Slovenská Technická Univerzita v Bratislave Fakulta informatiky a informačných technológií

Prepínanie a smerovanie v IP sieťach

Softvérový viacvrstvový prepínač

Zadanie

Navrhnite a implementujte softvérový viacvrstvový prepínač na základe znalostí získaných z predmetu Počítačové a komunikačné siete (PKS). Pri spracovaní koncepcie návrhu prepínača uvažujte viacportový prepínač. Ako výsledná implementácia postačuje riešenie s **dvojportovým prepínačom** (dve sieťové karty, port 1 a port 2), pričom ovládanie sieťových rozhraní realizujte príslušnými paketovými ovládačmi. Prepínač navrhnite a implementujte v jazyku **C++** alebo **C#** (ďalšími povolenými jazykmi sú **Java** alebo **Python**). Navrhnite prepínač tak, aby spĺňal požiadavky z úloh 1-4.

Úloha 1: Prepínacia tabuľka

Zobrazoval **prepínaciu tabuľku** vo formáte *MAC adresa – číslo portu – aktuálny časovač záznamu*. Prepínač sa obsah svojej prepínacej tabuľky učí priebežne a **aktuálny stav zobrazuje** cez grafické používateľské rozhranie (obsah sa **automaticky** aktualizuje, nie pomocou tlačidla). Umožnite **vyčistiť** prepínaciu tabuľku pomocou **tlačidla**. Časovač pre vypršanie záznamov nech je konfigurovateľný (pozn.: nezabudnite **ošetriť vytiahnutie** kábla, ako aj výmenu **káblov medzi portami**).

Úloha 2: Štatistiky

Poskytoval **štatistické informácie** vrstvy 2-4 RM OSI o počte (prijatých/odoslaných) PDU na každom porte v **smere IN** aj **OUT**, ktoré budú zreteľne zobrazovať správne fungovanie prepínača. Umožnite **resetovať** štatistické informácie. Štatistické informácie nech zobrazujú minimálne informácie o PDU typu **Ethernet II**, **ARP**, **IP**, **TCP**, **UDP**, **ICMP**, **HTTP**.

Úloha 3: Filtrácia komunikácie

Filtroval komunikáciu na 2.-4. vrstve RM OSI vrátane **portov transportnej vrstvy** a **typov ICMP** (bez použitia vstavaných PCAP funkcií filtrovania). Riešenie navrhnite ako **zoznam pravidiel** vyhodnocovaných sekvenčne tak, aby bolo možné naraz realizovať ľubovoľnú kombináciu filtrov. Napr. pre danú IP povoliť iba HTTP komunikáciu a zároveň pre danú MAC zakázať "ping". Umožnite aj **kombináciu** zdrojových a cieľových MAC a IP adries, príp. portov. **Zobrazujte tabuľku** zadaných **pravidiel** a umožnite ich aj jednotlivo odstraňovať. Filtre rozlišujte **v smere "in/out"** na každom porte prepínača (takisto zohľadniť v návrhu). Napr. Host A sa nedostane von na web (HTTP), ale u neho bežiaci server nginx (HTTP) bude dostupný.

Úloha 4: CDP alebo Syslog

Realizoval jednu z nasledujúcich funkcionalít (príp. inú po dohode s cvičiacim – zmena musí byť schválená cvičiacim do začiatku 3. cvičenia):

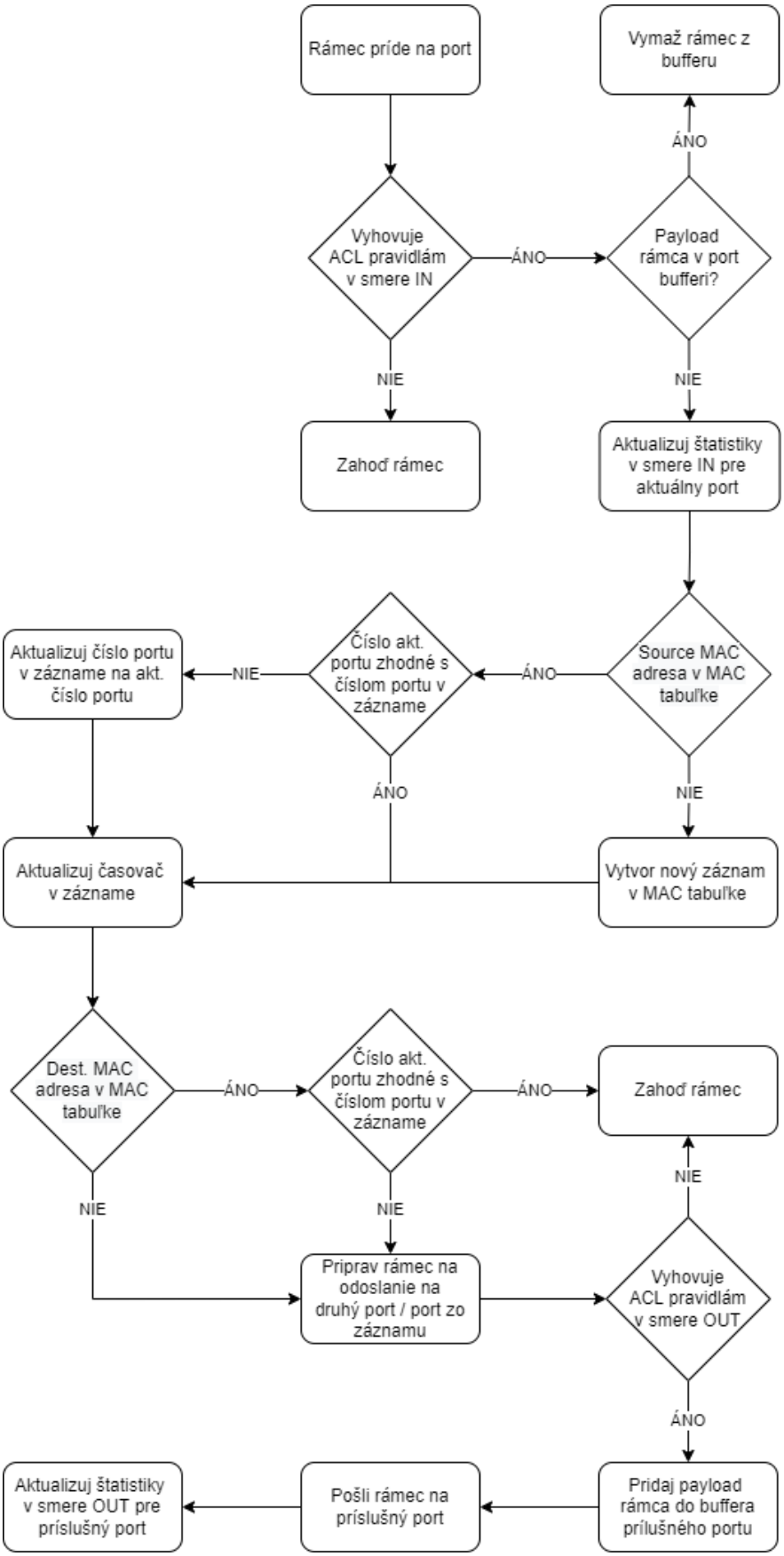
Variant A: Cisco Discovery Protocol (CDP)

Implementácia protokolu CDP, pričom stačí:
1. Prehľadne ukázať pri každom zázname o susedovi: remote hostname - local port - remote port.
2. Lokálne **označenie zariadenia** nech je **konfigurovateľné**.
3. Zabezpečiť vypršanie **časového limitu pre susedov** (timeout), podporovať **viacerých susedov na 1 porte** (segmente).
4. Zabezpečiť **kompatibilitu s Cisco zariadeniami** (rozpozná ho ako suseda). Umožnite spustenie/zastavenie CDP funkcionality na prepínači. Semestrálny projekt z predmetu Prepínanie a smerovanie v IP sieťach, LS 2021/2022

Variant B: System Logging (Syslog)

Implementácia Syslog klienta, pričom je potrebné:
1. Zabezpečiť **aspoň 3 úrovne** dôležitosti správ (severity level).
2. Umožniť nakonfigurovať prepínaču **zdrojovú IP adresu**, z ktorej sa budú správy odosielať.
3. **Nakonfigurovať IP adresu** vzdialeného Syslog **servera**.
4. Zasielané správy musia obsahovať **časovú pečiatku** (angl. timestamp).
5. Zvoľte **aspoň 5 činností** (descriptions), ktoré budete pomocou Syslog zaznamenávať (napr. „Zariadenie s MAC X sa premiestnilo z portu 1 na port 2“).
Syslog server bude aplikácia TFTPD32 bežiaca na niektorom počítači (prípadne Networkers' Toolkit pre GNS3). Umožnite spustenie/zastavenie Syslog funkcionality na prepínači.

