2. Configuración openVPN

2.1. Generación de certificados

2.1.1. Los ficheros de certificados y claves privadas que has generado y en qué carpetas los has almacenado en cada una de las máquinas.

En la máquina pc1, creamos el certificado de CA y los parámetros DH. Una vez generado, se guardara en /rsa/keys, si hacemos un ls de ese directorio nos aparecerán los ficheros:

ca.crt ca.key dh1024.pem index.txt serial

La clave privada será el fichero ca.key, y el certificado ca.crt

Después de generar ca configuramos algunos parametros:

Servidor VPN en r4:

pc1: ./build-key-server r4

```
root@pc1:~/rsa/keys# ls
        01.pem  ca.key      index.txt       index.txt.old  r4.csr  serial
        ca.crt  dh1024.pem  index.txt.attr  r4.crt         r4.key  serial.old

root@pc1:~/rsa/keys# cp r4.crt /hostlab/r4.old/etc/openvpn/
root@pc1:~/rsa/keys# cp ca.crt /hostlab/r4.old/etc/openvpn/
root@pc1:~/rsa/keys# cp r4.key /hostlab/r4.old/etc/openvpn/
root@pc1:~/rsa/keys# cp dh1024.pem /hostlab/r4.old/etc/openvpn/

root@r4:/etc/openvpn# cp /hostlab/r4.old/etc/openvpn/r4.crt .
root@r4:/etc/openvpn# cp /hostlab/r4.old/etc/openvpn/ca.crt .
root@r4:/etc/openvpn# cp /hostlab/r4.old/etc/openvpn/r4.key .
root@r4:/etc/openvpn# cp /hostlab/r4.old/etc/openvpn/dh1024.pem .
```

Cliente VPN en r1 y en pc3:

pc1: ./build-key r1

```
root@pc1:~/rsa/keys# ls
        01.pem  ca.key      index.txt.attr      r1.crt  r4.crt  serial
        02.pem  dh1024.pem  index.txt.attr.old  r1.csr  r4.csr  serial.old
        ca.crt  index.txt   index.txt.old       r1.key  r4.key

root@pc1:~/rsa/keys# cp r1.key /hostlab/r1.old/etc/openvpn/
root@pc1:~/rsa/keys# cp r1.crt /hostlab/r1.old/etc/openvpn/
root@pc1:~/rsa/keys# cp ca.crt /hostlab/r1.old/etc/openvpn/

root@r1:/etc/openvpn# cp /hostlab/r1.old/etc/openvpn/r1.crt .
root@r1:/etc/openvpn# cp /hostlab/r1.old/etc/openvpn/r1.key .
root@r1:/etc/openvpn# cp /hostlab/r1.old/etc/openvpn/ca.crt .

pc1: ./build-key pc3

root@pc1:~/rsa/keys# ls
```

```
01.pem  ca.crt     index.txt          index.txt.old  pc3.key  r1.key  r4.key
02.pem  ca.key     index.txt.attr     pc3.crt        r1.crt   r4.crt  serial
03.pem  dh1024.pem index.txt.attr.old pc3.csr        r1.csr   r4.csr  serial.old
```

```
root@pc1:~/rsa/keys# cp ca.crt /hostlab/pc3.old/etc/openvpn/
root@pc1:~/rsa/keys# cp pc3.crt /hostlab/pc3.old/etc/openvpn/
root@pc1:~/rsa/keys# cp pc3.key /hostlab/pc3.old/etc/openvpn/

root@pc3:/etc/openvpn# cp /hostlab/pc3.old/etc/openvpn/ca.crt .
root@pc3:/etc/openvpn# cp /hostlab/pc3.old/etc/openvpn/pc3.key .
root@pc3:/etc/openvpn# cp /hostlab/pc3.old/etc/openvpn/pc3.crt .
```

