



EINDHOVEN

Bijlage 1: Beschrijving huidige situatie

**Europese aanbesteding Onderhoud en support netwerkinfrastructuur
inclusief vervangingen / uitbreidingen
Gemeente Eindhoven MTK01062023**

Gemeente Eindhoven
IB - Informatisering & Beheer, DNST - Diensten
Versie 1.0 Initiatiefase
maart 2023

Inhoudsopgave

	Inhoudsopgave	2
1	Inleiding	3
2	MAN module	4
2.1	BRE Glasvezelnetwerk	4
2.2	Infinera multiplexers	4
3	Service module	5
3.1	Service core	5
4	Access Management	6
4.1	Cisco ISE	6
4.2	Access control LAN	6
4.3	Access control WLAN	6
4.4	Access control netwerkkapparatuur	6
5	DNA Campus netwerk	7
5.1	DNA-controllers	7
5.2	DNA Core-laag	7
5.2	DNA Distributie-laag	7
5.2.1	Distributiemodel A	8
5.2.2	Distributiemodel B	8
5.2.3	Distributiemodel C	10
5.3	Access-laag LAN	11
5.4	Wireless netwerk	11
5.4.1	WLC wireless controllers	11
5.4.2	Wireless Access Points	12
6	Data Center netwerk	12
6.1	DataCenter ACI-netwerk	13
6.1.1	Data Center switches	13
6.2	Datacenter ILO-netwerk	13
7	Internet module	14
7.1	Internet edge	14
7.2	Public DMZ	14
7.3	Private DMZ ten behoeve van virtuele netwerken	14
8	VRI en OOV-CAMERA netwerk	15
8.1	VRI-netwerk	15
8.2	OOV-Camera netwerk	16
9	Cisco Enterprise Agreement	16
10	Onderhoudsvormen huidig contract	17
11	Huidige netwerk monitoring tooling	17
12	Aanpalende netwerk of security gerelateerde componenten	17

1 Inleiding

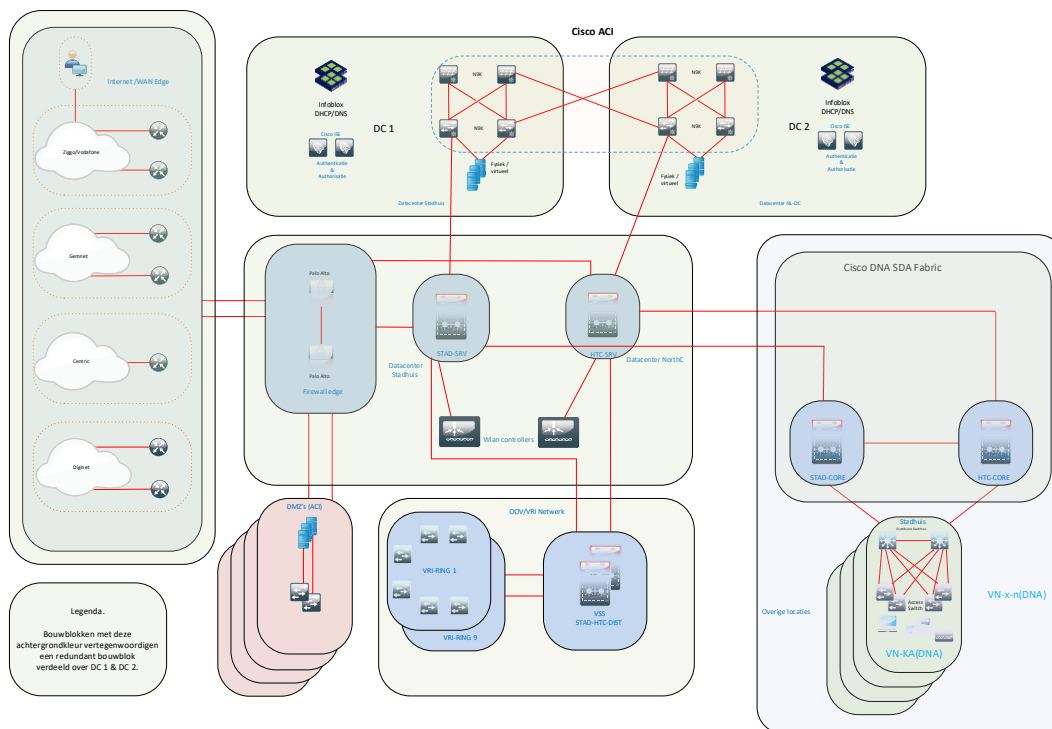
Deze bijlage heeft als doel de inschrijver een zo goed en compleet mogelijk beeld van de huidige situatie te geven en hiermee bij te dragen aan de meest optimale aanbesteding.

