Bachelor's thesis

Information and Communications Technology

2019

Mikko Jaakonsaari

IMPLEMENTATION OF CISCO FLEXCONNECT

TURKU AMK

TURKU UNIVERSITY OF
APPLIED SCIENCES

BACHELOR’S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering

2019 | 38 pages.

Mikko Jaakonsaari

IMPLEMENTATION OF CISCO FLEXCONNECT

Controller-dependant & centrally switched wireless access points are easy to manage and set up. However when the amount of sites increases, wireless performance may become sub-optimal. Cisco FlexConnect enables access points to switch user data locally at a remote site, thus improving network performance and optimizing routing.

This thesis describes the implementation of FlexConnect, describing necessary changes and configurations for each participating network device and server. The thesis also describes alternatives to the chosen solution that provide the same functionality similar to FlexConnect on other vendors’ network equipment. Due to the nature of the thesis, the majority of the source material is available online, and consists of vendor documentation and standards based off of International Electrotechnical Commission (IEC) and Internet Engineering Taskforce’s (IETF) Requests For Comments (RFC).

Network performance was tested by comparing routes to servers located in various data centers and by comparing download and upload speeds over the wireless network. The tests were performed before and after the FlexConnect implementation to provide comparable data.

The results demonstrated improved routing performance in a multiple site network environment. Recommendations for further actions were also provided for next steps in improving wireless performance.

KEYWORDS:

Network, Wireless, Cisco, Implementation.

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

tieto- ja viestintätekniikka

2019 | 38 sivua.

Mikko Jaakonsaari

CISCO FLEXCONNECT - KÄYTTÖÖNOTTO

Controller-hallitut ja keskitetysti kytketyt langattomat tukiasemat ovat helppoja ottaa käyttöön ja hallita, mutta kun toimistojen määrä kasvaa, saattaa langattoman verkon suorituskyky laskea. Cisco FlexConnectin avulla tukiasemat kykenevät kytkemään käyttäjän liikennettä paikallisesti, parantaen verkon suorituskykyä ja optimoiden reititystä.

Tämä opinnäytetyö kuvaa laitetyyppi kerrallaan tarvittavat konfiguraatiomuutokset Cisco FlexConnectin käyttöönottoa varten. Opinnäytetyössä myös kuvataan muiden laitevalmistajien teknologioita, joilla saavutetaan sama toiminnallisuus. Opinnäytetyön lähteet perustuvat pääasiassa verkkolähteisiin, valmistajien dokumentaatioon, International Electrotechnical Commissionin (IEC) standardeihin ja Internet Engineering Taskforcen (IETF) Request For Comments – artikkeleihin (RFC).

Langattoman verkon suorituskykyä testattiin vertailemalla reititystä eri konesaleissa sijaitseviin palvelimiin, sekä suorittamalla siirtonopeustestejä ennen ja jälkeen käyttöönoton.

Opinnäytetyön tulokset havainnollistavat saavutetun parannuksen reititykseen moni-sijaintisessa verkkoympäristössä. Opinnäytetyössä myös linjataan mahdollisia seuraavia toimenpiteitä verkon suorituskyvyn parantamiseksi.

ASIASANAT:

Tietoverkko, WLAN, Cisco, Käyttöönotto.

CONTENTS

LIST OF ABBREVIATIONS

AD	Active Directory
AP	Access Point
BGP	Border Gateway Protocol
CE	Customer Edge (router)
CLI	Command Line Interface
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
FHRP	First-Hop Redundancy Protocol
FIB	Forwarding Information Base
GUI	Graphical User Interface
HA	High-Availability
H-REAP	Hybrid Remote Edge Access Point
HSRP	Hot Standby Router Protocol
IOS	Internetwork Operating System
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LSP	Label Switch Patch
LSR	Label Switch Router

MPLS	Multi-Protocol Label Switching
OSI	Open Systems Interconnection model
PE	Provider Edge (router)
RFC	Request For Comment
RSVP	Resource Reservation Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VLSM	Variable-Length Subnet Mask
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WLC	Wireless Controller

1 INTRODUCTION

Controller-dependant & centrally switched wireless access points are easy to manage and set up. However when the amount of sites increases, wireless performance may become sub-optimal. Cisco FlexConnect enables access points to switch user data locally at a remote site, thus improving network performance and optimizing routing. The goal of this thesis is to find a solution to improve the wireless network performance and routing of branch sites in office environments, as the initial wireless configuration is causing unneccesary routing which is believed to affect network performance negatively.

The solution to be implemented is a Cisco proprietary feature called FlexConnect (also known as Hybrid Remote Edge Access Point, 'H-REAP'), and the solution is to be implemented for office wireless network along with new subnets added to the existing MPLS (Multi-Protocol Layered Switching) network. The goal of the thesis is to implement Cisco FlexConnect, along with new networks and network services such as Dynamic Host Configuration Protocol (DHCP). This thesis describes Cisco FlexConnect and the necessary configuration changes in every participating network device and server.

The structure is as follows: Chapter 1 describes the background and the need for the implemented technology. Chapter 2 describes Cisco FlexConnect and the changes it presents to the wireless network behavior. Chapter 3 describes the environment in which the implementation takes place, including physical locations, network topology, network devices, and servers. Chapter 4 describes the implementation and necessary changes for every participating network device and server. Chapter 5 shows the performance tests and their results. Chapter 6 describes the conclusions of the thesis.

This thesis was commissioned by Meyer Turku Oy.

2 CISCO FLEXCONNECT

Cisco Systems (from now on referenced as “Cisco”) is multinational corporation founded in San Francisco in 1984. Cisco manufactures and designs network hardware, including network switches, routers, and wireless access points. Cisco has also broadened their catalog to include security products such as firewalls and collaboration tools such as Voice over IP (VoIP) software such as Jabber and Webex, and video collaboration tools such as Webex Devices [1].

With Aironet series – Access Points (APs) and Wireless Controller (WLC), WLC acts as the mastermind for the wireless environment, by provisioning and managing the access points, providing them Service Set Identifiers (SSID) to advertise, and forwarding user authentication requests to the Remote Authentication Dial-In User Service (RADIUS) server. By default, Aironet series APs are entirely dependant on the WLC. Access points need to connect to a WLC in order to know which wireless networks to advertise, which radio frequencies to use and to be able to authenticate users. To do this, the AP forms a Control and Provisioning of Wireless Access Points (CAPWAP) – tunnel between the AP and the WLC. All network traffic, including user data and AP management data, is forwarded into the CAPWAP tunnel. WLC then makes the switching decision for user data. This is illustrated in Figure 1, where both management and user data are tunneled to the WLC.

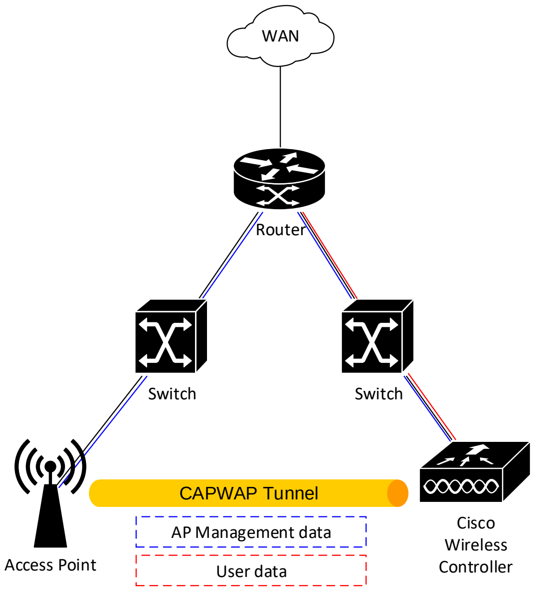


Figure 1. Default access point behaviour.

