ULAK CSIRT

UlakNet Computer Security Incident Response Team

TÜBİTAK ULAKBİM

FREE RADIUS VE LDAP ILE 802.1x AG KIMLIK DENETIMI

Ulak-CSIRT Kimlik Denetimi Çalisma Grubu

Hüseyin YÜCE, Gökhan AKIN, Hüsnü DEMIR

Basliklar

- Tanimlar
  - IEEE 802.1x
  - Authentication, Authorization ve Accounting (AAA)
  - Extensible Authentication Protocol (EAP)
  - EAP Çesitleri
  - Sifreleme Teknikleri
    - Simetrik Sifreleme
    - Asimetrik Sifreleme
  - Sertifika
  - Hash
  - Imzalama
  - LDAP
  - RADIUS

Basliklar

- FreeRADIUS
  - PEAP – TTLS Kimlik Denetimi
  - Kurulum
- OpenLDAP
  - Kurulum
- OpenLDAP ? FreeRADIUS Entegrasyonu
- AG CIHAZI TANIMLARI

Tanimlar

- **IEEE 802.1x**

  IEEE 802.1x port tabanli ag erisim kontrol standardidir. Kullanici bilgileri (kullanici adi-parola) yardimi ile aga baglanilmasina izin verilmesini saglar (Bazi özel durumlarda MAC adreside kullanilmaktadir.). Kullanici dogrulama sirasinda EAP (Extensible Authentication Protocol) yöntemi kullanilir. Bu sekilde ag erisimi isteyen cihazdan dogrulama yapan mekanizmaya kadar kullanici bilgilerin sürekli sifreli gitmesini saglanir.

Tanimlar

- **EAP**
- Genisletilebilir Kimlik Kanitlama Protokolü (EAP - Extensible Authentication Protocol) [RFC 3748] kimlik kanitlama için bir iletim protokolüdür, bir kimlik kanitlama yöntemi degildir.
- EAP kimlik kanitlama sürecinde, kimlik kanitlama sunucusu ile istemci arasinda geçen ve taraflarin hangi kimlik kanitlama yöntemini kullanacaklarini belirler. EAP kimlik kanitlama yöntemi olarak MD5, TLS, TTLS, PEAP, LEAP kullanir.

Tanimlar

- **EAP Çesitleri**

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Sunucu Sertifikasi	Hayir	Hayir	Evet	Evet	Evet
Istemci Sertifikasi	Hayir	Hayir	Evet	Hayir	Hayir
WPA Anahtar Degisimi	Hayir	Evet	Evet	Evet	Evet
Güvenilirlik	Hayir	Hayir	Evet	Evet	Evet

Tanimlar

- **Hash**
- Hash belirli bir matematik fonksyonu ile verinin tek yönlü (yani veri geri elde edilemiyecek sekilde) bir kontrol numarasi elde etme teknigidir. Hash kaynaginin dogrulanmasi ve veri bütünlügünü test etmek için kullanilir.
- MD5 ve SHA1 günümüzde kullanilan popüler bir hash algoritmalaridir. Kimlik dogrulama için EAP tüneli yöntemlerinde ve sertifika imzala amaci ile Kullanilmaktadirlar.

Tanimlar

- **Simetrik Sifreleme:**

Ayni anahtar kelime ile verinin hem sifrelenmesi hemde geri çözülmesi seklinde çalisan tekniktir.

Veri + Anahtar = Sifreli Veri

Sifreli Veri + Anahtar = Veri

Az sistem kaynagi tüketen bir sifreleme sistemidir ancak anahtarin karsilikli haberlesirken taraflara güvenli ulastirilmasi zordur.

Tanimlar

- **Asimetrik Sifreleme:**

Iki anahtardan olusan bu sistemde anahtar1'in sifreledigini anahtar2, anahtar2'nin sifreledigi ise anahtar1 açabilir.

Veri + Anahtar1 = Sifreli Veri (Public)

Sifreli Veri + Anahtar2 = Veri (Private)

Not:Çift yönlü güvenli haberlesme için 2 çift anahtar gerekir.

Not2: Asimetrik sifreleme çok sistem kaynagi tükettiginden daha çok simetrik anahtarin tasinmasi için kullanlilir.

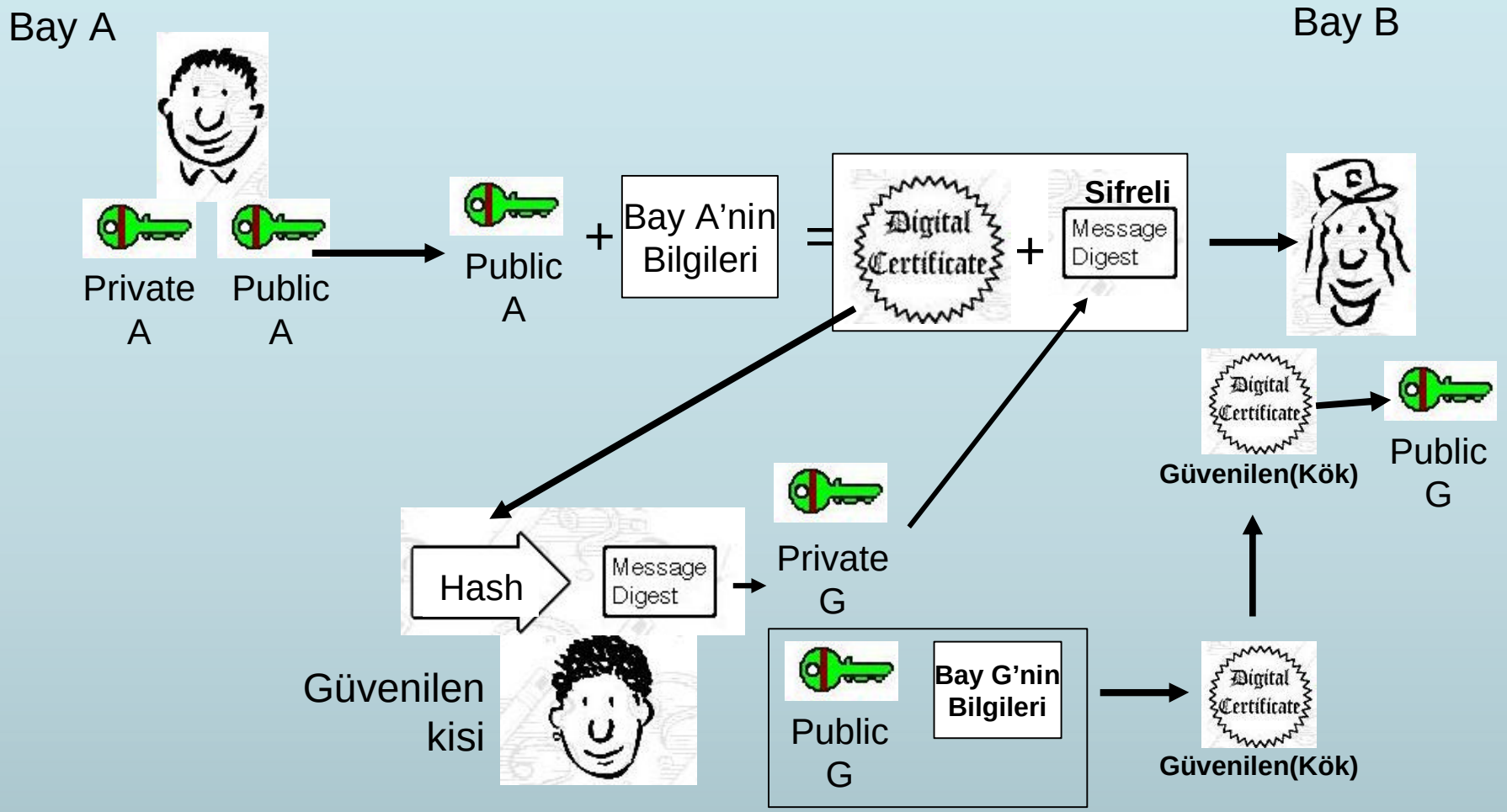
Tanimlar

- **Sertifika**

- Sertifika Public anahtari ve bunun yani sira hizmet alinacak kurumun Adi, web adresi, mail adresi ...vs bilgileri barindiran bir dökümana verilen addir.

