

Verification of client-server connectivity

Dr. Daniel Guasch Murillo
Dr. Rafael Vidal Ferré

July 2024



P

Practical case...

Security and Network Administration

It's a quiet Thursday before the Security and Network Administration (SEAX) class...

Some students of the subject commented on difficulties in accessing the Athena service.

So, the teacher proposes a problem to be solved for the next session...

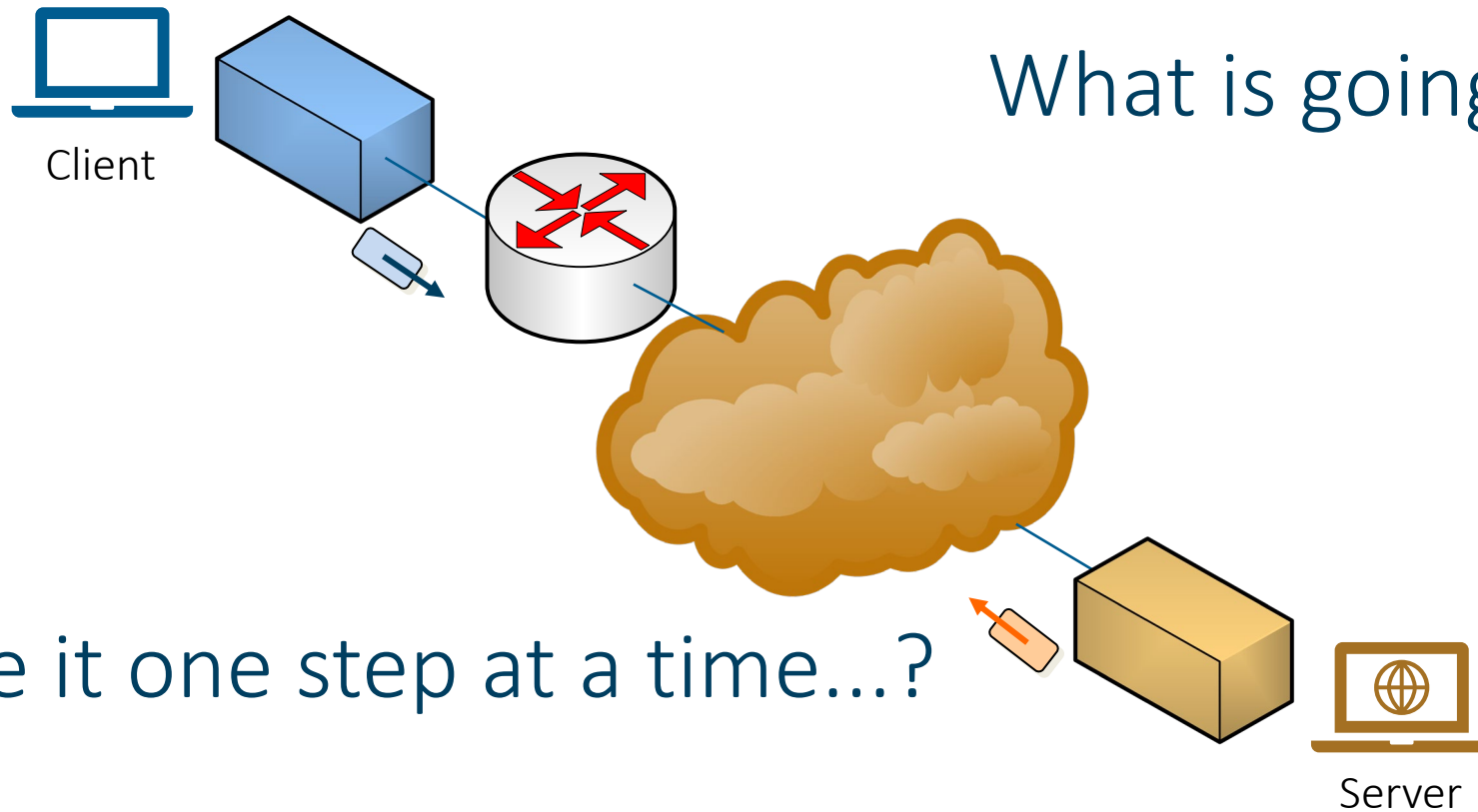
How do you verify connectivity to a server?

Links

The case of client and server

Stage

There are problems when trying to make a web query



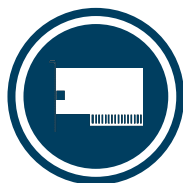
Let's take it one step at a time...?



Customer team

Physical level

Does the network device exist?



```
root@debian:~# lspci | grep -i -e "Ethernet" -e "Wireless"
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:08.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:09.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:0a.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
root@debian:~#
```



```
root@debian:~# lsusb | grep -i -e "Ethernet" -e "Wireless"
Bus 001 Device 004: ID 0b05:17d1 ASUSTek Computer, Inc. AC51 802.11a/b/g/n/ac Wireless Adapter [Mediatek MT7610U]
Bus 001 Device 003: ID 0bda:8187 Realtek Semiconductor Corp. RTL8187 Wireless Adapter
Bus 001 Device 002: ID 0b05:17d1 ASUSTek Computer, Inc. AC51 802.11a/b/g/n/ac Wireless Adapter [Mediatek MT7610U]
root@debian:~#
```

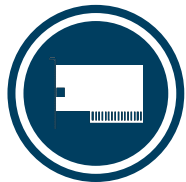


<< The driver must be installed >>
 root@debian:~# apt install driver

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Physical level

Is it the right driver?



```
root@debian:~# lsmod | grep -i ^e100
e1000                163840  0
...
root@debian:~# modinfo e1000 |grep ^desc
description:        Intel(R) PRO/1000 Network Driver
```



```
root@debian:~# lsmod | grep 802
mac80211             995328  7 mt76,mt76_usb,mt76x02_lib,mt76x02_usb,mt76x0_common,rt18187,mt76x0u
cfg80211             983040  5 mt76,mt76x02_lib,mac80211,mt76x02_usb,rt18187
...
root@debian:~# modinfo mac80211 |grep ^desc
description:        IEEE 802.11 subsystem
```

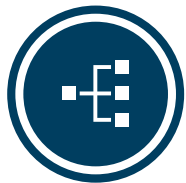


<< The driver must be installed >>
 root@debian:~# apt install driver

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Link level

Does the interface exist? Is it active?



```
root@debian:~# ip -br link
```

lo	UNKNOWN	00:00:00:00:00:00	<LOOPBACK,UP,LOWER_UP>	
enp0s3	UP	08:00:27:1d:97:61	<BROADCAST,MULTICAST,UP,LOWER_UP>	
enp0s8	UP	08:00:27:6e:ed:dd	<BROADCAST,MULTICAST,UP,LOWER_UP>	
enp0s9	DOWN	08:00:27:84:9c:c0	<NO-CARRIER,BROADCAST,MULTICAST,UP>	(1)
enp0s10	DOWN	08:00:27:cf:7f:6a	<BROADCAST,MULTICAST>	(2)
wlx04d9f511b8c3	UP	04:d9:f5:11:b8:c3	<BROADCAST,MULTICAST,UP,LOWER_UP>	
wlx001aef0caebc	DOWN	00:1a:ef:0c:ae:bc	<NO-CARRIER,BROADCAST,MULTICAST,UP>	(3)
wlxfc3497286aac	DOWN	fc:34:97:28:6a:ac	<BROADCAST,MULTICAST>	(2)



- (1) << Ethernet cable disconnected >>
- (2) << Interface not raised >>
- (3) << Interface not associated with an Access Point >>
- (4) root@debian:~# ip link set interface up

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Link level

Is the Wi-Fi interface associated with an AP?

```
root@debian:~# iw wlan0 scan
BSS b8:69:f4:3a:6e:10 (on wlan0)
    TSF: 61625851770 usec (0d, 17:07:05)
    freq: 2412
    beacon interval: 100 TUs
    capability: ESS Privacy ShortPreamble ShortSlotTime (0x0431)
    signal: -48.00 dBm
    SSID: seax
    DS Parameter set: channel 1
```

...

```
root@debian:~# wpa_cli status
Selected interface 'wlan0'
bssid=b8:69:f4:3a:6e:10
ssid=seax
mode=station
```

...



