**B: SCHICHTENMODELL 1 Theorie**

**Der TCP/IP-Stack im Vergleich zum ISO-OSI-Schichtenmodell**

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

Automatisch generierte Beschreibung *Weitere Beispiele zu Implementationen finden sie hier:*[*https://www.juergarnold.ch/TCPIPstack/OSILayersA.jpg*](https://www.juergarnold.ch/TCPIPstack/OSILayersA.jpg)[*https://www.juergarnold.ch/TCPIPstack/OSILayersB.jpg*](https://www.juergarnold.ch/TCPIPstack/OSILayersB.jpg))

## 

**Ein Webseitenaufruf aus Layer-Sicht**

Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Diagramm, Schrift enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Diagramm, Schrift enthält.

Automatisch generierte Beschreibung

**Der Network-Sniffer Wireshark - Wiresharkfilter anwenden**

Um die Datenflut etwas einzudämmen, sollte man bei Wireshark Filter einsetzen. Einerseits gibt es Capture-Filter und andererseits Display-Filter. Capture-Filter (z.B. tcp port 80) sind nicht mit Display-Filtern (z.B. tcp.port == 80) zu verwechseln. Capture-Filter sind viel eingeschränkter und werden verwendet, um die Grösse einer Rohpaketerfassung zu reduzieren. Display-Filter werden verwendet, um einige Pakete aus der Paketliste zu verstecken.

Capture-Filter werden vor Beginn einer Paketerfassung festgelegt und können während der Erfassung nicht geändert werden. Display-Filter hingegen haben diese Einschränkung nicht und können jederzeit geändert werden. Im Hauptfenster findet man den Capture-Filter direkt über der Schnittstellenliste und im Schnittstellendialog. Der Display-Filter kann über der Paketliste geändert werden. Capture-Filter haben eine andere Syntax als Display-Filter! Im Internet findet sich dazu viel entsprechendes Material. Zum Beispiel hier: https://wiki.wireshark.org/Home

Hier ein paar nützliche Display-Filter:

Capture-Fenster löschen, ohne Wireshark neu zu starten und Filter neu setzen: (3 Versionen!)  
→ Auf die grüne Haifischflosse neben der roten "Stop" Taste klicken  
→ Menü Aufzeichnen > Neustart  
→ Ctrl-R

Zeigt nur den Datenverkehr im 192.168.1.0-Netzwerk:  
ip.src==192.168.1.0/24 and ip.dst==192.168.1.0/24

Zeigt nur den Datenverkehr von und zu dieser IP-Adresse:  
ip.addr == 192.168.1.15 ist identisch mit  
ip.src == 192.168.1.15 or ip.dst == 192.168.1.15

Zeige allen Datenverkehr ausser den von und zu dieser IP-Adresse  
! ( ip.addr == 192.168.1.15 )

Zeigt nur SMTP (Port25) und ICMP-Datenverkehr  
tcp.port eq 25 or icmp

Zeigt nur DHCP-Datenverkehr:  
dhcp.option.type == 53  
  
DNS Anfrage für juergarnold.ch  
dns.qry.name == "juergarnold.ch"

Verknüpfung:  
dns and ip.dst==159.25.78.7 or dns and ip.src==159.57.78.7

Zeigt «Post» von einem (unverschlüsselten!) Webseitenformular:  
http.request.method == "POST"  
  
*Tipp : Um mit Wireshark oberhalb Layer-4 mitzulesen, muss man zuerst einmal eine unverschlüsselte Webseite finden, die sind heutzutags – mit gutem Grunde – nämlich meistens verschlüsselt. Eine Ausnahme ist z.B.* [*http://neverssl.com*](http://neverssl.com)

**Wireshark und verschlüsselte HTTPS-Webseiten:**Beim Aufruf von verschlüsselten Webseiten wirkt oberhalb TCP das Verschlüsselungsprotokoll SSL/TLS (Heutzutags TLS, SSL war sein Vorgänger). Das bedeutet, dass Wireshark oberhalb TLS nichts anzeigen kann, da verschlüsselt. Dies ist auch erwünscht, weil dabei für Drittpersonen nicht einsehbar ist, was Webclient und Webserver miteinander austauschen, insbesondere Formulare, Passwörter etc. Ab HTTP 1.1 wird bei einem Webseitenaufruf die URL mitgegeben, weil es ja durchaus üblich ist, dass unter einer IP-Adresse mehrere Webseiten gehostet werden und darum der Server wissen muss, welche Webseite nun gemeint ist. Nun könnte man meinen, mit TLS wäre es nicht mehr möglich herauszufinden, welche Webseite aufgerufen wurde, weil sich diese Angabe nur im Application-Layer befindet. Dem ist aber nicht so. Im TLS-Layer findet man nämlich auch einen entsprechenden Hinweis. Und das geht so:

* Wireshark-Displayfilter: ssl.handshake.extensions\_server\_name (Zeigt alle "Client Hello")
* Eine der angezeigten Zeilen auswählen und TLS (Transport Layer Security) aufklappen.
* Danach: TLSv1.x Record Layer: Handshake Protocol: Client Hello
* Danach: Handshake Protocol: Client Hello
* Danach: Extension: server\_name
* Danach: Server Name Indication extension
* Und man erhält: Server Name: xxxxxx.yyyyy.zzz
* Nun könnte man Rechtsklick → "Als Spalte anwenden" und hätte im oberen Fenster alle URLs angezeigt.

*Hintergrund-Info: Server Name Indication (SNI) ist eine Erweiterung von TLS, um mehrere verschlüsselte Webseiten auf einem Server aufzurufen. Jede Domain hat ein anderes Zertifikat und der Server muss wissen, welches er liefern muss. Das wird ihm unverschlüsselt über die SNI vom Client geliefert.*

**B: SCHICHTENMODELL 2 Praxis**

**Aufgaben:**

1. Was bringt ein **Schichtmodell** wie das OSI-Modell in der Datenkommunikation **für Vorteile**?  
   -Bei Problemen lässt sich die Ursache leichter Identifizieren.  
   -Flexible Standardisierung da die Protokolle nicht spezifiziert werden müssen sondern die Aufgaben davon.  
   - Das Model stellt Standards fest.  
   Man kann mit dem Model komplexere Systeme organisieren und ordnen.
2. Können sie alle **7 Layer des Schichtenmodells** mit Protokollbeispielen auswendig aufsagen?  
   1. Physical Layer,  
   2.Data Link Layer,   
   3.Network Layer ,  
   4.Transport Layer,   
   5.Session layer,   
   6.Presentation layer,   
   7.ApplicationLayer  
   Nein leider konnte ich nicht alle auswendig sagen.
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:  
      0-65535
   2. Der Portnummer-Bereich der sogenannten System Ports oder Wellknown Ports beginnt und endet bei welcher Nummer?  
      0 bis 1023
   3. Der Portnummer-Bereich der sogenannten Registered Ports oder User Ports beginnt und endet bei welcher Nummer?  
      1024 bis 49151
   4. Der Portnummer-Bereich der sogenannten Dynamic Ports beginnt und endet bei welcher Nummer?  
      49152 bis 65535
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: Hypertext Transfer Protocol :80
   2. HTTPS (HTTP + TLS): Hypertext transfer Protocol Secure :443
   3. FTP: File Transport Protocol: 21, 20
   4. FTPS (FTP + TLS): File Transport Protocol Secure : 990, 989
   5. SMTP: Simple Mail Transport Protocol: 25
   6. SMTPS (SMTP + TLS): Simple Mail Transfer Protocol Secure: 587
   7. SMTP/MSA: Mail Submission Agent: 587
   8. POP3: Post Office Protocol version 3: 110
   9. POP3S (POP + TLS): Post Office Protocol version 3 Secure: 995
   10. IMAP: Internet Message Access Protocol 143
   11. IMAPS (IMAP + TLS): Internet Message Access Protocol 993
   12. SSH: Secure Shell : 22
   13. SNMP: Simple Network Management Protocol: 161
   14. Echo/Ping: Port 7
   15. DNS:Domain Name System: 53
   16. DNS mit TLS: DNS over TLS DoT 853
   17. DHCPv4: Dynamic host Protocol version 4: 67
   18. DHCPv6: Dynamic host Protocol : 546
   19. Telnet:Telnet: 23
   20. Telnet over TLS: Telnet over Transport Layer Security: 992
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?  
      Mit einem gerät ein anderes Gerät im anderen Subnetz anpingen und schauen ob dieser erreicht wird.
   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.  
      Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

      Automatisch generierte Beschreibung  
      Protokol ICMP wird verwendet.
   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?  
Beim eingeben von arp -a zeigt mir die tabele die Mac adresse des Routers mit dem jeweiligen Interface an.

