DOCUMENTACIÓN TÉCNICA DE RED

Práctica Final

Descripción breve

Documento técnico que describe la implementación, configuración y seguridad de una red empresarial simulada en Cisco Packet Tracer, Incluyendo enrutamiento OSPF, servicios de red y segmentación por VLANs

Miguel Angel Adames Morillo

20240779@itla.edu.do

Indice

RESUMEN EJECUTIVO

Este documento constituye la especificación técnica completa de una red LAN corporativa diseñada para emular un entorno empresarial escalable y seguro. La infraestructura implementa tecnologías avanzadas de networking que garantizan operación estable, gestión eficiente y protección de datos, cumpliendo con los estándares actuales de la industria.

La arquitectura de red se fundamenta en tres pilares principales: segmentación lógica mediante VLANs, enrutamiento dinámico con OSPF para optimización de tráfico, y servicios centralizados de conectividad. Se ha desplegado una topología jerárquica que integra routers de distribución (configurados con metodología router-on-a-stick) y switches multicapa interconectados mediante enlaces troncales 802.1Q, permitiendo el transporte eficiente de múltiples dominios de broadcast mientras se mantiene aislamiento de seguridad.

Para garantizar disponibilidad de servicios, se implementaron protocolos clave: OSPF en el área 0 para convergencia rápida de rutas entre dispositivos de capa 3, DHCP con exclusiones específicas para asignación automática de direcciones IP, y políticas de seguridad perimetral mediante NAT overload en la conexión a Internet. La infraestructura incluye además servidores internos críticos (RADIUS para autenticación AAA y syslog para monitoreo centralizado) accesibles solo desde VLANs autorizadas mediante ACLs estratificadas.

La documentación presente detalla minuciosamente todos los componentes de la red, incluyendo:

- Diagramas topológicos físicos y lógicos
- Esquema completo de direccionamiento IP por segmento
- Configuraciones dispositivo por dispositivo en formato CLI
- Matrices de conectividad y políticas de seguridad
- Protocolos implementados con sus parámetros técnicos

Este ecosistema de red ha sido diseñado con capacidades de expansión para incorporar futuras tecnologías como QoS para priorización de tráfico, VPNs sitio-a-sitio adicionales, y virtualización de funciones de red. La información aquí contenida servirá como línea base para mantenimiento preventivo, auditorías de seguridad, y planes de crecimiento tecnológico alineados con las necesidades empresariales.

INTRODUCCIÓN

En el ámbito de las redes empresariales modernas, la correcta documentación técnica es fundamental para garantizar la operatividad, seguridad y escalabilidad de la infraestructura. Este documento presenta el diseño, configuración y buenas prácticas implementadas en una red LAN corporativa segmentada, diseñada para ofrecer conectividad segura, eficiente y de alta disponibilidad para distintos departamentos y servicios críticos.

Esta red ha sido construida bajo un enfoque jerárquico (core-distribución-acceso), integrando tecnologías esenciales como **VLANs para segmentación lógica**, **enrutamiento dinámico OSPF** para una convergencia eficiente de rutas, y servicios centralizados como **DHCP**, **autenticación AAA mediante RADIUS** y **gestión de tráfico mediante ACLs**. Además, se han implementado medidas de seguridad avanzadas, incluyendo port-security en switches, filtrado entre VLANs y túneles IPsec para comunicaciones remotas seguras.

El propósito de este documento es servir como referencia técnica completa para el equipo de TI, facilitando el mantenimiento, la resolución de incidencias y futuras expansiones. Aquí se detallan:

- La **topología física y lógica** de la red.
- Las **tablas de direccionamiento IP y VLANs**.
- Las **configuraciones específicas** de routers y switches.
- Las **políticas de seguridad** aplicadas.
- Los **protocolos y servicios** implementados.

Esta documentación no solo refleja el estado actual de la red, sino que también establece las bases para mejoras futuras, como la implementación de redundancia en gateways (HSRP/VRRP), la migración a IPv6 o la integración de soluciones SDN (Software-Defined Networking).

Con un diseño robusto y escalable, esta infraestructura está preparada para soportar las demandas de conectividad de una organización en crecimiento, garantizando altos niveles de disponibilidad, seguridad y eficiencia en la gestión de la red.

DIAGRAMA DE LA TOPOLOGIA

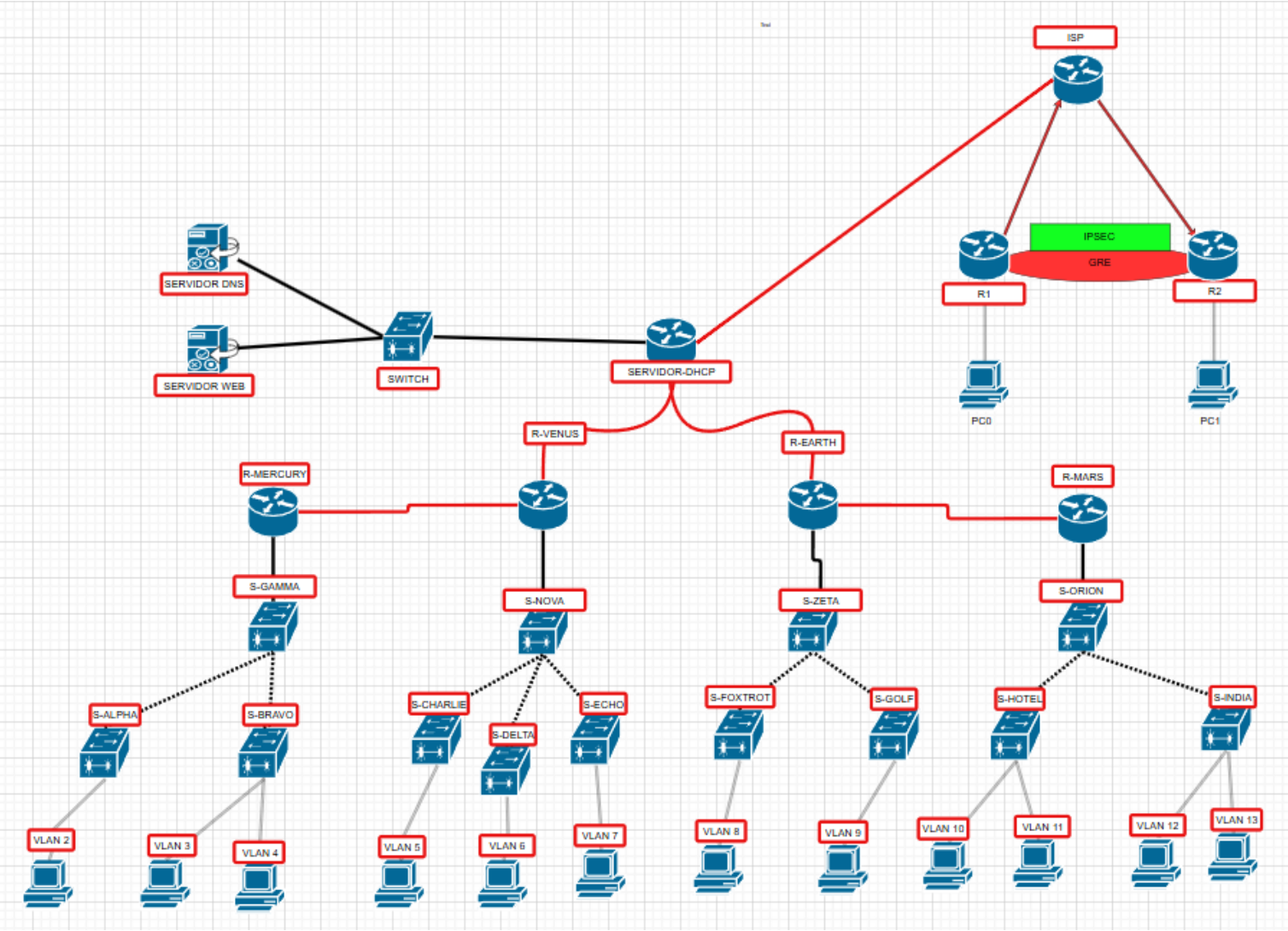

TABLA DE CONFIGURACIÓN DE RED

Dispositivo	Interfaz	IP Address	Subred	Descripción	VLAN (si aplica)
R-Mercury	G0/0.2	192.168.79.1	/28	Interfaz VLAN2	2
R-Mercury	G0/0.3	192.168.79.17	/28	Interfaz VLAN3	3
R-Mercury	G0/0.4	192.168.79.33	/28	Interfaz VLAN4	4
R-Mercury	S0/0/0	10.10.10.1	/30	Hacia R-Venus	N/A
R-Venus	G0/0.5	192.168.79.49	/28	Interfaz VLAN5	5
R-Venus	G0/0.6	192.168.79.65	/28	Interfaz VLAN6	6
R-Venus	G0/0.7	192.168.79.81	/28	Interfaz VLAN7	7
R-Venus	S0/0/0	10.10.10.2	/30	Hacia R-Mercury	N/A
R-Venus	S0/1/0	20.20.20.1	/30	Hacia DHCP-SERVER	N/A
DHCP-SERVER	S0/0/1	20.20.20.2	/30	Hacia R-Venus	N/A
DHCP-SERVER	S0/1/0	30.30.30.1	/30	Hacia R-Earth	N/A
DHCP-SERVER	G0/0	8.8.8.0	/8	Hacia Servidor WEB y DNS	N/A
DHCP-SERVER	G0/1	80.80.80.3	/24	Hacia ISP	N/A
R-Earth	G0/0.8	192.168.79.97	/28	Interfaz VLAN8	8
R-Earth	G0/0.9	192.168.79.113	/28	Interfaz VLAN9	9
R-Earth	S0/1/0	30.30.30.2	/30	Hacia DHCP-SERVER	N/A
R-Earth	S0/0/1	40.40.40.1	/30	Hacia R-Mars	N/A
R-Mars	G0/0.10	192.168.79.129	/28	Interfaz VLAN10	10
R-Mars	G0/0.11	192.168.79.145	/28	Interfaz VLAN11	11
R-Mars	G0/0.12	192.168.79.161	/28	Interfaz VLAN12	12
R-Mars	G0/0.13	192.168.79.177	/28	Interfaz VLAN13	13
R-Mars	S0/0/0	40.40.40.2	/30	Hacia R-Earth	N/A
R-ISP	G0/0	80.80.80.2	/24	Hacia DHCP-SERVER	N/A
R-ISP	Serial0/0/0	200.0.0.1	/30	Hacia R1	N/A
R-ISP	Serial0/0/1	200.0.0.6	/30	Hacia 2R	N/A
Router1 (R1)	Gig0/0	192.168.10.1	/24	LAN R1	N/A
Router1 (R1)	Serial0/0/0	200.0.0.1	/30	VPN a R2	N/A
Router2 (R2)	Gig0/0	192.168.20.1	/24	LAN R2	N/A
Router2 (R2)	Serial0/0/1	200.0.0.6	/30	VPN a R1	N/A
SW-Alpha	VLAN2	192.168.79.14	/28	Switch VLAN2	2
SW-Bravo	VLAN3	192.168.79.30	/28	Switch VLAN3	3
SW-Charlie	VLAN5	192.168.79.62	/28	Switch VLAN5	5
SW-Delta	VLAN6	192.168.79.78	/28	Switch VLAN6	6
SW-Echo	VLAN7	192.168.79.94	/28	Switch VLAN7	7
SW-Foxtrot	VLAN8	192.168.79.110	/28	Switch VLAN8	8
SW-Golf	VLAN9	192.168.79.126	/28	Switch VLAN9	9

SW-Hotel	VLAN10	192.168.79.142	/28	Switch VLAN10	10
SW-India	VLAN12	192.168.79.174	/28	Switch VLAN12	12

