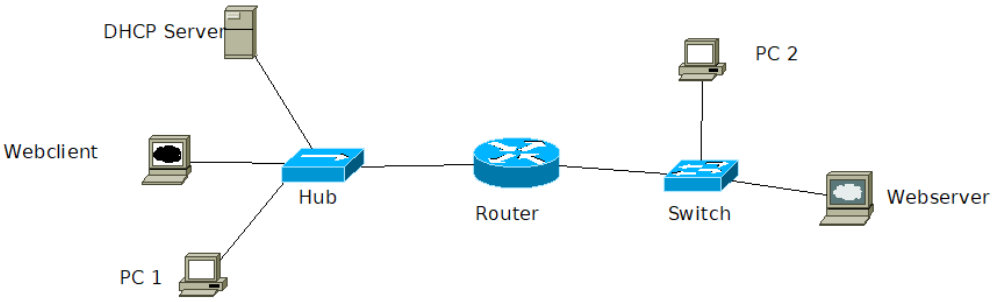
Übung 09: Ethernet, IP, Ports

Aufgabe 1: Ethernet, Subnetze, IP



a) Kreuzen Sie mit „Ja“ oder „Nein“ an, welche „Komponente“ (MAC bzw. IP Adresse, ARP-Tabelle, Routingtabelle) jeweils ***zwingend*** bei welchem Gerät vorhanden sein muss.

„Komponente“	**Router**	**Switch**	**Hub**	**PC**
MAC Adresse				
IP Adresse				
ARP-Tabelle				
Routingtabelle				

b) Weisen Sie allen Geräten eine sinnvolle IPv4 Adresse zu. Anforderungen:
- Der DHCP Server hat die IP 192.168.0.100. Der DHCP Server weist den PCs im gleichen Subnetz eine IP Adresse zu.
- Verwenden Sie ansonsten soweit als möglich (beliebige) ***öffentliche*** IPv4 Adressen.

c) Welche statischen Routen werden benötigt, damit der Webclient den Webserver erreichen kann? (***Stichpunkte***)

<u>Annahme für die folgenden Teilaufgaben: Alle Geräte können sich erfolgreich pingen.</u>

d) Alle ARP Tabellen seien leer. Sie senden nun eine Ping von `PC1` an `PC2`. Welche Einträge sehen Sie danach in der ARP Tabelle von `PC1` und dem `Router`?

e) `PC1` und `PC2` senden jeweils eine ARP Request („Who has …“) bzgl. einer beliebigen IP, die genaue IP spielt keine Rolle. Welche Geräte sehen jeweils den ARP Request?

f) Ist gleichzeitige Kommunikation möglich? Der `Router` sendet Frames über den Hub an den `Webclient`. Gleichzeitig sendet `PC1` ein *DHCP Discover*.

Aufgabe 2: Portnummern

Client *A* baut zu einem Server *S* eine SSH[1] Session auf. Gleichzeitig baut Client *B* eine SSH Session zu Server *S* auf. Für SSH wird der standardisierte Port (Internetrecherche!) verwendet. Nennen Sie ***mögliche*** Source und Destination Ports für

a) Segmente von *A* zu *S*
b) Segmente von *B* zu *S*
c) Segmente von *S* zu *A*
d) Falls *A* und *B* verschiedene Hosts sind, ist es möglich, dass der Source-Port in den Segmenten von *A* zu *S* gleich ist wie der von *B* zu *S*?
e) Wie lautet die Antwort auf d) falls es sich um den gleichen Host handelt?

[1] SSH verwendet in der Transport Layer TCP.

Aufgabe 3: Scanning mit `nmap`

Vorsicht: Exzessives Scanning im öffentlichen LAN, z.B. Studentenwohnheim, kann zur Sperrung Ihres Zugangs führen. Nehmen Sie nur ein WLAN/LAN, das Sie selbst administrieren!

a) Verbinden Sie sich mit Ihrem Heim-WLAN oder LAN!

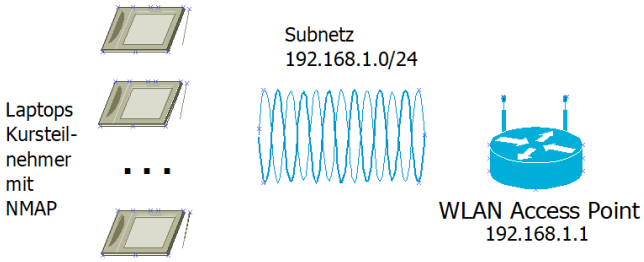
b) Falls nicht bereits vorhanden: Installieren Sie `nmap` auf Ihrem PC und starten Sie das Programm ggfs. mit Administratorrechten! Link: https://nmap.org/download.html

c) Hosterkennung[2]: `nmap -sn <CIDR-Präfix>`

- Finden Sie heraus, welche Hosts /IPs im Subnetz 192.168.1.0/24 aktiv sind?
- Erklären Sie mit einer Wireshark-Aufzeichnung was im Hintergrund passiert!

d) Port Scanning[3]: `nmap -sS <target-ip>`

- Legen Sie sich auf eine „Opfer“ IP-Adresse fest.
- Finden Sie nun heraus, welche Ports auf diesem Host offen sind!
- Schneiden Sie wieder parallel in Wireshark mit, erklären Sie was passiert.



e) Nachdem Sie aktive Hosts und Port kennengelernt haben, können Sie mit `nmap` versuchen, noch mehr herauszufinden. Wer möchte kann folgende Kommandos testen.

- Erkennen des Betriebssystems: `nmap <active port> -O <target-ip>`
- Erkennung der Anwendung hinter Port: `nmap -sV <active port> -O <target-ip>`

[2] https://nmap.org/man/de/man-host-discovery.html
[3] https://nmap.org/man/de/man-port-scanning-techniques.html