



OZonE  
CIBERSECURITY

# VLSM Y CIBERSEGURIDAD

Guia de subnetting con ULSM  
y su importancia en  
ciberseguridad con ejemplos.

Ruben Apablaza Muñoz  
-OzonE-

## INTRODUCCION

Este documento nace de la necesidad de saber porque es importante para un ciberseguro/a saber “subnetear” y porque es importante VLSM para la ciberseguridad.

Saber “subnetear” con VLSM es útil en ciberseguridad porque permite entender y controlar mejor la segmentación de redes, lo que impacta directamente en la capacidad de:

- Reducir la superficie de ataque separando recursos críticos en distintas subredes.
- Aplicar políticas de firewall más precisas, dicho de otra forma, si se segmenta bien, se filtra tráfico de forma granular.
- Detectar anomalías con redes bien definidas, esto quiere decir que cualquier tráfico fuera de su rango previsto se ve de inmediato como sospechoso.
- Optimizar recursos de red, por lo tanto no vamos a desperdiciar direcciones IP, algo importante en redes corporativas grandes.

En resumen no se trata solo de **“ahorrar IPs”**, sino de diseñar redes seguras y ordenadas. Si un profesional o estudiante de ciberseguridad no domina esto, le costará entender muchas arquitecturas defensivas, auditorías o configuraciones de firewalls y routers.

En las páginas siguientes, te comarto además de las razones, y ejemplos aplicados al campo de ciberseguridad, la forma o método que a mí se me hizo mas sencillo realizar el Subneteo con VLSM.

OZONE

**EJEMPLOS EN QUE EL SUBNETTING ES UTIL EN  
CIBERSEGURIDAD (ATAQUE Y DEFENSA)**

OZONE

OZONE

## Ejemplo 1:

**Red de una universidad o empresa con segmentación por funciones**

**Escenario real:**

Una universidad tiene redes separadas para:

- Profesores: datos sensibles, acceso a servidores internos
- Estudiantes: navegación básica, correo
- Invitados: solo acceso a Internet

**¿Por qué VLSM importa aquí?**

- Cada grupo tiene diferente cantidad de hosts por lo tanto no se puede asignar /24 a todos.
- Segmentación con VLSM y aplicación de políticas de firewall distintas.

Por ejemplo:

- ***Estudiantes no pueden escanear puertos a la LAN de "Profesores".***
- ***Invitados bloqueados de todo salvo salida a Internet.***

**¿Ciberseguridad?**

- Así limitamos el movimiento lateral si alguien conecta un equipo comprometido.
- Podemos detectar un host que "salta" de una subred a otra, por lo tanto se genera la alerta inmediata.

## **Ejemplo 2:**

### **Un pentester escaneando una red mal segmentada**

#### **Escenario real:**

- Un pentester llega a una red donde todos los equipos están en una única subred **/24**.
- Desde su PC conectada en la red de “Estudiantes”, puede escanear y detectar servidores de administración o bases de datos.

#### **¿Qué pasó?**

- No usaron VLSM ni segmentaron.
- Todo está expuesto en el mismo dominio de broadcast.

#### **¿Ciberseguridad?**

- Si hubieran usado VLSM y firewalls entre subredes, el pentester no habría visto nada más allá de su segmento.

## **Ejemplo 3: Detección de anomalías desde el SOC**

### **Escenario real:**

- El equipo SOC (Security Operations Center) ve en los logs de red que una IP de la subred de "Invitados" está intentando acceder a un servidor del dominio.

### **¿Cómo lo detectaron tan rápido?**

- Porque saben que la subred 192.168.50.64/26 es solo para invitados.
- Cualquier intento desde ahí hacia recursos internos es anómalo.

### **¿Ciberseguridad?**

- Sin subneteo definido y documentado, este tipo de alerta pasa desapercibida.
- Segmentar te permite aplicar reglas SIEM más precisas.

#### **Ejemplo 4:**

#### **Firewall mal configurado por mala planificación de subredes**

#### **Escenario real:**

- Una empresa tiene servidores de producción y servidores de pruebas en la misma subred grande.
- Una regla de firewall abre un puerto a “toda la subred” para que desarrollo haga pruebas.

#### **¿Qué pasó?**

- Por no usar VLSM ni separar funciones, un error humano expone servidores productivos.

#### **¿Ciberseguridad?**

- Esto es muy común. Con VLSM, se podría haber dado /27 para pruebas y /27 para producción, aplicando reglas distintas.

#### **En resumen:**

***VLSM y subneteo no son un tema “de redes” solamente. En ciberseguridad son herramientas para diseñar redes más seguras, más vigilables y más defendibles.***

***Si no lo dominamos, no podremos auditar ni defender bien una red. Y si hacemos pentesting, no vamos a entender por qué algunas cosas no responden o están aisladas.***

OZONE

VLSM

**MI MÉTODO APLICADO**

OZONE

OZONE

## DIRECCIONAMIENTO IPv4

De acuerdo a las necesidades establecidas por "**ABC CORPORATION**" se da la siguiente dirección de **clase B: 172.16.0.0/16** a la que habrá que aplicar **VLSM** considerando la cantidad de dispositivos en cada segmento para facilitar el enrutamiento. Las necesidades de subredes son las siguientes:

- a. 860 host para la Subred\_1
  - b. 496 host para la Subred\_2
  - c. 3100 host para la Subred\_3
  - d. 63 host para la Subred\_4
  - e. 2 Sub Redes de 35 host para invitados
  - f. 3 subredes de 2 host

El primer paso que se realiza es crear un esquema de direccionamiento que permita ordenar la información entregada:

Para efectos de facilitar la tarea de cálculo de redes con VLSM, me hice una tabla de referencia para ordenar los octetos y prefijos de la red:

	OCTETO 1								OCTETO 2								OCTETO 3								OCTETO 4							
Bits	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1			
Octeto	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Binario	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
prefijo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	

A continuación, ordenamos la información de acuerdo a la cantidad de subredes solicitadas, para esto se completa como primer paso la columna de “cantidad de host” e iniciamos desde la subred más grande en orden descendente, considerando que se debe sumar a cada subred solicitada, 2 direcciones ip adicionales; una correspondiente a ip de la subred y la otra ip al Broadcast quedando de la siguiente forma:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION					
cant de host	IP Red (SR)		Campo de host		Mascara (SR)
	Prefijo	Mascara			
3100 + 2					
860 + 2					
496 + 2					
63 + 2					
35 + 2					
35 + 2					
2 + 2					
2 + 2					
2 + 2					

Por lo tanto queda así:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION						
cant de host	IP Red (SR)		Campo de host		Broadcast	Mascara (SR)
	Prefijo	Mascara				
3102						
862						
498						
65						
37						
37						
4						
4						
4						

Para el siguiente paso se coloca la dirección de red en la primera subred:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION					
cant de host	IP Red (SR)		Celdas de broadcast		
3102	172	16	0	0	
862					
498					
65					
37					
37					
4					
4					
4					

Para la primera subred necesitamos 3102 hosts y de acuerdo a nuestra tabla es el octeto 3 prefijo 20, con 4096 hosts, el que satisface esta necesidad, ya que si eligiéramos el 21 tendríamos un máximo de 2048 hosts que en este caso serían insuficientes para cubrir esos 3102 hosts solicitados y el valor más cercano que cubre la necesidad es el prefijo 20 como ya se ha explicado:

	OCTETO 1								OCTETO 2								OCTETO 3								OCTETO 4							
Bits	####	####	####	####	####	####	####	####	####	####	####	####	####	####	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1				
Octeto	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Binario	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
prefijo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

OCTETO 3													
####	####	####	####	####	8192	4096	2048	1024	512	256	128	64	32
4	2	1	128	64	32	16	8	4	2	1	128	64	32
1	1	1	1	1	1	1							
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Por lo tanto en la columna prefijo colocamos el prefijo correspondiente a la primera subred (20).

A continuación, completamos las casillas de mascara; como el prefijo es **20** y de acuerdo a nuestra tabla cae en el **tercer octeto**, por lo que procedemos a sumar los hosts del tercer octeto desde el prefijo 17 al 20 lo que resulta en  **$128+64+32+16=240$**  para la máscara de red que queda de la siguiente forma:

OCTETO 3										
#	####	####	####	8192	4096	2048	1024	512	256	128
1	128	64	32	16	8	4	2	1	128	
1	1	1	1	1						
16	17	18	19	20	21	22	23	24	25	

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION													
cant de host	IP Red (SR)				Campo de host				Broadcast		Mascara (SR)		
	Prefijo	Mascara											
3102	172	16	0	0					20	255	255	240	0
862													
498													
65													
37													
37													
4													
4													
4													

CORPORATION						
Broadcast	Mascara (SR)					
	Prefijo	Mascara				
	20	255	255	240	0	

OCTETO 3										
#	####	####	####	8192	4096	2048	1024	512	256	128
	1	128	64	32	16	8	4	2	1	128
	1	1	1	1	1					
	16	17	18	19	20	21	22	23	24	25

A continuación, y de acuerdo a que el **prefijo 20** cae en los **16** bits del tercer octeto, la siguiente subred avanza 16 quedando así:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION											
cant de host	IP Red (SR)				Campo de host				Broadcast	Mascara (SR)	
	Prefijo	Mascara									
3102	172	16	0	0						20	255
862	172	16	16	0						255	240
498											
65											
37											
37											
4											
4											
4											

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION						
cant de host	IP Red (SR)					
	Prefijo	Mascara				
3102	172	16	0	0		
862	172	16	16	0		
498						
65						
--						

Y repitiendo esta lógica rellenamos la columna de prefijo, mascara e IP Red (Subred)

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION											
cant de host	IP Red (SR)				Campo de host				Broadcast	Mascara (SR)	
	Prefijo	Mascara									
3102	172	16	0	0						20	255
862	172	16	16	0						22	255
498	172	16	20	0						23	255
65	172	16	22	0						25	255
37	172	16	22	128						26	255
37	172	16	22	192						26	255
4	172	16	23	0						30	255
4	172	16	23	4						30	255
4	172	16	23	8						30	255

Ahora se procede a llenar la columna del Broadcast que es básicamente **la última IP antes de la siguiente red**; en nuestro caso como la segunda IP de red es 172.16.**16.0** el Broadcast para la primera Subred es 172.16.**15.255** que se muestra a continuación:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION										
cant de host	IP Red (SR)				Broadcast	Mascara (SR)				
	Prefijo	Mascara								
3102	172	16	0	0	172.16.15.255	20	255	255	240	0
862	172	16	16	0		22	255	255	252	0
498	172	16	20	0		23	255	255	254	0
65	172	16	22	0		25	255	255	255	128
37	172	16	22	128		26	255	255	255	192
37	172	16	22	192		26	255	255	255	192
4	172	16	23	0		30	255	255	255	252
4	172	16	23	4		30	255	255	255	252
4	172	16	23	8		30	255	255	255	252

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION						
Host	Broadcast				Mascara	
	Prefijo	Mascara				
	172.16.15.255	20	255			
		22	255			
		23	255			
		25	255			

Siguiendo la lógica anterior completamos la columna del Broadcast:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION										
cant de host	IP Red (SR)				Broadcast	Mascara (SR)				
	Prefijo	Mascara								
3102	172	16	0	0	172.16.15.255	20	255	255	240	0
862	172	16	16	0	172.16.19.255	22	255	255	252	0
498	172	16	20	0	172.16.21.255	23	255	255	254	0
65	172	16	22	0	172.16.22.127	25	255	255	255	128
37	172	16	22	128	127.16.22.191	26	255	255	255	192
37	172	16	22	192	172.16.22.255	26	255	255	255	192
4	172	16	23	0	172.16.23.3	30	255	255	255	252
4	172	16	23	4	172.16.23.7	30	255	255	255	252
4	172	16	23	8	172.16.23.11	30	255	255	255	252

Finalmente solo queda llenar la columna del campo de host donde se coloca “**desde la IP siguiente a la IP de red**” , “**hasta la última IP previo al Broadcast**”, por ejemplo, como en nuestro caso, la primera IP de red es 172.16.0.**0**, por lo tanto la primera dirección del campo de host será 172.16.0.**1** y como nuestro primer broadcast es 172.16.**15.255** nuestro último host disponible es 172.16.**15.254**.

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION									
cant de host	IP Red (SR)				Campo de host	Broadcast	Mascara (SR)		
	Prefijo	Mascara							
3102	172	16	0	0	172.16.0.1 - 172.16.15.254	172.16.15.255	20	255	255
862	172	16	16	0		172.16.19.255	22	255	255
498	172	16	20	0		172.16.21.255	23	255	255
65	172	16	22	0		172.16.22.127	25	255	255
37	172	16	22	128		127.16.22.191	26	255	255
37	172	16	22	192		172.16.22.255	26	255	255
4	172	16	23	0		172.16.23.3	30	255	255
4	172	16	23	4		172.16.23.7	30	255	255
4	172	16	23	8		172.16.23.11	30	255	255

Finalmente completando la columna del campo de host nuestro esquema de direccionamiento queda de la siguiente forma:

ESQUEMA DIRECCIONAMIENTO RED ABC CORPORATION									
cant de host	IP Red (SR)				Campo de host	Broadcast	Mascara (SR)		
	Prefijo	Mascara							
3102	172	16	0	0	172.16.0.1 - 172.16.15.254	172.16.15.255	20	255	255
862	172	16	16	0	172.16.16.1 - 172.16.19.254	172.16.19.255	22	255	255
498	172	16	20	0	172.16.20.1 - 172.16.21.254	172.16.21.255	23	255	255
65	172	16	22	0	172.16.22.1 - 172.16.22.126	172.16.22.127	25	255	255
37	172	16	22	128	172.16.22.129 - 172.16.22.190	172.16.22.191	26	255	255
37	172	16	22	192	172.16.22.193 - 172.16.22.254	172.16.22.255	26	255	255
4	172	16	23	0	172.16.23.1 - 172.16.23.2	172.16.23.3	30	255	255
4	172	16	23	4	172.16.23.5 - 172.16.23.6	172.16.23.7	30	255	255
4	172	16	23	8	172.16.23.9 - 172.16.23.10	172.16.23.11	30	255	255

## DIRECCIONAMIENTO IPv6

a. Dada la red de IPv6 de ABC Corporation

**2001 : 0db8 : 57b2 : 0000 : 0000 : 0000 : 0000 : 0000 / 64**

Aplicando las reglas para reducir la notación de direcciones IPv6, queda de la forma:

**2001 : db8 : 57b2 : 0 : 0 : 0 : 0 : 0 / 64**

**2001 : db8 : 57b2 :: / 64**

Si consideramos 14 subredes con 64 bits de host para cada una; el esquema IPv6 para ABC Corporation queda de la siguiente forma:

Direccionamiento IPv6 ABC Corporation									
Sub red	Prefijo de red			Id de SR	Id de Interfaz				Mascara
SR0	2001	0db8	57b2	<b>0000</b>	0000	0000	0000	0000	<b>/64</b>
SR1	2001	0db8	57b2	<b>0001</b>	0000	0000	0000	0000	<b>/64</b>
SR2	2001	0db8	57b2	<b>0002</b>	0000	0000	0000	0000	<b>/64</b>
SR3	2001	0db8	57b2	<b>0003</b>	0000	0000	0000	0000	<b>/64</b>
SR4	2001	0db8	57b2	<b>0004</b>	0000	0000	0000	0000	<b>/64</b>
SR5	2001	0db8	57b2	<b>0005</b>	0000	0000	0000	0000	<b>/64</b>
SR6	2001	0db8	57b2	<b>0006</b>	0000	0000	0000	0000	<b>/64</b>
SR7	2001	0db8	57b2	<b>0007</b>	0000	0000	0000	0000	<b>/64</b>
SR8	2001	0db8	57b2	<b>0008</b>	0000	0000	0000	0000	<b>/64</b>
SR9	2001	0db8	57b2	<b>0009</b>	0000	0000	0000	0000	<b>/64</b>
SR10	2001	0db8	57b2	<b>000A</b>	0000	0000	0000	0000	<b>/64</b>
SR11	2001	0db8	57b2	<b>000B</b>	0000	0000	0000	0000	<b>/64</b>
SR12	2001	0db8	57b2	<b>000C</b>	0000	0000	0000	0000	<b>/64</b>
SR13	2001	0db8	57b2	<b>000D</b>	0000	0000	0000	0000	<b>/64</b>

## OK, PEEERO... ¿Por qué IPv6?

**Explicación sobre cómo el direccionamiento IPv6 aborda las limitaciones del direccionamiento IPv4 y proporciona una capacidad de direccionamiento más amplia**

Debido al agotamiento global de direcciones IPv4 y la llegada del IoT (Internet de las cosas) que demanda una gran cantidad de direcciones IP, es que se hace necesaria la migración hacia el esquema IPv6.

IPv4 utiliza direcciones de **32 bits** que limita el espacio de direcciones a:

**4.294.967.296 ( $2^{32}$ ) direcciones posibles.**

En cambio IPv6 utiliza direcciones de **128 bits** lo que le da capacidad de albergar **340 sextillones ( $2^{128}$ )** de direcciones o lo que es lo mismo

**340.282.366.920.938.463.463.374.607.431.768.211.456  
direcciones posibles.**

Por lo tanto y con solo ver estos números podemos dar cuenta de la capacidad de direccionamiento mucho más amplia que tiene IPv6 por sobre IPv4. Básicamente todos los dispositivos que existen y que existirán por muchos años podrán tener su propia IPv6 única en el todo el globo.

**Pero ¿porque entonces no se han acabado las direcciones IPv4 y sigue siendo el standard? Se supone que ya superamos esos poco mas de 4 mil millones de direcciones posibles.**

Entre las razones tenemos principalmente 3, aunque la primera es la más importante:

### **1. NAT (Network Address Translation)**

Una sola IP pública puede servir a cientos o miles de equipos privados.

- Gracias a NAT, una empresa u hogar puede usar IP privadas como 192.168.x.x, 10.x.x.x, etc., y **salir a Internet con una sola IP pública**.
- Esto alarga “*artificialmente*” la vida de IPv4.
- Ejemplo: tu PC, el celular y el Smart TV están usando la misma IP pública ahora mismo. No necesitas una IP pública por cada dispositivo.

### **2. Infraestructura antigua y compatibilidad**

IPv4 demasiado arraigado en routers, firewalls, ISPs, software, IoT, etc.

- Cambiar todo a IPv6 cuesta tiempo, plata y pruebas.
- Muchos dispositivos antiguos no soportan bien IPv6, sobre todo en países donde la inversión tecnológica es baja.
- Algunas **aplicaciones críticas** aún **dependen** de IPv4.
- Se prefiere mantener IPv4 y hacer convivir ambos protocolos cuando se puede (dual stack).

### **3. Sigue habiendo direcciones... pero recicladas o revendidas**

Organizaciones que recibieron bloques grandes en los años 90 ahora revenden o subarriendan IPs.

- Hay un mercado negro y oficial de IPv4.
- Empresas como Amazon, Microsoft, etc., compran bloques enteros a universidades o entidades que no los usan.
- A veces se recuperan IPs de dispositivos viejos o mal asignadas.
- Técnicamente no hay nuevas IPs, pero sigue habiendo circulación.

### **Entonces... ¿por qué no IPv6 ya?**

- IPv6 no es retrocompatible con IPv4 → necesitas adaptar todo.
- IPv6 requiere que todos los routers y servicios intermedios lo soporten bien.
- No todos los ISPs lo ofrecen aún.
- Muchos admins no saben configurarlo bien o simplemente no lo entienden.

***En ciberseguridad, toca conocer ambos: atacar y defender en entornos mixtos es la realidad actual.***

## **Consideraciones de Transición:**

Debido a que la transición de IPv4 a IPv6 está recién comenzando y tardara algunos años en ser el standard, lo cierto es que pueden coexistir en la actualidad sin que ocurran interrupciones significativas en la conectividad.

Debido a que IPv4 sigue siendo el protocolo más utilizado globalmente, la transición a IPv6 no puede ser llevada de la noche a la mañana y para que dicha transición se pueda realizar de forma suave y sin mayores sobresaltos, existen 3 técnicas para la migración y coexistencia de ambos protocolos en la actualidad.

- **Dual Stack**

Dicho en palabras sencillas esta técnica permite que IPv4 e IPv6 coexistan en la misma red.

Los dispositivos ejecutan stacks de protocolos IPv4 e IPv6 de manera simultánea, esto propone que los hosts y enrutadores de la red del operador ISP tengan soporte dual de Protocolo IP. Esto es, todo dispositivo de red tiene soporte dual y simultáneo de los Protocolos IPv6 e IPv4.

En general, la razón principal de usar IPv4 e IPv6 al mismo tiempo son los problemas de compatibilidad. En realidad, IPv4 e IPv6 no son compatibles entre sí, lo que significa que los dispositivos no pueden comunicarse directamente y Dual Stack se hace cargo.

- **Tunneling**

Básicamente esta técnica consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras.

- **Traducción**

Una técnica que implica traducir un protocolo en el otro. Con las técnicas de traducción, los dispositivos finales con IPv6 pueden comunicarse libremente con dispositivos finales con IPv4. Un proxy IPv6 se usa para traducir un protocolo a otro protocolo. Este proxy puede ser un servidor colocado al final de una red para interceptar todos los paquetes IP y traducirlos al otro protocolo.