Liste de control al accesului (ACL)

În această temă se învață următoarele:

Ce sunt **Access Control Lists**?

Când se folosesc Access Control Lists?

Tipuri de Access Control Lists

Implementarea ACLs pe interfețele unui ruter

Exemple de ACLuri

Ce sunt Access Control Lists?

Listele de control al traficului sunt un set de condiții specificate de administrator pentru identificarea unor anumite tipuri de trafic. Traficul identificat poate fi **filtrat, controlat, asociat cu alte acțiuni** sau **altera**t. Există mai multe criterii de identificare atraficului:

- După adresa IP: -Adresa sursă sau adresa destinație
- După protocol: - IPv4, IPv6, IPX, AppleTalk
  -TCP, UDP
  - ICMP
- După port sau tip
  - Port sursă sau port destinație
  -Tip de mesaj ICMP

ACLs sunt filtre de rețea folosite de rutere şi de unele switchuri pentru a controla (a permite sau a restricționa) accesul fluxurilor de date pe interfețele de rețea. Un ACL conține reguli pentru controlul accesului.

Fiecare regulă:

- Identifică diferite tipuri de trafic pe baza unor criterii
- Specifică acțiunea ce trebuie făcută în cazul îndeplinirii criteriului (există potrivire):
  - Permite traficul: ***permit***
  - Refuză traficul: ***deny***

Atunci când se configurează un ACL pe o interfață, echipamentul de rețea analizează datele ce urmează a trece pe acea interfață, le compară cu criteriile de trecere stabilite pe acea interfață şi permite sau nu trecerea lor. Parcurgerea unei liste se face secvențial, de sus în jos, până se

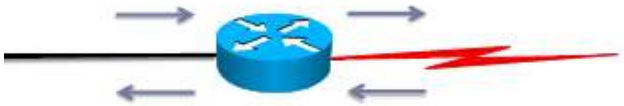
găseşte o regulă care se potriveşte (match) şi se aplică acţiunea, iar restul ACL-ului nu se mai verifică. Dacă nu se găseşte nicio potrivire, se parcurge lista până la sfârşit unde se găseşte un ***deny any*** implicit.

ACL-urile de filtrare se pot aplica:

- Pentru fiecare protocol de nivel 3 (IP, IPv6 etc.)
- Pentru fiecare interfață
- Pentru fiecare directie

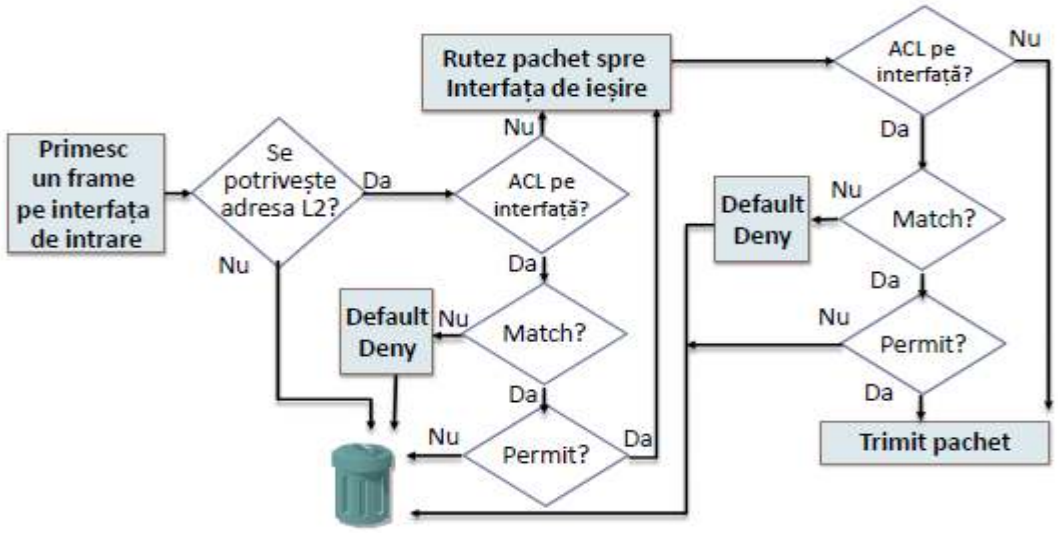
  Inbound pentru traficul de intrere
  Outband pentru traficul de ieşire

De exemplu pentru un ruter cu două interfețe pe care rulează stiva dual IP şi IPv6 pot fi aplicate maximum 2 (interfete)x2(protocoale)x2(in si out)=liste.



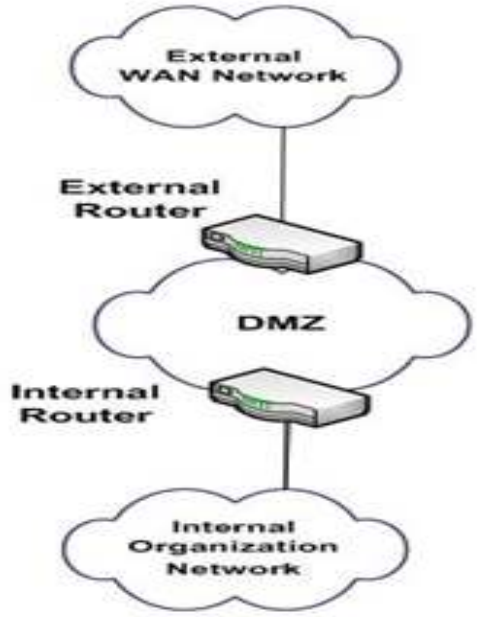
Există o multitudine de motive pentru care se folosesc ACL-urile. Un prim motiv este că ACL asigură un prim nivel de securitate pentru datele din rețea. Desigur, nu este la fel de profund ca un firewall, dar poate produce o protecție pe interfețele spre linii de mare viteză, acolo unde un firewall poate fi restrictiv. De asemeni, ACL pot fi folosite pentru a restricționa actualizările de rutare între entitățile pereche şi poate fi un bun instrument de control al fluxului în rețea.

Funcționarea ACL-urilor se poate vedea în fig. următoare.



Când se folosesc Access Control Lists?

Deşi nu sunt la fel de performante ca firewall-urile, pot oferi multe capabilități asemănătoare acestora. ACL-urile pot fi folosite pe interfețele externe ale unei rețele pentru a filtra traficul şi a restricționa protocoalele care se cunosc a fi surse de vulnerabilitate. Una dintre cele mai cunoscute metode de securizare a unei rețele este configurarea unei "zone demilitarizate", DMZ. Această arhitectură este implementată cu două dispositive de rețea separate. Un astfel de exemplu este infigura de mai jos.



Ruterul exterior asigură toate conexiunile din afara rețelei. ACL-urile setate pe acesta vor permite doar accesul protocoalelor absolute necesare şi le va bloc pe celelelte. Ceeace estefoarte important şi util în acelaşi timp, este că regulile de acces pe interfețele ruterului se pot configure independent pe sensurile de intrare si de ieşire din rețea.

În DMZ se plasează acele sisteme care au nevoie să cominice în mod current în Internet, cele mai cunoscute fiind serverele web, serverele DNS si sistemele acces VPN.

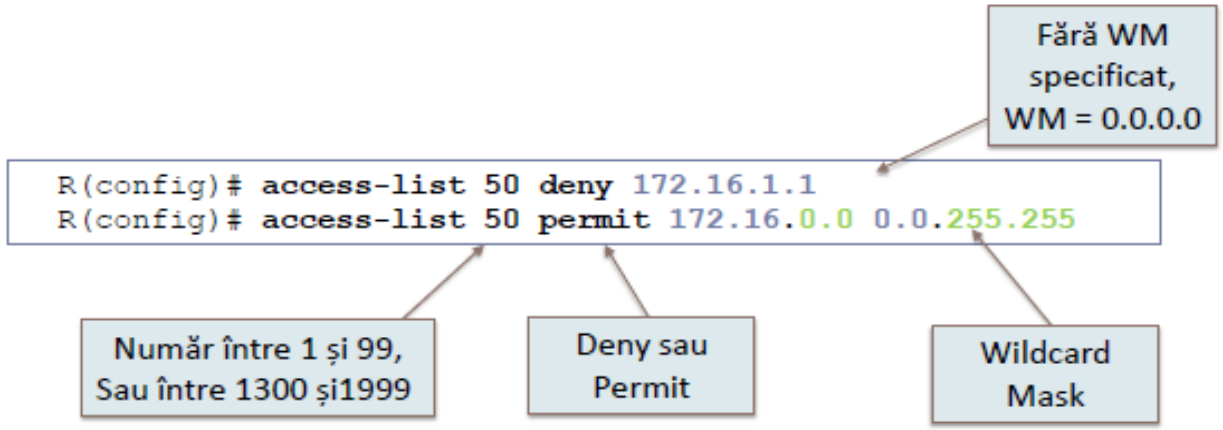
Ruterul intern al unui DMZ poate conține ACL-uri mult mai restrictive, destinate protecției rețelei interne contra amenințărilor posibile. ACL-urile pot tine seama de adrese IP, de protocoale de aplicații, de protocoale de comunicare etc.

Tipuri de Access Control Lists

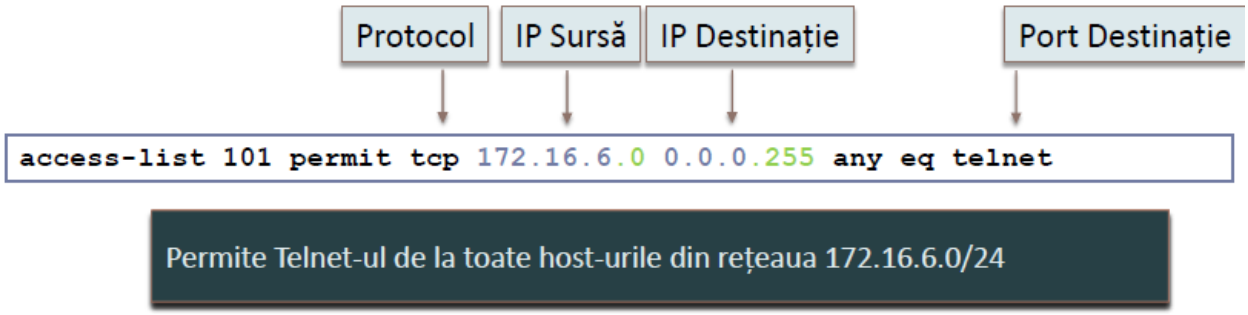
Există mai multe tipuri de ACL-uri şi cele mai multe sunt definite pentru scopuri distinct sau protocoale distincte. Pe rutere Cisco există două tipuri principale: standard si extinse. Se pot define şi liste de control avansate, cum ar fi cele de tip reflexive şi de tip avansat.

ACL clasice sunt la rândul lor de două tipuri: **standard** sau **extinse**, identificate astfel după numărul (ID-ul) listei.

ACL standard au numere de identificare între 1şi 99 pentru IOS-urile mai vechi sau între 1300 şi 1999 pentru IOS-uri mai noi. Ele **filtrează pachetele doar în funcție de sursă**. Forma uneiasemenealisteesteurmătoarea:



ACL extinse sunt identificate prin numere între **100 şi 199** sau între **2000 şi 2699** pentru IOS-uri mai noi. Ele pot filtra traficul **atât după sursă şi destinație**, cât şi după **protocol şi port**. Forma unei liste extinse este următoarea:



ACL-uri cu nume folosesc nume în loc de numere pentru a le identifica, numele fiind mai sugesive decât numerele pentru ceea ce fac ele. Este posibilă şi numerotarea regulilor care sunt afdăugate, modificarea şi completarea lor fără a şterge complet lista.

- •Pot fi fie **standard**, fie **extinse**
- •Oferă **flexibilitate mai mare** decât listele standard sau extinse
- •Recomandate să fie folosite fa□ă de cele cu număr

Câteva exemple sunt în figura următoare.

```
R(config)#ip access-list extended FILTER_LAN_IN
R(config-ext-nacl)#20 permit ip any any
```

Dacă am uitat 2 reguli ce trebuiau definite înainte..

```
R(config-ext-nacl)#5 permit icmp host 10.0.0.0 any
R(config-ext-nacl)#10 deny icmp any any
```

Dacă am greșit regula de pe linia 5...

```
R config-ext-nacl)#no 5
R config-ext-nacl)#5 permit icmp host 10.0.0.1 any
```

După definire, pot aplica ACL-ul pe interfață

```
R(config)#interface fastEthernet 0/1
R(config-if)#ip access-group FILTER_LAN_IN in
```

În editarea ACL-urilor se pot introduce remarci care să le facă mai explicite. Un comentariu poate avea maximum 100 de caractere. De exemplu, explicarea faptului că este permis traficul către rețeaua A şi este respinstraficul spre rețeaua B se poate scrie astfel:

```
R(config)# access-list 50 remark permit traficul spre A
R(config)# access-list 50 permit 172.16.0.0 0.0.255.255
R(config)# access-list 50 remark opresc traficul spre B
R(config)# access-list 50 deny 192.168.10.15
```

Implementarea ACLs pe interfețele unui ruter

Pe interfețele unui ruter traficul este bilateral (traffic de intrare şi traffic de ieşire), aşa cum se poate vedea în fig următoare.

```
R(config)# interface fastethernet 0/0
R(config-if)# ip access-group ?
<1-199>      IP access list (standard or extended)
<1300-2699>  IP expanded access list (standard or extended)
WORD         Access-list name
R(config-if)#ip access-group 10 ?
in   inbound packets
out  outbound packets
```

Notă 1. În configurarea unui ACL pe un ruter, adresa IP trebuie însoțită de wildcard mask. Un wildcard mask este este o mască ce se suprapune peste o adresă IP şi prin care se poate identifica partea comună a unor adrese. Este reprezentată pe 32 de biți, biții 0 făcînd match, iar biții 1 ignoră partea respectivă din adresa IP. Poate fi privită ca inversul măştii de rețea obişnuite. În exemplul următor, ruterul va verifica doar primii 16 biți din adresele IP şi îi va compara cu cei din adresa IP. Această declara□ie va permite traficul având ca sursă 172.16.*.*
Biții de 0–fac match

Biții de 1–sunt ignorați

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.255.255
```

Notă 2. În ACL se pot folosi două cuvinte cheie:

any–înseamnă adresa IP0.0.0.0şi WM 255.255.255.255, toate IP-urile vor face match
host–testează egalitatea cu o adresă de host, echivalent cu WM 0.0.0.0

Verificareaconținutului ACL-urilorşi**poziționarealorpeinterfețe** se poate face cu comenzile:

Comanda	Descriere
`show ip interface`	Informații privind numărul de ACL-uri de intrare și ieșire
`show access-list`	Afișează conținutul ACL-urilor configurate pe router
`show running-config`	Afișează, printre altele, poziționarea și conținutul ACL-urilor configurate

Exemple de ACLuri

1. ***O listă de acces care să permit doar traficul de la staţia 193.230.2.1*** poate fi astfel:

```
R(config)# access-list 1 permit host 193.230.2.1
           sau
R(config)# access-list 2 permit 193.230.2.1 0.0.0.0
           sau
R(config)# access-list 3 permit 193.230.2.1
```

   Sau folosind un ACL extins

```
R(config)# access-list 101 permit ip host 193.230.2.1 any
```

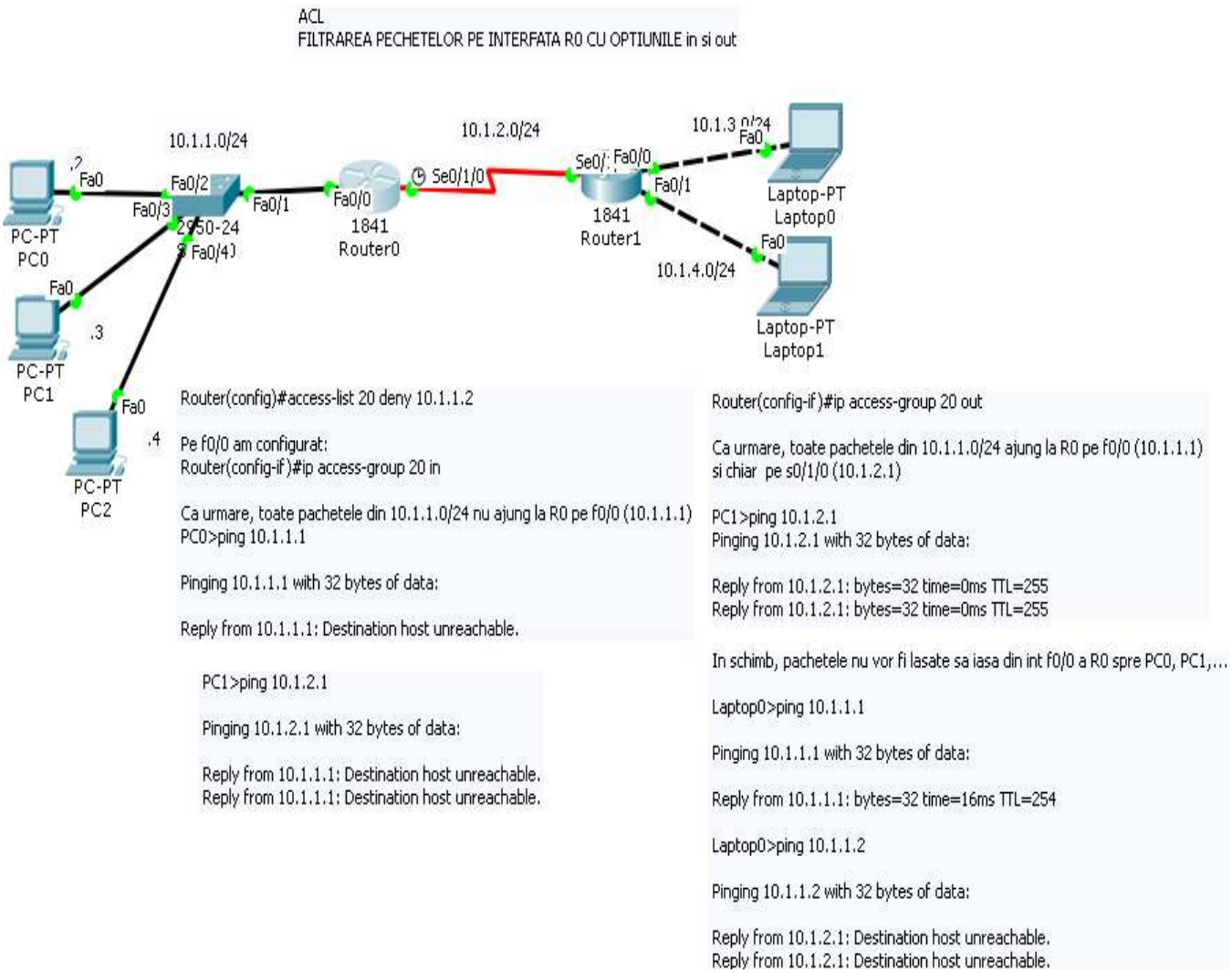
2. ***Construirea şi aplicarea pe interfaţa Ethernet 1 a unei liste care să permit doar traficul de la adresele 11.2.2.90 şi 11.2.2.91*** arată astfel:

```
R(config)# acces-list 18 permit host 11.2.2.90
R(config)# acces-list 18 permit host 11.2.2.91
           sau
R(config)# acces-list 18 permit 11.2.2.90 0.0.0.1



R(config)# interface ethernet 1
R(config-if)# ip acces-group 18 in
```

3. Care este efectul aplicării următoareil iste de acces:

```
R(config)# acces-list 18 permit host 11.2.2.90
R(config)# acces-list 18 permit host 11.2.2.91
          sau
R(config)# acces-list 18 permit 11.2.2.90 0.0.0.1


R(config)# interface ethernet 1
R(config-if)# ip acces-group 18 in
```

4. Fig 3. Exemplu de configurare ACL pe rutere



Sumar

Listele de control al accesului sunt un element important de securitate în rețelele de calculatoare şi înțelegerea funcționării lor şi a poziționării corecte sunt esențiale în protejarea eficientă a traficului. ACL-urile se configurează pe ruter şi se aplică pe interfețe specificând atât acțiunea, cât şi sensul de aplicare.