ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA
GRADO EN INGENIERIA DE COMPUTADORES

DISEÑO, IMPLEMENTACIÓN Y SIMULACIÓN DEL INTERNET DE LAS COSAS (IdC) MEDIANTE SENSORES EN UNA RED CORPORATIVA

DESIGN, IMPLEMENTATION AND SIMULATION OF INTERNET OF THINGS (IoT) USING SENSORS IN A CORPORATE NETWORK

Realizado por
José Luis Reina Gil
Tutorizado por
Cipriano Galindo Andrades
Departamento
Ingeniería de Sistemas y Automática

UNIVERSIDAD DE MÁLAGA
MÁLAGA, OCTUBRE 2018

Fecha defensa:
El secretario del Tribunal

RESUMEN

Este Trabajo Fin de Grado (TFG) plantea el caso de una empresa genérica, que requiere de la realización de un diseño de red estructurado y segmentado partiendo de una serie de requisitos previos y de ciertas limitaciones tanto físicas como lógicas. El sistema a diseñar incluye tanto una red de ordenadores, como elementos del Internet de las Cosas (IdC), como por ejemplo sensores ambientales, actuadores, etc.

El diseño de red estructurado y segmentado resultante será testeado con un simulador de red, que permite, además de simular redes convencionales, la inclusión de elementos IdC y su interconexión.

Para llegar a un diseño óptimo, se debe llevar a cabo una labor compleja que requiere de un estudio preliminar detallado antes de realizar el propio diseño y un futuro despliegue real. Dicho estudio se realiza teniendo en cuenta las necesidades de dicha empresa genérica.

El punto de partida de este TFG comienza con un análisis preliminar de la empresa y de un estudio pormenorizado de qué elementos son necesarios para llegar a la consecución de los requerimientos inicialmente marcados, teniendo en cuenta las limitaciones físicas y lógicas del entorno.

Una vez se han establecido los requerimientos y se ha realizado el estudio pormenorizado se pasa a definir el diseño, implementándolo en el simulador de red incluyendo todos los elementos de IdC.

Posteriormente, se simulan distintos comportamientos de los elementos de IdC y de la red definida para comprobar su correcto funcionamiento. Finalmente, se aporta el diseño optimizado a la empresa genérica, la cual será la responsable de un posible despliegue en el futuro empleando para ello, los mismos elementos utilizados en el simulador.

Palabras claves: internet de las cosas, sensor, simulador, microcontroladora, red corporativa, cisco packet tracer

ABSTRACT

This Final Degree Project (FDP) presents the case of a company which demands the implementation of a structured and segmented network design based on a series of previous requirements and some physical and logical limitations. The system to be designed includes both a network of computers and elements of the Internet of Things (IoT), such as environmental sensors, actuators, etc.

The structured and segmented network design that results will be tested with a network simulator, which will allow the inclusion of IoT elements and their interconnection besides the simulation of conventional networks.

In order to achieve an optimal design, a detailed preliminary study is needed before the realization of the design itself and its implementation/deployment. This research is carried out taking into consideration the company needs.

This Final Degree Project (FDP) begins with a preliminary analysis of the company and a detailed study of the components/elements which are needed to meet the initial requirements, keeping in mind the physical and logical limitations of the environment.

Once the requirements have been determined and the detailed study has been carried out, the design is defined and implemented in the network simulator including all the IoT elements.

Afterwards, the different behaviors of the IoT elements and the defined network are simulated to verify its right functioning. At last, the optimized design is provided to the company, which will be responsible for its future deployment making use of the same elements used in the simulator.

Keywords: internet of things, sensor, simulator, microcontroller, corporate network, cisco packet tracer

ÍNDICE

INTRODUCCIÓN **1**

OBJETIVOS 1

SIMULADOR 3

ESTRUCTURA DEL DOCUMENTO 4

CAPÍTULO 1 ..... **7**

1.1 INTERNET DE LAS COSAS (IDC) 7

1.2 CISCO SYSTEMS 8

1.3 METODOLOGÍA 9

CAPÍTULO 2 ..... **11**

2.1 FASE DE PREPARACIÓN 11

2.2 FASE DE PLANIFICACIÓN 13

2.2.1 CARACTERIZACIÓN *14*

2.2.2 UBICACIÓN *15*

PLANTA 4ª 16

PLANTA 5ª 17

PLANTA 6ª 19

FACHADA DEL EDIFICIO 21

2.2.3 RESTRICCIONES *22*

2.3 FASE DE DISEÑO 24

2.3.1 DIRECCIONAMIENTOS DE RED *24*

DIRECCIONAMIENTO PARA LAS PLANTAS 24

DIRECCIONAMIENTO PARA LOS ELEMENTOS IDC 26

DIRECCIONAMIENTO PARA LA ADMINISTRACIÓN 27

DIRECCIONAMIENTO PARA EL CPD 27

2.3.2 DISPOSITIVOS UTILIZADOS *28*

INFRAESTRUCTURA DE RED 28

CONMUTADORES DE LA CAPA DE ACCESO 28

CONMUTADOR DE LA CAPA DE DISTRIBUCIÓN-NÚCLEO 31

ENRUTADOR CORPORATIVO 33

SERVIDOR CORPORATIVO 34

EQUIPOS INFORMÁTICOS 35

ELEMENTOS IDC 35

LUCES AUTOMÁTICAS 35

ACCESO A SALA DE COMUNICACIONES 36

BLOQUEO DE VENTANAS POR VIENTO 38

VENTILACIÓN AUTOMÁTICA 39

DETECTOR DE HUMO 40
PUERTA DE ACCESO A PLANTA 41
ACCESO AL CPD 42
BLOQUEO DE VENTANA DEL CPD POR VIENTO 43
VENTILACIÓN AUTOMÁTICA DEL CPD 44
AIRE ACONDICIONADO CENTRALIZADO DEL CPD 45
MONITOR DE FUEGO EN EL CPD 46
AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA 47
LUCES AUTOMÁTICAS DE LA FACHADA 49
SERVIDOR IDC 50
2.3.3 LISTADO DE EQUIPAMIENTO REQUERIDO 53

CAPÍTULO 3 57

3.1 FASE DE IMPLEMENTACIÓN 57
3.1.1 CISCO PACKET TRACER 57
3.1.2 MODOS DE VISUALIZACIÓN 59
3.1.3 INFRAESTRUCTURA DE RED 61
CONFIGURACION DE LA INFRAESTRUCTURA DE RED 64
CONEXIÓN FÍSICA DE LOS DISPOSITIVOS DE RED 66
CONMUTADORES CAPA DE ACCESO 67
VISUALIZACIÓN LÓGICA 67
VISUALIZACIÓN FÍSICA 68
ENDURECIMIENTO DEL DISPOSITIVO 69
HABILITAR PORTFAST 69
PROTECCIÓN DE INTERFAZ POR MAC 70
PROTECCIÓN POR SUPLANTACIÓN DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) 71
PROTECCIÓN DE TORMENTA BROADCAST 72
DESACTIVACIÓN DEL SERVICIO CISCO DISCOVERY PROTOCOL (CDP) 74
CONFIGURACIÓN DE INTERFACES TRONCALES (TRUNK) 74
CONFIGURACIÓN DEL CLIENTE VLAN TRUNKING PROTOCOL (VTP) 75
CONFIGURACIÓN DEL AGREGADO DE ENLACES (LAG) 76
CONMUTADOR DE CAPA DE DISTRIBUCIÓN-NÚCLEO 78
VISUALIZACIÓN LÓGICA 78
VISUALIZACIÓN FÍSICA 79
ENDURECIMIENTO DEL DISPOSITIVO 80
CONFIGURACIÓN DEL SERVIDOR DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) 80
CONFIGURACIÓN DE INTERFACES TRONCALES 83
CONFIGURACIÓN DEL SERVIDOR VLAN TRUNKING PROTOCOL (VTP) 84
CONFIGURACIÓN DE ROOT SPANNING-TREE 85
CONFIGURACIÓN DEL AGREGADO DE ENLACES (LAG) 86
ENRUTAMIENTO ENTRE VLANS Y RUTA POR DEFECTO 88
RESTRICCIONES ENTRE VLANS 90

ENRUTADOR CORPORATIVO 101
VISUALIZACIÓN LÓGICA 101
VISUALIZACIÓN FÍSICA 102
ENDURECIMIENTO DEL DISPOSITIVO 103
CONFIGURACIÓN DE TRADUCCIÓN DE DIRECCIONES DE RED (NAT) 103
ENRUTAMIENTO BÁSICO Y RUTA POR DEFECTO 104
CONFIGURACIÓN DEL DIRECCIONAMIENTO IP 106
3.1.4 EQUIPAMIENTO 108
SERVIDOR CORPORATIVO 108
VISUALIZACIÓN LÓGICA 108
VISUALIZACIÓN FÍSICA 109
EQUIPOS INFORMÁTICOS 111
VISUALIZACIÓN LÓGICA 111
VISUALIZACIÓN FÍSICA 112
ELEMENTOS IDC 114
LUCES AUTOMÁTICAS 115
ACCESO A SALA DE COMUNICACIONES 117
BLOQUEO DE VENTANAS POR VIENTO 119
VENTILACIÓN AUTOMÁTICA 120
DETECTOR DE HUMO 122
PUERTA DE ACCESO A PLANTA 125
ACCESO AL CPD 126
BLOQUEO DE VENTANA DEL CPD POR VIENTO 128
VENTILACIÓN AUTOMÁTICA DEL CPD 130
AIRE ACONDICIONADO CENTRALIZADO DEL CPD 131
MONITOR DE FUEGO EN EL CPD 133
AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA 135
LUCES AUTOMÁTICAS DE LA FACHADA 137
SERVIDOR IDC 139
3.1.5 IMPLEMENTACIÓN FINAL 144
3.2 FASE DE OPERACIÓN 146
CORREO ELECTRÓNICO ENTRE USUARIOS 146
RESTRICCIONES ENTRE DEPARTAMENTOS 147
ACCESO AL SERVIDOR IDC DESDE EL EXTERIOR 149
ELEMENTO IDC: ACCESO A SALA DE COMUNICACIONES 150
ELEMENTO IDC: ACCESO AL CPD 152
ELEMENTO IDC: DETECTOR DE FUEGO 153
ELEMENTO IDC: AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA 154
3.3 FASE DE OPTIMIZACIÓN 155
CONCLUSIONES Y TRABAJOS FUTUROS 157

REFERENCIAS BIBLIOGRÁFICAS..... 161

ANEXOS TÉCNICOS 163

ÍNDICE DE FIGURAS Y TABLAS

FIGURA 1. SIMULADOR CISCO PACKET TRACER *3*
FIGURA 2. ENTORNO DEL SIMULADOR CISCO PACKET TRACER *4*
FIGURA 3. LOGO CISCO SYSTEMS *9*
FIGURA 4. FASES PPDIOO *10*
FIGURA 5. MODELO JERÁRQUICO DE TRES CAPAS *12*
FIGURA 6. MODELO JERÁRQUICO DE DOS CAPAS *14*
FIGURA 7. MODELO JERÁRQUICO DE DOS CAPAS COMPACTO *15*
FIGURA 8. PLANO DEPARTAMENTAL Y ELEMENTOS IDC 4ª PLANTA *16*
TABLA 1. ELEMENTOS IDC 4ª PLANTA *17*
FIGURA 9. PLANO DEPARTAMENTAL Y ELEMENTOS IDC 5ª PLANTA *18*
TABLA 2. ELEMENTOS IDC 5ª PLANTA *19*
FIGURA 10. PLANO DEPARTAMENTAL Y ELEMENTOS IDC 6ª PLANTA *20*
TABLA 3. ELEMENTOS IDC 6ª PLANTA *21*
FIGURA 11. FACHADA ELEMENTOS IDC *21*
TABLA 4. ELEMENTOS IDC FACHADA *22*
FIGURA 12. RESTRICCIONES ESTABLECIDAS ENTRE LAS PLANTAS *23*
TABLA 5. DIRECCIONAMIENTO IP *25*
FIGURA 13. DIRECCIONAMIENTO IP Y CONEXIONES PERMITIDAS *25*
TABLA 6. DIRECCIONAMIENTO IP - VLAN 456 ..... *26*
FIGURA 14. CONEXIÓN DE LOS ELEMENTOS IDC CON EL SERVIDOR IDC *26*
TABLA 7. DIRECCIONAMIENTO IP - VLAN 250 ..... *27*
TABLA 8. DIRECCIONAMIENTO IP - VLAN 654 ..... *28*
TABLA 9. RESUMEN DE INTERFACES *29*
TABLA 10. RESUMEN DE INTERFACES EN CAPA DISTRIBUCIÓN-NÚCLEO *33*
TABLA 11. RESUMEN DE INTERFACES EN EL ENRUTADOR CORPORATIVO *34*
TABLA 12. LUCES AUTOMÁTICAS *36*
TABLA 13. LUCES AUTOMÁTICAS OPTIMIZADAS *36*
TABLA 14. ACCESO A SALA DE COMUNICACIONES *37*
TABLA 15. ACCESO A SALA DE COMUNICACIONES OPTIMIZADO *38*
TABLA 16. BLOQUEO DE VENTANAS POR VIENTO *39*
TABLA 17. VENTILACIÓN AUTOMÁTICA *40*
TABLA 18. DETECTOR DE HUMO *41*
TABLA 19. PUERTA DE ACCESO A PLANTA *42*
TABLA 20. ACCESO AL CPD *43*
TABLA 21. BLOQUEO DE VENTANA DEL CPD POR VIENTO *44*
TABLA 22. VENTILACIÓN AUTOMÁTICA DEL CPD *45*
TABLA 23. AIRE ACONDICIONADO CENTRALIZADO DEL CPD *46*
TABLA 24. AIRE ACONDICIONADO CENTRALIZADO DEL CPD OPTIMIZADO *46*
TABLA 25. MONITOR DE FUEGO EN EL CPD *47*
TABLA 26. MONITOR DE FUEGO EN EL CPD OPTIMIZADO *47*
TABLA 27. AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA *48*
TABLA 28. LUCES AUTOMÁTICAS DE LA FACHADA *49*
TABLA 29. LUCES AUTOMÁTICAS DE LA FACHADA OPTIMIZADAS *50*
TABLA 30. REGLAS A IMPLEMENTAR *52*
TABLA 31. RESUMEN DE EQUIPOS INFORMÁTICOS Y SERVIDORES NECESARIOS *53*
TABLA 32. RESUMEN DE ELEMENTOS IDC *54*
TABLA 33. RESUMEN DE ELEMENTOS IDC POR UBICACIÓN *55*
TABLA 34. ELEMENTOS DE LA INFRAESTRUCTURA DE RED *55*

FIGURA 15. ENTORNO DE TRABAJO EN CISCO PACKET TRACER 58
FIGURA 16. MODOS DE VISUALIZACIÓN..... 59
FIGURA 17. PLANO DE MÁLAGA CAPITAL Y ACCESO AL EDIFICIO..... 60
FIGURA 18. ALZADO Y ACCESO A LAS PLANTAS 60
FIGURA 19. MAPA DE PLANTA..... 61
FIGURA 20. ARMARIO RACK CON CONMUTADORES CONECTADOS..... 61
TABLA 35. ELECCIÓN DE LOS DISPOSITIVOS DE RED..... 62
FIGURA 21. SWITCH 3650 24PS CON DOBLE FUENTE DE ALIMENTACIÓN 62
TABLA 36. NOMENCLATURA DE LOS DISPOSITIVOS DE RED 63
FIGURA 22. DISPOSITIVOS DE RED EN VISUALIZACIÓN LÓGICA..... 63
FIGURA 23. ACCEDIENDO A CADA DISPOSITIVO DE RED SE PUEDE ABRIR LA LÍNEA DE COMANDO CLI..... 64
FIGURA 24. VISUALIZACIÓN DE LA LÍNEA DE COMANDO CLI..... 65
FIGURA 25. LÍNEA DE COMANDO CLI..... 65
TABLA 37. CONEXIONES FÍSICAS ENTRE LOS DISPOSITIVOS DE RED..... 66
FIGURA 26. DISPOSITIVOS INTERCONECTADOS EN VISUALIZACIÓN LÓGICA..... 67
FIGURA 27. DISPOSITIVOS DE LA CAPA DE ACCESO EN VISUALIZACIÓN LÓGICA 68
FIGURA 28. ARMARIO RACK 4ª PLANTA 68
TABLA 38. ENDURECIMIENTO DEL DISPOSITIVO DE RED 69
FIGURA 29. PORTFAST NO ACTIVADO (COLOR NARANJA) VS PORTFAST ACTIVADO (COLOR VERDE) 70
FIGURA 30. COMANDO PARA HABILITAR PORTFAST..... 70
TABLA 39. PROTECCIÓN DE INTERFAZ 71
TABLA 40. PROTECCIÓN POR SUPLANTACIÓN DE DHCP 72
TABLA 41. PROTECCIÓN DE TORMENTA BROADCAST..... 73
TABLA 42. DESACTIVACIÓN DEL PROTOCOLO CDP 74
TABLA 43. CONFIGURACIÓN DE INTERFACES TRONCALES EN LA CAPA DE ACCESO..... 75
TABLA 44. CONFIGURACIÓN DEL CLIENTE VTP 76
TABLA 45. CONFIGURACIÓN DE ETHERCHANNEL ACTIVO 78
FIGURA 31. CAPA DE DISTRIBUCIÓN-NÚCLEO EN VISUALIZACIÓN LÓGICA 79
FIGURA 32. CONMUTADOR DE LA CAPA DE DISTRIBUCIÓN-NÚCLEO EN VISUALIZACIÓN FÍSICA..... 79
TABLA 46. RANGO DE DIRECCIONES IP SEGÚN PLANTA Y VLAN..... 80
TABLA 47. CONFIGURACIÓN DEL SERVIDOR DHCP..... 81
FIGURA 33. EXCLUSIONES DE LOS GRUPOS 82
FIGURA 34. DEFINICIÓN DE LOS GRUPOS DEL SERVIDOR DHCP 82
TABLA 48. ASIGNACIÓN DE DIRECCIÓN IP A CADA VLAN 83
TABLA 49. CONFIGURACIÓN DE LAS INTERFACES TRONCALES EN LA CAPA DE DISTRIBUCIÓN-NÚCLEO 84
TABLA 50. CONFIGURACIÓN DEL SERVIDOR VTP..... 84
TABLA 51. RESUMEN DE LOS ENLACES ETHERCHANNEL 87
TABLA 52. CONFIGURACIÓN DE ENLACES ETHERCHANNEL PASIVOS 87
FIGURA 35. ENLACES ETHERCHANNEL EN FUNCIONAMIENTO..... 88
TABLA 53. ENRUTAMIENTO CON EL PROTOCOLO RIP 89
TABLA 54. RUTA POR DEFECTO..... 89
TABLA 55. CONFIGURACIÓN DE LA INTERFAZ POR DEFECTO 90
TABLA 56. RESTRICCIONES VLAN 41..... 90
TABLA 57. ACL VLAN 41..... 91
TABLA 58. ACL APLICADA A VLAN 41 91
TABLA 59. RESTRICCIONES VLAN 42..... 92
TABLA 60. ACL VLAN 42..... 92
TABLA 61. ACL APLICADA A VLAN 42 92
TABLA 62. RESTRICCIONES VLAN 51..... 93
TABLA 63. ACL VLAN 51..... 93
TABLA 64. ACL APLICADA A VLAN 51 94

TABLA 65. RESTRICCIONES VLAN 52 ..... *94*
TABLA 66. ACL VLAN 52 ..... *95*
TABLA 67. ACL APLICADA A VLAN 52 ..... *95*
TABLA 68. RESTRICCIONES VLAN 53 ..... *95*
TABLA 69. ACL VLAN 53 ..... *96*
TABLA 70. ACL APLICADA A VLAN 53 ..... *96*
TABLA 71. RESTRICCIONES VLAN 61 ..... *96*
TABLA 72. ACL VLAN 61 ..... *97*
TABLA 73. ACL APLICADA A VLAN 61 ..... *97*
TABLA 74. RESTRICCIONES VLAN 62 ..... *98*
TABLA 75. ACL VLAN 62 ..... *98*
TABLA 76. ACL APLICADA A VLAN 62 ..... *98*
TABLA 77. RESTRICCIONES VLAN 63 ..... *99*
TABLA 78. ACL VLAN 63 ..... *99*
TABLA 79. ACL APLICADA A VLAN 63 ..... *100*
TABLA 80. RESTRICCIONES VLAN 456 ..... *100*
TABLA 81. ACL VLAN 456 ..... *101*
TABLA 82. ACL APLICADA A VLAN 456 ..... *101*
FIGURA 36. ENRUTADOR CORPORATIVO EN VISUALIZACIÓN LÓGICA *102*
FIGURA 37. ENRUTADOR CORPORATIVO EN VISUALIZACIÓN FÍSICA *102*
TABLA 83. CONFIGURACIÓN DE INTERFAZ INTERNA Y EXTERNA *104*
TABLA 84. CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIP *104*
FIGURA 38. RUTAS APRENDIDAS POR PROTOCOLO DE ENRUTAMIENTO RIP *105*
TABLA 85. CONFIGURACIÓN DE LA INTERFAZ DE SALIDA HACIA EL PROVEEDOR DE INTERNET *105*
TABLA 86. CONFIGURACIÓN DE LA INTERFAZ HACIA LA CAPA DE DISTRIBUCIÓN-NÚCLEO *105*
TABLA 87. DIRECCIONES IP DE VLAN 250 DE ADMINISTRACIÓN *106*
TABLA 88. ASIGNACIÓN DE DIRECCIÓN IP A VLAN 250 ..... *106*
TABLA 89. DIRECCIONES IP DEFINIDAS EN CADA INTERFAZ/VLAN DEL CONMUTADOR MLSA *107*
TABLA 90. DIRECCIONES IP DEFINIDA EN CADA INTERFAZ DEL ENRUTADOR CORPORATIVO *107*
FIGURA 39. SERVIDOR CORPORATIVO EN VISUALIZACIÓN LÓGICA *108*
FIGURA 40. SERVIDOR CORPORATIVO EN VISUALIZACIÓN FÍSICA *109*
FIGURA 41. ACTIVACIÓN DEL SERVICIO DNS *110*
FIGURA 42. ACTIVACIÓN DEL SERVICIO EMAIL *111*
FIGURA 43. EQUIPOS INFORMÁTICOS EN VISUALIZACIÓN LÓGICA *112*
FIGURA 44. EQUIPOS INFORMÁTICOS EN VISUALIZACIÓN FÍSICA *112*
FIGURA 45. PROPIEDADES DEL EQUIPO INFORMÁTICO *113*
FIGURA 46. CONFIGURACIÓN DE DHCP EN LA PESTAÑA CONFIG *113*
FIGURA 47. ACTIVACIÓN DEL SERVICIO DHCP EN EL EQUIPO INFORMÁTICO *113*
FIGURA 48. REGISTRO DEL ELEMENTO IDC EN EL SERVIDOR IDC *114*
FIGURA 49. LUCES AUTOMÁTICAS EN VISUALIZACIÓN LÓGICA *115*
FIGURA 50. LUCES AUTOMÁTICAS EN VISUALIZACIÓN FÍSICA *116*
FIGURA 51. PROGRAMACIÓN BLOCKLY DEL ELEMENTO IDC (LUCES AUTOMÁTICAS) *117*
FIGURA 52. ACCESO A SALA DE COMUNICACIONES EN VISUALIZACIÓN LÓGICA *117*
FIGURA 53. ACCESO A SALA DE COMUNICACIONES EN VISUALIZACIÓN FÍSICA *118*
FIGURA 54. PROGRAMACIÓN BLOCKLY DEL ELEMENTO IDC (ACCESO A SALA DE COMUNICACIONES) *118*
FIGURA 55. BLOQUEO DE VENTANAS POR VIENTO EN VISUALIZACIÓN LÓGICA *119*
FIGURA 56. BLOQUEO DE VENTANAS POR VIENTO EN VISUALIZACIÓN FÍSICA *120*
FIGURA 57. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (BLOQUEO DE VENTANAS POR VIENTO) *120*
FIGURA 58. VENTILACIÓN AUTOMÁTICA EN VISUALIZACIÓN LÓGICA *121*
FIGURA 59. VENTILACIÓN AUTOMÁTICA EN VISUALIZACIÓN FÍSICA *121*
FIGURA 60. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (VENTILACIÓN AUTOMÁTICA) *122*

FIGURA 61. DETECTOR DE HUMO EN VISUALIZACIÓN LÓGICA *122*
TABLA 91. CONEXIONES DEL ELEMENTO IDC *123*
FIGURA 62. DETECTOR DE HUMO EN VISUALIZACIÓN FÍSICA *123*
FIGURA 63. PROGRAMACIÓN DEL ELEMENTO IDC (DETECTOR DE HUMO) EN 4ª PLANTA *124*
FIGURA 64. PROGRAMACIÓN DEL ELEMENTO IDC (DETECTOR DE HUMO) EN 5ª PLANTA *124*
FIGURA 65. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (DETECTOR DE HUMO) EN 6ª PLANTA *124*
FIGURA 66. PUERTA INTELIGENTE (A LA IZQUIERDA) Y LECTOR RF CON TARJETA VÁLIDA (A LA DERECHA) *125*
FIGURA 67. LECTOR RF JUNTO A TARJETA Y PUERTA INTELIGENTE DE 6ª PLANTA *125*
FIGURA 68. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (PUERTA DE ACCESO A PLANTA) *126*
FIGURA 69. ACCESO AL CPD EN VISUALIZACIÓN LÓGICA *127*
TABLA 92. CONEXIONES DEL ELEMENTO IDC *127*
FIGURA 70. ACCESO AL CPD EN VISUALIZACIÓN FÍSICA *127*
FIGURA 71. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (ACCESO AL CPD – LECTOR RF) *128*
FIGURA 72. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (ACCESO AL CPD - MOVIMIENTO) *128*
FIGURA 73. BLOQUEO DE VENTANA DEL CPD EN VISUALIZACIÓN LÓGICA *129*
FIGURA 74. BLOQUEO DE VENTANA DEL CPD EN VISUALIZACIÓN FÍSICA *129*
FIGURA 75. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (BLOQUEO DE VENTANA DEL CPD POR VIENTO) ... *129*
FIGURA 76. VENTILACIÓN AUTOMÁTICA DEL CPD EN VISUALIZACIÓN LÓGICA *130*
FIGURA 77. VENTILACIÓN AUTOMÁTICA EN VISUALIZACIÓN FÍSICA *130*
FIGURA 78. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (VENTILACIÓN AUTOMÁTICA DEL CPD) *131*
FIGURA 79. AIRE ACONDICIONADO CENTRALIZADO DEL CPD EN VISUALIZACIÓN LÓGICA *132*
FIGURA 80. AIRE ACONDICIONADO CENTRALIZADO DEL CPD EN VISUALIZACIÓN FÍSICA *132*
FIGURA 81. PROGRAMACIÓN DE REGLAS DEL ELEMENTO IDC (AIRE ACONDICIONADO CENTRALIZADO DEL CPD) *133*
FIGURA 82. MONITOR DE FUEGO EN EL CPD EN VISUALIZACIÓN LÓGICA *133*
FIGURA 83. MONITOR DE FUEGO EN EL CPD EN VISUALIZACIÓN FÍSICA *134*
FIGURA 84. PROGRAMACIÓN BLOCKLY DEL ELEMENTO IDC (MONITOR DE FUEGO EN EL CPD) *134*
FIGURA 85. AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA EN VISUALIZACIÓN LÓGICA *135*
TABLA 93. CONEXIONES DEL ELEMENTO IDC *136*
FIGURA 86. AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA EN VISUALIZACIÓN FÍSICA *136*
FIGURA 87. PROGRAMACIÓN DE REGLAS DEL IDC (MODO FRÍO) *136*
FIGURA 88. PROGRAMACIÓN DE REGLAS DEL IDC (MODO CALOR) *137*
FIGURA 89. PROGRAMACIÓN DE REGLAS DEL IDC (MODO AUTO) *137*
FIGURA 90. PROGRAMACIÓN DE REGLAS DEL IDC (MODO OFF) *137*
FIGURA 91. LUCES AUTOMÁTICAS DE LA FACHADA EN VISUALIZACIÓN LÓGICA *138*
FIGURA 92. LUCES AUTOMÁTICAS DE LA FACHADA EN VISUALIZACIÓN FÍSICA *138*
FIGURA 93. PROGRAMACIÓN BLOCKLY DEL ELEMENTO IDC (LUCES AUTOMÁTICAS DE LA FACHADA) *139*
FIGURA 94. SERVIDOR IDC EN VISUALIZACIÓN LÓGICA *140*
FIGURA 95. SERVIDOR IDC EN VISUALIZACIÓN FÍSICA *140*
TABLA 94. SERVICIOS NECESARIOS *141*
FIGURA 96. CONFIGURACIÓN DEL SERVICIO DE CORREO ELECTRÓNICO *141*
FIGURA 97. HABILITAR SERVICIO IOT (IDC) EN EL SERVIDOR IDC *142*
FIGURA 98. ACCESO A IOT MONITOR EN LA PESTAÑA DESKTOP *143*
FIGURA 99. ACCESO AL SERVIDOR WEB DE IOT (IDC) *143*
FIGURA 100. VISUALIZACIÓN DEL APARTADO HOME Y CONDITIONS DEL SERVIDOR IDC *144*
FIGURA 101. VISUALIZACIÓN LÓGICA DEL SIMULADOR CON TODOS LOS ELEMENTOS IDC Y DISPOSITIVOS *145*
FIGURA 102. CONFIGURACIÓN DE CLIENTE DE CORREO Y ENVÍO DE CORREO ELECTRÓNICO *146*
FIGURA 103. ACCESO AL CLIENTE DE CORREO (EMAIL) Y COMPROBACIÓN DEL CORREO ELECTRÓNICO *147*
FIGURA 104. PROPIEDADES DEL EQUIPO INFORMÁTICO Y ACCESO A COMMAND PROMPT *147*
TABLA 95. COMPROBACIONES DE RESTRICCIONES DESDE JLREINA *148*
TABLA 96. COMPROBACIONES DE RESTRICCIONES DESDE SPASCUAL *149*
FIGURA 105. PROPIEDADES DEL TERMINAL MÓVIL Y ACCESO AL NAVEGADOR WEB *149*

FIGURA 106. ACCESO A SERVIDOR WEB Y VISUALIZACIÓN DE LISTADO DE ELEMENTOS IDC..... 150
FIGURA 107. ESTADOS DEL ELEMENTO IDC (ACCESO A SALA DE COMUNICACIONES)..... 150
FIGURA 108. ACCESO AL CLIENTE DE CORREO (EMAIL) 151
FIGURA 109. REVISIÓN DE CORREO ELECTRÓNICO 151
FIGURA 110. ACCESO DENEGADO VS ACCESO VÁLIDO 152
FIGURA 111. DETECCIÓN DE MOVIMIENTO VS SIN DETECCIÓN 152
FIGURA 112. BLOQUEO DE LA PUERTA DEL CPD..... 153
FIGURA 113. ELEMENTO IDC EN REPOSO VS ELEMENTO IDC EN FUNCIONAMIENTO 153
FIGURA 114. TERMINAL MÓVIL RECIBIENDO NOTIFICACIÓN CRÍTICA..... 154
TABLA 97. MODOS DE FUNCIONAMIENTO 154
TABLA 98. OPTIMIZACIÓN DE PROTOCOLO DE ENRUTAMIENTO RIP 156
FIGURA 115. VISUALIZACIÓN DEL RESTO DE REGLAS Y POSIBILIDAD DE AÑADIR NUEVAS REGLAS..... 159
ANEXO 1. PLANO GLOBAL 163
ANEXO 2. PLANO INTERMEDIO 164
ANEXO 3. PLANO CORTO - 4ª PLANTA..... 165
ANEXO 4. PLANO CORTO - 5ª PLANTA..... 166
ANEXO 5. PLANO CORTO - 6ª PLANTA..... 167
ANEXO 6. PLANO CORTO - ARMARIOS RACKS..... 168

ACRÓNIMOS

TFG: **T**rabajo **F**in de **G**rado.

IdC: **I**nternet **d**e las **C**osas.

IoT **I**nternet **o**f **T**hings.

VPN: **V**irtual **P**rivate **N**etwork.

CCNA: **C**isco **C**ertified **N**etwork **A**ssociate.

CCNP: **C**isco **C**ertified **N**etwork **P**rofessional.

CCIE: **C**isco **C**ertified **I**nternetwork **E**xpert.

MIT: **M**assachusetts **I**nstitute of **T**echnology.

IEEE: **I**nstitute of **E**lectrical and **E**lectronic **E**ngineers.

LAG: **L**ink **Ag**gregation.

CPD: **C**entro de **P**rocesamiento de **D**atos

VLSM: **V**ariable **L**ength **S**ubnet **M**ask.

VLAN: **V**irtual **LAN**.

IP: **I**nternet **P**rotocol.

MCU/SBC: **M**icro**C**ontroller **U**nit/ **S**ingle-**B**oard **C**omputer.

RF: **R**adio **F**requency.

AC: **A**ir **C**onditioning.

POE: **P**ower **O**ver **E**thernet.

QoS: **Q**uality **o**f **S**ervice.

MAC: **M**edia **A**ccess **C**ontrol.

DHCP: **D**ynamic **H**ost **C**onfiguration **P**rotocol.

CDP: **C**isco **D**iscovery **P**rotocol.

VTP: **V**irtual **T**runking **P**rotocol

LAN: **L**ocal **A**rea **N**etwork.

WAN: **W**ide **A**rea **N**etwork.

NAT: **N**etwork **A**ddress **T**ranslation

HTTP: **H**yper**T**ext **T**ransfer **P**rotocol.

TFTP: **T**rivial **F**ile **T**ransfer **P**rotocol.

FTP: **F**ile **T**ransfer **P**rotocol.

DNS: **D**omain **N**ame **S**ystem.

NTP: **N**etwork **T**ime **P**rotocol.

CLI: **C**ommand-**L**ine **I**nterface.

PAgP: **P**ort **Ag**gregation **P**rotocol.

LACP: **L**ink **A**ggregation **C**ontrol **P**rotocol.

RIP: **R**outing **I**nformation **P**rotocol,

ACL: **A**ccess **C**ontrol **L**ist.

INTRODUCCIÓN

La implantación de una red corporativa o la modificación de la ya existente por parte de empresas de cierta envergadura implica una gran inversión y reto estratégico no exento de problemas debido, entre otras cuestiones, a que no cuentan con personal cualificado para realizar tal labor.

Este punto es fundamental para la empresa, debe realizarse con todas las garantías, cuidando al máximo y contemplando todos aquellos factores y elementos que pueden hacer que la solución adoptada no sea la más adecuada para la empresa. Es por ello, que se requiere de personal cualificado y del asesoramiento por parte de profesionales para realizar la mejora o la puesta en marcha de la red corporativa, teniendo en cuenta todas las necesidades empresariales actuales y previsibles en el futuro.

Realizar un proyecto de implantación de una red corporativa requiere de unos conocimientos que muchas veces no se poseen en la propia empresa o se contratan a empresas externas que no poseen dichos conocimientos, lo que provoca que los proyectos de implantación suelan alargarse en el tiempo y/o los resultados no siempre sean los deseados, teniendo que *parchear* repetidamente el diseño antes de llegar a una red “estable”. A veces, incluso, la solución implantada no cumple con todos los requisitos reales que la empresa necesita, lo que provoca otra serie de inconvenientes como, por ejemplo, pérdida de rendimiento, lentitud en los servicios e incluso caídas de los mismos, etc. Por lo tanto, es muy necesario disponer de personal cualificado o contratar una empresa especializada que haga un asesoramiento y análisis correcto antes de realizar un proyecto de tal envergadura.

OBJETIVOS

El objetivo principal de este Trabajo Fin de Grado es cubrir las necesidades de diseño e implementación de nuevas soluciones en sus redes corporativas incluyendo elementos del Internet de las Cosas (IdC). Estas necesidades pueden ser desde una mejora de una instalación en funcionamiento hasta la puesta en marcha de una nueva ubicación con la inclusión de una gran diversidad de elementos. En nuestro

caso, se va a realizar la solución partiendo de cero, en las nuevas instalaciones de una empresa genérica, dónde se quiere implementar el Internet de las Cosas (IdC).

Por empresa genérica nos referimos a una mediana empresa con más de 60 puestos de trabajo, organizados por secciones en diferentes plantas. Los requisitos que se toman como punto de partida para este trabajo fin de grado están basados en las necesidades de una empresa real de la que no podemos desvelar ningún tipo de información.

La solución para nuestra empresa genérica debe contemplar los siguientes puntos:

- **Diseño Físico:** el diseño físico se realiza teniendo en cuenta la nueva ubicación de la empresa, definiendo el emplazamiento de los distintos departamentos y dotando a cada puesto informático del punto de acceso necesario. Además, dicho diseño físico incluye todos los elementos IdC que la empresa considere necesarios.
- **Diseño Lógico:** el diseño lógico se estructura de forma jerárquica y segmentada según se establecen en los diseños actuales de redes corporativas, indicando cada una de las capas utilizadas (Acceso, Distribución y Núcleo). La empresa también establece ciertas restricciones de acceso entre los distintos departamentos, así como otras limitaciones que serán tratadas más adelante. El diseño lógico debe contemplar la red de elementos IdC, así como, las restricciones que en dicha red sean necesarias.
- **Prototipo:** se realiza un prototipo mediante la utilización del simulador Cisco Packet Tracer. Hay que indicar, que dicho simulador es una herramienta muy potente y la utilización de éste, es lo más parecido a realizar el diseño en un entorno real. Se puede revisar el estado en cualquier momento de los dispositivos simulados e incluso se puede inyectar tráfico o realizar diferentes actividades obteniendo una respuesta inmediata en el diseño.

Para ello, la empresa facilita la información necesaria (planos de las distintas plantas, información sobre los departamentos y la ubicación de los mismos) para la consecución de los siguientes objetivos:

- Despliegue de una red corporativa incluyendo elementos IdC.
- Seguridad corporativa y restricción de accesos.
- Escenarios contemplados por el diseño.

SIMULADOR

Entre las distintas tecnologías que existen para la realización y simulación de redes hay que destacar las ofrecidas por tres grandes compañías:

- Huawei.
- Juniper.
- Cisco Systems.

Estas tres compañías cuentan con simuladores muy potentes para la realización de diseños de red de gama empresarial. La utilización de uno simulador u otro depende en gran medida de qué se quiere realizar y sobre todo de la decisión de qué dispositivos de red se quiere utilizar.

En nuestro caso, la tecnología que se va a utilizar es la de Cisco Systems, ya que la empresa ha decidido adquirir dispositivos de la marca Cisco Systems y por lo tanto el simulador a utilizar será el simulador de Cisco Systems.

Cisco Systems es uno de los mayores fabricantes del mundo cuya tecnología de red está entre las mejores por su robustez, fiabilidad, rendimiento y prestaciones. El simulador que ofrece Cisco Systems se llama **Cisco Packet Tracer**.

Figura 1. Simulador Cisco Packet Tracer

Entre los muchos simuladores de red que hay en el mercado destaca el Cisco Packet Tracer. Este simulador es propiedad de Cisco y es muy completo, ya que permite realizar tanto el diseño físico como el diseño lógico de la red corporativa en la misma herramienta. A continuación, se detallan algunas de sus características:

- Potente *herramienta de simulación*, visualización, creación y evaluación de redes complejas.
- Posibilidad de *simular una red de forma "real"* con un número casi ilimitado de dispositivos conectados.
- Programación de los dispositivos mediante *línea de comando*.
- Posibilidad de incluir *elementos IdC*, así como programarlos.
- *Inyección de paquetes* y verificación paso a paso del tráfico generado.

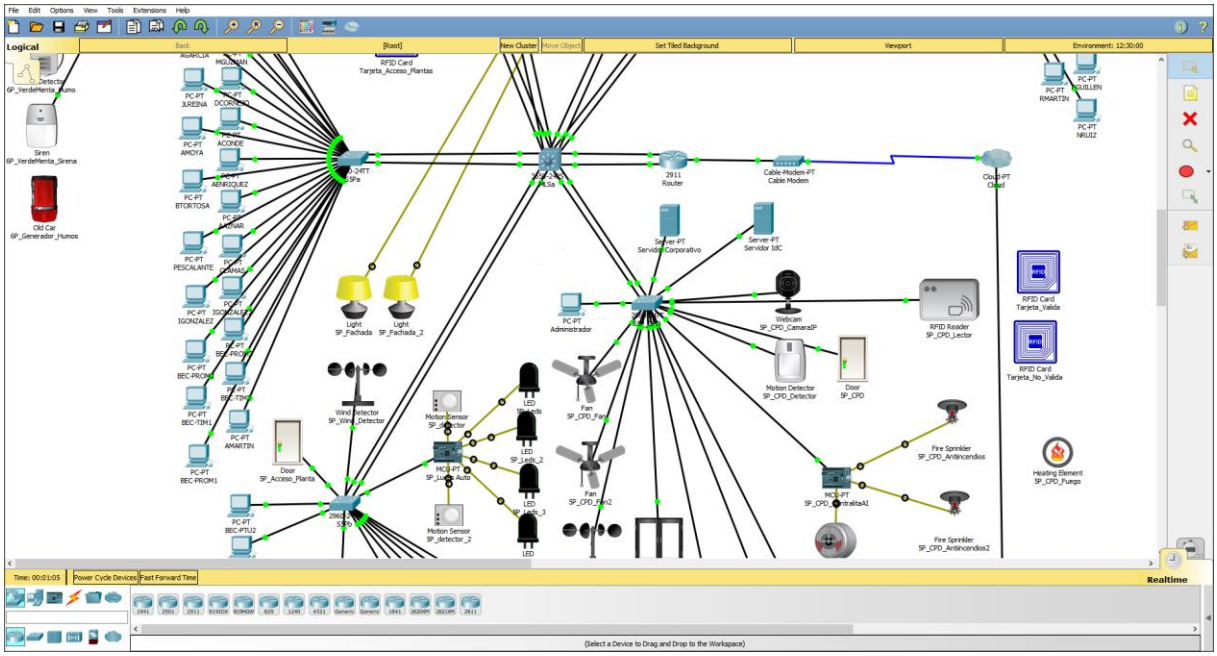


Figura 2. Entorno del simulador Cisco Packet Tracer

De estas simulaciones se puede comprobar el correcto funcionamiento del diseño, así como, detectar posibles anomalías y realizar mejoras en el diseño realizado.

ESTRUCTURA DEL DOCUMENTO

El Trabajo Fin de Grado está formado por una serie de capítulos donde se van desarrollando el diseño físico, el diseño lógico, así como la implementación y la simulación de este Trabajo Fin de Grado. Su estructura es la siguiente:

- **Capítulo 1**: se trata todo lo referente al Internet de las Cosas (IdC), así como una breve introducción de la compañía Cisco Systems. Además, se establecen cada una de las fases que Cisco Systems utiliza para el desarrollo de una red

corporativa. Estas fases se denominan **PPDIOO** y definen los pasos a seguir para llegar a un correcto despliegue de una red corporativa.

- **Capítulo 2**: se analizan las tres primeras fases (PPD). Estas fases son las referidas a la preparación y obtención de toda la información necesaria y a la realización del diseño de red, tanto físico como lógico.
- **Capítulo 3**: se realiza la implementación del diseño de red junto a la operativa y optimización del diseño, verificando su correcto funcionamiento en todo momento. Este capítulo se corresponde con las tres siguientes fases (IOO). Además, se realiza una simulación para realizar pruebas de comportamiento de la red y de los elementos IdC ante determinadas situaciones.
- **Conclusiones y trabajos futuros**: se exponen las conclusiones obtenidas de la experiencia de trabajar con el simulador de Cisco Systems, así como mejoras y trabajos futuros posibles en base al trabajo realizado.

CAPÍTULO 1

INTERNET DE LAS COSAS Y CISCO SYSTEMS

En este capítulo se describen los principales elementos que se han utilizado a lo largo de este Trabajo Fin de Grado (TFG), concretamente se trata de una visión general del Internet de las Cosas (IdC) y de una descripción de la compañía Cisco Systems. Para finalizar este capítulo, se describe la metodología empleada por Cisco Systems para la elaboración de redes corporativas.

1.1 INTERNET DE LAS COSAS (IDC)

El concepto de Internet de las Cosas (IdC) ó Internet of Things (IoT) nace de la evolución en las relaciones entre los distintos objetos y las personas, permitiendo la conexión permanente de los objetos cotidianos entre sí y la nube para dotar a las personas de más información [7]. La información generada y los datos obtenidos que se recogen de estos objetos se almacenan y se tratan de forma centralizada permitiendo un análisis posterior de los mismos. Son inmensas las posibles aplicaciones que tiene la obtención de dichos datos generados por los objetos para una empresa, como, por ejemplo:

- Monitorización de la temperatura, humedad, luminosidad, etc.
- Información del nivel de desgaste de maquinaria, del vehículo, etc.
- Detección de movimiento, humo, fuego, etc.
- Información de nuestro estado mediante la utilización de biosensores.
- Control del estado de las instalaciones:
    - Ventanas abiertas.
    - Puertas bloqueadas.
    - Luces encendidas.
    - Alarmas desconectadas.

Los avances tecnológicos que ofrece la utilización del Internet de las Cosas (IdC) son enormes y su aplicación tanto a nivel empresarial como a nivel doméstico son realmente muy interesantes [8].

Un ejemplo para el ámbito doméstico sería si nuestra nevera fuera capaz de avisarnos cuando un producto está próximo a caducar o ha caducado, o incluso, nos avisara si la nevera está perdiendo demasiada temperatura por algún tipo de anomalía en su sistema. Otro ejemplo interesante sería, por ejemplo, poder monitorizar desde nuestro móvil el estado de nuestra casa, si nos hemos dejado las luces, las puertas o las ventanas abiertas por descuido, la alarma desconectada o incluso el aire acondicionado encendido. Con el Internet de las Cosas (IdC) podríamos controlar todos estos dispositivos y muchos más, así como poder gestionarlos desde el propio smartphone.

Este concepto nació en el Instituto de Tecnología de Massachusetts (MIT), fue en 2009 cuando Kevin Ashton, profesor del MIT usó la expresión Internet of Things (IoT) de forma pública por primera vez, y desde entonces, el crecimiento ha ido en aumento de forma exponencial. Esta tecnología ya se encuentra entre nosotros y ha llegado destinada a cambiar la concepción de la sociedad tal y como la conocemos hoy en día. Aunque la tecnología implicada parece ser un proceso bastante avanzado, la realidad es que el Internet de las Cosas (IdC) es realmente sencillo de implementar.

Además, la capacidad de adaptar estos objetos a las necesidades de cada usuario es otra de las grandes ventajas que tiene esta tecnología. Por lo que, el futuro será un mundo interconectado, con sensores, objetos y dispositivos, los cuales serán de distinta índole, permitiendo identificarse, saber dónde se encuentran y dónde han estado, comunicar su estado y sus características, informar sobre el entorno que los rodea, etc. El Internet de las Cosas (IdC) hará que tanto el mundo como las personas permanezcamos conectados, mezclando nuestro día a día y el mundo digital en uno sólo.

1.2 CISCO SYSTEMS

Cisco Systems es una multinacional líder en dispositivos de red y de redes de Internet. El nombre de la compañía proviene de una casualidad. Los fundadores de la compañía trabajaban en la universidad de Stanford en los años 80 y desde la ventana se veía un cartel en donde decía “San Francisco”. Un árbol tapaba una parte del cartel de manera que sólo se podía observar *Cisco*. De ahí surgió el nombre de

la compañía, sin imaginar sus fundadores en lo que se convertiría con el paso de los años.

