

Network Sniffing

Chapter 1

Network & Security

Gildas Avoine

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

TCP/IP	ISO	Protocols
Application	Application	SMTP, HTTP
	Presentation	
	Session	
Transport	Transport	TCP, UDP
Internet	Network	IP, X25 PLP
Network Access	Data Link	Ethernet, PPP, X25 LAPB
	Physical	

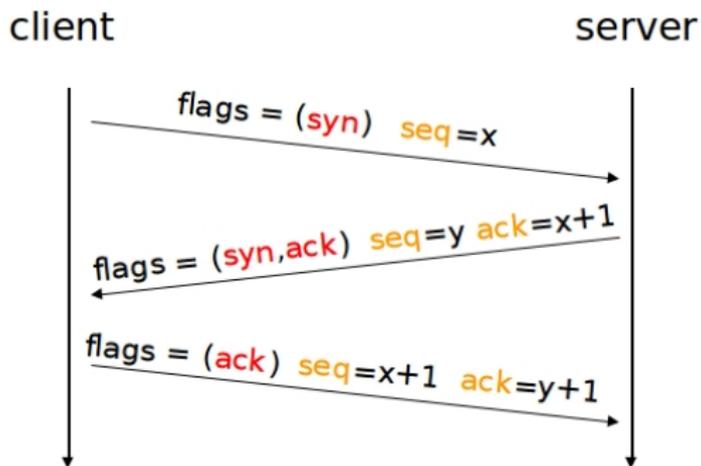
IP Header

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	U R G	A C K	P S H	R S T	S Y N	F I N	Windows
Checksum				Urgent pointer				
Options						Padding		
Data								

TCP 3-way Handshake



TCP 3-way Handshake (Wireshark)

The image shows a Wireshark capture of a TCP 3-way handshake. The filter is set to 'tcp only'. The capture shows three packets:

- Packet 1: SYN from the laptop to the server.
- Packet 2: SYN, ACK from the server to the laptop.
- Packet 3: ACK from the laptop to the server.

The details pane for the selected packet (Frame 2) shows the following information:

- Source: site.b-rail.be
- Destination: wifi-secure1-187.sri.ucl.ac.be
- Protocol: TCP
- Info: rat1 > http [SYN, ACK] Seq=2468243585 Ack=3754094981 Win=24840 Len=0
- Transmission Control Protocol, Src Port: http (80), Dst Port: rat1 (2449), Seq: 2468243585, Ack: 3754094981, Len: 0
- Source port: http (80)
- Destination port: rat1 (2449)
- Sequence number: 2468243585
- Acknowledgement number: 3754094981
- Header length: 24 bytes
- Flags: 0x12 (SYN, ACK)
- 0... .. = Congestion Window Reduced (CWR): Not set
- .0... .. = ECN-Echo: Not set
- ..0... .. = Urgent: Not set
- ...1... .. = Acknowledgment: Set
-0... .. = Push: Not set
-0... .. = Reset: Not set
-0... .. = SYN: Set
-0... .. = FIN: Not set
- Window size: 24840
- Checksum: 0xcc71 [correct]
- Options: (4 bytes)
- [SEQ/ACK analysis]

```
rat1 > http [SYN] Seq=3754094980 win=16384 Len=0 MSS=1460
http > rat1 [SYN, ACK] Seq=2468243585 Ack=3754094981 win=24840
rat1 > http [ACK] Seq=3754094981 Ack=2468243586 win=16560 Len=0
GET /main/E/ 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

eth1 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
8	0.008705	192.168.1.22	212.27.63.3	TCP	74	38834 > ftp [SYN] Seq=1416128761 Win=1
9	0.036853	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [SYN, ACK] Seq=801175440 A
10	0.036897	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=6
11	0.062993	212.27.63.3	192.168.1.22	FTP	140	Response: 220 Serveur de mise a jour c
12	0.063054	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=6
13	3.292595	192.168.1.22	212.27.63.3	FTP	74	Request: USER gildas.avoine
14	3.319677	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [ACK] Seq=801175527 Ack=14
15	3.326153	212.27.63.3	192.168.1.22	FTP	96	Response: 331 Password required for gi
16	3.326259	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128782 Ack=8
17	5.462989	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.11? Tell 192.168.1.
18	5.511446	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.15? Tell 192.168.1.

▶ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