* 1. Pingen Sie jetzt den anderen Computer im gleichen Netzwerk. Achten Sie auf den Datenverkehr, der auf den Leitungen angezeigt wird. Was fällt auf?  
     Ein Bild, das Text, Screenshot, Display, Schrift enthält.

     Automatisch generierte Beschreibung  
     Die Nachricht gelangt direkt auf den Client und kommt wieder zurück
  2. Untersuchen sie erneut den arp-Cache mit dem arp-Befehl. Was hat sich geändert?  
     Die Mac addresse wurde in die tabelle eingetragen  
     Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

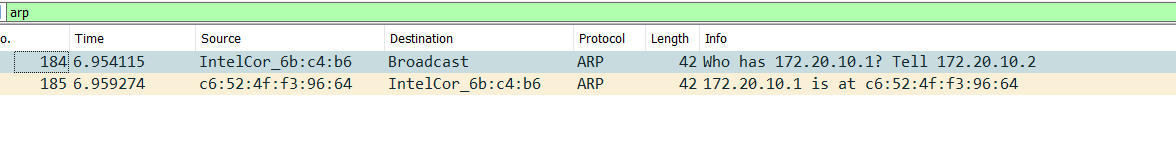
     Automatisch generierte Beschreibung
  3. Pingen Sie jetzt einen Computer im anderen Netzwerk an. Achten Sie wieder Datenverkehr der auf den Leitungen angezeigt wird, die Leitungen leuchten jeweils kurz auf. Was fällt auf?  
     das Paket geht über den Gateway und direkt auf den Client und wieder zurück.  
     Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

     Automatisch generierte Beschreibung
  4. Schauen Sie wieder mit arp nach was geändert hat.  
     es hat sich nichts geändert. Die arp Tabelle ist gleich geblieben.
  5. Erklären sie zusammenfassend, wozu ARP dient.  
     ARP wird benötigt um IPV4 Adressen in Mac Adressen aufzulösen.
  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.  
       
     Es die anfrage wurde an alle geräte gesendet und nur der server hat zurückgeantwortet  
     Ein Bild, das Text, Screenshot, Software, Display enthält.

     Automatisch generierte Beschreibung  
       
     Ein Bild, das Text, Elektronik, Screenshot, Display enthält.

     Automatisch generierte Beschreibung  
       
     Ein Bild, das Text, Elektronik, Screenshot, Display enthält.

     Automatisch generierte Beschreibung

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.  
     
   ARP Spoofing: ein gemeinnütziges gerät antwortet schneller zu einer ARP anfrage sodass danach immer dieses Gerät eine Antwort erhält und nicht das vorhergesehene Gerät  
     
   der ARP-Cache kann bis zu 20 Minuten lang gespeichert werden oder bis ein Neustart des Systems getätigt wurde.  
   

## **Unterrichtsreflexion dieses Kapitels-B**

* Unterrichtsziele:  
  -Aufbau der TCP/IP Model verstehen  
  - Aufbau von OSI Model verstehen  
  -Der Unterschied beider Modele kennen.

- Die 4 bzw. 7 Layer kennen und verstehen, wie dieser aufgebaut wird.  
- Die Netzwerkprotokole kennen und wie d

* Unterrichtsresultate:  
  Gelernt wie eine http Anfrage aufgebaut ist und welche Applikations Ports benötigt werden.  
  Das Anwenden von Cisco Packetracer gelernt die Funktionen wie CMD oder http requests zu machen.  
  Die verschiedenen Applikationsprotokolle kennengelernt und dessen Port gelernt.  
  Gelernt dass die Mac Addresse immer benötigt wird.
* Probleme/Knacknüsse:  
  ARP commands kennen.  
  Cisco packet tracer event Viewer anschauen und Filterung finden.  
  Verständnis wieso sich die Absender Adresse der IP nicht ändert bei änderung des Subnetzes  
  Wie genau der ARP funktioniert.
* Neu Tools:
* Offene Fragen: Wie filtere ich die ARP Frames auf Wireshark?