Landssjúkrahúsið

The National Hospital of the Faroe Islands

Network High-Level Design Document

16 November 2021
Version 1.5

Table of Contents

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Figures

Tables

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

1 Version control

Revision number	Revision date	Description of changes in version	Responsible
1.0	22-02-2021	Document startup	cka@conscia.com
1.1	12-03-2021	Document review	miche@conscia.com
1.2	17-03-2021	Document update based on RN 1.1	cka@conscia.com
1.3	07-04-2021	Review	frl@conscia.com
1.4	21-04-2021	Document update based on RN 1.3	cka@conscia.com
1.5	03-05-2021	Review by Conscia Marketing	

2 Abbreviations

Abbreviation	Description
BGP	Border Gateway Protocol
DNAC	Digital Network Architecture Center
DCNM	Data Center Network Manager
ECMP	Equal Cost Multi Path
EVPN	Ethernet VPN
IRB	Integrated Routing and Bridging
MP-BGP	Multi Protocol BGP
OSPF	Open Shortest Path First
STP	Spanning-Tree Protocol
VLAN	Virtual Local Area Network
VNI	Virtual Network Instanse
VRF	Virtual Routing Forwarding
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual Extensible LAN
WLC	Wireless Controller

3 Table of Appendix

Appendix	Name
A	IP Plan | Excel spreadsheet

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

4 About this document

This document has been created by Conscia, Claus Andersen and holds information about the new network design and implementation for Landssjúkrahúsið, Thorshavn, Faroe Islands.

4.1 Document Authors

Name	Role	Company
Claus Andersen	Author - Network Architecture	Conscia
Jesper Voss	Author - Network Architecture	Conscia
Finn Rud	Author - Network Architecture	Conscia

4.2 Document Purpose

The recommendations in this document are based on input from Landssjúkrahúsið engineers, Conscia engineers, Cisco and industry-wide best practices. The intent of this document is to document the High-Level design for Landssjúkrahúsið Torshavn's site.

The design document contains a high-level description of the chosen design, along with hardware choices and physical layout necessary to successfully implement the design. The document will serve as a baseline for creating a Low-Level Design document and the bill of material.

4.3 Intended Audience

This document is intended for use by Landssjúkrahúsið network operations and management teams. Furthermore, the document can be used by the project steering committee to agree on the Network refresh, project design and scope.

4.4 Document and Project Scope

The scope of this document includes new LAN Core, distribution, server block, WAN block, access switches, wireless LAN controllers and access-points. Furthermore, it also covers firewalls introduced by the project.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

5 Solution Context

5.1 Network Requirement

The main goal is to create a stable and scalable medical grate network to serve the Landssjúkrahúsið for several years into the future. The network will address several things like:

- Industry standard based
- Medical grade network
- High availability
- High level of security
- Converged network infrastructure

5.1.1 Operational Challenges

The day-to-day maintenance of the network must be easy, effective and in some terms as self-healing as possible. Tasks need to be automated where possible.

5.2 High-Level Scope

The scope of this high-level design document includes:

- Physical units overview
- Design principals
- Naming standard
- Logical design
- Building blocks
- Management and monitoring

6 Logical Design

6.1 Architecture Overview

The architecture is built using a concept of PINs (Place in the Network), where each PIN constitutes a network building block, which can be easily built, operated, or scaled without affecting other PINs in the network. The defined PINs are:

- Core, which forms the backbone of the network
- Distribution, which aggregates access layer towards the core
- Access, for end-user endpoints
- Server, for servers and appliances
- WAN, for terminating external connections

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

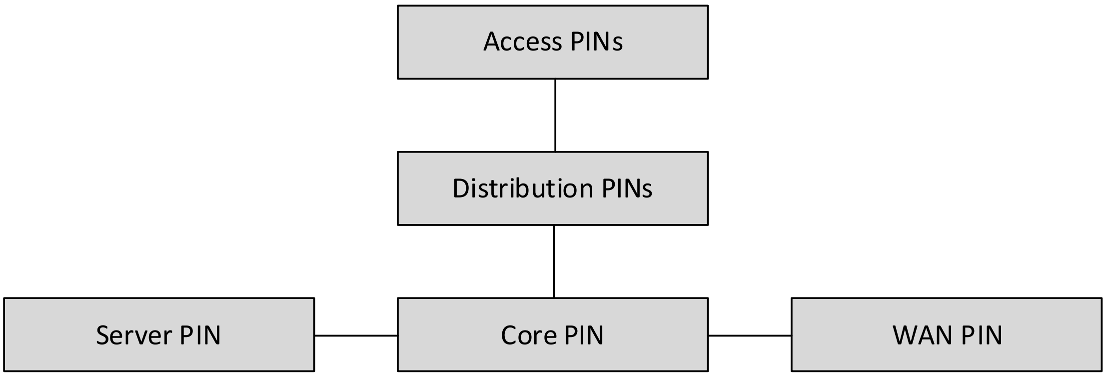

Figure 1 - Logical PIN Overview

Some PINs will exist only in a single instance, while others exist in multiple instances. In this architecture, there will only be a single Core PIN, WAN PIN and Server PIN, while there will be multiple Distribution and Access PINs

The network architecture is:

- Simple, because it is built on simple network protocols used on well-defined PINs, and with few management points
- Resilient, because it offers redundant connections, equipment, and power supplies, and because there are no Layer 2 loops and no dependency on STP (Spanning Tree Protocol)
- Fast, because it offers Gigabit Ethernet to all access endpoints, and 10-25-100 Gigabit Ethernet on all connections between all network, and because core switching components can run full, non-blocking performance on all ports at the same time
- Secure, because it offers multiple security zones on an isolated network and via the control it is offering administrators and operators of the network.

6.1.1 CORE

The core PIN serves as a backbone for the complete network, providing non-blocking packet-switching between multiple other PINs.
This layer serves as the connection point between the distribution PINs, WAN PIN and Server PIN, which implement all end-point connectivity and services. The core PIN only provides connectivity to network devices, not end-points, and does not in itself implement services. Full redundancy is needed since all other PINs depend on the core PIN.
All links connecting to the core PIN are terminated at layer 3 (routing) for added stability and large scalability.
The core will not be VRF aware and only perform routing for forwarding.
All connections to the core switches must be using 100GigabitEthernet.

6.1.2 DISTRIBTION

The distribution PIN serves to aggregate connections from the access layer towards the core PIN, thereby minimizing the number of ports needed in the core.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

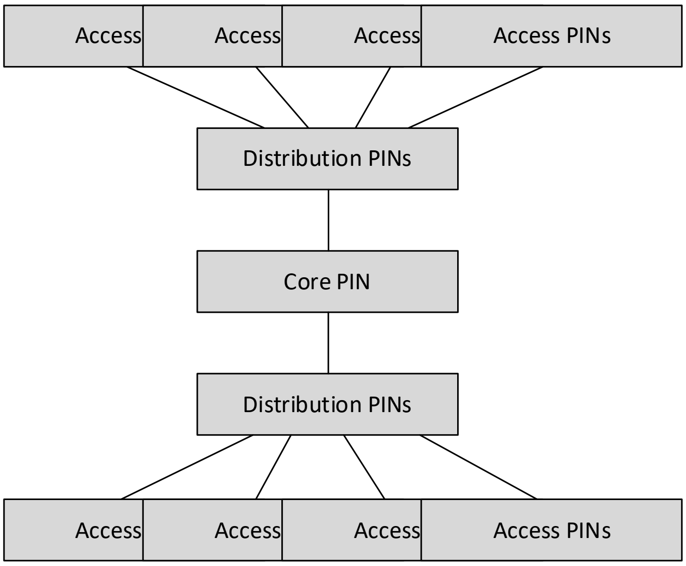

Figure 2 - Distribution PINs

The distribution switches must be interconnected and uplinked using 100GigabitEthernet. There will be no endpoint clients connected to any distribution PINs.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

6.1.3 ACCESS

The access PIN is where the endpoints connect to the network. The access switches typically map traffic from physical ports to a specific VLAN, which is then routed across the distribution and core layer towards servers or other endpoints.

