Exercici 1 del mòdul 14 de CISCO - Protocol ICMP

PART 1

1- Què és i quin és el principal propòsit del protocol ICMP?

És un protocol auxiliar que dóna suport al protocol IP i que tè com a propòsits:

- Permetre proves de connectivitat entre equips
- Enviament de missatge d'error i informatius entre 2 equips que es comuniquen per internet. Per exemple, un router pot informar a un ordinador que un paquet IP no s'ha pogut reenviar a la destinació.

Sense aquest protocol les xarxes i internet poden funcionar però d'altra banda és molt útil per solucionar problemes de connexió entre equips.

2- Principals tpics d'enviament d'un missatge ICMP:

Hi ha molts motius per enviar missatges ICMP però els més típics són:

- Missatges enviats des d'un equip a un altre per fer proves d'accessibilitat. Aquest missatges serveixen per comprovar si des del meu equip tinc accés (connectivitat) a un l'altre equip de la xarxa local o Internet. En altres paraules, fer un ping.
- Missatge de destinació o servei inabastable (no es pot arribar). Quan un equip intermedi (normalment un router) vol informar a un equip origen que un missatge no es pot fer arribar a l'equip destinació, genera un misstge d'aquest tipus que envia a l'equip que originar origen. Aquest missatge poden ser necessaris per informar que una xarxa, equip, port o servei demanat no és abastable.
- Un misssatge de temps superat (excedido) s'envia quan un equip intermedi (normalment un router) vol informar a l'equipo origen de dades que el camp TTL d'un paquet IP ha arribat a 0 i s'ha descartat.

3- Un missatge RA

a) És enviat per un Router cada 200seg per informar a la xarxa de la seva existència i enviar configuració de xarxa que pugi ser utilitzat per equips que treballen amb configuració de xarxa dinàmica autòmatica IPv6.

b) És enviat per un equip que s'acaba de connectar a la xarxa per demanar configuració IPv6.

c) Per comprovar que la seva IPv6 no està repetida i és única

d) Per trobar l'adreça MAC d'un equip a partir de la seva adreça IPv6

4- Un missatge RS

a) És enviat per un Router cada 200seg per informar a la xarxa de la seva existència i enviar configuració de xarxa que pugi ser utilitzat per equips que treballen amb configuració de xarxa dinàmica autòmatica IPv6.

b) És enviat per un equip que s'acaba de connectar a la xarxa per demanar configuració IPv6.

c) Per comprovar que la seva IPv6 no està repetida i és única

d) Per trobar l'adreça MAC d'un equip a partir de la seva adreça IPv6

5- Un missatge NS

a) És enviat per un Router cada 200seg per informar a la xarxa de la seva existència i enviar configuració de xarxa que pugi ser utilitzat per equips que treballen amb configuració de xarxa dinàmica autòmatica IPv6.

b) És enviat per un equip que s'acaba de connectar a la xarxa per demanar configuració IPv6.

c) Per comprovar que la seva IPv6 no està repetida i és única.

d) Per trobar l'adreça MAC d'un equip a partir de la seva adreça IPv6

6- Un missatge NA

a) És enviat per un Router cada 200seg per informar a la xarxa de la seva existència i enviar configuració de xarxa que pugi ser utilitzat per equips que treballen amb configuració de xarxa dinàmica autòmatica IPv6.

b) És enviat per un equip que s'acaba de connectar a la xarxa per demanar configuració IPv6.

c) Per comprovar que la seva IPv6 no està repetida i és única

d) Per trobar l'adreça MAC d'un equip a partir de la seva adreça IPv6.

7- Quines són les proves de connectivitat típiques que es poden fer amb el programa ping?

- Ping a la interfície de loopback local → ping 127.0.0.1 o ping localhost
- Ping a la pròpia IP de l'equip local
- Ping a altres equips de la xarxa local
- Ping a l'adreça IP del router
- Ping a un equip (host) extern, és qualsevol ordinador que està a l'altra banda del nostre router.

8- Què funció realitza l'ordre traceroute?. Quina tècnica utilitza per dur a terme aquesta funció?

- L'ordre traceroute es fa servir per una llista de tots els salts que fa un paquet IP des de l'origen fins a la destinació. Un salt d'un paquet IP pot ser:
  - L'enviament del paquet del PC/Portàtil/Mòbil,etc a un Router
  - L'enviament del paquet IP d'un router a un altre router
  - L'enviament d'un paquet IP d'un router a un PC/Portàtil/Mòbil,etc..

- El programa traceroute ens presentarà per pantalla la llista de routers i equips pels quals ha passat el paquet IP, indicant les seves IPs, noms i temps d'espera.

- El programa traceroute ens permet veure per on viatja un paquet i saber a on hi han problemes i si pot ser, solucionar-los.

- Per poder fer aquesta funció el traceroute:
  - Envia primer un paquet amb una TTL=1 de manera el primer router descarta el paquet i envia un missatge de resposta a l'origen de tipus Code=0 i Type=11 que vol dir Time-to-live exceeded (temps de vida superat) i d'aquesta manera es pot saber l'adreça IP del primer router.
  - Després envia paquets amb TTL= 2, 3,4,... i així es van descobrint les IPs de nous routers fins arribar a l'adreça IP destinació.
  - Quan arriba a l'adreça IP destinació, l'equip destinació enviarà un missatge de tipus Type=3 Code=3 que vol dir Destination Inabastable i això servirà perquè l'equip origen finalitzi traceroute.
  - Amb tota aquesta informació es pot fer una llista del routers pels quals ha passat el paquet i fins tot saber la seva localització aproximada.

- El progama traceroute ens dóna el temps de resposta en ms de cada salt o un * si hi ha un problema (no hi ha resposta o el paquet es perd). Això ens pot permetre localitzar un router problemàtic i solucionar el problema si es troba dins de la nostra xarxa.

9- Indica els camps de capçalera d'un missatge ICMP i quina és la seva funció:

- Type i Code → Combinats serveixen per identificar el tipus de missatge ICMP i enviar informació addicional per acabar d'identificar-lo. Per exemple:
  - Tipus = 8 i Code = 0 → Missatge de petició d'eco, enviat per l'equip que fa el ping a un altre
  - Tipus = 0 i Code = 0 → Missatge de resposta d'eco, enviat per l'equip que respon a un ping
  - Tipus = 11 i Code = 0 → Temps de vida superat.
  - Tipus = 3 Code = 3 → Destinació inabastable. Port inabastable.
  - Tipus = 3 Code = 1 → Destinació inabastable. Equip (IP) inabastable.
- Checksum → Codi de detecció d'errors de la capçalera del missatge ICMP.
- Body Message → El seu contingut és variable i depén de la informació que es vulgui enviar associada al Type i Code del missatge. Per exemple, si es fa un ping, el Body Message inclou:
  - Identitfier: Identifica tots els missatge de petició/resposta d'eco entre 2 equip iniciats per un ping. Dos ping diferents tindran un identifier diferent
  - Sequence number: Identifica cada missatge de petició/resposta dins d'un mateix ping

10- Indica:
a) A on s'encapsula un missatge ICMP → Dins del camp de dades d'un paquet IP
b) Que s'encapsula dins d'un missatge ICMP → No es pot encapsular cap altre protocol.

PART 2

1.- Descarrega el fitxer de captures icmp.pcapng**. Posa en marxa wireshark, obre el fitxer descarregat i crea el següent filtre: *icmp*.**

2.- Inidica de quin tipus són els missatge ICMP de les captures 1 a 8 i que està passant d'acord amb la informació mostrada pel wireshark.

- Totes aquests missatges formen part d'una mateixa seqüència perquè el camp Identifier val (utilitzant BE) 0x0cef.
- Tots els missatges son de Type = 8 i Code = 0. Això vol dir que estem enviant un missatge de Petició d'Eco. Una petició d'eco vol dir que demanem a l'equip destinatari que enviï un missatge de resposta d'eco.
- Si analitzo els missatges ICMP no trobo cap missatge de resposta d'eco que tingui el mateix valor del camp Identifier de les peticions realitzades.
- Sabem que l'equip destinació no respon a les peticions d'eco, però no sabem si és perquè no està connectat, perquè no hi ha cap equip amb l'adreça IP de destinació o perquè l'equip no respon a missatge ICMP de petició d'eco.

3- Que estem veient a la captura 41?. Quin router està enviant aquesta informació?

- És un missatge de tipus 11 i codi 0
- Segon l'IANA, el tipus 11 correspon a Time Exceeded. Això vol dir que hi ha algún problema amb el TTL del paquet IP. El codi 0 vol Time to Live exceeded in Transit.
- Per tant, que està passant?→ Doncs que el paquet IP quan viatjava de Router en Router fins arribar a la destinació el seu TTL ha arribat a 0 i el paquet ha estat descartat pel darrer Router.
- El Router ha enviat aquest missatge ICMP a l'ordinador origen del paquet per avisar-lo del problema

4- Que estem veient a la captura 68?. Quin router està enviant aquesta informació (Mira Annex)?

- Estem veient el resultat d'utilitzar l'ordre traceroute (o tracert).
- Estem observant que un Router amb l'adreça IP 81.46.34.73 ha descartat un missatge enviat pel traceroute i ha generat un missatge de resposta que podem utilitzar per anar traçant la ruta que segueix un paquet IP per arribar a la seva destinació (en aquest cas www.google.com)
- Si mirem l'annex, veurem que el Router que envia el missatge formava part de la xarxa routers de la companyia Telefònica (Movistar).

5- Què estem veient a la captura 98?. Quin equip envia aquest missatge? És un host o un router l'equip que envia aquest missatge?

- Si mirem el tipus és igual a 3 i per tant, en parla de que els paquets IP no podem arribar a la destinació demanada. Però no poder arribar pot voler: que no podem arribar a la xarxa de l'ordinador, o no podem arribar a l'ordinador, o no podem arribar a un port dins de l'ordinador, etc..
- En aquest cas, el problema és que no podem accedir a un Port perquè el codi del missatge és 3.
- Si busquem dins del missatge ICMP, veurem que el problema està a l'adreça IP 142.250.200.68 i dins d'aquest amb un port de tipus UDP i número 33466.

PART 3

1- Fes l'exercici de packet tracer de l'apartat 12.2.6 del curs de cisco i escriu les respostes.

- Part 1
  - Pas 1:
    - IPv4 de PC1 → 10.10.1.100/27 (interfície FastEthernet0)
    - IPv4 de PC2 → 10.10.1.20/28 (interfície FastEthernet0)
  - Pas2:
    - IPv6 de PC1 → 2001:DB8:1:1::A/64 (interfície FastEthernet0)
    - IPv6 de PC2 → 2001:DB8:1:4::A/64 (interfície FastEthernet0)

- Part 2
  - El resultat de la verificació de connectivitat de PC1 amb PC2 és correcte perquè hem enviat 4 missatges ICMP de petició d'eco des de PC1 i n'hem rebut 4 de resposta d'eco des de PC2:

```
C:\>ping 10.10.1.20

Pinging 10.10.1.20 with 32 bytes of data:

Reply from 10.10.1.20: bytes=32 time=2ms TTL=125
Reply from 10.10.1.20: bytes=32 time=40ms TTL=125
Reply from 10.10.1.20: bytes=32 time=2ms TTL=125
Reply from 10.10.1.20: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 40ms, Average = 11ms
```

  - El resultat de la verificació de connectivitat de PC2 amb PC1 és correcte perquè hem enviat 4 missatges ICMP de petició d'eco des de PC2 i n'hem rebut 4 de resposta d'eco des de PC1:

```
C:\>ping 10.10.1.100

Pinging 10.10.1.100 with 32 bytes of data:

Reply from 10.10.1.100: bytes=32 time=68ms TTL=125
Reply from 10.10.1.100: bytes=32 time=2ms TTL=125
Reply from 10.10.1.100: bytes=32 time=2ms TTL=125
Reply from 10.10.1.100: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 68ms, Average = 18ms
```

