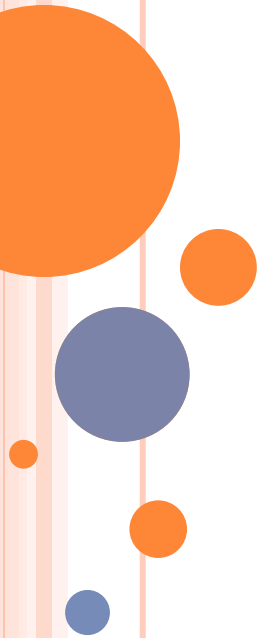


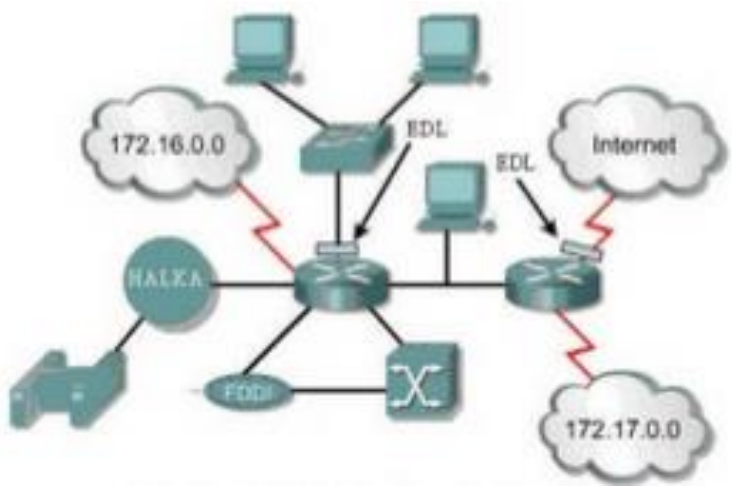
Erişim Denetim Listeleri
(Access Control Lists-ACL)

Sunum İçeriği

- Erişim Denetim Listeleri nedir?
- EDL'lerin işlevleri
- EDL'lerin genel yazımı
- EDL çeşitleri
- EDL örnekleri

Erişim Denetim Listeleri Nedir?

- EDL'ler bir yönlendirici arabirimi üzerinde geçiş yapan veri trafiğine uygulanacak olan koşullar listesidir.
- Bu listeler yönlendiriciye kendisine gelen veri paketlerinden hangilerinin iletilip hangilerinin reddedileceğini söyler.



Erişim Denetim Listeleri Nedir? (Devam)

- EDL'ler protokol, yön veya port temelli olarak tanımlanır.
- EDL'ler trafiği arabirim üzerinde, tek bir yönde ve tek zamanda kontrol ederler.
- Her farklı yön için ayrı ayrı EDL yazılması gerekmektedir. Hem giriş için hem çıkış için.

EDL'NİN İŞLEVLERİ

- Ağ trafiğini sınırlar ve ağ performansını artırır.
- Ağdaki trafik akışının kontrolünü sağlar.
- Ağ erişiminde temel bir güvenlik düzeyi sağlar.
- Yönlendirici arabirimlerinde hangi tip trafiğe yol verileceği ya da bloke edileceğine karar verir.

EDL'LERİN GENEL YAZİMİ

- Genel tanımlama şu şekildedir:
  Router(config)# access-list **ACL_id** **permit/deny** koşul
- Daha sonra ilgili arayüzün içerisine girip şu komutu yazıyoruz:
  Router(config-if)# ip access-group **ACL_id** **in/out**

```
Router(config)#
Router(config)# access-list 2 deny    192.168.1.2
Router(config)# access-list 2 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 2 deny    192.168.0.0 0.0.255.255
Router(config)# interface serial 0
Router(config-if)# ip access-group 2 in
```

EDL'LERİN GENEL YAZİMİ (DEVAM)

- EDL'leri oluştururken dikkat edilmesi gereken temel konular şu şekildedir:

- Protokol ve yön temelli bir erişim listesi olmalıdır.
- Standart erişim listesi alıcı adresine en yakın olmalıdır.
- Uzatılmış erişim listesi kaynağa en yakın olmalıdır.
- Giriş ve çıkış arabirim referansları yönlendiricinin içinden sanki "porta bakıyormuş" gibi kullanılmalıdır.

EDL ÇEŞİTLERİ

- 2 tip erişim denetim listesi vardır:
  - Standart EDL
  - Genişletilmiş (Extented) EDL

STANDART EDL

Access-list [liste numarası] [permit | deny] [IP adresi] [joker maske(isteğe bağlı)]

Bileşenler:

Liste numarası

Erişim liste numarası 1'den 99 ve 1300 den 1999'a kadar olabilir.

Permit | deny

Her ikisi de olabilir. Permit belirttiğiniz ip adresini, bir eşleme girişini içerir.

IP adresi

Bir IP adresi, belirlenmiş kuralları içeren IP adreslerini eşlemede ve kararlaştırmada kullanılır.

Joker maske

İsteğe bağlı olarak kullanılan joker maske eşlemede bir IP adresindeki bitlerin değerlerini (0/1) kontrol eder.

GENİŞLETİLMİŞ EDL

Access-list [liste numarası] [permit | deny] [protokol] [kaynak belirtme] [hedef belirtme] [protokol niteleme] [logging]

Bileşenler:

Liste numarası

Erişim liste numarası 100'den 199'a ve 2000'den 2699'a kadar olabilir.

Permit | deny

Her ikisi de olabilir. Permit belirttiğiniz ip adresini bir eşleme girişini içerir.

Protokol belirtme

Paket protokolüdür. Burası, IP,TCP,EDP veya ICMP ve diğer IP protokollerinden biri olabilir. Bununla birlikte İP protokol numarası da olabilir.

Kaynak belirtme

[Ip adresi] [joker maske] [port numarası belirtme (sadece UDP ve TCPiçin kullanılır)] biçiminde belirtilir.

Hedef belirtme

[Ip adresi] [joker maske] [port numarası belirtme (sadece UDP ve TCP çin kullanılır)] biçiminde belirtilir.

Genişletilmiş Edl (Devam)

IP adresi

Bir IP adresini eşlemek için kullanılır.

Joker maske

İsteğe bağlı olarak kullanılan joker maske eşlemede bir IP adresindeki bitlerin değerlerini 0/1) kontrol eder.

Port numarası belirtme

İsteğe bağlı belirtme, port için bir dizi numaralara karar verir.

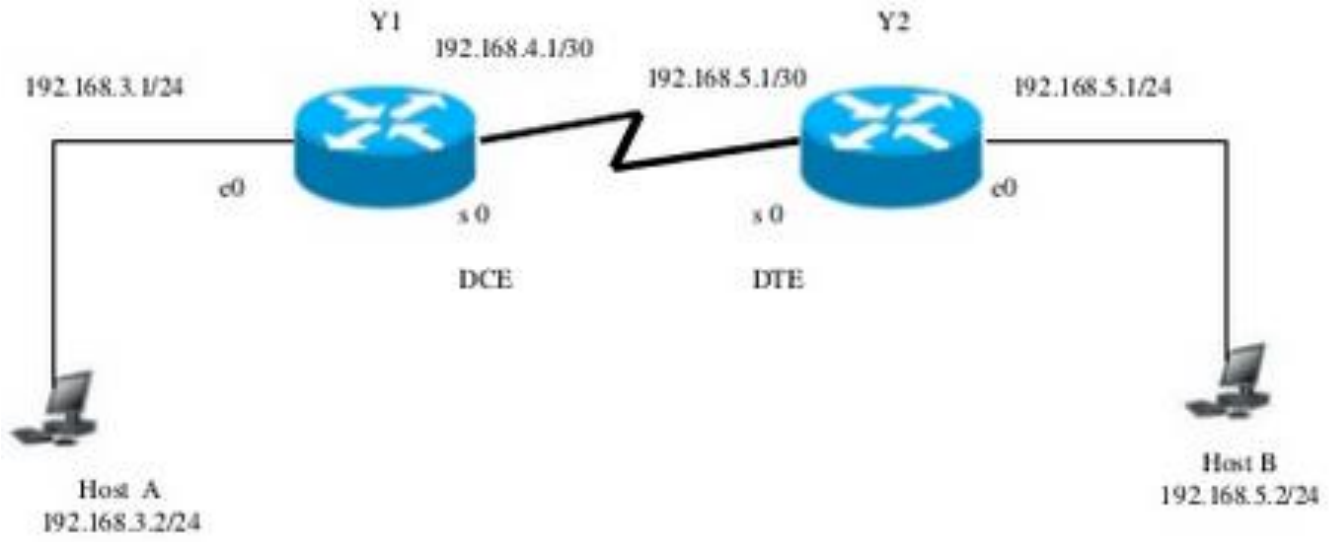
Protokol niteleme

İsteğe bağlı belirtme, protokol numaralarına daha fazla özellik tanımlar.

Logging (Kayıtlama)

Logging anahtar kelimesi. Erişim liste girişlerinin eşlendiğinde paket bilgilerini hepsini kayıt altına alır.

UYGULAMA 1


Y1
192.168.4.1/30
Y2
192.168.3.1/24
192.168.5.1/30
192.168.5.1/24
e0
s 0
s 0
e0
DCE
DTE
Host A
192.168.3.2/24
Host B
192.168.5.2/24

UYGULAMA 1 (DEVAM)

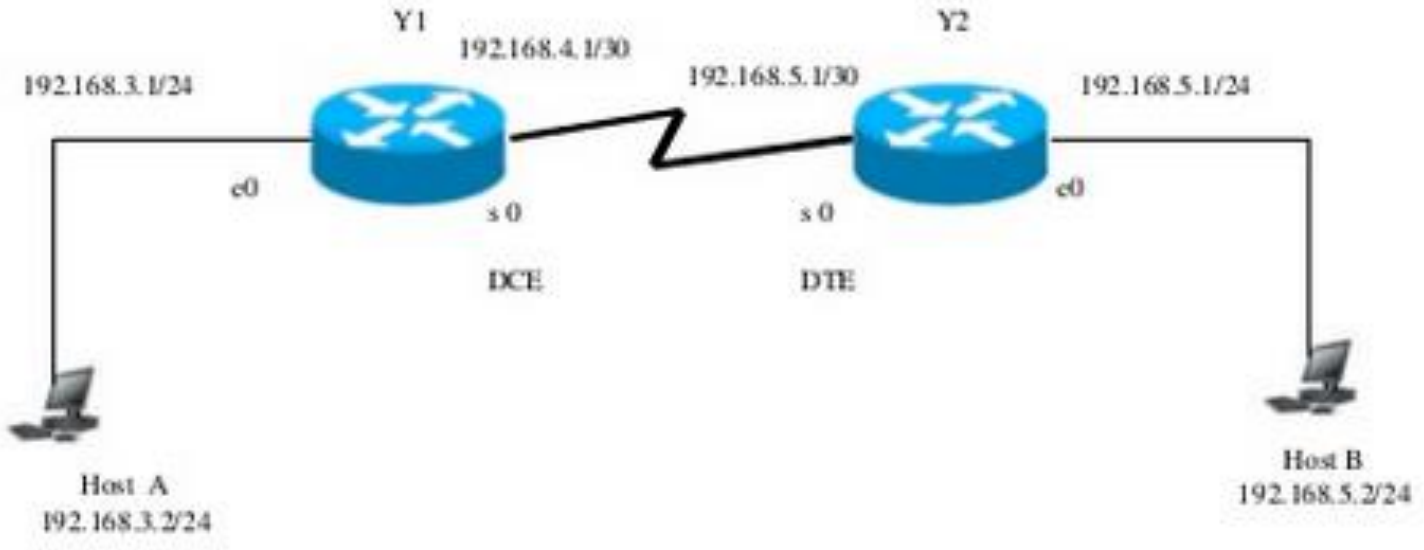
Yukarıdaki resimde Host B' den çıkan paketlerin 192.168.3.0 ağına erişmesini engellemek için.

Y1 Yönlendiricisinde;
Y1(config)#access-list 1 deny 192.168.5.2 0.0.0.0
Y1(config)#access-list 1 permit any
Y1(config)#inter serial 0
Y1(config-if)#ip access-group 1 in

veya

Y2 yönlendiricisinde;
Y2(config)#access-list 1 deny 192.168.5.2 0.0.0.0
Y2(config)#access-list 1 permit any
Y2(config)#inter ethernet 0
Y2(config-if)#ip access-group 1 in

UYGULAMA 2


Y1
192.168.4.1/30
192.168.5.1/30
Y2
192.168.3.1/24
192.168.5.1/24
e0
s 0
s 0
e0
DCE
DTE
Host A
192.168.3.2/24
Host B
192.168.5.2/24

UYGULAMA 2 (DEVAM)

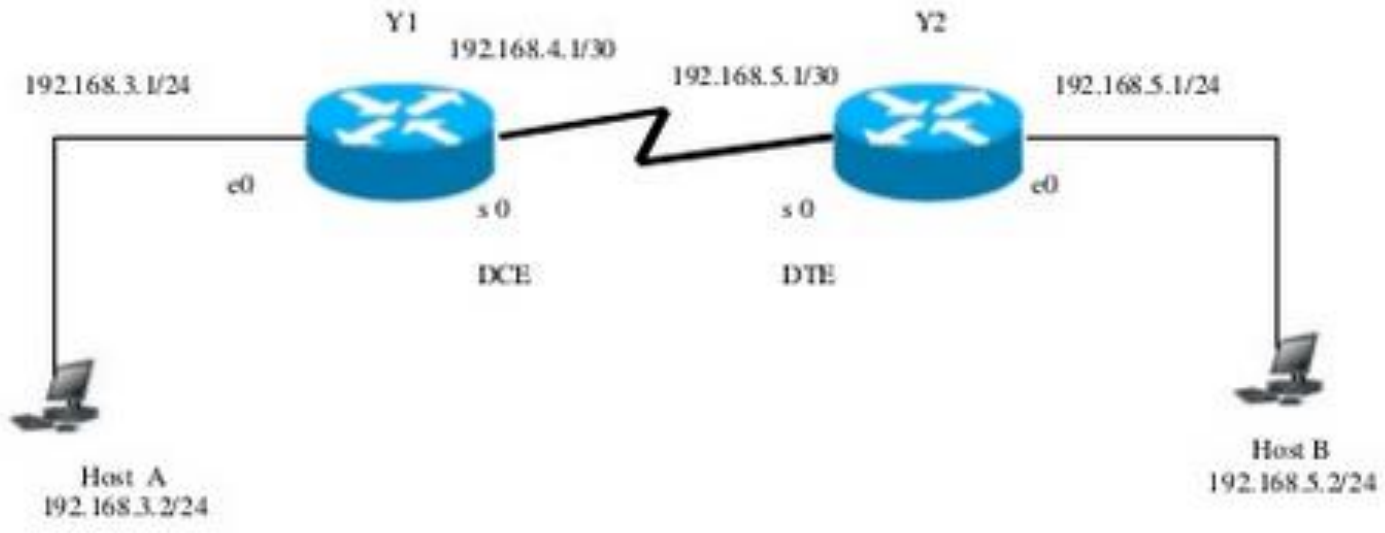
192.168.5.0 networkunun tamamının 192.168.3.0 networkuna erişmesini engellemek için.

Y1 yönlendiricisinde;
Y1 (config)#access-list 1 deny 192.168.5.2 0.0.0.255
Y1 (config)#access-list 1 permit any
Y1 (config)#inter serial 0
Y1 (config-if)#ip access-group 1 in

veya

Y2 yönlendircisinde;
Y2 (config)#access-list 1 deny 192.168.5.2 0.0.0.255
Y2 (config)#access-list 1 permit any
Y2 (config)#inter ethernet 0
Y2 (config-if)#ip access-group 1 in

UYGULAMA 3 (DEVAM)



UYGULAMA 3 (DEVAM)

Host A da bulunan FTP Server ve Web Server'a 192.168.5.2 bilgisayarının erişmesini engellemek (Kalan trafik akışı normal devam etmeli) için.

```
Y1(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 80
Y1(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 21
Y1(config)#access-list 101 permit ip any any
Y1(config)#
Y1(config)#inter serial 0
Y1(config-if)#ip access-group 101 in
Y1(config-if)#
```

veya

```
Y2(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 80
Y2(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 21
Y2(config)#access-list 101 permit ip any any
Y2(config)#
Y2(config)#inter ethernet 0
Y2(config-if)#ip access-group 101 in
Y2(config-if)#
```