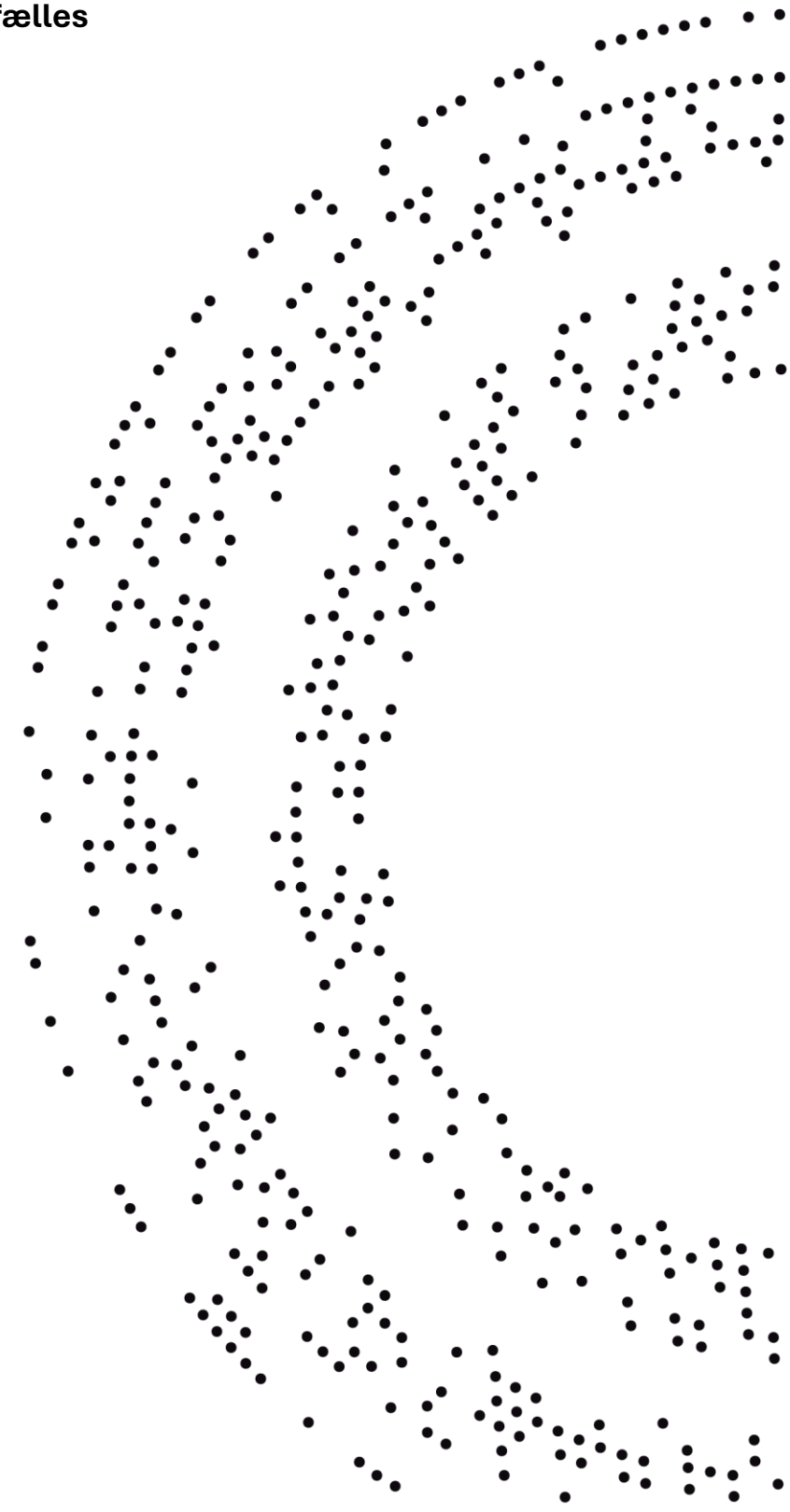
2.2 Teknisk målbillede – LAN/WAN

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3



Indhold

Dette dokument bygger på de arkitekturprincipper, der er fastlagt i hoveddokumentet, og som er kvalificeret gennem en analyse- og workshopfase med deltagelse fra relevante kommunale aktører. Principperne afspejler dermed både et fagligt perspektiv og de erfaringer og behov, der er identificeret på tværs af kommunerne.

Dokumentet består af udvalgte arkitekturprincipper og tilhørende anbefalinger baseret på erfaringer, analyser, best practice og standarder, som vurderes at være centrale for at understøtte en stabil, sikker og robust fælleskommunal IT-drift.

Dokumentet er et fagligt udgangspunkt for det videre arbejde med at etablere en konkret arkitektur og implementeringsplan i den enkelte IT-serviceorganisation. Dette arbejde forudsætter lokal tilpasning og skal gennemføres i samspil med ejerkommunerne samt med inddragelse af eksisterende producenter og leverandører, hvor det er relevant.

Det endelige ambitionsniveau for sikkerhed, drift og servicemodel fastlægges af den enkelte IT-serviceorganisation på baggrund af ejerkommuners behov, prioriteringer og risikovurderinger.

1 Introduktion

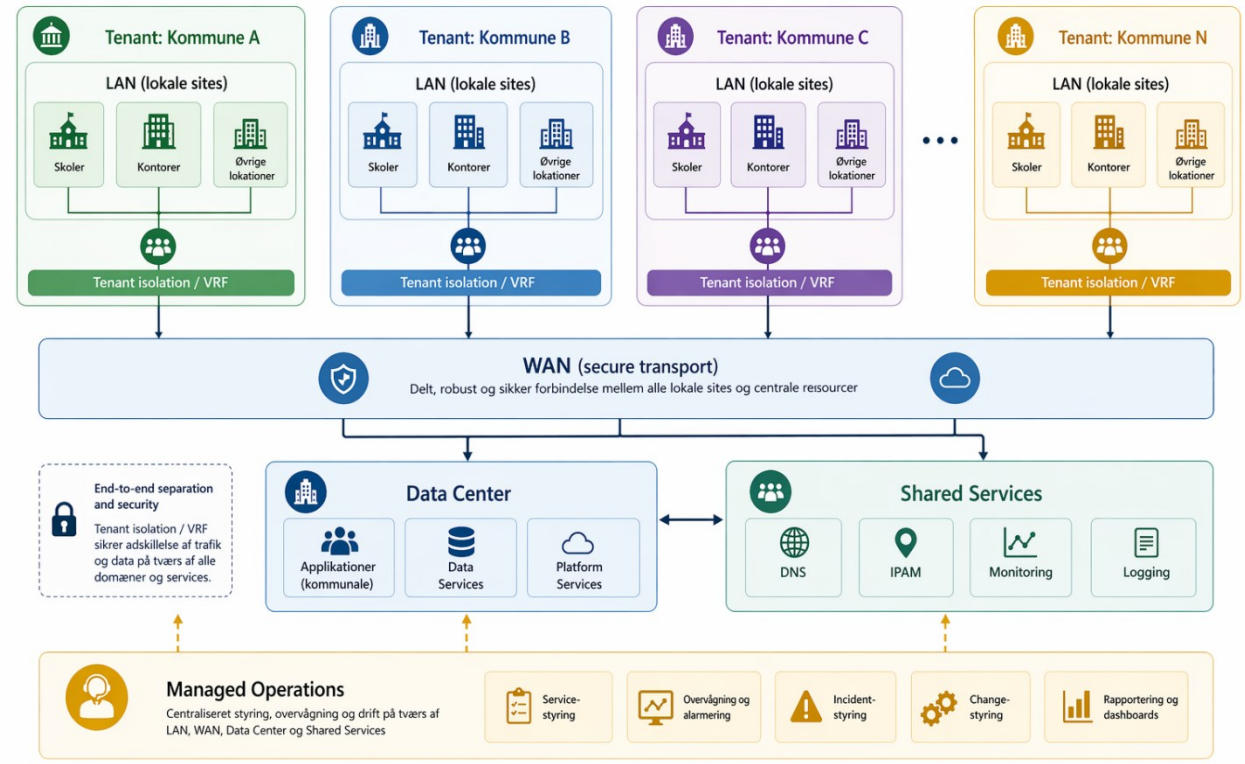
Dette dokument definerer det tekniske målbillede for fælleskommunal LAN/WAN drift i forbindelse med konsolideringen af kommunal IT-infrastruktur under de 5 tværkommunale IT-serviceorganisationer. Dokumentet er udarbejdet på baggrund af en samlet analyse af KL's strategiske arkitekturramme, modenhedsvurderingsmodeller, arkitekturprincipper, tekniske minimumskrav samt udkast til opgavesnit og transitionsplanlægning.

