

LINUX

A UN CLIC



ANTES DE EMPEZAR

**“Se ha vuelto
terriblemente obvio
que nuestra tecnología
ha superado nuestra
humanidad.”**

ALBERT EINSTEIN



AGENDA

- CONCEPTUALIZACION: TELNET
- CONCEPTUALIZACION: TELNET
- RETO



CONFIGURACION DE RED

DHCP

El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP



CONFIGURACION DE RED

DHCP

Este protocolo se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131 .



CONFIGURACION DE RED

SIMPLIFICA LA ADMINISTRACION

La razón principal por la que se necesita DHCP es para simplificar la administración de las direcciones IP en las redes. No hay dos hosts que puedan tener la misma dirección IP, y configurarlos manualmente puede generar errores. Incluso en redes pequeñas la asignación manual de direcciones IP puede ser confusa, especialmente con dispositivos móviles que requieren direcciones IP de forma no permanente.



CONFIGURACION DE RED

ASIGNACION DE IP

- Asignación manual o estática
- Asignación dinámica



CONFIGURACION DE RED

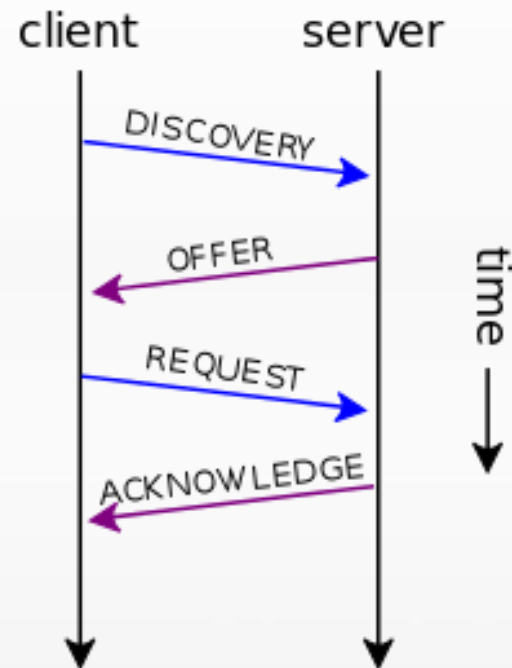
PARAMETROS

- Dirección del servidor DNS
- Nombre DNS
- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (broadcast address)
- Máscara de subred
- Tiempo máximo de espera del ARP
- MTU (Unidad de Transferencia Máxima según siglas en inglés) para la interfaz
- Servidores NIS (Servicio de Información de Red según siglas en inglés)
- Dominios NIS
- Servidores NTP (Protocolo de Tiempo de Red según siglas en inglés)
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor de nombres de Windows (WINS)



CONFIGURACION DE RED

OPERACION



CONFIGURACION DE RED

FUNCIONAMIENTO

- **DHCPDISCOVER** (para ubicar servidores DHCP disponibles)
- **DHCPOFFER** (respuesta del servidor a un paquete DHCPDISCOVER, que contiene los parámetros iniciales)
- **DHCPREQUEST** (solicitudes varias del cliente, por ejemplo, para extender su concesión)



CONFIGURACION DE RED

FUNCIONAMIENTO

- **DHCPACK** (respuesta del servidor que contiene los parámetros y la dirección IP del cliente)
- **DHCPNAK** (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea)



CONFIGURACION DE RED

FUNCIONAMIENTO

- **DHCPDECLINE** (el cliente le anuncia al servidor que la dirección ya está en uso)
- **DHCPRELEASE** (el cliente libera su dirección IP)
- **DHCPINFORM** (el cliente solicita parámetros locales, ya tiene su dirección IP)



CONFIGURACION DE RED

DHCP DISCOVERY

DHCPDISCOVER			
IP: source=0.0.0.0; destination=255.255.255.255			
UDP: source port=68; destination port=67			
Octet 0	Octet 1	Octet 2	Octet 3
OP	HTYPE	HLEN	HOPS
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0x00000000			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s, or overflow space for additional options; BOOTP legacy			
[Magic cookie]			
0x63825363			
DHCP options			
0x350101 53: 1 (DHCP Discover)			
0x3204c0a00164 50: 192.168.1.100 requested			
0x370401030f06 55 (Parameter Request List):Plantilla:Unordered list			
0xff 255 (Endmark)			



CONFIGURACION DE RED

DHCPOFFER

DHCPOFFER			
IP: source=192.168.1.1; destination=255.255.255.255			
UDP: source port=67; destination port=68			
Octet 0	Octet 1	Octet 2	Octet 3
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x08	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
53: 2 (DHCP Offer)			
1 (subnet mask): 255.255.255.0			
3 (Router): 192.168.1.1			
51 (IP address lease time): 86400s (1 day)			
54 (DHCP server): 192.168.1.1			
6 (DNS servers):Plantilla:Unordered list			



CONFIGURACION DE RED

DHCP REQUEST

DHCPREQUEST				
	OP	HTYPE	HLEN	HOPS
0x01	0x01	0x08	0x00	
XID				
0x3903F326				
SECS		FLAGS		
0x0000		0x0000		
CIADDR				
0x00000000				
YIADDR				
0x00000000				
SIADDR				
GIADDR				
0x00000000				
CHADDR				
0x00053C04				
0x8D590000				
0x00000000				
0x00000000				
192 octets of 0's. BOOTP legacy				
Magic Cookie				
0x63825363				
DHCP Options				
DHCP option 53: DHCP Request				
DHCP option 50: 192.168.1.100 requested				
DHCP option 54: 192.168.1.1 DHCP server.				



CONFIGURACION DE RED

DHCP ACK

DHCPACK			
UDP Src=192.168.1.1			
sPort=67 Dest=255.255.255.255 dPort=68			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0xC0A80164			
SIADDR (Server IP Address)			
0x00000000			
GIADDR (Gateway IP Address switched by relay)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0's. BOOTP legacy			
Magic Cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP ACK			
DHCP option 1: 255.255.255.0 subnet mask			
DHCP option 3: 192.168.1.1 router			
DHCP option 51: 1 day IP lease time			
DHCP option 54: 192.168.1.1 DHCP server			



CONFIGURACION DE RED

PUERTOS

UDP (No Orientado a la conexión)

- 67/UDP (servidor)
- 68/UDP (cliente)



CONFIGURACION DE RED

¿QUE ES UNA CONCESIÓN?

Para optimizar los recursos de red, las direcciones IP se asignan con una fecha de inicio y de vencimiento para su validez. Esto es lo que se conoce como "concesión". Un cliente que detecta que su concesión está a punto de vencer, puede solicitarle al servidor una extensión de la misma por medio de un DHCPREQUEST. Del mismo modo, cuando el servidor detecta que una concesión va a vencer, enviará un DHCPNAK para consultarle al cliente si desea extenderla. Si el servidor no recibe una respuesta válida, convertirá la dirección IP en una dirección disponible.



CONFIGURACION DE RED

¿IP FIJA O AUTOMATICA?



RETO

CONFIGURAR UN SERVICIO DHCP



TELNET

Telnet (Telecommunication Network) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.



TELNET - SEGURIDAD

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar).



TELNET

- Los dominios de uso general del telnet tienen varias vulnerabilidades descubiertas a lo largo de los años, y varias más que podrían aún existir.
- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.
- Telnet carece de un esquema de autenticación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

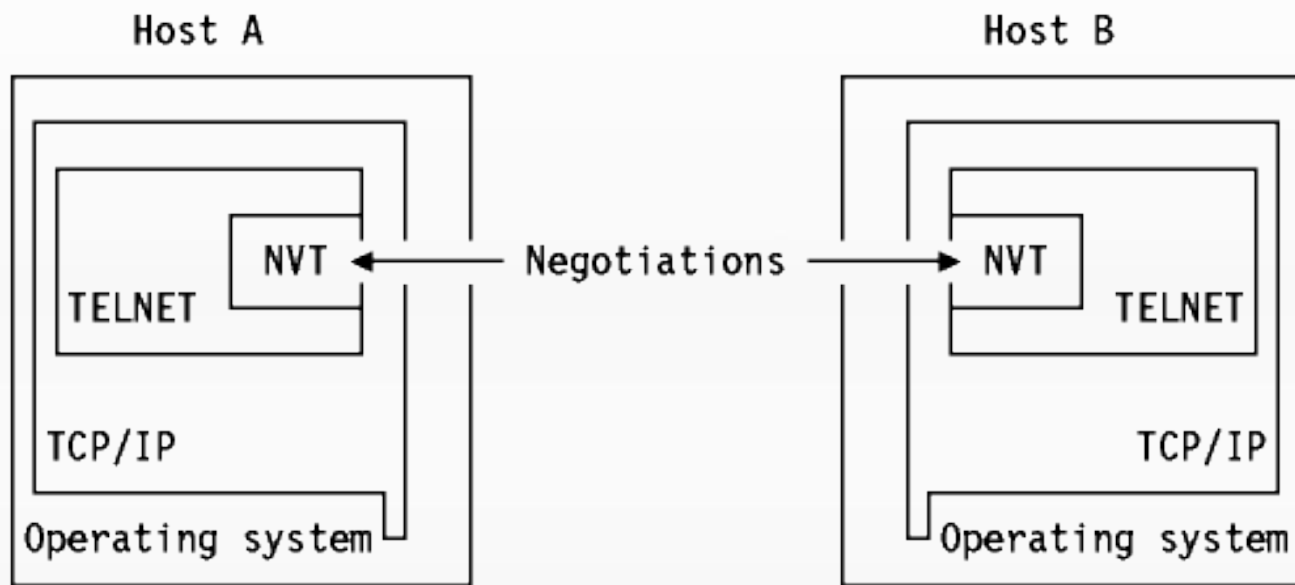


TELNET

- Los dominios de uso general del telnet tienen varias vulnerabilidades descubiertas a lo largo de los años, y varias más que podrían aún existir.
- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.
- Telnet carece de un esquema de autenticación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.



TELNET



RETO

CONFIGURAR UN SERVICIO TELNET



¿PREGUNTAS?



GRACIAS

