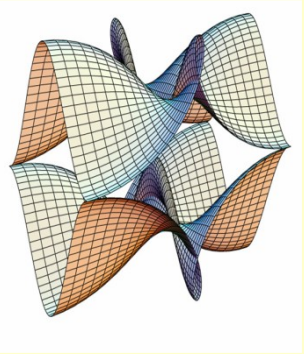
Sveučilište u Zagrebu
PMF – Matematički odsjek

MREŽE RAČUNALA
Predavanja 2022/2023



Poglavlje 17: Mehanizam dojave grešaka – ICMP

Sastavili: Luka Grubišić i Robert Manger
01.12.2014

Uvod

- IP ostvaruje komunikaciju zasnovanu na traženju najboljeg rješenja (*best effort delivery*).
- Pritom IP ne garantira komunikaciju bez grešaka. Takvu garanciju daju tek viši slojevi u stogu protokola.
- Ipak, tijekom svog rada IP otkriva i dojavljuje greške.
- U ovom predavanju opisujemo mehanizam dojave grešaka koji je ugrađen u IP.
- Mehanizam se također pokazao korisnim za skupljanje informacija o mreži.

Semantika traženja najboljeg rješenja

- IP definira semantiku *best-effort communication* u kojoj je moguće da datagrami budu dupliciranI, izgubljeni, kasne ili stignu u slučajnom poretku.
- Moglo bi izgledati da za takvu vrstu komunikacije nije nužno imati mehanizam dojave grešaka.
- Ipak, IP pokušava spriječiti greške te dojaviti probleme kad do njih dođe.
- Primjer detekcije greške kojeg smo već vidjeli bilo je provjeravanje kontrolnog zbroja za zaglavlje IP datagrama.
- Ako se otkrije greška u kontrolnom zbroju, tada se cijeli datagram briše, bez slanja ikakve poruke o grešci. Ne može se ništa drugo učiniti zato jer se ne zna se je li IP adresa pošiljatelja korumpirana.

Internet Control Message Protocol ICMP (1)

- Problemi koji su manje rizični od greške u transmisiji se dojavljuju.
- U TCP/IP stogu protokola to rješava kolekcija protokola ICMP.
- Svaka standardna implementacija IP protokola mora sadržavati i ICMP protokole.
- IP i ICMP ovise jedan o drugom:
  - IP koristi ICMP kad šalje poruke o greškama;
  - ICMP koristi IP za transportiranje poruka.
- Osim za dojavu grešaka, ICMP poruke mogu služiti i za slanje drugih informacija.

Internet Control Message Protocol ICMP (2)

- Na slici vidimo popis svih ICMP poruka.

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20-29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37-255	Reserved

ICMP - poruke o greškama

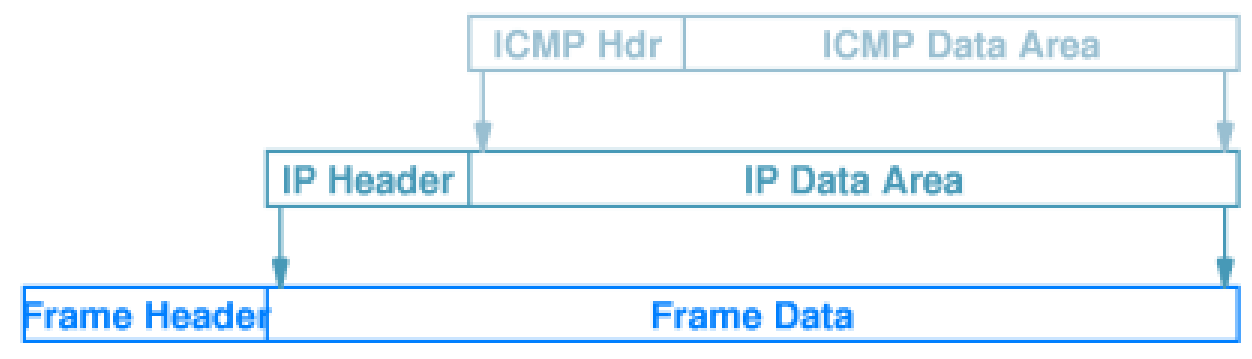
- Source Quench:Usmjernik šalje ovu poruku kada u njegovom spremniku nema dovoljno mjesta. Pošiljatelj mora reagirati smanjivanjem brzine generiranja novih datagrama.
- Time Exceded: Generira se kada je usmjernik spustio TIME TO LIVE na nulu ili kada host pri ponovnom sklapanju fragmentirane poruke prekorači REASEMBLY TIMER.
- Destination Unreachable: Šalje se kad usmjernik ustanovi da se datagram ne može isporučiti na svoje odredište. Iskazuje se razlika između nedostupnog hosta i nedostupne mreže.
- Redirect: Ukoliko usmjernik utvrdi da bi datagram trebao biti poslan po drugoj ruti, šalje ovu poruku. Može zahtijevati promjenu za host ili za mrežu.

