IPv4 a protokol ICMP

Tato prezentace vysvětluje funkci a význam protokolu **ICMP (Internet Control Message Protocol)**, který je úzce spjat s IPv4. Dozvíme se, jak ICMP pomáhá s oznamováním chyb a diagnostikou sítě (např. příkazy ping a traceroute), jak fungují ICMP zprávy a proč je ICMP zásadní pro stabilní provoz internetu.

Seznámíme se s různými typy zpráv, jejich formáty a bezpečnostními aspekty.

Úvod do IPv4 a ICMP

IPv4 rekapitulace

- IPv4 je klíčový protokol na síťové vrstvě v modelu TCP/IP.
- Přenáší datagramy mezi sítěmi a určuje směrování.

Proč ICMP?

- IP samo o sobě nemá vestavěný mechanismus pro sdělování chyb či informací o doručování.
- ICMP proto doplňuje IP a umožňuje diagnostiku, oznamování chyb, řízení přenosu.

Pozice ICMP v modelu

- Funguje „nad“ IP, ale často se označuje jako součást síťové vrstvy, nebo „IPv4 control protocol“.

Základní principy ICMP

Typy a kódy

- Každá ICMP zpráva má typ a kód, které definují konkrétní význam (např. Echo Request = typ 8, Echo Reply = typ 0).

Hlavní funkce

1. **Chybové zprávy** – informují o nemožnosti doručit paket, zkažené hlavičce atd.
2. **Informační (diagnostické) zprávy** – ping (echo/echo reply), traceroute (time exceeded).

IP hlavička

- ICMP zpráva je zapouzdřena v IPv4 datagramu; IP protokol tedy dopraví ICMP zprávu k cíli.

Chybové zprávy ICMP

Destination Unreachable (typ 3)

- Oznamuje, že cíl není dosažitelný (např. síť nedostupná, port nedostupný).
- Různé kódy (0 = síť unreachable, 1 = host unreachable, 3 = port unreachable atd.).

Time Exceeded (typ 11)

- IP pole TTL (Time to Live) kleslo na 0 → router odhodí paket a pošle tuto ICMP zprávu zpět odesilateli.
- Používá se např. v traceroute pro zjištění cesty.

Source Quench (typ 4, historický)

- Dříve se používal k omezování toku dat (flow control), dnes prakticky nevyužívaný.

Redirect (typ 5)

- Router říká: „Měl bys posílat do jiného routeru, je to efektivnější cesta.“

Diagnostické zprávy – Echo Request / Echo Reply

Echo Request (typ 8), Echo Reply (typ 0)

- Slouží k ověření, zda je vzdálený uzel na síti živý a reaguje.
- Implementované v nástroji **ping**.

ping

- Program vyšle ICMP Echo Request, pokud cíl odpoví Echo Reply, víme, že je dostupný a měříme latenci.
- Např. ping 8.8.8.8 pro test dostupnosti DNS serveru Google.

Formát

- Zahrnuje identifikátor a sekvenční číslo → usnadnění spárování žádosti a odpovědi.

Traceroute a ICMP

Princip traceroute

- Odesílá IP pakety s postupně rostoucí hodnotou TTL (1, 2, 3 ...).
- Jakmile TTL klesne na 0, router pošle zpět zprávu **Time Exceeded** (typ 11).
- Nástroj tak postupně mapuje každý router na cestě k cíli.

ICMP / UDP verze

- V některých implementacích traceroute využívá UDP s neexistujícím portem, což vyvolá Destination Unreachable.
- Windows tracert používá ICMP Echo s proměnlivým TTL.

Bezpečnostní a provozní aspekty ICMP

ICMP blokování

- Někteří správci blokují ICMP (např. ping) z bezpečnostních důvodů – kvůli utajení sítě či ochraně před DoS.
- Ovšem úplné blokování ICMP může narušit normální funkci (Path MTU Discovery, atd.).

ICMP Flood (DoS útok)

- Útočník zasílá obrovské množství ICMP Echo Request, aby zahltil cílový systém.

Path MTU Discovery

- ICMP zpráva **Fragmentation Needed and DF** set (typ 3, kód 4) pomáhá zjišťovat největší MTU na trase.
- Blokování této zprávy může vést k poruchám přenosu.

Struktura ICMP zprávy

Hlavička ICMP

- **Type (8 bitů)**: druh ICMP zprávy.
- **Code (8 bitů)**: podkategorie zprávy.
- **Checksum (16 bitů)**: kontrolní součet.
- **Další pole**: u Echo Request/Reply např. identifikátor, sekvence; u Destination Unreachable část původního paketu.

Zapouzdření

- ICMP je vloženo do IP datagramu. IP header → ICMP header → ICMP data.

Shrnutí

ICMP slouží k:

1. **Oznámení chyb** (destination unreachable, time exceeded, redirect).
2. **Diagnostice** (ping – echo request/reply, traceroute).
3. **Podpoře** některých mechanismů (Path MTU Discovery).

Význam

- ICMP je nezbytný pro správnou funkci internetu a IPv4 sítí.
- Umožňuje identifikovat problémy s doručováním paketů a jejich trasou.

Doporučení

- Nezablokovat ICMP zcela, abychom nezpůsobili komplikace s diagnostikou a Path MTU Discovery.
- Řešit bezpečnost a nastavit filtry jen pro některé ICMP typy, je-li to nutné.

Kontrolní otázky

1. Proč byl protokol ICMP navržen a v čem doplňuje funkce samotného IP?
2. Jaké typy ICMP zpráv se využívají pro „ping“ a jaké kódy indikují nedostupnost cíle?
3. Vysvětlete, jak traceroute využívá ICMP (případně UDP) k mapování cesty.
4. Proč může úplné blokování ICMP zpráv narušit některé síťové funkce (např. Path MTU Discovery)?
5. Co znamenají zprávy typu „Destination Unreachable“ a „Time Exceeded“ a kdy mohou vznikat?
6. Jak by mohl útočník zneužít ICMP k DoS útoku a jak se lze bránit?

Kontrolní otázky

1. **Tanenbaum, A. S., Wetherall, D.**: *Počítačové sítě*, 5. vydání (v českém překladu) – Kapitoly o IP a ICMP.
2. **Kurose, J. F., Ross, K. W.**: *Computer Networking: A Top-Down Approach* – Přehled protokolu ICMP, ping, traceroute.
3. **Cisco Networking Academy**: *CCNA materiály* – Příklady ICMP ve směrování a diagnostice.
4. **RFC 792** – Původní specifikace ICMP pro IPv4.
5. **Další RFC** (např. RFC 950, 1191) – Path MTU Discovery a související ICMP zprávy.