LAN/WAN-anbefalingerne er baseret på behovet for at kunne drive et meget varieret infrastrukturlandskab som én samlet platform. Derfor fokuserer målbilledet på standardiserede designprincipper, segmentering og centraliseret styring, som reducerer kompleksitet, øger sikkerheden og gør det muligt at skalere driften uden tilsvarende stigning i ressourceforbrug. Målbilledet er struktureret omkring fire strategiske søjler, der tilsammen udgør grundlaget for en sikker, skalerbar og standardiseret fælleskommunal drift:

1. Sikkerhed: NIS2-compliant cybersikkerhed med krypteret datatransport, tenant separeret SIEM, 802.1X-baseret adgangskontrol og systematisk kategorisering af systemer.
2. Standardisering: Ensartet netværksdesign baseret på hierarkiske modeller, centraliseret IPAM, standardiserede routingprotokoller og formaliseret hardware livscyklus.
3. Konsolidering: multi-tenant datacenterarkitektur, ensartede topologiprofiler og kategorier, Infrastructure as Code og automatisering.
4. Segmentering: VRF baseret makrosegmentering for juridisk dataisolation, mikrosegmentering for kategoriserede systemer og standardiseret zonemodellering.

Det er dokumentets overordnede betragtning, at de fire søjler tilsammen etablerer det tekniske og operationelle fundament for en *Network as a Service (NaaS)* leverancemodel, hvor IT-serviceorganisationerne leverer sikker, standardiseret connectivity som en fuldt managed ydelse til de enkelte kommuner. I denne model ejer og driver IT-serviceorganisationen al netværksinfrastruktur, og ejerkommunen modtager differentieret secure connectivity tilpasset den enkelte afdelings behov og systemkategorisering. NaaS modellen udfoldes i kapitel 7 som dokumentets visionære perspektiv.

I læsevejledningen til denne dokumentpakke findes begrebsforklaringer og kildehenvisninger.



Figur 1 – Målarkitektur

Det anbefales, at hver kommune gennemfører en modenhedsvurdering baseret på den integrerede scoringsmodel (27 vurderingsområder, score 27–135), hvorefter individuelle transitionsplaner udarbejdes med prioriterede leverancer.

2 Nuværende situation (as-is kortlægning)

2.1 Overordnet landskab

As-is kortlægningen, gennemført i efteråret 2025, har afdækket et kommunalt netværkslandskab præget af betydelig heterogenitet. De 98 kommuner råder tilsammen over en infrastruktur bestående af ca. 13.500 fysiske lokationer, 150.000 access points, 45.000 routere og switches samt 400 firewalls. Hertil kommer, at 70 ud af 98 kommuner driver egne fiberforbindelser.

Det vurderes, at denne infrastruktur repræsenterer en betydelig variation i både teknologivalg, kompetenceniveau og modenhedsgrad. Mange kommunale netværk kan være udviklet gradvist over tid, ofte med fokus på løbende behov frem for et samlet arkitekturprincip, hvilket medfører fragmenterede løsninger med begrænset skalerbarhed og dokumentation. Denne variation kan i nogle tilfælde udgøre en udfordring i forhold til at levere connectivity som en mere standardiseret, managed ydelse.

2.2 Forventede variationer og modenhedsforskelle

a) Netværksarkitektur og design

Det vurderes, at der kan være markante forskelle i netværksarkitekturen på tværs af kommunerne. Nogle opererer med fuldt modulært design med definerede byggeblokke (campus-, datacenter-, WAN edge- og DMZ moduler), mens andre vil have netværk, der er vokset ad hoc uden overordnet arkitekturprincip. Hierarkiske modeller (core/distribution/access) forventes hyppigst forekommende konsistent implementeret i de større kommuner. Hardware standardisering kan variere fra formaliserede produktporteføljer med lifecycle styring til heterogene miljøer med udstyr fra adskillige generationer og leverandører. Denne variation vanskeliggør en ensartet serviceleverance og forhindrer skalerbar drift.

b) Segmentering og sikkerhed

Segmenteringsniveauet vil variere fra avanceret VRF baseret multi-tenancy til helt flade netværk uden logisk adskillelse. Mikrosegmentering med granulære sikkerhedszoner ses sjældent implementeret. 802.1X-baseret netværksadgangskontrol (NAC) er typisk aktiveret for trådløst netværk, men sjældent konsistent på kablede porte. Systematisk kategorisering af systemer efter kritikalitet og dataklassifikation er ofte fraværende eller ikke formaliseret. Uden en konsistent kategoriseringsmodel er det ikke muligt at levere differentierede serviceniveauer til forskellige kommunale funktionsområder – en forudsætning for en operationel effektiv og skalerbar NaaS model.

c) IP-adressering, routing og sporbarhed

Det forventes, at et betydeligt antal kommuner anvender overlappende RFC 1918-adresserum, potentielt også internt mellem segmenter (VRF'er). Anvendelsen af central IPAM forventes at være undtagelsen snarere end normen. DNS arkitekturen er muligvis fragmenteret med lokale servere uden

central delegering, og DNS sikkerhed er sjældent implementeret. Routing kan ventes at være baseret på statiske ruter uden redundans. Overlappende adresserum udgør en direkte transitionsbarriere for etablering af centraliserede NaaS services, idet management på tværs af tenants forudsætter entydige IP-allokeringer for konsistent tilgængelighed.

d) WAN og transport

WAN teknologivalg varierer fra selv ejede fiberforbindelser til SD-WAN med central orkestrering over imod simple internetbaserede VPN-tunneler. Kryptering af *data in motion* er ikke konsistent implementeret – især MPLS-trafik vil ofte sendes ukrypteret. QoS er sjældent implementeret end-to-end, og WAN redundans er primært tilgængelig for større lokationer. I en NaaS kontekst er transportkvalitet og -sikkerhed en integreret del af den ydelse, IT-serviceorganisationen påtager sig ansvar for – SLA-baseret tilgængelighed, QoS og krypteret transport er derfor grundlæggende krav.

e) Sikker management og overvågning

Usikre managementprotokoller (Telnet, SNMPv1/v2c, ukrypteret syslog) forventes fortsat i brug i en række kommuner. Centraliseret AAA med individuelle brugerkonti og RBAC kan være undtagelsen, mens delte lokale adgangskoder forventes udbredt. SIEM integration er begrænset, og auditeringsprocesser og -politikker er sjældent på plads. I transitionsfasen forudsættes det, at kommunernes eksisterende lognings- og overvågningssetup er struktureret og dokumenteret på en måde, der muliggør indpasning i en fælles SIEM løsning med tenant separation under IT-serviceorganisationens ansvar, og at IT-serviceorganisationen har fuld operationel synlighed og kontrol. Centraliseret, sikker management er en forudsætning for at kunne garantere serviceaftaler og sikre lav *Meantime-to-Repair (MTTR)*.

f) Governance og automatisering

Infrastructure as Code (IaC) og netværksautomatisering er i de fleste kommuner på et tidligt stadie eller endnu ikke i overvejelserne. Konfigurationsstyring med versionering og *drift-detection* er sjælden. Dokumentation vil ofte være forældet og personafhængig. Automatisering er den primære katalysator for stordrift og dermed for en NaaS model – uden automatiseret provisionering, overvågning og konfigurationsstyring kan IT-serviceorganisationerne ikke opnå den operationelle skalerbarhed, der kræves for at betjene 98 kommuner med en standardiseret ydelse. Dokumentation er et vigtigt element i at kunne udarbejde en transitionsplan.

2.3 Overordnet modenhedsvurdering

På baggrund af den samlede analyse vurderes det, at hovedparten af kommunerne befinder sig i det gule scoringsinterval (62–111 point ud af 135 mulige), svarende til et funktionelt fundament med identificerede gaps. Disse kommuner vurderes generelt i stand til at indgå i en managed LAN/WAN driftsmodel, men med behov for målrettede tekniske og organisatoriske tilpasninger forud for eller som del af driftsovertagelsen.

Et mindre antal kommuner vurderes at befinde sig i det røde interval (27–61 point), hvor den nuværende LAN/WAN arkitektur endnu ikke understøtter konsolideret drift i tilstrækkelig grad. For disse kommuner vil konsolidering forudsætte en grundlæggende transformationsindsats, herunder styrket standardisering, dokumentation, segmentering og governance, før driftsovertagelse kan gennemføres på forsvarlig vis.

Kun et fåtal kommuner vurderes at være konsolideringsparate i det grønne interval (112–135 point). Disse kommuner har et modent LAN/WAN fundament med høj grad af standardisering, styring og teknisk sammenhæng, som gør det muligt at overgå til fælles drift med begrænsede forudgående tilpasninger.

