

TRABAJO PRÁCTICO N° 1

EJERCICIO N° 1

Teniendo en cuenta que una empresa tiene 5 sucursales distribuidas de la siguiente manera:

- SUCURSAL 1 (SAN RAFAEL): 14 HOST.
- SUCURSAL 2 (MENDOZA): 30 HOST.
- SUCURSAL 3 (BUENOS AIRES): 22 HOST.
- SUCURSAL 4 (CORDOBA): 31 HOST.
- SUCURSAL 5 (SANTA FE): 8 HOST.

RESOLVER LO SIGUIENTE:

- 1) Realizar el direccionamiento utilizando una red /24 para cada una de las sucursales.
- 2) Realizar el direccionamiento óptimo utilizando solo una red /24.
- 3) Llenar las siguientes tablas para cada uno de los casos anteriores y analizar los resultados.

Sucursal	Dirección de Red	Mascara de Subred	Dirección de Broadcast	Rango de IP	Nº host totales	Nº host usados	Nº host libres
1	192.168.1.0	255.255.255.0	192.168.1.255	192.168.1.1 a 192.168.1.254	254	14	240
2	192.168.2.0	255.255.255.0	192.168.2.255	192.168.2.1 a 192.168.2.254	254	30	224
3	192.168.3.0	255.255.255.0	192.168.3.255	192.168.3.1 a 192.168.3.254	254	22	232
4	192.168.4.0	255.255.255.0	192.168.4.255	192.168.4.1 a 192.168.4.254	254	31	223
5	192.168.5.0	255.255.255.0	192.168.5.255	192.168.5.1 a 192.168.5.254	254	8	246

Sucursal	Dirección de Red	Mascara de Subred	Dirección de Broadcast	Rango de IP	Nº host totales	Nº host usados	Nº host libres
1	192.168.1.0	255.255.255.192	192.168.1.63	192.168.1.1 a 192.168.1.62	62	31	31
2	192.168.1.64	255.255.255.224	192.168.1.95	192.168.1.65 a 192.168.1.94	30	30	0
3	192.168.1.96	255.255.255.224	192.168.1.127	192.168.1.97 a 192.168.1.126	30	22	8
4	192.168.1.128	255.255.255.240	192.168.1.143	192.168.1.129 a 192.168.1.142	14	14	0
5	192.168.1.144	255.255.255.240	192.168.1.169	192.168.1.145 a 192.168.1.168	14	8	6

EJERCICIO N° 2

Indicar si las siguientes direcciones IP son de host, red o broadcast.

Por qué?

- a. 192.168.1.16/29 RED

11000000.10101000.00000001.00010000 = Dir. IP

11111111.11111111.11111111.11111000 = Masc. de red

10000000.10101000.00000001.00010000 = Resultado

- b. 10.59.58.255/23 HOST

00001010.00111011.00111010 .11111111 = Dir. IP

11111111.11111111.11111110.00000000 = Masc. de red

00001010.00111011.00111011.00000000 = Resultado

- c. 126.255.255.255/16 BROADCAST

01111110.11111111.11111111.11111111 = Dir. IP

11111111.11111111.00000000.00000000 = Masc. de red

01111110.11111111.00000000.00000000 = Resultado

- d. 172.16.0.1/16 HOST

10101100.00010000.00000000.00000001 = Dir. IP

11111111.11111111.00000000.00000000 = Masc. de red
10101100.00010000.00000000.00000000 = Resultado

e. 192.168.1.18/29 HOST
11000000.10101000.00000001.00010010 = Dir. IP
11111111.11111111.11111111.11111000 = Masc. de red
11000000.10101000.00000001.00010000 = Resultado

f. 150.32.248.0/18 HOST
10010110.00100000.11111000.00000000 = Dir. IP
11111111.11111111.11000000.00000000 = Masc. de red
10010110.00100000.11000000.00000000 = Resultado

