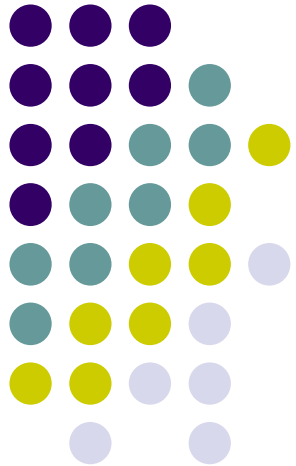
UNIVERSITETI AAB



Lënda: Rrjetat TCP/IP

Ligjerata 7

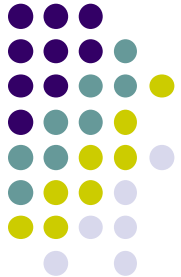
Profesori: Dr.sc. Arianit Maraj

2015

Temat

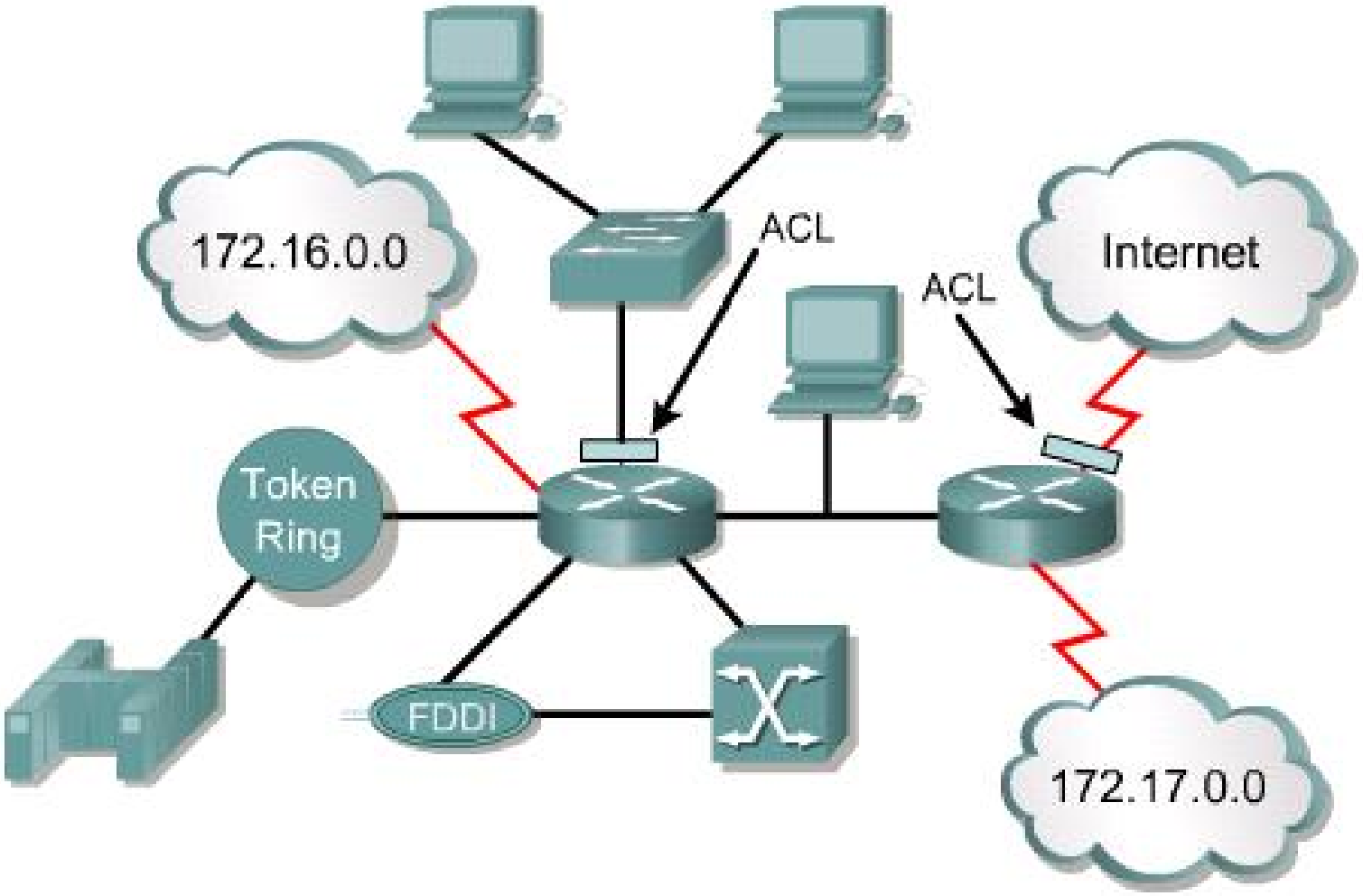
- Konceptet kryesore te ACL-ve
- Llojet e ACL-ve dhe krijimi i tyre
- Komandat kryesore për krijimin e ACL-ve standarde dhe atyre te zgjeruara
- Vendosja e ACL-ve ne interfejs

Çka janë listat kontrolluese te qasjes (ACL-Access Control Lists)



- ACL-te janë lista qe përmbajnë kushte te cilat aplikohen për trafikun qe transmetohet neper interfejsat e rutereve.
- Këto lista u tregojnë rutereve se cfare lloje te paketave te pranohen e c'fare te refuzohen.
- Pranimi dhe refuzimi i paketave mund te bazohet ne kushte te caktuara.
- ACL-te mundësojnë menaxhimin e trafikut dhe siguri ne qasje prej dhe nga një rrjet i caktuar.

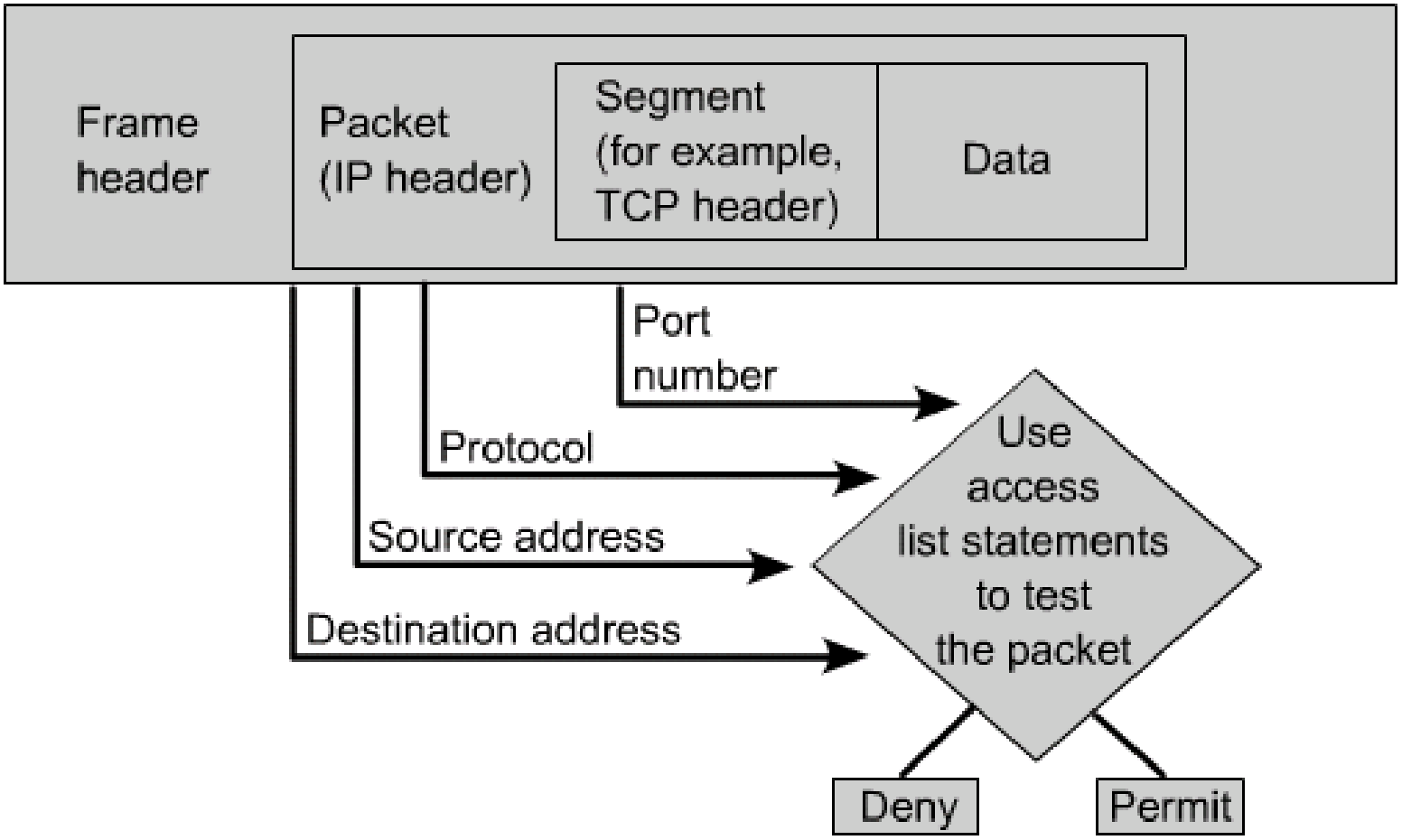
ACL-te, rrjeti ku mund te vendosen



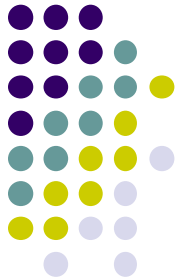
ACL – definicione te pergjithshme

- ACL-te mund te krijohen për te gjitha llojet e protokolleve, siç është IP dhe IPX (internetwork Packet Exchange).
- ACL-te duhet te definohen per-protokoll, per drejtim ose për një port te caktuar.
- ACL-te kontrollojnë trafikun ne një drejtim ne një interfejs te caktuar.
- Nevojitet te krijohen ACL te ndryshme për secilin drejtim, një për trafikun ne ardhje dhe një për trafikun ne shkuarje.
- Ne fund, secili interfejs mund te ketë shume protokolle dhe shume drejtime te definuara.

