Engineer

Nätverksport

numret som pekar ut en tjänst på en värddator

Vad det är

En nätverksport är ett 16-bitars tal i huvudet på varje TCP- och UDP-segment, och talet säger åt den mottagande maskinen vilket av dess program datan ska till. Adressen tar paketet till rätt värddator; porten tar det till rätt process när det väl är framme. I vardagligt tal heter det bara port, portnummer när man vill vara exakt, och i plural, portar, menas oftast de som en server lyssnar på. Ordet har ingenting med den fysiska porten på en switch att göra, och inte heller med att porta programvara till en annan plattform.

Fältet är 16 bitar brett, så det rymmer 65 536 värden, från 0 till 65535, och TCP och UDP har var sin uppsättning: TCP-port 53 och UDP-port 53 är två skilda saker som DNS råkar använda båda två. TCP-specifikationen, RFC 9293, definierar en socket som en internetadress sammanfogad med en port, och en anslutning som ett par socketar. Det ger fyra värden: klientens adress, klientens port, serverns adress och serverns port. Det förklarar också hur en enda serverport kan bära tusentals samtal samtidigt. Varje samtal skiljer sig i minst ett av de tre andra värdena, oftast i klientporten.

RFC 6335 delar intervallet i tre. Portarna 0–1023 är systemportar (System Ports), 1024–49151 är användarportar (User Ports) och 49152–65535 är dynamiska portar (Dynamic Ports), som IANA aldrig tilldelar någon. IANA för registret som kopplar ett tjänstenamn till ett nummer: 22 för SSH, 53 för DNS, 443 för HTTPS och 5432 för PostgreSQL. En registrering är en konvention som klienter förlitar sig på. Vilket program som helst kan lyssna på vilket ledigt nummer som helst, och det är så SSH hamnar på en port som ingen skulle gissa.

Klientsidan av en anslutning får för det mesta en port som den aldrig har valt. När ett program ansluter utåt plockar operativsystemet en ur sitt intervall av tillfälliga portar (ephemeral ports), och Linux använder som standard 32768–

60999 i stället för IANA:s dynamiska intervall. Att be om att binda port 0 betyder samma sak: ge mig vilken ledig port som helst.

Använd begreppet i ett beslut

Använd ”Vad är en nätverksport?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Wi-Fi, brandväggar och fjärråtkomst uppsatta så att personalen kan arbeta varifrån som helst och bara rätt personer kommer in.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Förvaltade 30 VPS-instanser med Ubuntu Linux — 30 förvaltade Linux-servrar, med en plan för återställning

Förvaltade 30 VPS-instanser med Ubuntu Linux Hör av er →

Varför det spelar roll

Bakom varje port ligger ett beslut om exponering: vilka program som svarar utifrån, och på vilken adress. En port utan lyssnare ger ett avvisat anslutningsförsök. En port med en lyssnare är ett stycke mjukvara som vem som helst som når adressen kan prata med, buggar inräknade. Den billigaste tjänsten att säkra är den som lyssnar på 127.0.0.1, eftersom paket från andra maskiner aldrig når loopback-adressen, vad brandväggen än säger.

Den första frågan för varje tjänst är alltså om den över huvud taget behöver nås utifrån. En databas som bara applikationen på samma maskin pratar med hör hemma på loopback. Ett verktyg som bara administratörer använder kan också stanna på loopback och nås via en hoppserver eller ett VPN. Det som blir kvar, typiskt 80 och 443 för en webbplats och en port för SSH, är den publika ytan. Att hålla den kort är lika mycket ett kostnadsbeslut som ett säkerhetsbeslut, eftersom varje publik lyssnare ska patchas, loggas och ha en brandväggsregel som matchar den.

Den andra frågan är numret. Standardportar kostar ingenting i konfiguration: webbläsare, klienter och restriktiva nätverk räknar med 443 och släpper igenom den. Att flytta SSH från 22 minskar bruset från skannrar som bara provar standardporten, och loggarna blir lättare att läsa. Men en skanning av hela intervallet hittar den ändå, och varje verktyg som hänvisar till porten måste lära sig det nya numret. Det är den sista delen som team glömmer.

Den tredje gäller privilegier och delning. På Linux behöver en process root eller förmågan (capability) CAP_NET_BIND_SERVICE för att binda en port under 1024, om inte ip_unprivileged_port_start har sänkts från sitt standardvärde 1024.

Normalt äger dessutom ett enda program en viss kombination av adress och port, så två tjänster som båda vill ha 443 behöver något framför sig som delar upp trafiken. Oftast är det en omvänd proxy (reverse proxy) som läser vilket värdnamn klienten bad om.

