ACL

ACL (Access Control List), bir kaynağa erişimleri filtrelemek için kullanılan kontrol listeleri olarak tanımlanabilir. Access Control List;

- Router arayüzlerine gelen-giden trafiği filtrelerken
- InterVLAN haberleşmesinde, trafiği filtrelenmek istenen VLAN'ları belirlerken
- Belirli ip adres aralığı için veya belirli protokoller için QoS tanımı yapılırken
- OSPF protokolüyle öğrenilen networklerin belirli routerlara öğretilmesi sağlanırken ve daha bunlar gibi birçok noktada filtreleme işlemi için kullanılıyor.

ACL açıklamada da belirtildiği gibi aslında paketleri filtrelerken değerlendirilmesi istenen özelliklerin satır satır tanımlandığı bir erişim listesidir. Her bir satırına **ACE** (**Access Control Entires**) denilmektedir. İki farklı tipte ACL tanımı yapılabilmektedir.

- **Standart ACLs**, sadece kaynak ip adresine göre filtreleme yapılması gerektiğinde kullanılıyor.
- **Extended ACLs**, hedef-kaynak ip veya port bilgilerine bakılarak filtreleme yapılması gereken durumlarda kullanılıyor.

ACL'ler oluşturulduktan sonra bu listelerin kullanılabilmesi için routerlarda **hangi arayüze hangi yönde** uygulanacağının belirtilmesi gerekiyor (Routerlarda olduğu gibi L2-L3 switch portlarına da uygulanabiliyor). Bir ACL router arayüze "in" veya "out" olmak üzere iki yönde uygulanabiliyor.

- ACL router arayüzüne "in" yönünde uygulandığında, paketler routerda uygulanan arayüze girerken ACL kontrolünden geçer.
- ACL routerde "out" yönünde uygulanmışsa paketler routerun uygulandığı arayüzden çıkış yaparken ACL kontrolünden geçer.

Her protokol (IPv4 veya IPv6) için bir arayüze, giriş ve çıkış yönlerinde sadece birer tane ACL uygulanabiliyor. Yani Dual-Stack çalışan bir topolojide bir arayüze IPv4 protokolü için giriş ve çıkış yönlerinde birer tane, IPv6 protokolü için giriş ve çıkış yönlerinde birer tane olmak üzere toplamda sadece 4 tane ACL uygulanabiliyor.

ACL yapısını birkaç cümleyle özetlemek gerekirse;

1- ACL satır satır yazılır ve her satırda belirli kurallar tanımlanır.
2- Kurallar satır satır kontrol edilir. ACL'in en üst satırında tanımlı kural alttaki satırlarda tanımlanan kurallara göre daha önceliklidir. Bu nedenle ACE'lerin tanımlanma sırası önemlidir. Kurallar özleden gelene (yukarıdan-aşağıya) doğru yazılmalıdır.
3- Paketler ACL'in üst satırlarında tanımlanan kurallardan biriyle eşleştiğinde, bu paket için alt satırlarda tanımlanan kuralların geçersiz sayılmasına neden olacaktır. Yani paketin eşleştiği ilk kural satırı pakete doğrudan uygulanır.
4- Paketler tanımlanan hiçbir satırla eşleşmediği durumda ACL'in en alt satırında bulunan **"implicit deny"** satırıyla eşleşir. Bu satırla eşleşen paketler drop edilir.

Standart ACL Konfigürasyonu

- Standart ACL genelde firewall kuralı yazmak için kullanılmaz. Daha çok NAT tanımlamaları gibi kaynak ip ile gerçeklştirilecek işlemlerde kullanılıyor.
- Konfigürasyonunda "**access-list <ACL Number> (deny | permit) <Source Network Address> <Wildcard Mask>**" komutu kullanılıyor. Bu tanımda ilk kısımda ACL'i benzersiz kılacak bir numara tanımlanıyor. Bu numaraya göre ACL'in Standar ACL mi? yoksa Extended ACL mi? olduğu anlaşılıyor. Ardından "permit" (izin ver), "deny" (engelle) kullanılarak kurala eşlenen paketlere uygulanacak filtre tipi belirtiliyor. Son olarak da kuralın uygulanacağı **kaynak network veya kaynak ip** adres bilgisiyle Wildcard maskesi tanımlanıyor.

		Kontrol Tipi	Kaynak Ip	
access-list	<1-99>	permit deny remark	Host <Ip> <network Addr>< Wild. Mask> any	log

|→ 0-99 veya 1300-1999 -> Standart ACL aralığıdır.
|→ Permit veya deny yerine "**remark**" (açıklama yazmak için) anahtar kelimesi kullanılarak açıklama da yazılabilir. Yazılan açıklama sadece yorum satırı olarak işleniyor. Herhangi bir kural olarak uygulanmıyor.
|→ Kaynak ip bilgisi olarak "**any**" kelimesi ile bütün ip adresleri de tamsil edilebiliyor.
|→ Kaynak ip adresi olarak sadece bir ip adresi tanımlanacaksa "**host**" anahtar kelimesiyle sadece ip adresinin tanımlanması yeterli oluyor (yani ayrıca Wildcard (0.0.0.0) maskesini tanımlamaya gerek kalmıyor).
|→ ACL tanımının sonuna "**log**" anahtar kelimesi eklenerek kurallarla eşleşen bir paket geldiğinde routerun bunu loglaması sağlanabiliyor (gelen paket ip adres bilgiler, geldiği saat bilgisi vs.).

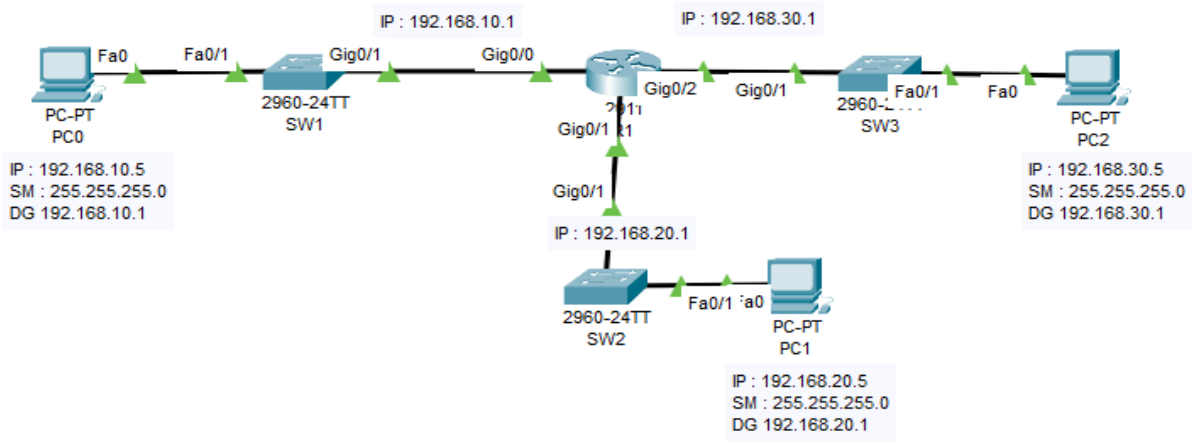
```
R1(config)#access-list ?
  <1-99>      IP standard access list
  <100-199>   IP extended access list
R1(config)#access-list 10 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
R1(config)#access-list 10 deny ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
R1(config)#access-list 10 deny host 10.0.0.1
R1(config)#access-list 10 remark ?
  LINE  Comment up to 100 characters
R1(config)#access-list 10 remark "Aciklama 1"
R1(config)#access-list 10 permit ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
R1(config)#access-list 10 permit any
R1(config)#
```

- ACL içerisine uygulanması istenen kurallar tanımlandıktan sonra uygulanacak teknolojiye bağlı olarak uygulama komutu değişiklik gösteriyor.
    - Örnek olarak bir arayüzlere gelen her pakete uygulanması için kuralların uygulanacağı arayüze giriş yapılarak "**ip access-group <ACL Number> (in | out)**" komutuyla ACL'in numara bilgisini ve porta hangi yönde uygulanacağı belirtiliyor.

```
R1(config)#access-list 5 deny 10.0.0.0 0.0.0.255
R1(config)#int gi 0/0/0
R1(config-if)#ip access-group 5 out
R1(config-if)#exit
```

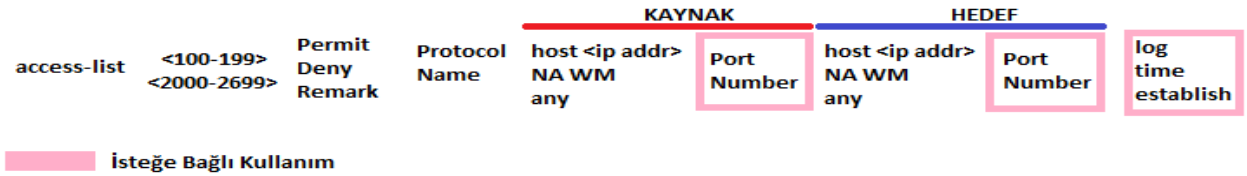
ACL'in router uygulandığı arayüz ve yön çok önemlidir. Eğer ki ACL doğru arayüze doğru yönde uygulanmazsa çoğu zaman hiçbir işe yaramaz. Hatta sorunlara neden olacaktır. Örnek olarak aşağıdaki görselde olduğu gibi, bir topolojide 192.168.10.0/24 networkünün 192.168.20.0/24 networküne erişminin engellenmesi istendiğinde "**access-list 10 deny 192.168.10.0 0.0.0.255**" kuralına sahip 10 numaralı bir ACL tanımlanıyor. Daha sonra kuralla eşleşmeyen paketlere izin verilmesi için (aksi taktirde "implicit deny" satırı uygulanır) "**access-list 10 permit any**" komutu eklenyor. Bu ACL R1 routerunda;

- Gi0/0 arayüzüne out yönünde uygulanırsa ACL işe yaramayacaktır (Bu arayüze kaynak ip adresi 192.168.10.0/24 networküne ait paketler gelmeyecektir).
- Gi0/0 arayüzüne in yönünde uygulanırsa 192.168.10.0/24 networkü hiçbir networke erişemeyecektir (Bu arayüzden çıkan paketlerin hepsinin kaynak ip adresi 192.168.10.0/24 olacağı için paketlerin hepsi drop edilecektir).
- Gi0/1 arayüzüne in uygulanırsa hiçbir işe yarmayacaktır (bu şekilde sadece kaynak ip adresi 192.168.20.0/24 networküne ait paketler gelecektir).
- Gi0/1 arayüzüne out yönünde uygulanırsa 192.168.10.0/24 networkü sadece 192.168.20.0/24 networküne erişemeyecektir. Yani dört olası durumdan sadece Gi0/1 arayüzüne out yönünde uygulandığında istenen durumu karşılamaktadır.



Extended ACL Konfigürasyonu

Extended ACL'ler kullanılarak ip ve port bazlı kısıtlamalar yapılabiliyor. Extended ACL konfigürasyonu için "**access-list <ACL Number> (deny | permit) <Protocol Name> <Src Ip Address> <Src Port No> <Dst Ip Address> <Dst Port No>**" komutu kullanılıyor. Kullanılan komutta ilk olarak bir ACL numarası belirtilir. Ardından kural kısıtı ve protokol adı (IP, ICMP, TCP, UDP ...) belirtilmek zorundadır. Son olarak kuralın uygulanacağı kaynak ve hedef ip adresleri belirtilir. Opsiyonel olarak ip adreslerinin hemen ardından kaynak ve hedef port bilgileri tanımlanabiliyor (port belirtilmezse "**any**" yani herhangi bir port olarak kabul edilecektir) (isteğe bağlı olarak komut sonunda "**log**", "**time**" veya "**establish**" gibi parametreler de kullanılabiliyor).



|→ Protocol Name kısmında "ip" kelimesinin kullanılması, kuralın 4. Katman protokolü (TCP, UDP, OSPF, ICMP ...) gözetmeksizin uygulanması demektir (yani "ip" kullanıldığında kullanılan port bilgisinin bir önemi kalmıyor).

İsteğe bağlı seçenekler;

- **log**, herhangi bir satırla eşleşen paket geldiğinde log tutar.
- **time**, ACL'in belirli zaman aralıklarında uygulanması istenebiliyor. ACL'in uygulanacağı zaman aralığı belirtilebiliyor.
- **established**, TCP bağlantılarında ACK bitlerinin set edilip edilmediğini kontrol eder. Bu sayede gönderilen trafiğin yeni bir oturum kurmak isteyip istemediği anlaşılır. Paket yeni bir oturum kurmak istiyorsa engellenir (ACL'in uygulandığı arayüzde ve yönde yeni bir oturum oluşturulamaz).
  |→ Yani eğer ki sadece SYN biti set edilmiş bir paket gelmişse bu paketin yeni bir oturum başlatmak istediğini gösterir. "established " kelimesi kullanıldığında ise paket tanımlı kuralla eşleşiyorsa yeni oturum kurmak istediğinden dolayı engellenir. **Bu sayede ACL'in tanımlandığı arayüz ve yönde sadece kurulu oturumlardan veri aktarımına izin verilir.**

```
RX(config)#access-list 160 permit tcp 10.0.0.0 0.0.0.255 any eq 80
RX(config)#access-list 160 permit tcp 10.0.0.0 0.0.0.255 any eq 443
RX(config)#access-list 160 permit udp 10.0.0.0 0.0.0.255 host 8.8.8.8 eq 53
RX(config)#int gi 0/0/0
RX(config-if)#ip access-group 160 in
RX(config-if)#exit
```

Port Belirtirken

- **eq (equal)**, sadece bir port belirtilirken kullanılıyor.
- **lt (less than)**, belirtilen port haricinde daha düşük port numaralarını temsil etmek için kullanılıyor.
- **gt (greater than)**, belirtilen port numarası haricide daha yüksek port numaralarını temsil etmek için kullanılıyor.
- **range**, iki port aralığı belirtilebiliyor.
- **neq (not equal)**, belitrilen port numarası dışındaki port numaralarını temsil etmek için kullanılıyor.

```
RX(config)#access-list 105 permit tcp any 10.0.2.15 0.0.0.0 ?
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  range        Match only packets in the range of port numbers
  <cr>
```

Standart veya Extended ACL tanımlamaları sayı yerine isim verilerek de tanımlanabiliyor. Bunun için öncelikle global konfigürasyon modunda "**ip access-list standart <ACL Name>**" veya "**ip access-list extended <ACL Name>**" komutuyla bir isim veriliyor. Bu komut sonrasında bir alt arayüze giriş yapılıyor ve burada doğrudan tanımlamak istenen satırlar ekleniyor. ACL oluşturulduktan sonra tanımlanan isim kullanılarak herhangi bir arayüze giriş veya çıkış yönünde uygulanabiliyor.

```
RX(config)#ip access-list standard NONAME
RX(config-std-nacl)#?
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
RX(config-std-nacl)#deny 192.168.10.0 0.0.0.255
RX(config-std-nacl)#permit any
RX(config-std-nacl)#exit
RX(config)#int gi 0/0/0
RX(config-if)#ip access-group NONAME out
RX(config-if)#exit
```

ACL Üzerinde Değişiklik Yapmak

Bir ACL oluşturulduktan sonra üzerinde düzenleme yapılmak istendiğinde, bu işlem iki farklı şekilde gerçekleştirilebiliyor.

1- İlk olarak "**sh run**" komutuyla tanımlı ACL'in bir kopyası alınarak text editörüne yapıştırılır. Ardından "**no access-list <ACL Number or Name>**" komutuyla tanımlanan ACL routerdan kaldırılır. Text editörüne kopyalanan ACL sarılarında istenen değişiklikler yapıldıktan sonra ACL routerda yeniden oluşturulur.

```
RX(config)#no access-list 10
RX(config)#access-list 10 deny host 10.0.0.5
RX(config)#access-list 10 deny host 10.0.2.15
RX(config)#access-list 10 permit any
```

2- ACL'lerde tanımlı her satıra bir sıra numarası verilir ("**sh access-list**" komutuyla verilen sıra numaraları görülebilir). Bu sıra numaralar kullanılarak tanımlı satırlar değiştirilebilirken aynı zamanda satır aralarına yeni kurallar eklenip çıkartılabiliyor. Bunun için isimli ACL tanımlamasında olduğu gibi "**ip access-list standart <ACL Number or Name>**" komutuyla tanımlı ACL altına girilerek başında tanımlı satır numarası olacak şekilde yeni kurallar eklenebiliyor.

