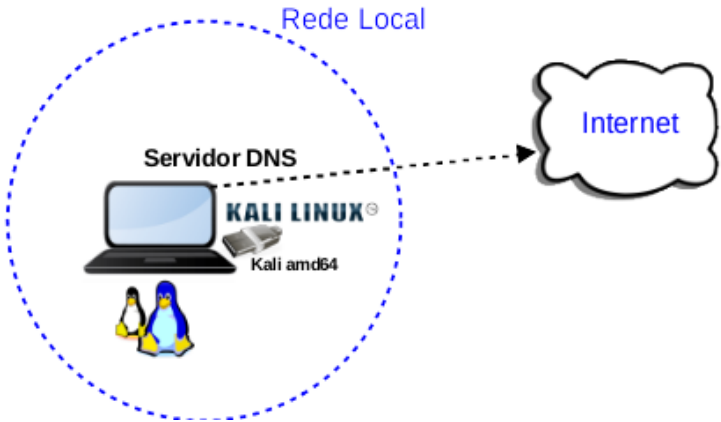


TALLER SR – PRÁCTICA 12 – Servizo DNS: bind9		
NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: Servizo DNS (bind9)

Portátil: USB  
Rede Local Live Kali amd64  
MAC filtrada (con acceso)  
Servidor DNS: IP dinámica según MAC Address



**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 DNS – bind9
<ul style="list-style-type: none"><li>■ Portátil</li><li>■ Regleta</li><li>■ USB Live amd64 Kali</li><li>■ Cableado de rede</li><li>■ [1] <a href="#">Titorial DNS</a></li><li>■ [2] <a href="#">bind</a></li><li>■ [3] <a href="#">Práctica 11</a></li><li>■ [4] <a href="#">Práctica 1</a></li><li>■ [5] <a href="#">Servidor DNS Caché</a></li><li>■ [6] <a href="#">Debian Wiki - bind9</a></li><li>■ [7] <a href="#">Kali - bind9</a></li></ul>	<p>(1) Prerrequisito: <a href="#">Práctica 11</a> [3] e <a href="#">Práctica 1</a> [4]</p> <p>(2) Portátil:</p> <ul style="list-style-type: none"><li>a) Conectar portátil á roseta da aula.</li><li>b) Arrancar co USB Live amd64 Kali</li><li>c) Instalar e configurar o servidor DNS: <a href="#">bind9</a> [1][2][5]</li><li>d) Comprobar orde resolución DNS (/etc/nsswitch.conf)</li><li>e) Comprobar funcionamento servidor DNS</li><li>f) Comprobar funcionamento servidor caché DNS</li></ul>



## Procedemento:

- (1) Conectividade no segmento da rede da aula:
  - (a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.
  - (b) Conectar co cableado de rede creado na [Práctica 1](#) [4] o portátil á roseta da aula.
- (2) Portátil:
  - (a) Arrancar cun USB Live amd64 Kali GNU/Linux
    - I. Editar o xestor de arranque para modificar o hostname:
      - a) Escoller a primeira opción coas frechas de selección.
      - b) Entrar no modo edición premendo a tecla Tab ↹
      - c) Ao final das opcións de arranque escribir:  
hostname=portatil-grupoN

*NOTA: Substituír N polo número de grupo, por exemplo o grupo 6, escribirá:*

*hostname=portatil-grupo6*



- d) Premer a tecla Enter ↵ para arrancar.

- (b) Comprobar que tedes acceso á rede local e a Internet. Abrir unha consola e executar:

```
$ setxkbmap es #Configurar teclado en español
$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar a configuración de rede paa a NIC eth0
$ ping -c4 www.google.es #Enviar 4 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.
```

- (c) Instalar o servidor DNS bind9 [1][2][5]. Executar na consola anterior:

```
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt -y install bind9 #Instalar o paquete bind9, é dicir, instalar o servidor DNS bind9. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

(d) Arrancar o servidor DNS bind9 [1][2][5]. Executar na consola anterior:

```
# A=$(grep -n '}$' /etc/apparmor.d/usr.sbin.named | cut -d':' -f1)#Atopar a liña onde aparece o patrón buscado } no ficheiro de configuración /etc/apparmor.d/usr/sbin.named e gardalo na variable A

# sed -i "${A}s|.*/sys/kernel/mm/transparent_hugepage/enabled r,\n|}" /etc/apparmor.d/usr.sbin.named
#Engadir ao arquivo de configuración /etc/apparmor.d/usr.sbin.named, as directivas necesarias para que apparmor permita o arranque do servidor DNS bind9 (named)

# A=$(grep -n '}$' /etc/apparmor.d/usr.sbin.named | cut -d':' -f1)#Atopar a liña onde aparece o patrón buscado } no ficheiro de configuración /etc/apparmor.d/usr/sbin.named e gardalo na variable A

