



INSTITUTO
NEBRIJA

**Formación
Profesional**



ANTONIO DE NEBRIJA
500 AÑOS

o

Trabajo Final Sistemas Informáticos

Propuesto por:

Prof. Carmelo Escribano

Realizado por:

Estudiantes:

David Dobeson

Juan Carlos Guillardí

Aran Gonzalez

Alejandro García

Trabajo Final Sistemas Informáticos

20/05/25 – 10/06/25



ANTONIO DE NEBRIJA
500 AÑOS



INSTITUTO
NEBRIJA

**Formación
Profesional**



CO

Introducción y contexto

En las comunidades rurales de Honduras, la falta de acceso a tecnología educativa representa una barrera significativa para el desarrollo académico. La organización **Nebrija Tech**, especializada en proyectos educativos tecnológicos, nos ha encargado el diseño e implementación de un aula TIC completamente equipada para una escuela en estas condiciones. El proyecto contempla la creación de una infraestructura de red funcional y segura, utilizando una **topología en estrella** como solución óptima. Esta configuración centralizada, donde todos los dispositivos (computadoras, impresoras) se conectan a un switch principal, ofrece ventajas clave: simplicidad de instalación, facilidad de mantenimiento y aislamiento de fallos (un problema en un equipo no afecta a los demás).

Para garantizar el éxito, emplearemos metodologías ágiles (Scrum para la gestión del proyecto y Kanban para el seguimiento de tareas), y documentaremos todo el proceso en GitHub. La simulación previa con Cisco Packet Tracer nos permitirá validar el diseño antes de la implementación física. Este proyecto no solo dotará de herramientas tecnológicas a la escuela, sino que sentará las bases para un programa educativo sostenible que pueda replicarse en otras comunidades, contribuyendo así a reducir la brecha digital en la región. El enfoque en una topología simple pero robusta asegurará que los recursos limitados se aprovechen al máximo, mientras que la capacitación garantizará que la tecnología sea realmente útil para la comunidad educativa.

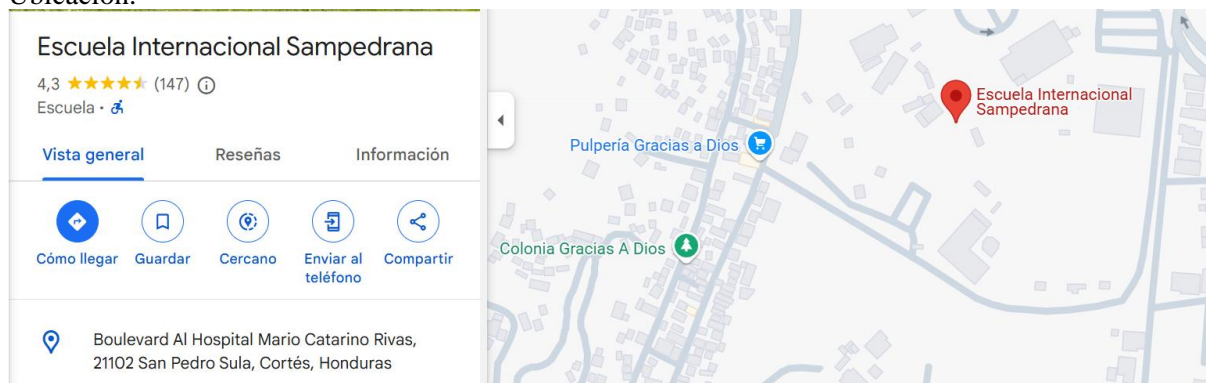
Análisis de necesidades

Educación: primaria y secundaria (Educación básica y común, cursos: I-III ciclo; ciclo común, cursos: 10° y 11°)

Escuela: Escuela Internacional Sampedrana

Asistencia: 80-95% (500-700).

Ubicación:



Modalidad: Educación bilingüe (inglés-español) con una orientación internacional. Su modalidad educativa abarca desde el nivel preescolar hasta el 12.º grado, siguiendo un currículo estadounidense que prepara a los estudiantes para ingresar a universidades en Honduras, Estados Unidos y otros países.

Servicios: Educativos y extracurriculares diseñados para proporcionar una formación integral a sus estudiantes.



Educación bilingüe, Currículo Internacional, Acreditaciones, Deportes, Artes y Cultura, Clubes Académicos, Orientación y Consejería.

Características de la Escuela

Infraestructura - Equipos:

- **35 computadoras de escritorio**, distribuidas en dos laboratorios tecnológicos para cubrir la demanda de una matrícula alta en turnos diferenciados.
- **2 servidor local** con capacidad ampliada para almacenamiento compartido, gestión de usuarios y servicios de red educativa.
- **2 impresoras multifunción** (impresión, escaneo y copia), ubicadas en sectores administrativos y docentes.
- **2 router principal(1 por clase), 3 switches de 24 puertos y 2 puntos de acceso WiFi**, distribuidos estratégicamente para garantizar cobertura completa en laboratorios, áreas administrativas y zonas comunes.
- Estaciones conectadas mediante **cableado estructurado CAT6**, con canalizaciones seguras y soporte para futuras ampliaciones.
- Implementación de **VLANs** para segmentar el tráfico entre estudiantes, docentes, personal administrativo y servicios.

Software:

- Sistema operativo **Linux Zorin OS Education** en todas las máquinas por su compatibilidad, estabilidad y enfoque educativo.
- **LibreOffice** como suite ofimática gratuita y funcional.
- Programas educativos como **GCompris, TuxMath, TuxPaint**, entre otros recursos adaptados a niveles básicos y medios.
- Sistema **UTM (Unified Threat Management)** para control de acceso a contenidos, firewall y filtrado de navegación.
- **Antivirus ClamAV** instalado en todos los equipos cliente para protección contra software malicioso.

Organización Operativa

- **Dos aulas tecnológicas** de aproximadamente **50 m² cada una**, con buena ventilación, iluminación natural y artificial.
- **Mobiliario ergonómico**: 16 estaciones dobles por aula (capacidad total para 30 estudiantes simultáneamente), distribuidas en turnos.
- **Área de proyección y capacitación** equipada con **pizarra digital o proyector**, altavoces y mesa para el docente.
- **Horarios rotativos** para asegurar que todos los grados tengan acceso semanal a los laboratorios, desde primero hasta 11º grado.

Financiación y Sostenibilidad

- Adquisición de **equipos reacondicionados** de calidad verificada para reducir costos sin sacrificar funcionalidad.
- Uso exclusivo de **software libre** para evitar gastos en licencias y fomentar la autonomía tecnológica.
- Impulso de una **red de participación comunitaria** (padres, docentes, egresados) en labores de mantenimiento, vigilancia y gestión de recursos



Presupuesto General del Proyecto Tecnológico Educativo

Para la implementación de una infraestructura tecnológica completa en una escuela rural con entre 500 y 700 estudiantes, se estima un presupuesto total de aproximadamente **\$32,640**

1. Equipos de Cómputo

Se adquirirán **35 computadoras de escritorio reacondicionadas** de grado empresarial. Cada equipo tiene un costo aproximado de **\$180**, sumando un total de **\$6.300**. Además, se incluirán **35 monitores reacondicionados** con un valor de **\$50** cada uno, lo que representa un total de **\$1,750**.

Se instalará dos **servidores locales**, con un costo estimado de **\$700 lo que supondrá un coste de 1400\$**. También se integrarán dos **impresoras multifunción**, a un precio de **\$250** cada una, para un total de **\$500**.

2. Red y Conectividad

La infraestructura de red incluirá **un router empresarial** valorado en **\$120**, tres switches de 24 puertos a **\$100** cada uno (**\$300** en total), y dos puntos de acceso **WiFi**, cada uno con un costo aproximado de **\$90**, sumando **\$180**.

3. Mobiliario y Acondicionamiento del Espacio

Se equiparán dos aulas tecnológicas con **16 estaciones dobles con sillas ergonómicas**, cada una valorada en **\$120**, lo que representa **\$1,920** en total. Además, el **acondicionamiento de las aulas** tendrá un costo estimado de **\$3,000** (unos **\$1,500 por aula**).

Cada aula contará con un **proyector o pizarra digital**, incluyendo equipo de audio básico, con un presupuesto de **\$400 por unidad**, para un total de **\$800**.

4. Software y Seguridad

Se optará por el uso exclusivo de **software libre**, lo que permite eliminar el costo de licencias. Las computadoras funcionarán con **Zorin OS Education**, acompañado de **LibreOffice** y software educativo como **GCompris**, **TuxMath** y **TuxPaint**. Estos recursos no tendrán costo.

5. Capacitación y Mantenimiento

La capacitación de los **6 docentes** en tres niveles tendrá un costo de **\$100 por docente**, sumando **\$600**. Se invertirán **\$500** en la impresión de manuales y materiales pedagógicos adaptados al contexto rural.

El mantenimiento preventivo anual de los equipos y la red se estima en **\$800**, y se destinarán **\$300** para el soporte técnico comunitario inicial, que incluye formación básica de personal de la comunidad para apoyar en tareas de revisión y vigilancia del aula tecnológica.



Diseño de red (lógico y físico)

Hardware

Equipos Individuales

Opción Recomendada: Ordenadores de Sobremesa Reacondicionados HP EliteDesk

- **Procesador:** Intel Core i5 de 4ª generación (mínimo), modelo común en torres EliteDesk.
- **RAM:** 8 GB DDR3 o DDR4 (según la placa base).
- **Almacenamiento:** SSD de 256 GB para asegurar velocidad en el arranque y fluidez general.
- **Pantalla:** No incluida en el chasis, se conecta a monitor externo de al menos 19" Full HD.
- **Puertos:** USB 2.0 y 3.0 frontales, VGA/DisplayPort/HDMI traseros (según versión).
- **Ventajas:** Fácil ampliación (más RAM, discos), ventilación superior, mayor vida útil que portátiles bajo uso fijo.

Justificación:

La elección de torres HP EliteDesk reacondicionadas ofrece una solución económica, fiable y duradera. Son ideales para entornos educativos con puestos fijos, permitiendo mantenimiento sencillo, mejor disipación térmica, y posibilidad de expansión en el futuro. Su rendimiento es suficiente para tareas ofimáticas, navegación, aprendizaje digital y software educativo.

Software:

Sistema Operativo Recomendado: Chrome OS Flex:

Ventajas: Ligero, seguro, actualizaciones automáticas, ideal para hardware reacondicionado.

Justificación: Chrome OS Flex optimiza el rendimiento en equipos con recursos limitados y simplifica la gestión del software

Subnetting y direccionamiento

Hemos usado una red diferente para cada clase. Nos hemos decidido por una red de clase C con direcciones privadas, ya que no necesitamos acceso desde fuera de la red local y así evitamos posibles problemas de seguridad.

Para organizar mejor las clases, hemos hecho subnetting. En concreto:

- Para la clase A hemos usado la red **192.168.0.0**
- Para la clase B hemos usado la red **192.168.1.0**

Configuración de dispositivos (routers, switches, puntos de acceso)

Para conectar las dos clases hemos utilizado **enrutamiento RIP versión 2**, usando una red de clase A (**10.0.0.0**) como red común entre los routers.



Cada clase cuenta con un **punto de acceso (Access Point)** para que cualquier persona pueda conectarse a la red vía Wi-Fi, además de un **switch** para conectar los dispositivos por cable.

En cuanto a la configuración de red:

- **Router de la clase A:** 192.168.0.1
- **Router de la clase B:** 192.168.1.1
- **Servidor de la clase A:** 192.168.0.2
- **Servidor de la clase B:** 192.168.1.2

Ambos servidores están configurados con **protocolo DHCP**, lo que permite asignar direcciones IP automáticamente a los dispositivos que se conectan a la red.

Correspondencia con el modelo OSI

Para entender cómo se estructura y funciona nuestra red TIC, es fundamental relacionar los componentes del sistema con el **modelo OSI**, que divide la comunicación de red en siete capas. A continuación, se detalla cómo cada capa se corresponde con elementos concretos del proyecto:

Capa 1 – Capa física

- **Ejemplos en el proyecto:** cables de red CAT6, switches, routers, puntos de acceso WiFi, tarjetas de red.
- **Función:** Transmisión física de datos a través del medio (cableado o señales inalámbricas).
- **Aplicación:** Se utilizaron canalizaciones seguras para el cableado estructurado, garantizando una conexión estable y preparada para futuras ampliaciones.

