

**Caso Final Integrador**

**Álvaro Martín Romero**

**Índice**

**1.**[**Diseño y Modelado de la Arquitectura de Comunicación**](#_1._Diseño_y)

[**1.1. Análisis de modelos**](#_1.Análisis_de_modelos)

**1.2.**[**Integración de los Modelos OSI y TCP/IP en los Servicios Municipales del Ayuntamiento de Coslada**](#_Integración_de_los)

**1.3.**[**Adaptaciones al diseño para Coslada (resumen técnico)**](#_Adaptaciones_al_diseño)

[**2. Capa Física – Cálculos y Selección de Tecnologías**](#_2._Capa_Física)

**2.1.**[**Cálculo de la Capacidad de los Enlaces:**](#_1._Cálculo_de)

**2.**[**2.Selección de Técnicas de Modulación**](#_2.Selección_de_Técnicas)

**2.**[**3.Evaluación de la Eficiencia del Encapsulamiento**](#_3.Evaluación_de_la)

**2.**[**4.Plano de cobertura**](#_4.Plano_de_cobertura)

**2.**[**5.Cableado estructurado**](#_5.Cableado_estructurado)

[**3.Capa de Red – Direccionamiento, Subneteo y Enrutamiento**](#_3.Capa_de_Red)

**3.**[**1.Diseño del Esquema de Direccionamiento IP**](#_1.Diseño_del_Esquema)

**3.**[**2.Enrutamiento y Rutas Óptimas**](#_2._Enrutamiento_y)

[**4.Capa de Transporte – Selección de Protocolos y Cálculo del Tamaño de Ventana**](#_4._Capa_de)

[**4.1. Selección de Protocolos de Transporte**](#_4.1Selección_de_Protocolos)

[**4.2. Cálculo del Tamaño de Ventana Óptima en TCP**](#_4.2Cálculo_del_Tamaño)

[**6. Seguridad – Estrategias y Configuración**](#_6._Seguridad_–)

[**6.1. Políticas y Medidas de Seguridad**](#_6.1._Políticas_y)

[**6.2. Cifrado y Autenticación**](#_6.2Cifrado_y_Autenticación)

# **Diseño y Modelado de la Arquitectura de Comunicación**

## 1.Análisis de modelos

**Modelo OSI (Open Systems Interconnection) – 7 Capas**

| **Capa** | **Nombre** | **Función principal en la ciudad inteligente** |
| --- | --- | --- |
| 7 | Aplicación | Interfaces con el usuario: portales web, apps ciudadanas, CCTV, servicios en la nube. |
| 6 | Presentación | Cifrado/descifrado, compresión: HTTPS, streaming de video, datos IoT en JSON/XML. |
| 5 | Sesión | Establece/mantiene sesiones: conexiones a portales, transmisiones de emergencia. |
| 4 | Transporte | Control de flujo y errores: TCP (fiabilidad) y UDP (baja latencia) para video/IoT. |
| 3 | Red | Direccionamiento y enrutamiento: IPv4/IPv6, OSPF, EIGRP, RIPng. |
| 2 | Enlace de datos | Transmisión fiable entre nodos: Ethernet, Wi-Fi, VLANs, STP, seguridad MAC. |
| 1 | Física | Medio de transmisión: fibra óptica, cableado UTP, antenas Wi-Fi, LoRa, 5G. |

**Modelo TCP/IP – 4 Capas**

| **Capa TCP/IP** | **Equivalente OSI** | **Aplicación en la ciudad inteligente** |
| --- | --- | --- |
| Aplicación | OSI 5–7 | Portales web, CCTV, VoIP, APIs RESTful para sensores IoT. |
| Transporte | OSI 4 | TCP (datos críticos), UDP (telemetría, video en tiempo real). |
| Internet | OSI 3 | IPv6, OSPFv3, túneles GRE, IPsec, direccionamiento lógico. |
| Acceso a red | OSI 1–2 | Ethernet, Wi-Fi 6, LoRaWAN, VLANs, protocolos 802.11ac/ax, switches, enlaces físicos. |

**Aplicación al proyecto de ciudad inteligente**

| **Servicio** | **Capas críticas involucradas** |
| --- | --- |
| Servicios gubernamentales | Aplicación (correo, portales), Red (enrutamiento), Transporte (TCP). |
| Seguridad pública | Transporte (UDP para video), Red (QoS + redundancia), Enlace (Wi-Fi en puntos). |
| Transporte y sensores IoT | Aplicación (MQTT/CoAP), Transporte (UDP), Enlace (LoRa/5G), Física (antenas). |
| Streaming y multimedia | Aplicación (HTTP/RTSP), Transporte (UDP), Red (multicast, QoS). |
| Seguridad y cifrado | Presentación (TLS, SSL), Red (IPsec, VPNs), DNSSEC en Aplicación. |

## Integración de los Modelos OSI y TCP/IP en los Servicios Municipales del Ayuntamiento de Coslada

Para garantizar una red de comunicaciones moderna, escalable y segura, el Ayuntamiento de Coslada adoptará una arquitectura de red basada en los modelos OSI y TCP/IP. Esta arquitectura permitirá integrar los distintos departamentos municipales y servicios ciudadanos con una infraestructura robusta y eficiente, habilitando funcionalidades clave como vigilancia, servicios en línea, IoT ambiental y comunicaciones de emergencia.

