Nätverksteknik A - Introduktion till Wildcardmaskar

Lennart Franked

Avdelningen för informationssystem och -teknologi (IST)
Mittuniversitetet

22 oktober 2018

Innehållsförteckning

Glosor

- Konvergeringstid
- Distans vector
- Link-State
- IGP/EGP

Glosor

- Konvergeringstid
- Distans vector
- Link-State
- IGP/EGP

Glosor

- Konvergeringstid
- Distans vector
- Link-State
- IGP/EGP

Glosor

- Konvergeringstid
- Distans vector
- Link-State
- IGP/EGP

- Inverterad subnätmask.
- ’0’ innebär att motsvarande fält måste vara lika
- ’1’ innebär att motsvarande fält ignoreras.

- Inverterad subnätmask.
- ’0’ innebär att motsvarande fält måste vara lika
- ’1’ innebär att motsvarande fält ignoreras.

- Inverterad subnätmask.
- ’0’ innebär att motsvarande fält måste vara lika
- ’1’ innebär att motsvarande fält ignoreras.

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0.	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

Figur 1: Wildcard [1]

Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

Example 2

	Decimal	Binary
IP Address	192.168.1.0	11000000.10101000.00000001.00000000
Wildcard Mask	0.0.254.255	00000000.00000000.11111110.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000
	All odd numbered subnets in the 192.168.0.0 major network	

Figur 2: Wildcard [1]

Beräknas enkelt genom att subtrahera subnätmask från 255.255.255.255

Example 1

```
  255.255.255.255
- 255.255.255.000
-----------------
  000.000.000.255
```

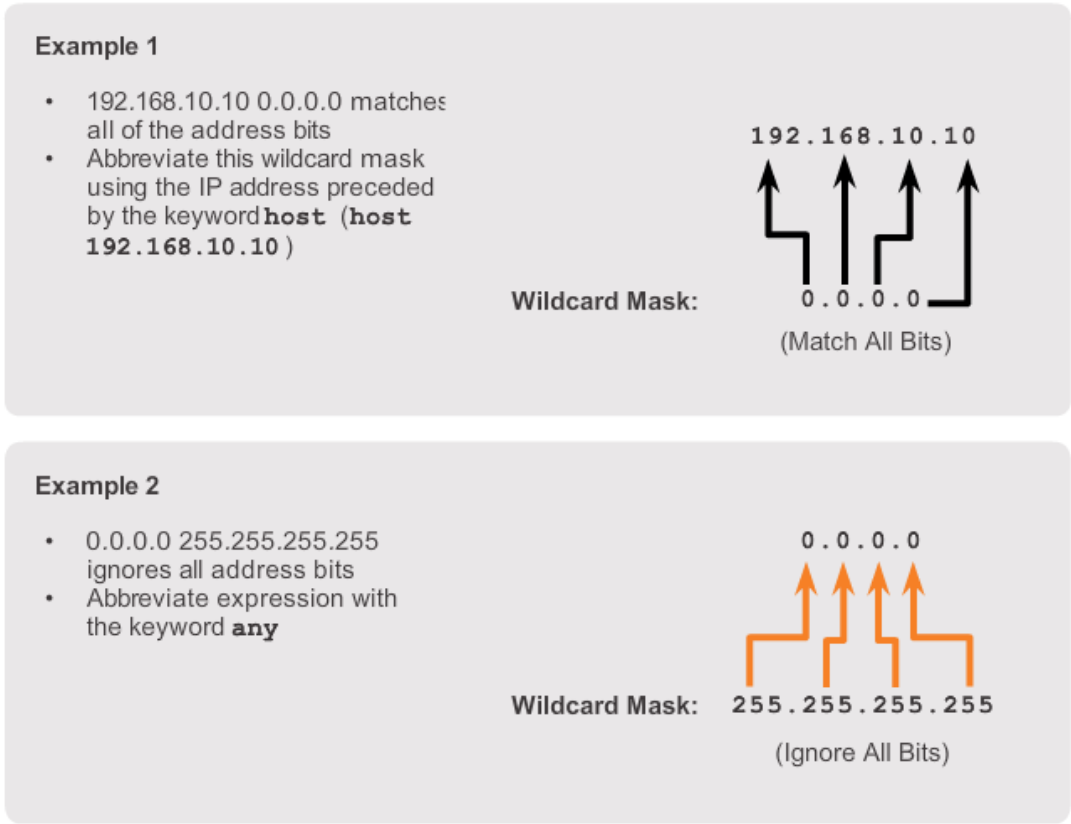
Example 2

```
  255.255.255.255
- 255.255.255.240
-----------------
  000.000.000.015
```

