

Anycast

Anycast je síťová adresovací a směrovací metoda, při které jsou pakety z jednoho odesílatele směrovány k **nejbližšímu** uzlu ze skupiny potenciálních příjemců, kteří sdílejí stejnou IP adresu.

Na rozdíl od standardního směrování, kde jedna IP adresa odpovídá jednomu konkrétnímu zařízení, Anycast umožňuje existenci více identických cílů rozprostřených po celém světě.

Jak Anycast funguje?

Anycast využívá protokol **BGP** (Border Gateway Protocol) k propagaci stejné IP adresy (nebo celého prefixu) z různých míst internetu.

1. Více serverů v různých datacentrech (např. v Praze, New Yorku a Tokiu) oznámí do internetu stejnou IP adresu. 2. Směrovače (routery) v síti si tuto informaci uloží a vypočítají nejkratší cestu. 3. Když uživatel z Evropy pošle dotaz na tuto IP, routery jej automaticky nasměrují do Prahy, protože tato cesta má nejnižší metriku (obvykle počet skoků - hopů).

Srovnání metod směrování

V encyklopedii je užitečné srovnat Anycast s ostatními metodami:

Metoda	Popis	Použití
Unicast	Jeden odesílatel → jeden konkrétní příjemce (1:1).	Standardní prohlížení webu.
Broadcast	Jeden odesílatel → všichni v síti (1:all).	ARP dotazy v lokální síti.
Multicast	Jeden odesílatel → skupina přihlášených příjemců (1:many).	Streamování videa, IPTV.
Anycast	Jeden odesílatel → nejbližší z mnoha příjemců (1:1-z-mnoha).	DNS, CDN síť.

[Image comparing Unicast, Multicast, Broadcast and Anycast routing]

Hlavní výhody Anycastu

1. Nízká latence

Protože je uživatel vždy obslužen serverem, který je mu síťově nejbližší, odezva služby je minimální. To je kritické pro systémy jako DNS.

2. Vysoká dostupnost a redundance

Pokud jeden ze serverů v síti Anycast selže, BGP trasy se automaticky aktualizují a provoz je přeměrován na další nejbližší funkční server. Uživatel si výpadku často ani nevšimne.

3. Odolnost proti DDoS útokům

Anycast přirozeně „rozměňuje“ útok typu Distributed Denial of Service. Protože se útočný provoz směřuje na nejbližší uzly, útok z botnetu se rozprostře po celém světě a nezahltí jedno jediné místo.

Typické využití

- **DNS (Domain Name System):** Většina kořenových (root) DNS serverů a velkých poskytovatelů (jako Google 8.8.8.8 nebo Cloudflare 1.1.1.1) používá Anycast pro zajištění rychlosti a stability.
- **CDN (Content Delivery Networks):** Služby jako Cloudflare nebo Akamai využívají Anycast k tomu, aby uživatelům doručily statický obsah (obrázky, skripty) z nejbližšího „edge“ serveru.
- **Load Balancing:** Rozložení zátěže na globální úrovni bez nutnosti složitých DNS triků.

Omezení a nevýhody

- **Složitost konfigurace:** Vyžaduje pokročilé znalosti protokolu BGP a vlastní IP prefixy (vlastní AS - Autonomní systém).
- **Stavové protokoly (TCP):** Anycast je ideální pro bezstavové protokoly (UDP/DNS). U TCP může teoreticky dojít k „zakolísání“ trasy (route flapping) uprostřed spojení, což by vedlo k rozpadu relace, protože paket by dorazil na jiný fyzický server, který o spojení nic neví. Moderní implementace však tento problém efektivně řeší.

Související pojmy: IP adresa, BGP, DNS, CDN, Latence, DDoS.

From:
<https://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:
<https://serviceit.cz/doku.php?id=anycast>

Last update: **2025/12/31 18:58**