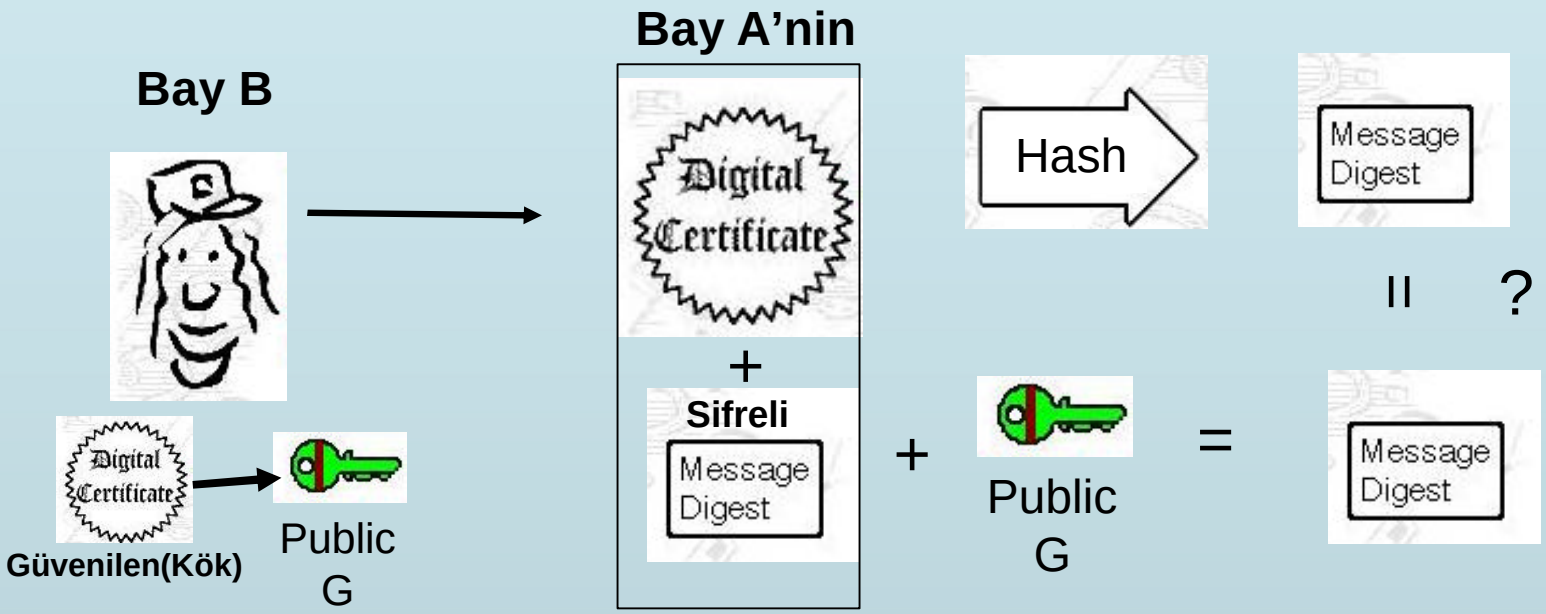
Tanimlar

- **Imza - 1**



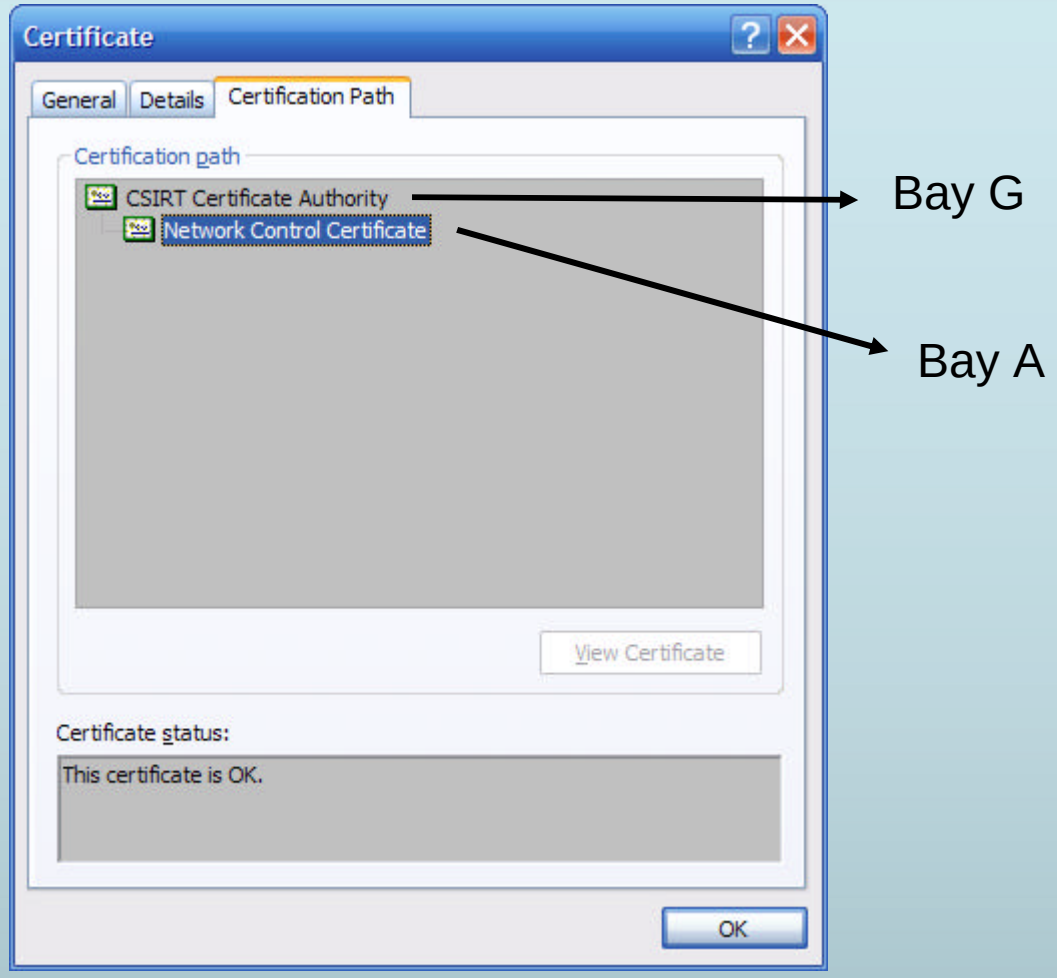
Tanimlar

- **Imza - 2**



Tanimlar

- **Imza - 3**



Tanimlar

- **EAP Çesitleri**

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Sunucu Sertifikasi	Hayir	Hayir	Evet	Evet	Evet
Istemci Sertifikasi	Hayir	Hayir	Evet	Hayir	Hayir
WPA Anahtar Degisimi	Hayir	Evet	Evet	Evet	Evet
Güvenilirlik	Hayir	Hayir	Evet	Evet	Evet

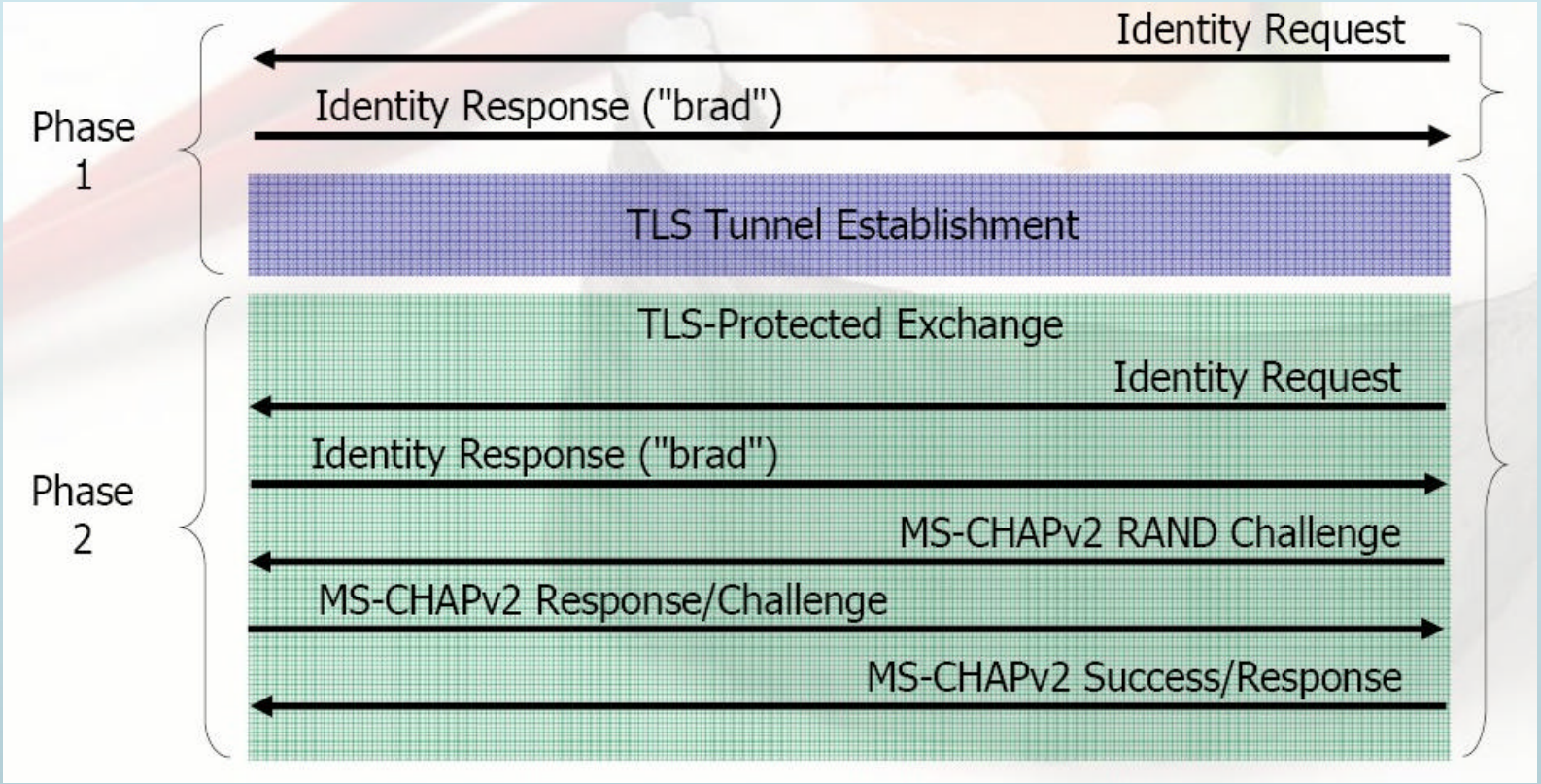
Tanimlar

- **EAP-TLS**
- TLS (Iletim Katmani Güvenligi), Secure Sockets Layer (SSL) in atasi olan bir kriptografi protokolüdür.

- Protokol iki katmandan olusur.
- TLS kayit protokolü : TLS kayit protokolü ile veriler simetrik sifreleme anahtarlari ile sifrelenir.
- TLS el sikisma (handshake) protokolü : Bu anahtar TLS el sikisma protokolü kullanilarak alici ve verici tarafindan paylasilir. TLS el sikisma protokolü ile haberlesecek taraflarin birbirlerini yetkilendirmeleri, sifreleme algoritmasi ve anahtarlarin karsilikli degisimi saglanir.
-
- Bu çift yönlü dogrulama özelligi ile EAP-TLS en güvenilir EAP yöntemlerinden biri olarak bilinir. Ancak her istemciye özgün sertifika üretilerek, güvenli bir sekilde dagitilmasini gerektiren bu yöntemin uygunalmasi zordur.

Tanimlar

- **PEAP**



Tanimlar

- **AAA**
- **Authentication (Yetkilendirme) :** Kullanici ya da kullanicilara sisteme, programa veya aga erisim hakkinin verilmesidir.
- **Authorization (Kimlik Dogrulama) :** Sunucu, anahtar veya yönlendirici kullanimlarinda cihaz ya da kullanicinin kimliginin onaylanmasidir.
- **Accounting (Hesap Yönetimi) :** Herhangi bir kullanicinin ne yaptigi, kullanici hareketleri kullanici veri baglantilari ve kullanici sistem kayitlarinin izlenebilmesi amaciyla yapilan islemdir.

RADIUS Uygulamalari

- FreeRADIUS
- Windows IAS
- Cisco ACS
- Juniper SBR

FreeRADIUS

- Çalisma Grubu Kapsaminda GPL lisansina sahip FreeRADIUS ile çalisilistir.
- FreeRADIUS : PAP,CHAP,MS-CHAP,EAP-MD5, EAP-TLS, PEAP, EAP-TTLS ...VS ile kimlik denetimi yapabilmektedir.
- Ayrica kendi bünyesinde Kullanici veritabani olusturulabildigi gibi harici bir kaynaktanda kullanici denetimi yapabilmektedir.
- Kurulum ile ilgili detaylari FreeRADIUS kurulum sunumunda bulabilirsiniz.

LDAP Nedir

- LDAP (Lightweight Directory Access Protocol : Hafif Dizin Erisim Protokolü)
- Dizin ifadesi LDAP'in yapisi ve içerdigi bilgi itibari ile "veritabani" olarak adlandirilmaktadir.
- LDAP da ki ana amaç aranan verinin mümkün olan en kisa sürede bulunmasidir.
- LDAP’da veriler hiyerarsik nesneler seklindedir.
- Nesneler giris (entry) olarak adlandirilir.

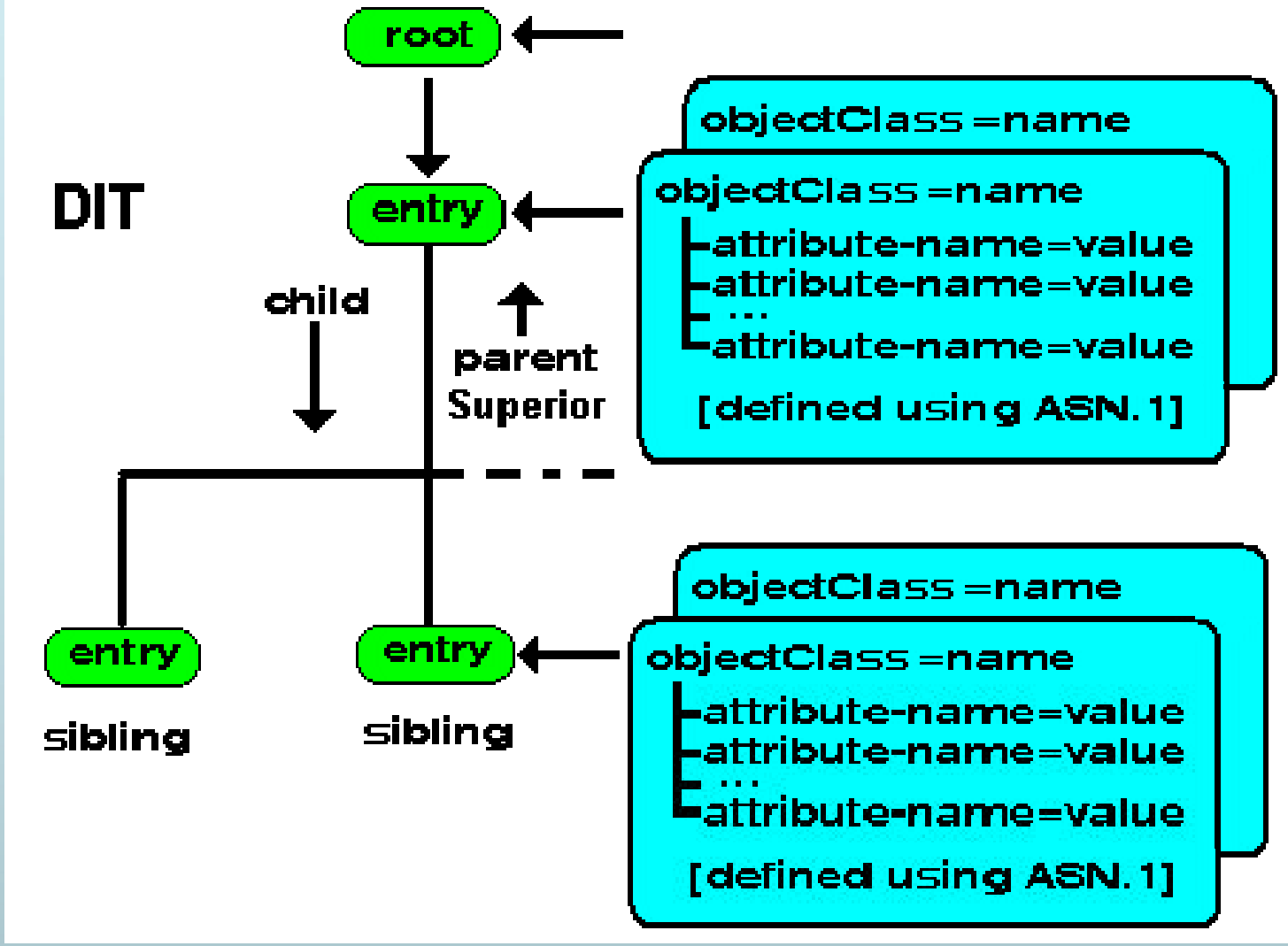
LDAP Nedir

- "objectclass" bir entry içinde bulunabilecek attribute 'lari tanimlar.
- Objectclass'larin tanimlari schema dosyalarinda tanimlanir.
- Agaç yapisi seklinde olan bu yapiya Data Information Tree (DIT) denir.
- Veri bilgi agacinin tepesinde ise kök (root) vardir.
- LDAP dizinine entry'ler LDIF (LDAP Data Interchange Format) girdi dosyasi ile eklenir

LDAP Nedir

- Sart olmamakla birlikte genellikle agaç yapisinin tepe noktasi yani kök 'o' (organization)'dur.
- Daha altinda genellikle 'ou' (organizational unit)'ler bulunur.
- Her organization'un altinda çesitli 'cn' (common name)'ler bulunur. Bir ou'nun altina baska bir ou konabilir.

LDAP Yapisi


root
DIT
entry
child
parent
Superior
objectClass =name
objectClass =name
attribute-name=value
attribute-name=value
...
attribute-name=value
[defined using ASN.1]
entry
entry
sibling
sibling
objectClass =name
objectClass =name
attribute-name=value
attribute-name=value
...
attribute-name=value
[defined using ASN.1]

LDAP Uygulamalari

- Ücretsiz LDAP Uygulamalari
  - OpenLDAP,
  - Fedora Directory Server,
  - OpenDS,
  - ApacheDS
- Ücretli LDAP Uygulamalari
- MS Active Directory
- Novel e-Directory

OpenLDAP

- OpenLDAP uygulamasi öntanimli olarak kuruldugunda yapilandirma dosyalari Linux sistemlerde “/etc/openldap”, BSD sistemlerde “/usr/local/etc/openldap” klasöründe bulunur.
- Düzenlenecek olan ilk yapilandirma dosyasi “slapd.conf” dir.

OpenLDAP (slapd.conf)

- **include /usr/local/etc/openldap/schema/core.schema**
- **Include /usr/local/etc/openldap/schema/cosine.schema**

Bu iki girdi gerekli olan LDAPv3 sistemini ve X.500 tanimlar

- **pidfile /var/run/openldap/slapd.pid**
- **argsfile /var/run/openldap/slapd.args**

- “pidfile” direktifi OpenLDAP (slapd)’in PID’i nereye yazacagini tanimlar.
- ”argsfile” direktifi, OpenLDAP’in komut satirinda hangi parametre ile çalisacagini belirler.
- **/usr/local/libexec/slapd -h ldapi://%2fvar%2frun%2fopenldap%2fldapi/ ldap://0.0.0.0/ -u ldap -g ldap**

OpenLDAP (slapd.conf)

- **`modulepath /usr/local/libexec/openldap`**
- **`moduleload back_bdb`**

- “modulepath” direktifi, OpenLDAP tarfindan yüklenebilir modüllerin (overlays) yerini
- gösterir.
- “moduleload” direktifi ile verilen tanim bu dizinde olmalidir. Burada “back_bdb” kullanilmistir.
- Bu sekilde “Berkeley Database” kullanilabilecektir.

OpenLDAP (slapd.conf)

- **`database bdb`**
- **`suffix "dc=marmara,dc=edu,dc=tr"`**
- **`rootdn "cn=root,dc=marmara,dc=edu,dc=tr"`**
- **`rootpw {SSHA}K73K9RFa7ti+Dz+RpCyG9L6M0YXyb5SE`**

- “database” direktifi Data Information Tree (DIT)’nin veritabani çesidini belirler
- “suffix” direktifi veritabaninda tutulacak Data Information Tree (DIT)’nin hiyerarsisini yada Distinguished Name’in en üst dügüm noktasini belirler.
- “rootdn” en üst dügüm noktasini “rootpw” direktifinde verilen sifre ile erisebilecek süper kullanici tanimini belirler.
- rootpw” direktifi süper kullanicinin veritabanina erisimi için kullanilir.
- komut satirinda “slappasswd -h {SSHA} -s konya” kullanilarak hash li bir sifre olusturulabilir.

OpenLDAP (slapd.conf)

```
directory       /var/db/openldap-data
index           objectClass     eq
index           uid             eq
```

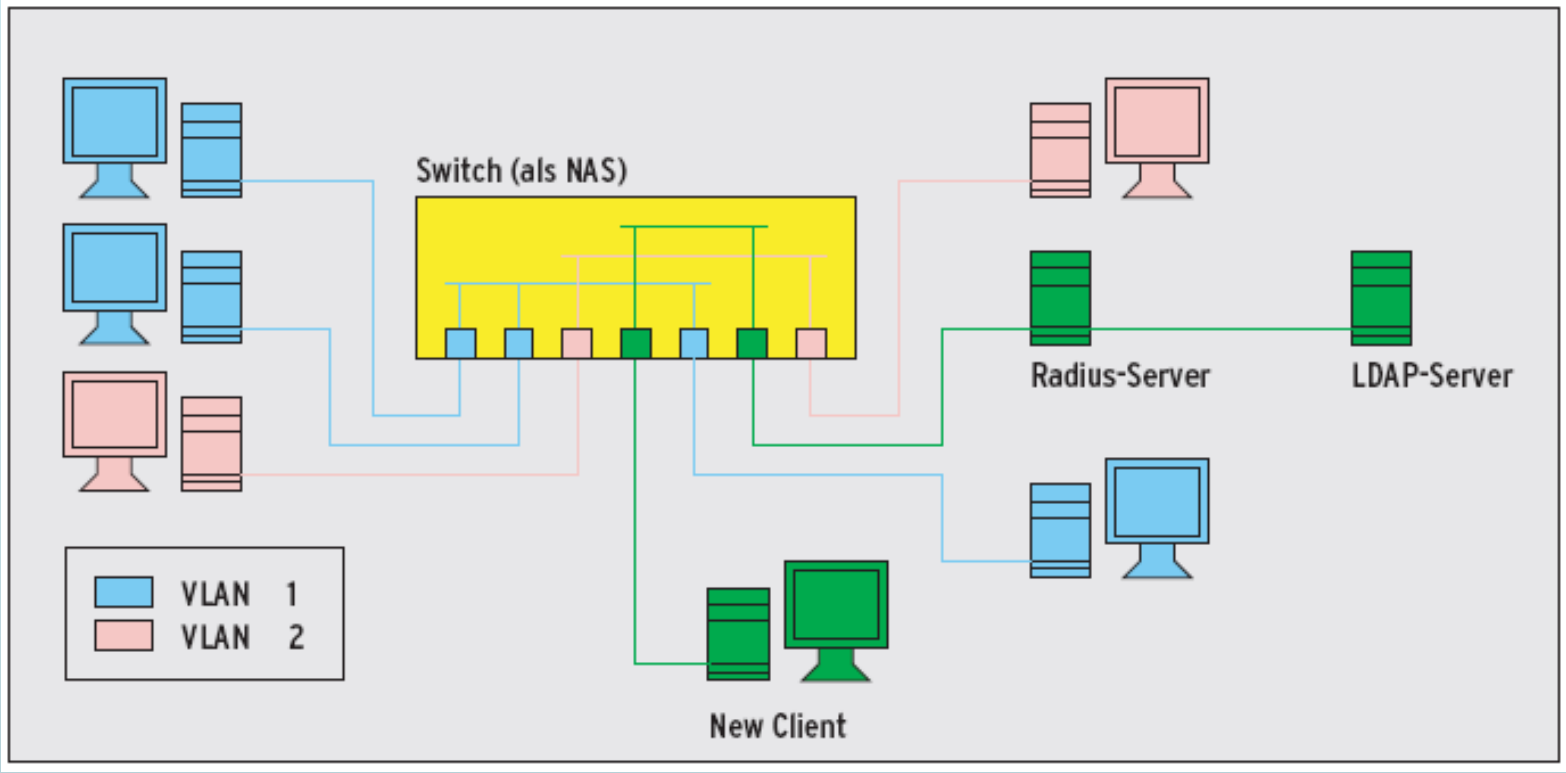
- “directory” direktifi veritabaninin hangi dizinde tutulacagini belirler
- “index” direktifi ile hangi alanlarin indekslemesi yapilacagi belirlenir. Bu sekilde daha hizli sorgulama yapilabilir.

LDAP Data Interchange Files (LDIF)

- **base.ldif**
  - `dn: dc=marmara,dc=edu,dc=tr`
  - `objectclass: dcObject`
  - `objectclass: organization`
  - `o: Marmara Universitesi LDAP Sunucusu`
  - `dc: marmara`

- `#ldapadd -H ldap://127.0.0.1 -x -D "cn=root,dc=marmara,dc=edu,dc=tr" -f base.ldif –W`

OpenLDAP ? FreeRADIUS Entegrasyonu



OpenLDAP ? FreeRADIUS

- FreeRADIUS kimlik dogrulamasinda, kullanici kimlikleri bilgileri ve erisim tanimlari sunucu üzerinde yapilabilecegi gibi kullanim kolayligi saglayacak LDAP sunucusunda da yapilabilir.
- LDAP sunucunda daha önceden tanimlanmis kullanici tanimlarini da kullanmak mümkündür.
- Daha önce kurulan FreeRADIUS'la birlikte gelen RADIUS LDAP sema dosyasini "/usr/local/share/doc/freeradius/ldap_howto.txt" dosyasindan düzenleyerek RADIUS-LDAPv3.schema adinda OpenLDAP schema dizinine kopyalanmasi gerekir.

OpenLDAP ? FreeRADIUS

- “slapd.conf” dosyasina asagidaki girdinin girilmesi gerekir.

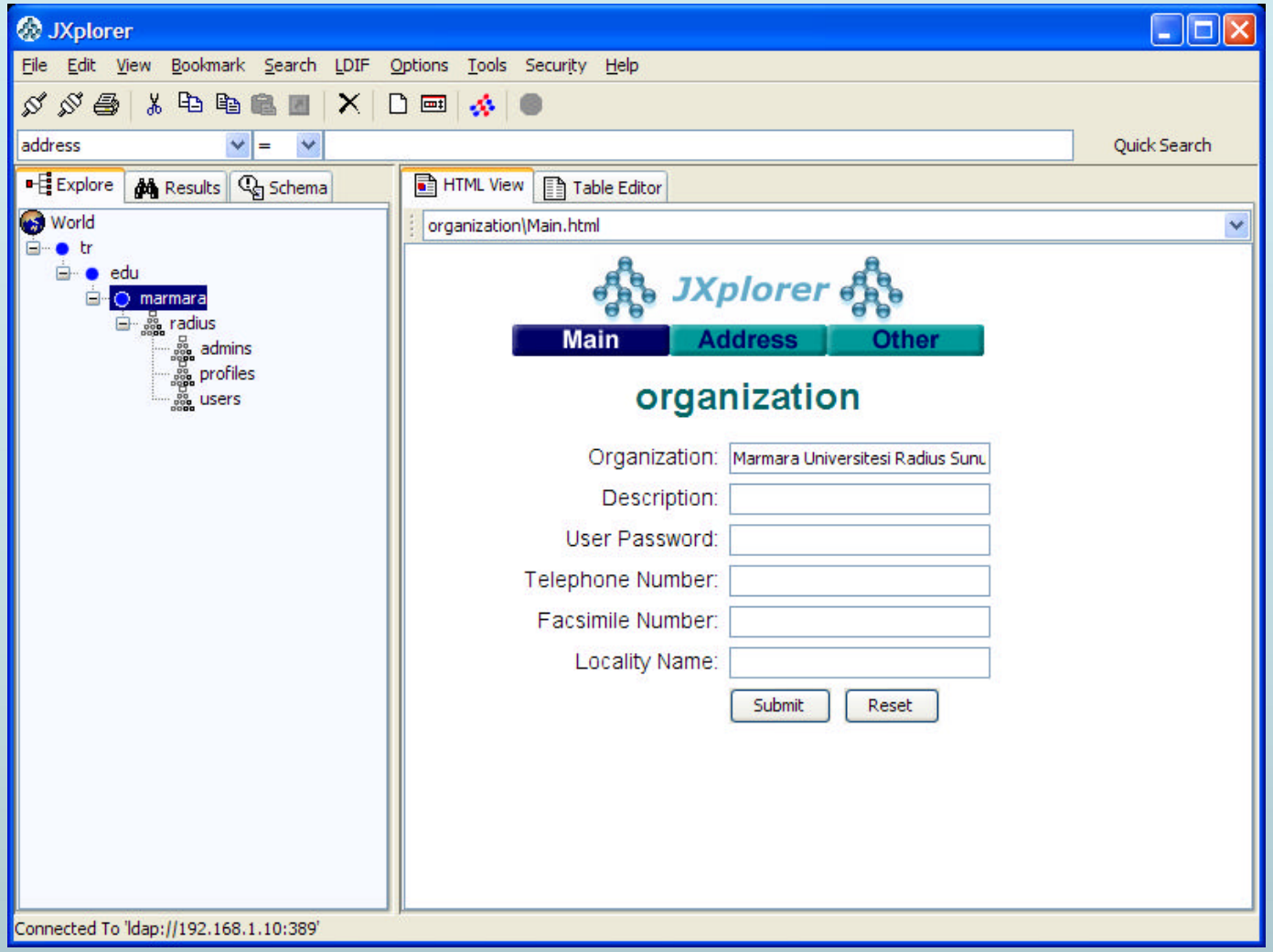
```
include /usr/local/etc/openldap/schema/RADIUS-
  LDAPv3.schema
```

freeradiusbase.ldif

```
dn: ou=radius,dc=marmara,dc=edu,dc=tr
objectclass: organizationalunit
ou: radius
dn: ou=profiles,ou=radius,dc=marmara,dc=edu,dc=tr
objectclass: organizationalunit
```

```
#ldapadd -H ldap://127.0.0.1 -x -D "cn=root,dc=marmara,dc=edu,dc=tr"
-f freeradiusbase.ldif
```

```
objectclass: organizationalunit
ou: users
dn: ou=admins,ou=radius,dc=marmara,dc=edu,dc=tr
objectclass: organizationalunit
ou: admins
```


JXplorer
File Edit View Bookmark Search LDIF Options Tools Security Help
address
=
Quick Search
Explore
Results
Schema
World
tr
edu
marmara
radius
admins
profiles
users
HTML View
Table Editor
organization\Main.html
JXplorer
Main
Address
Other
organization
Organization:
Marmara Universitesi Radius Sunu
Description:
User Password:
Telephone Number:
Facsimile Number:
Locality Name:
Submit
Reset
Connected To 'ldap://192.168.1.10:389'

freeradius.ldif

dn: uid=vlan_02,ou=profiles,ou=radius,dc=marmara,dc=edu,dc=tr
uid: vlan_02
radiusTunnelMediumType: IEEE-802
radiusTunnelType: VLAN
radiusTunnelPrivateGroupId: 2
objectClass: radiusprofile

dn: uid=hyuce,ou=users,ou=radius,dc=marmara,dc=edu,dc=tr
objectclass: radiusprofile
uid: hyuce
userPassword: hyuce
radiusGroupName: vlan_02

freeradius.ldif

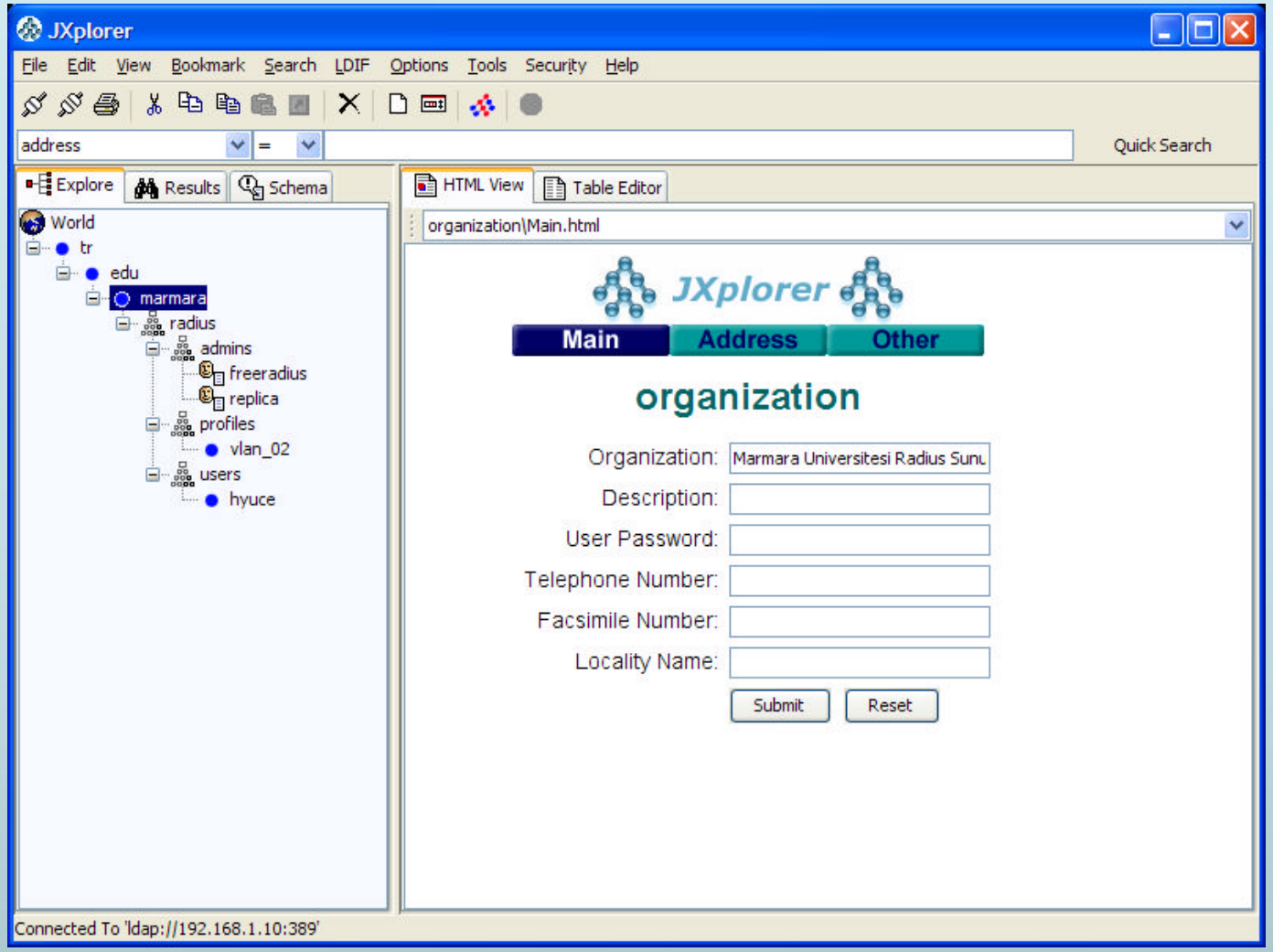
```
dn:cn=freeradius,ou=admins,ou=radius,dc=marm
  ara,dc=edu,dc=tr
objectclass: person
sn: freeradius
cn: freeradius
userPassword: freeradius

dn:cn=replica,ou=admins,ou=radius,dc=marmara
   dc=edu,dc=tr
```

```
#ldapadd -H ldap://127.0.0.1 -x -D "cn=root,dc=marmara,dc=edu,dc=tr"
-f freeradiusbase.ldif
```

```
sn: replica
cn: replica
userPassword: replica
```

ldapsearch

- #ldapsearch -x -b "ou=radius,dc=marmara,dc=edu,dc=tr" "(uid=hyuce)"
- # hyuce, users, radius, marmara.edu.tr
- dn:uid=hyuce,ou=users,ou=radius,dc=marmara,dc=edu,dc=tr
- objectClass: radiusprofile
- uid: hyuce
- radiusGroupName: vlan_02
- userPassword:: aHl1Y2U=


JXplorer
File Edit View Bookmark Search LDIF Options Tools Security Help
address
=
Quick Search
Explore
Results
Schema
World
tr
edu
marmara
radius
admins
freeradius
replica
profiles
vlan_02
users
hyuce
HTML View
Table Editor
organization\Main.html
JXplorer
Main
Address
Other
organization
Organization:
Marmara Universitesi Radius Sunu
Description:
User Password:
Telephone Number:
Facsimile Number:
Locality Name:
Submit
Reset
Connected To 'ldap://192.168.1.10:389'

FreeRADIUS

- Radius sunucu için kullanacagimiz yapilandirma dosyalari “radiusd.conf” , “eap.conf”, “users” , “clients.conf” ve raddb/certs dizindeki “ca.cnf” , “client.cnf” , “server.cnf” dosyalaridir.
- raddb/certs dinindeki sertifika bilgilerin istege göre düzenlenebilir. Bu yapilandirma dosyalarinda ki “input_password” ve “output_password” girdileri daha sonra kullanilacagindan degistirilmesi uygun olacaktir. Bu degisikliklerden sonra sertifika olusturmak için “make” komutunu kullanarak sertifikalarin olusturulmasi saglanir.

radiusd.conf


```
modules {
$INCLUDE eap.conf
        # Lightweight Directory Access Protocol (LDAP)
        #
        ldap {
                server = "127.0.0.1"
        #identity =
"cn=freeradius,ou=admins,ou=radius,dc=marmara,dc=edu,dc=tr"
        #       password = freeradius
                basedn = "ou=radius,dc=marmara,dc=edu,dc=tr"
                filter = "(uid=%{Stripped-User-Name:-%{User-
Name}})"
        #       base_filter = "(objectclass=radiusprofile)"
                tls {
                        start_tls = no
                }
                dictionary_mapping = ${confdir}/ldap.attrmap
                password_attribute = userPassword
        }
authorize {
    eap
    suffix
    ldap
}
authenticate {
        eap
}
```

users

```
DEFAULT Auth-Type := LDAP
        Fall-Through = 1
```

eap.conf

```
eap {
                default_eap_type = ttls
                timer_expire     = 60
                ignore_unknown_eap_types = no
                cisco_accounting_username_bug = no
                ## EAP-TLS
                tls {
                        certdir = ${confdir}/certs
                        cadir = ${confdir}/certs
                        private_key_password = marmara
                        private_key_file = ${certdir}/server.pem
                        certificate_file = ${certdir}/server.pem
                        CA_file = ${cadir}/ca.pem
                        dh_file = ${certdir}/dh
                        random_file = ${certdir}/random
                        make_cert_command = "${certdir}/bootstrap"
                }
               ttls {
                        default_eap_type = md5
                        copy_request_to_tunnel = no
                        use_tunneled_reply = yes
                }
        }
```

clients.conf

```
client localhost {
        ipaddr = 127.0.0.1
        secret = testing123
        shortname = localhost
        require_message_authenticator = no
        nastype     = other
}
```

Test

```
# radtest hyuce "hyuce" localhost 1 testing123
Sending Access-Request of id 241 to 127.0.0.1 port 1812
        User-Name = "hyuce"
        User-Password = "hyuce"
        NAS-IP-Address = 192.168.1.10
        NAS-Port = 1
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812,
  id=241, length=20

#radtest hyuce "hyucex" localhost 1 testing123
Sending Access-Request of id 217 to 127.0.0.1 port 1812
        User-Name = "hyuce"
        User-Password = "hyucex"
        NAS-IP-Address = 192.168.1.10
        NAS-Port = 1
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812,
  id=217, length=20
```

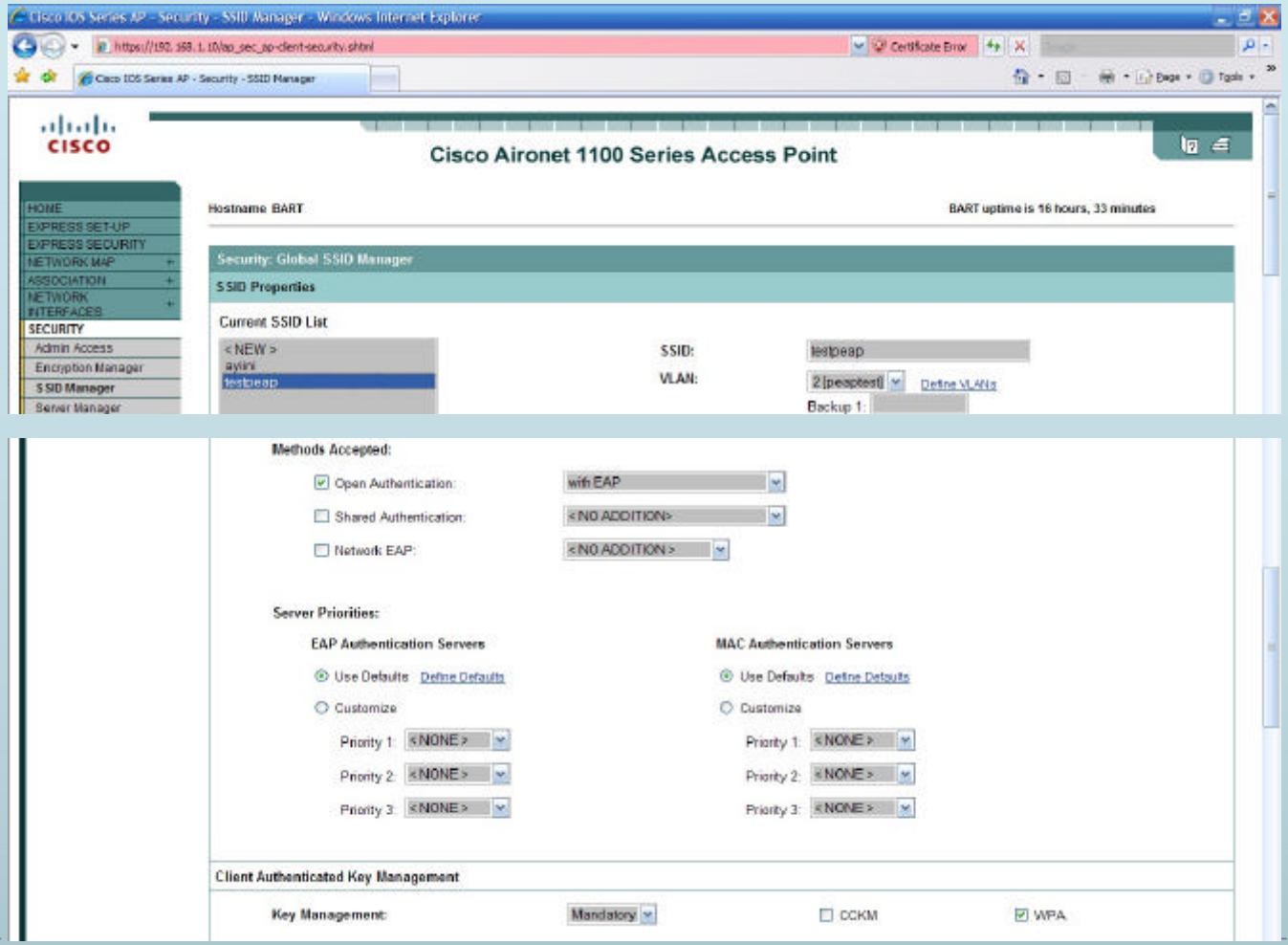
Örnek Ag Cihazi Tanimlari

- **Cisco 2950 Ethernet Anahtari**
- aaa new-model
- aaa authentication login default group line
- aaa authentication dot1x default group radius
- aaa accounting system default start-stop group radius
- dot1x system-auth-control
- radius-server host 192.168.1.103 auth-port 1812 acct-port 1813 key 1234

- interface FastEthernet0/1
- switchport mode access
- dot1x port-control auto

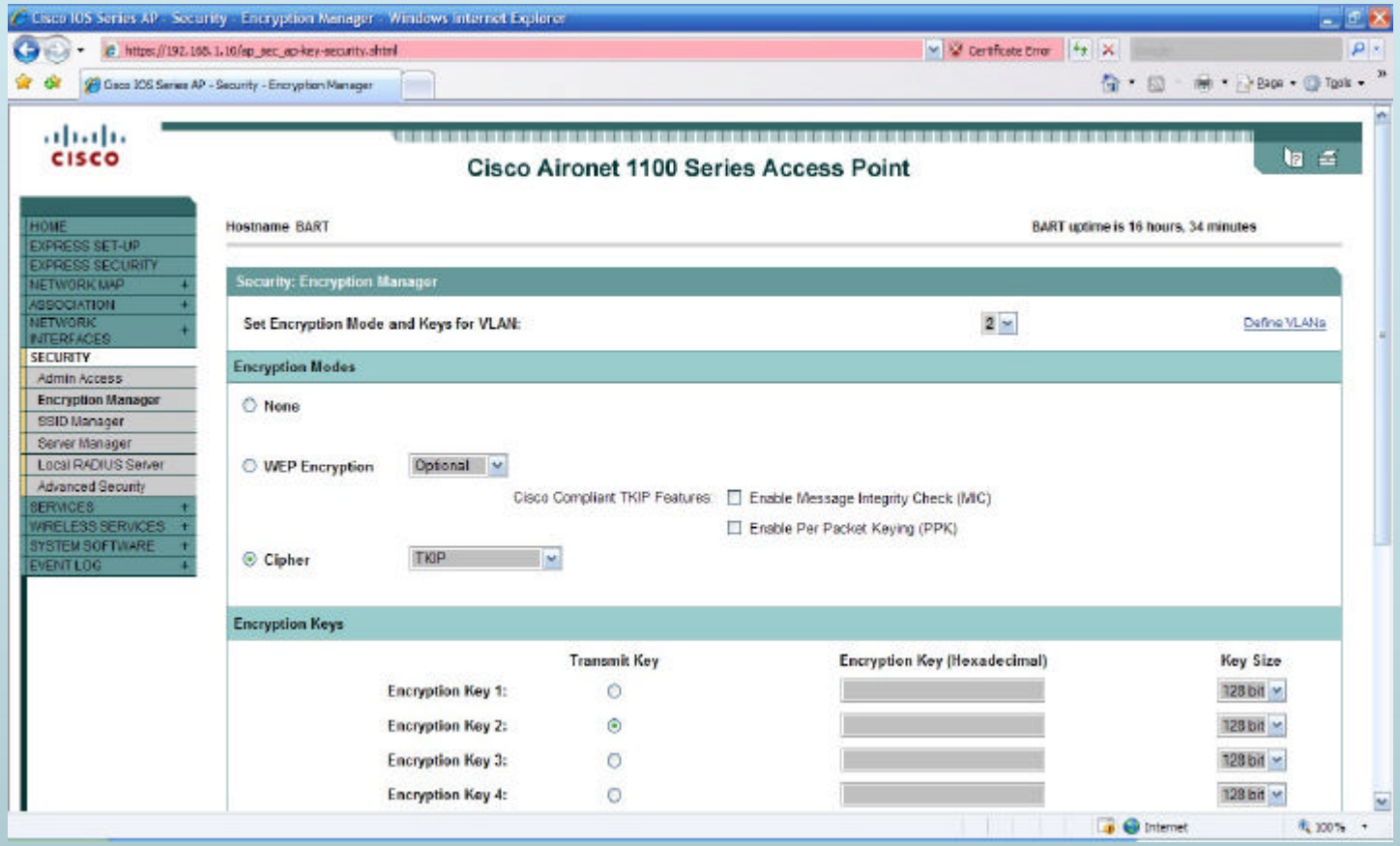
Örnek Ag Cihazi Tanimlari

- **Cisco Aironet Kablosuz Erisim Cihazi - 1**



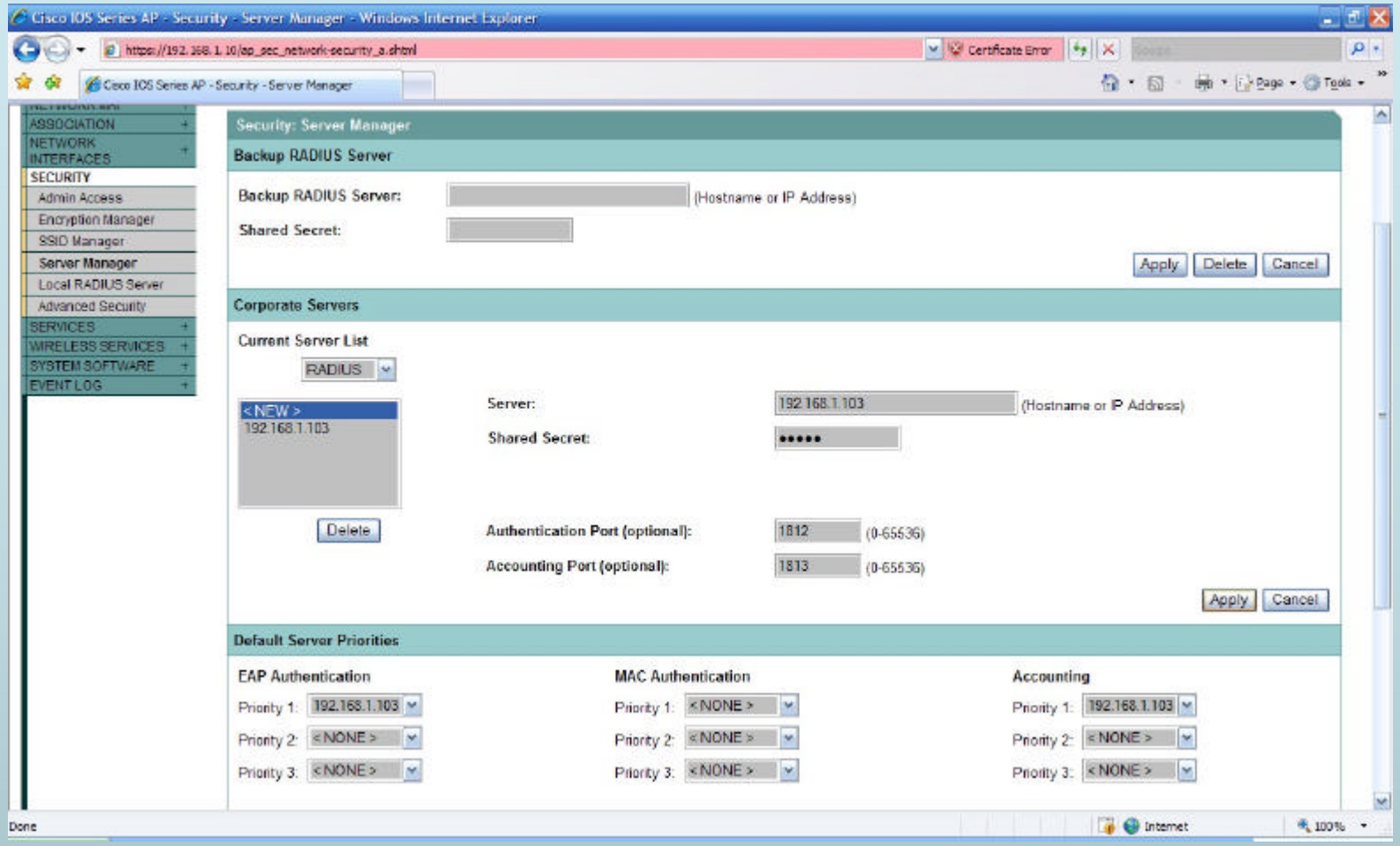
Örnek Ag Cihazi Tanimlari

- **Cisco Aironet Kablosuz Erisim Cihazi - 2**



Örnek Ag Cihazi Tanimlari

- **Cisco Aironet Kablosuz Erisim Cihazi - 3**



TESEKKÜRLER