**B: SCHICHTENMODELL 2 Praxis**

**Aufgaben:**

1. Was bringt ein **Schichtmodell** wie das OSI-Modell in der Datenkommunikation **für Vorteile**?
2. Können sie alle **7 Layer des Schichtenmodells** mit Protokollbeispielen auswendig aufsagen?
3. Eine Port-Nummer (Protokoll) ist der Teil einer Netzwerk-Adresse, der die Zuordnung von TCP/UDP-Verbindungen bzw. Datenpaketen zu Client/Server-Applikationen durch das Betriebssysteme bewirkt. Zu jeder Verbindung dieser beiden Protokolle gehören zwei Ports, je einer auf Seiten des Clients und des Servers.
   1. Der gesamte Portnummer-Bereich beginnt und endet bei:
   2. Der Portnummer-Bereich der sogenannten System Ports oder Wellknown Ports beginnt und endet bei welcher Nummer?
   3. Der Portnummer-Bereich der sogenannten Registered Ports oder User Ports beginnt und endet bei welcher Nummer?
   4. Der Portnummer-Bereich der sogenannten Dynamic Ports beginnt und endet bei welcher Nummer?
4. Schreiben sie die Abkürzungen der Protokolle aus und nennen sie die entsprechenden Wellknown-Port-Nummern. Einige dieser Applikationen haben «sichere» bzw. verschlüsselte Varianten über TLS «Transport Layer Security».   
   (TLS liegt zwischen Applikations- und Transportlayer)
   1. HTTP:
   2. HTTPS (HTTP + TLS):
   3. FTP:
   4. FTPS (FTP + TLS):
   5. SMTP:
   6. SMTPS (SMTP + TLS):
   7. SMTP/MSA:
   8. POP3:
   9. POP3S (POP + TLS):
   10. IMAP:
   11. IMAPS (IMAP + TLS):
   12. SSH:
   13. SNMP:
   14. Echo/Ping:
   15. DNS:
   16. DNS mit TLS:
   17. DHCPv4:
   18. DHCPv6:
   19. Telnet:
   20. Telnet over TLS:
5. Realisieren Sie mit **CISCO-Packettracer** das folgende Netzwerk:  
   Ein Bild, das Screenshot, Diagramm, Reihe, Design enthält.

   Automatisch generierte Beschreibung  
   Das ganze Netz besteht aus zwei IP-Netzen (192.168.1.0/24 und 192.168.2.0/24).   
   In beiden Netzen sind je zwei Computer, verbunden über einen Switch.  
   Die beiden Netze sind mit einem Router verbunden.  
   Konfigurieren Sie die Geräte gemäss Adressierungen im Schema.  
   Verwenden sie die folgenden **Packettracer-Komponenten: Switch=2960; Router=1941**  
   Da der Router nur zwei Netze bedient, muss man sich hier nicht um die Routingtabelle kümmern.
   1. Kontrollieren Sie, ob alle Geräte kommunizieren können. Wie machen Sie das?
   2. Alles ok? Schauen wir etwas in den Datenverkehr, inzwischen ist schon viel kommuniziert worden:  
      Schalten sie dazu Packettracer von Realtime auf Simulation um.  
      Untersuchen Sie den Datenverkehr bei z.B. einem ping von PC1\_1 auf PC 2\_2.Was für Protokolle sind beteiligt? Sie können dazu auf die farbigen Briefumschläge klicken, die im Netzwerk ausgetauscht werden.
   3. Studieren sie das Adress-Resolution-Protokolls bzw. der Datenaustausch übers Netzwerk und der jeweilige arp-Cache des PC’s

Starten Sie die Simulation neu mit langsamer Geschwindigkeit.  
Gehen Sie in die Befehlszeile eines Computers und geben arp ein, was sehen Sie?

* 1. Pingen Sie jetzt den anderen Computer im gleichen Netzwerk. Achten Sie auf den Datenverkehr, der auf den Leitungen angezeigt wird. Was fällt auf?
  2. Untersuchen sie erneut den arp-Cache mit dem arp-Befehl. Was hat sich geändert?
  3. Pingen Sie jetzt einen Computer im anderen Netzwerk an. Achten Sie wieder Datenverkehr der auf den Leitungen angezeigt wird, die Leitungen leuchten jeweils kurz auf. Was fällt auf?
  4. Schauen Sie wieder mit arp nach was geändert hat.
  5. Erklären sie zusammenfassend, wozu ARP dient.
  6. Kreieren sie einen Webserver mit der IP-Adresse 192.168.2.13 und schliessen sie ihn an Switch-2-1 an. Im Webserver deaktivieren sie https, wir verwenden nur http. Der Webserver hat auch schon eine rudimentäre Webseite vorbereitet. Sie können von einem Client die Webseite ohne DNS wie folgt aufrufen: <http://192.168.2.13/index.html>. Im Simulationsbetriebsmodus lassen sich die angezeigten Protokolle einschränken. Zeigen sie nur arp und http an. Untersuchen sie nun Schritt für Schritt den Webseitenaufruf.

1. Das ARP-Protokoll kann auch auf ihrem Notebook in der realen Umgebung untersucht werden. Hilfreich dabei ist der Network-Sniffer Wireshark. Suchen sie in den Datenströme von und zu ihrem Notebook nach ARP-Frames. Den ARP-Vorgang können sie auslösen, wenn sie ein Router, PC, Server etc. erreichen wollen, mit dem sie vorher noch nicht kommuniziert haben. Zeigen sie sich zu verschiedenen Zeitpunkten den ARP-Cache auf Ihrem Notebook an. Wie lange bleiben die Einträge im ARP-Cache bestehen?  
   Googeln sie nach ARP-Spoofing.