SUBNETTING

TAMARA SANCHEZ

DEFINICIÓN

El Subnetting o subneteo es la técnica de subdividir una gran red IP física en varias redes lógicas más pequeñas, de forma que cada una de estas subnets funcionen como una red individual respecto a envíos y recepción de paquetes, aunque sigan perteneciendo a una misma red principal y a un mismo dominio. Este proceso debe ser realizado cuidadosamente, para así no desaprovechar direcciones IPv4.
Para la realización de esta técnica, se establece como dirección única al router que hace la conexión entre la red e internet. Sin embargo, pueden existir varios hosts ocultos, por lo que el número de hosts que quedan disponibles para el administrador aumentará de forma considerable.

MOTIVOS

1-Reducir o ampliar la red
2-Optimización de la red (tráfico de broadcast)
3-Mejor organización(secciones o áreas)
4-Mayor seguridad y control de tráfico(podemos segmentárlas VLANs
=switch,l2 y usar diferente direccionamiento IP,l3,para permitir o denegar tráfico en diferentes equipos

broadcast=es la última dirección IP , es la dirección especial que envía datos a todos los hosts

https://www.redeszone.net/tutoriales/redes-cable/calcular-subnetting-ip-red-mascara-subred-ipv4/

Binario	Decimal	Notación CIDR	Máximo número de host
11111111.11111111.11111111.11111111	255.255.255.255	/32	
11111111.11111111.11111111.11111110	255.255.255.254	/31	
11111111.11111111.11111111.11111100	255.255.255.252	/30	2
11111111.11111111.11111111.11111000	255.255.255.248	/29	6
11111111.11111111.11111111.11110000	255.255.255.240	/28	14
11111111.11111111.11111111.11100000	255.255.255.224	/27	30
11111111.11111111.11111111.11000000	255.255.255.192	/26	62
11111111.11111111.11111111.10000000	255255255128	/25	126
11111111.11111111.11111111.00000000	255.255.255.0	/24	254
11111111.11111111.11111110.00000000	255.255.254.0	/23	510
11111111.11111111.11111100.00000000	255.255.252.0	/22	1022
11111111.11111111.11111000.00000000	255.255.248.0	/21	2046
11111111.11111111.11110000.00000000	255.255.240.0	/20	4094
11111111.11111111.11100000.00000000	255.255.224.0	/19	8190
11111111.11111111.11000000.00000000	255.255.192.0	/18	16382
11111111.11111111.10000000.00000000	255.255.128.0	/17	32766
11111111.11111111.00000000.00000000	255.255.0.0	/16	65534
11111111.11111110.00000000.00000000	255.254.0.0	/15	131070
11111111.11111100.00000000.00000000	255.252.0.0	/14	262142
11111111.11111000.00000000.00000000	255.248.0.0	/13	524286
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048574
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097150
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194302
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388606
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777214
11111110.00000000.00000000.00000000	254.0.0.0	/7	33554430
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108862
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217726
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435454
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870910
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741822
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483646
00000000.00000000.00000000.00000000	0.	/0	4294967294

Estas pueden ralentizar el funcionamiento de la red. Siempre que hagamos una división en subredes, es muy recomendable hacer uso de VLANs a nivel L2 o capa de enlace, de esta manera, vamos a poder crear diferentes VLANs en los switches gestionables de toda la red, para separar las subredes de forma correcta y proporcionar la mejor seguridad posible. El router también debe ser capaz de «entender» el protocolo 802.1Q, de lo contrario, las VLANs no podrán comunicarse unas con otras, algo que es totalmente necesario en ciertos escenarios, por lo que debes tenerlo muy en cuenta.

Siguiendo con el apartado de la seguridad, otro punto a tener en cuenta es que dividir la red en distintas subredes aumenta precisamente en gran medida la seguridad de la misma, de distintas formas, empezando por que puede controlarse el flujo utilizando por ejemplo QoS o mapas de enrutamiento que nos permiten al mismo tiempo identificar las diferentes amenazas y cerrarle los puntos de entrada.

También podemos realizar uso de distintos routers para dividir nuestra red y realizar configuración de ACL entre dichos routers y los switches y como resultado de esto, todos los dispositivos que pertenezcan a esa subred, no serán capaces de acceder a la totalidad de dicha red y esto minimiza el riesgo de que se propaguen amenazas si algún dispositivo se ve comprometido.