Prácticas de laboratorio

de

Redes de Ordenadores

Práctica 6 Solución:

SNMP

Written by

IngTeleco

http://ingteleco.iespana.es

ingtelecoweb@hotmail.com

La dirección URL puede sufrir modificaciones en el futuro. Si no funciona contacta por email

Práctica 6: Protocolo SNMP

3. GUIÓN DE LA PRACTICA

3.2 Operación de SNMP

- ✓ ¿Mediante qué protocolos de capas inferiores es transferido SNMP?
  IP y UDP

- ✓ ¿A qué puertos de origen y destino se envían los mensajes SNMP?
  Puerto origen: 1043
  Puerto destino: 161 (SNMP)

- ✓ El monitor de red identifica uno de estos números con el asignado al protocolo SNMP, ¿cuál de los dos?
  161

- ✓ El otro número de puerto no es reconocido, ¿qué explicación se podría dar a este hecho?
  El SO asigna puertos aleatorios a petición de las aplicaciones, sólo el servidor debe cumplir el estándar en cuanto a los puertos de las aplicaciones, en este caso el puerto 161 (SNMP)

- ✓ ¿Cuál es la longitud total en bytes correspondiente a la parte SNMP?
  42 bytes

- ✓ ¿Cuál es el rendimiento de la trama?
  El rendimiento es ... 42/84=0'5

- ✓ Incluir la trama en la memoria.

```
Fram Time         Src MAC Addr   Dst MAC Addr   Protoc
Description                                       Src
Other Addr Dst Other Addr Type O
35   7.465000     KYE SY04F7E7   00D058AD53E8   SNMP
SNMPv1; community = public; Get request; Request
172.10.10.63   172.10.10.51

+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet
Protocol
+ IP: ID = 0x1B1E; Proto = UDP; Len: 70
+ UDP: Src Port: Unknown, (1043); Dst Port: SNMP (161);
Length = 50 (0x32)
+ SNMP: SNMPv1; community = public; Get request; Request
ID = 56762; Length = 42 (0x2A)

00000:  00 D0 58 AD 53 E8 00 C0 DF 04 F7 E7 08 00 45 00
.ÐX-Sè.ÀßÑ÷ç..E.
```

```
00010:  00 46 1B 1E 00 00 80 11 B3 02 AC 0A 0A 3F AC 0A
.F....?.³.¬..?¬.
00020:  0A 33 04 13 00 A1 00 32 77 5A 30 28 02 01 00 04
.3...¡.2wZ0(....
00030:  06 70 75 62 6C 69 63 A0 1B 02 03 00 DD BA 02 01
.public ....Ýº..
00040:  00 02 01 00 30 0E 30 0C 06 08 2B 06 01 02 01 01
....0.0...+.....
```

- ✓ Seleccionar un mensaje de tipo Get request y localizar su mensaje Response correspondiente. Observar el valor del campo Request-id de ambos mensajes, ¿cuál es su valor? ¿Por qué crees que puede ser necesaria esta técnica?

Get Request

```
Fram Time         Src MAC Addr   Dst MAC Addr   Protoc
Description                                       Src
Other Addr Dst Other Addr Type O
35   7.465000     KYE SY04F7E7   00D058AD53E8   SNMP
SNMPv1; community = public; Get request; Request
172.10.10.63   172.10.10.51

+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet
Protocol
+ IP: ID = 0x1B1E; Proto = UDP; Len: 70
+ UDP: Src Port: Unknown, (1043); Dst Port: SNMP (161);
Length = 50 (0x32)
+ SNMP: SNMPv1; community = public; Get request; Request
ID = 56762; Length = 42 (0x2A)

00000:  00 D0 58 AD 53 E8 00 C0 DF 04 F7 E7 08 00 45 00
.ÐX-Sè.ÀÞ.÷ç..E.
00010:  00 46 1B 1E 00 00 80 11 B3 02 AC 0A 0A 3F AC 0A
.F....?.³.¬..?¬.
00020:  0A 33 04 13 00 A1 00 32 77 5A 30 28 02 01 00 04
.3...¡.2wZ0(....
00030:  06 70 75 62 6C 69 63 A0 1B 02 03 00 DD BA 02 01
.public ....Ýº..
00040:  00 02 01 00 30 0E 30 0C 06 08 2B 06 01 02 01 01
....0.0...+.....
```