Så ser det ut i praktiken

Tre delar av företagets infrastrukturarbete hänger på portnummer: en handlar om var en lyssnare sitter, en om en port som flyttade och en om att ta reda på vilka portar som faktiskt är öppna.

När företaget satte upp sin egen git-forge i juli 2026 lades forgens SSH-lyssnare på loopback-gränssnittet, port 23231, och den som sitter utanför når den via en hoppserver. Antalet publika portar stod därmed still. En multiplexer som skulle servera HTTPS och git över SSH från en och samma publika port, genom att titta på de första bytena i varje anslutning, är skriven och avslagen. En lyssnare som ingen använder skulle ändå behöva försvaras.

I augusti 2026 fann en härdningsgranskning att SSH hade flyttats till port 1986 under värdens första härdning, medan jailen som spärrar intrångsförsök fortsatte att bevaka 22. Varje spärr som jailen skrev gällde en port där ingenting lyssnade, så skyddet hade aldrig en enda gång slagit till. Åtgärden var liten. Det som blev kvar var en regel: varje säkerhetsskydd paras ihop med en kontroll som faktiskt prövar det.

Värden har 464 MB minne och ingen dashboard, så frågorna om den besvaras av sju rapportroller som bara läser och återger maskinen i drift som Markdown. Faktarapporten listar de lyssnande socketarna, alltså portarna så som de finns i en körande systemkärna och inte så som konfigurationen beskriver dem. Bland de verkliga saker som rapporterna har hittat fanns en lyssnande port som ingen deklaration nämnde.

Var det går fel

En tjänst som var tänkt för maskinen själv svarar hela internet. Många program lyssnar som standard på alla adresser, vilket syns som `0.0.0.0`, `[::]` eller `*` i socketlistan, och en databas eller adminpanel som skulle vara lokal är då ett enda brandväggsmisstag från att exponeras. Sätt bindningsadressen uttryckligen till `127.0.0.1` eller `::1` och bekräfta den i kolumnen för lokal adress:

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

Ett skydd fortsätter att bevaka en port som tjänsten har lämnat. Tjänsten flyttade till ett nytt nummer, och brandväggsregeln, jailen, sonden för övervakning eller en klientkonfiguration nämner fortfarande det gamla. Vart och ett av verktygen fortsätter att fungera korrekt mot en port där ingen daemon lyssnar. Håll numret i en enda variabel som alla som använder det läser, och lägg till en kontroll som jämför den lyssnande socketen med det som varje skydd bevakar.

Utgående anslutningar börjar fallera under last med ”Cannot assign requested address”. Varje utgående anslutning tar en lokal port ur det tillfälliga intervallet, och en stängd anslutning håller sina fyra värden reserverade i TIME_WAIT en stund efteråt. Med standardintervallet i Linux, 32768–60999, kan en klientadress hålla 28 232 anslutningar mot samma serveradress och port, öppna eller nyss stängda. En proxy eller arbetsprocess som öppnar en ny anslutning per begäran mot en och samma backend gör slut på dem. Återanvänd anslutningar med keep-alive eller en pool först; att bredda intervallet eller lägga till källadresser köper bara marginal.

En tjänst som startas som vanlig användare stannar med ”Permission denied” på port 80. Att binda under 1024 kräver privilegier. Ge tjänsten förmågan CAP_NET_BIND_SERVICE i dess unit-fil för systemd, lägg den på en hög port bakom en omvänd proxy eller, på en värd där varje lokal användare är betrodd, sänk ip_unprivileged_port_start. Att köra hela tjänsten som root för att komma åt en enda port är den sämsta av avvägningarna.

Starten stannar med ”Address already in use”. En annan process håller porten, ofta en gammal kopia av samma tjänst som fortfarande håller på att stänga ned, eller en andra tjänst med samma standardvärde (8080 är ett populärt). `ss -tlnp` visar vem som äger den. Bestäm vilken tjänst som äger numret och ge var och en en uttrycklig port i sin konfiguration, i stället för att förlita dig på standardvärden.

Läs mer

- RFC 9293, section 4: Glossary — TCP-specifikationens egna definitioner av port, socket och anslutning.

- RFC 6335: IANA Procedures for the Management of the Service Name and Transport Protocol Port Number Registry — de tre portintervallen och hur nummer inom dem tilldelas.
- Service Name and Transport Protocol Port Number Registry — IANA:s lista över vilken tjänst som är registrerad på vilket nummer.
- RFC 768: User Datagram Protocol — UDP-specifikationen på tre sidor, käll- och destinationsportar inräknade.
- RFC 6056: Recommendations for Transport-Protocol Port Randomization — hur en klient bör välja sina tillfälliga portar så att de blir svåra att gissa.
- IP Sysctl — inställningar i Linux-kärnan, bl.a. ip_local_port_range och ip_unprivileged_port_start.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är en nätverksport?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/port/