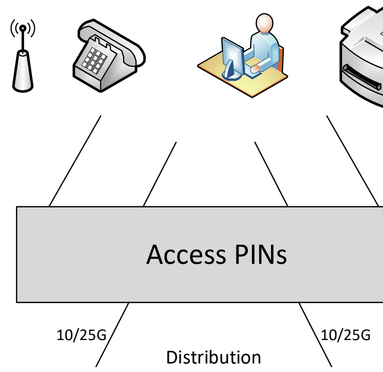

Figure 3 - Access PINs

The access PIN exists in multiple, and potentially many, instances. At least one switch is placed in each wiring closet where wired access is required, or wireless access points need to interface into the wired network, providing physical network access for ports terminated at that wiring closet. The access switches connect directly to the distribution switches for connections to the rest of the network.

The 10/25Gbps uplinks will be running as Layer 3 routed links using ECMP

6.1.4 WAN

The WAN PIN serves to connect all networks external to Landssjúkrahúsið corporate LAN. This includes networks behind external MPLS, External VPN connections and Firewalls connecting the Internet. Furthermore, any traffic between multiples virtual networks (VRFs) in Landssjúkrahúsið will need to transit the FirePower Firewall also terminated in the WAN PIN.
The Wireless controller will also be terminated in the WAN PIN and wireless clients will be routed from this point.

Figure 4 - WAN PIN

6.1.5 DATACENTER

The server PIN will serve to connect all servers and on-prem services in the datacenter in Torshavn. It will aggregate these services towards the core.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Figure 5 - Server PIN

7 Physical Design

7.1 Hardware Platforms

This section describes the different hardware platforms used in the design.

7.1.1 Core PIN

Landssjúkrahúsið will use the C9500-32C model in the LAN Core, as it can deliver 100GigabitEthernet between the core switches, datacenter and distribution blocks in non-blocking.


Figure 6 - C9500-32C

The C9500-32QC has 32x fixed 100Gbps Interfaces QSFP interfaces. The 32 ports are handled by 32x 100Gbps ASICs. This allows the switch to operate as a 32x 100Gbps switches also. Any combination of 100Gbps and 40Gbps interfaces can be used. Landssjúkrahúsið will use 12 ports 100Gbps towards LAN distribution, four ports 100Gbps towards Datacenters, two ports towards WAN PIN and two port 100Gbps between Core devices.

7.1.2 Distribution PIN

Landssjúkrahúsið will use the C9500-48Y4C model in the LAN Distribution


Figure 7 - C9500-48Y4C

The C9500-48Y4C has 48x 1/10/25 Gigabit-Ethernet SFP28 interfaces and four QSFP 40/100 Gigabit-Ethernet interfaces. Each switch will have redundant 650 Watts power supplies.
The switch scales to:

- 32.000 MAC addresses
- 212.000 IPv4 routes
- 32.000 Multicast routes

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.1.3 WAN PIN

Landssjúkrahúsið will use the C9500-24Y4C model in the WAN Distribution

Figure 8 - C9500-24Y4C-A

The C9500-24Y4C has 24x 1/10/25 Gigabit-Ethernet SFP28 interfaces and four QSFP 40/100 Gigabit-Ethernet interfaces. Each switch will have redundant 650 Watts power supplies.
The switch scales to:

- 32.000 MAC addresses
- 212.000 IPv4 routes
- 32.000 Multicast routes

7.1.4 Access PIN

There will be four different types of access switches in the access PIN.

7.1.4.1 Cisco Catalyst 9300

The Cisco Catalyst 9300 Series Switches are Cisco's lead stackable enterprise switching platform built for security, IoT, mobility and cloud. This is the next generation of the industry's most widely deployed switching platform.
The 9300 platform will be used for access switches in the old buildings.

The C9300-48UXM is a 48-port switch with each interface supporting speed of 100Mbps, 1Gbps and 2,5Gbps. 12 of those also Multigigabit (5Gbps and 10Gbps)

Figure 9 - C9300-48UXM-A

All ports support UPOE delivering up to 60W for Power over Ethernet. The total PoE budget for the switch is 635 Watts. Each switch will have one 1100 Watts power supply.

Each Cisco 9300 switch will be fitted with a two port SFP28 25 GigabitEthernet module. The C9300-NM-2Y will be used for uplink.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Figure 10 - C9300-NM-2Y

7.1.4.2 Cisco Catalyst 3560CX

The Cisco Catalyst 3560-CX and Series Compact Switches help optimize network deployments. These fan-less, small form-factor switches are ideal for space-constrained deployments where multiple cable runs would be challenging.

Cisco Catalyst 3560CX switch will be used in building H.

7.1.4.3 WS-C3560CX-12PD

The Cisco WS-C3560CX-12PD is a 12 port with each interface supporting speeds of 10Mbbps, 100Mbps or 1Gbps. Uplinks are fixed with two 1Gbps cupper or two 10Gbps SFP+ ports.

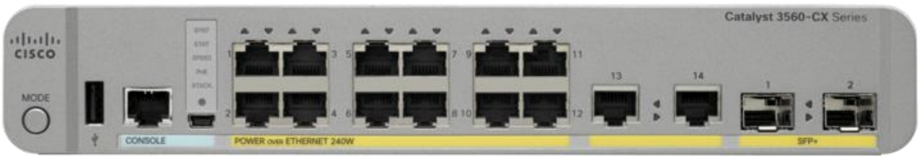

Figure 11 - WS-C3560CX-12PD-S

All ports support PoE+ delivering up to 30W for Power over Ethernet. The total PoE budget for the switch is 240 Watts. There is no option for redundant power supply.

7.1.4.4 WS-C3560CX-8XPD

The Cisco WS-C3560CX-8PD is an 8 port with each interface supporting speeds of 10Mbbps, 100Mbps or 1Gbps. Two of the eight ports support MultiGigabitethernet speeds of 2,5Gbps, 5Gbps or 10Gbps. Uplinks are fixed with two ports supporting speeds of 10Gbps.

Figure 12 - WS-C3560CX-8XPD-S

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

All ports support PoE+ delivering up to 30W for Power over Ethernet. The total PoE budget for the switch is 240 Watts. There is no option for redundant power supply.

7.1.4.5 Catalyst 3850

Some of Landssjúkrahúsið old Catalyst 3850 will remain in operation. They will be connected to the Distribution PIN just like a Catalyst 3560cx.

7.1.5 Wireless Access

7.1.5.1 Cisco Catalyst 9100

The Cisco Catalyst® 9120AX Series Access Points are the next generation of enterprise access points. They are resilient, secure, and intelligent and offer latest technology support like full WiFi6 feature sets. The AP support duale 4x4:4 and full MU-MIMO and downlink/uplink OFDMA

Figure 13 - C9120AX

7.1.6 Cisco Nexus 9300

Cisco Nexus® 9300-FX3 Series is the latest generation of datacenter access switches. Building on the successful Nexus 9300-FX series, the platform supports cost-effective cloud-scale deployments, an increased number of endpoints, and is capable of wire-rate security and telemetry. The platform is built on modern system architecture designed to provide high performance and meet the evolving needs of highly scalable datacenters and growing enterprises.

7.1.7 N9K-C93180YC-FX3S

The Cisco Nexus 93180YC-FX3 Switch is a 1RU switch that supports 3.6 Tbps of bandwidth and 1.2 bpps. The 48 downlink ports on the 93180YC-FX3 can support 1-, 10-, or 25-Gbps Ethernet, offering deployment flexibility and investment protection. The 6 uplink ports can be configured as 40 and 100-Gbps Ethernet, offering flexible migration options.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Figure 14 - N9K-C93180YC-FX3S

7.1.8 Out of Band

The Out of Band PIN is a separate management network, only used to manage network and datacenter equipment.

7.1.8.1 Cisco Catalyst 9200

The Cisco Catalyst 9200 switch

The C9200 switch will be used as Out of Band switch for core network and datacenter equipment.