- Part 3
  - Pas 1
    - Tracert des de PC1 a PC2

```
C:\>tracert 10.10.1.20

Tracing route to 10.10.1.20 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.1.97
  2    1 ms      1 ms      0 ms      10.10.1.5
  3    2 ms      0 ms      1 ms      10.10.1.10
  4    0 ms      0 ms      2 ms      10.10.1.20

Trace complete.
```

Adreces trobades	Equips trobats	Interfícies dels equips trobats
10.10.1.97	R1	GigabitEthernet0/0
10.10.1.5	R2	Serial0/0/0
10.10.1.10	R3	Serial0/0/0
10.10.1.20	PC2	FastEthernet0

    - Tracert des de PC2 a PC1 (tracert a 10.10.1.100)

Adreces trobades	Equips trobats	Interfícies dels equips trobats
10.10.1.17	R3	GigabitEthernet0/0
10.10.1.9	R2	Serial0/0/1
10.10.1.6	R1	Serial0/0/1
10.10.1.100	PC1	FastEthernet0

  - Pas 2
    - Tracert de PC1 a PC2

```
C:\>tracert 2001:DB8:1:4::A

Tracing route to 2001:DB8:1:4::A over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      2001:DB8:1:1::1
  2    1 ms      1 ms      1 ms      2001:DB8:1:2::1
  3    1 ms      1 ms      2 ms      2001:DB8:1:3::2
  4    10 ms     0 ms      2 ms      2001:DB8:1:4::A

Trace complete.
```

Adreces trobades	Equips trobats	Interfícies dels equips trobats
2001:DB8:1:1::1	R1	GigabitEthernet0/0
2001:DB8:1:2::1	R2	Serial0/0/0
2001:DB8:1:3::2	R3	Serial0/0/0
2001:DB8:1:4::A	PC2	FastEthernet0

    - Tracert des de PC2 a PC1 (tracert a 2001:DB8:1:1::A)

Adreces trobades	Equips trobats	Interfícies dels equips trobats
2001:DB8:1:4::1	R3	GigabitEthernet0/0
2001:DB8:1:3::1	R2	Serial0/0/1
2001:DB8:1:2::2	R1	Serial0/0/1
2001:DB8:1:1::A	PC2	FastEthernet0

Annex

```
daniel@sh3:~$ traceroute www.google.com
traceroute to www.google.com (142.250.200.68), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.349 ms  0.450 ms  0.643 ms
 2  141.red-81-46-38.customer.static.ccgg.telefonica.net (81.46.38.141)  5.926 ms  5.917 ms  5.892 ms
 3  73.red-81-46-34.customer.static.ccgg.telefonica.net (81.46.34.73)  11.223 ms  11.219 ms  12.371 ms
 4  * 133.red-81-46-34.customer.static.ccgg.telefonica.net (81.46.34.133)  11.122 ms *
 5  1.red-80-58-106.staticip.rima-tde.net (80.58.106.1)  14.852 ms * *
 6  * * 176.52.253.97 (176.52.253.97)  11.155 ms
 7  5.53.0.176 (5.53.0.176)  10.955 ms 5.53.1.74 (5.53.1.74)  10.738 ms 209.85.149.88 (209.85.149.88)  10.820 ms
 8  142.251.231.147 (142.251.231.147)  11.933 ms 192.178.110.155 (192.178.110.155)  13.260 ms 108.170.252.225 (108.170.252.225)  11.691 ms
 9  142.250.232.27 (142.250.232.27)  11.825 ms  11.899 ms 142.250.232.11 (142.250.232.11)  10.455 ms
10  mad07s24-in-f4.1e100.net (142.250.200.68)  10.597 ms  11.839 ms  10.430 ms
```