Juraj Ševčík
Cvičenie: Streda 10:00
12.3.2022

Dokumentácia projektu PSIP

Zadanie

Navrhnite a implementujte softvérový viacvrstvový prepínač na základe znalostí získaných z predmetu Počítačové a komunikačné siete (PKS). Pri spracovaní koncepcie návrhu prepínača uvažujte viac portový 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 úloh1-4.

Úloha 1: Prepínaciatabuľka

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 (obsahsa 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 vrstvya 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 servernginx(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 osusedovi: remote hostname-local port-remote port. 2.Lokálne označenie zariadenianech 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.

Juraj Ševčík 12.3.2022
Cvičenie: Streda 10:00

Semestrálny projekt z predmetu Prepínanie a smerovanie v IP sieťach, LS 2021/2022Variant B: System Logging (Syslog)Implementácia Syslog klienta, pričom je potrebné:1.Zabezpečiť aspoň 3úrovnedôležitosti správ (severity level).2.Umožniť nakonfigurovať prepínaču zdrojovú IP adresu, z ktorej sa budú správy odosielať.3.NakonfigurovaťIP adresu vzdialeného Syslog servera.4.Zasielané správy musia obsahovať časovú pečiatku(angl. timestamp).5.Zvoľte aspoň 5činností(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. Podmienky absolvovania Pre účasť na skúške je potrebná implementácia minimálne funkcionality prepínača (nestačí hub), t.j. úlohy 1 a2.Bez splnenia tejto podmienky nebude študent pripustený ku skúške.

Obsah dokumentácie

Dokumentácia musí obsahovať:

1.Zadanieúlohy.

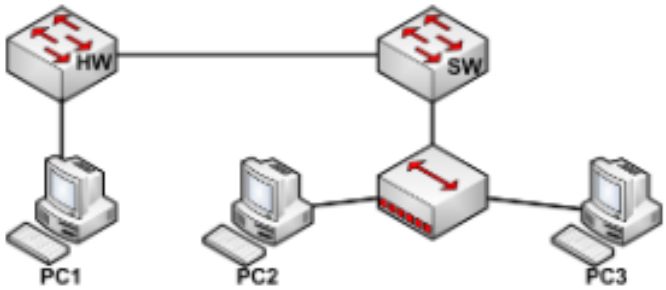
2.Návrh riešenia obsahujúci podrobné diagramy spracovania rámcov s opisom čo sa kde a ako bude vykonávať(úlohy 1-3).

3.Analýzuprotokolov CDP alebo Syslog(implementácia bez dostatočnej analýzy nebude hodnotená), ak sa rozhodnete implementovať úlohu

4.Dokumentáciu ako aj výsledný prepínač musí študent odovzdať do príslušného miesta odovzdania v AIS (po vložení súborov nezabudnúť súbory odoslať/odovzdať).

Všetky termíny určené miestom odovzdania v AIS sú konečné a za neskoré odovzdanie bude študent hodnotený 0b.HodnoteniezadaniaZadanie sa prezentuje a hodnotí priebežne po častiach, podľa pokynov cvičiaceho. Za oneskorené odovzdanie(t.j. študent nestihne do daného cvičenia/týždňa vypracovať určenú časť zadania) bude študent hodnotený 0bzpríslušnej časti zadania. Predbežný plán odovzdávania a bodovania zadania:•3. cvičenie (3b): prototyp, ktorý musí vedieť prijímať a posielať komunikáciu (odchytiť prichádzajúci rámec na porte a poslať rámec von portom) + štatistiky. koniec 4. týždňa (2b+ 1b): dokumentácia(max 2bza úlohy 1-3,1b za úlohu 4).•7. cvičenie (10b): základná funkcionalita prepínača(úlohy 1-3).•koniec 10. týždňa (9b): filtre(4b) + CDP alebo Syslog(5b-len v prípade splnenia všetkých podmienok uvedených v zadaní, inak 0b).

Semestrálny projekt z predmetu Prepínanie a smerovanie v IP sieťach, LS 2021/2022Základná preberacia topológia Prepínač SW predstavuje počítač s vašim softvérovým prepínačom, HW je hardvérový (Cisco)prepínač. Pozn. prepínač implementujte univerzálne(nie presne na túto topológiu), otestujte sa aj na iných topológiách.



