الوحدة الاولى: خادم RADIUS

ادارة شبكات متقدمة

م. غنام الجعبري

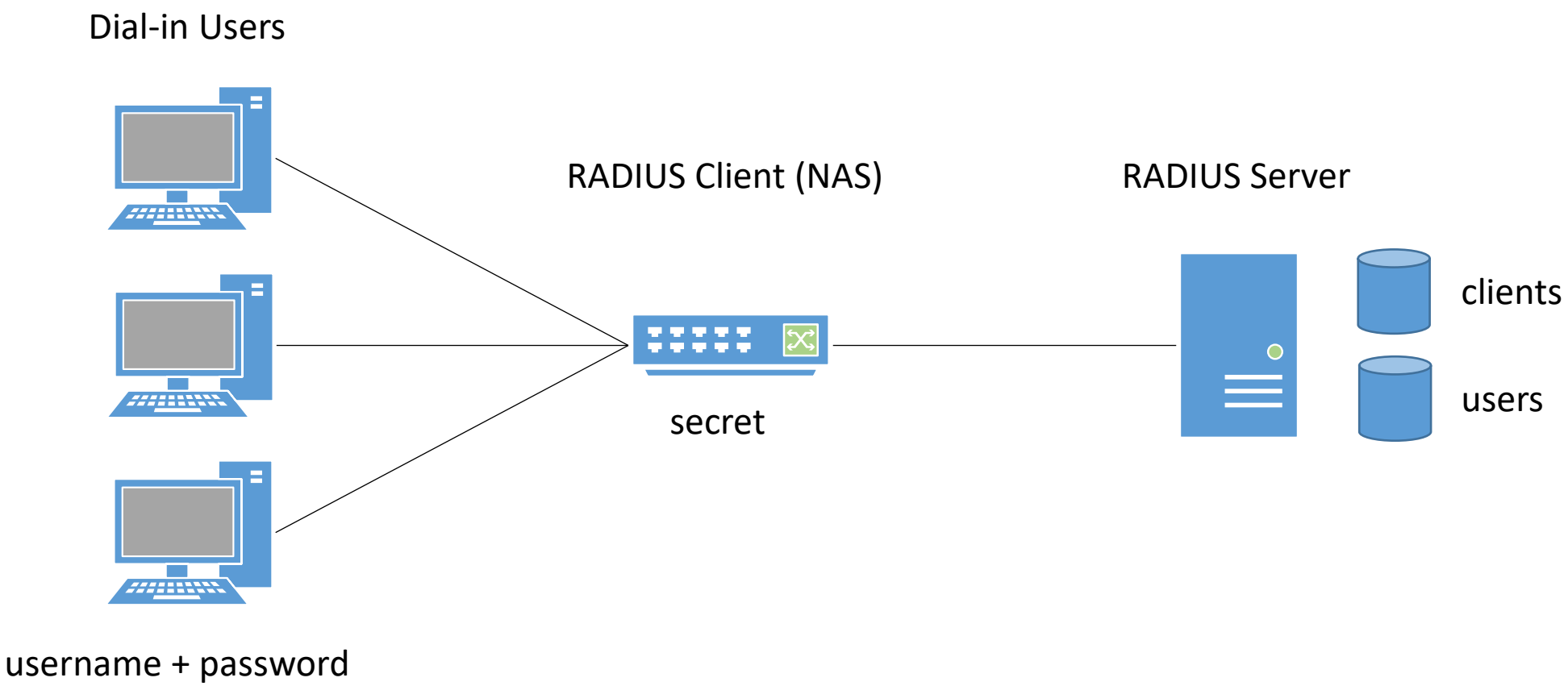
خوادم لينكس

- خادم DHCP
- خادم DNS
- خادم LDAP
- خادم Proxy
- خادم RADIUS
- خادم البريد الالكتروني

خادم RADIUS

- يرجع الاختصار RADIUS الى خدمة التحقق من هوية المتصل عن بعد (Remote Authentication Dial In User Service)
- يستخدم خادم RADIUS في التحقق من الهوية او المصادقة (Authentication) وتحديد صلاحيات الوصول الى الشبكة او التصريح (Authorization) وتسجيل الاحداث المتعلقة بعمليات الوصول الى الشبكة او التدوين (Accounting)، ويشار اليها بالاختصار AAA
- تحتوي بعض اجهزة الشبكة مثل الموزعات (switches) ونقاط الوصول اللاسلكية (access points) على مكونات برمجية تلعب دور العميل للتحكم بالوصول الى الشبكة عبر الاتصال مع خادم RADIUS والتحقق من هوية المتصل قبل إنشاء اتصال مع الشبكة والحصول على عنوان IP

خادم RADIUS


Dial-in Users
RADIUS Client (NAS)
RADIUS Server
clients
users
secret
username + password

خادم RADIUS

- يتم اعداد بطاقة الشبكة في لينكس عبر تحرير الملف التالي:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

