ICMPv6

ICMPv6 (Internet Control Message Protocol version 6) je **síťový protokol pro IPv6**, který slouží k přenosu řídicích a chybových zpráv v IPv6 sítích. Je to základní součást IPv6 a hraje zásadnější roli než ICMPv4 v IPv4.

Co je ICMPv6

ICMPv6 je protokol síťové vrstvy (Layer 3 v OSI modelu), který:

- Hlásí **chyby** při doručování paketů
- Poskytuje **diagnostické** funkce (ping, traceroute)
- Zajišťuje **Neighbor Discovery** (nahrazuje ARP z IPv4)
- Podporuje **automatickou konfiguraci** (SLAAC)
- Implementuje **Path MTU Discovery**
- Zpracovává **Multicast Listener Discovery** (MLD)

Základní informace:

- **Číslo protokolu:** 58 (v IPv6 hlavičce)
- **Standard:** RFC 4443 (hlavní), RFC 4861 (Neighbor Discovery)
- **Povinný:** Musí být implementován na všech IPv6 zařízeních
- **Nástupce:** ICMPv4 (IPv4)

Rozdíly oproti ICMPv4

ICMPv6 má **rozšířené funkce** oproti ICMPv4:

Funkce	ICMPv4	ICMPv6
Hlášení chyb	Ano	Ano
Ping/Echo	Ano	Ano
Neighbor Discovery	Ne (používá ARP)	**Ano**
Router Discovery	ICMP Router Discovery	**Integrováno**
Path MTU Discovery	Volitelné	**Povinné**
Multicast Management	IGMP (separátní)	**MLD (součást ICMPv6)**
Autokonfigurace	DHCP	**SLAAC + DHCPv6**

Struktura ICMPv6 paketu

```
IPv6 hlavička
+------------------+
| Next Header = 58 | (ICMPv6)
+------------------+
```

```
ICMPv6 hlavička
+------------------+
| Type (8 bitů)    | Typ zprávy (0-255)
+------------------+
| Code (8 bitů)    | Podtyp zprávy
+------------------+
| Checksum (16 b)  | Kontrolní součet
+------------------+
| Data (proměnná)  | Závislé na typu zprávy
+------------------+
```

Pole:

- **Type** - typ ICMPv6 zprávy (např. 128 = Echo Request)
- **Code** - upřesnění typu (většinou 0)
- **Checksum** - kontrolní součet pro detekci chyb
- **Data** - specifická data podle typu zprávy

Typy ICMPv6 zpráv

ICMPv6 zprávy se dělí do dvou hlavních kategorií:

1. Chybové zprávy (Error Messages)

Type hodnoty **1-127** jsou rezervovány pro chybové zprávy:

Type	Název	Význam
1	Destination Unreachable	Cíl nedosažitelný
2	Packet Too Big	Paket je příliš velký
3	Time Exceeded	Vypršel čas (TTL = 0)
4	Parameter Problem	Problém s hlavičkou paketu

Příklad - Destination Unreachable (Type 1):

Code hodnoty:

- 0 - No route to destination (žádná cesta)
- 1 - Communication administratively prohibited (zakázáno firewallem)
- 3 - Address unreachable (adresa nedosažitelná)
- 4 - Port unreachable (port nedostupný)

2. Informační zprávy (Informational Messages)

Type hodnoty **128-255** jsou pro informační zprávy:

Type	Název	Význam
128	Echo Request	Ping požadavek

Type	Název	Význam
129	Echo Reply	Ping odpověď
133	Router Solicitation	Hledání routeru
134	Router Advertisement	Oznámení routeru
135	Neighbor Solicitation	Hledání souseda (jako ARP)
136	Neighbor Advertisement	Odpověď souseda
137	Redirect	Přesměrování na lepší cestu

Neighbor Discovery Protocol (NDP)

Nejdůležitější funkce ICMPv6 - nahrazuje ARP, ICMP Router Discovery a další z IPv4.

Hlavní funkce NDP

1. Router Discovery - Nalezení routerů v síti

- Router Solicitation (Type 133) - „Kdo je tady router?“
- Router Advertisement (Type 134) - „Já jsem router, tady jsou parametry sítě“

2. Address Resolution - Zjištění MAC adresy (náhrada ARP)

- Neighbor Solicitation (Type 135) - „Kdo má IPv6 adresu X?“
- Neighbor Advertisement (Type 136) - „To jsem já, moje MAC je Y“

3. Duplicate Address Detection (DAD) - Kontrola, zda adresa již není používána

4. Redirect - Router řekne hostiteli o lepší cestě

Příklad: Address Resolution (náhrada ARP)

```
Hostitel A chce komunikovat s hostitelem B:

1. A pošle Neighbor Solicitation (Type 135):
   Src: fe80::1
   Dst: ff02::1:ff00:2 (solicited-node multicast)
   "Kdo má adresu 2001:db8::2? Pošli svoji MAC adresu!"

2. B odpoví Neighbor Advertisement (Type 136):
   Src: 2001:db8::2
   Dst: fe80::1
   "To jsem já! Moje MAC je 00:11:22:33:44:55"

3. A si uloží do Neighbor Cache:
   2001:db8::2 -> 00:11:22:33:44:55
```

Příklad: Router Discovery

```
Hostitel se připojí do sítě:

1. Hostitel pošle Router Solicitation (Type 133):
   Src: fe80::1
   Dst: ff02::2 (all-routers multicast)
   "Kdo je tady router?"

2. Router odpoví Router Advertisement (Type 134):
   Src: fe80::a
   Dst: ff02::1 (all-nodes multicast)
   "Já jsem router!"
   "Prefix: 2001:db8::/64"
   "Default gateway: fe80::a"
   "MTU: 1500"
   "Hop Limit: 64"

3. Hostitel si nakonfiguruje adresu pomocí SLAAC:
   2001:db8::1234:5678:9abc:def0/64
```

SLAAC (Stateless Address Autoconfiguration)

ICMPv6 umožňuje **automatickou konfiguraci IPv6 adres** bez DHCP serveru:

Proces SLAAC:

```
1. Hostitel vygeneruje link-local adresu:
   fe80::interface-id

2. DAD (Duplicate Address Detection):
   Neighbor Solicitation na vlastní adresu
   Pokud nikdo neodpoví -> adresa je unikátní

3. Router Discovery:
   Router Solicitation -> Router Advertisement
   Získá prefix sítě (např. 2001:db8::/64)

4. Vytvoření globální adresy:
   Prefix + interface-id = 2001:db8::interface-id

5. Konfigurace default gateway:
   Link-local adresa routeru (fe80::router-id)
```

Path MTU Discovery

ICMPv6 **povinně** implementuje PMTU Discovery (v IPv4 volitelné):

Jak funguje:

```
1. Hostitel pošle paket velikosti 1500 bytů

2. Někde na cestě je MTU pouze 1280 bytů

3. Router pošle ICMPv6 Packet Too Big (Type 2):
   "Váš paket je moc velký, maximální MTU je 1280"

4. Hostitel upraví velikost paketů na 1280 bytů

5. Pakety procházejí bez problémů
```

Důležité: IPv6 **neumožňuje fragmentaci** na routerech! Pouze odesílatel může fragmentovat.

Minimální MTU pro IPv6: 1280 bytů (povinné)

Multicast Listener Discovery (MLD)

MLD je součástí ICMPv6 a nahrazuje IGMP z IPv4. Používá se pro správu multicast skupin.

MLD zprávy:

- **Type 130** - Multicast Listener Query
- **Type 131** - Multicast Listener Report (MLDv1)
- **Type 132** - Multicast Listener Done (MLDv1)
- **Type 143** - MLDv2 Report

Ping v IPv6

Echo Request a Echo Reply fungují podobně jako v IPv4:

```
# Linux/Unix
ping6 2001:db8::1
ping6 -c 4 2001:db8::1

# Windows
ping 2001:db8::1
ping -6 2001:db8::1

# Ping link-local adresy (nutno zadat rozhraní)
ping6 fe80::1%eth0
```

ICMPv6 zprávy:

- **Type 128** - Echo Request (požadavek)
- **Type 129** - Echo Reply (odpověď)

Příklad výstupu:

```
PING 2001:db8::1(2001:db8::1) 56 data bytes
64 bytes from 2001:db8::1: icmp_seq=1 ttl=64 time=0.123 ms
64 bytes from 2001:db8::1: icmp_seq=2 ttl=64 time=0.098 ms
64 bytes from 2001:db8::1: icmp_seq=3 ttl=64 time=0.115 ms

--- 2001:db8::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss
```

Traceroute v IPv6

```
# Linux/Unix
traceroute6 2001:db8::1
tracepath6 2001:db8::1

# Windows
tracert 2001:db8::1
```

Princip:

- Postupně zvyšuje Hop Limit (TTL)
- Router vrací ICMPv6 Time Exceeded (Type 3)
- Ukazuje cestu paketu přes síť

ICMPv6 a bezpečnost

Důležitost ICMPv6

NIKDY neblokujte ICMPv6 kompletně! Na rozdíl od ICMPv4 je ICMPv6 kriticky důležité pro:

- Neighbor Discovery (bez něj síť nefunguje)
- Path MTU Discovery (bez něj problémy s velkými pakety)
- SLAAC (automatická konfigurace)

Doporučení pro firewall

Povolte minimálně tyto ICMPv6 zprávy:

Příchozí (Inbound):

- Type 1 (Destination Unreachable)
- Type 2 (Packet Too Big) - **kritické pro PMTU**
- Type 3, Code 0 (Time Exceeded)
- Type 128 (Echo Request) - pokud chcete odpovídat na ping
- Type 133 (Router Solicitation)

- Type 135 (Neighbor Solicitation) - **kritické pro NDP**

Odchozí (Outbound):

- Type 129 (Echo Reply)
- Type 134 (Router Advertisement) - pokud jste router
- Type 136 (Neighbor Advertisement) - **kritické pro NDP**

Bezpečnostní hrozby:

- **Rogue Router Advertisements** - falešné routery
- **Neighbor Discovery DoS** - záplavy NS/NA zpráv
- **SLAAC attacks** - útok na autokonfiguraci
- **ICMPv6 floods** - zahlcení zpráv

Ochrana:

- RA Guard - ochrana proti falešným routerům
- NDP Inspection - validace NDP zpráv
- Rate limiting - omezení množství ICMPv6 zpráv

Diagnostické nástroje

Linux/Unix:

```
# Sledování ICMPv6 provozu
tcpdump -i eth0 icmp6

# Filtrování konkrétních typů
tcpdump -i eth0 'icmp6 and ip6[40] == 135'  # Neighbor Solicitation

# Wireshark filtr
icmpv6.type == 135  # Neighbor Solicitation
icmpv6.type == 136  # Neighbor Advertisement

# Zobrazení Neighbor Cache
ip -6 neigh show
```

Windows:

```
# Neighbor Cache
netsh interface ipv6 show neighbors

# Interface konfigurace
netsh interface ipv6 show interface

# Route tabulka
netsh interface ipv6 show route
```

Příklad: Analýza ICMPv6 paketu

Neighbor Solicitation zachycený Wiresharkem:

```
Frame 42: 86 bytes on wire
Ethernet II
  Destination: 33:33:ff:00:00:01
  Source: 00:0c:29:3e:7f:a1
  Type: IPv6 (0x86dd)

Internet Protocol Version 6
  Source: fe80::20c:29ff:fe3e:7fa1
  Destination: ff02::1:ff00:1 (solicited-node multicast)
  Next Header: ICMPv6 (58)

Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x1234 [correct]
  Target Address: 2001:db8::1
  ICMPv6 Option (Source link-layer address)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: 00:0c:29:3e:7f:a1
```

Shrnutí

ICMPv6 je kriticky důležitý protokol pro IPv6:

Hlavní funkce:

- Hlášení chyb a diagnostika (ping, traceroute)
- **Neighbor Discovery** - náhrada ARP
- **Router Discovery** - nalezení default gateway
- **SLAAC** - automatická konfigurace bez DHCP
- **Path MTU Discovery** - detekce maximální velikosti paketu
- **Multicast** - správa multicast skupin (MLD)

Klíčové rozdíly oproti ICMPv4:

- Mnohem důležitější - **nesmí být blokován**
- Integruje funkce ARP, IGMP, DHCP
- Povinné pro všechna IPv6 zařízení
- Robustnější bezpečnostní mechanismy

Pamatujte:

- Bez ICMPv6 IPv6 síť **nefunguje**
- Vždy povolte minimálně NDP zprávy (Type 133-137)

- Path MTU Discovery vyžaduje Type 2 (Packet Too Big)