KONIE

Juraj Ševčík
Cvičenie: Streda 10:00 12.3.2022

Návrh riešenia

Prostriedky

Projekt používa programovací jazyk C# a knižnicu Pcap na zachytávanie a predostielanie packetov.

Prepínacia tabuľka

Údaje do prepínacej, MAC, tabuľky sa budú získavať z prijatých rámcov ich source/zdrojovej adresy. Pri prijatí rámca je potrebné ho dočasne uložiť keďže sa budeme používať store-and-forward switching.

Keď rámec uložíme pozrieme sa na kontrolne bity na konci a skontrolujeme neporušenosť rámca.

Ak je rámec neporušený pokračujeme v jeho spracovaný inak ho zahodíme.

Po jeho uložený a skontrolovaný bude potrebné skontrolovať či sa jeho zdrojová MAC adresa nachádza v našej tabuľke, ak sa nenachádza, tak ju uložíme spolu aj s číslom portu z ktorého sme packet dostali a na koniec k záznamu pridáme aj časovač po ktorého prekročený je záznam vymazaný.

V prípade že sa MAC adresa v tabulke síce nachádza ale port z ktorého packet prišiel nezodpovedá informácii v tabuľke tak sa tabuľka prepíše podľa prijatého rámca

V prípade že sa táto MAC adresa v tabuľke už nachádza tak pri tejto informácii skontrolujeme či sa port zhoduje s MAC adresou a resetujeme časovač na zvolenú hodnotu, štandardne 300s.

Po uložený záznamu do MAC tabuľky sa pozrieme či sa v nej nachádza adresa na ktorú chceme odoslať packet. Ak informáciu o tejto adrese máme packet prepošleme len na túto adresu. Ak však túto adresu nemáme packet budeme musieť preposlať na všetky nám dostupné porty okrem portu z ktorého sme packet dostali.

Ošetrenie vytiahnutia kábla:

Pri odpojený a prepojený kábla čo budeme detegovať tak že na port nebude určití čas chodiť žiadna komunikáciu. V takomto prípade premažeme celú MAC tabuľku pre prislúchajúci port preto že pri opätovnom pripojený kábla už nemusí byť pravdivá.

Pri prijatý packetu medzi jeho skontrolovaným a odoslaným na cieľový port budem viesť referovateľnú štatistiku o tom aký protokol prišiel a z akého portu. Informácie budem získavať z packetou pomocou nožnicových príkazov. Pri packetoch pri ktorých budem používať brodcast sa budú tieto štatistiky zapisovať do samostatného počítadla. Rozlišovať sa budú podľa zadania.

Poskytovanie štatistík

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.

Juraj Ševčík 12.3.2022
Cvičenie: Streda 10:00

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 servernginx (HTTP) bude dostupný.

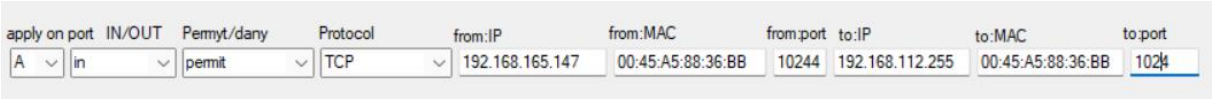
Filtrovanie

Pri používaný filtrov sa packet príjme a filtre budú aplikované v kroku podľa diagramu (niižšie). Po prijatý packetu sa pomocou funkcie z knižnice získajú informácie (zdrojová/cieľová IP/MAC , protokol, port)

