NETWORKING

CAPAS DEL MODELO OSI

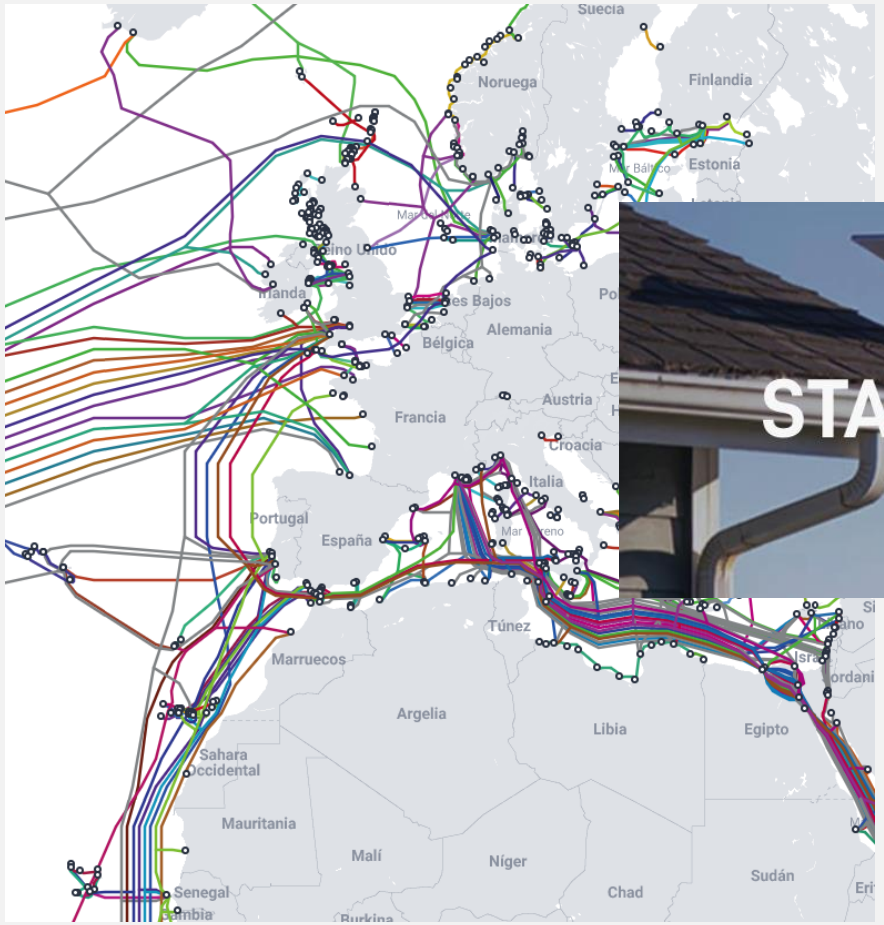
https://osi-model.com

1. Física
2. Enlace datos
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

https://www.submarinecablemap.com

FÍSICA

- **Ethernet**
- **Bluetooth**
- **IRDA**
- **DSL**



ENLACE DATOS

```
ubuntu@vps-167c03b8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether fa:16:3e:18:16:bd brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 51.91.56.42/32 metric 100 scope global dynamic ens3
       valid_lft 65070sec preferred_lft 65070sec
    inet6 2001:41d0:305:2100::54c9/56 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe18:16bd/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

```
ubuntu@vps-167c03b8:~$ ping vbo.damiansu.com
PING vbo.damiansu.com (51.91.56.42) 56(84) bytes of data.
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=4 ttl=64 time=0.035 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=5 ttl=64 time=0.039 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=6 ttl=64 time=0.041 ms
64 bytes from vps-167c03b8.vps.ovh.net (51.91.56.42): icmp_seq=7 ttl=64 time=0.066 ms
^C
--- vbo.damiansu.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6129ms
rtt min/avg/max/mdev = 0.025/0.041/0.066/0.011 ms
```

```
mtr vbo.damiansu.com
```

```
                                  My traceroute  [v0.95]
ps-167c03b8 (51.91.56.42) -> vbo.damiansu.com (51.91.56.42)                2025-01-28T14:47:47+0000
eys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets                 Pings
Host                                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
1. vps-167c03b8.vps.ovh.net                             0.0%     6    0.1   0.1   0.1   0.1   0.0
```