```
0000 b8 26 6c 07 d5 b4 d4 be d9 5d b5 b5 08 00 45 10 .&l....]....E.
0010 00 3c 3d d0 40 00 40 06 27 ff c0 a8 01 16 d4 1b .<=.@.'.....
0020 3f 03 97 b2 00 15 54 68 68 fa 2f c0 f7 e7 50 18 ?.....Th h./...P.
0030 39 08 d5 0b 00 00 55 53 45 52 20 67 69 6c 64 61 9.....US ER gilda
0040 73 2e 61 76 6f 69 6e 65 0d 0a s.avoine ..
```

Apache Authentication Sniffed with Wireshark

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

```
eth1 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
23 6.942066 192.168.1.22 176.9.47.209 TCP 74 51307 > http [SYN] Seq=2464656181 Win=
24 6.945995 192.168.1.1 192.168.1.22 DNS 90 Standard query response A 176.9.47.209
25 6.946016 192.168.1.22 192.168.1.1 ICMP 118 Destination unreachable (Port unreacha
26 6.991198 176.9.47.209 192.168.1.22 TCP 74 http > 51307 [SYN, ACK] Seq=2935579539
27 6.991243 192.168.1.22 176.9.47.209 TCP 66 51307 > http [ACK] Seq=2464656182 Ack=
28 6.991386 192.168.1.22 176.9.47.209 HTTP 433 GET /cours/basic HTTP/1.1
29 7.043244 176.9.47.209 192.168.1.22 TCP 66 http > 51307 [ACK] Seq=2935579540 Ack=
30 7.086488 176.9.47.209 192.168.1.22 HTTP 779 HTTP/1.1 401 Authorization Required (
31 7.086527 192.168.1.22 176.9.47.209 TCP 66 51307 > http [ACK] Seq=2464656549 Ack=
32 7.088593 176.9.47.209 192.168.1.22 TCP 66 http > 51307 [FIN, ACK] Seq=2935580253
33 7.128094 192.168.1.22 176.9.47.209 TCP 66 51307 > http [ACK] Seq=2464656549 Ack=
Authorization: Basic YXZvaW5lOmZha2VfcHdk\r\n
0000 65 70 74 3a 20 74 65 78 74 21 b8 74 bd bc 2c b1 ept: text/html,a
000e 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c pplication/xhtml
00f0 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,application
