TJENESTEBESKRIVELSE BEDRIFTSNETT IP-VPN

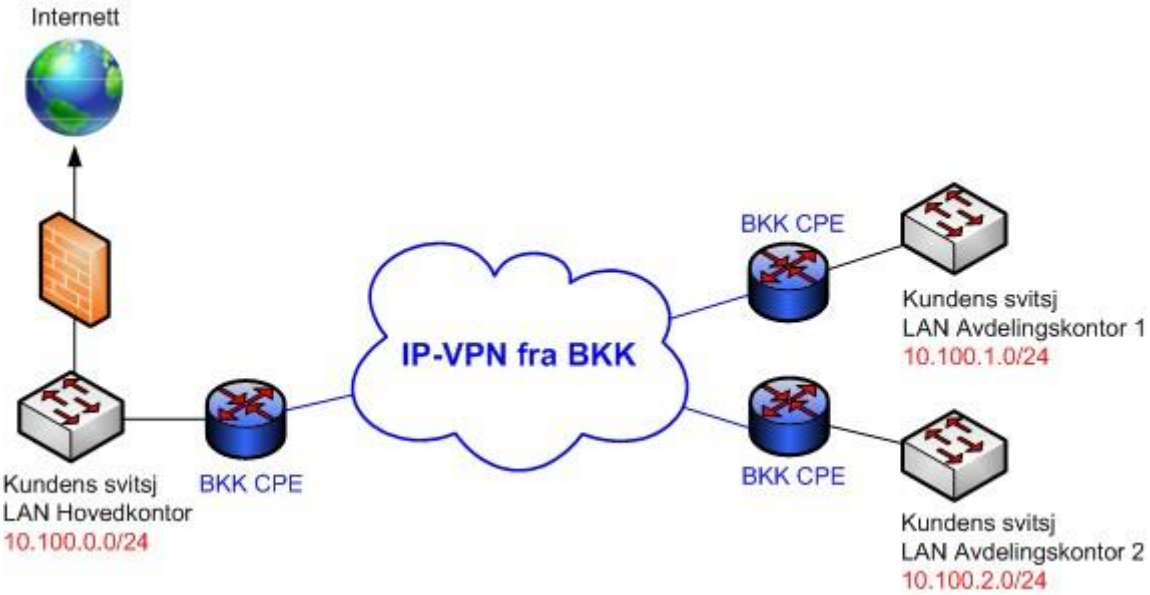
T: 55 12 90 00 | E: fiber@bkk.no

Innhold

BKKs IP-VPN tjenester

Bedriftsnett IP-VPN fra BKK er en sikker og stabil løsning for kommunikasjon mellom to eller flere lokasjoner. Bedriftsnett IP-VPN blir bygget på BKKs MPLS infrastruktur. Dette gir BKK mulighet til å levere en stabil tjeneste med høy oppetid og god kvalitet. Ved ønske om tilknytning i IP-VPN nettverket i et område der BKK ikke har egen infrastruktur, kan BKK levere sambandet gjennom en av våre samarbeidspartnere, og vi kan således levere Bedriftsnett IP-VPN med aksesser over hele landet.

I et Bedriftsnett IP-VPN er all trafikk 100% adskilt fra andre kunders trafikk, og IP-VPN benyttes av bedrifter og institusjoner med høye krav til sikkerhet.



Skissen over viser et eksempel på Bedriftsnett IP-VPN fra BKK. Rent logisk ser et IP-VPN ut som en rutet tjeneste som knytter sammen to eller flere LAN fra ulike lokasjoner. Vanligvis har hovedkontoret en internettlinje som også avdelingskontorene benytter gjennom IP-VPN nettverket. Bedriftsnett IP-VPN er svært skalerbart, og det er ingen praktisk øvre grense for hvor mange lokasjoner som kan tilknyttes IP-VPN nettverket. Konfigurasjon av IP-VPN linjene utføres av BKK i henhold til spesifikasjonene gitt fra kunde. BKK kan bistå kunden med design av IP-VPN nettverket.