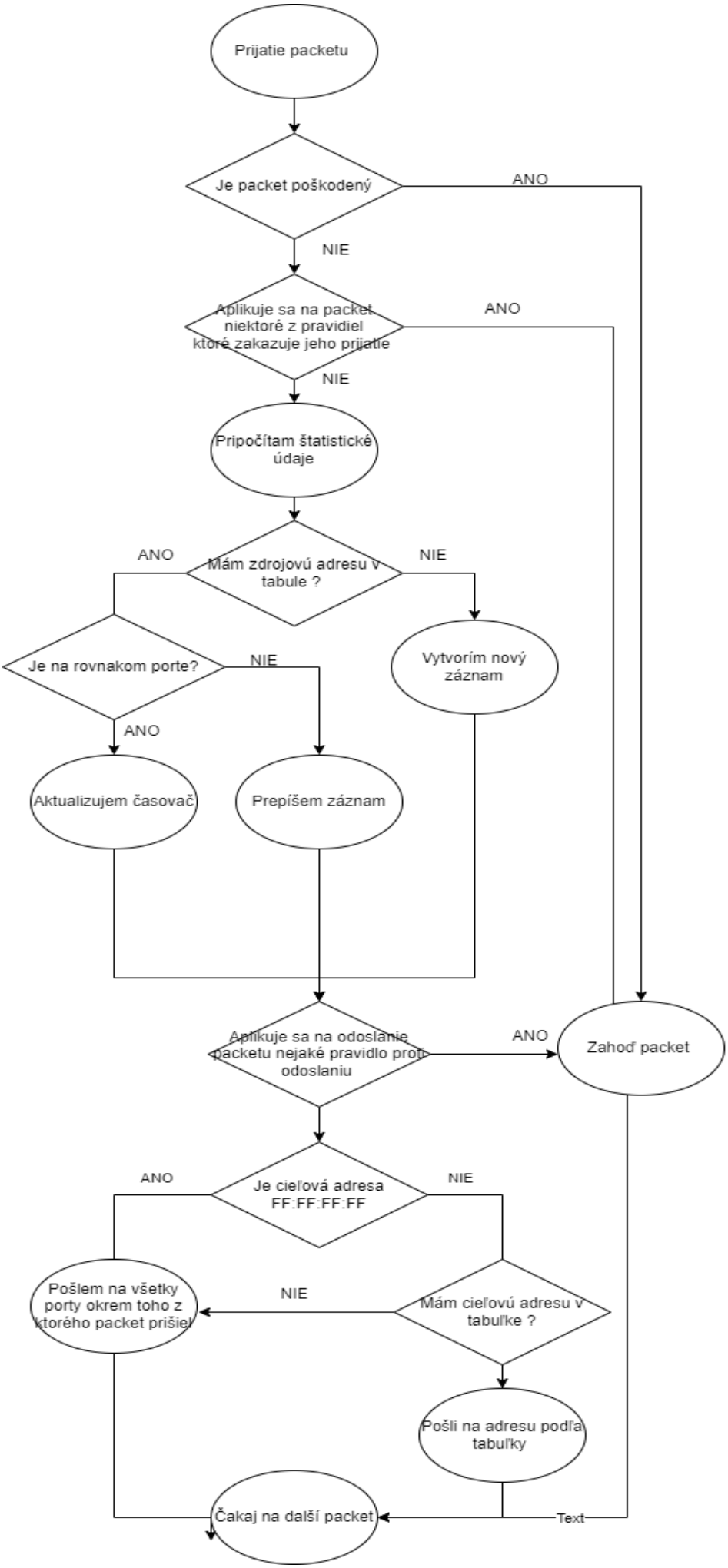
Pri nasadávaný filtrovania sa packet uloží ale pred upraveným štatistík sa skontrolujú pravidlá a ak existuje pravidlo zakazujúce jeho prijatie packet bude odstránený. Podobne pri odoslaní sa skontrolujú všetky pravidlá a ktoré je možné jednoducho nastaviť a je ich opäť možné jednotlivo zmazať aby sa dalo filtrovanie kontrolovať. Ak odoslanie packetu nie je zakázané tak sa upravia štatistiky a packet sa odošle.

Ako posledné pravidlo bude ‘allow all‘ takže všetka premávka ktorá nebude zakázaná bude povolená.

Formát pravidla:



Juraj Ševčík 12.3.2022
Cvičenie: Streda 10:00



Juraj Ševčík
Cvičenie: Streda 10:00 12.3.2022

Syslog

Ide o protokol na zaznamenávanie udalostí, ako názov napovedá. Udalosti sú vygenerované systémom a majú rôzne stupne závažnosti.