2.1.2. Incluye en la memoria el resultado de imprimir de forma legible cada uno de los certificados que has creado.

Pc1: openssl x509 -in ca.crt -text

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         ed:d7:e9:35:c0:2a:aa:a4
   Signature Algorithm: sha1WithRSAEncryption
                        Issuer: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT,
CN=pc1/name=Saul/emailAddress=mail@host.domain
      Validity
         Not Before: Apr  6 15:20:14 2017 GMT
         Not After : Apr  4 15:20:14 2027 GMT
                      Subject: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT,
CN=pc1/name=Saul/emailAddress=mail@host.domain
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
               00:a1:a2:d7:74:05:28:df:67:13:54:2a:df:9a:3f:
               6f:64:97:f3:86:1a:50:54:f7:ec:5e:6e:04:22:e0:
               ce:71:8d:25:86:34:a0:a4:fe:98:4d:7e:2c:7c:4c:
               c2:4e:0e:d4:84:ff:5e:ab:e0:b7:30:97:93:7f:9d:
               48:47:a2:ec:8b:7b:1d:83:5e:2b:82:b1:53:a2:80:
               69:59:47:4a:7e:ba:94:c0:44:49:d1:6a:c4:4e:7d:
               bc:1d:a1:5d:d2:47:83:12:bd:22:ef:25:0e:86:16:
               74:d9:9f:1d:af:a3:39:a4:46:ab:13:13:b1:e8:ae:
               89:d9:9e:2c:96:3e:eb:de:8d
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Key Identifier:
            C4:7D:1B:65:CF:94:97:1B:F8:5A:77:9A:AA:9A:C4:3C:80:55:C1:14
         X509v3 Authority Key Identifier:
            keyid:C4:7D:1B:65:CF:94:97:1B:F8:5A:77:9A:AA:9A:C4:3C:80:55:C1:14
```

DirName:/C=ES/ST=Madrid/L=Fuenlabrada/O=Saul/OU=IT/CN=pc1/name=Saul/emailAddress=mail@host.domain
serial:ED:D7:E9:35:C0:2A:AA:A4

X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
46:65:ef:b8:a4:90:67:01:01:d1:24:9f:68:c6:1f:c7:4d:cc:
5a:4f:37:c8:3d:6f:e1:72:86:7d:47:f6:d9:d6:e3:d5:34:3b:
84:34:56:ef:1d:e0:cc:55:26:28:24:dd:fd:cd:4a:dd:bf:ea:
4f:09:24:aa:ef:bb:65:86:8a:70:aa:b3:b8:10:9e:1a:95:31:
32:de:e6:e7:bc:60:9b:2d:87:75:20:d0:f9:47:7e:c9:bf:3a:
a8:28:bd:8b:71:c0:3c:16:05:7c:5b:76:96:dc:69:cf:a0:9d:
3a:28:97:65:5d:e1:2e:6d:c5:63:94:67:87:48:dc:79:0c:fe:
0b:8d

-----BEGIN CERTIFICATE-----
MIIDkzCCAvygAwIBAgIJAO3X6TXAKqqkMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYDV
QQGEwJFUzEPMA0GA1UECBMGTWFkcmlkMRQwEgYDVQQHEwtGdWVubGFicmFkYTEN
MAsGA1UEChMEU2F1bDELMAkGA1UECxMCSVQxDDAKBgNVBAMTA3BjMTENMAsGA
1UEKRMEU2F1bDEfMB0GCSqGSIb3DQEJARYQbWFpbEBob3N0LmRvbWFpbjAeFw0xNzA
0MDYxNTIwMTRaFw0yNzA0MDQxNTIwMTRaMIGOMQswCQYDVQQGEwJFUzEPMA0GA
1UECBMGTWFkcmlkMRQwEgYDVQQHEwtGdWVubGFicmFkYTENMAsGA1UEChMEU2F1
bDELMAkGA1UECxMCSVQxDDAKBgNVBAMTA3BjMTENMAsGA1UEKRMEU2F1bDEfM
B0GCSqGSIb3DQEJARYQbWFpbEBob3N0LmRvbWFpbjCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAoaLXdAUo32cTVCrfmj9vZJfzhhpQVPfsXm4EIuDOcY0lhjSgpP6YTX4sfEzCT
g7UhP9eq+C3MJeTf51IR6Lsi3sdg14rgrFTooBpWUdKfrqUwERJ0WrETn28HaFd0keDEr0i7yUO
hhZ02Z8dr6M5pEarExOx6K6J2Z4slj7r3o0CAwEAAaOB9jCB8zAdBgNVHQ4EFgQUxH0bZc+U
lxv4WneaqprEPIBVwRQwgcMGA1UdIwSBuzCBuIAUxH0bZc+Ulxv4WneaqprEPIBVwRShgZS
kgZEwgY4xCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZNYWRyaWQxFDASBgNVBAcTC
0Z1ZW5sYWJyYWRhMQ0wCwYDVQQKEwRTYXVsMQswCQYDVQQLEwJJVDEMMAoGA
1UEAxMDcGMxMQ0wCwYDVQQpEwRTYXVsMR8wHQYJKoZIhvcNAQkBFhBtYWlsQGhv
c3QuZG9tYWluggkA7dfpNcAqqqQwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAO
BgQBGZe+4pJBnAQHRJJ9oxh/HTcxaTzfIPW/hcoZ9R/bZ1uPVNDuENFbvHeDMVSYoJN39zUr
dv+pPCSSq77tlhopwqrO4EJ4alTEy3ubnvGCbLYd1IND5R37JvzqoKL2LccA8FgV8W3aW3GnPo
J06KJdlXeEubcVjlGeHSNx5DP4LjQ==
-----END CERTIFICATE-----

R4:

root@r4:/etc/openvpn# openssl x509 -in r4.crt -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT, CN=pc1/name=Saul/emailAddress=mail@host.domain
Validity
Not Before: Apr 6 15:43:31 2017 GMT
Not After : Apr 4 15:43:31 2027 GMT

```
            Subject: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT,
CN=r4/name=Saul/emailAddress=mail@host.domain
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b9:28:b8:c9:0b:4f:08:98:01:ee:f3:49:5a:62:
                    30:63:a7:16:33:6e:d4:79:49:2a:18:62:c1:4e:ef:
                    23:cd:ae:a7:5b:1f:3b:4b:77:dc:11:a2:6a:eb:81:
                    fb:8e:21:3a:da:67:e3:b3:1f:36:fb:14:24:05:e4:
                    03:20:4b:b1:c7:7b:a3:52:fb:8d:af:60:2c:b2:ce:
                    81:91:0c:3d:36:b0:29:5d:82:28:48:f5:29:2d:a0:
                    71:ff:d6:0b:8f:ed:d6:d0:0a:36:6b:53:7f:7a:38:
                    e1:e7:a5:f4:c3:ba:3d:55:50:d6:4f:73:75:0d:54:
                    41:5f:4b:b8:65:0c:a8:30:e3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                Easy-RSA Generated Server Certificate
            X509v3 Subject Key Identifier:
                BE:4D:3F:08:D5:1B:13:31:6B:B9:4A:76:9B:91:79:40:6D:31:52:55
            X509v3 Authority Key Identifier:
                keyid:C4:7D:1B:65:CF:94:97:1B:F8:5A:77:9A:AA:9A:C4:3C:80:55:C1:14
                  DirName:/C=ES/ST=Madrid/L=Fuenlabrada/O=Saul/OU=IT/CN=pc1/name=Saul/email
Address=mail@host.domain
                serial:ED:D7:E9:35:C0:2A:AA:A4

