

Ethernet/Data Link frame capture (Evesdropping Lab)

i310 Lab 1/12/2016:

JF (Network Protocols/Protocol Analyzers) – *attached related slides*

Lab Exercise – Class/individuals will do a live capture of Ethernet frames, then decode and analyze the frames.

The lab requires a wired interface into a shared Ethernet hub where all lab devices will connect.

As an alternative – you can load Wireshark on your device. It does require you install the software on your machine – it is free. I will be providing at least several laptops with wired interfaces and Wireshark loaded as a lab resource, important hands-on skill for you to have and be aware of. There should also be a copy posted to Canvas library/share.

Deliverable: email (to Canvas site) lab write-up detailing your explanation of the lab, how to capture and Ethernet frame, and how this tool would prove useful in network troubleshooting and other cases (*please state at least one scenario besides networking troubleshooting, how it would be used*)

Wireshark Website: the website contains information on the tool, and also the software for people that want to directly download the tool to their personal device.

<http://www.wireshark.org/>

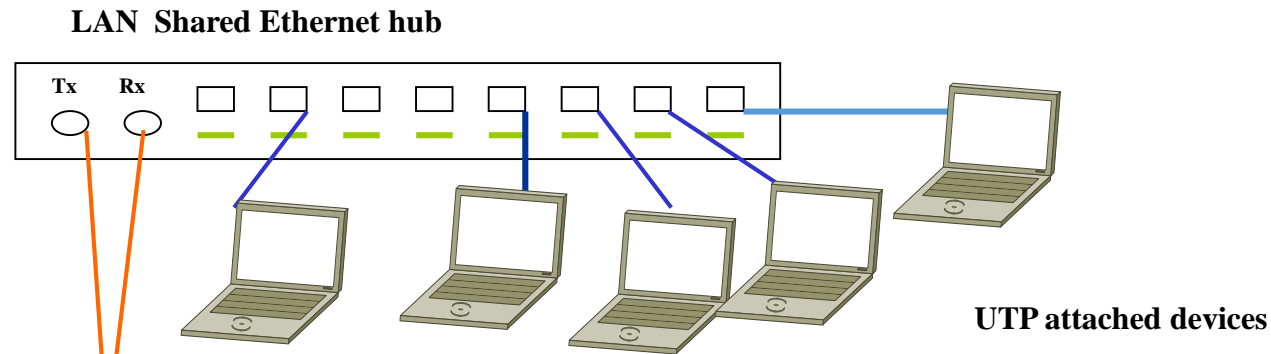
Ethernet/Data Link frame capture/evesdropping Lab

Deliverable: write-up detailing ***your*** explanation of the lab – approx. 1 page email (to Canvas site): ***Due 1/19/2016 8pm PST***

1. Brief description of how to capture an Ethernet frame (30 %)
2. Briefly describe one recommendation how you might use a similar tool to troubleshoot a technical issue or possibly provide analysis and/or forensics in IA/Cyber Security (30 %)
4. Summary of what you learned in lab (and how you may apply this knowledge in future (40 %)

Lab Topology (Ethernet hub to hub)

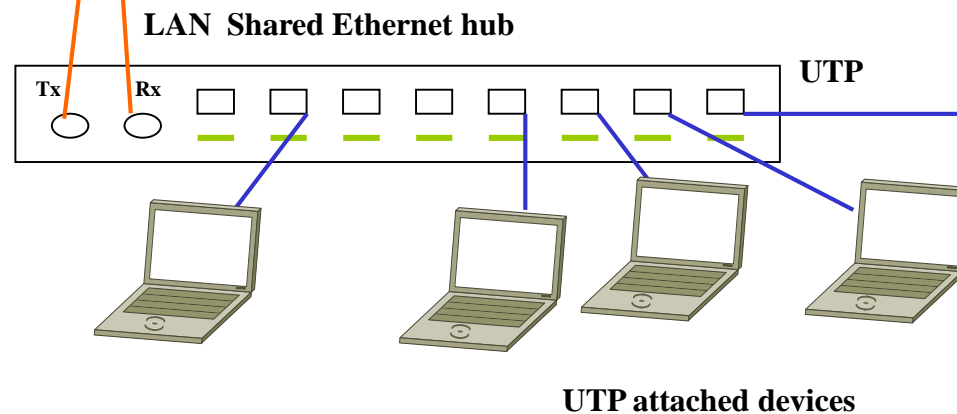
Front of class



Pair MMfiber
2000 ft (10-Base-F)

