

BSM 471-AĞ GÜVENLİĞİ

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

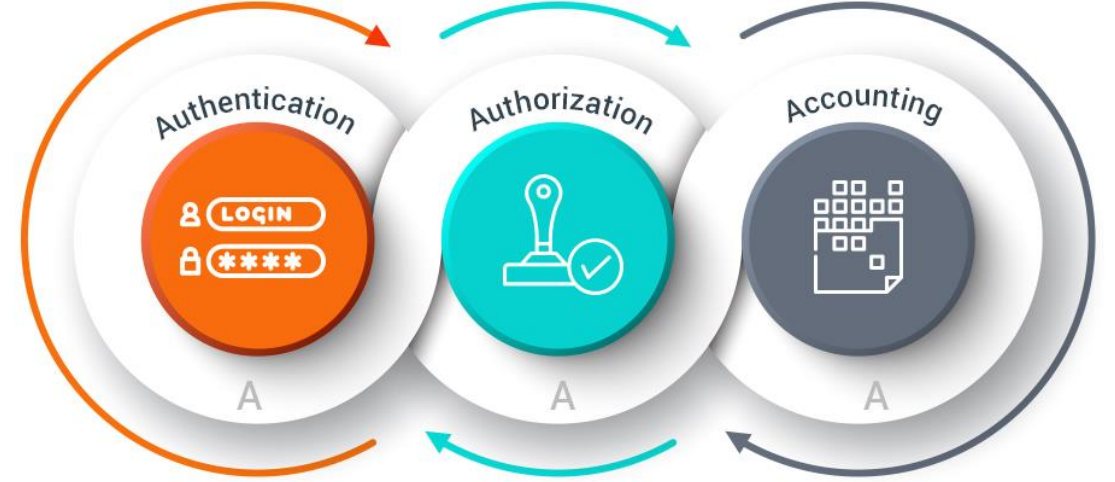
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

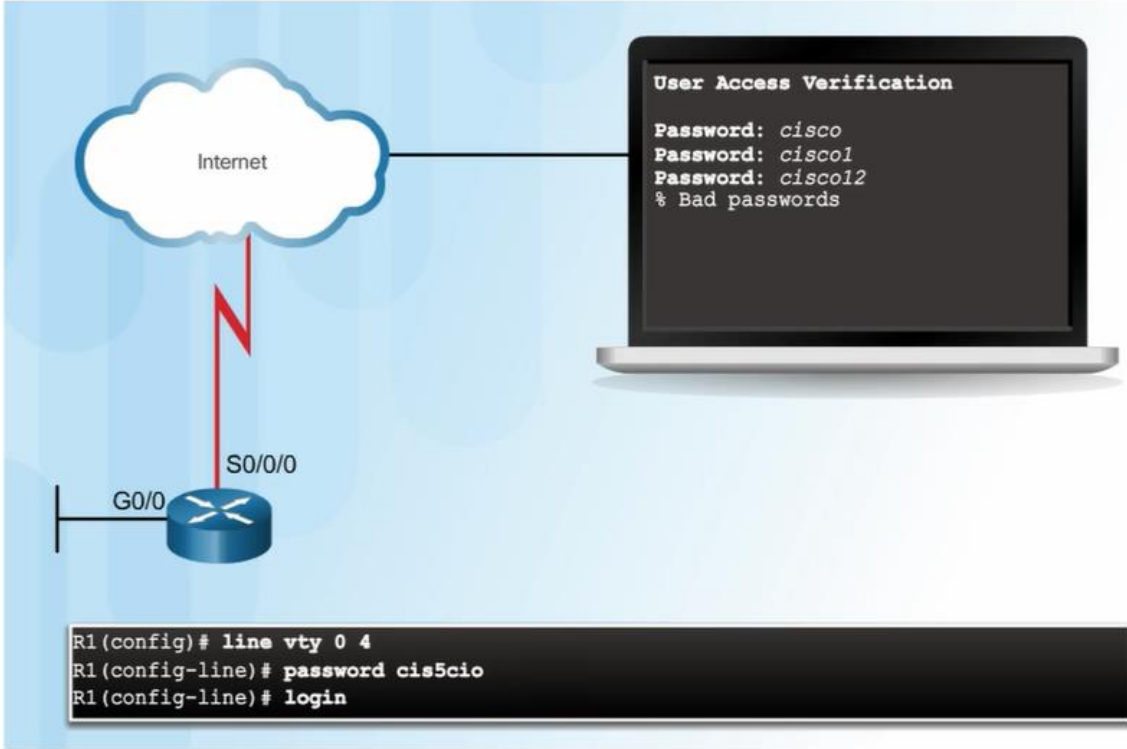
- Kimlik Doğrulama, Yetkilendirme ve Hesap Yönetimine Giriş
- Network Tarafı AAA
 - Yerel AAA Doğrulama
 - Sunucu Bazlı Doğrulama
 - TACAS+ ve RADIUS Protokolleri
 - Sunucu Bazlı Yetkilendirme
 - Sunucu Bazlı Hesap Yönetimi
 - 802.1x Kimlik Tabanlı Ağ Güvenliği
- Sistem Tarafı AAA
 - Aktif Dizin Yapısı
 - Aktif Dizin Yapı Servisleri
 - Aktif Dizin Mantıksal Bileşenleri
 - Aktif Dizin Saldırıları
 - Aktif Dizin Güvenlik Önlemleri

AAA Giriş

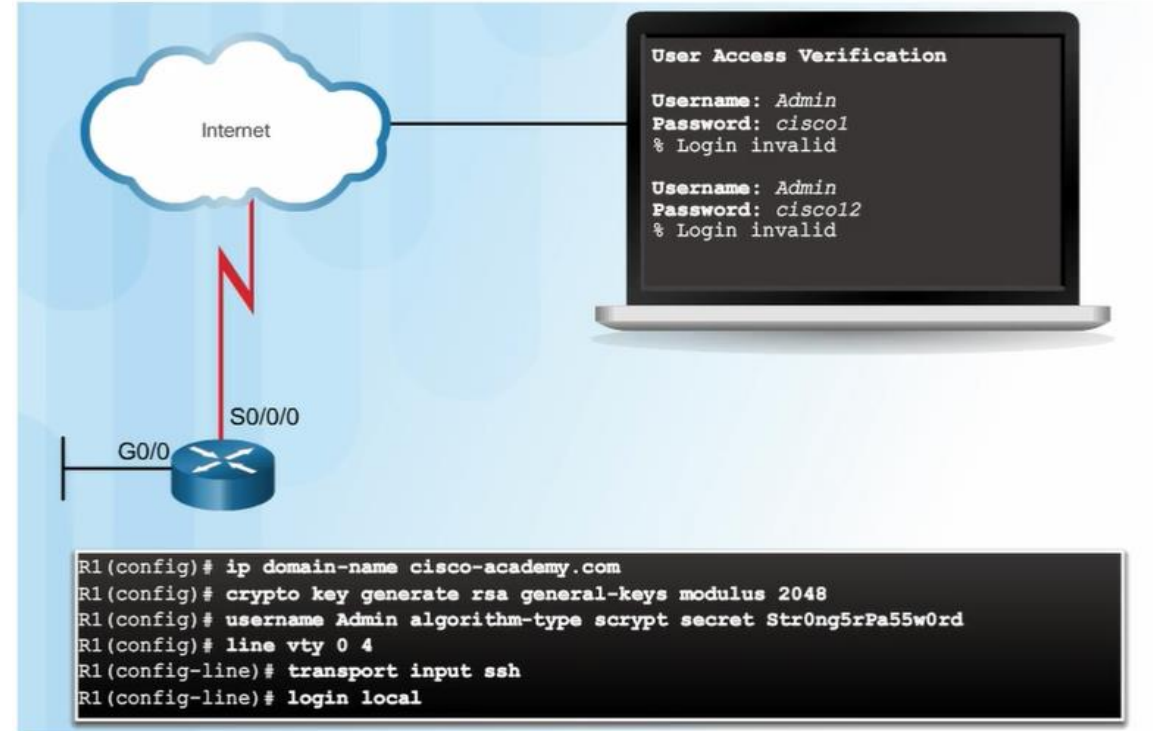
- **Authentication**; kullanıcının sisteme bağlanabilmesi için gerekli olan ilk adımdır. 2 aşaması mevcuttur:
 - Yerel AAA Doğrulaması
 - Sunucu-Tabanlı AAA Doğrulaması
- **Authorization**; Kullanıcı adı ve şifre doğrulaması sağlanan kullanıcıların sisteme, programa veya ağa hangi yetkilerle erişim hakkına 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



Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Account Number 1234-567-890	Statement Closing Date 01-31-01	Current Amount Due \$278.50
--------------------------------	------------------------------------	--------------------------------

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 19900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 001782550000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name JOE EMPLOYEE	Account Number 1234-456-890	Statement Closing Date 01-31-01
---------------------------------	--------------------------------	------------------------------------

Statement Date: 02-01-01	Payment Due Date: 03-01-01
Closing Date: 01-31-01	
Credit Limit: \$1,500.00	Credit Available: \$1221.50
New Balance: \$278.50	Minimum Payment Due: \$20.00

Account Summary

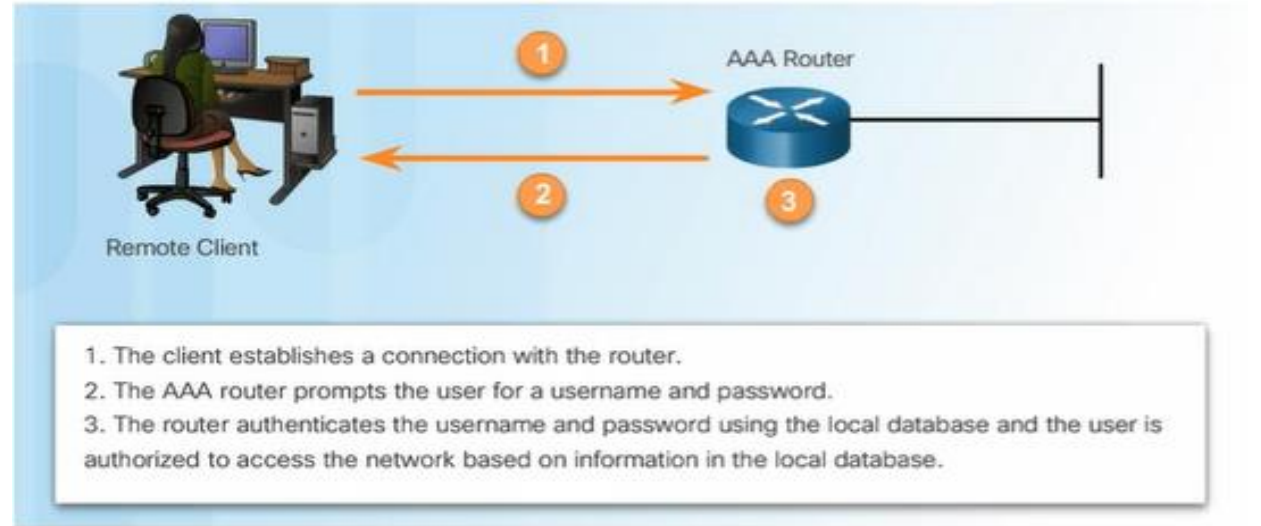
Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
23455678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

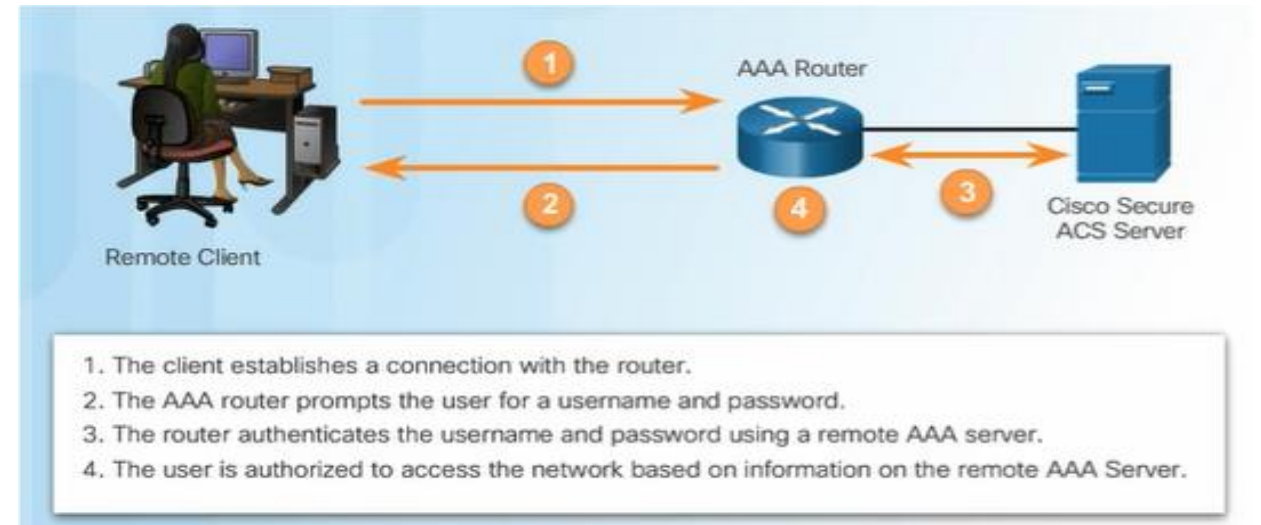
PAGE 1 OF 1

AAA-Kimlik Doğrulama Metotları

Yerel AAA Doğrulaması

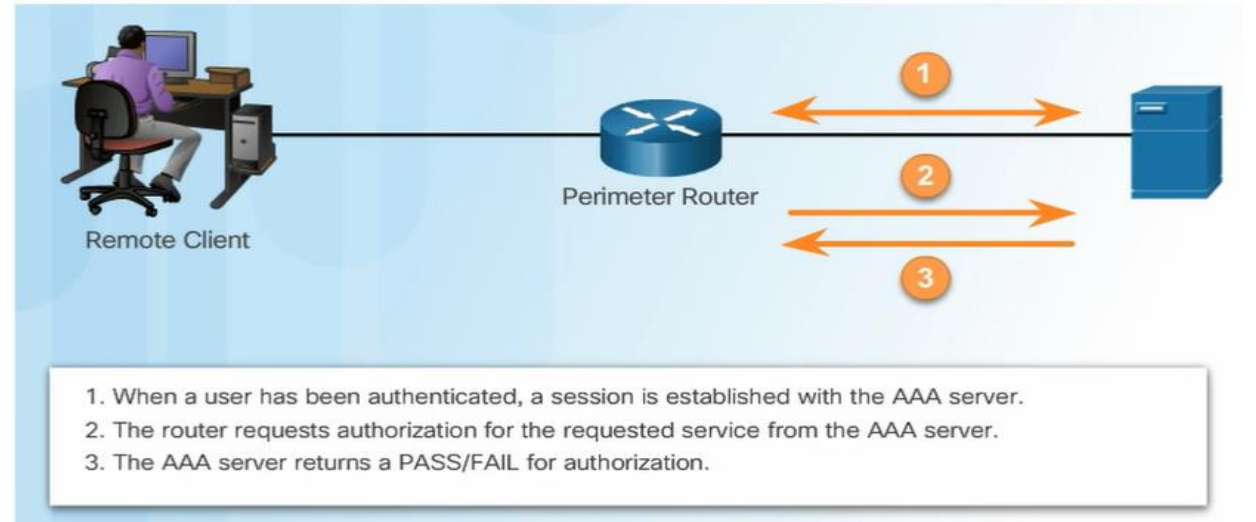


Sunucu-Tabanlı AAA Doğrulaması

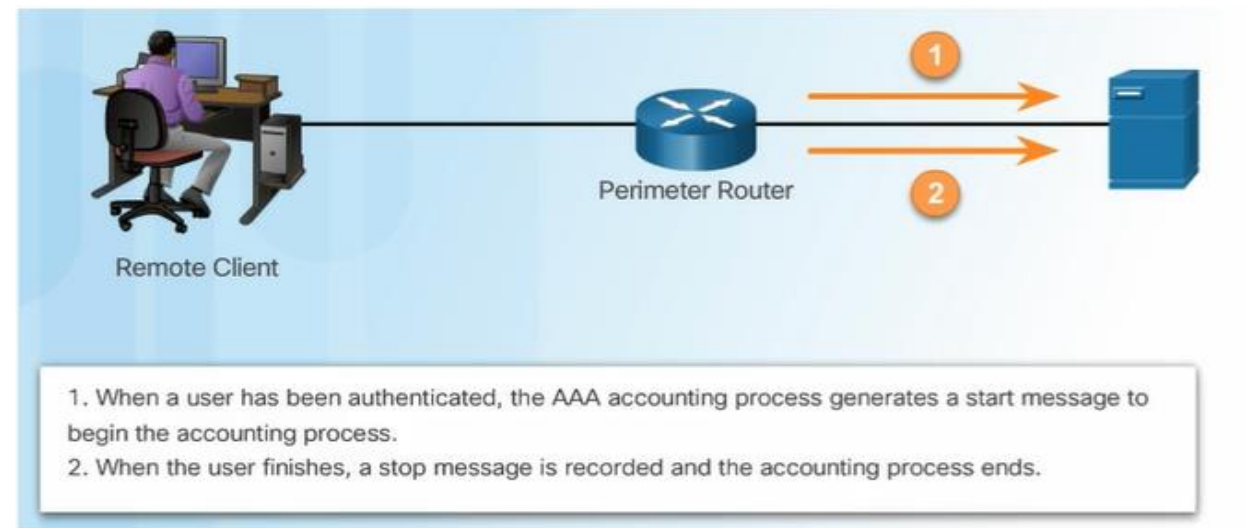


AAA-Yetkilendirme ve Hesap Yönetimi Metotları

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 <i>group-name</i>	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.
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>method1...[method4]</i>	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
<i>number-of-unsuccessful-attempts</i>	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
```

```
JR-ADMIN
```

```
Lock time
```

```
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
```

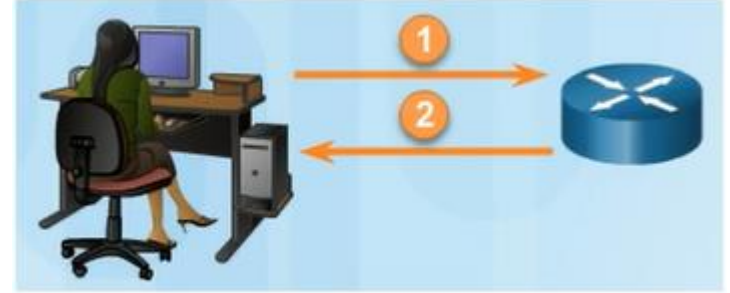
```
Idle Time: 0
```

