**ACL** (Access Control Lists)

-Triediace a kontrolné zoznamy

-Najznámejšie nasadenie ako pravidlá riadenia IP prevádzky (FW)

-Použité aj všade tam kde je potrebná nejaká klasifikácia alebo identifikácia toku

**Úlohy**

-Obmedzenie nechcenej prevádzky

-Riadenie prevádzky

-Riadenie IP toku

-Poskytnutie základnej bezpečnosti

**ACL paketový filter**

-Zoznam testovacích podmienok, ktoré sa aplikujú na IP prevádzku prechádzajúcu rozhraniami smerovača

-Podmienky určujú - Povoľ (Permit) danú prevádzku ak spĺňa podmienku

- Zakáž (Deny) danú prevádzku ak spĺňa podmienku

**Ako ACL pracuje**

-ACL je zoznam podmienok **-** prehľadávaný sekvenčne, ak je zhoda na podmienku (paket je povolený (permit) alebo zahodený (deny)), pri zhode podmienky už ďalej nepokračujem

**Nasadenie ACL**

-Inbound ACLs- Smer paketov je do (in) smerovača, Vstupujúce pakety sú spracované skôr ako sú

Smerované, šetrím výkon smerovača, nerobím routing pre discard pakety

-Outbound ACLs- Smer paketov je von (out) zo smerovača, Skôr ako je paket postupený ACL je vykonané

Smerovanie

**Typy ACL**

-Štandardné (standard) ACL - Kontroluje sa len zdrojová adresa na podmienku

-Rozšírené (extended) ACL - Kontroluje sa zdrojová aj cieľová adresa na podmienku

**Ber do úvahy**

-ACL musí byť implementované na rozhranie aby nabralo na funkčnosti

-Na rozhranie môžem nasadiť len jeden acl per protokol a per smer

-Standard ACL - „Najbližšie k cieľu“

-Extended ACL - „Najbližšie k zdroju“

**Konfigurácia standard ACL**

-**Router(config)#access-list ACCESS-LIST-# [deny | permit | remark] TEST\_PODMIENKA [WILDCARD] [log]**

- **ACCESS-LIST-#:** Číslo acl - ACL môže mať veľa podmienok, ich príslušnosť k danému ACL je uvedená

týmto číslom

-**Deny**: zakáž paket splňujúci podmienku

-**Permit**: povoľ paket splňujúci podmienku

-**Remark**: vlož poznámku o nasledujúcej položke

-**TEST\_PODMIENKA**: Identifikátor podmienky vo forme IP adresy (bit pattern). Voči tejto podmienke sa budú porovnávať zdrojové IP adresy vstupujúcich paketov

-**WILDCARD**: voliteľné. Špecifikácia, ktoré bity zdrojovej IP adresy zdroja sa budú porovnávať voči podmienke uvedenej v TEST\_PODMIENKA.

-**Log**: loguje pakety, ktoré odpovedajú kritériu

**Wildcard Mask** - Definuje, ktoré bity IP adresy z paketu sa budú porovnávať s testovanou podmienkou ACL listu.

-Bity masky uvedené ako „0“ - Odpovedajúce bity zdrojovej IP adresy z paketu sa musia

porovnať s bitmi podmienky

-Bity masky uvedené ako „1“ - Odpovedajúce bity zdrojovej IP adresy z paketu sa

nemusia porovnať s bitmi podmienky

-Počítanie WM masky môže byť zjednodušené odčítaním masky siete od 255.255.255.255

**Priradenie ACL na rozhranie**

**-Router(config)#interface TYPE SPEC**

**Router(config-if)#ip access-group {ACCESS-LIST-# | ACCESS-LIST-NAME} {in | out}**

-**ACCESS-LIST-#** : Číslo acl, ktoré priraďujem na rozhranie

-**ACCESS-LIST-NAME** : alebo meno ACL, ktoré priraďujem

-**IN | OUT**: v akom smere aplikujem ACL

**Konfigurácia pomenovaného standard ACL**

-Výhoda pomenovaných ACL: Jednoduchšia identifikácia, V možnosti ich neskoršej editácie

**! Vytvorenie menneho ACL**

**! Meno je alfa numericky retazec, ktory nesmie zacinat cislom**

Router(config)#ip access-list [standard | extended] NAME

**! Zadanie testovacich podmienok menneho ACL**

**! Poradie testovacich podmienkok je dane defaultne od 10 s krokom 10**

**! Zadanie “no” a cislo riadku acl vyhodi podmienku**

Router(config-std-nacl)#[permit | deny | remark ] TEST\_CONDITION WM [log]

**! Priadenie menneho ACL na rozhranie**

Router(config-if)#ip access-group NAME [in | out]