Older dev - Disable wireless interfaces (can confuse OS)

Back of class



** Any significance to the Topology ? Why such old hubs and not new switches ?*

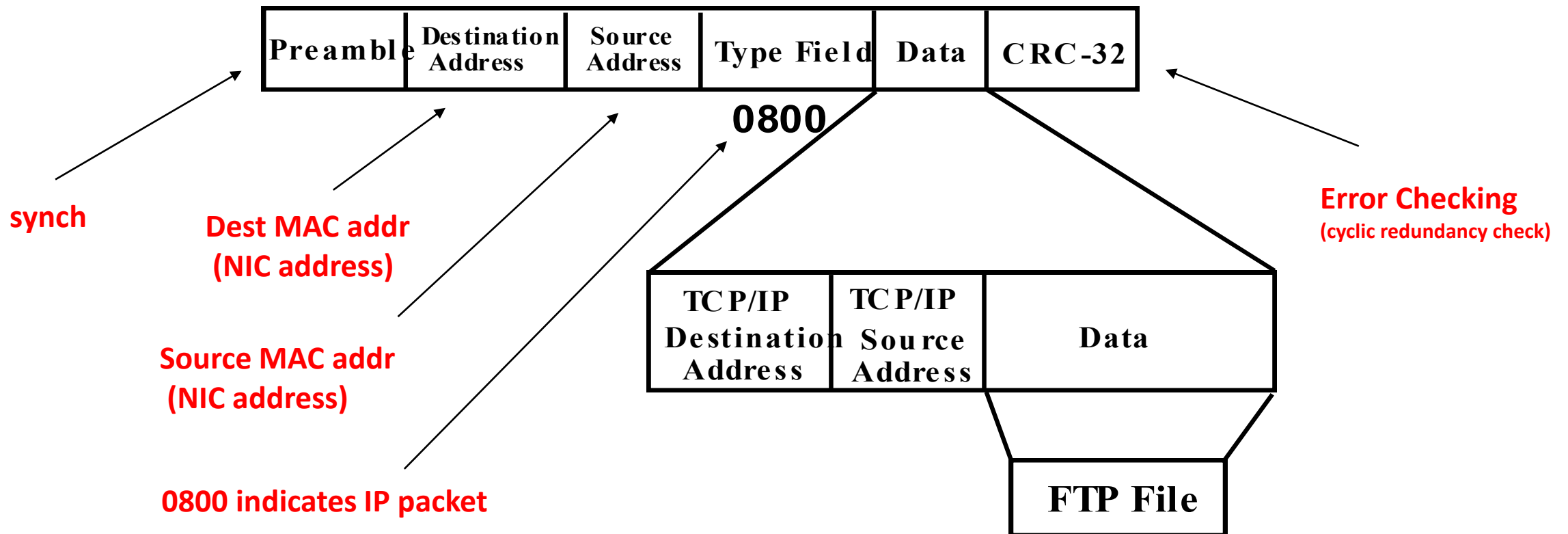
Ethernet frames and TCP/IP Packets

The following group of slides is intended to provide background information on Ethernet frame and TCP/IP packet structure/content. Additionally, there are slides that demonstrate how to filter (to display only desired traffic) – as well as discovery telnet/http data (i.e. passwords sent in clear)

PDU (Protocol Data Unit) - the contents of an Ethernet frame

An Ethernet frame may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, AppleTalk, SNA, MOP, LAT....)

The following diagram illustrates a FTP (file transfer) request from an end user in a TCP/IP packet inside an Ethernet frame.



