TecnoCampus
Escola Superior
Politècnica

Centre adscrit a la
upf. Universitat Pompeu Fabra Barcelona

Grau en Enginyeria Informàtica de Gestió i Sistemes d'Informació

DESIGN AND CONFIGURATION OF A NETWORK INFRASTRUCTURE FOR VIDEOGAME EVENTS

Memòria

Pere Castillo Japón

TUTOR: Léonard Janer

Curs 2017-2018

TecnoCampus
Mataró-Maresme

Agraïments

Vull donar les gràcies a totes les persones que han fet aquest treball possible. Al meu tutor, Léonard, per tota la ajuda que m'ha donat al llarg del desenvolupament del projecte, totes les hores que m'ha ajudat a resoldre dubtes i preguntes. A la gent de SIRT, que gràcies a ells he entès molts conceptes tècnics i descobert tecnologies que m'han permès portar a terme aquest treball. I especialment a la meva família, per tot el suport emocional que m'han donat al llarg d'aquest curs. Moltes gràcies a tots.

Abstract

The development of this project is based on the theoretical study of the state of the art in network configurations for the videogame industry and a suggestion of a case for its study and proposal and argument of multiple solutions given the case's needs. In our case we will provide configuration solutions based on Cisco network infrastructures and following Best practices established by this manufacturer.

Resum

La realització d'aquest projecte es basa en l'estudi teòric de l'estat de l'art en configuracions de xarxa útils pel món dels videojocs i la proposta d'un cas pràctic pel seu estudi i la presentació i argumentació de diverses solucions donades les necessitats d'aquest. En el nostre cas es proporcionen solucions de configuració de fabricant Cisco seguint les *Best practices* establertes per aquest.

Resumen

La realización de este proyecto se basa en el estudio teórico del estado del arte en configuraciones de red útiles para el mundo de los videojuegos, la propuesta de un caso práctico para su estudio i presentación i argumentación de diversas soluciones dadas las necesidades de este. En nuestro caso se proporcionan soluciones de configuración de fabricante Cisco siguiendo las *Best practices* establecidas por este.

Index

Figure Index

Table Index

1. Object of the project

This project defines the bases needed to configure a network for videogame events and to help everyone who wants to organize a videogame event assuring to take into account key facts such as low latency and high availability and helps to prioritize what features are the most important for non-massive local videogame events.

The idea of this project was chosen due to the exponential growth of the videogame industry and its own market space apart from personal preference for network configurations and videogames.

2. State of the art

2.1. Events

2.1.1. Introduction

Along this year, numerous sports, videogames, technology, television, music and film related events took place.

The focus of this project will be those technology and videogame related events such as *Mobile World Congress*, *Barcelona Games World*, *Gamergy*, *Electronic Entertainment Expo*, *DreamHack*, *Gamescom* or *Euskal Encounter*.

However, before digging into these precise events we need to establish the bases and general information about how they are distributed and what are their current network needs.

2.1.2. Zones

2.1.2.1. What are Zones?

Cambridge English definition of **zone**:

An area, especially one that is different from the areas around it because it has different characteristics or is used for different purposes.

2.1.2.2. Types of Zones

Zones are classified by the number of functionalities they offer. There are two types:

- Single functionality zones: Those zones that only fulfil a single functionality to solve a single need and give only one specific service.
- Joint functionality zones: Those zones that fulfil multiple functionalities to solve more than one need or give more than one specific service.

Joint functionality zones can be composed of multiple single functionality zones.

A par from the number of functionalities classification, each one can be divided depending on the functionality they fulfil.

The single functionality zone types that exist are the following ones:

- Stands
    - Cambridge English definition of **stand**:
        - *"a small shop or stall or an area where products can be shown, usually outside or in a large public building, at which people can buy things or get information*"
- Stages
    - Modified definition from Cambridge English definition of **stage**:
        - *"the area in a theatre or space that is often raised above ground level and on which actors or entertainers perform"*
- User-interaction zones
    - Custom definition of **user-interaction zone**:

        - *"zone with devices prepared to offer or to let visitors test a functionality"*
- Shops
    - Cambridge English definition of **shop**:
        - *"a place where you can buy goods or services"*
- Rest zones
    - Custom **rest zone** definition:
        - *"zone for the visitors and/or the speakers to rest and disconnect from their surroundings momentarily"*

Joint functionality zone types that exist are the following ones:

- VIP zones
    - Custom **VIP zone** definition:
        - *"zone for speakers and those visitors who acquired a higher quality entrance, where they can enjoy the functionalities of the single functionality zones with higher quality"*
- Press zones
    - Custom **Press zone** definition:
        - *"zone specially designed to fulfil the needs of the press visitors"*

2.1.2.3. Zone types and network needs

The needs that each zone requires depend of its classification. Given the previously done classification the needs for each type of single and joint functionality zone are the following ones.

Stands:

- They require a filtered connectivity for the offers exposition devices to make sure no external device, apart from the ones related to the stand and the maintenance devices, can access the inner network.
- In case there is billing, they require a secured connection for the ATM.
- They require an access point for the visitors’ Wi-Fi network.
- Electric supply non- accessible to visitors that will grant electricity to the network and the stand devices.

Stages:

- They require a filtered or isolated connectivity for the stage devices with the corresponding display screens to make sure no external device apart from the maintenance one and the ones related to the stage can access that inner network.
- A high availability and low latency architecture to prevent the stage expositions interruptions.
- Grandstands with Wi-Fi connectivity to the visitors’ generic Wi-Fi network.
- Electric supply for the stage devices non-accessible to visitors.

User-interaction zones:

- They require connectivity for the devices available to the public depending on their applications and features needed to run those applications.
- Network securitization to not allow the devices from this zone to access other inner networks however, allowing them to access the internet if needed.
- Wi-Fi connectivity to the visitors’ generic network.
- Electric supply for the devices not accessible to visitors.

Shops:

- They require a filtered connectivity for the shop devices to make sure no external device, apart from the ones related to the shop and the maintenance devices, can access the inner network.
- Secure connectivity for the store ATMs.
- Wi-Fi connectivity to the visitors' generic network.
- Electric supply non-accessible to visitors.

Rest zones:

- They require Wi-Fi connectivity to the visitors' generic network.
- An Ethernet connection area for a *Bring Your Own Device* area.
- Display connections.
- Electric supply accessible to visitors.

Press zones:

- They require a higher speed connection network to let the press members publish or share their articles soon.
- Filtered connectivity for the *Bring Your Own Device* area to make sure no non-authorized device accesses the inner network and to not let the devices from this network access the other inner networks.
- Electric supply accessible to the press members.

Due to the fact that VIP zones are joint functionality zones, their network needs are different depending on the functionalities that are assigned to them. However, they must offer a higher quality version of the requirement fulfilment.

2.1.3. Previously organized events

2.1.3.1. Gamergy

Gamergy is the most important Spanish videogame event. Organized by *Liga de Videojuegos Profesional*(LVP) and *Institución Ferial de Madrid*(IFEMA). It contains the most relevant amateur and professional videogame competitions from Spain. It takes place in Madrid at the IFEMA Fair from December the 16th until December the 18th 2017.

The major company in the network configuration process is the Spanish internet service provider Orange.

In Gamergy's latest edition the number of participants reached the 32000 number of attendants and the 320000 number of on-line viewers. (1)

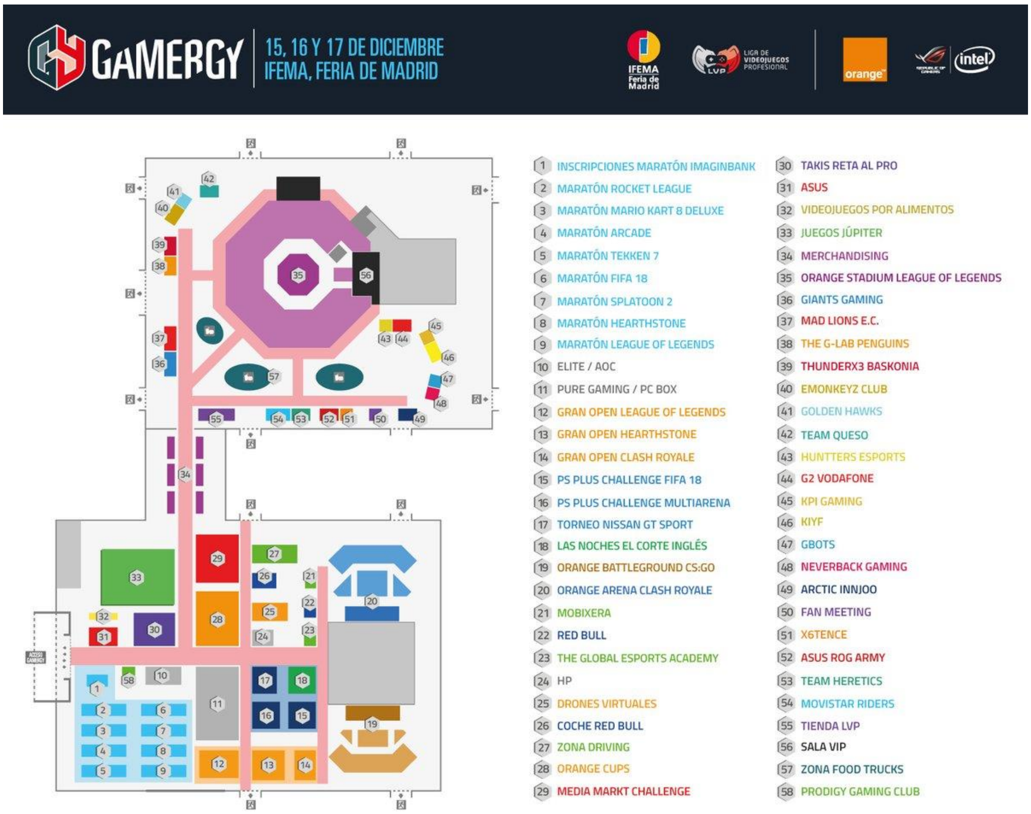


Figure 1: Gamergy activity map

As shown in Figure 1 there are lots of activities and zones offered by the event organization. However, they can be divided in fewer more descriptive groups.

The grouped activities and zones are the following from which we could describe some of their technological needs:

- Videogame professional and amateur competitions. (VoIP communication for team competitions, Low latency, High availability).
- Videogame challenges. (VoIP communication for team games, low latency).
- Food establishments (zone described as Shop with its needs).
- Thematic zones to try videogames and get merchandise from that videogame. (VoIP communication for team games, high availability, low latency)(Zones described as Stands and user-interaction zones).
- IT shops. (Zones described as Stands and Shops).

- Fan meeting zones. (User-interaction zones).
- VIP zone. (Zone described previously).

2.1.3.2. Barcelona Games World

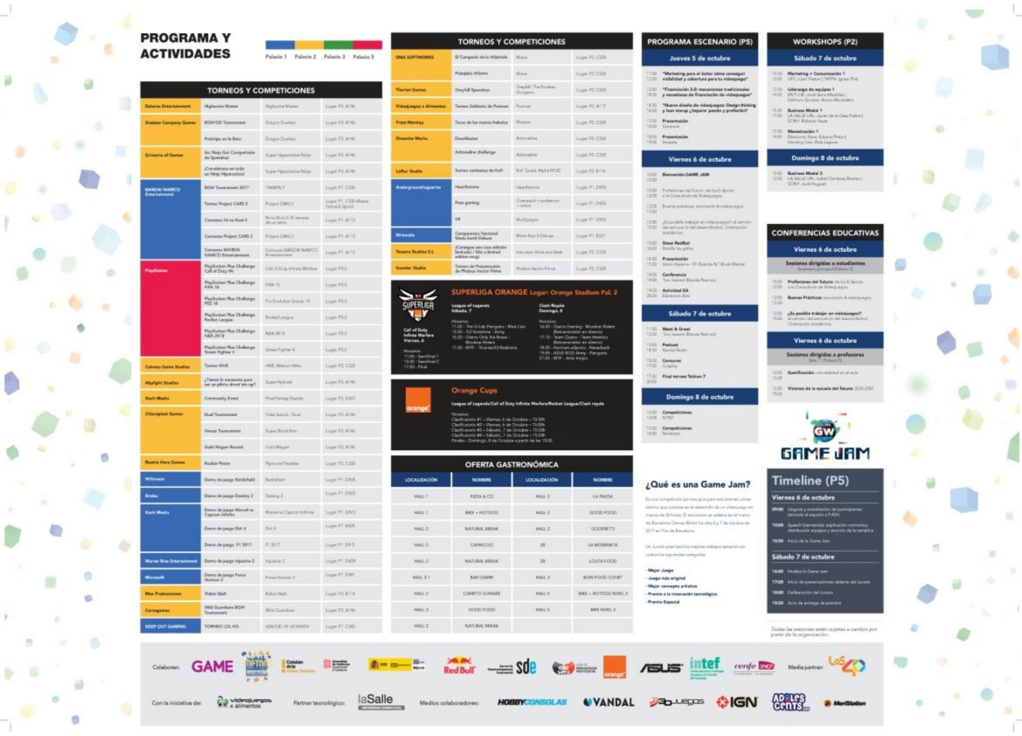
Barcelona Games World is a videogame and e-Sports event that serves as an exhibitor for videogame developing industries, as a place to have fun for visitors that want to play videogames or watch people play videogames, as a place for professional e-Sports players to show off their skills and as a rally point for people who love retro videogames.

Barcelona Games World takes place in Barcelona at Barcelona's Fair between Montjuïc and Gran Via from October the 5th until October the 8th 2017.

The major company in the network configuration process is the Spanish internet service provider Orange.

In Barcelona Games World latest edition the number of attendants reached the 135000, without taking into account the number of videogame developer industries which reach the 210 exhibitor companies.

It made available more than 1500 devices for the attendants to try upcoming videogames or play those who they wanted. (2)



PROGRAMA Y ACTIVIDADES

Palacio 1 Palacio 2 Palacio 3 Palacio 5

TORNEOS Y COMPETICIONES

Deleres Entertainment	Highscore Master	Highscore Master	Lugar P2. A146
Shadow Company Games	BGW DD Tournament	Dragon Duelists	Lugar P2. A146
	Participa en la Beta	Dragon Duelists	Lugar P2. A146
Grimorio of Games	Go Ninja Go! Competición de Speedrun	Super Hyperactive Ninja	Lugar P2. A146
	¡Conviértete en todo un Ninja Hiperactivo!	Super Hyperactive Ninja	Lugar P2. A146
BANDAI NAMCO Entertainment	BGW Tournament 2017	TEKKEN 7	Lugar P1. C330
	Torneo Project CARS 2	Project CARS 2	Lugar P1. C330 (Arena Game E-Sport)
	Concurso Ni no Kuni II	Ni no Kuni II: El renacer de un reino	Lugar P1. A110
	Concurso Project CARS 2	Project CARS 2	Lugar P1. A110
	Concurso BANDAI NAMCO Entertainment	Concurso BANDAI NAMCO Entertainment	Lugar P1. A110
PlayStation	PlayStation Plus Challenge Call of Duty IW	Call of Duty Infinite Warfare	Lugar P5.0
	PlayStation Plus Challenge FIFA 18	FIFA 18	Lugar P5.0
	PlayStation Plus Challenge PES 18	Pro Evolution Soccer 18	Lugar P5.0
	PlayStation Plus Challenge Rocket League	Rocket League	Lugar P5.0
	PlayStation Plus Challenge NBA 2K18	NBA 2K18	Lugar P5.0
	PlayStation Plus Challenge Street Fighter V	Street Fighter V	Lugar P5.0
Catness Game Studios	Torneo HIVE	HIVE: Altenum Wars	Lugar P2. C328
Abylight Studios	¿Tienes lo necesario para ser un piloto shoot 'em up?	Super Hydorah	Lugar P2. A146
Koch Media	Community Event	Final Fantasy Dissidia	Lugar P2. D407
Chloroplast Games	Duel Tournament	Yokai Sword - Duel	Lugar P2. A146
	Versus Tournament	Super Block Rain	Lugar P2. A146
	Gold Wagon Record	Gold Wagon	Lugar P2. A146
Rookie Hero Games	Rookie Pirate	Flynn and Freckles	Lugar P2. C328
Wilkinson	Demo de juego Battlefield	Battlefield	Lugar P1. D435
Bindea	Demo de juego Destiny 2	Destiny 2	Lugar P1. D425
Koch Media	Demo de juego Marvel vs Capcom Infinite	Marvel vs Capcom Infinite	Lugar P1. D423
	Demo de juego Dirt 4	Dirt 4	Lugar P1. E425
	Demo de juego F1 2017	F1 2017	Lugar P1. E415
Warner Bros Entertainment	Demo de juego Injustice 2	Injustice 2	Lugar P1. D439
Microsoft	Demo de juego Forza Horizon 3	Forza Horizon 3	Lugar P1. D441
Moe Producciones	Robot Slash	Robot Slash	Lugar P2. B116
Corsegames	Wild Guardians BGW Tournament	Wild Guardians	Lugar P2. A146
KEEP OUT GAMING	TORNEO LOL KO	LEAGUE OF LEGENDS	Lugar P1. C340

TORNEOS Y COMPETICIONES

DNA SOFTWORKS	El Campeón de la Atlántida	Khara	Lugar P2. C328
	Psicojista Atlante	Khara	Lugar P2. C328
Therion Games	Greyfall Speedrun	Greyfall: The Endless Dungeon	Lugar P2. C328
Videojuegos x Alimentos	Torneo Solidario de Pacman	Pacman	Lugar P2. A117
Frost Monkey	Tazas de los monos helados	Mosaic	Lugar P2. C328
Dinamita Works	DinoMaster	Actionaline	Lugar P2. C328
	Actionaline challenge	Actionaline	Lugar P2. C328
Loftur Studio	Sorteo camisetas de Kofi	Kofi Quest: Alpha MOD	Lugar P2. B116
Anderground/ogaerías	Hearthstone	Hearthstone	Lugar P1. D400
	Free gaming	Overwatch + pokemon + varios	Lugar P1. D400
	VR	Multijuegos	Lugar P1. D400
Nintendo	Campeonato Nacional Mario Kart 8 Deluxe	Mario Kart 8 Deluxe	Lugar P1. B221
Tessera Studios S.L	¡Consigue una taza edición limitada! / Win a limited edition mug!	Intruders: Hide and Seek	Lugar P2. C328
Gunstar Studio	Torneo de Presentación de Phobos Vector Prime	Phobos Vector Prime	Lugar P2. C328

SUPERLIGA ORANGE Lugar: Orange Stadium Pal. 2

SUPERLIGA

Call of Duty Infinite Warfare Viernes, 6

Horarios:
11:00 - Semifinal 1
13:30 - Semifinal 2
17:00 - Final

League of Legends Sábado, 7

Horarios:
11:30 - The G-Lab Penguins - Mad Lion
13:30 - G2 Vodafone - Army
15:30 - Giants Only the Brave - Movistar Riders
17:30 - KIYF - ThunderX3 Baskonia

Clash Royale Domingo, 8

Horarios:
16:00 - Giants Gaming - Movistar Riders (Retransmisión en directo)
17:15 - Team Queso - Team Heretics (Retransmisión en directo)
18:30 - Huntians eSports - Neverback
19:45 - ASUS ROG Army - Penguins
21:00 - KIYF - Antz Inejos

Orange Cups

orange

League of Legends/Call of Duty Infinite Warfare/Rocket League/Clash royale

Horarios:
Clasificatorio #1 – Viernes, 6 de Octubre – 10:30h
Clasificatorio #2 – Viernes, 6 de Octubre – 15:00h
Clasificatorio #3 – Sábado, 7 de Octubre – 10:30h
Clasificatorio #4 – Sábado, 7 de Octubre – 15:00h
Finales - Domingo, 8 de Octubre a partir de las 10:00

OFERTA GASTRONÓMICA

LOCALIZACIÓN	NOMBRE	LOCALIZACIÓN	NOMBRE
HALL 1	PIZZA & CO	HALL 3	LA PAUSA
HALL 1	BIKE + HOTDOG	HALL 3	GOOD FOOD
HALL 2	NATURAL BREAK	HALL 3	GOOFRETTI
HALL 2	CAPRICCIO	28	LA MORENETA
HALL 2	NATURAL BREAK	28	LOLITA FOOD
HALL 2.1	BAR DAMM	HALL 3	BGW FOOD COURT
HALL 2	CARRITO GUIXARE	HALL 5	BIKE + HOTDOG NIVEL 2
HALL 3	GOOD FOOD	HALL 5	BIKE NIVEL 3
HALL 3	NATURAL BREAK		

PROGRAMA ESCENARIO (P5)

Jueves 5 de octubre

11:00 12:30 "Marketing para el éxito: cómo conseguir visibilidad y cobertura para tu videojuego"
12:30 14:00 "Financiación 3.0: mecanismos tradicionales y novedosos de financiación de videojuegos"
14:30 16:00 "Nuevo diseño de videojuegos: Design thinking y lean startup ¿Separar pasión y profesión?"
17:00 18:00 Presentación [illegible]
18:00 19:00 Presentación [illegible]

Viernes 6 de octubre

10:00 10:30 Bienvenida GAME JAM
10:30 12:00 Profesiones del futuro: de los E-Sports a la Consultoría de Videojuegos
12:00 13:30 Buenas prácticas: educación & videojuegos
13:30 15:00 ¿Es posible trabajar en videojuegos?: el camino del servicio [illegible] del desarrollador. Orientación académica
15:30 16:00 Show RedBull [illegible]
16:30 17:30 Presentación [illegible]
18:00 19:00 Conferencia [illegible]
19:00 20:00 Actividad EA Electronic Arts

Sábado 7 de octubre

11:30 12:30 Meet & Greet [illegible]
13:00 14:30 Podcast [illegible]
15:00 17:00 Concurso Cosplay
17:30 20:00 Final torneo Tekken 7

Domingo 8 de octubre

10:30 13:00 Competiciones SONY
13:30 16:00 Competiciones Nintendo

WORKSHOPS (P2)

Sábado 7 de octubre

10:30 12:00 Marketing + Comunicación 1 UPC [illegible] | TAPFK: Ignasi Prat
12:30 14:00 Liderazgo de equipos 1 ENTI-UB: Jordi Sanz Mobilles | Delirium Studios: Arturo Monedero
15:30 17:00 Business Model 1 LA SALLE URL: Javier de la Osa Fabra | SONY: Roberto Yeste
17:30 19:00 Monetización 1 Electronic Bliss: Eduard Pintor | Herding Cats: Rafa Laguna

Domingo 8 de octubre

10:30 12:00 Business Model 2 LA SALLE URL: Isabel Giménez Álvarez | SONY: Jordi Hugues

CONFERENCIAS EDUCATIVAS

Viernes 6 de octubre

Sesiones dirigidas a estudiantes
Escenario principal (Palacio 5)

10:30 12:00 Profesiones del futuro: de los E-Sports a la Consultoría de Videojuegos
12:00 13:30 Buenas Prácticas: educación & videojuegos
13:30 15:00 ¿Es posible trabajar en videojuegos? el camino del servicio [illegible] del desarrollador. Orientación académica

Viernes 6 de octubre

Sesiones dirigidas a profesores
Sala 1 (Palacio 5)

12:00 13:30 Gamificación: [illegible]
13:30 15:00 Visiones de la escuela del futuro: 2020-2050

GW GAME JAM

¿Qué es una Game Jam?

[illegible]

- Mejor Juego
- Juego más original
- Mejor concepto artístico
- Premio a la innovación tecnológica
- Premio Especial

Timeline (P5)

Viernes 6 de octubre

09:00 Llegada y acreditación de participantes [illegible]
10:00 Speech bienvenida: explicación normativa, distribución equipos y anuncio de la temática
10:30 Inicio de la Game Jam

Sábado 7 de octubre

16:00 Finaliza la Game Jam
17:00 Inicio de presentaciones delante del Jurado
18:00 Deliberación del Jurado
18:30 Acto de entrega de premios

Todas las sesiones están sujetas a cambio por parte de la organización.

Colaboran: GAME · Catalan Arts Video Games · Red Bull · sde · orange · ASUS · intef · renfe · Media partner: Los40

Con la iniciativa de: videojuegos x alimentos · Partner tecnológico: laSalle · Medios colaboradores: HOBBYCONSOLAS · VANDAL · 3DJuegos · IGN · Adolescents · MeriStation

Figure 2: BGW Activity list

As shown in Figure 2 there are lots of activities and zones offered by the event organization. However, they can be divided in fewer more descriptive groups.

The grouped activities and zones are the following from which we could describe some of their technological needs:

- Game Jam: Videogame development competition for university students. (Zone described as a user-interaction zone).
- Educational Conferences. (Zone described as a Stage).
- Workshops. (Zone described as a user-interaction zone).
- Food establishments. (Zone described as Shop with its needs).
- Videogame professional and amateur competitions. (VoIP communication for team competitions, high availability, low latency) (Stages for professional competitions).
- Stage Programs. (Zone described as Stage) (High availability).
- Merchandise stores. (Zone described as shop and stand).
- Game developers Conferences. (Zone described as Stage).

- Free gaming. (Public videogame devices)(Zone described as user-interaction zone)(VoIP communication for team games).
- Professional gaming stars meetings.

2.1.3.3. Euskal Encounter

Euskal Encounter is a massive meeting point for people who love information technology and professionals to exchange knowledge and do any sort of activity related to IT. (3)

Euskal Encounter takes place in Bilbao at Bilbao Exhibition Centre from July the 22nd until July the 25th 2017.

The major company in the network configuration process is the Spanish internet service provider Euskaltel.

At Euskal Encounter attendants can participate in different activities grouped as follows:

- Digital creativity:
    - Digital Art: The space for visual arts and music. A place where participants can show off their artistic skills using their computer and the latest technologies and software as a tool.
    - Demoscene: It is an IT subculture that promotes artistic expression through programming techniques.

Hardware:

- Robotics:
    - National robotics league. (Zone with devices configured to provide a comfortable programming environment)
    - Introduction to educational robotics. (Zone with devices configured to provide a comfortable programming environment)
    - Introduction to competitive robotics: Sprinters. (Zone with devices configured to provide a comfortable programming environment)
    - Introduction to competitive robotics: Minisumo. (Zone with devices configured to provide a comfortable programming environment)

- Arduino:
    - IOT Arduino UNO through the internet.(Zone with devices configured to provide a comfortable programming environment)
    - Arduino workshop.(Zone with devices configured to provide a comfortable programming environment)
    - Rubik’s Cube Structure course.
- Virtual Reality (VR):
    - VR Experience zone.(Zone with devices configured to provide a comfortable trial environment)
- 3D printing. (3D printing specific devices)
- Drones (Drone building and configuring specific devices)

Free software:

- Hack it/Solve it. (Isolated Network environment to prevent the activity from interfering with the general event network)
- Fast FoSS Game. (Game developing)
- Artificial Intelligence contest. (AI development environment)
- Smash CTF (Isolated Network environment to prevent the activity from interfering with the general event network)

Games:

- Videogame tournaments. (VoIP communication for team competitions, high availability, low latency).(Stages for professional competitions)

Conferences and workshops (Stages)

BYOD. (User-interaction zones or Rest zones)

2.2. Technology

2.2.1. Wireless

As Internet of Things (IOT) becomes a more and more accepted and developed part of the industry, the need to support connectivity from various devices to the internet through Wi-Fi becomes a must in a network solution for any problem.

Even though everyone knows about Wi-Fi, few people know how this technology works.

Wi-Fi is a radio-wave based communication technology for wireless local area networking with devices based on the IEEE 802.11 standards. It most commonly works with the 2.4 GHz and 5GHz radio bands, and each radio band is divided in channels.

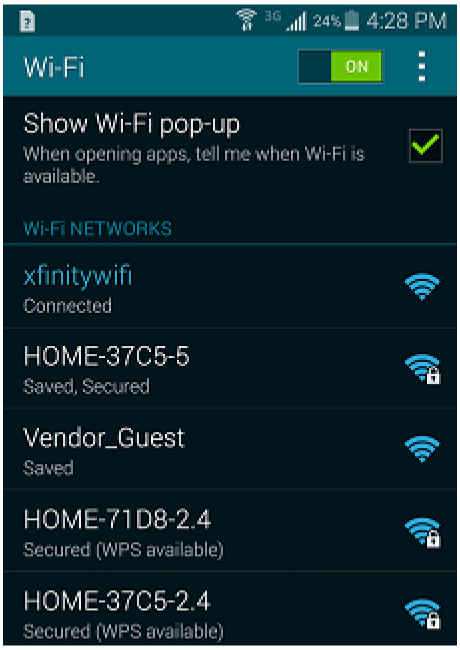
Wi-Fi connections can be disrupted or the Internet speed lowered by having multiple devices on the same area. This is caused by having those devices configured to work with the same radio band channel or the neighbour radio band channels. Other devices that work with 2.4GHz bands like microwave ovens, security cameras, ZigBee devices, Bluetooth devices and more can cause additional interference.(4)

Each Wi-Fi connection can be associated to a Service Set Identifier (SSID).

A service set is the group of all devices associated with a particular network. Therefore, a Service Set Identifier is a mechanism to distinguish each network or subnet.

Each SSID can be assigned to one or more Access Points (AP) which will spread its signal allowing people with the required security credentials to access the Internet.

Figure 3 shows a device detecting all available surrounding SSIDs that it is identifying.



Show Wi-Fi pop-up
When opening apps, tell me when Wi-Fi is available. ☑

WI-FI NETWORKS

xfinitywifi
Connected

HOME-37C5-5
Saved, Secured

Vendor_Guest
Saved

HOME-71D8-2.4
Secured (WPS available)

HOME-37C5-2.4
Secured (WPS available)

Figure 3: Device detecting available SSIDs

2.2.1.1. IEEE 802.11

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard.

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. 802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n, and 802.11ac. Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which may also include corrections to a previous specification.(5)

2.2.1.1.1 IEEE 802.11b and IEEE 802.11g

IEEE 802.11b-1999 or 802.11b and IEEE 802.11g-2003 or 802.11g , both are amendments to the IEEE 802.11 wireless networking specification which extend throughput to average 11 Mbit/s and 22 Mbit/s accordingly, and 802.11g also extends the throughput up to 54 Mbit/s for forward error correction codes, using the 2.4GHz band.

Both amendments are used in a point-to-multipoint configuration where an access point communicates via an omnidirectional antenna with mobile clients within the range of the access point. Allowable bandwidth is shared across clients in discrete channels.

802.11g and 802.11b work on the same channels in 2.4GHz band.

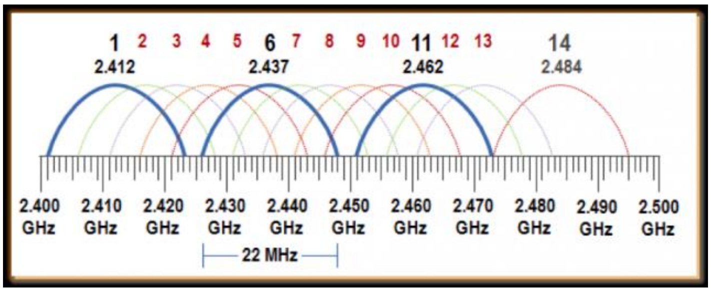
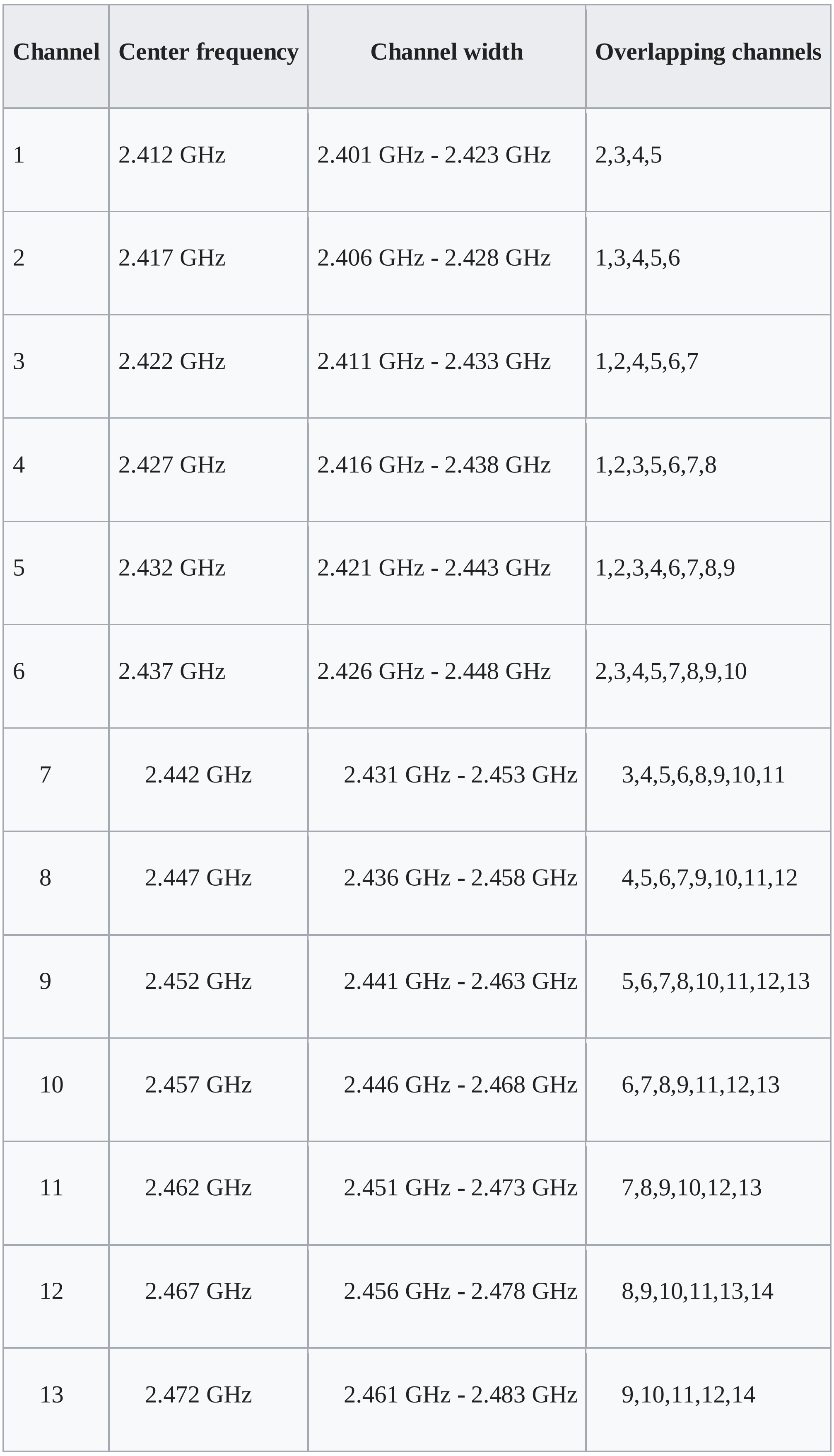


Figure 4: Channels and overlapping

They use the channels 1 to 13 and, exclusively in other countries, 14 as shown in Figure 4. However, their channel configuration cannot use channels which overlap each other because that would lead to channel interference and a major efficiency flaw.

The usable channel combination must assure that no channel is width is overlapping with another channel width. Channel widths and overlapping can be seen in Table 1.



Channel	Center frequency	Channel width	Overlapping channels
1	2.412 GHz	2.401 GHz - 2.423 GHz	2,3,4,5
2	2.417 GHz	2.406 GHz - 2.428 GHz	1,3,4,5,6
3	2.422 GHz	2.411 GHz - 2.433 GHz	1,2,4,5,6,7
4	2.427 GHz	2.416 GHz - 2.438 GHz	1,2,3,5,6,7,8
5	2.432 GHz	2.421 GHz - 2.443 GHz	1,2,3,4,6,7,8,9
6	2.437 GHz	2.426 GHz - 2.448 GHz	2,3,4,5,7,8,9,10
7	2.442 GHz	2.431 GHz - 2.453 GHz	3,4,5,6,8,9,10,11
8	2.447 GHz	2.436 GHz - 2.458 GHz	4,5,6,7,9,10,11,12
9	2.452 GHz	2.441 GHz - 2.463 GHz	5,6,7,8,10,11,12,13
10	2.457 GHz	2.446 GHz - 2.468 GHz	6,7,8,9,11,12,13
11	2.462 GHz	2.451 GHz - 2.473 GHz	7,8,9,10,12,13
12	2.467 GHz	2.456 GHz - 2.478 GHz	8,9,10,11,13,14
13	2.472 GHz	2.461 GHz - 2.483 GHz	9,10,11,12,14

14	2.484 GHz	2.473 GHz - 2.495 GHz	12,13

Table 1: Channels and bandwidths of 2.4GHz frequency

2.2.1.1.2 IEEE 802.11a, IEEE 802.11n and IEEE 802.11ac

IEEE 802.11a-1999 or IEEE 802.11a is an amendment of the IEEE 802.11 standard which defined requirements for orthogonal frequency division multiplexing (OFDM) communication system.

IEEE 802.11n-2009 or IEEE 802.11n is another amendment of the IEEE 802.11 standard which features an improve of the network throughput over the 802.11a and 802.11g amendments with an increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s with the use of four streams at a channel width of 40 MHz. It is also referred to as MIMO (Multiple Input and Multiple Output). MIMO is a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing (SDM), which spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth.

IEEE 802.11ac is yet another amendment of the IEEE 802.11 standard which provides high-throughput WLANs. The specification has multi-station throughput of at least 1 gigabit per second and single-link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by extending the air-interface concepts embraced by 802.11n: wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to eight), downlink multi-user MIMO (up to four clients), and high-density modulation (up to 256-QAM).

All three of the described amendments work on the 5GHz band, and the 802.11n can also be used in the 2.4GHz bands. When using the 5GHz bands the channels can be grouped and assigned to work with a single SSID to increase its maximum throughput.

The number of channels available for the 5GHz and 2.4GHz bands is subjected to the country legislation.

2.2.1.1.3 5G

5th generation wireless systems, also known as 5G, are in-development improved networks deploying in 2018 and later. The primary technologies of those networks include: Millimeter wave bands which work at 26, 28,38 and 60 GHz which offer performance as high as 20 Gbps but are highly susceptible of interference from the weather and humidity, Massive MIMO which have from 64 to 256 antennas which work in frequencies from 600 MHz to 6 GHz.

As an in-development technology there is not much information available for its study.

2.2.1.2. Access Points

The access points are devices in charge of spreading the signal of SSIDs. These devices, nowadays work with 2.4GHz and 5GHz frequency bands, being able to spread SSIDs assigned on channels of each frequency.

Figure 5:Cisco Aironet 1830 series

Access points can be configured to work in three different modes, autonomous also known as standalone, lightweight and mobility express.

