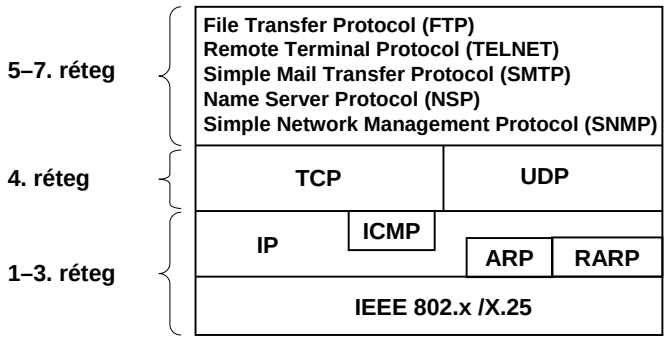
Internet Control Message Protocol (ICMP)
Az Internet hiba- és vezérlő üzenet továbbító protokollja

Készítette:
Schubert Tamás (BMF)

Tartalom

TCP/IP protokollkészlet



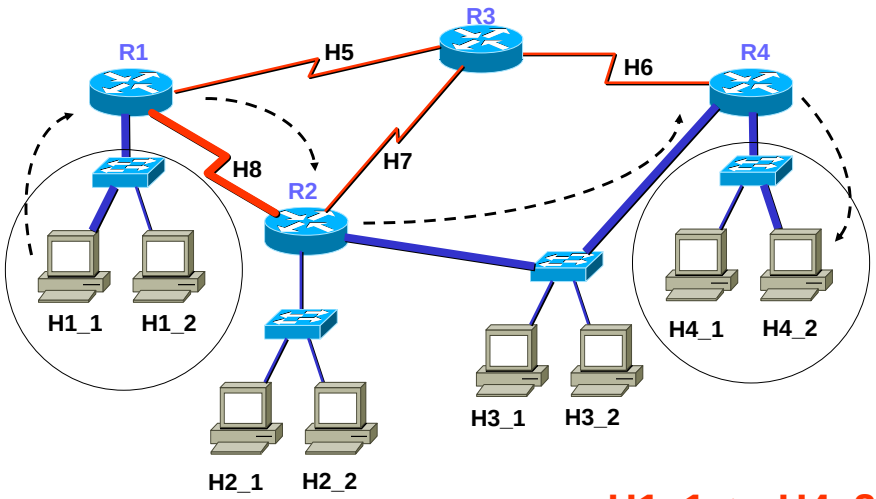
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
ICMP	Internet Control Message Protocol

Az Internet Control Message Protocol

A csomag útja során forgalomirányítók sorozatán halad, míg eléri célállomását. Ha egy forgalomirányító nem képes továbbítani a csomagot, vagy valamilyen rendellenességet tapasztal (pl. torlódás) értesítenie kell a csomagot feladó számítógépet, hogy orvosolja a problémát.

Az állomások és forgalomirányítók az ICMP protokoll segítségével küldhetnek hiba- és vezérlő információt.

A csomag haladása forrástól a célig



H1_1 -> H4_2

Internet Control Message Protocol

Az Internet Control Message Protocol

Néhány lehetséges hiba, ami miatt hibajelzésről gondoskodni kell:

- Vonalak, hardver eszközök meghibásodása,
- Az IP nem tudja eljuttatni a csomagot a célba, mert a célállomás átmenetileg vagy véglegesen ki van kapcsolva, vagy nincs csatlakoztatva a hálózatra.
- A Time-to-Live számláló értéke eléri a 0-át.
- A forgalomirányítókon torlódnak a csomagok.

Internet Control Message Protocol

A hibák jelzését a TCP/IP protokoll család ICMP protokollja segítségével oldják meg.

Az ICMP üzenetek az IP üzenetek adatrészében utaznak.

Az ICMP üzenet célja nem az alkalmazói program vagy felhasználó, hanem a célállomás ICMP modulja.

Majd az ICMP modul dönti el, hogy mit kezd az üzenettel, melyik szoftver modult értesíti.

