

الوحدة الثانية: خادم DHCP وخادم DNS

ادارة شبكات 2

م. غنام الجعبري

خادم DHCP

- يستخدم خادم DHCP (DHCP Server) في تزويد الأجهزة المتصلة بالشبكة بإعدادات الشبكة تلقائياً (automatic) بدلاً من ضبط إعدادات كل جهاز على الشبكة يدوياً (static)
- يوفر خادم DHCP إدارة أكثر سهولة للشبكة لأن أي تغيير على إعدادات الاتصال بالشبكة يتم بشكل مركزي من خلال الخادم
- ابرز الإعدادات التي يوفرها خادم DHCP للأجهزة:
 - عنوان IP فريد لكل جهاز على الشبكة ضمن نطاق معين من العناوين (IP range)
 - عنوان العبارة الافتراضية (gateway)
 - عنوان خادم DNS الأساسي (primary) والثانوي (secondary)
 - اسم نطاق البحث (search domain) لإضافته إلى أسماء الأجهزة بشكل تلقائي عند عدم إلحاق نطاق معين إلى اسم الجهاز في الاتصال

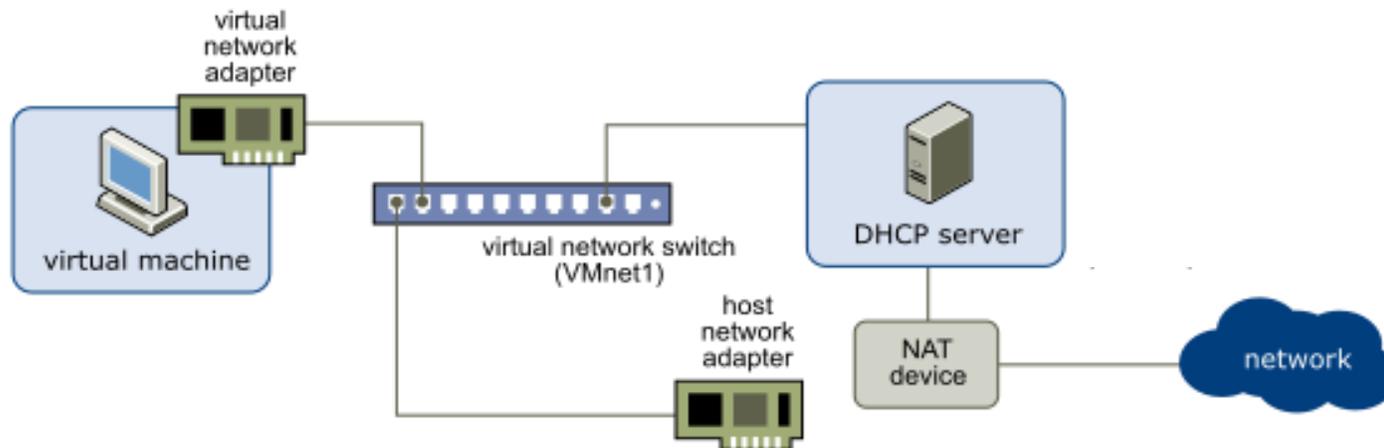
خادم DHCP

- عملية الحصول على عنوان IP من خادم DHCP تتضمن اربع رسائل تدعى (DORA):
 - اكتشاف (Discover): يقوم العميل بارسالها لكافة الاجهزة على الشبكة للبحث عن خادم DHCP
 - عرض (Offer): يقوم خادم DHCP بارسالها الى العميل لتقديم عنوان IP
 - طلب (Request): يقوم العميل بارسالها الى خادم DHCP للموافقة على العرض
 - تسليم (Acknowledge): يقوم خادم DHCP بارسالها الى العميل وتتضمن عنوان IP



خادم DHCP

- يتطلب اعداد خادم DHCP باستخدام برنامج VMware Workstation انشاء شبكة افتراضية (Host-only) على البرنامج تتكون من جهازين افتراضيين: الجهاز الاول يلعب دور خادم DHCP والجهاز الثاني يلعب دور العميل
- يحتوي خادم DHCP على بطاقتين للشبكة: البطاقة الاولى متصلة بالانترنت (NAT) باستخدام عنوان تلقائي والبطاقة الثانية متصلة بالشبكة الافتراضية (Host-only) باستخدام عنوان ثابت مثلا 192.168.1.10/24



