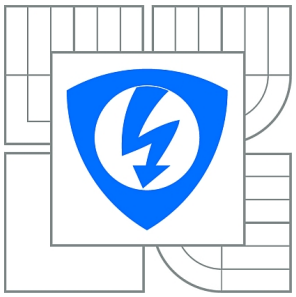
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MONITOROVÁNÍ PROVOZU SÍTĚ POMOCÍ DLOUHODOBĚ PRACUJÍCÍHO ANALYZÁTORU

NETWORK TRAFFIC MONITORING USING LONG WORKING ANALYSER

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

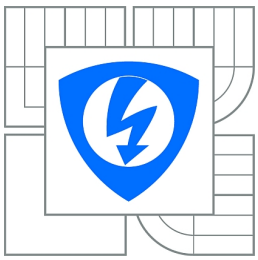
AUTOR PRÁCE — Bc. ALEŠ GILÍK

AUTHOR

VEDOUCÍ PRÁCE — Ing. VÁCLAV OUJEZSKÝ

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Aleš Gilík	***ID:***	119411
Ročník:	2	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Monitorování provozu sítě pomocí dlouhodobě pracujícího analyzátoru

POKYNY PRO VYPRACOVÁNÍ:

Detailně prostudujte a popište problematiku současných možností monitoringu IP sítí pro dohledová centra SOC (Security Operations Centre) využívající IDS / IPS pro distribuční a páteřní spoje. Seznamte se s technologií a zařízeními ENDACE (v současné době převzala firma EMULEX) v laboratořích SIX a popište jejich strukturu. Zabývejte se součástmi EndaceProbe, EndaceVision. Seznamte se s využitím webových služeb, protokolem SOAP (Simple Object Access Protocol) a formátem pro popis rozhraní webové služby WSDL (Web Services Description Language) daného zařízení. V druhé části vypracujte návrh obsáhlejších laboratorních úloh pro detekci provozu, a to včetně teoretického výkladu, přípravy podkladů, a také vzorového řešení. Součástí vybrané laboratorní úlohy uvažujte využití webových služeb pro zařízení ENDACE. Laboratorní úlohy koncipujte i se zapojením technologie CISCO v laboratoři SIX. EndaceProbe uvažujte jako vnořenou sondu. Diskutujte nad vytvořenými laboratorními úlohami a výsledky možností využití webových služeb daného zařízení.

DOPORUČENÁ LITERATURA:

[1] PUŽMANOVÁ, R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007
[2] ENDACE, firemní dokumentace, stránky http://www.utko.feec.vutbr.cz/~skorpil/fpga

Termín zadání:	9.2.2015	***Termín odevzdání:***	26.5.2015

Vedoucí práce: Ing. Václav Oujezský
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Diplomová práce se zaměřuje na monitorování sítí. V teoretické části jsou popsány používané detekční a prevenční systémy, vlastnosti těchto systémů, jejich komponenty i používané detekční techniky. Další část práce se zabývá analyzátorem EndaceProbe, jeho vlastnostmi a analytickou aplikací EndaceVision. Taktéž obsahuje popis webových služeb, popis programovacího jazyka WSDL a protokolu SOAP. Praktická část se věnuje vytvoření tří laboratorních úloh pro detekci provozu a práci se zařízením EndaceProbe. Součástí laboratorních úloh je generátor provozu IXIA a směrovače společnosti Cisco s využitím funkce vzdáleného zrcadlícího portu směrovače. Dále jsou použity webové služby zařízení EndaceProbe, programovací jazyk WSDL a SOAP protokol.

KLÍČOVÁ SLOVA

Endace, EndaceProbe, EndaceVision, IDS, IPS, monitorování sítí, NetBeans, RSPAN, SOAP, webové služby, WSDL, XSD.

ABSTRACT

This diploma thesis is focused on network monitoring. The theoretical part describes using of detection and prevention systems, properties of these systems, their components and detection techniques. Next part of the thesis is focused on EndaceProbe analyzer and analytic application EndaceVision. Also web services, programming language WSDL and protocol SOAP are described. The practical part is focused on creating three laboratory exercises for network monitoring and for using EndaceProbe. Components of the exercises are the traffic generator IXIA and Cisco switches with the application of remote switched port analyzer. There are also used web services EndaceProbe, programming language WSDL and SOAP protocol.

KEYWORDS

Endace, EndaceProbe, EndaceVision, IDS, IPS, network monitoring, NetBeans, RSPAN, SOAP, web services, WSDL, XSD.

GILÍK, A. *Monitorování provozu sítě pomocí dlouhodobě pracujícího analyzátoru.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2015. 98 s. Vedoucí diplomové práce Ing. Václav Oujezský.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma „Monitorování sítě pomocí dlouhodobě pracujícího analyzátoru“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následku porušení ustanovení § 11 a následujících autorského zákona c. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonu (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne 25.5.2015 .....

podpis autora

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Poděkování

Děkuji vedoucímu práce Ing. Václavovi Oujezskému za velmi užitečnou metodickou pomoc, cenné rady při zpracování práce a jeho čas, který mi věnoval při konzultacích.
Dále děkuji svým rodičům za trvalou a bezmeznou podporu po celou dobu mých studií.

V Brně dne 25.5.2015 .....

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Monitorování sítí je velmi důležitou činností k zajištění přehledu o stavu sítě, její funkčnosti a řízení. V pozici síťového administrátora nebo pracovníka dohledového centra je nutné mít přehled o tom, co se děje v dané síti a to z důvodu prevence, detekce a i řešení nastalých neobvyklých situací. Tyto neobvyklé situace nejsou pouze poruchy v sítí, ale taktéž čím dál tím častější útoky. Takovýto přehled je možné získat trvalým monitorováním sítě a tato diplomová práce se zabývá touto velmi důležitou oblastí v síťových technologiích.

První kapitola diplomové práce souhrnně analyzuje způsoby monitorování sítí, používané detekční a prevenční systémy, jejich vlastnosti, komponenty i techniky. Obsahuje popis i moderní techniky monitorování síťových toků a popis nejpoužívanějších zařízení pro detekci a prevenci narušení včetně programových řešení.

Druhá kapitola se zabývá konkrétním zařízením pro monitorování sítí a to síťovým rekordérem a analyzátorem společnosti Endace. Kromě detailního popisu vlastností tohoto analyzátoru a jeho analytické aplikace EndaceVision jsou v této kapitole dále popsány webové služby, programovací jazyk WSDL a protokol SOAP, který je používán pro programovatelnou správu tohoto zařízení.

V praktické části práce jsou vytvořeny tři laboratorní úlohy pro detekci provozu a práci se zařízením EndaceProbe, včetně analytické aplikace EndaceVision. Součástí laboratorních úloh je i využití webových služeb pro zařízení EndaceProbe a také zapojení zařízení Cisco v laboratoři transportních sítí, která je součástí výzkumného centra SIX. Ke každé laboratorní úloze jsou rovněž vytvořeny pokyny pro vyučující.

Na konci diplomové práce jsou přiloženy přílohy doplňující tuto diplomovou práci, jako jsou nastavení aplikací použitých při laboratorní úloze a výstupy jednotlivých laboratorních úloh.

1 MONITOROVÁNÍ SÍTÍ

Monitorování sítí je rozsáhlá činnost v oblasti síťových technologií. Existuje více důvodů proč monitorovat sítě. Mezi stále aktuálnější důvody patří bezpečnost sítě, ochrana dat a uživatelů. Dalším podstatným důvodem je kontrola nad funkčností používaných technologií, nalézání technických nedostatků a získávání podkladů pro vylepšování sítí, jak změnou konfigurací, tak změnou použitých technologií. Taktéž může být potřeba monitorovat a zaznamenávat dané komunikace mezi sítovými uzly nebo uživateli, pro případné dohledávání bezpečnostních narušení.

Je používáno velké množství technik pro monitorování sítí a v této kapitole jsou některé z nich popsány, vzhledem k jejich použití pro systémy typu IDS/IPS (Intrussion Detection System / Intrusion Prevention System). Jelikož vzniklý útok je potřeba zpozorovat co nejdříve, abychom mu dokázali zabránit nebo omezit jeho rizika, jako je například ztráta důležitých dat nebo omezení důležitých služeb, je vhodné používat moderní systémy pro detekci průniků. Přesné informace o aktuálním stavu sítě nám dokáží poskytnou technologie založené na monitorování síťových toků. Pro informace o stavu síťových prvků se již od roku 1990 používá protokol SNMP (Simple Network Management Protocol), který je v první kapitole taktéž dále popsán.

1.1 Detekční a prevenční systémy

V následujících podkapitolách je popsáno, co jsou to detekční a prevenční systémy, jaké mají klíčové vlastnosti, typické komponenty a jaké detekční techniky používají, včetně jejich popisu.

1.1.1 IDS

Systém detekce narušení IDS je automatizovaný proces sledování událostí, probíhajících v počítači nebo v sítí. Provádí jejich analýzu pro nalezení příznaků mimořádných událostí narušení bezpečnosti, jako je například napadení viry, útoky hackerů, neoprávněných osob nebo užití sítě pro neoprávněné účely. [1]

1.1.2 IPS

Systém prevence narušení IPS je systém se stejnými schopnosti jako IDS, avšak má funkce, které se dokážou pokusit zastavit detekované mimořádné události, například změnou konfigurací sítě či ukončením síťového připojení. [1]

1.1.3 IDS/IPS

Jedná se o systémy, které kombinují funkce detekce narušení s funkcemi pro zastavení narušení. Jelikož systémy IDS a IPS nabízí mnoho stejných možností a administrátoři mohou obvykle zakázat funkce prevence v systémech IPS, tak aby fungovaly pouze detekčně, tedy jako systémy IDS, lze tyto systému označovat jedinou zkratkou - IDPS (Intrusion Detection and Prevention Systems). V textu této práce budu používat složené označení IDS/IPS. [1]

1.1.4 NGIPS

Systém IPS nové generace (Next-Generation Intrusion Prevention System) je označení, které používají někteří výrobci (například Cisco a HP) pro své nejmodernější IDS/IPS systémy. Z dokumentu společnosti HP [24] obsahující analýzu NGIPS systémů, provedenou společností Gartner [32] je patrné, že se z velké části jedná o marketingové označení a systémy NGIPS využívají principálně stejné mechanismy a techniky jako jiné moderní IDS/IPS systémy. Jedná se o vývoj a zdokonalování IPS systémů pro blokování široké škály útoků, ale s velmi nízkými počty falešných poplachů.

Za nejvýznamnější vylepšení jsou považována zdokonalená jádra IPS systémů s větším povědomím o obsahu a souvislostech síťového provozu a s vylepšenými detekcemi anomálií a analýzou protokolů. [24]

1.1.5 Klíčové vlastnosti IDS/IPS technologií

Existuje mnoho typů IDS/IPS technologií, které jsou odlišné především dle událostí, které dokáží rozeznat a metodami používanými pro identifikování incidentu. Klíčovými vlastnosti těchto technologií jsou:

- **Záznam informací týkajících se pozorovaných informací:** Informace jsou ukládány lokálně, nebo mohou být odeslány do centralizovaného serveru.
- **Upozornění daného administrátora na zpozorovanou událost:** Různými metodami, například e-mailem, varováním v IDS/IPS uživatelském rozhraní, pomocí SNMP, systémovými zprávami či voláním definovaných skriptů nebo programů.
- **Vytváření reportů:** které shrnují sledované události, nebo poskytují podrobnosti o jednotlivých provedených akcích. [1]

Techniky používané u systému IPS, lze rozdělit do následujících skupin:

- **Zastavení útoku samostatně**:
    - ukončením síťového připojení nebo relace uživatele, která je použita pro útok,
    - zablokování přístupu k cíli z podezřelého účtu uživatele, IP adresy nebo dle jiného jeho identifikátoru,

        - zablokováním veškerého přístupu k cíli útoku.
    - **Změnění bezpečnostního prostředí**:
        - změna konfigurace dalších bezpečnostních kontrol,
        - přenastavení sítových zařízení (bezpečnostních bran, směrovačů, přepínačů).
    - **Změnění obsahu útoku:**
        - některé IPS technologie dokáží vyjmout nebo vyměnit nebezpečné části útoku, tak aby byly neškodné. Například odstranit nebezpečnou přílohu z e-mailu, nebo i změnit záhlaví paketů. [1]

1.1.6 Typické komponenty

- **Senzor nebo agent** – monitorují a analyzují aktivitu. Základní prvek IDS/IPS systémů.
- **Řídící server** – centralizované zařízení, které přijímá data ze senzorů nebo agentů. Dále tyto data zpracovává a vyhodnocuje.
- **Databázový server** – slouží jako úložiště události, které jsou ukládány sensory, agenty nebo řídícím serverem.
- **Konzole** – programové rozhraní pro administraci celého systému. [1]

1.1.7 Detekční techniky

IDS/IPS technologie používají různé techniky pro detekci incidentů a tyto technologie často kombinují pro poskytnutí přesné a více obsáhlé detekce. Hlavní z těchto technik jsou níže popsány.

Detekce signatur

Jedná se o proces porovnávání signatur – vzorů chování, oproti jiným vzorům, typickými pro narušení bezpečnosti. Jednoduchým příkladem takovéhoto typického narušení může být příchozí e-mail s předmětem fotografie „freepics“ a s přílohou „freepics.exe“. [1]

Detekce založena na porovnání signatur je velmi účinná pro detekci známých hrozeb, ale velmi málo účinná pro detekci dosud neznámých hrozeb. Jedná se o nejjednodušší detekční metodu, jelikož pouze porovnává aktuální aktivitu, jako je průchozí paket nebo informace v záznamu chování zařízení se seznamem známých hrozeb. Různé systémy IDS nabízejí různé sady vzorů chování. [1]

Jelikož se jedná o detekci porovnávající známé hrozby, účinnost této detekce je velice závislá na aktuálnosti vzorů hrozeb, které musí výrobci IDS systémů aktualizovat.

Pro detekci signatur jsou důležité následující parametry a vlastnosti:

- IP adresy,
- čísla portů,
- neobvyklá fragmentace paketů,
- zvláštní kombinace TCP (Transmission Control Protocol) příznaků,
- neobvyklé ICMP (Internet Control Message Protocol) zprávy. [10]

Detekce anomálií

Jedná se o proces porovnávání definic, která aktivita je považována za normální oproti aktivitě pozorované s významnými odchylkami. IDS/IPS systémy používající detekci anomálií obsahují profily, které reprezentují normální chování prostředí – uživatelů, počítačů či aplikací. Tyto profily jsou vytvořeny monitorováním typické aktivity v průběhu času. Jako příklad lze například uvést situaci kdy linka připojená k internetu je běžně v průběhu pracovních hodin používaná na 13%, avšak náhle je používána mnohem více. IDS/IPS systém rozezná statistickými metodami danou anomálii a upozorní na ni správce, případně podnikne další nastavené kroky. Profily pro detekci anomálií mohou být vytvořeny dle mnoha typů chování uživatelů, nebo systému, jako je například i počet odeslaných e-mailů uživatelem, počet neúspěšných pokusů přihlášení nebo vyžívání procesoru.

Hlavní výhodou metod založených na detekcí anomálií je, že mohou být velmi účinné při odhalování doposud neznámých hrozeb.

Počáteční profil pro detekci anomálií je vytvářen specifickou dobu, zvanou učící perioda, která je dlouhá obvykle dny, případně týdny. Po této době záleží, zda systém používá pouze statické profily nebo dynamické. Statický profil není již nadále měněn, což může být považováno za nedostatek, jelikož v průběhu času se dané prostředí mění, počítačová síť se rozšiřuje, přibývají noví uživatelé apod. Dynamicky měněný profil se dokáže těmto změnám přizpůsobovat, avšak přináší bezpečností riziko, že nedokáže rozeznat útok, který je prováděn pozvolna, pomalu se zvyšující aktivitou a změny jím způsobné zanáší do profilu normální aktivity.

Mezi další negativum detekcí anomálií, mohou být vzniky falešných poplachů, například při činnosti údržby, aktualizací, zálohování, kdy se systémové prostředky využívají nad obvyklé hranice. [1]

Stavová analýza protokolů

Jedná se o proces porovnávání předdefinovaných profilů síťových protokolů vytvořených z obecně uznávaných definicí síťových protokolů s probíhajícími aktivitami protokolů a dle nalezených rozdílů rozpoznání hrozeb. Stavová analýza protokolů pro předdefinované profily používá modely protokolů, které jsou obvykle založeny na

standardech protokolů od dodavatelů programů a normalizačních orgánů (např. IETF - Internet Engineering Task Force, RFC - Request for Comments) typicky s úvahou možných odchylek. Nevýhodou je zde, že některé normy nejsou zcela kompletní, výrobci programů dané normy přesně nedodržují nebo u proprietárních protokolů kompletní informace pro vytváření modelů zcela chybí. V případě, že je daný protokol aktualizován, musí být aktualizován i jeho profil pro analýzu.

Touto analýzou lze identifikovat neočekávané sekvence příkazů, jako například zasílání stejného příkazu opakovaně nebo zaslání příkazů, bez předchozího příkazu, na který je závislý.

Hlavní nevýhodou stavových metod analýzy protokolů je jejich velká náročnost na systémové zdroje, z důvodu složitosti analýzy a sledování stavů pro mnoho souběžných relací. Nevýhodou je taktéž případ, kdy nelze analyticky detekovat útoky, které neporušují obecné uznávané definice síťových protokolů. [1]

1.2 Techniky monitoringu IP sítí

V následujících podkapitolách je zpracována problematika současných možností monitoringu IP sítí pro dohledová centra SOC (Security Operations Centre) využívající IDS/IPS pro distribuční a páteřní spoje.

1.2.1 Monitorování síťových toků

Technologie monitorování síťových toků je v posledních letech stále nutnější monitorovací metoda. Je založena na sběru a zpracování informací o síťových tocích v reálném čase, které jsou získávány z aktivních síťových prvků, specializovaných HW sond, nebo sond vytvořených z počítače s nainstalovaným specifickým softwarem. Nejrozšířenějším protokolem pro operace se síťovými toky je protokol NetFlow, vyvíjený společností Cisco. Mezi další používané protokoly patří IPFIX (Internet *Protocol* Flow Information Export), sFlow, J-Flow.

Síťový tok je definován pomocí sedmi unikátních údajů, kterými jsou:

- zdrojová IP adresa,
- cílová IP adresa,
- zdrojový port,
- cílový port,
- typ protokolu,
- TOS (Type of Service) / DSCP bajt (Differentiated Services Code Point),
- označení rozhraní (Interface Index value). [5]

Při záznamu síťových toků se ukládají výše uvedené identifikátory do souvislosti daných toků. Každý tok je jednostranný, obousměrná komunikace je tedy popsána alespoň dvěma toky. Tok vzniká zachycením paketu, který nebyl součástí jiného toku. Další pakety jsou řazeny k příslušným tokům. Zdroje záznamů toků ukládají probíhající toky do své paměti a po ukončení toku odesílají na kolektory pro další zpracování. Pro označení daného toku za ukončený se používá aktivní a pasivní časový limit. Aktivní časový limit se počítá od přijetí prvního paketu nového toku, pasivní časový limit se počítá od přijetí posledního paketu.

Neukládají se obsahy paketů, ale pouze informace o nich. Nelze tedy rozpoznat, která konkrétní uživatelská data byla předmětem komunikace, což zachovává soukromí uživatelů.

Příklady zdrojů záznamů na bázi IP toků:

- směrovače (např. Cisco, Juniper, HP),
- specializované sondy (např. FlowMon),
- programová řešení (např. tcpflow, nfdump tools, NfSen, nTop, nProbe, fProbe).

Zdroje záznamů se liší dle jejich výkonu, pořizovací ceny a možnosti umístění. Pro bezpečností aplikace může ztráta jediného paketu zanést nežádoucí nepřesnost. Proto bývá vyžadováno bezeztrátové vzorkování, což v případě vysokorychlostních sítí (10 Gb/s a více) přináší potřebu použití specializované hardwarové sondy. [2, 3, 4]

Sběr toku dat pomocí směrovačů

Řešení sběru toků dat ze směrovačů, jsou přidané funkce, k některým druhům směrovačů. Nevýhodou jsou zvýšené nároky na výkon směrovače, který je zaměřen primárně na směrování. Pro ušetření výkonu se zde často zavádí vzorkování při sběrů toků, díky čemuž vzniká nežádoucí nepřesnost. Další nevýhodou použití směrovače pro sběr toků je jeho typicky fixní umístění v sítí a možnost být cílem případného útoku. [3]

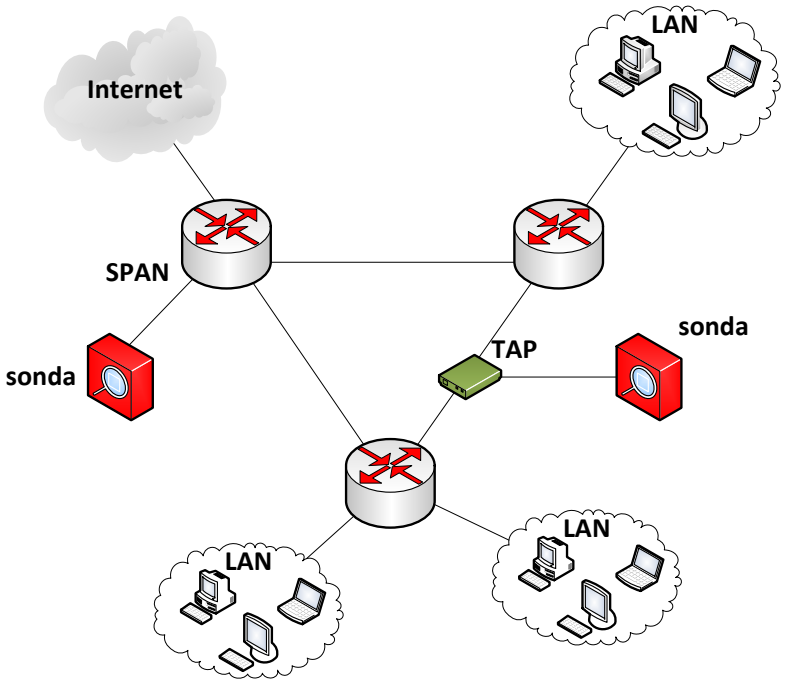
Sběr toku dat pomocí programového řešení

Programová řešení jsou založeny na běžných počítačích a síťových kartách. Mají limitovaný výkon a mohou mít problémy se stabilitou. Výhodou je existence velkého množství programů zdarma, s otevřeným kódem. [3]

Sběr toku dat pomocí specializovaných sond

Specializované sondy jsou hardwarová řešení, pro použití i v dnešních nejvýkonnějších sítích pro monitorování síťových toků. Takovýchto sond může v síti existovat více a informace o tocích odesílají na kolektory, řídící servery, kde se dále zpracovávají. Sondy

můžeme umístit do libovolného bodu v síti. Typicky na vstupní a výstupní body sítě, případně kritická místa či linky s největším přenosem dat. Připojení do linky se provádí pomocí zrcadlícího portu směrovače nebo přepínače (SPAN port), nebo přímým vložením do linky pomocí rozbočovače TAP (Test Access Point). Oba dva způsoby jsou znázorněny na obr. 1.1. [3]



Obr. 1.1: Ukázka zapojení sond pro sběr toků dat

1.2.2 Protokol SNMP

SNMP je asynchronní protokol aplikační vrstvy pro výměnu řídících informací mezi síťovými zařízeními. Díky své jednoduchosti a funkčnosti je nejpoužívanějším protokolem pro management sítí. Je transakčně orientovaný, založený na transakcích typu dotaz/odpověď mezi síťovým manažerem a agentem v síti. Zařízení s SNMP agentem není závislé pouze na jednom serveru, SNMP manažeru, ale může reagovat na žádosti několik na sobě nezávislých serverů. Pro výměnu zpráv se využívá komunikace založena na nespojově orientovaném protokolu UDP.

SNMP manažer – program pracující v dohledové stanici, který shromažďuje, třídí a vyhodnocuje informace o síťových prvcích. Slouží taktéž ke vzdálené konfiguraci testovacích procedur na daných síťových zařízeních.

SNMP agent – programový, případně i hardwarový modul implementovaný jako nadstandartní část daného sítového prvku. Sbírá informace o činnosti daného zařízení a na žádost či vznik nestandartní události odesílá stavové informace.

SNMP Existuje ve třech verzích, první verze SNMPv1 byla normována roku 1990 (RFC 1157). Druhá verze SNMPv2 vznikala v letech 1991 – 1993, avšak nebyla nikdy plně normována. Nejnovější verze SNMPv3 byla normována roku 2002, doplňuje protokol novým formátem zpráv, bezpečnostním mechanismem zpráv a řízením přístupu k síťovým zařízením. Bezpečnostní mechanismus je zaměřen především na ochranu zpráv SNMP při cestě sítí a ověřením zdroje zpráv SNMP.

Parametry na SNMP agentu jsou uloženy v databázi objektů MIB (Management Information Base). Každý objekt je zde definován pomocí identifikátoru. Struktura databáze je stromová hierarchická.

Přehled SNMPv3 příkazů:

- **get-request** – žádost přečtení hodnoty proměnné, identifikované číselným identifikátorem,
- **get-next-request** – žádost o postupné čtení všechny proměnných, bez znalosti jejich přesných identifikátorů, pomoci procházení struktury MIB,
- **get-response** – zpráva nesoucí výsledek výše uvedených operací,
- **set-request** – zapsání hodnoty proměnné objektu MIB,
- **trap** – jediný typ příkazu vysílaný SNMP manažerovi bez předchozího vyžádání. Jedná se o upozornění na nějakou událost, například poruchu. [6, 7]

Existuje velké množství síťových manažerů pro SNMP protokol. Mezi oblíbený patří například program SNMPc nebo komplexní systém Nagios, který je v této práci níže popsán.

1.3 Zařízení používaná pro detekci a prevenci narušení

V následující kapitole jsou popsána některá zařízení, která se prakticky používají pro detekci a prevenci narušení. Výběr vychází z analýzy trhu, provedeného společností Gartner a navíc obsahuje jedno zařízení české společnosti INVEA-TECH. [27]

1.3.1 FlowMon

Je portfolio výrobku společnosti INVEA-TECH, která je českým výrobcem řešení pro monitorování a bezpečnost počítačových sítí se specializací na IP flow monitoring (NetFlow/IPFIX), behaviorální analýzu sítě, hardwarově akcelerované aplikace (FPGA) a řešení pro ochranu proti kybernetickým útokům a kybernetické kriminalitě.

Do FlowMon produktů patří výkonné autonomní sondy pro generování síťových toků i na linkách s propustností až 100 Gb/s. Jedná se o zařízení o velikosti jedné nebo dvou jednotek rozvaděče s různými počty a typy monitorovacích portů.

Standardní modely (viz obr. 1.2) jsou kompaktní zařízení o velikosti jedné jednotky rozvaděče s 1 – 6 monitorovacími porty pro 10/100/1000 Mb/s Ethernet nebo až s 4 monitorovacími rozhraními pro desetigigabitový Ethernet. V nabídce se nachází i model s 40 Gb/s Ethernet i 100 Gb/s Ethernet portem. Většina modelů FlowMon sond obsahuje již integrovaný kolektor pro zobrazení a analýzu dat s vestavěnou kolektorovou aplikaci FlowMon Monitorovací Centrum, která umožňuje uložení a analýzu statistik vytvořených danou sondou.

Obr. 1.2: Standardní model FlowMon sondy [22]

V případě používání více FlowMon sond v síti, nebo potřeby většího prostoru pro uchovávání NetFlow statistik, je vhodné v síti použít FlowMon kolektory, ke sběru NetFlow statistik z více FlowMon sond a k jejich dlouhodobému uchovávání. [22]

1.3.2 Cisco

Společnost Cisco vyrábí velkou škálu zařízení zaměřených i na bezpečnost sítí. Tyto produkty jsou součástí architektury, kterou tato společnost označuje Cisco SecureX.

IPS senzory jsou zařízení Cisco IPS Sensor řady 4000, kdy nejvýkonnější model Cisco IPS 4520-XL Sensor má udávanou průměrnou propustnost 10 Gb/s a maximální udávanou propustnost 20 Gb/s. Jedná se o nejdůležitější komponentu Cisco SecureX architektury.

Dále společnost Cisco vyrábí produkty Cisco FirePOWER viz obr. 1.3, aktuálně nejnovější řady 8000, které označuje jako systémy IPS nové generace (NGIPS). Nejvýkonnější model Cisco FirePOWER 8390 má udávanou propustnost pro analýzu IPS až 60 Gb/s.

Systémy IPS jsou taktéž implementovány do Cisco ASA firewallů a dále do některých směrovačů, v závislosti na modelu a na verzi operačního systému IOS (Internetwork Operating Systém). [23]

Obr. 1.3: Cisco FirePOWER řady 8 000 [23]

1.3.3 HP

Společnost HP svou platformu pro IPS systémy tzv. nové generace označuje jménem HP TippingPoint NX viz obr. 1.4. Nejvýkonnější model S7500NX má udávanou propustnost pro analýzu až 20 Gb/s a jeho zajímavostí je jeho velikost pouze 2 jednotky rozvaděče. Každá šasi modelů NX podporuje až 4 zásuvné vstupní/výstupní moduly s různými porty, včetně modulu s přijímačem 40 Gb/s Ethernet QSFP+. NX platforma může celkem podporovat až 24 segmentů 1 Gb/s Ethernet, 16 segmentů 10 Gb/s Ethernet nebo 4 segmenty 40 Gb/s Ethernet. [25]

Obr. 1.4: HP TippingPoint NX [25]

1.3.4 McAffee

Společnost McAffee, která je nyní součásti Intel Security má velké portfolio produktů napříč síťovou a desktopovou bezpečností. IPS systémy této společnosti jsou označovaný jako Network Security Platform. Jejich nejvýkonnější model NS9300 (viz obr. 1.5) dokáže pracovat s reálnou propustností dat 40 Gb/s a maximální až 70 Gb/s. Umožňuje variabilní kombinaci vstupně/výstupních modulů, včetně až šestnácti 40 Gb/s Ethernet QSFP+ modulů. [26]

Obr. 1.5: McAfee NS9300 [26]

1.3.5 IBM

Produkty společnosti IBM zaměřené na detekci a prevenci průniků jsou označovány jako IBM Security Network Protection. Nejvýkonnější model XGS 7100 má udávanou propustnost pro analýzu dat až 20 Gb/s a jeho velikost jsou dvě jednotky rozvaděče. Je ho možné osadit až čtyřmi moduly s rozhraními, nejrychlejší možná rozhraní jsou 10Gb/s Ethernet. Na internetových stránkách IBM je oproti ostatním výrobcům, velmi málo informací o těchto produktech. Na obr. 1.6 je pro představu zobrazen nižší model. [29]

Obr. 1.6: IBM Security Network Protection XGS 5100 [29]

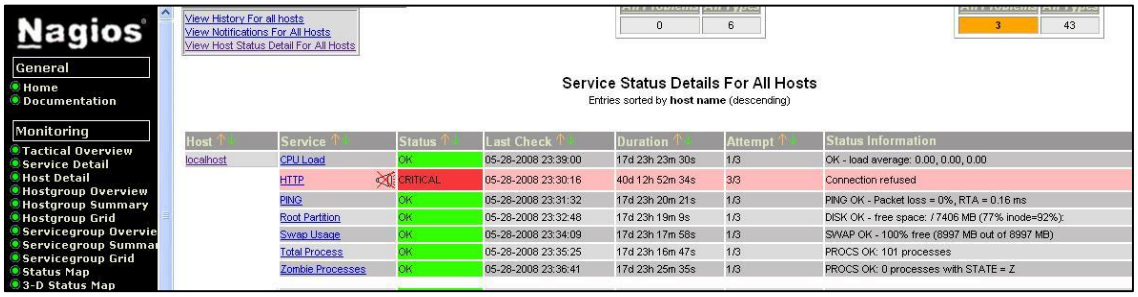
1.4 Programy používané pro detekci a prevenci narušení

Následující kapitola popisuje dva známé a oblíbené programové systémy, používané pro monitoring sítí a detekci narušení sítě a to systém Nagios a program Snort.

1.4.1 Nagios

Nagios je robustní monitorovací systém, rozšířitelný pomocí velkého množství zásuvných modulů, díky kterým lze monitorovat velké množství služeb, aplikací, či zařízení. Existuje pro operační systémy Linux a obsahuje grafické webové rozhraní, které je znázorněno na obr. 1.7. Systém je vyvíjen od roku 1999 a nyní existuje jeho čtvrtá

verze. I když se jedná o linuxový systém, dokáže i monitorovat systémy a aplikace založené na operačních systémech Windows.



Obr. 1.7: Ukázka prostředí systému Nagios [14]

Mezi vybrané schopnosti systému Nagios patří:

- **Komplexní monitorování:**
  - Možnosti sledování aplikací, služeb, operačních systémů, protokolů a dalších prvků infrastruktury.
  - Výkonné rozhraní pro používání vlastních skriptů pro monitorování uživatelských aplikací, služeb a systémů.
- **Přehlednost:**
  - Centralizovaný pohled na celou sledovanou infrastrukturu.
  - Detailní informace dostupné přes webové rozhraní.
- **Informovanost:**
  - Rychlá detekce výpadků infrastruktury.
  - Upozornění mohou být odesílána například pomoc e-mailu nebo SMS.
  - Stupňování upozornění pro informování zodpovědných osob.
- **Náprava problémů:**
  - Náprava známých problémů, například restartováním aplikací a služeb.
- **Reportování:**
  - Dostupné reporty pro zajištění SLA (Service Level Agreement).
  - Historické reporty obsahující záznamy upozornění.
  - Další přídavné doplňky pro rozšíření reportování.
- **Více uživatelské schopnosti:**
  - Přístup více uživatelů k webovému rozhraní, specifická zobrazení pro klienty infrastruktury.
- **Rozšířitelná architektura:**
  - Snadná integrace s aplikacemi třetích stran.
- **Přizpůsobitelný kód:**
  - Systém je s otevřeným zdrojovým kódem, s plným přístupem k němu.
  - Uvolněno pod licencí GPL (General Public License).

Techniky prováděných testů a monitorování jsou závislé na daných zásuvných modulech. Díky velkému množství těchto zásuvných modelů je možné se systémem Nagios monitorovat takřka vše od protokolu SNMP až po testování specifických aplikací. Lze jej použít i jako systém detekce narušení, například díky zásuvným modulům Tripwire a chkrootkit.

Nagios je dostupný jak ve verzi zdarma, která obsahuje základ/jádro systému, zvaná Nagios Core, tak v placené verzi Nagios XI, která již integruje veškeré jeho schopnosti, do komplexního předpřipraveného systému. [8, 9]

1.4.2 SNORT

Snort je zde uveden jako zástupce programového řešení systému IDS. Jedná se o volně šiřitelný a nejpoužívanější programový systém pro detekci narušení. Fyzické IDS/IPS systémy mohou mít program Snort integrován, příkladem jsou zařízení firmy SOURCEfire, kterou založil autor systému Snort. Tato společnost byla v roce 2013 zakoupena společností CISCO, která je nyní i vlastníkem systému Snort. Tento systém je primárně vyvíjen pro operační systémy GNU/Linux, existuje ale taktéž verze pro operační systémy Windows. Systém se ovládá a instaluje pomocí příkazového řádku.

Systém SNORT může být konfigurován do tří módů:

- **Mód odposlouchání (Sniffer mode):** dokáže zachytávat pakety a zobrazovat je průběžně v konzoli.
- **Mód záznamu paketů (Packet Logger mode):** mód sloužící k odposlouchávání paketů a k jejich ukládání na disk.
- **Mód detekce narušení sítě (NIDS - Network Intrusion Detection System mode**): nejdůležitější mód, sloužící k detekci a analýze síťového provozu.

V módu IDS aplikace Snort analyzuje pakety v síti dle vestavěných pravidel, které se aktualizují v závislosti, zda uživatel používá bezplatnou registraci nebo placenou registraci. Dále může uživatel vytvářet své vlastní pravidla a doprogramovat je. Díky existenci výstupních modulů, lze upozornění na nastalé situace prezentovat více způsoby, například výpisem na obrazovku, ukládáním do logovacích či jiných souborů. [30, 31]

2 ANALYZÁTOR ENDACE

Tato kapitola se zabývá popisem zařízení EndaceProbe a analytické aplikace EndaceVision. Taktéž jsou v posledních podkapitolách popsány webové služby, protokol SOAP (Simple Object Access Protocol), programovací jazyk WSDL (Web Services Description Language) a soubor XSD (XML Schema Definition).

2.1 Společnost Endace

Firma Endace vnikla v roce 2001 z výzkumného projektu na univerzitě ve Waikato na Novém Zélandu a to začátkem výroby jejich první komerční vysokorychlostní karty, schopné zachytávat 100% síťového provozu z celé řady síťových rozhraní. Díky úzké spolupráci s jejich zákazníky, identifikovali tržní příležitost a vytvořili první zachytávající serverovou platformu, která byla schopna pracovat v prostředí 10 Gb/s sítí zvanou NinjaBoxes. Vývojem jejich technologií vznikl analyzátor EndaceProbe a jeho programové analytické prostředí EndaceVison, o kterém pojednává následující kapitola.

V roce 2013 firmu Endace zakoupila korporace Emulex z Kalifornie, vyrábějící profesionální technologie pro síťová připojení. [11]

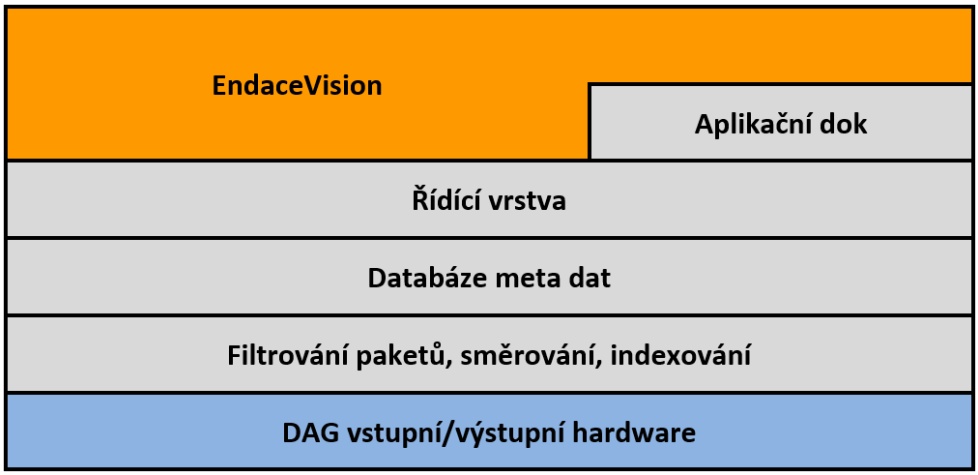
2.2 EndaceProbe 7000

Je velmi výkonný síťový rekordér vytvořen od základů pro zachycení, označení a uložení síťového provozu s udávanou 100% přesností, bez ohledu na rychlost sítě, nebo typ síťového provozu. Jeho vzhled je zobrazen níže na obr. 2.1.

Obr. 2.1: Síťový analyzátor EndaceProbe 7000 v laboratoři SIX

Systém analyzátoru Endace je založen na tradičním vrstvovém modelu (viz obr. 2.2) zahrnujícím komerční serverový hardware úzce integrovaný s proprietární technologií DAG (Data Acquisition Generation), proprietárním operačním systémem OSm (založeném na linuxové distribuci CentOS) a aplikační vrstvou zahrnující EndaceVison.

Systém analyzátoru Endace dále může obsahovat vlastní aplikace, nebo aplikace třetích stran běžící v aplikačním doku.



Obr. 2.2: Model architektury EndaceProbe [11]

Nejnižší vrstvou modelu architektury zařízení EndaceProbe jsou vstupně/výstupní DAG karty. Další vrstva slouží k filtrování dat dle vytvořených filtrů, následně ke směrování dat nakonfigurovanou datovou rourou do žádaného výstupu, například do tzv. rotačního souboru a k indexování paketů například časovou značkou. Vyšší vrstvou je databáze meta dat, do které se ukládají data potřebná pro generování vizualizací v aplikaci EndaceVision. Další vrstvou je vrstva řídící, sloužící pro konfigurování zařízení. Nejvyšší vrstva EndaceVision je analytická aplikace, která využívá záznamů z databáze metadat, pro vytváření vizualizací a analýzy zachyceného provozu. V modelu je zobrazen i aplikační dok, pro vlastní aplikace, nebo aplikace třetích stran. [33]

EndaceDAG technologie

Jedná se o monitorovací PCI karty určené pro zachytávání paketů. Jsou založeny na technologií FPGA a DMA (Direct Memory Access) tak aby zajistily, že 100% síťového provozu je zachyceno, označkováno a přeneseno beze ztráty do paměti hostitele. [11]

2.2.1 Vlastnosti systému Endace

- **100% přesné zachytávání paketů**: bez ohledu na jejich velikost nebo rychlosti linky při rychlostech až do 10 Gb/s.
- **Vysoce přesné časové značkování na rozhraní**: Časová razítka mají rozlišitelnost +/- 7,5 ns a přesnost značkování je +/- 50 ns.
- **Záznam na disk:** EndaceProbe umožnuje sledované pakety ukládat na lokální disk pro zpětnou analýzu řadou různých nástrojů. Podporuje až 64 TB lokální diskové úložiště a rychlost zápisu na disk až 12 Gb/s.

- **Zrychlené stahování:** Využívá technologii pěti násobného popisu ukládaného síťového provozu, čímž zajišťuje rychlé vyhledávání toků.
- **Identifikace protokolů v reálném čase:** Každému zachycenému toku je přiřazena identifikace aplikace.
- **Filtrace paketů, jejich více násobná duplikace:** Schopnost filtrovat pakety dle širokého spektra paketů. Taktéž je kopírovat, nebo násobit pro použití stejného paketu na různých místech v systému.
- **Indexování provozu:** Monitorované pakety jsou indexovány v reálném čase. Dané indexy jsou uloženy lokálně a obsahují širokou řadu informací včetně typu aplikace, IP adres, MAC adres, časových značek a jiných.
- **Centrální správa a zabezpečení přístupu:** Všechny části Endace systému obsahují jednotná rozhraní pro řízení a monitorování a dají se monitorovat a řídit z jednoho centrálního bodu.
- **Přeposílání paketů:** Pakety lze z Endace systému odesílat mimo systém Endace a to buď pomocí programovatelného XML (Extensible Markup Language) rozhraní nebo pomocí PCAP (Packet Capture) formátu.
- **Podpora vlastních aplikací a aplikací třetích stran:** Umožnuje instalaci aplikací třetích stran do EndaceProbe pomocí aplikačních doků. [11]

2.2.2 Technické parametry

V následující tabulce tab. 2.1 jsou vypsány důležité parametry EndaceProbe instalovaného v laboratoři transportních sítí, která je součástí výzkumného centra SIX.

Tab. 2.1: Parametry EndaceProbe EP7010-PS-FC [12]

Parametr	Hodnota
Operační paměť	48 GB DDR3
Systémový pevný disk	160 GB SSD
Úložné pevné disky	9,6 TB (16x 600 GB, RAID 50)
Řídící rozhraní	2x 10/100/1 GbE and 1x IPMI
Velikost	3 U – 3 jednotky v rozvaděči
Monitorovací porty	2 x SFP+ (Small Form-factor Pluggable)

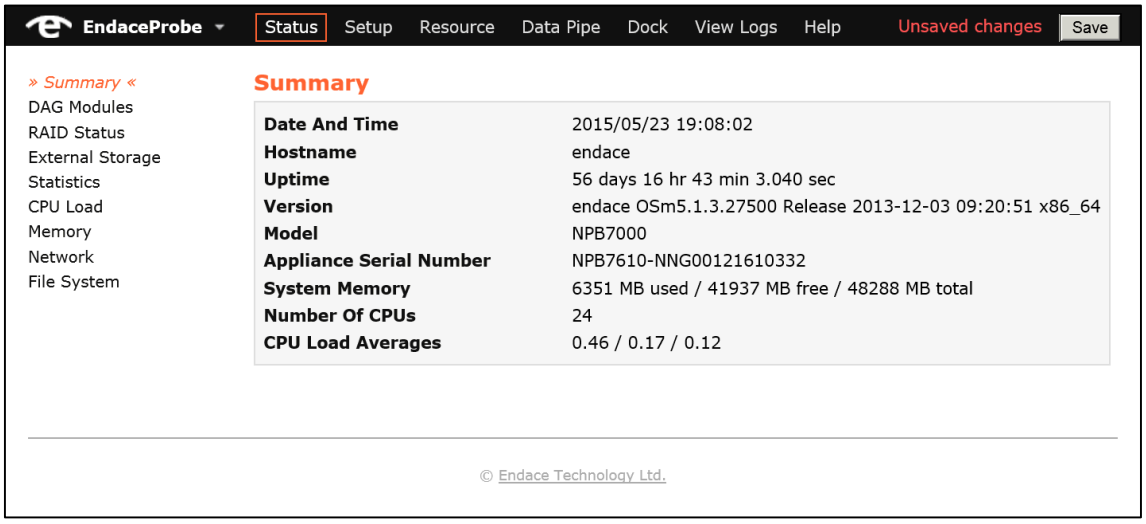
2.2.3 Monitorovací DAG karta

V zařízení EndaceProbe je nainstalovaná monitorovací karta DAG 9.2X2. Jedná se o kartu se dvěma optickými 10 Gb/s SFP+ rozhraními. Obě rozhraní je možné používat nezávisle

na sobě. Sběrnice, kterou je monitorovací karta připojena, umožňuje propustnost dat až do rychlosti 20 Gb/s. [33]

2.2.4 Konfigurace EndaceProbe

Konfigurace se primárně provádí skrze přehledné grafické webové rozhraní, na které se uživatel dostane přes webový prohlížeč po zadání IP adresy zařízení. Toto grafické rozhraní je zobrazeno na obr. 2.3. Zařízení lze taktéž ovládat příkazovým řádkem z terminálu přes zabezpečené SSH spojení. Další možností je ovládání pomocí SOAP rozhraní, které umožňuje programovatelnou správu EndaceProbe, směrování živého nebo uloženého síťového provozu na vzdálená zařízení pro analýzu a získávání dat a jejich extrakci dle zájmů do jiného lokálního zařízení.



Obr. 2.3: Grafické prostředí pro konfiguraci EndaceProbe

2.3 EndaceVision

Jedná se o plně integrovanou analytickou aplikaci předinstalovanou v EndaceProbe, poskytující organizaci síťového provozu a bezpečnostní analýzu. Grafické rozhraní je kompatibilní se všemi hlavními prohlížeči (Firefox, Internet Explorer, Chrome, Safari) a operačními systémy. Není potřeba instalovat žádné aplikace na uživatelský počítač. EndaceVision umožnuje přístup více uživatelů ve stejný čas, kdy každý uživatel má vlastní upravitelné pracovní prostředí. [13]

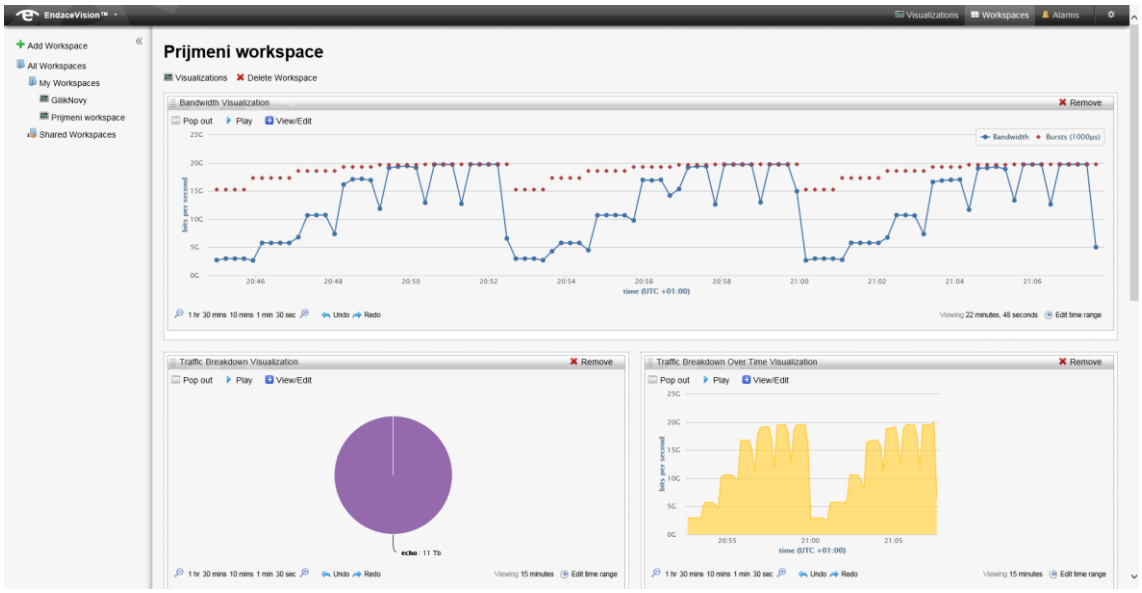
EndaceVision obsahuje:

- EndaceVision Dashboard - uživatelské webové rozhaní.
- Vizuálně přehledné grafické znázornění síťového provozu.
- Analýzu síťového provozu z jedné sondy, nebo seskupené z více sond.

- Analýzu v reálném čase a zpětnou analýzu integrovanou do jediného uživatelského rozhraní.
- Integrace a zobrazování událostí z jiných aplikaci jako je Endace Security Manager a Endace Latency Monitoring.

Pro vytváření vizualizací používá EndaceVision informace o paketech tzv. metadata generovaná v EndaceProbe při jejich záznamu. Toto vytváření metadat je nutné v EndaceProbe aktivovat, při vytváření rotačního souboru (což je soubor do kterého se ukládají zachycená data). Vytvořené vizualizace lze seskupovat v tzv. pracovních plochách. Ukázka prostředí a pracovní plochy je vyobrazena na obr. 2.4.

Z EndaceVision lze vytvářet přehledné reporty ve formátu PDF, vhodné i pro začínající uživatele.



Obr. 2.4: Pracovní plocha v EndaceVision

2.3.1 Typy vizualizací v EndaceVision

V aplikaci EndaceVision lze prohlížet provoz v několika typech grafických vizualizací. Ve vizualizacích lze aplikovat filtry, pro omezení zobrazených dat. Níže je uveden popis možných vizualizací.

Šířka pásma v průběhu času a analýza shluků bitů (burst)

Základní analýza, která zobrazuje využití šířky pásma v časové ose s nastavitelným rozlišením. Přehledem využití šířky pásma mohou být objeveny neobvyklé špičky v síťovém provozu.

Přehled síťového provozu v kruhovém grafu

Umožňuje uživateli přehled síťového provozu dle specifikovaného kritéria. Tyto kritéria jsou: typ aplikace, typ transportního protokolu, verze IP protokolu, VLAN (Virtual Local Area Network), MPLS (Multiprotocol Label Switching), zdrojový a cílový port, zdrojová a cílová IP adresa, zdrojová a cílová MAC (Media Access Control) adresa. Přehled je zpracován do kruhového grafu.

Přehled síťového provozu v závislosti na čase

Zobrazuje síťový provoz dle specifikovaného kritéria v nastavené časové ose. Kritéria pro analýzu jsou stejná, jako ve výše uvedeném přehledu.

Nejvíce komunikující uzly

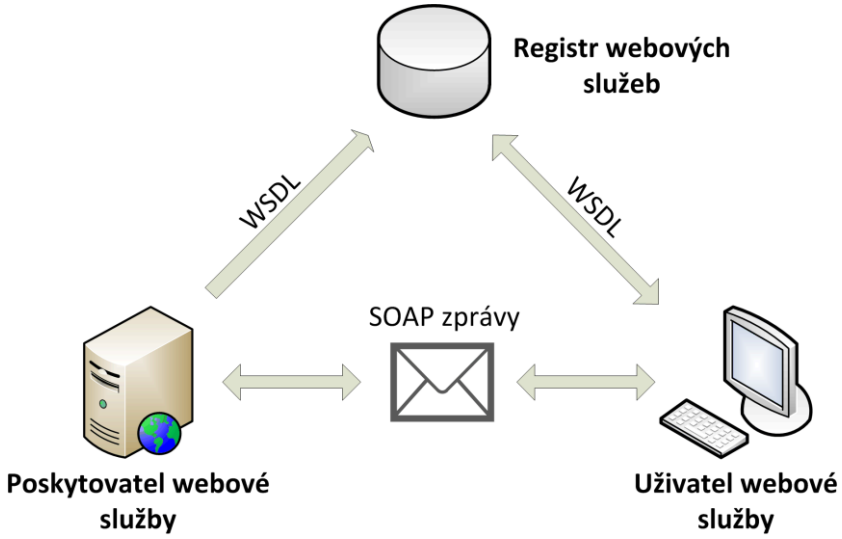
Tato vizualizace zobrazuje nejvíce aktivní hosty v síti, a to dle jejich IP nebo MAC adresy. Zobrazení je formou sloupcového grafu.

Tabulka konverzací

Zobrazuje přehled síťového provozu mezi dvěma koncovými body, rozlišitelnými dle MAC adresy, IP adresy, nebo kombinace IP adresy a portů. Tato vizualizace umožňuje uživatelům rychle identifikovat konverzace mezi hosty a může být použita ve spojení s vizualizací nejvíce komunikujících uzlů. [18]

2.4 Webové služby

Webové služby jsou programová rozhraní pro komunikaci mezi aplikacemi, přístupná skrze internet. Určují rámec pro zasílání zpráv mezi aplikacemi napříč internetem a jediným požadavkem na použití webových služeb je použití standartních internetových protokolů. Na obr. 2.5 se nachází jejich zjednodušené schéma. Webové služby jsou nezávislé na platformách a programovacích jazycích užitých při vývoji aplikací. Tato nezávislost je jedna z klíčových výhod pro implementace webových služeb. Nejběžnější webové služby volají procedury na vzdálených serverech a tyto servery jím odesílají výsledek dané procedury dle přijatých argumentů.



Obr. 2.5: Schéma webových služeb [16]

2.5 SOAP

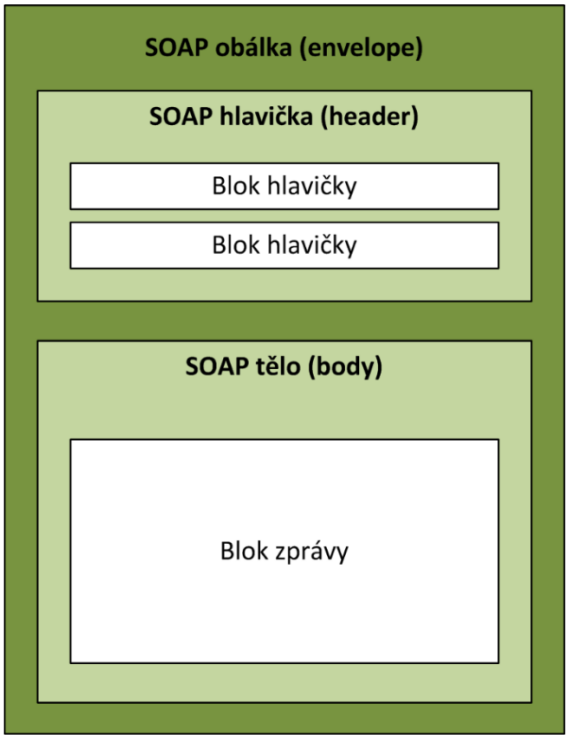
Jedná se o protokol pro posílání zpráv ve webových službách. Definuje pravidla založená na jazyku XML pro přenos zpráv (žádostí a odpovědí) mezi webovými službami. Pro přenos používá protokol HTTP, případně SMTP.

Jeho hlavní čtyři oblasti jsou:

- Popis formátu zprávy, jak může být jednosměrná komunikace zabalena do XML dokumentu.
- Popis způsobu jak by měla být SOAP zpráva přenášená pomocí protokolu HTTP nebo SMTP.
- Soubor pravidel, která je třeba dodržovat při zpracování SOAP zprávy a jednoduchou klasifikaci subjektů, podílejících se na zpracování SOAP zprávy.
- Sada konvencí pro volání vzdálených procedur (RPC).

Principem se jedná o jednoduchý protokol, který umožňuje aplikacím komunikaci mezi různými systémy v distribuovaném prostředí. Má pouze dvě základní vlastnosti, a to odesílat a přijímat HTTP (případně SMTP) pakety a zpracovávat zprávy XML.

Struktura SOAP zprávy se skládá z obálky (`Envelope`), která musí obsahovat jeden povinný element tělo (`Body`) a může obsahovat volitelné hlavičky (`Header`) jak je znázorněno na obr. 2.6.



Obr. 2.6: Struktura SOAP zprávy [16]

Obsah daných elementů je definovaný aplikacemi a nejedná se o část SOAP specifikací. Element „hlavička“ obsahuje blok informací, popisující jak bude se zprávou nakládáno. Část „tělo“ je oblast, kde jsou vyměňovány XML data ve zprávě. [15, 16]

2.6 WSDL

Je programovací jazyk webových služeb na bázi XML. Slouží k detailnímu popisu kompletního rozhraní webových služeb, a je tedy prostředkem pro přístup k webové službě. Popisuje mechaniky interakce s konkrétními webovými službami. WSDL je nezávislý na platformě. Primárně slouží pro popis SOAP služeb. [17]

WSDL má tři hlavní části:

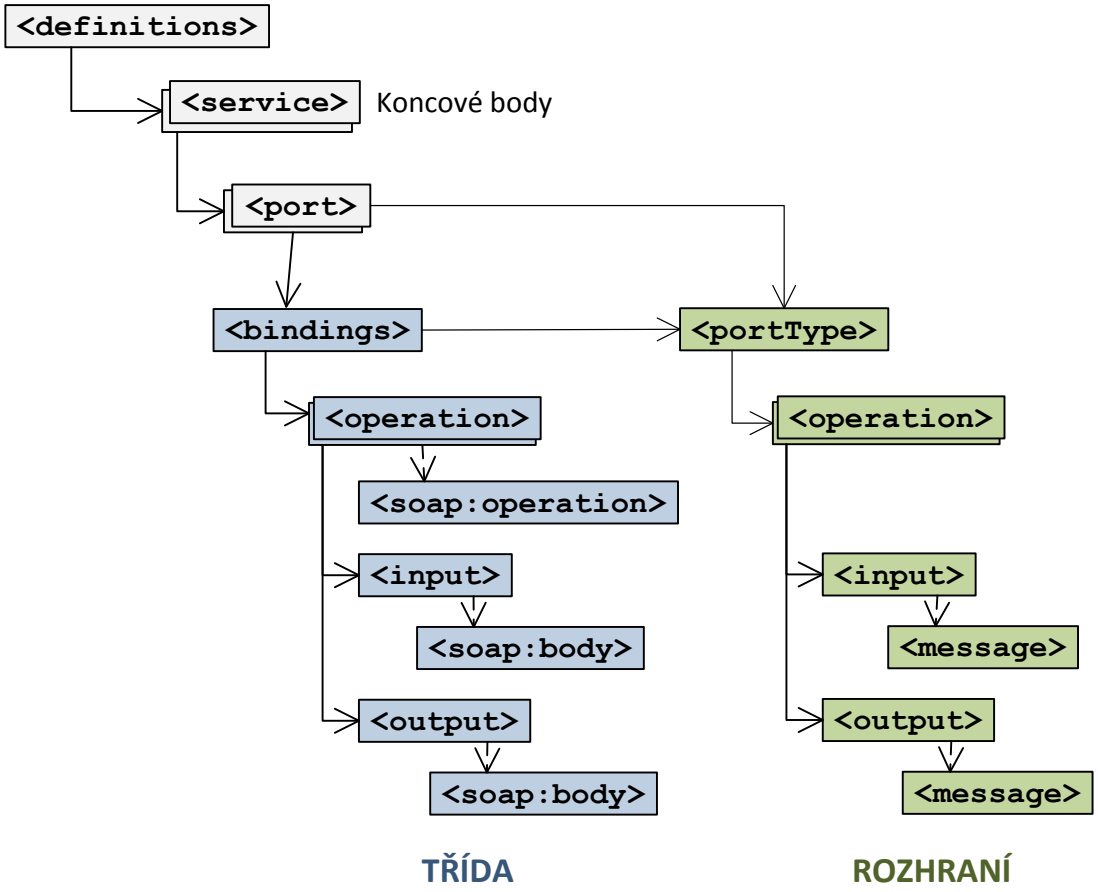
- **Definice** – definice služeb.
- **Operace** – popisují akce pro zprávy podporované webovou službou.
- **Vazby mezi službami** – propojují porty operací s konkrétní síťovou adresou a portem.

WSDL dokument se skládá z následujících elementů [19]:

- `<definitions>` – Obsahuje definice jedné, nebo více služeb.
- `<types>` – Obsahuje definice datových typů. V případě že jsou užity standartní datové typy, nemusí tato sekce být použita ve WSDL dokumentu.

- `<message>` – Abstraktní definice dat, které budou přenášeny.
- `<operation>` – Abstraktní definice akcí podporované službou.
- `<portType>` – Abstraktní sada operací podporovaná jedním nebo více koncovými body.
- `<binding>` – Popisuje jak je operace použita specifickým konkrétním protokolem.
- `<port>` – Určuje koncový bod služby jako adresu pro připojení.
- `<service>` – Specifikuje adresu portu pro připojení. Jedná se o kolekci koncových bodů nebo portů.
- `<import>` – Import jiných XML dokumentů.

Na následujícím obr. 2.7 je vyobrazena struktura WSDL dokumentu s vazbami mezi danými elementy.



Obr. 2.7: Struktura WSDL dokumentu [19]

2.6.1 XSD

Soubor XSD slouží pro popis struktury XML, v našem případě WSDL souborů. Jedná se soubor schématu XML.

XML schéma definuje:

- prvky, které se mohou objevit v dokumentu,
- atributy, které se mohou objevit v dokumentu,
- prvky, které jsou podřazené jiným prvkům,
- pořadí podřazených prvků,
- počet podřazených prvků,
- zda je prvek prázdný, nebo obsahuje text,
- datové typy pro prvky a atributy,
- standartní, nebo výchozí hodnoty prvků a atributů.

XSD soubor může taktéž obsahovat specifické doplňující informace o dokumentu, jako jsou normalizační informace. [20]

3 PRAKTICKÁ ČÁST – LABORATORNÍ ÚLOHY

V následující části se nachází tři vypracované laboratorní úlohy, které jsou připraveny pro použití ve výuce.

První laboratorní úloha se jmenuje „Seznámení s analyzátorem EndaceProbe 7000 a analýza síťového provozu z generátoru IXIA“. Studenti se během práce na této laboratorní úloze seznámí s analyzátorem EndaceProbe 7000, jeho konfigurací v grafickém režimu a s jeho analytickou aplikací EndaceVision. Taktéž se seznámí s generátorem provozu IXIA XM2-02 a spuštěným zátěžovým testem sítí. Prakticky si vyzkouší všechny potřebné kroky pro zachytávání a analyzování síťového provozu.

Druhá laboratorní úloha s názvem „Analýza síťového provozu v laboratorní síti pomocí analyzátoru EndaceProbe 7000 připojeného pomocí vzdáleného zrcadlícího portu přepínače“ seznámí studenty s analyzátorem EndaceProbe 7000 a vysvětluje principy zachytávání a analýzy reálného síťového provozu, který je generován v interní laboratorní síti, včetně nastavení alarmů pro neobvyklé situace. Cílem je seznámit se s možností připojení analyzátoru do analyzované počítačové sítě pomocí vzdáleného zrcadlícího portu přepínače a s nastavením tohoto vzdáleného zrcadlícího portu směrovače na zařízeních Cisco.

Třetí laboratorní úloha se jmenuje „Přístup k analyzátoru EndaceProbe 7000 pomocí SOAP rozhraní a vytváření webových služeb“. Jedná se o základní seznámení s analyzátorem EndaceProbe 7000, s vývojovým prostředím NetBeans a vytvářením webových služeb. Je zde prakticky probráno co je to protokol SOAP, programovací jazyk WSDL a soubor XSD. Jsou zde ve vývojovém prostředí NetBeans použity existující operace webových služeb ale i vytvořeny vlastní operace webových služeb. Také je zde vygenerován vlastní WSDL soubor s vlastní webovou službou.

Ke každé laboratorní úloze jsou taktéž vytvořeny pokyny pro vyučující a každá laboratorní úloha se nachází v příloze na DVD v samostatných souborech PDF, určených pro vytisknutí a okamžité použití ve výuce. Výstupy z laboratorních úloh a konkrétní nastavení aplikací se nachází v přílohách na konci diplomové práce a v přiložených souborech na disku DVD.

3.1 Laboratorní úloha 1 – Seznámení s analyzátorem EndaceProbe 7000 a analýza síťového provozu z generátoru IXIA.

3.1.1 Zadání úlohy

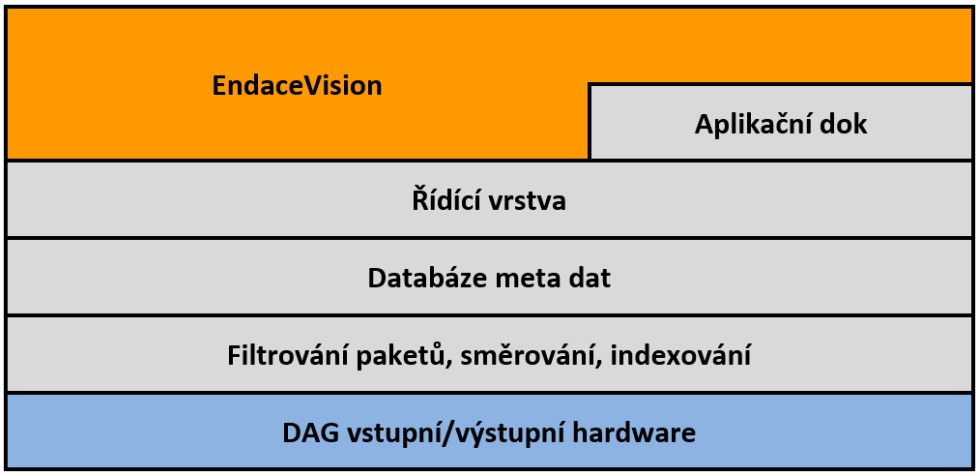
Seznamte se s analyzátorem a rekordérem 10 Gb/s sítí EndaceProbe 7000. Pomocí jeho grafického uživatelského prostředí proveďte potřebné kroky pro zachytávání, ukládání a analýzu síťového provozu, který bude generovat generátor síťových toků IXIA, dle přednastaveného testu. V aplikaci EndaceVision vámi zachycený síťový provoz analyzujte pomocí vytvořených vizualizací umístěných ve vámi vytvořené pracovní ploše a odpovězte na kontrolní otázky na konci úlohy.

3.1.2 Teoretický úvod

EndaceProbe 7000 je velmi výkonný síťový analyzátor a rekordér vytvořen od základů pro zachycení, označení a uložení síťového provozu s udávanou 100% přesností, bez ohledu na rychlost sítě, nebo typ síťového provozu, včetně 10 Gb/s sítí. Jedná se o model z nejvyšší řady společnosti Emulex, která firmu Endace zakoupila v roce 2013. Na obr. 3.1 je vidět vzhled daného analyzátoru, který se nachází v prvním rozvaděči v laboratoři transportních sítí centra SIX.

Obr. 3.1: Síťový analyzátor EndaceProbe 7000 v laboratoři SIX

Systém analyzátoru Endace je založen na tradičním vrstvovém modelu (viz obr. 3.2) zahrnujícím komerční serverový hardware úzce integrovaný s proprietární technologií DAG (Data Acquisition Generation - monitorovací PCI karty pro zachytávání paketů), proprietárním operačním systémem OSm (založeném na linuxové distribuci CentOS) a aplikační vrstvou zahrnující EndaceVison. Systém analyzátoru Endace dále může obsahovat vlastní aplikace, nebo aplikace třetích stran běžící v aplikačním doku.



Obr. 3.2: Schéma vrstvového modelu

Na následující tab. 3.1 jsou uvedeny parametry EndaceProbe.

Tab. 3.1: Parametry EndaceProbe EP7010-PS-FC

Parametr	Hodnota
Operační paměť	48 GB DDR3
Systémový pevný disk	160 GB SSD
Úložné pevné disky	9,6 TB (16x 600 GB, RAID 50)
Řídící rozhraní	2x 10/100/1 GbE a 1x IPMI
Velikost	3 U – 3 jednotky v rozvaděči
Monitorovací porty	2 x SFP+ (Small Form-factor Pluggable)

EndaceVision

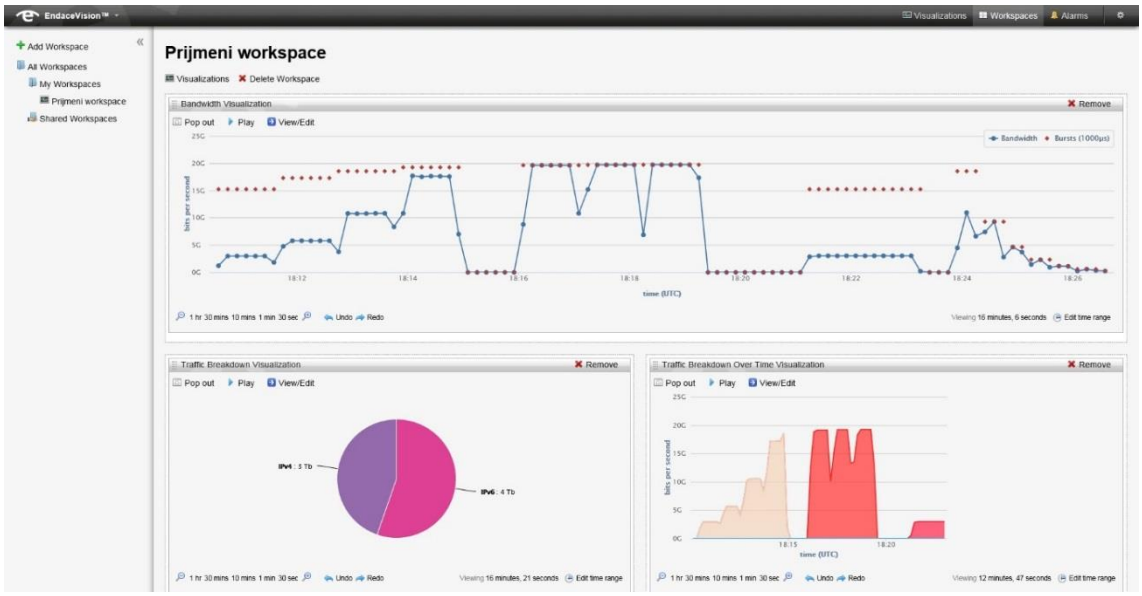
Jedná se o plně integrovanou analytickou aplikaci předinstalovanou v EndaceProbe, poskytující organizaci síťového provozu a bezpečnostní analýzu. Grafické rozhraní je kompatibilní se všemi hlavními prohlížeči (Firefox, Internet Explorer, Chrome, Safari) a operačními systémy. Není potřeba instalovat žádné aplikace na uživatelský počítač. EndaceVision umožnuje přístup více uživatelů ve stejný čas, kdy každý uživatel má vlastní upravitelné pracovní prostředí.

EndaceVision obsahuje:

- EndaceVision Dashboard - uživatelské webové rozhaní.
- Vizuálně přehledné grafické znázornění síťového provozu.

- Analýzu síťového provozu z jedné sondy, nebo seskupené z více sond.
- Analýzu v reálném čase a zpětnou analýzu integrovanou do jediného uživatelského rozhraní.
- Integrace a zobrazování událostí z jiných aplikaci jako je Endace Security Manager a Endace Latency Monitoring.

Pro vytváření vizualizací používá EndaceVision informace o paketech tzv. metadata generovaná v EndaceProbe při jejich záznamu. Toto vytváření metadat v EndaceProbe je nutné aktivovat, při vytváření rotačního souboru (což je soubor do kterého se ukládají zachycená data). Vytvořené vizualizace mohou být seskupovány v tzv. pracovních plochách. Ukázka prostředí a pracovní plochy je vyobrazena na obr. 3.3. Z EndaceVision lze vytvářet přehledné reporty ve formátu PDF, vhodné i pro začínající uživatele.



Obr. 3.3: Pracovní plocha v EndaceVision

V aplikaci EndaceVision lze prohlížet provoz v několika typech grafických vizualizací. Ve vizualizacích lze aplikovat filtry pro omezení zobrazených dat. Úkolem laboratorní úlohy je otestovat jednotlivé vizualizace. Proto také nejsou tyto vizualizace v samotném úvodu popsány.

Generátor provozu IXIA XM2-02

Generátor provozu IXIA viz obr. 3.4 je testovací platforma pro testování širokého spektra služeb od druhé až do sedmé vrstvy ISO/OSI modelu s primárním zaměřením na druhou a třetí vrstvu. Šasi modelu XM2 obsahuje dva sloty pro měřící karty. První instalovaná karta obsahuje 4 testovací porty pro 10/100/1000 Mb/s Ethernet, a v to v provedení konektoru RJ45 i SFP (Small Form-factor Pluggable). Druhá instalovaná karta, která je

použita v této laboratorní úloze obsahuje čtyři 10 GBase-LR porty. Použitá karta je schopna generovat plně duplexní provoz o přenosové rychlosti do 10 Gb/s, a to na každém rozhraní současně. V laboratorní úloze jsou použity dvě rozhraní a směrem k analyzátoru Endace jsou generována data až do součtu přenosové rychlosti 20 Gb/s.

Obr. 3.4: Generátor provozu IXIA XM2 v laboratoři SIX

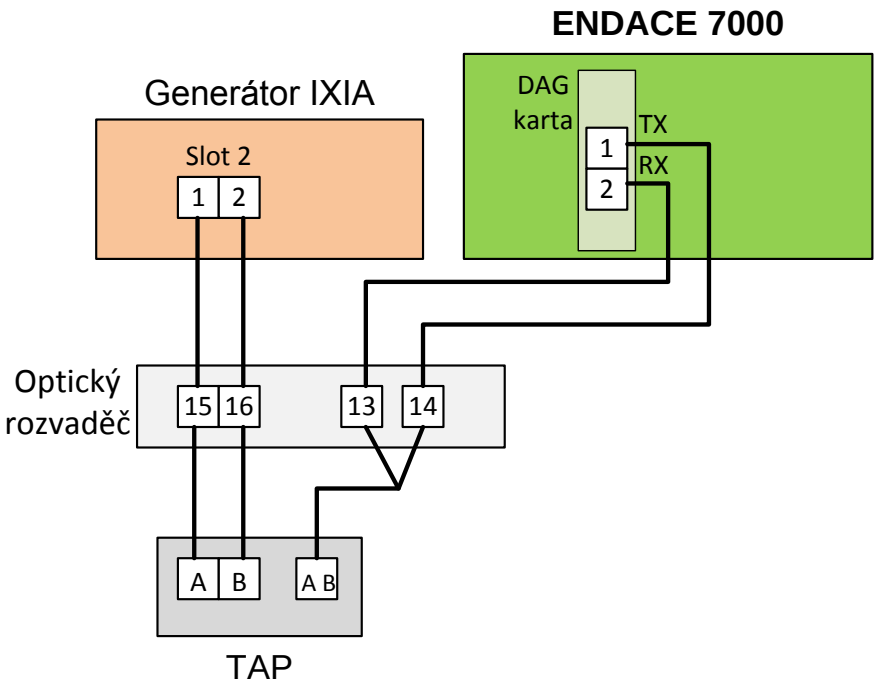
Na generátoru IXIA je spuštěn přednastavený test z doporučení RFC 2544 s názvem „Back to Back“. Jedná se o zátěžový test, který generuje přednastavená data o různé velikosti datových rámců. Pro síť Ethernet se dle daného doporučení jedná o velikosti rámců 64, 128, 256, 512, 1024, 1280 a 1518 bajtů [21]. Každá velikost rámce je generována po dobu jedné minuty, kdy se zvyšuje množství shluků rámců a tím tedy množství generovaných dat a přenosová rychlost. Po té se velikost rámce zvýší, případně po největší velikosti rámce 1518 bajtů se celý test opakuje, v dostatečně dlouhé době, aby byla možnost zachytit a zanalyzovat alespoň jeden průběh testu, a to o délce přibližně 7 minut.

Tento test primárně slouží pro testování rámcové kapacity zařízení. K otestování, kdy daná síť nebo síťové zařízení začne díky přetížení rámce ztrácet, což se dále analyzuje na generátoru IXIA. Tato situace nenastane, ale následujícím úkolem je vypozorovat určité ztráty rámců pro analýzu v EndaceProbe.

3.1.3 Schéma zapojení

Na následujícím obr. 3.5 je zobrazeno schéma zapojení této laboratorní úlohy. Jako zdroj síťového provozu slouží zátěžový generátor IXIA XM2-02, jehož výstupní porty jsou zapojeny do optického rozvaděče. Následně má port 1 propojen s jeho portem 2 v zařízení TAP (Test Access Point), což je pasivní zařízení, které veškerý provoz, který jím prochází, kopíruje na jeho výstupní port, určený pro monitorování sítí. Výstup ze zařízení TAP jde taktéž do optického rozvaděče, kde jsou směry RX a TX rozděleny do samostatných optických kabelů, které jsou připojeny do vstupních portů v SFP+ modulech v našem zařízení Endace takovým způsobem, že v každém ze dvou portů je zapojen pouze jeden směr RX nebo TX a druhá zdířka v konektorech SPF+ modulu je

zaslepena. Toto zapojení, kdy každý směr je zapojen samostatně do portů v SPF+ modulech, umožňuje do analyzátoru Endace přenášet plně duplexní provoz o úhrnné teoretické rychlosti až 20 Gb/s.



Obr. 3.5: Schéma zapojení laboratorní úlohy

3.1.4 Úkoly

Jednotlivé úkoly jsou rozděleny následovně:

1. Přihlásit se do aplikace EndaceProbe.
2. Vytvořit soubor, do kterého se bude ukládat zachytávaná komunikace, tzv. rotační soubor.
3. Nastavit propojení mezi monitorovací DAG kartou a vytvořeným rotačním souborem.
4. Přejít do analytické aplikace EndaceVision.
5. Vytvořit pracovní plochu s vizualizacemi vámi zachytávaného provozu.
6. Analyzovat daný provoz.
7. Odpovědět na kontrolní otázky.

3.1.5 Pracovní postup

1. Přihlášení k EndaceProbe

Na ploše počítače otevřete program Putty a připojte se na předpřipravený profil k serveru `endacev.utko.feec.vutbr.cz`.
Otevře se konzole, kde pro přihlášení použijte následující údaje:

login as: `student.user`
password: sdělí vám vyučující

Nyní spusťte webový prohlížeč a přejděte na adresu `https://localhost:8888`
Zobrazí se přihlašovací stránka do grafické konfigurace systém EndaceProbe, do které se přihlaste zadáním následujících údajů:

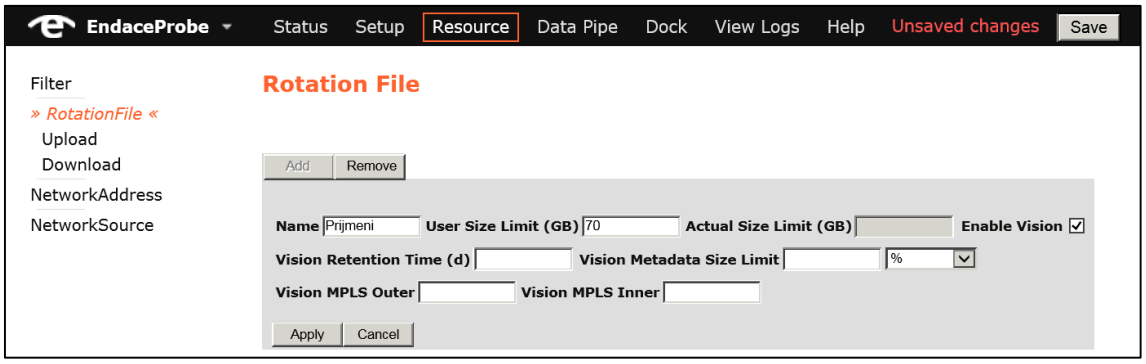
Account: `student.user`
Password: sdělí vám vyučující

Po přihlášení je otevřena stránka zobrazující informace o daném analyzátoru. Z této stránky je možné zjistit dobu nepřetržitého provozu, verzi operačního systému OSm, označení modelu a další doplňkové informace.

Nastavená uživatelská práva umožní si prohlédnout většinu možností nastavení EndaceProbe, avšak bez možností provádění změn, mimo potřebných úkonů pro tuto laboratorní úlohu.

2. Vytvoření rotačního souboru

Rotační soubor, tedy soubor, do kterého je ukládán monitorovaný provoz, vytvoříte v záložce *Resource*. Zde dále klikněte na *RotationFile* a pomocí tlačítka *Add* jej přidejte. Do kolonky *Name* zadejte vaše příjmení. *User size limit* nastavte na 70 GB a zaškrtněte políčko *Enable Vision*, což zviditelní daný rotační soubor pro následnou analýzu v aplikaci Endace Vision. Po zaškrtnutí tohoto tlačítka budou spolu se všemi pakety ukládány do rotačního souboru taktéž informace o daných paketech, sloužící pro generování vizualizací v EndaceVision. Tyto tzv. metadata jsou ukládána do oddělené databáze. Další políčka není nutné v tomto případě nastavovat (automaticky se nastaví na základní hodnoty) a nastavení dokončete potvrzením tlačítka *Apply*. Výše popsané nastavení je zobrazeno na obr. 3.6.



Obr. 3.6: Vytvoření rotačního souboru

Zbývající volby mají následující význam:

- *Vision Retention Time (d)* – maximální počet dní, po které budou ukládány metadata o ukládaném provozu.
- *Vision Metadata Size Limit (% or GB)* – nastavení limitu velikosti databáze s metadaty. Lze zadat konkrétní maximální velikost v GB nebo poměr velikosti z daného rotačního souboru.
- *Vision MPLS Outer* – definuje MPLS vrstvu (hloubku MPLS zásobníku značek) bližší k linkové vrstvě.
- *Vision MPLS Inner* – definuje MPLS vrstvu vrstvu (hloubku MPLS zásobníku značek) bližší k síťové vrstvě.

3. Provázání monitorovací karty s rotačním souborem

Po vytvoření rotačního souboru, je nutné nastavit ukládání zachyceného provozu monitorovací DAG kartou. Toto vytvoříme pomocí tzv. Data Pipe, tedy datové roury, která je propojením mezi vstupem paketů a výstupem těchto paketů.

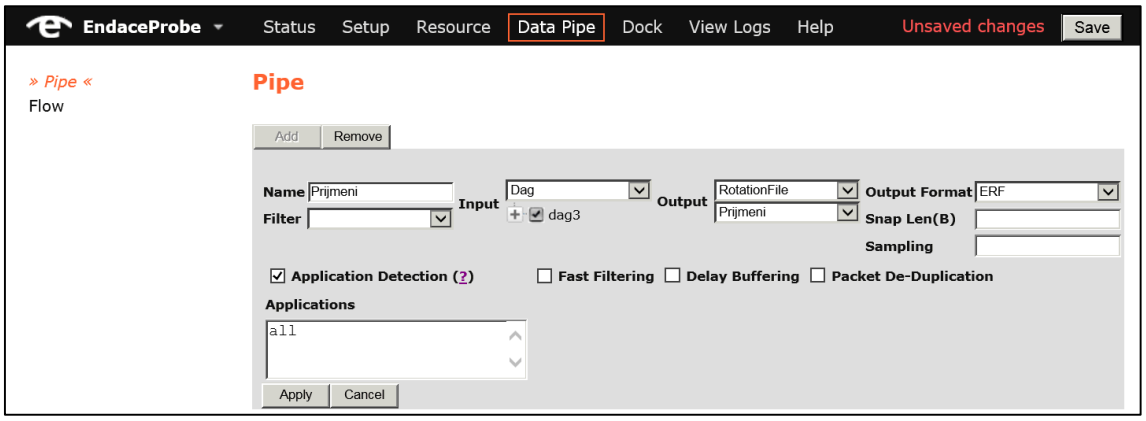
Přejděte do záložky *Data Pipe* a klikněte na tlačítko *Add*. Jako jméno opět zvolte vaše příjmení. *Filter* není žádný vytvářen, toto nastavení proto zůstává beze změny. V položce *Input* zvolte *Dag*, tedy monitorovací kartu. Pod roletkovým menu zaškrtněte *dag3*. Všimněte si, že jako vstup lze taktéž zvolit rotační soubor, *NIC* rozhraní (Network Interface Card, jedno ze dvou řídících rozhraní, které se používá především pro konfiguraci), *vDAG* rozraní (virtuální DAG rozhraní používané ve virtuálních zařízeních, které je možno v EndaceProbe vytvářet) a *NetworkSource* (předem definovaný síťový zdroj).

Jako výstup zvolte z roletkové nabídky *RotationFile* a pod ní vyberte vámi vytvořený rotační soubor s vašim příjmením. *Output Format* ponechte *ERF*. Poslední dva parametry nenastavujte. Parametr *Snap Len(B)* nastavuje maximální velikost ukládaných paketů, parametr *Sampling* nastavuje poměr vzorkování, v případě že ho chceme využívat.

Dále zaškrtneme položku *Application Detection*, která slouží k zapnutí detekce aplikací v provozu, v objeveném seznamu aplikací ponechte *all*. Další položky nebudete používat. Zde jsou uvedeny jejich funkce:

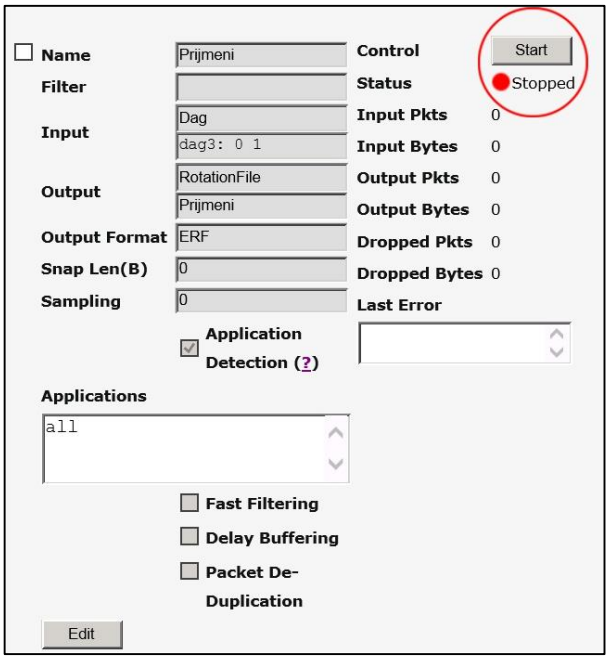
- *Fast Filtering* slouží pro odstranění specifických paketů.
- *Delay Buffering* umožňuje nastavit zpožďovací dobu, po kterou budou v zásobníku datové roury data drženy, před odesláním na výstup.
- *Packet De-duplication* slouží k vytváření duplicit paketů, které mají využití v některých specifických použitích EndaceProbe.

Na následujícím obr. 3.7 je zobrazeno správné nastavení datové roury. Nyní jí můžete již vytvořit stisknutím tlačítka *Apply*.



Obr. 3.7: Vytvoření datové roury

Takto vytvořenou datovou rouru je nutné ještě zapnout, a to stisknutím tlačítka *Start*, nacházejícím se vedle informací o již vytvořené datové rouře, jak je zobrazeno na obr. 3.8. Po zapnutí se vedle informací zobrazí graf, znázorňující tok dat v datové rouře.



Obr. 3.8: Zapnutí datové roury

4. Přechod do EndaceVision

Přejděte do analytické aplikace EndaceVision z hlavní nabídky *EndaceProbe* kliknutím na nabídku *Vision*.

5. Vytvoření pracovní plochy s vizualizacemi

Pokud v EndaceVision ještě neexistují žádné vytvořené Vizualizace, lze vaši pracovní plochu vytvořit velmi jednoduše, vybráním zdrojových dat pro vizualizace a kliknutím na tlačítko *Create workspace with visualizations*. Tímto se vytvoří všechny možné vizualizace ze zadaného rotačního souboru a automaticky se taktéž vytvoří individuální pracovní plocha.

V případě že nějaké vizualizace zůstaly v EndaceVision uloženy, je nutné je odstranit kliknutím na křížek a potvrdit jejich vymazání. Poté pokračujte tak jak je popsáno výše. Vytvořené vizualizace prozkoumejte, pro detailnější analýzu můžete změnit zobrazení časové osy.

6. Analýza zachyceného provozu

Po 10 minutách zachytávání provozu samostatně prozkoumejte vizualizace daného provozu. Dané vizualizace pomocí tlačítka *View/Edit* nastavte tak, abyste dokázali odpovědět na otázky na konci laboratorní úlohy.

7. Analýza provozu v datové rouře

Přejděte zpět do správy EndaceProbe kliknutím na volbu *Probe Management* z hlavního menu a v záložce *Data Pipe* prozkoumejte graf toku dat ve vámi vytvořené datové rouře. Využijte tlačítek +/- pro zmenšení nebo zvětšení měřítka. Je zde možno si všimnout jevu, který se projevuje u největších velikostí rámců, tedy u nejvyšších přenosových rychlostí. Odpovězte na kontrolní otázky, které se dané situace týkají.

8. Odpovědění na otázky a ukončení úlohy

Připravte si odpovědi na všechny otázky uvedené na konci úlohy a zobraze graf vaší datové roury v EndaceProbe a vizualizace ve vaší pracovní ploše v programu EndaceVision.

Po ukončení laboratorní úlohy odstraňte z Endace systémů vše co jste vytvořili, tedy vaší pracovní plochu, vizualizace, datovou rouru i rotační soubor.

Zavřete VNC Viewer a v konzoli zadejte příkaz: `vncserver -kill :3` a následně `exit`.

3.1.6 Kontrolní otázky

1. Jaká monitorovací DAG karta je osazena v našem EndaceProbe?
2. K čemu slouží tzv. Data Pipe?
3. Co zobrazuje v EndaceVision vizualizace Traffic Breakdown Over Time Visualization?
4. Které uzly spolu nejčastěji komunikovaly?
5. Které aplikace měly v síťovém provozu zastoupení?
6. K čemu docházelo v datové rouře při vyšších přenosových rychlostech?
7. Při jakých velikostech datových rámců docházelo k jevu zjištěnému v předchozí otázce?

3.2 Laboratorní úloha 1 – pokyny pro vyučující

3.2.1 Zapnutí provozu

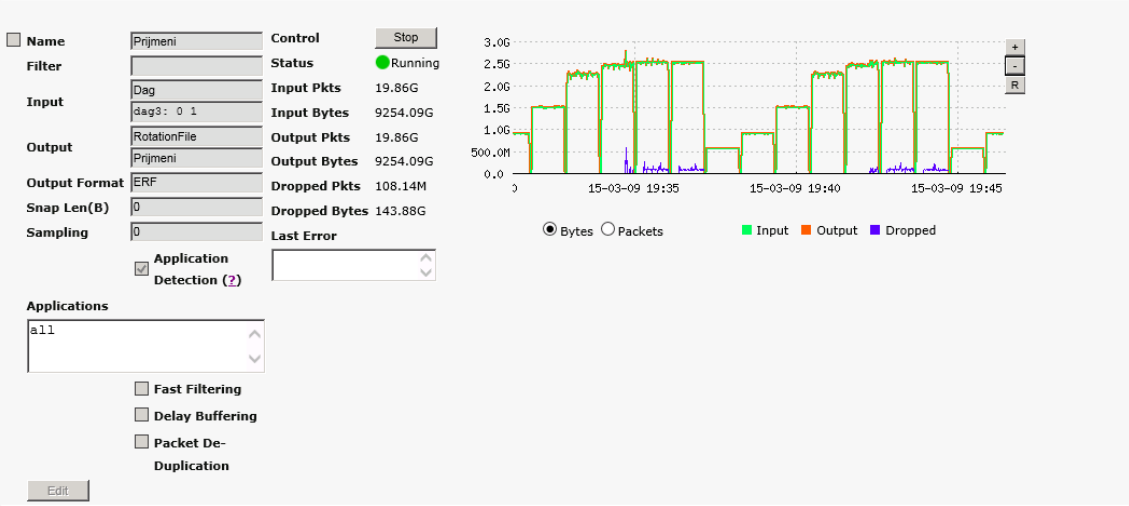
Na serveru *wfpga.utko.feec.vurbr.cz* spusťte aplikaci Aptixia IxAutomate. V pravé dolní části aplikace v okně Configurations nalezněte ve stromové struktuře *RFC 2544 – IPv6 Benchmark -> Back to Back* test s názvem „Lab 1 - Seznámení se s analyzátorem EndaceProbe 7000“. Po kliknutí na tento test se načte konfigurace testu a bude možné jej spustit tlačítkem *Start* v levné horní liště, případně klávesovou zkratkou F5.

V případě že zde konfigurace není, můžete ji naimportovat z nabídky *File -> Import Configuration* ze souboru „test Lab 1 - Seznámení se s analyzátorem EndaceProbe 7000.tcl“.

Daný test je nastaven tak, že se bude přibližně po sedmi minutách opakovat a celková doba trvání testu je přibližně dvě hodiny.

3.2.2 Vzorové grafy a vizualizace

Graf provozu v datové rouře

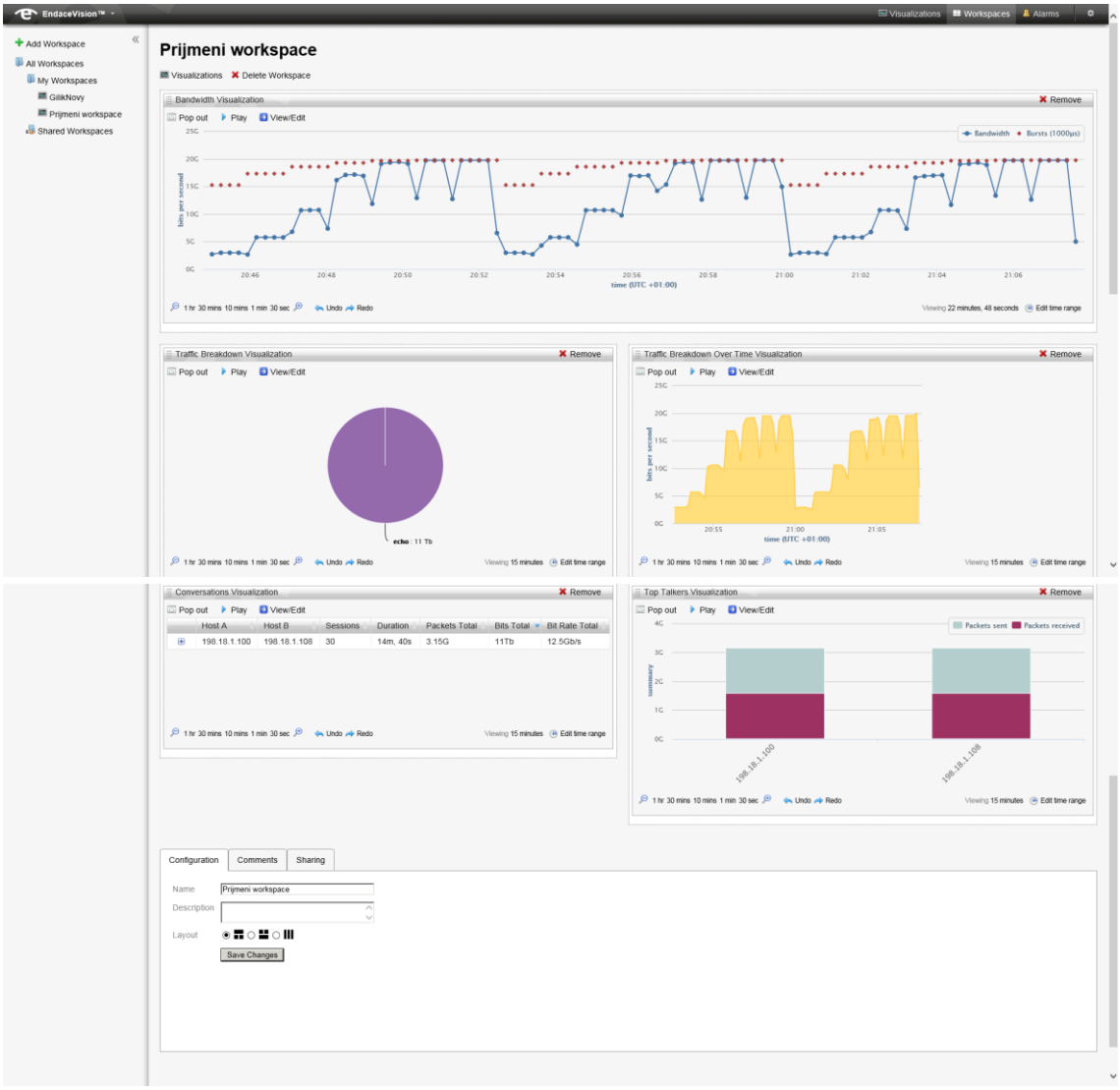


Obr. 3.9: Výsledek úlohy č. 7.: Analýza provozu v datové rouře

Na daném grafu si má student všimnout, že u vyšších přenosových rychlostí dochází k zahazování paketů (v grafu vykresleno modře), které datovou rourou neprošly a nejsou uloženy v rotačním soubory a zanalyzovány pro zpracování v EndaceVision.

Toto je způsobeno přetížením EndaceProbe, které i přes uváděnou 100% přesnost, některé pakety při hraniční přenosové rychlosti 10 Gb/s při plně duplexním režimu nedokáže zpracovat. Tyto rychlosti jsou dosahovány pro velikosti rámce 1024, 1280 a 1518 bajtů. Na daném obrázku je vidět že bylo zahozeno 143,88 Gb dat z celkového množství 9 254,09 Gb dat.

Výsledné vizualizace zobrazené přehledně ve vygenerované pracovní ploše.



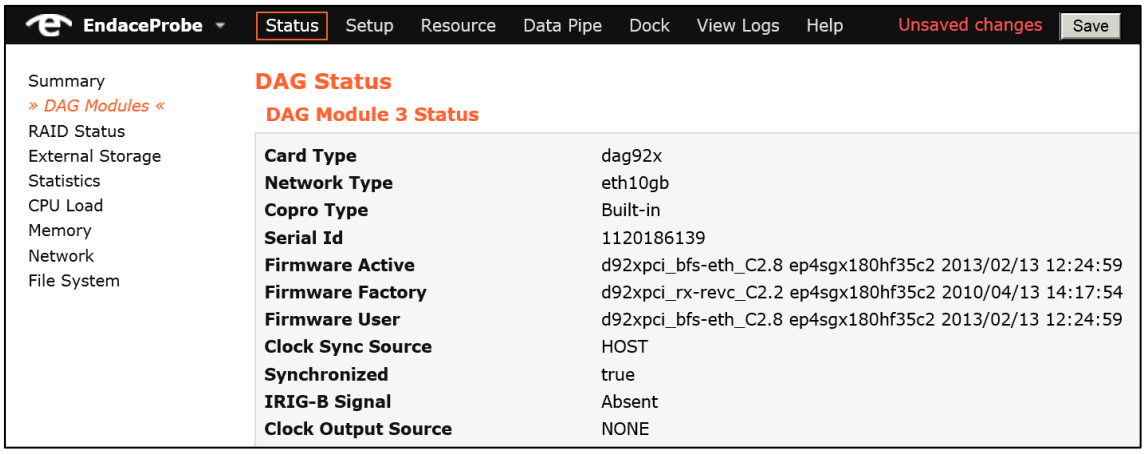
Obr. 3.10: Výsledek úlohy č. 5.: Vytvoření pracovní plochy s vizualizacemi

3.2.3 Odpovědi na otázky

1. Jaká monitorovací DAG karta je osazena v našem EndaceProbe?

- DAG 9.2X (dag92x)

Lze zjistit v nastavení EndaceProbe, v záložce *Status*, v nabídce *DAG modules*.



Obr. 3.11: Výpis DAG karet

2. K čemu slouží tzv. Data Pipe?

Data Pipe, neboli datová roura slouží k propojení vstupu paketů do analyzátoru s jejich výstupem, v našem případě rotačním souborem.

3. Co zobrazuje v EndaceVision vizualizace Traffic Breakdown Over Time Visualization?

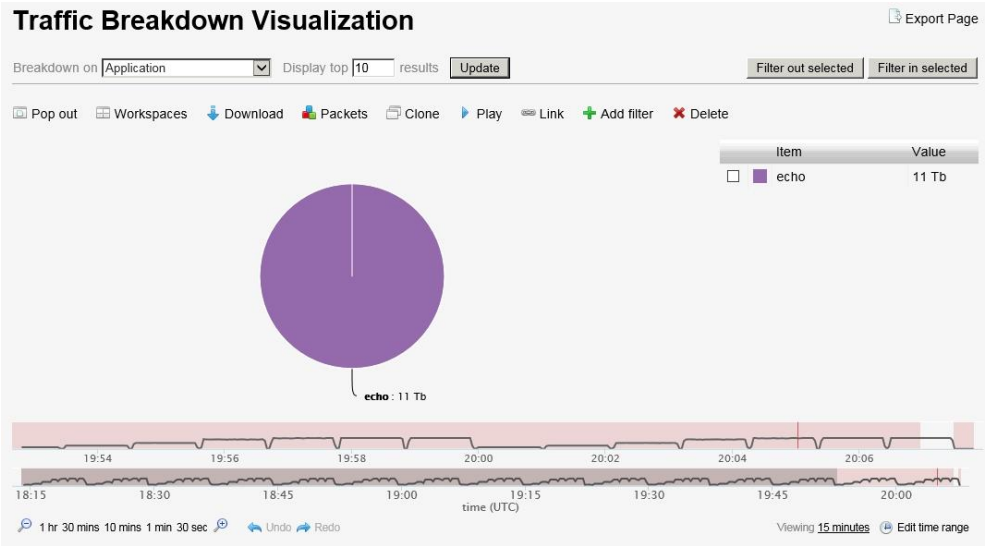
Přehled síťového provozu v závislosti na čase. Zobrazuje síťový provoz dle specifikovaného kritéria v nastavené časové ose. Kritéria pro analýzu jsou: typ aplikace, typ transportního protokolu, verze IP protokolu, VLAN, MPLS, zdrojový a cílový port, zdrojová a cílová IP adresa, zdrojová a cílová MAC adresa.

4. Které uzly spolu komunikovaly?

Zobrazuje vizualizace „*Top Talkers*“, která umožňuje zobrazit hosty dle IP nebo MAC adresy. V měřeném testu spolu komunikovaly uzly s IP adresami 198.18.1.100 a 198.18.1.108

5. Které aplikace měly v síťovém provozu zastoupení?

Zobrazuje pomocí kruhových grafů vizualizace „*Traffic Breakdown Visualization*“ viz obr. 3.12 s nastaveným kritériem pro zobrazení aplikací. Po umístění kurzoru na danou výseč kruhového grafu se zobrazí procentuální hodnota.



Obr. 3.12: Přehled aplikací v zachyceném síťovém provozu

V měřeném testu se nachází pouze data z aplikace echo. Další parametry dat: UDP transportní protokol, IP verze 4, žádné VLAN, žádné MPLS, zdrojový a cílový port UDP/7: echo.

6. K čemu docházelo v datové rouře při vyšších přenosových rychlostech?

Docházelo zde k zahazování paketů, což lze vidět v grafu, viz obr. 3.9.

7. Při jakých velikostech datových rámců docházelo k jevu zjištěnému v předchozí otázce?

K zahazování paketů docházelo při testech s velikosti rámců 1024, 1280 a 1518 bajtů, což lze rozeznat z grafu, jelikož v zadání úlohy je uvedeno, že měřený test se provádí s velikosti rámců 64, 128, 256, 512, 1024, 1280 a 1518 bajtů.

3.3 Laboratorní úloha 2 – Analýza síťového provozu v laboratorní síti pomocí analyzátoru EndaceProbe 7000 připojeného pomocí vzdáleného zrcadlícího portu přepínače.

3.3.1 Zadání úlohy

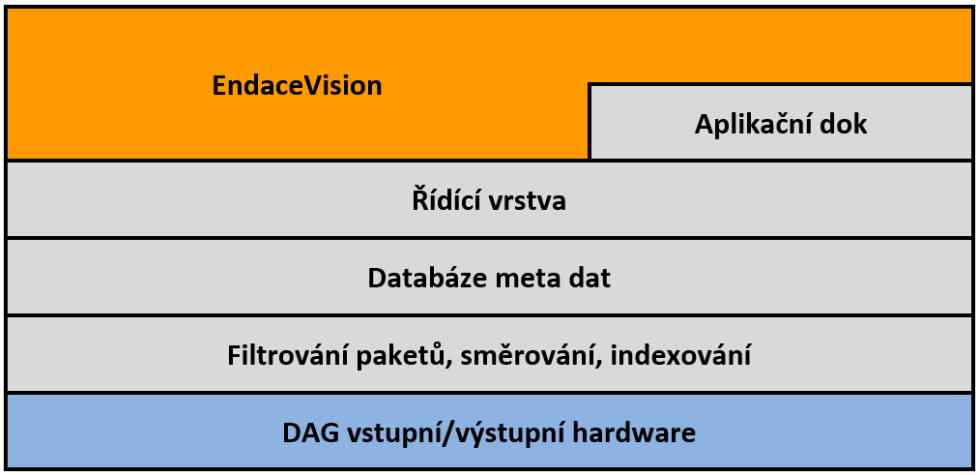
Cílem této úlohy je zachytávání provozu v laboratoři pomoci analyzátoru a rekordéru 10 Gb/s sítí EndaceProbe 7000. V integrované analytické aplikaci EndaceVision analyzujte zachytávaný provoz pomocí vytvořených vizualizací umístěných ve vytvořené pracovní ploše a určenou vizualizaci vyexportujte do souboru PDF. V této aplikaci dále vytvořte alarmy upozorňující na vámi zvolené vlastnosti zachytávaného síťového provozu. Na konci laboratorní úlohy odpovězte na kontrolní otázky.

3.3.2 Teoretický úvod

EndaceProbe 7000 je velmi výkonný síťový analyzátor a rekordér vytvořen od základů pro zachycení, označení a uložení síťového provozu s udávanou 100% přesností, bez ohledu na rychlost sítě, nebo typ síťového provozu, včetně 10 Gb/s sítí. Jedná se o model z nejvyšší řady společnosti Emulex, která firmu Endace zakoupila v roce 2013. Na obr. 3.13 je vidět vzhled daného analyzátoru, který se nachází v prvním rozvaděči v laboratoři transportních sítí centra SIX.

Obr. 3.13: Síťový analyzátor EndaceProbe 7000 v laboratoři SIX

Systém analyzátoru Endace je založen na tradičním vrstvovém modelu (viz obr. 3.14) zahrnujícím komerční serverový hardware úzce integrovaný s proprietární technologií DAG (Data Acquisition Generation - monitorovací PCI karty pro zachytávání paketů), proprietárním operačním systémem OSm (založeném na linuxové distribuci CentOS) a aplikační vrstvou zahrnující EndaceVison. Systém analyzátoru Endace dále může obsahovat vlastní aplikace, nebo aplikace třetích stran běžící v aplikačním doku.



Obr. 3.14: Schéma vrstvového modelu

Na následující tab. 3.2 jsou uvedeny parametry EndaceProbe.

Tab. 3.2: Parametry EndaceProbe EP7010-PS-FC

Parametr	Hodnota
Operační paměť	48 GB DDR3
Systémový pevný disk	160 GB SSD
Úložné pevné disky	9,6 TB (16x 600 GB, RAID 50)
Řídící rozhraní	2x 10/100/1 GbE a 1x IPMI
Velikost	3 U – 3 jednotky v rozvaděči
Monitorovací porty	2 x SFP+ (Small Form-factor Pluggable)

EndaceVision

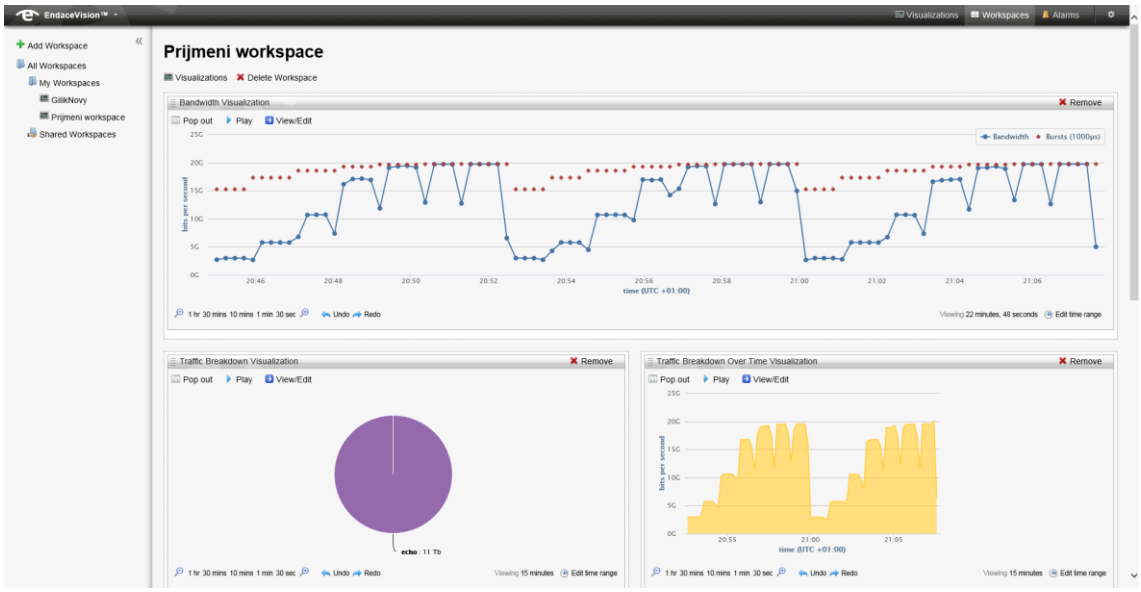
Jedná se o plně integrovanou analytickou aplikaci předinstalovanou v EndaceProbe, poskytující organizaci síťového provozu a bezpečnostní analýzu. Grafické rozhraní je kompatibilní se všemi hlavními prohlížeči (Firefox, Internet Explorer, Chrome, Safari) a operačními systémy. Není potřeba instalovat žádné aplikace na uživatelský počítač. EndaceVision umožnuje přístup více uživatelů ve stejný čas, kdy každý uživatel má vlastní upravitelné pracovní prostředí.

EndaceVision obsahuje:

- EndaceVision Dashboard - uživatelské webové rozhaní.

- Vizuálně přehledné grafické znázornění síťového provozu.
- Analýzu síťového provozu z jedné nebo více sond.
- Analýzu v reálném čase a zpětnou analýzu integrovanou do jediného uživatelského rozhraní.
- Integrace a zobrazování událostí z jiných aplikaci jako je Endace Security Manager a Endace Latency Monitoring.

Pro vytváření vizualizací používá EndaceVision informace o paketech tzv. metadata generovaná v EndaceProbe při jejich záznamu. Toto vytváření metadat v EndaceProbe je nutné aktivovat, při vytváření rotačního souboru (což je soubor do kterého se ukládají zachycená data). Vytvořené vizualizace mohou být seskupovány v tzv. pracovních plochách. Ukázka prostředí a pracovní plochy je vyobrazena na obr. 3.15. Z EndaceVision lze vytvářet přehledné reporty ve formátu PDF, vhodné i pro začínající uživatele.



Obr. 3.15: Pracovní plocha v EndaceVision

V aplikaci EndaceVision lze prohlížet provoz v několika typech grafických vizualizací. Ve vizualizacích lze aplikovat filtry pro omezení zobrazených dat. Úkolem laboratorní úlohy je otestovat jednotlivé vizualizace. Proto také nejsou tyto vizualizace v samotném úvodu popsány.

SPAN

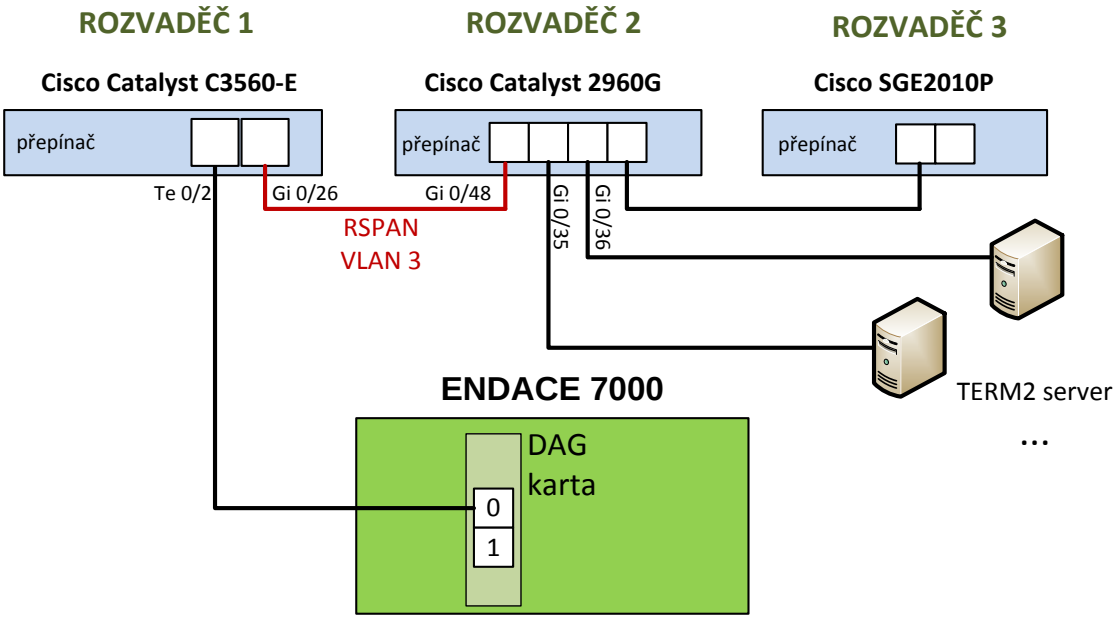
SPAN (Switched Port Analyzer) je zrcadlící port směrovače, na který dokáže přepínač nebo směrovač, který má tuto funkci, kopírovat veškerý, nebo vybraný provoz probíhající na daném přepínači/směrovači. Tento zrcadlící port je určen pro analýzu síťového provozu nebo pro připojení IDS/IPS systému. [23]

RSPAN

Analyzátor Endace je v laboratorní sítí připojen do vzdáleného zrcadlícího portu směrovače, který se označuje jako Remote Switched Port Analyzer. Na vzdálený zrcadlící port dokáže přepínač kopírovat provoz ze vzdáleného přepínače/směrovače a daný provoz se přenáší ve speciálně nakonfigurované virtuální sítí RSPAN VLAN skrz ostatní přepínače/směrovače. [23]

3.3.3 Schéma zapojení

Na následujícím obr. 3.16 je zobrazeno schéma zapojení této laboratorní úlohy. Mezi přepínači v rozvaděči 1 a 2 je vytvořena virtuální síť RSPAN VLAN 3, ve které se dle níže uvedené konfigurace přenáší síťový provoz z určený virtuálních sítí VLAN. Analyzátor EndaceProbe 7000 je připojen na port Te0/2 na přepínači v rozvaděči 1 a tento port je nakonfigurován jako cílový RSPAN port. Zdrojový RSPAN port je port Gi 0/48 na směrovači v rozvaděči 2, v kterém probíhá i síťový provoz ze serveru TERM2 a dalších prvků laboratorní sítě.



Obr. 3.16: Schéma zapojení laboratorní úlohy

3.3.4 Konfigurace přepínačů

Vytvoření rozhraní RSPAN VLAN

Prvním krokem nakonfigurování rozhraní RSPAN je vytvoření virtuální sítě VLAN, která bude tzv. RSPAN VLAN a bude sloužit pro přenos veškerého monitorovaného provozu skrze síť, dle zapojení které potřebujeme. Tuto síť RSPAN VLAN je potřeba vytvořit na

všech přepínačích zúčastněných v RSPAN. V tomto případě je virtuální síť RSPAN VLAN nakonfigurována na přepínači 2960G (s názvem Switch) a C3560-E (s názvem NetCopeSwitch) následujícími příkazy:

```
Switch(config)# vlan 3
Switch(config-vlan)# remote-span
Switch(config-vlan)# end

NetCopeSwitch(config)# vlan 3
NetCopeSwitch(config-vlan)# remote-span
NetCopeSwitch(config-vlan)# end
```

Z konfigurace je patrné označení virtuální sítě VLAN číslem 3 a nastavení této virtuální sítě VLAN jako virtuální sít určenou pro RSPAN.

Vytvoření RSPAN na zdrojovém přepínači

Na přepínači, z kterého se analyzuje síťový provoz, musí být provedena následující konfigurace.

```
Switch(config)# monitor session 1 source vlan 1, 17 – 18, 800
Switch(config)# monitor session 1 destination remote vlan 3
Switch(config)# end
```

Těmito příkazy se vytvoří monitorovací relace s označením 1, jejichž zdroj dat pro monitorování jsou virtuální sítě VLAN 1, 17, 18 a 800, které jsou již vytvořeny a obsahují síťový provoz, který bude v laboratoři monitorován.

Vytvoření RSPAN na cílovém přepínači

Na cílovém přepínači, na který se přenáší analyzovaný provoz, musí být provedena následující konfigurace:

```
NetCopeSwitch(config)#  monitor session 1 source remote vlan 3
NetCopeSwitch(config)#  monitor session 1 destination interface Te0/2
NetCopeSwitch(config)#  end
```

Cílové rozhraní TenGigabitEthernet0/2 musí být nastaveno do jiné virtuální sítě VLAN, než je použita pro RSPAN VLAN. Rozhraní je nastaveno jako přístupové rozhraní virtuální sítě VLAN 4 viz následující konfigurace:

```
NetCopeSwitch(config)#  interface TenGigabitEthernet0/2
NetCopeSwitch(config-if)#  description destination of RSPAN
VLAN 3
NetCopeSwitch(config-if)#  switchport access vlan 4
NetCopeSwitch(config-if)#  switchport mode access
NetCopeSwitch(config-if)#  end
```

Porty, kterými jsou tyto dva přepínače spojeny jsou nakonfigurovaný do tzv. trunk módu, který umožnuje přenos daných VLAN skrze tyto porty dále do sítě. Tohoto je dosaženo následujícími příkazy.

```
Switch(config)#  interface GigabitEthernet0/48
Switch(config-if)#  description ENDACE RSPAN
Switch(config-if)#  switchport trunk allowed vlan 3
Switch(config-if)#  switchport mode trunk

NetCopeSwitch(config)#  interface GigabitEthernet0/26
NetCopeSwitch(config-if)#  description ENDACE RSPAN
NetCopeSwitch(config-if)#  switchport trunk encapsulation
dot1q
NetCopeSwitch(config-if)#  switchport trunk allowed vlan 3
NetCopeSwitch(config-if)#  switchport mode trunk
```

Na přepínači NetCopeSwitch je navíc použit příkaz dot1q, který slouží pro nastavení zapouzdření - označkování rámců technikou IEEE 802.1Q. Na přepínači Switch tento příkaz není použit, jelikož tento přepínač podporuje pouze IEEE 802.1Q zapouzdření. Toto zapouzdření je metoda, která vkládá značky do hlaviček rámců a těmito značkami identifikuje rámce dle konkrétních virtuálních sítí VLAN. [23]

Ověření konfigurace RSPAN

Konfiguraci RSPAN lze prohlédnout příkazem `show monitor`, který zobrazí následující výpis na zdrojovém přepínači Switch:

```
Switch# show monitor
Session 1
---------
Type                    : Remote Source Session
Source VLANs            :
    Both                : 1,17-18,800
Dest RSPAN VLAN         : 3
```

3.3.5 Úkoly

Jednotlivé úkoly jsou rozděleny následovně:

1. Přihlásit se do aplikace EndaceProbe.
2. Vytvořit soubor, do kterého se bude ukládat zachytávaný síťový provoz, tzv. rotační soubor.
3. Nastavit propojení mezi monitorovací DAG kartou a vytvořeným rotačním souborem.
4. Přejít do analytické aplikace EndaceVision.
5. Vytvořit pracovní plochu s vizualizacemi vámi zachytávaného provozu.
6. Analyzovat daný provoz.
7. Exportovat vizualizace zachytávaného síťového provozu do souboru PDF.
8. Vytvořit alespoň 2 alarmy upozorňující na vámi vybrané vlastnosti zachytávaného síťového provozu.
9. Odpovědět na kontrolní otázky.

3.3.6 Pracovní postup

1. Přihlášení k EndaceProbe

Na ploše počítače otevřete program Putty a připojte se na předpřipravený profil k serveru `endacev.utko.feec.vutbr.cz`.
Otevře se konzole, kde pro přihlášení použijte následující údaje:

login as: `student.user`
password: sdělí vám vyučující

Nyní spusťte webový prohlížeč a přejděte na adresu `https://localhost:8888`
Zobrazí se přihlašovací stránka do grafické konfigurace systém EndaceProbe, do které se přihlaste zadáním následujících údajů:

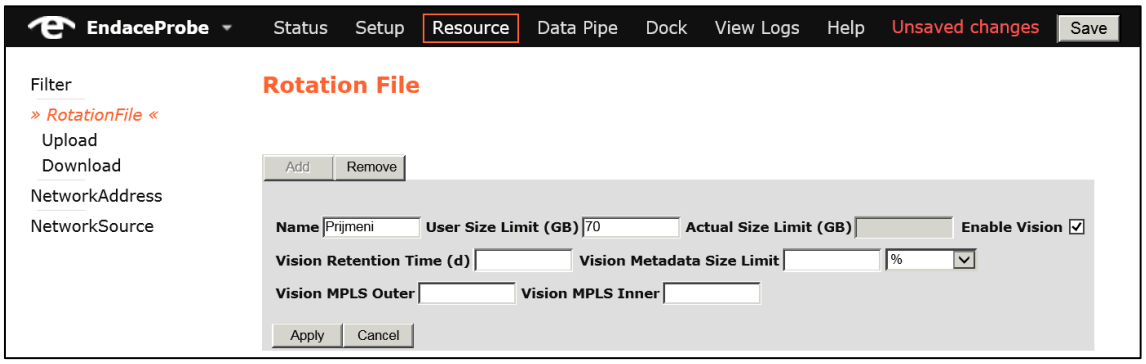
Account: `student.user`
Password: sdělí vám vyučující

Po přihlášení je otevřena stránka zobrazující informace o daném analyzátoru. Z této stránky je možné zjistit dobu nepřetržitého provozu, verzi operačního systému OSm, označení modelu a další doplňkové informace.

Nastavená uživatelská práva umožní si prohlédnout většinu možností nastavení EndaceProbe, avšak bez možností provádění změn, mimo potřebných úkonů pro tuto laboratorní úlohu.

2. Vytvoření rotačního souboru

Rotační soubor, tedy soubor, do kterého je ukládán monitorovaný provoz, vytvoříte v záložce *Resource*. Zde dále klikněte na *RotationFile* a pomocí tlačítka *Add* jej přidejte. Do kolonky *Name* zadejte vaše příjmení. *User size limit* nastavte na 70 GB a zaškrtněte políčko *Enable Vision*, což zviditelní daný rotační soubor pro následnou analýzu v aplikaci Endace Vision. Po zaškrtnutí tohoto tlačítka budou spolu se všemi pakety ukládány do rotačního souboru taktéž informace o daných paketech, sloužící pro generování vizualizací v EndaceVision. Tyto tzv. metadata jsou ukládána do oddělené databáze. Další políčka není nutné v tomto případě nastavovat (automaticky se nastaví na základní hodnoty) a nastavení dokončete potvrzením tlačítka *Apply*. Výše popsané nastavení je zobrazeno na obr. 3.17.



Obr. 3.17: Vytvoření rotačního souboru

Zbývající volby mají následující význam:

- *Vision Retention Time (d)* – maximální počet dní, po které budou ukládány metadata o ukládaném provozu.
- *Vision Metadata Size Limit (% or GB)* – nastavení limitu velikosti databáze s metadaty. Lze zadat konkrétní maximální velikost v GB nebo poměr velikosti z daného rotačního souboru.
- *Vision MPLS Outer* – definuje MPLS vrstvu (hloubku MPLS zásobníku značek) bližší k linkové vrstvě.
- *Vision MPLS Inner* – definuje MPLS vrstvu vrstvu (hloubku MPLS zásobníku značek) bližší k síťové vrstvě.

3. Provázání monitorovací karty s rotačním souborem

Po vytvoření rotačního souboru, je nutné nastavit ukládání zachyceného provozu monitorovací DAG kartou. Toto vytvoříme pomocí tzv. Data Pipe, tedy datové roury, která je propojením mezi vstupem paketů a výstupem těchto paketů.

Přejděte do záložky *Data Pipe* a klikněte na tlačítko *Add*. Jako jméno opět zvolte vaše příjmení. *Filter* není žádný vytvářen, toto nastavení proto zůstává beze změny. V položce *Input* zvolte *Dag*, tedy monitorovací kartu. Pod roletkovým menu zaškrtněte

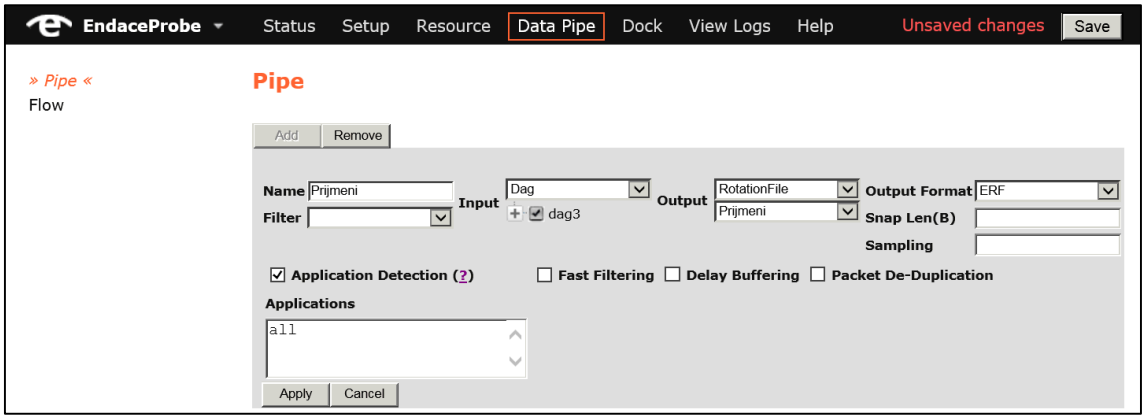
dag3. Všimněte si, že jako vstup lze taktéž zvolit rotační soubor, *NIC* rozhraní (Network Interface Card, jedno ze dvou řídících rozhraní, které se používá především pro konfiguraci), *vDAG* rozraní (virtuální DAG rozhraní používané ve virtuálních zařízeních, které je možno v EndaceProbe vytvářet) a *NetworkSource* (předem definovaný síťový zdroj).

Jako výstup zvolte z roletkové nabídky *RotationFile* a pod ní vyberte vámi vytvořený rotační soubor s vašim příjmením. *Output Format* ponechte *ERF*. Poslední dva parametry nenastavujte. Parametr *Snap Len(B)* nastavuje maximální velikost ukládaných paketů, parametr *Sampling* nastavuje poměr vzorkování, v případě že ho chceme využívat.

Dále zaškrtneme položku *Application Detection*, která slouží k zapnutí detekce aplikací v provozu, v objeveném seznamu aplikací ponechte *all*. Další položky nebudete používat. Zde jsou uvedeny jejich funkce:

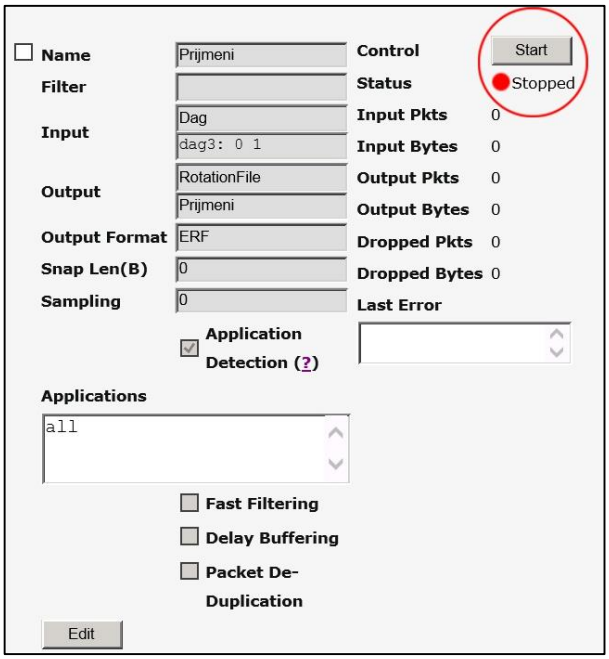
- *Fast Filtering* slouží pro odstranění specifických paketů.
- *Delay Buffering* umožňuje nastavit zpožďovací dobu, po kterou budou v zásobníku datové roury data drženy, před odesláním na výstup.
- *Packet De-duplication* slouží k vytváření duplicit paketů, které mají využití v některých specifických použitích EndaceProbe.

Na následujícím obr. 3.18 je zobrazeno správné nastavení datové roury. Nyní jí můžete již vytvořit stisknutím tlačítka *Apply*.



Obr. 3.18: Vytvoření datové roury

Takto vytvořenou datovou rouru je nutné ještě zapnout, a to stisknutím tlačítka *Start*, nacházejícím se vedle informací o již vytvořené datové rouře, jak je zobrazeno na obr. 3.19. Po zapnutí se vedle informací zobrazí graf, znázorňující tok dat v datové rouře.



Obr. 3.19: Zapnutí datové roury

4. Přechod do EndaceVision

Přejděte do analytické aplikace EndaceVision z hlavní nabídky *EndaceProbe* kliknutím na nabídku *Vision*.

5. Vytvoření pracovní plochy s vizualizacemi

Pokud v EndaceVision ještě neexistují žádné vytvořené Vizualizace, lze vaši pracovní plochu vytvořit velmi jednoduše, vybráním zdrojových dat pro vizualizace a kliknutím na tlačítko *Create workspace with visualizations*. Tímto se vytvoří všechny možné vizualizace ze zadaného rotačního souboru a automaticky se taktéž vytvoří individuální pracovní plocha.

V případě že nějaké vizualizace zůstaly v EndaceVision uloženy, je nutné je odstranit kliknutím na křížek a potvrdit jejich vymazání. Poté pokračujte tak jak je popsáno výše. Vytvořené vizualizace prozkoumejte, pro detailnější analýzu můžete změnit zobrazení časové osy.

6. Analýza zachyceného provozu

Alespoň 10 minut ponechte zachytávání provozu a během tohoto času můžete prozkoumávat možnosti a funkce EndaceVision, které budete dále používat. Po té samostatně prozkoumejte vizualizace daného provozu. Dané vizualizace pomocí tlačítka *View/Edit* nastavte tak, abyste dokázali odpovědět na otázky na konci laboratorní úlohy.

7. Export vizualizace do PDF souboru

Vyexportuje do PDF souboru vizualizaci z EndaceVision znázorňující přehled aplikací komunikujících v zachytávaném síťovém provozu. Export se z dané vizualizace provádí pomocí tlačítka *Export Page*, v horní části okna.

8. Alarmy

V EndaceVision v horní záložce *Alarms*, lze nakonfigurovat alarmy, které budou upozorňovat na vzniklé situace, dle vašeho nastavení. Pomocí tlačítka *Set alarm* vytvořte alespoň dva alarmy (alespoň jeden na detekci aplikace). Tyto alarmy zvolte dle vašeho uvážení a znalosti zachytávaného provozu z předchozího bodu zadání. Alarmům přiřaďte vhodnou úroveň závažnosti a alarmy zapněte pomocí tlačítka *Enable* a přidejte do seznamu sledovaných alarmů, pomocí tlačítka *Alarms watchlist* nacházející se v horní části stránky.

9. Odpovědění na otázky a ukončení úlohy

Připravte si odpovědi na všechny otázky uvedené na konci úlohy, zobrazte vizualizace ve vaší pracovní ploše v programu EndaceVision, vizualizaci vyexportovanou v PDF souboru a váš seznam sledovaných alarmů.

Po ukončení laboratorní úlohy odstraňte z Endace systémů vše co jste vytvořili, tedy alarmy, vaší pracovní plochu, vaše vizualizace, vaší datovou rouru i váš rotační soubor.

Zavřete VNC Viewer a v konzoli zadejte příkaz `vncserver –kill :3` a následně `exit`.

3.3.7 Kontrolní otázky

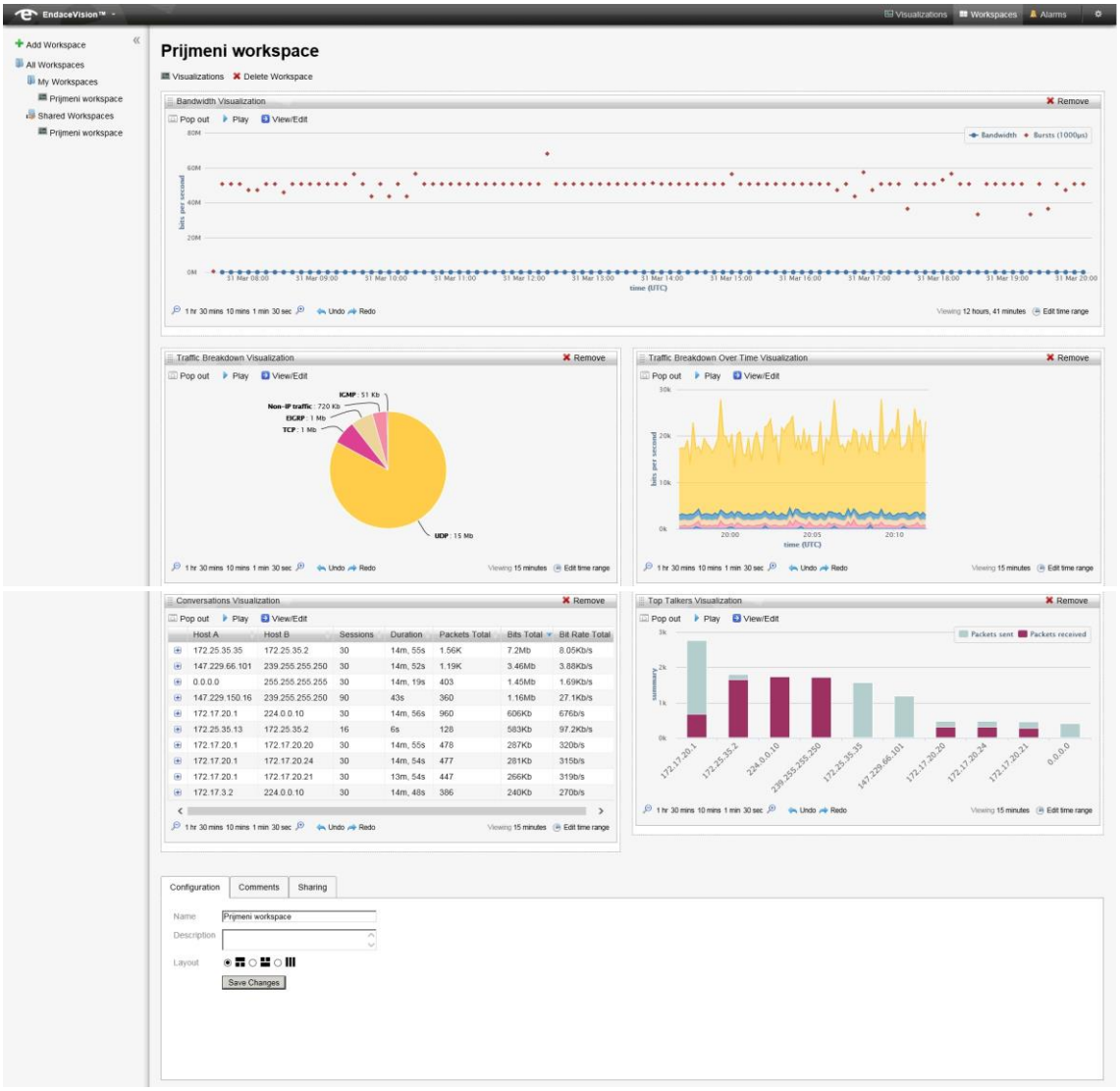
1. Obsahuje zachycený provoz protokol IPv6? Dokažte pomocí vhodné vizualizace.
2. Jaký směrovací protokol je používán v analyzované síti?
3. Jaké procentuální podíly mají transportní protokoly TCP a UDP?
4. Na jakých portech funguje DHCP a jak je v analyzovaném provozu zobrazeno?
5. Jaký je rozdíl mezi SPAN a RSPAN?

3.4 Laboratorní úloha 2 – pokyny pro vyučující

3.4.1 Vzorové grafy a vizualizace

Úkol č. 5: Vytvoření pracovní plochy s vizualizacemi

Na obr. 3.20 se nachází výsledné vizualizace zobrazené přehledně ve vygenerované pracovní ploše. Vizualizace mohou být odlišné, dle aktuálního síťového provozu a nastavení zobrazení jednotlivých vizualizací.



Obr. 3.20: Vytvořená pracovní plocha s vizualizacemi

Úkol č. 7: Export vizualizace do PDF souboru

Řešení úkolu se nachází v příloze A: Vzorový export do PDF souboru z 2. lab. úlohy.

Úkol č. 8: Alarmy

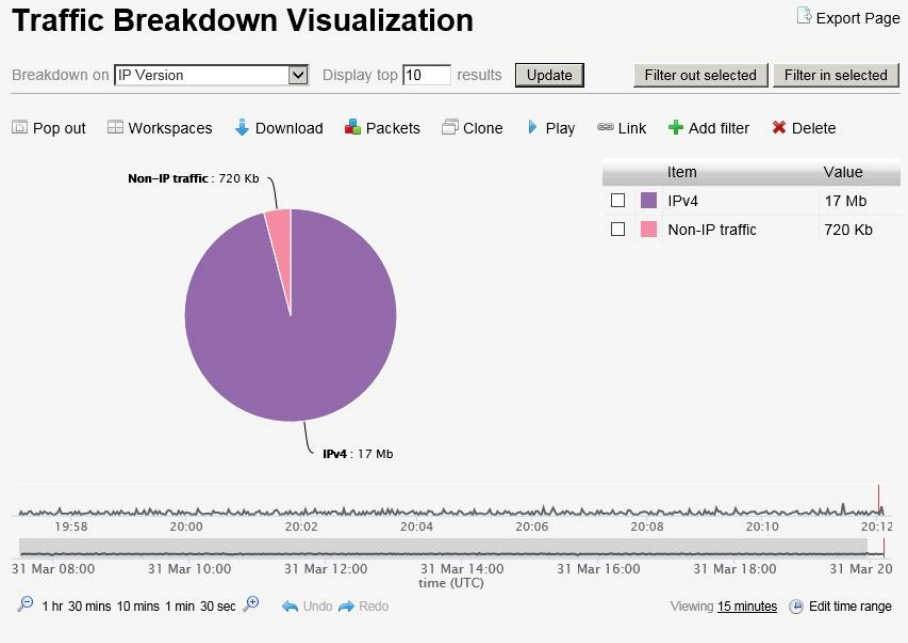
Na následujícím obr. 3.21 se nachází ukázka možného seznamu sledovaných alarmů. Úkolem bylo vytvořit dva alarmy a z toho jeden musí být na detekci aplikace. Na obrázku se jedná o alarm upozorňující na SIP protokol se závažností informativní. Druhý alarm je nakonfigurován na přenosovou shlukovou rychlost nad 30 Mb/s, kdy má nastavenou závažnost „varování“. Rychlost 30 Mb/s je nastavena z důvodu, aby se alarm aktivoval v laboratorní síti, kde přenosová rychlost shluků není velká. Ve sloupci „Fired“ se nachází počet vyvolaných alarmů, za daný časový úsek.

Obr. 3.21: Ukázka vytvořených alarmů v seznamu sledovaných alarmů

3.4.2 Odpovědi na otázky

1. **Obsahuje zachycený provoz protokol IPv6? Dokažte pomocí vhodné vizualizace.**

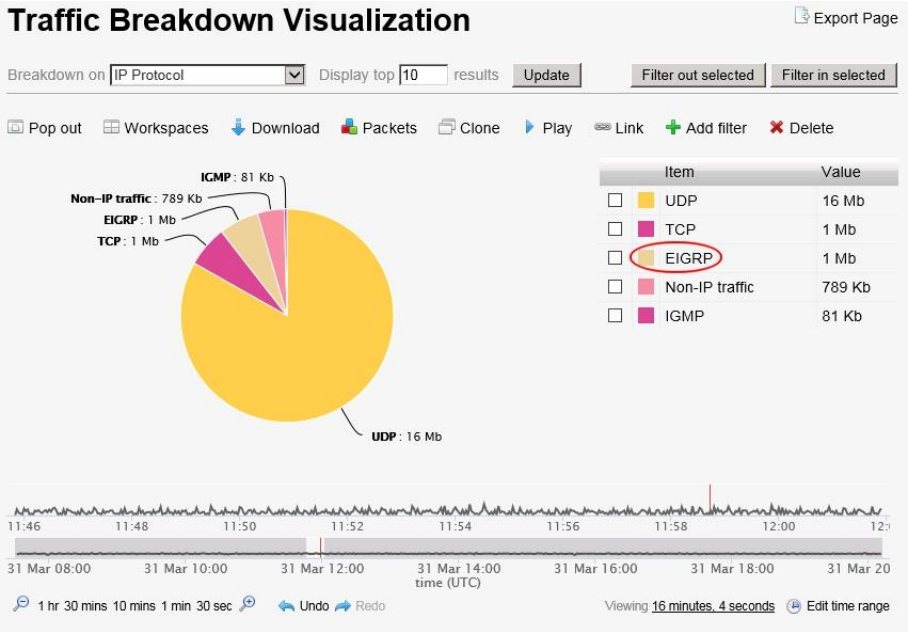
Dle vizualizace zobrazené na obr. 3.22 neobsahuje. Se změnami v laboratoři se toto může změnit.



Obr. 3.22: Verze IP protokolu v zachyceném síťovém provozu

2. Jaký směrovací protokol je používán v analyzované síti?

V laboratorní síti je používán směrovací protokol EIGPR, jak je patrné z vizualizace zobrazené na obr. 3.23.



Obr. 3.23: Přehled protokolů zachycených v síťovém provozu

3. Jaké procentuální podíly mají transportní protokoly TCP a UDP?

Ve vizualizaci z předchozí otázky, viz obr. 3.23 je patrný poměr protokolu TCP a UDP a po umístění kurzoru na danou část grafu se zobrazí procentuální podíl. V ukázce se jedná o 6% podílu TCP a 83% podílu UDP transportního protokolu.

4. Na jakých portech funguje DHCP a jak je v analyzovaném provozu zobrazeno?

V EndaceVision je DHCP protokol zobrazen jako protokol Bootstrap, který používá stejné porty a je předchůdcem DHPC protokolu.

Z vizualizace „Traffic Breakdown Visualization“ se zaměřením na zdrojové a cílové porty lze vyčíst, že zdrojový port DHPC je tedy port UDP/68 označený názvem bootpc a cílový port DHCP je UDP/67 označený názvem bootps.

5. Jaký je rozdíl mezi SPAN a RSPAN?

Zrcadlící port SPAN (Switched Port Analyzer) je lokální zrcadlící port na přepínači nebo směrovači. Na SPAN port se zasílá kopie síťového provozu probíhajícího pouze na daném zařízení.

RSPAN (Remote SPAN) je vzdálený zrcadlící port a síťový provoz, který se na něj kopíruje, pochází z jiného zařízení v dané síti a přenáší se na cílové zařízení ve speciální virtuální RSPAN VLAN síti skrz ostatní přepínače/směrovače.

3.5 Příprava pro třetí laboratorní úlohu

3.5.1 Prostředí virtuálního počítače

Na serveru Dell v laboratoři transportních sítí centra SIX je v systému Hyper-V vytvořen virtuální počítač s operačním systémem CentOS 6.6. Tento operační systém byl vybrán, jelikož je podporován integračními službami technologie Hyper-V. V daném operačním systému pracují studenti v rámci třetí laboratorní úlohy a do systému byl nainstalován program NetBeans IDE 8.0.1. a bylo do něj doinstalováno potřebné prostředí a zásuvné moduly.

Jsou použity následující prostředí a zásuvné moduly:

- Java Development Kit (JDK) ve verzi 1.7 – vývojové prostředí pro programování aplikací v jazyce Java.
- GlassFish server – aplikační server pro Java EE (Enterprise Edition).
- XML Tools – sada nástrojů pro práci s XML dokumenty v programu NetBeans.

3.5.2 Definice SOAP rozhraní zařízení Endace Probe

SOAP rozhraní EndaceProbe je definované ve WSDL souboru, který je možné stáhnout z EndaceProbe pod následujícím odkazem:

```
https://<IP adresa EndaceProbe>/services/fwif?wsdl
```

Popis datových typů a elementů používaných ve WSDL souboru u žádostí a odpovědí obsahuje přidružený XSD soubor, který je možné stáhnout z EndaceProbe pod následujícím odkazem:

```
https://<IP adresa EndaceProbe>/services/ninjaprobe.xsd
```

S těmito výše uvedenými soubory WSDL a XSD je použit program NetBeans s doinstalovanými XML nástroji, pro volání již existujících operací webových služeb zařízení EndaceProbe, vytváření nových operací webových služeb a ke generování vlastního WSDL souboru a SOAP zpráv.

3.5.3 SSL certifikát

S Endace Probe SOAP rozhraním lze komunikovat pouze přes zabezpečené připojení SSL. Toto vyžaduje přítomnost Endace Probe SSL certifikátu v klíčence v systému, kde je aplikace spouštěna. Prvně je nutné vyexportovat SSL certifikát a níže je popsán postup, jak jej lze získat při použití prohlížeče Internet Explorer verze 11.

1. V Internet Exploreru při zobrazené stránce systému EndaceProbe klikneme na *Soubor -> Vlastnosti*
2. Klikneme na tlačítko *Certifikáty*
3. Zobrazí se informace o použitém SSL certifikátu. Vybereme záložku *Podrobnosti* a v ní klikneme na tlačítko *Kopírovat do souboru*.
4. V průvodci klikneme na tlačítko *Další*, napíšeme název souboru pro export certifikátu (v našem případě endace) a jeho místo uložení.
5. Klikneme na tlačítko *Dokončit* a certifikát se uloží pod zvoleným názvem na určené místo v počítači.

Uložený SSL certifikát musí být naimportován do systému, a to následujícím příkazem:

```
keytool -import -keystore ${HOME}/.keystore -file
endace.crt -sigalg RSA
```

3.6 Laboratorní úloha 3 – Přístup k analyzátoru EndaceProbe 7000 pomocí SOAP rozhraní a vytváření webových služeb

3.6.1 Zadání úlohy

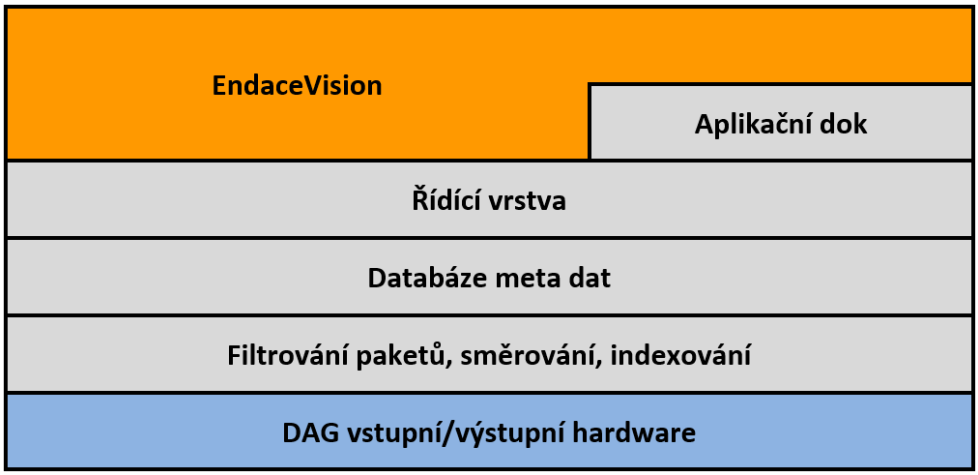
Cílem této úlohy je seznámení se se zařízením EndaceProbe, webovými službami, SOAP rozhraním a programovacím jazykem webových služeb WSDL a XSD. V prostředí NetBeans vytvořte nový projekt, naimportuje ze zařízení EndaceProbe existující webové služby, tyto služby prozkoumejte a vytvořte jednu vlastní funkci webové služby. Svou vlastní webovou služby vyexportujte do WSDL souboru.

3.6.2 Teoretický úvod

EndaceProbe 7000 je velmi výkonný síťový analyzátor a rekordér vytvořen od základů pro zachycení, označení a uložení síťového provozu s udávanou 100% přesností, bez ohledu na rychlost sítě, nebo typ síťového provozu, včetně 10 Gb/s sítí. Jedná se o model z nejvyšší řady společnosti Emulex, která firmu Endace zakoupila v roce 2013. Na obr. 3.24 je vidět vzhled daného analyzátoru, který se nachází v prvním rozvaděči v laboratoři transportních sítí centra SIX.

Obr. 3.24: Síťový analyzátor EndaceProbe 7000 v laboratoři SIX

Systém analyzátoru Endace je založen na tradičním vrstvovém modelu (viz obr. 3.25) zahrnujícím komerční serverový hardware úzce integrovaný s proprietární technologií DAG (Data Acquisition Generation - monitorovací PCI karty pro zachytávání paketů), proprietárním operačním systémem OSm (založeném na linuxové distribuci CentOS) a aplikační vrstvou zahrnující EndaceVison. Systém analyzátoru Endace dále může obsahovat vlastní aplikace, nebo aplikace třetích stran běžící v aplikačním doku.



Obr. 3.25: Schéma vrstvového modelu

Na následující tab. 3.3 jsou uvedeny parametry EndaceProbe.

Tab. 3.3: Parametry EndaceProbe EP7010-PS-FC

Parametr	Hodnota
Operační paměť	48 GB DDR3
Systémový pevný disk	160 GB SSD
Úložné pevné disky	9,6 TB (16x 600 GB, RAID 50)
Řídící rozhraní	2x 10/100/1 GbE a 1x IPMI
Velikost	3 U – 3 jednotky v rozvaděči
Monitorovací porty	2 x SFP+ (Small Form-factor Pluggable)

NetBeans

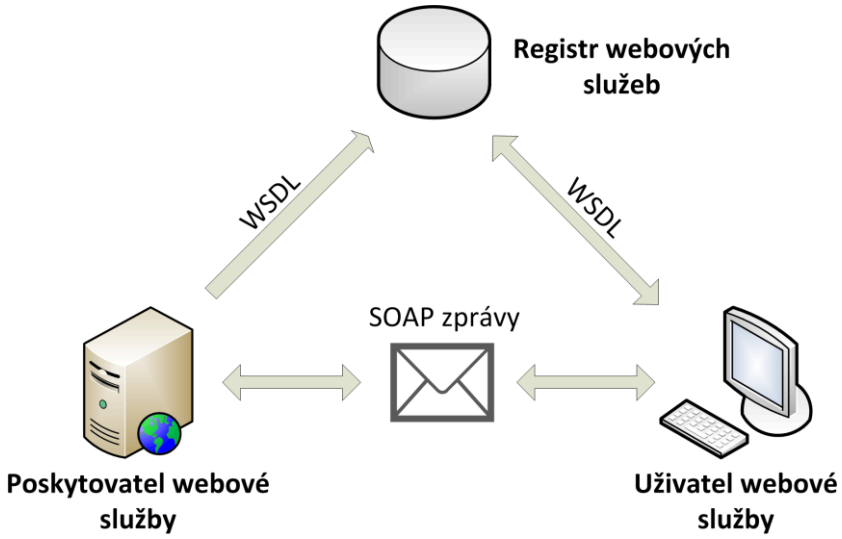
Je integrované vývojové prostředí oficiálně určené pro programovací jazyk Java, v kterém bylo i vytvořeno. Umožňuje vytvářet desktopové, mobilní i webové aplikace. Díky modulárnosti a velkému množství přídavných nástrojů je toto prostředí vhodně pro programování aplikací i v jiných jazycích. Hojně se využívá pro programování v jazycích C/C++ a díky námi použitými zásuvnými moduly, jej lze použít i pro programování webových služeb v jazyku WSDL. Toto vývojové prostředí je zdarma a lze jej spustit na všech operačních systémech podporujících Javu, tedy na operačních systémech Windows, GNU/Linux i Mac OS. V rámci laboratorní úlohy je použita verze NetBeans IDE 8.0.1. [28]

Dále byly použity následující prostředí nebo zásuvné moduly:

- Java Development Kit (JDK) ve verzi 1.7 – vývojové prostředí pro programování aplikací v jazyce Java.
- GlassFish server – aplikační server pro Java EE (Enterprise Edition).
- XML Tools – sada nástrojů pro práci s různými XML dokumenty v programu NetBeans.

Webové služby

Webové služby jsou programová rozhraní pro komunikaci mezi aplikacemi, přístupná skrze internet. Určují rámec pro zasílání zpráv mezi aplikacemi napříč internetem a jediným požadavkem na použití webových služeb je použití standartních internetových protokolů. Na obr. 3.26 se nachází jejich zjednodušené schéma. Webové služby jsou nezávislé na platformách a programovacích jazycích užitých při vývoji aplikací. Tato nezávislost je jedna z klíčových výhod pro implementace webových služeb. Nejběžnější webové služby volají procedury na vzdálených serverech a tyto servery jím odesílají výsledek dané procedury dle přijatých argumentů.



Obr. 3.26: Schéma webových služeb [16]

SOAP

Jedná se o protokol pro posílání zpráv ve webových službách. Definuje pravidla založená na jazyku XML pro přenos zpráv (žádostí a odpovědí) mezi webovými službami. Pro přenos používá protokol HTTP, případně SMTP.

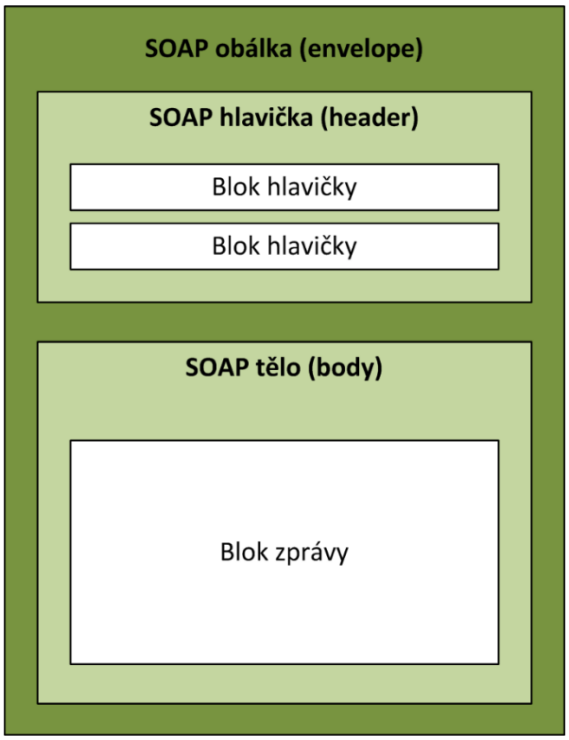
Jeho hlavní čtyři oblasti jsou:

- Popis formátu zprávy, jak může být jednosměrná komunikace zabalena do XML dokumentu.

- Popis způsobu jak by měla být SOAP zpráva přenášená pomocí protokolu HTTP nebo SMTP.
- Soubor pravidel, která je třeba dodržovat při zpracování SOAP zprávy a jednoduchou klasifikaci subjektů, podílejících se na zpracování SOAP zprávy.
- Sada konvencí pro volání vzdálených procedur (RPC).

Principem se jedná o jednoduchý protokol, který umožňuje aplikacím komunikaci mezi různými systémy v distribuovaném prostředí. Má pouze dvě základní vlastnosti, a to odesílat a přijímat HTTP (případně SMTP) pakety a zpracovávat zprávy XML.

Struktura SOAP zprávy se skládá z obálky (`Envelope`), která musí obsahovat jeden povinný element tělo (`Body`) a může obsahovat volitelné hlavičky (`Header`) jak je znázorněno na obr. 3.27.



Obr. 3.27: Struktura SOAP zprávy [16]

Obsah daných elementů je definovaný aplikacemi a nejedná se o část SOAP specifikací. Element „hlavička“ obsahuje blok informací, popisující jak bude se zprávou nakládáno. Část „tělo“ je oblast, kde jsou vyměňovány XML data ve zprávě. [15, 16]

WSDL

Je programovací jazyk webových služeb na bázi XML. Slouží k detailnímu popisu kompletního rozhraní webových služeb, a je tedy prostředkem pro přístup k webové

službě. Popisuje mechaniky interakce s konkrétními webovými službami. WSDL je nezávislý na platformě. Primárně slouží pro popis SOAP služeb. [17]

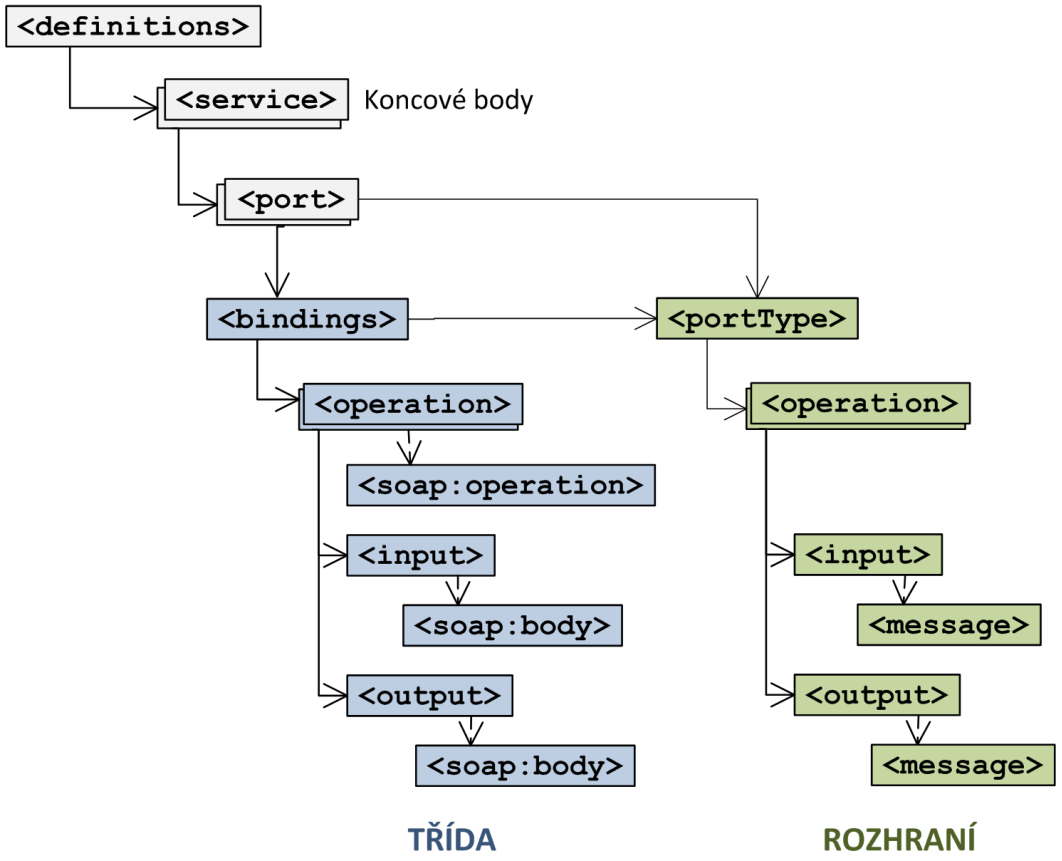
WSDL má tři hlavní časti:

- **Definice**: definice služeb.
- **Operace**: popisují akce pro zprávy podporované webovou službou.
- **Vazby mezi službami:** propojují porty operací s konkrétní síťovou adresou a portem.

WSDL dokument se skládá z následujících elementů [19]:

- `<definitions>` – Obsahuje definice jedné, nebo více služeb.
- `<types>` – Obsahuje definice datových typů. V případě že jsou užity standartní datové typy, nemusí tato sekce být použita ve WSDL dokumentu.
- `<message>` – Abstraktní definice dat, které budou přenášeny.
- `<operation>` – Abstraktní definice akcí podporované službou.
- `<portType>` – Abstraktní sada operací podporovaná jedním nebo více koncovými body.
- `<binding>` – Popisuje jak je operace použita specifickým konkrétním protokolem.
- `<port>` – Určuje koncový bod služby jako adresu pro připojení.
- `<service>` – Specifikuje adresu portu pro připojení. Jedná se o kolekci koncových bodů nebo portů.
- `<import>` – Import jiných XML dokumentů.

Na následujícím obr. 3.28 je vyobrazena struktura WSDL dokumentu s vazbami mezi danými elementy.



Obr. 3.28: Struktura WSDL dokumentu [19]

XSD

Soubor XSD slouží pro popis struktury XML, v našem případě WSDL souborů. Jedná se soubor schématu XML.

XML schéma definuje:

- prvky, které se mohou objevit v dokumentu,
- atributy, které se mohou objevit v dokumentu,
- prvky, které jsou podřazené jiným prvkům,
- pořadí podřazených prvků,
- počet podřazených prvků,
- zda je prvek prázdný, nebo obsahuje text,
- datové typy pro prvky a atributy,
- standartní, nebo výchozí hodnoty prvků a atributů.

XSD soubor může taktéž obsahovat specifické doplňující informace o dokumentu, jako jsou normalizační informace. [20]

3.6.3 Úkoly

Jednotlivé úkoly jsou rozděleny následovně:

1. Přihlásit se pomocí aplikace Putty a programu VNC Viewer na vzdálený virtuální počítač, v kterém budete pracovat.
2. Vytvořit projekt aplikaci NetBeans.
3. Vytvořit klienta webových služeb.
4. Prozkoumat nakopírované soubory ze zařízení EndaceProbe.
5. Umístit projekt na webový server GlassFish.
6. Vytvořit vlastní webovou službu.
7. Volat operaci webové služby.
8. Vytvořit vlastní operaci webové služby.
9. Vygenerovat SOAP zprávy.
10. Vygenerovat vlastní WSDL soubor.
11. Odpovědět na kontrolní otázky.

3.6.4 Pracovní postup

1. Přihlášení se ke vzdálenému počítači.

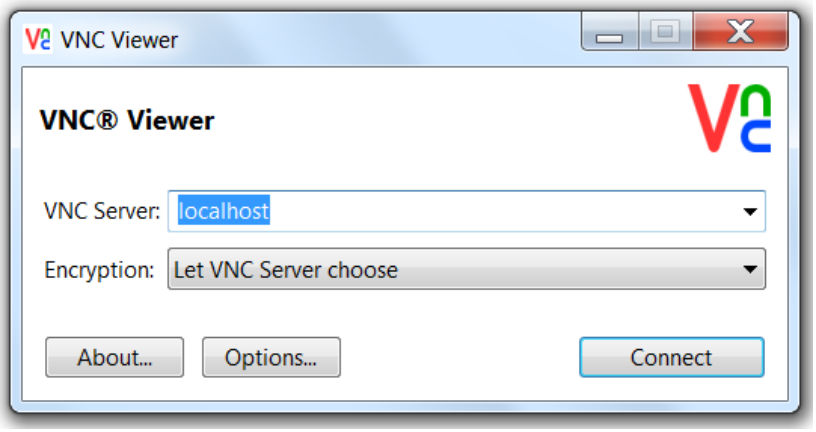
Na ploše počítače otevřete program Putty a připojte se na předpřipravený profil k serveru `endacev.utko.feec.vutbr.cz`.

Vytvoří se zabezpečené SSH tunelové připojení ke vzdálenému počítači a otevře se konzole, kde pro přihlášení použijte následující údaje:

login as: `student.user`
password: sdělí vám vyučující

Po přihlášení zadejte příkaz: `vncserver :3 –localhost`

Nyní spusťte na vašem počítači pomocí ikony z plochy aplikaci VNC Viewer. Tak jak je zobrazeno na obr. 3.29 v položce VNC Server zadejte `localhost` a klikněte na *Connect*.



Obr. 3.29: VNC Viewer

Budete vyzváni k zadání stejného uživatelského hesla, jaké jste použili pro přihlášení ke vzdálenému počítači. Po té bude otevřena vzdálená plocha k systému s operačním systémem CentOS, na kterém se na ploše nachází ikona aplikace NetBeans, kterou spusťte.

2. Vytvoření projektu v NetBeans

Následujícími kroky vytvořte projekt v programu NetBeans za účelem využití webových služeb zařízení Endace.

1. Vyberte z menu *File* položku *New Project.*
2. Z kategorií vyberte *Java Web* a projekt *Web Application.*
3. V dalším kroku pojmenujte projekt vaším příjmením, nastavení složek neměňte.
4. Jako server zvolte *GlassFish* server a zvolte nejnovější verzi *Javy EE 7 Web*.
5. V dalším kroku nevybírejte žádný *Framework* a vytváření projektu dokončete stiskem tlačítka *Finish*.

Následně se nám vytvoří projekt, který lze vidět v pracovním prostředí v NetBeans. Nyní vytvoříme klienta webových služeb, což naimportuje WSDL a XSD soubor z Endace do našeho projektu.

3. Vytvoření klienta webových služeb

Klikněte pravým tlačítkem myši na název projektu a vyberete položku *New – Web Service Client*. V zobrazené nabídce vyberte volbu WSDL URL a zadejte adresu umístění WSDL souboru v zařízení Endace, který se nachází na následující adrese:

```
https://<IP adresa EndaceProbe>/services/fwif?wsdl
```

a klikněte na tlačítko *Finish*. Následně se zobrazí dotaz, zda chcete přijmout bezpečnostní certifikát této zabezpečené webové stránky, na které se nachází WSDL soubor. Certifikát přijměte stiskem tlačítka *Yes*.

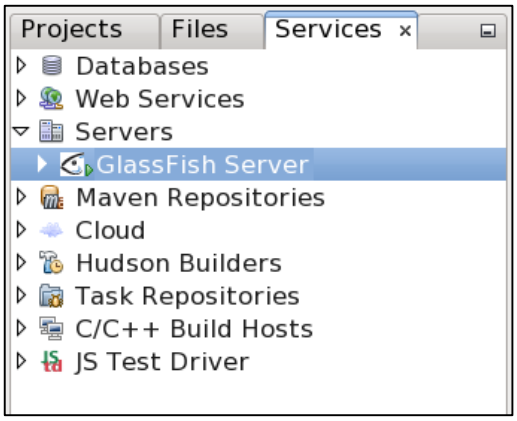
Do našeho projektu se ve stromové struktuře do položky *Generated Sources (jax-ws)* nakopírovaly všechny funkce webových služeb získané z WSDL souboru. A do položky *Configuration Files* se nakopírovaly kompletní soubory *fwif.wsdl* a *ninjaprobe.xsd*.

4. Prozkoumání nakopírovaných souborů

Prozkoumejte soubory, které se ze zařízení EndaceProbe nakopírovaly do vašeho projektu. Dvojitým kliknutím na dané soubory *fwif.wsdl* a *ninjaprobe.xsd* je lze otevřít.

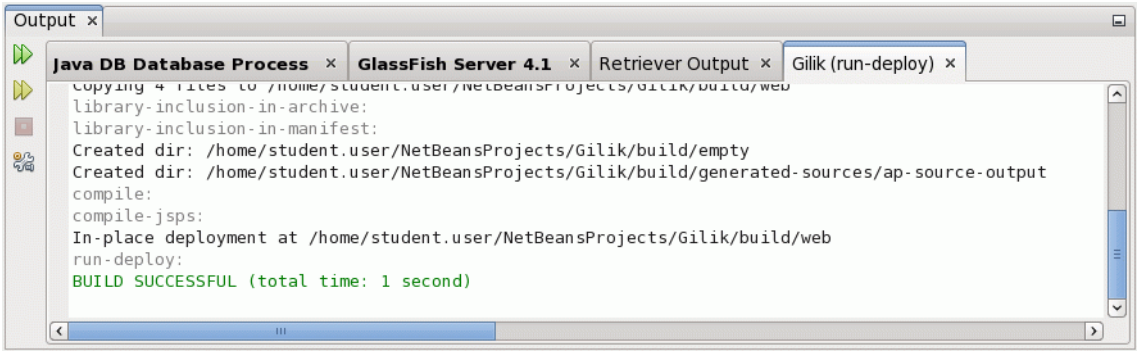
5. Umístění projektu na webový server GlassFish

Dalším krokem projekt umístíme na virtuální webový server GlassFish. Klikněte pravým tlačítkem myši na název vašeho projektu a vyberte položku *Deploy*. Webový server GlassFish se automaticky spustí, což můžete ověřit v záložce *Services* v nabídce *Servers*. Zde se u něj po jeho spuštění zobrazí malá zelená ikonka symbolu *Play*, jak je vidět na obr. 3.30. V této nabídce můžeme tento server i zapnout manuálně, případně vypnout, nebo restartovat.



Obr. 3.30: Spuštěný GlassFish server

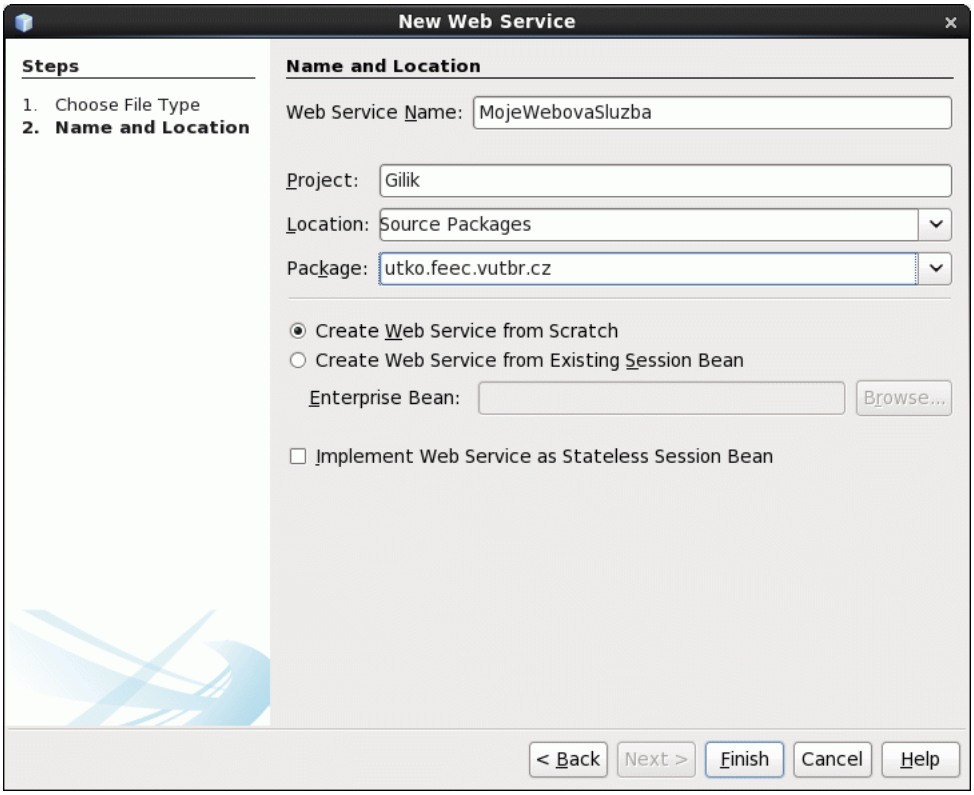
Úspěšným umístěním našeho projektu na webový server jsme si ověřili, že projekt je v pořádku, což lze vyčíst ze záznamu programu NetBeans ve výstupní části okna, viz obr. 3.31.



Obr. 3.31: Úspěšné sestavení projektu

6. Vytvoření vlastní webové služby

Nyní vytvoříme vlastní webovou službu, a také službu využívající zařízení Endace. Klikněte pravým tlačítkem myši na název projektu a vyberte položku *New – Web Service*. Zadejte název vaší webové služby „MojeWebovaSluzba“, zadejte název nového balíčku, který se vytvoří „utko.feec.vutbr.cz“, ponechte volbu *Create Web Service from Scratch*, tedy vytvořit webovou službu od začátku a klikněte na tlačítko *Finish*. Tyto volby jsou zobrazeny na obr. 3.32.



Obr. 3.32: Vytvoření nové webové služby

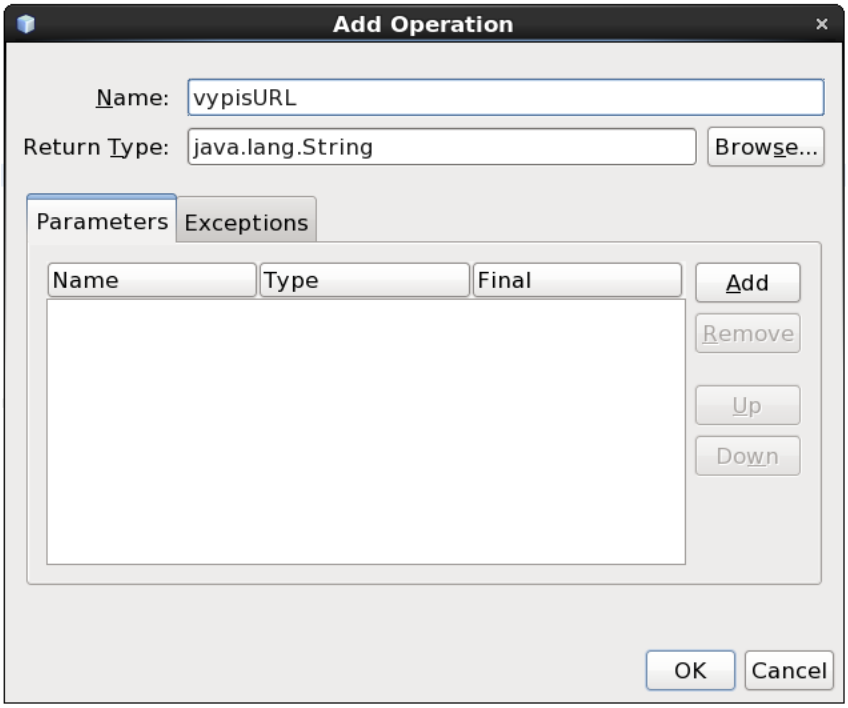
Následně se vytvoří ve stromové struktuře projektu položka *Web Services*, ve které se nachází vámi vytvořená webová služba, která automaticky obsahuje funkci *Hello*. Znovu umístěte váš aktuální projekt na server GlassFish pomocí volby *Deploy*. Po úspěšném sestavení projektu klikněte pravým tlačítkem ve stromové struktuře projektu na název vaší webové služby a vyberte volbu *Test Web Service*. Spustí se webový prohlížeč, ve kterém můžete vyzkoušet automaticky vytvořenou funkci *Hello*, která po stisknutí tlačítka *hello* vrací text napsaný ve vstupním poli, které se nachází vedle tohoto tlačítka na dané webové stránce.

7. Volání operace webové služby

Při programování vlastních webových služeb je možné volat operace, které se naimportovaly z původního WSDL souboru ze zařízení Endace. Klikněte pravým tlačítkem myši kdekoliv v kódu vaší webové služby, vyberte položku *Insert Code* a z dalších voleb vyberte *Call Web Service Operation*. Otevře se okno, kde si můžete zobrazit seznam všech operací, které lze volat ze souboru *fwif.wsdl*, který jste naimportovali v třetím kroku. Vyberte první operaci, která se jmenuje *DagListAll* a klikněte na tlačítko *OK*. Na konec vaší třídy *MojeWebovaSluzba* se vložil kód, privátní funkce s názvem *DAGList*, na začátek vaší třídy se vložila cesta k WSDL souboru a privátní proměnná. Taktéž se naimportovaly potřebné balíčky. Dále s importovanou funkcí nebudeme pracovat a vyzkoušíme si vytvoření vlastní operace webové služby.

8. Vytvoření vlastní operace webové služby

Vytvoříme vlastní operaci webové služby, která nám vypíše umístění importovaného WSDL souboru. Klikněte znovu pravým tlačítkem myši do vaší třídy *MojeWebovaSluzba*, vyberte položku *Insert Code* a z dalších voleb vyberte *Add Web Service Operation.* Zobrazí se okno, které je zobrazeno na obr. 3.33, do kterého zadejte pouze do pole *Name* jméno vaší operace „vypisURL“ a klikněte na tlačítko *OK*. Do kolonky *Parametrs* by jsme mohli zadat vstupní parametry a jejich typy a do kolonky *Exceptions* výjimky.



Obr. 3.33: Přidání operace webové služby

Do naší třídy se vygeneruje následující funkce, která ještě neobsahuje žádné proměnné a objekty funkce:

```
@WebMethod(operationName = "vypisURL")
    public String vypisURL() {
        //TODO write your implementation code here:
        return null;
    }
```

Nyní doprogramujeme tuto funkci tak, že vytvoříme v této webové operaci proměnou typu URL, kterou nazveme „adresa“ a do této proměnné přiřadíme URL adresu WSDL dokumentu, pomocí funkce *getWSDLDocumentLocation()* z třídy *service*. Návratovou hodnotu operace změníme na naší proměnou „adresa“, která bude převedena na řetězec znaků.

Výsledek vypadá takto:

```
@WebMethod(operationName = "vypisURL")
    public String vypisURL() {
     URL adresa = service.getWSDLDocumentLocation();
        return adresa.toString();
    }
```

Na začátek projektu musím přidat k naimportováni třídu *java.net.URl* a to následujícím příkazem: `import java.net.URL;`

9. Vygenerované SOAP zprávy

Znovu umístěte váš aktuální projekt na server GlassFish pomocí volby *Deploy*. Po úspěšném sestavení projektu klikněte pravým tlačítkem ve stromové struktuře projektu na název vaší webové služby a vyberte volbu *Test Web Service*. Spustí se znovu webový prohlížeč, kde se již bude nacházet tlačítko pro spuštění i vaší nové webové operace vypisURL, tak jak je zobrazeno na obr. 3.34. Po stisknutí tohoto tlačítko se operace provede. Na webové stránce se zobrazí vrácená hodnota, tedy adresa URL importovaného WSDL souboru a vypíšou se vygenerované zprávy *SOAP Request* a *SOAP Response*.

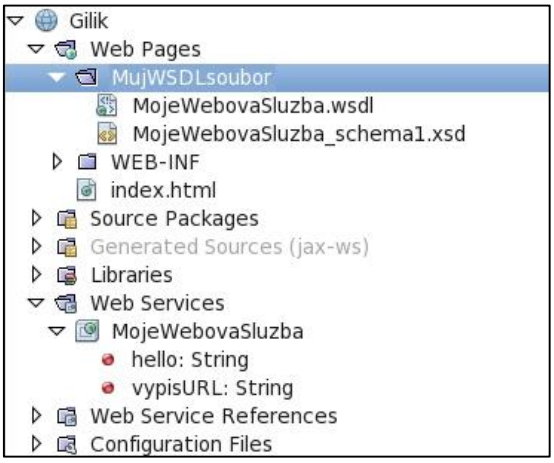
Obr. 3.34: Testování webové služby

10. Vygenerování vlastního WSDL souboru

Nyní již pouze zbývá vygenerování vlastního WSDL souboru obsahujícího naší webovou službu. Prvně vytvoříme složku pro tento soubor, která se bude nacházet ve složce *Web Pages*. Klikněte tedy pravým tlačítkem myši ve stromové struktuře projektu na složku *Web Pages* a vyberte položku *New -> Folder*. Jako název vaší složky zadejte „MujWSDLsoubor“ a klikněte na tlačítko *Finish*.

Vygenerování vlastního WSDL souboru proveďte kliknutím pravým tlačítkem myši na název vaší vytvořené webové služby v položce *Web Services* a vyberte volby *Generate*

and Copy WSDL. V otevřeném okně vyberte vámi vytvořenou složku „MujWSDLsoubor“ a klikněte na tlačítko *OK*. Do dané složky se vygeneruje WSDL soubor obsahující vaše webové služby a soubor XSD, popisující datové typy a elementy ve WSDL souboru. Struktura projektu s touto složkou je zobrazena na obr. 3.35.



Obr. 3.35: Struktura projektu

11. Odpovědění na otázky a ukončení úlohy

Připravte si odpovědi na všechny otázky uvedené na konci úlohy a předveďte vygenerované zprávy *SOAP Request* a *SOAP Response* zobrazené ve webovém prohlížeči a váš WSDL soubor v NetBeans. Po ukončení vymažte váš projekt v programu NetBeans pomocí pravého tlačítka myši a volby *Delete* a před potvrzením zaškrtněte taktéž volbu *„Also delete sources under folder“*. Zavřete aplikaci VNC Viewer a v konzoli zadejte příkaz: `vncserver -kill :3` a následně `exit`.

3.6.5 Otázky

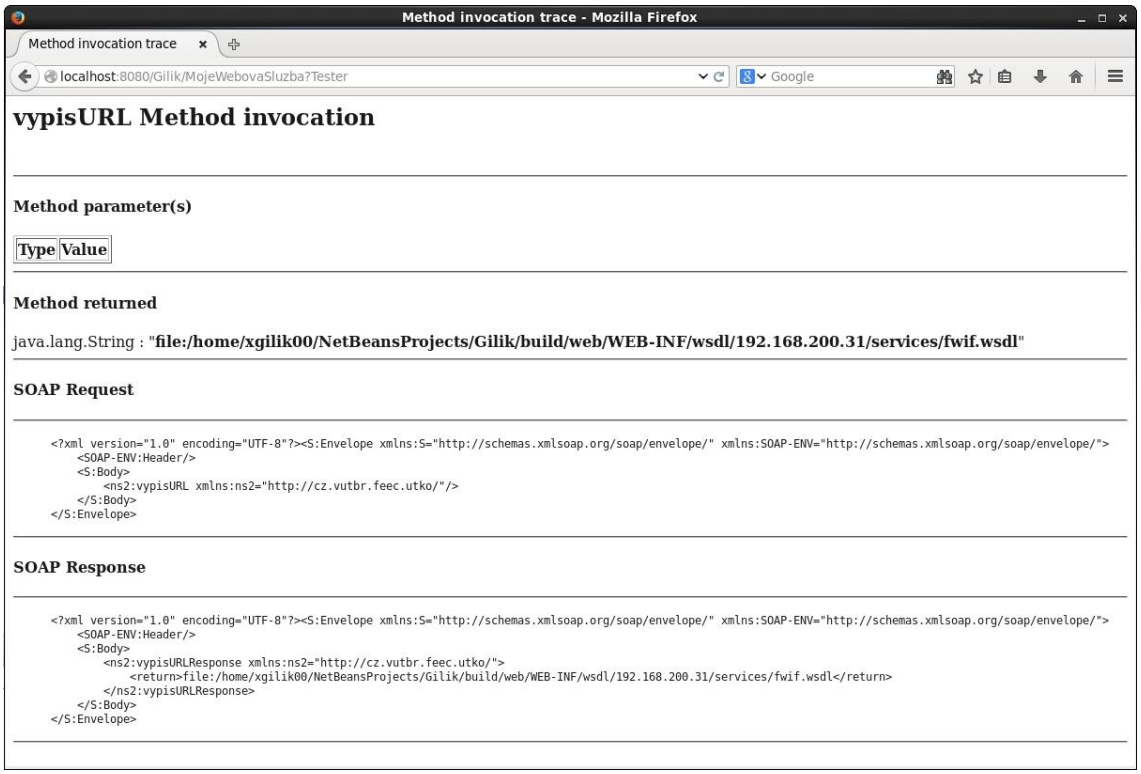
1. Co jsou to webové služby?
2. K čemu slouží protokol SOAP?
3. Z čeho se skládá struktura SOAP zprávy?
4. K čemu slouží programovací jazyk WSDL?
5. Navrhněte vhodné použití webových služeb zařízení EndaceProbe.

3.7 Laboratorní úloha 3 – pokyny pro vyučující

3.7.1 Výsledky práce studentů

Úkol č. 9 - Vygenerované SOAP zprávy

Na následujícím obr. 3.36 jsou vidět vygenerované zprávy *SOAP Request* a *SOAP Response*.



Obr. 3.36: Vygenerované zprávy SOAP Request a SOAP Response

Výsledný kód webové služby

```
package utko.feec.vutbr.cz;

import com.endace.ninjaprobe.DAGList;
import com.endace.ninjaprobe.Fwif_Service;
import com.endace.ninjaprobe.ReturnStatus_Exception;
import java.net.URL;
import javax.jws.WebService;
import javax.jws.WebMethod;
import javax.jws.WebParam;
import javax.xml.ws.WebServiceRef;

@WebService(serviceName = "MojeWebovaSluzba")
```

```
public class MojeWebovaSluzba {
    @WebServiceRef(wsdlLocation = "WEB-
    INF/wsdl/192.168.200.31/services/fwif.wsdl")
    private Fwif_Service service;

    @WebMethod(operationName = "hello")
     public String hello(@WebParam(name = "name") String
     txt) {
     return "Hello " + txt + " !";
    }

    private DAGList dagListAll() throws
    ReturnStatus_Exception {
    com.endace.ninjaprobe.Fwif port = service.getFwif();
    return port.dagListAll();
    }

    @WebMethod(operationName = "vypisURL")
    public String vypisURL() {
    URL adresa = service.getWSDLDocumentLocation();
      return adresa.toString();
    }
}
```

3.7.2 Odpovědi na otázky

1. Co jsou to webové služby?

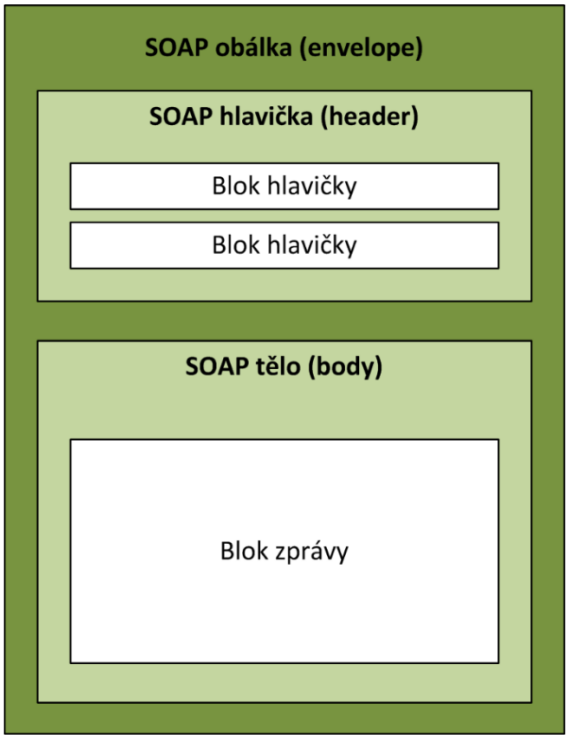
Webové služby jsou programová rozhraní pro komunikaci mezi aplikacemi, přístupná skrze internet. Určují rámec pro zasílání zpráv mezi aplikacemi přes internet a jediným požadavkem na použití webových služeb je použití standartních internetových protokolů.

2. K čemu slouží protokol SOAP?

Jedná se o protokol pro posílání zpráv ve webových službách. Definuje pravidla založená na jazyku XML pro přenos zpráv (žádostí a odpovědí) mezi webovými službami. Pro přenos používá protokol HTTP, případně SMTP.

3. Z čeho se skládá struktura SOAP zprávy?

Struktura SOAP zprávy se skládá z obálky (`Envelope`), která musí obsahovat jeden povinný element tělo (`Body`) a může obsahovat volitelné hlavičky (`Header`) jak je znázorněno na obr. 3.37.



Obr. 3.37: Struktura SOAP zprávy [16]

4. K čemu slouží programovací jazyk WSDL?

WSDL je programovací jazyk webových služeb na bázi XML. Slouží k detailnímu popisu kompletního rozhraní webových služeb, a je tedy prostředkem pro přístup k webové službě. Popisuje mechaniky interakce s konkrétními webovými službami. WSDL je nezávislý na platformě. Primárně slouží pro popis SOAP služeb.

5. Navrhněte vhodné použití webových služeb zařízení EndaceProbe.

Ve vlastní aplikaci pro monitorování sítí, která by mohla být nasazena na jakémkoliv serveru a přistupovala by k webovým službám Endace z vlastního prostředí.

4 ZÁVĚR

V první kapitole této diplomové práce byly popsány používané technologie pro monitorování IP sítí. Byly zde vysvětleny principy detekčních a prevenčních systémů, včetně jejich klíčových vlastností, používaných komponent a popisu tří detekčních technik. Nachází se zde i popis používaných technik monitoringu sítí v dohledových centrech, především monitorování síťových toků a popis protokolu SNMP. První kapitola rovněž obsahuje popis nejpoužívanějších zařízení pro detekci a prevenci narušení včetně dvou programových řešení.

Druhá kapitola se zabývala síťovým rekordérem a analyzátorem firmy Endace. Kromě detailního popisu vlastností tohoto analyzátoru a jeho analytické aplikace EndaceVision jsou v této kapitole dále popsány webové služby, programovací jazyk WSDL a protokol SOAP, který lze použít pro programovatelnou správu tohoto zařízení.

Ve třetí kapitole se nachází praktická část této diplomové práce a byly v ní vytvořeny tři laboratorní úlohy pro detekci provozu a práci se zařízením EndaceProbe, včetně analytické aplikace EndaceVision dle zadání diplomové práce. Součástí první laboratorní úlohy byl i generátor provozu IXIA, který generoval síťový provoz dle nakonfigurovaného testu. V druhé laboratorní úloze byly zahrnuty dva směrovače společnosti Cisco, které sloužily pro nakonfigurování vzdáleného portu směrovače. Součástí třetí laboratorní úlohy byly webové služby zařízení EndaceProbe, programovací jazyk WSDL a použití SOAP protokolu.

Na konci laboratorních úloh se nachází kontrolní otázky pro ověření znalostí získaných během laboratorní úlohy. K laboratorním úlohám jsou vytvořeny i potřebné pokyny pro vyučující a správné odpovědi na kontrolní otázky.

Při práci na třetí laboratorní úloze byl objeven problém s autentizací při volání webových služeb Endace. V dokumentaci společnosti Endace zabývající se SOAP rozhraním, byla tato část nekompletní a bez ní nebylo možné vytvořit autentizované spojení nutné pro volání webových služeb zařízení EndaceProbe. Přes technickou podporu byla kontaktována společnost Endace, ohledně řešení tohoto problému. V termínu dokončení diplomové práce avšak tento požadavek nebyl vyřízen.

Vytvoření laboratorních úloh a ověření funkčnosti jejich konfigurací bylo realizováno v laboratoři transportních sítí VUT Brno. Výsledky praktické části mohou být s přínosem používány ve výuce a na základě třetí laboratorní úlohy bylo vytvořeno řešení, které umožňuje využití webových služeb zařízení Endace v aplikacích webových služeb, které mohou být nasazeny na vzdálených serverech. Tímto řešením lze přistupovat k webovým službám zařízení Endace z vlastních uživatelských prostředí.

LITERATURA

[1] SCARFONE, Karen a Peter MELL. *Guide to Intrusion Detection and Prevention Systems (IDPS)* [online]. Gaithersburg, MD: National Institute of Standards and Technology, 20.2.2007 [cit. 2014-10-18]. Dostupné z: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50951

[2] VYKOPAL, Jan. NetFlow, monitorování IP toků a bezpečnost sítě. In: *Sborník příspěvků z 35. konference EurOpen.CZ, 4.–7. října 2009* [online]. Plzeň: EurOpen.CZ, 2009, s. 63-70 [cit. 2014-10-18]. ISBN 978-80-86583-17-4. Dostupné z: http://www.europen.cz/Anot/35/sbornik.pdf

[3] VYKOPAL, Jan. *NetFlow, monitorování IP toků a bezpečnost sítě* [online]. Ústav výpočetní techniky, Masarykova univerzita, 2009 [cit. 2014-10-18]. Dostupné z: http://www.europen.cz/Proceedings/35/vykopal.pdf

[4] KOŠŇAR, Tomáš. Benefity a úskalí plošného souvislého sledování IP provozu na bázi toků při řešení bezpečnostních hlášení. In: *Sborník příspěvků z 34. konference EurOpen.CZ, 17.–20. května 2009* [online]. Plzeň: EurOpen.CZ, 2009, s. 23-37 [cit. 2014-10-18]. ISBN 978-80-86583-16-7. Dostupné z: http://www.europen.cz/Anot/34/HLAVNI.pdf

[5] *Cisco IOS NetFlow Overview* [online]. Cisco Systems, Inc, © 2004 [cit. 2014-10-18]. Dostupné z: http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_presentation0900aecd80311f57.pdf

[6] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualizované vydání. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.

[7] PATALA, P. *Správa sítí na bázi protokolu IP*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 88 s. Vedoucí diplomové práce doc. Ing. Vít Novotný, Ph.D.

[8] *Nagios: The Industry Standard In IT Infrastructure Monitoring And Alerting* [online]. Saint Paul, MN: Nagios Enterprises, LLC, © 2009-2014 [cit. 2014-10-27]. Dostupné z: http://www.nagios.com/

[9] MONTES, M. Cardenas, E. Perez CALLE a F.J. Rodriguez CALONGE. *Using Nagios for intrusion detetection* [online]. Madrid: CIEMAT [cit. 2014-10-27]. Dostupné z: https://indico.cern.ch/event/0/session/12/contribution/164/material/paper/0.pdf

[10] Network Intrusion Detection Signatures: Part Two. FREDERICK, Karen Kent. *Symantec Connect: All of Connect* [online]. Symantec Corporation, 22.1.2002, 3.11.2010 [cit. 2014-10-27]. Dostupné z: http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-two

[11] *Emulex Corporation* [online]. Costa Mesa, CA: Emulex Corporation, © 2013 [cit. 2014-10-31]. Dostupné z: http://www.emulex.com/

[12] *EndaceProbe™ 7000 Series: Intelligent Network Recorder* [online]. Emulex, ©2014 [cit. 2014-10-31]. Dostupné z: http://www.emulex.com/artifacts/bf4d469c-68ab-4f3b-ba9f-1c0c84fa384e/end_ds_all_endaceprobe_7000.pdf

[13] *EndaceProbe Technical Overview: EDM09-63 - Version 2* [online]. Endace Technology Ltd, © 2010-2012 [cit. 2014-10-31].

[14] Nagios 3.0 Jumpstart Guide For Linux: Overview, Installation and Configuration. NATARAJAN, Ramesh. *The Geek Stuff* [online]. © 2008–2014 [cit. 2014-11-16]. Dostupné z: http://www.thegeekstuff.com/2008/05/nagios-30-jumpstart-guide-for-red-hat-overview-installation-and-configuration/

[15] SOAP: Simple Object Access Protocol. P. PAPAZOGLOU, Mike. *Web Services: Principles & Technology* [online]. Pearson Education, © 2008 [cit. 2014-11-27]. Dostupné z: http://www.cs.colorado.edu/~kena/classes/7818/f08/lectures/lecture_3_soap.pdf

[16] SNELL, James, Doug TIDWELL a Pavel KULCHENKO. *Programming Web services with SOAP* [online]. O'Reilly, 2001, xiii, 244 s. [cit. 2014-11-27]. ISBN 05-960-0095-2. Dostupné z: http://it-ebooks.info/book/316/

[17] Describing Web services. P. PAPAZOGLOU, Mike. *Web Services: Principles & Technology* [online]. Pearson Education, © 2008 [cit. 2014-11-27]. Dostupné z: http://www.cs.colorado.edu/~kena/classes/7818/f08/lectures/lecture_3_wsdl.pdf

[18] *EndaceVision User Guide: EDM09-87 - Version 2* [online]. Endace Technology Ltd, © 207-2013 [cit. 2014-11-29].

[19] Structure of a WSDL Document. *Oracle: Hardware and Software, Engineered to Work Together* [online]. © 1997-2004 [cit. 2014-12-12]. Dostupné z: http://download.oracle.com/otn_hosted_doc/jdeveloper/1012/web_services/ws_wsdlstructure.html

[20] XML Schema Tutorial. *W3Schools Online Web Tutorials* [online]. Refsnes Data, 2015 [cit. 2015-05-23]. Dostupné z: http://www.w3schools.com/schema/default.asp

[21] RFC 2544. *Benchmarking Methodology for Network Interconnect Devices*. IETF, 1999. Dostupné z: http://www6.ietf.org/rfc/rfc2544

[22] *INVEA-TECH: High-Speed Networking and FPGA Solutions* [online]. INVEA-TECH a.s., © 2007 - 2015 [cit. 2015-03-10]. Dostupné z: https://www.invea.com/cs

[23] *Cisco Systems, Inc* [online]. San Jose, USA: Cisco Systems [cit. 2015-03-18]. Dostupné z: http://www.cisco.com

[24] *HP TrippingPoint Provides Next-Generation Network Service: Featuing Analyst Research* [online]. Hewlett-Packard Development Company, © 2014 [cit. 2015-04-06]. Dostupné z: http://www.gartner.com/technology/media-products/pdfindex.jsp?g=hp_sw_vol3_iss1&elq=587368d072744bb09e09f39752afe13a&elqCampaignId=

[25] *HP TippingPoint NX Platform Next Generation Intrusion Prevention Systems: Runs faster than your business* [online]. rev. 3. Hewlett-Packard Development Company, May 2013 [cit. 2015-04-06]. Dostupné z: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-1063ENW.pdf

[26] Intrusion Prevention System: Network Security Platform | McAfee Products. *McAfee: Antivirus, Encryption, Firewall, Email Security, Web Security, Risk & Compliance* [online]. McAfee, © 2014-2015 [cit. 2015-04-06]. Dostupné z: http://www.mcafee.com/uk/products/network-security-platform.aspx

[27] Magic Quadrant for Intrusion Prevention Systems. HILS, Adam, Greg YOUNG a Jeremy D'HOINNE. *Gartner* [online]. 29 December 2014 [cit. 2015-04-06]. Dostupné z: http://www.gartner.com/technology/reprints.do?id=1-26MDU0D&ct=141230&st=sb

[28] *Welcome to NetBeans* [online]. Oracle Corporation, © 2015 [cit. 2015-05-01]. Dostupné z: https://netbeans.org/

[29] IBM Security Network Protection. *IBM: United States* [online]. IBM Corporation, © 2015 [cit. 2015-05-03]. Dostupné z: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=SP&htmlfid=WGD03017USEN

[30] *Snort.org* [online]. 2015. Cisco [cit. 2015-05-10]. Dostupné z: https://www.snort.org/

[31] *SNORT Users Manual: 2.9.7* [online]. 2014. The Snort Project [cit. 2015-05-10]. Dostupné z: https://www.snort.org/documents/1

[32] Gartner Inc.: Technology Research [online]. Gartner, 2015 [cit. 2015-05-23]. Dostupné z: http://www.gartner.com/technology/home.jsp

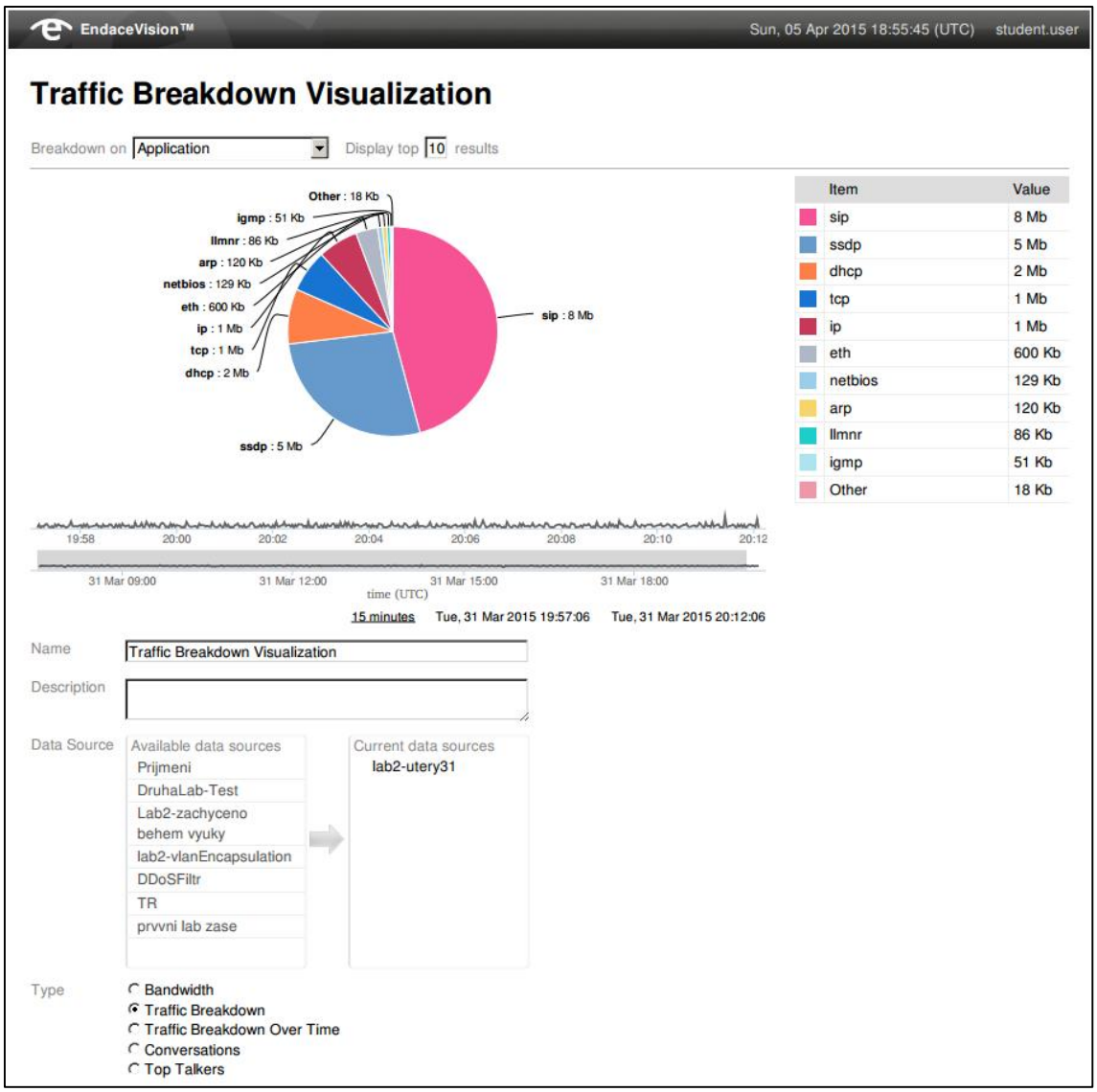
[33] *EndaceProbe and EndaceSensor User Guide: EDM09-10* [online]. Version 50. Endace Technology, 2013 [cit. 2015-05-23].

SEZNAM POUŽITÝCH ZKRATEK

CentOS	Community Enterprise Operating System
DAG	Data Acquisition Generation
DMA	Direct Memory Access
DSCP	Differentiated Services Code Point
FPGA	Field Programmable Gate Array
GPL	General Public License
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention System
MAC	Media Access Control
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NGIPS	Next-generation Intrusion Prevention System
NIC	Network Interface Card
PCAP	Packet Capture
RFC	Request for Comments
RSPAN	Remote Switched Port Analyzer
SFP	Small Form-factor Pluggable
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SIX	Sensor, Information and Communication Systems Research Center
SOAP	Simple Object Access Protocol
SOC	Security Operations Centre
SPAN	Switched Port Analyzer
SSH	Secure Shell
SSL	Secure Sockets Laye
TAP	Test Access Point
TCP	Transmission Control Protocol
TOS	Type of Service
vDAG	Virtual Data Acquisition Generation
VLAN	Virtual Local Area Network
VTP	VLAN Trunk Protocol
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

SEZNAM PŘÍLOH

A VZOROVÝ EXPORT DO PDF SOUBORU Z 2. LAB. ÚLOHY



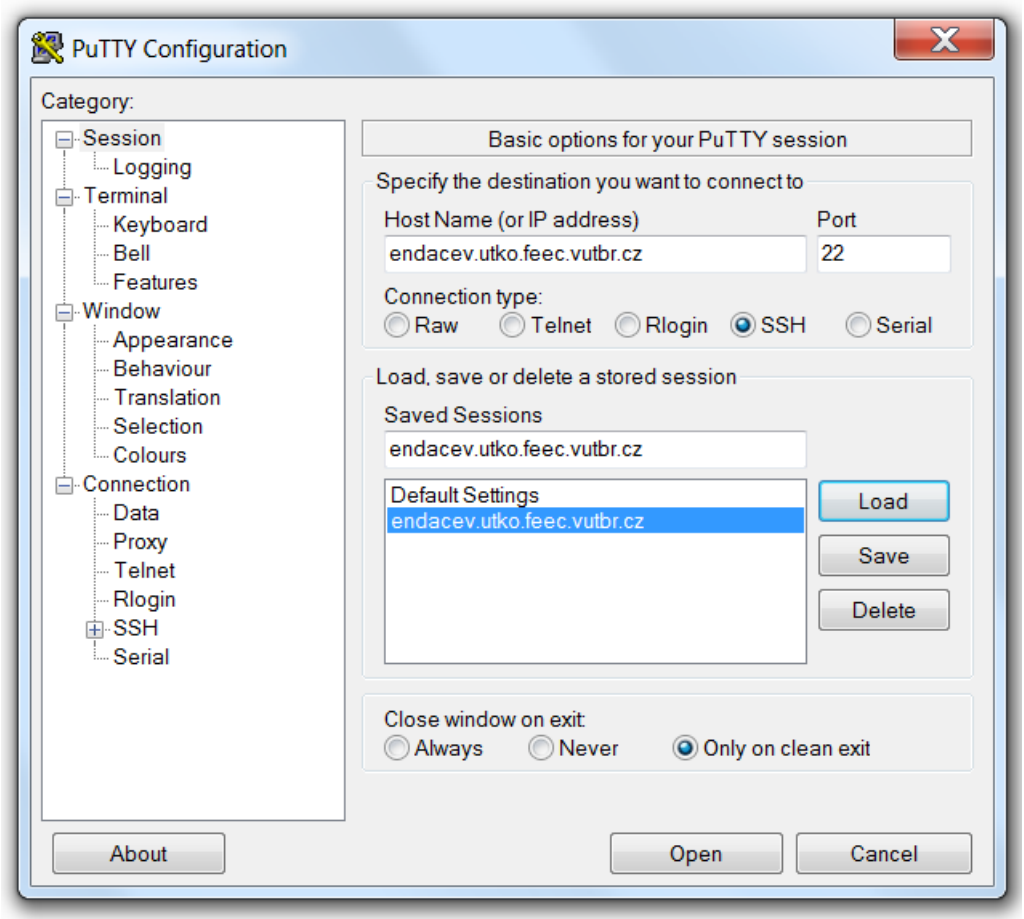
B NASTAVENÍ APLIKACE PUTTY PRO 1. A 2. LABORATORNÍ ÚLOHU

V této příloze se nachází popis nastavení aplikace PuTTY pro vytvoření tunelového připojení ke konfiguraci zařízení EndaceProbe.

V nastavení *Session* použijte následující nastavení:

Host Name: `endacev.utko.feec.vutbr.cz`
Port: `22`

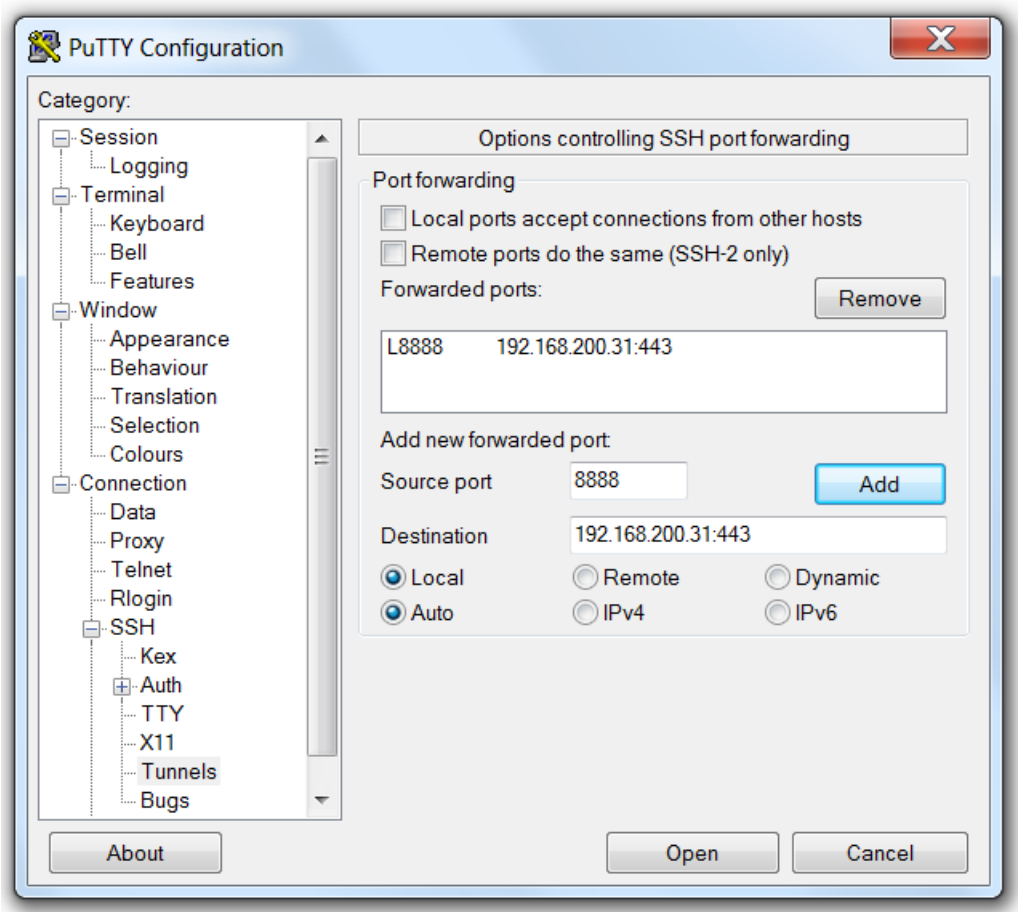
Následně nastavení uložte tlačítkem *Save*.



V nastavení *Connection -> SSH -> Tunnels* zadejte následující nastavení:

Source port: `8888`
Destination: `192.168.200.31:443`

a stiskněte tlačítko *Add*.



Po té se již lze tlačítkem *Open* připojit na nastavený vzdálený server a vytvoří se tunelové připojení.

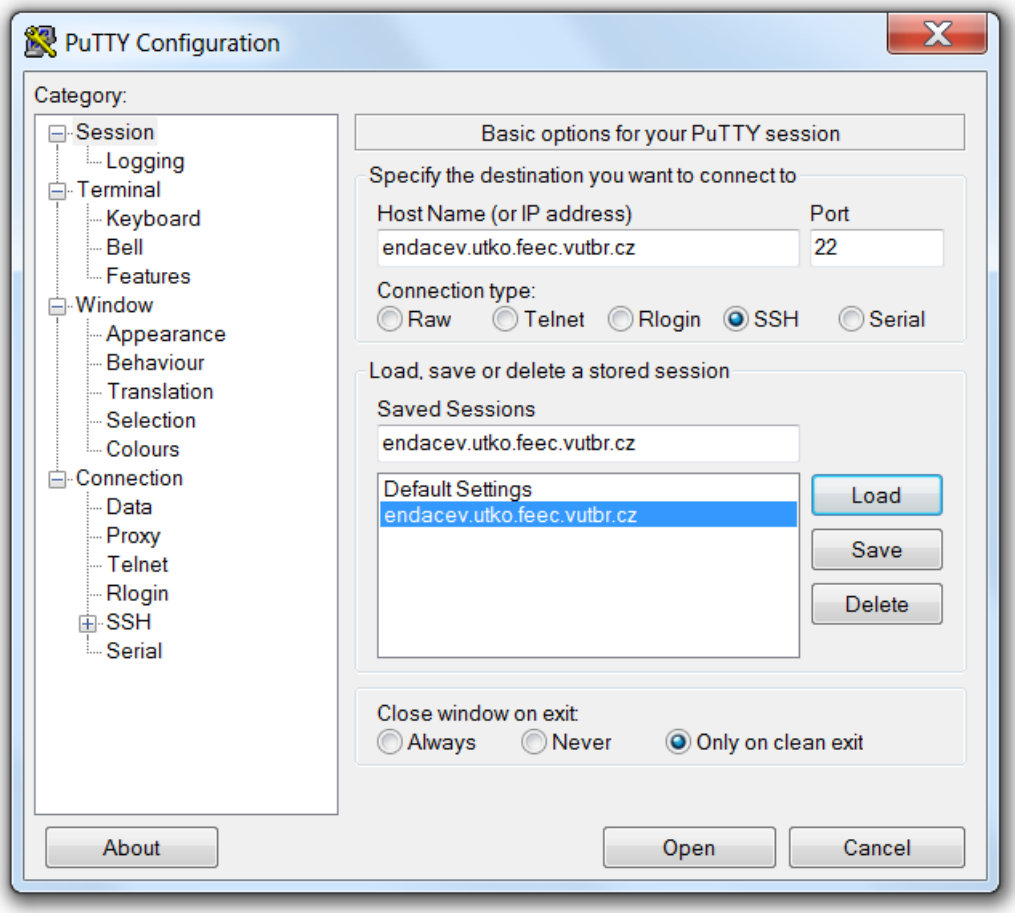
C NASTAVENÍ APLIKACE PUTTY PRO 3. LABORATORNÍ ÚLOHU

V této příloze se nachází popis nastavení aplikace PuTTY pro vzdálené připojení se k virtuálnímu serveru endacev.utko.feec.vutbr.cz na kterém se nachází operační systém CentOS, určený pro práci na laboratorních úlohách.

V nastavení *Session* zadejte do položky:

Host Name: `endacev.utko.feec.vutbr.cz`
Port: `22`

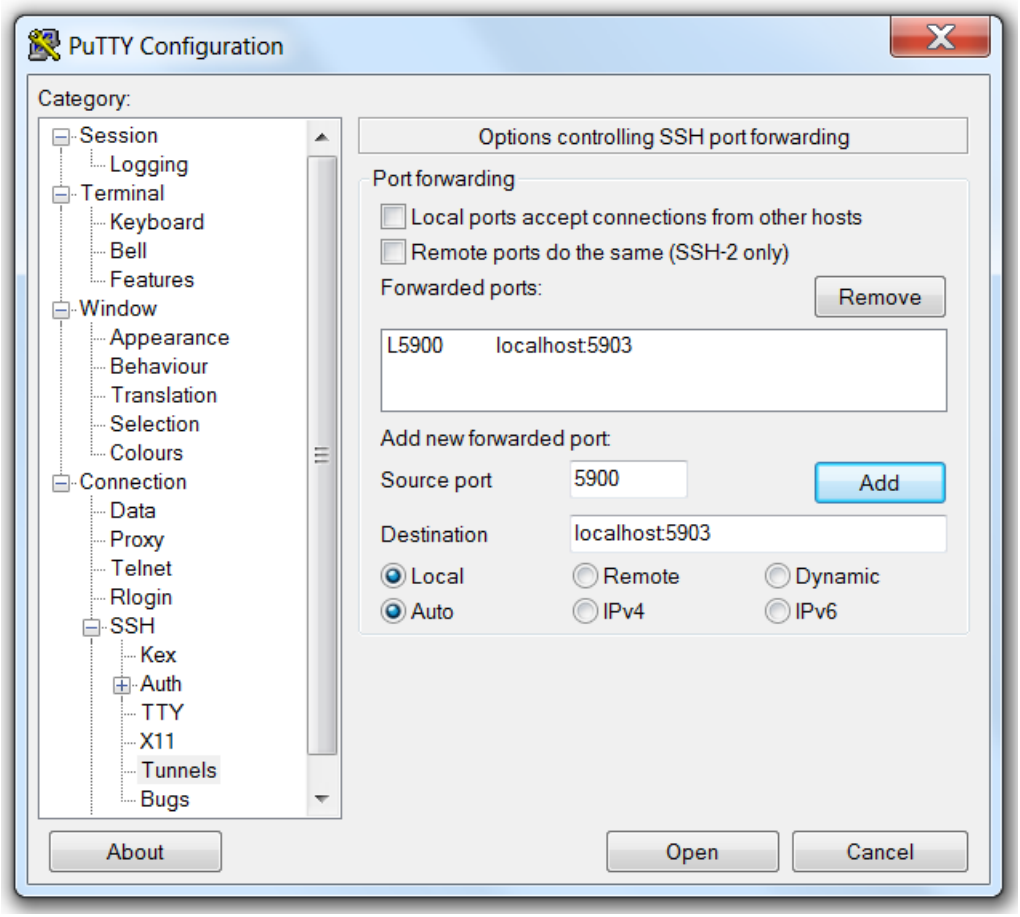
Následně nastavení uložte tlačítkem *Save*.



V nastavení *Connection -> SSH -> Tunnels* zadejte následující nastavení:

Source port: `5900`
Destination: `localhost:5903`

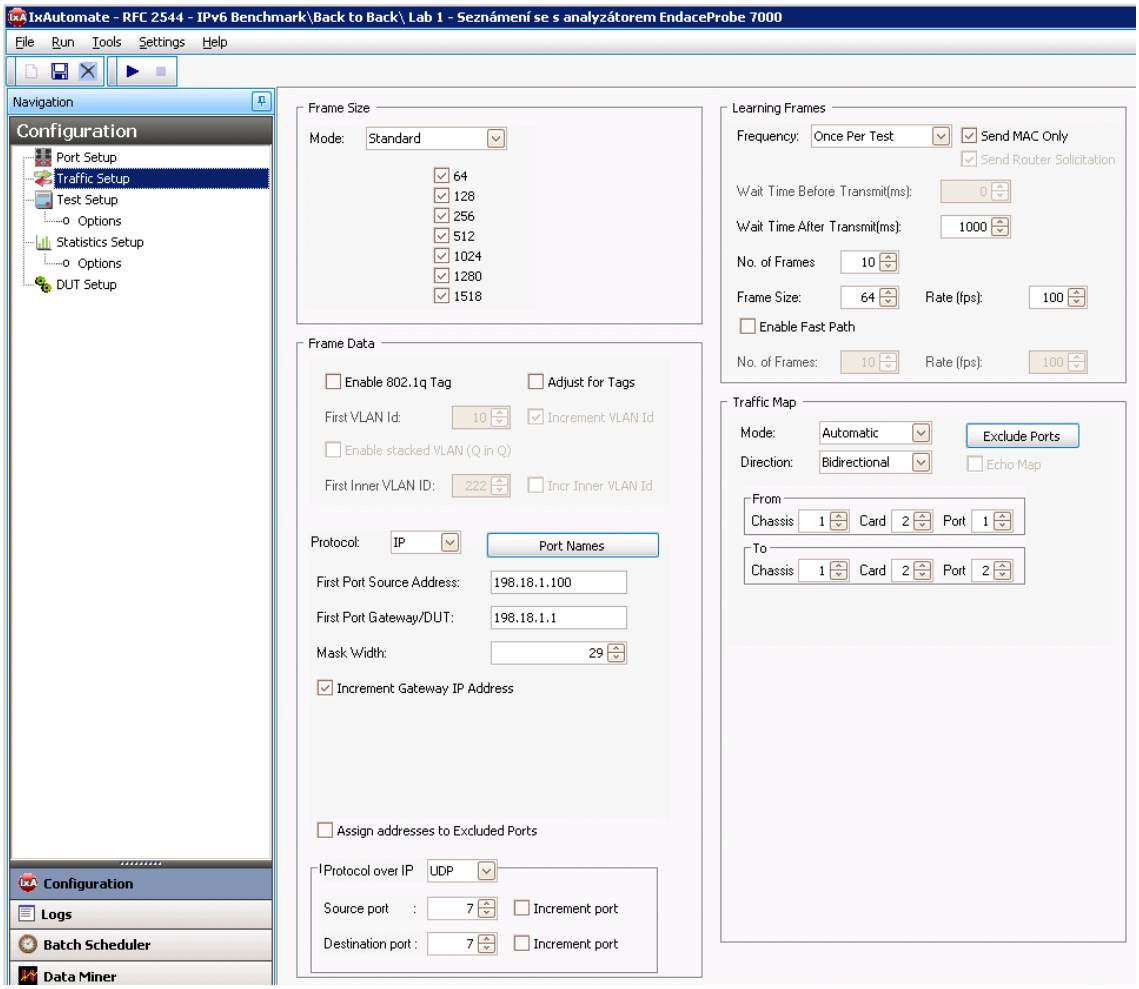
a stiskněte tlačítko *Add*.

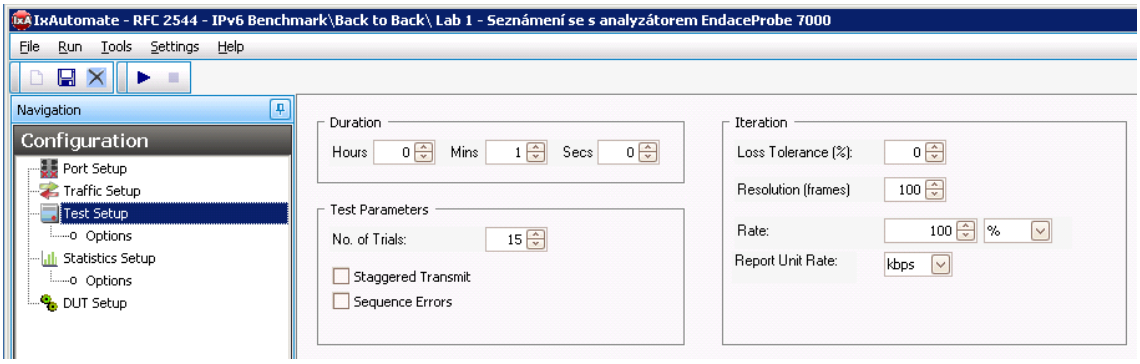


Po té se již lze tlačítkem *Open* připojit na nastavený vzdálený server.

D NASTAVENÍ TESTU NA GENERÁTORU PROVOZU IXIA

Na následujících obrázcích je vidět nastavení testu, který je speciálně nakonfigurován pro 1. laboratorní úlohu. Dané nastavení se nachází i na přiloženém DVD, v souboru určeném pro import do aplikace IxAutomate s názvem „Lab 1 - Seznámení se s analyzátorem EndaceProbe 7000.tcl“.





E OBSAH PŘILOŽENÉHO DVD

- Diplomová práce ve formátu PDF.
- Konfigurační soubor testu pro 1. laboratorní úlohu nazvaný „Lab 1 - Seznámení se s analyzátorem EndaceProbe 7000.tcl“, určený pro import do aplikace IXIA IxAutomate, ve složce „Konfigurační soubor IXIA“
- Vzorová vyexportovaná vizualizace z 2. laboratorní úlohy v souboru „Úloha č. 7 - Vzorovy export do PDF souboru.pdf“
- Vzorový projekt z programu NetBeans z 3. laboratorní úlohy, vyexportovaný v souboru „TretiLabUloha.zip“
- Vlastní WSDL a XSD soubor z 3. laboratorní úlohy, ve složce „WSDL a XSD soubor“
- Všechny laboratorní úlohy v samostatných souborech PDF, připravených pro vytisknutí a použití ve výuce, ve složce „Laboratorní úlohy“.
- Pokyny pro vyučující k laboratorním úlohám v samostatných souborech PDF, ve složce „Pokyny pro vyučující“.