Set i et LAN/WAN perspektiv understreger modenhedsfordelingen, at konsolideringsparathed varierer betydeligt, og at transitionen mod en fælles managed driftsmodel og et muligt NaaS scenarie kræver differentierede transitionsplaner. Kommuner med lavere modenhed prioriteres med større opgraderings- og modningsindsatser, mens kommuner med højere modenhed tidligere kan indgå i konsolideret drift og fungere som reference- eller pilotkommuner i den videre modningsrejse

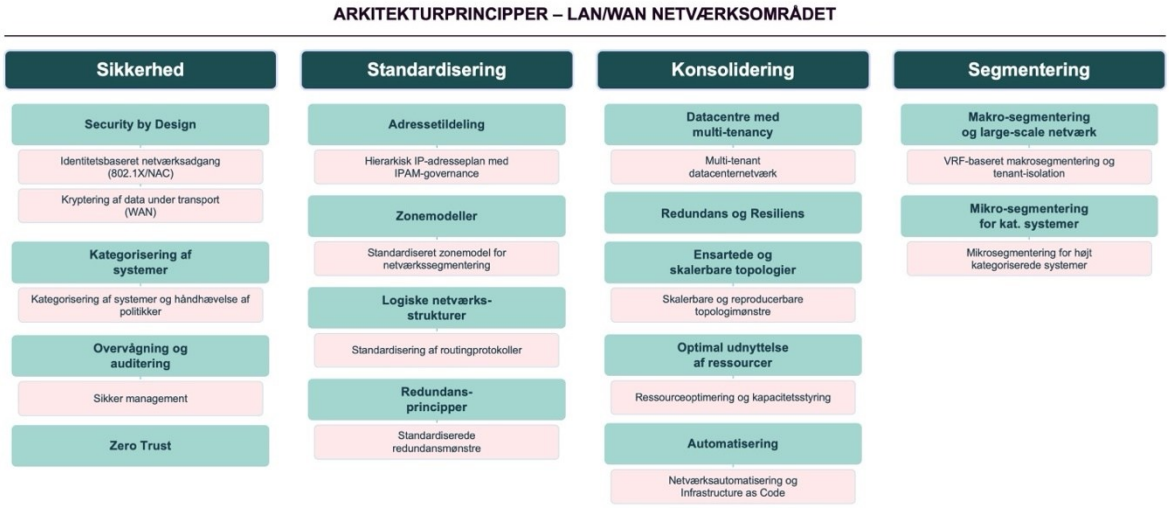
3 Arkitekturprincipper

De følgende arkitekturprincipper beskriver den ønskede målarkitektur for fælleskommunal LAN/WAN drift i en fuldt etableret IT-serviceorganisation. Principperne udtrykker den tilstand, hvor kommuner og IT-serviceorganisationer er konsolideret omkring fælles standarder, sikkerhedsmodeller og driftsprocesser, og hvor Network as a Service leverancemodellen kan fungere som tilsigtet.

Principperne skal læses som et fælles pejlemærke for både kommuner og IT-serviceorganisationer: for kommunerne som en arkitektonisk retning, der understøtter strategiske og tekniske valg over tid, og for IT-serviceorganisationerne som et blueprint for den ydelse og de kapabiliteter, der skal kunne leveres i fælles drift.

Arkitekturprincipperne beskriver således ikke kommunernes aktuelle modenhedsniveau, men den måltilstand, der gradvist realiseres gennem en modnings- og transitionsrejse. Den konkrete parathed og progression mod målarkitekturen vurderes i kapitel 4 gennem den integrerede modenhedsmodel.

Retningslinjerne under arkitekturprincipperne er bevidst formuleret normativt og teknologiuafhængigt for at sikre langsigtet robusthed, leverandøruafhængighed og skalerbar drift. Afvigelser fra retningslinjerne kan forekomme, men skal være bevidste, dokumenterede og håndteret som led i en planlagt transition mod fælles målarkitektur.



Figur 2 – Arkitekturprincipper

3.1 Tværgående princip: Leverandøruafhængighed

Det tilstræbes, at leverandøruafhængighed er et tværgående strategisk princip. Princippet indebærer, at valg af proprietære løsninger skal være bevidst og dokumenteret, med vurdering af merværdi og veldefineret risikovurdering. Målbilledet for LAN/WAN baseres videst muligt på åbne standarder (f.eks. IEEE 802.1X, OSPF/IS-IS, BGP, VRF, VXLAN/EVPN, IPsec/IKEv2, SNMPv3, SSH, NETCONF/RESTCONF) for at kunne imødekomme kommunernes strategiske valg i en sammenhængende løsning. I denne kontekst er leverandøruafhængighed et væsentligt strategisk hensyn, da bindinger til proprietære

teknologier på sigt kan skabe unødig kompleksitet, f.eks. ved teknologisk udfasning eller ændrede organisatoriske rammer i kommunesamarbejdet.

3.2 Sikkerhed

Retningslinje 1: Identitetsbaseret netværksadgang (802.1X/NAC)
Arkitekturprincip: Security by Design

Al netværksadgang autentificeres via 802.1X med central RADIUS/AAA-infrastruktur. Dynamisk VLAN-tildeling baseres på brugeridentitet og enhedstype. Endpoint profilering med posture assessment integreres, og certifikatbaseret autentificering (EAP-TLS) foretrækkes. MAC Authentication Bypass (MAB) accepteres udelukkende som fallback for legacy-enheder. NAC er en grundkomponent i målbilledet, idet den sikrer, at kun autoriserede enheder får adgang til infrastrukturen.

Stordriftsfordele: Central adgangskontrolpolitik på tværs af alle 98 kommuner via én RADIUS-platform. Investering i enterprise NAC retfærdiggøres ved skala.

Retningslinje 2: Kryptering af data under transport (WAN)
Arkitekturprincip: Security by Design

Al trafik mellem lokationer og driftscentre krypteres for at beskytte dataintegritet og forhindre uautoriseret adgang. Kryptering implementeres med moderne og godkendte algoritmer (f.eks. AES-256, IKEv2 og DH-gruppe 19+/Curve25519), og certifikatbaseret tunnelautentificering via intern PKI anvendes som udgangspunkt. Krypteringspolitikken dokumenteres som en del af sikkerhedspolitikken. MACsec kan indgå i punkt-til-punkt forbindelser på egne fiberkabler, mens IPsec eller tilsvarende anvendes over infrastruktur, som er uden for IT-serviceorganisationen og kommunernes egen administration. Princippet er som udgangspunkt transportagnostisk og gælder for al netværkstrafik.

Stordriftsfordele: Centraliseret PKI og certifikatstyring reducerer per-tunnel-omkostninger. Standardiseret krypteringspolitik eliminerer inkonsistente sikkerhedsniveauer.

Retningslinje 3: Sikker management
Arkitekturprincip: Overvågning og auditering

Al CLI-adgang sker via SSHv2. Telnet og SNMPv1/v2c er deaktiveret i målarkitekturen og udfases konsekvent i overgangsperioder. SNMPv3 authPriv (SHA-256/AES-256) er minimumskrav. Syslog transporteres over TLS til central logindsamling. NTP synkroniseres via autentificeret NTS eller en alternativ autentificeringsmetode. Sikker management er IT-serviceorganisationens operationelle livsnerve – det er den kanal, hvorigennem NaaS ydelsen provisioneres, overvåges og vedligeholdes.

Stordriftsfordele: Skala retfærdiggør centraliseret SIEM med krypteret log-ingest og dedikeret SOC-kapacitet.

Retningslinje 4: Kategorisering af systemer og håndhævelse af politikker
Arkitekturprincip: Kategorisering af systemer

Alle systemer kategoriseres med minimum tre niveauer: høj, middel og basis. Kategoriseringen afspejles direkte i netværksarkitekturen via placering i tilsvarende sikkerhedszoner. Systemer kategoriseret 'høj' (sundhedsdata, CPR-systemer) placeres i dedikerede mikrosegmenterede zoner med whitelisted trafikflows. Systemkategoriseringen er den primære mekanisme, der driver differentieringen af serviceniveauer i IT-serviceorganisationernes leverancemodel; en sundhedsafdelings serviceprofil med øgede SLA-krav adskiller sig fundamentalt fra en skoles basale internetadgang.

Stordriftsfordele: Central kategoriseringsmodel sikrer konsistens. Differentieret sikkerhed reducerer unødig kompleksitet for lavt kategoriserede systemer.