Entre sus múltiples dispositivos existentes en el mercado destacan los dispositivos de redes informáticas (enrutadores y conmutadores), dispositivos de seguridad (cortafuegos y concentradores de VPN), dispositivos de Telefonía IP (teléfonos y callmanager), software de gestión de red (*CiscoWorks*), equipos para redes de almacenamiento, comunicaciones ópticas, interfaces y módulos, etc. Además de todos estos dispositivos, Cisco posee otra serie de servicios, como son sus prestigiosas certificaciones a nivel mundial CCNA, CCNP y CCIE. También cabe destacar sus cursos de formación basados en su plataforma *netacad* y su potente simulador para realizar toda la formación de forma práctica, en un entorno lo más real posible sin tener el dispositivo físico delante. Dicho simulador será el empleado en este proyecto.

Figura 3. Logo Cisco Systems

1.3 METODOLOGÍA

Para llegar a la consecución del Trabajo Fin de Grado se va a utilizar la metodología empleada por Cisco para el ciclo de la vida de una red. Esta metodología consiste en 6 fases conocidas como **PPDIOO**. Estas fases definen las actividades necesarias en cada una de ellas para ayudar a asegurar la excelencia de los servicios ofrecidos. Cada una de las fases se relacionan con sus antecesoras y sus predecesoras. Los principales beneficios de esta metodología son cuatro:

- *Reducción del coste total* en tecnología y en la planificación frente a cambios originados en la infraestructura y en los recursos utilizados.
- *Incremento en la disponibilidad* de la red producido por el diseño y la operatividad de la misma.

- *Mejora la capacidad de la empresa* para establecer los requerimientos empresariales y estrategias tecnológicas más adecuadas.
- *Mejora la velocidad de acceso a las aplicaciones y servicios* mejorando la disponibilidad, seguridad, escalabilidad y rendimiento de la red en general.

A continuación, se indican cada una de las fases por separado y una breve descripción. En capítulos posteriores se analizan con mayor profundidad cada una de las fases PPDIOO.

Esquema de las fases PPDIOO:

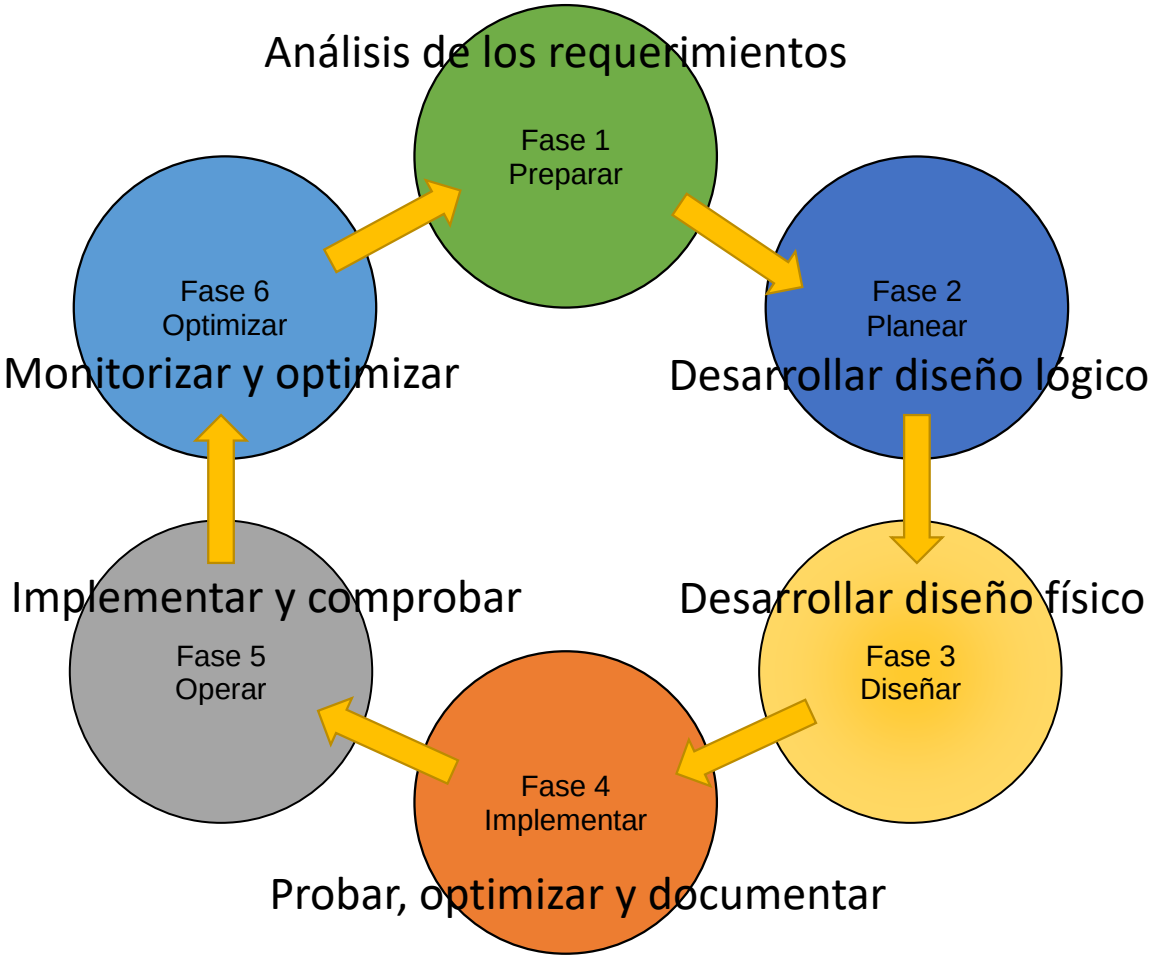


Figura 4. Fases PPDIOO

CAPÍTULO 2

En este capítulo se comienza con las tres primeras fases de la metodología PPDIOO correspondientes a las fases de Preparación, Plan y Diseño. En la fase de preparación se recopila toda la información posible de las necesidades de la empresa. En la fase de Plan se identifican y se profundiza en las necesidades detectadas detallándolas. En la fase de diseño se desarrollan todos los requerimientos técnicos obtenidos en las fases anteriores.

2.1 FASE DE PREPARACIÓN

La fase de preparación es aquella fase dónde se identifican las características técnicas de la red. Estas características están formadas tanto por los tipos de usuarios, las aplicaciones utilizadas, los servicios empleados, los equipos utilizados y los medios de transmisión empleados.

La fase de preparación es aquella en la que se obtiene toda la información necesaria para las futuras fases. Una fase de preparación con escasa información o insuficiente preparación provocará que el resultado final tenga deficiencias importantes y no se cubran aspectos importantes no detectados en esta fase o en las siguientes fases del proyecto. Es importante la realización de un análisis en profundidad de todas las necesidades, así como de las limitaciones tanto físicas como lógicas que puedan repercutir en el diseño final. Por lo tanto, tanto esta fase como las siguientes fases son de vital importancia para la consecución satisfactoria del proyecto. Dicha información es actualizada a medida que se va avanzando en las distintas fases del proyecto. La información es una información viva, es decir, a medida que se va avanzando se producen modificaciones tanto en las restricciones como en el diseño propiamente, así como en la documentación generada, adaptándose a la nueva información encontrada.

En el caso que nos ocupa la empresa genérica pretende realizar una implementación y futuro despliegue de su red corporativa incluyendo elementos IdC en una nueva ubicación partiendo de cero.

La red corporativa a implementar debe ser jerárquica y estructurada, siguiendo el modelo jerárquico de tres capas de Cisco [6]. Dicho modelo jerárquico tiene las siguientes capas:

- **Capa de Acceso** (*access layer*). Aquella donde se conectan los usuarios y los distintos dispositivos finales.
- **Capa de Distribución** (*distribution layer*). Aquella donde se redirecciona y se filtra el tráfico generado. Además, en esta capa se implementan las políticas de red, como, por ejemplo, enrutamiento, filtrado de paquetes y las listas de control de acceso (*access-list*).
- **Capa de Núcleo** (*core layer*). Aquella donde se transporta el tráfico tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz, por lo que la latencia y la velocidad son factores importantes en esta capa.

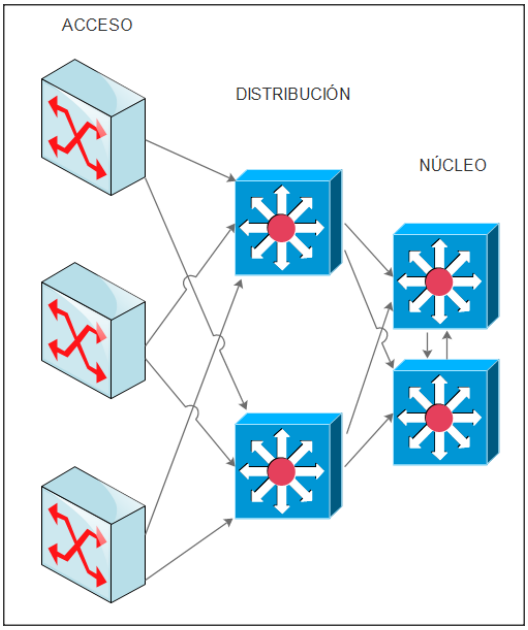


Figura 5. Modelo jerárquico de tres capas

Dependiendo del tamaño de la red corporativa se implementa un modelo simplificado o se utiliza un modelo más sofisticado.

Los beneficios del modelo de red jerárquico son los siguientes:

- *Escalabilidad*. Las redes jerárquicas pueden expandirse fácilmente añadiendo más dispositivos de red, permitiendo una mayor modularidad en el diseño.

- *Redundancia*. La redundancia en las capas núcleo y distribución permiten asegurar la disponibilidad de las distintas rutas en la red interna.
- *Rendimiento*. Se utilizan el agregado de enlaces (LAG) entre distintas capas para permitir mayor velocidad en toda la red agrupando interfaces físicas en una interfaz lógica.
- *Seguridad*. Se implementan protocolos de puerto en la capa de acceso y políticas de red en la capa de distribución que hacen que la red sea más segura.
- *Facilidad de administración*. La consistencia entre los conmutadores en cada una de las capas hace que la administración sea más simple.

Dentro de la red corporativa se pretende incluir varios elementos IdC controlados desde la propia red. Los elementos IdC pueden ser configurados en base a determinados criterios, como, por ejemplo, reglas o condicionantes. Además, pueden ser consultados en cualquier momento, lo que permite proporcionar información acerca de los elementos, así como del estado de la propia infraestructura de red. ¿Quién no se ha olvidado alguna vez las luces encendidas de la vivienda, o incluso el aparato de aire acondicionado funcionando? Utilizando elementos IdC se puede consultar el estado desde el interior de la vivienda o incluso desde el exterior utilizando un teléfono móvil o cualquier otro dispositivo con Internet de forma centralizada. Incluso se puede activar o apagar uno o varios elementos IdC, lo que proporciona un control total de los elementos IdC en nuestra red.

2.2 FASE DE PLANIFICACIÓN

En esta fase se identifican, con una mayor profundidad, los requerimientos de red realizando una caracterización y evaluación de la red, además, se realiza un análisis más exhaustivo de las necesidades encontradas en el proyecto. Un plan de proyecto es desarrollado para administrar las tareas, hitos y recursos necesarios para hacer el diseño, así como, su implementación. Este plan de proyecto es seguido durante todas las fases del proyecto, actualizándose a medida que se detectan nuevas necesidades en el proyecto.

2.2.1 CARACTERIZACIÓN

Para nuestra red corporativa y siguiendo el modelo de Cisco mencionado anteriormente, se opta por una red simplificada en dos capas, una capa de Acceso, para la conexión de los distintos dispositivos finales, y una capa de Distribución-Núcleo, para el control y el enrutamiento del tráfico. Este tipo de diseño en dos niveles se denomina diseño de red de núcleo contraído, ya que la capa núcleo y la capa distribución se contraen para formar una única capa. Esta decisión se toma al no ser excesivamente grande la red corporativa y al constar únicamente de un edificio dividido en plantas. La red corporativa consta de, aproximadamente, 160 elementos, teniendo en cuenta tanto los dispositivos y estaciones de trabajo, como los distintos elementos IdC.

Las ventajas de modelo en dos capas son principalmente:

- *Reducción de costes* al necesitar menos dispositivos de red.
- *Simplicidad del diseño* manteniendo la mayoría de los beneficios del modelo jerárquico de tres capas.

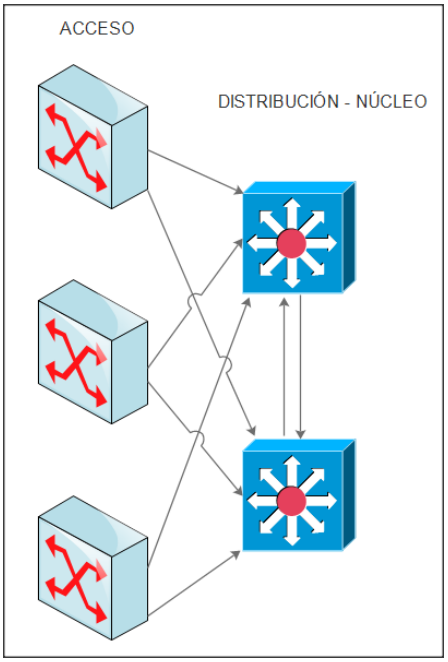


Figura 6. Modelo jerárquico de dos capas

Debido a limitaciones de coste es necesario utilizar un modelo jerárquico compacto de dos capas. Este modelo mantiene las propiedades de los modelos jerárquicos anteriores con una salvedad, la capacidad de tolerancia a fallos en la capa de distribución-núcleo se pierde. En caso de fallo físico de la capa de

distribución-núcleo la infraestructura de red dejaría de funcionar adecuadamente, mientras que en el modelo anterior (Figura 6) si toleraría fallos en uno de los dispositivos de la capa de distribución-núcleo.

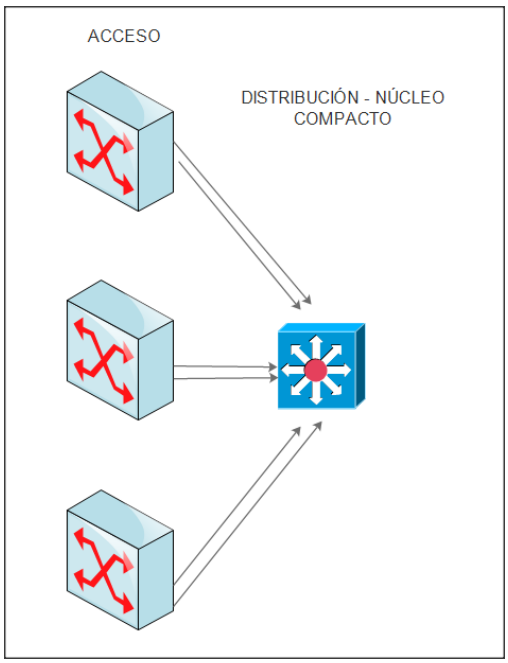


Figura 7. Modelo jerárquico de dos capas compacto

En este modelo se conectan de forma redundante varios enlaces a la capa de distribución-núcleo para dotar de redundancia ante fallos en el cableado físico, permitiendo cierta redundancia y a su vez, permitiendo el balanceo de la carga entre varios enlaces.

Una vez establecido el modelo a utilizar (Figura 7), se pasa a analizar con más detalle la ubicación de la red corporativa que se pretende diseñar.

2.2.2 UBICACIÓN

La nueva ubicación es un edificio de varias plantas cerca del centro de Málaga capital. En dicho edificio se ocupan las plantas 4ª, 5ª y 6ª. En cada una de las plantas se establece una **sala de comunicaciones**, donde se conectan todos los elementos de cada una de las plantas.

La empresa facilita los planos de las plantas para el análisis y la planificación de los trabajos en las distintas plantas. En cada una de las plantas se establece una sala de comunicación dónde se instalan los elementos de red necesarios. También

se indican los distintos elementos IdC que se desean, así como las ubicaciones en cada una de las plantas.

PLANTA 4ª

La 4ª planta es la primera de las plantas que se van a analizar. Esta planta tiene un total de **28 puntos de accesos** repartidos en dos departamentos. El departamento de color amarillo pálido tiene un total de 20 puntos de acceso mientras que el departamento de color celeste tiene 8 puntos de acceso para los usuarios.

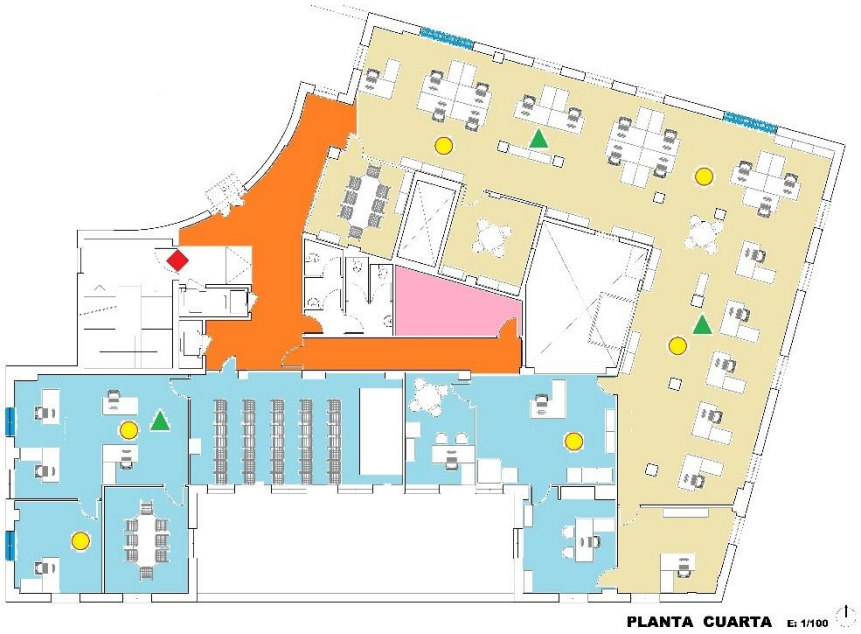


Figura 8. Plano departamental y elementos IdC 4ª planta

Entre los elementos IdC que se quieren incluir en esta planta están:

- *Luces automáticas* (zona naranja). Al detectar movimiento en la zona se encienden las luces automáticamente y éstas no se apagan hasta que, pasado un tiempo, no se detecte movimiento.
- *Acceso a la sala de comunicaciones* (zona rosa). El acceso a la sala se realiza mediante un pulsador. Al accionar el pulsador, se debe registrar el intento de acceso a la sala de comunicaciones.
- *Bloqueo de ventanas* (color azul). Las ventanas exteriores se bloquean al detectar fuertes rachas de viento en el exterior del edificio para impedir que la ventana se abra de forma abrupta.

- *Ventilación automática* (circulo amarillo). Tras abrir alguna de las ventanas inteligentes (color azul), la ventilación se activa para favorecer la correcta ventilación de la habitación.
- *Detector de humo* (triangulo verde). Si se detecta humo cerca del sensor, éste hace disparar una sirena en toda la planta en señal de emergencia.
- *Control de puerta de acceso a la planta* (rombo rojo). Sistema de seguridad controlado desde la 6ª planta para el acceso a las distintas plantas por las escaleras. Se utiliza tarjeta RF para abrir y cerrar las puertas.

Teniendo en cuenta los elementos IdC indicados se calcula el número total de elementos necesarios inicialmente (Tabla 1):

ELEMENTOS	FORMA/COLOR	UNIDADES
Luces automáticas	Zona naranja	2 + 1
Acceso a sala de comunicaciones	Zona rosa	1 + 1 + 1
Bloqueo de ventanas por viento	azul	4 + 1
Ventilación automática	Circulo amarillo	6
Detector de humo	Triangulo verde	3 + 3
Puerta de acceso a planta	Rombo rojo	1
	TOTAL	**24**

Tabla 1. Elementos IdC 4ª planta

PLANTA 5ª

La 5ª planta es la planta principal de la empresa, en ella, la empresa quiere que se ubique el Centro de Procesamiento de Datos (CPD), donde estarán los servidores centrales. Además, tendrá una sala de comunicaciones como el resto de las plantas.

En la 5ª planta hay un total de **25 puntos de acceso** y un total de tres departamentos. El departamento marrón tiene un total de 7 puntos de acceso, el departamento rosa tiene 13 puntos de acceso y el departamento amarillo un total de 5 puntos de acceso.

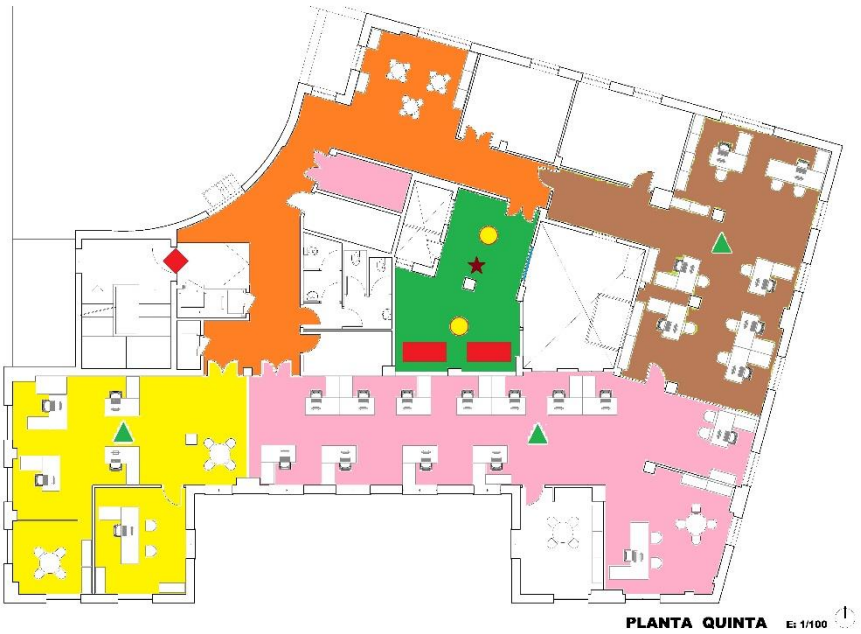


Figura 9. Plano departamental y elementos IdC 5ª planta

La empresa quiere incluir en esta planta los siguientes elementos IdC:

- *Luces automáticas* (zona naranja). Al detectar movimiento en la zona se encienden las luces automáticamente y éstas no se apagan hasta que, pasado un tiempo, no se detecte movimiento.
- *Acceso a la sala de comunicaciones* (zona rosa). El acceso a la sala se realiza mediante un pulsador. Al accionar el pulsador, se debe registrar el intento de acceso a la sala de comunicaciones.
- *Acceso al CPD* (zona verde). El acceso al CPD se realiza mediante el uso de tarjeta de radiofrecuencia (RF). Además, se debe realizar la grabación de los accesos por movimiento.
- *Bloqueo de ventana* (color azul). La ventana exterior del CPD se bloquea al detectar fuertes rachas de viento en el patio interior del edificio para impedir que la ventana se abra de forma abrupta.
- *Ventilación automática* (circulo amarillo). Tras abrir la ventana del CPD inteligente (color azul), la ventilación se activa para favorecer la correcta ventilación de la habitación. Este modo se emplearía en caso de emergencia.
- *Detector de humo* (triangulo verde). Si se detecta humo cerca del sensor, éste hace disparar una sirena en toda la planta en señal de emergencia.

- *Aire acondicionado centralizado en el CPD* (rectángulo rojo). Se instalan dos aparatos de aire acondicionado, los cuales entran en funcionamiento tras detectar temperaturas superiores a 15ºC.
- *Monitor de fuego* (estrella marrón). Se coloca dentro del CPD un detector de fuego conectado a varios aspersores y a una alarma, en caso de detección de conato se activan los aspersores y la alarma, así como, se activa una alerta que es enviada a una empresa externa.
- *Control de puerta de acceso a la planta* (rombo rojo). Sistema de seguridad controlado desde la 6ª planta para el acceso a las distintas plantas por las escaleras. Se utiliza tarjeta RF para abrir y cerrar las puertas.

Teniendo en cuenta los elementos IdC indicados se calcula el número de elementos necesarios, en este caso, serían:

ELEMENTOS	FORMA/COLOR	UNIDADES
Luces automáticas	Zona naranja	2 + 1
Acceso a sala de comunicaciones	Zona rosa	1 + 1 + 1
Acceso al CPD	Zona verde	2 + 2
Bloqueo de ventana del CPD por viento	Azul	2
Ventilación automática del CPD	Circulo amarillo	2
Detector de humo + sirena	Triangulo verde	3 + 3
Aire acondicionado centralizado	Rectángulo rojo	1 + 2 + 2
Monitor de fuego en el CPD	Estrella marrón	1 + 1 + 2 + 1
Puerta de acceso a planta	Rombo rojo	1
	TOTAL	**31**

Tabla 2. Elementos IdC 5ª planta

PLANTA 6ª

Por último, la 6ª planta también posee una sala de comunicaciones en la cual se conectan todos los elementos IdC y los puntos de acceso de los usuarios. Esta planta tiene un total de **27 puntos de acceso** y un total de tres departamentos. El departamento morado tiene un total de 13 puntos de acceso, el departamento rojo tiene 6 puntos de acceso y el departamento verde menta tiene 8 puntos de acceso para los usuarios.

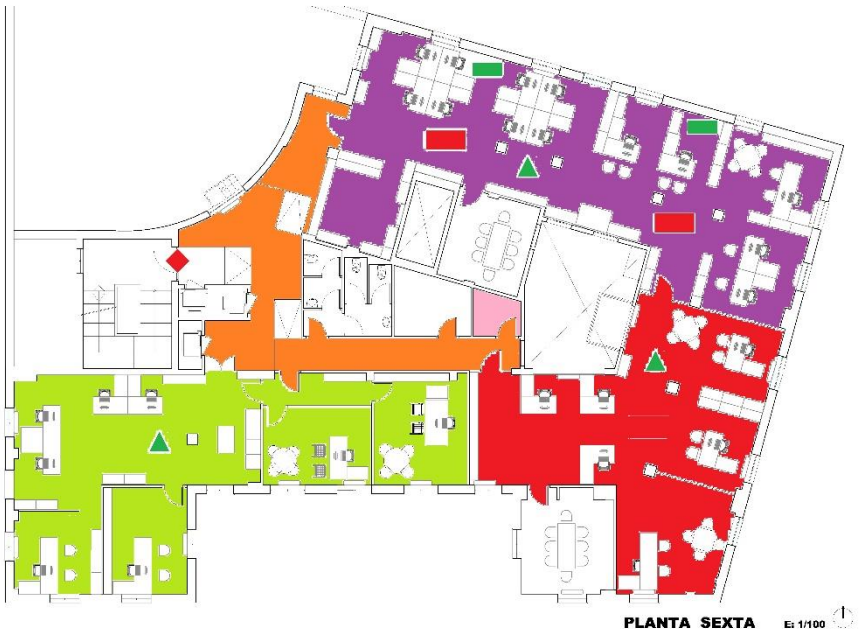


Figura 10. Plano departamental y elementos IdC 6ª planta

Entre los elementos IdC que la empresa quiere incluir en esta planta están:

- *Luces automáticas* (zona naranja). Al detectar movimiento en la zona se encienden las luces automáticamente y éstas no se apagan hasta que, pasado un tiempo, no se detecte movimiento.
- *Acceso a la sala de comunicaciones* (zona rosa). El acceso a la sala se realiza mediante un pulsador. Al accionar el pulsador, se debe registrar el intento de acceso a la sala de comunicaciones.
- *Detector de humo* (triangulo verde). Si se detecta humo cerca del sensor, éste hace disparar una sirena en toda la planta en señal de emergencia.
- *Aire Acondicionado y Calefacción centralizada* (rectángulo rojo y verde). Control del aire acondicionado y la calefacción desde un único mando sin posibilidad de modificar la temperatura por parte del usuario.
- *Control de puerta de acceso a la planta* (rombo rojo). Sistema de seguridad controlado desde esta planta permitiendo o denegando el acceso por las escaleras a las distintas plantas. Se utiliza tarjeta RF para abrir y cerrar las puertas.

Teniendo en cuenta los elementos IdC indicados se calcula el número de elementos necesarios, en este caso, serían:

ELEMENTOS	FORMA/COLOR	UNIDADES
Luces automáticas	Zona naranja	2 + 1
Acceso a sala de comunicaciones	Zona rosa	1 + 1 + 1
Detector de humo	Triangulo verde	3 + 3
Aire acondicionado y calefacción centralizada	Rectángulo rojo y verde	2 + 2 + 1
Puerta de acceso a planta + lector RF	Rombo rojo	1 + 1
	TOTAL	**19**

Tabla 3. Elementos IdC 6ª planta

FACHADA DEL EDIFICIO

Se quiere dotar a la fachada del edificio de iluminaria automática al detectar como el día va anocheciendo. Para ello, se pretende utilizar un sensor de luminosidad y luces tipo led de bajo consumo.

Figura 11. Fachada elementos IdC

Se pretende realizar la instalación de la iluminación en la fachada tal y como se muestra en la (Figura 11).

ELEMENTO	FORMA/COLOR	UNIDADES
Luces automáticas de fachada	Rectángulo Amarillo	6 + 1 + 1
	TOTAL	**8**

Tabla 4. Elementos IdC fachada

El número total de elementos IdC para dotar al edificio de iluminación de la fachada automática según el detector de luminosidad son **8 elementos**.

2.2.3 RESTRICCIONES

La infraestructura debe permitir la conexión entre los distintos puestos de trabajo limitando los accesos según el departamento, es decir, no todos los dispositivos pueden tener acceso a todos los dispositivos de otros departamentos. Cada una de las plantas es dividida en departamentos, los cuales, se colorean de distintos colores para diferenciarlos y poder definir las restricciones entre ellos. Se establecen las siguientes limitaciones y restricciones (Figura 12):

- Todos los departamentos de 4ª planta pueden comunicarse entre ellos y también pueden hacerlo con el departamento de color morado de 6ª planta y el departamento color marrón de 5ª planta (Flechas de color Azul).
- El departamento color amarillo de 5ª planta puede comunicarse con el departamento color verde menta de 6ª planta y con el departamento color rosa de 5ª planta. (Flechas de color Naranja).
- El departamento color morado de 6ª planta puede comunicarse con el departamento color verde menta de la misma planta (Flechas de color Dorado).
- La comunicación con el CPD está permitida para todos los departamentos.
- El resto de las comunicaciones se consideran no permitidas.

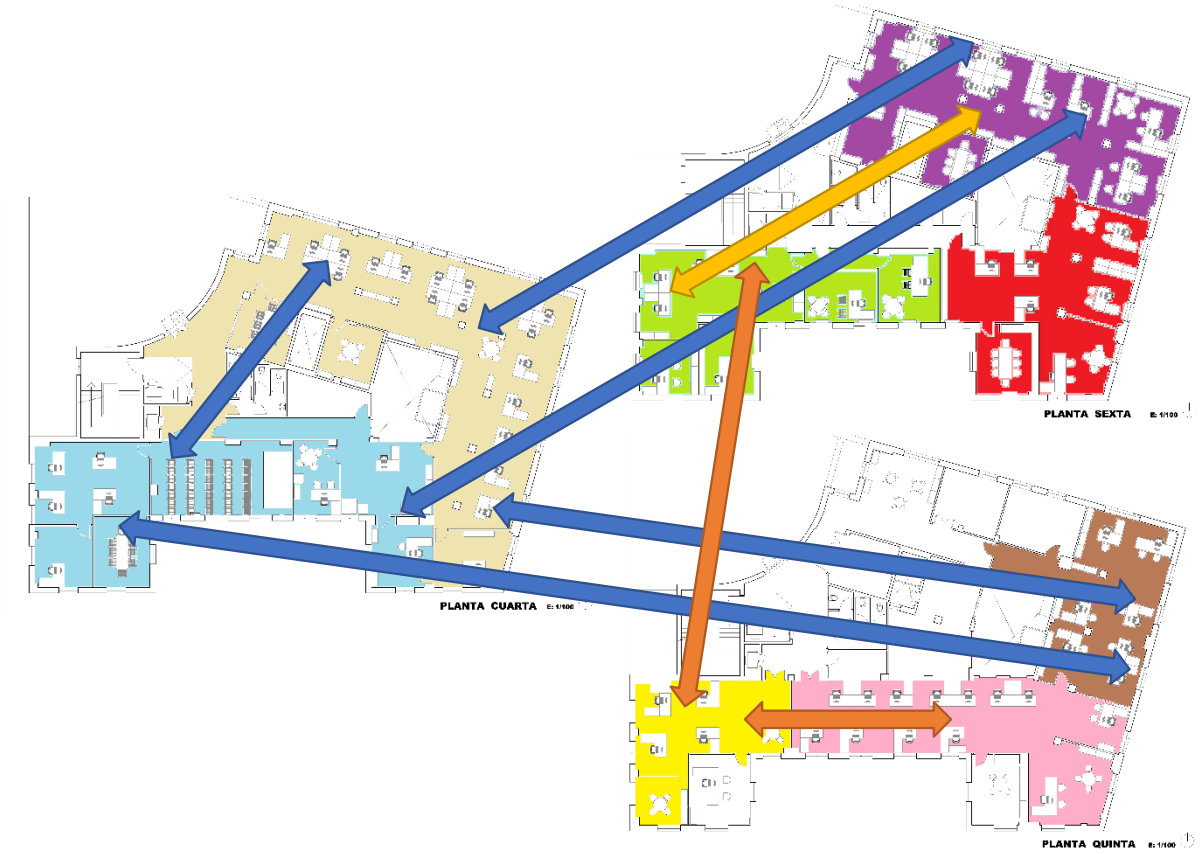


Figura 12. Restricciones establecidas entre las plantas

A todas estas restricciones hay que añadir la siguiente:

- Restringir el acceso a la red de los elementos IdC. No serán accesibles los elementos IdC por ningún dispositivo del resto de redes internas de la empresa. El único dispositivo accesible de la red de elementos IdC será el servidor IdC para poder consultar el estado de los elementos IdC desde el **exterior** de la empresa.

Además, se pretende establecer otras series de medidas de seguridad en la infraestructura de red, como son:

- Acceso seguro a los dispositivos de red. Se establecen medidas de seguridad para el acceso a los dispositivos mediante la utilización de usuario y contraseña.
- Gestión centralizada de la infraestructura de red, registro de logs, así como de las notificaciones e incidencias detectadas.
- Agregación de enlaces (LAG). Permite utilizar varios enlaces físicos como un enlace lógico para ofrecer redundancia y evitar pérdidas de conexión, además de permitir balanceo de carga entre varios enlaces.

2.3 FASE DE DISEÑO

En esta fase se realiza el diseño de la red. La red es desarrollada sobre los requerimientos técnicos obtenidos en las fases anteriores. Esta fase incluye el diagrama de red y la lista de los dispositivos requeridos. El plan de proyecto es actualizado con información más detallada para la implementación, ya que después de la aprobación de esta fase comenzaría la fase de implementación.

2.3.1 DIRECCIONAMIENTOS DE RED

A continuación, se van a ir detallando cada uno de los direccionamientos utilizados para la red de datos, para la red de elementos IdC y para las redes de administración y la red del Centro de Procesamiento de Datos (CPD).

DIRECCIONAMIENTO PARA LAS PLANTAS

El direccionamiento empleado para la red corporativa pertenece al rango 192.168.*p*0.*xx*. Cada departamento tiene su propia red de área local virtual (VLAN) dentro del segmento 192.168.*p*0.*xx*, donde *p* es la planta y *xx* según el departamento de cada una de las plantas. El direccionamiento en cada red de área local virtual se establece de forma que permita, como mínimo, el número de puntos de acceso definidos anteriormente. Para ello, se utiliza la técnica de máscaras de subred de tamaño variable (VLSM), lo que permite un aprovechamiento del rango de direcciones, evitando el desperdicio de éstas. Si se empleara un rango de direcciones de máscara de subred de tamaño fijo, todas las subredes tendrían el mismo tamaño independientemente de si realmente las direcciones se estuvieran utilizando, encontrándose situaciones en que una red de hasta 256 dispositivos tuviera tan sólo 4 dispositivos reales conectados. Es por ello, que esta técnica es utilizada para optimizar el rango de direcciones de la red corporativa tal y como se muestra a continuación:

PLANTA	Nº DPTO	VLAN	Nº PUNTOS	DIRECCIONAMIENTO	Nº MAX
4ª	1 (a. pálido)	41	20	192.168.40.0/27	32
	2 (celeste)	42	8	192.168.40.32/28	16

5ª	1 (amarillo)	51	5	192.168.50.0/28	16
	2 (rosa)	52	13	192.168.50.16/28	16
	3 (marrón)	53	7	192.168.50.32/28	16
6ª	1 (morado)	61	13	192.168.60.0/27	32
	2 (rojo)	62	6	192.168.60.32/28	16
	3 (v. menta)	63	8	192.168.60.48/28	16

Tabla 5. Direccionamiento IP

El número de la planta unido al número del departamento indica la VLAN a la que pertenece y el direccionamiento que le corresponde (Tabla 5). En la última columna se indica el número máximo de puntos de acceso que el direccionamiento establecido es capaz de suministrar. Se deja cierto margen por si fuera necesario ampliar, en un momento dado, el número de puntos de acceso inicialmente definidos. Por ejemplo, la inclusión de un dispositivo más, como podría ser una impresora de red, podría dejar agotado el rango de direccionamiento establecido si estuviera demasiado ajustado.

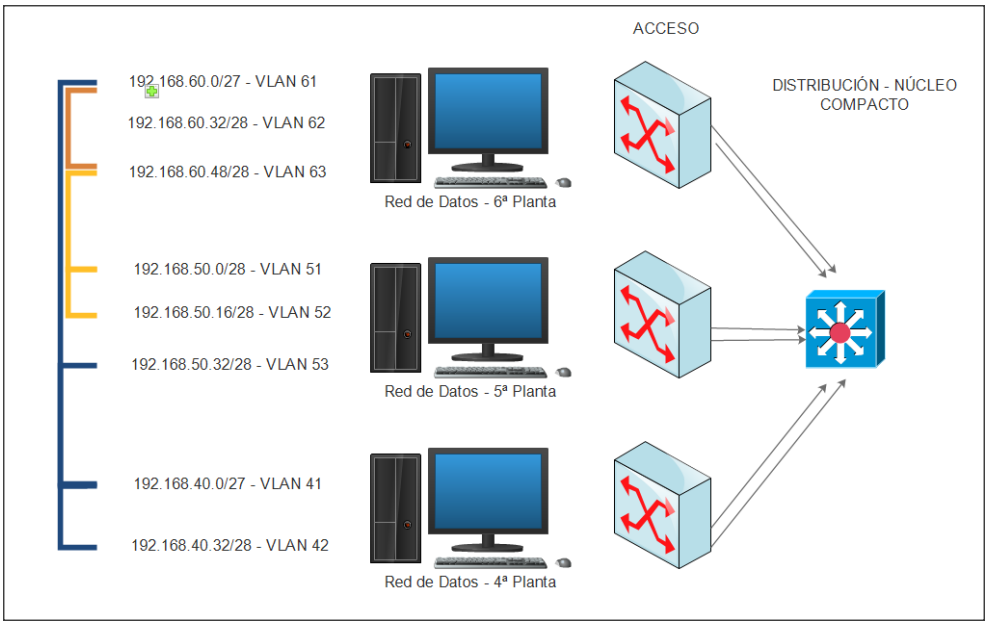


Figura 13. Direccionamiento IP y conexiones permitidas

En la Figura 13 se muestran los diferentes rangos de direcciones utilizados y las conexiones permitidas entre los diferentes rangos.

DIRECCIONAMIENTO PARA LOS ELEMENTOS IDC

El rango empleado para el direccionamiento de los elementos IdC es 172.16.0.0. Se utiliza la red de área local virtual (VLAN) número *456* con un total de 82 elementos IdC inicialmente, por lo que, la máscara de subred óptima seria la 255.255.255.128 al permitir hasta 128 dispositivos (Tabla 6).

PLANTA	VLAN	Nº PUNTOS	DIRECCIONAMIENTO	Nº MAX
4ª, 5ª y 6ª	456	82	172.16.0.0/25	128

Tabla 6. Direccionamiento IP - VLAN 456

En esta ocasión, la VLAN de los elementos IdC es común en toda la infraestructura de red, ya que necesitan poder verse entre ellos y desde el servidor IdC. Un elemento ubicado en 4ª planta tendrá un direccionamiento dentro del rango de un elemento de la 5ª y 6ª planta, permitiendo la comunicación entre los mismos.

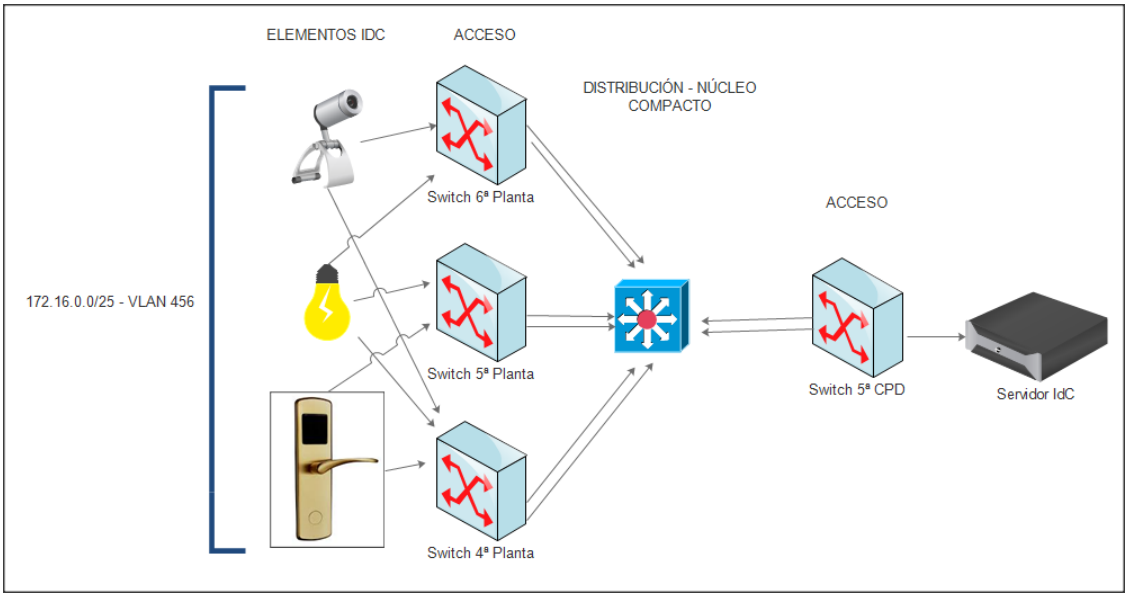


Figura 14. Conexión de los elementos IdC con el servidor IdC

Todos los elementos IdC se conectan con el servidor IdC, dónde se registran. Además, desde el servidor IdC son monitorizados y controlados sus posibles estados y sus comportamientos (Figura 14).

DIRECCIONAMIENTO PARA LA ADMINISTRACIÓN

En toda red corporativa es necesario disponer de una subred independiente para la administración de la infraestructura de red. El rango que se va a utilizar para administrar los dispositivos de red (conmutadores y enrutadores) va a ser el 192.168.250.0. Este direccionamiento es común a todos los dispositivos a administrar en la infraestructura de red de todas las plantas, por lo que, comparten una misma red de área local virtual (VLAN). Toda esta información se recopila en la siguiente tabla (Tabla 1):

PLANTA	VLAN	Nº PUNTOS	DIRECCIONAMIENTO	Nº MAX
4ª, 5ª y 6ª	250	9	192.168.250.0/28	16

Tabla 7. Direccionamiento IP - VLAN 250

La máscara de subred más próxima según el número de direcciones necesarias es 255.255.255.240. Con un máximo de elementos a administrar de 16 dispositivos de red. En este caso al ser superior a 8 se ha tenido que optar por ampliar el rango a 16 dispositivos. Hay que tener en cuenta que el número de dispositivos de red suele ser estable y no suele incrementarse habitualmente, sin embargo, los dispositivos empleados por los usuarios (ordenadores personales, portátiles, etc) si suelen hacerlo con mayor frecuencia.

DIRECCIONAMIENTO PARA EL CPD

Hasta el momento se habían contemplado las redes de datos para las distintas plantas y departamentos, pero no se había planteado la necesidad de tener un rango de direcciones propio para la red del CPD. Esta red es necesaria por motivos de seguridad y organizativos. En esta red es dónde se van a ubicar los servidores principales de la organización. Muchas empresas suelen tener los servidores en el mismo rango de direcciones de las estaciones de trabajo, sin hacer subredes ni adoptando las medidas de seguridad necesarias para proteger sus servidores de accesos no autorizados. Lo más óptimo y seguro es ubicar los servidores en un segmento de red diferente y aislado, con unas políticas de seguridad y restricciones mayores y con un mayor control que el resto de los segmentos de la red empresarial, permitiendo realizar un análisis más exhaustivo sobre los dispositivos que tienen acceso a la red del CPD. Establecer políticas de

seguridad corporativas que ayuden a gestionar y monitorizar el correcto acceso a los servidores empresariales añaden una capa extra de seguridad dentro de la infraestructura de red de una empresa.

En el caso que nos ocupa, tan sólo se dispone de un servidor central, por lo que la dirección de red y la máscara de red quedan de la siguiente forma:

PLANTA	VLAN	Nº PUNTOS	DIRECCIONAMIENTO	Nº MAX
5ª	654	1	172.16.1.0/30	2

Tabla 8. Direccionamiento IP - VLAN 654

2.3.2 DISPOSITIVOS UTILIZADOS

En este apartado se introducen los elementos utilizados para realizar el diseño e implementación de la red corporativa, Para ello, se definirá y se establecerá cómo deberían de funcionar, así como, qué servicios tendrán habilitados por defecto.

INFRAESTRUCTURA DE RED

En esta sección se introducen todos los dispositivos de la infraestructura de red a diseñar junto a sus características fundamentales y los servicios y configuraciones que necesitan.

CONMUTADORES DE LA CAPA DE ACCESO

Los conmutadores de acceso son aquellos dispositivos de red dónde se conectan todos los dispositivos finales, como pueden ser:

- Equipos informáticos.
- Impresoras.
- Portátiles.
- Puntos de acceso wifi.
- Etc.

Estos conmutadores dan conectividad a los dispositivos finales y tienen unas características y funciones concretas:

- *Switching de capa 2*. Se encarga de conmutar paquetes entre sus interfaces a gran velocidad.
- *Alta disponibilidad*. Poseen la capacidad de redundar sus enlaces y/o fuentes de alimentación para que el sistema esté siempre disponible.
- *Seguridad de puerto*. Se aplican configuración de seguridad directamente contra las interfaces del conmutador para protegerlo de ataques.
- *Alimentación por puerto ethernet (POE).* El conmutador es capaz de suministrar energía a través de sus interfaces a los dispositivos directamente conectados.
- *Clasificación y marcado Quality of Service (QoS).* Es posible establecer políticas de calidad de servicio para mejorar el desempeño de las interfaces.
- Etc.

En nuestro caso, son necesarios varios conmutadores para cubrir las diferentes plantas, por lo que se tendrán que ubicar dentro de la sala de comunicaciones de cada una de las plantas. El número de conmutadores de capa de acceso necesarios dependerá del número de dispositivos que se tengan que conectar en cada una de las plantas.

Teniendo en cuenta los datos recopilados en las fases anteriores, a continuación, se muestra el número de conmutadores necesarios para cubrir las necesidades de cada planta:

UBICACIÓN	DISP. FINALES	ELEMENTOS IDC	TOTAL	CONMUTADORES
4ª	28	19	47	2 x (24+2)
5ª	25	10	35	2 x (24+2)
CPD	3	12	15	1 x (24+2)
6ª	27	15	42	2 x (24+2)

Tabla 9. Resumen de interfaces

El número de conmutadores por planta sería de dos unidades de 24 puertos más 2 puertos para la conexión con la capa de distribución-núcleo. Por lo tanto, serían necesarios 6 conmutadores para la capa de acceso para cubrir las

necesidades de las 3 plantas y un conmutador para cubrir las necesidades del CPD. Estos conmutadores deberán tener al menos 24 interfaces más alguna interfaz más para conectar con la capa de distribución-núcleo.

