



Belastingdienst



AANSLUITVOORWAARDEN NETWERK AANSLUITDIENSTEN DATACENTER BASISKOPPELNETWERK

Datum	7-4-2025
Status	v1.6

1	DOCUMENTEIGENSCHAPPEN	3
2	INLEIDING	4
3	UITGANGSPUNTEN	5
4	ALGEMENE INFORMATIE	6
4.1	BASISKOPPELNETWERK	6
4.2	POINT OF DELIVERY	6
4.3	GENERIEK	7
4.3.1	<i>CE functionaliteit</i>	7
4.3.2	<i>QoS</i>	7
4.3.3	<i>Shaping</i>	8
4.3.4	<i>L3 VPN connectiviteit:</i>	9
4.3.5	<i>IPv6</i>	9
4.3.6	<i>Multicast</i>	9
4.3.7	<i>Onderhoud</i>	9
5	CONNECTIVITEIT POD'S	11
5.1	INTERFACE SPECIFICATIE	11
5.2	INTERFACE FUNCTIONALITEIT	11
5.3	POD CONNECTIVITEIT	12
5.4	AFNEEMBARE DIENSTEN	13
6	VERKLARENDE WOORDENLIJST	14
	BIJLAGE 1 - UBG1	15

1 Documenteigenschappen

Versie voor externe distributie gemaakt door DCS afdeling Netwerken op 2-04-2019 met goedkeuring van afdelings-management.

2 Inleiding

Dit document is opgesteld om duidelijkheid te verschaffen in de faciliteiten die door de Belastingdienst netwerk infrastructuur geleverd worden, en de voorwaarden die door de Belastingdienst netwerk infrastructuur gesteld worden aan oplossingen die aan het Basiskoppelnnetwerk worden aangesloten.

De aansluitvoorwaarden in dit document zijn van toepassing op de bouwsteen Basiskoppelnnetwerk, en gelden voor partijen die willen koppelen aan het Basiskoppelnnetwerk binnen het ODC Belastingdienst.

In het document worden de aansluitvoorwaarden beschreven als **STANDAARD**, **MOGELIJK** of **OPTIE**. Daarmee wordt het volgende bedoeld:

STANDAARD	Een aansluitvoorwaarde die als standaard gedefinieerd is binnen de service.
MOGELIJK	Een keuzemogelijkheid die ontworpen is en beschikbaar binnen de service.
OPTIE	Een optie is een keuzemogelijkheid die niet breed beschikbaar is of verder ontworpen kan worden binnen de service. Opties moeten aangevraagd.

3 Uitgangspunten

Voor aansluiting van oplossingen aan het Basiskoppelnetwerk in het datacenter van de Belastingdienst zijn een aantal uitgangspunten belangrijk:

- IP Multicast wordt op dit moment niet ondersteund binnen de service Network Connectiviteit.
- Het BKN is volledig IPv6 geschikt, maar bepaalde domeinen binnen de Infrastructuur zijn op dit moment nog niet helemaal geschikt voor IPv6. Daarom is IPv6 connectiviteit voor oplossingen die aan het Basiskoppelnetwerk worden aangesloten in deze gevallen geen standaard afneembare dienst.
- L2VPN diensten worden niet geleverd op het BKN.

4 Algemene informatie

4.1 Basiskoppelnetwerk

Het Basiskoppelnetwerk (BKN) levert de functionaliteit om binnen het OverheidsDataCenter (ODC) van de Belastingdienst, Belastingdienst omgevingen en andere overheidspartijen te kunnen koppelen. Uitgangspunt daarbij is dat de verkeersstromen logisch gescheiden lopen van de verkeersstromen van de Belastingdienst om de continuïteit voor de verschillende onderdelen van de Belastingdienst en andere overheidspartijen te garanderen.

Het Basiskoppelnetwerk is een verbindend bouwblok binnen de bouwblokken van de datacenter infrastructuur.

Geconfigureerde verkeerstromen mogen elkaar niet beïnvloeden en moeten logisch volledig gescheiden zijn om de beveiliging (beschikbaarheid, exclusiviteit, integriteit en controleerbaarheid) te kunnen waarborgen voor de aangesloten omgevingen.

4.2 Point Of Delivery

Een Point of Delivery (POD) is een modulaire zelfstandige infrastructuur waar binnen stacks, platformen, netwerken, storage, beheer en beveiliging ingericht is.

Een POD is een schaalbare omgeving met een specifieke functionaliteit. Deze kan generiek inzetbaar zijn of een specifiek inzet gebied hebben voor een klant.

Voor een POD geldt dat er een duidelijke scheiding van verantwoordelijkheden is. De verantwoordelijkheid voor de POD ligt bij één partij, de eigenaar van de POD.

Een POD wordt zelfstandig beheerd en maakt tevens gebruik van gemeenschappelijke voorzieningen in de generieke infrastructuur.

POD's kunnen met elkaar verbonden worden voor schaalbaarheid en continuïteit.

De gemeenschappelijke ODC-netwerk infrastructuur wordt aangeboden op het niveau Semi-vertrouwd. Departementaal Vertrouwelijk.

Voorwaarden voor beheer:

- Er is een beheer omgeving binnen het ODC van waaruit de generieke ODC diensten beheerd worden door en voor de ODC service organisatie.
- Een POD is zelf verantwoordelijk voor een beveiligde beheer omgeving.

Voorwaarden voor (netwerk)beveiliging:

- Een POD is zelf verantwoordelijk voor de beveiliging op het gewenste niveau conform de richtlijnen in de BIO en VIR-BI.
- Beveiliging in lijn met de NORA beveiligingspatronen¹ voor netwerk zonering.
- Indien een POD verstoring veroorzaakt op de netwerkinfrastructuur buiten de eigen POD omgeving, behoudt DCS zich het recht voor deze af te sluiten.

Een POD is een op zichzelf staande omgeving die als eenheid uniek gekoppeld wordt aan het BKN. Het koppelvlak (de CE) is per POD uniek.

4.3 Generiek

4.3.1 CE functionaliteit

Er is een grote verscheidenheid aan producenten van CE (Consumer Edge) devices. Elk merk, of type CE heeft zijn eigen features en/of beperkingen welke van invloed kunnen zijn op de flexibiliteit en functionaliteit van het koppelvlak. Bij sommige types is het bijvoorbeeld niet mogelijk L3 VPN's op dezelfde fysieke link aan te bieden. Daarom is het verstandig om voorafgaand aan de koppeling van een POD afstemming te hebben over de te gebruiken CE.

De verantwoordelijkheid voor de CE ligt bij de eigenaar van de POD.

4.3.2 QoS

Quality Of Service is een mechanisme dat er bij congestie voor kan zorgen dat bepaalde verkeersstromen voorrang krijgen op andere. Om dit goed te laten functioneren dient QoS end-to-end ingericht te zijn.

DE BKN infrastructuur is transparant voor QoS markeringen die binnen een POD worden aangebracht. Dat wil zeggen dat wat aan de BKN infrastructuur wordt aangeboden door het BKN met dezelfde markering op de bestemming wordt afgeleverd.

Om te voorkomen dat queues vollopen, en daardoor verkeer wordt weggegooid worden queueing maatregelen genomen.

Binnen de BKN infrastructuur wordt verkeer over 4 queues verdeeld:

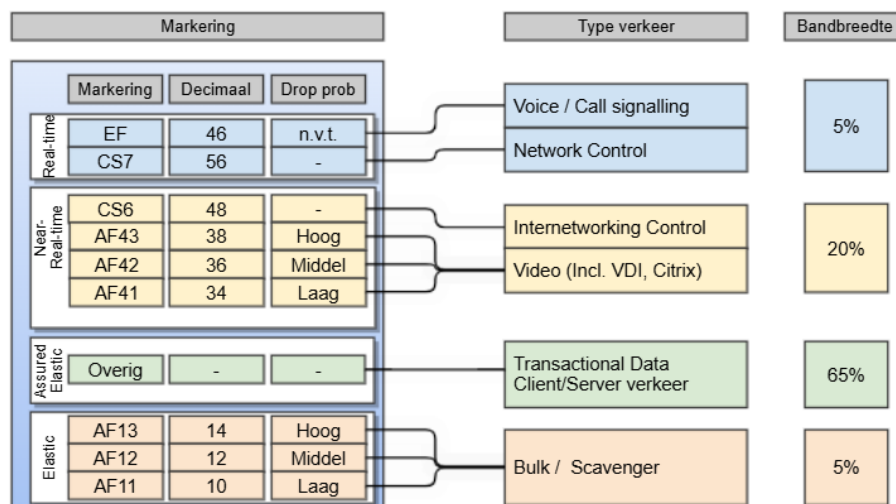
- Real-time, Near Real-time, Assured-Elastic, Elastic

	Markering	Decimaal	Drop prob
Real-time	EF	46	n.v.t.
	CS7	56	-
Near-Real-time	CS6	48	-
	AF43	38	Hoog
	AF42	36	Middel
	AF41	34	Laag
Assured-Elastic	Overig	-	-
Elastic	AF13	14	Hoog
	AF12	12	Middel
	AF11	10	Laag

Figuur 1; QoS marking/queue mapping binnen BKN

¹ Bijvoorbeeld deze patronen voor externe koppelingen:
https://www.noraonline.nl/wiki/Patroon_voor_extern_koppelvlakken

Hieronder volgt een voorzet voor de mapping van bepaalde typen verkeer op het model en de daarbij behorende bandbreedte reserveringen per klasse.



Figuur 2; QoS mapping typen verkeer

4.3.3

Shaping

De POD dient het verkeer aan te bieden op de bandbreedte die op het BKN koppelvlak (PE-CE) is afgesproken. Verkeer aangeboden buiten de afgesproken bandbreedte wordt niet getransporteerd.

4.3.3.1

Ingress en egress QoS

Voor verkeer dat door de POD aan de BKN infrastructuur wordt aangeboden gelden de volgende reserveringen:

QoS Profile	Reservering
Real-time	5% van de beschikbare bandbreedte
Near Real-time	20% van de beschikbare bandbreedte
Assured-Elastic	65% van de beschikbare bandbreedte
Elastic	5% van de beschikbare bandbreedte

Tabel 1; Ingress en egress QoS

4.3.4 *L3 VPN connectiviteit:*

Voor alle L3 VPN's gelden de volgende voorwaarden:

- Eén VLAN nummer per VRF voor de point-to-point link tussen PE en CE.
- Eén IP adres (default /31 en optioneel /30) per interface voor de point-to-point link tussen PE en CE voor verkeer naar het internet. Het IPv4 en IPv6 adres wordt door DCS toegekend.
- Maximaal 1000 routes (prefixen) per VPN. Meer prefixen moeten expliciet aangevraagd worden.
- Prefixen worden gefilterd alvorens ze op een VPN worden aangeboden.
Publieke reeksen worden naar het Internet VPN gerouteerd, private reeksen naar één of meerdere data VPN's. Welke reeksen op welk VPN worden aangeboden dient tussen DCS en de klant te worden afgestemd.
Het BKN verzorgt geen filtering van/voor verkeer binnen een VPN.

4.3.5 *IPv6*

Het BKN is volledig IPv6 geschikt, maar bepaalde domeinen binnen de Infrastructuur zijn op dit moment nog niet helemaal geschikt voor IPv6. Daarom is IPv6 connectiviteit voor oplossingen die aan het Basiskoppelnnetwerk worden aangesloten in deze gevallen geen standaard afneembare dienst.

- Eén VLAN nummer per VRF voor de point-to-point link tussen PE en CE.
- Eén /64 subnet per interface voor de point-to-point link tussen PE en CE voor verkeer naar het internet. Het IPv6 subnet wordt door DCS toegekend.
- Maximaal 1000 routes (prefixen) per VPN. Meer prefixen moeten expliciet aangevraagd worden.
- Prefixen worden gefilterd alvorens ze op een VPN worden aangeboden.
Publieke reeksen worden naar het Internet VPN gerouteerd, private reeksen naar één of meerdere data VPN's. Welke reeksen op welk VPN worden aangeboden dient tussen DCS en de klant te worden afgestemd.
Het BKN verzorgt geen filtering van/voor verkeer binnen een VPN.

