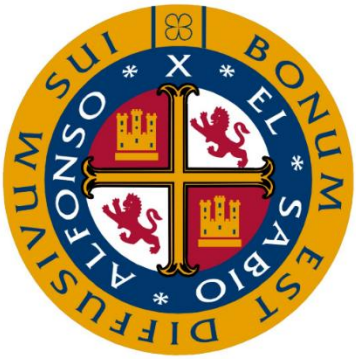


UNIVERSIDAD
ALFONSO X EL SABIO

Por: Juan Pablo Lobato

Índice:

Diseño y Modelado de la Arquitectura de Comunicación 3
Análisis de Modelos 3
Diseño Lógico y Segmentación 4
2. Capa Física – Cálculos y Selección de Tecnologías 5
2.1 Cálculo de la capacidad de los enlaces 5
2.2 Selección de Técnicas de Modulación 5
2.3 Evaluación de la Eficiencia del Encapsulamiento 6
3. Capa de Red – Direccionamiento, Subneteo y Enrutamiento 7
3.1 Diseño del esquema de direccionamiento IP: 7
3.2 Enrutamiento y rutas óptimas: 8
4. Capa de Transporte – Selección de Protocolos y Cálculo del Tamaño de Ventana 8
4.1 Selección de Protocolos de Transporte 8
4.2 Cálculo del Tamaño de Ventana en TCP 9
5. Capa de Aplicación – Servicios, Multiplexación y Multimedia 9
5.1 Implementación de Servicios y Resolución de Nombres 9
5.2 Servicios Multimedia 9
6. Seguridad – Estrategias y Configuración 10
6.1 Políticas y Medidas de Seguridad 10
6.2 Cifrado y Autentificación 10
7. Implementación en Cisco Packet Tracer 10
7.1 Construcción de la Topología 11
7.2 Configuración de Protocolos y Servicios 15