```
                                  My traceroute  [v0.95]
vps-167c03b8 (51.91.56.42) -> osi-model.com (45.32.184.51)                 2025-01-28T14:49:37+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets                 Pings
 Host                                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway                                             0.0%    23    0.2   0.2   0.2   0.3   0.1
 2. 192.168.143.254                                      0.0%    23    0.3   0.3   0.2   0.4   0.0
 3. 10.225.18.190                                        0.0%    23    0.4   0.4   0.3   0.6   0.1
 4. 10.225.17.138                                        0.0%    23    0.4   0.4   0.3   0.6   0.1
 5. 10.225.17.154                                        0.0%    23    0.5   0.5   0.4   0.7   0.1
 6. 10.73.2.214                                          0.0%    23    0.4   0.4   0.3   0.5   0.1
 7. 10.95.33.10                                          0.0%    23   85.4  10.5   1.3  85.4  24.4
 8. 10.200.4.147                                         0.0%    23    7.1   7.0   6.8   7.7   0.2
 9. 10.200.4.135                                         0.0%    22    6.3   6.4   6.3   6.6   0.1
10. 80.249.212.38                                        0.0%    22    7.6   9.7   6.9  24.2   5.0
11. (waiting for reply)
12. (waiting for reply)
13. (waiting for reply)
14. web.cia.li                                           0.0%    22    6.8   6.9   6.8   7.0   0.0
```

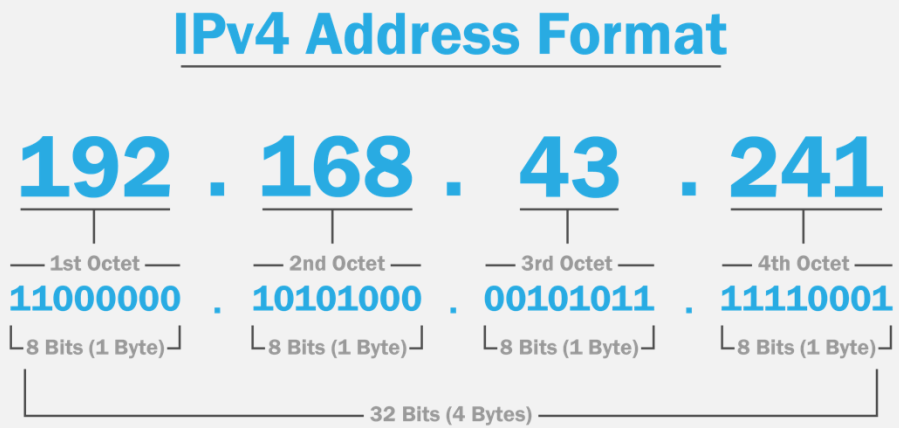
```
sudo apt install net-tools
```

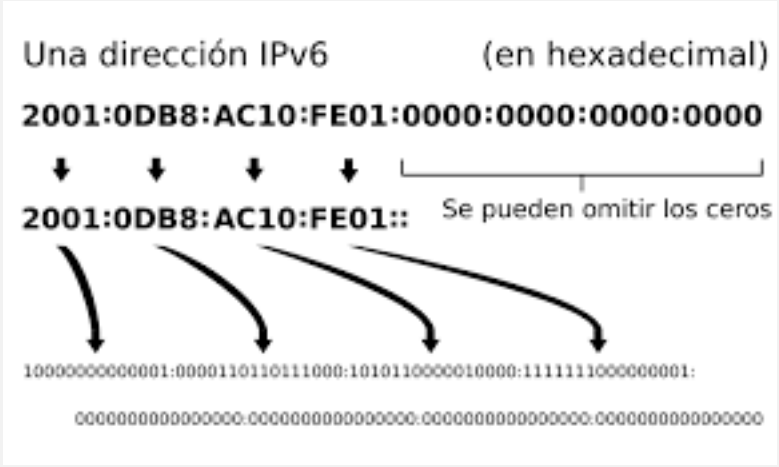
```
ubuntu@vps-167c03b8:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   4a:85:19:6c:3e:46   C                     ens3
Entries: 1      Skipped: 0      Found: 1
```

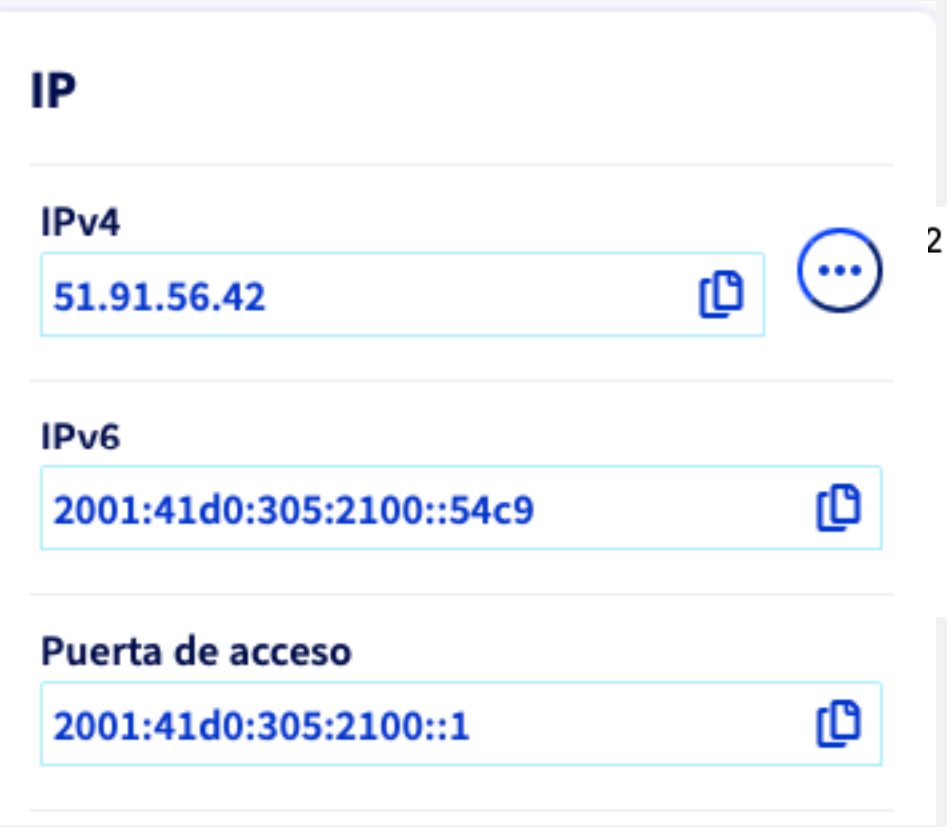
```
Interfaz: 192.168.1.119 --- 0xc
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1            2c-96-82-75-c3-fa     dinámico
  192.168.1.49           84-a4-66-ec-95-70     dinámico
  192.168.1.50           24-ce-33-d0-80-0f     dinámico
  192.168.1.62           2c-f0-5d-a1-fb-2e     dinámico
  192.168.1.106          50-c2-e8-ca-ef-69     dinámico
  192.168.1.255          ff-ff-ff-ff-ff-ff     estático
  224.0.0.2              01-00-5e-00-00-02     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático
```

RED

