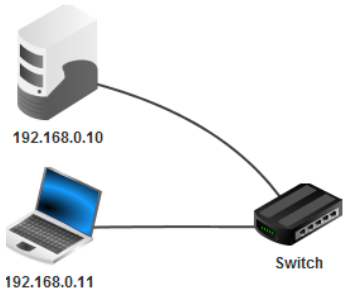
Simulation von Netzwerken mit FILIUS II



Öffne dein zuletzt gespeichertes FILIUS-Netzwerk. (Version 01)
(Vorlagedatei: v01-filius01.fls); (*vgl. 251-materialien\filius\filius01.fls*)
Im Programm FILIUS kann man die Netzwerkaktivitäten beobachten. Dazu öffnest du im *Aktionsmodus* mit der rechten Maustaste das Kontextmenü des Notebooks und wählst *Datenaustausch anzeigen* ... an.
Das Datenaustauschfenster könnte nach der Eingabe des Kommandos `ping 192.168.0.10` unter anderem die folgenden Resultate anzeigen:

Datenaustausch

192.168.0.11

Nr.	Zeit	Quelle	Ziel	Protokoll	Schicht	Bemerkungen
2	06:04:54.783	192.168.0.11	192.168.0.10	ARP	*Vermittlung*	Suche nach MAC für 192.168.0.10, 192.168.0.11: 03:9A:55:A0:64:47
3	06:04:54.814	192.168.0.10	192.168.0.11	ARP	*Vermittlung*	192.168.0.10: 7C:EA:E0:21:42:35
4	06:04:54.845	192.168.0.11	192.168.0.10	ICMP	*Vermittlung*	ICMP Echo Request (ping)
5	06:04:55.032	192.168.0.10	192.168.0.11	ARP	*Vermittlung*	192.168.0.10: 7C:EA:E0:21:42:35
6	06:04:55.095	192.168.0.10	192.168.0.11	ICMP	*Vermittlung*	ICMP Echo Reply (pong)

- Zeilen 2,3 und 5: Das Adress Resolution Protocol (ARP) ermittelt in IP Version 4 die zu einer IP-Adresse zugehörige MAC-Adresse. Anmerkung: Da dieses Protokoll ein Sicherheitsrisiko war (ARP-Spoofing), wurde das ARP in IPv6 durch das NDP (Neighbor Discovery Protocol) ersetzt.
  - Zeile 2: Der anfragende Computer sendet die IP-Adresse des gesuchten Computers mit seiner IP- und MAC-Adresse an alle Computer des lokalen Netzwerks.
    Ein solcher „Rundruf“ wird als **Broadcast** bezeichnet.
  - Zeile 3: Die Broadcast-Adresse FF:FF:FF:FF:FF:FF nehmen alle Computer im Netz entgegen.
    Der gesuchte Computer sendet in einer ARP-Antwort (ARP-Request) seine IP- und MAC-Adresse an die MAC-Adresse des anfragenden Computers.
- Zeilen 4 und 6: Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informationen und Fehlermeldungen in Netzwerken. Es ermöglicht Echo-Anfragen (das „Anpingen“ von Computern). Durch Senden eines ICMP Echo-Requests („ping“) kann man sicherstellen, dass ein Host erreichbar ist, wenn dieser mit einem ICMP Echo-Reply („pong“) antwortet.
  Hinweis: Wenn ein Host nicht antwortet, bedeutet das nicht unbedingt, dass er nicht erreichbar ist: Aus Sicherheitsgründen beantworten viele Hosts keine ICMP-Anfragen.