4.3.6 *Multicast*

Op dit moment is Multicast voor POD's nog geen afneembare dienst.

4.3.7 *Onderhoud*

Om onderhoud te kunnen uitvoeren op de BKN infrastructuur, zonder dat de aangesloten POD's daar hinder van ondervinden zijn 3 mechanismes ingericht.

4.3.7.1 *Multi-exit discriminator (MED)*

Door middel van het BGP MED attribuut wordt aangegeven wat het beste pad is naar het BKN. Hierbij zal de laagste MED bepalend zijn. In geval van onderhoud op het BKN wordt middels het MED attribuut de PE die in onderhoud wordt genomen het minst aantrekkelijk gemaakt waardoor deze door de POD niet meer gebruikt wordt en in onderhoud genomen kan worden.

Tijdens het onderhoud zal er een vermindering zijn van de beschikbare bandbreedte zijn ten opzichte van de normale situatie.

4.3.7.2 Community (optioneel)

Het BGP community attribuut maakt het mogelijk om prefixen van een label te voorzien.

In geval van onderhoud op het BKN wordt een label aan de prefixen toegevoegd. Bij detectie van dit label wordt de local preference voor die prefix aangepast waardoor de POD de betreffende PE voor deze prefix uiteindelijk niet meer gebruikt, en deze in onderhoud genomen kan worden.

Tijdens het onderhoud zal er een vermindering zijn van de beschikbare bandbreedte zijn ten opzichte van de normale situatie.

4.3.7.3 AS Prepending

BGP AS prepending maakt het mogelijk om prefixen te voorzien van extra Autonomous System's (AS).

In geval van onderhoud op het BKN wordt het BKN AS 5x aan de prefixen toegevoegd (geprepend). Hierdoor wordt het AS pad voor deze prefixen langer, en daarmee onaantrekkelijker gemaakt.

De POD zal deze prefixen niet meer prefereren en de kortere paden gebruiken, waardoor de betrokken PE kan in onderhoud genomen kan worden.

Tijdens het onderhoud zal er een vermindering zijn van de beschikbare bandbreedte zijn ten opzichte van de normale situatie.

5 Connectiviteit POD's

Interface specificatie		
Onderwerp	Keuze	Opmerking
100 Gbps fiber	STANDAARD: Fiber Multi en Single Mode met LC connector QSFP form factor	Deze optics liggen niet standaard op voorraad en dienen besteld te worden.
10 Gbps fiber	OPTIONEEL: Fiber Multi Mode SFP+ form factor	Deze optics liggen niet standaard op voorraad en dienen besteld te worden. 10 Gbps koppeling op basis van een breakout kabel.
connectiviteit	STANDAARD: redundante koppeling (2 CE's koppelen aan 2 PE's) MOGELIJK: enkelvoudige koppeling (1 CE koppelen aan 1 of 2PE's)	Flow-based Loadbalancing op basis van ECMP Een enkelvoudige koppeling heeft tot gevolg dat er bij onderhoud door DCS in sommige gevallen verstoring voor de POD kan optreden.

Interface functionaliteit		
Onderwerp	Keuze	Opmerking
Routing	STANDAARD: BGP	Authenticatie BGP peers d.m.v. een wachtwoord.
MTU	STANDAARD: 8800 bytes	
VRF	STANDAARD: Verkeer wordt op basis van VRF aan de CE aangeboden.	
BFD	OPTIE: BFD	Omdat BFD zich tussen verschillende merken en platformen anders kan gedragen is BFD niet standaard.
BGP opties/timers	STANDAARD: KeepAlive Interval 30 seconden Hold down Timer 90 seconden	
QoS	STANDAARD: 4 queues per POD MOGELIJK: 4 queues per tenant.	Voor meer details omtrent de inrichting van QoS zie paragraaf 4.3.2

Interface functionaliteit		
POD connectiviteit		
Onderwerp	Keuze	Opmerking
L3 BD VPN	MOGELIJK: Connectiviteit naar de Belastingdienst omgeving met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	Dit VPN is bedoeld om PODs welke diensten voor de Belastingdienst levert, te koppelen.
L3 DC-I VPN	MOGELIJK: Connectiviteit tussen de POD en een backend omgeving in een ander ODC met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	DC-I is datacenter interconnect. Dit VPN is bedoeld voor communicatie tussen backends (datacenter omgevingen) binnen de rijksoverheid.
L3 WAN-I VPN	MOGELIJK: Connectiviteit tussen een POD en andere partijen met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	WAN-I is bedoeld voor connectiviteit tussen werkplekken en VPN gateways van de rijksoverheden.
L3 Partner-I VPN	MOGELIJK: Connectiviteit tussen een POD en eindgebruikers met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	Partner-I is bedoeld voor communicatie tussen partijen binnen en buiten (zoals gemeentes, provincies) de rijksoverheid.
L3 Internet VPN	MOGELIJK: Connectiviteit naar Internet via het beveiligde koppelvlak van de Belastingdienst met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	Dit VPN is bedoeld om een POD op internet te ontsluiten. Let op: beveiliging van de naar Internet gerichte communicatie ligt bij de POD eigenaar. Voor Belastingdienst diensten Internet ontsluiting kan ook gebruik gemaakt worden van de Belastingdienst DMZ.
L3 specifiek VPN	OPTIE: Specifieke connectiviteit naar een andere dan de generieke omgevingen kan gerealiseerd worden in overleg met vooraf afgestemde maximale bandbreedte. (Zie paragraaf 4.4.4)	Connectiviteit met een specifiek VPN moet ontworpen worden.
IP adressen Koppelnetwerken	STANDAARD: IP adressen voor koppelnetwerken worden door ODC Belastingdienst uitgegeven uit de in het Rijksnummerplan ICT aan ODC Belastingdienst toegewezen reeksen.	

Interface functionaliteit		
IP adressen Interne PODS	STANDAARD: IP adressen voor gebruik binnen de POD worden door ODC Belastingdienst uitgegeven uit de in het Rijksnummerplan ICT aan ODC Belastingdienst toegewezen reeksen.	
IP adressen externe PODS	STANDAARD: IP adressen voor gebruik binnen de POD worden door het ODC van de ICT dienstverlener van de POD eigenaar uitgegeven uit de in het Rijksnummerplan ICT aan het betreffende ODC toegewezen reeksen.	
AS nummers	STANDAARD: AS nummers van alle aangesloten POD's (zowel intern als extern) worden door ODC Belastingdienst uitgegeven en komen uit de reeks 32-bit AS nummers die zijn toegewezen in het Globaal Ontwerp RON.	

Afneembare diensten		
Onderwerp	Keuze	Opmerking
NTP	MOGELIJK: NTP stratum 1 tijd afname.	
DNS	MOGELIJK: Forwarding relatie	

6 Verklarende woordenlijst

VRF	Virtual Routing and Forwarding. Een techniek om meerdere gescheiden en onafhankelijke routerings tabellen op één enkele router te implementeren
BGP	Border Gateway Protocol. Een routeringsprotocol voor de uitwisseling van routeringsinformatie tussen routers onderling.
MTU	Maximum Transmission Unit Is de grootste data-eenheid die door een TCP/IP netwerk kan worden afgeleverd
BFD	Bidirectional Forwarding Detection. Een protocol voor snelle detectie van fouten op verbindingen.
VPN	Virtual Private Network. Een techniek om een netwerk 'getunneld' over een ander netwerk te transporteren.

Bijlage 1 - UBG

UBG staat voor Uitvoeren, Beoordelen, Goedkeuren Informeren.

Deze bijlage met namen van medewerkers, functies, review details en akkoorden is niet geschikt voor externe communicatie en is daarom een separaat bestand.