```
ubuntu@vps-167c03b8:~$ ping vbo.damiansu.com
PING vbo.damiansu.com (51.91.56.42) 56(84) bytes of data.
```





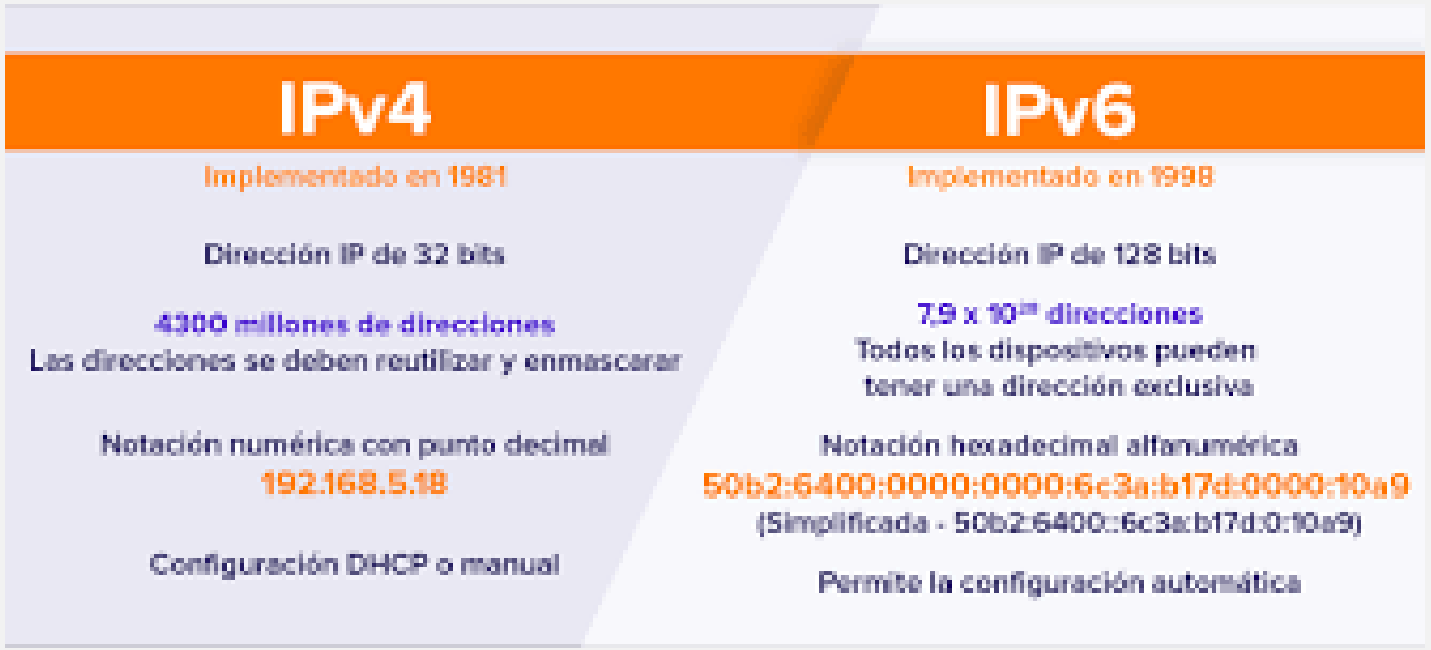



```
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    link/ether fa:16:3e:18:16:bd brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 51.91.56.42/32 metric 100 scope global dynamic ens3
       valid_lft 63707sec preferred_lft 63707sec
    inet6 2001:41d0:305:2100::54c9/56 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe18:16bd/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

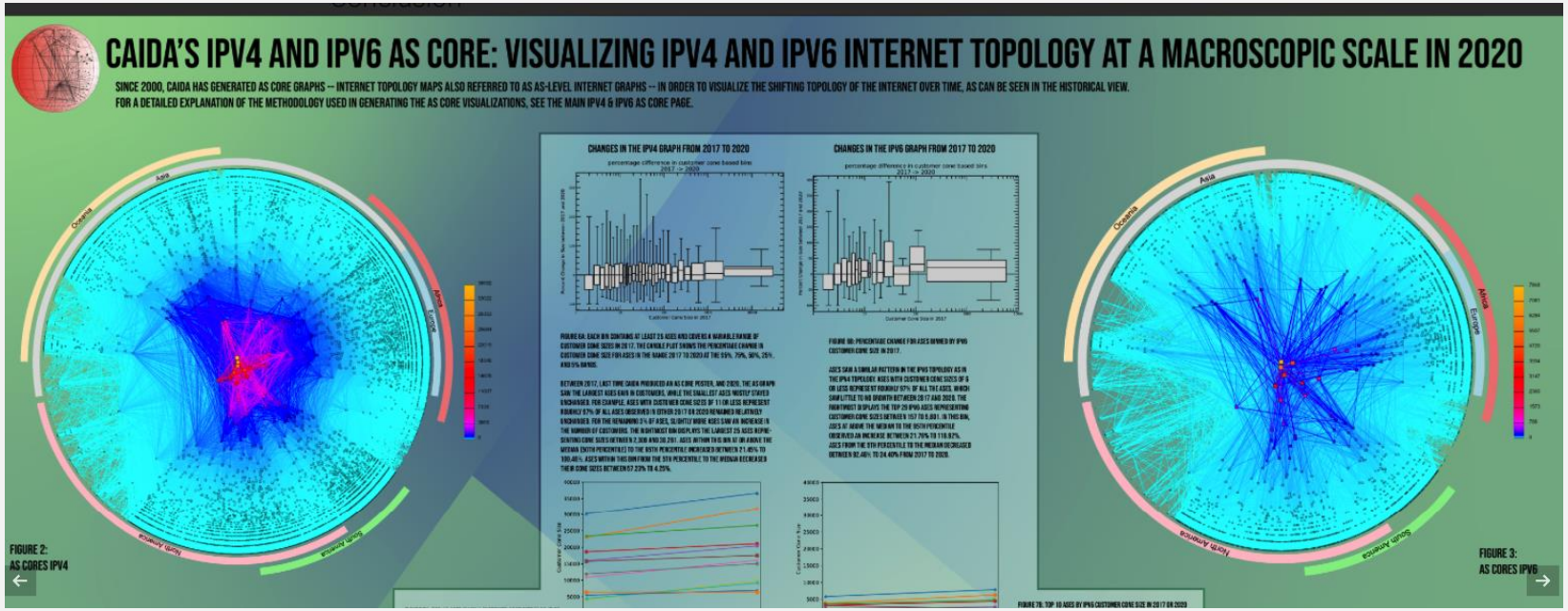
```
ubuntu@vps-167c03b8:~$ ping -4 google.com
PING google.com (142.250.178.142) 56(84) bytes of data.
64 bytes from par21s22-in-f14.1e100.net (142.250.178.142): icmp_seq=1 ttl=111 time=4.49 ms
64 bytes from par21s22-in-f14.1e100.net (142.250.178.142): icmp_seq=2 ttl=111 time=4.55 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.485/4.517/4.549/0.032 ms
ubuntu@vps-167c03b8:~$ ping -6 google.com
PING google.com (2a00:1450:4007:819::200e) 56 data bytes
64 bytes from par21s22-in-x0e.1e100.net (2a00:1450:4007:819::200e): icmp_seq=1 ttl=111 time=5.34 ms
64 bytes from par21s22-in-x0e.1e100.net (2a00:1450:4007:819::200e): icmp_seq=2 ttl=111 time=4.79 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.787/5.062/5.338/0.275 ms
```

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$.

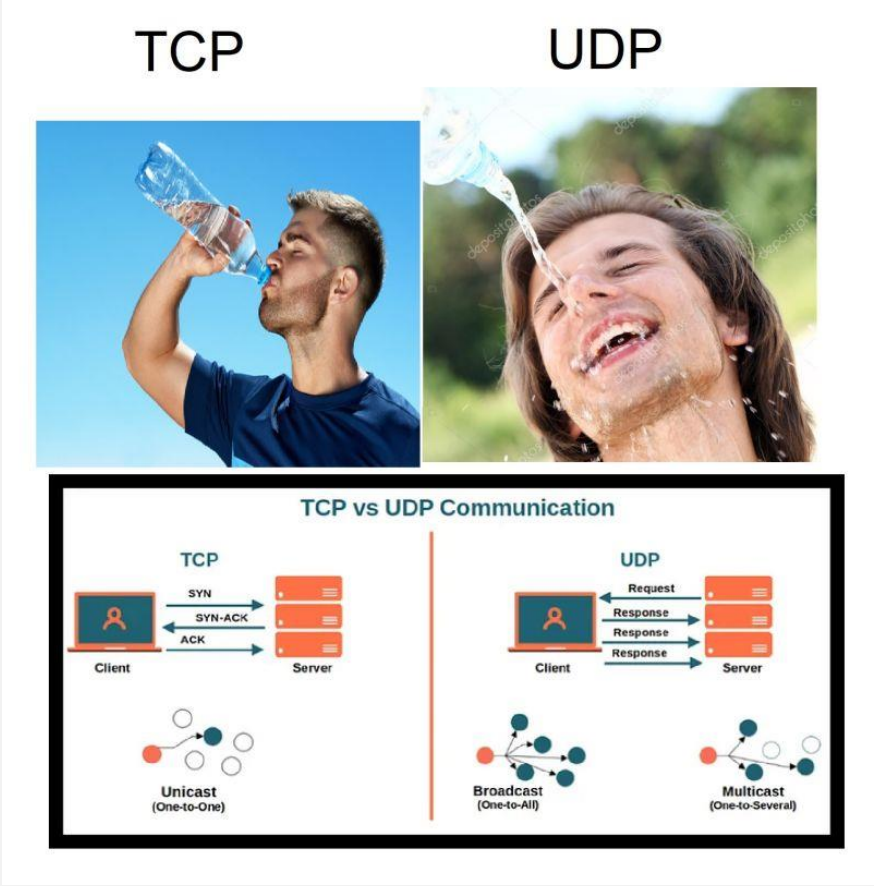
Descomposición de la representación de la dirección IPv4 de cuatro valores, a su equivalente binario. El IPv4 utiliza direcciones de 32 bits que limitan el espacio de direcciones a **4 294 967 296 (2^{32}) direcciones posibles**.



