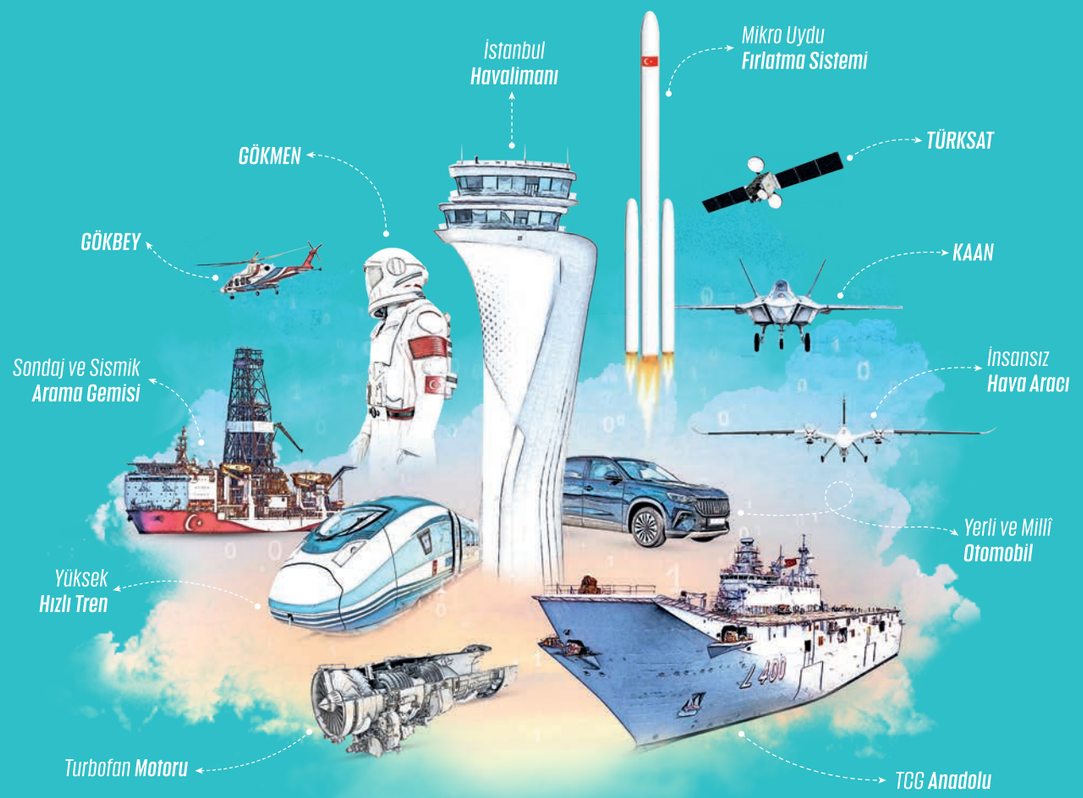
Bu kitaba sığmayan daha neler var!

eba
www.eba.gov.tr

Karekodu okut, bu kitapla ilgili EBA içeriklerine ulaş!

Teknoloji Yolculuğumuz



BU DERS KİTABI MİLLÎ EĞİTİM BAKANLIĞINCA ÜCRETSİZ OLARAK VERİLMİŞTİR.
PARA İLE SATILAMAZ.

ISBN: 978-975-11-7131-3

Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin Beşinci Maddesinin İkinci Fıkrası Çerçevesinde Bandrol Taşıması Zorunlu Değildir.

BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ PROJESİ

11-12

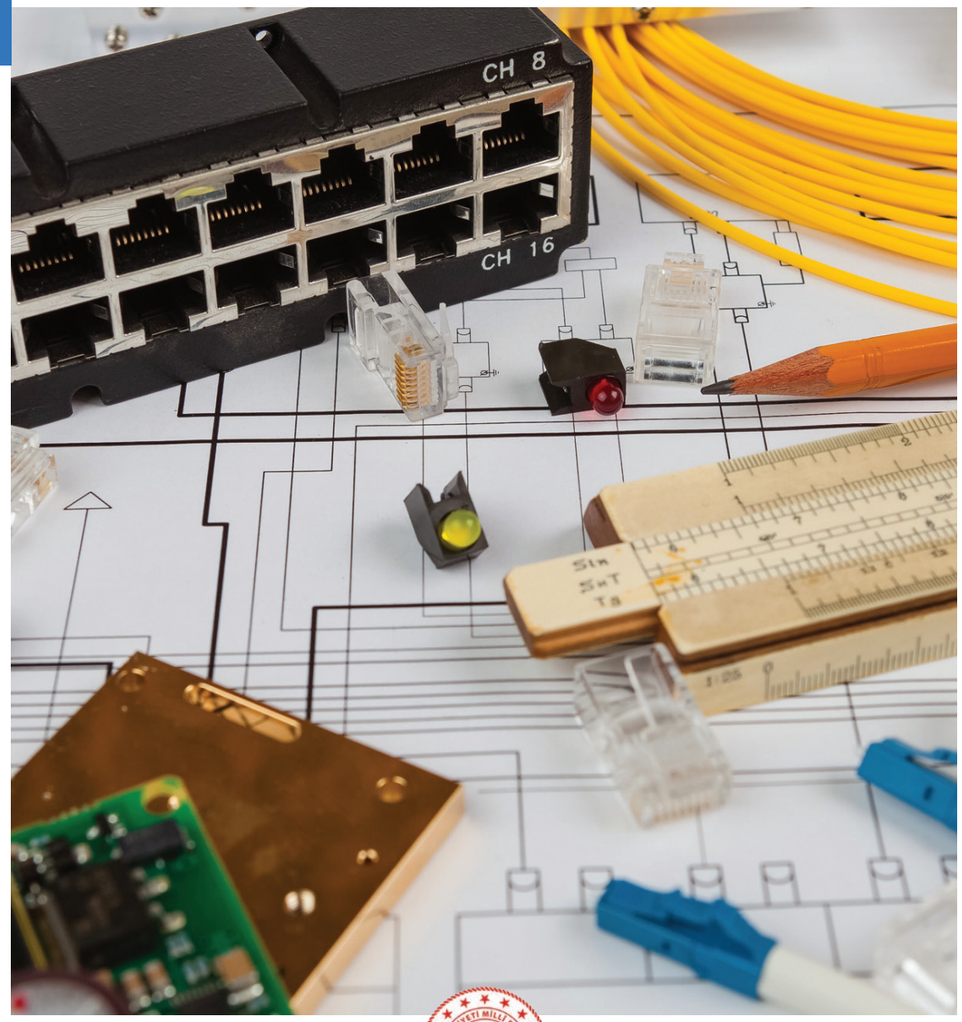
DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

11-12 DERS MATERYALİ

AĞ PROJESİ



MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

AĞ PROJESİ
11-12
DERS MATERYALİ

Yazarlar

Dr. Arzu KİLİTÇİ CALAYIR
Ahmet KARBUKAN
Murat KARATAŞ
Volkan ÇINAR

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI..... : 8346
YARDIMCI VE KAYNAK KİTAP DİZİSİ..... : 2238

Her hakkı saklıdır ve Millî Eğitim Bakanlığına aittir. Ders materyalinin metin, soru ve şekilleri kısmen de olsa hiçbir surette alınıp yayımlanamaz.

HAZIRLAYANLAR

Dil Uzmanı
Muhammet YILDIRIM

Program Geliştirme Uzmanı
Emel DOLDUR

Ölçme ve Değerlendirme Uzmanı
Hatice GÜRDİL EGE

Rehberlik Uzmanı
Ahmet ÖNAL

Görsel Tasarım Uzmanı
Cem Emrah GÜN

ISBN: 978-975-11-7131-3

Millî Eğitim Bakanlığının 24.12.2020 gün ve 18433886 sayılı oluru ile Meslekî ve Teknik Eğitim Genel Müdürlüğünce ders materyali olarak hazırlanmıştır.



İSTİKLÂL MARŞI

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.

Çatma, kurban olayım, çehreni ey nazlı hilâl!
Kahraman ırkıma bir gül! Ne bu şiddet, bu celâl?
Sana olmaz dökülen kanlarımız sonra helâl.
Hakkıdır Hakk'a tapan milletimin istiklâl.

Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim, bendimi çiğner, aşarım.
Yırtarım dağları, enginlere sığmam, taşarım.

Garbın âfâkını sarmışsa çelik zırhlı duvar,
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
Medeniyyet dediğin tek dişi kalmış canavar?

Arkadaş, yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayâsızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın;
Kim bilir, belki yarın, belki yarından da yakın.

Bastığın yerleri toprak diyerek geçme, tanı:
Düşün altındaki binlerce kefensiz yatanı.
Sen şehit oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da bu cennet vatanı.

Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Cânı, cânânı, bütün varımı alsın da Huda,
Etmesin tek vatanımdan beni dünyada cüda.

Ruhumun senden İlâhî, şudur ancak emeli:
Değmesin mabedimin göğsüne nâmahrem eli.
Bu ezanlar -ki şehadetleri dinin temeli-
Ebedî yurdumun üstünde benim inlemeli.

O zaman vecd ile bin secde eder -varsa- taşım,
Her cerîhamdan İlâhî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'şım;
O zaman yükselerek arşa değer belki başım.

Dalgalan sen de şafaklar gibi ey şanlı hilâl!
Olsun artık dökülen kanlarımın hepsi helâl.
Ebediyyen sana yok, ırkıma yok izmihlâl;
Hakkıdır hür yaşamış bayrağımın hürriyyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

Mehmet Âkif Ersoy

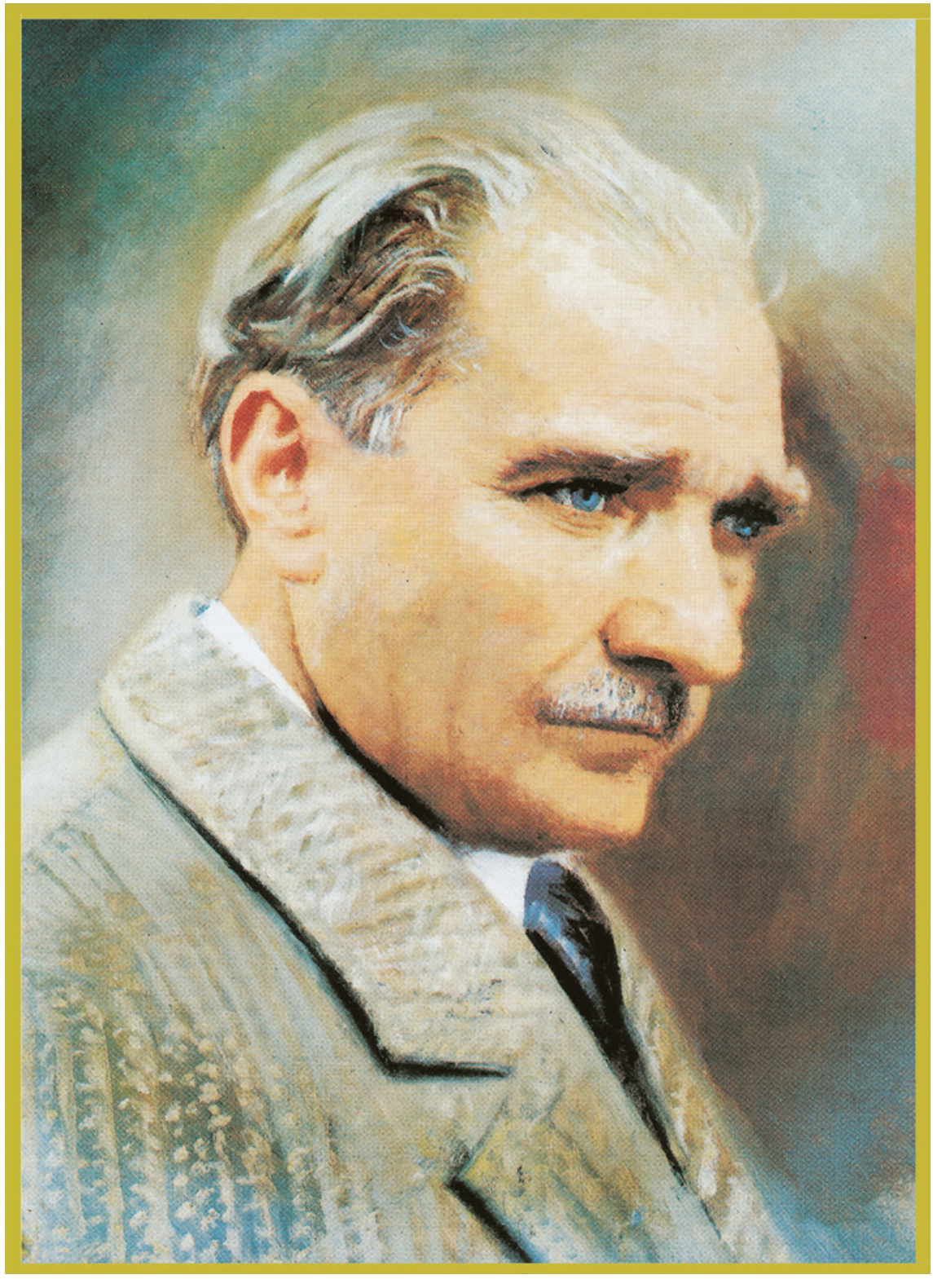
GENÇLİĞE HİTABE

Ey Türk gençliği! Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.

Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek dâhilî ve hâricî bedhahların olacaktır. Bir gün, istiklâl ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şeraitini düşünmeyeceksin! Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir. İstiklâl ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şeraitten daha elîm ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlîlerin siyasî emelleriyle tevhit edebilirler. Millet, fakr u zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklâl ve cumhuriyetini kurtarmaktır. Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

İÇİNDEKİLER

DERS MATERYALİNİN TANITIMI 11



1. ÖĞRENME BİRİMİ: PROJE HAZIRLIK 13
1.1. PROJE HAZIRLIK AŞAMALARI 14
1.2. PROJE UYGULAMA SÜRECİ 16
1.3. PROJE SONUÇ RAPORU 18
ÖLÇME VE DEĞERLENDİRME 20



2. ÖĞRENME BİRİMİ: AĞ SİSTEMLERİ PROJESİ HAZIRLAMA 21
2.1. PLANLAMA 22
2.1.1. Ölçeklenebilir Ağ Tasarımı 22
2.1.2. Ağ Tasarım İlkeleri 22
2.1.3. Yedekli Bağlantılar 23
2.1.4. Ölçeklenebilir Yönlendirme Protokolü 24
2.1.5. Arıza Etki Boyutunu Sınırlama 25
2.1.6. Anahtar Bloğu Dağıtımı 25
2.1.7. Bant Genişliğini Artırın 25
2.1.8. Erişim Katmanını Genişletme 26
2.1.9. Anahtar Donanımının Belirlenmesi 26
2.1.10. Yönlendirici Donanımının Belirlenmesi 26
2.2. KURULUM 27
2.2.1. Fiziksel Topoloji 27
2.2.2. Mantıksal IPv4 Ağ Topolojisi 27
2.3. TEST VE BAKIM 33
2.3.1. Sorun Giderme 46
2.4. RAPOR 55
2.4.1. Yönlendirici Cihaz Belgeleri 55
2.4.2. Anahtar Cihaz Belgeleri 56
2.4.3. Sistem Dokümantasyon Dosyaları 56
2.4.4. Veri Ölçümü 57
ÖLÇME VE DEĞERLENDİRME 58



3. ÖĞRENME BİRİMİ: AĞ CİHAZLARI YAPILANDIRMA PROJESİ 59
3.1. PLANLAMA ADIMLARI 60
3.2. YAPILANDIRMA ADIMLARI 61
3.2.1. IP Havuzu Yapılandırması ve DHCP Server Uygulaması 61
3.2.2. VLAN Oluşturulması 62
3.2.3. Erişim Kontrol Listelerinin Oluşturulması 63
3.2.4. Statik ve Dinamik Yönlendirme 64
3.2.5. Kablosuz LAN Bağlantısı 64
3.2.6. Ağ Güvenliği 69

3.2.7. Örnek Proje 70
3.3. TEST VE BAKIM ADIMLARI 80
3.3.1. Test Aşamaları 80
3.3.1. Ağ İzleme 82
3.4. PROJE RAPORU 84
ÖLÇME VE DEĞERLENDİRME 86

4. ÖĞRENME BİRİMİ: SUNUCU PROJESİ HAZIRLAMA 87
4.1. SUNUCU PROJESİ PLANLAMA AŞAMASI 88
4.1.1. Sunucu Seçimi ve Planlanması 88
4.1.2. Sunucu Odası Plan ve Raporlaması 90
4.2. SUNUCU İŞLETİM SİSTEMİ YAPILANDIRMASI 92
4.2.1. Active Directory Yapılandırması 92
ÖLÇME VE DEĞERLENDİRME 114

CEVAP ANAHTARLARI 115
KAYNAKÇA 116



Öğrenme biriminin adını gösterir.

Öğrenme biriminin numarasını gösterir.

Öğrenme biriminin konularını gösterir.

Öğrenme biriminde neler öğrenileceğini gösterir.

Öğrenme biriminin kavramlarını gösterir.

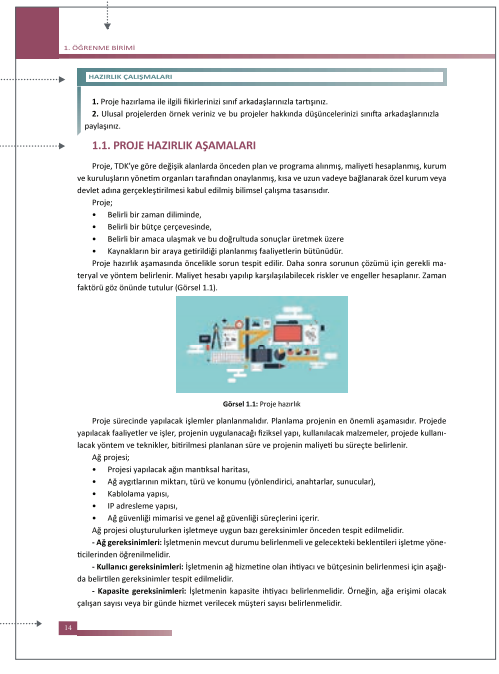


Öğrenme biriminin numarasını gösterir.

Derse başlamadan önce yapılacak hazırlıkları gösterir.

Alt konu başlıklarını gösterir.

Sayfa numarasını gösterir.



1. ÖĞRENME BİRİMİ

HAZIRLIK ÇALIŞMALARI

1. Proje hazırlama ile ilgili fikirlerinizi sınıf arkadaşlarınızla tartışınız.
2. Ulusal projelerden örnek veriniz ve bu projeler hakkında düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

1.1. PROJE HAZIRLIK AŞAMALARI

Proje, TDK'ye göre değişik alanlarda önceden plan ve programa alınmış, maliyeti hesaplanmış, kurum ve kuruluşların yönetim organları tarafından onaylanmış, kısa ve uzun vadeye bağlanarak özel kurum veya devlet adına gerçekleştirilmesi kabul edilmiş bilimsel çalışma tasarısıdır.

Proje;

- Belirli bir zaman diliminde,
- Belirli bir bütçe çerçevesinde,
- Belirli bir amaca ulaşmak ve bu doğrultuda sonuçlar üretmek üzere
- Kaynakların bir araya getirildiği planlanmış faaliyetlerin bütünüdür.

Proje hazırlık aşamasında öncelikle sorun tespit edilir. Daha sonra sorunun çözümü için gerekli materyal ve yöntem belirlenir. Maliyet hesabı yapılıp karşılaşılabilecek riskler ve engeller hesaplanır. Zaman faktörü göz önünde tutulur (Görsel 1.1).

Görsel 1.1: Proje hazırlık

Proje sürecinde yapılacak işlemler planlanmalıdır. Planlama projenin en önemli aşamasıdır. Projede yapılacak faaliyetler ve işler, projenin uygulanacağı fiziksel yapı, kullanılacak malzemeler, projede kullanılacak yöntem ve teknikler, bitirilmesi planlanan süre ve projenin maliyeti bu süreçte belirlenir.

Ağ projesi;

- Projesi yapılacak ağın mantıksal haritası,
- Ağ aygıtlarının miktarı, türü ve konumu (yönlendirici, anahtarlar, sunucular),
- Kablolama yapısı,
- IP adresleme yapısı,
- Ağ güvenliği mimarisi ve genel ağ güvenliği süreçlerini içerir.

Ağ projesi oluşturulurken işletmeye uygun bazı gereksinimler önceden tespit edilmelidir.

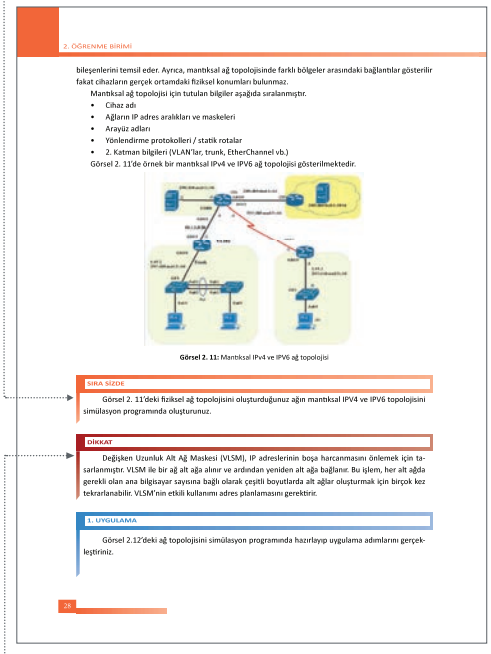
- **Ağ gereksinimleri:** İşletmenin mevcut durumu belirlenmeli ve gelecekteki beklentileri işletme yöneticilerinden öğrenilmelidir.
- **Kullanıcı gereksinimleri:** İşletmenin ağ hizmetine olan ihtiyacı ve bütçesinin belirlenmesi için aşağıda belirtilen gereksinimler tespit edilmelidir.
- **Kapasite gereksinimleri:** İşletmenin kapasite ihtiyacı belirlenmelidir. Örneğin, ağa erişimi olacak çalışan sayısı veya bir günde hizmet verilecek müşteri sayısı belirlenmelidir.

14

Konu içindeki öğrenci çalışmalarını gösterir.

Uygulama faaliyetlerini gösterir.

Öğrenme biriminin adını gösterir.



2. ÖĞRENME BİRİMİ

bileşenlerini temsil eder. Ayrıca, mantıksal ağ topolojisinde farklı bölgeler arasındaki bağlantılar gösterilir fakat cihazların gerçek ortamdaki fiziksel konumları bulunmaz.

Mantıksal ağ topolojisi için tutulan bilgiler aşağıda sıralanmıştır.

- Cihaz adı
- Ağların IP adres aralıkları ve maskeleri
- Arayüz adları
- Yönlendirme protokolleri / statik rotalar
- 2. Katman bilgileri (VLAN'lar, trunk, EtherChannel vb.)

Görsel 2. 11'de örnek bir mantıksal IPv4 ve IPV6 ağ topolojisi gösterilmektedir.

Görsel 2. 11: Mantıksal IPv4 ve IPV6 ağ topolojisi

SIRA SİZDE

Görsel 2. 11'deki fiziksel ağ topolojisini oluşturduğunuz ağın mantıksal IPV4 ve IPV6 topolojisini simülasyon programında oluşturunuz.

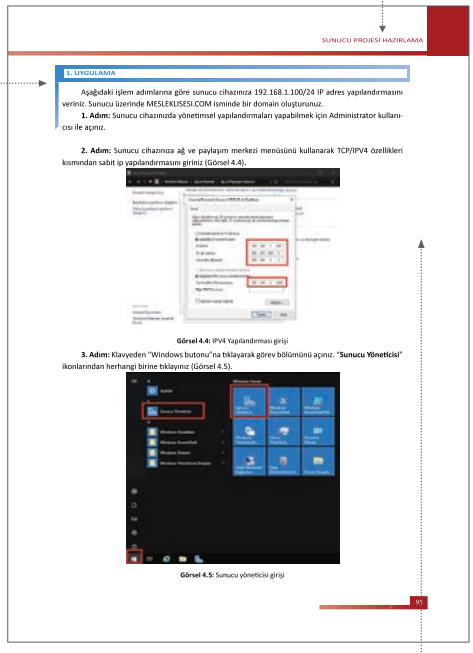
DİKKAT

Değişken Uzunluk Alt Ağ Maskesi (VLSM), IP adreslerinin boşa harcanmasını önlemek için tasarlanmıştır. VLSM ile bir ağ alt ağa alınır ve ardından yeniden alt ağa bağlanır. Bu işlem, her alt ağda gerekli olan ana bilgisayar sayısına bağlı olarak çeşitli boyutlarda alt ağlar oluşturmak için birçok kez tekrarlanabilir. VLSM'nin etkili kullanımı adres planlamasını gerektirir.

1. UYGULAMA

Görsel 2.12'deki ağ topolojisini simülasyon programında hazırlayıp uygulama adımlarını gerçekleştiriniz.

28



SUNUCU PROJESİ HAZIRLAMA

1. UYGULAMA

Aşağıdaki işlem adımlarına göre sunucu cihazınıza 192.168.1.100/24 IP adres yapılandırmasını veriniz. Sunucu üzerinde MESLEKLISESI.COM isminde bir domain oluşturunuz.

1. Adım: Sunucu cihazınızda yönetimsel yapılandırmaları yapabilmek için Administrator kullanıcısı ile açınız.

2. Adım: Sunucu cihazınıza ağ ve paylaşım merkezi menüsünü kullanarak TCP/IPV4 özellikleri kısmından sabit ip yapılandırmasını giriniz (Görsel 4.4).

Görsel 4.4: IPV4 Yapılandırması girişi

3. Adım: Klavyeden "Windows butonu"na tıklayarak görev bölümünü açınız. "**Sunucu Yöneticisi**" ikonlarından herhangi birine tıklayınız (Görsel 4.5).

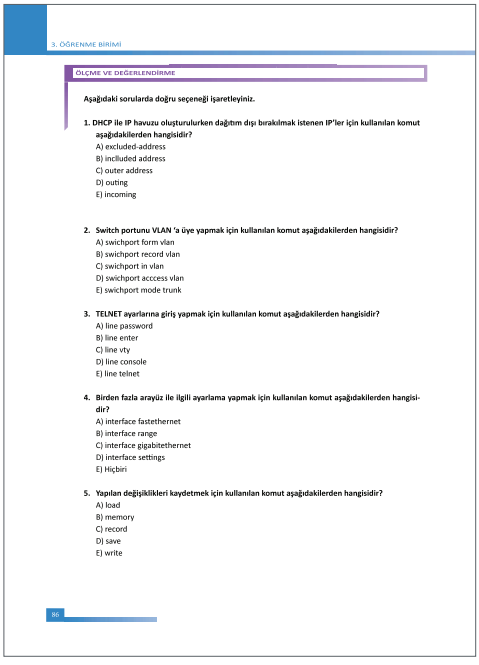
Görsel 4.5: Sunucu yöneticisi girişi

95

Konu içinde dikkat edilmesi gereken yerleri gösterir.

Etkileşimli kitap, video, ses, animasyon, uygulama, oyun, soru vb. kaynaklara ulaşılabilecek link ve karekodu gösterir.

Ölçme ve değerlendirme sayfasını gösterir.



3. ÖĞRENME BİRİMİ

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçeneği işaretleyiniz.

1. DHCP ile IP havuzu oluşturulurken dağıtım dışı bırakılmak istenen IP'ler için kullanılan komut aşağıdakilerden hangisidir?
A) excluded-address
B) incluided address
C) outer address
D) outing
E) incoming

2. Switch portunu VLAN 'a üye yapmak için kullanılan komut aşağıdakilerden hangisidir?
A) swichport form vlan
B) swichport record vlan
C) swichport in vlan
D) swichport acccess vlan
E) swichport mode trunk

3. TELNET ayarlarına giriş yapmak için kullanılan komut aşağıdakilerden hangisidir?
A) line password
B) line enter
C) line vty
D) line console
E) line telnet

4. Birden fazla arayüz ile ilgili ayarlama yapmak için kullanılan komut aşağıdakilerden hangisidir?
A) interface fastethernet
B) interface range
C) interface gigabitethernet
D) interface settings
E) Hiçbiri

5. Yapılan değişiklikleri kaydetmek için kullanılan komut aşağıdakilerden hangisidir?
A) load
B) memory
C) record
D) save
E) write

86

1. ÖĞRENME BİRİMİ
PROJE HAZIRLIK

KONULAR

1.1. PROJE HAZIRLIK AŞAMALARI
1.2. PROJE UYGULAMA SÜRECİ
1.3. PROJE SONUÇ RAPORU

NELER ÖĞRENECEKSİNİZ?

- Proje kavramı
- Ağ projesi hazırlık aşaması
- Ağ projesi uygulama süreci
- Rapor yazımı

TEMEL KAVRAMLAR
Proje, Proje süreci, Proje raporu



HAZIRLIK ÇALIŞMALARI

1. Proje hazırlama ile ilgili fikirlerinizi sınıf arkadaşlarınızla tartışınız.

2. Ulusal projelerden örnek veriniz ve bu projeler hakkında düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

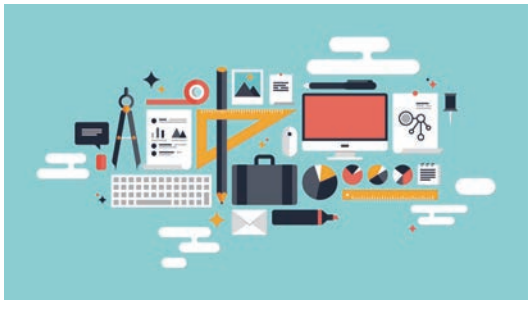
1.1. PROJE HAZIRLIK AŞAMALARI

Proje, TDK'ye göre değişik alanlarda önceden plan ve programa alınmış, maliyeti hesaplanmış, kurum ve kuruluşların yönetim organları tarafından onaylanmış, kısa ve uzun vadeye bağlanarak özel kurum veya devlet adına gerçekleştirilmesi kabul edilmiş bilimsel çalışma tasarısıdır.

Proje;

- Belirli bir zaman diliminde,
- Belirli bir bütçe çerçevesinde,
- Belirli bir amaca ulaşmak ve bu doğrultuda sonuçlar üretmek üzere
- Kaynakların bir araya getirildiği planlanmış faaliyetlerin bütünüdür.

Proje hazırlık aşamasında öncelikle sorun tespit edilir. Daha sonra sorunun çözümü için gerekli materyal ve yöntem belirlenir. Maliyet hesabı yapılıp karşılaşılabilecek riskler ve engeller hesaplanır. Zaman faktörü göz önünde tutulur (Görsel 1.1).



Görsel 1.1: Proje hazırlık

Proje sürecinde yapılacak işlemler planlanmalıdır. Planlama projenin en önemli aşamasıdır. Projede yapılacak faaliyetler ve işler, projenin uygulanacağı fiziksel yapı, kullanılacak malzemeler, projede kullanılacak yöntem ve teknikler, bitirilmesi planlanan süre ve projenin maliyeti bu süreçte belirlenir.

Ağ projesi;

- Projesi yapılacak ağın mantıksal haritası,
- Ağ aygıtlarının miktarı, türü ve konumu (yönlendirici, anahtarlar, sunucular),
- Kablolama yapısı,
- IP adresleme yapısı,
- Ağ güvenliği mimarisi ve genel ağ güvenliği süreçlerini içerir.

Ağ projesi oluşturulurken işletmeye uygun bazı gereksinimler önceden tespit edilmelidir.

- Ağ gereksinimleri: İşletmenin mevcut durumu belirlenmeli ve gelecekteki beklentileri işletme yöneticilerinden öğrenilmelidir.

- Kullanıcı gereksinimleri: İşletmenin ağ hizmetine olan ihtiyacı ve bütçesinin belirlenmesi için aşağıda belirtilen gereksinimler tespit edilmelidir.

- Kapasite gereksinimleri: İşletmenin kapasite ihtiyacı belirlenmelidir. Örneğin, ağa erişimi olacak çalışan sayısı veya bir günde hizmet verilecek müşteri sayısı belirlenmelidir.

- **Amaç:** Ağın kullanımdaki amaçlarının belirlenmesidir. Örneğin, ağ üzerinden çalıştırılacak yazılım, yazıcı, depolama birimleri ve sayıları gibi unsurlar belirlenmelidir.

- **Performans gereksinimleri:** İşletmenin ağ kullanımında ihtiyaç duyduğu hız gibi unsurların belirlenmesidir. Örneğin, ağ üzerinde cihazlar arasında kabul edilebilir yanıt süreleri belirlenmelidir.

- **Konum gereksinimi:** Ağ projesinin uygulanacağı fiziki yapının belirlenmesidir. Örneğin, hepsi tek bir ofiste, birden fazla binada veya uzaktan çalışanların fiziki yapı koşulları belirlenmelidir.

- **Zaman kısıtlayıcıları:** Projenin uygulama süresidir. Örneğin, proje için gereken süre bir ay olarak belirlenebilir.

- **Bütçe kısıtlamaları:** Proje için ayrılabilecek bütçe miktarıdır. Örneğin, gerekli hizmeti sağlamak için harcanabilecek maksimum miktar hesaplanmalıdır.

- **Teknik gereksinim:** Kullanıcı gereksinimlerine göre kullanıcı sayısı, bilgisayar, yazıcı gibi son kullanıcı cihazları, depolama çözümleri, yazılım ve bant genişliği ihtiyacı gibi teknik ihtiyaçların belirlenmesidir.

Uygulanacak ağ projesinin gereksinimleri belirlendikten sonra ağ yapısının uygulanacağı yerin fiziki yapısı (ofisler, cihaz odaları gibi mimarı durumu) çizilmelidir. Bu fiziki yapı içinde bilgisayarların, yazıcı vb. cihazların bulundukları noktalar tespit edilmelidir. Fiziki yapının durumuna ve bilgisayar gibi cihazların konumuna göre kullanılacak switch (anahtar), repeater (tekrarlayıcı), router (yönlendirici), Firewall (güvenlik duvarı), modem, wireless cihazlarının konumu belirlenmelidir. Modem ve yönlendirici gibi cihazlar mümkün olduğunca binanın fiziki yapısına göre merkez noktaya yakın konumlandırılmalıdır. Böylece ağ cihazlarından diğer uç birimlere çekilecek kablo mesafesi kısalmış olur. Kullanılacak kablo metrajı ve konnektör sayıları belirlenir.

DİKKAT

Kablo mesafesinin uzunluğu arttıkça sinyal kayıplarına sebep olur.

Kablolamanın planı çizilmeden önce hangi ağ topolojisi kullanılacağı belirlenmelidir. Belirlenen topoloji yapısına uygun kablolamanın nasıl yapılacağı, hangi odaya kaç tane uç bırakılması gerektiği, kablonun çekileceği hat projesinin uygulanacağı fiziki yapının planı çizilmelidir. Plan hazırlanırken işletmenin büyüme stratejisine göre kullanılacak cihazlar ve ağa sonradan çeşitli cihazların eklenebileceği göz önünde bulundurulmalıdır.

Kablolama planı belirlendikten sonra ağ yapısında alt ağlar oluşturulup oluşturulmayacağı belirlenmeli ve buna göre IP adresi dağıtımı hazırlanmalıdır.

Ağ projesi için hazırlanan tüm dokümanlara göre alınacak donanım, yazılım gibi ekipmanlar listelenmeli ve fiyatlandırılarak proje bütçesi belirlenmelidir.

Projenin ne kadar sürede gerçekleştirileceği, olası aksaklıklar göz önünde tutularak belirlenmelidir.

1. UYGULAMA

Yeni açılan işletmenin bir bina içinde üç odası vardır. Bu odalardan ikisi ofis olarak kullanılmaktadır. Ofislerde beş çalışan ve bilgisayarlar bulunmaktadır. Çalışanların bir ağ yazıcısı üzerinden çıktıları almaları gerekmektedir. İşletmenin ağ projesi için planlama işlemlerini yapınız.

1. Adım: Öncelikle fiziksel topolojide çalışan bilgisayarların konumlarını belirleyiniz.

2. Adım: Fiziksel topolojideki bilgisayar konumlarına göre anahtar ve modemin konumlarını belirleyiniz.

3. Adım: Anahtar, bilgisayarlar ve yazıcı arasında yapılacak kablolama hatlarını çiziniz ve kablo mesafesini ölçünüz.

4. Adım: Projenin yaklaşık tamamlama süresini hesaplayınız.

5. Adım: Projesi alınacak cihazların fiyatlarını ve projenin işçilik maliyetini hesaplayarak proje bütçesini çıkarınız.

SIRA SİZDE

1. uygulama için alınacak cihazları, cihaz adedi ve fiyatlarını aşağıda örneği verilen Tablo 1.1'deki gibi oluşturarak proje bütçesini hesaplayınız.

Tablo 1.1 : Proje Bütçesi

Sıra No	Cihaz ve Malzeme Adı	Adedi	Birim Fiyatı	Toplam Fiyat
1	Anahtar	2	..... ₺	..... ₺
2	Modem	1	..... ₺	..... ₺
...	Cat 6 kablo	100 m	..... ₺	..... ₺
...	.....			
...	İşçilik			..... ₺
			Genel Toplam	..... ₺

1.2. PROJE UYGULAMA SÜRECİ

Proje uygulama süreci, planlanan ve faaliyetleri belirlenen projenin bu planlara göre faaliyetlerinin izlenerek gerçekleştirilmesi aşamasıdır.

