



YILDIZ TECHNICAL UNIVERSITY
FACULTY OF ELECTRICAL AND ELECTRONICS

Computer Networking Technologies
(BLM 3022)
LAB 2 REPORT

18011052 – Faruk Veli Özdemir

veli.ozdemir@std.yildiz.edu.tr

DEPARTMENT OF COMPUTER ENGINEERING

1. INTRODUCTION

Tasarlanan bu ağda Ring Topolojisi kullanıldı. 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 9 farklı PC ve 3 farklı switch kullanılmıştır. Aynı zamanda her switch bir departmanı temsil etmektedir ve her departmanda 3 VLAN grubuna bağlı 3 tane PC bulunmaktadır.

2. METHOD

Öncelikle ağıımızda bulunan 3 switchte ‘Student’ isimli VLAN 10, ‘Lecturers’ isimli VLAN 20 ve ‘AdministrativeStaff’ isimli VLAN 30 oluşturuluyor. Ardından her switch bir departmanı temsil ettiği için her departmanda bulunacak olan PC’ler switchlere bağlanıyor. Her switchte bağlı olan alt PC2lerin IP adresleri atanıyor. Aynı local ağda bulunan PC’lerin IP adreslerinin ilk üç hanesi aynı olacak şekilde konfigüre ediliyor.

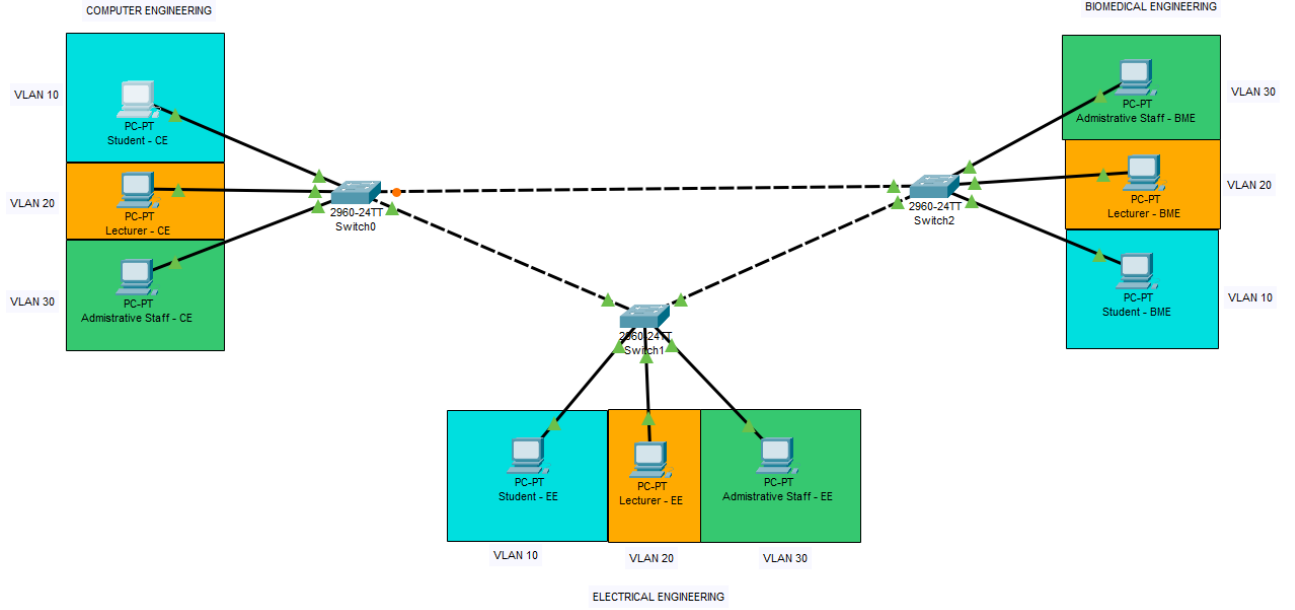
PC’lerin subnetmask değeri ise 255.255.0.0 olarak düzenleniyor. Bunun sebebi ise bir PC’nin farklı bir fiziksel ağda bulunan fakat aynı VLAN içerisinde bulunan başka bir PC’ye veri göndermek istediğinde Subnetmask değeriyle alıcı IP’sinin aynı fiziksel ağda olup olmadığının kontrolünün yapılması ve aynı 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’lerin 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 switch 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 departmanlardaki aynı grupta bulunan PC’ler arası iletişime izin verilmiş oldu. Bu kısımda eğer bir switchte 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.

3. RESULTS



Şekil - 1

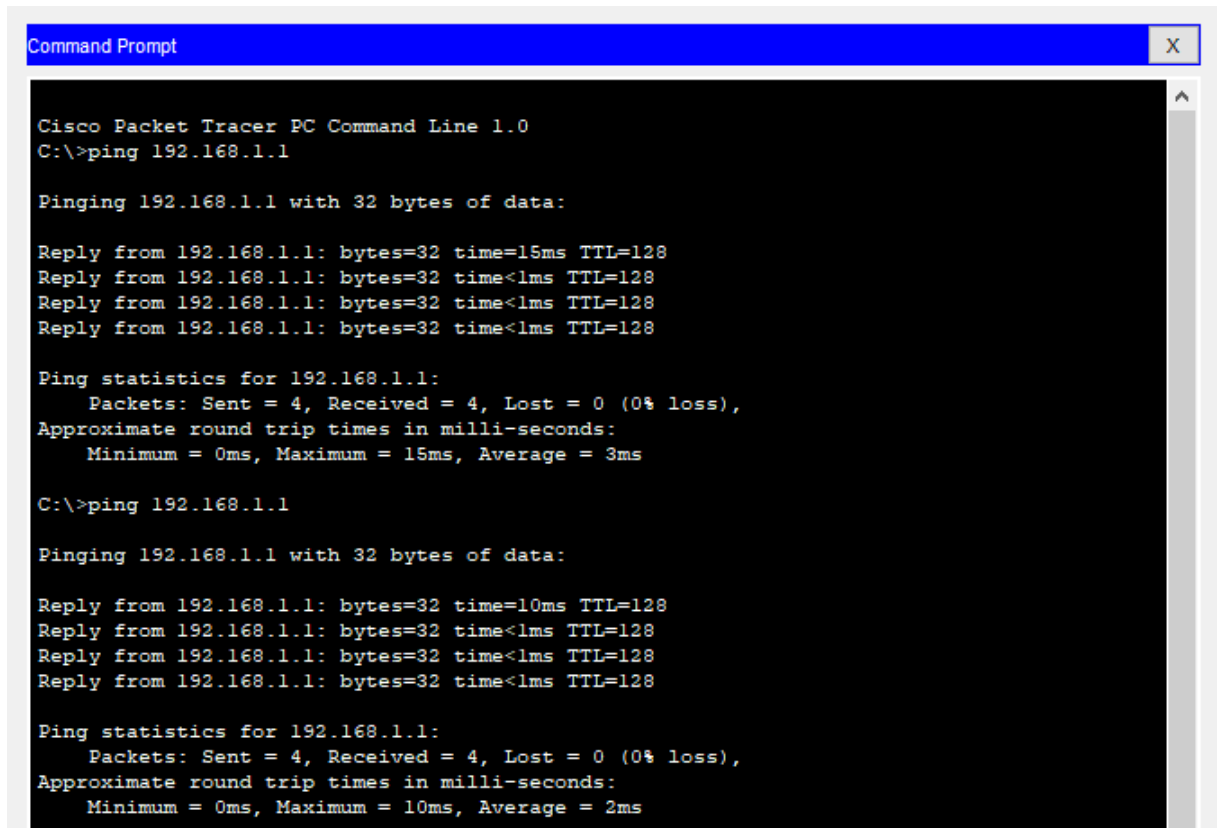
Şekil – 1’de tasarlanan ağ yapısı departman isimleri verilmiştir ve grup isimleriyle birlikte aynı gruplara ait PC’ler renkli bir fon ile belirtilmiştir.

Şekil – 2’de ise simülasyonun PDU özelliği kullanılarak farklı cihazlar arasında veri gönderimi yapılarak ağın istenilen şekilde çalışıp çalışmadığı test edilmiştir.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Student - CE	Student - EE	ICMP		0.000	N	0	(edit)	
	Failed	Student - CE	Lecturer - CE	ICMP		0.000	N	1	(edit)	
	Successful	Lecturer - EE	Lecturer - CE	ICMP		0.000	N	2	(edit)	
	Failed	Administrative Staff - EE	Student - CE	ICMP		0.000	N	3	(edit)	

Şekil - 2

Aşağıda verilen Şekil – 3’te ise Command Prompt yardımıyla aynı gruba ait farklı bir departmanda bulunan bilgisayara ping atılmıştır. Ping ölçümü için gönderilen 4 paketten ilkinin 15ms sürdüğü diğerlerinin 1ms’den daha kısa sürede gittiği bilgisi alınmıştır. Bunun üzerine aynı cihaza tekrar ping gönderildiğinde ise ilk paketin gönderimi 10ms sürerken diğer üçünün yine 1ms’den kısa sürdüğü gözlemlenmiştir.



```
Command Prompt X

Cisco Packet Tracer PC Command Line 1.0
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=15ms 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

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 = 15ms, Average = 3ms

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=10ms 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

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 = 10ms, Average = 2ms
```

Şekil - 3