Aufgaben

1. Welche Netzwerktopologie liegt bei dem Beispiel oben vor?

   Netzwerktopologie: *Stern*

2. Welche Vernetzungstechnik wird verwendet? Nenne das zugehörige Zugriffsverfahren.

   Vernetzungstechnik: *Ethernet – Zugriffsverfahren: CSMA/CD*

3. Ordne die verwendeten Netzwerkkomponenten in das OSI-Schichtenmodell ein.

   Kabel: *Schicht 1 (Bitübertragung)*

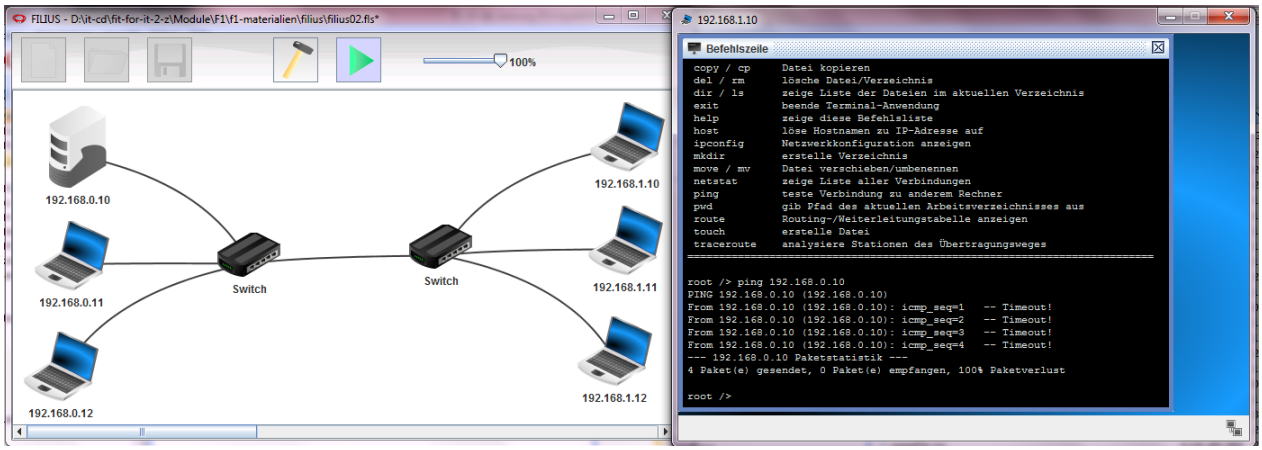
   Switch: *Schicht 2 (Sicherung)*

4. Welcher OSI-Schicht ist die MAC-Adresse zuzuordnen? Wofür ist sie erforderlich?

   Schicht 2 – die MAC-Adresse ist zur Identifikation der Netzwerkadapter erforderlich.

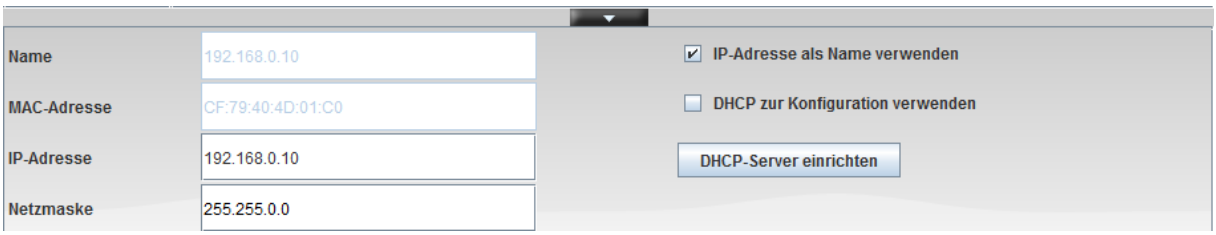
5. Ergänze in deinem Filius-Netz ein drittes Notebook mit der IPv4-Adresse 192.168.0.12. Damit könnte es jetzt ein großes lokales Netz mit vielen Computern sein, zum Beispiel ein Computerraum.
   - Baue ein weiteres Netz mit einem Switch und drei Rechnern auf. Das könnte ein weiterer Computerraum sein. Um einfach unterscheiden zu können, in welchem der Räume der jeweilige Rechner steht, vergibst du für den neuen Raum die IPv4-Adressen 192.168.1.10 bis 192.168.1.12.
   - Verbinde die beiden Switches mit Hilfe eines Kabels.
   - Installiere auf dem Rechner 192.168.1.10 eine *Befehlszeile*.

Hinweis: Mit dieser Konfiguration wird keine Kommunikation möglich sein. Du kannst gerne probieren, den Rechner 192.168.0.10 vom Rechner 192.168.1.10 aus anzupingen.



