****

**İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU**

**BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ**

**BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ (İ.Ö) PROGRAMI**

**İLERİ AĞ TEKNOLOJİLERİ**

**FİNAL PROJE ÖDEVİ**

**HAZIRLAYAN**

**FURKAN YURTSEVEN – 220175144**

**MUSTAFA YURTALAN – 220175094**

**ÖDEV DANIŞMANI**

**Öğr. Gör. Mehmet ATICI**

**İSTANBUL 2023**

**ÖDEV TANITIM FORMU**

YAZAR ADI SOYADI : FURKAN YURTSEVEN , MUSTAFA YURTALAN

ÖDEVİN DİLİ : TÜRKÇE

ÖDEVİN ADI : FİNAL PROJE ÖDEVİ

BÖLÜM : BİLGİSAYAR TEKNOLOJİLERİ

PROGRAM : BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ (İ.Ö)

ÖDEVİN TÜRÜ : FİNAL ÖDEVİN TES. TARİHİ : 28/12/2023

SAYFA SAYISI : 27

ÖDEV DANIŞMANI : Öğr. Gör. Mehmet Atıcı

**ÖZET**

Bu Cisco Packet Tracer projesi, öğrencilere enerji üretim endüstrisindeki gerçek dünya uygulamalarını anlama fırsatı sunan kapsamlı bir simülasyonu temsil etmektedir. Proje, bir hidroelektrik santralin kontrol ve izleme sistemini tasarlamak, simüle etmek ve optimize etmek üzerine odaklanmaktadır.

Sensörler ve Veri Toplama aşamasında, hidroelektrik santrallerin etkin çalışması için su seviyeleri, akış hızları, türbin hızları gibi önemli verilerin sürekli izlenmesi gerekmektedir. Bu aşamada, öğrenciler sensörlerin stratejik noktalara yerleştirilmesi ve hangi tür sensörlerin kullanılacağı konusunda kararlar alacaklardır.

Uzaktan İzleme ve Kontrol aşamasında, santralin etkin bir şekilde yönetilebilmesi için uzaktan izleme ve kontrol sistemleri tasarlanacaktır. Güvenli uzaktan erişim, otomasyon ve acil durum müdahale mekanizmaları bu aşamada önemli bir rol oynayacaktır.

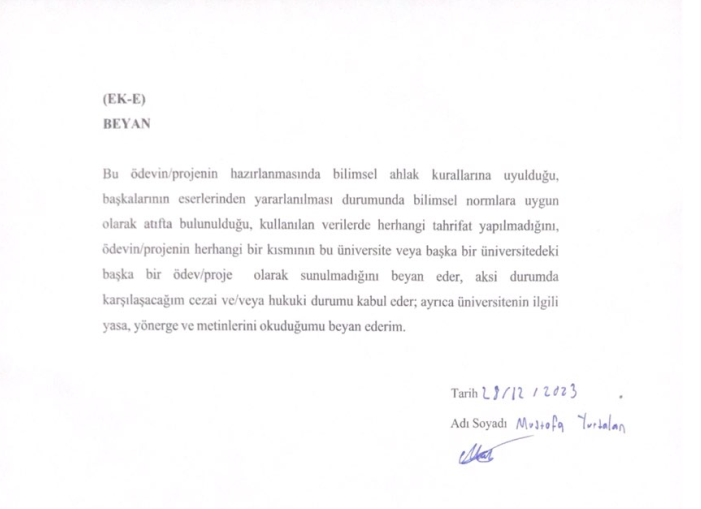
Veri Analizi ve Tahminleme aşamasında, toplanan verilerin analizi enerji üretiminin optimizasyonu için kritiktir. Öğrenciler, enerji üretim tahmin modelleri oluşturarak ve analiz yaparak enerji kaynaklarını daha etkili bir şekilde kullanmayı planlayacaklardır.

Güvenlik ve Veri Gizliliği aşamasında, proje santraldeki kritik verilerin güvenliğini sağlamak amacıyla ağ güvenliği protokollerini ve veri şifreleme yöntemlerini içerecektir.

Yedekleme ve Felaket Kurtarma aşamasında, sürekli enerji üretimi için yedekleme ve felaket kurtarma stratejileri ele alınacak, sistemlerin kesintisiz çalışma ve felaket durumlarında hızlı bir şekilde toparlanma yeteneği planlanacaktır.

Enerji Depolama Entegrasyonu aşamasında, yenilenebilir enerji kaynaklarının değişken doğası göz önüne alındığında, enerji depolama sistemlerinin entegrasyonu simüle edilecek ve enerji talebi ile arzı dengeleme yeteneği incelenecektir.

Sonuçlar ve Değerlendirme kısmında, bu proje öğrencilere enerji sektöründeki yenilikleri ve sürdürülebilirlik çözümlerini değerlendirme fırsatı sunarak, aynı zamanda ağ tasarımı, enerji üretimi ve kontrol sistemleri arasındaki karmaşıklıkları anlama konusunda geniş bir perspektif kazandırmayı amaçlamaktadır. Proje, öğrencilere endüstri uygulamaları üzerine kapsamlı bir anlayış geliştirmelerine olanak tanımaktadır.

**BEYAN**

İÇİNDEKİLER

ÖDEV TANITIM FORMU [i](#_Toc132112609)

[ÖZET ii](#_Toc132112609)

[İÇİNDEKİLER iii](#_Toc132112610)

[ÖN SÖZ iv](#_Toc132112610)

[GİRİŞ v](#_Toc132112610)

[Senaryo 1](#_Toc132112611)

[Santral 1 2](#_Toc132112611)

[Santral 2 2](#_Toc132112611)

[Santral 3 5](#_Toc132112611)

[Santral 4 7](#_Toc132112611)

[Santral 5 9](#_Toc132112611)

[Santral 6 11](#_Toc132112611)

[Santral 7 16](#_Toc132112611)

[OSPF Bağlantısı 18](#_Toc132112611)

[Kaynakça 21](#_Toc132112611)

**ÖN SÖZ**

Bu çalışmamda cisco packet tracer programı üzerinde 6 tane hidro elektirik santrali arasında iletişim sağlayan bir ağ oluşturduk.

Bu çalışmanın gerçekleştirilmesinde destek ve katkılarından dolayı Öğr. Mehmet Atıcı’ya teşekkürlerimi sunarım.

Çalışmam boyunca yanımda olan yakınlarıma bana verdikleri destekten dolayı teşekkür ederim.

Furkan Yurtseven

Mustafa Yurtalan

**GİRİŞ**

Günümüzde enerji sektörü, küresel çapta sürdürülebilir ve temiz enerji üretimi hedefine yönelik yenilikçi çözümler arayışında sürekli bir evrim geçiriyor. Bu kapsamda, hidroelektrik santraller, doğal kaynakları etkili bir şekilde kullanarak çevre dostu enerji sağlama potansiyeli nedeniyle öne çıkan bir role sahiptir. Bu projenin odak noktası, hidroelektrik santrallerin kontrol ve izleme sistemlerini simüle ederek, öğrencilere enerji üretimi ve kontrol sistemlerinin entegrasyonunun karmaşıklığını ve endüstri standartlarındaki pratik uygulamaları anlama imkanı sunmaktır.

Projenin ilk aşamasında, sensör teknolojileri kullanılarak su seviyeleri, akış hızları ve türbin hızları gibi kritik verilerin sürekli olarak izlenmesi hedeflenmektedir. Bu sayede, hidroelektrik santralinin performansı anlık olarak takip edilebilecek ve optimize edilebilecektir. Uzaktan izleme ve kontrol sistemleri tasarımında, güvenli uzaktan erişim, otomasyon ve acil durum müdahale yeteneklerini içeren bir ağ altyapısı geliştirilerek santralin etkin yönetimi amaçlanmaktadır.

Veri analizi ve tahminleme aşamasında, toplanan verilerin derinlemesine analizi ile enerji üretim tahmin modelleri oluşturularak, sistemin daha verimli çalışması sağlanacaktır. Bu süreç, enerji kaynaklarının etkin bir şekilde kullanılmasını ve enerji üretiminin optimizasyonunu hedeflemektedir. Güvenlik ve veri gizliliği önlemleri, santraldeki kritik verilerin güvenliğini sağlamak adına ağ güvenliği protokollerinin ve veri şifreleme yöntemlerinin entegrasyonunu içermektedir.

Yedekleme ve felaket kurtarma stratejilerinin ele alındığı bir sonraki aşama, sürekli enerji üretimi için kesintisiz operasyonları desteklemeyi amaçlamaktadır. Enerji depolama entegrasyonu, yenilenebilir enerji kaynaklarının değişken doğasını dengeleyerek enerji talebi ile arzı optimize etmeyi hedeflemektedir.

Bu kapsamlı projenin tamamlanması, öğrencilere sadece teorik bilgiler değil, aynı zamanda enerji sektöründeki güncel teknolojileri ve sürdürülebilirlik çözümlerini anlamada pratik bir deneyim sunacaktır. Projede ele alınan konular, öğrencilere enerji sektöründeki geleceğin taleplerine uygun olarak donanımlı bir şekilde hazırlanmalarında önemli bir adım olacaktır.

**Senaryo**

Günümüzde enerji sektörü, hızla değişen ve genişleyen bir alan olup, sürdürülebilir enerji üretimi ve yönetimi konularında giderek artan bir öneme sahiptir. Bu bağlamda, bu senaryo, öğrencilere bu karmaşık sektörde karşılaşılabilecek gerçek dünya sorunlarını çözme yeteneği kazandırmak amacıyla özel olarak tasarlanmış bir Hidroelektrik Santral Kontrol Sistemi projesine odaklanmaktadır.

Projede ilk adım, hidroelektrik santralinin temel bileşenlerini etkili bir şekilde izlemek amacıyla sensör teknolojilerinin stratejik yerleştirilmesidir. Su seviyeleri, akış hızları ve türbin hızları gibi önemli verilerin sürekli olarak toplanması, enerji üretim sürecini optimize etmek adına kritik bir rol oynamaktadır. Bu aşama, öğrencilere sensör teknolojilerinin pratik uygulamalarını keşfetme fırsatı sunarak teorik bilgilerini gerçek dünya senaryolarında nasıl kullanacaklarını anlamalarına yardımcı olacaktır.

İkinci aşamada, uzaktan izleme ve kontrol sistemleri tasarlanarak santralin operasyonlarının etkin bir şekilde yönetilmesi hedeflenmektedir. Güvenli uzaktan erişim, otomasyon ve acil durum müdahale yeteneklerinin entegrasyonu, öğrencilere karmaşık sistemlerin nasıl yönetileceği konusunda derinlemesine bir anlayış kazandıracaktır. Bu aşama, enerji sektöründeki pratik zorluklarla baş etme yeteneğini artırmak adına önemli bir deneyim sunacaktır.

Üçüncü aşama, toplanan verilerin analizi ve enerji üretim tahmin modellerinin oluşturulmasını içermektedir. Büyük veri analitiği, makine öğrenimi ve istatistiksel yöntemler kullanılarak elde edilen bilgiler, enerji üretiminin daha verimli ve etkili bir şekilde yönetilmesini sağlamak amacıyla kullanılacaktır. Bu süreç, öğrencilere analitik düşünme becerisi kazandırarak karmaşık veri setlerini çözme yeteneklerini geliştirecektir.

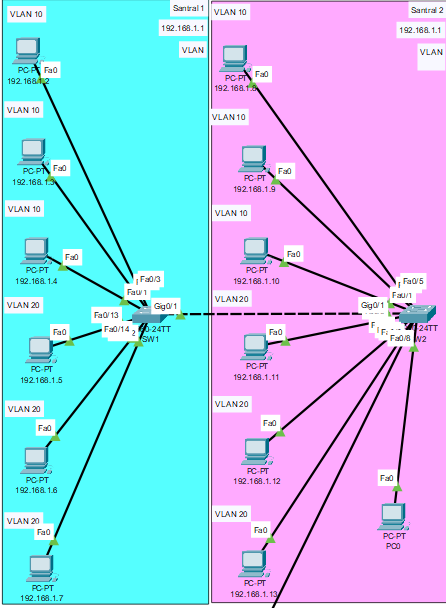
Dördüncü aşama, enerji sistemlerindeki güvenlik risklerini ele alarak, ağ güvenliği protokollerinin ve veri şifreleme yöntemlerinin entegrasyonunu içermektedir. Kritik verilerin güvenliği, enerji sektöründeki siber tehditlere karşı etkili bir koruma sağlamak için öğrencilere pratik bir anlayış kazandıracaktır.

Beşinci aşama, sürekli enerji üretimi için yedekleme ve felaket kurtarma stratejilerini içermektedir. Bu stratejiler, öğrencilere sistemlerin kesintisiz çalışma ve felaket durumlarında hızlı bir şekilde toparlanma yeteneği üzerine planlama yapma becerisi kazandıracaktır. Bu aşama, enerji sektöründeki sürekliliği sağlamak adına kritik bir öneme sahiptir.

Altıncı ve son aşama, enerji depolama sistemlerinin entegrasyonunu içermektedir. Yenilenebilir enerji kaynaklarının değişken doğasını dengelemek ve enerji talebi ile arzı optimize etmek amacıyla enerji depolama teknolojilerinin kullanılması, öğrencilere enerji üretimi ve depolama süreçlerini bütünsel bir şekilde yönetme yeteneği kazandıracaktır.

Bu kapsamlı proje, öğrencilere enerji sektöründeki karmaşık sorunları çözme yeteneği kazandırarak, geleceğin enerji ihtiyaçlarına yönelik yenilikçi çözümler üretmelerine katkıda bulunmayı hedeflemektedir. Projedeki her aşama, öğrencilerin sadece teorik bilgilerle değil, aynı zamanda gerçek dünya senaryolarıyla başa çıkma becerisi kazanmalarına odaklanarak, onları sektördeki liderlik pozisyonlarına hazırlamayı amaçlamaktadır.

**Santral 1 Ve Santral 2**



Santral 1 ve Santral 2 adlı iki hidroelektrik santralın entegre bir ağ altyapısına ihtiyaç duyulmuştur. Bu kapsamlı proje, her iki santralın verimli bir şekilde iletişim kurabilmesi, güvenli bir ağ yapısına sahip olabilmesi ve ölçeklenebilir bir Virtual Local Area Network (VLAN) altyapısı oluşturabilmesi amacıyla tasarlanmıştır.

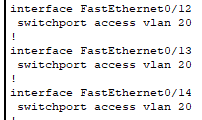
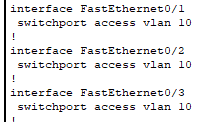
Projeye başlarken, her iki santralın coğrafi konumları, enerji üretim kapasiteleri ve iletişim ihtiyaçları detaylı bir şekilde incelenmiştir. Bu analiz, enerji üretim verileri, su seviyeleri, türbin hızları gibi kritik bilgilerin her iki santral arasında paylaşılabilmesi için bir VLAN ağı oluşturulmasının gerekliliğini ortaya koymuştur.

VLAN konfigürasyonu aşamasında, her iki santral için farklı departmanları ve işlevleri temsil eden ayrı VLAN'lar oluşturulmuştur. Bu sayede, enerji üretim birimi, bakım departmanı ve güvenlik birimi gibi farklı işlevlere sahip gruplar, kendi VLAN segmentleri içinde izole edilerek veri güvenliği artırılmıştır.

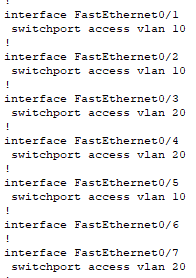
IP adreslemeler belirlenerek, her VLAN için özel bir IP adresleme planı oluşturulmuştur. Bu plan, her bir santralin kendi içindeki departmanlar arasında güvenli bir iletişimi sağlamak üzere tasarlanmıştır.

S**antral 1 Ve Santral 2’de Vlan Nasıl Kuruldu ?**

**Switch 1 Üzerindeki İşlemler**

****Bu kısımda Santral 1’deki bilgisayarları vlanlara atıyoruz.

**Switch 2 Üzerindeki İşlemler**

Bu kısımda Santral 2’deki bilgisayarları vlanlara atıyoruz. Bu işlemlerin hepsini tamamladıktan sonra iki switch arasındaki bağlantıyı oluşturmamız gerekiyor.

**Switch 1 Ve Switch 2 Üzerindeki İşlemler**



Yukarıda görmüş olduğumuz komutları switch 1 ve switch 2 üzerinde yazarak iki switch arasındaki bağlantıyı kuruyoruz. Böylelikle vlan ağımızı sorunsuz bir şekilde oluşturmuş bulunmaktayız. Şimdi bunların test aşamalarına geçebiliriz.

S**antral 1 Ve Santral 2’deki Test Aşamaları**

**VLAN 10 Ağı**

PC – 192.168.1.2

PC – 192.168.1.3

PC – 192.168.1.4

PC – 192.168.1.8

PC – 192.168.1.9

PC – 192.168.1.10

Yukarıdaki ip adresine sahip bilgisayarlar aralarında iletişim kurabilir.



**VLAN 20 Ağı**

PC – 192.168.1.5

PC – 192.168.1.6

PC – 192.168.1.7

PC – 192.168.1.11

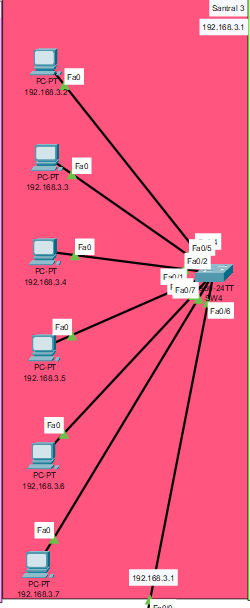
PC – 192.168.1.12

PC – 192.168.1.13

Yukarıdaki ip adresine sahip bilgisayarlar aralarında iletişim kurabilir.



**Santral 3**



Santral 3'ün bilgi işlem altyapısı, altı adet bilgisayarın bir yerel ağ switch'i aracılığıyla birbirine bağlanmasıyla oluşturulmuştur. Bu bilgisayarlar, enerji üretim süreçleri ve iş güvenliği yönetimi gibi belirli görevlere odaklanan bir yerel ağda etkileşimde bulunmaktadır. Aynı ağ switch'i, aynı zamanda bir router'a bağlanarak, OSPF (Open Shortest Path First) protokolü üzerinden router ile iletişim sağlar. Her bilgisayar, özel IP adresleriyle atanmıştır, bu da her bir bilgisayarın belirli bir bölümde izole bir şekilde çalışmasına olanak tanır ve ağ trafiğini optimize eder.

Router üzerindeki OSPF bağlantısı, dinamik yönlendirme protokollerinden biri olarak kullanılarak, bilgisayarlar arasında en kısa ve en güvenli yolu otomatik olarak belirler. Bu protokol, ağ topolojisi değiştikçe güncellenir ve en uygun rota seçimini sağlar. Ayrıca, enerji üretim süreçlerini izlemek ve kontrol etmek amacıyla her bilgisayarda özel uygulamalar bulunmaktadır. Bu uygulamalar, enerji üretim verilerini toplamak, analiz etmek ve operasyonel süreçlere müdahale etmek için kullanılmaktadır.

**Santral 3’deki Test Aşamaları**

**İletişimler**

PC – 192.168.3.2

PC – 192.168.3.3

PC – 192.168.3.4

PC – 192.168.3.5

PC – 192.168.3.6

PC – 192.168.3.7

Yukarıdaki ip adresine sahip bilgisayarların hepsi sadece aralarında iletişim kurabilmektedir.



**OSPF Test Kısmı**

**Santral 3**

PC – 192.168.3.2

PC – 192.168.3.3

PC – 192.168.3.4

PC – 192.168.3.5

PC – 192.168.3.6

PC – 192.168.3.7

**Santral 6**

PC – 192.168.6.2

PC – 192.168.6.3

Yukarıdaki ip adresine sahip bilgisayarların hepsi ospf bağlantısı aracılığıyla aralarında iletişim kurabilmektedir.

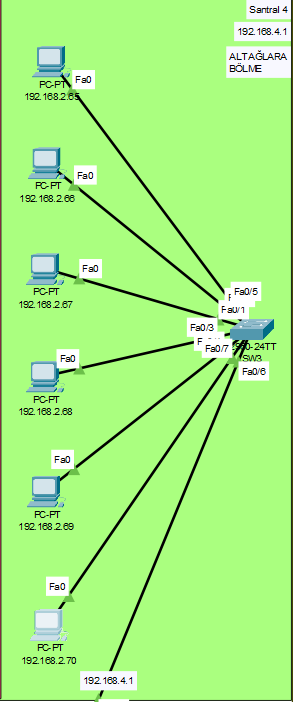
Not: Ospf bağlantısı nedeniyle bu aşamada ilk göndermeye çalıştığımız pdu failed sonucu döndürebiliyor fakat aynı bilgisayarlara tekrardan pdu işlemini uygularsak sonucun succesful döndüğünü göreceksiniz.

**İlk Deneme Aşamasındaki Failed Görüntüsü**



**İkinci Deneme Aşamasındaki Succesful Görüntüsü**



**Santral 4**

Santral 4, enerji üretim süreçlerini daha etkili bir şekilde yönetmek ve bilgi işlem altyapısını güçlendirmek amacıyla alt ağlara bölünmüş bir yapıya sahiptir. Bu alt ağ yapısı, her biri belirli görevlere odaklanan altı adet bilgisayarı kapsamaktadır. Planlama aşamasında, her bir alt ağın enerji üretim süreçlerindeki farklı işlevleri daha etkili bir şekilde yerine getirebilmesi için özel olarak tasarlandığı bir alt ağ planlaması yapılmıştır.

Alt ağlar, kendilerine özgü alt ağ ID'si ve IP adresleme planına sahiptir, bu sayede izolasyon sağlanarak her bir alt ağın bağımsız olarak çalışmasına ve kendi operasyonel süreçlerine odaklanmasına imkân tanınmıştır. Alt ağlar arasındaki iletişim, özel bir router üzerinden yönlendirilerek kontrol altında tutulmaktadır, bu da ağ içindeki güvenliği artırmakta ve her bir alt ağın kendi işlevselliğini sürdürebilmesine katkı sağlamaktadır.

**Alt Ağlara Bölme Nasıl Yapıldı ?**

192.168.2.64/26 bir CIDR (Classless Inter-Domain Routing) gösterimidir. Bu gösterimdeki "/26" ifadesi, IP adresinin ilk 26 bitinin ağ kısmını (alt ağı) belirtir. Bu durumda, son 6 bit host kısmını temsil eder. Aşağıda bu IP adresini alt ağlara bölmek için adım adım bir açıklama bulunmaktadır:

**Alt Ağ Maskesini Belirleme :** "/26" ifadesi, ilk 26 bitin ağ kısmını belirtir. Geriye kalan 32 - 26 = 6 bit ise host kısmını temsil eder. Alt ağ maskesi, 32 bitlik bir IP adresindeki ağ ve host kısımlarını belirler. Bu durumda alt ağ maskesi şu şekildedir: 11111111.11111111.11111111.11000000, yani ondalık olarak 255.255.255.192.

**Alt Ağ Sayısını Belirleme :** "/26" ifadesindeki "26", ağ kısmının kaç bit olduğunu belirtir. 32 bit toplam bir IP adresidir, bu nedenle host kısmı için kullanılabilir bit sayısı 32 - 26 = 6 bit'tir. Bu durumda, 2^6 = 64 adet IP adresi kullanılabilir.

**Alt Ağları Belirleme**

Alt ağları belirlemek için, ağ kısmının başlangıç IP adresinden başlayarak 2^6 (62) adet IP adresini gruplamamız gerekiyor.

Alt Ağ 1: 192.168.2.64 (Başlangıç IP adresi)

Alt Ağ 2: 192.168.2.128

Alt Ağ 3: 192.168.2.192

Her bir alt ağın başlangıç IP adresi, o alt ağın ağ adresidir. Bir sonraki alt ağın başlangıç IP adresi, bir önceki alt ağın son IP adresine bir eklenir. Örneğin, ikinci alt ağın başlangıç IP adresi, birinci alt ağın son IP adresine 1 eklenerek bulunur.

**Her Alt Ağın Sınırlarını Belirleme**

Alt Ağ 1: 192.168.2.64 - 192.168.2.127

Alt Ağ 2: 192.168.2.128 - 192.168.2.191

Alt Ağ 3: 192.168.2.192 - 192.168.2.255

Her bir alt ağın sınırlarını belirleyerek, hangi IP adreslerinin o alt ağa ait olduğunu ve hangi IP adreslerinin host olarak kullanılabileceğini belirlemiş olursunuz.

**Santral 4’deki Test Aşamaları**

**İletişim**

PC – 192.168.2.65

PC – 192.168.2.66

PC – 192.168.2.67

PC – 192.168.2.68

PC – 192.168.2.69

PC – 192.168.2.70

Yukarıdaki ip adresine sahip bilgisayarlar sadece aralarında iletişim kurabilir.

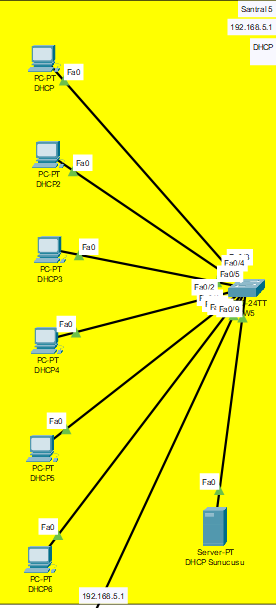


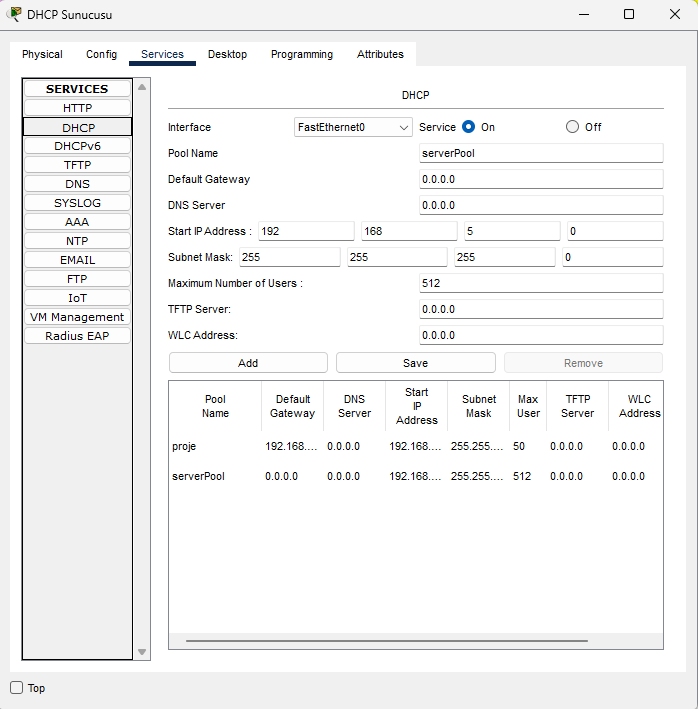
**Santral 5**

Santral 5, ağ yönetimini daha esnek ve otomatik hale getirmek amacıyla DHCP (Dynamic Host Configuration Protocol) kullanarak IP adresleme süreçlerini optimize etmektedir. Bu senaryo, Santral 5'in DHCP bağlantısı ve IP adresleme stratejisinin nasıl yapılandırıldığını ve ağ yönetiminin nasıl daha etkili bir hale getirildiğini detaylı bir şekilde açıklamaktadır.

DHCP kullanımı, ağdaki cihazlara otomatik olarak ve dinamik bir şekilde IP adresi tahsis etme esnekliği sağlar. Bu, yeni cihazların ağa bağlanması veya ağdan ayrılması durumlarında daha hızlı ve etkili bir yönetim olanağı sunar. Ayrıca, DHCP sunucusu, IP adresleme hatalarını otomatik olarak düzeltebilir ve ağdaki tüm IP adreslerini sürekli olarak izleyerek çatışmaları önleyebilir.

Santral 5'in DHCP altyapısı, ağa yeni cihazlar eklendiğinde veya mevcut cihazlar ağdan çıkarıldığında genişletilebilir bir yapıya sahiptir. Bu, ağın büyüklüğü ve karmaşıklığı arttıkça daha verimli bir IP adres yönetimi sağlamaktadır.





**DHCP Kurulumu Nasıl Yapıldı ?**

Sol tarafta görünen kısım bizim dhcp kurulumunda kullandığımız sunucumuzun ayar kısmıdır. İlk aşamada oluşturmak istediğimiz dhcp kurulumuna bir isim belirlememiz gerekmektedir. Sonraki aşama olarak aşağıdaki kısımdan bilgisayalarla verilmesi gereken ip adreslerinin başlangıcını ve subnet maskların ne olacağını gösteren ayarlamalar yapmaktayız. Ardından yukarıda bulunan service kısmıdaki butonu on haline getirmeyi unutmamız gerekmektedir. Bu ayarlamaları yaptıksan son add butonuna tıklayarak dhcp kurulumunu gerçekleştirmiş bulunmaktayız. Buradan çıkıp bilgisayarlara verilmiş olan ip adreslerini ve subnet masklarını kontrol ederek test işlemlerimize başlayabiliriz.

**Santral 5’deki Test Aşamaları**

**İletişim**

PC – DHCP

PC – DHCP2

PC – DHCP3

PC – DHCP4

PC – DHCP5

PC – DHCP6

Yukarıdaki ip adresine sahip bilgisayarlar sadece aralarında iletişim kurabilir.

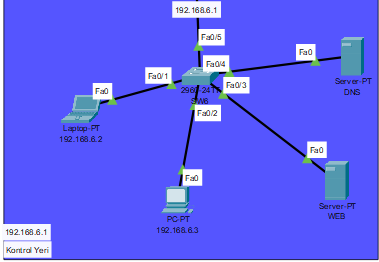


**Santral 6 (Kontrol Merkezi)**

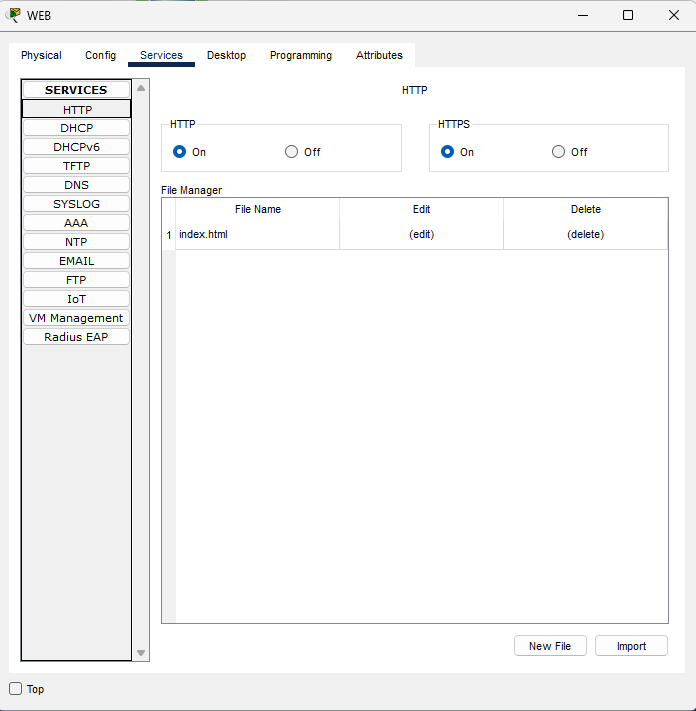
Santral 6, enerji üretim süreçlerini destekleyen bir bilgi işlem altyapısına sahip olup, bu altyapı içerisinde Web ve DNS hizmetlerini entegre bir şekilde kullanmaktadır. Bu entegrasyon, santralin operasyonlarını daha etkili ve kullanıcı dostu hale getirerek, enerji üretim verilerine erişimi ve yönetimi optimize etmeyi amaçlamaktadır.

Santral 6'nın web hizmetleri, enerji üretim verilerini anlık olarak izleme, analiz etme ve raporlama imkânı sunmaktadır. Kullanıcılar, bu hizmetler aracılığıyla enerji tüketimi istatistikleri, bakım durumları, ve acil durum senaryoları gibi kritik bilgilere kolayca erişebilirler. Bu sayede, enerji sektöründeki paydaşlar, süreçleri daha iyi anlayabilir ve operasyonları daha etkili bir şekilde yönetebilirler.

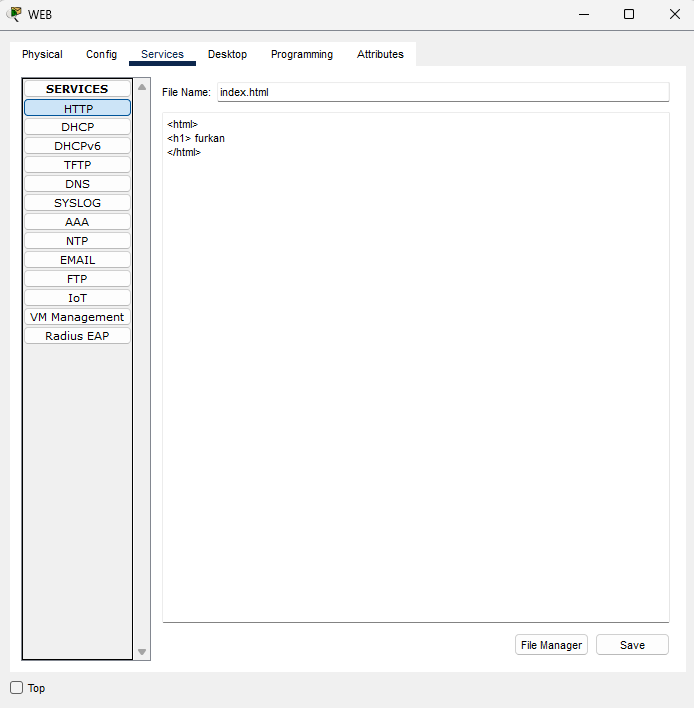
DNS entegrasyonu ise, ağ içindeki cihazların ve dış paydaşların daha kolay ve anlamlı erişimini sağlamaktadır. Santral içindeki cihazlara verilen isimler, DNS aracılığıyla IP adresleriyle eşleştirilir ve bu, kullanıcıların cihazlara isim bazlı erişimini mümkün kılar. Ayrıca, dış paydaşlar için sunulan web hizmetlerine erişim, DNS aracılığıyla kolaylaştırılır ve güvenli bir şekilde yönlendirilir.



**Web Sunucusu Nasıl Kuruldu ?**

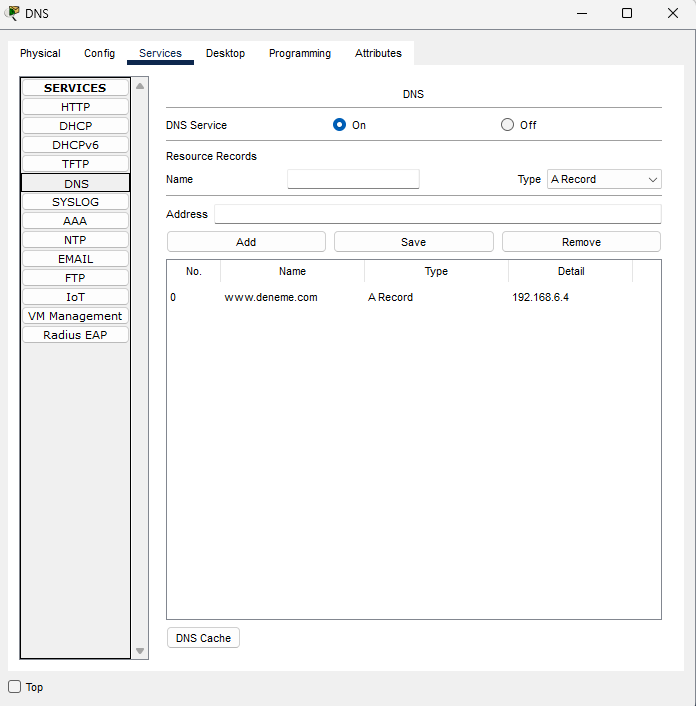


Yukarıdaki web sunucumuzun services kısmına giriş sağlıyoruz. Açılan sol taraftaki menümüzden HTTP kısmına giriş sağlıyoruz açılacak sayfamızın içeriğini değiştirmek için index.html dosyasının içerisine giriş yapıp girdiğimiz sayfada ne gözükmesini istiyorsak onu orayı o şekilde değiştiriyoruz.



Yukarıdaki kısımdan sayfamız açılınca Furkan yazısının çıkacağı kısmı ayarlamış olduk.

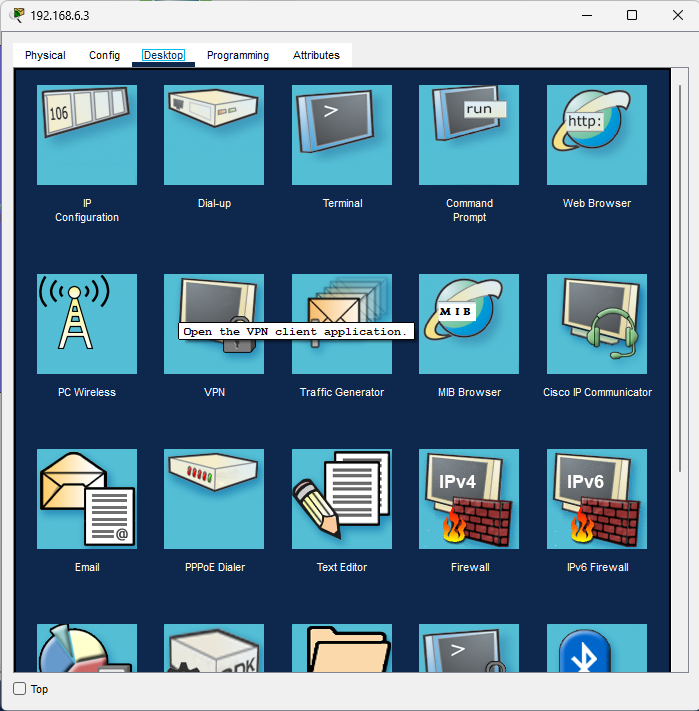
**DNS Sunucusu Nasıl Kuruldu ?**



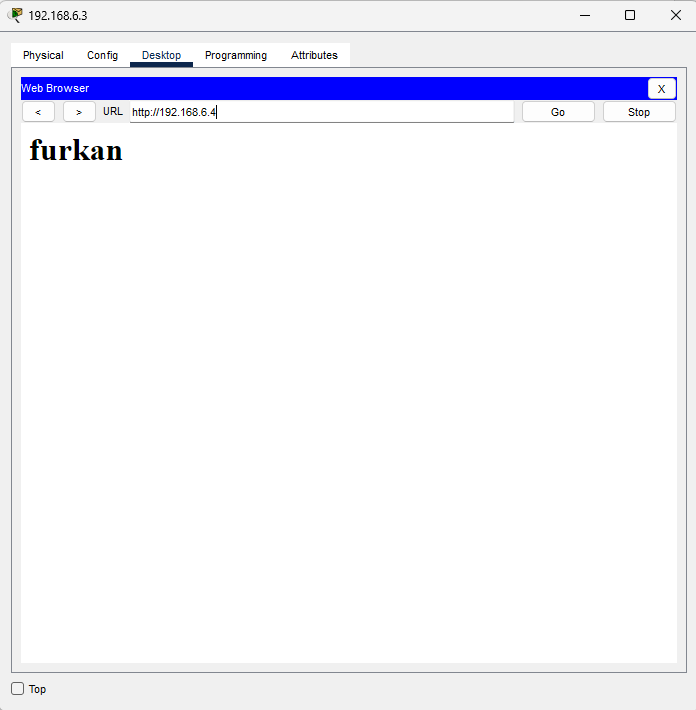
Yukarıdaki web sunucumuzun services kısmına giriş sağlıyoruz. Açılan sol taraftaki menümüzden DNS kısmına giriş sağlıyoruz giriş yapmamız gereken web sayfasının ayarlarını yapmak için aşağı tarafta bulunan name kısmına sayfamızı hangi ismiyle aratmamızı istiyorsak onu giriyoruz. Address kısmınada dns sunucumuzun ip adresini girip save butonuna tıklıyoruz. Bu şekilde DNS ve Web sunucularının bağlantılarını gerçekleştirdik. Şimdi test aşamalarına geçebiliriz.

**DNS Test Aşaması**

Santral 6’daki bir pc üzerine tıklıyoruz.



Bu kısımdan Web Browser kısmını Açıyoruz. Açılan kısımdan daha önceden ayarladığımız ayarların testini gerçekleştireceğiz.

****

Yukarıdaki arama kısmına DNS sunucumuzun ip adresini yazarak aratma yapıyoruz. Bu şekilde http kısmında ayarlamış olduğumuz sayfa içeriği ile karşılaşabiliriz.

Biz bu kısımda arama kısmına dns sunucumuzun ip adresi olan 192.168.6.4 yazarak aratma yaptığımızda bu ekran ile karşılaşıyoruz.

**Santral 6’deki Test Aşamaları**

**İletişim**

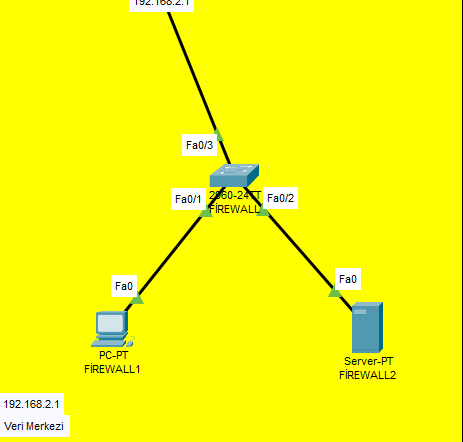
Server - DNS

Server - WEB

PC – 192.168.6.2

PC – 192.168.6.3

Yukarıdaki ip adresine sahip bilgisayarlar sadece aralarında iletişim kurabilir.

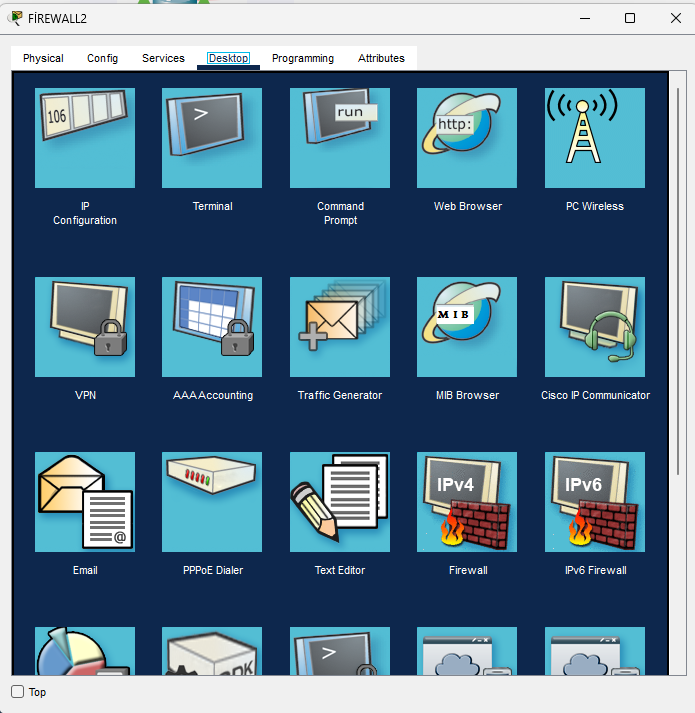
**Santral 7 (Veri Merkezi)**

Santral 7, enerji üretim süreçlerini güvence altına almak ve ağ güvenliğini en üst düzeye çıkarmak amacıyla benimsediği güçlü firewall altyapısıyla öne çıkmaktadır. Bu kapsamlı güvenlik stratejisi, çeşitli katmanlardaki güvenlik önlemlerini entegre ederek, potansiyel tehditlere karşı etkili bir koruma sağlamayı hedeflemektedir.

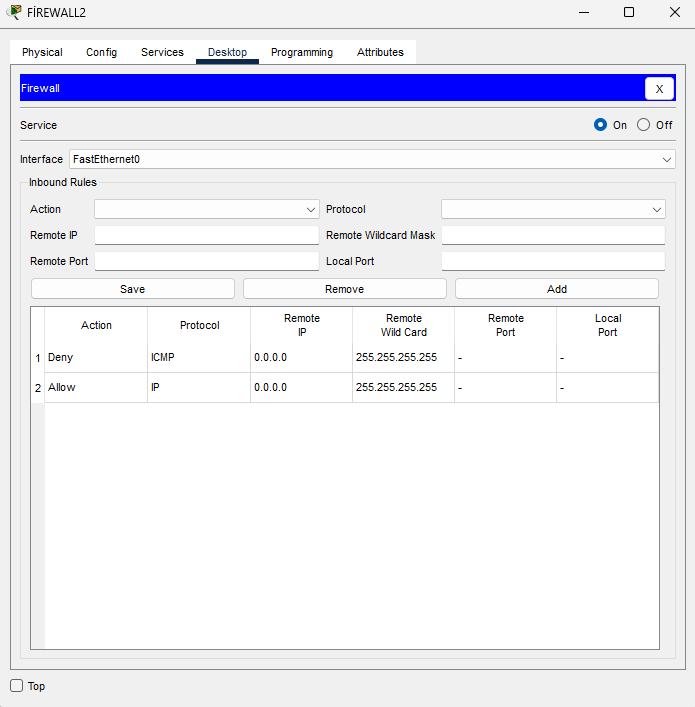
Santral 7'nin firewall altyapısı, ağ trafiğini sürekli olarak izleyerek güvenli olmayan bağlantıları otomatik olarak engelleyen dinamik bir yaklaşımı benimsemektedir. Ayrıca, erişim kontrol politikaları sıkı bir şekilde tanımlanmıştır, bu da belirli kullanıcıların ve cihazların ağa erişimini kontrol altında tutarak yetkilendirilmemiş erişimleri önlüyor.

Güvenlik duvarları ve protokoller aracılığıyla ağ trafiğini izleyen Santral 7, potansiyel zararlı yazılımlar, saldırı girişimleri ve güvenlik açıkları konusunda anında müdahale sağlamaktadır. Ayrıca, veri güvenliğini en üst düzeye çıkarmak adına iletişimi şifreleme protokolleriyle güvence altına alır.

**Firewall Sunucusu Nasıl Kuruldu ?**



Yukarıdaki kısımdan Firewall menüsüne seçip giriyoruz.



Bu açılan kısımdan Action , Protocol , Remote Ip , Remote Wild Card aşamaları aşağıdaki doldurduğumuz gibi hem Deny Action kısmı için hemde Allow Action kısmı için uygulayıp kaydediyorum. Bu sayede basit firewall yapımızı kurmuş oluyoruz.

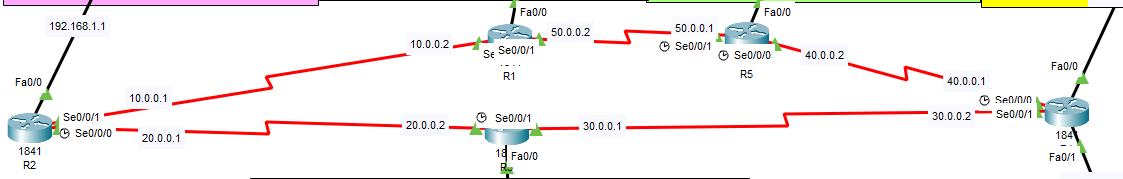
**Santral 7’deki Test Aşamaları**

**İletişim**

Server - FİREWALL

PC – FİREWALL

Yukarıdaki ip adresine sahip bilgisayarlar aralında iletişim kuramaz. Bunun sebebi sunucudaki aktif olan firewall sistemidir. Bu sistem aktif olduğu sürece aralarında iletişim kurulamayacaktır.



**OSPF Bağlantısı**

Hidroelektrik santral, 7 farklı merkezden oluşmaktadır. Ana Kontrol Merkezi, sistem genelindeki ana kontrolü üstlenirken Baraj Kontrol Merkezi, su seviyelerini, baraj kapaklarını ve su akışını yönetir. Türbin Merkezi enerji üretimini sağlarken, Enerji Dağıtım Merkezi oluşturulan enerjiyi belirlenen bölgelere iletmek ve dağıtmakla sorumludur. Güvenlik Merkezi, fiziksel güvenliği sağlamak ve ağ güvenliğini denetlemek üzere kurulmuştur. Bakım Merkezi, tesisin bakımını planlar ve yönetirken, Veri Yedekleme Merkezi ise sistem verilerinin yedeklenmesini ve kriz durumlarında kullanılabilirliğini sağlar.

Bu merkezler arasında iletişim ve veri aktarımı için bir ağ kurulmuştur. Bu ağ, 5 adet Cisco router ile OSPF protokolü kullanılarak yapılandırılmıştır. Ana Kontrol Merkezi, diğer merkezlerle OSPF protokolü aracılığıyla bağlanmıştır. Her bir merkez, kendi işlevselliğine göre ağ içinde belirli roller üstlenir ve OSPF protokolü kullanarak bu merkezler arasında en iyi veri yolları belirlenir. Böylelikle enerji üretimi, dağıtımı, güvenlik, bakım ve veri yedekleme gibi farklı süreçlerin iletişimi ve koordinasyonu sağlanmış olur.

Bu ağ yapılandırması sayesinde, her bir merkez kendi işlevlerini etkin bir şekilde yerine getirebilir ve aynı zamanda diğer merkezlerle iletişim halinde olabilir. OSPF protokolü, veri iletimi için en kısa ve en hızlı yolları belirlerken, aynı zamanda ağın güvenliğini ve bütünlüğünü de sağlar. Bu da hidroelektrik santralinin verimli bir şekilde çalışmasını ve farklı birimler arasında koordinasyonu sağlar.

**OSPF Bağlantısı Nasıl Kuruldu ?**

Öncelikle tüm routerlar arasında kurmuş olduğumuz ip atamaları kısmından bahsedelim.

R1 = FastEthernet 0/0 = 192.168.3.1 , 255.255.255.0

R1 = Serial 0/0/0 = 10.0.0.2 , 255.0.0.0

R1 = Serial 0/0/1 = 50.0.0.2 , 255.0.0.0

R2 = FastEthernet 0/0 = 192.168.1.1 , 255.255.255.0

R2 = Serial 0/0/0 = 10.0.0.1 , 255.0.0.0

R2 = Serial 0/0/1 = 20.0.0.1 , 255.0.0.0

R3 = FastEthernet 0/0 = 192.168.6.1 , 255.255.255.0

R3 = Serial 0/0/0 = 20.0.0.2 , 255.0.0.0

R3 = Serial 0/0/1 = 30.0.0.1 , 255.0.0.0

R4 = FastEthernet 0/0 = 192.168.5.1 , 255.255.255.0

R4 = Serial 0/0/0 = 30.0.0.2 , 255.0.0.0

R4 = Serial 0/0/1 = 40.0.0.1 , 255.0.0.0

R5 = FastEthernet 0/0 = 192.168.4.1 , 255.255.255.0

R5 = Serial 0/0/0 = 40.0.0.2 , 255.0.0.0

R5 = Serial 0/0/1 = 50.0.0.1 , 255.0.0.0

Yukarı tarafta yazılan kodlar bizim routarlarımızın içerisinde hem santral aralarındaki bağlantılar için yazılmış ip adreslerini barındırmaktadır. Hemde router bağlantıları arasında yazılan ip adreslerinin bağlantısı bulunmaktadır.

**Routerlar Arası Bacakların İp Atamaları**

R1 – R2 : 10.0.0.2 , 10.0.0.1

R2 – R3 : 20.0.0.1 , 20.0.0.2

R3 – R4 : 30.0.0.1 , 30.0.0.2

R4 – R5 : 40.0.0.1 , 40.0.0.2

R5 – R1 : 50.0.0.1 , 50.0.0.2

Tüm ip atamalarından bahsettiğimize göre şimdi ospf bağlantısını nasıl gerçekleştireceğimize bakalım.

Bu aşamada yapılacak tüm işlemleri her router için gerçekleştireceğiz.

**Router 1**

R1(config)#router ospf 10

R1(config-router)#network 192.168.3.1 0.0.0.255 area 0

R1(config-router)#network 10.0.0.0 0.0.0.3 area 0

R1(config-router)#end

**Router 2**

R2(config)#router ospf 10

R2(config-router)#network 10.0.0.0 0.0.0.3 area 0

R2(config-router)#network 192.168.1.0 0.0.0.255 area 0

R2(config-router)#end

Yukarıda bulunan kodları router 1 ve router 2 için yazdık. Bu bağlantıları tüm birbirine bağlanan 2 routerlar arasında gerçekleştiriyoruz. Bu kısımları tamamladıktan sonra ospf bağlantımızın test aşamasına geçebiliriz.

**OSPF Bağlantısının Test Aşamaları**

**İletişim**

Santral 3

Santral 6

Yukarıdaki belirtilmiş olan santraller arasından ospf bağlantısı ile iletişim kurulabilir. Onun dışındaki iletişim kurulmaya çalışan yerlerde bu işlem başarısız olmaktadır.

Not: Ospf bağlantısı nedeniyle bu aşamada ilk göndermeye çalıştığımız pdu failed sonucu döndürebiliyor fakat aynı bilgisayarlara tekrardan pdu işlemini uygularsak sonucun succesful döndüğünü göreceksiniz.

**İlk Deneme Aşamasındaki Failed Görüntüsü**



**İkinci Deneme Aşamasındaki Succesful Görüntüsü**



Not : Tüm routerlar şifrelenmiştir. Router Şifreleri 12345 olarak ayarlanmıştır.

**Kaynakça**

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://alms-cdn.gelisim.edu.tr/BlmsFileRepo/1/course/811257/activity/821232/2\_hafta\_uygulama.pdf

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://alms-cdn.gelisim.edu.tr/BlmsFileRepo/1/course/811257/activity/817415/cisco\_uygulama\_1.pdf