            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
    Signature Algorithm: sha1WithRSAEncryption
        5a:f2:df:f7:88:b9:da:f3:65:10:de:f0:24:51:e1:b9:b3:1b:
        d2:86:a5:64:0e:34:6c:59:53:1d:0c:e0:93:15:ee:76:88:ee:
        2a:c1:30:6c:64:69:be:ab:3b:63:eb:66:d0:23:9c:f6:13:35:
        18:3e:14:84:1f:f7:96:45:62:eb:d1:45:84:b5:57:43:15:05:
        32:02:1b:b5:a5:e3:f2:59:bf:f8:17:03:ee:6c:77:97:af:85:
        fd:4e:d0:21:a4:8a:64:16:2d:55:92:57:88:17:d8:7a:3c:37:
        ae:ff:7e:3d:16:b4:10:c3:0d:4a:e6:b5:b0:66:95:20:63:a6:
        30:d6
-----BEGIN CERTIFICATE-----
MIID9DCCA12gAwIBAgIBATANBgkqhkiG9w0BAQUFADCBjjELMAkGA1UEBhMCRVMxDz
ANBgNVBAgTBk1hZHJpZDEUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFN
hdWwxCzAJBgNVBAsTAklUMQwwCgYDVQQDEwNwYzExDTALBgNVBCkTBFNhdWwxHz
AdBgkqhkiG9w0BCQEWEG1haWxAaG9zdC5kb21haW4wHhcNMTcwNDA2MTU0MzMxWhc
NMjcwNDA0MTU0MzMxWjCBjTELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1hZHJpZD
```

EUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFNhdWwxCzAJBgNVBAsTAkl
UMQswCQYDVQQDEwJyNDENMAsGA1UEKRMEU2F1bDEfMB0GCSqGSIb3DQEJARYQb
WFpbEBob3N0LmRvbWFpbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuSi4yQtPC
JgB7vNJWmIwY6cWM27UeUkqGGLBTu8jza6nWx87S3fcEaJq64H7jiE62mfjsx82+xQkBeQDIE
uxx3ujUvuNr2Asss6BkQw9NrApXYIoSPUpLaBx/9YLj+3W0Ao2a1N/ejjh56X0w7o9VVDWT3N
1DVRBX0u4ZQyoMOMCAwEAAaOCAV8wggFbMAkGA1UdEwQCMAAwEQYJYIZIAYb4Qg
EBBAQDAgZAMDQGCWCGSAGG+EIBDQQnFiVFYXN5LVJTQSBHZW5lcmF0ZWQgU2Vy
dmVyIENlcnRpZmljYXRlMB0GA1UdDgQWBBS+TT8I1RsTMWu5SnabkXlAbTFSVTCBwwY
DVR0jBIG7MIG4gBTEfRtlz5SXG/had5qqmsQ8gFXBFKGBlKSBkTCBjjELMAkGA1UEBhMC
RVMxDzANBgNVBAgTBk1hZHJpZDEUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNV
BAoTBFNhdWwxCzAJBgNVBAsTAklUMQwwCgYDVQQDEwNwYzExDTALBgNVBCkTBF
NhdWwxHzAdBgkqhkiG9w0BCQEWEG1haWxAaG9zdC5kb21haW6CCQDt1+k1wCqqpDATBg
NVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBaAwDQYJKoZIhvcNAQEFBQADg
YEAWvLf94i52vNlEN7wJFHhubMb0oalZA40bFlTHQzgkxXudojuKsEwbGRpvqs7Y+tm0COc9h
M1GD4UhB/3lkVi69FFhLVXQxUFMgIbtaXj8lm/
+BcD7mx3l6+F/U7QIaSKZBYtVZJXiBfYejw3rv9+PRa0EMMNSua1sGaVIGOmMNY=
-----END CERTIFICATE-----

R1:

root@r1:/etc/openvpn# openssl x509 -in r1.crt -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
  Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT, CN=pc1/name=Saul/emailAddress=mail@host.domain
    Validity
      Not Before: Apr 6 15:54:02 2017 GMT
      Not After : Apr 4 15:54:02 2027 GMT
        Subject: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT, CN=r1/name=Saul/emailAddress=mail@host.domain
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (1024 bit)
        Modulus:
          00:cc:5b:57:af:e9:11:e8:81:49:a8:e3:1f:8f:89:
          46:02:b8:6f:6b:c7:81:2d:0e:e9:82:08:ec:02:72:
          0b:23:8e:0c:78:02:a7:76:9f:50:4c:b5:4d:db:da:
          23:b5:8a:48:4c:6b:c4:92:ed:16:d6:9d:8c:0f:a5:
          0b:52:e4:6e:7e:4f:47:da:23:f2:2c:b0:75:d8:71:
          44:96:f2:e9:e5:d4:4a:ac:cb:41:79:1c:2a:db:3b:
          51:4f:d1:9e:d2:89:2c:1a:01:99:fd:11:12:e6:84:
          fe:a1:85:21:d0:b4:6b:11:48:ff:4d:41:14:db:55:
          17:aa:20:bf:97:1d:ff:89:e3
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE

```
        Netscape Comment:
            Easy-RSA Generated Certificate
        X509v3 Subject Key Identifier:
            8A:4F:33:97:2A:08:3F:E5:78:65:DE:DA:97:87:77:D6:C8:C9:BB:24
        X509v3 Authority Key Identifier:
            keyid:C4:7D:1B:65:CF:94:97:1B:F8:5A:77:9A:AA:9A:C4:3C:80:55:C1:14
              DirName:/C=ES/ST=Madrid/L=Fuenlabrada/O=Saul/OU=IT/CN=pc1/name=Saul/email
Address=mail@host.domain
            serial:ED:D7:E9:35:C0:2A:AA:A4