Proje ürününün teslim edilmesi sürecinde, proje ürün hizmeti işletmenin kullanabileceği şekilde oluşturulur veya mevcut sisteme entegre edilir. Gerekli olan kullanıcı eğitimleri, pilot uygulamalar, denemeler bu aşamada hayata geçirilir ve işletmeden onay alınır.

İşletmenin durumu ve ihtiyacına göre proje planı hazırlandıktan sonra bu planda belirlenen işlemler sırasıyla uygulanmalıdır. Bu uygulama süreci aşamaları aşağıda sıralanmıştır.

a) Proje uygulama sürecinde öncelikle projede kullanılacak anahtar, yönlendirici, modem gibi donanımlar temin edilmelidir.

b) Donanımlar temin edildikten sonra projenin uygulanacağı fiziki yapıya göre cihazların montajı yapılmalıdır.

c) Donanımların montajları tamamlandıktan sonra topolojiye uygun olarak yapısal kablolama işlemleri yapılmalıdır.

ç) Ağ topolojisine ve varsa alt ağlara uygun IP yapılandırma bilgileri girilmelidir.

d) Anahtar, yönlendirici, Wi-Fi, modem yapılandırmaları tamamlanmalıdır.

e) Güvenlikle ilgili ayarlar yapılmalıdır.

f) Yapılandırmalar test edilmeli ve varsa hatalı olanlar düzeltilmelidir.

Proje uygulama sürecinde gerekli donanım malzemelerinin temini ve montajından sonra yapısal kablolama işlemi gerçekleştirilir.

Ağ sistemlerinin kesintisiz sağlanması ve problemlerin hızlı çözülebilmesi için yapısal kablolama doğru planlanmalıdır. Yapılan bu plana göre kablolama uygulanmalıdır. Yapısal kablolama, ağ sistemlerinde uzun süreli kullanılan sistem elemanıdır. Kullanılan veri kablolarından bina mimarisine kadar pek çok değişken mevcuttur. İhtiyaçlara uygun ve doğru malzemelerle kurulan sistemlerin gelişen ihtiyaçlara da cevap ve-

rebilecek şekilde planlanması gerekir.

Yapısal kablolamanın avantajları şunlardır:

- Kablolama arızaları kısa sürede tespit edilip giderilebilir.
- Gelişen ağ ihtiyaçlarına hızlı cevap verebilir.
- Ses ve veri iletişim maliyetleri azaltılabilir.

Çok yönlü kullanıma izin verdiği için ihtiyaç duyulan intranet, video konferans, IP telefonu vb. uygulamaları destekler. Bilgisayar, yazıcı, güvenlik kamerası vb. aktif sistemler aynı kablolama üzerinde çalışabilir.

Yapısal kablolama işleminin tamamlanmasından sonra mutlaka test işlemleri gerçekleştirilmelidir. Bu test işlemlerinde tüm kablolamanın sorunsuz olduğu ve haberleşmenin sağlandığı teyit edilmelidir.

Son kullanıcıların bilgisayar, yazıcı gibi cihazlarına ait IP yapılandırması elle girilecekse ağ topolojisine uygun olarak belirlenen IP adresleri yapılandırma bilgileri girilmelidir. Otomatik olarak atanacaksa cihazların ayarları kontrol edilmelidir.

Anahtar, yönlendirici, Wi-Fi gibi ağ cihazlarının gerekli yapılandırma işlemleri sırayla yapılmalıdır. Yapılandırma işlemleri tamamlandıktan sonra ayarlar kontrol edilmelidir. Herhangi bir sorun varsa ayarlarda gerekli düzeltmeler yapılarak sorun giderilmelidir.

Gerekli güvenlik ayarları, kullanıcı erişim izinleri ayarlanmalıdır. Güvenlik ayarları, yetkisiz kullanıcıların sistem ayarlarına erişimi ve değişiklik yapması engellenecek şekilde ayarlanmalıdır.

Tüm uygulama sürecinin sonunda hazırlanan sistem genel olarak kontrol edilmelidir. Bu kontrol esnasında ağ sistemine dâhil tüm cihazların çalışmaları ve haberleşmelerinde sorun olup olmadığı test edilmelidir. Olası sorunlar giderilmelidir. Ağ sisteminin genişleyeceği düşünülerek yeni kullanıcı ve cihaz eklenmesi durumu da kontrol edilmelidir.

2. UYGULAMA

Yeni açılan işletmenin bir bina içinde üç odası vardır. Bu odalardan ikisi ofis olarak kullanılmaktadır. Ofislerde beş çalışan ve bilgisayarlar bulunmaktadır. Bir ağ yazıcısı üzerinden çıktıların alınması gerekmektedir. İşletmenin ağ projesi için uygulama süreci işlemlerini yapınız.

1. Adım: Plana uygun donanım cihazlarını temin ediniz.

2. Adım: Temin edilen cihazların sağlamlığını kontrol ediniz.

3. Adım: Uygulama süreci boyunca kullanacağınız ekipmanlarınızı hazırlayınız ve kontrol ediniz.

4. Adım: Planladığınız çalışmaya göre bilgisayar ve diğer ağa bağlanacak cihazların konumlarının doğruluğunu kontrol ediniz.

5. Adım: Anahtar ve modemin belirlediğiniz konumlara montajını yapınız.

6. Adım: Anahtar, bilgisayarlar ve yazıcı arasında belirlediğiniz hatlara uygun kablolama işlemlerini yapınız. Hazırladığınız her kablonun çalışmasını ölçü aletinizle test ediniz.

7. Adım: Modemin gerekli ayarlarını yapınız.

8. Adım: IP yapılandırmalarını giriniz.

9. Adım: Yazıcının ağa dâhil edilme ve yazdırma ayarlarını yapınız.

10. Adım: İşlemlerinizi tamamladıktan sonra gerekli kontrolleri yapınız ve cihazların çalışma raporlarını alınız.

1.3. PROJE SONUÇ RAPORU

Proje raporu, seçilen konu hakkında başlangıçtan bitişe kadar yapılan her türlü bilimsel çalışmanın (araştırma, gözlem, deney) ürünüdür. Bu rapor; belirlenen problemin çözümü için gerekli ve geçerli verilerin neler olduğunu, onun çözümü için izlenen yolu ve elde edilen verilerin değerlendirilmesi ile ulaşılan sonuçları ortaya çıkartır.

Proje raporu yazımında dikkat edilmesi gerekenler aşağıda sıralanmıştır.

a) Gözlem ve ölçüm sonuçları yazılarak kaydedilmelidir.

b) Proje raporunda gereksiz ayrıntılara girilmemelidir.

c) Rapor olabildiğince öz ve anlaşılır olmalıdır.

Ağ projesi uygulama sürecinin sonunda yapılan kontrollerle sistemin çalıştığı tespit edilerek tüm proje süreci boyunca yapılan işlemler raporlanmalıdır. Ağ projesinin planlamasının nasıl yapıldığı, yapısal kablolama şeması, IP yapılandırma bilgileri, anahtar, yönlendirici gibi ağ cihazlarının ayarları, test sonuçları proje raporunda yer almalıdır. Özellikle yapısal kablolama şeması ve ağ cihazlarından alınan sistem dokümantasyonlarının çıktıları mutlaka eklenmelidir.

Ağ proje raporu genel olarak şu başlıkları içermelidir:

1. Projenin Adı: Projenin adı ve hangi işletmeye yapılacağı yazılır.

2. Projenin Amacı: Bu bölümde proje çalışması ile neyin amaçlandığı kısaca açıklanır. Uygun ise amaçlar maddeler hâlinde sıralanabilir.

3. Proje Planlaması: Proje çalışmasında mevcut durum ve yapılacak işlemler açıklanır. Mümkünse işlemler basamaklar hâlinde verilir.

4. Proje Uygulama Süreci: Proje uygulama sürecinde yapılan işlemler maddeler hâlinde belirtilmelidir. Anahtar, yönlendirici gibi cihaz yapılandırmaları eklenmelidir.

5. Test ve Sonuç: Proje uygulama sürecinin sonunda yapılan test işlemleri yazılır. Cihazlardan alınan sonuçlar eklenmelidir.

3. UYGULAMA

Yeni açılan işletmenin bir bina içinde üç odası vardır. Bu odalardan ikisi ofis olarak kullanılmaktadır. Ofislerde beş çalışan ve bilgisayarlar bulunmaktadır. Bir ağ yazıcısı üzerinden çalışanların çıktıları almaları gerekmektedir. İşletmenin ağ projesi için rapor hazırlama işlemlerini yapınız.

1. Adı: Projenizin adını veriniz (..... İşletmesi Ağ Projesi Raporu).

2. Adım: Projenin amacını yazınız (Yeni açılan işletmenin ağ altyapısı planlanıp gerekli kurulum ve ayarlar yapılacaktır.).

3. Adım: Projesi yapılacak işin mevcut durumu ve yapılması planlanan işlemleri yazınız.

*** Mevcut durum**

- İki ofiste beş tane bilgisayar ve bir tane ağ yazıcısı vardır.
- Ağ altyapısına ait hiçbir ekipman ve çalışma yoktur.
- İşletmenin bulunduğu bölgede VDSL internet altyapısı vardır.

*** Yapılacak İşlemler**

- İnternet bağlantısı için bir adet VDSL destekli wireless özelliği olan modem temin edilip kurulumu yapılacaktır.
- Bilgisayar ve yazıcının ağ bağlantıları için bir adet 8 portluk anahtar temin edilecek ve kurulumu yapılacaktır.
- Gerekli olan yapısal kablolama işlemleri UTP CAT6 kablo kullanılarak yapılacaktır.
- IP yapılandırma işlemleri tamamlanacaktır.
- Wireless ayarları yapılacaktır.
- Yazıcının ağ üzerinden yazdırması için gerekli ayarlar yapılacaktır.
- Yapılan işlemler test edilerek kontrolü sağlanacaktır.

4. Adım: Proje uygulama sürecinde yapılan işlemleri maddeler hâlinde yazınız.

- Belirlenen modem ve anahtar temin edildi.
- Modem ve anahtarın belirlenen konumlara montajı yapıldı.
- Modemin internet bağlantıları yapılıp gerekli ayarları yapıldı.
- Modemle anahtar arasında kablolama işlemi yapıldı.
- Anahtarla bilgisayarlar arasındaki yapısal kablolama işlemleri sırayla yapıldı ve kabloların sağlamlığı ölçü aleti ile kontrol edildi.
- Anahtarla yazıcı arasındaki kablolama işlemi yapıldı ve kablonun sağlamlığı ölçü aleti ile kontrol edildi.
- Yazıcının IP yapılandırması girildi ve ayarları yapıldı.
- Bilgisayarların IP yapılandırmaları girildi ve ağın sorunsuz bir şekilde bağlantılarının kontrolü yapıldı.
- Bilgisayarların yazıcı ile bağlantısı ve gerekli yazdırma ayarları yapıldı.
- Modemin wireless ayarları yapıldı.

5. Adım: Proje uygulama sürecinin sonunda yapılan test işlemleri ve sonuçlarını ekleyiz.

- Yapılan işlemler kontrol edilerek sorun olmadığı teyit edildi.
- Cihazların çalışma raporları yazdırıldı ve rapora eklendi.
- Kullanıcılara gerekli bilgilendirmeler yapıldı.
- Modem, yazıcı ve wireless ile ilgili kullanıcı adı, şifre gibi bilgiler rapor dosyasına eklendi.

SIRA SİZDE

Yeni açılan işletmenin bir bina içinde dört odası vardır. Bu odalardan biri müdür odası, ikisi çalışanların ofisi, biri de çok amaçlı ofis olarak kullanılmaktadır. Müdür odasında müdürün kullanımı için bir bilgisayar vardır. İki ofiste sekiz çalışan için bilgisayarlar ve bir ağ yazıcısı vardır. Çok amaçlı salonda sunum yapmak üzere bir bilgisayar bulunmaktadır. İşletmenin ağ projesi için proje hazırlık, uygulama süreci ve raporlama işlemlerini yapınız.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçeneği işaretleyiniz.

1. Problem belirlenirken aşağıdakilerden hangisi dikkat edilmesi gereken noktalardan biri değildir?

A) İlgi çekici olmalıdır.
B) Çözebilecek yeterlilikte olunmalıdır.
C) Konusu soyut olmalıdır.
D) Çözüm yöntemi olmalıdır.
E) Yeterli kaynak materyal bulunmalıdır.

2. Proje hazırlamak için yapılacak ilk basamak aşağıdakilerden hangisidir?

A) Hipotez kurma
B) Materyal toplama
C) Planlama yapma
D) Problemleri tespit etme
E) Yöntem ve teknikleri belirleme

3. Aşağıdakilerden hangisinin projede bulunması gerekmez?

A) Bilimsellik
B) İnsan
C) Kalite
D) Maliyet
E) Zaman

4. "Her problemin çözümü belli bir sürece bağlıdır." ifadesiyle problem çözmenin aşağıda verilen hangi özelliği üzerinde durulmaktadır?

A) Zaman
B) Orijinalliği
C) Kaynak bulunması
D) Maliyeti
E) Güncelliği

2. ÖĞRENME BİRİMİ
PROJE HAZIRLIK

KONULAR

2.1. PLANLAMA

2.2. KURULUM

2.3. TEST VE BAKIM

2.4. RAPOR

NELER ÖĞRENECEKSİNİZ?

- Ağ planlaması ve tasarımı
- Fiziksel ve mantıksal topoloji
- Test ve bakım süreçleri
- Rapor yazımı

TEMEL KAVRAMLAR

Ağ tasarımı, Topoloji,Katmanlı mimari, Yönlendirici, Anahtar



HAZIRLIK ÇALIŞMALARI

1. Topoloji nedir, topoloji çeşitleri nelerdir?
2. IP ve değişen uzunluklu maske (VLSM) nedir?

2.1. PLANLAMA

İnsanların ve nesnelerin birbiriyle iletişim kurduğu günümüz dünyasında verilerin farklı ortam ve cihazlardan kesintisiz ulaşılabilir olması beklenmektedir. Bu beklentiler güvenli, güvenilir ve yüksek seviyede kullanılabilen yeni nesil ağ tasarımlarının yapılmasını gerektirmektedir.

Yeni nesil ağlar sadece mevcut beklenti ve ekipmanları desteklememeli, aynı zamanda eski platformlarla da bütünleşik çalışabilmelidir.

2.1.1. Ölçeklenebilir Ağ Tasarımı

İşletmeler, kritik görev hizmetleri sağlamak için ağ altyapılarına giderek daha fazla ihtiyaç duymaktadır. Özellikle işletmeler büyüdükçe ve geliştikçe daha fazla çalışanı işe alır, şubeler açar ve küresel pazarlara açılabilir. Bu değişiklikler, işletmenin ihtiyaçlarını karşılamak için ölçeklendirilebilmesi gereken bir ağın gereksinimlerini de ortaya koyar.

Ölçeklenebilirlik; kullanılabilirlik ve güvenilirliği kaybetmeden büyüyebilen bir ağ için kullanılan terimdir. Büyük, orta veya küçük bir ağı desteklemek için ağ tasarımcısının ağın kullanılabilir olmasını sağlamalıdır. Etkin ve kolay ölçeklendirilebilmesi için ağ tasarımcısının bir strateji geliştirmesi gerekir. Temel bir ağ tasarım stratejisine gerekenler aşağıda sıralanmıştır.

- Yetenekleri artırmak için kolayca yükseltilebilen, genişletilebilir modüler ekipman veya kümelenmiş cihazlar kullanınız.
- Ağın diğer işlevsel alanlarının tasarımını etkilemeden gerektiğinde eklenebilen, yükseltilebilen ve değiştirilebilen modülleri içeren hiyerarşik bir ağ tasarlayınız.
- Hiyerarşik bir IPv4 ve IPv6 adres stratejisi oluşturunuz. Dikkatli yapılan mantıksal adres planlaması, ek kullanıcıları ve hizmetleri desteklemek için ağı yeniden adresleme ihtiyacını ortadan kaldıracaktır.
- Yayınları sınırlandırmak ve ağdan gelen diğer istenmeyen trafiği filtrelemek için yönlendiricileri veya çok katmanlı anahtarları seçiniz. Ağ çekirdeğine giden trafiği filtrelemek ve azaltmak için üçüncü katman aygıtlarını kullanınız.

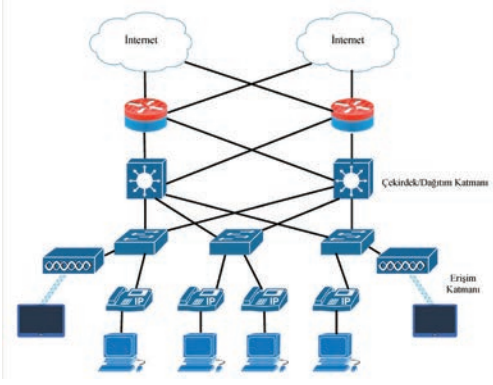
2.1.2. Ağ Tasarım İlkeleri

Ağ tasarımında en yüksek düzeyde kullanılabilirlik, esneklik, güvenlik ve yönetilebilirlik sağlamak için ağ tasarım ilkelerinin kullanılmasını gerekir. Ağ tasarımları hem mevcut hem de gelecekteki hizmet ve teknoloji gereksinimlerini karşılamalıdır. Ağ tasarımında dikkat edilemesi gereken tasarım ilkeleri aşağıda sıralanmıştır.

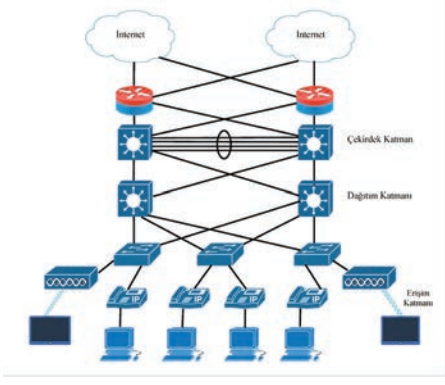
- **Hiyerarşik:** Hiyerarşik tasarım her bir katmanda yer alan cihazın görevinin anlaşılmasını kolaylaştırır. Aynı zamanda yönetimi kolaylaştırır.
- **Modülerlik:** Modüler tasarım, isteğe bağlı olarak kesintisiz ağ genişlemesinin yapılmasına ve farklı hizmetlerin ağda etkinleştirilmesine olanak sağlar.
- **Dayanıklılık:** Ağın her zaman çalışabilir olması için kullanıcı beklentilerini karşılar.

- **Esneklik:** Ağ kaynaklarını kullanarak ağ trafik yükünün paylaşımına izin verir.

Katmanlı tasarımlardaki üç önemli katman; erişim, dağıtım ve çekirdek katmanıdır (Görsel 2.1, Görsel 2.2).



Görsel 2. 1: İki katmanlı model



Görsel 2. 2: Üç katmanlı model

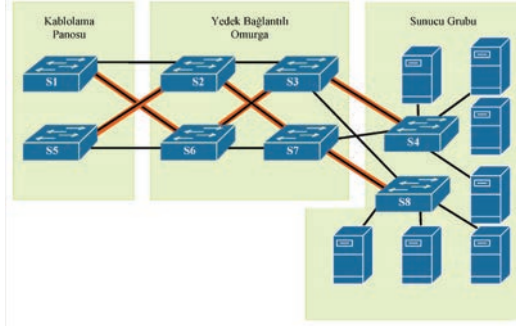
Erişim Katmanı: Erişim katmanının öncelikli amacı kullanıcıya ağ erişimi sağlamaktır. Erişim katmanı anahtarları yönlendirme, hizmet kalitesi ve güvenlik gibi temel ağ gereksinimlerine cevap veren dağıtım katmanı anahtarlarına bağlanır.

Dağıtım Katmanı: Bu katman, erişim katmanıyla çekirdek katmanı arasında bağlantı sağlar. Son kullanıcıya yedek dağıtım katmanı anahtarları aracılığıyla yüksek kullanılabilirlik sağlar. Ayrıca çekirdek katmanına erişimde eşit maliyetli yollar sunar.

Çekirdek Katman: Ağın omurgası olarak ifade edilir. Birincil amacı yanlış yalıtımı ve yüksek hızlı omurga bağlantısını sağlamaktır. Birkaç ağ katmanını birbirine bağlar. Çekirdek katman, tüm dağıtım katmanı aygıtları için toplayıcı görevindedir.

2.1.3. Yedekli Bağlantılar

Ağda kritik cihazlar arasında ve erişim katmanıyla çekirdek katmanı cihazları arasında yedekli bağlantılar uygular (Görsel 2.3).



Görsel 2. 3: Yedeklilik planı

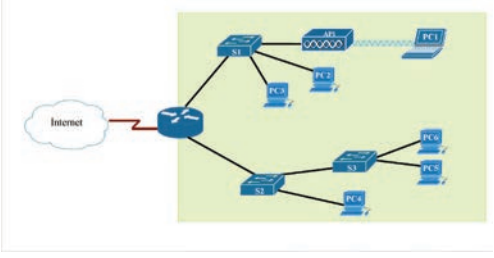
Yedeklilik Planı: Yedeklilik, ağ tasarımının önemli bir parçasıdır. Tek bir arıza noktası olasılığını en aza indirerek ağ hizmetlerinin kesintiye uğramasını önleyebilir. Yedeklilik uygulama yöntemlerinden biri, yinelenen ekipmanı yüklemek ve kritik cihazlar için yük devretme hizmetleri sağlamaktır.

Yedeklilik uygulamanın başka bir yöntemi de yedekli yollar, verilerin ağdan geçmesi için alternatif fiziksel yollar sunar. Anahtarlamalı ağdaki yedekli yollar yüksek kullanılabilirliği destekler. Bununla birlik-

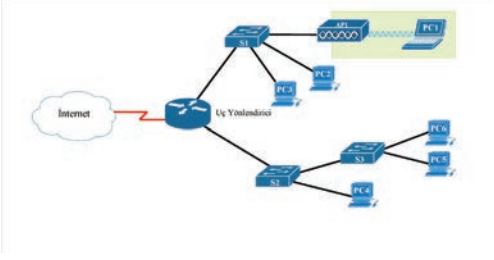
te anahtarların çalışması nedeniyle, anahtarlamalı bir ethernet ağındaki yedekli yollar mantıksal katman döngülerine neden olabilir. Bu nedenle, Spanning Tree Protokolü (STP) gereklidir. STP, döngüsüz mantıksal topoloji oluşturmak için anahtarlamalı ortamda kullanılan açık standart bir protokoldür.

Hata Etki Alanı Boyutunu Azaltma: İyi tasarlanmış bir ağ sadece trafiği kontrol etmekle kalmaz, aynı zamanda hata alanlarının boyutunu da sınırlar.

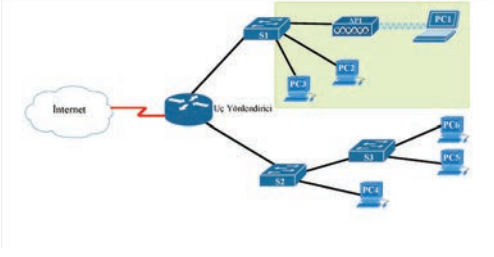
Yedek bağlantıların ve güvenilir kurumsal sınıf ekipmanların kullanılması, bir ağdaki kesinti olasılığını en aza indirir. Daha küçük hata etki alanları, arızanın şirket üretkenliği üzerindeki etkisini azaltır. Ayrıca sorun giderme işlemini basitleştirir, böylece tüm kullanıcılar için arıza süresini kısaltır (Görsel 2.4, Görsel 2.5, Görsel 2.6).



Görsel 2. 4: Hata etki alanı



Görsel 2. 5: Kablosuz ağ hata etki alanı



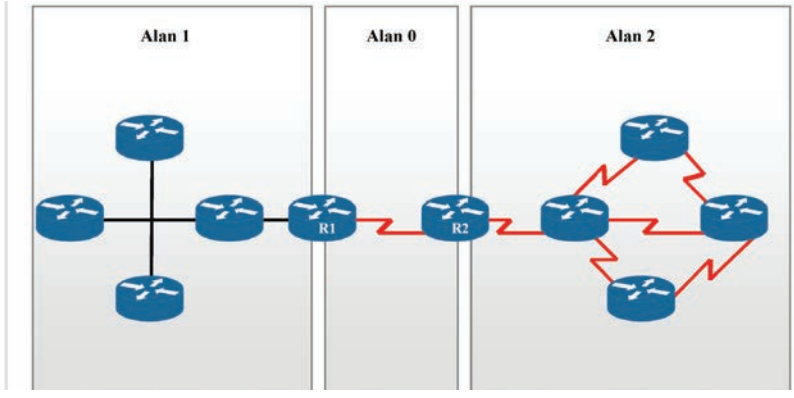
Görsel 2. 6: Anahtar hata etki alanı

2.1.4. Ölçeklenebilir Yönlendirme Protokolü

Ölçeklenebilir bir yönlendirme protokolü; yönlendirme güncellemelerini izole etmek ve yönlendirme tablosunun boyutunu en aza indirmek için kullanılır. Örneğin, büyük ağlarda Open Shortest Path First (OSPF) gibi gelişmiş yönlendirme protokolleri kullanılır.

OSPF, bağlantı durumu yönlendirme protokolüdür. Görsel 2.7'de gösterildiği gibi OSPF, hızlı yakınsamanın önemli olduğu daha büyük hiyerarşik ağlarda iyi çalışır. OSPF yönlendiricileri, diğer bağlı OSPF yönlendiricileri ile komşu bitişiklikleri kurar ve korur. OSPF yönlendiricileri, bağlantı durumu veri tabanlarını senkronize eder. Ağ değişikliği gerçekleştiğinde bağlantı durumu güncellemeleri gönderir, bu da diğer

OSPF yönlendiricilerini değişiklik hakkında bilgilendirir ve varsa yeni bir en iyi yol oluşturur.



Görsel 2. 7: Çok alanlı OSPF

2.1.5. Arıza Etki Boyutunu Sınırlama

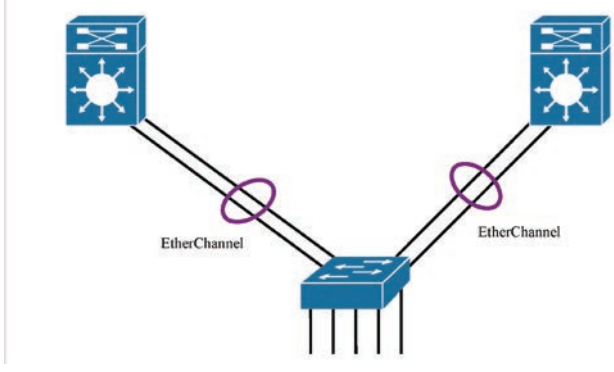
Ağın çekirdek katmanındaki arıza ağda büyük bir etkiye sahip olabilir. Bu durumda ağ sorumlusu arızaları önlemek için çaba gösterir. Hiyerarşik tasarım modelinde, dağıtım katmanındaki hata etki alanı boyutunu kontrol etmek kolay ve ucuzdur. Bu yüzden dağıtım katmanında, ağ hataları daha küçük alanda yer alır ve daha az kullanıcıyı etkiler.

2.1.6. Anahtar Bloğu Dağıtımı

Yönlendiriciler veya çok katmanlı anahtarlar genellikle, aralarında eşit olarak bölünmüş erişim katmanı anahtarlarıyla çiftler olarak ağda yer alır. Bu durumda ağda tek bir cihazın arızalanması ağın tamamen hizmet veremez duruma geçmesini engeller. Anahtar bloğunun tamamının arızalanması söz konusu olsa bile bu durum çok sayıda son kullanıcıyı etkilemez.

2.1.7. Bant Genişliğini Artırın

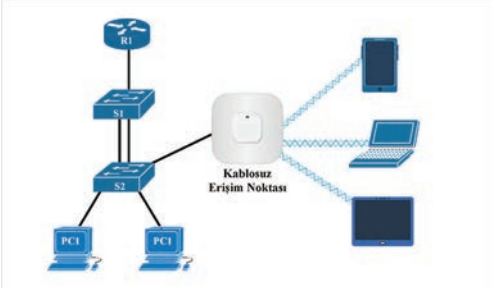
Görsel 2.8'de her biri bir anahtara iki bağlantılı, iki çok katmanlı anahtar vardır. Hiyerarşik ağ tasarımında, erişim ve dağıtım anahtarları arasındaki bazı bağlantıların diğer bağlantılardan daha büyük miktarda trafiği işlemesi gerekebilir. Bu durumda EtherChannel bağlantı toplama, yöneticinin birkaç fiziksel bağlantısını birleştirerek tek bir mantıksal bağlantı oluşturmasına ve cihazlar arasındaki bant genişliği miktarını arttırmasına olanak sunar.



Görsel 2. 8: EtherChannel bağlantısı

2.1.8. Erişim Katmanını Genişletme

Ağ, birey ve cihazların ağa erişimini gerektiğinde genişletebilecek biçimde olmalıdır. Erişim katmanı bağlantısını genişletmek için kablosuz bağlantı kullanılabilir. Kablosuz bağlantı; esneklik, düşük maliyetler ve değişen ağ ve iş gereksinimlerinde hızlı büyüme ve uyum sağlama yeteneği gibi avantajlar sunar (Görsel 2.9).



Görsel 2. 9: Kablosuz bağlantı

2.1.9. Anahtar Donanımının Belirlenmesi

Hiyerarşik ve ölçeklenebilir ağlar oluşturmak için doğru donanım kullanılmalıdır. Ağ tasarlarken mevcut ağ gereksinimlerini karşılamak ve ağ büyümesine izin vermek için uygun donanım seçilmelidir. Bu anlamda kurumsal ağ içinde hem anahtarlar hem de yönlendiriciler ağ iletişiminde kritik rol oynar.

Kampüs LAN Anahtarları: Kurumsal LAN'da ağ performansını ölçeklendirmek için çekirdek, dağıtım, erişim ve kompakt anahtarlar bulunur. Bu anahtar platformları, sekiz sabit portlu fansız anahtardan yüzlerce portu destekleyen anahtarlara kadar çeşitlilik gösterebilir.

Bulut Yönetimli Anahtarlar: Ağ sorumlusunun anahtar cihazın yanında bulunmadan web üzerinden anahtar portunu izlemesini ve yapılandırmasını sağlar.

Veri Merkezi Anahtarları: Veri merkezlerinde altyapı ölçeklenebilirliğini, operasyonel sürekliliği ve veri aktarım esnekliğini destekleyen anahtarlar kullanılmalıdır.

İletme Hızları: Anahtar seçerken iletim hızlarının dikkate alınması gerekir. Eğer anahtar iletim hızı çok düşükse, tüm anahtar portlarında kablo hızında iletişim sağlanamaz. Kablo hızı, anahtardaki her Ethernet portunun erişebileceği en yüksek veri hızıdır. Veri hızları 100 Mbps, 1 Gbps, 10 Gbps veya 100 Gbps olabilir.

Ethernet Üzerinden Güç: Anahtarın mevcut ethernet kabloları üzerinden cihaza güç sağlamasına izin verir. Bu özellik, IP telefonları ve bazı kablosuz erişim noktaları tarafından kullanılabilir.

Çok Katmanlı Anahtarlama: Çok katmanlı anahtarların (multilayer switch) yönlendirme tablosu oluşturma, yönlendirme protokolünü destekleme ve IP paketlerini ikinci katmana iletme hızına yakın bir hızda iletebilme özellikleri bulunur.

Anahtar seçiminde önemli noktalar; maliyet, port yoğunluğu, güç, güvenilirlik karşılaştırması, port hızı, arabellek ve ölçeklenebilirliktir.

2.1.10. Yönlendirici Donanımının Belirlenmesi

Router seçiminiz önemli bir karardır. Yönlendiriciler, paketleri uygun hedefe yönlendirmek için hedef IP adresinin ağ bölümünü (öneki) kullanır. Bağlantı koparsa alternatif yol seçerler. Yerel ağdaki tüm hostlar, IP yapılandırmalarında yerel yönlendirici arayüzünün IP adresini belirtir. Bu yönlendirici arayüzü, varsayılan ağ geçididir.

2.2. KURULUM

Ağdaki sorunları gidermede ağ ile ilgili dokümantasyonun iyi olması, ağ sorumlusunun işini kolaylaştıracaktır. Bu yüzden ağları etkin izlemek ve ağ sorunlarını gidermek için aşağıda sıralanmış ağ belgeleri yaygın olarak kullanılır.

1. Fiziksel ve mantıksal ağ topoloji şeması
2. Ağdaki cihazların bilgilerinin bulunduğu ağ cihazı belgeleri
3. Ağ performans belgeleri

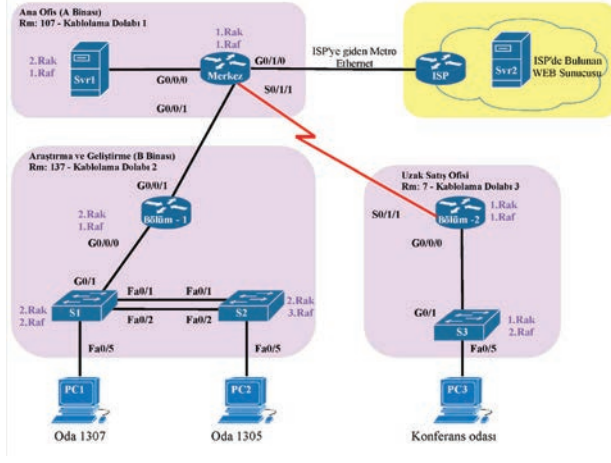
Ağ sorumlularına tavsiye edilen tüm ağ belgelerinin basılı kopyalarını oluşturmak ya da belgeleri korumalı bir sunucuda tek bir konumda saklamaktır. Bunun yanı sıra ağ sorumlularına yedek belgeleri de farklı bir konumda saklamaları tavsiye edilir.

2.2.1. Fiziksel Topoloji

Fiziksel ağ topolojisi, ağda bağlı bulunan tüm cihazların fiziksel yerleşimini gösterir. Özellikle fiziksel katman sorunlarını çözmek için bu cihazların fiziksel olarak nasıl bağlandığını bilmek gerekir. Fiziksel topolojide kaydedilen bilgiler aşağıda sıralanmıştır.

- Cihazın adı
- Cihazın konumu (konum, oda numarası, kabinet konumu)
- Arayüzler ve aktif portlar
- Kablo türü

Görsel 2. 10'da örnek bir fiziksel ağ topoloji şeması gösterilmektedir.



Görsel 2. 10: Fiziksel ağ topolojisi

SIRA SİZDE

Görsel 2. 10'daki fiziksel ağ topolojisini simülasyon programında oluşturunuz.

2.2.2. Mantıksal IPv4 Ağ Topolojisi

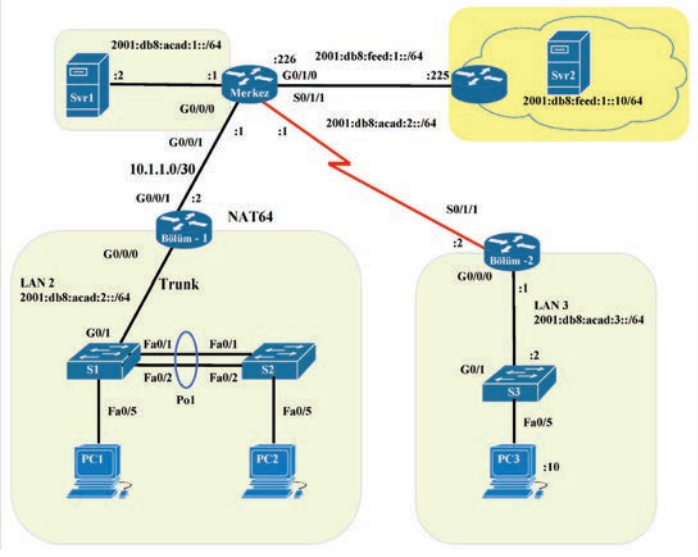
Mantıksal ağ topolojisi, ağ cihazlarının ağa mantıksal bağlantısıyla ilgili bilgi içerir. Mantıksal ağ topolojisi ağ cihazlarının ağdaki diğer cihazlarla iletişim kurarken ağ üzerinden veri aktarımını nasıl gerçekleştirdiğini ifade eder. Router (yönlendirici), switch (anahtar) , server (sunucu) ve host (bilgisayar) gibi ağ

bileşenlerini temsil eder. Ayrıca, mantıksal ağ topolojisinde farklı bölgeler arasındaki bağlantılar gösterilir fakat cihazların gerçek ortamdaki fiziksel konumları bulunmaz.

Mantıksal ağ topolojisi için tutulan bilgiler aşağıda sıralanmıştır.

- Cihaz adı
- Ağların IP adres aralıkları ve maskeleri
- Arayüz adları
- Yönlendirme protokolleri / statik rotalar
- 2. Katman bilgileri (VLAN'lar, trunk, EtherChannel vb.)

Görsel 2. 11'de örnek bir mantıksal IPv4 ve IPV6 ağ topolojisi gösterilmektedir.