Cisco FlexConnect (or H-REAP, Hybrid Remote Edge Access Point) is Cisco proprietary solution for Wireless Controller (WLC)-dependant APs. The FlexConnect solution enables Aironet-series APs to locally switch user data. The access point is still dependant on the WLC, but only for management and user authentication [2]. In FlexConnect mode, AP switches the user traffic locally, similarly to a LAN switch. FlexConnect can also be configured to provide local authentication in case the connection to the controller is lost.

FlexConnect's greatest change is in the switching, and in a topology where multiple sites share the same WLC and this also causes changes in the routing. As the user data does not pass the WLC in Flexconnect, in environments which have interconnected remote sites, wireless user data will take the shortest route to the destination network. This is illustrated in Figure 2.

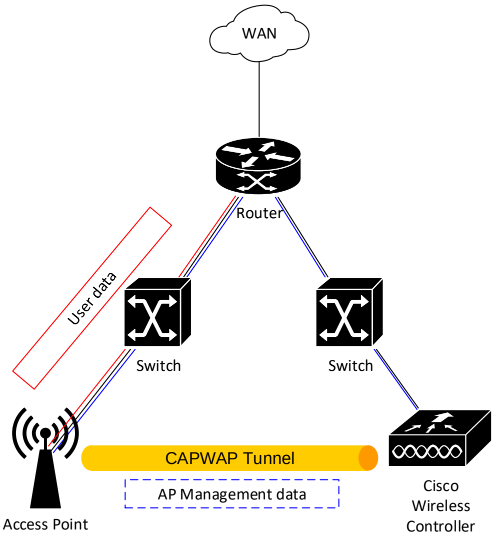


Figure 2. FlexConnect local-switching access point behaviour.

3 BACKGROUND STUDY

Meyer Turku Oy is a shipbuilding company specializing in cruise ships, and is based in Turku, Finland. Meyer Turku specializes in designing, building and outfitting of their cruise ships. Information technology is involved in every level of shipbuilding, from designing to logistics to customer relations [3].

3.1 Physical Environment

The following sections describe the sites, their amount of users, and their identifiers. Every site is connected via a MPLS network. The site vary in size and in location. Their Identifiers and user amounts are listed in Table 1.

Table 1. List of sites and their user amounts.

Name	User amount
Site A	300
Site B	100
Site C	100
Site D	50
Site E	30
Site F	40

3.2 Network Topology

On the top-level of the network topology, all of the sites are interconnected via Multi-Protocol Layer Switching (MPLS) network. Each site is connected to the MPLS by having a Customer Edge

(CE) router connect to the Provider Edge (PE) router which acts as the Label Edge Router (LER), which is the gateway to the MPLS network. The firewall sits on the top of the topology, acting as the gateway for public internet services, as illustrated in Figure 3.

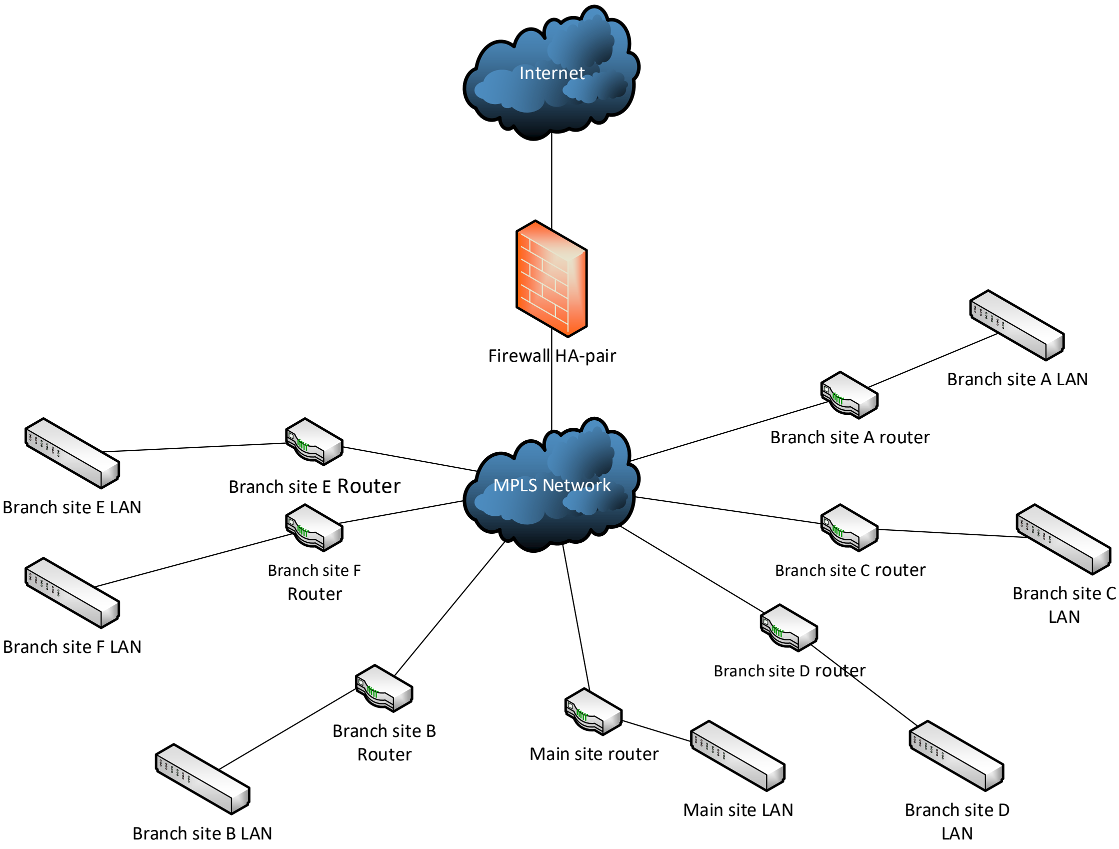


Figure 3. Topology of sites.

3.3 Network Devices

This section describes network devices and servers that are present in the topology, and which require configuration in order for FlexConnect to function in local switching, central authentication mode.

3.3.1 Routers and Uplink Connections

Main site’s Wide Area Network (WAN) device is a Huawei AR2200 series [4].

Branch sites are equipped with Cisco ME3400 series layer 3 switches. Layer 3 refers to the OSI model layer 3, the network layer. The switches are thus capable of routing [5]. Each site has the network connection speed adjusted to their use and user count.

3.3.2 Switches

Meyer Turku’s distribution and access switches consists of Cisco Catalyst series switches.

3.3.3 Wireless Controller

The Wireless controller (WLC) for all Meyer Turku’s locations is a Cisco 5500 series Wireless Controller, located at the main site. While other types of network devices work in a HA pair that is based in a common protocol, such as the VRRP or HSRP protocol, no information can be found regarding the protocol Cisco WLC uses for HA.

3.3.4 Access Points

For office use access points, Cisco Aironet series access points are used. Both indoor and external installation versions can be found. Out of the box, these access points are dependant of the WLC, as they require a wireless controller to authenticate the end user and to do the switching. Aironet series access points use Control And Provisioning of Wireless Access Points (CAPWAP) protocol to communicate with the WLC.

Access point operation modes

Cisco Aironet series access points can work in a multitude of different modes. The default one is the local mode, where the AP creates a CAPWAP-tunnel to the WLC and forwards all traffic for the WLC. In this mode, AP is entirely dependant of its connection to the WLC.

