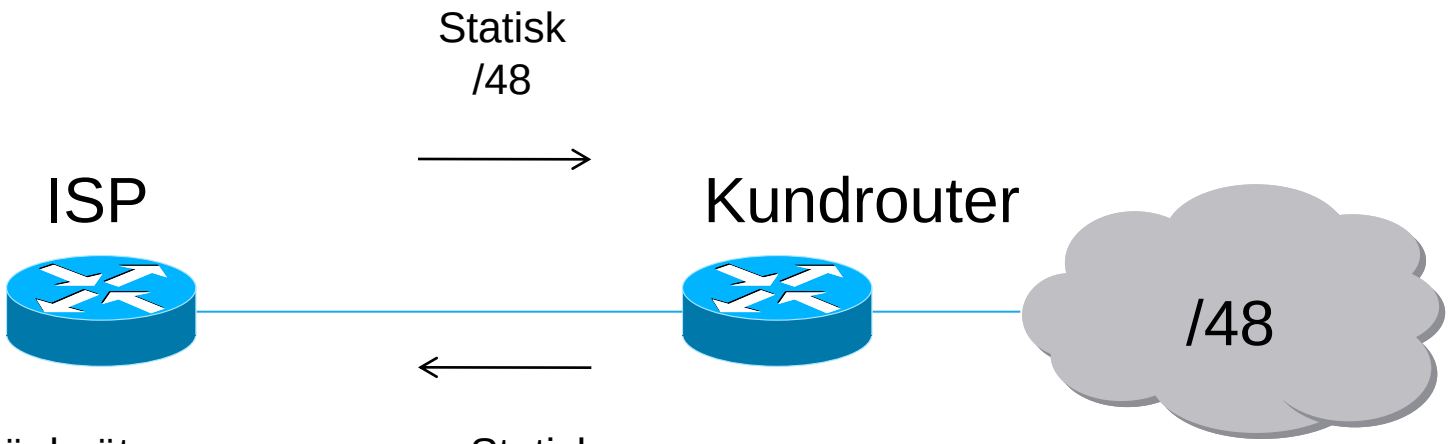
Olika varianter av IPv6-access

Mikael Abrahamsson
Tele2

