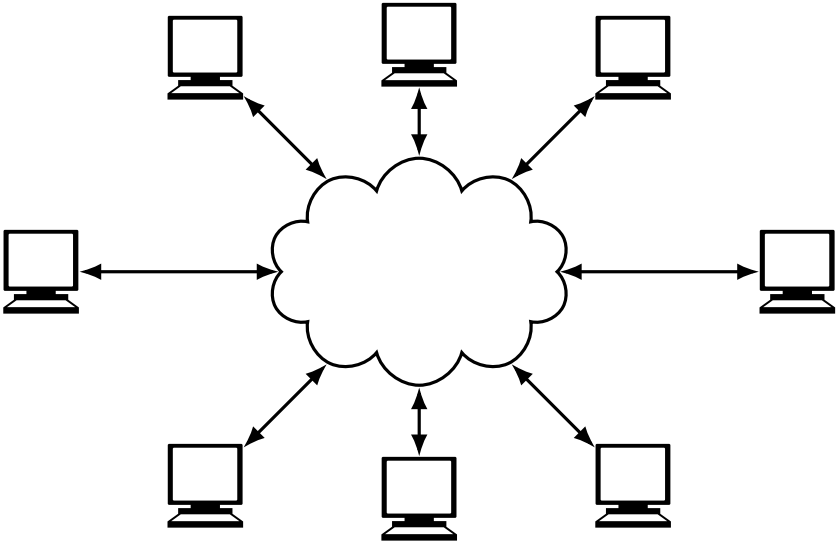
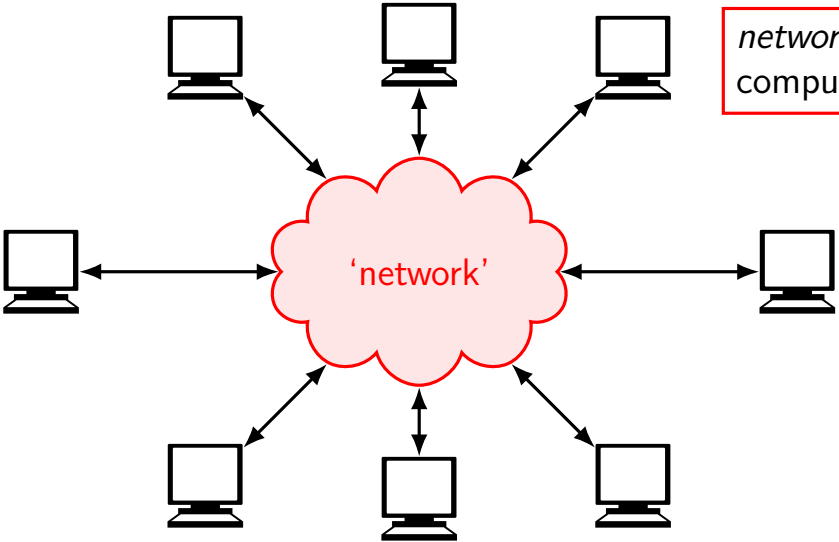
networks / hosts aka end systems

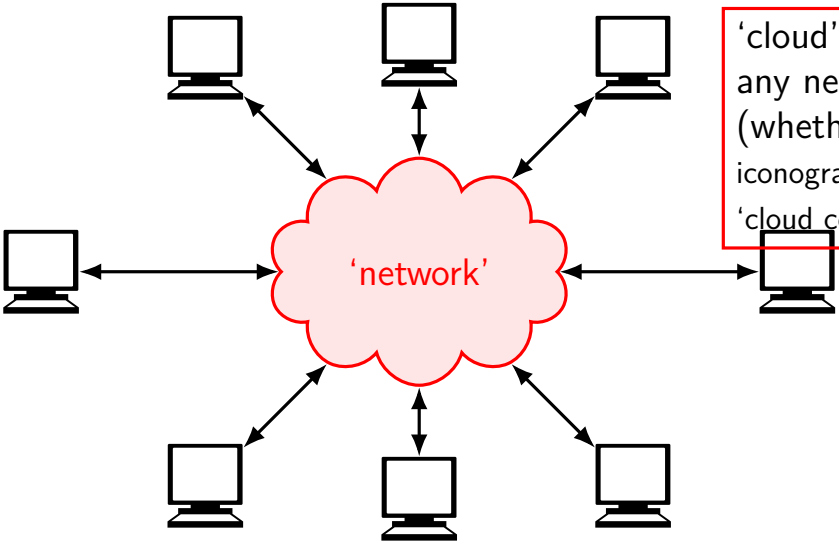


networks / hosts aka end systems



networks connect computers

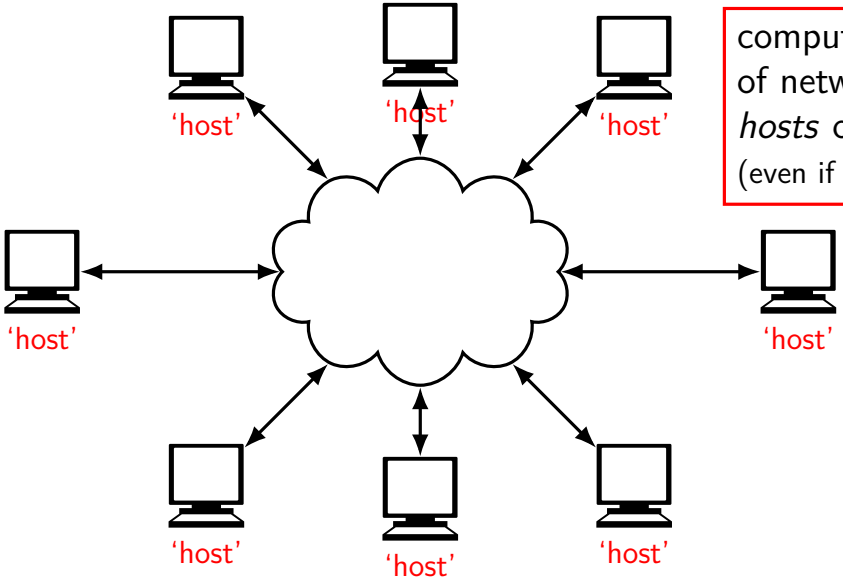
networks / hosts aka end systems



'cloud' represents any network (whether local or not)

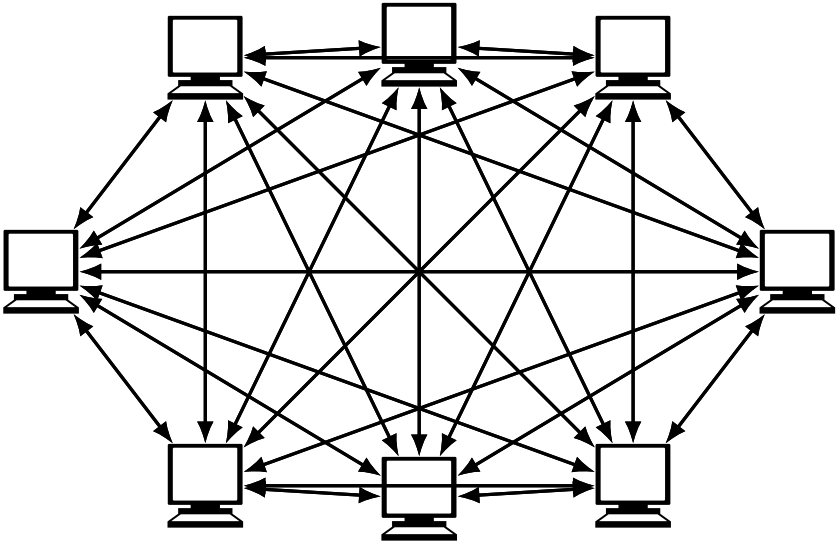
iconography predates 'cloud computing'

networks / hosts aka end systems

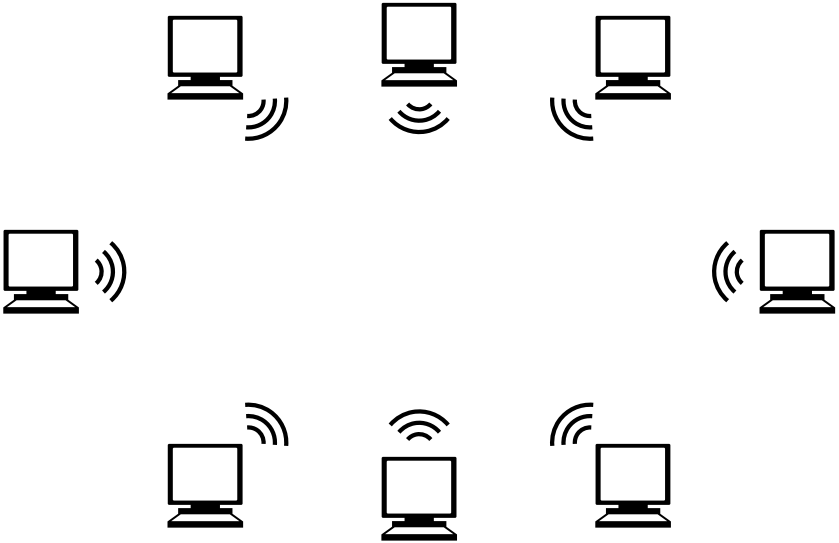


computers on edge of network called *hosts* or *end systems* (even if also 'servers')

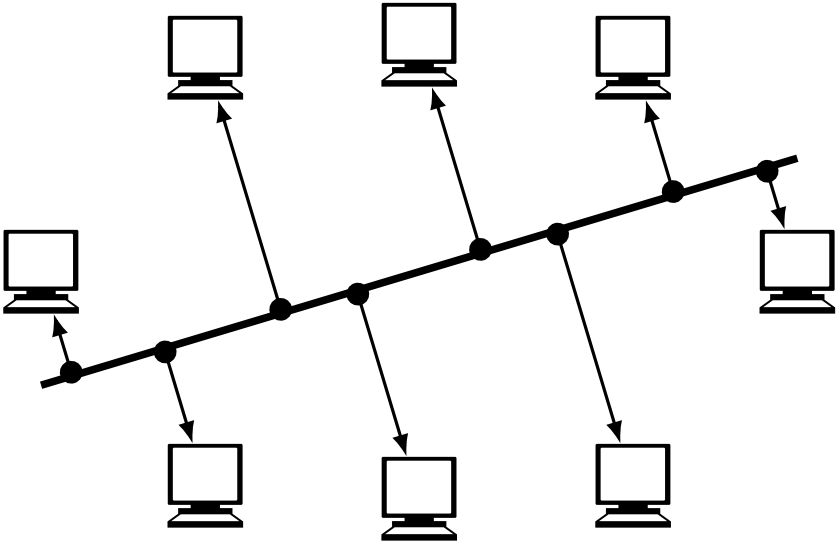
direct connections?



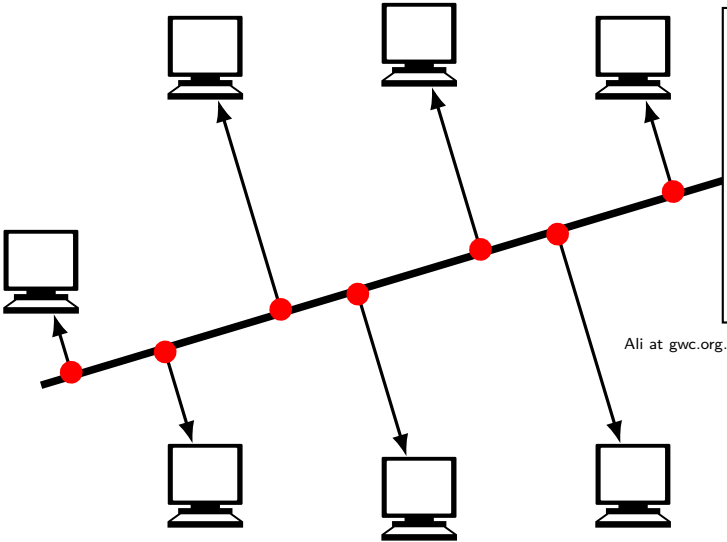
shared medium: radio?

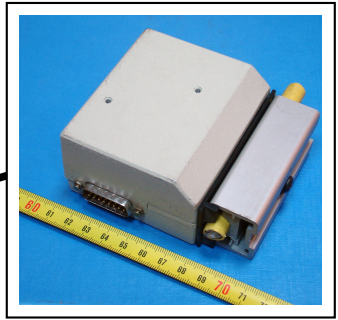


shared medium: wires

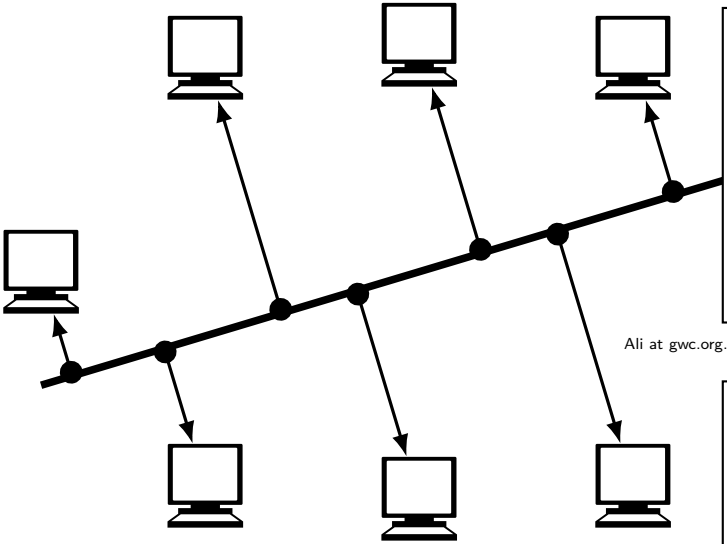


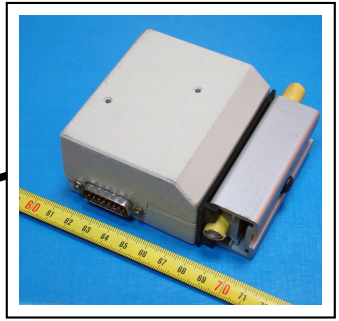
shared medium: wires





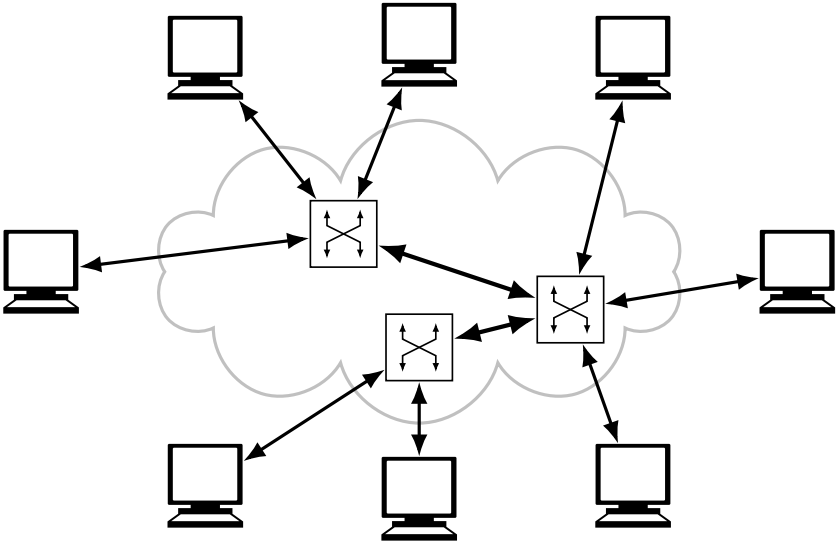
shared medium: wires



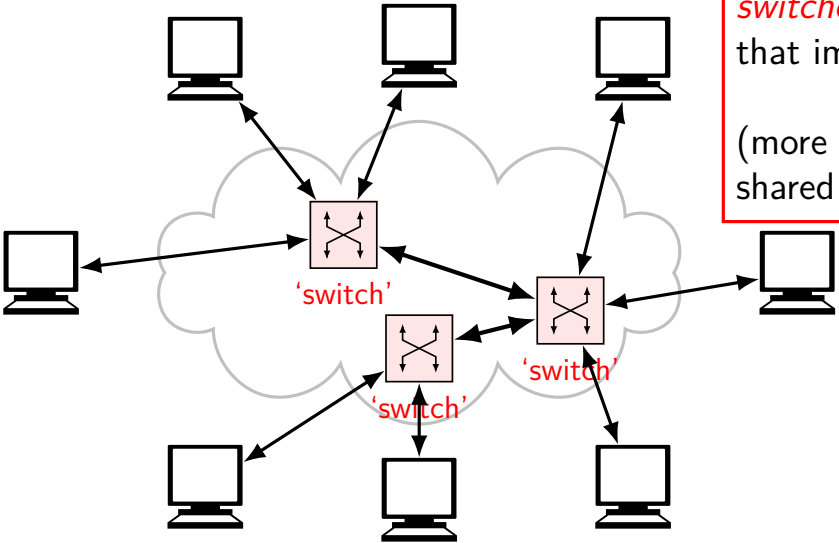


Ali at gwc.org.uk / Alistair1978 via Wikimedia commons / CC-BY-SA 2.5

switches / nodes / links



switches / nodes / links

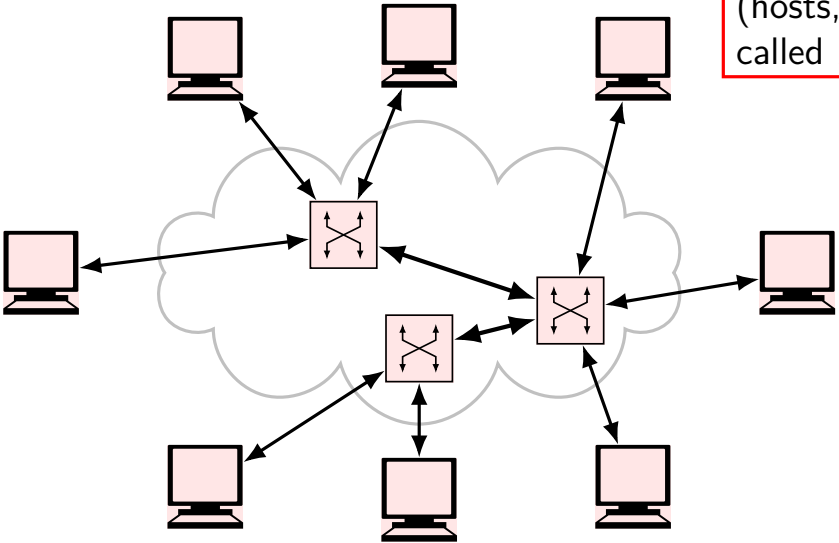


hosts directly connected to *switches* that implement network

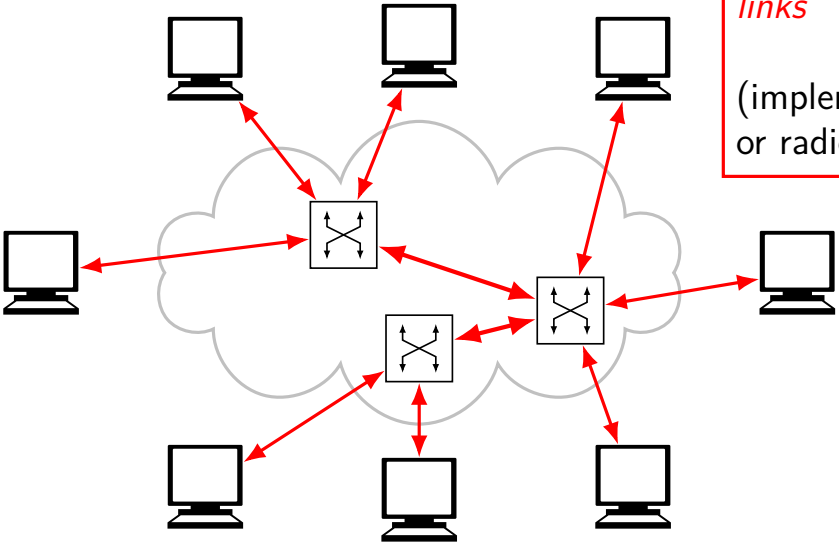
(more efficiently than shared medium)

switches / nodes / links

machines on network (hosts, switches, ...) called *nodes*



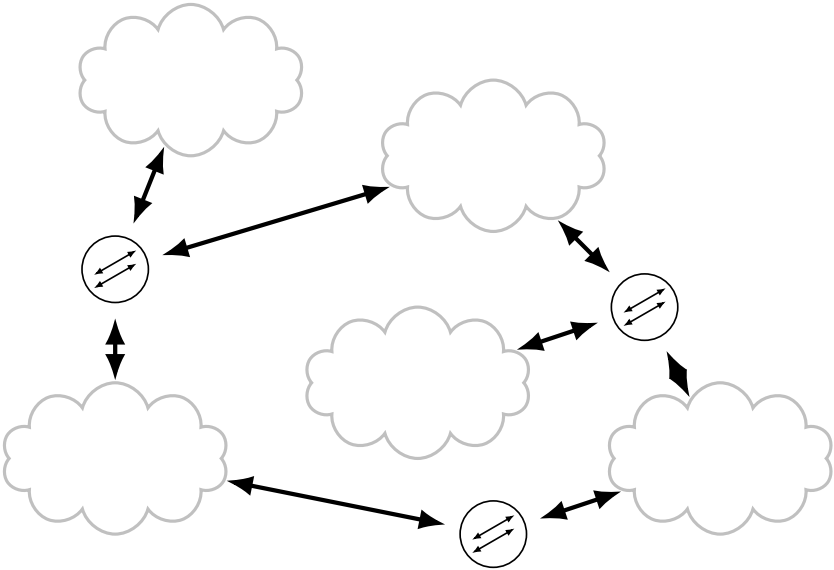
switches / nodes / links



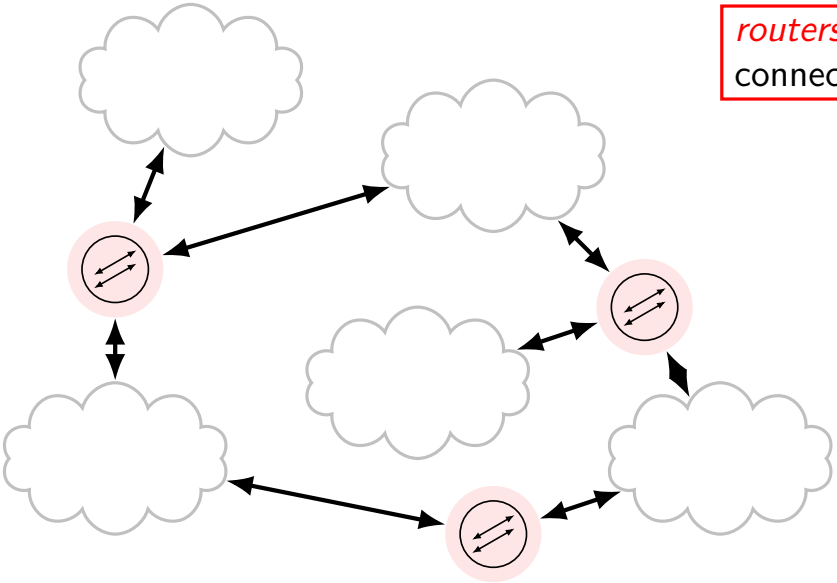
nodes connected by *links*

(implemented by wires or radio or ...)

routers / internetwork

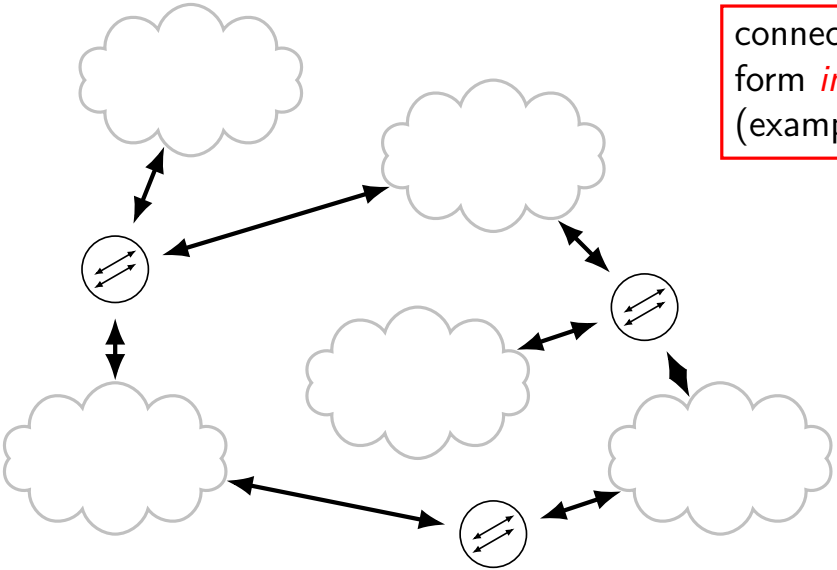


routers / internetwork



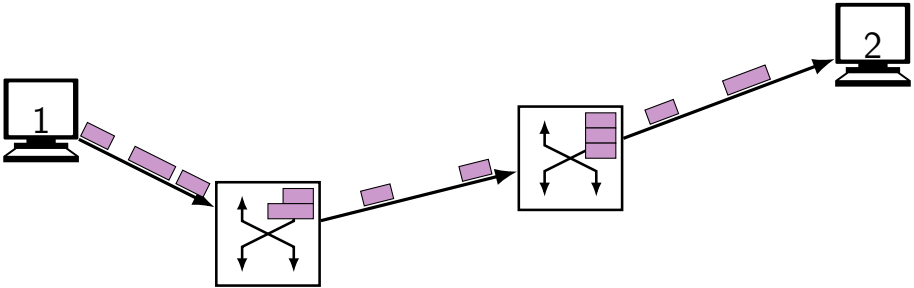
routers or *gateways* connect networks

routers / internetwork



connected networks form *internetwork* (example: the Internet)

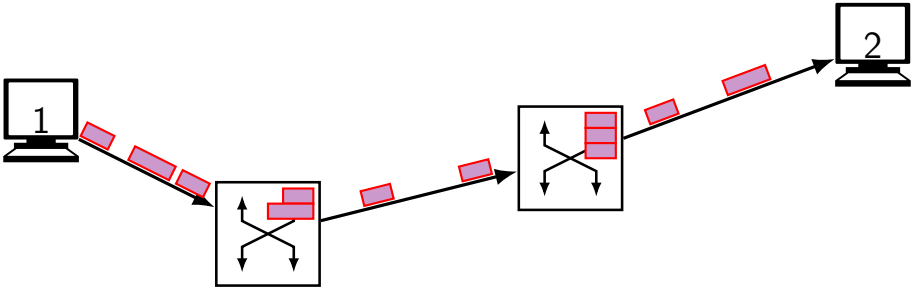
flows / packets



flow of data between two machines

flow is very general term
will depend on context how it relates to connections, sockets, etc.

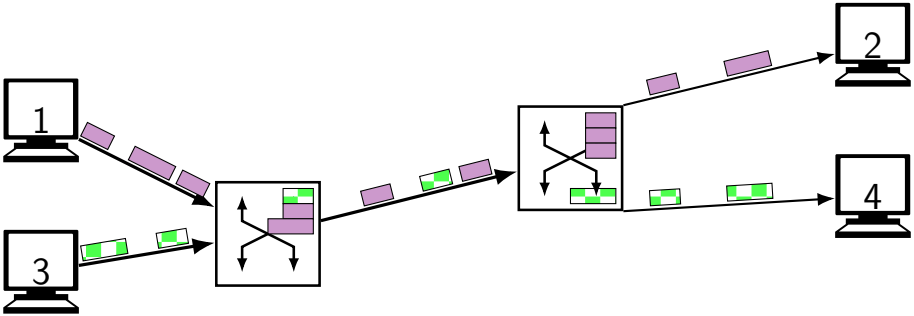
flows / packets



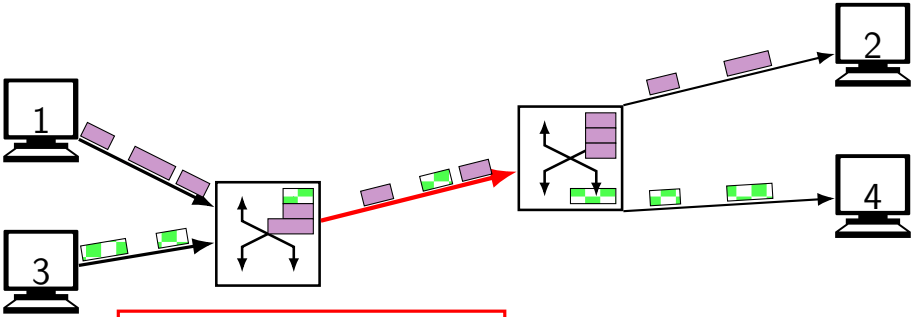
flow of data between two machines

possibly divided up into pieces,
called *packets*, *frames*, *segments*
(which name is best depends on context)

(de)multiplexing

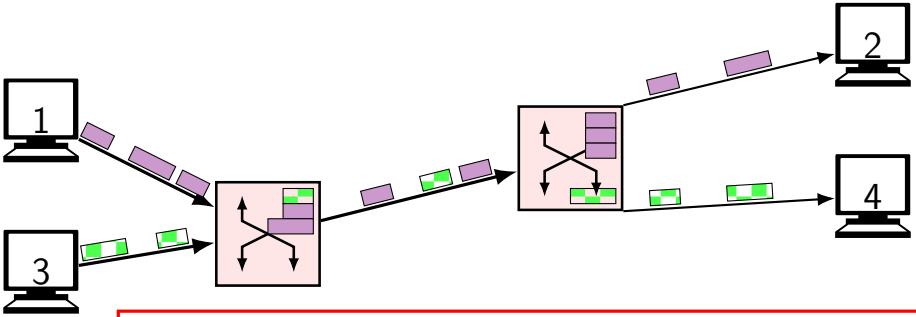


(de)multiplexing



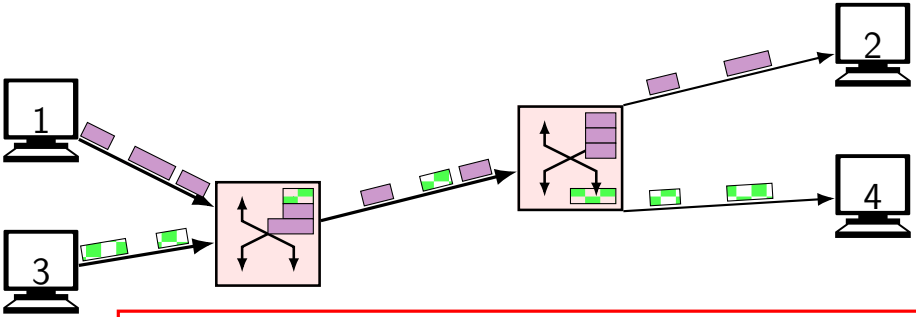
two or more flows can share one or more links

(de)multiplexing



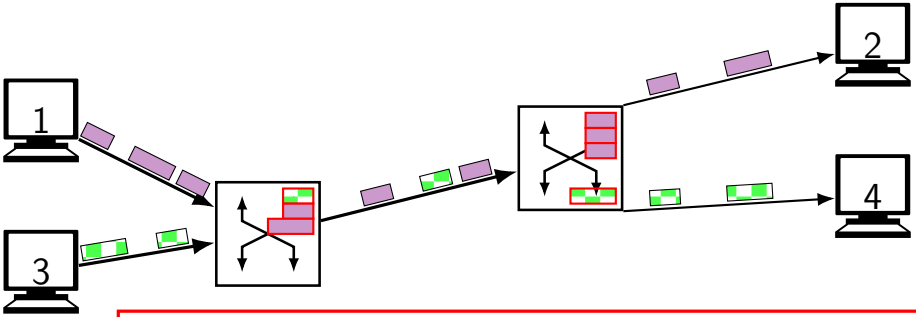
left switch *multiplexes* the two flows onto one link
right switch *demultiplexes* them to separate them

(de)multiplexing



this picture: multiplexed by dividing up *time* on link

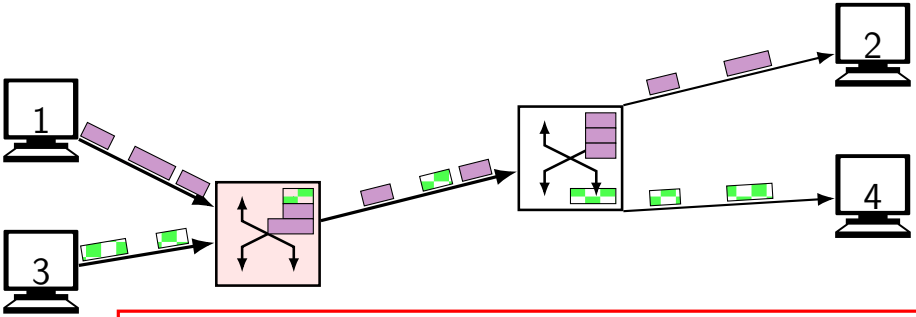
(de)multiplexing



switches usually have *buffers* (also called *queues*) hold waiting packets

absorbs temporary "bursts" where packets come faster than outgoing link can handle

(de)multiplexing

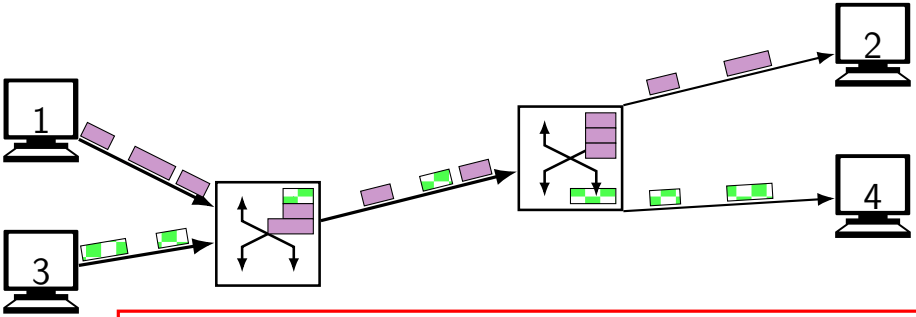


incomplete list of causes of ‘bursts’:

multiple unsynchronized flows

fast links produce packets faster for slow can send

(de)multiplexing

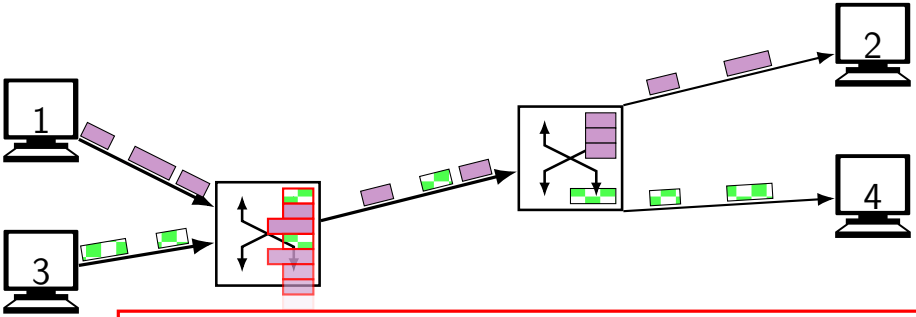


incomplete list of causes of ‘bursts’:

multiple unsynchronized flows

fast links produce packets faster for slow can send

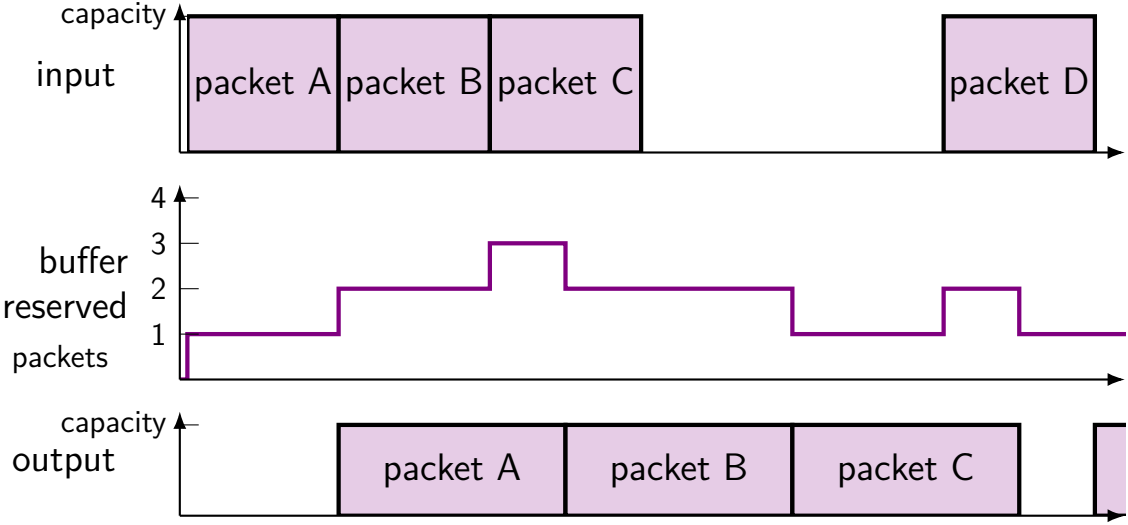
(de)multiplexing



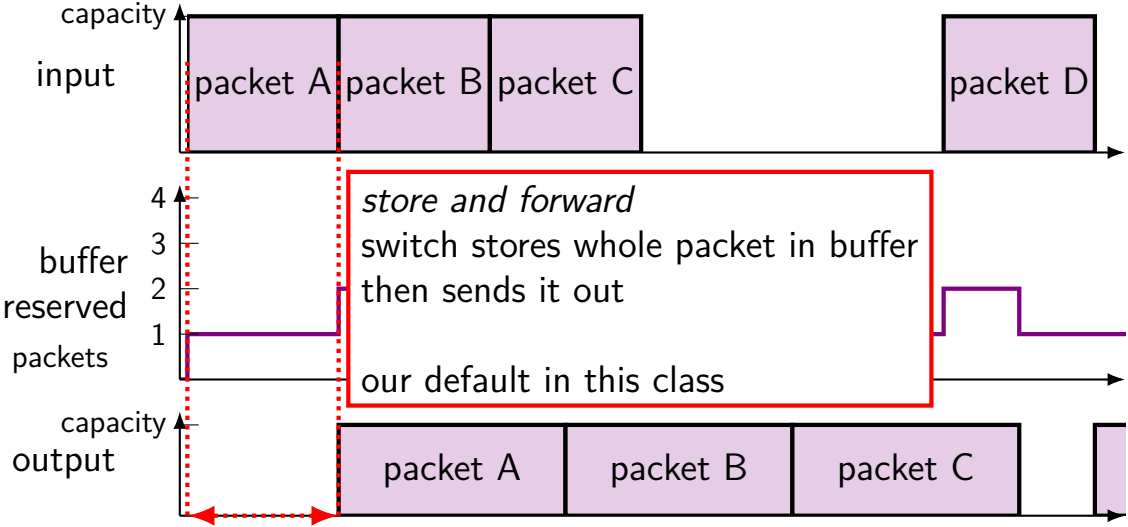
if buffer full, switch must *drop* packets
will happen eventually if overall rate faster than outgoing link

scenario is called *congestion*

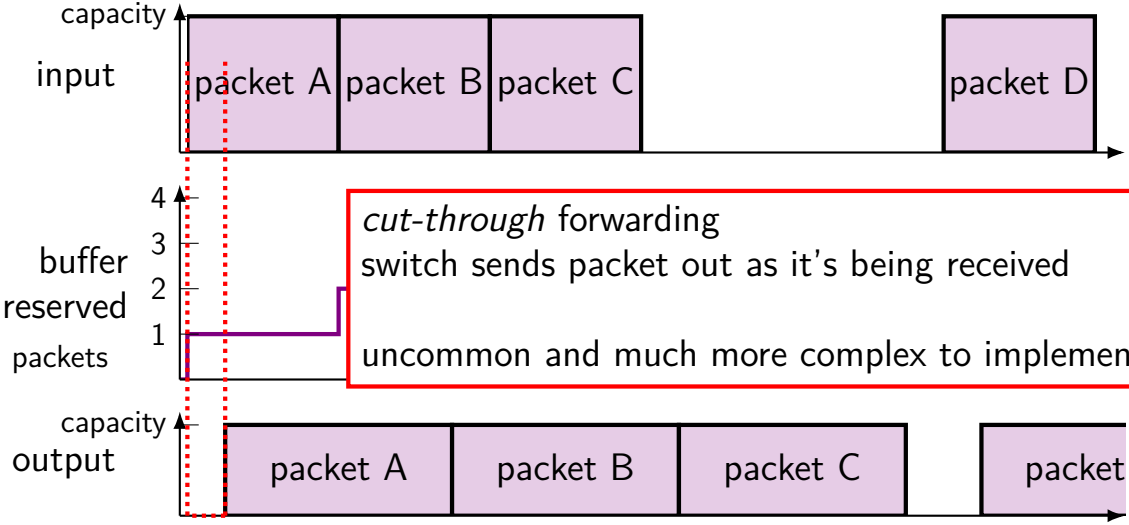
buffer usage: fast to slow, store + forward



buffer usage: fast to slow, store + forward



buffer usage: fast to slow, cut-through



cut-through forwarding
switch sends packet out as it's being received

uncommon and much more complex to implement

channel abstractions

want to avoid custom network for each application

but applications have different needs

$\rightarrow$ multiple application interfaces to networks

common implementation of common patterns

some abstractions

stream

- continuous stream of bytes from one program to another
- 'connection' from one program to another

datagrams

- send small messages (*datagrams*)
- each datagram's destination independently set

remote procedure calls

- make function calls that run on remote machine

remote memory access

- read/write bytes of data in remote memory

...

some abstractions

stream

- continuous stream of bytes from one program to another
- 'connection' from one program to another

datagrams

- send small messages (*datagrams*)
- each datagram's destination independently set

remote procedure calls

- make function calls that run on remote machine

remote memory access

- read/write bytes of data in remote memory

...

focus on streams

this class: focus on implementing *streams of bytes*

why?

- most commonly used by applications on the Internet
- many common tasks with other abstractions

stream abstraction and sockets

BSD *sockets* are most used abstract for using *streams*

server (passive end)

- create socket (`socket()`)
- select address (`bind()`)
- wait for+get connection (`listen()`+`accept()`)
- read+write on connection(`read()`+`recv*()`+`write()`+`send*()`)

client (active end)

- create socket (`socket()`)
- connect to address (`connect()`
- read+write on connection(`read()`+`recv*()`+`write()`+`send*()`)

sockets and other options

sockets can also provide *datagram* abstraction

difference: mode where read/write keeps messages together

socket details later

we're doing mostly bottom-up approach

will actually talk in detail about socket interface later in semester

client/server

server = entity that waits for + responds to *clients*

server:

- always-on
- well-known how to contact

client

- sometimes on
- only contacted by server responding to it

not client/server?

not everything fits into client/server neatly

sometimes something is both client and server

sometimes no distinguished entities (“peer-to-peer”)

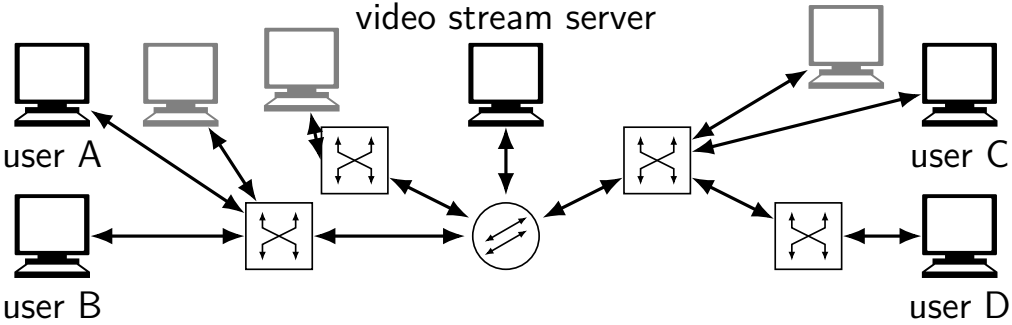
client/server and channels

can have channels without client/server model

but the interface sockets provide assume client/server

(so you have to make something server-like to do peer-to-peer with sockets)

exercise



if each of users A–D are receiving (potentially different) video and audio from the video streaming server, then…

- how many flows?
- how many nodes are involved?
- how many switches/routers?

IETF

IETF = Internet Engineering Task Force

- part of non-profit called *Internet Society*

most common internet protocols standardized by IETF

most IETF documents called RFCs

- requests for comment
- have unique number

`https://rfc-editor.org`

other standard orgs

Bluetooth Special Interest Group

IEEE (Institute of Electrical and Electronics Engineers)

- Wifi, Ethernet, ...

3GPP (3rd Generation Partnership Project)

- cellular phone networks

SCTE (Society of Cable Televsion Engineers)

ITU (International Telecommunication Union)

ISO (International Organization for Standardization)

some challenges for streams

separating data into pieces network can handle

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

handling transmission errors

some challenges for streams

separating data into pieces network can handle

putting pieces back together

getting network to send piece to correct remote network

getting ne

lots of work! don't want to implement all at once!

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

handling transmission errors

some challenges for streams

separating data into pieces network can handle

putting

some parts need to be different for different local networks

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

handling transmission errors

some challenges for streams

separa

some parts should not concern local network implementors

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

handling transmission errors

some challenges for streams

separating

some parts should be same for different abstraction

putting pieces back together

getting network to send piece to correct remote network

getting network to send piece to correct machine

getting machine to send data to correct program

getting pieces into format wires/radio/fiber/etc. can handle

handling transmission errors

layered model

networking implemented in ‘layers’

upper layers implemented by making calls to lower layers

example: network implements ‘send data to (remote) machine’ function (“network layer”)

stream implementation calls this to implement ‘send stream to remote application’

OSI model

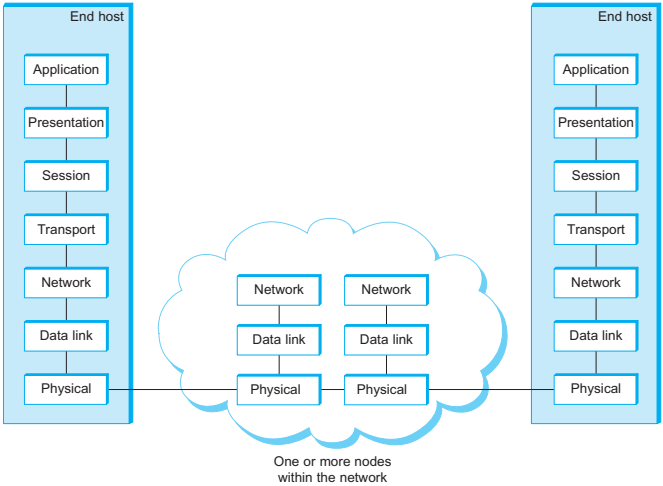
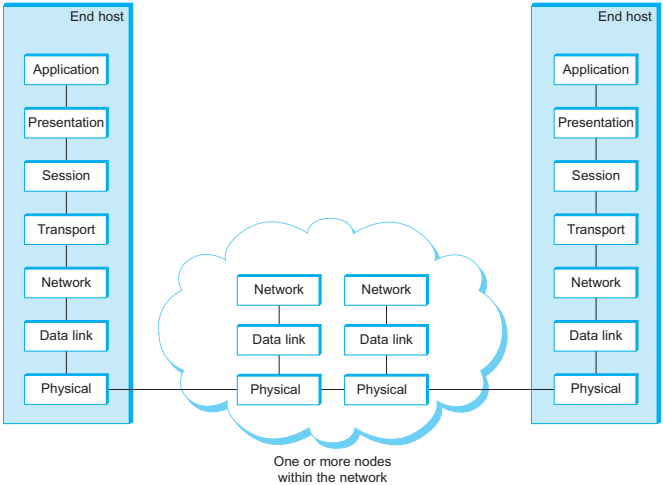


Figure 13 of Chapter 1 of Computer Networks: A Systems Approach (6th ed) (Peterson and Davie)

OSI model

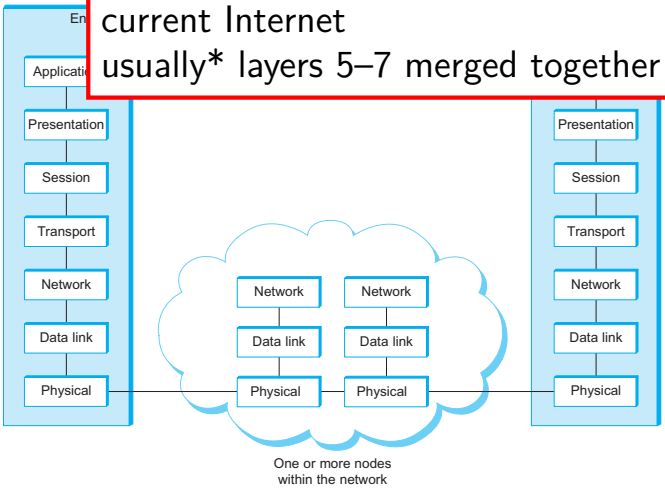


(7) application:
what requests/etc.
(6) presentation:
data format
(5) session:
manage group of streams
(4) transport:
streams of data
(3) network:
message to correct network
(2) data link:
message → bits
message to correct machine
(1) physical:
send bits/...

Figure 13 of Chapter 1 of Computer Networks: A Systems Approach (6th ed) (Peterson and Davie)

OSI model

current Internet
usually* layers 5–7 merged together



(7) application:
what requests/etc.
(6) presentation:
data format
(5) session:
manage group of streams
(4) transport:
streams of data
(3) network:
message to correct network
(2) data link:
message → bits
message to correct machine
(1) physical:
send bits/...

Figure 13 of Chapter 1 of Computer Networks: A Systems Approach (6th ed) (Peterson and Davie)

OSI model

standardized by ISO (International Standards Organization) and ITU (International Telecommunications Union)

full set of protocols...

- file transfer, message sending, directory lookups ...

that were often implemented and sometimes used...

but mostly lost out to IETF-standardized Internet protocols

- Internet Engineering Task Force

OSI influence (1)

term ‘layer 7’, ‘layer 4’, ‘layer 3’, etc. almost always refer to OSI model

...even though most of Internet does not follow it

- early Internet protocols predate OSI

OSI influence (2)

are a lot of Internet protocols influenced by OSI protocols

OSI's DAP (directory access protocol)

- adapted into IETF's LDAP (lightweight directory access protocol)

OSI presentation layer ASN.1 used in...

- telephony (between telephone companies)
- inter-bank messaging
- lots of cryptography-related protocols
- ...

OSI's routing protocol IS-IS still common in large Internet-connected networks

- (adapted to work alongside IETF protocols)

Internet layers

OSI layer	name	examples	purpose
7	application	HTTP, SSH, SMTP, DNS, ...	application-defined meanings
4	transport	TCP, UDP, ...	reach correct program, reliablity/streams
3	network	IPv4, IPv6, ...	reach correct machine (across networks)
2	link	Ethernet, Wi-Fi, ...	coordinate shared wire/radio
1	physical	...	encode bits for wire/radio

Internet layers

OSI layer	name	examples	purpose
7	application	HTTP, SSH, SMTP, DNS, ...	application-defined meanings
4	transport	TCP, UDP, ...	reach correct program, reliablity/streams
3	network	IPv4, IPv6, ...	reach correct machine (across networks)
2	link	Ethernet, Wi-Fi, ...	coordinate shared wire/radio
1	physical	...	encode bits for wire/radio

Internet protocols and layers (non-exhaustive)

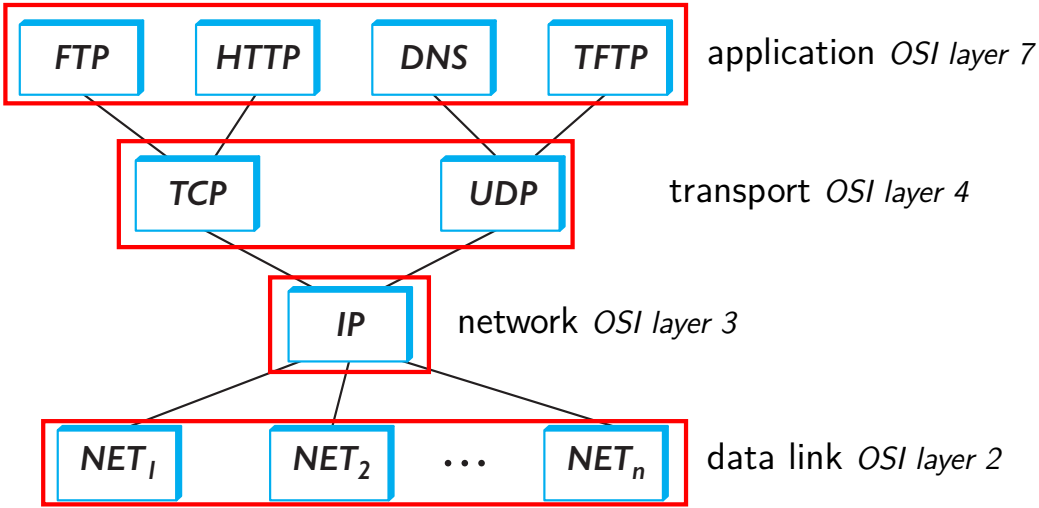


Figure 14 of Chapter 1 of Computer Networks: A Systems Approach (6th ed) (Peterson and Davie)

Internet protocols and layers (non-exhaustive)

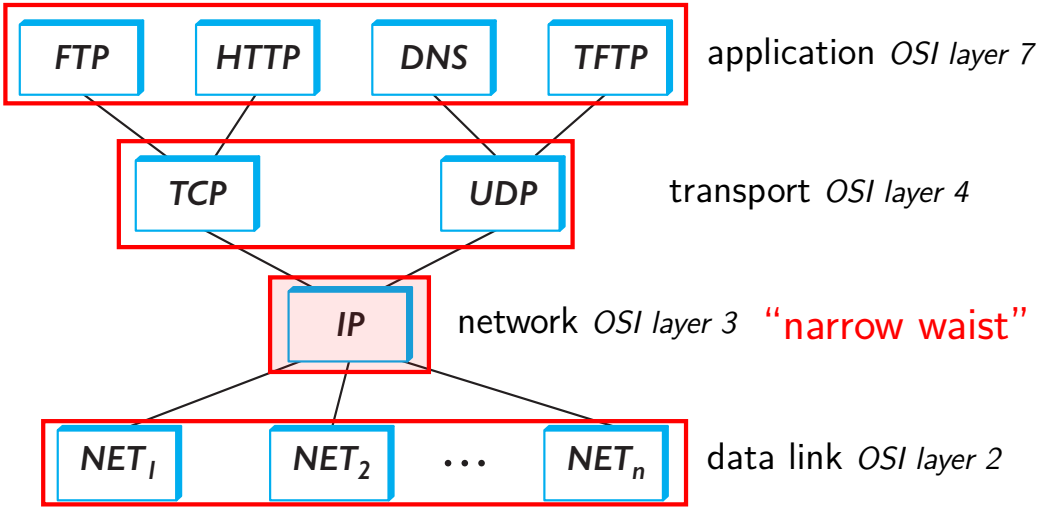


Figure 14 of Chapter 1 of Computer Networks: A Systems Approach (6th ed) (Peterson and Davie)

fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer...

- so seems like a transport layer protocol?

fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer...

- so seems like a transport layer protocol?

used to send errors/control messages about routing...

- routing is the network layer's job
- so ICMP is part of network layer?

fuzzy layers (1)

ICMP (Internet Control Message Protocol)...

implemented using a network layer...

- so seems like a transport layer protocol?

used to send errors/control messages about routing...

- routing is the network layer's job
- so ICMP is part of network layer?

I think saying network layer is probably better...

but we're not going to be picky about it

fuzzy layers (2)

TLS (Transport Control Protocol)...

implemented on top of TCP...

- so seems like a application layer protocol?

fuzzy layers (2)

TLS (Transport Control Protocol)...

implemented on top of TCP...

- so seems like a application layer protocol?

used to send other application layer protocols

- so maybe a transport layer?
- or presentation layer?

I'll call it an application layer...

‘extra’ layers

layer terminology doesn’t always work cleanly

- often “extra” layers in practice

e.g. HTTPS:

- HTTP (app layer) on TLS (another app layer) on TCP (network) on ...

e.g. DNS over HTTPS:

- DNS (app layer) on HTTP on on TLS on TCP on ...

e.g. SFTP:

- SFTP (app layer??) on SSH (another app layer) on TCP on ...

e.g. HTTP over OpenVPN:

- HTTP on TCP on IP on OpenVPN on UDP on different IP on ...

‘extra’ layers

layer terminology doesn’t always work cleanly

often “extra” layers in practice

e.g. HTTPS:

HTTP (app layer) on TLS (another app layer) on TCP (network) on ...

e.g. DNS over HTTPS:

DNS (app layer) on HTTP on on TLS on TCP on ...

e.g. SFTP:

SFTP (app layer??) on SSH (another app layer) on TCP on ...

e.g. HTTP over OpenVPN:

HTTP on TCP on IP on OpenVPN on UDP on different IP on ...

protocols usually over HTTP

SOAP (Simple Object Access Protocol) — messaging/remote procedure calls

gRPC (originally form Google) — remote procedure calls

HLS (HTTP Live Streaming) — video streaming

DASH (Dynamic Adaptive Streaming over HTTP) — video streaming

...

packet capture tools

packet capture = log of everything sent/received on some link(s)

wireshark is popular tool for making, analyzing packet captures

will be showing screenshots from that

you can download these packet captures, follow along in wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15			Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15			ponse 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4			/dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

wireshark window

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 199
    Identification: 0xd07b (53371)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7e03 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·******
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ******6·
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·******· %···!··!
0090  d6 9e ec 48 5b d1 cc 83  03 00 b6 c4 8b ab 0b c0   ···H[··· ********
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1··
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:·
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Source Address (ip.src), 4 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 199
    Identification: 0xd07b (53371)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7e03 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%·· ···!··!
0090  d6 9e ec 48 5b d1 cc 83  03 00 b6 c4 8b ab 0b c0   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Source Address (ip.src), 4 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4			d query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15			0510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15			0510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4			[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

packet list

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 199
    Identification: 0xd07b (53371)
  ▸ 010. .... = Fla
    ...0 0000 0000
    Time to Live: 6
    Protocol: TCP (
    Header Checksum: 0x7e03 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

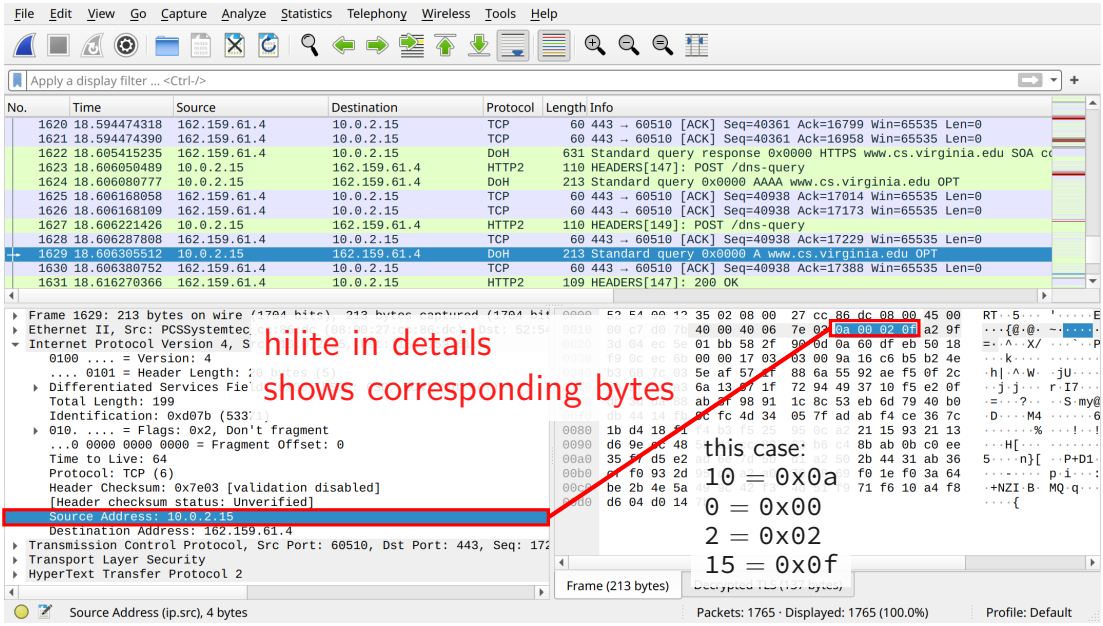
packet details

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6|
0080  1b d4 18 f1 f4 [illegible] 13   ·····% ···!··!·
0090  d6 9e ec 48 5b [illegible] ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad [illegible] 36   5····n}[ ··P+D1·
00b0  cf f0 93 2d 95 [illegible] 64   ···-···· p·i··:
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

packet bytes

Frame (213 bytes) | Decrypted TLS (137 bytes)

Source Address (ip.src), 4 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1620 18.594474318 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621 18.594474390 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622 18.605415235 162.159.61.4 10.0.2.15 DoH 631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623 18.606050489 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[147]: POST /dns-query
1624 18.606080777 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625 18.606168058 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626 18.606168109 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627 18.606221426 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[149]: POST /dns-query
1628 18.606287808 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629 18.606305512 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 A www.cs.virginia.edu OPT
1630 18.606380752 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631 18.616270366 162.159.61.4 10.0.2.15 HTTP2 109 HEADERS[147]: 200 OK
Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
Ethernet II, Src: PCSSystemtec
Internet Protocol Version 4, S
0100 .... = Version: 4
.... 0101 = Header Length: 2
Differentiated Services Fie
Total Length: 199
Identification: 0xd07b (533
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x7e03 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 162.159.61.4
Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
Transport Layer Security
HyperText Transfer Protocol 2
0000 52 54 00 12 35 02 08 00 27 cc 86 dc 08 00 45 00
0010 00 c7 d0 7b 40 00 40 06 7e 03 0a 00 02 0f a2 9f
0020 3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18
0030 f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4e
0040 b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2c
0050 6a 13 67 1f 72 94 49 37 10 f5 e2 0f
0060 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0
0070 9c fc 4d 34 05 7f ad ab f4 ce 36 7c
0080 1b d4 18 51 21 15 93 21 13
0090 d6 9e 6c 48 8b ab 0b c0 ee
00a0 35 5f d5 e2 2b 44 31 ab 36
00b0 e7 f0 93 2d f0 1e f0 3a 64
00c0 be 2b 4e 5a 71 f6 10 a4 f8
00d0 d6 04 d0 14
RT··5··· ·····E
···{@·@· ~·····
=···^··X/ ····P
···k···· ·····
·h|·^·W· jU····
··j·j··· r·I7···
·=···?·· ··S·my@
·D···M4 ·····6
·····% ···!··!
···H[··· ·····
5···n}[··P+D1
····-··· p·i··:
·+NZI·B· MQ·q··
····{
hilite in details
shows corresponding bytes
this case:
10 = 0x0a
0 = 0x00
2 = 0x02
15 = 0x0f
Frame (213 bytes)
Source Address (ip.src), 4 bytes
Packets: 1765 · Displayed: 1765 (100.0%)
Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP		Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2		r /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP		Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH		0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP		Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2		

‘protocol’

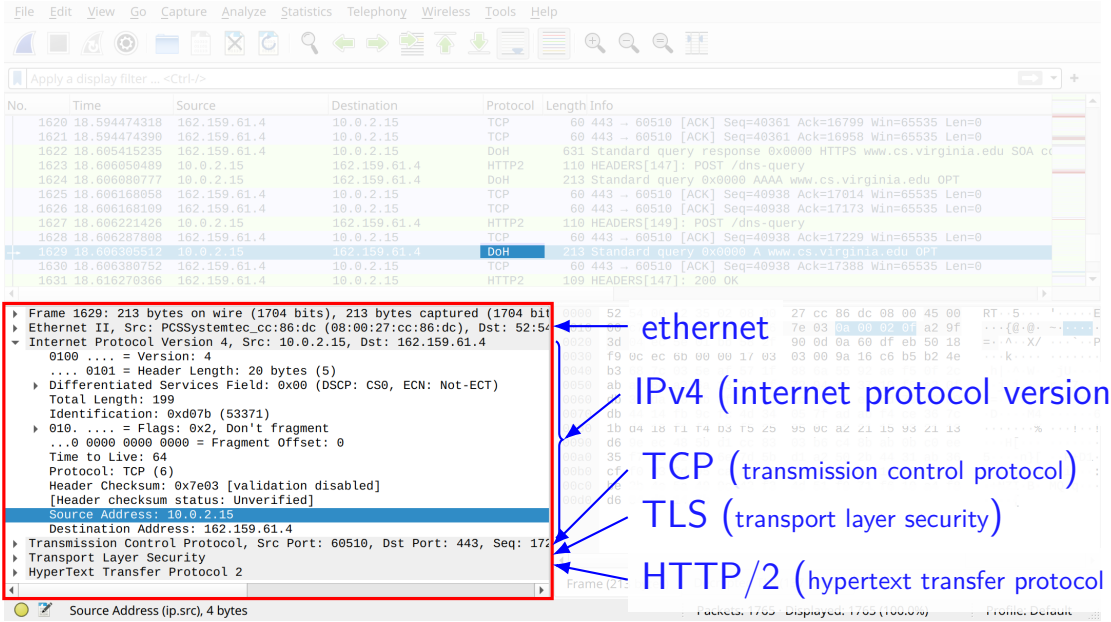
the highest-layer protocol decoded

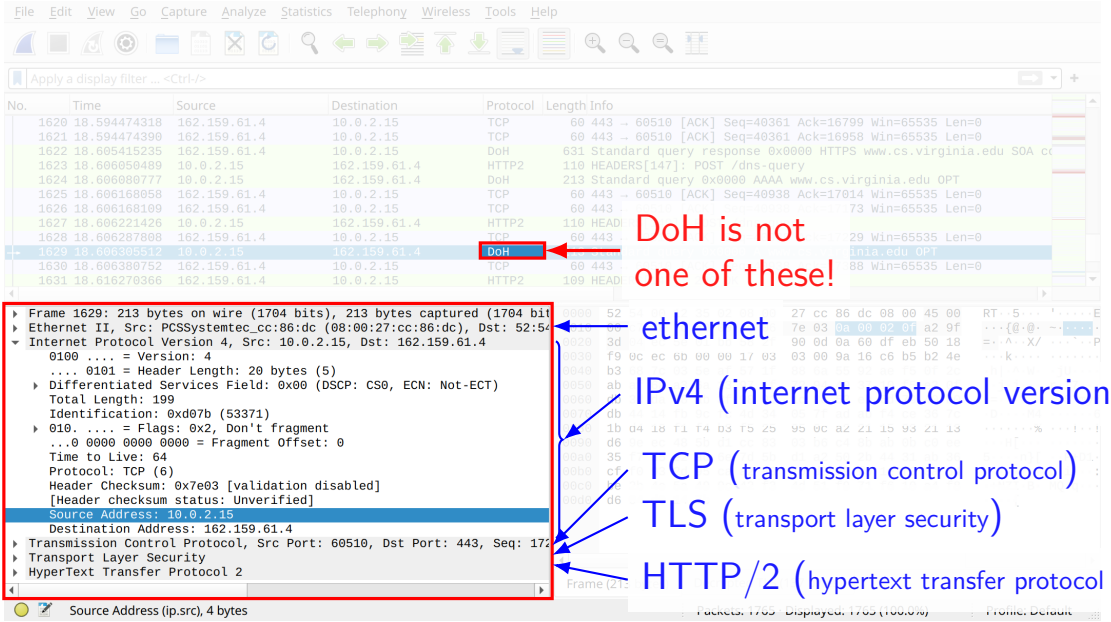
```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bi
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 199
    Identification: 0xd07b (53371)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7e03 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

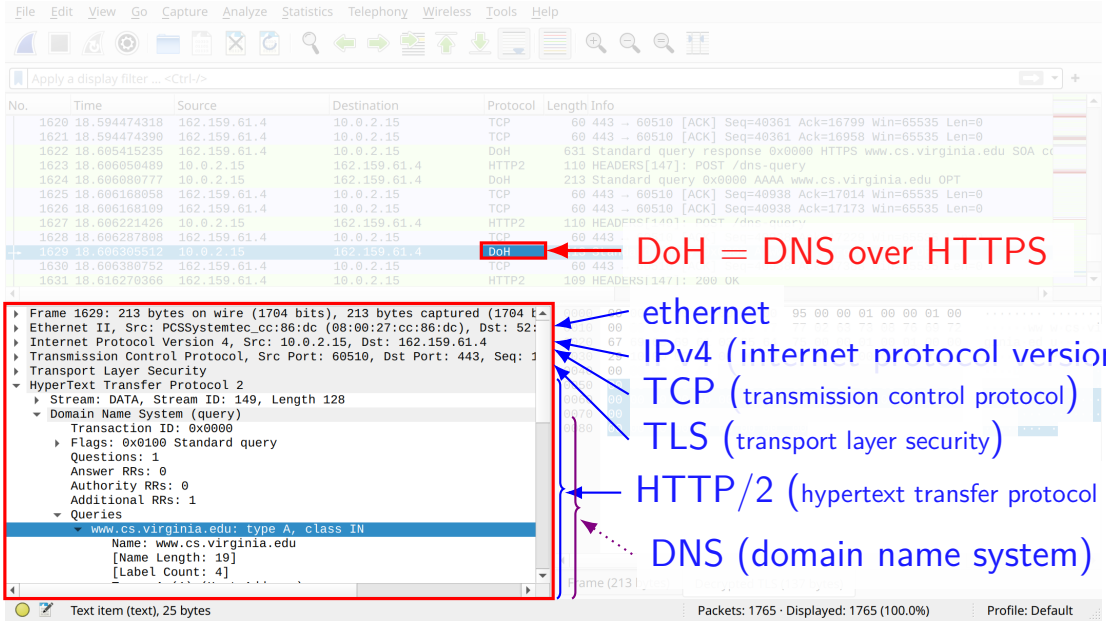
```
0000  52 54 00 12 35 02 08 00 27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06 7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f 90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03 03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f 88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f 72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91 1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34 05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6
0080  1b d4 18 f1 f4 b3 f5 25 95 0c a2 21 15 93 21 13   ·····%·· ···!··!
0090  d6 9e ec 48 5b d1 cc 83 03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0 70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3 4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                    ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Source Address (ip.src), 4 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1620 18.594474318 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621 18.594474390 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622 18.605415235 162.159.61.4 10.0.2.15 DoH 631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co
1623 18.606050489 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[147]: POST /dns-query
1624 18.606080777 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625 18.606168058 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626 18.606168109 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627 18.606221426 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[149]: POST /dns-query
1628 18.606287808 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629 18.606305512 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 A www.cs.virginia.edu OPT
1630 18.606380752 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631 18.616270366 162.159.61.4 10.0.2.15 HTTP2 109 HEADERS[147]: 200 OK
Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 199
Identification: 0xd07b (53371)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x7e03 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 162.159.61.4
Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
Transport Layer Security
HyperText Transfer Protocol 2
Source Address (ip.src), 4 bytes
ethernet
IPv4 (internet protocol version 4)
TCP (transmission control protocol)
TLS (transport layer security)
HTTP/2 (hypertext transfer protocol 2)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1620 18.594474318 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621 18.594474390 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622 18.605415235 162.159.61.4 10.0.2.15 DoH 631 Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA
1623 18.606050489 10.0.2.15 162.159.61.4 HTTP2 110 HEADERS[147]: POST /dns-query
1624 18.606080777 10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625 18.606168058 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626 18.606168109 162.159.61.4 10.0.2.15 TCP 60 443
1627 18.606221426 10.0.2.15 162.159.61.4 HTTP2 110
1628 18.606287808 162.159.61.4 10.0.2.15 TCP 60 443
1629 18.606305512 10.0.2.15 162.159.61.4 DoH
1630 18.606380752 162.159.61.4 10.0.2.15 TCP 60 443
1631 18.616270366 162.159.61.4 10.0.2.15 HTTP2 109
Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 199
Identification: 0xd07b (53371)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x7e03 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 162.159.61.4
Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
Transport Layer Security
HyperText Transfer Protocol 2
Source Address (ip.src), 4 bytes
DoH is not one of these!
ethernet
IPv4 (internet protocol version 4)
TCP (transmission control protocol)
TLS (transport layer security)
HTTP/2 (hypertext transfer protocol 2)



DoH = DNS over HTTPS

ethernet

IPv4 (internet protocol version 4)

TCP (transmission control protocol)

TLS (transport layer security)

HTTP/2 (hypertext transfer protocol 2)

DNS (domain name system)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·******N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ******6|
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·******% ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ********
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Ethernet (eth), 14 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·******N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ******6|
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·******% ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ********
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1··6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Ethernet (eth), 14 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6|
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%·· ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Internet Protocol Version 4 (ip), 20 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%·· ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Internet Protocol Version 4 (ip), 20 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%·· ···!··!
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Transmission Control Protocol (tcp), 20 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%·· ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Transmission Control Protocol (tcp), 20 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·******
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ******6·
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   *******% ***!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ********
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1··
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ******** p·i···:·
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Transport Layer Security (tls), 159 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bit
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:54
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 172
▸ Transport Layer Security
▸ HyperText Transfer Protocol 2
```

```
0000  52 54 00 12 35 02 08 00  27 cc 86 dc 08 00 45 00   RT··5··· '·····E·
0010  00 c7 d0 7b 40 00 40 06  7e 03 0a 00 02 0f a2 9f   ···{@·@· ~·····
0020  3d 04 ec 5e 01 bb 58 2f  90 0d 0a 60 df eb 50 18   =··^··X/ ···`··P·
0030  f9 0c ec 6b 00 00 17 03  03 00 9a 16 c6 b5 b2 4e   ···k···· ·····N
0040  b3 68 7c 03 5e af 57 1f  88 6a 55 92 ae f5 0f 2c   ·h|·^·W· ·jU····,
0050  ab af 6a a3 6a 13 97 1f  72 94 49 37 10 f5 e2 0f   ··j·j··· r·I7····
0060  db 3d da 88 ab 3f 98 91  1c 8c 53 eb 6d 79 40 b0   ·=···?·· ··S·my@·
0070  db 44 14 fb 9c fc 4d 34  05 7f ad ab f4 ce 36 7c   ·D····M4 ····· 6|
0080  1b d4 18 f1 f4 b3 f5 25  95 0c a2 21 15 93 21 13   ·····%· ···!··!·
0090  d6 9e ec 48 5b d1 cc 83  03 b6 c4 8b ab 0b c0 ee   ···H[··· ·····
00a0  35 f7 d5 e2 ad 6e 7d 5b  d1 a2 50 2b 44 31 ab 36   5····n}[ ··P+D1·6
00b0  cf f0 93 2d 95 ca a2 a0  70 d8 69 f0 1e f0 3a 64   ···-···· p·i···:d
00c0  be 2b 4e 5a 49 9c 42 f3  4d 51 f9 71 f6 10 a4 f8   ·+NZI·B· MQ·q····
00d0  d6 04 d0 14 7b                                     ····{
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Transport Layer Security (tls), 159 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 b
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1
▸ Transport Layer Security
▾ HyperText Transfer Protocol 2
  ▸ Stream: DATA, Stream ID: 149, Length 128
  ▾ Domain Name System (query)
      Transaction ID: 0x0000
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▾ www.cs.virginia.edu: type A, class IN
          Name: www.cs.virginia.edu
          [Name Length: 19]
          [Label Count: 4]
```

```
0000  00 00 80 00 01 00 00 00  95 00 00 01 00 00 01 00   ........ ........
0010  00 00 00 00 01 03 77 77  77 02 63 73 08 76 69 72   ......ww w.cs.vi
0020  67 69 6e 69 61 03 65 64  75 00 00 01 00 01 00 00   ginia.ed u.......
0030  29 10 00 00 00 00 00 00  50 00 08 00 04 00 01 00   )....... P.......
0040  00 00 0c 00 44 00 00 00  00 00 00 00 00 00 00 00   ....D... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00                        ........ .
```

setup step: got Firefox to output cryptographic keys (using SSLKEYLOGFILE)

Frame (213 bytes) | Decrypted TLS (137 bytes)

HyperText Transfer Protocol 2 (http2), 137 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 b
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1
▸ Transport Layer Security
▾ HyperText Transfer Protocol 2
  ▸ Stream: DATA, Stream ID: 149, Length 128
  ▾ Domain Name System (query)
      Transaction ID: 0x0000
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▾ www.cs.virginia.edu: type A, class IN
          Name: www.cs.virginia.edu
          [Name Length: 19]
          [Label Count: 4]
```

```
0000  00 00 80 00 01 00 00 00  95 00 00 01 00 00 01 00   ........ ........
0010  00 00 00 00 01 03 77 77  77 02 63 73 08 76 69 72   ......ww w.cs.vi
0020  67 69 6e 69 61 03 65 64  75 00 00 01 00 01 00 00   ginia.ed u.......
0030  29 10 00 00 00 00 00 00  50 00 08 00 04 00 01 00   )....... P.......
0040  00 00 0c 00 44 00 00 00  00 00 00 00 00 00 00 00   ....D... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00                        ......... .
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

HyperText Transfer Protocol 2 (http2), 137 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 b
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1
▸ Transport Layer Security
▾ HyperText Transfer Protocol 2
  ▸ Stream: DATA, Stream ID: 149, Length 128
  ▾ Domain Name System (query)
      Transaction ID: 0x0000
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▾ www.cs.virginia.edu: type A, class IN
          Name: www.cs.virginia.edu
          [Name Length: 19]
          [Label Count: 4]
```

```
0000  00 00 80 00 01 00 00 00  95 00 00 01 00 00 01 00   ····· ·····
0010  00 00 00 00 01 03 77 77  77 02 63 73 08 76 69 72   ····ww w·cs·vi
0020  67 69 6e 69 61 03 65 64  75 00 00 01 00 01 00 00   ginia·ed u·····
0030  29 10 00 00 00 00 00 00  50 00 08 00 04 00 01 00   )····· P·····
0040  00 00 0c 00 44 00 00 00  00 00 00 00 00 00 00 00   ····D··· ·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0080  00 00 00 00 00 00 00 00  00                        ····· ·
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

HyperText Transfer Protocol 2 (http2), 137 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 b
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1
▸ Transport Layer Security
▾ HyperText Transfer Protocol 2
  ▸ Stream: DATA, Stream ID: 149, Length 128
  ▾ Domain Name System (query)
      Transaction ID: 0x0000
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▾ www.cs.virginia.edu: type A, class IN
          Name: www.cs.virginia.edu
          [Name Length: 19]
          [Label Count: 4]
```

```
0000  00 00 80 00 01 00 00 00  95 00 00 01 00 00 01 00   ........ ........
0010  00 00 00 00 01 03 77 77  77 02 63 73 08 76 69 72   ......ww w.cs.vi
0020  67 69 6e 69 61 03 65 64  75 00 00 01 00 01 00 00   ginia.ed u.......
0030  29 10 00 00 00 00 00 00  50 00 08 00 04 00 01 00   )....... P.......
0040  00 00 0c 00 44 00 00 00  00 00 00 00 00 00 00 00   ....D... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00                        ......... .
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Domain Name System (dns), 128 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1620	18.594474318	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16799 Win=65535 Len=0
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA c
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17388 Win=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15	HTTP2	109	HEADERS[147]: 200 OK

```
▸ Frame 1629: 213 bytes on wire (1704 bits), 213 bytes captured (1704 b
▸ Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:cc:86:dc), Dst: 52:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 162.159.61.4
▸ Transmission Control Protocol, Src Port: 60510, Dst Port: 443, Seq: 1
▸ Transport Layer Security
▾ HyperText Transfer Protocol 2
  ▸ Stream: DATA, Stream ID: 149, Length 128
  ▾ Domain Name System (query)
      Transaction ID: 0x0000
    ▸ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▾ www.cs.virginia.edu: type A, class IN
          Name: www.cs.virginia.edu
          [Name Length: 19]
          [Label Count: 4]
```

```
0000  00 00 80 00 01 00 00 00  95 00 00 01 00 00 01 00   ........ ........
0010  00 00 00 00 01 03 77 77  77 02 63 73 08 76 69 72   ......ww w.cs.vi
0020  67 69 6e 69 61 03 65 64  75 00 00 01 00 01 00 00   ginia.ed u.......
0030  29 10 00 00 00 00 00 00  50 00 08 00 04 00 01 00   )....... P.......
0040  00 00 0c 00 44 00 00 00  00 00 00 00 00 00 00 00   ....D... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00                        ......... .
```

Frame (213 bytes) | Decrypted TLS (137 bytes)

Domain Name System (dns), 128 bytes | Packets: 1765 · Displayed: 1765 (100.0%) | Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1621	18.594474390	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40361 Ack=16958 Win=65535 Len=0
1622	18.605415235	162.159.61.4	10.0.2.15	DoH	631	Standard query response 0x0000 HTTPS www.cs.virginia.edu SOA co
1623	18.606050489	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[147]: POST /dns-query
1624	18.606080777	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 AAAA www.cs.virginia.edu OPT
1625	18.606168058	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17014 Win=65535 Len=0
1626	18.606168109	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=40938 Ack=17173 Win=65535 Len=0
1627	18.606221426	10.0.2.15	162.159.61.4	HTTP2	110	HEADERS[149]: POST /dns-query
1628	18.606287808	162.159.61.4	10.0.2.15			K] Seq=40938 Ack=17229 Win=65535 Len=0
1629	18.606305512	10.0.2.15	162.159.6			0x0000 A www.cs.virginia.edu OPT
1630	18.606380752	162.159.61.4	10.0.2.15			in=65535 Len=0
1631	18.616270366	162.159.61.4	10.0.2.15			
1632	18.616270417	162.159.61.4	10.0.2.15			.cs.virginia.edu SOA co

- Frame 1627: 110 bytes on wire (880 bits), 110 byte
- Ethernet II, Src: PCSSystemtec_cc:86:dc (08:00:27:
- Internet Protocol Version 4, Src: 10.0.2.15, Dst:
- Transmission Control Protocol, Src Port: 60510, Ds
- Transport Layer Security
- HyperText Transfer Protocol 2

```
08 00 45 00   RT··5··· ·····E
02 0f a2 9f   ··z@·@·· ~k·····
df eb 50 18   =··^··X/ ···`··P
ab 13 1e e4   ····· ··3····
08 1e 8e 52   ··g·{·^· ·····
2b 50 4c 32   w··v···· 4···+PL
a0 3b         :·\i·E·L ·sF2·;
```

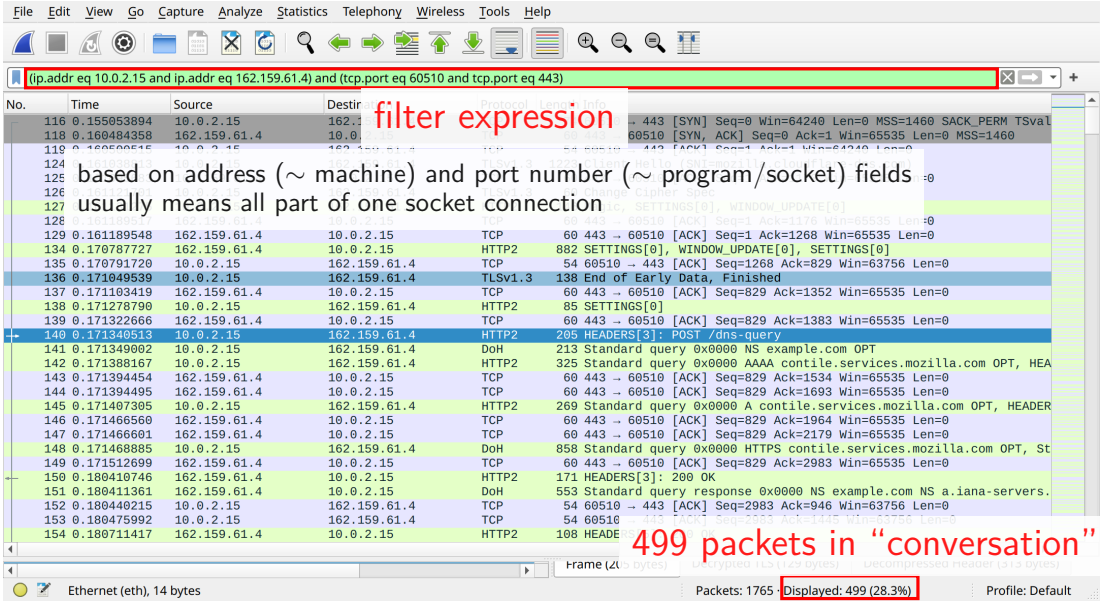
Ethernet (eth), 14 bytes

ompressed Header (313 bytes)

(100.0%) Profile: Default

- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comments
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

- BPv7
- DCCP
- CIP Connection
- Ethernet
- F5 TCP
- F5 UDP
- F5 IP
- IEEE 802.15.4
- IPv4
- IPv6
- LTP
- TCP
- UDP
- ZigBee Network Layer
- PN-IO AR



No.	Time	Source	Destination	Protocol	Length	Info
116	0.155053894	10.0.2.15	162.159.61.4	TCP	74	60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
118	0.160484358	162.159.61.4	10.0.2.15	TCP	74	443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
129	0.161189548	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
134	0.170787727	162.159.61.4	10.0.2.15	HTTP2	882	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
135	0.170791720	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
136	0.171049539	10.0.2.15	162.159.61.4	TLSv1.3	138	End of Early Data, Finished
137	0.171103419	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1352 Win=65535 Len=0
138	0.171278790	10.0.2.15	162.159.61.4	HTTP2	85	SETTINGS[0]
139	0.171322666	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0
140	0.171340513	10.0.2.15	162.159.61.4	HTTP2	205	HEADERS[3]: POST /dns-query
141	0.171349002	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 NS example.com OPT
142	0.171388167	10.0.2.15	162.159.61.4	HTTP2	325	Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
143	0.171394454	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0
144	0.171394495	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
145	0.171407305	10.0.2.15	162.159.61.4	HTTP2	269	Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
146	0.171466560	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
147	0.171466601	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
148	0.171468885	10.0.2.15	162.159.61.4	DoH	858	Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
149	0.171512699	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
150	0.180410746	162.159.61.4	10.0.2.15	HTTP2	171	HEADERS[3]: 200 OK
151	0.180411361	162.159.61.4	10.0.2.15	DoH	553	Standard query response 0x0000 NS example.com NS a.iana-servers.
152	0.180440215	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
153	0.180475992	10.0.2.15	162.159.61.4	TCP	54	60510
154	0.180711417	162.159.61.4	10.0.2.15	HTTP2	108	HEADE

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)

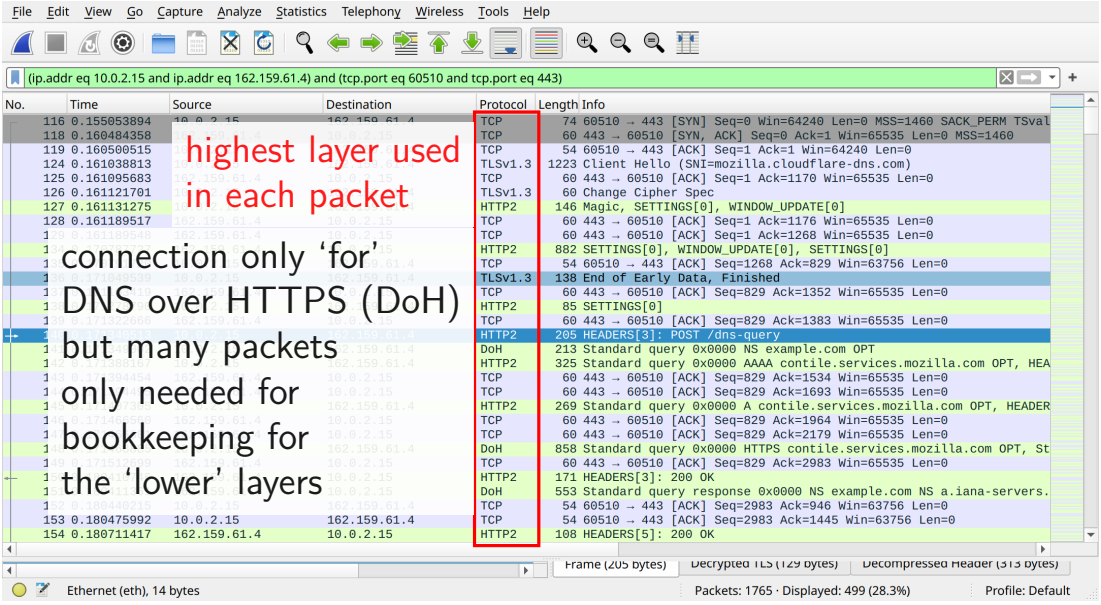
No.	Time	Source	Destination	Protocol	Length	Info
116	0.155053894	10.0.2.15	162.159.61.4	TCP	74	60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
118	0.160484358	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
119	0.160500515	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
124	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	ello (SNI=mozilla.cloudflare-dns.com)
125	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	510 [ACK] Seq=1 Ack=1170 Win=65535 Len=0
126	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	ipher Spec
127	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	ETTINGS[0], WINDOW_UPDATE[0]
128	0.161189517	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1176 Win=65535 Len=0
129	0.161189548	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
134	0.170787727	162.159.61.4	10.0.2.15	HTTP2	882	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
135	0.170791720	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
136	0.171049539	10.0.2.15	162.159.61.4	TLSv1.3	138	End of Early Data, Finished
137	0.171103419	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1352 Win=65535 Len=0
138	0.171278790	10.0.2.15	162.159.61.4	HTTP2	85	SETTINGS[0]
139	0.171322666	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0
140	0.171340513	10.0.2.15	162.159.61.4	HTTP2	205	HEADERS[3]: POST /dns-query
141	0.171349002	10.0.2.15	162.159.61.4	DoH	213	Standard query 0x0000 NS example.com OPT
142	0.171388167	10.0.2.15	162.159.61.4	HTTP2	325	Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
143	0.171394454	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0
144	0.171394495	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
145	0.171407305	10.0.2.15	162.159.61.4	HTTP2	269	Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
146	0.171466560	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
147	0.171466601	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
148	0.171468885	10.0.2.15	162.159.61.4	DoH	858	Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
149	0.171512699	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
150	0.180410746	162.159.61.4	10.0.2.15	HTTP2	171	HEADERS[3]: 200 OK
151	0.180411361	162.159.61.4	10.0.2.15	DoH	553	Standard query response 0x0000 NS example.com NS a.iana-servers.
152	0.180440215	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
153	0.180475992	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0
154	0.180711417	162.159.61.4	10.0.2.15	HTTP2	108	HEADERS[5]: 200 OK

some packets not shown from filter

Frame (205 bytes) Decrypted TLS (129 bytes) Decompressed Header (313 bytes)

Ethernet (eth), 14 bytes

Packets: 1765 · Displayed: 499 (28.3%) Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)
No. Time Source Destination Protocol Length Info
116 0.155053894 10.0.2.15 162.159.61.4 TCP 74 60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
118 0.160484358 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
119 0.160500515 10.0.2.15 162.159.61.4 TCP 54 60510 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
124 0.161038813 10.0.2.15 162.159.61.4 TLSv1.3 1223 Client Hello (SNI=mozilla.cloudflare-dns.com)
125 0.161095683 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=1 Ack=1170 Win=65535 Len=0
126 0.161121701 162.159.61.4 10.0.2.15 TLSv1.3 60 Change Cipher Spec
127 0.161131275 10.0.2.15 162.159.61.4 HTTP2 146 Magic, SETTINGS[0], WINDOW_UPDATE[0]
128 0.161189517 162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=1 Ack=1176 Win=65535 Len=0
162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
10.0.2.15 162.159.61.4 HTTP2 882 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
162.159.61.4 10.0.2.15 TCP 54 60510 → 443 [ACK] Seq=1268 Ack=829 Win=63756 Len=0
10.0.2.15 162.159.61.4 TLSv1.3 138 End of Early Data, Finished
162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=829 Ack=1352 Win=65535 Len=0
10.0.2.15 162.159.61.4 HTTP2 85 SETTINGS[0]
162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=829 Ack=1383 Win=65535 Len=0
162.159.61.4 10.0.2.15 HTTP2 205 HEADERS[3]: POST /dns-query
10.0.2.15 162.159.61.4 DoH 213 Standard query 0x0000 NS example.com OPT
162.159.61.4 10.0.2.15 HTTP2 325 Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
10.0.2.15 162.159.61.4 TCP 60 443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0
10.0.2.15 162.159.61.4 TCP 60 443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
162.159.61.4 10.0.2.15 HTTP2 269 Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
162.159.61.4 10.0.2.15 TCP 60 443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
10.0.2.15 162.159.61.4 TCP 60 443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
162.159.61.4 10.0.2.15 DoH 858 Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
10.0.2.15 162.159.61.4 TCP 60 443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
162.159.61.4 10.0.2.15 HTTP2 171 HEADERS[3]: 200 OK
10.0.2.15 162.159.61.4 DoH 553 Standard query response 0x0000 NS example.com NS a.iana-servers.
162.159.61.4 10.0.2.15 TCP 54 60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
153 0.180475992 10.0.2.15 162.159.61.4 TCP 54 60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0
154 0.180711417 162.159.61.4 10.0.2.15 HTTP2 108 HEADERS[5]: 200 OK
Frame (205 bytes) Decrypted TLS (129 bytes) Decompressed Header (313 bytes)
Ethernet (eth), 14 bytes
Packets: 1765 · Displayed: 499 (28.3%)
Profile: Default
highest layer used
in each packet
connection only 'for'
DNS over HTTPS (DoH)
but many packets
only needed for
bookkeeping for
the 'lower' layers

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 10.0.2.15 and ip.addr eq 162.159.61.4) and (tcp.port eq 60510 and tcp.port eq 443)

No.	Time	Source	Destination	Protocol	Length	Info
116	0.155053894	10.0.2.15	162.159.61.4	TCP	74	60510 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
118	0.160484358	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
119	0.160500515	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
124	0.161038813	10.0.2.15	162.159.61.4	TLSv1.3	1223	Client Hello (SNI=mozilla.cloudflare-dns.com)
125	0.161095683	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1170 Win=65535 Len=0
126	0.161121701	10.0.2.15	162.159.61.4	TLSv1.3	60	Change Cipher Spec
127	0.161131275	10.0.2.15	162.159.61.4	HTTP2	146	Magic, SETTINGS[0], WINDOW_UPDATE[0]
128	0.161189517	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1176 Win=65535 Len=0
129	0.161189548	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=1 Ack=1268 Win=65535 Len=0
134	0.170787727	162.159.61.4	10.0.2.15	HTTP2	882	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
135	0.170791720	10.0.2.15	162.159.61.4	[illegible]	[illegible]	[illegible] Len=0
136	0.171049539	10.0.2.15	162.159.61.4	[illegible]	[illegible]	[illegible]
137	0.171103419	162.159.61.4	10.0.2.15	[illegible]	[illegible]	[illegible] Len=0
138	0.171278790	10.0.2.15	162.159.61.4	[illegible]	[illegible]	[illegible]
139	0.171322666	162.159.61.4	10.0.2.15	[illegible]	[illegible]	[illegible] Len=0
140	0.171340513	10.0.2.15	162.159.61.4	[illegible]	[illegible]	[illegible]
141	0.171349002	10.0.2.15	162.159.61.4	[illegible]	[illegible]	[illegible]
142	0.171388167	10.0.2.15	162.159.61.4	HTTP2	325	Standard query 0x0000 AAAA contile.services.mozilla.com OPT, HEA
143	0.171394454	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1534 Win=65535 Len=0
144	0.171394495	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1693 Win=65535 Len=0
145	0.171407305	10.0.2.15	162.159.61.4	HTTP2	269	Standard query 0x0000 A contile.services.mozilla.com OPT, HEADER
146	0.171466560	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=1964 Win=65535 Len=0
147	0.171466601	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2179 Win=65535 Len=0
148	0.171468885	10.0.2.15	162.159.61.4	DoH	858	Standard query 0x0000 HTTPS contile.services.mozilla.com OPT, St
149	0.171512699	162.159.61.4	10.0.2.15	TCP	60	443 → 60510 [ACK] Seq=829 Ack=2983 Win=65535 Len=0
150	0.180410746	162.159.61.4	10.0.2.15	HTTP2	171	HEADERS[3]: 200 OK
151	0.180411361	162.159.61.4	10.0.2.15	DoH	553	Standard query response 0x0000 NS example.com NS a.iana-servers.
152	0.180440215	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=2983 Ack=946 Win=63756 Len=0
153	0.180475992	10.0.2.15	162.159.61.4	TCP	54	60510 → 443 [ACK] Seq=2983 Ack=1445 Win=63756 Len=0
154	0.180711417	162.159.61.4	10.0.2.15	HTTP2	108	HEADERS[5]: 200 OK

bookkeeping packets sent in both directions

Frame (205 bytes) Decrypted TLS (129 bytes) Decompressed Header (313 bytes)

Ethernet (eth), 14 bytes

Packets: 1765 · Displayed: 499 (28.3%) Profile: Default

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

- error in hardware/software on sending machine reading file
- bits being flipped in memory on forwarding machine
- communication system flipping bits in data
- hosts crashing during communication

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

- error in hardware/software on sending machine reading file
- bits being flipped in memory on forwarding machine
- communication system flipping bits in data
- hosts crashing during communication

communication system can't help a lot of these things

example: reliable file transfer

want to make sure correct data transferred

want to protect against:

- error in hardware/software on sending machine reading file
- bits being flipped in memory on forwarding machine
- communication system flipping bits in data
- hosts crashing during communication

communication system can't help a lot of these things

authors experienced router with bad memory/processor

solution: end-to-end checks

want reliable transfer: compare final files (with hash or similar)

"end-to-end" — doesn't care what middle systems do

end-to-end argument

Saltzer, Reed, Clark, "End-to-End Arguments in System Design"

"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)"

end-to-end in practice

"narrow waist" of IP doesn't provide many gaurnetees

- no gaurentees about reliable transmission, duplicate suppression, message order, ...

but try to provide good service ("best effort")

in design: typically middle systems won't know/care about what's forwarded

- but many exceptions

backup slides