0100 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 /xml;q=0.9,*/*;q
0110 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e =0.8..Accept-Lan
0120 67 75 61 6f 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b guage: en-us,en;
0130 71 3d 30 2e 38 2c 66 72 3b 71 3d 30 2e 35 2c 66 q=0.8,fr;q=0.5,f
0140 72 2d 66 72 3b 71 3d 30 2e 33 0d 0a 41 63 63 65 r-fr;q=0.3..Acce
0150 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encoding: gzi
0160 70 2c 20 64 65 6e 6c 61 74 65 0d 0a 43 6f 6e 6e p, deflate..Conn
0170 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ction: keep-aliv
0180 76 65 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f ve..Authenticatio
0190 6e 3a 20 42 61 73 69 63 20 59 58 5a 76 61 57 35 n: Basic YXZvaW5l
01a0 6c 4f 6d 5a 68 61 32 56 66 63 48 64 6b 0d 0a 0d OmZha2VfcHdk..;
01b0 0a
```

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**.

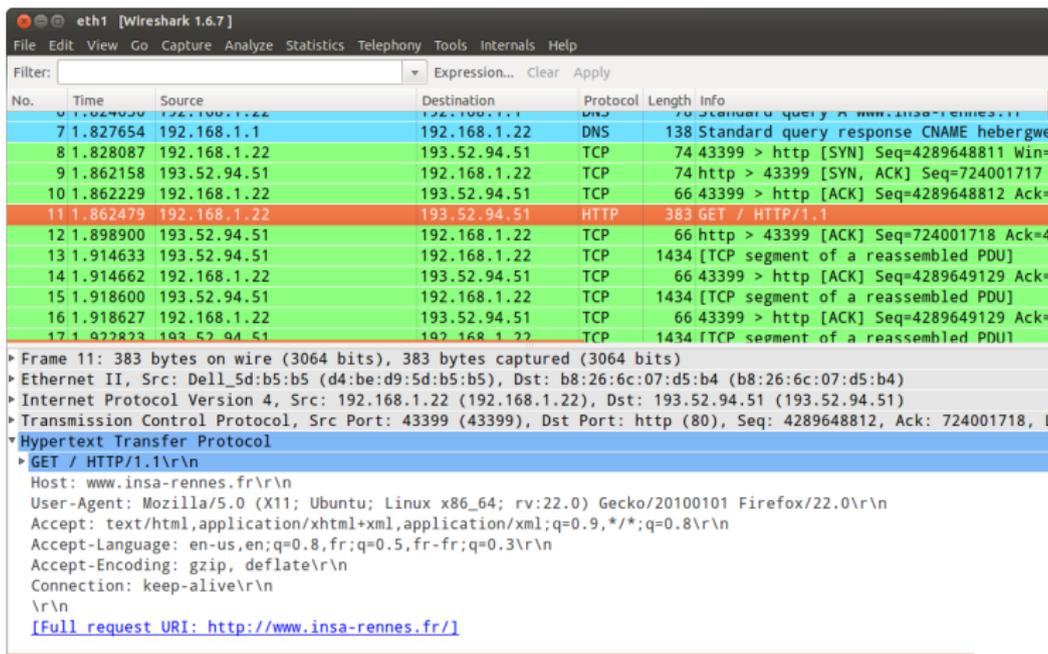
The image shows a Wireshark capture of network traffic on the eth1 interface. The packet list pane shows several packets, with packet 17 highlighted in red. Packet 17 is a TCP segment of a reassembled PDU, which is an HTTP GET request. The packet details pane shows the structure of the request, including the Host field (www.amazon.fr) and the Cookie field (x-wl-uid=1tjdQJ/7Mp vYwWlrM/zqfFSBjhs2 QkWFw00mKsMR5Kmq GH0vrgokem/d/nVj P1fJ8z/IyKhdS10y fs=; patn=/; domain=amazon.fr; expires=Mon, 31-Dec-2035 00:00:00 GMT).

No.	Time	Source	Destination	Protocol	Length	Info
9	1.139373	192.168.1.18	192.168.1.255	NBNS	92	Name query NB WPAD<00>
10	1.597716	192.168.1.22	192.168.1.1	DNS	73	Standard query A www.amazon.fr