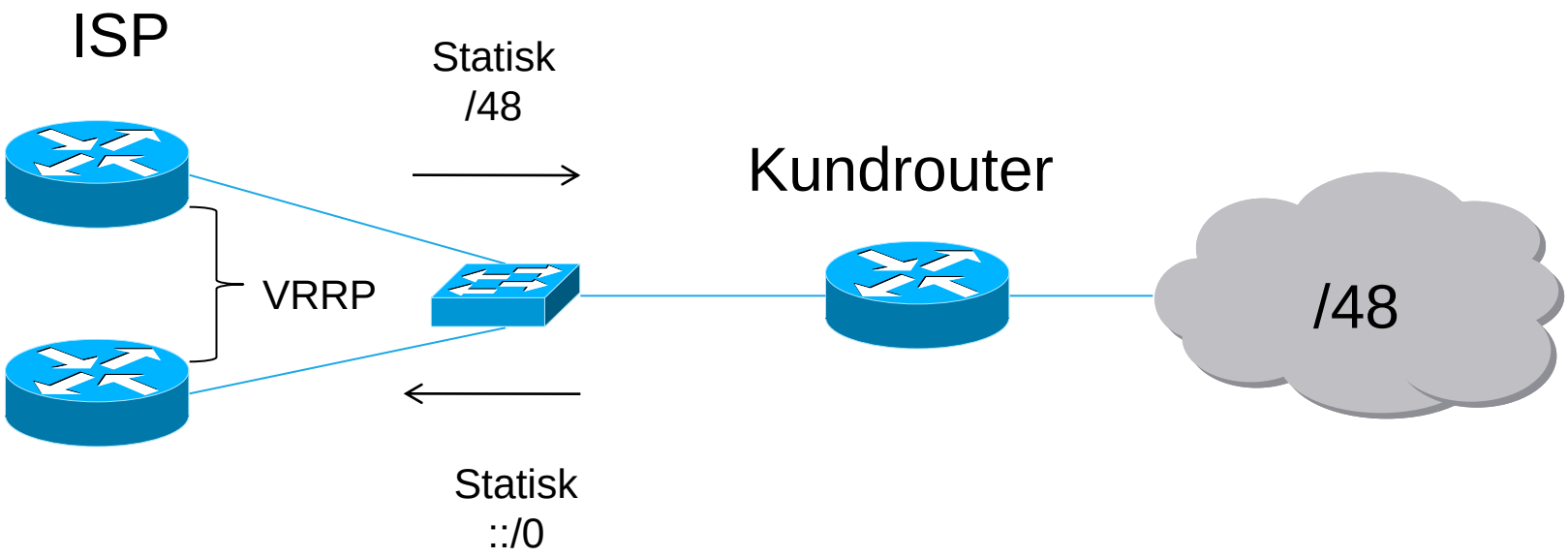
Företagsaccess



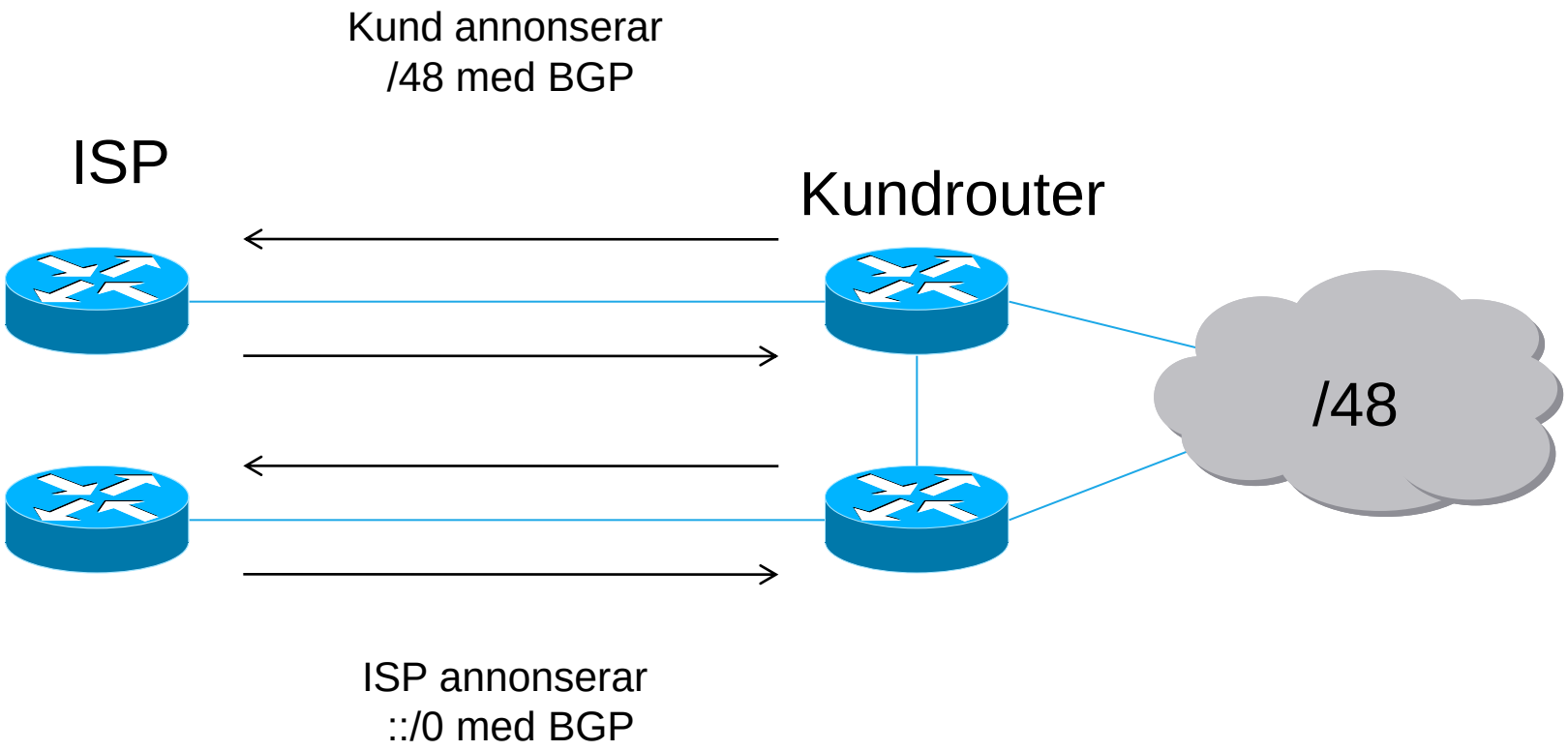
Statiskt länknät
Kan vara t ex:

- /127
- /126
- /125
- /120
- /112
- /64

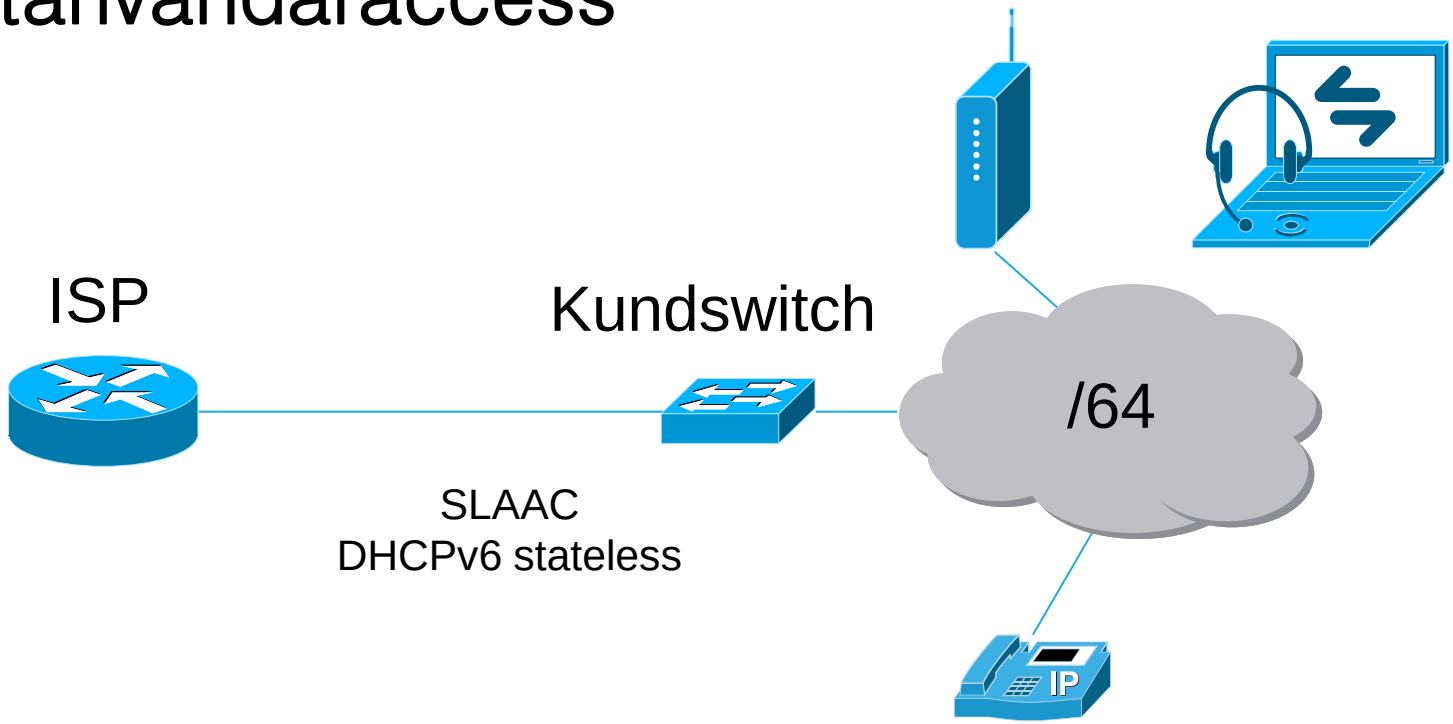
Redundant företagsaccess