3.3 Standardisering

Retningslinje 5: Hierarkisk IP-adresseplan med IPAM-governance
Arkitekturprincip: Adressetildeling

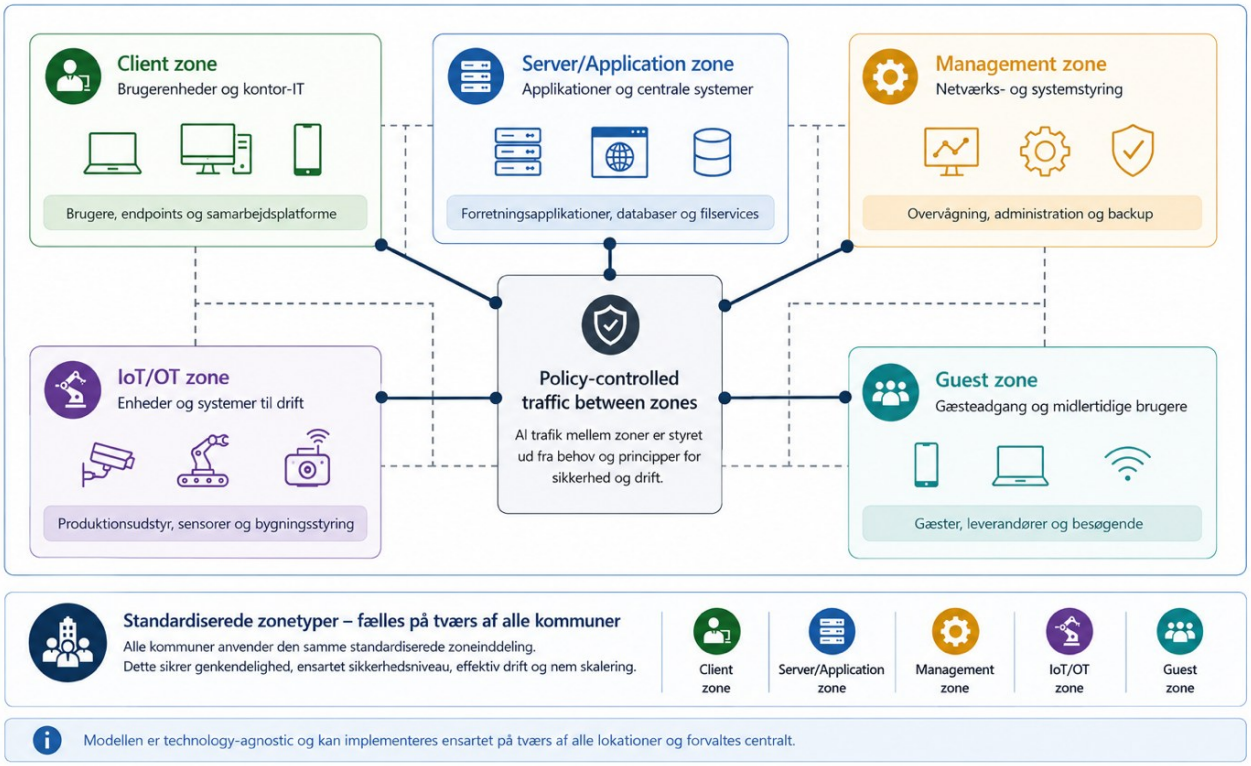
En samlet hierarkisk IP plan (version 4 og 6) med dedikerede supernets pr. IT-serviceorganisation og subnetallokering pr. tenant, zone og funktion. Alle allokeringer registreres i central IPAM med audit trail og brugbare API'er til automatiseringsformål. IPAM er fundamentet for en skalerbar drift; automatiseret tildeling af adresserum ved onboarding af en ny kommunal lokation eller tjeneste er en kerneoperation i en managed service.

Retningslinje 6: Standardisering af routingprotokoller
Arkitekturprincip: Logiske netværksstrukturer

Intern routing standardiseres på én IGP-protokol (OSPF eller IS-IS). Routing ved grænsesnit til netværk uden for ejerkommunens eller IT-serviceorganisationens administrative kontrol (f.eks. NSP-/carrier-net, internet-edges eller grænsesnit mod IT-serviceorganisationer) baseres på BGP (eBGP) for skalerbarhed og policy-kontrol. Ensartet routing er en forudsætning for, at IT-serviceorganisationerne kan fejlsøge, automatisere og garantere SLA på den leverede netværkstjeneste.

Retningslinje 7: Standardiseret zonemodel for netværkssegmentering
Arkitekturprincip: Zonemodeller

En ensartet zonemodel faciliterer anvendelsen af forskellige regelsæt og adgangsprofiler for forskellige typer af endpoints: Server/Applikation, Klient, Management, IoT/OT, Gæst, DMZ og Shared Services. Zonemodellen (zonetyper og navngivning) er fælles og ensrettet på tværs af IT-serviceorganisationerne, mens konkrete policy- og adgangsprofiler kan differentieres efter systemkategorisering og netværksprofiler. En zone *kan* f.eks. have standardiseret VLAN-interval, IP-allokering og interzone-firewallpolitik. Zonemodellen bør være skalerbar og tilpasses efter netværksydelserne i IT-serviceorganisationerne. Zonemodellen udgør fundamentet for differentierede netværkstjenester inden for én kommune: f.eks. modtager en IoT-zone en anden policy profil end en klientzone.



Figur 3 - Eksempel zonemodel

Retningslinje 8: Standardiserede redundansmønstre

Arkitekturprincip: Redundans principper

Redundansmønstre standardiseres pr. lokationstype og realiseres som definerede redundansprofiler. WAN redundans baseres som udgangspunkt på separat fremførte dataforbindelser, mens basisredundans kan etableres med defineret failover til alternativ transport (f.eks. mobilt backup), hvor fuld diversitet ikke er hensigtsmæssig. Failover scenarier bør testes jævnligt. Redundansmønstrene knytter sig direkte til managed service-SLA serviceniveauerne: En lokation med højt kategoriserede systemer modtager en netværkstjeneste med fuld redundans, mens en mindre lokation kan betjenes med en basisredundansprofil.

3.4 Konsolidering

Retningslinje 9: Multi-tenant datacenternetværk

Arkitekturprincip: Datacentre med multi-tenancy.

Multi-tenant arkitekturen i datacenternetværket er fundamentet for den tekniske og juridiske adskillelse mellem kommuner. Logisk isolation realiseres via dedikerede routingsdomæner (VRF, VXLAN VNI), mens shared services placeres i særskilte domæner med kontrollerede integrationspunkter. Netværket designes som et moderne fabric-baseret datacenterdesign, og onboarding af nye tenants standardiseres og automatiseres for at sikre ensartethed, sporbarhed og kontrolleret isolation.

Retningslinje 10: Skalerbare og reproducerbare topologimønstre

Lokationstypologi standardiseres (f.eks. Type A: stor campus >500 endpoints; Type B: medium 100–500; Type C: fjernt kontor <100) med veldefinerede blueprints pr. type. De konkrete tærskler og kriterier operationaliseres og vedligeholdes som del af fælles governance i IT-serviceorganisationerne. Topologier er templatebaserede og understøtter automatiseret provisionering. Lokationstypologien udgør rammen for den infrastrukturprofil, som lokationen etableres med – herunder definerede krav til kapacitet, redundans og serviceniveau – mens zoner og systemkategorisering anvendes oven på denne infrastruktur.

Retningslinje 11: Netværksautomatisering og Infrastructure as Code
Arkitekturprincip: Automatisering

Netværkskonfigurationer beskrives som kode (Infrastructure as Code) og versionsstyres i et centralt repository, der fungerer som autoritativ kilde. Ændringer implementeres via CI/CD-pipelines, og provisionering af nye lokationer, tenants og zoner automatiseres end-to-end. Automatiseringsværktøjer bør baseres på åbne standarder (f.eks. Ansible, Python/Nornir, NETCONF/RESTCONF). Automatisering er en grundlæggende forudsætning for konsistent, skalerbar og effektiv netværksdrift på tværs af et stort og komplekst infrastrukturlandskab.

