VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2018 Jaroslav Bošeľa

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ DOHLEDOVÝ SYSTÉM
LABORATORY MONITORING SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jaroslav Bošeľa**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Vladislav Škorpil, CSc.**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Jaroslav Bošeľa ***ID:*** 173617
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Laboratorní dohledový systém

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte řešení uceleného dohledového systému pro laboratoř transportních sítí. Součástí je revize stávajícího řešení, návrh a implementace řešení nového včetně konfigurace síťových zařízení a dohledového systému. V teoretické části porovnejte v současné době dodávaná řešení z licenčně dostupných pro akademické použití. Popište jej a vyberte nejvýhodnější řešení z hlediska použitelnosti pro laboratorní účely. V praktické části navrhněte síťovou strukturu dohledové sítě, její konfiguraci a proveďte implementaci vybraného řešení.

DOPORUČENÁ LITERATURA:

[1] DOOLEY, K., BROWN, I.J. Cisco IOS cookbook. 2nd ed. (Revised and updated). Sebastopol, CA: O'Reilly, c 2007. ISBN 9780596527228.

[2] PUŽMANOVÁ, R. Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 8025112780.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 29.5.2018

Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.
Konzultant: Ing. Václav Oujezský, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto bakalárska práca sa zaoberá riešením dohľadového monitorovacieho systému pre školské laboratórium. Popisuje laboratórne prvky, ich účel a stav pred aplikovaním konfigurácie, zároveň obsahuje porovnanie komerčných dohľadových systémov a výber jedného ktorý bol aplikovaný. Podstata práce je zameraná na protokol SNMP a jeho využitie pri monitorovaní laboratórnej siete. V praktickej časti práce je vytvorená konfigurácia dohľadového systému, ktorý je aplikovaný v sietí laboratória a zabezpečuje tak monitoring a dohľad nad sieťovým laboratóriom.

KĽÚČOVÉ SLOVÁ

Monitoring, dohľadový systém, VLAN, IP, PRTG, SNMP, Trap, Cisco, prepínač, smerovač

ABSTRACT

This bachelor thesis deals with network monitoring solution for school laboratory network. Describes the laboratory network devices, their purpose and condition before applying configuration, it also contains a comparison of commercial supervision network systems and the choice of one that has been used. The essence of the thesis is focused onto SNMP protocol, its use in laboratory network monitoring. In the practical part of the thesis is created the system supervision configuration, which is applied into laboratory network and ensures the supervision and monitoring for whole laboratory network.

KEYWORDS

Monitoring, supervision system,VLAN, IP, PRTG, SNMP, Trap, Cisco, switch, router

BOŠEĽA, Jaroslav. *Laborátorní dohledový systém*. Brno, 2018, 65 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: doc. Ing. Vladislav Škorpil, CSc.

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Laborátorní dohledový systém“ vypracoval(a) samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Vladislavovi Škorpilovi, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Rovnako bych rád poděkoval konzultantovi práce Ing. Václavovi Oujezskému, Ph.D, za veľmi podnetné návrhy, pomoc s pochopením topológie laboratória, trpezlivosť, odbornú pomoc a rady k vypracovaniu práce.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno ....

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM VÝPISOV

ÚVOD

V modernej dobe sledujeme trend veľmi rýchleho rastu sieťovej prevádzky a nárast počtu sietí ako takých. Tento trend so sebou nesie rovnako aj potrebu smerovania toku dát cez viaceré uzly alebo zariadenia , a zároveň vyžaduje dostupnosť služieb pre túto prevádzku. Vznikajú kancelárske, výučbové, laboratórne(experimentálne), domáce a iné siete, rôznych veľkostí od pár zariadení až po niekoľko sto zariadení a smerovacích uzlov. Napríklad experimentálne(laboratórne) siete častokrát majú len jedno spojenie do vonkajšej siete - Internetu a aj to hlavne z dôvodu bezpečnosti špecifických služieb, vzdialenej správy alebo z potrieb iných služieb bežiacich na týchto separovaných sieťach ale aj na otvorených vonkajších sieťach.

Dostupnosť jednotlivých služieb v týchto sieťach musí byť pre potreby užívateľov v týchto sieťach zabezpečená a rovnako s rastom objemu dát rastie aj potreba údržby a prevádzkyschopnosti týchto zariadení a zároveň ich monitorovanie. Dôležitým aspektom je udržanie týchto sietí v plnej prevádzke, predchádzanie zlyhaniam a zabezpečená rýchla oprava, poškodených častí alebo služieb. Rovnako je dôležité vedieť informácie o prevádzke na týchto sietí z dôvodu optimalizácie, plynulého chodu, bezpečnosti a dostupnosti služieb.

Na tento účel sa dnes využíva komplexný sieťový manažment(network management), ktorý má za úlohu práve bezchybnú prevádzku na sieťach, detekovanie chýb, zlyhaní a zvyšuje bezpečnosť na týchto sieťach.

Jednou z najdôležitejších častí sieťového manažmentu sú monitorovacie nástroje, sú to nástroje komplexne vyvinuté na to aby uľahčovali prácu sieťovým administrátorom, zabezpečili rýchlu detekciu chýb, nefunkčných služieb, protokolov alebo sieťových prístrojov. Tieto nástroje rovnako zvyšujú zabezpečenie týchto sietí, je nimi možné zistiť pripojenia, používané protokoly a služby, a rovnako či sú tieto pripojenia zabezpečené.

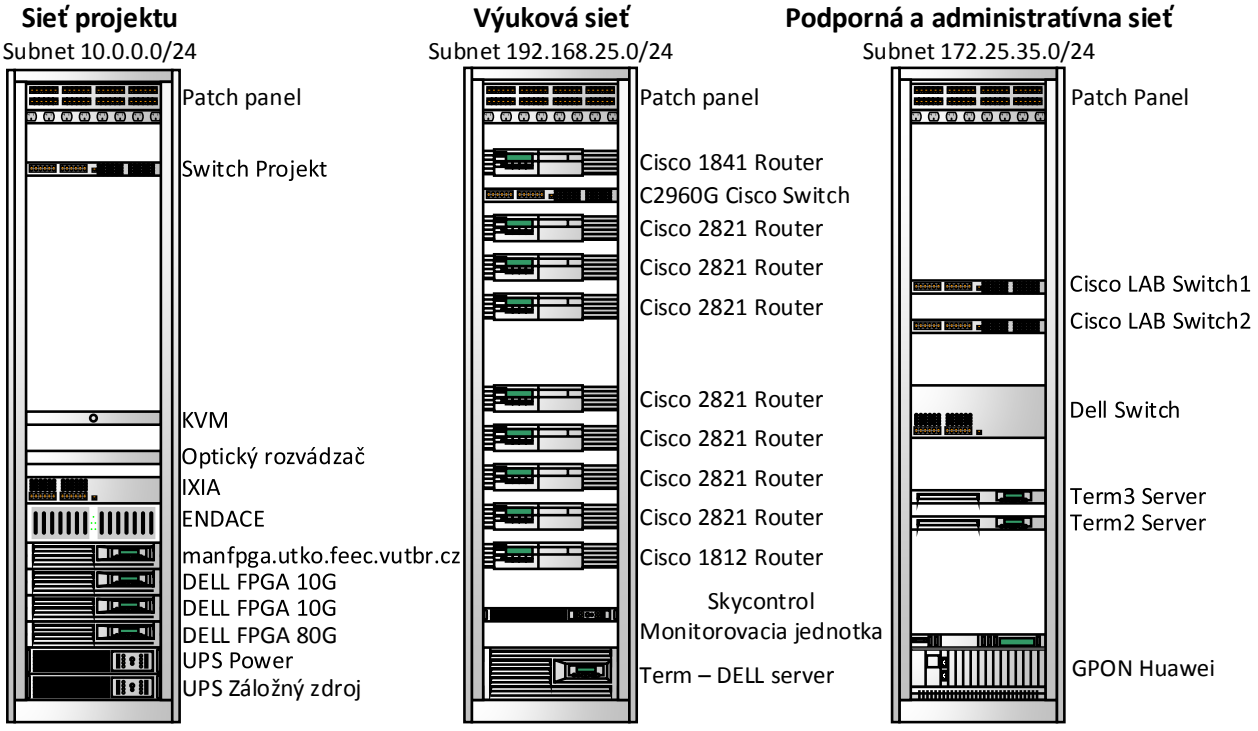
Táto práca sa zaoberá praktickým aplikovaním monitorovacích nástrojov, porovnaním dostupných nástrojov, úpravu a zlúčením experimentálnych sietí do jedného monitorovacieho nástroja pomocou VLAN (virtuálna lokálna sieť – Virtual Local Area Network), popisom jednotlivých sietí a ich účelu, a popisom protokolov ktoré tieto monitorovacie nástroje používajú a kontrolujú.

1 REVÍZIA PÔVODNEJ KONFIGURÁCIE LABORATÓRNEJ SIETE

V rámci bakalárskej práce sme začali s revíziou dovtedajšieho riešenia laboratória. Jedná sa o výukové a experimentálne laboratórium Transportných sítí SC 5.35 nachadzajúce sa na Fakulte Elektrotechniky a Komunikačných technológií, Vysokého Učení Technického v Brne. Požiadavka práce bola popísať doterajšie riešenie v laboratóriu, popísať monitorovanie týchto sietí, použité protokoly a konfiguráciu.

Výukové(experimentálne laboratórium) je tvorené viacerými sieťami, ktoré je potreba monitorovať a zabezpečiť tak bezchybný chod týchto laboratórií, jednotlivých zariadení a služieb v týchto sieťach pomocou monitorovacích a manažmentových protokolov, senzorov a konfigurácií. V laboratóriu prebieha viacero výukových a experimentálnych činností, ktoré môžu byť výpadkom obmedzené.

Laboratórium Transportných sítí tvoria základné tri separované siete, čo môžeme vidieť na obrázku 1.1, ktorých zariadenia sú rozdelené v troch stojanoch(rackoch) ktoré sú pomocou prepojovacích(patch) panelov prepojené tak aby bolo možné vzdialene pristupovať na prvky týchto sietí.



Obr. 1.1: Usporiadanie jednotlivých sieťových prvkov v stojanoch(rackoch)

V sieťach je prítomných aj viacero virtuálnych serverov a klientov, ktoré bežia na fyzických zariadeniach a sú využívané ako v projekte ktorý v laboratóriu prebieha, rovnako tak aj na výuku, podporu databáz a základného klientského manažmentu siete - DHCP, DNS, FTP. Najväčším problémom zapojenia týchto sietí je to, že prvky nie sú praktický monitorované a nie je možný rýchly zásah v prípade zlyhania prvkov, rovnako je problém aj to že na jednoduché overenie funkčnosti jednotlivých prvkov v sieťach je potrebné zdĺhavé prihlasovanie sa na jednotlivé terminálové počítače odkiaľ je povolený prístup na jednotlivé prvky a siete.

Takéto riešenie výrazne predlžuje čas za ktorý je možné jednotlivé chybné prvky siete alebo chyby v konfigurácií detekovať a vyžaduje sa prakticky vždy zásah sieťového administrátora, ktorý musí absolvovať zdĺhavé procesy na zisťovanie funkčnosti jednotlivých sietí alebo prvkov. Tento problém je zreteľný najmä v čase výuky alebo práce na jednotlivých projektoch kedy môže dojsť k výpadku niektorých zariadení na analýzu sieťovej prevádzky, poprípade k chybe na prepínačoch alebo smerovačoch, ktoré tieto informácie smerujú ku koncovým užívateľom alebo študentom. Podobný prípad môže nastať priamo v čase výuky, kedy môže dôjsť k výpadku virtuálnych klientov, databáz, poprípade stratu spojenia na smerovače, cez ktorý študenti pristupujú k jednotlivým úlohám alebo využívajú pomocné nástroje, ktoré sú dostupné práve na týchto virtuálnych systémoch poprípade sieťových prvkoch. Takýto prípad výpadku znamená, že v dovtedajšom riešení nebolo v silách a možnostiach človeka pracujúceho v laboratóriu, poprípade vyučujúceho aby bol schopný zistiť kde nastal problém a urgentne reportovať tento problém sieťovému administrátorovi, už len s ohľadom na problematiku znalosti hesiel a prístupových(terminálových) počítačov k jednotlivým zariadeniam, celkovej topológie siete a bežiacich služieb.

Z tohto dôvodu sa po konzultácií so sieťovým administrátorom laboratória Transportných sítí, dospelo k riešeniu porovnať a vybrať ucelený monitorovací softvér, ktorý pobeží na jednoduchom monitorovacom servery, ktorý bude zároveň prepojený na každú separovanú sieť a bude teda zabezpečovať zber údajov a monitorovacích protokolov aj od jednotlivých prvkov danej siete.

Toto riešenie prinieslo celistvosť v monitorovaní a zabezpečilo dostupnosť všetkých sietí v laboratóriu, jednotlivých bodov a prvkov z jedného centrálneho bodu. Aby tento centrálny bod, monitorovací server, mohol zabezpečovať takúto dostupnosť, bolo potrebné pristúpiť ku konfigurácií, ktorá by zabezpečila dostupnosť týchto sietí a zariadení v nich. Konfigurácia je založená na prepojení sietí pomocou VLAN (virtuálna lokálna sieť – Virtual Local Area Network), ďalšie monitorovanie a získavanie funguje pomocou manažmentových protokolov a protokolov na overenie dostupnosti, rozsiahlejšie informácie v kapitole implementácia riešenia.

1.1 Typy Laboratórnych sietí

1.1.1 Školská Výuková sieť Cisco

Jednu z troch navzájom prepojených sietí v laboratóriu tvorí výuková Cisco sieť. Táto sieť slúži na prístup k viacerým výukovým úlohám a zabezpečuje predpripravenú konfiguráciu pre jednotlivé úlohy v Cisco IOS. Tvorí ju sedem smerovačov integrovaných služieb – Cisco 2821 obrázok 1.2, jeden Cisco 871 smerovač, jeden Cisco 1812 smerovač a jeden Linuxový server, na ktorých bežia konfigurácie k výukovým úlohám ako napr. - MPLS (Multiprotokolové značkované prepínanie – Multiprotocol Label Switching), MGCP(Kontrolný protokol brány médií – Media Gateway Control Protocol), TFTP(Jednoduchý protokol na prenos súborov – Trivial File Transfer Protocol), VoIP(Prenos hlasu Internetovým protokolom – Voice over Internet Protocol) a sú pripojené k hlavnému prepínaču Cisco C2960G, ktorý spojuje všetky siete laboratória a zároveň je trunk VLAN linkou spojený na monitorovací systém kde dochádza k prepínaniu troch VLAN z troch hlavných sietí a tieto VLAN spojenia v sebe nesú ako normálne dátové pakety tak aj pakety, ktoré nesú nami nadefinované monitorovacie a manažmentové protokoly. Na realizáciu jednotlivých laboratórnych úloh sa na pripojenie používa Cisco 1841 smerovač, ktorý je pomocou VLAN spojený s Cisco prepínačom C2960G, ktorý zároveň posiela kontextové menu na smerovač 1841, kde dochádza k výberu jednotlivých úloh podľa zadania vyučujúceho a tým k pripojeniu sa ku konkrétnej úlohe.

Obr. 1.2: Cisco 2821 Smerovač Integrovaných služieb

1.1.2 Sieť externého projektu

Sieť vytvorená a prioritne používaná na účely externých projektov, simulácie sieťových prvkov a ich správania, analyzovania sieťovej prevádzky. Tvorí ju niekoľko hlavných vysokorýchlostných sieťových nástrojov:

- **ENDACE** - Analyzátor sieťovej prevádzky. Hlavné funkcie sú zachytávanie, následné ukladanie a súvislé preposielanie dátového toku cez jeho 10Gb/s

linku. Analyzátor je schopný uložiť až 10 minút 10Gb dátového toku v obojsmernej plnej prevádzke(full duplex), zároveň je možné filtrovať všetky typy dátovej prevádzky vo všetkých vrstvách RM OSI(Otvorený systém prepojení Referenčný Model – Open Systems Interconnection Reference Model) a filtrovať ju cez užívateľský definované(user defined) filtre. [1]

- **GPON** - Gigabytová Pasívna Optická sieť. V školskom laboratóriu sa využíva šasi Huawei MA5683T, jedná sa o centrálnu jednotku GPON OLT(Optický linkový terminál – Optical Line Terminal), ktorá slúži ako poskytovateľ služieb a koncový bod pasívnej optickej siete, pasívnej preto lebo v nej nie je potreba využívať ďalšie aktívne napájané sieťové prvky medzi ústredňou a koncovým užívateľským prevodným zariadením, ktoré môže byť ONT(Optický sieťový terminál – Optical Network Terminal) čo je zariadenie priamo u užívateľa alebo zákazníka alebo môže byť medzi OLT spojený s medziľahlým bodom ONU(Optická sieťová jednotka – Optical Network Unit). [2]
- **FPGA)** - Vývojový server FPGA COMBO-SET 10G/40G/100G INVEA-TECH, je systém prevažne navrhnutý na výskum 10Gb/s aktívnych sieťových zariadení, hlavne výskum algoritmov pre smerovanie, prepínanie, odovzdávanie paketov a filtrovanie sieťovej prevádzky a jej zrýchlenie. Systém tvoria 3 sieťové vývojové dosky FPGA(Pole Programovatelných hradiel – Field Programmable Gate Array), každá doska je uložená na vlastnom DELL servery, na ktorom bežia dva virtuálne systémy CentOS Linux a MS Windows 2008 R2 Datacenter v Hyper-V. [3]

1.1.3 Podporná administratívna sieť

Tretia sieť ktorá v laboratóriu zastáva úlohu podpornej a virtualizačnej siete pre projekt a vyúku. V tejto sietí sa nachádzajú viaceré zariadenia a servere, ktoré zaisťujú prostriedky pre virtualizáciu systémov, administráciu týchto systémov, služby sieťových protokolov, vzdialených úložísk a simulačných prostriedkov pre výuku. Významnú rolu tu zaujímajú hlavne tri terminálové servery, senzorický monitorovací systém, prepojovací prepínač DELL, virtuálna platforma BIG IP a dva Cisco prepínače.

Prepojovací prepínač DELL - je hlavným prepojovacím prvkom medzi zariadením GPON, podpornou sieťou a sieťou projektu, je pripojený priamo na prepojovací panel.

Terminálové servere :

1. **Term1** je server na ktorom bežia viaceré virtuálne systémy, jedným z nich je aj Windows 10 na ktorom bežia podporné aplikácie pre Cisco úlohy, menovite Cisco network Assistant, Cisco Configuration Professional, ďalej sa tu

nachádza TFTP Server na zálohovanie konfiguračných súborov, laboratórne aplikácie VKS a PTS, GNS3, rovnako tu bežia služby DHCP a NAT .

2. **Term2** je konzolový server pre administratívnu podporu výuky a vývoja, beží tu ESXi server a databázový systém.
3. **Term3** najhlavnejším prvkom ktorý tu beží je softvérové riešenie F5 BIG-IP. Obidva konzolové servery Term2 a Term3 sú virtualizované na architektúre Supermicro server management.

F5 BIG-IP - BIG-IP je softvérové a hardvérové riešenie pre podporu aplikácií, kontroly prístupu a bezpečnostných riešení. Výrobca BIG-IP, ponúka ako hardvérové riešenie v podobe šasi s propietárným softvérom a systémom alebo ako vlastné virtualizované softvérové riešenie ktoré sa nachádza vo výukovom laboratóriu.

BIP-IP Softvér je skupina licencovaných modulov, ktoré bežia na vrchu vlastného systému F5 Traffic Management Operation System(TMOS). Tento vlastný operačný systém bol špeciálne navrhnutý na kontrolu prevázky siete a aplikácií a aby bol zároveň schopný vykonávať rozhodnutia v reálnom čase založené na základe poskytnutej konfigurácie. Virtualizované systémy poskytujú funkcionalitu BIG-IP softvéru tam kde nie je možná hardvérová implementácia [4]. Tento prípad je implementovaný vo vývojovom laboratóriu kde systém BIG-IP beží na virtuálnom servery Term3 a je súčasťou laboratórnej úlohy. BIG-IP hlavné softvérové moduly:

- **BIG-IP Local Traffic Manager(LTM)** - je modul poskytujúci platformu na vytváranie virtuálnych serverov, výkonnostných služieb, protokolov, autentizačných služieb a bezpečnostných profilov na definovanie tvaru vlastnej aplikačnej prevádzky. Veľké množstvo ďalších BIG-IP modulov využíva LTM modul ako základ pre rozšírené služby.
- **BIG-IP DNS** - pôvodne Global Traffic Manager, BIG-IP DNS poskytuje podobné vlastnosti pre bezpečnosť a rozdelenie záťaže(load balancing) ako LTM, avšak v globálnom merítku. BIG-IP DNS ponúka služby na distribúciu a zabezpečenie DNS prevádzky, ktorá nesie priestor pre názvy vlastných aplikácií.
- **BIG-IP Access Policy Manager (APM)** - Poskytuje federáciu, SSO(Single Sign-On), aplikačné prístupové pravidlá a zároveň zabezpečenie webového tunelu. Rovnako ponúka rozprestretý prístup k rôznym aplikáciam, virtualizovaným desktoptovým riešeniam a VPN(Virtual Private Network) tunelom.
- **Secure Web Gateway Services(SWG)** - Je spárovaný s APM, SWG umožňuje kontrolu prístupu k použitiu internetu. Je možné povoliť, blokovať, overovať a vytvárať logy z prevádzky za pomoci APM prístupových práv, zároveň služba ponúka flexibilitu pri používaní naprieč internetom a webovými aplikáciami.
- **BIG-IP Application Security Manager(ASM)** - Web aplikačné firewal-

lové(WAF) riešenie od F5, založené na tom že tradičné firewally a ochranné mechanizmy na tretej vrstve nie sú schopné pochopiť zložitosti veľkého množstva web aplikácií, preto ASM dovoľuje prispôsobenie prijateľného a očakávaného správania na základe každej aplikácie. Zero-Day útoky, DoS útok, podvodné klikanie sa spoliehajú práve na neschopnosť tradičného bezpečnostného mechanizmu chrániť unikátne potreby aplikácií, preto ASM vypĺňa medzeru medzi tradičnými ochrannými mechanizmami - firewallom a prispôsobenou aplikačnou ochranou.

- **BIG-IP Advanced Firewall Manager(AFM)** - AFM je navrhnuté na redukciu hardvéru a extra skokov v prípade, že ADC(Appilication delivery controller) je spárovaný s tradičným firewallom. AFM pracuje na tretrej a štvrtej vrstve na ochranu prevádzky smerujúcej do data centra, spojením s ASM je možné implementovať ochranu služieb na úrovní L3 až L7 vrstiev pre komplexné riešenie bezpečnosti a ADC v jednom zariadení alebo virtuálnom prostredí. [4]

Senzorický monitorovací systém SkyControl – V laboratóriu Transportných sítí sa nachádza vzdialená monitorovacia jednotka SC8100 od spoločnosti Skycontrol. Je to systém priestorového monitorovania zariadení, narušenia priestorov a podmienok v týchto priestoroch. Za pomoci senzorov je možné takouto jednotkou merať teplotu, detekovať dym, úniky vody, pokles napätia a rôzne iné. Jednotka SC8100 je plne kompatibilná s radou senzorov od spoločnosti Skycontrol a ponúka tak celistvé riešenie pre priestorový, prístupový a bezpečnostný monitorovací systém.

Systém SC8100 ja založený na OS Linux, beží na CPU jednotke iMX257 a úložné miesto je možné rozšíriť SD kartou. Je plne kompatibilný s TCP/IP, monitoring je založený na nízkoenergetickom web servery, ktorý zahŕňa HTTPS(SSL), SMTP, DHCP, SNMP(podporované v1, v2c, v3), FTP, Syslog, LDAP, Radius. Systém je vybavený HTLM5 GUI rozhraním. Zariadenie obsahuje dva CAN RJ12 porty a 8 analógových senzorových ethernet portov, zariadenie môžeme vidieť na obrázku 1.3.

Obr. 1.3: Monitorovacia jednotka Skycontrol SC8100

2 POROVNANIE MONITOROVACÍCH SIEŤOVÝCH NÁSTROJOV

Dnešné prepojené siete vyžadujú stály sieťový dohľad a z toho dôvodu je na trhu veľké množstvo sieťových monitorovacích nástrojov a softvérov. Sieťový monitorovací softvér poskytuje základnú líniu na sledovanie celkovej výkonnosti siete, je schopný detekovať problémy plynúce z preťaženia siete alebo problémy v rámci serverov a sieťového pripojenia. Monitorovací softvér sa rovnako používa aj na ďalšiu radu činnosti medzi ktoré patrí napríklad : meranie času odozvy, konzistencie siete, spoľahlivosti siete a jej uzlov, a rovnako aj celkovú prevádzku siete založenej na reálnom čase a historických dátach.

Monitorovanie siete prináša množstvo benefitov z ktorých môže IT sieťový administrátor ťažiť z výhod ako je úspora času, nákladov na opravu siete a s tým znížených výpadkov siete a služieb na týchto sieťach bežiacich. Ak sieť vypadne alebo dôjde k neočakávanej odchýlke od základného nastavenia siete je administrátor upozornený, čím sa znižuje čas a vážnosť na ďalšiu opravu siete alebo únik dát. Monitorovacie nástroje umožňujú vizualizovať ako dáta tak aj zariadenia pre lepšie pochopenie sieťovej architektúry, tok dát a zaťaženie jednotlivých zariadení alebo uzlov. U množstva softvérov je možné vytváranie vlastných sieťových máp, kde je možné definovať vyčlenené skupiny prvkov alebo sietí, ktoré majú byť v mapách zobrazené a zároveň je možné vzdialene posielanie ako webové odkazy a tým sa umožňuje základná kontrola siete aj iným užívateľom ako je vyhradený sieťový administrátor.

Monitorovacie softvéry majú podobnú funkčnosť ako softvér na meranie výkonnosti služieb aplikácií, avšak sieťový monitorovací softvér je aplikovaný na celú sieť narozdiel od konkrétnej webovej aplikácie a zároveň je možné prepojenie monitorovacieho softvéru s monitorovaním aplikácie a využívaním týchto dát.[5]

2.1 Kvalitatívne požiadavky na sieťový monitorovací softvér

Konštantné monitorovanie výkonu celej siete – Neustále sledovanie definovaných parametrov a celej siete v reálnom čase, sledovanie reálnej prevádzky, toku dát, zaťaženia a výpadkov jednotlivých služieb a protokolov, zariadení alebo celej siete.[5]

Vytvorenie základnej metriky na monitoring siete – V základnom ponímaní ide o skupinu metrík(atribútov) ktoré sú použité pri monitorovaní siete a definujú správanie siete a zariadení pri normálnych podmienkach. Použitie základnej metriky

respektíve základnej línie sieťového výkonu dovoľuje porovnávať a zachytávať zmeny v sieti a identifikovať tak problém. Ďalšia výhoda plynúca z nastavenia základnej metriky siete je možnosť skorého odhalenia kapacity siete pre sieťové požiadavky rôznych aplikácií a tým plánované navýšenie kapacity v budúcnosti. Spojením základnej línie výkonnosti s existujúcimi systémami SLA(servis level agreements) môžu pomôcť sieti udržať sa v rámci kapacitných parametrov definovaných pre špecifické služby(prenos hlasu, špecifické protokoly) a zároveň identifikovať tieto výkonnostné problémové oblasti. Príklad základnej výkonnostnej línie môžeme nájsť u výrobcu Cisco, ktorý neodporúča viac ako 60% využitie procesora na smerovačoch, pri prekročení posiela SNMP správy na monitorovanie tejto štatistiky. Nastavenie základnej výkonnostnej línie sa prevádza pomocou analyzovania prevádzky na sieti počas behu na sieťovej infraštruktúre pri zaťažením bežnými užívateľmi a službami.

Celkový obraz o výkonnosti siete je použiteľným indikátorom zdravia siete avšak nedokáže rozpoznať využívanie jednotlivých služieb, to by mohlo byť dosiahnuté len zbieraním a analyzovaním jednotlivých balíčkov dát a paketov, čo by spôsobilo veľké zaťaženie siete. Z tohto dôvodu sa využívajú protokoly NetFlow alebo sFlow, ktoré sú navrhnuté na to aby boli menej náročné na ukladanie zachytenej sieťovej prevádzky a aj to len v určených intervaloch. NetFlow/sFlow sú použité v mnohých smerovačoch a sú schopné prenášať vzorkované zachytené dáta na monitorovanie v sieti, bez toho aby zaťažili paketový zachytávač(sniffer) a zároveň poskytli relevantné údaje o používaní siete jednotlivými službami a aplikáciami. Analýza týchto dát ďalej umožňuje priradiť percentuálne využitie siete jednotlivým aplikáciam v porovnaní s celkovým využitím siete. [6]

Upozornenie administrátora v prípade výpadku siete, zariadení alebo odlišnosti od normálnej prevádzky – V podstate ide o okamžité reakcie a zároveň notifikácie pri zmene siete a jej nastavenia smerom k sieťovému administrátorovi, prípade mechanizmom ktoré okamžite upozornia administrátora na zmeny(emailová notifikácia, aktualizácia webového rozhrania, poprípade vzdialeného webového odkazu nesúceho alarmy, sondy a mapy sieťovej infraštruktúry).

Návrh riešenia v prípade vzniku výkonnostných problémov – Monitorovací softvér by mal byť schopný odhaliť neúmerné zaťaženie siete, portov, poprípade prílišne prekročenie využitia procesorov, diskov a iných periférií a navrhnúť aspoň najzákladnejšie riešenie ako zväčšenie priepustnosti portov, zmena prevádzky na portoch a sietí a iné.

Vizualizácia výkonnostných dát siete a vizualizácia sieťovej infraštruktúry – Softvér by mal byť schopný graficky zobrazovať zaťaženie siete, celkový čas výpadku siete aj jednotlivých senzorov a zariadení. Tieto dáta ďalej prevádzať na rôzne formy grafov a ukazovateľov, s ktorými je možné ďalej pracovať, zisťovať preťaženia, výpadky jednotlivých služieb, čas ich odozvy a spätné historické dáta. Ďalšou

funkciou ktorou by mal disponovať je vizualizácia sieťovej infraštruktúry, jednoduché pridávanie zariadení, ich zmysluplný prehľad v systéme a vytváranie máp sieťovej infraštruktúry, vlastných aj základných pre rôzne špecifické služby, oddelené siete alebo zariadenia.[5]

2.2 Komerčne dostupné monitorovacie softvéry

SolarWinds Network Performace Monitor – Sieťový monitorovací softvér od firmy SolarWinds, využíva riešenie typu „všetko zobrazenie v jednom okne“, čo znamená že všetky prispôsobené webové okná, tabuľky a grafy sú zobrazované v jednom okne na jednom prístupnom mieste. Samozrejmosťou je webové rozhranie odkiaľ je možné plná funkcionalita. Všetky výkonnostne údaje siete sú rozložené v ľahko čitateľnom zobrazení, je možné ich upravovať podľa špecifických preferencií topológie, potrieb a odlišnosti siete.

Produkt od firmy SolarWinds je schopný automatický zisťovať a mapovať sieťové zariadenia pomocou SNMP, zároveň zbierať sieťové informácie a formovať ich do detailného sieťového súpisu. Takéto riešenie uľahčuje tradičnú prácu, kedy je potrebné zariadenia ručne vyhľadávať a mapovať, čo je časovo náročné a vyžaduje to dodatočný softvér na zápis. SNMP môže ďalej použiť tieto informácie na posúdenie zariadení a získanie chýb, dostupnosti a výkonnostnej metriky u týchto zariadení, SNMP tak monitoruje zdravie každého zariadenia na ktorom je to povolené.

Využitie automatického mapovania siete sa prejaví hlavne pri zmene siete, doplnení alebo výmene zariadení, kedy odpadá povinnosť tieto zmeny ručne zapisovať. SolarWinds dokáže zmeny automatický sledovať, zapisovať ich do máp aj grafov, tým sa docieli stále aktuálna topológia bez ohľadu na zmeny siete, zároveň dokáže automatický zisťovať L2/L3(Spojenia na 2 vrstve/Spojenia na 3 vrstve) spojenia medzi zariadeniami a umožňuje vizualizovať využitie spojenia a tak prispôsobiť konkrétne spojenie požiadavkam siete. V praxi to znamená, že táto vizualizácia napomáha zistiť, ktoré časti vyžadujú viac zariadení alebo ktoré časti siete práve vyžadujú menej sofistikovanejšie zariadenia. Týmto spôsobom sa redukujú náklady a optimalizujú sa zariadenia pre jednotlivé časti siete. Softvér je schopný spracovať IP SLA reporty, Syslogy a vytvárať vlastné MIB definované databázy, ďalej disponuje inteligentnými alarmami, podporu pre bezdrôtovú prevádzku a vizualizáciu pokrytia bezdrôtového signálu, implementáciu protokolov multi-výrobcov do monitoringu a vizualizácia hlavných kritických ciest pomocou hop-by-hop analýzy. Samozrejmosťou je telefonická, emailová a tiketová technická podpora a zákaznícke služby. Softvér je široko používaný množstvom firiem a spoločnosti a ide o jeden z najpoužívanejších komerčných riešení monitoringu.

Nevýhody softvéru sú: obmedzená časová funkcionalita voľnej verzie, cena, a z pohľadu práce mierne zložitejšie nastavovanie jednotlivých manažmentových protokolov, menej prehľadné hlavné okno a hardvérová náročnosť, rovnako inštalácia hlavného core serveru je možná len na OS Windows(klientský agent možný aj na Linux).

Nagios Core – Open source sieťový monitorovací softvér schopný monitorovať väčšinu hlavných protokolov (HTTP, FTP, SSH, SMTP, POP3, SNMP, MySQL). Je to voľný softvér bežiaci pod podmienkami GNU General Public License verzie 2 a je publikovaný FSF(Free Software Foundation). Softvér je vytvorený na Linuxovom jadre a serverová časť beží na Linuxe, avšak dnes je možné ho inštalovať aj na iné Unixové varianty, klientská časť funguje aj pre Windows systémy. Softvér sa inštaluje pomocou príkazového riadku v Linuxe, celkovo je náročnejší na modifikácie a nastavenie. Modifikácie systému sú založené na vytvorených pluginoch ktoré sa aplikujú na klientské a serverové časti a tak dovoľujú rôzne formy monitoringu. Pomocou pluginov je možné monitorovať sieťové služby (SMTP, HTTP, ICMP, SNMP, FTP a iné), monitorovať výpočtové zdroje (využitie procesora, využitie disku, systémové logy) na hlavných operačných systémoch, monitorovať teplotné senzory, priestorové alarmy, príkazy, odozvy a stavy.

Vzdialené monitorovanie prebieha cez SSH alebo SSL kryptované tunely a je možné pomocou Nagios Remote Plugin Executor, čo je zavádzač ktorý spúšťa skripty na vzdialenom systéme. Nagios Core je flexibilný, nenáročný systém ktorý je možné prispôsobiť podľa vlastných preferencií, pomocou pluginov a zavádzačov je možné ho používať a monitorovať aj Windows systémy ako klientov, avšak je k tomu potrebný monitoring agent, čo je aplikačné programové rozhranie vyvinuté na komunikáciu medzi rôznymi operačnými systémami.

Nagios Core je vhodný pre menšie podnikové siete, nie je schopný autodetekcie sieťových prvkov a každú zmenu je treba ručne aktualizovať, prepisovať pluginy do špecifickej podoby a upravovať kód. Má jednoduché webové rozhranie, kde je možné zistiť stav siete, notifikácie, históriu výpadkov, súbory logov. Softvér je pomocou pluginov schopný posielať rôzne notifikácie o výpadkoch, rovnako je možné definovať grafické zobrazenie dát a vytvárať mapy siete. Softvér je nenáročný na hardvér, má dnes už množstvo vytvorených pluginov, má voľnú licenciu a je možné si ho kompletne pomocou vlastných definovaných pluginov meniť do špecifickej podoby. Pri správnom nakonfigurovaní pluginov je však systém stabilný a optimalizovaný aj pre väčšie siete.

Nevýhody softvéru sú: náročnosť na konfiguráciu a funkčnosť softvéru, serverová inštalácia na Linuxové/Unixové systémy, potreba množstva pluginov na bežné monitorovanie, nemožnosť autodetekcie zmien a tým pracné programovanie zmien v pluginoch , menej prehľadné webové rozhranie a menej fungujúca podpora.

Spiceworks Network Monitor – Monitorovací softvér od spoločnosti Spiceworks, založený na bezplatnej licencií, vhodný aj do akademického prostredia. Ponúka monitorovanie siete a štatistiky v reálnom čase pre servery a sieťové zariadenia pomocou SNMP. Monitorovací softvér beží na rozličných verziách OS Windows, inštalácia prebieha v pár krokoch a je jednoduchá. Na prihlásenie do monitorovacieho systému sa vyžaduje Spiceworks účet pozostávajúci z mena, heslá a emailovej adresy. Pri prihlásení sa zobrazí základné monitorovacie okno na vrchu kde môžeme vidieť maximálne tri okná s alarmami na zariadeniach, na ľavej strane sa nachádza zoznam serverov s grafickým vyjadrením ich zdravia(využitie procesora, využitie disku, zaplnená operačná pamäť, aktívne sieťové adaptéry), napravo sa nachádza zoznam sieťových zariadení, kde sa opäť nachádza grafické vyjadrenie jednotlivých monitorovaných parametrov sieťových zariadení(prepínače, smerovače), na spodnej strane základého okna sa nachádza priestor kde je možné definovať ďalšie vlastné zariadenia, avšak nie je tu už priestor pre grafické zobrazenie jednotlivých parametrov, je možný len zoznam ktorý zobrazuje status zariadenia a to či je dostupné alebo ide o výpadok. Všetky zariadenia môžeme vidieť v karte Devices(zariadenia), kde nájdeme všetky zariadenia, ich stavy a parametre.

Softvér je schopný monitorovať 26 rôznych parametrov pre každé zariadenie, ktoré sú rozdelené do piatich kategórií : pripojené zariadenie, CPU, Disk, a sieť. Takto je možné monitorovať špecificke podmienky ako napríklad : vysoké zaťaženie procesora, výkyvy v použití operačnej pamäti, málo miesta na disku, a nedostatky v sietí. Nemá schopnosť monitorovať špecifické procesy a hoci softvér má veľa možnosti upozornení nie je tu možnosť vytvorenia vlastných alarmov pre špecifické chybné stavy, je možná len zmena parametrov na už definovaných upozorneniach.

Riešenie od Spiceworks neponúka autodetekciu alebo mapovanie siete a je potreba ďalšieho mapovacieho softvéru od Spiceworks. Spiceworks Help Desk je ďalším nástrojom, ktorý na seba preberá úlohu tiketovacieho systému pre monitorovanie siete a overovanie užívateľov a nie je súčasťou sofvéru Network Monitor, a je potreba ho doinštalovať. Monitorovací softvér od Spiceworks je spoľahlivý, rýchly systém, ktorý má jednoduché nastavenie a má prehľadné spracovanie.

Nevýhody softvéru sú : nemožnosť definovať si vlastné upozornenia, mapovanie siete je možné len s ďalším softvérom, rovnako aj vytváranie tiketov s alarmami pre rôznych užívateľov, zároveň má softvér obmedzené možnosti monitorovania a zobrazuje reklamy. Samotná spoločnosť Spiceworks softvér doporučuje ako riešenie pre siete s najviac 25 monitorovanými zariadeniami, teda je vhodný len pre menšie siete.

PRTG Network Monitor – Monitorovací softvér od nemeckej spoločnosti Paessler AG. Softvér má voľnu verziu na 100 monitorovacích sond, teda je vhodný do malých sietí alebo do menšej laboratórnej siete a dá sa využívať v akademickom prostredí. Softvérové riešenie sa zameriava hlavné na sieťový monitoring a jednotný manažment infraštruktúry. PRTG umožňuje monitorovať sieťové zariadenia ako prístupové body, smerovače, prepínače, rozbočovače, servery, tlačiarne, záložné zdroje a pracovné stanice. Softvér ďalej disponuje monitorovaním softvéru a infraštruktúry nasadzovanej v cloude vrátane aplikácií, serverových služieb a ukladacích priestorov. Dokáže monitorovať zariadenia pomocou množstva protokolov a preddefinovaných sieťových monitorovacích senzorov veľkého množstva výrobcov(Cisco, Dell, Windows a iný.), ktoré sú špecifické priamo pre zariadenia týchto výrobcov a vo veľkej miere tak uľahčuje prvotné nastavenie.

Architektúra systému PRTG zahŕňa aspoň jeden hlavný server so sondami nasadenými v celej sieti. Systém nevyžaduje žiadneho obsluhujúceho agenta pre jednotlivé zariadenia, jediné čo sa vyžaduje sú prípadné prihlasovacie údaje a nastavenie SNMP protokolu. Funkcia automatického vyhľadávania sa postará o nájdenie väčšiny zariadení v sietí a utvorení základnej hierarchie monitoringu a topológie siete. Centrálny server PRTG obsahuje inštaláciu lokálnej sondy(monitorovací server), vlastnú databázu, webový server, systém výpisov(report system), notifikačný systém, definície objektov pre MIB tabuľky využité pre SNMP protokol, systém senzorov a ďalšie hlavné súčastí ktoré sú potrebné pre správnu funkčnosť systému.

Inštalácia hlavného centrálneho servera prináša niekoľko možnosti pre administratívne využitie. Webová aplikácia založená na AJAX, umožňuje sledovanie z ľubovoľného počítača pomocou webového prehliadača. Aplikácia pre Microsoft Windows Enterprise Console ponúka sledovanie a nastavovanie celého softvéru na hlavnom servery, podobne ako webové rozhranie, ďalšia funkcia ktorou Eneterprise Console disponuje je možnosť prístupu a konfigurácie k ďalším hlavným serverom PRTG. Vytvára to možnosť spravovať monitorovanie centrálne aj keď sa šíri cez rôzne servery. Dostupné sú aj mobilné aplikácie pre Android a Apple iOS zariadenia na kontrolu monitorovania.

Pomocou sond je sieť možné nielen monitorovať ale aj identifikovať zariadenia a služby, ktoré budú zahrnuté do monitoringu. Ak nastane problém s tým, že lokálna sonda nie je schopná komunikovať so sieťou, je možné nainštalovať vzdialenú sondu, ktorá bude komunikovať spätne do hlavného monitorovacieho serveru. V systéme hierarchie monitorovania, je možné vytvárať skupiny, kde je možné združovať zariadenia podľa sietí, zbieraných dát, alebo ako skupiny podobných zariadení. Aplikovanie nastavení na skupinu sa prejaví pre všetky zariadenia v skupine. PRTG ponúka aj manuálne pridanie zariadení do viacerých skupín, čo však môže byť problém pri zmene pravidiel na úrovni skupiny, kde môže dochádzať k zámene pravidiel

pre jednotlivé skupiny a zariadenia.

Softvér PRTG ponúka návrh senzorov pre zariadenia založené na výsledkoch sieťového skenovania, je možné ich nájsť na obrazovke s podrobnosťami o zariadení. Každý dátový bod vyžaduje senzor, ktorý môže byť podľa potreby monitorovaný alebo ignorovaný. Senzory je možné pridávať, odstraňovať, pozastaviť na základe podmienok alebo ich pozastaviť na rôzne dlhý čas. Senzory sú flexibilné a je možné definovať senzory na meranie čohokoľvek v sietí. Spoločnosť Paessler AG usporadúva každoročne súťaž o najviac unikátne použitie ich senzorov s názvom „PRTG Sensor Contest“ [1]. Spoločnosť udržiava skripty senzorov a umožňuje tak používateľom ľahšie rozvíjať senzory [2]. PRTG takto združuje veľké množstvo senzorov, ktoré sú presne definované pre sieťové zariadenia alebo sondy od mnohých výrobcov hardvéru a softvéru.

Enterprise Console má prehľadné zobrazenie o výstrahách a počítadlách výkonu na každej úrovni hierarchie obr. 2.2. Umožňuje rýchly prehľad o celej sietí, individuálne upozornenia na servery a viacero úrovni detailov medzi nimi. Upozornenia sa zobrazujú na viacerých miestach a je tak jednoduché špecifikovať ktoré zariadenie má výpadok alebo kde nastal alarm. Notifikácie na alarmy a výpadky môžu byť konfigurované na viacerých miestach v hierarchií objektov. Softvér umožňuje nastaviť upozornenia podľa množstva udalostí, podmienok alebo pri prekročení určitých hodnôt. Napríklad je možné nastaviť upozornenie ak nedokáže ping monitor overiť dostupnosť alebo iba ak je vzdialený server nedosiahnuteľný viac ako 15 minút, poprípade ak prekročí zaťaženie procesora určitú hodnotu a podobne. Upozornenia zahŕňajú množstvo typov : email, záznamy logov, push upozornenia, SMS upozornenia, SNMP trap alebo system log(syslog) správy. Dostupné sú aj pokročilejšie funkcie ako HTTP akcia alebo spustenie programu.

Webové rozhranie je veľmi podobné konzolovému zobrazeniu, avšak disponuje ešte lepšou prehľadnosťou nastavení a alarmov. PRTG ponúka pokročilý systém vytvárania reportov z monitorovania obrázok2.3, na nasledujúcich stranách . Poskytuje preddefinované šablóny(grafy, rôzne výkyvy a maximá, zoznamy a iné), ponúka bezpečnostný kontext kde sa definuje kto vytvára report a report bude tvorený len zo senzorov a zariadení ku ktorým má špecifický účet prístup alebo ich môže vidieť, ďalej sa definuje ktoré senzory sa podľa značky(tagovania) zahrnú do reportu, ako často sa bude report tvoriť a aký bude časový rozsah reportu. Do reportu je možné zahrnúť aj CSV alebo XML súbory(šablóny s dátovými tabuľkami). PRTG má aj tiketovací systém kde je možné vytvárať tikety a prideliť ich definovaným účtom, umožňujú pridať komentár a prioritu.

Posledná významná funkcionalita, ktorou monitorovací softvér PRTG disponuje

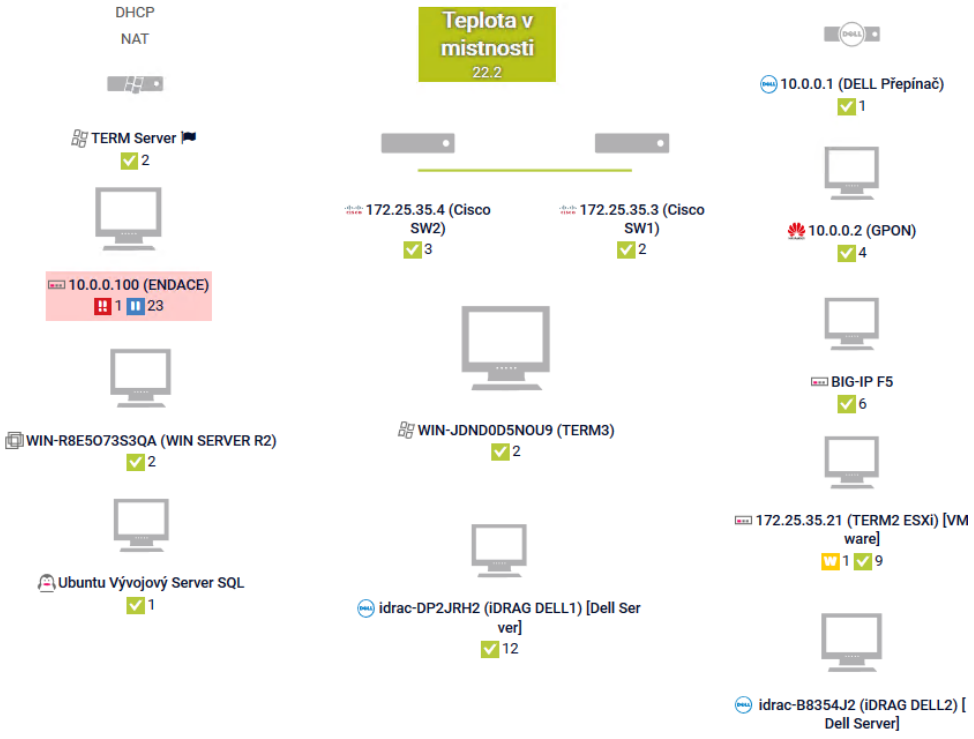
[1] Viac na stránke https://go.paessler.com/sensor-story/

[2] Zoznam senzorov dostupný na stránke https://www.paessler.com/script-world/all/all/all

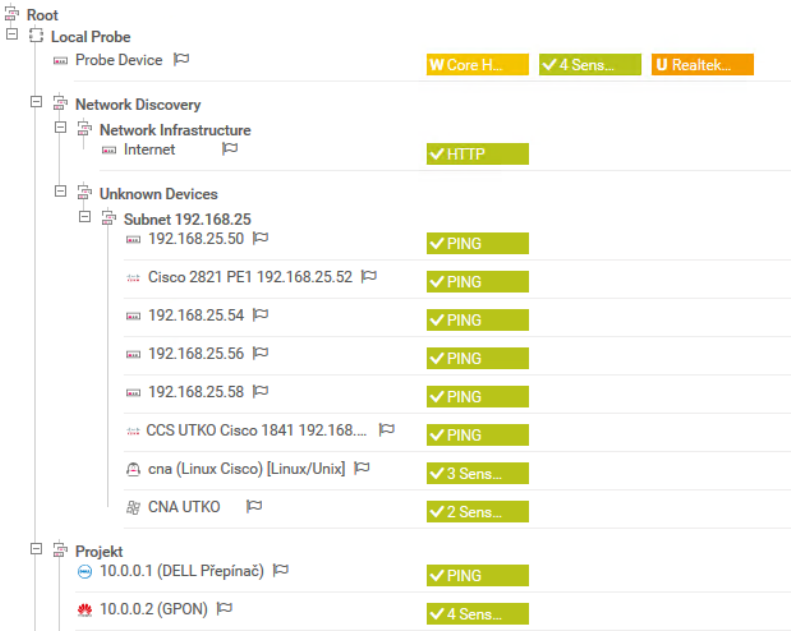
je vytváranie interaktívnych máp topológie – obrázok2.1 na nasledujúcej strane, založených na HTML a fungujúcich ako aktívne monitorovacie okno, ktoré ma podobnú funkciu ako základné monitorovacie okno a je tam možné vidieť alarmy na zariadeniach, prípade definované hodnoty ktoré sa majú zobrazovať. Mapy je možné rôzne upravovať, vytvárať si skupiny, používať rôzne druhy objektov(grafy, alarmy, výkonnostne zoznamy). Mapu je možné pomocou url odkazu a bezpečnostného kódu zdieľať na ľubovoľnom počítači a získať tak prehľad o sietí, v prípade vlastnej stránky sa dá využiť HTML kód a takýmto spôsobom vložiť mapu na stránku a mať neustály dohľad nad sieťou.

PRTG je flexibilný, stabilný a výkonný monitorovací systém s nenáročnými hardvérovými požiadavkami a veľkou možnosťou nastavení senzorov. Voľná licencia je dostupná pre 100 sieťových sond a odhad firmy Paessler je, že množstvo sieťových zariadení vyžaduje medzi 5 až 10 sond , čo sa do veľkej miery potvrdzuje v testovacej laboratórnej sieti. Sieťový administrátor mal už predošlé skúsenosti s testovaním PRTG, tak po konzultácií a zvážení ostatných monitorovacích systémov sa pristúpilo práve k použitiu PRTG systému.

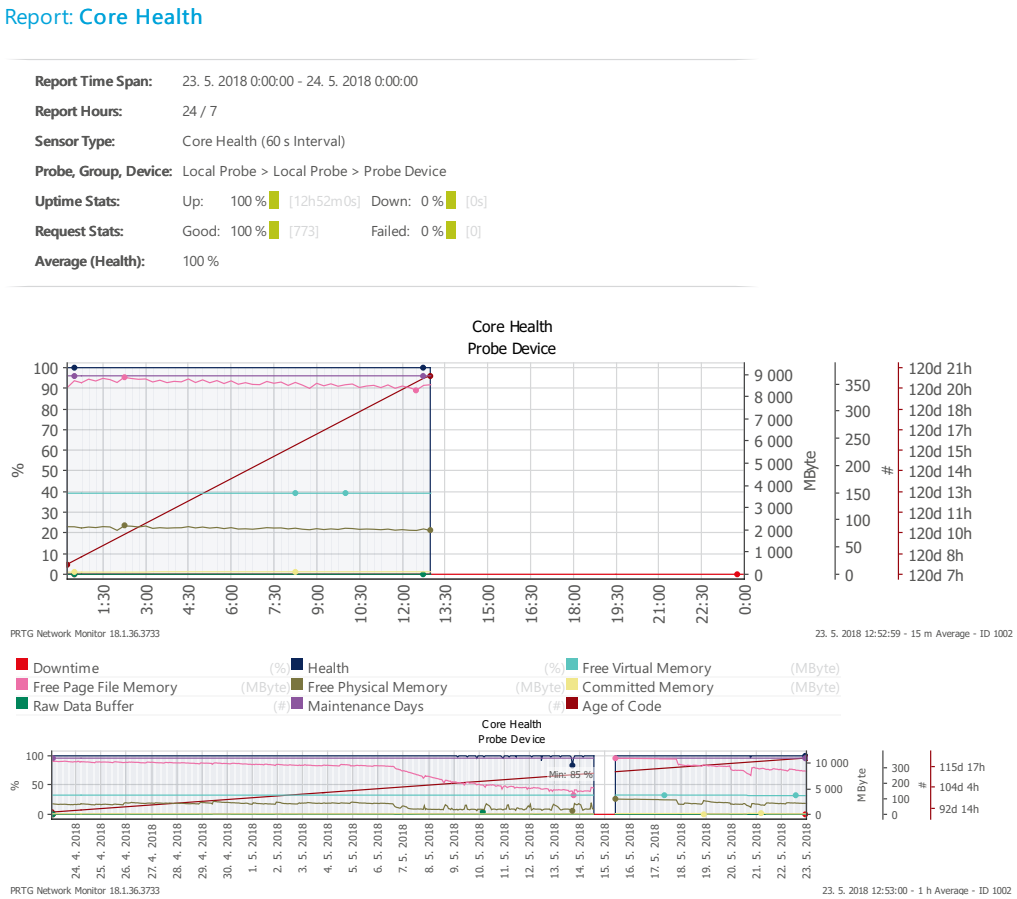
Nevýhody softvéru sú: voľná licencia len pre 100 sieťových sond, cena licencie rastie s počtom sieťových sond čo sa nemusí vyplatiť veľkým sieťam, úprava mapovej topológie a vytváranie reportov je obtiažnejšie na slabších serveroch pre výpočové nároky.



Obr. 2.1: Topologická mapa siete v PRTG s aktívnim zobrazením sond



Obr. 2.2: Ukážka časti hierarchickej štruktúry zariadení v PRTG



Obr. 2.3: Časť reportu zo školskej laboratórnej siete – Zdravie hlavného systému

3 PROTOKOL SNMP

Jednoduchý protokol na správu siete (protokol jednoduchého sieťového manažmentu – Simple Network Management Protokol). Jadro SNMP tvorí jednoduchý súbor operácií a informácií, ktoré tieto operácie zbierajú a tak dávajú administrátorom možnosť meniť stav zariadení založených na SNMP alebo zbierať o nich informácie. Pomocou SNMP je možné vypnúť port na vzdialenom smerovači alebo je možné zistiť informácie o rýchlosti s ktorou pracuje Ethernet port. SNMP môže byť dokonca nastavený na monitorovanie teploty na prepínači a ak teplota prekoná nejakú hranicu, tak SNMP zašle varovanie.

SNMP je obvykle spájaný so správou smerovačov, avšak môže byť použitý na správu veľkého množstva typov zariadení. Predchodca SNMP, protokol SGMP (Protokol jednoduchého manažmentu brány – Simple Gateway Management Protokol), bol vyvinutý pre manažment Internetových smerovačov, SNMP môže byť použitý na manažovanie Unix systémov, Windows systémov, tlačiarni, modemových stojanov. záložných zdrojov, rozbočovačov, opakovačov a iných. Každé zariadenie alebo softvér(webové servere, databázy) ktoré podporuje získavanie SNMP informácií, môže byť takto spravované. [8]

3.1 História SNMP protokolu

SNMP, protokol bol prvýkrát predstavený v roku 1988 a hneď sa stal hlavným protokolom sieťového manažmentu v sieťach založených na architektúre TCP/IP.

IETF (komisia pre technickú stránku Internetu – Internet Engineering Task Force) tento protokol vytvorila hlavne za účelom vzdialeného manažmentu pre zariadenia bežiace na architektúre IP, pričom využíva štandardizovanú skupinu operácií a štandardov. V dnešnej dobe je tento protokol široko používaný a podporovaný radami sieťových zariadení - prepínače, smerovače, rozbočovače, modemy, servery, rovnako aj záložné systémy UPS, tlačiarne a iné zariadenia pracujúce s TCP/IP architektúrou. [7].

Štandardy protokolu SNMP definujú oveľa viac ako len komunikačný protokol pre manažment sieťovej prevádzky, tieto štandardy definujú aj to ako je s dátami nakladané, ako sa k dátam pristupuje a ako sú tieto dáta ukladané, rovnako definujú distribuované rámce SNMP agentov a serverov. IETF uznáva SNMP ako plný štandard IP protokolovej sady. Oficiálnu definíciu SNMP protokolu môžeme nájsť v dokumente RFC(Request for Comments) 1157.

SNMP verzia 2(SNMPv2) prišla v roku 1993, priniesla vylepšenia v lepšom narábaní s chybami, väčšie počítadla pre dáta(64–bit), zlepšenie efektivity(get-bulk transfers), potvrdzovanie výsledných notifikácií a hlavne bezpečnostné vylepšenia.

Avšak, SNMPv2 nebol širšie prijatý, pretože IETF organizácia, nebola schopná dôjsť ku zhode ohľadom SNMP bezpečnostných vlastností. V roku 1996 prišla revízia protokolu SNMPv2 na verziu SNMPv2c, ktorý obsahoval všetky zamýšľané vylepšenia z predchádzajúcej verzie 2, avšak s výnimkou bezpečnostného vylepšenia a používal rovnaký nezabezpečený model ako protokol SNMPv1, problémom u tejto verzie je to, že sa spolieha na heslá, nazývané *komunitné reťazce(community strings)* ktoré putujú sieťou úplne nezabezpečené ako čistý text. Rovnako ako SNMPv2 ani verzia SNMPv2c nikdy nezažila rozšírenie do IP komunity a veľa organizácií ďalej pokračovalo v používaní SNMPv1 protokolu.

V roku 1998 IETF začala pracovať na protokole SNMPv3, ktorý je definovaný v RFC 2571-2575. V podstate je SNMPv3 súbor bezpečnostných vylepšení ktoré sú využívané a spojené s SNMPv2c, toto v základe znamená, že SNMPv3 nie je štandardný, nezávislý manažmentový protokol a nenahradzuje SNMPv2c alebo SNMPv1. SNMPv3 umožňuje zabezpečené spôsoby na prístup k zariadeniam používajúc autentifikáciu, integritu správ a šifrovanie SNMP paketov, ktoré putujú sieťou.[7]

3.2 Komponenty SNMP

Komponenty SNMP :

1. **Manažované zariadenie (Managed devices)** - Obvykle sa jedná o niekoľko bodov siete. Menovite to sú smerovače, prístupové servery, prepínače, mosty, rozbočovače, tlačiarne, počítače a dnes už aj IoT(Internet vecí – Internet of things) zariadenia, ktoré sú schopné dorozumieť sa SNMP.
2. **Agent** - V svojej podstate je to softvérový modul, ktorý dokáže prekladať informácie o zariadení do zrozumiteľnej formy SNMP, tak aby zariadenie mohlo byť prístupne na monitorovanie pomocou SNMP, agent beží na manažovaných zariadeniach a môže byť implemetovaný ako špeciálny program alebo ako súčať operačného systému
3. **Systém sieťového manažmentu(NMS - Network Management System)** - Jedná sa o systém ktorý poskytuje väčšinu procesných a pamäťových zdrojov pre sieťový manažment, zároveň na ňom bežia monitorovacie aplikácie. NMS takto zbierá SNMP informácie od jednotlivých agentov, ktorý bežia na spravovaných zariadeniach [9]

3.2.1 Komunikácia pri SNMP manažmente

V podstate ide o normálnu komunikáciu typu klient/server. Riadiaca entita začne komunikáciu aby dostala odpoveď pomocou dotazu *GetRequest*, na dotaz odpovedá

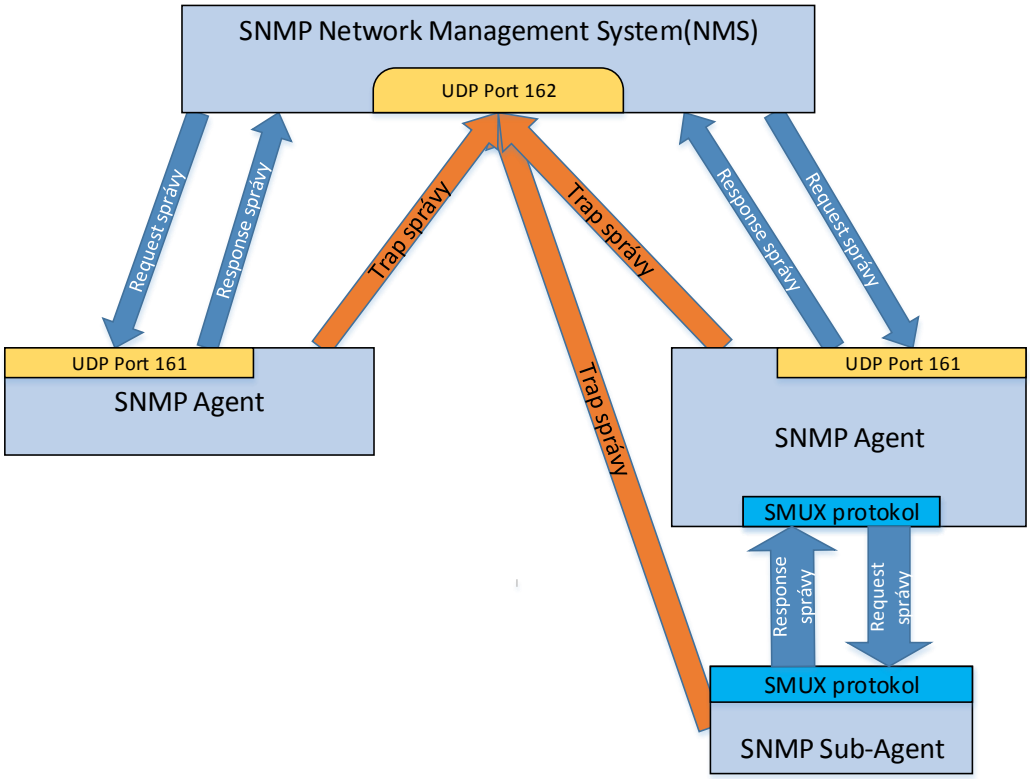
dotazované spravované zariadenie odpoveďou *Response* . Avšak v SNMP existuje ešte ďalší typ komunikácie ktorý nie je závislý na predchádzajúcej žiadosti ale komunikácia sa spustí od riadeného zariadenia smerom k riadiacej entite(monitorovací počítačový server) bezprostredne po určitej udalosti(zlyhanie disku, preťaženie procesora, zvýšenie teploty), typ týchto správ sa volá *SNMP Trap.*[11]

Komunikácia v rámci SNMP protokolu je založená na rovnakom princípe ako normálne dátové pakety, ktoré smerujú sieťou, medzi dvoma alebo viacerými komunikujúcimi bodmi. Avšak v prípade SNMP, sú komunikujúcimi stranami riadiaca entita(NMS) na jednej strane, napríklad počítač v laboratóriu na ktorom beží monitorovací softvér, a na strane druhej je to spravované alebo riadené zariadenie(na ktorom beží agent) – prepínač, smerovač, serverové skrine alebo iné zariadenia ktoré chceme monitorovať. SNMP používa UDP(užívateľský datagramový protokol – User Datagram Protocol) na komunikáciu medzi agentom a manažérom. Pre štandardnú komunikáciu sa využíva UDP port 161, pre posielanie Trap správ sa využíva UDP port 162.

Protokol UDP bol implementovaný pretože nevytvára end to end spojenia. Znamená to, že jediné spojenie sa uskutočňuje medzi agentom a manažérom len vtedy keď sú posielané datagramy tam a späť. Tento aspekt UDP spôsobuje to, že UDP je nespoľahlivý, pretože neexistuje potvrdenie straty datagramov na úrovni protokolov. Toto rieši aplikácia SNMP, ktorá ma za úlohu zistiť či sa datagramy stratili a či je potreba ich preposlať znova. Toto sa dosahuje jednoduchým časovým limitom, NMS takto odošle UDP žiadosť(Request) na adresu agenta a podľa nastaveného času čaká na odpoveď. Dĺžka čakania závisí od konfigurácie NMS a ak NMS do zadaného časového limitu neobdrží odpoveď, tak považuje paket so žiadosťou za stratený a odošle žiadosť znovu. Podobný problém sa vyskytuje pri SNMP Trap správach, keďže agent, ktorý posiela Trap správy nevyžaduje odpoveď a potvrdenie na ne, tým pádom sa môžu SNMP trapy jednoducho stratiť a neinformovať NMS o výpadku alebo neštandardnej situácií.

Z tohto dôvodu je pri nastavení NMS potrebné použiť rozumné časové intervaly na zisťovanie stavu zariadení. Počet opakovaných žiadosti, rovnako aj dĺžku času medzi opakovanými žiadosťami je rovnako možné nastaviť na NMS. Veľkou výhodou použitia UDP je jednoduchosť, efektívnosť a malé výkonové zaťaženie siete. [8]

SNMP agent dokáže komunikovať aj s ďalšími podriadenými agentmi, pomocou SNMP multiplexing protokol(SMUX). Týmto protokolom sa definuje komunikácia medzi nadriadeným SNMP agentom a ďalšími podriadenými agentami alebo ich procesmi. Tento protokol je zadefinovaný v RFC 1227 z roku 1991 ako súčasť SNMP. [10]



Obr. 3.1: Komunikácia v SNMP medzi NMS a agentami

3.3 Typ SNMP operačných správ

Existuje množstvo typov SNMP správ , ktoré v sebe nesú špecifické vyžadované operácie pre fungovanie SNMP, v sietí sa používajú podľa vyžadovanej operácie správy:

- **GetRequest** – Najčastejšia SNMP správa, ktorú SNMP manažér odosiela na vyžiadanie dát. Cielené zariadenie odpovedá vyžiadanou hodnotou v Response správe.
- **GetNextRequest** – SNMP manažer môže posielať tento typ správy aby zistil, ktoré informácie sú dostupné zo zariadenia. Začína na OID 0 a SNMP manažér môže ďalej pokračovať až pokiaľ už nie sú žiadne ďalšie dáta dostupné. Toto je spôsob ako dostať z určitého zariadenia všetky dostupné dáta aj bez predchádzajúcej znalosti odpovedajúceho systému alebo zariadenia.
- **GetBulkRequest** – Optimalizovaná novšia verzia GetNextRequest, doplnená v SNMP verzie 2. Požadovaná odpoveď bude obsahovať tak veľa dát, koľko je povolených žiadosťou. Týmto spôsobom je možné dostať viacero GetNextRequest správ naraz a umožňuje tak používateľom vytvoriť zoznam všetkých

dostupných dát a parametrov.

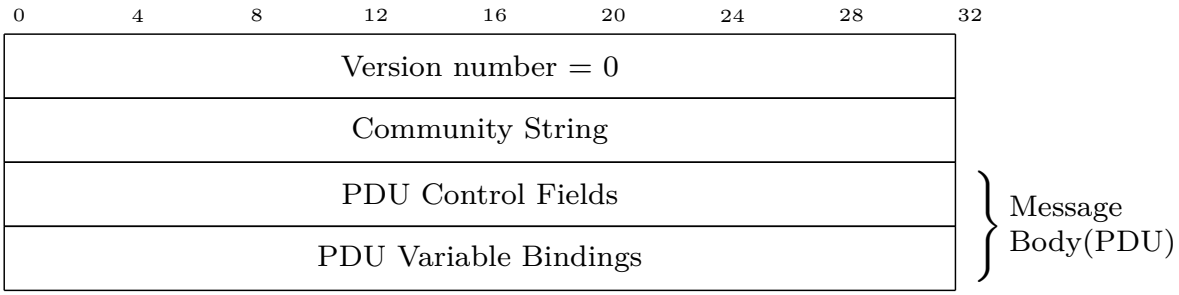
- **SetRequest** – Príkaz od SNMP manažéra na nastavenie alebo zmenu parametrov pre dotazované zariadenie alebo systém cez SNMP. Správa môže byť použitá na správu alebo aktualizovanie konfiguračných nastavení alebo iných parametrov. Nesprávne aplikovanie SetRequest správy môže spôsobiť poškodenie systému alebo nastavenie siete.
- **Response** – Je to správa, ktorú posiela zariadenie ako odpoveď na správu Request od manažéra. Ak posiela odpoveď na správu typu GetRequest, tak paket obsahuje vyžiadané dáta alebo hodnoty. V prípade, že odpovedá na správu SetRequest, tak paket odpovedá čerstvo nastavenou hodnotou ako potvrdenie toho, že správa SetRequest bola úspešne dokončená.
- **Trap(v2)** – Správa doslova pretlačená SNMP agentom bez toho aby bola vyžiadaná manažérom. Trap správy sú posielané na základe definovaných podmienok, napríklad v prípade chyby alebo v prípade prekročení určitých prahových hodnôt. SNMP Trapy prinášajú benefity v proaktívnom monitoringu siete, avšak je dobré ich prvotne nakonfigurovať pomocou SNMP manažéra.
- **InformRequest** – Informačný typ správy ktorý bol pridaný do SNMP verzie 2. Umožňuje manažérovi potvrdiť, že prijal SNMP Trap od agenta. Niektorí agenti posielajú SNMP trapy až do prijatia InformRequest správy SNMP manažérom.[12]

3.3.1 Formát SNMP správ

SNMPv1 – formát správy bol definovaný v originál SNMP protokole verzie 1. Správa je jednoduchá, krátka a má nízku úroveň bezpečnosti. Typy správ pri SNMPv1 majú všetky rovnaký formát, okrem Trap-PDU. Správy sa rozlišujú podľa prvej položky v správe: PDU Type. V správe sú aj položky ktoré podľa typu správy naberajú význam ako napríklad Error Status alebo Error Index, ktoré majú význam len pri odpovedi, nie pri žiadosti.[13] Bežný formát a obsah SNMP PDU, na nasledujúcej strane na obrázku 3.4

Názov	*Syntax*	*Veľkosť(v bytoch)*	*Popis*
Version	Integer	4	***Číslo verzie*** : Popisuje číslo SNMP verzie pre zachovanie kompatiblity medzi verziami. Pre SNMPv1 je to číslo **0**, nie **1**.
Community	Octet String	Variable	***Community String (Názov komunity):*** Definuje SNMP komunitu v ktorej odosielateľ a príjemca sú priradený. Tento spôsob je implementovaný do jednoduchého SNMP bezpečnostného mechanizmu založenom práve na komunite.
PDU	-	Variable	***Protocol Data Unit*** (Dátová jednotka protokolu) : PDU sa definuje ako telo správy.

Obr. 3.2: Základný formát správy SNMP verzie 1

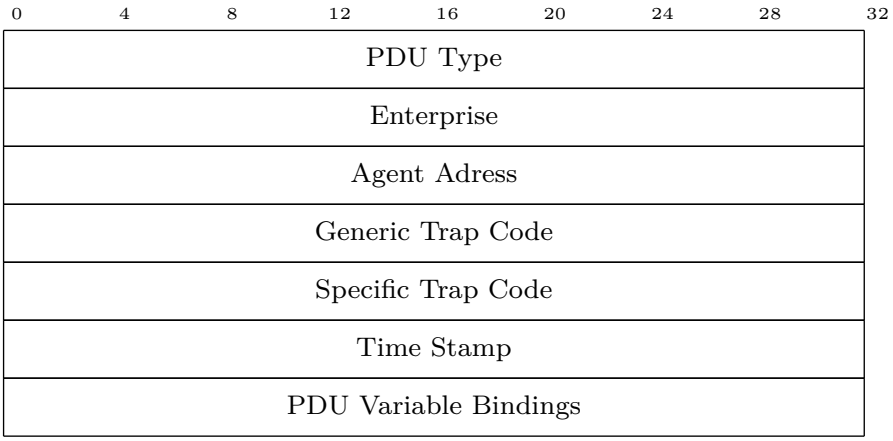


Obr. 3.3: Obecný Formát správy SNMP verzie 1

Názov	*Syntax*	*Veľkosť(v bytoch)*	*Popis*
PDU Type	Integer	4	0 - GetRequest-PDU 1 - GetNextRequest-PDU 2 - Response-PDU 3 - SetRequest-PDU
Request ID	Integer	4	Číslo používané k párovaniu žiadosti s odpoveďami. Je generované zariadením, ktoré posiela žiadosť, odpovedajúce zariadenie túto hodnotu skopíruje a pridá do *GetResponse-PDU*.
Error Status	Integer	4	Používa sa v *GetResponse-PDU* na to aby informoval žiadajúcu SNMP entitu o výsledku žiadosti. Hodnota nula indikuje žiadnu chybu, ostatné chyby sú: **0 - noError**, žiadna chyba nenastala, používa sa v Request PDU. **1 - tooBig**, veľkosť odpovede GetResponse-PDU je príliš veľká. **2 - noSuchName**, meno vyžiadaného objektu nebolo nájdené. **3 - badValue**, hodnota v žiadosti sa nezhoduje so štruktúrou objektu, ktorú má definovanú príjmateľ. **4 - readOnly**, pokus o zmenu objektu, ktorý slúži len na čítanie. **5 - genErr**, vyskytol sa iný druh chyby ako štyri predom definované typy
Error Index	Integer	4	Ak je *Error Status* nenulový, tak toto pole obsahuje ukazovateľ, ktorý špecifikuje ktorrý objekt generoval chybu. Vždy nula v žiadosti.
Variable Bindings	Variable	Variable	Obsahuje hodnoty, ktoré definujú MIB objekty v PDU.

Obr. 3.4: Formát PDU(Protocol Data Unit) správy SNMP verzie 1 a obsah jednotlivých polí

SNMPv1 Trap – Trap správa má špecifický formát, čím sa odlišuje od iných SNMP správ v SNMPv1 protokole. Trap správu definuje položka PDU Type s hodnotou 4, obrázok.3.6



Obr. 3.5: Formát Trap správy SNMP verzie 1

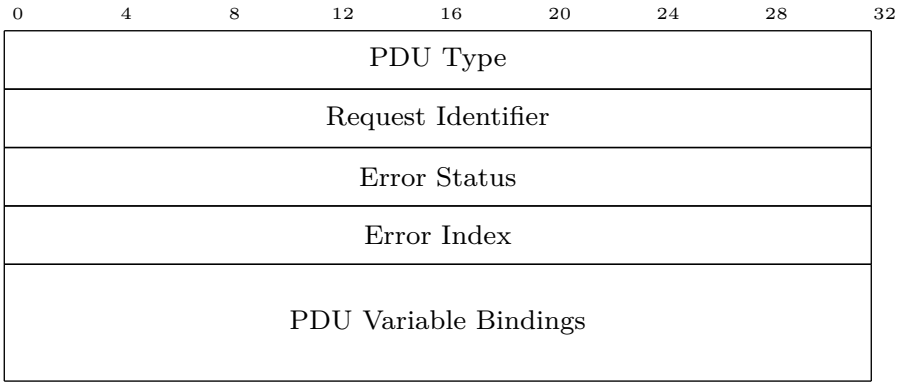
Názov	*Syntax*	*Veľkosť(v bytoch)*	*Popis*
PDU Type	Integer	4	***PDU Type*** : Hodnota integer , ktorá definuje PDU Typ, pre Trap-PDU správu je to **4.**
Enterprise	Sequence of Integer	Variable	***Enetrprise*** : Je to objektový identifikátor skupiny, na bližšie špecifikovanie typu objektu ktorý vygeneroval trap.
Agent Addr	Network Address	4	***Agent Address*** : IP adresa SNMP agenta, ktorý generuje Trap správy.
Generic Trap	Integer	4	***Generic Trap Code*** : Hodnota, ktorá špecifikuje niektorý preddefinovaný generický typ trap správy.
Specific Trap	Integer	4	***Specific Trap Code:*** Hodnota definujúca špecifický implementovaný typ trapu.
Time Stamp	Integer	4	Time Stamp: Čas od poslednej incializácie alebo reincializácie SNMP agenta, používa sa na zálohovanie v logoch.
Variable Bindings	Variable	Variable	Obsahuje hodnoty, ktoré definujú MIB objekty v PDU.

Obr. 3.6: Obsah a formát PDU Trap správy SNMP verzie 1

SNMPv2 prinieslo viacero typov komunikačných protokolov SNMP, ktoré sa od seba líšia komplexnosťou, úrovňou zabezpečenia, typom ich správ a dátových jednotiek(PDU). Trap správa verzie 2 sa však neodlišuje iným typom dátovej jednotky(PDU) od iných typov PDU SNMPv2 ako je to v SNMPv1, odlišnosť je len v čísle verzie(Trap-PDU má číslo 7), inak je Trapv2 PDU rovnaká ako napríklad PDU GetRequest, v tele správy sa mení len typ PDU pre Trap.[13]

- **SNMPv2p**(party based) originál bol založený na princípe komunikujúcich strán a ich identifikátoroch v SNMP správach. Je pomerne zložitý, komunikácia definuje zdrojovú a cieľovú stranu a odkaz na kontext ktorý definuje súbor objektov MIB prístupných konkrétnej entite.
- **SNMPv2u**(user based) komunikácia je založená na komunikujúcich používateľoch. Tento typ vznikol ako voliteľný bezpečnostný model v čase vzniku a štandardizovania SNMPv2c protokolu.[13] V tejto v práci sa používa SNMPv2c protokol, tak vo výpise je len pár bezpečnostných premenných na ilustráciu, ktoré obsahuje správa SNMPv2u. Správa je veľmi komplexná a obsahuje množstvo bezpečnostných variabilných premenných, napríklad :
  - QoS(Quality of service – indikuje či je použité overovanie a či je povolené generovanie reportov).
  - Agent ID(identifikátor agenta, ktorý posiela správu).
  - User Lenght(dĺžka používateľského mena).
  - User name(meno používateľa).
  - Authentication Digest(hodnota autentizačného spracovania na overenie identity).
- **SNMPv2c**(community based) oproti SNMPv1 priniesla dva typy nových správ, správu *GetBulkRequest* a správu *InformRequest*. Tieto správy sú bližšie popísané v kapitole 3.3. Protokol využíva vylepšenia SNMPv2p avšak vracia sa späť k SNMPv1 jednoduchému bezpečnostnému modelu.

Formát správ SNMPv2c je v tabuľkách nižšie, SNMPv2 má špeciálny formát PDU odlišujúci sa od iných správ tejto verzie len pre správu *GetBulkRequest*.



Obr. 3.7: SNMPv2 polia v PDU

Názov	*Syntax*	*Veľkosť(v bytoch)*	*Popis*
PDU Type	Integer	4	0 - GetRequest-PDU 1 - GetNextRequest-PDU 2 - Response-PDU 3 - SetRequest-PDU 4 - Trap-PDU SNMPv1 : vo verzií SNMPv2 sa už nepoužíva 5 - GetBulkRequest-PDU : má svoj vlstný formát PDU 6 - InformRequest-PDU 7 - Trapv2-PDU 8 - Report-PDU
Request ID	Integer	4	Číslo používané k párovaniu žiadosti s odpoveďami. Je generované zariadením, ktoré posiela žiadosť, odpovedajúce zariadenie túto hodnotu skopíruje a pridá do *GetResponse-PDU*.
Error Status	Integer	4	Používa sa v Response-PDU na to aby informoval žiadajúcu SNMP entitu o výsledku žiadosti. Hodnota nula indikuje žiadnu chybu, ostatné hodnoty definujú aké typy chyby vznikli. Prvý šesť hodnôt(0 až 5) sa používa tak ako v SNMPv1 pre kompatibilitu, ale SNMPv2 prináša mnoho ďalších nových chybových kódov, ktoré špecifikujú presnú povahu chyby(SNMPv2 chyby v nasledujúcej tabuľke). *GenErr* kód sa stále používa v prípade, keď žiadný zo špecifických typov chýb nie je možné aplikovať(ani zo starých alebo nových chybových kódov).
Error Index	Integer	4	Ak je *Error Status* nenulový, tak toto pole obsahuje ukazovateľ, ktorý špecifikuje ktorrý objekt generoval chybu. Vždy nula v žiadosti.
Variable Bindings	Variable	Variable	Obsahuje hodnoty, ktoré definujú MIB objekty v PDU.

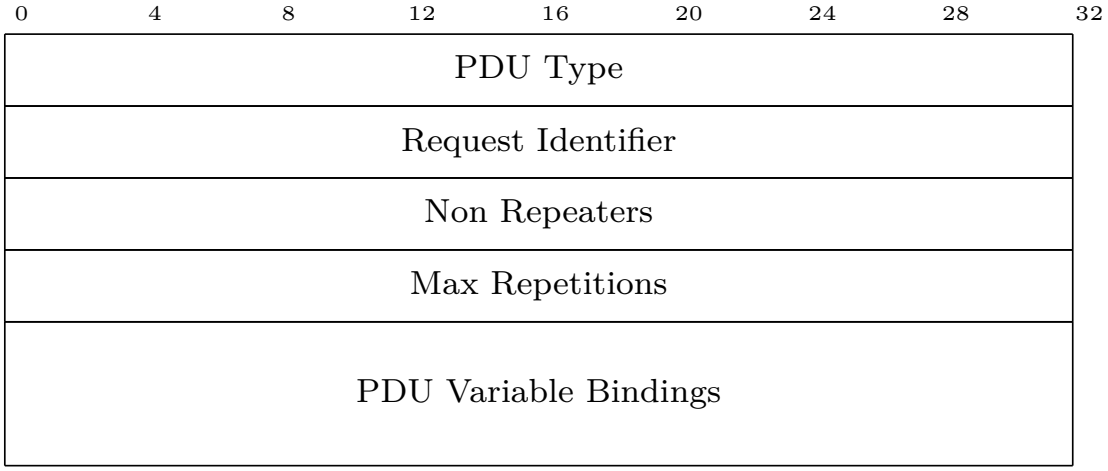
Obr. 3.8: Bežný formát SNMPv2c správy, chybové kódy SNMPv2 na obrázku3.9

Hodnota Chyby	Kód Chyby	Popis Chyby
0	*noError*	Nenastala žiadna chyba, kód je používaný aj vo všetkých PDU žiadostí, keď nemajú žiadny chybový stav na hlásenie.
1	*tooBig*	Veľkosť odpovede *Response-PDU* by bola príliš veľká.
2	*noSuchName*	Meno požadovaného objektu nebolo nájdené.
3	*badValue*	Hodnota v žiadosti sa nezhoduje so štruktúrou, ktorú má príjemca definovanú pre objekt.
4	*readOnly*	Pokus o zmenu objektu ktorý slúži len na čítanie.
5	*genErr*	Vyskytol sa iný druh chyby ako je definovaný v tejto tabuľke.
6	*noAccess*	Prístup k objektu bol odmietnutý pre bezpečnostné dôvody.
7	*wrongType*	Typ objektu, ktorý je vo *Variable Binding,* je pre daný objekt nesprávny.
8	*wrongLength*	Dĺžka, ktorá je vo *Variable Binding,* je pre daný objekt nesprávna.
9	*wrongEncoding*	Kódovanie, ktoré je vo *Variable Binding* , je pre daný objekt nesprávne.
10	*wrongValue*	Hodnota uvedená vo *Variable Binding,* nie je pre daný objekt možná.
11	*noCreation*	Špecifikovaná premenná neexistuje a nemôže byť vytvorená.
12	*inconsistentValue*	Hodnota, ktorú špecifikuje *Variable Binding,* danému objektu vyhovuje ale momentálne mu nemôže byť priradená.
13	*resourceUnavaliable*	Nastavenie premennej vyžaduje prostriedok, ktorý nie je k dispozícií.
14	*commitFailed*	Pokus o nastavenie konkrétnej premennej zlyhal.
15	*undoFailed*	Pokus o nastavenie konkrétnej premennej ako časti skupiny premenných zlyhal, a pokus o zrušenie nastavenia iných premenných bol neúspešný.
16	*authorizationError*	Vznikol problém pri autorizácií.
17	*notWritable*	Premenná nemôže byť prepísaná alebo vytvorená.
18	*inconsistentName*	Názov, ktoý je vo *Variable Binding* , špecifikuje premennú ktorá neexistuje.

Obr. 3.9: Kódy chybových stavov položky Error Status v SNMPv2c

Názov	*Syntax*	*Veľkosť(v bytoch)*	*Popis*
PDU Type	Integer	4	***PDU Type:*** Hodnota Integer ktorá definuje typ PDU, GetBulkRequest-PDU správa má číslo 5.
Request ID	Integer	4	Číslo používané k párovaniu žiadosti s odpoveďami. Je generované zariadením, ktoré posiela žiadosť, odpovedajúce zariadenie túto hodnotu skopíruje a pridá do GetResponse-PDU
Non Repeaters	Integer	4	***Non Repeaters*** **:** Určuje počet pravidelne neodpovedajúcich objektov na začiatku zoznamu premenných v žiadosti.
Max Repetitions	Integer	4	***Max Repetitions:*** Počet opakovaní v tabuľke, ktorú čítajú opakujúce sa objekty.
Variable Bindings	Variable	Variable	Obsahuje hodnoty, ktoré definujú MIB objekty v PDU.

Obr. 3.10: SNMPv2 GetBulk obsah PDU správy



Obr. 3.11: SNMPv2 GetBulk PDU správa

SNMPv3 priniesol najmä rozšírenie bezpečnosti. Formát správy sa teda prispôsobil aspektu bezpečnosti, bola rozšírená o položky ktoré súvisia a špecifikujú použitý bezpečnostný model.

SNMPv3 sa snažil vyriešiť najmä problémy SNMPv2, ktoré priniesli jeho rôzne verzie, avšak verzia 3 prebrala veľa komponentov z SNMPv2 ako typy operácií, PDU typy a PDU správy. PDU zostalo takmer nezmenené a používa formát predchádzajúcej SNMPv2c verzie, bolo však rozšírené o položky *Context Engine ID* a *Context Name*, obsah PDU SNMPv3 na obrázku 3.12

Názov	***Syntax***	***Veľkosť(v bytoch)***	***Popis***
MSG Version	Integer	4	***Message Version Number:*** Popisuje verziu SNMP protokolu, pre SNMPv3 je hodnota 3.
Msg ID	Integer	4	***Message Indetifier:*** Číslo používané k párovaniu žiadosti s odpoveďami. Je generované zariadením, ktoré posiela žiadosť, odpovedajúce zariadenie odpovedá správou s rovnakým indetifikačným číslom.
Msg Max Size	Integer	4	***Maximum Message Size:*** Maximálna veľkosť správy, ktorú odosielateľ tejto správy môže prijať. Minimálna hodnota je 484.
Msg Flags	Octet String	1	***Message Flags:*** Slúžia pre riadenie spracovania správy. Štruktúra bližšie popísaná v RFC 3412
Msg Security Model	Integer	4	***Message Security Model:*** Hodnota popisuje typ použitého bezpečnostného modelu, pre SNMPv3(user based) je to 3.
Msg Security Parameters	-	Variable	***Message Security Parameters:*** Bližšie špecifikujú parametry potrebné pre konkrétny bezpečnostný model
Scoped PDU	-	Variable	***Context Engine ID -*** identifikuje, ktorej aplikácií ma byť PDU odoslané na spracovanie. ***Context Name -*** identifikátor objektu, špecifikujúci konkrétny kontext asociovaný s PDU. ***PDU*** **-** prenášaná jednotka protokolových dát.

Obr. 3.12: SNMPv3 obsah PDU

3.4 MIB, SMI a ASN.1

O SNMP protokole sa nedá povedať, že je protokol, ktorý presne definuje sadu príkazov, napríklad na čítanie, zápis, nastavenia nejakého parametru alebo vykonanie nejakej akcie priamo na zariadení. Takýto typ protokolov má presne stanovené príkazy na získanie jednotlivých informácií, napríklad špecifický príkaz pre zistenie toho, ako dlho zariadenie pracuje ale iný príkaz na vypnutie daného zariadenia alebo alebo zmenu jeho nastavenia. Takáto sada príkazov je unifikovaná a značne rozsiahla pre konkrétne typy a skupiny zariadení ktoré budú takýto špecifický protokol používať a zároveň je takýto špecifický protokol naviazaný na daný hardvér a musí byť prispôsobený pri vzniku nového zariadenia, čo znova ovplyvňuje množstvo zariadení.

SNMP je označovaný ako informačne orientovaný protokol, pretože pracuje s objektami(premennými) z ktorých môže získavať informácie, prípade do nich zapisovať informácie. Napríklad, na získanie času, ako dlho pracuje zariadenie prečíta premennú, ktorá obsahuje práve túto informáciu. SNMP preto stačí len malý počet základných operácií, ako prečítaj obsah premennej alebo do nej zapíš, na základné fungovanie. Objekty s informáciami o zariadeniach je tak možné rozširovať bez potreby zásahov do formy protokolu.

Objekty s informáciami sa líšia v závislosti na zariadení, tieto objekty pre SNMP špecifikuje **Management Information Base(MIB)**. SNMPv1 definovalo len jediný štandard, ktorý popisoval celý MIB. Dnes to už však neplatí, pretože existuje množstvo prídavných modulov a rozšírení, ktoré definujú sady objektov pre dané zariadenie. Rozšírenia a prídavné moduly sú zvyčajne poskytované výrobcom zariadenia spolu so zariadením.

Štandard **Structure of Management Information(SMI)** zabezpečuje univerzálnosť MIB objektov, zároveň definuje spôsob akým je celý modul MIB konštruovaný a ako sú jednotlivé objekty popisované. SMI tiež vytvára hierarchickú štruktúru objektov podobnú stromu tzv. object tree(strom objektov) aby bolo možné objekty jednoducho pomenovať a adresovať. v SMI, sú MIB objekty špecifikované pomocou jazyka **Abstract Syntax Notation 1(ASN.1)** ISO(Medzinárodná organizácia pre normalizáciu – International Organization for Standardization), ktorý presne definuje dáta, ich štruktúry, kódovania a dekódovania.

Podstata SNMP spočíva v troch úrovniach s ktorými pracuje. SNMP protokol prenáša informácie o stave zariadení, MIB definuje aké informácie je možné prenášať a SMI popisuje definíciu jednotlivých objektov MIB. SNMP sám o sebe nedefinuje aké informácie by mal spravovaný systém ponúknuť ani to aké informácie má NMS vyžadovať. Existujú dva hlavné štandardy SMI. Originál SMIv1 ako súčasť SNMPv1, efinovaný v RFC 1155, a druhý SMIv2, ktorý bol definovaný ako súčasť SNMPv2p v RFC 1442 a neskôr upravený pre novšie verzie SNMP a pre SNMPv3 v RFC 2578.

Verzie SMI sú podobné, avšak novšie verzie definujú viac typov objektov ako aj štruktúru MIB modulov.[14]

3.4.1 MIB objekty, ich štruktúra a dátové typy objektov

SMIv1 a SMIv2 sú podobné najmä v definícií objektov, avšak SMIv2 ponúka možnosť asociovať viac informácií s každým objektom. Základná štruktúra MIB objektov obsahuje päť povinných charakteristík a premenlivý počet voliteľných charakteristík:

- ***Object name*** – obsahuje identifikátor objektu, ktorý sa skladá z dvoch mien: textového mena *Object Descriptor* a čísleného *Object Identifier*, ktorý špecifikuje miesto objektu v MIB menovej hierarchií.
- ***Syntax*** – definuje dátový typ objektu a popisuje jeho štruktúru. Používajú sa buď regulárne dátové typy definované ASN.1, alebo tabuľkové dáta, čo je zbierka viacerých dátových prvkov. SMIv2 rozšírilo názvy niektorých dátových typov o číslicu 32, aby z nich bola jasná ich bitová veľkosť. Tabuľka dátových typov na nasledujúcej strane na obrázku 3.13
- ***Access*** – pole, ktoré definuje spôsob použitia a prístupu SNMP aplikácie k objektu. V SMIv1 môže pole nadobúdať štyri možné hodnoty: read-only, read-write, write-only a not-accessible. V SMIv2 sa pole *Access* volá *Max-Access* a je rozšírené na päť možných hodnôt: read-create, read-write, read-only, accessible-for-notify, not-accessible. Vyššia úroveň prístupu zahŕňa aj nižšie úrovne, napríklad objekt s read-create prístupom (čítanie, prepisovanie a vytváranie), je možné použiť aj vo všetkých režimov pod ním ako napríklad read-write(čítanie a prepisovanie), avšak nie naopak.
- ***Status*** – popisuje stav definície. V SMIv1 nadobúda tri hodnoty: mandatory, optional a obsolete, v SMIv2 len dve a to: current a deprecated.
- ***Definition*** – V SMIv2 *Description*, a je to textový opis objektu.
- ***Optional Characteristics*** – voliteľné pole, ktoré obsahuje rozširujúce informácie k objektu, napríklad referencie k doplnkovým dokumentom alebo iným informáciám čo sa týkajú objektu. Prípade obsahuje index, ak sa jedná o komplexnejší objekt.[15]

Na nasledujúcej strane je výpis 3.1, kde môžeme vidieť skutočnú definíciu SMIv2 objektu SNMPv2-MIB, zariadenia ENDACE, ktorý popisuje stratu paketov v prevádzke alebo na porte zariadenia komunikujúceho SNMP protokolom.

Výpis 3.1: Definícia SMIv2 MIB objektu zariadenia ENDACE

```
streamDropEnabled OBJECT-TYPE
  SYNTAX INTEGER      {enabled(1), disabled(2)}
  MAX-ACCESS           read-only
  STATUS               current
  DESCRIPTION         "Indicates whether dropping
                       of packets occurs at the stream
                       or port level. If enabled (1)then
                       dropping occurs at the individual
                       stream that has filled up, otherwise (2)
                       dropping will be occurring on a per
                       port basis."
  ::= { streamDropEntry 3 }
```

Dátový typ	*SNMPv1*	*SNMPv2*	*Popis*
Integer/Integer32	x	x	32 bitové celé číslo so znamienkom, rozsah od -2,147,483,648 do +2,147,483,647, môže byť tiež použitý ako výčtový typ kde jednotlivé čísla predstavujú iné konštanty.
Octet String	x	x	Textový ale binárny reťazec premenlivej dĺžky.
Null	x	-	Typ pre označenie prázdnej hodnoty.
Bits	-	x	Vyčíslenie pomenovaných bitov. Používa sa na to aby sa skupiny bitov dala použiť ako dátový typ.
Unsigned	-	x	32 bitové bezznamienkové celé číslo od 0 do 4,294,967,295.
Network Address/Ip Address	x	x	IP adresa, kódovaná ako štvorbajtový reťazec oktetov
CounterCounter32	x	x	32 bitové bezznamienkové celé číslo čo narastá od 0 do 4,294,967,295, potom sa vráti späť na 0.
Gauge/Gauge32	x	x	32 bitové bezznamienkové celé číslo od 0 do 4,294,967,295. Zvyčajne má asociované minimum a maximum indikujúce jeho rozsah.
TimeTicks	x	x	32 bitové bezznamienkové celé číslo indikujúce počet stotín sekúnd od istého momentu.
Opaque	x	x	Dáta používajúce vlastnú ASN.1 syntax, ktoré sú zasielané medzi zariadeniami bez toho, aby boli interpretované. Termín"opaque", teda "neprístupný", znamená že k dátam sa stavia ako ku čiernej skrinke, nezaujíma ho ich obsah.
Counter64	-	x	Podobne ako Counter32, ale s dĺžkou 64 bitov. Môže nadobúdať hodnoty od 0 do 18,446,744,073,709,551,615.

Obr. 3.13: Dátové typy MIB Objektov

3.4.2 Popis MIB objektov a ich hierarchická štruktúra

Každý objekt v MIB má svoje textové meno a číselný identifikátor. Meno objektu slúži najmä na lepšiu predstavu objektu a jeho účelu. S veľkým počtom objektom prichádza potreba využívať štruktúru týchto objektov tak, aby bola dostatočne flexibilná, ľahko rozšíriteľná a aby sa v nej dalo ľahko a rýchlo vyhľadávať. Z tohto dôvodu je štruktúra MIB objektov veľmi podobná štruktúre DNS(Domain Name System) a preto obsahuje objekty v tzv. „stromovej štruktúre".

Objekty sú vo vrstvách od najobecnejších po najšpecifickejšie a každý objekt má svoje presné umiestnenie. Prechádzaním stromu od najvrchnejších vrstiev k najspodnejším vznikajú mená objektov, teda identifikátory objektov, ktoré sú v konečnom zápise objektu oddelené bodkami a pomocou týchto mien je, tak možné objekt jednoznačne identifikovať. Takáto stromová štruktúra je pripravená na rozširovanie, pretože umožňuje pridávať celé podstromy(MIB Moduly)pre nové zariadenia. MIB moduly podstromov si vytvárajú a spravujú práve výrobcovia zariadení. Zachovanie celej hierarchie MIB objektov má na starosti organizácia International Organization for Standardization(ISO) a International Telecommunication Union(ITU – Medzinárodná Telekomunikačná únia).

Mená objektov sú okrem textových mien označené aj číselnými identifikátormi, ktoré sú pevne zviazané s textovými menami. Na identifikáciu sa využívajú práve číslicové identifikátory, ktoré tvoria rovnakú stromovú štruktúru a rovnako sa oddeľujú bodkou. Sú však oveľa kratšie na zápis, aj keď neposkytujú taký prehľadný zápis ako textové mená. [16]

Vo výpise SMIv2 objektu ENDACE 3.1, môžeme vidieť na konci nasledujúci text:

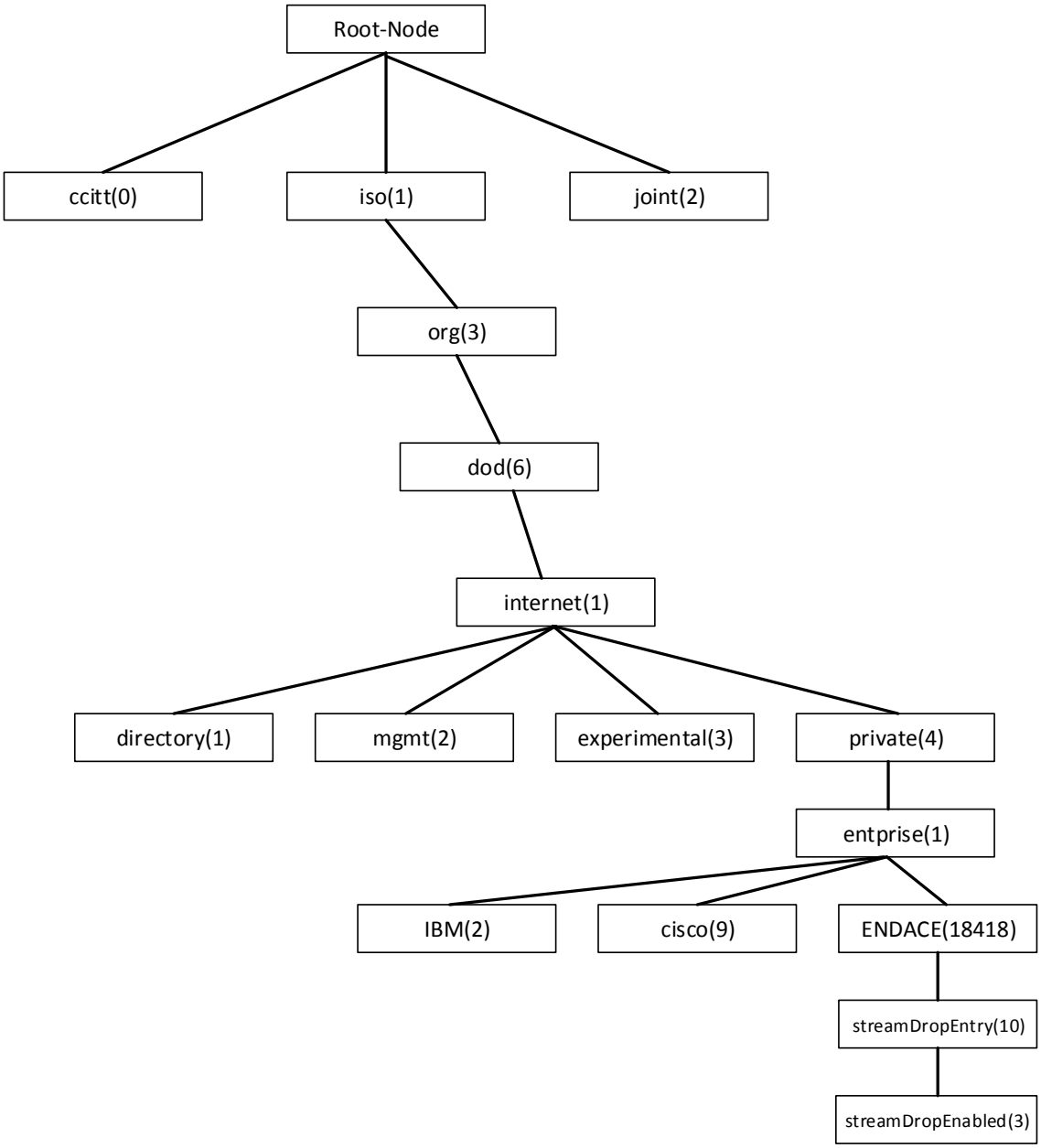
Výpis 3.2: Číselná a skupinová definícia MIB objektu ENDACE *streamDropEnabled*

```
::= { streamDropEntry 3 }
```

Pre tento objekt je pomenovanie *streamDropEnabled* a jeho číselný identifikátor je *3*. Znamená to, že to je tretí objekt v podstrome objektu *streamDropEntry*, čo je objekt a následný podstrom dodaný výrobcom zariadenia ENDACE a má číslo *10*. Celý identifikátor je *1.3.6.1.4.1.18418.10.3*, kde číslo *18418* znamená výrobcu – ENDACE[1], číslo *10* je podstrom *streamDropEntry*. Číslo *1* pred výrobcom patrí skupine objektov *enterprise*, číslo *4* je podstrom pre objekty *private*. Následné čísla sú obecnejšie dané a znamenajú : *1* pre *internet*, *6* pre *dod(department of defence)*, *3* pre *identified-organizaton* a *1* pre *ISO*. Objekty v hierarchickej štruktúre sa snažia vytvárať skupiny objektov a združovať sa na základe typu alebo určenia.

[1]OID informácie o objekte na stránke http://oidref.com/1.3.6.1.4.1.18418

Skupiny rovnako môžu mať svoje skrátené kódy, ktoré sú potom vsunuté do názvov jednotlivých objektov a tak je prehľadné do akej skupiny objektov, objekt patrí. Definovaný MIB strom s textovými aj číselnými identifikátormi je na obrázku 3.14



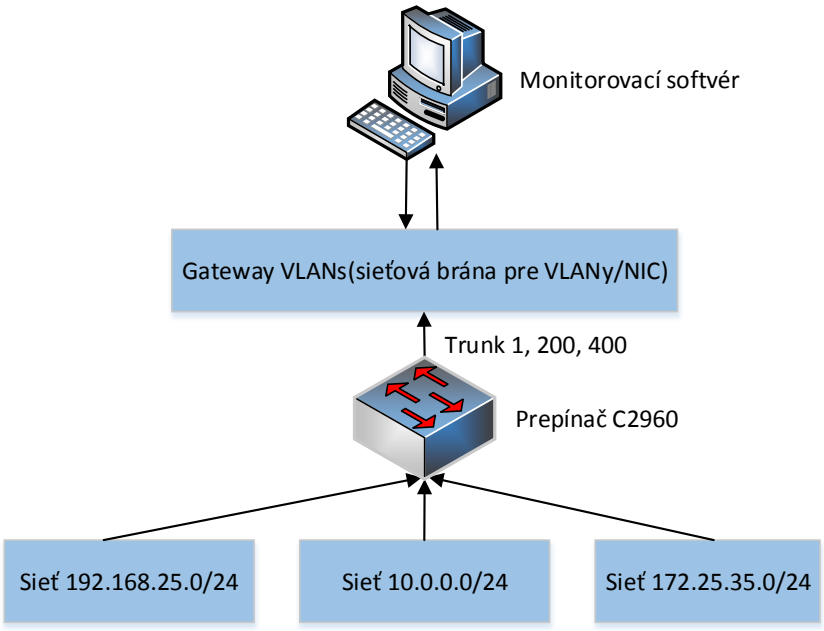
Obr. 3.14: Znázornenie MIB stromu

4 IMPLEMENTÁCIA RIEŠENIA A KONFIGURÁCIA SIETE

Po konzultácií so sieťovým administrátorom v laboratórnej sieti, sa rozhodlo monitorovací softvér nainštalovať na externý počítač, ktorý bude slúžiť ako monitorovací server a zároveň ako sieťová monitorovacia brána pre všetky tri laboratórne siete. Takéto riešenie odporúča aj rada výrobcov monitorovacieho softvéru, hlavne z dôvodu spoľahlivosti, bezpečnosti, výkonnosti a nezávislosti takéhoto systému.

Ako monitorovací server sa použil jednoduchý desktopový počítač, ktorý nemal dovtedajšie využitie v laboratóriu. Výkonnostne sa jedná o slabší počítač, teda bolo dôležité uvažovať aký softvér použiť a aké hardvérové nároky pri monitorovaní laboratórnej siete bude tento softvér mať.

Z toho dôvodu je optimálnym riešením softvér PRTG, pretože jeho hardvérové nároky do počtu 1000 senzorov(približne 100 zariadení) sú 2 fyzické CPU jadrá, 3 GB RAM a 250 GB HDD. Počítač, ktorým laboratórium disponuje má špecifikácie: 2 fyzické jadrá Intel(R) Celeron(R) G1820 s taktom 2,70GHz, 4GB RAM pamäte a 300GB HDD. Na počítači beží systém Windows 8 Pro, na ktorý je použitá akademická licencia z laboratória.



Obr. 4.1: Štruktúra monitoringu

4.1 Konfigurácia VLAN a monitorovacích senzorov na jednotlivých zariadeniach

Desktopový počítač v laboratóriu využíva sieťovú kartu Realtek PCIe GBE Family Controller, ktorá disponuje 1Gb/s rozhraním. Sieťová karta tohto typu však nedisponuje priamo rozšírením VLAN(virtual local area network), preto spočiatku nebolo možné počítač nakonfigurovať pre VLAN rozhrania priamo v nastaveniach OS, avšak riešenie ponúka priamo firma Realtek, ktorá dodáva softvér, diagnostické rozšírenie Ethernet Diagnostic Utility[1], v ktorom je možné nakonfigurovať VLAN aj pre karty ktoré toto rozšírenie priamo nepodporujú v operačnom systéme.

```
interface GigabitEthernet0/41
 description DOHLED
 switchport trunk native vlan 300
 switchport trunk allowed vlan 1,200,400
 switchport mode trunk
```

Obr. 4.2: Konfigurácia na prepínači G2960 port Ge0/41 pre dohledové PC

Vytvorili sme teda tri VLAN siete 1, 200 a 400 a na pripojenom Cisco prepínači c2960 na porte GigabitEthernet0/41 , ktorý je priamo spojený s DOHLEDOVÝM PC. Tri trunkové VLAN siete 1, 200 a 400 [2] sú zase zapuzdrené do neoznačenej native VLAN 300, ktorá takto prenáša dáta z troch sietí do jedného bodu, konfigurácia na prepínači obrázok.4.2

```
interface GigabitEthernet0/13
 description DOHLED-172-25-35-0
 switchport access vlan 200
 switchport mode access
```

Obr. 4.3: Konfigurácia na prepínači G2960 port Ge0/13 pre VLAN200

Na obrázku4.3 môžeme vidieť konfiguráciu rozhrania Ge0/13 do ktorého je pripojená VLAN 200 ktorá posiela dáta cez sieť 172.25.35.0 a umožňuje takto prístup do tejto siete. Typ VLAN je *switchport mode access* z dôvodu, že nie je potreba zapuzdrovať ďalšie dáta a prenáša len dáta VLAN 200.

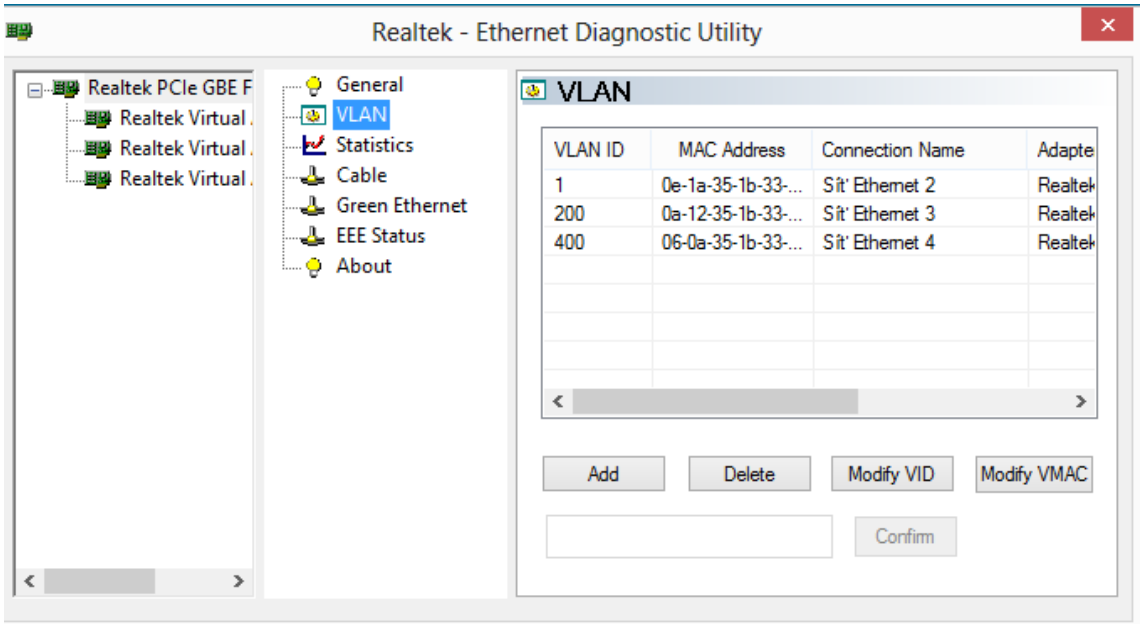
[1] Voľné dostupný na stiahnutie na http://www.realtek.com.tw/Downloads/downloadsView.aspx?Conn=4&DownTypeID=3&Langid=1&Level=5&PFid=5&PNid=13

[2] trunk – VLAN sieť ktorá v sebe nesie zapuzdrené dáta z iných VLAN

```
interface GigabitEthernet0/16
 description DOHLED-10-SITE
 switchport access vlan 400
 switchport mode access
```

Obr. 4.4: Konfigurácia na prepínači G2960 port Ge0/16 pre VLAN400

Na obrázku4.4 môžeme vidieť konfiguráciu rozhrania Ge0/16 do ktorého je pripojená VLAN 400 ktorá posiela dáta cez sieť 10.0.0.0 a umožňuje takto prístup do tejto siete. Typ VLAN je rovnako *switchport mode access* z dôvodu, že nie je potreba zapuzdrovať ďalšie dáta a prenáša len dáta VLAN 400.



Obr. 4.5: Rozšírenie VLAN Realtek

Pretože je VLAN 1 na prepínači použitá v sietí 192.168.25.0, tak sa dáta prenášajú na DOHLEDOVÝ PC pomocou VLAN 300 ktorá na PC nie je viditeľná lebo vystupuje ako VLAN 1, alebo teda ako základná sieťová karta, čo môžeme vidieť na obrázku 4.5.

Pripojením Cisco prepínača c2960, sme získali prístup do siete 192.168.25.0, kde prebieha základný monitoring pre pár výukových Cisco zariadení, o ktorých je dôležité mať prehľad z dôvodu výuky.

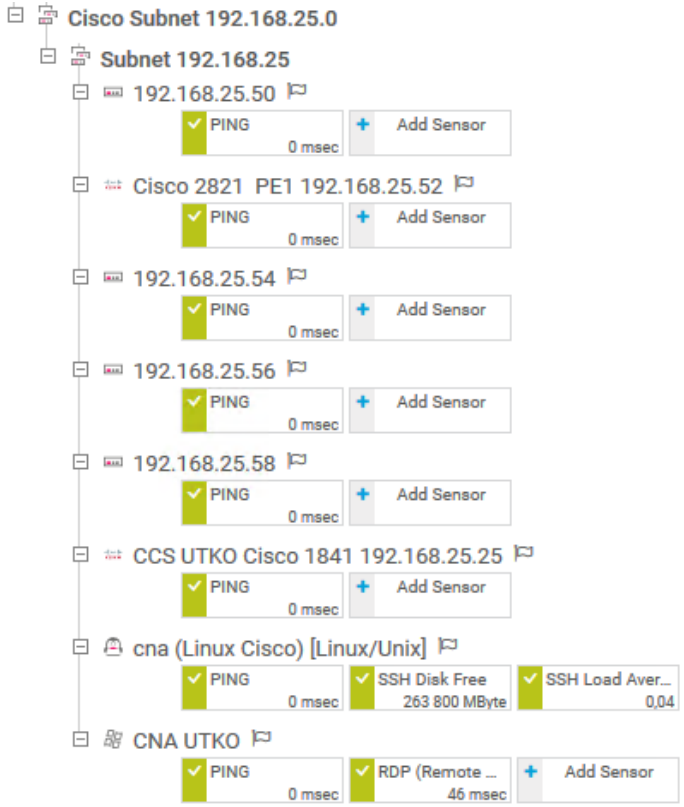
4.1.1 Konfigurácia siete 192.168.25.0 a zariadení v nej

Na obrázku4.6 môžeme vidieť monitorovanie zariadení v sietí, 192.168.25.0, kde je päť výukových zariadení, jeden CSS UTKO smerovač 1841 na ktorom beží kon-

textové menu a na ktorý sa pripájajú študenti pri výuke. Pretože sú to výukové zariadenia a neprebieha na nich stála činnosť, tak požiadavka bola monitorovať len ich stav dostupnosti pomocou sieťového nástroja PING.

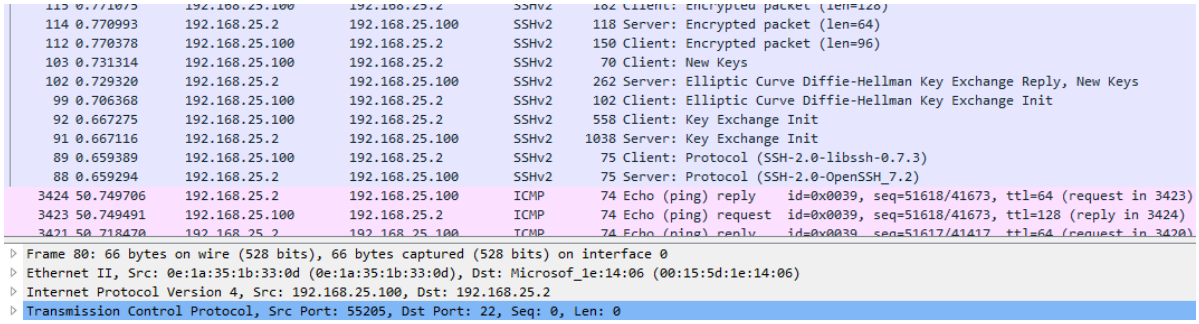
Ďalej môžeme vidieť zariadenie cna(IP 192.168.25.2), čo je Linuxový systém pre podporu Cisco úloh pri výuke bežiaci na terminálovom servery. Na tento systém vzišla požiadavka monitorovať jeho dostupnosť(PINGom) protokolom ICMP, diskovú kapacitu(SSH Disk Free) a počet využití Secure Shell (SSH) senzorom(SSH Load Average), všetky tieto senzory obsahuje knižnica PRTG. Senzor SSH Disk Free dokáže prechádzať stromovú štruktúru Linuxu a zistiť tak aktuálne hodnoty pre voľné miesto na disku. Pre SSH senzory je potrebné zadať len prihlasovacie údaje SSH.

Posledné zariadenie ktoré je monitorované, je CNA UTKO, ide vlastne o virtuálny systém Windows 10 na ktorom sú potrené materiály pre Cisco výuku, beží rovnako na terminálovom servery a využíva monitirovanie dostupnosti a protokol RDP(Remote Desktop Protokol – protokol vzdialenej plochy), oba senzory sú v základe dostupné v PRTG.



Obr. 4.6: Monitorovanie subnetu 192.168.25.0 v PRTG softvéry

Na obrázku4.7 môžeme vidieť sieťovú komunikáciu Cna Linux Systému(192.168.25.2) s monitorovacím systémom(192.168.25.100), ktorú sme zachytávali pomocou sieťového paketového analyzátora Wireshark[3]. Rovnako sme overovali konfigurácie pre všetky monitorované zariadenia siete 192.168.25.0.



Obr. 4.7: Zachytená komunikácia SSHv2 a ICMP(Ping) protokolov Wiresharkom

4.1.2 Konfigurácia siete 10.0.0.0

Sieť 10.0.0.0 je sieť na ktorej beží projekt a sú v nej zahrnuté zariadenia z dvoch stojanov(rackov). Hlavná konfigurácia pre túto sieť beží na Dell prepínači, ktorý je v treťom stojane. Dell prepínač zároveň prepojuje zariadenia projektu – GPON, Terminálové servery 2 a 3 s prvým stojanom kde sa nachádza FPGA a ENDACE systém. Sú vytvorené dve základné VLAN - VLAN 2 ktorá reprezentuje sieť 10.0.0.0 a VLAN 172 siete 172.25.35.0. obrázok. 4.8

```
vlan 2
name "interni_sit"
vlan 172
name "laboratorni_sit"
exit
```

Obr. 4.8: Základné VLAN siete na Dell prepínači

```
interface vlan 2
ip address 10.0.0.1 255.255.255.0
exit
interface vlan 172
ip address dhcp
exit
```

Obr. 4.9: IP adresy priradené vo VLAN 2 a 172

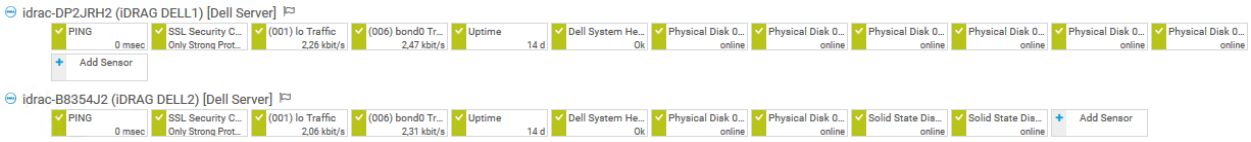
[3]Voľne dostupný na stiahnutie https://www.wireshark.org/download.html

```
interface Gi1/0/1
description "iDRAC-R550"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Gi1/0/2
description "iDRAC-T330"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Gi1/0/3
description "eSXI-T550"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Gi1/0/4
description "TERM3"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Gi1/0/5
description "Laborator-R550"
spanning-tree portfast
switchport access vlan 2
exit
```

Obr. 4.10: VLAN Konfigurácie pre iDrag prepínače a TERM3 v sietí 10.0.0.0

Takto sme priradili do jednotlivých VLAN všetky zariadenia v sietí 10.0.0.0 a sieť 172.25.35.0, kde rozsah priraďuje Term DHCP server 172.25.35.2.

Týmto spôsobom sme zabezpečili viditeľnosť iDrag Dell Serverov pre monitorovací softvér. Následné sme vybrali v softvéry PRTG senzory na monitorovanie jednotlivých atribútov týchto serverov a na obrázku 4.11 môžeme vidieť kompetnú sadu senzorov pre tieto servery. Monitorujeme dostupnosť(PING), zabezpečenie komunikácie (SSL), jednotlivé prevádzku na portoch(Traffic senzor), čas spustenia(UpTime), celkové zdravie zariadení(Dell System Health) a jednotlivé pevné disky(SSD a HDD senzor).



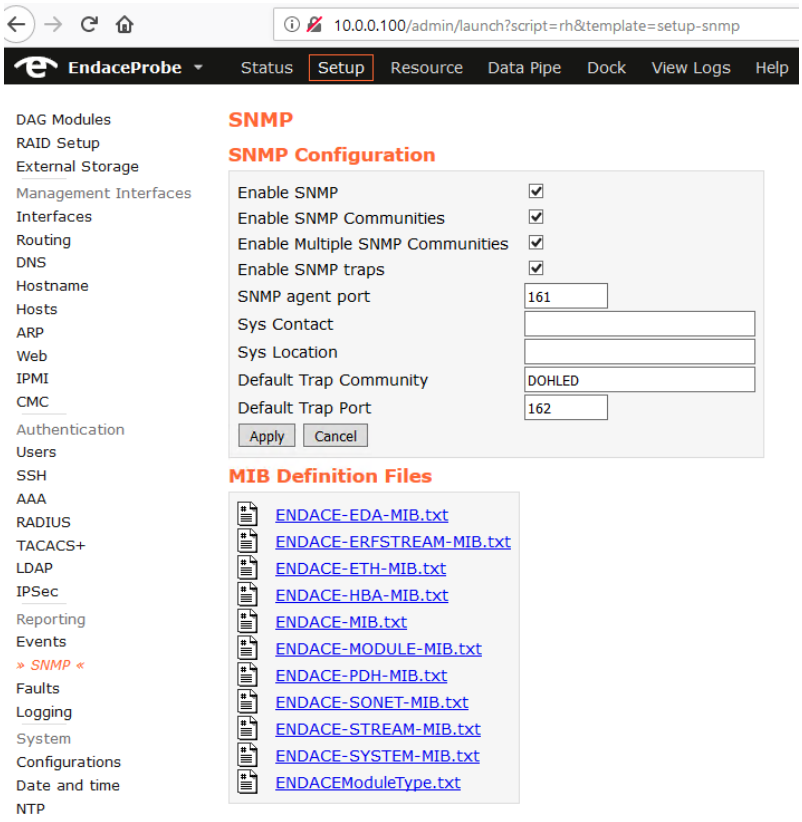
Obr. 4.11: Konfigurácie pre iDrag prepínače a TERM3 v sietí 10.0.0.0 a ich zaradenie vo VLAN

4.1.3 Konfigurácia GPON a ENDACE

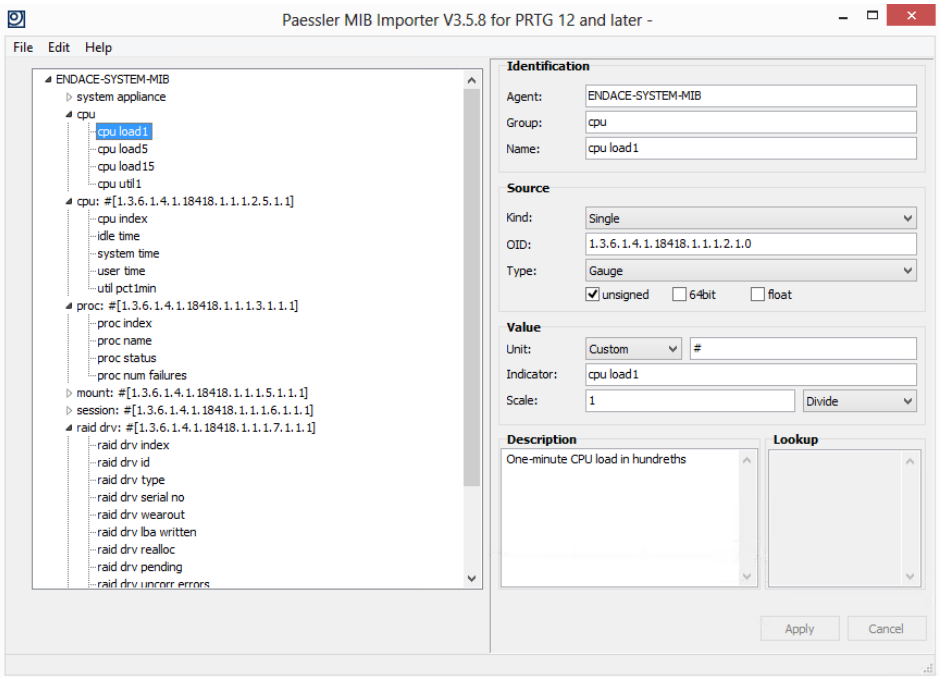
Na obrázku 4.12 môžeme vidieť priradenie ďalších zariadení do jednotlivých VLAN a distribuovanie týchto VLAN na DOHLEDOVÝ PC. Sú tu najmä dve dôležité zariadnie na monitoring a to zariadenie **ENDACE** a zariadenie **GPON**. Obe zariadenia bolo potrebné nastaviť na SNMP dohľad.

```
description "KALI-LINUX-L53.5-6A-Zasuvka"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Gi1/0/14
description "to-laborator-cisco-switch"
spanning-tree portfast
switchport access vlan 172
exit
!
interface Gi1/0/15
description "trunk-to-TERM3-new-SQL-KALI"
spanning-tree portfast
switchport mode trunk
switchport access vlan 172
switchport trunk allowed vlan 2,172
exit
!
interface Gi1/0/16
description "DOHLED-PC"
spanning-tree portfast
switchport access vlan 2
switchport trunk allowed vlan 2,172
exit
!
interface Gi1/0/23
description "ENDACE-Management"
spanning-tree portfast
switchport access vlan 2
exit
!
interface Te1/0/2
description "GPON-uplink"
spanning-tree portfast
switchport mode trunk
switchport trunk allowed vlan 2
```

Obr. 4.12: Konfigurácie pre ostatné zariadenia v sietí 172.25.35.0 a 10.0.0.0



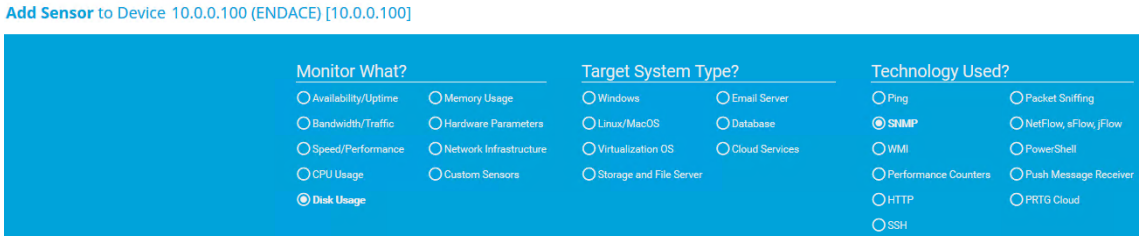
Obr. 4.13: Konfigurácia SNMP protokolu pre ENDACE pomocou web rozhrania



Obr. 4.14: Import MIB Endace súborov do PRTG

Obrázok 4.13 zobrazuje konfiguráciu SNMP protokolu pre zariadenie ENDACE.

Na SNMP sa používa port *161*, Trap port je *162* a *Trap Community* DOHLED. V spodnej časti obrázka, môžeme vidieť definíciu MIB súborov pre monitorovanie cez SNMP priamo od výrobcu zariadenia. Tieto súbory boli importované priamo do PRTG[4], obrázok 4.14. Získali sme tak možnosť nastaviť si vlastné SNMP senzory priamo z definovaných súborov výrobcu.



Obr. 4.15: Menu na pridanie senzorov v PRTG

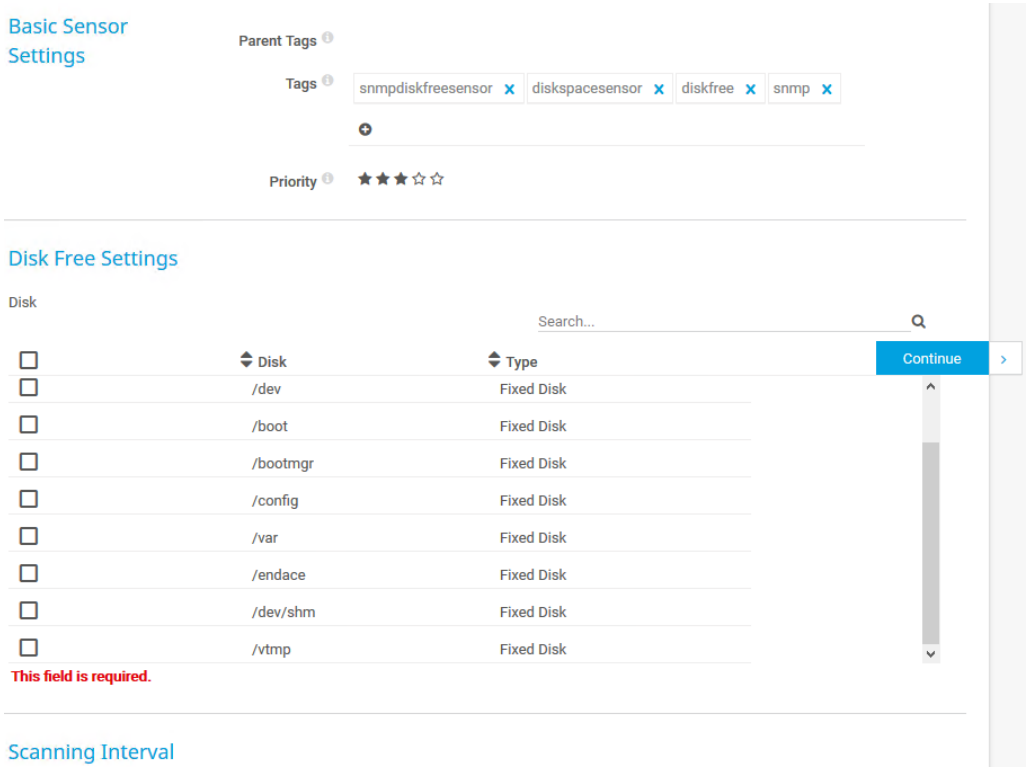
Obr. 4.16: Príkladový senzor kapacity disku pre ENDACE

Menu pre senzory, obrázok 4.15, ktoré bolo používané na výber senzorov pre všetky monitorované zariadenia v laboratórnej sietí, v menu je možné bližšie špecifikovať účel monitoringu, ktoré protokoly sa majú použiť , prípadne typ cieľového systému.

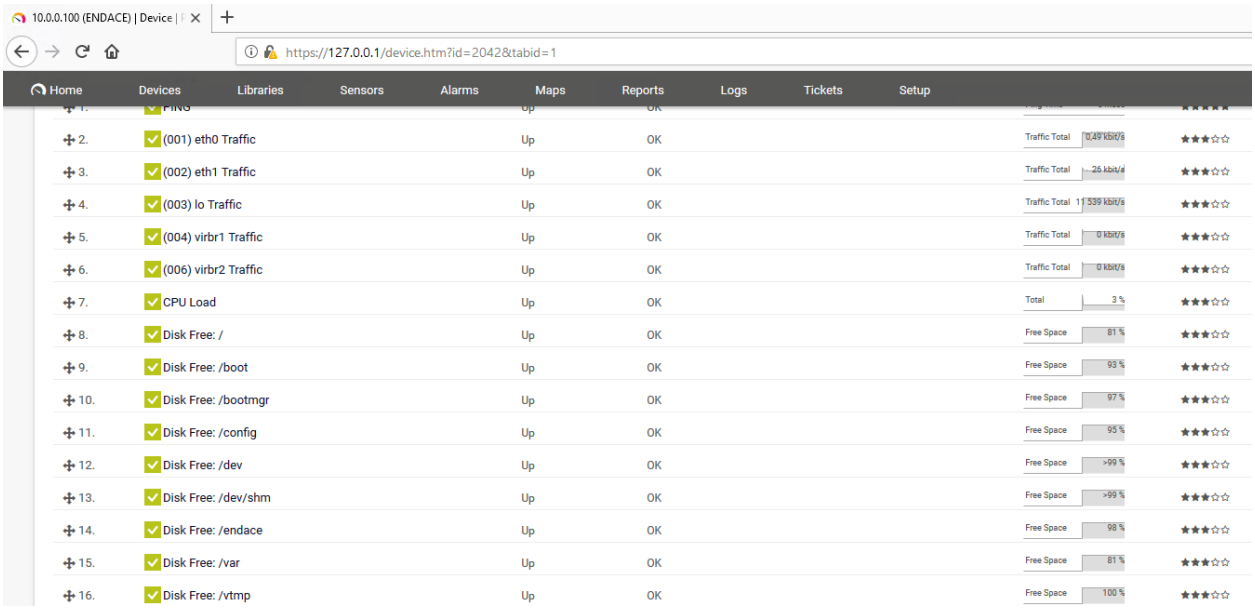
Nesledujúci obrázok 4.16 zobrazuje už konkrétny typ SNMP senzoru, ktorý bol použitý, išlo konkrétne o senzor *Disk Free*, ktorý monitoruje voľnú kapacitu pevného disku na ENDACE.

[4]PRTG MIB Importer dostupný na stránke https://www.paessler.com/tools/mibimporter

Na obrázku 4.17 vidíme stromovú štruktúru pre senzor *Disk Free*, takto je možné vybrať presne ktoré zložky a štruktúry disku budú monitorované. Obrázok 4.18 znázorňuje už fungujúce a nastavené monitorovacie senzory pre ENDACE.



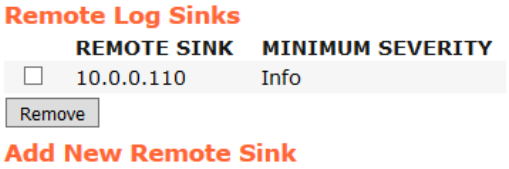
Obr. 4.17: Stromová štruktúra pre senzor SNMP Disk Free



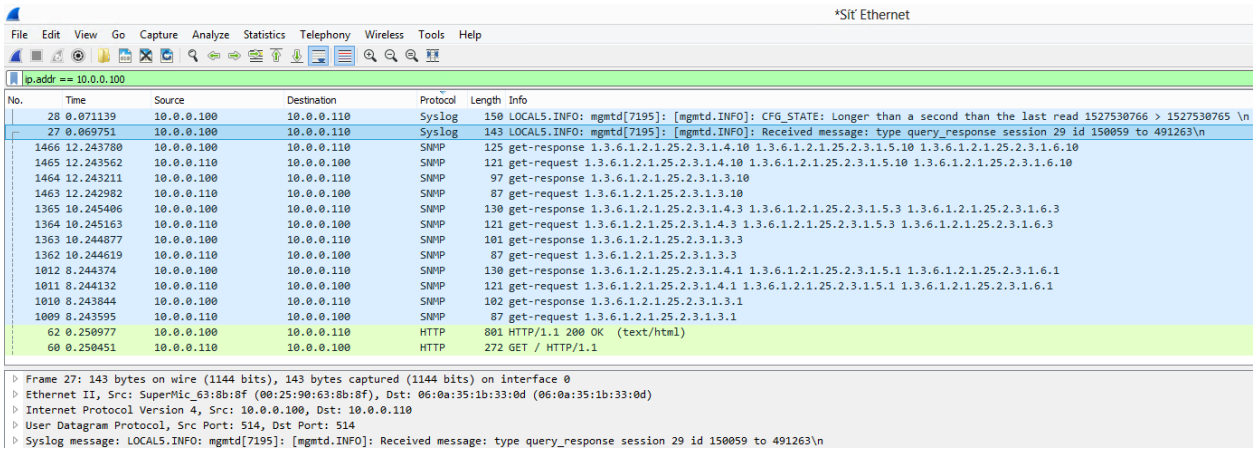
Obr. 4.18: Bežiace monitorovacie senzory na ENDACE

Nastavenie Trapv2 správ a Syslog na ENDACE sa uskutočnilo rovnako vo web rozhraní, kde sa pridal port pre Trap správy UDP 162 a nastavil sa Community string na DOHLED obrázok 4.19. Overenie prijímania správ sa uskutočnilo analyzátorom Wireshark, kde sa filtrovala IP adresa ENDACEu a tak sme overili, funkčnosť SNMP protokolu, obrázok4.21

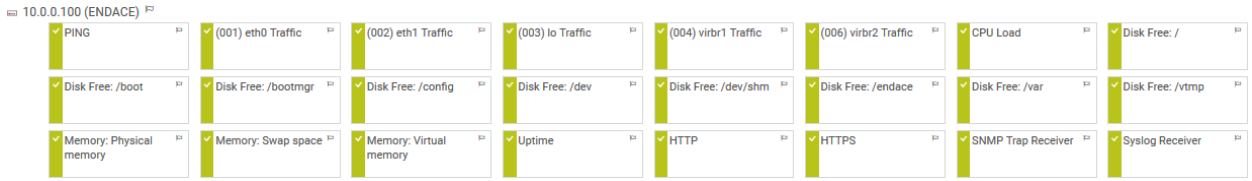
Obr. 4.19: ENDACE Trapv2c na DOHLED-PC 10.0.0.110



Obr. 4.20: ENDACE Syslog na DOHLED-PC 10.0.0.110



Obr. 4.21: Overenie SNMP a Syslog komunikácie medzi ENDACE a DOHLED-PC

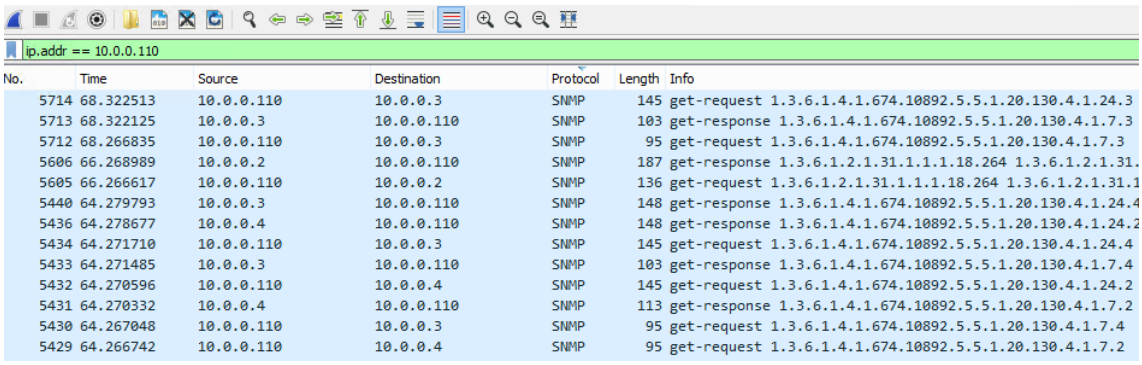


Obr. 4.22: Všetky monitorovacie senzory na ENDACE

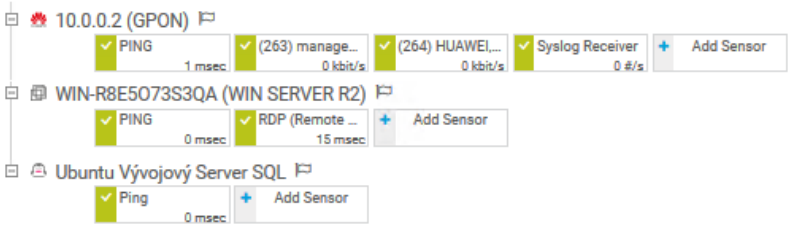
Konfigurácia SNMP protokolu pre zariadenie **GPON** od Huawei je na obrázku 4.23, za ňou nasleduje overenie SNMP komunikácie medzi GPON(10.0.0.2) a DOHLED-PC(10.0.0.110), rovnako tam môžeme vidieť aj SNMP komunikáciu Dell iDrag Serverov(10.0.0.3 a 10.0.0.4) a DOHLED-PC(10.0.0.110). Na spodnom obrázku4.25 môžeme vidieť bežiace senzory pre GPON a dva servery(Ubuntu a WinR2), boli použité senzory z ponuky PRTG a pridali sme ich rovnako ako v prípade zariadenia ENDACE. 4.15

```
MA5683T#config
MA5683T(config)#snmp-agent sys-info
{ contact<K>|location<K>|version<K> }:version
{ all<K>|v1<K>|v2c<K>|v3<K> }:v2c

MA5683T(config)#snmp-agent community
{ read<K>|write<K> }:read
{ communityname<S><Length 1-32,50> }:GPON

   display snmp-agent community read
Community name: GPON
   Storage type: nonVolatile
   View name: ViewDefault
```

Obr. 4.23: Konfigurácia SNMP na zariadení Huawei GPON



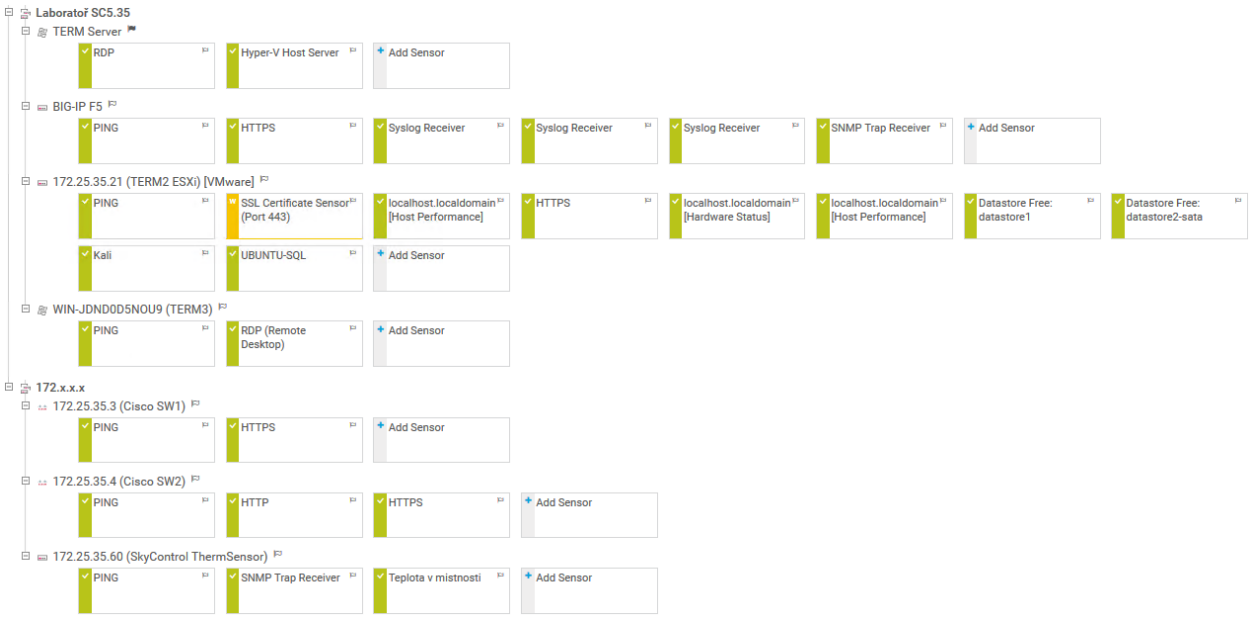
Obr. 4.24: Komunikácia SNMP GPON a dvoch iDrag Dell serverov s DOHLED-PC



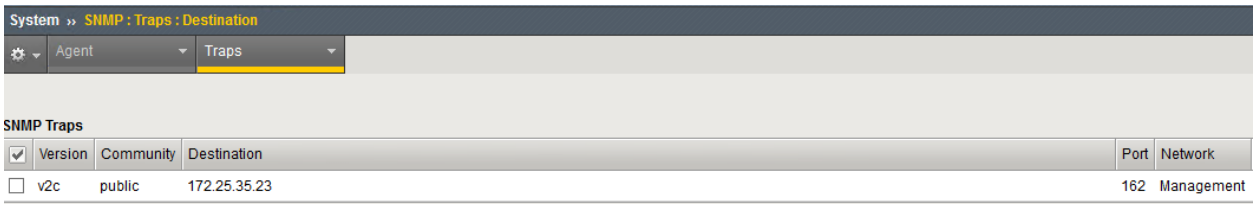
Obr. 4.25: Senzory na GPON, Ubuntu a WINR2 serveroch

4.1.4 Sieť 172.25.35.0, BIG IP a teplotný senzor SkyControl

Tretia a posledná monitorovaná sieť je **172.25.35.0**, obrázku 4.26. Prvé monitorované zariadenie je virtuálny TERM Server(172.25.35.2), na ktorom beží RDP senzor(Remote Desktop protocol) a Hyper-V Host Server, obidva senzory sa nachádzajú v základnom senzorickom vybavení PRTG, preto nie je potrebné ich konfigurovať a stačí ich len pridať na virtuálne zariadenie.



Obr. 4.26: Senzory na zariadeniach v sietí 172.25.35.0



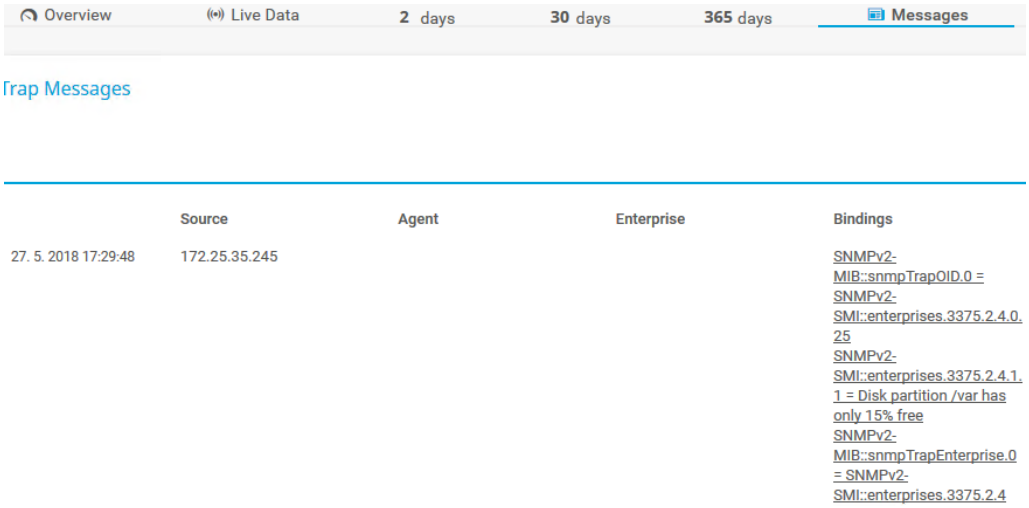
Obr. 4.27: SNMPv2c Trap na zariadení f5 BIG IP

Obrázok 4.27 zobrazuje konfiguráciu SNMPv2c Trap správ na zariadení f5 BIG IP, konfigurácia prebieha vo webovom rozhraní, v časti *System>SNMP>Traps* a je potrebné nastaviť IP adresu destinácie(serveru) kde sa budú Trap správy posielať, rovnako treba nastaviť *Community string* a port na 162.

Z obrázku 4.26 vidíme senzory na serveroch Term2 a Term3. Term2 je virtuálny EXSi server v systéme VMWare, na monitoring virtuálnych serverov má PRTG pripravené senzory priamo od výrobcov. Preto v prípade známeho výrobcu alebo známej platformy pre virtuálne servery nie je potrebné senzory zložite konfigurovať

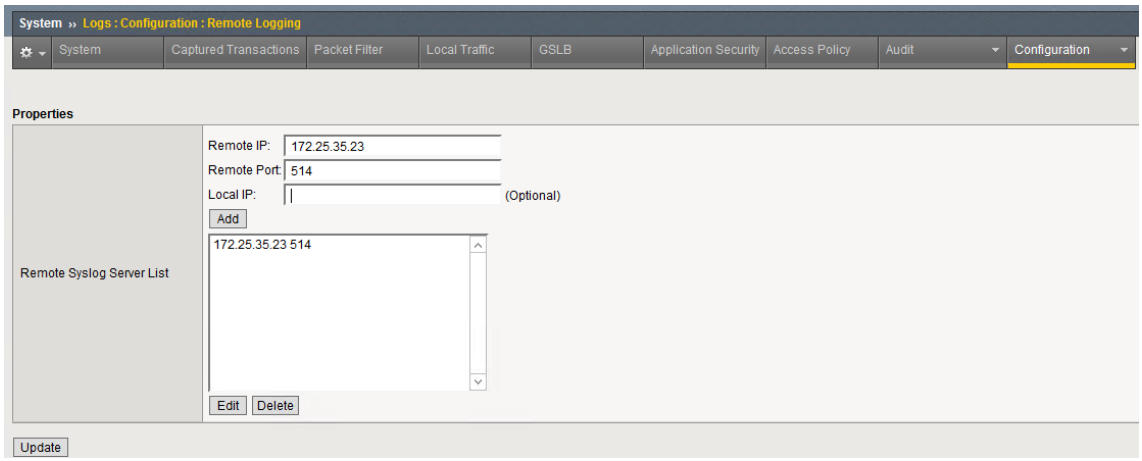
a PRTG sám zvládne namapovať celý virtuálny systém a dať potom na výber čo sa má monitorovať. Term3 používa len monitorovanie dostupnosti PING a RDP senzor.

Overenie prijatého SNMP Trapu na PRTG servery, obrázok 4.28. Trap správa sa posiela každých 5 minút ak je to potrebné a v časti *Bindings* môžeme vidieť dôvod zasielania Trap správy od zariadenia(BIG IP 172.25.35.245) a tým je zmenšujúce sa miesto na disku kde ostáva posledných 15% voľných.

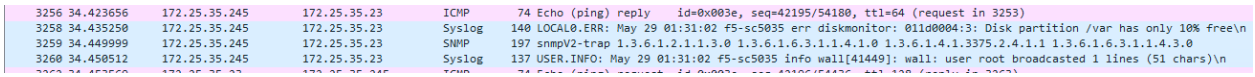


Obr. 4.28: Prijatá SNMP Trapv2c správa na PRTG servery

Tu môžeme vidieť nastavenie Syslog správ s logmi, ktoré posiela zariadenie na vzdialený monitorovací server 172.25.35.23

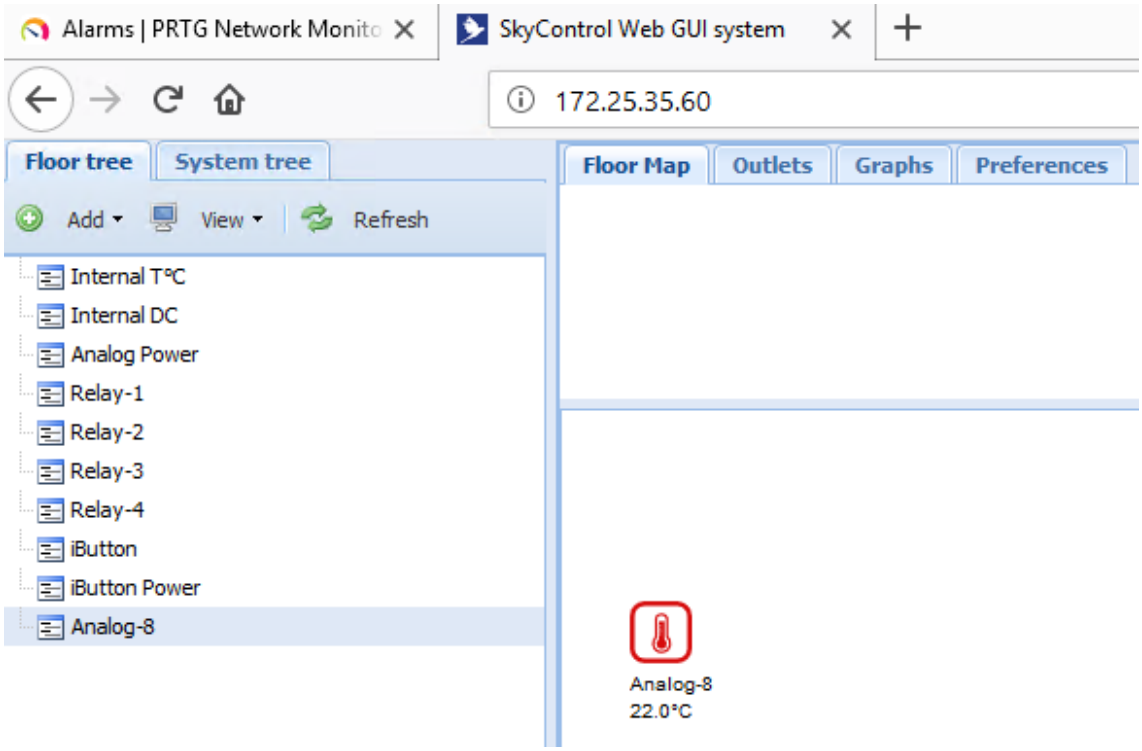


Obr. 4.29: Nastavenie Syslog na BIG IP zariadení



Obr. 4.30: SNMP Trap a Syslog zo zariadenia BIG IP zachytený Wiresharkom

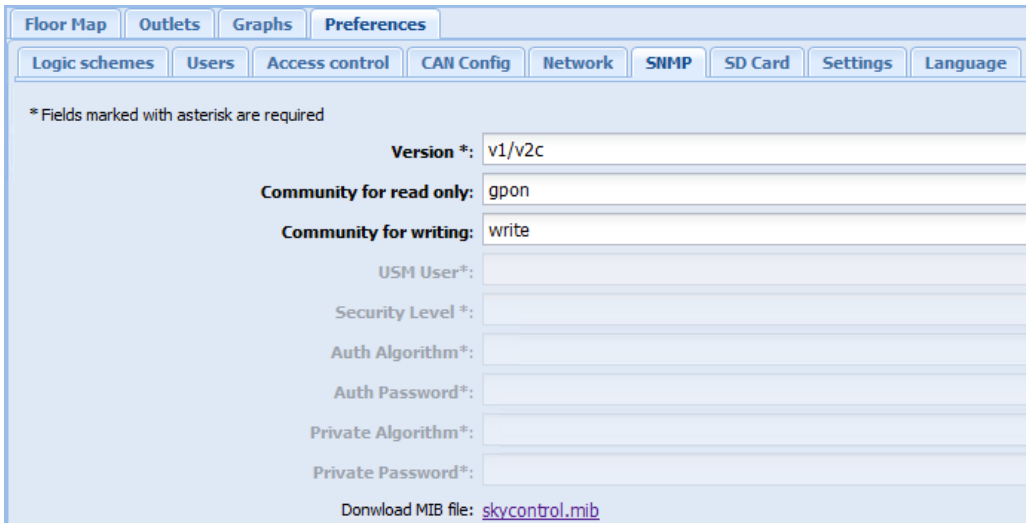
Posledným významným zariadením, ktoré bola potreba monitorovať je systém **SkyControl(IP 172.25.35.60)**a jeho analógový teplotný senzor, ktorý posiela informácie o aktuálnej teplote v laboratórnej miestnosti. Na obrázku 4.31 je možné vidieť analógovú teplotnú sondu a jej aktuálnu teplotu.



Obr. 4.31: Analógový Senzor Teploty systému SkyControl

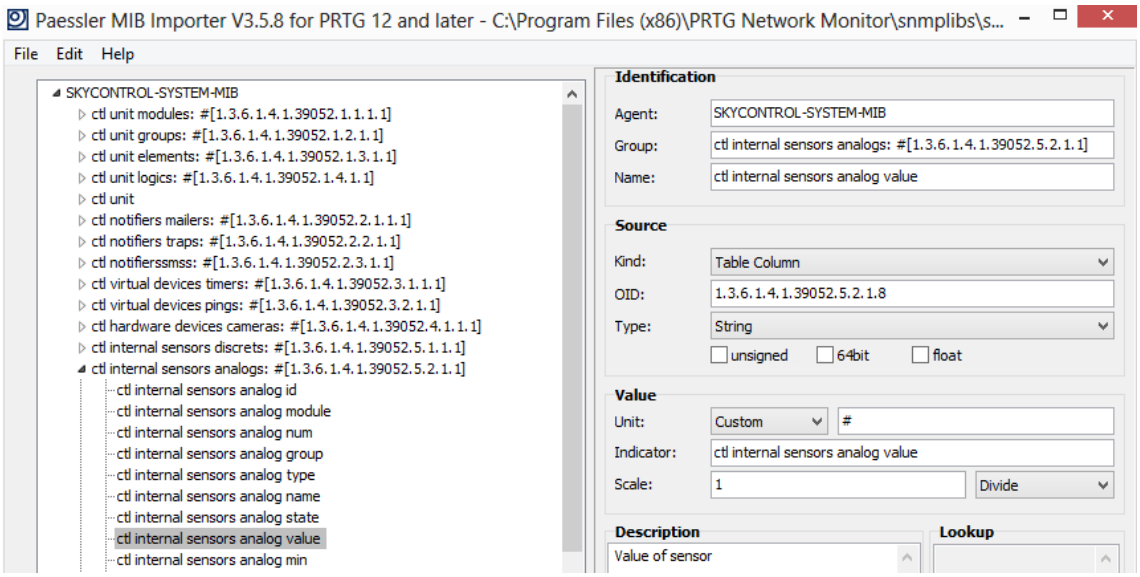
Nastavenie SNMP protokolu na zariadení SkyControl prebieha v menu *Preferences>SNMP*. Je potrebné nastaviť verziu a *Community String* pre čítanie SNMP správ.

Následné môžeme použiť niektorý z PRTG ponúkaných senzorov pre SNMP. V SNMP menu je tiež dostupný súbor MIB priamo od výrobcu SkyControl.

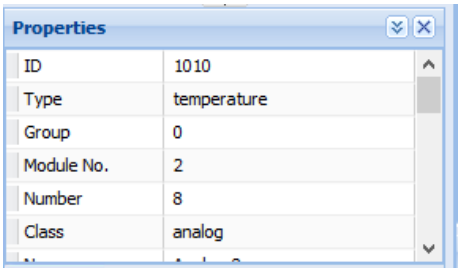


Obr. 4.32: Nastavenie SkyControl SNMP

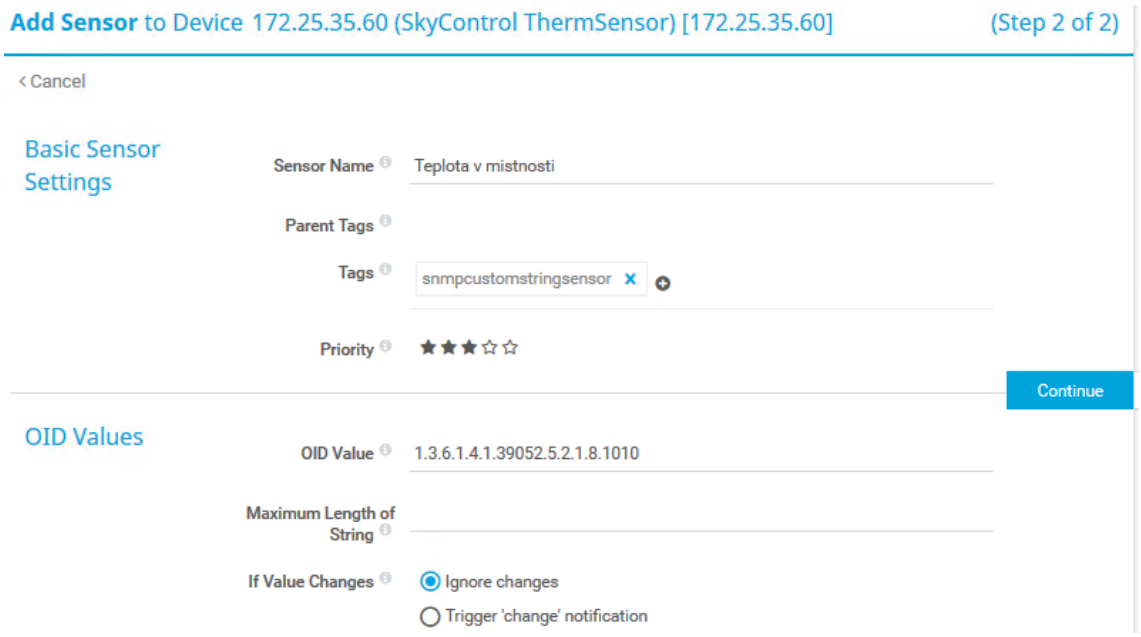
Avšak na monitorovanie teploty, potrebujeme definovať vlastný SNMP Custom String senzor. Na to použijeme MIB súbor skycontrol 4.32, priamo od výrobcu, ktorý pomocou PRTG MIB Importer naimportujeme do PRTG knižníc, obrázok 4.33. Vo vlastnostiach senzoru sme zistili, že teplotný senzor má číslené označenie *1010*, toto označnenie teda stačí dodať na koniec číselného zápisu senzoru pri vytváraní senzora. PRTG začne prehľadávať importované MIB a zistí, že nami zadané OID(object ID) s doplnkovou hodnotou na konci odpovedá danému analógovému teplotnému senzoru.



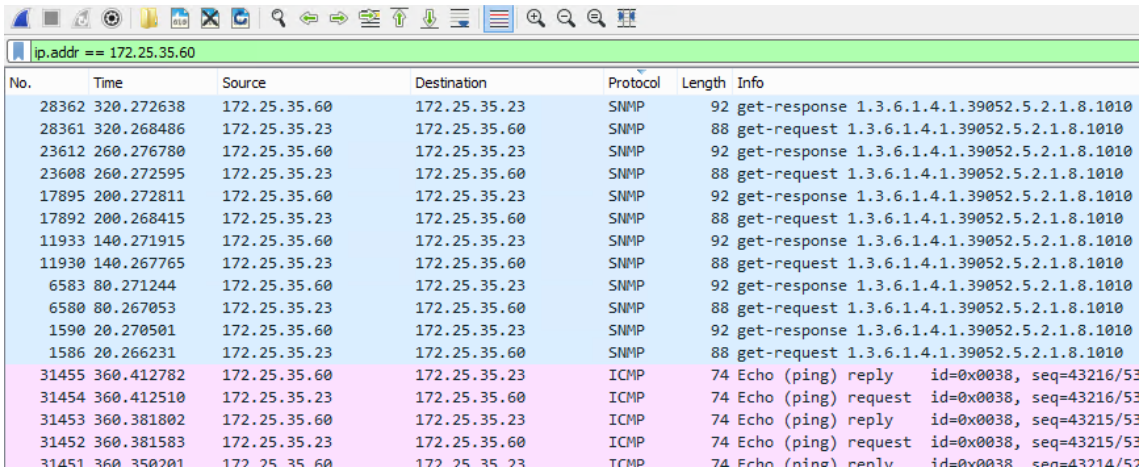
Obr. 4.33: Štruktúra MIB SkyControl a OID pre senzory



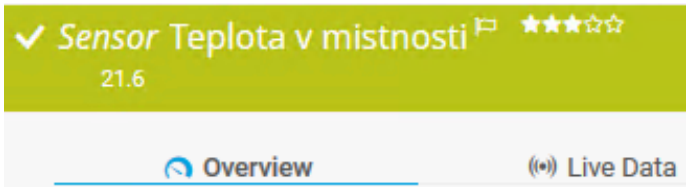
Obr. 4.34: Označenie teplotného senzora v SkyControl systéme



Obr. 4.35: Označnie OID a nastavenie senzoru v PRTG



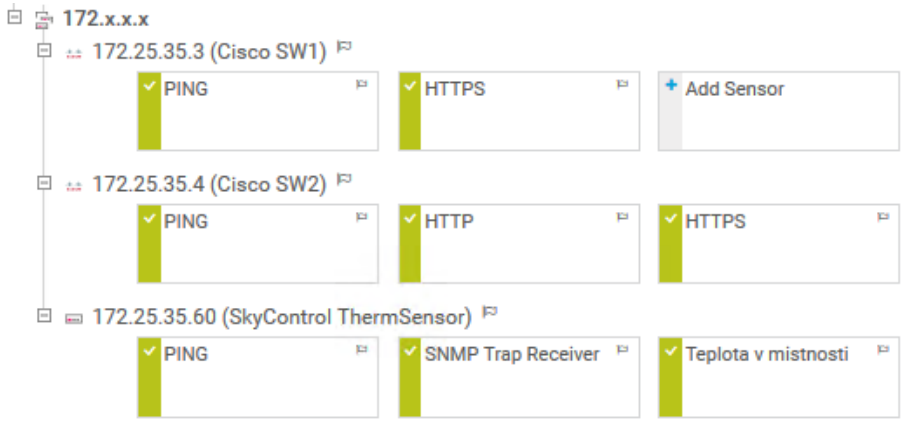
Obr. 4.36: Overenie komunikácie SNMP medzi SkyControl a DOHLED-PC



Obr. 4.37: Overenie funkčnosti SNMP senzoru teploty

Obrázok 4.35 je konfigurácia a nastavenie senzoru pre PRTG, z MIB súborov vieme, že senzor má číslené označenie *1.3.6.1.4.1.39052.5.2.1.8.1010*. Funkčnosť komunikácie overíme Wiresharkom 4.36 medzi systémom SkyControl(172.25.35.60) a DOHLED-PC(172.25.35.23). Posledné overenie funkčnosti je prijatie hodnoty SkyControl temperature senzoru na monitorovacom servery a následné vykreslenie v PRTG, obrázok 4.37.

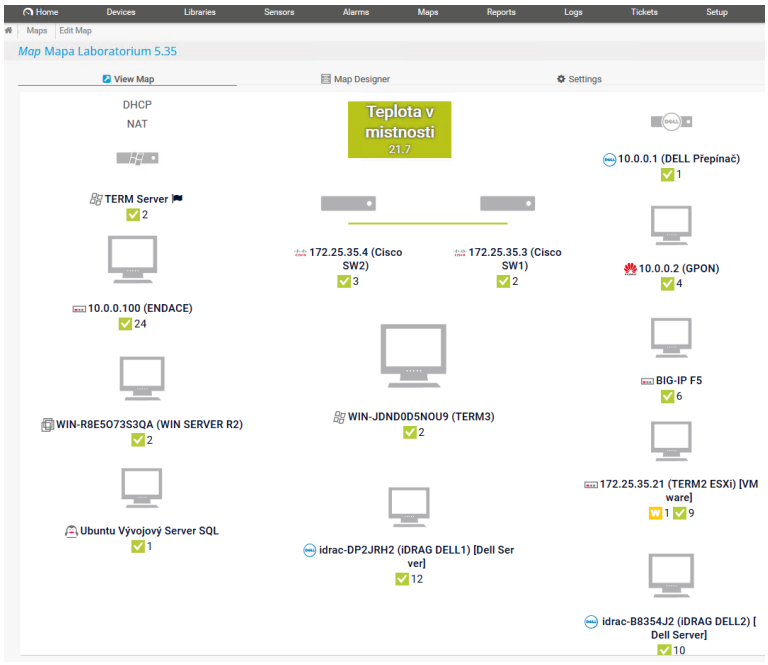
Posledné dve zariadenia – zásuvkové prepínače Cisco SW1 a Cisco SW2, obrázok 4.38, sú monitorované jednoduchými nástrojmi na zistenie dostupnosti PING a ďalej sa monitorujú aplikačné hypertextové prenosové protokoly(HTTP) a ich bezpečnejšia verzia HTTPS. Senzory na toto monitorovanie sú dostupné už priamo v PRTG, teda stačí úplne základné nastavenie senzorov.



Obr. 4.38: Senzory na Cisco prepínačoch SW1 a SW2 a SkyControl

4.2 Monitorovacie mapy

Posledným významným prvkom, ktorý je v PRTG konfigurovaný sú rôzne monitorovacie mapy. Na ukážku máme dve mapy, jednu normálnu a ďalšiu tzv.koláčovú mapu.



Obr. 4.39: Normálna mapa monitoringu laboratórnej siete

Obr. 4.40: „Koláčová“ mapa monitoringu siete

5 ZÁVĚR

Cieľom tejto bakalárskej práce bolo navrhnúť ucelený dohľadový systém pre školské laboratórium transportných sietí a implementovať tento systém.

V teoretickej časti je popísané zapojenie laboratória, prvkov v ňom a revízia dovtedajšieho riešenia. Sú detailne opísané hlavné sieťové prvky, ich činnosti a využitie v laboratóriu.

Ďalej sa v teoretickej časti nachádza porovnanie štyroch dodávaných monitorovacích softvérov. Sú popísané ich výhody a nevýhody a možnosti v akademickom prostredí. Rovnako sú definované hlavné kvalitatívne požiadavky pre monitorovací softvér.

Neskôr je detailne popísaný hlavný manažmentový protokol SNMP. Jeho história, časti, typy operačných správ, prenosy a štruktúry MIB stromov, názvy OID.

V praktickej časti práce sa práca zameriava na konfiguráciu jednotlivých sietí, protokolov a zariadení. Vytvorili sa tri VLAN siete, ktoré sú v konečnom dôsledku zlúčené do jednej monitorovacej entity(serveru). Takéto riešenie prinieslo prehľadnosť do množstva sieťových zariadení a umožnilo monitorovať viaceré odlišné siete z jedného miesta.

Následné prebehla konfigurácia jednotlivých zariadení a konfigurácia manažmentových protokolov aby bol možný neustály dohľad a zabezpečená dostupnosť zariadení.

Na záver bola urobená konfigurácia teplotného senzoru, ktorý takto informuje sieťového administrátora o teplotách v laboratóriu a umožni tak zasiahnúť v prípade vysokých teplôt.

Celý dohľad je vizualizovaný monitorovacou mapou, ktorú je možné zdieľať sieťou a tak utvoriť rýchly pohľad na funkčnosť laboratórnej siete. Je to vizualizácia kde je dostatočný prehľad o jednotlivých senzoroch a zariadeniach.

Bol implementovaný monitorovací softvér, ktorý mal najväčšie výhody pre akademické prostredie, s pomocou softvéru sa vytvára dohľadový systém, ktorý monitoruje množstvo zariadení a zabezpečuje tak plynulý a bezproblémový chod laboratória transportných sietí.

LITERATÚRA

[1] NSR VUT *Network Research Group/ENDACE* [online]. [cit. 25. 02. 2018]. Dostupné z URL: <http://nsr.utko.feec.vutbr.cz/endace.php/>.

[2] prof. Raj Jain *Passive Optical Networks* [online]. [cit. 14. 03. 2018]. Dostupné z URL: <http://www.cse.wustl.edu/~jain/talks/ftp/itcom03.pdf/>.

[3] NSR VUT *Network Research Group/FPGA* [online]. [cit. 18. 04. 2018]. Dostupné z URL: <http://nsr.utko.feec.vutbr.cz/fpga.php/>.

[4] Chase Abbott F5 *What is BIG IP* [online]. [cit. 20. 03. 2018]. Dostupné z URL: <https://devcentral.f5.com/articles/what-is-big-ip-24596/>

[5] G2Crowd *Network-Monitoring* [online]. [cit. 23. 03. 2018]. Dostupné z URL: <https://www.g2crowd.com/categories/network-monitoring/>

[6] Michael Brandenburg *How to set a network performance baseline for network monitoring* [online]. [cit. 24. 03. 2018]. Dostupné z URL: <https://searchnetworking.techtarget.com/How-to-set-a-network-performance-baseline-for-network-monitoring/>

[7] DOOLEY, Kevin. , Ian J. BROWN. *Cisco IOS cookbook. 2nd ed. (Revised and updated)* [kniha]. Sebastopol, CA: O'Reilly, 2007, [cit. 11. 3. 2018]. ISBN 978-0-596-52722-8.

[8] MAURO, Douglas R. a Kevin J. SCHMIDT. *Essential SNMP. 2nd ed. (Revised and updated)* [kniha]. Sebastopol, CA: O'Reilly, 2005, [cit. 15. 3. 2018]. ISBN 978-0-596-00840-6.

[9] PAESLLER *How do SNMP, MIBs and OIDs work* [online]. [cit. 18. 03. 2018]. Dostupné z URL: <https://kb.paessler.com/en/topic/653-how-do-snmp-mibs-and-oids-work/>.

[10] ROSE, M. *RFC 1227 SMUX* [online]. [cit. 26. 04. 2018]. Dostupné z URL: <https://www.ietf.org/rfc/rfc1227.txt/>.

[11] PAESLLER *SNMP monitoring via OIDs MIBs* [online]. [cit. 13. 03. 2018]. Dostupné z URL: <https://blog.paessler.com/snmp-monitoring-via-oids-mibs/>.

[12] PAESLLER *It explained SNMP* [online]. [cit. 24. 03. 2018]. Dostupné z URL: <https://www.paessler.com/it-explained/snmp/>.

[13] Charles M. Kozierok *SNMP Protocol Message Format* [online]. [cit. 17. 03. 2018]. Dostupné z URL: <https://http://www.tcpipguide.com/free/t_SNMPProtocolMessagingandMessageFormats.htm/>

[14] Charles M. Kozierok *Structure of Management Information (SMI) and Management Information Bases (MIBs) Overview* [online]. [cit. 30. 03. 2018]. Dostupné z URL: <http://www.tcpipguide.com/free/t_TCPIPStructureofManagementInformationSMIandManagem.htm/>

[15] Charles M. Kozierok *TCP/IP MIB Objects, Object Characteristics and Object Types* [online]. [cit. 28. 03. 2018]. Dostupné z URL: <http://www.tcpipguide.com/free/t_TCPIPMIBObjectsObjectCharacteristicsandObjectTypes.htm>

[16] Charles M. Kozierok *TCP/IP MIB Object Descriptors and Identifiers and the Object Name Hierarchy and Name Notation* [online]. [cit. 19. 03. 2018]. Dostupné z URL: <http://www.tcpipguide.com/free/t_TCPIPMIBObjectDescriptorsandIdentifiersandtheObjec-2.htm>

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

VLAN virtuálna lokálna sieť – Virtual Local Area Network

SNMP protokol jednoduchého sieťového manažmentu – Simple Network Management Protokol

SGMP Protokol jednoduchého manažmentu brány – Simple Gateway Management Protokol

PING Packet Internet Groper – program PING

UDP užívateľský datagramový protokol – User Datagram Protocol

TCP/IP protokol riadenia prenosu/internetový protokol – Transmission Control Protocol/Internet Protocol

ISO Medzinárodná organizácia pre normalizáciu – International Organization for Standardization

TCP protokol riadenia prenosu – Transmission Control Protocol

IETF komisia pre technickú stránku Internetu – Internet Engineering Task Force

RFC Request for Comments

IoT Internet vecí – Internet of things

NMS Systém sieťového manažmentu – Network Management System

MPLS Multiprotokolové značkované prepínanie – Multiprotocol Label Switching

MGCP Kontrolný protokol brány médií – Media Gateway Control Protocol

TFTP Jednoduchý protokol na prenos súborov – Trivial File Transfer Protocol

VoIP Prenos hlasu Internetovým protokolom – Voice over Internet Protocol

OSI Otvorený systém prepojení Referenčný Model – Open Systems Interconnection Reference Model

OLT Optický linkový terminál – Optical Line Terminal

ONT Optický sieťový terminál – Optical Network Terminal

ONU Optická sieťová jednotka – Optical Network Unit

FPGA Pole Programovatelných hradiel – Field Programmable Gate Array

SSO Jednotné prihlasovanie – Single Sign-On

VPN Virtuálny privátny tunel sieťou – Virtual Private Newtwork