https://www.caida.org/projects/as-core/2020/



TRANSPORTE


TCP
UDP
TCP vs UDP Communication
TCP
SYN
SYN-ACK
ACK
Client
Server
UDP
Request
Response
Response
Response
Client
Server
Unicast
(One-to-One)
Broadcast
(One-to-All)
Multicast
(One-to-Several)

```
ubuntu@vps-167c03b8:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        1      0 127.0.0.1:44526         127.0.0.1:8080          CLOSE_WAIT
tcp        0     88 51.91.56.42:22          83.39.186.21:60646      ESTABLISHED
tcp        0      0 51.91.56.42:22          158.69.186.214:35582    ESTABLISHED
tcp        1      0 127.0.0.1:57504         127.0.0.1:8080          CLOSE_WAIT
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::8080                 :::*                    LISTEN
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 51.91.56.42:68          0.0.0.0:*
```

```
ubuntu@vps-167c03b8:~$ netstat -an | grep "tcp"
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        1      0 127.0.0.1:44526         127.0.0.1:8080          CLOSE_WAIT
tcp        0      0 51.91.56.42:22          45.118.147.13:49076     ESTABLISHED
tcp        0     52 51.91.56.42:22          83.39.186.21:60646      ESTABLISHED
tcp        1      0 127.0.0.1:57504         127.0.0.1:8080          CLOSE_WAIT
tcp        0      0 51.91.56.42:22          158.69.186.214:42546    ESTABLISHED
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 51.91.56.42:8080        83.63.17.10:33274       ESTABLISHED
ubuntu@vps-167c03b8:~$ netstat -an | grep "udp"
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 51.91.56.42:68          0.0.0.0:*
```

```
ubuntu@vps-167c03b8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state U
    link/ether fa:16:3e:18:16:bd brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 51.91.56.42/32 metric 100 scope global dynamic ens3
       valid_lft 62317sec preferred_lft 62317sec
    inet6 2001:41d0:305:2100::54c9/56 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe18:16bd/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
ubuntu@vps-167c03b8:~$ sudo tcpdump -i ens3
```

```
gth 36
5:28:33.760534 IP cyber214.altomarketing.net.46706 > vps-167c03b8.vps.ovh.net.ssh: Flags [P.], seq
037:1053, ack 1442, win 269, options [nop,nop,TS val 2703789982 ecr 472956401], length 16
5:28:33.760534 IP cyber214.altomarketing.net.46706 > vps-167c03b8.vps.ovh.net.ssh: Flags [P.], seq
053:1121, ack 1442, win 269, options [nop,nop,TS val 2703789982 ecr 472956401], length 68
5:28:33.760605 IP vps-167c03b8.vps.ovh.net.ssh > cyber214.altomarketing.net.46706: Flags [.], ack 1
21, win 524, options [nop,nop,TS val 472956489 ecr 2703789982], length 0
5:28:33.760763 IP vps-167c03b8.vps.ovh.net.ssh > cyber214.altomarketing.net.46706: Flags [P.], seq
442:1510, ack 1121, win 524, options [nop,nop,TS val 472956490 ecr 2703789982], length 68
5:28:33.776085 IP 21.red-83-39-186.dynamicip.rima-tde.net.60646 > vps-167c03b8.vps.ovh.net.ssh: Fla
s [.], ack 112609, win 2040, options [nop,nop,TS val 606100573 ecr 1394437665], length 0
5:28:33.776491 IP 21.red-83-39-186.dynamicip.rima-tde.net.60646 > vps-167c03b8.vps.ovh.net.ssh: Fla
s [.], ack 112997, win 2041, options [nop,nop,TS val 606100573 ecr 1394437665], length 0
5:28:33.776867 IP 21.red-83-39-186.dynamicip.rima-tde.net.60646 > vps-167c03b8.vps.ovh.net.ssh: Fla
s [.], ack 113593, win 2048, options [nop,nop,TS val 606100573 ecr 1394437666], length 0
```

SESIÓN

NetBIOS	Network Basic Input Output System
PAP	Password Authentication Protocol
PPTP	Point-to-Point Tunneling Protocol
RPC	Remote Procedure Call Protocol
RTCP	Real-time Transport Control Protocol
SMPP	Short Message Peer-to-Peer
SCP	Session Control Protocol
SOCKS	the SOCKS internet protocol, see Internet socket
ZIP	Zone Information Protocol
SDP	Sockets Direct Protocol

