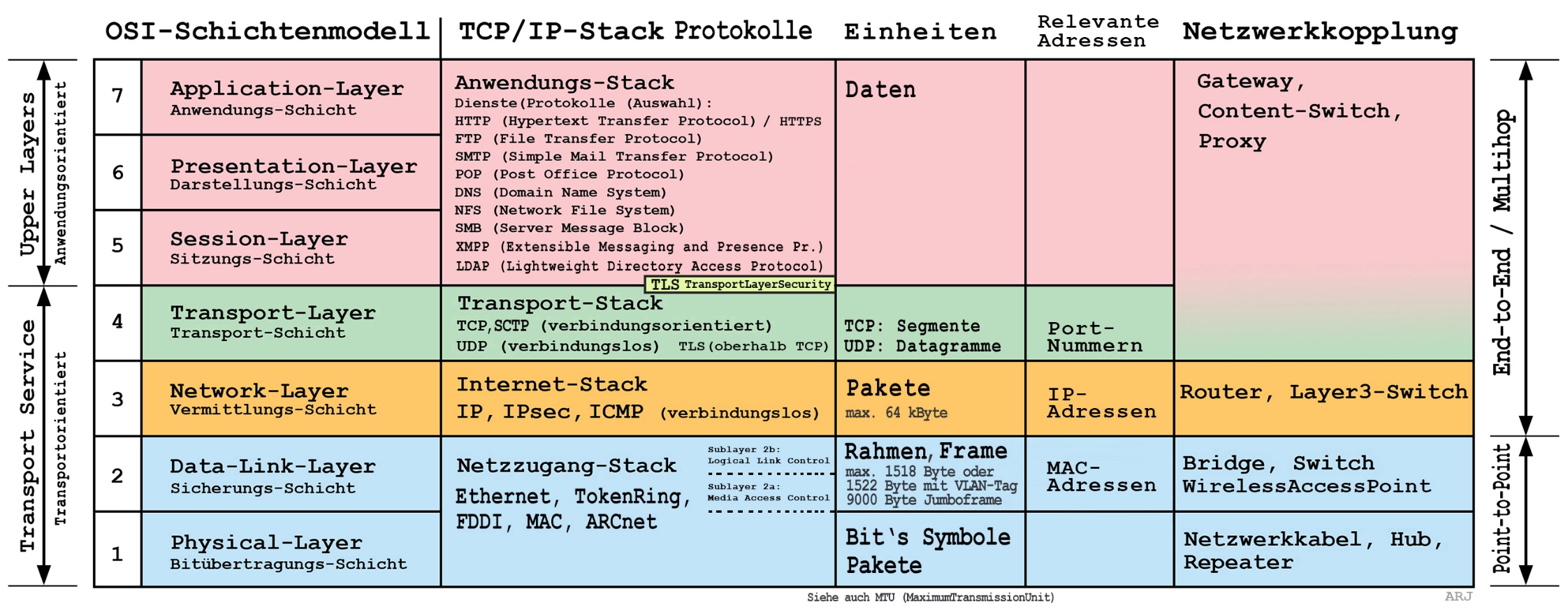
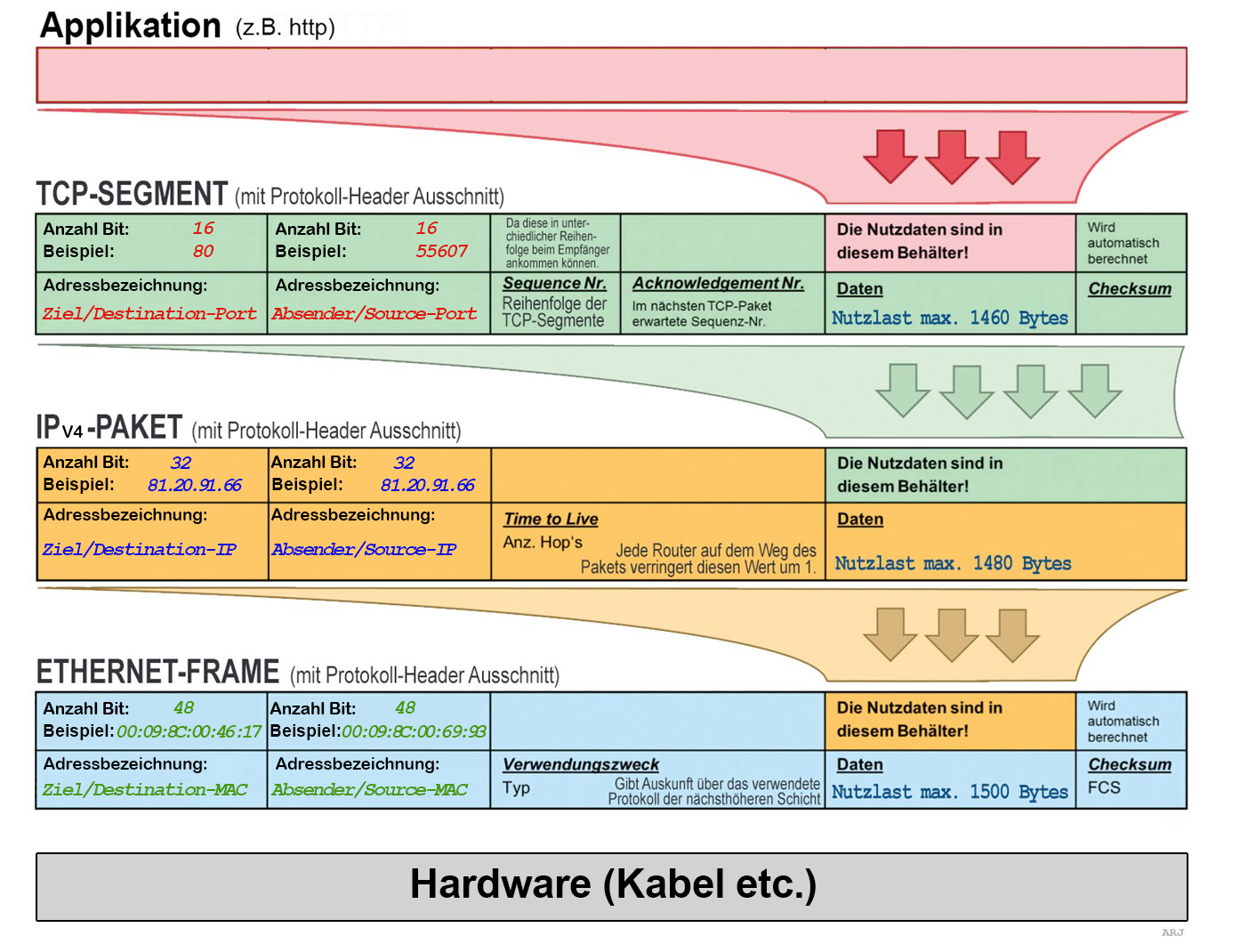
**B: SCHICHTENMODELL 1 Theorie**

