Network Sniffing

Chapter 1

Network & Security

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

SUMMARY OF CHAPTER 1

- TCP/IP Basics
- Sniffing Data on the Network
- Hub, Switch, and Router
- Conclusion and References

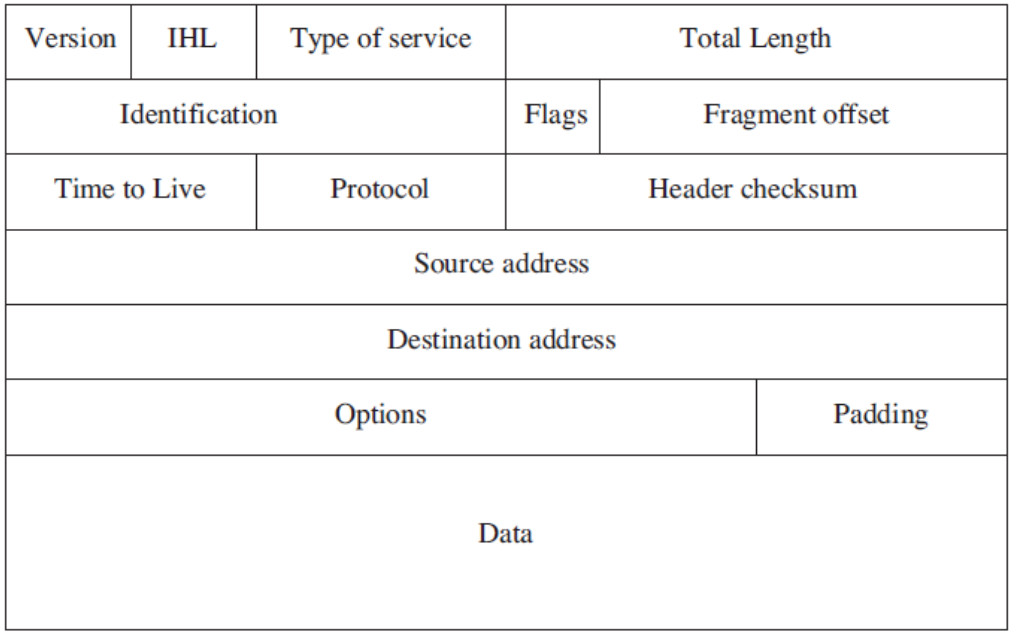
TCP/IP BASICS

- TCP/IP Basics
- Sniffing Data on the Network
- Hub, Switch, and Router
- Conclusion and References

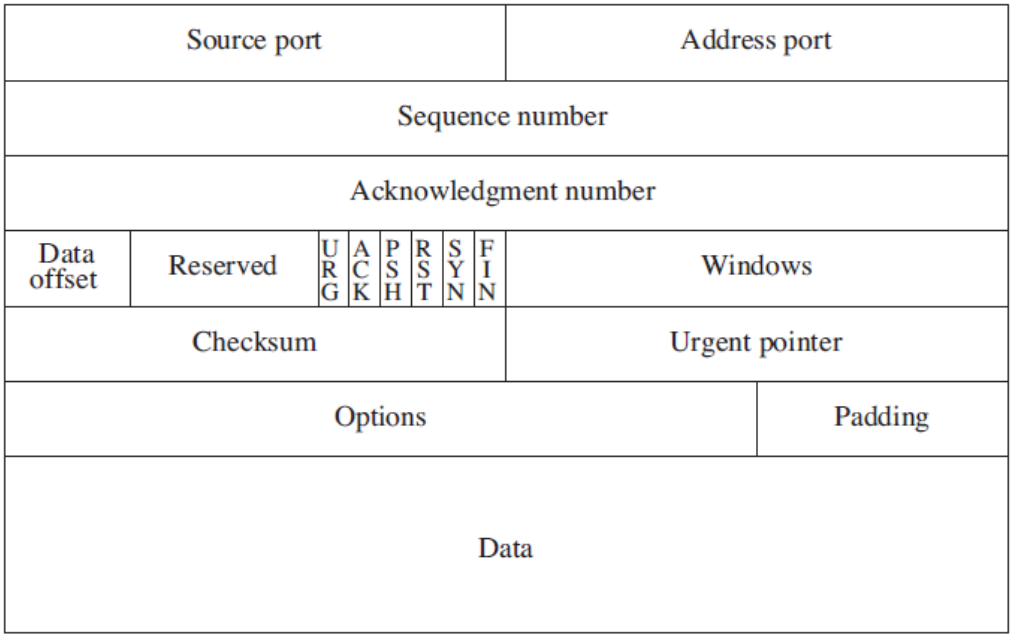
Layered Models

<table>
<tr><th>TCP/IP</th><th>ISO</th><th>Protocols</th></tr>
<tr><td rowspan="3">Application</td><td>Application</td><td rowspan="3">SMTP, HTTP</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td><td>TCP, UDP</td></tr>
<tr><td>Internet</td><td>Network</td><td>IP, X25 PLP</td></tr>
<tr><td rowspan="2">Network Access</td><td>Data Link</td><td rowspan="2">Ethernet, PPP, X25 LAPB</td></tr>
<tr><td>Physical</td></tr>
</table>