Sniffer - Local, SX - [IPARP: Decode, 4/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25]	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PRO	60	0:00:48.026	0.000.855	
9		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WIN	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642589	60	0:00:48.033	0.001.230	
11		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	
12		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.001.545	
13		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.000.675	
14		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 IAC Will Echo	60	0:00:48.042	0.001.080	
15		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn	246	0:00:48.054	0.011.505	
16		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642787 WIN=28474	60	0:00:48.204	0.150.345	
17		[144.116.200.10]	[144.116.200.1]	Telnet: C PORT=1024 IAC Do Suppress go-ahead	60	0:00:48.231	0.027.180	
18		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 IAC Don't Terminal-type	60	0:00:48.233	0.001.905	

LOOP: ----- LOOPBACK Version 2.0 Frame -----

- LOOP:
- LOOP: Skip Count = 0
- LOOP: Message type = Reply message
- LOOP: Receipt number = 27726
- LOOP:

```
00000000: 00 00 0c 00 b5 22 00 00 0c 00 b5 22 90 00 00 00  ....µ"....µ"....
00000010: 01 00 4e 6c 02 b1 c8 40 7d 01 00 a0 00 00 f4 f4  ..N1.±E@}.....ôô
00000020: 03 00 38 84 01 00 0a 40 03 40 00 00 00 01 11 00  ..8|...@.@.....
00000030: 06 c0 01 ff ff 00 06 c0 02 80 00 00 0c c0 0b 53  ..À.ÿÿ..À.!.À.S
00000040: 4e 49 46 46 45 52 00 00 12 40 0c 00 00 00 00 00  NIFFER...@.....
00000050: 00 00 00 00 00 00 00 00 00 71 71 a2 3f 00 34 35  .....qqç?.45
00000060: 36 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00  67.....
00000070: 00 00 00 00 00 00
```

Highlighted frame (#4) high level ether frame

Expert Decode Matrix Host Table Protocol Dist. Statistics

For Help, press F1

start Sniffer - Local, SX - [I... Wireshark Protocol Tr...

11:12 AM

Sniffer - Local, SX - [IPARP: Decode, 7765 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25]	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PRO	60	0:00:48.026	0.000.855	
9		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WIN	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=36429	60	0:00:48.033	0.001.230	
11		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	
12		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.001.545	
13		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.000.675	
14		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 IAC Will Echo	60	0:00:48.042	0.001.080	
15		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn	246	0:00:48.054	0.011.505	
16		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642787 WIN=28474	60	0:00:48.204	0.150.345	
17		[144.116.200.10]	[144.116.200.1]	Telnet: C PORT=1024 IAC Do Suppress go-ahead	60	0:00:48.231	0.027.180	
18		[144.116.200.1]	[144.116.200.10]	Telnet: R PORT=1024 IAC Don't Terminal-type	60	0:00:48.233	0.001.905	

DLC: ----- DLC Header -----

- DLC: Frame 7 arrived at 10:55:45.0257; frame size is 60 (003C hex) bytes.
- DLC: Destination = BROADCAST FFFFFFFF, Broadcast
- DLC: Source = Station UB 076082
- DLC: Ethertype = 0806 (ARP)

ARP: ----- ARP/RARP frame -----

- ARP: Hardware type = 1 (10Mb Ethernet)
- ARP: Protocol type = 0800 (IP)
- ARP: Length of hardware address = 6 bytes
- ARP: Length of protocol address = 4 bytes
- ARP: Opcode 1 (ARP request)
- ARP: Sender's hardware address = 00DD01076082
- ARP: Sender's protocol address = [144.116.200.107]
- ARP: Target hardware address = 000000000000
- ARP: Target protocol address = [144.116.200.1]

00000000: ff ff ff ff ff ff 00 dd 01 07 60 82 08 06 00 01 vvvvvv.Y...|...

Expert Decode Matrix Host Table Protocol Dist. Statistics

For Help, press F1

start Sniffer - Local, SX - [I... Wireshark Protocol Tr... Sniffer_IP-ARP_ENC 11:16 AM

**Highlighted frame (#7)
high level ether frame**

**Details of Ethernet frame/PDU
(dest MAC addr, Ether type field,
TCP/UDP port #**

Sniffer - Local, SX - [IPARP: Decode, 9/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25]	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PRO	60	0:00:48.026	0.000.855	
9		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642	60	0:00:48.033	0.001.230	
11		[144.116.200.10]	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	
12		[144.116.200.1]	[144.116.200.10]	TCP: D=1024 S=23 ACK=4290181122 WIN=28672	60	0:00:48.041	0.001.545	

TCP: ----- TCP header -----

- TCP:
- TCP: Source port = 1024
- TCP: Destination port = 23 (Telnet)
- TCP: Initial sequence number = 4290181121
- TCP: Next expected Seq number = 4290181122
- TCP: Data offset = 24 bytes
- TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
- TCP: Flags = 02
- TCP: ...0... = (No urgent pointer)
- TCP: ...0... = (No acknowledgment)
- TCP: ...0... = (No push)
- TCP: ...0... = (No reset)
- TCP: ...1... = SYN
- TCP: ...0... = (No FIN)
- TCP: Window = 28672
- TCP: Checksum = 7B4F (correct)
- TCP: Urgent pointer = 0
- TCP:
- TCP: Options follow
- TCP: Maximum segment size = 1381
- TCP:

DLC: Frame padding= 2 bytes

**Highlighted frame (#9)
high level ether frame**

**Details of TCP packet
port #'s, sequence #'s, window parms**

00000000: 00 00 0c 00 b5 22 00 dd 01 07 60 82 08 00 45 00p.Y...E.

00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74 ...Où...}tEkIt

00000020: 08 01 04 00 00 17 ff b6 f8 01 00 00 00 00 60 02 ...

Telnet app capture (multiple frames)

The image shows a Wireshark packet capture window. The top bar indicates the capture is on the 'i310-telnet_1-26-15.pcap' file. The main pane displays a list of 23 captured packets. The selected packet (No. 71) is a frame of 69 bytes. The bottom pane shows the raw data of this frame in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.100.10	239.255.255.250	UDP	Source port: 1237 Destination port: 3702
2	0.251682	fe80::f2bf:97ff:fe	ff02::fb	MDNS	Standard query PTR _googlecast._tcp.local, "QM" question
3	0.251753	fe80::f2bf:97ff:fe	ff02::fb	MDNS	Standard query PTR _googlecast._tcp.local, "QM" question
4	0.273622	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
5	0.274103	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
6	0.392637	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
7	0.393130	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
8	0.415854	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
9	0.416322	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
10	0.620397	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
11	0.620820	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
12	0.877543	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
13	0.878010	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
14	0.954661	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
15	0.955152	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
16	1.248707	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
17	1.249176	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
18	1.347383	fe80::f2bf:97ff:fe	ff02::fb	MDNS	Standard query PTR _lpps._tcp.local, "QM" question PTR _lpp...
19	1.380700	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
20	1.381170	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
21	1.383423	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
22	1.383907	fe80::ad39:f6e7:3d	ff02::c	SSDP	NOTIFY * HTTP/1.1
23	1.639651	169.254.73.92	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

Frame 71 (69 bytes on wire, 69 bytes captured)
 Arrival Time: Jan 26, 2015 17:43:26.850380000
 [Time delta from previous packet: 0.003062000 seconds]
 [Time since reference or first frame: 7.488206000 seconds]
 Frame Number: 71
 Packet Length: 69 bytes
 Capture Length: 69 bytes
 Frame is marked: false

Offset	Hex	ASCII
0000	00 15 62 5a de 7e 00 14 22 cf 7a 47 08 00 45 00	..bZ~... ".zG..E.
0010	00 37 06 7a 40 00 80 06 aa ea c0 a8 64 0a c0 a8	.7.z@... ..d...
0020	64 01 04 d6 00 17 eb 53 43 15 70 da d0 20 50 18	d.....S C.p.. P.
0030	44 70 49 86 00 00 ff fb 18 ff fd 03 ff fb 03 ff	OpI.....
0040	fd 01 ff fb 1f

