



SNEAK PEEK

Cisco Community Live event

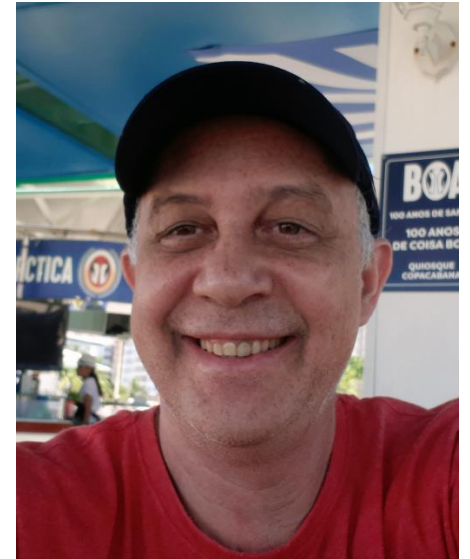
Basic Wireshark for Networking students

April 14th, 2020

with Dr. Moises Andre Nisenbaum

Register Now:

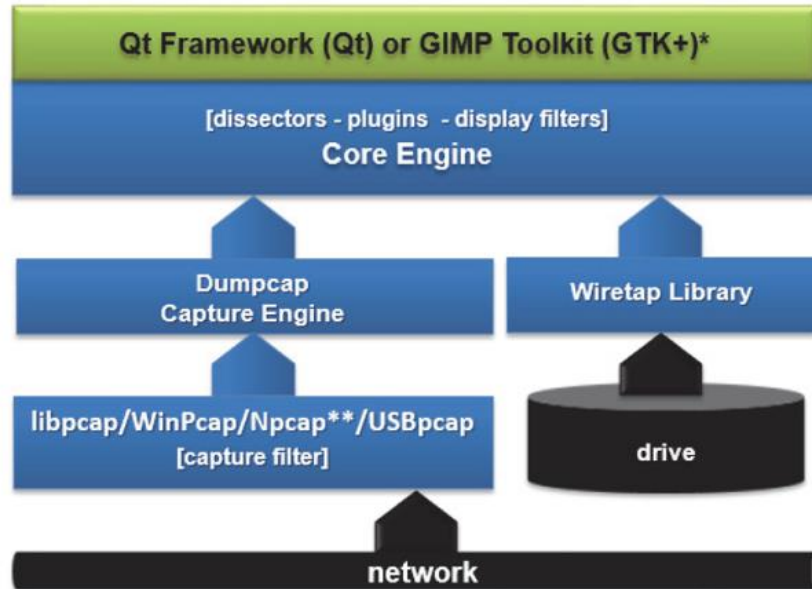
<https://bit.ly/cl-EN-apr2020>



Agenda

- Introduction to Wireshark and typical applications
- Explanation of basic TCP and UDP
- How to use SPAN to capture packets
- Explanation of some ICMP and OSPF messages

How Wireshark captures (and shows) traffic



* GTK support will eventually be discontinued in Wireshark v2.

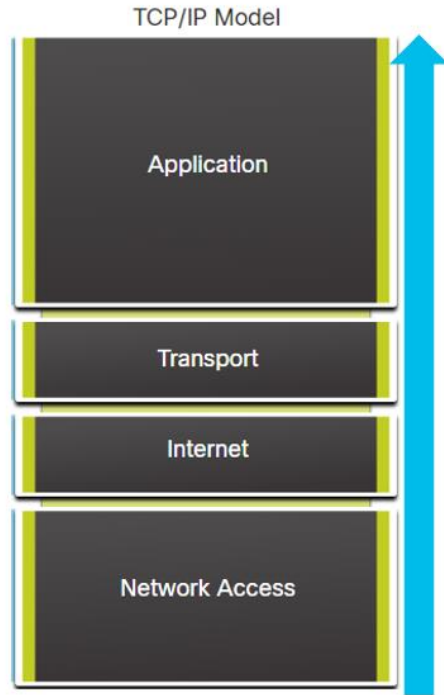
** Early releases of Wireshark v2 do not include Npcap – visit Npcap.org for more information.