```
CT Call Handle: 0
```

Sunucu Tabanlı Kimlik Doğrulama

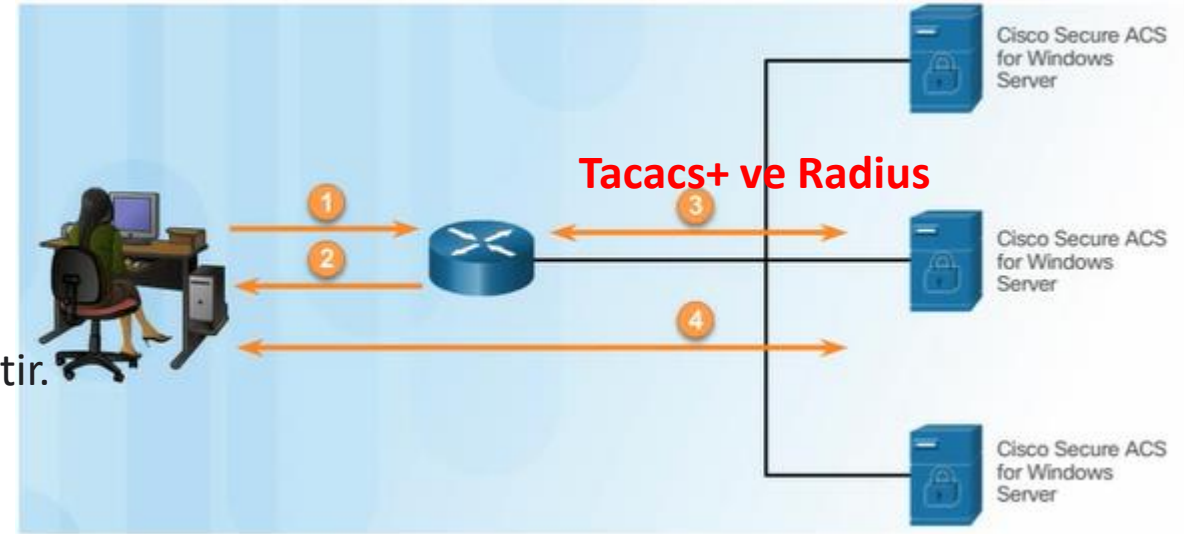
- **Yerel Doğrulama;**

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



- **Sunucu-Tabanlı Doğrulama;**

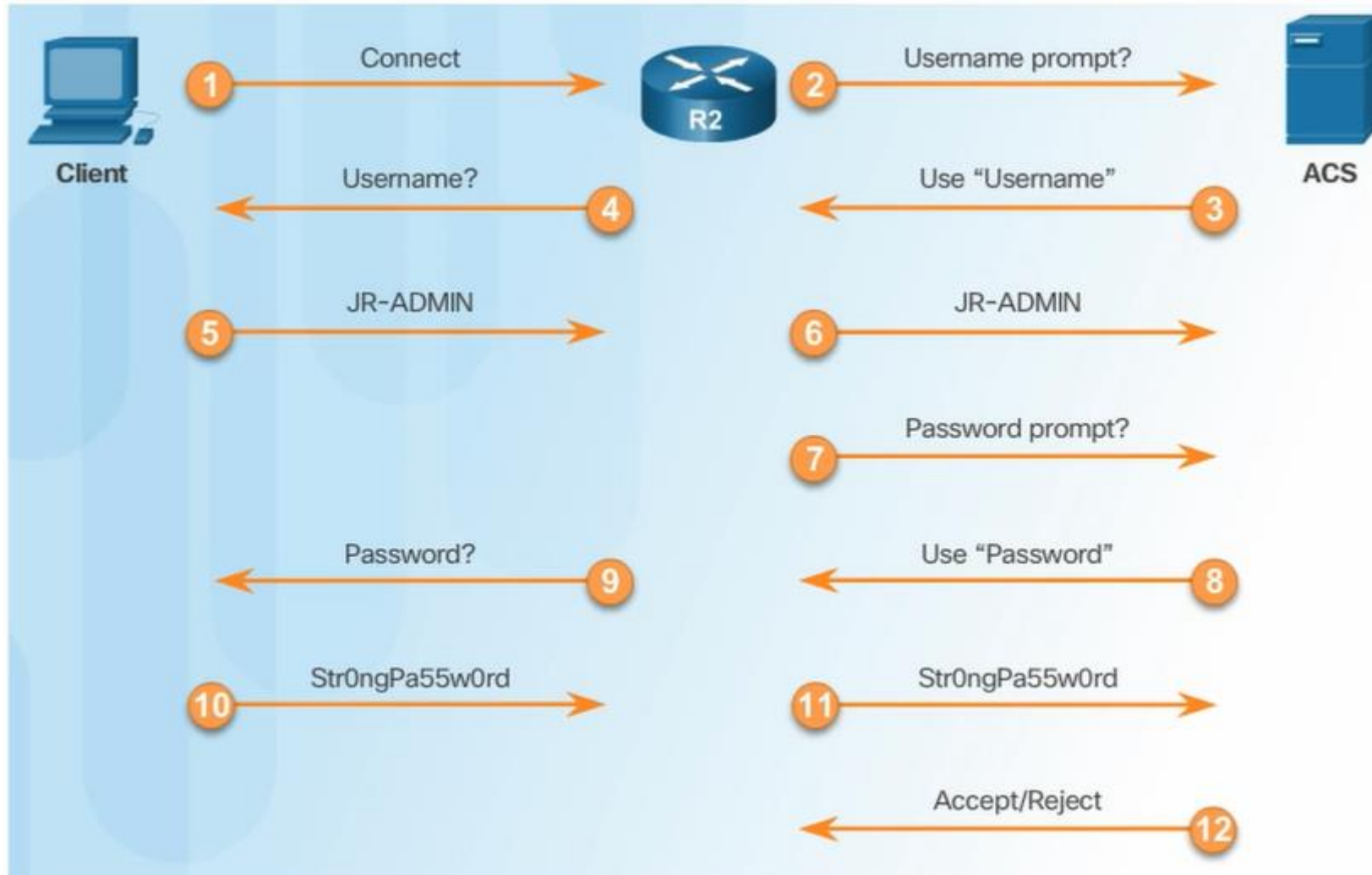
- Kullanıcı yönlendirici ile bağlantı kurar.
- Yönlendirici, kullanıcıdan bir kullanıcı adı ve parola ister.
- Yönlendirici, kullanıcı adını ve şifreyi Cisco Secure ACS'ye iletir.
- Cisco Secure ACS, kullanıcının kimliğini doğrular.



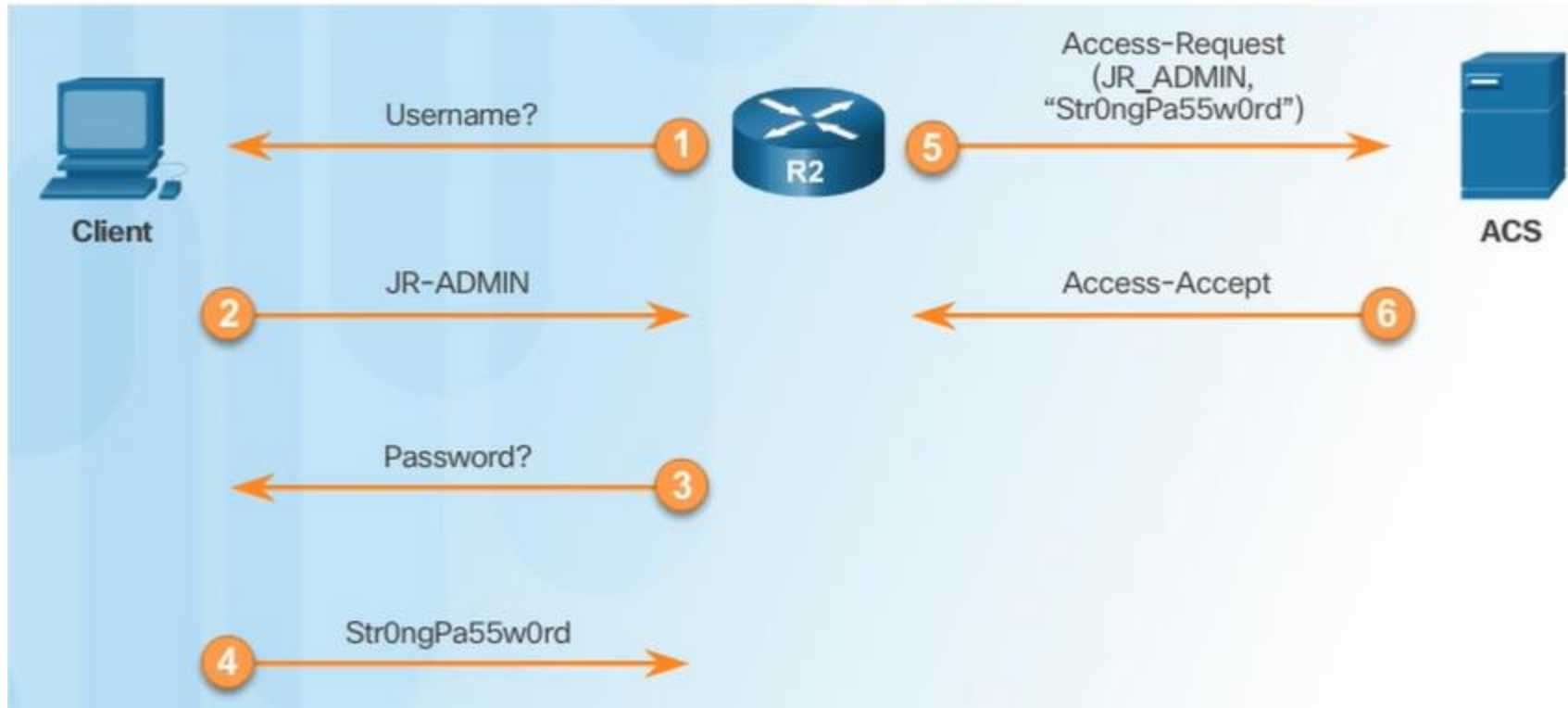
TACACS+ ve RADIUS Protokolleri

	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)

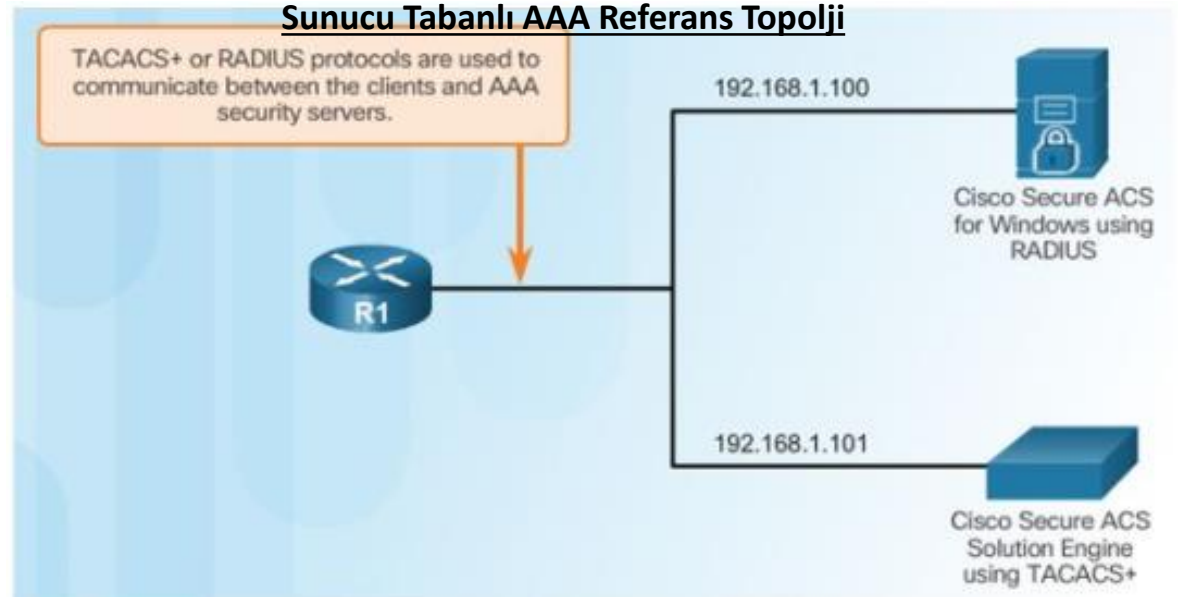
1. AAA'yı aktif etme
2. ACS sunucusunun IP adresini belirtin.
3. Gizli anahtarı yapılandırın.
4. RADIUS veya TACACS+ sunucusunu kullanmak için kimlik doğrulamayı yapılandırın.

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.
```

```
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.
```

Yetkilendirme Methodları Listesi

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.
```

```
R1(config)#
```

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

Hesap Yönetimi Methodları Listesi

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

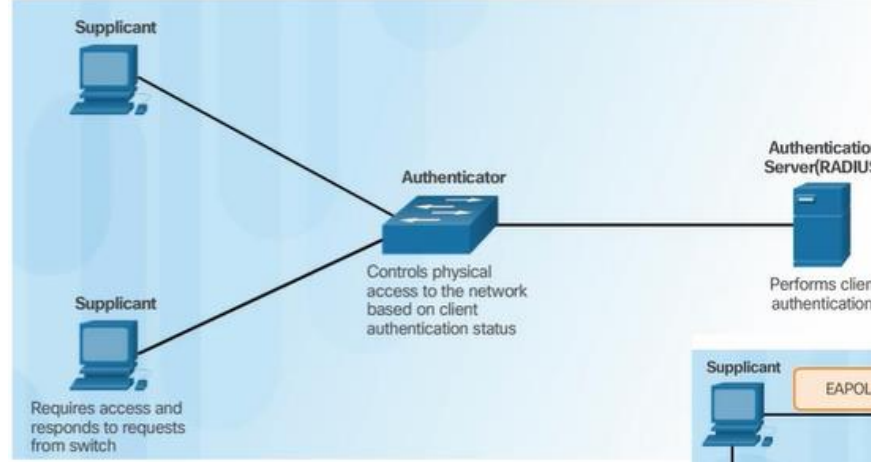
```
R1(config)# aaa accounting exec default start-stop group?  
WORD      Server-group name  
radius     Use list of all Radius hosts.  
tacacs+    Use list of all Tacacs+ hosts.
```

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+
```

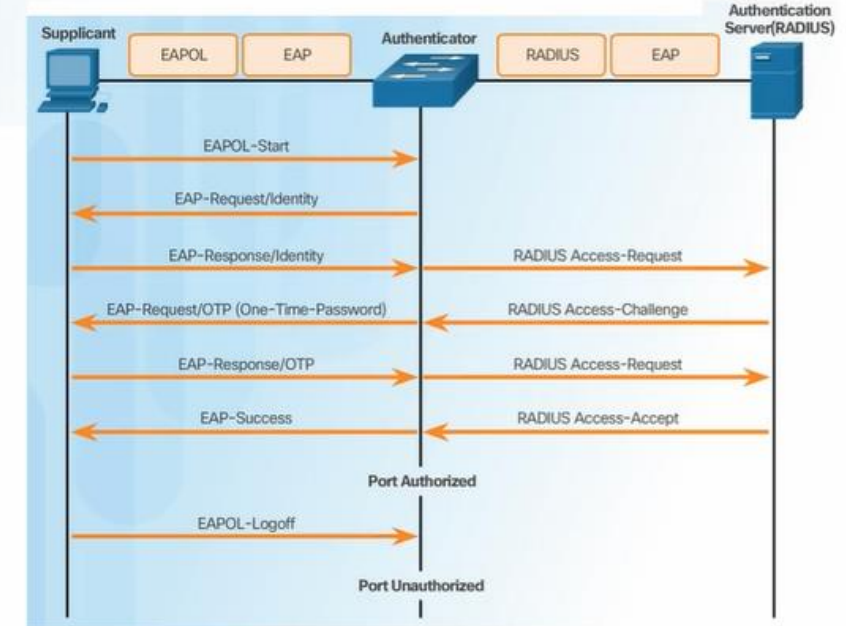
IEEE 802.1X Port Tabanlı Kimlik Doğrulama

- 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.

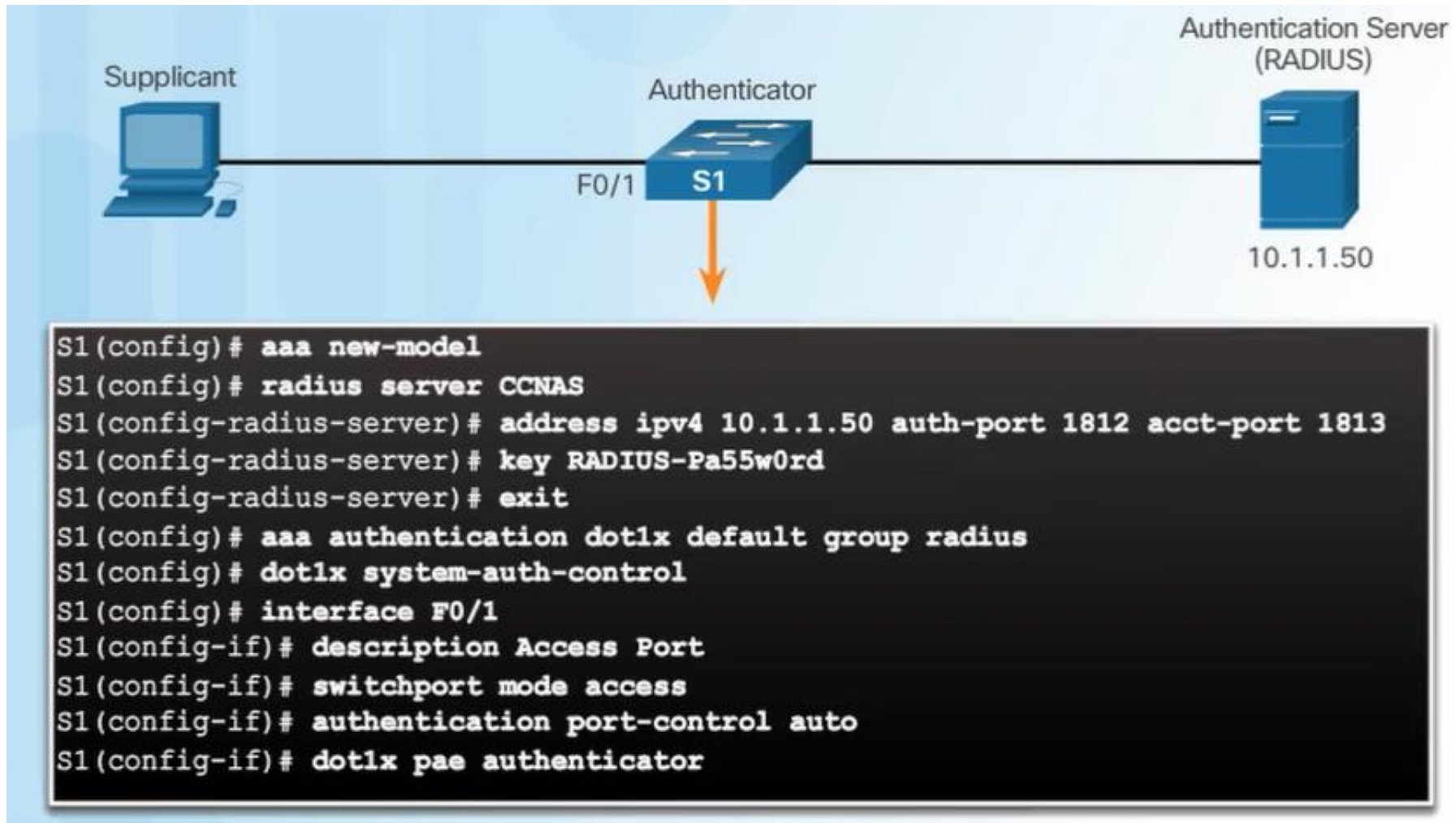


802.1X Roles

802.1X Message Exchange



IEEE 802.1X Örnek Uygulama



Active Directory (Aktif Dizin) Kavramı

- Aktif dizin; Microsoft tarafından Windows etki alanı ağları için geliştirilen bir dizin hizmetidir:
 - Bir grup kullanıcı için dosyalar, yazıcılar, kişiler ve uygulamalar da dahil olmak üzere ağ kaynaklarını **tanımlamak, yönetmek, bunlara erişmek** ve **güvenliğini** sağlamak için kullanılır.
- Active Directory gönderilen kullanıcı adını ve şifreyi kontrol eder ve kullanıcının sistem yöneticisi mi yoksa yönetici olmayan bir kullanıcı mı olduğunu belirler. Ayrıca bilgilerin yönetimine ve depolanmasına izin verir, kimlik doğrulama ve yetkilendirme mekanizmaları sağlar ve diğer ilgili hizmetlerin dağıtımı için bir çerçeve oluşturur:
 - Sertifika Hizmetleri, Active Directory Federasyon Hizmetleri, Basit Dizin Hizmetleri ve Hak Yönetimi Hizmetleri
- Active Directory, Basit Dizin Erişim Protokolü ([LDAP](#)) sürüm 2 ve 3'ü, Microsoft'un [Kerberosv5](#) sürümünü, SSLv3 ve TLSv3 ve DNS'yi kullanır.

