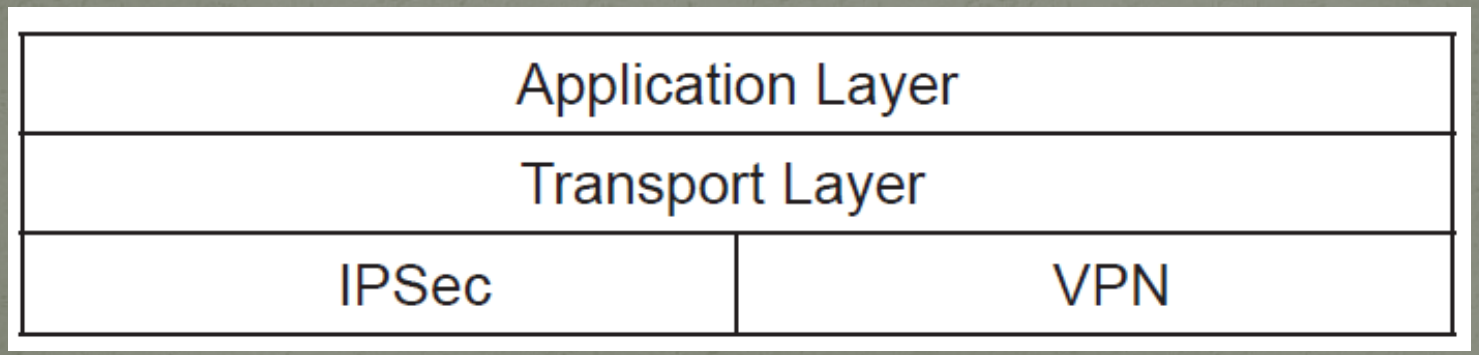
COMPUTER NETWORK SECURİTY PROTOCOLS

Network Layer

Data Link Layer

Network Katmanında Güvenlik

- IPSec (IP Security)
- VPN (Virtual Private Network)



IPSec

Temel Kavramlar

- Güvenli bir ağ bağlantısı oluşturmaya yarayan protokol
- Ipv4 ve Ipv6 ile uyumlu
- Mevcut uygulamalarda veya ağ yapısında değişiklik yapmaya gerek yok, ip üzerinde çalışır

IPSec Hizmetleri

IPSec Network katmanı üzerinde aşağıdaki özellikleri destekler

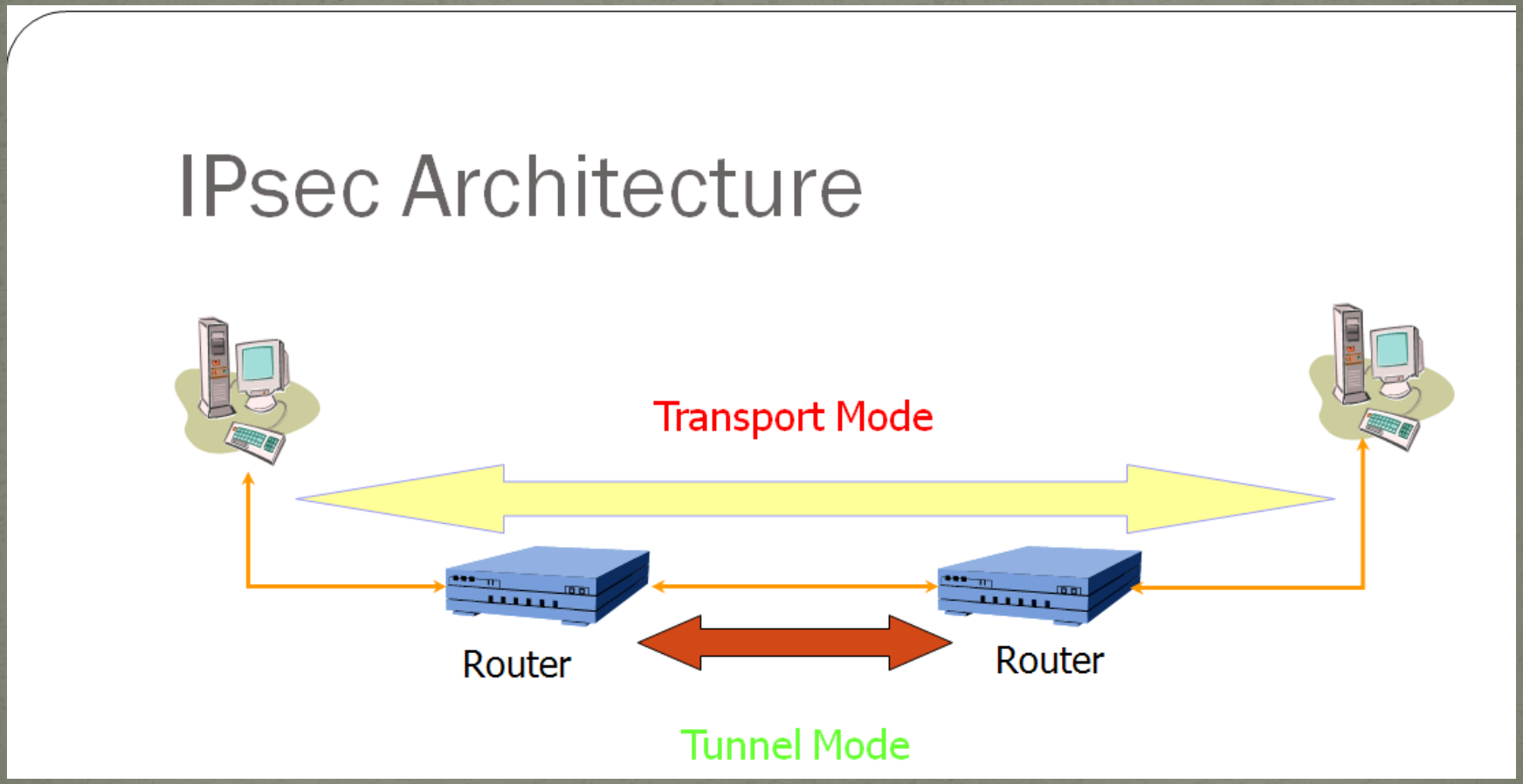
- Authentication (kimlik denetimi)
- Integrity (bütünlük)
- Confidentiality (gizlilik)
- Replay attack protection

IPSec Modları

İki farklı modda kullanılabilir

- Transport Mode :
  - client to client
  - ip paketinin payload kısmı kapsüllenir
- Tunnel Mode :
  - gateway to gateway
  - tüm ip paketi kapsüllenir

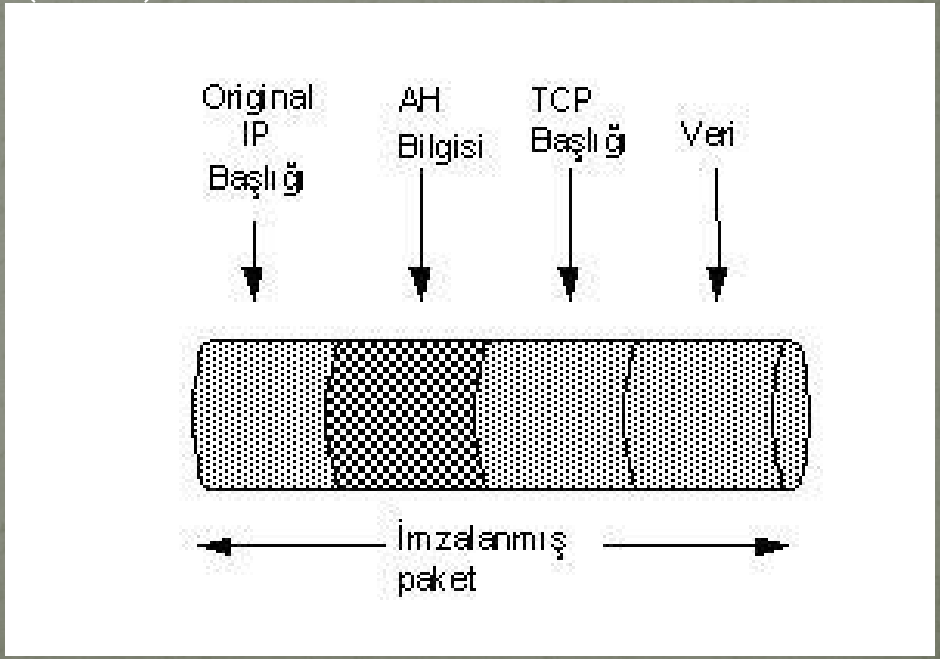
Transport Mode – Tunnel Mode



IPSec te Güvenlik Protokolleri

Güvenliği sağlanacak datagrama iki farklı güvenlik protokolü uygulanabilir.

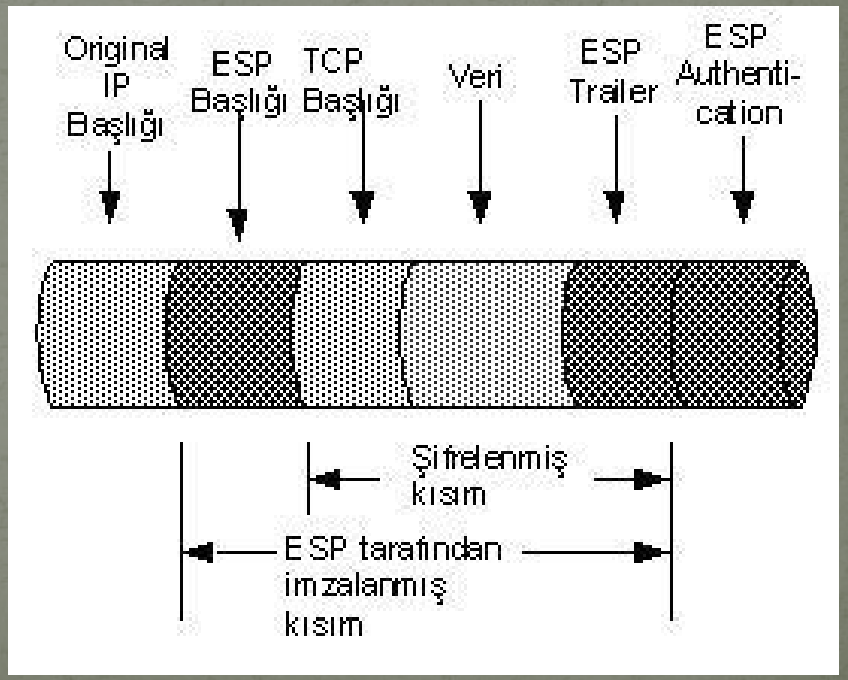
- Authentication Header (AH)
  - Kimlik Denetimi
  - Veri Bütünlüğü



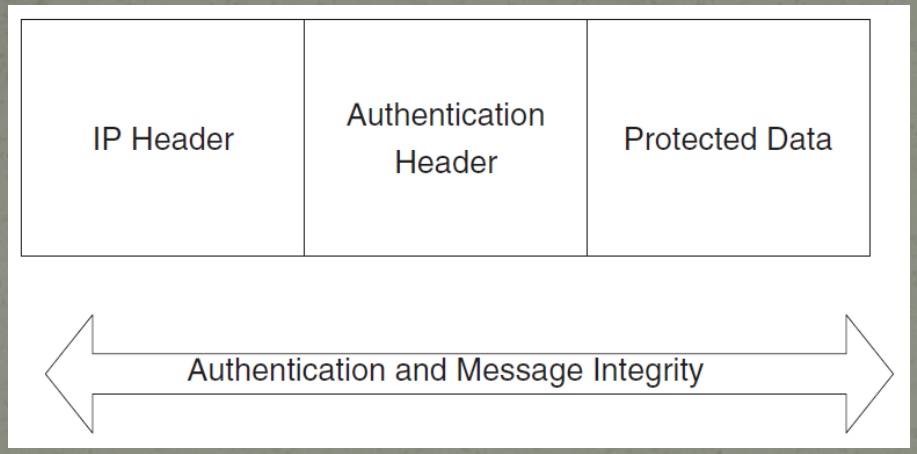
IPSec te Güvenlik Protokolleri

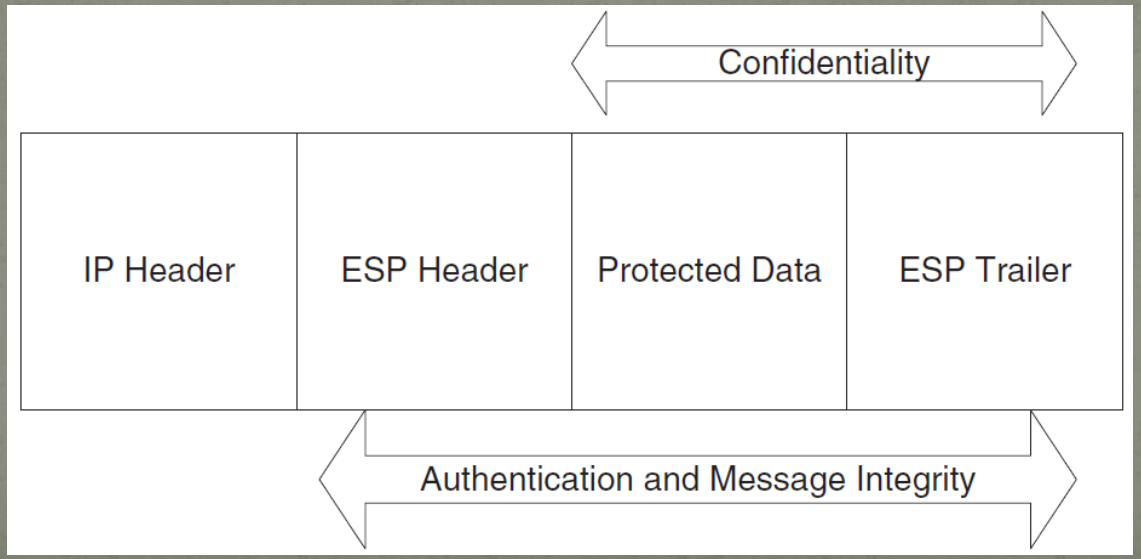
Güvenliği sağlanacak datagrama iki farklı güvenlik protokolü uygulanabilir.

- Encapsulating Security Payload (ESP)
  - Kimlik Denetimi
  - Veri Bütünlüğü
  - Gizlilik



Authentication Header (AH)
Encapsulating Security Payload (ESP)





Güvenlik Görüşmeleri (Security Negotiations)

IPSec kullanarak iletişim kuracak bilgisayarların, bu iletişim sırasında hangi algoritmaları ve protokolleri kullanacaklarını belirlemeleri gerekir.

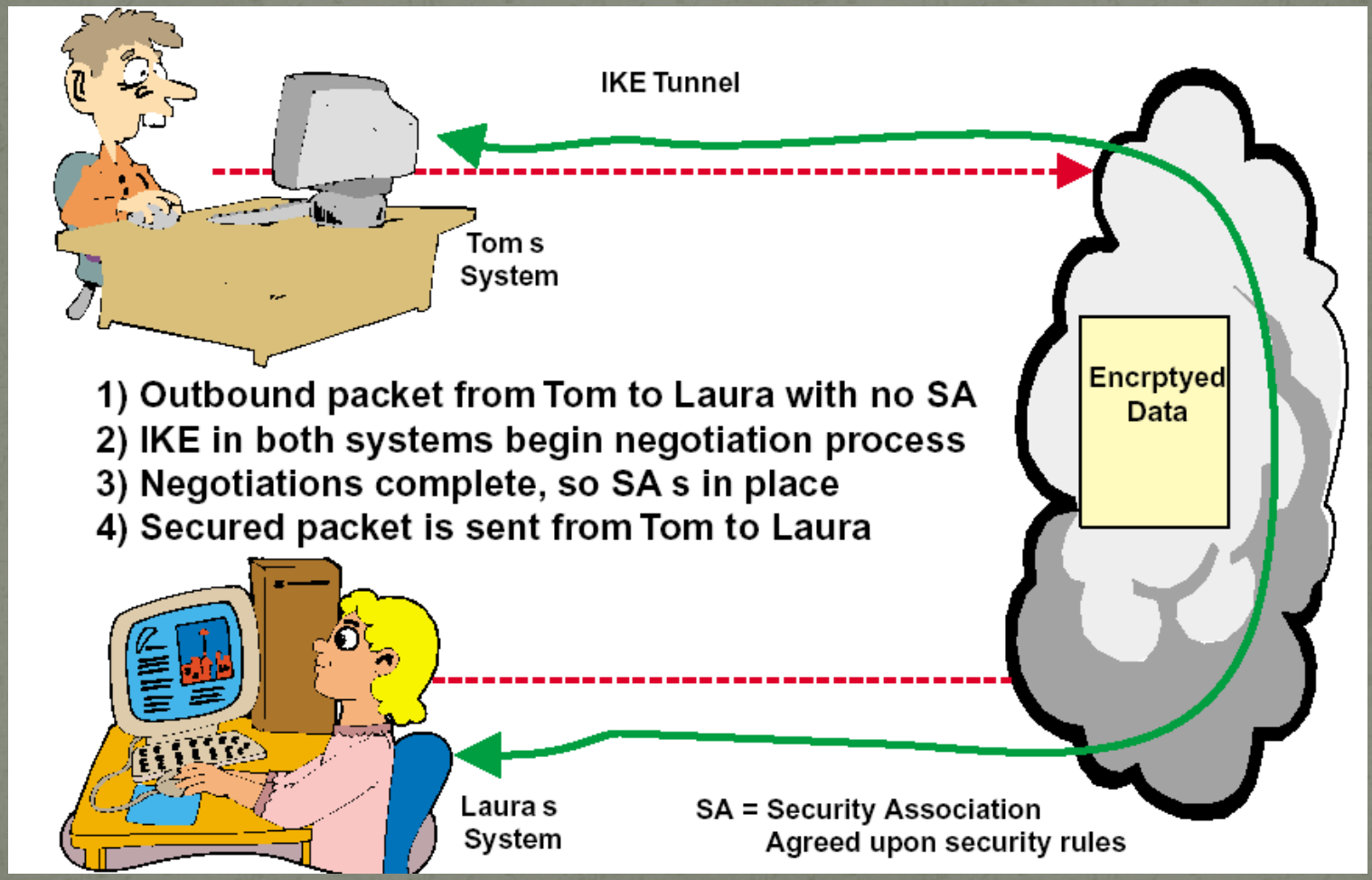
- IPSec'de, iletişim sırasında kullanılacak metodların hangileri olacağını belirleme işlemine ***security associations (SA)*** denir.
  - Kurulan SA'ları birbirinden ayırt edebilmek için Security Parameters Index (SPI)'ler kullanılır
  - Güvenlik İlişkileri her IPSec bilgisayarda belirli bir veritabanında saklanır (Security Association Database(SAD))

Security Associations (SA)

Her bir SA' da aşağıdaki parametreler belirlenir.

- Şifreleme algoritması (DES, 3DES..)
- Kimlik doğrulama algoritması (SHA1, MD5..)
- Oturum Anahtarı (Internet Key Exchange (IKE) aracılığıyla belirlenir)

Security Associations (SA)

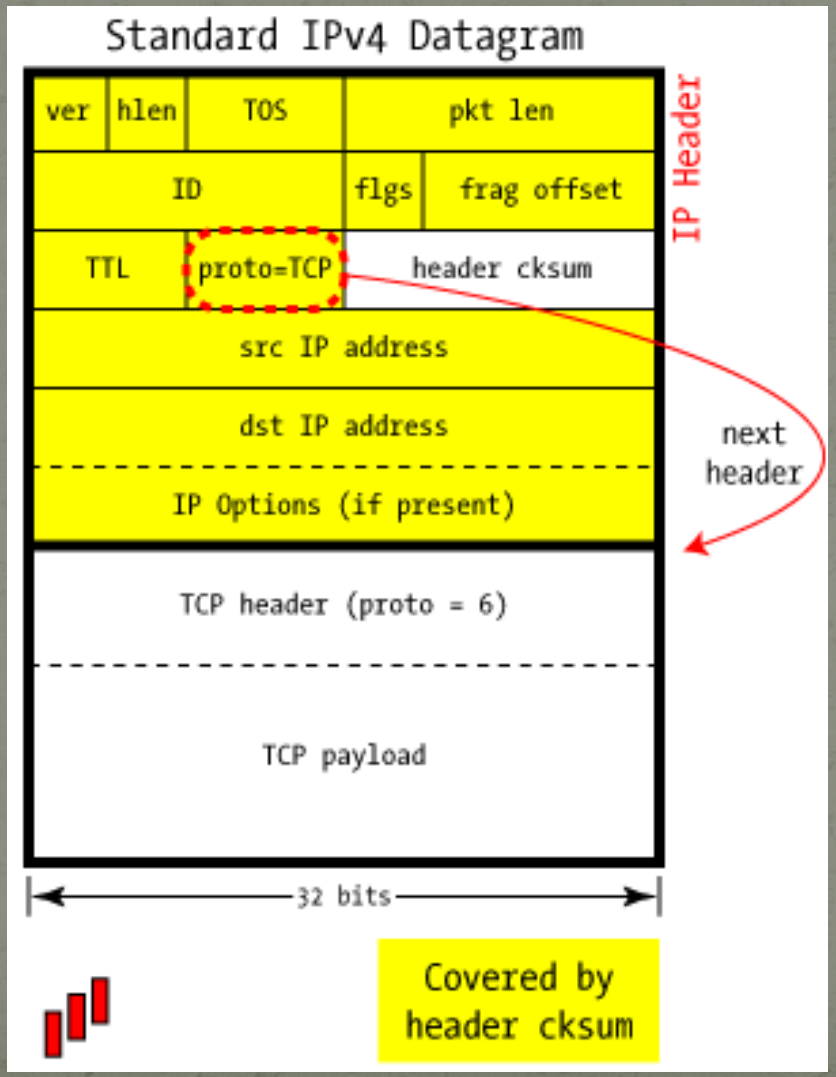


IKE (Internet Key Exchange)

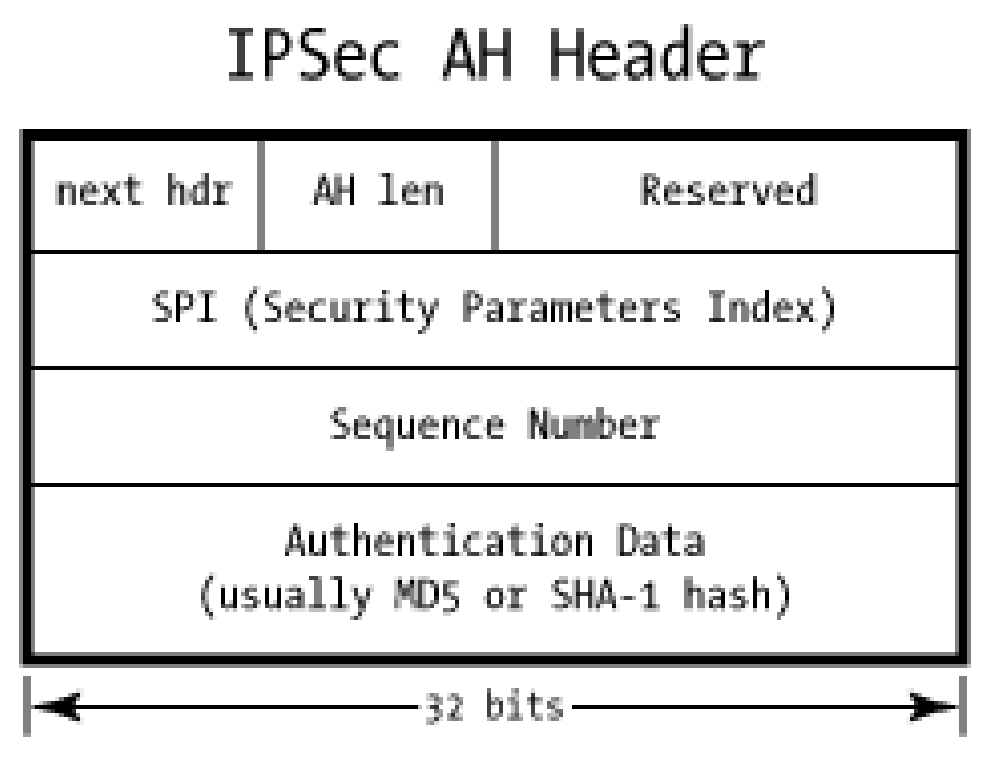
- IKE protokolü uç noktalarının hangi güvenlik politikalarında anlaşacaklarını kararlaştırmak için kullanılan bir metotdur.
  - Uç noktalara karşılıklı doğrulama için yöntem sağlar

- Yani IKE SA`ların yaratılmasını üstlenir ve bilgiyi güvenli hale getirmede kullanılacak anahtarları yaratır. Bu teknik veriyi kriptolayıp dekriptolamada kullanılacak anahtarların yaratılmasını sağlar.
  - Yeni IPSEC bağlantıları oluşturur (SA'ler yaratır)

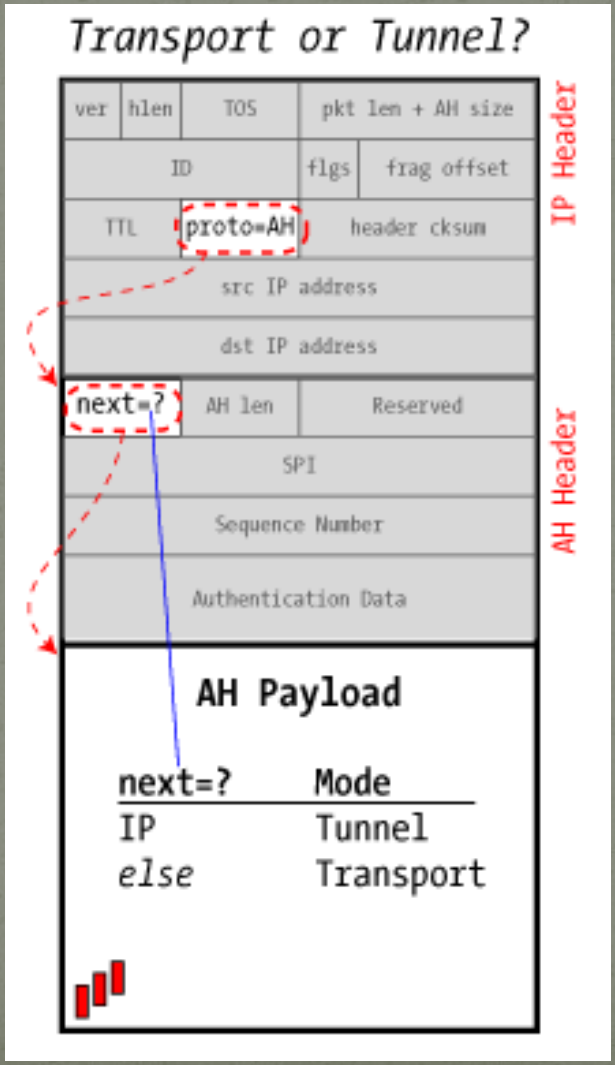
Standart IPv4 Datagramı



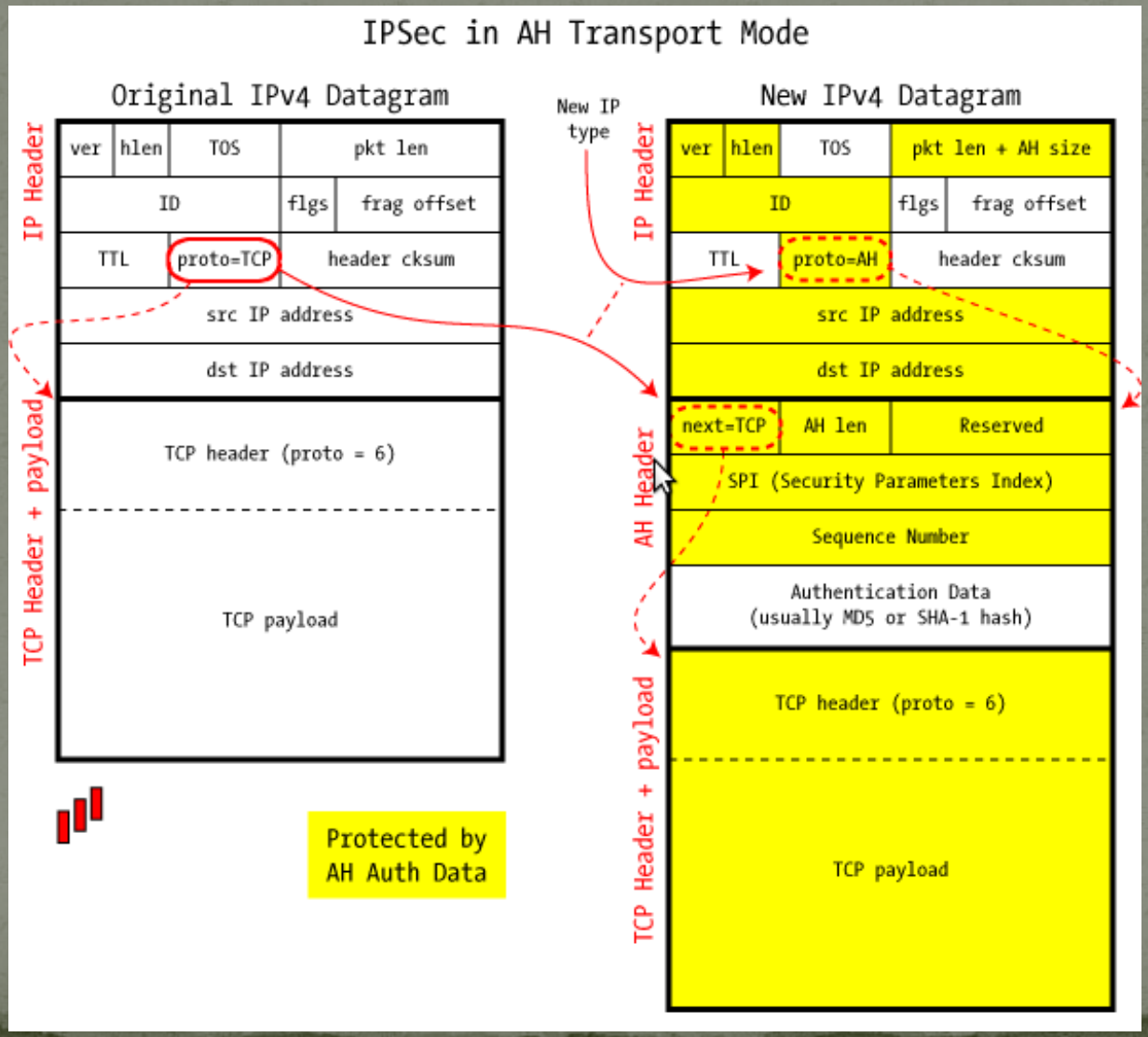
Authentication Header



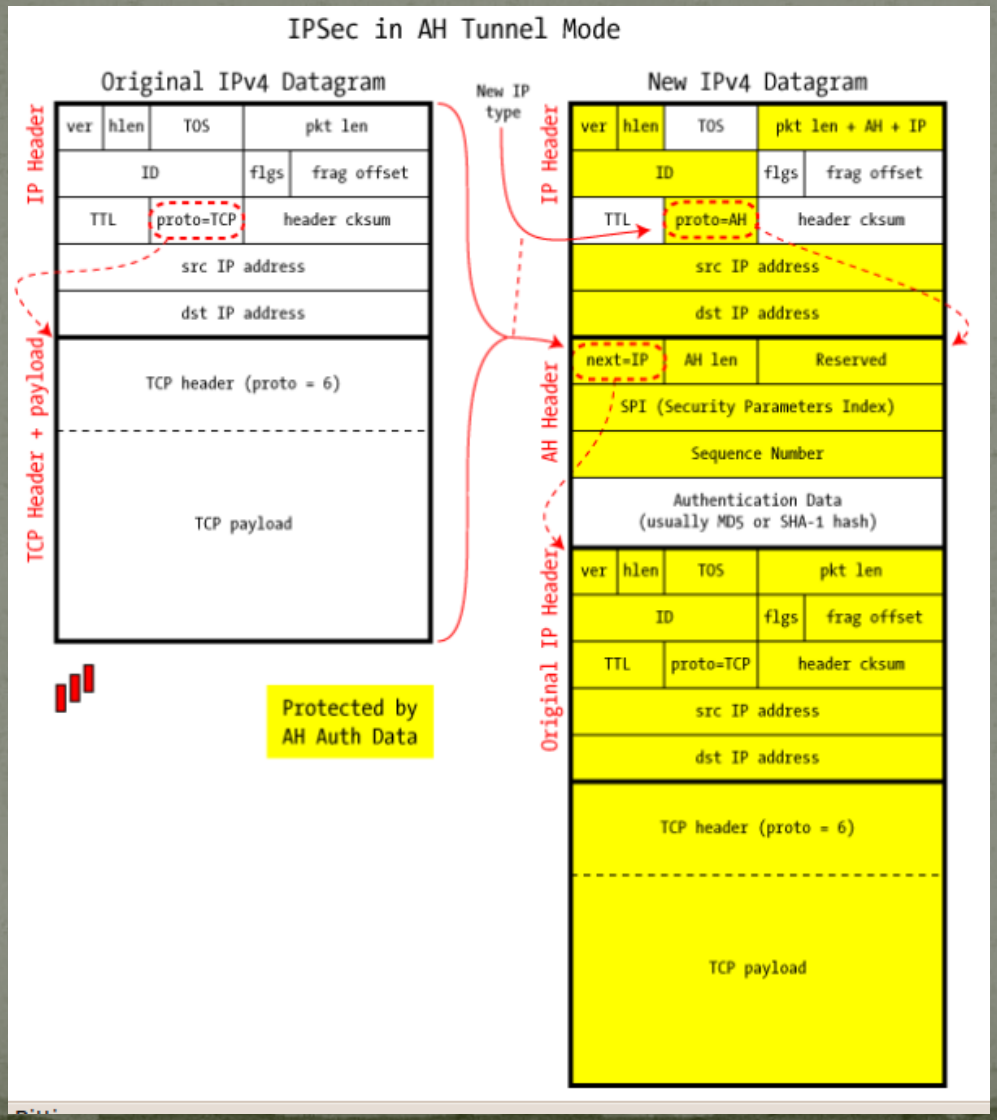
Hangisi?
Transport mode - Tunnel mode



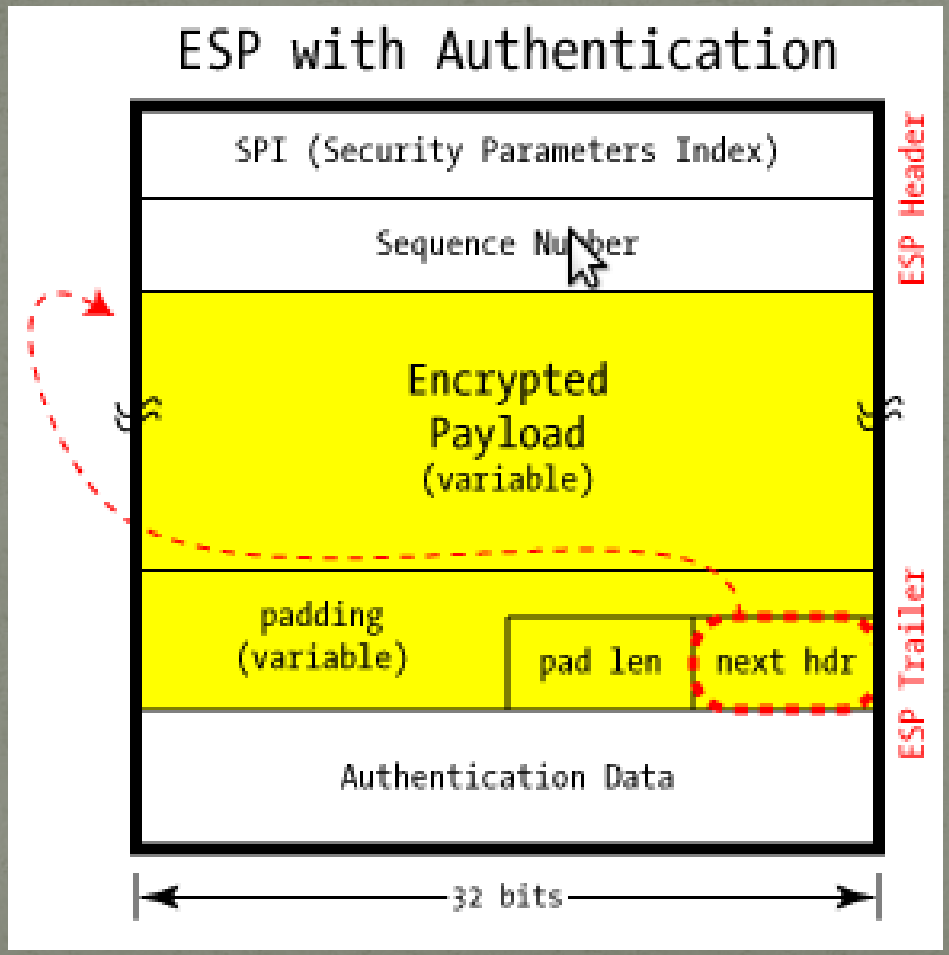
IPSec in AH Transport Mode



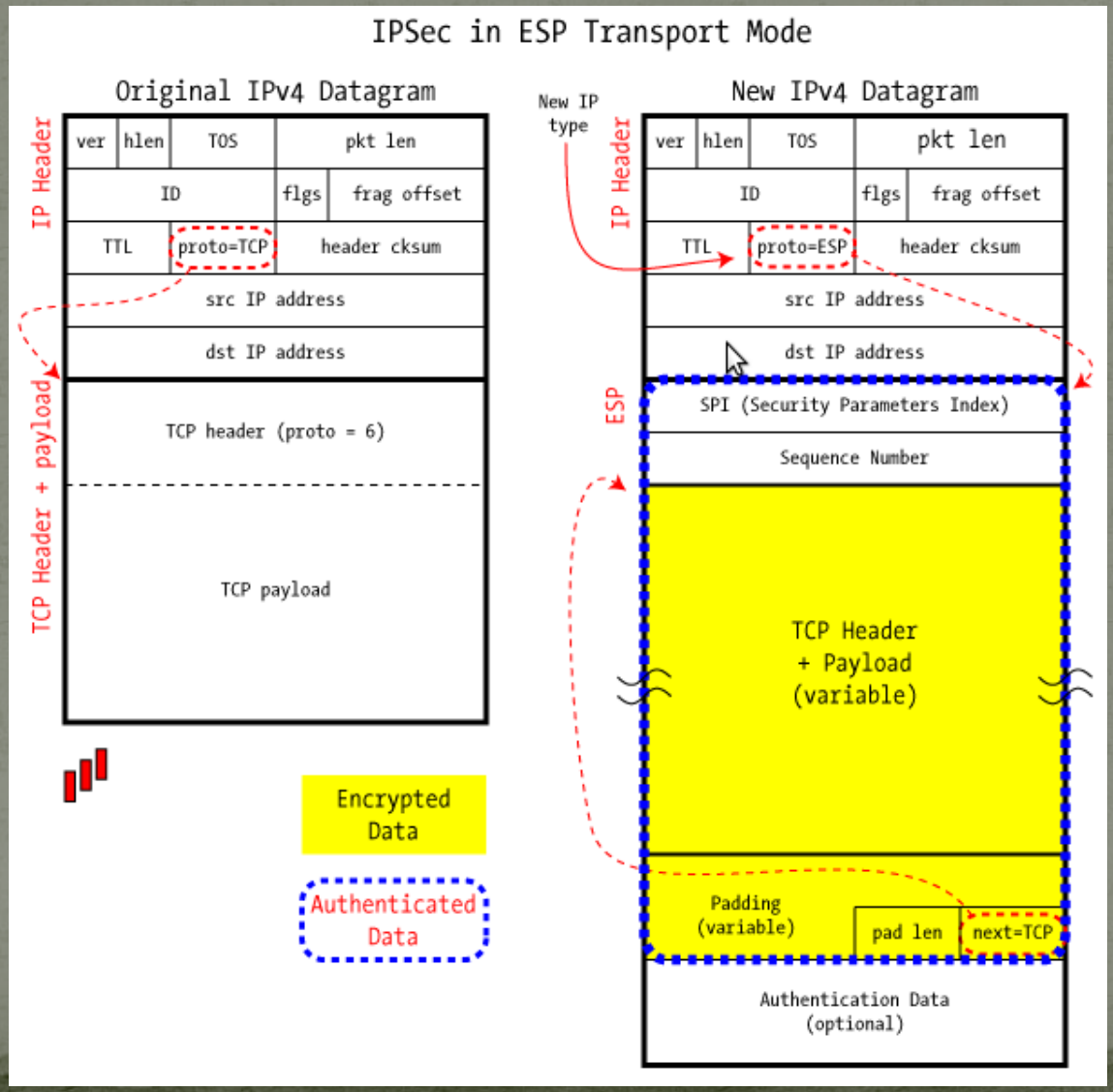
IPSec in AH Tunnel Mode



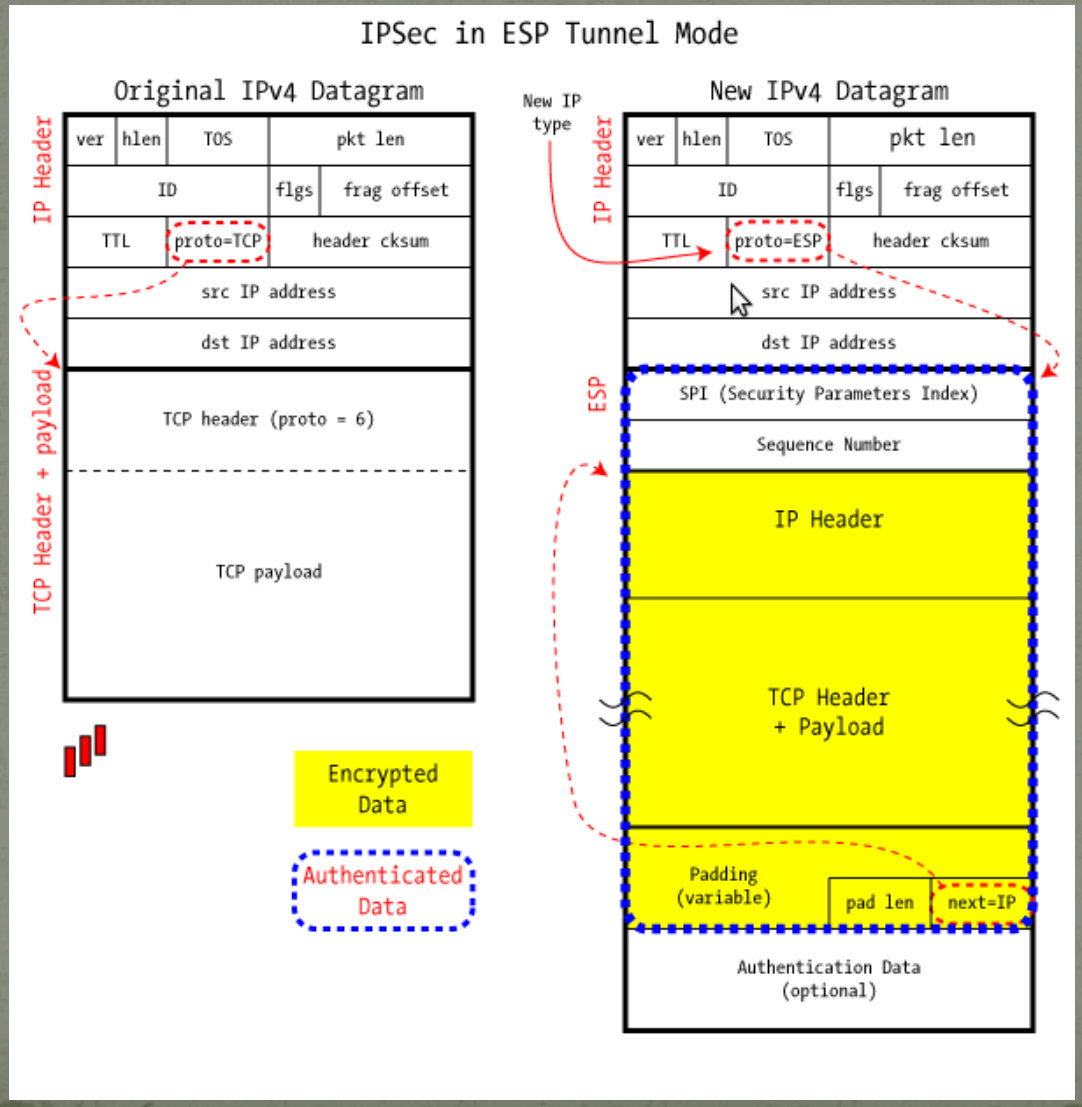
Encapsulating Security Payload



IPSec in ESP Transport Mode



IPSec in ESP Tunnel Mode



Virtual Private Network (VPN)

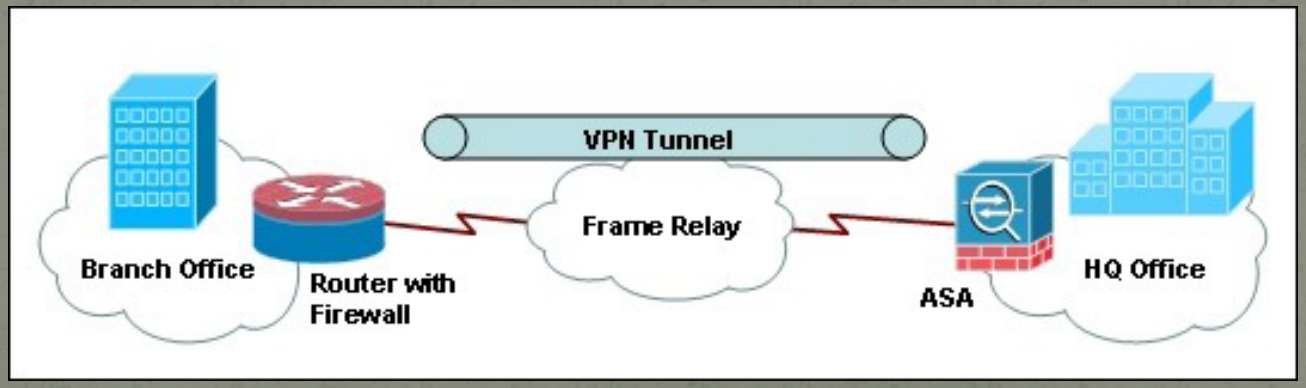
- Sanal Özel Ağ (Virtual Private Network : Uzakta yer alan bir ağdan yerel ağa erişerek bilgisayarın yerel ağdaymış gibi çalışabilmesini sağlayan bir alt yapıdır.

- VPN platforma bağlı olmayan bir yapıdır ve çeşitli yazılımsal veya donanımsal çözümler kullanılarak farklı mimariler ile oluşturulabilir.

- İnternet gibi geniş bir alana yayılmış bir ağın, kurumsal bir işletmenin çok uzaktaki ofislerinin veya trafik yoğunluğu çok fazla olmayan şubelerinin güvenli bir iletişim yapılacak biçimde internet üzerinden bağlanması sanal ağ oluşturması anlamına gelir.

Tünel

- Genel kullanıma açık olan ağ yapısını kullanıyor olması bir takım güvenlik endişeleri doğurabilir. Bu durum göz önünde bulundurularak bağlandığı nokta ile bilgisayar arasında şifreli bir tünel bağlantısı sayesinde bilgi akışının güvenliği arttırılmıştır.



VPN Örnekleri

- **Intranet VPN**
  - Farklı lokasyonlardaki ağların (örneğin bir şirketin farklı şubeleri) tek bir özel ağmış gibi birbirine bağlanması
- **Remote Access VPN**
  - Bir hostun uzak bir ağa (örneğin bir çalışan kendi şirket ağına) sanki ağın içindeymiş gibi bağlanması
- **Extranet VPN**
  - Birbirleri ile ortak bir ağ oluşturmak isteyen farklı iki ağın (örneğin bir iş üzerinde birlikte çalışan iki şirket) bazı kurallar ile yeni ağ oluşturmaları

VPN

Avantajları

- VPN'nin Avantajları
  - Maliyet
  - Esneklik
  - Mobility (hareketlilik)

Dezavantajları

- VPN'nin Dezavantajları
  - Mevcut bandwidth ten daha az trafik
  - Performans
  - Güvenlik (Lan ile kıyaslandığında)

Güvenlik Açısından VPN Çeşitleri

- Trusted VPN
- Secure VPN
- Hybrid VPN

Trusted VPN

- İlk çıkan VPN çeşididir.
- Servis sağlayıcılardan bir veya daha fazla devre (circuit) kiralanıp kuruluyor. Müşteri bu devreyi fiziksel bir kabloymuş gibi kullanıyor.
- Güvenli DEĞİL!

Secure VPN

- Trusted VPN'ler güvenliği sağlayamadığı için geliştirildi.
- Paketler kaynak bilgisayarda veya ağ geçidinde şifreleme yapılarak gönderilir.
- Güvenli

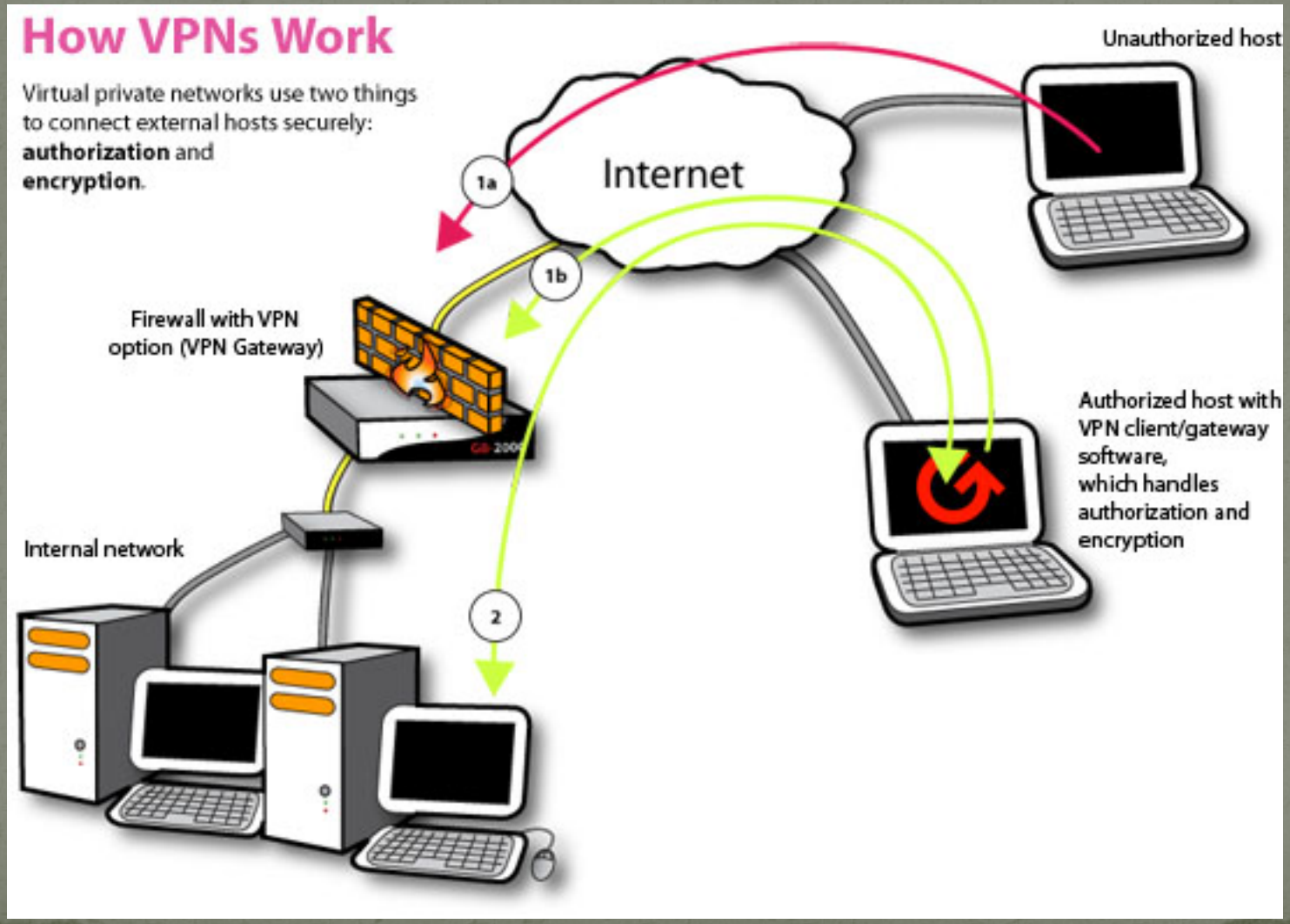
Hybrid VPN

- Bu tarz VPN'ler Trusted VPN'lerin sağladığı özellikler ile birlikte güvenliğin de istenmesi sonucunda ortaya çıkmıştır.
- Secured VPN, Trusted VPN nin bir parçası olarak çalışır.
- Yarı Güvenli

VPN güvenliği bu özellikler ile sağlanır.

- Kimlik Denetimi
- Şifreleme
- Paket Filtreleme
- Güvenlik Duvarı
- Yetkilendirme

VPN Güvenliği



VPN Güvenliği

- Authentication
  - Kimlik denetimi uzaktan erişim söz konusu olduğunda en önemli fonksiyondur. Güçlü bir kişilik belirleme olmaksızın ağ'a girişin kontrol altına alınması olanaksızdır ve bunun sonucu kurumsal bilgilerin yetkilendirilmemiş kişilerin eline geçmesi çok kolay olacaktır.
- Encryption
  - Güçlü şifreleme yöntemleri kullanılmalıdır.
  - Genel olarak VPN bağlantıları için şifreleme işlemleri istemci ve VPN server arasında sağlanır.

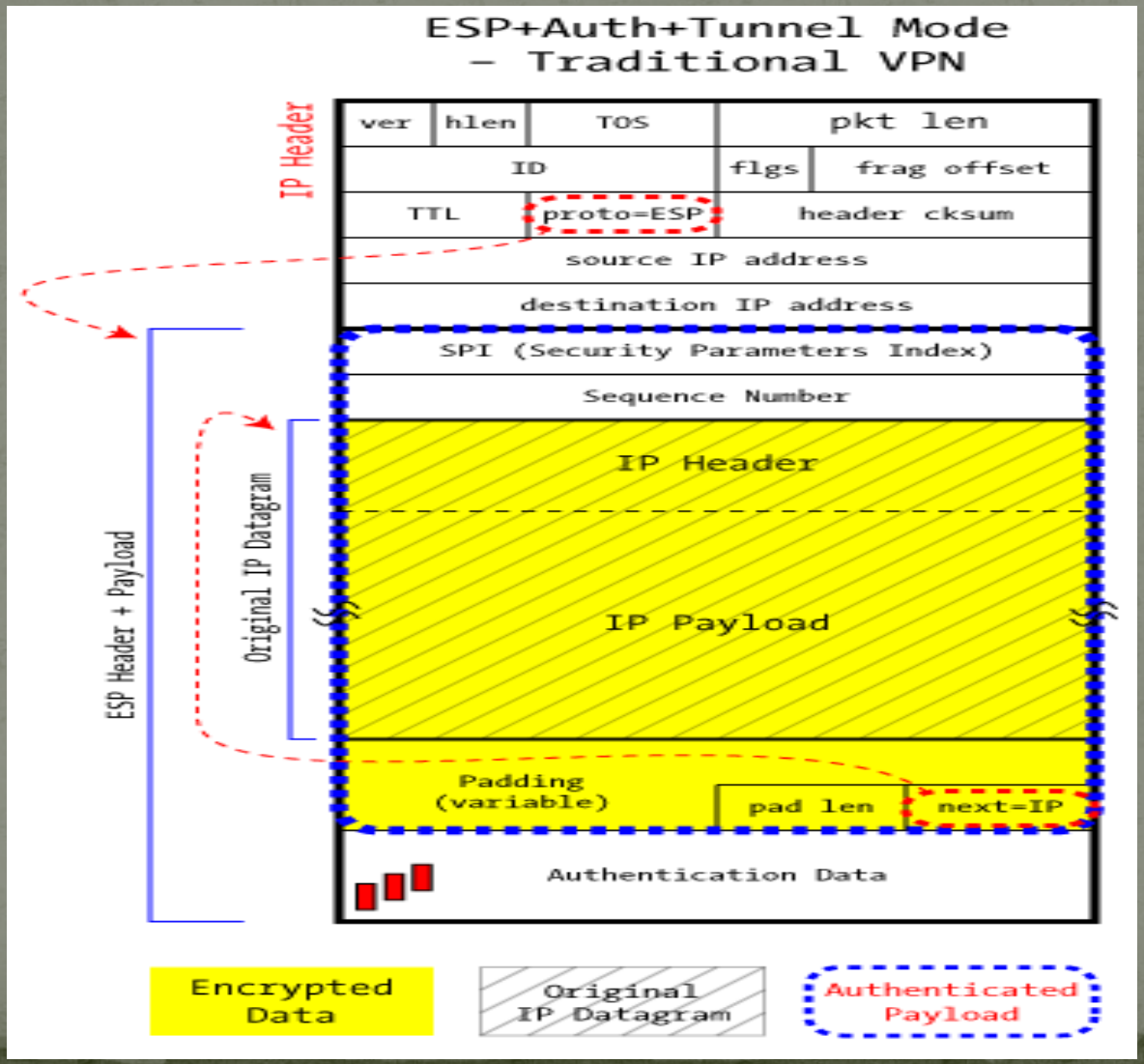
VPN Güvenliği

- Güvenlik Duvarı
  - Özel ağ ve internet arasında güçlü bir duvar oluşturur. Hangi türde paketlerin geçtiğine, hangi protokollerin izinli olduğuna ve açık portların sayısına göre firewall ayarlanabilir.
- Paket Filtreleme
  - Güvenliği artırmak için paket filtreleme kullanılmalıdır.
- Yetkilendirme
  - Kullanıcıların yetkileri tam ve açık bir şekilde belirlenmelidir. Kişilik belirleme ile yetkilendirmenin sınırı her zaman kesin çizgilerle belli değildir, genellikle kişilik belirleme işlemini izleyerek uygulanır.

IPSec ile VPN Güvenliği

- Güvenli bir VPN oluşturmak için en çok kullanılan protokoldür.
- En iyi şifreleme algoritmaları ve çok kapsamlı kimlik sorgulama gibi güvenlik özelliklerini sunar.

Traditional VPN
IPSec with ESP Tunnel Mode



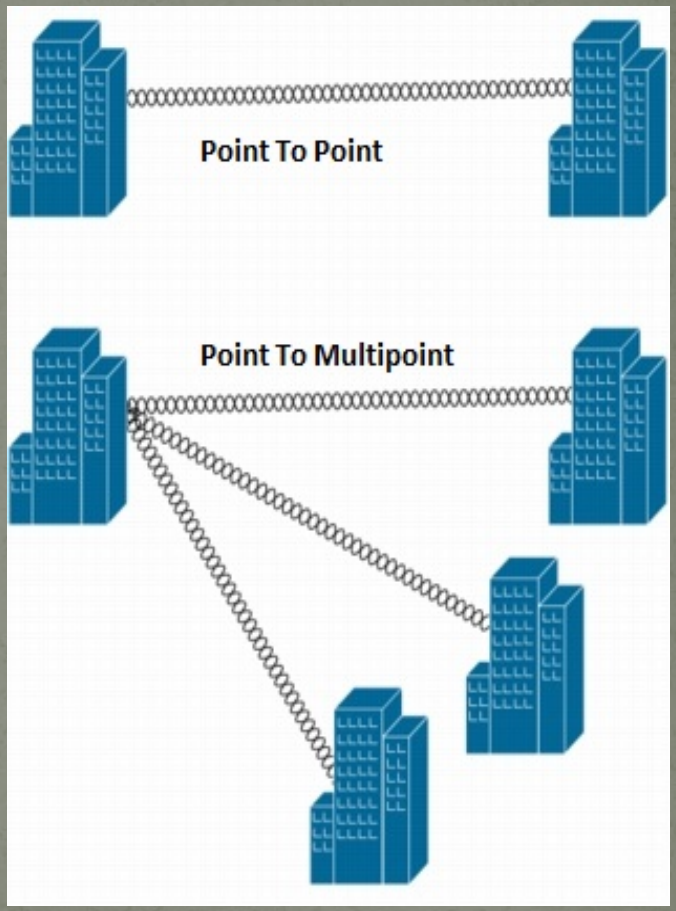
Data Link Layer

Üç tane protokol tanımlanabilir.

- Point to Point Protocol(PPP-Noktadan Noktaya Protokolü),
- RADİUS Protokolü,
- TACACS+ Protokolü.

Point to Point Protocol

- Noktadan noktaya protokolü kısaca, veri alışverişi yapmak isteyen iki noktanın birbiriyle telefon hattı gibi bir hat üzerinden çift yönlü olarak bağlanmasıdır.
- RFC 1661 ve RFC 1134'te tanımlanmıştır.
- Hata düzeltme, veri sıkıştırma, kimlik denetimi, adresleme gibi özelliklere sahiptir.
- Senkron hatlar üzerinde çalışabilir



PPP'nin Çalışma Mekanizması

PPP protokolün çalışma mekanizmasını üç ana protokol oluşturur, bunlar;

- Kapsülleme(Encapsulation),
- Bağlantı Kontrol Protokolü(Link Control Protocol),
- Ağ Kontrol Protokolü(Network Control Protocol).

PPP'nin Çalışma Mekanizması

Kapsülleme

- Bütün ağ bağlantılarında verinin iletiminden önce 'enkapsüle' edilerek frame(çerçeve) haline getirilmelidir.
- PPP'nin kapsülleme özelliği sayesinde farklı ağ katmanı protokolleri aynı bağlantıda çalışabilir.
- Temel Kapsülleme metodu HDLC'dir(Yüksek seviyede veri bağlantı protokolü).

PPP'nin Çalışma Mekanizması

HDLC Enkapsülasyonu

- Hatasız iletişimin sağlanması için eş zamanlı seri iletim kullanır.
- Hata ve akış kontrolü için veri bağlantı katmanına özgü bir çerçeve tanımlar.
- Standart HDLC de birden fazla protokol desteği verilmemiştir. Sorunun çözümü için Cisco tarafından Cisco HDLC geliştirilmiştir.

PPP'nin Çalışma Mekanizması

- Bayrak Alanı: Çerçeve başı ve sonunu işaret eder.
- Adres Alanı: Gidilecek bir sonraki hedefin adresini tutar.
- Kontrol Alanı: Üç farklı biçimde olabilir (bilgi çerçevesi; üst katman bilgisi taşır, denetleyici çerçeve; kontrol bilgisi ile iletim başlama-bitiş talebi bilgisi taşır, numarasız çerçeve; kontrol bilgisi taşır).
- Veri Alanı: Yol bilgi birimi(Path information) veya değişim kimlik taraması(Exchange identification) bilgileri bulunur.
- Frame Kontrol Dizisi : Döngüsel fazlalık testi(cyclic redundancy check) hesaplamasından arta kalan kısımdır.
- Protokol Alanı: Çerçeve ile birlikte enkapsüle edilen protokol bilgisi belirtilir.

PPP Yapılanması

- Point to point protoklü tarafından yapılan işin büyük kısmı bağlantı kontrol protokolü(Link kontrol protocol LCP) ve ağ kontrol protokolünde(Network control protocol NCP) yapılır.
- LCP(bağlantı kontrol protokolü), PPP bağlantı kısmı ile ilgilenir.
- NCP(ağ kontrol protokol) ise üst katman protokolleri ile ilgili yapılandırmanın yapılması ile ilgilenir.

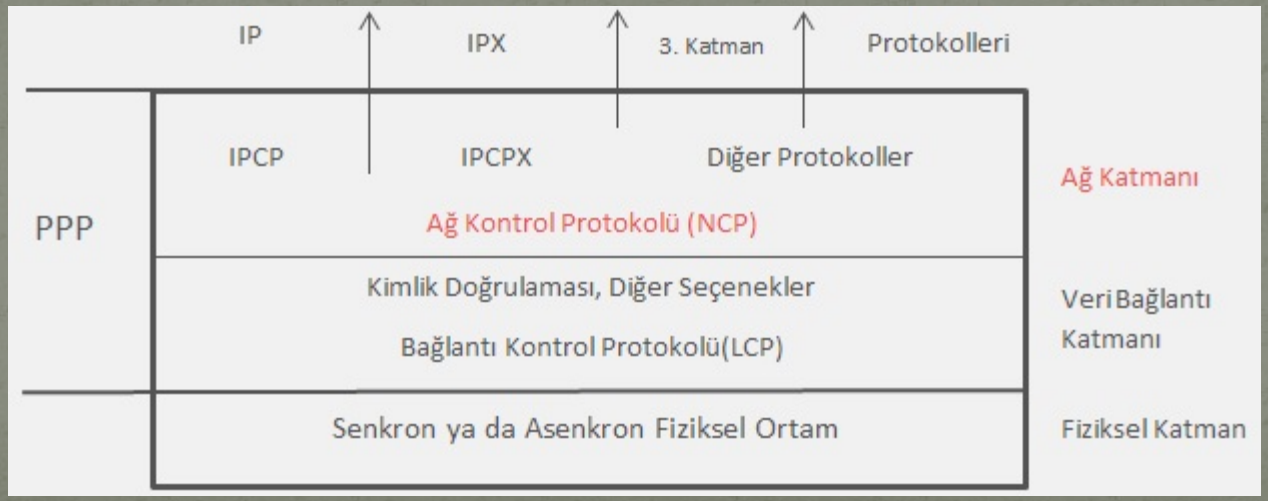
Bağlantı Kontrol Protokolü(LCP)

Başlıca görevleri;

- PPP'ni asıl çalışan kısmı, bağlantı kurulması, yapılandırılması, test edilmesi, parametrelerinin ayarlanması ve bağlantının kapanmasından sorumludur.
- Paket boyutu üzerindeki limitleri düzenler,
- Yapılandırma hatalarını tespit eder,
- Bağlantının hatalı çalışıp çalışmadığını test eder.

Ağ Kontrol Protokolü(NCP)

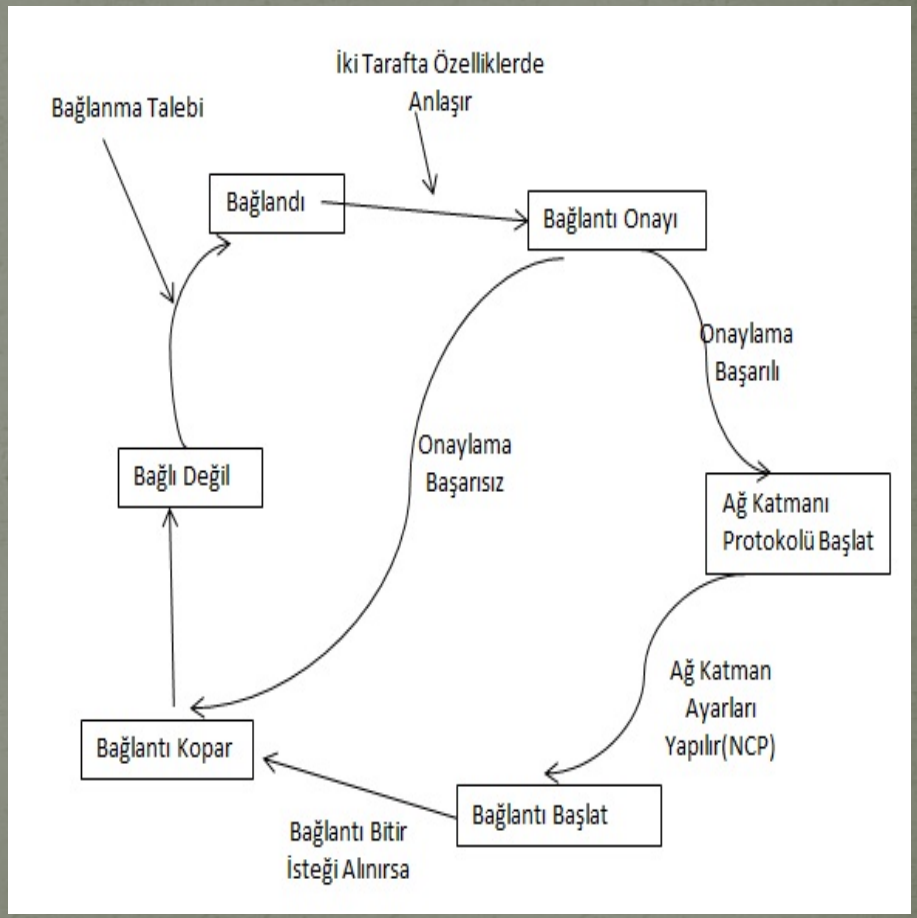
- Noktadan noktaya protokolü(PPP) ağ protokolleri ile olan problemleri daha da kötüleştirebilir.(IP adreslerinin atanması ve yönetimi gibi problemler noktadan noktaya bağlantılarda içinden çıkılmaz hale gelebilir). PPP bu kötüleşmeyi önlemek için NCP kullanır.
- PPP aynı bağlantıda birden fazla ağ katmanı protokolüne izin verirken, her protokol için ayrı bir NCP kullanır.(IP için IPCP, IPX için IPXCP kullanır).



PPP Bağlantısının Şematik Gösterimi

PP kurulurken gerçekleşen adımlar:

- Bağlı olmama durumu, bağlantının kopması ya da taraflardan birinin bağlantıdan ayrılması.
- Bağlantı kurulumu, LCP 'nin bağlantı kurduğu aşama, bağlantı onayına göre ya doğrudan NCP ayarları adımına ya da bağlantı onay kısmına geçilir.
- Bağlantı onayı, aktif ise tarafların kimlik doğrulamasından geçip geçmediğinin sınandığı durum,
- Bağlantının sonlandırılması, taraflardan birinin bağlantıyı bitirme isteği ya da kimlik doğrulama hatası alındığında gelinebilecek durumdur.



PPP Güvenlik Doğrulaması

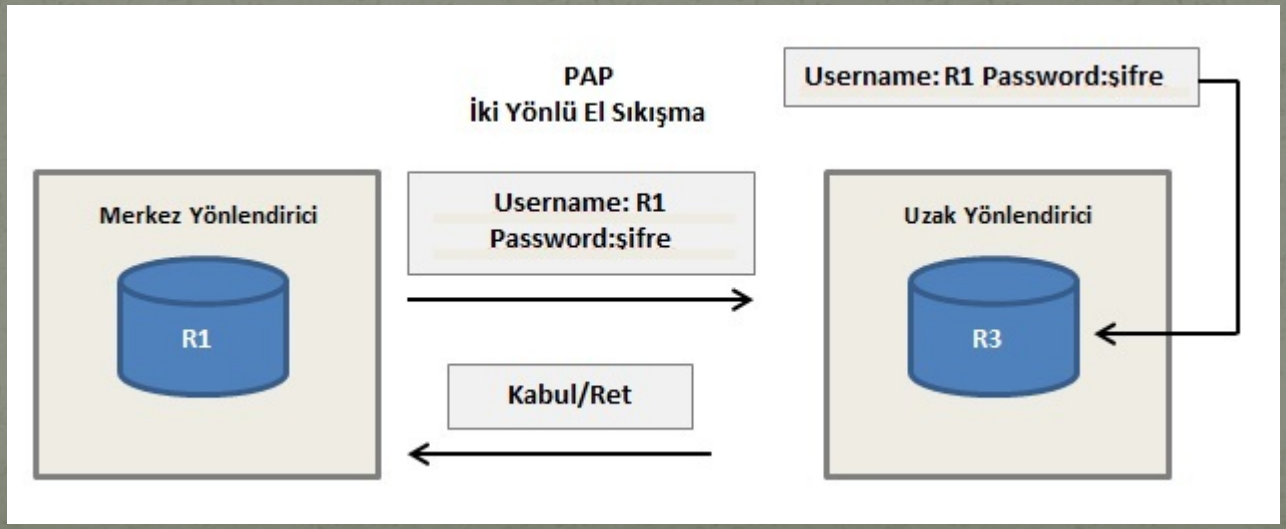
- Diğer katmanlarda uygulanan güvenlik protokollerine ek olarak 2 protokol daha uygular;

1. PAP (Password Authentication Protocol- şifre doğrulama protokolü)
2. CHAP(Challenge Handshake Authentication Protocol-Karşılıklı kimlik doğrulama protokolü)

PPP Güvenlik Doğrulaması

PAP(şifre doğrulama protokolü)

- 2 yönlü el sıkışma yönetimiyle kimlik denetimi yapar,
- Kimlik denetimini açık şekilde yapar

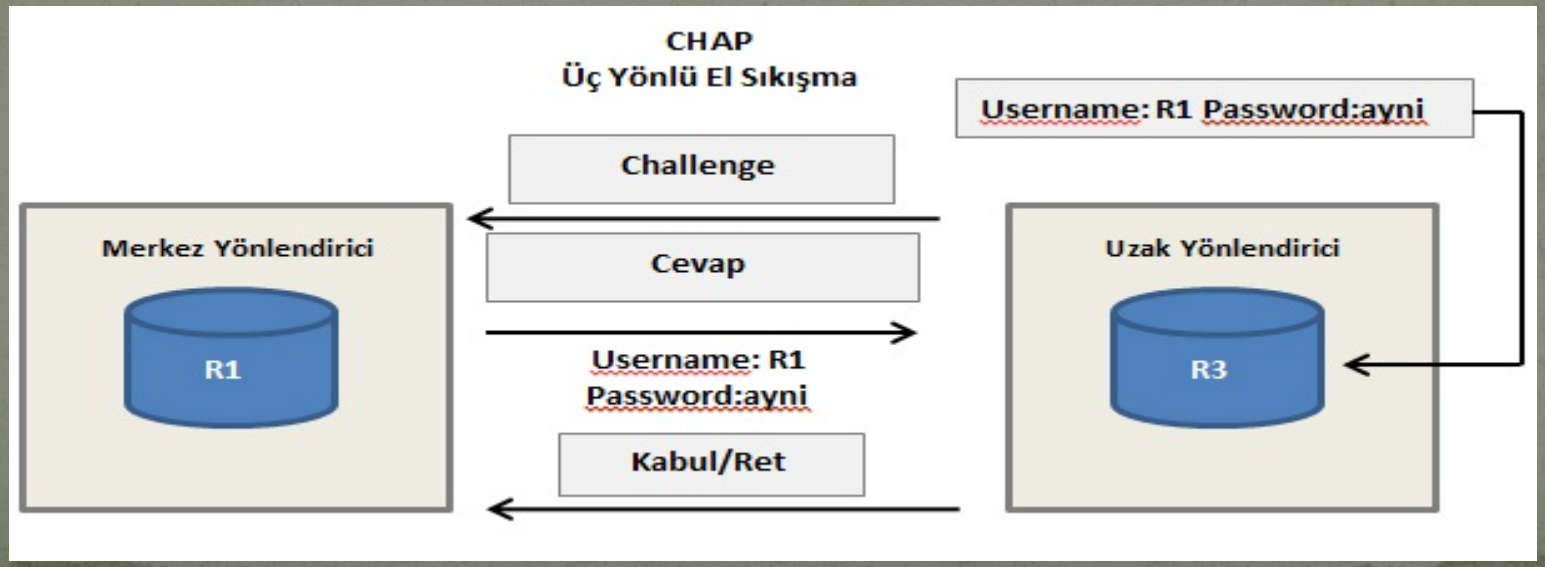


PPP güvenlik Doğrulaması

CHAP(karşılıklı kimlik doğrulama protokolü)

-PAP'tan farklı olarak 3 yönlü el sıkışması protokolü kullanır,

1. R3 üçlü el sıkışmayı başlatır R1 e davet(challenge) isimli rastlantısal bir değer gönderir.
2. 2)R1 kullanıcı adi, şifre ve davet değerinin MD5 e sokulmuş halini R3'e gönderir,
3. 3) R3 veri tabanından kullanıcı adi, şifre ve davet değerini MD5'e tabi tuttuğu elde ettiği değerle R1'den geleni karşılaştırır kabul ya da ret eder.



PPP güvenlik Doğrulaması

PAP(şifre doğrulama protokolü)	CHAP(karşılıklı kimlik doğrulama protokolü)
2 yönlü el sıkışma var,	3 yönlü el sıkışma var,
Kullanıcı adı ve şifre açık olarak gönderilir,	Kullanıcı adı ve şifre MD5 ile şifrelenip gönderilir,
Bağlantı kurulduktan sonra kimlik denetimi yapılmaz,	Kimlik denetimi belirli aralıklarla tekrar edilir,
İki tarafta kullanılan şifreler aynı olmak zorunda değildir.	Şifrelerin aynı olması gerekir.

PPP Kullanıldığı Yerler

- Telefon haberleşmesi, fiber optik haberleşme
- Radyo iletişim ortamı, cep telefonu haberleşmesi,
- Mesajlaşma , dosya paylaşım programlarında,
- ADSL öncesi Dial-Up bağlantılarda,
- Adsl hatları üzerinde geliştirilen PPPoE(Ethernet üzerinden noktadan noktaya erişim protokolü) ve PPPoA(ATM üzerinden noktadan noktaya iletişim protokolü).

RADİUS

- RADİUS RFC 2865,2866ve 2138 ‘te tanımlanmıştır
- RADİUS(***R**emote **A**uthentication **D**ial-**i**n **U**ser **S**ervice*) bir AAA(authentication, accounting, authorization) protokolüdür.
- RADİUS, uzaktan bağlanan kullanıcılar için kullanıcı isim-şifre doğrulama (authentication), hesap yönetimi/erişim süresi (accounting) ve yetkilendirme (authorization) işlemlerini yapan servisler olarak tanımlanabilir.
- RADİUS kimlik doğrulama ve hesap oluşturma için gönderilen iletileri UDP ile gönderilir.

RADİUS

- Accounting(hesap yönetimi):Kullanıcı erişim saatleri, yaptıkları işleri kısaca **kullanıcı aktivitelerinin izlenmesi işidir.**
- Authorization(yetkilendirme): Kullanıcıların sistemdeki **yetkilerinin belirlenme işidir.**
- Authentication(kullanıcı doğrulama): Sisteme erişmek isteyen kişinin kullanıcı adı ve şifresi ile sistemde olup olmadığına bakılıp onay durumuna göre **sisteme giriş izni verilmesi işidir.**

RADİUS

RADİUS İleti Türleri

- Erişim isteği: İstemci tarafından bağlantı girişimi için gönderilir,
- Erişim onayı: İstemciden gelen erişim isteğine Radius sunucusunun onay göndermesidir.
- Erişim reddi: Erişim isteğine karşı gönderilen olumsuz onaydır.
- Erişim itirazı: Erişim isteyen kullanıcıya server tarafından gönderilir, yanıt isteyen istemciye bir itirazdır.
- Hesap oluşturma isteği: hesap oluşturma bilgileri

TACACS+

- Bolt, Beranec &Newmen(BBN), US Department of Defence(DOD) tarafından geliştirilmiş RFC 1492'de belirtilmiş bir AAA metodudur.
- TACACS, merkezi veri tabanı veya ağ işletim sisteminin kullanılarak bağlantı listelerinin bakımını sağlama fikrinden doğmuştur.
- CISCO TACACS'in güçlü bir destekçisi olmuş, sonraki sürümleri XTACACS ve TACACS+ da desteklemiştir.
- Özellikle son sürüm olan TACACS+ fonksiyonel olarak RADİUS'a çok benzemektedir.

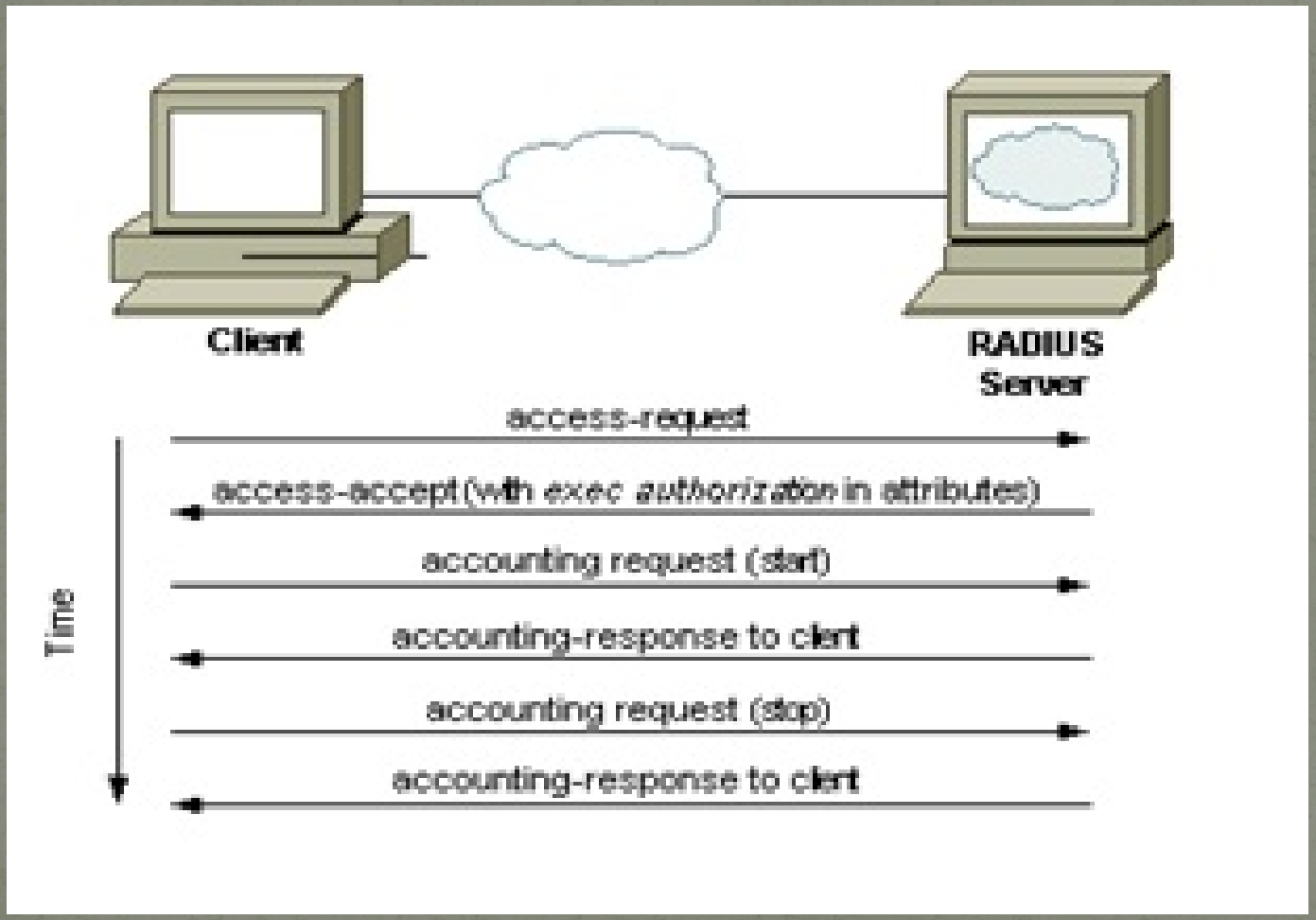
RADİUS VS TACACS+

RADIUS	TACACS+
Seçilen ağ elemanları farklı kurumlardan sağlanıyorsa seçilmelidir	TACACS+ CISCO bağımlı protokollerde kullanışlıdır
UDP dolayısıyla bağlantısız IP ilişkisi sağlar.	TCP dolayısıyla bağlantı uyumlu uygulama ile IP ilişkisi sağlanır.(daha güvenli TCP dolayısıyla)
Erişim istek paketinde sadece gönderilen şifreyi şifreler	Erişim istek paketlerinde gönderilen her şeyi şifreler
Kimlik doğrulama ve yetkilendirmeyi birleştirir (çözüme ulaşmayı zorlaştır)	Tüm AAA mimarilerini ayrık olarak sunar(kimlik doğrulama kerberos ile diğer 2 mimari TACACS+ ile gerçeklenebilir)

RADİUS VS TACACS+

RADIUS	TACACS+
Yönlendirici kontrolünü kullanıcıya vermez	Yönlendirici kontrolünü kullanıcı ya da gruba verebilir.
AppleTalk, uzaktan erişim protokolü, Netbios çerçeve kontrolü, Novell asenkron hizmet ara yüzü,, X.25 PAD gibi protokolleri desteklemez.	Sayılan protokolleri destekler.

RADİUS TRAFİK ÖRNEĞİ



TACACS+ TRAFİK ÖRNEĞİ