Response

```
Fram Time         Src MAC Addr   Dst MAC Addr   Protoc
Description                                       Src
Other Addr Dst Other Addr Type O
36   7.486000     00D058AD53E8   KYE SY04F7E7   SNMP
SNMPv1; community = public; Response; Request ID
172.10.10.51   172.10.10.63

+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet
Protocol
+ IP: ID = 0x33E8; Proto = UDP; Len: 78
+ UDP: Src Port: SNMP, (161); Dst Port: Unknown (1043);
Length = 58 (0x3A)
+ SNMP: SNMPv1; community = public; Response; Request ID
= 56762; Length = 50 (0x32)

00000:  00 C0 DF 04 F7 E7 00 D0 58 AD 53 E8 08 00 45 00
.Àß.÷ç.ÐX-Sè..E.
00010:  00 4E 33 E8 00 00 FF 11 1B 30 AC 0A 0A 33 AC 0A
.N3è..ÿ..0¬..3¬.
00020:  0A 3F 00 A1 04 13 00 3A 40 04 30 30 02 01 00 04
.?.¡...:@.00....
00030:  06 70 75 62 6C 69 63 A2 23 02 03 00 DD BA 02 01
.public¢#...Ýº..
00040:  00 02 01 00 30 16 30 14 06 08 2B 06 01 02 01 01
....0.0...+.....
```

✓ Incluir en la memoria una trama Response cuya petición ha sido errónea.

```
Frame    Time         Src MAC Addr    Dst MAC Addr
Protocol    Description
Src Other Addr     Dst Other Addr     Type Other Addr
88       14.825000    00D058AD53E8    TL008-01
SNMP        SNMPv1; community = public; Response; Request
ID  172.10.10.51       TL008-01           IP


page 4


Network Monitor trace  Mon 11/25/02 09:31:00
capturaSNMP.txt

+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet
```

```
Protocol
+ IP: ID = 0x149D; Proto = UDP; Len: 66
+ UDP: Src Port: SNMP, (161); Dst Port: Unknown (1734);
Length = 46 (0x2E)
+ SNMP: SNMPv1; community = public; Response; Request ID
= 184; Length = 38 (0x26)

00000:  00 C0 DF 04 F7 E7 00 D0 58 AD 53 E8 08 00 45 00
.Àß.÷ç.ÐX-Sè..E.
00010:  00 42 14 9D 00 00 FF 11 3A 87 AC 0A 0A 33 AC 0A
.B.•..ÿ.:?¬..3¬.
00020:  0A 3F 00 A1 06 C6 00 2E 17 FD 30 24 02 01 00 04
.?.¡.Æ...ý0$....
00030:  06 70 75 62 6C 69 63 A2 17 02 02 00 B8 02 01 02
.public¢....¸...
00040:  02 01 01 30 0B 30 09 06 04 2B 06 01 01 06 01 00
...0.0...+......
```

¿Qué campos muestran que es una petición errónea? ¿Qué valores tienen estos campos en una petición sin y con error?

El error se refleja en el campo error status y error index, cuando no se produce error tienen valor 0. En el error tienen valor: no such name /1 (0x01)

- ✓ ¿Cuál es el contenido del campo community de la cabecera de una trama Trap? ¿coincide con el del resto de mensajes?