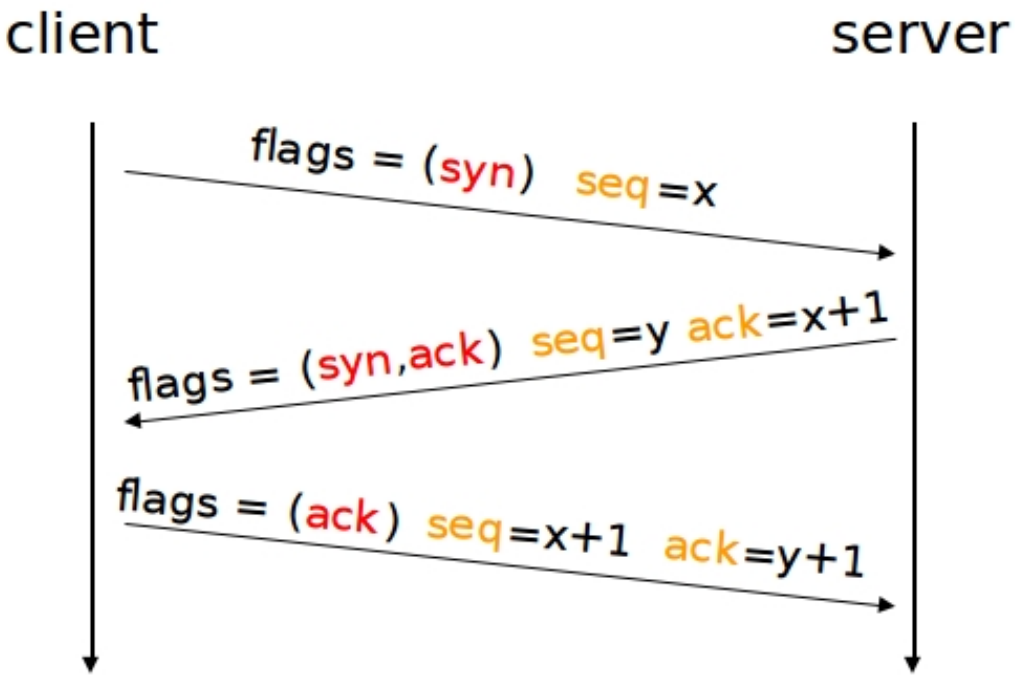
IP Header


Version
IHL
Type of service
Total Length
Identification
Flags
Fragment offset
Time to Live
Protocol
Header checksum
Source address
Destination address
Options
Padding
Data

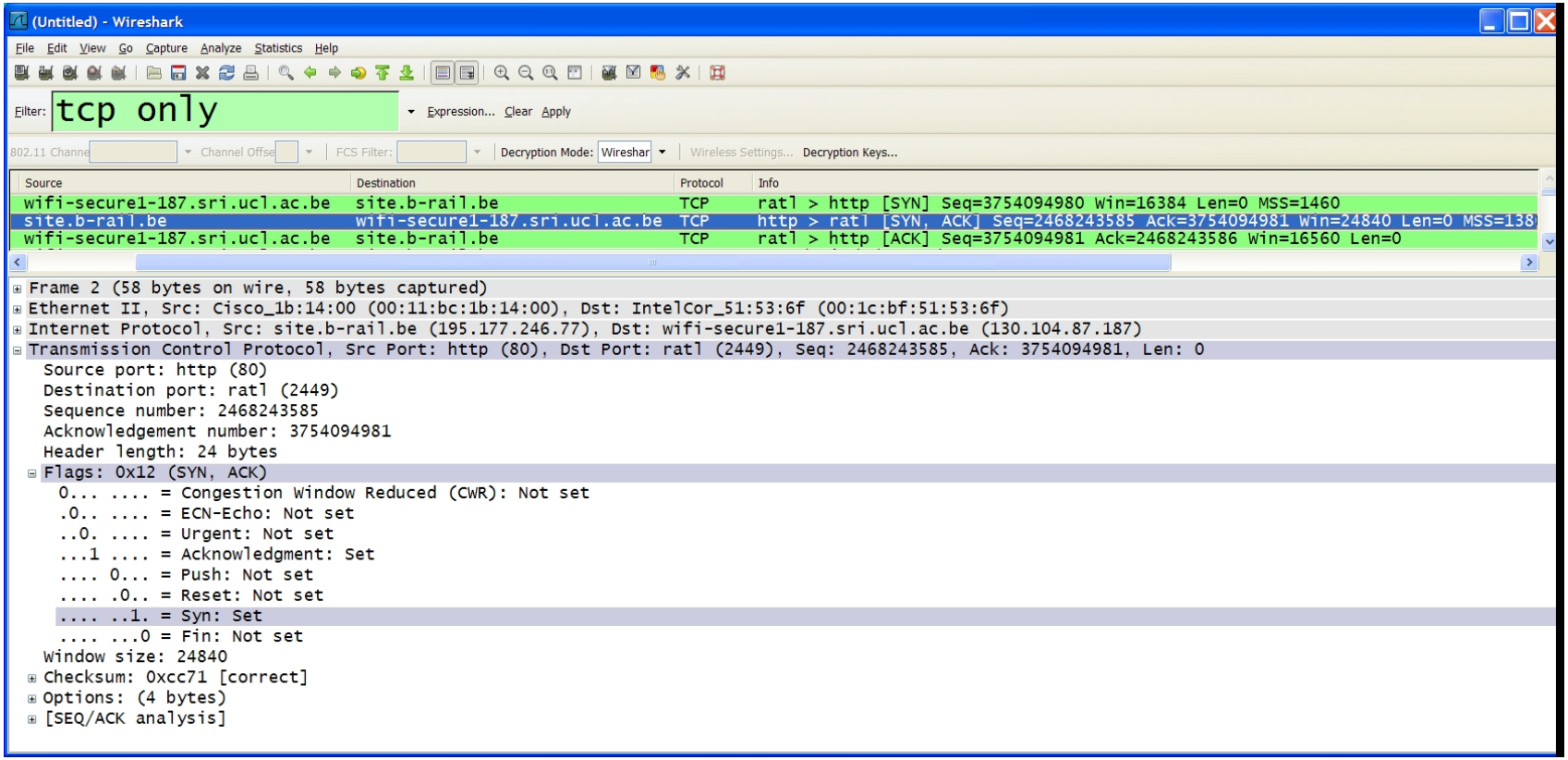
TCP Header


Source port
Address port
Sequence number
Acknowledgment number
Data offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Windows
Checksum
Urgent pointer
Options
Padding
Data