Frame (frame), 69 bytes | P: 169 D: 169 M: 0

i310-telnet_1-26-15.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: telnet

No.	Time	Source	Destination	Protocol	Info
71	7.488206	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
72	7.488494	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
73	7.489834	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
74	7.489857	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
75	7.490617	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
76	7.491037	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
78	7.491148	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
79	7.492384	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
84	9.352728	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
87	9.635329	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
89	10.006239	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
91	10.205881	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
93	10.405914	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
95	10.605901	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
97	10.900730	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
98	10.903394	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
107	12.206916	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
108	12.209716	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
114	12.428966	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
115	12.431635	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
118	12.777168	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
119	12.779878	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
120	12.780140	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...

Frame 71 (69 bytes on wire, 69 bytes captured)

Arrival Time: Jan 26, 2015 17:43:26.850380000

[Time delta from previous packet: 7.488206000 seconds]

[Time since reference or first frame: 7.488206000 seconds]

Frame Number: 71

Packet Length: 69 bytes

Capture Length: 69 bytes

Frame is marked as failed

```
0000  00 15 62 5a de 7e 00 14 22 cf 7a 47 08 00 45 00  ..bZ.~... ".ZG..E.
0010  00 37 06 7a 40 00 80 06 aa ea c0 a8 64 0a c0 a8  .7.z@... ....d...
0020  64 01 04 d6 00 17 eb 53 43 15 70 da d0 20 50 18  d.....S C.p.. P.
0030  44 70 49 86 00 00 ff fb 18 ff fd 03 ff fb 03 ff  DpI.....
0040  fd 01 ff fb 1f                                     .....
```

File: "C:\Documents and Settings\James\Desktop\i310-telnet_1-26-15.pcap" 48 KB 00:00:19 P: 169 D: 50 M: 0

Enter telnet on filter line to only view telnet frames (app used in lab) <enter>

Notice how now only see telnet frames (easier to decode/view)

Wireshark interface showing a capture of Telnet traffic. The filter is set to 'telnet'. The packet list shows multiple Telnet frames. The selected packet (Frame 84) is expanded, showing the Ethernet II, IP, and Transmission Control Protocol (TCP) details. The TCP details show the source port as 1238 and the destination port as telnet (23). The Telnet data field shows the character 'u'.

Filter: telnet

No.	Time	Source	Destination	Protocol	Info
71	7.488206	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
72	7.488494	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
73	7.489834	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
74	7.489857	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
75	7.490617	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
76	7.491037	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
78	7.491148	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
79	7.492384	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
84	9.352728	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
87	9.635329	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
89	10.006239	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
91	10.205881	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
93	10.405914	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
95	10.605901	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
97	10.900730	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
98	10.903394	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
107	12.206916	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
108	12.209716	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
114	12.428966	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
115	12.431635	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
118	12.777168	192.168.100.10	192.168.100.1	TELNET	Telnet Data ...
119	12.779878	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...
120	12.780140	192.168.100.1	192.168.100.10	TELNET	Telnet Data ...

Frame 84 (55 bytes on wire, 55 bytes captured)

- Ethernet II, Src: Dell_cf:7a:47 (00:14:22:cf:7a:47), Dst: Cisco_5a:de:7e (00:15:62:5a:de:7e)
 - Destination: Cisco_5a:de:7e (00:15:62:5a:de:7e)
 - Source: Dell_cf:7a:47 (00:14:22:cf:7a:47)
- Type: IP (0x0800)
- Internet Protocol, Src: 192.168.100.10 (192.168.100.10), Dst: 192.168.100.1 (192.168.100.1)
- Transmission Control Protocol, Src Port: 1238 (1238), Dst Port: telnet (23), Seq: 36, Ack: 427, Len: 1
- Telnet
 - Data: u

0000 00 15 62 5a de 7e 00 14 22 cf 7a 47 08 00 45 00 ..bZ.~... ".zG..E.
0010 00 29 06 7e 40 00 80 06 aa f4 c0 a8 64 0a c0 a8 .).~@...d...
0020 64 01 04 d6 00 17 eb 53 43 38 70 da d1 ca 50 18 d.....S C8p...P.
0030 42 c6 49 78 00 00 75 B.Ix..u

Type (eth.type), 2 bytes P: 169 D: 50 M: 0

telnet frame & detailed data view should first letter of password as sent asynch (1 char at a time)

Why 1 char at a time ?