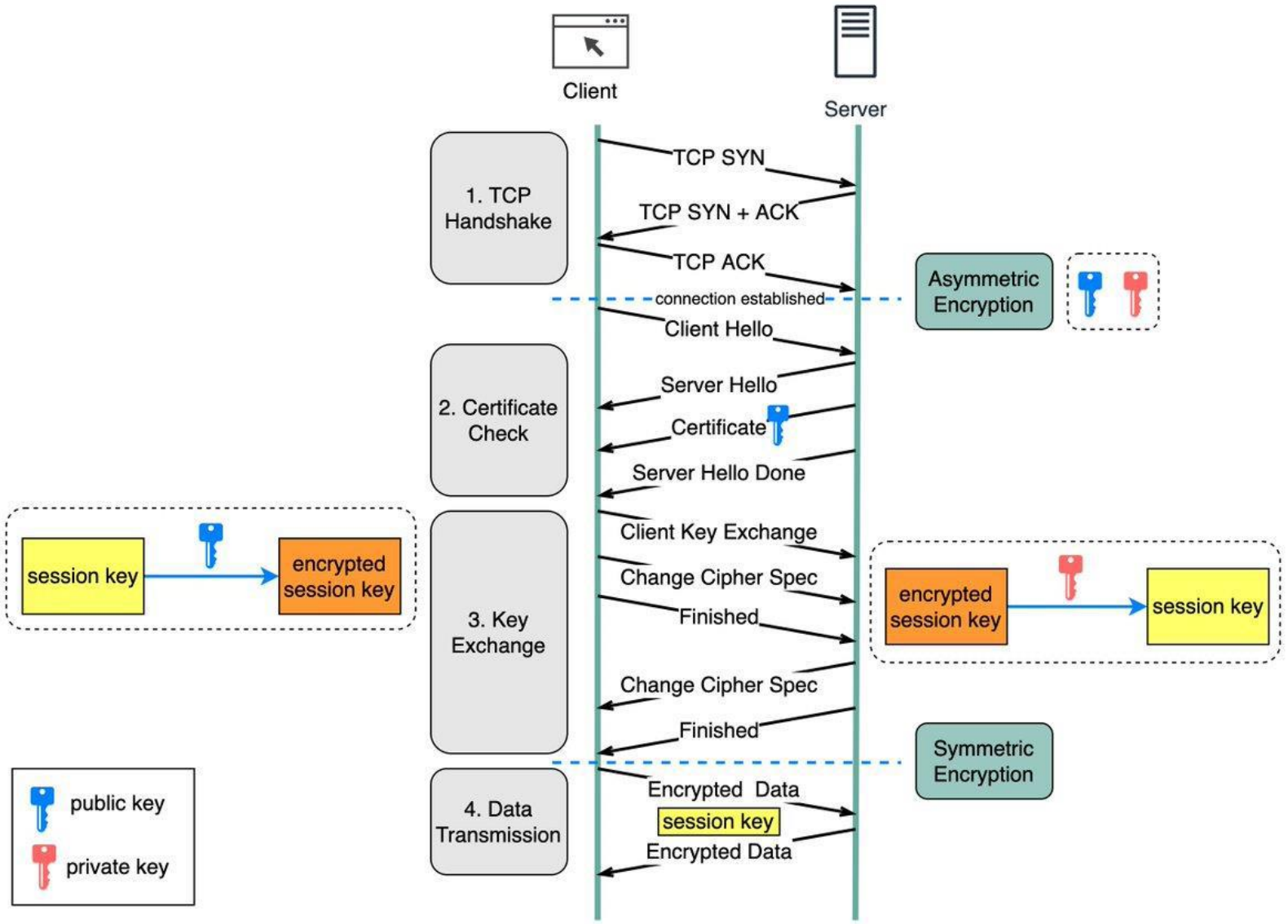
PRESENTACIÓN

Resumen de las diferencias: SSL en comparación con TLS

	SSL	TLS
Qué significa	*SSL* son las siglas de Secure Sockets Layer (capa de sockets seguros).	*TLS* son las siglas de Transport Layer Security (seguridad de la capa de transporte).
Historial de versiones	TLS sustituyó SSL. SSL pasó por las versiones 1.0, 2.0 y 3.0.	TLS es la versión mejorada de SSL. TLS ha pasado por las versiones 1.0, 1.1, 1.2 y 1.3.
Actividad	Todas las versiones de SSL están obsoletas.	Las versiones 1.2 y 1.3 de TLS se utilizan activamente.
Mensajes de alerta	SSL solo tiene dos tipos de mensajes de alerta. Los mensajes de alerta no están cifrados.	Los mensajes de alerta de TLS están cifrados y son más diversos.
Autentificación de mensajes	SSL usa MAC.	TLS usa HMAC.
Conjuntos de cifrado	SSL admite algoritmos más antiguos con vulnerabilidades de seguridad conocidas.	TLS utiliza algoritmos de cifrado avanzados.
Protocolo de enlace	Un protocolo de enlace SSL es complejo y lento.	Un protocolo de enlace TLS tiene menos pasos y una conexión más rápida.

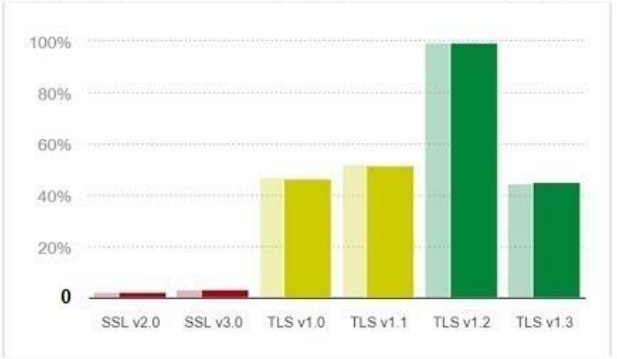
How does HTTPS Work?

blog.bytebytego.com



SSL/TLS Versions

SSL 1.0	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
1994	1995	1996	1999	2006	2008	2018



Part 2

Practical TLS

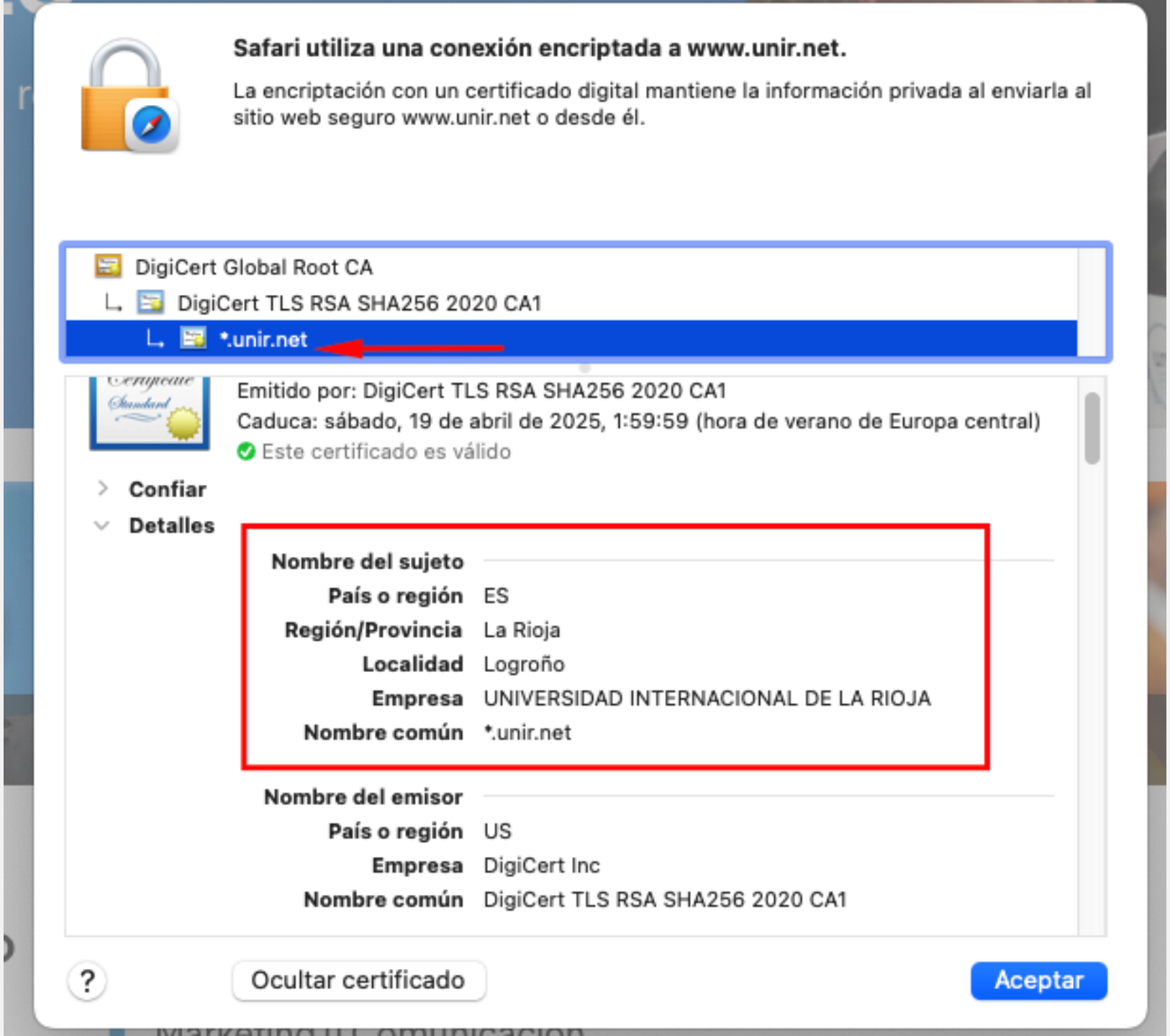
```
ubuntu@vps-167c03b8:~$ openssl
help:

Standard commands
```