خادم DHCP

- لتثبيت واعداد خادم DHCP، نقوم اولا بتحديث قائمة الحزم البرمجية على الانترنت:

```
sudo apt update
```

- ثم تثبيت خادم DHCP على نظام لينكس باستخدام الامر التالي:

```
sudo apt install isc-dhcp-server
```

- يتطلب اعداد خادم DHCP تعديل الملف التالي:

```
sudo nano /etc/dhcp/dhcpd.conf
```

- غالبا نقوم بإضافة نطاق من العناوين لتوزيعها على الأجهزة بشكل عشوائي كما في المثال التالي:

خادم DHCP

```
# minimal sample /etc/dhcp/dhcpd.conf
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.200;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.10, 192.168.1.11;
  option domain-name "example.com";
  default-lease-time 600;
  max-lease-time 7200;
}
```

- يتيح هذا المثال إسناد عناوين من 192.168.1.100 إلى 192.168.1.200 بشكل عشوائي لوقت أدناه 600 ثانية وأقصاه 7200 ثانية مع إسناد عنوان العبارة الافتراضية 192.168.1.1 وعنوان خادم DNS الأساسي 192.168.1.10 والثانوي 192.168.1.11 واسم نطاق البحث example.com

خادم DHCP

- اذا كان الخادم يحتوي على اكثر من بطاقة شبكة، يجب تحديد بطاقة الشبكة التي توفر خدمة DHCP عبر تحرير الملف التالي:

```
sudo nano /etc/default/isc-dhcp-server
```

- ثم اضافة اسم بطاقة الشبكة في الملف كما في المثال التالي:

```
INTERFACESv4="ens37"
```

- يمكن معرفة اسم بطاقة الشبكة من خلال تنفيذ الامر التالي:

```
ip addr
```

خادم DHCP

- بعد حفظ الإعدادات على الملف يجب إعادة تشغيل الخادم باستخدام الأمر التالي:

```
sudo systemctl restart isc-dhcp-server.service
```

- والتأكد من تشغيل خادم DHCP بنجاح باستخدام الأمر التالي:

```
sudo systemctl status isc-dhcp-server.service
```

- يمكن حجز عنوان IP لأحد الأجهزة على الشبكة من خلال خادم DHCP كما في المثال التالي:

```
host printer1 {  
    hardware ethernet 00:11:22:33:44:55;  
    fixed-address 192.168.1.20;  
}
```

- يتيح هذا المثال حجز 192.168.1.20 لطابعة لديها العنوان الفيزيائي 00:11:22:33:44:55

خادم DHCP

- يحتفظ خادم DHCP بالعناوين التي اسندها في الملف `/var/lib/dhcpd/dhcpd.leases`
- يمكن طباعة قائمة بالأجهزة التي حصلت على عنوان IP من خادم DHCP باستخدام الامر `dhcp-lease-list`
- يمكن إعادة تشغيل خادم DHCP في إصدارات لينكس السابقة باستخدام الامر التالي:

```
sudo service isc-dhcp-server restart
```

- والتأكد من تشغيل خادم DHCP بنجاح باستخدام الامر التالي:

```
sudo service isc-dhcp-server status
```

تمرين: خادم DHCP

- اصف نطاق من العناوين على خادم DHCP لتوزيعها على الاجهزة المتصلة بالشبكة من الشبكة الفرعية 172.16.0.0/24 تبدأ بالعنوان 172.16.0.100 وتنتهي بالعنوان 172.16.0.200 مع اسناد عنوان العبارة الافتراضية 172.16.0.1 وعنوان خادم DNS 172.16.0.10 على هذه الاجهزة لمدة 24 ساعة
- احجز العنوان 172.16.0.90 لطابعة متصلة بالشبكة من نوع Laser من خلال خادم DHCP علما بان عنوان MAC للطابعة 00:11:22:33:44:55