<< You need to be associated with an Access Point >>
 root@debian:~# ifup (wpa-supPLICANT)

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level**
- 1 Physical level

Link level



Is the Wi-Fi interface blocked?

```
root@debian:~# rfkill list all
0: phy0: Wireless LAN
   Soft blocked: no
   Hard blocked: no
1: phy1: Wireless LAN
   Soft blocked: no
   Hard blocked: no
2: phy2: Wireless LAN
   Soft blocked: no
   Hard blocked: no
root@debian:~#
```

```
root@debian:~# iw dev
phy#2    Interface wlxfc3497286aac...
phy#1    Interface wlx001aef0caebc...
phy#0    Interface wlx04d9f511b8c3...
root@debian:~#
```



<< Need to unlock the >>
interfaceroot@debian:~# rfkill unblock all/wlan

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level**
- 1 Physical level

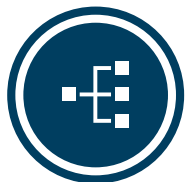
Link level

Has there been traffic through the interfaces?

```

root@debian:~# ip -s -h link
...
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
   link/ether 08:00:27:6e:ed:dd brd ff:ff:ff:ff:ff:ff
   RX: bytes  packets  errors  dropped missed  mcast
   2.52M      2.79k      0       0       0       0
   TX: bytes  packets  errors  dropped carrier collsns
   278k       3.83k      0       0       0       0 ...
6: wlx04d9f511b8c3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default qlen 1000
   link/ether 04:d9:f5:11:b8:c3 brd ff:ff:ff:ff:ff:ff
   RX: bytes  packets  errors  dropped missed  mcast
   24.0M      100.0k    0       0       0       0
   TX: bytes  packets  errors  dropped carrier collsns
   72.7k       523      0       0       0       0
8: wlxfc3497286aac: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000
   link/ether fc:34:97:28:6a:ac brd ff:ff:ff:ff:ff:ff
   RX: bytes  packets  errors  dropped missed  mcast
   0          0        0       0       0       0
   TX: bytes  packets  errors  dropped carrier collsns
   0          0        0       0       0       0
...

```



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level**
- 1 Physical level



<< Interface statuses need to be verified >>

Network level

Is the network service active?



```

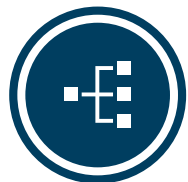
root@debian:~# service networking status
• networking.service - Raise network interfaces
  Loaded: loaded (/lib/systemd/system/networking.service; enabled; vendor preset: enabled)
  Active: active (exited) since Tue 2023-03-14 16:36:26 CET; 20min ago
  Docs: man:interfaces(5)
  Process: 345 ExecStart=/sbin/ifup -a --read-environment (code=exited, status=0/SUCCESS)
  Main PID: 345 (code=exited, status=0/SUCCESS)
  CPU: 9ms

mar 14 16:36:26 debian systemd[1]: Starting Raise network interfaces...
mar 14 16:36:26 debian systemd[1]: Finished Raise network interfaces.
root@debian:~#
    
```



<< The service must be activated >>
 (/etc/network/interfaces -> ifup, ifdown)
 root@debian:~# service networking start
 root@debian:~# update-rc.d networking enable

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Network level

Does the interface have IP addressing?

```

root@debian:~# ip -br address
lo                UNKNOWN    127.0.0.1/8     ::1/128
enp0s3            UP         10.1.1.143/24   fdbc:af07:7e18:482c:a00:27ff:fe1d:9761/64
enp0s8            UP         10.0.3.15/24
enp0s9            DOWN
enp0s10           DOWN
wlx04d9f511b8c3  UP         10.1.1.109/24   fdbc:af07:7e18:482c:6d9:f5ff:fe11:b8c3/64
wlx001aef0caebc  DOWN
wlxfc3497286aac  DOWN
root@debian:~#
    
```

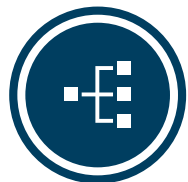


<< Need to get IP address >>

```

root@debian:~# ifup interfície
root@debian:~# ip address add 10.1.1.111/24 broadcast 10.1.1.255
                        dev interfície
root@debian:~# dhclient interfície
    
```

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level**
- 2 Link level
- 1 Physical level



Network level

Are the computer interfaces responsive?

```
root@debian:~# ping -c 1 localhost
PING localhost(localhost (:::1)) 56 data bytes
64 bytes from localhost (:::1): icmp_seq=1 ttl=64 time=0.019 ms
--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.019/0.019/0.019/0.000 ms
```

```
root@debian:~# ping -c 1 10.0.3.15
PING 10.0.3.15 (10.0.3.15) 56(84) bytes of data.
64 bytes from 10.0.3.15: icmp_seq=1 ttl=64 time=0.013 ms
--- 10.0.3.15 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.013/0.013/0.013/0.000 ms
```

```
root@debian:~# ping -c 1 10.1.1.109
PING 10.1.1.109 (10.1.1.109) 56(84) bytes of data.
64 bytes from 10.1.1.109: icmp_seq=1 ttl=64 time=0.014 ms
--- 10.1.1.109 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.014/0.014/0.014/0.000 ms
```



