# ICMP (Internet Control Message Protocol)

**ICMP** je nedílnou součástí protokolu IP. Zatímco IP se stará o doručení paketů z bodu A do bodu B, ICMP funguje jako „zpětná vazba“. Pokud paket nelze doručit, router nebo cílový hostitel pošle odesílateli ICMP zprávu s vysvětlením, co se stalo.

## 1. Klíčové funkce ICMP

- **Hlášení chyb:** Pokud je síť přetížena, cílový uzel je nedostupný nebo vypršela životnost paketu (TTL), ICMP o tom informuje odesílatele.
- **Diagnostika:** Umožňuje testovat, zda je konkrétní zařízení „naživu“ a jak rychle odpovídá.
- **Řízení toku:** Může informovat odesílatele, aby zpomalil vysílání dat (Source Quench - dnes již méně používané).

## 2. Nejpoužívanější nástroje

ICMP je základem dvou nejznámějších diagnostických utilit:

### Ping (Packet InterNet Groper)

Využívá zprávy typu **Echo Request** a **Echo Reply**.

```
1. Váš počítač pošle "Echo Request" na cílovou IP.
2. Cílový počítač odpoví "Echo Reply".
3. Výsledkem je informace o dostupnosti a latenci (RTT - Round Trip Time).
```

### Traceroute (Tracepath)

Slouží k mapování cesty paketu přes internet. Využívá zprávy **Time Exceeded**. Postupně posílá pakety se zvyšujícím se TTL (1, 2, 3...). Každý router na cestě TTL sníží na nulu, paket zahodí a pošle zpět ICMP zprávu, čímž o sobě dá vědět.

## 3. Struktura ICMP zprávy

ICMP zprávy jsou zapouzdřeny přímo v IP paketech. Každá zpráva obsahuje:

- **Type (Typ):** Hlavní kategorie (např. 8 pro Echo Request, 3 pro Destination Unreachable).
- **Code (Kód):** Podrobnější specifikace (u typu 3 může kód 1 znamenat „Host Unreachable“, kód 3 „Port Unreachable“).
- **Checksum:** Kontrolní součet pro ověření integrity zprávy.

# 4. Bezpečnostní rizika

Správci sítí často ICMP (nebo jeho část) na firewallech blokují. Proč?

- **Reconnaissance:** Útočníci používají ping ke zmapování aktivních zařízení v síti.
- **Smurf Attack:** Typ DDoS útoku zneužívající ICMP broadcast.
- **ICMP Tunneling:** Skrytí běžného datového provozu do ICMP zpráv pro obcházení firewallů.

# 5. ICMPv6 (pro IPv6)

V sítích IPv6 je ICMPv6 mnohem důležitější než v IPv4. Kromě hlášení chyb zajišťuje i:

- **Neighbor Discovery (NDP):** Náhrada za protokol ARP.
- **Multicast Listener Discovery:** Správa skupinového vysílání.
- **Path MTU Discovery:** Zjišťování maximální velikosti paketu na celé cestě.

> **Zajímavost:** Pokud dostanete chybu „Destination Unreachable (Port Unreachable)“, znamená to, že jste se pokusili připojit na UDP port, na kterém žádná aplikace nenaslouchá. U TCP byste místo toho dostali přímo TCP RST (reset) paket.

Zpět na Sítě