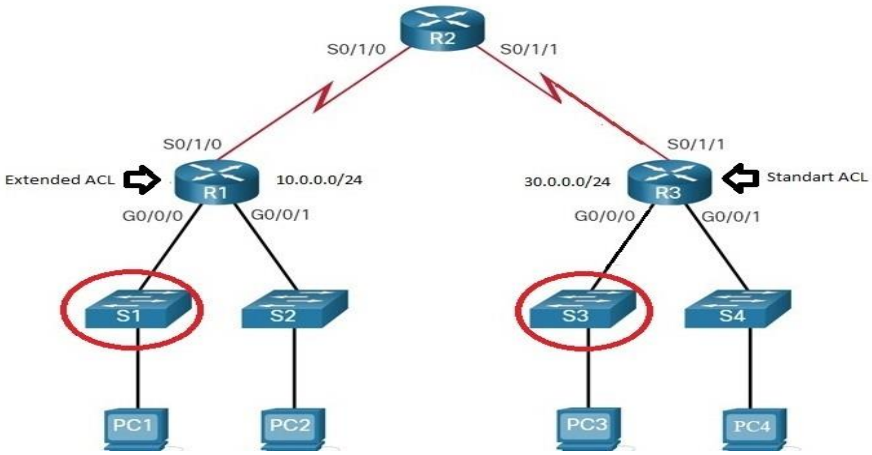
```
RX(config)#do sh access-list
Standard IP access list 10
    10 deny host 10.0.0.1
    20 deny host 10.0.2.15
    30 permit any

RX(config)#ip access-list standard 10
RX(config-std-nacl)#15 deny host 192.168.1.5
RX(config-std-nacl)#do sh access-list
Standard IP access list 10
    10 deny host 10.0.0.1
    15 deny host 192.168.1.5
    20 deny host 10.0.2.15
    30 permit any

RX(config-std-nacl)#
```

ACL'ler L3 switchlerde VLAN'lere ip adresleri atandığında bütün VLAN'lar aralarında haberleşebiliyordu. ACL'ler (Standar veya Extended) kullanılarak hangi VLAN'ların aralarında haberleşebileceğini belirlemek için de kullanılıyor. Tanımlanan ACL'ler VLAN arayüzlerine uygulanarak istenilen VLAN trafiği filtrelenebiliyor (**ACL tanımlarında "implicit deny" satırını unutma – VLAN portlarında uygulanan yönlere dikkat et**).

```
L3SWX(config)#access-list 50 permit 10.0.0.0 0.0.0.255
L3SWX(config)#access-list 50 permit 20.0.0.0 0.0.0.255
L3SWX(config)#interface vlan 10
L3SWX(config-if)#ip access-group 50 in
L3SWX(config-if)#exit
```

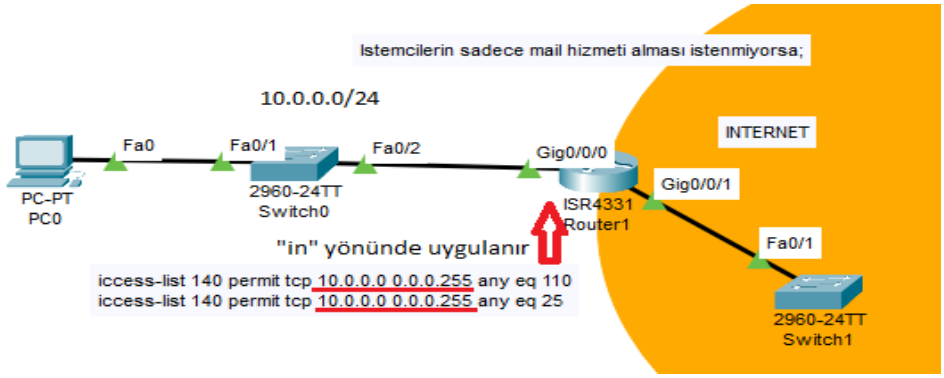
NOT:

- ACL'lerde kurallar satır satır kontrol edildiği için genelde daha fazla cihazı kapsayan kurallar üst satırlara yazılmaya çalışılır. Bu sayede ACL uygulanırken alt satırlara kadar tek tek gezmek yerine üst kısımlarda tanımlı kurallarla eşleşeceği için daha az gecikmeye neden olacaktır.
- ACL kaynağa en yakın konumda tanımlanmaya çalışılır. Örnek olarak 10.0.0.0/24 networkünün 30.0.0.0/24 networküne erişimini engelleyebilmek için uygulanabilecek iki seçenek bulunuyor.
  1- R1 G0/0/0 arayüzüne hedef netowork adresi 30.0.0.0/24 paketlere engel koyulabilir. Bu durumda Extended ACL tanımlaması gerekiyor (Bu ACL R2 veya R3'e de uygulanabilir ama bu durumda paket R1'den R2'ye veya R3'e gereksiz yere gönderilecek ve gereksiz yere bant genişliği kullanılacaktır).
  2- R3 G0/0/0 arayüzüne kaynak network adresi 10.0.0.0/24 paketlere engel koyulabilir. Bunun için Standart veya Extended ACL kullanılabilir.



- Tanımlamalarda tek bir ip adres ifadesi "10.0.0.1 0.0.0.0" veya "host 10.0.0.1" olmak üzere iki farklı şekilde yapılabiliyor.
- Tanımlamalarda herhangi bir ip adres ifadesi "50.0.0.1 255.255.255.255" veya "any" olmak üzere iki farklı şekilde temsil edilebiliyor.
- **ACL tanımlamalarında satır sonunda kurallarla uyuşmayan bütün paketlere izin verilmek isteniyorsa "access-list <1-99> permit any" veya "access-list <100-199> permit ip any any" komutunun eklenmesi gerekiyor. Aksi taktirde hiçbir satırla uyuşmayan paketler "implicit deny" satırıyla eşleştirilecek ve paketler drop edilecektir.**

- Routerlarda “**sh access-list**” komutunun çıktısında tanımlı kural satırlarıyla berabe satır sonrarında “**<number> matches**” gibi bir bilgi daha bulunmaktadır. Bu bilgi routera gelen paketlerden kaç paketin tanımlı satıra eşleştiğini göstermektedir. Bu bilgi “**clear access-list counters**” komutuyla sıfırlanabilmektedir.
- Extended ACL tanımlarken networkten çıkan paketler için kural yazılırken kaynak ip adresi kısmında “any” kullanmak yerine bir network ip adresini verilmesi network içerisinde ip spoofing saldırılarının önüne geçecektir. Yani ACL‘de kaynak ip belirli bir network adresi olduğunda istemciler farklı ip adresleri kullanarak ACL’den geçemezler.



- ACL tanımlamalarında bir servise kısıtlama yazılmak isteniyorsa yazılan satırla eşleşmeyen paketlerin “**imlicit deny**” satırıyla eşleşmemesi için genel izin kuralı ekleniyor. Tanımlanan genel izin kuralının istenen kısıtlamayı atlatmaması için ayrıca engellenecek aralığın da belirtilmesi gerekiyor.
  |→ Örnek olarak bir 192.168.100.5 adresine sadece 192.168.40.0/24 networkündeki istemcilerin SSH yapması isteniyorsa öncelikle bu network için izin kuralı tanımlanıyor. Ardından farklı networkteki istemcilerin 192.168.100.5 adresine SSH yapamaması için engel kuralı ekleniyor (Bu sayede sadece belirtilen networke SSH izni veriliyor). Son satırda ise SSH dışında hizmetlerin kullanılabilemsi için bütün trafiğe izin veriliyor.

```
access-list 155 permit tcp 192.168.40.0  0.0.0.255 host 192.168.100.5 eq 22
access-list 155 deny tcp any host 192.168.100.5 eq 22
access-list 155 permit ip any any
```

- Bir routera veya switche Telnet veya SSH yapılmasına kısıt koyulmak isteniyorsa tanımlanacak ACL’ler (Standart ACL ile kaynak ip verilmesi yeterli oluyor) line vty arayüzlerine “**access-class**” komutuyla uygulanıyor. Nedeni router veya switchin portlarına uygulanan ACL’ler portlardan/arayüzlerden geçen bütün trafiğe uygulanıyor. ACL’deki satırların sayısı arttıkça da cihalar üzerinden geçen trafik gereksiz yere kontrol edilecektir. “line vty” arayüzüne tanımlanan ACL’ler sadece cihaza Telnet veya SSH yapılılacak trafiği kontrol ediyor.
  |→ Yeni bir istemcinin veya networkün routera SSH/Telnet yapması isteniyorsa ACL’e bir satır daha eklemek yeterli olacaktır.

```
RX(config)#access-list 50 permit host 192.168.10.1
RX(config)#line vty 0 15
RX(config-line)#access-class 50 in
RX(config-line)#exit
```

  |→ Bunun gibi cihaz üzerinde daha birçok noktaya tanımlanan ACL’ler uygulanarak trafikler filtrelenebiliyor.

Kontrol Komutları

- sh access-lists