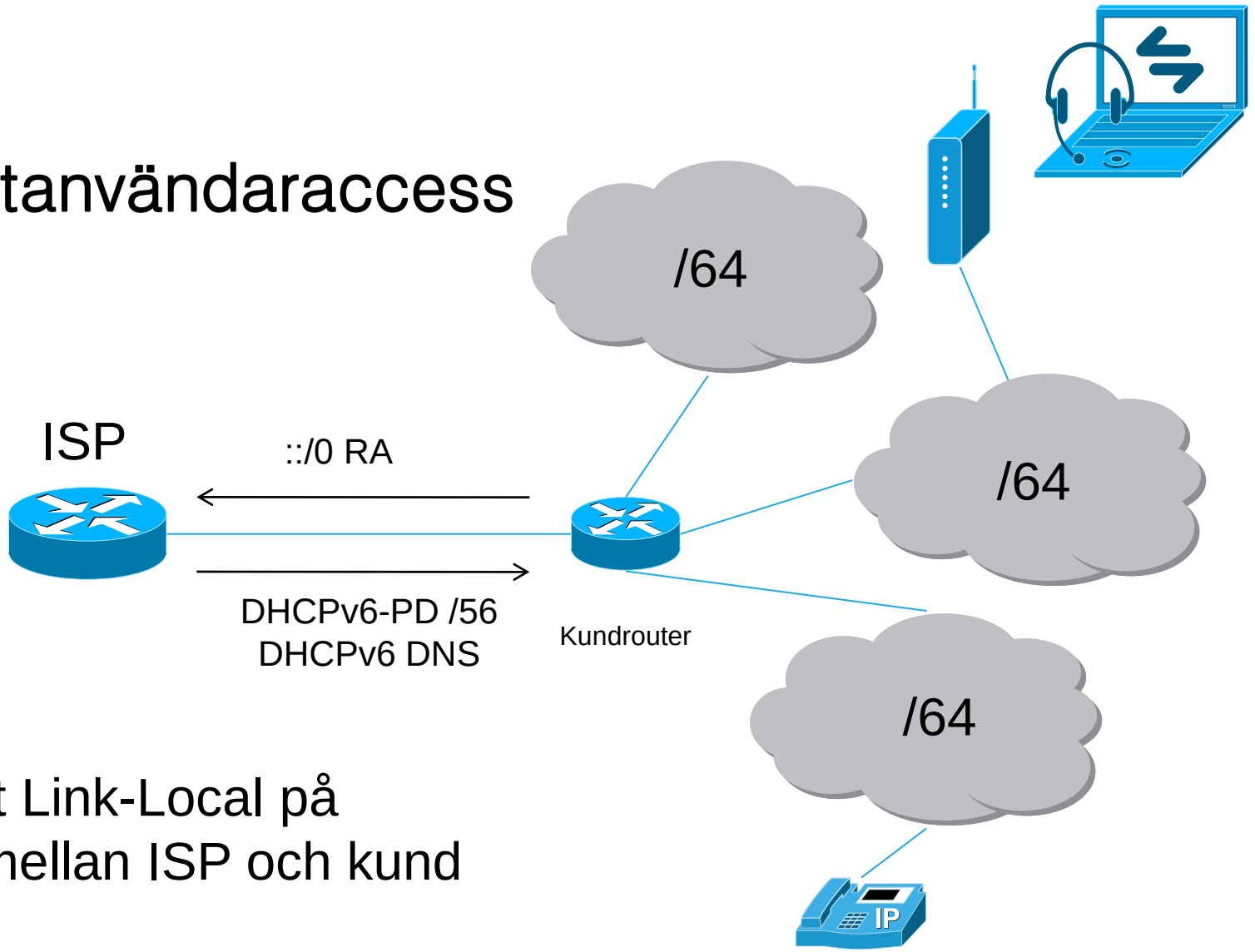
Redundant företagsaccess



Privatanvändaraccess

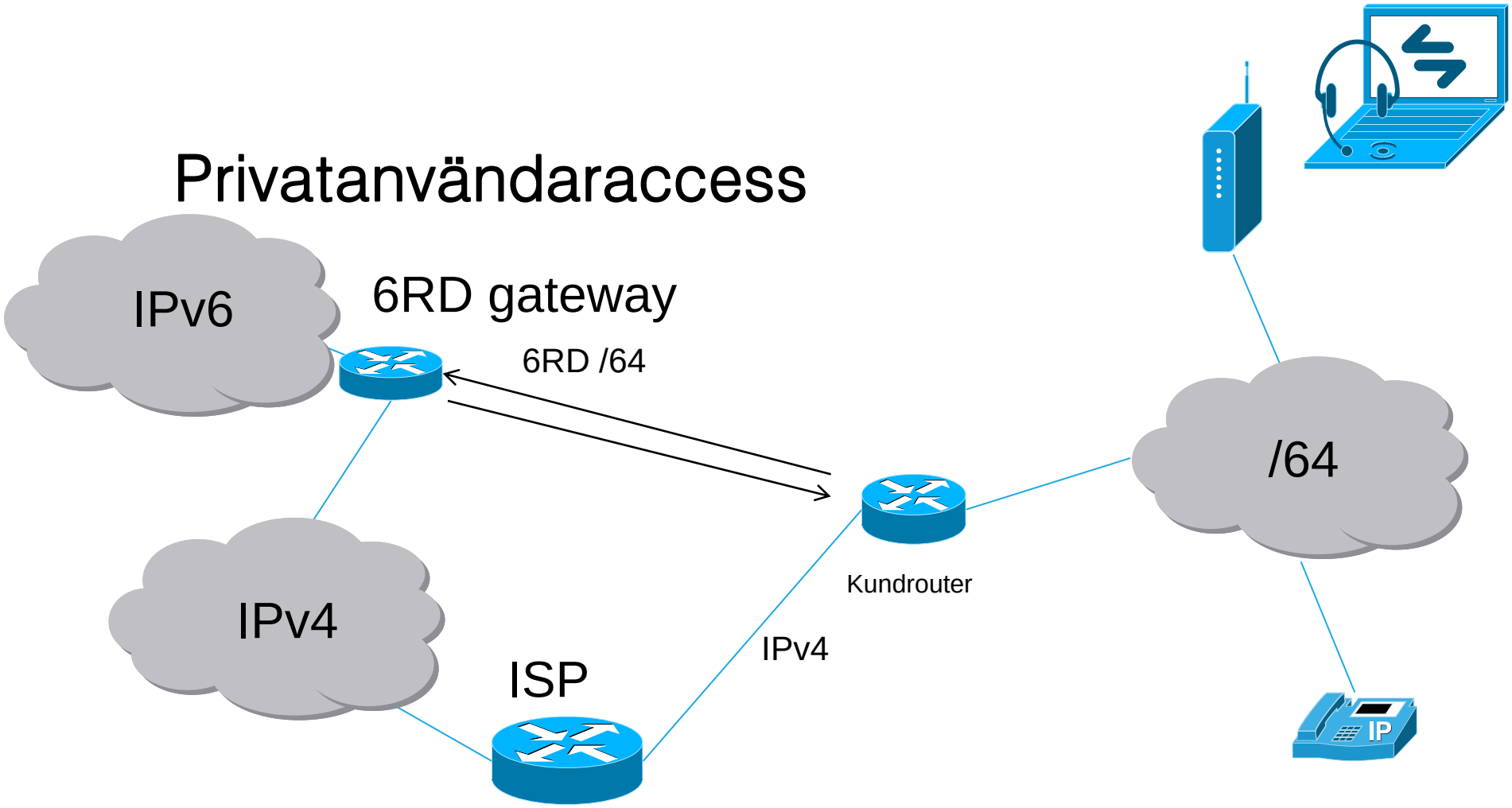


