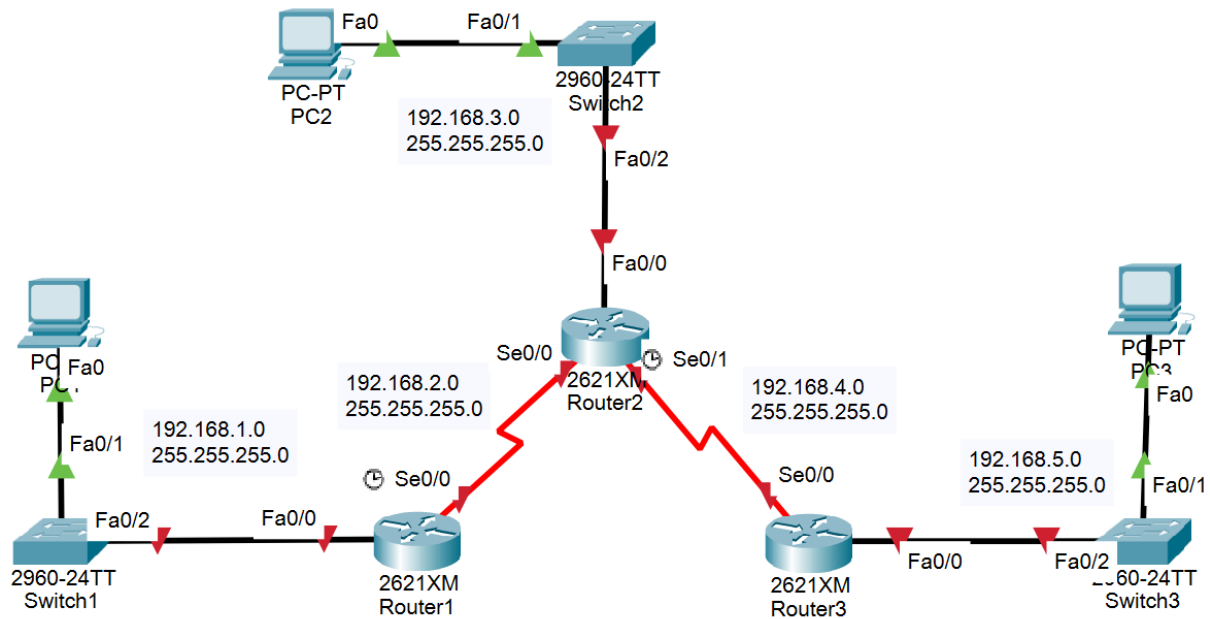


**Ankara University**  
**Department of Computer Engineering**  
**BLM3032**  
**LAB 6**

**TOPOLOGY DIAGRAM**



**Addressing Table**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
	S0/0/1	192.168.4.2	255.255.255.0	N/A
R3	Fa0/0	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.4.1	255.255.255.0	N/A
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NIC	192.168.3.10	255.255.255.0	192.168.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

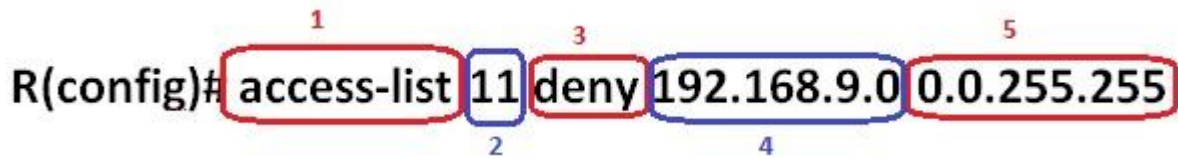
**SECTION I: STANDARD ACCESS CONTROL LISTS**

**Standard Access Control Lists (ACLs)** control traffic by comparing source address of the IP packet to the address specified in access control list.

Configure all the interfaces of all the routers on given topology. Configure the hosts on the

Ethernet segment.

R(config)# **access-list** **11** **deny** **192.168.9.0** **0.0.255.255**



1. Access List komutu
2. Kuralın ismi (Standart ACL'de 1 ile 99 arası isimler verilebilir.)
3. Deny (Reddet) veya Permit (İzin ver) komutları arkasından gelen IP'yi wildcard'a uygulayarak izin verir veya onu reddeder.
4. IP adresi 192.168.9.0 (11000000.10101000.00001001.00000000)
5. Wildcard'da belli bir noktaya kadar bitler 0 olur daha sonra gerekirse 1 olur. Sol baştan itibaren 0 olan bit sayısı kadar 4 numaralı alandaki IP'deki sol baştaki bitler alınır ve 3 numaralı alandaki deny veya permit uygulanır. Bu örnekte bakacak olursak Wildcard'da sol baştan 16 bit 0 ve sonra 16 bit 1. Buna göre 4 numaralı alandan ilk 16 bit alınır (11000000.10101000.), bu ağa gelecek olan ve 11000000.10101000 (192.168.) ile başlayan tüm ağlar 3 numaralı alandaki kurala göre değerlendirilir (izin verilir veya reddedilir.) Eğer Wildcard 0.15.255.255 (00000000.00001111.11111111.11111111) olsaydı yönlendirici (router) 192.168.9.0'un ilk 12 bitini değerlendirecek idi. Gelen IP'lerin ilk 12 bitine bakacak ve kalanları önemsemeyecekti.

**Kuralı çalıştırmak için aşağıdaki kalıpta kod yazılabilir.**

R3(config-if)# **ip access-group** **11** **in**



1. Kuralı çalıştırmak için komut.
2. Daha önce oluşturulmuş olan ve şimdi çalıştırılmak istenen kuralın ismi
3. Gelen erişim isteklerinin fastEthernet'ten router'a girerken (in) veya router'dan fastEthernet'e çıkarken (out) engellenecekleri bu alandaki komutla belirlenir.

Create an access list that will prevent access from the 192.168.1.0 network

**R1(config)#access-list 1 deny 192.168.1.0 0.0.0.255**

**R1(config)#access-list 1 permit any**

**R1(config)#interface fastEthernet 0/0**

**R1(config-if)#ip access-group 1 in**

Create an access list that will prevent access from the 192.168.3.0 network

```
R2(config)#access-list 1 deny 192.168.3.0 0.0.0.255
```

```
R2(config)#access-list 1 permit any
```

```
R2(config)#interface fastEthernet 0/0
```

```
R2(config-if)#ip access-group 1 in
```

Create an access list that will prevent access from the 192.168.5.0 network

```
R3(config)#access-list 1 deny 192.168.5.0 0.0.0.255
```

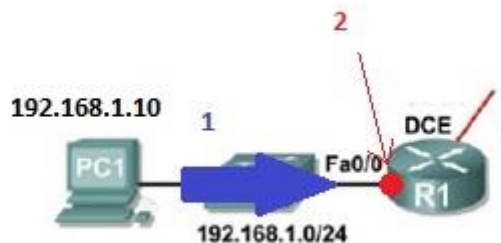
```
R3(config)#access-list 1 permit any
```

```
R3(config)#interface fastEthernet 0/0
```

```
R3(config-if)#ip access-group 1 in
```

Ping the router FastEthernet 0/0 interface or various interfaces on the network to test your access control lists.

Yukarıda yazılan kodlara göre her grup kendi bilgisayarından fastEthernet üzerinden router'a girişi engellemiş olur. Her grup ağdaki diğer bilgisayarlara ping atmayı denediğinde router'a bile ulaşamadıkları için "Hedef ana bilgisayar ulaşılamaz." hatası alınır.



1. PC 1'den PC 2 veya PC 3'e ping atıldığında, ping fastEthernet'ten geçer.
2. Bu noktada PC 1'in koyduğu kural devreye girer. Router ping'in geldiği noktaya bakar (192.168.1.10) ve kuraldaki IP ve wildcard ile karşılaştırır.
  - a. Wildcard 0.0.0.255 (00000000.00000000.00000000.11111111) buna göre kuraldaki IP ile pingin geldiği IP'nin ilk 24 biti karşılaştırılır. İkisi de 192.168.1 olduğu için ve fast Ethernetten routera giriş yapıldığı için (in) router erişime izin vermez.
  - b. Ping atan bilgisayarda "Hedef ana bilgisayar ulaşılamaz." hatası alınır.

PC 2 ve PC 3 de ayrı ayrı kendi ağlarından router'a girişi engelledikleri için aynı hatayı onlar

da alacaklardır.

**Önemli Not:** Ping yapısından dolayı karşıdaki bilgisayara gider ve geri döner. Örneğin Router 2'de ki kural kaldırılırsa ve PC 2'den PC 1'e ping atılırsa, ping Router 2'den geçecek Router 1'den de kurala takılmadan geçecektir (Router'dan fastEthernete çıkıyor - out). Ancak PC 1'e ulaştıktan sonra geri dönerken Router 1'deki kurala takılacaktır (Ping artık PC 1'den geliyor ve fastEthernet'ten router'a giriş Router 1'deki kural ile engellendi.) Bu durumda PC 2'deki bilgisayarda "İstek zaman aşımına uğradı!" hatası alınacaktır.

## SECTION II: EXTENDED ACCESS CONTROL LISTS

**Extended Access Control Lists** control traffic by comparing source and destination addresses of the IP packet to the addresses specified in access control list.