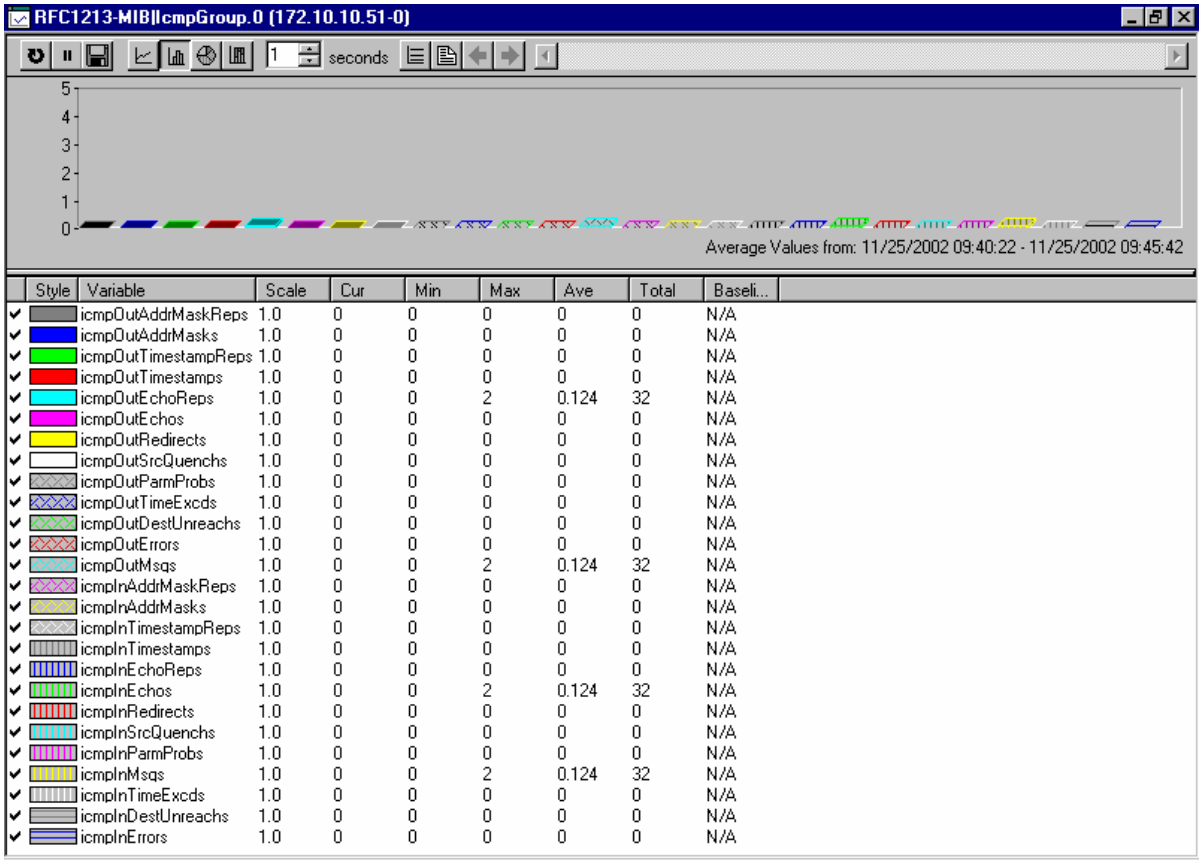
255.255.0.0. No coincide con los demás, el resto tiene el valor public.

3.3 Uso de la aplicación de gestión SNMP5c de Castle Rock

- ✓ Herramienta Poll Object, ¿qué equipo es el que hace las peticiones? ¿A qué protocolo pertenecen?
  Equipo:TL018 / 172.10.10.18
  Protocolo: SNMP