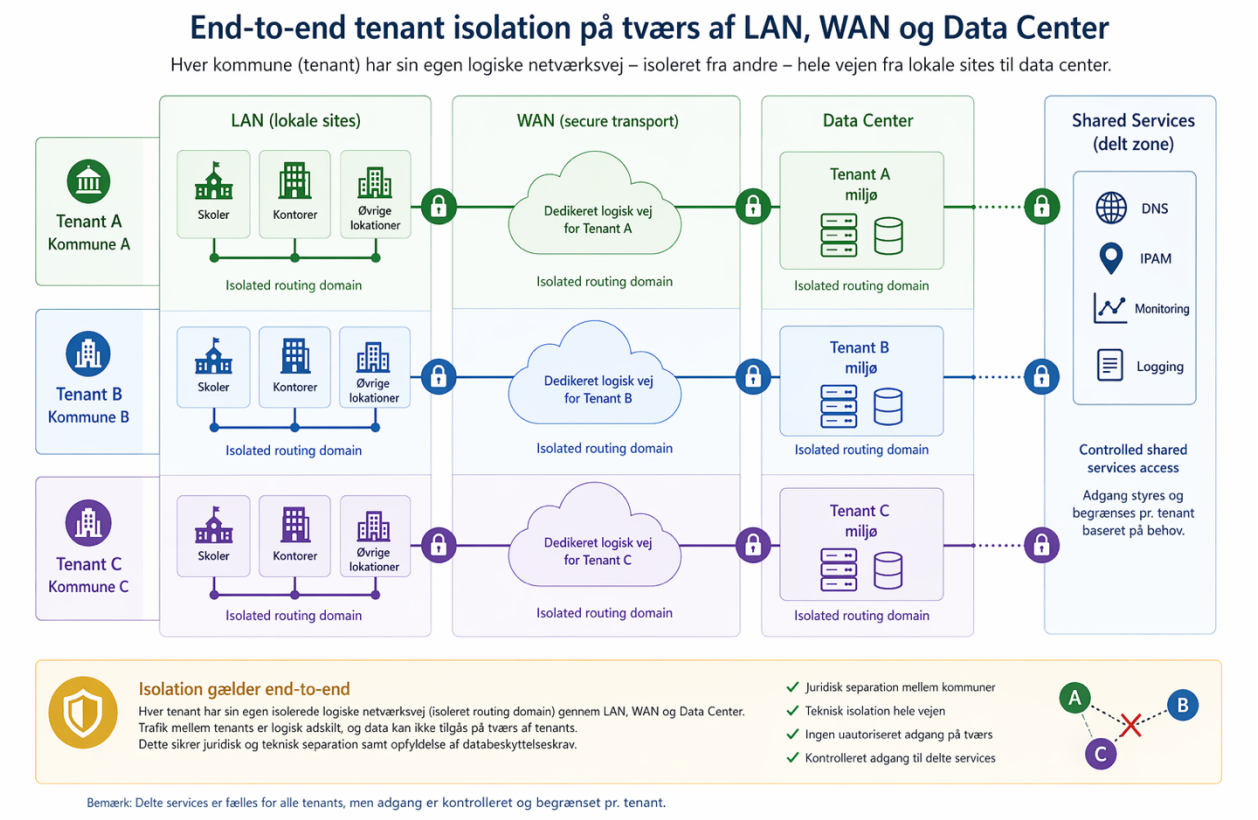
Retningslinje 12: Ressourceoptimering og kapacitetsstyring
Arkitekturprincip: Optimal udnyttelse af ressourcer

Kapacitetsplanlægning baseres på trenddata fra network management-systemer (NMS) med automatiseret forecasting. Delt infrastruktur dimensioneres ud fra aggregerede kapacitetskrav for at sikre effektiv udnyttelse og rettidig skalering. Hardware standardisering anvendes, hvor det er hensigtsmæssigt, med henblik på at understøtte fælles reservedelspool og forenklet drift, uden at fastlåse kommunerne i bestemte leverandørvalg. Arkitekturvalg tilrettelægges således, at leverandørafhængigheder minimeres, og teknologisk fleksibilitet bevares på tværs af infrastrukturlandskabet. Kapacitetsstyring varetages proaktivt for at sikre rettidig opgradering og dermed undgå driftsmæssige kapacitetsbegrænsninger på tværs af infrastrukturen.

3.5 Segmentering

Retningslinje 13: VRF baseret makrosegmentering og tenant isolation
Arkitekturprincip: Makro-segmentering og large-scale netværk

Hver tenant (kommune, enhed el. lign.) tildeles et dedikeret VRF domæne med isoleret routingtabel, forwarding og policy. VRF baseret tenant isolation er måltilstanden i IT-serviceorganisationerne og realiseres gradvist gennem transition og konsolidering. Management- og shared services trafik placeres i særskilte VRF'er. VRF designet er end-to-end og strækker sig fra LAN over WAN til datacenter, mens eventuelt route leaking udelukkende sker via kontrollerede route targets. VRF baseret isolation udgør det tekniske og juridiske fundament for adskillelse mellem selvstændige kommunale entiteter og er en forudsætning for at opfylde krav til databehandling og databeskyttelse, herunder GDPR.



Retningslinje 14: Mikrosegmentering for højt kategoriserede systemer

Arkitekturprincip: Mikrosegmentering for kat. systemer

Systemer kategoriseret som 'høj' placeres i dedikerede sikkerhedszoner med mikrosegmentering baseret på princippet om mindst mulige adgang. Inden for den VRF baserede makrosegmentering anvendes streng policy-kontrol, hvor al kommunikation som udgangspunkt er afvist, og trafik udelukkende tillades via eksplicit definerede og dokumenterede flows. Mikrosegmentering anvendes målrettet for at reducere angrebsfladen og begrænse spredning af angreb inden for miljøet, særligt for systemer der håndterer følsomme eller forretningskritiske data.

Højt kategoriserede systemer adskiller sig fra middel- og lavt kategoriserede systemer ved at håndtere data eller funktioner med særlig høj forretningsmæssig, juridisk eller samfundsmæssig betydning. Hvor lavt og middel kategoriserede systemer typisk kan placeres i bredere zoner med standardiseret segmentering og fælles sikkerhedspolitikker, stiller højt kategoriserede systemer krav om strengere isolation, eksplicit adgangskontrol og dokumenterede trafikflows. Mikrosegmentering anvendes derfor selektivt for disse systemer, mens lavere kategorier håndteres gennem den overordnede zonemodel og makrosegmentering.

4 Modningsrejse (transition og transformation)

Modningsrejsen beskriver den faseopdelte vej fra kommunernes nuværende as-is-tilstand til en konsolideret og standardiseret driftsmodel for fælleskommunal LAN/WAN drift. Formålet er at etablere det tekniske og operationelle grundlag, der gør IT-serviceorganisationerne i stand til at overtage og levere en ensartet, sikker og skalerbar managed netværksydelse på tværs af kommunerne. Network as a Service (NaaS) er et ønsket langsigtet scenarie, hvor managed drift videreudvikles til en mere operationelt modnet leverancemodel med differentierede serviceprofiler. Modningsrejsen skal derfor læses som en planlægningsramme, der både understøtter driftsovertagelse i en managed model og – hvor relevant – gradvis modning mod NaaS. Det er afgørende, at transitionsplanen respekterer de betydelige modenhedsforskelle mellem kommunerne og prioriterer de indsatser, der har størst effekt på konsolideringsparatheden og stabil drift.

4.1 Transitionsperioden (nu – 31. december 2027)

Transitionsperioden har til formål at etablere grundlaget for driftsovertagelse og geare kommunerne mod en standardiseret managed driftsmodel (og hvor relevant gradvis modning mod NaaS):

1. As-is-kortlægning: Alle kommuner gennemfører en komplet as-is-kortlægning, herunder VRF struktur, hardware inventory, konfigurationsbaseline og dokumenteret netværksarkitektur.
2. Modenhedsvurdering: Hver kommune scores iht. 27-punktsmodellen i samarbejde med IT-serviceorganisationen. Resultaterne danner grundlag for individuelle transitionsplaner.
3. Overlap håndtering: Proaktiv kortlægning af IP-adresseoverlap pr. VRF instans – en kritisk barriere for konsolidering og driftsovertagelse.
4. Hardware gæld: End-of-support udstyr identificeres og prioriteres til udskiftning under IT-serviceorganisationens ejerskab.
5. Protokolhærdning: Deaktivering af usikre protokoller som akut sikkerhedsforanstaltning.
6. NAC-fundament: 802.1X på trådløst som minimumskrav. Planlægning af 802.1X-udrulning på kablet netværk.
7. Ejerskabstransition: Planlægning af overdragelse af hardwareejerskab fra kommuner til IT-serviceorganisationer som forudsætning for driftsovertagelse og leveranceansvar i en managed model.

4.2 Transformationsperioden (2028–2030)

Transformationsperioden fokuserer på modning mod Niveau 5 og etablering af en fuldt standardiseret, sikker og skalerbar managed netværksleverance (og, hvor relevant, gradvis produktisering mod NaaS):

1. Fuld VRF baseret makrosegmentering med end-to-end tenant isolation. Juridisk dataisolation som grundprincip.
2. Mikrosegmentering for højt kategoriserede systemer med differentierede service- og sikkerhedsprofiler.

3. Centraliseret IPAM og DNS med VRF separation, DNS sikkerhed og automatiseret provisionering.
4. IaC-baseret drift med kontrollerede deployments og automatiseret validering – den operationelle motor i skalerbar managed drift.
5. SIEM integration, krypteret logtransport og NIS2-compliant retention.
6. End-to-end WAN kryptering med certifikatbaseret tunnelautentificering via intern PKI.
7. Servicekatalog: Definition og lancering af standardiserede managed connectivity profiler per lokationstype og systemkategorisering (NaaS som muligt produktiseringslag).

4.3 Risikofaktorer og afbødning

- IP-konflikt som transitionsbarriere: Overlappende adresserum kan forhindre konsolidering og driftsovertagelse i en standardiseret managed driftsmodel.
- Kompetencegab: Netværksautomatisering kræver kombination af netværks- og softwarekompetencer.
- Blast radius ved automatisering: Fejl i automatiseringskode kan påvirke alle enheder simultant.
- Patchgæld og sikkerhedsgæld: Sårbarheder i én kommunes infrastruktur udgør risiko for hele fællesskabet.
- Politisk modstand: Kommuner kan have forbehold mod fuld ejerskabsoverdragelse. Klar kommunikation om juridisk isolation og servicefordele er påkrævet.
- Bemyndigelse under cyberangreb: Eksplicit bemyndigelse for IT-serviceorganisationens isolation af kommunesegmenter er påkrævet.

4.4 Faseopdelt roadmap

Område	2026–2027 (Transition)	2028–2029 (Transformation)	2030 (Managed drift operationel)
Netværksarkitektur	As-is kortlægning. Hardware gæld adresseret. Topologitemplates designet. Ejerskabstransition planlagt.	Modulært design implementeret. Standardiseret hierarki. Automatiseret provisionering fra templates.	Managed leveranceklar. Fuld template-baseret drift. Niveau 5.
Segmentering	VLAN-grundsegmentering. Zonemodel defineret. NAC på wireless. Kategoriseringsmodel vedtaget.	VRF makrosegmentering. 802.1X på alle porte. Mikrosegmentering for høj-kat. systemer.	Differentierede service- og sikkerhedsprofiler baseret på kategorisering. Niveau 5.

Område	2026–2027 (Transition)	2028–2029 (Transformation)	2030 (Managed drift operationel)
Adressering	Overlap kortlægning. IPAM-valg og governance. DHCP-konsolidering.	Central IPAM med VRF allokering. DNS delegation. DNS sikkerhed. Automatiseret tildeling.	Automatiseret provisionering via IPAM-workflow. Dual-stack. Fuld sporbarhed. Niveau 5.
WAN og transport	WAN kryptering påbegyndt. QoS model designet. Redundansvurdering.	End-to-end kryptering med central certifikatstyring. QoS implementeret. Diversificeret WAN.	SLA-monitoreret transport som del af managed leverancen. Niveau 5.
Management	Protokolhærdning. Central AAA etableret. Logning centraliseret.	SIEM med tenant separation. Privilegeret adgangsstyring. Flow-telemetri til drift og sikkerhed.	SOC-klar. NIS2-compliant. Operationelt dashboard for managed drift. Niveau 5.
Governance	Dokumentation opdateret. Konfigurationsbackup. IaC-pilot.	IaC-baserede arbejdsprocesser. Compliance-scanning. Change management. Servicekatalog for standardiserede ydelser.	Fuld IaC-baseret drift. Selvbetjening for standardydelser. Niveau 5.

5 Driftsmodel for fælleskommunal LAN/WAN drift

5.1 Overordnet driftsmodel

Driftsmodellen baseres på fem bærende søjler. I en fælles driftskontekst udgør disse søjler de kvalitative dimensioner, som den leverede managed netværksydelse måles på:

1. Cybersikkerhed: Ensartet højt sikkerhedsniveau baseret på NIS2, ISO 27001 og Statens Tekniske Minimumskrav. Fælles CERT- og SOC-kapabiliteter integreret i den managed leverance.
2. Driftssikkerhed: Strukturerede transitionsplaner med kontrolleret overdragelse. SLA-baseret drift med målbare kvalitetskriterier.
3. Kundetilfredshed: Tæt samarbejde med den enkelte kommune. Klar rollefordeling. Lokalt kundefokus med central leverancekvalitet.
4. Standardisering: Kommuner modtager standardiserede managed netværksydelser fra deres IT-serviceorganisation. Enheden bestemmer, hvordan ydelserne leveres.
5. Stordriftsfordele: Geninvestering af stordriftsgevinster i fælles løsninger, konsolidering og øget sikkerhed.

5.2 Opgavesnit og ansvarsfordeling

I den fælles driftsmodel varetager IT-serviceorganisationen driften af LAN/WAN som en standardiseret managed netværksydelse. Ejerskab og leverancemodel kan aftales og udvikles over tid (herunder fuldt ejerskab og produktisering mod NaaS), men IT-serviceorganisationen påtager sig driftsansvaret uanset leverancemodel.

IT-serviceorganisationen varetager:

Netværksdrift (managed kerneydelse)

- Indkøb, ejerskab, konfiguration og levering af alt netværksudstyr.
- LAN-drift: VLAN-administration, portpolitikker, segmentering.
- WiFi: Centralstyret trådløst netværk med gæste- og medarbejderadgang.
- WAN: Kryptering, QoS, redundans, carrierstyring.
- DNS og DHCP: Central administration med kommuneafgrænset governance.
- Adgangskontrol: 802.1X, NAC, endpoint-compliance som integreret del af connectivity-ydelsen.
- Lifecycle management: Proaktiv hardwareudskiftning som del af leveranceansvaret i den managed model.

Cybersikkerhed (integreret i den managed leverance)

- Detektion og beskyttelse mod angreb samt styrket sikkerhed for centrale netværkstjenester (herunder DNS sikkerhed) og relevante domæner og tjenester.

- Firewall: Central administration med zonebaseret politik.
- DDoS-beskyttelse og sårbarhedsscanning.
- Logning med tenant isolation. Sikkerhedsrapportering og compliance-dokumentation.
- 24/7 SOC på tværs af enheder.

Governance og automatisering

- Automatiseret patch management og softwareopdateringer.
- Konfigurationsstyring med versionering og drift-detektion.
- Incident-, problem- og release management.
- Asset management, kapacitetsstyring og servicerapportering.

5.3 Governance-struktur

- Strategisk niveau: Kommunerne bevarer det strategiske ansvar. IT-serviceorganisationerne rapporterer på KPI'er knyttet til de fem bærende principper.
- Taktisk niveau: SLA-klassificering af service- og leveranceprofiler med dokumenterede redundans- og sikkerhedskrav. Regelmæssige service reviews.
- Operationelt niveau: Standardiserede ITIL-baserede processer. Kommuneafgrænset eskalation.

5.4 NIS2-relevans og compliance

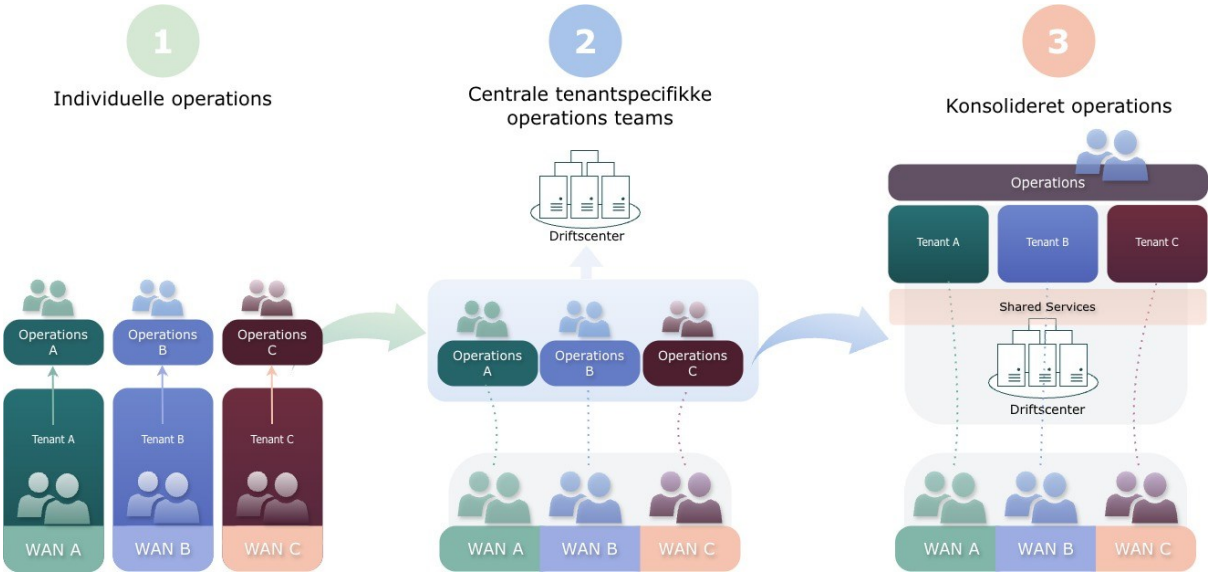
Den managed netværksleverance er designet med eksplicit hensyntagen til NIS2-krav:

- Dokumenteret IP-sporbarhed via central IPAM og DHCP-logging.
- Krypteret logtransport og tenant separeret SIEM med defineret retention-politik.
- Kryptografisk beskyttelse af al trafik over offentlige netværk.
- Risiko-baseret segmentering med systematisk kategorisering af systemer.
- Struktureret incident response med koordineret CERT-kapabilitet.
- Auditspor pr. kommune fremvisningsparat for tilsynsmyndigheder.

