UTN.BA UNIVERSIDAD TECNOLÓGICA NACIONAL FACULTAD REGIONAL BUENOS AIRES | Centro de e-Learning Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Módulo 1:

Diseño de redes seguras

Unidad 2:

Instalación y configuración en redes

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Presentación

En esta segunda Unidad del curso, nos introducimos en la comprensión de la temática correspondiente a lo que hay que tener en cuenta antes de empezar el armado de una red.

Se explicará la importancia de un direccionamiento IP adecuado, para poder identificar correctamente los dispositivos.

Se verán distintos dispositivos de seguridad, donde los mismos cobran importancia mayor en cuanto a la distribución de donde ubicarlos.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Objetivos

Que los participantes logren…

- Conocer los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.

- Aprender a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bloques temáticos

1. Modelo TCP/IP.
2. Direccionamiento IP.
3. Seguridad en redes.

Modelo TCP/IP

Conocido como una “suite de protocolos”, ya que está formado por dos protocolos: **TCP** (Transmission Control Protocol) e IP (Internet Protocol).

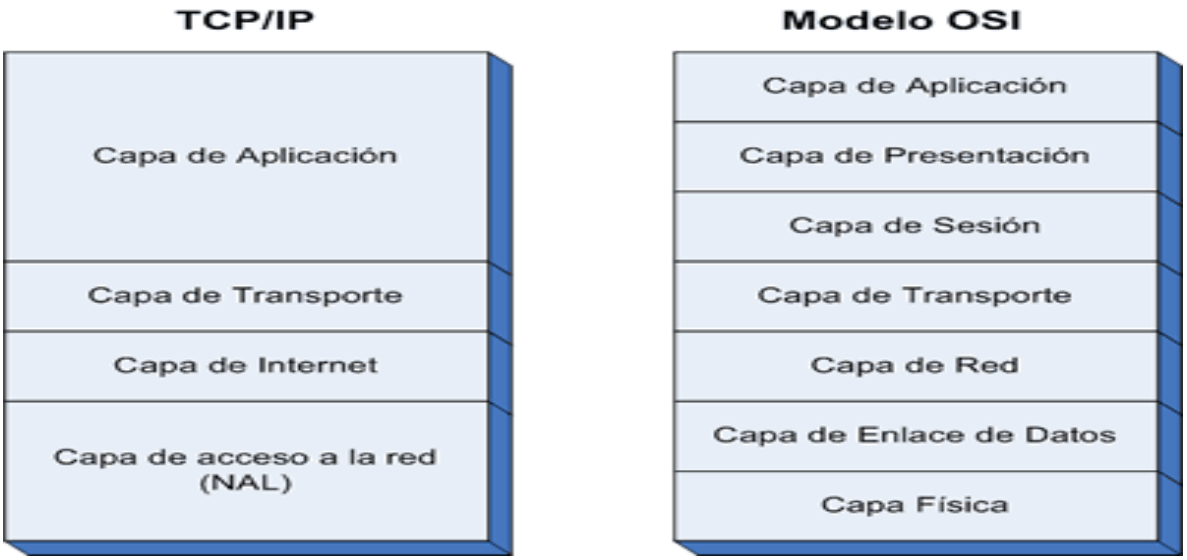
Provee todos los servicios necesarios para poder conectar distintos dispositivos en redes formadas por distintos tipos de dispositivos.

Un dispositivo puede tener una configuración diferente a lo habitual, pero mientras siempre y cuando se use **TCP/IP**, se podrá comunicar con los demás dispositivos.

Todos los equipos permiten el uso de **TCP/IP** para sus comunicaciones, siendo esta la configuración utilizada por los administradores de red.

A diferencia del **MODELO OSI, TCP/IP** tiene 4 capas.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Aplicación, Transporte, Internet y Acceso a la red

En la capa de Aplicación, se engloban las mismas actividades que se realizan en el Modelo **OSI** (Aplicación, Presentación y Sesión).

Esta capa administra todas las funciones utilizadas y requeridas por las aplicaciones y los servicios que tengan una relación directa con el usuario final: **HTTP, SMTP, FTP, ETC.**

La capa de Transporte, corresponde a la misma que el Modelo **OSI.**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

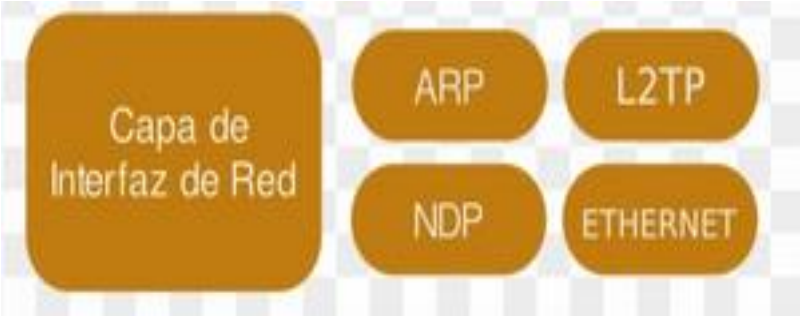
Se encarga de proveer la conectividad de punta a punta entre el origen (emisor) y el destinatario (receptor) y permite intercambiar los roles de emisor y receptor dinámicamente.

La capa de Internet, corresponde a la capa de red del Modelo **OSI**.

Se encarga de definir el esquema de direccionamiento lógico de los equipos que se conecten a la red y el direccionamiento de c/u de los equipos de la red.

Contamos también con un servicio de enrutamiento, para todos los equipos que estén conectados a la red, donde contará con toda la información relacionada a los equipos de origen y destino en la comunicación.

Por último, tenemos la capa de Acceso a la red correspondiendo a las capas de enlace de datos y física del modelo **OSI.**



Aquí se define el acceso de modo de acceso físico a la red, y la traducción del direccionamiento físico al lógico.

Por eso encontraremos que trabaja con el protocolo ARP, lo mismo que en la capa de enlace de datos del modelo **OSI.**

Acá operan todos los protocolos encargados de preparar el ambiente físico y lógico necesario para realizar las comunicaciones.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

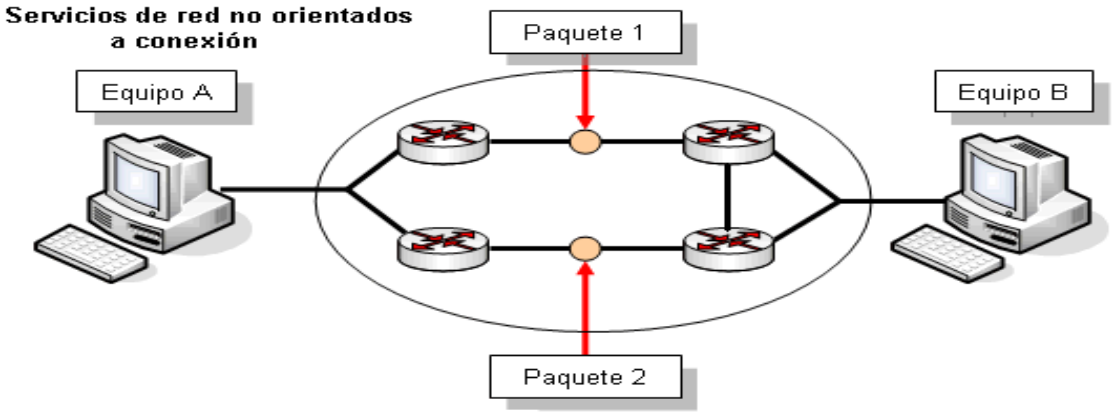
Protocolo IP

Es un protocolo de comunicación de datos en la Capa de Red según el modelo internacional **OSI.**

Su función es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo **no orientado a conexión** que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma **OSI** de enlace de datos.

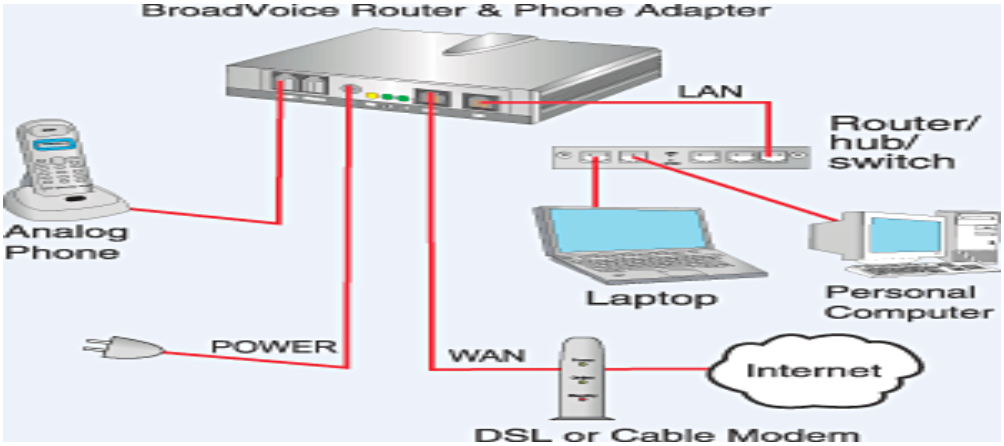
No orientado a la conexión significa una comunicación entre dos puntos finales de una red en los que un mensaje puede ser enviado desde un punto final a otro sin acuerdo previo.

Los paquetes pueden tomar distintas rutas para atravesar la red, pero se vuelven a ensamblar cuando llegan a su destino y en un sistema no orientado a conexión, no se hace contacto con el destino antes de que se envíe el paquete.



Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que enviarán los paquetes.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



IP provee un servicio de datagramas no fiable (también llamado del "***mejor esfuerzo***"), lo hará lo mejor posible pero garantizando poco).

IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de sus cabeceras y no de los datos transmitidos.

Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la ***capa de transporte*** como ***TCP***.

TIPS: Direccionamiento vs Enrutamiento

Cuando hablamos de **direccionamiento**, nos estamos refiriendo a una "etiqueta" que nos encontramos en el dispositivo o elemento de la red.

Dentro de una red, necesitamos "identificar" a todos los dispositivos para la comunicación entre ellos o con agentes externos.

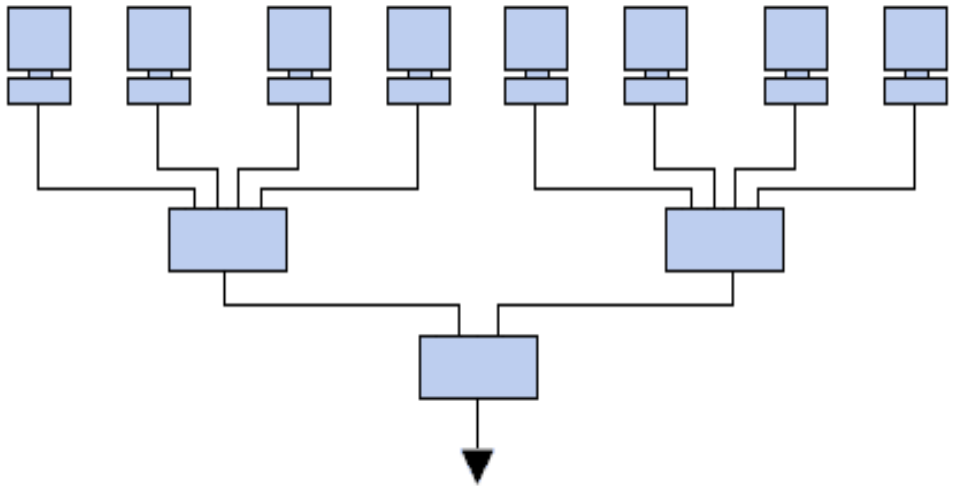
Enrutamiento, significa "aprender" la manera de encontrar un equipo o una determinada "IP" dentro de esa red.

En la tabla de enrutamiento, se encuentran todas las redes publicadas y/o aprendidas, por intermedio de protocolos de enrutamiento (BGP, EIGRP, IGRP, RIP, rutas estáticas, etc.).

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

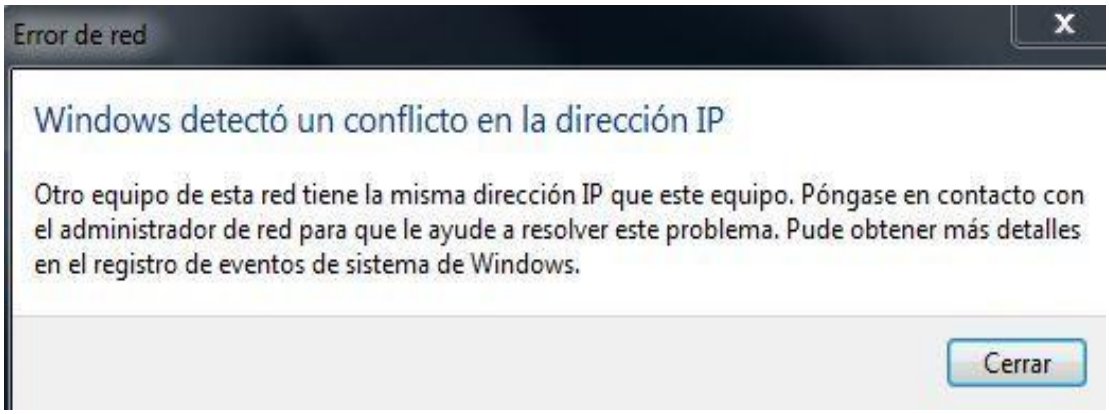
Direccionamiento IP

Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo dentro de una red que utilice el protocolo de Internet.



Observando una red como el dibujo anterior, es imposible relacionar un equipo con otro para que puedan comunicarse entre sí, al menos una etiqueta que los identifique.

Una dirección IP asignada a un equipo es única (no pueden existir dos equipos en la misma red con la misma dirección).



El mismo sistema operativo, interpretará que no es posible la comunicación debido a esa reiteración de direccionamiento **IP**.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

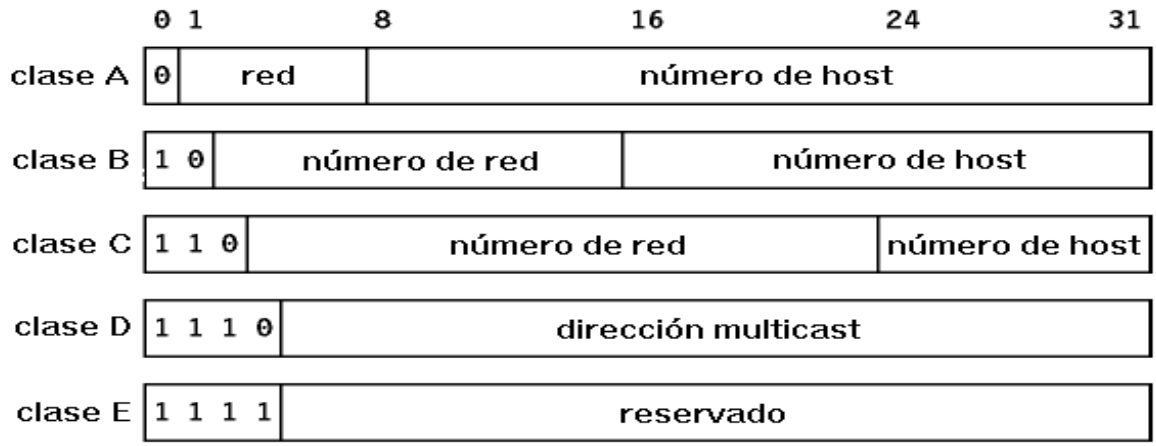
La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras.

/8	255.0.0.0	/20	255.255.240.0
/9	255.128.0.0	/21	255.255.248.0
/10	255.192.0.0	/22	255.255.252.0
/11	255.224.0.0	/23	255.255.254.0
/12	255.240.0.0	/24	255.255.255.0
/13	255.248.0.0	/25	255.255.255.128
/14	255.252.0.0	/26	255.255.255.192
/15	255.254.0.0	/27	255.255.255.224
/16	255.255.0.0	/28	255.255.255.240
/17	255.255.128.0	/29	255.255.255.248
/18	255.255.192.0	/30	255.255.255.252
/19	255.255.224.0		

El número que viene después de la "/" es la suma de los bits que se utilizan para la máscara de red, esa identificación se la conoce como **CIDR**.

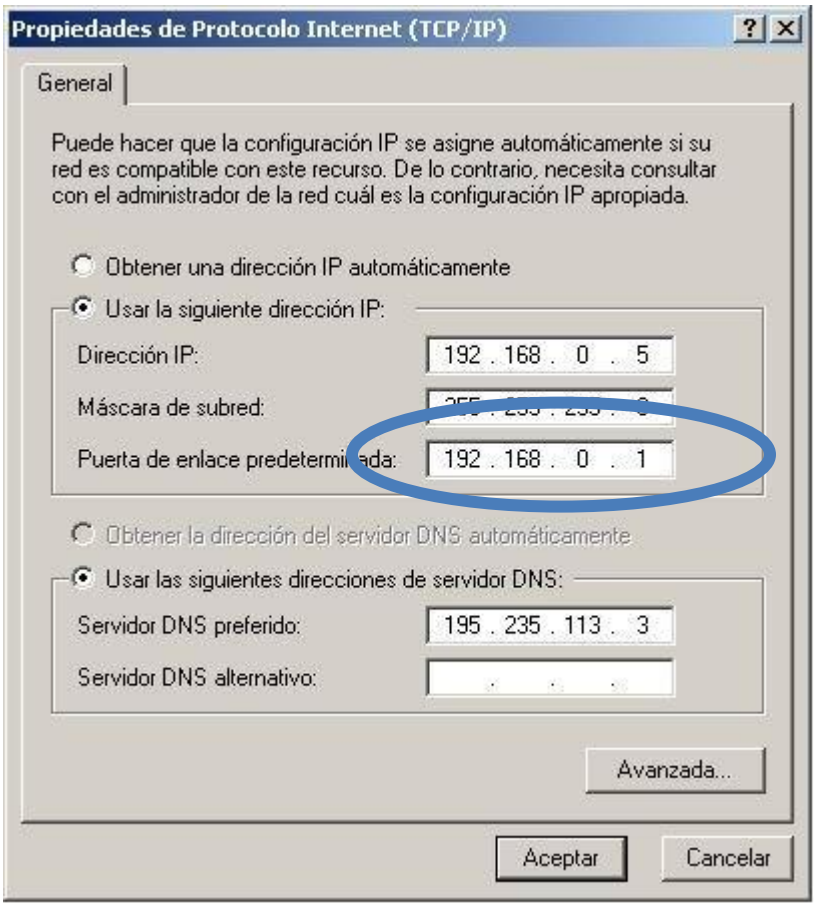
La función principal de la máscara de red es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Los primeros bits nos indicarán los distintos segmentos.



Una puerta de enlace o Gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Su función es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.



Atención con ese valor, dado que el mismo se puede configurar manualmente o por intermedio de un servidor de **DHCP**.

Esa **IP** que se encuentra como puerta de enlace o default Gateway, indicará al "tráfico de red" generado, por donde tiene que salir (generalmente es la IP de un router).

En conclusión: DIRECCIÓN IP – MASCARA - GATEWAY

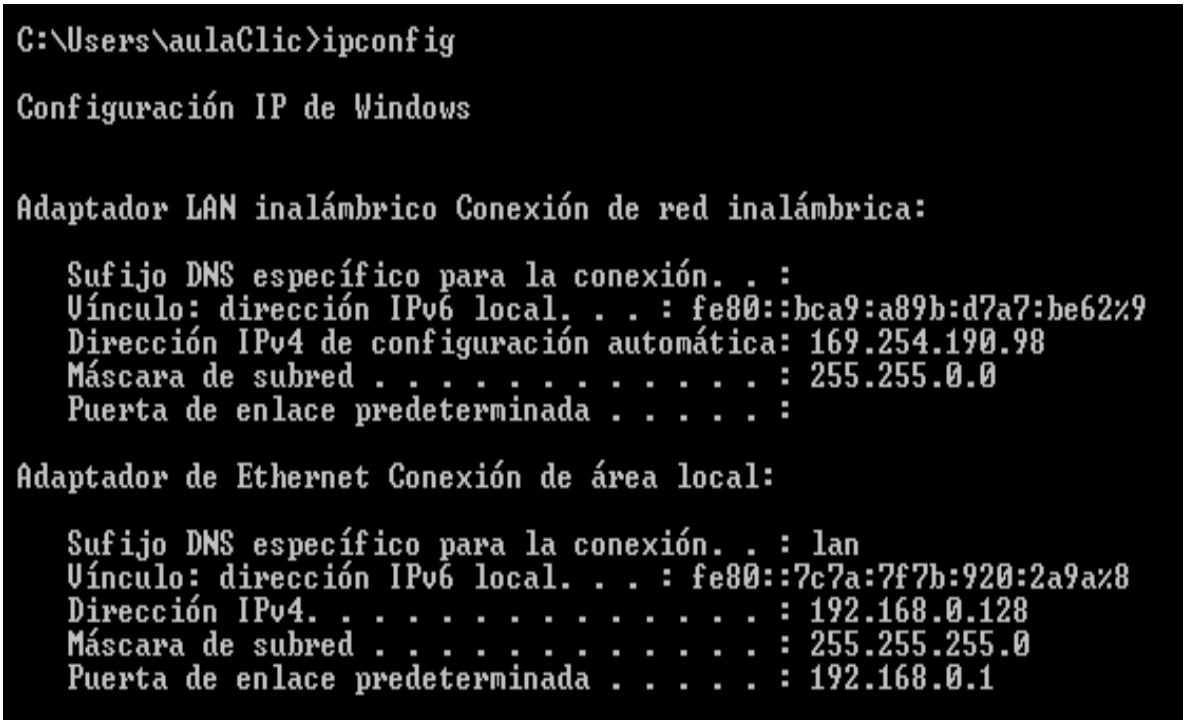
Ejemplo:

IP de Dispositivo: 192.168.0.128

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Máscara de red: 255.255.255.0

Default Gateway/Puerta de enlace: 10.10.10.1



QUE SON LAS DIRECCIONES IP FIJAS o ESTÁTICAS – IP DINAMICAS

Cuando nos conectamos desde nuestra casa u oficina a **INTERNET** utilizamos una dirección IP

Esta dirección puede cambiar al reiniciar el dispositivo, lo que ese cambio de dirección de la IP se denomina ***"IP dinámica"***

Los sitios de Internet que visitamos necesitan estar siempre conectados, generalmente tienen una ***"IP fija";*** es decir, no cambia con el tiempo

Los servidores de correo, DNS, FTP públicos, servidores web, conviene que tengan una dirección IP fija o estática, ya que de esta forma se facilita su ubicación.

Hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (***ICANN***).

Clase A, Clase B y Clase C (la D y la E son reservadas).

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Estos rangos se separan lo que es direccionamiento privado y público, donde el privado es para la red **LAN** y el público para todo lo que sea **WAN** (esto incluye servidores o servicios que se expongan a Internet, aun siendo de una **LAN**).

Direccionamiento RESERVADO Y PRIVADO:

Red o rango	Uso
127.0.0.0	Reservado (fin clase A)
128.0.0.0	Reservado (inicio Clase B)
191.255.0.0	Reservado (fin clase B)
192.0.0.0	Reservado (inicio Clase C)
224.0.0.0	Reservado (inicio Clase D)
240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0	Privado
172.16.0.0 – 172.31.0.0	Privado
192.168.0.0 – 192.168.255.0	Privado

Todo direccionamiento no expuesto, es considerado direccionamiento público

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 1 Unidad 2

Crear un informe explicando que son las bases de datos "**WHOIS**" y cuáles son las correspondientes a nuestra zona (continente) y país.

ATENCIÓN: en Linux existe un comando llamado "WHOIS", no estamos refiriendo a eso, sino a comprender quienes son los que manejan y exponen las bases de direccionamiento en el mundo.

Los datos que se puedan obtener, son necesarios para realizar un reconocimiento de quienes son los dueños de un sitio, servicio, etc.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Explicando: Direccionamiento IP

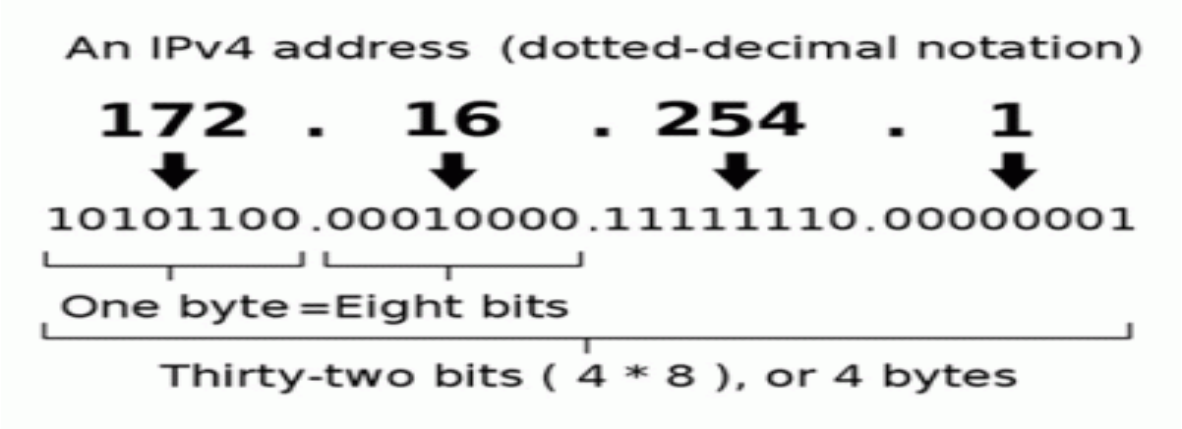
Las direcciones IPv4 se interpretan SIEMPRE como un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles (Binario= 0 y 1).

Cada dirección *IP* se expresa como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos.

[xxx].[xxx].[xxx].[xxx] Decimal

[xxxxxxxx].[xxxxxxxx].[xxxxxxxx].[xxxxxxxx] Binario

También interpretamos que una dirección IP está compuesta por 4 bytes.



El valor decimal de cada octeto está comprendido en el rango de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

1	1	1	1	1	1	1	1	
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128 +	64 +	32 +	16 +	8 +	4 +	2 +	1	= 255

1	1	0	0	0	0	0	0	
2^7	2^6							
128 +	64							= 192

1	0	1	0	1	1	0	0	
2^7		2^5		2^3	2^2			
128	+	32	+	8 +	4			= 172

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Vamos a realizar un ejemplo:

192.168.16.24

Si tomamos el primer octeto (192) en binario seria:

1 1 0 0 0 0 0 0

1	**1**	**0**	**0**	**0**	**0**	**0**	**0**
---	---	---	---	---	---	---	---
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Se suma siempre desde la izquierda a derecha y formando el número solicitado (128+64 = 192)

Sigamos con el ejemplo, ahora tomemos el segundo octeto (168) en binario sería:

1 0 1 0 1 0 0 0

1	**0**	**1**	**0**	**1**	**0**	**0**	**0**
---	---	---	---	---	---	---	---
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Se suma siempre desde la izquierda a derecha y formando el número solicitado (128+32+8 = 168).

¿Cómo serían los próximos octetos?

Tomamos el 16:

0 0 0 1 0 0 0 0

0	**0**	**0**	**1**	**0**	**0**	**0**	**0**
---	---	---	---	---	---	---	---
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Tomamos por último el 24:

0 0 0 1 1 0 0 0

0	**0**	**0**	**1**	**1**	**0**	**0**	**0**
---	---	---	---	---	---	---	---
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Otra forma de pasar decimal a binario: dividir siempre por 2

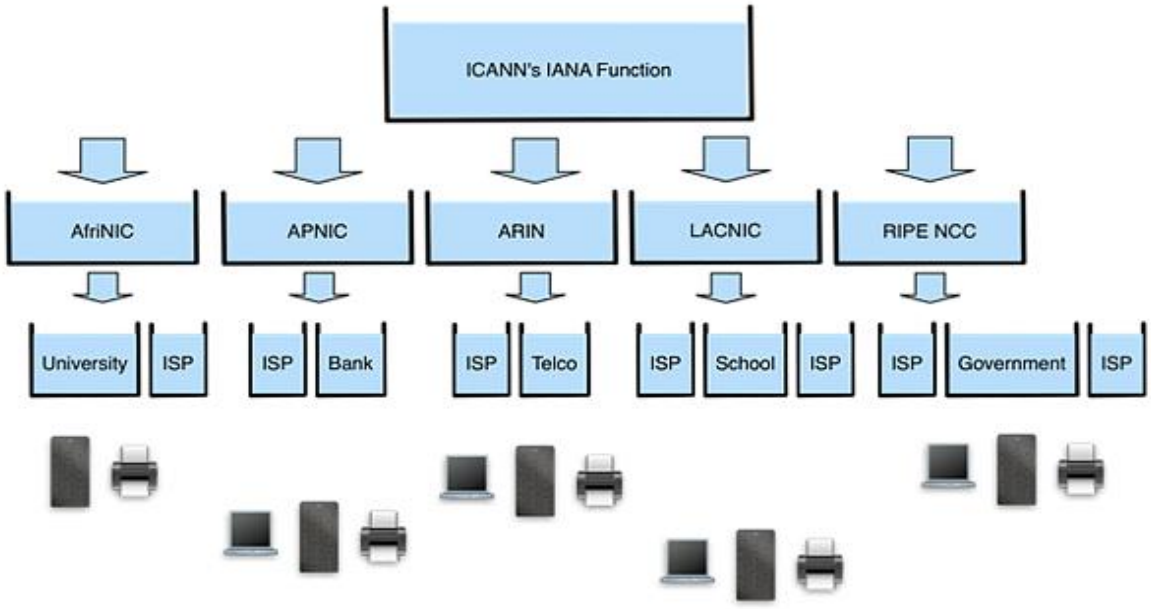
Transformar el número decimal 145 en binario.

145 dividido 2 da 72 y el resto es igual a 1
72 dividido 2 da 36 y el resto es igual a 0
36 dividido 2 da 18 y el resto es igual a 0
18 dividido 2 da 9 y el resto es igual a 0
9 dividido 2 da 4 y el resto es igual a 1
4 dividido 2 da 2 y el resto es igual a 0
2 dividido 2 da 1 y el resto es igual a 0
1 dividido 2 da 0 y el resto es igual a 1

Ordenando los restos, del último al primero: **10010001**

Total=145

El **direccionamiento IP** se gestiona a nivel global por la **corporación ICANN**, que reparte los grandes bloques de direccionamiento a cinco regiones, por lo tanto, la adopción de esta evolución tecnológica afecta a todos los países.



Las direcciones IPs son “públicas”, se pueden acceder desde cualquier lugar del mundo.

Esto hace que dos equipos en el mundo no tengan la misma IP evitando la duplicación de la misma.

Dentro del ambiente direccionamiento “privado”, ya explicamos que nos encontraremos con tres clases:

Clase A: 10.0.0.0 /8

Clase B: 172.16.0.0 /16 hasta la 172.31.0.0 /16

Clase C: 192.168.0.0 /24 hasta la 192.168.255.0 /24

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 2 Unidad 2

Buscar en Internet 4 direcciones IP y examinarlas.

¿Cómo buscarlas?

Es sencillo, haga un ping al sitio seleccionado, por ejemplo, en la ventana de comandos (o solo símbolo de sistemas) escriben:

Ping ***www.ejemplo.com*** y la conversión expondrá cual es la IP Pública

Transformar a las mismas en binario y subirlas al foro correspondiente.

Tabla aporte:

0 - 127	01001011 .	00111101 .	10101001 .	01000100 Clase A
128 - 191	10011011 .	00111101 .	10101001 .	01000100 Clase B
192 - 223	11011011 .	10001111 .	10101001 .	01000100 Clase C

Primer octeto		Direcciones IP				
Primeros bits	Rango de valores	CLASE	Máscara de red	Red y máquina	Número de Redes	Número de máquinas ó hosts
0	0–127	A	255.0.0.0	N.h.h.h	2^7=128	16.777.214
10	128–191	B	255.255.0.0	N.N.h.h	2^14=16.384	65.534
110	192–223	C	255.255.255.0	N.N.N.h	2^21=2.097.152	254
1110	224 – 239	D	No aplicable	Reservado	No aplicable	No aplicable
1111	240 – 255	E	No aplicable	Reservado	No aplicable	No aplicable

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Seguridad en redes

Dentro de una red, encontraremos maneras de poder securizar la misma, mediante la instalación y configuración de dispositivos que cumplen con las medidas necesarias brindando un comportamiento de cuidado en la red.

Dispositivos como: **Firewall / IDS / IPS / NIDS / HIDS.**

También en los routers y switches, existen configuraciones y appliances que nos brindarían esa seguridad.

Dentro de estos dispositivos, por ejemplo, existe lo que se llama **ACL** (access-list), que nos da la posibilidad de negar o permitir un determinado servicio o comunicación en la red.

El **Firewall** es un dispositivo de red, donde su función principal es la de bloquear todo acceso hacia la red y desde ella, mediante configuraciones llamadas “reglas o políticas”.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

El mismo trabaja revisando todo tráfico especificado y comparándolo con la lógica de permitir o negar según criterios de comportamiento.

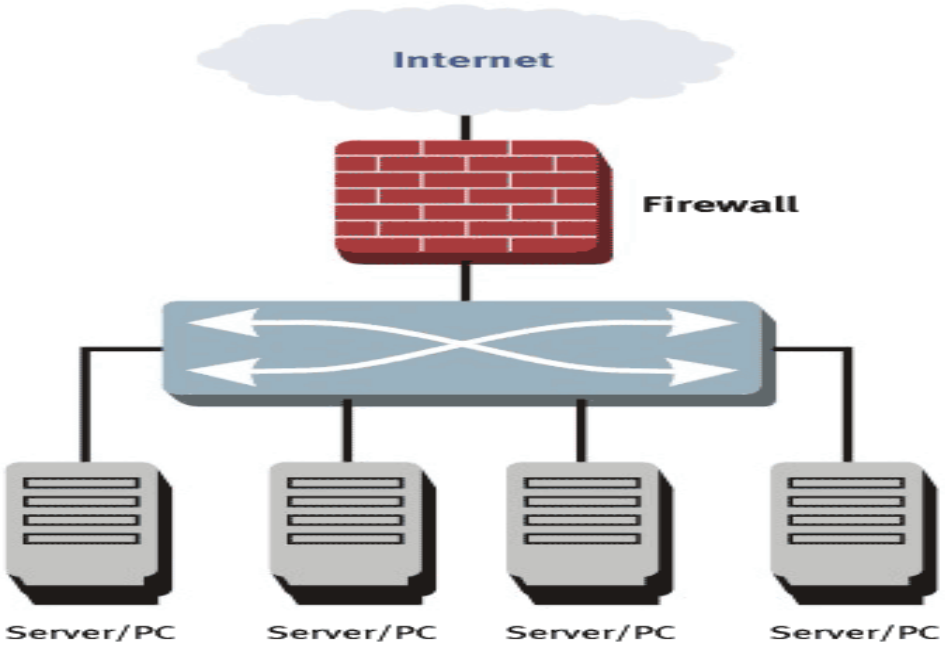
Restrictivo: lo que no sea explícitamente permitido, será negado.

Permisivo: lo que no sea explícitamente negado, será permitido.

Un **firewall** puede ser no solamente un dispositivo de red, sino que también lo podemos encontrar mediante un software de un sistema operativo, cumpliendo igualmente la función de permitir o negar.

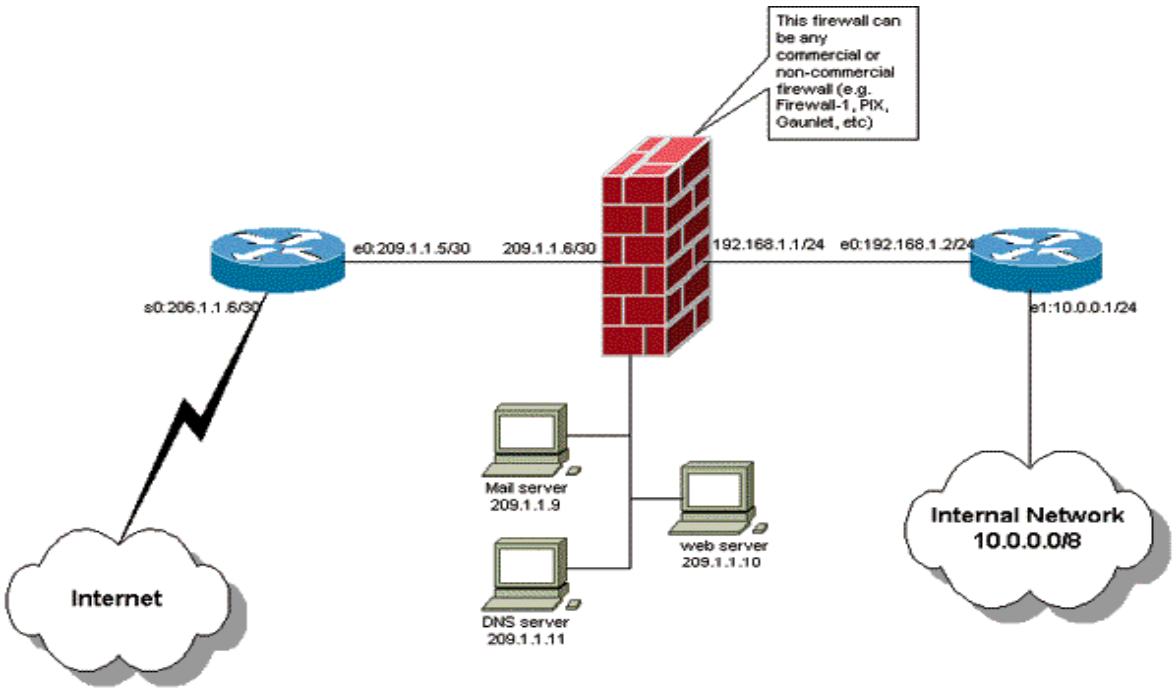
Donde se instale el **firewall**, nos indicará como intermedia las comunicaciones de la red que desea inspeccionar o proteger.

 DUAL-HOMED FIREWALL: el equipo cuenta con dos dispositivos o interfaces, que permitirán interactuar tanto con la red pública como con la privada.

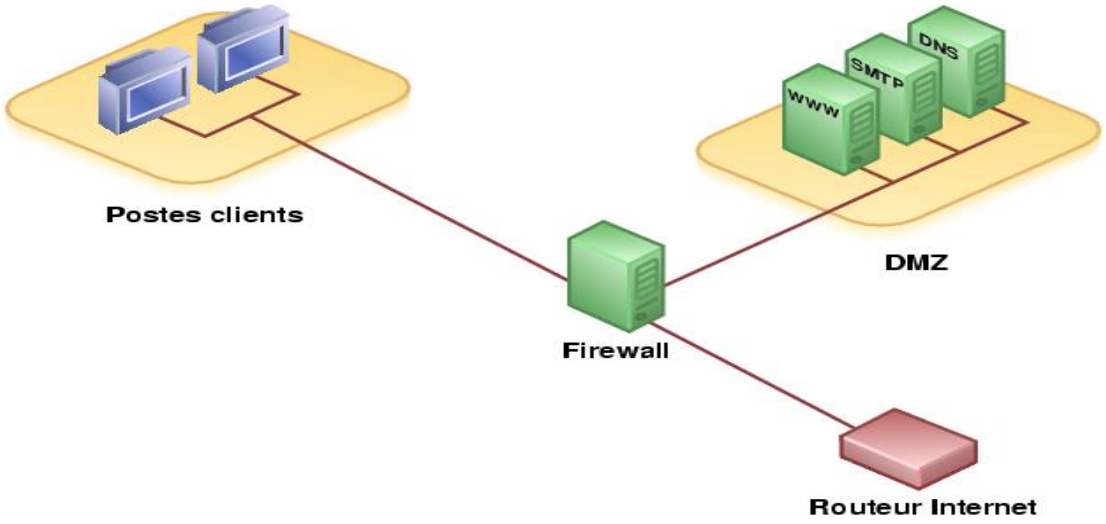


Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

 MULTI-HOMED FIREWALL: el equipo cuenta con varios dispositivos, que permitirán interactuar con varias redes distintas, dando la posibilidad de implementar políticas y reglas diferentes para cada una.



 DMZ: una **zona desmilitarizada** (*demilitarized zone*) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.



Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Uno de los objetivos de una ***DMZ*** es que las conexiones desde la red interna y la externa a la DMZ estén permitidas

Generalmente se posicionan en esa **DMZ**, los servicios que se quieren publicar en una red pública (Internet) como servidores de correo electrónico, Web y DNS

Dentro de la familia de los **FIREWALLS**, también podemos encontrar servicios tales como **packet filtering** (filtrado de paquetes), **application layer** (análisis de capas) y **statefull** (recuerdo de sesiones establecidas)

Otro elemento que se puede encontrar y ayudarnos a "censar" el tipo de tráfico que tengamos en la red es el **IDS** (**Intrusion Detection Systems**)

Mediante el análisis de cada paquete que esté circulando dentro de su rango de cobertura, tiene la capacidad de detectar anomalías o firmas, dando la posibilidad de programar reglas.

Un **IDS basado en patrones**, analiza paquetes en la red y los compara con patrones de ataques conocidos, y preconfigurados. Estos patrones se denominan firmas.

Debido a esta técnica, existe un periodo de tiempo entre el descubrimiento del ataque y su patrón, hasta que este es finalmente configurado en un **IDS**. Durante este tiempo, el **IDS** será incapaz de identificar el ataque.

Un **IDS basado en heurística**, determina actividad normal de red, como el orden de ancho de banda usado, protocolos, puertos y dispositivos que generalmente se interconectan, y alerta a un administrador o usuario cuando este varía de aquel considerado como normal, clasificándose como anómalo.

Cuenta con una base de datos (firmas) de donde basándose en la técnica de "censar" paquetes, los compara y actúa en consecuencia, respetando los parámetros asignados a los que se configuran (envío de alarmas, mails, etc.).

¿QUE HACEN LOS IDS?

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**

  Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).

- **Envío de una trampa SNMP a un hipervisor externo**

  Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa.

- **Envío de un correo electrónico a uno o más usuarios**

  Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión sería.

- **Registro del ataque**

  Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.

- **Almacenamiento de paquetes sospechosos**

  Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.

- **Apertura de una aplicación:**

  Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).
- **Notificación visual de una alerta**

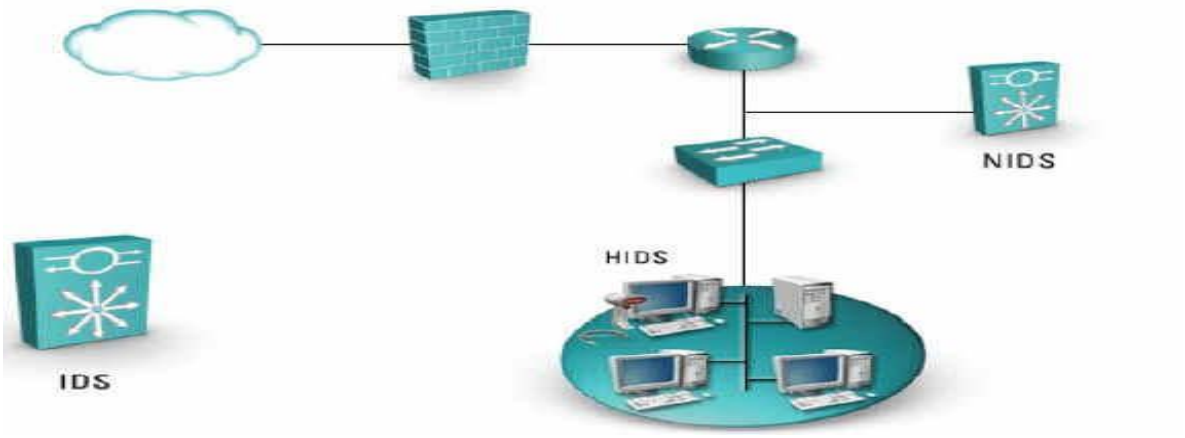
  Se muestra una alerta en una o más de las consolas de administración.

Imagen delantera y trasera de un IDS Cisco 4250

De acuerdo a su estructura, se cuentan con dos tipos que son especiales para redes:

NIDS: basados en hardware o software, para analizar segmentos de red donde estén conectados, garantizando la seguridad dentro de una red.

HIDS: basado en software, generalmente aplicado sobre el sistema operativo del equipo a proteger, garantizando la seguridad de un host.



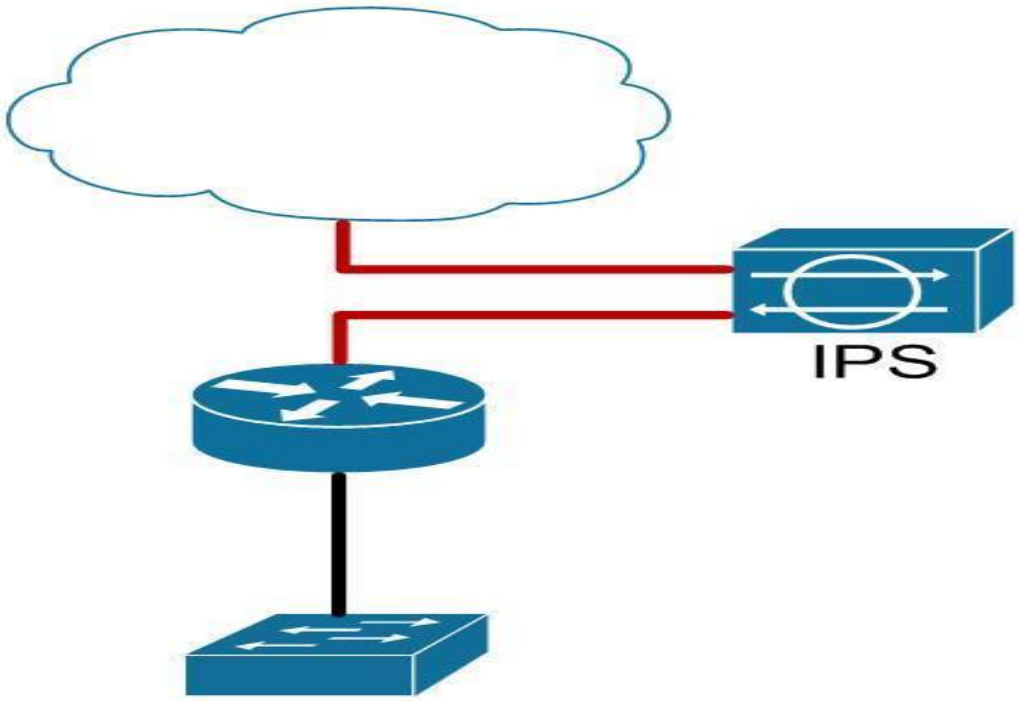
Los **HIDS**, analizan la información almacenada en registros, aparte de capturar paquetes que entran o salen del dispositivo, dando la posibilidad de detectar:

Ataques de denegación de servicio – Troyanos – Ejecución de códigos maliciosos – Ataques de desbordamiento de buffer – Intentos de acceso no autorizado.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Y por último tenemos el **IPS (Intrusion Prevention Systems)** que a diferencia de los **IDS**, este analiza en tiempo real, teniendo para contemplar esa posibilidad, un puerto de entrada y otro de salida.

Una de sus funciones más importantes es monitorear el tráfico de red y/o las actividades de un sistema en busca de actividad maliciosa.



Si bien es muy útil, hay que tener en cuenta, que analiza todo tráfico entrante y saliente, basándose en anomalías y firmas, por lo que habrá que hacer un chequeo exhaustivo para que no ocasione problemas de rendimiento en la red.

Cuenta con varios métodos de detección, explicaremos los más importantes:

- **Detección basada en firmas:**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto. Por ejemplo, los ataques contra los servidores Web generalmente toman la forma de URLs.

Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor web.

Sin embargo, como este tipo de detección funciona parecido a un antivirus, el administrador debe verificar que las firmas estén constantemente actualizadas.

- **Detección basada en políticas:**

Declarar específicamente las políticas de seguridad.

El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

- **Detección basada en anomalías:**

Se define qué se va entender **como SITUACIÓN NORMAL.**

Detección estadística de anormalidades: El **IPS** analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.

Detección no estadística de anormalidades: En este tipo de detección, es el administrador quien define el patrón «normal» de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

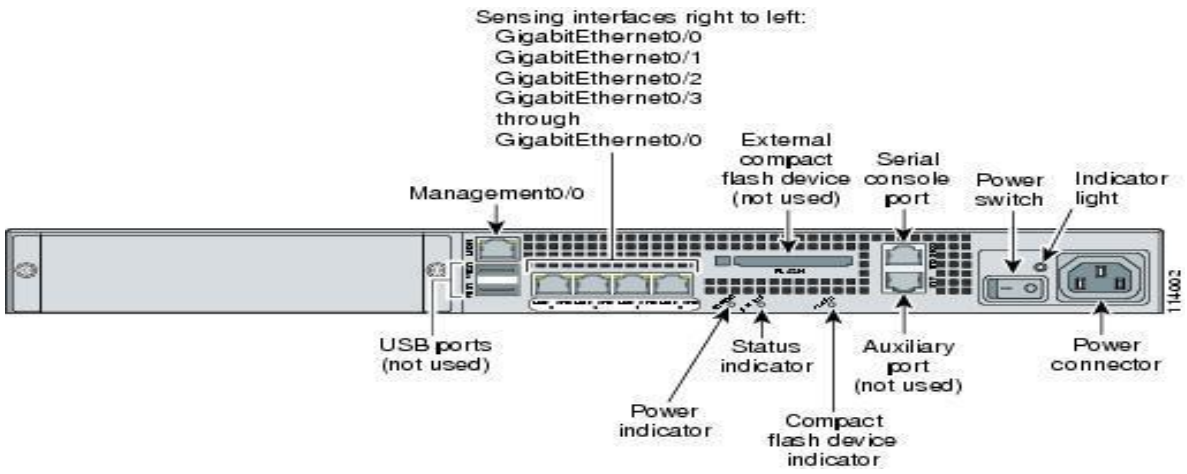


Imagen delantera y diagrama trasero de un IPS Cisco 4265

¿Qué es un Honeypot?

Un **honeypot** (en inglés «tarro de miel») es un sistema muy flexible dentro de la seguridad informática, que se encarga de **atraer** y **analizar** el comportamiento de los atacantes en internet, y que provee a un investigador o analista informático forense de una información extremadamente valiosa.

La pregunta sería: ¿para qué puede querer una persona atraer atacantes a su propio sistema? Esto puede resultar muy contradictorio, pero lo que se busca con esta implementación es capturar todo el tráfico de red entrante y conocer todos los detalles acerca de las **tendencias** y **metodologías de ataque** de los atacantes así como los fallos de seguridad en nuestra red con el fin de subsanarlos.

Los **honeypots** pueden ejecutarse bajo cualquier sistema operativo y bajo cualquier servicio. Los servicios configurados determinan los vectores de ataque disponibles para que el intruso comprometa y ponga a prueba el sistema.

Finalidad de los Honeypots

Estas son algunas de las posibilidades que nos ofrecen los honeypots:

- Desviar y distraer la atención del atacante.
- Detectar y aprender nuevas vulnerabilidades.
- Obtener información sobre el atacante (geolocalización, ip, puertos, etc).
- Obtener tendencias de ataque y países más atacados.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

- Detectar nuevas muestras de malware que aún no se conozcan.
- Recopilar y estudiar tendencias de ataque

Clasificación de Honeypots

Los honeypots se clasifican según su implementación (virtual o física) y su nivel de interacción (baja, media, alta).

SEGÚN SU IMPLEMENTACIÓN:

- **Para producción:** Al implementar un **honeypot** en una red de producción, el objetivo principal es la obtención de información sobre técnicas empleadas para tratar de vulnerar los sistemas que componen dicha infraestructura.

- **Para investigación:** Por otro lado, en este caso los **honeypots** constituyen recursos educativos de naturaleza demostrativa cuyo fin es recopilar la mayor cantidad de información que permita al investigador poder analizar las nuevas tendencias y métodos de ataque así como los distintos objetivos atacados y orígenes de los ataques.

SEGÚN SU INTERACCIÓN:

- **Alta interacción:** Este tipo de **honeypots** se trata de un sistema convencional, construidos con máquinas reales como el que podría utilizar cualquier usuario.

  Se sitúan generalmente en la red interna en producción y no tiene más utilidad que la de ser atacados, lo cual significa que el sistema está mal configurado.

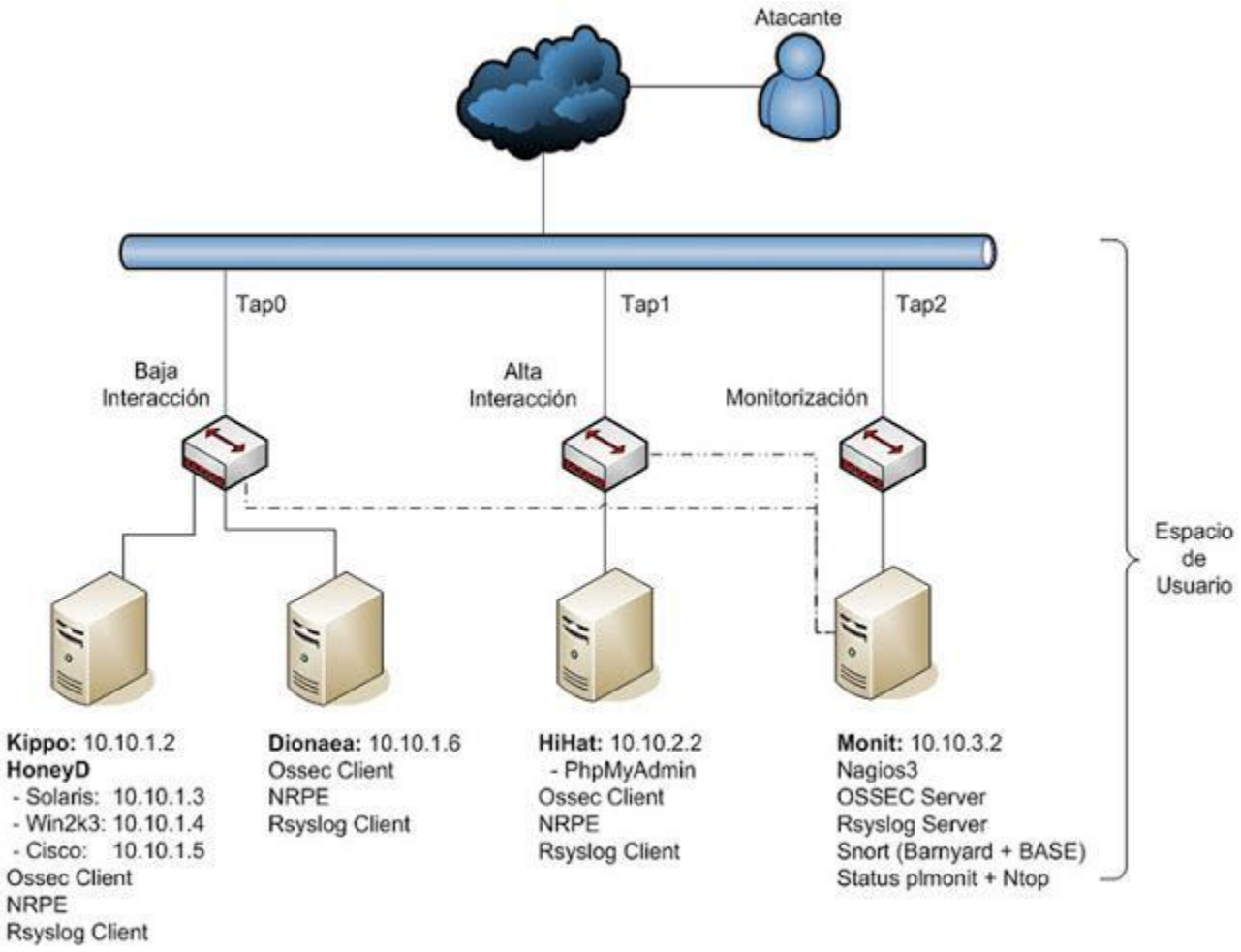
  Cada interacción con este honeypot se considera sospechosa por definición, y todo el tráfico debe ser monitorizado y almacenado en una zona segura de la red a la que un potencial atacante no tenga acceso.

- **Baja interacción:** Este tipo suele ser creado y gestionado por organizaciones dedicadas a la investigación de acciones fraudulentas en la red, con la cual se investiga acerca de nuevas amenazas en la red.

  Son más fáciles de utilizar y mantener, con un riesgo prácticamente nulo.

  Esta implementación se basa por lo general en una instalación de software de emulación de sistema operativo, utilizando herramientas conocidas como VMware o Virtual Box.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 3 Unidad 2

Realizar un gráfico con una topología a gusto de ustedes que contenga:

10 equipos (PCs)

2 switches

2 firewalls

1 IDS y 1 IPS

Una nube de proveedor de servicio (ISP)

Hay aplicaciones como EDRAW o Packet Tracer para poder dibujar redes, las mismas las pueden conseguir en Internet de forma gratuita.

Dibujar las conexiones de acuerdo a un orden de prioridades y explicarlas, por ejemplo, porque seleccionaron la topología y su ubicación

Se respetará la interpretación de cada uno, siempre y cuando la misma se explique en el ejercicio por el alumno.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy IMPORTANTE que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad .

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learni the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU

Link complementarios:

http://www.cisco.com

https://www.netacad.com/

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)