11	1.632377	192.168.1.1	192.168.1.22	DNS	89	Standard query response A 178.236.6.242
12	1.632698	192.168.1.22	178.236.6.242	TCP	74	60535 > http [SYN] Seq=2966224244 Win=0 Len=0
13	1.676658	178.236.6.242	192.168.1.22	TCP	62	http > 60535 [SYN, ACK] Seq=3182175785 Win=0 Len=0
14	1.676705	192.168.1.22	178.236.6.242	TCP	54	60535 > http [ACK] Seq=2966224245 Ack=3182175786
15	1.676818	192.168.1.22	178.236.6.242	HTTP	366	GET / HTTP/1.1
16	1.739155	178.236.6.242	192.168.1.22	TCP	60	http > 60535 [ACK] Seq=3182175786 Ack=2966224245
17	1.819213	178.236.6.242	192.168.1.22	TCP	1494	[TCP segment of a reassembled PDU]
18	1.819241	192.168.1.22	178.236.6.242	TCP	54	60535 > http [ACK] Seq=2966224557 Ack=3182175786
19	1.822102	178.236.6.242	192.168.1.22	TCP	1494	[TCP segment of a reassembled PDU]

TCP segment data (1440 bytes)	
0180	6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 Content-Type: text/html; char set=ISO-8859-15. Set-cookie: x-wl-uid=1tjdQJ/7Mp vYwWlrM/zqfFSBjhs2 QkWFw00mKsMR5Kmq GH0vrgokem/d/nVj P1fJ8z/IyKhdS10y fs=; patn=/; domain=amazon.fr; expires=Mon, 31-Dec-2035 00:00:00 GMT
0190	6d 6c 3b 20 63 68 61 72 73 65 74 3d 49 53 4f 2d
01a0	38 38 35 39 2d 31 35 0d 0a 53 65 74 2d 63 6f 6f
01b0	6b 69 65 3a 20 78 2d 77 6c 2d 75 69 64 3d 31 74
01c0	6a 64 51 4a 2f 37 4d 70 76 59 57 57 72 4d 2f 7a
01d0	71 46 53 42 6a 68 53 32 51 4c 57 66 57 4f 4f 6d
01e0	4b 73 4d 52 35 4b 6d 71 47 48 4f 76 72 67 6f 6b
01f0	65 6d 64 2f 6e 4e 56 6a 50 31 66 4a 38 7a 2f 49
0200	79 4b 68 64 35 6c 4f 79 66 73 3d 3b 20 70 61 74
0210	68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 61 6d 61
0220	7a 6f 6e 2e 66 72 3b 20 65 78 70 69 72 65 73 3d
0230	4d 6f 6e 2c 20 33 31 2d 44 65 63 2d 32 30 33 35