<< You need to verify the address >>

Network level

Does the computer have a default router?



```
root@debian:~# ip route
default via 10.0.3.2 dev enp0s8
10.0.3.0/24 dev enp0s8 proto kernel scope link src 10.0.3.15
10.1.1.0/24 dev enp0s3 proto kernel scope link src 10.1.1.143
10.1.1.0/24 dev wlx04d9f511b8c3 proto kernel scope link src 10.1.1.109
root@debian:~#
```



<< A default router must be configured >>
 root@debian:~# ip route add default 10.1.1.1 dev interface

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level**
- 2 Link level
- 1 Physical level

Network level

Can the computer communicate with the default router?



```

root@debian:~# ping -c 1 10.0.3.2
PING 10.0.3.2 (10.0.3.2) 56(84) bytes of data.
64 bytes from 10.0.3.2: icmp_seq=1 ttl=64 time=0.457 ms

--- 10.0.3.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.457/0.457/0.457/0.000 ms
root@debian:~#
    
```



<< You need to verify the correctness of the address >>
 root@debian:~# ip route add default 10.1.1.1 dev interface

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level**
- 2 Link level
- 1 Physical level

Network level

Does the computer establish a route to the destination server?



```
root@debian:~# ip route get 147.83.2.135
147.83.2.135 via 10.0.3.2 dev enp0s8 src 10.0.3.15 uid 0
  cache
root@debian:~#
```



<< It is necessary to verify the correctness of the routes >>
 root@debian:~# ip route show

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level**
- 2 Link level
- 1 Physical level

Network level

Is the team able to reach the destination server?



```
root@debian:~# ping -c 1 147.83.2.135
PING 147.83.2.135 (147.83.2.135) 56(84) bytes of data.
64 bytes from 147.83.2.135: icmp_seq=1 ttl=241 time=10.8 ms

--- 147.83.2.135 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.846/10.846/10.846/0.000 ms
```



<< Connectivity needs to be verified >>
 Possible cut to the Internet...
 Possible firewalls on the server...

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Network level

Is the computer able to resolve the DNS name of the server?



```

root@debian:~# dig www.upc.edu

; <<>> DiG 9.16.37-Debian <<>> www.upc.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18616
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.upc.edu.                IN      A

;; ANSWER SECTION:
www.upc.edu.                 66747  IN      CNAME   www.upc.es.
www.upc.es.                  2962   IN      A       147.83.2.135

;; Query time: 16 msec
;; SERVER: 10.1.1.1#53(10.1.1.1)
;; WHEN: Wed Mar 15 12:49:41 CET 2023
;; MSG SIZE rcvd: 69
    
```

root@debian:~#



<< Configure DNS servers need to be verified >>
 root@debian:~# nano /etc/resolv.conf

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



Network level

Can datagram fragmentation be occurring?

```
root@debian:~# ip address show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6e:ed:dd brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic enp0s8
        valid_lft 74064sec preferred_lft 74064sec
    inet6 fe80::a00:27ff:fe6e:eddd/64 scope link
        valid_lft forever preferred_lft forever
```

```
root@debian:~# ping -c 1 -s $((10000-28)) -M do 147.83.2.135
PING 147.83.2.135 (147.83.2.135) 9972(10000) bytes of data.
ping: local error: message too long, mtu=1500
```

```
--- 147.83.2.135 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

```
root@debian:~#
```



<< Reduce MTU >>

```
root@debian:~# ip link set mtu 1500 dev enp0s8
```

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



Transport level

Is the server responding to the expected port?

```
root@debian:~# nping --tcp-connect -p 80 -c 1 147.83.2.135
```

```
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2023-03-15 13:32 CET
```

```
SENT (0.0014s) Starting TCP Handshake > 147.83.2.135:80
```

```
RCVD (0.0104s) Handshake with 147.83.2.135:80 completed
```

```
Max rtt: 8.954ms | Min rtt: 8.954ms | Avg rtt: 8.954ms
```

```
TCP connection attempts: 1 | Successful connections: 1 | Failed: 0 (0.00%)
```

```
Nping done: 1 IP address pinged in 0.02 seconds
```

```
root@debian:~#
```



<< Verify the port number >>

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Transport level

Does the server respond with the expected service?