Capa 2 – Enlace de datos

- **Ejemplos:** direcciones MAC, switches gestionables, configuración de VLANs.
- **Función:** Control del acceso al medio y detección de errores en la transmisión de tramas.
- **Aplicación:** Se configuraron **VLANs** para separar el tráfico entre estudiantes, docentes y personal administrativo, mejorando el rendimiento y la seguridad.

Capa 3 – Red

- **Ejemplos:** routers, direccionamiento IP, protocolo RIP v2.
- **Función:** Encaminamiento de paquetes entre redes y asignación de direcciones IP.



- **Aplicación:** Cada aula tiene su propia subred (192.168.0.0 y 192.168.1.0), y se utiliza un router por aula con RIP v2 para la comunicación entre ellas a través de la red 10.0.0.0.

Capa 4 – Transporte

- **Ejemplos:** protocolos TCP y UDP.
- **Función:** Establecimiento de conexiones fiables o no fiables entre dispositivos.
- **Aplicación:** Aplicaciones como navegadores web o servicios de impresión hacen uso de TCP para garantizar una comunicación confiable entre cliente y servidor dentro del aula TIC.

Capa 5 – Sesión

- **Ejemplos:** control de sesiones en aplicaciones, acceso remoto o compartición de archivos.
- **Función:** Mantener y gestionar sesiones entre aplicaciones.
- **Aplicación:** Las sesiones entre el servidor local y los clientes permiten compartir recursos y gestionar el acceso a contenidos educativos centralizados.

Capa 6 – Presentación

- **Ejemplos:** cifrado de datos, formato de archivos.
- **Función:** Traducción, compresión y encriptación de datos.
- **Aplicación:** Se incluye cifrado de discos y uso de protocolos seguros (HTTPS, SSH) en configuraciones para proteger la información intercambiada en la red.

Capa 7 – Aplicación

- **Ejemplos:** Zorin OS, LibreOffice, GCompris, antivirus ClamAV, sistema UTM.
- **Función:** Proporcionar servicios y aplicaciones directamente al usuario final.
- **Aplicación:** Se han instalado sistemas operativos educativos, software libre y herramientas de seguridad (como firewall UTM y antivirus), accesibles desde las estaciones de trabajo del aula TIC.



1. Equipos informáticos y servidor

- **Riesgo:** Uso de sistemas operativos desactualizados o sin parches de seguridad.
- **Riesgo:** Contraseñas débiles o predeterminadas.
- **Riesgo:** Acceso físico no restringido al servidor.

2. Dispositivos de red (router, switches, APs)

- **Riesgo:** Interfaces de administración web sin cifrado (HTTP).
- **Riesgo:** Configuraciones predeterminadas (usuario/contraseña, SSID, etc.).
- **Riesgo:** APs abiertos o mal configurados.

3. VLANs y segmentación

- **Riesgo:** Puertos de switch mal configurados que permiten saltos entre VLANs (VLAN hopping).
- **Riesgo:** Sin reglas de firewall internas entre subredes sensibles.

4. Software y sistemas

- **Riesgo:** Instalación de software no autorizado (por alumnos o personal).
- **Riesgo:** Falta de control sobre dispositivos USB y medios extraíbles.
- **Riesgo:** No cifrado de datos en el servidor local.

5. Seguridad física y operativa

- **Riesgo:** Acceso no autorizado al aula TIC.
- **Riesgo:** Equipos vulnerables a picos de corriente o cortes de energía.
- **Riesgo:** Ausencia de monitoreo o registros de acceso.

6. Ciberhigiene y usuarios

- **Riesgo:** Usuarios poco capacitados pueden caer en phishing o malware.
- **Riesgo:** Ausencia de políticas de contraseñas o rotación de credenciales.

Posibles vulnerabilidades del Blue Team

1. Hardening de sistemas

- Instalar y mantener actualizados todos los sistemas operativos.
- Implementar políticas de contraseñas seguras y rotación periódica.
- Cifrado de discos en el servidor y estaciones docentes.

2. Seguridad en red

- Cambiar contraseñas predeterminadas de todos los dispositivos.



- Deshabilitar administración remota en router/switch si no se usa.
- Usar HTTPS o SSH para configuraciones.
- Aislar VLANs con reglas de firewall entre segmentos críticos (servidor ↔ alumnos).

3. Seguridad perimetral y endpoint

- Configurar el **firewall UTM** con reglas claras: whitelist de servicios, geoblocking si es necesario.
- Instalar **antivirus de código abierto** en todos los endpoints.
- Filtrado de contenidos web y protección contra DNS maliciosos.

4. Políticas y concienciación

- Implementar **protocolos de uso responsable** (como AUP: Acceptable Use Policy).
- Capacitar a docentes y alumnos en buenas prácticas de seguridad digital.
- Prohibir instalación de software no autorizado y bloquear ejecución desde USB.

5. Seguridad física

- Asegurar el aula con cerraduras, cámaras si es viable, y control de acceso.
- Uso de regletas con protección contra sobretensiones y UPS para el servidor.

6. Monitoreo y mantenimiento

- Mantener logs de actividad (acceso al servidor, cambios de configuración).
- Revisión trimestral de configuraciones y actualizaciones.
- Backups automatizados y pruebas periódicas de recuperación.

Mantenimiento y actualizaciones

Para asegurar la continuidad y buen funcionamiento del aula TIC, se establece un plan de mantenimiento estructurado, que incluye:

- **Mantenimiento preventivo trimestral** de todos los equipos informáticos, switches, routers y puntos de acceso.
- **Actualización periódica de software:** se mantendrán actualizados los sistemas operativos, antivirus y firewall, empleando siempre versiones estables de software libre.
- **Gestión comunitaria:** miembros de la comunidad capacitados (padres, docentes y egresados) colaborarán en tareas básicas de revisión, soporte técnico y vigilancia del aula.
- **Respaldo y recuperación:** implementación de copias de seguridad automatizadas en los servidores, con pruebas periódicas de restauración.
- **Monitoreo de seguridad:** revisión regular de logs de acceso y configuración, así como control del uso de dispositivos externos (USB, software no autorizado).



- **Formación continua:** se planificarán sesiones anuales de capacitación para docentes sobre buenas prácticas digitales y seguridad informática.

Gestión del proyecto (Scrum, Kanban)

Scrum Master:

Aran González

Repositorio GitHub

Enlace directo:

<https://github.com/D-0BE/trabajoFinalSistemas.git>

Conclusiones

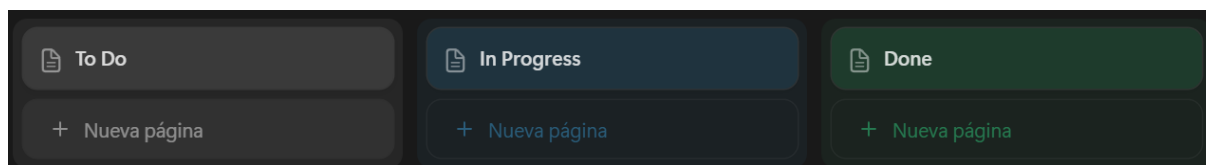
La creación de un aula TIC en una comunidad rural de Honduras ha sido mucho más que un simple proyecto tecnológico; ha significado un paso importante hacia un acceso más justo a la educación digital. En lugares donde la tecnología suele ser un lujo, este proyecto ha brindado una solución real, funcional y pensada para durar, utilizando recursos reacondicionados y software libre como pilares clave para hacerlo accesible y sostenible.

A lo largo del proceso, el uso de metodologías ágiles como Scrum y Kanban nos ayudó a organizarnos mejor como equipo, dividir el trabajo de forma clara y avanzar paso a paso hasta lograr un resultado concreto y útil. Esta manera de trabajar nos permitió aprovechar bien el tiempo y los recursos, adaptándonos a los desafíos que surgieron en el camino.

El diseño en topología de estrella que elegimos para la red no solo facilita la instalación y el mantenimiento, sino que también garantiza que si algo falla, no afecte al resto del sistema. Además, con las medidas de seguridad implementadas y la segmentación de la red por VLANs, se ha creado un entorno seguro para que estudiantes, profesores y personal puedan usar la tecnología sin riesgos.

En definitiva, este proyecto no solo ha dotado a la escuela de herramientas modernas, sino que ha sembrado las bases para un cambio educativo duradero, donde la comunidad también es parte activa del proceso. Es un modelo que puede replicarse y que demuestra que con planificación, compromiso y trabajo en equipo, es posible hacer una verdadera diferencia.

Anexos (capturas, simulaciones)



Esquema de modelo OSI y dispositivos a incluir en cada capa (que serán analizados en la memoria)

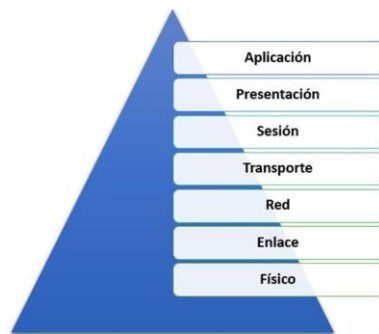
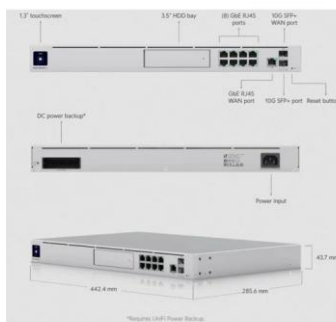


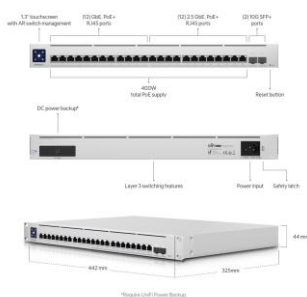
Foto routers, servidores, switches, impresoras y ordenadores que se podrían usar,



ROUTER: UBIQUITI UNIFI DREAM MACHINE PRO (UDM PRO)



SERVIDOR: DELL POWEREDGE T350



SWITCH: UBIQUITI UNIFI SWITCH ENTERPRISE 24 POE



IMPRESORA: HP LASERJET ENTERPRISE M507DN

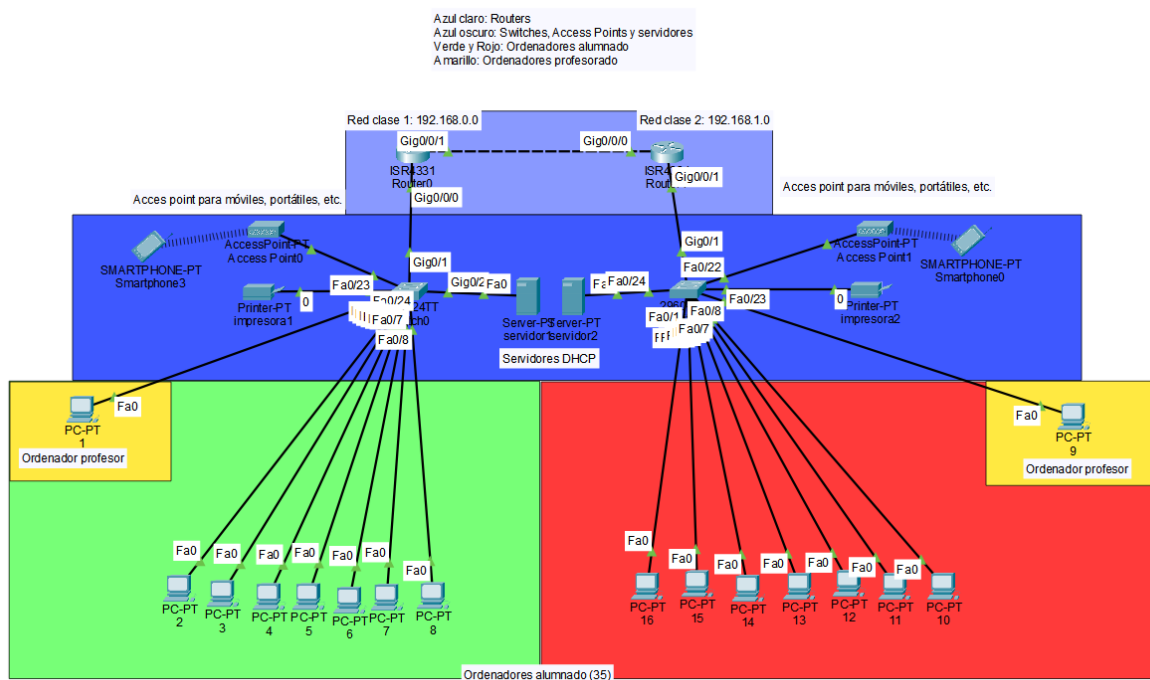


ORDENADORES: HP ELITE 800 G1



MONITOR: LCD HP COMPAQ LA2306X 23" 1920X1080 LED

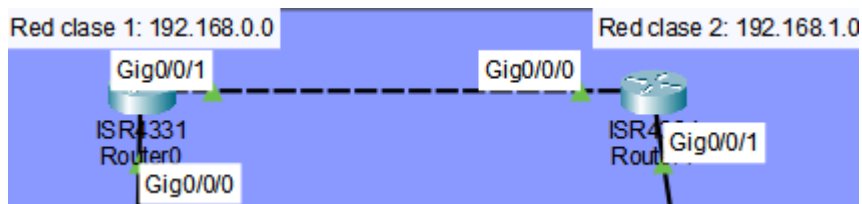
Vista general de la red:



Routers

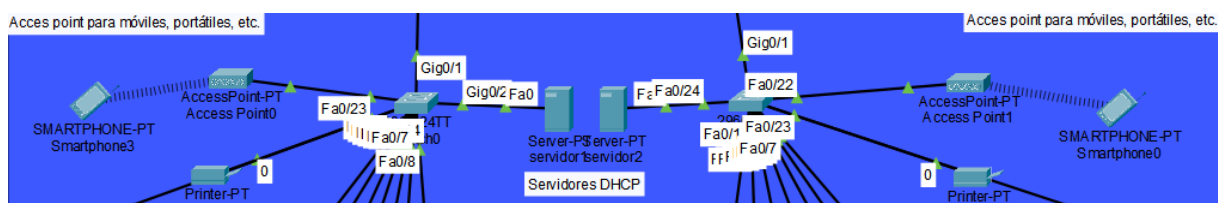
Configuración:

Redes: Entre los routers tienen una conexión tipo A (10.0.0.0), cada clase, en cambio, tiene una red de clase C (192.168.0.0 y 192.168.1.0)

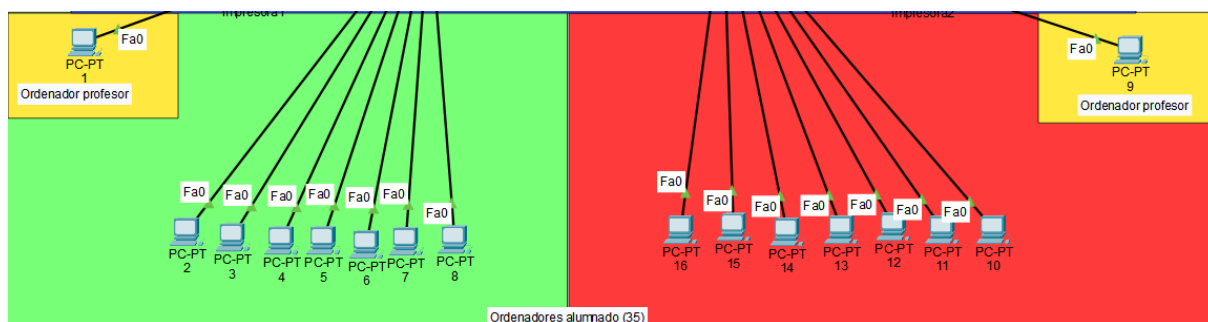


Dispositivos de conectividad de red (Servidores (DHCP), switches y access points).

La impresora y el móvil son dispositivos que se conectan a la red. La impresora se conecta directamente por el switch (la IP se la da el servidor mediante DHCP), y los dispositivos inalámbricos se conectan automáticamente a través del access point



Ordenadores del alumnado y los profesores



Protocolo RIP Routing para que las dos redes se puedan comunicar entre si.

RIP Routing (v2)

Network	
	Add
Network Address	
10.0.0.0	
192.168.0.0	
192.168.1.0	

Configuración DHCP del servidor que da ip dinámicas a los dispositivos

DHCP

Interface	FastEthernet0			Service	<input checked="" type="radio"/> On <input type="radio"/> Off		
Pool Name	clase1						
Default Gateway	192.168.0.1						
DNS Server	192.168.0.2						
Start IP Address :	192	168	0	0			
Subnet Mask:	255	255	255	128			
Maximum Number of Users :	128						
TFTP Server:	0.0.0.0						
WLC Address:	0.0.0.0						

Add
Save
Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.0.1	192.168.0.2	192.168.0.0	255.255.2...	128	0.0.0.0	0.0.0.0
clase1	192.168.0.1	192.168.0.2	192.168.0.0	255.255.2...	128	0.0.0.0	0.0.0.0

Submascara de red personalizada para 126 dispositivos.

1

Physical
Config
Desktop
Programming
Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP

☐ Static

IPv4 Address 192.168.0.5

Subnet Mask 255.255.255.128

Default Gateway 192.168.0.1

DNS Server 192.168.0.2

Mejoras propuestas por el cliente:

Se pide: Una nueva clase con 15 equipos aprox, firewall para cada equipo (incluimos los servidores) y coste del firewall y sistema de actualización.

Seguridad:

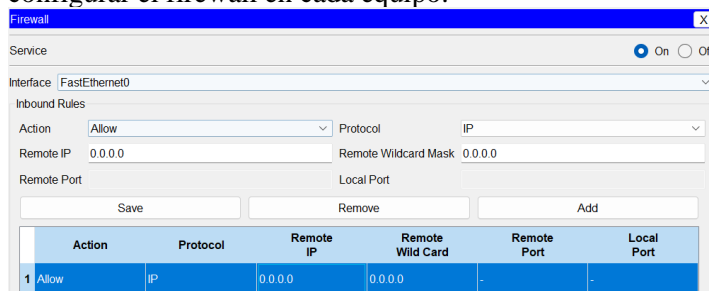
Para Endpoints (Ordenadores y Servidores):

- **Software Propuesto: Sophos Intercept X Advanced with XDR**
 - ¿Por qué Sophos? Ofrece una protección multicapa que va más allá de la detección de firmas, incluyendo prevención de exploits, protección contra ransomware (CryptoGuard), análisis de comportamiento (Malware-Free), y capacidades de Detección y Respuesta Extendida (XDR) para una visibilidad profunda y una respuesta automatizada a amenazas. Es gestionable centralmente, lo que simplifica su despliegue y mantenimiento en múltiples equipos.
 - Coste Estimado: El coste varía significativamente según el número de licencias y el tipo de suscripción. Para una pyme, el coste por usuario/año podría oscilar entre 30-60 EUR, con descuentos por volumen. Para 100 usuarios, esto podría ser aproximadamente 3.000 - 6.000 EUR/año. (Estos son precios de referencia y pueden variar).

Para la Red Perimetral (Cortafuegos de Red):

- **Software/Hardware Propuesto: FortiGate (Fortinet) o Cisco Firepower**
 - ¿Por qué un cortafuegos de nueva generación (NGFW)? Estos dispositivos no solo filtran el tráfico basado en puertos y protocolos, sino que también ofrecen inspección profunda de paquetes (DPI), prevención de intrusiones (IPS), filtrado web, control de aplicaciones y VPN. Son cruciales para proteger la red de amenazas externas y controlar el tráfico interno.
 - Coste Estimado: Un dispositivo NGFW con sus licencias de seguridad anuales puede tener un coste inicial de 1.500 - 5.000 EUR para un modelo adecuado para una pyme, más un coste de suscripción anual de 500 - 2.000 EUR para las actualizaciones de inteligencia de amenazas y funcionalidades de seguridad. Los modelos de gama alta para grandes empresas serían significativamente más caros.

Para la limitación de velocidad de conexión, es suficiente la del propio cable (Fast ethernet) y para configurar el firewall en cada equipo:



	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	0.0.0.0	0.0.0.0	-	-

Se necesita activar y luego seleccionamos Allow (permitir) para permitir el tráfico y el protocolo de IP. Por último, ponemos 0.0.0.0 en remote IP y Mask para cualquier IP y máscara de red.

Así queda finalmente la red con los nuevos 15 equipos.