TCP 3-way Handshake



TCP 3-way Handshake (Wireshark)




```
ratl > http [SYN] Seq=3754094980 Win=16384 Len=0 MSS=1460
http > ratl [SYN, ACK] Seq=2468243585 Ack=3754094981 Win=24840
ratl > http [ACK] Seq=3754094981 Ack=2468243586 Win=16560 Len=0
GET /main/F/ HTTP/1.1
```

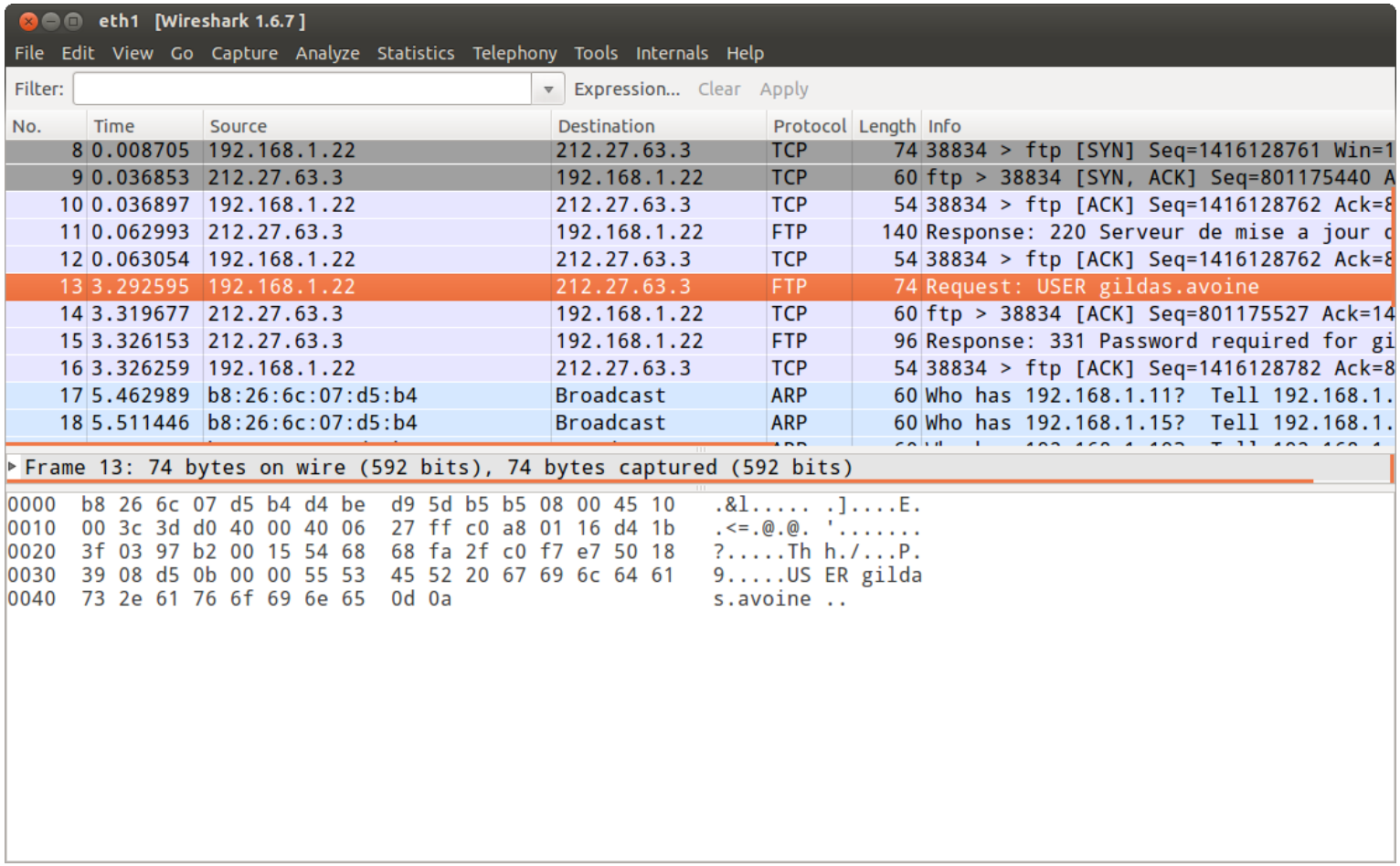
SNIFFING DATA ON THE NETWORK

- TCP/IP Basics
- Sniffing Data on the Network
- Hub, Switch, and Router
- Conclusion and References

