System Administration

Week 06, Segment 1

Networking II: A Simple Request

Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

Photo by Markus Spiske on Unsplash
$ telnet www.yahoo.com 80
Trying 2001:4998:124:1507::e000...
Escape character is ']'.
HEAD / HTTP/1.0

HTTP/1.0 200 OK
Date: Wed, 10 Mar 2021 15:36:06 GMT
Via: http/1.1 media-router-fp7004.canary.media.bf1.yahoo.com (ApacheTrafficServer [c s f ])
Server: ATS
Cache-Control: no-store, no-cache, max-age=0, private
Content-Type: text/html
Content-Language: en
Expires: -1
X-Frame-Options: SAMEORIGIN
Content-Length: 12

Connection closed by foreign host.
$
A simple request

What exactly happens?

• Local host connects to remote host.
• Local host sends data.
• Remote host replies with data.
• The End.
Flags [.] , ack 20, win 224, options [nop,nop,TS val 3439151957 ecr 8], length 0
IP6 2001:4998:44:3507::8000.80 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.65422:
Flags [P.], seq 1:234, ack 20, win 224, options [nop,nop,TS val 3439151958 ecr 8], length 233: HTTP: HTTP/1.0 200 OK
IP6 2001:4998:44:3507::8000.80 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.65422:
Flags [F.], seq 234, ack 20, win 224, options [nop,nop,TS val 3439151958 ecr 8], length 0
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.65422 > 2001:4998:44:3507::8000.80:
Flags [.] , ack 235, win 4110, options [nop,nop,TS val 9 ecr 3439151958], length 0
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.65422 > 2001:4998:44:3507::8000.80:
Flags [F.], seq 20, ack 235, win 4140, options [nop,nop,TS val 9 ecr 3439151958], length 0
IP6 2001:4998:44:3507::8000.80 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96.65422:
Flags [.] , ack 21, win 224, options [nop,nop,TS val 3439151992 ecr 9], length 0
IP6 fe80::7e12:b688:167c:785f.546 > ff02::1:2.547: dhcp6 renew
IP6 fe80::caa:49ff:feaf:1815.547 > fe80::7e12:b688:167c:785f.546: dhcp6 reply
IP6 fe80::7e12:b688:167c:785f > ff02::1: ICMP6, neighbor advertisement, tgt is 2
600:1f18:400c:b800:bc3c:63cc:7e5d:1f96, length 32
IP6 fe80::7e12:b688:167c:785f > fe80::caa:49ff:feaf:1815: ICMP6, neighbor solicitation, who has fe80::caa:49ff:feaf:1815, length 32
IP6 fe80::7e12:b688:167c:785f > ff02::1: ICMP6, neighbor advertisement, tgt is 2
600:1f18:400c:b800:bc3c:63cc:7e5d:1f96, length 32
#
23263 23263 telnet RET poll 1
23263 23263 telnet CALL sendto(5,0x1a7225980,2,0,0,0)
23263 23263 telnet MISC msghdr: [name=0x0, namelen=0, iov=0xffffffffbe804279bf50, iovlen=1, control=0x0, controllen=2440071040, flags=0]
23263 23263 telnet GIO fd 5 wrote 2 bytes
"\r\n"
23263 23263 telnet RET sendto 2
23263 23263 telnet CALL poll(0x7f7fffac9250,3,0)
23263 23263 telnet RET poll 0
23263 23263 telnet CALL poll(0x7f7fffac9250,3,0xffffffff)
23263 23263 telnet RET poll 1
23263 23263 telnet CALL recvfrom(5,0x1a7225580,0x400,0,0,0)
23263 23263 telnet MISC msghdr: [name=0x0, namelen=1115275264, iov=0xffffffffbe804279bf40, iovlen=1, control=0x0, controllen=1115275264, flags=0]
23263 23263 telnet GIO fd 5 read 233 bytes
"HTTP/1.0 200 OK\r\nDate: Wed, 10 Mar 2021 23:17:18 GMT\r\nServer: ATS\r\nCache-Control: no-store, no-cache, max-age=0, private\r\nContent-Type: text/html\r\nContent-Language: en\r\nExpires: -1\r\nX-Frame-Options: SAMEORIGIN\r\nContent-Length: 12\r\n"
23263 23263 telnet RET recvfrom 233/0xe9
23263 23263 telnet CALL poll(0x7f7fffac9250,3,0)
23263 23263 telnet RET poll 2
23263 23263 telnet CALL recvfrom(5,0x1a7225580,0x400,0,0,0)
A simple request

What exactly happens?

• Local host connects to remote host.
• Local host sends data.
• Remote host replies with data.
• The End.
A simple request

What exactly happens?
• Local host connects to remote host.
  • turn remote hostname into IP address
  • open socket to requested port on remote IP
• Local host sends data.
• Remote host replies with data.
• The End.
A simple request

What exactly happens?

• Local host connects to remote host.
  • turn remote hostname into IP address
    • determine how to resolve hostnames by via /etc/nsswitch.conf
    • look in /etc/hosts, then fail over to DNS
    • determine DNS server to use via /etc/resolv.conf
    • open socket to well-defined port on DNS server, send query, receive response
  • open socket to requested port on remote IP
• Local host sends data.
• Remote host replies with data.
• The End.
A simple request

What exactly happens?

• Local host connects to remote host.
  • turn remote hostname into IP address
    • determine how to resolve hostnames by via /etc/nsswitch.conf
    • look in /etc/hosts, then fail over to DNS
    • determine DNS server to use via /etc/resolv.conf
    • open socket to well-defined port on DNS server, send query, receive response
  • open socket to requested port on remote IP
• Local host sends data.
• Remote host replies with data.
• The End?
Exercises

• Repeat this exercise on an Ubuntu Linux, a RedHat Linux, and an OmniOS instance using `strace(1)/dtrace(1)` — what’s different?

• Our example mixed IPv4 and IPv6. Configure a system to be IPv6 only and repeat the exercise — has anything changed?

• What changes if you add an entry for the destination address to `/etc/hosts`?

• We saw in our trace that the application made two separate requests to the DNS server — why is that?

Coming up: back to `tcpdump(8)`