ACL – definicione te pergjithshme

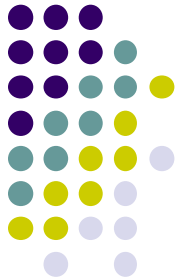


Arsyet per krijimin e ACL-ve



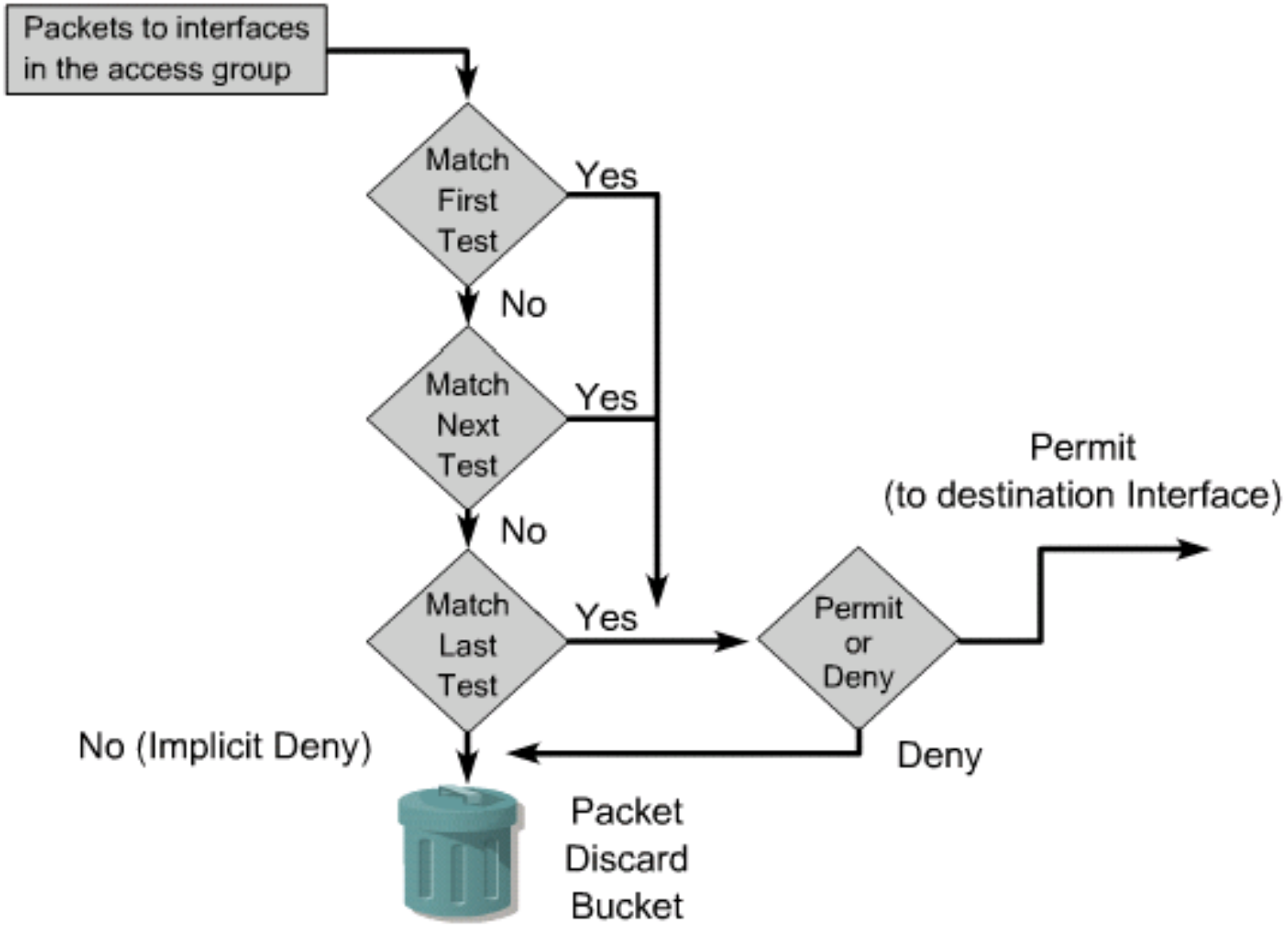
- Me poshte jane disa nga arsyet pse duhet te krijohen ACL-te:
  - Limitojne trafikun ne rrjet dhe rrisin performancen e rrjetit
  - Ofrojne kontrolle te trafikut. ACL-te mund te limitojne shperndarjen e perditesimeve te rutitmi (routing updates)
  - Ofrojne nivel bazik te sigurise ne rrjet
  - Vendosin se cili lloj I trafikut duhet te riorientohet ose te bllokohet ne interfejsin e ruterit
  - Lejojne nje administrator qe te kontrolloje se ku mund te kene qasje kliente te ndryshem

Si funksionojne ACL-te?



- Nje ACL eshte nje grup i deklarateve (statements) qe definojne nese paketat duhet te pranohen apo te refuzohen ne nje interfejs
- Keto vendime behen duke e bere pershtatjen e gjendjes se deklarates ne nje ACL dhe mandej duke e ekzekutuar aksionin e definuar ne deklarate
- Renditja e deklarateve ne ACL eshte shume e rendesishme

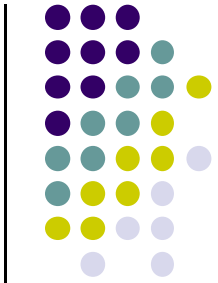
Algoritmi i funksionimit te ACL-ve



Deklaratat e ACL-ve

- "*Deklaratat" e ACL-ve* janë në esencë filtrues të paketave që veprojnë në përputhje me rrethanat e ndryshme.
- Njëherë kur të krijohen ACL-të, ato mund të zbatohen në trafikun e brendshëm ose në atë të jashtëm të ndonjë interfejsi (ndërfaqeje).
- Gjatë aplikimit të ACL-ve, ruteri "obligohet" që të bëjë një analizë të të gjitha paketave që udhëtojnë në rrjet në drejtime të ndryshme.
- Po ashtu, ruteri "detyrohet" që të marrë vendime të duhura për riorientimin e paketave, bazuar në konfigurimet përkatëse të ACL-ve.