Sniffing Passwords

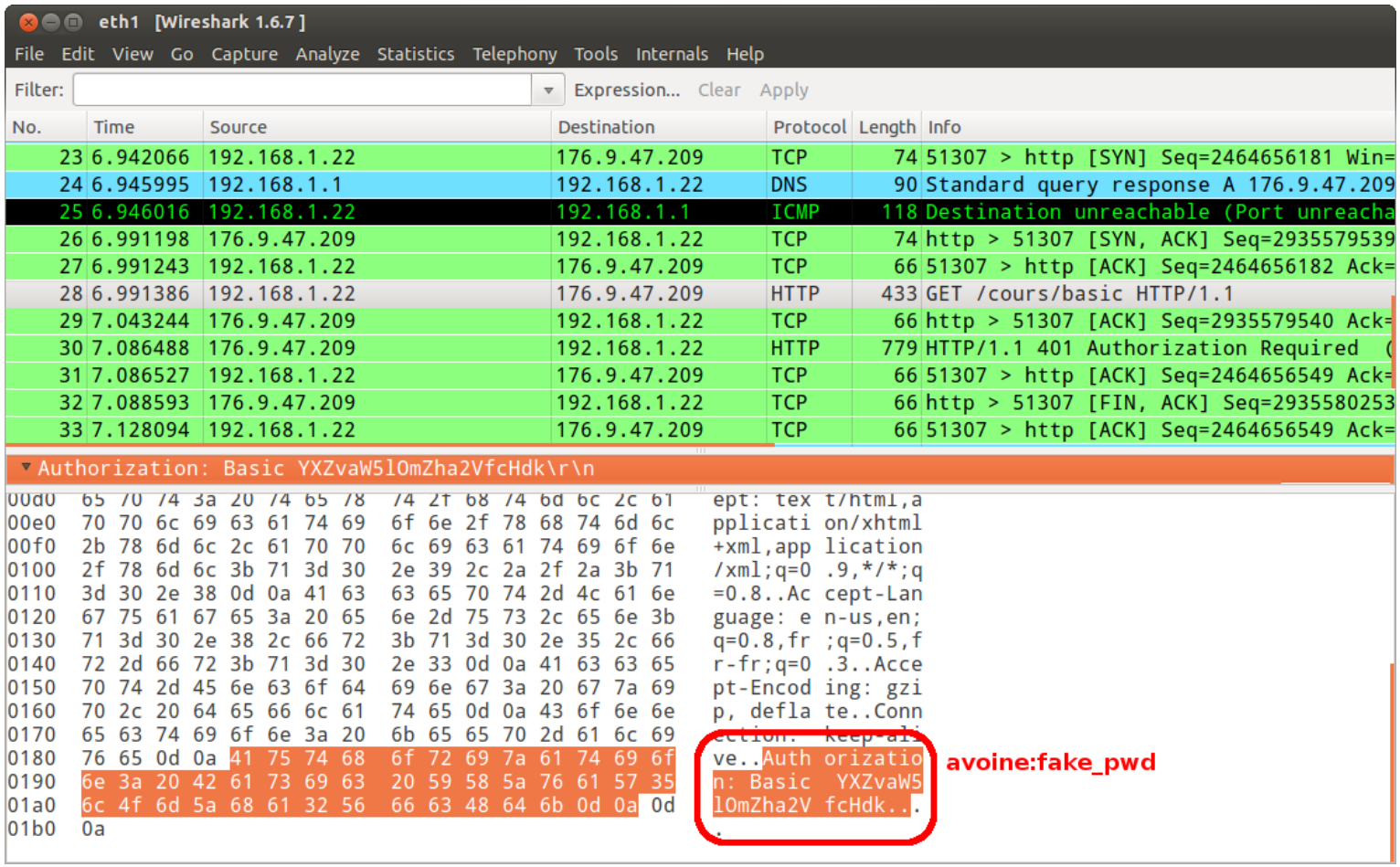
- Many protocols use clear text authentication.
- By eavesdropping traffic on a network section, we can obtain usernames and passwords.
- A password gives access to a remote machine from which we can sniff and further obtain new passwords.

FTP Session Sniffed with Wireshark



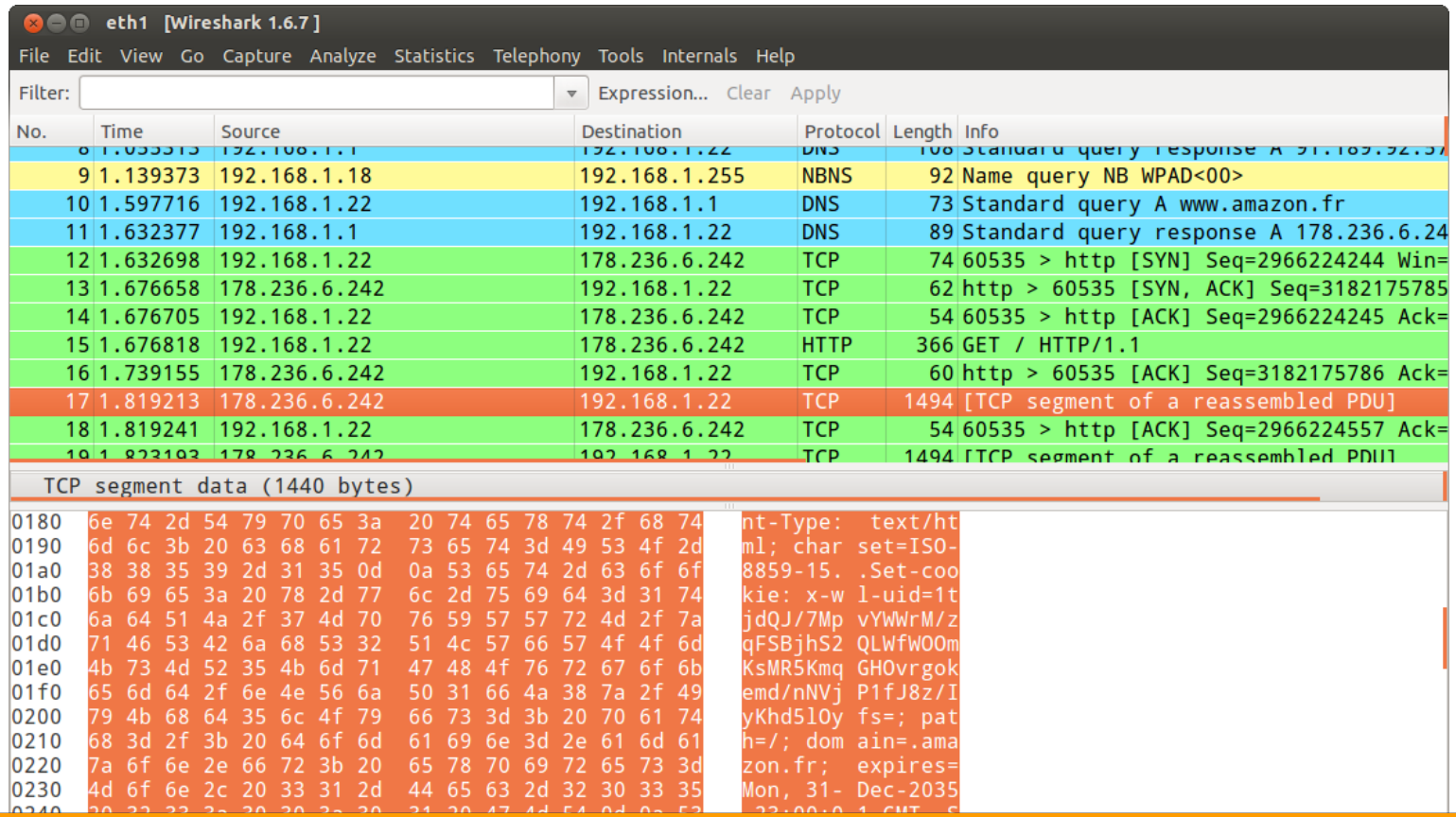
Apache Authentication Sniffed with Wireshark

- In Basic authentication mode, password is sent in the clear.
- The Digest mode is does not reveal the password.