Diagram spracovania rámca



Prepínacia tabuľka

Nový záznam

Ak príde na port switchu rámec, ktorého zdrojová MAC adresa sa nenachádza v prepínacej tabuľke, tak sa v nej vytvorí nový záznam, ktorý bude obsahovať MAC adresu, číslo portu a časovač. Časovač predstavuje dobu, počas ktorej bude záznam v prepínacej tabuľke uložený.

Aktualizácia záznamu

Pokiaľ sa zdrojová MAC adresa prichádzajúceho rámca už nachádza v zázname prepínacej tabuľky a číslo portu v zázname je zhodné s číslom portu, tak sa aktualizuje (zvýši) časovač tohto záznamu.

Pokiaľ sa číslo portu v zázname prepínacej tabuľky nezhoduje s číslom portu aktuálneho rozhrania, tak sa číslo portu v zázname aktualizuje na číslo portu aktuálneho rozhrania a časovač tohto záznamu sa aktualizuje (zvýši).

Zmazanie záznamu

Pokiaľ časovač záznamu v prepínacej tabuľke vyprší, záznam sa automaticky z tabuľky, vymaže.

Štatistiky

Pri spracovaní rámca na porte/rozhraní sa zistí, či rámec obsahuje **Ethernet II** hlavičku. Ak áno, tak sa zvýšia sa štatistiky pre Ethernet II a rámec sa začne skúmať hlbšie, či obsahuje nasledujúce hlavičky:

- **ARP** – zvýšia sa štatistiky pre ARP
- **IP** – zvýšia sa štatistiky pre IP a skúma sa hlbšie, či obsahuje hlavičky:
  - **ICMP** – zvýšia sa štatistiky pre ICMP
  - **UDP** – zvýšia sa štatistiky pre UDP
  - **TCP** – zvýšia sa štatistiky pre TCP a skontroluje sa zdrojový a cieľový port
    - **HTTP** – pokiaľ sa zdrojový alebo cieľový port rovná 80, tak sa zvýšia štatistiky pre http

Odpojenie a výmena kábla

Odpojenie kábla

Pokiaľ switch zistí, že z portu bol odpojený kábel (už dlhší čas na port neprichádza žiadna sieťová premávka), tak všetky záznamy v prepínacej tabuľke, ktoré prislúchajú k tomuto portu budú vymazané.

Výmena kábla

Pokiaľ switch zistí, že kábel bol vymenený, zapojený do druhého portu (v prepínacej tabuľke sa nachádza záznam so zdrojovou MAC adresou prichádzajúceho rámca, ale číslo portu v zázname je odlišné od čísla aktuálneho portu), tak sa v prepínacej tabuľke vyhľadajú všetky záznamy, ktoré prislúchajú číslu aktuálneho portu alebo číslu portu zo záznamu. Následne sa všetky tieto záznamy vymažú z prepínacej tabuľky a pre zdrojovú MAC adresu prichádzajúceho rámca sa vytvorí nový záznam, ktorý bude prislúchať aktuálnemu portu s novým časovačom.

Filtrácia komunikácie pomocou Access Control Lists (ACL)

ACL predstavuje usporiadaný zoznam pravidiel pre sieťovú premávku, pričom každé pravidlo špecifikuje komunikáciu, ktorej sa týka a akciu, ktorá sa má vykonať. Akcia definuje, či sa daná komunikácia má povoliť alebo zakázať.

Existujú sa dva základné typy ACL pravidiel:

- Štandardné – filtrovanie len na základe zdrojovej IP adresy
- Rozšírené – filtrovanie na základe zdrojovej aj cieľovej IP adresy, použitého protokolu a tiež zdrojového a cieľového portu

Pre každú komunikáciu sa ACL kontroluje vždy od začiatku (od prvého pravidla) a ak sa kontrolované pravidlo týka danej komunikácie, tak sa vykoná príslušná akcia a ďalšie pravidlo sa už nekontroluje. Ak sa kontrolované pravidlo netýka danej komunikácie, tak sa pokračuje ďalším pravidlom v poradí.

Ak sa žiadne pravidlo v ACL netýka danej komunikácie, tak sa použije implicitné pravidlo zakazujúce všetky ostatné komunikácie. Takže každý ACL musí obsahovať aspoň jedno povoľovacie pravidlo, inak zakáže všetky komunikácie.

Každé pravidlo má pridelený jednoznačný identifikátor v podobe tzv. sekvenčného čísla. Na základe neho vie zariadenie určiť poradie pravidiel, podľa ktorého sa majú jednotlivé pravidlá vyhodnocovať.

Jednotlivé ACL s pravidlami sa aplikujú pre konkrétne rozhranie (port) v smere IN pre prichádzajúcu komunikáciu a v smere OUT pre odchádzajúcu komunikáciu.

Cisco Discovery Protocol (CDP)

CDP je proprietárny protokol Cisco, ktorý sa používa na zhromažďovanie informácií o priamo pripojených susedných zariadeniach ako sú napríklad:

- názov zariadenia
- verzia softvéru
- typ hardvéru
- číslo portu z ktorého bol CDP odoslaný
- atď.

Princíp fungovania

Všetky zariadenia Cisco pravidelne vysielajú pakety CDP (60s). Tieto pakety propagujú hodnotu TTL (time-to-live) v sekundách, ktorá udáva počet sekúnd, počas ktorých sa paket musí uchovávať, kým môže byť vyradený (180s).

- Pakety CDP sa odosielajú s hodnotou doby životnosti, ktorá je nenulová po povolení (spustení) rozhrania
- S hodnotou nulovej doby životnosti bezprostredne pred vypnutím rozhrania. To poskytuje rýchle zistenie stavu.
- CDP funguje iba na priamo pripojených rozhraniach.
- Správy sú určené na L2 multicast adresu 01:00:0C:CC:CC:CC
- CDP beží na všetkých médiách, ktoré podporujú protokol SNAP (Subnetwork Access Protocol)

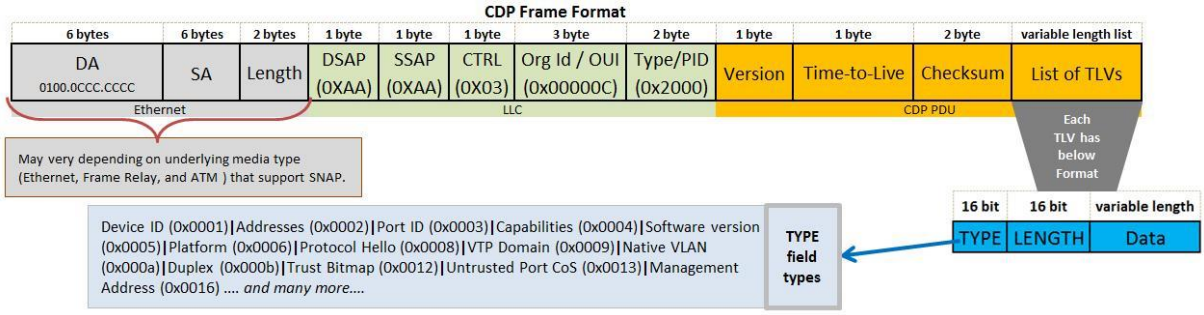
Všetky zariadenia Cisco prijímajú CDP pakety, spracovávajú ich a ukladajú informácie v pakete do vyrovnávacej pamäte. Zariadenia Cisco nikdy nepreposielajú CDP pakety. Ak sa od posledného prijatého paketu zmenia nejaké informácie, nové informácie sa uložia do vyrovnávacej pamäte a staršie informácie sa zahodia, aj keď ich hodnota doby životnosti ešte neuplynula.

Formát SNAP hlavičky:

CDP používa v SNAP hlavičke pre pole Type hodnotu HDLC protokolu (0x2000), takže CDP môže bežať na všetkých médiách, ktoré podporujú SNAP. To sú napríklad LAN, Frame Relay a ATM.

- LLC
  - DSAP – 0xAA
  - SSAP – 0xAA
  - CTRL – 0x03
- SNAP
  - Vendor Code (Org ID) – 0x00000C
  - Type (HDLC) – 0x2000

Formát CDP rámca



Popis políčok

Pole		Popis
Version		Verzia CDP, ktorá sa používa
Time-to-Live		Čas v sekundách, ktorý predstavuje dobu, počas ktorej by si mal prijímač pamätať informácie poskytnuté prostredníctvom prijatého CDP paketu. Predvolená hodnota je nastavená na 180 sekúnd.
Checksum		Štandardný checksum
Type/Length/Value (TLV)	**Type**	CDP typ (Device ID, Port ID, Software version, atď.)
	Length	Celková dĺžka TLV poľa v bajtoch (Type + Length + Value)
	Value	Samotné dáta TLV poľa

Všeobecné informácie

- Vývojové prostredie
  - Visual Studio 2022
- Programovací jazyk
  - *C# .NET Framework 4.7.2*
- Použité knižnice
  - *SharpPcap*
  - *PacketDotNet*

Použité zdroje:

[1] https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x
[2] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html
[3] https://wiki.wireshark.org/CDP
[4] https://www.geeksforgeeks.org/what-is-cisco-discovery-protocol-cdp/