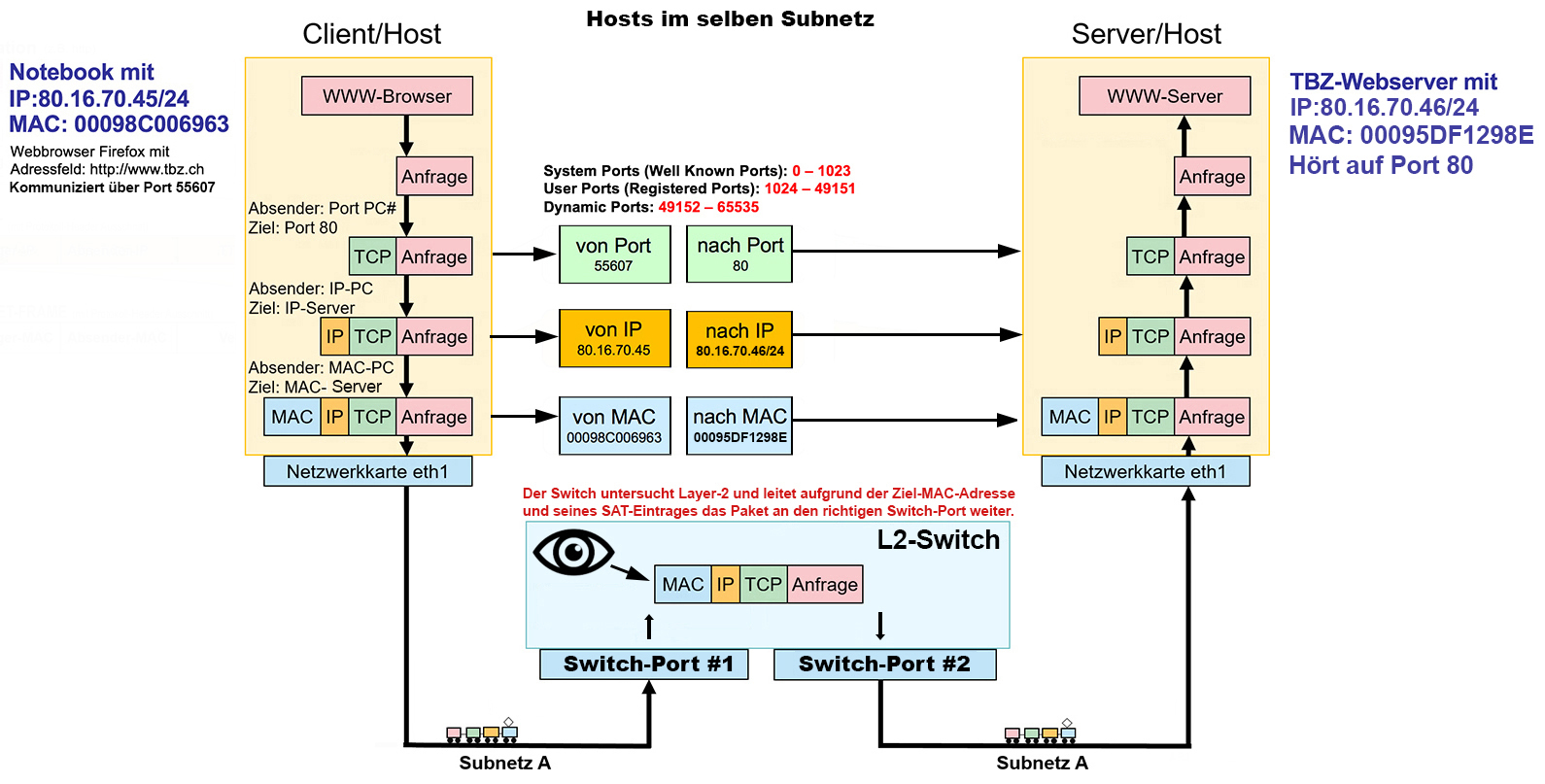
**Der TCP/IP-Stack im Vergleich zum ISO-OSI-Schichtenmodell**

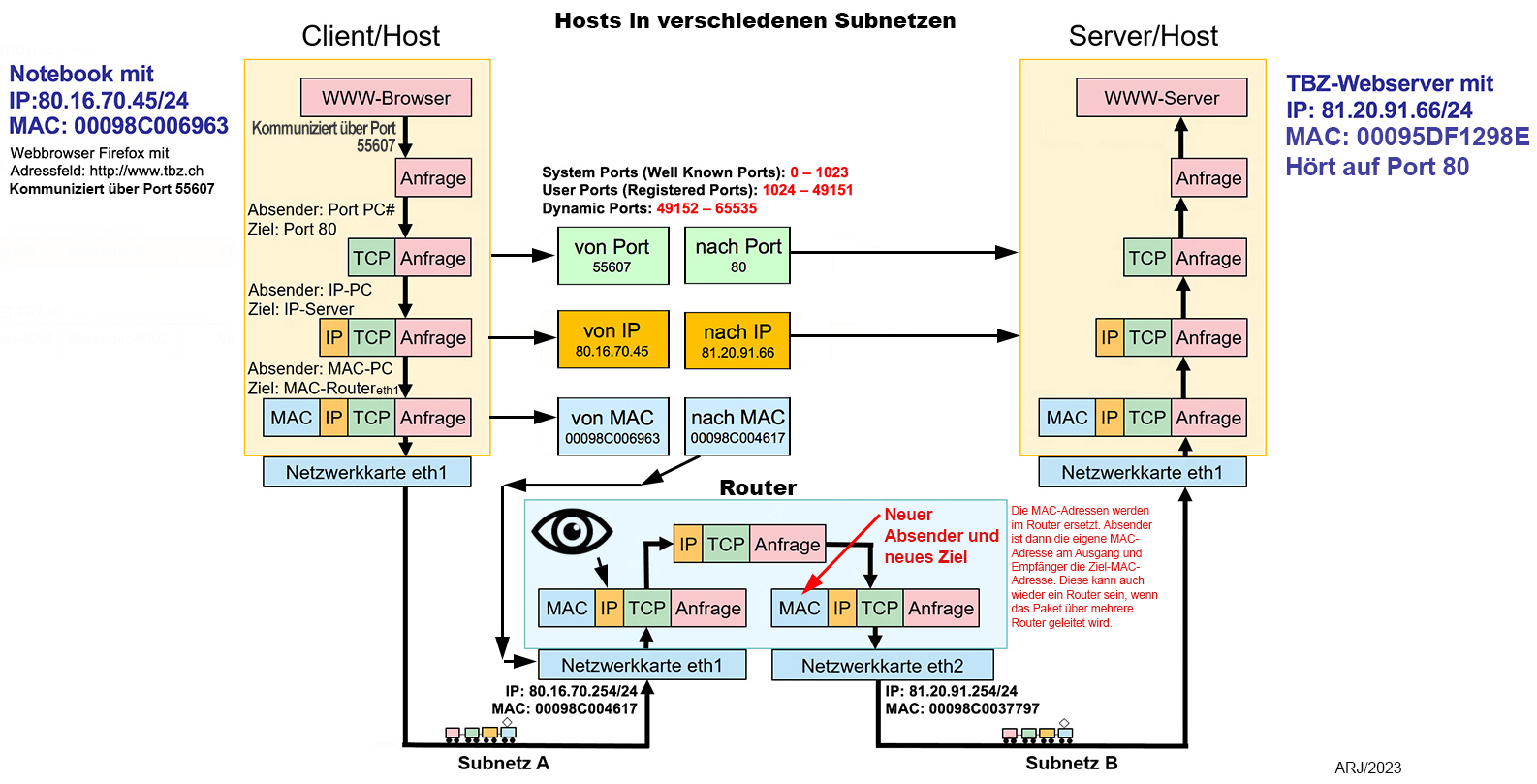
 *Weitere Beispiele zu Implementationen finden sie hier:*[*https://www.juergarnold.ch/TCPIPstack/OSILayersA.jpg*](https://www.juergarnold.ch/TCPIPstack/OSILayersA.jpg)[*https://www.juergarnold.ch/TCPIPstack/OSILayersB.jpg*](https://www.juergarnold.ch/TCPIPstack/OSILayersB.jpg))

## 

**Ein Webseitenaufruf aus Layer-Sicht**







**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.*