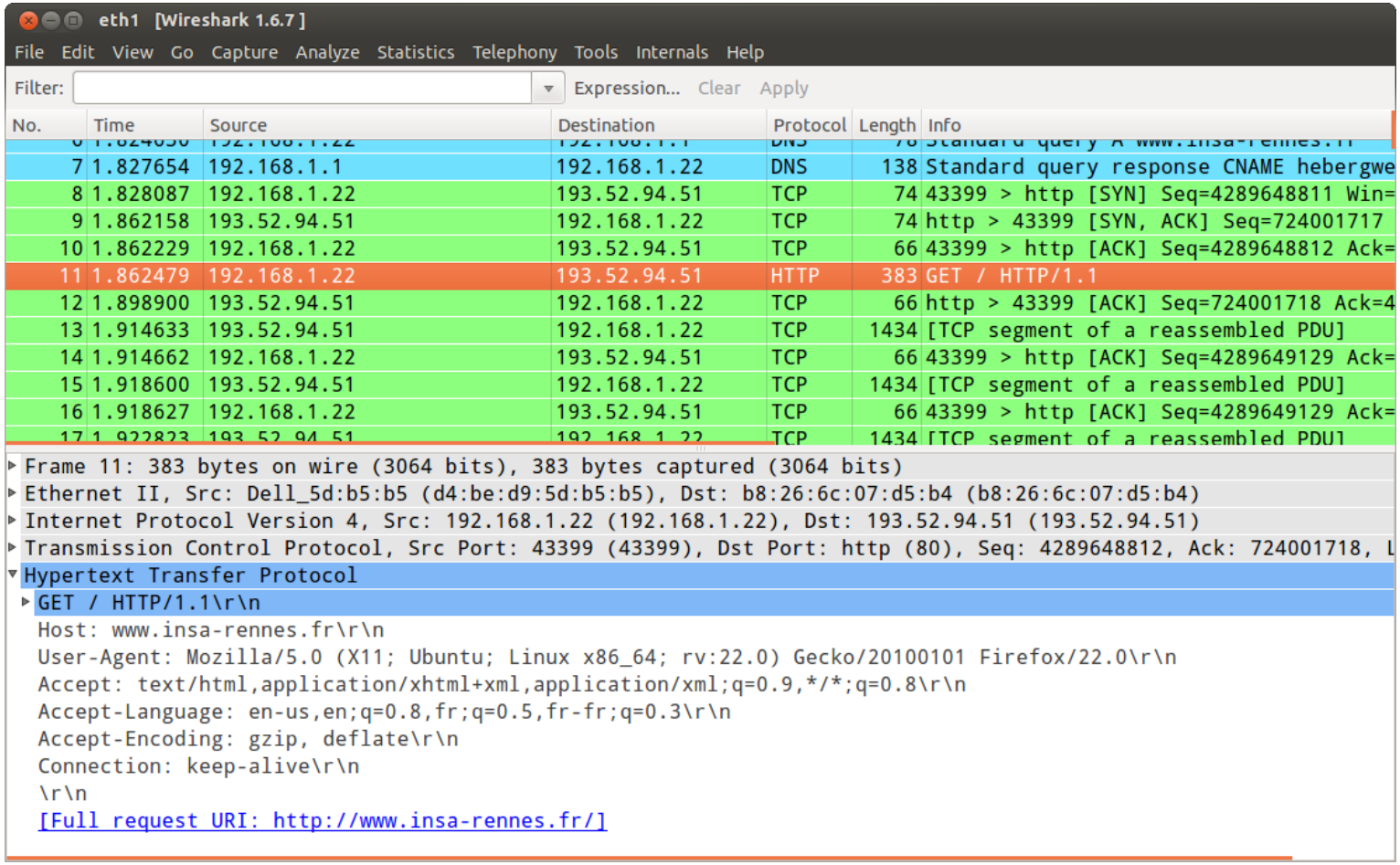
Cookies

- Cookie: information sent by a web server and stored by the user.
- Only the cookie owner (server domain) can get access to it.
- Cookies allow web servers to simulate http sessions.
- Users can potentially be tracked.



Browser Fingerprinting

- Browsers leak information about the user's environment.
- Users can potentially be tracked. See www.amiunique.org.



HUB, SWITCH, AND ROUTER

- TCP/IP Basics
- Sniffing Data on the Network
- Hub, Switch, and Router
- Conclusion and References

Hub

- A hub is used to connect segments of a LAN.
- When a packet arrives at a port of the hub, it is broadcasted to the other ports so that all devices on any segment of the LAN can see that packet.
- The network bandwith is shared by all the devices on the LAN.

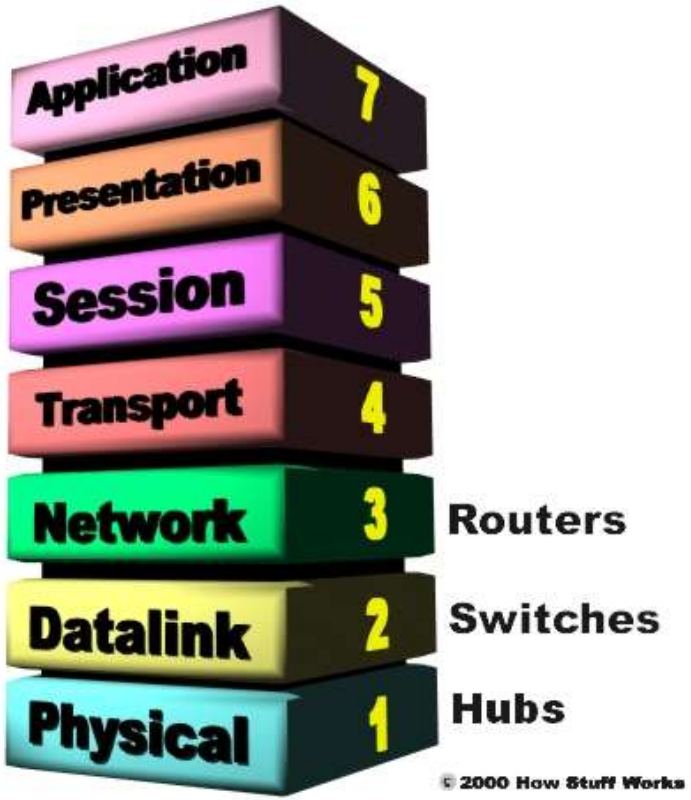
Switch

- A switch is used to connect segments of a LAN.
- A switch filters and forwards packets between LAN segments.
- A switch operates at the data link layer (layer 2) and sometimes the network layer (layer 3).
- It keeps a record of the MAC addresses of the connected devices: when a frame is received, it knows which port to send it to.

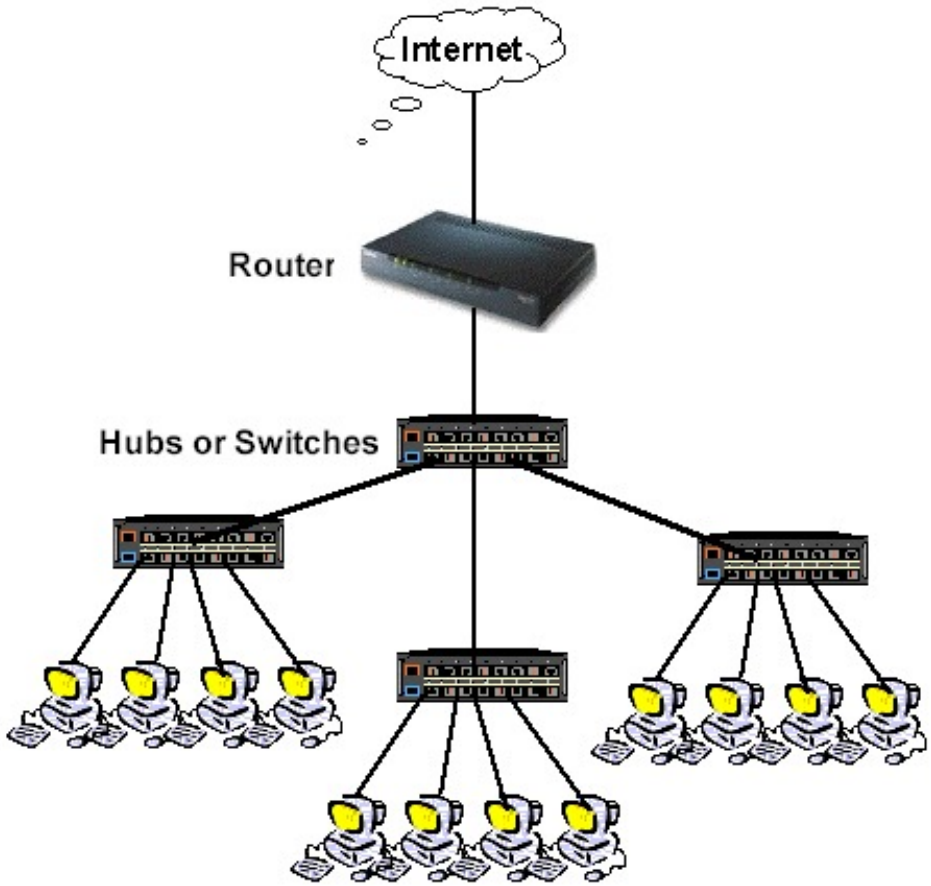
Router

- A router is typically used to connect 2 LANs or a LAN with ISP.
- Routers are located at gateways.
- Routers use forwarding tables to determine the best path for forwarding the packets.
- They communicate with each other using procotocols as ICMP.
- A router is typically connected to a DSL modem for broadband Internet service.
- A router commonly integrates a switch.

Hubs, Switches, and Routers through the Layers

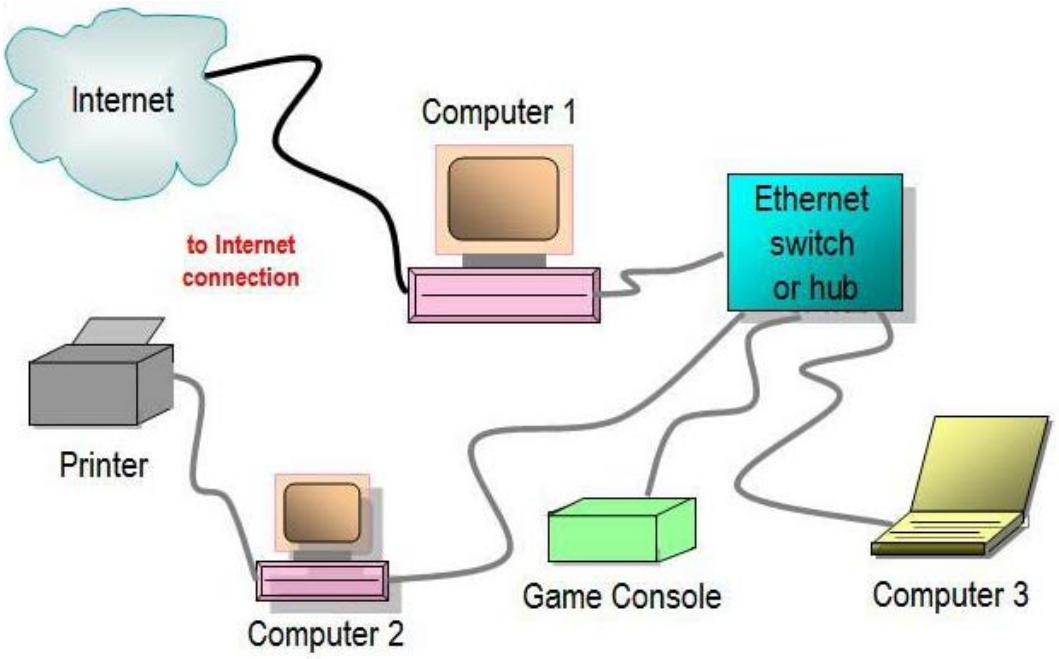


Network Example 1/4



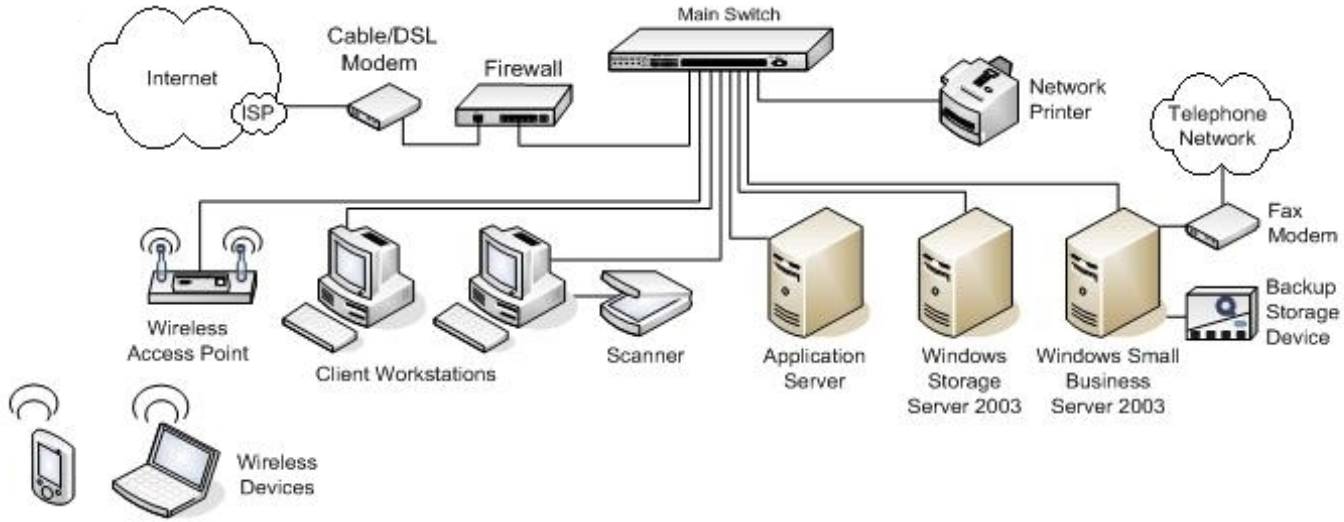
www.practicallynetworked.com

Network Example 2/4



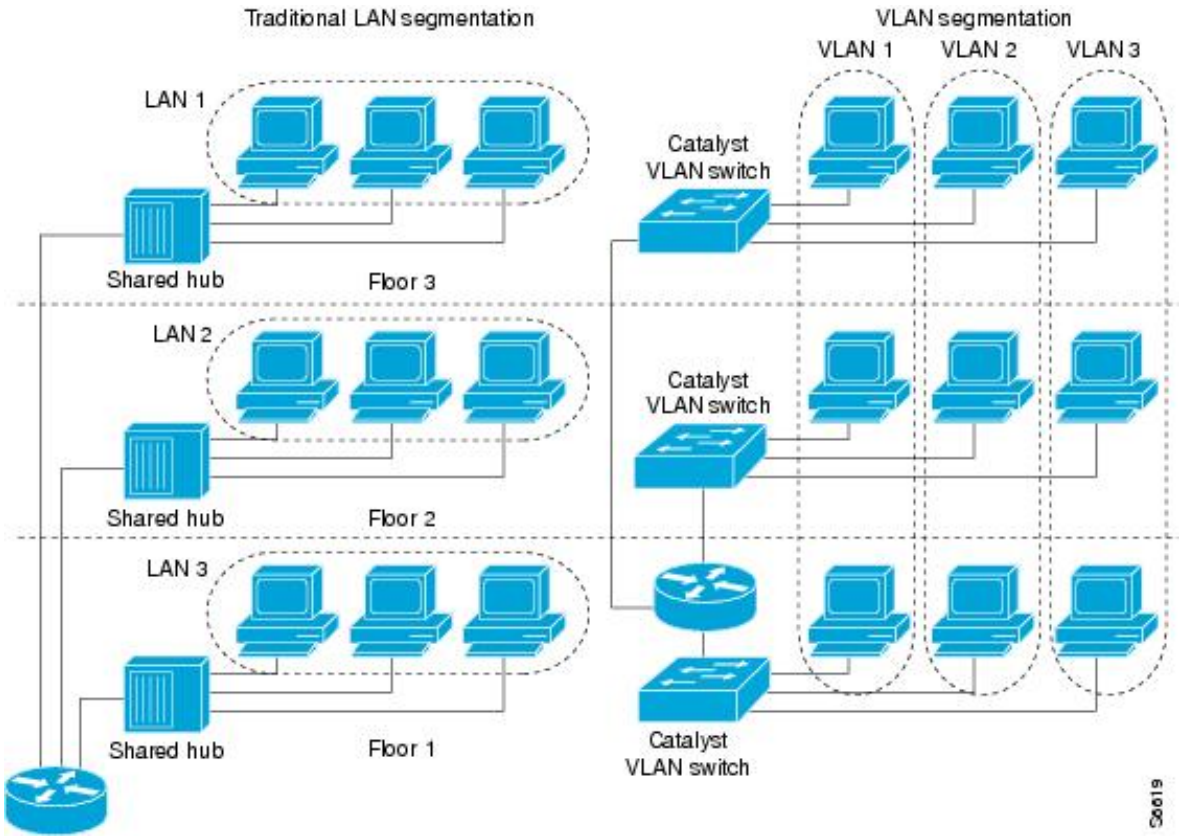
f.tqn.com

Network Example 3/4



iwatchsystems.com

Network Example 4/4



www.cisco.com

Behind the Switch... (1/2)