Privatanvändaraccess



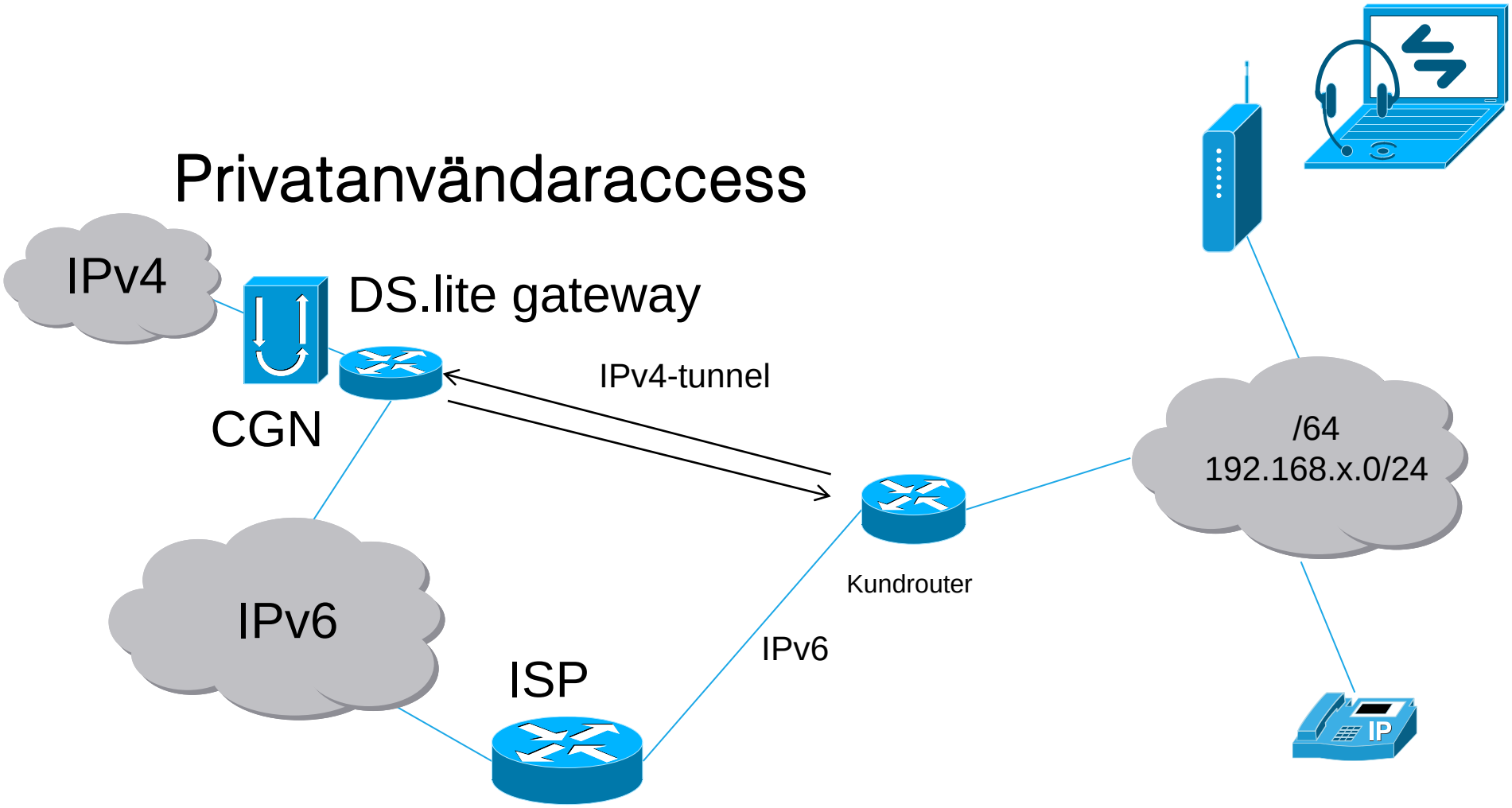
Enbart Link-Local på
Länknätet mellan ISP och kund

Privatanvändaraccess



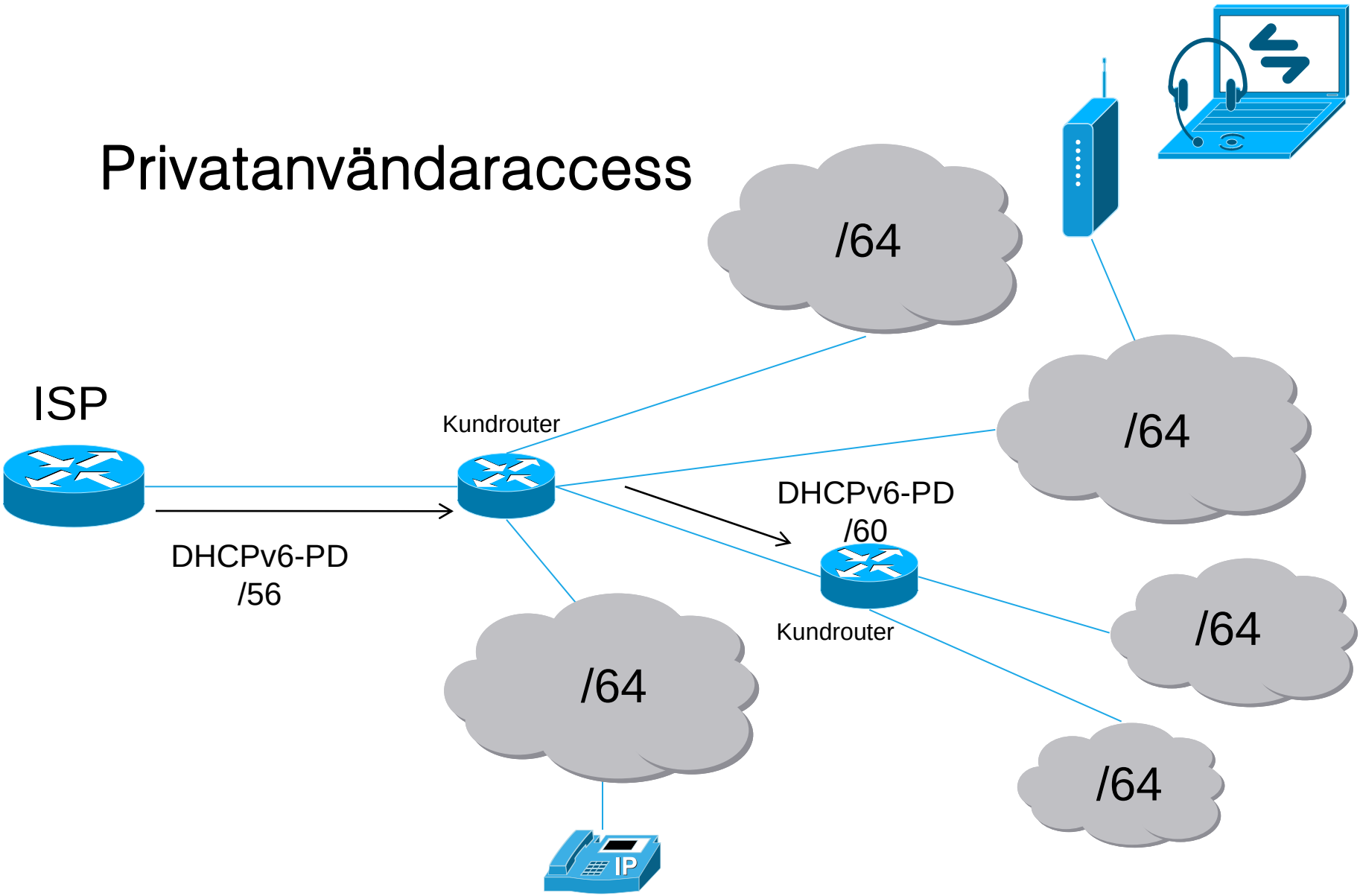
6RD = IPv6 över IPv4-access

Privatanvändaraccess

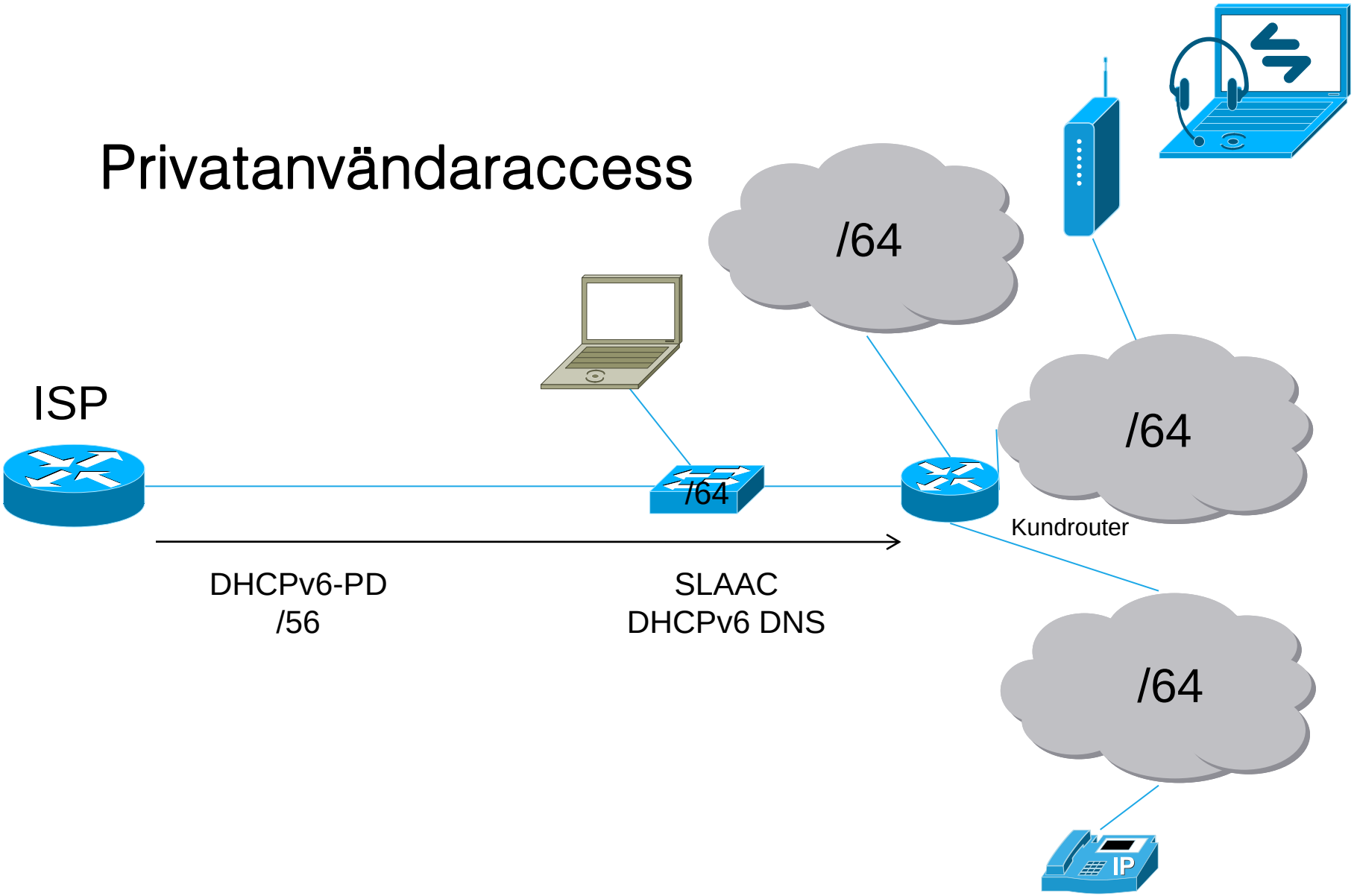


DS.lite = IPv4 över IPv6-access

Privatanvändaraccess



Privatanvändaraccess



Säkerhet

IETF SAVI WG – Source Address Validation Improvements

Presentation: draft-ietf-savi-threat-scope-05

För att skydda ”Internet” från enskilda användare

Hanterar bl a

- Man in the middle (MITM)
- Spoofing
- Flooding

Exempel på problem

SLAAC med /64: Maskiner får inte utdelat adresser, utan tar sig adresser. Problem med ND-skalning

- Maskin på lokala nätet kan ta sig 10000-tals adresser.
- Enhet på Internet skickar paket till 10000-tals adresser som inte används (storlek på ND-cache)

Spoofing

- Kund skickar paket med förfalskad avsändaradress
- Kan vara med ”Internet-adress”, kan vara lokal adress, kan försöka få andra att tro att den är gateway för att genomföra MITM (rogue RA)