```
root@debian:~# nmap -sS -A -p 80,443 -oG upc 147.83.2.135
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-15 14:45 CET
Nmap scan report for www.upc.edu (147.83.2.135)
Host is up (0.0035s latency).
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx 1.23.2
443/tcp	open	ssl/http	nginx 1.23.2

...



<< Verify the version of the protocols >>

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



Transport level

Are there any active firewalls?

```
root@debian:~# nft list ruleset
...

root@debian:~# iptables -S
...
```



<< Firewall rules need to be reviewed >>
 Entry Rules...
 Exit Rules...

Transport level

Is there a connection to the server?

```
root@debian:~# wget www.upc.edu -b ; for i in $(seq 1 100); do ss -apt '( dst = 147.83.2.135 or src = 147.83.2.135 )'; done >file
Continuing in the background, ask 9751.
```

The output will be written to "wget-log.10".

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
SYN-SENT	0	1	10.0.3.15:45240	147.83.2.135:http	users:(("wget",pid=9751,fd=4))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
ESTAB	0	0	10.0.3.15:45240	147.83.2.135:http	users:(("wget",pid=9751,fd=4))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
CLOSE-WAIT	0	0	10.0.3.15:45240	147.83.2.135:http	users:(("wget",pid=9751,fd=4))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
SYN-SENT	0	1	10.0.3.15:35714	147.83.2.135:https	users:(("wget",pid=9751,fd=5))
CLOSE-WAIT	0	0	10.0.3.15:45240	147.83.2.135:http	users:(("wget",pid=9751,fd=4))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
ESTAB	0	517	10.0.3.15:35714	147.83.2.135:https	users:(("wget",pid=9751,fd=5))
CLOSE-WAIT	0	0	10.0.3.15:45240	147.83.2.135:http	users:(("wget",pid=9751,fd=4))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
ESTAB	0	0	10.0.3.15:35714	147.83.2.135:https	users:(("wget",pid=9751,fd=5))
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
FIN-WAIT-2	0	0	10.0.3.15:35714	147.83.2.135:https	
...					
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
TIME-WAIT	0	0	10.0.3.15:35714	147.83.2.135:https	



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level**
- 3 Network level
- 2 Link level
- 1 Physical level



<< Verify Multiple Connections >>
 Impractical in short connections...