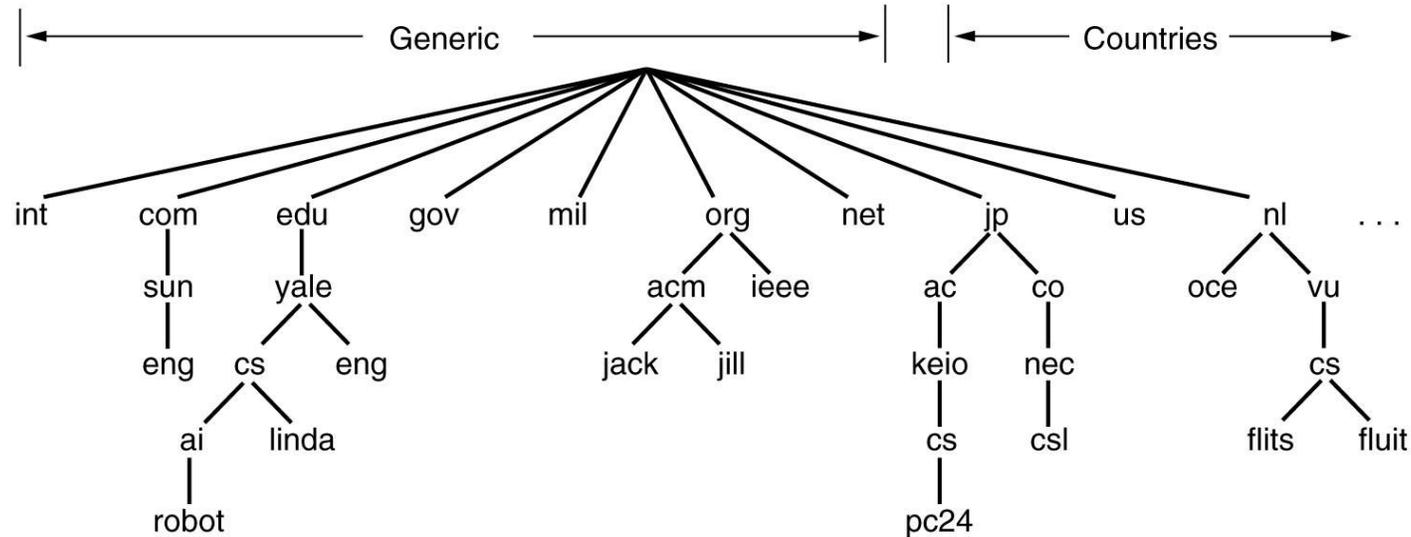
خادم DNS

- يستخدم خادم DNS (DNS Server) في تحويل أسماء النطاقات (domain names) إلى عناوين انترنت (IP addresses) وبالعكس
- يعتمد نظام اسماء النطاقات (DNS) في عمله على قاعدة بيانات (DB) موزعة على شبكة الإنترنت تحتوي على معلومات النطاقات وأسماء المواقع وعناوينها تحت كل نطاق
- يتكون اسم النطاق من مقطعين مثل example.com، يطلق على .com نطاق المستوى الاعلى (Top-Level Domain) او اختصارا، ويطلق على example.com نطاق المستوى الثاني (Second-Level Domain) او اختصارا



