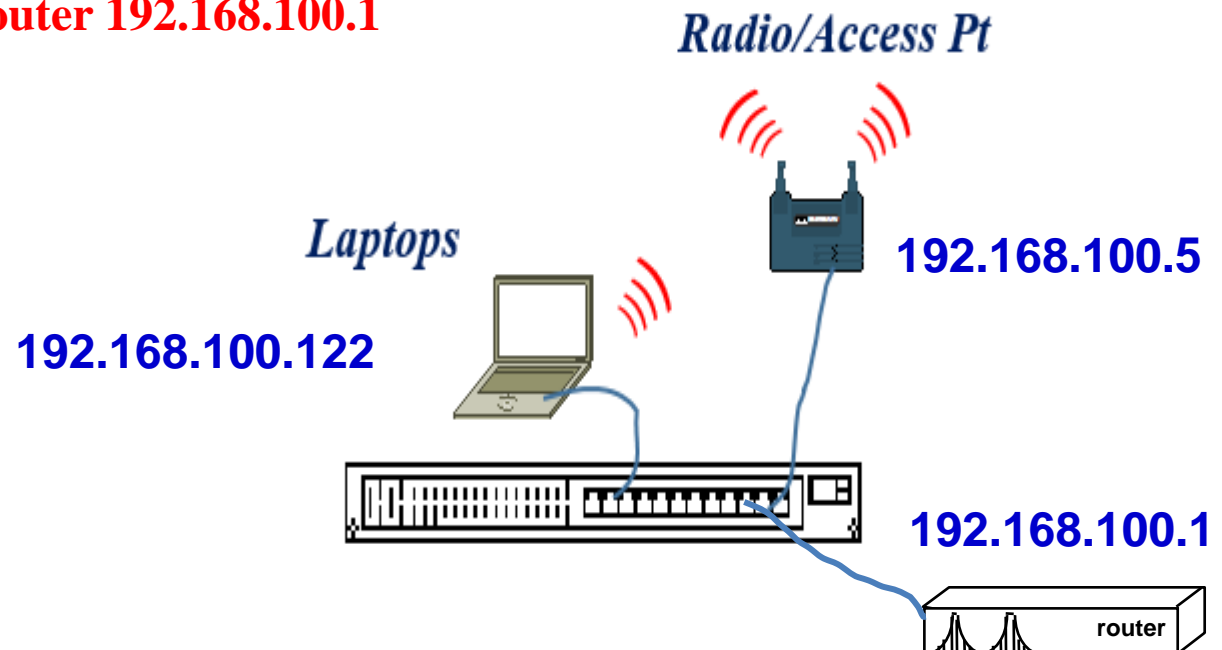


HTTP trace *(over Ethernet)*



1. I already started Wireshark session live capturing in background which will “see” all frames on Ethernet.
2. I am at browser of laptop (.122) entering IP add of 100.5 to HTTP into cisco router 192.168.100.1



* The following pages are screen captures of Wireshark Traces of these devices

ARP – trying to resolve MAC & IP add

***Ethernet**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
38	39.837866	00000000.0000813986...	00000000.ffffffffffff...	IPX SAP	60	Nearest Query
39	39.027770	192.168.100.122	192.168.111.125	TCP	66	50055→53048 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
40	39.030382	192.168.100.1	192.168.100.122	ICMP	70	Destination unreachable (Host unreachable)
41	39.058888	192.168.100.122	192.168.111.125	TCP	66	50056→3910 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
42	39.709283	Dell_18:e9:2b	Broadcast	ARP	42	Who has 192.168.100.5? Tell 192.168.100.122
43	39.710061	CiscoInc_3e:62:3e	Dell_18:e9:2b	ARP	60	192.168.100.5 is at 00:14:1c:3e:62:3e
44	39.710085	192.168.100.122	192.168.100.5	TCP	66	50057→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
45	39.711285	192.168.100.5	192.168.100.122	TCP	60	80→50057 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
46	39.711472	192.168.100.122	192.168.100.5	TCP	54	50057→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0

[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]

✓ Ethernet II, Src: Dell_18:e9:2b (28:f1:0e:18:e9:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: Dell_18:e9:2b (28:f1:0e:18:e9:2b)
Type: ARP (0x0806)

✓ Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Dell_18:e9:2b (28:f1:0e:18:e9:2b)
Sender IP address: 192.168.100.122
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.100.5

0000 ff ff ff ff ff 28 f1 0e 18 e9 2b 08 06 00 01(. ...+....
0010 08 00 06 04 00 01 28 f1 0e 18 e9 2b c0 a8 64 7a(. ...+..dz
0020 00 00 00 00 00 00 c0 a8 64 05 d.

You can see the destination fffffff's in ether frame

Type field – DIX Ethernet

Doesn't know the target MAC destination add (to put on Ethernet frame)

TCP (initial sequence # - syn, ack)

setting up HTTP session

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
40	39.030382	192.168.100.1	192.168.100.122	ICMP	70	Destination unreachable (Host unreachable)
41	39.058888	192.168.100.122	192.168.111.125	TCP	66	50056→3910 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
42	39.709283	Dell_18:e9:2b	Broadcast	ARP	42	Who has 192.168.100.5? Tell 192.168.100.122
43	39.710061	CiscoInc 3e:62:3e	Dell_18:e9:2b	ARP	60	192.168.100.5 is at 00:14:1c:3e:62:3e
44	39.710085	192.168.100.122	192.168.100.5	TCP	66	50057→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
45	39.711285	192.168.100.5	192.168.100.122	TCP	60	80→50057 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
46	39.711472	192.168.100.122	192.168.100.5	TCP	54	50057→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
47	39.711656	192.168.100.122	192.168.100.5	HTTP	373	GET / HTTP/1.1
48	39.728289	192.168.100.5	192.168.100.122	HTTP	246	HTTP/1.1 401 Unauthorized

Source: 192.168.100.5
Destination: 192.168.100.122
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 80, Dst Port: 50057, Seq: 0, Ack: 1, Len: 0

Source Port: 80
Destination Port: 50057
[Stream index: 6]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 24 bytes

Flags: 0x012 (SYN, ACK)
Window size value: 4128
[Calculated window size: 4128]
Checksum: 0x1901 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Options: (4 bytes), Maximum segment size

```
0000 28 f1 0e 18 e9 2b 00 14 1c 3e 62 3e 08 00 45 00  (....+..>b>..E.
0010 00 2c 00 00 00 00 ff 06 71 fb c0 a8 64 05 c0 a8  .,.....q...d...
0020 64 7a 00 50 c3 89 5b b8 cc c5 c0 41 78 8b 60 12  dz.P..[. ...Ax.`.
0030 10 20 19 01 00 00 02 04 05 b4 00 00                . ....
```

HTTP Protocol – Application Layer

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows a series of HTTP requests from 192.168.100.122 to 192.168.100.5. The packet details pane shows the selected packet (No. 109) with its Ethernet II and Internet Protocol Version 4 headers. Red arrows point from the title to the 'Protocol' column and the 'Info' column. A red circle highlights the 'Protocol' column for the selected packet. A blue arrow points from the text 'Are the frames and sequences are making better sense ?' to the 'Internet Protocol Version 4' header details.

No.	Time	Source	Destination	Protocol	Length	Info
47	39.711656	192.168.100.122	192.168.100.5	HTTP	373	GET / HTTP/1.1
48	39.728289	192.168.100.5	192.168.100.122	HTTP	246	HTTP/1.1 401 Unauthorized
67	48.437078	192.168.100.122	192.168.100.5	HTTP	408	GET / HTTP/1.1
93	48.586549	192.168.100.122	192.168.100.5	HTTP	436	GET /sitewide.js HTTP/1.1
94	48.586582	192.168.100.122	192.168.100.5	HTTP	434	GET /appsui.js HTTP/1.1
101	48.588124	192.168.100.122	192.168.100.5	HTTP	433	GET /forms.js HTTP/1.1
102	48.588150	192.168.100.122	192.168.100.5	HTTP	434	GET /config.js HTTP/1.1
109	48.590885	192.168.100.122	192.168.100.5	HTTP	435	GET /cookies.js HTTP/1.1

▼ Ethernet II, Src: Dell_18:e9:2b (28:f1:0e:18:e9:2b), Dst: CiscoInc_3e:62:3e (00:14:1c:3e:62:3e)
 > Destination: CiscoInc_3e:62:3e (00:14:1c:3e:62:3e)
 > Source: Dell_18:e9:2b (28:f1:0e:18:e9:2b)
 Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.100.122, Dst: 192.168.100.5
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 359

Are the frames and sequences are making better sense ?

HTTP Protocol – Application Layer

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http

lo.	Time	Source	Destination	Protocol	Length	Info
→	47.39.711656	192.168.100.122	192.168.100.5	HTTP	373	GET / HTTP/1.1
→	48.39.728289	192.168.100.5	192.168.100.122	HTTP	246	HTTP/1.1 401 Unauthorized
→	67.48.437078	192.168.100.122	192.168.100.5	HTTP	408	GET / HTTP/1.1
→	93.48.586549	192.168.100.122	192.168.100.5	HTTP	436	GET /sitewide.js HTTP/1.1

[Destination GeoIP: Unknown]

✓ Transmission Control Protocol, Src Port: 50057, Dst Port: 80, Seq: 1, Ack: 1, Len: 319

Source Port: 50057

Destination Port: 80

[Stream index: 6]

[TCP Segment Len: 319]

Sequence number: 1 (relative sequence number)

[Next sequence number: 320 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 20 bytes

> Flags: 0x018 (PSH, ACK)

Window size value: 65535

[Calculated window size: 65535]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x4b2a [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

✓ Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0

```
0020 64 05 c3 89 00 50 c0 41 78 8b 5b b8 cc c6 50 18 d....P.A x.[...P.
0030 ff ff 4b 2a 00 00 47 45 54 20 2f 20 48 54 54 50 ..K*..GE T / HTTP
0040 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 /1.1..Ac cept: te
0050 78 74 2f 68 74 6d 6c 2c 20 61 70 70 6c 69 63 61 xt/html, applica
0060 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 20 tion/xhtml+xml,
```

HTTP enveloped in TCP
TCP enveloped in IP
IP enveloped in Ethernet (Dlink)
Dlink on copper media (CSMA/CD)



http

No.	Time	Source	Destination	Protocol	Length	Info
47	39.711656	192.168.100.122	192.168.100.5	HTTP	373	GET / HTTP/1.1
48	39.728289	192.168.100.5	192.168.100.122	HTTP	246	HTTP/1.1 401 Unauthorized
67	48.437078	192.168.100.122	192.168.100.5	HTTP	408	GET / HTTP/1.1
93	48.586549	192.168.100.122	192.168.100.5	HTTP	436	GET /sitewide.js HTTP/1.1

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 80, Dst Port: 50057, Seq: 1, Ack: 320, Len: 192

Source Port: 80

Destination Port: 50057

[Stream index: 6]

[TCP Segment Len: 192]

Sequence number: 1 (relative sequence number)

[Next sequence number: 193 (relative sequence number)]

Acknowledgment number: 320 (relative ack number)

Header Length: 20 bytes

> Flags: 0x010 (ACK)

Window size value: 3809

[Calculated window size: 3809]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xf715 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

Hypertext Transfer Protocol

> HTTP/1.1 401 Unauthorized\r\n

Date: Fri, 01 Mar 2002 00:50:44 GMT\r\n

Server: cisco-IOS\r\n

Connection: close\r\n

This is the banner in cisco as
Logging into the AP device

0000	28 f1 0e 18 e9 2b 00 14 1c 3e 62 3e 00 00 45 00	(...+...>b>...E.
0010	00 e8 00 01 00 00 ff 06 71 3e c0 a8 64 05 c0 a8 q>..d...
0020	64 7a 00 50 c3 89 5b b8 cc c6 c0 41 79 ca 50 10	dz.P..[. ...Ay.P.
0030	0e e1 f7 15 00 00 48 54 54 50 2f 31 2e 31 20 34HT TP/1.1 4
0040	30 31 20 55 6e 61 75 74 68 6f 72 69 7a 65 64 0d	01 Unaut horized.
0050	0e 14 01 74 05 00 00 45 72 60 00 00 00 00 00 4d	Date: Fri, 01 Mar 2002 00:50:44 GMT