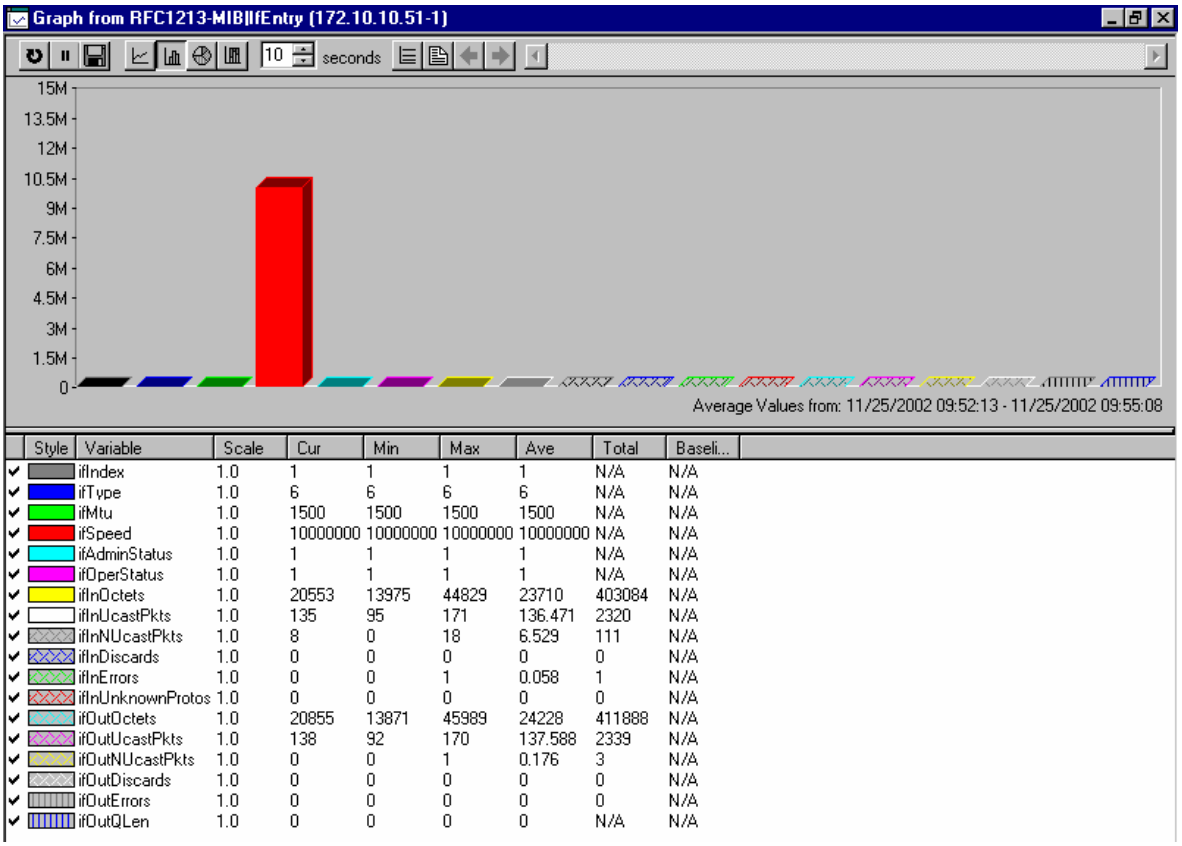
- ✓ Hubview

  Gráfica de estadísticas ICMP



Style	Variable	Scale	Cur	Min	Max	Ave	Total	Baseli...
✔	icmpOutAddrMaskReps	1.0	0	0	0	0	0	N/A
✔	icmpOutAddrMasks	1.0	0	0	0	0	0	N/A
✔	icmpOutTimestampReps	1.0	0	0	0	0	0	N/A
✔	icmpOutTimestamps	1.0	0	0	0	0	0	N/A
✔	icmpOutEchoReps	1.0	0	0	2	0.124	32	N/A
✔	icmpOutEchos	1.0	0	0	0	0	0	N/A
✔	icmpOutRedirects	1.0	0	0	0	0	0	N/A
✔	icmpOutSrcQuenchs	1.0	0	0	0	0	0	N/A
✔	icmpOutParmProbs	1.0	0	0	0	0	0	N/A
✔	icmpOutTimeExcds	1.0	0	0	0	0	0	N/A
✔	icmpOutDestUnreachs	1.0	0	0	0	0	0	N/A
✔	icmpOutErrors	1.0	0	0	0	0	0	N/A
✔	icmpOutMsgs	1.0	0	0	2	0.124	32	N/A
✔	icmpInAddrMaskReps	1.0	0	0	0	0	0	N/A
✔	icmpInAddrMasks	1.0	0	0	0	0	0	N/A
✔	icmpInTimestampReps	1.0	0	0	0	0	0	N/A
✔	icmpInTimestamps	1.0	0	0	0	0	0	N/A
✔	icmpInEchoReps	1.0	0	0	0	0	0	N/A
✔	icmpInEchos	1.0	0	0	2	0.124	32	N/A
✔	icmpInRedirects	1.0	0	0	0	0	0	N/A
✔	icmpInSrcQuenchs	1.0	0	0	0	0	0	N/A
✔	icmpInParmProbs	1.0	0	0	0	0	0	N/A
✔	icmpInMsgs	1.0	0	0	2	0.124	32	N/A
✔	icmpInTimeExcds	1.0	0	0	0	0	0	N/A
✔	icmpInDestUnreachs	1.0	0	0	0	0	0	N/A
✔	icmpInErrors	1.0	0	0	0	0	0	N/A