Összefoglalva:

Az ICMP lehetővé teszi, hogy állomások vagy forgalomirányítók hiba- vagy vezérlőüzenetet küldjenek más állomásoknak vagy forgalomirányítóknak.

Az ICMP mindig két gép IP szoftvere között biztosít kommunikációt.

Hibajelzés vagy hibajavítás

Az ICMP technikailag egy hibajelző mechanizmus.

Amikor egy üzenet (IP csomag) hibát okoz, az ICMP jelzi a hibát a csomag eredeti feladójának.

A feladó állomásnak kell a hibát összekapcsolnia a megfelelő alkalmazással, vagy megtenni a szükséges intézkedést a hiba kiküszöbölésére.

A hibák egy része az üzenet eredeti feladójától származik, más része nem.

Az ICMP mégis mindig az üzenet eredeti feladóját értesíti, a közbenső forgalomirányítókat nem képes értesíteni.

Hibajelzés vagy hibajavítás

Pl.

Tegyük fel, hogy az üzenet az

R_1, R_2, … R_k forgalomirányítókon halad keresztül.

Ha R_k hibás irányítási információk alapján R_E -nek továbbítja a csomagot, R_E nem tudja az ICMP-vel értesíteni az R_k forgalomirányítókat, hanem csak a csomag eredeti feladóját.

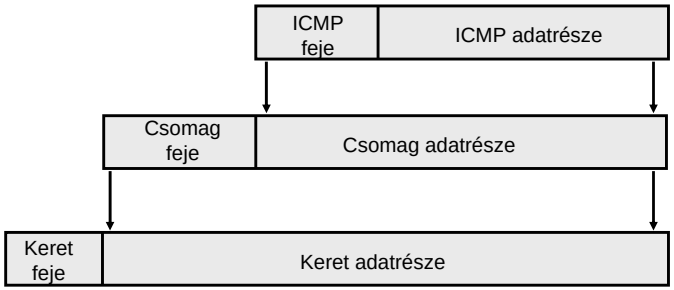
Ennek oka az IP üzenet struktúrájában rejlik.

Az IP fejrésze csak a feladó és a célállomás IP címét tartalmazza.

A forgalomirányítók nem rendelkeznek azon eszközök címével, amelyeken a csomag áthaladt.

Az ICMP üzenetkézbesítés

Az ICMP üzenet egy IP csomagban utazik az interneten. Ugyanúgy halad forgalomirányítókon keresztül, mint a normális adatot szállító IP csomag. Az ICMP üzenet továbbítása is lehet sikertelen, azonban egy ICMP üzenetet szállító IP csomag elakadásáról újabb ICMP üzenet nem generálódik!



ICMP beágyazása csomagba, majd a csomag keretbe foglalása

Az ICMP üzenetkézbesítés

Az ICMP üzenet IP csomagba ágyazódik, az ICMP mégsem tekinthető magasabb szintű protokollnak.

Az ICMP az IP szükséges része.

Az ICMP üzenet nem továbbítható közvetlenül a fizikai hálózaton, mivel a célállomás eléréséhez általában több fizikai hálózaton kell keresztülhaladnia.

Az ICMP üzenetformátuma

Mindegyik ICMP üzenet saját formátummal rendelkezik, az első 3 mezőjük azonos:

TYPE	Azonosítja az üzenetet
CODE	További információt ad az üzenet típusáról
CHECKSUM	Az ICMP üzenet ellenőrző összege

A fentieken kívül azon üzenetek, amelyek valamilyen hibát jeleznek, mindig tartalmazzák a hibát okozó üzenet első 64 bitjét.

Az ICMP TYPE mező meghatározza az üzenet jelentését és a formáját:

Az ICMP üzenet formátuma

Type mező	ICMP üzenettípus
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
11	Time Exceeded for Datagram
12	Parameter Problem on Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Reply (obsolete)
17	Address Mask Request
18	Address Mask Reply

A célállomás elérhetőségének tesztelése

A hálózati problémák feltárásához nyújt segítséget az *echo request* és *echo reply* üzenet.

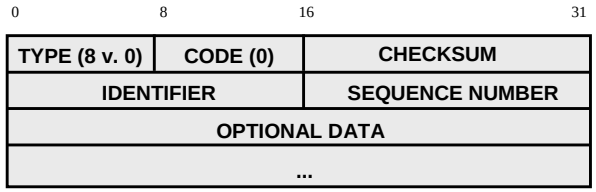
Minden gép, amely kap egy echo request üzenetet, egy echo reply üzenetben megválaszolja.

Ezzel tesztelhető a hálózati alrendszer.

A legtöbb operációs rendszer a *ping* programmal teszi ezt a mechanizmust közvetlenül elérhetővé a felhasználók számára.

Az Echo Request és Echo Reply üzenetformátum

OPTIONAL DATA	A feladó kitöltheti ezt a mezőt tetszőleges adattal, a célállomás a válaszüzenetébe átmásolja ezt.
IDENTIFIER	A kérést és a választ rendeli egymáshoz
SEQUENCE NUMBER	A kérést és a választ rendeli egymáshoz
TYPE	kérés = 8; válasz = 0

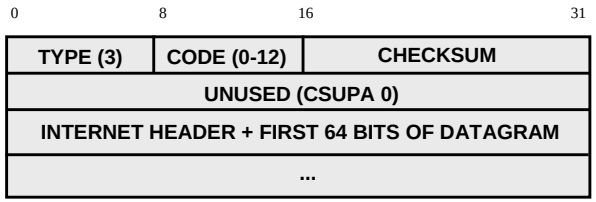


ICMP visszhang kérés és válasz

Elérhetetlen célállomás (destination unreachable)

Ha egy forgalomirányító nem tudja kézbesíteni vagy továbbítani a csomagot, ezt az üzenetet küldi az eredeti feladónak.

A forgalomirányítók azonban nem mindig észlelik a hibát. Pl. Ethernet hálózaton MAC szinten nincs visszaigazolás.



ICMP cél nem elérhető

Elérhetetlen célállomás (destination unreachable)

Az ICMP CODE mező részletezi a hiba okokat:

Code	Jelentés
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation needed and DF set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

Torlódás és adatfolyam vezérlés (Congestion and Datagram Flow Control)

Torlódás akkor fordul elő, ha a forgalomirányító nem képes olyan gyorsan továbbítani a csomagokat, mint amilyen gyorsan érkeznek. Ennek alapvetően két oka lehet:

- Gyors forrás
- A csomagok több forrásból származnak

A forgalomirányítókban és a állomásokban lévő pufferek átmenetileg kiküszöbölhetik a forgalmi csúcsokat, de tartósan megnőtt forgalmat nem tudnak feloldani.

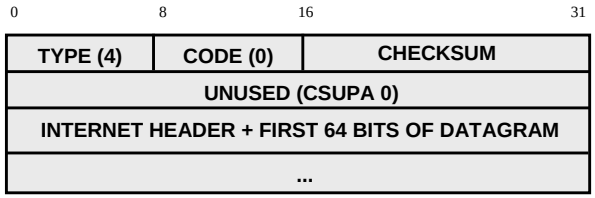
A gépek az ICMP forráselfojtás üzenettel jelezhetik a forrásnak a torlódást. A forgalomirányítók minden eldobott csomagról generálnak egy forráselfojtás üzenetet.

Egyes forgalomirányítók csak a legnagyobb forgalmat generáló forrást értesítik, vagy már a torlódás bekövetkezte előtt (hosszú várakozó sorok) elküldik a hibaüzenetet.

Torlódás és adatfolyam vezérlés (Congestion and Datagram Flow Control)

A forráselfojtás üzenetnek nincs fordított párja. Ezért az állomás IP protokollja úgy működik, hogy ha adott célállomásra küldött üzenetről forráselfojtás üzenetet kap, addig csökkenti a sebességet, amíg a hibaüzenetek megszűnnek, majd fokozatosan növeli az üzenetek gyakoriságát addig, amíg újra forráselfojtás üzenet nem érkezik.

Forráselfojtás (Source Quench)



Útvonal megváltoztatás kérés Irányítási hurok vagy túl hosszú útvonal

Útvonal megváltoztatás kérés (Route Change Request)

Az állomások általában csak egyetlen forgalomirányító címét ismerik, és neki küldik az összes továbbítandó csomagot. A forgalomirányító, ha az adott célállomásra jobb kiinduló forgalomirányítót ismer, ICMP üzenetben jelzi az állomásnak, hogy a többi csomagot melyik forgalomirányítónak továbbítsa ezután.

Irányítási hurok vagy túl hosszú útvonal (Time exceeded for a datagram)

A hibás irányítótáblákból eredő hurkokat, és a túl hosszú útvonalakat a Time to Live számlálóval küszöbölik ki. Ha a TTL miatt kell egy csomagot eldobni, ezt az ICMP üzenetet generálja a forgalomirányító.

Egyéb problémák jelzése
Órák szinkronizálása és csomag haladási idejének becslése

Egyéb problémák jelzése (Parameter problem on datagram)

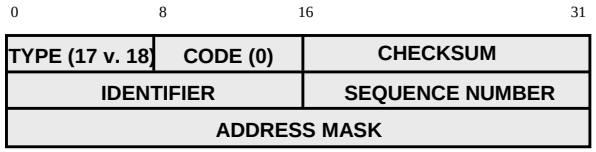
Általában a hibás csomagfejléceket jelzik ezzel az ICMP üzenettel.

Órák szinkronizálása és csomag haladási idejének becslése (Timestamp request and reply)

A gépek lekérdezhetik a másik gép óráját, amely korrigálható a csomagok haladási idejével. Ezzel a mechanizmussal egyúttal a csomag haladási ideje is becsülhető az adott útvonalon.

Maszk kérés és válasz (Address mask request and reply)

Alhálózat használata esetén az alhálózati maszk határozza meg, hogy az adott osztályú cím állomásokat azonosító részéből mely bitek határozzák meg az adott fizikai hálózatot. Ez a maszk beállítható az állomás hálózati konfigurálásakor, de ezzel az ICMP kéréssel be is szerezhető a forgalomirányítótól. A kérés a forgalomirányítónak közvetlenül is elküldhető, vagy szórással is kérhető.



ICMP cím-maszk kérés és válasz

A Ping segédprogram

Cél elérhetőségének tesztelése:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

-t	Ping the specifed host until interrupted.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet.
-i TTL	Time To Live.
-v TOS	Type Of Service.
-r count	Record route for count hops.
-s count	Timestamp for count hops.
-j host-list	Loose source route along host-list.
-k host-list	Strict source route along host-list.
-w timeout	Timeout in milliseconds to wait for each reply.

Feladatok

Analizáljuk az előre felvett hálózati forgalom ICMP üzeneteit!

Az Ethereal vagy WireShark programmal vegyük fel a hálózati forgalmat, szűrjük ki az ICMP üzeneteket, elemezzük ezeket!

Generáljunk olyan hálózati forgalmat, amely kiváltja a forrás elfojtás üzenetet!

Használjuk a ping programot állomások és forgalomirányítók elérhetőségének vizsgálatára!

Próbáljunk meg elérni egy nem létező szervert a helyi hálózati szegmensen és egy távoli szegmensen. Melyik esetben kapunk hibaüzenetet, és miért?

Irodalom

- Stallings W.
  Data and Computer Communications, Fifth Edition. Prentice-Hall, Inc. 1997.

- Fred Halsall.
  Data Communications, Computer Networks and Open Systems, Fourth Edition. Addison-Wesley Publishers Ltd. 1996.

- Andrew S. Tanenbaum.
  Számítógép-hálózatok, Panem Könyvkiadó Kft. 2004.
  Második kiadás