

LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: Servizo DHCP – MS Windows – Logs
 Portátil Regleta Switch 5-Port Gigabit Adaptadores USB-RJ45 Máquina virtual Windows Server 2019 Hosts alumnado Cableado de rede, [1] Protocolo DHCP [2] DHCP Windows Server [3] Administrador de servidores [4] Práctica 1 [5] Práctica 6 [6] Rexistros de eventos [7] Análisis archivos rexistro DHCP-Server [8] APIPA 	 Prerrequisito: Práctica 1 [4] e Práctica6 [5] Conectar portátil e hosts do alumnado ao switch. HostA alumnado: Arrancar máquina virtual Windows Server 2019 Configurar a rede según o escenario. Instalar e configurar o servidor DHCP Portátil: Arrancar co USB Live Kali amd64 Cliente DHCP Hosts alumnado:

Procedemento:

- (1) Conectar no mesmo segmento de rede o portátil e os hosts do alumnado.
 - a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.
 - b) Conectar o switch á regleta.
 - c) Desconectar o portátil da roseta da aula e conectalo ao switch.
 - d) Desconectar o cableado de rede nos equipos do alumnado.
 - e) Conectar os adaptadores USB-RJ45 nos equipos do alumnado.
 - f) Conectar eses adaptadores USB-RJ45 co cableado de rede creado na <u>Práctica 1</u> [4] os vosos equipos de alumnado ao switch.
 - g) Non conectar o switch á roseta da aula.

(2) HostA alumnado: Arrancar a máquina virtual Microsoft Windows Server 2019 [5]

- a) Configurar a rede según o escenario. Abrir unha consola e executar:
 - > systeminfo #Amosar información de configuración detallada sobre o equipo e o seu sistema operativo > ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.
- b) Realizar a instalación e configuración do servidor DHCP en Microsoft Windows [1][2][3] según [5], é dicir, realizar o procedemento comentado no apartado (2.c) da <u>Práctica 6</u>.
- c) Avisar ao docente para a revisión
- (3) Portátil:
 - a) Arrancar co USB Live Kali amd64.

b) Configurar a rede para a NIC eth0. Executar nunha consola:

\$ setxkbmap es #Configurar teclado en español

\$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

/etc/init.d/avahi-daemon stop || systemctl stop avahi-daemon #Parar o demo avahidaemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.

/etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo networkmanager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

ip addr show eth0 #Amosar información sobre a NIC eth0.

dhclient -v eth0 #Solicitar configuración de rede para a NIC eth0. Como agora temos a MAC Address con permisos podemos obter a configuración de rede para o portátil.

- # ip addr show eth0 #Amosar información sobre a NIC eth0.
- # ip route #Amosar a táboa de enrutamento.

cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración
os servidores DNS a empregar para a resolución de nomes.

- c) Avisar ao docente para revisión.
- (4) Servidor DHCP: Visualizar os rexistros do servizo DHCP.
 - a) Visor de sucesos [6]



Figura 1: Windows + x (Atallo de Teclado).

Abrir Visor de eventos



Figura 2: Administrador de servidor - Herramientas - Abrir Visor de eventos

🛃 Visor de eventos				– 🗆 X
Archivo Acción Ver Ayuda				
🗢 🔿 🙇 📰 🛛 🗊				
Visor de eventos (local)	^	Windows		Acciones
 Vistas personalizadas Registros de Windows 		Nombre	^	Windows 🔺
 Registros de aplicaciones y servicios Fventos de hardware 		Desired State Configuration DeviceGuard		 Abrir registro Crear vista per
i Licenso de Inducese i Internet Explorer ✓ Microsoft		DeviceManagement-Enterprise-Diagnostics-Provider Devices-Backaround		Importar vista
> AppV		DeviceSetupManager		Ver
User Experience Virtualization Windows		DeviceSync DeviceUpdateAgent		Actualizar
> AD > All-User-Install-Agent		Dhcp-Client DHCP-Server		DHCP-Server
> 🧮 AllJoyn > 🎬 Aplicaciones-API		DHCPv6-Client		Abrir
> 🧮 AppHost > 🔛 AppID		Diagnosis-PCW		👔 Ayuda
> ApplicabilityEngine		Diagnosis-PLA Diagnosis-Scheduled		
> Application Server-Applications		Diagnosis-Scripted		
> 🛗 AppLocker > 🛗 AppModel-Runtime		Diagnosis-ScriptedDiagnosticsProvider Diagnostics-Networking		
> AppReadiness		DirectoryServices-Deployment		
> Apps	~		>	
-	-			1

Figura 3: Registros de aplicaciones y servicios - Microsoft - Windows - DHCP Server



Figura 4: Registros de aplicaciones y servicios - Microsoft - Windows - DHCP Server - Abrir

Como podemos observar na Figura 4 de momento non temos rexistros sobre o servidor DHCP. No voso caso, ao seguir os pasos anteriores indicar que acontece e o por que.

b) Administrador DHCP: Concesiones de direcciones

🟆 DHCP				_	×
Archivo Acción Ver Ayuda					
🗢 🄿 🗾 🖬 🖳 🖬					
DHCP	Dirección IP del clie	Nombre	Expiración de cesión	Acciones	
VIN-CID6KG9HJ4D	No.	lan alamantan diamani	l las an asta cinta	Concesiones de direcciones	
V b IPv4		nay elementos disponi	bies en esta vista.		
✓				Acciones adicionales	•
Conjunto de direcciones					
🔀 Concesiones de direcciones	N >				
> 📓 Reservas	ver /				
Copciones de ámbito	Actualizar				
📓 Directivas	Evnortar lista				
😭 Opciones de servidor	Exportal lista				
Directivas	Ayuda				
> 📝 Filtros					
> 🛃 IPv6					

Figura 5: Administrador DHCP - Concesiones de direcciones - Actualizar



Figura 6: kali - 10.10.10.100

Ao actualizar no voso servidor DHCP deberíades obter unha situación similar á da Figura 6. No voso caso, ao seguir os pasos anteriores indicade que acontece e o por que.

c) Rexistros depuración servidor DHCP C:\Windows\System32\dhcp*.log [6]

🏆 DHCP		
Archivo Acción	Ver Ayuda	
🗢 🄿 🔁 📊	🗎 🗟 📄 🛛 🛅 📮 🖳	
	Contenido del servidor DHCP Ámbito [10.0.0.0] Rede_10.10.1 Mostrar estadísticas Ámbito nuevo Superámbito	10.
> 🐻 IPvé	Nuevo ámbito de multidifusión Configurar conmutación por error Replicar ámbitos de conmutación por error Definir clases de usuario Definir clases de proveedor	
Abre el cuadro o	Reconciliar todos los ámbitos	
	Configurar opciones predeterminadas Ver > Actualizar Exportar lista	
	Propiedades	
	Ayuda	

Figura 7: Administrador DHCP - IPv4 - Propiedades

Propiedades: IPv4	?	×
General DNS Filtros Conmutación por error Opciones avanzadas		
Especifique el número de veces que el servidor DHCP debería intentar la detección de una dirección IP antes de que el servidor conceda la dirección a un cliente.		
Intentos de detección de conflictos:		
R <u>u</u> ta del archivo de registro de auditoría: C:\Windows\system32\dhcp <u>Ex</u> aminar		
Cambiar los enlaces de las conexiones del servidor: E <u>n</u> laces		
Credenciales de registro de actualizaciones (Cre <u>d</u> enciales) dinámicas de DNS:		
Aceptar Cancela	r A	Apli <u>c</u> ar

Figura 8: Ruta archivo de registro de auditoría: C:\Windows\System32\dhcp

Abrir unha consola powershell e executar:
> cd c:\windows\system32\dhcp #Acceder ao directoro c:\windows\system32\dhcp.
> dir #Ver o contido do directorio.
> \$dia=get-date -Format "dddd" #Crear a variable dia a cal contén o valor do nome do día da semana na que estás a executar o comando.
> \$diaAbrev=\$dia.Substring(0,2) #Crear a variable diaAbrev a ca contén como valor os 2 primeiros caracteres do valor da variable dia.
> more DhcpSrvLog-\$diaAbrev*.log #Ver de forma paxinada por pantalla o contido do ficheiro do rexistro de auditorái do día de hoxe (do día que estás a executar este comando).
Consultar [7] e indicar a saída que proporciona este log?

- (5) Avisar ao docente para revisión.
- (6) Actualizar o visor de eventos.

Visor de eventos		1				
Archivo Acción V Archivo Acción V	/er Al- iceMar	Abrir registro guardado Crear vista personalizada Importar vista personalizada				
> 🛄 Devi > 🛄 Devi	ices-Ba iceSetu	Ver	>	we-DHCD Server Events / Administrative	Tipo	Númer
> Devi	iceSync iceUpd	Actualizar		ws-DHCP Server Events/Notificaciones de filtros	Administrativo	0
> 🔛 Dhcp 🗸 🛄 DHC	p-Clier P-Server	Ayuda	>	ws-DHCP Server Events/Operativo	Operativo	0
I N	Microsoft-Wi Microsoft-Wi	ndows-DHCP ndows-DHCP				