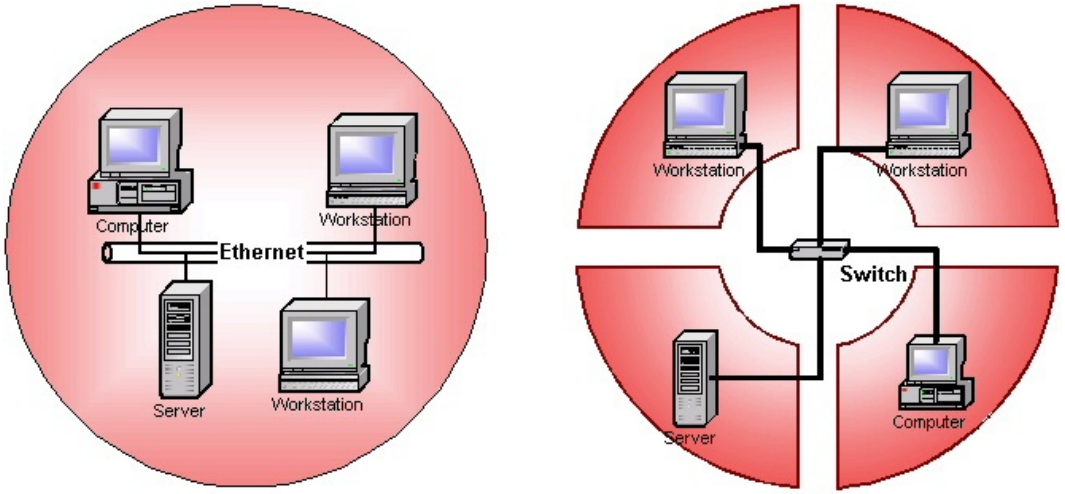
www.sopratel.ma

Behind the Switch... (2/2)

www.outofuse.com

Switched Networks

- Switched networks limit sniffing possibilities.




File View Help
Start GPS
Intel(R) Wireless WiFi Link 5300
Stop
MAC Address SSID FSSI Channel Vendor Privacy Max Rate Network Type First Seen Last
00:1A:2B:58:2B:93 NUMERIC.. -85 11 Ayecom Tec... WEP 54 Infrastructure 10:38:59 PM 10:45
00:1C:F0:9D:2D:51 gaster -85 7 D-Link Corpo.. WEP 54 Infrastructure 10:38:59 PM 10:46
00:1E:8C:C0:62:49 NUMERIC.. -91 6 ASUSTek C... WEP 54 Infrastructure 10:38:59 PM 10:46
00:1F:C6:50:3F:D1 NUMERIC.. -89 6 ASUSTek C... WEP 54 Infrastructure 10:38:59 PM 10:46
00:22:75:CC:CD:4F JB -89 6 Belkin Intern.. RSNA-CCMP 54 Infrastructure 10:38:59 PM 10:46
5C:33:8E:1B:7F:BD anja_wifi -86 1 Alpha Netwo WEP 54 Infrastructure 10:38:59 PM 10:46
00:1D:6A:9C:13:70 saba -44 1 Alpha Netwo... WPA-TKIP 54 Infrastructure 10:38:59 PM 10:46
00:19:7D:39:93:44 alhambra -88 1 Z-Com, Inc. WPA-TKIP 54 Infrastructure 10:38:59 PM 10:46
00:19:7D:47:9A:FE John -88 1 Z-Com, Inc. WPA-TKIP 54 Infrastructure 10:38:59 PM 10:46
00:1A:2B:58:31:7A THEATER -91 6 Ayecom Tec WEP 54 Infrastructure 10:39:15 PM 10:46
00:21:86:EC:BB:C4 reeves -88 1 USI WPA-TKIP 54 Infrastructure 10:39:33 PM 10:46
00:19:7D:1E:3D:CA Pelicanboys -88 1 Z-Com, Inc. WEP 54 Infrastructure 10:40:20 PM 10:46
00:0C:42:0C:0F:51 OzoneBE ... 88 11 Routerboard... None 54 Infrastructure 10:40:49 PM 10:45
00:1A:2B:58:58:3C NUMERIC.. -90 2 Ayecom Tec... WEP 54 Infrastructure 10:41:49 PM 10:43
News
Time Graph
2.4 GHz Channels
5 GHz Channels
Filters
GPS
Amplitude [dB]
-20
-30
-40
-50
-60
-70
-80
-90
-100
10:42
10:43
10:44
10:45
10:46
NUMERICABLE-CD08
gaster
NUMERICABLE-C9A2
NUMERICABLE 8912
JB
anja_wifi
saba
alhambra
John
THEATERHOTEL 5

CONCLUSION AND REFERENCES

- TCP/IP Basics
- Sniffing Data on the Network
- Hub, Switch, and Router
- Conclusion and References

Conclusion

- Sniffing a network is easy and hardly detectable.
- Sniffing an arbitrary network is not allowed.
- Encrypting the channel is highly recommended.
- Using Wireshark is a convenient way to see what is going on.

References

- *Computer Networks*, Andrew S. Tanenbaum, Prentice Hall, 5th edition, October 2010, 960 pages, ISBN 978-0132126953.
- *Wireshark 101: Essential Skills for Network Analysis*, Laura Chappell, February 2013, 370 pages, 978-1893939721.
- https://www.wireshark.org/