هيكلية DNS

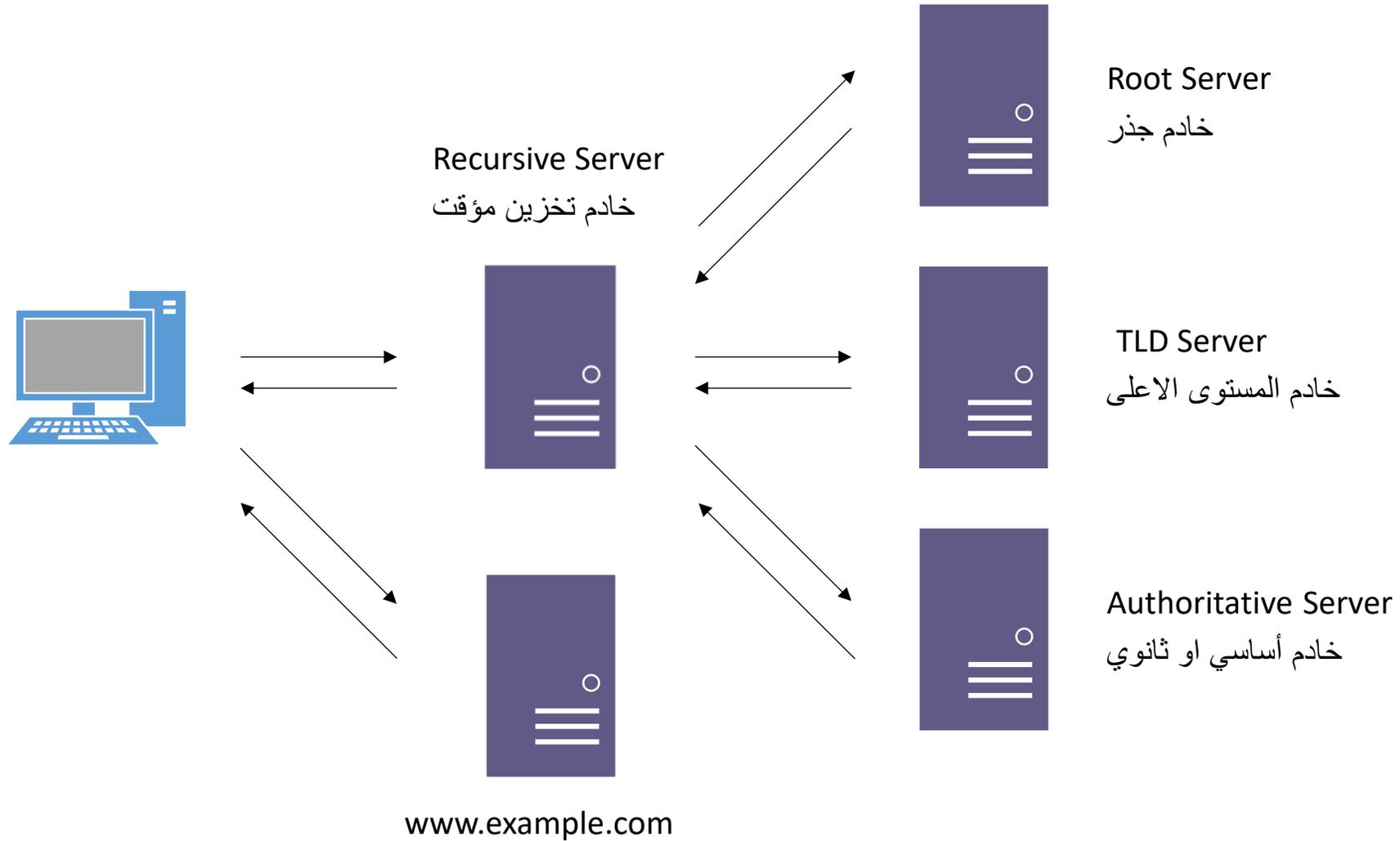
- يبدأ الاستعلام عن النطاقات من خوادم الجذر (root servers) وعددها 13 حول العالم
- نطاقات المستوى الاعلى (TLD) نوعان:
 - نطاقات المستوى الاعلى العامة (generic TLD)، او gTLD اختصارا، مثل .edu و .net و .com.
 - نطاقات المستوى الاعلى للدول (country code TLD)، او ccTLD اختصارا، مثل .uk و .jo و .ps.



خادم DNS

- يعمل خادم DNS على تخزين وإدارة معلومات النطاقات محليا ويتيح الوصول إليها عالميا
- يمكن اعداد خادم DNS ليلعب الأدوار التالية:
 - خادم تخزين مؤقت (Caching DNS Server)
 - خادم أساسي (Primary DNS Server)
 - خادم ثانوي (Secondary DNS Server)
- الهدف من اعداد خوادم التخزين المؤقت هو تقليل الطلب على الخوادم الأساسية او الثانوية وتسريع الحصول على رد في الاستعلام عن النطاقات الشائعة او الأكثر تكرارا

خادم DNS



خادم تخزين مؤقت

- يستخدم خادم التخزين المؤقت للاستعلام عن أسماء النطاقات وتحويلها إلى عناوين IP ثم تخزين نتائج الاستعلام بشكل مؤقت لتلبية الطلب بسرعة عند الاستعلام عنها مجدداً
- يستخدم خادم التخزين المؤقت عادة من قبل مزودي خدمات الانترنت (ISPs) لتحويل اسماء النطاقات الى عناوين IP على أجهزة المستخدمين
- الخطوة الأولى هي تثبيت خادم DNS على نظام لينكس:

```
sudo apt update  
sudo apt install bind9
```

- تثبيت خادم DNS يتضمن اعداد الخادم بشكل افتراضي ليقوم بدور خادم تخزين مؤقت
- يمكن معاينة عناوين خوادم الجذر (root servers) التي يستخدمها خادم DNS في الاستعلام عن أسماء النطاقات من الملف `/usr/share/dns/root.hints`

خادم تخزين مؤقت

- يمكن إضافة خوادم DNS عامة لتوجيه طلبات الاستعلام إليها أولاً قبل الاستعلام من خوادم DNS الجذر عبر تحرير الملف التالي:

```
sudo nano /etc/bind/named.conf.options
```

- ثم إضافة عناوين خوادم DNS العامة الى الملف كما في المثال التالي:

```
forwarders {  
    8.8.8.8;  
    1.1.1.1;  
};
```

- لتفعيل الاعدادات الجديدة، يجب إعادة تشغيل خادم DNS:

```
sudo systemctl restart bind9.service
```

خادم تخزين مؤقت

- والتأكد من تشغيل خادم DNS بنجاح باستخدام الأمر:

```
sudo systemctl status bind9.service
```

- يستخدم الأمر dig في الاستعلام عن أسماء النطاقات من خوادم DNS:

```
dig www.google.com
```

- يمكن الاستعلام عن أسماء النطاقات من خادم DNS عام كما في المثال التالي:

```
dig www.google.com @8.8.8.8
```

- أو الاستعلام عن أسماء النطاقات من خادم DNS محلي كما في المثال التالي:

```
dig www.google.com @192.168.1.10
```

خادم DNS أساسي

- يستخدم خادم DNS الأساسي لاستضافة النطاقات المسجلة والنطاقات الفرعية التابعة لها
- لكل نطاق على خادم DNS ملف يحتوي على مجموعة من السجلات المتعلقة بهذا النطاق يطلق عليها Resource Record أو اختصاراً RR
- أشهر أنواع السجلات المستخدمة في ملف النطاق:
 - NS – تحديد اسم خادم DNS المسؤول عن النطاق
 - MX – تحديد اسم خادم البريد الإلكتروني (Email) المسؤول عن النطاق
 - A – تحديد عنوان IP المقابل لاسم النطاق أو اسم الجهاز
 - PTR – تحديد اسم النطاق المقابل لعنوان IP
 - CNAME – تحديد نفس عنوان IP المستخدم في اسم نطاق آخر
- لإنشاء موقع ويب يتم إضافة سجل من نوع A إلى ملف النطاق أو سجل من نوع CNAME

انواع ملفات النطاقات

- هنالك نوعين من ملفات النطاقات على خادم DNS:
 - ملف نطاق امامي (forward zone) يستخدم في تحويل اسماء النطاقات الى عناوين IP
 - ملف نطاق عكسي (reverse zone) يستخدم في تحويل عناوين IP إلى اسماء نطاقات
- يستخدم النطاق in-addr.arpa في ملف النطاق العكسي في تحويل عناوين IPv4، على سبيل المثال للاستعلام عن اسم النطاق المقابل للعنوان 192.168.24.5 يتم إضافة سجل من نوع PTR للنطاق 5.24.168.192.in-addr.arpa

www.example.com → 192.168.24.5

conventional DNS resolution

www.example.com ← 192.168.24.5

reverse DNS resolution

خادم DNS أساسي

- يتم تحويل خادم DNS الى خادم اساسي للنطاق example.com عبر تحرير الملف التالي:

```
sudo nano /etc/bind/named.conf.local
```

- ثم اضافة zone الى الملف من نوع master:

```
zone "example.com" {  
    type master;  
    file "/etc/bind/db.example.com";  
};
```

- يمكن إنشاء ملف للنطاق example.com عن طريق نسخ أحد ملفات النطاقات المتوفرة واستخدامها كقالب:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

خادم DNS أساسي

- ثم تحرير ملف النطاق example.com:

```
sudo nano /etc/bind/db.example.com
```

- واستبدال localhost بالنطاق example.com والعنوان 127.0.0.1 بعنوان خادم DNS وإضافة سجل من نوع A لاسم النطاق ns.example.com حتى يبدو الملف كما يلي:

```
;  
; BIND data file for example.com  
;  
$TTL      604800  
@         IN      SOA    example.com. admin.example.com. (  
                2          ; Serial  
                604800     ; Refresh  
                86400      ; Retry  
                2419200    ; Expire  
                604800 )   ; Negative Cache TTL  
  
@         IN      NS     ns.example.com.  
@         IN      A      192.168.1.10  
ns        IN      A      192.168.1.10
```

خادم DNS أساسي

- بعد حفظ التغييرات على الملف، نقوم بإعادة تشغيل خادم DNS لتفعيل الإعدادات الجديدة:

```
sudo systemctl restart bind9.service  
sudo systemctl status bind9.service
```

- للتأكد من الإعدادات الجديدة، نستخدم الأمر dig للاستعلام عن النطاق example.com

```
dig example.com @192.168.1.10
```

- يمكن إعداد نظام لينكس للاستعلام بشكل افتراضي من خادم DNS عبر تحرير ملف إعدادات الشبكة في المجلد /etc/netplan/ كما في المثال التالي:

```
ens33:  
  addresses:  
    - 192.168.1.10/24  
  nameservers:  
    addresses: [192.168.1.10]
```

خادم DNS أساسي

- يمكن إضافة سجل من نوع CNAME الى ملف النطاق لتحويل `www.example.com` الى نفس عنوان IP المستخدم في استضافة `example.com`

```
;
; BIND data file for example.com
;
$TTL      604800
@         IN      SOA     example.com. root.example.com. (
                        2             ; Serial
                        604800        ; Refresh
                        86400         ; Retry
                        2419200       ; Expire
                        604800 )      ; Negative Cache TTL

@         IN      NS      ns.example.com.
@         IN      A       192.168.1.10
ns        IN      A       192.168.1.10
www       IN      CNAME   example.com.
```

- ثم نستخدم الامر `dig` للاستعلام عن `www.example.com`

```
dig www.example.com
```

خادم DNS ثانوي

- يستخدم خادم DNS الثانوي لتوفير معلومات عن النطاقات في حال تعطل الخادم الأساسي
- يحتوي خادم DNS الثانوي على نسخة مماثلة من ملفات النطاقات على خادم DNS الأساسي وتحديث معلومات النطاق يتم عبر تحديث قاعدة البيانات على الخادم الأساسي فقط
- الخطوة الأولى هي السماح بنقل معلومات النطاق من خادم DNS الأساسي إلى خادم DNS الثانوي عبر تحرير الملف التالي على الخادم الأساسي:

```
sudo nano /etc/bind/named.conf.local
```

- وإضافة `allow-transfer` و `also-notify` الى الملف كما في المثال التالي:

```
zone "example.com" {  
    type master;  
    file "/etc/bind/db.example.com";  
    allow-transfer { 192.168.1.11; };  
    also-notify { 192.168.1.11; };  
};
```

خادم DNS ثانوي

- الخطوة الثانية هي تثبيت خادم DNS على جهاز جديد وتحويل خادم DNS الى خادم ثانوي للنطاق example.com عبر تحرير الملف التالي:

```
sudo nano /etc/bind/named.conf.local
```

- اضافة zone الى الملف من نوع slave:

```
zone "example.com" {  
    type slave;  
    file "db.example.com";  
    masters { 192.168.1.10; };  
};
```

- ثم تحرير ملف النطاق example.com على خادم DNS الاساسي:

```
sudo nano /etc/bind/db.example.com
```

خادم DNS ثانوي

- إضافة سجل من نوع NS الى ملف النطاق example.com حتى يبدو الملف كما في المثال التالي:

```
$TTL      604800
@         IN      SOA   example.com. admin.example.com. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL

@         IN      NS    ns.example.com.
@         IN      NS    ns2.example.com.
@         IN      A     192.168.1.10
ns        IN      A     192.168.1.10
ns2       IN      A     192.168.1.11
www       IN      CNAME  example.com.
```

خادم DNS ثانوي

- ثم إعادة تشغيل خدمة DNS على الخادمين: الاساسي والثانوي لتفعيل الاعدادات الجديدة:

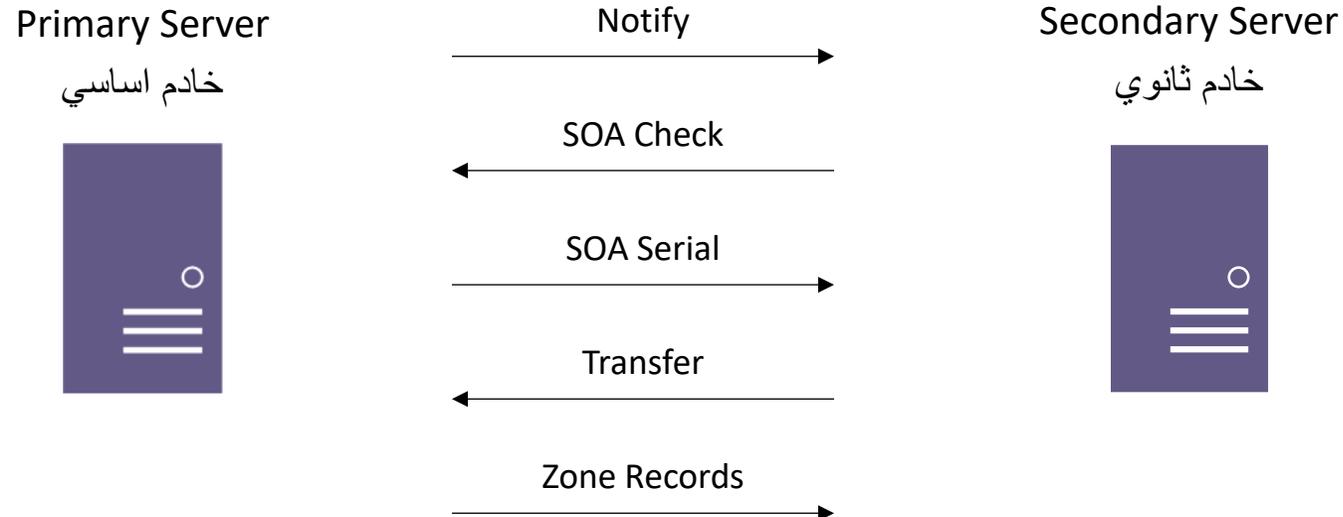
```
sudo systemctl restart bind9.service  
sudo systemctl status bind9.service
```

- للتأكد من نقل معلومات النطاق من الخادم الاساسي الى الثانوي، نستخدم الامر **dig**:

```
dig example.com @192.168.1.11  
dig www.example.com @192.168.1.11
```

خادم DNS ثانوي

- كيف يتم نقل معلومات النطاق من خادم DNS الاساسي الى خادم DNS الثانوي؟
- يقوم الخادم الاساسي بارسال اشعار الى الخادم الثانوي بتوفر تحديث على معلومات النطاق عبر زيادة قيمة Serial في سجل SOA، وبعد ان يتأكد الخادم الثانوي من قيمة Serial يتم ارسال طلب لنقل معلومات النطاق بالكامل (AXFR) او نقل التحديثات الاخيرة فقط (IXFR)



تمرين: خادم DNS

- اضع اسم النطاق home.com على خادم DNS لاستضافة النطاق والنطاقات الفرعية التابعة له
- اضع سجل من نوع A على ملف قاعدة البيانات لتحويل اسم النطاق home.com الى العنوان 172.16.0.11
- اضع سجل من نوع NS على الملف لتحديد خادم DNS الاساسي ns.home.com على العنوان 172.16.0.10
- اضع سجل من نوع CNAME على الملف لاستضافة اسم النطاق www.home.com على نفس العنوان المستخدم في اسم النطاق home.com
- اضع سجل من نوع A على ملف قاعدة البيانات لتحويل اسم النطاق ldap.home.com الى العنوان 172.16.0.12