Grensesnitt

Standard grensesnitt for tilkobling av sluttbrukers utstyr er RJ45 med FastEthernet 100Base-TX for hastigheter opp til og med 100Mbit/s. Sammenkobling gjøres med TP (Twisted Pair) kabel. Det anbefales å benytte Auto hastighet og Auto dupleks.

Ved behov kan det avtales andre grensesnitt som 10Base-T eller 1000Base-TX/SX/LX. Ved leveranser av hastigheter over 100Mbit/s benyttes 1000Base-TX/SX/LX.

Hvis det benyttes fibergrensesnitt er det vanlig med singelmodus fibermoduler i endeutstyret og fiberkonnektorer av typen SC eller LC. Det vil spesifiseres ved leveranse hvilken konnektor type som benyttes. Kunde må ha tilsvarende fibermodul i eget utstyr.

Kunderuter (CPE)

IP-VPN fra BKK leveres som standard med kunderuter på hver lokasjon. Dette gir BKK god kontroll over tjenesten som blir levert, med rask og effektiv feilsøking ved eventuelle feilsituasjoner, samt mulighet for tilleggsprodukter som QoS, oppdeling i flere tjenestenett, overvåking og rapportering. Det tas automatisk backup av konfigurasjon på kunderuterne. Til kunderutere benytter BKK kvalitetsprodukter fra Cisco.

Kunden kan få SNMP lesetilgang til kunderuterne i sitt IP-VPN, og har anledning til å hente trafikkdata og annen informasjon inn i kundens egne overvåking- og management systemer.

IP-adresser

Bedriftsnett IP-VPN er en rutet lag3-tjeneste, og det må derfor etableres egne subnett på hver lokasjon. Kunden er ansvarlig for tildeling av LAN-adresser på alle lokasjoner. BKK konfigurerer disse LAN-adressene på kunderuterne og sørger for ruting mot LAN-adressene i IP-VPN nettverket.

BKK kan levere IP-VPN med dual-stack IPv4 og IPv6. Kunden administrerer hvilke IPv6 LAN-adresser som skal benyttes på hver lokasjon, ut fra IPv6-adressene som kunden har fått tildelt fra sin internettleverandør, enten det er BKK eller en annen leverandør.

MTU

IP-VPN fra BKK leveres med MTU (maksimal pakkestørrelse) på 1500 byte.

Dynamisk ruting

Hvis kunden ønsker dynamisk ruting i IP-VPN nettverket og mellom BKKs kunderuter og kundens eget utstyr, kan dette konfigureres. BKK kan da konfigurere enten BGP, OSPF eller RIP mot kundens utstyr.

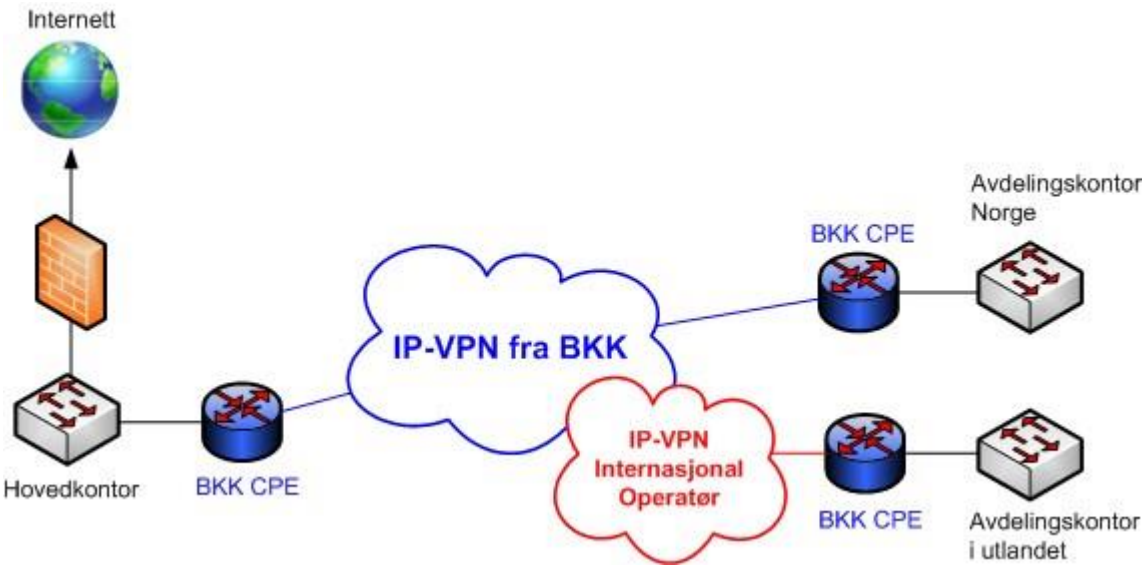
Service Level Agreement (SLA)

BKK tilbyr tre servicenivåer Gull, Sølv og Bronse for alle tjenester. Bronse leveres som standard vederlagsfritt. For tjenester man ønsker et høyere servicenivå for, kan man velge enten servicenivå Sølv eller Gull.

Høyere servicenivå gir en bedre garanti for oppetid, raskere respons i feilsituasjoner, samt mulighet for feilhåndtering utover det som er normal åpningstid.

Internasjonalt IP-VPN

BKK kan i samarbeid med andre internasjonale operatører tilby IP-VPN-samband til hele verden. Et slikt samband realiseres som et virtuelt dedikert samband for kunden, og blir ikke rutet over internett. Dette medfører en mer driftssikker og stabil tjeneste, siden BKK og BKKs samarbeidspartnere har kontroll over nettverket fra ende til ende.



IP-VPN Unmanaged

Med IP-VPN Unmanaged administrerer og drifter kunden sine egne kunderutere i IP-VPN nettverket. Kunden har dermed full kontroll over utstyrsvalg, funksjonalitet, konfigurasjon, overvåking, feilsøking og sikkerhet på alle lokasjoner.

BKK anbefaler at det konfigureres dynamisk ruting med BGP mellom kunderuter og IP-VPN nettverket. På denne måten får kunden en standardisert og fleksibel tjeneste, og kan etablere og endre LAN-adressering i nettverket etter behov, uten å måtte involvere BKK.

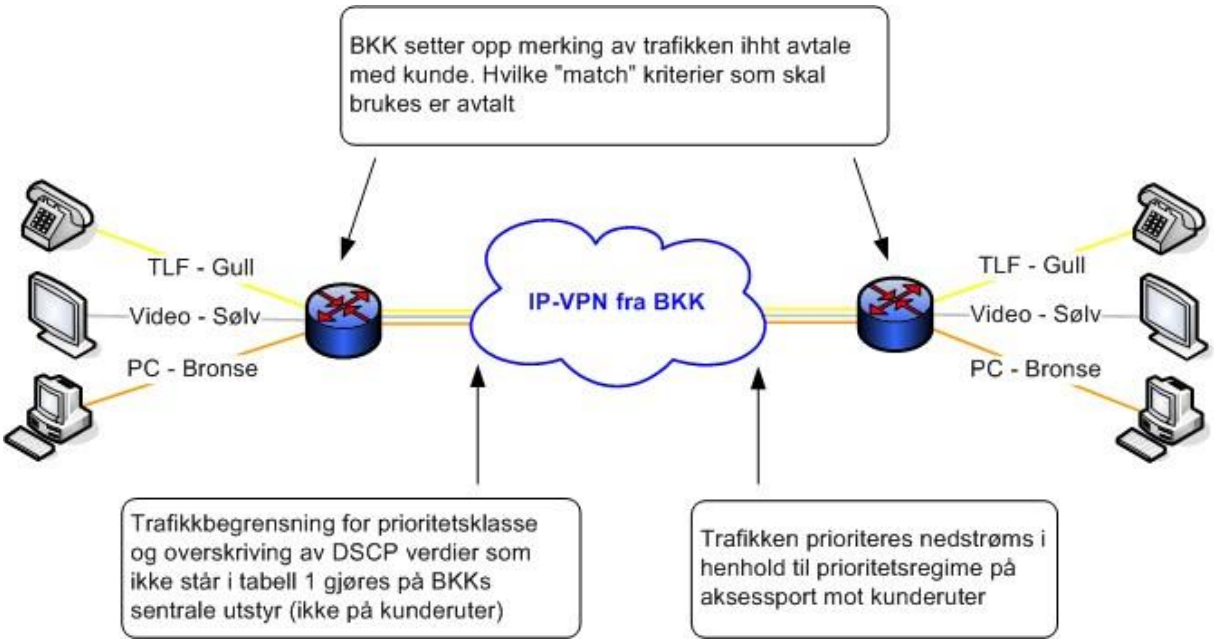
Ta kontakt med BKK for mer informasjon.

Tilleggstjenester

QoS

QoS kan benyttes hvis kunden har trafikktyper, applikasjoner og tjenester som er viktigere enn annen trafikk og som av den grunn må sikres mot pakketap og/eller jitter. Trafikk som merkes med en høyere prioritet blir prioritert og beskyttet gjennom nettet.

QoS kan leveres på samband levert på BKKs egen infrastruktur, og på samband der aksessen leveres via enkelte av BKKs underleverandører.



Merking av trafikk

Det tilbys tjenesteklasser som er basert på DSCP-verdi i pakken. De ulike trafikktypene merkes med klassens tilhørende DSCP verdi før de sendes inn i BKK sitt nett, se tabell under.
Hvilken trafikk som skal klassifiseres i de ulike klassene må avtales mellom kunde og BKK. Det finnes flere måter å klassifisere trafikken på. Dette avtales før QoS implementeres i IP-VPN tjenesten.

Klasse	DSCP	Precedence	Eksempel på bruk
Gull	46 (EF)	5	IP telefoni
Sølv	32	4	Video, kritisk data
Bronse	24	3	Standard data
Best Effort	0	0	Internett trafikk

Vanlige metoder som benyttes for å merke trafikk og skille trafikktypene fra hverandre er:

- IP adresse
- TCP/UDP portnummer
- Protokoll (ved hjelp av NBAR)
- Ingress fysisk og logisk port

All klassifisering foregår oppstrøms sett fra kunde (ingress på port).

Prioritering av trafikk

All prioritering foregår nedstrøms sett fra kunde (egress på port). Prioriteringsmekanismene benytter seg av DSCP verdiene i pakkene og prioriterer basert på disse. Hvilke mekanismer som benyttes er plattformavhengig, men som hovedregelregel benyttes LLQ eller tilsvarende der plattformen støtter det.

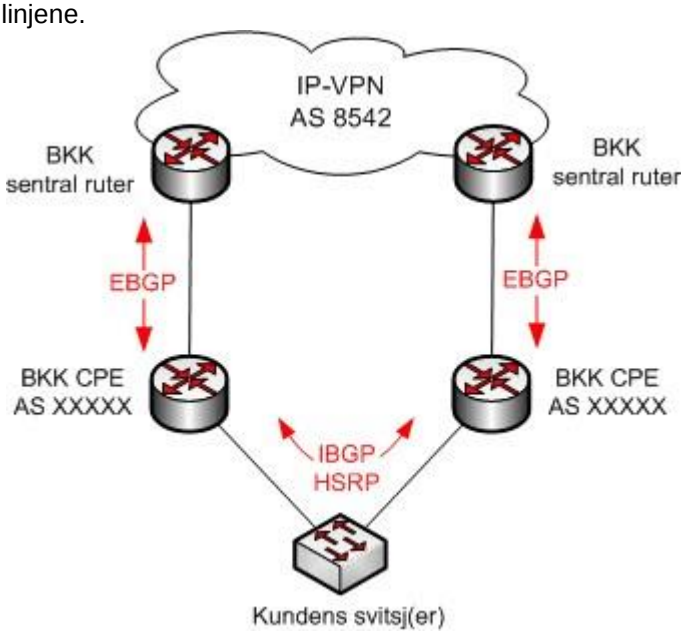
Alle policyer benytter seg av følgende fordeling mellom klassene:

Klasse	Prioritet / garanti	Merknad
Gull	PQ (Priority Queue)	All trafikk i denne kø sendes først uansett. Trafikk i klasse Sølv, Bronse og BE sendes først når alle pakker i klasse Gull er sendt.
Sølv	40% av resterende kapasitet	Garantert minimum 40% av resterende kapasitet etter at "Gull-klassen" har sendt det som skal sendes.
Bronse	40% av resterende kapasitet	Garantert minimum 40% av resterende kapasitet etter at "Gull-klassen" har sendt det som skal sendes
Best Effort	20% av resterende kapasitet	Garantert minimum 20% av resterende kapasitet etter at "Gull-klassen" har sendt det som skal sendes

Kunde kan i utgangspunktet sende inntil 40% av aksesshastighet i trafikklasse Gull inntil en øvre grense på 50 Mbit/s. Dersom 40% av aksesshastighet overstiger 50 Mbit/s settes denne til 50 Mbit/s.

IP-VPN Redundans

BKK kan tilby redundans på IP-VPN-linjer, for å sikre høyest mulig oppetid på sambandet. Redundans oppnås ved å etablere to uavhengige IP-VPN-linjer til samme lokasjon, og etablere dynamisk ruting for automatisk failover ved brudd på den ene linjen. BKK etablerer de to redundante IP-VPN-linjene på helt separate steder i BKKs nettverk, slik at en feil i én del av BKKs nettverk vil ikke påvirke begge linjene.



Kunderuter (CPE)
BKK leverer som standard en komplett redundant løsning med to CPEer, ferdig konfigurert med dynamisk ruting og automatisk failover. BKK leverer alltid redundans med to CPEer for å sikre høyest mulig oppetid.

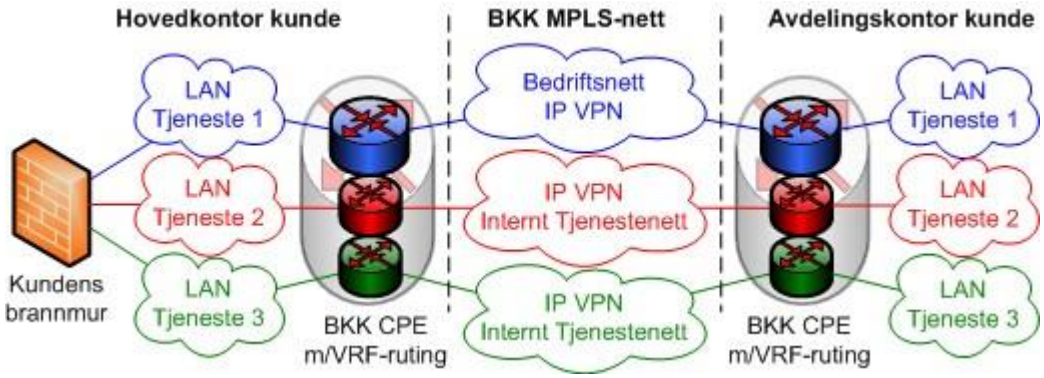
Dynamisk ruting
BGP (Border Gateway Protocol) benyttes som dynamisk ruting protokoll, og settes opp mellom CPEer hos kunde, og mellom CPEer og BKKs sentrale rutere, både på hovedlinje og backuplinje.

HSRP
Mellom BKKs CPEer, på LAN-siden, konfigureres HSRP (Hot Standby Router Protocol) for å gi automatisk failover til backupruter hvis hovedruter skulle gå ned. For at HSRP og den redundante løsningen skal fungere, må BKKs CPEer kobles sammen via kundens lokalnett.

Automatisk failover ved brudd
Ruting-informasjon utveksles ved hjelp av ruting protokollen BGP mellom CPE-ene hos kunden og BKKs sentrale rutere. Den IP-VPN-linjen som er konfigurert som hovedlinje er foretrukket, og trafikken vil gå her i normalsituasjon. Ved et brudd på hovedlinjen vil trafikken automatisk legge seg over på backuplinjen. Når hovedlinjen kommer opp igjen, vil trafikken automatisk legge seg tilbake på den.