Figure 1. How Wireshark handles traffic from a live capture or from a saved trace file.

Source: Chappell, L. (2017). Wireshark
101

- Live capture or saved file
- Special link-layer drivers:
 - Windows – npcap
 - Linux – libcap
- Default trace file format:
.pcapng
- Core Engine: Wireshark goldmine
- Qt Framework: User Interface

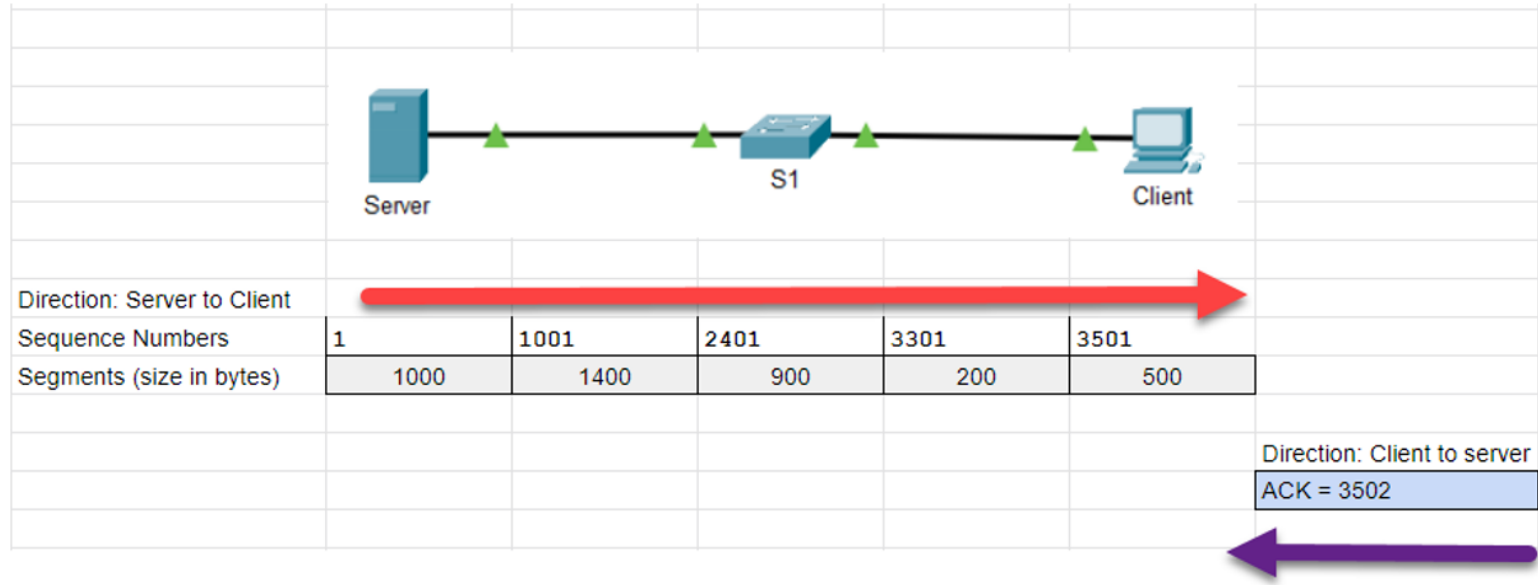
TCP/IP model and wireshark details pane



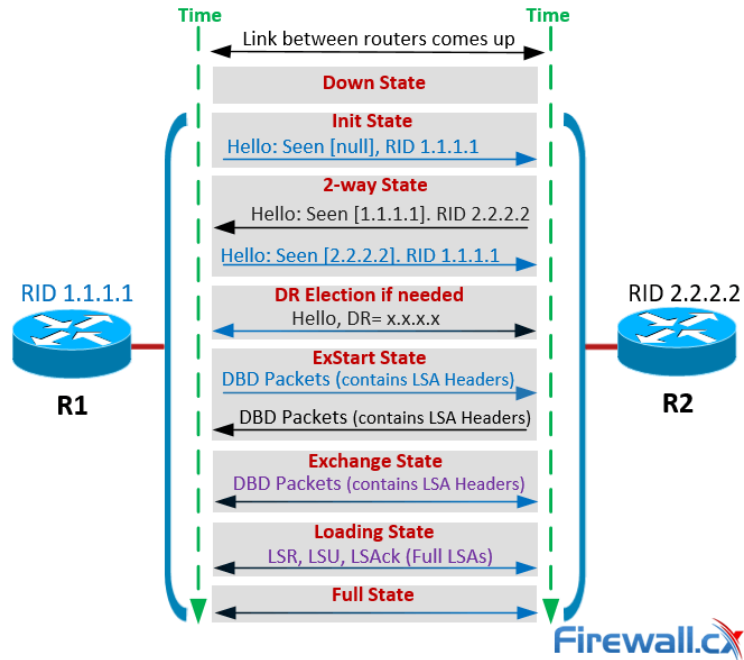
The image shows a screenshot of the Wireshark details pane for a captured frame. The pane lists several protocol layers, with the Hypertext Transfer Protocol layer highlighted in blue. A blue arrow points downwards from the top of the details pane towards the Network Access layer of the TCP/IP model diagram.

```
> Frame 86: 555 bytes on wire (4440 bits), 555 bytes captured  
> Ethernet II, Src: Dell_fb:ce:85 (84:7b:eb:fb:ce:85), Dst: AF  
> Internet Protocol Version 4, Src: 10.10.9.128, Dst: 128.59.1  
> Transmission Control Protocol, Src Port: 4027, Dst Port: 80,  
> Hypertext Transfer Protocol
```

Sequence & Ack numbers. Window size. (demo 5)

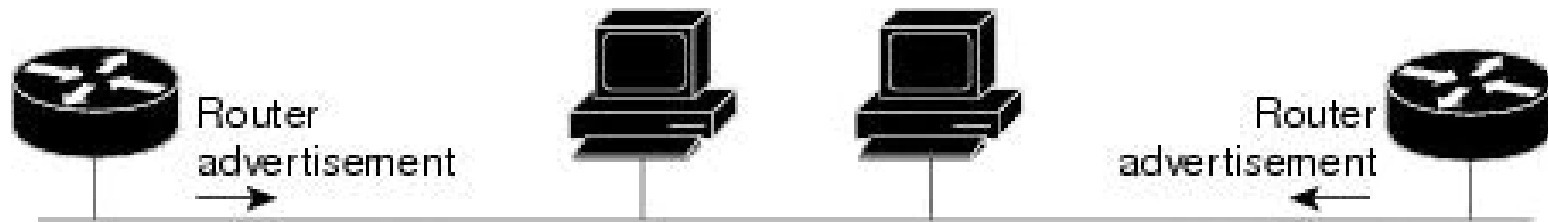


OSPF states and messages



Source: <http://www.firewall.cx/networking-topics/routing/ospf-routing-protocol/1142-ospf-adjacency-neighbor-states-forming-process.html>

IPv6 Neighbor Discovery: RA Message



Router advertisement packet definitions:

ICMPv6 Type = 134

Src = router link-local address

Dst = all-nodes multicast address

Data = options, prefix, lifetime, autoconfig flag

52.074

Check out some additional information on [Wireshark](#) on the [Cisco Community](#) or [Cisco.com](#)

UNDERSTANDING SIP TRACES

<https://community.cisco.com/t5/collaboration-voice-and-video/understanding-sip-traces/thread/3137704>

Wireshark emulator

https://www.cisco.com/assets/sol/sb/WAP581_Emulators/WAP581_Emulator_v1-0-1-3/help/t_Wireshark.html

If you are not yet a registered user on the community, [Click here](#) to register and become an active participant on the community.



Hope you enjoyed this little peek into the live event.
Remember it was just a peek. April 14th you get a chance to see the whole thing.



Register Now: <https://bit.ly/cl-EN-apr2020>

At the event you will be able to learn so much more and get a chance to submit questions for the expert to answer during the broadcast.
We'll see you there!