In autonomous mode, access points are configured as self-sufficient devices which are individually managed, they are also in charge of assigning an IP address to each user that connects to an SSID and route the traffic to its assigned default gateway. With that concept in mind, the management of a network with multiple access points becomes a hard task due to having to take into consideration the different individual configurations, channels and frequencies that each access point works with for later changes which could lead to an unwanted channel overlapping or misconfigurations.

In lightweight mode, access points are not configured individually. Instead, they retrieve their configuration from a device called Wireless LAN Controller (WLC). In this mode the access points first establish a CAPWAP tunnel between the WLC and them, to be able to retrieve their assigned configuration and any configuration changes that the WLC makes to that AP.

WLC is a device which unifies all the configurations of SSIDs, frequencies, VLANs assigned to the SSIDs and assigns a configuration to each access point depending on the existing access points configuration that were previously assigned.

Having a centralized point for configuring a high number of access points makes its management easier, more cost-efficient and less time consuming than having to configure each access point individually. It also contributes to make it easier to know which configurations are defined for each access point to prevent misconfigurations or assignments of overlapping channels to access points that are close to each other.

In Mobility express mode, one of the APs of the network assumes the role of the WLC when it does not detect any WLC in that network. In this case the access point is in charge of configuring and communicating with the other APs.

Figure 5 shows a Cisco Aironet AP which can be configured in all three modes.

2.2.2. Wired

2.2.2.1. VLANs

A VLAN (Virtual Local Area Network) is a broadcast domain that is divided and isolated in a network at the Data link layer. They work by applying tags to network packets and handling these tags in networking systems creating the appearance and functionality of network traffic that is physically on a single network but acts as if split between separate networks. This way VLANS keep network applications isolated despite being connected to the same physical network.

They are also used to group hosts and devices together even if they are not directly connected to the same switch. This feature provides network segmentation which increases the scalability, security and makes the network easier to manage. It also helps manage broadcast traffic by forming multiple broadcast domains.

A common infrastructure shared across VLAN trunks can provide a measure of security with great flexibility for a comparatively low cost. Quality of service schemes can optimize traffic on trunk links for real-time (e.g. VoIP) or low-latency requirements (e.g. SAN). However, VLANs as a security solution should be implemented with great care as they can be defeated unless implemented very carefully.

2.2.2.1.1 IEEE 802.1Q

IEEE 802.1Q, often referred to as Dot1q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridgesand switches in handling such frames.

802.1Q adds a 32-bit field between the source MAC address and the EtherTypefields of the original frame. This field is divided by two sub-fields which are the Tag Protocol identifier (TPID) and the Tag Control Information (TCI).

The TPID contains a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.

The TCI contains another three sub-fields. The Priority Code Point (PCP) which maps the frame priority level, the Drop Eligible Indicator (DEI) which indicates frames eligible to be dropped when there is congestion formerly used for the Canonical Format Indicator (CFI), and VLAN Identifier (VID) which specifies the VLAN to which this frame belongs. (6)

Figure 6shows the placement of the 802.1Q header.

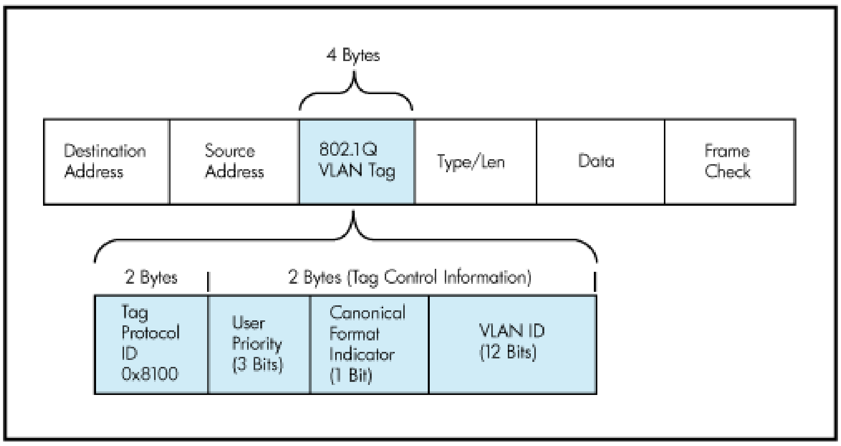


Figure 6: 802.1Q Header location

2.2.2.1.2 VLAN Routing and switching

Switches that are directly connected to a VLAN have their directly connected port in mode access and with the id of the VLAN they are connected to. When they receive traffic from that port, switches tag this traffic with the 802.1Q header and send them to another switch through a trunk mode port, in case there is only one VLAN it could be an access mode port, however, it is not recommended and it is a bad practice. When the next switch receives that traffic, it sends it to the following switch through a trunk port or to a router through another trunk port. The router interface which is the one connected to the switch that is sending traffic is divided in subinterfaces, one for each VLAN, so then the router knows from which VLAN is he receiving the traffic and to which VLAN, if the traffic's destination is another VLAN, it is going to send that traffic. The router also works as a bridge to external connectivity.

2.2.3. Security

Network security consists of policies and practices adopted to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources.

This concept starts with the Authentication Authorization and Accounting (AAA) which refers to a family of protocols which mediate network access.

2.2.3.1. Wireless threats

As a shared media, wireless is more susceptible to suffer an attack. Possible threats include, but are not limited to:

- Network sniffing to eavesdrop: Unlike Wire-based LANS, the wireless LAN user is not restricted to the physical area of a company or to a single access point. An attacker targeting an unprotected WAP (Wireless AP) needs only to be in the vicinity of the target and no longer requires specialized skills to break into a network.
- Denial of Service: Potential attackers who cannot gain access to your Wireless LAN can nonetheless pose security threats by jamming or flooding your wireless network with static noise that causes wireless signals to collide and produce CRC errors.
- Rogue/Unauthorized Access Points: WAPs can be easily deployed by anyone with access to a network connection, anywhere within a corporation or business.
- Incorrectly configured Access Points: Incorrectly configured access points are an avoidable but significant hole in WLAN security. Many access points are initially configured to openly broadcast SSIDs to authorized users. Many honest network administrators have incorrectly used SSIDs as passwords to verify authorized users. However, because the SSID is being broadcasted, this a large configuration error that allows intruders to easily steal an SSID and have the AP assume they are allowed to connect.
- Network abuses: Authorized users can also threaten the integrity of the network with abuses that drain connection speeds, consume bandwidth, and hinder a WLAN's overall performance. A few users who clog the network by trading MP3 files can affect the productivity of everyone on the wireless network. This ultimately leads to users who are trying to be productive complaining that the network is slow or that they keep losing connection.(7)

2.2.3.2. Wired Threats

As a non-shared media, wired networks are slightly more secure than wireless; however, they are not threat-proof. A list of possible attacks is described below:

- Man in the middle: An unwanted devices establishing a connection between two other devices and sniffing all the traffic that both devices exchange.
- Spoofing: The act of masquerading as a valid entity through falsification of data such as IP address or MAC address.
- Tampering: Malicious modification of products.
- Privilege escalation: An attacker is able to elevate their privileges or access level without authorization.
- Backdoors: A secret method of bypassing normal authentication or security controls. (8)

2.2.3.3. Frontier security and network monitoring

A higher level of network security can be achieved through the usage of Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and Firewalls.

2.2.3.3.1 Intrusion Detection Systems

An Intrusion Detection System (IDS) is a device in charge of monitoring a network or a group of systems to detect malicious activity or policy violations.

By analysing the traffic in a network, malicious activity can be detected through two different methods:

1- Signature Based Detection: It detects attacks through a specific pattern such as byte sequences in network traffic or known malicious instruction sequences used by malware. This method is also used by anti-virus software.

2- Anomaly Based Detection: It uses machine learning to create a model of trustworthy activity, and then compare new behaviour against this model.

2.2.3.3.2 Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) are devices that, as an extension of an IDS, also monitor network traffic and system activities for malicious activity. The main differences between them and IDSs are that IPSs are placed in-line and are able to block or prevent intrusions that are detected.

They work with the same methods as an IDS, signature-based detection, anomaly-based detection, and an additional method called Stateful protocol analysis detection which identifies deviations of protocol states by comparing observed events with “pre-determined profiles of generally accepted definitions of benign activity"(9)

2.2.3.3.3 Firewalls

Firewalls are network security systems which monitor and control incoming and outgoing network traffic based on predetermined security rules. It is commonly used as a barrier between a trusted internal network and untrusted external network.

Firewalls can serve multiple functionalities. They can work as packet filters on the network layer not allowing packets to pass through unless they match a given rule set, as an application layer filter intercepting packets travelling from or to an application working with Deep Package Inspection (DPI), as proxies acting as gateways from one network to another for a specific network application, and as Network Address Translation devices protecting the internal IP addresses from the external network hiding their range with another range of public IP addresses.(10)

2.2.3.4. Network Access Control (NAC)

Network Access Control is an approach to computer security that attempts to unify endpoint security technology, user system authentication and network security enforcement.

The main goals of NAC are the following:

1. Mitigation of non-zero-day attacks.
2. Authentication Authorization and Accounting of network connections.
3. Encryption of traffic to the wireless and wired network using protocols for 802.1X such as EAP-TLS or EAP-PEAP.
4. Role-based controls of user, device, application or security posture post authentication.
5. Automation with other tools to define network role based on other information such as known vulnerabilities, jailbreak status etc.
6. Policy enforcement.
7. Identity and access Management.

Cisco’s solution for this precise feature is called Identity Services Engine (ISE) and fulfils most of the goals described previously.

2.2.4. Management

Traditional devices were configured to work as standalone units that could work independently of the network, however, this feature comes with a major flaw in maintainability due to having to go device by device changing each configuration individually which leads to wasting more time having to connect to each device than configuring it. (see previously mentioned standalone APs 2.2.1.2)

Later, more devices started to be managed through a central unit which was in charge of managing every device connected to it and configuring each one of them. For example, the WLC controlled APs.

This need of having multiple devices controlled to a centralized management unit originated what is now called Software Defined Networks.

One of the most recent implementations of SDNs is Cisco Meraki’s Cloud based Management. Which creates a central dashboard on which you can easily configure devices and networks as a whole. Meraki’s solution allows you to manage a network topology from any place where you have internet connectivity, allowing you to remotely control, manage and view the state of your network configuration and devices.

3. Methodology

First, we will define our project schema. Once we have done the schema we will establish the activities and the timetable that we follow when working in the project.

Afterwards, we will gather information about the previously configured events.

To gather the information, we need to carry out this project we will meet the representatives of companies that took part in the design and configuration of the network architecture of the previously mentioned events. Apart from that, we will gather information about Cisco’s similar network architecture solutions to use it in our project’s standard videogame event configuration.

The criteria that will be used to filter the technological and the architecture solutions will be the following:

1- Functionality fulfilment: Does this solution fulfil all the network requirements defined for our standard videogame event?
2- Availability: Could we easily obtain the technology to define a prototype if we decided to use this solution as a part of ours?
3- Cost: Is it affordable or cost efficient? Correlation between functionalities and cost.

While doing the information research, we will define our standard videogame event and its needs.

From that point onwards, we will use the information gathered to design a first topology through the use of LucidChart conceptual network design functionality.

Once we have a solid topology we use GNS3 to emulate a semi-real-life environment in which the devices properly configured will work in.

When we have the solid topology in GNS3 designed, we will build a prototype to test its functionality in a real-life environment.

4. Case Study

4.1. Introduction

Tecnocampus wants to organize a medium size videogame event, and we are the ones in charge of studying possible configuration options and presenting a best configuration design according to how they want to organize the space and areas that they dispose of, and how many people they expect to come.

Disclaimer: Our solution will not take into account the existing devices forming the current network topology, however, it will take into account all the connections and wired infrastructure when deciding where to place our new devices.

4.2. Description

The areas that Tecnocampus wants to use for the event organization are the following:

- A floor called *Foyer* in the TCM2 building: This area will be used to carry out the main activities of the event. It is divided into two different subareas, the *Foyer* itself and an auditorium. The auditorium will be used as a stage zone for tournaments and videogame speeches and the *Foyer* will be used for user-interaction zones, a second smaller stage, stands and rest zones.
- The outdoors area: This area will be used mostly for stands, shops and rest zones.

Both zones are shown in Figure 7.

Therefore, the Foyer zone must include both wired and wireless connectivity and the outdoors area will only have wireless connectivity.

The devices thought to deliver connectivity to the outdoors area must be rough weather resistant and should support electrical supply through both POE and copper cable.

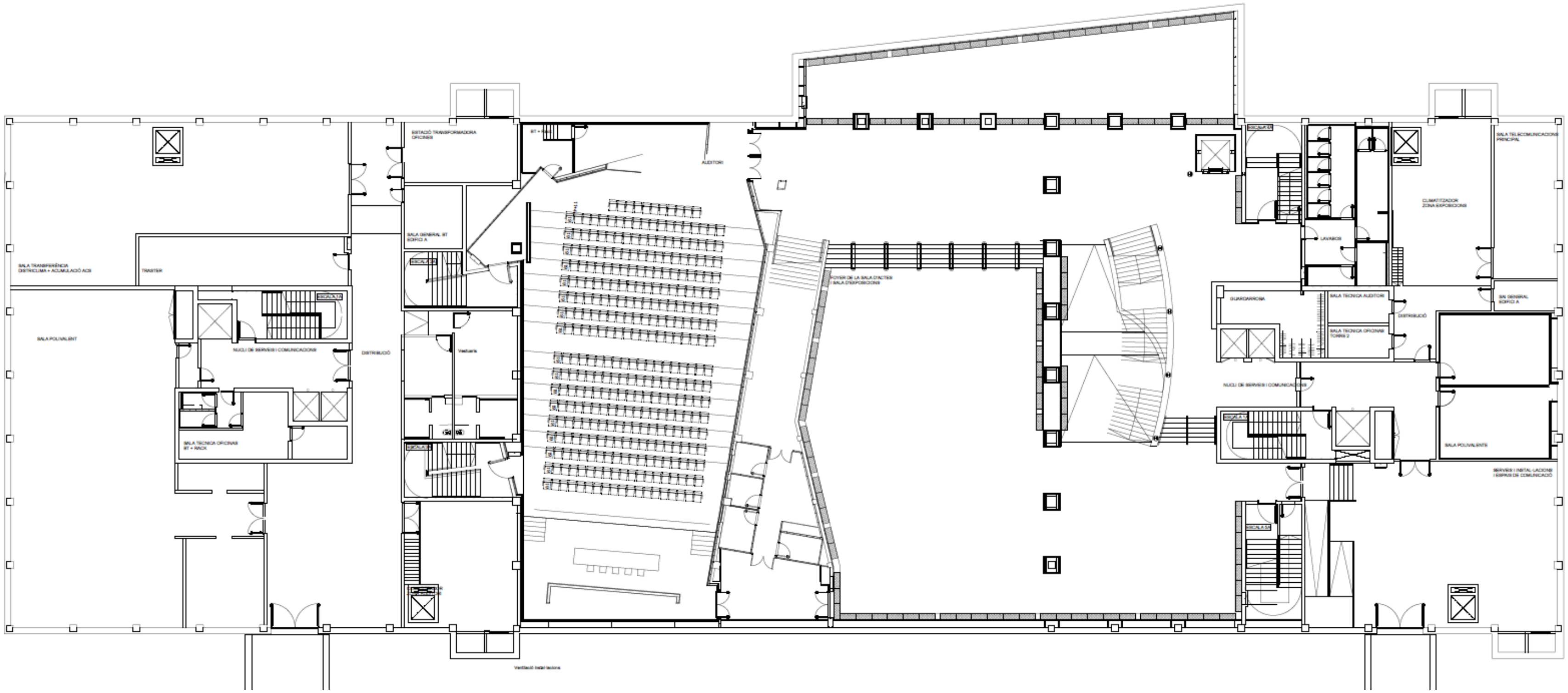


Figure 7: Foyer floor map

4.3. Possible solutions

Given that the case described before matches with a small-medium videogame event, the most important features that we will take into account when offering a solution to the network configuration are the following:

- Scalability: Easy to replicate and redeploy the network components configuration.
- Easy to deploy and dismount and reusability: Due to temporality we might want to reuse the devices for other events therefore the network topology should be as easy to deploy and dismount as possible.
- Easy to manage, troubleshoot and update: being a small event means that there will be less devices required to deliver the connectivity, however, as the number of devices required decrease, the remaining devices become more critical when providing that connectivity. Which means that a single device malfunctioning could cause a higher impact in a network with less devices than in a network with a large number of devices. Therefore, if a device goes down or starts malfunctioning, the lower the time it takes to identify the problem and implement a solution the better.
- Failure tolerance, High availability (HA): When a network device malfunctions the other *healthy* devices must be able to redistribute the current connections that the malfunctioning device had to themselves or other *healthy* devices.

With those key concepts in mind and using Cisco’s devices we propose the following configuration options for wireless, wired, security and management based on the infrastructure shown in Figure 8.

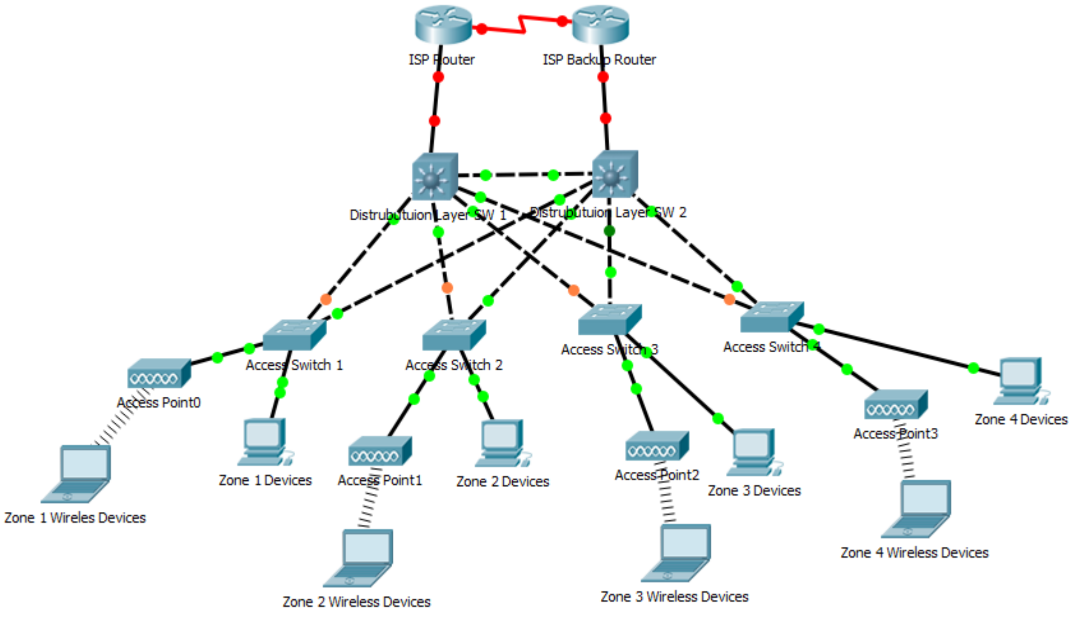


Figure 8: Base Network Topology

4.3.1. Wireless

For the wireless infrastructure, access points must be managed through a Wireless LAN Controller or a device which acts as one allowing the network administrators to maintain, update and configure all the access points from only one place reducing time and effort costs.

Therefore, a WLC device can be used directly or an access point that supports the Mobility Express mode which allows this access point to work as both an access point and a WLC.

Then we have a network with a WLC device and multiple access points in lightweight mode, or a network with an access point in Mobility express mode acting as a WLC and multiple access points in lightweight mode.

The solution using an access point as a WLC is not recommended for high density events, due to the fact that having the responsibility of a WLC while serving as an access point with numerous connections can impair the performance of that access point and the WLC, leading to an impaired performance of the rest of access points.

Configuration wise, the WLC should configure the access point to know each SSID and VLAN that they will spread and define the management VLAN which will be used for all the network topology devices for management purposes.

A part from the solutions using WLC devices and access points in Mobility Express mode, there is a third solution which involves Meraki's cloud managed devices, however as it mostly includes features about management we explain it in the Management section.

4.3.2. Wired

The wired structure that we will use only includes the access layer and the distribution layer due to the event not being complex enough to integrate a core layer. In case the event was more complex we could use a core layer and the devices (switches) according to that layer.

For wired infrastructure, switches should be differentiated between access layer switches, which will grant connectivity to the end devices that need it, and distribution layer switches which will provide connectivity to other network devices.

The access layer switches are the ones in charge to tag and mark the VLANs from which the traffic starts or where it goes. Therefore, when configuring those devices we must take into consideration port VLAN tagging or enabling port VLAN trunk ports.

Port VLAN tagging is mostly used when directly connected to end devices which are associated to specific VLANs, and trunk ports are used when those ports connect to a device which manages multiple VLANs, for example an access point with multiple SSIDs and a VLAN for each one or another switch.

Therefore we must define a VLAN for each of the device groups that we are going to have in the event to be able to tag the switch ports accordingly and ease the device management for each VLAN.

As we defined before, there will be devices that will be open for use in user-interaction zones, devices in the scenario zone, and wireless devices. A part from those we should differentiate between the devices which the management staff will use to monitor and control the network while the event is taking place and the VIP devices.

Then, as a summary of VLANs we should have:

1- A VLAN for free access devices which would be called OpenDevices
2- A VLAN for management or corporative devices called EventCorp.
3- A VLAN for Guests, which will be used in wired and wireless connections, called EventGuests.
4- A VLAN for VIP Guests, which will be used in wired and wireless connections, called EventVIPGuests.
5- A VLAN for the Stage devices called StagePCs.
6- A VLAN for quarantined devices.

Defining those VLANs will help us establish Quality of Service Policies for each of them individually defining preferences and package priorities, and establish the security policies to follow.

Our Wired infrastructure will be defined following a Circular structure, which means that to access the same device or connection there will be more than one path to follow, however, this could cause loops if not correctly defined, therefore we will use the Spanning Tree Protocol to avoid the presence of loops establishing route priorities. This structure helps us assure one of the High Availability requirements due to the fact that if one of the links to a device falls or malfunctions, the device can still get the connection through another route until the link recovers.

4.3.3. Security

In our security solutions we must take into consideration 2 different concepts. Internal network device access security and external network device access security.

As our internal network device access security we could use different configurations such as:

- Having each device to define locally management usernames and passwords with privilege levels that can be used by network administrators to modify, update or manage device configurations.
- Having an external authentication server through TACACS+ or RADIUS. In this case you should register all the users allowed to manage the network devices in the external AAA server. Also, using an external authentication server you could define what

commands each user is allowed to perform a part from setting their privilege level like in the previous solution.

As our external network device access (or accessing the internet) we have some essential configurations which include:

1- For the wireless section:
   a. To define a WPA2-PSK password for each of the SSIDs that we are going to spread.
2- For the wired section:
   a. To define access lists to allow or deny connections to specific IPs or between different VLANs which we do not want them to see one another.
   b. To have security policies which filter the layer 7 access depending on the contents and category of that page.

A part from those we can have more optional security configurations like the following:

1- For the wireless section:
   a. To define a captive portal for guest users where they must register to get access to the internet.
   b. SMS authentication: which proves that the person that is trying to access the SSID is really a person due to the fact that all mobile numbers are associated to a NIF/DNI.
2- For the wired section:
   a. To define an authentication server to manage connection from devices which are trying to access the internet through the wired environment.
   b. To know all the ports that the applications which are going to be used in that event will use and then cap all other connections that are not going to or coming from those ports.

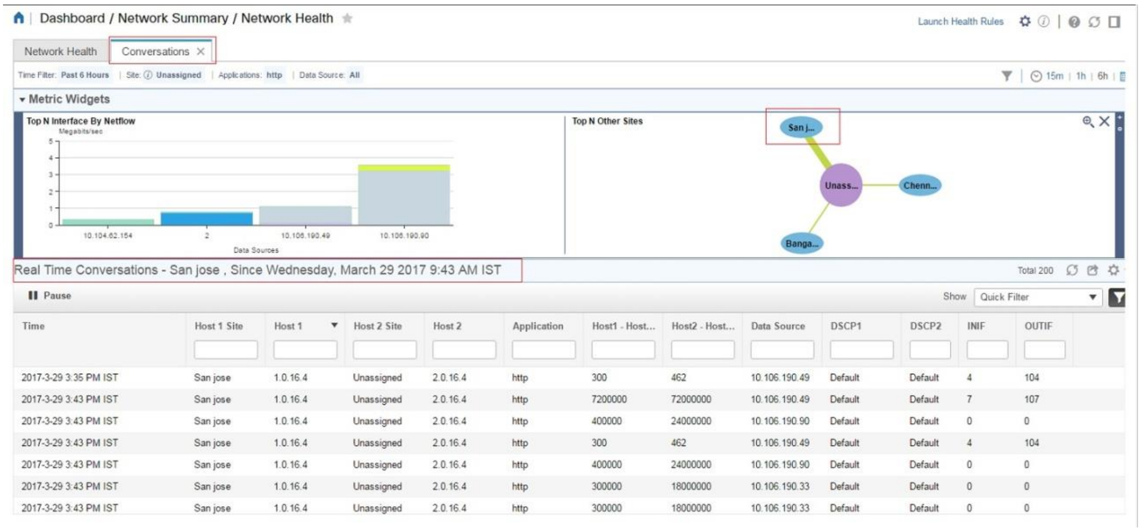
A part from preventive security we should consider including active security through the usage of an IPS or at least the usage of an IDS, even if the connectivity gets a bit slower, we prefer not risking the whole network robustness for a little speed.

4.3.4. Management

In our management solution proposals the concept of scalability is the most important one, given that managing a dense network with no scalability means having to manage each device individually and doing that implies a huge waste of time whereas managing a scalable infrastructure you will most likely have a centralized management panel or dashboard which will allow you to manage all or most of your devices from a single place.

Having that in mind the proposals are the following:

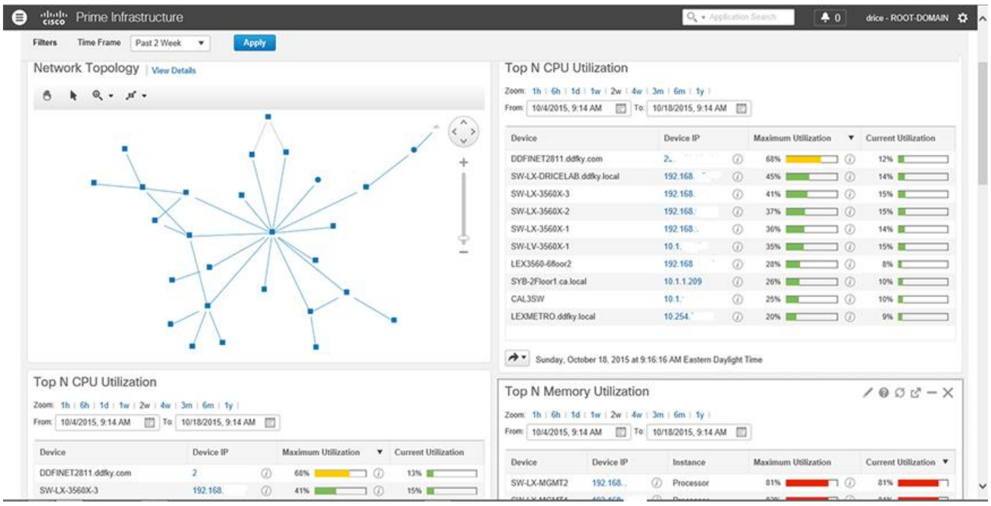
- Using Cisco's Prime Infrastructure. Which allows us to see the status of each topology device in real time and the events that took place during a period of time through a dashboard, a part from showing the connections established and connection requests and establishments as shown in Figure 9 and Figure 10.



Real Time Conversations - San jose , Since Wednesday, March 29 2017 9:43 AM IST

Time	Host 1 Site	Host 1	Host 2 Site	Host 2	Application	Host1 - Host...	Host2 - Host...	Data Source	DSCP1	DSCP2	INIF	OUTIF
2017-3-29 3:35 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300	462	10.106.190.49	Default	Default	4	104
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	7200000	72000000	10.106.190.49	Default	Default	7	107
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	400000	24000000	10.106.190.90	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300	462	10.106.190.49	Default	Default	4	104
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	400000	24000000	10.106.190.90	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300000	18000000	10.106.190.33	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300000	18000000	10.106.190.33	Default	Default	0	0

Figure 9: Cisco's Prime Infrastructure Connection Dashboard



Filters Time Frame Past 2 Week

Network Topology | View Details

Top N CPU Utilization

Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y |

From: 10/4/2015, 9:14 AM To: 10/18/2015, 9:14 AM

Device	Device IP	Maximum Utilization	Current Utilization
DDFINET2811.ddfky.com	2..	68%	12%
SW-LX-DRICELAB.ddfky.local	192.168.	45%	14%
SW-LX-3560X-3	192.168.	41%	15%
SW-LX-3560X-2	192.168.	37%	15%
SW-LX-3560X-1	192.168.	36%	14%
SW-LV-3560X-1	10.1.	35%	15%
LEX3560-6floor2	192.168	28%	8%
SYB-2Floor1.ca.local	10.1.1.209	26%	10%
CAL3SW	10.1.	25%	10%
LEXMETRO.ddfky.local	10.254.	20%	9%

Sunday, October 18, 2015 at 9:16:16 AM Eastern Daylight Time

Top N CPU Utilization

Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y |

From: 10/4/2015, 9:14 AM To: 10/18/2015, 9:14 AM

Device	Device IP	Maximum Utilization	Current Utilization
DDFINET2811.ddfky.com	2	68%	13%
SW-LX-3560X-3	192.168.	41%	15%

Top N Memory Utilization

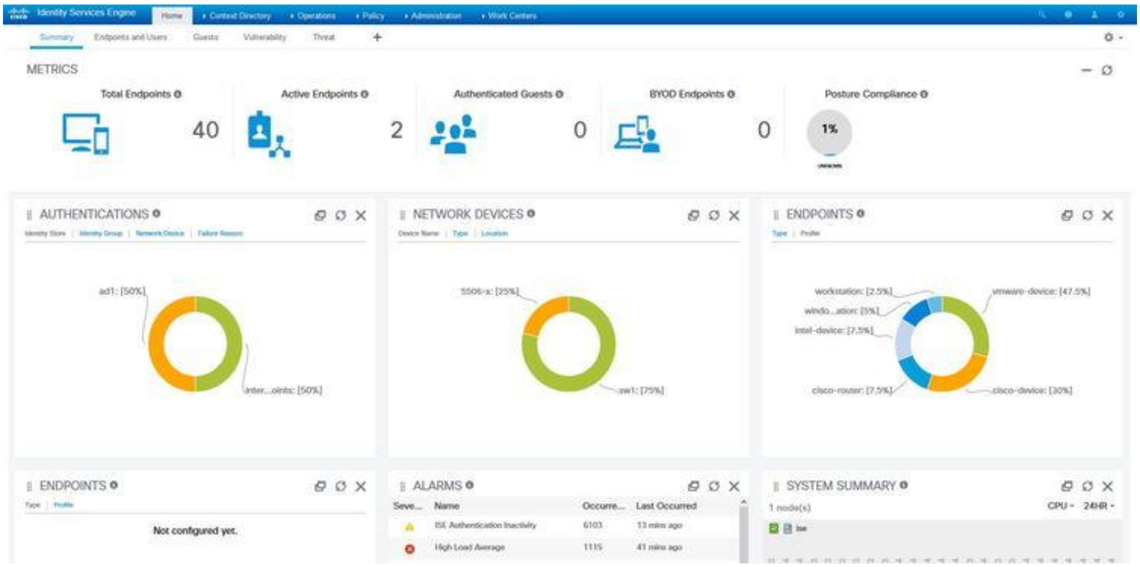
Zoom: 1h | 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y |

From: 10/4/2015, 9:14 AM To: 10/18/2015, 9:14 AM

Device	Device IP	Instance	Maximum Utilization	Current Utilization
SW-LX-MGMT2	192.168..	Processor	81%	81%

Figure 10: Cisco's Prime Infrastructure Dashboard

- Using another Cisco solution called Identity Services Engine: Which allows us to control the access to our network and define policies accordingly, contain threats through assessing vulnerabilities. It can also catalogue each end user device depending on each security police that they fulfil and grant access to the network or deny it, through a feature called Posture it follows the sequence described in Figure 11Figure 11. It also allows us to see the amount of connections and devices currently connected to our network through a dashboard, see Figure 12. This solution can also work as an AAA server which allows integration with device authorization. A part from those features, it also includes a BYOD area configuration functionality which allows us to define an authentication methodology for those end user devices which are not permanent on our network. The Cisco ISE also includes a functionality called Profiling which identifies each device depending on its category, for example end-user device or network device; its model and version, for example a Cisco Catalyst 2960 or a Nexus 6k, the OS that they use, if they use a Linux distribution, Windows or IOS, etcetera, and it uses that information to allow the administrator to define policies according to the type of device. See Figure 13.



Not configured yet.

Seve...	Name	Occurre...	Last Occurred
⚠	ISE Authentication Inactivity	6103	13 mins ago
⊗	High Load Average	1115	41 mins ago

Figure 12: ISE Dashboard

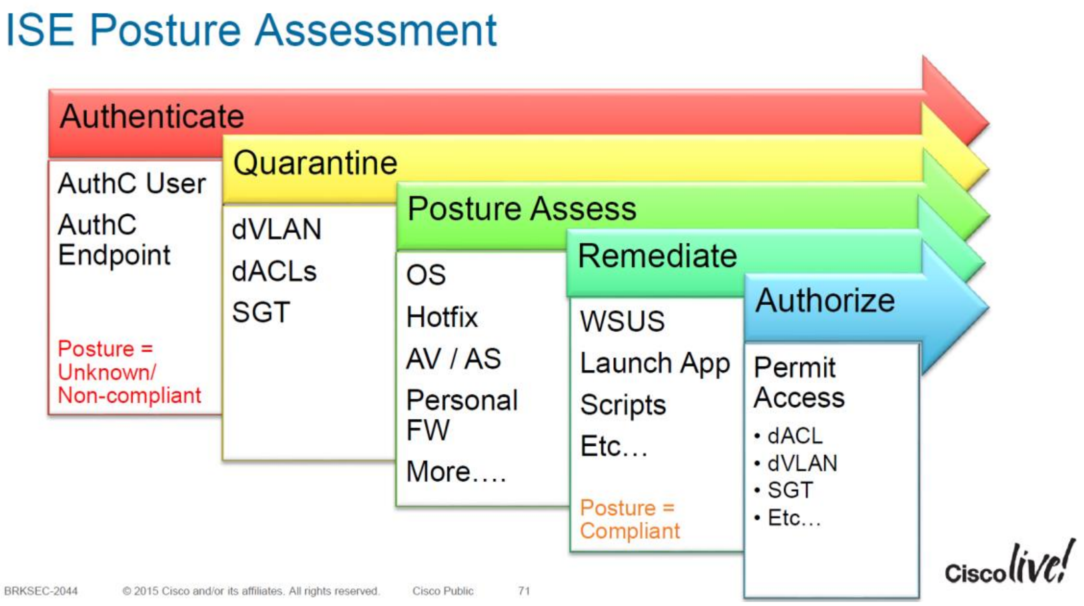
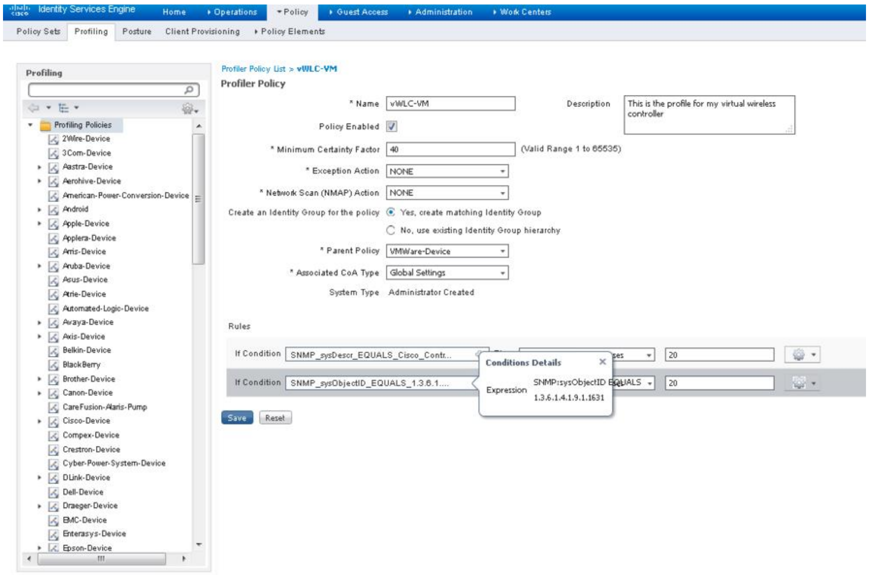

ISE Posture Assessment

Figure 11: ISE Posture Assesment



Profiler Policy List > vWLC-VM

Profiler Policy

* Name: vWLC-VM

Description: This is the profile for my virtual wireless controller

Policy Enabled: ☑

* Minimum Certainty Factor: 40 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy: VMWare-Device

* Associated CoA Type: Global Settings

System Type: Administrator Created

Rules

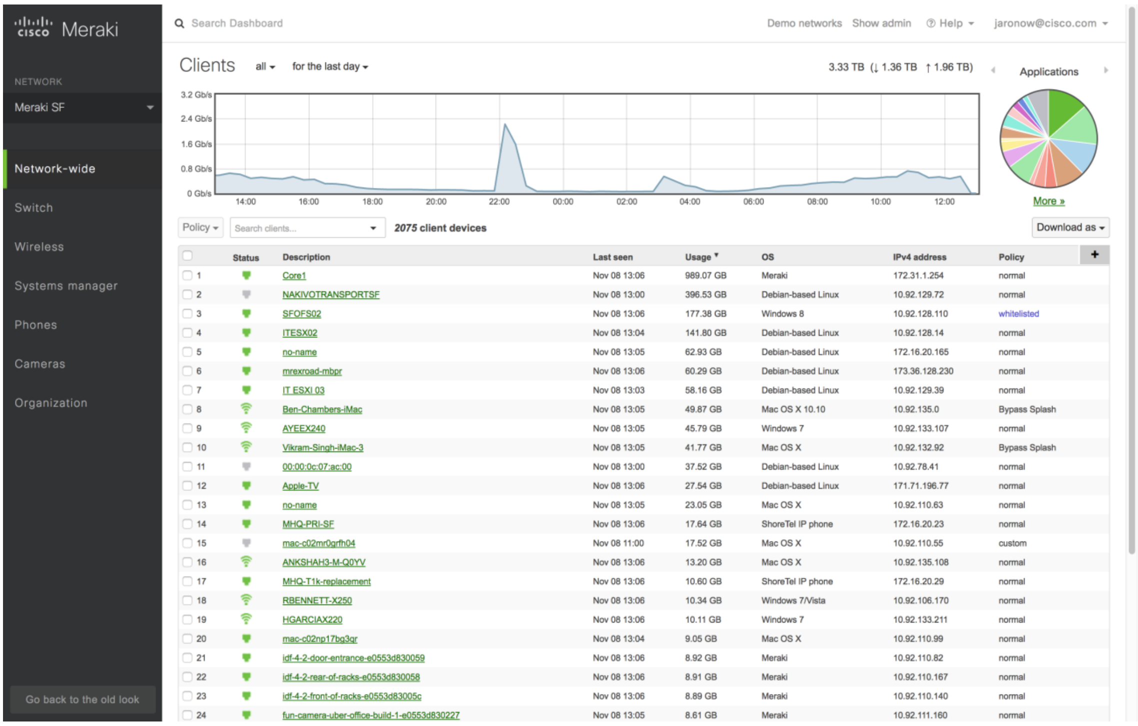
If Condition SNMP_sysDescr_EQUALS_Cisco_Contr... ses 20

If Condition SNMP_sysObjectID_EQUALS_1.3.6.1.... EQUALS 20

Conditions Details

Expression: SNMP:sysObjectID EQUALS 1.3.6.1.4.1.9.1.1631

Figure 13: ISE Profiling Menu



2075 client devices

□	Status	Description	Last seen	Usage ▾	OS	IPv4 address	Policy
□ 1	🟩	Core1	Nov 08 13:06	989.07 GB	Meraki	172.31.1.254	normal
□ 2	⬜	NAKIVOTRANSPORTSF	Nov 08 13:00	396.53 GB	Debian-based Linux	10.92.129.72	normal
□ 3	🟩	SFOFS02	Nov 08 13:06	177.38 GB	Windows 8	10.92.128.110	whitelisted
□ 4	🟩	ITESX02	Nov 08 13:04	141.80 GB	Debian-based Linux	10.92.128.14	normal
□ 5	🟩	no-name	Nov 08 13:05	62.93 GB	Debian-based Linux	172.16.20.165	normal
□ 6	🟩	mrexroad-mbpr	Nov 08 13:06	60.29 GB	Debian-based Linux	173.36.128.230	normal
□ 7	🟩	IT ESXI 03	Nov 08 13:03	58.16 GB	Debian-based Linux	10.92.129.39	normal
□ 8	📶	Ben-Chambers-iMac	Nov 08 13:05	49.87 GB	Mac OS X 10.10	10.92.135.0	Bypass Splash
□ 9	📶	AYEEX240	Nov 08 13:05	45.79 GB	Windows 7	10.92.133.107	normal
□ 10	📶	Vikram-Singh-iMac-3	Nov 08 13:05	41.77 GB	Mac OS X	10.92.132.92	Bypass Splash
□ 11	⬜	00:00:0c:07:ac:00	Nov 08 13:00	37.52 GB	Debian-based Linux	10.92.78.41	normal
□ 12	🟩	Apple-TV	Nov 08 13:06	27.54 GB	Debian-based Linux	171.71.196.77	normal
□ 13	🟩	no-name	Nov 08 13:05	23.05 GB	Mac OS X	10.92.110.63	normal
□ 14	🟩	MHQ-PRI-SF	Nov 08 13:06	17.64 GB	ShoreTel IP phone	172.16.20.23	normal
□ 15	⬜	mac-c02mr0grfh04	Nov 08 11:00	17.52 GB	Mac OS X	10.92.110.55	custom
□ 16	📶	ANKSHAH3-M-Q0YV	Nov 08 13:06	13.20 GB	Mac OS X	10.92.135.108	normal
□ 17	🟩	MHQ-T1k-replacement	Nov 08 13:06	10.60 GB	ShoreTel IP phone	172.16.20.29	normal
□ 18	📶	RBENNETT-X250	Nov 08 13:06	10.34 GB	Windows 7/Vista	10.92.106.170	normal
□ 19	📶	HGARCIAX220	Nov 08 13:06	10.11 GB	Windows 7	10.92.133.211	normal
□ 20	🟩	mac-c02np17bg3qr	Nov 08 13:04	9.05 GB	Mac OS X	10.92.110.99	normal
□ 21	🟩	idf-4-2-door-entrance-e0553d830059	Nov 08 13:06	8.92 GB	Meraki	10.92.110.82	normal
□ 22	🟩	idf-4-2-rear-of-racks-e0553d830058	Nov 08 13:06	8.91 GB	Meraki	10.92.110.167	normal
□ 23	🟩	idf-4-2-front-of-racks-e0553d83005c	Nov 08 13:06	8.89 GB	Meraki	10.92.110.140	normal
□ 24	🟩	fun-camera-uber-office-build-1-e0553d830227	Nov 08 13:05	8.61 GB	Meraki	10.92.111.160	normal

Figure 14: Meraki Application usage by client

- Using Meraki cloud managed devices: Meraki uses a cloud based management dashboard to which all its devices register and get their configuration details from. Being a cloud based dashboard allows the network administrator to access it from any device as long as it has the appropriate URL and credentials. It also has a mobile app which allows the administrator to manage the network through his mobile device. In this dashboard there are multiple views that show the network usage per client, application usage per client, see Figure 14, amount of traffic that is currently under use, network health and connection errors, as well as authentication errors, security assessment through air marshalling and rogue AP and SSID detection. It is a very powerful management and configuration infrastructure which allows you to configure all network devices from one place, such as firewalls, switches and access points. It also includes support to IP cameras and phones. With this dashboard you can locate each device by network, physical location and organization.

4.4. Chosen solution

As we described before, our event does not require a permanent deployment of infrastructure and it needs to be easy and fast to configure manage and troubleshoot, a part from having basic security measures and monitoring.

Therefore we chose to implement a Meraki-based infrastructure to fulfil all our previously defined requirements.

4.4.1. Explanation

Meraki, as we stated before, is a cloud based solution, which means that all the management, troubleshooting, device and security configurations and monitoring can be done through the dashboard hosted on the cloud. This means that we do not need to physically deploy any centralized management devices on the network infrastructure because it is already on the cloud.

To deploy our network we just need to register the serial number of our Meraki devices and licence them into our dashboard and we can configure them right away without even having to turn them on. This way, when the event takes place we just need to plug them into an Ethernet cable and a power supply and they will get their configurations from our dashboard, and we will only need to polish their configurations and monitor their status and usage.

Before configuring our network we need to define the amount of devices and series that we are going to use to give internet access for our wireless and wired infrastructure as well as the security firewall that we are going to use.

For our wireless coverage we will use 6 MR42 Wireless Access points to cover the Foyer and auditorium area shown in Figure 15, three MR74 Outdoor Wireless Access points to cover the outdoor area of the Tecnocampus shown in Figure 16.

For our wired coverage we will use one MS210-24 for the Auditorium which will hold up to 24 devices connected at the stage area of the auditorium, two MS250-48 in stack to hold up to 96 devices connected for the Foyer zones and two MS410-16 in stack as our distribution layer switches.

As our Firewalls, we will use two MX100 in HA stack with the advanced security licenses. This will allow us to keep track of and prevent or identify all the malicious activity in our network.

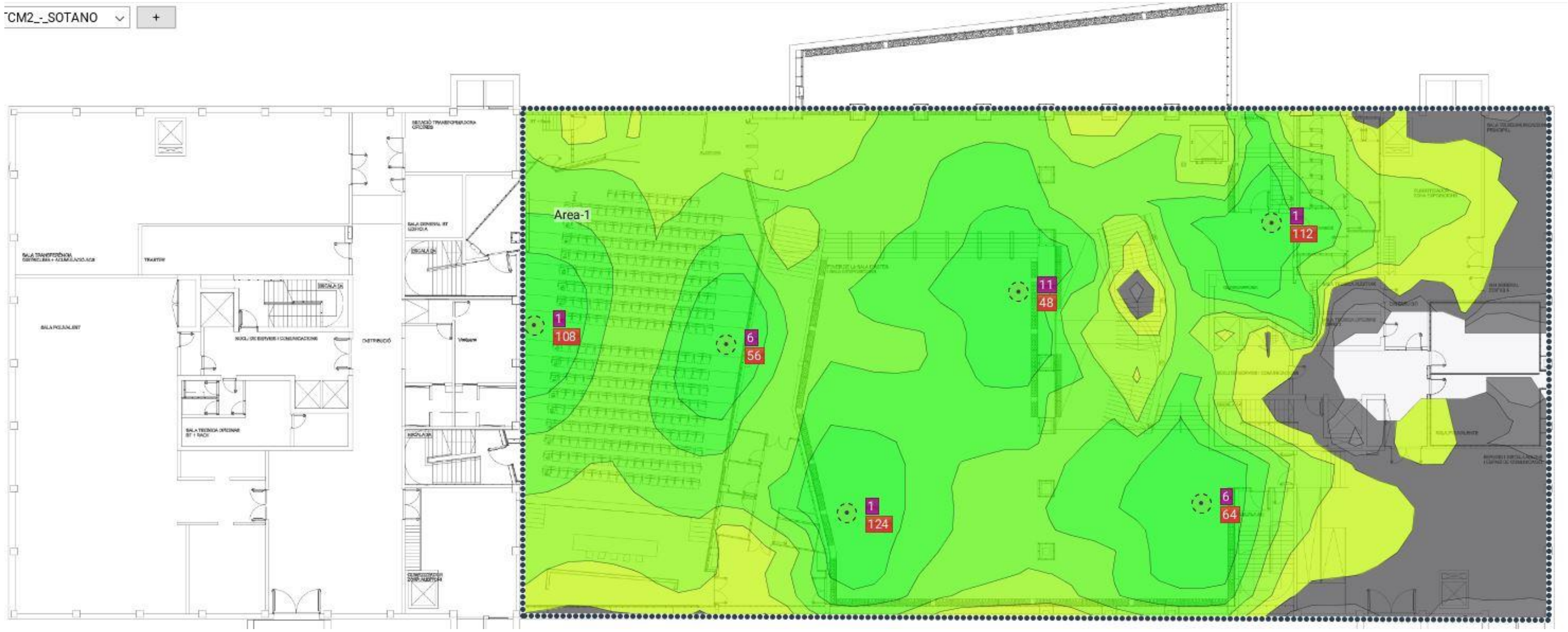


Figure 15: Foyer Coverage and AP distribution

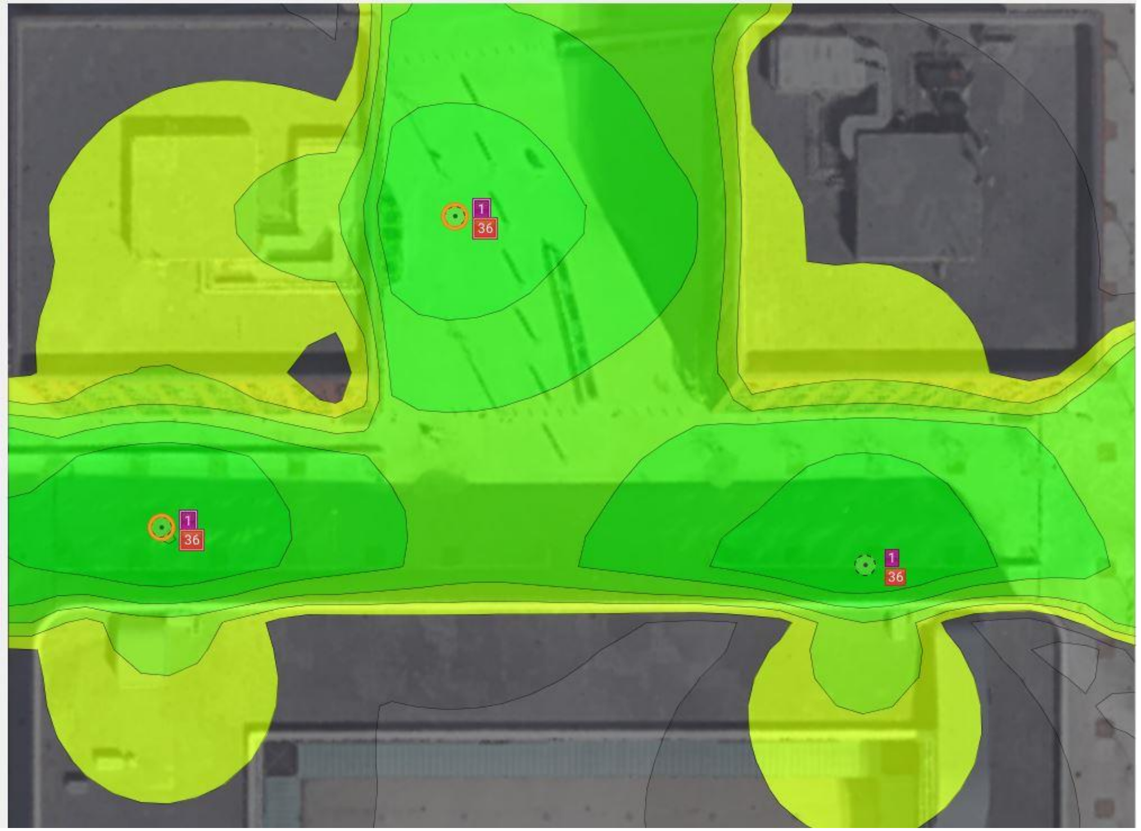


Figure 16: Outdoors Wireless Coverage

4.5. Viability analysis

4.5.1. Technological viability

To develop our network solution for this event, we require the following resources:

1- Internet connectivity to access the Meraki Dashboard.

2- The Meraki devices that we are going to configure and their licences.

3- An end user device, like a personal laptop or desktop, from which we will access the Meraki Dashboard.

4- Wires and cabling.

4.5.2. Economical viability

4.5.2.1. Budget

Even though this is just a case study, we define the approximate cost of deploying the solution proposed.

The needed budget is calculated through the Meraki devices and license pricing, the average salary of a Networking professional and the amortization of the computer. All the costs are shown in Table 2.

Disclaimer: We are not taking into account the wire and cabling costs due to the lack of knowledge of the amount of meters of cable required.

Item	Quantity	Cost per unit	Total
Meraki MR42	6	729,90€	4.379,40€
Meraki 3 Year MR Enterprise License	9	205,95€	1.235,70€
Meraki MR74	3	965,31€	2.895,93€
Meraki MR74	3	153,98€	461,94€

Omni Antenna			
Meraki MS210-24 3 Year Enterprise License	1	238,00€	238,00€
Meraki MS210-24	1	2.060,00€	2.060,00€
Meraki MS250-48	2	4.000,00€	8.000,00€
Meraki MS250-48 3 Year Enterprise License	2	644,00€	1.288,00€
Meraki MS410-16	2	5.695,00€	11.390,00€
Meraki MS410-16 3 Year Enterprise License	2	700,00€	1.400,00€
Meraki MX100	2	3.246,75€	6.493,50€
Meraki MX100 3 Year Advanced Security License	1	3.500,00€	3.500,00€
Network professional Salary	600 (hours)	25,00€	15.000,00€
Computer	1	1.500,00€*4y*(3/4)*(20/50)	1.800,00€
Total			60.142,47€

Table 2: Case Study Budget

The computer price was calculated through the following formula: Price*life-span*(project time in years)*(hours of use per week for the project/total hours of use per week). We only require one advanced security license due to the fact that HA/Warm-spare firewalls of Meraki only require one license.

4.5.3. Environmental viability

While the devices function normally the environmental impact that they generate is limited to the emission of radiofrequency waves for the wireless SSID spreading and the small amount of radiation from the electronic parts of the devices.

When the devices malfunction they can produce harmful radiofrequency emissions or get statically charged which could lead to major injuries. Therefore, Cisco has established an Return of Merchandise Authorization which allows the return and replacement of the malfunctioning devices in little amounts of time and requires the malfunctioning devices to be disconnected and replaced from the network to prevent them from harming people.

4.6. Deployment and Configuration guide

First of all we need to register the devices to our dashboard; we do this in the “Add devices” menu on our Meraki organization shown in Figure 17, and then we click on the “Claim” button to upload the serial numbers of the devices shown in Figure 18.

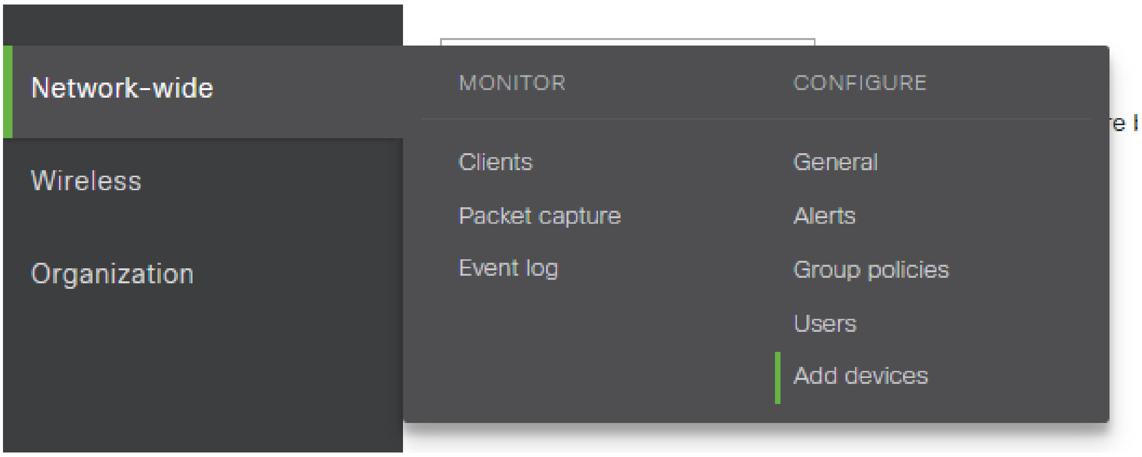
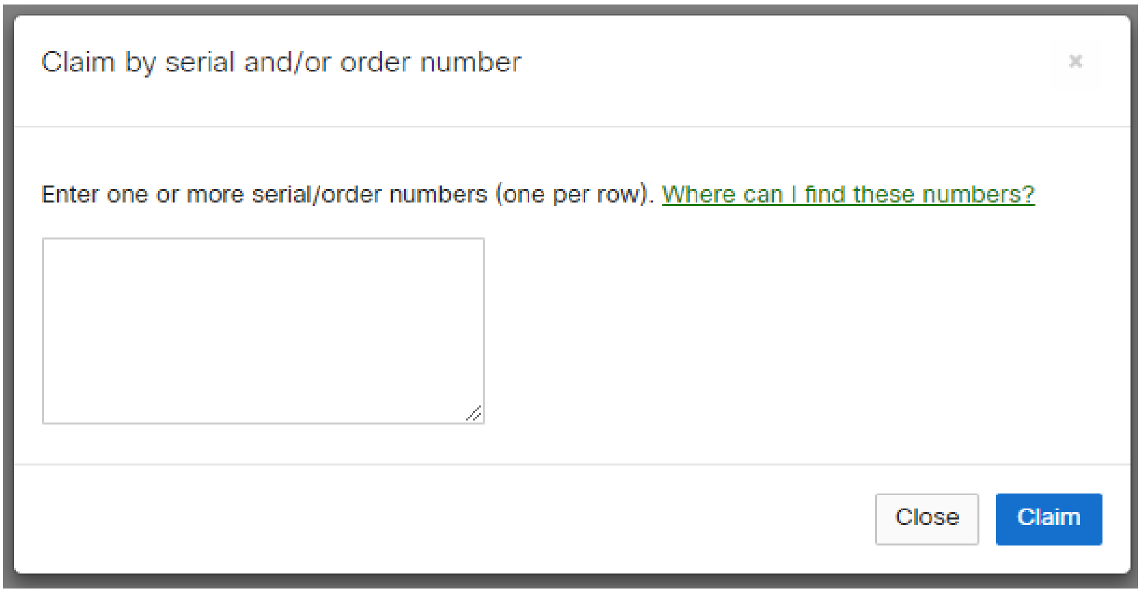


Figure 17: Add devices menu

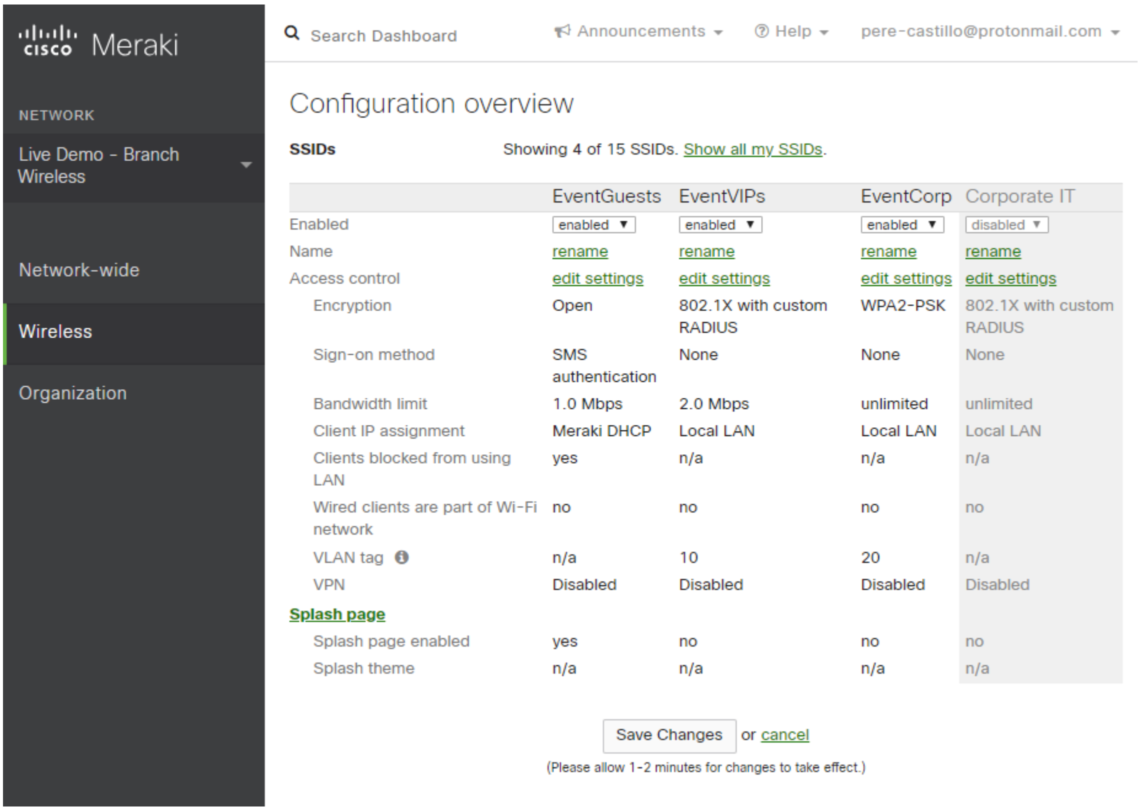

Claim by serial and/or order number

Enter one or more serial/order numbers (one per row). Where can I find these numbers?

Figure 18: Claim device menu

After claiming the devices we configure the wireless and wired devices through different dashboards.

For the Wireless devices we can configure the SSIDs through the Configuration SSID option of the wireless menu shown in Figure 19. There we can define which SSIDs we want to use in our event; in this case we will have the SSIDs EventGuests, EventVIPs and EventCorp, each one assigned to their corresponding VLAN.



Configuration overview

SSIDs Showing 4 of 15 SSIDs. Show all my SSIDs.

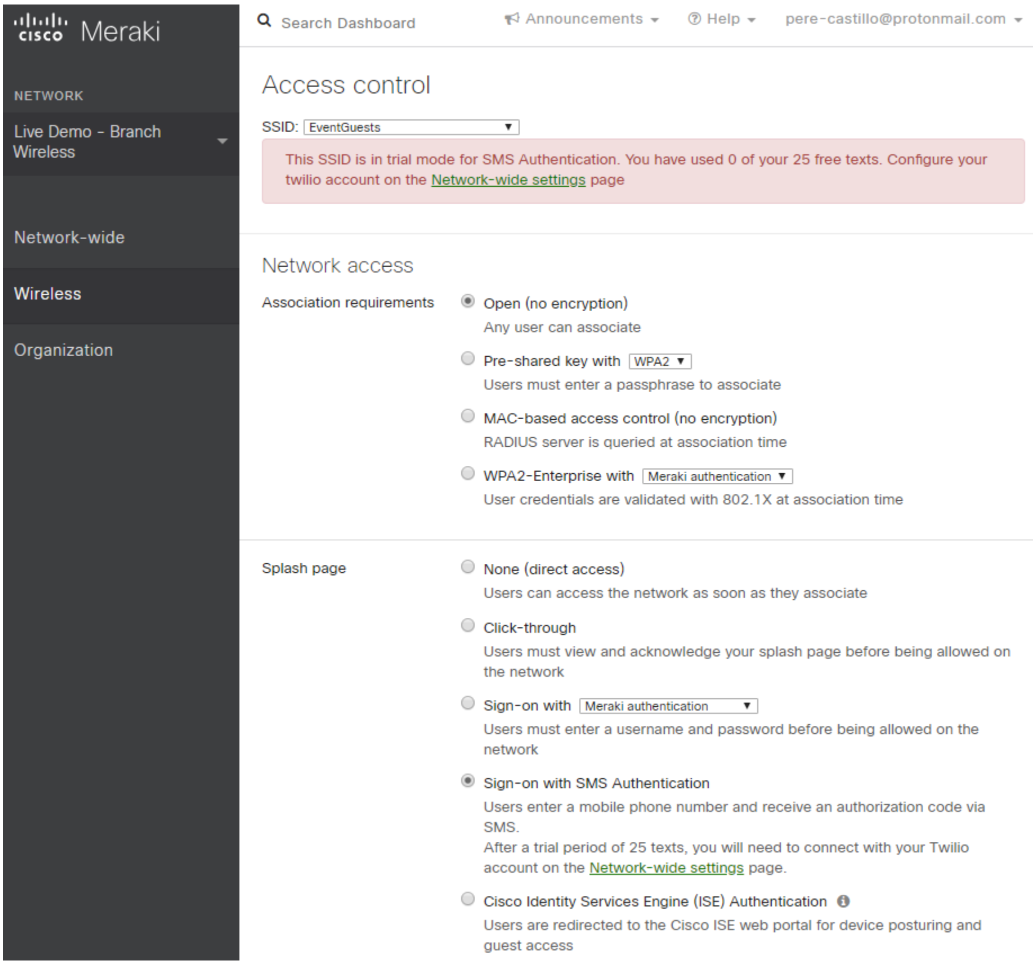
	EventGuests	EventVIPs	EventCorp	Corporate IT
Enabled	enabled ▼	enabled ▼	enabled ▼	disabled ▼
Name	rename	rename	rename	rename
Access control	edit settings	edit settings	edit settings	edit settings
Encryption	Open	802.1X with custom RADIUS	WPA2-PSK	802.1X with custom RADIUS
Sign-on method	SMS authentication	None	None	None
Bandwidth limit	1.0 Mbps	2.0 Mbps	unlimited	unlimited
Client IP assignment	Meraki DHCP	Local LAN	Local LAN	Local LAN
Clients blocked from using LAN	yes	n/a	n/a	n/a
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	n/a	10	20	n/a
VPN	Disabled	Disabled	Disabled	Disabled
Splash page				
Splash page enabled	yes	no	no	no
Splash theme	n/a	n/a	n/a	n/a

Save Changes or cancel

(Please allow 1-2 minutes for changes to take effect.)

Figure 19: SSID configuration menu

To configure each of them individually we must click on the edit settings option of the corresponding SSID and enter the access control menu for that SSID, shown in Figure 20, there you can define its VLAN, association requirements, the splash page (if needed), the NAC policy to follow, group policies by device, the client IP management, content filtering, band selection and minimum bit-rates.



Access control

SSID: EventGuests

This SSID is in trial mode for SMS Authentication. You have used 0 of your 25 free texts. Configure your twilio account on the Network-wide settings page

Network access

Association requirements

● Open (no encryption)
Any user can associate

○ Pre-shared key with WPA2
Users must enter a passphrase to associate

○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time

Splash page

○ None (direct access)
Users can access the network as soon as they associate

○ Click-through
Users must view and acknowledge your splash page before being allowed on the network

○ Sign-on with Meraki authentication
Users must enter a username and password before being allowed on the network

● Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS.
After a trial period of 25 texts, you will need to connect with your Twilio account on the Network-wide settings page.

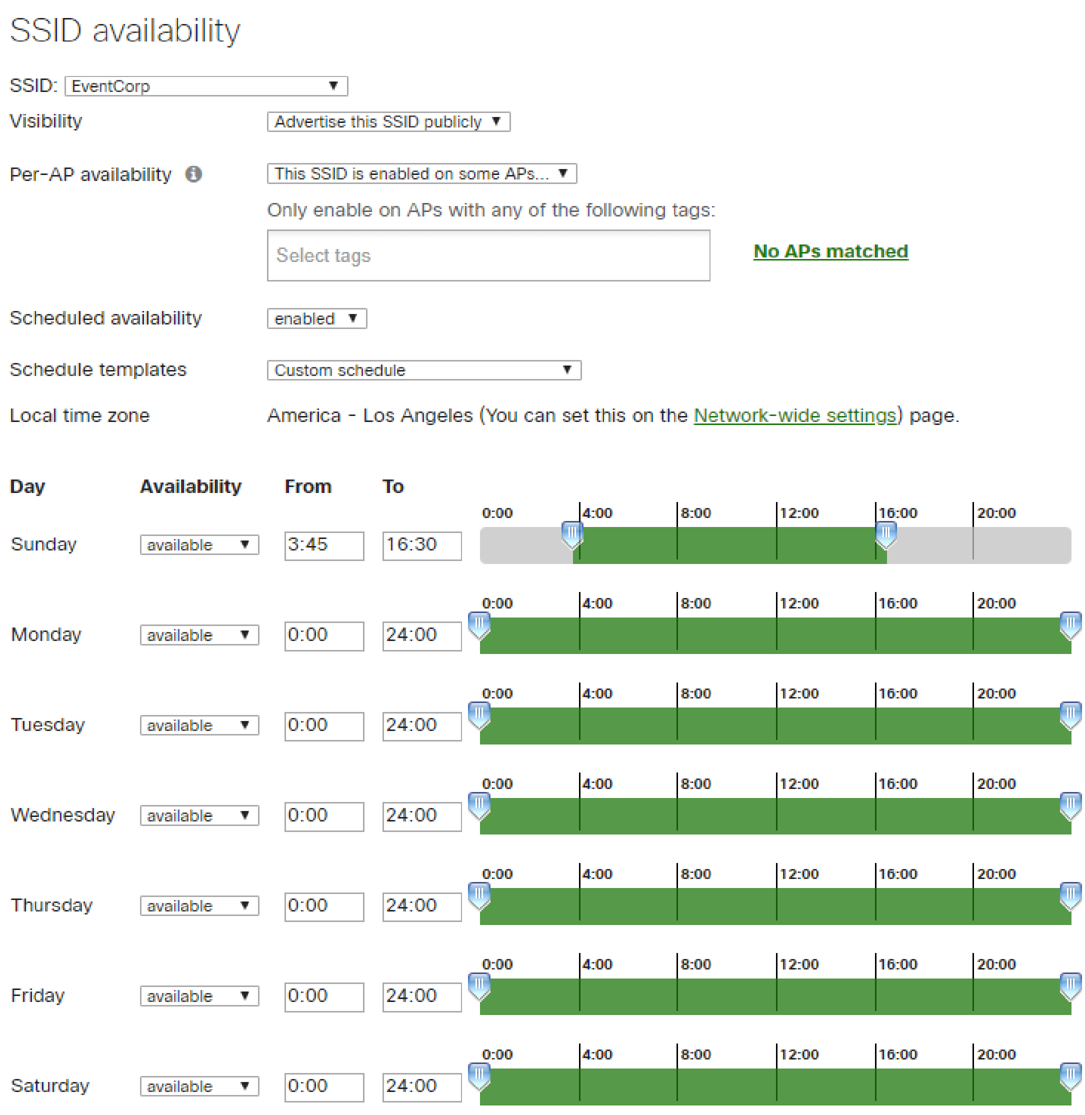
○ Cisco Identity Services Engine (ISE) Authentication
Users are redirected to the Cisco ISE web portal for device posturing and guest access

Figure 20: Access Control menu

A part from that you can also configure Firewall rules and traffic shaping for each SSID in the "Firewall & Traffic shaping" option in the wireless menu.

Each SSID can be assigned to all of the access points of our network or just to some of them, and we can adjust its availability by time schedules. This is done in the SSID availability option in the Wireless menu, shown in Figure 21.

Figure 21: SSID Availability menu



SSID availability

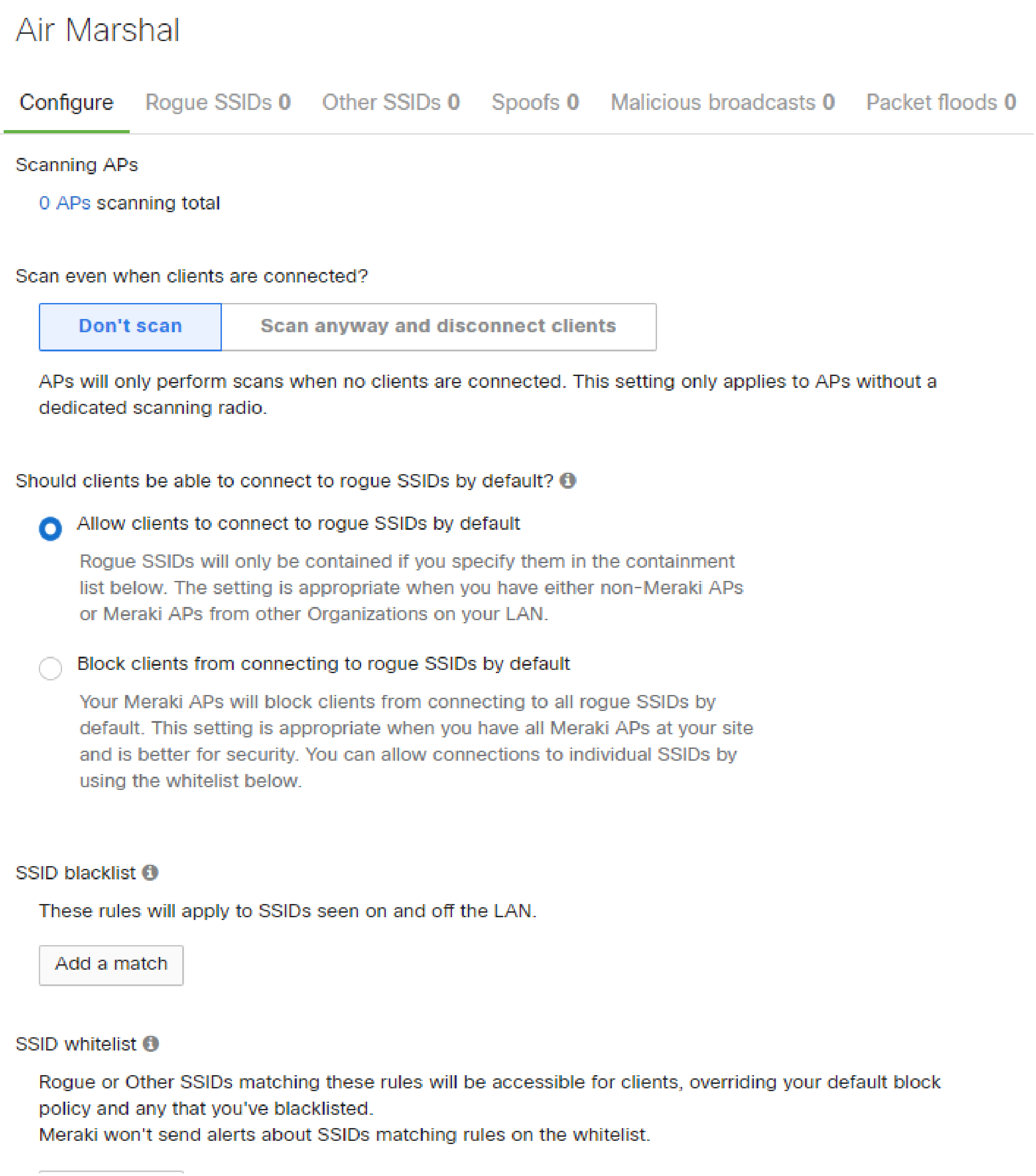
SSID: EventCorp ▼

Visibility	Advertise this SSID publicly ▼
Per-AP availability	This SSID is enabled on some APs... ▼ Only enable on APs with any of the following tags: Select tags No APs matched
Scheduled availability	enabled ▼
Schedule templates	Custom schedule ▼
Local time zone	America - Los Angeles (You can set this on the Network-wide settings) page.

Day	Availability	From	To
Sunday	available ▼	3:45	16:30
Monday	available ▼	0:00	24:00
Tuesday	available ▼	0:00	24:00
Wednesday	available ▼	0:00	24:00
Thursday	available ▼	0:00	24:00
Friday	available ▼	0:00	24:00
Saturday	available ▼	0:00	24:00

A part from the previously mentioned wireless features, there is an additional, more important one called “Air Marshal” on the wireless menu. This feature allows us to enable AP scanning, SSID whitelist and blacklist and SSID alerting. It also allows us to identify Rogue SSIDs, SSID spoofs, malicious broadcasts and packet floods in our wireless network. See Figure 22.

Figure 22: Air Marshal Dashboard



Air Marshal

Scanning APs

0 APs scanning total

Scan even when clients are connected?

[✓ Don't scan] Scan anyway and disconnect clients

APs will only perform scans when no clients are connected. This setting only applies to APs without a dedicated scanning radio.

Should clients be able to connect to rogue SSIDs by default?

● Allow clients to connect to rogue SSIDs by default

Rogue SSIDs will only be contained if you specify them in the containment list below. The setting is appropriate when you have either non-Meraki APs or Meraki APs from other Organizations on your LAN.

○ Block clients from connecting to rogue SSIDs by default

Your Meraki APs will block clients from connecting to all rogue SSIDs by default. This setting is appropriate when you have all Meraki APs at your site and is better for security. You can allow connections to individual SSIDs by using the whitelist below.

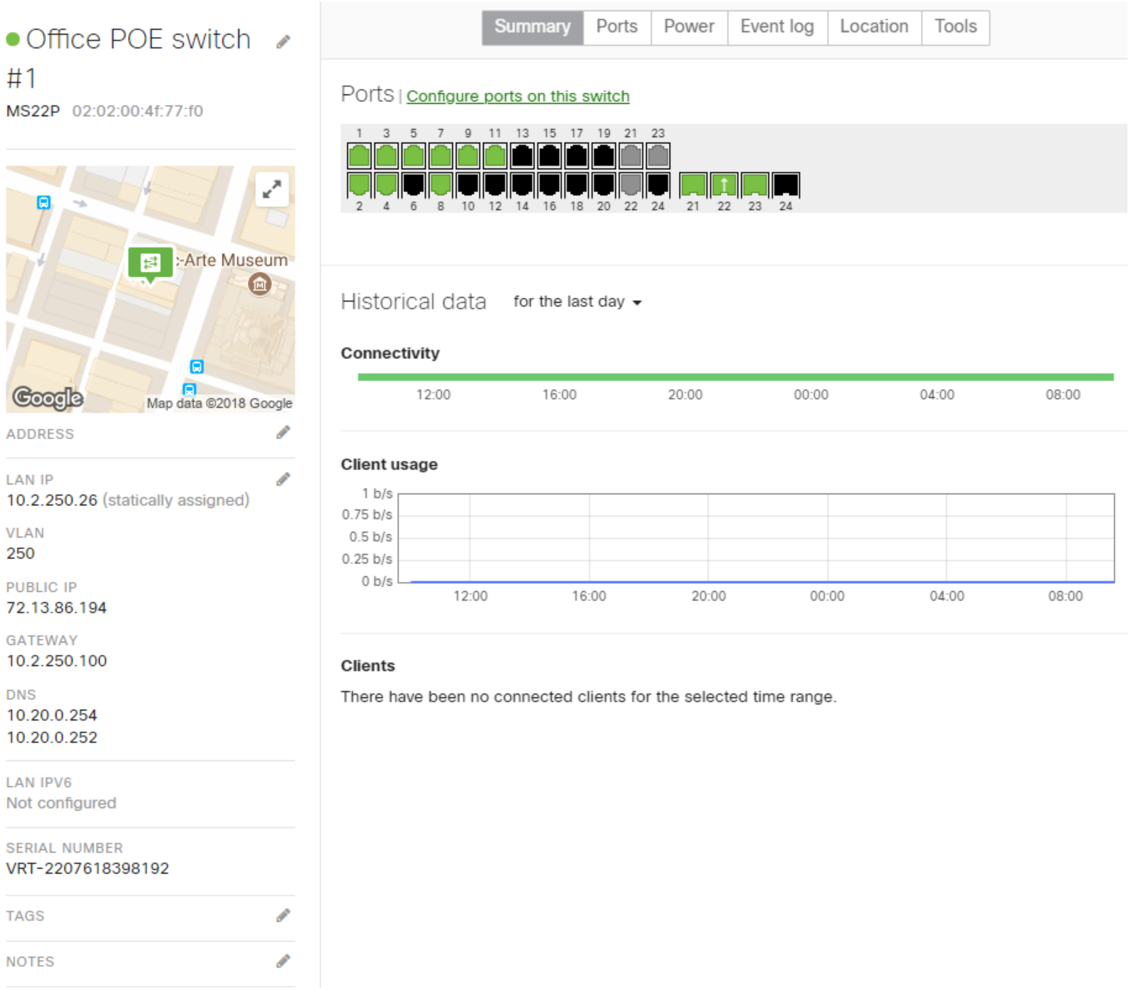
SSID blacklist

These rules will apply to SSIDs seen on and off the LAN.

SSID whitelist

Rogue or Other SSIDs matching these rules will be accessible for clients, overriding your default block policy and any that you've blacklisted.
Meraki won't send alerts about SSIDs matching rules on the whitelist.

As for wired infrastructure configuration, once the switches are registered you can individually configure the ports, its management IP and VLAN, the DNS, gateway, firmware, routing and DHCP, access policies, Quality of Service, MTUs, STP and Multicast settings. See Figure 23.



Office POE switch #1

MS22P 02:02:00:4f:77:f0

ADDRESS

LAN IP
10.2.250.26 (statically assigned)

VLAN
250

PUBLIC IP
72.13.86.194

GATEWAY
10.2.250.100

DNS
10.20.0.254
10.20.0.252

LAN IPV6
Not configured

SERIAL NUMBER
VRT-2207618398192

TAGS

NOTES

Ports | Configure ports on this switch

Historical data for the last day

Connectivity

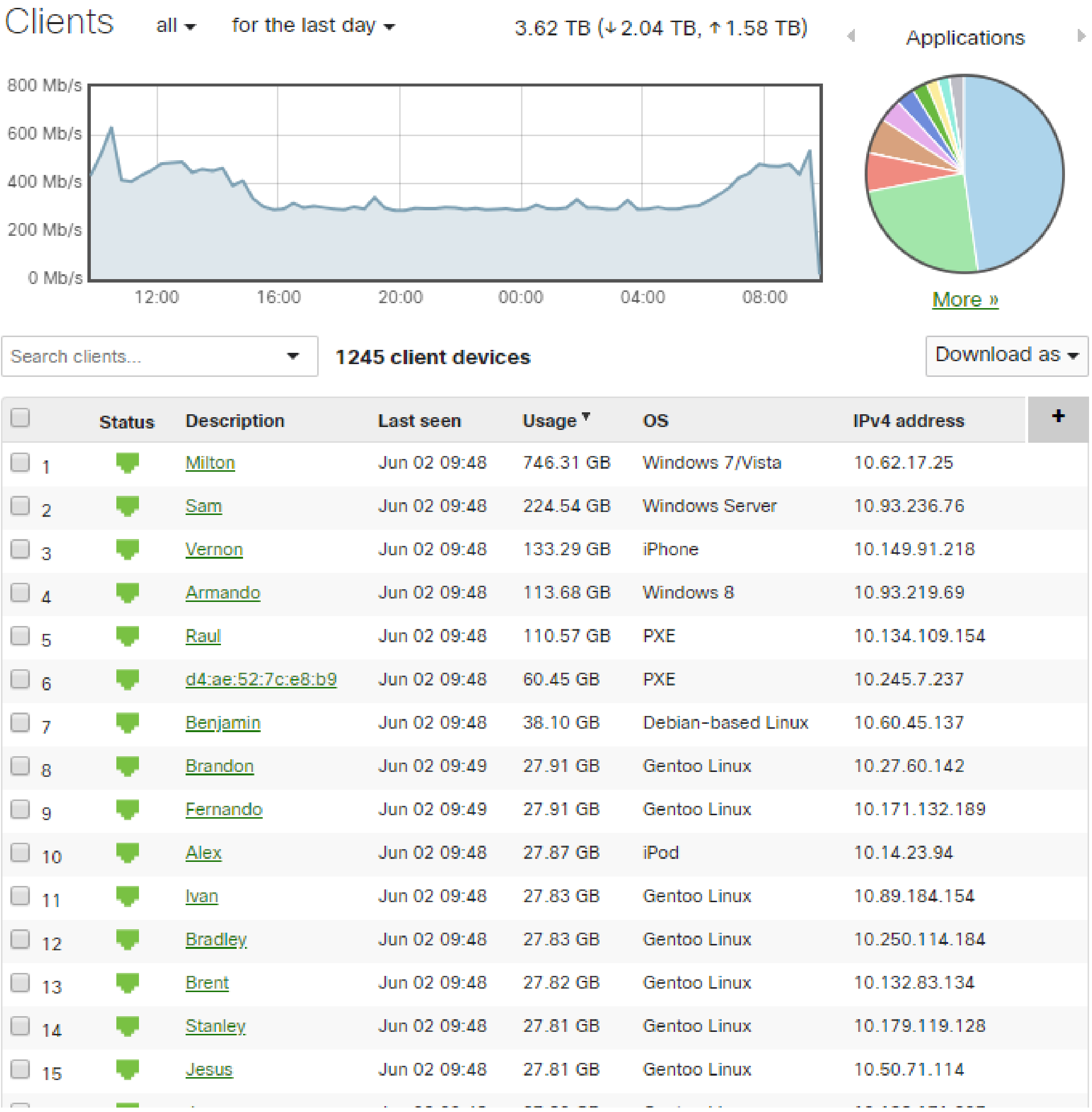
Client usage

Clients

There have been no connected clients for the selected time range.

Figure 23: Switch Configuration Summary Menu

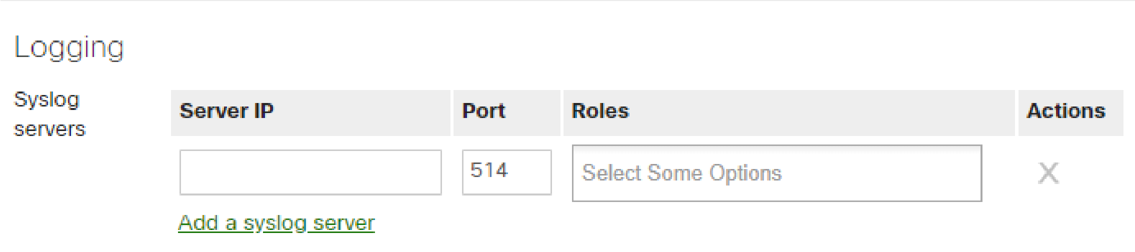
Also, a part from configuring the switches you can also monitor the traffic, application usage by client and bandwidth usage by client from the entire network. See Figure 24.



□	Status	Description	Last seen	Usage ▾	OS	IPv4 address	+
□ 1	🟩	Milton	Jun 02 09:48	746.31 GB	Windows 7/Vista	10.62.17.25	
□ 2	🟩	Sam	Jun 02 09:48	224.54 GB	Windows Server	10.93.236.76	
□ 3	🟩	Vernon	Jun 02 09:48	133.29 GB	iPhone	10.149.91.218	
□ 4	🟩	Armando	Jun 02 09:48	113.68 GB	Windows 8	10.93.219.69	
□ 5	🟩	Raul	Jun 02 09:48	110.57 GB	PXE	10.134.109.154	
□ 6	🟩	d4:ae:52:7c:e8:b9	Jun 02 09:48	60.45 GB	PXE	10.245.7.237	
□ 7	🟩	Benjamin	Jun 02 09:48	38.10 GB	Debian-based Linux	10.60.45.137	
□ 8	🟩	Brandon	Jun 02 09:49	27.91 GB	Gentoo Linux	10.27.60.142	
□ 9	🟩	Fernando	Jun 02 09:49	27.91 GB	Gentoo Linux	10.171.132.189	
□ 10	🟩	Alex	Jun 02 09:48	27.87 GB	iPod	10.14.23.94	
□ 11	🟩	Ivan	Jun 02 09:48	27.83 GB	Gentoo Linux	10.89.184.154	
□ 12	🟩	Bradley	Jun 02 09:48	27.83 GB	Gentoo Linux	10.250.114.184	
□ 13	🟩	Brent	Jun 02 09:48	27.82 GB	Gentoo Linux	10.132.83.134	
□ 14	🟩	Stanley	Jun 02 09:48	27.81 GB	Gentoo Linux	10.179.119.128	
□ 15	🟩	Jesus	Jun 02 09:48	27.81 GB	Gentoo Linux	10.50.71.114	

Figure 24: Network usage by client

As a best practice we recommend setting up a syslog server to backup all configuration changes, accesses, logins, wireless associations and general events that take place in our network. This can be done through a general option in the Network-Wide menu. See Figure 25



Logging

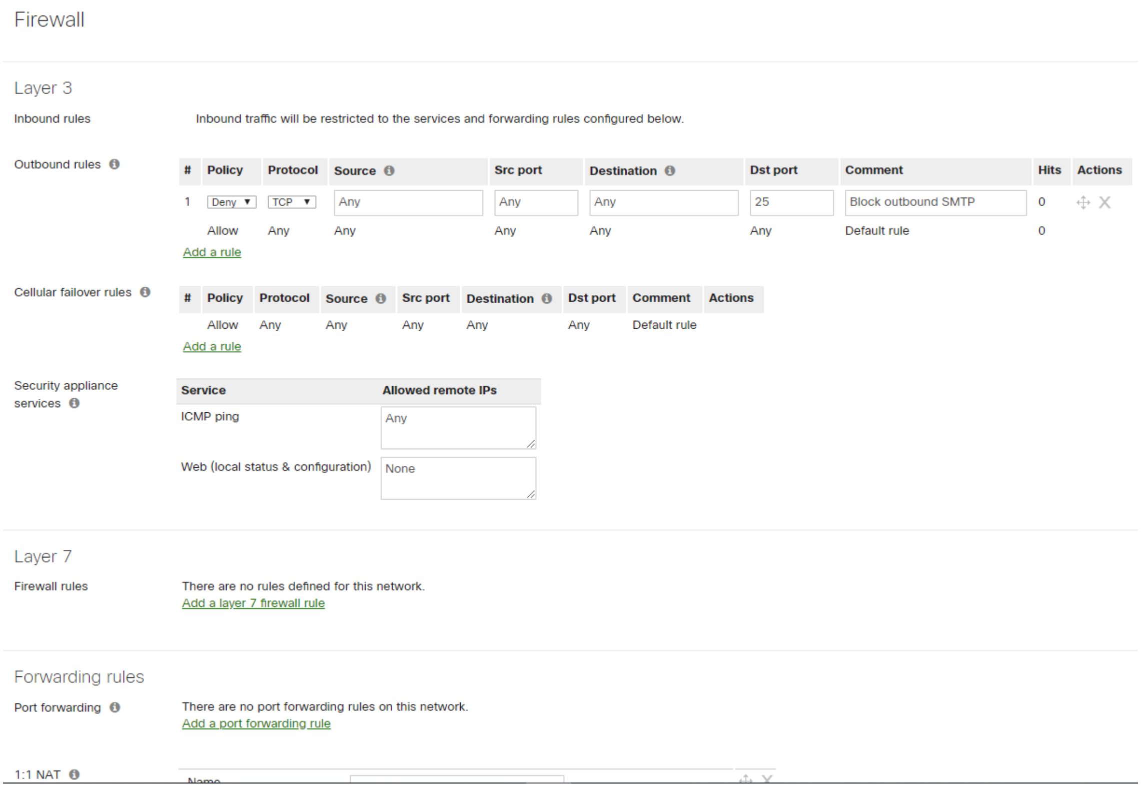
Syslog servers

Server IP	Port	Roles	Actions
	514	Select Some Options	X

Add a syslog server

Figure 25: Syslog Setup

As for our security configurations we can manage and define Layer 4 and Layer 7 firewall rules, forwarding rules, NATs, VPNs (see Figure 26), access control through Active Directory or local logins depending on the VLAN tag (see Figure 27), traffic shaping, load balancing, flow preferences and global bandwidth limits (see Figure 28).



Firewall

Layer 3

Inbound rules: Inbound traffic will be restricted to the services and forwarding rules configured below.

Outbound rules

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Hits	Actions
1	Deny ▼	TCP ▼	Any	Any	Any	25	Block outbound SMTP	0	✥ X
	Allow	Any	Any	Any	Any	Any	Default rule	0	

Add a rule

Cellular failover rules

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Actions
	Allow	Any	Any	Any	Any	Any	Default rule	

Add a rule

Security appliance services

Service	Allowed remote IPs
ICMP ping	Any
Web (local status & configuration)	None

Layer 7

Firewall rules: There are no rules defined for this network.
Add a layer 7 firewall rule

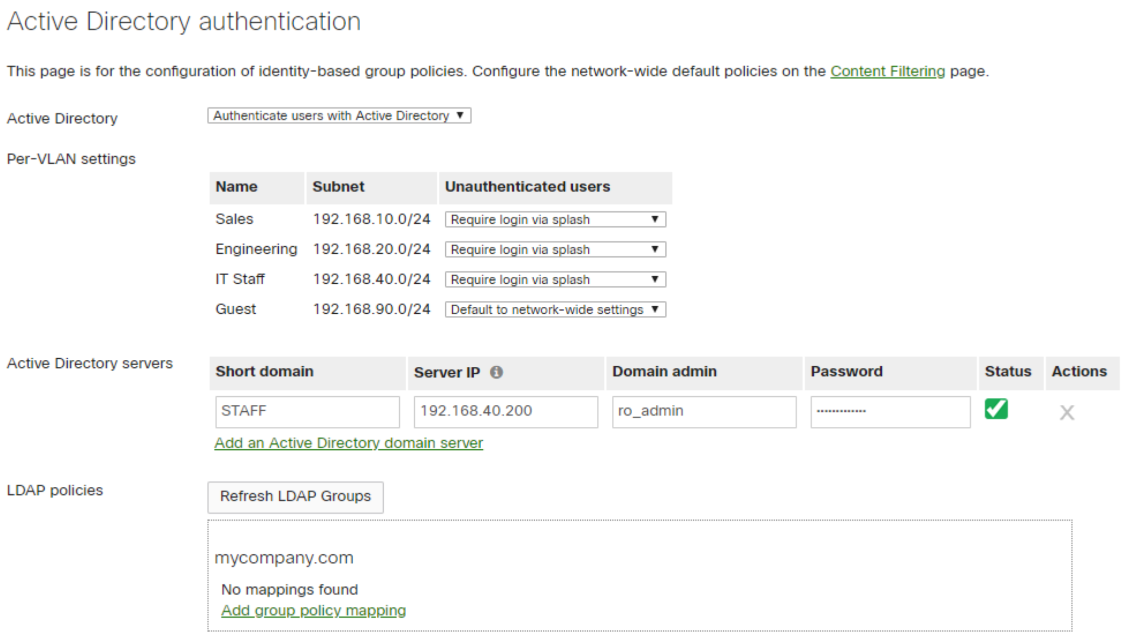
Forwarding rules

Port forwarding: There are no port forwarding rules on this network.
Add a port forwarding rule

1:1 NAT

Name

Figure 26: Firewall Options



Active Directory authentication

This page is for the configuration of identity-based group policies. Configure the network-wide default policies on the Content Filtering page.

Active Directory: Authenticate users with Active Directory ▾

Per-VLAN settings

Name	Subnet	Unauthenticated users
Sales	192.168.10.0/24	Require login via splash ▾
Engineering	192.168.20.0/24	Require login via splash ▾
IT Staff	192.168.40.0/24	Require login via splash ▾
Guest	192.168.90.0/24	Default to network-wide settings ▾

Active Directory servers

Short domain	Server IP	Domain admin	Password	Status	Actions
STAFF	192.168.40.200	ro_admin	•••••••••••••	✓	X

Add an Active Directory domain server

LDAP policies

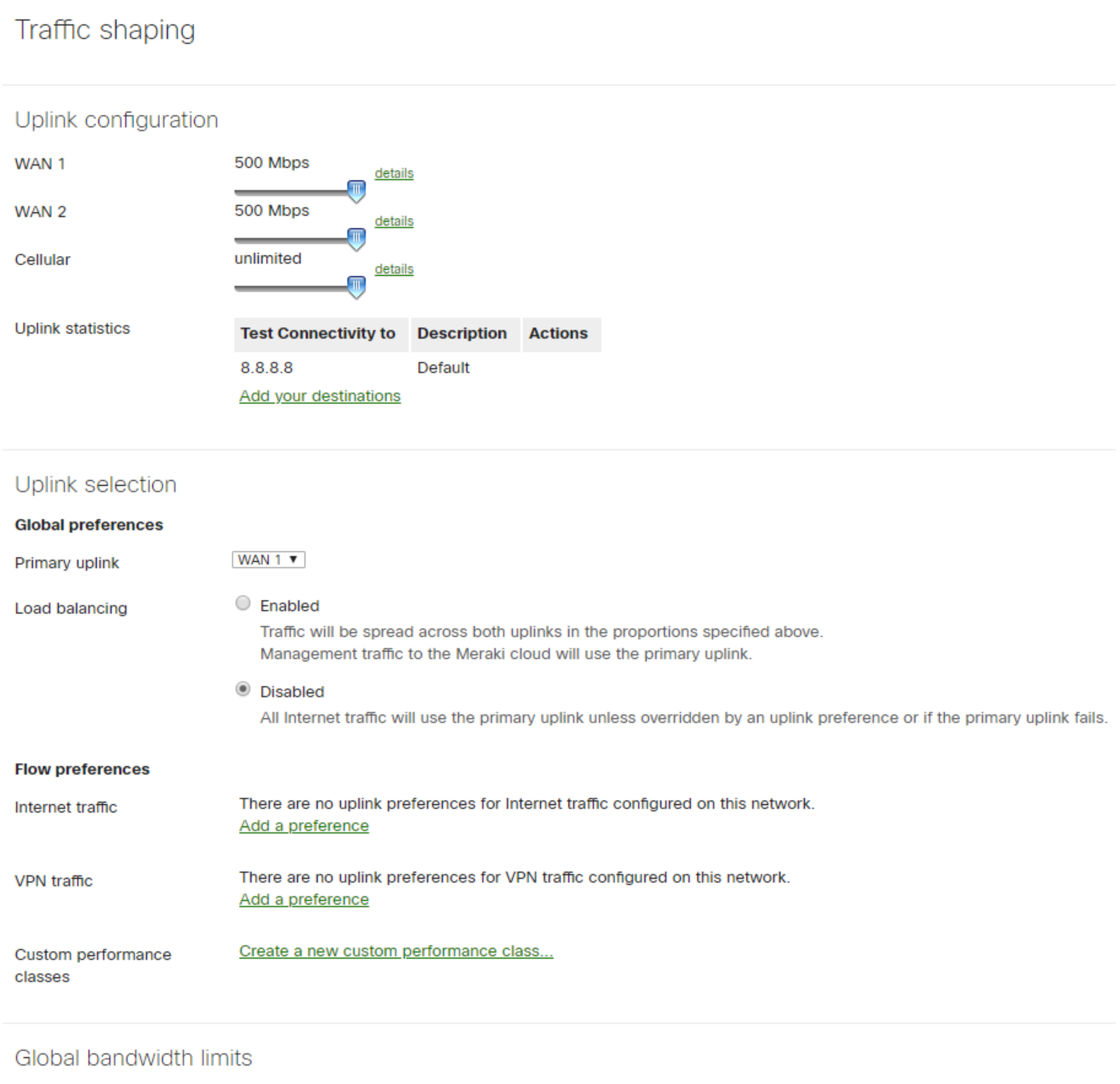
Refresh LDAP Groups

mycompany.com

No mappings found

Add group policy mapping

Figure 27: Access control options



Traffic shaping

Uplink configuration

WAN 1 500 Mbps details

WAN 2 500 Mbps details

Cellular unlimited details

Uplink statistics

Test Connectivity to	Description	Actions
8.8.8.8	Default	

Add your destinations

Uplink selection

Global preferences

Primary uplink: WAN 1 ▼

Load balancing

○ Enabled
Traffic will be spread across both uplinks in the proportions specified above.
Management traffic to the Meraki cloud will use the primary uplink.

● Disabled
All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Flow preferences

Internet traffic: There are no uplink preferences for Internet traffic configured on this network.
Add a preference

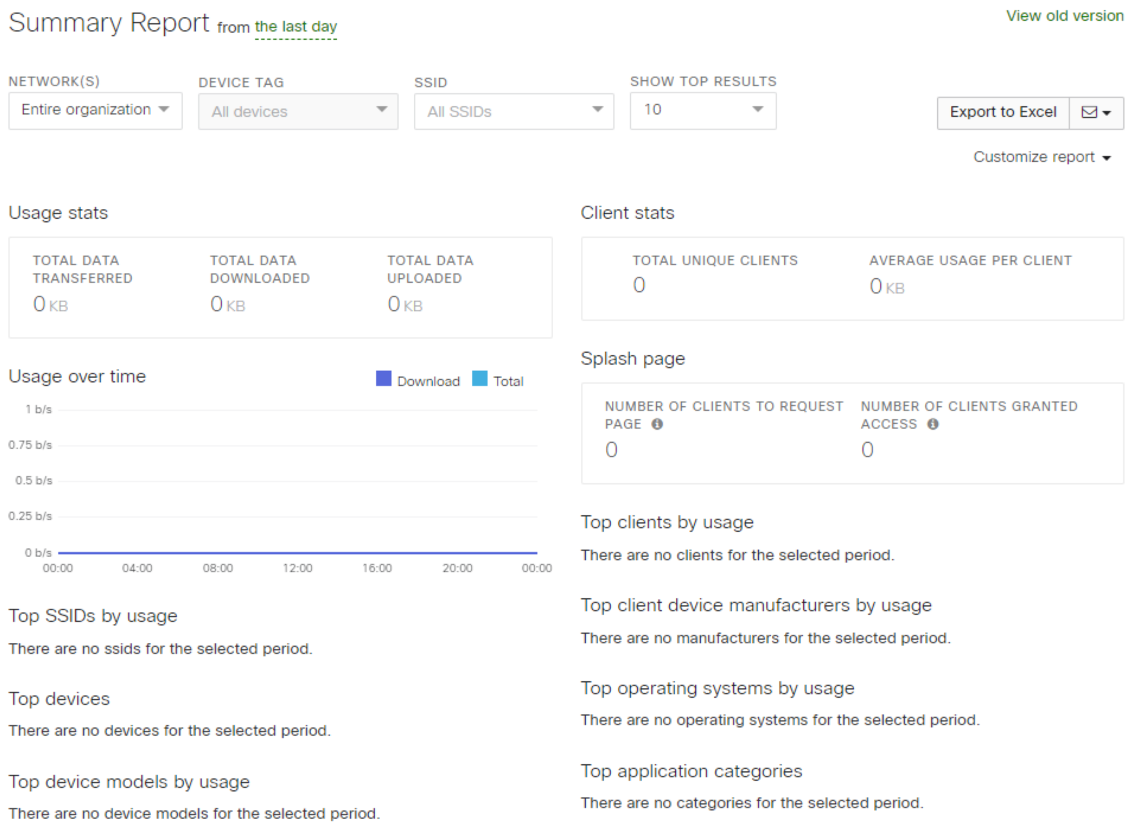
VPN traffic: There are no uplink preferences for VPN traffic configured on this network.
Add a preference

Custom performance classes: Create a new custom performance class...

Global bandwidth limits

Figure 28: Traffic Shaping options

A part from those options we also have a summary report dashboard which briefly shows all the events that took place in the network. See Figure 29.



Summary Report from the last day

View old version

NETWORK(S): Entire organization

DEVICE TAG: All devices

SSID: All SSIDs

SHOW TOP RESULTS: 10

Usage stats

TOTAL DATA TRANSFERRED	TOTAL DATA DOWNLOADED	TOTAL DATA UPLOADED
0 KB	0 KB	0 KB

Client stats

TOTAL UNIQUE CLIENTS	AVERAGE USAGE PER CLIENT
0	0 KB

Usage over time

Splash page

NUMBER OF CLIENTS TO REQUEST PAGE	NUMBER OF CLIENTS GRANTED ACCESS
0	0

Top clients by usage

There are no clients for the selected period.

Top SSIDs by usage

There are no ssids for the selected period.

Top client device manufacturers by usage

There are no manufacturers for the selected period.

Top devices

There are no devices for the selected period.

Top operating systems by usage

There are no operating systems for the selected period.

Top device models by usage

There are no device models for the selected period.

Top application categories

There are no categories for the selected period.

Figure 29:Summary Report Dashboard

5. Viability Analysis

5.1. Planning

5.1.1. Initial planning

In this section we will review all the initially planned activities to perform this project.

The entirety of the initial planning activities and their correlations are described in Table 3 and Figure 30.

TaskName	Start Date	Due date	Assigned to	Duration	Precedence
Define TFG **schema**	20/11/17	21/12/17	Pere Castillo Japón	24d	
Plan the timetables for the project	22/12/17	22/12/17	Pere Castillo Japón	1d	1
Gather information about the technology and the solutions proposed in previously planned events.	22/12/17	26/01/18	Pere Castillo Japón	26d	1
AvantProjecte	26/01/18	26/01/18	Pere Castillo Japón	0	3
Define our standard videogame event and its needs.	29/01/18	05/02/18	Pere Castillo Japón	6d	4
Search for possible network device candidates to take part in our solution.	06/02/18	27/02/18	Pere Castillo Japón	16d	5
Define a contact form, with questions to ask to the previously planned event's organizers.	28/02/18	02/03/18	Pere Castillo Japón	3d	6
Meet with the representatives of the companies that took place in the design and configuration of a network structure architecture solution for the previously planned events.	05/03/18	14/03/18	Pere Castillo Japón	8d	7
Analyze and filter the data gathered in meetings with the organizers to meet with our standard videogame event needs.	15/03/18	19/03/18	Pere Castillo Japón	3d	8
Partial delivery	19/03/18	19/03/18	Pere Castillo Japón	0	9
Propose a first possible implementation solution, with the filtered and analyzed data.	20/03/18	26/03/18	Pere Castillo Japón	5d	10
Design a first conceptual topology from the proposed solution.	27/03/18	06/04/18	Pere Castillo Japón	9d	11
Analyze the first conceptual topology for improvements and make those improvements (Iterate).	09/04/18	09/04/18	Pere Castillo Japón	1d	12

Configure through GNS3 a first schema of our network topology solution.	**10/04/18**	**17/04/18**	**Pere Castillo Japón**	**6d**	**13**
Analyze the first schema for improvements and make those improvements. **Iterate until we have a solid solution.**	**18/04/18**	**23/04/18**	**Pere Castillo Japón**	**4d**	**14**
Build a first prototype in real-life devices of our final implementation.	**24/04/18**	**01/05/18**	**Pere Castillo Japón**	**6d**	**15**
Analyze the prototype and improve it	**02/05/18**	**21/05/18**	**Pere Castillo Japón**	**14d**	**16**
Final delivery	**21/05/18**	**21/05/18**	**Pere Castillo Japón**	**0**	**17**

Table 3: Project's initial planning

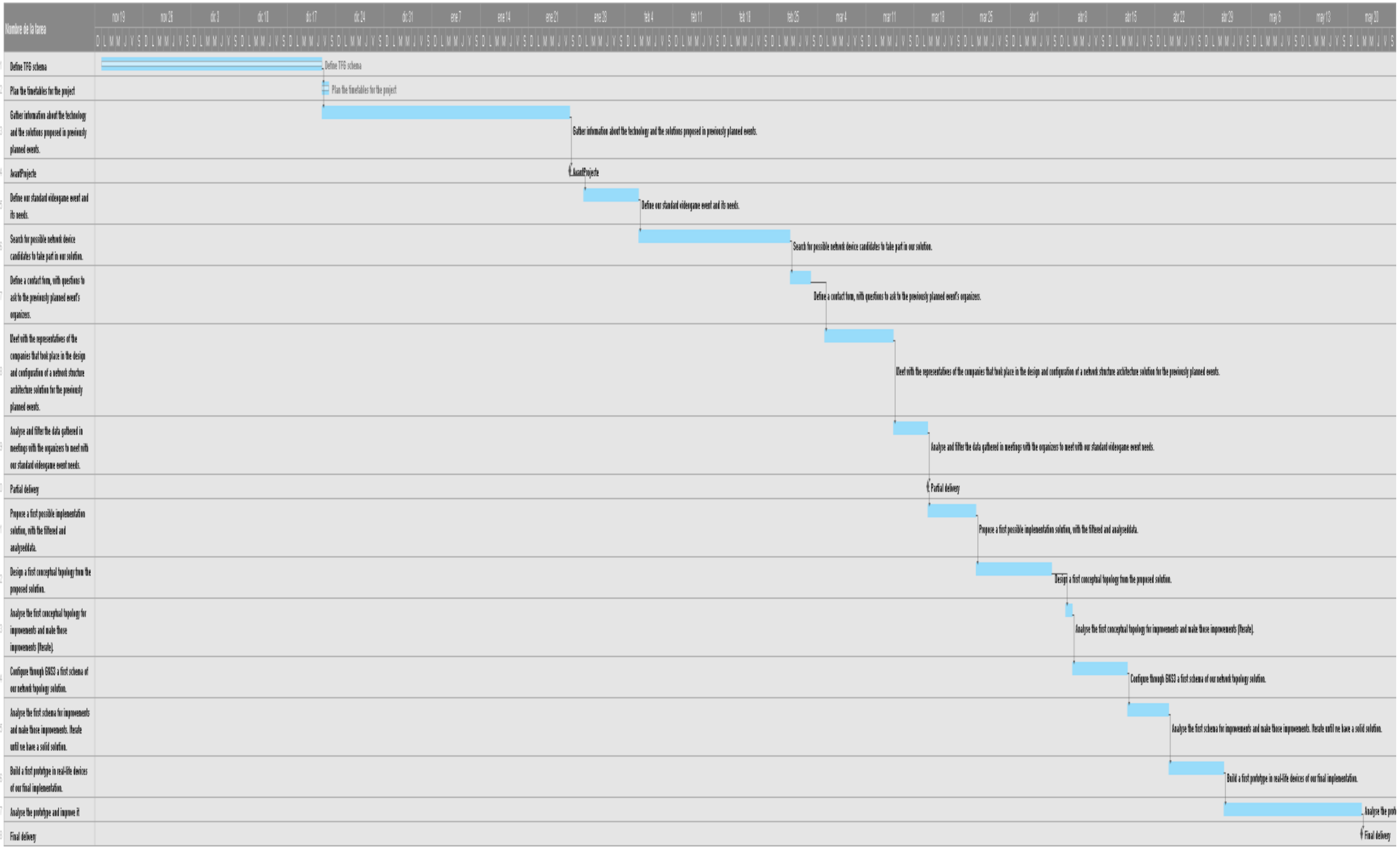


Figure 30: Gantt diagram of the initial planning

5.2. Planning changes

Initially we planned to use information gathered from previous event organizers and companies, however, we realized that most of the event organizers knew very little about their network infrastructure configuration, which shows that those people who configured the entire infrastructure where external organizations somehow related to them. To solve this issue, we took information from Cisco's public Case Studies which had similar points to an event organization and adapted their requirements and network needs to our videogame event case.

A part from this issue, we decided to implement an entire use case for our videogame event and explain possible topology solutions and configurations instead of using Lucid Chart and GNS3 to design and configure only one topology.

Another major fact to consider not using GNS3 for our device emulation is the lack of ISOs from the devices we want to use for our chosen solution

5.3. Technical viability

Since this project is a based on a theoretical study of the state of the art and establishment of best practices to follow through a Case study the technical requirements of this project consist of the following:

1- Internet connectivity to access data and information about different network architectures from Cisco.

2- A personal computer to develop the project.

3- Cisco Packet Tracer software to design the architecture of our network solution proposal.

4- Access to a limited-feature demonstration version of a Meraki Dashboard to explain the solution we propose.

In our previous planning we required access to a LucidChart educational license and a GNS3 compatible IOS database. However, the LucidChart educational license did not offer as much as we intended and the GNS3 compatible IOS database was not accessible throughout the development of the project. Therefore, we had to change the requirements to work with Cisco Packet Tracer and the demonstration version of the Meraki Dashboard.

5.4. Economical viability analysis

Since this project is a based on a theoretical study of the state of the art and establishment of best practices to follow through a Case study, therefore the project can only be charged to an enterprise if they request this kind of studies. Otherwise there is no economical viability of doing a project of such scale.

We also added an economical viability analysis to the Case Study solution proposal. Refer to page 46 for more detailed information.

5.4.1. Budget

This projects budget and production cost is calculated through the average salary of a junior engineer and the average cost amortization of the device that will be used for the development of this project, in this case a personal computer. See Table 4.

Item	Quantity	Price per unit	Total
Engineer hours of work	600	15,00€	9.000,00€
Computer	1	1.500,00€*4y*(3/4)*(20/50)	1.800,00€
Total			10.800,00€

Table 4: Project Budget

The computer price was calculated through the following formula: Price*life-span*(project time in years)*(hours of use per week for the project/total hours of use per week).

5.5. Environmental viability

Being a theoretical study the only environmental impacts are those coming from the malfunctioning of the personal computer, such as over-heat, static discharges or battery poisoning. This is solved through a personal computer or broken parts replacement.

5.6. Legal Aspects

This project is protected under the CC BY-NC-SA Creative Commons license.

Disclaimer: All resources used in this project are under the “Educational Purposes, Fair Use: non-profit and non-commercial purposes” regulation.

6. Conclusions

From the development of our project we can draw he following conclusions:

1- There is no videogame event which is exactly the same as another. Each event has different and precise features and requirements, which make them unique. Therefore each one of them must have a customized configuration.

2- Even though no event is equal to another, there are general characteristics that must be taken into account in any event network design, which we defined as zones and their network needs.

3- For just one event there are multiple solutions. In this project we encountered a vast amount of solutions to the same requirement event just working with one manufacturer, Cisco. Therefore the amount of solutions that can be provided taking into account multiple manufacturers is enormous.

7. Possible enhancements

As this project's possible enhancements we have the following:

1- Work with multiple manufacturers: Take into account solutions from Huawei, Netgear, Juniper or other manufacturers a part from Cisco.

2- Take into account other kind of events that require a strong network configuration a part from videogame events to use them as reference when defining network event solutions.

3- Define a bigger videogame Case Study: Bigger videogame events require of a more complex network infrastructure design and configuration.

4- Enter into more detail when explaining the configuration guide for the Case Study.

8. Bibliography

1. **González, Alberto.** Vandal. *Vandal.* [Online] 30 6 2016. [Cited: 15 11 2017.] http://www.vandal.net/noticia/1350678619/la-liga-de-videojuegos-profesional-y-el-evento-gamergy-regresaran-en-diciembre/.

2. **La Vanguardia.** La Vanguardia. *La Vanguardia.* [Online] 10 10 2017. [Cited: 6 11 2017.] http://www.lavanguardia.com/economia/20171008/431906524861/barcelona-games-world-visitantes.html.

3. **Euskadi Tecnologia.** Euskadi Tecnologia. *Euskadi Tecnologia.* [Online] 26 7 2017. [Cited: 5 11 2017.] https://www.euskaditecnologia.com/euskal-encounter-25-valoracion/.

4. **Wikipedia.** Wi-Fi. *Wi-Fi.* [Online] Wikipedia, 7 Marzo 2018. [Cited: 10 Marzo 2018.] https://en.wikipedia.org/wiki/Wi-Fi.

5. —. IEEE 802.11 standard. *IEEE 802.11 standard.* [Online] Wikipedia, 20 Marzo 2018. [Cited: 26 Marzo 2018.] https://en.wikipedia.org/wiki/IEEE_802.11.

6. —. IEEE 802.1Q standard. *IEEE 802.1Q standard.* [Online] Wikipedia, 22 Marzo 2018. [Cited: 26 Marzo 2018.] https://en.wikipedia.org/wiki/IEEE_802.1Q.

7. **Thomas, Thomas M.** Wireless Security. *Wireless Security.* [Online] Cisco Press, 16 Julio 2004. [Cited: 26 Marzo 2018.] http://www.ciscopress.com/articles/article.asp?p=177383&seqNum=5.

8. **Wikipedia.** Computer Security. *Computer Security.* [Online] Wikipedia, 26 Marzo 2018. [Cited: 26 Marzo 2018.] https://en.wikipedia.org/wiki/Computer_security.

9. —. Intrusion Detection Systems. *Intrusion Detection Systems.* [Online] Wikipedia, 23 Febrero 2018. [Cited: 30 Marzo 2018.] https://en.wikipedia.org/wiki/Intrusion_detection_system.

10. —. Firewalls. *Firewalls.* [Online] Wikipedia, 28 Marzo 2018. [Cited: 30 Marzo 2018.] https://en.wikipedia.org/wiki/Firewall_(computing).

11. **Meraki.** Meraki Docs. *Meraki Docs.* [Online] Cisco Meraki, 12 Diciembre 2017. [Cited: 5 Marzo 2018.] https://documentation.meraki.com/.