Engineer

# Netværksport

tallet, der vælger en tjeneste på en vært

## Hvad det er

En netværksport er et 16-bit tal i hovedet på hvert TCP- og UDP-segment, som fortæller den modtagende maskine, hvilket af dens programmer dataene skal til. Adressen bringer datapakken frem til den rigtige vært, og porten bringer den videre til den rigtige proces derinde. I daglig tale siger danske udviklere bare port eller portnummer, i flertal porte, og portene på en server er dem, den lytter på. Ordet har intet med de fysiske porte på en switch at gøre, og heller intet med at portere software til en anden platform.

Feltet er 16 bit bredt, så der findes 65.536 værdier fra 0 til 65535, og TCP og UDP har hver deres sæt: TCP-port 53 og UDP-port 53 er to forskellige ting, som DNS tilfældigvis bruger begge af. TCP-specifikationen, RFC 9293, definerer en socket som en internetadresse sat sammen med en port og en forbindelse som et par af sockets. Det giver fire værdier: klientens adresse, klientens port, serverens adresse og serverens port. Det forklarer også, hvorfor én serverport kan bære tusindvis af samtaler på samme tid. Hver samtale adskiller sig i mindst én af de tre andre værdier, som regel klientens port.

RFC 6335 deler intervallet i tre. Port 0–1023 er System Ports, 1024–49151 er User Ports, og 49152–65535 er Dynamic Ports, som IANA aldrig tildeler. IANA fører registret, der kobler et tjenestenavn til et nummer: 22 til SSH, 53 til DNS, 443 til HTTPS og 5432 til PostgreSQL. En registrering er en konvention, som klienterne regner med, og ethvert program kan lytte på et hvilket som helst ledigt nummer. Det er sådan, SSH ender på en port, ingen ville gætte.

Klientsiden af en forbindelse får som regel en port, den aldrig selv har valgt. Når et program forbinder udad, tager operativsystemet en fra sit interval af flygtige porte (ephemeral ports), og Linux bruger som standard 32768–60999 i stedet for

IANA's dynamiske interval. At bede om at binde port 0 betyder det samme: giv mig en hvilken som helst ledig.

Brug begrebet i en beslutning

Brug »Hvad er en netværksport?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Wi-Fi, firewalls og fjernadgang sat op, så medarbejdere kan arbejde hvor som helst, og kun de rette kommer ind.

**Se vores ydelser** Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har administreret 30 Ubuntu Linux VPS-instanser — 30 Linux-servere driftet, med en plan for gendannelse

**Har administreret 30 Ubuntu Linux VPS-instanser** Kontakt os →

## Hvorfor det betyder noget

Beslutningen bag hver port handler om eksponering: hvilke programmer der svarer udefra, og på hvilken adresse. En port uden lytter giver et afslag. En port med en lytter er et stykke software, som alle, der kan nå adressen, kan tale med, fejl og huller inklusive. Den billigste tjeneste at sikre er den, der lytter på 127.0.0.1, for pakker fra andre maskiner når aldrig frem til loopback-adressen, uanset hvad firewallen siger.

Det første spørgsmål for hver tjeneste er derfor, om den overhovedet skal kunne nås udefra. En database, som kun applikationen på samme maskine taler med, hører hjemme på loopback. Et værktøj, som kun administratorer bruger, kan ligge på loopback bag en jump host eller en VPN. Det, der er tilbage, typisk 80 og 443 til et website og én port til SSH, er den offentlige flade. At holde den kort er lige så meget et spørgsmål om omkostninger som om sikkerhed, for hver offentlig lytter skal patches, logges og have en firewallregel, der passer til den.

Det andet spørgsmål er nummeret. Standardporte koster ingenting i konfiguration: browsere, klienter og stramme netværk forventer 443 og lukker den igennem. At flytte SSH væk fra 22 dæmper støjen fra scannere, der kun prøver standardporten, så logfilerne bliver lettere at læse, men en skanning af hele intervallet finder den alligevel, og hvert værktøj, der henviser til porten, skal lære det nye nummer. Det sidste er det, teams glemmer.

Det tredje er rettigheder og deling. På Linux kræver det root eller capability'en CAP_NET_BIND_SERVICE at binde en port under 1024, medmindre ip_unprivileged_port_start er sat ned fra standardværdien 1024. Og normalt ejer

ét program en given adresse og port, så to tjenester, der begge vil have 443, skal have noget foran sig, der deler trafikken. Som regel er det en omvendt proxy, der læser det værtsnavn, klienten bad om.

## Sådan ser det ud i praksis

Tre stykker af virksomhedens infrastrukturarbejde drejer sig om portnumre: ét om, hvor en lytter står, ét om en port, der flyttede, og ét om at finde ud af, hvilke porte der faktisk er åbne.

Da virksomheden satte sin egen git-forge op i juli 2026, blev forgens SSH-lytter bundet til loopback på port 23231, og man kommer til den udefra via en jump host, så antallet af offentlige porte forblev det samme. En multiplexer, der kunne servere HTTPS og git over SSH fra en enkelt offentlig port, ud fra de første bytes i hver forbindelse, er skrevet og slået fra. En lytter uden brugere skulle stadig forsvares.

I august 2026 opdagede en hærdningsgennemgang, at SSH-dæmonen var flyttet til port 1986, da værten første gang blev hærdet, mens den jail, der skulle spærre angribere ude, blev ved med at holde øje med 22. Hver blokering, den skrev, gjaldt en port, hvor intet lyttede, så beskyttelsen havde aldrig virket en eneste gang. Rettelsen var lille. Det, der blev hængende, var en regel: hver sikkerhedskontrol følges af en assertion, der afprøver den.

Værten har 464 MB hukommelse og intet dashboard, så dens spørgsmål besvares af syv rapporteringsroller, der kun læser og gengiver den kørende maskine som Markdown. Faktarapporten lister de lyttende sockets, altså den portoversigt, kernen faktisk har, og ikke den, konfigurationen beskriver. Blandt de reelle fund i rapporterne var en lyttende port, som ingen erklæring nævnte.

## Hvor det går galt

**En tjeneste, der var tænkt til maskinen selv, svarer hele internettet.** Mange programmer lytter som standard på alle adresser, vist som `0.0.0.0`, `[::]` eller `*` i socketlisten, og en database eller et administrationspanel, der skulle være lokalt, er så én firewallfejl fra at ligge åbent. Sæt bindingsadressen eksplicit til `127.0.0.1` eller `::1`, og bekræft det i kolonnen med den lokale adresse:

```
ss -tlnp
ss -ulnp
```

**En beskyttelse holder øje med en port, tjenesten har forladt.** Tjenesten flyttede til et nyt nummer, og firewallreglen, jailen, overvågningsproben eller en klientkonfiguration nævner stadig det gamle. Hvert af værktøjerne arbejder korrekt videre mod en port, hvor ingen dæmon lytter. Hold nummeret i én variabel, som alle forbrugere læser, og tilføj en kontrol, der sammenligner den lyttende socket med det, hver beskyttelse holder øje med.

**Udgående forbindelser begynder at fejle under belastning med »Cannot assign requested address«.** Hver udgående forbindelse tager en lokal port fra det flygtige interval, og en lukket forbindelse holder sine fire værdier reserveret i TIME_WAIT et stykke tid efter. Med Linux' standardinterval på 32768–60999 kan én klientadresse have 28.232 forbindelser til den samme serveradresse og port, åbne eller nyligt lukkede. En proxy eller worker, der åbner en ny forbindelse for hver anmodning til én backend, løber tør. Genbrug forbindelser via keep-alive eller en pulje først; et bredere interval eller flere kildeadresser køber kun luft.

**En tjeneste, der startes som almindelig bruger, stopper med »Permission denied« på port 80.** At binde under 1024 kræver rettigheder. Giv tjenesten capability'en CAP_NET_BIND_SERVICE via dens unit-fil, læg den på en høj port bag en omvendt proxy, eller sæt ip_unprivileged_port_start ned på en vært, hvor alle lokale brugere er betroede. At køre hele tjenesten som root for at få én port er den dårligste byttehandel.

**Opstarten stopper med »Address already in use«.** En anden proces holder porten, ofte en gammel kopi af samme tjeneste, der stadig er ved at lukke ned, eller en anden tjeneste med samme standard (8080 er populær). `ss -tlnp` viser ejeren. Beslut, hvilken tjeneste der ejer nummeret, og giv hver tjeneste en eksplicit port i sin konfiguration i stedet for at stole på standarder.

## Læs mere

- RFC 9293, section 4: Glossary — TCP-specifikationens egne definitioner af port, socket og forbindelse.
- RFC 6335: IANA Procedures for the Management of the Service Name and Transport Protocol Port Number Registry — de tre portintervaller, og hvordan numrene i dem tildeles.

- Service Name and Transport Protocol Port Number Registry — IANA's liste over, hvilken tjeneste der er registreret på hvilket nummer.
- RFC 768: User Datagram Protocol — UDP-specifikationen på tre sider, kilde- og destinationsport inklusive.
- RFC 6056: Recommendations for Transport-Protocol Port Randomization — hvordan en klient bør vælge sine flygtige porte, så de er svære at gætte.
- IP Sysctl — Linux-kernens indstillinger, blandt dem ip_local_port_range og ip_unprivileged_port_start.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

**Se, hvad det koster** Kontakt os →

# Gør begreberne praktiske

Spørg, hvordan »Hvad er en netværksport?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

**Se vores ydelser**

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

**Lavet med kærlighed af D.**

**CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N**

**Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.**

**Udskrevet fra https://engineer.company/da/glossary/port/**