Diseño y Modelado de la Arquitectura de Comunicación

Análisis de Modelos

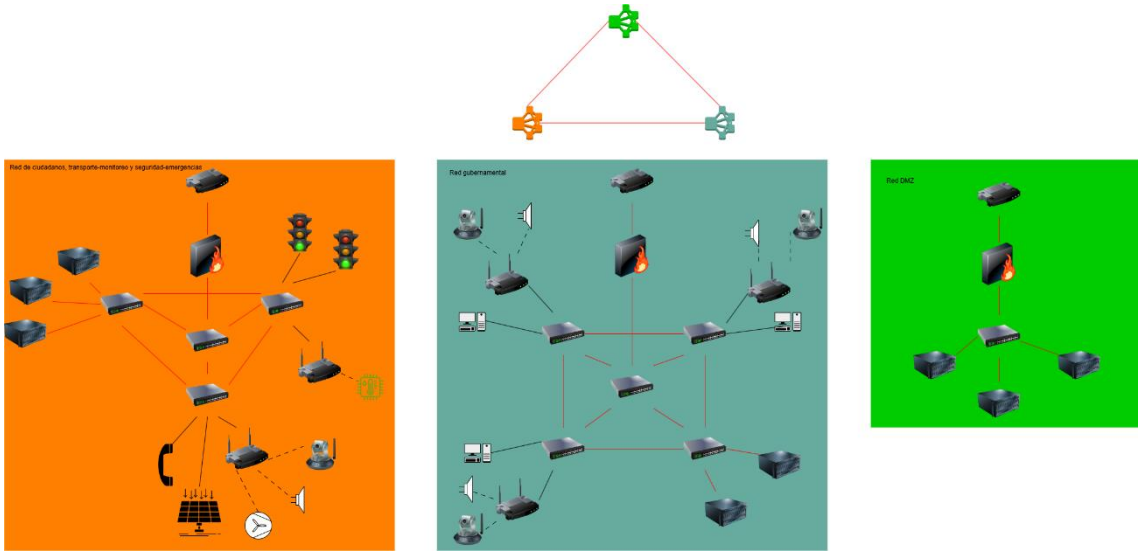
Modelo OSI

Capa 7: Aplicación	• Función: interfaz entre el usuario final y las aplicaciones. • Protocolos: HTTP/HTTPS, FTP, SMTP, SNMP, DNS, Telnet. • Integración: portales web para los ciudadanos, interfaces de control de tráfico, sistemas de gestión, aplicaciones de monitores ambiental
Capa 6: Presentación	• Función: traducción de datos entre formatos ya sea cifrado, descifrado o de compresión o descompresión. • Protocolos: SSL/TLS, JPEG, MPEG, ASCII, Unicode. • Integración: conversión de formatos para imágenes de videovigilancia, cifrado de datos, compresión de stream.
Capa 5: Sesión	• Función: establece, administra y finaliza conexiones entre aplicaciones locales y remotas. • Protocolos: NetBIOS, RPC, SIP. • Integración: gestión de sesiones para videoconferencias, gestión de sesiones para sistemas de control de acceso en edificios públicos.
Capa 4: Transporte	• Función: segmentación, corrección de errores y control de flujo de extremo a extremo. • Protocolos: TCP, UDP. • Integración: TCP para transacciones críticas, UDP para streaming de cámaras y sensores IoT.
Capa 3: Red	• Función: enrutamiento de paquetes, optimización de caminos y direccionamiento lógico. • Protocolos: IP (IPv4/IPv6), ICMP, OSPF, BGP. • Integración: interconexión entre los diferentes segmentos de la red.
Capa 2: Enlace de Datos	• Función: acceso al medio, direccionamiento físico (MAC), detección de errores. • Protocolos: Ethernet, Wi-Fi, PPP, ATM, Frame Relay. • Integración: switches en redes internas, conexión Wi-Fi para ciertos usuarios, enlaces punto a punto entre segmentos de la red.
Capa 1: Física	• Función: transmisión de bits a través del medio físico • Protocolos: Cables (UTP, fibra óptica), conectores, frecuencia de radio. • Integración: cableado de fibra en los edificios y en las ciudades, cableado cat6a en cada para conectar con el dispositivo final y radioenlace entre edificios.

Modelo TCP/IP

Capa 4: Aplicación	• Función: une la función de las tres capas 5, 6 y 7 de OSI. • Protocolos: HTTP, FTP, SMTP, Telnet, SSH, SNMP, DNS. • Relación con modelo OSI: combina la interfaz de usuario, representación de datos y control de sesión. • Integración: los servicios de aplicación que requieren los diferentes servicios.
Capa 3: Transporte	• Función: entrega de datos extremo a extremo • Protocolos: TCP y UDP • Relación con modelo OSI: corresponde a la capa de transporte, capa 4. • Integración: asegura la fiabilidad en las comunicaciones y la eficiencia en la transmisión.
Capa 2: Internet	• Función: enruaminto de datagramas a través de redes. • Protocolos: IP, ICMP, IGMP, ARP. • Relación con modelo OSI: capa red, capa 3. • Integración: enrutamiento entre redes.
Capa 1: Acceso de la Red	• Función: interfaz con hardware de red y medios físicos. • Protocolos: Ethernet, Token Ring, FDDI, Wi-Fi • Relación con modelo OSI: combina las capas Físicas y de Enlace de Datos. • Integración: infraestructura física y de enlace que permite la comunicación local y entre ubicaciones.

Diseño Lógico y Segmentación



2. Capa Física – Cálculos y Selección de Tecnologías

2.1 Cálculo de la capacidad de los enlaces

Fórmula de Shanon

$C = B * \log_2(1 + SNR)$

Donde:
C = Capacidad del canal en bits por segundo (bps)

B = Ancho de banda del canal en Hertzios (Hz)

SNR = Relación señal-ruido (debe convertirse de dB a escala lineal)

Cómo convertir SNR de dB a escala lineal

SNRlineal = 10^(SNR(dB)/10)

Aplicación a nuestra infraestructura:

1. Para enlaces inalámbricos entre edificios

B = 80 MHz

SNR = 18 dB

SNRlineal = 10^(18/10) = 10^1,8 = 63,1

Formula de Shannon → $C = 80000000 * \log_2(1 + 63{,}1) = 480000000\ bps = 480\ Mbps$

2. Para enlaces críticos, fibra óptica

B = 400 MHz

SNR = 30 dB

SNRlineal = 10^(30/10) = 1000

Formula de Shannon → $C = 400000000 * \log_2(1 + 1000) = 3990000000\ bps = 3{,}99\ Gbps$

3. Para enlaces con cable Cat 6a

B = 500 MHz

SNR = 35dB

SNRlineal = 10^(35/10) = 10^3,5 = 3162,28

Formula de Shannon → $C = 500000000 * \log_2(1 + 3162{,}28) = 5815000000\ bps = 5{,}82\ Gbps$

2.2 Selección de Técnicas de Modulación

Modulación	Bits por símbolo	Eficiencia espectral	Robustez frente a ruido	Aplicaciones adecuadas

BPSK	1	Baja	Muy alta	Enlaces críticos con bastante ruido
QPSK	2	Media	Alta	Comunicaciones móviles básicas
16-QAM	4	Alta	Media	Wi-Fi, enalces con buena SNR
64-QAM	6	Muy alta	Baja	LAN, enlaces con excelente SNR
256-QAM	8	Extremadamente alta	Muy baja	Fibra óptica, enlaces óptimos

Selección para la infraestructura:
Enlaces cableados:

- Dentro de edificios: modulación **256-QAM**, debido a su alta eficiencia espectral.
- Entre edificios cercanos: modulación **16-QAM**, compleja pero velocidad alta.

