

Q2

HTTP request packet:

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows a GET request to /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwclxKjU5RSOU... from 10.4.8.18 to 172.21.10.4.8.18. The packet details pane shows the request structure: GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwclxKjU5RSOU... [Expert Info (Chat/Sequence): GET /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwclxKjU5RSOU... [Severity level: Chat] [Group: Sequence] Request Method: GET Request URI: /edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwclxKjU5RSOU... Request Version: HTTP/1.1 Connection: Keep-Alive\r\n Accept: */*\r\n Accept-Encoding: identity\r\n If-Unmodified-Since: Fri, 22 Jan 2021 00:49:50 GMT\r\n Range: bytes=0-1119\r\n User-Agent: Microsoft BITS/7.8\r\n Host: redirector.gvt1.com\r\n

HTTP response packet

The image shows a Wireshark packet capture of an HTTP 302 Found response. The packet list pane shows a 302 Found response from 172.21.10.4.8.18 to 10.4.8.18. The packet details pane shows the response structure: HTTP/1.1 302 Found (text/html) [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n [Severity level: Chat] [Group: Sequence] Response Version: HTTP/1.1 Status Code: 302 [Status Code Description: Found] Response Phrase: Found Date: Thu, 04 Feb 2021 13:28:12 GMT\r\n Pragma: no-cache\r\n Expires: Fri, 01 Jan 1990 00:00:00 GMT\r\n Cache-Control: no-cache, must-revalidate\r\n [truncated]Location: http://r4--sn-gwpa-ccpe.gvt1.com/edgedl/release2/chrome_component/A036NrjicXasB105ddVmdvk_88.253.200/dCwclxKjU5RSOU52LSQXQ?cms_redirect=yes&mh=-W&mi Content-Type: text/html; charset=UTF-8\r\n Server: ClientMapServer\r\n X-XSS-Protection: 0\r\n X-Frame-Options: SAMEORIGIN\r\n Accept-Ranges: none\r\n Content-Length: 480\r\n Via: HTTP/1.1 forward.http.proxy:3128\r\n Connection: keep-alive\r\n [HTTP response 1/12] [Time since request: 0.142761000 seconds] [Request in frame: 14697] [Next request in frame: 14629]

TCP and UDP Statistics

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
User Datagram Protocol	2.7	536	0.0	4288	119	0	0	0
Transmission Control Protocol	89.3	17571	93.5	11691801	325 k	9521	4097282	114 k

=====
=====

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst
rate	Burst start						

IPv6 Statistics/IP Protocol Types:

IP Protocol Types		83	0.0003	100%	0.0600	
10.162						
UDP	80	0.0003	96.39%	0.0600	10.162	
NONE	3	0.0000	3.61%	0.0100	17.228	

Info			* Source Port	Source IP	Destination IP	Destination Port	HTTP host	HTTPS Server Time
22 → 50717 [SYN, ACK]	Seq=0 Ack=1 Win=2920...	22	10.1...	10.4.8.18	50717			2021-02-04 13:29:16.126435
443 → 50610 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	137...	10.4.8.18	50610			2021-02-04 13:27:32.194119
443 → 50611 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50611			2021-02-04 13:27:34.170969
443 → 50612 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	216...	10.4.8.18	50612			2021-02-04 13:27:34.486420
443 → 50613 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50613			2021-02-04 13:27:34.805466
443 → 50614 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50614			2021-02-04 13:27:35.361519
443 → 50615 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50615			2021-02-04 13:27:35.449303
443 → 50616 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	103...	10.4.8.18	50616			2021-02-04 13:27:35.538416
443 → 50617 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	82.1...	10.4.8.18	50617			2021-02-04 13:27:35.544556
443 → 50618 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	172...	10.4.8.18	50618			2021-02-04 13:27:36.115514
443 → 50619 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	103...	10.4.8.18	50619			2021-02-04 13:27:36.127417
443 → 50620 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50620			2021-02-04 13:27:36.128164
443 → 50621 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	37.1...	10.4.8.18	50621			2021-02-04 13:27:36.182050
443 → 50622 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	172...	10.4.8.18	50622			2021-02-04 13:27:37.673781
443 → 50624 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	142...	10.4.8.18	50624			2021-02-04 13:27:38.874292
443 → 50625 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	172...	10.4.8.18	50625			2021-02-04 13:27:40.850617
443 → 50626 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	172...	10.4.8.18	50626			2021-02-04 13:27:41.010562
443 → 50627 [SYN, ACK]	Seq=0 Ack=1 Win=292...	443	216...	10.4.8.18	50627			2021-02-04 13:27:41.010754
» Frame 14605: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{B807628E-622D-4299-8AD8-5D9F}								
» Ethernet II, Src: Cisco_5a:ab:40 (28:f6:7f:5a:ab:40), Dst: LCFChEFe_41:a3:c8 (28:d2:44:41:a3:c8)								
» Internet Protocol Version 4, Src: 172.217.166.46, Dst: 10.4.8.18								
» Transmission Control Protocol, Src Port: 80, Dst Port: 50698, Seq: 0, Ack: 1, Len: 0								

TCP and UDP packets whose dstport==80

(tcp.dstport==80 or udp.dstport==80)									
Protocol	Destination Port	Info				Source Port	Source IP	Destination IP	
TCP	80	50698 → 80	[FIN, ACK]	Seq=3529	Ack=10448	Win=...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=893	Ack=2842	Win=1049856...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=589	Ack=1728	Win=1051136...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=3529	Ack=10448	Win=10511...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=3529	Ack=10447	Win=10511...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=305	Ack=1115	Win=1049856...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=2941	Ack=8720	Win=105113...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=2657	Ack=8107	Win=104985...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=2353	Ack=6965	Win=105113...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=2069	Ack=6352	Win=104985...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=1765	Ack=5210	Win=105113...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=1177	Ack=3455	Win=105113...	50698	10.4...	172.217...
TCP	80	50698 → 80	[ACK]	Seq=1	Ack=1	Win=1051136	Len=0	50698	10.4...
TCP	80	50609 → 80	[FIN, ACK]	Seq=1	Ack=1	Win=513	Len=...	50609	10.4...
TCP	80	50609 → 80	[ACK]	Seq=2	Ack=2	Win=513	Len=0	50609	10.4...
TCP	80	50608 → 80	[FIN, ACK]	Seq=1	Ack=1	Win=4106	Le...	50608	10.4...
TCP	80	50608 → 80	[ACK]	Seq=2	Ack=2	Win=4106	Len=0	50608	10.4...

ARP Packets

arp									
Protocol	Destination Port	Info				Source Port	Source IP	Destination IP	HTTP host
ARP		Who has 10.4.8.52?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:28:37.217966
ARP		Who has 10.4.8.52?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:28:37.207843
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.769702
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.759486
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.749274
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:15.056455
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:15.036210
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:15.015962
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:28:37.192694
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:28:37.182534
ARP		Who has 10.4.8.51?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:28:37.172431
ARP		Who has 10.4.8.50?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.734072
ARP		Who has 10.4.8.50?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.723856
ARP		Who has 10.4.8.50?	Tell 10.4.8.18	LCFC...	Broadcast				2021-02-04 13:30:22.713637