**Účel a charakteristika ACL**

* ACL — Něco jako firewall → filtruje provoz v síti podle specifického nastavení — Paketový filtr
* Na Cisco Routerech a L3 switchích lze nastavit paketový filtr použitím ACLs
* Další využití: Zabezpečení sítě, Policy Based routing
* Charakteristika:
  + řazený seznam pravidel řídích přístup k objektu (permit a deny)
  + pravidla = Access control entries
  + ACL můžeme identifikovat pomocí čísla nebo jména
  + Nová pravidla se přidávají vždy na konec seznamu
  + Pravidlo first-fit – seznam se prochází od začátku, jakmile dojde ke shodě, dále se neprochází
  + Na ciscu prázdný seznam deny evrything
  + Specifická pravidla je vhodné umístit na začátek a obecná na konec seznamu
  + Při používání ACL dochází ke zpomalení zařízení

**ACLs — Access Control Lists**

* Posloupnost pravidel, který povoluje či zakazuje průchod paketům přes rozhraní, na základě údajům v hlavičce protokolů vrstev jako síťové a transportní
  + Zdrojová IP — Standard ACL
  + Cílová IP — Extended ACL
  + Typ protokolu — Extended ACL
  + Port komunikace — Extended ACL
* Jsou zde dva druhy ACL:
  + Standard
  + Extended
* Když je paket kontrolován, vždy prochází postupně všemi pravidly do té doby, než jedno pravidlo nevyhoví → a to pravidlo buďto zakáže paket (**deny**) či povolí (**permit**)
* ACL lze implementovat na rozhraní dvoumy způsoby:
  + Inbound komunikace → Komunikace, která přichází na rozhraní
    - Efektivnější → Pakety se filtrují již před routováním
  + Outbound komunikace → Komunikace, která odchází z rozhraní (routeru)

<aside> 💡 **ACL se neaplikuje na pakety, které vzniknou na routeru**

</aside>

* ACL se označují pomocí čísla či jména — pojmenování ACL je lepší, jelikož je lehčí na pozdější správu

<aside> 💡 Čísluje se v určitých intervalech:

* + 1-99 & 1300-1999 → Standard ACL
  + 100-199 & 2000-2699 → Extended ACL </aside>

<aside> 💡 Výchozí pravidlo ACL → deny any any - Zablokuje všechny pakety - proto je důležité si dávat pozor, ať v ACL je alespoň jedno permit pravidlo, aby se všechny pakety nezahodili

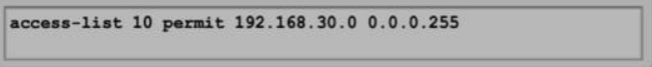
</aside>

**Wildcard maska**

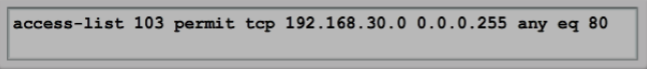
* Součástí ACL je tzv. wildcard maska, neboli inverzní maska
* Používá se k filtraci určitých adres či skupin adres
  + Filtruje se pomocí 0 a 1 v wildcard masce:
    - 0 → Označuje, že bit v IP zapsané v ACE a v porovnávající IP musí být stejný
    - 1 → Nezáleží; můžou být rozdílné
* Příklady:
  + 255.255.255.255 → Odpovídá na všechny IP, zapisováno taky jako keyword any
  + 0.0.0.0 → Odpovídá právě jako jedna IP, zapsáno taky jako keyword host
  + Např. pro síť, s maskou 255.255.255.0 by wildcard maska byla 0.0.0.255

**ACE — Access Control Entry a jejich vytváření**

* Standard ACL’s ACE se skládá z:
  + akce, pokud vyhoví kontrole: permit / deny
    - deny — Zablokuje paket
    - permit — Povolí paket
  + Zdrojová IP — Zdrojová…IP
  + Wildcard maska



* Extended ACL’s ACE se skládá z:
  + akce, permit / deny
  + protokol, tcp / udp / icmp / atd.
  + Zdrojová IP
  + Wildcard maska
  + Cílová IP
  + porovnávací keyword a port
    - Např. eq 80 → Rovná se portu 80
    - lze místo portu zapsat i jméno protokolu, např. http



**Pravidla při vytváření ACL**

tzv. Three Ps:

1. Jedno ACL pro IPv4 a IPv6
2. Jedno ACL pro každý směr
3. Jedno ACL pro každé síťové rozhraní

Také co se týče místa nastazení ACL:

* Standard ACL bude nejlepší nejblíž k cíli
* Extended ACL nejblíže k zdroji

<aside> 💡 Záleží na topologii.. Někdy Extended ACL nemůže být nejblíže ke zdroji, jelikož by zablokovalo komunikaci, kterou bychom my chtěli mít povolenou

</aside>

**IPv6 ACL**

* Jsou zde jen extended pravidla a named
* IP se píší v IPv6 (logicky)
* Délka prefixu je zapsána jako např. /64, né wildcard maska
* Na interface se nastazuje příkazem ipv6 traffic-filter <ACL name> <in/out>
* Povolení ICMPv6 Neighbor Advertisment/Discovery zpráv:
  + permit icmp any any nd-na
  + permit icmp any any nd-ns