# Sekundär DNS - sunic.sunet.se

## Ny förbättrad design

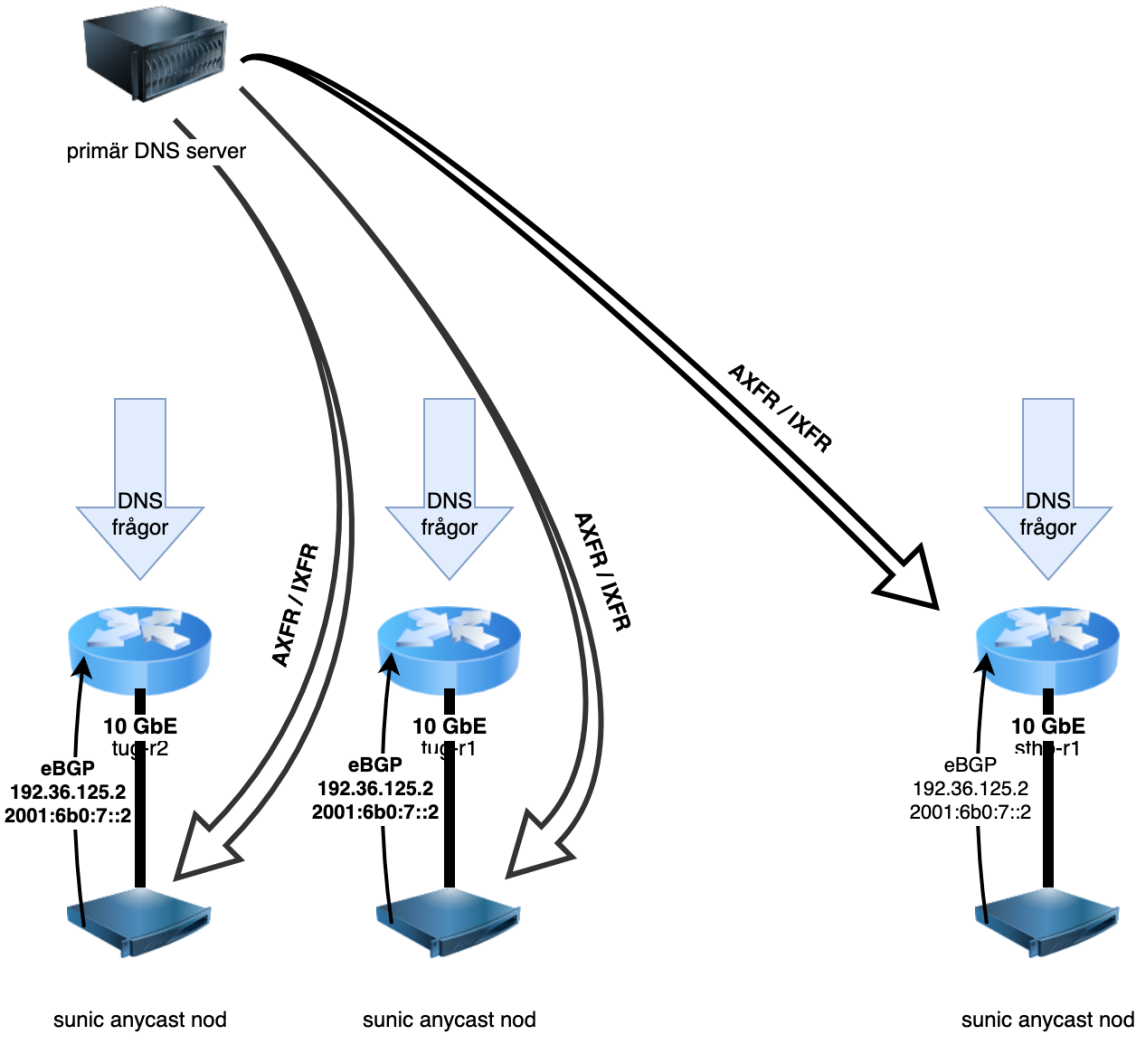
SUNIC.sunet.se har alltid varit **en** fysisk server sen starten (runt 1989) och det har fungerat bra då DNS (Domain Name System) har redundans inbyggd i standarden från början.

På senare tid har det dock blivit vanligare med störande trafik från en eller flertalet klienter som scannar nät & portar eller skickar orimligt mycket DNS-frågor ("brute-force") samt även de som försöker skapa DoS attacker ("Denial of Service") mot t.ex. DNS-servrar. SUNIC har historiskt ändå fungerat bra, och det är endast ett fåtal tillfällen som vi råkat ut för DoS-trafik som gjort att sunic.sunet.se DNS tjänst ej varit 100% tillgänglig. Med ökad trafik och ett flertal DoS-attacker som gamla generationens hårdvara inte klarade av,  så det blev hög tid att förnya det gamla konceptet med **en** fysisk server på ett delat LAN (Local area network).

## Ny design med aktiv (dynamisk) blockering

SUNIC har sedan många år använt sig av NSD som programvara för auktoritär DNS. SUNET har sponsrat NLnetLabs för att även NSD ska få proxyv2-protokoll-stöd, för att kunna sätta ett sk "frontend" programvara framför. Nu är det arbetet nästan helt klart. Vi har därför nu installerat programvaran dnsdist som DNS-frontend framför alla NSD-instanser, för att dynamiskt kunna blockera klienter beter sig illa och på nått sätt trakaserar SUNIC.sunet.se.

## Schemaskiss, senast uppdaterad installation




## Högre port-hastighet (10 GbE), Anycast för redundansen samt fler servrar som delar på lasten

Nya SUNICs upplänk är nu uppgraderad till 10 GbE, som dessutom är direktansluten i SUNETs routrar. Detta för att ta bort risken att en (D)DoS inte ska påverka ev. tjänster på det LAN som sunic tidigare varit anslutit till (Pilsnet).

SUNIC blir nu för första gången 3 st servrar (initialt), dels för lastdelning (teoretiskt 3x 10 GbE) samt för att få site-redundans. Tillsammans med övergången till anycast och "multi-server", så kommer det att ge möjligheten till avbrottsfritt underhåll av SUNIC-instanserna.

SUNIC IPv4/IPv6-adress blir nu Anycast (det är så lastdelningen löses enklast mellan olika instanser och olika fysiska lokationer). Det har länge varit vanligt att de större namnserver-installationerna har använt sig av Anycast för att kunna sprida lasten geografiskt. Drabbas en SUNIC-server av en större DDoS-attack, så påverkas bara en del av Internet-trafiken av att just den DNS-tjänsten inte är nåbar för tillfället.

## Framtida planer/ ytterligare förbättringar

Fler geografiskt skiljda instanser, och åtminstone en närmare "transit" (uppströms Internet-anslutningarna)