**Aplicación del Modelo OSI**

| **Capa OSI** | **Aplicación en Coslada** |
| --- | --- |
| 7. Aplicación | Servicios digitales de atención ciudadana, portales web del ayuntamiento, plataformas de gestión interna. |
| 6. Presentación | Uso de cifrado TLS/SSL para asegurar la información entre usuarios y servicios. |
| 5. Sesión | Mantenimiento de sesiones entre dispositivos y servicios para autenticación y streaming continuo. |
| 4. Transporte | Protocolos TCP (fiables) para servicios administrativos y UDP (rápidos) para video vigilancia y sensores. |
| 3. Red | Enrutamiento eficiente con OSPF/OSPFv3 y direccionamiento dual-stack IPv4/IPv6. |
| 2. Enlace | VLANs segmentadas por departamentos (ej. Urbanismo, Seguridad, Hacienda), Wi-Fi corporativo y QoS. |
| 1. Física | Fibra óptica para backbone, cableado estructurado para oficinas y enlaces inalámbricos para IoT y movilidad. |

**3. Aplicación del Modelo TCP/IP**

| **Capa TCP/IP** | **Servicios de Coslada Soportados** |
| --- | --- |
| Aplicación | Archivo, Cultura, Urbanismo, Vivienda, Servicios Sociales, Educación, Participación Ciudadana, etc. |
| Transporte | TCP para ERP municipales, UDP para CCTV, VoIP de emergencias, y tráfico IoT de sensores. |
| Internet | Uso de IPv6 con túneles GRE/IPSec, soporte de DNSSEC, redundancia con rutas dinámicas. |
| Acceso a red | Interconexión segura de dependencias municipales por switches y puntos de acceso Wi-Fi 6. |

**4. Integración por Tipos de Servicio**

**🔹 Gubernamentales (Ej. Secretaría General, Hacienda, Recursos Humanos)**

* Infraestructura centralizada con VLANs dedicadas.
* VPN segura para acceso remoto de funcionarios.
* Servicios de correo, gestión documental y CRM por TCP/IP.

**🔹 Seguridad y Emergencias**

* Videovigilancia con cámaras IP.
* Comunicación prioritaria por VLANs dedicadas.

**🔹 Transporte y Medio Ambiente (Transición ecológica, Limpieza, Jardines)**

* Sensores IoT sobre redes LoRaWAN/Wi-Fi para calidad del aire y temperatura.
* Semáforos inteligentes conectados mediante IPv6.
* Gestión en tiempo real desde centro de control.

**🔹 Servicios Sociales, Salud y Educación**

* Aplicaciones con datos sensibles protegidas por cifrado
* Acceso seguro por dispositivos móviles de trabajadores sociales.
* Videollamadas o streaming en centros de atención o actividades educativas.

**🔹 Servicios al Ciudadano (Agenda, Participación, Cultura, Deportes)**

* Portales y aplicaciones con interfaces responsivas (capa aplicación).
* Streaming de eventos municipales vía UDP
* Accesibilidad garantizada en puntos de información digital.

**5. Medidas de Seguridad Integradas**

* Cifrado extremo a extremo (IPsec).

### Adaptaciones al diseño para Coslada (resumen técnico)

| **Servicio** | **Implementación realista en Packet Tracer** |
| --- | --- |
| Videovigilancia | Cámaras IP conectadas a switches → a servidores de video |
| Redes gubernamentales | VLANs por departamento + routers ISR con EIGRP |
| Transporte e IoT | Sensores IoT conectados vía Home Gateway + IoT Server |
| Streaming y eventos | Servidor de web + servidor multimedia + PC de streaming |
| Seguridad y emergencias | VLAN dedicada , cifrado de paquetes y control de acceso por ip |
| Conectividad ciudadana | Wi-Fi con WLC simulado + portal web en servidor |

# 2. Capa Física – Cálculos y Selección de Tecnologías

## 1. Cálculo de la Capacidad de los Enlaces:

**Contexto:**

* En cada sede hay zonas con conectividad inalámbrica crítica (puntos de acceso, áreas de atención al público, IoT, etc.).
* Se usarán tecnologías Wi-Fi 6 o enlaces punto a punto de alta frecuencia.
* Excluimos zonas oscuras (almacenes, cuartos de archivo cerrados, etc.) del cálculo.

**Parámetros elegidos para el cálculo:**

| **Parámetro** | **Valor** |
| --- | --- |
| Ancho de banda (𝐵) | 300 MHz |
| SNR (dB) | 20 dB |

**Justificación de los parámetros elegidos:**

| **Parámetro** | **Valor** | **Razón de elección** |
| --- | --- | --- |
| **Ancho de banda (𝐵)** | **300 MHz** | Este valor simula el uso de tecnologías avanzadas como **Wi-Fi 6E**, que opera en la banda de **6 GHz** y puede usar canales anchos de hasta **320 MHz**. Elegí 300 MHz como valor redondeado y realista en despliegues urbanos de alto rendimiento. |
| **SNR (dB)** | **20 dB** | Un **SNR de 20 dB** representa una **calidad de señal buena pero no perfecta**, bastante común en escenarios con múltiples dispositivos, interferencias moderadas o paredes en interiores. Permite modelar condiciones **realistas, no ideales**, lo cual es clave en una sede con cobertura parcial. |

**Alternativas posibles según escenario:**

| **Escenario** | **Ancho de Banda sugerido** | **SNR típico** |
| --- | --- | --- |
| Oficinas estándar con Wi-Fi 5 | 80–160 MHz | 15–20 dB |
| Centros críticos con Wi-Fi 6E | 160–320 MHz | 20–30 dB |
| IoT de bajo consumo (LoRa, etc.) | < 1 MHz | 0–10 dB |
| Zonas muy congestionadas | 80 MHz | < 15 dB |

**Conversión de SNR a escala lineal:**

*SNR lineal=*

**Aplicando la fórmula de Shannon:**

**Resultado**

La **capacidad máxima teórica del canal inalámbrico crítico** con 300 MHz de ancho de banda y una SNR de 20 dB es:

1997 Mbps (≈ 2 Gbps)

**Aplicación práctica por sede**

| **Sede** | **Tecnología recomendada** | **Cobertura calculada** | **Zonas oscuras (excluidas)** |
| --- | --- | --- | --- |
| 🏛️ Sede Central | Wi-Fi 6E / Enlaces punto a punto | Oficinas, salas de reuniones | Almacenes de archivo |
| 🚨 Sede de Seguridad | Wi-Fi 6 + repetidores outdoor | Centro de mando, recepción | Cámaras selladas, depósitos |
| 🚦 Sede Infraestructura IoT | Enlaces 5 GHz + LPWAN (LoRa, etc.) | Talleres, centro de sensores | Trasteros sin sensores |
| 📺 Sede Multimedia y Ciudadana | Wi-Fi 6 público y para eventos | Áreas de atención, patios | Áreas de mantenimiento cerradas |

## 2.Selección de Técnicas de Modulación

Elegir la técnica de modulación adecuada es **clave** para equilibrar **velocidad, eficiencia espectral y robustez** frente al ruido o interferencias.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Modulación** | **Bits/símbolo** | **Eficiencia espectral** | **Robustez ante ruido** | **Complejidad** | **Usos típicos** |
| **BPSK** | 1 | Baja | **Muy alta** | Baja | Redes muy ruidosas, sistemas militares, IoT |
| **QPSK** | 2 | Media | Alta | Moderada | Satélites, 4G, enlaces Wi-Fi básicos |
| **16-QAM** | 4 | Alta | Media | Alta | Wi-Fi, 4G, 5G, redes de alta capacidad |
| **64-QAM** | 6 | Muy alta | Baja | Muy alta | Wi-Fi 5/6 en entornos con poca interferencia |
| **256-QAM** | 8 | Máxima | **Muy baja** | Muy alta | Redes cableadas (Ethernet 10G, DOCSIS 3.1), Wi-Fi 6 |

**Selección por Tipo de Enlace**

**Enlaces Inalámbricos (Wi-Fi, sensores, etc.):**

| **Entorno** | **Modulación recomendada** | **Justificación** |
| --- | --- | --- |
| Zonas críticas, mucho ruido | **QPSK** | Mejor equilibrio entre robustez y eficiencia. Apta para señal estable sin exigir SNR alto. |
| Zonas controladas, señal fuerte | **16-QAM / 64-QAM** | Mayor velocidad donde la calidad de señal es buena (p.ej. sedes con Wi-Fi 6). |
| IoT (bajo ancho, largo alcance) | **BPSK / LoRa (CSS)** | Alta robustez, ideal para sensores de bajo consumo y bajo bit rate. |

**Enlaces Cableados (Fibra, Ethernet, backbone):**

| **Tipo de medio** | **Modulación recomendada** | **Justificación** |
| --- | --- | --- |
| Ethernet (1G–10G) | **PAM-5 / 16-QAM / 256-QAM** | Muy alta eficiencia, ya que el ruido es bajo y el canal es muy limpio. |
| Fibra óptica | **QAM-64/256 o más** | Se usan esquemas densos con corrección de errores (FEC), gracias al altísimo SNR. |
| Enlaces eléctricos cortos | **QAM-16** | Buen compromiso si hay pequeñas interferencias (cables trenzados no apantallados). |

**Conclusión**

| **Tipo de Enlace** | **Modulación Seleccionada** | **Motivo** |
| --- | --- | --- |
| Inalámbrico interior | QPSK o 16-QAM | Buen rendimiento con robustez media, ideal para Wi-Fi en zonas urbanas |
| Inalámbrico exterior | QPSK o BPSK | Más tolerancia al ruido y obstáculos (zonas públicas, IoT) |
| Backbone cableado | 64-QAM o 256-QAM | Alta eficiencia donde las condiciones físicas lo permiten (fibra o 10G LAN) |
| IoT largo alcance | BPSK o modulación LoRa | Menor consumo energético y mayor robustez |

## 3.Evaluación de la Eficiencia del Encapsulamiento

**Ejemplo práctico: Evaluación de la eficiencia del encapsulamiento**

**Supuestos del caso:**

* Se transmite un **mensaje de aplicación** (por ejemplo, un archivo o paquete de datos) de **1000 bytes de carga útil (datos de aplicación)**.
* Se usan tecnologías **Ethernet estándar** (IEEE 802.3) sobre una red IP con TCP.

### Tamaño de cada cabecera por capa:

| **Capa** | **Cabecera** | **Tamaño típico** |
| --- | --- | --- |
| Transporte (TCP) | TCP header | 20 bytes |
| Red (IP) | IPv4 header | 20 bytes |
| Enlace de Datos | Ethernet header | 18 bytes |
| Física | Preambulo + CRC | 8 bytes |
| **Total Overhead** |  | **66 bytes** |

**Cálculo de eficiencia:**

**Eficiencia=**

Eficiencia= ​= ​≈0.9389=93.89%​

**¿Qué pasa si el mensaje es más pequeño?**

Si en vez de 1000 bytes se transmiten 100 bytes, veamos el resultado:

**Conclusión:**

| **Tamaño del mensaje** | **Overhead** | **Eficiencia total** |
| --- | --- | --- |
| 1000 bytes | 66 bytes | 93.89 % |
| 100 bytes | 66 bytes | 60.24 % |
| 50 bytes (IoT típico) | 66 bytes | 43.10 % |

Cuanto menor es el paquete, mayor impacto tiene la sobrecarga del encapsulamiento, lo cual es crítico en redes de sensores o sistemas IoT.

## 4.Plano de cobertura

Para diseñar un plano de cobertura se plantea un esquema general escalable que se aplicara a todas y cada una de las sedes

Forma, Polígono

El contenido generado por IA puede ser incorrecto.

## 5.Cableado estructurado

Se presenta el siguiente cableado para la construcción de las distintas redes:

**SEDE CENTRAL**

| **Dispositivo** | **Medio** | **Función Principal** |
| --- | --- | --- |
| **Router Central** | Serial | Conexión con otras redes |
| **Switch de Acceso** | UTP Cat 6 | Distribución de red local |
| **APs** | UTP Cat 6 | Acceso inalámbrico |
| **PCs** | UTP Cat 6 | Estaciones de trabajo administrativas |

**SEDE DE SEGURIDAD**

| **Dispositivo** | **Medio** | **Función Principal** |
| --- | --- | --- |
| **Router** | UTP | Red interna |
| **Router** | Serial | Conexión con todas las redes |
| **Switch de Acceso** | UTP Cat 6 | Distribución a cámaras, APs y PCs |
| **Cámaras IP** | UTP Cat 6 | Vigilancia (PoE si es posible) |
| **APs / PCs** | UTP Cat 6 | Uso por personal operativo |

**SEDE DE INFRAESTRUCTURA**

| **Dispositivo** | **Medio** | **Función Principal** |
| --- | --- | --- |
| **Router** | UTP | Manejo de dispositivos internos |
| **Router** | Serial | Conexión con todas las redes |
| **Switch de Acceso** | UTP Cat 6 | IoT, sensores, PCs |
| **APs / SensorHub / PCs** | UTP Cat 6 | Cobertura y monitoreo técnico |

**SEDE MULTIMEDIA**

| **Dispositivo** | **Medio** | **Función Principal** |
| --- | --- | --- |
| **Router** | Serial | Conexión con todas las redes |
| **Router LAN local** | UTP | Acceso local para streaming y web |
| **Switch de Acceso** | UTP Cat 6 | Kioskos, APs, PCs |
| **APs / Kiosko / PCs** | UTP Cat 6 | Servicios al ciudadano |

**Resumen de Enlaces de Alta Velocidad (Fibra óptica)**

| **Dispositivo de Origen** | **Dispositivo de Destino** | **Medio** |
| --- | --- | --- |
| Router A (SEDE Cuidadana) | Router Central | Fibra óptica |
| Router Central | Router B (SEDE MULTIMEDIA) | Fibra óptica |
| Router Central | Switch3 (SEDE CENTRAL - Servidores) | Fibra óptica |
| Switch3 | Switch4 (Servidor FTP, etc.) | Fibra óptica |

**Resumen de Enlaces de Red Local (UTP Cat 6)**

| **Dispositivo de Origen** | **Dispositivo de Destino** | **Medio** |
| --- | --- | --- |
| Router A / Switches (SEDE Ciudadana) | APs, PCs, Servidores locales | UTP Cat 6 |
| Switches (SEDE CENTRAL) | PCs, Servidores, Access Points | UTP Cat 6 |
| Switches (SEDE MULTIMEDIA) | PCs, Cámaras IP, SensorHub | UTP Cat 6 |

# 3.Capa de Red – Direccionamiento, Subneteo y Enrutamiento

## 1.Diseño del Esquema de Direccionamiento IP

## Bloques de direccionamiento ip

Sede Iot

| **Descripción** | **VLAN** | **Subred IPv4** | **Subred IPV6** | **Gateway** |
| --- | --- | --- | --- | --- |
| Subred Sensores | 50 | 192.168.50.0/24 | 2001:2882:1::/64 | 192.168.50.1 |
| Subred Videovigilancia | 60 | 192.168.60.0/24 | 2001:2882:2::/64 | 192.168.60.1 |
| Enlace a rúter Central | — | 10.0.0.0/30 |  | 10.0.0.1 (Router B)10.0.0.2 (Central) |

Sede Ciudadana

| **Descripción** | **VLAN** | **Subred IPv4** | **Gateway** |
| --- | --- | --- | --- |
| Subred uso público | 10 | 192.168.10.0/24 | 192.168.10.1 |
| Subred uso público | 20 | 192.168.20.0/24 | 192.168.20.1 |
| Enlace a rúter Central | — | 10.0.2.0/30 | 10.0.2.1 (Router A)10.0.2.2 (Central) |

Sede Central

| **Descripción** | **VLAN** | **Dirección IP** | **Gateway** |
| --- | --- | --- | --- |
| Enlace a Router A | - | 10.0.0.2 | - |
| Enlace a Router C | - | 10.0.1.2 | - |
| Enlace a Router B | - | 10.0.2.2 | - |
| Subred interna 1 | 30 | 192.168.30.0/24 | 192.168.30.1 |
| Subred interna 2 | 40 | 192.168.40.0/24 | 192.168.40.1 |

## Dirección de red, dirección de broadcast y rango de direcciones válidas para los hosts

**Sede Ciudadana**

| **Subred** | **VLAN** | **Dirección de red** | **Broadcast** | **Rango de hosts válidos** | **Gateway** |
| --- | --- | --- | --- | --- | --- |
| Uso público | 10 | 192.168.10.0/24 | 192.168.10.255 | 192.168.10.1 – 192.168.10.254 | 192.168.10.1 |
| Uso interno | 20 | 192.168.20.0/24 | 192.168.20.255 | 192.168.20.1 – 192.168.20.254 | 192.168.20.1 |
| Enlace a Central | — | 10.0.2.0/30 | 10.0.2.3 | 10.0.2.1 – 10.0.2.2 | 10.0.2.1 / .2 |

**Sede Seguridad Pública (IoT y Videovigilancia)**

| **Subred** | **VLAN** | **Dirección de red** | **Broadcast** | **Rango de hosts válidos** | **Gateway** |
| --- | --- | --- | --- | --- | --- |
| Sensores IoT | 50 | 192.168.50.0/24 | 192.168.50.255 | 192.168.50.1 – 192.168.50.254 | 192.168.50.1 |
| Videovigilancia | 60 | 192.168.60.0/24 | 192.168.60.255 | 192.168.60.1 – 192.168.60.254 | 192.168.60.1 |
| Enlace a Central | — | 10.0.0.0/30 | 10.0.0.3 | 10.0.0.1 – 10.0.0.2 | 10.0.0.1 / .2 |

**Sede Central**

| **Subred** | **VLAN** | **Dirección de red** | **Broadcast** | **Rango de hosts válidos** | **Gateway** |
| --- | --- | --- | --- | --- | --- |
| Interna 1 | 30 | 192.168.30.0/24 | 192.168.30.255 | 192.168.30.1 – 192.168.30.254 | 192.168.30.1 |
| Interna 2 | 40 | 192.168.40.0/24 | 192.168.40.255 | 192.168.40.1 – 192.168.40.254 | 192.168.40.1 |
| Enlace a Router A | — | 10.0.0.0/30 | 10.0.0.3 | 10.0.0.1 – 10.0.0.2 | 10.0.0.2 |
| Enlace a Router B | — | 10.0.2.0/30 | 10.0.2.3 | 10.0.2.1 – 10.0.2.2 | 10.0.2.2 |
| Enlace a Router C | — | 10.0.1.0/30 | 10.0.1.3 | 10.0.1.1 – 10.0.1.2 | 10.0.1.2 |

**Sede IoT – Direccionamiento IPv4 e IPv6**

| Subred | VLAN | Dirección de Red (IPv4) | Broadcast (IPv4) | Rango de Hosts IPv4 | Gateway IPv4 | Subred IPv6 | Gateway IPv6 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sensores | 50 | 192.168.50.0/24 | 192.168.50.255 | 192.168.50.1 – 192.168.50.254 | 192.168.50.1 | 2001:2882:1::/64 | 2001:2882:1::1 |
| Videovigilancia | 60 | 192.168.60.0/24 | 192.168.60.255 | 192.168.60.1 – 192.168.60.254 | 192.168.60.1 | 2001:2882:2::/64 | 2001:2882:2::1 |
| Enlace a Central | — | 10.0.0.0/30 | 10.0.0.3 | 10.0.0.1 – 10.0.0.2 | 10.0.0.1 / .2 | — | — |

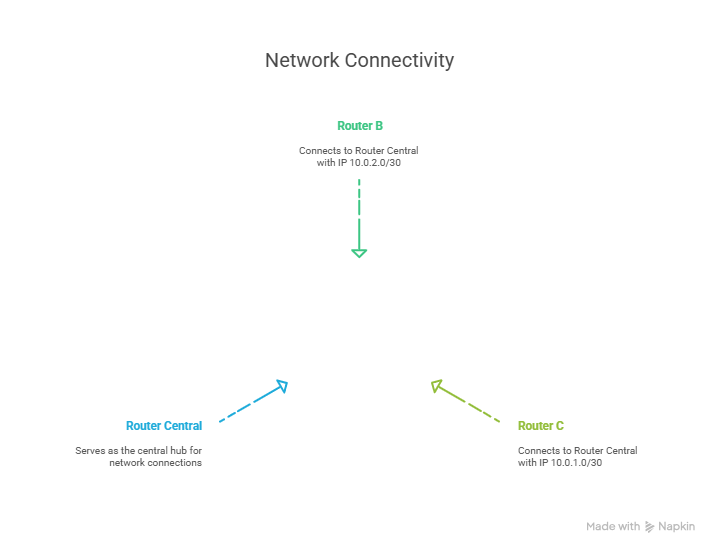
## 2. Enrutamiento y Rutas Óptimas

**Algoritmo de Dijkstra – Rutas Óptimas entre Segmentos**

**🔹 Escenario**

Se requiere determinar la ruta más corta desde la **sede de Seguridad Pública (Router B)** hacia la **sede Central**, así como hacia otras sedes como IoT (Router A) y Multimedia (Router C), para propósitos de servicios de emergencia y coordinación.

**Red Simplificada (Topología de Backbone)**



**Modelo para Dijkstra (Coste por Enlace = 1)**

| **Nodo** | **Vecinos** | **Costes** |
| --- | --- | --- |
| B | Central | 1 |
| Central | A, B, C | 1 |
| A | Central | 1 |
| C | Central | 1 |

**Cálculo paso a paso de Dijkstra desde B**

**Paso 1** – Inicialización:

* Nodo origen: **B**
* Distancias: B=0, Central=∞, A=∞, C=∞
* Visitados: ∅

**Paso 2** – Evaluar vecinos de B:

* Central: 0 + 1 = **1**
* Distancias: B=0, Central=1, A=∞, C=∞
* Visitados: B

**Paso 3** – Nodo con menor distancia no visitado: **Central**

* Vecinos: A, C
* A: 1 + 1 = **2**
* C: 1 + 1 = **2**
* Distancias: B=0, Central=1, A=2, C=2
* Visitados: B, Central

**Paso 4** – Restantes nodos:

* A y C, ambos con coste 2
* Ruta óptima:
  + **B → Central** (coste 1)
  + **B → Central → A/C** (coste 2)

**Rutas Resultantes**

| **Origen** | **Destino** | **Ruta** | **Coste** |
| --- | --- | --- | --- |
| B | Central | B → Central | 1 |
| B | A (IoT) | B → Central → A | 2 |
| B | C | B → Central → C | 2 |

**Enrutamiento por Inundación – Método de Respaldo**

El **enrutamiento por inundación (flooding)** reenvía todos los paquetes entrantes por todas las interfaces *excepto por la que lo recibió*, sin necesidad de rutas predefinidas.

**¿Cuándo se usa?**

* Como **respaldo** ante la caída de enlaces clave o rutas desconocidas.
* Muy útil en **topologías críticas** o en redes sin convergencia inmediata.

**Ejemplo práctico de flooding**

**Escenario de fallo**:

* Falla el enlace **B ↔ Central (10.0.2.0/30)**

**Proceso**:

1. Router B no tiene ruta directa.
2. Inunda el paquete hacia cualquier otro router accesible.
3. Si está conectado a Router A o Router C (vía un switch, por ejemplo), estos reenvían hacia sus propios vecinos.
4. Eventualmente, el paquete llega al Router Central **por rutas alternativas**.

**Resumen Técnico**

| **Enfoque** | **Ventaja** | **Desventaja** |
| --- | --- | --- |
| Dijkstra | Rutas óptimas con métricas precisas | Requiere cálculo previo y convergencia |
| Inundación | Respaldo automático sin rutas previas | Ineficiente, posible duplicación de tráfico |

En redes reales, protocolos como **OSPF, EIGRP** implementan variantes de Dijkstra con respaldo automático. La **inundación** queda reservada para situaciones críticas o descubrimiento inicial.

# 4. Capa de Transporte – Selección de Protocolos y Cálculo del Tamaño de Ventana

## 4.1Selección de Protocolos de Transporte

**TCP (Transmission Control Protocol)**

**Usos recomendados:**

* Transferencia de archivos (FTP, SCP)
* Servicios de correo electrónico
* Sincronización de bases de datos
* Consultas web críticas

**Justificación:**

* **Fiabilidad:** TCP garantiza la entrega de datos, reenvía paquetes perdidos y reordena los que llegan fuera de orden.
* **Control de congestión y flujo:** Se ajusta automáticamente a las condiciones de la red para evitar sobrecargas.
* **Conexión orientada:** Establece una conexión antes de transmitir datos, asegurando que ambas partes están listas.

**UDP (User Datagram Protocol)**

**Usos recomendados:**

* Transmisión en tiempo real (video vigilancia IP, voz sobre IP)
* Alertas instantáneas (tráfico, sensores de IoT)
* Juegos en red o telemetría

**Justificación:**

* **Menor latencia:** Al no tener control de errores, es más rápido que TCP.
* **No orientado a conexión:** Ideal para tráfico que puede tolerar pérdidas menores pero no retrasos.
* **Menor sobrecarga de cabecera:** UDP usa solo 8 bytes frente a los 20+ de TCP.

## 4.2Cálculo del Tamaño de Ventana Óptima en TCP

La **ventana TCP óptima** determina cuántos datos pueden enviarse sin recibir una confirmación (ACK), maximizando el uso del canal.

**Fórmula:**

Ventana óptima=Ancho de banda×RTT

**Parámetros Supuestos**

* **RTT (Round Trip Time):** 50 ms = 0.050 segundos
* **MSS (Maximum Segment Size):** 1,500 bytes
* **Ancho de banda:** 10 Mbps = 10,000,000 bits por segundo

**Paso a Paso: Conversión y Cálculo**

1. **Convertimos el RTT a segundos:**

50ms=0.05s

**Multiplicamos por el ancho de banda:**

Ventana óptima=10,000,000 bps \* 0.05s = 500,000 bits

**Convertimos la ventana a bytes:**

500,000bits÷8=62,500bytes

Calculamos cuántos segmentos MSS caben en esa ventana:

**Resultado Final**

* **Ventana óptima TCP:** 62,500 bytes
* **Cantidad máxima de segmentos MSS en tránsito sin esperar ACK:** **41**

# **Paso 5: Capa de Aplicación – Servicios, Multiplexación y Multimedia**

## 5.1.Implementación de Servicios y Resolución de Nombres

**Servidor FTP/SFTP**

* **FTP (Puerto 21):** Permite transferencia de archivos en texto claro (solo con fines de demostración interna).
* **SFTP (Puerto 22):** Protocolo seguro sobre SSH. Garantiza confidencialidad e integridad.
* **Usuarios:** Los ciudadanos y empleados usan SFTP para subir/bajar documentos. Solo empleados tienen acceso completo.

**Servidor HTTP/HTTPS**

* **HTTP (Puerto 80):** Usado para sitios web informativos básicos.
* **HTTPS (Puerto 443):** Usado para portales interactivos, incluyendo control de cámaras, sensores y accesos ciudadanos.
* **Certificado SSL:** Instalado para encriptar las comunicaciones en HTTPS.
* **Servicios alojados:**
  + Panel de control IoT
  + Visualización de cámaras
  + Acceso a archivos vía navegador

**Proceso de Resolución de Nombres**

1. Un cliente (PC) solicita acceder a ftp.ayuntamiento.local.
2. Consulta al servidor DNS configurado en su adaptador de red.
3. El servidor DNS responde con la IP correspondiente (ej. 192.168.X.10).
4. El cliente se conecta al servidor FTP/SFTP utilizando la IP resuelta.

Esto permite que los usuarios no necesiten memorizar direcciones IP, y que las aplicaciones puedan cambiar de IP sin afectar a los clientes.

**Gestión de Múltiples Solicitudes – Multiplexación**

La red implementa **multiplexación por puertos TCP/UDP**, una técnica clave para permitir múltiples conexiones simultáneas a un mismo servidor. Esto funciona así:

* Cada servicio usa un **número de puerto específico**:
  + DNS → puerto 53
  + FTP → puerto 21
  + SFTP → puerto 22
  + HTTP → puerto 80
  + HTTPS → puerto 443
* Cada cliente usa un **puerto de origen aleatorio** y se conecta al **puerto de destino del servicio**.
* Esto permite que cientos de usuarios usen simultáneamente el mismo servidor sin conflictos, ya que las conexiones se diferencian por los puertos y direcciones.

**Ejemplo:**  
Un mismo servidor con IP 192.168.1.10 puede atender al mismo tiempo:

* A un cliente accediendo a la web (192.168.1.20:50678 → 192.168.1.10:443)
* A otro descargando archivos por SFTP (192.168.1.30:50533 → 192.168.1.10:22)
* A otro resolviendo un dominio (192.168.1.40:54000 → 192.168.1.10:53)

## 5.2.Servicios Multimedia

**Transmisión en Tiempo Real**

Para brindar servicios de video en tiempo real, como cámaras de seguridad o transmisiones de eventos públicos, se han considerado dos métodos de streaming:

**1. UDP Streaming (Unicast/Multicast)**

* **Uso:** Ideal para **cámaras IP en tiempo real** conectadas a la sede de seguridad.
* **Ventajas:**
  + Baja latencia.
  + No requiere retransmisiones.
* **Desventajas:**
  + No garantiza entrega de paquetes (puede haber pérdida en redes congestionadas).
* **Implementación:** Transmisión unicast o multicast desde el servidor de cámaras al cliente de monitoreo.

**2. Adaptive HTTP Streaming (DASH)**

* **Uso:** Ideal para **eventos públicos**, charlas o sesiones grabadas reproducidas por usuarios ciudadanos.
* **Funcionamiento:**
  + El video se divide en segmentos y versiones de distinta calidad (resoluciones/bitrates).
  + El cliente (navegador o app) **detecta el ancho de banda disponible** y solicita la calidad más adecuada dinámicamente.
* **Ventajas:**
  + Adaptación automática a condiciones variables de red.
  + Compatible con HTTP/HTTPS, facilitando su distribución en redes corporativas.

**Adaptación de Calidad según Ancho de Banda**

Para evitar interrupciones o sobrecarga de red, se implementan técnicas de **adaptación de calidad (bitrate switching)**, como:

* **Medición del buffer del cliente** y del ancho de banda actual.
* **Cambios automáticos entre calidades:** baja (360p), media (480p), alta (720p/1080p).
* **Priorización de tráfico sensible:** mediante QoS, se puede dar prioridad al tráfico UDP de videovigilancia frente al tráfico no crítico.

**Seguridad en Streaming**

* **HTTPS + DASH:** garantiza privacidad e integridad de los contenidos ciudadanos.
* **ACLs y VLANs:** evitan el acceso no autorizado a transmisiones internas (como las de cámaras de seguridad).
* **VPN/IPsec:** se usa cifrado extremo a extremo entre sedes que visualizan el video remotamente.

# 6. Seguridad – Estrategias y Configuración

## 6.1. Políticas y Medidas de Seguridad

**VPN para interconexión segura**

**Presente:**

* Hay túneles Tunnel configurados entre distintas sedes (como 192.168.30.0, 40.0, 50.0 y 60.0).
* Se ha aplicado **IPsec** a través de crypto map, lo cual proporciona **confidencialidad, integridad y autenticación** del tráfico.
* Esto cumple con la política de interconectar segmentos sensibles como la **sede de seguridad y las oficinas municipales**.

**Firewalls y ACLs**

**Parcialmente presente:**

* Se han configurado **ACL extendidas** en los routers que bloquean el acceso desde la VLAN de los ciudadanos (VLAN 40) hacia dispositivos críticos como:
  + Cámaras
  + Servidores IoT
* Ejemplo: access-list 110 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
* Sin embargo, **no se han configurado firewalls dedicados (como dispositivos ASA)**. Estás usando los ACLs como medida de filtrado básico a nivel de router.

## 6.2.Cifrado y Autenticación

**Uso de TLS/SSL para Comunicaciones Críticas**

TLS (Transport Layer Security) y su predecesor SSL se utilizan ampliamente para cifrar comunicaciones entre clientes y servidores, especialmente en servicios como:

* **HTTPS:** Portales ciudadanos, cámaras IP, interfaces IoT.
* **SFTP:** Transferencia de archivos de forma segura (sobre SSH).
* **Correo electrónico, VoIP y otros servicios web.**

**Importante:** Aunque Cisco Packet Tracer no permite simular el cifrado real con certificados digitales, en una red real:

* Se instalan certificados TLS/SSL en los servidores web y de cámaras.
* Se configura el uso de puertos seguros (443 para HTTPS).
* Se valida la identidad del servidor mediante certificados autofirmados o de una Autoridad Certificadora (CA).

**Implementación de RSA**

RSA es un sistema de cifrado **asimétrico** utilizado para proteger la confidencialidad de datos mediante un par de claves:

* **Clave pública:** Se comparte con otros para que cifren los mensajes.
* **Clave privada:** Se mantiene en secreto y se usa para descifrar los mensajes.

**Ejemplo simplificado de RSA (conceptual)**

1. **Generación de claves:**
   * Elegimos dos números primos grandes: p = 17, q = 11
   * Calculamos: n = p × q = 187
   * Calculamos: φ(n) = (p−1)(q−1) = 160
   * Elegimos e = 7 (coprimo con 160)
   * Calculamos d = 23, ya que 7 × 23 mod 160 = 1

Resultado:

* + Clave pública: (e = 7, n = 187)
  + Clave privada: (d = 23, n = 187)

1. **Cifrado (por el cliente):**
   * Mensaje M = 88
   * Cifrado: C = M^e mod n = 88^7 mod 187 = 11
2. **Descifrado (por el servidor):**
   * Descifrado: M = C^d mod n = 11^23 mod 187 = 88

Este ejemplo demuestra cómo un mensaje cifrado con la **clave pública** solo puede ser leído con la **clave privada**, garantizando confidencialidad.

**DNSSEC: Seguridad para el Servicio DNS**

**DNSSEC (DNS Security Extensions)** protege las consultas DNS mediante firmas digitales, evitando:

* **DNS Spoofing** (suplantación de respuestas DNS)
* **Ataques de envenenamiento de caché**

**¿Cómo funciona DNSSEC?**

* Cada zona DNS tiene un conjunto de claves criptográficas (clave de firma y clave de zona).
* Las respuestas DNS vienen firmadas digitalmente.
* El cliente puede verificar que la respuesta proviene del servidor legítimo.

**¿Por qué no se ha implementado TLS, RSA y DNSSEC en este proyecto?**

1. **Limitaciones del simulador (Cisco Packet Tracer):**
   * No permite configurar certificados TLS ni simular conexiones HTTPS reales.
   * No tiene soporte para generación y uso de claves RSA.
   * DNSSEC **no está disponible ni en servidores ni en clientes** dentro del simulador.
2. **Enfoque educativo y de infraestructura:**
   * Este proyecto prioriza la **estructura lógica de red, segmentación, ACLs, VPN y túneles IPsec**, los cuales **sí son simulables**.
   * La seguridad se ha garantizado principalmente mediante:
     + **VPNs IPsec**
     + **ACLs extendidas**
     + **Topología segmentada con VLANs**
3. **Implementación teórica o futura:**
   * Se deja documentado el uso de TLS/RSA/DNSSEC para su futura implementación en entornos reales o simuladores más avanzados como GNS3, EVE-NG o redes reales con equipos Cisco.

Aunque el **Servicio DNS (Domain Name System)** es fundamental en redes reales para la resolución de nombres, en este proyecto no se ha implementado por las siguientes razones técnicas y prácticas:

**1.Limitaciones del simulador Cisco Packet Tracer**

* **DNS en Packet Tracer es muy básico:** solo permite responder con IPs a nombres fijos y no simula realmente una base de datos DNS completa ni registros dinámicos.
* **No se puede simular DNSSEC, zonas inversas, ni delegaciones reales**, por lo que su utilidad en el entorno simulado es limitada.

**2.Enfoque en servicios críticos**

* El proyecto prioriza otros servicios más directamente aplicables y funcionales en Packet Tracer:
  + FTP / SFTP
  + TFTP
  + HTTP / HTTPS (en parte simulados)
  + Videovigilancia y IoT
* Todos estos servicios pueden operar correctamente usando direcciones IP directamente, sin necesidad de resolución de nombres.

**3.Simplificación para pruebas de conectividad**

* Al no usar DNS, los **comandos de prueba como ping, ftp, telnet o http://** se aplican directamente sobre IPs, evitando errores de resolución que podrían complicar la validación del funcionamiento de la red.
* Esto permite una **comprobación más directa** del comportamiento de la red en etapas tempranas del diseño.