Das liegt an der gewählten *Subnetzmaske*: In IPv4 gibt die Subnetzmaske an, wie viele Bits am Anfang der IP-Adresse den Netzwerkteil festlegen. Bei IPv6 entspricht das der *Präfixlänge*.
Im Beispiel lautet die Subnetzmaske 255.255.255.0. Mit den ersten drei Byte (255) wird festgelegt, dass der Netzwerkteil 24 bit groß ist, für den Geräteteil bleibt also ein Byte. Die IPv4-Adresse nach dem Classless Inter-Domain Routing (CIDR; vgl. Arbeitsblatt 2.5.1-09) wäre also 192.168.0.10/24.
IP-Adressen, die im Netzwerkteil übereinstimmen, werden im selben Netz gesucht, IP-Adressen, die sich im Netzwerkteil unterscheiden, sind nur über Router in anderen Netzen erreichbar. Innerhalb eines Netzes müssen also die Subnetzmaske und der Netzwerkteil identisch sein.
Das Problem lässt sich einfach beheben: Der private IPv4-Adressbereich 192.168.n.n lässt Subnetzmasken mit 16 Bit großem Netzwerkteil zu, so dass im Beispiel die IPv4-Adressen 192.168.0.10/16 bzw. 192.168.1.10/16 verwendet werden können:

6. Ändere für alle Rechner die Subnetzmaske auf 255.255.0.0.



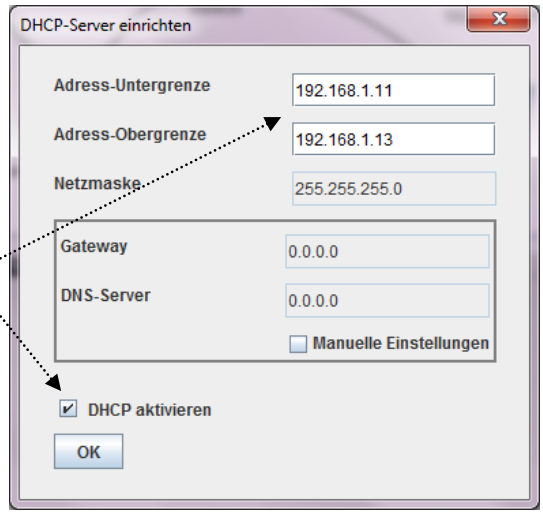
   - Starte auf dem Rechner 192.168.1.10 die *Befehlszeile* und pinge den Rechner 192.168.0.10 an. Jetzt sollte der Kommunikationsvorgang funktionieren.
     Speichere dein FILIUS-Netzwerk unter der Bezeichnung „Version02“.
     (*vgl. 251-materialien\filius\filius02.fls*)

➢ Das vorliegende Netzwerk ist ein stark vereinfachtes Beispiel für eine Baumstruktur in einem LAN.

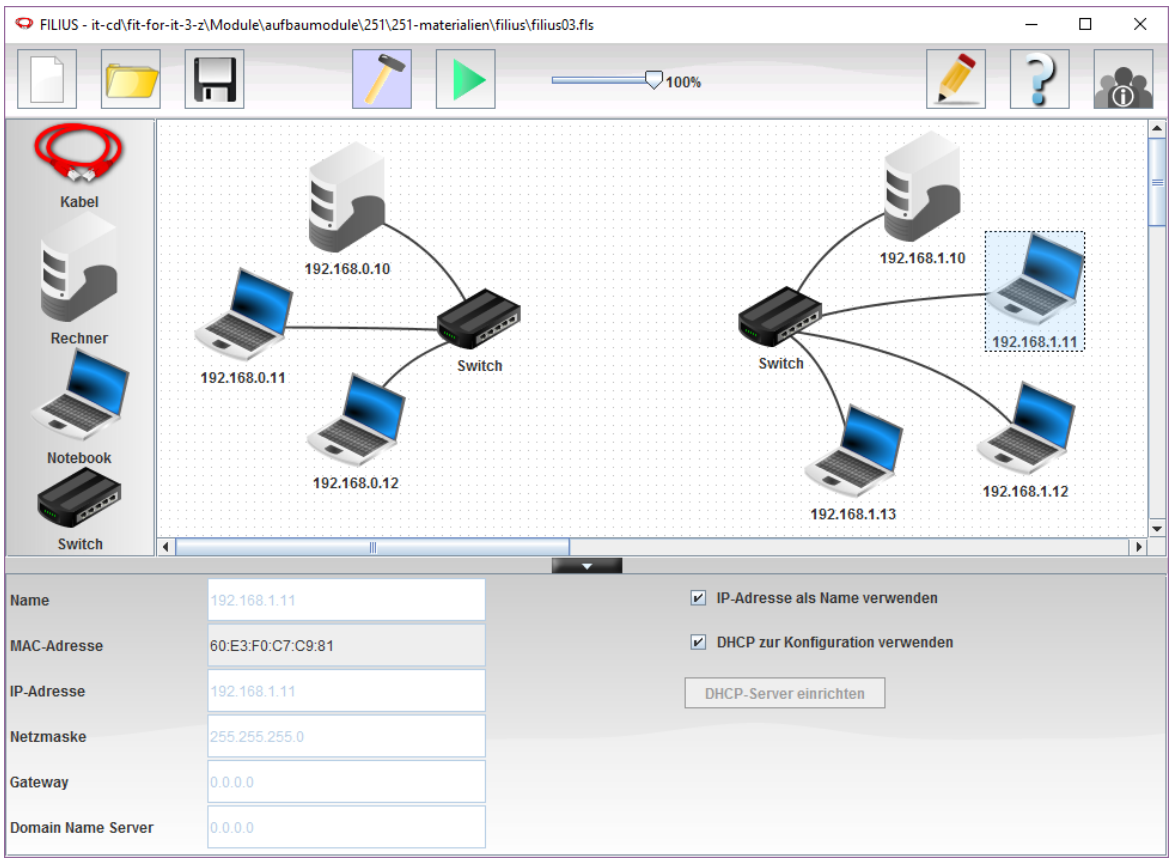
Für die weiteren Aufgabenstellungen sollen zwei unterschiedliche Netze aufgebaut werden. Die Netzwerke links und rechts werden dann also Beispiele für zwei weit voneinander entfernte lokale Netzwerke sein.

