

Projekt do předmětu SPS

**Nastavování hodnoty TTL v rozhraní Sockets
Nastavování Dont'fragment příznaku
Generování ICMP zpráv
Implementace Path MTP Discovery**

Martin Dařílek
dar022@vsb.cz

Úvod

Projekt si klade za cíl předvedení způsobu generování ICMP paketů a dále jejich příjem a dekodování. Jako praktická ukázka byla zvolena vlastní implementace programu *traceroute*, který slouží pro zjišťování komunikační cesty pro zadanou cílovou adresu.

Princip trasování paketu

Trasování funguje na principu nastavování hodnoty TTL (*Time To Live*) v hlavičce IP datagramu. Každý směrovač je povinen hodnotu TTL průchozího datagramu snížit o jedničku a pokud TTL dosáhne nuly, je datagram zničen a k odesílateli je vysláno chybové hlášení v podobě ICMP paketu (chyba *Time exceeded* – viz dále). Postupným zvyšováním hodnoty TTL tak lze zjišťovat směrovače, přes které datagram prochází. Generování paketů a inkrementování hodnoty TTL probíhá do okamžiku, dokud nezískáme odezvu od cílového počítače nebo dokud příslušný směrovač nenahlásí, že požadovaný cíl není dostupný.

ICMP datagram

V rámci trasování komunikační cesty lze s výhodou využít protokolu ICMP, který se používá pro diagnostiku sítě (přenos speciálních zpráv týkajících se chyb a jiných zvláštností při přenosu datagramů).

ICMP zapouzdřuje zprávy do IP datagramu:

Nové IP záhlaví	ICMP záhlaví	Původní IP záhlaví	8 oktetů původního IP datagramu
--------------------	--------------	-----------------------	---------------------------------------

Formát ICMP hlavičky:

Typ zprávy (8b)	Kód zprávy (8b)	Kontrolní součet (16b)
-----------------	-----------------	------------------------

Typů i kódů je pro ICMP protokol definována celá řada, v rámci projektu byly využity následující typy zpráv a kódy:

Typ	Význam
0	Echo reply – odpověď na žádost o odezvu (zpřesněno pomocí kódu)
3	Destination unreachable – cíl je nedostupný (cílový port, stanice, nebo síť jsou nedostupné), nebo byla nutná fragmentace, kterou ale příznak v hlavičce IP zakazoval
8	Echo request – žádost o odezvu
11	Time exceeded – překročena životnost datagramu (TTL dosáhlo hodnoty 0)

Kód	Význam
0	Network unreachable – síť není dosažitelná
1	Host unreachable – cíl není dostupný
3	Port unreachable – cíl je dostupný, ale specifikovaný port ne

Při zjišťování trasy tedy generujeme ICMP packet typu 8 (echo request), u kterého postupně inkrementujeme hodnotu TTL, a který je zasílán na cílovou adresu na neexistující port. Poté čekáme na odezvu (opět čekáme ICMP packet) a dekodováním zprávy určíme výsledek. Za úspěch lze považovat stav, kdy po určitém počtu inkrementací TTL přijde ICMP packet typu 0, s kódem 3 – tedy neexistující port na cílové stanici.

Implementace

Program je napsán v jazyce C/C++ a pro práci se síťovými prostředky využívá API knihovny Winsock. Tato knihovna je založena na využívání rozhraní *sockets*, stejně jako je tomu v prostředí unixových systémů, nicméně kvůli drobným odlišnostem není zdrojový kód přímo přenositelný bez dalších úprav.

Jako vývojové prostředí bylo použito IDE Dev-C++ (<http://www.bloodshed.net>), které využívá kompilátor MinGW (<http://www.mingw.org>).

Komentář k principu funkčnosti algoritmu

Trasování probíhá v následujících krocích:

- **Inicializace**
 - Kontrola parametrů (cílová adresa)
 - Kontrola verze Winsock (minimálně verze 2.x)
 - Dekódování cílové adresy pomocí funkce *gethostbyname()*, takže lze zadávat jak IP adresu tak i DNS název cíle
 - Inicializace socketu
 - Nastavení příznaku zákazu fragmentace, pomocí fce *setsockopt()*
 - Alokování paměti pro odesílaný ICMP paket a inicializace základních parametrů:
 - Typ – Echo Request
 - Kód 0
 - Identifikátor paketu (zvoleno číslo aktuálního procesu), pomocí kterého rozlišujeme příchozí ICMP pakety (abychom brali v úvahu jen ty, které jsme sami generovali)
- Trasování vygenerovaného paketu
 - Spočtení CRC ICMP
 - Nastavení aktuální TTL IP paketu - funkce *setsockopt()*
 - Odeslání paketu
 - Čekání určitou dobu na odezvu (timeout nastaven na 5s) – přijetí odpovědi
 - Při timeoutu čekání (odpověď nedorazila), se postupuje dál navýšením TTL
 - Pokud přijde odpověď je na výstup zalogována informace o odesílateli a testuje se typ a kód příchozího ICMP paketu.
 - Pokud je příchozí paket vyhodnocen jako odpověď od cílové stanice (nedosažitelný port) je program ukončen, jinak se navyšuje TTL a pokračuje se dál.

Příznak *Don't fragment*

Nastavením toho příznaku lze zakázat fragmentaci datagramu. Při cyklickém zvyšování délky datagramu tak lze např. testovat max. propustnost komunikační cesty k cíli. Dokud získáváme odezvu od cíle, lze zvyšovat délku datagramu až do okamžiku, než obdržíme ICMP paket typu 0, kód 4 (*Fragmentation needed*).