0240	3e 33 23 2e 3e

Browser Fingerprinting

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



The screenshot shows the Wireshark interface with a packet list table and a packet details pane. The packet list table shows a sequence of network traffic, with packet 11 highlighted in red, indicating it is selected. The packet details pane shows the structure of the selected HTTP GET request, including the host, user-agent, and other headers.

No.	Time	Source	Destination	Protocol	Length	Info
7	1.827654	192.168.1.1	192.168.1.22	DNS	138	Standard query response CNAME hebergwe
8	1.828087	192.168.1.22	193.52.94.51	TCP	74	43399 > http [SYN] Seq=4289648811 Win=
9	1.862158	193.52.94.51	192.168.1.22	TCP	74	http > 43399 [SYN, ACK] Seq=724001717
10	1.862229	192.168.1.22	193.52.94.51	TCP	66	43399 > http [ACK] Seq=4289648812 Ack=
11	1.862479	192.168.1.22	193.52.94.51	HTTP	383	GET / HTTP/1.1
12	1.898900	193.52.94.51	192.168.1.22	TCP	66	http > 43399 [ACK] Seq=724001718 Ack=4
13	1.914633	193.52.94.51	192.168.1.22	TCP	1434	[TCP segment of a reassembled PDU]
14	1.914662	192.168.1.22	193.52.94.51	TCP	66	43399 > http [ACK] Seq=4289649129 Ack=
15	1.918600	193.52.94.51	192.168.1.22	TCP	1434	[TCP segment of a reassembled PDU]
16	1.918627	192.168.1.22	193.52.94.51	TCP	66	43399 > http [ACK] Seq=4289649129 Ack=
17	1.922822	193.52.94.51	192.168.1.22	TCP	1434	[TCP segment of a reassembled PDU]

Frame 11: 383 bytes on wire (3064 bits), 383 bytes captured (3064 bits)
Ethernet II, Src: Dell_5d:b5:b5 (d4:be:d9:5d:b5:b5), Dst: b8:26:6c:07:d5:b4 (b8:26:6c:07:d5:b4)
Internet Protocol Version 4, Src: 192.168.1.22 (192.168.1.22), Dst: 193.52.94.51 (193.52.94.51)