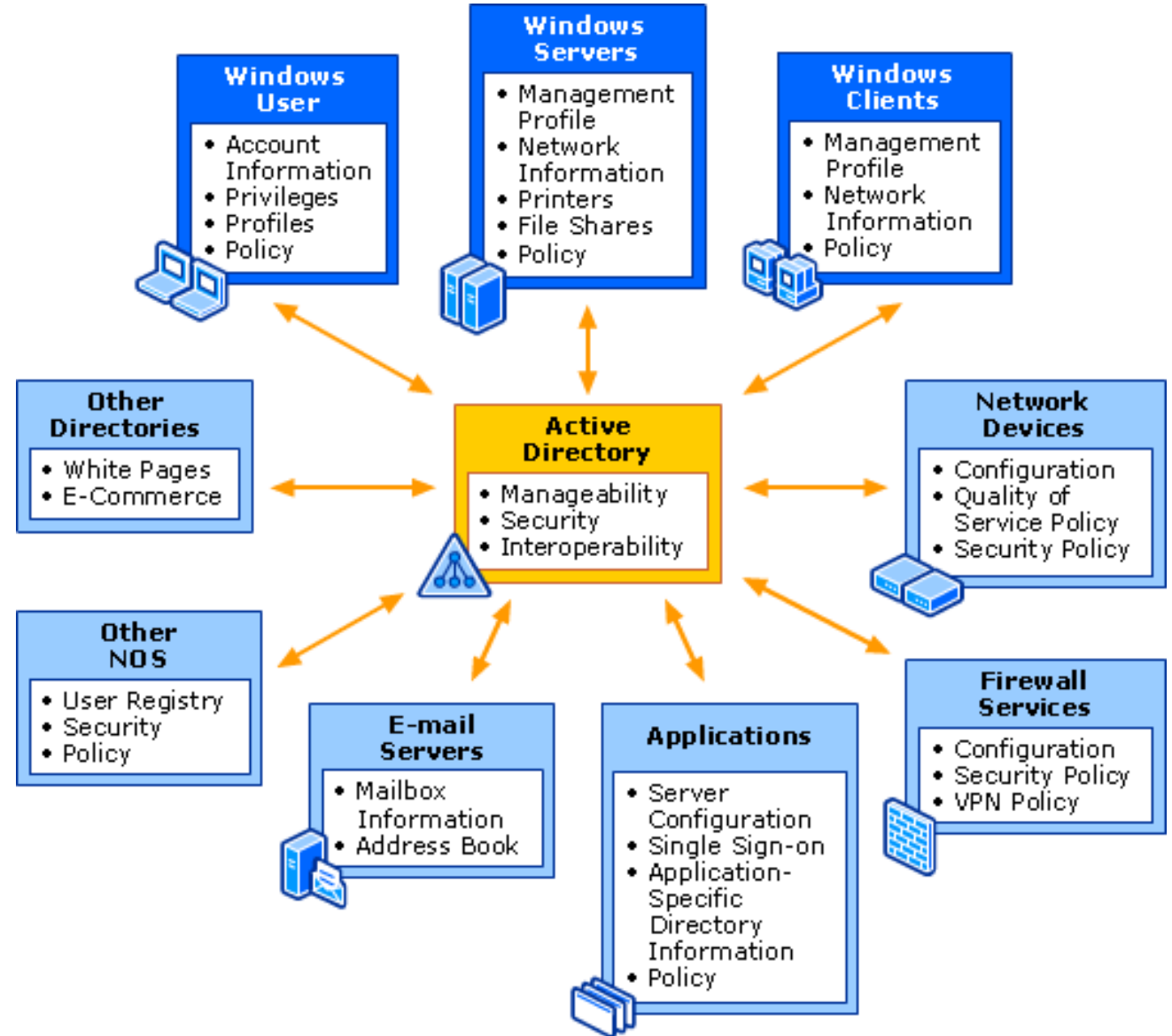
Aktif Dizin Çalışma Yapısı

- AD, etki alanları ve etki alanı denetleyicileri arasındaki iletişim için Basit Dizin Erişim Protokolü'nü (LDAP) kullanır.
- LDAP, bir IP ağı üzerinden dağıtılmış dizin hizmetlerinin yönetimini sağlayan bir dizin hizmeti protokolüdür.
- Ayrıca AD, bir ağ üzerinden kimlik doğrulama için güvenli bir kimlik doğrulama protokolü olan Kerberos'u kullanır.
- Ağ kaynaklarını verimli bir şekilde yönetmek için Active Directory, Grup İlkesi Nesnelerini (GPO'lar) kullanır.
- GPO'lar, ağ genelinde güvenlik ilkelerini, yazılım dağıtımını ve diğer yönetim görevlerini denetlemek ve uygulamak için kullanılırlar.
- AD ayrıca, ağ kaynaklarının uzaktan yönetimine izin veren Uzaktan Yordam Çağrılarını (RPC'ler) için destek sağlar. Bu, ağ yöneticilerinin, kaynakların konumundan bağımsız olarak ağ kaynaklarını merkezi bir konumdan verimli bir şekilde yönetebilmelerini sağlar.

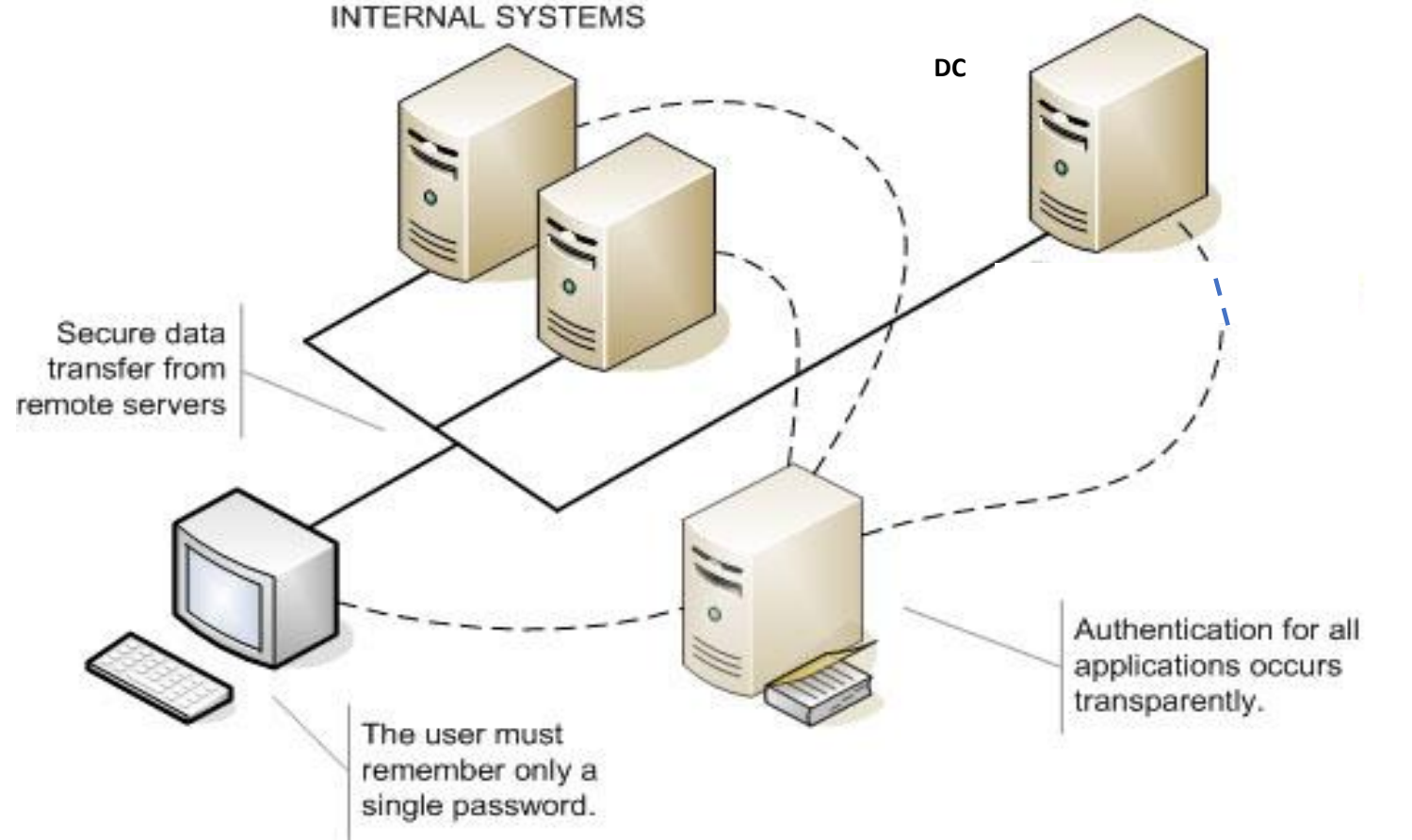
Active Directory (Aktif Dizin) Avantajları

- Aktif dizin yapısının sağlamış olduğu bazı faydalar şu şekildedir:
 - Merkezi Kaynak ve Güvenlik Yönetimi
 - Ağ kaynaklarına erişim için tek oturum açma
 - Hata toleransı ve yedeklilik
 - Basitleştirilmiş kaynak konumu

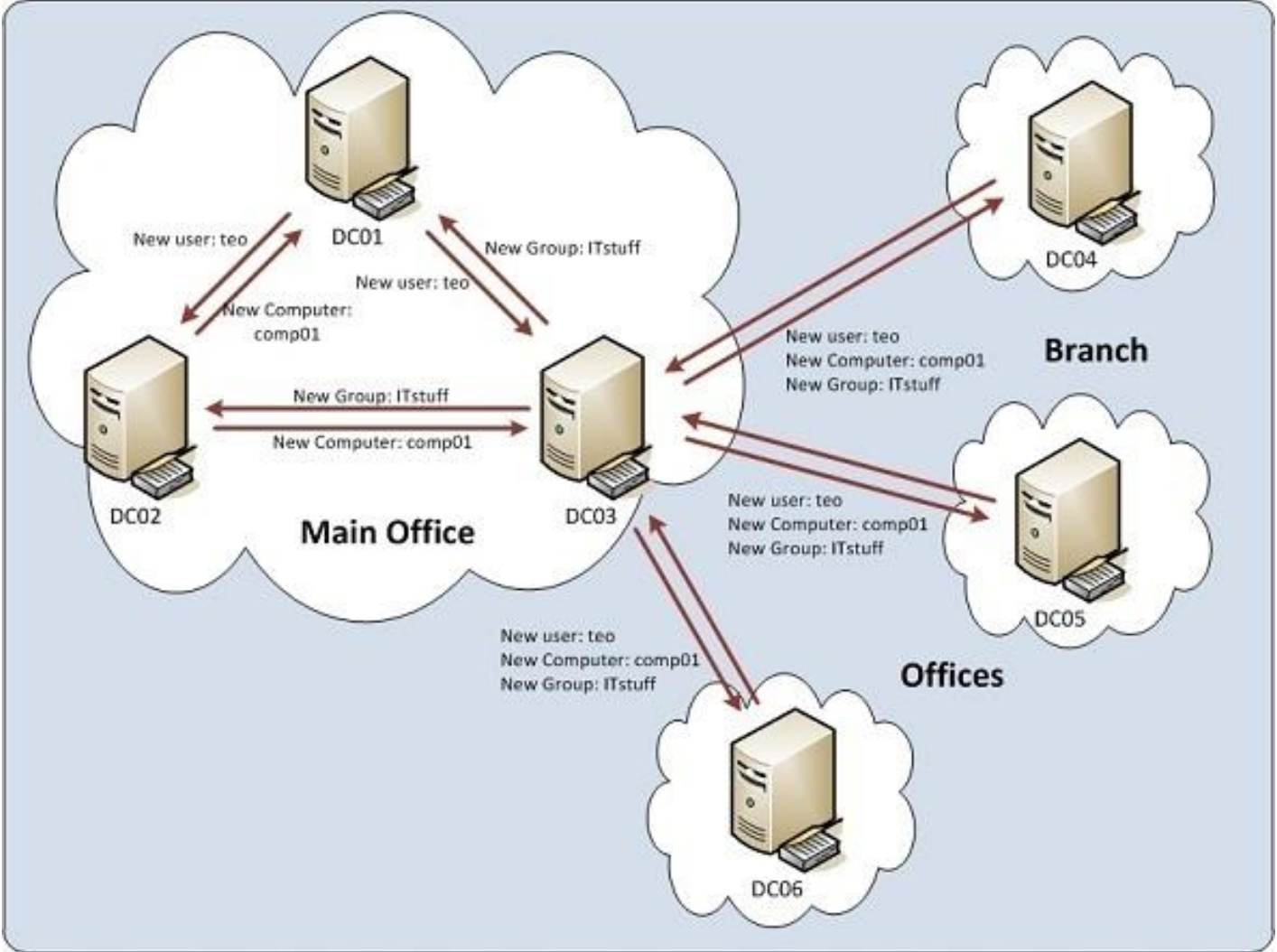
Merkezi Kaynak ve Güvenlik Yönetimi



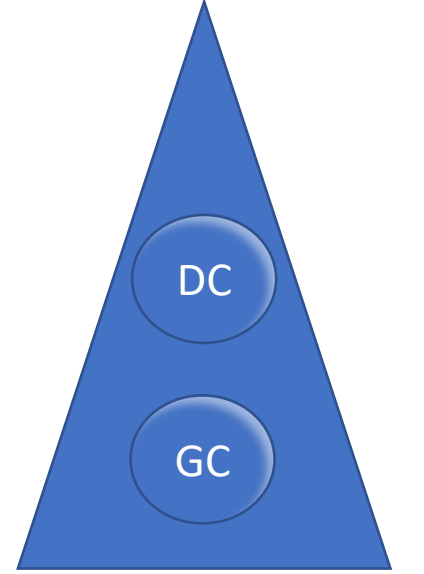
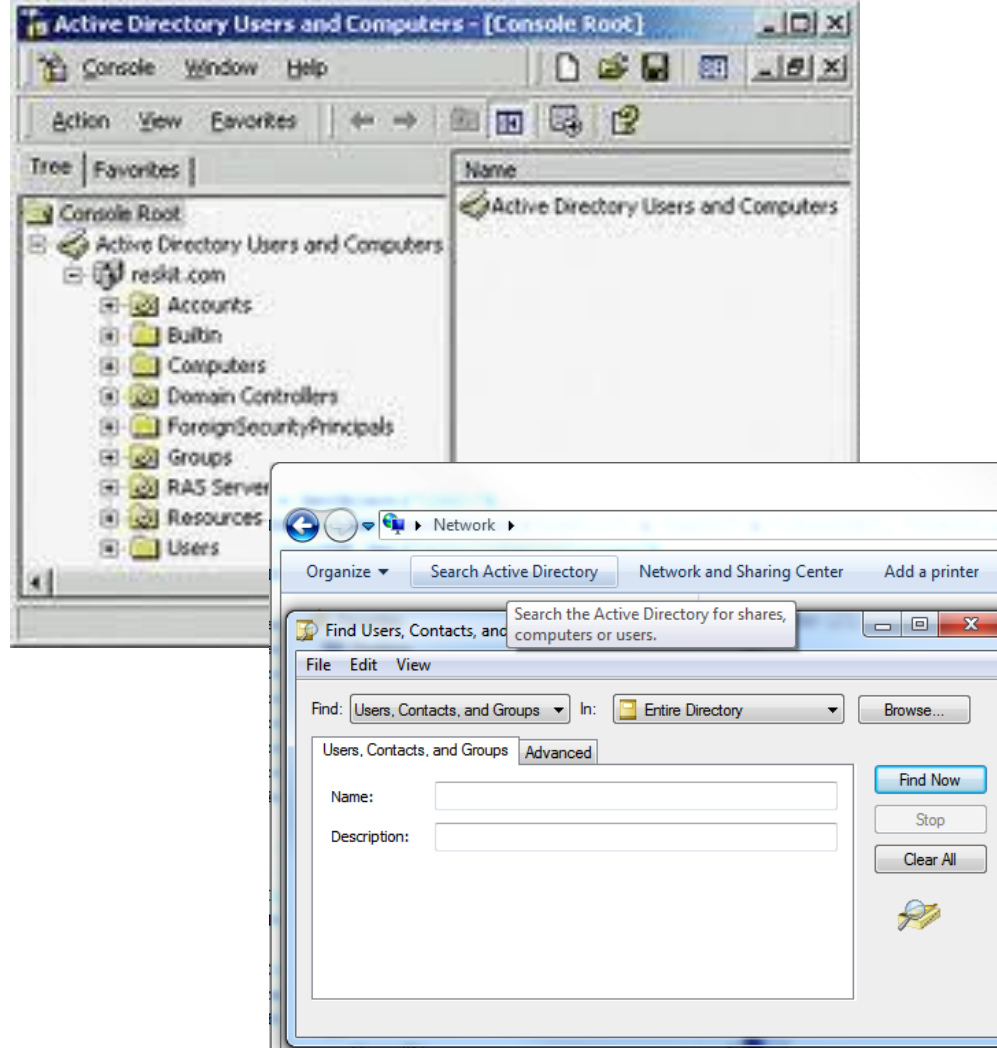
Ağ Kaynaklarına Erişim için Tek Oturum Açma



Hata Toleransı Ve Yedeklilik



Basitleştirilmiş Kaynak Konumu



Aktif Dizin Hizmetleri

- Domain Services
- Lightweight Directory Services
- Certificate Services
- Federation Services
- Rights Management Services

Domain Services

- Active Directory Etki Alanı Hizmetleri (AD DS), her Windows etki alanı ağının temelidir. Cihazlar ve kullanıcılar da dahil olmak üzere etki alanı üyeleri hakkındaki bilgileri saklar, kimlik bilgilerini doğrular ve erişim haklarını tanımlar. Bu hizmeti çalıştıran sunucuya etki alanı denetleyicisi adı verilir. Bir kullanıcı bir cihazda oturum açtığı anda, ağ üzerinden başka bir cihaza eriştiğinde veya bir makineye yüklenen iş kolu Metro tarzı bir uygulamayı çalıştırdığında, etki alanı denetleyicisiyle iletişim kurulur.
- Diğer Active Directory hizmetleri (aşağıda açıklandığı gibi LDS hariç) ve çoğu Microsoft sunucu teknolojisi Etki Alanı Hizmetlerine dayanır veya bunları kullanır; örnekler arasında Grup İlkesi, Şifreleme Dosya Sistemi, BitLocker, Etki Alanı Adı Hizmetleri, Uzak Masaüstü Hizmetleri, Exchange Sunucusu ve SharePoint Sunucusu yer alır.
- Kendi kendine yönetilen Active Directory DS'nin, bir bulut ürünü olan yönetilen Azure AD DS'den farklı olması gerekir.

Lightweight Directory Services

- Daha önce Active Directory Uygulama Modu (ADAM) olarak adlandırılan Active Directory Basit Dizin Hizmetleri (AD LDS), AD DS için LDAP protokolünü uygular.
- Windows Server'da bir hizmet olarak çalışır ve eşit bir API dahil olmak üzere AD DS ile aynı işlevleri sunar.
- Ancak AD LDS, etki alanlarının veya etki alanı denetleyicilerinin oluşturulmasını gerektirmez.
- Dizin verilerini depolamak için bir Veri Deposu ve LDAP Dizin Hizmeti Arayüzüne sahip bir Dizin Hizmeti sağlar.
- AD DS'den farklı olarak, birden fazla AD LDS örneği aynı sunucuda çalışabilir.

Certificate Services

- Active Directory Sertifika Hizmetleri (AD CS), şirket içi bir ortak anahtar altyapısı kurar. Bir kuruluşun dahili kullanımları için ortak anahtar sertifikaları oluşturabilir, doğrulayabilir, iptal edebilir ve diğer benzer eylemleri gerçekleştirebilir.
- Bu sertifikalar, dosyaları (Şifreleme Dosya Sistemi ile kullanıldığında), e-postaları (S/MIME standardına göre) ve ağ trafiğini (sanal özel ağlar, Aktarım Katmanı Güvenliği protokolü veya IPSec protokolü tarafından kullanıldığında) şifrelemek için kullanılabilir.
- AD CS, Windows Server 2008'den öncesine dayanmaktadır ancak adı yalnızca Sertifika Hizmetleri'dir.
- AD CS, bir AD DS altyapısı gerektirir.

Federation Services

- Active Directory Federasyon Hizmetleri (AD FS), tek oturum açma hizmetidir. AD FS altyapısı mevcut olduğunda, kullanıcılar, merkezi bir konumda depolanan tek bir kimlik bilgisi setini kullanarak çeşitli web tabanlı hizmetleri (örn. internet forumu, blog, çevrimiçi alışveriş, web postası) veya ağ kaynaklarını kullanabilirler; bunun yerine, kendilerine verilmesi gerekmemektedir. her hizmet için özel bir kimlik bilgileri kümesi.
- AD FS, belirteç kimlik bilgilerini iletmek için SAML, OAuth veya OpenID Connect gibi birçok popüler açık standardı kullanır. AD FS, SAML iddialarının şifrelenmesini ve imzalanmasını destekler. AD FS'nin amacı, AD DS'nin bir uzantısıdır: AD DS, kullanıcıların tek bir kimlik bilgisi kümesi kullanarak aynı ağın parçası olan aygıtlarda kimlik doğrulaması yapmasına ve bu aygıtları kullanmasına olanak tanır. İlki, aynı kimlik bilgilerini farklı bir ağda kullanmalarına olanak tanır.
- Adından da anlaşılacağı gibi AD FS, birleşik kimlik kavramına dayalı olarak çalışır.
- AD FS, bir AD DS altyapısı gerektirir, ancak federasyon ortağı bunu gerektirmeyebilir.

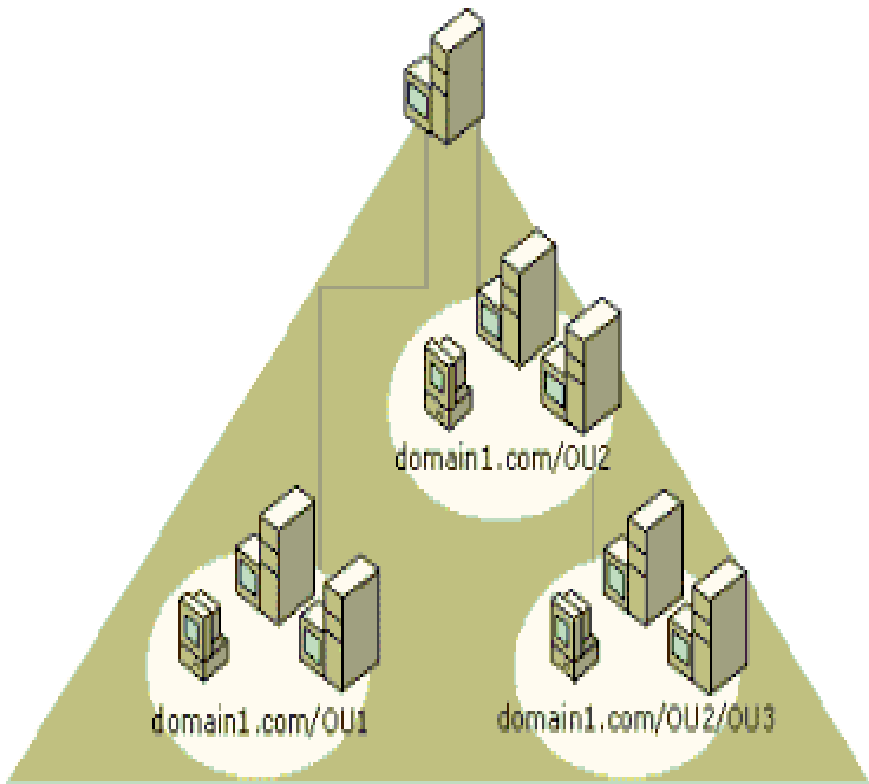
Rights Management Services

- Windows Server 2008'den önce Hak Yönetimi Hizmetleri veya RMS olarak bilinen Active Directory Hak Yönetimi Hizmetleri (AD RMS), Windows Server'da bulunan, bilgi hakları yönetimine olanak tanıyan sunucu yazılımıdır.
- Kurumsal e-postalar, Microsoft Word belgeleri ve web sayfaları gibi çeşitli belgelere erişimi kısıtlamak için şifreleme ve seçici reddetmeyi kullanır. Ayrıca yetkili kullanıcıların bunlar üzerinde gerçekleştirebileceği görüntüleme, düzenleme, kopyalama, kaydetme veya yazdırma gibi işlemleri de sınırlar.
- BT yöneticileri kolaylık sağlamak amacıyla son kullanıcılara yönelik önceden ayarlanmış şablonlar oluşturabilir, ancak son kullanıcılar yine de içeriğe kimlerin erişebileceğini ve hangi eylemleri gerçekleştirebileceklerini tanımlayabilir.

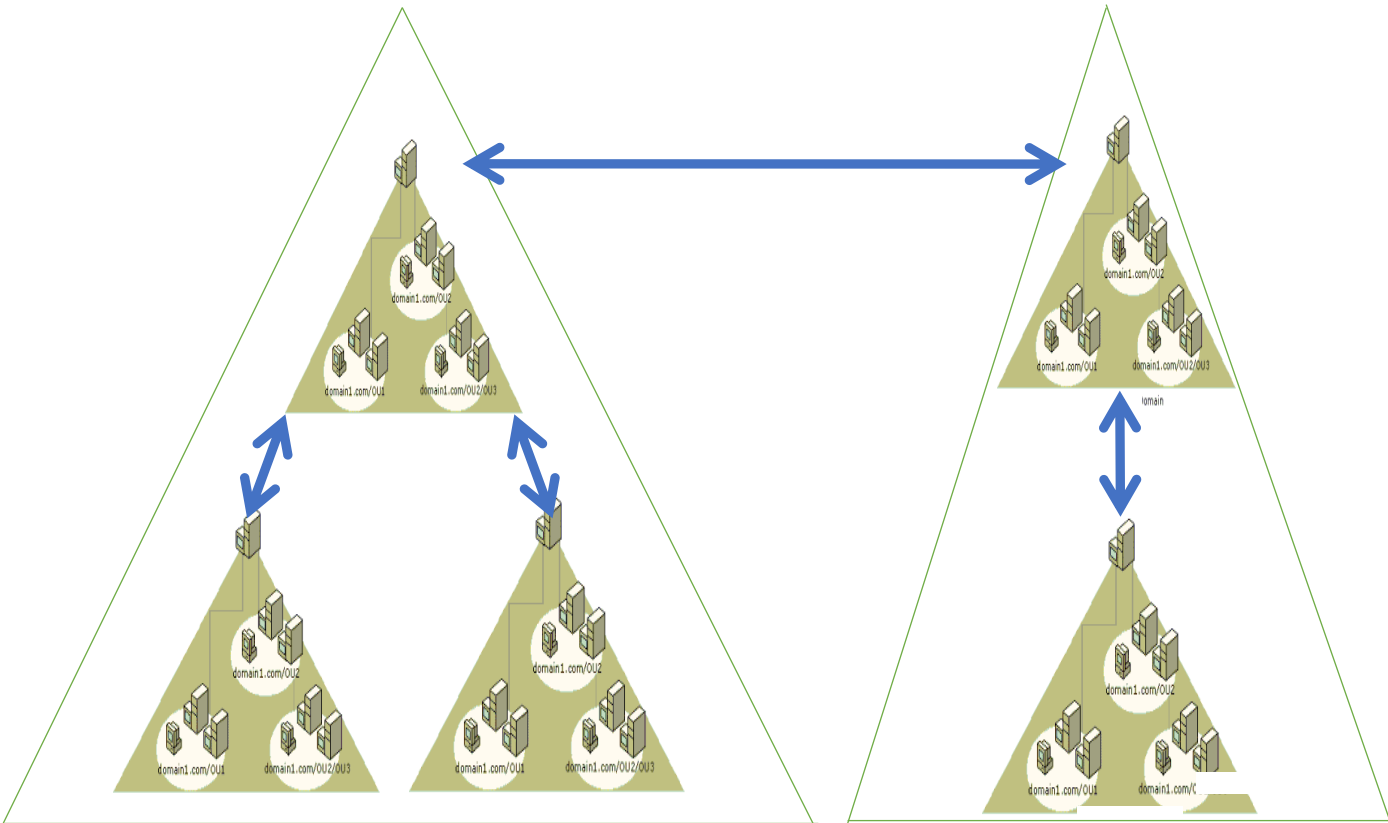
Aktif Dizin Mantıksal Bileşenleri

- Domain and Organizational Unit (OU)
- Tree and Forest
- Schema and DNS

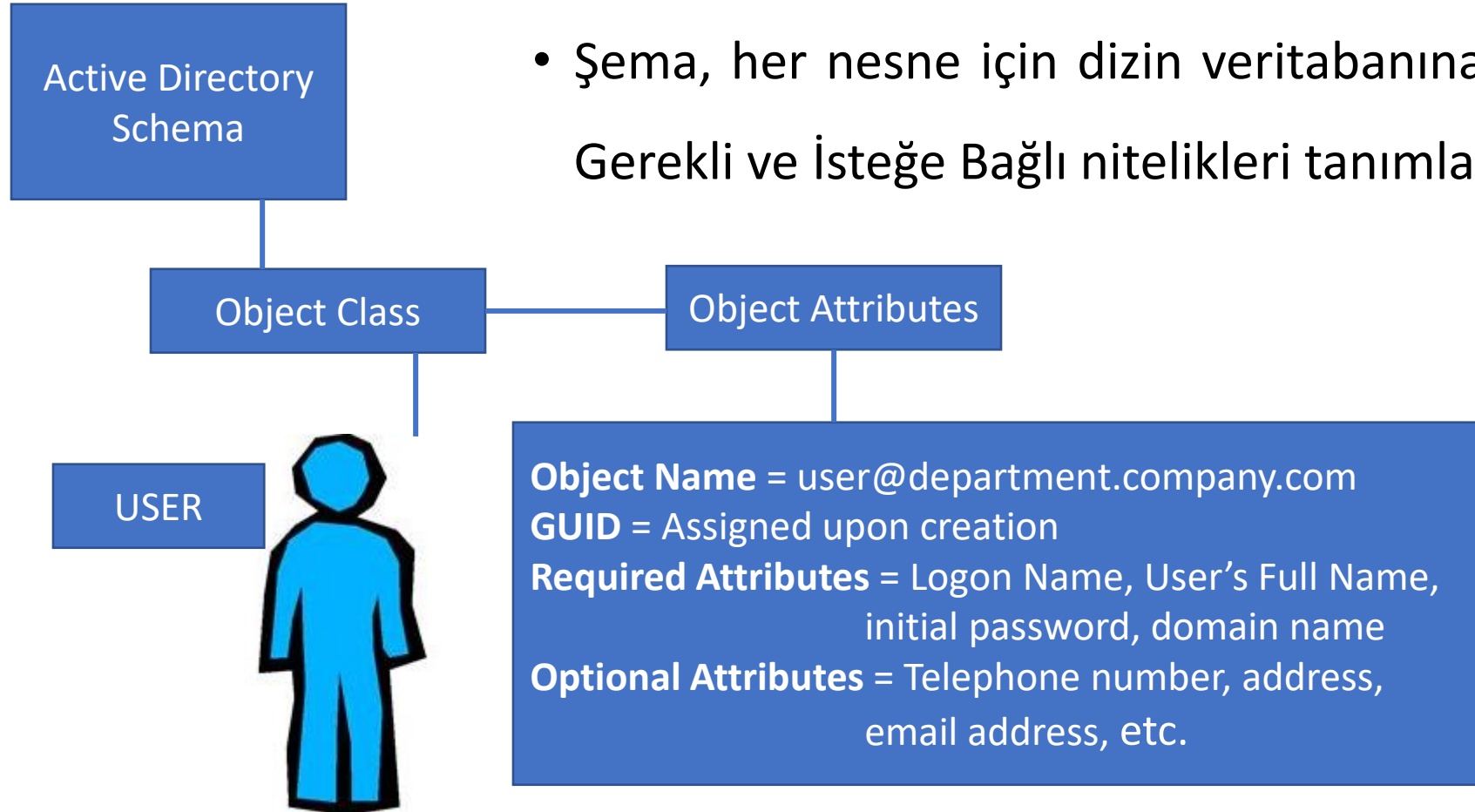
Domain and Organizational Unit (OU)