Konvergenstid som er tiden det tar fra hovedlinje går ned til trafikken er lagt over på backuplinjen vil variere avhengig av hvilken feil som oppstår, og hvor den oppstår. Maksimal konvergenstid vil være 30 sekunder.

Internt Tjenestenett
IP-VPN Internt Tjenestenett kan benyttes hvis kunden har behov for å kjøre noe trafikk i et dedikert og adskilt nett. Trafikken i et Internt Tjenestenett går helt adskilt fra trafikk i kundens Bedriftsnett IP-VPN, og fra trafikk i andre interne tjenestenett hvis kunden har flere slike nett. Dette gir kunden mulighet til å filtrere trafikk mellom ulike interne tjenestenett i en sentral brannmur. På denne måten kan kunden blant annet sikre at sensitive data blir beskyttet, og at ulike sikkerhets- og tilgangspolicyer blir implementert for ulike deler av nettet sitt.



IP-VPN Internt Tjenestenett blir konfigurert på samme fysiske linje ut til kunden som benyttes av kundens Bedriftsnett IP-VPN-samband, og deler båndbredde med dette sambandet. Hvis det er behov for økt båndbredde, må Bedriftsnett IP-VPN-sambandet oppgraderes med høyere båndbredde.

IP-VPN Internt Tjenestenett blir konfigurert som et eget IP-VPN i BKKs MPLS-nettverk, og rutes i en egen VRF rutingprosess på kunderuter. Trafikk mellom ulike nett er 100% adskilt. IP-VPN Internt

Tjenestenett krever kunderutere som har støtte for VRF-ruting, og kan innebære behov for oppgradering av software på kunderuter.

BKK tildeler WAN-adresser som benyttes mellom BKKs MPLS-nett og kunderuter. Kunden administrerer selv LAN-adresser på alle sine lokasjoner. Kunden får ved bestilling tilsendt et skjema som må fylles med informasjon blant annet om ønskede LAN-adresser. Utfylt skjema sendes til BKKs leveranseavdeling. Det kan konfigureres ruting av flere subnett i ulike VLAN på hver lokasjon. De ulike VLAN kan enten konfigureres på en 802.1Q trunk mot kundens utstyr, eller konfigureres på separate aksessporter hvis dette er tilgjengelig på kunderuter.

Overvåkning og rapportering

BKK kan tilby to ulike rapporter for IP-VPN linjer som er en oppetidsrapport og en kapasitetsrapport. Rapportene blir generert månedlig og er tilgjengelig fra Dinken (Din kundekonto på web). Rapportene viser data fra forrige måned. All data som blir presentert i disse rapportene er samlet inn på kunderuteren fra BKK. Rapportene leveres for linjer med SLA Gull.

Oppetidsrapport viser to ulike variabler:

- Nåbarhet (Reachability) – Viser i % nåbarheten av ruteren sett fra BKK. Det vil si at BKK sine systemer har hatt kontakt med ruteren. Dersom det er problemer med linjen eller at kunderuteren ikke er i orden trekkes dette fra nåbarheten.
- Oppetid (Availability) - Viser i % oppetiden på selve ruteren (System Uptime). Dette er en verdi som viser om ruteren selv har vært operativ. For eksempel hvis ruteren mister strømmen vil dette trekkes fra oppetiden.

Kapasitetsrapport:

- Rapporten viser total trafikk i nettverket med en grafisk representasjon av trafikken. Den kan benyttes til å identifisere overordnede trender i nettverket. Rapporten viser de mest belastede sambandene og kan identifisere problemer slik som for eksempel overbelastede linker. Nye data sammenlignes med ”baseline/normalen” slik at man får frem endringer i trafikken. Det kan estimeres når det er riktig å oppgradere en linje, slik at man ligger i forkant av potensielle problemer. Det er en stor fordel å kunne planlegge og gjennomføre endringer før de begynner å påvirke tjenestene.