Transmission Control Protocol, Src Port: 43399 (43399), Dst Port: http (80), Seq: 4289648812, Ack: 724001718, L
Hypertext Transfer Protocol
GET / HTTP/1.1
Host: www.insa-rennes.fr
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.8,fr;q=0.5,fr-fr;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
[Full request URI: http://www.insa-rennes.fr/]

HUB, SWITCH, AND ROUTER

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

- 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 bandwidth 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.

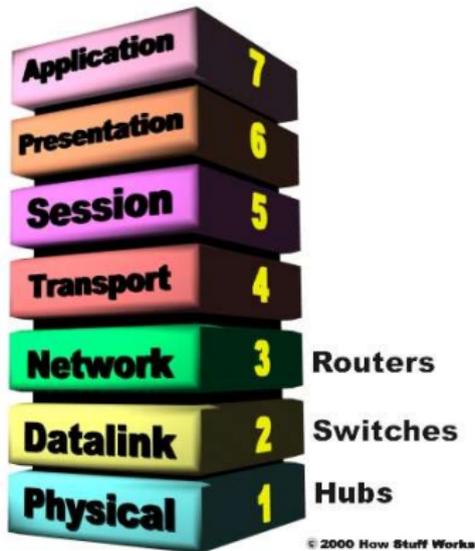


Router

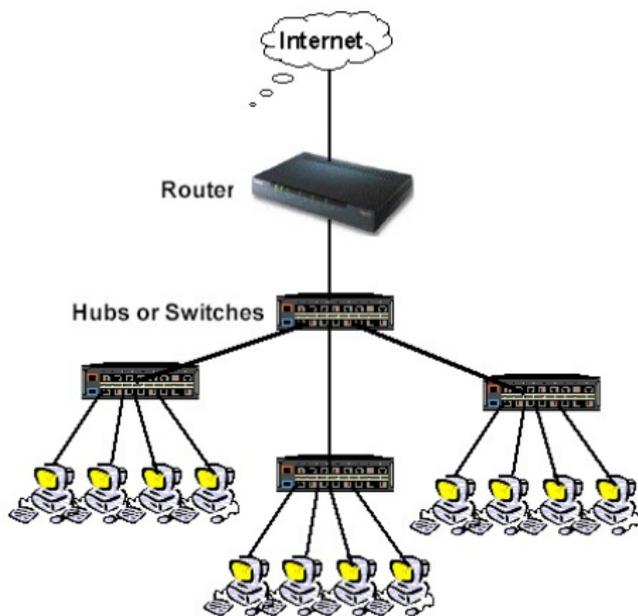
- A **router** is typically used to connect 2 LANs or a LAN with ISP.
- Routers are located at **gateways**.
- Routers use forwarding tables to determine the **best path** for forwarding the packets.
- They communicate with each other using protocols as **ICMP**.
- A router is typically connected to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



Hubs, Switches, and Routers through the Layers

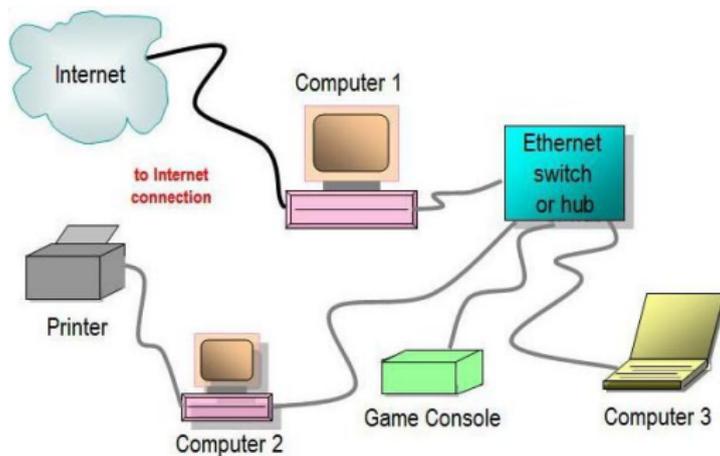


Network Example 1/4



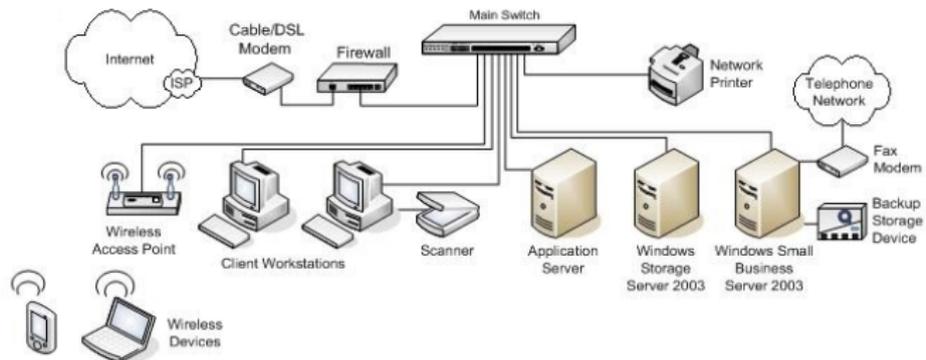
www.practicallynetworked.com

Network Example 2/4



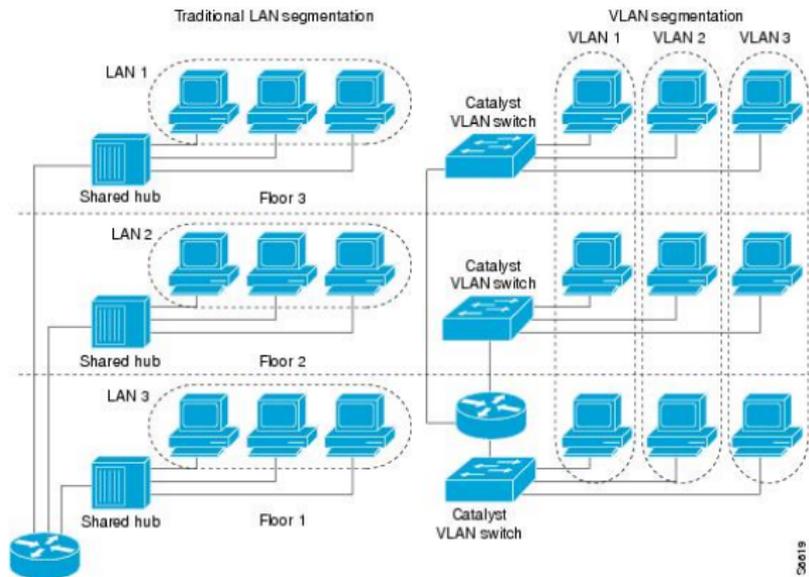
f.tqn.com

Network Example 3/4



iwatchsystems.com

Network Example 4/4



www.cisco.com

Behind the Switch... (1/2)



www.sopratel.ma

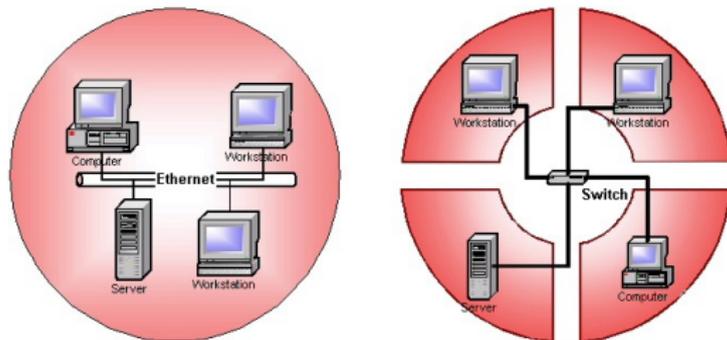
Behind the Switch... (2/2)



www.outofuse.com

Switched Networks

- Switched networks limit sniffing possibilities.



Wireless Networks



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.

- *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/>