EJERCICIO N° 3

Para las siguientes redes indicar cuales con las primeras 5 direcciones IP disponibles para hosts y las últimas 5 direcciones IP disponibles para hosts:

a. 159.22.21.0/26
Primeras 5 direcciones:

159.22.21.1
159.22.21.2
159.22.21.3
159.22.21.4
159.22.21.5

Ultimas 5 direcciones:
159.22.21.58
159.22.21.59
159.22.21.60
159.22.21.61
159.22.21.62

b. 52.168.0.0/14
Primeros 5 direcciones:
52.168.0.1

52.168.0.2
52.168.0.3
52.168.0.4
52.168.0.5

Últimas 5 direcciones:

52.171.255.250
52.171.255.251
52.171.255.252
52.171.255.253
52.171.255.254

c. 200.115.66.0/30
2 direcciones disponibles.
200.115.66.1
200.115.66.2

EJERCICIO N° 4

Dada la red 192.168.0.0/24, desarrolle un esquema de direccionamiento que cumpla con los siguientes requerimientos. Optimice el espacio de direccionamiento tanto como sea posible.

1. Una subred de 30 hosts para Profesores
2. Una subred de 90 hosts para Estudiantes
3. Una subred de 20 hosts para Invitados
4. Tres subredes de 2 hosts para enlaces entre enrutadores.

1er Subred (90 host para estudiantes):

Dirección de red: 192.168.0.0

dirección de broadcast: 192.168.0.127

Rango de host: 192.168.0.1 a 192.168.0.126

Host libres: 36

2da Subred (30 hosts para profesores):

dirección de red: 192.168.0.128

dirección de broadcast: 192.168.0.159

Rango de host: 192.168.0.129 a 192.168.0.158

Host libres: 0

3er Subred (20 hosts para invitados):

dirección de red: 192.168.0.160

dirección de broadcast: 192.168.0.191

Rango de host: 192.168.0.161 a 192.168.0.190

Host libres: 10

4ta Subred (enlaces):

Enlace 1(2):

dirección de red: 192.168.0.192/30

dirección de broadcast: 192.168.0.195

Rango de host: 192.168.0.193 a 192.168.0.194

Enlace 2(2):

dirección de red: 192.168.0.196/30

dirección de broadcast: 192.168.0.199

Rango de host: 192.168.0.197 a 192.168.0.198

Enlace 3(2):

dirección de red: 192.168.0.200/30

dirección de broadcast: 192.168.0.203

Rango de host: 192.168.0.201 a 192.168.0.202

EJERCICIO N° 5

En una red Ethernet, un host tiene configurada la dirección IP 150.10.10.12/26. Debe enviar un paquete a la dirección 150.10.10.58/26.

- a. Describa y muestre la operación que debe hacerse para saber si la IP destino pertenece a la misma red.

150.10.10.12/26

Red: 10010110.00001010.00001010.00001100

Máscara: 11111111.11111111.11111111.11000000

10010110.00001010.00001010.00000000

150.10.10.0 dir de red

Rango de host: 150.10.10.0 hasta 150.10.10.62

La dirección 150.10.10.58 está dentro de la misma red.

- b. Realice la misma operación que "a" si ahora la dirección IP destino es 150.10.10.88/26.

150.10.10.88/26

Red: 10010110.00001010.00001010.01011000

Máscara: 11111111.11111111.11111111.11000000

10010110.00001010.00001010.01000000

150.10.10.64 dir de red

150.10.10.127 Dirección de broadcast

La dirección 150.10.10.88 no se encuentra en la misma red

- c. Describa las diferencias.

Básicamente una está dentro del rango de direcciones de red(punto a) y la otra no(punto b).

