YILDIZ TECHNICAL UNIVERSITY

FACULTY OF ELECTRICAL AND ELECTRONICS

Computer Networking Technologies

(BLM 3022)

LAB 3 REPORT

18011052 – Faruk Veli Özdemir

veli.ozdemir@std.yildiz.edu.tr

DEPARTMENT OF COMPUTER ENGINEERING

1. INTRODUCTION

Tasarlanan bu ağda Ring Topolojisini kullandı. Bu topolojide iletilmek istenen veri bütün cihazların bağlı olduğu halka yapısındaki bir iletim hattında dolaşmaya başlar. Cihazlar iletilen verinin alıcı adresine bakarlar ve veri kendilerine gelmişse veriyi alırlar. Eğer veride bulunan alıcı adres kendileri değilse veriyi halka yapısındaki ağda bir sonraki cihaza gönderirler.

Bu topolojinin bir dezavantajı bütün cihazların gelen veriyi sahibi bulunana kadar kontrol etmesidir. Fakat VLAN yapısı sayesinde cihazlar mertebesine inmeden switch katında bu kontrol yapılır ve veri sadece ilgili cihaza yönlendirilir.

Tasarlanan ağda 12 farklı PC ve 9 farklı switch kullanılmıştır. Merkezlerde bulunan 3 switch her farklı binaları alt katmanda bulunan switchler ise bağlı bulundukları binanın farklı katlarını temsil etmekte ve her katta da 3 farklı VLAN'a bağlı olan 3'er PC bulunmaktadır.

Bu topolojinin bir diğer dezavantajı ise bir switch ağda bulunmayan bir MAC adresine veri göndermek istediğinde karşımıza çıkıyor.

Bir switch hedef switchin MAC adresini kendi MAC adres listesinde arar, bu listede bulunuyorsa hedef switchle arasında bir bağlantı vardır demektir ve veriyi hedefe gönderir. Kendi listesinde yoksa komşu switche sorar ve komşu switchin MAC listesinde olup olmadığı kontrol edilir. Bu şekilde hedef MAC adresli switch bulunana kadar komşudan komşuya bir arama başlar. Bu arama birbirine bağlı LAN'lar arasında dolandıktan sonra verinin kaynağı olan switche kadar gelir ve yeni bir arama döngüsü başlar.

Bu döngü halini kırmak STP (Spanning-tree Protocol) ile bir noktada kırılma imkanı vardır. Ağ içerisinde en düşük MAC adresli switchte bulunan alternate port arama işleminin son çıkış portu demektir ve bu porta gelen veri dolaşıma tekrar verilmez ve döngü kırılır.

Aynı zamanda spanning-tree algoritması, köprü ve anahtarlayıcı temelli ağlarda kullanılır ve trafiğin kaynaktan hedefe giderken geçebileceği en iyi yola karar verir. Bu algoritma tüm yedek yolları da göz önünde bulundurup, herhangi bir anda bunlardan yalnızca birini aktif hale getirir.

Spanning-tree Protokolü'nün aktif olarak kullanıldığı ağlarda her bir ağ başına bir tane kök köprü (root bridge), her bir kök olmayan köprüde (non-root bridge) bir tane kök portu (root port), ve her bir parçada trafiğin geçmesi için bir tane atanmış port (designated port) bulunur.

2. METHOD

Öncelikle ağımızda bulunan bütün switchlerde VLAN 10, VLAN 20 ve VLAN 30 oluşturuluyor. Ardından her merkezi switch bir binayı temsil ettiği için her katta bulunan switchler de bu merkezi switchlere bağlanılıyor. Ardından her katta bulunan PC'ler katta bulunan switclere bağlanıyor. Her switche bağlı olan alt PC'lerin IP adresleri atanıyor. Aynı local ağda bulunan yani aynı binada bulunan PC'lerin IP adreslerinin ilk üç hanesi aynı olacak şekilde konfigüre ediliyor.

PC'lerin subnetmast değeri ise 255.255.0.0 olarak düzenleniyor. Bunun sebebi ise bir PC'nin farklı bir fiziksel ağda bulunan fakat aynı VLAN içerisinde bulunan başka bir PC'ye veri göndermek istediğinde Subnetmask değeriyle alıcı IP'sinin aynı fiziksel ağda olup olmadığının kontrolünün yapılması ve aynı fiziksel ağda değilse Default Gateway'e gönderilmesi. Ağ yapımızda router kullanmadığımız için PC'lerin farklı bir fiziksel ağa veri göndermek istediğinde subnetmask kısıtlamasına takılmasını istemiyoruz. Bu şekilde yaptığımız zaman verinin her ağa gönderilebileceği ihtimalini de VLAN yapısıyla switch katında kısıtlıyoruz.

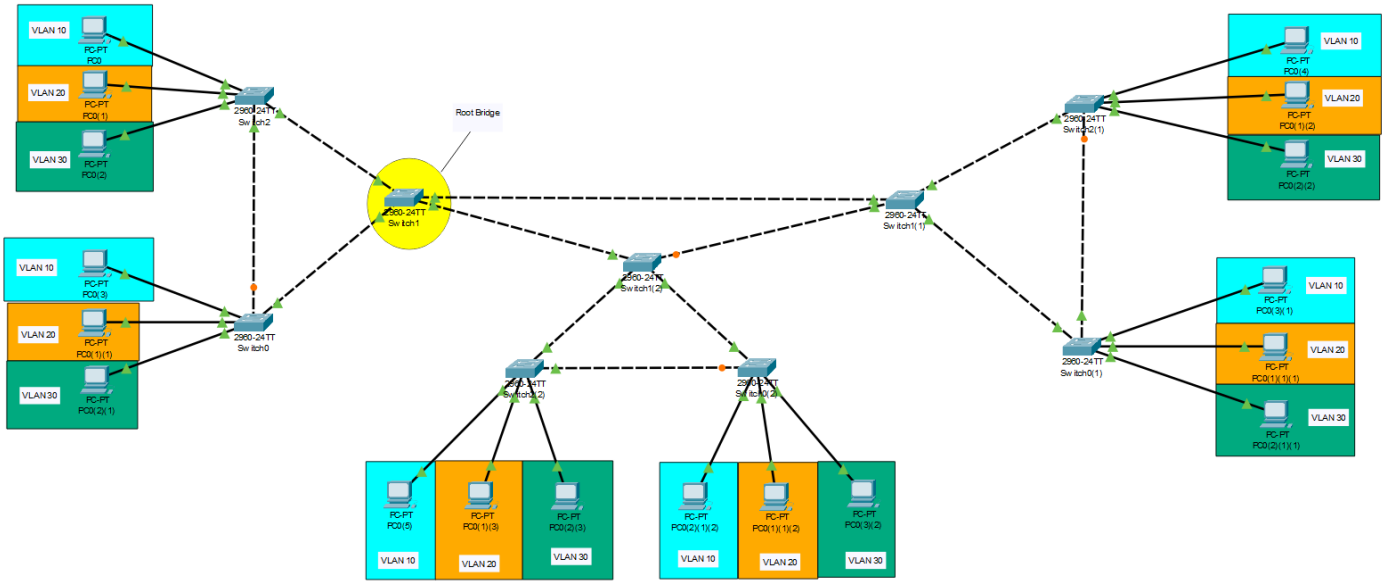
Aynı gruplara ait PC'lerin bağlı oldukları switch portlarını aynı VLAN değerini vererek o porta sadece başka bir fiziksel ağda olsa da aynı gruba ait bir PC'den veri gelmesini sağlıyoruz. Bu şekilde hem dışarıdan gelecek olan verinin sadece ilgili VLAN a sahip porta yönlendirilmesini sağlıyoruz hem de aynı fiziksel ağ içinde bulunan farklı gruplara ait PC'erin arasındaki iletişimi kısıtlayarak kesiyoruz.

Switch cihazlarının VLAN ile ayırdığımız ve PC bağlı olan portlarına Access modunda sadece ilgili VLAN'a erişim sağlayabilmesini ayarlarken başka bir swtich ile arasındaki bağlantıyı sağlayan portlarını trunk moduna ayarlıyoruz. Bu sayede bir port üzerinden farklı VLAN'lara ait verilerin geçişini sağlayabiliyoruz. Temel olarak Access mode ve Trunk mode arasındaki fark ; Access mode sadece belirtilen bir tane VLAN'a ait verilerin porttan geçişine izin verirken Trunk mode birden çok VLAN'a ait verilerin bir port üzerinden geçişine izin veriyor.

Trunk mode ile switchler arasında birden çok VLAN'a ait verilerin geçişine izin vererek farklı binalardaki aynı grupta bulunan PC'ler arası iletişime izin verilmiş oldu. Bu kısımda eğer bir switche belirlenen VLAN 10 , 20, 30 dışında farklı bir VLAN'dan ya da herhangi bir VLAN'a ait olmayan veri geldiğinde bu verileri kabul edip dağıtan default bir VLAN belirlememiz gerekiyor. Bunun için de zaten switch cihazının default olarak kullanmaya başladığımız zaman hali hazırda default olarak ayarlanmış olan VLAN 1'i native VLAN olarak ayarlıyoruz ve harici gelecek olan verileri bu VLAN'a yönlendiriyoruz.

Şimdiye kadar yapılan işlemler VLAN işlemleridir. Kullanılan Cisco Packet Tracer programı oluştulan ağda otomatik olarak STP uyguladığı için STP konfigürasyonu adına yapılacak işlem kalmamıştır. Sadece her switchin CLI bölümüne gerekli komutlar girilerek switchlerin MAC adresleri tespit edilir. MAC adresleri incelenerek simülasyonda test edilecek bağlantılar bulunuyor. Oluşturulan ağda '0000.0CB1.296A' MAC adresli Switch1 isimli switch en düşük MAC adresine sahip olduğu için Root Switch olduğu tespit edilmiştir.

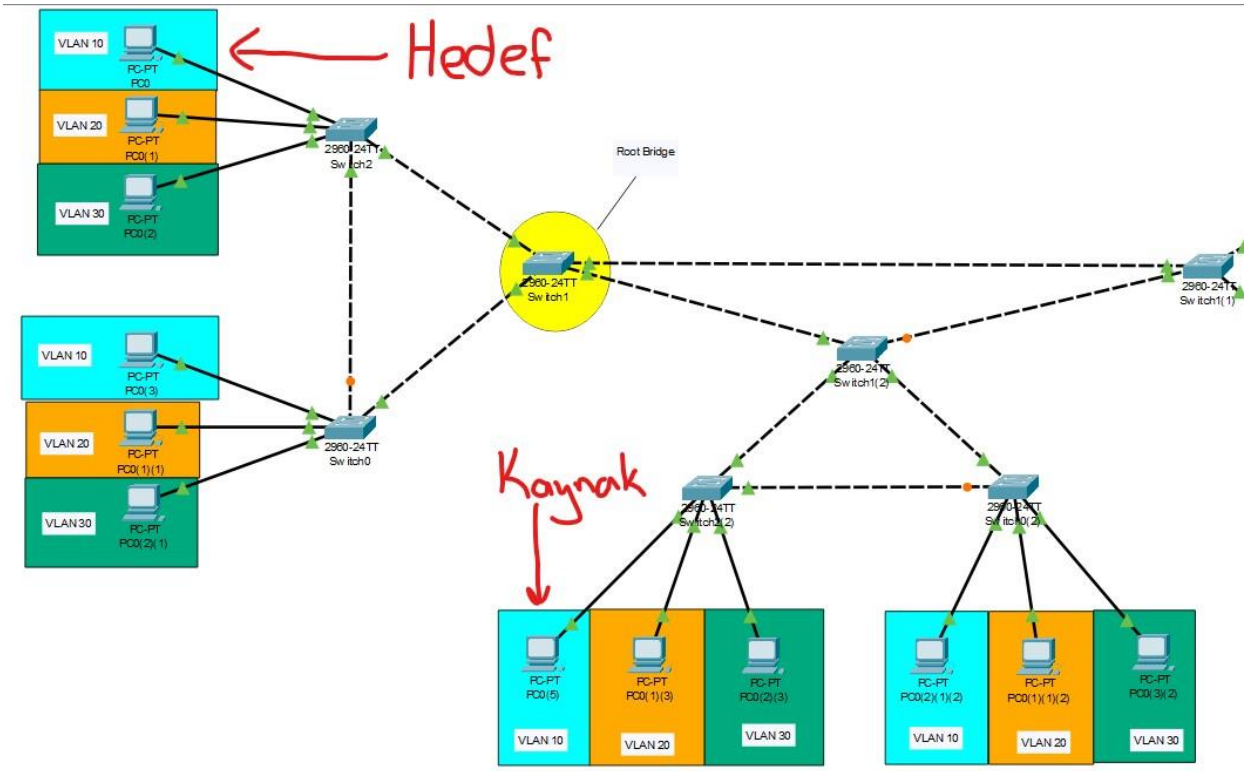
3. RESULTS



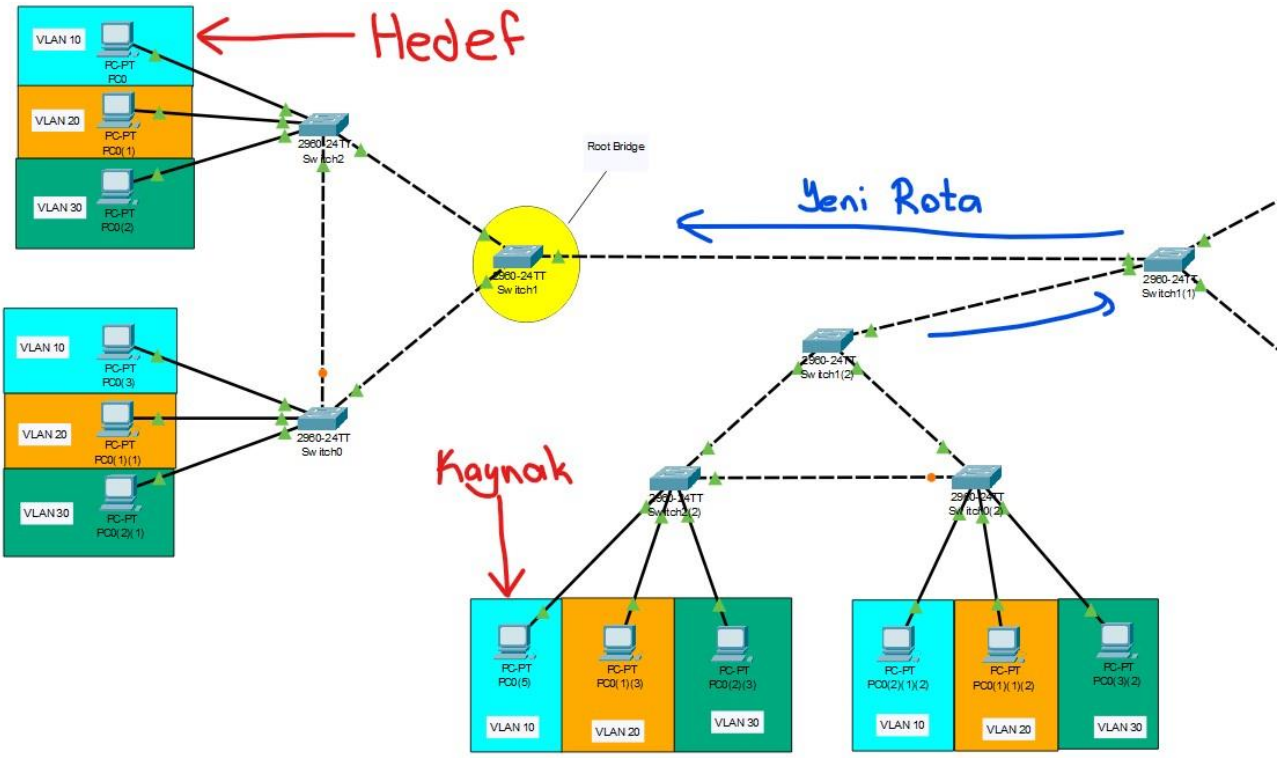
Şekil - 1

Şekil – 1'de tasarlanan ağ yapısında STP ile belirlenen root bridge ve aynı VLAN gruplarına ait PC'ler renkli bir fon ile belirtilmiştir.

Şekil – 2'de ise veri alışverişi yapılacak iki PC belirleniyor.



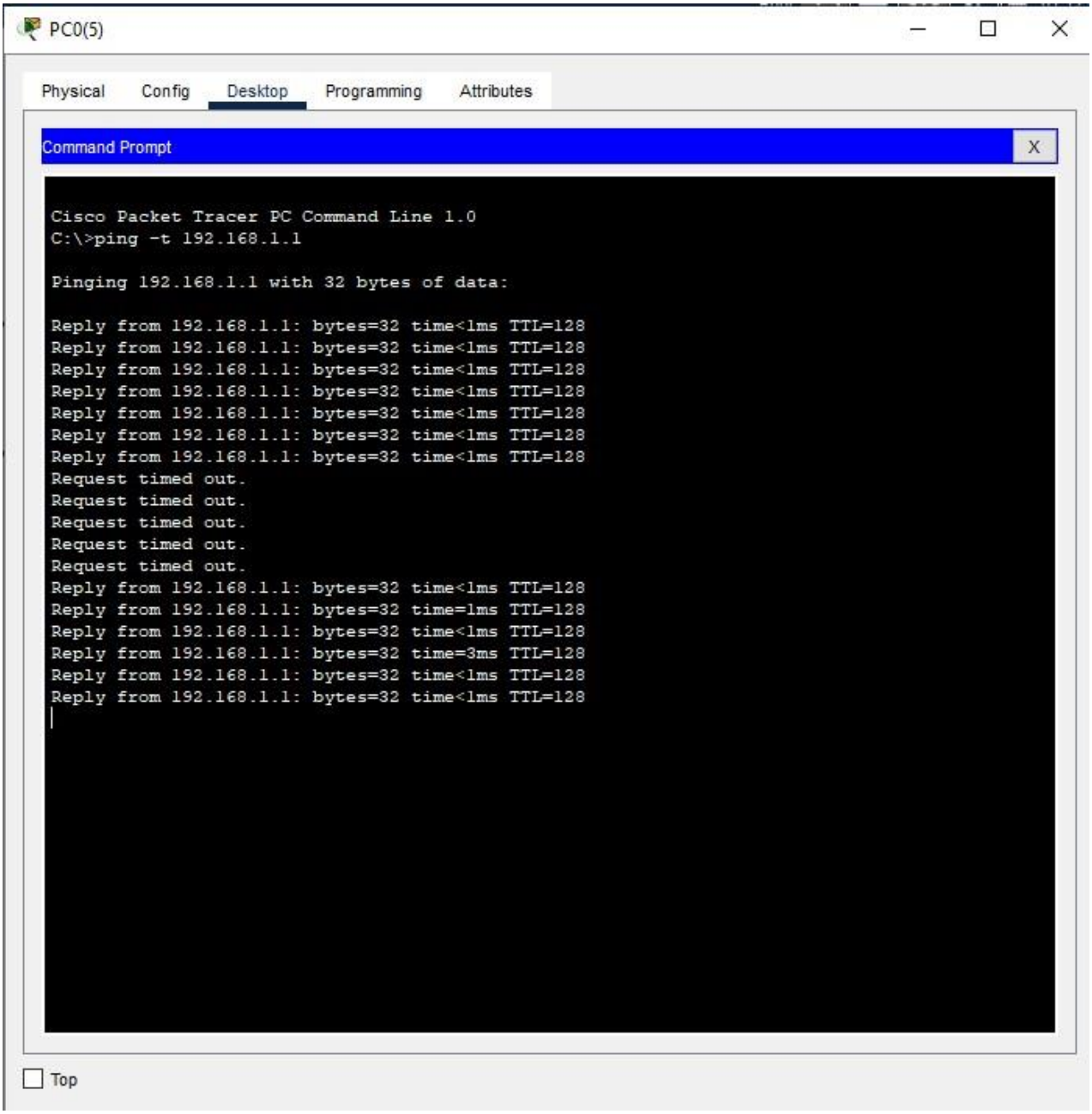
Şekil-2



Şekil - 3

Yukarıda gösterilen Şekil – 3'te ise veri alışverişinde kullanılan en az maliyetli rotadan bir bağlantı koparılıyor. STP protokolünce yeni bir rota belirlenene kadar yaklaşık 50sn geçiyor ve ardından yeni rotadan veri akışı daha maliyetli bir şekilde devam ediyor.

Son olarak aşağıda Şekil – 4'te görülen command prompt ekranında veri akışının sağlandığı yolda bulunan aksaklık 'Request timed out' dönüşü ile görülüyor. Bu süre boyunca ağda yeni bir rota belirleme işlemi yapılıyor ve yeni rota tespit edildiğinde ise veri gönderimi devam ediyor.


PC0(5)
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping -t 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=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Top

Şekil – 4