Enlaces inalámbricos:

- Radioenlaces punto a punto: modulación **16-QAM**, equilibrio entre velocidad y resistencia a interferencias.
- Redes Wi-Fi: modulación **64-QAM**, alta eficiencia espectral con capacidad de adaptarse a distintas condiciones, podemos cambiarlo a BPSK en condiciones malas.
- Red de IoT: modulación **QPSK**, gran robustez frente a interferencias externas, y buena para transmisión de video en lo que importa es la velocidad.

2.3 Evaluación de la Eficiencia del Encapsulamiento

Ejemplo Práctico: Datos de una cámara de videovigilancia

Datos útiles: 1400 bytes

Sobrecarga por capa:

4. Capa Aplicación (RTP para video): 12 bytes

3. Capa Transporte (UDP): 8 bytes

2. Capa de Red (IPv4): 20 bytes

1. Capa Enlace (Ethenet): 18 bytes

Preámbulo y delimitadores: 8 bytes

Total: 66 bytes

Cálculo de la eficiencia:

Tamaño total del paquete: 1400 + 66 = 1466 bytes

Eficiencia = (Datos útiles / Tamaño total) x 100 = (1400/1466) x 100) = 95,5%

La eficiencia es de un 95,5% debido al tamaño de los datos.

3. Capa de Red – Direccionamiento, Subneteo y Enrutamiento

3.1 Diseño del esquema de direccionamiento IP:

Segmento	Bloque de dirección IP	Máscara	CIDR
Servicios Gubernamentales	10.1.0.0	255.255.254.0	/23
Seguridad pública y emergencias	10.2.0.0	255.255.254.0	/23
Transporte y monitoreo ambiental	10.4.0.0	255.255.254.0	/23
Servicios Multimedia	10.3.0.0	255.255.254.0	/23
Gestión y administración de red	10.0.254.0	255.255.254.0	/23

Cálculos para servicios gubernamentales – 10.0.0.0/24

- Dirección de red: 10.0.0.0
- Dirección broadcast: 10.0.0.255
- Rango de direcciones válidas para host: 10.0.0.1 – 10.0.0.254
- Número total de hosts disponibles: 254

Cálculos para seguridad pública – 10.0.1.0/24

- Dirección de red: 10.0.1.0
- Dirección broadcast: 10.0.1.255
- Rango de direcciones válidas para hosts: 10.0.1.1 – 10.0.1.254
- Número total de hosts disponibles: 254

Cálculo para transporte y monitoreo – 10.0.2.0/24

- Dirección de red: 10.0.2.0
- Dirección broadcast: 10.0.2.255
- Rango de direcciones válidas para hosts: 10.0.2.1 – 10.0.2.254
- Número total de hosts disponibles: 254

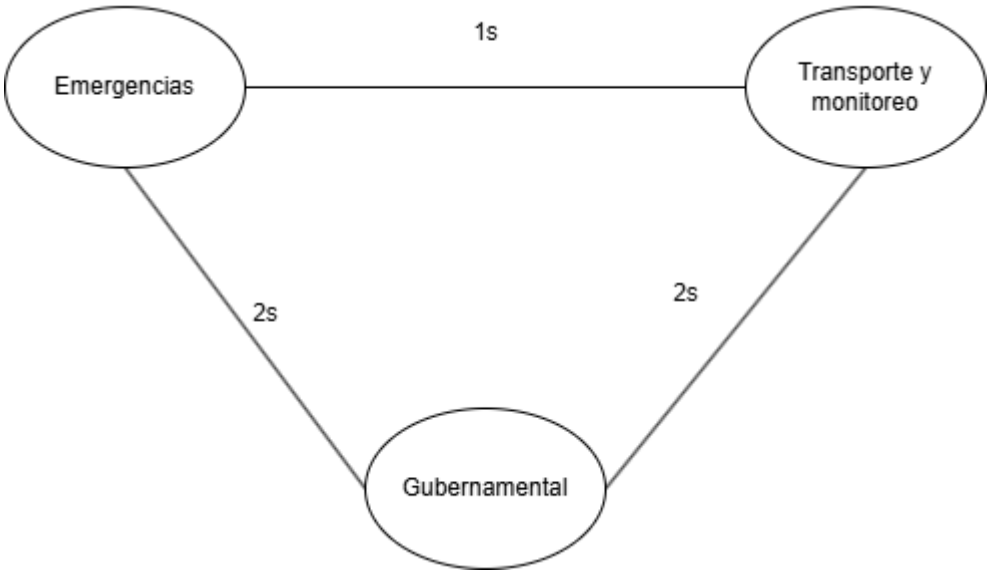
Cálculo para servicios multimedia – 10.0.3.0/24

- Dirección de red: 10.0.3.0
- Dirección broadcast: 10.0.3.255
- Rango de direcciones válidas para hosts: 10.0.3.1 – 10.0.3.254
- Número total de hosts disponibles: 254

Explicación de porque la máscara /24

La he elegido por varias razones, entre ellas porque proporciona 254 direcciones IP utilizables (2^8-2), más que de sobra para los servicios municipales y porque limita el tráfico de broadcast a segmentos de un tamaño que se puede administrar con facilidad.

3.2 Enrutamiento y rutas óptimas:



En este algoritmo de dijktra vemos que en lo que más tarda en comunicar es a la red de emergencia, da igual por donde vayas porque la red de emergencias y transporte-monitoreo esta en una sola.

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

4.1 Selección de Protocolos de Transporte

Características	TCP	UDP	Servicio municipal óptimo
Orientado a conexión	Sí	No	TCP: servicios gubernamentales críticos
Control de flujo	Sí	No	TCP: transmisión de documentos oficiales
Control de congestión	Sí	No	TCP: servicios ciudadanos
Detección/corrección de errores	Sí	No	TCP: datos financieros
Entrega ordenada	Sí	No	TCP: bases de datos distribuidas
Bajo overhead	No	Sí	UDP: streaming de cámaras
Baja latencia	No	Sí	UDP: aviso de emergencias
Multicast/broadcast	No	Sí	UDP: avisos a ciudadanos

1. Servicios gubernamentales:
   Protocolo: TCP
   Justificación: lo principal que buscamos en estas transacciones son la integridad de los datos y la seguridad, ya que cualquier error en ellos puede conllevar a problemas legales.
2. Servicios de seguridad pública y emergencias:
   Protocolo: Híbrido (UDP para video, TCP para datos)
   Justificación: las cámaras necesitan rapidez en la transmisión de datos, no importa si un frame se pierde ocasionalmente.
3. Transporte y monitoreo ambiental:
   Protocolo: UDP

Justificación: los sensores IoT envían datos continuamente lo que colapsaría el protocolo TCP.

4. Servicios multimedia para ciudadanos:
   Protocolo: UDP para streaming y TCP para VoD
   Justificación: para el streaming al ser en vivo debemos ceder la posible pérdida de algunos frame.

4.2 Cálculo del Tamaño de Ventana en TCP

Ventana óptima = Ancho de banda x RTT

RTT = 50 ms = 0,050 s

MSS = 1500 bytes

Ancho de banda = 300 Mbps (esto es una suposición) = 300000000 bps

Ventana óptima = 300000000 bps x 0,050 s = 15000000 bits

Convierto de bits a bytes:

15000000 / 8 = 1875000 bytes

Número de segmentos MSS en tránsito simultáneamente:

Número de segmentos = Tamaño de ventana / MSS = 1875000 bytes / 1500 bytes/segmento = 1250 segmentos

5. Capa de Aplicación – Servicios, Multiplexación y Multimedia

5.1 Implementación de Servicios y Resolución de Nombres

- DNS: configurare un servidor DNS para la red. Así la red podrá traducir el nombre de un dominio en una dirección IP.
- FTP/SFTP: en la red gubernamental pondré un servidor de archivos para poder almacenarlos todos.
- HTTP/HTTPS: para colocar web para la ciudadanía y como web del ayuntamiento.

5.2 Servicios Multimedia

- Servicio de Streming con protocolo UDP, se utilizará en cámaras de vigilancia y eventos públicos. Así garantizamos una baja latencia a pesar de perder de vez en cuando un poco de información en los paquetes
- Protocolo adaptativo: DASH para adaptarse a los cambios del ancho de banda: cat 6a, fibra o inalámbrica.

6. Seguridad – Estrategias y Configuración

6.1 Políticas y Medidas de Seguridad

Diseño de la red

Voy a dividir las zonas en 3, incluyendo la zona DMZ siendo 0 la más crítica donde más seguridad debe haber y 3 la menos. Esto facilitara la expansión de segmentos de la red en un futuro.

Zona	Nivel de Seguridad	Recursos Protegidos	Medidas Principales
Zona 0	Crítico	Base de datos, sistemas financieros	Aislamiento físico, autentificación MFA, cifrado total
Zona 1	Alto	Sistemas de emergencia, servidores de control	Firewalls, IPS/IDS, VPN
Zona 2	Medio	Redes, servicios de administración	VLANs y firewall

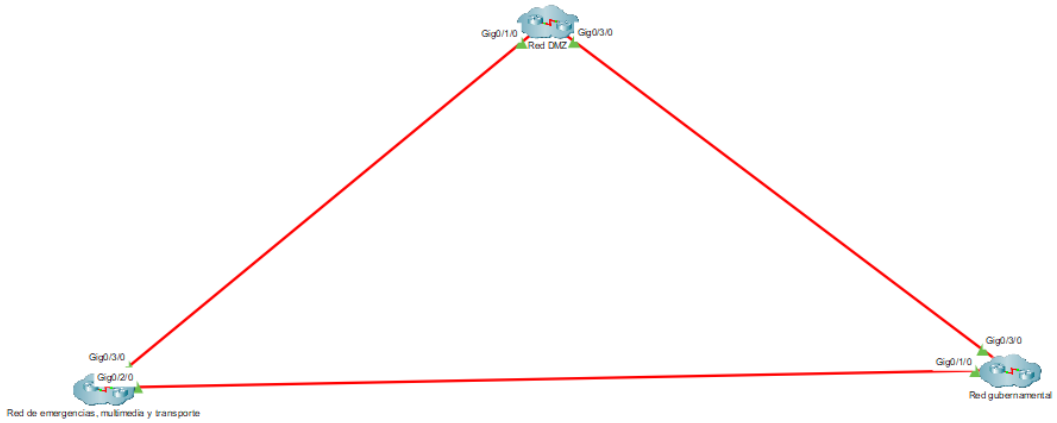
Para interconectar de forma segur los diferentes segmentos sensibles, configuraremos túneles VPN Ipsec site-to-site

6.2 Cifrado y Autentificación

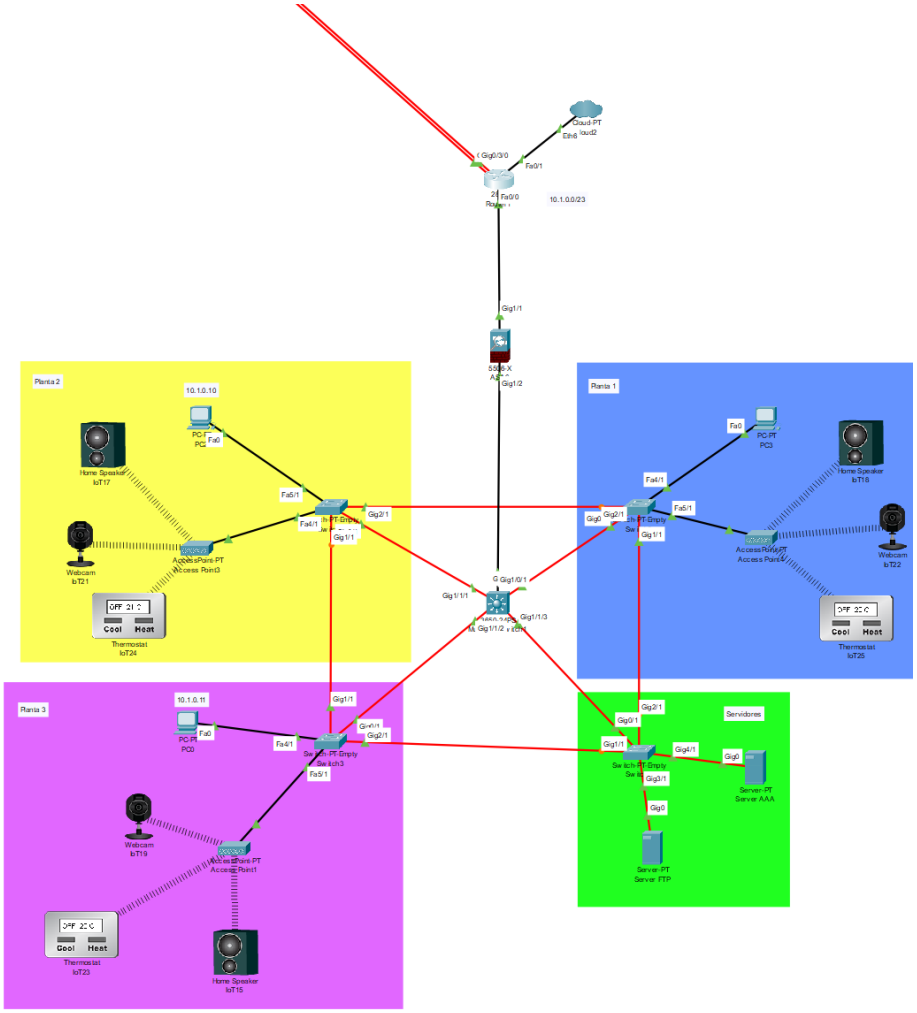
- TSL/SSL: configuración para cifrar las comunicaciones críticas, por ejemplo portales web y transferencia.
- AAA: protocolo para autentificar a los usuarios, se implementara en un servidor.

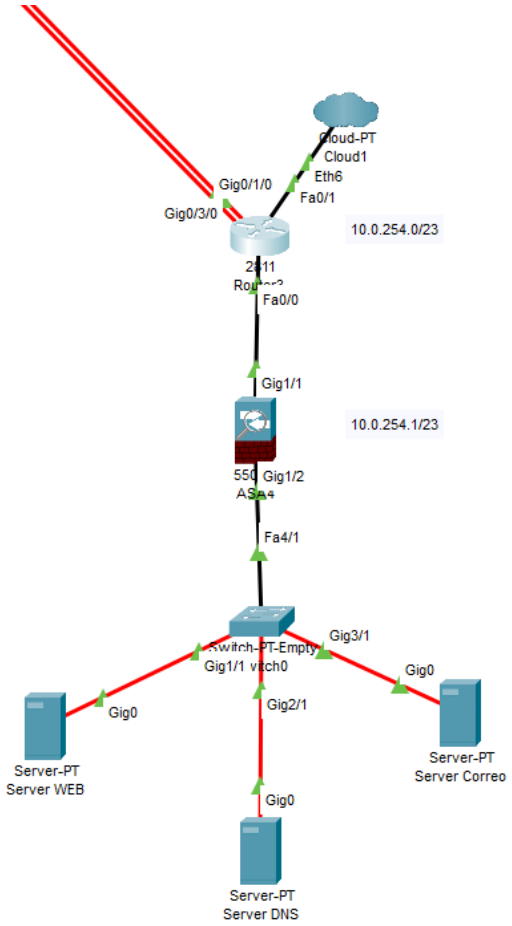
7. Implementación en Cisco Packet Tracer

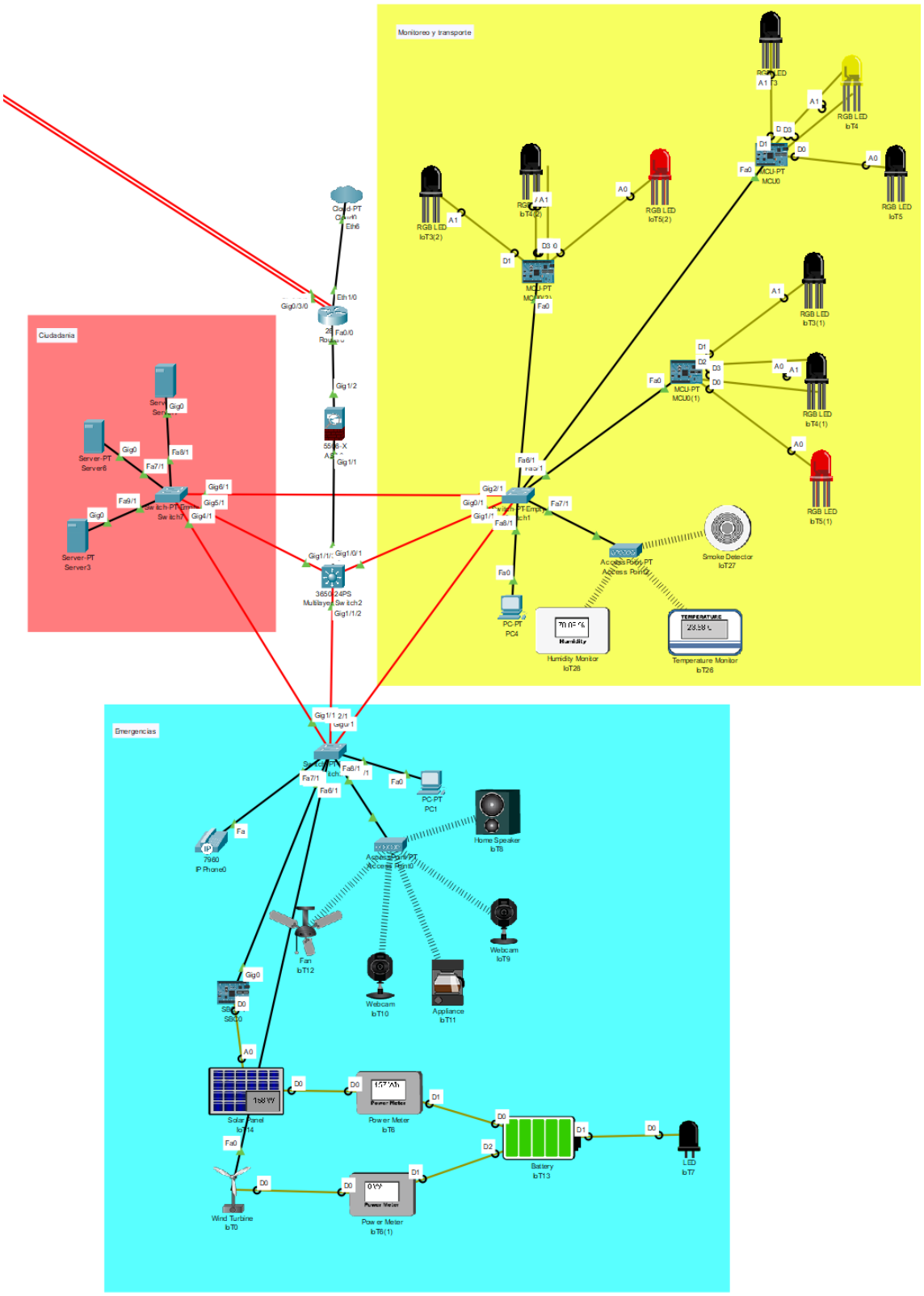
La red la hemos estructurado en tres router's: dmz, gubernamental y ciudadanía-transporte-emergencias:



Fotos por segmentos:



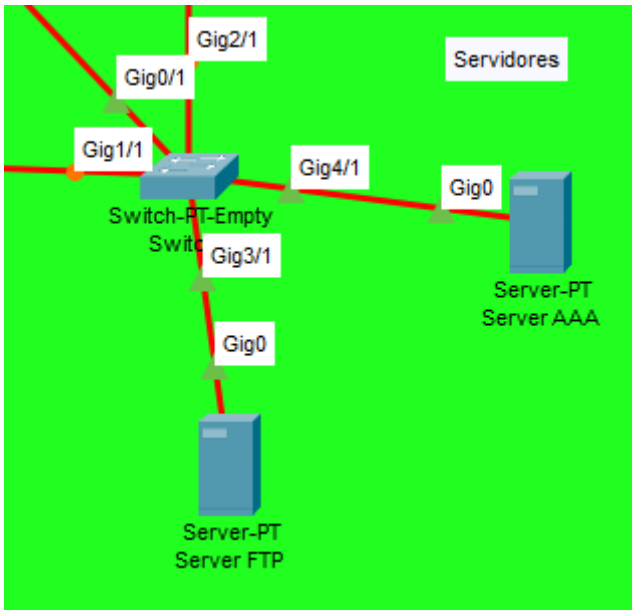

Cloud-PT
Cloud1
Eth6
Fa0/1
Gig0/1/0
Gig0/3/0
10.0.254.0/23
Fa0/0
Gig1/1
10.0.254.1/23
Gig1/2
Fa4/1
Gig3/1
Gig1/1
Gig0
Gig0
Gig2/1
Gig0
Server-PT
Server WEB
Server-PT
Server Correo
Server-PT
Server DNS

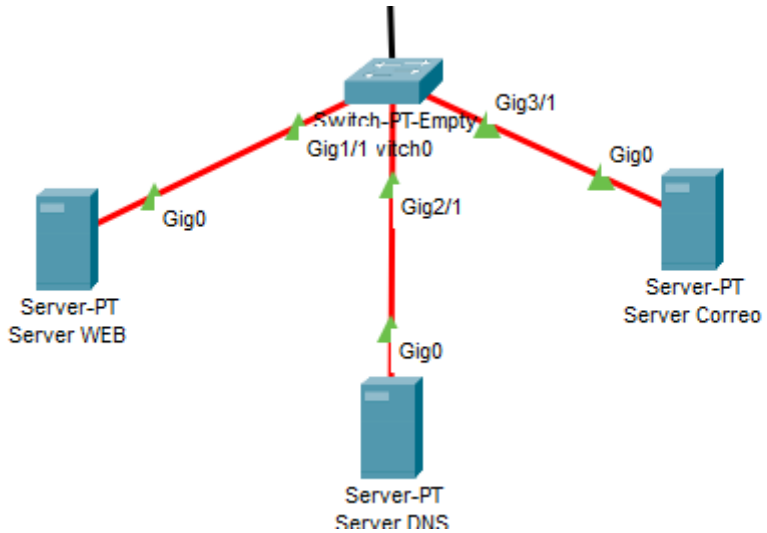

Monitoreo y transporte
Ciudadania
Emergencias
RGB LED IoT3(2)
RGB LED IoT4(2)
RGB LED IoT5(2)
RGB LED IoT4
RGB LED IoT5
RGB LED IoT3(1)
RGB LED IoT4(1)
RGB LED IoT5(1)
MCU-PT MCU0
MCU-PT MCU0(1)
Smoke Detector IoT27
Humidity Monitor IoT28
Temperature Monitor IoT26
Home Speaker IoT8
Webcam IoT9
Webcam IoT10
Appliance IoT11
Fan IoT12
Battery IoT13
Solar Panel IoT14
Power Meter IoT6
Power Meter IoT6(1)
Wind Turbine IoT0
LED IoT7
PC-PT PC1
PC-PT PC4
IP Phone0
Server-PT Server3
Server-PT Server6

7.1 Construcción de la Topología

Hemos creado servidores FTP, HTTP, DNS y AAA para almacenar datos autentificar al usuario hacer web proteger la web y traducir el dominio por la dirección ip correspondiente. También vpn, algunos acls y configuración en los firewalls.

Aquí algunas pruebas:



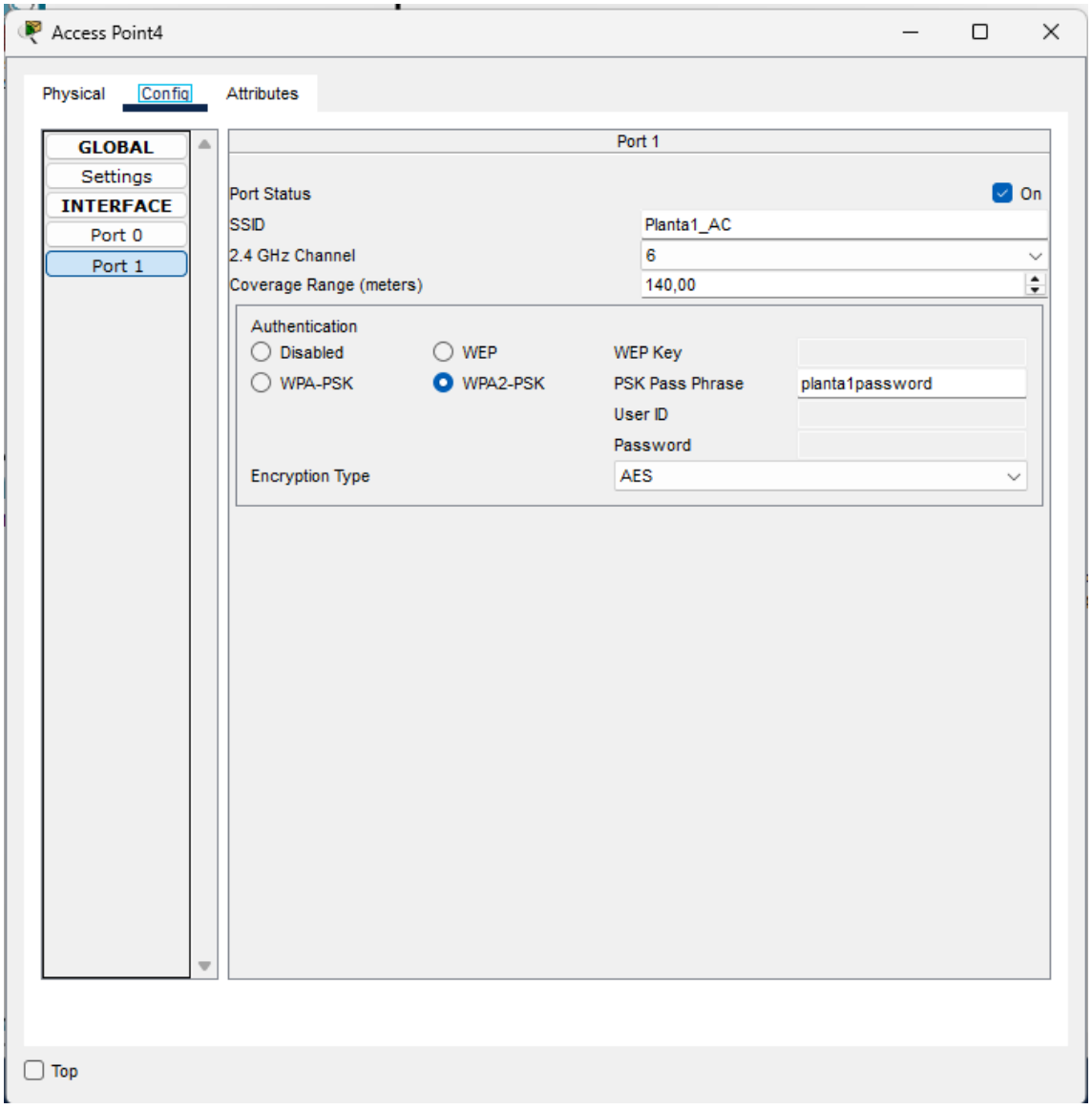


El ACL en un firewall:

```
ciscoasa(config)#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list outside-in; 1 elements; name hash: 0x85d4ba4a
access-list outside-in line 1 extended permit ip 10.0.0.0 255.0.0.0 any(hitcnt=0)
0xd5bc6bc0
ciscoasa(config)#
ciscoasa#
```

7.2 Configuración de Protocolos y Servicios

Capturas de pruebas del funcionamiento de la red y su configuración:
La configuración de un ACS, todos siguen el mismo patron:



La web de la dmz: