# 802.1X Port Tabanlı Kimlik Kanıtlama NASIL


Yazan:
**Lars Strand**
<lars (at) unik.no>

Düzenleyen:
**Rick Moen**
0.0 taslağının dil düzenlemesi

Çeviren:
**Olcay Kabal**
<okabal (at) comu.edu.tr>



2004–08–18



**Özet**

Bu belge arka–uç Kimlik Kanıtlama Sunucusu olarak **FreeRADIUS**[B1] ile birlikte **Xsupplicant**[B2] kullanarak IEEE 802.1X Port Tabanlı Ağ Erişim Denetimi[B3]'ni kurmak ve kullanmak için yazılımı ve yordamları tanımlar.


## Konu Başlıkları


***1. Giriş*** . . . 4
- *1.1. 802.1X nedir?* . . . 4
- *1.2. 802.11i nedir?* . . . 5
  - *1.2.1. WEP* . . . 5
  - *1.2.2. 802.11i* . . . 6
  - *1.2.3. Anahtar Yönetimi* . . . 6
    - *1.2.3.1. Dinamik anahtar değişimi ve yönetimi* . . . 6
    - *1.2.3.2. Önpaylaşımlı Anahtar* . . . 8
  - *1.2.4. TSN (WPA) / RSN (WPA2)* . . . 8
- *1.3. EAP nedir?* . . . 8
- *1.4. EAP kimlik kanıtlama yöntemleri* . . . 8
- *1.5. RADIUS nedir?* . . . 9

***2. Sertifikaların Sağlanması*** . . . 9

***3. Kimlik Kanıtlama Sunucusu: FreeRADIUS'un Kurulması*** . . . 10
- *3.1. FreeRADIUS'un Kurulumu* . . . 10
- *3.2. FreeRADIUS'un Yapılandırılması* . . . 10

***4. İstemci: Xsupplicant'ın Kurulması*** . . . 13
- *4.1. Xsupplicant'ın Kurulumu* . . . 13
- *4.2. Xsupplicant'ın Yapılandırılması* . . . 13

***5. Kimlik Kanıtlayıcı: Kimlik Kanıtlayıcının Kurulması (Erişim Noktası)*** . . . 15
- *5.1. Erişim Noktası* . . . 15
- *5.2. Linux Kimlik Kanıtlayıcı* . . . 16

***6. Deneme Ağı*** . . . 16
- *6.1. Deneme Sistemi* . . . 16
- *6.2. Bazı denemeler* . . . 17

***7. Xsupplicant ve Sürücü desteği hakkında*** . . . 19

***8. SSS*** . . . . . 20
***9. Faydalı Kaynaklar*** . . . . . 21
***10. Teşekkür vs.*** . . . . . 22
*10.1. Bu belge nasıl üretildi?* . . . . . 22
*10.2. Geri bildirim* . . . . . 22
*10.3. Teşekkür* . . . . . 22
*GNU Free Documentation License* . . . . . 22

### Bu çevirinin sürüm bilgileri:

| | | |
|---|---|---|
| 1.0 | Aralık 2005 | OK |
| İlk çeviri | | |

### Özgün belgenin sürüm bilgileri:

| | | |
|---|---|---|
| 1.0 | 2004-10-18 | LKS |
| TLDP tarafından gözden geçirilen İlk Sürüm. | | |
| 0.2b | 2004-10-13 | LKS |
| Çeşitli güncellemeler. Dil gözden geçirmesi için Rick Moen'e <rick (at) linuxmafia.com> teşekkür ederim. | | |
| 0.0 | 2004-07-23 | LKS |
| İlk taslak. | | |



### Yasal Açıklamalar

# 1. Giriş

Bu belge kimlik kanıtlama yöntemi olarak PEAP'li (PEAP/MS–CHAPv2) **Xsupplicant**[B6]'ı ve arka–uç Kimlik Kanıtlama Sunucusu olarak **FreeRADIUS**[B7]'u kullanarak IEEE 802.1X Port Tabanlı Ağ Erişim Denetimi[B8]'ni kurmak ve kullanmak için yazılımı ve yordamları tanımlar.

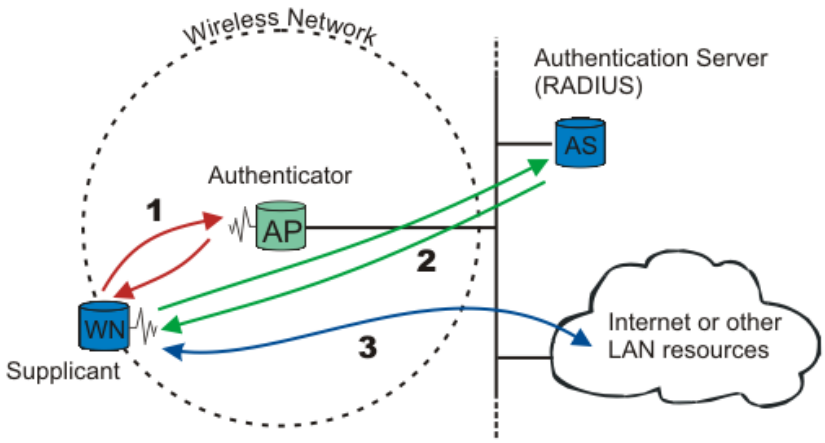
Eğer PEAP'ten başka bir kimlik kanıtlama mekanizması tercih edilirse, örneğin, EAP–TLS veya EAP–TTLS, sadece az sayıda yapılandırma seçeneğinin değiştirilmesine gerek vardır. PEAP/MS–CHAPv2 de Windows XP SP1/Windows 2000 SP3 tarafından desteklenir.

## 1.1. 802.1X nedir?

802.1X–2001 standardı şudur:

> "Port tabanlı ağ erişim denetimi, noktadan–noktaya bağlantı özelliklerine sahip bir yerel ağ portuna takılan cihazların *kimlik doğrulaması* ve *yetkilendirme* için ve bu sayede kimlik doğrulaması ve yetkilendirmesi başarısız olması durumunda o portu *erişimden koruyarak* IEEE 802 yerel ağ altyapılarının fiziksel erişim özelliklerinin kullanımına olanak sağlar. Bu bağlamda bir port, yerel ağ altyapısına ekli tekil bir noktadır."
>
> – – 802.1X–2001, sayfa 1.

**Şekil 1. 802.1X**




Bir kablosuz düğümün diğer yerel ağ kaynaklarına erişebilmesi için kimlik kanıtlaması yapılmalıdır.

1. Yeni bir telsiz düğüm (TD) bir yerel ağ kaynağına erişim isterse, erişim noktası (EN) TD'nin kimliğini sorar. *TD'nin kimliği doğrulanmadan EAP'den başka hiçbir akışa izin verilmez ("port" kapalıdır).*

   Kimlik kanıtlaması isteyen telsiz düğüme genellikle *İstemci* denir, aslında telsiz düğümün bir İstemci *içerdiğini* söylemek daha doğru olur. İstemci güven ortamını oluşturacak Kimlik Kanıtlayıcı veriye cevap vermekle sorumludur. Aynısı erişim noktası için de geçerlidir; *Kimlik Kanıtlayıcı* erişim noktası değildir. Şöyle ki, erişim noktası bir Kimlik Kanıtlayıcı içerir ama Kimlik Kanıtlayıcı erişim noktasında olmasa da olur; harici bir unsur da olabilir.

   Kimlik kanıtlama için kullanılan EAP ilk olarak çevirmeli PPP için kullanıldı. Kimlik olarak kullanıcı adı ile birlikte PAP veya CHAP [RFC1994[B9]] tarafından doğrulaması yapılacak kullanıcı parolası kullanılır. Kimlik açık (şifrelenmemiş) gönderildiği için kötü niyetli bir dinleyici kullanıcının kimliğini öğrenebilir. O zaman "Kimlik saklama" (Identity hiding) kullanılır; şifrelenmiş TLS tüneli kurulmadan gerçek kimlik gönderilmez.

2. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. İstemci ve Kimlik Kanıtlayıcı arasında kullanılan protokol EAP'tır; veya daha doğru olarak EAP kaplamalı yerel ağ'dır (EAPOL). Kimlik Kanıtlayıcı EAP iletilerini RADIUS biçimine yeniden dönüştürür ve onları Kimlik Kanıtlayıcı Sunucuya aktarır.

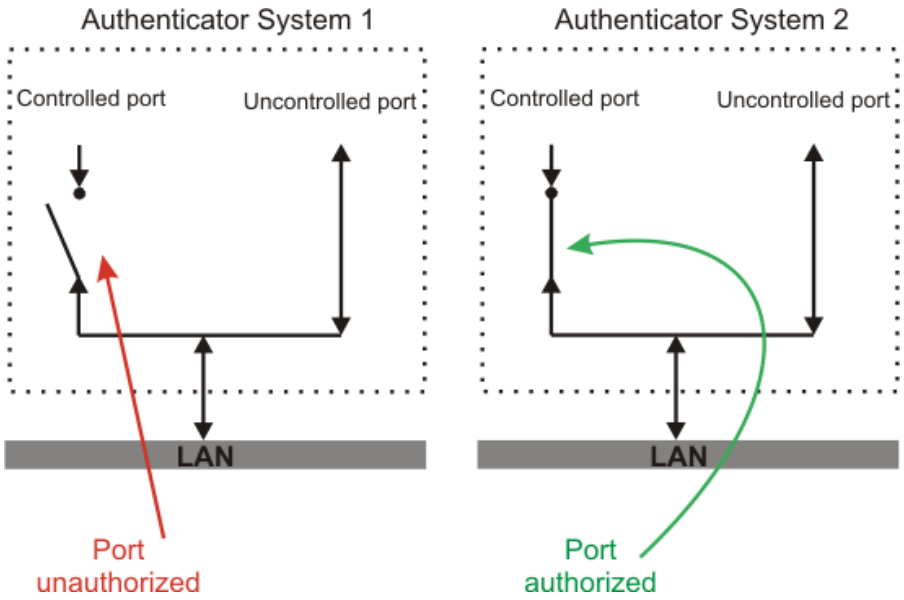
   Kimlik kanıtlama süresince, Kimlik Kanıtlayıcı sadece İstemci ve Kimlik Kanıtlama Sunucusu arasında paketleri nakleder. Kimlik kanıtlama süreci bittiğinde Kimlik Kanıtlama Sunucusu başarı (veya doğrulama başarısız olursa, başarısızlık) iletisi gönderir ve *Kimlik Kanıtlayıcı "port"'u İstemci için açar.*

3. Başarılı bir kimlik kanıtlamadan sonra İstemci diğer yerel ağ kaynaklarına/Internete erişmeye hak kazanır.

Açıklama için *802.1X* (sayfa: 4)'e bakınız.

Neden "port" tabanlı kimlik kanıtlama deniyor? Çünkü, Kimlik Kanıtlayıcı *denetimli* ve *denetimsiz* portlarla uğraşır. Denetimli port da denetimsiz port da mantıksal varlıklardır (sanal portlar); ama yerel ağa aynı fiziksel bağlantıyı kullanırlar (aynı bağlama noktası).

**Şekil 2. 802.1X denetimli/denetimsiz port**




Denetimli portun yetkilendirme durumu.

Kimlik kanıtlama öncesinde sadece denetimsiz port "açıktır". Sadece EAPOL trafiğine izin verilir; *802.1X denetimli/denetimsiz port* (sayfa: 5)'de Authenticator System 1'e bakınız. İstemci kimliği kanıtlandıktan sonra, denetimli port açılır ve diğer yerel ağ kaynaklarına erişim hakkı verilir; *802.1X denetimli/denetimsiz port* (sayfa: 5)'de Authenticator System 2'ye bakınız.

802.1X, yeni IEEE telsiz standardı 802.11i'de önemli bir rol oynar.

## 1.2. 802.11i nedir?

### 1.2.1. WEP

Asıl 802.11 standartının parçası olan Wired Equivalent Privacy (WEP) güvenilirlik sağlamalıydı. Maalesef WEP güçsüz tasarlanmıştır ve kolayca kırılır. Kimlik kanıtlama mekanizması yoktur, erişim denetimi için sadece zayıf bir form mevcuttur (iletişim kurmak için paylaşımlı anahtara sahip olunmalıdır). Daha fazlasını buradan[B13] okuyun.

WEP'in bozuk güvenliğine cevap olarak, IEEE 802.11i olarak isimlendirilen yeni bir telsiz güvenlik standartı ile gelmiştir. 802.1X bu yeni standartta önemli bir rol oynar.

### 1.2.2. 802.11i

Haziran 2004'te onaylanan yeni güvenlik standartı, 802.11i tüm WEP zayıflıklarını onarır. Üç ana kategoriye ayrılır:

1. *Geçici Anahtar Tümleşikliği Protokolü* (Temporary Key Integrity Protocol TKIP) tüm WEP zayıflıklarını onaran kısa–vadeli bir çözümdür. TKIP eski 802.11 ekipmanlarıyla kullanılabilir (sürücü/aygıt yazılımı güncellemesinden sonra) ve tümleşiklik ile güvenilirlik sağlar.
2. *CBC–MAC ile Sayaç Modu Protokolü* (Counter Mode with CBC–MAC Protocol CCMP) [RFC2610[B14]] tepeden tırnağa yeni bir protokoldür. Şifreleme algoritması olarak AES [FIPS 197[B15]] kullanır ve bu RC4'ten (WEP ve TKIP'ta kullanıldı) daha yoğun işlemci kullandığından yeni 802.11 donanımına ihtiyaç duyulabilir. Bazı sürücüler yazılımda CCMP'yi uygulayabilirler. CCMP tümleşiklik ve güvenilirlik sağlar.
3. *802.1X Port Tabanlı Ağ Erişim Denetimi:* TKIP veya CCMP kullanılırken kimlik kanıtlama için 802.1X kullanılır.

Ek olarak, seçimlik bir şifreleme yöntemi olan "Wireless Robust Authentication Protocol" (WRAP) CCMP'nin yerine kullanılabilir. WRAP, 802.11i için AES–tabanlı asıl teklifti, ama sahiplik yükümlülükleriyle sorun yaşanınca CCMP ile değiştirildi. WRAP için destek seçime bağlıdır, ama 802.11i'de CCMP desteği zorunludur.

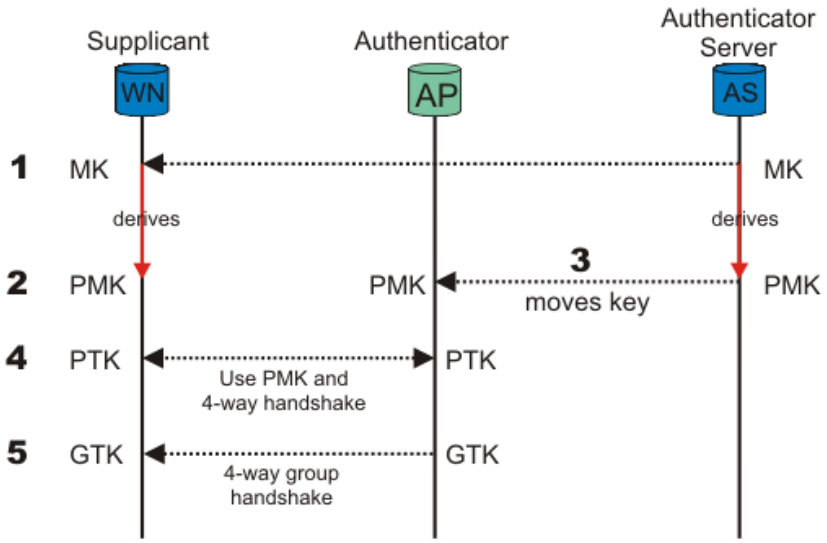
802.11i bir sonraki kısımda tanımlanan genişletilmiş bir anahtar türetme/yönetim işlevine sahiptir.

### 1.2.3. Anahtar Yönetimi

#### 1.2.3.1. Dinamik anahtar değişimi ve yönetimi

Şifreleme ve tümleşiklik algoritmaları kullanarak bir güvenlik kuralları bütünü oluşturmak için anahtarlar kullanılmalıdır. Neyse ki 802.11i bir anahtar türetme/yönetim tarzını içerir. Aşağıdaki şekle bakınız.

**Şekil 3. 802.1X Anahtar Yönetimi**



802.11i'de anahtar yönetimi ve dağıtımı.

1. İstemci (WN) ve Kimlik Kanıtlama Sunucusu (AS) doğrulama yaparken AS'den gönderilen doğrulamanın başarılı olduğunu söyleyen son iletilerden biri bir *Ana Anahtar*'dır (MK – Master Key). Gönderildikren sonra MK sadece WN ve AS tarafından bilinir. MK, WN ve AS arasındaki bu oturuma bağlıdır.

2. Hem WN hem AS, MK'dan bir *Ana Oturum Anahtarı* (PMK – Pairwise Master Key) üretir.

3. O zaman PMK AS'den Kimlik Kanıtlayıcıya (AP) taşınır. PMK'yi sadece WN ve AS türetebilir, bunun yanında AP, AS'nin yerine erişim–denetim kararları verebilir. PMK, WN ve AP arasındaki bu oturuma bağlı yepyeni bir simetrik anahtardır.

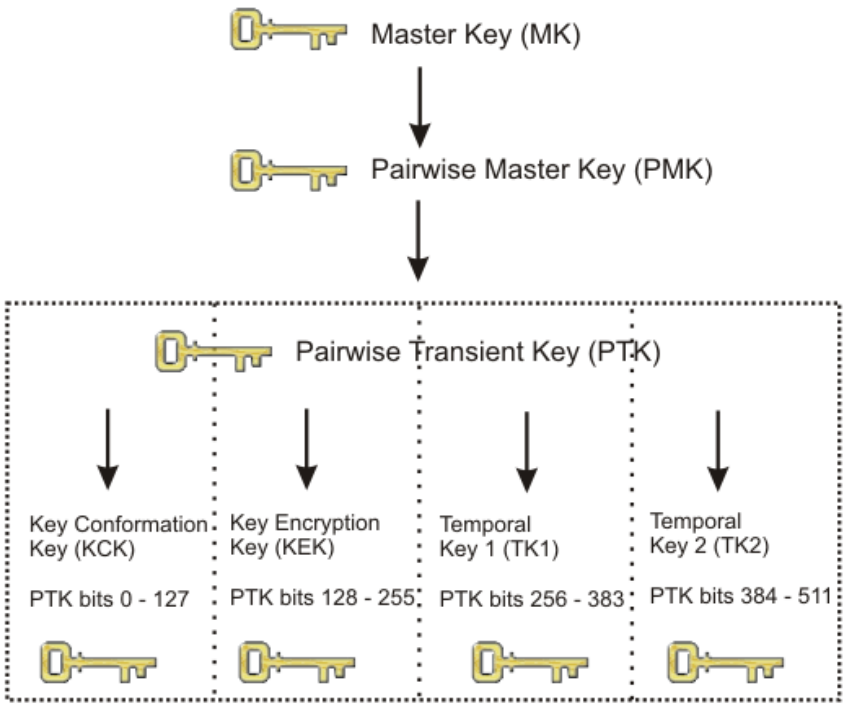
4. *Ana Oturum Anahtarını* türetmek, bağlamak ve doğrulamak için WN ve AP arasında PMK ve 4 yönlü el sıkışma kullanılır. PTK işletimsel anahtarlar topluluğudur:

   - *Anahtar Doğrulama Anahtarı* (KCK – Key Confirmation Key ), isminden de anlaşılacağı üzere PMK'ye sahipliği kanıtlamak ve PMK'yi AP'ye bağlamak için kullanılır.
   - *Anahtar Şifreleme Anahtarı* (KEK – Key Encryption Key), *Grup Geçiş Anahtarı* (GTK – Group Transient Key) dağıtımı için kullanılır. Aşağıda tanımlanmıştır.
   - *Geçici Anahtar 1 ve 2* (TK1/TK2 – Temporal Key 1 & 2) şifreleme için kullanılır. TK1 ve TK2'nin kullanımı şifreleme türüne özeldir.

   Ana Oturum Anahtarına göz atmak için *Ana Oturum Anahtarı (PMK) Düzeni* (sayfa: 7)'e bakınız.

5. KEK ve 4 yönlü grup elşıkışması AS'den WN'ye *Grup Geçiş Anahtarı*nı (GTK) göndermek için kullanılır. GTK aynı Kimlik Kanıtlayıcıya bağlı tüm İstemciler (WN'ler) arasında paylaşılan bir anahtardır ve çoğa gönderimli iletişim akışını güvenli kılmak için kullanılır.

**Şekil 4. Ana Oturum Anahtarı (PMK) Düzeni**



Ana Oturum Anahtarı Düzeni

#### 1.2.3.2. Önpaylaşımlı Anahtar

Küçük çalışma odaları / evdeki çalışma odaları, amaca–yönelik ağlar veya ev kullanımı için Önpaylaşımlı Anahtar (PSK – Pre–Shared Key) kullanılabilir. PSK kullanırken tüm 802.1X kimlik kanıtlama sürecinde birşeyler eksik olur. EAP (ve RADIUS) kullanan WPA'ya "Kurumsal WPA" veya sadece "WPA" dendiği gibi buna da "Kişisel WPA" (WPA–PSK) denmiştir.

[RFC2898[B17]]'den PBKDFv2 kullanılarak verilen bir paroladan 256 bitlik PSK üretilir ve yukarıdaki anahtar yönetim usulünde tanımlandığı gibi Ana Anahtar (MK) olarak kullanılır. Tüm ağ için tek bir PSK (emniyetsiz) veya her İstemciye bir PSK olabilir (daha emniyetli).

### 1.2.4. TSN (WPA) / RSN (WPA2)

Endüstrinin 802.11i standartının tamamlanmasını bekleyecek kadar vakti yoktu. WEP sorunlarının hemen onarılmasını istediler. Wi–Fi Alliance[B18] baskıyı hissetti, standardın (3. taslağa dayanan) "bir anlık görüntüsünü" aldı ve ona *Wi–Fi Korumalı Erişim* (WPA – Wi–Fi Protected Access) dedi. Tek gereksinim mevcut 802.11 ekipmanının WPA ile kullanılabilmesiydi, dolayısıyla WPA temelde TKIP + 802.1X'tir.

WPA uzun vadeli çözüm değildir. *Çok Güvenli Ağ* (RSN – Robust Secure Network) elde etmek için donanım CCMP'yi desteklemeli ve kullanmalıdır. RSN temel olarak CCMP + 802.1X'tir.

CCMP'nin yerine TKIP kullanan RSN'ye *Geçiş Güvenlik Ağı*'da(TSN – Transition Security Network) denir. RSN'ye WPA2 de denir, bu sayede piyasanın aklı karışmaz.

Aklınız mı karıştı?

Temel olarak:

- TSN= TKIP + 802.1X= WPA(1)
- RSN= CCMP + 802.1X= WPA2

Önceki bölümde tanımlandığı gibi bunlar kendi anahtar yönetimleri ile gelir.

## 1.3. EAP nedir?

*Genişletilebilir Kimlik Kanıtlama Protokolü* (EAP – Extensible Authentication Protocol) [RFC 3748[B19]] kimlik kanıtlama için sadece iyileştirilmiş bir iletim protokolüdür, kendisi bir kimlik kanıtlama yöntemi değildir:

> "EAP çoklu kimlik kanıtlama yöntemlerini destekleyen bir kimlik kanıtlama çalışma çerçevesidir. EAP tipik olarak Point–to–Point Protokol(PPP) veya IEEE 802 gibi doğrudan veri iletim katmanları üzerinde IP'ye ihtiyaç duymadan çalışır. EAP çift eleme ve tekrar iletim için kendi desteğini sağlar, ama daha düşük seviyeli garantilere güvenmek durumundadır. EAP'nin kendisinde serpiştirme desteklenmez; bununla birlikte, başka bazı EAP yöntemleri bunu destekleyebilir."
>
> – – RFC 3748, sayfa 3

## 1.4. EAP kimlik kanıtlama yöntemleri

802.1X EAP kullanıyor olduğundan çok farklı kimlik kanıtlama planları eklenebilir; akıllı kartlar, Kerberos, açık anahtar, bir kerelik parolalar ve diğerleri dahil.

En çok kullanılan EAP kimlik kanıtlama mekanizmalarından bazıları aşağıda listelenmiştir. Kayıtlı EAP kimlik kanıtlama türlerinin tam bir listesi IANA'da http://www.iana.org/assignments/eap-«numbers adresinde mevcuttur:

**Uyarı**

Tüm kimlik kanıtlama mekanizmalarının güvenli olduğu düşünülmez!

- **EAP–MD5:** MD5'li Kimlik Kanıtaması kullanıcı adı/parolaya gereksinim duyar ve PPP CHAP protokolünün [RFC1994[B21]] eşdeğeridir. Bu yöntem sözlük saldırısı direnci, karşılıklı kimlik kanıtlama veya anahtar türetimi içermez ve telsiz kimlik kanıtlama ortamında az kullanılır.
- **Hafif EAP (LEAP):** Kimlik kanıtlama için Kimlik Kanıtlama Sunucusuna (RADIUS) bir kullanıcı adı/parola çifti gönderilir. Leap, Cisco tarafından geliştirilmiş müseccel bir protokoldür ve güvenli olduğu düşünülmez. Cisco LEAP'i PEAP niyetine sunmuştur. Yayınlanmış bir standarta en yakın şey burada[B22] bulunabilir.
- **EAP–TLS:** EAP ile İstemci ve Kimlik Kanıtlama Sunucusu arasında bir TLS oturumu oluşturur. Hem sunucu hem istemci(ler) geçerli bir sertifikaya (x509) ve bununla birlikte bir PKI'ya ihtiyaç duyar. bu yöntem her iki yönde kimlik kanıtlama sağlar. EAP–TLS RFC2716[B23]]'da tanımlanmıştır.
- **EAP–TTLS:** Kimlik kanıtlama verisinin emniyetli iletimi için şifreli bir TLS tüneli kurar. TLS tünelinden diğer (herhangi) kimlik kanıtlama yöntemleri faydalanır. Funk Software ve Meetinghouse tarafından geliştirlmiştir ve şu an bir IETF taslağı halindedir.
- **Korumalı EAP (PEAP):** EAP–TTLS gibi şifreli bir TLS tüneli kullanır. Hem EAP–TTLS hem EAP–PEAP için istemci (WN) sertifikaları seçimliktir, ama sunucu (AS) sertifikaları gereklidir. Microsoft, Cisco ve RSA Security tarafından geliştirimiştir ve şu an bir IETF taslağıdır.
- **EAP–MSCHAPv2:** Kullanıcı adı/parolaya ihtiyaç duyar ve temel olarak MS–CHAP–v2'nin [RFC2759[B24]] EAP kaplamalı olanıdır. Genellikle PEAP şifreli tünelde kullanılır. Microsoft tarafından geliştirilmiştir ve şu an bir IETF taslağıdır.

## 1.5. RADIUS nedir?

Uzaktan Aramalı Kullanıcı Kimlik Kanıtlama Servisi (RADIUS – Remote Authentication Dial–In User Service) (ve arkadaşları) [RFC2865[B25]]'te tanımlanmıştır ve ilk olarak, kullanıcılar, ISS'nin ağını kullanmak için yetkilendirilmeden önce kullanıcı adı ve parola doğrulaması yapacak olan ISS'ler tarafından kullanılmıştır.

802.1X ne çeşit bir arka–uç kimlik kanıtlama sunucusu olması gerektiğini belirtmez, ama RADIUS, 802.1X'te kullanılan fiili arka–uç kimlik kanıtlama sunucusudur.

Mevcut birçok AAA (Authentication, Authorization, Accounting) protokolü yoktur, ama hem RADIUS hem DIAMETER [RFC3588[B26]] (genişletmeler dahil) tam AAA desteği sağlarlar. AAA, Authentication (Kimlik Kanıtlama), Authorization (Yetkilendirme) ve Accounting (Hesap Yönetimi) kelimelerinin baş harflerinden oluşur (IETF'nin AAA Çalışma Grubu[B27]).

# 2. Sertifikaların Sağlanması

**Bilgi**

EAP–TLS, EAP–TTLS veya PEAP'i kullanmak için OpenSSL kurulmalıdır!

EAP–TLS'yi kullanırken hem Kimlik Kanıtlama Sunucusu hem de tüm istemciler sertifikalara ihtiyaç duyar [RFC2459[B28]]. EAP–TTLS veya PEAP'i kullanırken ise sadece Kimlik Kanıtlama Sunucusu sertifikalara gereksinim duyar; İstemci sertifikaları seçimliktir.

Sertifikaları yerel sertifika yetkilisinden (SY) alırsınız. Eğer hiç yerel SY yoksa **OpenSSL** kendinden–imzalı sertifikalar üretmek için kullanılabilir.

**FreeRADIUS** kaynağına dahil edilmiş, kendinden–imzalı sertifikalar üretmek için bazı yardımcı betikler mevcuttur. Betikler, **FreeRADIUS** kaynağında bulunan `scripts/` klasörünün altında bulunmaktadır:

`CA.all` sorduğu bazı sorulara dayanarak sertifikalar üreten bir kabuk betiğidir. `CA.certs` betiğin başlangıcında önceden tanımlanmış bilgiye dayanarak etkileşimsiz olarak sertifikalar üretir.

**Bilgi**

Betikler OpenSSL'de mevcut olan `CA.pl` denilen bir Perl betiği kullanır. `CA.all` ve `CA.certs`'te bu Perl betiğine olan yol, betiğin çalıştırılabilmesi için değiştirilmeye ihtiyaç duyabilir.

**İpucu**

Kendi sertifikalarınızı nasıl üretebileceğiniz hakkında daha fazla bilgiyi SSL certificates HOWTO[B29] belgesinde bulabilirsiniz.

# 3. Kimlik Kanıtlama Sunucusu: FreeRADIUS'un Kurulması

**FreeRADIUS** tamamen GPL'li RADIUS sunucu uygulamasıdır. Kimlik kanıtlama mekanizmalarını geniş çapta destekler, ama bu belgede örnek olarak PEAP kullanılmıştır.

## 3.1. FreeRADIUS'un Kurulumu

**Yönerge 1. Kurulum**

1. **FreeRADIUS** sitesine gidin, `http://www.freeradius.org/` ve en son sürümü indirin.

```
# cd /usr/local/src
# wget ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.0.tar.gz
# tar zxfv freeradius-1.0.0.tar.gz
# cd freeradius-1.0.0
```

2. Paketi yapılandırın, derleyin ve kurun:

```
# ./configure
# make
# make install
```

**configure** *betiğini çalıştırırken seçenek belirtebilirsiniz. Daha fazla bilgi için* **./configure --help** *kullanın veya README dosyasını okuyun.*

Çalıştırabilir dosyalar `/usr/local/bin` ve `/usr/local/sbin`'e, yapılandırma dosyaları ise `/usr/local/etc/raddb` altına kurulur.

Eğer birşey yanlış giderse, kaynakla birlikte gelen `INSTALL` ve `README` dosyalarını okuyun. RADIUS SSS[B31]'de değerli bilgiler içerir.

## 3.2. FreeRADIUS'un Yapılandırılması

**FreeRADIUS** büyük ve güçlü bir yapılandırma dosyasına sahiptir. O kadar büyüktür ki, bu dosya daha küçük birkaç dosyaya parçalanıp daha sonra bu dosyalar ana `radius.conf` dosyasına "dahil edilmektedir".

İstediğinizi yapmanız için FreeRADIUS'u kullanmanın ve ayağa kaldırmanın çeşitli yolları vardır: örn., kullanıcı bilgisini LDAP, SQL, PDC, Kerberos, vs.'den alın. Bu belgede, düz metin dosyası `users`'taki kullanıcı bilgisi kullanılmaktadır.

**İpucu**

Yapılandırma dosyalarına ayrıntılı bir şekilde yorum satırları eklenmiştir, ama eğer yeterli gelmezse kaynakla birlikte gelen `doc/` dizini ek bilgi içerir.

**Yönerge 2. Yapılandırma**

1. Yapılandırma dosyaları `/usr/local/etc/raddb/` altında bulunabilir.

```
# cd /usr/local/etc/raddb/
```

2. Ana yapılandırma dosyası`radiusd.conf`'u açın, *ve yorum satırlarını okuyun!* Şifreli PEAP tüneli içinde, MS–CHAPv2 kimlik kanıtlama mekanizması kullanılır.

   a. MPPE [RFC3078[B32]] PMK'yi AP'ye göndermekten sorumludur. Aşağıdaki ayarların yapıldığından emin olun:

```
# MODULES altında mschap'ın yorum satırı gibi yer
# almadığından emin olun!
mschap {
  # authtype değeri, eğer varsa, kimlik kanıtlama süresince
  # Auth-Type'ın üstüne yazmak (veya eklemek) için kullanılacak.
  # Normalde, MS-CHAP olmalı.
  authtype = MS-CHAP

  # eğer use_mppe no'ya ayarlanmamışsa, mschap,
  # MS-CHAPv2 için,MS-CHAPv1 ve MS-MPPE-Recv-Key/MS-MPPE-Send-Key
  # için MS-CHAP-MPPE-Keys ekleyecektir.
  use_mppe = yes

  # eğer mppe etkinse, require_encryption ile
  # şifreleme etkinleştirilebilir.
  #
  require_encryption = yes

  # require_strong her zaman 128 bitlik anahtar
  # şifrelemesi gerektirir.
  #
  require_strong = yes

  authtype = MS-CHAP
  # modül kimlik kanıtlamayı kendi kendine yapabilir VEYA
  # bir Windows Domain Controller kullanabilir. Bunun nasıl
  # yapılacağı için radius.conf dosyasına bakınız.
}
```

   b. `authorize` ve `authenticate`'in şunları içerdiğinden emin olun:

```
authorize {
    preprocess
    mschap
```

```
    suffix
    eap
    files
}

authenticate {

      #
      #  MSCHAP kimlik kanıtlaması.
      Auth-Type MS-CHAP {
            mschap
      }

      #
      #  EAP kimlik kanıtlamasına izin ver.
      eap
  }
```

3. `clients.conf` dosyasını hangi ağa hizmet ettiğini belirlemek için değiştirin:

```
# Burada, hangi ağa hizmet verdiğimizi belirliyoruz:
client 192.168.0.0/16 {
    # Bu Kimlik Kanıtlayıcı (erişim noktası) ve Kimlik
    # Kanıtlama Sunucusu (RADIUS) arasında paylaşılan sırdır.
    secret          = SharedSecret99
    shortname       = testnet
}
```

4. `eap.conf` da oldukça açık olmalı.

   a. `default_eap_type`'ı `peap`'e ayarlayınız:

```
default_eap_type = peap
```

   b. PEAP TLS kullandığı için TLS bölümü şunları içermeli:

```
tls {
    # Özel anahtar parolası
       private_key_password = SecretKeyPass77
    # Özel anahtar
    private_key_file = ${raddbdir}/certs/cert-srv.pem
    # Güvenilir Üst Sertifika Yetkilisi
    CA_file = ${raddbdir}/certs/demoCA/cacert.pem
    dh_file = ${raddbdir}/certs/dh
    random_file = /dev/urandom
    }
```

   c. `peap` bölümünü bulun ve aşağıdakini içerdiğinden emin olun:

```
peap {
  #  Tünelli EAP oturumu tünelsiz EAP modülünden farklı
  #  bir EAP türüne ihtiyaç duyar.
  #  PEAP tünelinde Windows istemcileri tarafından
  #  desteklenen öntanımlı tür olarak MS-CHAPv2
  #  kullanmanızı tavsiye ederiz.
  default_eap_type = mschapv2
}
```

5. Kullanıcı bilgisi bir düz metin dosyası olan `users`'ta tutulur. Kullanıcı bilgisini tutmak için daha karmaşık bir çözüm tercih edilebilirdi (SQL, LDAP, PDC, vs.)., şu an bir IETF taslağıdır.

`users` dosyasının aşağıdaki kaydı içerdiğinden emin olun:

```
"testuser"      User-Password == "Secret149"
```

# 4. İstemci: Xsupplicant'ın Kurulması

İstemci kimlik kanıtlamasına gereksinim duyan genellikle bir dizüstü bilgisayar veya diğer başka bir (telsiz) aygıttır. **`Xsupplicant`** IEEE 802.1X–2001 standartının "İstemci" parçası olduğunu bildirir.

## 4.1. Xsupplicant'ın Kurulumu

**Yönerge 3. Kurulum**

1. En güncel kaynağı `http://www.open1x.org/` adresinden indirin.

```
# cd usr/local/src
# wget http://belnet.dl.sourceforge.net/sourceforge/open1x/xsupplicant-
1.0.tar.gz
# tar zxfv xsupplicant-1.0.tar.gz
# cd xsupplicant
```

2. Paketi yapılandırın, derleyin ve kurun:

```
# ./configure
# make
# make install
```

3. Eğer yapılandırma dosyası `etc` dizininin altına kurulmamışsa kendiniz yapın:

```
# mkdir -p /usr/local/etc/1x
# cp etc/tls-example.conf /usr/local/etc/1x
```

Eğer kurulum başarısız olursa kaynağa dahil edilmiş olan `README` ve `INSTALL` dosyalarını okuyun. Ayrıca, Resmi Belgelendirme[B34]'yi de okuyabilirsiniz.

## 4.2. Xsupplicant'ın Yapılandırılması

**Yönerge 4. Yapılandırma**

1. İstemci root sertifikasına erişebilmelidir.

   Eğer İstemci Kimlik Kanıtlama Sunucusundan (çift yönlü) doğrulamaya ihtiyaç duyuyorsa, İstemci sertifikalarına da erişebilmelidir.

   Bir sertifika dizini oluşturun ve sertifikaları onun içine taşıyın:

```
# mkdir -p /usr/local/etc/1x/certs
# cp root.pem /usr/local/etc/1x/certs/
# (seçimlik istemci sertifikalarını aynı dizine kopyalayın)
```

2. Yapılandırma dosyasını açın ve düzenleyin:

```
# startup_command: Xsupplicant ilk başlatılırken çalıştırılacak komut.
# Bu komut, kartın ağ ile kusursuz ilişkilendirilmesi için yapılandırılması
# gibi şeyleri yapabilir.
startup_command = <BEGIN_COMMAND>/usr/local/etc/1x/startup.sh<END_COMMAND>
```

   `startup.sh` çabucak oluşturulacak.

3. İstemcinin kimlik doğrulaması olunca, bir DHCP isteği iletecektir veya elle bir IP adresi atayacaktır. Burada, İstemci kendi IP adresini `startup2.sh` dosyasında elle ayarlıyor:

```
# first_auth_command: Xsupplicant telsiz bir ağa kimlik doğrulaması
#   yapacağı zaman çalıştırılacak ilk komut. Bu genellikle
#   bir DHCP istemci sürecini başlatmak için kullanılır.
#first_auth_command = <BEGIN_COMMAND>dhclient %i<END_COMMAND>
first_auth_command=<BEGIN_COMMAND>/usr/local/etc/1x/startup2.sh<END_COMMAND>
```

4. `-i` sadece hata ayıklama amacıyla (geliştiricilere göre bu seçenek çıkarılabilir) kullanılabileceği için, `allow_interfaces` ayarlanmalı:

```
allow_interfaces = eth0
deny_interfaces = eth1
```

5. Sonra, NETWORK SECTION'ın altında, PEAP'i yapılandıracağız:

```
# PEAP'i kullanıyor olacağız
allow_types = eap_peap

# İlk aşamada (şifrelenmemiş aşama) kullanıcı adını
# öğrenmek için kulak misafiri olmak isteyenleri istemiyoruz,
# bu nedenle 'identity hiding' kullanılır
# (sahte bir kullanıcı adı kullanılır).
identity = <BEGIN_ID>anonymous<END_ID>

eap-peap {
  # tls'de olduğu gibi ya bir root sertifikası ya da
  # root sertifikalarırı içeren bir dizin tanımlayın.
  root_cert = /usr/local/etc/1x/certs/root.pem
  #root_dir = /path/to/root/certificate/dir
  #crl_dir = /path/to/dir/with/crl
  chunk_size = 1398
  random_file = /dev/urandom
  #cncheck = myradius.radius.com   # Sunucu sertifikasının CN alanında
                                   # bu değere sahip olduğundan emin olun.
  #cnexact = yes                   # Tam bir eşleşme olmalı mı?
  session_resume = yes

  # Şu an 'all' sadece mschapv2.
  # Eğer hiç allow_types tanımlanmamışsa 'all' öntanımlıdır.
  #allow_types = all # burada all = MSCHAPv2, MD5, OTP, GTC, SIM
  allow_types = eap_mschapv2

  # Şimdi, PEAP'te bu yöntemlerden her hangi birini uygulayabilirsiniz:
  eap-mschapv2 {
    username = <BEGIN_UNAME>testuser<END_UNAME>
    password = <BEGIN_PASS>Secret149<END_PASS>
  }
}
```

6. İstemci ilk olarak erişim noktası ile ilişkilendirilmeli. `startup.sh` betiği o işi yapar. O aynı zamanda **`Xsupplicant`**'ın çalıştırdığı ilk komuttur.

**Bilgi**

**`iwconfig`**'e verdiğimiz sahte anahtara dikkat edin (*enc 000000000*)! Bu anahtar sürücüye şifreli kipte çalışmasını söyler. Anahtar, başarılı kimlik kanıtlamanın ardından başkasıyla değiştirilir. Eğer

şifreleme AP'de (deneme amacıyla) kapalıysa bu `enc off`'a ayarlanabilir.

`startup.sh` ve `startup2.sh`, her ikisi de `/usr/local/etc/1x/` altında olmalı.

```
#!/bin/bash
echo "$0: işlem başlatılıyor"
# Arayüzü devredışı bırakın (eğer çalışıyor ise)
/sbin/ifconfig eth0 down
# Rotaların boşaltıldığından emin olmak için
sleep 1
# Arayüzü sahte bir anahtarla yapılandırın
/sbin/iwconfig eth0 mode managed essid testnet enc 000000000
# Arayüzü başlatın ve çoğa gönderim paketlerini dinlediğinden emin olun
/sbin/ifconfig eth0 allmulti up
echo "$0: işlem tamam"
```

7. Sonraki dosya IP adresini statik olarak ayarlamak için kullanılır. Eğer bir DHCP sunucusu varsa (birçok erişim noktasında genellikle vardır), bu dosya olmayabilir.

```
#!/bin/bash
echo "$0: işlem başlatılıyor"
# IP adresinin atanması
/sbin/ifconfig eth0 192.168.1.5 netmask 255.255.255.0
echo "$0: işlem tamam"
```

# 5. Kimlik Kanıtlayıcı: Kimlik Kanıtlayıcının Kurulması (Erişim Noktası)

Kimlik kanıtlama işlemi süresince Kimlik Kanıtlayıcı sadece İstemci ve Kimlik Kanıtlama Sunucusu (RADIUS) arasındaki iletileri taşır. İstemci ile Kimlik Kanıtlayıcı arasında EAPOL ve Kimlik Kanıtlayıcı ile Kimlik Kanıtlama Sunucusu arasında UDP kullanılır.

## 5.1. Erişim Noktası

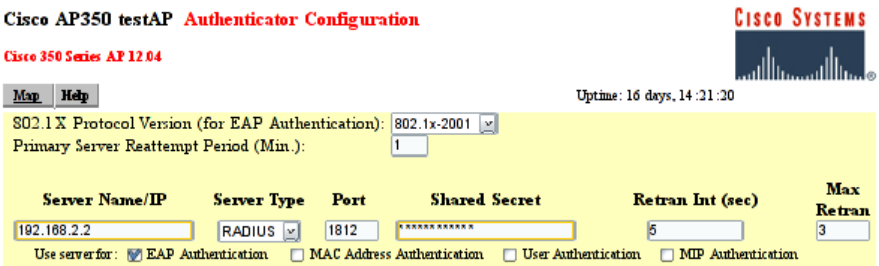
Birçok erişim noktası 802.1X (ve RADIUS) kimlik kanıtlaması için desteğe sahiptir. Önce 802.1X kimlik kanıtlaması kullanabilmesi için yapılandırılmalıdır.

**Bilgi**

*EN'de 802.1X'i yapılandırma ve ayarlama işlemleri satıcılar arasında farklılık gösterebilir.* Aşağıda Cisco AP350'yi çalıştırmak için gereken ayarlar listelenmiştir. TIKP, CCMP vs. gibi diğer ayarlar da ayrıca yapılabilir.

AP, ESSID'i deneme ağına ayarlanmalı ve etkinleştirilmeli:

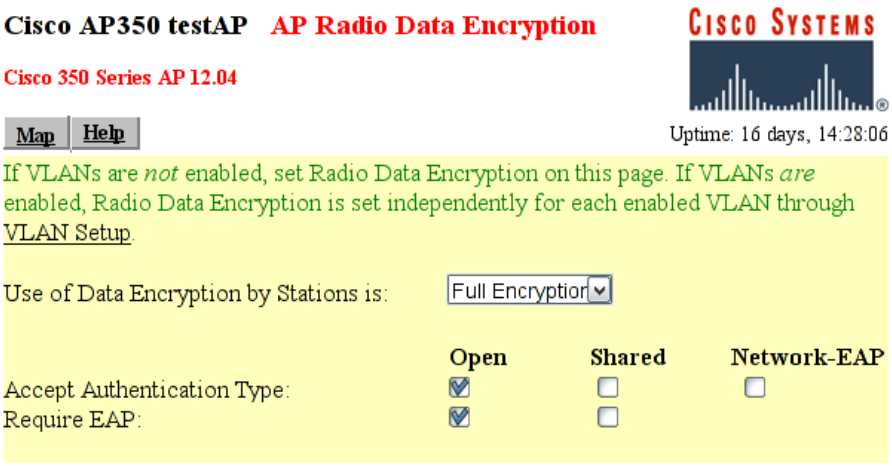
**Şekil 5. Cisco AP350 RADIUS yapılandırma ekranı**



Cisco AP–350 için RADIUS yapılandırma ekranı

- *802.1X–2001:* 802.1X Protokol sürümünün "802.1X–2001" 'e ayarlandığından emin olun. Bazı eski Erişim Noktaları 802.1X standartının sadece taslak sürümünü destekler (ve bu nedenle çalışmayabilir).
- *RADIUS Sunucu:* RADIUS sunucunun isim/IP adresi ve RADIUS sunucu ile Erişim Noktası arasında paylaşılan sır (ki bu belgede "SharedSecret99" olarak geçer). *Cisco AP350 RADIUS yapılandırma ekranı* (sayfa: 15)'e bakınız.
- *EAP Kimlik Kanıtlama:* RADIUS sunucu EAP kimlik kanıtlaması için kullanılmalıdır.

**Şekil 6. Cisco AP350 Şifreleme yapılandırma ekranı**




Cisco AP–350 için Şifreleme yapılandırma ekranı

- Sadece şifreli akışa izin vermek için *Tam Şifreleme* kullanılır. 802.1X'in şifrelemesiz kullanılabileceğine dikkat edin.
- Şifreleme anahtarları gelmeden önce İstemci ile Erişim Noktasını ilişkilendirmek için *Açık Kimlik Kanıtlama* kullanılır. İlişkilendirme yapılır yapılmaz İstemci, EAP kimlik kanıtlamasına başlayabilir.
- "Açık Kimlik Kanıtlama" için *EAP'ye ihtiyaç duyulur*. Bu, sadece kimlik kanıtlaması yapılmış kullanıcıların ağa girmesine izin verilmesini sağlar.

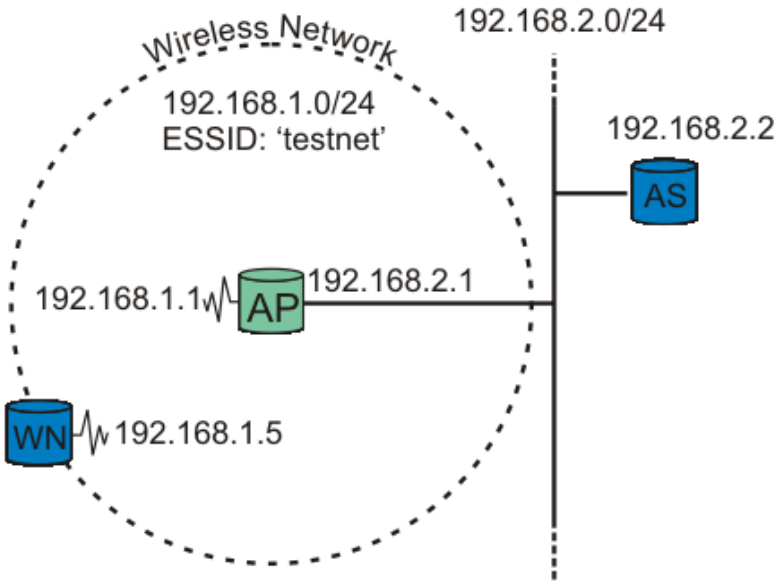
## 5.2. Linux Kimlik Kanıtlayıcı

Sıradan bir Linux düğümü bir telsiz Erişim Noktası ve Kimlik Kanıtlayıcı gibi davranacak şekilde ayarlanabilir. Linux'un AP olarak nasıl kurulup kullanılacağı bu belgenin kapsamı dışındadır. Simon Anderson'un Linux Wireless Access Point HOWTO[B36] belgesi size kılavuzluk edebilir.

# 6. Deneme Ağı

## 6.1. Deneme Sistemi

**Şekil 7. Deneme Sistemi**




Telsiz bir düğüm kimlik doğrulaması isteğinde bulunuyor.

Bizim deneme sistemimiz iki düğüm ve bir Erişim Noktasından (AP) oluşur. Bir düğüm İstemci (WN) gibi, diğeri RADIUS (AS) çalıştıran artalan Kimlik Kanıtlama Sunucusu gibi davranır. Erişim Noktası Kimlik Kanıtlayıcıdır. Açıklama için *Deneme Sistemi* (sayfa: 16)'ye bakınız

**Önemli**

Erişim Noktasının Kimlik Kanıtlama Sunucusuna erişebilmesi (ping) ve tam tersi son derece önemlidir!

## 6.2. Bazı denemeler

**Yönerge 5. bazı denemeler**

1. RADIUS sunucu hata ayıklama kipinde başlatılır. Bu *çok miktarda* hata ayıklama bilgisi üretir. Önemli noktalar aşağıdadır:

```
# radiusd -X
Starting - reading configuration files ...
reread_config:  radiusd.conf'u okuyor
Config:   including file: /usr/local/etc/raddb/proxy.conf
Config:   including file: /usr/local/etc/raddb/clients.conf
Config:   including file: /usr/local/etc/raddb/snmp.conf
Config:   including file: /usr/local/etc/raddb/eap.conf
Config:   including file: /usr/local/etc/raddb/sql.conf
......
Module: Loaded MS-CHAP
  mschap: use_mppe = yes
  mschap: require_encryption = no
  mschap: require_strong = no
  mschap: with_ntdomain_hack = no
  mschap: passwd = "(null)"
  mschap: authtype = "MS-CHAP"
  mschap: ntlm_auth = "(null)"
Module: Instantiated mschap (mschap)
```

```
......
Module: Loaded eap
  eap: default_eap_type = "peap" ①
  eap: timer_expire = 60
  eap: ignore_unknown_eap_types = no
  eap: cisco_accounting_username_bug = no
rlm_eap: Loaded and initialized type md5
  tls: rsa_key_exchange = no ②
  tls: dh_key_exchange = yes
  tls: rsa_key_length = 512
  tls: dh_key_length = 512
  tls: verify_depth = 0
  tls: CA_path = "(null)"
  tls: pem_file_type = yes
  tls: private_key_file = "/usr/local/etc/raddb/certs/cert-srv.pem"
  tls: certificate_file = "/usr/local/etc/raddb/certs/cert-srv.pem"
  tls: CA_file = "/usr/local/etc/raddb/certs/demoCA/cacert.pem"
  tls: private_key_password = "SecretKeyPass77"
  tls: dh_file = "/usr/local/etc/raddb/certs/dh"
  tls: random_file = "/usr/local/etc/raddb/certs/random"
  tls: fragment_size = 1024
  tls: include_length = yes
  tls: check_crl = no
  tls: check_cert_cn = "(null)"
rlm_eap: Loaded and initialized type tls
  peap: default_eap_type = "mschapv2" ③
  peap: copy_request_to_tunnel = no
  peap: use_tunneled_reply = no
  peap: proxy_tunneled_request_as_eap = yes
rlm_eap: Loaded and initialized type peap
  mschapv2: with_ntdomain_hack = no
rlm_eap: Loaded and initialized type mschapv2
Module: Instantiated eap (eap)
......
Module: Loaded files
  files: usersfile = "/usr/local/etc/raddb/users" ④
......
Module: Instantiated radutmp (radutmp)
Listening on authentication *:1812
Listening on accounting *:1813
İstekleri işlemek için hazır. ⑤
```

① Varsayılan EAP türü PEAP'e ayarlanmıştır.

② RADIUS'un TLS ayarları burada ilklendirilir. Sertifika türü, yer ve parola burada listelenir.

③ PEAP tünelinin içinde MS–CHAPv2 kullanılır.

④ Kullanıcı adı/parola bilgisi `users` dosyasında bulunur.

⑤ RADIUS sunucu başarılı bir şekilde başladı. Gelen istekler için bekliyor.

Radius sunucu istekleri işlemek için artık hazır!

En ilginç çıktı yukarıda gösterilmiştir. Eğer en son satırın yerine her hangi bir hata iletisi alıyorsanız yapılandırmaya (yukarıda) dikkatli bir şekilde bakın.

2. Şimdi İstemci kimlik doğrulaması için hazır. **`Xsupplicant`**'ı hata ayıklama kipinde başlatın. İki başlatma betiği tarafından üretilen çıktıyı göreceğimize dikkat edin: `startup.sh` ve `startup2.sh`.

```
# xsupplicant -c /usr/local/etc/1x/1x.conf -i eth0 -d 6
/etc/1x/startup.sh: işlem başlatılıyor
/etc/1x/startup.sh: işlem tamam
/etc/1x/startup2.sh: işlem başlatılıyor
/etc/1x/startup2.sh: işlem tamam
```

3. Aynı zamanda RADIUS sunucu da çok miktarda çıktı üretiyor olacak. Başlıca bilgiler aşağıda gösterilmiştir:

```
......
rlm_eap: Request found, released from the list
rlm_eap: EAP/peap
rlm_eap: processing type peap
rlm_eap_peap: Authenticate
rlm_eap_tls: processing TLS ①
eaptls_verify returned 7
rlm_eap_tls: Done initial handshake
eaptls_process returned 7
rlm_eap_peap: EAPTLS_OK ②
rlm_eap_peap: Session established.  Decoding tunneled attributes.
rlm_eap_peap: Received EAP-TLV response.
rlm_eap_peap: Tunneled data is valid.
rlm_eap_peap: Success
rlm_eap: Freeing handler
modcall[authenticate]: module "eap" returns ok for request 8
modcall: group authenticate returns ok for request 8
Login OK: [testuser/<no User-Password attribute>] (from client testnet port
37 cli 0002a56fa08a)
Sending Access-Accept of id 8 to 192.168.2.1:1032 ③
      MS-MPPE-Recv-Key = 0xf21757b96f52ddaefe084c343778d0082c2c8e12ce18ae10
a79c550ae61a5206 ④
      MS-MPPE-Send-Key = 0x5e1321e06a45f7ac9f78fb9d398cab5556bff6c9d003cdf8
161683bfb7e7af18
      EAP-Message = 0x030a0004
      Message-Authenticator = 0x00000000000000000000000000000000
      User-Name = "testuser"
```

① TLS oturumu başlatılıyor. TLS el sıkışması yapılıyor.

② TLS oturumu (PEAP–şifreli tünel) çalışıyor.

③ İstemcinin RADIUS sunucu tarafından başarıyla kimlik kanıtlaması yapılmıştır. "Access–Accept" iletisi gönderilir.

④ *MS–MPPE–Recv–Key* [RFC2548[B38] bölüm 2.4.3], Kimlik Kanıtlayıcıya (erişim noktası) yönelmiş, MPPE Protokolüyle [RFC3078[B39]] şifrelenmiş Kimlik Kanıtlayıcı ve Kimlik Kanıtlama Sunucusu arasında paylaşılan sırrı anahtar olarak kullanan Ana Oturum Anahtarını (PMK) içerir. İstemci *Anahtar Yönetimi* (sayfa: 6) bölümünde tanımlandığı gibi MK'den aynı PMK'yi türetir.

4. Kimlik Kanıtlayıcı (erişim noktası) buna benzer günlük kayıtları gösterebilir:

```
00:02:16 (Info): Station 0002a56fa08a Associated
00:02:17 (Info): Station=0002a56fa08a User="testuser" EAP-Authenticated
```

İşte bu! İstemicini artık Erişim Noktasını kullanması için kimlik doğrulaması yapılmış oldu!

# 7. Xsupplicant ve Sürücü desteği hakkında

*Anahtar Yönetimi* (sayfa: 6) bölümünde açıklandığı gibi 802.1X ile Dynamic WEP/802.11i kullanmanın büyük avantajlarından biri oturum anahtarları için destektir. Her bir oturum için yeni bir şifreleme anahtarı üretilir.

**Xsupplicant** bu belge yazılırken sadece "Dynamic WEP" 'i destekliyordu. WPA ve RSN/WPA2 için destek (802.11i) üzerinde çalışılıyor ve Chris Hessing'e (**Xsupplicants** geliştiricilerinden biri) göre 2004/2005 sonuna kadar destekleneceği tahmin ediliyor.

Tüm telsiz ürünler dynamic WEP'i veya WPA'yı desteklemez. RSN'yi (WPA) kullanmak için donanımda yeni desteğe dahi gereksinim duyulabilir. Birçok eski sürücü ağda her hangi bir zamanda tek bir WEP anahtarı kullanılacağını farzeder. Anahtar değiştirildiğinde yeni anahtarın etkinleşmesi için kart yeniden başlatılır. Bu yeni bir kimlik kanıtlamayı tetikler ve hiç bitmeyen bir döngü vardır.

Yazım sırasında temel Linux çekirdeğindeki telsiz sürücülerin çoğu dynamic WEP/WPA'nın çalışması için yamalanmaya gereksinim duyuyordu. Zamanla bu yeni özellikleri destekleyecek şekilde güncelleneceklerdir. Bununla birlikte çekirdeğin dışında geliştirilen birçok sürücü dynamic WEP için desteğe sahiptir; HostAP, madwifi, Orinoco ve atmel sorunsuz çalışmalıdır.

Xsupplicant kullanmak yerine, wpa_supplicant[B42] kullanılabilir. Hem WPA hem RSN (WPA2) hem de geniş çapta EAP kimlik kanıtlama yöntemleri için desteği vardır.

# 8. SSS

FreeRADIUS[B43] (mutlaka tavsiye edilir!) ve Xsupplicant[B44] Web sitelerinin SSS bölümlerine bakmayı unutmayın.

**8.1. Global bir yapılandırma dosyası yerine kullanıcıya özel Xsupplicant yapılandırmasına izin vermek mümkün mü?**
**8.2. PEAP'i kullanmak istemiyorum; Onun yerine EAP–TTLS veya EAP–TLS'yi kullanabilir miyim?**
**8.3. GNU/Linux yerine bir Windows Supplicant (istemci) kullanabilir miyim?**
**8.4. Kullanıcı kimlik kanıtlamaları için bir Active Directory kullanabilir miyim?**
**8.5. Hiç Windows Supplicant istemcisi var mı?**

**8.1. Global bir yapılandırma dosyası yerine kullanıcıya özel Xsupplicant yapılandırmasına izin vermek mümkün mü?**

Hayır, şu an değil.

**8.2. PEAP'i kullanmak istemiyorum; Onun yerine EAP–TTLS veya EAP–TLS'yi kullanabilir miyim?**

Evet. EAP–TTLS'yi kullanmak için bu belgede kullanılan yapılandırmaya sadece ufak değişiklikler yapmanız gerekir. EAP–TLS'yi kullanmak için istemci sertifikaları kullanılmalıdır.

**8.3. GNU/Linux yerine bir Windows Supplicant (istemci) kullanabilir miyim?**

Evet. Windows XP SP1/Windows 2000 SP3 PEAP MSCHAPv2 için desteğe sahip (bu belgede kullanıldı). Bir Windows NASIL'ı burada bulunabilir: FreeRADIUS/WinXP Authentication Setup[B45]

**8.4. Kullanıcı kimlik kanıtlamaları için bir Active Directory kullanabilir miyim?**

Evet. FreeRADIUS "ntlm_auth"'u kullanarak AD'den kullanıcı kimlik kanıtlamalarını yapabilir.

**8.5. Hiç Windows Supplicant istemcisi var mı?**

Evet. Windows XP SP1 veya Windows 2000 SP3 ile WPA (PEAP/MS–CHAPv2) için destek mevcuttur. Diğer istemciler (denenmedi) Secure W2[B46] (ticari olmayan kullanım için bedavadır) ve WIRE1X[B47] içerir. Funk Software[B48] de ticari bir istemciye sahiptir.

# 9. Faydalı Kaynaklar

Genel olarak sadece 12 aydan daha eski olan IEEE standartları halka açıktır (şu bağdan "IEEE 802 Programını Alın"([B49]). Dolayısıyla yeni *802.11i* ve *802.1X–2004* standartlarının belgeleri mevcut değildir. Gelişim sürecindeki her hangi bir taslak/iş ile alakalı makalelere erişmek için IEEE katılımcısı olmalısınız (ki bu gerçekten hiç de zor değildir – sadece bir e–posta listesine katılın ve ilgili olduğunuzu söyleyin).

1. FreeRADIUS Sunucu Projesi
   http://www.freeradius.org/
2. P Open1x: IEEE 802.1X'in Açık Kaynak Uygulaması (Xsupplicant)
   http://www.open1x.org/
3. Open1x Kullanıcı Klavuzu
   http://sourceforge.net/docman/display_doc.php?docid=23371\&group_id=60236
4. Port–Tabanlı Ağ Erişim Denetimi (802.1X–2001)
   http://standards.ieee.org/getieee802/download/802.1X-«2001.pdf
5. RFC2246: TLS Protokolü Sürüm 1.0
   http://www.ietf.org/rfc/rfc2246.txt
6. RFC2459: Internet X.509 Açık Anahtar Altyapı Sistemi – Sertifika ve CRL Profili
   http://www.ietf.org/rfc/rfc2459.txt
7. RFC2548: Microsoft Satıcıya Özel RADIUS Özellikleri
   http://www.ietf.org/rfc/rfc2548.txt
8. RFC2716: PPP EAP TLS Kimlik Kanıtlama Protokolü
   http://www.ietf.org/rfc/rfc2716.txt
9. RFC2865: Uzaktan Aramalı Kullanıcı Kimlik Kanıtlama Hizmeti (RADIUS)
   http://www.ietf.org/rfc/rfc2865.txt
10. RFC3079: Microsoft Noktadan–Noktaya Şifreleme (MPPE) ile kullanmak için Anahtarlar Türetmek
    http://www.ietf.org/rfc/rfc3079.txt
11. RFC3579: EAP için RADIUS desteği
    http://www.ietf.org/rfc/rfc3579.txt
12. RFC3580: IEEE 802.1X RADIUS Kullanım Yönergeleri
    http://www.ietf.org/rfc/rfc3580.txt
13. RFC3588: Çap Tabanlı Protokol
    P http://www.ietf.org/rfc/rfc3588.txt
14. RFC3610: CBC–MAC (CCM) ile Sayaç
    http://www.ietf.org/rfc/rfc3610.txt
15. RFC3748: Genişleyebilir Kimlik Kanıtlama Protokolü (Extensible Authentication Protocol) (EAP)
    http://www.ietf.org/rfc/rfc3748.txt
16. Linux Telsiz Erişim Noktası NASIL
    http://oob.freeshell.org/nzwireless/LWAP-«HOWTO.html
17. SSL Sertifikaları NASIL
    http://www.tldp.org/HOWTO/SSL-«Certificates-«HOWTO/
18. OpenSSL: x509(1)
    http://www.openssl.org/docs/apps/x509.html

# 10. Teşekkür vs.

## 10.1. Bu belge nasıl üretildi?

Bu belge Emacs kullanılarak DocBook XML olarak yazıldı.

## 10.2. Geri bildirim

Öneriler, düzeltmeler ve eklemelere açığım. Katkıda bulunmak isteyenler benimle iletişime geçebilirler.Yıkıcı eleştiriler istemiyorum.

Bana <lars (at) unik.no> adresinden her zaman ulaşabilirsiniz.

Ana sayfa: http://www.gnist.org/~lars/

## 10.3. Teşekkür

Andreas Hafslund'a <andreha (at) unik.no> ve Thales Communication'a desteklerinden ötürü teşekkür ederim.

Değerleri katkıları için Artur Hecker'e <hecker (at) enst.fr>, Chris Hessing'e <chris.hessing (at) utah.edu>, Jouni Malinen'e <jkmaline (at) cc.hut.fi> ve Terry Simons'a da <galimore (at) mac.com> teşekkür ederim!

Dil gözden geçirmesi için Rick Moen'e teşekkür ederim! <rick (at) linuxmafia.com>

# GNU Free Documentation License

Version 1.2, November 2002



1. PREAMBLE

   The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

   This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

   We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

2. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world–wide, royalty–free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front–matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front–Cover Texts or Back–Cover Texts, in the notice that says that the Document is released under this License. A Front–Cover Text may be at most 5 words, and a Back–Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine–readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ascii without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard–conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine–generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements",

or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

3. VERBATIM COPYING

   You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

   You may also lend copies, under the same conditions stated above, and you may publicly display copies.

4. COPYING IN QUANTITY

   If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front–Cover Texts on the front cover, and Back–Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

   If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

   If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine–readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer–network location from which the general network–using public has access to download using public–standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

   It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

5. MODIFICATIONS

   You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

   A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front–matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—-for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front–Cover Text, and a passage of up to 25 words as a Back–Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front–Cover Text and one of Back–Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

6. COMBINING DOCUMENTS

   You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

   The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

   In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

7. COLLECTIONS OF DOCUMENTS

   You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

   You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

8. AGGREGATION WITH INDEPENDENT WORKS

   A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

   If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

9. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

10. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

11. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

## ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
  Copyright (C)  year  your name.
  Permission is granted to copy, distribute and/or modify this document
  under the terms of the GNU Free Documentation License, Version 1.2
  or any later version published by the Free Software Foundation;
  with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
  A copy of the license is included in the section entitled "GNU
  Free Documentation License".
```

If you have Invariant Sections, Front–Cover Texts and Back–Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

## Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(*B1*) http://www.freeradius.org

(*B2*) http://www.open1x.org

(*B3*) http://standards.ieee.org/getieee802/download/802.1X-«2001.pdf

(*B6*) http://www.open1x.org

(*B7*) http://www.freeradius.org

(*B8*) http://standards.ieee.org/getieee802/download/802.1X-«2001.pdf

(*B9*) http://www.ietf.org/rfc/rfc1994.txt

(*B13*) http://www.isaac.cs.berkeley.edu/isaac/wep-«faq.html

(*B14*) http://www.ietf.org/rfc/rfc3610.txt

(*B15*) http://csrc.nist.gov/publications/fips/fips197/fips-«197.pdf

(*B17*) http://www.ietf.org/rfc/rfc2898.txt

(*B18*) http://www.wi-«fi.org/

(*B19*) http://www.ietf.org/rfc/rfc3748.txt

(*B21*) http://www.ietf.org/rfc/rfc1994.txt

(*B22*) http://lists.cistron.nl/pipermail/cistron-«radius/2001-«September/002042.html

(*B23*) http://www.ietf.org/rfc/rfc2716.txt

(*B24*) http://www.ietf.org/rfc/rfc2759.txt

(*B25*) http://www.ietf.org/rfc/rfc2865.txt

(*B26*) http://www.ietf.org/rfc/rfc3588.txt

(*B27*) http://www.ietf.org/html.charters/aaa-«charter.html

(*B28*) http://www.ietf.org/rfc/rfc2459.txt

(*B29*) http://www.tldp.org/HOWTO/SSL-«Certificates-«HOWTO/

(*B31*) http://www.freeradius.org/faq/

(B32) http://www.ietf.org/rfc/rfc3078.txt

(B34) http://sourceforge.net/docman/display_doc.php?docid=23371\&group_id=60236

(B36) http://oob.freeshell.org/nzwireless/LWAP-“HOWTO.html

(B38) http://www.ietf.org/rfc/rfc2548.txt

(B39) http://www.ietf.org/rfc/rfc3078.txt

(B42) http://hostap.epitest.fi/wpa_supplicant/

(B43) http://www.freeradius.org/faq/

(B44) http://sourceforge.net/docman/display_doc.php?docid=23371\&group_id=60236#ch7

(B45) http://text.dslreports.com/forum/remark,“9286052~mode=flat

(B46) http://www.securew2.com

(B47) http://wire.cs.nthu.edu.tw/wire1x/

(B48) http://www.funk.com

(B49) http://standards.ieee.org/getieee802/

Bu dosya (p8021x-howto.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007