        X509v3 Extended Key Usage:
            TLS Web Client Authentication
        X509v3 Key Usage:
            Digital Signature
    Signature Algorithm: sha1WithRSAEncryption
        7d:14:fc:aa:21:6f:54:6e:79:0d:ed:df:86:30:04:d3:ec:f6:
        d8:aa:db:f6:cf:65:56:bd:2a:60:eb:d8:5e:2f:00:bd:3a:c7:
        78:61:98:8e:26:4c:1e:ba:e7:f0:ce:20:84:21:81:9c:87:2a:
        3b:a1:1d:6c:ef:89:c9:65:b8:f8:6a:09:6e:c5:16:85:4d:b2:
        c3:cb:b5:57:ec:b2:bb:6e:db:19:7a:a0:8b:1d:65:c5:e8:66:
        59:69:5d:6a:3e:2c:c9:69:5d:03:cc:85:1d:bb:70:32:f1:d5:
        0b:da:0c:8f:f3:35:9c:1e:ad:81:8f:51:53:ed:07:35:41:53:
        73:40
-----BEGIN CERTIFICATE-----
MIID2jCCA0OgAwIBAgIBAjANBgkqhkiG9w0BAQUFADCBjjELMAkGA1UEBhMCRVMxDz
ANBgNVBAgTBk1hZHJpZDEUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFN
hdWwxCzAJBgNVBAsTAklUMQwwCgYDVQQDEwNwYzExDTALBgNVBCkTBFNhdWwxHz
AdBgkqhkiG9w0BCQEWEG1haWxAaG9zdC5kb21haW4wHhcNMTcwNDA2MTU1NDAyWhcN
MjcwNDA0MTU1NDAyWjCBjTELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1hZHJpZDE
UMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFNhdWwxCzAJBgNVBAsTAklU
MQswCQYDVQQDEwJyMTENMAsGA1UEKRMEU2F1bDEfMB0GCSqGSIb3DQEJARYQbW
FpbEBob3N0LmRvbWFpbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzFtXr+kR6IF
JqOMfj4lGArhva8eBLQ7pggjsAnILI44MeAKndp9QTLVN29ojtYpITGvEku0W1p2MD6ULUuRu
fk9H2iPyLLB12HFElvLp5dRKrMtBeRwq2ztRT9Ge0oksGgGZ/RES5oT+oYUh0LRrEUj/TUEU2
1UXqiC/lx3/ieMCAwEAAaOCAUUwggFBMAkGA1UdEwQCMAAwLQYJYIZIAYb4QgENBCA
WHkVhc3ktUlNBIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUik8zlyoIP+V4Z
d7al4d31sjJuyQwgcMGA1UdIwSBuzCBuIAUxH0bZc+Ulxv4WneaqprEPIBVwRShgZSkgZEwg
Y4xCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZNYWRyaWQxFDASBgNVBAcTC0Z1ZW5
sYWJyYWRhMQ0wCwYDVQQKEwRTYXVsMQswCQYDVQQLEwJJVDEMMAoGA1UEAx
MDcGMxMQ0wCwYDVQQpEwRTYXVsMR8wHQYJKoZIhvcNAQkBFhBtYWlsQGhvc3QuZ
G9tYWluggkA7dfpNcAqqqQwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCwYDVR0PBAQDAg
eAMA0GCSqGSIb3DQEBBQUAA4GBAH0U/Kohb1RueQ3t34YwBNPs9tiq2/bPZVa9KmDr2F4
vAL06x3hhmI4mTB665/DOIIQhgZyHKjuhHWzviclluPhqCW7FFoVNssPLtVfssrtu2xl6oIsdZcXo
ZllpXWo+LMlpXQPMhR27cDLx1QvaDI/zNZwerYGPUVPtBzVBU3NA
-----END CERTIFICATE-----
```

PC3:

```
root@pc3:/etc/openvpn# openssl x509 -in pc3.crt -text
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
    Signature Algorithm: sha1WithRSAEncryption
                                Issuer: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT,
CN=pc1/name=Saul/emailAddress=mail@host.domain
        Validity
          Not Before: Apr  6 16:01:33 2017 GMT
          Not After : Apr  4 16:01:33 2027 GMT
                                Subject: C=ES, ST=Madrid, L=Fuenlabrada, O=Saul, OU=IT,
CN=pc3/name=Saul/emailAddress=mail@host.domain
        Subject Public Key Info:
          Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
              00:b2:65:fe:08:47:db:bb:ad:ac:7a:87:31:52:7b:
              fd:7b:bc:4b:75:fb:80:84:52:fc:2a:1f:20:4a:f3:
              9e:d2:ab:03:58:de:61:1f:8b:28:d2:d2:d6:6b:4e:
              0d:e4:6f:ed:6b:e1:41:6c:d0:65:df:37:51:c6:ba:
              90:52:f4:46:ba:31:94:3f:8b:8c:2d:b3:52:d4:44:
              50:bc:01:1b:86:71:7e:5b:eb:58:93:ce:d6:bc:61:
              ae:c5:c3:a3:f5:a3:6a:60:07:55:bf:e2:c6:a3:7e:
              b8:a9:95:00:53:6b:a7:0f:0e:fd:5b:98:96:b3:39:
              a6:89:40:ec:fb:5a:aa:7a:31
            Exponent: 65537 (0x10001)
        X509v3 extensions:
          X509v3 Basic Constraints:
            CA:FALSE
          Netscape Comment:
            Easy-RSA Generated Certificate
          X509v3 Subject Key Identifier:
            9C:32:49:5B:E6:57:17:3B:3A:C4:9B:ED:8B:78:D4:83:36:90:AF:44
          X509v3 Authority Key Identifier:
            keyid:C4:7D:1B:65:CF:94:97:1B:F8:5A:77:9A:AA:9A:C4:3C:80:55:C1:14
              DirName:/C=ES/ST=Madrid/L=Fuenlabrada/O=Saul/OU=IT/CN=pc1/name=Saul/email
Address=mail@host.domain
            serial:ED:D7:E9:35:C0:2A:AA:A4