TABLA DE DIRECCIONAMIENTO

VLAN	Subred	Máscara	Gateway	Rango Usable	Broadcast
2	**192.168.79.0**	**255.255.255.240**	**192.168.79.1**	**192.168.79.1 – 192.168.79.14**	**192.168.79.15**
3	**192.168.79.16**	**255.255.255.240**	**192.168.79.17**	**192.168.79.17 – 192.168.79.30**	**192.168.79.31**
4	**192.168.79.32**	**255.255.255.240**	**192.168.79.33**	**192.168.79.33 – 192.168.79.46**	**192.168.79.47**
5	**192.168.79.48**	**255.255.255.240**	**192.168.79.49**	**192.168.79.49 – 192.168.79.62**	**192.168.79.63**
6	**192.168.79.64**	**255.255.255.240**	**192.168.79.65**	**192.168.79.65 – 192.168.79.78**	**192.168.79.79**
7	**192.168.79.80**	**255.255.255.240**	**192.168.79.81**	**192.168.79.81 – 192.168.79.94**	**192.168.79.95**
8	**192.168.79.96**	**255.255.255.240**	**192.168.79.97**	**192.168.79.97 – 192.168.79.110**	**192.168.79.111**
9	**192.168.79.112**	**255.255.255.240**	**192.168.79.113**	**192.168.79.113 – 192.168.79.126**	**192.168.79.127**
10	**192.168.79.128**	**255.255.255.240**	**192.168.79.129**	**192.168.79.129 – 192.168.79.142**	**192.168.79.143**

11	**192.168.79.144**	**255.255.255.240**	**192.168.79.145**	**192.168.79.145 – 192.168.79.158**	**192.168.79.159**
12	**192.168.79.160**	**255.255.255.240**	**192.168.79.161**	**192.168.79.161 – 192.168.79.174**	**192.168.79.175**
13	**192.168.79.176**	**255.255.255.240**	**192.168.79.177**	**192.168.79.177 – 192.168.79.190**	**192.168.79.191**
LAN R1	**192.168.10.0**	**255.255.255.0**	**192.168.10.1**	**192.168.10.1 – 192.168.10.254**	**192.168.10.255**
LAN R2	**192.168.20.0**	**255.255.255.0**	**192.168.20.1**	**192.168.20.1 – 192.168.20.254**	**192.168.20.255**

TABLA DE ENRUTAMIENTO

Router	Protocolo	Red de Destino	Máscara	Next Hop	Interfaz Saliente
R-Mercury	**OSPF**	**192.168.79.0**	**255.255.255.240**	**–**	**GigabitEthernet0/0.2**
	OSPF	**192.168.79.16**	**255.255.255.240**	**–**	**GigabitEthernet0/0.3**
	OSPF	**192.168.79.32**	**255.255.255.240**	**–**	**GigabitEthernet0/0.4**
	OSPF	**10.10.10.0**	**255.255.255.252**	**–**	**Serial0/0/0**
R-Venus	**OSPF**	**10.10.10.0**	**255.255.255.252**	**–**	**Serial0/0/0**
	OSPF	**20.20.20.0**	**255.255.255.252**	**–**	**Serial0/1/0**
	OSPF	**192.168.79.48**	**255.255.255.240**	**–**	**GigabitEthernet0/0.5**

	OSPF	**192.168.79.64**	**255.255.255.240**	**–**	**GigabitEthernet0/0.6**
	OSPF	**192.168.79.80**	**255.255.255.240**	**–**	**GigabitEthernet0/0.7**
DHCP-Server	**OSPF**	**8.8.8.0**	**255.0.0.0**	**–**	**GigabitEthernet0/0**
	OSPF	**80.80.80.0**	**255.255.255.0**	**–**	**GigabitEthernet0/1**
	OSPF	**20.20.20.0**	**255.255.255.252**	**–**	**Serial0/0/1**
	OSPF	**30.30.30.0**	**255.255.255.252**	**–**	**Serial0/1/0**
R-Earth	**OSPF**	**30.30.30.0**	**255.255.255.252**	**–**	**Serial0/1/0**
	OSPF	**40.40.40.0**	**255.255.255.252**	**–**	**Serial0/0/1**
	OSPF	**192.168.79.96**	**255.255.255.240**	**–**	**GigabitEthernet0/0.8**
	OSPF	**192.168.79.112**	**255.255.255.240**	**–**	**GigabitEthernet0/0.9**
R-Mars	**OSPF**	**40.40.40.0**	**255.255.255.252**	**–**	**Serial0/0/0**
	OSPF	**192.168.79.128**	**255.255.255.240**	**–**	**GigabitEthernet0/0.10**
	OSPF	**192.168.79.144**	**255.255.255.240**	**–**	**GigabitEthernet0/0.11**
	OSPF	**192.168.79.160**	**255.255.255.240**	**–**	**GigabitEthernet0/0.12**
	OSPF	**192.168.79.176**	**255.255.255.240**	**–**	**GigabitEthernet0/0.13**
ISP	**–**	**80.80.80.0**	**255.255.255.0**	**–**	**GigabitEthernet0/0**
	–	**200.0.0.0/30**	**255.255.255.252**	**–**	**Serial0/0/0**
	–	**200.0.0.4/30**	**255.255.255.252**	**–**	**Serial0/0/1**
Router1 (R1)	**Static**	**0.0.0.0/0**	**0.0.0.0**	**200.0.0.2**	**Serial0/0/0**
	Static	**192.168.20.0**	**255.255.255.0**	**10.10.10.2**	**Tunnel0**
Router2 (R2)	**Static**	**0.0.0.0/0**	**0.0.0.0**	**200.0.0.5**	**Serial0/0/1**

	Static	**192.168.10.0**	**255.255.255.0**	**10.10.10.1**	**Tunnel0**

CONFIGURACIÓN DETALLADA DE ROUTERS Y SWITCHES

1. Switch Inter

- **Hostname**: Inter
- **VLANs**: Solo VLAN1 activa (nativa)
- **Interfaces**:
  - Todas las FastEthernet (0/1-0/24) y GigabitEthernet (0/1-0/2) sin configuración específica
  - VLAN1 con IP 8.8.8.5/8
- **Seguridad**:
  - AAA con autenticación RADIUS (servidor en 8.8.8.9) y local
  - Usuarios locales: supportrecov y supportrecov2
  - SSH versión 2 habilitado
- **Spanning Tree**: Modo PVST con extended system-id
- **Gateway por defecto**: 8.8.8.1
- **Logging**: Envía traps a 8.8.8.9

2. Router DHCP (Server-dhcp)

- **Hostname**: Server-dhcp
- **Funcionalidad DHCP**:
  - Pools para VLANs 2-13 con rangos específicos
  - Direcciones excluidas en cada VLAN
  - DNS server 8.8.8.8 para todos los pools

- **Interfaces**:
    - Gig0/0: 8.8.8.0/8 (NAT inside)
    - Gig0/1: 80.80.80.3/24 (NAT outside)
    - Serial0/0/0: Deshabilitada
    - Serial0/0/1: 20.20.20.2/30 (NAT inside)
    - Serial0/1/0: 30.30.30.1/30 (NAT inside)
- **NAT**:
    - Overload en Gig0/1 para tráfico de la lista de acceso 1
    - ACL 1 permite todo excepto 80.80.80.0/24
- **OSPF**:
    - Router ID 3.3.3.3
    - Anuncia redes 20.20.20.0/30, 30.30.30.0/30, 8.8.8.0/8 y 80.80.80.0/24
- **Seguridad**:
    - AAA con RADIUS
    - Banner MOTD de acceso restringido

3. Router ISP

- **Hostname**: ISP
- **Interfaces**:
    - Gig0/0: 80.80.80.2/24
    - Serial0/0/0: 200.0.0.2/30
    - Serial0/0/1: 200.0.0.5/30

- **Seguridad**:
    - Contraseñas en consola y líneas VTY

    - Banner MOTD con información de monitoreo
- **Sin routing dinámico configurado**

4. Router R1

- **Hostname**: Router1
- **Funcionalidad DHCP**: Pool para LAN_R1 (192.168.10.0/24)
- **VPN**:
    - Configuración IPSec con transform-set TSET (AES y SHA-HMAC)
    - Crypto map "VPN" apuntando a 200.0.0.6
    - ISAKMP policy 10 con autenticación pre-shared key "cisco123"
- **Interfaces**:
    - Gig0/0: 192.168.10.1/24 (NAT inside)
    - Serial0/0/0: 200.0.0.1/30 (NAT outside)
    - Tunnel0: 10.10.10.1/30 (GRE over IPSec)
- **NAT**: Overload en Serial0/0/0 para tráfico de 192.168.10.0/24
- **Routing**:
    - Ruta estática por defecto a 200.0.0.2
    - Ruta estática para 192.168.20.0/24 a través del túnel

5. Router R2

- **Hostname**: Router2
- **Funcionalidad DHCP**: Pool para LAN_R2 (192.168.20.0/24)

- **VPN**:
    - Configuración IPSec espejo de R1

- Mismo transform-set y pre-shared key

- **Interfaces**:
  - Gig0/0: 192.168.20.1/24 (NAT inside)
  - Serial0/0/1: 200.0.0.6/30 (NAT outside)
  - Tunnel0: 10.10.10.2/30 (GRE over IPSec)
- **NAT**: Overload en Serial0/0/1 para tráfico de 192.168.20.0/24
- **Routing**:
  - Ruta estática por defecto a 200.0.0.5
  - Ruta estática para 192.168.10.0/24 a través del túnel

6**. Router Mercurry (R-Mercury)**

- **Hostname**: R-Mercury
- **Interfaces**:
  - Subinterfaces Gig0/0.2 (VLAN2), .3 (VLAN3), .4 (VLAN4)
  - Serial0/0/0: 10.10.10.1/30
- **OSPF**:
  - Router ID 1.1.1.1
  - Anuncia redes 10.10.10.0/30, VLAN2, VLAN3 y VLAN4
- **ACLs**:
  - ACL 2: Permite solo 192.168.79.2 en VLAN4
  - ACL 3: Niega 192.168.79.18 en VLAN3
- **Seguridad**: AAA con RADIUS, logging a 8.8.8.9

7. Switch Gamma (SW-Gamma)

- **Hostname**: SW-Gamma

- **VLANs**: 2, 3, 4, 99, 100
- **Trunking**:
  - Gig0/1: VLANs 2,99
  - Gig1/1: VLANs 3-4,99
  - Gig2/1: VLANs 2-4,99 (DHCP snooping trust)
- **DHCP Snooping**: Habilitado para VLANs 2-4
- **Seguridad**:
  - VTP modo transparente
  - Banner MOTD de acceso restringido

8. Switch Alpha (SW-Alpha)

- **Hostname**: SW-Alpha
- **VLANs**: 2, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN2 con port-security (MAC sticky)
  - Portfast y bpduguard habilitados
- **Trunking**: Gig0/1 para VLANs 2,99
- **Seguridad**:
  - AAA con RADIUS
  - SSH habilitado
  - VLAN2 con IP 192.168.79.14/28

9. Switch Bravo (SW-Bravo)

- **Hostname**: SW-Bravo
- **VLANs**: 3, 4, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN3 con port-security
  - Fa0/3-0/4: VLAN4 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN3 con IP 192.168.79.30/28
  - Gateway 192.168.79.17

10. Router Venus (R-Venus)

- **Hostname**: R-Venus
- **Interfaces**:
  - Subinterfaces Gig0/0.5 (VLAN5), .6 (VLAN6), .7 (VLAN7)
  - Serial0/0/0: 10.10.10.2/30
  - Serial0/1/0: 20.20.20.1/30
- **OSPF**:
  - Router ID 2.2.2.2
  - Anuncia VLANs 5-7 y enlaces seriales
- **ACLs**:
  - ACL 110: Niega ping desde VLAN5 a 8.8.8.9
  - ACL 111: Niega tráfico desde VLAN6
- **Seguridad**: AAA con RADIUS

11. Switch Nova (SW-Nova)

- **Hostname**: SW-Nova
- **VLANs**: 5, 6, 7, 99, 100
- **Trunking**:
  - Gig0/1: VLAN5,99
  - Gig1/1: VLAN6,99
  - Gig2/1: VLAN5-7,99 (DHCP snooping trust)
- **DHCP Snooping**: Habilitado para VLANs 5-7
  - 12. Switch Charlie (SW-Charlie)
- **Hostname**: SW-Charlie
- **VLANs**: 5, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN5 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN5 con IP 192.168.79.62/28
  - Gateway 192.168.79.49

13. Switch Delta (SW-Delta)

- **Hostname**: SW-Delta
- **VLANs**: 6, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN6 con port-security

- **Seguridad**:
  - AAA con RADIUS
  - VLAN6 con IP 192.168.79.78/28
  - Gateway 192.168.79.65

14. Switch Echo (SW-Echo)

- **Hostname**: SW-Echo
- **VLANs**: 7, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN7 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN7 con IP 192.168.79.94/28
  - Gateway 192.168.79.81

15. Router Earth (R-Earth)

- **Hostname**: R-Earth
- **Interfaces**:
  - Subinterfaces Gig0/0.8 (VLAN8), .9 (VLAN9)
  - Serial0/0/1: 40.40.40.1/30
  - Serial0/1/0: 30.30.30.2/30
- **OSPF**:
  - Router ID 4.4.4.4
  - Anuncia VLANs 8-9 y enlaces seriales

- **ACLs**:
  - ACL 113: Controla tráfico entre VLAN8 y VLAN9 (permite DNS, niega FTP y otro tráfico IP)
- **Seguridad**: AAA con RADIUS

16. Switch Zeta (SW-Zeta)

- **Hostname**: SW-Zeta
- **VLANs**: 8, 9, 99, 100
- **Trunking**:
  - Gig0/1: VLAN8,99
  - Gig1/1: VLAN9,99
  - Gig2/1: VLAN8-9,99 (DHCP snooping trust)
- **DHCP Snooping**: Habilitado para VLANs 8-9
  - 17. Switch Foxtrot (SW-Foxtrot)
- **Hostname**: SW-Foxtrot
- **VLANs**: 8, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN8 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN8 con IP 192.168.79.110/28
  - Gateway 192.168.79.97

18. Switch Golf (SW-Golf)

- **Hostname**: SW-Golf
- **VLANs**: 9, 99, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN9 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN9 con IP 192.168.79.126/28
  - Gateway 192.168.79.113
  - CDP deshabilitado globalmente

19. Router Mars (R-Mars)

- **Hostname**: R-Mars
- **Interfaces**:
  - Subinterfaces Gig0/0.10 (VLAN10), .11 (VLAN11), .12 (VLAN12), .13 (VLAN13)
  - Serial0/0/0: 40.40.40.2/30
- **OSPF**:
  - Router ID 5.5.5.5
  - Anuncia VLANs 10-13 y enlace serial
- **ACLs**:
  - ACL 115: Estricto control en VLAN12-13 (permite OSPF, SSH, ICMP, DHCP)
  - ACL 117: Niega tráfico desde 192.168.79.146 (VLAN11)
  - ACL 118: Niega ICMP a 80.80.80.0/24

- **Seguridad**:
  - AAA con RADIUS
  - SSH requerido para VTY 0-4

20. Switch Orion (SW-Orison)

- **Hostname**: SW-Orison
- **VLANs**: 10, 11, 12, 13, 99, 100
- **Trunking**:
  - Gig0/1: VLAN10-11,99
  - Gig1/1: VLAN12-13,99
  - Gig2/1: VLAN10-13,99 (DHCP snooping trust)
- **DHCP Snooping**: Habilitado para VLANs 10-13

21. Switch Hotel (SW-Hotel)

- **Hostname**: SW-Hotel
- **VLANs**: 10, 11, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN10 con port-security
  - Fa0/3-0/4: VLAN11 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN10 con IP 192.168.79.142/28
  - Gateway 192.168.79.129

22. Switch India (SW-India)

- **Hostname**: SW-India
- **VLANs**: 12, 13, 100
- **Puertos**:
  - Fa0/1-0/2: VLAN12 con port-security
  - Fa0/3-0/4: VLAN13 con port-security
- **Seguridad**:
  - AAA con RADIUS
  - VLAN12 con IP 192.168.79.174/28
  - Gateway 192.168.79.161

CONFIGURACIÓN DETALLADA DE SERVIDORES

- Servicio Web (HTTP/HTTPS)
- **Estado**: Activo (On)
- **Archivos gestionados**:
  - index.html (editado)
- **Protocolos soportados**:
  - HTTP
  - HTTPS (habilitado)
- Servicio AAA (Autenticación, Autorización y Contabilidad)
- **Configuración RADIUS**:
  - Puerto: 1645
  - Clave compartida: Cisco123 para todos los dispositivos

Dispositivos registrados:

Switches:

- SW-Alpha (192.168.79.14)
- SW-Bravo (192.168.79.30)
- SW-Charlie (192.168.79.62)
- SW-Delta (192.168.79.78)
- SW-Echo (192.168.79.94)
- SW-Foxtrot (192.168.79.110)
- SW-Golf (192.168.79.126)
- SW-Hotel (192.168.79.142)
- SW-India (192.168.79.174)

Routers:

- R-Venus (20.20.20.1)
- R-Earth (30.30.30.2)
- R-Mars (40.40.40.2)
- R-Mercury (10.10.10.1)

Usuarios locales:

Username	Password
Carlos	Edwin#21
Edward	Arturo01
Ikaury	Ikaury
Javier	Jeedano
Jona	Muyayos
Manuel	Angel07

Miguel	Cisco123
Muyayos	Muyayios
Natacha	Stephanie25
Paulino	Pismael

SERVICIO FTP

Configuración:

- Servidor habilitado
- Acceso RADIUS para autenticación
- Dispositivos autorizados:
  - R-Mercury (10.10.10.1)
- Clave compartida: Cisco123

TABLA DE PUERTOS Y SERVICIOS

Dispositivo	Servicio	Puerto	Protocolo	Descripción
Todos los dispositivos	**SSH**	**22**	**TCP**	**Acceso seguro a dispositivos**
	RADIUS	**1645**	**UDP**	**Autenticación AAA**
	Syslog	**-**	**UDP**	**Envío de logs a 8.8.8.9**
Router DHCP	**DHCP**	**67/68**	**UDP**	**Servicio DHCP para VLANs 2-13**
	NAT	**-**	**-**	**Traducción de direcciones**
	OSPF	**89**	**TCP/IP**	**Enrutamiento dinámico (Área 0)**
Routers R1/R2	**IPsec**	**500/4500**	**UDP**	**VPN Site-to-Site**
	GRE	**-**	**Protocolo 47**	**Túneles GRE**

Switches	**DHCP Snooping**	**-**	**-**	**Protección contra ataques DHCP**
	Port Security	**-**	**-**	**Seguridad por puerto con MAC sticky**
Servidor RADIUS	**AAA**	**1812/1813**	**UDP**	**Autenticación y autorización / Contabilidad**

DOCUMENTACIÓN DE LA CONFIGURACIÓN

La red implementada consiste en una infraestructura compleja con múltiples dispositivos Cisco, incluyendo switches y routers, configurados para proporcionar conectividad, seguridad y servicios de red. La configuración muestra una red segmentada en VLANs con múltiples subredes, utilizando OSPF como protocolo de enrutamiento dinámico.

Elementos clave de la configuración:

1. **Segmentación de red:**
   - Múltiples VLANs configuradas (VLAN 2-13)
   - Subredes /28 para cada VLAN (ej. 192.168.79.0/28, 192.168.79.16/28, etc.)
   - VLAN nativa 99 para tráfico de administración
2. **Servicios DHCP:**
   - Configuración de pools DHCP para cada VLAN
   - Direcciones excluidas para dispositivos de infraestructura
   - Helper addresses configurados en interfaces de router
3. **Enrutamiento:**
   - Protocolo OSPF implementado en todos los routers
   - Router IDs configurados (1.1.1.1, 2.2.2.2, etc.)
   - Rutas estáticas para tráfico específico
4. **VPN Site-to-Site:**
   - Configuración IPSec entre Router1 y Router2
   - Tunnel GRE sobre IPSec
   - Transform set con AES y SHA-HMAC

DOCUMENTACIÓN DE SEGURIDAD IMPLEMENTADA

1. Autenticación y Autorización

- **AAA (Authentication, Authorization, Accounting)**:
  - Configuración AAA en todos los dispositivos
  - Autenticación contra servidor RADIUS (8.8.8.9)
  - Autenticación local como fallback
  - Accounting para registrar actividades de usuarios
- **Contraseñas**:
  - Contraseñas encriptadas usando MD5 (secret 5)
  - Contraseñas complejas para acceso a consola y líneas VTY
  - Usuarios administrativos con privilegio 15

2. Seguridad de Puertos en Switches

- **Port Security**:
  - Direcciones MAC sticky configuradas en puertos de acceso
  - Violación de seguridad activa (shutdown por defecto)
  - Protección contra MAC flooding
- **BPDU Guard y PortFast**:
  - Habilitado en todos los puertos de acceso
  - Previene ataques STP y bucles de red
- **DHCP Snooping**:
  - Implementado en switches para prevenir ataques DHCP spoofing
  - Puertos de confianza configurados apropiadamente

LISTAS DE CONTROL DE ACCESO (ACLS)

Las Listas de Control de Acceso (ACLs) implementadas en esta red tienen como objetivo principal fortalecer la seguridad interna, limitar el tráfico no deseado entre VLANs y garantizar el cumplimiento de las políticas establecidas para el uso de servicios específicos. Se utilizaron tanto ACLs estándar como extendidas, aplicadas en entradas y salidas de interfaces clave según el flujo del tráfico.

Objetivos principales de las ACLs:

- **Segmentación de tráfico entre VLANs**, permitiendo solo comunicación autorizada.
- **Permitir acceso exclusivo a servicios críticos** (por ejemplo, DNS, HTTP, SSH).
- **Bloqueo de IPs y rangos específicos** considerados inseguros o no autorizados.
- **Filtrado de protocolos sensibles** como ICMP, SSH y tráfico hacia redes públicas.

Ejemplos notables de ACLs configuradas:

- **ACL 2:** Permite exclusivamente la IP 192.168.79.2 en la salida hacia VLAN 4.
- **ACL 3:** Niega el acceso a la IP 192.168.79.18 desde la VLAN 3.
- **ACL 4:** Restringe el rango de direcciones 192.168.79.0/28 hacia VLAN 5, bloqueando accesos no autorizados.
- **ACL 110:** Bloquea tráfico ICMP (ping) desde VLAN 5 hacia el servidor público 8.8.8.9, previniendo posibles escaneos.
- **ACL 111:** Niega completamente el tráfico de entrada proveniente de VLAN 6, aislándola por completo.
- **ACL 112:** Permite libre comunicación desde VLAN 7 hacia VLAN 8, necesaria para servicios compartidos.
- **ACL 113:** Autoriza únicamente tráfico DNS entre VLAN 8 y VLAN 9, y bloquea tráfico FTP hacia 8.8.8.9.
- **ACL 115:** Aplica reglas estrictas para la VLAN 12, permitiendo únicamente tráfico SSH desde la IP 192.168.79.162.
- **ACL 116:** Permite tráfico HTTP hacia el servidor interno únicamente desde VLAN 10, controlando el acceso web.
- **ACL 117:** Bloquea todo el tráfico proveniente de la IP sospechosa 192.168.79.146.
- **ACL 118:** Limita el tráfico ICMP generado desde el router hacia la red externa (ISP), reduciendo riesgos de exposición.

4. Seguridad de Protocolos de Administración

- **SSH**:
  - Versión 2 habilitada en todos los dispositivos
  - Acceso restringido a líneas VTY
  - Dominio configurado (Miguel.com)
- **Deshabilitación de servicios innecesarios**:
  - CDP deshabilitado en puertos de acceso
  - Servicios no esenciales desactivados (ej. HTTP server)

5. Protección de Capa 2

- **STP Hardening**:
  - PVST como protocolo Spanning Tree
  - System-ID extendido habilitado
  - BPDU Guard en puertos de acceso

- **VTP Seguro**:
  - Modo transparente configurado en switches
  - Previene modificaciones no autorizadas en base de datos VLAN

6. NAT y Filtrado

- **NAT Overload**:
  - Configurado en routers de borde
  - Listas de acceso para definir tráfico a traducir
- **Filtrado de tráfico**:
  - Reglas específicas para tráfico entrante/saliente
  - Bloqueo de tráfico no deseado hacia/desde Internet

7. Monitoreo y Registro

- **Syslog**:
    - Configuración de logging a servidor 8.8.8.9
    - Nivel de logging debugging
- **Banners**:
    - Banners MOTD configurados con advertencias legales
    - Mensajes de acceso restringido

BUENAS PRÁCTICAS IMPLEMENTADAS

1. **Principio de mínimo privilegio**:
    - Usuarios tienen solo los permisos necesarios
    - Acceso restringido a funciones administrativas
2. **Defensa en profundidad**:
    - Múltiples capas de seguridad (ACLs, port security, AAA)
    - Controles en diferentes niveles de la red
3. **Segmentación estricta**:
    - VLANs separadas para diferentes propósitos
    - Control de tráfico inter-VLAN
4. **Protección contra amenazas comunes**:
    - DHCP spoofing
    - MAC flooding
    - STP attacks
    - Acceso no autorizado
5. **Controles de redundancia**:
    - Autenticación local como fallback de RADIUS
    - Múltiples métodos de autenticación

INVENTARIO DE EQUIPOS

Routers Cisco 1941

- **Cantidad**: 7 + 1 ISP
- **Puertos**: entre 2 y 4 seriales, 2 GigabitEthernet
- **MAC**: No se modificaron y se dejaron las generadas por Packet Tracer.
- **Función**: Enrutamiento inter-VLAN, OSPF, NAT, ACL y DHCP Relay.

Nombre	MAC
ISP	00D0.D305.0EE4
DHCP-SERVER	00D0.D304.CC3C
R-Mercury	0030.A3CE.736E
R-Venus	0003.E498.D273
R-Earth	00D0.975D.DC39
R-Mars	00E0.B007.BC44
R1	00D0.FF68.2C01
R2	0001.96E1.69BB

Switches Cisco 2960-24TT

- **Cantidad**: 13
- **Puertos**: 24 FastEthernet, 2 GigabitEthernet
- **MAC**: No se modificaron y se dejaron las generadas por Packet Tracer.
- **Función**: VLAN, Port Security, STP, DHCP Snooping

Nombre	MAC
SW-Alpha	00E0.B0CC.B58D
SW-Bravo	0002.1698.E326
SW-Charlie	0001.6314.CC00
SW-Delta	0010.1159.9EA2
SW-Echo	00D0.D31B.5B25
SW-Foxtrot	0000.0C9C.5E8E
SW-Golf	0060.2F29.271B
SW-Hotel	000A.F350.278D
SW-India	00D0.D371.7D7C
SW-Gamma	00D0.9763.5C49
SW-Nova	0060.47A5.D259
SW-Zeta	000A.41C0.41B4
SW-Orio	00E0.A360.CB37

Servidores Genéricos

- **Cantidad**: 2
- **Conexión**: FastEthernet a switch
- **Función**: Uno actúa como servidor DNS, el otro como servidor WEB, FTP y AAA
- **MAC DNS**: 00E0.8F75.494E
- **MAC WEB**: 00E0.F984.8AA2

PCs Genéricas

- **Cantidad**: 24 (2 por VLAN) + 2 por la LAN de R1 y R2
- **Conexión**: FastEthernet a switches
- **Función**: Clientes en VLANs

- **MAC**: Se quedaron como las proporciono Packet Tracer

Nombre	MAC
PC-A1	0000.0C89.13C9
PC-A2	00D0.BABA.EB16
PC-A3	0006.2AED.446C
PC-A4	0002.4AB2.1364
PC-A5	00D0.FF74.01D0
PC-A6	0002.17C3.B63C
PC-A7	00D0.FF06.9547
PC-A8	000C.CFBA.E09A
PC-A9	0002.165E.484D
PC-A10	0001.637B.4151
PC-A11	0001.C912.7A6D
PC-A12	0001.C943.2207

Nombre	MAC
PC-B1	0002.160C.D262
PC-B2	0002.4AD1.97E5
PC-B3	0090.2B88.5261
PC-B4	000D.BD11.85A3
PC-B5	000B.BE62.5BE4
PC-B6	000A.F37A.82EB
PC-B7	00D0.FFB2.6A85
PC-B8	0050.0FA8.3454
PC-B9	0090.0C73.B122
PC-B10	0001.C973.B60B
PC-B11	0060.2FAD.29B9
PC-B12	0000.0C77.47BC

Nombre	MAC
LAN-R1	0030.A33E.AC4E
LAN-R2	000C.CF79.03E2

NOMENCLATURA DE LOS NOMBRES DE EQUIPOS

- **Routers**: R-[Nombre de planeta] (ej. R-Mars)
- **Switches**: SW-[Alfabeto/clave] (ej. SW-Alpha, SW-Bravo)
- **Interfaces**: [Tipo][Puerto] (ej. G0/0.1, F0/5)
- **VLANs**: Números correlativos según segmento de red

PROBLEMAS CONOCIDOS O RIESGOS POTENCIALES

PROBLEMAS CONOCIDOS

- **Interoperabilidad con equipos antiguos**: Algunos switches pueden tener problemas de compatibilidad con dispositivos que no soportan VLAN tagging (802.1Q).
- **Rendimiento en enlaces seriales**: Los enlaces WAN con ancho de banda limitado (ej. 2 Mbps) pueden saturarse con tráfico inter-VLAN.
- **Dependencia del servidor RADIUS (8.8.8.9)**: Si falla, la autenticación AAA depende del modo local, lo que podría generar cuellos de botella.
- **Vulnerabilidad en contraseñas MD5**: Las contraseñas están cifradas con MD5, que es considerado inseguro hoy en día.

LIMITACIONES DEL DISEÑO

Limitaciones técnicas

- **Escalabilidad limitada**: El diseño actual soporta hasta 13 VLANs, pero si crece la red, puede requerir reconfiguración de subnets.
- **Single Point of Failure (SPOF)**: El servidor RADIUS (8.8.8.9) es crítico; si falla, afecta la autenticación AAA.
- **NAT Overload en un solo router**: El router ISP maneja todo el tráfico saliente, lo que puede generar congestión.

REFERENCIAS TÉCNICAS

- Cisco Networking Academy - CCNA
- RFC 2131 - DHCP
- RFC 2328 - OSPFv2
- NIST SP 800-41 - Directrices de configuración de routers
- Cisco SAFE Arquitectura de seguridad en switches y routers
- NIST SP 800-53 Controles de seguridad para AAA y logging
- Cisco Best Practices Configuración de OSPF, Port Security y DHCP Snooping

GLOSARIO O LEYENDA

Término/Acrónimo	Definición
AAA	**Authentication, Authorization, Accounting** (Autenticación, Autorización y Registro)
ACL	Access Control List (Lista de Control de Acceso)
BPDU	**Bridge Protocol Data Unit** (Unidad de Datos del Protocolo de Puente)
BPDU Guard	**Protección contra ataques de Spanning Tree Protocol** (Bloquea BPDUs en puertos de acceso)
CDP	**Cisco Discovery Protocol** (Protocolo de Descubrimiento de Cisco, usado para identificar dispositivos vecinos)
DAI	**Dynamic ARP Inspection** (Inspección dinámica de ARP para prevenir ataques de envenenamiento)
DHCP	**Dynamic Host Configuration Protocol** (Protocolo para asignación automática de direcciones IP)
DHCP Snooping	**Filtrado de tráfico DHCP malicioso** (Previene servidores DHCP no autorizados)
DTP	**Dynamic Trunking Protocol** (Protocolo para negociación automática de enlaces troncales)
NAT	**Network Address Translation** (Traducción de Direcciones de Red para acceso a Internet)
OSPF	**Open Shortest Path First** (Protocolo de enrutamiento dinámico basado en el algoritmo Dijkstra)
Port Security	**Restricción de direcciones MAC en puertos de switch** (Previene conexiones no autorizadas)
SPOF	**Single Point of Failure** (Punto Único de Falla en la red)
STP	**Spanning Tree Protocol** (Protocolo para evitar bucles en redes conmutadas)
VLAN	**Virtual Local Area Network** (Segmentación lógica de redes en switches)
VLAN Hopping	**Ataque para saltar entre VLANs no autorizadas** (Explota configuraciones incorrectas de trunking)

CONCLUSIÓN

El diseño e implementación de esta red corporativa demuestra un enfoque integral que combina segmentación avanzada, enrutamiento dinámico, seguridad robusta y alta disponibilidad. A través de VLANs (/28) y OSPF, se logró una estructura escalable y eficiente, mientras que las políticas de seguridad (AAA, ACLs, Port Security, DHCP Snooping) garantizan la protección contra amenazas internas y externas.

Logros Clave

1. **Segmentación Efectiva:**
    - 13 VLANs con subredes dedicadas, optimizando el espacio de direcciones y aislando tráfico crítico.
    - Switches configurados con VLANs de administración (99) y troncales para evitar VLAN hopping.
2. **Conectividad y Redundancia:**
    - OSPF como protocolo de enrutamiento dinámico, asegurando convergencia rápida y tolerancia a fallos.
    - VPN IPSec/GRE entre R1 y R2 para conexión segura de LANs remotas (192.168.10.0/24 y 192.168.20.0/24).
3. **Seguridad Multinivel:**
    - Autenticación centralizada con RADIUS (8.8.8.9) y fallback local.
    - ACLs restrictivas (ej: ACL 113 bloquea FTP entre VLAN8 y VLAN9).
    - Hardening de switches: Port Security, BPDU Guard, y deshabilitación de CDP.
4. **Servicios de Red:**
    - DHCP escalable con pools para cada VLAN y exclusiones para dispositivos críticos.
    - NAT Overload en el router ISP para acceso a Internet, filtrado por ACLs.

Limitaciones y Mejoras Futuras

- Resiliencia: Implementar un servidor RADIUS secundario para evitar SPOF.
- Rendimiento: Migrar enlaces seriales a tecnologías de mayor ancho de banda (ej: MPLS).
- Seguridad: Actualizar cifrado de contraseñas a SHA-256 en lugar de MD5.

Impacto del Diseño

Esta arquitectura no solo cumple con los estándares de Cisco y las RFCs relevantes (OSPFv2, DHCP), sino que también sigue las mejores prácticas de NIST y Cisco SAFE. La combinación de segmentación, enrutamiento dinámico y controles de seguridad crea una red empresarial confiable, auditable y preparada para escalar.

En conclusión, el proyecto refleja un equilibrio entre funcionalidad, seguridad y mantenibilidad, sirviendo como base para futuras expansiones o integraciones con tecnologías emergentes (SDN, IoT). Las lecciones aprendidas —como la importancia de la redundancia en AAA— serán clave para iteraciones futuras.