# sed -i "${A}s|.*/etc/ssl/kali.cnf r,\n|}" /etc/apparmor.d/usr.sbin.named #Engadir ao arquivo de configuración /etc/apparmor.d/usr.sbin.named, a directiva necesarias para que apparmor permita o arranque do servidor DNS bind9 (named)

# apparmor_parser -r /etc/apparmor.d/usr.sbin.named #Facer efectivos os cambios de configuración de apparmor realizados anteriormente no ficheiro /etc/apparmor.d/usr.sbin.named

# /etc/init.d/named start #Arrancar o servidor DNS bind9 (named)

# /etc/init.d/named status #Ver o estado do servizo named, é dicir, o estado so servidor DNS bind

# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local do usuario kali.
```

(e) Avisar ao docente para revisión. ☐

(f) Comprobar o contido do ficheiro /etc/hosts. Executar na consola anterior:

```
$ cat /etc/hosts #Ver o contido do ficheiro /etc/hosts, o cal contén unha táboa estática para procura de hostnames, é dicir, asocia unha IP cun hostname ou varios.
```

(g) Comprobar a orde de resolución DNS (/etc/nsswitch.conf (Name Server Switch ou NSS) para o equipo local, neste caso o portátil. Executar na consola anterior:

```
$ cat /etc/nsswitch.conf #Ver o contido do ficheiro de configuración /etc/nsswitch.conf, o cal na “base de datos” hosts determina a orde de procura da resolución DNS do equipo local.

$ grep hosts /etc/nsswitch.conf #Buscar o patrón hosts en /etc/nsswitch.conf, é dicir, ver o contido do ficheiro de configuración /etc/nsswitch.conf referente á “base de datos” hosts, o cal determina a orde de procura da resolución DNS do equipo local.
```

(h) Comprobar o contido do ficheiro /etc/resolv.conf. Executar na consola anterior:

```
$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
```

(i) Comprobar a táboa de enrutamento. Executar na consola anterior:

```
$ ip route #Ver a táboa de rutas do sistema.
```

(j) Cubrir a seguinte táboa:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)	IP Servidor DNS (eth0)
Portátil					

(k) Comprobar o funcionamento como servidor DNS caché:

I. Executar na consola anterior:

```
$ ping -c2 localhost #Comprobar conectividade coa máquina localhost. Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada localhost que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E se a entrada non existe intentárase coa seguinte fonte definida no ficheiro /etc/nsswitch.conf.

$ ping -c2 localhost.local #Comprobar conectividade coa máquina localhost.local Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada localhost que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E como non existe, compróbase coa segunda entrada mdns4_minimal [NOTFOUND=return] a cal emprega o servizo avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este servizo non resolve o código [NOTFOUND=return] indica que non se continúe buscando nas seguintes fontes.

$ ping -c2 $(hostname) #Comprobar conectividade coa máquina portatil-grupoN (sendo N o número do grupo - ver apartado (2.I.c)-. Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada referente ao nome do equipo resultado da execución $(hostname), que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E se a entrada non existe intentárase coa seguinte fonte definida no ficheiro /etc/nsswitch.conf.
```

\$ ping -c2 \$(hostname).local #Comprobar conectividade coa máquina portatil-grupoN (sendo N o número do grupo - ver apartado (2.I.c)-. Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada referente ao nome do equipo resultado da execución \$(hostname), que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E como non existe, compróbase coa segunda entrada mdns4\_minimal [NOTFOUND=return] a cal emprega o servizo avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este servizo non resolve o código [NOTFOUND=return] indica que non se continúa buscando nas seguintes fontes.

II. Indica nos 4 comandos anteriores (apartado I) en cales e por que existe ou non conectividade?

III. Executar na consola anterior:

\$ ping -c2 www.google.es #Comprobar conectividade coa máquina www.google.es Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada referente ao nome dns www.google.es, que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E como non existe, compróbase coa segunda entrada mdns4\_minimal [NOTFOUND=return] a cal emprega o servizo avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este servizo non resolve, e non sendo o nome dns .local, continúaase buscando nas seguintes fontes, neste caso na fonte dns, a cal comproba se é posible a resolución con servidores dns especificados no ficheiro /etc/resolv.conf

Cubrir as seguintes táboas:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)	IP Servidor DNS (eth0)
Portátil					

Host	IP www.google.es (ver saída comando ping)	Servidor/es DNS que otorgan a IP de google
Portátil		

IV. Executar na consola anterior:

\$ dig @localhost www.google.es #Obriga a resolver o nome do dominio www.google.es mediante o servidor DNS local instalado e arrancado nos apartados (2.c) e (2.d) respectivamente, sen ter en conta o o ficheiro /etc/nsswitch.conf

\$ dig @localhost www.google.es #Obriga a resolver o nome do dominio www.google.es mediante o servidor DNS local instalado e arrancado nos apartados (2.c) e (2.d) respectivamente, sen ter en conta o o ficheiro /etc/nsswitch.conf

Fíxate nos tempos de conexión (Query time). Apúntaos na táboa do apartado (3.a).

Cubrir as seguintes táboas:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)	IP Servidor DNS (eth0)
Portátil					

Host	IP www.google.es (ver saída comando ping)	Servidor/es DNS que otorgan a IP de google
Portátil		



V. Executar na consola anterior:

\$ ping -c2 www.google.es #Comprobar conectividade coa máquina www.google.es Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada referente ao nome dns www.google.es, que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E como non existe, compróbase coa segunda entrada mdns4\_minimal [NOTFOUND=return] a cal emprega o servizo avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este servizo non resolve, e non sendo o nome dns .local, continúaase buscando nas seguintes fontes, neste caso na fonte dns, a cal comproba se é posible a resolución con servidores dns especificados no ficheiro /etc/resolv.conf

Cubrir as seguintes táboas:

Host	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)	IP Servidor DNS (eth0)
Portátil					

Host	IP www.google.es (ver saída comando ping)	Servidor/es DNS que otorgan a IP de google
Portátil		

VI. Comparar as táboas dos apartados III, IV, e V. Indica que acontece e por que?

VII. Editar o ficheiro de configuración /etc/resolv.conf. Executar na consola anterior:

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