➢ Jetzt müssten die Netzmasken wieder für alle Rechner in 255.255.255.0 geändert werden.
Das ist mühsam, **weshalb du es nicht tust**: Bei jeder Änderung die Einstellungen an allen Rechnern anzupassen ist recht umständlich. Auch muss sichergestellt werden, dass innerhalb eines Netzes jede IP-Adresse nur genau einmal vergeben wird.
Deshalb wurde für IPv4 das *Dynamic Host Configuration Protocol* (DHCP) entwickelt. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

7. In FILIUS wird dazu der **DHCP-Server** aktiviert.
   - Lösche die Kabelverbindung zwischen den beiden Switches (rechte Maustaste – Kabel entfernen). (Vorlagedatei: v02-filius02.fls)
   - Ergänze im Netz rechts einen Server mit der IPv4-Adresse 192.168.1.10 und installiere hier einen DHCP-Server („*DHCP-Server einrichten*“). Hier muss der Bereich für die IP-Adressen eingetragen werden. Für das Gateway und den DNS-Server ist die Voreinstellung 0.0.0.0 korrekt.
   - Konfiguriere den DHCP-Server des Rechners 192.168.0.10 entsprechend im Bereich von 192.168.0.11 bis 192.168.0.12. Vergiss nicht, die Netzmaske auf 255.255.255.0 zu setzen.