Syslog má štandardný port 514.

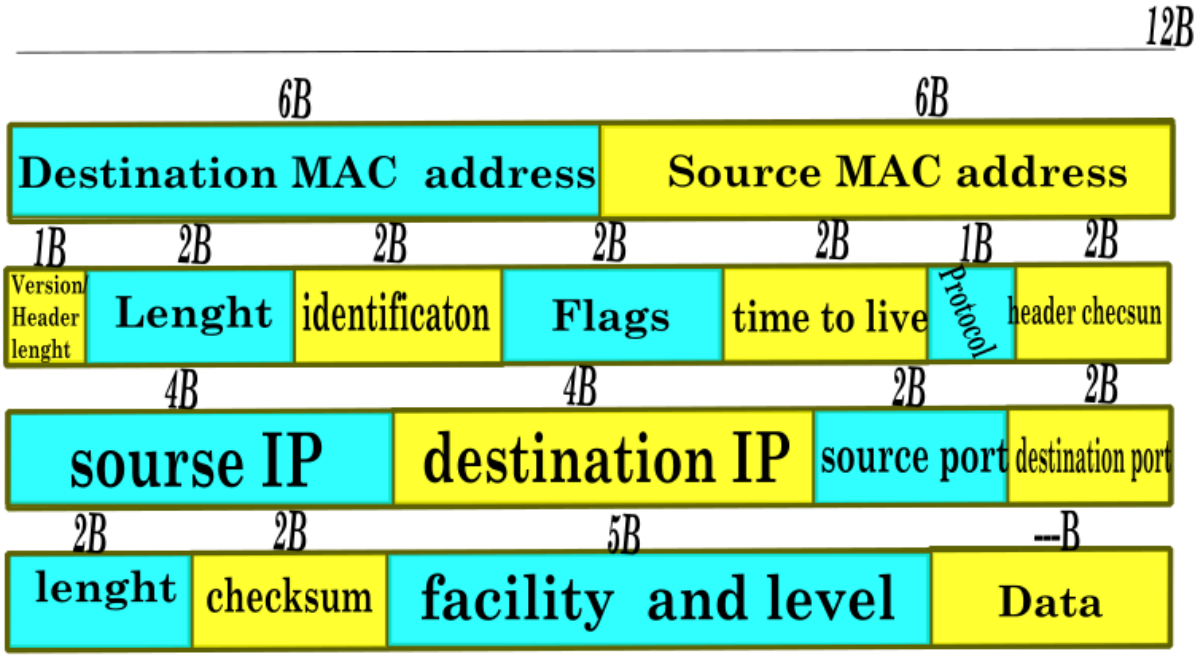
Štruktúra

(poznámka: obrázky obsahujú rovnakú informáciu ale považujem farebnú verziu za prehľadnejšiu)

6B	6B	2B	1B
destination MAC address	source MAC address	ethertype	version/header length

2B	2B	2B	1B	1B	2B	4B	4B
length	Identification	flags	time to life	protocol	header checksum	source IP	destination IP

2B	2B	2B	2B	5B
source port	destination port	length	checksum	facility + level	message



Juraj Ševčík 12.3.2022
Cvičenie: Streda 10:00

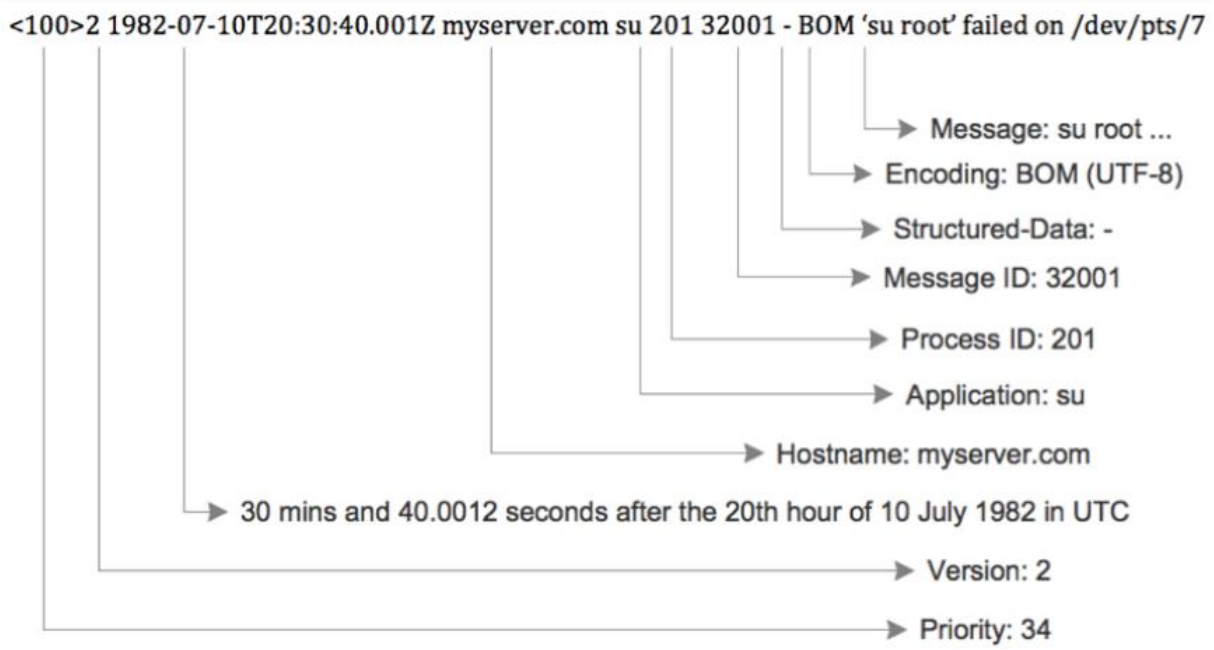
NAME :	SIZE:	DESCRIPTION:	VALUE: (hexa)
destination MAC address	6B		
source MAC address	6B	MAC adresa zariadenia posielajúceho správu	
ethertype	2B	IPv4	08 00
version/header length	1B	Internet protocol version: 4 Header lenght: 20 bytes	45
Total lenght	2B	Dĺžka celého packetu – 14B	
Identification	2B	Poradové čislo syslog správy	
Flags	2B	Informácie o packete – nebudú sa nastavovať	
time to life	1B	Po uplynutí sa packet zahodí	60
protocol	1B	Protokol – UDP	11
heder checksum	2B	Hodnota na skontrolovanie neporušenosti hlavičky	
Source IP	4B	IP adresa zariadenia ktoré posiela syslog	
Destination IP	4B	Nastavená na predvolené zariadenia (ideálne zariadenie administrátora)	
Source port	2B	514	514
Destination port	2B	514	514
Length	2B	Dĺžka packetu -34B	
Checksum	2B		
facility + level	5B	Úroveň závažnosti správy	
message	0B-XB	Naformátovaná správa	

Message

Štruktúra syslog správy obsahuje Prioritu + verziu + časovú pečiatku + hostname + aplikaciu + proces ID + message id. Za týmito údajmi sa nachádza správa ktorú chceme odoslať.

NÁZOV:	POPIS:	PRÍKLAD HODNOTY:
Message ID	Poradové číslo správy	<1>
Priority	0 – 4 0- Najvyššia priorita, vyžaduje okamžitú pozornosť 1- Dôležitá správa – oprav čo najskôr 2- Niečo nie je v poriadku ale nemusíš sa ponáhľať 3- Keď sa budeš nudiť toto je celkom zaujímavé 4- Debugovacia správa	4
Version	Verzia formátu správy	1
Časová pečiatka	Aktuálny čas	2022-3-10T11:32:21.001Z
Hostname	Meno zariadenia ktoré posiela správu – static IP	<192.168.12.5>
Aplikácia	Aplikácia ktorá posiela hlášku	<MyApp>
Proces ID	Číslo procesu ktorý zlyhal	<154>

Pr. <1>4 2022-3-10T11:32:21.001Z host MyApp 154 – error has ocured on /dev/etc/



https://blog.rapid7.com/content/images/post-images/63449/Untitled.png;