7.1.8.2 C9200L-48T-4G-A

The C9200L-48T-4G is a 48-port switch with each interface supporting speed of 100Mbps and 1Gbps.

Figure 15 - C9200L-48T-4G-A

Uplinks are fixed 4x 1Gbps.

7.2 Physical LAN Design

The LAN design consists of five different types of PINs. Core PIN, distribution PIN, Access PIN, Server block and WAN PIN.

There are single mode optic fiber cables running between the buildings. These are routed different ways, to optimize redundancy.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

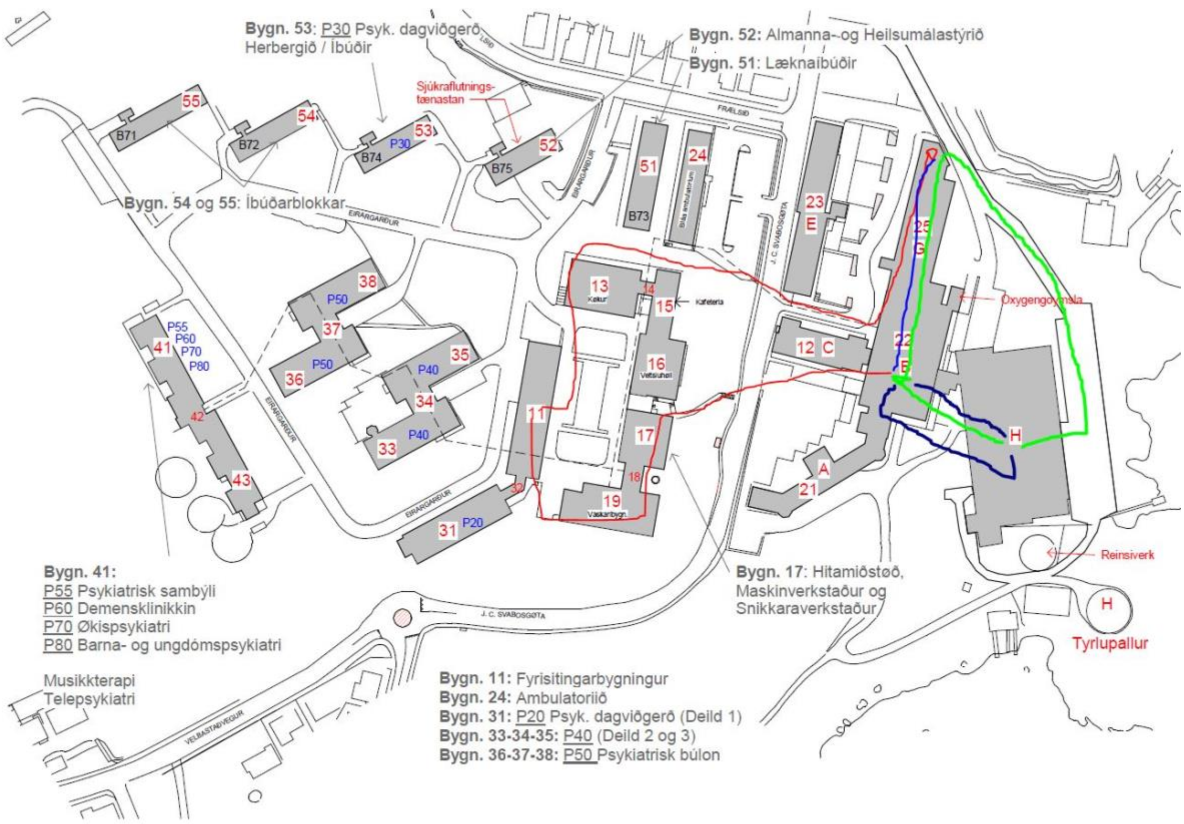

Figure 16 - Fiber cable routing

To further optimize redundancy, the different network blocks need to split their uplink to the core, to be sure that not a single damaged fiber cable can put down a complete network block.

7.2.1 Physical LAN Core Interconnect

The core layer consists of two Catalyst 9500-32C core switches. There Is one located in datacenter building B and one in datacenter building H.

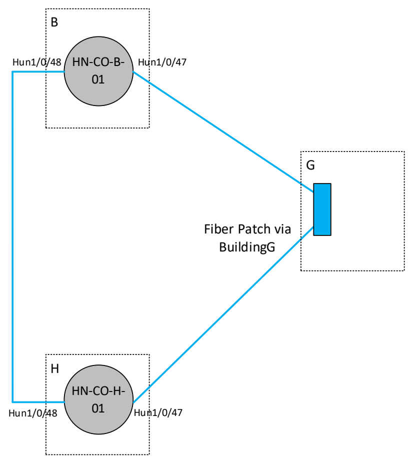

Table 1 - Core connections

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

The two core switches will be connected with two 100Gbps connections. They will be routed physically via redundant paths.

7.2.2 Physical LAN Core to Server Block Interconnect

The server block consists of eight Cisco Nexus 93180YC-FX3 switches. They are located in Datacenter building B and H, rack 1 and 2.

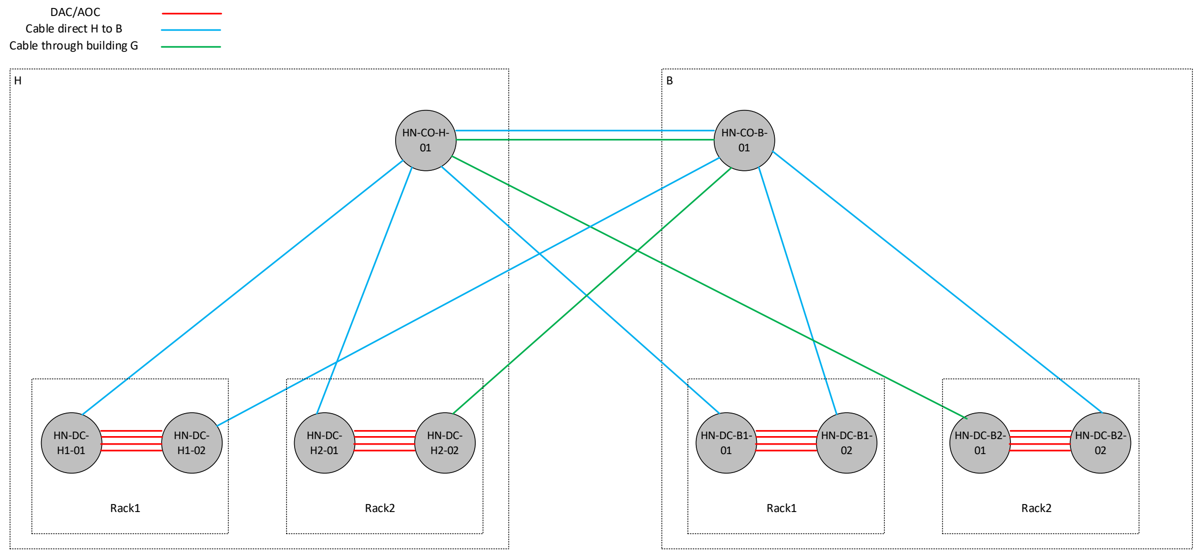

Figure 17 - Datacenter connections

There are two server rooms in the hospital. Each room will have two racks with two Cisco Nexus switches. Each Cisco Nexus will have one uplink to the Core PIN, switch one to Core in building H and switch two to Core in Building B.

All connections between Nexus switches and the core connections will be with speeds of 100Gbps. For redundancy purpose, one of the redundant connections will be via building G to prevent totally loss of connection, if a fiber cable is damaged.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.2.3 Physical Core to Distribution Interconnect

Each LAN distribution blocks consist of two distribution switches. The interconnection link between the two distribution switches is using a single 100Gbps routed interface. Each distribution switch has a 100Gbps routed link towards the two cores.

Each switch has forty-eight 10/25GigabitEthernet downlinks, the total downstream bandwidth will be maximum of 1200Gbps. With uplink bandwidth of two 100GigabitEthernet links, the total upstream bandwidth will be 200Gbps. The over-subscription ratio for the PIN will be 6:1.