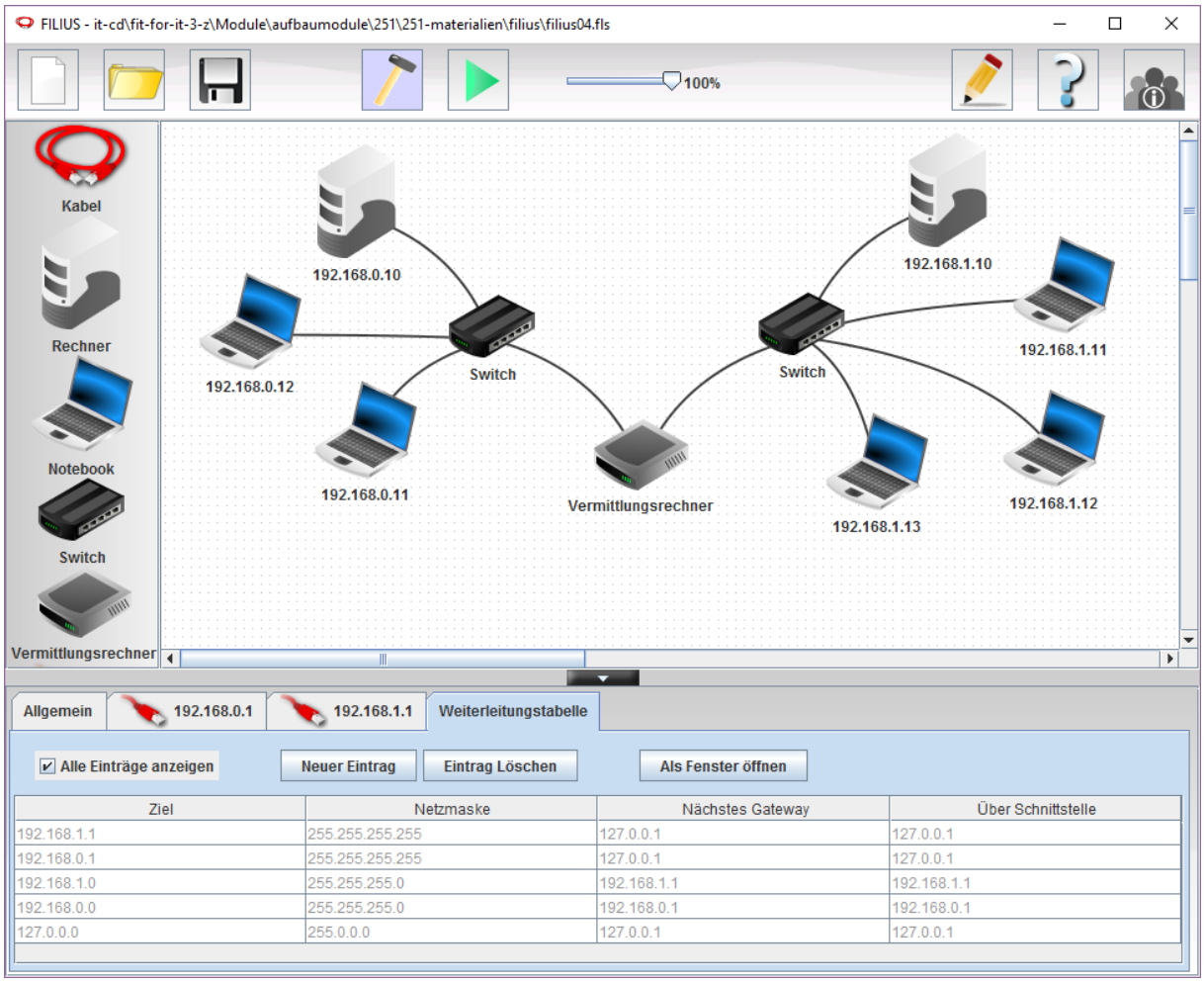
   - Dann muss bei allen Rechnern die Option „DHCP zur Konfiguration verwenden“ aktiviert werden.
   - Durch Wechsel in den *Aktionsmodus* wird der DHCP-Dienst aktiviert und die IP-Adressen neu vergeben. Das Netzwerk stellt sich dann so dar (Version03) (*vgl. 251-materialien\filius\filius03.fls*):



Ein Switch kann Daten lediglich innerhalb eines Netzwerks weiterleiten, weil er nur MAC-Frames verarbeitet, also in der OSI-Schicht 2 arbeitet.

- Um zwei unterschiedliche Netze miteinander zu verbinden, benötigt man einen *Router*, der IP-Pakete verarbeiten kann, also in der OSI-Schicht 3 (Netzwerk) arbeitet.

8. Verbinde die beiden Switches mittels eines solchen „*Vermittlungsrechners*“, wie er in FILIUS genannt wird (2 Schnittstellen reichen aus). (Vorlagedatei: v03-filius03.fls)
   Verwende für die Netzwerkkarten 1 und 2 des Routers die IPv4-Adressen 192.168.0.1 und 192.168.1.1. Der Router konfiguriert selbstständig eine Weiterleitungstabelle zwischen den beiden internen Netzwerkadaptern (*vgl. 251-materialien\filius\filius04.fls*):



- Wenn Pakete an ein anderes Netz gesendet werden sollen, benötigen die Hosts die Angabe des Gateways, über das Pakete geroutet werden.

9. Bei dem DHCP-Server links muss deshalb noch das *Gateway* 192.168.0.1 eingetragen werden, bei dem DHCP-Server rechts das *Gateway* 192.168.1.1 als *manuelle Einstellung* (Version04).
   Außerdem müssen die Gateway-Einstellungen für die Rechner, auf denen der DHCP-Server installiert ist, manuell vorgenommen werden.
   Teste die Datenübertragung, indem du im *Aktionsmodus* vom Rechner 192.168.0.11 aus, auf dem noch die Befehlszeile installiert ist, die Rechner 192.168.1.10 und 192.168.1.11 anpingst.
   Durch abwechselnde farbige Hervorhebung der Leitungen wird der Kommunikationsvorgang in FILIUS dargestellt. Um den Kommunikationsvorgang detailliert nachzuvollziehen, kannst du auch das Fenster *Netzwerkaktivitäten* einblenden.