In FlexConnect mode, the authentication and management data is sent to the WLC, where as user data is switched locally by the AP. Since the switching is done at the access point, a temporary loss of connection to the WLC will not cause a connection distruption to the end users connected to a FlexConnect-enabled wireless network via an access point that is in FlexConnect mode.

In monitor mode, the access points starts monitoring wireless channels its' radios allow it to listen for, providing information on traffic, rogue devices and channel overlap. Every aironet-series access point monitors the wireless channels, but only temporarily. In monitor mode, the access point is dedicated for the monitor duty.

Sniffer mode dedicates an access point to create packet capture from the wireless clients in its' vicinity. This data can then be analyzed in tools such as Airopeek or Wireshark. In order to configure an access point to sniffer mode, the AP needs to be booted to sniffer mode from the WLC, assign it a channel to sniff and provide it a server to which the captured data will be sent.

Service Set Identifiers

Service Set Identifier (SSID) is the name of the wireless network and has the length limit of 32 octets, but it is usually displayed in human-readable format [6]. To connect to a wireless network, the access point must either broadcast the SSID beacon, or the end device needs to be configured with the said SSID.

Office_SSID is the office WLAN, with access to the most of the internal services.

3.3.5 Firewall

Palo Alto PA-5000 series firewall (FW) is used as the main firewall for outbound connections.The firewall is located in located in Finland in service provider's datacenter. Palo Alto firewalls are Next-Generation Firewalls (NGFWs), meaning that on top of traditional firewall security policy - based access control they are also capable of inspecting the packet data, detecting used applications and can provide Intrusion Prevention System (IPS) services [7]. The functions of this FW is to act as the gateway for various VRF tables present in the network.

3.3.6 Dynamic Host Configuration Protocol Server

Dynamic Host Configuration Protocol (DHCP) services for Meyer Turku are run on a dedicated server. During the prestudy, a bug was discovered, related to the compatibility of Microsoft DHCP server and Cisco products, that caused IP conflicts within DHCP leases, which rendered addresses unusable and changes the value of the lease to “BAD_ADDRESS”, dropping it from the pool of valid addresses. Cisco has issued a workaround fix to this issue [8].

3.4 Network Protocols

The following chapter describes protocols that create the Meyer Turku IP Network.

3.4.1 Virtual Local Area Network

Virtual Local Area Network (VLAN) is a technology that allows running multiple separate Local Area Networks (LANs) simultaneously using the same network switches. VLANs are used to separate different types of end devices from each other and to decrease the size of broadcast domains [9].

Meyer Turku’s network uses VLAN to separate different types of end devices from each other, as well as to limit the broadcast domain sizes. Table 1 describes the relevant VLANs to the implementation.

Table 2. Description of VLANs.

Name	VLAN ID	Usage
Management	999	Management
Office LAN	100	Office LAN
Flex_Office_SSID	120	Office flexconnect WLAN

3.4.2 First-Hop Redundancy Protocols

Every site that has two routers is running a First-hop redundancy protocol (FHRP). FHRP is used to create a virtual default gateway for a LAN network. Two participating physical routers are assigned a priority value, in which the higher priority acts as the primary router, and the lower priority acts as the backup router.

When a router is acting as the active router in FHRP, all traffic is forwarded to the virtual gateway address, but routed through the active router. In the event of a equipment failure in the active router, or a fault in internet service provider's network, FHRP switches the active router to the backup router. The traffic is still forwarded to the virtual gateway address, but the routing process is done by the backup router [10].

FHRP is an umbrella term used to describe multitude of similar protocols. In Meyer Turku's environment, two FHRP protocols are used. These are the industry standard Request for Comment (RFC) 2338 - based Virtual Router Redundancy Protocol (VRRP) and the Cisco proprietary Hot-Standby Router Protocol (HSRP), which is defined in RFC 2281 [11,12].

3.4.3 Control And Provisioning of Wireless Access Points

Control And Provisioning of Wireless Access Points (CAPWAP) is a protocol created to provide access controllers (AC), or in Cisco's catalogue, WLCs, a way to communicate with access points and provide the means for centralized access point management, authorization and policy management. CAPWAP is defined in the RFC 5415 [13]. CAPWAP is not tied to any wireless technology, thus being extremely flexible.

3.4.4 Dynamic Host Configuration Protocol

In Dynamic Host Configuration Protocol (DHCP) is a protocol used to transport configuration parameters from a server to end devices. These parameters are called options. Most common uses of DHCP are to provide end devices a leased IP address, a default gateway, and a domain name system (DNS) server address. DHCP is defined in RFC 1531 [14]. DHCP can also be used to provide end devices vendor-specific configuration options, which are defined in RFC 1497 [15].

3.4.5 Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) is a routing technology separate from IP, published in 2001 and defined in RFC 3031 and later updated with RFCs 6178 and 6790. In traditional IP routing process, the router needs to decapsulate the IP packet to find out the destination address. After that, the router performs a route lookup for the address in its route table and tries to find the longest matching route entry. In complex networks these tasks become demanding, as these steps must be repeated on every router along the packet's route. Looking for the longest matching route entry is also demanding for the Central Processing Unit (CPU) of the router.

In MPLS, the first Label Switch Router (LSR), also known as Label Edge Router (LER), which usually is the Provider Edge (PE) router, takes a packet from the Customer Edge (CE) router, decapsulates it, and checks the destination address. After this, a route lookup is made on the Forwarding Information Base (FIB), and a correspondingly on the Label Forwarding Information Base table (LFIB). Each LSR has a LFIB table. In this table, there are four columns; inbound label, inbound interface, outbound label, and outbound interface. From these entries the LSR picks the exact match. LSR then adds two headers to the packet; the source label, which is the LSR's own label, and the destination label, which is the label of the destination LER. After this, the first LSR sends the packet forward (using the outbound interface listed in the label table) to the second LSR. The second LSR inspects the label headers, replaces the source label (this is called label popping) with its own label number, and forwards the packet to the next router according to its LFIB table. This process is repeated until the packet reaches the destination LER. The destination LER then takes the packet, strips it from the label headers, decapsulates the packet, and routes the packet according to the underlying routing protocol [16].

MPLS works with multiple underlying protocols; the packet in the example could have been a TCP, Frame Relay, or a Digital Subscriber Line (DSL) packet. Since the packet is decapsulated only at the LERs, and since label lookup is only looking for exact matches, compared to IP route lookup where we are trying to find the longest match, the process is lighter on the CPUs of the participating routers. Initially the paths LSRs took, known as Label Switch Paths (LSP), across the MPLS network were static; with the introduction of Label Distribution Protocol (LDP) and Resource Reserve Protocol (RSVP) these could become dynamic. In the case of a equipment fault, these protocols could switch to another path in 50 milliseconds [16].

In Meyer Turku’s environment, each site is interconnected via MPLS network. Every CE router is connected to a PE router acting as a LER. Meyer Turku is also connected to other corporate locations in Germany. Before the traffic enters the MPLS network, it is routed according to a Virtual Routing and Forwarding (VRF) table.

3.4.6 Border Gateway Protocol

Border Gateway Protocol (BGP) is a path vector – based routing protocol. The first version of BGP, named BGP-1, saw its inception in 1989, and has since been updated multiple times. The latest version of BGP is BGP-4, which has been in use since 1994, is defined in RFC-4271.

BGP is commonly used as an exterior protocol, meaning it is meant to share routes provided by an interior protocol to other BGP routers. BGP is also the backbone protocol to most of the internet [17].