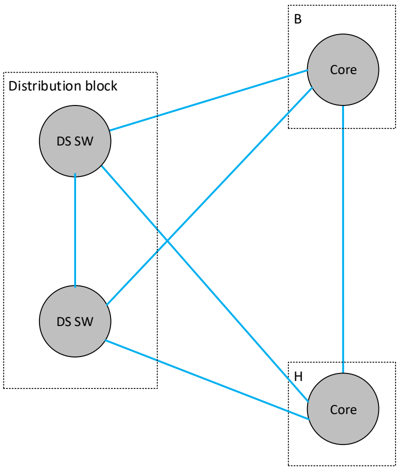

Figure 18 - Core to distribution connections

7.2.4 Physical Core to WAN Interconnect

The WAN distribution block consists of two C9500H 24 ports switches. One in the DC room in building H and the other in the DC room building B. The switches will be interconnected with two 100Gbps connections. One of the links will run as a layer 2 stretch to service both internal firewall failover links, but also external connections to service providers that are only able to use HSRP or another layer 2 failover service.
The other link will run as a routed link.

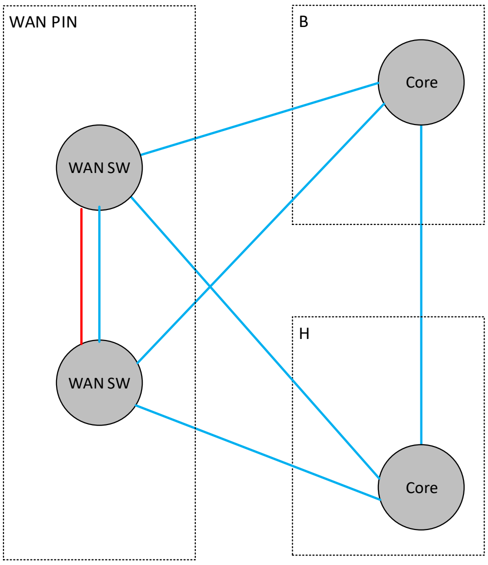

Figure 19 - Core to WAN connections

7.2.5 Physical LAN Distribution to Access Layer Interconnection

7.2.5.1 Building H

To interconnect each access layer switch, two 10 Gigabit Ethernet fiber optic connections will be used. An access switch must be connected to a single distribution switch block.

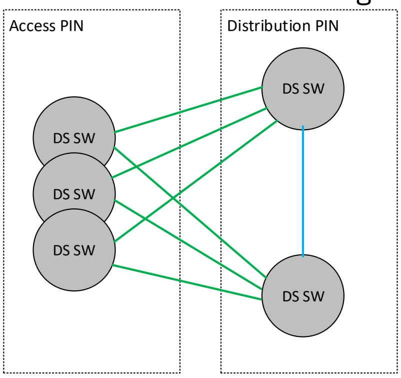

Figure 20 - Distribution to Access connection.

7.2.5.2 Building A and B

As In bulding H, each access layer switch will be connected to the distribution switch with two 10Gigabit Ethernet fiber optics. See figure 20.

In building A and B there will be some access switches consisting of multiple Catalyst 9300, connected in a stack. There can be a maximum of eight switches in one stack. The Catalyst 9300 are equipped with 25Gbps uplink interfaces.

Stack switches will only have two uplinks for one stack. The diagram below shows a switch stack of three switches connected to a distribution block.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

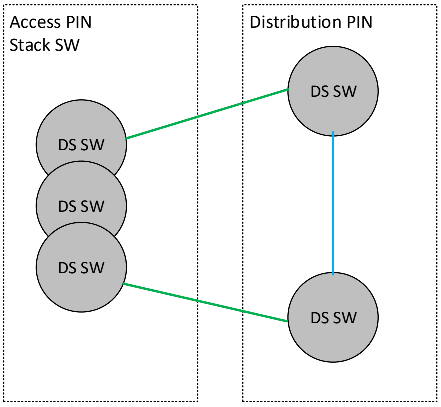

Figure 21 - Distribution to access stack connection

7.2.6 Physical Firewall Interconnect

There are several sets of firewalls active in the network at LS. They are implemented and handle different tasks. Below is the list of firewall sets.

- Internet
- External MPLS / site-2-site VPN
- Application / Datacenter firewall

Internet and MPLS/s2s firewall both are connected in the WAN PIN with both a layer 2 and a layer 3 connection. The connections are all 1Gbps connections.

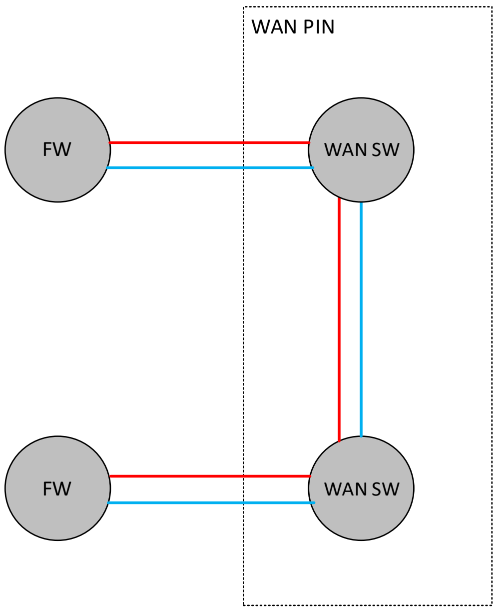

Figure 22 - WAN to Firewall connection

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

The Application firewall Is connected in Rack 1 in both the datacenter in building B and H. The connections of the Application firewall are all 10Gbps and will also have both layer 2 and layer 3 connections. The interfaces will be bundled to form an ether-channel.

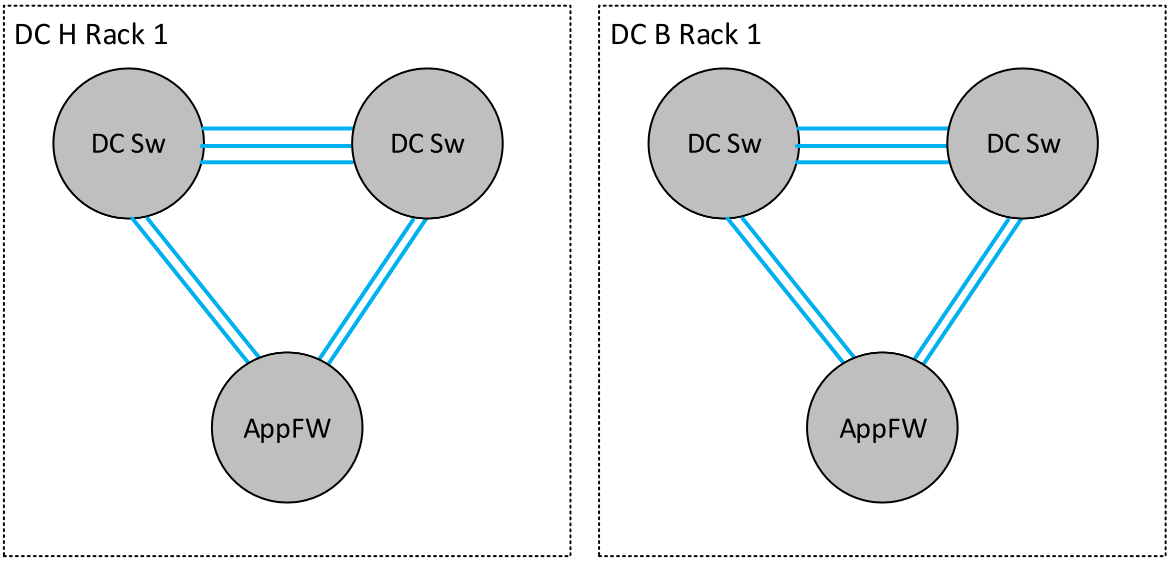

Figure 23 - AppFW to DC switch connection

7.2.7 Physical Wireless Catalyst 9800 Interconnect

The Cisco 9800-LF Wireless LAN Controllers will be configured as a High Availability cluster. The cluster will exist as a service in the WAN. One will be installed in building B and the other in building H.

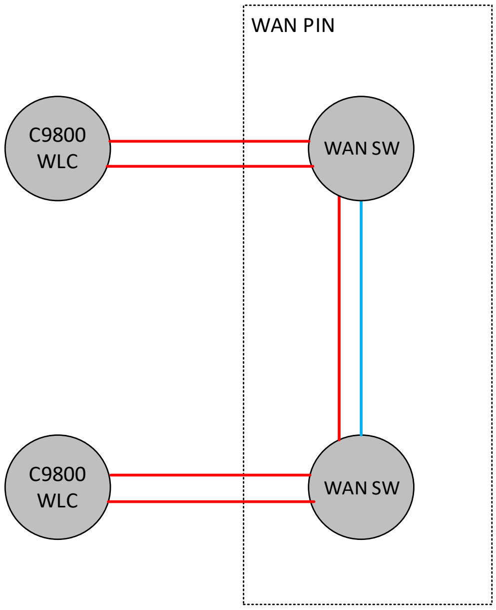

Figure 24 - C9800 Interconnect

The WLC will be connected using 10GigabitEthernet SFP-10G-CU7M. Due to combability issues, it is not possible to use a shorter cable.

Please note. The WLC will support 5 Gbps, only 10 If Performance license Is Installed.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.3 Physical allocation

7.3.1 Core Units

Hostname	Placement	Description
HN-CO-H-01	DC building H Rack 5	Core at building H
HN-CO-B-01	DC Building B Rack X	Core at building B

Table 2 - Core Units

7.3.2 Distribution Units

Hostname	Placement	Description
HN-DS-H-101	Patch room building H	Distribution H Pair 1
HN-DS-H-102	Patch room building B	Distribution H Pair 1
HN-DS-H-201	Patch room building H	Distribution H Pair 2
HN-DS-H-202	Patch room building B	Distribution H Pair 2
HN-DS-H-301	Patch room building H	Distribution H Pair 3
HN-DS-H-302	Patch room building B	Distribution H Pair 3
HN-DS-H-401	Patch room building H	Distribution H Pair 4
HN-DS-H-402	Patch room building B	Distribution H Pair 4
HN-DS-A-01	Old DC building A Rack X	Distribution A Pair 1
HN-DS-A-02	Old DC building A Rack X	Distribution A Pair 1
HN-DS-B-01	DC building B Rack X	Distribution B Pair 1
HN-DS-B-02	DC building B Rack X	Distribution B Pair 1

7.3.3 Server Block Units

Hostname	Placement	Description
HN-DC-HR1-01	DC building H Rack 1	DC H switch Rack 1 switch 1
HN-DC-HR1-02	DC building H Rack 1	DC H switch Rack 1 switch 2
HN-DC-HR2-01	DC building H Rack 2	DC H switch Rack 2 switch 1
HN-DC-HR2-02	DC building H Rack 2	DC H switch Rack 2 switch 2
HN-DC-BR1-01	DC building B Rack 1	DC B switch Rack 1 switch 1
HN-DC-BR1-02	DC building B Rack 1	DC B switch Rack 1 switch 2
HN-DC-BR2-01	DC building B Rack 2	DC B switch Rack 2 switch 1
HN-DC-BR2-02	DC building B Rack 2	DC B switch Rack 2 switch 2

7.3.4 WAN Block Units

Hostname	Placement	Description
HN-WS-H-01	DC building H Rack 5	WAN switch at building H

HN-WS-B-01	DC Building B Rack X	WAN switch Core at building B

7.4 Logical Segmentation

One of the key requirements of the design is to accommodate the need for segmentation. Using different virtualization techniques, the same physical network implementation will offer infrastructure services to nodes belonging to different security zones, logical segments and domains.
This design will have layer 3 and layer 2 segmentation. For layer 3, the switches will be using VRF (Virtual Routing and Forwarding) instances. The VRFs will ensure that each virtual network will have its own interface, routing and forwarding table. Each VRF will not be able to communicate with a different VRF without going through a router or a firewall that stitches them together.

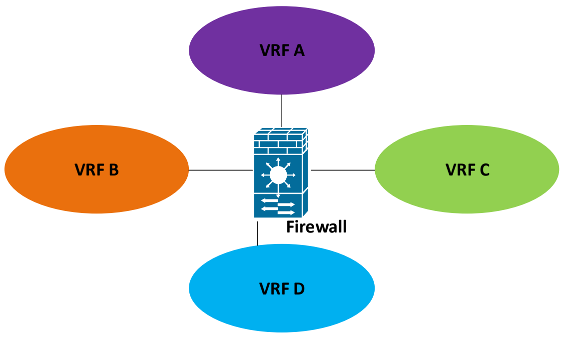

Figure 25 - VRF concept

For layer 2 segmentation VLAN (Virtual Local Area Network) will be used. VLANs will ensure that the switches have multiple different broadcast domains to separate layer 2.

Note. The Wireless LAN controller will not use VRF to forward all traffic to its default gateway, which will be the WAN PIN.

7.4.1 Layer 3 Segmentation

Landssjúkrahúsið will be needing nine different layer 3 logical segments.[1] Catalyst 3560cx supports up to 26 different logical segments including the global.

- Global routing table (Default table - not a VRF)
  - For infrastructure management
- EntAccess
  - For end-user clients and printers, etc. connecting to the access PINs
- Medico
  - Logical segment for Medical equipment nodes
- CareCall

[1] More VRFs might be added as part of the HLD evaluation or migration planning.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

    - Logical segment that allows controlled IoT devices to access the Internet
- CTS
    - Logical segment for environmental building control
- CCTV
    - Logical segment that allows controlled CCTV devices to access the Internet
- Salto
    - Logical segment for door control
- IoT-Untrusted
    - Logical segment that allows uncontrolled IoT devices to access the Internet
- Guest
    - Logical segment that allows guests to access the Internet[2]

In other words, all layer 3 switches will be segmented into at least eight logical virtual routers. To interconnect to switches with multiple VRFs on both switches, BGP EVPN will be used.
In Building H were Cisco Catalyst 3560cx are used as access switches, which are not capable of BGP EVPN, VRF lite with a routed sub interface pr VRF will be used, between the distribution block and the access layer.

Sub-interfaces use 802.1Q layer 2 segmentation to separate the different logical segment frames from each other. Sub interfaces are not supported on C3560cx, SVIs will be used in the access switch end.

[2] VRF Guest will only exist in the WAN Block

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

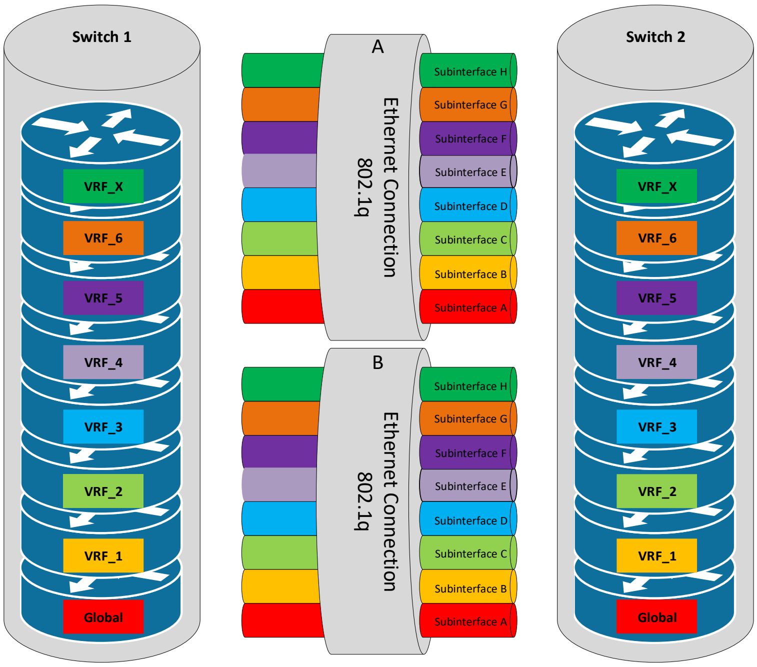

Figure 26 – Sub-interface concept

7.4.2 VRF naming

Each VRF will be created without using a name referring to the service running in the VRF segment. The VRF to service mapping is done in documentation and not in the switches. This ensures that if a service leaves a VRF empty, this VRF can be reused for another service without needing to change VRF name on all the switches. Furthermore, it makes it possible to preconfigure VRFs, that have not yet been assigned to a service.

VRF Name	Logical name	Security zone
global	Management	Trusted - Access Controlled
v2100	Enterprise Access	Trusted - Access Controlled
v2200	Medico	Trusted - Access Controlled
v2300	CareCall	Trusted - Access Controlled
v2400	CTS	Trusted - Internet access only
v2500	CCTV	Trusted - Internet access only
v2600	Salto	Trusted - Internet access only
v2700	IoT untrusted	Untrusted - Internet Access Only
v2800	Guest	Untrusted - Internet Access Only[3]
v2900	unused	
v3000	unused	
v3100	unused	
v3200	unused	
v3300	unused	
v3400	unused	
v3500	unused	

[3] VRF Guest will only exist in the WAN PIN. Only wireless clients will be able to connect to the Guest network

v3600	unused	

Table 3 - VRF names

7.4.3 Layer 2 Segmentation

Each layer 2 broadcast domain will serve as a layer 2 segment. VLANs in the access layer will be locally significant for the access layer switch itself. A VLAN cannot span from one access switch to another access switch. Please be aware that the same VLAN ID can be used on two different access switches, but they will be two different layer 2 segments, and will only be able to communicate using their individual default gateways.

VLANs in the server PIN will be spanned between each server block switch. For this BGP EVPN will be used. Two nodes in different server switches will be able to communicate over layer 2 if they share the same VLAN.

VLANs in the WAN block will be spanned between each WAN Inside switch. Two nodes in different WAN switches will be able to communicate over layer 2 if they share the same VLAN.

7.4.4 Spanning-Tree

As the network mainly is a Layer 3 routed access network, the design does not need to rely on Spanning-tree protocol to ensure a loop free topology.

As there is no Layer 2 spanning from one access switch to another, each access switch will have its own spanning-tree domain. Spanning-tree will be enabled to protect against internal cabling loops in the wiring closet.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

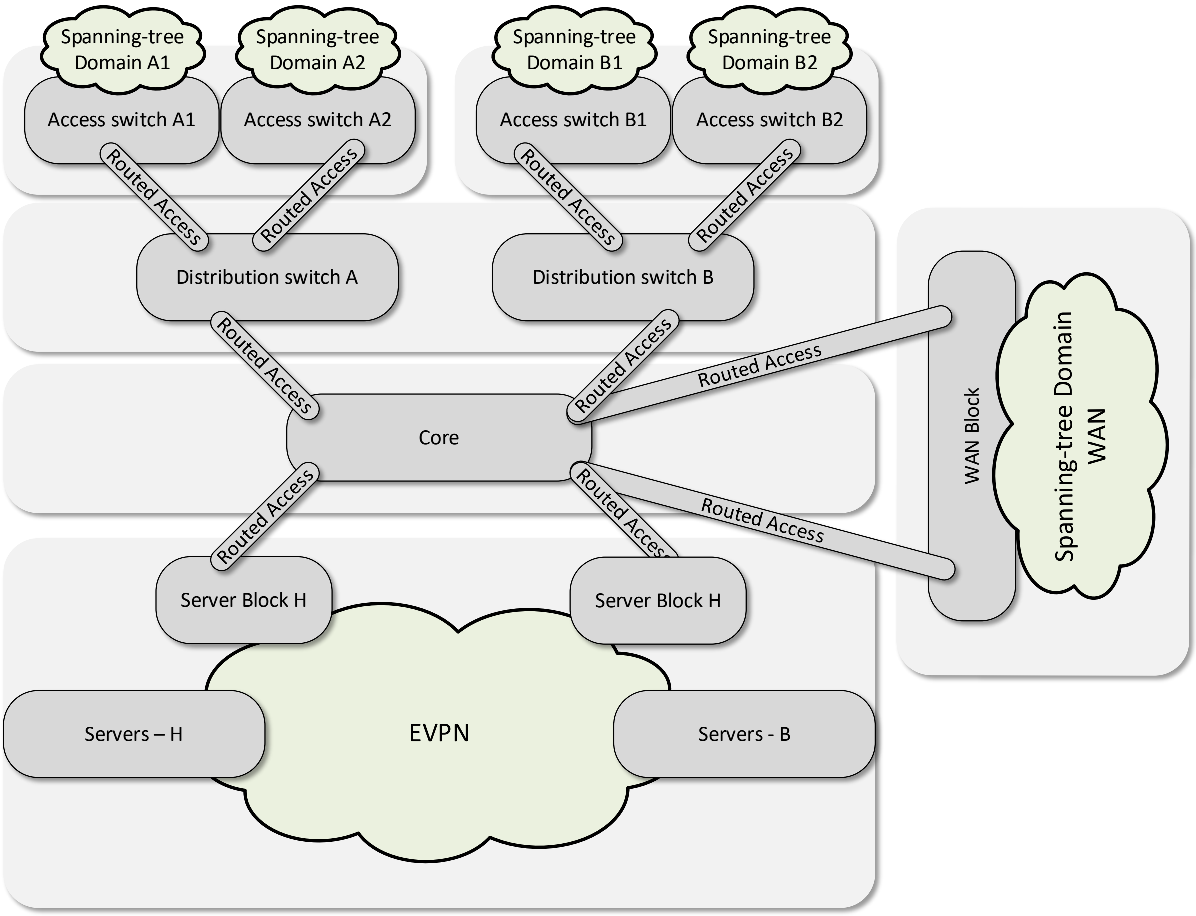

Figure 27 - Spanning-Tree Domains

In the Server Block, Spanning-tree domains will be limited to the rack closet. The switch pair in a rack, will be a spanning-tree domain. The switch pair will run vPC to enable Multi Chassis Etherchannels. VLANs will be spanned between server racks using EVPN, thereby eliminating Spanning-Tree between the server racks and mitigating the risk of spanning-tree loops.

WAN PIN Spanning-tree

Layer 2 is needed in the WAN PIN for some of the failover setup with the service provider. As the switch in building H is primary, this will also be the root bridge in the spanning-tree.

This design will be using RPVST+, which offers good flexibility, interoperability with other types of Cisco equipment, and fallback to IEEE 802.1D.

Server PIN layer 2

The server PIN is separated in four different layer 2 domains. To support IP mobility between the four domains, BGP EVPN will be used.

7.5 Layer 3

7.5.1 Layer 3 Termination Points

Core
All interfaces will be routed interfaces. As described in section 7.2.1. VXLAN will be used to support multiple VRFs on any link. The core will not be aware of any VRF.

Distribution
Distribution switch will be encapsulating the different VRFs in VXLAN

Due to the hardware limitation, the Cisco Catalyst 3560cx is not capable of running MPLS. Due to this, there will be two different types of distribution blocks: One running as a MPLS P node, with no knowledge of VRFs and one being aware of VRFs and running one sub-interface per VRF downstream to the access switch.

Building H
In the distribution switches, all interfaces will be routed interfaces. As described in section **Error! Reference source not found.** sub-interfaces will be used to support multiple segments on the same physical routed interfaces.

Building A and B
In the distribution all interfaces will be routed interfaces. As described in section 7.2.1. MPLS VPNv4 will be used to support multiple segments on the same physical routed interface

Server Block
The server block will be running routed interfaces towards the core. Also, the server block switches will terminate VLANs in Switched Virtual Interfaces.

Access Layer
Each access-layer switch will terminate the VLANs used on that switch. Each VLAN will have a corresponding SVI that will serve as a gateway for that individual subnet. There will be no HSRP, as each access layer PIN only consists of one switch.

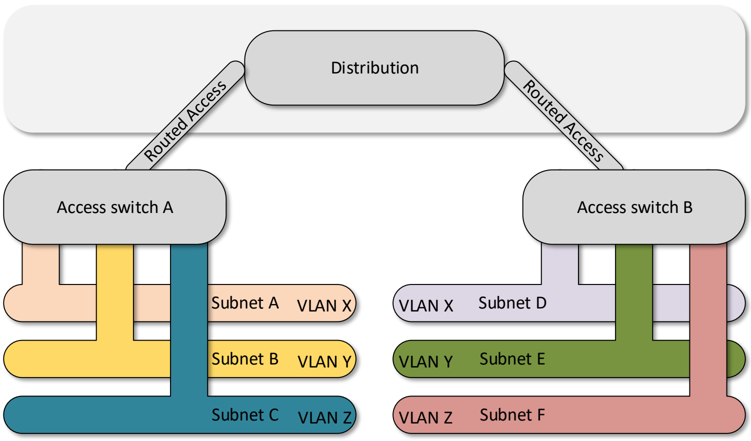

Figure 28 - Access layer SVIs

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.5.2 Dynamic Routing Protocols

Underlay

To ensure that all layer 3 blocks can dynamically exchange routing information with each other, OSPF will be used. Open Shortest Path First Protocol (OSPF) is an advance interior gateway protocol suited for many different topologies and media. In a well-designed network, OSPF scales well and provides extremely quick convergence times with minimal traffic loss.

Routing protocols can use load-balancing or Equal Cost Multipath (ECMP) to share traffic across multiple paths. Load-balancing distributes the traffic across all the paths, sharing the traffic load across interfaces. For all L3 links, ECMP will be used to utilize all L3 paths.

OSPF uses Areas to ensure scalability and fault containment. The core Area is always area 0. Any other area must be connected to Area 0 using an Area Border Router.

Overlay

Border Gateway Protocol EVPN, will be used as an overlay protocol to distribute VRFs between PE nodes

To ensure full reachability BGP EVPN will be used. EVPN is originally made to transport layer 2 packets over layer 3. It has been extended to also be able to announce IPv4 and IPv6 prefixes. BGP EVPN will be enabled in the Server PIN, WAN PIN.

For layer two mobility between racks in the datacenter and to transport VRFs, VXLAN will be deployed.

MPLS Segment-Routing will be enabled on core, datacenter, distribution, and access switches, if the access switch is a Catalyst 9300. VRF-lite will be used from the distribution switch down to the access switch if the access switch is Catalyst 3560cx or Catalyst 3850.

Initially Catalyst 3560cx will only be installed in building H, but to ensure any future requirements of C3560cx in the other distribution block, all will be configured to be able to run with VRF-lite. BGP will be used to ensure routing in every VRF.

BGP will be used to route from the access layer in all VRFs. This protocol will also support the wish for using Philips IntelliVue system

To eliminate the need for a full mesh iBGP peering, BGP route-reflectors will be used. The WAN PIN will be implemented as route reflector for all address families.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.5.3 Multicast

Today Landssjúkrahúsið has multicast running to support several services. Multicast will be configured. Both to support the services running today, but also to support the overlay vxlan.

7.5.4 Quality of Service

As more and more systems and applications are being enabled on the same converged network, the need for QoS to ensuring a reliable delivery of critical applications compared to non-critical applications comes into play.

Quality of Service has been implemented End-to-End, in all layers of the network, including the core, distributions and access layers to “protect the good and punish the bad” applications. QoS policies are used to protect mission-critical applications, while giving a lower class of service to suspect traffic.

QoS is also used to protect the network from suffering from the lack of bandwidth, which Internet worms, denial of service attacks, as well as bandwidth stealing applications can flood links even in a high-speed network environment.

7.5.5 IP Plan

The overall IP allocation scheme must follow these guidelines:

- Loopback must be allocated as /32
- Point-to-Point Link networks must be allocated as /30 subnets
    - 100.96.0.0/11 (RFC 6598), segmented per VRF.
- Link networks towards firewalls can be allocated as /29 subnets
- Wired Access layer per switch
    - Enterprise pr: /24 for Heilsunet
    - Medical network /26
    - /28 in every other VRF
- WiFi subnet for Client access should be /22 subnet as default
        - Guest network like a /21

7.6 Security

7.6.1 Security Zones

Each VRF is a complete separate network and will need to go through a firewall to connect to other network segments.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

The Internet firewall will be the default choice for a VRF. The Internet firewall will be a physical firewall with an interface in each VRF and an interface in the WAN MPLS / Internet segment. This firewall will enforce access-control between the VRFs and between each VRF and the WAN.

The overall network can be segmented into three different security zone types (Trusted - Access Controlled, Trusted - Internet Access Only & Untrusted - Internet Access Only). A node will have full access to all other nodes in the same VRF, but not necessarily to other VRFs in the same security zone. All access control will be handled by the firewall.

Zone	Description
Trusted - Access Controlled	For trusted nodes that are controlled by Landssjúkrahúsið. All access will be controlled.
Trusted - Internet Access only	For controlled nodes that only need Internet.
Untrusted - Internet Access Only	For uncontrolled nodes like IoT devices. Nodes will have access to Internet only.

Table 4 -Security Zone Table

7.6.2 Link Encryption

To further secure the network links will be encrypted. MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The Catalyst 9000 series switch supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication and MACsec encryption between switches.

7.6.3 Layer 2 security

To harden the access layer and to mitigate unauthorized access to Landssjúkrahúsið's network, some of the integrated security features in the access switches will be enabled. These features will be:

- DHCP snooping
- arp inspection
- storm-control

7.6.4 ISE

Cisco Identity Service Engine (ISE) is the policy decision point in an SDA implementation. Cisco ISE is an advanced RADIUS server focused on network policy decisions.

An ISE policy consists of three concepts – Authentication, Authorization and Accounting. These concepts are described in the section below.

7.6.5 Authentication Mechanisms in ISE

An ISE deployment works with three primary authentication mechanisms.