VT100 protocol

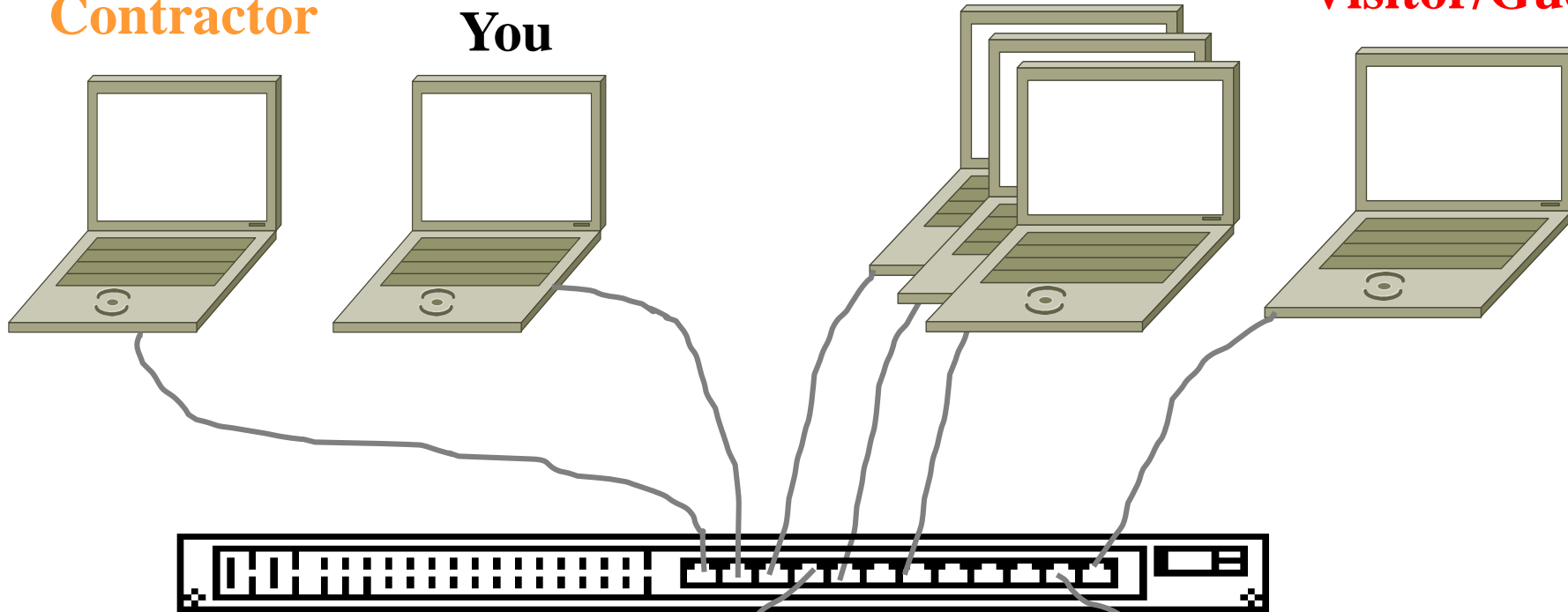
VLANs (Virtual LANs)

Supplier/Vendor
Contractor

You

Work Peers

Visitor/Guest



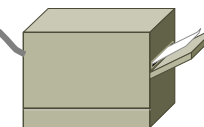
Ethernet Frame Protocol Decodes

A screenshot of a network protocol analyzer (Wireshark) showing a packet capture. The packet list on the left shows several Ethernet II frames. The packet details pane on the right shows the structure of an Ethernet II frame, including the destination MAC address, source MAC address, and type. The packet bytes pane at the bottom shows the raw data of the frame.

Shared Ethernet LAN

Eavesdropping

Printer



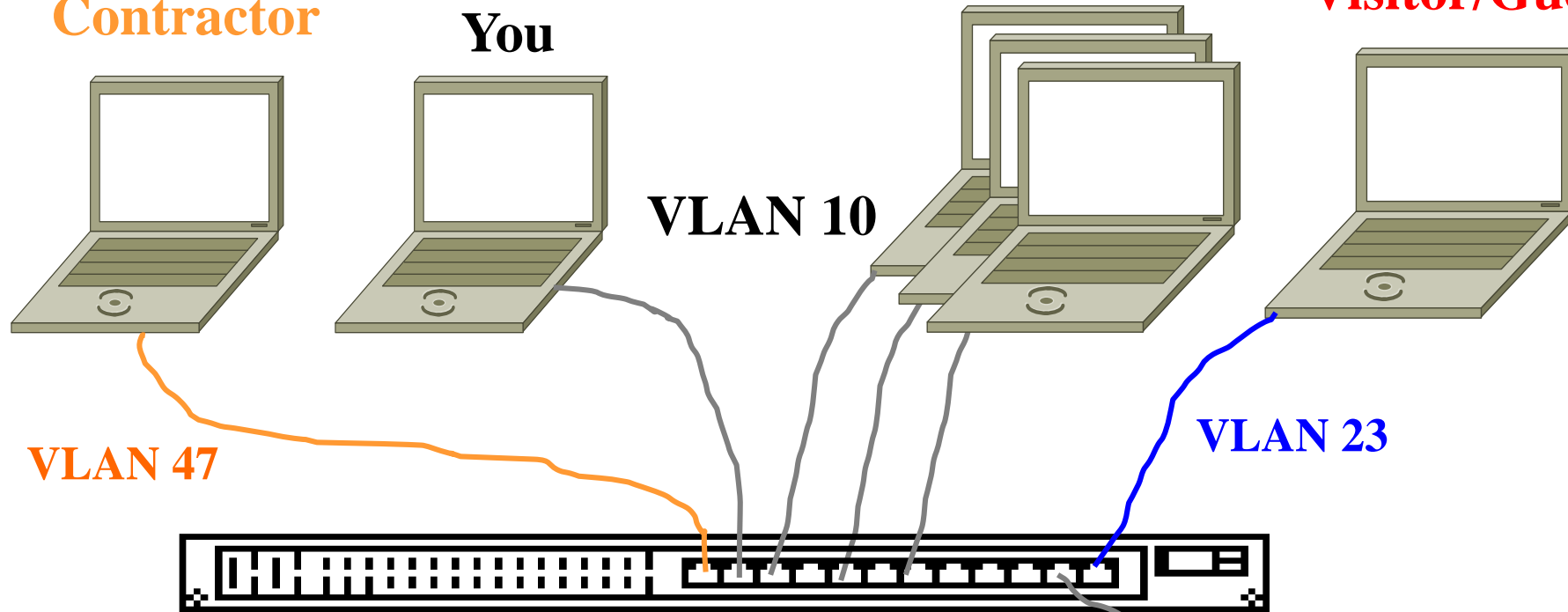
VLANs (Virtual LANs)

Supplier/Vendor
Contractor

You

Work Peers

Visitor/Guest



*Different Logical LANs
(Virtual LANs) share same physical switch
each LAN air-gapped from the others*

