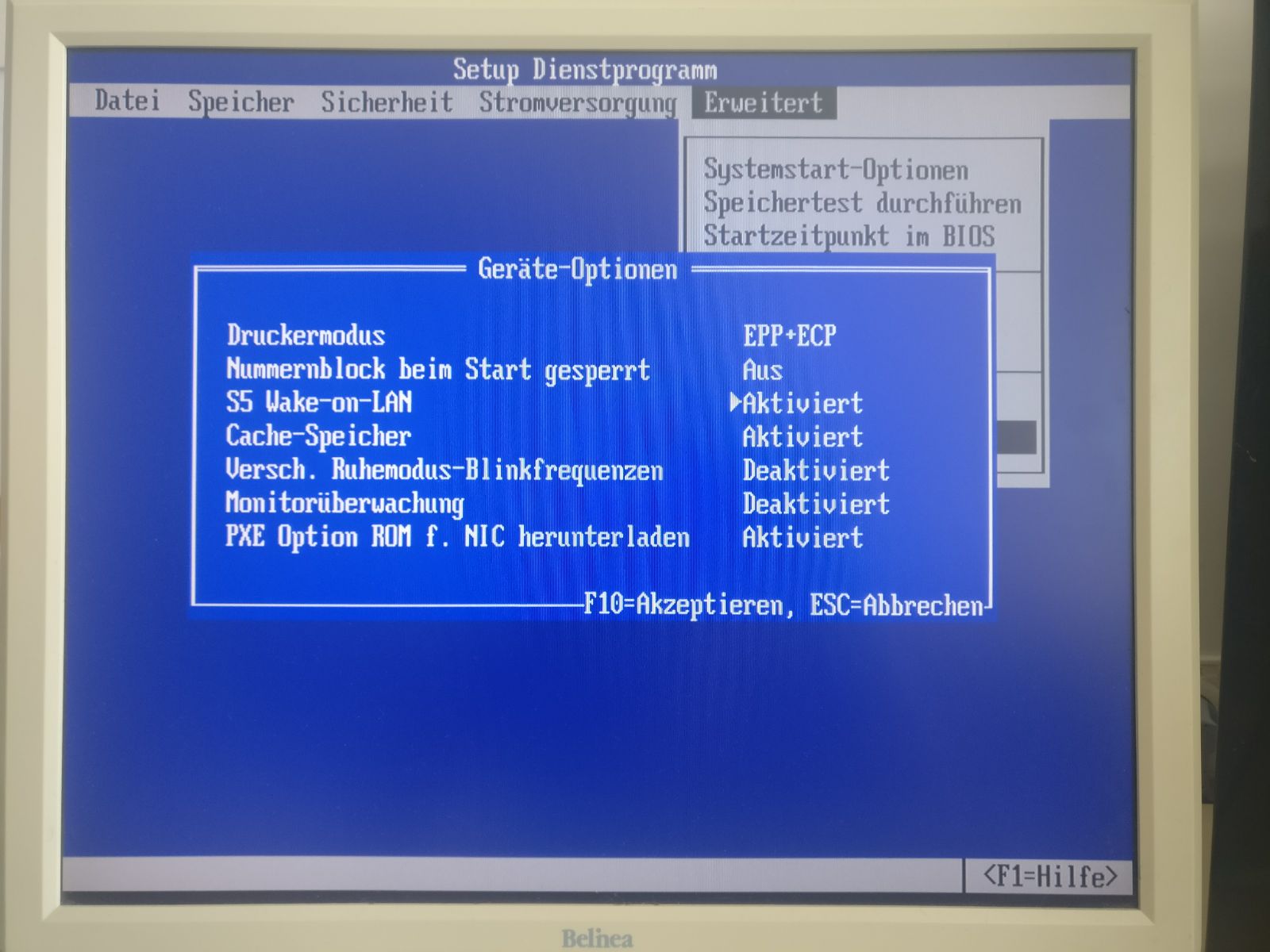


Hauptbildschirm mit Einstellungen

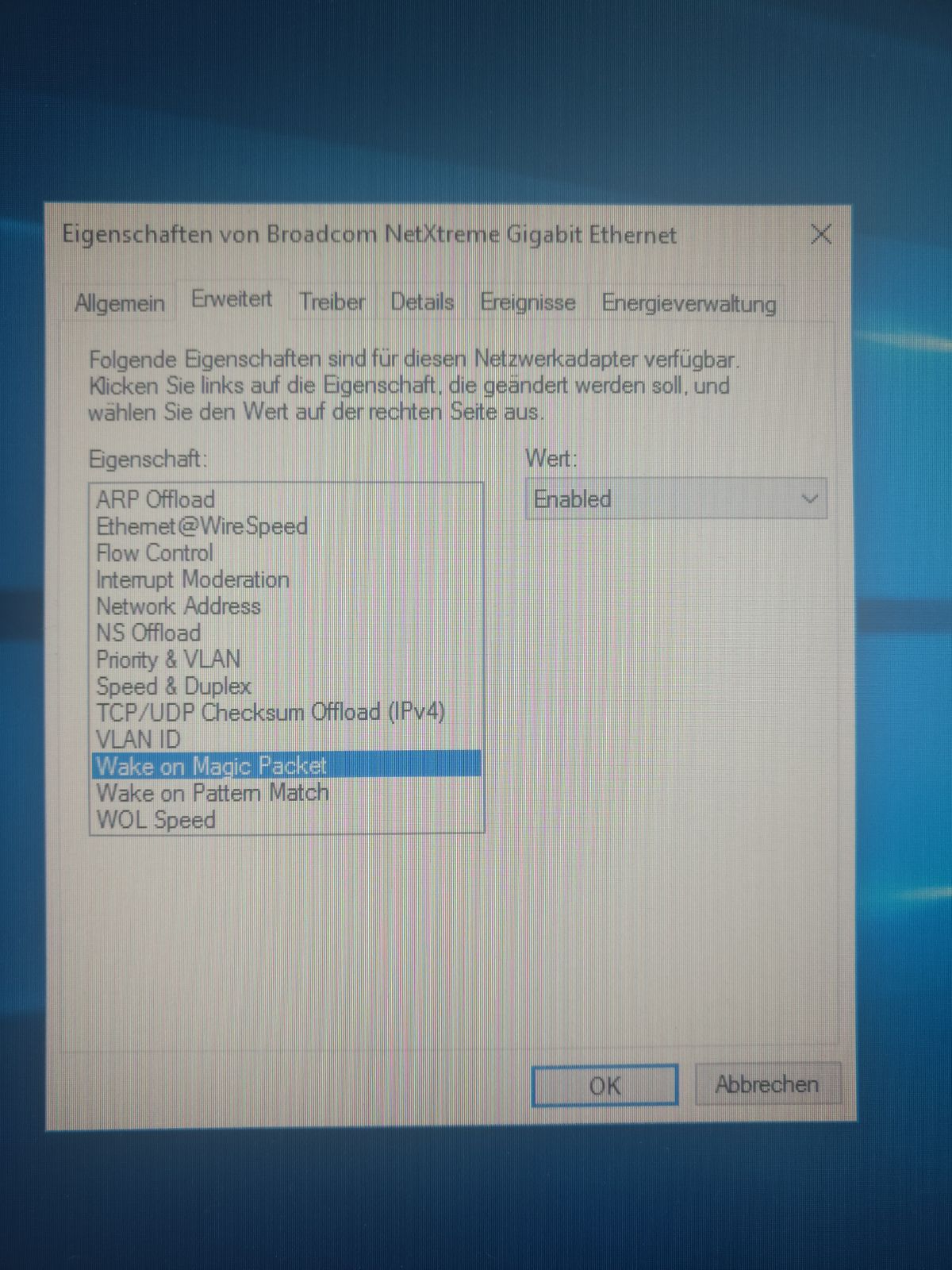


Session auf einem   
anderen PC

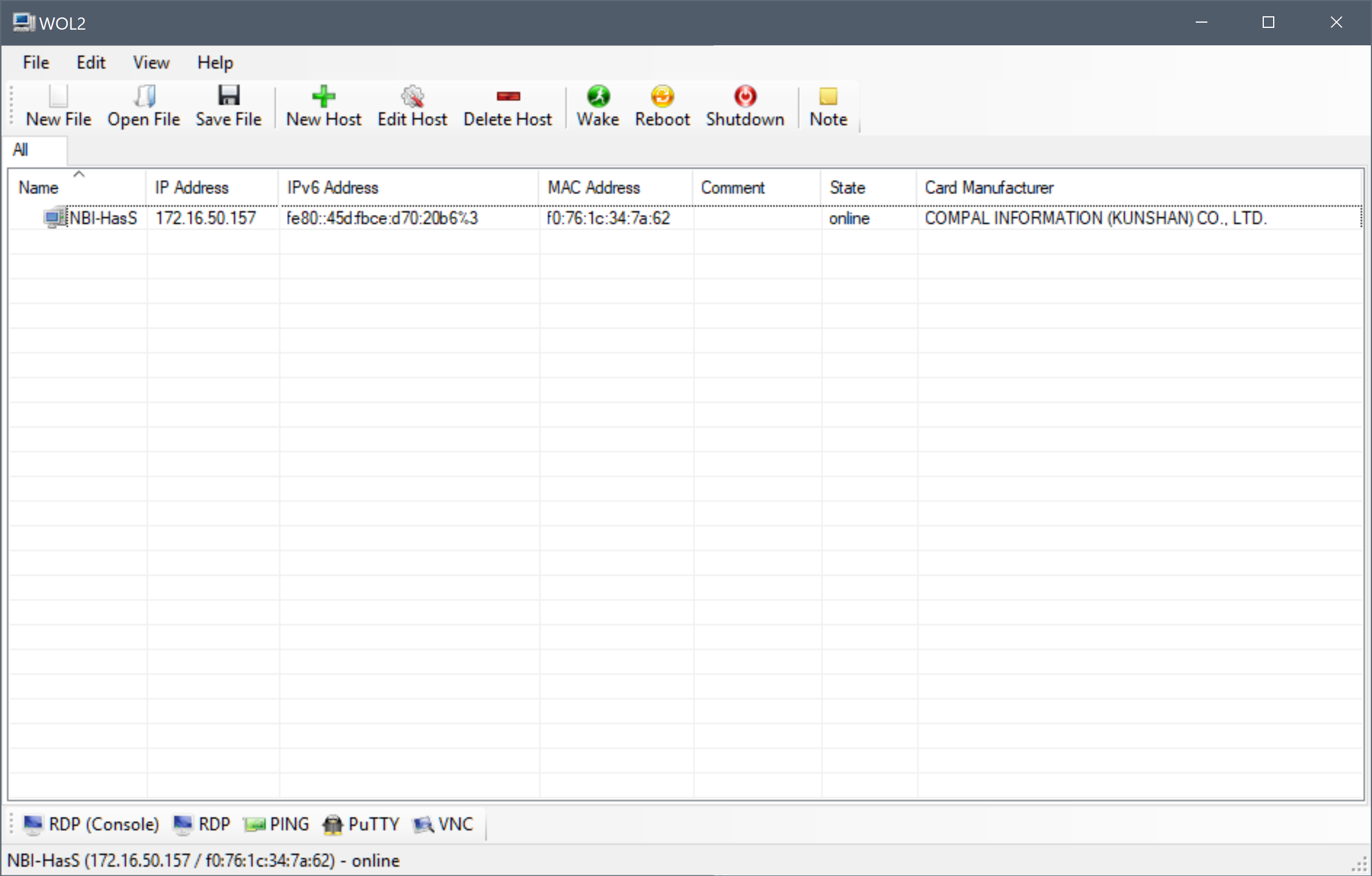
WoL-Screenshots:

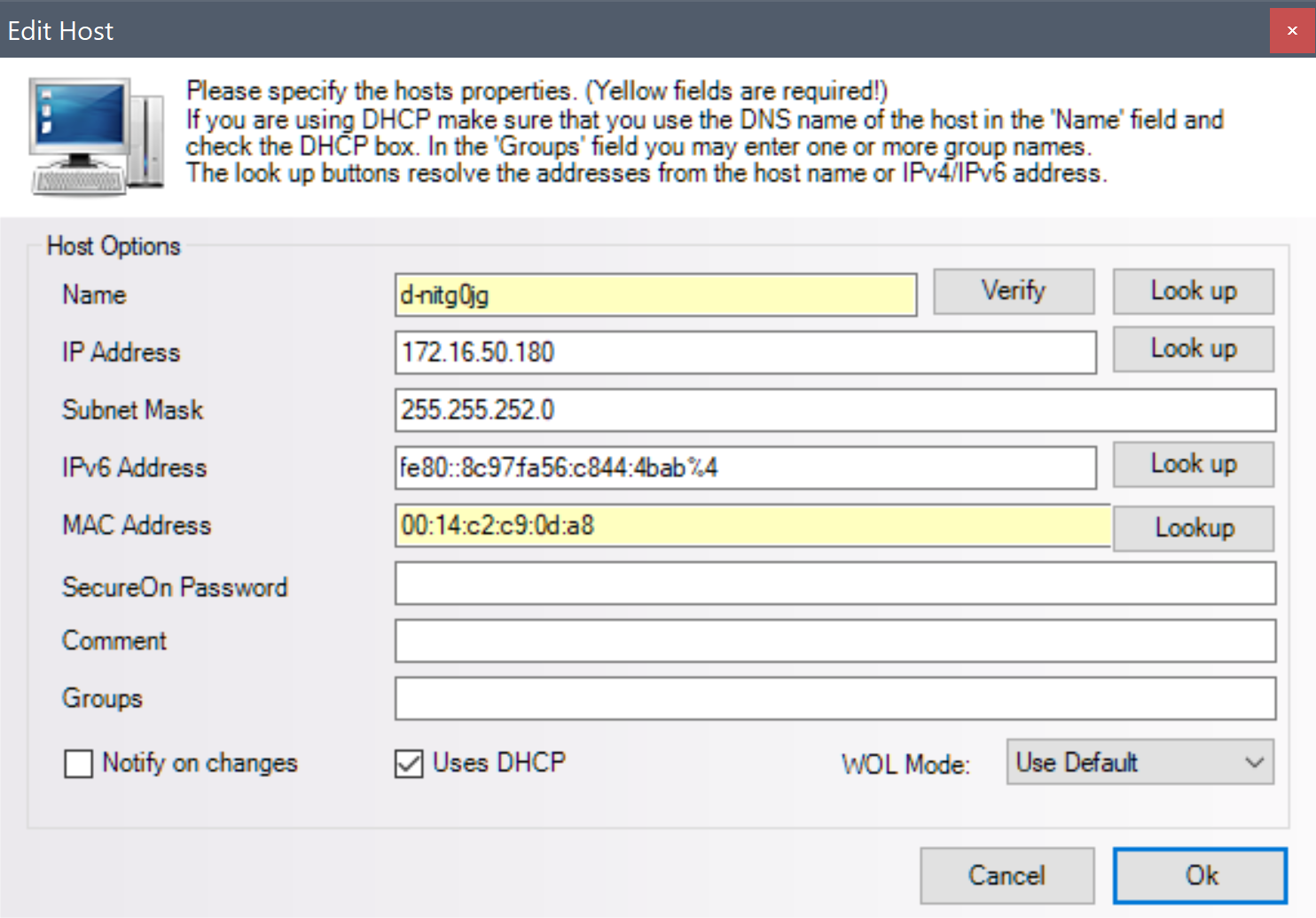


Aktivieren von S5-WoL im BIOS



Aktivieren von WoL in den Netzwerkadaptereigenschaften

WoL Programm auf Windows

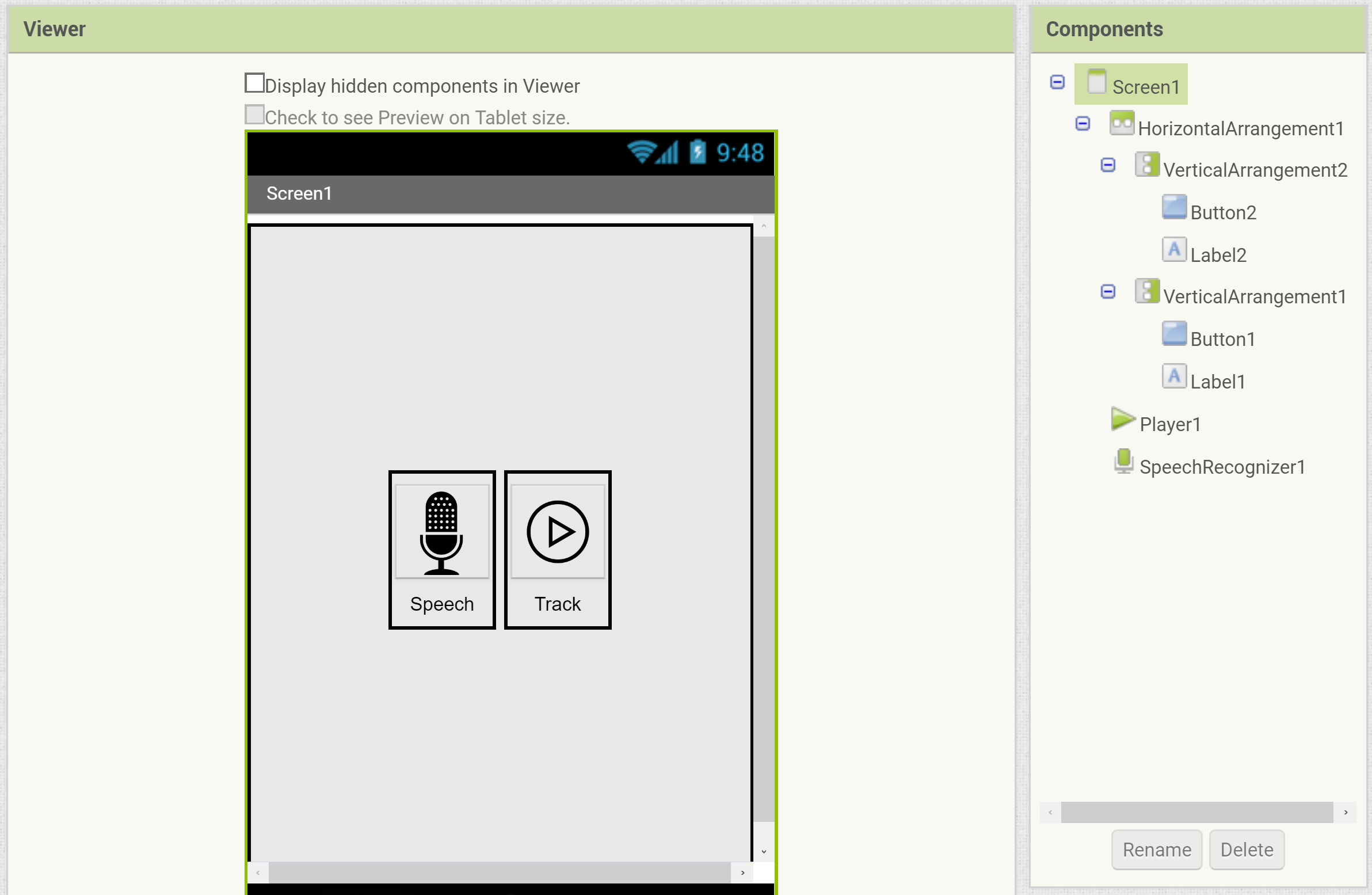
Konfiguration eines Ziel-Hosts

Android Apps erstellen mit dem MIT App Inventor

Was ist der MIT App Inventor?

[Der MIT App Inventor](http://ai2.appinventor.mit.edu/) vereinfach das Programmieren von Android-Apps durch sein einfaches Layout und das Prinzip von Drag and Drop zum erstellen von Code. Sowohl einfache Logik als auch komplexer Code können hier ohne großen Aufwand und vor allem ohne besonders gute Programmierkenntnisse schnell und unkompliziert erstellt werden.   
Auch der grafische Aufbau der App entsteht durch Drag and Drop.

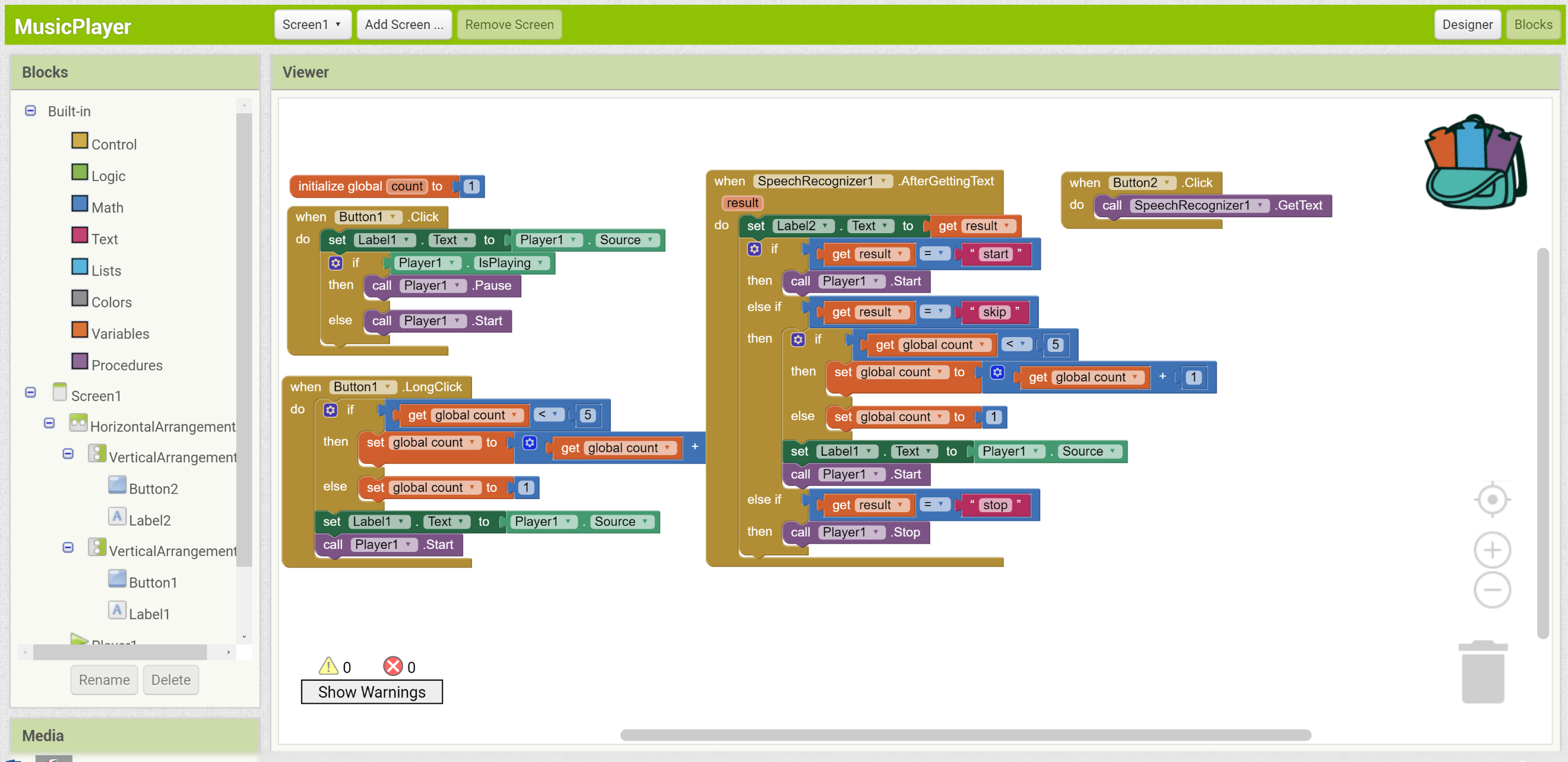
Beispiel: Sprachgesteuerter Musik-Player



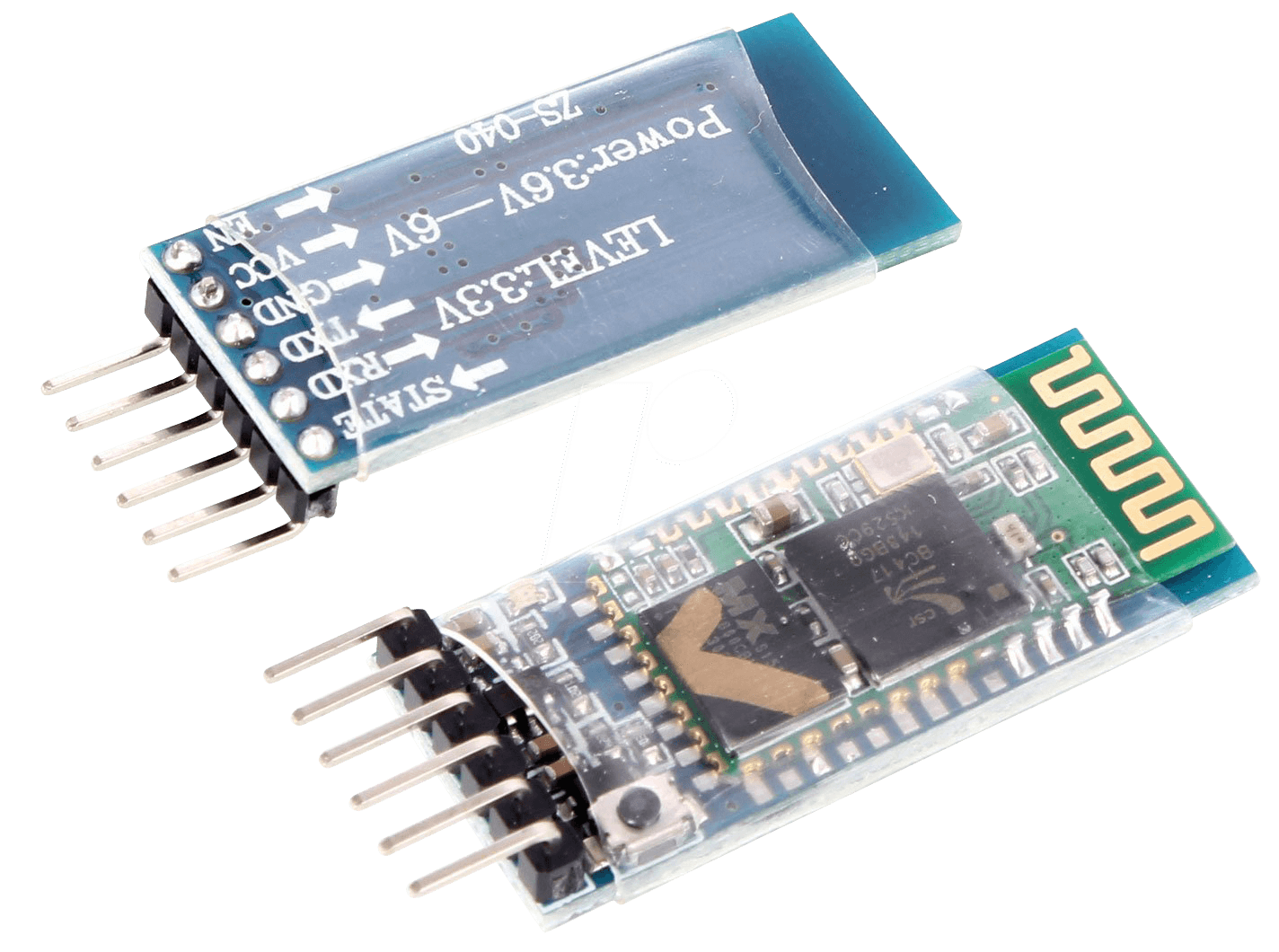
Layout-Aufbau mit dem App Inventor



*Diese Projektfiles können einfach in den App Inventor importiert werden*



Layout-Aufbau mit dem App Inventor

Arduino Bluetooth apps

Bluetooth Module

Es gibt viele Bluetooth-Module für den Arduino. Besonders im Internet findet man Unmengen an Geräten, wovon die meisten gleiche oder zumindest ähnliche Funktionen aufweisen. Für dieses Projekt wurde das Bluetooth-Modul „HC05“ ausgewählt, da es eines der häufigsten Module ist und somit bereits eine große und aktive Community an eifrigen Testern besteht.

Das HC05 muss für die Benutzung konfiguriert werden. Dafür wird dieses Programm ausgeführt:



Software Serial

#define BT 38400

#include <SoftwareSerial.h>

SoftwareSerial mySerial(10, 11); // RX, TX

char data = 0;

void setup() {

pinMode(1, OUTPUT);

Serial.begin(BT);

mySerial.begin(BT);

Serial.println("Done\n");

}

void loop() {

if(Serial.available() > 0) // Send data only when you receive data:

{

data = Serial.read(); //Read the incoming data & store into data

Serial.print(data); //Print Value inside data in Serial monitor

Serial.print("\n");

}

if (mySerial.available()) {

data = mySerial.read(); //Read the incoming data & store into data

Serial.print(data); //Print Value inside data in Serial monitor

Serial.print("\n");

}

}

Die Seriellen Pins (Rx & Tx) beschränken sich beim Arduino auf die Pins 0 und 1. Wenn man das Bluetooth-Modul hier ansteckt, kann eine direkte Kommunikation zwischen Modul und Arduino erfolgen.