1. 802.1X
2. Mac Authentication Bypass

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

3. Profiling

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

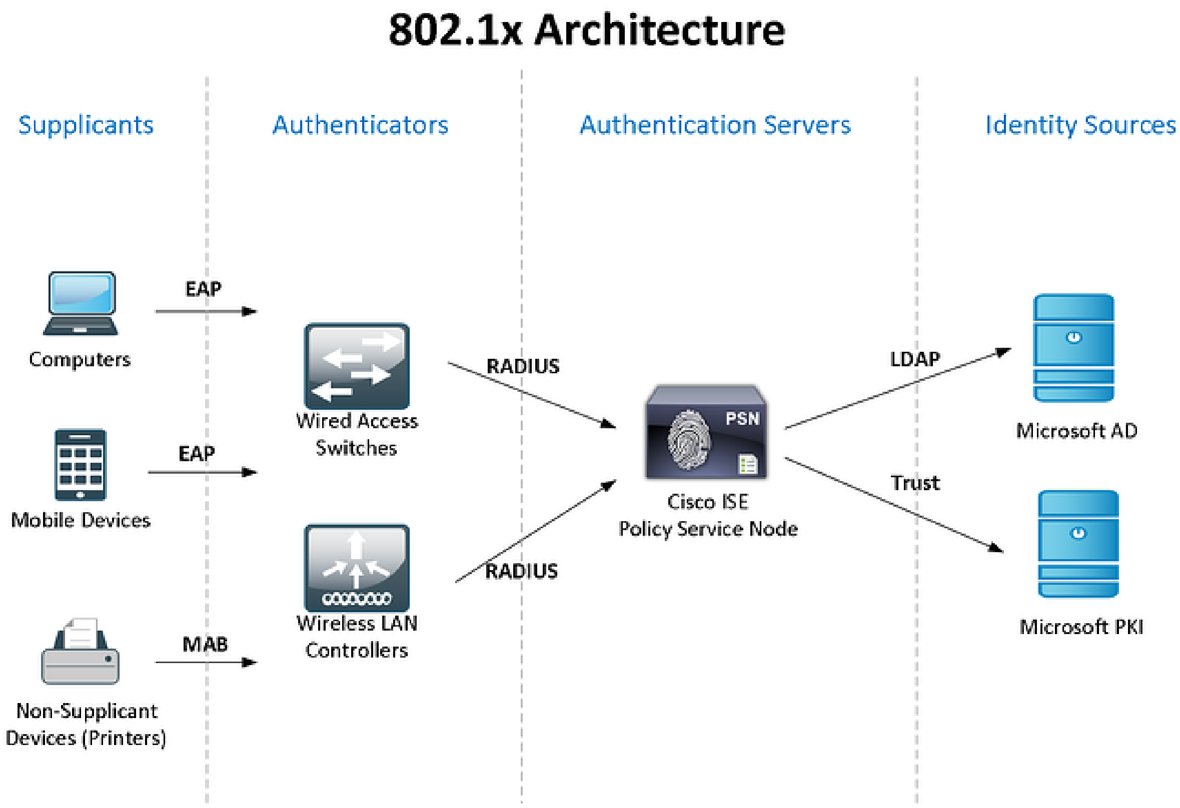

Figure 29 - 802.1x overview

7.6.5.1 802.1X

802.1X is an authentication mechanism that requires a username/password combination or a certificate for example. The primary 802.1X authentications, which we will use in the deployment, is EAP-TEAP.
Microsoft now has support for EAP-FASTv2 EAP-TEAP (RFC7170) in windows 10 Build 2004

Pros: Native Microsoft supplicant
Controlled by GPO
Secure method to user & machine
RFC7170 compliance

Cons: TEAP is a new Microsoft feature, not well tested in windows 10

7.6.5.2 MAB

Mac Authentication Bypass is an authentication mechanism that validates the MAC address against a database. If the MAC address exists in the database, the authentication is passed. The database can exist locally in ISE or in an external DB, LDAP server or Active Directory.
MAC computers will be MAB authenticated. ITM systematic don´t want to support MAC computers.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

7.6.5.3 Profiling

Profiling is a mechanism where ISE evaluates a set of attributes forwarded to ISE from network devices, data received on a SPAN ports, telemetry from Netflow, device sensor or an NMAP scan of the endpoint to identify the type of device. Once identified, the ISE can make policy decisions on the endpoint.

Once the endpoint has successfully authenticated, a decision on the authorization must be made. The authorization policy is very flexible, but an example is that a specified group of MAC Addresses will be authorized to a specific VLAN, where an 802.1X user will be authorized to another VLAN.
The use of SGTs will allow us to create policies between endpoints in the same VLAN which will also be widely used in the implementation at Systematic. SGTs is described in detail in a section further along in this document.

7.6.5.4 Certificates

All Landssjúkrahúsið endpoints shall have a valid machine -or user certificate installed. These certificates will be used for authentication & authorization.
ISE will have a complete certificate path installed in ISE “Trusted Certificate Store”.
ISE will also have a certificate in ISE “System Certificate Store” used for EAP authentication.
ISE will generate a CSR file for Systematic PKI infrastructure.

8 Naming Guidelines

Network devices are named after a standard provided by Landssjúkrahúsið.

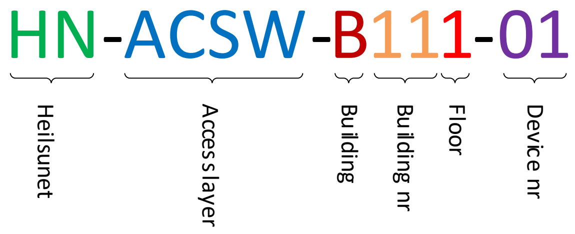

Figure 30 - Naming standard

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

9 Management and Monitoring

9.1 SSH & HTTPS

Management access to network devices should be done using SSH or HTTPS. Access to the management interface should only be allowed from designated IP addresses, i.e. Jumphosts and management systems.

9.2 AAA

All access to switches must be controlled through individual usernames and passwords. There will be no general SSH or enable password on the devices; only a fallback username and password will be configured in case a switch cannot access the AAA (Authentication, Authorization, Accounting) servers. This will increase the overall security for all platforms.

Ideally, the fallback password would be stored in a safe and only taken out when needed. However, this is not practical as the fallback password is likely to be required in a troubleshooting situation in the middle of the night. The fallback password should be defined and kept by Landssjúkrahúsið.

The AAA functionality will be by the already installed Cisco ISE server, managed by Landssjúkrahúsið. The Cisco ISE will use Microsoft AD as user backend, providing access rights based on AD Security Groups.

ISE fully supports the use of Role Based Access Control, ensuring that users can get differentiated access rights. Users that are members of one Security Group might get full administrative privileges, while members of other Security Groups might get none or partly administrative privileges.

9.3 Syslog server

The SYSLOG protocol can be used to send logging information from the switches to a central server. This server should be able to perform proper filtering of log messages to make them useful. Landssjúkrahúsið already has a SYSLOG engine to collect information. This SYSLOG server will be used for all network infrastructure devices. Syslog will be configured per Landssjúkrahúsið guidelines.

9.4 SNMP

It will be possible to manage the devices using SNMP. Landssjúkrahúsið will use multiple management systems, such as Cisco DNAC and Solarwinds Orion, to monitor the network infrastructure.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj

Access to SNMP will be controlled through a combination of communities and access lists. Only known hosts should be allowed to connect via SNMP. SNMP version 3 should be preferred over version 2.

10Automation-Ready Network

Market trends indicate that over the next 3-5 years control and management of the enterprise networks are expected to become more automated. The increasing demands for security and segmentation will make the network configuration highly complex and the number of incidents and problems caused by manual human configuration will probably increase. Furthermore, more insight into what is being transferred over the network will be required. Big data will need to be collected and processed to ensure that the network is stable, secure, and compliant. The data intelligence will be used by the automation engine to change the network configuration in real time. Faster and with fewer errors than with human operators.

Cisco's Software Defined Access does all the above.

- Consistent management of wired and wireless network provisioning and policy
- Automated network segmentation and group-based policy
- Contextual insights for fast issue resolution and capacity planning
- Open and programmable interfaces for integration with third-party solutions
- It will offer the same revolution for the wired network as the Wireless LAN Controller was to the wireless network

The transition into software defined network can bring huge changes to both the business and the operation teams running the network. Therefore, this design focuses on getting the network hardware and infrastructure SDA ready, but not an SDA solution. Cisco SDA can be implemented at a later phase. This also allows for the SDA solution and technology to evolve further during the implementing this project.

The Cisco Software-Defined Access solutions overview is attached to this document.

Please note. The DNA-Center will be able to monitor Hardware like Routers, switches, AP, WLC and maybe most important, the online (wired and wireless) users. The DNA-VC will be able to do this in a historical way and you can track users back in time. This Is a very strong tool for troubleshooting

11Deployment and Automation

As mentioned in section **Error! Reference source not found.**, the network must support the use of automation and software-controlled management and deployment. Cisco Digital Network Architecture delivers a frameset for Software Defined networks. The DNA-Center is a physical appliance, that works as a network controller and delivers API capabilities towards the network platform. DNA-Center also have multiple ready to use Apps, like the Cisco Software Defined Access and Plug'n'Play.
Even though this design will not be built using Software Defined Access, it will include the DNA Center. The main functions used will be the Software Image Management (SWIM) and the Plug'n'Play engine for easy onboarding of new network devices. Using these features alone, will mainly ensure a more standardized platform and not necessarily ease the operational tasks. To ease the deployment and operational tasks, software is needed to ensure that the different workflows and templates will be deployed automatically and in the right order. This software works as the glue between a standard operating procedure and the DNA Center templates for each workflow. This software must be built directly to support Landssjúkrahúsið's design and workflows.

The enrollment goal is to deploy the access-layer using DNA Center and software automated workflows or plug'n'play configurations.

All other layers will be deployed by hand.

Phone +45 70 20 77 80 • www.conscia.dk • East: Kirkebjerg Parkvej 9, 2605 Brøndby • West: Nannasvej 7, 8230 Åbyhøj