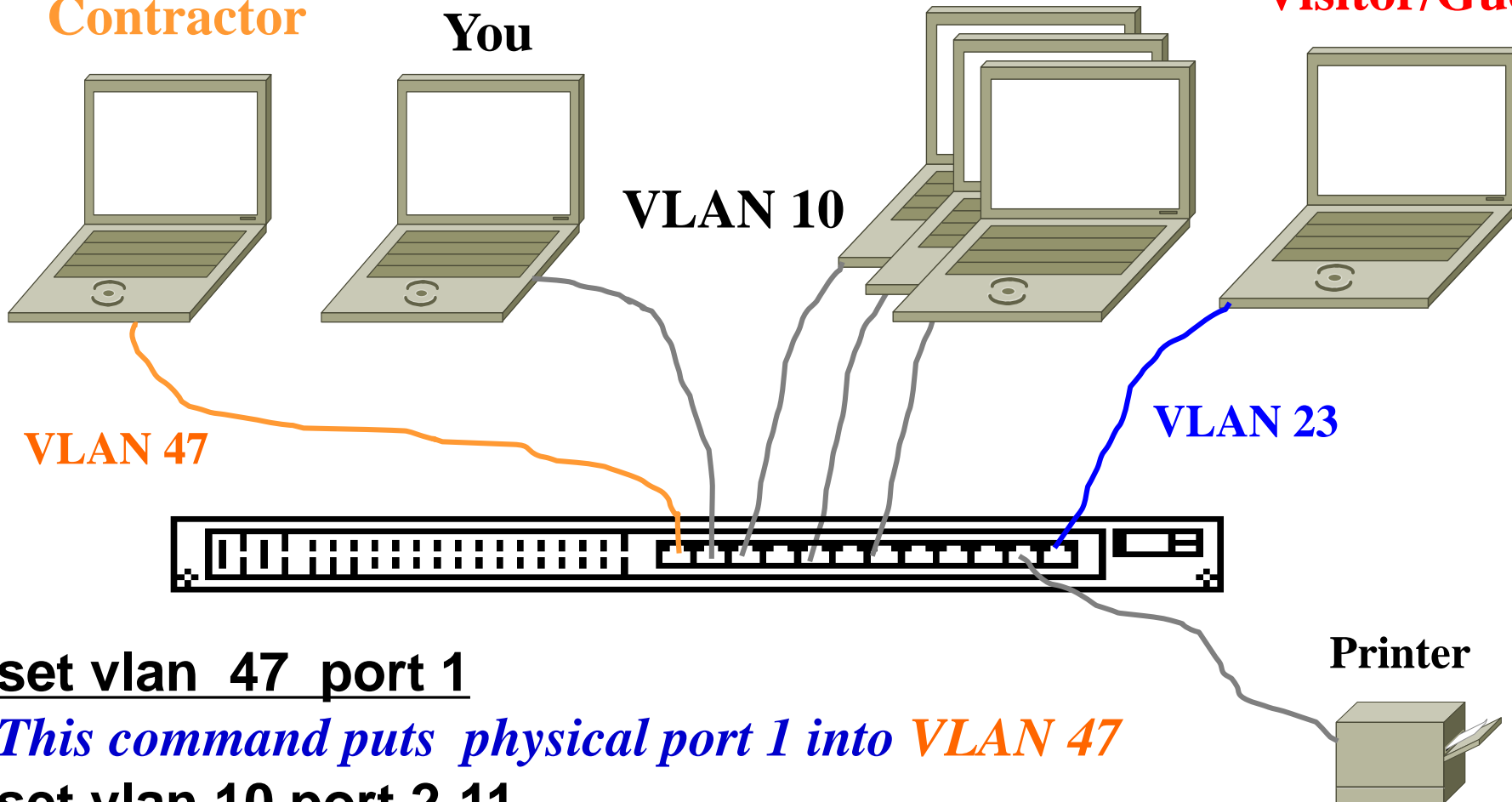
VLANs (Virtual LANs)

Supplier/Vendor
Contractor

You

Work Peers

Visitor/Guest



set vlan 47 port 1

This command puts physical port 1 into VLAN 47

set vlan 10 port 2-11

This would put physical ports 2 thru 11 into VLAN 10

Question: What command set for Visitor/Guest port into VLAN 23 ?

So now you have implemented LANs to segment internal and external traffic as a good security mechanism:

what threats/vulnerabilities has this eliminated ?