BSM 471-AĞ GÜVENLİĞİ

Hafta3: Kimlik Doğrulama, Yetkilendirme ve Hesap Yönetimi
(Authentication) (Authorization) (Accounting)

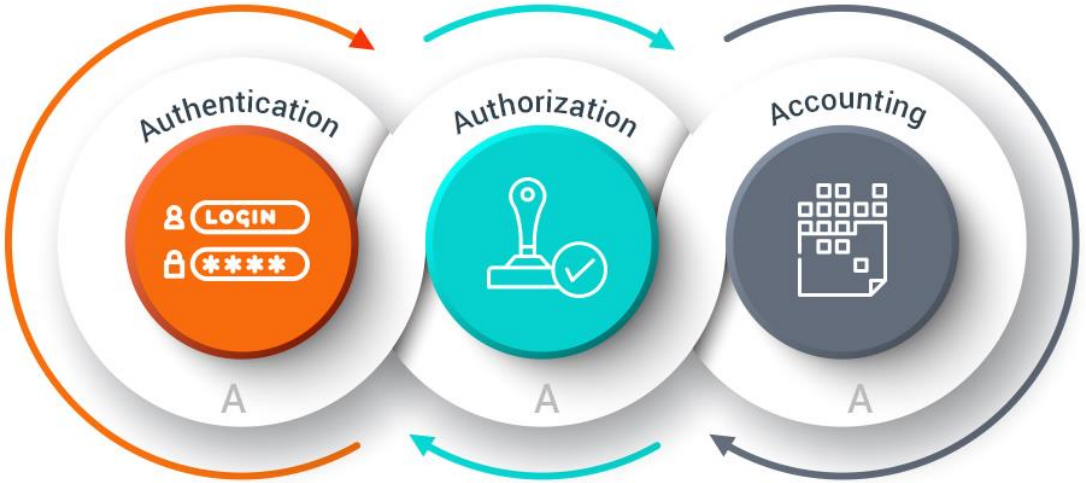
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

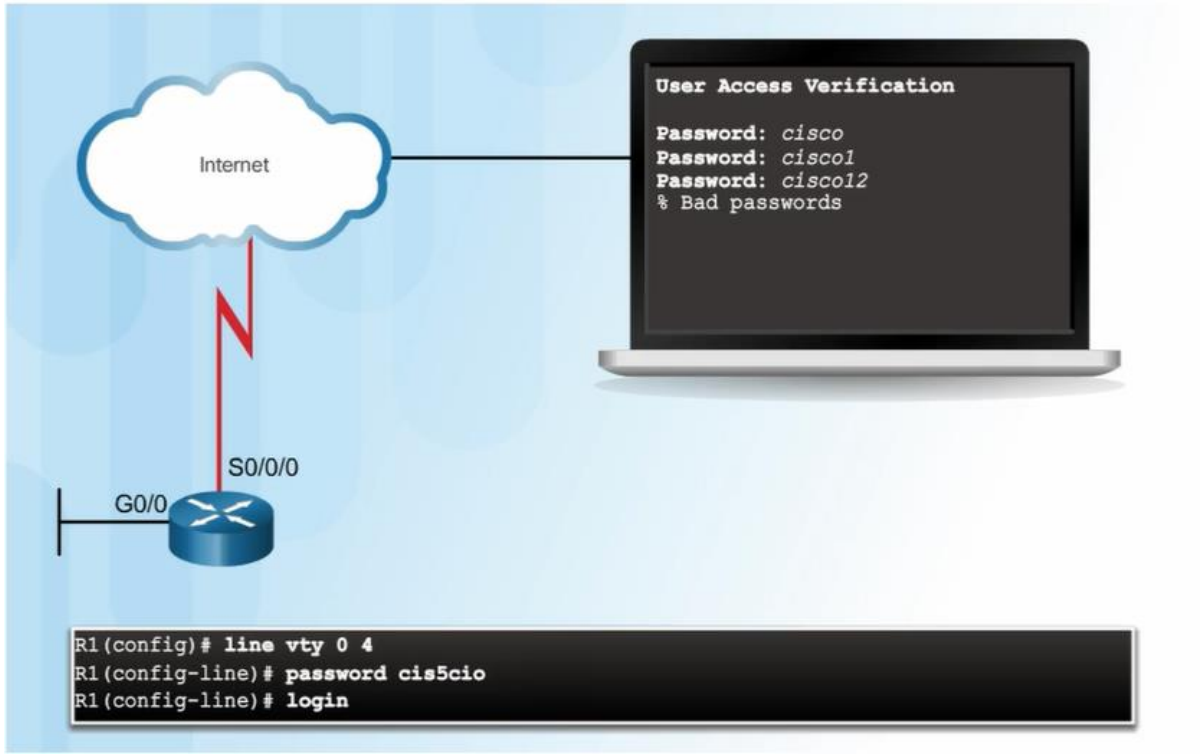
- Kimlik Doğrulama, Yetkilendirme ve Hesap Yönetimine Giriş
- Yerel AAA Doğrulama
- Sunucu Bazlı Doğrulama
- TACAS+ ve RADIUS Protokolleri
- Sunucu Bazlı Yetkilendirme
- Sunucu Bazlı Hesap Yönetimi
- 802.1x Kimlik Tabanlı Ağ Güvenliği

AAA Giriş

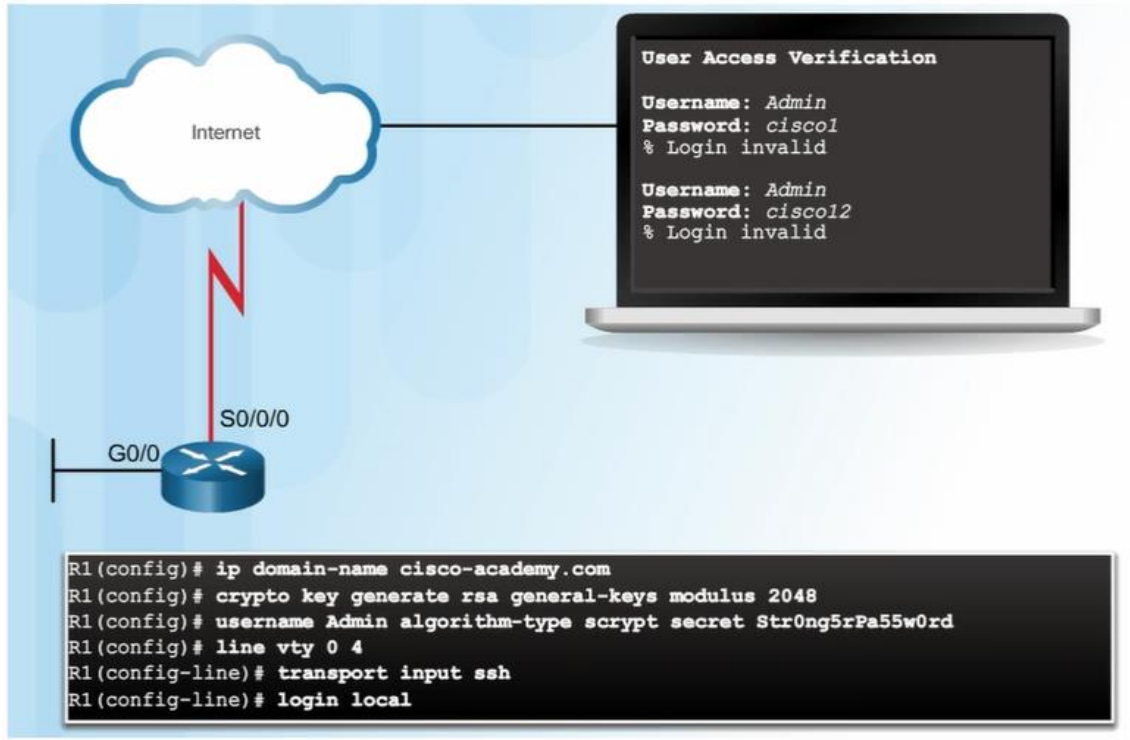
- ***Authentication;*** kullanıcının sisteme bağlanabilmesi için gerekli olan ilk adımdır. 2 aşaması mevcuttur:
  - Yerel AAA Doğrulaması
  - Sunucu-Tabanlı AAA Doğrulaması
- ***Authorization***; Kullanıcı adı ve şifre doğrulaması sağlanan kullanıcıların sisteme, programa veya ağa hangi yetkilerle erişim hakkına sahip olduklarını belirten sisteme denir.
- ***Accounting;*** Bir sorun ile karşılaşıldığında sorunun tespitinin sağlanabilmesi için kullanılan sisteme denir.



AAA Olmadan Doğrulama

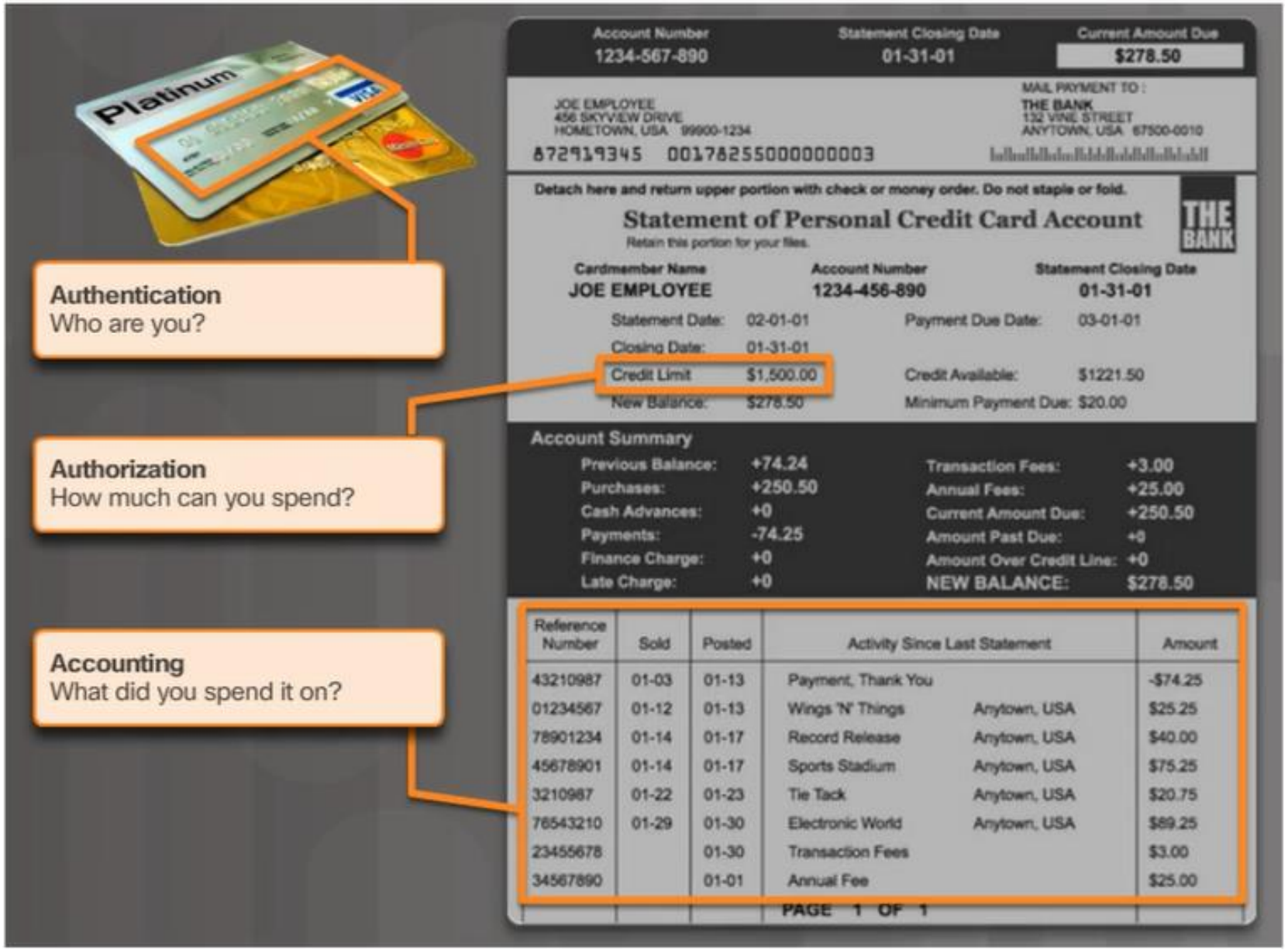


Telnet Bağlantısı



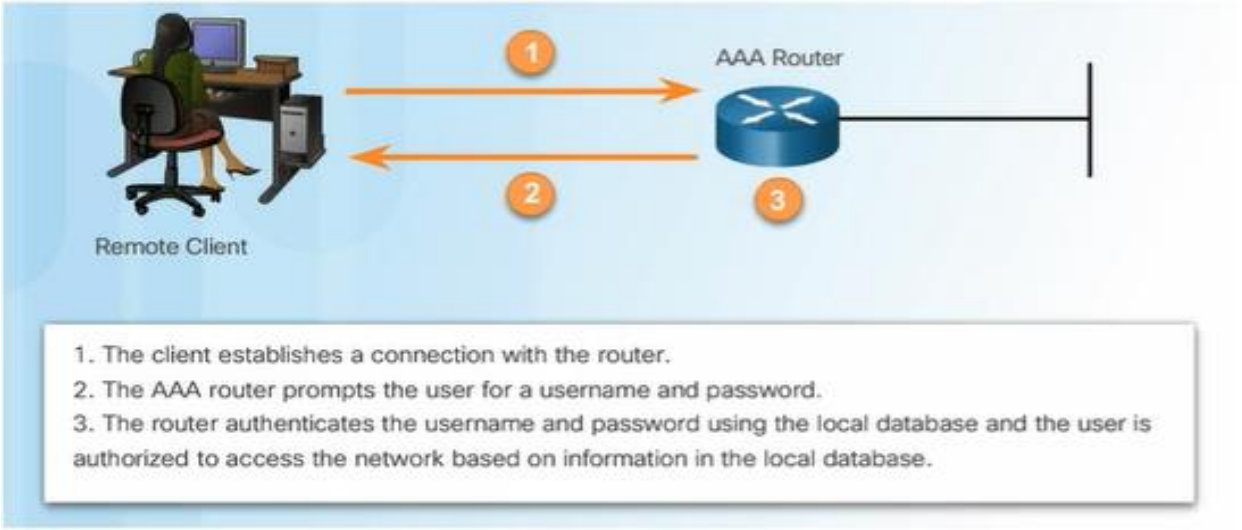
SSH ve Yerel Veritabanı Bağlantısı

AAA Bileşenleri

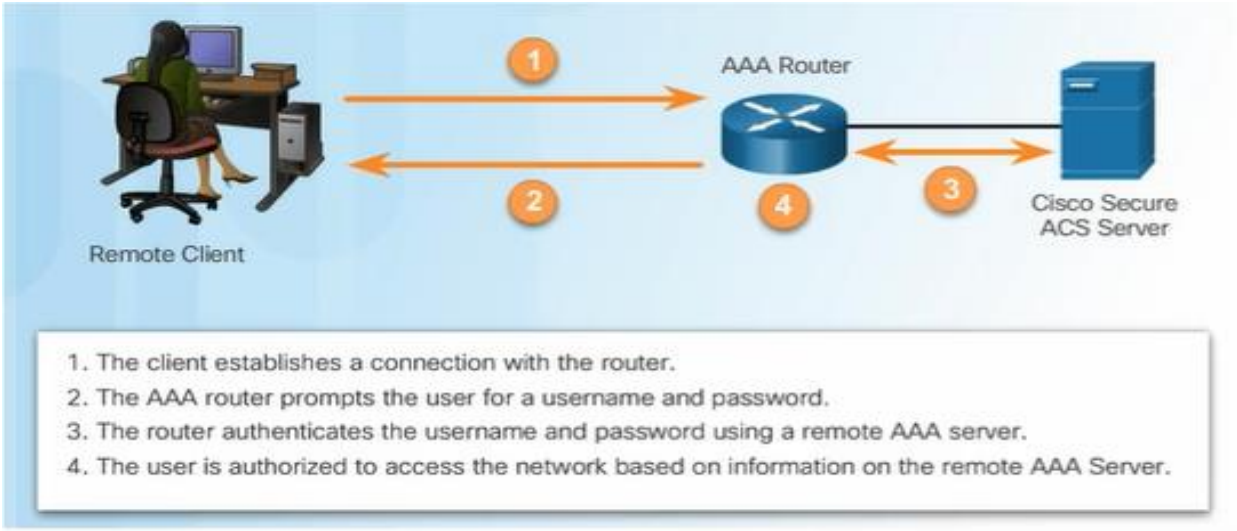


AAA-Kimlik Doğrulama Metotları

Yerel AAA Doğrulaması

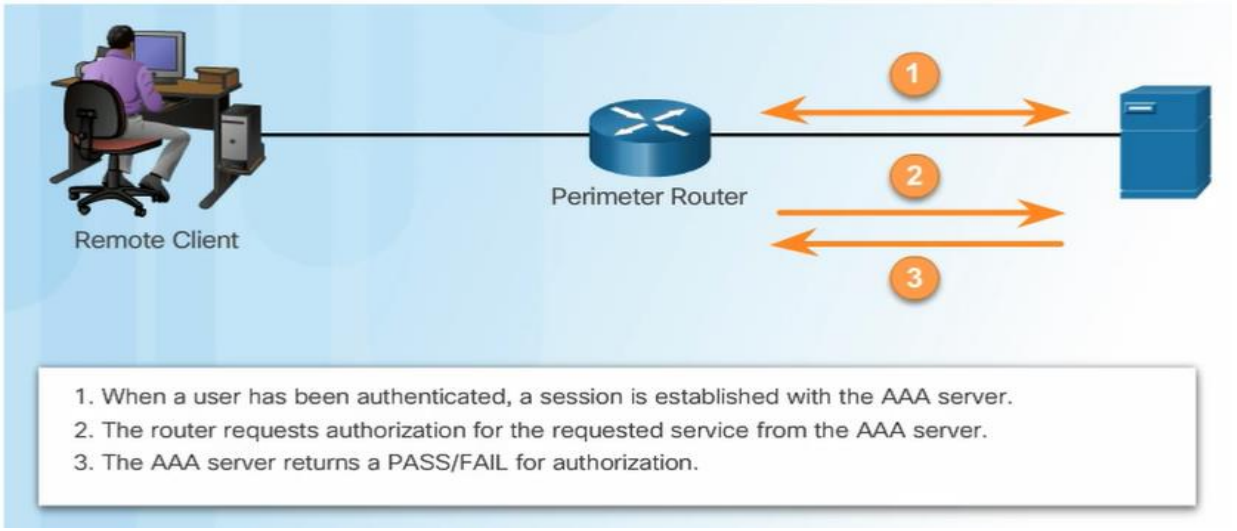


Sunucu-Tabanlı AAA Doğrulaması

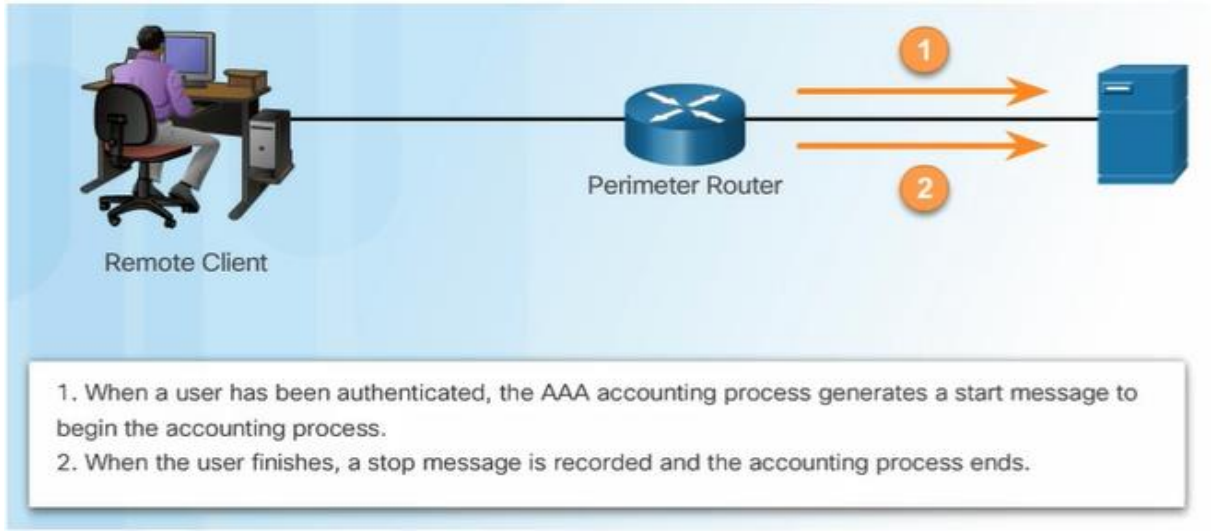


AAA-Yetkilendirme ve Hesap Yönetimi Metotları

Yetkilendirme



Hesap Yönetimi



Yerel AAA Kimlik Doğrulaması Yapılandırması (CLI ile)

Yönetici Erişiminin Doğrulanması;

1. Yönlendiriciye yönetici erişimine ihtiyaç duyan kullanıcılar için yerel yönlendirici veritabanına kullanıcı adları ve parolalar ekleyin
2. Yönlendiricide küresel olarak AAA'yı etkinleştirin.
3. Yönlendiricide AAA parametrelerini yapılandırın.
4. AAA yapılandırmasını onaylayın ve sorunları giderin.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)#
```

Yerel AAA Kimlik Doğrulaması Yapılandırması (CLI ile) - devam

Doğrulama Methodları:

Method Type Keywords	Description
`enable`	Uses the enable password for authentication.
`local`	Uses the local username database for authentication.
`local-case`	Uses case-sensitive local username authentication.
`none`	Uses no authentication.
`group radius`	Uses the list of all RADIUS servers for authentication.
`group tacacs+`	Uses the list of all TACACS+ servers for authentication.
`group` *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the `aaa group server radius` or `aaa group server tacacs+` command.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```

```
router(config-line)#
aaa authentication login {default | list-name} method1…[method4]
```

Command	Description
`default`	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1...[method4]	Identifies the list of methods that the AAA authentication process will query in the given sequence. At least one method must be specified. A maximum of four methods may be specified.

Yerel AAA Kimlik Doğrulaması Detaylı Yapılandırma

Command Syntax

```
Router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Command	Description
number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts before a connection is dropped and the user account is locked.

Display Locked Out Users

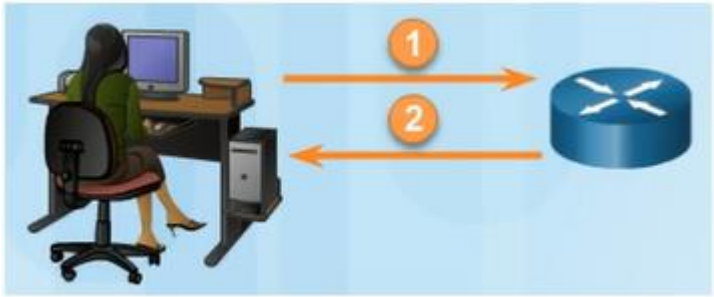
```
R1# show aaa local user lockout
              Local-user          Lock time
              JR-ADMIN            04:28:49 UTC Sat Dec 27 2015
```

Show Unique ID of a Session

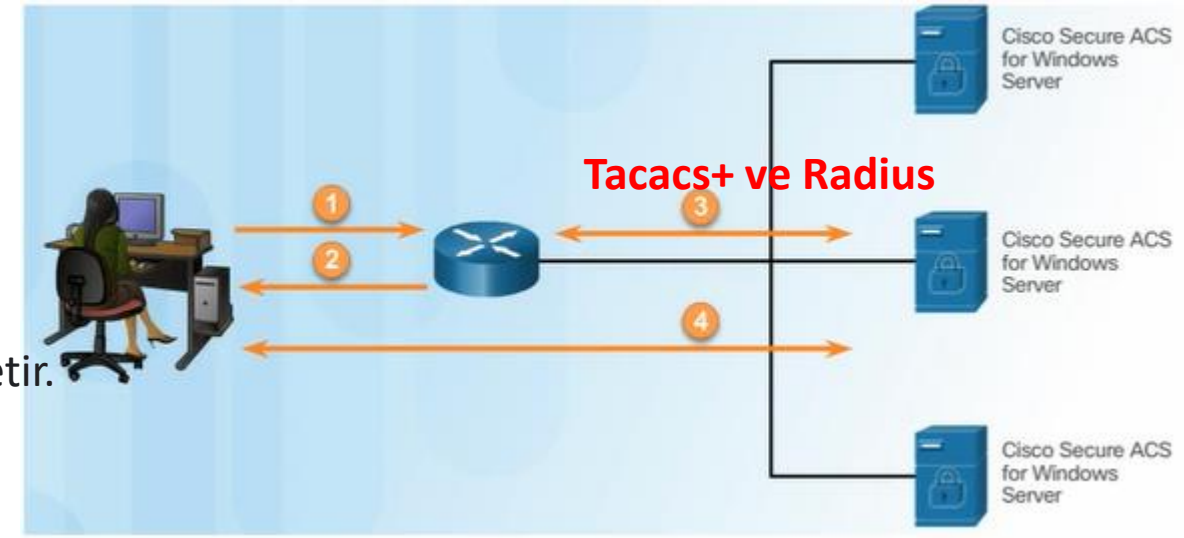
```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
    Unique Id: 175
    User Name: ADMIN
    IP Address: 192.168.1.10
    Idle Time: 0
    CT Call Handle: 0
```

Sunucu Tabanlı Kimlik Doğrulama

- ***Yerel Doğrulama;***
- Kullanıcı yönlendirici ile bağlantı kurar.
- Yönlendirici, kullanıcıdan bir kullanıcı adı ve parola ister, yerel bir veritabanı kullanarak kullanıcıyı doğrular.



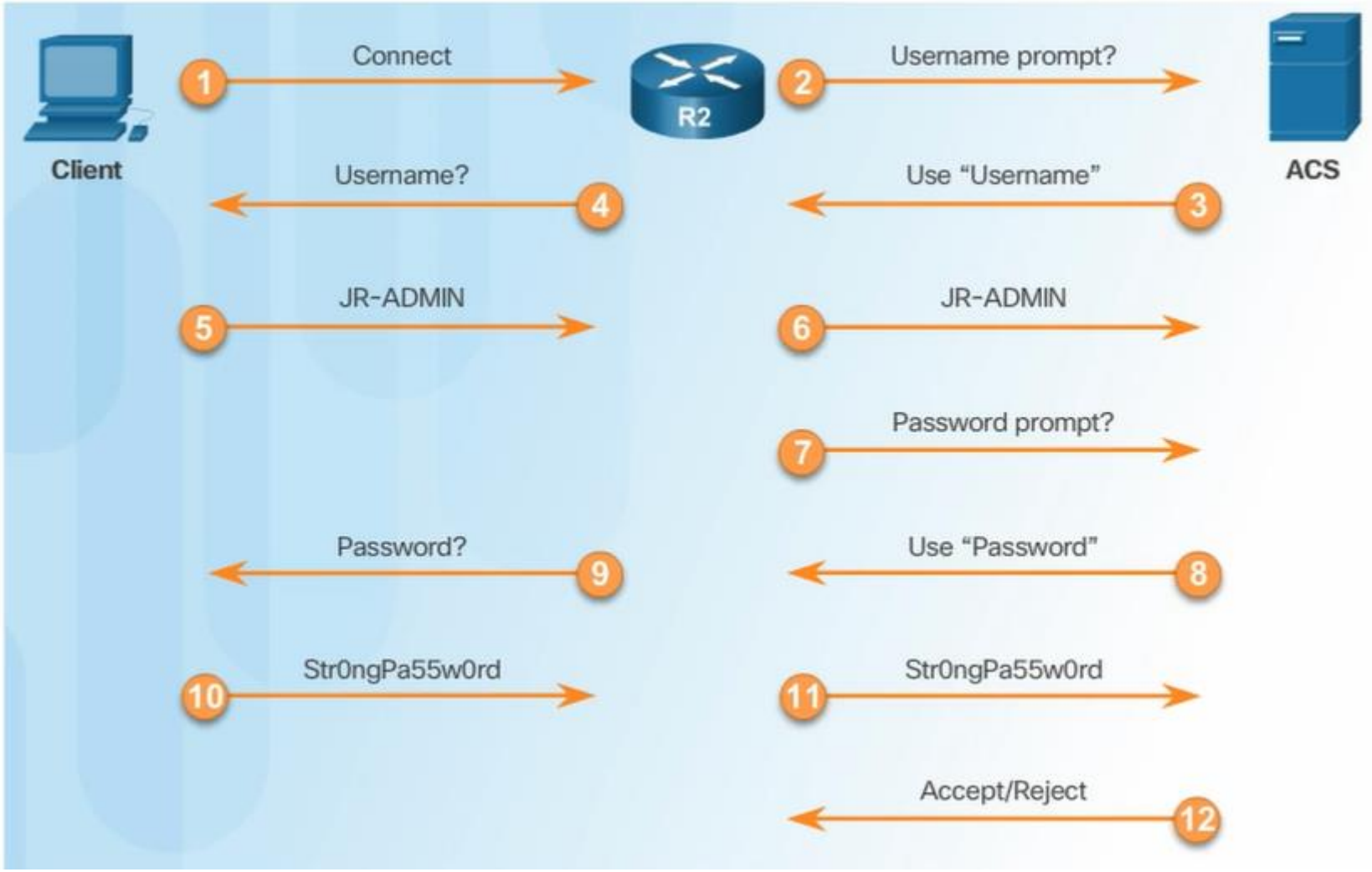
- ***Sunucu-Tabanlı Doğrulama;***
- Kullanıcı yönlendirici ile bağlantı kurar.
- Yönlendirici, kullanıcıdan bir kullanıcı adı ve parola ister.
- Yönlendirici, kullanıcı adını ve şifreyi Cisco Secure ACS'ye iletir.
- Cisco Secure ACS, kullanıcının kimliğini doğrular.



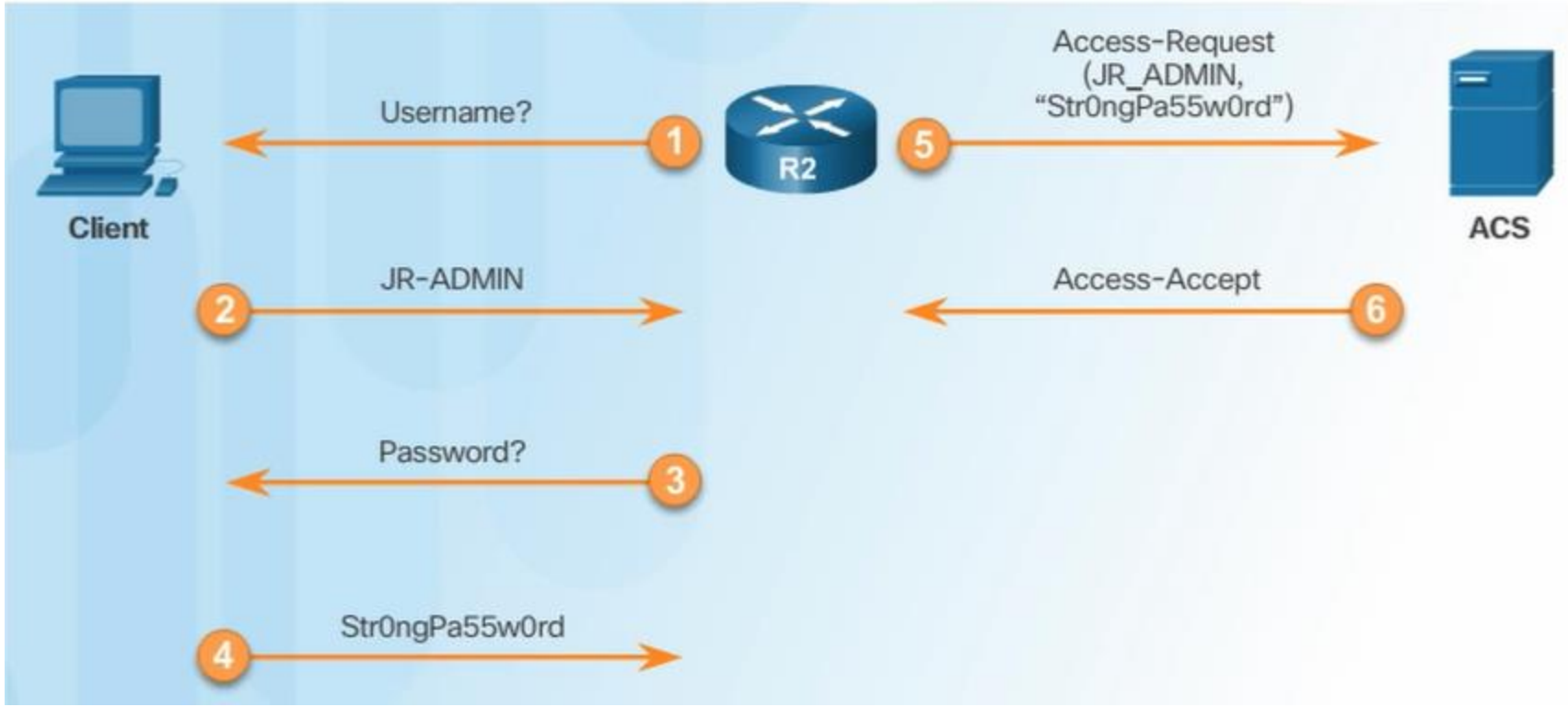
TACACS+ ve RADIUS Protokolleri

	TACACS	RADIUS
İşlevsellik	AAA mimarisi kendi içerisinde ayırır, güvenlik sunucu entegresine izin verir.	Kullanıcı doğrulama ve yetkilendirmeyi birleştirir ama hesap yönetimini ayırır, TACACS'a göre kısıtlı esneklik
Standart	Genellikle Cisco Destekli	Açık kaynak/RFC standart
Taşıma Katmanı Protokolü	TCP	UDP
CHAP	Çift yönlü iletişim	Tek yönlü iletişim
Protokol desteği	Birçok protokol desteği var	Birçok protokol desteği var
Gizlilik	Tüm paket şifreli	Parola şifreli
Özelleştirme	Her kullanıcı ve her grup için yönlendirici yetkilendirme sağlar.	Böyle bir opsiyon yok.
Hesap Yönetimi	Kısıtlı	Geniş

TACACS+ Doğrulama Methodu



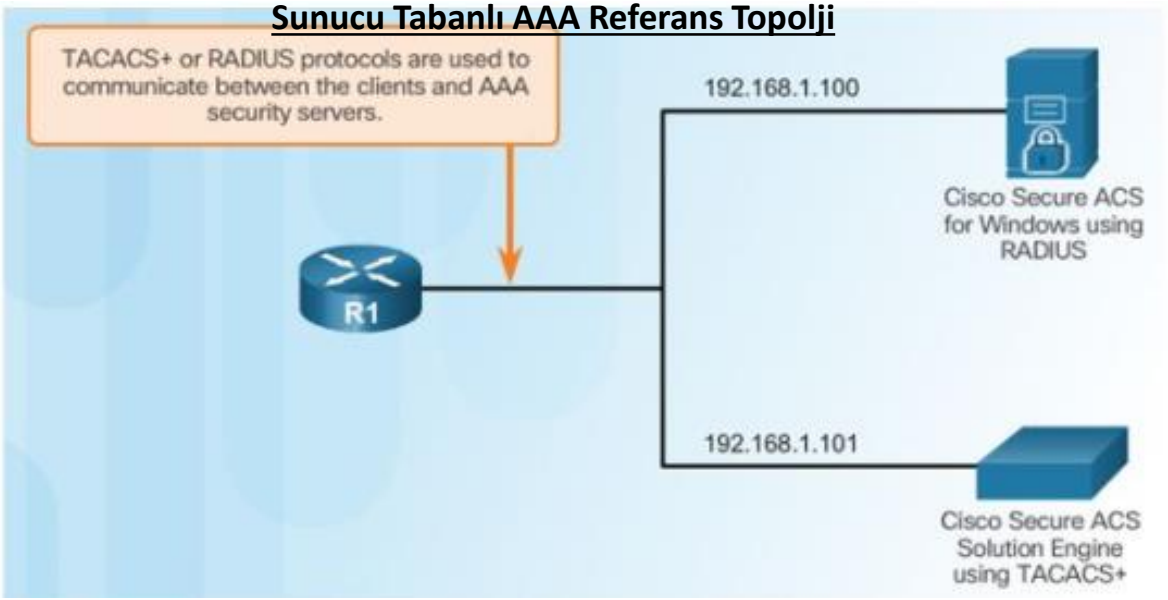
RADIUS Doğrulama Methodu



Sunucu Tabanlı AAA Kimlik Doğrulaması Yapılandırması (CLI ile)

1. AAA'yı aktif etme
2. ACS sunucusunun IP adresini belirtin.
3. Gizli anahtarı yapılandırın.
4. RADIUS veya TACACS+ sunucusunu kullanmak için kimlik doğrulamayı yapılandırın.

Sunucu Tabanlı AAA Referans Topolji



AAA TACACS+ Sunucusunun Yapılandırması

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.101
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
```

AAA RADIUS Sunucusunun Yapılandırması

```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
```

Sunucu Tabanlı AAA Yetkilendirme Yapılandırması (CLI ile)

Komut Söz Dizimi

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec ?
  WORD     Named authorization list.
  default  The default authorization list.
```

Yetkilendirme Methodları Listesi

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec default ?
  cache              Use Cached-group
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Örnek Yapılandırma

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Sunucu Tabanlı AAA Hesap Yönetimi Yapılandırması (CLI ile)

Komut Söz Dizimi

```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]

R1(config)# aaa accounting exec?
  WORD        Named Accounting list.
  default     The default accounting list.
```

Hesap Yönetimi Methodları Listesi

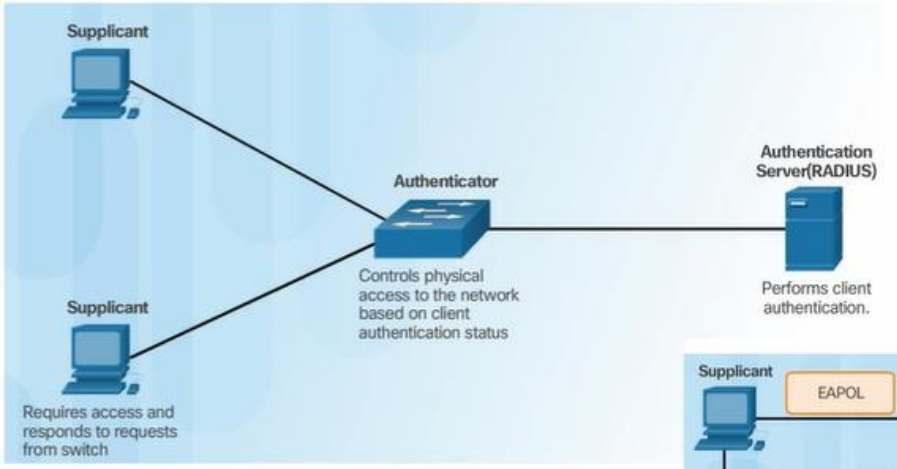
```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]

R1(config)# aaa accounting exec default start-stop?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

R1(config)# aaa accounting exec default start-stop group?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

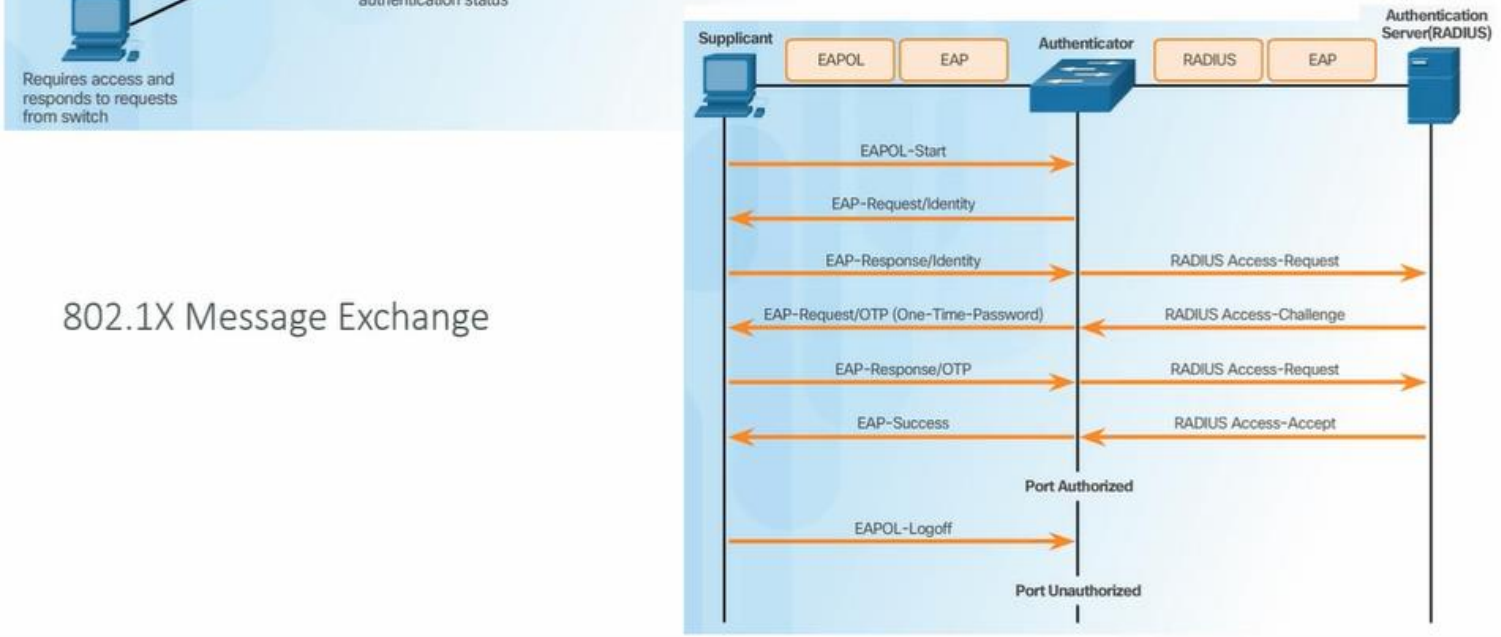
Örnek Yapılandırma

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

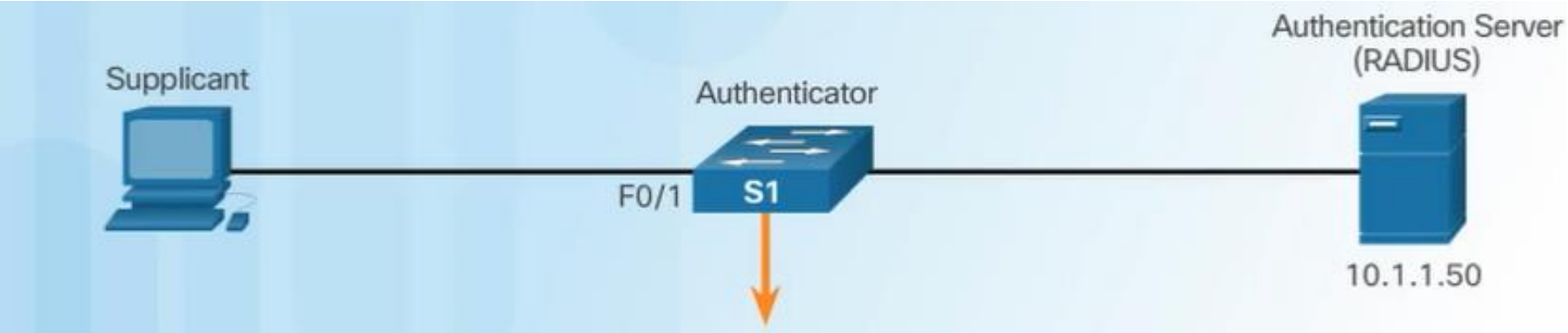
IEEE 802.1X Port Tabanlı Kimlik Doğrulama

- Noktadan noktaya bağlantılara sahip LAN portuna takılmış cihazların kimlik doğrulama ve yetkilendirilmesine olanak sağlayan port tabanlı ağ erişim denetimidir.
- Kullanıcı doğrulama; MAC adresi, switch portu ya da harici bir yetkilendirme politikası ile sağlanır. Ağa kimin hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirmesi kullanıcı odaklı, ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir.





IEEE 802.1X Örnek Uygulama




```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```