Görsel 2. 11: Mantıksal IPv4 ve IPV6 ağ topolojisi

SIRA SİZDE

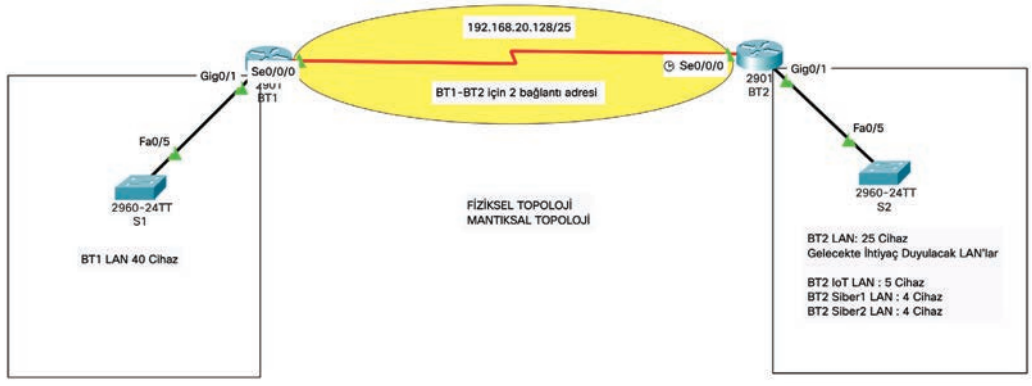
Görsel 2. 11'deki fiziksel ağ topolojisini oluşturduğunuz ağın mantıksal IPV4 ve IPV6 topolojisini simülasyon programında oluşturunuz.

DİKKAT

Değişken Uzunluk Alt Ağ Maskesi (VLSM), IP adreslerinin boşa harcanmasını önlemek için tasarlanmıştır. VLSM ile bir ağ alt ağa alınır ve ardından yeniden alt ağa bağlanır. Bu işlem, her alt ağda gerekli olan ana bilgisayar sayısına bağlı olarak çeşitli boyutlarda alt ağlar oluşturmak için birçok kez tekrarlanabilir. VLSM'nin etkili kullanımı adres planlamasını gerektirir.

1. UYGULAMA

Görsel 2.12'deki ağ topolojisini simülasyon programında hazırlayıp uygulama adımlarını gerçekleştiriniz.



Görsel 2. 12: Ağ topolojisi

1. Adım: Görsel 2.12'de bilişim teknoloji alanı CCNA laboratuvarı için topolojide görüntülenen ağ için bir adres şeması geliştirmek üzere 192.168.20.128/25 ağ adresi kullanılmaktadır. Bu ağ adresine göre tasarım için gereksinimlerinizi belirleyiniz.

a) Bir / 25 ağında kaç adet cihaz adresi bulunur?

126

b) Topoloji diyagramına ihtiyaç duyulan toplam cihaz adresinin sayısı nedir?

80

c) Ağ topolojisinde kaç alt ağa ihtiyaç vardır?

6

ç) BT1 LAN alt ağında kaç tane IP adresi gereklidir?

40

d) 40 adet bilgisayar adresi için hangi alt ağ maskesi gerekmektedir?

/26 veya 255.255.255.192

e) Bu alt ağ maskesi toplam kaç ana bilgisayar adresini destekleyebilir?

62

f) Bu alt ağı desteklemek için 192.168.20.128/25 ağ adresini alt ağa bağlayabilir misiniz?

Evet

g) Bu alt ağda kullanılabilecek ağ adresleri nelerdir? Bu alt ağ için ağın ilk kullanılabilir adresini kullanınız.

192.168.20.128/26 ve 192.168.20.192/26

ğ) İkinci büyük alt ağı belirleyiniz.

BT2 LAN

h) İkinci en büyük alt ağ için kaç IP adresi gerekmektedir?

25

ı) 25 adet bilgisayar adresini hangi alt ağ maskesi destekleyebilir?
/27 or 255.255.255.224

i) Bu alt ağ maskesi toplam kaç ana bilgisayar adresini destekleyebilir?
30

j) Kalan alt ağı tekrar alt ağa bağlayabilir ve bu alt ağı desteklemeye devam edebilir misiniz?
Evet

k) Bu alt ağda kullanılabilecek ağ adresleri nelerdir?
192.168.20.192/27 ve 192.168.20.224/27

l) Üçüncü büyük alt ağı belirleyiniz.
BT2 IoT LAN

m) Bir sonraki en büyük alt ağ için kaç IP adresi gerekmektedir?
5

n) 5 adet host adresini hangi alt ağ maskesi destekleyebilir?
/29 veya 255.255.255.248

o) Bu alt ağ maskesi toplam kaç ana bilgisayar adresini destekleyebilir?
6

ö) Kalan alt ağı tekrar alt ağa bağlayabilir ve bu alt ağı desteklemeye devam edebilir misiniz?
Evet

p) Bu alt ağda kullanılacak ağ adresleri nelerdir?
192.168.20.224/29, 192.168.20.232/29, 192.168.20.240/29 ve 192.168.20.248/29

r) Dördüncü en büyük alt ağı belirleyiniz.
BT1-BT2

s) Bir sonraki en büyük alt ağ için kaç IP adresi gereklidir?
2

ş) 2 adet bilgisayar adresini hangi alt ağ maskesi destekleyebilir?
/30 veya 255.255.255.252

t) Bu alt ağ maskesi toplam kaç ana bilgisayar adresini destekleyebilir?
2

u) Kalan alt ağı yeniden alt ağa bağlayabilir ve bu alt ağı desteklemeye devam edebilir misiniz?
Evet

ü) Bu alt ağda kullanılabilecek ağ adresleri nelerdir?
192.168.20.248/30 ve 192.168.20.252/30

2. Adım: VLSM adres şemasını tasarlayınız (Tablo 2.1).

Tablo 2.1: Oluşturulan Ağ Topolojisinin VLSM Adres Şeması Tablosu

Alt Ağ Açıklaması	Gerekli Cihaz Sayısı	Ağ Adresi /CIDR	İlk Cihaz Adresi	Genel Yayın (Broadcast) Adresi
BT1 LAN	40	192.168.20.128/25	192.168.20.129	192.168.20.191
BT2 LAN	25	192.168.20.192/27	192.168.20.193	192.168.20.223
BT2 IoT LAN	5	192.168.20.224/29	192.168.20.225	192.168.20.231
BT2 SIBER1 LAN	4	192.168.20.232/29	192.168.20.233	192.168.20.239
BT2 SIBER2 LAN	4	192.168.20.240/29	192.168.20.241	192.168.20.247
BT1-BT2	2	192.168.20.248/30	192.168.20.249	192.168.20.251

3. Adım: Cihaz arayüz adres tablosunu doldurunuz.

Alt ağdaki ilk cihaz adresi ile Ethernet arayüzünü yapılandırınız. BT1-BT2 bağlantısındaki BT1'i ilk cihaz adresi ile yapılandırınız (Tablo 2.2).

Tablo 2. 2: Oluşturulan Ağ Topolojisinin Cihaz Bilgileri ve IP Adresleme Tablosu

Cihaz	Arayüz	IP Adresi	Subnet Mask	Cihaz Arayüzü
BT1	Se0/0/0	192.168.20.249	255.255.255.252	BT1-BT2
	Gig0/1	192.168.20.129	255.255.255.192	40 Cihaz
BT2	Se0/0/0	192.168.20.250	255.255.255.252	BT1-BT2
	Gig0/1	192.168.20.193	255.255.255.224	25 Cihaz

4. Adım: VLSM adres şemasını kullanarak yönlendiricileri yapılandırınız.

a) Yönlendiricilere cihaz adını atayınız.

```
R1(config)# hostname BT1
R2(config)# hostname BT2
```

b) Yönlendiricilerin yanlış girilen komutları ana bilgisayar adları gibi çevirmeye çalışmasını önlemek için DNS aramasını devre dışı bırakınız.

```
BT1(config)# no ip domain lookup
BT2(config)# no ip domain lookup
```

c) Her yönlendirici için ayrıcalıklı EXEC şifreli parolası için 29Ekim kullanınız.

```
BT1(config)# enable secret 29Ekim
BT2(config)# enable secret 29Ekim
```

ç) Her yönlendirici için "23Nisan" konsol parolasını atayınız ve girişi etkinleştiriniz.

```
BT1(config)# line con 0
BT1(config-line)# password 23Nisan
BT1(config)# login
BT2(config)# line con 0
BT2(config-line)# password 23Nisan
BT2(config)# login
```

d) Her yönlendirici için "23Nisan VTY" parolasını atayınız ve girişi etkinleştiriniz.

```
BT1(config)# line vty 0 4
BT1(config-line)# password 23Nisan
BT1(config-line)# login
BT2(config)# line vty 0 4
BT2(config-line)# password 23Nisan
BT2(config-line)# login
```

e) Tüm yönlendiricilerde açık metin parolalarını şifreleyiniz.

```
BT1(config)# service password-encryption
BT2(config)# service password-encryption
```

f) Cihaza erişen herkesi, her iki yönlendiricide de yetkisiz erişimin yasak olduğu konusunda uyaracak bir başlık oluşturunuz.

```
BT1(config)# banner motd $ Yetkisiz Giris Yasaktir $
BT2(config)# banner motd $ Yetkisiz Giris Yasaktir $
```

5. Adım: Her yönlendiricideki arayüzleri yapılandırınız.

```
BT1(config)# interface Se0/0/0
BT1(config-if)# ip address 192.168.20.249 255.255.255.252
BT1(config-if)# interface Gig0/1
BT1(config-if)# ip address 192.168.20.129 255.255.255.192
BT2(config)# interface Se0/0/0
BT2(config-if)# ip address 192.168.20.250 255.255.255.252
BT2(config-if)# interface Gig0/1
BT2(config-if)# ip address 192.168.20.192 255.255.255.224
BT1(config)# interface Se0/0/0
BT1(config-if)# description BT1-BT2
BT1(config-if)# interface Gig0/1
BT1(config-if)# description S1
BT2(config-if)# interface Se0/0/0
BT2(config-if)# description BT1-BT2
BT2(config-if)# interface Gig0/1
BT2(config-if)# description S2
BT1(config)# interface Se0/0/0
BT1(config-if)# no shutdown
BT1(config-if)# interface Gig0/1
BT1(config-if)# no shutdown
BT2(config)# interface Se0/0/0
BT2(config-if)# no shutdown
BT2(config-if)# interface Gig0/1
BT2(config-if)# no shutdown
```

6. Adım: Yapılandırmayı tüm cihazlara kaydediniz.

```
BT1# copy running-config startup-config
BT2# copy running-config startup-config
```

DİKKAT

Yapılandırmayı kaydetmek için kullanıcı düzeyine göre "WR" ya da "DO WR" komutu kullanılabilir.

SIRA SİZDE

Bağlantıları test ediniz.

a. BT1'den, BT2'nin G0 / 0/0 arayüzüne ping atınız.

b. BT2'den, BT1'in G0 / 0/0 arayüzüne ping atınız.

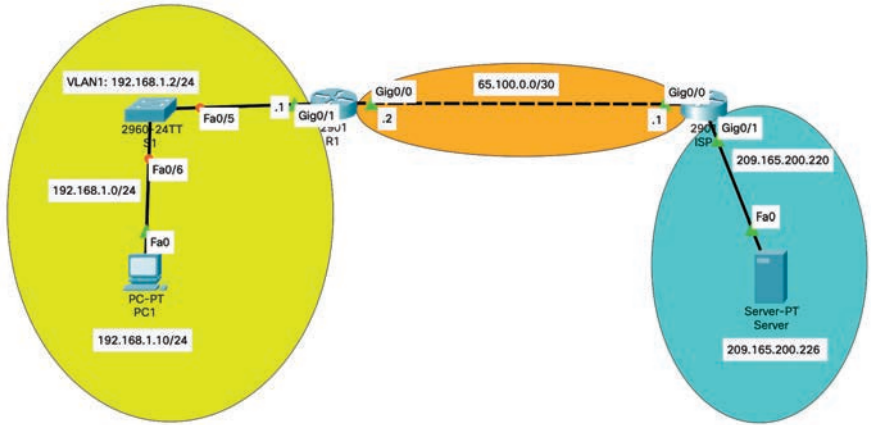
c. Ping başarılı değilse yönlendirme protokolü yapılandırmasını gerçekleştiriniz.

2.3. TEST VE BAKIM

Hazırlanan senaryoyu mutlaka test ediniz, varsa hataları düzeltiniz.

2. UYGULAMA

Görsel 2.13'teki ağ topolojisini Tablo 2.3'te verilen adres bilgilerine göre simülasyon programında hazırlayıp test ve bakım için uygulama adımlarını gerçekleştiriniz.



Görsel 2. 13: Ağ topolojisi

Tablo 2.3: Görsel 2.13'teki Adres Tablosu

Cihaz	Arayüz	IP Adresi / Ön Ek	Default Gateway	Genel Yayın (Broadcast) Adresi
R1	Gig0/0	65.100.0.2 /30	-	192.168.20.191
R1	Gig0/1	192.168.1.1 /24	-	192.168.20.223
ISP	Gig0/0	65.100.0.1 /30	-	192.168.20.231
ISP	Gig0/1	209.165.200.220/27	-	192.168.20.239
S1	VLAN 1	192.168.1.2 /24	192.168.1.1	192.168.20.247
Server	NIC	209.165.200.226 /27	209.165.200.225	192.168.20.251

1. Adım: "Ping" ve **"traceroute"** komutları TCP/IP ağ bağlantısını test etmek için kullanılır. **"Ping"** komutu ağdaki cihazın erişilebilirliğini test etmek için kullanılır fakat ağdaki sorunun yerini gösteremez. **"Traceroute"** komutu ise hedef yolu veya rotayı izlemek ve ağdaki paketlerin gecikmelerini ölç-

mek için kullanılır. Ping başarılı olmadığında **Tracert** (veya **traceroute**) komutu, ağ gecikmesini ve yol bilgilerini görüntüleyebilir. Aşağıda sağlanan ilk yapılandırmaları kullanarak R1 ve ISP yönlendiricilerini ve S1 anahtarını yapılandırınız.

R1 ön yapılandırması

```
hostname R1
no ip domain lookup
interface Gig0/0
 ip address 65.100.0.2 255.255.255.252
 ip nat outside
 no shutdown
interface GIG0/1
 ip add 192.168.1.1 255.255.255.0
 ip nat inside
 no shutdown
ip route 0.0.0.0 0.0.0.0 65.100.0.1
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface Gig0/0 overload
```

ISP ön yapılandırması

```
hostname ISP
no ip domain lookup
interface Gig0/0
 ip address 65.100.0.1 255.255.255.252
 no shutdown
interface GIG0/1
 ip add 209.165.200.220 255.255.255.224
 no shutdown
```

SIRA SİZDE

S1'deki kullanımda olmayan arayüzleri kapatınız. Örnek olarak aşağıdaki komutları kullanabilirsiniz.

```
S1 (config)# interface range fa0/1 – 4, fa0/7 – 24, Gig0/1 - 2
S1 (config)# shutdown
```

S1 ön yapılandırması

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

2. Adım: R1 yönlendiricisinde IP hostları yapılandırınız.

```
ip host Server 209.165.200.226
ip host ISP 65.100.0.1
ip host PC1 192.168.1.10
ip host R1 65.100.0.2
ip host S1 192.168.1.2
end
```

3. Adım: PC1 kullanarak R1 ağından ağ bağlantısını test ediniz. Ağ topolojideki PC1'den diğer cihazlara yapılan tüm "ping"ler başarılı olmalıdır. Eğer başarısızsa, topoloji ile kablolamanın ve cihazlar ile PC'lerin yapılandırmasını kontrol ediniz. R1'in GigabitEthernet 0/1 arayüzünü kullanarak PC1'dan varsayılan ağ geçidine ping atınız. PC1'den, aşağıdaki tablodaki hedep IP adreslerine ping atınız ve ortalama gidiş dönüş süresi ile IPv4 TTL değerini tabloya yazınız (Tablo 2.4).

```
C:\> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Tablo 2.4: Ortalama Gidiş Dönüş Süresi ve Yaşam Süresi Tablosu

Hedef	Ortalama	IP Adresi / Ön Ek
Gidiş Dönüş Süresi	Ortalama	65.100.0.2 /30
(Round Trip Time) (ms)	Yaşam Süresi (TTL) / Bağlantı Noktası (Hop Limit)	192.168.1.1 /24
192.168.1.10	<1	128
192.168.1.1 (R1)	<1	255
192.168.1.2 (S1)	1	255
65.100.0.2 (R1)	1	255
65.100.0.1 (ISP)	<1	254
209.165.200.220 (ISP Gig0/1)	1	254
209.165.200.226 (Server)	1	126
209.165.200.226 (Server)	1	126

DİKKAT

İlk ICMP için "İstek zaman aşımına uğradı." mesajı görülebilir. ARP protokolü gecikme ile paket kaybına neden olur.

5. Adım: PC1' de ping komutlarını kullanınız.

a) Komut satırına ping yazın ve Enter tuşuna basınız.

```
C:\> ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
Options:
   -t            Ping the specified host until stopped.
                 To see statistics and continue - type Control-Break;
                 To stop - type Control-C.
   -a            Resolve addresses to hostnames.
   -n count      Number of echo requests to send.
   -l size       Send buffer size.
   -f            Set Don't Fragment flag in packet (IPv4-only).
   -i TTL        Time To Live.
   -v TOS        Type Of Service (IPv4-only. This setting has been deprecated
                 and has no effect on the type of service field in the IP Header).
   -r count      Record route for count hops (IPv4-only).
   -s count      Timestamp for count hops (IPv4-only).
   -j host-list  Loose source route along host-list (IPv4-only).
   -k host-list  Strict source route along host-list (IPv4-only).
   -w timeout    Timeout in milliseconds to wait for each reply.
   -R            Use routing header to test reverse route also (IPv6-only).
   -S srcaddr    Source address to use.
   -4            Force using IPv4.
   -6            Force using IPv6
```

b) –t parametresini kullanarak, Server'ın erişilebilir olduğunu doğrulamak için Server'a ping atınız.

```
C:\Users\User1> ping –t 209.165.200.226
Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
```

ISP yönlendiricisi ile Server arasındaki kabloyu çıkarınız veya ISP yönlendiricisindeki GigabitEthernet 0/1 arayüzünü kapatınız.

```
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
Reply from 65.100.0.1: Destination host unreachable.
Reply from 65.100.0.1: Destination host unreachable.
```

c) Ethernet kablosunu tekrar bağlayınız veya ISP yönlendiricisinde GigabitEthernet 0/1 arayüzünü etkinleştiriniz (no shutdown). Yaklaşık 30 saniye sonra ping tekrar başarılı olmalıdır.

```
Reply from 65.100.0.1: Destination host unreachable.
Request timed out.
Request timed out.
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
```

Reply from 209.165.200.226: bytes=32 time<1ms TTL=126

d) Ping komutunu durdurmak için Ctrl + C tuşlarına basınız.

e) ISP yönlendiricideki GigabitEthernet 0/1 arayüzünü (no shutdown) etkinleştiriniz. Yaklaşık 30 saniye sonra ping tekrar başarılı olmalıdır.

6. Adım: R1'den ağ bağlantısını test ediniz.
a) R1 yönlendiriciden 209.165.200.226 IP adresini kullanarak Server'a ping atınız.
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1 yönlendiricisinden Server'a ping'in başarılı olduğunu gösterir. % 100 başarı oranıyla gösterildiği gibi gidiş dönüş, paket kaybı olmadan ortalama 1 ms sürer.

b) R1 yönlendiricisinden Server'a ping atınız.
R1# ping Server
Kullanılan IP adresi nedir?
209.165.200.226

c) R1 yönlendiricisinde "ping" komutunu kullanınız.
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 10000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!
Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms
Not: Aynı sonuçlar için aşağıdaki komutları da kullanabilirsiniz:
R1# ping 209.165.200.226 repeat 1000

7. Adım: PC1'dan Server'a tracert komutunu kullanınız.
a) Komut istemine tracert 209.165.200.226 yazınız.
C:\> tracert 209.165.200.226
Tracing route to Server [209.165.200.226]
Over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms 192.168.1.1
2 1 ms <1 ms <1 ms 65.100.0.1
3 1 ms <1 ms <1 ms [209.165.200.226]
Trace complete.

8. Adım: Tracert komutunun seçeneklerini keşfediniz.

a) Komut istemine tracert yazınız ve mevcut seçenekleri görmek için Enter tuşuna basınız.

```
C:\> tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
   -d                 Do not resolve addresses to hostnames.
   -h maximum_hops    Maximum number of hops to search for target.
   -j host-list       Loose source route along host-list (IPv4-only).
   -w timeout         Wait timeout milliseconds for each reply.
   -R                 Trace round-trip path (IPv6-only).
   -S srcaddr         Source address to use (IPv6-only).
   -4                 Force using IPv4.
   -6                 Force using IPv6.
```

b) -d parametresini kullanınız. 209.165.200.226 IP adresinin çözümlenmesine dikkat ediniz.

```
C:\> tracert –d 209.165.200.226
Tracing route to 209.165.200.226 over a maximum of 30 hops:
  1   <1 ms   <1 ms   <1 ms   192.168.1.1
  2    1 ms   <1 ms   <1 ms   65.100.0.1
  3    1 ms   <1 ms   <1 ms   209.165.200.226
Trace complete.
```

9. Adım : R1 yönlendiricisinden Server'a traceroute komutunu kullanınız. Komut satırında, R1 yönlendiricisinde traceroute 209.165.200.226 yazınız.

```
R1# traceroute 209.165.200.226
Type escape sequence to abort.
Tracing the route to Server (209.165.200.226)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (65.100.0.1) 1 msec 1 msec 1 msec
  2 Server (209.165.200.226) 1 msec 1 msec 1 msec
```

10. Adım: S1'den Server'a "traceroute" komutunu kullanınız. S1 cihazında "traceroute" 209.165.200.226 yazınız.

```
S1# traceroute 209.165.200.226
Type escape sequence to abort.
Tracing the route to 209.165.200.226
  1 192.168.1.1 0 msec 0 msec 0 msec
  2 65.100.0.1 8 msec 0 msec 0 msec
  3 209.165.200.226 0 msec *  0 msec
```

11. Adım: Aşağıdaki yapılandırmayı kopyalayıp ISP yönlendiricisine yapıştırınız.

```
hostname ISP
interface Gig0/0
 ip address 65.100.0.1 255.255.255.252
```

```
no shutdown
interface GIG0/1
 ip address 192.168.8.1 255.255.255.0
no shutdown
end
```

12. Adım: ISP ağındaki sorunu gidermek ve düzeltmek için ping, tracert veya traceroute komutlarını kullanınız.

a) PC1'deki ping ve tracert komutlarını kullanınız.

```
C:\> tracert 209.165.200.226
Tracing route to 209.165.200.226 over a maximum of 30 hops
 1   <1 ms   <1 ms   <1 ms  192.168.1.1
 2   <1 ms   <1 ms   <1 ms  65.100.0.1
 3  65.100.0.1  reports: Destination host unreachable.
Trace complete.
```

PC1'in 65.100.0.1 IP adresiyle ISP yönlendirici Gig0/0 arayüzüne ulaşıp ulaşamayacağını belirleyiniz.

```
C:\> ping 65.100.0.1
```

b) PC1, ISP yönlendiricisine ulaşabilir. PC1'den ISP yönlendiriciye başarılı ping sonuçlarına göre, ağ bağlantısı sorunu 209.165.200.224/24 ağındadır. Varsayılan ağ geçidini, ISP yönlendiricisinin GigabitEthernet 0/1 arayüzü olan Server'ı pingleyiniz.

```
C:\> ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics for 209.165.200.225:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Ping komutunun sonuçlarında görüldüğü üzere, PC1 ISP yönlendiricinin GigabitEthernet 0/1 arayüzüne erişememektedir.

Tracert ve ping sonuçları, PC1'in R1 ve ISP yönlendiricilerine erişebileceği, Server veya varsayılan ağ geçidine ulaşamayacağı sonucuna varılır.

c) ISP yönlendiricisinin çalışan yapılandırmalarını görüntülemek için show komutlarını kullanınız.

```
ISP# show ip interface brief
```

Interface	IP-Address	OK?	Method Status	Protocol
GigabitEthernet0/0/0	65.100.0.1	YES	manual up	up
GigabitEthernet0/1	192.168.8.1	YES	manual up	up
Serial0/1/0	unassigned	YES	unset up	up
Serial0/1/1	unassigned	YES	unset up	up
GigabitEthernet0	unassigned	YES	unset down	down

```
ISP# show run
<output omitted>
interface GigabitEthernet0/0/0
 ip address 65.100.0.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/1
 ip address 192.168.8.1 255.255.255.0
 negotiation auto
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
<output omitted>
```

show run ve show ip interface brief komutları GigabitEthernet 0/1 arayüzünün çalıştığını ancak yanlış bir IP adresiyle yapılandırıldığını göstermektedir.

d) Yapılandırma sorunlarını düzeltiniz.

```
ISP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)# interface GigabitEthernet 0/1
ISP(config-if)# no ip address 192.168.8.1 255.255.255.0
ISP(config-if)# ip address 209.165.200.220 255.255.255.224
Close configuration window
```

e) PC1'den Server'a ping atabildiğinizi ve tracert yapabildiğinizi doğrulayınız.

```
C:\> ping 209.165.200.226
Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time=44ms TTL=126
Reply from 209.165.200.226: bytes=32 time=41ms TTL=126
Reply from 209.165.200.226: bytes=32 time=40ms TTL=126
Reply from 209.165.200.226: bytes=32 time=41ms TTL=126
Ping statistics for 209.165.200.226:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\> tracert 209.165.200.226
Tracing route to SERVER [209.165.200.226]
Over a maximum of 30 hops:
```

```
 1   <1 ms   <1 ms   <1 ms   192.168.1.1
 2    1 ms   <1 ms   <1 ms   65.100.0.1
 3    1 ms   <1 ms   <1 ms   [209.165.200.226]
```

Trace complete.

13. Adım: Cihaz yapılandırmalarını kontrol ediniz.

R1# show run
Building configuration...
Current configuration : 1806 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip host Server 209.165.200.226
ip host ISP 65.100.0.1
ip host PC1 192.168.1.10
ip host S1 192.168.1.2
no ip domain lookup
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
mode none
!

```
interface GigabitEthernet0/0/0
 ip address 65.100.0.2 255.255.255.252
 ip nat outside
 negotiation auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 negotiation auto
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
!
ip nat inside source list 1 interface GigabitEthernet0/0/0 overload
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 65.100.0.1
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
control-plane
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
End
ISP# show run
Building configuration...
Current configuration : 1337 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
```

```
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 ip address 65.100.0.1 255.255.255.252
 negotiation auto
 !
interface GigabitEthernet0/1
 ip address 209.165.200.220 255.255.255.224
 negotiation auto
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
control-plane
!
line con 0
```

```
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
S1# show run brief
Building configuration...
Current configuration : 1699 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
no ip domain-lookup
!
crypto pki trustpoint TP-self-signed-3822041216
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3822041216
 revocation-check none
 rsakeypair TP-self-signed-3822041216
!
crypto pki certificate chain TP-self-signed-3822041216
 certificate self-signed 01
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
```

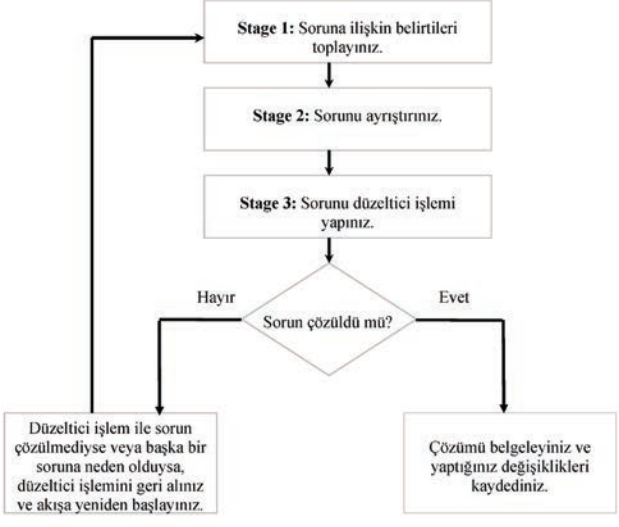
```
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
```

```
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip classless
ip http server
ip http secure-server
!
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
end
```

2.3.1. Sorun Giderme

Ağlar, sorunlar farklı olduğundan ve sorun giderme deneyimi değişiklik gösterdiğinden sorun giderme zaman alıcı olabilir.

- Yapılandırılmış bir sorun giderme yöntemi kullanmak genel sorun giderme süresini kısaltır.
- Bir sorunu çözmek için kullanılabilecek birkaç sorun giderme işlemi vardır.
- Basitleştirilmiş üç aşamalı sorun giderme sürecinin mantıksal akış diyagramını görüntüler (Görsel 2.14).



Görsel 2. 14: Sorun Giderme Akış Şeması

1. Sorunu tanımlamak: Bir sorun olduğunu doğrulayınız ve sonrasında sorunu doğru bir şekilde tanımlayınız.

2. Bilgi toplamak: Bilgisayarlar ya da cihazlar ile ilgili bilgi toplayınız.

3. Bilgileri analiz etmek: Ağ belgelerini, ağ performans bilgilerini kullanarak olası nedenleri belirleyiniz.

4. Olası nedenleri ortadan kaldırmak: En olası nedeni belirlemek için olası nedenleri aşamalı olarak test ediniz.

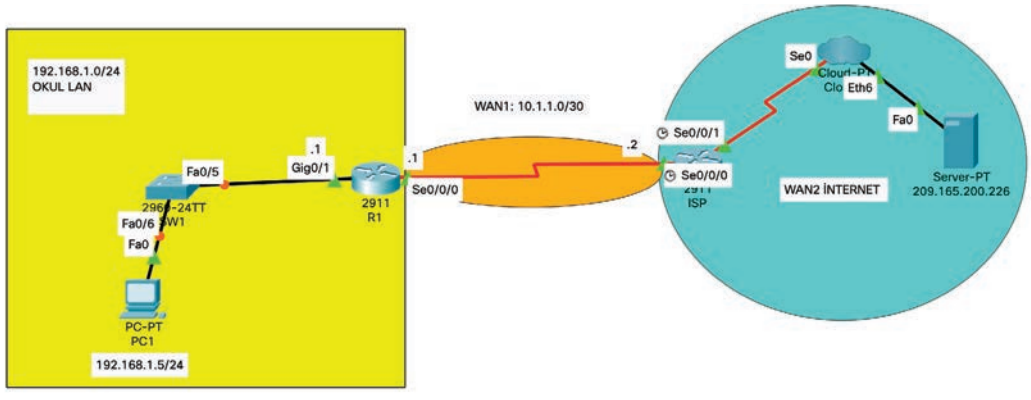
5. Hipotez önerisi: Tespit edilen en olası neden için çözüm geliştiriniz.

6. Hipotezi test etmek: Sorunun aciliyetini değerlendiriniz. Öncelik sıralamanıza göre çözümü uygulayıp çözümü doğrulayınız.

7. Problemi çözmek: Çözüme ulaşıldığında ilgili herkesi bilgilendiriniz. Ayrıca gelecekteki sorunları çözmeye yardımcı olmak için çözümün nedenini ve çözümü belgeleyiniz.

3. UYGULAMA

Görsel 2.15'teki ağ topolojisini simülasyon programında hazırlayıp uygulama adımlarını gerçekleştiriniz.



Görsel 2.15: Ağ topolojisi

1. Adım: Bilişim teknolojileri alanı laboratuvarında "Yerel Alan Ağı" (LAN) ile sorunlar yaşanmaktadır. Laboratuvarda yaşanan ağ sorunları çözülmek istenmektedir.

İlk aşamada, LAN üzerindeki cihazlara bağlanılır. Ağ sorunlarını belirlemek için sorun giderme araçlarını kullanarak sorunun kaynağı ile ilgili bir teori oluşturunuz. Sonrasında bu teori test edilir. İkinci aşamada sorunu çözmek ve uygulamak için eylem planı oluşturunuz. Üçüncü aşamadaysa sistemin istenen şekilde çalıştığı doğrulayınız. Dördüncü aşamadaysa LAN cihazlarında yapılan yapılandırma değişiklikleri ve sorun giderme bulgularını belgelendiriniz.

2. Adım: Görsel 2.15'teki ağ topolojisine ilişkin Tablo 2.5'te verilen Arayüz, IP Adresi, Subnet Mask ve Default Gateway ayarlarını yapınız .

Tablo 2.5: Görsel 2.15'teki Ağ Topolojisinin Adres Tablosu

Cihaz	Arayüz	IP Adresi	Subnet Mask	Default Gateway
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	SE0/0/0	10.1.1.1	255.255.255.252	N/A
ISP	SE0/0/0	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.226	255.255.255.255	N/A
SW1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC1	NIC	192.168.1.5	255.255.255.0	192.168.1.1

3. Adım: Cihazlara ön yapılandırma yapınız.

Topolojide gösterilen cihazlarda aşağıda verilen yapılandırmalar bulunmaktadır. Laboratuvarı başlatmadan önce yapılandırmaları belirtilen cihazlarda yapınız.

PC1

IP Adresi: 192.168.1.5

Alt Ağ Maskesi: 255.255.255.0

SW1:

```
no ip domain-lookup
hostname SW1
ip domain-name ccna-lab.com
username BTadmin privilege 15 secret 19Mayis1919
interface FastEthernet0/1
shutdown
interface FastEthernet0/2
 shutdown
interface FastEthernet0/3
 shutdown
interface FastEthernet0/4
 shutdown
interface FastEthernet0/5
 speed 10
 duplex half
interface Vlan1
ip address 192.168.1.2 255.255.255.0
ip default-gateway 192.168.1.0
banner motd # Sadece Yetkili Girisi! #
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
 transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

R1

```
hostname R1
no ip domain lookup
ip domain name ccna-lab.com
username BTadmin privilege 15 secret 19Mayis1919
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 no negotiation auto
 speed 100
no shutdown
interface Se0/0/0
ip address 10.1.1.1 255.255.255.252
no shutdown
banner motd $ Sadece Yetkili Girisi! $
line vty 0 4
 login local
transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

ISP

```
hostname ISP
no ip domain lookup
interface Se0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
interface Lo0
ip address 209.165.200.226 255.255.255.255
ip route 0.0.0.0 0.0.0.0 10.1.1.1
end
```

4. Adım: Sorunu / sorunları tanımlayınız.

Ağ sorunuyla ilgili edinilen bilgi, kullanıcıların ağ haberleşmesinde yavaş yanıt süreleri yaşamaları ve 209.165.200.226 IP adresine sahip suncuya internet erişememeleridir. Bu ağ sorunlarının olası nedenlerini belirlemek için ağ topolojisinde gösterilen LAN'daki ağ komutlarını ve araçlarını kullanmak gerekir.

DİKKAT

19Mayis1919 parolasına sahip **BTadmin** kullanıcı adı, cihazda oturum açmak için kullanılacaktır.

5. Adım: Ağ sorunlarını gideriniz.

Ağdaki sorunları gidermek için kullanabileceğiniz araçları seçiniz. Sizden beklenen sunucuya bağlantıyı geri yüklemek ve ağdaki yavaş yanıt sürelerini ortadan kaldırmaktır.

DİKKAT

Ağ cihazlarına bağlanmak için SSH kullanırken SSH konsoluna günlük çıkışını etkinleştirmek için terminal monitör ayrıcalıklı exec komutunu veriniz.

6. Adım: Çalışanların yaşadığı ağ sorunlarının olası nedenlerini listeleyiniz. Keşfettiğiniz sorunları ağ sorumlusuyla paylaşınız. Değişiklikleri onayladığınızda uygulayınız.

1. PC1 varsayılan ağ geçidi ayarlanmamıştır.
2. SW1 arayüzünde Fa0/5, yarım dupleks ve hızı da 10 olarak ayarlanmıştır.
3. SW1 varsayılan ağ geçidi 192.168.1.0 olarak ayarlanmıştır.
3. R1 G0/0/1 hızı 100'e ayarlanmış ve otomatik anlaşma devre dışı bırakılmıştır.
4. R1'de ağ geçidi ayarlanmamıştır.

7.Adım: Ağ değişikliklerini uygulayınız.

- PC1'in varsayılan ağ geçidini 192.168.1.1 olarak ayarlayınız.
- SW1'de duplex ve ağ geçidi ayarlarını yapınız.

! duplex full
! ip default-gateway 192.168.1.1

-R1 'de hız, otomatik anlaşma ve varsayılan yönlendirme ayarlarını yapınız.

! speed 100
! negotiation auto
!ip route 0.0.0.0 0.0.0.0 10.1.1.2

8. Adım: Değişiklikleri doğrulayınız. Cihazların çalışan yapılandırmasını "sh run" komutunu kullanarak kontrol ediniz. Ayrıca PC1'den, SW1 ve R1 sunucusuna ulaşınız. PC1'den sunucuya yapılan ping yanıtlarında ve yanıt sürelerinde önemli bir değişiklik göstermemesine dikkat ediniz.

R1# show run
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
ip domain name ccna-lab.com
!

```
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
username BTadmin  privilege 15 secret 5 $1$/Iz6$7tWVeWuJQPAk5G2fySfl0/
!
redundancy
 mode none
!
interface Se0/0/0
 ip address 10.1.1.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 negotiation auto
!
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
banner motd $ Sadece Yetkili Girisi! $
!
line con 0
 logging synchronous
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
end
```

```
SW1# show run
Building configuration...
Current configuration : 1585 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
username BTadmin privilege 15 secret 5 $1$y6iJ$uy3VBz1/JYXksFH99dKGa1
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
ip domain-name ccna-lab.com
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 duplex full
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```

```
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
 shutdown
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
```

```
banner motd $ Sadece Yetkili Girisi!  $
!
line con 0
 logging synchronous
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```

ISP# show run

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname ISP
!
boot-start-marker
boot-end-marker
no aaa new-model
!
no ip domain lookup
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.255
!
interface Se0/0/0
 ip address 10.1.1.2 255.255.255.252
 negotiation auto
!
```

```
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
control-plane
!
line con 0
 logging synchronous
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
end
```

9. Adım: Değişiklikleri belgeleyiniz. Sorun giderme sırasında bulunan sorunları ve bu sorunları çözmek için yapılan yapılandırma değişikliklerini belgelemek için hazırlayacağınız belgelendirme raporuna yazınız.

Belgelendirme farklı şekillerde oluşturulabilir fakat oluşturulacak belgede; sorun gidermenin gerçekleştirildiği tarih, test edilen cihazlar, kullanılan komutlar, keşfedilen sorunlar ve bu sorunları çözmek için uygulanan yapılandırma değişiklikleri bulunmalıdır.

DİKKAT

Sizce sorun giderme metodolojisini uygulamanın farklı bir yolu var mıdır?

Sorun giderme metodolojisinde farklı bir yol da başka bir cihaza geçmeden önce bir cihazdaki 6 adımı tamamlamaktır. Örneğin, PC'de varsayılan ağ geçidinin ayarlanmadığı belirlendikten sonra varsayılan ağ geçidi ayarı yapılır ve çalıştığı doğrulanır. Ağ sorunları hâlâ devam ediyorsa bu örnekte bir sonraki cihaz olan SW1'e geçersiniz. SW1'de sorun giderme işlemi tamamlandığında ve sorunlar devam ettiğinde R1'e geçersiniz. Bu süreç, tam ağ işlevselliği elde edilene kadar devam eder.

2.4. RAPOR

Ağ sistemleri projesi kapsamında yapılan tüm işlemler, uygulanan çözümler, sonuçları ve cihaz belgeleri bir raporda toplanmalıdır.

2.4.1. Yönlendirici Cihaz Belgeleri

Ağ cihaz belgeleri, ağ donanımı ve yazılımına ilişkin doğru ve güncel kayıtları içermelidir. Ayrıca belgelerde, ağ cihazları ile ilgili tüm bilgiler bulunmalıdır. Ağ yöneticileri ilgili cihaz bilgilerini tutmak için elektronik tablolama programlarından yararlanabilir. Raporda fiziksel, mantıksal topolojileri, sistem dokümasyon

ve cihaz belgelerine yer verilir (Tablo 2.6 ve Tablo 2.7).

Tablo 2.6: İki Yönlendirici İçin Cihaz Belgeleri

Cihaz	Model	Açıklama	Konum	IOS	Lisans
Merkezi	İSR 4321	Merkezi Kenar Router	Bina A Rm: 137	Cisco IOS XE Yazılımı, Sürüm 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9
Arayüz	**Açıklama**	**IPv4 Adresi**	**IPv6 Adresi**	**MAC Adresi**	**Yönlendirme**
G0/0/0	SVR-1'e bağlanır	10.0.0.1/30	2001:db8:acad:1:: 1/64	a03d.6fe1.e180	OSPF
G0/0/1	Şube-1'e bağlanır	10.1.1.1/30	2001:db8:acad:a001:: 1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	ISP'ye Bağlanır	209.165.200.226/30	2001:db8:besleme:1:: 2/64	a03d.6fc3.a132	Varsayılan
S0/1/1	Şube-2'ye Bağlanır	10.1.1.2/24	2001:db8:acad:2:: 1/64	Yok	OSPFv3
Cihaz	**Model**	**Açıklama**	**Site**	**IOS**	**Lisans**
Şube-1	ISR 4221	Şube-2 Kenar Router	Bina B Rm: 107	Cisco IOS XE Yazılımı, Sürüm 16.09.04 flash:isr4200-universalk9.16.09.04.SPA.bin	ipbasek9 securityk9
Arayüz	**Açıklama**	**IPv4 Adresi**	**IPv6 Adresi**	**MAC Adresi**	**Yönlendirme**
G0/0/0	S1'e bağlanır	Router-on-a-stick	Router-on-a-stick	a03d.6fe1.9d90	OSPF
G0/0/1	Merkeze Bağlanır	10.1.1.2/30	2001:db8:acad:a001:: 2/64	a03d.6fe1.9d91	OSPF

2.4.2. Anahtar Cihaz Belgeleri

Tablo 2.7: Anahtar İçin Ağ Cihaz Belgeleri

Cihaz	Model	Açıklama	MGT. IP Adresi	IOS			VTP	
S1	Cisco Catalyst WS-C2960-24TC-L	Şube-1 LAN1 switch	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M			Alan Adı: CCNA Modu: Sunucu	
Port	**Açıklama**		**Erişim**	**VLAN**	**Trunk**	**EtherChannel**	**Yerel**	**Etkin**
Fa0/1	Port Channel 1 trunk to S2 Fa0/1		-	-	Evet	Port Kanalı 1	99	Evet
Fa0/2	Port Channel 1 trunk to S2 Fa0/2		-	-	Evet	Port Kanalı 1	99	Evet
Fa0/3	*** Not in use ***		Evet	999	-	-		Kapat
Fa0/4	*** Not in use ***		Evet	999	-	-		Kapat
Fa0/5	Kullanıcıya erişim portu		Evet	10	-	-		Evet
...					-	-		-
Fa0/24	Kullanıcıya erişim portu		Evet	20	-	-		Evet
Fa0/24	*** Not in use ***		Evet	999	-	-		Kapat
G0/1	Şube-1'e trunk bağlantısı		-	-	Evet	-	99	Evet
G0/2	*** Not in use ***		Evet	999		-		

2.4.3. Sistem Dokümantasyon Dosyaları

Sistem belgelerinde sunucular, ağ yönetim konsolları ve kullanıcı bilgisayarlarında kullanılan donanım ve yazılımla ilgili bilgiler bulunur. Yanlış yapılandırılmış bir son kullanıcı cihazının ağın genel performansı üzerinde olumsuz etkisi olabilir. Bu yüzden cihazların güncel sistem belgelerine erişim sağlamak, sorun giderme esnasında yararlı olabilir (Tablo 2.8).

Tablo 2.8: Sistem Cihaz Belgeleri

Cihaz	OS	Servisler	MAC Adresi	IPv4 / IPv6 Adresleri	Varsayılan Ağ Geçidi	DNS
SRV1	MS Server 2016	SMTP, POP3, Dosya Hizmetleri, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1:: 2/64	2001:db8:acad:1:: 1	2001:db8:acad:1:: 1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:besleme:1:: 10/64	2001:db8:besleme:1:: 1	2001:db8:besleme:1:: 1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1:: 251/64	2001:db8:acad:1:: 1	2001:db8:acad:1:: 1

2.4.4. Veri Ölçümü

Ağ belgelendirme oluşturuken routerlardan ve switchlerden doğrudan bilgi toplamak gerekir. Açıkça görülen kullanışlı ağ belgeleme komutları, **ping, traceroute, telnet** ve **show** komutlarını içerir.

SIRA SİZDE

Görsel 2. 17'deki ağ topolojisini simülasyon programında oluşturarak yönlendirici (router) ve anahtarlama (switch) cihazlarında Tablo 2.9'da verilen komutları kullanarak elde ettiğiniz sonuçların dokümanını oluşturunuz. Rapor olarak sununuz.

Tablo 2.9: Sistem Cihaz Belgeleri İçin Komutlar

Komut	Açıklama
show version	Cihaz yazılımı ve donanımı için çalışma süresini, sürüm bilgilerini görüntüler.
show ip interface [brief] show ipv6 interface [brief]	• Bir arayüzde ayarlanan tüm arayüzlerin yapılandırmasını görüntüler. • brief anahtar sözcüğünü yalnızca IP arayüzlerinin yukarı / aşağı durumunu ve her arayüzün IP adresini görüntülemek için kullanılır.
show interfaces	•Her arayüzün yapılandırması ayrıntılı olarak izlenir. •Sadece bir arayüzün ayrıntılı yapılandırmasını görüntülemek için komuta, arayüz türü ve numarası eklenir (Örneğin Gigabit Ethernet0/0/0).
show ip route show ipv6 route	• Yönlendiricideki doğrudan bağlı ve öğrenilen uzak ağlar listelenerek yönlendirme tablosu içeriği görüntülenir. • Sadece rotaları görüntülemek için static, eigrp veya ospf ifadeleri eklenir.
show arp show ipv6 neighbors	ARP tablosu (IPv4) ve komşu tablosunun içeriği görüntülenir (IPv6).
show running-config	Cihazdaki mevcut yapılandırma görüntülenir.
show vlan	Switchteki VLAN'ların durumu görüntülenir.
show port	Switchteki portların durumu görüntülenir.
show tech-support	Sorun giderme amacıyla cihaz hakkında bilgi toplamak için kullanılır.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçeneği işaretleyiniz.

1. Hiyerarşik bir ağ tasarımında yedeklilik planlanırken aşağıdaki işlemlerden hangisi gerçekleştirilmelidir?

A) STP PortFast yapılandırması
B) Alternatif fiziksel yolların belirlenmesi
C) İşlevsiz cihazların değiştirilmesi
D) EtherChannel yapılandırması
E) VLAN yapılandırması

2. Aşağıdakilerden hangisi iyi tasarlanmış, ölçeklenebilir bir ağ tasarımı için gerekli özelliklerden değildir?

A) Yedekli bağlantılar
B) Çoklu bağlantılar
C) Genişletilebilir, modüler ekipman
D) Kablosuz bağlantı
E) NTP

3. Aşağıdakilerden hangisi anahtarın saniyede ne kadar veri işleyebileceğini açıklamak için kullanılır?

A) Güç
B) Kablo hızı
C) İletim hızı
D) Güvenirlik
E) Güvenlik

4. Aşağıdakilerden hangisi anahtarlarda birden fazla fiziksel bağlantıyı tek bir mantıksal bağlantıda birleştirerek anahtar bant genişliğini arttırmak için kullanılır?

A) Trunk port
B) Alt arayüz
C) VLAN
D) EtherChannel
E) Mantıksal topoloji

5. Bir teknisyen, ağ bağlantısını test etmek istiyor. "Ping" komutuyla aynı alt ağdaki iş istasyonlarından başarılı iletim yanıtı alabiliyor fakat uzak iş istasyonlarından başarılı iletim yanıtı alamıyor. Aşağıdakilerden hangisi bunun sebebidir?

A) Varsayılan ağ geçidinin yanlış yapılandırması
B) İşletim sistemi
C) Güncel olmayan NIC
D) Bant genişliği
E) Ağ trafiği

3. ÖĞRENME BİRİMİ
AĞ CİHAZLARI YAPILANDIRMA PROJESİ

KONULAR

3.1. PLANLAMA ADIMLARI
3.2. YAPILANDIRMA ADIMLARI
3.3. TEST VE BAKIM ADIMLARI
3.4. PROJE RAPORU

NELER ÖĞRENECEKSİNİZ?

- DHCP Server uygulama
- VLAN oluşturma
- ACL oluşturma
- Statik ve dinamik yönlendirme
- Ağ cihazlarının güvenliği sağlama

TEMEL KAVRAMLAR

WAN, DHCP, VLAN, Statik yönlendirme, Dinamik Yönlendirme



HAZIRLIK ÇALIŞMALARI

1. Bir ağ oluşturmak için hangi ögelere ihtiyaç vardır? Araştırma sonuçlarını sınıf arkadaşlarınızla paylaşınız.

3.1. PLANLAMA ADIMLARI

Firmanın isteği doğrultusunda oluşturulacak ağ için ön fizibilite çalışması yapılır. Yapılan bu çalışma sonunda ihtiyaç listesi, cihazların konumu, bağlantı şekilleri gibi adımlar planlanır ve bir çizelge hâlinde kâğıda dökülür.

Örnek:

İki ayrı şubesi olan bir firma şubeleri arasında bilgi alışverişinde bulunuyor. Firma yetkilisi bilgi işlem personelinden;

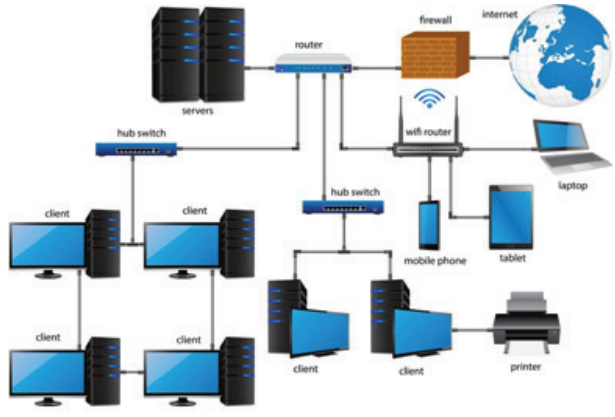
- Her iki şubenin birbiriyle haberleşebilmesini,
- IP'lerin yönlendiriciler tarafından otomatik dağıtılmasını,
- Çalışan bilgisayarlarının yönlendiricilere uzaktan bağlanmasının engellenmesini,
- Laptopların ağa kablosuz bağlanmasını istiyor.

Bilgi işlem personelinin bu bilgilere göre oluşturduğu planlama çizelgesi şu şekildedir.

Ağ gereksinimleri: İşletmede şu an herhangi bir ağ bulunmamaktadır. Yeni kurulacak ağ için işletmenin beklentisi her şubesinde en fazla 6 yönetici ve 18 çalışan bilgisayarı bulundurmaktır.
Kullanıcı gereksinimleri: İşletmenin kullanıcılar arasında iletişime mutlak ihtiyacı olduğu kurulacak ağın işletmenin sağlıklı çalışabilmesi açısından şart olduğu tespit edilmiştir.
Kapasite gereksinimleri: İşletmenin 6 yönetici ve 18 çalışan bilgisayarının aynı anda kullanılabilmesi için birbirinden bağımsız alanları, yönlendirici ve anahtarları güvenli bir şekilde barındırabilecek bir sistem odasına sahip olduğu tespit edilmiştir.
Amaç: Ağ üzerinde her şube için 1 adet yönlendirici, 1 adet anahtar, 1 adet kabin, 1 adet erişim noktası cihazı, 300 metre CAT5 kablo, 150 metre kablo kanalı, 100 adet RJ45 jak'a ihtiyaç olduğu belirlenmiştir.
Performans gereksinimleri: İşletmenin ihtiyacını karşılayacak hız ve kapasiteye uygun cihazlar belirlenip siparişleri verilmiştir.
Konum gereksinimi: İşletmenin yapısı değerlendirilmiş ve üç katlı olması sebebiyle işletmenin ikinci katında bulunan 24 numaralı oda tüm odalara yakınlığı ve yüksek güvenlikli konumu sebebiyle sistem odası olarak belirlenmiştir. Bu şekilde odalara çekilecek kablonun ve kablo kanalının maliyeti de düşürülmüştür. Aynı zamanda odanın kapısının üstüne erişim noktası cihazının konumlandırılmasına karar verilmiştir.
Zaman kısıtlayıcıları: Projenin 3 haftada tamamlanması öngörülmektedir.
Bütçe kısıtlamaları: İşletmeye kurulacak ağın maliyeti 50 bin TL olarak belirlenmiştir.
Teknik gereksinim: İşletmenin hâlihazırda kullanıcı bilgisayarları ve yazılımları olduğu için herhangi bir teknik maliyet belirlenmemiştir.

3.2. YAPILANDIRMA ADIMLARI

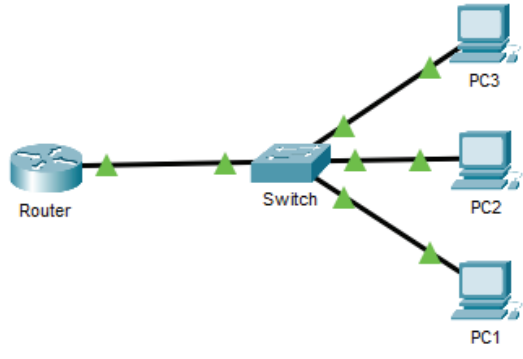
İşletmenin durumu ve ihtiyacına göre proje planı hazırlandıktan sonra bu planda belirlenen yapılandırma adımları sırayla uygulanmalıdır. Böylece işletmenin ihtiyacı olan bilgisayar ağı projeye uygun olarak oluşturulur (Görsel 3.1).



Görsel 3.1: Bilgisayar ağı

3.2.1. IP Havuzu Yapılandırması ve DHCP Server Uygulaması

Ağdaki bir yönlendiriciden ağdaki cihazlara IP dağıtılmak istendiğinde öncelikle yönlendiricide dağıtım için bir IP havuzu oluşturulmalıdır (Görsel 3.2).



Görsel 3.2: DHCP senaryosu

IP havuzu oluşturulması için yönlendirici komut ekranı açıldıktan sonra yazılması gereken komutlar aşağıda sıralanmıştır.

Router>enable ----- Privilege Exec Mode'a geçilir.
Router#configure terminal ----- Config Mode'a geçilir.
Router(config)#ip DHCP pool AG10KASIM ------ Havuza isim verilir ve oluşturulur.
Router(DHCP-config)#network 192.168.1.0 255.255.255.0 ----- Dağıtılacak IP aralığı belirlenir.
Router(DHCP-config)#default-router 192.168.1.1 ----- Default Gateway adresi belirlenir.
Router(DHCP-config)#dns-server 192.168.1.1 ----- Dns Server adresi belirlenir.
Router(DHCP-config)#exit
Router(config)#ip DHCP excluded-address 192.168.1.1 ----- Dağıtım dışı bırakılacak IP'ler belirlenir.

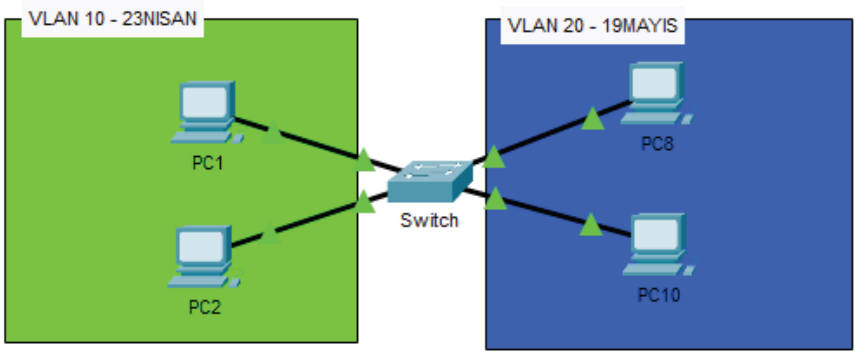
Sistemde bulunan PC1, PC2 ve PC3 yönlendiriciden otomatik IP almaya başlayacaktır.

SIRA SİZDE

Farklı laboratuvarların bulunduğu okul ortamında her laboratuvarda bulunan cihazlar için farklı ağdan IP dağıtımı istenmektedir. Bu yapılandırma için gereken IP havuzlarını oluşturunuz.

3.2.2.VLAN Oluşturulması

Ağda bir anahtar varken ağdaki cihazların birbirinden ayrılması gerektiğinde VLAN denen sanal ağların oluşturulması, anahtar cihazının portlarının bu sanal ağlara üye yapılarak birbirinden ayrılması gerekir (Görsel 3.3).



Görsel 3.3: VLAN senaryosu

Bu işlem için anahtar komut satırına girildikten sonra yazılması gereken kodlar aşağıda sıralanmıştır.

Switch>enable ----- Privilege Exec Mode'a geçilir.
Switch#configure terminal ----- Config Mode'a geçilir.
Switch(config)#vlan 10 ----- vlan oluşturulur
Switch(config-vlan)#name 23NISAN ----- vlan'a isim verilir.
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name 19MAYIS
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1 ----- arayüz içinde girilir.
Switch(config-if)#switchport mode access ----- switch modu erişim olarak değiştirilir.
Switch(config-if)#switchport access vlan 10 ----- vlan 10'a erişmesi sağlanır.
Switch(config-if)#exit
Switch(config-if)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config-if)#interface fastEthernet 0/4

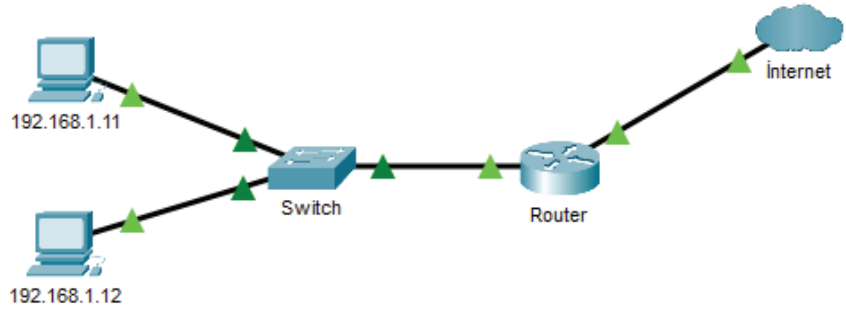
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config-if)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface range fastEthernet 0/6-10 ----- aynı işlemler tek tek tüm arayüzlere yapılacağı gibi bir aralık dâhilindeki arayüzlere de uygulanabilir.
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit

SIRA SİZDE

Her sanal ağın kendi içinde haberleşebileceği bir anahtar üzerinde iki ayrı laboratuvar oluşturunuz ve sanal ağlara ayırınız.

3.2.3.Erişim Kontrol Listelerinin Oluşturulması

Bilgi işlem personelinden bir ağ içinde bazı cihazların kısıtlanması istenebilir. Bu gibi durumlarda ACL (Erişim Kontrol Listeleri) devreye girer ve bu cihazların bazı veri alışverişlerine kısıtlama getirilebilir. Bu kısıtlama genel ve özel olarak iki şekilde yapılabilir. Yani bu cihazların tüm iletişimi kesilebilir veya sadece belli bir trafiği kullanması engellenebilir (Görsel 3.4).



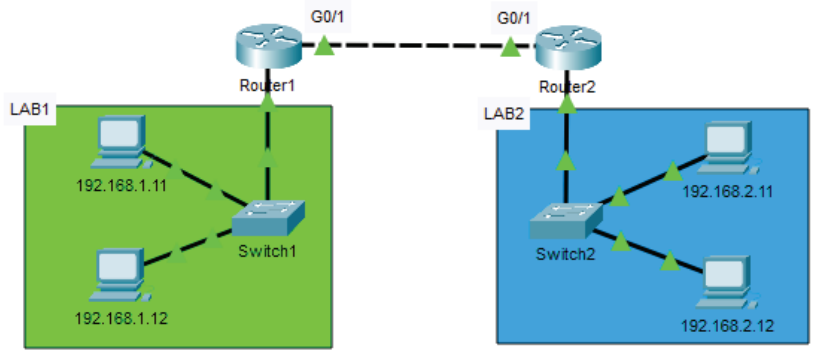
Görsel 3.4: ACL senaryosu

Görsel 3.5'te 192.168.1.11 IP'li bilgisayarın internete çıkmasını engellemek için yönlendirici komut ekranına girdikten sonra yazılması gereken komutlar aşağıda sıralanmıştır.

Router>enable ----- Privilege Exec Mode a geçilir.
Router#configure terminal ----- Config Mode a geçilir.
Router(config)#access-list 150 deny tcp host 192.168.1.11 any eq 80 ----- IP adresinin 80 ve 443 No.lu interne portunu kullanımı kısıtlanır.
Router(config)#access-list 150 deny tcp host 192.168.1.11 any eq 443
Router(config)#access-list 150 permit any any ----- Geri kalan tüm trafiğe izin verilir.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 150 in ----- Routerın ilgili pc ye bakan portu yazılan ACL'ye üye yapılır.

3.2.4. Statik ve Dinamik Yönlendirme

Ağ içinde birden fazla yönlendirici kullanılması gerektiğinde bu yönlendiriciler arası ağların haberleşebilmesi için yönlendirme protokollerinden biri kullanılmalıdır. Bu yönlendirme işlemi iki şekilde yapılabilir: statik ve dinamik. Görsel 3.5'teki yapılandırmada yönlendiricilerden birine dinamik, diğerine statik yönlendirme yapmak için yönlendiricilerin komut ekranına girildikten sonra yazılması gereken komutlar aşağıda sıralanmıştır.

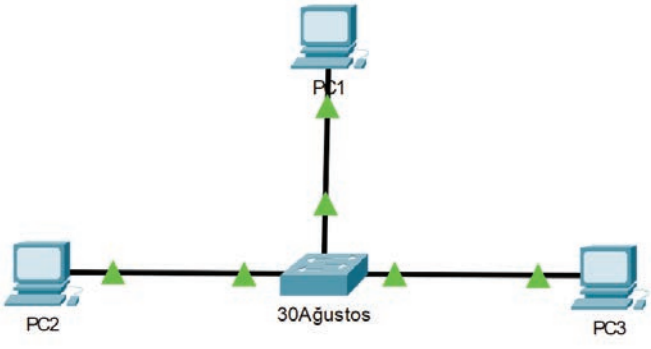


Görsel 3.5: Yönlendirme

Router1>enable ----- Privilege Exec Mode a geçilir.
Router1#configure terminal ----- Config Mode'a geçilir.
Router1(config-router)#network 192.168.1.0 ----- Router e bağlı ağlar tanımlanır.
Router1(config-router)#network 192.168.3.0
Router1(config-router)#exit
Router2>enable ----- Privilege Exec Mode a geçilir.
Router2#configure terminal ----- Config Mode'a geçilir.
Router2(config)#ip route 192.168.1.0 255.255.255.0 gigabitEthernet 0/1 ----- 192.168.1.0 ağına hangi arayüzden gidileceği tanımlanır.

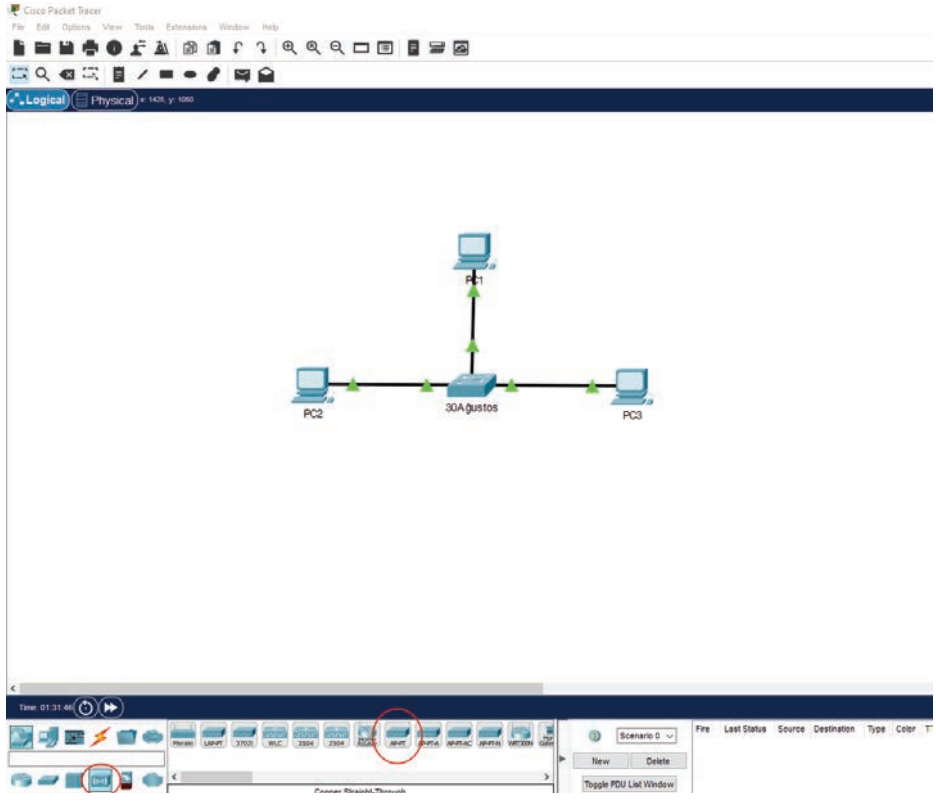
3.2.5.Kablosuz LAN Bağlantısı

Görsel 3.6'da masaüstü bilgisayarlar 30Ağustos isimli anahtara kablolu şekilde direkt bağlıdır. Cisco Packet Tracer programında ağa kablosuz olarak 1 adet dizüstü bilgisayar eklenir.

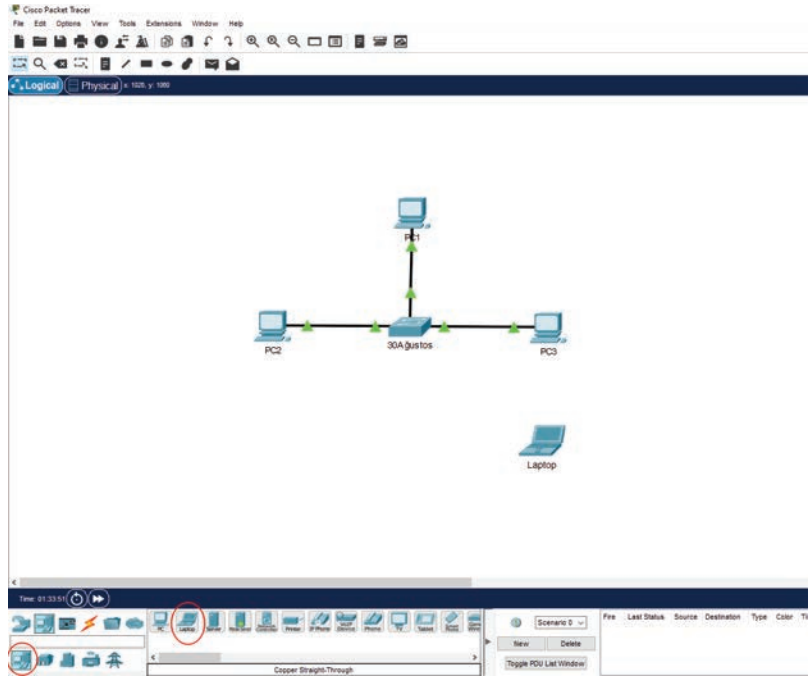


Görsel 3.6: Kablolu ağ

Görsel 3.7'deki Wireless Devices ve Görsel 3.8'deki End Devices alanlarını kullanarak senaryoya bir adet Access Point ve bir adet dizüstü bilgisayarı sürükle - bırak yöntemiyle ekleyiniz.

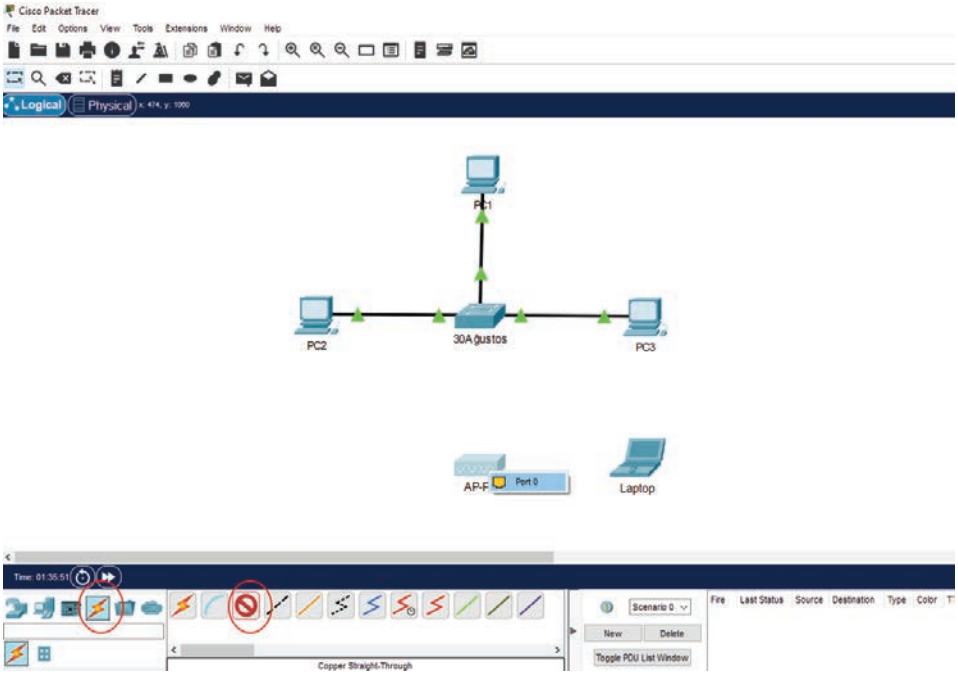


Görsel 3.7: Devices ekranı

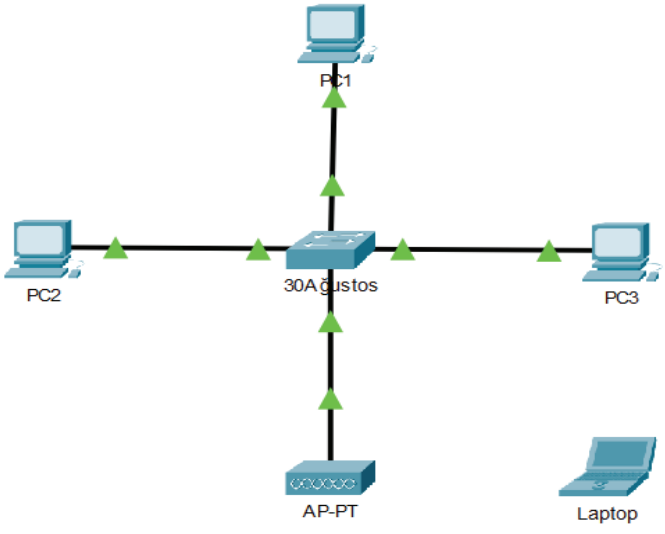


Görsel 3.8: Son kullanıcı cihazları

Görsel 3.9'da görüldüğü gibi kablolar kısmından düz kabloyu seçerek AP-1453 Access Point cihazının Port 0 portunu 30Ağustos anahtarının herhangi bir portuna bağlayınız. Görsel 3.10'daki görüntüyü elde ediniz.

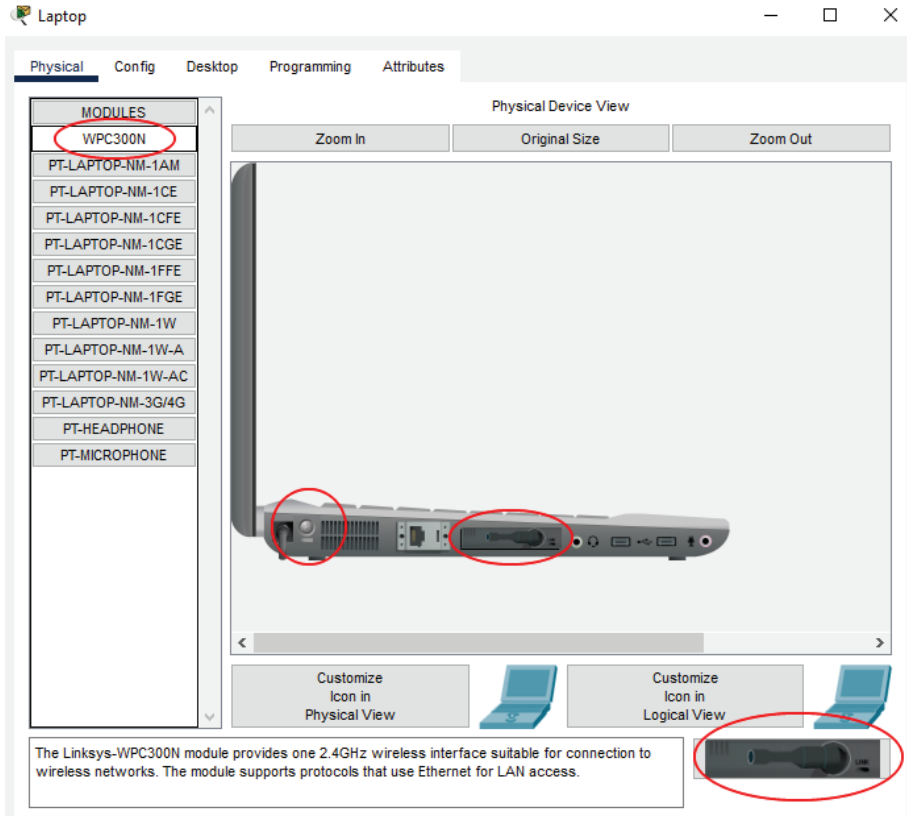


Görsel 3.9: Kablolar



Görsel 3.10: AP ekleme

Senaryoya eklediğiniz dizüstü bilgisayara sol tuş ile tıklayıp açılan Görsel 3.11'deki pencereden WP-C300N aygıtını seçiniz. Daha sonra 1 No.lu alandan dizüstü bilgisayarı kapatıp 2 No.lu alandaki aygıtı 3 No.lu alana sürükleyiniz ve tekrar 1 No.lu alana tıklayarak dizüstü bilgisayarı çalıştırınız.

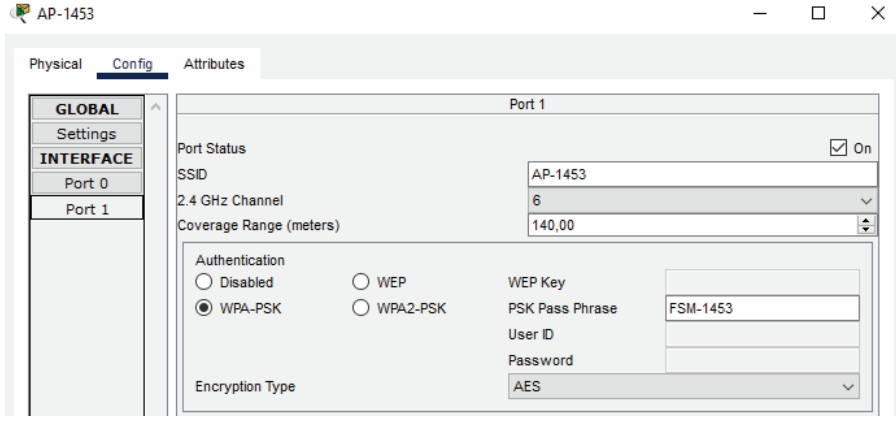


Görsel 3.11: Modül ekleme

AP-PT isimli Access Point cihazına tıklayıp açılan Görsel 3.12'deki pencereden Config sekmesine gelerek Port 1 alanına basınız. Burada SSID kısmına AP-1453 yazınız. Authentication alanından şifreleme türünü WPA-PSK seçiniz. Şifre olarak FSM-1453 yazınız.

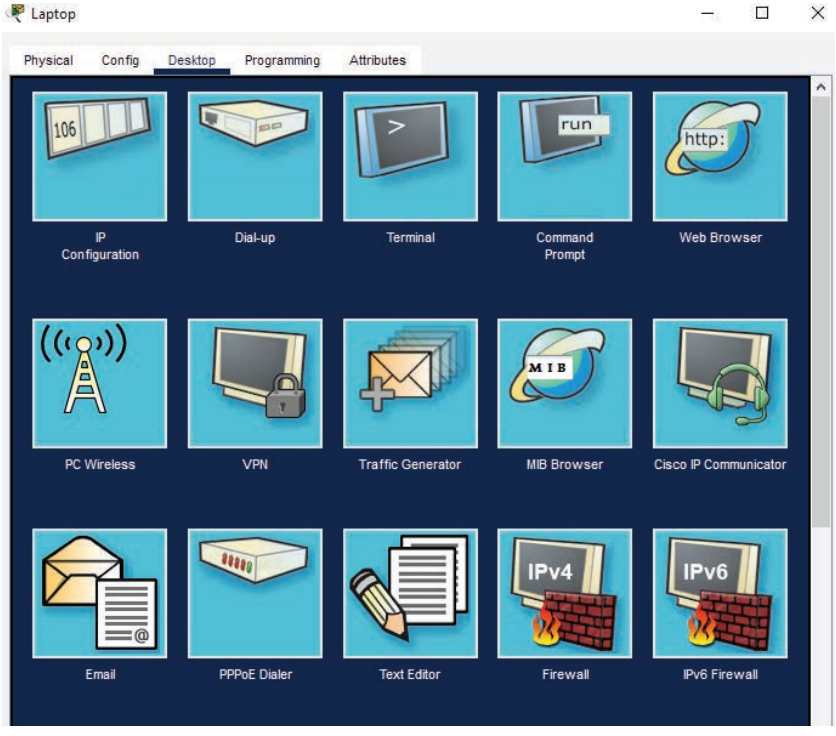
DİKKAT

Aynı pencerenin global>settings alanından AP cihazının adını AP-1453 yapabilirsiniz.



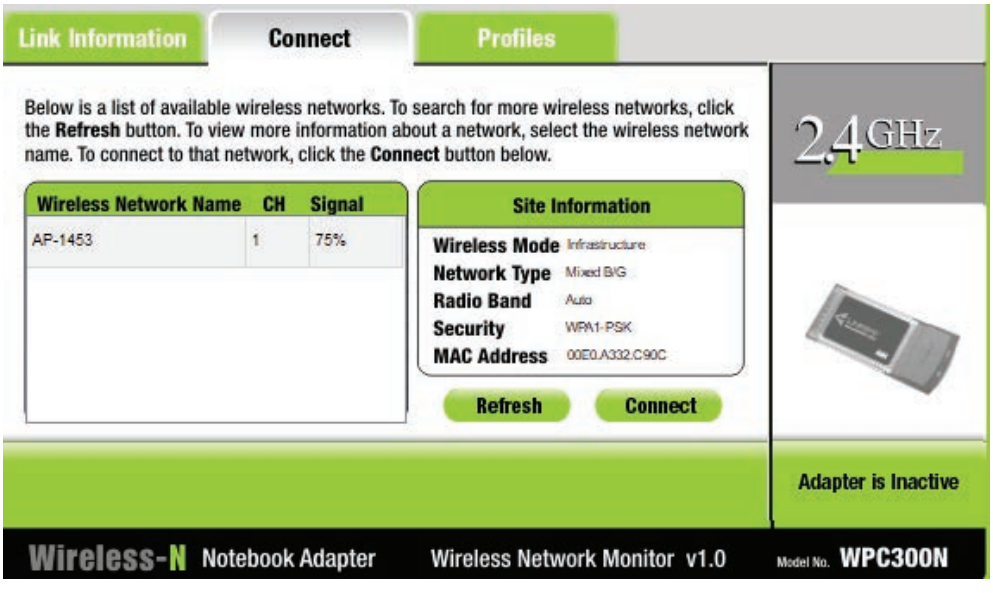
Görsel 3.12: AP ayarları

Dizüstü bilgisayar cihazına tıklayarak açılan pencerede üst taraftaki **Desktop** sekmesine geçiniz ve **PC Wireless** uygulamasını çalıştırınız (Görsel 3.13).



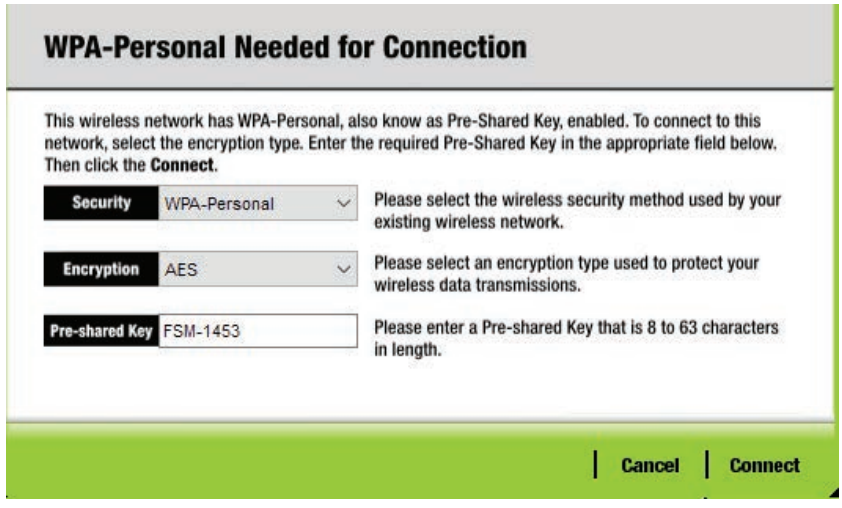
Görsel 3.13: Desktop

Açılan pencereden **Connect** sekmesine geçiniz ve **Refresh** butonuna basınız. Biraz beklediğinizde AP-1453 kablosuz ağını bulacaktır. Ardından **Connect** tuşuna basınız (Görsel 3.14).

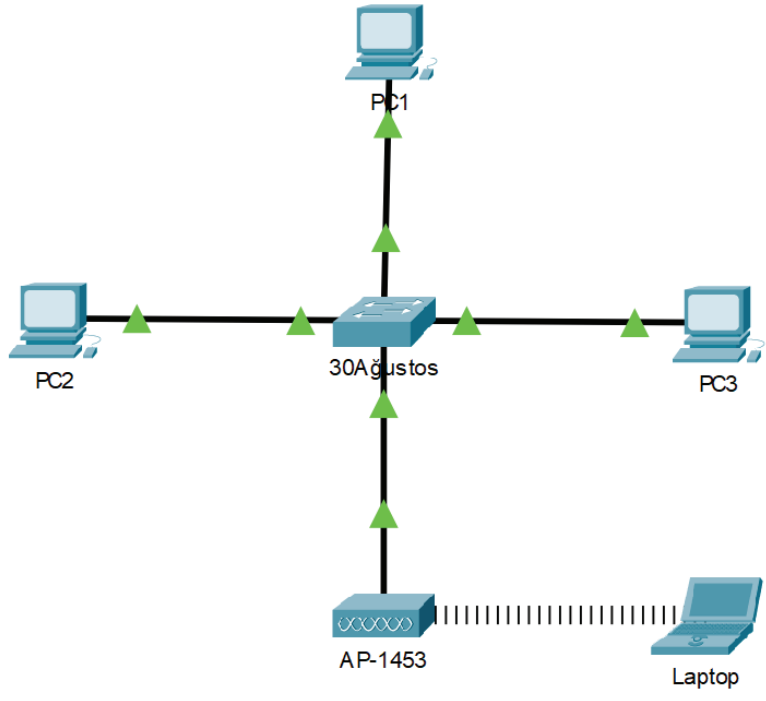


Görsel 3.14: Wireless bağlantı

Karşınıza gelen Görsel 3.15'teki pencereden **Pre-shared Key** alanına belirlediğiniz FSM-1453 şifresini girerek **Connect** butonuna basınız ve dizüstü bilgisayar kablosuz ağa dâhil edilmiş olur (Görsel 3.16).



Görsel 3.15: Şifre ekranı



Görsel 3.16: Kablosuz ağ simülasyonu

3.2.6. Ağ Güvenliği

Yönlendirici ve anahtar cihazlarının yapılandırmasını dış müdahalelerden korumak için yetkili girişlerinin güvenliği sağlanmalıdır. Bunun için ayrıcalıklı çalışma modu, konsol bağlantısı, telnet bağlantısı gibi ulaşım türlerine parola oluşturmak gerekir. Bu parolaların oluşturulması için yazılması gereke kodlar aşağıda sıralanmıştır.

Router>enable ----- Privilege Exec Mode a geçilir.
Router#configure terminal ----- Config Mode a geçilir.
Router(config)#enable secret 19MAYIS1919 ----- Privilege Exec Mode parolası belirleme.
Router(config)#exit
Router(config)#line vty 0 15 ----- Telnet şifresi belirleme.
Router(config-line)#enable
Router(config-line)#password 29EKIM1923
Router(config-line)#login
Router(config-line)#exit
Router(config)#line console 0 ----- Konsol bağlantı şifresi belirleme.
Router(config-line)#password 10KASIM1938
Router(config-line)#login
Router(config-line)#exit

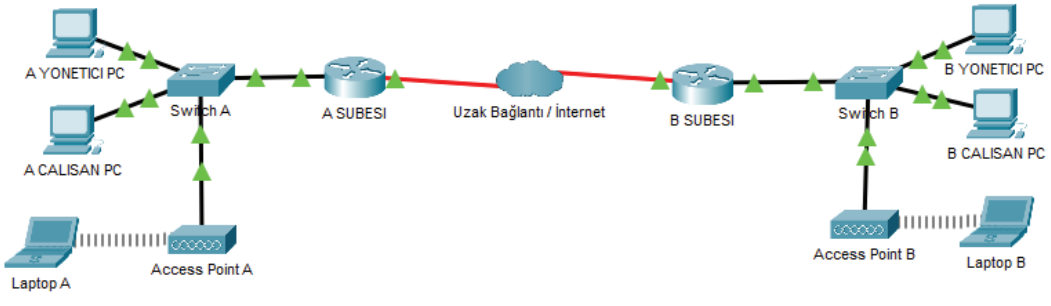
Ayrıca anahtarın bağlantı arayüzlerine başka bir anahtar takılmasını engellemek amacıyla MAC adres bazlı koruma yapılmalıdır. Bu işlem için yazılması gereken kodlar aşağıda sıralanmıştır.

Switch>enable ----- Privilege Exec Mode a geçilir.
Switch#configure terminal ----- Config Mode a geçilir.
Switch(config)#interface range fastEthernet 0/1-24
Switch(config-if-range)#switchport mode access ----- Port Security modu seçilir.
Switch(config-if-range)#switchport port-security mac-address sticky ----- MAC Adreslerini otomatik kaydemesi sağlanır.
Switch(config-if-range)#switchport port-security maximum 1 ----- Ayarüze takılacak maksimum MAC adresi belirlenir.
Switch(config-if-range)#switchport port-security violation shutdown ----- MAC adres limiti aşıldığında nasıl davranacağı belirlenir.

3.2.7. Örnek Proje

Görsel 3.17'deki gibi iki ayrı şubesi olan bir firma, şubeleri arasında bilgi alışverişinde bulunuyor. Firma yetkilisi bilgi işlem personelinden;

- Her iki şubenin birbiriyle haberleşebilmesini,
- IP'lerin yönlendiriciler tarafından otomatik dağıtılmasını,
- Çalışan bilgisayarlarının yönlendiricilere uzaktan bağlanmasının engellenmesini,
- Laptopların ağa kablosuz bağlanmasını istiyor.



Görsel 3.17: Proje örneği

Buna göre yapılması gereken planlama, işlemler ve yazılması gereken kodlar aşağıda sıralanmıştır.

1. Adım: Senaryoya cihazları ekleyiniz. Bağlantıları aşağıdaki tabloda verildiği gibi yapınız (Tablo 3.1).

Tablo 3.1: Arayüz Bağlantı Tablosu

Cihaz	Arayüz		Arayüz	Cihaz
A YONETICI PC	FastEthernet0		FastEthernet0/1	SwitchA
A CALISAN PC	FastEthernet0		FastEthernet0/10	SwitchA
SwitchA	GigabitEthernet0/1		GigabitEthernet0/1	RouterA
AccessPoint A	Port 0		GigabitEthernet0/2	SwitchA
RouterA	Serial0/0/0		Serial0/0/0	RouterB
B YONETICI PC	FastEthernet0		FastEthernet0/1	SwitchB
B CALISAN PC	FastEthernet0		FastEthernet0/10	SwitchB
SwitchB	GigabitEthernet0/1		GigabitEthernet0/1	RouterB
AccessPoint B	Port 0		GigabitEthernet0/2	SwitchB

2. Adım: Tüm anahtar ve yönlendirici cihazların isimlerini değiştiriniz.

Switch>enable
Switch#configure terminal
Switch(config)#hostname SwitchA
SwitchA(config)#do write
Building configuration…
[OK]

Switch>enable
Switch#configure terminal
Switch(config)#hostname SwitchB
SwitchB(config)# do write
Building configuration…
[OK]

Router>enable
Router#configure terminal
Router(config)#hostname RouterA
RouterA(config)# do write
Building configuration…
[OK]

Router>enable
Router#configure terminal
Router(config)#hostname RouterB
RouterB(config)# do write
Building configuration…
[OK]

3. Adım: Kullanılan anahtar üzerinde yönetici bilgisayarlarına ve çalışan bilgisayarlarına ayrı arayüzler rezerve ediniz. Örnekte 2 portlu 2960 anahtarın ilk 6 arayüzünü yöneticilere, kalan 18 arayüzünü çalışanlara ayırınız. Bilgisayarların kablolarını bu ayrıma uygun olarak ilgili arayüzlere takınız.

4. Adım: Anahtar cihazına yönetici ve çalışanlar için VLAN'lar oluşturup arayüzleri bu VLAN'lara üye yapınız.

```
Switch>enable
Switch#configure terminal
SwitchA(config)#vlan 10
SwitchA(config-vlan)#name YONETICI
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#name CALISAN
SwitchA(config-vlan)#exit
SwitchA(config)#
SwitchA(config)#interface range fastEthernet 0/1-6
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range fastEthernet 0/7-24
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 20
SwitchA(config-if-range)#exit
SwitchA(config)#interface GigabitEthernet 0/2
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport access vlan 20
SwitchA(config-if-range)#exit
SwitchA(config)#do write
Building configuration...
[OK]

Switch>enable
Switch#configure terminal
SwitchB(config)#vlan 30
SwitchB(config-vlan)#name YONETICI
SwitchB(config-vlan)#exit
SwitchB(config)#vlan 40
SwitchB(config-vlan)#name CALISAN
SwitchB(config-vlan)#exit
SwitchB(config)#
SwitchB(config)#interface range fastEthernet 0/1-6
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 30
SwitchB(config-if-range)#exit
SwitchB(config)#interface range fastEthernet 0/7-24
```

SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 40
SwitchB(config-if-range)#exit
SwitchB(config)#interface GigabitEthernet 0/2
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport access vlan 40
SwitchB(config-if-range)#exit
SwitchB(config)#do write
Building configuration…
[OK]

5. Adım: VLAN'ların haberleşebilmesi ve dışarı çıkış yapabilmesi için anahtardan yönlendiriciye giden hattı "trunk" moda alınız. Yönlendirici arayüzünü alt arayüzlere ayırınız.

SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#do wr
Building configuration…
[OK]

SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#do wr
Building configuration…
[OK]

RouterA(config)#interface gigabitEthernet 0/0.10
RouterA(config-subif)#encapsulation dot1Q 10
RouterA(config-subif)#ip address 192.168.10.1 255.255.255.0
RouterA(config-subif)#no shutdown
RouterA(config-subif)#exit
RouterA(config)#interface gigabitEthernet 0/0.20
RouterA(config-subif)#encapsulation dot1Q 20
RouterA(config-subif)#ip address 192.168.20.1 255.255.255.0
RouterA(config-subif)#no shutdown
RouterA(config-subif)#exit
RouterA(config)#do write
Building configuration…
[OK]

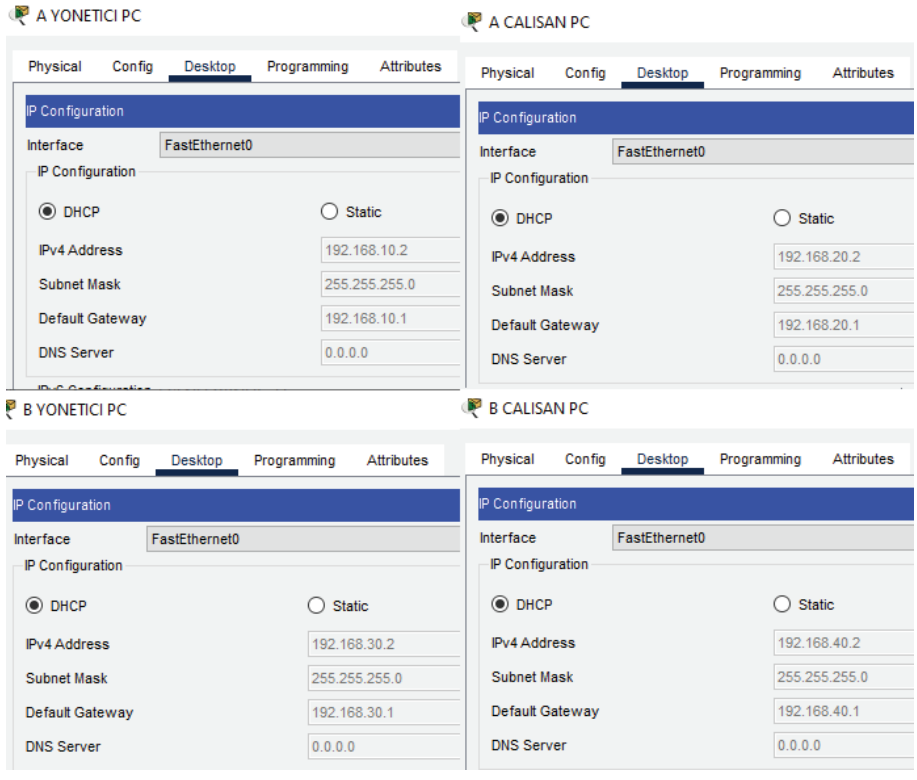
RouterB(config)#interface gigabitEthernet 0/0.30
RouterB(config-subif)#encapsulation dot1Q 30
RouterB(config-subif)#ip address 192.168.30.1 255.255.255.0
RouterB(config-subif)#no shutdown
RouterB(config-subif)#exit
RouterB(config)#interface gigabitEthernet 0/0.40

RouterB(config-subif)#encapsulation dot1Q 40
RouterB(config-subif)#ip address 192.168.40.1 255.255.255.0
RouterB(config-subif)#no shutdown
RouterB(config-subif)#exit
RouterB(config)#do write
Building configuration...
[OK]

6. Adım: Bilgisayarların otomatik IP alabilmeleri için yönlendiricilere gerekli IP havuzunu oluşturunuz.
RouterA(config)#ip DHCP pool YONETIM
RouterA(DHCP-config)#network 192.168.10.0 255.255.255.0
RouterA(DHCP-config)#default-router 192.168.10.1
RouterA(DHCP-config)#exit
RouterA(config)#ip DHCP excluded-address 192.168.10.1
RouterA(config)#ip DHCP pool CALISAN
RouterA(DHCP-config)#network 192.168.20.0 255.255.255.0
RouterA(DHCP-config)#default-router 192.168.20.1
RouterA(DHCP-config)#exit
RouterA(config)#ip DHCP excluded-address 192.168.20.1
RouterA(config)#do write
Building configuration...
[OK]

RouterB(config)#ip DHCP pool YONETIM
RouterB(DHCP-config)#network 192.168.30.0 255.255.255.0
RouterB(DHCP-config)#default-router 192.168.30.1
RouterB(DHCP-config)#exit
RouterB(config)#ip DHCP excluded-address 192.168.30.1
RouterB(config)#ip DHCP pool CALISAN
RouterB(DHCP-config)#network 192.168.40.0 255.255.255.0
RouterB(DHCP-config)#default-router 192.168.40.1
RouterB(DHCP-config)#exit
RouterB(config)#ip DHCP excluded-address 192.168.40.1
RouterB(config)#do write
Building configuration...
[OK]

Bu adıma kadar olan yapılandırma sorunsuz tamamlanmışsa ağdaki bilgisayarlar ilgili IP havuzlarından otomatik IP alacaktır (Görsel 3.18).



Görsel 3.18: IP bilgi ekranı

7. Adım: Şubelerin birbirleri ile haberleşebilmesi için yönlendiriciler arası arayüzlere (Serial 0/0/0) IP'leri verilir ve aşağıdaki yönlendirme komutları yazılır. İşlemi tamamlayınca rotalama sonucunu görüntüleyiniz (Görsel 3.19).

Dinamik Rotalama ile

```
RouterA(config)#interface serial 0/0/0
RouterA(config-if)#ip address 192.168.50.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#router rip
RouterA(config-router)#network 192.168.10.0
RouterA(config-router)#network 192.168.20.0
RouterA(config-router)#network 192.168.50.0
RouterA(config-router)#exit
RouterA(config)#do write
Building configuration...
[OK]

RouterA(config)#interface serial 0/0/0
RouterA(config-if)#ip address 192.168.50.2 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#router rip
```

RouterA(config-router)#network 192.168.30.0
RouterA(config-router)#network 192.168.40.0
RouterA(config-router)#network 192.168.50.0
RouterA(config-router)#exit
RouterA(config)#do write
Building configuration...
[OK]

Statik Rotalama ile

RouterA(config)#interface serial 0/0/0
RouterA(config-if)#ip address 192.168.50.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#ip route 192.168.30.0 255.255.255.0 Serial 0/0/0
RouterA(config)#ip route 192.168.40.0 255.255.255.0 Serial 0/0/0
RouterA(config)#do write
Building configuration...
[OK]

RouterB(config)#interface serial 0/0/0
RouterB(config-if)#ip address 192.168.50.2 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#ip route 192.168.10.0 255.255.255.0 Serial 0/0/0
RouterB(config)#ip route 192.168.20.0 255.255.255.0 Serial 0/0/0
RouterB(config)#do write
Building configuration...
[OK]

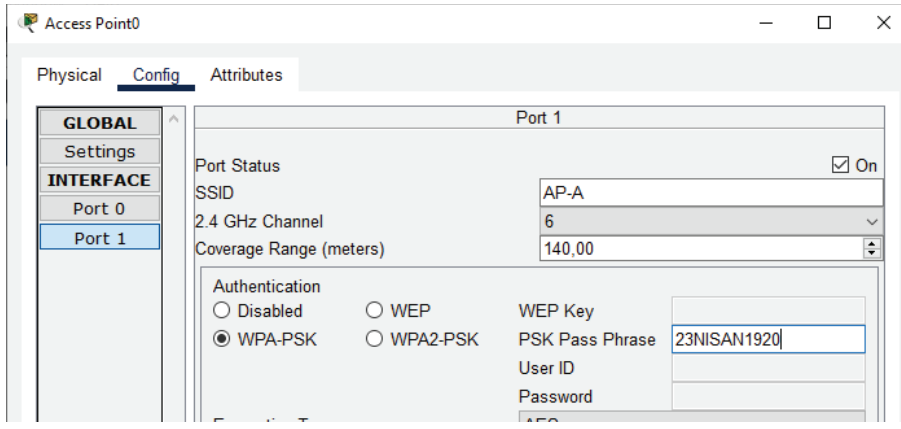
```
RouterA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
R    192.168.30.0/24 [120/1] via 192.168.50.2, 00:00:04, Serial0/0/0
R    192.168.40.0/24 [120/1] via 192.168.50.2, 00:00:04, Serial0/0/0
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, Serial0/0/0
L       192.168.50.1/32 is directly connected, Serial0/0/0
```

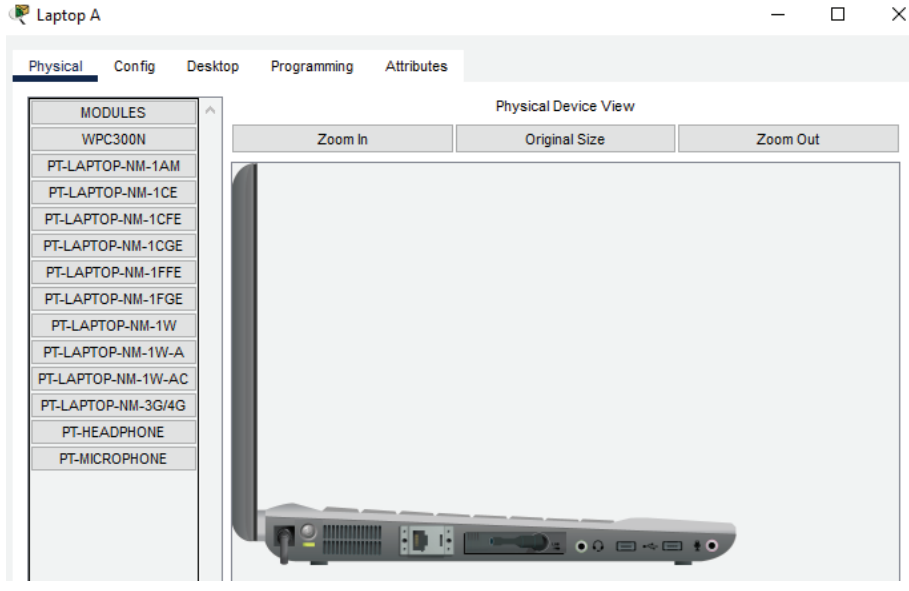
Görsel 3.19: RouterA rotalama sonucu

8. Adım: Access Point cihazının SSID ayarlarını ve kablosuz dizüstü bilgisayar bağlantısını yapınız.



Görsel 3.20: Erişim noktası ayar ekranı

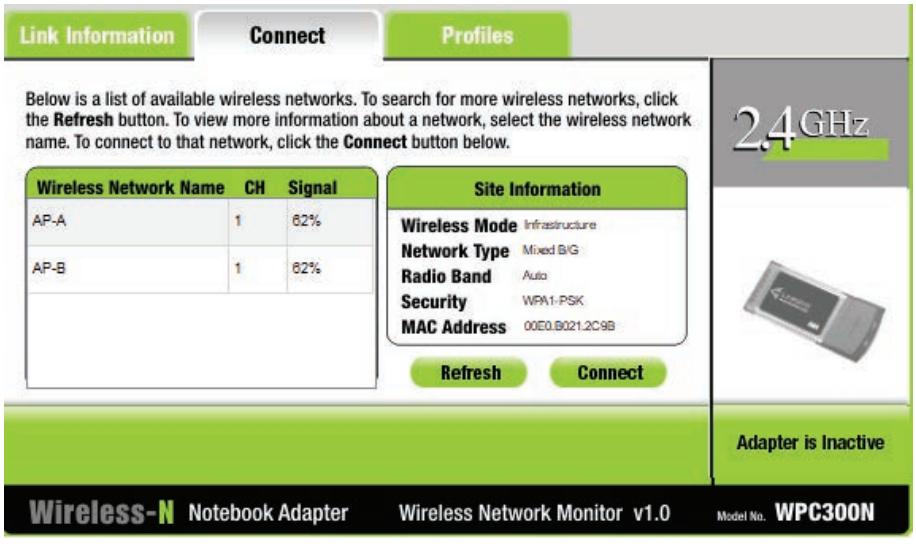
Görsel 3.20'deki gibi Port 1 arayüzünde SSID alanına AP-A, Authentication kısmında WPA-PSK şifreleme alanına 23NISAN1920 şifresini yazınız.



Görsel 3.21: Kablosuz aparat takma

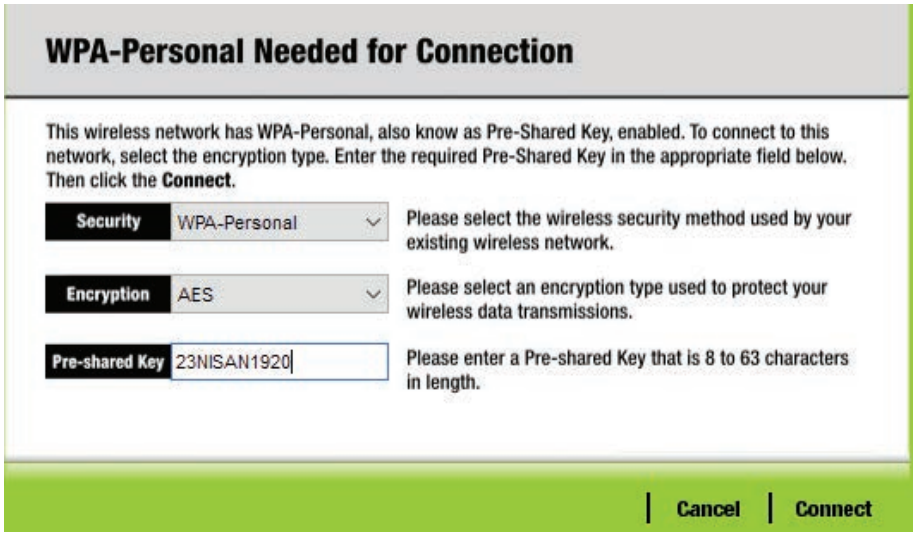
Görsel 3.21'deki gibi Physical sekmesinden WPC300N eklentisini dizüstü bilgisayarda ilgili alana takınız.

Dizüstü bilgisayarda masaüstü uygulamalarının bulunduğu ekrandan **PC Wireless** uygulamasını çalıştırınız. Görsel 3.22'deki **Connect** sekmesine gelerek **Refresh** butonuna basınız. Listelenen SSID isimlerinden **AP-A** olanı seçip **Connect** butonuna basınız.



Görsel 3.22: Kablosuz ağ tarama

Karşınıza gelen Görsel 3.23'teki pencerede **Pre-shared Key** alanına **23NISAN1920** olarak belirlediğiniz şifreyi yazarak **Connect** butonuna basınız.



Görsel 3.23: Kablosuz güvenlik ekranı

9. Adım: Yönlendirici güvenliğini sağlamak için konsol ve telnet bağlantısı için şifre belirleyiniz ve anahtarların port güvenliğini arttırınız.

RouterA>enable
RouterA#configure terminal
RouterA(config)#enable secret 19MAYIS1919
RouterA(config)#line vty 0 15
RouterA(config-line)#enable
RouterA(config-line)#password 29EKIM1923
RouterA(config-line)#login
RouterA(config-line)#exit
RouterA(config)#line console 0
RouterA(config-line)#password 10KASIM1938
RouterA(config-line)#login
RouterA(config-line)#exit
RouterA(config)#do write
Building configuration…
[OK]

RouterB>enable
RouterB#configure terminal
RouterB(config)#enable secret 19MAYIS1919
RouterB(config)#line vty 0 15
RouterB(config-line)#enable
RouterB(config-line)#password 29EKIM1923
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#line console 0
RouterB(config-line)#password 10KASIM1938
RouterB(config-line)#login
RouterB(config-line)#exit
RouterB(config)#do write
Building configuration…
[OK]

SwitchA>enable
SwitchA#configure terminal
SwitchA(config)#interface range fastEthernet 0/1-24
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport port-security mac-address sticky
SwitchA(config-if-range)#switchport port-security maximum 1
SwitchA(config-if-range)#switchport port-security violation shutdown
SwitchA(config-if-range)#do write
Building configuration…
[OK]

SwitchB>enable
SwitchB#configure terminal
SwitchB(config)#interface range fastEthernet 0/1-24
SwitchB(config-if-range)#switchport mode access
SwitchB(config-if-range)#switchport port-security mac-address sticky
SwitchB(config-if-range)#switchport port-security maximum 1
SwitchB(config-if-range)#switchport port-security violation shutdown
SwitchB(config-if-range)#do write
Building configuration…
[OK]

10. Adım: Çalışan bilgisayarların telnet ile yönlendiricilere uzaktan bağlanmasını engelleyiniz.
RouterA>enable
RouterA#configure terminal
RouterA(config)#access-list 10 permit 192.168.10.0 0.0.0.255
RouterA(config)#access-list 10 deny any
RouterA(config)#line vty 0 15
RouterA(config-line)#access-class 10 in
RouterA(config-line)#exit
RouterA(config)# do write
Building configuration…
[OK]

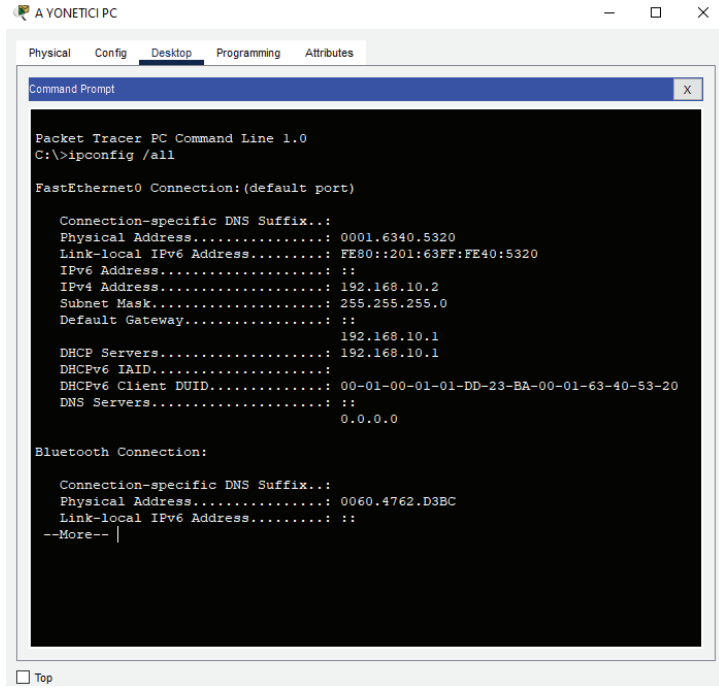
RouterB>enable
RouterB#configure terminal
RouterB(config)#access-list 10 permit 192.168.30.0 0.0.0.255
RouterB(config)#access-list 10 deny any
RouterB(config)#line vty 0 15
RouterB(config-line)#access-class 10 in
RouterB(config-line)#exit
RouterB(config)# do write
Building configuration…
[OK]

3.3. TEST VE BAKIM ADIMLARI

Hazırlanan senaryoyu mutlaka test ediniz, varsa hataları düzeltiniz.

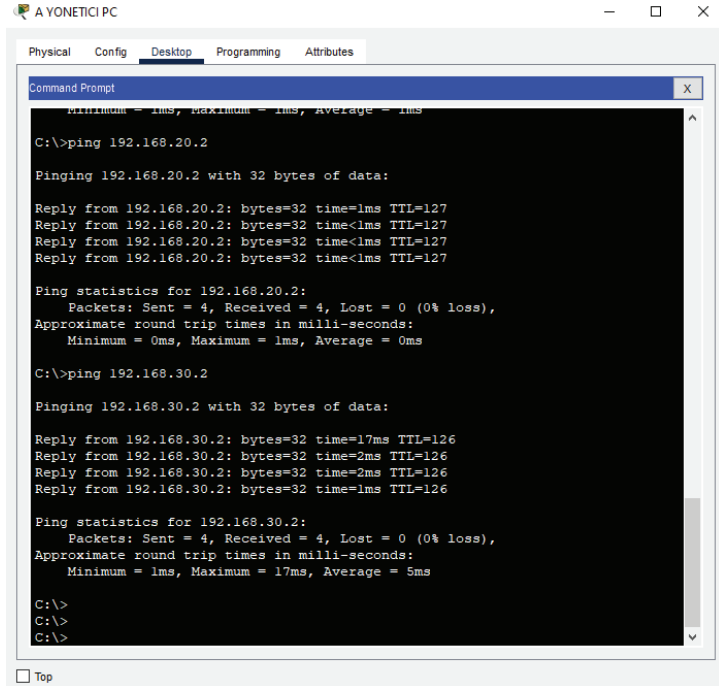
3.3.1 Test Aşamaları

Ağdaki herhangi bir bilgisayarda ipconfig komutunu çalıştırarak havuzdan otomatik IP alıp almadığını kontrol ediniz. Bu işlem için bilgisayarda komut satırı penceresini açarak Görsel 3.24'teki komutları yazınız ve sonucunu kontrol ediniz.



Görsel 3.24: İpconfig komutu çıktısı

Bilgisayarlar arası iletişimin gerçekleşip gerçekleşmediğini kontrol ediniz. Bu işlem için Görsel 3.25'teki komutları çalıştırarak ağ içindeki ve ağ dışındaki bir bilgisayara **ping** atınız. Atılan ping'in ulaşıp ulaşmadığını kontrol ediniz.

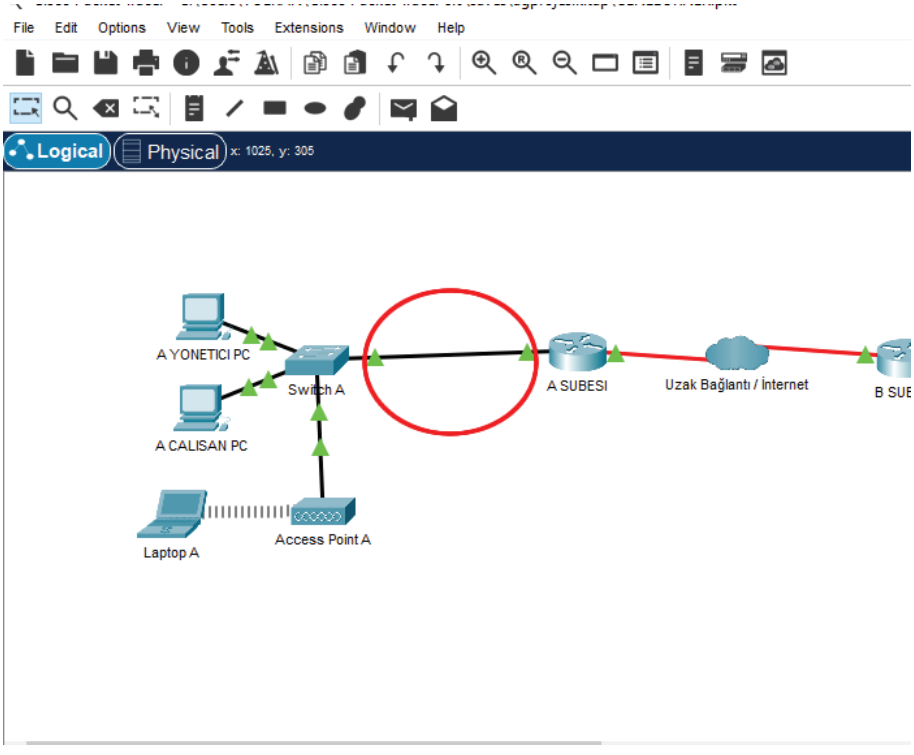


Görsel 3.25: Ping komutu çıktısı

3.3.1 Ağ İzleme

Ağ içindeki veri alışverişini izleyebilmek için çeşitli yazılımlar ve cihazlar kullanılır. **Sniffer** da bu yazılımı kullanan cihazlardan biridir. **Sniffer** kullanarak ağı izlemek için aşağıdaki adımları uygulayınız.

1. Adım: Ağın izlenmesi istenen bölgesini Görsel 3.26'daki gibi belirleyiniz.



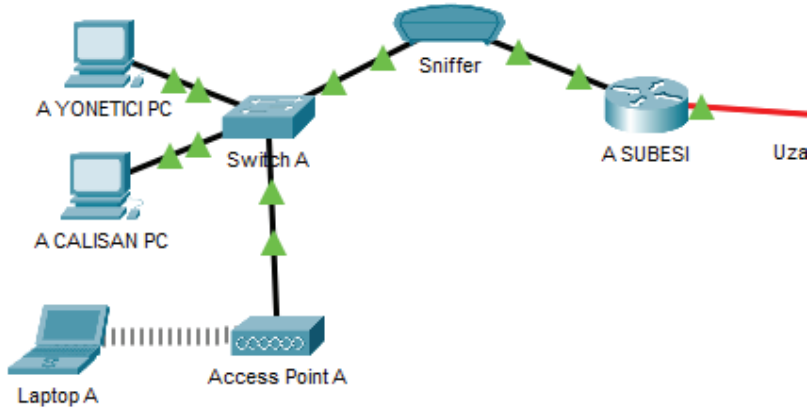
Görsel 3.26: Packet tracer ana ekran

2. Adım: Görsel 3.27'deki End Devices alanından Sniffer aygıtını senaryoya ekleyiniz.



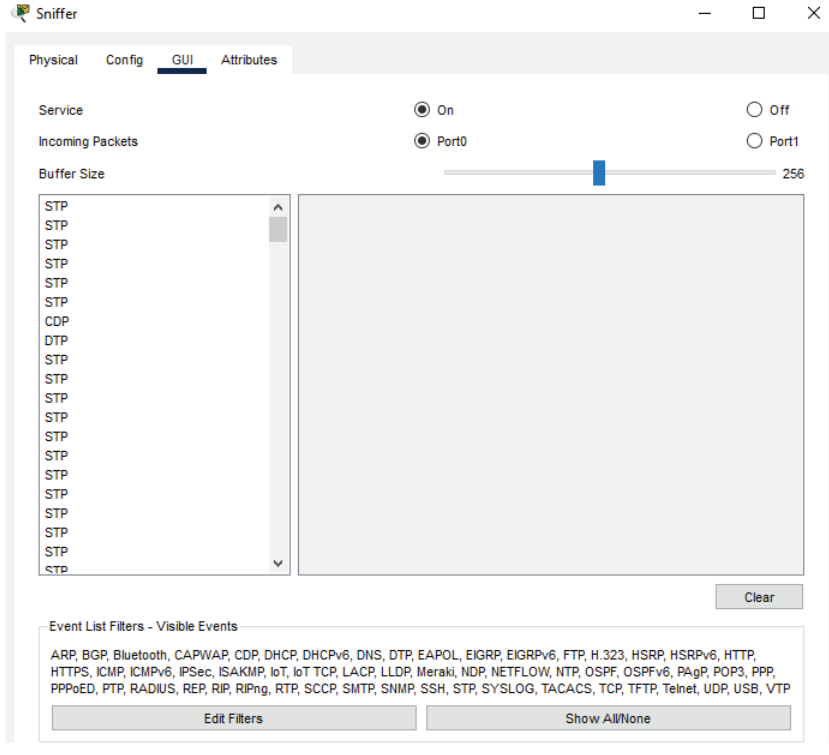
Görsel 3.27: End Devices alanı

3. Adım: Sniffer cihazının bağlantılarını Görsel 3.28'deki gibi yapınız. SwitchA anahtar cihazının GigabitEthernet0/1 portunu Sniffer cihazının Ethernet0 portuna, Sniffer cihazının Ethernet1 portunu A SUBESI yönlendiricisinin GigabitEthernet0/1 portuna bağlayınız.



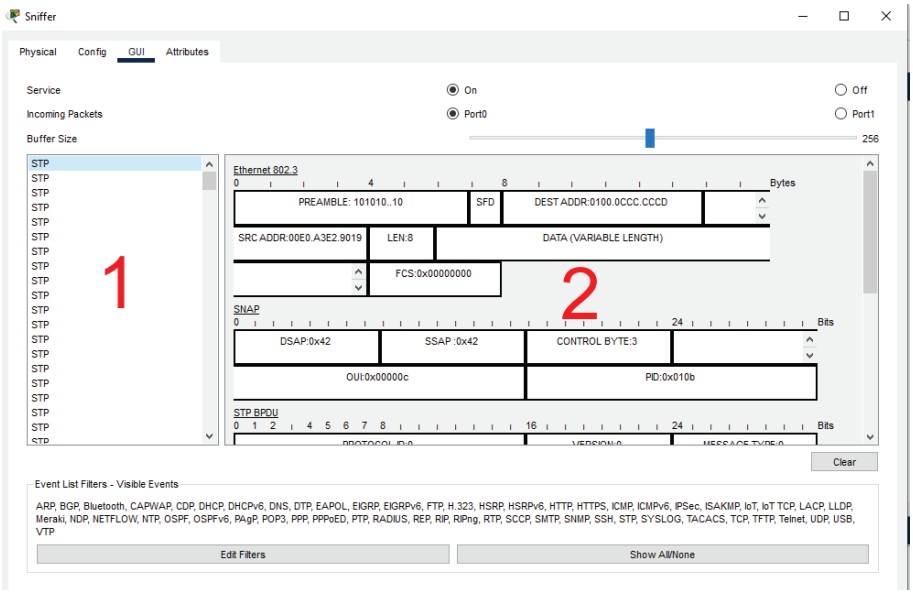
Görsel 3.28 Sniffer cihazı bağlantısı

4. Adım: Sniffer cihazının GUI sekmesini açarak Service alanını On yapınız ve Incoming Packets alanından paketlerin hangi yönde izleneceğini seçiniz (Görsel 3.29).



Görsel 3.29: Sniffer ana ekran

5. Adım: Sniffer cihazının GUI sekmesinde Görsel 3.30'da görüldüğü gibi Buffer Size alanının 1 No.lu kısmında paketlerin türü listelenir. Bu alandan seçilen paketin içeriğiyse 2 No.lu kısımda görüntülenir. Paketleri tek tek inceleyiniz.



Görsel 3.30: Sniffer grafik arayüz

3.4. PROJE RAPORU

İşletme için istenen ağ oluşturulur ve yapılan işin sonunda aşağıdaki rapor oluşturulur.

Projenin Adı: MEB Firması Şubeleri Ağ Kurulumu
Projenin Amacı: Ağ altyapısı bulunmayan MEB firmasının ağ altyapısı oluşturmak.
Projenin Planlanması Firmanın her iki şubesinde de ayrı ayrı 3 yönetici, 10 çalışan bilgisayarı bulunmaktadır. Herhangi bir ağ altyapısı bulunmamaktadır. Her şube için; 1 adet yönlendirici, 1 adet anahtar, 1 adet kabin, 1 adet erişim noktası cihazı, 300 metre CAT5 kablo, 150 metre kablo kanalı, 100 adet RJ45 jak'a ihtiyaç olduğu belirlenmiştir.

Projenin Uygulaması

Kabin sistem odası olarak belirlenen odaya monte edildi.

Yönlendirici ve anahtar kabinde ilgili alana monte edildi.

Erişim noktası cihazı belirlenen noktaya monte edildi.

Sistem odasından tüm odalara kablo kanalları döşendi.

Anahtar cihazdan tüm bilgisayarlara döşenen kablo kanallarından CAT5 kablo çekildi ve uçlarına RJ45 jak çakıldı.

Anahtar ve yönlendirici yazılımı programlandı.

Tüm kablolar bilgisayarlara takıldı.

Erişim noktası cihazına kablosuz bağlanacak cihazların SSID ve şifre bilgileri girildi ve ağa dâhil edildi.

Test ve Sonuç

Tüm kablolar iki taraflı kablo test cihazı yardımıyla kopukluk veya hatalı uç yapımına karşı test edildi.

Tüm cihazlardan ping, ipconfig vb. test komutları çalıştırılarak ip almaları, ağ üzerinde haberleşmeleri kontrol edildi ve sorun olmadığı yazılı olarak raporlandı.

Kablosuz ağ bilgileri, ağ diyagramı, IP adresleme yapısı sistem odasına dosya hâlinde oluşturuldu; bazı bilgiler görünecek şekilde kabin üzerine asıldı.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçeneği işaretleyiniz.

1. DHCP ile IP havuzu oluşturulurken dağıtım dışı bırakılmak istenen IP'ler için kullanılan komut aşağıdakilerden hangisidir?

A) excluded-address
B) inclluded address
C) outer address
D) outing
E) incoming

2. Switch portunu VLAN 'a üye yapmak için kullanılan komut aşağıdakilerden hangisidir?

A) swichport form vlan
B) swichport record vlan
C) swichport in vlan
D) swichport acccess vlan
E) swichport mode trunk

3. TELNET ayarlarına giriş yapmak için kullanılan komut aşağıdakilerden hangisidir?

A) line password
B) line enter
C) line vty
D) line console
E) line telnet

4. Birden fazla arayüz ile ilgili ayarlama yapmak için kullanılan komut aşağıdakilerden hangisidir?

A) interface fastethernet
B) interface range
C) interface gigabitethernet
D) interface settings
E) Hiçbiri

5. Yapılan değişiklikleri kaydetmek için kullanılan komut aşağıdakilerden hangisidir?

A) load
B) memory
C) record
D) save
E) write

4. ÖĞRENME BİRİMİ
SUNUCU PROJESİ HAZIRLAMA

KONULAR

4.1. SUNUCU PROJESİ PLANLAMA AŞAMASI

4.2. SUNUCU İŞLETİM SİSTEMİ YAPILANDIRMASI

NELER ÖĞRENECEKSİNİZ?

- DHCP Server uygulama
- VLAN oluşturma
- ACL oluşturma
- Statik ve dinamik yönlendirme
- Ağ cihazlarının güvenliği sağlama

TEMEL KAVRAMLAR

Sunucu, İstemci, Etki Alanı, Ağaç, DNS, FTP, SMTP



HAZIRLIK ÇALIŞMALARI

1. Sunucular, hangi hizmetleri istemcilere verir? Araştırarak sınıfta arkadaşlarınızla paylaşınız.

2. Sunucuların iyi planlanmadan yapılandırılması ne tür problemler oluşturur? Düşüncelerinizi sınıfta arkadaşlarınızla paylaşınız.

4.1. SUNUCU PROJESİ PLANLAMA AŞAMASI

Ağ üzerinde bulunan istemci cihazlara veri, kaynak ve dosya paylaşımları yapan, bunun yanında çeşitli hizmetler sunan donanımsal olarak üst düzey cihazlara sunucu ya da server ismi verilmektedir.

Sunucular; istemci cihazların kaynak paylaşımını, İP dağıtımını, DNS yönetimini, kısıtlama işlemlerini, uzaktan bağlanma ve yazıcı hizmetlerini yönetme, veri tabanı barındırma, çevrim içi oyunlar için alan sağlama gibi birçok görevi yerine getirebilen gelişmiş cihazlardır.

Sunucular içlerinde RAM, işlemci, yerel disk gibi klasik bilgisayarlarda bulunan donanımlara sahiptir. Fakat bu donanımlar evlerde ve ofislerde kullandığımız bilgisayarlardan çok daha gelişmiş özelliklere sahip, çok daha fazla kişi ve cihaza hizmet verebilecek kapasitede bilgisayarlardır.

Sunucular gelişmiş hizmetleri kullanıcılara verebilmek için özel yazılımlara ihtiyaç duyar. Sunucu işletim sistemleri denen bu yazılımlar sayesinde daha hızlı, güvenli ve daha fazla kişiye hizmet verebilecek yapıya sunucu sahip olur.

Bir sunucunun en temel özelliği verileri güvenli, hızlı ve kesintisiz bir performansla verdiği hizmeti istemcilere sunabilmesidir (Görsel 4.1).



Görsel 4.1: Sunucu projesi planlama

4.1.1. Sunucu Seçimi ve Planlanması

Sunucular vermiş oldukları hizmet ve servislere göre isimlendirilir. Birden fazla servisi ve hizmeti aynı cihaz üzerinden verebilir. Sunucuların verdiği hizmet ve servisler için ayrı ayrı sunucular olabilir. Sunucular bir web sitesini barındırmak, e-posta hizmeti sunmak, veri tabanı servislerini üzerinde bulundurmak gibi verilerin çok önemli olduğu hizmetleri de verebilir. Sunucunun vermiş olduğu hizmetler aşağıda sıralanmıştır.

- Dosya sunucu
- Veri tabanı sunucu

- Site yayınlama sunucusu
- Vekil sunucu (proxy server)
- DNS sunucusu
- DHCP sunucusu
- Yazıcı sunucusu
- SMTP sunucusu

Yukarıda yazılan hizmetlere bakarak doğru sunucuyu doğru bir şekilde yapılandırmak verilen hizmetin kalitesi açısından önemlidir. Veri tabanı sunucusu ile yazıcı sunucusunun aynı cihaz üzerinden hizmet vermesi büyük sorunlara yol açabilir. Bu yüzden doğru sunucu seçimi planlaması yapılmalıdır.

Sunucu seçimi yapılırken kurumların ihtiyaçları belirlenmeli ve planlamalarının doğru ve ölçeklenebilir olması gerekir. Kurumların sunucu projesi için ayırdığı bütçe, kullanılacak cihazlar, verilecek hizmetler, altyapı, güvenlik ve kurumların özel ihtiyaçları sunucu seçiminde önemli olan unsurlardır. Doğru seçilmemiş bir sunucu ve doğru planlama yapılmamış bir sunucu projesi hizmetlerin aksamasına, verilerin kaybolmasına, maddi ve manevi kayıpların oluşmasına yol açabilir (Görsel 4.2).



Görsel 4.2: Sunucu rolleri

Doğru sunucu seçiminde aşağıda sıralanan unsurlar dikkate alınmalıdır.

İşlemci Mimarisi: Sunucu seçiminde ve performansında en önemli kıstaslardan biri işlemci mimarisinin seçimidir. Seçilen işlemci modeline göre verilen hizmetin performansı ve hizmet verilen sayısı artabilir. Seçilen işlemcinin çekirdek sayısı, ön bellek hızı performansı doğrudan etkileyen unsurların başında gelir. Kesintisiz hizmet veren sunucularda işlemcinin ısınması ve performans düşüklüğü büyük problemlere yol açar. Çeşitli markaların veri merkezleri sunucularına özel olarak üretilen işlemci modelleri bulunur. Tercih ederken ev ve küçük işletmelere yönelik işlemciler yerine veri merkezlerine yönelik olarak üretilen işlemciler tercih edilmelidir.

Disk ve Raid Sistemi Seçimi: Sabit disk teknolojileri geçmişten günümüze değişime uğramıştır. Sabit disklerdeki bu gelişim, verilerin aktarımının daha hızlı olmasına ve verinin önem arz ettiği işlerde performansın artmasını sağlamıştır. Sabit disklerin dönme hızı (RPM) ve dönerken ısınması, sunucuların performansını etkiler. Hâliyle sabit disk seçimi verilecek hizmetin planlanması aşamasında önemlidir. Günümüzdeyse SSD en yaygın ve en çok kullanılan disk teknolojileri arasındadır. SSD diskler sabit disklere oranla daha hızlı, daha düşük gerilimlerde çalışması ve mekanik kısımlarının fazla olmaması sebebiyle çok daha hızlı veri akışı sağlayabilmektedir. Disklerin seçiminin ardından kullanılacak olan RAID disk yapısı da yine projenin planlama aşamasında yapılması gereken önemli işlerden biridir. Verinin hızlı aktarılması, yedek-