Transport level

What happens during the connection to the server?



```

root@toc:~# tcpdump -n host 147.83.2.135
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens18, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:46:57.366725 IP 10.0.3.15.47556 > 147.83.2.135.80: Flags [S], seq 3550533459, win 64240, options [mss 1460,sackOK,TS val 1512823040 ecr 0,nop,wscale 7], length 0
15:46:57.368412 IP 147.83.2.135.80 > 10.0.3.15.47556: Flags [S.], seq 3417459063, ack 3550533460, win 14600, options [mss 1460,nop,wscale 0,sackOK,TS val 3854371925 ecr 1512823040], length 0
15:46:57.368458 IP 10.0.3.15.47556 > 147.83.2.135.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1512823041 ecr 3854371925], length 0
15:46:57.368513 IP 10.0.3.15.47556 > 147.83.2.135.80: Flags [P.], seq 1:125, ack 1, win 502, options [nop,nop,TS val 1512823041 ecr 3854371925], length 124: HTTP: GET / HTTP/1.1
15:46:57.369908 IP 147.83.2.135.80 > 10.0.3.15.47556: Flags [P.], seq 1:110, ack 125, win 14600, options [nop,nop,TS val 3854371927 ecr 1512823041], length 109: HTTP: HTTP/1.0 302 Moved Temporarily
15:46:57.369909 IP 147.83.2.135.80 > 10.0.3.15.47556: Flags [F.], seq 110, ack 125, win 14724, options [nop,nop,TS val 3854371927 ecr 1512823041], length 0
15:46:57.369914 IP 10.0.3.15.47556 > 147.83.2.135.80: Flags [.], ack 110, win 502, options [nop,nop,TS val 1512823043 ecr 3854371927], length 0
15:46:57.377624 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [S], seq 673605146, win 64240, options [mss 1460,sackOK,TS val 1512823050 ecr 0,nop,wscale 7], length 0
15:46:57.379259 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [S.], seq 3293003581, ack 673605147, win 14600, options [mss 1460,nop,wscale 0,sackOK,TS val 3854371936 ecr 1512823050], length 0
15:46:57.379302 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 1, win 502, options [nop,nop,TS val 1512823052 ecr 3854371936], length 0
15:46:57.380165 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [P.], seq 1:518, ack 1, win 502, options [nop,nop,TS val 1512823053 ecr 3854371936], length 517
15:46:57.381488 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], ack 518, win 15117, options [nop,nop,TS val 3854371938 ecr 1512823053], length 0
15:46:57.382659 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 1:5734, ack 518, win 15117, options [nop,nop,TS val 3854371939 ecr 1512823053], length 5733
15:46:57.382681 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 5734, win 485, options [nop,nop,TS val 1512823056 ecr 3854371939], length 0
15:46:57.383838 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [P.], seq 518:644, ack 5734, win 501, options [nop,nop,TS val 1512823057 ecr 3854371939], length 126
15:46:57.385065 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], ack 644, win 15243, options [nop,nop,TS val 3854371942 ecr 1512823057], length 0
15:46:57.385749 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 5734:5785, ack 644, win 15243, options [nop,nop,TS val 3854371943 ecr 1512823057], length 51
15:46:57.387579 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [P.], seq 644:797, ack 5785, win 501, options [nop,nop,TS val 1512823060 ecr 3854371943], length 153
15:46:57.388957 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], ack 797, win 15396, options [nop,nop,TS val 3854371946 ecr 1512823060], length 0
15:46:57.410219 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 5785:7567, ack 797, win 15396, options [nop,nop,TS val 3854371967 ecr 1512823060], length 1782
15:46:57.410383 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 7567, win 497, options [nop,nop,TS val 1512823083 ecr 3854371967], length 0
15:46:57.410569 IP 10.0.3.15.47556 > 147.83.2.135.80: Flags [F.], seq 125, ack 111, win 502, options [nop,nop,TS val 1512823083 ecr 3854371927], length 0
15:46:57.411050 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [P.], seq 797:1097, ack 7567, win 501, options [nop,nop,TS val 1512823084 ecr 3854371967], length 300
15:46:57.411843 IP 147.83.2.135.80 > 10.0.3.15.47556: Flags [.], ack 126, win 14724, options [nop,nop,TS val 3854371969 ecr 1512823083], length 0
15:46:57.412378 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], ack 1097, win 15696, options [nop,nop,TS val 3854371969 ecr 1512823084], length 0
15:46:57.413956 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 7567:23965, ack 1097, win 15696, options [nop,nop,TS val 3854371971 ecr 1512823084], length 16398
15:46:57.413996 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 23965:27824, ack 1097, win 15696, options [nop,nop,TS val 3854371971 ecr 1512823084], length 3859
15:46:57.413997 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 27824:27972, ack 1097, win 15696, options [nop,nop,TS val 3854371971 ecr 1512823084], length 148
15:46:57.414013 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 27824, win 414, options [nop,nop,TS val 1512823087 ecr 3854371971], length 0
15:46:57.415372 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 27972:50992, ack 1097, win 15696, options [nop,nop,TS val 3854371972 ecr 1512823087], length 23020
15:46:57.415377 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 50992, win 417, options [nop,nop,TS val 1512823088 ecr 3854371971], length 0
15:46:57.416800 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], seq 50992:75608, ack 1097, win 15696, options [nop,nop,TS val 3854371973 ecr 1512823088], length 24616
15:46:57.416802 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 75608:77056, ack 1097, win 15696, options [nop,nop,TS val 3854371973 ecr 1512823088], length 1448
15:46:57.416809 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 75608, win 886, options [nop,nop,TS val 1512823090 ecr 3854371973], length 0
15:46:57.418456 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], seq 77056:100224, ack 1097, win 15696, options [nop,nop,TS val 3854371975 ecr 1512823090], length 23168
15:46:57.418459 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 100224:104568, ack 1097, win 15696, options [nop,nop,TS val 3854371975 ecr 1512823090], length 4344
15:46:57.418465 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 100224, win 1270, options [nop,nop,TS val 1512823091 ecr 3854371973], length 0
15:46:57.418492 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 104568, win 1338, options [nop,nop,TS val 1512823091 ecr 3854371975], length 0
15:46:57.420020 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [P.], seq 104568:127374, ack 1097, win 15696, options [nop,nop,TS val 3854371977 ecr 1512823091], length 22806
15:46:57.420024 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 127374, win 1695, options [nop,nop,TS val 1512823093 ecr 3854371977], length 0
15:46:57.420665 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [F.], seq 1097, ack 127374, win 1695, options [nop,nop,TS val 1512823094 ecr 3854371977], length 0
15:46:57.421837 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [.], ack 1098, win 15696, options [nop,nop,TS val 3854371979 ecr 1512823094], length 0
15:46:57.422158 IP 147.83.2.135.443 > 10.0.3.15.37468: Flags [F.], seq 127374, ack 1098, win 15696, options [nop,nop,TS val 3854371979 ecr 1512823094], length 0
15:46:57.422170 IP 10.0.3.15.37468 > 147.83.2.135.443: Flags [.], ack 127375, win 1695, options [nop,nop,TS val 1512823095 ecr 3854371979], length 0
^C
44 packets captured
44 packets received by filter
0 packets dropped by kernel
root@toc:~#
    
```