6 Use cases

6.1 Operationel transformation

Til at illustrere den operationelle transformation tager dette afsnit udgangspunkt i én konkret driftsopgave: håndtering af et kritisk udfald på en lokation (f.eks. en skole), hvor brugerne mister adgang til centrale it-tjenester. Use casen viser, hvordan den samme hændelse håndteres i tre stadier, og hvilke gevinster der opnås, efterhånden som driften flyttes fra lokale teams til central drift og senere til et konsolideret operationsteam.



Figur 4 - Operationel transformation

Stadie 1 - Lokale operationsteams i hver kommune (før IT-serviceorganisation)

Hændelse: Skolen mister forbindelsen til WAN, og undervisning/administration påvirkes.

- **Responsmønster**: Lokal it-drift modtager henvendelser, triagerer ud fra lokalt kendskab og eskalerer ved behov til leverandør/transportpart.
- **Styrke**: Hurtig lokal kontekst (hvad plejer at være galt på netop denne lokation) og kort vej til lokale interessenter.
- **Udfordring**: Varierende metoder og værktøjer mellem kommuner giver uens håndtering og uforudsigelig genopretningstid.
- **Udfordring**: Viden er personafhængig; fravær og vagtbelastning påvirker responstid og kvalitet.
- **Udfordring**: Manglende ensretning gør det svært at sammenligne hændelser på tværs og lære systematisk.

Stadie 2 – Centraliseret drift med kommuneopdelt administration

- **Responsmønster:** Hændelsen håndteres af et centralt team, men med kommuneafgrænset ansvar, dataadskillelse og eskalation. De samme basale driftstrin (triage, fejlafgrænsning, eskalation, kommunikation) udføres efter fælles processer.

- **Gevinst:** Ensrettede driftsprocesser giver mere forudsigelig håndtering, tydeligere eskalationsveje og bedre rapportering på tværs af kommuner.
- **Gevinst:** Bedre bemanding og vagtstruktur reducerer sårbarhed ved sygdom/ferie og mindsker personafhængighed.
- **Gevinst:** Central overvågning gør det muligt at opdage udfald tidligere og arbejde mere proaktivt.
- **Begrænsning:** Fejlhåndtering og ændringer udføres stadig i praksis pr. kommune (tenant), hvilket kan give gentagelser og parallel indsats.

Stadie 3 – Konsolideret operations team på tværs af tenants

- **Responsmønster:** Hændelsen håndteres af ét samlet operations team med ensartede standarder, værktøjer og arbejdsgange på tværs af kommuner, samtidig med at dataadskillelse og ansvar fortsat er kommuneafgrænset. Teamet arbejder ud fra standardiserede lokationstyper, profiler og fælles driftsprincipper.
- **Gevinst:** Hurtigere fejlafgrænsning, fordi netværksdesign, overvågning og procedurer er ensrettede på tværs af kommuner og lokationstyper.
- **Gevinst:** Gentagelser reduceres: én forbedring i overvågning, standarder eller procedure løfter alle kommuner samtidigt.
- **Gevinst:** Lavere genopretningstid ved hændelser, fordi standardiserede redundans- og failover-mønstre giver mere forudsigelig adfærd.
- **Gevinst:** Bedre kapacitetsudnyttelse og mulighed for specialisering, fordi kompetencer samles og anvendes der, hvor behovet er størst.

Opsummering: Den operationelle gevinst ved transformationen er, at den samme hændelse går fra at være person- og kommuneafhængig til at blive håndteret efter ensrettede standarder og med højere forudsigelighed. Samtidig fastholdes kommuneafgrænsning og dataseparation, mens driftens kapacitet og kvalitet gradvist løftes gennem centralisering og senere konsolidering.

7 Visionært perspektiv: Network as a Service

7.1 Strategisk vision

Det er dette målbilledes overordnede betragtning, at summen af de beskrevne arkitekturprincipper, modenhedskrav og driftsmodellen peger mod en stadig mere standardiseret og industrialiseret leverancemodel for fælleskommunal LAN/WAN drift. Network as a Service (NaaS) beskrives i dette kapitel som et visionært og langsigtet scenarie, hvor en managed netværksleverance videreudvikles og produktificeres, så IT-serviceorganisationerne kan levere secure connectivity som en ensartet ydelse med klare service- og sikkerhedsprofiler.

I NaaS scenariet transformeres IT-serviceorganisationernes rolle fra at være tekniske driftsorganisationer til at være professionelle serviceleverandører. Kommunen aftager en ydelse – secure connectivity – og kan i stigende grad undlade at forholde sig til den underliggende infrastruktur, på samme måde som kommunen i dag aftager el og vand som forsyningsydelser.

7.2 NaaS modellens kerneelementer

a) Fuldt managed ejerskab

I NaaS scenariet ejer, indkøber, konfigurerer, overvåger, vedligeholder og udskifter IT-serviceorganisationen al netværksinfrastruktur – fra access-switchene i den enkelte skole til core-routerne i driftscentret og de krypterede WAN forbindelser imellem. Kommunen modtager connectivity som en ydelse, som kan afregnes via en abonnementsmodel per lokation og serviceniveau. Hardware lifecycle, firmware-opdateringer og kapacitetsudvidelser er IT-serviceorganisationens ansvar og indgår i den leverede pakke.

b) Secure connectivity som leverance

NaaS ydelsen er ikke blot netværkstransport – det er secure connectivity. Sikkerhedselementerne er integrerede og uadskillelige fra transportlaget:

- 802.1X-baseret adgangskontrol: Kun autoriserede enheder får adgang til den leverede connectivity.
- End-to-end kryptering: Al trafik mellem lokationer og driftscentre er krypteret som standard.
- Zonebaseret segmentering: Trafikken inden for den leverede connectivity er segmenteret efter standardiseret zonemodel.
- Tenant isolation: Kommunens data er juridisk og teknisk adskilt fra alle andre kommuners.
- SIEM og SOC: Overvågning, detektion og respons er integreret i ydelsen.

c) Differentierede serviceniveauer inden for kommunen

En væsentlig styrke ved NaaS modellen er muligheden for at levere differentieret connectivity tilpasset den enkelte kommunale funktions behov. I en managed leverance kan samme differentiering forstås som service- og leveranceprofiler, mens den i NaaS scenariet afspejles i konkrete NaaS profiler.

Differentieringen drives af systemkategoriseringen (høj, middel, basis) og afspejles i konkrete NaaS profiler:

NaaS profil	Kategorisering	Eksempler på funktions-områder	Connectivity-karakteristik	Sikkerhedsniveau
NaaS Premium	Høj (3)	Sundhedsafdelinger med adgang til sundhedsdata, CPR-registre, kritiske socialfaglige systemer, OT-anlæg	Fuld redundans med diversificerede forbindelser og dokumenteret failover. SLA med hurtig konvergens. Prioriteret trafik (QoS) og dimensioneret kapacitet.	Mikrosegmentering med whitelistede flows. Dedikeret VRF domæne. Forstærkede NAC-krav (EAP-TLS og endpoint-compliance). Udvidet logning og overvågning.
NaaS Standard	Middel (2)	Administrative afdelinger, økonomi, HR, kommunale sagsbehandlingssystemer, borgerservice	WAN redundans på større lokationer. Standardiseret QoS. Dimensioneret båndbredde med definerede tærskler.	Zonebaseret segmentering. NAC (802.1X). Krypteret WAN. Standard SIEM dækning. Kategoriseret adgangskontrol.
NaaS Basis	Basis (1)	Skoler (undervisningsnetværk), biblioteker, idrætsanlæg, gæstenetværk, IoT-sensorer (ikke-kritiske)	Basisredundans (single WAN med failover til mobilt backup). Best-effort QoS. Kapacitet dimensioneret til typisk forbrug.	Makrosegmentering (VRF). Basis-NAC (kontrolleret MAB for IoT/legacy, 802.1X for brugere). Krypteret WAN. Standard logning.

Det er væsentligt at understrege, at differentiering sker inden for den enkelte kommune – ikke mellem kommuner. Alle kommuner har adgang til alle tre NaaS profiler og tildeler dem baseret på deres interne systemkategorisering. En kommune med et større sundhedsområde vil naturligt have flere lokationer på NaaS Premium, mens en kommune med primært administrative funktioner vil have hovedparten af lokationerne på NaaS Standard.

7.3 Kategorisering som driver for service- og sikkerhedsprofiler

Systemkategoriseringen, beskrevet i arkitekturprincip 4, er den primære mekanisme, der kobler kommunens forretningsbehov til differentierede service- og sikkerhedsprofiler i den managed leverance (og i NaaS scenariet til konkrete NaaS profiler). Kategoriseringen bygger på to dimensioner:

- Datakritikalitet: Hvilke data håndteres af systemerne på lokationen? Sundhedsdata og CPR-oplysninger kræver den højeste kategorisering og dermed den højeste serviceprofil (NaaS Premium i NaaS scenariet).

- Driftskritikalitet: Hvad er konsekvensen af nedetid? Systemer med direkte borgerpåvirkning (nødkald, akutfunktioner) kræver højere redundans end interne administrative systemer.

Kategoriseringen gennemføres i samarbejde mellem kommunens forretning og IT-serviceorganisationen og registreres, så den automatisk kan afspejles i netværkssegmenteringen og den tildelte service- og sikkerhedsprofil (NaaS profil i NaaS scenariet).

7.4 Forudsætninger for NaaS scenariet

En vellykket realisering af NaaS scenariet forudsætter, at den fælles managed netværksleverance er modnet og standardiseret, så IT-serviceorganisationerne kan levere ensartede service- og sikkerhedsprofiler. Følgende fundament skal være på plads:

- Standardisering (Niveau 5): Ensartet netværksdesign, routing, zonemodel og hardware portefølje på tværs af alle lokationer. Uden standardisering kan NaaS scenariet ikke leveres konsistent.
- Automatisering (Niveau 5): IaC-baseret provisionering, overvågning og konfigurationsstyring. Uden automatisering kan den produktificerede leverance (NaaS scenariet) ikke skalere til 13.500 lokationer.
- Segmentering (Niveau 5): VRF baseret tenant isolation og zonebaseret segmentering. Uden segmentering kan den produktificerede leverance (NaaS scenariet) ikke differentieres eller juridisk forsvares.
- Sikkerhed (Niveau 5): NAC, kryptering, SIEM og SOC som integrerede elementer. Uden sikkerhed kan den produktificerede leverance (NaaS scenariet) ikke opfylde forventede compliance-krav.
- Ejerskabstransition (forudsætning for NaaS scenariet): Overdragelse af hardware ejerskab fra kommuner til IT-serviceorganisationer. Uden ejerskab kan IT-serviceorganisationen ikke ensrettet og end-to-end garantere lifecycle, kapacitet og SLA som et standardiseret produkt i en produktificeret leverancemodel.

Det vurderes, at de fire første forudsætninger opnås gennem den modningsrejse, der er beskrevet i kapitel 5, med mål om Niveau 5 på tværs af alle 27 vurderingsområder. Den femte forudsætning – ejerskabstransition – kræver en særskilt juridisk og økonomisk afklaring og er særligt relevant ved realisering af NaaS scenariet som produktificeret leverancemodel.

7.5 Stordriftsfordele ved NaaS

Fælles drift som standardiseret managed leverance muliggør en række stordriftsfordele, som ikke er tilgængelige i det nuværende fragmenterede landskab. Ved produktificering mod NaaS kan flere af fordelene realiseres mere konsekvent og i større skala:

- Central adgangskontrolpolitik på tværs af lokationer via fælles autentificerings- og autorisationsinfrastruktur (AAA/RADIUS).
- Central certifikatstyring til understøttelse af identitetsbaseret adgang og kryptering, med reducerede per-tunnel-omkostninger.

- Central overvågning, detektion og respons (SIEM/SOC-kapabilitet) retfærdiggjort ved skala.
- Automatiseret kontrol og rapportering af compliance og standarder på tværs af tusindvis af enheder.
- Delt reservedelspool med typisk 60–70 % reduktion i lagerinvestering.
- Kollektive indkøbsaftaler med bedre priser og vilkår.
- Muliggør deling af specialistkompetencer på tværs af kommuner.
- Forudsigelige omkostninger for kommunerne: mere ensartede og planlagte drifts- og investeringsomkostninger, f.eks. via standardiserede afregningsmodeller.
- Skaber bedre rammer for, at ejerkommunens IT-ressourcer kan prioriteres i forhold til kerneforretning og digital udvikling.

7.6 NaaS som transformationsmål

Sammenfattende er det dette målbilledes vurdering, at Network as a Service (NaaS) kan fungere som et langsigtet transformationsmål, hvor den fælles managed netværksleverance videreudvikles og produktificeres til en mere ensartet leverancemodel med klare service- og sikkerhedsprofiler. Ikke som en teknologisk ambition for teknologiens skyld, men som en mulig konklusion på den modningsrejse, der er beskrevet i dette dokument: Når standardisering, segmentering, sikkerhed og automatisering er på Niveau 5, er grundlaget i høj grad etableret til at kunne realisere NaaS scenariet oven på en stabil managed leverance.

NaaS scenariet kan realiseres gradvist i takt med, at kommunerne når de påkrævede modenhedsniveauer. Kommuner i det grønne scoringsinterval (70–81 point) kan fungere som piloter for en produktificeret leverance allerede i slutningen af transitionsperioden, mens kommuner i det røde interval typisk må gennemgå den fulde transformationsindsats før scenariet kan aktiveres.

Det lægges til grund, at IT-serviceorganisationerne påbegynder udarbejdelsen af et servicekatalog for standardiserede connectivity profiler med tilhørende SLA-rammer og afregningsmodel som en konkret leverance i transformationsperioden 2028–2029, med sigte på at kunne understøtte en produktificeret leverancemodel fra 2030.

7.7 AI i relation til LAN/WAN drift

Anvendelsen af kunstig intelligens (AI) i drift af netværksinfrastruktur er et område under hastig udvikling, men vurderes på nuværende tidspunkt ikke at være tilstrækkeligt modent til at forestå autonom drift af komplekse LAN/WAN miljøer i en fælleskommunal kontekst. Netværksdrift er kendetegnet ved høj kompleksitet, mange afhængigheder og et behov for deterministisk kontrol, hvilket fortsat kræver stærk menneskelig ekspertise og veldefinerede driftsprocesser.

Der ses imidlertid en tendens til at anvende AI som et assisterende værktøj – særligt inden for fejlanalyse (troubleshooting), mønstergenkendelse og proaktiv identifikation af afvigelser. Moderne AI modeller kan identificere korrelationer i store mængder telemetridata, som ellers kan være vanskelige at afdække manuelt, og kan dermed på sigt bidrage til hurtigere fejlsøgning og reduceret *mean time to*

repair (MTTR). Denne udvikling understøtter i særlig grad en centraliseret og standardiseret driftsmodel, hvor datagrundlaget er tilstrækkeligt ensartet og omfattende.

Realiseringen af egentlig AIOps funktionalitet forudsætter imidlertid et solidt fundament af strukturerede data, konsistent telemetri og høj grad af automatisering. Initiativer som Infrastructure as Code (IaC), centraliseret IPAM, standardiserede topologier og ensartede konfigurationsmønstre er ikke blot vigtige for driftsstabilitet og skalerbarhed, men udgør samtidig en nødvendighed for at kunne anvende avancerede analyse- og AI værktøjer effektivt. Uden et sådant fundament vil AI løsninger sandsynligvis have begrænset værdi, da inputdata vil være fragmenterede og inkonsistente.

På længere sigt kan AI forventes at blive en integreret del af den samlede driftsplatform, hvor den understøtter beslutningstagning, kapacitetsplanlægning, sikkerhedsmonitorering og automatiseret respons inden for klart definerede rammer. I en sådan model vil AI ikke erstatte den centrale drift, men fungere som en forstærkende kapabilitet, der gør det muligt at håndtere et stadigt voksende og mere komplekst infrastrukturlandskab med højere effektivitet og kvalitet.

Det anbefales derfor, at arbejdet med standardisering, segmentering og automatisering prioriteres, ikke alene for at understøtte den ønskede managed driftsmodel og NaaS vision, men også for at etablere de nødvendige forudsætninger for fremtidig anvendelse af AI i netværksdriften.