Figura 11: Visor de eventos - Actualizar

Visor de eventos			
Archivo Acción Ver Ayuda			
🗢 🔿 🔁 🗊 🖬			
> 🧮 DeviceManagement-Enterprise	DHCP-Server		
> Devices-Background	Nombre	Tino	Númerr
> DeviceSetupManager		A L C C L C	4
> 🔛 DeviceSync	Microsoft-Windows-DHCP Server Events/Administrativo	Administrativo	1
> DeviceUpdateAgent	Microsoft-Windows-DHCP Server Events/Notificaciones de filtros	Administrativo	0
> 🧮 Dhcp-Client	Microsoft-Windows-DHCP Server Events/Operativo	Operativo	0
✓ I DHCP-Server			
Microsoft-Windows-DHCP:			
Microsoft-Windows-DHCP	~		

Figura 9: Visor de eventos - DHCP Server - Administrativo

Visor de eventos				
Archivo Acción Ver Ayuda				
🗢 🔿 🔁 📰 🛛 🖬				
> 📔 DeviceManagement-Enterprise 🔺	OHCP-Server			
> 🧮 Devices-Background	Newskar		Time	Méren
> 🧮 DeviceSetupManager	Nombre		Про	Numero
> 🧾 DeviceSync	Microsoft-Windows-DHCP Server Events/Adm	inist	A desinistrativo	1
> DeviceUpdateAgent	Microsoft-Windows-DHCP Server Events/Notif	icac Abrir	ativo	0
> 📔 Dhcp-Client	Microsoft-Windows-DHCP Server Events/Oper	ative Propiedad	es	0
✓ ☐ DHCP-Server		Avuda		
Microsoft-Windows-DHCP		Ayuuu		
📓 Microsoft-Windows-DHCP 🗸				
<>	c			>

Figura 10: Visor de eventos - DHCP Server - Administrativo - Abrir

Ricardo Feijoo Costa

Que acontece? Podedes ver rexistros novos? En tal caso: cales e que indican?

Avisar ao docente para revisión.

- (7) Hosts alumnado:
 - a) Crear e arrancar unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):
 - i. RAM ≥ 2048MB
 - ii. CPU ≥ 2
 - iii. PAE/NX habilitado
 - iv. Rede: Soamente unha tarxeta activada en modo bridge (ponte). Escoller a NIC correspondente ao adaptador USB-RJ45
 - v. ISO: Kali Live amd64
 - vi. Nome: Practica9-Cliente-DHCP
 - b) O xestor de redes NetworkManager está habilitado. Por defecto, está xerada unha conexión da interface eth0 solicitando a configuración de rede mediante DHCP. Comprobar se isto é correcto, deberiades ver unha imaxe similar á seguinte:

		<u></u>	مىلىيە بىغانىيە	🗂 🔌 🌲 🛢 11:10 🛛 🖴 G-
				 Enable <u>Networking</u> Enable N<u>o</u>tifications Connection <u>Information</u>
		Network Connect	tions	Edit Connections
		ion1		2014
	Editing Wired connection	1	00	8
Connection name Wired conn	ection 1			
General Ethernet 80	02.1X Security DCB	Proxy IPv4 Settings	IPv6 Settings	
Method Automatic (DHCP)			-	
Additional static addresses				
Address	Netmask	Gateway	Add	

c) Executar nunha consola,

- \$ setxkbmap es #Configurar teclado en español
- \$ ip addr show eth0 #Amosar información sobre a NIC eth0.
- \$ ip route #Amosar a táboa de enrutamento.

\$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes.

- d) Realizar de novo os apartados (4.b), (4,c) e (6) Que acontece? Por que?
- e) Avisar ao docente para revisión.

(8) Hosts alumnado:

- a) Crear unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):
 - i. RAM ≥ 2048MB
 - ii. CPU ≥ 2
 - iii. PAE/NX habilitado
 - iv. Rede: Soamente unha tarxeta activada en modo bridge (ponte). Escoller a NIC correspondente ao adaptador USB-RJ45
 - v. Sistema operativo instalado: Windows amd64
 - vi. Nome: Practica9-Cliente-Windows-DHCP

- b) Arrancar cada máquina virtual.
- (9) Hosts alumnado: Máquinas virtuais Practica9-Cliente-Windows-DHCP
 - a) Configurar o xestor de redes de Microsoft Windows para que a conexión ethernet solicite a configuración de rede mediante DHCP:

Conexiones de red	. 🗌	\times
A Section A sectio	ones de red	P
Organizar 👻 Deshabilitar este dis	•	?
Organizar Desnabilitar este dis Ethernet Red Intel(R) PRO/1000 MT Deskt Funciones de red Conectar con: Intel(R) PRO/1000 MT Desktop Adapter Intel(R) PRO/1000 MT Deskt Intel(R) PRO/1000 MT Desktop Adapter Configurar Esta conexión usa los siguientes elementos: Image: Programador de paquetes QoS Propriedades: Protocolo de Internet versión 4 (TCP/IPv4) Propriedades: Protocolo de Internet versión 4 (TCP/IPv4) X General Configuración alternativa Vede hacer que la configuración IP se asigne automáticamente si la	- •	•
A		
1 elemento 1 elemento seleccionado O Usar las siguientes direcciones de servidor DNS:		i== 📼

b) Abrir unha consola e comprobar a configuración de rede. Executar:

> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede. >

c) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?

(10) HostA alumnado - Máquina virtual Microsoft Windows Server 2019:

- a) Parar o servizo DHCP. Abrir unha consola e executar:
 - > net start #Amosar cales son os servizos en execución.
 - > net stop "servidor dhcp" #Deter o servizo DHCP.
 - > net start #Amosar cales son os servizos en execución.
- b) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?
- c) Realizar de novo o apartado (3). Que configuración de rede obtedes para o portátil? Cubrir a seguinte táboa:

Host	IP	Máscara Subrede	Gateway	Servidores DNS
Portátil				

- d) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?
- e) Avisar ao docente para a revisión.
- f) Arrancar o servizo DHCP. Abrir unha consola e executar:
 - > net start "servidor dhcp" #Arrancar o servizo DHCP.
 - > net start #Amosar cales son os servizos en execución.
- g) Realizar de novo os apartados (4.b), (4.c) e (6) Que acontece? Por que?
- h) Avisar ao docente para a revisión.

(11) HostA alumnado - Máquina virtual Microsoft Windows Server 2019:

a) Consultar no visor de eventos os rexistros xenéricos de Windows:



Figura 12: Visor de eventos – Registros de Windows - Sistema

b) Buscar no rexistro xenérico Sistema o patrón dhcp:





🛃 Visor de eventos					
Archivo Acción Ver Ayuda					
🗢 🔿 📶 🛛 🖬					
Visor de eventos (local)		^	Sistema Número de eve	entos: 4.172	
 Vistas personalizadas Registros de Windows Aplicación Seguridad Instalación Sistema 	Buscar		Nivel (i) Información (i) Información (i) Información	Fecha y hora 15/10/2022 20:43:50 15/10/2022 20:42:42 15/10/2022 20:40:12	×
 Registros de aplicaciones y servicios Eventos de hardware 	Buscar:	dhcp		Siguiente	
 Internet Explorer Microsoft AppV User Experience Virtualization Windows 			El servicio Servicio de	Cancelar implementación de Ap	pX (AppXS

Figura 14: Buscar - dhcp

c) Consultar todos os sucesos atopados premendo en Siguiente:

🛃 Visor de eventos							
Archivo Acción Ver Ayuda							
🗢 🔿 🙍 🖬 🛛 🖬							
Visor de eventos (local)		^	Sistema	Número de e	ventos: 4.	172 (!) Nuevos ev	entos disponibles
 Vistas personalizadas Registros de Windows 			Nivel		Fecha	a y hora	Ori
📓 Aplicación			1 Inform	ación	15/10	/2022 20:32:13	Ser
😭 Seguridad			Advert	encia	15/10	/2022 20:32:13	Tin
Instalación	Buscar					×	< Ser
🛃 Sistema							DH
Eventos reenviados	Buscar:	dhcp				Siguiente	Ser
Registros de aplicaciones y servicios							
😭 Eventos de hardware					- I	Cancelar	1
📔 Internet Explorer							1
✓ Microsoft		_					
> 🚞 AppV							
> 🚞 User Experience Virtualization			El serv	icio Servidor L	HCP entr	o en estado "en o	ejecución".
✓							

Figura 15: Buscar dhcp - Siguiente

- d) Indicar se agora sodes quen de atopar os rexistros da parada (stop) e da execución (start) do servidor DHCP realizado no apartado (10). Se é así, cubride cada rexistro start/stop atopado na Táboa Registros de Windows (ver última páxina). Se é preciso xerade máis táboas seguindo este modelo.
- e) Avisar ao docente para revisión.
- (12) Contesta e razoa brevemente:
 - a) Nalgún apartado desta práctica os clientes DCHP obtiveron unha IP dentro do seguinte rango: 169.254.0.0-169.254.255.255 [8]. Se é o caso indica onde foi rexistrado ese suceso, ou como pode consultarse.
 - b) Avisar ao docente para a entrega e revisión da práctica.

Revisión:



	Registros de Windows - Sistema								
Estado DHCP- Server	Nivel	Fecha y hora	Origen	ld. del evento	Categoría de la tarea	General	Detalles		
start									
stop									