Gráfica de estadísticas de salida del interfaz Ethernet 0



Style	Variable	Scale	Cur	Min	Max	Ave	Total	Baseli...
	ifIndex	1.0	1	1	1	1	N/A	N/A
	ifType	1.0	6	6	6	6	N/A	N/A
	ifMtu	1.0	1500	1500	1500	1500	N/A	N/A
	ifSpeed	1.0	10000000	10000000	10000000	10000000	N/A	N/A
	ifAdminStatus	1.0	1	1	1	1	N/A	N/A
	ifOperStatus	1.0	1	1	1	1	N/A	N/A
	ifInOctets	1.0	20553	13975	44829	23710	403084	N/A
	ifInUcastPkts	1.0	135	95	171	136.471	2320	N/A
	ifInNUcastPkts	1.0	8	0	18	6.529	111	N/A
	ifInDiscards	1.0	0	0	0	0	0	N/A
	ifInErrors	1.0	0	0	1	0.058	1	N/A
	ifInUnknownProtos	1.0	0	0	0	0	0	N/A
	ifOutOctets	1.0	20855	13871	45989	24228	411888	N/A
	ifOutUcastPkts	1.0	138	92	170	137.588	2339	N/A
	ifOutNUcastPkts	1.0	0	0	1	0.176	3	N/A
	ifOutDiscards	1.0	0	0	0	0	0	N/A
	ifOutErrors	1.0	0	0	0	0	0	N/A
	ifOutQLen	1.0	0	0	0	0	N/A	N/A

Tabla de información del protocolo ARP

10 sec

IfIndex	NetAddress	PhysAddress	Type
1	172.10.10.1	00 c0 df 0d 5b 73	dynamic
1	172.10.10.2	00 c0 df 0d 5b 61	dynamic
1	172.10.10.3	00 c0 df 0d 5b 60	dynamic
1	172.10.10.4	00 c0 df 0d 5b 6d	dynamic
1	172.10.10.5	00 c0 df 0d 5b 70	dynamic
1	172.10.10.7	00 c0 df 05 4c 07	dynamic
1	172.10.10.8	00 c0 df 0d 5b 64	dynamic
1	172.10.10.10	00 c0 df 0d 5b 5c	dynamic
1	172.10.10.11	00 c0 df 0d 5b 71	dynamic
1	172.10.10.12	00 c0 df 0d 5b 5f	dynamic
1	172.10.10.14	00 c0 df 0b 73 d9	dynamic
1	172.10.10.17	00 c0 df 02 0a 59	dynamic
1	172.10.10.18	00 c0 df 0d 5b 6a	dynamic
1	172.10.10.19	00 c0 df 0d 5b 6c	dynamic
1	172.10.10.20	00 c0 df 02 0a 72	dynamic
1	172.10.10.51	00 d0 58 ad 53 e8	other
1	172.10.10.63	00 c0 df 04 f7 e7	dynamic

- ✓ MIB Browser

  - ✓ ¿A qué estándares pertenecen las distintas variables?
    Estándar: SNMP

  - ✓ Descubrir a qué variables les corresponden los siguientes identificadores: 1.3.6.1.2.1.6.13.1.1 y 1.3.6.1.2.1.5.4, ¿qué tipo de variables son? ¿Cuál es su valor?

OID	1.3.6.1.2.1.6.13.1.1	1.3.6.1.2.1.5.4
Nombre	TCP conn state	Icmp In Time Exceds
Tipo	Integer	Counter
MIB	RFC 1213-MIB	RFC 1213-MIB

  - ✓ Descubrir qué identificadores OID son los que corresponden a las variables mgmt/interfaces/ifNumber y mgmt/IP/ipInReceives, ¿Qué tipo de variables son?¿cuál es su valor?

Nombre	mgmt/interfaces/ifNumber	mgmt/IP/ipInReceives
OID	1.3.6.1.2.1.2.1	1.3.6.1.2.1.4.3
Tipo	Integer	Counter
MIB	RFC 1213-MIB	RFC 1213-MIB