<< It is necessary to analyze the traffic >>
 root@debian:~# tcpdump -n host 147.83.2.135

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level**
- 3 Network level
- 2 Link level
- 1 Physical level

Application level

What happens during the connection to the server?

```

root@debian:~# wget www.upc.edu -b

--2023-03-15 15:46:57-- http://www.upc.edu/
Resolviendo www.upc.edu (www.upc.edu)... 147.83.2.135, 2001:40b0:7500:1::21
Conectando con www.upc.edu (www.upc.edu)[147.83.2.135]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Moved Temporarily
Localización: https://www.upc.edu/ [siguiendo]
--2023-03-15 15:46:57-- https://www.upc.edu/
Conectando con www.upc.edu (www.upc.edu)[147.83.2.135]:443... conectado.
Petición HTTP enviada, esperando respuesta... 301 Moved Permanently
Localización: https://www.upc.edu/ca [siguiendo]
--2023-03-15 15:46:57-- https://www.upc.edu/ca
Reutilizando la conexión con www.upc.edu:443.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 117942 (115K) [text/html]
Grabando a: «index.html»

  0K ..... 43% 3,95M 0s
 50K ..... 86% 3,73M 0s
100K ..... 100% 60,1M=0,03s

2023-03-15 15:46:57 (4,38 MB/s) - «index.html» saved [117942/117942]
    
```



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



<< You need to verify the registration with that of the server >>

S

Server Team

Equivalent series

It is also necessary to apply all the above considerations to the client in a reciprocal way to the server.



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



<< Equivalent measures must be applied >>

Transport level

Are the ports associated with the service in listening mode?



```

root@www:~# ss -tlnp
State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
LISTEN  0        4096    0.0.0.0:https      0.0.0.0:*           users:(("docker-proxy",pid=2593,fd=4))
LISTEN  0        4096    0.0.0.0:http       0.0.0.0:*           users:(("docker-proxy",pid=2615,fd=4))
LISTEN  0        128     0.0.0.0:ssh        0.0.0.0:*           users:(("sshd",pid=455,fd=3))
LISTEN  0        4096    [::]:https        [::]:*              users:(("docker-proxy",pid=2600,fd=4))
LISTEN  0        4096    [::]:http         [::]:*              users:(("docker-proxy",pid=2622,fd=4))
LISTEN  0        128     [::]:ssh          [::]:*              users:(("sshd",pid=455,fd=4))
root@www:~#
    
```



<< Ports must be configured in LISTEN mode >>

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level

Transport level

Are the ports associated with the service responsive?

```
root@www:~# nping --tcp-connect -p 80 -c 1 localhost
```

```
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2023-03-15 17:06 CET
SENT (0.0015s) Starting TCP Handshake > localhost:80 (127.0.0.1:80)
RCVD (0.0015s) Handshake with localhost:80 (127.0.0.1:80) completed
```

```
Max rtt: 0.017ms | Min rtt: 0.017ms | Avg rtt: 0.017ms
TCP connection attempts: 1 | Successful connections: 1 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 0.00 seconds
root@www:~# nping --tcp-connect -p 443 -c 1 localhost
```

```
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2023-03-15 17:06 CET
SENT (0.0015s) Starting TCP Handshake > localhost:443 (127.0.0.1:443)
RCVD (0.0015s) Handshake with localhost:443 (127.0.0.1:443) completed
```

```
Max rtt: 0.014ms | Min rtt: 0.014ms | Avg rtt: 0.014ms
TCP connection attempts: 1 | Successful connections: 1 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 0.00 seconds
root@www:~#
```



- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



<< The corresponding processes must be verified >>

Application level

Is the service to be offered active?



```

root@www:~# systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-12-11 10:12:19 CET; 3 months 2 days ago
 TriggeredBy: ● docker.socket
            Docs: https://docs.docker.com
   Main PID: 454 (dockerd)
     Tasks: 52
    Memory: 238.3M
       CPU: 57min 26.983s
    CGroup: /system.slice/docker.service
            └─ 454 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
               └─ 2593 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 443 -container-ip 172.18.0.3 -contai>
                  └─ 2600 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 443 -container-ip 172.18.0.3 -container-p>
                     └─ 2615 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 80 -container-ip 172.18.0.3 -contai>
                        └─ 2622 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80 -container-ip 172.18.0.3 -container-po>

dic 11 10:12:17 www dockerd[454]: time="2022-12-11T10:12:17.919042671+01:00" level=info msg="Default bridge (docker0)>
dic 11 10:12:18 www dockerd[454]: time="2022-12-11T10:12:18.661180816+01:00" level=info msg="Loading containers: done>
dic 11 10:12:18 www dockerd[454]: time="2022-12-11T10:12:18.708025273+01:00" level=info msg="Docker daemon" commit=30>
dic 11 10:12:18 www dockerd[454]: time="2022-12-11T10:12:18.708423038+01:00" level=info msg="Daemon has completed ini>
dic 11 10:12:19 www systemd[1]: Started Docker Application Container Engine.
root@www:~#
    
```

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



<< The service must be activated >>
 root@debian:~# service servei start
 root@debian:~# update-rc.d servei enable

Application level

Are the processes associated with the service active?



```

root@www:~# ps aux | grep docker-proxy
root      2593  0.0  0.1 1592008 15468 ?        S1   2022   0:49 /usr/bin/docker-proxy -proto tcp -
host-ip 0.0.0.0 -host-port 443 -container-ip 172.18.0.3 -container-port 443
root      2600  0.0  0.1 1222196 13216 ?        S1   2022   0:08 /usr/bin/docker-proxy -proto tcp -
host-ip :: -host-port 443 -container-ip 172.18.0.3 -container-port 443
root      2615  0.0  0.1 1296184 15128 ?        S1   2022   0:08 /usr/bin/docker-proxy -proto tcp -
host-ip 0.0.0.0 -host-port 80 -container-ip 172.18.0.3 -container-port 80
root      2622  0.0  0.1 1148464 15096 ?        S1   2022   0:08 /usr/bin/docker-proxy -proto tcp -
host-ip :: -host-port 80 -container-ip 172.18.0.3 -container-port 80
root      811943  0.0  0.0  6252  640 pts/0    S+   16:52   0:00 grep docker-proxy
root@www:~#
    
```



<< The corresponding processes must be verified >>

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



Application level

What information is in the service log?

```

root@www:/var/log# docker ps
CONTAINER ID   IMAGE                                COMMAND                                CREATED        STATUS        PORTS
NAMES
f7c883ff6c68   wordpress-wordpress                 "docker-entrypoint.s..."           3 months ago  Up 6 hours   0.0.0.0:80->80/tcp,
:::80->80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp   catac_wordpress
35ecd8ceba52   mysql:5.7                           "docker-entrypoint.s..."           3 months ago  Up 6 hours   3306/tcp, 33060/tcp
catac_wordpress_db
root@www:/var/log#
root@www:/var/log# docker logs f7c883ff6c68 | grep 147.83.158.232
...
www.catac.upc.edu:80 147.83.158.232 - - [15/Mar/2023:15:46:57 +0000] "GET / HTTP/1.1" 302 301 580 "-" "Wget/1.21"
    
```

- 7 Application level
- 6 Presentation level
- 5 Session level
- 4 Transport level
- 3 Network level
- 2 Link level
- 1 Physical level



<< Verification of the registration with the customer's registration >>



Conclusion

Conclusion

And if despite everything the connectivity between client and server has not yet been resolved...

It is necessary to review
SEAX practices

Links

The case of client and server



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH



Aquest treball es publica amb una llicència Creative Commons
Reconeixement – No Comercial 4.0 Internacional (CC BY-NC 4.0)