```
# sed -i 's/nameserver/#nameserver/' /etc/resolv.conf #Comentar as liñas correspondentes ás entradas dos servidores DNS no ficheiro /etc/resolv.conf
```

```
# echo 'nameserver 127.0.0.1' » /etc/resolv.conf #Engadir a entrada do servidor DNS local (127.0.0.1) no ficheiro /etc/resolv.conf, é dicir, activar localhost como servidor DNS.
```

```
# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local do usuario kali.
```

VIII. Realizar de novo os comandos:

\$ ping -c2 www.google.es #Comprobar conectividade coa máquina www.google.es Para iso, lese a “base de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita, sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada referente ao nome dns www.google.es, que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E como non existe, compróbase coa segunda entrada mdns4\_minimal [NOTFOUND=return] a cal emprega o servizo avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este servizo non resolve, e non sendo o nome dns .local, continúaase buscando nas seguintes fontes, neste caso na fonte dns, a cal comproba se é posible a resolución con servidores dns especificados no ficheiro /etc/resolv.conf

\$ dig @localhost www.google.es #Obriga a resolver o nome do dominio www.google.es mediante o servidor DNS local instalado e arrancado nos apartados (2.c) e (2.d) respectivamente, sen ter en conta o o ficheiro /etc/nsswitch.conf

Fíxate na IP da resolución DNS do comando ping e no rexistro A da resolución co comando dig. Indica que acontece e por que?

(I) Avisar ao docente para revisión. ☐



(3) Contesta e razoa brevemente:

(a) Realizado o apartado (2.k.IV) cubre a seguinte táboa:

Host	Tempo execución	Tempo execución
	Primeiro comando dig (RR rexistro A)	Segundo comando dig (RR rexistro A)
Portátil		

Existe algunha diferenza nos tempos de execución?

(b) O apartado anterior indica que o servidor bind9 instalado é por defecto un servidor DNS caché?

(c) Limpar caché DNS. Executar na anterior consola:

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

# rndc flush #Eliminar a caché DNS

# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local do usuario
kali.

$ ping -c2 www.google.es #Comprobar conectividade coa máquina www.google.es Para iso, lese a “base
de datos” hosts do ficheiro /etc/nsswitch.conf, comprobando as fontes que aparecen de esquerda a dereita,
sendo a primeira que aparece files, co cal, compróbase no ficheiro /etc/hosts se existen unha entrada
referente ao nome dns www.google.es, que apunte a unha IP á cal enviar os paquetes ICMP do comando ping. E
como non existe, compróbase coa segunda entrada mdns4_minimal [NOTFOUND=return] a cal emprega o servizo
avahi-daemon: se este servizo resolve prodúcese o envío dos paquetes ICMP do comando ping, e se este
servizo non resolve, e non sendo o nome dns .local, continúaase buscando nas seguintes fontes, neste caso
na fonte dns, a cal comproba se é posible a resolución con servidores dns especificados no ficheiro
/etc/resolv.conf

$ dig @localhost www.google.es #Obriga a resolver o nome do dominio www.google.es mediante o
servidor DNS local instalado e arrancado nos apartados (2.c) e (2.d) respectivamente, sen ter en conta o o
ficheiro /etc/nsswitch.conf

$ dig @localhost www.google.es #Obriga a resolver o nome do dominio www.google.es mediante o
servidor DNS local instalado e arrancado nos apartados (2.c) e (2.d) respectivamente, sen ter en conta o o
ficheiro /etc/nsswitch.conf
```

Fíxate nos tempos de conexión (Query time). Indica que acontece e por que?

(d) Avisar ao docente para revisión. ☐