Para el CPD se utilizará un conmutador independiente para conectar los distintos servidores y servicios que se ofrecen a los usuarios finales. En el CPD se ubican el servidor IdC y el servidor corporativo. Además, se conecta a este conmutador un equipo informático ubicado fuera del CPD, en una habitación próxima donde el administrador monitorizará el estado de los elementos IdC, así como las notificaciones recibidas. Además de estos dispositivos se conectan todos los elementos IdC pertenecientes al CPD.

Es muy importante tener aislado el direccionamiento de los servidores del CPD así como tenerlos ubicados de forma independiente. Para ello, se necesita disponer de un conmutador exclusivo para los servidores de la empresa. Dicho conmutador tiene unas características especiales por estar ubicado dentro del CPD y conectado a los servidores. Se les denominan conmutadores para *Data Center* y suelen tener unas características algo diferentes a los conmutadores de capa de acceso. Entre las características más importantes destacan sus menores tiempos de respuesta, latencia y mayor memoria interna. Los tiempos de respuesta deben ser muy bajos para ofrecer un mejor rendimiento a los servidores.

Para el CPD el conmutador a utilizar debería de ser un conmutador para Data Center, con mejores prestaciones y características.

Entre los servicios básicos que tendrán activos y las configuraciones a realizar en los conmutadores de capa de acceso están los siguientes:

- *Endurecimiento del dispositivo*. Protección contra accesos no deseados mediante usuario y contraseña.
- *Habilitar Portfast*. Mejora la conectividad de las interfaces permitiendo enviar tráfico rápidamente.
- *Protección de interfaz por MAC*. Le permite aprender y asociar la MAC del dispositivo conectado a la interfaz, limitando el número de MACs por interfaz.

- *Protección por suplantación del Protocolo de Configuración Dinámica de Host (DHCP).* Limita el número de peticiones DHCP por interfaz para evitar posibles ataques.
- *Protección por tormenta de paquetes broadcast.* Limita el envío de paquetes broadcast (paquetes que se transmiten de uno a todos) en las interfaces de dispositivos finales.
- *Desactivación del servicio Cisco Discovery Protocol (CDP).* Evita fugas de información a través de las interfaces con el servicio CDP activo.
- *Configuración de interfaces troncales.* Modo de funcionamiento que permite enviar tráfico de red a diferentes VLANs por la misma interfaz.
- *Configuración del cliente VLAN Trunking Protocol (VTP).* Bloquea la creación, modificación y eliminación de VLANs, siendo el servidor VTP el responsable de la creación, modificación y eliminación de las VLANs.
- *Configuración del Agregado de Enlaces (LAG).* Consiste en utilizar varias interfaces físicas en una interfaz lógica, introduciendo redundancia y mejorando el ancho de banda de la interfaz lógica creada.

CONMUTADOR DE LA CAPA DE DISTRIBUCIÓN-NÚCLEO

El conmutador de la capa de distribución-núcleo es el más importante de la infraestructura de red dado que es el conmutador donde se conectan todos los conmutadores de la capa de acceso y es el responsable del correcto enrutamiento del tráfico, así como, el que proporciona la salida hacia el enrutador principal de la empresa.

Estos conmutadores se conocen como conmutadores multicapa ya que combinan funciones de enrutamiento propia de los enrutadores y características de los conmutadores. Además, poseen muchos más servicios que los conmutadores de capa de acceso, entre los que destacan:

- Establece *restricciones sobre el tráfico de red y políticas de acceso* a la red.
- Posee un *mayor rendimiento* al tener que manejar mayores volúmenes de tráfico, al agregar enlaces de distintos armarios de conexiones.
- Proporciona *mayores funcionalidades*, mecanismos redundantes y tolerancia a fallos.

- Proporciona *servicios diferenciados* a distintas clases de aplicaciones de servicio en el perímetro de red, estableciendo calidad de servicio (QoS).

Los servicios y configuraciones que se deben proporcionar al conmutador de capa de distribución-núcleo son los siguientes:

- *Endurecimiento del dispositivo.* Protección contra accesos no deseados mediante usuario y contraseña.
- *Configuración del servidor del Protocolo de Configuración Dinámica de Host (DHCP).* El conmutador se encarga de suministrar las direcciones IP a los distintos dispositivos de la red.
- *Configuración de interfaces troncales.* Modo de funcionamiento que permite enviar tráfico de red a diferentes VLANs por la misma interfaz.
- *Configuración del servidor VLAN Trunking Protocol (VTP).* Permite la distribución de las VLANs definidas en el servidor al resto de clientes VTP.
- *Configuración de Root Spanning-Tree.* Se habilita esta protección del protocolo Spanning-Tree para garantizar que el nodo principal (Root) de la infraestructura de red va a ser el deseado.
- *Configuración del Agregado de Enlaces (LAG).* Mejora para utilizar varias interfaces físicas como una interfaz lógica, introduciendo redundancia y mejorando el ancho de banda de la interfaz lógica creada.
- *Enrutamiento entre VLANs y ruta por defecto.* Se habilita un protocolo de enrutamiento para garantizar la comunicación entre las distintas VLANs y se define una ruta por defecto para permitir la salida a Internet y el acceso desde el exterior.
- *Restricciones entre VLANs.* Implementación de las restricciones definidas entre las VLANs de los distintos departamentos para comunicarse entre sí (Figura 12).

Teniendo en cuenta los datos anteriores, a continuación, se muestra el número de interfaces requeridas para cubrir las necesidades de conexión entre las distintas ubicaciones teniendo en cuenta que dicha conexión se hace por pares de interfaces para ofrecer redundancia:

UBICACIÓN	INTERFACES	CONEXIÓN CON
4ª	4	Switch capa de acceso

		Switch capa de acceso
5ª	6	Switch capa de acceso Switch capa de acceso Router corporativo
CPD	2	Switch capa de acceso
6ª	4	Switch capa de acceso Switch capa de acceso
TOTAL:	**16**	

Tabla 10. Resumen de interfaces en capa distribución-núcleo

El modelo que más se ajusta siguiendo las características y los requerimientos anteriormente mencionados sería un modelo de 24 interfaces a 10/100/1000Mbps, dado que las interfaces de conexión con la capa de acceso deben de ser a 1000Mbps. Además, debe tener características de enrutamiento, así como el suficiente rendimiento para garantizar unos tiempos de respuesta bajos.

ENRUTADOR CORPORATIVO

El enrutador debe ser un enrutador de gama empresarial, con suficientes interfaces para conectar la red interna (LAN) con la red externa (WAN).

La configuración y los servicios que se van a configurar son los siguientes:

- *Endurecimiento del dispositivo*. Protección contra accesos no deseados mediante usuario y contraseña.
- *Configuración de traducción de direcciones de red (NAT)* para acceso desde el exterior al servidor IdC. Dada una dirección IP pública asignada al enrutador se pueda acceder al servidor IdC para consultar el estado de los elementos IdC.
- *Enrutamiento básico y ruta por defecto.* Se habilita protocolo de enrutamiento para comunicación con la empresa y se habilita ruta por defecto para salida a Internet y acceso desde el exterior.

Teniendo en cuenta que la capa de distribución-núcleo es la capa que se conecta con el enrutador, ésta requiere de dos interfaces 10/100/1000Mbps. Una

para uso administrativo y otra como ruta por defecto de la capa de distribución-núcleo. Además de estas interfaces, se requiere de una interfaz de salida WAN para la conexión con Internet. Por lo tanto, el enrutador queda de la siguiente forma:

UBICACIÓN	INTERFACES	EQUIPAMIENTO
5ª	2 IN / 1 OUT	Enrutador corporativo

Tabla 11. Resumen de interfaces en el enrutador corporativo

SERVIDOR CORPORATIVO

El servidor corporativo tendrá todos los servicios que la empresa desee que tenga, en principio y, al no haber sido especificado, se han activado los siguientes servicios:

- **Servidor Hypertext Transfer Protocol (HTTP)**. El servidor corporativo almacena la página corporativa de la empresa.
- **Servidor Trivial File Transfer Protocol (TFTP).** Protocolo para la transferencia de ficheros de forma simple.
- **Servidor File Transfer Protocol (FTP).** Protocolo para la transferencia de ficheros.
- **Servidor Domain Name System (DNS).** El servidor corporativo asigna nombres de dominio a ciertas direcciones IP para traducirlas rápidamente.
- **Servidor SYSLOG.** Protocolo de red que envía mensajes del estado del sistema. En este caso, el servidor corporativo recibe los mensajes de estado de los dispositivos de red.
- **Servidor Network Time Protocol (NTP).** Protocolo para sincronizar los relojes de los distintos dispositivos.
- **Servidor de correo electrónico (EMAIL).** El servidor corporativo tendrá alojado el servidor de correo corporativo.

En principio, todos los equipos informáticos tienen acceso al servidor corporativo y a todos sus servicios, sin restricción alguna.

El servidor corporativo se conecta al conmutador del CPD y se aloja dentro del mismo para darle mayor seguridad.

EQUIPOS INFORMÁTICOS

Los equipos informáticos que se van a utilizar tendrán el *servicio DHCP activo* por defecto para obtener una dirección IP dentro del rango asignado, según el departamento en el que se encuentren.

ELEMENTOS IDC

Los elementos IdC que se van a utilizar son de diversas naturalezas, cada uno es diferente de los otros, por lo que, se requiere de un análisis de cada uno de ellos por separado. Dicho análisis trata de optimizar y de reducir el número de elementos necesarios, así como, el número de interfaces necesarios para conectarlos con la infraestructura de red si fuera posible.

LUCES AUTOMÁTICAS

El primer elemento que se va a analizar son las luces automáticas. Este elemento actúa cuando se detecta movimiento en el entorno. Para ello, se utilizan sensores de movimiento, los cuales, al detectar movimiento dentro de su rango de acción provoca que las luces se enciendan y que notifiquen su encendido. Además, las luces deben de permanecer varios segundos encendidas siempre y cuando no vuelva a detectarse movimiento en el entorno.

Por lo tanto, dicho elemento IdC está compuesto de:

- *Detectores de movimiento*: sensores que al detectar movimiento dentro de su rango envían una señal indicando que hay movimiento.
- *Luces*: leds que se iluminan cuando reciben una señal.
- *MCU/SBC*: microcontroladora encargada de, una vez recibida la señal de movimiento, activar los leds.

La utilización de dicho elemento se realiza en todas las plantas (4ª, 5ª y 6ª planta) para cubrir la iluminación de cada uno de los pasillos.

El número de interfaces necesarias inicialmente se establece en tres interfaces, dos para los sensores de movimiento y una para la microcontroladora. Se

conectan inicialmente los sensores de movimiento y la microcontroladora para poder monitorizar desde el servidor IdC su estado.

La microcontroladora debe activar las luces leds cuando detecte movimiento en alguno de los dos sensores de movimiento, así como mantener la luz pasado un tiempo sin detectar movimiento alguno. Además, la microcontroladora envía una notificación de encendido de las luces.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Luces automáticas	3	2 detectores de movimiento. 1 MCU/SBC.
5ª	Luces automáticas	3	2 detectores de movimiento 1 MCU/SBC.
6ª	Luces automáticas	3	2 detectores de movimiento 1 MCU/SBC.

Tabla 12. Luces automáticas

Tras analizar con mayor profundidad este elemento se llega a la conclusión de que no es necesario poder monitorizar, desde el servidor IdC, el estado de los detectores de movimiento, la microcontroladora se encargaría de monitorizar sus estados y de activar las luces. Por lo tanto, este elemento podría ser optimizado liberando interfaces no necesarias. El resultado sería una única interfaz por microcontroladora:

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Luces automáticas	1	1 MCU/SBC.
5ª	Luces automáticas	1	1 MCU/SBC
6ª	Luces automáticas	1	1 MCU/SBC

Tabla 13. Luces automáticas optimizadas

ACCESO A SALA DE COMUNICACIONES

Este elemento permite el acceso a la sala de comunicaciones de las distintas plantas. Para ello, se dota al elemento de un pulsador, que tras ser accionado permita el acceso a la sala mediante el desbloqueo de una puerta inteligente. Dicha puerta permanecerá bloqueada por defecto y hasta que no sea accionado el pulsador, no se desbloqueará. Además, como medida de seguridad, pasados

5 segundos la puerta inteligente vuelve a ser bloqueada. Además, al accionar el pulsador, se envía una notificación vía email de intento de acceso a la sala.

Por lo tanto, dicho elemento IdC está compuesto de:

- *Pulsador*: tras ser pulsado envía señal para que se desbloquee la puerta inteligente.
- *Puerta inteligente*: puerta de seguridad que por defecto permanece bloqueada. Es posible desbloquearla manualmente a través del servidor IdC en caso de emergencia.
- *MCU/SBC*: microcontroladora encargada de, una vez activado el pulsador, desbloquear la puerta y enviar la notificación por email del intento de acceso.

La utilización de este elemento también se realiza en todas las plantas (4ª, 5ª y 6ª planta) en cada una de las salas de comunicaciones.

El número de interfaces necesarias inicialmente se establece en tres interfaces, una interfaz para el pulsador, otra para la puerta inteligente y otra para la microcontroladora. Se conectan el pulsador, la puerta inteligente y la microcontroladora para poder monitorizar sus estados.

La microcontroladora desbloquea la puerta inteligente al recibir la señal del pulsador y envía una notificación por email indicando la sala de comunicaciones que es accedida.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Acceso a sala de comunicaciones	3	1 pulsador. 1 puerta inteligente. 1 MCU/SBC.
5ª	Acceso a sala de comunicaciones	3	1 pulsador. 1 puerta inteligente. 1 MCU/SBC.
6ª	Acceso a sala de comunicaciones	3	1 pulsador. 1 puerta inteligente. 1 MCU/SBC.

Tabla 14. Acceso a sala de comunicaciones

Tras analizar el elemento IdC se observa que también podría ser optimizado, El estado de la puerta y del pulsador no es necesario para el servidor IdC. El servidor IdC únicamente tiene que saber el estado de la microcontroladora, si está operativa o no. Por lo tanto, la microcontroladora se encargará del pulsador y de la puerta inteligente:

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Acceso a sala de comunicaciones	1	1 MCU/SBC.
5ª	Acceso a sala de comunicaciones	1	1 MCU/SBC.
6ª	Acceso a sala de comunicaciones	1	1 MCU/SBC.

Tabla 15. Acceso a sala de comunicaciones optimizado

BLOQUEO DE VENTANAS POR VIENTO

Este elemento, como su nombre indica, bloquea las ventanas inteligentes al detectar fuertes rachas de viento en el exterior. No permite que las ventanas sean abiertas y además, cierra las ventanas al detectar dichas rachas de viento. No siendo posible abrirlas hasta que el sensor no detecte fuertes rachas de viento.

Por lo tanto, este elemento IdC está compuesto de:

- *Ventana inteligente*: ventana que por defecto se permite abrir, pero se bloquea y se cierra, si estuviera abierta, en caso de detectar rachas fuertes de viento.
- *Detector de viento*: anemómetro que mide la velocidad del aire. Al detectar rachas fuertes de viento envía una señal de activación.

La utilización de este elemento se realiza en la 4ª planta única y exclusivamente. Para ello, se colocan en dos departamentos distintos dos ventanas inteligentes. El comportamiento de estas dos ventanas inteligentes es independiente en cada uno de los departamentos, afectando sólo al departamento en el que se encuentre.

El número de interfaces necesarias inicialmente se establece en cinco interfaces, cuatro interfaces para las ventanas inteligentes y una para el detector

de viento. Se conectan tantos las ventanas como el detector al servidor IdC para ser monitorizados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Bloqueo de ventanas por viento	5	4 ventanas inteligentes.
5ª	Bloqueo de ventanas por viento	1	1 detector de viento.

Tabla 16. Bloqueo de ventanas por viento

En este caso, no es posible realizar ninguna optimización, al no utilizar ninguna microcontroladora, el servidor IdC es el responsable de gestionar el comportamiento y de definir las reglas de funcionamiento de este elemento IdC. Además, es necesaria la supervisión de cada uno de los elementos, ya que se actúa directamente sobre ellos.

El detector de viento será ubicado en la 5ª planta, por lo que se debe contabilizar en elementos de la 5ª planta. Las ventanas inteligentes si serán ubicadas en la 4ª planta.

VENTILACIÓN AUTOMÁTICA

Este elemento activa la ventilación interior cuando se detecta que hay alguna ventana inteligente en la zona que está abierta. Este comportamiento se realiza para expulsar el aire caliente o viciado del departamento, favoreciendo la correcta oxigenación del departamento.

Para ello, este elemento IdC requiere de:

- *Ventilador de interior*: ubicado en el techo de las instalaciones, el cual se activa cuando detecta que alguna de las ventanas inteligentes del departamento está abierta.

La utilización de este elemento se realiza en la 4ª planta única y exclusivamente, siendo testeado su funcionamiento para futuras implementaciones en el resto del edificio.

El número de interfaces necesarias inicialmente se establece en seis interfaces, una interfaz por cada ventilador de interior utilizado. Se conectan los ventiladores de interior al servidor IdC para ser monitorizados.

Hay que indicar que la activación de los ventiladores se hará conforme a la ventana inteligente abierta, es decir, se activan los ventiladores de interior que estén dentro del departamento dónde se encuentre la ventana inteligente abierta. Los ventiladores de interior son instalados en dos departamentos distintos, por lo que en cada departamento su puesta en funcionamiento dependerá de la ventana inteligente abierta y de su ubicación.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Ventilación automática	6	6 ventiladores de interior.

Tabla 17. Ventilación automática

Este elemento IdC no posee ninguna microcontroladora que los gestione, por lo que es el servidor IdC el responsable de gestionarlos y de definir su comportamiento.

DETECTOR DE HUMO

Este elemento se encarga de detectar humo en las distintas plantas y activa las sirenas de emergencia en el caso en que se detecte un exceso de humos. Las sirenas de emergencia activadas corresponderán a las de la planta que ha detectado el exceso de humo.

Para ello, este elemento IdC está compuesto de:

- *Detector de humo*: sensor que se activa cuando la acumulación de humo supera cierto umbral (50% de CO^2).
- *Sirena de emergencia*: la sirena se activa cuando recibe una señal del detector de humo indicando que se ha superado el umbral permitido. Dicha sirena se desactiva cuando la acumulación de humo sea inferior o igual al 20%.

La utilización de este elemento se realiza en todas las plantas de la empresa (4ª, 5ª y 6ª planta), activándose todas las sirenas de la planta dónde se detecte que se ha sobrepasado el umbral permitido.

El número de interfaces necesarias inicialmente se establece en seis interfaces, tres interfaces para los detectores de humo y tres interfaces para las sirenas de emergencia. Se conectan tantos los detectores como las sirenas al servidor IdC para ser monitorizados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Detector de humo	6	3 detectores de humo. 3 sirenas de emergencia.
5ª	Detector de humo	6	3 detectores de humo. 3 sirenas de emergencia.
6ª	Detector de humo	6	3 detectores de humo. 3 sirenas de emergencia.

Tabla 18. Detector de humo

Este elemento IdC tampoco posee microcontroladora, siendo necesaria su gestión por parte del servidor IdC.

PUERTA DE ACCESO A PLANTA

El elemento de puerta de acceso a planta trata de controlar la entrada o salida a través de la puerta de acceso a las escaleras. Por defecto, las puertas de acceso están bloqueadas para que nadie pueda utilizarlas. La persona autorizada las habilita por la mañana y/o por la tarde, según el horario laboral, y las bloquea por las noches mediante la utilización de este elemento.

Por lo tanto, este elemento IdC está compuesto de los siguientes dispositivos:

- *Puerta inteligente*: puerta de seguridad que permite el acceso a las escaleras. Por defecto está bloqueada y hasta que no se habilita, no puede ser abierta.
- *Lector RF*: sistema lector de tarjetas de radiofrecuencia (RF). Pasando una tarjeta RF válida se bloquean o se desbloquean las puertas inteligentes.
- *Tarjeta RF*: tarjeta válida utilizada para activar o desactivar las puertas.

La utilización de este elemento se realiza en todas las plantas de la empresa (4ª, 5ª y 6ª planta). El lector RF se ubica en la 6ª planta y las puertas se ubican una por cada planta a controlar el acceso (4ª, 5ª y 6ª planta).

El número de interfaces necesarias inicialmente se establece en una interfaz, con la salvedad, de que en 6ª planta se ubica el lector RF. Por lo que, en 6ª planta el número de interfaces necesarias será de dos. Tanto las puertas inteligentes como el lector RF son conectados al servidor IdC para ser monitorizados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Puerta de acceso a planta	1	1 puerta inteligente.
5ª	Puerta de acceso a planta	1	1 puerta inteligente.
6ª	Puerta de acceso a planta	2	1 puerta inteligente. 1 lector RF.

Tabla 19. Puerta de acceso a planta

El servidor IdC es el responsable de gestionar el funcionamiento y el encargado de definir las reglas de comportamiento de este elemento IdC, no siendo posible su optimización.

ACCESO AL CPD

El elemento de acceso al Centro de Procesamiento de Datos (CPD) es algo más complejo que el acceso a sala visto anteriormente. El acceso al CPD se realiza mediante tarjeta de radiofrecuencia (RF). Una vez el acceso es autorizado mediante la utilización de la tarjeta RF válida se realiza una grabación de los accesos al CPD. Para ello se utiliza un sensor de movimiento y una cámara que grabará todo lo que ocurra en el interior del CPD.

Para la realización de este elemento IdC se necesita lo siguiente:

- *Puerta inteligente*: puerta de seguridad que permite el acceso al CPD. Por defecto está bloqueada y hasta que no se utiliza una tarjeta RF válida, no puede ser abierta.
- *Lector RF*: sistema lector de tarjetas de radiofrecuencia (RF). Pasando una tarjeta RF válida se desbloquea la puerta inteligente del CPD.
- *Tarjeta RF*: tarjeta válida utilizada para activar o desactivar la puerta del CPD.

- *Detector de movimiento*: sensor que detecta si hay movimiento dentro del CPD, enviando una señal cuando se detecta movimiento.
- *Cámara de seguridad*: Cámara que graba cuando el detector de movimiento se activa. La grabación parará cuando el detector de movimiento indique que no se están produciendo movimientos.

La utilización de este elemento se realiza únicamente en la 5ª planta para asegurar el CPD de la empresa.

El número de interfaces necesarias inicialmente se establece en cuatro interfaces, una para la puerta inteligente, una para el lector RF, otra para el detector de movimiento y, por último, otra para la cámara de seguridad. Todos estos elementos son conectados al servidor IdC para ser monitorizados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Acceso al CPD	4	1 puerta inteligente. 1 lector RF. 1 detector de movimiento. 1 cámara de seguridad.

Tabla 20. Acceso al CPD

Este elemento IdC no puede ser optimizado dado que es necesario conocer el estado de cada uno de los dispositivos en el servidor IdC. Las reglas serán definidas en el servidor IdC.

BLOQUEO DE VENTANA DEL CPD POR VIENTO

El elemento que nos ocupa es similar al definido anteriormente como bloqueo de ventanas por viento, con la diferencia de que se realiza como un elemento independiente.

El comportamiento es exactamente igual, bloquea la ventana del CPD si se detecta racha fuerte de viento en el exterior, con la salvedad de que se utiliza un anemómetro independiente ubicado en el ojo patio interior. Esta independencia es necesaria dado que es de vital importancia que el elemento IdC funcione independientemente de si el elemento bloqueo de ventanas por viento lo está haciendo.

Para ello, este elemento IdC necesita lo siguiente:

- *Ventana inteligente*: ventana que por defecto se puede abrir, pero se bloquea y se cierra, si estuviera abierta, en caso de detectar fuertes rachas de viento.
- *Detector de viento*: anemómetro que mide la velocidad del viento. Al detectar fuertes rachas de viento envía una señal de activación.

La utilización de este elemento se realiza únicamente en la 5ª planta para controlar la correcta ventilación del CPD.

El número de interfaces necesarias inicialmente se establece en dos interfaces, una para la ventana inteligente y otra para el detector de viento. Ambos elementos se conectan con el servidor IdC para ser gestionados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Bloqueo de ventana del CPD por viento	2	1 ventana inteligente. 1 detector de viento.

Tabla 21. Bloqueo de ventana del CPD por viento

El servidor IdC será el responsable de gestionar este elemento IdC controlando y definiendo las reglas de comportamiento.

VENTILACIÓN AUTOMÁTICA DEL CPD

Este elemento es muy similar al elemento ventilación automática, teniendo el mismo comportamiento y funcionamiento. La ventilación del CPD se activa cuando se detecta que la ventana del CPD está abierta. Este comportamiento se utilizaría si hubiera algún problema en el aire acondicionado del CPD y fuera necesario expulsar el calor acumulado por los servidores corporativos. El funcionamiento de la ventilación se realiza a máxima potencia.

Para ello, este elemento IdC requiere de:

- *Ventilador de interior*: ubicado en el techo del CPD, el cual se activa cuando detecta que está abierta la ventana inteligente del CPD

La utilización de este elemento se realiza en la 5ª planta única y exclusivamente dentro del CPD.

El número de interfaces necesarias inicialmente se establece en dos interfaces, una interfaz por cada ventilador de interior utilizado. Se conectan los ventiladores de interior al servidor IdC para ser monitorizados.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Ventilación automática del CPD	2	2 ventiladores de interior.

Tabla 22. Ventilación automática del CPD

El servidor IdC gestionará este elemento IdC directamente. No es posible realizar ningún tipo de optimización.

AIRE ACONDICIONADO CENTRALIZADO DEL CPD

El elemento que viene a continuación es un elemento muy importante para toda empresa, como es el aire acondicionado en su CPD. En este caso, se va a diseñar dando redundancia a los aparatos de aire acondicionado y evitando, en la medida de lo posible, la intervención humana en la puesta en funcionamiento de dichos aparatos de aire acondicionado.

Para realizar este elemento IdC se requiere de:

- *Aire acondicionado (AC):* ubicado en el techo del CPD, el cual se activa cuando el monitor de temperatura lo activa o cuando el termostato es encendido de manera manual.
- *Termostato*: Mando del aire acondicionado que permite su puesta en marcha manualmente.
- *Monitor de temperatura*: dispositivo que controla la temperatura ambiente del CPD. Si la temperatura ambiente es superior o igual a 15ºC activa los ACs y si es inferior o igual a 5ºC los desactiva.

La utilización de este elemento se realiza en la 5ª planta única y exclusivamente dentro del CPD.

El número de interfaces necesarias inicialmente se establece en cinco interfaces, una interfaz por cada aparato de aire acondicionado, dos termostatos y un monitor de temperatura. Todos los elementos son registrados en el servidor IdC para su gestión y monitorización.

Los aparatos de aire acondicionado entran en funcionamiento cuando la temperatura ambiente sea superior o igual a 15ºC y dejan de funcionar si la temperatura ambiente es inferior o igual a 5ºC. Se permite que en caso de que deje de funcionar el monitor de temperatura, los aparatos puedan ser activados de forma manual empleando sus correspondientes termostatos.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Aire acondicionado centralizado del CPD	5	2 ACs. 2 termostatos. 1 monitor de temperatura.

Tabla 23. Aire acondicionado centralizado del CPD

En este caso, es posible reducir el número de interfaces utilizadas, dado que no es necesario conocer si está o no funcionando los distintos aparatos de aire acondicionado. El servidor IdC no va a trabajar directamente contra los aparatos de aire acondicionado, sino lo hará contra sus termostatos, indicándoles el modo de funcionamiento y definiendo las reglas sobre estos y sobre el monitor de temperatura.

UBICACIÓN	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
CPD	Aire acondicionado centralizado del CPD	3	2 termostatos. 1 monitor de temperatura.

Tabla 24. Aire acondicionado centralizado del CPD optimizado

MONITOR DE FUEGO EN EL CPD

Este elemento es ubicado dentro del CPD y cuya función básicamente es detectar si se ha producido fuego dentro del propio CPD. Si se produjera la detección, éste envía una señal que activaría los aspersores para sofocar el fuego y activaría una alarma, a su vez, se enviaría una notificación crítica a una empresa externa vía email.

Para poder implementar dicho elemento IdC es necesario lo siguiente:

- *Monitor de fuego*: sensor que comprueba la existencia de fuego dentro del CPD. Si detectará fuego, activaría una señal de peligro.
- *Aspersores*: sistema que utiliza agua o cualquier otro elemento para sofocar el fuego.

- *Alarma*: sistema que emite luz y sonido de alerta.
- *MCU/SBC*: se utiliza una microcontroladora para poder activar los aspersores y la alarma tras la llegada de la señal de peligro por parte del monitor de fuego, y, a su vez, también la microcontroladora realiza el envío de la notificación de la emergencia vía email.

La utilización de este elemento se realiza en la 5ª planta única y exclusivamente dentro del CPD.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Monitor de fuego en el CPD	5	1 monitor de fuego. 1 alarma. 2 aspersores. 1 MCU/SBC.

Tabla 25. Monitor de fuego en el CPD

Este elemento IdC si puede ser optimizado dejando únicamente la microcontroladora como elemento a conectar con el servidor IdC. La microcontroladora se encargará de supervisar el monitor de fuego y de activar los aspersores y la alarma en caso de emergencia, además de, enviar una notificación de emergencia.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
5ª	Monitor de fuego en el CPD	1	1 MCU/SBC.

Tabla 26. Monitor de fuego en el CPD optimizado

AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA

Este elemento es muy recomendado para la mayoría de las empresas dado que evita que los usuarios puedan manipular el aire acondicionado. El elemento funciona del siguiente modo:

- **Desactivado (Off):** el elemento no actúa ni cuando hace frío ni calor en la zona.
- **Frío (Cool):** el elemento activa los ACs cuando la temperatura es superior o igual a 15ºC y desactiva los ACs con la temperatura es inferior o igual a 0ºC.

- **Calor (Heat):** el elemento activa la calefacción cuando la temperatura es inferior o igual a 0ºC y desactiva la calefacción cuando la temperatura es superior o igual a 15ºC.
- **Auto**: el elemento activa y desactiva tanto la calefacción como los ACs. Los ACs son activados y la calefacción desactivada cuando la temperatura es superior o igual a 15ºC y la calefacción es activada y los ACs desactivados cuando la temperatura es inferior o igual a 0ºC.

Para poder realizar dicho elemento IdC es necesario lo siguiente:

- *ACs*: aparato de aire acondicionado que enfría el entorno.
- *Calefactor*: aparato de calefacción que calienta el entorno.
- *Termostato*: mando central dónde se activan los distintos modos para adecuar la temperatura del entorno.

La utilización de este elemento se realiza en la 6ª planta única y exclusivamente. Será implementado en uno de los departamentos de la 6ª planta como experiencia piloto, si el resultado fuera satisfactorio, se implantaría en el resto de los departamentos y plantas. El rango de temperaturas se ha establecido en esos márgenes para poder apreciar en el simulador el correcto funcionamiento del aire acondicionado.

Este sistema permite únicamente el activar o desactivar el modo, sin posibilidad de seleccionar la temperatura deseada, evitando que los usuarios cambien la temperatura.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
6ª	Aire acondicionado y calefacción centralizada	5	2 ACs. 2 aparatos de calefacción. 1 termostato.

Tabla 27. Aire acondicionado y calefacción centralizada

En esta ocasión, no es posible realizar ninguna optimización. El servidor IdC es el encargado de, dependiendo de la consigna en el termostato, activar o desactivar los distintos dispositivos. Por lo que, todas las interfaces son necesarias.

LUCES AUTOMÁTICAS DE LA FACHADA

Este elemento permite activar las luces de la fachada automáticamente cuando se detecte que está anocheciendo. Para ello se utiliza un detector de luminosidad, el cual, llegado a un umbral, activa las luces de la fachada.

Para poder realizar dicho elemento IdC es necesario lo siguiente:

- *Detector de luminosidad*: sensor que detecta la luminosidad en el ambiente. Si detecta que la luminosidad es inferior a un 20%, envía una señal de activación y notifica su encendido. La ubicación del sensor será en la parte alta de la fachada.
- *Luces*: leds de alta luminosidad que se activan y se desactivan según estado del detector de luminosidad.
- *MCU/SBC*: se utiliza una microcontroladora para. una vez se reciba la señal de falta de luminosidad, active las luces de la fachada y envíe notificación de encendido.

La utilización de este elemento se realiza en todas las plantas (4ª, 5ª y 6ª planta) en la fachada de las mismas. El detector de luminosidad se ubica en la parte alta de la fachada.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Luces automáticas de la fachada	2	2 leds de alta intensidad.
5ª	Luces automáticas de la fachada	2	2 leds de alta intensidad.
6ª	Luces automáticas de la fachada	4	2 leds de alta intensidad. 1 detector de luminosidad. 1 MCU/SBC.

Tabla 28. Luces automáticas de la fachada

Este elemento IdC si es posible optimizarlo, ya que dispone de una microcontroladora propia. Por lo que, los distintos leds de alta intensidad pueden ser conectados directamente a la microcontroladora, así como el detector de luminosidad, dejando sólo una interfaz como necesaria para realizar la conexión entre la MCU/SBC y el servidor IdC. Además, la microcontroladora envía una notificación cada vez que se produzca el encendido de la iluminación exterior.

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
6ª	Luces automáticas de la fachada	1	1 MCU/SBC.

Tabla 29. Luces automáticas de la fachada optimizadas

SERVIDOR IDC

Este elemento es fundamental para el desarrollo que este Trabajo Fin de Grado. En él, se registran todos los elementos IdC enumerados y se establecen las reglas de funcionamiento de los mismos, modelando sus comportamientos.

Aquellos elementos que no posean una microcontroladora (MCU/SBC) propia tendrán que ser gestionados mediante reglas por el servidor IdC. Estas reglas dependerán del comportamiento que se desee sobre los elementos IdC. A continuación, se detallan las reglas definidas anteriormente para el correcto funcionamiento de los elementos IdC independientemente de si necesitan o no una microcontroladora:

ELEMENTO IDC	MCU/SBC	REGLAS
Luces automáticas	Sí	Si detecta movimiento entonces se encienden las luces.
Acceso a sala de comunicaciones	Sí	Si se ha pulsado entonces se abre la puerta y se envía notificación.
Bloqueo de ventanas por viento	No	Si se detecta fuertes rachas de viento entonces se cierran y/o bloquean las ventanas.
Ventilación automática	No	Si hay ventana abierta entonces se activa la ventilación.
Detector de humo	No	Si se detecta que la concentración de humo es superior al 50% entonces se activan las sirenas de emergencia de la planta. Si la concentración de humo baja del 20% entonces se desactivan las sirenas.

Puerta de acceso a planta	No	Si el lector RF lee una tarjeta válida entonces se desbloquean o bloquean las puertas de acceso de las distintas plantas.
Acceso a CPD	No	Si el lector RF lee una tarjeta válida entonces se desbloquea la puerta del CPD. Si el lector RF lee una tarjeta inválida entonces permanece la puerta bloqueada. Si se detecta movimiento entonces la cámara comienza a grabar. Si no se detecta movimiento entonces la cámara para de grabar o permanece parada. Si la puerta se abre entonces se bloquea cuando se cierre y se activa el lector RF.
Bloqueo de ventana del CPD por viento	No	Si se detecta fuertes rachas de viento entonces la ventana se cierra y/o bloquea.
Ventilación automática del CPD	No	Si la ventana inteligente del CPD está abierta entonces se activa la ventilación a máxima potencia. Si la ventana está cerrada entonces se desactiva la ventilación.
Aire acondicionado centralizado del CPD	No	Si el monitor de temperatura detecta temperatura superior o igual a 15ºC entonces activa los ACs. Si el monitor de temperatura detecta temperatura inferior o igual a 5ºC entonces desactiva los ACs.
Monitor de fuego en el CPD	Sí	Si el monitor de fuego se activa entonces se envía una señal a la

		microcontroladora, la cual activa los aspersores y la alarma, y envía notificación de emergencia.
Aire acondicionado y calefacción centralizada	No	Si se activa el termostato y dependiendo del modo de funcionamiento, entonces: Off: permanece desactivada tanto la calefacción como los ACs. Frio: activa los ACs si la temperatura es superior o igual a 15ºC y los desactiva si es inferior o igual a 0ºC. Calor: activa la calefacción si la temperatura es inferior o igual a 0ºC y los desactiva si es superior o igual a 15ºC. Auto: activa los ACs y desactiva la calefacción si la temperatura es superior o igual a 15ºC y desactiva los ACs y activa la calefacción si la temperatura es inferior o igual a 0ºC.
Luces automáticas de la fachada	Si	Si el sensor detecta que la luminosidad es inferior a un 20% entonces activa las luces de la fachada y notifica su encendido.

Tabla 30. Reglas a implementar

El servidor IdC tendrá dos servicios fundamentalmente activos:

- **Servicio IdC**. Para que pueda actuar como servidor IdC y así poder registrar los elementos IdC.
- **Servicio de correo electrónico (EMAIL)**. Para enviar las notificaciones de los elementos IdC.

Este servidor también debe ser conectado al conmutador del CPD y alojado en el CPD.

2.3.3 LISTADO DE EQUIPAMIENTO REQUERIDO

Tras analizar y comprobar el número de elementos que se van a incluir en la red corporativa se pasa a definir un listado de equipamiento necesario para poder interconectar todos estos dispositivos incluidos los elementos IdC.

UBICACIÓN	Nª ELEMENTOS	EQUIPAMIENTO
4ª	28	Equipos Informáticos.
5ª	25	Equipos Informáticos.
6ª	27	Equipos Informáticos.
CPD	3	Servidor IdC. Servidor corporativo. Equipo Monitorización.

Tabla 31. Resumen de equipos informáticos y servidores necesarios

El listado de los elementos IdC queda del siguiente modo tras realizar la optimización en algunos de los elementos:

PLANTA	ELEMENTO IDC	INTERFACES	DESCRIPCIÓN
4ª	Luces automáticas	3 → 1	1 MCU/SBC.
4ª	Acceso a sala de comunicaciones	3 → 1	1 MCU/SBC.
4ª	Bloqueo de ventanas por viento	4	4 ventanas inteligentes.
4ª	Ventilación automática	6	6 ventiladores de interior.
4ª	Detector de humo	6	3 detectores de humo. 3 sirenas de emergencia.
4ª	Puerta de acceso a planta	1	1 puerta inteligente.
5ª	Luces automáticas	3 → 1	1 MCU/SBC.
5ª	Bloqueo de ventanas por viento	1	1 detector de viento.
5ª	Acceso a sala de comunicaciones	3 → 1	1 MCU/SBC.
5ª	Detector de humo	6	3 detectores de humo.

			3 sirenas de emergencia.
5ª	Puerta de acceso a planta	1	1 puerta inteligente.
CPD	Acceso al CPD	4	1 lector de tarjetas RF. 1 puerta inteligente. 1 detector de movimiento. 1 cámara.
CPD	Bloqueo de ventana del CPD por viento	2	1 ventana inteligente. 1 detector de viento.
CPD	Ventilación automática del CPD	2	2 ventiladores de interior.
CPD	Aire acondicionado centralizado del CPD	5 → 3	2 termostatos. 1 monitor de temperatura.
CPD	Monitor de fuego en el CPD	5 → 1	1 MCU/SBC.
6ª	Luces automáticas	3 → 1	1 MCU/SBC.
6ª	Acceso a sala de comunicaciones	3 → 1	1 MCU/SBC.
6ª	Detector de humo	6	3 detectores de humo. 3 sirenas de emergencia.
6ª	Aire acondicionado y calefacción centralizada	5	2 ACs. 2 calefactores. 1 termostato.
6ª	Puerta de acceso a planta	2	1 puerta inteligente. 1 lector de tarjetas RF.
Fachada	Luces automáticas de la fachada	8 → 1	1 MCU/SBC.
	TOTAL	82 → **57**	

Tabla 32. Resumen de elementos IdC

Se ha reducido el número total de interfaces necesarias para los elementos IdC de 82 interfaces a 57 interfaces (Tabla 32). Esto provoca que el espacio de direcciones para los elementos IdC pueda ser reducido, pasando de una máscara de red 255.255.255.128 a una máscara de subred 255.255.255.192, o lo que es lo

mismo de una /25 a una /26. El número máximo de direcciones para los elementos IdC será de 64.

UBICACIÓN	Nª ELEMENTOS	EQUIPAMIENTO
4ª	19	Elementos IdC
5ª	10	Elementos IdC
CPD	12	Elementos IdC
6ª	15	Elementos IdC
Fachada	1	Elemento IdC

Tabla 33. Resumen de elementos IdC por ubicación

El elemento IdC ubicado en la fachada será conectado a la 6ª planta por ser el punto más cercano de conexión.

El servidor IdC se conectará a la infraestructura de red habilitada para el CPD junto con el servidor corporativo y con el equipo de monitorización. También son conectados al CPD todos los elementos IdC que forman parte del CPD.

Con respecto a la infraestructura de red se ha determinado la necesidad de dos conmutadores de capa de acceso por planta 10/100Mbps con enlaces hacia la capa de distribución-núcleo a 10/100/1000Mbps, así como un conmutador exclusivo para el Centro de Datos (*Data Center*) en el CPD. Además, para la capa de distribución-núcleo se requiere un conmutador multicapa a 10/100/1000Mbps con enlaces redundantes y con *doble fuente de alimentación* si fuera posible.

El equipamiento necesario para la infraestructura de red es la siguiente:

UBICACIÓN	CAPA	Nª ELEMENTOS	EQUIPAMIENTO
4ª	Acceso	47	2 x conmutador capa acceso (24)
5ª	Acceso	35	2 x conmutador capa acceso (24)
CPD	Acceso	15	conmutador capa acceso (24)
6ª	Acceso	43	2 x conmutador capa acceso (24)
5ª	Dist-Núcleo	16	Conmutador Multicapa (24)
5ª	WAN	3	Enrutador Corporativo (3)

Tabla 34. Elementos de la infraestructura de red

Para terminar la fase de diseño se define la escala de incidencias a reportar según la gravedad detectada del siguiente modo:

- **Información**: Se informa de eventos sin repercusión en la infraestructura de red. Como pueden ser el encendido de las luces automáticas de las plantas o las luces de la fachada.
- **Prioritarios**: Eventos importantes que han sido detectados. Como, por ejemplo, el acceso a las salas de comunicaciones.
- **Críticos**: Eventos extremadamente importante que requieren supervisión. Como, por ejemplo, la detección de fuego en el CPD. Esta incidencia será enviada a un ente externo por su gravedad.

Esta escala será utilizada para las notificaciones enviadas por correo electrónico, indicando el nivel de gravedad en el asunto.

CAPÍTULO 3

En este capítulo se van a tratar el resto de las fases de la metodología PPDIOO pendientes entre las que se encuentran las fases de implementación, operación y optimización. La fase de implementación corresponde a la instalación y configuración del equipamiento dentro del simulador. La fase de operación corresponde con el mantenimiento del estado de la red supervisando que todos los elementos funcionan correctamente. La fase de optimización trata de realizar mejoras y correcciones antes de que afecten a la red. Para finalizar, se realiza una simulación completa de todos los elementos para verificar su correcto funcionamiento ante determinadas situaciones.

3.1 FASE DE IMPLEMENTACIÓN

En esta fase se instala y se configura el equipamiento dentro del simulador. El plan de proyecto debe seguir durante esta fase y los cambios deben ser comunicados, con la necesaria aprobación para continuar con el proceso. Cada paso en la implementación debe incluir una descripción y una guía de implementación, detallando el tiempo estimado y los pasos necesarios a realizar en caso de fallo y la información de referencia adicional.

Para la instalación del equipamiento y la configuración se utiliza la herramienta Cisco Packet Tracer. Esta herramienta fue brevemente introducida en la *Introducción* y, en esta ocasión, se va a desarrollar en detalle.

3.1.1 CISCO PACKET TRACER

La herramienta Cisco Packet Tracer es el simulador oficial de Cisco para el diseño y testeo de redes corporativas, así como, para que sus usuarios aprendan a manejar los distintos dispositivos que ofrece Cisco Systems, permitiendo utilizarlos como si estuvieran delante de los dispositivos físicos [9]. Es un simulador que permite la incorporación tanto de dispositivos de red Cisco como elementos genéricos, como ordenadores personales, portátiles, impresoras, móviles, así como elementos del Internet de las Cosas (IdC).

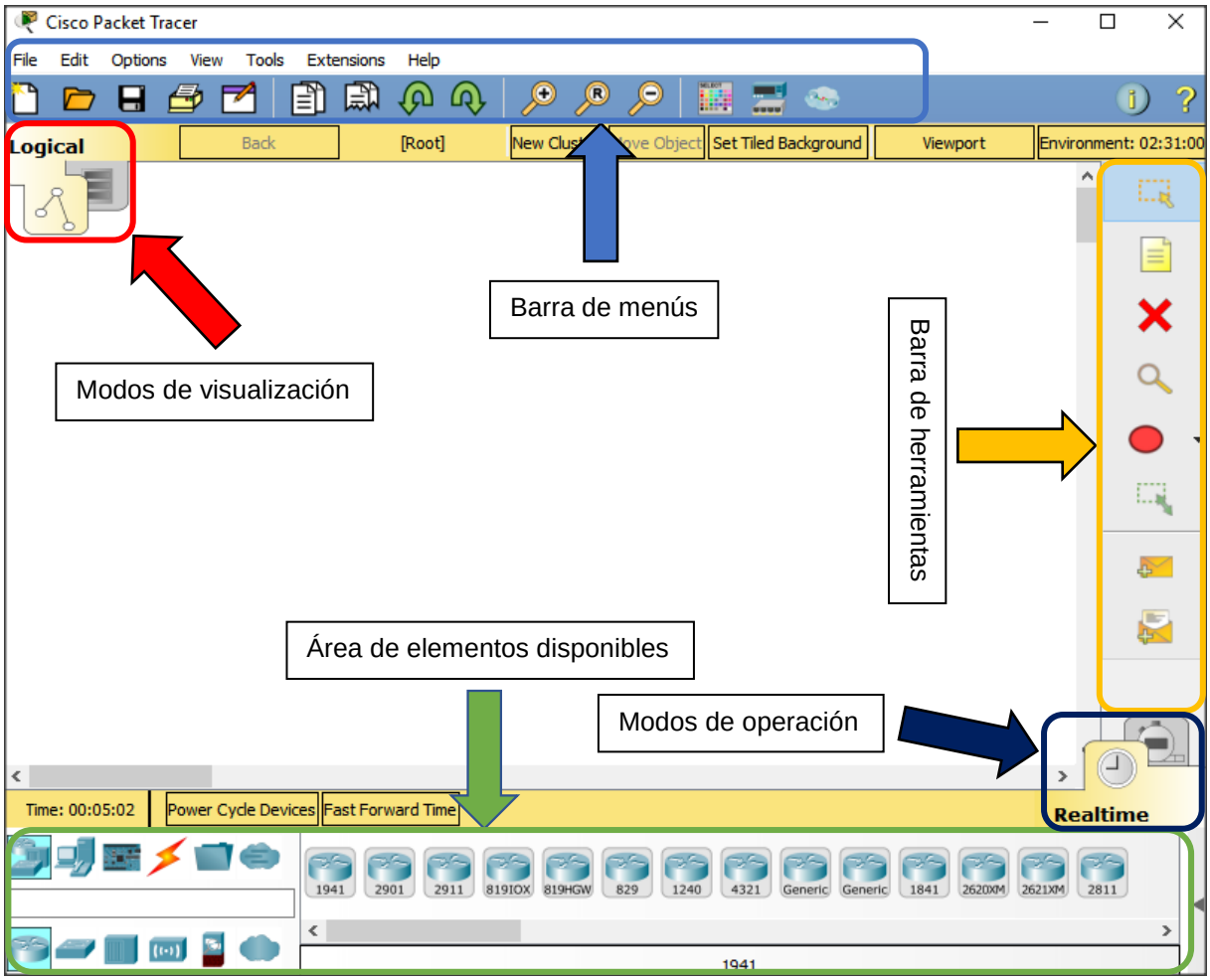


Figura 15. Entorno de trabajo en Cisco Packet Tracer

El entorno del simulador contiene varias secciones importantes, como son:

- **Barra de menús**: es la zona dónde se encuentran las opciones del programa y la configuración del software.
- **Barra de herramientas**: permite seleccionar dispositivos, mover el espacio de trabajo y analizar parámetros específicos de los dispositivos.
- **Modos de visualización**: permite cambiar entre el esquema *lógico* y el esquema *físico*. Lo habitual es trabajar con el esquema lógico.
- **Modos de operación**: permite cambiar entre el modo *tiempo real* o el modo *emulación*, el cual permite realizar análisis más detallado sobre el tráfico generado en la red.
- **Área de elementos disponibles**: permite seleccionar los elementos a incluir en el espacio de trabajo, así como la conexión entre estos. Los elementos están agrupados según el tipo de dispositivo que sea.

3.1.2 MODOS DE VISUALIZACIÓN

El simulador Cisco Packet Tracer posee dos *modos de visualización*, la visualización lógica y la visualización física. Ambas visualizaciones son muy importantes.

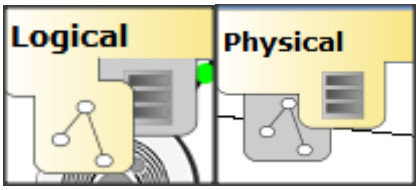


Figura 16. Modos de visualización

La visualización lógica es la que, hasta ahora, se ha venido implementando y muestra la relación entre los distintos dispositivos independientemente de su ubicación física. Es la visualización más utilizada porque permite visualizar todos los dispositivos del sistema, independientemente de su ubicación real.

La visualización física establece la ubicación de los distintos dispositivos y elementos en un entorno real mediante la utilización de imágenes de fondo. Por ello, es necesario estructura la visualización física de forma conveniente según su nivel de profundidad. Para ello, se definen los siguientes niveles de profundidad:

- *Plano global*: Plano de Málaga capital (Figura 17).
- *Plano intermedio*: Plano del edificio (Figura 18).
- *Plano corto*: Plano de las distintas plantas (Figura 19).

Cada uno de los niveles llevará consigo una imagen de fondo asociada, para así, poder ubicar de forma efectiva los elementos dentro de la imagen.

Se establece como estado inicial el *plano global*, que corresponde con un plano general de Málaga capital, lugar dónde se encuentra la nueva ubicación de la empresa (Figura 17). Es posible cambiar de plano pulsando sobre cierta área de la imagen.

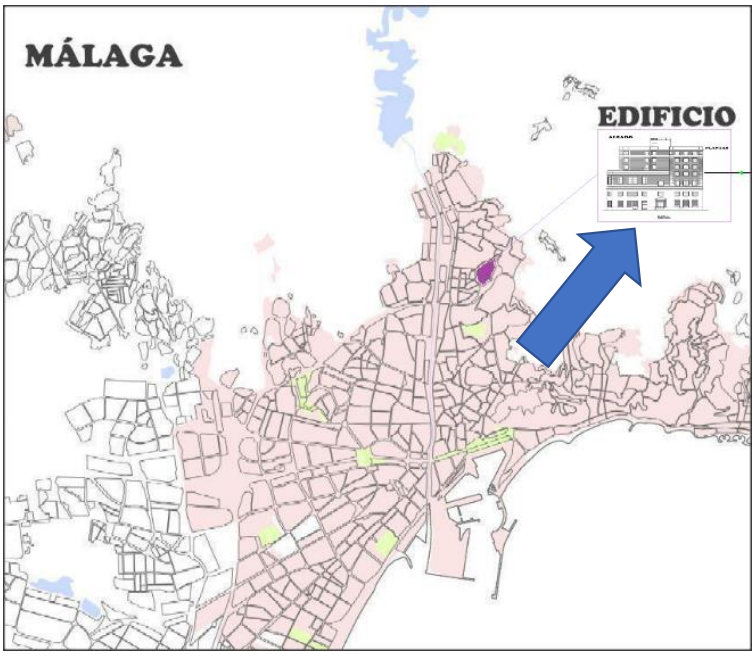


Figura 17. Plano de Málaga capital y acceso al edificio

Para cambiar del plano global al plano intermedio (Figura 18) hay que pulsar sobre la imagen del edificio enmarcado. Al pulsar sobre ella, se accede al plano intermedio, donde se ve el alzado del edificio.

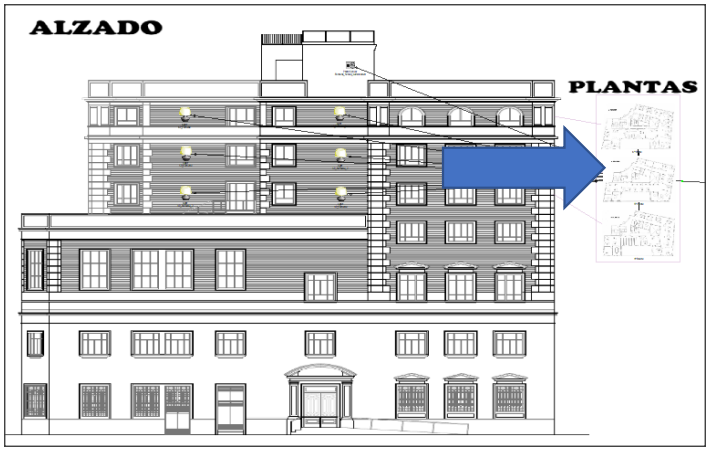


Figura 18. Alzado y acceso a las plantas

Si se desea cambiar el plano intermedio por el plano corto (Figura 19) se debe pulsar sobre la zona habilitada con cada plano de planta.

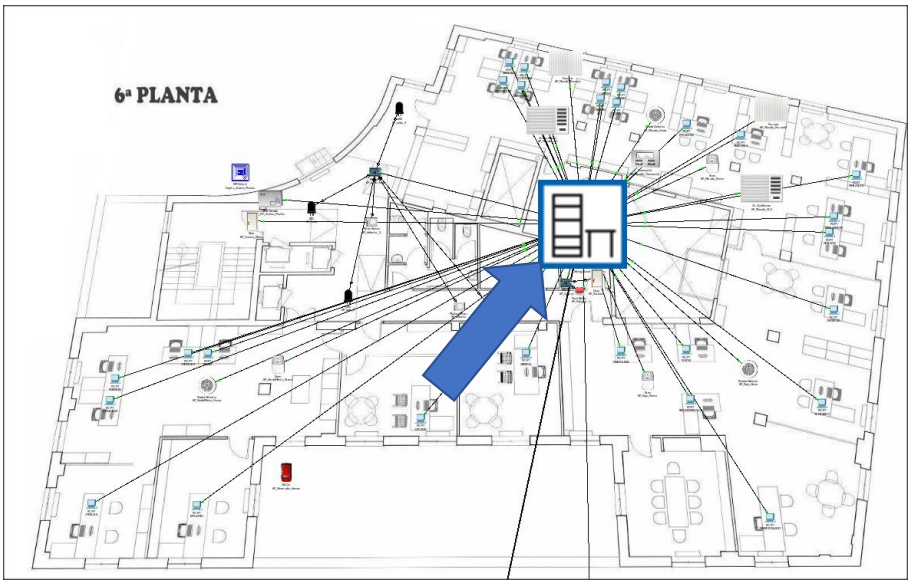


Figura 19. Mapa de planta

En el plano corto aparece un elemento cuadrado con borde azul, que corresponde con la ubicación de los armarios rack en cada una de las plantas. Si se pulsa sobre dicho recuadro se observan los elementos instalados en el armario rack de la 6ª planta (Figura 20).

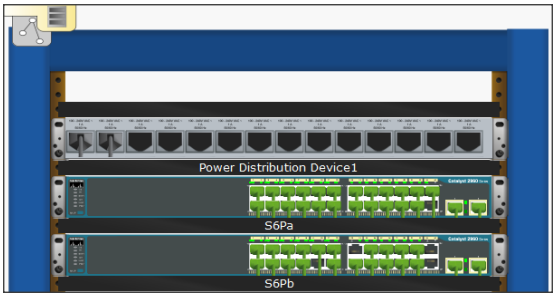


Figura 20. Armario rack con conmutadores conectados

En este caso, al ser el armario de la 6ª planta, se observan dos conmutadores con sus correspondientes conexiones, tal y como se describió en la fase de diseño del capítulo 2.

3.1.3 INFRAESTRUCTURA DE RED

Para comenzar la fase de implementación, se van a ir instalando los elementos requeridos y enumerados en el capítulo anterior, comenzando con el esqueleto de la infraestructura de red, de dónde dependerán todos los elementos que, posteriormente, se van a instalar.

Para ello, se comienza la implementación del diseño instalando los conmutadores y elementos necesarios para el correcto funcionamiento de la infraestructura de red.

Revisando los distintos conmutadores disponibles en el simulador se deben seleccionar aquellos modelos que cumplen con las características dadas en la fase de diseño.

Los conmutadores que cumplen con las características definidas anteriormente son:

UBICACIÓN	CAPA	INTERFACES	EQUIPAMIENTO
4ª	Acceso	52	2 x Switch 2960 24TT (24+2)
5ª	Acceso	52	2 x Switch 2960 24TT (24+2)
CPD	Acceso	26	Switch 2960 24TT (24+2)
6ª	Acceso	52	2 x Switch 2960 24TT (24+2)
5ª	Dist-Núcleo	28	Switch 3650 24PS (24+4)
5ª	WAN	3	Router 2911 (3)

Tabla 35. Elección de los dispositivos de red

Para el CPD no ha sido posible encontrar un modelo para Centro de Datos (*Data Center*) dentro del simulador, por lo que se ha optado por montar un equipo de capa de acceso similar a los utilizados en las distintas plantas.

Las conexiones que se van a utilizar para interconectar los distintos dispositivos de red serán las dos interfaces 10/100/1000Mbps que posee cada uno de los conmutadores de acceso, dotando a la infraestructura de red de redundancia ante la rotura o desconexión de un enlace.

El switch 3650 24PS posee la opción de conectar dos fuentes de alimentación en el mismo conmutador, lo que lo hace ideal para nuestra infraestructura de red, ya que el diseño elegido sólo tiene un conmutador en la capa de distribución-núcleo, por lo que, de esta forma se habilita la redundancia ante problemas eléctricos.

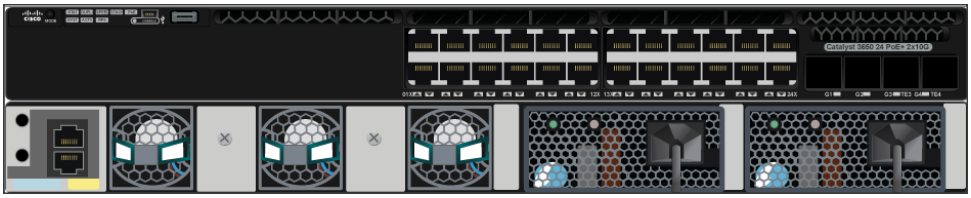


Figura 21. Switch 3650 24PS con doble fuente de alimentación

El direccionamiento utilizado para la administración de los distintos dispositivos está dentro del rango 192.168.250.0/28. Se establece a cada uno de los dispositivos su dirección IP de administración y su nomenclatura dentro del diseño según la siguiente tabla:

UBICACIÓN	NOMENCLATURA	DIRECCION IP	MODELO
4ª	S4Pa	192.168.250.4	Switch 2960 24TT
	S4Pb	192.168.250.7	Switch 2960 24TT
5ª	S5Pa	192.168.250.5	Switch 2960 24TT
	S5Pb	192.168.250.8	Switch 2960 24TT
CPD	S5P_CPD	192.168.250.3	Switch 2960 24TT
6ª	S6Pa	192.168.250.6	Switch 2960 24TT
	S6Pb	192.168.250.9	Switch 2960 24TT
5ª	MLSa	192.168.250.1	Switch 3650 24PS
5ª	Router	192.168.250.2	Router 2911

Tabla 36. Nomenclatura de los dispositivos de red

La visualización lógica de los distintos dispositivos de red se muestran en la Figura 22:

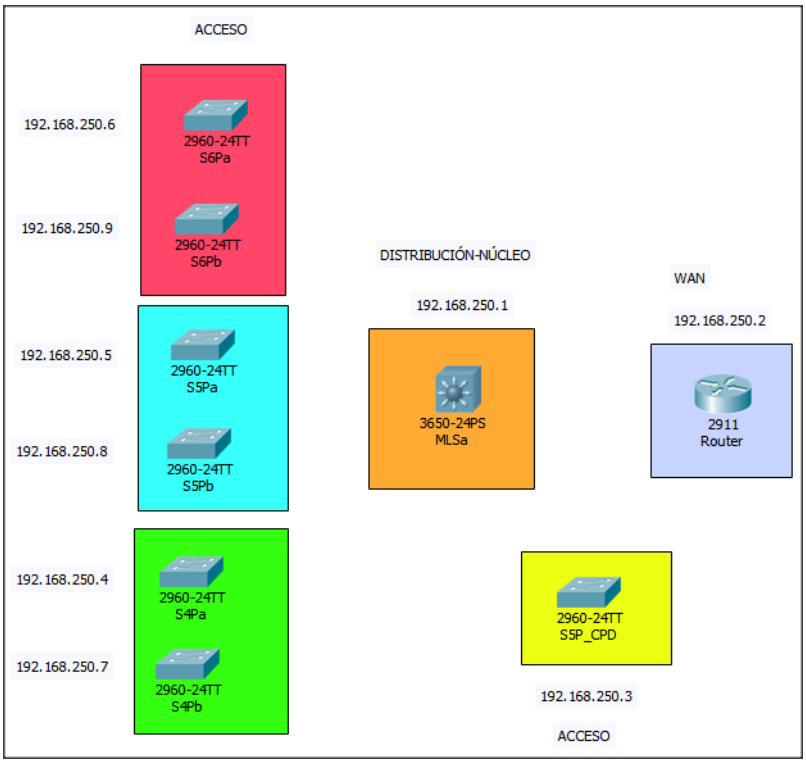


Figura 22. Dispositivos de red en visualización lógica

CONFIGURACION DE LA INFRAESTRUCTURA DE RED

A continuación, se van a configurar cada uno de los servicios necesarios en los distintos conmutadores y en el enrutador de la infraestructura de red. Para ello, se programa la configuración de los dispositivos mediante la utilización de la **línea de comando** (*CLI*).

El acceso a la línea de comando de los dispositivos se realiza a través de su ventana de propiedades (Figura 23).

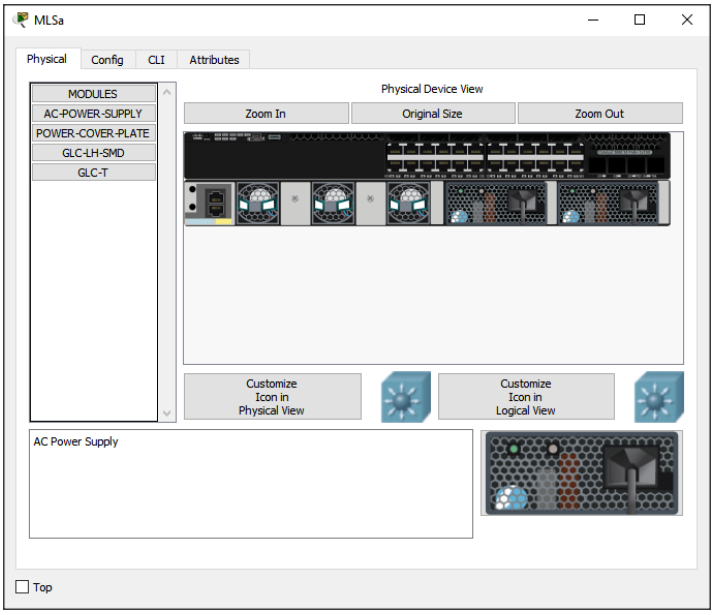


Figura 23. Accediendo a cada dispositivo de red se puede abrir la línea de comando CLI

En la *pestaña CLI*, se abre la línea de comando del dispositivo. Se pulsa la tecla **ENTER** y ya se puede comenzar a configurar el dispositivo. Este acceso a la línea de comando se realiza desde la consola del propio dispositivo, como si nos encontráramos delante del dispositivo.

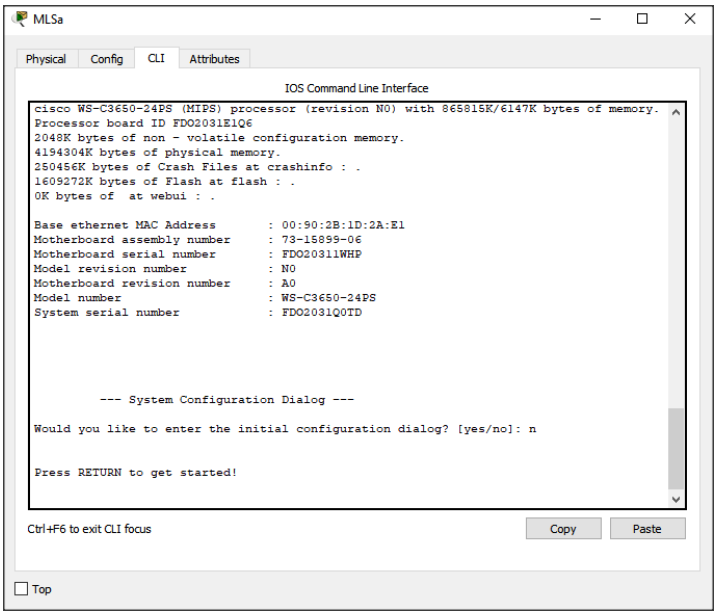


Figura 24. Visualización de la línea de comando CLI

Lo primero que se va a proceder a realizar es renombrar cada uno de los dispositivos siguiendo la nomenclatura definida en la Tabla 36.

Para ello se utiliza el siguiente comando:

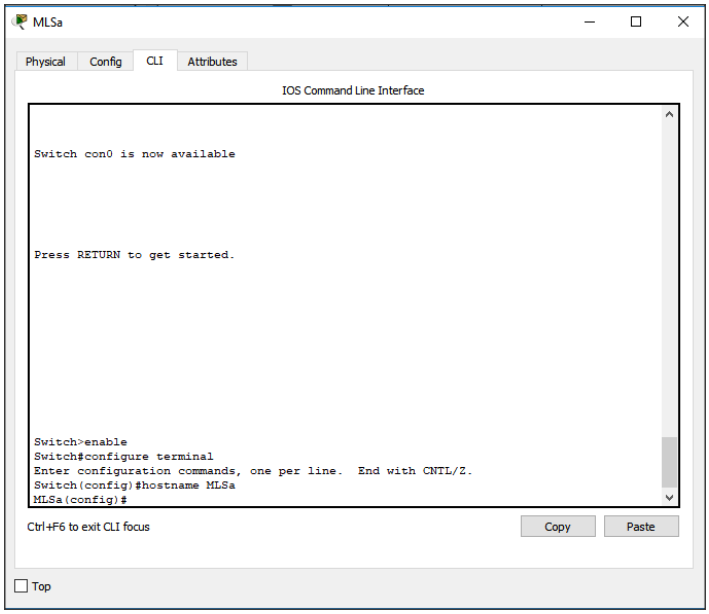


Figura 25. Línea de comando CLI

Para entrar en el modo configuración del conmutador inicialmente hay que introducir los comandos **enable** y **configure terminal** [1]. Posteriormente, ya se podría establecer el nombre del dispositivo utilizando el comando **hostname** *nombre_dispositivo* tal y como se muestra en la imagen (Figura 25).

CONEXIÓN FÍSICA DE LOS DISPOSITIVOS DE RED

A continuación, se conectan los distintos dispositivos entre ellos, teniendo en cuenta el diseño de dos capas compacto. Para ello, se conectan cada uno de los conmutadores de la capa de acceso con el conmutador de la capa de distribución-núcleo. Esta conexión se realiza de forma redundante, conectando dos interfaces 10/100/1000Mbps en cada extremo siguiendo la siguiente tabla (Tabla 37):

ORIGEN	INTERFAZ ORIGEN	DESTINO	INTERFAZ DESTINO
S4Pa	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/1
S4Pa	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/2
S4Pb	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/3
S4Pb	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/4
S5Pa	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/5
S5Pa	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/6
S5Pb	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/7
S5Pb	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/8
S6Pa	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/9
S6Pa	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/10
S6Pb	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/11
S6Pb	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/12
S5P_CPD	GigabitEthernet0/1	MLS5a	GigabitEthernet1/0/13
S5P_CPD	GigabitEthernet0/2	MLS5a	GigabitEthernet1/0/14
MLS5a	GigabitEthernet1/0/23	Router	GigabitEthernet0/1
MLS5a	GigabitEthernet1/0/24	Router	GigabitEthernet0/2

Tabla 37. Conexiones físicas entre los dispositivos de red

Los dispositivos de red se conectan entre sí para dar la siguiente visualización lógica:

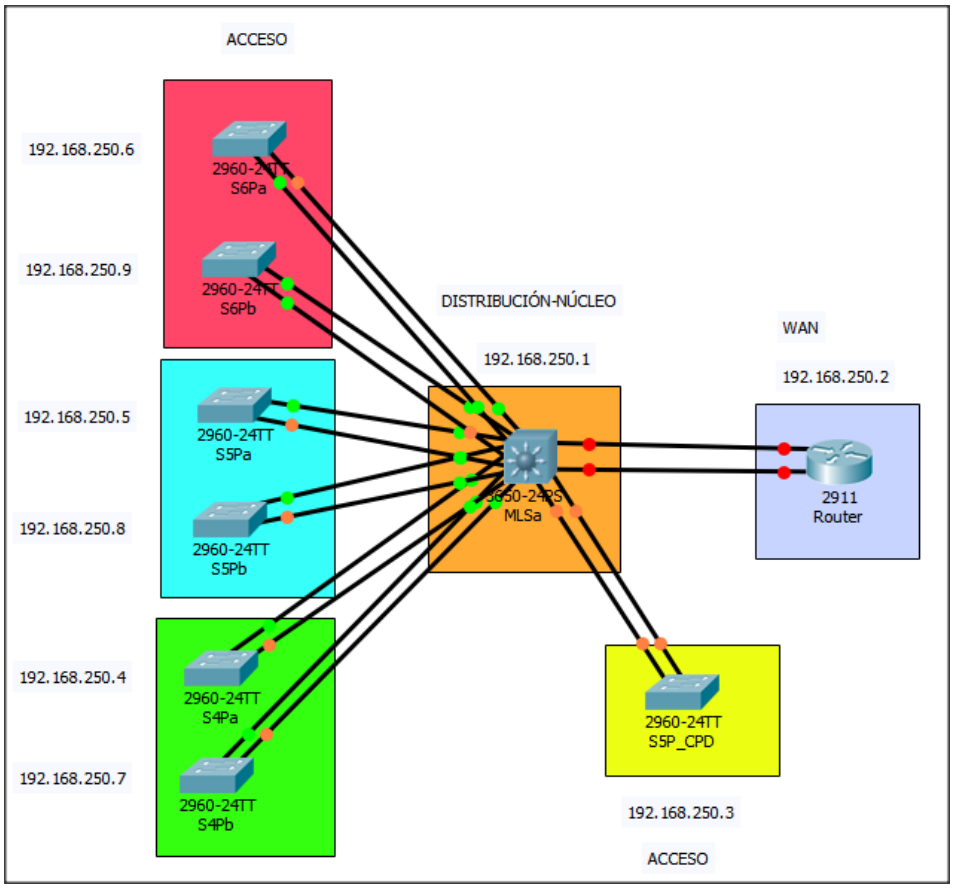


Figura 26. Dispositivos interconectados en visualización lógica

Una vez se han conectado cada uno de los dispositivos de red se procede a configurar cada uno de los conmutadores con los servicios necesarios tanto para la capa de acceso como para la capa de distribución-núcleo sin olvidar el propio enrutador.

CONMUTADORES CAPA DE ACCESO

En este apartado se desarrolla la configuración y la puesta en marcha de los servicios definidos en la fase de diseño para los conmutadores de la capa de acceso.

VISUALIZACIÓN LÓGICA

Los conmutadores de la capa de acceso se encuentran en la parte izquierda e inferior de la Figura 27:

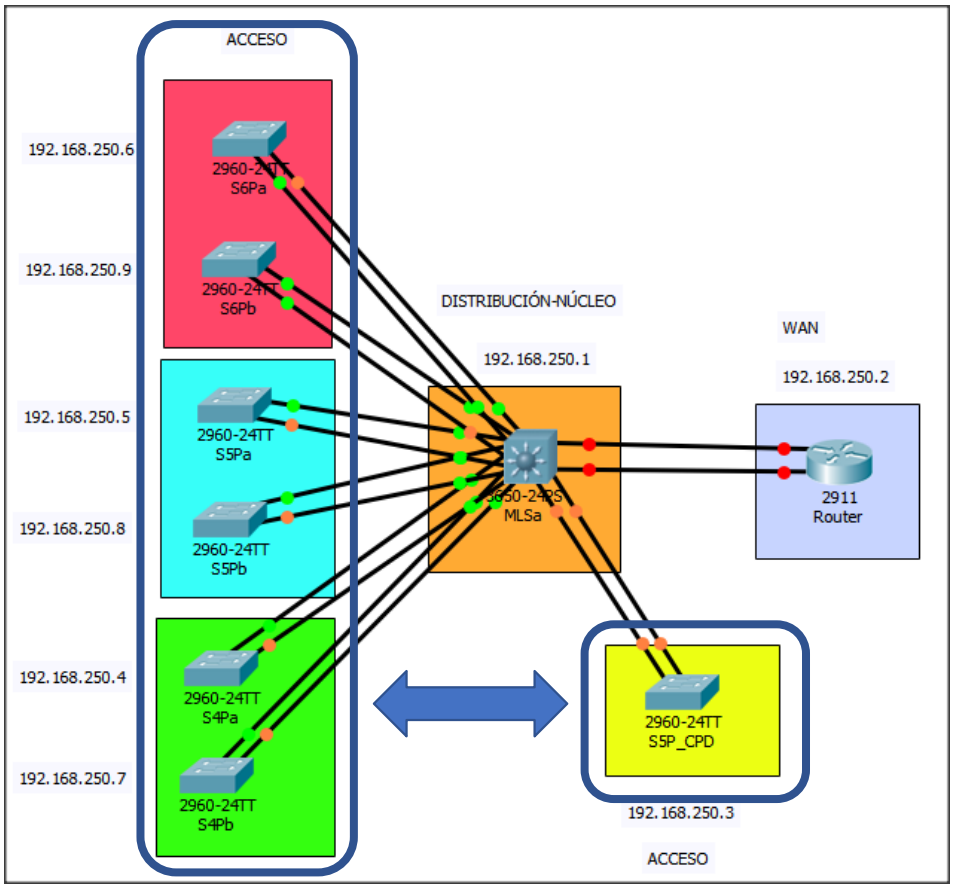


Figura 27. Dispositivos de la capa de acceso en visualización lógica

VISUALIZACIÓN FÍSICA

Los conmutadores de la capa de acceso están ubicados en cada una de las plantas, en sus respectivos armarios de conexiones dentro de las salas de comunicaciones.

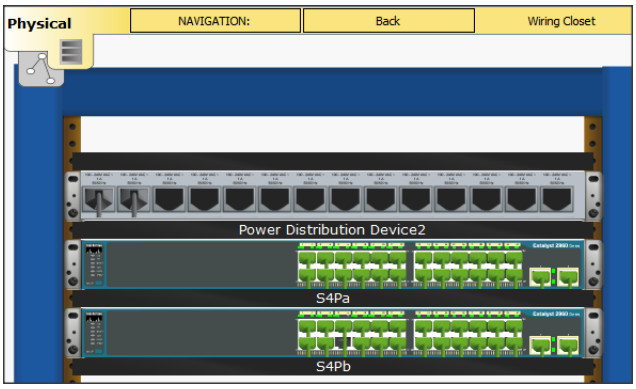


Figura 28. Armario rack 4ª planta

Los conmutadores de la capa de acceso proveen de una serie de servicios y protocolos, los cuales se definieron en la fase de diseño. Estos servicios y

protocolos habilitan ciertas características utilizadas frecuentemente en la capa de acceso. A continuación, se configuran y habilitan estas características:

ENDURECIMIENTO DEL DISPOSITIVO

Para el acceso a los distintos dispositivos se necesita establecer un usuario y contraseña de acceso y una contraseña para entrar en el modo privilegiado. El modo privilegiado es aquel en el que se puede configurar el dispositivo Cisco mediante comandos [2]. Es esencial tener los dispositivos asegurados para evitar accesos no autorizado a los mismos. Para ello, se utilizan los siguientes comandos:

COMANDO	DESCRIPCIÓN
`(config)#enable secret level 15 0 Admin`	Se establece contraseña de acceso al nivel privilegiado.
`(config)#username admin secret Admin`	Se establece un usuario y contraseña con acceso.
`(config)#line vty 0 15`	Se seleccionan todos los puertos virtuales.
`(config-line)#login local`	Se indica que debe utilizar los usuarios locales para logarse.
`(config)#line console 0`	Se selecciona línea de consola
`(config-line)#login local`	Se indica que debe utilizar los usuarios locales para logarse.

Tabla 38. Endurecimiento del dispositivo de red

HABILITAR PORTFAST

Uno de los servicios más interesantes es el denominado *Portfast*. Habilitar *Portfast* permite reducir el tiempo que tarda una interfaz recién encendida antes de poder enviar tráfico, permitiendo a los dispositivos finales enviar tráfico rápidamente. Si no estuviera activado este servicio, los dispositivos tendrían que esperar mucho más tiempo antes de poder enviar tráfico.

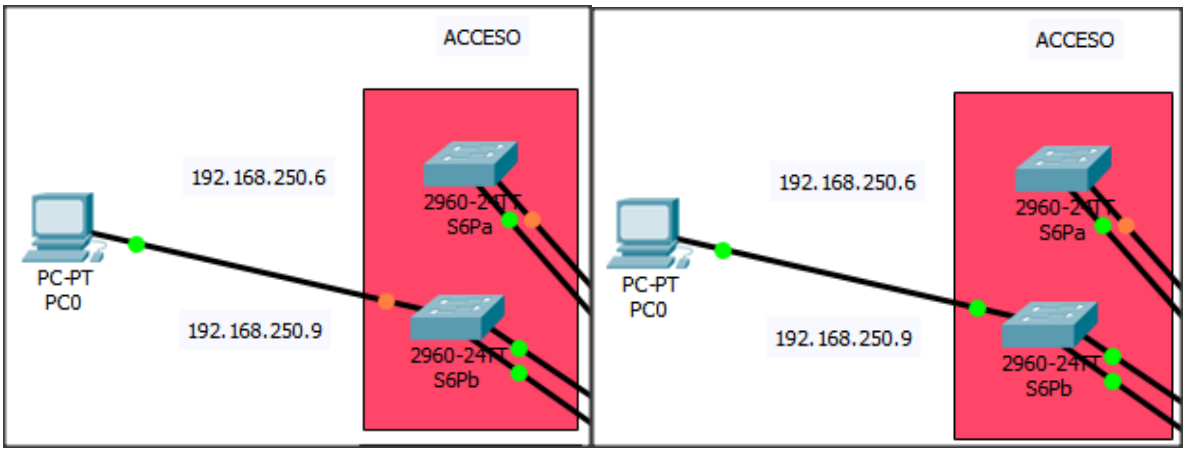


Figura 29. Portfast no activado (color naranja) vs Portfast activado (color verde)

En la Figura 29 se observa como la interfaz conectada al conmutador del equipo PC0 está con un círculo de color naranja, lo que significa que está negociando con la interfaz del equipo, mientras que la imagen de la derecha muestra como la interfaz conectada al conmutador del equipo PC0 está con un círculo de color verde, lo que significa que está operativa y enviando tráfico al conmutador.

Para habilitar *Portfast* de forma global se utiliza el siguiente comando:

```
Switch(config)#spanning-tree portfast default
Switch(config)#
```

Figura 30. Comando para habilitar Portfast

Este comando habilitaría *Portfast* de forma global en todos las interfaces de acceso. Normalmente, las interfaces de acceso suelen corresponder con las interfaces de los dispositivos finales.

Este comando se aplicaría en todos los conmutadores de la capa de acceso, así como en el conmutador del CPD.

PROTECCIÓN DE INTERFAZ POR MAC

Esta mejora protege la interfaz permitiendo sólo un número de dispositivos por interfaz del conmutador. Normalmente, esta protección se utiliza sobre las interfaces de los dispositivos finales. Estos suelen permanecer conectados a la misma interfaz, como es el caso de las estaciones de trabajo. Si en la misma interfaz se desconectara la estación de trabajo y se conectara otro dispositivo, no podría conectarse a nuestra red corporativa como medida de seguridad. Al habilitar esta protección, se guardan las MACs de los dispositivos finales en la

configuración del conmutador. En nuestra infraestructura, la protección habilitada en las interfaces sólo permite una MAC por interfaz conectada a un dispositivo final. La secuencia de comandos sería la siguiente:

COMANDO	DESCRIPCIÓN
`(config)#interface fastEthernet0/1`	Se selecciona interfaz.
`(config-if)#switchport port-security`	Se habilita la protección de la interfaz.
`(config-if)#switchport port-security maximum 1`	Se establece a uno el número de MACs permitidas.
`(config-if)#switchport port-security mac-address sticky`	La MAC será aprendida y guarda en la configuración del conmutador.
`(config-if)#switchport port-security violation restrict`	En caso de violación de seguridad, será incrementado el contador de violaciones y el tráfico será descartado.

Tabla 39. Protección de interfaz

Si se deseara cambiar un dispositivo final de una interfaz a otra, se tendría que limpiar la MAC guardada en la configuración del conmutador para así permitir el aprendizaje del dispositivo en su nueva ubicación. Esto se realiza del siguiente modo:

```
Switch# clear port-security sticky
```

Con este comando se limpian las MACs aprendidas y se vuelven a realizar el proceso de aprendizaje en todos y cada una de las interfaces donde esté configurada la protección de interfaz.

PROTECCIÓN POR SUPLANTACIÓN DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP)

Esta característica permite proteger al servidor legítimo encargado de dar direcciones IP (servidor DHCP) de posibles falsos servidores [4]. Para ello, se activa en cada uno de los conmutadores que puedan ser conectados a algún equipo que tenga instalado un servidor DHCP falso. Por lo tanto, esta mejora se

aplica, en nuestro caso, sobre la capa de acceso, que es dónde se conectan los dispositivos finales.

Al activar esta característica de seguridad hay que indicar qué interfaces son confiables y cuáles no son confiables, es decir, la interfaz o interfaces confiables serán aquellas que conectan directa o indirectamente con el servidor DHCP legítimo, el resto de interfaces se consideran no confiables, dado que podría haber algún dispositivo inesperado conectado intentando suplantar al servidor DHCP legítimo, lo cual provocaría problemas en la asignación de direcciones IP. De esta forma sólo se confía en el tráfico DHCP recibido en las interfaces confiables, descartando el resto.

A continuación, se indican los pasos para activar la protección (Tabla 40):

COMANDO	DESCRIPCIÓN
`(config)#ip dhcp snooping`	Habilita la protección DHCP.
`(config)#ip dhcp snooping vlan 41,42,51,52,53,61,62,63,456`	Habilitar protección sobre las VLANs definidas en el servidor DHCP que ofrecen direcciones IP a los clientes.
`(config)#Interface range fastEthernet 0/1-24`	Se selecciona rango de interfaces no confiables.
`(config-if)#ip dhcp snooping limit rate 100`	Se limita a 100 peticiones por segundo en interfaces no confiables.
`(config)#Interface range gigabitEthernet0/1-2`	Se selecciona rango de interfaces confiables.
`(config-if)#Ip dhcp snooping trust`	Se indica que dichas interfaces son confiables.

Tabla 40. Protección por suplantación de DHCP

Esta configuración se aplica única y exclusivamente a la capa de acceso.

PROTECCIÓN DE TORMENTA BROADCAST

Una *tormenta de broadcast* sucede cuando los paquetes que circulan por la red entran en bucle y son retransmitidas por los dispositivos de red hasta que, los mismos dispositivos de red se saturan o el bucle termina.

La utilización de *broadcast* debe ser controlada en la medida de lo posible, ya que utiliza ancho de banda innecesariamente, consume recursos de los dispositivos de red que deben procesar estos paquetes y consume también recursos de los dispositivos finales que los reciben, que deben analizarlos.

El tráfico Broadcast se genera cuando un dispositivo envía paquetes a todos los dispositivos de la red, por ejemplo, cuando un equipo informático está buscando un servidor DHCP, éste enviará paquetes *broadcast* de forma que todos los dispositivos de la red lo recibirán y lo procesarán.

Por lo tanto, no se puede eliminar al completo la utilización de estos paquetes, dado que son necesarios. Lo que sí se puede es controlar dichos paquetes para que no lleguen a saturar la red. Para ello, se utiliza esta protección. Básicamente, esta protección consiste en limitar el porcentaje de paquetes de *broadcast* en una interfaz, evitando que se sature.

En las interfaces dónde están los dispositivos finales es dónde hay que configurar dicha protección:

COMANDO	DESCRIPCIÓN
`(config)#interface range fastEthernet0/1-24`	Se seleccionan las interfaces de dispositivos finales.
`(config-if)#storm-control broadcast level 20`	Se activa la protección cuando el tráfico broadcast supera el 20% de la velocidad del enlace. Al superarlo, comienza a descartar todos los paquetes broadcast hasta que se reduzca por debajo del 20%.

Tabla 41. Protección de tormenta Broadcast

Se establece en el 20% de la velocidad del enlace, dependiendo de la infraestructura de red, así como de su tamaño, este porcentaje variará según necesidad.

DESACTIVACIÓN DEL SERVICIO CISCO DISCOVERY PROTOCOL (CDP)

El protocolo *CDP* es un protocolo de red propietario de capa 2 de Cisco y es utilizado para compartir información entre dispositivos Cisco directamente conectados indicando su versión de sistema operativo, así como su propia dirección IP.

Cisco recomienda que sea desactivado en las interfaces conectadas a los dispositivos finales para evitar ataques a través de este protocolo. Este protocolo ofrece información a la interfaz destino sobre el dispositivo que está conectado, enviando cierta información que podría ser utilizada para realizar un ataque. Por lo tanto, dicho servicio debe de estar únicamente activo en aquellas interfaces en las cuales haya un intercambio de información seguro, como, por ejemplo, las interfaces conectadas con otros conmutadores Cisco confiables de la infraestructura de red. En estas interfaces si tiene sentido el tener activo el servicio *CDP* que, por defecto, viene habilitado en todas las interfaces.

Para desactivar el servicio *CDP* basta con realizar los siguientes pasos:

COMANDO	DESCRIPCIÓN
`(config)#interface range fastEthernet0/1-24`	Se seleccionan las interfaces de los dispositivos finales.
`(config-if)#no cdp enable`	Se desactiva el protocolo CDP en las interfaces de los dispositivos finales.

Tabla 42. Desactivación del protocolo CDP

CONFIGURACIÓN DE INTERFACES TRONCALES (TRUNK)

Las interfaces troncales son aquellas que permiten la transmisión de tráfico de más de una VLAN. Estas interfaces son necesarias para nuestra infraestructura, dado que se necesitan tener más de una VLAN en cada uno de los distintos conmutadores de la capa de acceso. Estas VLANs corresponden con los distintos direccionamientos de cada uno de los departamentos que se definieron en la fase anterior (Tabla 5). Estos direccionamientos son diferentes para cada uno de los departamentos de las distintas plantas.

Por lo tanto, las interfaces que conectan la capa de acceso con la capa de distribución-núcleo necesitan transportar más de una VLAN por sus enlaces. Es por ello necesaria la configuración de interfaces troncales que permitan comunicar las distintas VLANs entre sí, a través del conmutador de la capa de distribución-núcleo. Para hacer esto, hay que introducir los siguientes comandos en los conmutadores de la capa de acceso:

COMANDO	DESCRIPCIÓN
`(config)#interfaces range gigabitEthernet0/1-2`	Se seleccionan las interfaces que serán interfaces troncales.
`(config.if)#switchport mode trunk`	Se indica el modo troncal como modo de funcionamiento de la interfaz.

Tabla 43. Configuración de interfaces troncales en la capa de acceso

La configuración debe realizar en ambos extremos del enlace, tanto en la capa de acceso como en la capa de distribución-núcleo. La configuración para la capa de distribución-núcleo se verá en su correspondiente apartado.

CONFIGURACIÓN DEL CLIENTE VLAN TRUNKING PROTOCOL (VTP)

VTP son las siglas de VLAN Trunking Protocol y se trata de un protocolo de capa 2 usado para configurar y administrar las VLANs en los dispositivos Cisco. Permite crear, borrar y renombrar VLANs de una forma centralizada, reduciendo la necesidad de configurar una misma VLAN en todos y cada uno de los dispositivos Cisco de la infraestructura de red.

VTP puede operar de 3 formas distintas:

- **Servidor**. Es el modo por defecto y permite crear, eliminar y modificar VLANs. Su cometido es anunciar su configuración al resto de conmutadores que estén correctamente configurados en su mismo dominio y con la misma contraseña. Para ello, utiliza las interfaces troncales o puertos *trunk* definidos previamente.

- **Cliente**. En este modo no se pueden eliminar, modificar ni crear VLANs. Tan sólo sincroniza su información de VLANs con las del servidor, actualizándola si fuera necesario.
- **Transparente**. Permite crear, modificar y eliminar VLANs, pero éstas son de carácter local. No procesa las actualizaciones VTP enviadas por el servidor, pero sí reenvía dichas actualizaciones a los conmutadores del mismo dominio.

Para el caso que nos ocupa, los conmutadores de capa de acceso serán configurados en el **modo cliente** siendo el conmutador de la capa de distribución-núcleo el encargado de distribuir las VLANs al resto de conmutadores de la capa de acceso.

Para configurar el conmutador como cliente VTP se necesita realizar la siguiente configuración:

COMANDO	DESCRIPCIÓN
`(config)#vtp mode client`	Se habilita el modo cliente VTP.
`(config)#vtp domain` *`Empresa`*	Se establece el dominio VTP.
`(config)#vtp versión 2`	Se selecciona la versión 2 de VTP.
`(config)#vtp password` *`E5PmlsVTP2`*	Se establece la contraseña de VTP.

Tabla 44. Configuración del cliente VTP

Utilizando esta configuración, queda configurado el cliente VTP en los conmutadores de la capa de acceso. En el apartado correspondiente se configurará el servidor VTP utilizando el mismo dominio y la misma contraseña para que pueda distribuir correctamente las VLANs que se creen.

CONFIGURACIÓN DEL AGREGADO DE ENLACES (LAG)

El agregado de enlaces (LAG) permite formar un enlace lógico utilizando para ello varias interfaces físicas, con las mismas características de velocidad y modo de funcionamiento, permitiendo ampliar el ancho de banda, balanceo de carga y habilitando la tolerancia a fallos de las interfaces físicas que lo componen.

Para que funcione correctamente esta tecnología, debe ser configurada en los dos extremos del enlace. En nuestro caso, debe ser configurada en la capa de acceso y en la capa de distribución-núcleo.

Cisco utiliza la tecnología EtherChannel, que se basa en el estándar de agregado de enlaces 802.3ad de IEEE. El agregado de enlaces te permite tener hasta ocho interfaces físicas conectadas simultáneamente para ofrecer redundancia, ampliar el ancho de banda y balanceo de carga [2]. Al configurar las interfaces físicas como agregado de enlaces, éstas se verían como una única interfaz lógica formada por tantas interfaces físicas como se desee hasta un máximo de ocho interfaces. En nuestro caso, estarán formados por dos interfaces 10/100/1000Mbps.

Los modos de funcionamiento de un EtherChannel pueden ser:

- **PAgP**: es un protocolo propietario de Cisco. El protocolo se encarga de agrupar las interfaces con características similares. Se pueden configurar de dos modos:
  - **Desirable**: establece la interfaz en modo activo, negociará el estado y puede iniciar una negociación.
  - **Auto**: configura la interfaz en modo pasivo y sólo responderá a paquetes PAgP recibidos, nunca inicia una negociación.
- **LACP**: es similar a PAgP y es un protocolo definido en el estándar 802.3ad. Tiene también dos modos de configuración:
  - **Active**: está habilitado para iniciar una negociación.
  - **Passive**: no puede iniciar una negociación, pero sí puede responder a negociaciones generadas por otras interfaces.

La configuración que se va a utilizar es **LACP** en **modo Active**. Para poder formar un enlace EtherChannel con LACP uno de los extremos tiene que estar en modo *Active* y el otro extremo en modo *Passive*.

La configuración del EtherChannel se realiza del siguiente modo:

COMANDO	DESCRIPCIÓN
`(config)#interface range gigabitEthernet0/1-2`	Se seleccionan las interfaces que formarán el EtherChannel.
`(config-if)#-channel-group 1 mode active`	Se habilita mediante el comando channel-group. Se establece el identificador 1 para el EtherChannel. Se establece el modo *LACP active*.

Tabla 45. Configuración de EtherChannel activo

La decisión de configurar el extremo del conmutador de la capa de acceso como modo *Active* corresponde a buenas prácticas de seguridad perimetral, dado que el conmutador de la capa de distribución-núcleo no negociará con ningún conmutador que se conecte a él a menos que éste inicie la negociación.

CONMUTADOR DE CAPA DE DISTRIBUCIÓN-NÚCLEO

En este apartado se realiza la implementación de aquellos servicios y configuraciones para el conmutador de la capa de distribución-núcleo.

VISUALIZACIÓN LÓGICA

El conmutador de la capa de distribución-núcleo se encuentra en la parte central de la visualización lógica.

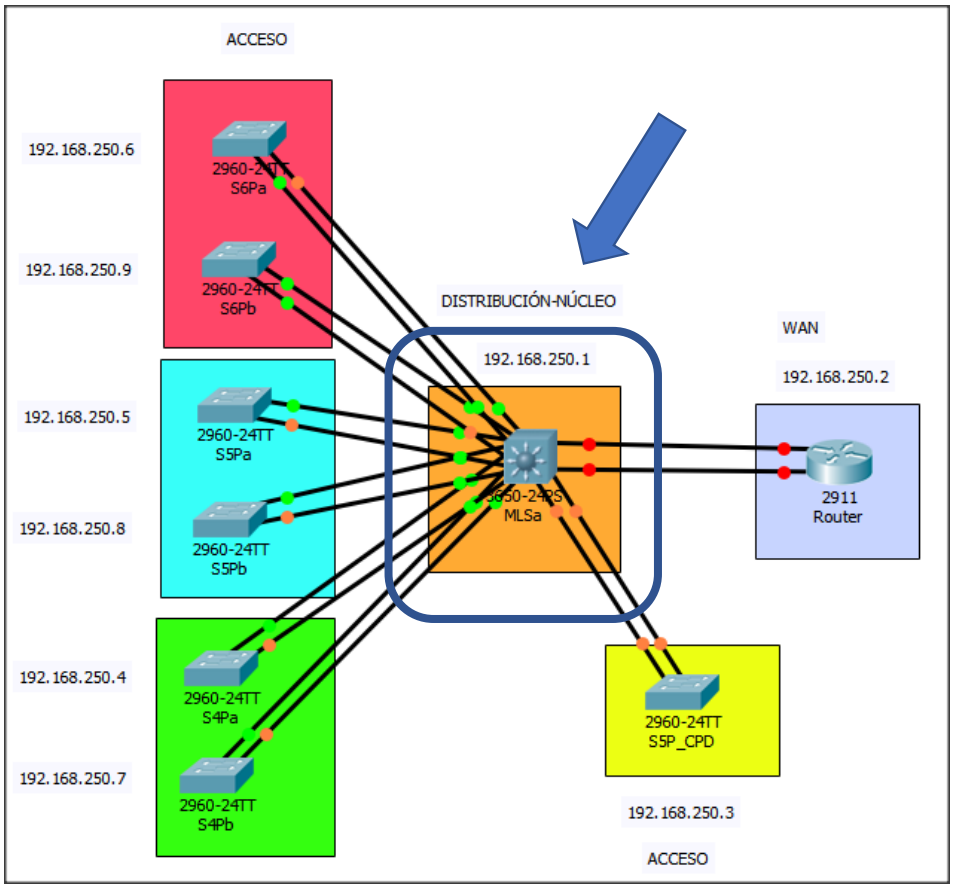


Figura 31. Capa de distribución-núcleo en visualización lógica

En la Figura 31, se puede observar cómo todos los conmutadores de la capa de acceso se conectan al conmutador de la capa de distribución-núcleo utilizando dos enlaces para ofrecer redundancia. Además, el enrutador corporativo también se conecta al conmutador de la capa de distribución-núcleo para ofrecer Internet y acceso externo.

VISUALIZACIÓN FÍSICA

El conmutador de la capa de distribución-núcleo se ubica en la 5ª planta en el armario rack de la Sala de comunicaciones de dicha planta.

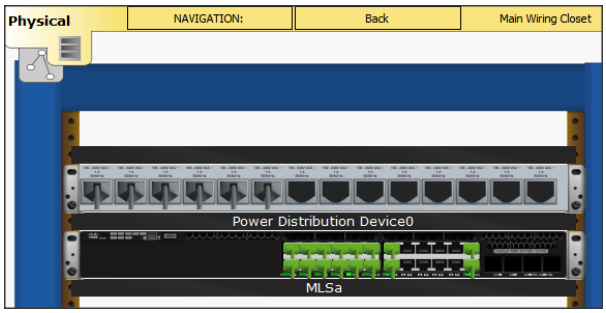


Figura 32. Conmutador de la capa de distribución-núcleo en visualización física

A continuación, para el conmutador de la capa de distribución-núcleo también es necesario configurar una serie de servicios y protocolos. Las características que habilitan estos servicios y protocolos son las siguientes:

ENDURECIMIENTO DEL DISPOSITIVO

Para el acceso a los distintos dispositivos se necesita establecer un usuario y contraseña de acceso y una contraseña para entrar en el modo privilegiado. El modo privilegiado es aquel en el que se puede configurar el dispositivo Cisco mediante comandos. Es esencial tener los dispositivos asegurados para evitar accesos no autorizado a los mismos. Para ello, se utilizan los comandos vistos en la Tabla 38.

CONFIGURACIÓN DEL SERVIDOR DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP)

En el conmutador de la capa de distribución-núcleo es dónde se va a configurar el servidor DHCP, el cual suministra las distintas direcciones para cada uno de los dispositivos ubicados en las distintas plantas. Para llevar a cabo está configuración se necesita la información de cada uno de los direccionamientos que suministrará el servidor DHCP. Para ello, se utiliza la siguiente tabla:

PLANTA	VLAN	DIRECCIONAMIENTO	MÁSCARA	GRUPO
4ª	41	192.168.40.0/27	255.255.255.224	1D4P
	42	192.168.40.32/28	255.255.255.240	2D4P
5ª	51	192.168.50.0/28	255.255.255.240	1D5P
	52	192.168.50.16/28	255.255.255.240	2D5P
	53	192.168.50.32/28	255.255.255.240	3D5P
6ª	61	192.168.60.0/27	255.255.255.224	1D6P
	62	192.168.60.32/28	255.255.255.240	2D6P
	63	192.168.60.48/28	255.255.255.240	3D65P
4ª, 5ª y 6ª	456	172.16.0.0/26	255.255.255.**192***	IDC

Tabla 46. Rango de direcciones IP según planta y VLAN

*Dato actualizado tras optimización en la fase de diseño

Los comandos que se deben utilizar para definir cada uno de los grupos de direcciones son los siguientes:

COMANDO	DESCRIPCIÓN
`(config)#ip dhcp excluded-address 192.168.40.1`	Se indica la dirección IP excluida del grupo a crear. En este caso es la dirección de la puerta de enlace.
`(config-if)#ip dhcp pool 1D4P`	Se crea el grupo con nombre 1D4P que corresponde con el primero a crear.
`(dhcp-config)#network 192.168.40.0 255.255.255.224`	Se establece el grupo de direcciones IP a suministrar.
`(dhcp-config)#default-router 192.168.40.1`	Se define la puerta de enlace.
`(dhcp-config)#dns-server 172.16.1.2`	Se define el servidor DNS.

Tabla 47. Configuración del servidor DHCP

Este proceso se realiza con cada uno de los grupos indicados anteriormente. Un total de 9 grupos diferentes de direcciones a suministrar, dependiendo de la VLAN a la que pertenezca. La puerta de enlace se corresponde con la primera dirección IP posible dentro del grupo (*pool*) definido y se le asignará al conmutador de la capa de distribución-núcleo, ya que será la puerta de enlace de cada uno de los grupos definidos.

El servidor DNS corresponderá con el servidor corporativo, el cual posee el servicio DNS activo. Un ejemplo para el que se utiliza el servidor DNS es para resolver la IP del servidor de correo o del servidor IdC, aunque este tema, se tratará más adelante.

El grupo *IDC* correspondiente a los elementos IdC tiene dos direcciones excluidas, la puerta de enlace y el servidor IdC. La puerta de enlace corresponde a la primera dirección IP posible y al servidor IdC se le asigna la siguiente dirección IP posible (172.16.0.2) (ver Figura 33).

Tras configurar cada uno de los grupos utilizando los comandos anteriores, la configuración final queda del siguiente modo:

```
ip dhcp excluded-address 172.16.0.1 172.16.0.2
ip dhcp excluded-address 192.168.60.1
ip dhcp excluded-address 192.168.50.1
ip dhcp excluded-address 192.168.60.33
ip dhcp excluded-address 192.168.60.49
ip dhcp excluded-address 192.168.50.17
ip dhcp excluded-address 192.168.50.33
ip dhcp excluded-address 192.168.40.1
ip dhcp excluded-address 192.168.40.33
```

Figura 33. Exclusiones de los grupos

Se han excluido del grupo las direcciones correspondientes a las distintas puertas de enlace.

```
ip dhcp pool IDC
 network 172.16.0.0 255.255.255.192
 default-router 172.16.0.1
 dns-server 172.16.1.2
ip dhcp pool 2D6P
 network 192.168.60.32 255.255.255.240
 default-router 192.168.60.33
 dns-server 172.16.1.2
ip dhcp pool 3D6P
 network 192.168.60.48 255.255.255.240
 default-router 192.168.60.49
 dns-server 172.16.1.2
ip dhcp pool 1D5P
 network 192.168.50.0 255.255.255.240
 default-router 192.168.50.1
 dns-server 172.16.1.2
ip dhcp pool 2D5P
 network 192.168.50.16 255.255.255.240
 default-router 192.168.50.17
 dns-server 172.16.1.2
ip dhcp pool 3D5P
 network 192.168.50.32 255.255.255.224
 default-router 192.168.50.33
 dns-server 172.16.1.2
ip dhcp pool 1D4P
 network 192.168.40.0 255.255.255.224
 default-router 192.168.40.1
 dns-server 172.16.1.2
ip dhcp pool 2D4P
 network 192.168.40.32 255.255.255.240
 default-router 192.168.40.33
 dns-server 172.16.1.2
ip dhcp pool 1D6P
 network 192.168.60.0 255.255.255.224
 default-router 192.168.60.1
 dns-server 172.16.1.2
```

Figura 34. Definición de los grupos del servidor DHCP

Una vez realizada la configuración del servidor DHCP (Figura 33 y Figura 34), el siguiente paso es configurar cada una de las VLANs con sus respectivas direcciones IP. Este paso es necesario para vincular el grupo o pool a la VLAN correspondiente y para configurar la puerta de enlace. Por lo tanto, se realiza la siguiente configuración:

COMANDO	DESCRIPCIÓN
(config)##interface vlan 41	Se crea la VLAN 41 – 1D4P.
(config-if)#ip address 192.168.40.1 255.255.255.224	Asignación de IP a la puerta de enlace.
(config-if)#no shutdown	Se habilita la VLAN.
(config)##interface vlan 42	Se crea la VLAN 42 – 2D4P.
(config-if)#ip address 192.168.40.33 255.255.255.240	Asignación de IP a la puerta de enlace.
(config-if)#no shutdown	Se habilita la VLAN.
…	…
(config)##interface vlan 456	Se crea la VLAN 456 - IDC.
(config-if)#ip address 172.16.0.1 255.255.255.192	Asignación de IP a la puerta de enlace.
(config-if)#no shutdown	Se habilita la VLAN.

Tabla 48. Asignación de dirección IP a cada VLAN

Con este proceso quedan establecidas todas las puertas de enlace que utilizan el servidor DHCP. Indicar que hay 2 segmentos de red que no están contemplados en el servidor DHCP, como son el *direccionamiento de administración* y el *direccionamiento del CPD*. Ambos direccionamientos son estáticos, ya que los dispositivos siempre tendrán la misma dirección IP.

CONFIGURACIÓN DE INTERFACES TRONCALES

Como sucediera en el caso de la capa de acceso, en la capa de distribución-núcleo también es necesaria la configuración como interfaces troncales de las interfaces que conectan con la capa de acceso.

Para ello, bastaría con utilizar los mismos comandos que en la configuración de la capa de acceso, con una salvedad:

COMANDO	DESCRIPCIÓN
(config)#interfaces range gigabitEthernet0/1-2	Se seleccionan las interfaces que serán interfaces troncales.
(config-if)#switchport trunk encapsulation dot1q	Se indica la encapsulación a utilizar (dot1q) correspondiente al *modo troncal*.

`(config.if)#switchport mode trunk`	Se indica el *modo troncal* como modo de funcionamiento de la interfaz.

Tabla 49. Configuración de las interfaces troncales en la capa de distribución-núcleo

Esta salvedad es debida al modelo de conmutador utilizado, en conmutadores de capas superiores es necesario indicar el tipo de encapsulación a utilizar (*dot1q*) o no se puede habilitar el modo troncal (*trunk*) en la interfaz. De esta forma quedaría establecido el enlace troncal en ambos extremos.

CONFIGURACIÓN DEL SERVIDOR VLAN TRUNKING PROTOCOL (VTP)

A continuación, se configura VTP para que opere en **modo servidor**. Este modo si permite crear, eliminar y modificar las VLANs que se definan en el dispositivo servidor. Las VLANs creadas son distribuidas al resto de dispositivos que formen parte del dominio VTP.

Para realizar la configuración del servidor VTP en el conmutador de la capa de distribución-núcleo son necesarios los siguientes comandos:

COMANDO	DESCRIPCIÓN
`(config)#vtp mode server`	Se habilita el modo servidor VTP.
`(config)#vtp domain` *`Empresa`*	Se establece el dominio VTP.
`(config)#vtp versión 2`	Se selecciona la versión 2 de VTP.
`(config)#vtp password` *`E5PmlsVTP2`*	Se establece la contraseña de VTP.

Tabla 50. Configuración del servidor VTP

Utilizando esta configuración, queda configurado el servidor VTP en el conmutador de la capa de distribución-núcleo. A partir de entonces, todas las VLANs definidas en el conmutador comenzarán a distribuirse al resto de conmutadores de la capa de acceso que estén configurados con el mismo dominio y contraseña. Las interfaces troncales, que previamente han sido configurados, permiten la distribución de las VLANs.

CONFIGURACIÓN DE ROOT SPANNING-TREE

Spanning-Tree [12] es un protocolo de capa 2 que se utiliza en dispositivos de red. *Spanning-Tree* es capaz de generar y mantener una estructura en árbol libre de bucles entre sus nodos, donde los nodos son los dispositivos de red. Esta estructura es negociada entre los distintos dispositivos de red conectados entre sí, siendo elegido uno de ellos como *Root*. El *Root* es el responsable de la creación de esta estructura libre de bucles, así como el responsable de mantenerla, por lo que su elección es fundamental.

Si no se especifica, la elección de *Root* será un proceso en el cual los distintos dispositivos negocian entre ellos, obteniendo a veces un resultado no satisfactorio. Por lo tanto, es importante elegir correctamente el nodo principal o *Root* de la infraestructura de red.

Una forma de elegir el *Root* de *Spanning-Tree* es mediante la utilización del siguiente comando desde CLI:

```
MLSa(config)#spanning-tree vlan 41,42,51,52,53,61,62,63,250,456,654 priority 0
```

Si se analiza este comando con mayor profundidad se pueden observar los siguientes argumentos:

- *vlan 41,42,51,52,53,61,62,63,250,456,654:* Indica las VLANs que están implicadas. En este caso, corresponde con todas las VLANs que se han definido en la infraestructura de red.
  - *VLANs de 4ª planta*: 41 y 42.
  - *VLANs de 5ª planta*: 51, 52 y 53.
  - *VLANs de 6ª planta*: 61, 62 y 63.
  - *VLAN de Administración: 250.*
  - *VLAN de IdC*: 456.
  - *VLAN de CPD*: 654.
- *priority 0*: Se asigna la prioridad 0, siendo 0 la de mayor valor y 61440 la de menor valor.

Al aplicar este comando sobre el conmutador de la capa de distribución-núcleo se está indicando que el *Root* de *spanning-tree* sea él mismo.

Esto se hace para evitar que llegue a ser *Root* algún dispositivo no deseado. Imaginemos que alguien instala un nuevo conmutador dentro de la infraestructura de red y al iniciarse el proceso de elección del *Root*, este nuevo conmutador, es asignado como *Root*. Este hecho sería peligroso para la infraestructura de red. Una forma de evitarlo sería estableciendo quién va a ser el *Root* en nuestra infraestructura de red.

CONFIGURACIÓN DEL AGREGADO DE ENLACES (LAG)

El agregado de enlaces (LAG) que se va a implementar es el otro extremo del agregado de enlaces que se vio en la capa de acceso. El EtherChannel que se configuró en la capa de acceso, fue LACP en modo *Active*. En esta ocasión, se realiza la configuración **LACP** para la capa de distribución-núcleo en **modo Passive**.

Hay que tener en cuenta que el conmutador de capa de distribución-núcleo agrega todos los enlaces de la capa de acceso, por lo que, se requieren más de un EtherChannel en la configuración, un EtherChannel por cada conmutador de la capa de acceso incluyendo el ubicado en el CPD (Tabla 51).

A continuación, se muestra la distribución de los enlaces EtherChannel:

CAPA DE ACCESO		**CAPA DE DISTRIBUCIÓN-NÚCLEO**	
CONMUTADOR	**INTERFAZ**	**INTERFAZ**	**ETHERCHANNEL**
S4Pa	GigabitEthernet0/1	GigabitEthernet1/0/1	1
S4Pa	GigabitEthernet0/2	GigabitEthernet1/0/2	
S4Pb	GigabitEthernet0/1	GigabitEthernet1/0/3	2
S4Pb	GigabitEthernet0/2	GigabitEthernet1/0/4	
S5Pa	GigabitEthernet0/1	GigabitEthernet1/0/5	3
S5Pa	GigabitEthernet0/2	GigabitEthernet1/0/6	
S5Pb	GigabitEthernet0/1	GigabitEthernet1/0/7	4
S5Pb	GigabitEthernet0/2	GigabitEthernet1/0/8	
S6Pa	GigabitEthernet0/1	GigabitEthernet1/0/9	5
S6Pa	GigabitEthernet0/2	GigabitEthernet1/0/10	
S6Pb	GigabitEthernet0/1	GigabitEthernet1/0/11	6

S6Pb	GigabitEthernet0/2	GigabitEthernet1/0/12	
S5P_CPD	GigabitEthernet0/1	GigabitEthernet1/0/13	7
S5P_CPD	GigabitEthernet0/2	GigabitEthernet1/0/14	

Tabla 51. Resumen de los enlaces EtherChannel

La configuración de los enlaces EtherChannel de la capa de distribución-núcleo, en este caso, se realizan del siguiente modo:

COMANDO	DESCRIPCIÓN
`(config)#interface range gigabitEthernet0/1-2`	Se seleccionan las interfaces que formarán el EtherChannel.
`(config-if)#channel-group 1 mode passive`	Se habilita mediante el comando channel-group. Se establece el identificador 1 para el EtherChannel. Se establece el modo LACP passive.
…	
`(config)#interface range gigabitEthernet0/13-14`	Se seleccionan las interfaces que formarán el EtherChannel.
`(config-if)#channel-group 7 mode passive`	Se habilita mediante el comando channel-group. Se establece el identificador 7 para el EtherChannel. Se establece el modo LACP passive.

Tabla 52. Configuración de enlaces EtherChannel pasivos

Una vez realizada la configuración de los enlaces EtherChannel, los dispositivos de red comenzarán a negociar sus enlaces EtherChannel (Figura 35).

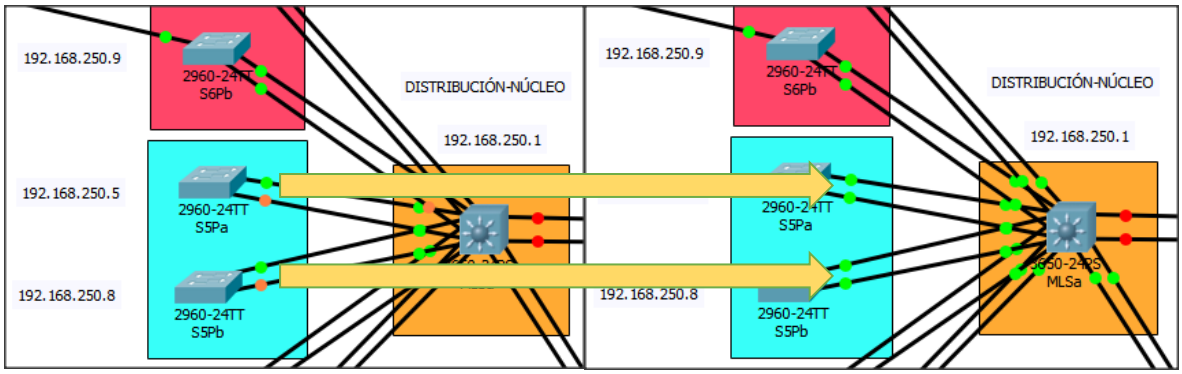


Figura 35. Enlaces EtherChannel en funcionamiento

En la Figura 35, cuando el estado de las interfaces cambie de color naranja al color verde se habrá terminado la negociación de los enlaces EtherChannel y estarán plenamente operativos.

ENRUTAMIENTO ENTRE VLANS Y RUTA POR DEFECTO

Uno de los servicios más importantes que debe ofrecer el conmutador de la capa de distribución-núcleo es el enrutamiento del tráfico de red [5]. El conmutador de la capa de distribución-núcleo es el responsable de enrutar el tráfico que normalmente proviene de la capa de acceso a su destino.

Inicialmente, se va a permitir la comunicación entre todas las VLANs y además, se va a dotar al conmutador de la capa de distribución-núcleo de una ruta por defecto para la salida hacia Internet.

El conmutador de la capa de distribución-núcleo debe configurarse como enrutador y, además, debe permitir que el enrutador de la empresa conozca las rutas que debe seguir para poder comunicarse con las diferentes VLANs de la red corporativa. Para ello, se utilizan los protocolos de enrutamiento. En nuestro caso, la configuración queda de la siguiente forma:

COMANDO	DESCRIPCIÓN
`(config)#ip routing`	Se habilita el conmutador como enrutador.
`(config)#router rip`	Se habilita el protocolo de enrutamiento.
`(config-router)#version 2`	Se utiliza la versión mejorada de RIP.

(config-router)#network 172.16.0.0	Se publican todas las rutas a las que puede accederse desde el conmutador.
(config-router)#network 192.168.0.0	
(config-router)#network 192.168.40.0	
(config-router)#network 192.168.50.0	
(config-router)#network 192.168.60.0	
(config-router)#no auto-summary	Se desactiva el resumen de rutas.

Tabla 53. Enrutamiento con el protocolo RIP

Con esta configuración el conmutador de la capa de distribución-núcleo habilita el protocolo de enrutamiento **Routing Information Protocol** (*RIP*) y publica las rutas accesibles por el conmutador.

A continuación, se habilita una ruta por defecto en el conmutador de la capa de distribución-núcleo para todos aquellos paquetes cuyo destino no sea conocido por el protocolo de enrutamiento RIP. Como, por ejemplo, los paquetes destinados a Internet.

Para ello, se realiza la siguiente configuración en el conmutador:

COMANDO	DESCRIPCIÓN
(config)#ip route 0.0.0.0 0.0.0.0 interface gigabitEthernet1/0/24	Se define la ruta por defecto a través de la interfaz conectada con el enrutador WAN.

Tabla 54. Ruta por defecto

Al definir la ruta por defecto, los paquetes cuyo destino no coincidan con ninguna de las rutas definidas en el protocolo de enrutamiento RIP utilizarán esta ruta como salida.

Una vez definida la interfaz de ruta por defecto es conveniente configurar dicha interfaz con una dirección IP. Al tratarse de una interfaz directamente conectada con el enrutador corporativo, únicamente es necesario un rango de direcciones para dos dispositivos, que corresponden con los dos extremos del enlace formado. El direccionamiento que se utiliza será 192.168.0.0/30.

COMANDO	DESCRIPCIÓN
(config)#interface gigabitEthernet1/0/24	Se define la ruta por defecto a través de la interfaz conectada con el enrutador WAN.

`(config-if)#no switchport`	Se indica que es una interfaz de capa 3.
`(config-if)#ip address 192.168.0.2 255.255.255.252`	Se configura su dirección IP y su máscara /30.

Tabla 55. Configuración de la interfaz por defecto

RESTRICCIONES ENTRE VLANS

En la fase de diseño se establecieron una serie de restricciones entre los distintos departamentos y sus respectivas VLANs. Para realizar las restricciones se utilizan las **Listas de Control de Acceso** (*ACL*) [3]. Las ACL permiten controlar el tráfico, permitiendo o denegando el tráfico de red. Hay diferentes tipos de ACL, las más utilizadas son las estándar (*standard*) y las extendidas (*extended*). Las estándar permiten filtrar por direcciones IP origen, mientras que las extendidas permiten filtrar por IP origen, IP destino y el puerto. En nuestro caso, es necesario utilizar las ACL extendidas ya que se necesita restringir el tráfico origen hacia un destino especificado. Estas ACLs se configuran lo más cerca posible del origen del tráfico, en la entrada de la puerta de enlace.

A continuación, se muestran las restricciones definidas para cada una de las VLANs, así como las ACLs a definir:

VLAN - ORIGEN		**ACCIÓN**	**VLAN - DESTINO**	
41	192.168.40.0/27	PERMITIR	42	192.168.40.32/28
		DENEGAR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		PERMITIR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		PERMITIR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 56. Restricciones VLAN 41

La ACL extendida debe, primero, denegar todo aquel tráfico no permitido y para finalizar, permitir el resto del tráfico. Por lo que, la ACL nombrada para la VLAN 41 queda del siguiente modo:

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended VLAN41`	Se crea ACL extendida llamada *VLAN41*.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.40.0 0.0.0.31 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 57. ACL VLAN 41

Una vez se ha definido la ACL para la VLAN 41 hay que aplicar la ACL sobre la interfaz correspondiente. En este caso, se aplica sobre la interfaz VLAN 41, que es la puerta de enlace, del siguiente modo:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 41`	Se entra en la configuración de la VLAN 41.
`(config-if)#ip access-group VLAN41 in`	Se vincula la ACL nombrada *VLAN41* a la entrada de tráfico de la interfaz VLAN 41.

Tabla 58. ACL aplicada a VLAN 41

Este proceso hay que realizarlo para cada una de las VLANs que tienen establecidas restricciones (ver Figura 12).

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
42	192.168.40.32/28	PERMITIR	41	192.168.40.0/27
		DENEGAR	51	192.168.50.0/28

		DENEGAR	52	192.168.50.16/28
		PERMITIR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		PERMITIR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 59. Restricciones VLAN 42

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended VLAN42`	Se crea ACL extendida llamada *VLAN42*.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.40.32 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 60. ACL VLAN 42

Una vez se ha definido la ACL para la VLAN 42 se aplicar sobre la interfaz de la puerta de enlace correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 42`	Se entra en la configuración de la VLAN 42.
`(config-if)#ip access-group VLAN42 in`	Se vincula la ACL nombrada *VLAN42* a la entrada de tráfico de la interfaz VLAN 42.

Tabla 61. ACL aplicada a VLAN 42

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
51	192.168.50.0/28	DENEGAR	41	192.168.40.0/27
		DENEGAR	42	192.168.40.32/28
		PERMITIR	52	192.168.50.16/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		PERMITIR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 62. Restricciones VLAN 51

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended` *VLAN51*	Se crea ACL extendida llamada *VLAN51*.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.40.0 0.0.0.31`	Se deniega tráfico a VLAN 41.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.40.32 0.0.0.15`	Se deniega tráfico a VLAN 42.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.60.0 0.0.0.31`	Se deniega tráfico a VLAN 61.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.50.0 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 63. ACL VLAN 51

Una vez se ha definido la ACL para la VLAN 51 se aplicar sobre la interfaz de la puerta de enlace correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 51`	Se entra en la configuración de la VLAN 51.

`(config-if)#ip access-group VLAN51 in`	Se vincula la ACL nombrada *VLAN51* a la entrada de tráfico de la interfaz VLAN 51.

Tabla 64. ACL aplicada a VLAN 51

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
52	192.168.50.16/28	DENEGAR	41	192.168.40.0/27
		DENEGAR	42	192.168.40.32/28
		PERMITIR	51	192.168.50.0/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 65. Restricciones VLAN 52

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended` *VLAN52*	Se crea ACL extendida llamada *VLAN52*.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.40.0 0.0.0.31`	Se deniega tráfico a VLAN 41.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.40.32 0.0.0.15`	Se deniega tráfico a VLAN 42.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.60.0 0.0.0.31`	Se deniega tráfico a VLAN 61.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.50.16 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.

`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 66. ACL VLAN 52

Una vez se ha definido la ACL para la VLAN 52 se aplicar sobre la interfaz correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 52`	Se entra en la configuración de la VLAN 52.
`(config-if)#ip access-group VLAN52 in`	Se vincula la ACL nombrada *VLAN52* a la entrada de tráfico de la interfaz VLAN 52.

Tabla 67. ACL aplicada a VLAN 52

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
53	192.168.50.32/28	PERMITIR	41	192.168.40.0/27
		PERMITIR	42	192.168.40.32/28
		DENEGAR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 68. Restricciones VLAN 53

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended` *VLAN53*	Se crea ACL extendida llamada *VLAN53*.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.60.0 0.0.0.31`	Se deniega tráfico a VLAN 61.

`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.50.32 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 69. ACL VLAN 53

A continuación, se aplica sobre la interfaz de la puerta de enlace correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 53`	Se entra en la configuración de la VLAN 53.
`(config-if)#ip access-group VLAN53 in`	Se vincula la ACL nombrada *VLAN53* a la entrada de tráfico de la interfaz VLAN 53.

Tabla 70. ACL aplicada a VLAN 53

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
61	192.168.60.0/27	PERMITIR	41	192.168.40.0/27
		PERMITIR	42	192.168.40.32/28
		DENEGAR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	62	192.168.60.32/28
		PERMITIR	63	192.168.60.48/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 71. Restricciones VLAN 61

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended VLAN61`	Se crea ACL extendida llamada *VLAN61*.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.60.0 0.0.0.31 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 72. ACL VLAN 61

A continuación, se aplica sobre la interfaz correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 61`	Se entra en la configuración de la VLAN 61.
`(config-if)#ip access-group VLAN61 in`	Se vincula la ACL nombrada *VLAN61* a la entrada de tráfico de la interfaz VLAN 61.

Tabla 73. ACL aplicada a VLAN 61

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
62	192.168.60.32/28	DENEGAR	41	192.168.40.0/27
		DENEGAR	42	192.168.40.32/28
		DENEGAR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	61	192.168.60.0/27
		DENEGAR	63	192.168.60.48/28

		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 74. Restricciones VLAN 62

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended` *VLAN62*	Se crea ACL extendida llamada *VLAN62*.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.40.0 0.0.0.31`	Se deniega tráfico a VLAN 41.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.40.32 0.0.0.15`	Se deniega tráfico a VLAN 42.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.60.0 0.0.0.31`	Se deniega tráfico a VLAN 61.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.60.32 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 75. ACL VLAN 62

A continuación, se aplica sobre la interfaz de la puerta de enlace correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 62`	Se entra en la configuración de la VLAN 62.
`(config-if)#ip access-group VLAN62 in`	Se vincula la ACL nombrada *VLAN62* a la entrada de tráfico de la interfaz VLAN 62.

Tabla 76. ACL aplicada a VLAN 62

VLAN - ORIGEN		ACCIÓN	VLAN - DESTINO	
63	192.168.60.48/28	DENEGAR	41	192.168.40.0/27
		DENEGAR	42	192.168.40.32/28
		PERMITIR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		PERMITIR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	456	172.16.0.0/26
		DENEGAR	250	192.168.250.0/28

Tabla 77. Restricciones VLAN 63

COMANDO	DESCRIPCIÓN
`(config)#ip access-list extended VLAN63`	Se crea ACL extendida llamada *VLAN63*.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.40.0 0.0.0.31`	Se deniega tráfico a VLAN 41.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.40.32 0.0.0.15`	Se deniega tráfico a VLAN 42.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 172.16.0.0 0.0.0.63`	Se deniega tráfico a VLAN 456.
`(config-ext-nacl)#deny ip 192.168.60.48 0.0.0.15 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 78. ACL VLAN 63

A continuación, se aplica sobre la interfaz correspondiente:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 63`	Se entra en la configuración de la VLAN 63.

`(config-if)#ip access-group VLAN63 in`	Se vincula la ACL nombrada *VLAN63* a la entrada de tráfico de la interfaz VLAN 63.

Tabla 79. ACL aplicada a VLAN 63

Una vez realizadas todas las ACLs extendidas para los departamentos de las distintas plantas, se procede a implementar las restricciones de la VLAN de los elementos IdC. Esta red no será accesible por ninguna VLAN interna a excepción de la VLAN del CPD, por lo que tampoco está permitido que la VLAN de los elementos IdC tenga comunicación con las VLANs internas a excepción de la VLAN del CPD.

VLAN - ORIGEN		**ACCIÓN**	**VLAN - DESTINO**	
456	172.16.0.0/26	DENEGAR	41	192.168.40.0/27
		DENEGAR	42	192.168.40.32/28
		DENEGAR	51	192.168.50.0/28
		DENEGAR	52	192.168.50.16/28
		DENEGAR	53	192.168.50.32/28
		PERMITIR	654	172.16.1.0/30
		DENEGAR	61	192.168.60.0/27
		DENEGAR	62	192.168.60.32/28
		DENEGAR	63	192.168.60.48/28
		DENEGAR	250	192.168.250.0/28

Tabla 80. Restricciones VLAN 456

COMANDO	**DESCRIPCIÓN**
`(config)#ip access-list extended VLAN456`	Se crea ACL extendida llamada *VLAN456*.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.40.0 0.0.0.31`	Se deniega tráfico a VLAN 41.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.40.32 0.0.0.15`	Se deniega tráfico a VLAN 42.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.50.0 0.0.0.15`	Se deniega tráfico a VLAN 51.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.50.16 0.0.0.15`	Se deniega tráfico a VLAN 52.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.50.32 0.0.0.15`	Se deniega tráfico a VLAN 53.

`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.60.0 0.0.0.31`	Se deniega tráfico a VLAN 61.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.60.32 0.0.0.15`	Se deniega tráfico a VLAN 62.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.60.48 0.0.0.15`	Se deniega tráfico a VLAN 63.
`(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.63 192.168.250.0 0.0.0.15`	Se deniega tráfico a VLAN 250.
`(config-ext-nacl)#permit ip any any`	Se permite el resto del tráfico.

Tabla 81. ACL VLAN 456

A continuación, se aplica sobre la interfaz de la VLAN 456:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 456`	Se entra en la configuración de la VLAN 456.
`(config-if)#ip access-group VLAN456 in`	Se vincula la ACL nombrada *VLAN456* a la entrada de tráfico de la interfaz VLAN 456.

Tabla 82. ACL aplicada a VLAN 456

Con estos pasos queda completamente definidas las restricciones de acceso de cada una de las VLANs de nuestra infraestructura de red.

ENRUTADOR CORPORATIVO

El enrutador corporativo debe ofrecer tanto salida a Internet a los equipos informáticos de la empresa como la conexión desde el exterior al servidor IdC para comprobar el estado de los elementos IdC.

VISUALIZACIÓN LÓGICA

El enrutador corporativo se encuentra en la parte derecha de la visualización lógica.

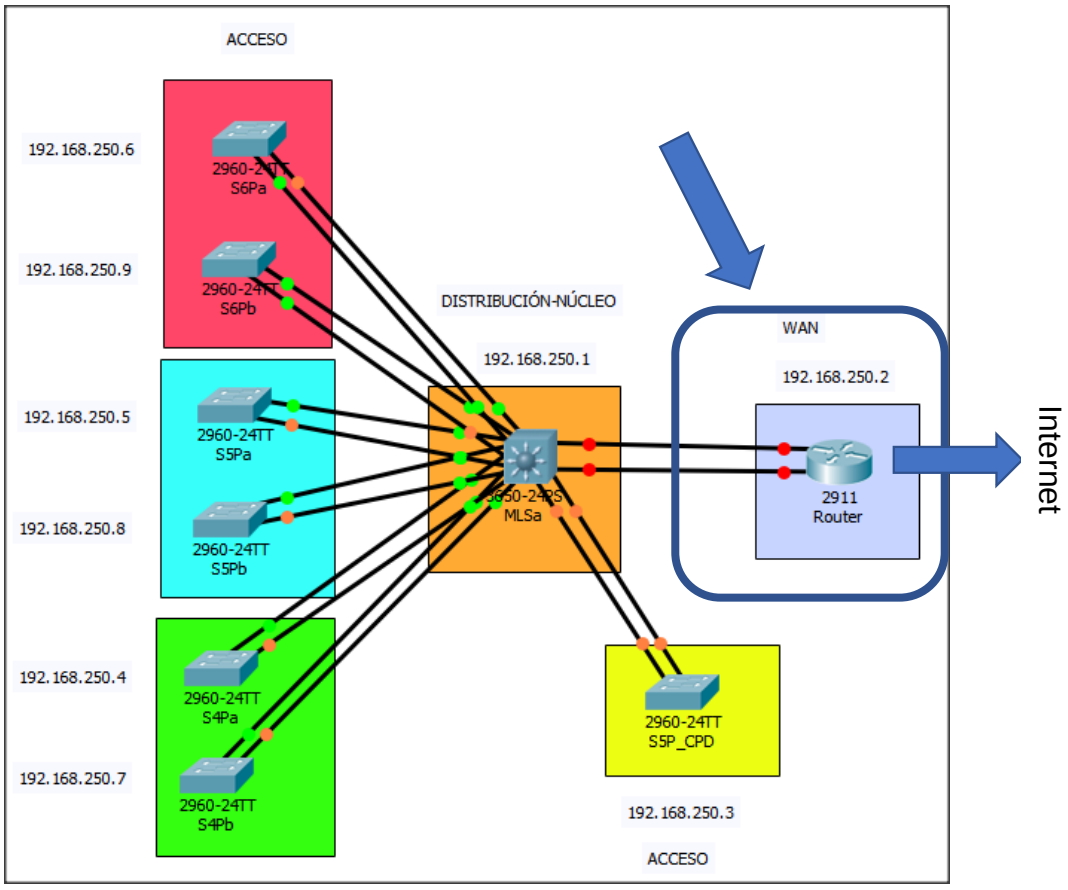


Figura 36. Enrutador corporativo en visualización lógica

El enrutador corporativo se conecta al conmutador de la capa de distribución-núcleo y a su vez se conecta con el proveedor de Internet para ofrecer Internet a los usuarios y acceso externo al servidor IdC.

VISUALIZACIÓN FÍSICA

El enrutador corporativo se instala en el armario rack de la 5ª planta junto al conmutador de la capa de distribución-núcleo.

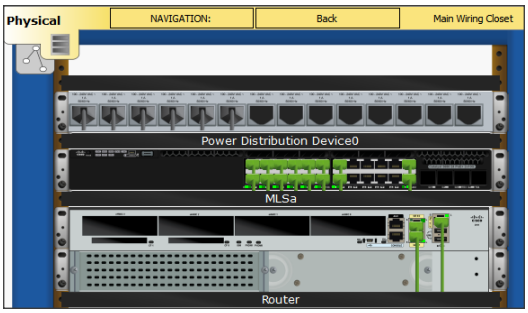


Figura 37. Enrutador corporativo en visualización física

Además de ofrecer Internet y acceso externo, son necesarios otros servicios y características activas las cuales se detallan a continuación:

ENDURECIMIENTO DEL DISPOSITIVO

Para el acceso al enrutador corporativo se realiza la misma configuración realizada que en el resto de los dispositivos de red, habilitando un usuario y contraseña de acceso y una contraseña para entrar en el modo privilegiado. Para ello, se utilizan los comandos vistos en la Tabla 38.

CONFIGURACIÓN DE TRADUCCIÓN DE DIRECCIONES DE RED (NAT)

El servicio de traducción de direcciones es necesario para tener acceso desde fuera al servidor IdC. Este servicio permite a los dispositivos externos conectarse con dispositivos internos mediante una dirección pública asignada.

Para poder realizar la conexión con el servidor IdC se utiliza el NAT estático, es decir, se asigna una dirección pública estática a la dirección interna del servidor IdC, permitiendo la conexión desde el exterior.

El primer paso a realizar para la configuración del NAT estático es crear la asignación de la dirección interna con la dirección pública estática asignada.

Para ello, se utiliza el siguiente comando:

```
(config)# ip nat inside source static 172.16.0.2 12.10.0.3
```

- 172.16.0.2: la dirección interna del servidor IdC
- 12.10.0.3: la dirección pública estática asignada.

De esta forma se configura el NAT estático en el enrutador.

El siguiente paso es indicar cuales son las interfaces implicadas en la traducción, indicando cuál es la interfaz interna y cuál es la interfaz externa.

INTERFAZ INTERNA	INTERFAZ EXTERNA
`(config)#interface GigabitEthernet0/2`	`(config)#interface GigabitEthernet0/0`
`(config-if)#ip nat inside`	`(config-if)#ip nat outside`

Tabla 83. Configuración de interfaz interna y externa

Con esta configuración quedaría configurado el NAT estático para poder acceder desde fuera al servidor IdC.

ENRUTAMIENTO BÁSICO Y RUTA POR DEFECTO

Para que el enrutador sea consciente de las distintas rutas posibles a cada uno de los departamentos requiere que sea configurado utilizando el mismo protocolo de enrutamiento que se utilizó en la capa de distribución-núcleo. El protocolo a configurar es **RIP** en su **versión 2**.

Para ello, basta introducir los siguientes comandos:

COMANDO	DESCRIPCIÓN
`(config)#router rip`	Se habilita el protocolo de enrutamiento.
`(config-router)#version 2`	Se utiliza la versión mejorada de RIP.
`(config-router)#network 192.168.0.0`	Se publican todas las rutas a las que puede accederse desde el conmutador.
`(config-router)#no auto-summary`	Se desactiva el resumen de rutas.

Tabla 84. Configuración de protocolo de enrutamiento RIP

Al activar *RIP* en el enrutador, pasado cierto tiempo, aprenderá las rutas que el conmutador de la capa de distribución-núcleo tiene para alcanzar los distintos departamentos de la empresa.

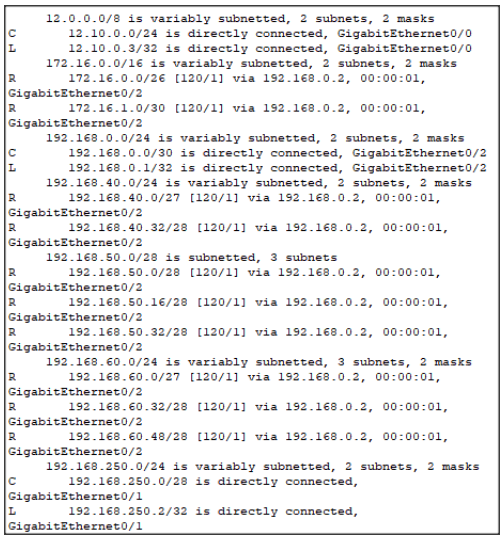


Figura 38. Rutas aprendidas por protocolo de enrutamiento RIP

Una vez se tienen las rutas aprendidas, se configura la ruta por defecto que se utilizará como salida hacia Internet.

```
(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
```

Se define la gigabitEthernet0/0 como interfaz de salida tal y como se definió en el NAT estático. Dicha interfaz de salida recibe su direccionamiento a través del proveedor de Internet, por lo que requiere la siguiente configuración:

COMANDO	DESCRIPCIÓN
`(config)#interface gigabitEthernet0/0`	Se accede a la interfaz de salida.
`(config-if)#ip address dhcp`	La dirección IP se negocia con el proveedor de Internet.

Tabla 85. Configuración de la interfaz de salida hacia el proveedor de Internet

Como ocurriera en el caso de la ruta por defecto en el conmutador de la capa de distribución-núcleo, la interfaz gigabitEthernet0/2 del enrutador necesita una dirección IP válida dentro del rango 192.168.0.0/30. Para ello, se realiza la siguiente configuración:

COMANDO	DESCRIPCIÓN
`(config)#interface gigabitEthernet0/2`	Se accede a la interfaz.
`(config-if)#ip address 192.168.0.1 255.255.255.252`	Se configura la dirección IP y su máscara /30.

Tabla 86. Configuración de la interfaz hacia la capa de distribución-núcleo

Una vez realizada la configuración de todos los servicios de las distintas capas del diseño de la red corporativo, así como la configuración del enrutador, el siguiente paso es configurar el direccionamiento IP de la VLAN de administración de cada uno de los dispositivos de red. Este paso no pudo realizarse antes, ya que faltaba por configurar el servidor VTP, las interfaces troncales y los enlaces EtherChannel para distribuir la VLAN de administración a cada conmutador.

CONFIGURACIÓN DEL DIRECCIONAMIENTO IP

A continuación, se configura en cada uno de los dispositivos de red la dirección IP de administración. La VLAN utilizada para la administración de los dispositivos de red es la **VLAN 250** y las direcciones IPs asignadas se toman de la siguiente tabla:

UBICACIÓN	NOMENCLATURA	DIRECCION IP
4ª	S4Pa	192.168.250.4
	S4Pb	192.168.250.7
5ª	S5Pa	192.168.250.5
	S5Pb	192.168.250.8
CPD	S5P_CPD	192.168.250.3
6ª	S6Pa	192.168.250.6
	S6Pb	192.168.250.9
5ª	MLSa	192.168.250.1
5ª	Router	192.168.250.2

Tabla 87. Direcciones IP de VLAN 250 de administración

Para ello, se utilizan los siguientes comandos:

COMANDO	DESCRIPCIÓN
`(config)#interface vlan 250`	Acceso a vlan 250
`(config-if)#ip address 192.168.250.4 255.255.255.240`	Configuración de IP para la VLAN 250.

Tabla 88. Asignación de dirección IP a VLAN 250

Una vez establecida la dirección IP de administración en cada uno de los dispositivos, se pasa a configurar el resto de direcciones IP necesarias. El conmutador de la capa de distribución-núcleo actúa como puerta de enlace para

cada una de las VLANs definidas, por lo que, hay que asignar una dirección IP válida a cada una de las interfaces VLAN creadas en el conmutador de la capa de distribución-núcleo.

En la siguiente tabla se muestran las direcciones IP asignadas a su respectiva VLAN o interfaz en el conmutador de la capa de distribución-núcleo y en el enrutador corporativo:

CONMUTADOR	INTERFAZ-VLAN	DIRECCION IP
MLSa	41	192.168.40.1
	42	192.168.40.33
	51	192.168.50.1
	52	192.168.50.17
	53	192.168.50.33
	61	192.168.60.1
	62	192.168.60.33
	63	192.168.60.49
	250	192.168.250.1
	456	172.16.0.1
	654	172.16.1.1
	GigabitEthernet1/0/24	192.168.0.2

Tabla 89. Direcciones IP definidas en cada interfaz/VLAN del conmutador MLSa

ENRUTADOR	INTERFAZ	DIRECCION IP
Router	GigabitEthernet0/0	Proveedor Internet
	GigabitEthernet0/1	192.168.250.2
	GigabitEthernet0/2	192.168.0.1

Tabla 90. Direcciones IP definida en cada interfaz del enrutador corporativo

3.1.4 EQUIPAMIENTO

Tras haber creado la estructura de red necesaria, se dispone a incluir el resto del equipamiento en el simulador tanto en la visualización lógica como en la visualización física.

Los elementos por incluir son tanto los equipos informáticos de los usuarios, los servidores corporativo e IdC, así como todos los elementos IdC desarrollados.

SERVIDOR CORPORATIVO

En este apartado se implementa el servidor corporativo de la empresa con los servicios que se indicaron en la fase de diseño.

VISUALIZACIÓN LÓGICA

El servidor corporativo se conecta al conmutador S5P_CPD de la capa de acceso.

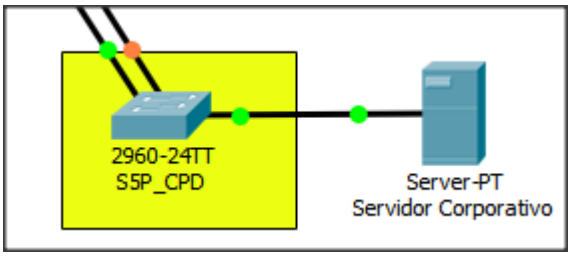


Figura 39. Servidor corporativo en visualización lógica

VISUALIZACIÓN FÍSICA

El servidor corporativo se ubica dentro del CPD en la 5ª planta.

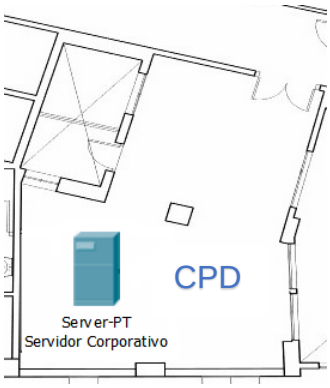


Figura 40. Servidor corporativo en visualización física

Una vez el servidor está ubicado físicamente, se procede a configurar los distintos servicios. Estos son los servicios por activar:

- **HTTP**. Activo por defecto.
- **TFTP**. Activo por defecto.
- **FTP**. Activo por defecto.
- **DNS**. Desactivado por defecto.
- **SYSLOG**. Activo por defecto.
- **NTP**. Activo por defecto.
- **EMAIL**. Desactivado por defecto.

Para configurar todos los servicios que va a tener activos el servidor corporativo hay que hacer clic sobre el dibujo del servidor corporativo y pulsar sobre la pestaña *Services*. En esta pestaña, aparecen todos los servicios que podría tener activos. Muchos de ellos están activos por defecto, como es el caso del servicio HTTP. Se configura aquellos que están desactivados por defecto, como es el caso del servicio *Domain Name System (DNS)* y el servicio de correo electrónico (*EMAIL*).

DOMAIN NAME SYSTEM (DNS)

Se activa el servicio pulsando sobre *On* y se definen los nombres a resolver.

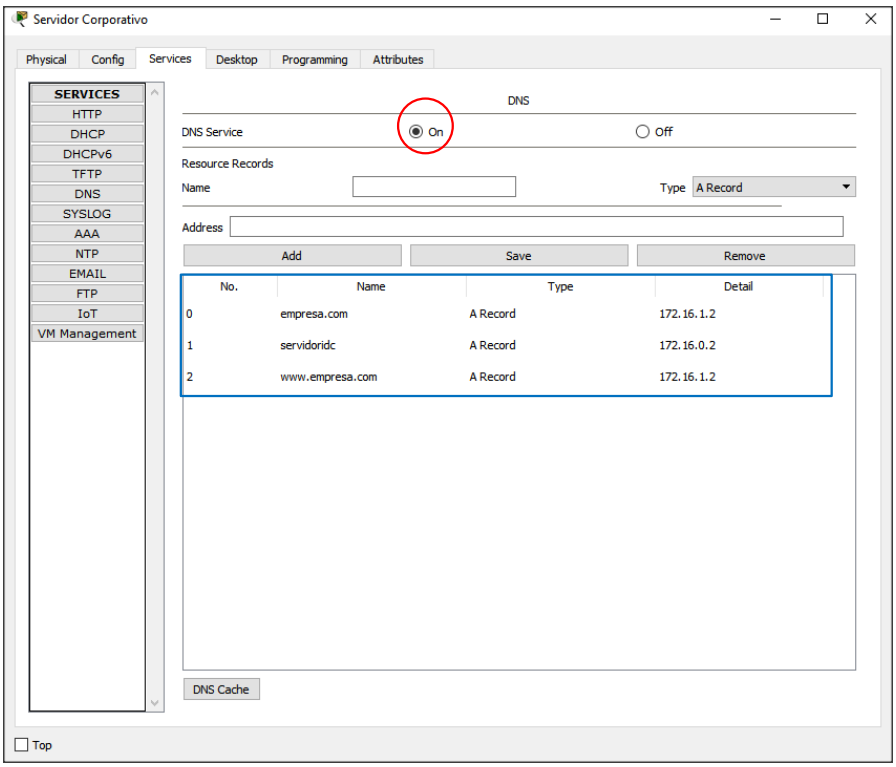


Figura 41. Activación del servicio DNS

Las direcciones URL empresa.com y www.empresa.com corresponden con la página web interna de la empresa, las cuales están alojadas en el servidor corporativo.

La dirección *servidoridc* corresponde con la dirección IP del servidor IdC, cualquiera que necesite resolver la dirección del servidor IdC podrá hacerlo, con independencia de si tiene acceso o no a dicha dirección IP, ya que se establecieron una serie de restricciones.

CORREO ELECTRÓNICO (EMAIL)

Se activa el servicio pulsando sobre *On* y se establece el nombre de dominio del servidor de correo (*empresa.com*).

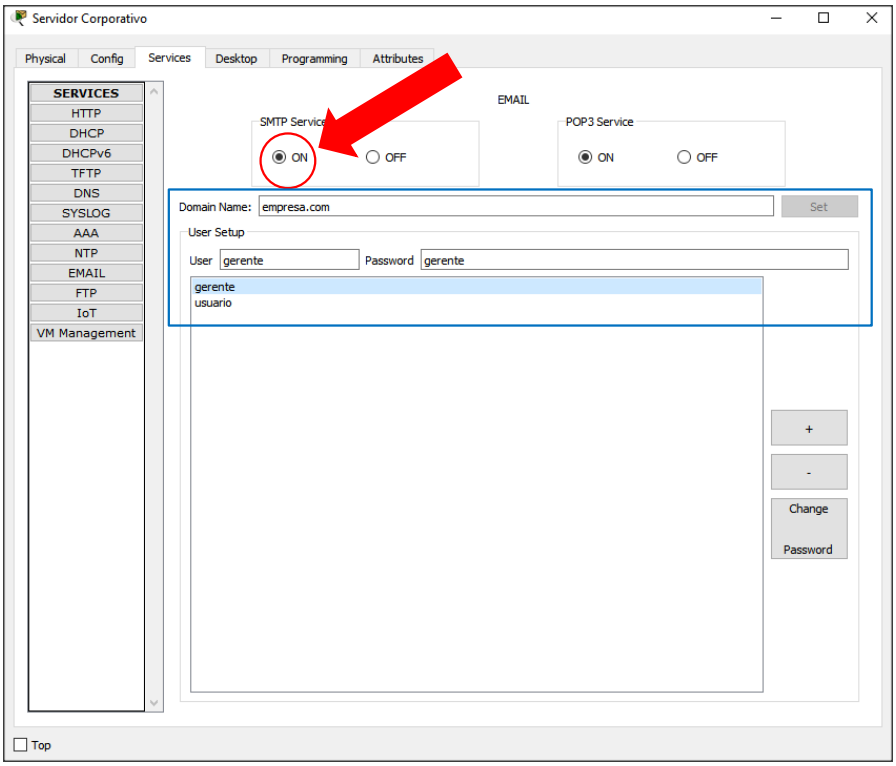


Figura 42. Activación del servicio Email

A continuación, se dan de alta dos cuentas de correo electrónico, gerente@empresa.com y usuario@empresa.com para verificar el correcto funcionamiento del servidor de correo corporativo.

EQUIPOS INFORMÁTICOS

En este apartado se conectan los equipos informáticos que forman parte de la empresa en las distintas plantas.

VISUALIZACIÓN LÓGICA

Los equipos informáticos son conectados a los conmutadores de la capa de acceso y renombrados para ser identificables.

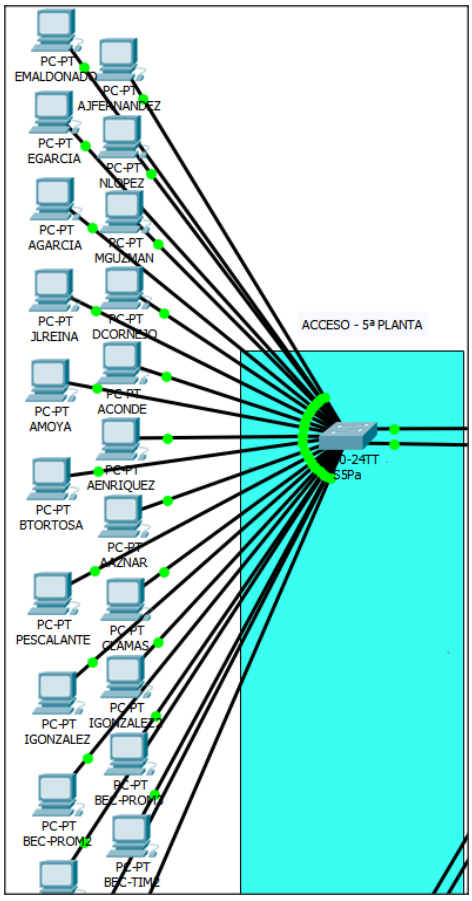


Figura 43. Equipos informáticos en visualización lógica

VISUALIZACIÓN FÍSICA

Los equipos informáticos son ubicados según su departamento y colocados sobre su puesto de trabajo para ser fácilmente localizables.

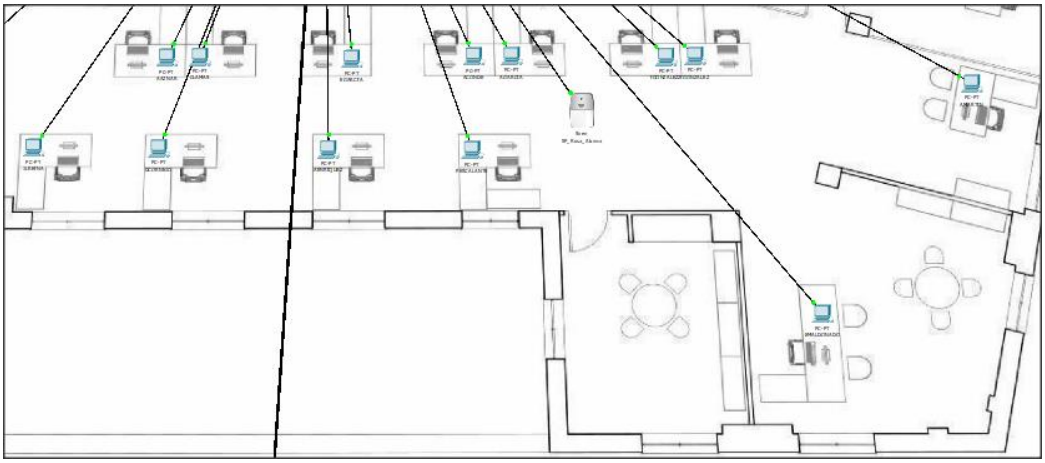


Figura 44. Equipos informáticos en visualización física

Todos los equipos informáticos obtienen su dirección IP mediante la utilización del servidor DHCP configurado.

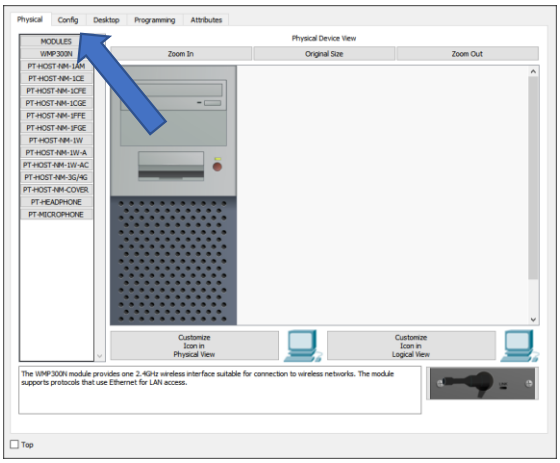


Figura 45. Propiedades del equipo informático

Para configurar el DHCP en los equipos informáticos hay que pulsar sobre la pestaña *Config*.

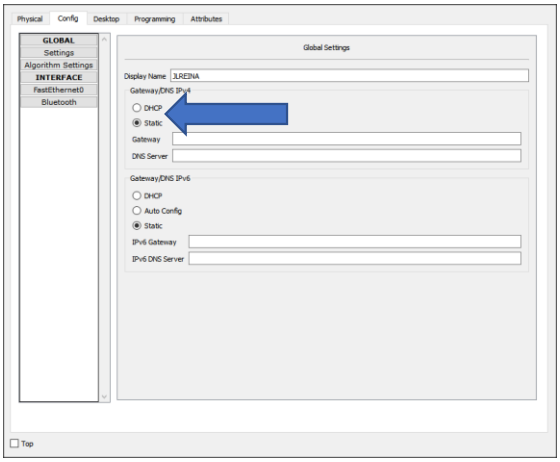


Figura 46. Configuración de DHCP en la pestaña Config

Se marca la opción *DHCP*, para que el equipo informático negocie y obtenga una dirección IP válida según su ubicación.

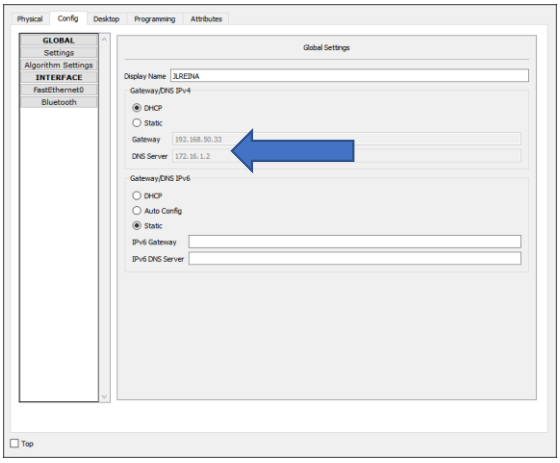


Figura 47. Activación del servicio DHCP en el equipo informático

Al activar el servicio DHCP se obtiene la dirección IP correspondiente como se puede observar en la Figura 47. El equipo informático ha recibido tanto la puerta de enlace como el servidor DNS.

De esta forma se realizaría la implantación de todos los equipos informáticos necesarios en cada una de las plantas del edificio.

ELEMENTOS IDC

En este apartado se va a realizar la implementación de cada uno de los elementos IdC definidos en la fase de diseño. Se trata el elemento IdC tanto en su visualización lógica como en su visualización física y se desarrollan las reglas que modelan su comportamiento, así como su programación si fuese necesaria [11].

Antes de integrar cada uno de los elementos IdC en el simulador es preciso conocer cómo se conectan al servidor IdC. Para ello, todos los elementos IdC al hacer clic sobre él presentan una serie de pestañas que permiten, entre otras cosas, conectar el dispositivo IdC al servidor IdC (pestaña de configuración (*Config*)).

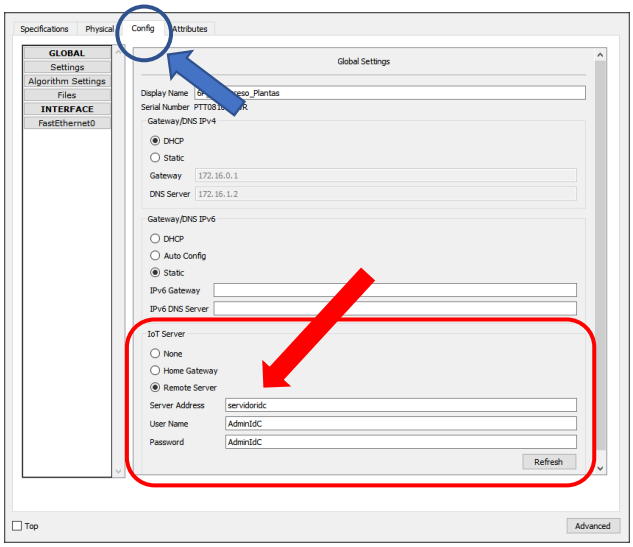


Figura 48. Registro del elemento IdC en el servidor IdC

En la parte inferior de la pestaña *Config* se encuentra una sección llamada IoT Server. Se selecciona *Remote Server* y se rellenan los campos (Figura 48).

- **La dirección del servidor IdC**. El servidor DNS configurado en el servidor corporativo se encarga de resolver el nombre de *servidoridc* a la IP del servidor IdC.
- **Nombre de usuario**. Se utiliza el mismo usuario que se dio de alta en el servicio IdC del servidor.
- **Contraseña**. Se utiliza la misma contraseña que se estableció al dar de alta el servicio IdC en el servidor.

Una vez completados los campos se pulsa sobre el botón **conectar** (*Connect*). Si la conexión se realiza satisfactoriamente, el elemento IdC se habrá registrado correctamente en el servidor IdC.

LUCES AUTOMÁTICAS

El elemento de luces automática se implementa en las tres plantas del edificio (4ª, 5ª y 6ª planta) en el pasillo principal de las mismas. Se instalan dos sensores de movimientos en los extremos del pasillo para ampliar la zona de detección y se distribuyen los leds para que abarquen la mayor superficie posible.

VISUALIZACIÓN LÓGICA

El elemento IdC es conectado con el conmutador de cada una de las plantas (4ª, 5ª y 6ª planta).

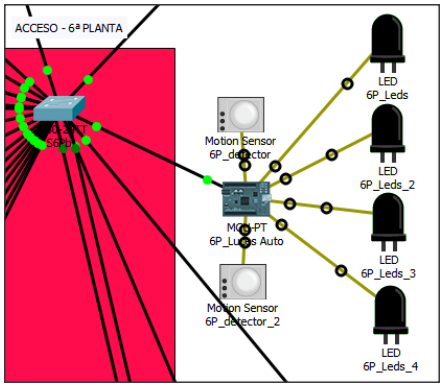


Figura 49. Luces automáticas en visualización lógica

VISUALIZACIÓN FÍSICA

El elemento se conecta a la interfaz *fastEthernet0/6* del conmutador de planta correspondiente (S4Pb, S5Pb y S6Pb) y se distribuye para iluminar la mayor parte del pasillo.

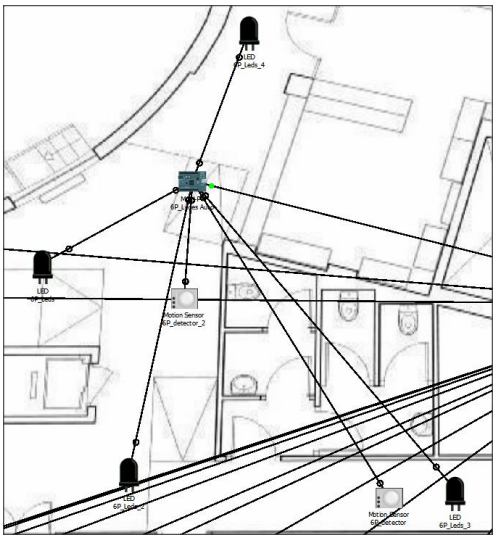


Figura 50. Luces automáticas en visualización física

La microcontroladora está limitada a seis dispositivos, por lo que se conectan cuatro leds y dos sensores de movimiento por elemento IdC en cada planta.

PROGRAMACIÓN

Este elemento contiene una microcontroladora la cual necesita ser programada para que una vez detectado movimiento en la zona encienda los leds y notifique el encendido de las luces. La Figura 51 muestra el código que implementa la lógica deseada para este elemento utilizando el lenguaje visual Blockly [10].

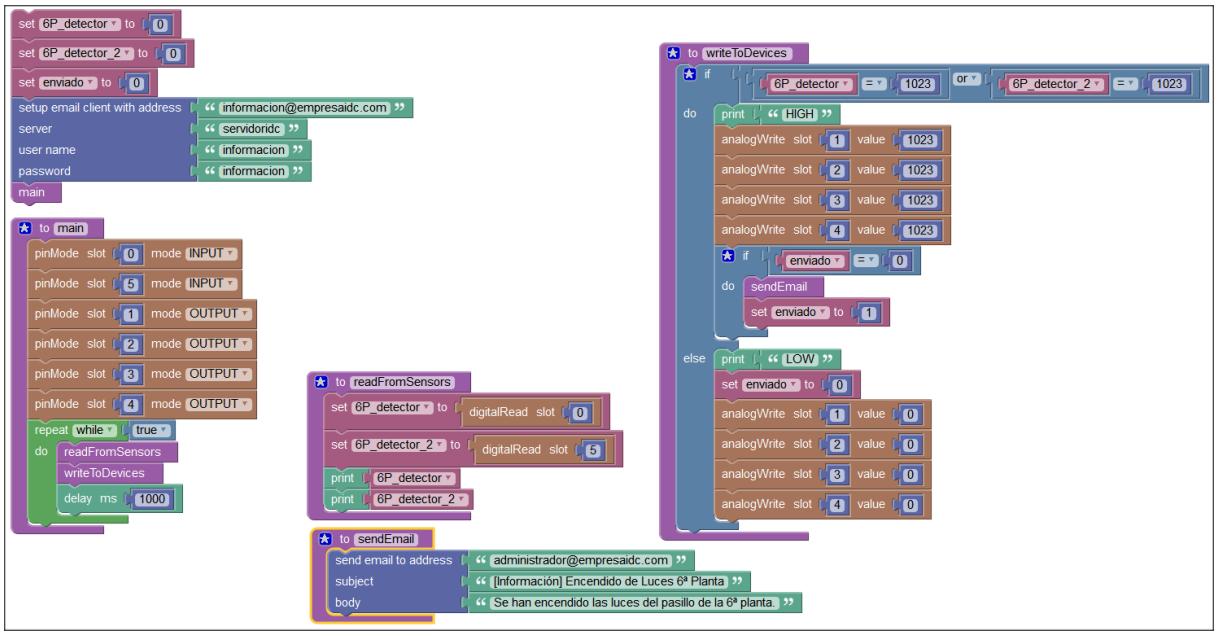


Figura 51. Programación Blockly del elemento IdC (luces automáticas)

ACCESO A SALA DE COMUNICACIONES

El acceso a las distintas salas de comunicaciones se realiza mediante la utilización de este elemento IdC. Al accionar el pulsador, la microcontroladora envía una señal a la puerta inteligente y a su vez envía una notificación de intento de acceso.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de cada planta (4ª, 5ª y 6ª planta).

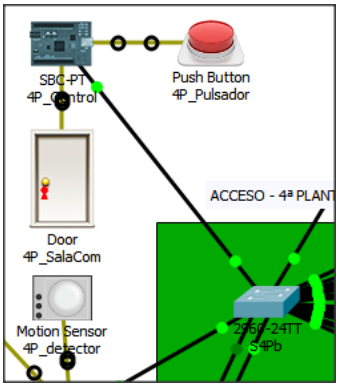


Figura 52. Acceso a sala de comunicaciones en visualización lógica

VISUALIZACIÓN FÍSICA

El elemento IdC se ubica próxima a la puerta a controlar de cada planta. La microcontroladora se conecta al conmutador de planta (S4Pb, S5Pb y S6Pb) en la interfaz *fastEthernet0/7*.

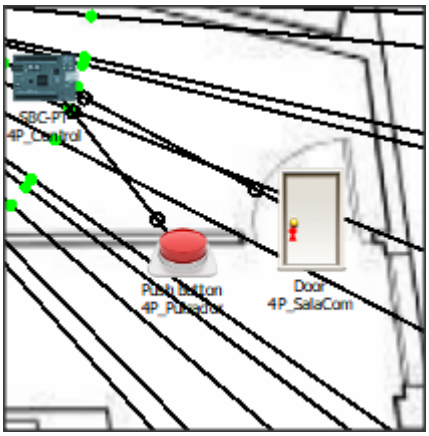


Figura 53. Acceso a sala de comunicaciones en visualización física

PROGRAMACIÓN

Al utilizar una microcontroladora, es necesario programar el comportamiento del elemento IdC para que cuando se accione el pulsador, se desbloquee la puerta inteligente y se envíe una notificación prioritaria del intento de acceso a la sala de comunicaciones. Pasado un tiempo la puerta vuelve a bloquearse. El código para este elemento se muestra en la Figura 54.

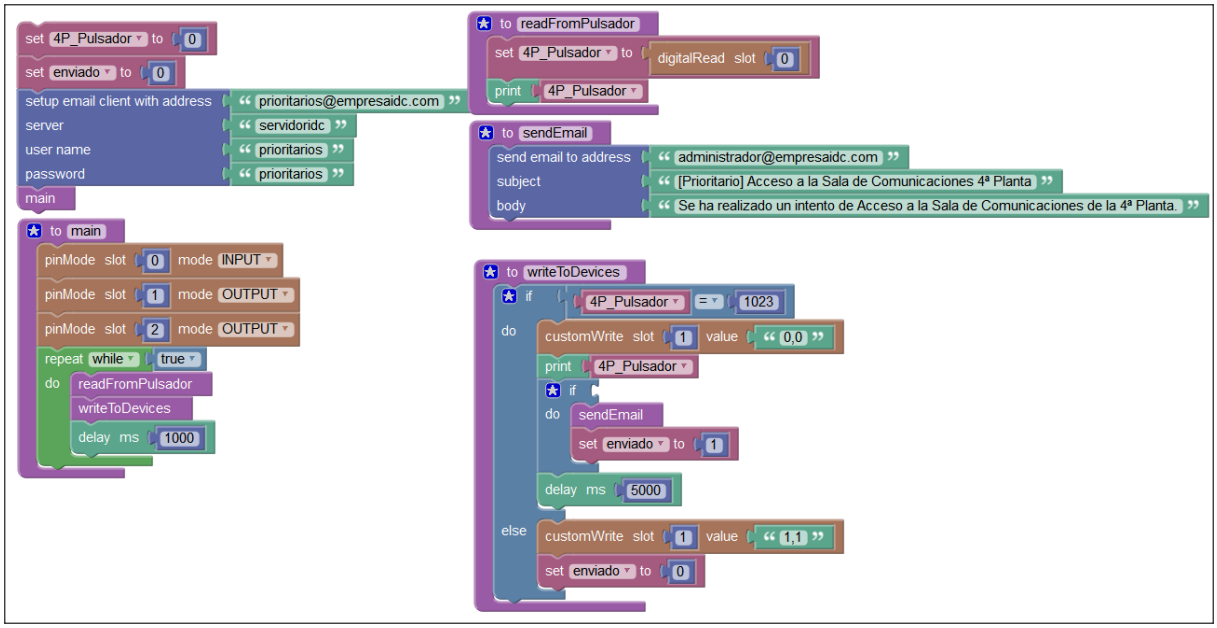


Figura 54. Programación Blockly del elemento IdC (acceso a sala de comunicaciones)

BLOQUEO DE VENTANAS POR VIENTO

El bloqueo de las ventanas por viento se hace por precaución, evitando que la ventana se abra o se cierre de forma abrupta. Mediante la utilización de un anemómetro, se controla la apertura de la ventana inteligente o su bloqueo.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de la 4ª planta y al conmutador de la 5ª planta.

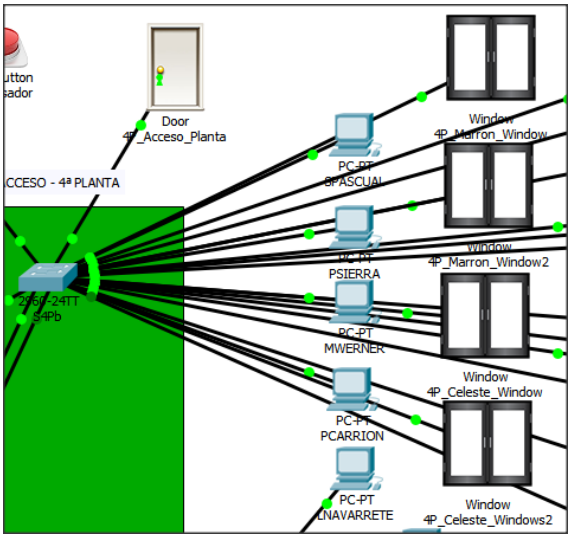


Figura 55. Bloqueo de ventanas por viento en visualización lógica

VISUALIZACIÓN FÍSICA

En este caso, las ventanas inteligentes son conectadas al conmutador de la 4ª planta S4Pb en las interfaces *fastEthernet0/15* hasta la *fastEthernet0/18*. El anemómetro es conectado a la interfaz *fastEthernet0/4* del conmutador de la 5ª planta S5Pb.

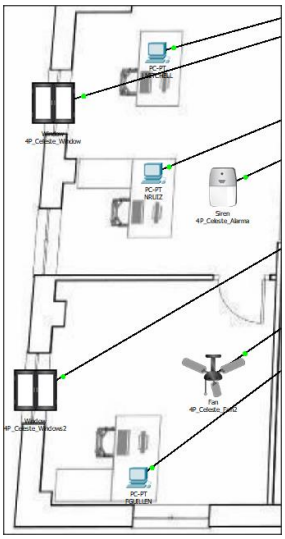


Figura 56. Bloqueo de ventanas por viento en visualización física

PROGRAMACIÓN

Si se detectan fuertes rachas de viento entonces se cierran o bloquean las ventanas inteligentes como medida de precaución. Esta programación se realiza en el servidor IdC en la pestaña de *Conditions*.

Edit Remove	Yes	4P_Ventanas	5P_Wind_Detector Wind is true	Set 4P_Celeste_Window On to false Set 4P_Celeste_Windows2 On to false Set 4P_Marron_Window On to false Set 4P_Marron_Window2 On to false

Figura 57. Programación de reglas del elemento IdC (bloqueo de ventanas por viento)

VENTILACIÓN AUTOMÁTICA

La ventilación automática actúa cuando detecta una de las ventanas inteligentes abierta, favoreciendo la renovación del aire de la habitación.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de la 4ª planta.

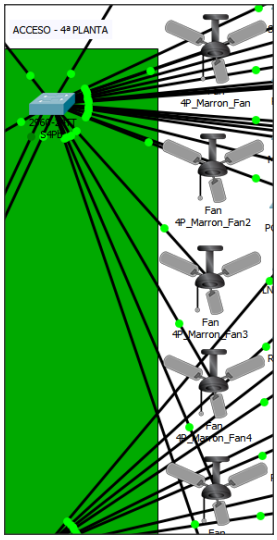


Figura 58. Ventilación automática en visualización lógica

VISUALIZACIÓN FÍSICA

Se conecta cada uno de los ventiladores de interior al conmutador de 4ª planta S4Pb en las interfaces *fastEthernet0/19* hasta la *fastEthernet0/24*.

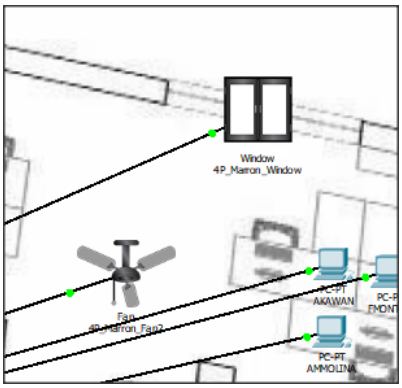


Figura 59. Ventilación automática en visualización física

PROGRAMACIÓN

Si se detecta una ventana inteligente abierta se activan los ventiladores de interior próximos a la zona a una velocidad baja. Esta programación se realiza en el servidor IdC en la pestaña *Conditions*.

Edit Remove	Yes	4P_Windows_Marron	Match any: • 4P_Marron_Window On is true • 4P_Marron_Window2 On is true	Set 4P_Marron_Fan Status to Low Set 4P_Marron_Fan2 Status to Low Set 4P_Marron_Fan3 Status to Low Set 4P_Marron_Fan4 Status to Low
Edit Remove	Yes	4P_Windows_Marron_End	Match all: • 4P_Marron_Window On is false • 4P_Marron_Window2 On is false	Set 4P_Marron_Fan Status to Off Set 4P_Marron_Fan2 Status to Off Set 4P_Marron_Fan3 Status to Off Set 4P_Marron_Fan4 Status to Off
Edit Remove	Yes	4P_Windows_Celeste	Match any: • 4P_Celeste_Window On is true • 4P_Celeste_Windows2 On is true	Set 4P_Celeste_Fan Status to Low Set 4P_Celeste_Fan2 Status to Low
Edit Remove	Yes	4P_Windows_Celeste_End	Match all: • 4P_Celeste_Window On is false • 4P_Celeste_Windows2 On is false	Set 4P_Celeste_Fan Status to Off Set 4P_Celeste_Fan2 Status to Off

Figura 60. Programación de reglas del elemento IdC (ventilación automática)

Se crean dos reglas por cada departamento, una para activar los ventiladores de interior y otra para desactivarlos.

DETECTOR DE HUMO

El detector de humo monitoriza el nivel de concentración de humo, activando una alarma en caso de que su concentración sea superior al 50%.

VISUALIZACIÓN LÓGICA

El elemento IdC es conectado a cada uno de los conmutadores de planta (4ª, 5ª y 6ª planta).

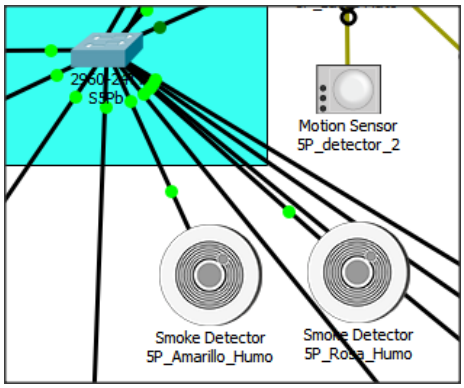


Figura 61. Detector de humo en visualización lógica

VISUALIZACIÓN FÍSICA

Los distintos dispositivos de este elemento IdC se conecta a las siguientes interfaces:

CONMUTADOR	INTERFAZ	DISPOSITIVO
S4Pb	fastEthernet0/9	Detector de humo
	fastEthernet0/10	Detector de humo
	fastEthernet0/11	Detector de humo
	fastEthernet0/12	Alarma
	fastEthernet0/13	Alarma
	fastEthernet0/14	Alarma
S5Pb	fastEthernet0/17	Alarma
	fastEthernet0/18	Detector de humo
	fastEthernet0/19	Detector de humo
	fastEthernet0/20	Alarma
	fastEthernet0/21	Detector de humo
	fastEthernet0/22	Alarma
S6Pb	fastEthernet0/8	Alarma
	fastEthernet0/9	Alarma
	fastEthernet0/11	Alarma
	fastEthernet0/20	Detector de humo
	fastEthernet0/21	Detector de humo
	fastEthernet0/22	Detector de humo

Tabla 91. Conexiones del elemento IdC

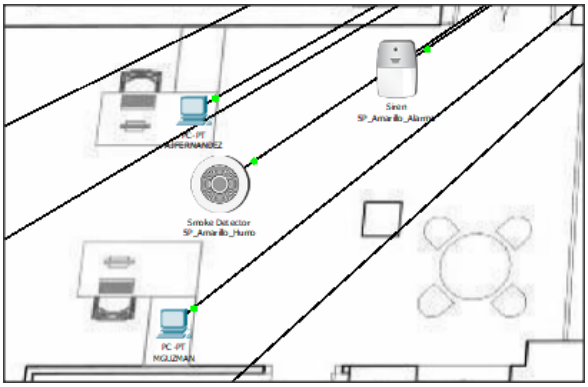


Figura 62. Detector de humo en visualización física

La instalación de este elemento IdC asocia un detector de humo con una alarma, siendo normalmente montada por pares (detector de humos, alarma).

PROGRAMACIÓN

Se define la regla en el servidor IdC de tal forma que si se detecta una concentración superior o igual al 50% entonces se activan las alarmas de emergencia de toda la planta, independientemente del sensor de humo que lo detectara. Cuando la concentración baje a un nivel inferior o igual al 20% entonces en todos los sensores de humo, se desactivan las alarmas.

Edit Remove	Yes	4P_Smoke_Detected	Match any: • 4P_Marron_Humo Level >= 5 • 4P_Marron_Humo2 Level >= 5 • 4P_Celeste_Humo Level >= 5	Set 4P_Marron_Alarma On to true Set 4P_Marron_Alarma2 On to true Set 4P_Celeste_Alarma On to true
Edit Remove	Yes	4P_Smoke_Out	Match all: • 4P_Marron_Humo Level <= 2 • 4P_Marron_Humo2 Level <= 2 • 4P_Celeste_Humo Level <= 2	Set 4P_Marron_Alarma On to false Set 4P_Marron_Alarma2 On to false Set 4P_Celeste_Alarma On to false

Figura 63. Programación del elemento IdC (detector de humo) en 4ª planta

Edit Remove	Yes	5P_Smoke_Detected	Match any: • 5P_Verde_Humo Level >= 5 • 5P_Rosa_Humo Level >= 5 • 5P_Amarillo_Humo Level >= 5	Set 5P_Verde_Alarma On to true Set 5P_Rosa_Alarma On to true Set 5P_Amarillo_Alarma On to true
Edit Remove	Yes	5P_Smoke_Out	Match all: • 5P_Verde_Humo Level <= 2 • 5P_Rosa_Humo Level <= 2 • 5P_Amarillo_Humo Level <= 2	Set 5P_Verde_Alarma On to false Set 5P_Rosa_Alarma On to false Set 5P_Amarillo_Alarma On to false

Figura 64. Programación del elemento IdC (detector de humo) en 5ª planta

Edit Remove	Yes	6P_Smoke_Detected	Match any: • 6P_Morado_Humo Level >= 5 • 6P_Rojo_Humo Level >= 5 • 6P_VerdeMenta_Humo Level >= 5	Set 6P_Morado_Alarma On to true Set 6P_Rojo_Alarma On to true Set 6P_VerdeMenta_Alarma On to true
Edit Remove	Yes	6P_Smoke_Out	Match all: • 6P_Morado_Humo Level <= 2 • 6P_Rojo_Humo Level <= 2 • 6P_VerdeMenta_Humo Level <= 2	Set 6P_Morado_Alarma On to false Set 6P_Rojo_Alarma On to false Set 6P_VerdeMenta_Alarma On to false

Figura 65. Programación de reglas del elemento IdC (detector de humo) en 6ª planta

Se configuran dos reglas por cada planta, una de activación y otra de desactivación de la alarma.

La activación se produce al 50% del valor máximo del detector de humo. El detector de humo trabaja con valores comprendidos entre 0 y 10, por lo que el 50% se expresa como 5 y el 20% como 2.

La desactivación se produce cuando la concentración es inferior o igual al 20% en todos los detectores de humos.

PUERTA DE ACCESO A PLANTA

Para asegurar una mayor protección de las instalaciones de la empresa se le dota de este elemento IdC. Este elemento bloquea las puertas de acceso de las distintas plantas mediante la utilización de una tarjeta de radiofrecuencia.

VISUALIZACIÓN LÓGICA

El elemento IdC se conecta en cada conmutador de planta (4ª, 5ª y 6ª planta).

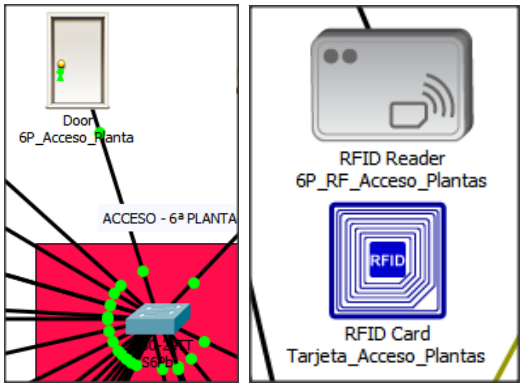


Figura 66. Puerta inteligente (a la izquierda) y lector RF con tarjeta válida (a la derecha)

VISUALIZACIÓN FÍSICA

La puerta inteligente de este elemento IdC se conecta a la interfaz *fastEthernet0/5* de los conmutadores S4Pb, S5Pb y S6Pb. El lector de radiofrecuencia se conecta al conmutador de la 6ª planta S6Pb en la interfaz *fastEthernet0/12*.

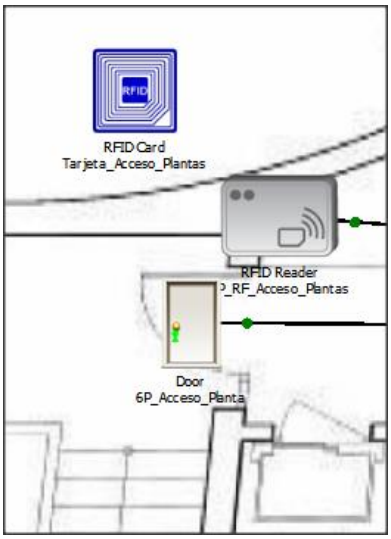


Figura 67. Lector RF junto a tarjeta y puerta inteligente de 6ª planta

PROGRAMACIÓN

Las reglas a definir en el servidor IdC serán tres reglas:

1- Si el lector RF lee la tarjeta válida, con un cierto código, por ejemplo, 5002, y las puertas inteligentes están bloqueadas entonces se desbloquean.
2- Si el lector RF lee la tarjeta válida y las puertas inteligentes están desbloqueadas entonces se bloquean.
3- Si alguna de las puertas inteligentes se abre el lector de tarjetas se vuelve a reactivar.

Edit Remove	Yes	6P_Acceso_Planta_Open	Match all: • 6P_RF_Acceso_Plantas Card ID = 5002 • 6P_Acceso_Planta Lock is Lock • 5P_Acceso_Planta Lock is Lock • 4P_Acceso_Planta Lock is Lock	Set 6P_Acceso_Planta Lock to Unlock Set 5P_Acceso_Planta Lock to Unlock Set 4P_Acceso_Planta Lock to Unlock Set 6P_RF_Acceso_Plantas Status to Valid
Edit Remove	Yes	6P_Acceso_Planta_Blocked	Match all: • 6P_RF_Acceso_Plantas Card ID = 5002 • 6P_Acceso_Planta Lock is not Lock • 5P_Acceso_Planta Lock is not Lock • 4P_Acceso_Planta Lock is not Lock	Set 6P_Acceso_Planta Lock to Lock Set 5P_Acceso_Planta Lock to Lock Set 4P_Acceso_Planta Lock to Lock Set 6P_RF_Acceso_Plantas Status to Valid
Edit Remove	Yes	6P_Acceso_Planta_Waiting	Match any: • 6P_Acceso_Planta Open is true • 5P_Acceso_Planta Open is true • 4P_Acceso_Planta Open is true	Set 6P_RF_Acceso_Plantas Status to Waiting

Figura 68. Programación de reglas del elemento IdC (puerta de acceso a planta)

ACCESO AL CPD

El control del acceso al CPD se realiza mediante la utilización de tarjetas de radiofrecuencia. Si el acceso es válido entonces se desbloqueado la puerta inteligente grabando mediante una cámara, siempre y cuando, se detecte movimiento en el interior del CPD.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de 5ª planta del CPD.

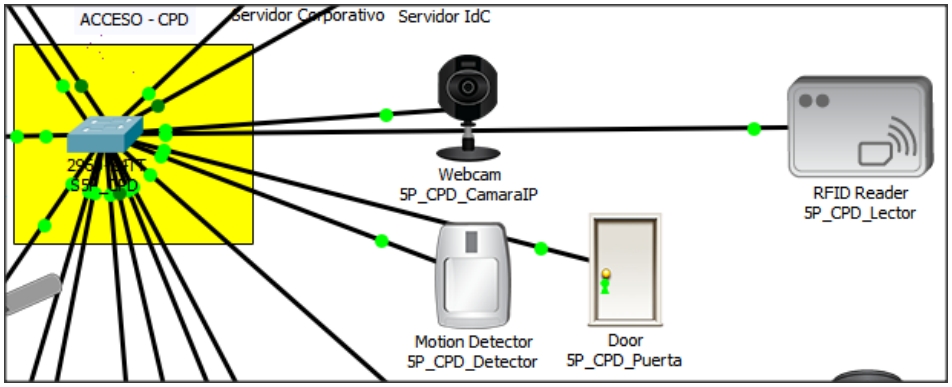


Figura 69. Acceso al CPD en visualización lógica

VISUALIZACIÓN FÍSICA

Los distintos dispositivos que forman este elemento IdC se conectan al conmutador S5P_CPD en las siguientes interfaces:

CONMUTADOR	INTERFAZ	DISPOSITIVO
S5P_CPD	fastEthernet0/4	Cámara IP
	fastEthernet0/5	Detector de movimiento
	fastEthernet0/7	Puerta inteligente
	fastEthernet0/8	Lector RF

Tabla 92. Conexiones del elemento IdC

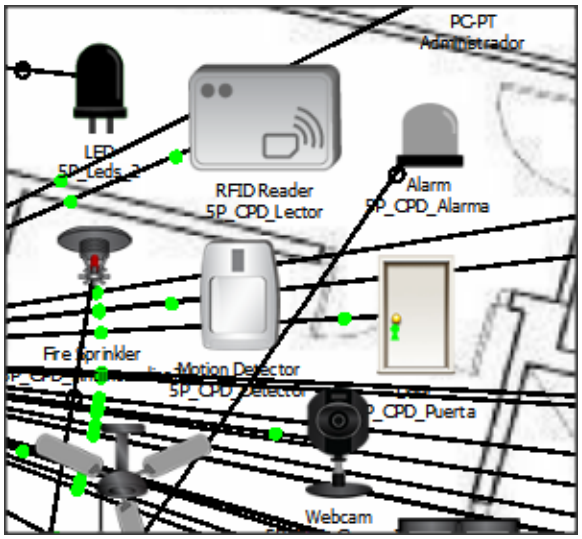


Figura 70. Acceso al CPD en visualización física

PROGRAMACIÓN

Si el lector RF lee la tarjeta válida, por ejemplo, con código 5000, entonces se desbloquea la puerta inteligente del CPD. Si, por el contrario, la tarjeta leída no es válida, la puerta inteligente permanece bloqueada.

Si la puerta se abre entonces se bloquea cuando se cierra y se reactiva el lector RF. El modelo de este comportamiento corresponde al servidor IdC realizarlo.

Edit Remove	Yes	5P_CPD_Lector_OK	Match all: • 5P_CPD_Lector Card ID = 5000 • 5P_CPD_Puerta Lock is Lock • 5P_CPD_Lector Status is not Valid	Set 5P_CPD_Puerta Lock to Unlock Set 5P_CPD_Lector Status to Valid
Edit Remove	Yes	5P_CPD_Puerta_Off	5P_CPD_Puerta Open is true	Set 5P_CPD_Puerta Lock to Lock Set 5P_CPD_Lector Status to Waiting
Edit Remove	Yes	5P_CPD_Lector_FAIL	Match all: • 5P_CPD_Puerta Lock is Lock • 5P_CPD_Lector Card ID != 5000 • 5P_CPD_Lector Status is not Valid	Set 5P_CPD_Puerta Lock to Lock Set 5P_CPD_Lector Status to Invalid

Figura 71. Programación de reglas del elemento IdC (acceso al CPD – lector RF)

Si se detecta movimiento en el interior entonces la cámara comienza a grabar, dejando de grabar cuando no se detecte movimiento (Figura 72).

Edit Remove	Yes	5P_Mov_CPD	5P_CPD_Detector On is true	Set 5P_CPD_CamaraIP On to true
Edit Remove	Yes	5P_Mov_CPD_End	5P_CPD_Detector On is false	Set 5P_CPD_CamaraIP On to false

Figura 72. Programación de reglas del elemento IdC (acceso al CPD - movimiento)

BLOQUEO DE VENTANA DEL CPD POR VIENTO

El bloqueo de la ventana del CPD se realiza cunado se detectan fuertes rachas de viento en el anemómetro instalado en el patio interior.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta con el conmutador de la 5ª planta del CPD.

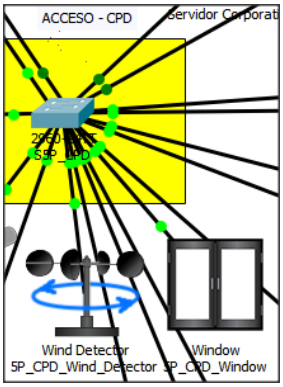


Figura 73. Bloqueo de ventana del CPD en visualización lógica

VISUALIZACIÓN FÍSICA

La conexión de la ventana inteligente se realiza en la interfaz *fastEthernet0/9* del conmutador S5P_CPD y la conexión del anemómetro se realiza en la interfaz *fastEthernet0/6* del mismo conmutador.

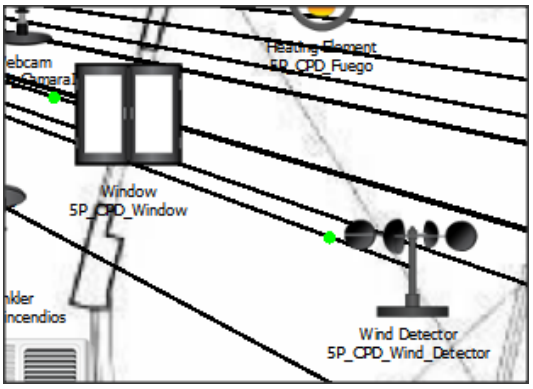


Figura 74. Bloqueo de ventana del CPD en visualización física

PROGRAMACIÓN

Este caso también se define en el servidor IdC y se activa cuando se detectan fuertes rachas de viento, momento en el que cierra o bloquea la ventana inteligente (Figura 75).

Edit Remove	Yes	5P_CPD_Wind	5P_CPD_Wind_Detector Wind is true	Set 5P_CPD_Window On to false

Figura 75. Programación de reglas del elemento IdC (bloqueo de ventana del CPD por viento)

VENTILACIÓN AUTOMÁTICA DEL CPD

La ventilación automática del CPD sucede cuando la ventana inteligente se abre. Indicar que este hecho debe de suceder en muy pocas ocasiones, ya que si sucediera indicaría que el aire acondicionado del CPD está averiado o tiene algún tipo de problema.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta con el conmutador de la 5ª planta del CPD.

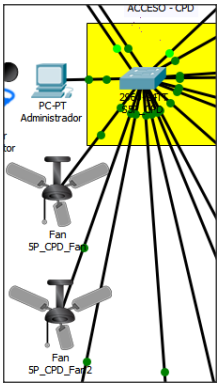


Figura 76. Ventilación automática del CPD en visualización lógica

VISUALIZACIÓN FÍSICA

Este elemento IdC se conecta a las interfaces *fastEthernet0/14* y *fastEthernet0/15* del conmutador S5P_CPD.

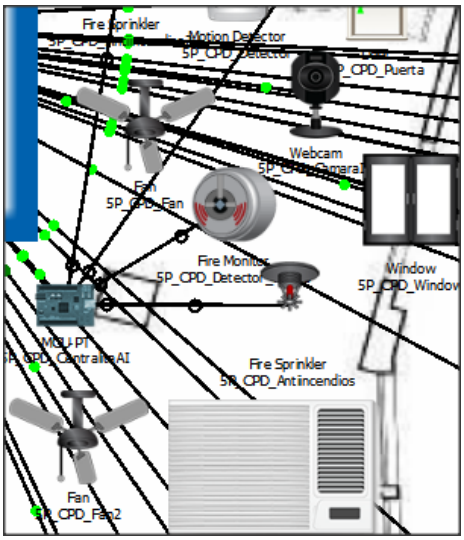


Figura 77. Ventilación automática en visualización física

PROGRAMACIÓN

Si la ventana inteligente del CPD está abierta entonces se activan los ventiladores de interior a máxima potencia. Si la ventana está cerrada los ventiladores de interior permanecen desactivados. Estas dos reglas se definen en el servidor IdC (Figura 78).

Edit Remove	Yes	5P_CPD_Fan_On	5P_CPD_Window On is true	Set 5P_CPD_Fan Status to High Set 5P_CPD_Fan2 Status to High
Edit Remove	Yes	5P_CPD_Fan_Off	5P_CPD_Window On is false	Set 5P_CPD_Fan Status to Off Set 5P_CPD_Fan2 Status to Off

Figura 78. Programación de reglas del elemento IdC (ventilación automática del CPD)

El hecho de que entren en funcionamiento a máxima potencia es para favorecer la eliminación del calor acumulado.

AIRE ACONDICIONADO CENTRALIZADO DEL CPD

El aire acondicionado del CPD es uno de los elementos más importantes del CPD dado que debe de estar operativo las 24 horas del día. Por lo tanto, es necesario optimizar el uso de los mismos. Si la temperatura es superior o igual a 15ºC, se activan los aires acondicionados y si la temperatura es inferior o igual a 5ºC, se desactivan.

Hay que indicar que dicho rango se establece así para apreciar el funcionamiento del sistema, en ningún caso serían las temperaturas ideales de funcionamiento para un CPD.

Este elemento permite ser activado de forma manual desde el termostato ubicado en cada uno de los ACs en caso de que fuera necesario.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de 5ª planta del CPD.

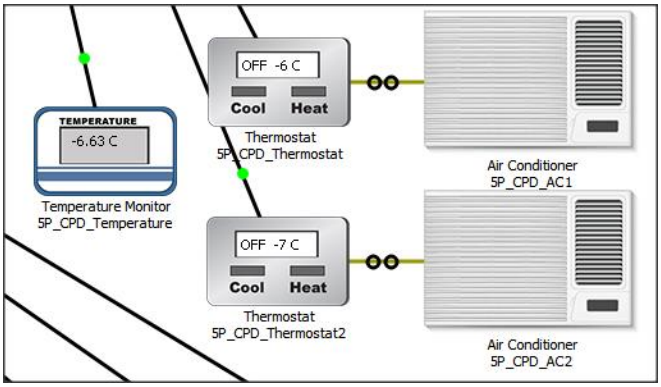


Figura 79. Aire acondicionado centralizado del CPD en visualización lógica

VISUALIZACIÓN FÍSICA

Este elemento necesita de varias interfaces en el conmutador S5P_CPD para conectar el monitor de temperatura y los dos termostatos. El monitor de temperatura se conecta a la interfaz *fastEthernet0/13* y los dos termostatos se conectan a las interfaces *fastEthernet0/11* y *fastEthernet0/12*.

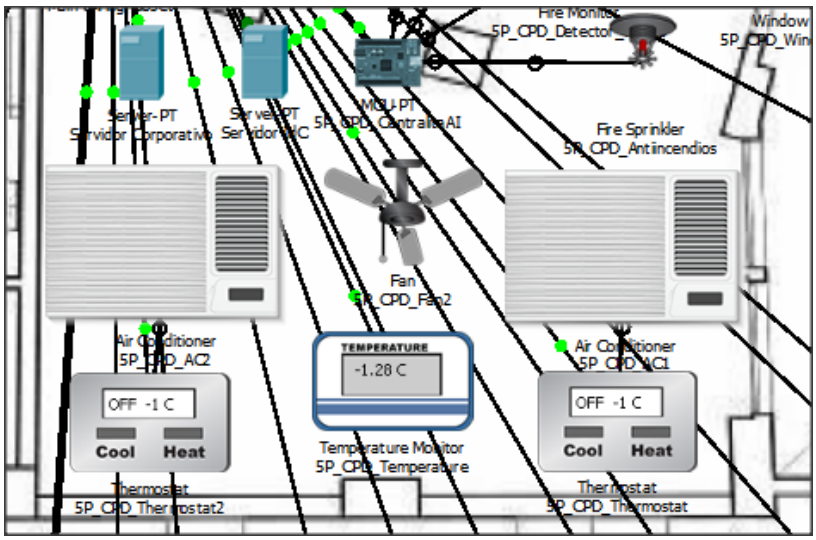


Figura 80. Aire acondicionado centralizado del CPD en visualización física

PROGRAMACIÓN

Si el monitor de temperatura detecta una temperatura superior o igual a 15ºC entonces activa los ACs. Si la temperatura es inferior o igual a 5ºC se desactivan los ACs.

Las dos reglas definidas en el servidor IdC en la pestaña de *Conditions* para este elemento son (Figura 81):

Edit Remove	Yes	5P_CPD_ACs_On	5P_CPD_Temperature Temperature >= 15.0 °C	Set 5P_CPD_Thermostat Status to Cooling Set 5P_CPD_Thermostat2 Status to Cooling
Edit Remove	Yes	5P_CPD_ACs_Off	5P_CPD_Temperature Temperature <= 5.0 °C	Set 5P_CPD_Thermostat Status to Off Set 5P_CPD_Thermostat2 Status to Off

Figura 81. Programación de reglas del elemento IdC (Aire acondicionado centralizado del CPD)

MONITOR DE FUEGO EN EL CPD

El monitor de fuego está compuesto por una microcontroladora que activa los aspersores y una alarma ubicada fuera del CPD. Además, envía una notificación a una empresa externa de extinción de incendios para que acudan al lugar donde se ha producido el fuego.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de 5ª planta del CPD.

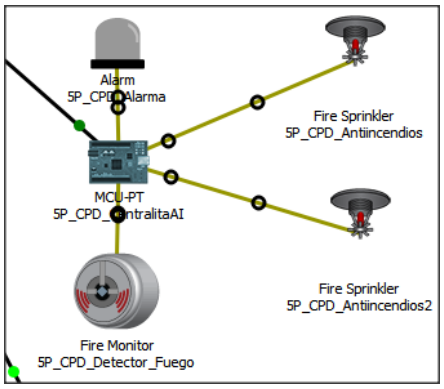


Figura 82. Monitor de fuego en el CPD en visualización lógica

VISUALIZACIÓN FÍSICA

Este elemento IdC necesita una única interfaz para conectar la microcontroladora al conmutador S5P_CPD. La interfaz utilizada es la *fastEthernet0/10*.

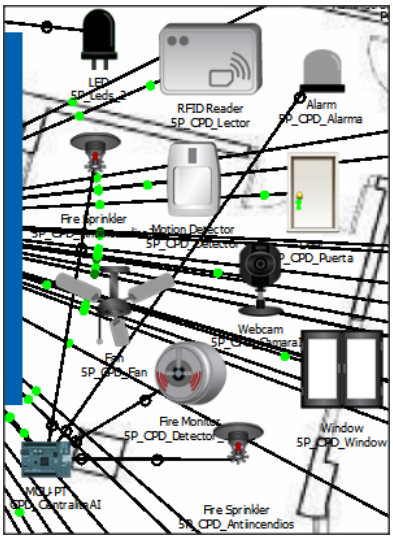


Figura 83. Monitor de fuego en el CPD en visualización física

PROGRAMACIÓN

En este caso, la microcontroladora es la encargada de modelar el comportamiento de este elemento IdC. Si se detecta fuego, el monitor de fuego envía una señal a la microcontroladora para que active los aspersores y la alarma. Además, la microcontroladora envía una notificación de carácter urgente. El código se presenta en la Figura 84.

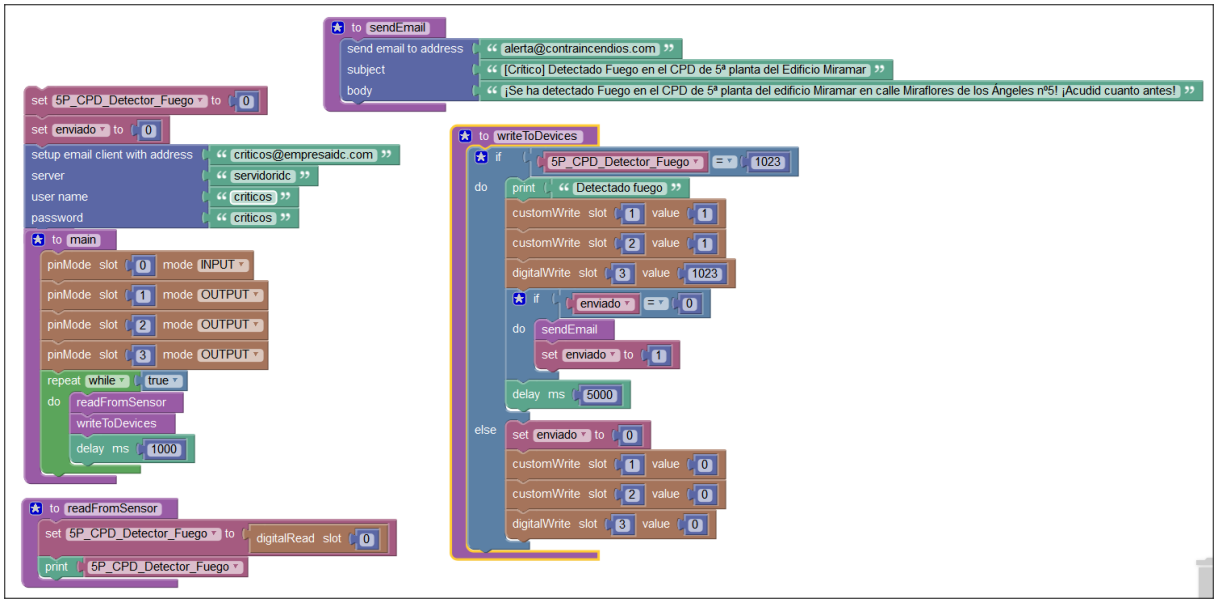


Figura 84. Programación Blockly del elemento IdC (monitor de fuego en el CPD)

AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA

El aire acondicionado y la calefacción centralizada es uno de los elementos IdC más interesantes que se implementan provisionalmente tan sólo en un departamento de la 6ª planta. Es un elemento que automáticamente va activando y desactivando dispositivos a medida que la temperatura va cambiando. Indicar que se han elegido unos rangos de temperatura amplios para poder comprobar el correcto funcionamiento del elemento IdC pero, en ningún caso, son los más óptimos ni eficientes para una empresa.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de la 6ª planta.

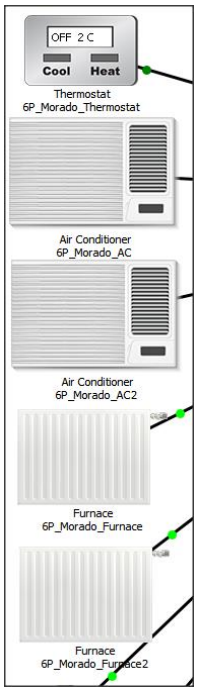


Figura 85. Aire acondicionado y calefacción centralizada en visualización lógica

VISUALIZACIÓN FÍSICA

Este elemento IdC necesita que todos sus dispositivos sean conectados al conmutador S6Pb. Las interfaces utilizadas son las siguientes:

CONMUTADOR	INTERFAZ	DISPOSITIVO
S6Pb	fastEthernet0/15	Termostato central
	fastEthernet0/16	Aire acondicionado

	fastEthernet0/17	Aire acondicionado
	fastEthernet0/18	Calefactor
	fastEthernet0/19	Calefactor

Tabla 93. Conexiones del elemento IdC

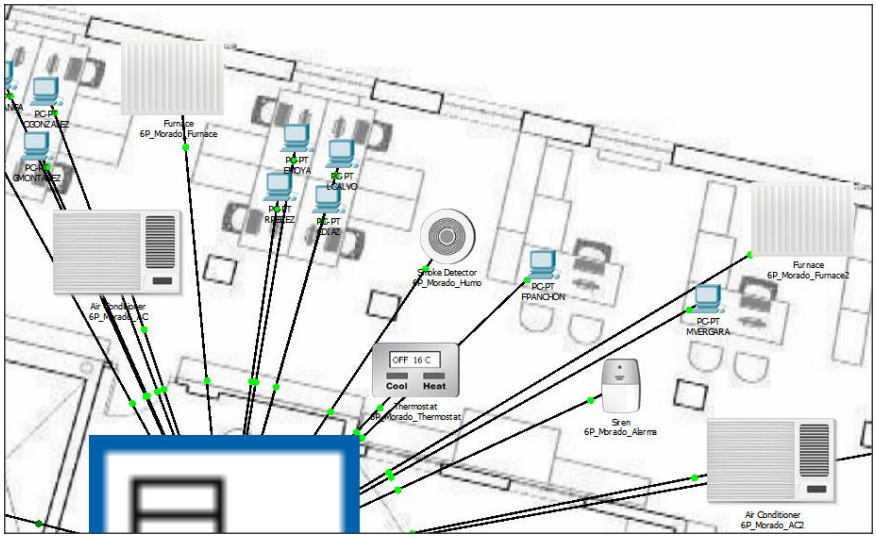


Figura 86. Aire acondicionado y calefacción centralizada en visualización física

Este elemento es muy interesante para todos los departamentos, aunque su implementación se realiza únicamente en el departamento morado para su testeo. Si dichas pruebas son satisfactorias se podría implementar en el resto de los departamentos como una futura mejora de las instalaciones.

PROGRAMACIÓN

Las reglas necesarias para modelar el comportamiento de este elemento corresponde implementarlas al servidor IdC.

Las reglas a implementar son las siguientes:

1. *Modo Frío.* Si la temperatura es superior o igual a 15ºC se activan los ACs y se apaga los calefactores. Si la temperatura es inferior o igual a 0ºC, se apagan los ACs (Figura 87).

Edit Remove	Yes	6P_Morado_Acs_Cooling_Off	Match all: • 6P_Morado_Thermostat Temperature <= 0.0 °C • 6P_Morado_Thermostat Status is Cooling	Set 6P_Morado_AC On to false Set 6P_Morado_AC2 On to false
Edit Remove	Yes	6P_Morado_Acs_Cooling_On	Match all: • 6P_Morado_Thermostat Status is Cooling • 6P_Morado_Thermostat Temperature >= 15.0 °C	Set 6P_Morado_AC On to true Set 6P_Morado_AC2 On to true Set 6P_Morado_Furnace On to false Set 6P_Morado_Furnace2 On to false

Figura 87. Programación de reglas del IdC (modo frío)

2. *Modo Calor.* Si la temperatura es inferior o igual a 0ºC se activan los calefactores y se desactivan los ACs. Si la temperatura es superior o igual a 15ºC se apagan los calefactores (Figura 88).

Edit Remove	Yes	6P_Morado_Furnace_On	Match all: • 6P_Morado_Thermostat Status is Heating • 6P_Morado_Thermostat Temperature <= 0.0 °C	Set 6P_Morado_Furnace On to true Set 6P_Morado_Furnace2 On to true Set 6P_Morado_AC On to false Set 6P_Morado_AC2 On to false
Edit Remove	Yes	6P_Morado_Furnace_Off	Match all: • 6P_Morado_Thermostat Status is Heating • 6P_Morado_Thermostat Temperature >= 15.0 °C	Set 6P_Morado_Furnace On to false Set 6P_Morado_Furnace2 On to false

Figura 88. Programación de reglas del IdC (modo calor)

3. *Modo Auto.* Si la temperatura es superior o igual a 15ºC se apagan los calefactores y se activan los ACs. Si la temperatura es inferior o igual a 0ºC, se activan los calefactores y desactivan los ACs (Figura 89).

Edit Remove	Yes	6P_Morado_Auto_Cooling_On	Match all: • 6P_Morado_Thermostat Status is Auto • 6P_Morado_Thermostat Temperature >= 15.0 °C	Set 6P_Morado_AC On to true Set 6P_Morado_AC2 On to true Set 6P_Morado_Furnace On to false Set 6P_Morado_Furnace2 On to false
Edit Remove	Yes	6P_Morado_Auto_Heating_On	Match all: • 6P_Morado_Thermostat Status is Auto • 6P_Morado_Thermostat Temperature <= 0.0 °C	Set 6P_Morado_Furnace On to true Set 6P_Morado_Furnace2 On to true Set 6P_Morado_AC On to false Set 6P_Morado_AC2 On to false

Figura 89. Programación de reglas del IdC (modo auto)

4. *Modo Off*, permanecen apagados tanto los ACs como los calefactores (Figura 90).

Edit Remove	Yes	6P_Morado_Acs_Furnaces_Off	6P_Morado_Thermostat Status is Off	Set 6P_Morado_AC On to false Set 6P_Morado_AC2 On to false Set 6P_Morado_Furnace On to false Set 6P_Morado_Furnace2 On to false

Figura 90. Programación de reglas del IdC (modo off)

LUCES AUTOMÁTICAS DE LA FACHADA

Las luces automáticas de la fachada permiten al edificio estar iluminado en aquellos momentos en los que hay poca luz solar. Para ello utiliza un detector de luminosidad y una microcontroladora para gestionar el encendido y apagado de las luces, así como el envío de una notificación de encendido.

VISUALIZACIÓN LÓGICA

Este elemento IdC se conecta al conmutador de la 6ª planta.

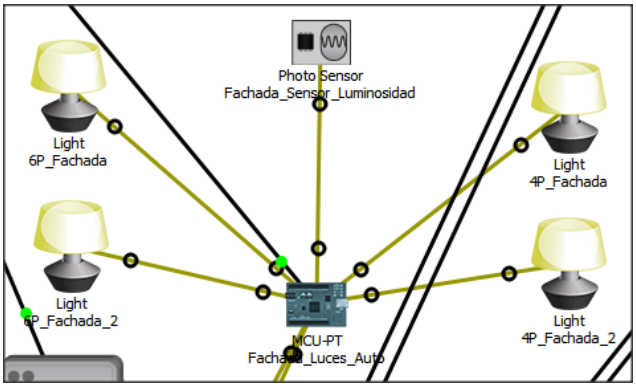


Figura 91. Luces automáticas de la fachada en visualización lógica

VISUALIZACIÓN FÍSICA

Cada una de las luces de este elemento IdC se ubican en la fachada en su respectiva planta y el detector de luminosidad se instala en la terraza del edificio. La microcontroladora se conecta al conmutador S6Pb en la interfaz *fastEthernet0/14*.

Figura 92. Luces automáticas de la fachada en visualización física

PROGRAMACIÓN

Cada vez que se produce una disminución importante en la luminosidad (inferior al 20% de luz) y es detectada por el sensor, la microcontroladora envía la señal para que se activen las luces y, además, envía una notificación de encendido al administrador.

Para modelar este elemento IdC se programa la microcontroladora del siguiente modo (Figura 93):

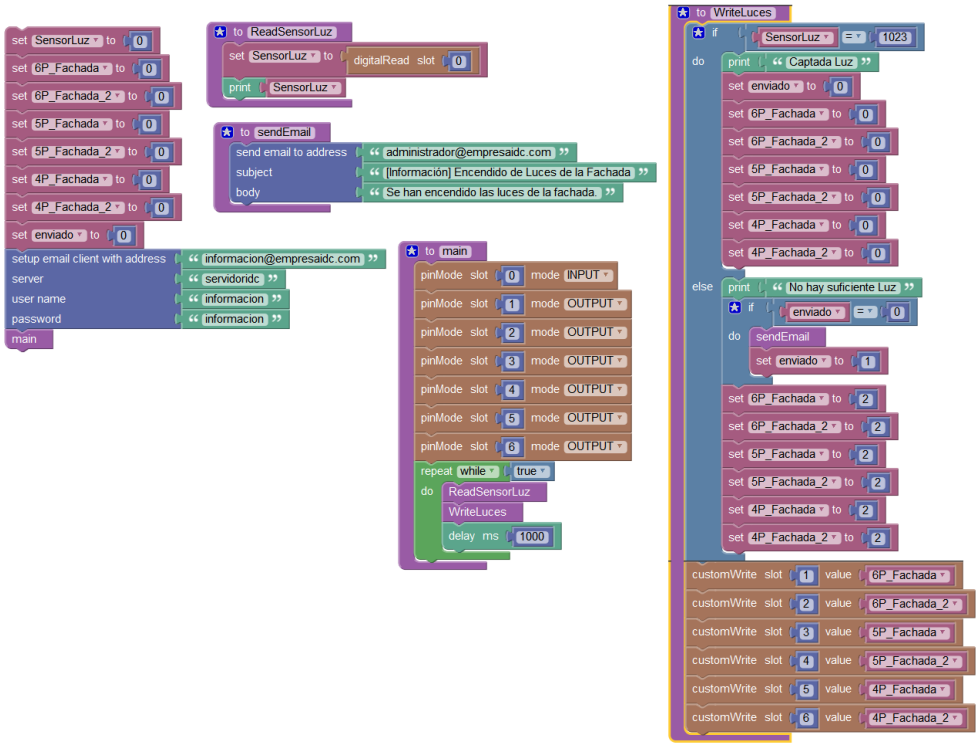


Figura 93. Programación Blockly del elemento IdC (luces automáticas de la fachada)

De este modo, cuando se detecta poca luminosidad, se activan las luces y se envía la notificación de encendido al administrador.

SERVIDOR IDC

El servidor IdC es el dispositivo más importante de todos los elementos IdC que se van a implementar, sin él, no sería posible realizar reglas de comportamiento sobre los elementos IdC ni tampoco sería posible conocer el estado de los mismos. Por eso es fundamental.

VISUALIZACIÓN LÓGICA

El servidor IdC se conecta al conmutador S5P_CPD de la capa de acceso.

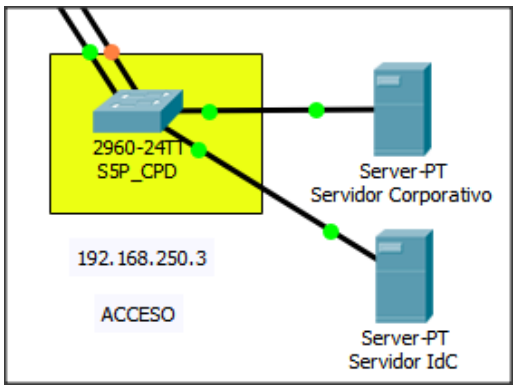


Figura 94. Servidor IdC en visualización lógica

VISUALIZACIÓN FÍSICA

El servidor IdC se ubica dentro del CPD que está en la 5ª planta dada su gran importancia y transcendencia, cerca del servidor corporativo.

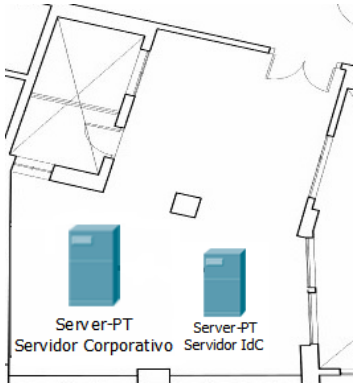


Figura 95. Servidor IdC en visualización física

El servidor IdC no es más que un servidor con el servicio del Internet de las Cosas activo. Además del servicio IdC activo, también necesita tener activo el servidor de correo, ya que las notificaciones serán realizadas por correo electrónico desde el servidor IdC. Este servidor tiene muchos servicios activos que deben ser desactivados, como, por ejemplo, los servicios de FTP, TFTP, NTP, etc.

SERVICIO	ACTIVADO
HTTP	Si
EMAIL	Si
IOT (IdC)	Si

Tabla 94. Servicios necesarios

El servicio HTTP está habilitado debido al servicio IOT (IdC), al activarlo se activa HTTP, ya que la gestión del servidor IdC se realiza a través del navegador web.

CORREO ELECTRÓNICO (EMAIL)

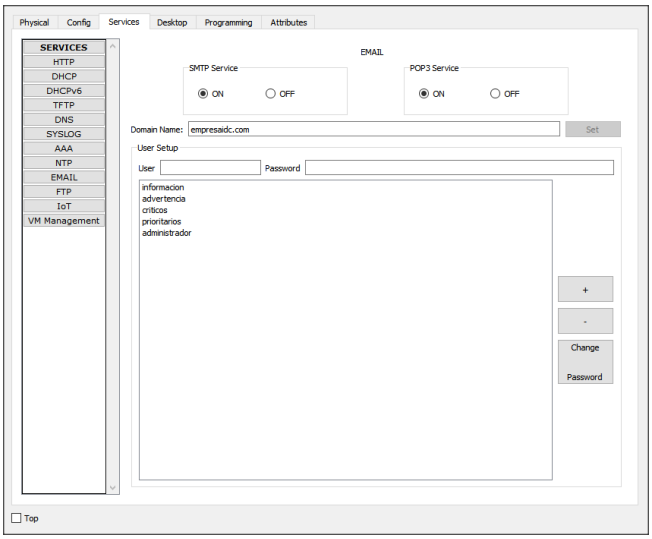


Figura 96. Configuración del servicio de correo electrónico

En la fase de diseño se definió una escala de incidencias según la gravedad de las incidencias y se establecieron tres categorías (*Información, Prioritarios y Críticos*). Por lo que, en el servidor de correo IdC, se da de alta una cuenta por cada categoría de la incidencia:

informacion@empresaidc.com. Notificaciones sobre el encendido de las luces.

prioritarios@empresaidc.com. Incidencias relacionadas con los accesos a las salas.

criticos@empresaidc.com. Incidencia grave al detectar fuego en el CPD.

Cada una de ellas será utilizada cuando ocurra alguna incidencia de su categoría, es decir, si se produce un encendido de luces de la fachada, por ejemplo, se enviará un correo electrónico desde la dirección de información@empresaidc.com al administrador de elementos IdC, que será el que reciba las incidencias que se van produciendo en los elementos IdC. Por lo tanto, es necesario crear una cuarta cuenta de correo electrónico, que será la del administrador. La cuenta de correo electrónico se llama administrador@empresaidc.com.

En caso de incidencias críticas, como sería el caso de detectar fuego en el CPD, se enviaría una notificación crítica a una empresa externa, cuya dirección de correo es alerta@contraincendios.com, reportando la gravedad de la incidencia e indicando los datos donde se encuentra el edificio, así como, donde se ha producido el incendio.

IOT (IDC)

Se activa el servicio del *Internet de las Cosas* (IdC) y se establece el usuario y la contraseña de acceso web al servidor IdC.

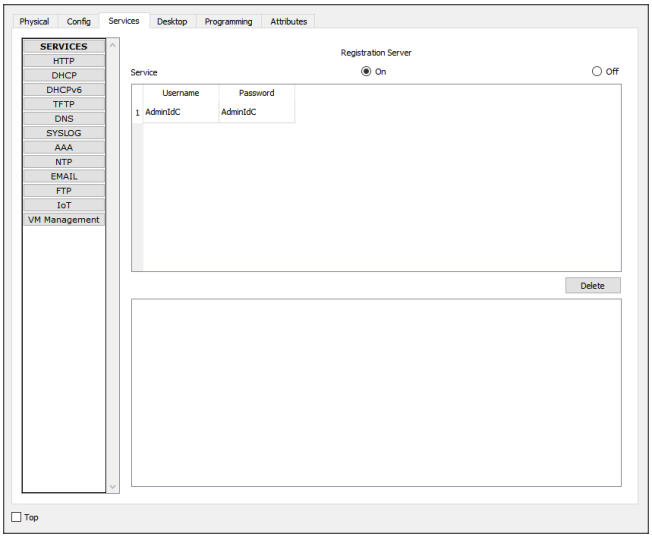


Figura 97. Habilitar servicio IoT (IdC) en el servidor IdC

Se establece como **usuario** *AdminIdC* y como **contraseña** *AdminIdC*.

Una vez activado el servicio, en la pestaña *Desktop* se puede acceder a la plataforma web de IoT. Para ello, se pulsa sobre el icono *IoT Monitor*.

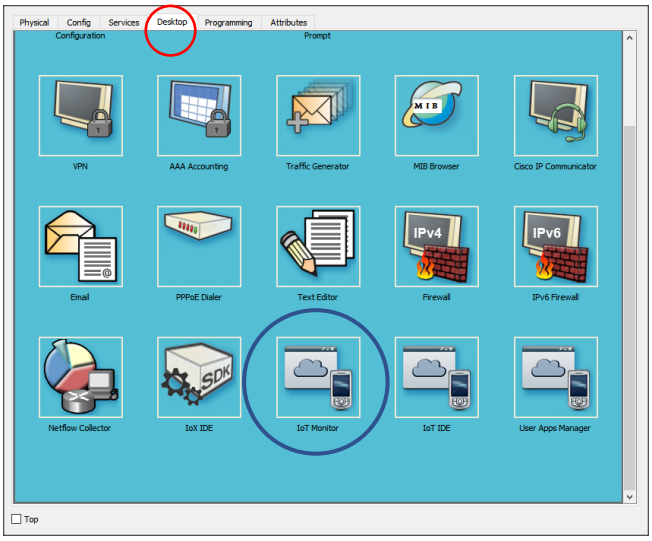


Figura 98. Acceso a IoT Monitor en la pestaña Desktop

A continuación, se introduce el usuario y contraseña definidos y se accedería al servidor IoT donde se pueden monitorizar los elementos IdC registrados.

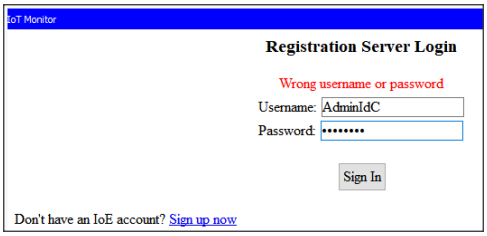


Figura 99. Acceso al servidor web de IoT (IdC)

Una vez se introducen las credenciales, se accede al servidor IoT (IdC), donde se observan cuatro apartados en la parte superior derecha (Figura 100):

- **Home**. Muestra todos los elementos IdC registrados y sus estados actuales. Dependiendo del elemento seleccionado, se puede interactuar con él, activando, desactivando o cambiando ciertos parámetros del mismo. Es la página por defecto.
- **Conditions**. Se muestran las reglas de comportamiento definidas para los elementos IdC. Además, se pueden crear, eliminar o modificar las reglas en dicho apartado.
- **Editor**. Permite la programación del servidor IdC mediante la utilización de JavaScript, Python o programación Visual.
- **Log Out**. Permite desconectarse del servidor IdC.

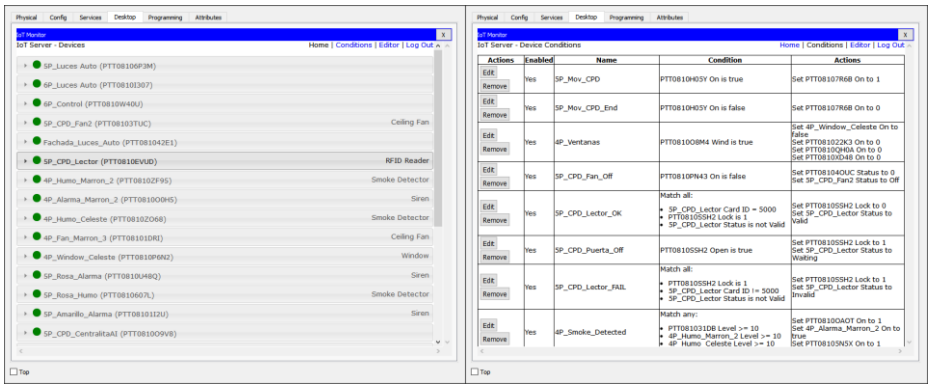


Figura 100. Visualización del apartado Home y Conditions del servidor IdC

A medida que se vayan registrando los elementos IdC en el servidor IdC, se irán definiendo las reglas de comportamiento si fuera necesario. Recordar de la fase de diseño del capítulo 2, que no todos los elementos necesitan reglas en el servidor, muchos de ellos, serán controlados por MCU/SBC por lo que requerirá una programación especial en la propia microcontroladora.

3.1.5 IMPLEMENTACIÓN FINAL

En este apartado se muestra el resultado de la implementación final con todos los elementos involucrados, tanto los equipos informáticos y dispositivos de red, así como los elementos IdC definidos en la fase de diseño del capítulo 2.

En la visualización lógica (Figura 101) se observa la gran cantidad de elementos introducidos en el simulador, aproximadamente 160 elementos dentro del área de trabajo. Además, se han introducido ciertos dispositivos de red para simular la comunicación con la empresa externa, ya sea, a través de un teléfono móvil o una Tablet. Desde ambos dispositivos se puede acceder al servidor IdC, así como recibir las notificaciones.

Todas las visualizaciones físicas de los distintos planos (global, intermedio y corto) pueden observarse en el anexo (ver Anexo 1). En estas visualizaciones físicas se aprecian todos los elementos que forman cada una de las plantas.

VISUALIZACIÓN LÓGICA

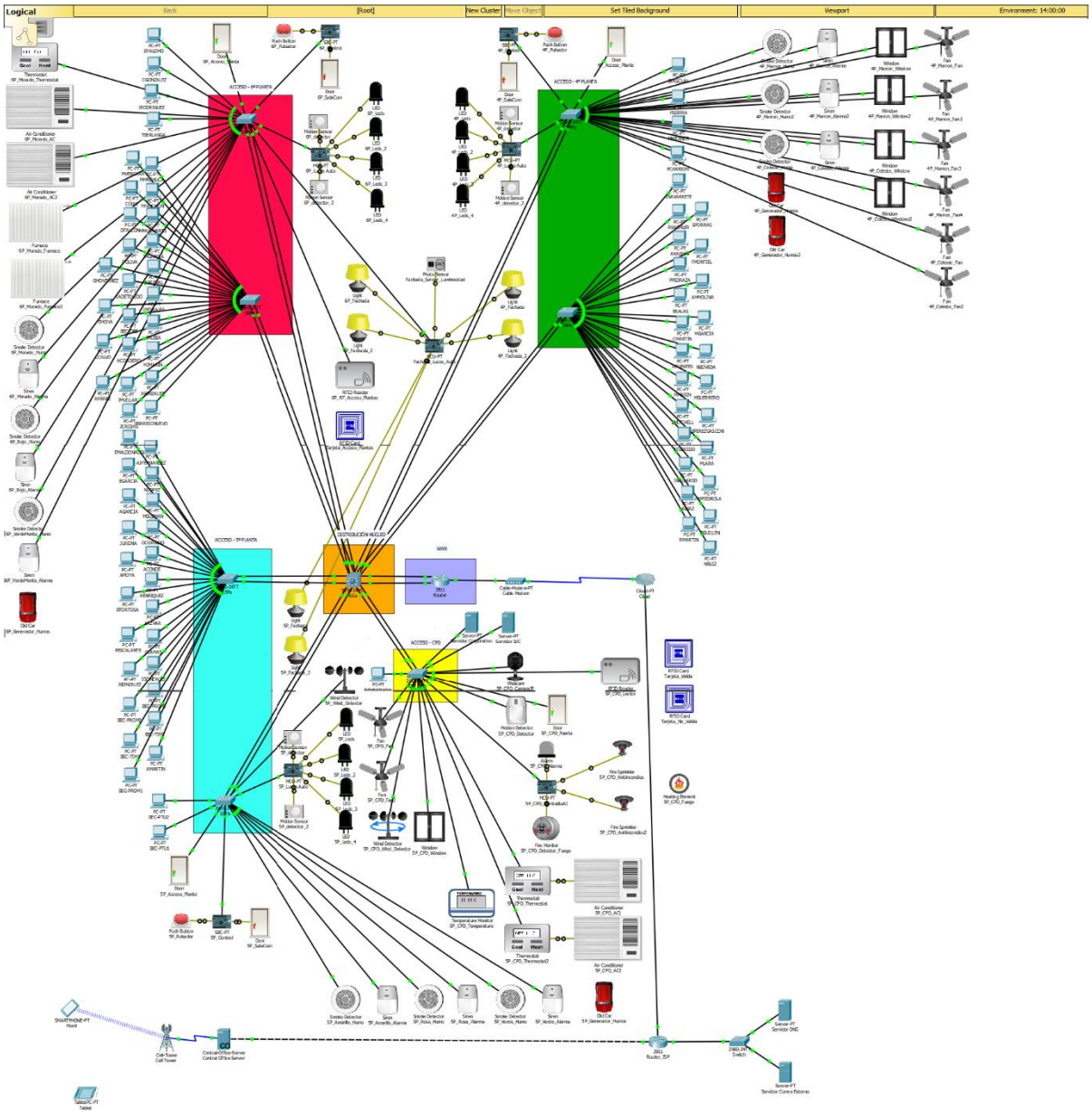


Figura 101. Visualización lógica del simulador con todos los elementos IdC y dispositivos

3.2 FASE DE OPERACIÓN

En esta fase se mantiene el estado de la red día a día. Esto incluye la administración y monitoreo de los componentes de la red, mantenimiento de ruteo, administración de las actualizaciones, administración del rendimiento, e identificación y corrección de errores de red. Esta fase es la prueba final de diseño.

El diseño es verificado realizando pruebas por separado de cada uno de sus elementos y comprobando que posteriormente su comportamiento con el resto de elementos del simulador.

En esta fase se han realizado una gran cantidad de pruebas de comportamiento sobre todos y cada uno de los elementos instalados en la red. De forma resumida, este capítulo describe algunas de las pruebas realizadas sobre los elementos más relevantes.

CORREO ELECTRÓNICO ENTRE USUARIOS

Se verifica el correcto funcionamiento del correo electrónico corporativo entre dos equipos informáticos ubicados en distintos departamentos y plantas.

El equipo informático que envía el correo electrónico es el denominado **RFUENTES**. Este equipo está ubicado en la 4ª planta y tiene configurado el cliente de correo electrónico con la cuenta usuario@empresa.com.

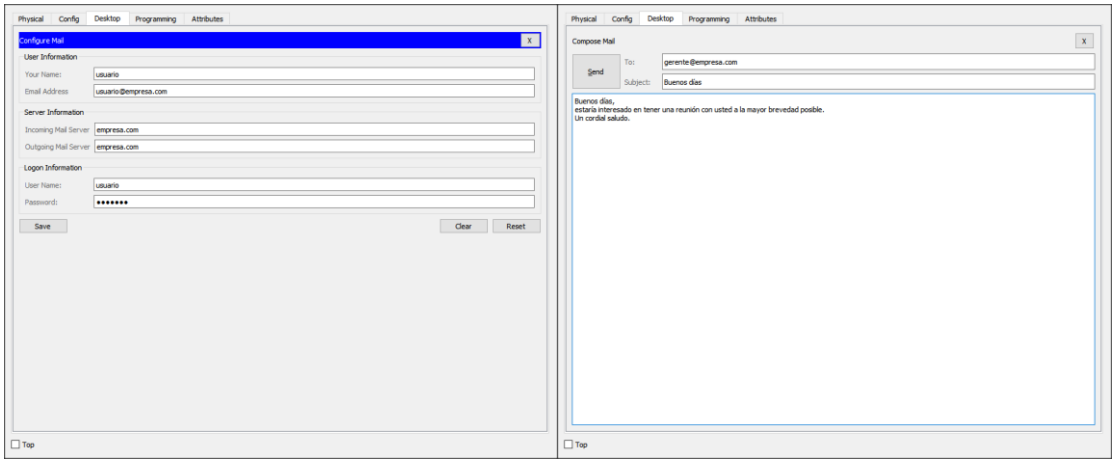


Figura 102. Configuración de cliente de correo y envío de correo electrónico

Este equipo realiza el envío de un correo electrónico a gerente@empresa.com. Siendo recibido por el equipo informático llamado **ABERNAL**, el cual se encuentra en la 6ª planta.

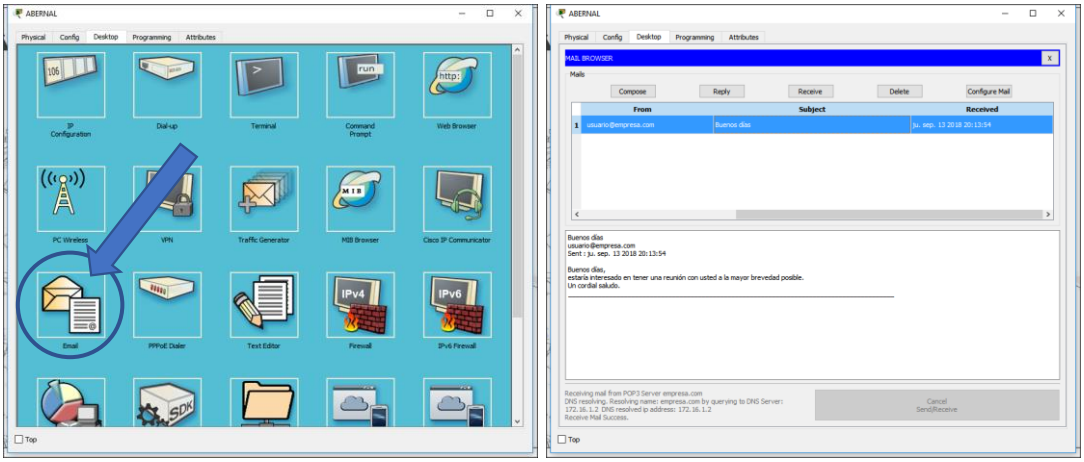


Figura 103. Acceso al cliente de correo (Email) y comprobación del correo electrónico

RESTRICCIONES ENTRE DEPARTAMENTOS

En este apartado se comprueba el correcto funcionamiento de las restricciones implantadas entre los departamentos (Figura 12). Para realizar la comprobación se utilizan los equipos informáticos de los distintos departamentos. Se eligen dos equipos informáticos de departamentos distintos para realizar las pruebas mediante la utilización del comando **ping** desde la línea de comando.

La línea de comando (*Command Prompt*) se encuentra en la pestaña *Desktop* de los equipos informáticos tal y como se muestra en la siguiente figura (Figura 104):

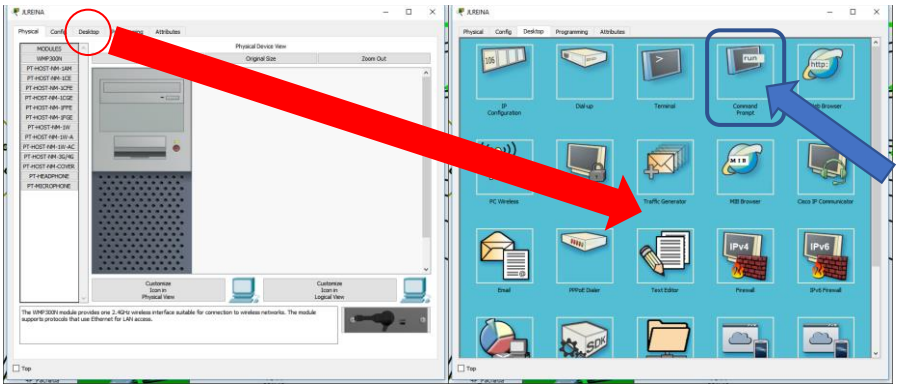


Figura 104. Propiedades del equipo informático y acceso a Command Prompt

Desde la línea de comando se verifica la comunicación con los distintos departamentos siguiendo las restricciones establecidas desde la Tabla 56 hasta la Tabla 80 de la fase de implementación.

Equipo **JLREINA**: 192.168.50.45 (ubicado en 5ª planta)

RESULTADOS	
PERMITIDO	**DENEGADO**

`C:\>ping 172.16.1.2`
 	
`Pinging 172.16.1.2 with 32 bytes of data:`
 	
`Reply from 172.16.1.2: bytes=32 time=27ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time=12ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time<1ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time<1ms TTL=127`
	`C:\>ping 192.168.50.2`
	
	`Pinging 192.168.50.2 with 32 bytes of data:`
	
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`

`C:\>ping 192.168.40.33`
 	
`Pinging 192.168.40.33 with 32 bytes of data:`
 	
`Reply from 192.168.40.33: bytes=32 time<1ms TTL=255`
`Reply from 192.168.40.33: bytes=32 time<1ms TTL=255`
`Reply from 192.168.40.33: bytes=32 time<1ms TTL=255`
`Reply from 192.168.40.33: bytes=32 time<1ms TTL=255`
	`C:\>ping 192.168.50.18`
	
	`Pinging 192.168.50.18 with 32 bytes of data:`
	
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`

`C:\>ping 192.168.40.6`
 	
`Pinging 192.168.40.6 with 32 bytes of data:`
 	
`Reply from 192.168.40.6: bytes=32 time=136ms TTL=127`
`Reply from 192.168.40.6: bytes=32 time<1ms TTL=127`
`Reply from 192.168.40.6: bytes=32 time<1ms TTL=127`
`Reply from 192.168.40.6: bytes=32 time<1ms TTL=127`
	`C:\>ping 172.16.0.2`
	
	`Pinging 172.16.0.2 with 32 bytes of data:`
	
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`
	`Reply from 192.168.50.33: Destination host unreachable.`

Tabla 95. Comprobaciones de restricciones desde JLREINA

El resultado obtenido es el resultado esperado. Han sido permitidas las conexiones al servidor corporativo (172.16.1.2) y a los dos departamentos de 4ª planta (192.168.40.33 y 192.168.40.6) y han sido rechazadas las conexiones con el servidor IdC (172.16.0.2) y con los dos departamentos restantes de la 5ª planta (192.168.50.2 y 192.168.50.18).

Equipo **SPASCUAL**: 192.168.40.24 (ubicado en 4ª planta)

RESULTADOS	
PERMITIDO	**DENEGADO**

`C:\>ping 172.16.1.2`
 	
`Pinging 172.16.1.2 with 32 bytes of data:`
 	
`Reply from 172.16.1.2: bytes=32 time=27ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time=12ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time<1ms TTL=127`
`Reply from 172.16.1.2: bytes=32 time<1ms TTL=127`
	`C:\>ping 192.168.60.33`
	
	`Pinging 192.168.60.33 with 32 bytes of data:`
	
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`

`C:\>ping 192.168.60.2`
 	
`Pinging 192.168.60.2 with 32 bytes of data:`
 	
`Reply from 192.168.60.2: bytes=32 time<1ms TTL=127`
`Reply from 192.168.60.2: bytes=32 time=86ms TTL=127`
`Reply from 192.168.60.2: bytes=32 time<1ms TTL=127`
`Reply from 192.168.60.2: bytes=32 time=1ms TTL=127`
	`C:\>ping 192.168.50.17`
	
	`Pinging 192.168.50.17 with 32 bytes of data:`
	
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`
	`Reply from 192.168.40.1: Destination host unreachable.`

```
C:\>ping 192.168.40.33

Pinging 192.168.40.33 with 32 bytes of data:

Reply from 192.168.40.33: bytes=32 time<1ms TTL=255
Reply from 192.168.40.33: bytes=32 time<1ms TTL=255
Reply from 192.168.40.33: bytes=32 time=12ms TTL=255
Reply from 192.168.40.33: bytes=32 time<1ms TTL=255
```

```
C:\>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 192.168.50.33: Destination host unreachable.
Reply from 192.168.50.33: Destination host unreachable.
Reply from 192.168.50.33: Destination host unreachable.
Reply from 192.168.50.33: Destination host unreachable.
```

Tabla 96. Comprobaciones de restricciones desde SPASCUAL

El resultado obtenido también es correcto según las restricciones establecidas. Se realiza satisfactoriamente conexión con el servidor corporativo (172.16.1.2) y con el departamento morado de 6ª planta (192.168.60.2) y con el departamento celeste de 4ª planta (192.168.40.33) y han sido rechazadas las conexiones con el servidor IdC (172.16.0.2) y con el departamento rojo de 6ª planta (192.168.60.33) y con el departamento rosa de 5ª planta (192.168.50.17).

Por simplificar el proceso tan sólo se muestran dos de las pruebas realizadas para verificar el correcto funcionamiento de las restricciones establecidas.

ACCESO AL SERVIDOR IDC DESDE EL EXTERIOR

En este apartado se verifica el correcto funcionamiento de la conexión desde el exterior al servidor IdC. Para ello, se utiliza el teléfono móvil o la tableta implementada en el plano global (Anexo 1). Al hacer clic sobre el terminal móvil se abre una ventana con las propiedades del dispositivo. En la pestaña *Desktop* aparecen las aplicaciones instaladas en el dispositivo (Figura 105).

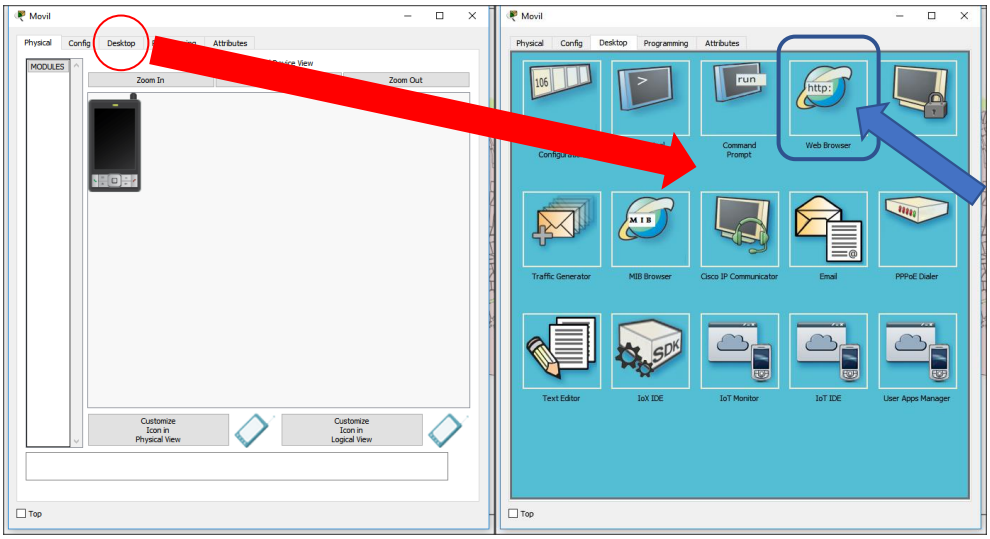


Figura 105. Propiedades del terminal móvil y acceso al navegador web

Se abre el navegador web que tiene instalado (*web browser*) y se teclea la dirección web de la empresa. En nuestro caso es http://www.empresaidc.com.

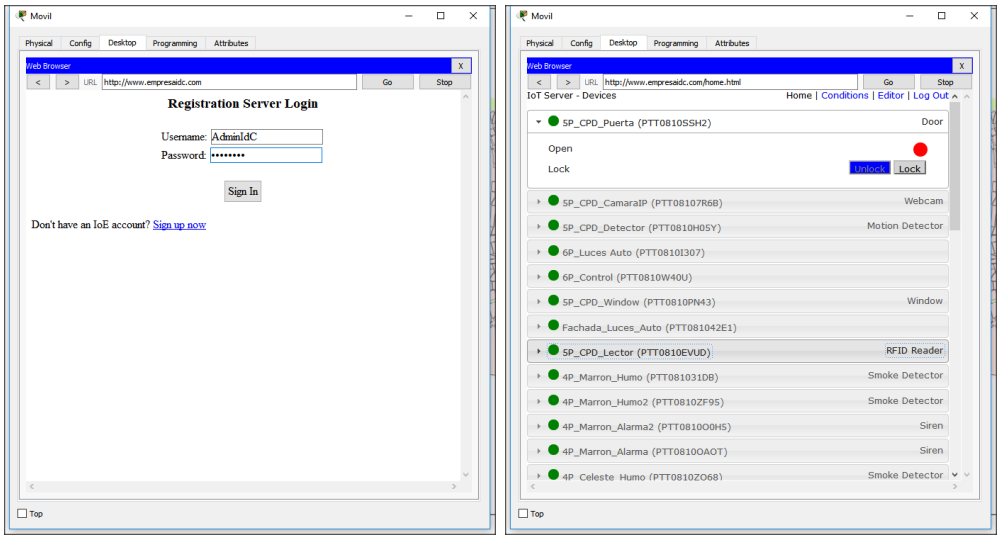


Figura 106. Acceso a servidor web y visualización de listado de elementos IdC

Se inicia sesión en el servidor IdC y se muestra a continuación el listado de los elementos IdC registrados en el servidor, siendo posible la monitorización y la gestión de los mismos desde el terminal móvil.

ELEMENTO IDC: ACCESO A SALA DE COMUNICACIONES

Uno de los elementos IdC más interesantes a analizar es éste, ya que conlleva la utilización de la programación Blockly realizada en la microcontroladora. Para ser más precisos, se van a realizar las pruebas sobre el acceso a la sala de comunicaciones de la 6ª planta.

Este elemento IdC estaba formado por un pulsador, el cual, al ser accionado, envía una señal a la microcontroladora para que desbloquee la puerta inteligente y envía una notificación prioritaria de intento de acceso al administrador.

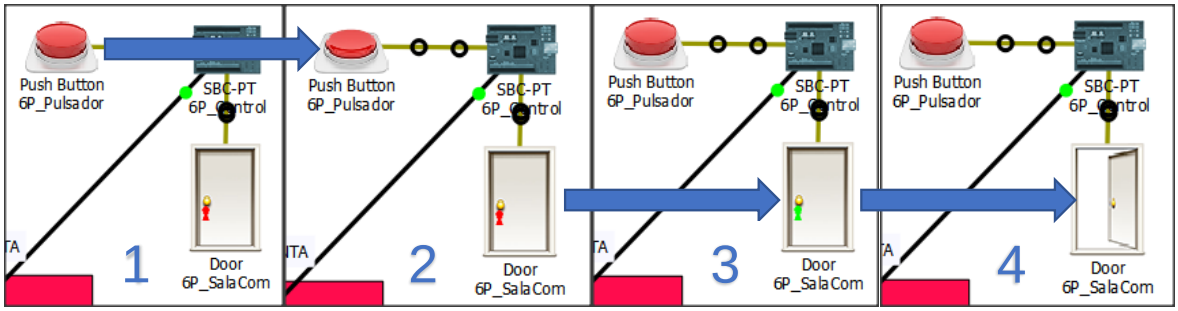


Figura 107. Estados del elemento IdC (acceso a sala de comunicaciones)

Como se observa en la secuencia de la Figura 107, se acciona el pulsador (2). La puerta inteligente es desbloqueada (3) y se procede a acceder a la sala (4).

Si se comprueba el correo electrónico del administrador, en la pestaña *Desktop* del equipo informático llamado **Administrador** se encuentra la aplicación de correo electrónico (*Email*).

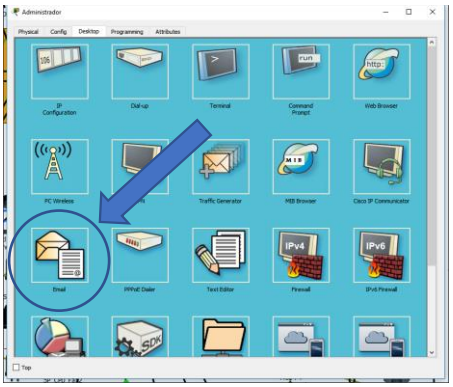


Figura 108. Acceso al cliente de correo (Email)

En dicha aplicación de correo electrónico el administrador recibe las notificaciones referentes al encendido de las luces de pasillo y fachada, así como de los intentos de acceso a las salas.

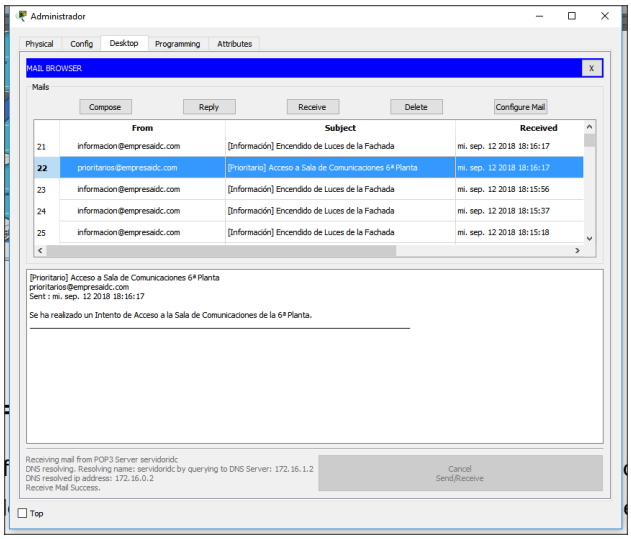


Figura 109. Revisión de correo electrónico

En la Figura 109, se observan los distintos correos recibidos entre los que se encuentra el intento de acceso a la sala de comunicaciones de la 6ª planta.

ELEMENTO IDC: ACCESO AL CPD

Otro elemento IdC interesante es el que controla el acceso al CPD por el número de elementos que lo componen. Otro aspecto que lo hace interesante es que no utiliza microcontroladora, por lo que las reglas se definen en el servidor IdC, el cual se encarga de comprobar el correcto funcionamiento del elemento IdC.

Este elemento se inicia con la utilización de una tarjeta RF. Dicha tarjeta se utiliza pasándola por el lector RF del CPD. Si la tarjeta es válida, la puerta inteligente se desbloquea, en caso contrario, la puerta permanece bloqueada (Figura 110).

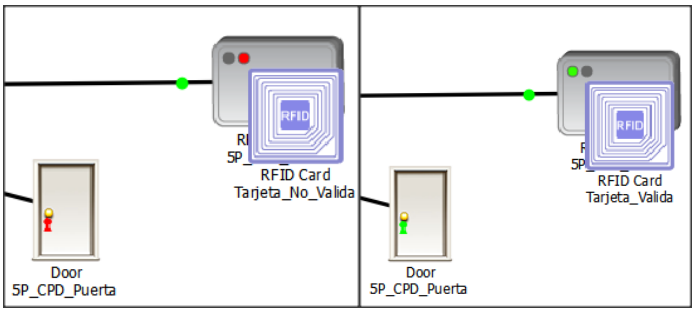


Figura 110. Acceso denegado vs Acceso válido

Si la tarjeta RF utilizada es válida, se habilita el acceso al CPD y es posible abrir la puerta inteligente. Una vez dentro del CPD el detector de movimiento se activa y la cámara comienza a grabar. Cuando cese el movimiento dentro del CPD la cámara dejará de grabar (Figura 111).

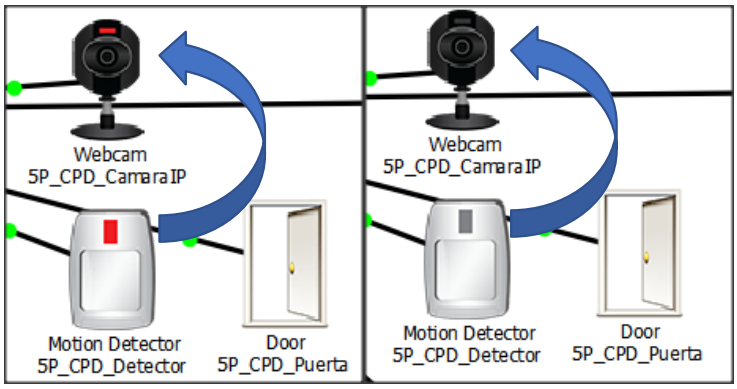


Figura 111. Detección de movimiento vs sin detección

Una vez finalizado el acceso al CPD, la puerta se bloquea al ser cerrada (Figura 112).

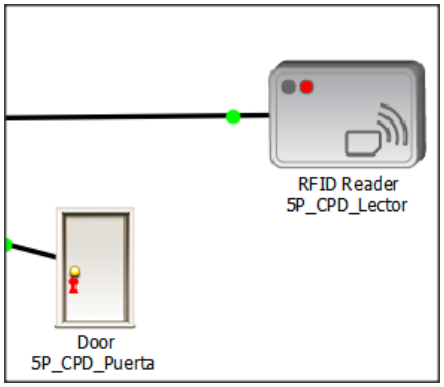


Figura 112. Bloqueo de la puerta del CPD

ELEMENTO IDC: DETECTOR DE FUEGO

Este elemento IdC resulta también bastante interesante, ya que necesita comunicación con el exterior al realizar la notificación a una empresa externa. Además, este elemento utiliza una microcontroladora para la activación del resto de elementos que lo forman y para la notificación al exterior de la incidencia.

Se inicia con la actuación del fuego cerca del detector de fuego. Al ser detectado el fuego se envía una señal a la microcontroladora para que active los aspersores y la alarma exterior ubicada fuera del CPD (Figura 113) y envíe la notificación crítica a la empresa externa.

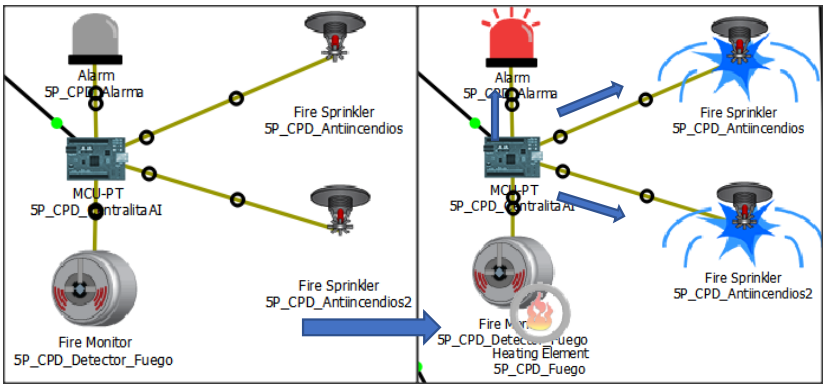


Figura 113. Elemento IdC en reposo vs elemento IdC en funcionamiento

La notificación crítica llega al terminal móvil de la empresa externa. En ella aparecen todos los datos necesarios para que acudan a la empresa a sofocar el fuego (Figura 114).

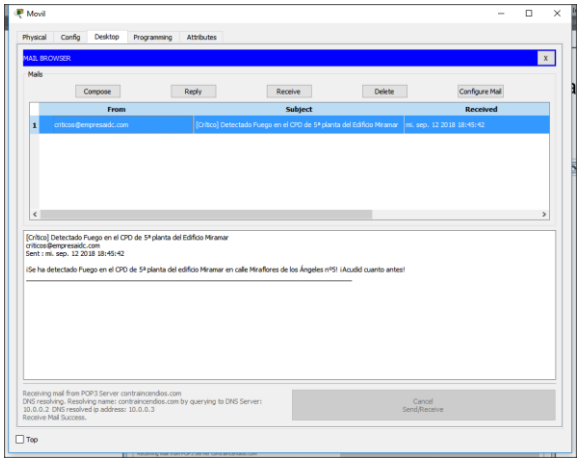


Figura 114. Terminal móvil recibiendo notificación crítica

ELEMENTO IDC: AIRE ACONDICIONADO Y CALEFACCIÓN CENTRALIZADA

La realización de este elemento IdC ha sido algo más compleja debido a que se han considerado cuatro modos de funcionamiento.

El comportamiento según el modo de funcionamiento es el siguiente:

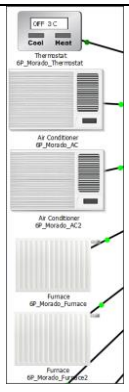
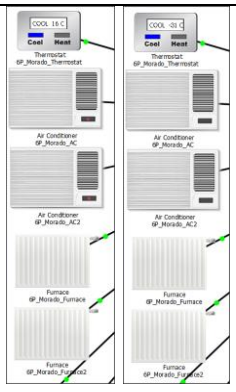
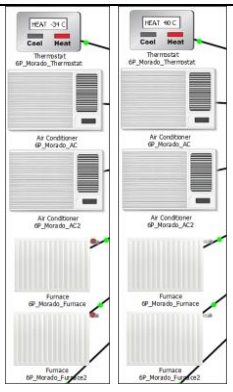
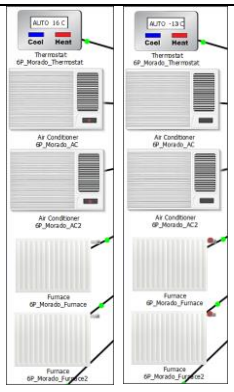
MODOS						
OFF	**COLD**		**HEAT**		**AUTO**	
						
Apagado	>=15ºC	<=0ºC	<=0ºC	>=15ºC	>=15ºC	<=0ºC

Tabla 97. Modos de funcionamiento

El Modo desactivado (*Off*) mantiene los aires acondicionados y los calefactores apagados.

El Modo frío (*Cold*) activa los aires acondicionados cuando la temperatura es superior o igual a 15ºC y los desactiva cuando la temperatura es inferior o igual a 0ºC.

El Modo calor (*Heat*) activa los calefactores cuando la temperatura es inferior o igual a 0ºC y los desactiva cuando la temperatura es superior o igual a 15ºC.

El Modo automático (*Auto*) activa los aires acondicionados cuando la temperatura es superior o igual a 15ºC y desactiva los calefactores, cuando la temperatura es inferior o igual a 0ºC desactiva los aires acondicionados y activa los calefactores.

Todos los modos han sido probados y su comportamiento ha sido el esperado. Indicar que el termostato genera aleatoriamente la temperatura inicialmente y que a medida que se activan y desactivan los distintos elementos la temperatura se actualiza en función de los elementos activados y de ese valor aleatorio generado.

3.3 FASE DE OPTIMIZACIÓN

En esta fase se trata de realizar una administración proactiva, identificando y resolviendo cuestiones antes de que afecten a la red. Esta fase puede crear una modificación al diseño si aparecen demasiados problemas, para mejorar el rendimiento o resolver cualquier problema detectado.

Por otro lado, se pueden realizar optimizaciones en determinados aspectos del diseño, como por ejemplo en la configuración de los enlaces EtherChannel realizada en los dispositivos de red. El Agregado de Enlaces (LAG)

La configuración del enlace EtherChannel puede optimizarse indicando el tipo de balanceo de carga que quiere realizar sobre el enlace, es decir, la forma de enviar el tráfico de red a través de los enlaces físicos. En los dispositivos de red que se han utilizado pueden utilizarse dos modos principalmente:

- *Balanceo por MAC origen*: los paquetes son distribuidos por el enlace EtherChannel según la MAC del origen. Es interesante su utilización en los conmutadores de capa 2 de acceso, ya que la mayor parte del tráfico generado se origina en los dispositivos finales, por lo que distribuir el tráfico de red según el origen generaría un mejor reparto de la carga sobre el enlace EtherChannel.

```
(config)#port-channel load-balance src-mac
```

- *Balanceo por IP origen e IP destino*. Los paquetes son distribuidos por el enlace EtherChannel según la combinación entre IP origen e IP destino. Este modo de balanceo de carga es el utilizado en conmutadores de capa 3 ubicados en distribución.

```
(config)#port-channel load-balance src-dst-ip
```

El protocolo de enrutamiento RIP también puede ser optimizado. Para ello, se puede configurar que el envío de actualizaciones del protocolo RIP se realice sólo por ciertas interfaces. Esta optimización es útil para evitar el envío de paquetes innecesarios a través de las interfaces. Para evitar dicho tráfico, hay que configurar las interfaces como *pasivas*. Los comandos que permiten desactivar las actualizaciones a través de la interfaz serían los siguientes:

COMANDO	DESCRIPCIÓN
`(config)#router rip`	Se habilita el protocolo RIP.
`(config-router)#passive-interface gigabitEthernet0/0`	Se desactiva el envío de notificaciones por la interfaz *gigabitEthernet0/0*.
`(config-router)#passive-interface gigabitEthernet0/1`	Se desactiva el envío de notificaciones por la interfaz *gigabitEthernet0/1*.

Tabla 98. Optimización de protocolo de enrutamiento RIP

Esta configuración se aplica al enrutador corporativo, dejando la interfaz *gigabitEthernet0/2* como la única que enviaría actualizaciones del protocolo RIP. También es posible realizarlo en el conmutador MLSa en todas las interfaces activas. La interfaz *gigabitEthernet1/0/24* es la única que debería enviar actualizaciones del protocolo RIP.

CONCLUSIONES Y TRABAJOS FUTUROS

Este trabajo fin de grado se ha centrado en la elaboración de un diseño de red corporativa integrando elementos del Internet de las Cosas (IdC) que pueda, en un futuro, ser desplegado en un entorno real. Para ello se ha considerado el software *Cisco Packet Tracer* para simular un entorno complejo, con un gran número de elementos interactuando, lo que genera una gran cantidad de información que debe ser recopilada, procesada y analizada para tomar las decisiones oportunas.

La realización de un diseño e implementación de una red corporativa es un proceso largo que requiere de un profundo análisis de las necesidades de la empresa, que conlleva muchas veces, la necesidad de replantear el diseño.

Dentro del diseño presentado en este trabajo cabe destacar el servidor IdC que es el encargado de recopilar, procesar y analizar la información, actuando mediante las reglas que modelan el comportamiento de los elementos IdC. Cabe mencionar que la simulación presentada se encuentra limitada por el software utilizado en cuanto al tipo de reglas que permite, pudiendo ser necesarias reglas de mayor complejidad.

Los resultados obtenidos de la utilización del simulador de Cisco y de los distintos dispositivos empleados hacen pensar que la utilización de elementos IdC en la vida cotidiana va a ser una realidad en un periodo corto de tiempo, dada la capacidad que tienen estos elementos para integrarse en las redes corporativas. Además, unido al hecho de dotar a prácticamente todos los dispositivos de acceso a Internet hace especular que las redes corporativas del futuro estarán formadas por una gran variedad de elementos IdC.

Se hace necesario tomar medidas de seguridad ante esta inmersión de elementos IdC en las redes corporativas, todo un reto para el futuro. Es cierto, que la inclusión de determinados elementos en las redes corporativas facilita enormemente la gestión y el control de las instalaciones, por lo que utilizarlos correctamente supondrá una gran ventaja y un gran ahorro para las empresas del futuro.

Los dispositivos de red Cisco utilizados emplean una línea de comando (CLI) bastante sencilla de utilizar para aquellas personas que estén familiarizadas con la programación de dispositivos de red, ya que es muy similar independientemente del fabricante. Estos dispositivos han tenido un comportamiento muy estable, aunque

limitado, debido fundamentalmente a que los dispositivos ejecutan un sistema operativo básico, por lo que no ofrece todo el potencial de un dispositivo real.

La utilización de la programación *Blockly* usada en los elementos IdC ha permitido modelar comportamientos que no habrían sido posible en el servidor IdC. Indicar que también es posible realizar la programación de las microcontroladoras MCU/SBC mediante los lenguajes de programación Python y JavaScript. Los ejemplos más clásicos de microcontroladoras que podrían utilizarse son Raspberry y Arduino, las cuales permiten su programación utilizando *Blockly*.

La utilización del simulador de Cisco se ha hecho en determinados momentos compleja debido a que el simulador no es capaz de gestionar correctamente tantos elementos conectados y en funcionamiento a la vez, provocando situaciones, en las que es imprescindible reiniciar los conmutadores para un correcto funcionamiento del simulador. Esto es debido fundamentalmente a que, al iniciar el proyecto, todos los dispositivos tratan de obtener una dirección IP válida mientras los dispositivos de red están negociando sus propios enlaces, saturando y provocando efectos no deseados en los distintos dispositivos de red. Una forma de “aliviar” este problema es reducir el número de elementos encendidos a la vez, por lo que se opta por apagar un gran número de equipos informáticos, simulando el funcionamiento normal de una red. En una red corporativa los usuarios no encienden sus ordenadores todos a la vez, si no que este hecho se va haciendo paulatinamente, a medida que los usuarios van llegando a su puesto de trabajo.

Además, se ha encontrado un pequeño fallo en la aplicación en la pestaña de *Conditions* dentro del servidor IdC. Debido a la gran cantidad de reglas definidas en el servidor IdC es necesario desplazarse hacia abajo para poder verlas, manipularlas o crear nuevas. Resulta que la barra de desplazamiento lateral no funciona. Para poder acceder a las últimas reglas definidas hay que editar alguna de las reglas visibles y pulsar cancelar. Al salir de la regla, sí se puede ir cambiando de regla pulsando tabulador, al hacerlo, se va cambiando de regla hasta que se visualizan aquellas reglas que antes no podían ser visualizadas.

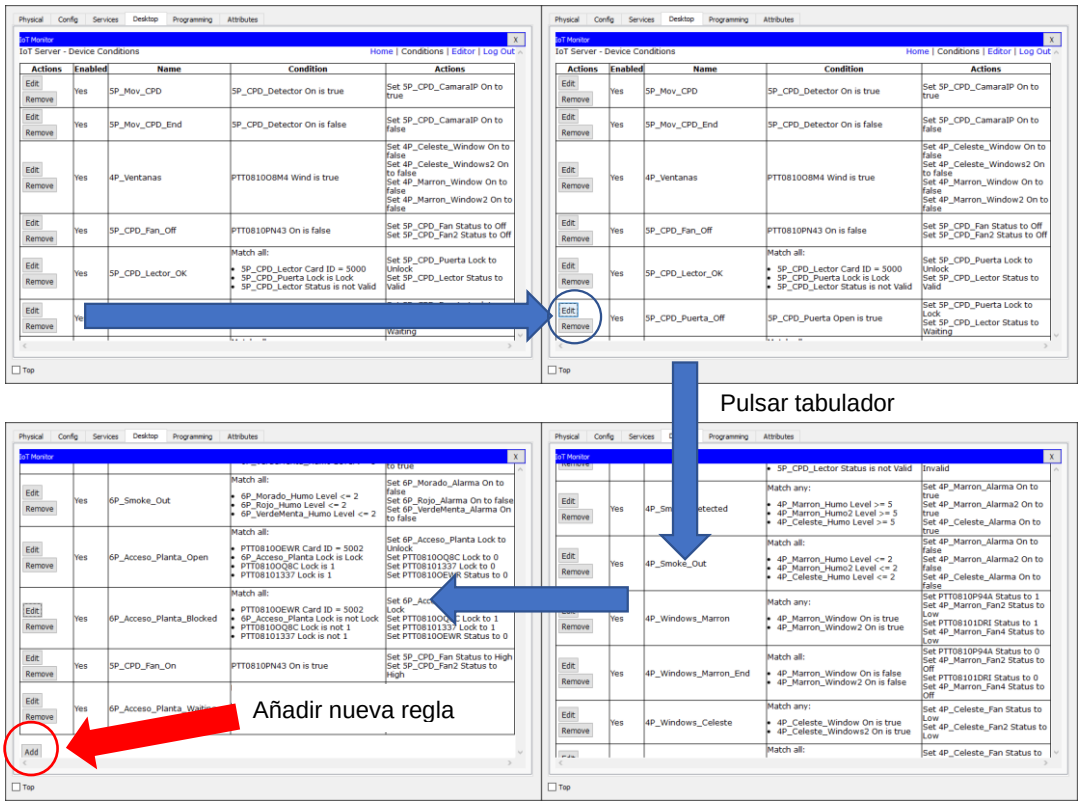


Figura 115. Visualización del resto de reglas y posibilidad de añadir nuevas reglas

Por otra parte, en este proyecto se han modelado algunos de los comportamientos más usuales para una empresa. Como trabajos futuros sería posible modelar otros tipos de empresas, como, por ejemplo, una industria textil, una multinacional con varias sedes, etc. También sería posible la utilización de otros tipos de elementos IdC que no se han utilizado al no tener cabida dentro del alcance de este proyecto.

Otros aspectos posibles de mejora serían la utilización de protocolos seguros para el acceso a los dispositivos de red, como, por ejemplo, Secure Shell (SSH), control de tráfico Multicast, etc.

REFERENCIAS BIBLIOGRÁFICAS

[1] Página oficial de Cisco, sección Command Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.pdf

[2] Cisco LAN Switching Configuration Handbook (Stave McQuerry) 2009.

[3] Listas de Control de Acceso (ACL). Universidad de Alcalá: http://atc2.aut.uah.es/~rosa/LabRC/Prac_5/Listas%20de%20Control%20de%20acceso.pdf

[4] Guía de Cisco para fortalecer los dispositivos Cisco IOS: https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/13608-21.html

[5] Configure InterVLAN Routing on Layer 3 Switches: https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

[6] Libro oficial CCDA 640-864 (Anthony Bruno) 2011.

[7] Internet of Things (IoT): https://www.cisco.com/c/es_es/solutions/internet-of-things/overview.html

[8] Información y casos prácticos de IoT: https://www.cisco.com/c/m/en_us/solutions/internet-of-things/iot-driving-digital.html

[9] Manual del simulador Packet Tracer y ejemplos: http://www.packettracernetwork.com/

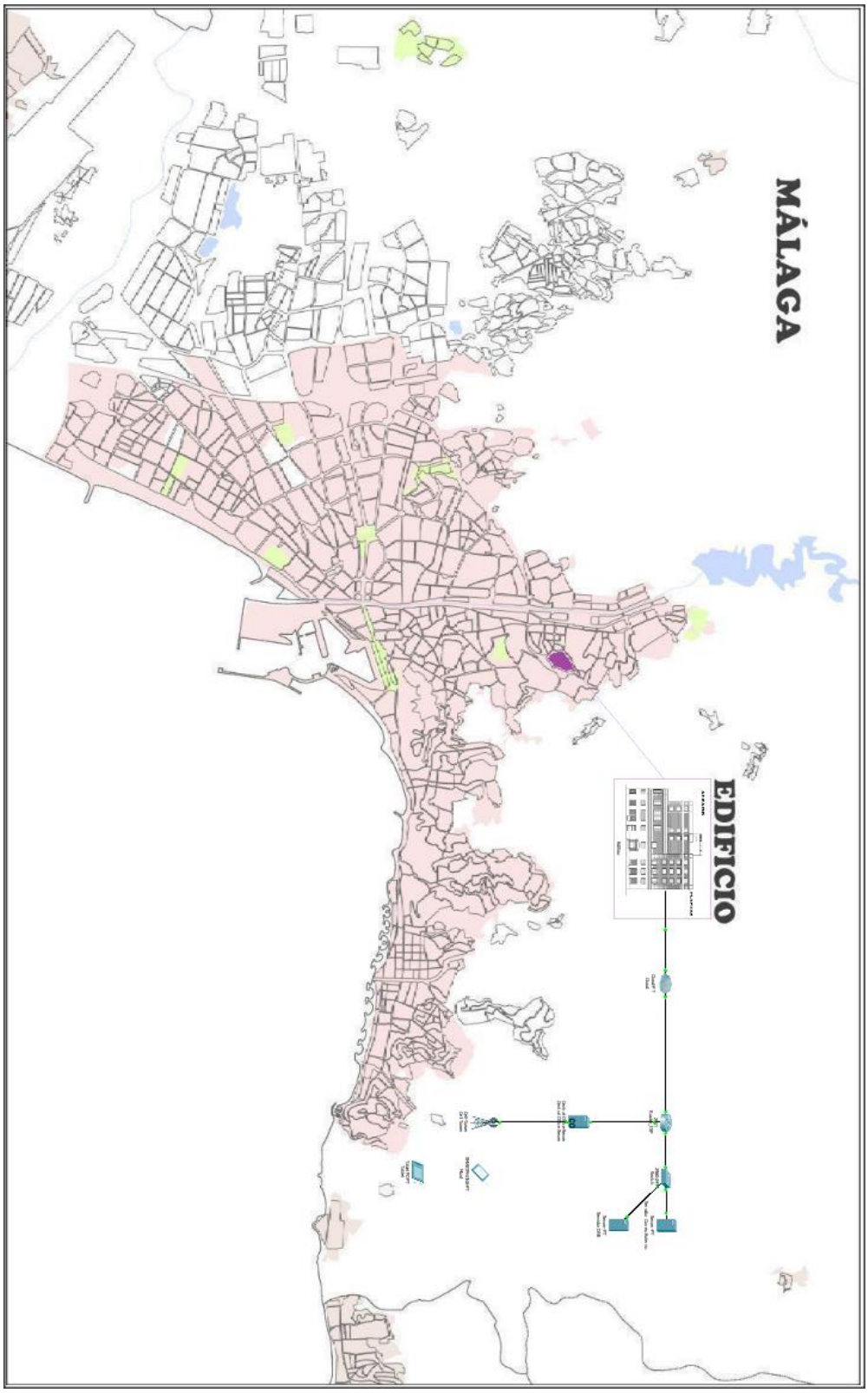
[10] IoT in Packet Tracer 7 – Use Blockly to program IoT devices: https://www.youtube.com/watch?v=pCoQE_gg-xk

[11] Packet Tracer – Connect and Monitor IoT Devices: http://honim.typepad.com/files/6.1.1.2-packet-tracer---connect-and-monitor-iot-devices.pdf

[12] Spanning-Tree mistakes and how to avoid them: https://www.auvik.com/media/blog/spanning-tree-mistakes/

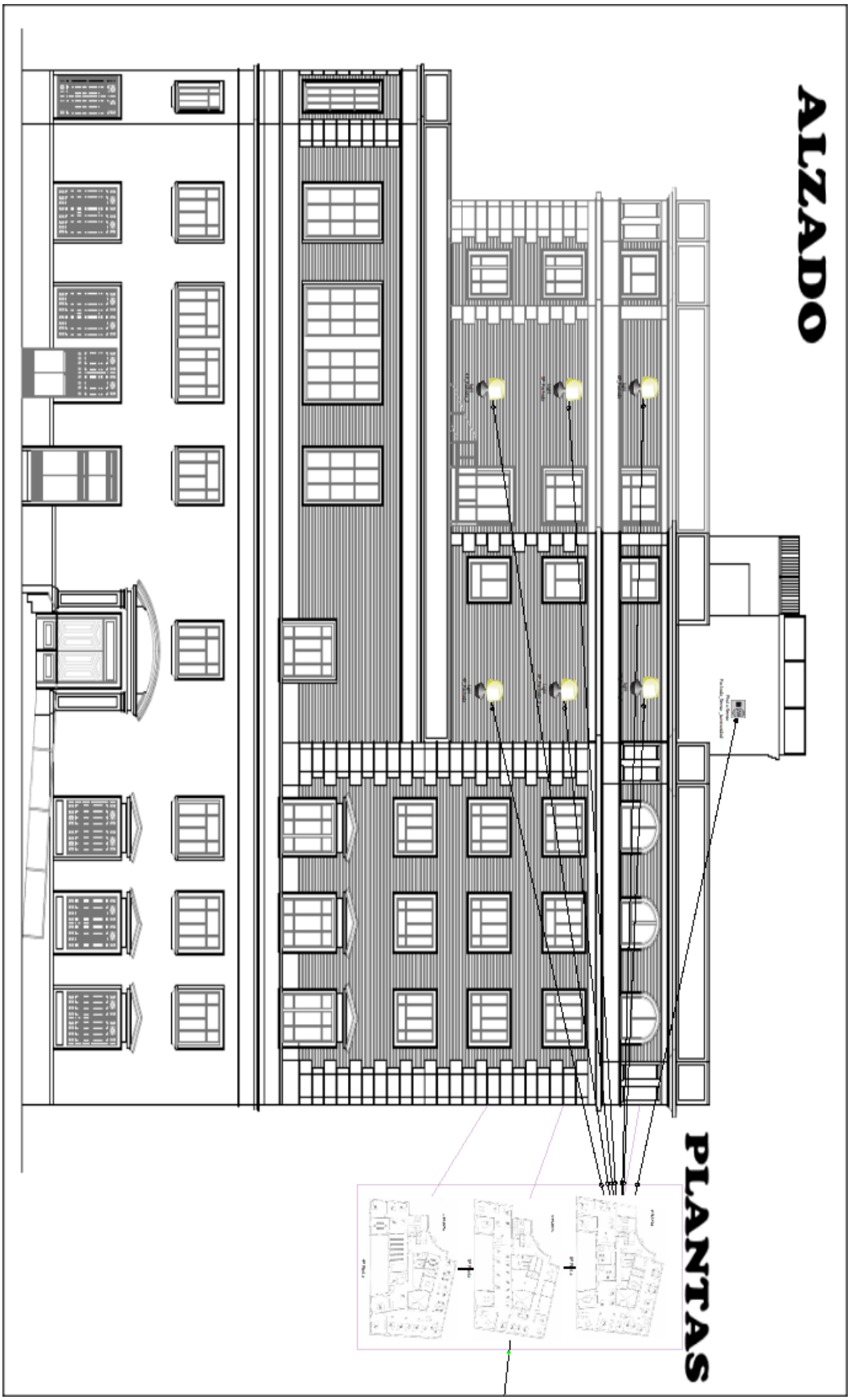
ANEXOS TÉCNICOS

VISUALIZACIÓN FÍSICA (PLANO GLOBAL)



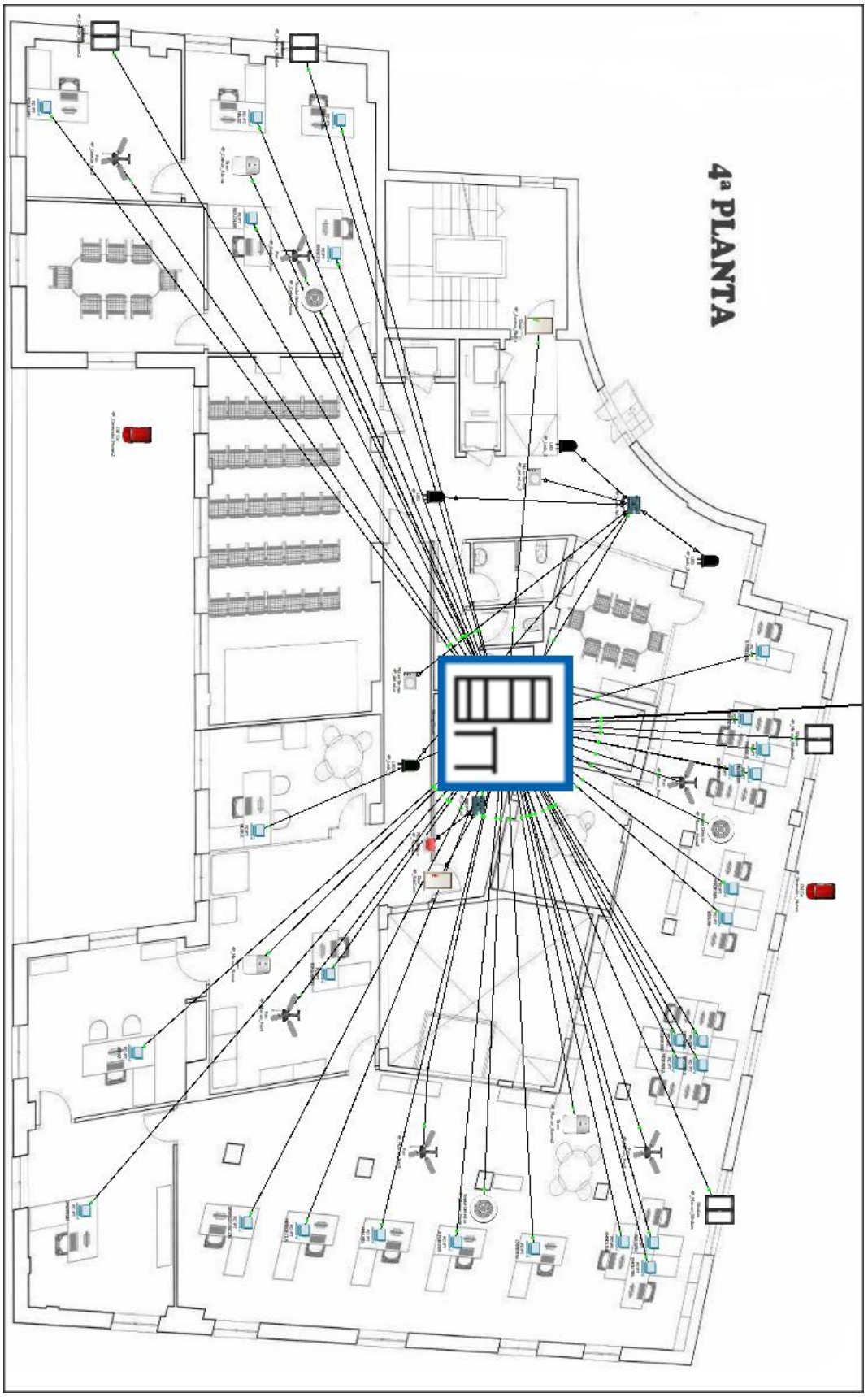
Anexo 1. Plano global

VISUALIZACIÓN FÍSICA (PLANO INTERMEDIO)



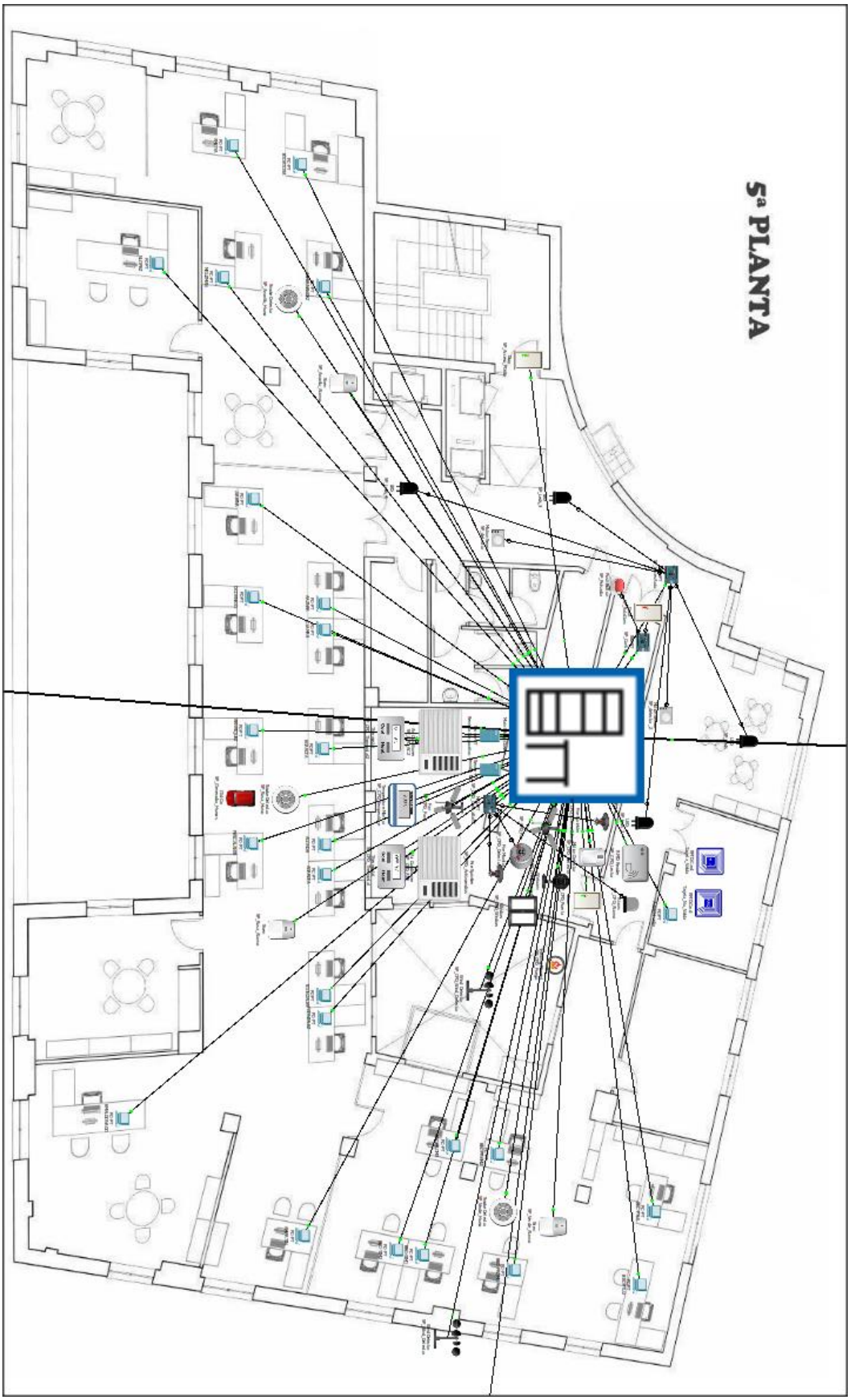
Anexo 2. Plano intermedio

VISUALIZACIÓN FÍSICA (PLANO CORTO 4ª PLANTA)



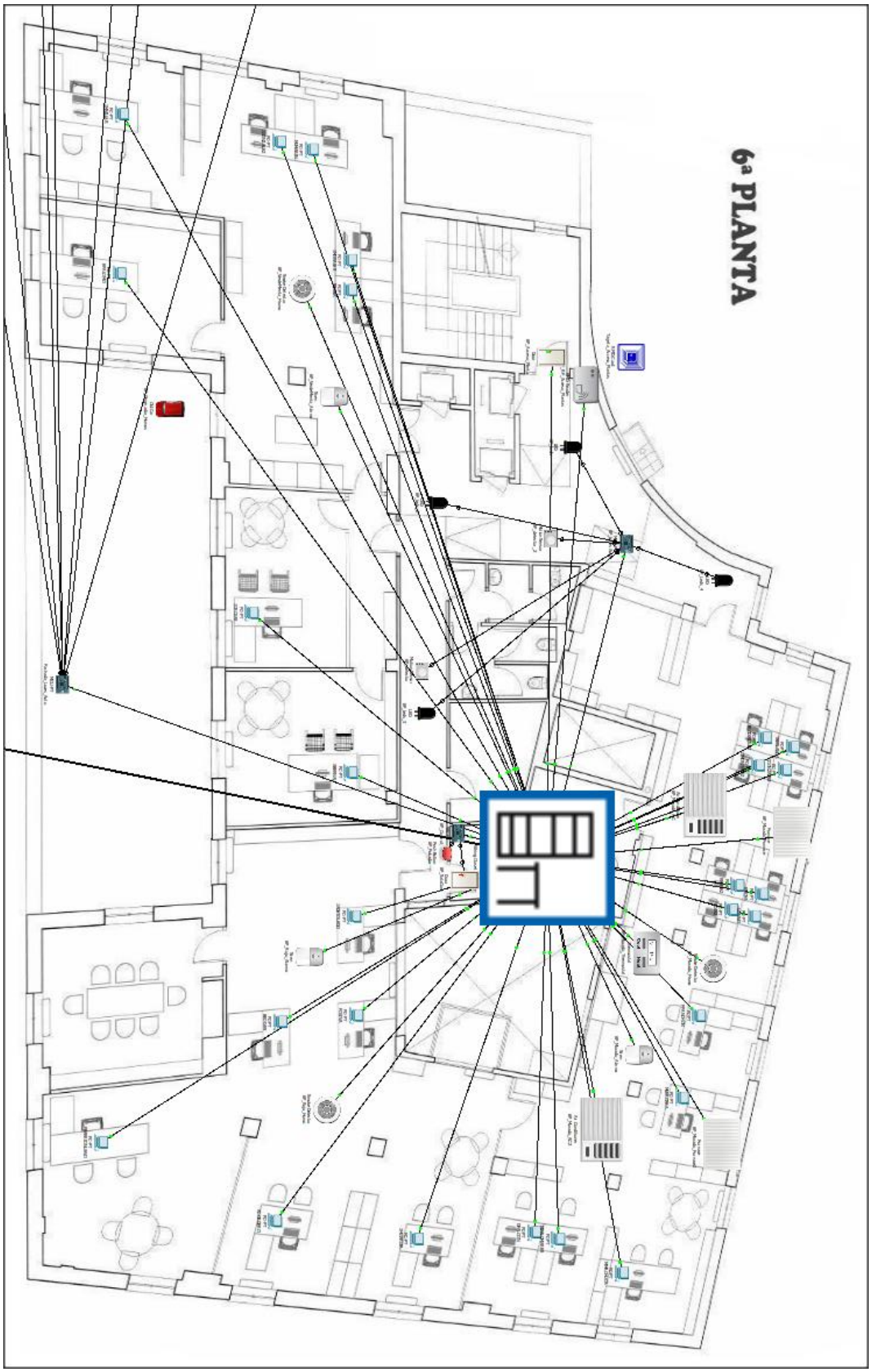
Anexo 3. Plano corto - 4ª planta

VISUALIZACIÓN FÍSICA (PLANO CORTO 5ª PLANTA)



Anexo 4. Plano corto - 5ª planta

VISUALIZACIÓN FÍSICA (PLANO CORTO 6ª PLANTA)



Anexo 5. Plano corto - 6ª planta

VISUALIZACIÓN FÍSICA (PLANO CORTO ARMARIOS RACKS)

Anexo 6. Plano corto - Armarios racks