ICMP - informativne poruke

- Echo Request/Reply: *Echo request* poruka može se slati ICMP software-u na bilo kojem čvoru. ICMP software mora reagirati slanjem *echo reply* poruke. Odgovor sadrži iste podatke kao i zahtjev.
- Address Mask Request/Reply: Prilikom svog *boot*-anja, host šalje *broadcast* upit o adresnoj masci. Usmjernik koji primi poruku šalje korektni 32-bitni broj koji sadrži adresnu masku za tu mrežu.

Slanje ICMP poruka

- ICMP koristi IP za slanje poruka.
- Koristi se dvostruka enkapsulacija, kao na slici.
- Datagrami s ICMP porukama nemaju posebni prioritet.
- Ako pri slanju i usmjeravanju same ICMP poruke dođe do greške, tada se ne šalje nikakva nova poruka o greški.



ICMP, ping i trace route (1)

- Ping koristi *echo request* da bi testirao dostupnost nekog host-a.
- Ping šalje *echo request* paket najviše dva puta. Ukoliko nema odgovora niti na ponovno poslani paket ili ako stigne poruka *destination unreachable,* ping deklarira da ne postoji put do udaljenog stroja.
- ICMP software po protokolu uvijek mora odgovoriti na *echo request* upit.
- Neki sistem inženjeri blokiraju ove odgovore iz sigurnosnih razloga.

ICMP, *ping* i *trace route* (2)

- Trace route koristi TIME TO LIVE polje u zaglavlju IP datagrama za ispitivanje puta između dva stroja.
- Generiraju se probni datagrami s TTL vrijednostima postavljenim na 1,2,...
- ICMP poruke *time exceeded* se koriste za određivanje liste usmjernika između početnog i krajnjeg čvora.
- ICMP poruka putuje u IP datagramu, pa je moguće iz IP zaglavlja odrediti IP adresu usmjernika koji je poslao ICMP poruku.

ICMP, *ping* i *trace route* (3)

- Trace route mora biti pripremljen za rješavanje problema duplikacije ili gubitka probnih datagrama, te stizanja odgovora u krivom redoslijedu.
- Teško je automatski izabrati vrijeme retransmisije probnog datagrama. Zato je to parametar kojeg korisnik sam određuje.
- Problem putova koji se dinamički mijenjaju nije lako riješiti. Trace route je najkorisniji u mrežama sa stabilnim putevima.
- Da bi dobio odgovor od konačnog odredišta, Trace route koristi jedan od sljedećih tipova probnih datagrama:
  - ICMP *echo request* poruka
  - UDP datagram nepostojećoj aplikaciji

ICMP, *ping* i *trace route* (4)

- *Microsoft*-ov tracert koristi prvi pristup. Tako kod svake retransmisije tracert prima ili ICMP *time exceeded* poruku ili ICMP *echo reply* od krajnjeg računala.
- UNIX-ov traceroute koristi UDP poruku (User Datagram Protocol) upućenu nepostojećem programu. Tako traceroute prima ICMP *time exceeded* ili ICMP *destination unreachable* od krajnjeg računala.
- Moguće je da pozivi tracert i traceroute generiraju različite odgovore na istim računalima.
  - *Echo reply* se šalje preko IP adrese sučelja preko kojega je stigao *echo request*.
  - Poruka o grešci pri slanju UDP poruke može ići i preko sučelja s drugom IP adresom (ukoliko ih ima na host-u).

ICMP i računanje MTU-a za put (1)

- Fragmentacija datagrama je postupak kojim se rješava problem slanja velikih datagrama kroz hetoregene mreže.
- Usmjernik troši CPU vrijeme na fragmentaciju.
- Moguće je optimizirati komunikaciju ukoliko se odredi najmanji MTU na putu u mreži, te se od aplikacije traži da šalje manje datagrame.
- Postoji FLAGS polje u IP zaglavlju koje osigurava da fragmentacija datagrama nije dozvoljena.
- ICMP poruka prenosi informaciju da je fragmentacija pokušana, ali nije bila dozvoljena.

ICMP i računanje MTU-a za put (2)

- MTU puta je najmanji MTU u nizu heterogenih mreža od polaznog do dolaznog host-a.
- IP software može odrediti MTU puta šaljući niz datagrama.
- Svaki datagram u zaglavlju ima označeno polje koje sprječava fragmentaciju, a njegova veličina varira tako da se odredi maksimalna veličina datagrama koja neće generirati ICMP poruku o neuspješnoj fragmentaciji.
- Putovi u Internetu su često stabilni nekoliko dana, pa ima smisla određivati MTU puta.

Sažetak

- Iako IP koristi semantiku najbolje usluge, u protokolu postoji mehanizam detekcije i dojave grešaka.
- Pored kontrolne sume za kontrolu zaglavlja, IP koristi niz protokola koji se zovu ICMP (Internet Control Message Protocol) za dojavu grešaka kao i za slanje informacija o mreži.
- ICMP protokol se može koristiti za testiranje interneta. Primjeri takvog korištenja su programi ping i traceroute. Daljnji primjer je slanje ICMP poruka u svrhu određivanja MTU-a za put.