APLICACIÓN - HTTP

```
root@vps-167c03b8:/home/ubuntu# telnet vbo.damiansu.com 80
Trying 51.91.56.42...
Connected to vbo.damiansu.com.
Escape character is '^]'.
GET /saludo.html HTTP/1.1
Host: hola

HTTP/1.1 200 OK
Date: Tue, 04 Feb 2025 14:58:22 GMT
Server: Apache/2.4.62 (Ubuntu)
Last-Modified: Tue, 04 Feb 2025 14:54:33 GMT
ETag: "5f-62d522fd1ba13"
Accept-Ranges: bytes
Content-Length: 95
Vary: Accept-Encoding
Content-Type: text/html

<html>
<header>
<header>
<body>
        <h1>Fue roja directa... no hay discusion</h1>
</body>
</html>
```

```
root@vps-167c03b8:/home/ubuntu# wget vbo.damiansu.com/saludo.html
--2025-02-04 15:01:30--  http://vbo.damiansu.com/saludo.html
Resolving vbo.damiansu.com (vbo.damiansu.com)... 51.91.56.42
Connecting to vbo.damiansu.com (vbo.damiansu.com)|51.91.56.42|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 95 [text/html]
Saving to: ‘saludo.html’

saludo.html                 100%[=======================================>]      95  --.-KB/s    in 0s

2025-02-04 15:01:30 (8.09 MB/s) - ‘saludo.html’ saved [95/95]

root@vps-167c03b8:/home/ubuntu# ls
index.html  saludo.html
root@vps-167c03b8:/home/ubuntu#
```

```
root@vps-167c03b8:/home/ubuntu# wget -d https://www.unir.net/
DEBUG output created by Wget 1.24.5 on linux-gnu.

Reading HSTS entries from /root/.wget-hsts
URI encoding = ‘UTF-8’
Converted file name 'index.html' (UTF-8) -> 'index.html' (UTF-8)
--2025-02-04 15:05:56--  https://www.unir.net/
Resolving www.unir.net (www.unir.net)... 2a02:26f0:e8::6856:6f4a, 2a02:26f0:e8::6856:6e58, 2.21.67.49, ...
Caching www.unir.net => 2a02:26f0:e8::6856:6f4a 2a02:26f0:e8::6856:6e58 2.21.67.49 2.21.67.8
Connecting to www.unir.net (www.unir.net)|2a02:26f0:e8::6856:6f4a|:443... connected.
Created socket 3.
Releasing 0x0000618640ef7200 (new refcount 1).
Initiating SSL handshake.
Handshake successful; connected socket 3 to SSL handle 0x0000618640f03b40
certificate:
  subject: CN=*.unir.net,O=UNIVERSIDAD INTERNACIONAL DE LA RIOJA,L=Logro\\C3\\B1o,ST=La Rioja,C=ES
  issuer:  CN=DigiCert TLS RSA SHA256 2020 CA1,O=DigiCert Inc,C=US
X509 certificate successfully verified and matches host www.unir.net
```


Safari utiliza una conexión encriptada a www.unir.net.
La encriptación con un certificado digital mantiene la información privada al enviarla al sitio web seguro www.unir.net o desde él.
DigiCert Global Root CA
DigiCert TLS RSA SHA256 2020 CA1
*.unir.net
Emitido por: DigiCert TLS RSA SHA256 2020 CA1
Caduca: sábado, 19 de abril de 2025, 1:59:59 (hora de verano de Europa central)
Este certificado es válido
Confiar
Detalles
Nombre del sujeto
País o región ES
Región/Provincia La Rioja
Localidad Logroño
Empresa UNIVERSIDAD INTERNACIONAL DE LA RIOJA
Nombre común *.unir.net
Nombre del emisor
País o región US
Empresa DigiCert Inc
Nombre común DigiCert TLS RSA SHA256 2020 CA1
?
Ocultar certificado
Aceptar

```
root@vps-167c03b8:/home/ubuntu# curl vbo.damiansu.com/saludo.html
<html>
<header>
<header>
<body>
        <h1>Fue roja directa... no hay discusion</h1>
</body>
</html>
```

```
root@vps-167c03b8:/home/ubuntu# curl -v vbo.damiansu.com/saludo.html
* Host vbo.damiansu.com:80 was resolved.
* IPv6: (none)
* IPv4: 51.91.56.42
*   Trying 51.91.56.42:80...
* Connected to vbo.damiansu.com (51.91.56.42) port 80
> GET /saludo.html HTTP/1.1
> Host: vbo.damiansu.com
> User-Agent: curl/8.9.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 04 Feb 2025 15:13:59 GMT
< Server: Apache/2.4.62 (Ubuntu)
< Last-Modified: Tue, 04 Feb 2025 14:54:33 GMT
< ETag: "5f-62d522fd1ba13"
< Accept-Ranges: bytes
< Content-Length: 95
< Vary: Accept-Encoding
< Content-Type: text/html
<
<html>
<header>
<header>
<body>
        <h1>Fue roja directa... no hay discusion</h1>
</body>
</html>
* Connection #0 to host vbo.damiansu.com left intact
root@vps-167c03b8:/home/ubuntu#
```

SEGURIDAD PERIMETRAL

FIREWALL

```
root@vps-167c03b8:/home/ubuntu# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? n
Aborted
root@vps-167c03b8:/home/ubuntu# ufw allow ssh
Rules updated
Rules updated (v6)
root@vps-167c03b8:/home/ubuntu# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@vps-167c03b8:/home/ubuntu#
```

```
root@vps-167c03b8:/home/ubuntu# ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

```
root@vps-167c03b8:/home/ubuntu# ufw allow http
Rule added
Rule added (v6)
root@vps-167c03b8:/home/ubuntu# ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
```

```
root@vps-167c03b8:/home/ubuntu# ufw allow 53/udp
Rule added
Rule added (v6)
root@vps-167c03b8:/home/ubuntu# ufw allow 443/tcp
Rule added
Rule added (v6)
root@vps-167c03b8:/home/ubuntu#
```

```
root@vps-167c03b8:/home/ubuntu# ufw allow 8080/tcp
Rule added
Rule added (v6)
```

```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
53/udp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
8080/tcp                   ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
53/udp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)
```