          X509v3 Extended Key Usage:
            TLS Web Client Authentication
          X509v3 Key Usage:
            Digital Signature
    Signature Algorithm: sha1WithRSAEncryption
         36:73:6b:47:be:8e:d9:5b:c6:81:76:e0:4d:cc:d1:b0:9d:8a:
         87:0a:ca:92:38:ba:29:63:e3:85:8f:05:6d:e4:f3:5a:6b:16:
         ed:c8:a5:24:8d:ef:e7:f6:d3:3f:4c:50:29:8e:53:8d:36:95:
         cf:a3:c0:59:9b:a5:fa:f8:3c:05:5d:39:78:4e:6c:6a:4f:b3:
         d4:de:7f:01:b3:c4:4e:b6:b3:12:60:0a:21:92:d3:ca:35:ff:
         f8:94:07:e5:d2:0a:01:47:1d:7f:a6:c1:cb:f7:59:2d:3e:4f:
         1a:5d:e5:d9:21:3a:c0:dd:c8:c9:ae:5e:55:a9:70:c1:4e:e6:
         79:e1
```

-----BEGIN CERTIFICATE-----
MIID2zCCA0SgAwIBAgIBAzANBgkqhkiG9w0BAQUFADCBjjELMAkGA1UEBhMCRVMxDz
ANBgNVBAgTBk1hZHJpZDEUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFN
hdWwxCzAJBgNVBAsTAklUMQwwCgYDVQQDEwNwYzExDTALBgNVBCkTBFNhdWwxHz
AdBgkqhkiG9w0BCQEWEG1haWxAaG9zdC5kb21haW4wHhcNMTcwNDA2MTYwMTMzWhc
NMjcwNDA0MTYwMTMzWjCBjjELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1hZHJpZD
EUMBIGA1UEBxMLRnVlbmxhYnJhZGExDTALBgNVBAoTBFNhdWwxCzAJBgNVBAsTAkl
UMQwwCgYDVQQDEwNwYzMxDTALBgNVBCkTBFNhdWwxHzAdBgkqhkiG9w0BCQEWE
G1haWxAaG9zdC5kb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALJl/ghH2
7utrHqHMVJ7/Xu8S3X7gIRS/CofIErzntKrA1jeYR+LKNLS1mtODeRv7WvhQWzQZd83Uca6kF
L0RroxlD+LjC2zUtREULwBG4ZxflvrWJPO1rxhrsXDo/WjamAHVb/ixqN+uKmVAFNrpw8O/Vu
YlrM5polA7PtaqnoxAgMBAAGjggFFMIIBQTAJBgNVHRMEAjAAMC0GCWCGSAGG+EIBD
QQgFh5FYXN5LVJTQSBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFJwyS
VvmVxc7OsSb7Yt41IM2kK9EMIHDBgNVHSMEgbswgbiAFMR9G2XPlJcb+Fp3mqqaxDyAVc
EUoYGUpIGRMIGOMQswCQYDVQQGEwJFUzEPMA0GA1UECBMGTWFkcmlkMRQwEgY
DVQQHEwtGdWVubGFicmFkYTENMAsGA1UEChMEU2F1bDELMAkGA1UECxMCSVQxD
DAKBgNVBAMTA3BjMTENMAsGA1UEKRMEU2F1bDEfMB0GCSqGSIb3DQEJARYQbWFp
bEBob3N0LmRvbWFpboIJAO3X6TXAKqqkMBMGA1UdJQQMMAoGCCsGAQUFBwMCMAs
GA1UdDwQEAwIHgDANBgkqhkiG9w0BAQUFAAOBgQA2c2tHvo7ZW8aBduBNzNGwnYqHC
sqSOLopY+OFjwVt5PNaaxbtyKUkje/n9tM/TFApjlONNpXPo8BZm6X6+DwFXTl4TmxqT7PU3
n8Bs8ROtrMSYAohktPKNf/4lAfl0goBRx1/psHL91ktPk8aXeXZITrA3cjJrl5VqXDBTuZ54Q==
-----END CERTIFICATE-----

2.1.3. Observa los números de serie de los certificados y explícalos.

El número de serie de pc1 es el más diferente ya que creó el primer certificado de CA y parámetros DH. Los números de serie de r4, r1, pc3, van en orden según se han ido creando sus certificados.

2.2. Configuración del extremo servidor r4

Se copia el fichero de ejemplo en /etc/openvpn y lo descomprimimos.

```
root@r4:/etc/openvpn# cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz .
root@r4:/etc/openvpn# gzip -d server.conf.gz
root@r4:/etc/openvpn# vim server.conf
port 1194
proto udp
dev tun
ca ca.crt
cert r4.crt
key r4.key
dh dh1024.pem
server 10.10.8.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log /var/log/openvpn.log
verb 5
```

2.3. Configuración del extremo cliente r1

root@r1:/etc/openvpn# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf .

client
dev tun
proto udp
remote 100.10.4.4 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert r1.crt
key r1.key
ns-cert-type server
comp-lzo
verb 5

2.4. Configuración del extremo cliente pc3

root@pc3:/etc/openvpn# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf .

client
dev tun
proto udp
remote 100.10.4.4 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert pc3.crt
key pc3.key
ns-cert-type server
comp-lzo
verb 5

2.5. Túnel entre pc3 y r4

R4:

```
root@r4:~# mkdir /dev/net
root@r4:~# mknod /dev/net/tun c 10 200
root@r4:~# tcpdump -i eth0 -s 0 -w /hosthome/openvpn-01.cap &
[1] 2660
root@r4:~# tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

root@r4:~# /etc/init.d/openvpn start
[ ok ] Starting virtual private network daemon: server.
root@r4:~# /etc/init.d/openvpn stop
[ ok ] Stopping virtual private network daemon: server.
root@r4:~# fg
tcpdump -i eth0 -s 0 -w /hosthome/openvpn-01.cap
^C184 packets captured
184 packets received by filter
0 packets dropped by kernel
```

PC3:

```
root@pc3:~# ping 100.10.4.4
PING 100.10.4.4 (100.10.4.4) 56(84) bytes of data.
64 bytes from 100.10.4.4: icmp_req=1 ttl=62 time=1.34 ms
64 bytes from 100.10.4.4: icmp_req=2 ttl=62 time=1.30 ms
64 bytes from 100.10.4.4: icmp_req=3 ttl=62 time=0.933 ms
^C
--- 100.10.4.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 0.933/1.194/1.346/0.187 ms
root@pc3:~# /etc/init.d/openvpn start
[ ok ] Starting virtual private network daemon: client.
root@pc3:~# ping -c 3 10.10.8.1
PING 10.10.8.1 (10.10.8.1) 56(84) bytes of data.
64 bytes from 10.10.8.1: icmp_req=1 ttl=64 time=3.05 ms
64 bytes from 10.10.8.1: icmp_req=2 ttl=64 time=2.84 ms
64 bytes from 10.10.8.1: icmp_req=3 ttl=64 time=2.64 ms

--- 10.10.8.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.647/2.849/3.054/0.177 ms
root@pc3:~# /etc/init.d/openvpn stop
[ ok ] Stopping virtual private network daemon: client.
```

2.5.1. ¿Qué dirección IP destino has especificado en el ping para enviar los paquetes desde pc3 a r4 utilizando el túnel y sin utilizar el túnel? ¿Por qué?

Sin utilizar el túnel, la ip destino era la de r4, 100.10.4.4, ya que es la dirección IP asignada por eth0 en r4.
Sin embargo, para usar la del túnel, se ha usado la de 10.10.8.1, ya que es la dirección IP que usa openVPN para el servidor.

2.5.2. Indica qué direcciones IP se han asignado al dispositivo tun0 en r4 y por qué.

El servidor de openVPN ya tenía asigada una dirección IP. En este caso 10.10.8.1.
También podemos visualizar (en el túnel abierto) la IP del túnel, realizando un ifconfig sobre la máquina.

2.5.3. Indica qué direcciones IP se han asignado al dispositivo tun0 en pc3 y por qué.

OpenVPN asigna prefijos 10.10.8.X/30 para cada cliente que se conecta al servidor. En este caso, pc3 tiene la IP: 10.10.8.6.

*Asigna esos prefijos porque así se lo hemos indicado en la configuración de los apartados anteriores.

2.5.4. Explica la tabla de encaminamiento de pc3.

root@pc3:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r5	0.0.0.0	UG	0	0	0	eth0
10.10.8.1	10.10.8.5	255.255.255.255	UGH	0	0	0	tun0
10.10.8.5	*	255.255.255.255	UH	0	0	0	tun0
100.10.7.0	*	255.255.255.0	U	0	0	0	eth0

root@pc3:~# /etc/init.d/openvpn stop
[ok] Stopping virtual private network daemon: client.
root@pc3:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r5	0.0.0.0	UG	0	0	0	eth0
100.10.7.0	*	255.255.255.0	U	0	0	0	eth0

Se puede observar, como cuando el túnel esta abierto, se crea una ruta hacia la dirección 10.10.8.1 a través de 10.10.8.5.

2.5.5. Explica la tabla de encaminamiento de r4.

root@r4:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r3	0.0.0.0	UG	0	0	0	eth0
10.10.2.0	*	255.255.255.0	U	0	0	0	eth1

10.10.8.0	10.10.8.2	255.255.255.0	UG	0	0	0	tun0
10.10.8.2	*	255.255.255.255	UH	0	0	0	tun0
100.10.4.0	*	255.255.255.0	U	0	0	0	eth0

root@r4:~# /etc/init.d/openvpn stop
[ok] Stopping virtual private network daemon: server.
root@r4:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r3	0.0.0.0	UG	0	0	0	eth0
10.10.2.0	*	255.255.255.0	U	0	0	0	eth1
100.10.4.0	*	255.255.255.0	U	0	0	0	eth0

Se puede observar, como cuando el túnel esta abierto, se crea una ruta hacia la dirección 10.10.8.0 a través de 10.10.8.2.

2.5.6. ¿Qué ocurre si se realiza un ping desde pc3 a cada una de las direcciones que muestra tun0 en r1? ¿Por qué?

root@r1:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r2	0.0.0.0	UG	0	0	0	eth1
10.10.1.0	*	255.255.255.0	U	0	0	0	eth0
10.10.8.1	10.10.8.9	255.255.255.255	UGH	0	0	0	tun0
10.10.8.9	*	255.255.255.255	UH	0	0	0	tun0
100.10.2.0	*	255.255.255.0	U	0	0	0	eth1

root@pc3:~# ping -c 3 10.10.8.9
PING 10.10.8.9 (10.10.8.9) 56(84) bytes of data.
From 100.10.6.3 icmp_seq=1 Destination Net Unreachable
From 100.10.6.3 icmp_seq=2 Destination Net Unreachable
From 100.10.6.3 icmp_seq=3 Destination Net Unreachable

--- 10.10.8.9 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 1999ms

Todos los paquetes se acaban perdiendo porque no está configurado r4 (servidor) para que se conecte pc3 y r1.

2.5.7. Abre la captura openvpn-01.cap en Wireshark y explica el contenido:

a. Indica el identificador de sesión local y remoto que se establece en los mensajes P_CONTROL_HARD_RESET y fíjate como aparece en todos los mensajes posteriores.

En la primera captura que esta P_CONTROL_HARD_RESET
Session ID = 16760842558817342502

En la segunda captura que esta P_CONTROL_HARD_RESET
Session ID = 12835453267561946142

Remote Session ID = 16760842558817342502

b. Observa el campo Message Packet-ID indica cuál es su valor incial para el cliente y para el servidor. Explica cómo va cambiando en cada uno de los paquetes P_CONTROL que se envían.

Tanto para cliente como para el servidor el valor inicial de cada uno de ellos en el campo Message-Packet-ID es 0, conforme se van viendo más campos, se observa que el valor se va incrementando en 1, tanto en servidor como en cliente.

c. ¿Por qué los mensajes P_ACK no llevan el campo Message Packet-ID?

Porque son mensajes de confirmación.

d. ¿En qué paquete se asiente el mensaje P_CONTROL_HARD_RESET_CLIENT_V2? ¿Cómo lo sabes?

Este mensaje lo asiente el servidor al recibir el mensaje de identificador de sesión del cliente, como el servidor tiene que enviar datos al cliente, aprovecha para incluir en ese mensaje los asentimientos.

Se sabe por el campo Message Packet-ID ArrayElement, en el viaja la cantidad de ACKs que se están enviando en el mensaje y en el campo Packet-ID Array viajan los números de secuencia que se están asintiendo.

e. ¿En qué paquete se asiente el mensaje P_CONTROL_HARD_RESET_SERVER_V2? ¿Cómo lo sabes?

Se asiente en el siguiente mensaje ACK en el cual coincida su Session_ID, que en este caso es en el mensaje número 17.

f. El primer mensaje que envía el cliente al servidor del SSL/TLS handshake es Client Hello. ¿Alguno de los campos viaja cifrado?

El mensaje que le manda el cliente no hay ninguno cifrado, ya que es el servidor el que elige en que tipo de cifrado se va a usar. El cliente manda las preferencias de cifrado según el orden de preferencia.

g. Localiza el primer mensaje que envía el servidor al cliente para establecer SSL/TLS handshake, es Server Hello. ¿Alguno de los campos viaja cifrado? Indica si contiene certificados y cuáles contiene. Localiza los parámetros Diffie-Hellman e indica la longitud de p y el valor de g. Fíjate como el servidor le envía un valor PubKey del servidor para crear el secreto compartido. Indica el algoritmo de cifrado que ha elegido el servidor.

El mensaje esta ubicado en la posición 66.
El servidor ha elegido como va a cifrar los campos, que en este caso va a ser:

Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)

Diffie-Hellman:

p Length: 128

p: 94e24a48b5a337a470c89727e63ec5f75c98482073eab206...
g Length: 1
g: 02

Uno de los certificados lleva el serial number 1, por lo que deducimos de la tabla sacada en el ejercicio 1, que lleva el certificado de r4.crt, luego hay otro serialNumber: -1308320749661279580, que será el número en decimal, en la tabla sacada anteriormente, había un número en hexadecimal, por lo que se habrá convertido a decimal, asique lleva también en certificado de ca.crt

Pubkey: 4fbb80b67d23c84d5ed3ad53a85eacb6d30497bfd1237fe7…

h. Localiza el siguiente mensaje que envía el cliente al servidor Certificate, Client key Exchange ....¿Alguno de los campos viaja cifrado? Indica si contiene certificados y cuáles contiene. Fíjate como el cliente le envía al servidor el valor PubKey del cliente.

Certificate: 308203db30820344a003020102020103300d06092a864886...
algorithmIdentifier (sha1WithRSAEncryption)
encrypted: 36736b47be8ed95bc68176e04dccd1b09d8a870aca9238ba…
Certificate: 30820393308202fca003020102020900edd7e935c02aaaa4...
algorithmIdentifier (sha1WithRSAEncryption)
encrypted: 4665efb8a490670101d1249f68c61fc74dcc5a4f37c83d6f...

Handshake Type: Client Key Exchange (16)
Diffie-Hellman Client Params
Pubkey Length: 128
Pubkey: 4a9ed858ee94c833cd368ad69936bb7239e85a16ad987f9c…

i. Localiza el siguiente mensaje que envía el servidor al cliente New session ticket .... ¿Alguno de los campos viaja cifrado?

El mensaje new session ticket se encuentra en la línea 136 de la captura, con el protocolo TLSv1

TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message.

j. Observa el contenido de los mensajes P_DATA. ¿Por qué no llevan el campo Message Packet-ID?

El message packet id es el identificador de paquete que solo lo llevan los mensajes de control, en P_DATA los mensajes van cifrados

k. ¿Qué crees que hay dentro de los mensajes P_DATA?

Los datos cifrados que envían el cliente y servidor a través del túnel.

2.6. Conectividad entre entre pc3 y pc2

2.6.1. ¿Qué crees que ocurrirá si desde pc3 se envía un ping a pc2?

No se conectará, ya que pc2 se encuentra dentro de una red privada.

2.6.2. Modifica la configuración de r4 para que el ping de pc3 a pc2 vaya a través del túnel OpenVPN. Explica en la memoria qué has modificado.

Para permitir que las subredes internas de un cliente sean alcanzables desde otro cliente a través del servidor openVPN es necesario definir en el fichero /etc/openvpn/server.conf

push “route 10.10.2.0 255.255.255.0”

2.6.3. Realiza una captura en r4(eth0) (fichero openvpn-02.cap) y en pc2 (fichero openvpn-03.cap) mientras ejecutas el ping y explica las capturas.

Primero se abre el túnel en r4 y en pc3

root@pc3:~# ping -c 3 10.10.2.20
PING 10.10.2.20 (10.10.2.20) 56(84) bytes of data.
64 bytes from 10.10.2.20: icmp_req=1 ttl=63 time=1.50 ms
64 bytes from 10.10.2.20: icmp_req=2 ttl=63 time=1.36 ms
64 bytes from 10.10.2.20: icmp_req=3 ttl=63 time=2.48 ms

--- 10.10.2.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 1.362/1.784/2.484/0.499 ms

Observamos que ahora si se puede comunicar pc3 y pc2

En la captura 2, se puede observar como el ping realizado por pc3 llega hasta la dirección 100.10.4.4 con el protocolo de VPN y con los data v1, que son los datos cifrados en el túnel.

En la captura 3, dice que la dirección desde la que se mando el ping es 10.10.8.6, que es una de las ip que se utiliza en el túnel.

2.6.4. Explica la tabla de encaminamiento que tiene pc3 y las diferencias con la tabla de encaminamiento que viste en el apartado anterior.

(tabla de encaminamiento del ejercicio anterior)
root@pc3:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r5	0.0.0.0	UG	0	0	0	eth0
10.10.8.1	10.10.8.5	255.255.255.255	UGH	0	0	0	tun0
10.10.8.5	*	255.255.255.255	UH	0	0	0	tun0
100.10.7.0	*	255.255.255.0	U	0	0	0	eth0

(tabla de encaminamiento de este ejercicio)
root@pc3:~# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r5	0.0.0.0	UG	0	0	0	eth0
10.10.2.0	10.10.8.5	255.255.255.0	UG	0	0	0	tun0
10.10.8.1	10.10.8.5	255.255.255.255	UGH	0	0	0	tun0
10.10.8.5	*	255.255.255.255	UH	0	0	0	tun0
100.10.7.0	*	255.255.255.0	U	0	0	0	eth0

Se observa que se ha añadido una nueva ruta a la subred 10.10.2.0, ahora pc3 puede acceder a la red privada a partir de un túnel.

2.6.5. ¿Crees que pc2 sabe que se está usando un túnel openVPN? ¿Por qué?

No, en la captura se observa que no hay mensajes de openVPN.

2.7. Túnel entre r1 y r4

1. ¿Qué crees que ocurrirá si desde r1 se envía un ping a pc2?

En este caso el ping conectara con pc2, ya que r4 está configurado para que tenga conectividad con la subred 10.10.2.0 del apartado anterior, a través del túnel de openVPN.

2. Explica la tabla de encaminamiento que tiene pc3 y las diferencias con la tabla de encaminamiento que viste en el apartado anterior.

Pc3 no ha sufrido ningún cambio en este ejercicio, por lo que su tabla de encaminamiento es igual a la del ejercicio anterior.

3. ¿Qué crees que ocurrirá si desde pc1 se envía un ping a pc2? ¿Por qué?

El servidor no esta configurado para que pueda entrar a la red privada a la que pertenece pc1, aunque r1 sea un cliente, por lo que el ping no llegará a su destino.

4. Modifica la configuración en r4 para permitir que r4 alcance las direcciones IP de la Subred1. Indica las modificaciones en la memoria. Comprueba que ahora funciona. No olvides guardar el fichero de configuración que has modificado en la máquina virtual.

El servidor(r4) debe incluir en su fichero server.conf:

```
client-config-dir ccd
route 10.10.1.0 255.255.255.0
```

El servidor debe crear la carpeta /etc/openvpn/ccd y añadir un fichero con el nombre del cliente (r1). El contenido del fichero debe ser el siguiente para que openVPN encamine el tráfico a dicha subred a través del cliente r1:

```
iroute 10.10.1.0 255.255.255.0
```

```
root@pc1:~# ping 10.10.2.20
PING 10.10.2.20 (10.10.2.20) 56(84) bytes of data.
64 bytes from 10.10.2.20: icmp_req=1 ttl=62 time=3.22 ms
64 bytes from 10.10.2.20: icmp_req=2 ttl=62 time=2.30 ms
64 bytes from 10.10.2.20: icmp_req=3 ttl=62 time=2.66 ms
^C
--- 10.10.2.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 2.303/2.729/3.222/0.378 ms
```

2.8. Conectividad entre entre pc3 y pc1

2.8.1. ¿Qué crees que ocurrirá si desde pc3 se envía un ping a pc1? ¿Por qué?

No llegarán los mensajes porque el servidor no tiene conexión para que pc3 acceda a la red privada 1.

2.8.2. Modifica la configuración en r4 para permitir que r4 anuncie las subredes internas del cliente r1 (Subred1) al cliente pc3. No olvides guardar el fichero que has modificado en la máquina virtual.

Para permitir que las subredes internas de un cliente sean alcanzables desde otro cliente a través del servidor openVPN es necesario definir en el fichero /etc/openvpn/server.conf

client-to-client
push "route 10.10.1.0 255.255.255.0"

(como el servidor y los clientes estaban arrancados, para que la configuración funcione, se debe apagar y volver a encender el túnel).

2.8.3. Realiza una captura de tráfico (openvlan-05.cap) en r4(eth0) que muestre que funciona un ping desde pc3 a pc1. Explica los paquetes capturados.

En la captura se observa que se ha utilizado el protocolo de OpenVPN, la captura empieza en cliente pc3 enviando la solicitud al servidor r4, y este le envía la petición al otro cliente, r1.
Después se puede ver como el cliente r1 responde a la petición de r4, y r4 le envía la respuesta a pc3.

2.8.4. Explica la tabla de encaminamiento que tienen pc3 y r1 y las diferencias con la tablas de encaminamiento que tenían previamente.

root@pc3:/etc/openvpn# route
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	r5	0.0.0.0	UG	0	0	0	eth0
10.10.1.0	10.10.8.5	255.255.255.0	UG	0	0	0	tun0
10.10.2.0	10.10.8.5	255.255.255.0	UG	0	0	0	tun0
10.10.8.0	10.10.8.5	255.255.255.0	UG	0	0	0	tun0
10.10.8.5	*	255.255.255.255	UH	0	0	0	tun0
100.10.7.0	*	255.255.255.0	U	0	0	0	eth0

Se ha añadido una nueva subred a la que tiene acceso el cliente pc3 a través del túnel, la 10.10.1.10

La tabla de encaminamiento de r1 no se ha modificado en relación a la que tenía anteriormente.