3.4.7 Virtual Routing and Forwarding Table

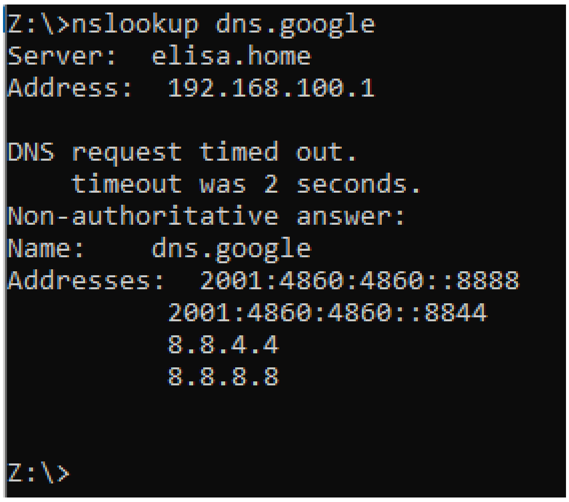
Virtual Routing and Forwarding Table (VRF) is a method of virtualizing the routing table of a router, and allowing running multiple routing tables separate from each other. VRFs can be considered to be the in similar position in OSI layer 3 as VLANs are on layer 2 [18].

Meyer Turku network environment runs multiple VRFs for separate types of traffic. For the context of this implementation, we are only working with the VRF intended for office use.

3.4.8 Domain Name System

Domain Name System (DNS) is a system to translate IP addresses to human readable format. Without DNS services available, only way to reach internet services would be to access them by their IP addresses [19]. DNS servers can be deployed in both public and private setting. In a private setting, the DNS servers can, for example, hold company’s own internal services’ DNS entries. In a public setting, DNS can provide the user with public internet services’ domain names. An example of a DNS lookup can be seen in Picture 1.

In Meyer Turku's environment, a public DNS server is provided by a service provider. The DNS server addresses are provided to the user by DHCP option 006.



```
Z:\>nslookup dns.google
Server:  elisa.home
Address:  192.168.100.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    dns.google
Addresses:  2001:4860:4860::8888
          2001:4860:4860::8844
          8.8.4.4
          8.8.8.8


Z:\>
```

Picture 1. An example of DNS lookup from the Windows' command prompt.

3.5 Requirements for Solution

In traditional controller-based wireless environment, all traffic from a wireless client is routed and switched through the WLC. When the userbase grows, so does the traffic that is passing the WLC. Also, when the client traffic is routed and switched through the WLC, unnecessary routing is created. Client traffic from e.g. Rauma, Finland, would in Meyer Turku's case first be tunneled to the WLC, before being routed to the proper destination. In order to improve client user experience and to reduce the traffic load on the WLC, a solution must be found that enables an AP to switch packets locally.

3.6 Alternatives to chosen solution

Similar technologies that enable controller-dependant APs to perform local switching can be found from other manufacturers' catalogs as well. This subchapter aims to describe them and their differences to FlexConnect.

3.6.1 Juniper Networks Local Switching

Juniper Networks Local Switching is Juniper Networks' equivalent to FlexConnect. Local switching is included in Junos Network Director, which is Juniper's centralized management system for WLCs, and layer 2 – and 3 – switches [20].

3.6.2 Meraki VLAN Tagging Access Points

Cisco Meraki is a division of Cisco, focusing in cloud–based solutions. As such, the WLC of the Meraki architecture is located in cloud. This provides flexibility and mobility, as there is no need to route management network across remote sites. As the Meraki WLC is in the cloud, there is no need for user data to be tunneled to the internet. By default, Meraki APs function as locally switching APs [21].

3.6.3 Aruba Remote Acess Points and Forward Mode

Aruba's solution for locally switched WLAN consists of two concepts, remote access points and forward mode. Remote access point technology enables an Aruba AP to connect to the WLC using Extended Authentication (XAuth) and Internet Protocol Security (IPSec) protocols. This technology enables an AP to connect to the WLC over the internet, as opposed to the AP locating in the same LAN environment.

Forward mode is used to define the operation mode of the AP. When compared to default Cisco AP's centrally switched behavior, Aruba's equivalent to this is tunnel mode. In tunnel mode, all traffic is forwarded to the WLC, including management and user data. Aruba provides two modes similar to FlexConnect, bridge and split-tunnel. Bridge mode enables the AP to work independent of the controller, bridging the WLAN to the LAN. Central authentication via the WLC is thus unavailable. In Split-tunnel mode, the traffic that is centrally switched is configured separately on the controller. Central authentication can thus be configured [22].

4 IMPLEMENTATION

As network access can be considered to be a critical part of any modern organisation, the implementation was applied so that the interruptions in connections for the end users during the process were minimal. Most of the changes, such as new subnet routing, DHCP and firewall configurations, did not cause any interruptions in client connectivity. However, switch configuration changes as well as some of the WLC configurations will cause APs to reboot, resulting in downtime for wireless access. Changes that were known to cause connectivity downtime were implemented outside business hours during preannounced and premeditated service windows.

4.1 Introducing New Networks

The implementation is started by ordering new subnets to the MPLS network. Separate networks are to be created per Service Set Identifier (SSID) and per site. Although only Office SSID is given new networks, this design decision allows the scaling of FlexConnect implementation to other SSIDs in future. Another design decision was to provide each site with enough addresses so that every employee could use WLAN simultaneously. Networks were created using Variable-Length Subnet Mask (VLSM) - subnetting. The subnetting is listed in Table 3.

Table 3. New subnets for meyNET.

Network	VLAN	Branch site	Router
192.168.100.0/23	120	A	Router-CE-Branch_A
192.168.102.0/24	120	D	Router-CE-Branch_D
192.168.103.0/25	120	C	Router-CE-Branch_C

Table 3 (continue).

192.168.103.128/25	120	B	Router-CE-Branch-B
192.168.104.0/26	120	E	Router-CE-Branch-E
192.168.104.64/26	120	F	Router-CE-Branch_F

4.2 DHCP Configurations

Each router subinterface is given helper addresses to the DHCP server, which provides the subnet with DHCP services. By giving each subinterface the helper address, host devices connected to the AP can now look for an IPv4 address by using Dynamic Host Configuration Protocol (DHCP). This is done by defining a DHCP scope. DHCP scope includes the address pool and scope options. Address pool is a subnet from which DHCP server leases end devices with an unique IP. With scope options DHCP is able to provide the end device additional information, such as DNS server address. DHCP scopes and their attributes are depicted in Table 4. In DHCP option 003 the default gateway is defined per DHCP scope. These are listed in Table 5.

Table 4. DHCP scope names and address pools.

Description	Scope start IP	Scope end IP	Info
Flex-Office-Site_A	192.168.100.1	192.168.101.254	Exclude 192.168.100.1
Flex-Office-Site_B	192.168.102.1	192.168.102.254	Exc.ude 192.168.102.1
Flex-Office-Site_C	192.168.103.1	192.168.103.127	Exclude 192.168.103.1
Flex-Office-Site_D	192.168.103.129	192.168.103.254	Exclude 192.168.103.129
Flex-Office-Site_E	192.168.104.1	192.168.104.64	Exclude 192.168.104.1

Table 4 (continue).

Flex-Office-Site_F	192.168.104.65	192.168.104.127	Exclude 192.168.104.65

Table 5. Default gateway option per DHCP scope.

Scope	Option 003 value
Flex-Office-Site_A	192.168.100.1
Flex-Office-Site_B	192.168.102.1
Flex-Office-Site_C	192.168.103.1
Flex-Office-Site_D	192.168.103.129
Flex-Office-Site_E	192.168.104.1
Flex-Office-Site_F	192.168.104.65

4.3 Firewall Configurations

The firewall is configured with static routes towards the office VRF. An address object is created for each branch site subnet. These are described in Table 6 and Table 7.

Table 6. Firewall router static routes for meyNET networks.

Destination	Interface
192.168.100.0net23_SiteA	Towards office VRF
192.168.102.0net24_SiteB	Towards office VRF
192.168.103.0net25_SiteC	Towards office VRF
192.168.103.128net25_SiteD	Towards office VRF
192.168.104.0net26_SiteE	Towards office VRF
192.168.104.64net26_SiteF	Towards office VRF

Table 7. Firewall address objects.

Name	Type	Address
192.168.100.0net23_SiteA	IP Netmask	192.168.100.0/23
192.168.102.0net24_SiteB	IP Netmask	192.168.102.0/24
192.168.103.0net25_SiteC	IP Netmask	192.168.103.0/25
192.168.103.128net25_SiteD	IP Netmask	192.168.103.128/25
192.168.104.0.net26_SiteE	IP Netmask	192.168.104.0/26
192.168.104.64.net26_SiteF	IP Netmask	192.168.104.64/26

4.4 Switch Configurations

When an AP is functioning in local mode, the switch configuration requires nothing more than a switchport in access mode and the access VLAN as the management VLAN. When introducing one or more FlexConnect local-switching SSIDs, The switchport needs to be able to access multiple VLANs.

The new VLANs used for the FlexConnect need to be propagated to each switch participating in the LAN. The ports that are connected to APs need to be configured to trunk mode, allowing them to carry out more than one VLAN's traffic to the neighboring device.

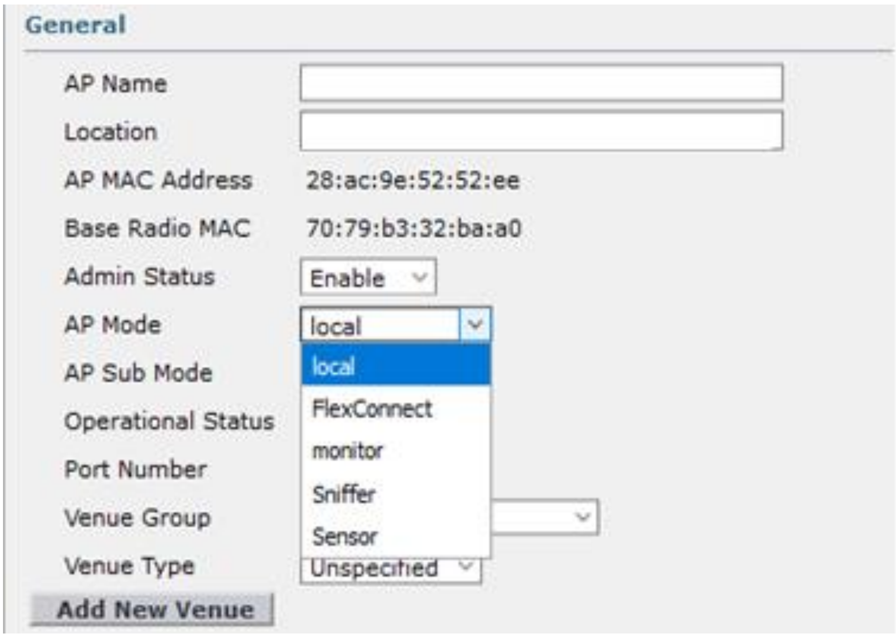
The native VLAN is set as the AP management VLAN of the LAN. The allowed VLANs on the trunk port are to be limited to the necessary VLANs, these VLANs being the management VLAN and the FlexConnect VLAN. The AP will use the native VLAN to acquire itself an IP address, as well as to communicate to the WLC. The FlexConnect VLAN is needed for the AP to be able to locally switch the FlexConnect-enabled SSIDs. Example of a port configuration is shown in Figure 4.

```
interface GigabitEthernet1/0/1
 switchport trunk native vlan 999
 switchport trunk allowed vlan 999,120
 switchport mode trunk
end
```

Figure 4. Example of switchport configuration that supports FlexConnect.

4.5 Access Point Configurations

To prepare an access point for FlexConnect, the AP needs to be set to FlexConnect mode. This can be done from the CLI of the AP or from the WLC GUI or CLI. After the mode is changed, the AP will reboot. Picture 2 shows how to change the mode from GUI.



General

AP Name

Location

AP MAC Address 28:ac:9e:52:52:ee

Base Radio MAC 70:79:b3:32:ba:a0

Admin Status Enable

AP Mode local

AP Sub Mode

Operational Status

Port Number

Venue Group

Venue Type Unspecified

Picture 2. Changing AP operating mode from WLC GUI.

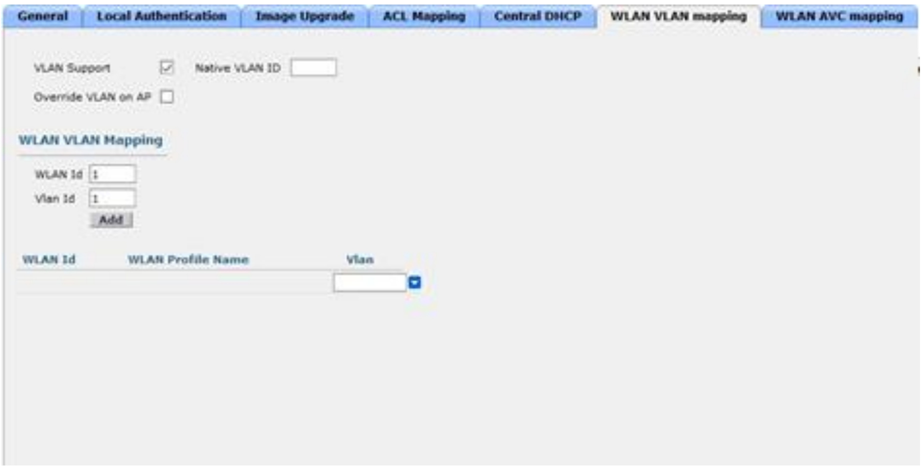
4.6 Wireless Controller Configurations

Preparing the WLC for FlexConnect starts with enabling an SSID to be locally switched. After this, a FlexConnect group will be created. There will be a FlexConnect group for each site that will have a FlexConnect-enabled SSID. FlexConnect group names are listed in Table 8, and Picture 3 shows the local-switching enabled SSID in the GUI.

Table 8. List of FlexConnect group names.

FlexConnect group name	Site
Flex-SiteA	Site A
Flex-SiteB	Site B
Flex-SiteC	Site C
Flex-SiteD	Site D
Flex-SiteE	Site E
Flex-SiteF	Site F

FlexConnect group configuration is started by enabling VLAN support and defining the native VLAN, which will be the management VLAN. WLAN-VLAN mapping will then be configured to connect a FlexConnect-enabled SSID to the VLAN that will be used for the local switching. Picture 4 shows where the VLAN-WLAN mapping is configured in the GUI.



VLAN Support ☑ Native VLAN ID

Override VLAN on AP □

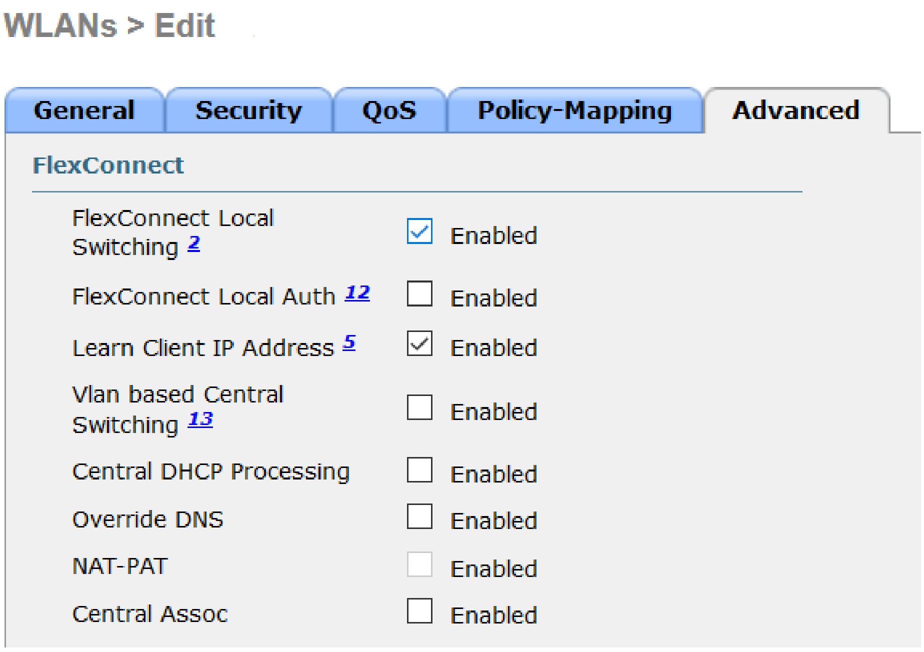
WLAN VLAN Mapping

WLAN Id 1

Vlan Id 1

WLAN Id	WLAN Profile Name	Vlan

Picture 3. Configuring WLAN-VLAN mapping on WLC GUI.



WLANs > Edit

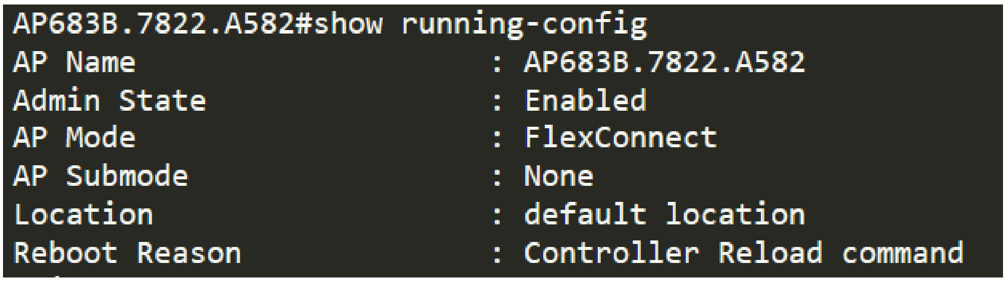
FlexConnect

FlexConnect Local Switching 2	☑ Enabled
FlexConnect Local Auth 12	□ Enabled
Learn Client IP Address 5	☑ Enabled
Vlan based Central Switching 13	□ Enabled
Central DHCP Processing	□ Enabled
Override DNS	□ Enabled
NAT-PAT	□ Enabled
Central Assoc	□ Enabled

Picture 4. Enabling SSID for local switching from WLC GUI.

Once the SSID is enabled for local switching and the WLAN-VLAN mapping is completed, the APs will be added to the FlexConnect group. These APs need to be in FlexConnect-Mode for them to be added to the group. Confirming the AP operating mode is depicted in Picture 5.

The WLAN-VLAN mapped SSIDs are now working in FlexConnect local switching mode on the APs that were configured for the FlexConnect group.



```
AP683B.7822.A582#show running-config
AP Name                         : AP683B.7822.A582
Admin State                     : Enabled
AP Mode                         : FlexConnect
AP Submode                      : None
Location                        : default location
Reboot Reason                   : Controller Reload command
```

Picture 5. Confirming AP operating mode from AP CLI.

5 RESULTS

To test the performance improvements and the to demonstrate changes in routing, route visibility, throughput and latency, tests were carried out in three phases; for the default environment with the APs in local mode, for APs in local mode with an RF profile and with FlexConnect implemented.

For the the test environment, we used Site A. Wireless network throughput was tested using LAN Speed Test version 1.3.1 by Tofusoft, and latency & routing were tested with pathping command against three targets in different locations. The latency & routing targets were two Meyer Turku servers located in different locations. In addition, latency & routing was tested against Google's public DNS.

Network throughput is tested using LAN Speed Test version 1.3.1 by Tofusoft. This software first writes and uploads a file of wanted size on to a folder of choosing, and then downloads and reads the file. The folder into which the files are written was a network drive. The tests were executed with 10MB and 100MB file sizes.

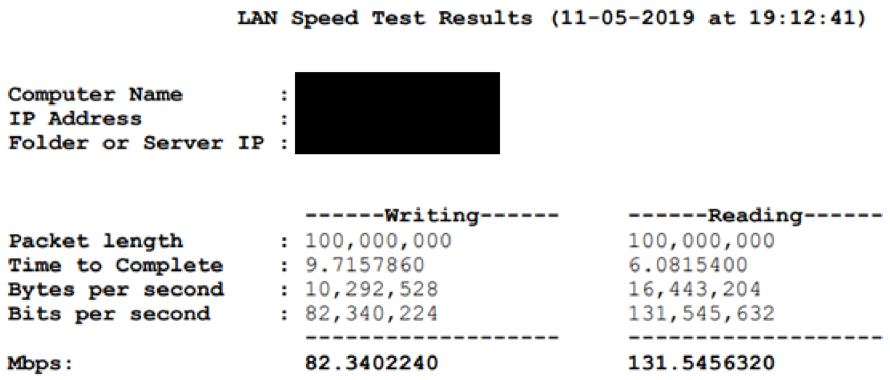
Routing tests were carried out using Windows command pathping, which provides us with information of the network hops the traffic has taken and the latency for each hop.

The test were executed on a company standard laptop running Windows 10 64-bit. The test laptop was connected to the same access point during all tests.

At the time of the tests, the wireless network had three client devices on 2,4 GHz band and 5 client devices on 5 GHz band.

5.1 Throughput tests

LAN Speed Test software provided a printable output of the results, demonstrated in Picture 6.



```
                   LAN Speed Test Results (11-05-2019 at 19:12:41)

Computer Name       : [redacted]
IP Address          :
Folder or Server IP :

                      ------Writing------       ------Reading------
Packet length       : 100,000,000               100,000,000
Time to Complete    : 9.7157860                 6.0815400
Bytes per second    : 10,292,528                16,443,204
Bits per second     : 82,340,224                131,545,632
                      -------------------       -------------------
Mbps:                 82.3402240                131.5456320
```

Picture 6. Printed output of LAN Speed Test results.

During throughput tests it was detected that the testing software had stability issues, as freezing and unresponsiveness was detected in the software, especially after a network or address change. As depicted in Figure 5, while a slight increase in download rates can be detected, this seemed to affect negatively to the upload speed. This, in addition to the detected stability issues, leads to conclusion that the software might be at fault. Another possible factor to the results is the writing speed of the network drive, as the drive is intended for mass storage.

As there were no significant changes to the throughput rates, we can deduce that centralized switching was not causing a bottleneck at the time of the testing. However, at the time of the testing the wireless network was under minimal stress. A more probable cause to the throughput rates might have been in the RF profile, where a channel bandwidth for 5GHz radios was set to 20MHz. Further testing with higher rates might provide improved performance.

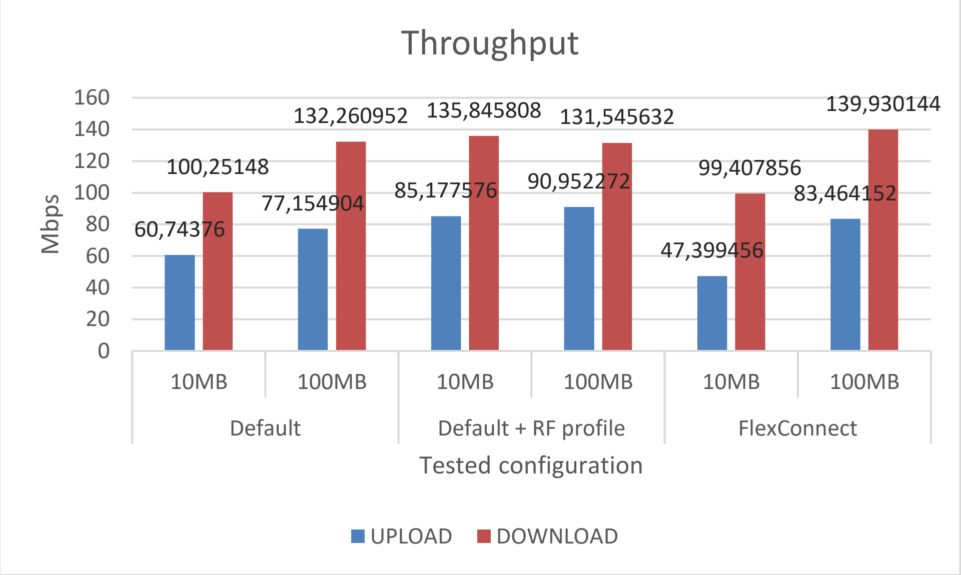


Figure 5. Throughput test results & comparison.

5.2 Routing tests

Routing tests to server 1 show similar routes in hop count, as illustrated in Table 9. In default route hop number 1 is located at the main site, in comparison to FlexConnect hop 1, which is located at Site A. In default route, the traffic first travels to the WLC, where it is routed according to the shipyard CE router. Geological difference in the routes is depicted in Figure 6.

Table 9. Comparison of routing to server 1.

Default	**Hop**	**FlexConnect**
default office subnet address	0	192.168.100.11
default office subnet gateway	1	192.168.100.1
ISP core network	2	ISP core network
DC1 FW	3	DC1 FW
DC1 LAN	4	DC1 LAN
Server 1	5	Server 1

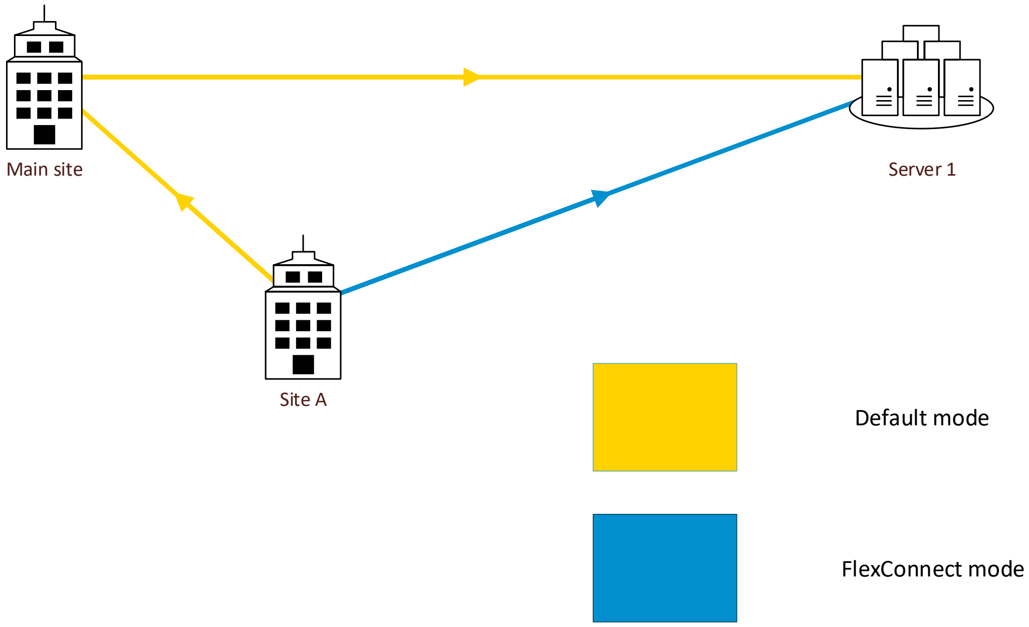


Figure 6. Geographical comparison of routing to server 1.

In the routes to server 2, depicted in Table 10, we can see a major difference. As by default user traffic is centrally switched at the WLC, for the end user the server seems to be two hops away. In FlexConnect, we receive extended visibility as the route goes through the Site A CE router, through ISP core network, and into main site CE router. Geographically there is no difference in the route, as depicted in Figure 7.

Table 10. Comparison of routing to server 2.

Default	**Hop**	**FlexConnect**
default office subnet address	0	192.168.100.11
default office subnet gateway	1	192.168.100.1
Server 2	2	ISP core network
	3	ISP core network
	4	main site CE router
	5	Server 2

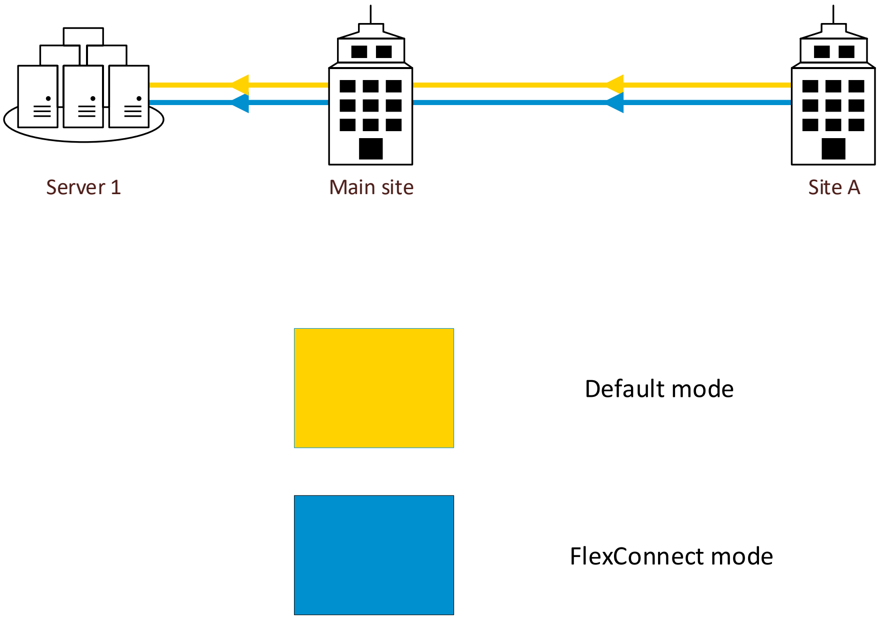


Figure 7. Geographical comparison of routing to server 2.

In route to dns.google, we can once again see the extra distance the extra distance default route takes, portrayed in Table 11 and Figure 8. After reaching hop 4, the traffic is routed to internet from the firewall.

Table 11. Comparison of routing to dns.google.

Default	Hop	FlexConnect
default office subnet address	0	192.168.100.11
default office subnet gateway	1	192.168.100.1
ISP core network	2	ISP core network
ISP core network	3	ISP core network
ISP core network	4	ISP core network
Firewall	5	Firewall
139.97.159.247	6	139.97.159.247
139.97.159.246	7	139.97.159.246
213.192.186.82	8	213.192.186.82
213.192.186.81	9	213.192.186.81
213.192.184.74	10	213.192.184.74
213.192.185.93	11	213.192.185.93
108.170.254.49	12	108.170.245.49

Table 11 (continue).

209.85.246.57	13	209.85.246.57
dns.google [8.8.8.8]	14	dns.google [8.8.8.8]

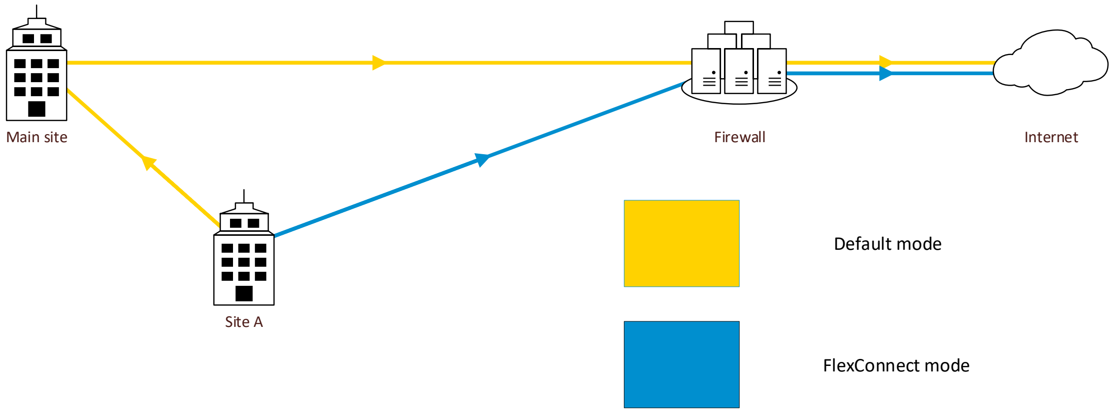


Figure 8. Geographical comparison of routing to dns.google.

5.3 Other notes

During testing it was detected that a communication application used globally across Meyer group did not function as intended when FlexConnect was in use. Final implementation was delayed until this issue was solved. No other application issues were detected during testing.

When an access point is switched to FlexConnect-mode, a level fault tolerance is achieved. As FlexConnect switching happens at the access point, already authenticated users do not lose connectivity in the event of a WLC connection failing. Already authenticated users will lose connectivity once their authentication session times out, but running FlexConnect should decrease the amount of short-term interruptions to user connectivity.

6 CONCLUSIONS

This thesis described the implementation of FlexConnect, describing necessary changes and configurations for each participating network device and server. The thesis also described alternatives to the chosen solution that provide the same functionality similar to FlexConnect on other vendors' network equipment. Due to the nature of the thesis, the majority of the source material was available online, and consisted of vendor documentation and standards based off of International Electrotechnical Commission (IEC) and Internet Engineering Taskforce's (IETF) Requests For Comments (RFC).

The implementation of FlexConnect succeeded in improving the routing by locally switching user data, and improved the performance of the wireless network by providing a throughput increase and improving the resiliency of the network in the event of a connection loss to the WLC. These results proved that there was no active bottleneck in the LAN that was affecting the throughput rate that was achieved when comparing default and FlexConnect test results. While the throughput testing methods could be improved upon, this information is enough to deduce the next course of action when improving the wireless network of Meyer Turku. While the final implementation of FlexConnect had to be delayed due to a misbehaving application, the routing test results provide enough base to implement the solution once the issue has been resolved.

The main purpose of the thesis was to implement Cisco FlexConnect to Meyer Turku Oy, and to improve their network performance. To further improve the performance of the wireless network, it is recommended to increase the 5GHz band channel bandwidth in order to rule out a possible bottleneck in the wireless network throughput.

REFERENCES

1. Annual Report Pursuant to Section 13 or 15(d) of the securities exchange act of 1943 for the fiscal year ended July 28,2012 [Internet]. Cisco Systems Inc. [cited 17.10.2019]. Available at: http://pdf.secdatabase.com/419/0001193125-12-388590.pdf

2. Cisco Wireless LAN Controller Configuration Guide, Release 7.2 - Chapter 15 - Configuring FlexConnect [Cisco Wireless LAN Controller Software] [Internet]. Cisco. Cisco; 2019 [cited 14.7.2019]. Available at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

3. Meyer. [Internet]. About the Shipyard. [cited 27.10.2019]. Available at: https://www.meyerturku.fi/en/meyerturku_com/shipyard/company/about_the_shipyard_1/about_the_shipyard.jsp

4. AR2200 Series Enterprise Routers [Internet]. Huawei. [cited 27.10.2019]. Available at: https://support.huawei.com/enterprise/en/routers/ar2200-pid-6078842/software

5. Simoneau P. The OSI Model: Understanding the Seven Layers of Computer Networks. 2006;:5. Available from: http://index-of.es/Networking/7 Layers of the OSI Model.pdf

6. ISO/IEC 8802-11: 1999 [IEEE Std 802.11-1999(R2003)] Information technology--Telecommunications and information exchange between systems-- Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

7. Miller LC. Next-generation firewalls for dummies: Hoboken, NJ: Wiley; 2011.

8. CSCuv61271 [Internet]. Cisco. [cited 5.10.2019]. Available at: http://www.cisco.com/c/en/us/applicat/camp/BugSearchTool_Layout.html

9. Overview of VLANs (Virtual LANs) [Internet]. Allied Telesis; 2008 [cited 27.10.2019]. Available at: https://www.alliedtelesis.com/sites/default/files/documents/how-alliedware/overview_vlans.pdf

10. Gokhan K. First Hop Redundancy Protocols [Internet]. https://ipcisco.com/. 2019 [cited 30.10.2019]. Available at: https://ipcisco.com/lesson/first-hop-redundancy-protocols/

11. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 [Internet]. IETF Tools. 2010 [cited 30.10.2019]. Available at: https://tools.ietf.org/html/rfc5798

12. Cisco Hot Standby Router Protocol (HSRP) [Internet]. IETF Tools. 1998 [cited 30.10.2019]. Available at: https://tools.ietf.org/html/rfc2281

13. Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification [Internet]. IETF Tools. 2009 [cited 30.10.2019]. Available at: https://tools.ietf.org/html/rfc5415

14. Dynamic Host Configuration Protocol [Internet]. IETF Tools. 1993 [cited 5.11.2019]. Available at: https://tools.ietf.org/html/rfc1531

15. DHCP Options and BOOTP Vendor Extensions [Internet]. IETF Tools. 1997 [cited 5.11.2019]. Available at: https://tools.ietf.org/html/rfc2132

16. De Ghein, L. (2007). MPLS Fundamentals. Indianapolis: Cisco Press. Pages 5 – 40, 291.

17. Pepelnjak I. 5 essential reasons for BGP in your IP network [Internet]. SearchNetworking. [cited 5.11.2019]. Available at: https://searchnetworking.techtarget.com/tip/5-essential-reasons-for-BGP-in-your-IP-network

18. VRF Basics [Internet]. Ipwithease. 2016 [cited 5.11.2019]. Available at: https://ipwithease.com/vrf-basics/

19. Domain names – implementation and specification [Internet]. IETF Tools. 1987 [cited 5.11.2019]. Available at: https://www.ietf.org/rfc/rfc1035.txt

20. Network Director User Guide [Internet]. Juniper Networks. [cited 27.10.2019]. Available at: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/information-products/pathway-pages/network-director-pwp.html.

21. Meraki Cloud Architecture [Internet]. Cisco Meraki. 2019 [cited 27.10.2019]. Available at: https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Meraki_Cloud_Architecture

22. 6.3.x [Internet]. Airheads Community. [cited 27.10.2019]. Available at: https://community.arubanetworks.com/t5/6-3-x/ct-p