Tree and Forest

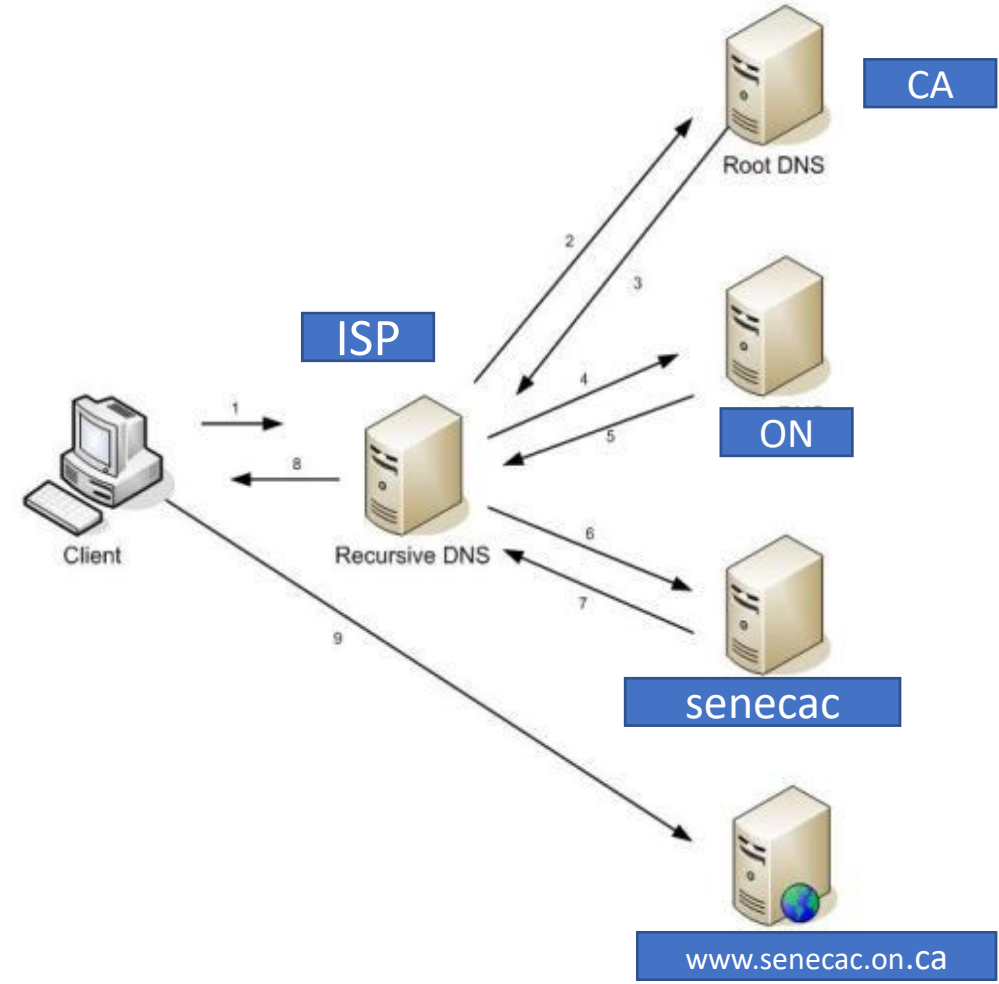


Schema and DNS



Schema and DNS-devam

- Bu örnekte, istemcinin `www.senecac.on.ca` çözümlemesi gerekiyor ancak ISP'nin DNS sunucusu `senecac` adresini bilmiyor.
- CA sunucusunun (kök sunucu) adresini biliyor. CA sunucusu ON sunucusuyla, ON sunucusu da `senecac` sunucusuyla iletişim kurar ve son olarak yanıt ISP'ye iletilir ve istemciye iletilir.



Aktif Dizin Yapısı ile Kullanıcılar ve Gruplar

- ***Yerel Kullanıcı Hesapları***

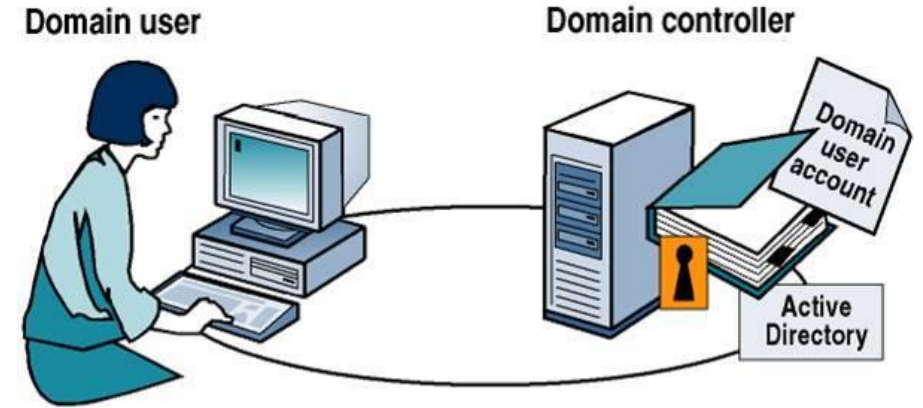
- Yerel bilgisayarda oluşturuldu
- Asla kopyalanmadı
- Etki alanı kaynaklarına erişim yok

- ***Etki Alanı Kullanıcı Hesapları***

- Etki alanı kaynaklarına erişmek için kullanılır
- Tüm DC'lere çoğaltıldı
- Alt küme Global Kataloğa kopyalandı

- ***Yerleşik Kullanıcı Hesapları***

- Yalnızca üye sunucuda veya bağımsız sunucuda oluşturulur
- DC'de yalnızca Yönetici ve Misafir oluşturuldu



Yönetici ve Konuk Hesapları

- Yalnızca yerel bilgisayardaki tüm dosya ve izinlerin tam kontrolü
- Etki Alanı Denetleyicisi
- Oluşturulduğu alanın tam kontrolü
- Etki alanının, kullanıcı hesaplarının, izinlerin, nesne oluşturma ve silmenin ve güvenlik politikasının tüm yönlerini yönetebilir
- Not: Yönetici hesabı hiçbir zaman silinemez ancak yeniden adlandırılabilir.
- Bir kullanıcının ağa geçici erişimi için kullanılır.
- Hesap silinmiyor.
- Güvenlik nedeniyle varsayılan olarak devre dışıdır.



- ***Yönetici Hesabını Yeniden Adlandırın***
- ***Güçlü bir şifre belirleyin***
- ***Yönetici şifresi bilgisini mümkün olduğunca az kişiyle sınırlandırın***
- ***Yönetici hesabını asla günlük aktiviteler için kullanmayın***

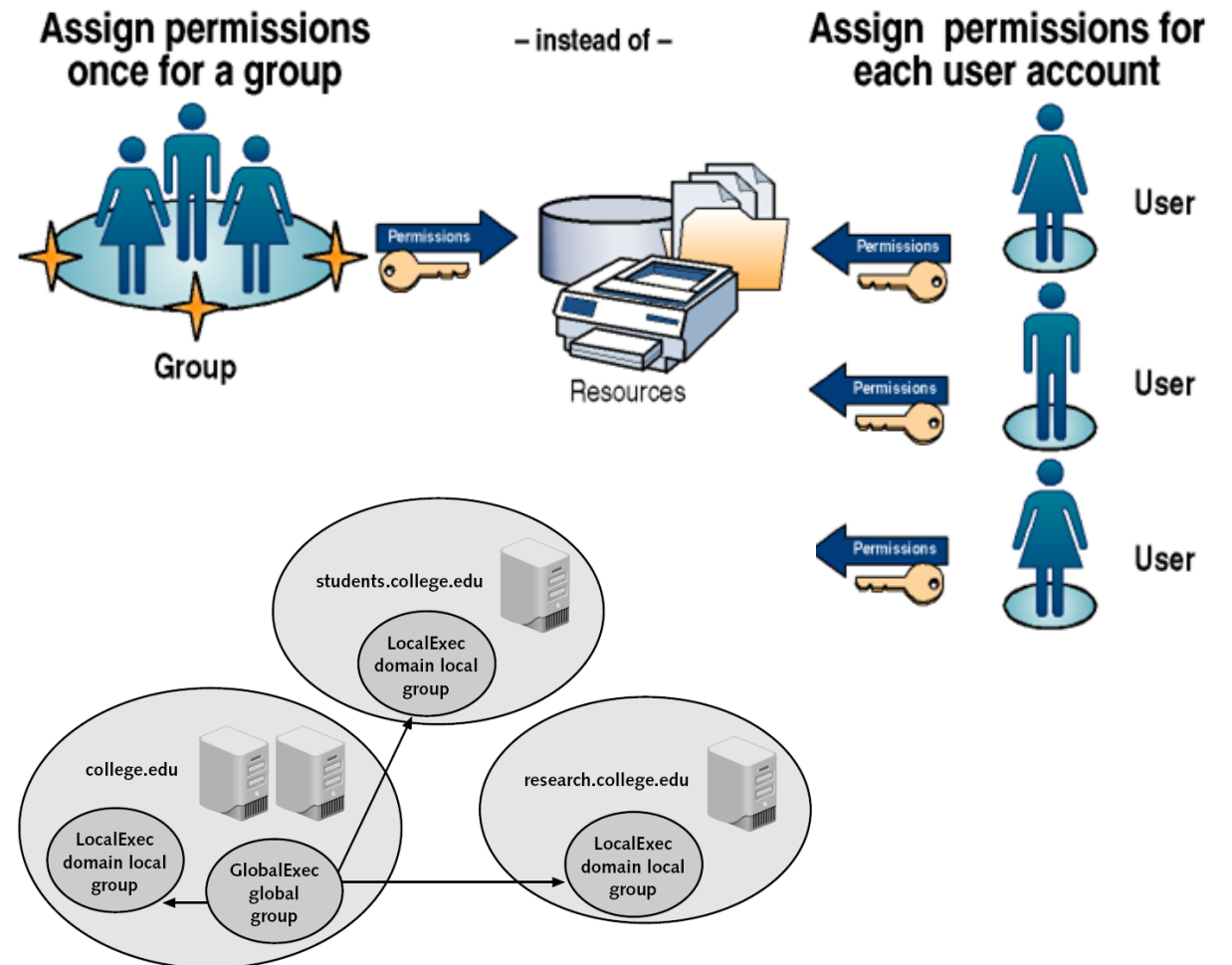
Grup Kavramı

- Kullanıcı hesaplarından oluşmaktadırlar.
- Üyeler gruplara girmek için izin verilirler.
- Kullanıcılar birden fazla grubun üyesi olabilirler.
- Gruplar başka gruplarında üyesi olabilirler.

➤ Domain Local Groups

► *Global Groups*

➤ *Universal Groups*



Aktif Dizin Saldırıları

- LLMNR POISONING
- Pass the Password ve Pass the Hash
- Gaining Shell Access
- SMB Relay
- LDAP Domain Dump
- Token Impersonation
- Kerberoasting

Aktif Dizin Güvenliđi iin Sıkılařtırma Yöntemleri

- Ortak Hesap Kullanan Kullanıcı Hesaplarının Tespit Edilmesi
- Uzun Süredir Oturum Açmamış Kullanıcı Hesaplarının Tespit Edilmesi
- Parolasını Hi Deđiřtirmemiş Olan Kullanıcı Hesaplarının Tespit Edilmesi
- Uzun Süredir Parolasını Deđiřtirmeyen Kullanıcı Hesaplarının Tespit Edilmesi
- Parolasını Deđiřtiremeyen Kullanıcı Hesaplarının Tespiti
- Süresi Geçmiş Kullanıcı Hesaplarının Tespit Edilmesi
- İsimlendirme Standardına Uymayan Kullanıcı Hesaplarının Tespit Edilmesi
- Kritik Gruplara Üye Olan Ortak Kullanılan Kullanıcı Hesaplarının Tespit Edilmesi
- Hibir Gruba Üye Olmayan Kullanıcı Hesaplarının Tespit Edilmesi
- Uzun Süredir Kullanılmayan Bilgisayar Hesaplarının Tespit Edilmesi
- “Computers” Konteynirında Bulunan Bilgisayar Hesaplarının Tespit Edilmesi
- İerisinde Nesne Bulunmayan Yapısal Birimlerin Tespit Edilmesi
- DNS Üzerinde Kaydedilmemiş Yerel Ağların Tespit Edilmesi