Een groot deel van de huidige installed-base van actieve netwerkcomponenten bij Gemeente Eindhoven is van het fabricaat Cisco. Dit omvat alle switches (access-, core- en datacenter) en de wireless voorziening. Een klein deel hiervan is verouderd. Zie hiervoor bijlage 1A (CMDB) welke netwerkcomponenten in deze aanbesteding als vervangingsvraag worden meegenomen. De huidige (next-gen) firewalls zijn van het fabricaat Palo Alto. De Onderhoudsvormen huidig contract zijn weergegeven in hoofdstuk 10.

Het huidige netwerkontwerp van de gemeente Eindhoven is de afgelopen jaren geëvolueerd. Dit wil zeggen dat het netwerkontwerp de laatste jaren is uitgebreid, verbeterd en geoptimaliseerd. Dit voldoet aan de netwerkbehoefte.

In onderstaande figuur zijn de verschillende netwerk modules van het netwerk van de Gemeente Eindhoven weergegeven.

In onderstaand figuur is ook te zien dat het netwerk twee datacenters heeft. In het document wordt met DC1 verwezen naar het datacenter stadhuis. Voor DC2 wordt verwezen naar het datacenter HTC (High Tech Campus).



Figuur 1: Overzicht Netwerk modules

De relevante onderdelen voor deze aanbesteding zijn:

- MAN module
- Service module
- Access Management
- Campus DNA-netwerk
- Data Center netwerk
- Internet module
- Camera OOV en VRI-netwerk

In de volgende (sub)paragrafen zullen de netwerkmodules van de Gemeente Eindhoven in detail worden uitgewerkt, gevolgd door informatie over de Cisco Enterprise Agreement

Medio februari 2024 verloopt de huidige Cisco Enterprise Agreement (CISCO ONE ELA) van de gemeente af. Inmiddels is door Cisco een opvolger van deze Enterprise Agreement beschikbaar, te weten de Enterprise Agreement 3.0. De leverancier moet in staat zijn om de gemeente te adviseren naar de best mogelijke inrichting van de Cisco Enterprise Agreement 3.0 tegen de best mogelijk TCO en wat de gevolgen hiervan zijn ten opzichte van de huidige losse licenties op netwerkcomponenten.

2 Onderhoudsvormen huidig contract

Onderhoud dient uitgevoerd te worden conform goed vakmanschap waarbij het totale netwerk met zijn onderlinge samenhang als LAN/WAN & Datacenternetwerk wordt beschouwd en als zodanig onder dit onderhoudsbestek valt.

3 Huidige netwerk monitoring tooling

In de huidige omgeving wordt door de netwerkbeheerders van de Gemeente Eindhoven voor monitoring van de netwerkomgeving gebruik gemaakt van de volgende tools:

- Cisco DNA Assurance;
- Cisco ACI Dashboard;
- KIWI Cattools;
- KIWI Syslog;
- Cacti (<https://www.cacti.net/>).

Aanpalende netwerk of security gerelateerde componenten in hoofdstuk 9.

4 MAN module

De MAN (metro area netwerk) module bestaat uit glasvezels van het BRE-netwerk en de Infinera Multiplexers. Dit netwerk verbindt de diverse gemeente locaties en de datacenters.

4.1 BRE Glasvezelnetwerk

De gemeente Eindhoven heeft in het verleden met een aantal andere gemeentes BRE (Breedband regio Eindhoven) opgezet om een hoogwaardig netwerk op basis van onder andere darkfiber glasvezelnetwerken te kunnen realiseren. Gemeente Eindhoven is voor een groot gedeelte aandeelhouder.

De verbindingen tussen de kantoren en de datacenters maken in alle gevallen gebruik van dit BRE-glasvezel netwerk. Daarnaast wordt voor het VRI en OOV-camera netwerk eveneens gebruik gemaakt van het BRE-netwerk.

4.2 Infinera multiplexers

In een aantal gevallen zijn Multiplexers kosten efficiënter dan alleen glasvezel. De gemeente Eindhoven heeft daarom 6 Infinera multiplexers van het type tm-301. Deze multiplexers zijn voorzien van een module TPMRH-L-16/G met 6 X 10 gbit/sec en een module GbE-MXP-10G-FEC met 9 X 1 gbit/sec. De multiplexer ondersteunt geen 40 gbit/sec verbindingen.

De multiplexers zijn ingezet in de datacenters om verbindingen tussen deze twee datacenters DC1 en DC2 te kunnen realiseren. Daarnaast is er een multiplexer ingezet op de locatie Mercado. In het verleden is dit een oud datacenter geweest met diverse verbindingen naar de gemeentelijke locaties. Na het opheffen van het oude datacenter Mercado zijn deze gemeentelijke locaties via een multiplexer verbonden met het datacenter DC2.

5 Service module

De service module van het netwerk binnen de Gemeente Eindhoven wordt gevormd door twee Cisco 9500 switches. Vanuit de core wordt het netwerkverkeer naar de verschillende onderdelen gerouteerd c.q. ontsloten, zoals, het DNA SDA Campus netwerk en de WLC's, het VRI/OOV-netwerk, het Cisco ACI Data Center netwerk, het ILO-netwerk en de Internet Edge.

5.1 Service core

De service core-laag van het netwerk van Gemeente Eindhoven is opgebouwd rondom 2 switches op basis van de Cisco Catalyst 9500-24Q met 24 ethernet poorten van 40 gbit/sec en voorzien van redundante voeding. Deze switches zijn verdeeld over de twee datacenters DC1 en DC2.

De service core-laag heeft als primaire taak routeren op basis van laag 3 en heeft daarom koppelingen middels gerouteerde verbindingen met de aangesloten switches. Voor de routing wordt gebruik gemaakt van het OSPF-protocol. Voor de koppeling met de Cisco DNA SDA cores wordt gebruik gemaakt van BGP.

Om het verkeer veilig te kunnen scheiden wordt gebruik gemaakt van een aantal virtuele netwerken (VRF's). Het verkeer tussen de virtuele netwerken wordt door de service core gerouteerd naar de Palo Alto firewalls. Op de Palo Alto firewalls zijn de security policies gedefinieerd ten behoeve van de beveiliging tussen de virtuele netwerken.

6 Access Management

Voor toegangscontrole binnen de access-laag (wireless en wired) en toegang tot het management van de netwerkapparatuur, wordt gebruik gemaakt van een 4-node Cisco ISE cluster, bestaande uit allemaal fysieke nodes. Hierbij wordt gebruik gemaakt van radius en 802.1x.

6.1 Cisco ISE

Voor de toegangscontrole van de devices op het netwerk wordt gebruik gemaakt van de Cisco ISE oplossing. De Cisco ISE is een radius oplossing en wordt voor de authenticatie van netwerk devices op zowel het Lan als op wireless netwerk toegepast.

De Cisco ISE oplossing bestaat uit een cluster van 4 ISE servers met de rollen admin, monitoring en policy server nodes. Voor de authenticatie van de netwerk devices wordt gebruik gemaakt van een interne CA om de authenticatie op basis van certificaten te kunnen uitvoeren. De Cisco ISE servers zijn daarnaast gekoppeld met het Windows AD ten behoeve van authenticatie en autorisatie van de netwerk devices. Verder zijn de Cisco ISE servers gekoppeld met de Cisco DNA-controllers op basis van pxgrid. Het toewijzen van een netwerk aan een netwerk client vindt plaats middels een IP-pool en SGT (scalable group tag).

6.2 Access control LAN

De Cisco ISE radius oplossing wordt toegepast op het LAN-netwerk op basis van EAP en mac authenticatie. Gemeentelijke notebooks en tablets authenticeren op basis van het netwerkprotocol EAP-TLS met de switch alvorens toegang wordt verleend tot het KA netwerk. Voor andere netwerken wordt afhankelijk van het vereiste beveiligingsniveau gebruik gemaakt van EAP of mac authenticatie. De gemeente Eindhoven heeft wel het voornemens om in de toekomst vanwege de hogere eisen vanuit de BIO meer netwerk clients te ontsluiten middels EAP-TLS, bijvoorbeeld de camera's.

6.3 Access control WLAN

Voor de wireless LAN-omgeving wordt altijd gebruik gemaakt van het EAP-protocol. Gemeentelijke notebooks en tablets authenticeren net als bij de LAN-oplossing op basis van EAP-TLS met de Cisco WLAN controllers. Andere devices zoals bijvoorbeeld Apple IPADs tablets gebruikt voor gemeentelijke toepassingen zijn altijd ontsloten middels EAP.

6.4 Access control netwerkapparatuur

Voor access control van de netwerkapparatuur is radius ingeregeld via Cisco ISE. In Cisco ISE is een policy aangemaakt dat alleen netwerkbeheerders die lid zijn van een specifieke Windows AD groep in kunnen loggen op de netwerkapparatuur.

7 DNA Campus netwerk

Het Cisco DNA netwerk is een software defined access netwerk (SD-A) en verbindt de 23 vestigingen met de service cores. De configuratie van het SDA-netwerk vindt plaats middels de DNA-controllers. Het DNA SDA netwerk bestaat verder uit een core, distributie- en een access-laag. Voor de underlay wordt gebruik gemaakt van de het OSPF routerings protocol en is handmatig voor alle netwerk devices geconfigureerd. De verschillende onderdelen worden in de onderstaande (sub) paragrafen verder beschreven.

7.1 DNA-controllers

Het Cisco DNA netwerk wordt aangestuurd/geconfigureerd vanuit de Cisco DNA-controllers. Het Cisco DNA cluster bestaat uit drie nodes van het type DN1-HW-APL. De DNA-controllers zijn aangesloten op de service cores. Twee Cisco DNA-controllers zijn aangesloten in DC1 en de andere node in DC2. Beheer van de Cisco switches vindt plaats via de DNA-controllers waaronder de upgrades van de switches. Verder is via de DNA-controllers de overlay geconfigureerd waaronder de verschillende virtuele netwerken alsmede de scalable group tags. De configuratie voor de underlay van de switches vindt niet plaats via de DNA-controllers. De underlay wordt nog handmatig op de switches geconfigureerd. Verder zijn vanuit de DNA-controllers de security policy voor de SGT's geconfigureerd alsmede de quality of service (QoS).

7.2 DNA Core-laag

De DNA core laag verbindt de locaties met de service-cores. De Cisco DNA cores zijn in de SDA-fabric zowel als border nodes als control nodes geconfigureerd.

De DNA core-laag van het netwerk van Gemeente Eindhoven is opgebouwd rondom 2 switches op basis van de Cisco Catalyst 9500-24Q met 24 ethernet poorten van 40 gbit/sec en voorzien van redundante voeding. Deze switches zijn verdeeld over twee datacenters.

De DNA core-laag is verbonden met de service cores op basis van 2 ethernet poorten van 40 gbit/sec. De routing tussen de Cisco DNA cores en de Cisco-service cores is voor de underlay met OSPF en voor de overlay met BGP geconfigureerd. Bij uitval van een core switch is er een convergentie van 30 seconden.

7.2 DNA Distributie-laag

De Gemeente Eindhoven heeft 23 vestigingen. De distributie-laag in het netwerk is direct gekoppeld aan de beide Cisco DNA core switches in DC1 en DC2 op basis van ethernet met een snelheid van 10 gbit/sec. Bij uitval van een distributie switch is er een convergentie van 2 seconden. De distributie switches zijn in de SDA-fabric als intermediate node of edge node geconfigureerd. De distributie-laag kent qua opzet de volgende 3 distributiemodellen, afhankelijk van de grootte van de locatie en haar toepassingen zijn deze gebaseerd op verschillende platformen:

- **Distributiemodel A** voor grotere locaties op basis van de Cisco 6880-X

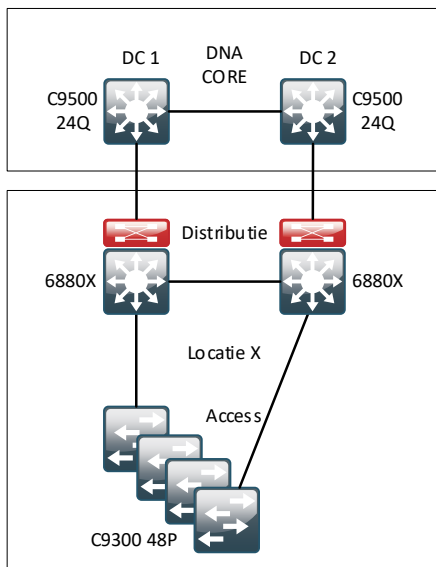
- **Distributiemodel B** voor de wat kleinere tot middelgrote locaties op basis van de Cisco C9300-48P.
- **Distributiemodel C** voor de klein(st)e locaties op basis van de Cisco C9300-48P vanuit DC1 en DC2, waarbij op de locaties alleen gebruik wordt gemaakt van een extended node C3560CX-8PC

Deze 3 distributiemodellen worden in de volgende (sub) paragrafen verder toegelicht, ondersteund door de bijbehorende afbeeldingen.

Enkele distributieswitches zijn aan vervanging toe. De Gemeente Eindhoven heeft de intentie m vervanging van enkele distributieswitches vanaf 2024 door te voeren. Zie hiervoor ook het overzicht van de huidige installed base, zie hoofdstuk 10 Lifecycle Status.

7.2.1 Distributiemodel A

Distributiemodel A wordt gebruikt voor de grotere locaties. Dit distributie model kent op elke locatie een set van distributieswitches op basis van het Cisco Catalyst 6880X platform en zijn redundant aangesloten op de DNA COREs. Deze switches zijn binnen de SDA-Fabric als intermediate node geconfigureerd en voorzien in layer 3 connectivity naar de dna cores- en access-switches binnen de locatie.



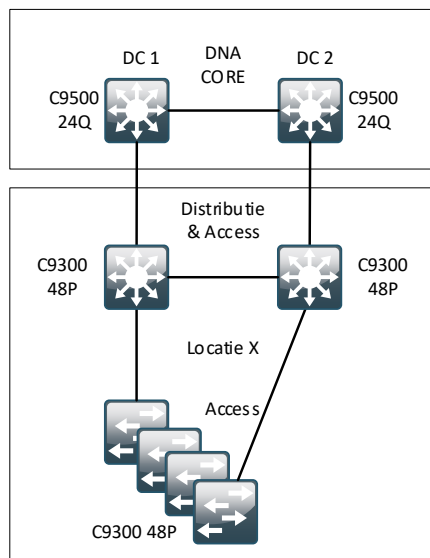
Figuur 2: Configuratie Distributiemodel A

Het **distributiemodel A** is ingericht voor de grotere locaties, te weten:

1. Stadhuis
2. Mercado
3. NRE
4. Tongelreep

7.2.2 Distributiemodel B

Het **distributiemodel B** is ingericht voor de kleinere tot middelgrote locaties. Dit distributie model kent op locatie een set van distributieswitches op basis van het Cisco Catalyst 9300 platform. De Cisco 9300 switches zijn in SDA-fabric geconfigureerd als edge-node zodat er ook extended nodes en netwerk clients kunnen worden aangesloten. Voor grotere locaties zijn slechts een beperkt aantal verbindingen van de distributie switches naar de netwerk clients gemaakt om de bekabeling naar de access switches overzichtelijk en netjes te houden. Op een aantal kleinere locaties is gekozen om de distributie switches ook de rol te geven van een access switch om de kosten te kunnen verlagen. Op de switches van de kleinere locaties zijn dan ook aanzienlijk meer netwerk clients aangesloten.



Figuur 3: Configuratie Distributiemodel B

De volgende locaties hebben twee distributie switches en elke distributie switch heeft een verbinding met DNA CORE in DC1 en DC2

1. Van Abbemuseum
2. Sportpark Eindhoven-Noord en Ottenbad

De volgende locaties hebben slechts een distributie switch waarop in een aantal geval een extended node is aangesloten. Deze distributie switch wordt ook gebruikt als access switch. Daarnaast zijn niet alle switches redundant aangesloten op de DNA-CORES. Per locatie is aangegeven of deze wel of niet redundant zijn aangesloten aan de DNA-Cores

De locaties met een redundante verbinding naar DNA COREs in DC1 en DC2:

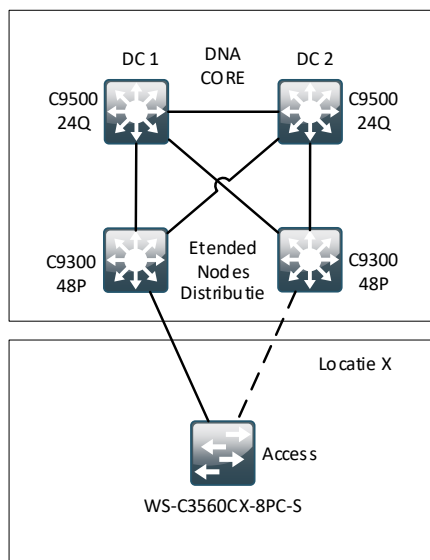
1. Biocentrale
2. Sportbedrijf De Karpen

De locaties met een enkelvoudige verbinding naar een van de DNA-Cores zijn als volgt:

1. Fietsendepot
2. Designhuis
3. Septemberplein
4. Expat Center
5. Werf Rooij akkerstraat

7.2.3 Distributiemodel C

Het **distributiemodel C** is ingericht voor kleine locaties met alleen een extended node switch van het type C3560CX-8PC. Voor dit distributie model geldt dat er op de locatie geen distributieswitch operationeel is; de distributieswitches voor deze locaties bevinden zich in DC1 en DC2, zoals onderstaande afbeelding laat zien. Deze distributieswitches zijn gebaseerd op het Cisco Catalyst 9300-x platform en zijn geconfigureerd als edge-node.



Figuur 4: Configuratie Distributiemodel C

De volgende locaties hebben een extended node switch die verbonden is met de Cisco Catalyst 9300-x switches in de datacenters DC1 en DC2:

1. Fietsenstalling de Heuvel
2. RHC (Regionaal Historisch Centrum)

7.3 Access-laag LAN

De access-laag van de Gemeente Eindhoven bestaat hoofdzakelijk uit het Cisco 9300 switches, maar er zijn ook een aantal extended nodes van het type switch C3560CX-PC-S.

De Cisco 9300 switches hebben een stack-wise configuratie en hebben een redundante uplink van 10 gbit/sec met de distributie switches. De Cisco 9300 hebben in de meeste gevallen een enkele voeding maar zijn onderling wel verbonden met power cables zodat de power over de volledig stack kan worden verdeeld. In de SDA-fabric zijn de switches ingesteld als edge nodes en voorzien in de connectiviteit voor PC's, thin-clients, IP-telefoons, access-points, printers, etc.

De extended nodes zijn enkelvoudig aangesloten met 1 gbit/sec op de Cisco 9300 distributie of accces switches. De extended nodes hebben geen ondersteuning voor SGTs. De gemeente Eindhoven heeft daarom het voornemens deze switches te vervangen door Cisco 9200 switches met volledig SDA-functionaliteit waaronder SGTs.

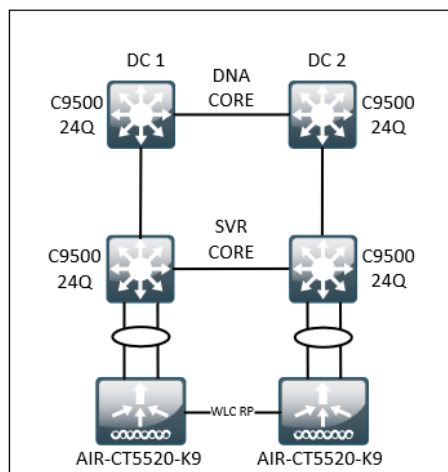
7.4 Wireless network

Het wireless netwerk bestaat uit de twee wireless controllers en bijna 500 access-points. In onderstaande paragrafen zijn deze verder gespecificeerd.

7.4.1 WLC wireless controllers

De huidige draadloze netwerkvoorziening is onderdeel van de Cisco SDA Fabric. Deze voorziening is opgebouwd rondom 2 Cisco WLC controllers van het type 5520. De WLC's zijn operationeel in DC1 en in DC2. De WLC's vormen samen een 'HA pair', waarvan er 1 WLC in elke DC is ondergebracht. Elke WLC-controller is middels een portchannel van 2x10 gbit/sec aangesloten op elk van de service core switches. Voor de communicatie tussen de WLC's ten behoeve van de high availability wordt gebruik gemaakt van de WLC redundancy ethernetpoorten van 1 gbit/sec. De WLC redundancy ethernet poorten zijn aangesloten op de Cisco-service cores.

Onderstaand schema toont de huidige opzet van de Cisco WLC controllers.



Figuur 5: Configuratie WLC Wireless Controller

7.4.2 Wireless Access Points

In totaal zijn er 447 van 488 access-points van het type AIR-AP2802I-E in gebruik.
Daarnaast zijn er nog 7 van de 8 access-points van het type AIR-AP2802E-E in gebruik.

De nieuwe types access-points ondersteunen altijd beide banden (2,4 en 5 GHz). De authenticatie van de access-points op het netwerk is op basis van het 802.1x protocol. De access-points zijn onderdeel van de Cisco DNA SDA fabric.

8 Data Center netwerk

Binnen de Gemeente Eindhoven zijn 2 primaire datacenter locaties actief, namelijk het DC1 (Stadhuis) en DC2 HTC (High Tech Campus). DC1 betreft datacenter in onder het Stadhuis. De serverracks van DC2 bevinden zich in het datacenter van NorthC datacenters op de High Tech Campus te Eindhoven.

Over de beide datacenters, is met de implementatie van de server en storage infrastructuur ook een moderne netwerk infrastructuur gebouwd op basis van de Cisco ACI datacenter technologie. Hierdoor is een stretched-fabric actief welke beschikbaar is op beide datacenter locaties.

Daarnaast is voor het beheer van de servers een apart ILO-netwerk in het datacenter aangelegd.

In de volgende (sub)paragrafen wordt het ACI-data center en ILO-netwerk besproken.

8.1 DataCenter ACI-netwerk

Het Cisco ACI datacenter netwerk wordt gebruikt om alle productieservers en storage componenten aan te sluiten. Het betreft een dual-data center concept waarbij in principe alle productieservers en storage componenten primair draaien op het HTC DC en alle OTA (en Disaster Recovery) componenten op het Stadhuis DC.

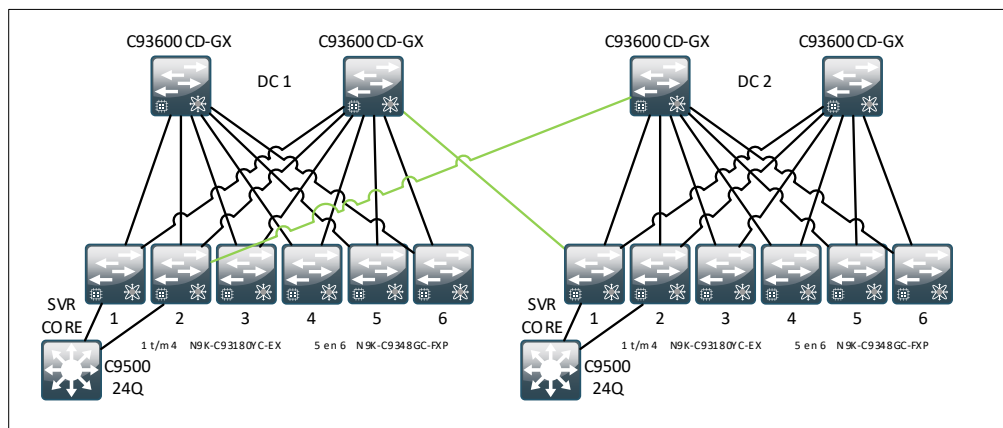
De productieservers bestaan voornamelijk uit Nutanix servers die dienen te worden vervangen in 2023. De huidige infrastructuur wordt door een nog nader te bepalen IAAS-oplossing op termijn vervangen.

8.1.1 Data Center switches

De Cisco ACI infrastructuur is opgebouwd uit de volgende componenten:

- 2x Cisco Nexus C93600CD-GX platform (als SPINE) binnen elke datacenter locatie
- 4x Cisco Nexus C93180YC-EX switches (als LEAF) binnen elke datacenter locatie
- 2x Cisco Nexus C9348GC-FXP switches (als LEAF) binnen elke datacenter locatie
- 3x APIC Controllers van het type APIC-SERVER-M3

De ACI-data center switches zijn verbonden met de Cisco-service cores op basis van OSFP gerouteerde verbindingen van 4 X 40 gbit/sec. De verbindingen in de Cisco ACI fabric tussen de spine en leaf switches zijn eveneens op basis van 40 gbit/sec. De verbindingen tussen de twee verschillende pods zijn aangesloten met 2X40 gbit/sec via darkfiber (groene lijn). De aangesloten apparatuur op de Cisco ACI switches zijn in de meeste gevallen redundant gekoppeld op basis van 1 of 10 gbit/sec.



Figuur 6: Configuratie 'nieuwe' DC spine en leaf switches

8.2 Datacenter ILO-netwerk

Het ILO-netwerk bestaat uit een virtuele switch (VSS) bestaand uit twee switches van het type C4500X-16. De VSS-switches staan op de datacenters DC1/DC2 en zijn op basis van gerouteerde verbindingen van 10 gbit/sec verbonden met de service core. Aan de VSS-switches zijn vervolgens 7 verouderde switches van het type Cisco C3560X-48P op basis van 1 gbit/sec aangesloten. Deze switches zijn verbonden met de verschillende ILO/management interfaces van de servers, waaronder de Nutanix servers.

9 Internet module

De internet module bestaat uit een firewall oplossing van het merk Palo Alto. Daarnaast bestaat deze module uit een public en private DMZ. De firewalls zijn aangesloten op de Cisco-service cores.

9.1 Internet edge

De firewall omgeving bestaat uit een redundante Palo Alto PA-5250 firewall oplossing. De firewalls zijn met redundante verbindingen gekoppeld aan het Internet. De maximale bandbreedte naar de serviceprovider is op dit moment 1 Gbit/sec. Op de firewalls vindt filtering plaats en wordt NAT toegepast om verbinding met het Internet op veilige manier mogelijk te maken.

Qua (hardware)onderhoud valt de Palo Alto firewall oplossing buiten de scope van deze aanvraag.

9.2 Public DMZ

De Public DMZ omgeving is vanaf Palo Alto aangesloten op de Cisco ACI omgeving op basis van 10 gbit/sec. De verschillende DMZ-zones zijn op basis van laag 2 verbonden met de Cisco ACI omgeving. De public DMZ-omgeving bestaat uit een aantal DMZ's waaronder bijvoorbeeld de DMZ webservers.

9.3 Private DMZ ten behoeve van virtuele netwerken

De Private DMZ omgeving is vanaf de Palo Alto aangesloten op de service cores op basis van 40 gbit/sec. Via deze verbinding vindt de routing en filtering plaats tussen de verschillende virtuele netwerken waaronder het KA, VOICE, Camera, gasten en externe partijen.

10 VRI en OOV-CAMERA netwerk

Binnen het netwerk is een 'gescheiden' netwerkdeel actief. Het gescheiden netwerk deel is een 'traditioneel' netwerk waarop alle VRI-apparatuur en alle OOV-camera's zijn aangesloten. De VRI-apparatuur bestaat uit verkeersregelininstallaties (kortweg VRI's) en VRI-camera's om het wegverkeer te kunnen monitoren. De OOV-camera's worden gebruikt voor toezicht van de openbare gelegenheden.

10.1 VRI-netwerk

Het VRI-netwerk bestaat uit een virtueel chassis van 2 switches (VSS) op basis van het Cisco Catalyst 6509 platform. De switches staan in de datacenters DC1 en DC2.

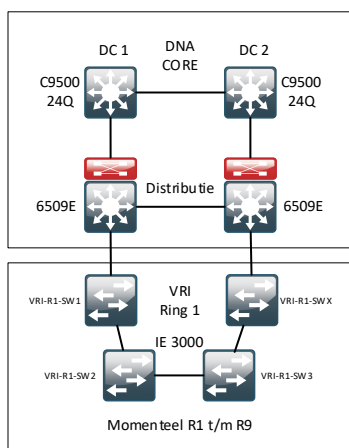
De VSS-switches zijn verbonden met de service core op basis van L3 portchannels van 2X2 gbit/sec. De primaire taak van deze switches is het routeren van het laag 3 verkeer met de service core. Binnen deze routing zijn VRF's gedefinieerd om de verschillende routerings domeinen te kunnen scheiden. Daarnaast zijn de VSS-switches op basis van laag 2 met 1 gbit/sec verbonden met de vri en oov switches.

De VSS-switches hebben de onderstaande specificaties:

- Voeding: dubbel uitgevoerd per chassis
- Supervisor modules: enkel uitgevoerd in elke chassis (SUP-2T)
- 48 poorts SFP 1G module

De infrastructuur ten behoeve van de VRI's is opgebouwd rondom het Cisco Catalyst 3000 Industrial Ethernet platform. Het betreft circa 168 switches verdeelt over 9 glas ringen. Deze glasringen zijn gekoppeld op de distributie-laag in DC1 en DC2. Redundantie binnen deze ringen is gerealiseerd op basis van het Resilient Ethernet Protocol (REP), wat een alternatief vormt voor het spanning tree protocol.

Momenteel valt het beheer en onderhoud voor een grootdeel onder de hoede van een derde partij. De Cisco 6500 VSS switches zijn technisch in beheer bij de Gemeente Eindhoven. De Cisco Catalyst 3000 switches zijn onder beheer bij deze externe partij. Echter technisch bekeken heeft de Gemeente Eindhoven hierin een regierol. Dit netwerkdeel dient naadloos aan te sluiten bij de rest van het netwerk.



Figuur 7: Configuratie VRI switches

Noot:

Qua (hardware)onderhoud vallen deze Cisco Catalyst 3000 IE switches buiten de scope van deze aanvraag!

10.2 OOV-Camera netwerk

Het OOV-Camera netwerk is de afgelopen jaren aanzienlijk gegroeid. Het OOV-netwerk maakt net als het VRI-netwerk gebruik van de Cisco 6500 VSS.

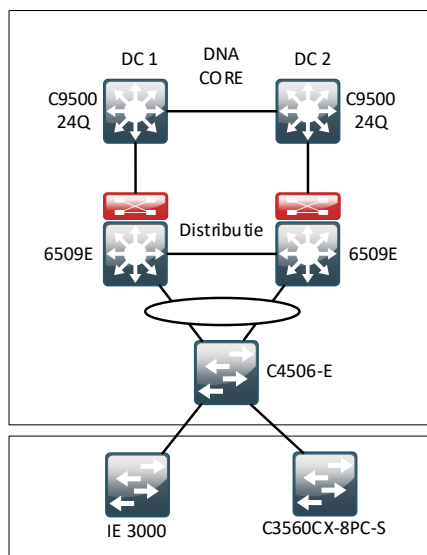
Op de Cisco 6500 VSS switch is een Cisco C9300-48S-A switch aangesloten op basis van een port-channel met 2X1 Gbit/sec. Op deze Cisco 9300 switch zijn de meeste OOV-camera's aangesloten.

Op de Cisco 9300 switch zijn verder vier Cisco IE-3000-4TC switches en een Cisco C3560CX-8PC-S switch op basis van 1 gbit/sec aangesloten. De Cisco IE-3000-4TC switches staan op diverse locaties in de stad waarop de oov-camera's zijn aangesloten.

Daarnaast zijn er een aantal OOV-camera's rechtstreeks met 1 gbit/sec aangesloten op de Cisco 6500 VSS switch.

Verder is er nog een externe leverancier die wifi Radware apparatuur heeft geleverd en in beheer heeft om OOV-camera's via wifi te kunnen ontsluiten.

Tenslotte is er nog externe leverancier aangesloten voor het ontsluiten van camera's ten behoeve van evenementen. Deze leverancier heeft een aantal verbindingen van 1 gbit/sec naar de Cisco 9300 switch.



Figuur 8: Configuratie OOV-CAM switches

11 Cisco Enterprise Agreement

Medio februari 2024 verloopt de huidige Cisco Enterprise Agreement (CISCO ONE ELA) van de gemeente af. Inmiddels is door Cisco een opvolger van deze Enterprise Agreement beschikbaar, te weten de Enterprise Agreement 3.0.

De leverancier moet in staat zijn om de gemeente te adviseren naar de best mogelijke inrichting van de Cisco Enterprise Agreement 3.0 tegen de best mogelijk TCO en wat de gevolgen hiervan zijn ten opzichte van de huidige losse licenties op netwerkcomponenten.

12 Onderhoudsvormen huidig contract

Onderhoud dient uitgevoerd te worden conform goed vakmanschap waarbij het totale netwerk met zijn onderlinge samenhang als LAN/WAN & Datacenternetwerk wordt beschouwd en als zodanig onder dit onderhoudsbestek valt.

13 Huidige netwerk monitoring tooling

In de huidige omgeving wordt door de netwerkbeheerders van de Gemeente Eindhoven voor monitoring van de netwerkomgeving gebruik gemaakt van de volgende tools:

- Cisco DNA Assurance;
- Cisco ACI Dashboard;
- KIWI Cattools;
- KIWI Syslog;
- Cacti (<https://www.cacti.net/>).

14 Aanpalende netwerk of security gerelateerde componenten

In de onderstaande tabel geeft de Gemeente Eindhoven een overzicht van aanpalende netwerk of security gerelateerde componenten, die **niet in scope** van deze aanbesteding vallen.

ID	Component	Functie
1.	Beyondtrust	Secure remote access
2.	F5 BIG-IP	Reverse proxy en load balancer => servers
3.	Infoblox	DNS en DHCP
4.	Palo Alto	Firewall

•