Lösningar

- Varje kund får egen L2-domän och filtrering görs på L3. ISPns L3-enhet måste fortfarande kunna skydda sig själv
- L2-nätet får SAVI-funktionalitet, t ex:
  - RA-guard (skyddar mot t ex Windows 6to4 ICS-maskin)
  - DHCPv6-snooping (och filter baserat på detta)
  - SAVI-FCFS (first-come-first-serve för SLAAC-nät)
- DHCPv6-PD med enbart Link Local
  - Fördel att ISPns utrustning inte behöver hantera enskilda kundenheters adresser

Länknätsstorlek

/64 SLAAC möjligt

/112 Jämn sista fält

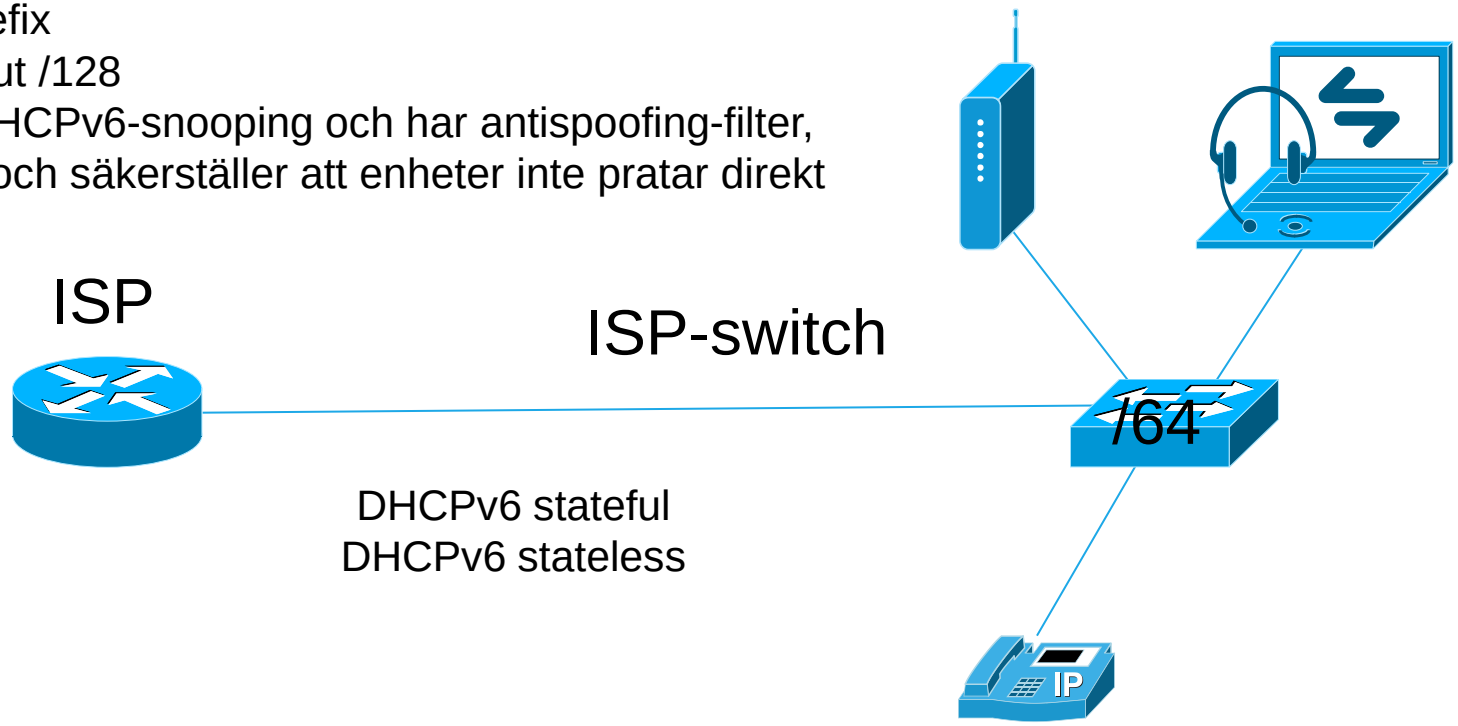
/125 Om man ska ha 4–6 enheter (t ex två routrar och VRRP)

/126 Minsta storleken med 2 enheter enl standard

/127 Föreslagen enl RFC, fungerar ofta redan idag

Delad access

- Router utannonserar sig som default gateway
- Inget on-net prefix
- DHCPv6 delar ut /128
- L2-enhet gör DHCPv6-snooping och har antispoofing-filter, RA-guard m m, och säkerställer att enheter inte pratar direkt med varandra



Användbara kombinationer

Med hjälp av RA kan man uppnå följande kombinationer:

- Inget on-net prefix == all trafik går via gateway
- Flagga för om on-net prefix får användas för SLAAC

  Om man vill köra DHCPv6 för adresser och inte tillåta SLAAC
- Flaggor (M och O) om DHCPv6 finns för adresser resp DNS-resolver
  M=Managed (för adresser) O=Other (annan information)