Software Serial gibt es, da ein angeschlossenes Gerät an den Pins 0 und 1 physisch mit der Programmierschnittstelle verbunden ist. Daher interferiert das Modul mit dem Flashvorgang und muss somit bei jeder Übertragung vom Arduino getrennt werden.

Mit einem einfachen Workaround kann man sich die Mühe sparen:  
Software Serial ändert die Pins der Seriellen Schnittstelle auf zwei vom Programmierer definierte. Dort schließt man dann Rx bzw. Tx an und kann somit das Modul verwenden und gleichzeitig den Arduino beschreiben.

Jegliche Doku zu Software Serial selbst findet sich hier:

<https://www.arduino.cc/en/Reference/SoftwareSerial>

Quellen **(19.09.17):**

* <https://de.wikipedia.org/wiki/Domain_(Internet)>
* <https://de.wikipedia.org/wiki/Netzwerkadress%C3%BCbersetzung>
* <https://de.wikipedia.org/wiki/Proxy_(Rechnernetz)>
* <https://de.wikipedia.org/wiki/Domain_Name_System>
* <https://de.wikipedia.org/wiki/MAC-Adresse>
* <https://de.wikipedia.org/wiki/Netzmaske>
* <https://de.wikipedia.org/wiki/Switch_(Netzwerktechnik)>
* <https://de.wikipedia.org/wiki/IP-Adresse>
* <https://de.wikipedia.org/wiki/Firewall>
* <https://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>
* <https://de.wikipedia.org/wiki/Router>
* <https://de.wikipedia.org/wiki/Datenpaket>
* <https://de.wikipedia.org/wiki/Port_(Protokoll)>
* <https://de.wikipedia.org/wiki/OSI-Modell>
* <https://de.wikipedia.org/wiki/Transmission_Control_Protocol>
* <https://de.wikipedia.org/wiki/User_Datagram_Protocol>
* <https://de.wikipedia.org/wiki/Wake_On_LAN> (26.09.17)