



Belastingdienst



AANSLUITVOORWAARDEN NETWERK AANSLUITDIENSTEN KANTOOR

Datum 11.6-2018
Status V1.0

1	INLEIDING	3
1.1	BASIS / PLUS / SPECIALS	3
1.2	STANDAARD / MOGELIJK / OPTIE	4
1.3	IP ADRESSEN EN NAAMGEVING	4
2	ALGEMENE INFORMATIE	5
2.1	UITGANGSPUNTEN	5
3	BEDRAAD NETWORK	6
3.1	COMPARTIMENTERING	6
3.1.1	<i>Departement Specifiek</i>	6
3.1.2	<i>toewijzing van een compartiment</i>	6
3.2	VOIP TELEFOON	8
3.3	POWER OVER ETHERNET	8
3.1	QoS	9
4	WIFI	11

1 Inleiding

Dit document is opgesteld om duidelijkheid te verschaffen in de faciliteiten die door DCS netwerk infrastructuur geleverd worden in de kantoor omgeving, en de voorwaarden die door DCS netwerk infrastructuur gesteld worden aan platformen die aansluiten op deze infrastructuur.

Deze aansluitvoorwaarden zijn van toepassing op de dienst
Netwerk Aansluitdiensten Kantoor.

De aansluitvoorwaarden zijn opgesplitst in 3 secties:

- Algemeen
- Bedraad.
- WiFi.

1.1 Basis / Plus / Specials

Er zijn drie typen ICT diensten te onderscheiden. De Basis- en Plusdiensten zijn beschreven in deze aansluitvoorwaarden. Van de beschrijvingen mag niet worden afgeweken, in geval van afwijken zal er een Special dienstverlening ontstaan.

Basisdiensten	Deze zijn verplicht aanwezig in elk rijkskantoor en worden doorbelast aan alle bewoners conform het prijsmodel wat bij de dienstbeschrijving is opgenomen.
Plusdiensten	Deze gestandaardiseerde diensten zijn in elk rijkskantoor leverbaar en kunnen worden besteld via bestaande bestelafspraken en systemen. Deze diensten worden doorbelast aan de aanvrager conform het prijsmodel dat bij de dienstbeschrijving is opgenomen. Afname van deze diensten is niet verplicht. Indien een plusdienst niet toe te wijzen is aan een specifieke aanvrager of gebruikersorganisatie, omdat deze in een gedeelde ruimte wordt geplaatst (zoals een vergaderzaal), volgt DCS het model voor de kostenverdeling van deze ruimte.
Specials	In bijzondere gevallen wordt met de basis- en plusdiensten geen invulling gegeven aan primaire functionele behoeften van de gebruikersorganisatie ¹ . In dit geval voert DCS in opdracht van de gebruikersorganisatie een onderzoek uit hoe deze functionele wensen kunnen worden ingevuld. Onderzoek, levering en beheer van specials wordt door DCS direct gefactureerd aan de gebruikersorganisatie. Na de onderzoeksfase moet de special voor goedkeuring worden ingediend bij CIO Rijk die het voorstel zal beoordelen en eventueel voorleggen aan de CTO raad. Deze procedure is noodzakelijk omdat een special altijd een negatieve impact heeft op de basisdienstverlening in het rijkskantoor. Specials worden na goedkeuring openbaar gemaakt op het rijksportaal.

¹ Afwijkingen van in de rijksPDC beschreven diensten of aanvullende diensten worden gekwalificeerd als special dienstverlening en zijn onderhevig aan de beschreven goedkeuringsprocedure

1.2 Standaard / Mogelijk / Optie

Binnen de ICT diensten Basis, Plus en Specials wordt onderscheid gemaakt in de aansluitopties. Deze zijn beschreven als STANDAARD, MOGELIJK of OPTIE. Daarmee wordt het volgende bedoeld:

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

1.3 IP adressen en naamgeving

IP adressen en naamgeving gebeurd op basis van onderstaande documenten:

Onderwerp	Titel	Versie/Datum
IP nummerplan	IPv4 nummerplan	1.1 / 28-03-2011
DNS naamgeving	IP management naamconventies	3.2 / 25-07-2011

Voor de laatste versies gelieve contact op te nemen met DCS Infra Netwerken.

2 Algemene informatie

Fysieke aansluitpunten in een kantoor worden geleverd door het Rijksvastgoedbedrijf conform het geldende HIB (Handboek ICT ruimtes en Bekabeling).
Binnen de Belastingdienst kantoren levert de CFD (facilitaire dienst) de patch bekabeling voor het patchen van de bedrade aansluitingen.
DCS conformeert zich aan de IDWOR kaders en de rPDC voor rijkskantoren.

2.1 Uitgangspunten

Voor aansluiting van bedrijfsmiddelen op de netwerk infrastructuur in de kantoren van de Belastingdienst zijn een aantal uitgangspunten belangrijk:

Algemene uitgangspunten		
Onderwerp	Keuze	Opmerking
IP Multicast	IP Multicast wordt niet ondersteund.	
IP Versie 6	IP Versie 6 wordt niet ondersteund.	- In de toekomst zal dit wel ingevoerd worden.
NTP	NTP wordt generiek aangeboden.	- Uitzondering hierop kan gegeven worden in het Departement specifiek compartiment.
DHCP	DHCP wordt generiek aangeboden.	- Uitzondering hierop kan gegeven worden in het Departement specifiek compartiment.
DNS	DNS wordt generiek aangeboden.	- Uitzondering hierop kan gegeven worden in het Departement specifiek compartiment.
End Point Isolation	Er wordt geen verkeer toegestaan tussen End-Points.	- Uitzondering hierop kan gegeven worden in het Departement specifiek compartiment.
MTU	Een IP-MTU van maximaal 1500 bytes wordt ondersteund.	

3 Bedraad netwerk

Onder Bedraad netwerk worden vaste aansluitingen voor werkplekken of andere eindgebruikers apparatuur (zoals printers en IP-telefoons) binnen de Belastingdienst locaties verstaan.

3.1 Compartimentering

Binnen de Belastingdienst locaties zijn de volgende compartimenten beschikbaar voor het bedraad aansluiten van bedrijfsmiddelen:

Belastingdienst-Intern

Bedoeld voor Belastingdienst bedrijfsmiddelen.

De werkplekken van de Belastingdienst worden t.z.t. gemigreerd naar het RijkskantoorRoam compartiment.

Als alle werkplekken over zijn naar het RijkskantoorRoam compartiment zullen de overgebleven devices worden verhuist naar een Belastingdienst_Gebouw-Gebonden-Compartiment. Belastingdienst-Intern komt op dat moment te vervallen.

RijkskantoorRoam

Bedoeld voor bedrijfsmiddelen verstrekt door de rijksoverheid

3.1.1 *Departement Specifiek*

Naast de hier boven genoemde compartimenten is het mogelijk om, in overleg, een eigen afwijkend compartiment in te richten. Hieraan zijn wel afspraken gebonden.

Verkeer tussen de compartimenten is niet toegestaan!

3.1.2 *toewijzing van een compartiment*

Voor toewijzing van een compartiment aan een device wordt gebruik gemaakt van 802.1x. Voor de authenticatie van het device dient deze voorzien te zijn van een geldig overheids certificaat waarbij de uitgever hiervan over DC-i benaderbaar dient te zijn vanuit DCS om de geldigheid van het certificaat te kunnen controleren.

Bij een negatieve authenticatie wordt er geen netwerk toegang verleend!

Geboden compartimenten		
Onderwerp	Keuze	Opmerking
Belastingdienst Intern netwerk	BASIS: Belastingdienst-Intern Voor Belastingdienst DWB werkplekken.	STANDAARD: - Alleen voor Belastingdienst bedrijfsmiddelen. - Toegang tot het netwerk wordt alleen verleend op basis van 802.1x authenticatie. - Het gebruik van certificaten is een vereiste voor 802.1x authenticatie. MOGELIJK:

		- 802.1x authenticatie kan op basis van UserID/Password. Echter heeft dit geen voorkeur. OPTIE: - 802.1x authenticatie op basis van MAC adres wordt alleen toegestaan onder voorwaarden.
RijkskantoorRoam	BASIS: RijkskantoorRoam Bedoeld voor door een IDV-G geleverde bedrijfsmiddelen.	STANDAARD: - Alleen voor bedrijfsmiddelen verstrekt door de rijksoverheid. - Toegang tot het netwerk wordt alleen verleend op basis van 802.1x authenticatie. - Het gebruik van certificaten is een vereiste voor 802.1x authenticatie. - Bied toegang tot de IDV-G frontend.
Dep-Specifiek	SPECIAL: Dep-Specifiek	STANDAARD: - Heeft een aanwijsbare verantwoordelijke afnemer. - Kan meerdere keren voorkomen op een locatie. - Toegang tot het netwerk wordt alleen verleend op basis van 802.1x authenticatie. - Het gebruik van certificaten is een vereiste voor 802.1x authenticatie. MOGELIJK: - 802.1x authenticatie kan op basis van UserID/Password. Echter heeft dit geen voorkeur. OPTIE: - 802.1x authenticatie op basis van MAC adres wordt alleen toegestaan onder voorwaarden.

Interface specificatie		
Onderwerp	Keuze	Opmerking
10/100 Mbps, 1 Gbps	STANDAARD: Autonegotiate, Koper met RJ45 connector.	
Connectiviteit	STANDAARD: Enkelvoudig.	De hoeveelheid toegestane MAC adressen per poort is beperkt tot maximaal 2, bridging achter werkplek aansluitingen wordt niet toegestaan.
Power over Ethernet	STANDAARD: IEEE802.1af/at Onderhandeling met LLDP anders standaard klasse 0	(Zie sectie Power over Ethernet).

	OPTIE: Klasse 1, 2, 3 of 4	
--	-------------------------------	--

3.2

Voip telefoon

Vaste telefonie wordt alleen vanuit DCS geleverd.

Bedrade netwerk connectiviteit via een patchpunt op een voip telefoon moet zo geconfigureerd zijn dat de standaard netwerk aansluitvoorwaarden van toepassing zijn voor deze aansluitpunten.

3.3

Power over Ethernet

Standaard wordt het vermogen tussen het eind device en de netwerk switch onderhandeld met het LLDP protocol. Zonder deze onderhandeling wordt vermogensklasse 0 (15,4W) ingesteld/gereserveerd. Het benodigde vermogen tussen een POE(+) device en de switch moet volgens de IEEE 802.3af / IEEE 802.3at standaard worden afgehandeld.

Klasse	IEEE Standaard	Minimum geleverd vermogen van de voedingsbron.	Maximum opgenomen vermogen van het te voeden apparaat.
0	IEEE 802.3af	15.4W	0.44 to 12.95W
1	IEEE 802.3af	4.0W	0.44 to 3.84W
2	IEEE 802.3af	7.0W	3.84 to 6.49W
3	IEEE 802.3af	15.4W	6.49 to 12.95W
4	IEEE 802.3at POE+	29.5W	12.95 to 29.5W

Tabel 1; IEEE 802.3af / at vermogensklassen van de voedingsbron en het te voeden apparaat.

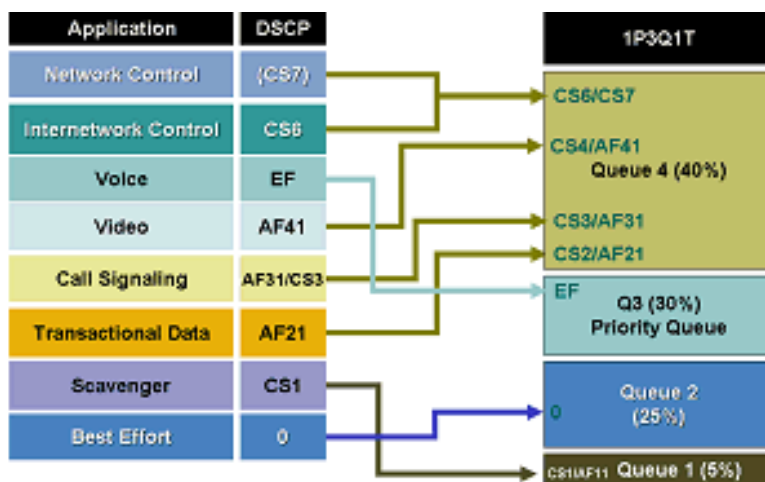
Interface functionaliteit		
Onderwerp	Keuze	Opmerking
VLAN	STANDAARD: VLAN toekenning gebeurt op basis van 802.1X. MOGELIJK: Poort met additioneel Voice VLAN. Voice VLAN toekenning gebeurt op basis van 802.1X. OPTIE: Poort geconfigureerd in vast data VLAN.	Voor het Voice VLAN is een beperkte vorm van IEEE802.1q geïmplementeerd.
Routing	STANDAARD: Systemen krijgen via DHCP een default gateway aangeboden.	

Packet forwarding	STANDAARD: Packet forwarding wordt niet toegestaan.	Packet forwarding is het routeren van pakketten op laag 3 van de TCP/IP stack op een systeem.
QoS (zie sectie QoS)	STANDAARD: Algemeen verkeer in Best Effort Queue. VoIP verkeer in Priority queue. Call Signalling in Call-Signalling Queue. OPTIE: Bepaalde verkeers-stromen in andere QoS klasse.	Aanvraag voor andere verkeersklassen in overleg.
IP adres	STANDAARD: Dynamische adres uitgifte via DHCP. OPTIE: Bij dynamische uitgifte worden de extra benodigde variabelen via DHCP optie 55 aangegeven. OPTIE: Op verzoek kunnen andere opties worden meegegeven.	Voor vaste telefonie wordt in de optionspace een 'vendor specific' option 43 gedefinieerd met alle relevante tags voor het toestel. Binnen de optie worden geen 'magic cookies' toegestaan, enkel tags met type, length, value. De Belastingdienst hanteert de 'vendor specific' aanbeveling uit RFC 2132.
DNS	STANDAARD: Dynamische DNS entries.	Dynamische DNS voor end-user devices.

3.1

QoS

Binnen het bedrade netwerk wordt gebruik gemaakt van Quality of Service. In onderstaande tabel is de technische invulling van de QoS weergegeven.



Figuur 1; overzicht QOS

In bovenstaande tabel is als voorbeeld voor VoIP per type verkeer de markering en de wijze waarop gemarkeerd wordt weergegeven. Het Voice verkeer (EF) wordt afgehandeld in de priority queue, deze queue heeft de hoogste prioriteit en gaat dus voor op al het andere verkeer in de overige queues. De call signaling (AF31/CS3) wordt afgehandeld in queue 'Call Signaling' welke een lagere prioriteit heeft.

4

WiFi

Naast het bedrade netwerk wordt er ook WiFi aangeboden.

Uitgangspunt voor dekking is dat de fysieke werkplekken, binnen de kantoren, en de vergader locaties voorzien zijn van dekking. In trappenhuizen, parkeerterrein, toiletten etc. wordt geen dekking gegarandeerd.

Toegang tot de Wifi netwerken Belastingdienst-Intern, RijkskantoorRoam en govroom wordt op basis van een user certificaat gegeven welke door de eigen IDV-G organisatie moet worden uitgegeven.

Een WiFi gast-account kan door de servicebalie in het verzamelgebouw worden aangemaakt.

Interface specificatie		
Onderwerp	Keuze	Opmerking
Frequentieband	STANDAARD: Banden AGN Frequentie 2,4 en 5 GHz.	De volgende standaarden worden geboden: - IEEE 802.11a / g / n / ac ac afhankelijk van het kantoor (2018-2020)
SSID voor Intern netwerk	STANDAARD: Belastingdienst-Intern voor Belastingdienst DWB werkplekken.	- Alleen voor DWB werkplekken. - Client dient de volgende security protocollen te ondersteunen: - WPA2 enterprise. - Geldig machine certificaat. - DWB werkplek dient voorzien te zijn van WiFi policy.
SSID voor Intern netwerk	STANDAARD: RijkskantoorRoam voor door een IDV-G geleverde bedrijfsmiddelen.	- Alleen voor bedrijfsmiddelen verstrekt door de rijksoverheid. - Client dient de volgende security protocollen te ondersteunen: - WPA2 enterprise. - Geldig machine certificaat .
SSID voor Extern netwerk	STANDAARD: govroom voor toegang tot Internet met overige hardware van govroom deelnemers.	- Voor toegang tot Internet voor Govroom deelnemers. - Client dient de volgende security protocollen te ondersteunen: - WPA2 enterprise. - PEAP MS Chap v2. - EAP-TLS.
SSID voor Extern netwerk	STANDAARD: Belastingdienst-Gasten voor toegang tot Internet voor gasten.	- Voor toegang tot Internet voor gasten. - Client dient de volgende security protocollen te ondersteunen: - WPA2 Pre Shared key. - PEAP MS Chap v2. (WPA wordt eind 2018 vervangen voor PEAP).

Interface functionaliteit

Onderwerp	Keuze	Opmerking
VLAN	STANDAARD: Het device krijgt dynamisch een VLAN toegewezen tijdens het aanmeld proces.	
Routing	STANDAARD: Systemen krijgen via DHCP een default gateway aangeboden.	
Packet forwarding	STANDAARD: Packet forwarding wordt niet toegestaan.	Packet forwarding is het routeren van pakketten op laag 3 van de TCP/IP stack op een systeem. Alleen verkeer naar de gateway is toegestaan.
WMM	STANDAARD: WMM is niet actief.	
Bandbreedte restrictie	STANDAARD: Voor Belastingdienst-Intern en RijkskantoorRoam gelden geen bandbreedte restricties. Voor govroam en Belastingdienst-Gasten geldt een restrictie van 10Mbps per device.	
IP adres	STANDAARD: Dynamische adres uitgifte via DHCP.	
DNS	STANDAARD: Dynamische DNS entries.	
Filtering	STANDAARD: Op de Internet toegang voor govroam en Belastingdienst-Gasten wordt een beperkte vorm van filtering en virusscanning toegepast.	Torrent verkeer en poort 25 worden gefilterd. Daarnaast wordt Virus scanning toegepast.

Mede gezien er geen sluitende dekking is binnen de kantoren wordt VOIP over Wifi op basis van best effort ondersteund.