Rregullat qe paketat iu nenshtrohen gjate krahasimit te ACL-ve

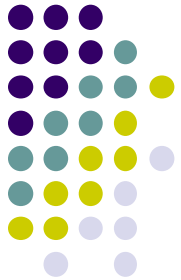


- Më poshtë janë dhënë disa rregulla të rëndësishme që paketat iu nënshtrohen, gjatë krahasimit me ACL:
- Paketat gjithmonë krahasohen me secilin rresht të Access Lista-ve në mënyre sekuenciale, çka do të thotë se ato gjithmonë fillojnë të krahasohen me rreshtin e parë të Access listës, pastaj me rreshtin e dytë, të tretë e kështu me radhë.
- Paketat krahasohen me rreshtat e Access listës vetëm deri sa të bëhet ndonjë ndërprerje. Kur paketa takohet me kushtin që caktohet nga Access lista, atëherë nuk do të bëhen krahasime të mëtejshme.

Llojet e ACL-ve

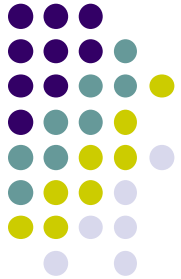
- **Ekzistojnë dy lloje kryesore të Access listave:**
  - **Listat Standarde të qasjes (Standard Access Control Lists)**
  - **Listat e Zgjeruara të qasjes (Extended access control lists)**

Listat Standarde të qasjes (Standard Access Control Lists)



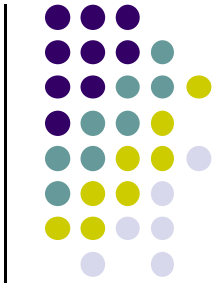
- Këto lloje të ACL-ve përdorin vetëm IP adresa të burimit në IP paketa, si kusht për testim.
- Të gjitha vendimet merren duke u bazuar në IP adresa të burimit.
- Kjo do të thotë që Standard Access Listat-t në parim i lejojnë apo i ndalojnë një bashkësi protokollesh të ndryshme.

Listat e Zgjeruara të qasjes (Extended access control lists)



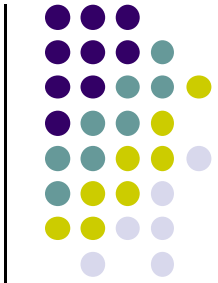
- Listat e zgjeruara ACL mund të përcaktojnë shumë fusha të tjera në shtresën e 3-të dhe në “header-et” e shtresës së 4-te të IP paketave.
- Këto lista mund të përcaktojnë po ashtu burimin dhe destinacionin e IP adresave,fushën e protokollit në ballinën e shtresës së rrjetit dhe numrin e portit në ballinën e shtresës së transportit.
- Kjo iu jep këtyre listave aftësi për të marrë vendime shumë më të detajuara gjatë kontrollimit dhe filtrimit të trafikut në rrjet

ACL-të e emërtuara (Named Access Lists)



- Më lartë u cek se ekzistojnë vetëm dy lloje të Access listave, mirëpo tani po e paraqesim edhe një tjetër!
- Në fakt këto Lista nuk janë ndonjë lloj i ri i ACL-listave,mirëpo ky lloj i tyre bën pjesë ose në Standard ose në Extended Access Lists.
- Këto lloje të listave janë krijuar dhe referuar ndryshe nga Standard dhe Extended listat, por për nga funksioni janë të njëjta.

Llojet e ACL-ve



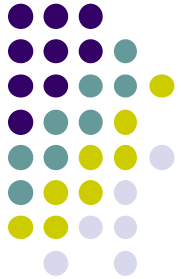
- <1-99> IP Access listë standarde
- <100-199> IP Access listë e zgjeruar
- <1100-1199> ACL bazuar në MAC adresa 48 bit të zgjeruara
- <1300-1999> IP Access liste standarde (rang i zgjeruar)
- <200-299> ACL e tipit protokoll
- <2000-2699> IP Access listë e zgjeruar (rang i zgjeruar)
- <700-799> ACL e bazuar në MAC adresa 48 bit

Aplikimi i ACL-ve ne interfejs

- Duhet të specifikojmë saktë se në cilin drejtim dëshirojmë t'i aplikojmë.
- Me specifikimin e drejtimit të trafikut do te na nevojitet të përdornim Access lista të ndryshme për trafik:
  - të brendshëm (inbound) dhe
  - të jashtëm (outbound)

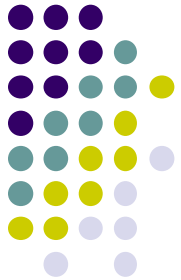
në një interfejs të vetëm

Filtrimi i Trafikut përmes ACL-ve (Traffic Filtering)



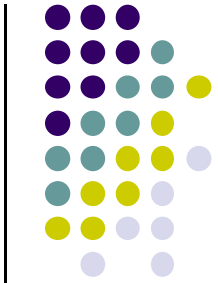
- Filtrimi i paketave mund të jetë i thjeshtë apo i ndërlikuar, ndalimi apo lejimi i trafikut bazohet në:
  - IP Adresën e burimit
  - IP Adresën e destinacionit
  - MAC Adresën (adresën fizike)
  - Protokolle dhe
  - Lloje të aplikacioneve

Procesi i konfigurimit të ACL-ve



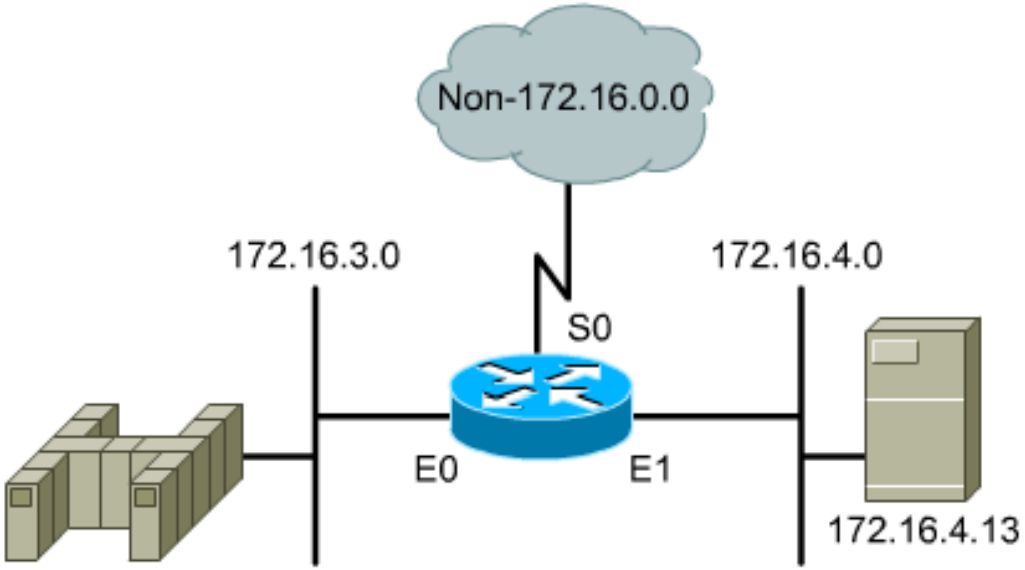
- Krijimi i ACL-ve bëhet duke e shkruar formën e përgjithshëm të konfigurimit.
- Duke e përdorur komandën e ACL-ve, shkruhet edhe deklarata e tyre.
- Sintaksa për deklaratat e ACL-ve standarde është:
  - *access-list [access-list-number]*
  - *[deny|permit] [source address]*
  - *[source-wildcard][log]*

Sintaksa per krijimin e ACL-ve standarde



- Të shohim një sintaksë që e përdorim gjatë krijimit të ACL-ve Standarde:
  - *deny* Refuzimi i paketave specifike
  - *permit* Përcjellja e paketave specifike
  - *remark* Komenti në fillim të ACL-ve

Krijimi i nje ACL-je standarde



Command Output

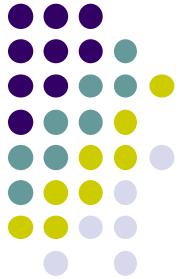
```
access-list 1 permit 172.16.0.0  0.0.255.255


interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

ACL-te e zgjeruara

- ACL-të janë të dizajnuara të filtrojnë trafikun që kalon përmes routerit.
- **IP ACL-të e zgjeruara (Extended) duhet të vendosën sa më afër burimit që është e mundshme.**
- Meqenëse ACL-të e zgjeruara mund të filtrojnë më shumë adresa dhe protokolle specifike, atëherë ne nuk dëshirojmë që trafiku të kaloj nëpër gjithë rrjetin dhe në fund të ndërpritet.
- Me vendosjen e këtyre listave sa me afër burimit të adresave, mund të bëhet filtrimi i trafikut para se ta përdorim bandwith-in e “çmuar”.

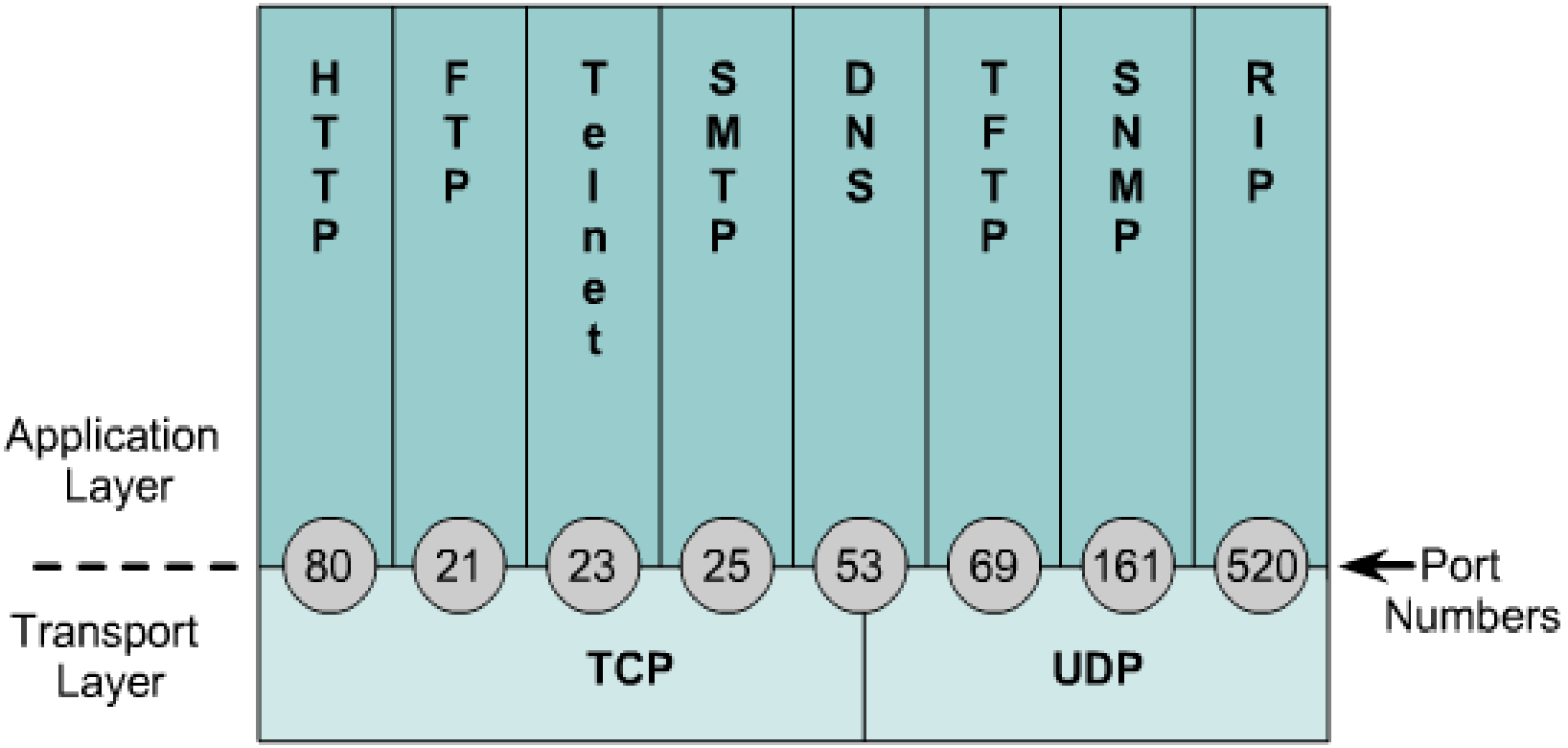
Krijimi i nje ACL-je te zgjeruar



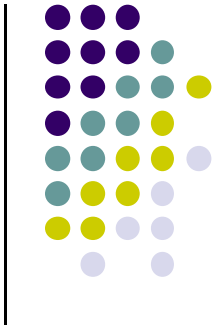
```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

Krijimi i ACL-ve te zgjeruara
Numri i ACL-ve te zgjeruara; rangu 100 - 199
Numri i protokollit i nivelit te 4-te modelit OSI
IP adresa e burimit dhe destinacionit
Aplikimi ne portin qe është me afër burimit

Transport – portet e shtreses se aplikacionit

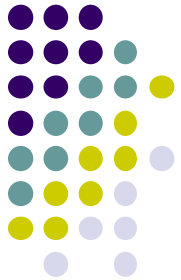


Maska “Wildcard



- Wildcard maska është një ‘maskë’ që tregon se cila pjesë e IP adresave është e gatshme për shqyrtim.
- Ato e tregojnë madhësinë e rrjetit apo subnet-it për disa protokolle të rutimit , si për shembull OSPF.
- Po ashtu, Wildcard maska shërben për të treguar se çfarë IP adresave lejohen apo jo në ACL, gjatë filtrimit të trafikut.

Përcaktim i WildCard Maskës për rrjete të ndryshme



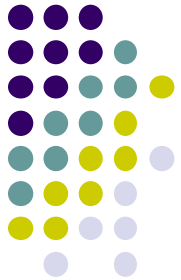
Wildcard maska e cila e lejon vetëm një host të vetëm:
172.16.22.87 0.0.0.0
Host 172.22.8.17

Wildcard maska e cila e lejon rangun e hosteve për rrjetin /24
172.16.22.0 0.0.0.255

Wildcard maska e cila lejon rrjetin hyrës /16:
172.16.0.0 0.0.255.255

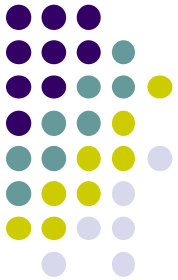
Wildcard maska e cila lejon rrjetin hyrës /8:
10.0.0.0 0.255.255.255

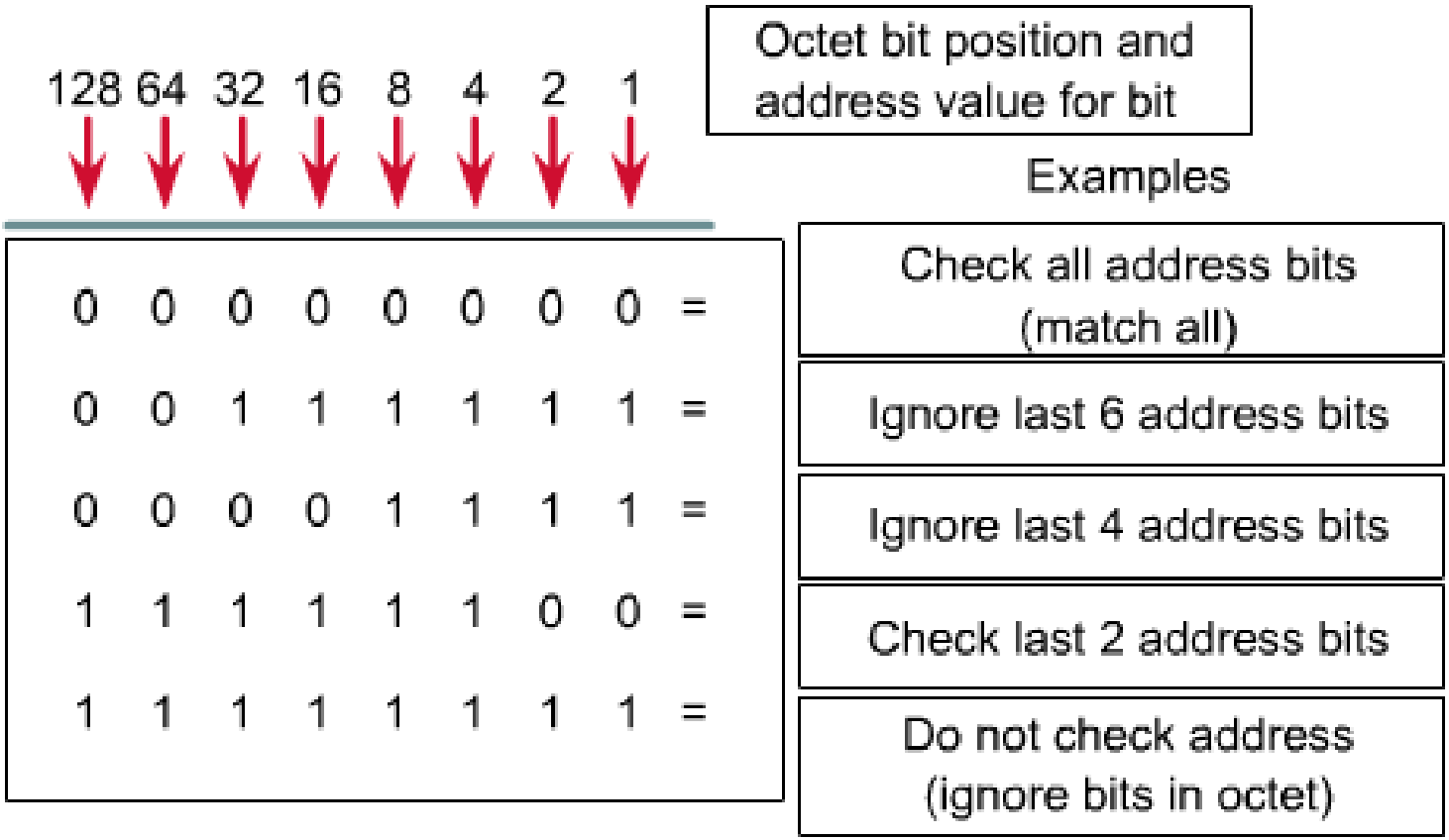
Shembull i perdorimit te WildcardMask ne ACL



- Me poshtë është dhënë një shembull, ku ‘urdhri’ i dhënë në ACL i lejon të gjitha hostet nga 192.168.1.0 dhe i bllokon të tjerët:
  - *access-list 1 permit 192.168.1.0* ***0.0.0.255***
- Te ky shembull, wildcard maska tregon se vetëm tri oktetet e para duhet të përputhen.
- Kështu, nëse 24 bitat e parë të paketës hyrëse përputhen me 24 bitat *e fushës se krahasimit*, atëherë paketa lejohet të udhëtojë nëpër rrjet.

Bitet ne Wildcard Mask (1)





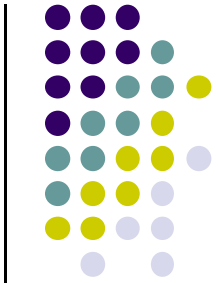
Struktura e një WildCard Maske

	Ekuivalenti Decimal	*Ekuivalenti Binar*
Krahasimi i Adresave	192.168.1.0	**11000000.10101000.00000001.00000000**
Wildcard Maska:	0.0.0.255	00000000.00000000.00000000.11111111
Krahasimi i bitave që përputhen	192.168.1.X	11000000.10101000.00000001.xxxxxxxx
Adresa e paketave që hyjnë në rrjet	192.168.1.27	11000000.10101000.00000001.00011011

Problemi i vendosjes së ACL-ve

- Eshtë shumë me rëndësi që ato të aplikohen në ruterin e duhur apo interfejsin e tij dhe në drejtim të duhur.
- Konfigurimi i saktë i ACL-ve, mirëpo aplikimi jo me vend i tyre është një nga gabimet më të shpeshta gjatë krijimit të tyre.
- ACL-të Standarde filtrojnë trafik vetëm në IP Adresat e burimit, kështu që vendosja e tyre duhet bërë sa me afër destinacionit.

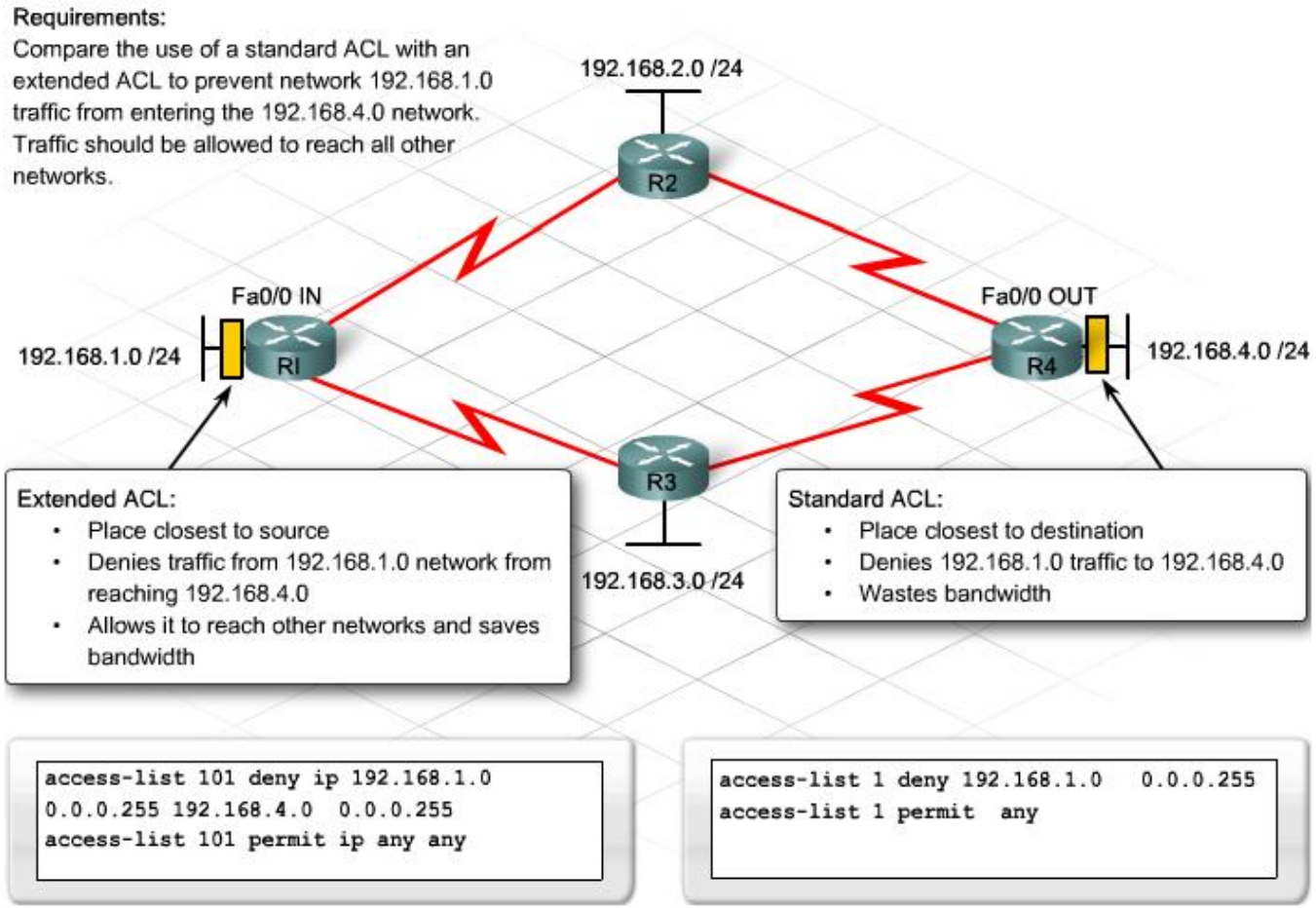
Problemi i vendosjes së ACL-ve



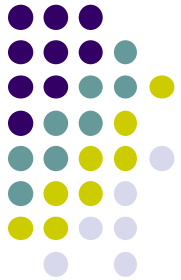
- Vendosja e ACL-ve afër destinacionit për fat të keq e lejon rrjedhën e trafikut përgjatë një apo me shumë segmenteve në rrjet para se ai te “ndalohet” nga ndonjë deklaratë e ACL-ve që përcakton një gjë të tillë gjatë konfigurimit të tyre.
- Kjo shkakton një humbje të konsiderueshme të bandwith-it.
- Duke i përdorur Extended ACL, i zgjidhim të dy këto çështje.

Krahasimi ndermjet ACL-se standarde dhe te zgjeruar

- Figura e mëposhtme jep një krahasim në përdorimin e ACL-ve Standarde dhe atyre të zgjeruara (Extended)



Disa komanda te rendesishme per krijimin e ACL-ve



- Jane dy fjale kyce qe perdoren ne ACL, “any” dhe “host”
- Thjeshte, vendoset opcioni **any** qe e zevendeson 0.0.0.0 per IP adrese dhe 255.255.255.255 per “wildcard mask”.

- Opcioni **host** zevendeson masken 0.0.0.0
- Ky opcion i pershtate vetem nje IP adrese

Shembull i opcioneve “any” dhe “host”

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Can be written as:

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

```
Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0
```

Can be written as:

```
Router(config)#access-list 1 permit host 172.30.16.29
```

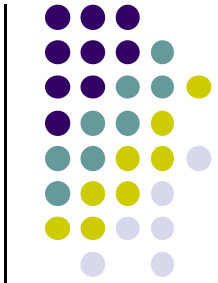
Vendosja e ACL-ve ne interfejs

- Krijimi i ACL-ve nuk do te funksionoje, nese nuk vendoset ne interfejsin e duhur.
- Pasi te krijohet nje ACL, atehere duhet te vendset ne interfejs, me komanen e meposhtme
  - ***Router (config-if): ip access-group 3 in***
- Me komanden e mesiperme, eshte vendisur ACL me nr 3 dhe kjo ACL aplikohet per trafikun ne hyrje

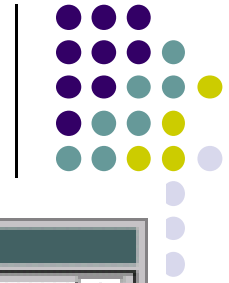
Shembull i krijimit dhe vendosjes se ACL-se standarde ne interfejs

```
Router#config t
Router(config)#access-list 50 permit 192.168.1.10
Router(config)#access-list 50 deny 192.168.1.0 0.0.0.255
Router(config)#access-list 50 permit any
Router(config)#interface Ethernet0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#ip access-group 50 out (applying the ACL)
```

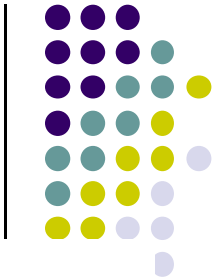
Verifikimi i ACL-ve



- Komanda **show ip interface** paraqet informatat për interfejsin dhe paraqet nëse është e vendosur ndonjë ACL ne ate interfejs.
- Komanda **show access-lists** paraqet përmbajtjen e te gjitha ACL-ve ne një ruter
- Komanda **show running-config** paraqet ACL-te ne ruter dhe interfejsat ku janë te vendosura ato.



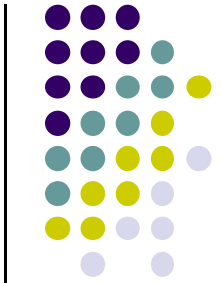
```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
```



```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Shembuj praktik

- Krijimi i ACL-ve me Packet tracer



Faleminderit!