Example 3

Exempel III

Wildcard maskar



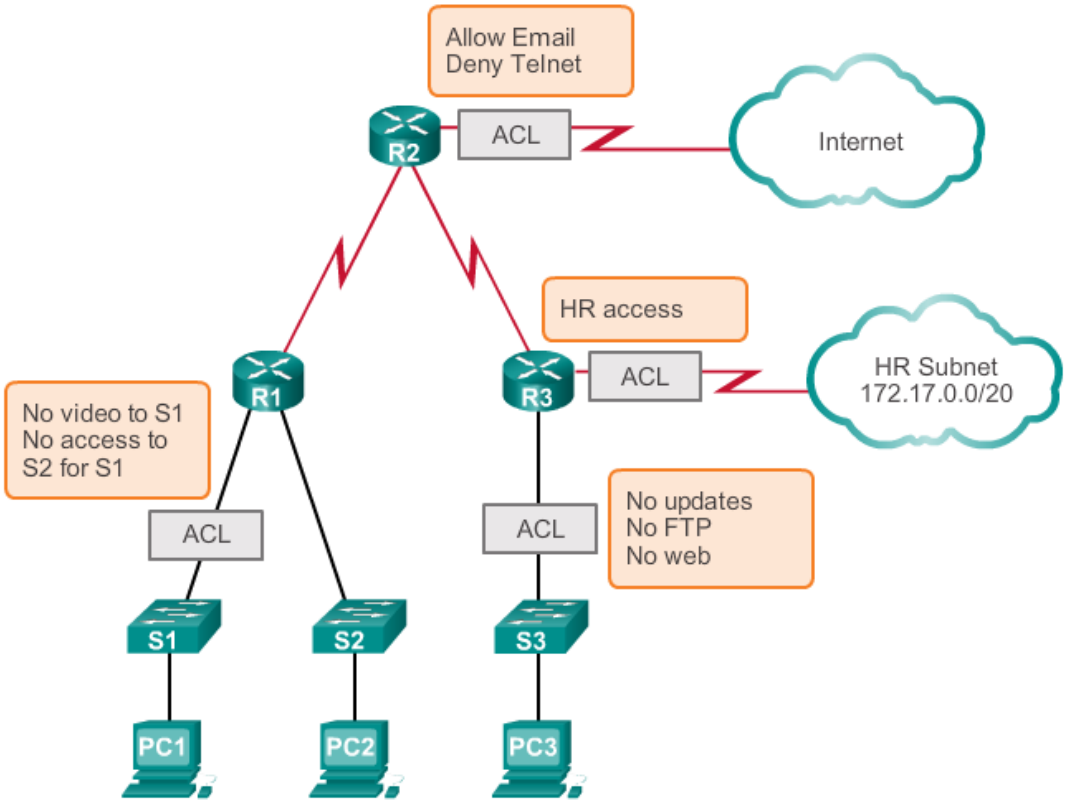
Figur 4: Wildcard [1]

Till skillnad från subnätmaskar måste de inte bestå utav en kontinuerlig sträng '0' eller '1'.

Exempel på godkända wildcardmaskar

```
00001100.00000000.011111011.11111111
11111111.00001000.011011011.11110111
11111111.11111111.111111111.11111111
00000000.00000000.000000000.00000000
```

Räkneexempel



Figur 5: Access Control Lists [1]

ACL Användningsområden

- Begränsa nätverkstrafik.
- Förse flödeskontrol.
- Grundläggande säkerhet.
- Specificera adressrymder.

ACL Användningsområden

- Begränsa nätverkstrafik.
- Förse flödeskontrol.
- Grundläggande säkerhet.
- Specificera adressrymder.

ACL Användningsområden

- Begränsa nätverkstrafik.
- Förse flödeskontrol.
- Grundläggande säkerhet.
- Specificera adressrymder.

ACL Användningsområden

- Begränsa nätverkstrafik.
- Förse flödeskontrol.
- Grundläggande säkerhet.
- Specificera adressrymder.

Figur 6: TCP konversation [1]

- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.

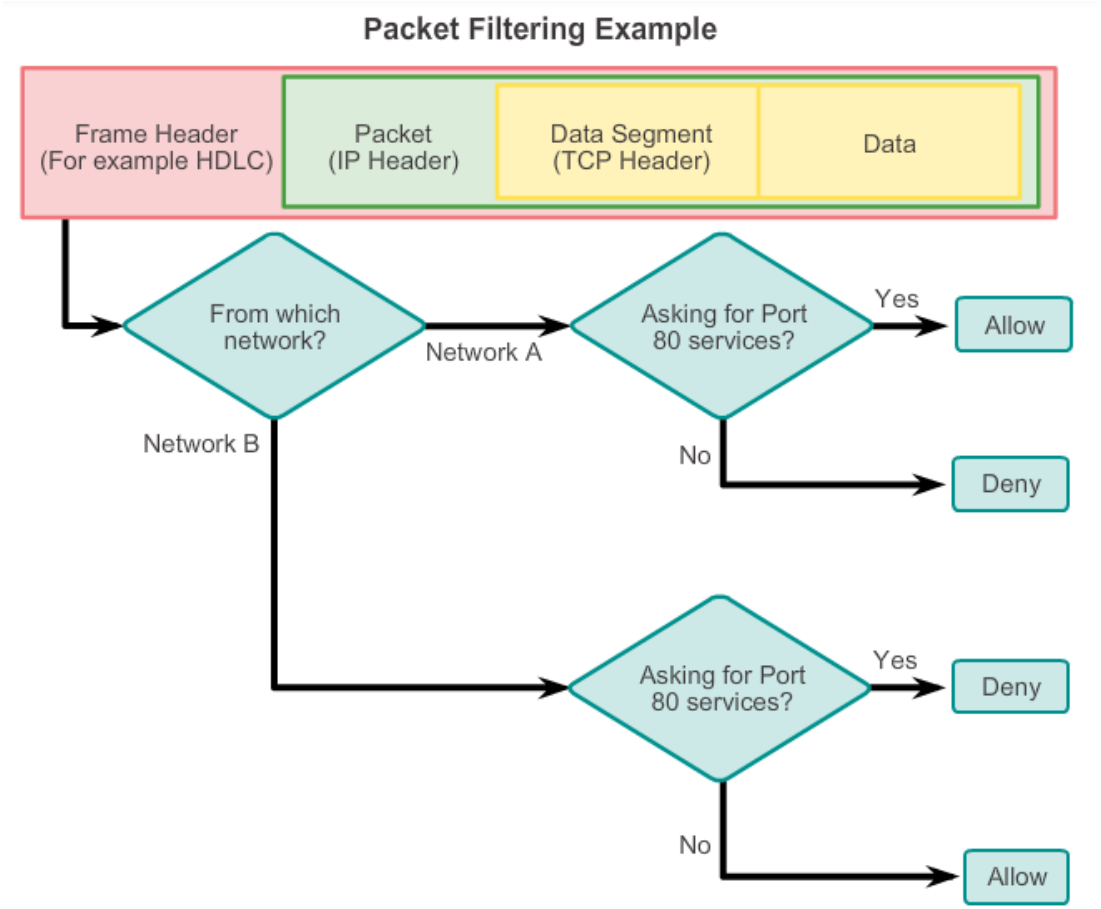
- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.

- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.

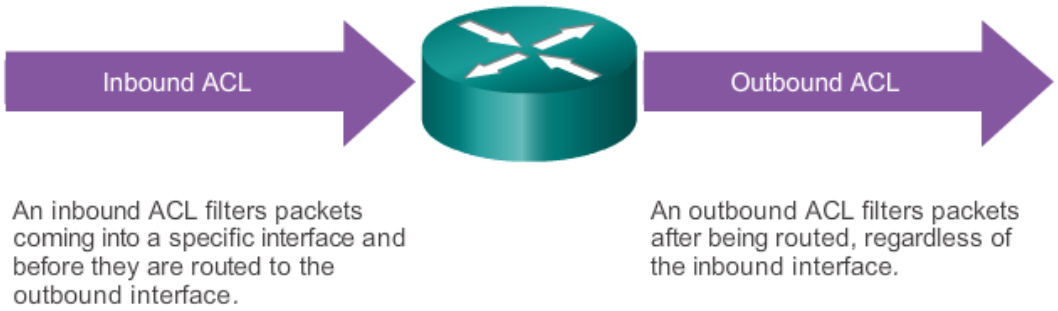
- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.

- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.

- Paketfiltrering / Statisk paketfiltrering
  - Analyserar paket utifrån givna kriterier
  - Exempelvis IP, Port, Protokoll.
- ACL är en sekventiell lista över regler som utvärderas.
- Access Control Entries
- Avslutas med en implicit 'Neka alla'.



Figur 7: Exempel [1]



Figur 8: Inkommande och utgående ACLer [1]

Standard ACL

Filtrerar enbart på källadressen.

Extended ACL

Filtrerar på:

- Käll och destinations IP-adress
- Käll och destinations Port
- Protokolltyp

Standard ACL

Filtrerar enbart på källadressen.

Extended ACL

Filtrerar på:

- Käll och destinations IP-adress
- Käll och destinations Port
- Protokolltyp

Standard ACL

Filtrerar enbart på källadressen.

Extended ACL

Filtrerar på:

- Käll och destinations IP-adress
- Käll och destinations Port
- Protokolltyp

Standard ACL

Filtrerar enbart på källadressen.

Extended ACL

Filtrerar på:

- Käll och destinations IP-adress
- Käll och destinations Port
- Protokolltyp

Standard ACL

Filtrerar enbart på källadressen.

Extended ACL

Filtrerar på:

- Käll och destinations IP-adress
- Käll och destinations Port
- Protokolltyp

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

Numrerad ACL

Anger ACL med hjälp utav siffror

- 1 - 99, 1300-1999 Standard ACL
- 100-199, 2000-2699 Extended ACL

Namngiven ACL

Anger ACL med namn

- Alfanumeriska tecken
- Versaler rekommenderat
- Ej punkt eller mellanslag

- Placera ACL mellan ett internt och externt nätverk.
- Placera ACL mellan två interna nätverk för at styra flödet mellan dem.

- Placera ACL mellan ett internt och externt nätverk.
- Placera ACL mellan två interna nätverk för at styra flödet mellan dem.

- Skapa en ACL per protokoll.
- Skapa en ACL per riktning.
- Skapa en ACL per interface.

- Skapa en ACL per protokoll.
- Skapa en ACL per riktning.
- Skapa en ACL per interface.

- Skapa en ACL per protokoll.
- Skapa en ACL per riktning.
- Skapa en ACL per interface.

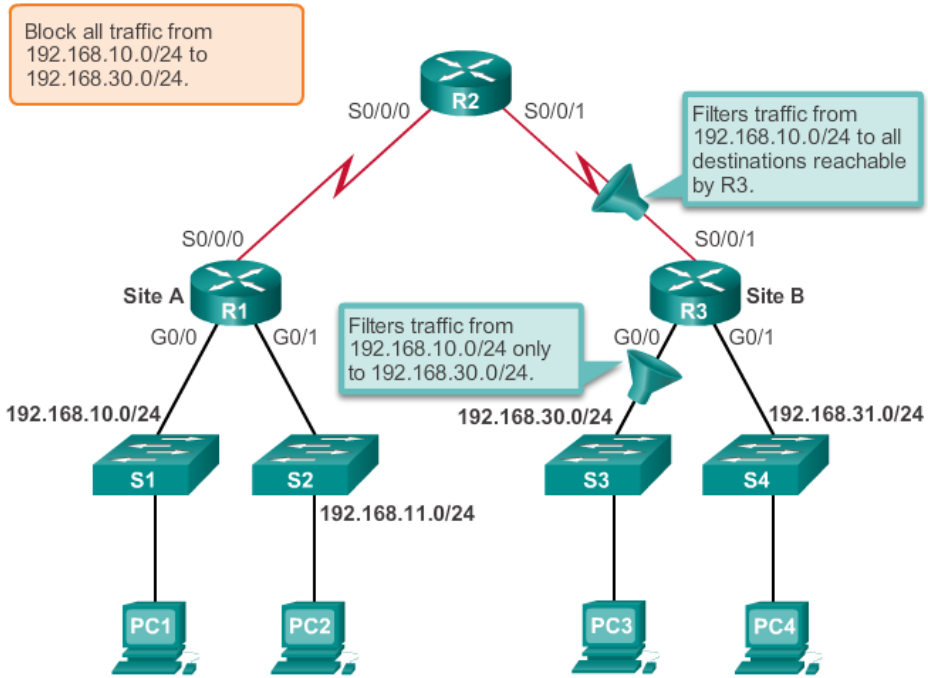
- Skriv ner hur du vill att reglerna ska fungera.
- Skriv ACL-kommandon i en textfil
- Lägg in reglerna i enheten.

- Skriv ner hur du vill att reglerna ska fungera.
- Skriv ACL-kommandon i en textfil
- Lägg in reglerna i enheten.

- Skriv ner hur du vill att reglerna ska fungera.
- Skriv ACL-kommandon i en textfil
- Lägg in reglerna i enheten.

Standard ACL

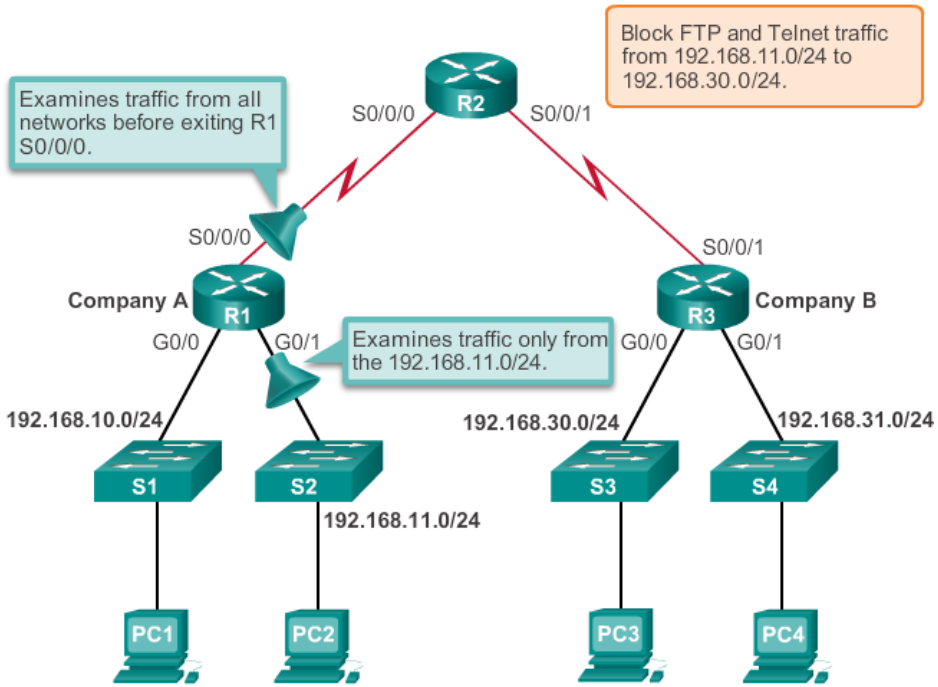
- Placeras så nära destinationen som möjligt.



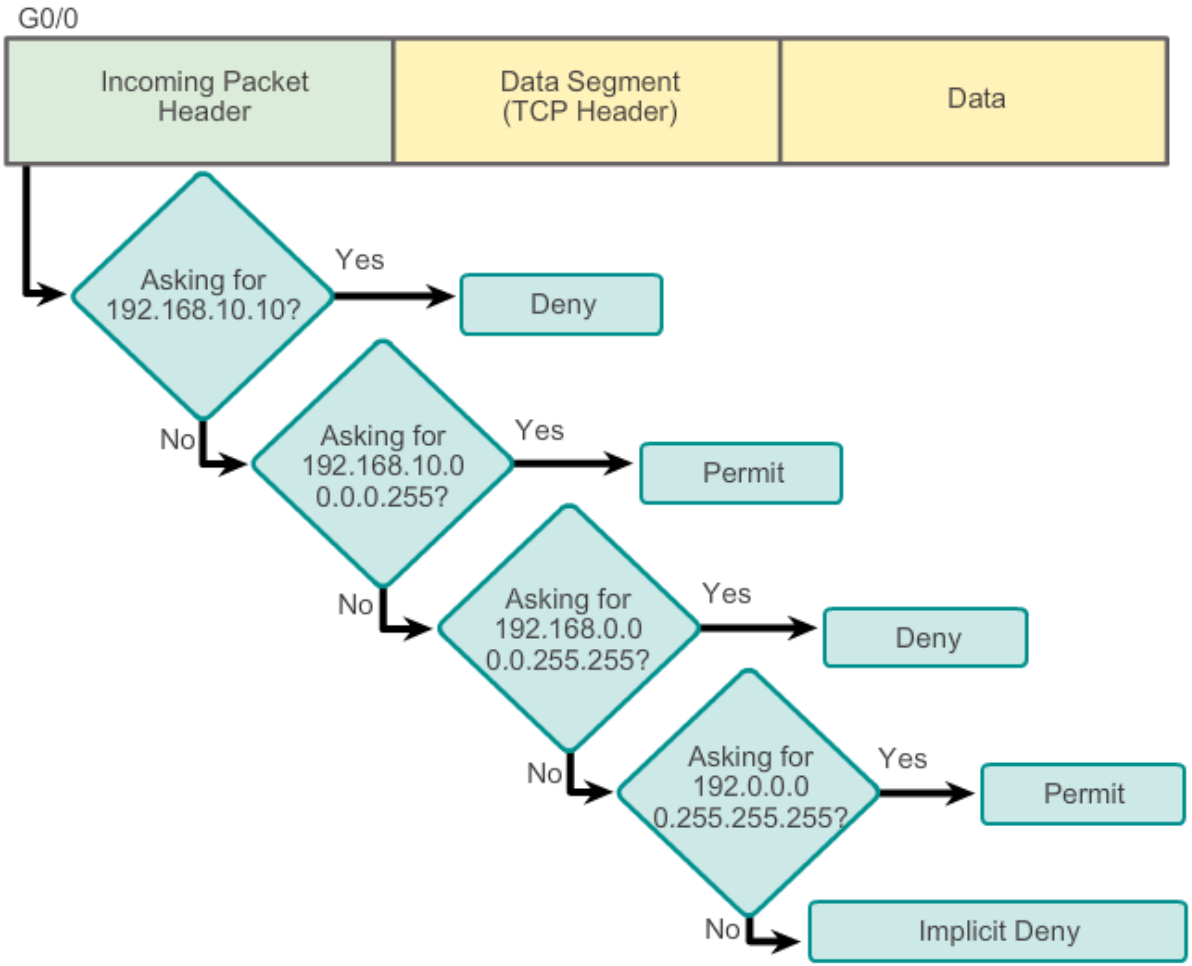
Figur 9: Standard ACL placering [1]

Extended ACL

- Placeras så nära källan som möjligt.



Figur 10: Utökad ACL placering [1]



Figur 11: Intern logik [1]

Ordningen av regler

- Regler kollas sekventiellt.
- Efter en träff så kollas inte kvarvarande regler.
- Ordningen man lägger dem i är därför viktig.

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3: Host statement conflicts with previous range statement.

Figur 12: Konflikt [1]

Ordningen av regler

- Regler kollas sekventiellt.
- Efter en träff så kollas inte kvarvarande regler.
- Ordningen man lägger dem i är därför viktig.

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3: Host statement conflicts with previous range statement.

Figur 12: Konflikt [1]

Ordningen av regler

- Regler kollas sekventiellt.
- Efter en träff så kollas inte kvarvarande regler.
- Ordningen man lägger dem i är därför viktig.

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3: Host statement conflicts with previous range statement.

Figur 12: Konflikt [1]

Inkommande paket

- Testas mot en existerande ACL *före* paketet routas.
- Om ingen träff på en 'permit'-regel sker en imlicit nekning.

Inkommande paket

- Testas mot en existerande ACL *före* paketet routas.
- Om ingen träff på en 'permit'-regel sker en imlicit nekning.

Utgående paket

- Testas mot en existerande ACL *efter* paketet routas.
- Saknas route, slängs paketen som vanligt.
- Om ingen ACL finns skickas paketet vidare.
- Finns ACL så testas paketet mot dessa regler.

Utgående paket

- Testas mot en existerande ACL *efter* paketet routas.
- Saknas route, slängs paketen som vanligt.
- Om ingen ACL finns skickas paketet vidare.
- Finns ACL så testas paketet mot dessa regler.

Utgående paket

- Testas mot en existerande ACL *efter* paketet routas.
- Saknas route, slängs paketen som vanligt.
- Om ingen ACL finns skickas paketet vidare.
- Finns ACL så testas paketet mot dessa regler.

Utgående paket

- Testas mot en existerande ACL *efter* paketet routas.
- Saknas route, slängs paketen som vanligt.
- Om ingen ACL finns skickas paketet vidare.
- Finns ACL så testas paketet mot dessa regler.

Utgående paket

- ACL arbetar på lager 3.
- Ingen kontroll sker förrän paketet granskas på lager 3.

```
Lager 1 -> Lager 3 -> Inkommande ACL -> Routing -> Utgående ACL
-> Vidarebefordra
```

Utgående paket

- ACL arbetar på lager 3.
- Ingen kontroll sker förrän paketet granskas på lager 3.

```
Lager 1 -> Lager 3 -> Inkommande ACL -> Routing -> Utgående ACL
-> Vidarebefordra
```

Utgående paket

- ACL arbetar på lager 3.
- Ingen kontroll sker förrän paketet granskas på lager 3.

```
Lager 1 -> Lager 3 -> Inkommande ACL -> Routing -> Utgående ACL
-> Vidarebefordra
```

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Standard ACL

- Kollar enbart på källadressen.

Extended ACL

1. Källadress
2. Källport
3. Källprotokoll
4. Destinationsadress
5. Destinationsport
6. Destinationsprotkoll

Enbart named extended.

Tre stora skillnader mellan dessa.

- `ipv6 traffic-filter` istället för `ip access-group`
- Inga wildcard maskar.
- utökat antal standard regler.
  - permit icmp any any nd-na
  - permit icmp any any nd-ns

Enbart named extended.

Tre stora skillnader mellan dessa.

- `ipv6 traffic-filter` istället för `ip access-group`
- Inga wildcard maskar.
- utökat antal standard regler.
  - permit icmp any any nd-na
  - permit icmp any any nd-ns

Enbart named extended.

Tre stora skillnader mellan dessa.

- `ipv6 traffic-filter` istället för `ip access-group`
- Inga wildcard maskar.
- utökat antal standard regler.
  - permit icmp any any nd-na
  - permit icmp any any nd-ns

Enbart named extended.

Tre stora skillnader mellan dessa.

- `ipv6 traffic-filter` istället för `ip access-group`
- Inga wildcard maskar.
- utökat antal standard regler.
  - permit icmp any any nd-na
  - permit icmp any any nd-ns

Enbart named extended.

Tre stora skillnader mellan dessa.

- `ipv6 traffic-filter` istället för `ip access-group`
- Inga wildcard maskar.
- utökat antal standard regler.
  - permit icmp any any nd-na
  - permit icmp any any nd-ns

Referenser

 Scott Empson och Cheryl Schmidt. *Routing and Switching Essentials – Companion Guide*. Cisco Press, 2014. ISBN: 978-1-58713-320-6.