EJERCICIO N° 6

Dada la siguiente dirección de red: 17.15.0.0/8, dividirla en subredes de las siguientes capacidades:

1. 3 subredes de 1000 hosts
2. 2 subredes 2000 hosts
3. 2 subredes de 5000 host
4. 1 subred de 15000 host
5. 1 subred de 70 hosts
6. 2 subredes de 2 hosts

Dirección de red	Máscara de subred	Dirección de broadcast	Rango de ip	Nº host totales	Nº host usados	Nº host libres
17.15.0.0	255.255.192.0	17.15.63.255	17.15.0.1-17.15.63.254	16.382	15000	1.382
17.15.64.0	255.255.224.0	17.15.95.255	17.15.64.1-17.15.95.254	8.190	5.000	3.190
17.15.96.0	255.255.224.0	17.15.127.255	17.15.96.1-17.15.127.254	8.190	5.000	3.190
17.15.128.0	255.255.248.0	17.15.135.255	17.15.128.1-17.15.135.254	2.046	2.000	46
17.15.136.0	255.255.248.0	17.15.143.255	17.15.136.1-17.15.143.254	2.046	2.000	46
17.15.144.0	255.255.252.0	17.15.147.255	17.15.144.1-17.15.147.254	1.022	1.000	22
17.15.148.0	255.255.252.0	17.15.151.255	17.15.148.1-17.15.151.254	1.022	1.000	22
17.15.152.0	255.255.252.0	17.15.155.255	17.15.152.1-17.15.155.254	1.022	1.000	22
17.15.156.0	255.255.255.128	17.15.156.127	17.15.156.1-17.15.156.126	126	70	56
17.15.156.128	255.255.255.252	17.15.156.131	17.15.156.129-	2	2	0

			17.15.156. 130			
--	--	--	-------------------	--	--	--

EJERCICIO N° 7

Utilizando la herramienta Wireshark, realice una captura de las tramas correspondientes a la realización de un comando ping (IP de la puerta de enlace) desde su computadora, capture un mensaje de echo request y uno de echo reply (mensaje de consulta y respuesta del comando ping). Resuelva:

- a. Marque las distintas capas del modelo TCP/IP.

Request:

```
Frame 95: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: b4:2e:99:e3:40:a5 (b4:2e:99:e3:40:a5), Dst: 60:32:b1:6f:13:3a (60:32:b1:6f:13:3a)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
Internet Control Message Protocol
```

Capa3

Capa2

Reply:

```
Frame 96: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 60:32:b1:6f:13:3a (60:32:b1:6f:13:3a), Dst: b4:2e:99:e3:40:a5 (b4:2e:99:e3:40:a5)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
Internet Control Message Protocol
```

- b. Marque las direcciones MAC e IP origen y destino, el tamaño total de cada trama y el tamaño y contenidos de los datos enviados (campo data).

MAC origen: Source: b4:2e:99:e3:40:a5

Destino: Destination: 60:32:b1:6f:13:3a

IP origen: Source: 192.168.0.104

Destino: Destination: 192.168.0.1

Tamaño total: Frame Length: 74 bytes (592 bits)

Campo data:

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f707172737475767761...

[Length: 32]

60 32 b1 6f 13 3a b4 2e 99 e3 40 a5 08 00 45 00	^2.o.:... .@....E.
00 3c f8 60 00 00 80 01 00 00 c0 a8 00 68 c0 a8	.<`.....h..
00 01 08 00 4c 00 00 01 01 5b 61 62 63 64 65 66L.... .[abcdef
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuvwxyz
77 61 62 63 64 65 66 67 68 69	wabcdefghijklm

EJERCICIO N° 8

Deje el correr el analizador unos 5 minutos, mientras usa distintos accesos a su red (ya sea en forma local o a Internet). Por ejemplo, navegue en Internet, acceda a su correo, acceda a su servidor de archivos, etc.

Analice ahora su captura e informe:

- a. En Statistics – Puntos finales indique cuales son las conversaciones que utilizaron más paquetes.

Address	packets	Bytes	packets A → B	Bytes A → B	packets B → A	Bytes B → A
60:32:b1:6f:13:3a	240 891	252 M	199935	245 M	40956	
b4:2e:99:e3:40:a5	240 350	252 M	41079	6460 k	199271	
ff:ff:ff:ff:ff:ff	492	29 k	0	0	492	
01:00:5e:7f:ff:fa	247	73 k	0	0	247	
01:00:5e:00:00:fb	17	890	0	0	17	
01:00:5e:00:00:fc	14	644	0	0	14	
01:00:5e:00:00:01	14	840	0	0	14	
33:33:00:00:00:fb	3	306	0	0	3	

- b. En Statistics – Conversaciones: indique cual fue el tráfico de mayor cantidad de bytes y entre que direcciones IP.

Address A	Address B	packets	Bytes	packets A → B	Bytes A → B	packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
138.97.176.45	192.168.0.104	124 157	142 M	110313	141 M	13844	1257 k	18.326434000	1683.310742	673 k	
138.97.176.44	192.168.0.104	50 452	57 M	44522	56 M	5930	616 k	18.717778000	1690.238747	269 k	
192.168.0.104	200.115.94.206	11 821	13 M	1642	181 k	10179	12 M	1433.205977000	110.056332	13 k	
142.251.133.69	192.168.0.104	6 405	5394 k	3795	5020 k	2610	373 k	41.350004000	275.245210	145 k	
172.217.173.150	192.168.0.104	5 071	5024 k	4052	4920 k	1019	104 k	17.415496000	1699.848528	23 k	
172.217.172.78	192.168.0.104	5 462	4226 k	3630	3387 k	1832	838 k	9.185855000	1707.983079	15 k	
142.250.79.110	192.168.0.104	3 921	3250 k	2401	2969 k	1520	281 k	32.130542000	1644.299756	14 k	
172.217.172.65	192.168.0.104	1 897	1950 k	1516	1909 k	381	40 k	69.339678000	1452.668403	10 k	
142.251.133.46	192.168.0.104	2 220	1872 k	1653	1717 k	567	155 k	8.776000000	241.312525	56 k	
142.250.79.102	192.168.0.104	1 642	1766 k	1376	1739 k	266	27 k	1029.988456000	120.626340	115 k	

- c. En Statistics – longitud de paquetes: indique los tamaños de paquetes medios. Cuál es el rango de tamaño más utilizado? Esto es bueno o malo, para el rendimiento de la red?

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	241014	1046.83	42	12944	0.1403	100%	9.2100	823.195
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	38608	70.60	42	79	0.0225	16.02%	0.8600	823.195
80-159	7792	96.11	80	159	0.0045	3.23%	0.8300	853.366
160-319	1760	227.77	160	319	0.0010	0.73%	0.2600	94.563
320-639	2075	463.85	320	639	0.0012	0.86%	0.2600	74.860
640-1279	2669	1023.15	640	1279	0.0016	1.11%	2.3600	1159.790
1280-2559	187935	1298.98	1280	2553	0.1094	77.98%	8.3100	823.195
2560-5119	170	3350.22	2615	5019	0.0001	0.07%	0.0600	833.137
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

El rango de tamaños de páquetes más utilizados es de 1280 a 2559, está dentro de un buen nivel de rendimiento ya que transporta bastantes datos de usuario pero sin llegar a sobrecargar la red

EJERCICIO N° 9

Uso del comando Ping:

- Ejecute el comando ping a su puerta de enlace predeterminada. Mostrar el resultado y comentar que significa cada campo de respuesta.

```
C:\Windows\system32>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Muestra la cantidad de datos enviados, tiempo que tarda desde que salió el paquete hasta que volvió y el tiempo de vida del paquete en este caso 64 “saltos” ya que estamos en un sistema Windows.

Luego muestra paquetes enviados recibidos y perdidos, también el tiempo en hacer el recorrido en milisegundos

- Ejecute el comando ping a la dirección IP 8.8.8.8. Mostrar resultado y verificar tiempo de respuesta.

```
C:\Windows\system32>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=109ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=120ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=58ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=51ms TTL=115

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 51ms, Máximo = 120ms, Media = 84ms
```

- c. Investigue para qué sirve el parámetro -l (-s en Linux) con el comando ping y realice una prueba. Escriba sus comentarios.

```
C:\Windows\system32>ping 8.8.8.8 -l 64

Haciendo ping a 8.8.8.8 con 64 bytes de datos:
Respuesta desde 8.8.8.8: bytes=64 tiempo=83ms TTL=115
Respuesta desde 8.8.8.8: bytes=64 tiempo=125ms TTL=115
Respuesta desde 8.8.8.8: bytes=64 tiempo=115ms TTL=115
Respuesta desde 8.8.8.8: bytes=64 tiempo=117ms TTL=115

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 83ms, Máximo = 125ms, Media = 110ms
```

Agregando el parámetro '-l' al comando ping setea el tamaño del búfer de datos a enviar, el tamaño que indique es mayor al por defecto lo cual se visualiza que tarda un poco más al ser más grande el tamaño de datos

- d. Ejecute el comando ping a 8.8.8.8 -i 3 (-t en Linux) . Mostrar el resultado y comentar que significa la respuesta, modifique el parámetro hasta que obtenga una respuesta positiva.

```
C:\Windows\system32>ping 8.8.8.8 -i 3

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 10.10.200.1: TTL expirado en tránsito.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
```

El parámetro '-i' en ping setea el tiempo de vida del paquete

```
C:\Windows\system32>ping 8.8.8.8 -i 9

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=69ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=84ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=100ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=119ms TTL=115

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 69ms, Máximo = 119ms, Media = 93ms
```

Con un mínimo de 9 me arroja una respuesta positiva

EJERCICIO N° 10

Ejecute el comando ping a 8.8.8.8 -n 1 -l 4000.

Si se obtuvo respuesta correcta, inicie el sniffer Wireshark, coloque el filtro ICMP y comience una captura, ejecute nuevamente el comando. Pare la captura e indique:

- a. Determine la cantidad de paquetes IP del envío.
- b. Represente y compare los campos de longitud total, flags y desplazamiento del fragmento para todos los paquetes.
- c. Indique el valor del campo protocolo de la cabecera de los fragmentos IP ¿es el mismo?
- d. Indique que tamaño de mensaje es necesario para generar un fragmento más.
- e. Indique la cantidad de bytes que viajan en cada paquete.

```
C:\Windows\system32>ping 8.8.8.8 -n 1 -l 4000

Haciendo ping a 8.8.8.8 con 4000 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
                (100% perdidos),
```

```

10 5.231079      192.168.0.104      8.8.8.8          ICMP      1082 Echo (ping) request  id=0x0001, seq=433/45313, ttl=128 (no response found!)

Frame 10: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface 0
Ethernet II, Src: b4:2e:99:e3:40:a5 (b4:2e:99:e3:40:a5), Dst: 60:32:b1:6f:13:3a (60:32:b1:6f:13:3a)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1068
    Identification: 0x1ddd (7645)
    > Flags: 0x00
    Fragment offset: 2960
    Time to live: 128
    Protocol: ICMP (1)
    > Header checksum: 0x0000 [validation disabled]
    Source: 192.168.0.104
    Destination: 8.8.8.8
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    > [3 IPv4 Fragments (4008 bytes): #8(1480), #9(1480), #10(1048)]
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf149 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 433 (0x01b1)
    Sequence number (LE): 45313 (0xb101)
    > [No response seen]
        > [Expert Info (Warn/Sequence): No response seen to ICMP request]
    > Data (4000 bytes)
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
        [Length: 4000]

```

EJERCICIO N° 11

Repita el ejercicio 10, pero agregando el parámetro **-f** (-M en Linux). ¿Qué resultado obtuvo? ¿Por qué?

```

C:\Windows\system32>ping 8.8.8.8 -n 1 -l 4000 -f
Haciendo ping a 8.8.8.8 con 4000 bytes de datos:
Es necesario fragmentar el paquete pero se especificó DF.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
                (100% perdidos),

```

El parámetro '**-f**' indica la opción expresa de no fragmentar(DF) el paquete, que excede el MTU y se debiera fragmentar; el protocolo no puede realizar ésta acción y el paquete se pierde.