The diagram shows the command `R2(config)#access-list 100 deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255` with numbered annotations: 1 points to `access-list`, 2 points to `100`, 3 points to `deny`, 4 points to `ip`, 5 points to the source address and wildcard `192.168.5.0 0.0.0.255`, and 6 points to the destination address and wildcard `192.168.3.0 0.0.0.255`.

1. Access List Komutu
2. Kuralın ismi (Extended ACL'de kurallar 100'den 199'a kadar isimlendirilebilir.)
3. Deny (Reddet) veya Permit (İzin ver) komutları arkasından gelen IP'yi Wildcard'a uygulayarak izin verir veya onu reddeder.
4. Standart ACL'den farklı olarak komuta ip de yazılması gerekmektedir.
5. Kaynak IP ve Wildcard'ı
6. Hedef IP ve Wildcard'ı

Create an access list that will that will deny IP access for any users on the 192.168.5.0 network if they are trying to access network 192.168.3.0.

```
R2(config)#access-list 100 deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255
```

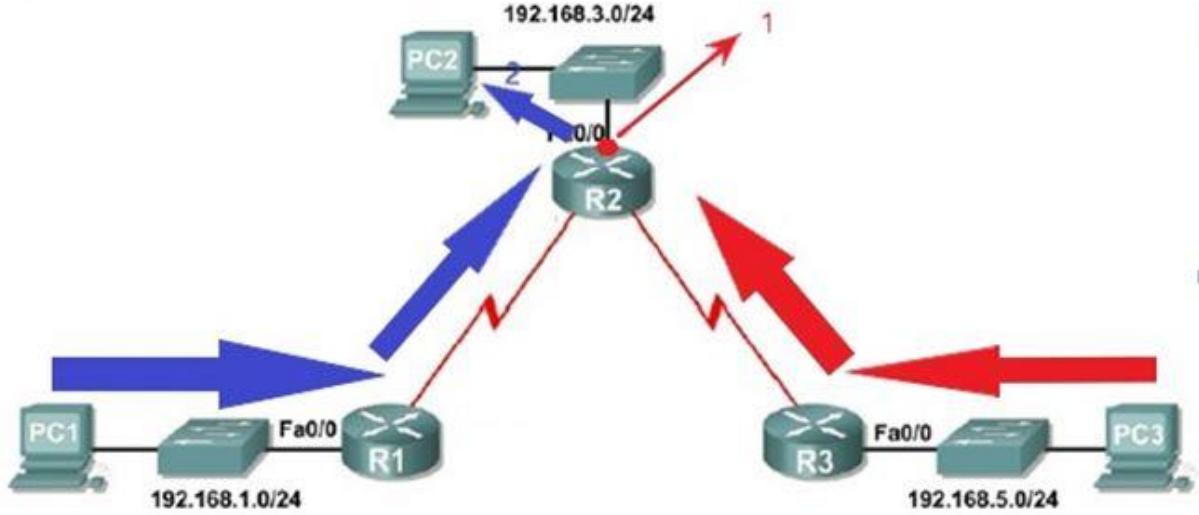
```
R2(config)#access-list 100 permit ip any any
```

```
R2(config)#interface fastEthernet 0/0
```

```
R2(config-if)#ip access-group 100 out
```

Ping the router R2 FastEthernet 0/0 interface from 192.165.5.0 and 192.168.1.0 networks to test your access control lists.

Buradaki kurala göre kaynak olan 192.168.5.0 ağından gelen, hedef olan 192.168.3.0 ağına giden ve Router 2'den fastEthernete çıkış (out) yapan erişimler engellenecektir.



1. PC 3'ten PC 2'ye atılan ping Router 2'den çıkarken (out) kurala göre test edilir. PC 3'ün IP si 192.168.5.10 ilk 24 biti (192.168.5) kuraldaki kaynak IP nin ilk 24 biti ile aynıdır. Hedef olarak seçilen PC 2'nin IP'si 192.168.3.10 ilk 24 biti (192.168.3) kuraldaki hedef biti ile aynı ve ping işlemi Router 2'den fastEthernete çıkış (out) yapıyor. Bu durumda bu ping engellenektir. PC 3'ün bilgisayarında "Hedef ağ ulaşılamaz!" uyarısı oluşacaktır.
2. PC 1'den PC 2'ye atılan ping ise Router 2'de kural tarafından engellenmeyecektir. Çünkü kaynak IP si olan 192.168.1.10 kuraldaki IP ile eşleşmez.

**Önemli Not:** Eğer PC 2, PC 3'e ping atarsa; Router 2'deki kurala takılmayacaktır. (Kaynak ve Hedef farklı ayrıca fastEthernet üzerinden Router 2'ye giriş (in) yapıyor.) Ancak PC 3'e ulaştıktan sonra geri dönerken Router 2'de kurala takılacaktır. Bu durumda PC 2'nin bilgisayarında "İstek zaman aşımına uğradı!" uyarısı görünecektir.