lenmesi ve güvenliğin boyutuna göre uygun RAID yapısı ve disk sistemi seçilmelidir.

Kurumların İstek ve Yapısı: Kişi veya kurumların sunucuyu hangi amaçla kullanmak istediğine dair rapor istenir, bu rapora göre doğru sunucu seçilmelidir. Kurumların istek ve yapıları genel olarak sunucu türünün ayrıca hizmet ve rollerin belirlenmesinde en önemli faktördür. Personel verilerinin tutulmasından gizliliği önemli bilgilerin saklanmasına kadar kurumların istekleri, sunucu seçiminde ve sunucu projelerinin planlamasında çok önemlidir. Kurumların mevcut personel, donanım ve fiziki yapısı da yine sunucu projelerinin hazırlanmasını etkileyen faktörlerdir. Sunucunun ölçeklenebilir, geliştirilebilir; kurumların istek ve yapılarına cevap verebilir olması sunucuyu projelendirirken maliyet ve performans açısından önemlidir.

Sistem Odası Tasarımı ve Kurulumu: Sistem odasının yerinin seçimi ve projelendirmesi, kullanılacak olan teknolojilerin ve kapasitelerinin belirlenmesi amacıyla mutlaka bir sistem odası tasarım raporu hazırlanmalıdır. Raporun içeriğinde sistem odasının fiziksel yerleşim konumu, kablolama altyapı planlaması, sunucu kapasitesi, sistem odası enerji altyapısı, ortam sıcaklığı, su baskınlarına ve diğer olağanüstü durumlara karşı yükseltilmiş taban, UPS güç kaynağı, trafo, sistem odasının kamera ile izlenmesi ve güvenlik kıstasları mutlaka olmalıdır. Kullanılacak teknoloji ve ekipmanların listesi hazırlanmalıdır. Hazırlanacak olan sistem odası tasarımının çizim programları ile desteklenmesi planlamanın daha verimli olmasını sağlar. Hazırlanacak planlama ve raporlarda öngörülen felaket senaryoları ve bunların çözümlerinin belirtilmesi önemlidir.

4.1.2 Sunucu Odası Plan ve Raporlaması

Örnek bir sistem odası tasarımında ve raporlanmasında aşağıdaki bilgiler kullanılır.

1. Sistem odası tasarımı için planlanan yerin ve çevrenin uygunluğu araştırılır ve aşağıdaki sorulara cevap aranarak veriler hazırlanır.

- Deprem tehlikesi var mı?
- Sel ve su baskını tehlikesi var mı?
- Çevrede elektromanyetizmayı etkiyecek unsurlar var mı?
- Terör vb. olaylar yönünden risk barındırıyor mu?
- Bina dışı çevresel koşullarda problem yaratacak bir durum var mı?
- Ekipmanların taşınıp yerleştirilmesi için yeterli alan mevcut mu?
- Oda içinde pencere var mı?

2. Sistem odasının tasarımı için gerekli ağ altyapısı raporu aşağıdaki bilgiler kullanılarak hazırlanır.

- Kurumun ihtiyaç duyduğu bağlantı hızı belirlenir.
- Ağ iletişiminde çıkabilecek problemler için yedekleme yolları hazırlanır.
- Sistem odası kablolama ve ağ cihazları tasarımı için gerekli hazırlıklar yapılır.
- Mantıksal ve fiziksel topolojiler hazırlanır.
- Ağ iletişiminde kullanılacak standartlar belirlenir.

3. Sistem odasının elektrik ve enerji altyapısı aşağıdaki bilgiler kullanılarak planlanır.

- Sistem odasının bulunduğu çevrenin trafo kapasitesi öğrenilir.
- Trafo kapasitesine göre büyüme kapasitesi hesaplanır.
- Şebeke enerjisinin kesilmesi durumunda jeneratörün devreye gireceği sistem planlanır.
- Klimalar ve diğer bilişim teknolojileri ekipmanlarının kullandığı enerji miktarlarına göre jeneratörler planlanır.

- UPS sistemi tasarımı ve yedekliliği planlanır.
- Elektrik panolarının ölçeklenebilirliği planlanır.
- Elektrik kablolama ve diğer elektrik ekipmanları için standartlar belirlenir.

4. Sistem odasında anahtarlama, yönlendirici, sunucu gibi birçok ısınma ve nem yapabilecek cihaz kullanılır. Sunucu projesi planlama aşamasında sistem odası iklimlendirme bilgileri aşağıdaki veriler kullanılarak planlama raporuna eklenir.

- Klimalar kaç adet ve kapasiteleri ne kadar olmalıdır? Rapora eklenir.
- Kabin ve klima yerleşimleri nasıl olmalıdır, rapora eklenir.
- Klimalar arıza yaptığında yedeklemenin devreye gireceği sistem projelendirilmelidir.

5. Sistem odasının fiziksel güvenliği mutlaka incelenip raporda sunulmalıdır. Raporlama yaparken aşağıdaki bilgiler rapora eklenir.

- Sistem odasını yetkisiz personeller rahatça kullanabiliyor mu?
- Kart okuyucu, parmak izi ya da görüntü işleme ile giriş çıkış yöntemleri maliyet ve kullanım açısından uygun mu?
- Kapılar, kurşun ve yangın geçirmez sistem ile oluşturulabilir mi?
- Kamera güvenlik sisteminin yerleşimi nasıl olmalıdır?
- UPS, trafo ve enerji noktalarının güvenliği sağlanmış durumda mı?

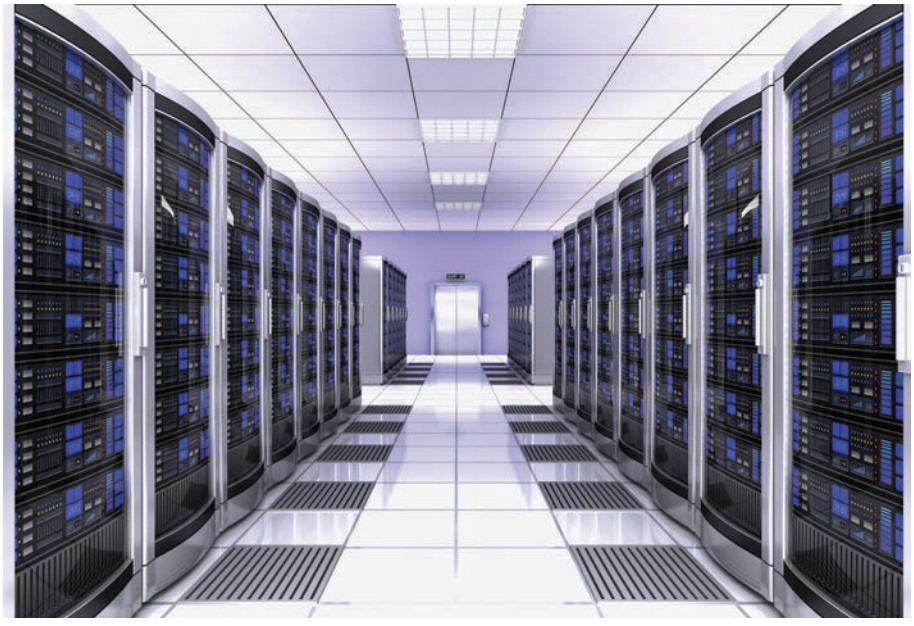
6. Yaşanabilecek doğal önlemlere karşı kriz planları hazırlanmalı ve raporda sunulmalıdır. Aşağıdaki planlamalar rapora eklenir.

- Elektrik kesintisi, su baskını, deprem ve diğer afet durumlarında sunucu güvenliği için planlama yapılır.
- Yaşanacak felaket senaryoları için uyarı ve ikaz sistemleri hazırlanır.
- Deprem yönetmeliğine uygun sistem odası tasarımı yapılır. Gerekirse güçlendirme yapılır.
- Yükseltilmiş zemin sistemleri ile su baskınlarına karşı önlem alınır.

7. Sistem merkezinde ortamın ve sunucunun verilerinin izlenmesi ve takip edilmesi önemlidir. Sunucu odası ve sistemi tasarımı yaparken bu planlamaların raporda sunulması gerekir. Raporda aşağıdaki bilgiler bulunur.

- Sunucu odasının nem, sıcaklık, hava kalitesi gibi bilgileri izlenir.
- Kabinet güvenliği izlenir.
- Su ve tesisat sistemi izlenir.
- Sunucu bilgi güvenliği mutlaka standartlarla takip edilir.

8. Proje çizimlerinde sunucu merkezi tasarımı, planlaması ve raporlaması önemlidir. Bütün detaylar, yedeklemeler ve fiziki alanlar çizimlerle hazırlanıp rapora eklenmelidir. Kablolama yapıları, tesisat yapıları çizim raporlarıyla beraber sunulmalıdır (Görsel 4.3).



Görsel 4.3: Planlanmış bir sunucu odası

4.2. SUNUCU İŞLETİM SİSTEMİ YAPILANDIRMASI

Sunucu odasının planlanması ve raporunun hazırlanmasının ardından sunucu sisteminin seçimi ve sunucunun vereceği hizmetin rollerinin belirlenmesi, hangi servislerin kullanılacağının tespitinin yapılması gerekir. Bunun yanında sunucuların raid disk sistemlerinin belirlenmesi, kullanılacaksa sanallaştırma teknolojilerinin nasıl kullanılacağı mutlaka belirlenmelidir.

Sunucular kullanım amacına göre aşağıdaki hizmetleri seçilecek rollerle verebilir. Aşağıda sunucu işletim sistemlerinin verebileceği hizmetlerden bazıları listelenmiştir.

- Web Sunucusu
- Yazdırma Sunucusu
- Terminal Sunucusu
- Dosya Paylaşım Sunucusu
- DHCP Sunucu
- DNS Sunucusu
- Uzak Masaüstü Hizmetleri Sunucusu
- Active Directory Sunucusu
- Veri Tabanı Sunucusu
- E-Posta Hizmetleri Sunucusu

Sunucular yukarıda belirtilen görevlere göre seçilerek gerekli yapılandırmalarının yapılması gerekir.

4.2.1 Active Directory Yapılandırması

Active Directory, içinde sunucu, istemci, kullanıcı, bilgisayar ve kullanıcı gruplarını barındıran bir veri tabanıdır. Active directory kullanımı sunucunun merkezi bir şekilde yönetilebilmesine imkân tanır. Group Policy kullanarak active directory içinde bulunan kullanıcı ya da kullanıcı gruplarına çeşitli kısıtlamalar yapabilir veya tek noktadan istenilen uygulama ve servislerin kullanılması sağlanabilir.

Active directory kullanmak, sunucuya aşağıdaki özellikleri kazandırır.

- Yönetilebilirlik
- Ölçeklenebilirlik
- Genişletilebilirlik
- Güvenlik Uyumu
- Diğer Dizin Servisleriyle Birlikte Çalışabilme
- Güvenli Kimlik Doğrulama ve Yetkilendirme
- Group Policy ile Yönetim
- Dns ve Dhcp gibi Servislerle Birlikte Çalışabilme Özelliği

4.2.1.1 Active Directory Mantıksal Yapısı

Active Directory mantıksal yapısı, kullanıcı ve yönetici açısından hiyerarşik bir yapı kurarak sistemin yönetilmesini sağlar.

Domain: Merkezî yönetimi sağlamak amacıyla kurulan çekirdek yönetim birimine verilen isimdir.

Domain Tree: Aynı isim altında toplanmış bir ya da daha fazla sayıda domainin hiyerarşik olarak oluşturulduğu yapıya verilen isimdir.

Forest: Birden fazla Tree'nin birleşmiş halidir. Oluşturulan ilk Domain bir Tree'yi ifade eder ve ilk Tree'nin oluşturulmasıyla Forest da oluşmuş olur. Sonradan bu Forest'a eklenecek olan Tree'ler, diğer Tree'lerle aynı isim aralığını paylaşmayacak olsalar da aynı Schema ve Global Catalog'a sahip olur. Forest oluşturulurken kurulmuş olan ilk Tree Forest-Root olarak bilinir ve diğer Tree'ler bu Forest Root altında toplanır.

Organizational Unit: Bir domain içinde kullanıcıları, bilgisayarları, grupları bir arada tutan objelerdir.

Temel işlevleri;

- Organizasyonun hiyerarşisini belirlemek,
- Organizational Unit seviyesinde delegasyon yapabilmek,
- Organizational Unit seviyesinde group policy'ler uygulayabilmektir.

Global Catalog: Global Catalog (GC), Active Directory Forest' ı içinde yer alan her objeyi bulunduran bir veri tabanıdır ve Global Catalog Server'larda tutulur. Bu barındırılan özellikler, varsayılan olarak sorgulamalar esnasında en sık kullanılan özelliklerdir. Global Catalog kullanıcılara şu hizmetleri sunar:

- Gereken verinin nerede olduğundan bağımsız olarak Active Directory objeleri hakkında bilgiler sunar.
- Bir ağa logon olunurken Universal Group Membership bilgisini kullanır.

Global Catalog Sunucusu Domain'deki bir Domain Controller'dır ve Domain'de oluşturulan ilk Domain Controller otomatik olarak Global Catalog seviyesine yükseltilir. Sonradan ek Global Catalog Sunucular eklenebilir.

Trust Relationship: İki farklı domain arasında veri ve kaynak paylaşımı için kurulan güven ilişkisine denir.

Active Directory Schema: Kullanıcı, grup, bilgisayar ve yazıcılar gibi bütün objelere ait bilgileri içerir. Forest içerisinde, sadece bir Schema bulunur ve bütün obje bilgileri bu Schema üzerine yazılır. Kullanıcıların çalıştıkları bölümler ve doğum yeri gibi bilgileri buna örnek olarak verebiliriz. Schema bilgileri, Active Directory veri tabanı (database) içinde depolanır.

- Kullanıcı uygulamaları için dinamik bir yapı sunar. Kullanıcıların obje araştırma işlemleri, Schema üzerinden gerçekleşir.

- Yeni oluşturulan veya değiştirilen obje dinamik olarak Schema içerisinde güncellenir.
- Obje sınıf ve niteliklerinin korunmasında, discretionary access control lists(DACLs) kullanılır.
- DACLs ile Schema üzerinde yalnızca yetkilendirilmiş kullanıcıların (authorized users) değişiklik yapabilmesi sağlanır.

4.2.1.2 Active Directory Fiziksel Yapısı

Active Directory içinde fiziksel yapı, mantıksal yapıdan bağımsız bir mimariye sahiptir. Mantıksal yapı ile ağ kaynakları organize edilirken fiziksel yapı ile ağ trafiğinin kontrolü ve yapılandırması gerçekleştirilebilir. Active Directory'nin fiziksel yapısını; DC (Domain Controller) ve Site'lar oluşturur. Active Directory'nin fiziksel yapısı, replikasyonun yer ve zamanı ile ağa katılımını (logon) belirler. Ağ trafiği ile katılım işlemlerinin optimizasyonu ve bu işlemlerde olabilecek hataların giderilmesi, fiziksel yapının anlaşılmasına bağlıdır.

Domain Controller: Domain Controller, üzerinde Active Directory veri tabanının bir kopyasını (replica) bulunduran sunucudur. Domain'de yapılan herhangi bir değişiklik bir Domain Controller üzerinde gerçekleştirilir ve daha sonra domain'deki tüm Domain Controller'lar bu değişiklikleri replikasyon yoluyla birbirlerine kopyalarlar. Domain Controller'lar dizin bilgisini bulundururlar ve kullanıcıların logon işlemlerini, kimlik doğrulama işlemlerini ve dizin arama işlemlerini yürütürler. Bir Domain'de bir veya daha çok Domain Controller olabilir. Küçük çaplı bir organizasyonda bir Domain Controller bir de Additional Domain Controller yeterli olurken farklı fiziksel lokasyonlara yayılmış büyük bir işletme için bölge başına bir veya iki Domain Controller daha uygun olacaktır. Bir Domain'e birden fazla Domain Controller yerleştirmenin amacı hem hata toleransı sağlamak hem de Domain Controller'lar arasında yük dağılımı yapar.

Sites: Bir Site, birbirlerine yüksek bant genişliğine sahip dış hatlarla bağlanmış bir veya birden fazla IP alt ağlarını ifade etmektedir. Site'ları doğru bir şekilde yapılandırarak kullanıcıların logon işlemlerinde oluşan ağ trafiğini ve replikasyon işlemleri sırasında oluşan yoğunluğu en aza indirgemek için Active Directory'nin alt ağlar arasındaki fiziksel bağlantıları en efektif şekilde kullanılması sağlanabilir. Site oluşturmaktaki başlıca sebepler şunlardır:

- Replikasyon trafiğinin optimize edilmesi
- Kullanıcıların logon esnasında en hızlı ve en güvenilir bağlantıyı kullanarak doğru Domain Controller'ı bulabilmeleri

Active Directory ve DNS: Active Directory ve DNS uyumu, sunucu işletim sisteminin en önemli özelliklerinden biridir. Active Directory ve DNS, objelerin hem Active Directory objeleri hem de DNS domainleri ve kaynak kayıtları (Resource Records) olarak sunulabilecek şekilde benzer bir hiyerarşik isimlendirme yapısına sahiptir. Bu uyumun sonucu olarak sunucu ağındaki bilgisayarlar, Active Directory'ye özgü birtakım servisleri çalıştıran bilgisayarların yerini öğrenmek için DNS sunucuları kullanmaktadır.

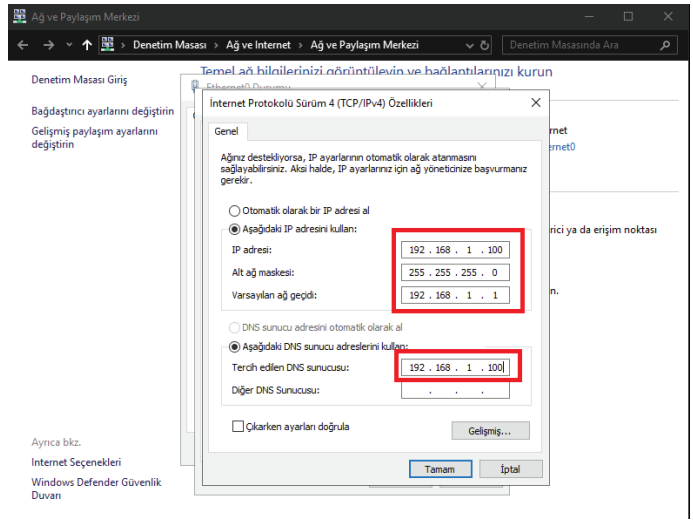
Örneğin, bir istemci Active Directory'ye logon olmak veya herhangi bir kaynağı (yazıcı veya paylaşılmış bir klasör) dizin içerisinde aratmak için bilmesi gereken Domain Controller IP adresini DNS sunucu üzerinde SRV kayıtlarından öğrenmektedir. Active Directory'nin sorunsuz bir şekilde çalışması için DNS sunucularının SRV kayıtlarını eksiksiz bir şekilde barındırması gerekmektedir. SRV kayıtlarının amacı, istemcilere logon esnasında veya herhangi bir kaynağa ulaşıyorken Domain Controller'ların yerlerini belirtmektir. SRV kayıtlarının olmadığı bir ortamda, client'lar Domain'e logon olamayacaktır. Ayrıca sunucu işletim sistemi, DNS bilgilerinin Active Directory veri tabanı ile tümleşik olarak saklanmasına olanak verir. Bu sayede DNS bilgilerinin replikasyonu daha efektif ve güvenli bir hâle gelir.

1. UYGULAMA

Aşağıdaki işlem adımlarına göre sunucu cihazınıza 192.168.1.100/24 IP adres yapılandırmasını veriniz. Sunucu üzerinde MESLEKLISESI.COM isminde bir domain oluşturunuz.

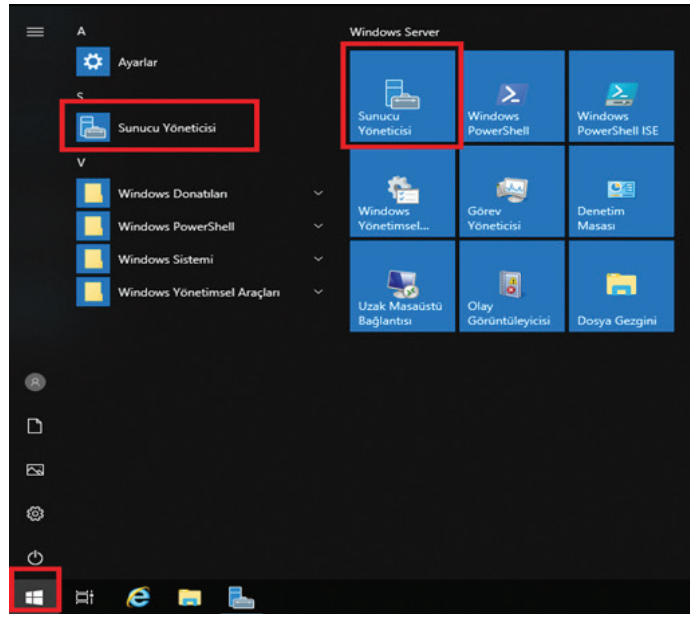
1. Adım: Sunucu cihazınızda yönetimsel yapılandırmaları yapabilmek için Administrator kullanıcısı ile açınız.

2. Adım: Sunucu cihazınıza ağ ve paylaşım merkezi menüsünü kullanarak TCP/IPV4 özellikleri kısmından sabit ip yapılandırmasını giriniz (Görsel 4.4).



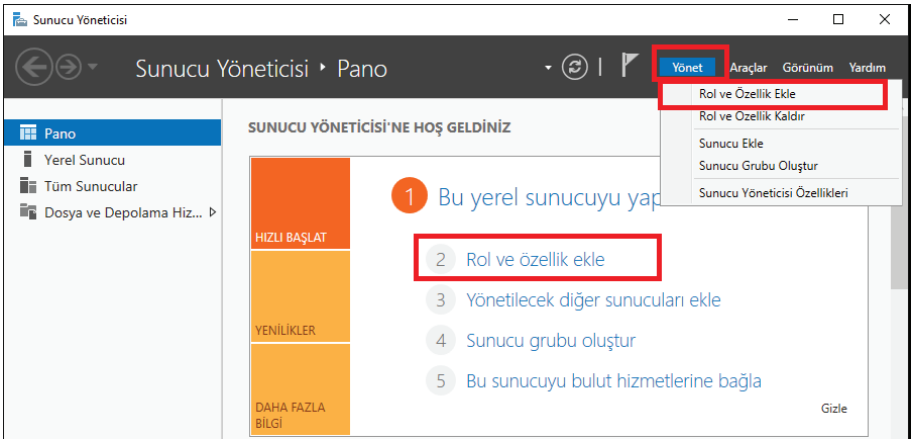
Görsel 4.4: IPV4 Yapılandırması girişi

3. Adım: Klavyeden "Windows butonu"na tıklayarak görev bölümünü açınız. "**Sunucu Yöneticisi**" ikonlarından herhangi birine tıklayınız (Görsel 4.5).



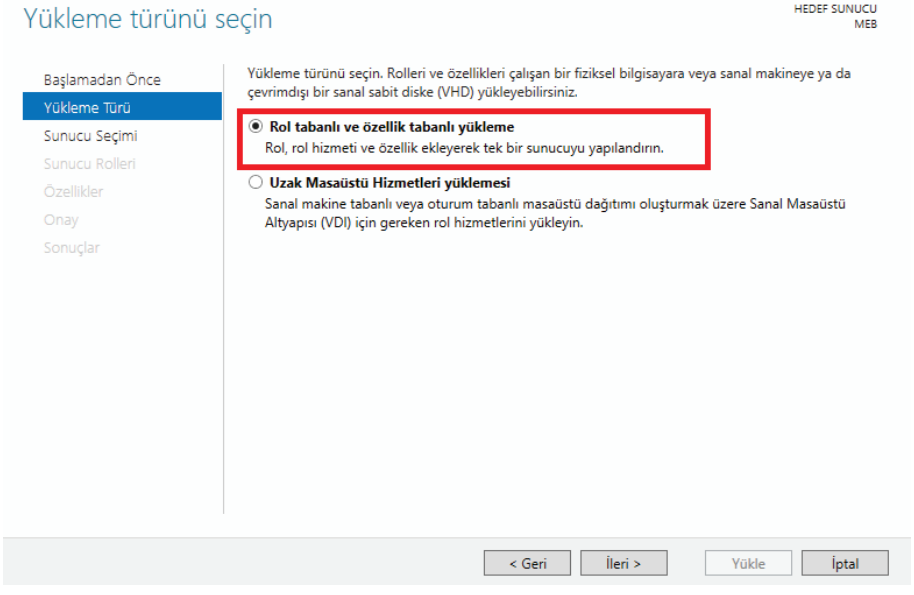
Görsel 4.5: Sunucu yöneticisi girişi

4. Adım: Sunucu Yöneticisi menüsünün sağ üst köşesindek "**yönet**" kısmını kullanarak ya da hızlı menüde "**rol ve özellik ekle**" seçeneğini kullanarak **DNS** kurulumunu başlatınız (Görsel 4.6).



Görsel 4.6: Rol ve özellik ekleme

5. Adım: Gelen ilk ekran bilgilendirme ekranıdır. Bu ekranda ilerle seçeneğini seçerek diğer adıma geçiniz. Gelen pencerede varsayılan olarak gelen "**rol tabanlı ve özellik tabanlı yükleme**" seçeneğini işaretli bırakarak diğer adıma geçiniz (Görsel 4.7).

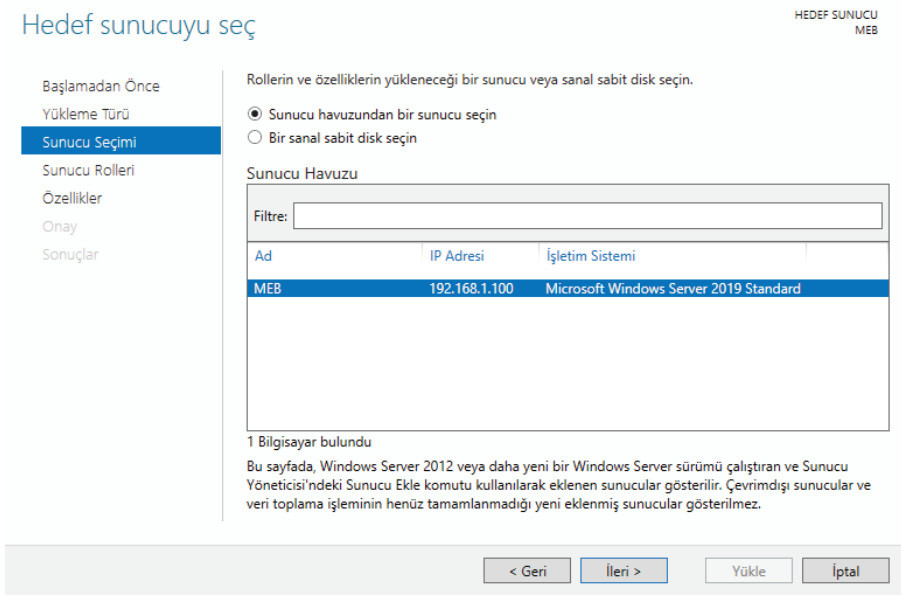


Görsel 4.7: Rol tabanlı özellik yükleme

6. Adım: Gelen ekranda hangi sunucuya rol kurmak istediğiniz sorulmaktadır. Şu an tek bir sunucunuz olduğu için karşınıza tek seçenek gelmektedir. İsmi ve IP adresi verilen sunucunuzu seçerek diğer adıma geçiniz (Görsel 4.8).

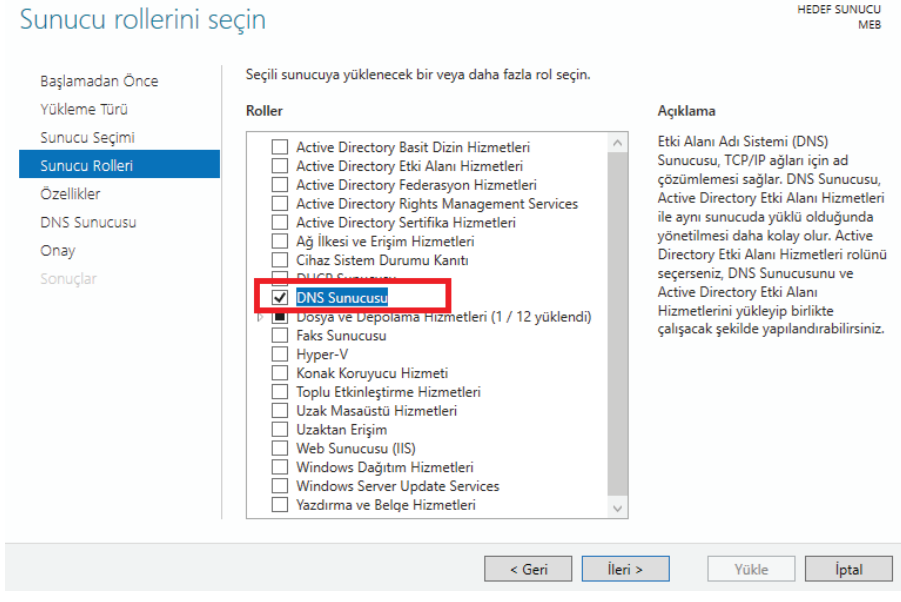
DİKKAT

Kurumsal işletmelerde birden fazla sunucu cihaz bulunabilir ve bu sunucu cihazlardan hangisi seçilirse o cihaza kurulum yapılır.



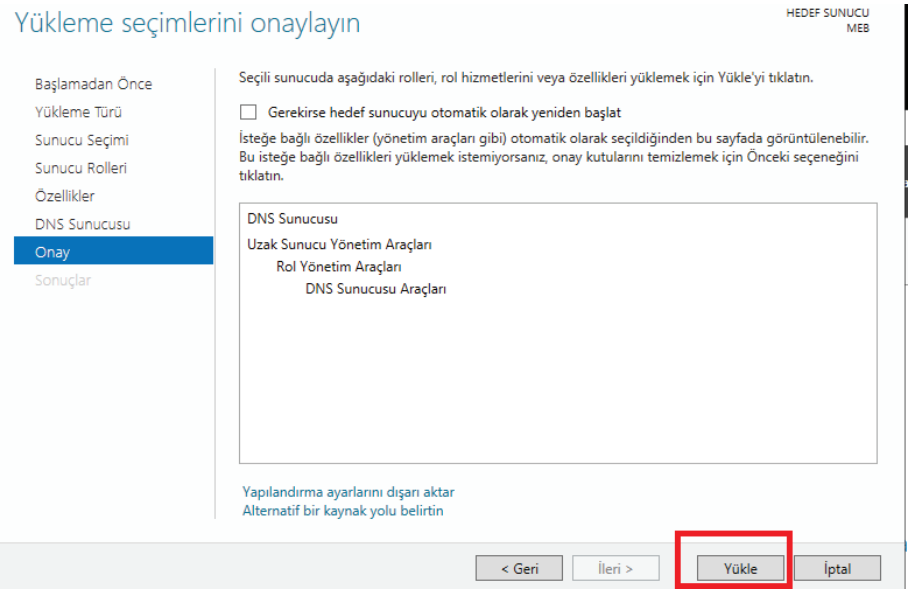
Görsel 4.8: Sunucu seçimi

7. Adım: Gelen ekrandan seçeceğiniz rol olan "DNS Server" kutucuğunu işaretleriz. Karşınıza eklemek isteyebileceğiniz yardımcı roller için bir seçenek gelecektir. Yönetim araçlarını ekle seçeneğinin işaretli olduğuna emin olduktan sonra ilerle diyerek diğer adıma geçiniz (Görsel 4.9).



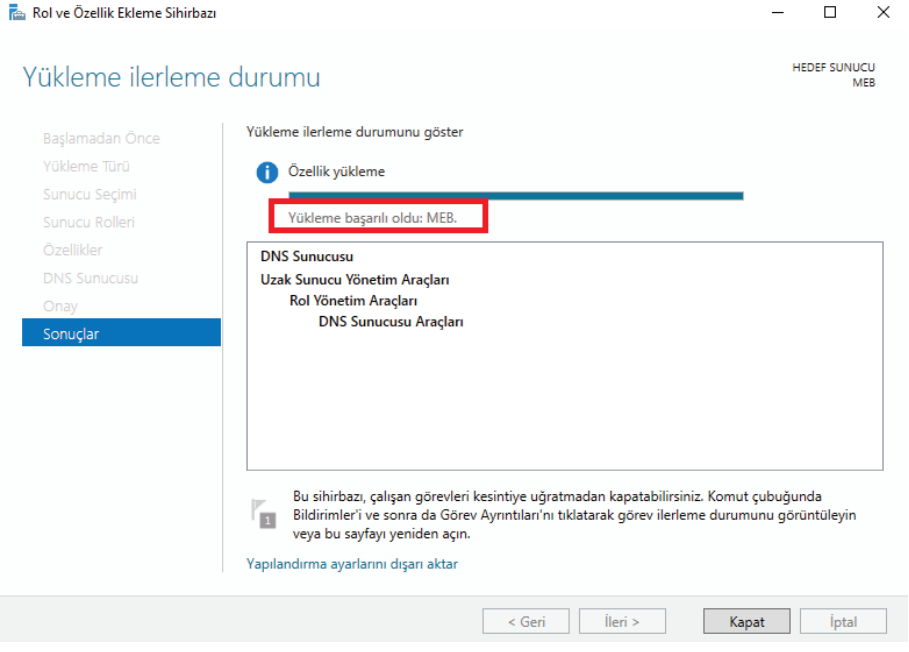
Görsel 4.9: DNS Sunucusu yükleme ekranı

8. Adım: Karşınıza gelecek ekranda herhangi bir ekstra özelliğe daha ihtiyaç varsa seçiniz yoksa ilerle diyerek devam ediniz. Bu ekrandan sonra tekrar bilgilendirme ekranı gelir ve bu ekranda yine ilerle seçilir. En son gelen pencere, işlemleri sonlandırıp DNS kurulumuna başlanan son ekrandır. Bu ekranda yükle butonuna tıklayınız ve DNS rolünü kurunuz (Görsel 4.10).

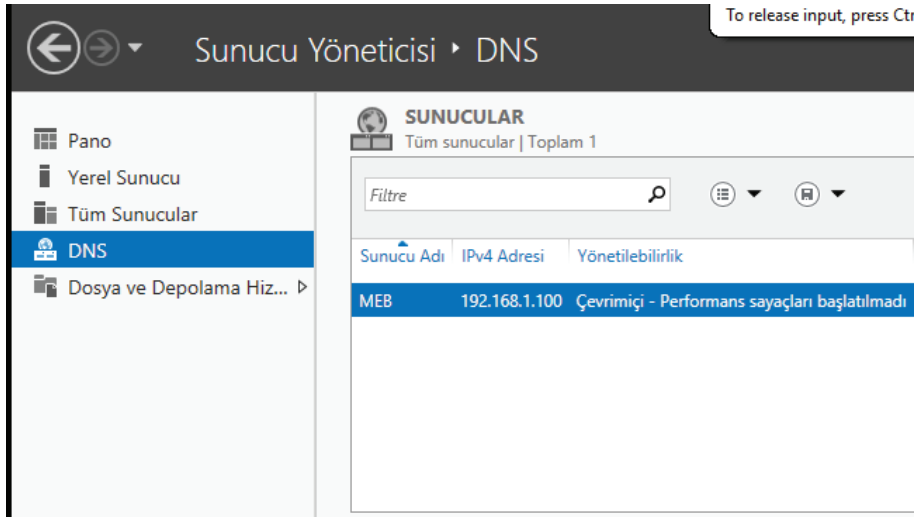


Görsel 4.10: Yükleme seçimlerini onaylama

9. Adım: DNS Server kurulumunun gerçekleştiği mesaj yoluyla aktarılır (Görsel 4.11). Sunucu Yönetimi menüsünden DNS Server kurulumunun doğruluğu kontrol ediniz (Görsel 4.12).



Görsel 4.11: Yükleme doğrulama ekranı

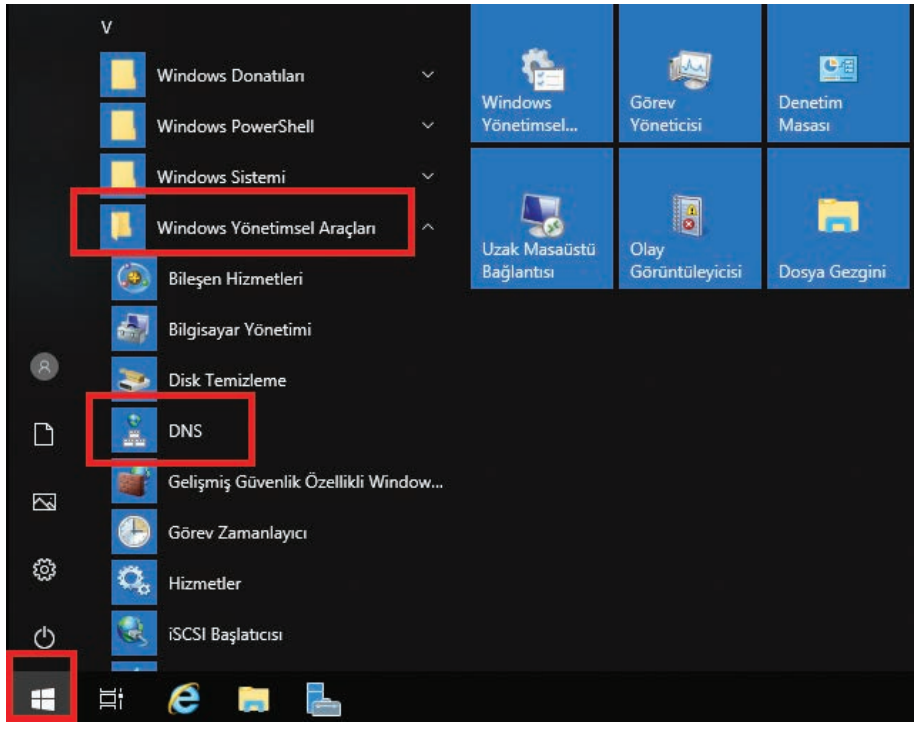


Görsel 4.12: Pano görüntüsü

2. UYGULAMA

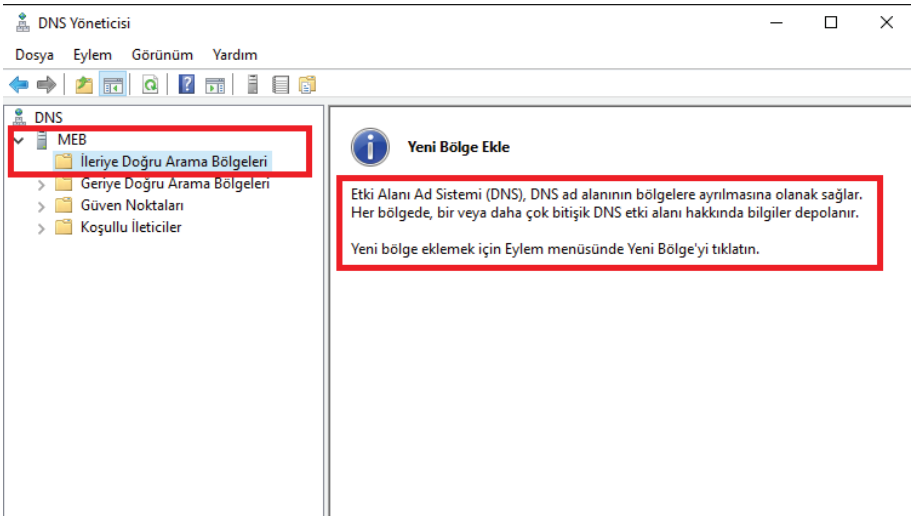
Aşağıdaki işlem adımlarına göre sunucu cihazınıza önceki uygulamada kurulmuş olan DNS Server üzerinde MESLEKLISESI.COM kaydını oluşturunuz.

1. Adım: Sunucu cihazınızda başlat menüsü, yönetimsel araçlar, dns yolunu kullanarak DNS Server panelini açınız (Görsel 4.13).



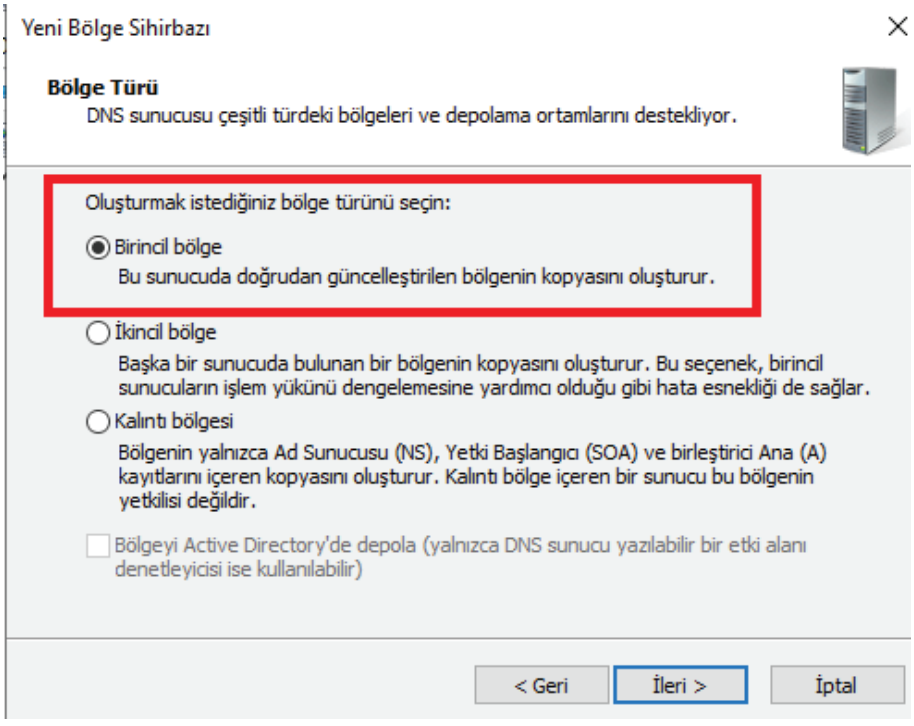
Görsel 4.13: DNS kaydı oluşturma

2. Adım: DNS yöneticisi panelinde ilk olarak MEB server isminin üzerine tıklayarak alt menüyü açınız. Menü açıldıktan sonra "İleriye Doğru Arama Bölgeleri" seçeneğinin üzerini tıklayınız. İleriye doğru arama bölgeleri seçeneğinin üzerine sağ tuşla tıklayınız, "Yeni Bölge" seçeneğini seçiniz ve diğer adıma geçiniz (Görsel 4.14).



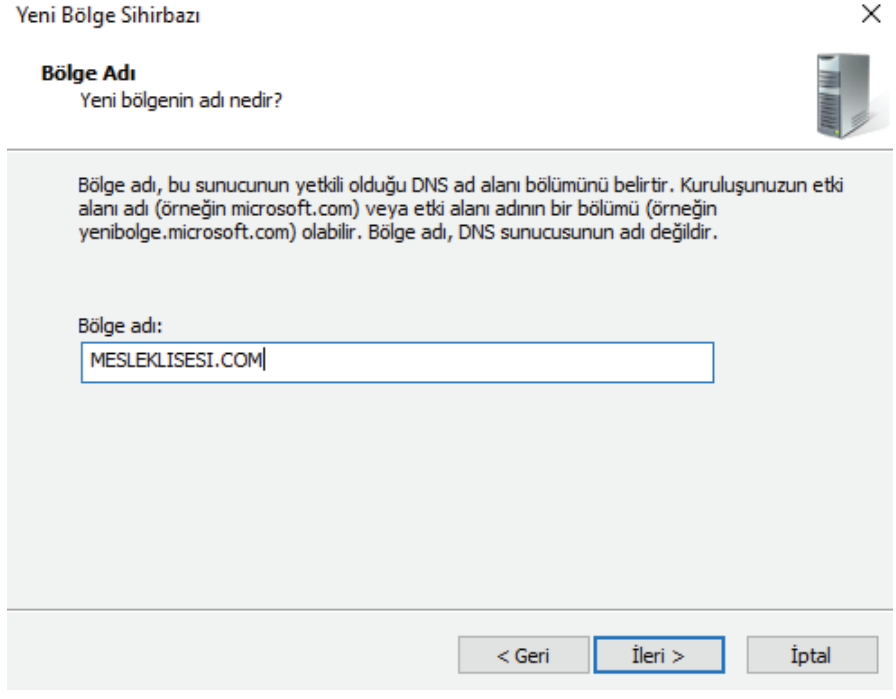
Görsel 4.14: İleriye doğru arama bölgesi ekleme

3. Adım: Yeni bölge kurulum adımlarında ilk seçenek ileri deyiniz ve diğer adıma geçiniz. Bu alanda oluşturmak istediğiniz bölge türünü seçiniz. Varsayılan olarak gelen "Birincil Bölge" seçeneği seçili halde kalarak ilerle tuşuna basınız ve diğer adıma geçiniz (Görsel 4.15).



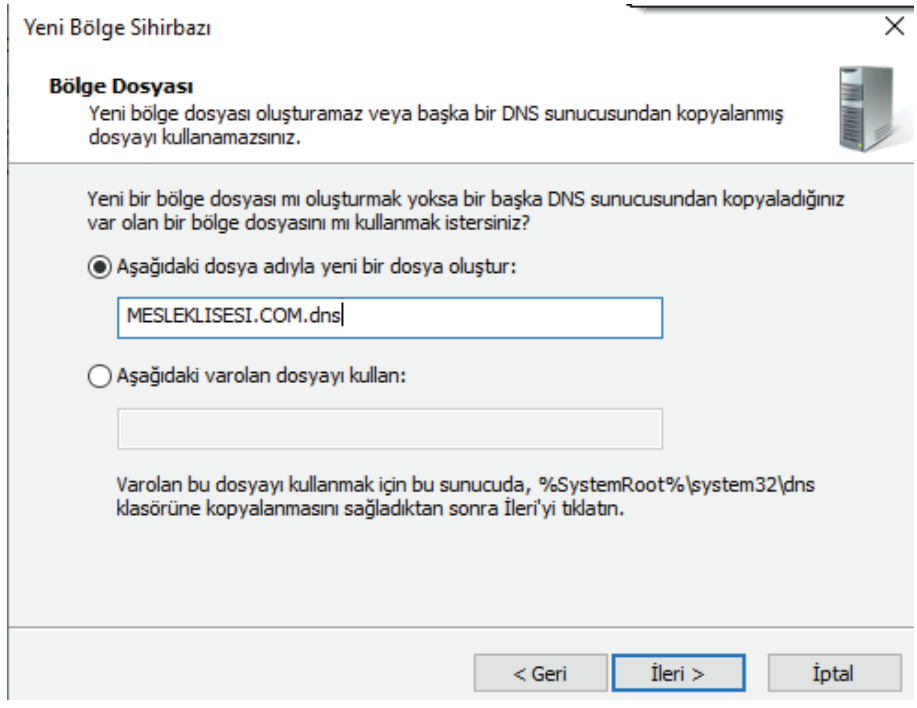
Görsel 4.15: Birincil bölge ekleme

4. Adım: Gelen ekranda oluşturmak istediğimiz **MESLEKLISESI.COM** kaydını Bölge adı alanına giriniz (Görsel 4.16).



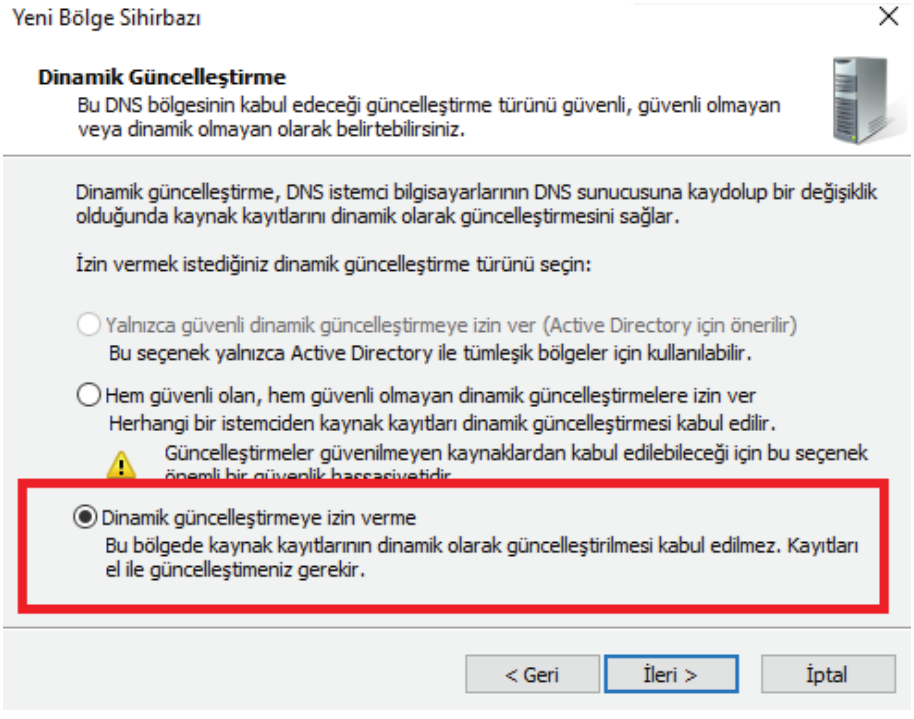
Görsel 4.16: Domain isim girişi

5. Adım: Gelen ekranda girdiğiniz ismi kontrol ederek hiçbir değişiklik yapmadan ileri butonu tıklayınız ve diğer adıma geçiniz (Görsel 4.17).



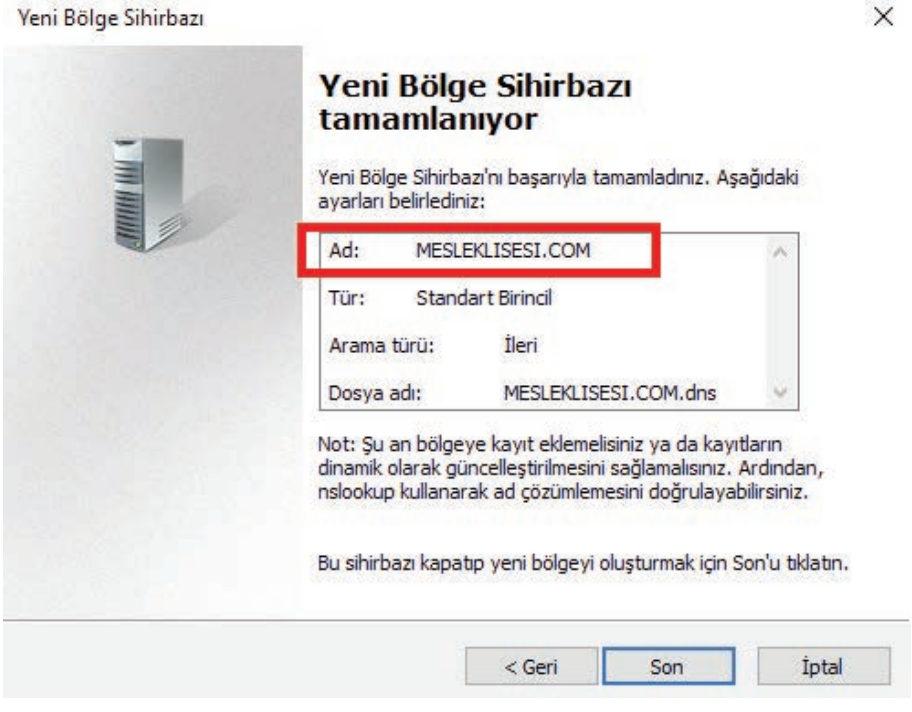
Görsel 4.17: Domain doğrulama

6. Adım: Dinamik güncellemeler izin verip vermek istemediğinize göre seçeneği işaretleyip diğer adıma geçiniz (Görsel 4.18).



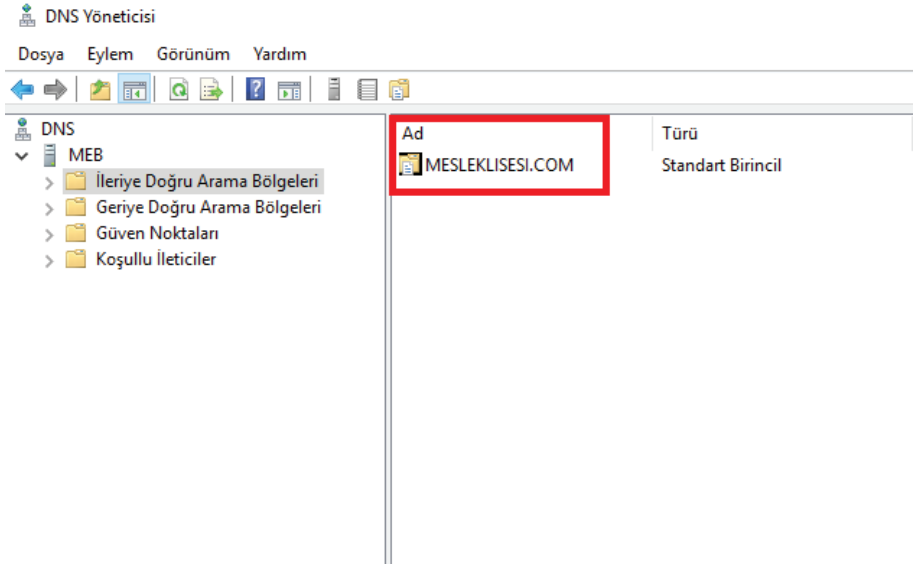
Görsel 4.18: Dinamik güncelleştirme

7. Adım: Gelen ekrandaki bilgileri kontrol ederek "son" seçeneği tıklayınız ve alanı oluşturunuz (Görsel 4.19).



Görsel 4.19: Yapılandırma özeti

8. Adım: DNS yöneticisi panelinden yapılan işlemleri kontrol ediniz ve doğrulayınız (Görsel 4.20).



Görsel 4.20: Yapılandırma doğrulama

3. UYGULAMA

Aşağıdaki işlem adımlarına göre sunucu Active Directory Etki Alanı kurulumunu gerçekleştiriniz. Sabit IP adresleri olarak önceki uygulamadaki adresleri kullanınız.

1. Adım: Sunucu cihazınızda yönetimsel yapılandırmaları yapabilmek için Administrator kullanıcısı ile açınız.

2. Adım: Sunucu cihazınıza ağ ve paylaşım merkezi menüsünü kullanarak TCP/IPV4 Özellikleri kısmından sabit IP yapılandırmasını giriniz.

3. Adım: Klavyeden "Windows butonu"na tıklayarak görev bölümü açınız. "**Sunucu Yöneticisi**" ikonlarından herhangi birine tıklayınız.

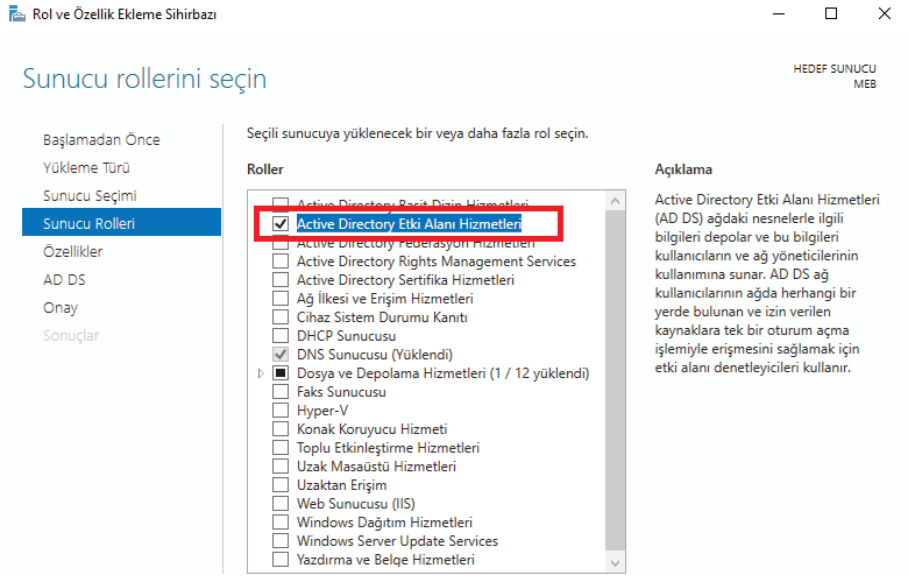
4. Adım: Sunucu Yöneticisi menüsünün sağ üst köşesindeki "**yönet**" kısmını kullanarak ya da hızlı menüde "**rol ve özellik ekle**" seçeneğini kullanarak **Active Directory Etki Alanı** kurulumunu başlatınız.

5. Adım: Gelen ilk ekran bilgilendirme ekranıdır, bu ekranda ilerle seçeneğini seçerek diğer adıma geçiniz. Gelen pencerede varsayılan olarak gelen "**rol tabanlı ve özellik tabanlı yükleme**" seçeneğini işaretli bırakarak diğer adıma geçiniz.

6. Adım: Gelen ekranda bizden hangi sunucuya rol kurmak istediğimiz soruluyor. Şu an tek bir sunucumuz olduğu için karşımıza tek seçenek gelmektedir. İsmi ve IP adresi verilen sunucumuzu seçerek diğer adıma geçilir.

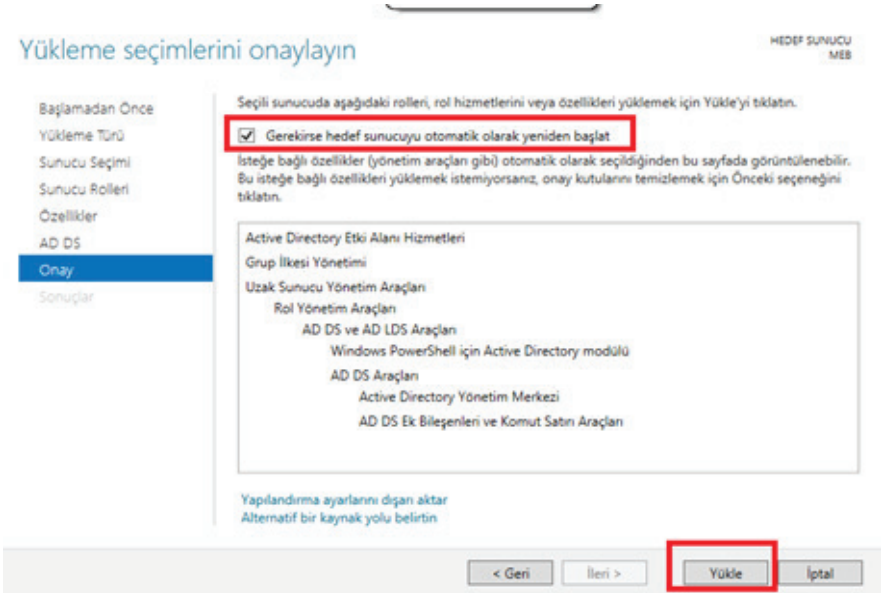
7. Adım: Gelen ekrandan seçeceğiniz rol olan "**Active Directory Etki Alanı Hizmetleri**" kutucuğunu işaretleyiniz. Karşınıza eklemek isteyebileceğiniz yardımcı roller için bir seçenek gelecektir. Yönetim

araçlarını ekle seçeneğinin işaretli olduğuna emin olduktan sonra ilerle diyerek diğer adıma geçiniz (Görsel 4.21).



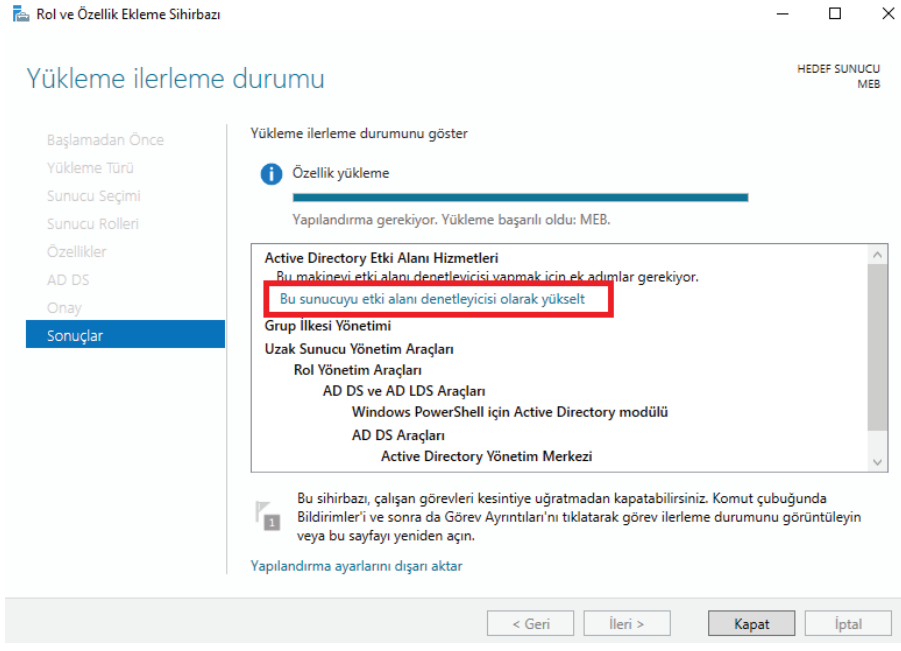
Görsel 4.21: Etki alanı yükleme işlemi

8. Adım: Karşınıza ilk olarak özellikler ekranı gelecektir ekrana herhangi bir özellik eklemeden ilerle seçeneğini seçiniz. Karşınıza bir bilgilendirme ekranı gelir. Bilgilendirme ekranını ilerle seçeneği ile geçiniz. Ardından yükleme seçimlerini onaylayacağınız ekran gelir. İlgili seçeneğini işaretleyiniz kurulumu **yükle** seçeneği ile başlatınız (Görsel 4.22).



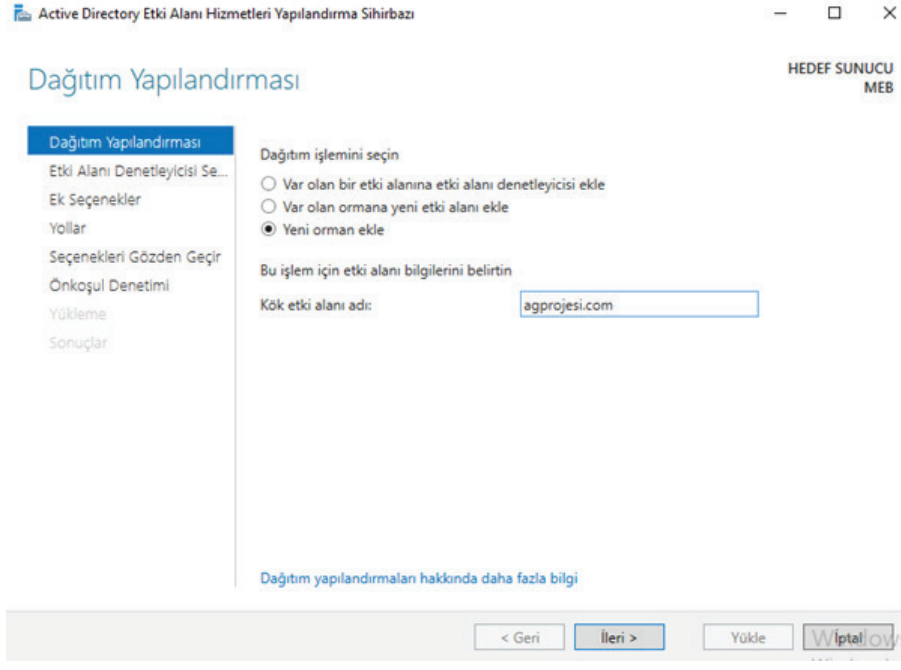
Görsel 4.22: Yapılandırma yükleme ekranı

9. Adım: Kurulum bittikten sonra bu ekranı kapatmadan "**Bu sunucuyu etki alanı denetleyicisi olarak yükselt**" seçeneğini seçiniz ve active directory yapılandırma işlemlerine geçiniz (Görsel 4.23).



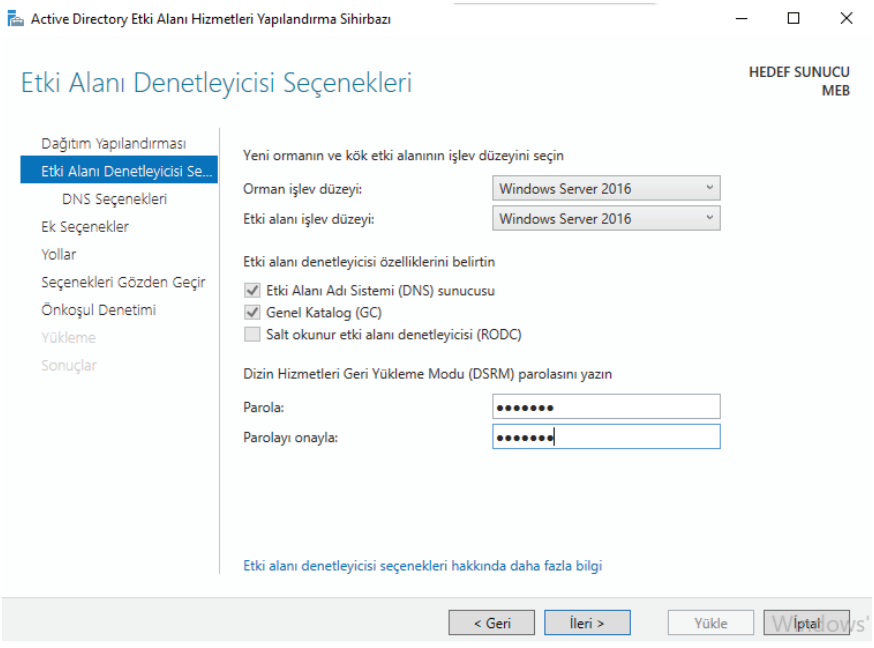
Görsel 4.23: Etki alanı denetleyicisi yükseltme

10. Adım: Yapılandırma ekranında yeni bir yapı oluşturacağı için "Yeni orman ekle" seçeneği işaretleyiniz. Etki alanı adı olarak ise "agprojesi.com" yazınız (Görsel 4.24).



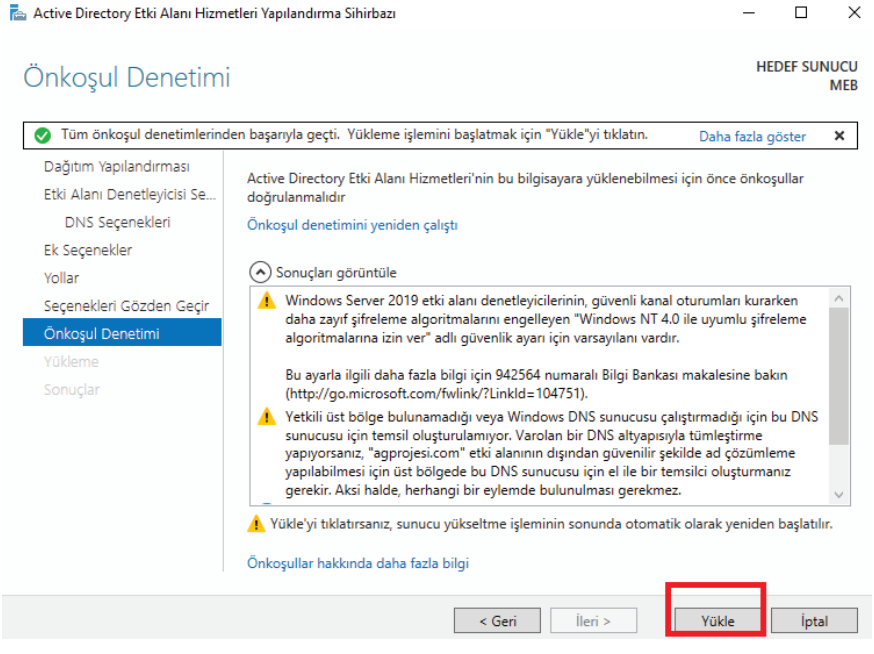
Görsel 4.24: Yeni orman ekleme ve etki alanı girişi işlemi

11. Adım: Karşınıza gelen ekranda Etki Alanı yapısında sorun çıkarsa kurtarma parolası girilmesi istenir. Bu ekranda kurtarma parolası giriniz ve ileri seçeneğini seçiniz (Görsel 4.25).



Görsel 4.25: Kurtarma parolası girişi

12. Adım: DNS parent zone uyarı ekranı ileri diyerek geçiniz. Sonraki ekranda Netbios ismi görüntülenir bu ekranda AGPROJESI ismini görüntüleyerek ileri seçeneğini seçiniz. Veri tabanı kurulum dosyalarının kaydedileceği ekran da ileri diyerek geçiniz. Özet ekranı karşınıza geldiğinde ileri seçeneği seçiniz. Eğer yapılandırmada bir hata varsa bu ekrandan sonra görüntülenme sağlanır. Ön gereksinim kontrolleri yapıldıktan sonra yükle seçeneği seçiniz ve yapılandırmayı yükleyiniz. İşlem bittikten sonra sunucuyu tekrar başlatınız (Görsel 4.26).

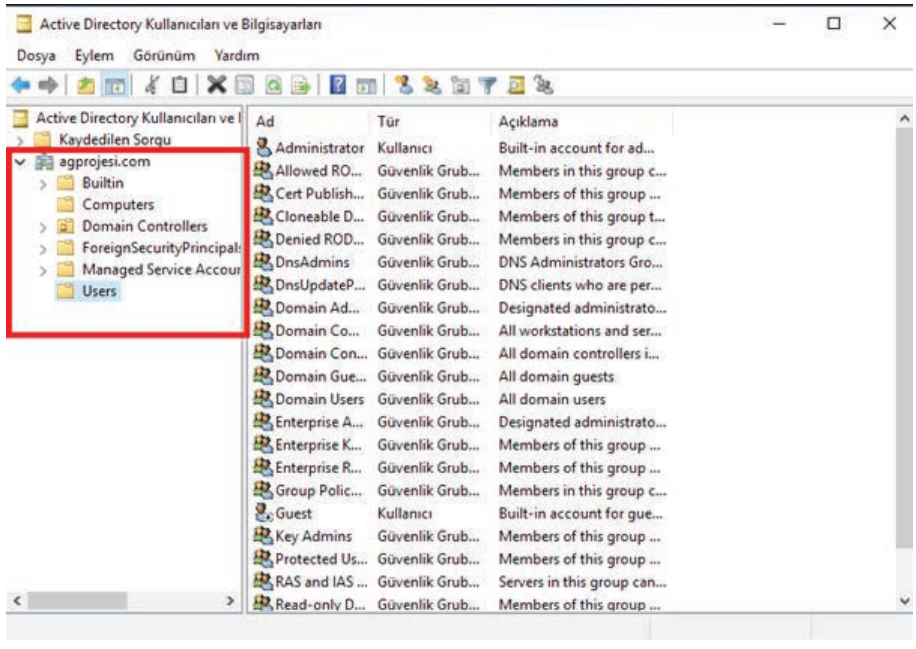


Görsel 4.26: Ön koşul denetim bilgileri

4. UYGULAMA

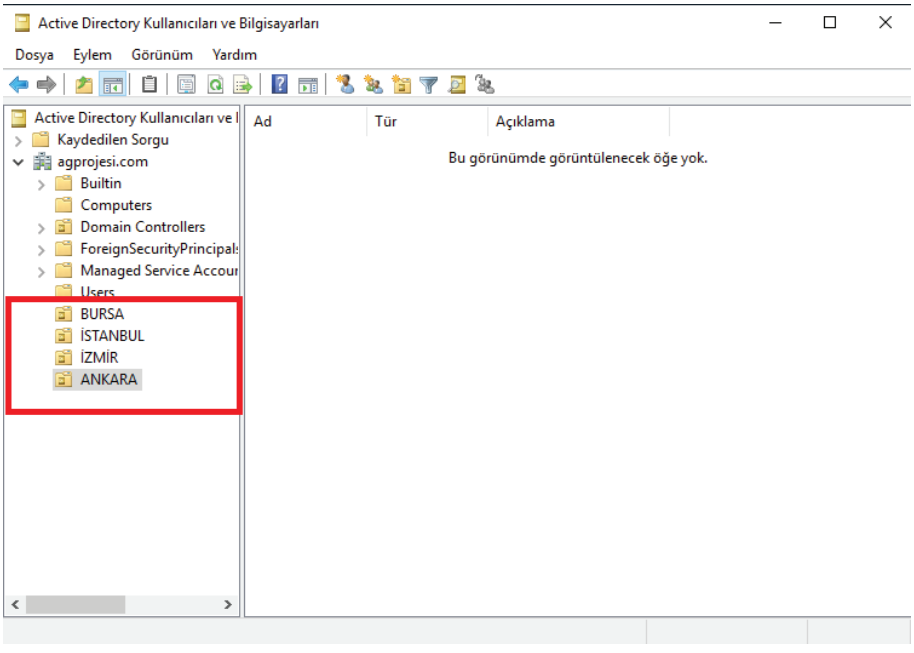
Aşağıdaki işlem adımlarına göre sunucu "Active Directory Kullanıcıları ve Bilgisayarları" panelinde BURSA, İZMİR, ANKARA, İSTANBUL isimlerinde "Yapısal Birimler" oluşturunuz. Oluşturduğunuz Bursa yapısal biriminin içerisine Fatih Sultan Mehmet isimli bir kullanıcı oluşturunuz. Kullanıcı şifresini değiştirmesine izin vermeyiniz ve parolanın süresiz kullanılmasını sağlayınız.

1. Adım: Sunucu cihazınızda Başlat, Windows Yönetimsel Araçlar, Etki Alanı Kullanıcıları ve Bilgisayarlar seçeneği ile yönetim panelini açınız (Görsel 4.27).



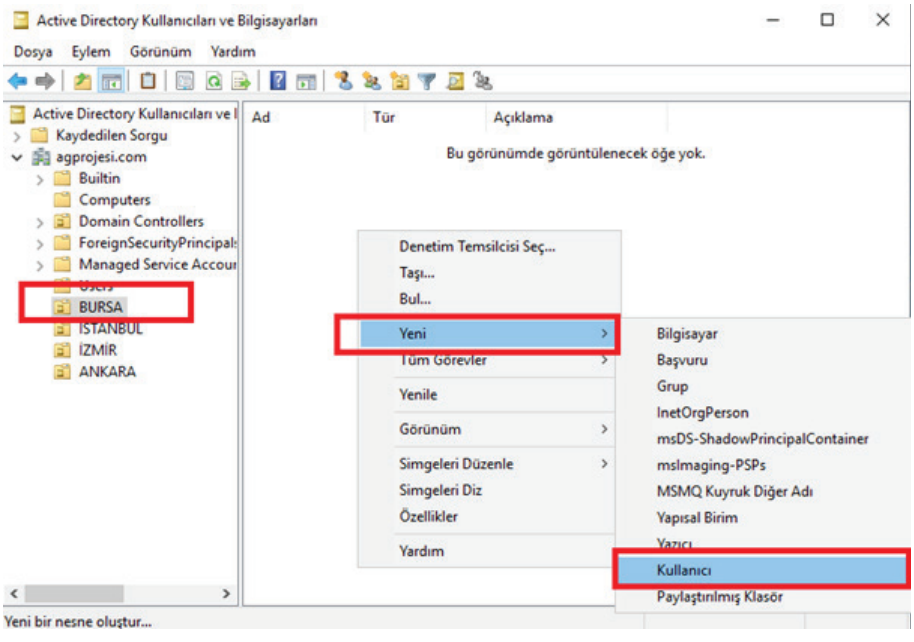
Görsel 4.27: Etki alanı kullanıcıları ve bilgisayarları paneli

2. Adım: Yönetim panelinde "agprojesi.com" domain ismi üzerinde sağ tık, yeni, yapısal birim yolunu kullanarak BURSA, İSTANBUL, ANKARA, İZMİR yapısal birimleri oluşturunuz (Görsel 4.28).



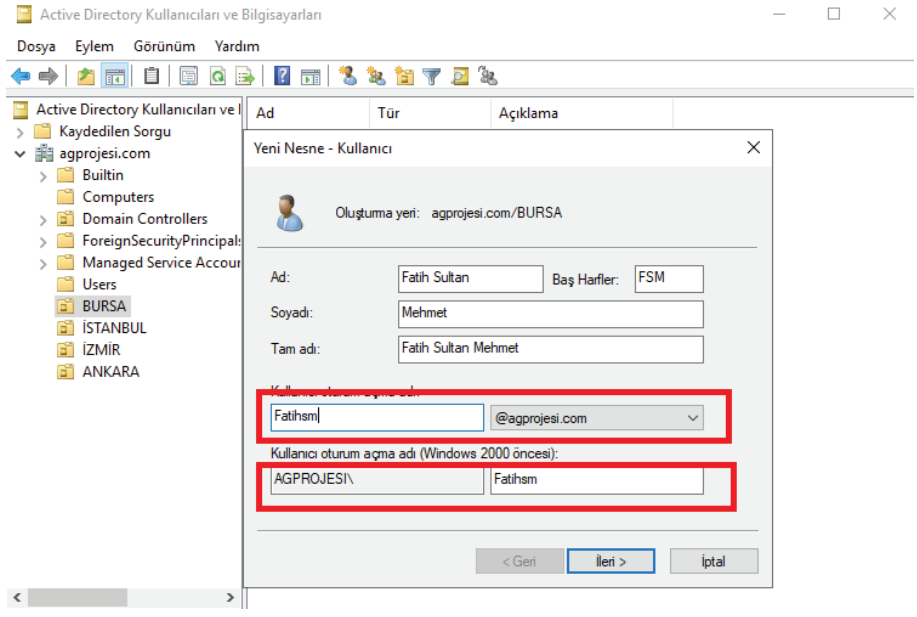
Görsel 4.28: Yapısal birim ekleme

3. Adım: Bursa yapısal birimi seçilerek içerisinde sağ tıklama, yeni, kullanıcı seçenekleri kullanılarak Fatih Sultan Mehmet isminde yeni kullanıcı oluşturunuz (Görsel 4.29).



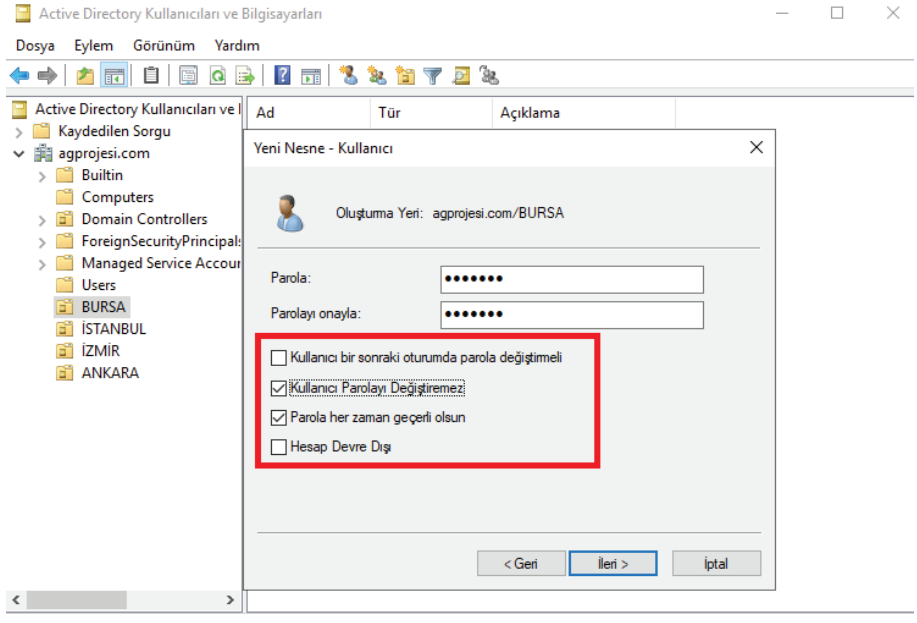
Görsel 4.29: Kullanıcı oluşturma

4. Adım: Kullanıcı bilgileri ve oturum açma bilgilerini giriniz. **Fatihsm@agprojesi.com** ya da **AGPROJESI\Fatihsm** oturum açma ismi ile yapılandırma hazırlanır (Görsel 4.30).



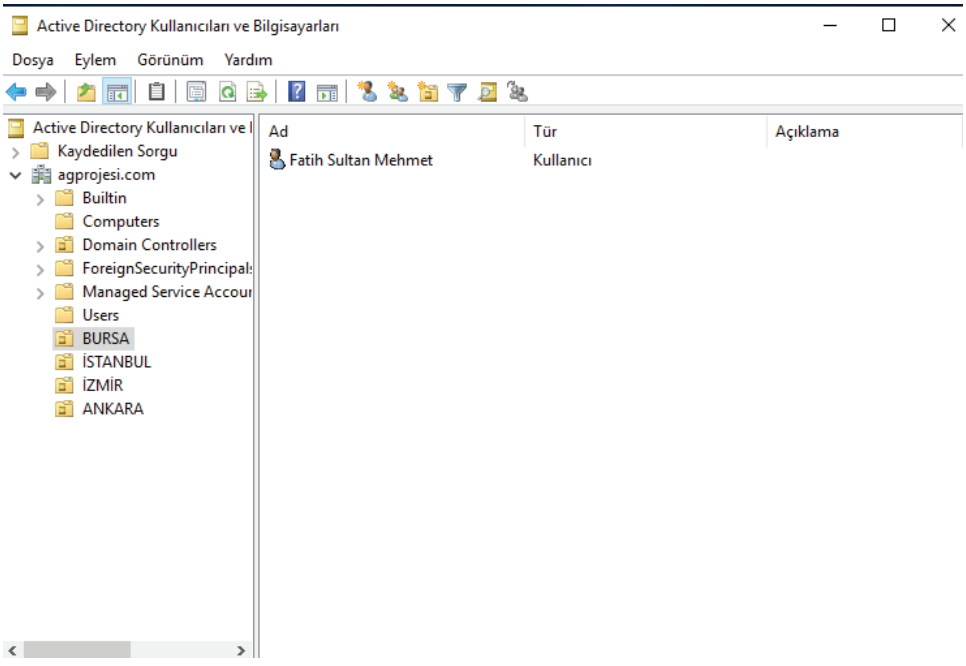
Görsel 4.30: Oturum açma bilgileri girişi

5. Adım: Oluşturulan kullanıcının şifre değiştirme ve şifre kullanım sürelerini ayarlayınız. Kullanıcı parolayı değiştiremez ve parola her zaman geçerli olsun seçeneklerini seçiniz (Görsel 4.31).



Görsel 4.31: Parola seçenekleri işlemi

6. Adım: Oluşturulan kullanıcıyı BURSA yapısal biriminin altında görüntüleyiniz (Görsel 4.32).

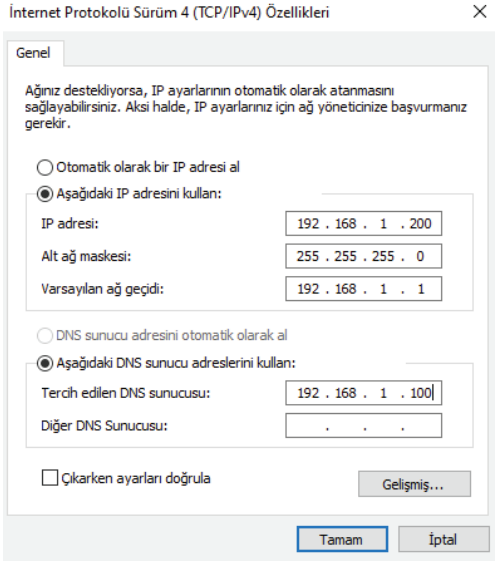


Görsel 4.32: Yapılandırma doğrulama

5. UYGULAMA

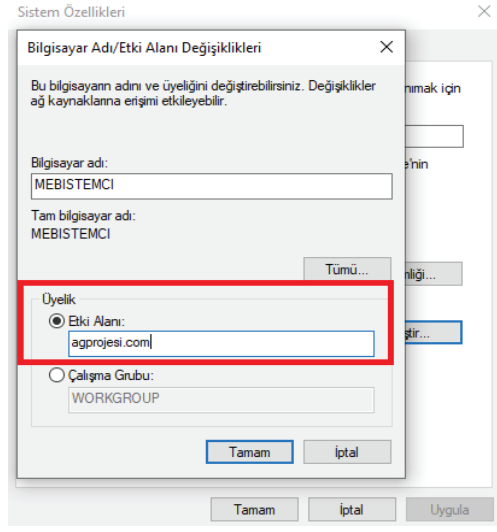
Aşağıdaki işlem adımlarına göre istemci bilgisayarı agprojesi.com etki alanına dâhil ediniz ve daha önce oluşturulan Fatihsm oturum açma ismi ile istemci cihazda oturum açınız.

1. Adım: İstemci cihazın IP yapılandırmasını hazırlayınız. 192.168.1.200 IP adresini, 255.255.255.0 varsayılan alt ağ maskesini, 192.168.1.1 varsayılan ağ geçidini ve 192.168.1.100 olarak daha önceden hazırlanmış DNS adresini giriniz IP yapılandırmasını tamamlayınız (Görsel 4.33).



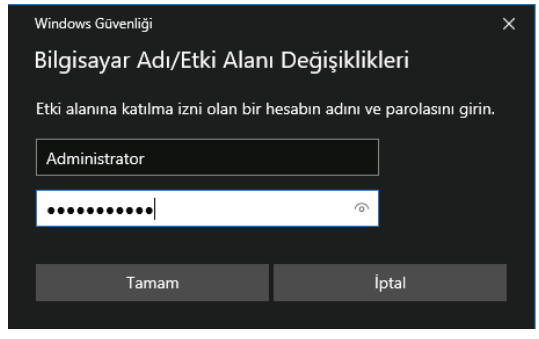
Görsel 4.33: IPV4 yapılandırması girişi

2. Adım: İstemci cihazda Bilgisayarım, sağ tıklama, özellikler ve ayarları değiştir seçeneğini kullanarak bilgisayarın agprojesi.com etki alanına girmesini sağlayınız (Görsel 4.34).



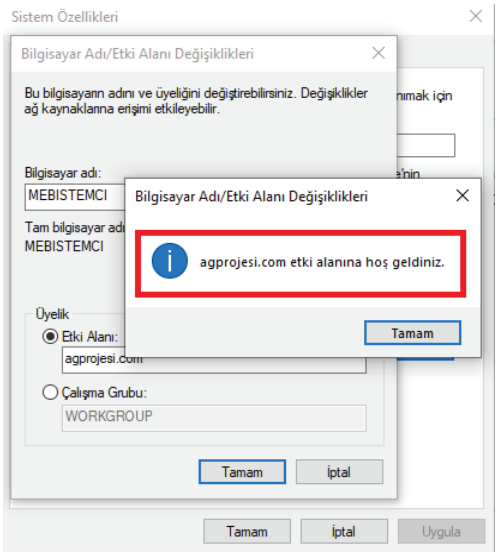
Görsel 4.34: Etki alanına dâhil etme

3. Adım: Etki alanına dâhil etmeden önce Administrator kullanıcı adını ve şifresinin girilmesi istenir. Şifreyi giriniz veTamam tuşuna basınız (Görsel 4.35).



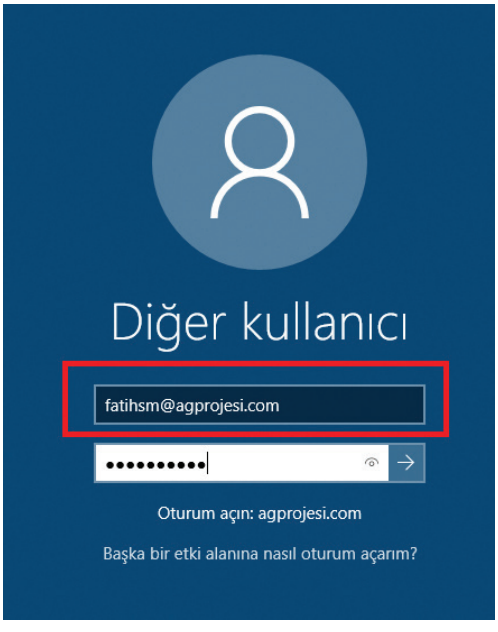
Görsel 4.35: Administrator onay ekranı

4. Adım: Sistem şifreyi doğruladıktan sonra etki alanına dahil olunduğunun mesajı alınır ve cihaz tekrar başlatılır (Görsel 4.36).



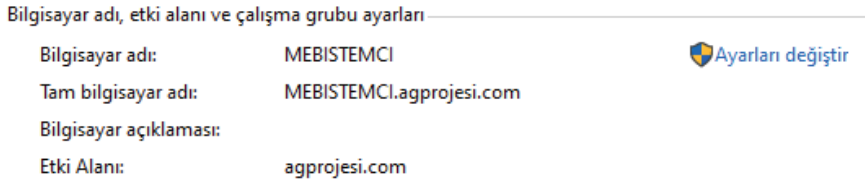
Görsel 4.36: Etki Alanına dâhil olma

5. Adım: Yeniden başlayan istemci cihazınıza etki alanında daha önce oluşturulan kullanıcı bilgileri ile giriş yapınız (Görsel 4.37).



Görsel 4.37: İstemci giriş ekranı

6. Adım: İstemci cihazınızdan bilgisayarım, özellikler ayarları değiştir kısmından etki alanına dâhil olunduğunun kontrolünü yapınız (Görsel 4.38).



Görsel 4.38: Yapılandırma doğrulama

SIRA SİZDE

Sunucu cihazında Active Directory kurulumunu gerçekleştiriniz. Etki alanı ismi olarak bilisimteknolojileri.com ismini kullanınız. Oluşturduğunuz yapıya NESNE, ROBOT, MOBIL, ANAHTARLAMA isimlerinde yapısal birimler oluşturunuz. Oluşturduğunuz yapısal birimlere birer kullanıcı ekleyiniz. Kullanıcıların cihazları ilk açtıklarında kendi şifrelerini belirlemesini ve kullanım sürelerinin sınırsız olacak şekilde yapılandırmasını sağlayınız.

SIRA SİZDE

Oluşturduğunuz kullanıcıların arka planlarını değiştirmelerini group policy kurallarını uygulayarak engelleyiniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki sorularda doğru seçeneği işaretleyiniz.

1. Aşağıdakilerden hangisi sunucu cihazların verdiği hizmetlerden biri <u>değildir</u>?

A) DHCP B) DNS C) TARAYICI
D) UZAK MASAÜSTÜ E) YAZICI

2. Aşağıdakilerden hangisi ile sunucu IP dağıtan bir birim hâline gelir?

A) DHCP B) DNS C) FTP
D) RDP E) SMTP

3. Aşağıdakilerden hangisi üzerinde Active Directory veri tabanının bir kopyasını (replica) bulunduran sunucudur?

A) Domain Controller B) Forest C) FTP
D) Global Katolog E) SMTP

4. Aşağıdakilerden hangisi gereken verinin nerede olduğundan bağımsız olarak Active Directory objeleri hakkında bilgiler sunar ?

A) Domain B) Domain Controller C) Forest
D) Sites E) Global Katalog

5. **I.** Yönetilebilirlik
II. Görsellik
III. Ölçeklenebilirlik
IV. Genişletilebilirlik
V. Güvenlik uyumu

Active directory kullanmak sunucuya yukarıda verilen özelliklerden hangilerini kazandırır?

A) I ve II. B) I, II ve III. C) I, II, III ve V.
D) I, III, IV ve V. E) II, III, IV ve V.

CEVAP ANAHTARLARI

1. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4
A	D	C	A

2. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
A	E	C	D	A

3. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
A	D	C	B	E

4. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

1	2	3	4	5
C	A	A	E	D

KAYNAKÇA

- Bilişim Teknolojileri Alanı Çerçeve Öğretim Programı, Ankara, 2020.
- Millî Eğitim Bakanlığı Mesleki ve Teknik Eğitim Genel Müdürlüğü "Ders Bilgi Formu" Bilişim Teknolojileri Alanı-Ağ Projesi 11-12.Sınıf, Ankara, 2020.
- Türk Dil Kurumu Türkçe Sözlük, Ankara, 2019.
- Türk Dil Kurumu Yazım Kılavuzu, Ankara, 2012.

Kaynakça atıf sistemi, TDK yazım kuralları ve kaynak gösterme biçimine göre düzenlenmiştir.

GÖRSEL KAYNAKÇA

http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=2420