- واضافة الاعدادات التالية في الملف:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens3:
      dhcp4: true
    ens4:
      addresses:
        - 192.168.1.10/24
```

- ثم تفعيل الاعدادات الجديدة باستخدام الامر التالي:

```
sudo netplan apply
```

خادم RADIUS

- من اشهر خوادم RADIUS التي تستخدم على نطاق واسع خادم مفتوح المصدر يدعى FreeRADIUS
- يدعم خادم FreeRADIUS العديد من بروتوكولات المصادقة والتشفير في شبكات ايثرنت والشبكات اللاسلكية مثل WPA/WPA2
- لتثبيت خادم RADIUS على نظام لينكس نستخدم الامر التالي:

```
sudo apt update
sudo apt-get install freeradius
```

- ثم نقوم بتسجيل الدخول على نظام لينكس بصلاحيات كاملة لاعداد خادم RADIUS:

```
sudo -i
```

خادم RADIUS

- يمكن اضافة الاجهزة التي تستخدم في التحكم بالوصول الى الشبكة (NAS) عبر تحرير الملف التالي:

```
nano /etc/freeradius/3.0/clients.conf
```

- ثم اضافة عنوان جهاز NAS وكلمة المرور المستخدمة من اجل الاتصال مع الخادم كما في المثال التالي:

```
client access-point-1 {
        ipaddr          = 192.168.1.254
        secret          = 12345
}
```

خادم RADIUS

- يمكن اضافة مستخدمين لتسجيل الدخول الى الشبكة عبر تحرير الملف التالي:

```
nano /etc/freeradius/3.0/users
```

- ثم اضافة اسم المستخدم وكلمة المرور من اجل الاتصال مع الخادم كما في المثال التالي:

```
bob Cleartext-Password := "hello"
```

- ثم اعادة تشغيل خادم RADIUS لتفعيل الاعدادات الجديدة:

```
systemctl restart freeradius.service
```

- او يمكن تشغيل الخادم بنمط التصحيح (debug mode) لمعاينة العمليات على الشاشة:

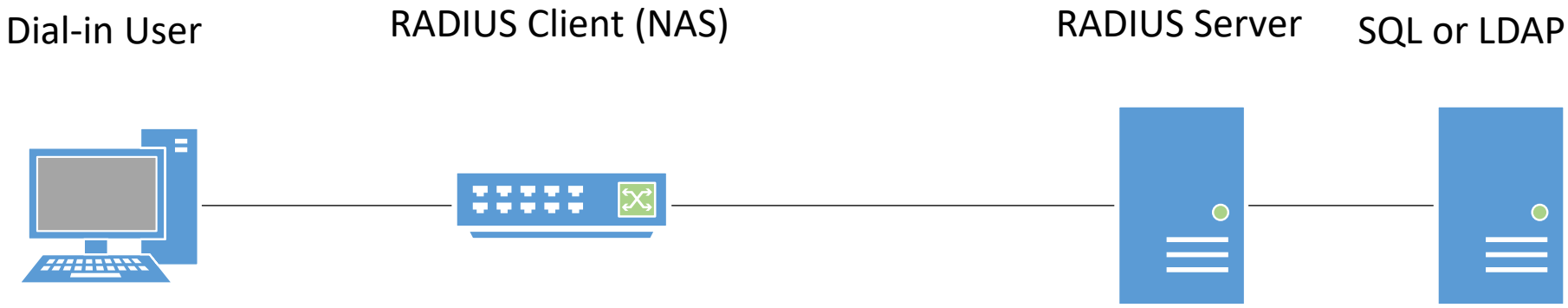
```
systemctl stop freeradius.service
freeradius -X
```

خادم RADIUS

- يمكن اختبار خادم RADIUS دون استخدام جهاز NAS عبر ارسال طلب استعلام عن اسم المستخدم وكلمة المرور الى الخادم بشكل مباشر كما في المثال التالي:

```
radtest bob hello localhost 0 testing123
```

- يمكن اعداد خادم FreeRADIUS لتمرير طلب الاستعلام عن المستخدمين الى خادم قواعد البيانات (SQL) او خادم LDAP قبل اجراء اتصال والحصول على عنوان IP



خادم LDAP

- قبل تثبيت خادم LDAP على نظام لينكس، نقوم بتسمية جهاز الحاسوب تحت اسم النطاق لانشاء الجذر في دليل LDAP كما في المثال التالي:

```
sudo hostname ldap.example.com
```

- لتثبيت خادم LDAP على نظام لينكس نستخدم الامر التالي:

```
sudo apt update
sudo apt install slapd ldap-utils
```

- اثناء تثبيت خادم LDAP سيتم انشاء الجذر dc=example,dc=com والسؤال عن ادخال كلمة المرور للمستخدم cn=admin,dc=example,dc=com الذي يمتلك صلاحيات كاملة لادارة دليل LDAP وتعبئة الدليل بالبيانات

خادم LDAP

- يمكن اعادة تهيئة خادم LDAP مرة اخرى بعد الانتهاء من التثبيت باستخدام الامر:

```
sudo dpkg-reconfigure slapd
```

- وسوف تظهر شاشة لادخال الاعدادات الاولية التالية:
  - اسم النطاق (domain name) لانشاء الجذر في الدليل مثل example.com
  - اسم المنظمة (organization name) مثل example
  - كلمة المرور للمستخدم admin

خادم LDAP

- لتعبئة الدليل ببعض البيانات، نقوم بانشاء ملف بصيغة LDIF باستخدام محرر النصوص:

```
nano base.ldif
```

- واضافة البيانات التالية الى الملف لانشاء وحدة تنظيمية (OU) في دليل LDAP يندرج المستخدمون (People) تحتها ووحدة تنظيمية اخرى للمجموعات (Groups):

```
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups
```

خادم LDAP

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f base.ldif
```

- ثم ادخال كلمة المرور للمستخدم admin لتعبئة البيانات في دليل LDAP
- لانشاء حساب للمستخدم في دليل LDAP، نقوم بانشاء الملف التالي:

```
nano user.ldif
```

- ثم اضافة البيانات التالية الى الملف:

```
dn: uid=user1,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
uid: user1
cn: User 1
sn: 1
userPassword: secret
```

خادم LDAP

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f user.ldif
```

- لانشاء مجموعة مستخدمين في دليل LDAP، نقوم بانشاء الملف التالي:

```
nano group.ldif
```

- ثم اضافة البيانات التالية الى الملف:

```
dn: cn=group1,ou=Groups,dc=example,dc=com
objectClass: groupOfNames
member: uid=user1,ou=People,dc=example,dc=com
```

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f group.ldif
```

خادم LDAP

- للتأكد من الاتصال مع خادم LDAP وتنفيذ الاستعلامات، نستخدم الامر التالي:

```
ldapsearch -x -LLL -H ldap://localhost -b dc=example,dc=com
```

- لتثبيت تطبيق phpLDAPadmin على نظام لينكس، نستخدم الامر التالي:

```
sudo apt install phpldapadmin
```

- يمكن الوصول لتطبيق phpLDAPadmin عن طريق ادخال اسم او عنوان خادم LDAP على المتصفح كما في المثال التالي:

```
http://ldap.example.com/phpldapadmin
```

- كيفية معالجة الخطأ في Ubuntu 22.04 بعد تثبيت تطبيق phpLDAPadmin:

```
sudo apt-get purge phpldapadmin
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/phpldapadmin/phpldapadmin_1.2.6.7-1_all.deb
sudo dpkg -i phpldapadmin_1.2.6.7-1_all.deb
```

خادم RADIUS

- بعد تثبيت واعداد خادم LDAP، نقوم بتثبيت وحدة المصادقة عن طريق LDAP على خادم RADIUS لتمرير طلب الاستعلام عن المستخدمين الى خادم LDAP:

```
sudo apt-get install freeradius-ldap
```

- ثم تحرير الملف التالي:

```
sudo -i
nano /etc/freeradius/3.0/sites-available/default
```

- واضافة المصادقة عن طريق LDAP في الملف:

```
Auth-Type LDAP {
    ldap
}
```

خادم RADIUS

- ثم تحرير الملف التالي:

```
nano /etc/freeradius/3.0/mods-available/ldap
```

- وتعديل اعدادات الاتصال مع خادم LDAP كما في المثال التالي:

```
server = 'localhost'
identity = 'cn=admin,dc=example,dc=com'
password = secret
base_dn = 'dc=example,dc=com'
```

- ثم تفعيل وحدة المصادقة عن طريق LDAP باستخدام الامر:

```
ln -s /etc/freeradius/3.0/mods-available/ldap
/etc/freeradius/3.0/mods-enabled/ldap
```

خادم RADIUS

- يتم السماح للاجهزة التي تعمل بنظام ويندوز من الاتصال مع خادم RADIUS عبر تحرير الملف التالي:

```
nano /etc/freeradius/3.0/mods-available/eap
```

- وتعديل طريقة المصادقة الافتراضية الى PEAP:

```
default_eap_type = peap
```

- ثم اعادة تشغيل خادم RADIUS لتفعيل الاعدادات الجديدة:

```
systemctl restart freeradius.service
```

- يمكن تشغيل خادم RADIUS تلقائيا عند بدء تشغيل الخادم باستخدام الامر:

```
systemctl enable freeradius.service
```

خادم RADIUS

- يمكن اختبار خادم RADIUS بعد دمجه مع خادم LDAP كما في المثال التالي :

```
radtest user1 secret localhost 0 testing123
```

- يمكن اعداد نقطة الوصول اللاسلكية لتأمين الشبكات اللاسلكية عبر بروتوكول RADIUS كما في المثال التالي: