UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Metody řešení problémů v architektuře počítačových sítí s použitím síťového analyzátoru Wireshark

Miloslav Holý

Bakalářská práce
2012

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Miloslav Holý**
Osobní číslo:	**I08055**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Metody řešení problémů v architektuře počítačových sítí s použitím síťového analyzátoru WireShark.**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Práce bude obsahovat popis prostředí a funkcí softwaru WireShark, včetně zdůvodnění výběru tohoto síťového analyzátoru. Zásady tvorby bezproblémových LAN sítí. Časté chyby v sítích LAN, jejich odstraňování a prevence jejich vzniku pomocí síťového analyzátoru. Demonstrace na řešených příkladech. Součástí práce bude návrh metodiky zjišťování topologie sítě, jejího nastavení, zabezpečení a odstraňování problémů za použití Wiresharku.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

SPORTACK, Mark. Směrování v IP sítích. první. Brno : Computer Press, 2004. 351 s. ISBN 80-251-0127-4.
OREBAUGH, Angela , et al. Wireshark a Ethereal : Kompletní průvodce analýzou a diagnostikou sítí. Brno : Computer Press, 2008. 448 s. ISBN :978-80-251-2048-4.
TEARE, Diane . Návrh a realizace sítí Cisco : Autorizovaný výukový průvodce. Brno : Computer Press, 2003. 784 s. ISBN 80-251-0022-7.

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **16. prosince 2011**
Termín odevzdání bakalářské práce: **11. května 2012**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 30. března 2012

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 20. 04. 2012 Miloslav Holý

Poděkování

Na tomto místě bych rád poděkoval své vedoucí bakalářské práce Ing. Soně Neradové za trpělivost a cenné rady. Rád bych také poděkoval své nejbližší rodině za podporu během studia. Mé díky patří také celému IT oddělení SG Equipment Finance, které mi poskytlo mnoho věcných připomínek a prostor na praktické pokusy.

Anotace

Bakalářská práce pojednává nejen o principech zachytávání dat procházejících skrze síť, ale i o jejich analýze. Dále se práce zabývá i následným zpracováním těchto dat. V práci jsou také zmíněny principy a metody návrhu sítě, časté chyby vyskytující se v počítačových sítích a jejich možné řešení.

Klíčová slova

počítačové sítě, síťové analyzátory, problémy v počítačových sítích, řešení síťových problémů, správné postupy řešení problémů, časté chyby v počítačových sítích

Title

Methods for solution of problems in the architecture of computer networks using network analyzer Wireshark.

Annotation

This bachelor work doesn’t describe only principles of capturing data going through network but analysis too. There is also described processing of captured data. In this work are mentioned principles and methods of network designing, common mistakes in computer networks and available solutions.

Keywords

computer networks, network analyzers, problems in computer networks, solutions of problems in computer networks, methods of solving network issues, common mistakes in computer networks

Obsah

Seznam zkratek

DoS	Denial of Service
IP	Internet Protocol
VOIP	Voice over IP
OSI	Open Systems Interconnection
SPAN	Switched Port Analyzer
RSPAN	Remote Switched Port Analyzer
OS	Operating system
MS	Microsoft
USB	Universal serial bus
ASCII	American standard code for information
SMTP	Simple mail transfer protocol
LAN	Local area network
DHCP	Dynamic Host Configuration Protocol
NAS	Network-attached storage
FTP	File Transfer Protocol
DNS	Domain Name System
QoS	Quality of Service
MAC	Media Access Control
RFB	Remote Frame Buffer
POP	Post Office Protocol
IRC	Internet Relay Chat
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
IPSec	Internet Protocol Security
CDP	Cisco Discovery Protocol
VTP	VLAN Trunking Protocol
DTP	Dynamic Trunking Protocol
STP	Spanning Tree Protocol
PAgP	Port Aggregation Protocol

Seznam obrázků

Seznam tabulek

Úvod

Vzhledem k obrovskému rozmachu počítačů v posledních několika desítkách let a potřebě sdílení informací napříč těmito systémy postupně vznikaly různé druhy počítačových sítí. Tyto sítě měly za úkol umožnit jednotlivým systémům přijímat, ale i odesílat informace potřebné k jejich funkci. S vývojem lokálních systémů se rovněž vyvíjejí i počítačové sítě. Díky tomuto vývoji se počítače i počítačové sítě stávají bezpečnějšími, rychlejšími, stabilnějšími a lépe využitelnějšími. Na druhou stranu se stávají komplexnějšími, robustnějšími, složitějšími a především pro člověka špatně srozumitelnými. Tato skutečnost se stane důležitou, pokud se vyskytne problém, či porucha. V podobných situacích je jedním z možných řešení použít síťový analyzátor, podrobně prozkoumat povahu příčiny nefunkčnosti sítě, vyvodit závěry a provést patřičné kroky k nápravě problému.

Nedílnou součástí počítačových sítí je jejich bezpečnost. S ohledem na množství škodlivého softwaru a počtu kybernetických útoků v dnešním světě se síťová bezpečnost stává jedním z nejdůležitějších měřítek kvality počítačových sítí. I v této oblasti má síťový analyzátor svoje místo. Především v odhalování této ilegální činnosti a prevenci proti jejímu vzniku.

Další z oblastí, kde se často dá síťový analyzátor využívat je při výkladu a studiu síťových protokolů, síťového provozu, komunikace apod. Student je seznámen nejen s teorií, ale je mu i demonstrována reálná situace potvrzující nastudovanou teorii.

Práce si klade za úkol poskytnout základní přehled možností a funkcí síťových analyzátorů, vysvětluje jejich princip, hodnotí jejich přínos a možnosti zneužití.

Z počátku je vysvětlena samotná funkce síťového analyzátoru včetně všech jeho částí. Postupně práce popisuje jednotlivé kroky od instalace Wiresharku přes jeho zprovoznění na počítačové síti až k samotnému popisu aplikace. Tyto kroky jsou obohaceny o teorii, díky které lze snadněji pochopit probíranou problematiku. Dále jsou v práci popsány zásady bezproblémových sítí LAN od způsobu návrhu síťového prostředí až po sledování a údržbu. Nedílnou součástí této práce je také další kapitola zabývající se návrhem metodiky pro zjišťování síťové topologie, zabezpečení a nastavení sítě samotné. Následující část obsahuje návrh metodiky řešení vzniklých problémů, kde je v práci rozebráno několik univerzálních metod na řešení problémů. Závěrem je uvedeno několik běžných problémů, které se vyskytují v počítačových sítích. Za pomocí Wiresharku jsou zde vysvětleny jak důvody vzniku problémů, tak i způsoby jejich odstranění.

1 SÍŤOVÉ ANALYZÁTORY

1.1 Pojem síťový analyzátor

Síťový analyzátor je program, nebo zařízení, které je schopno zachytávat informace ze sítě a následně zachycená data dekódovat do podoby srozumitelné lidem podle různých protokolů. Síťového analyzátoru se tedy využívá ke „čtení“, zkoumání a následnému zpracování dat přenášených skrze síť. (1)

1.2 Využití

Funkcí těchto analyzátorů využívají systémoví a síťoví administrátoři, síťoví programátoři, síťoví architekti, atd.

Jejich hlavními funkcemi jsou:

- Převod binárních dat uložených v packetech do lidmi srozumitelné podoby.
- Odstraňování síťových problémů.
- Analýza výkonu sítě.
- Detekce bezpečnostního narušení sítě.
- Zaznamenávání síťového provozu pro pozdější analýzu.
- Analýza a ladění funkcionality aplikací.
- Zjištění podrobností o vniknutí virusu, DoS útoku, či jiných nežádoucích aktivitách.
- Výukový prostředek k porozumění síťových protokolů.

Nutno podotknout, že ačkoliv síťové analyzátory jsou velice užitečnou pomůckou při řešení rozmanitých problémů, mohou se stát značně silnou zbraní v rukou útočníka, či hackera. Možné zneužití analyzátoru se vyskytuje především v oblastech:

- Zachytávání uživatelských jmen a hesel přenášených jako nešifrovaný text.
- Zachytávání a následné přehrávání VOIP telefonátů.
- Získávání citlivých informací (o společnosti, o jednotlivci, …).
- Získávaní informací o síti samotné.

1.3 Jednotlivé části analyzátoru

1.3.1 Hardware

Většina síťových analyzátorů je řešených jako software běžící na standardním operačním systému, využívající síťovou kartu k zachytávání informací. Lze se setkat i se speciálními zařízeními určenými přímo k analýze sítě. Tyto zařízení jsou schopné na rozdíl od softwarových řešení odhalit např. hardwarovou chybu spojení, napěťové výkyvy, apod. V této práci je popsáno pouze využití softwarového řešení.

1.3.2 Ovladač (capture driver)

Nezbytnou částí analyzátoru je ovladač umožňující zachytávání dat. Ten je zodpovědný za samotné zachycení „surových“ dat procházejících sítí a za případnou filtraci, kterou si uživatel navolil. Tyto informace jsou následně uloženy do vyrovnávací paměti.

1.3.3 Vyrovnávací paměť (buffer)

Vyrovnávací paměť zaznamenává zachycená data. Tyto data jsou ukládána tak dlouho, dokud je ve vyrovnávací paměti místo. Alternativní zápis dat po naplnění paměti vyhledává nejstarší záznam a ten přepisuje. Vyrovnávací paměť může být umístěna na pevném disku nebo i v operační paměti počítače.

1.3.4 Analýza v reálném čase

Této analýzy se využívá ke zpracování dat jdoucích přímo ze sítě, tedy v reálném čase.

1.3.5 Dekódování

Komponenta sloužící k „překladu“ informací ze sítě do člověku srozumitelné podoby. Dekódování je pro každý protokol odlišné a každý síťový analyzátor podporuje různé dekodéry.

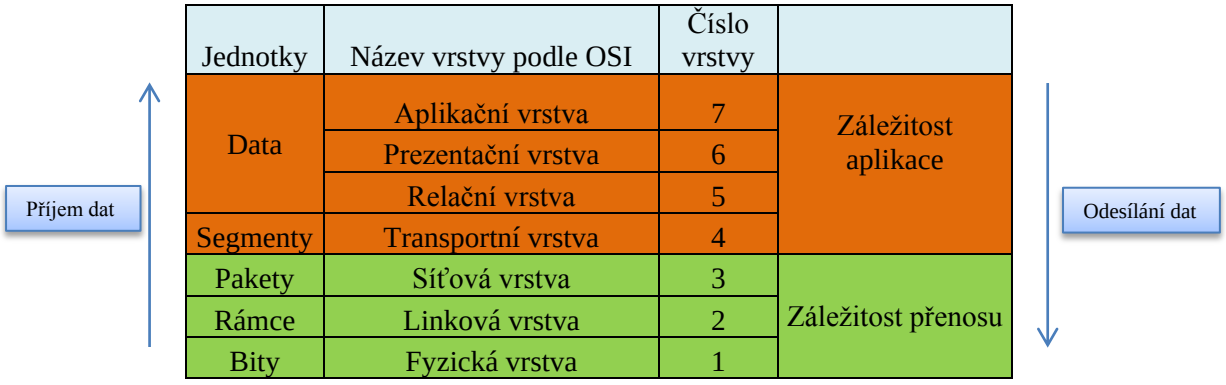
2 ZÍSKÁVÁNÍ PŘÍSTUPU K SÍTI

2.1 OSI model

„Mezinárodní standardizační organizace ISO (Open System Interconnection) vyvinula pro potřeby otevřeného propojování počítačových systémů takzvaný referenční model OSI (Open System Interconnection). Za otevřené propojení systémů považujeme takovou technologii, kterou je možné podporovat i v prostředí složeném ze zařízení různých výrobců. Zmíněný referenční model OSI identifikuje všechny funkce, potřebné pro navázání, používání, definování a zrušení komunikační relace mezi dvěma počítači, a uspořádává je do logicky definovaných vrstev; přitom je nezávislý na výrobci a architektuře propojených počítačů.“ (2)

OSI model se skládá celkem ze sedmi vrstev. Každá vrstva znamená jeden krok k zajištění úspěšného spojení. Vrstvy jsou uspořádány postupně tak, jako probíhá skutečná komunikace. Pro pochopení komunikace v počítačových sítích je tento model stěžejní znalostí. Model OSI je znázorněn v Tabulka 1.

Tabulka 1 – Model OSI



Jednotky	Název vrstvy podle OSI	Číslo vrstvy	
Data	Aplikační vrstva	7	Záležitost aplikace
	Prezentační vrstva	6	
	Relační vrstva	5	
Segmenty	Transportní vrstva	4	
Pakety	Síťová vrstva	3	Záležitost přenosu
Rámce	Linková vrstva	2	
Bity	Fyzická vrstva	1	

2.1.1 Fyzická vrstva

Fyzická vrstva je zodpovědná za přenos samotných bitů po médiu. Nedělá žádné rozhodovací procesy ani data jakkoliv nemění. Pracuje tedy přímo s elektrickými impulzy v případě měděných vodičů, s optickými signály v případě optických vláken, apod. Není zde žádné ověřování vadných dat, to se provádí až na druhé vrstvě modelu OSI. Na první vrstvě modelu OSI pracují huby.

2.1.2 Linková vrstva

Linková vrstva je zodpovědná za platnost přenášených dat. V případě odesílání dat „balí“ požadovaná data do rámců a ty poté putují na fyzickou vrstvu. V případě přijímání data „rozbaluje“ a poskytuje je vrstvě síťové. Na linkové vrstvě standardně pracují switche, z toho vyplývá, že na spojení více počítačů pomocí tohoto zařízení není za potřeby protokolů síťové vrstvy. Vrstva obsahuje kontrolní mechanizmus na ověření integrity dat.

2.1.3 Síťová vrstva

Síťová vrstva není nutnou součástí komunikace. Stává se nezbytnou až v okamžiku komunikace dvou zařízení umístěných v různých sítích nebo u přenosů vyžadující služby této vrstvy. Na síťové vrstvě fungují routery a jedním z nejpoužívanějších protokolů této vrstvy je známý IP. Tato vrstva nemá kontrolu integrity dat, spoléhá se na okolní vrstvy.

2.1.4 Transportní vrstva

Hlavní funkcí transportní vrstvy je ověření integrity dat a seřazení paketů ve správném pořadí k předání další vrstvě modelu OSI. Transportní vrstva bývá úzce spojena s vrstvou relační, podobně jako fyzická s linkovou. Dohromady pak tvoří například známou kombinaci protokolů TCP/IP.

2.1.5 Relační vrstva

Relační vrstva je pátou vrstvou modelu OSI. Zajišťuje synchronizaci a organizaci dialogů relačních vrstev obou systémů. Příkladem je služba QoS.

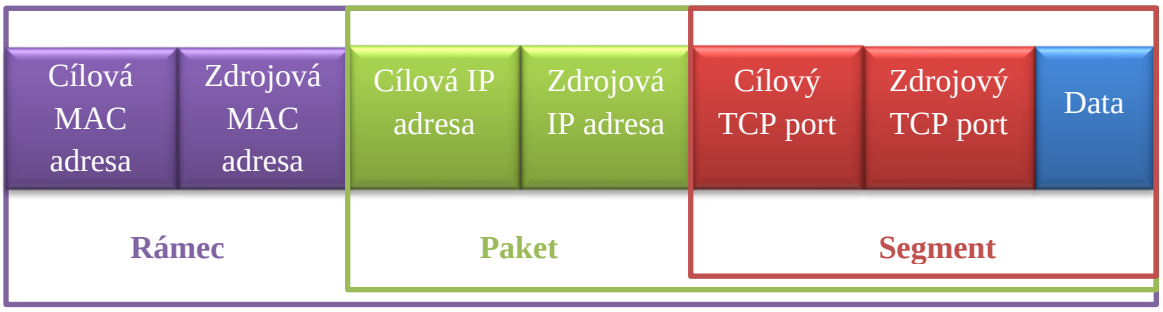
2.1.6 Prezentační vrstva

Prezentační vrstva především zajišťuje převody kódování, může také šifrovat, či dešifrovat služby.

2.1.7 Aplikační vrstva

Aplikační vrstva tvoří rozhraní mezi aplikacemi a síťovými službami. Tato vrstva je na začátku všech komunikačních relací. Aplikace žádající síťovou komunikaci inicializuje protokol vrstvy 7 a tím se vytvoří komunikační relace postupující skrze celý model OSI.

2.1.8 Zjednodušený model „balení“ dat podle OSI



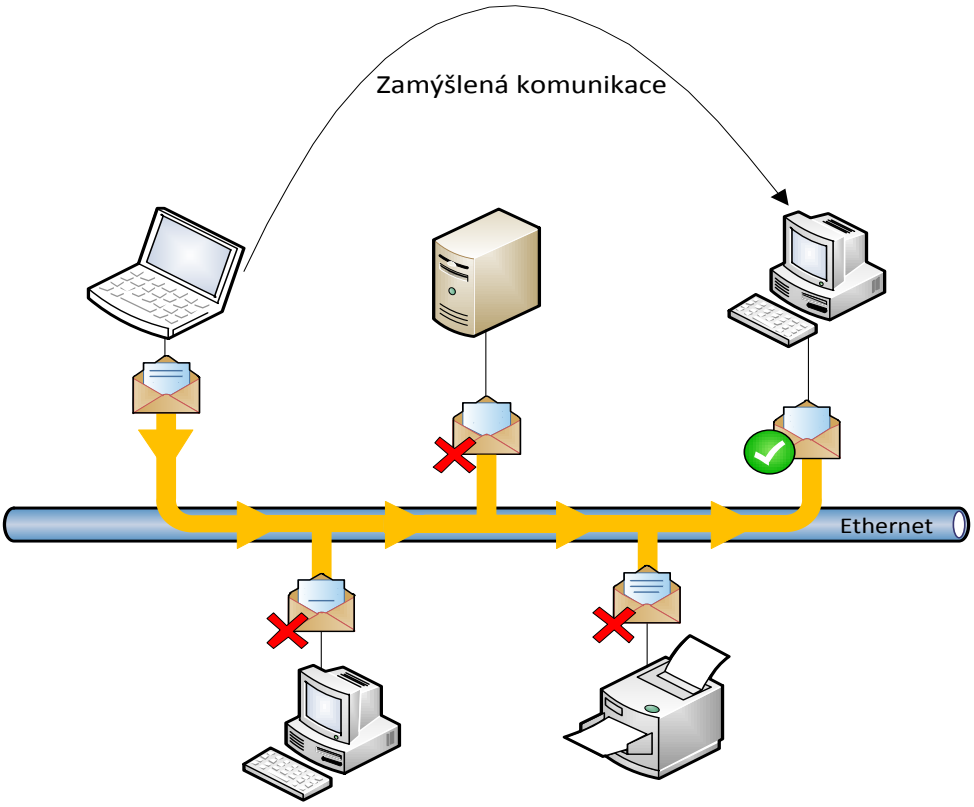
Obrázek 1 – Balení dat podle OSI

2.2 Princip funkce Ethernetu

Ethernet patří k nejrozšířenějším komunikačním protokolům mezi počítači vůbec, princip jeho fungování je založen na médiu, které je sdíleno jednotlivými zařízeními. Tyto zařízení spolu komunikují pomocí všesměrového vysílání. Každé vysílání je tedy směřováno na všechny zbývající zařízení v rámci dané kolizní domény. Přenášené informace jsou z důvodu snadnějšího a bezpečnějšího přenosu rozděleny do několika částí, v případě Ethernetu do rámců. Každý rámec obsahuje hlavičku, v které je uvedena, mimo jiné,

hardwarová adresa cílového zařízení. Přenášená data jsou tedy vyslána v rámci dané kolizní domény na všechna zařízení. Zařízení s adresou, která se shoduje s adresou uvedenou v hlavičce rámce, na vysílání odpoví a data přijme. Ostatní zařízení na úrovni síťového adaptéru data odfiltrují. Nicméně síťový analyzátor je schopen síťovému adaptéru poskytnout speciální ovladač, který jej přepne do promiskuitního módu. V tomto módu je síťový adaptér schopen přijímat data, která nejsou určena jeho adrese.

Následující obrázek (Obrázek 2) znázorňuje síť s komunikačním protokolem Ethernet.

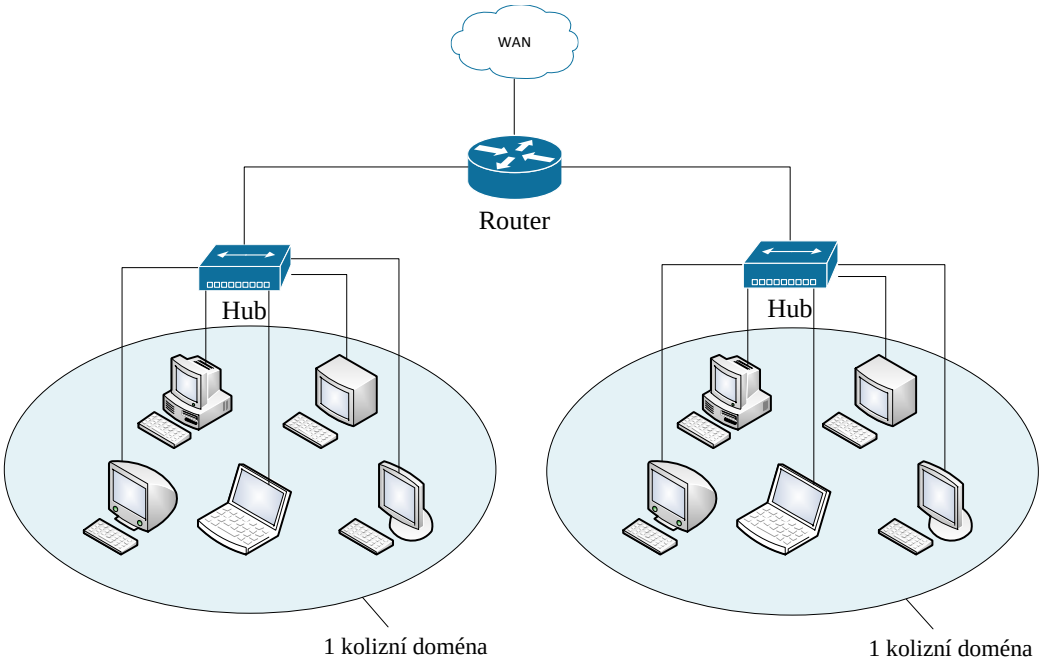


Obrázek 2 – Poslání zprávy prostřednictvím sítě Ethernet v rámci jedné kolizní domény

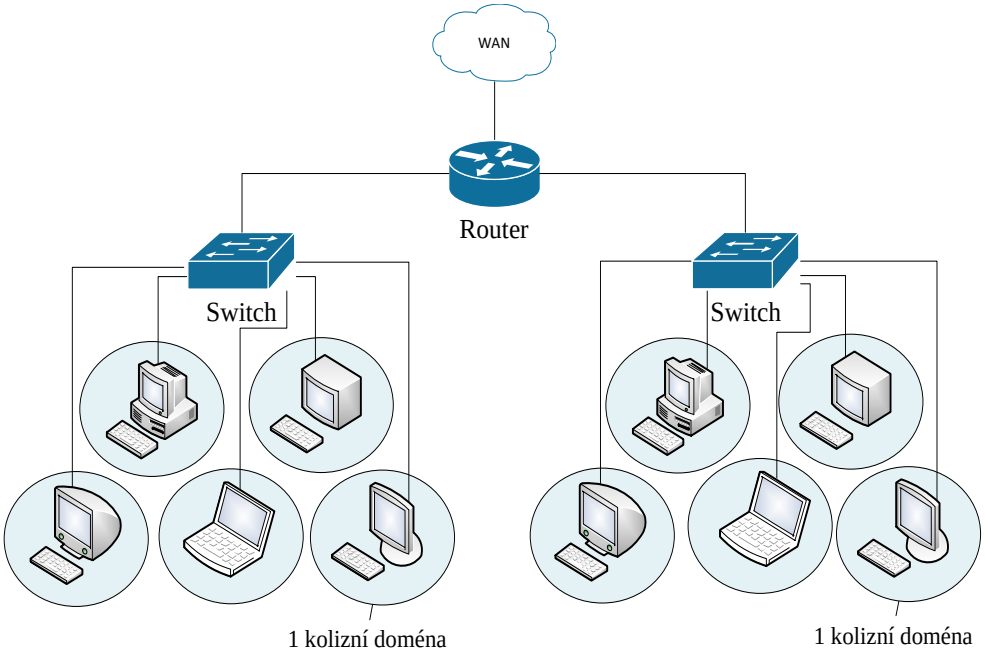
2.3 Kolizní doména

Velikost kolizní domény záleží na síťových zařízeních použitých v síti. Router i switch dělí kolizní doménu sítě na každém svém portu, to znamená, že každý port tvoří jednu kolizní doménu. Hub má na všech portech jednu kolizní doménu.

Na následujících obrázcích (Obrázek 3 a Obrázek 4) je znázorněný rozdíl v použití jednotlivých zařízení.



Obrázek 3 – Tvoření kolizních domén počítačové sítě při využití hubu



Obrázek 4 – Tvoření kolizních domén počítačové sítě při využití switche

Z předchozích obrázků (Obrázek 3 a Obrázek 4) lze vyvodit, že v síti obsahující pouze hub síťový analyzátor zachytí data nejen zařízení, na kterém je nainstalován, ale i data ostatních zařízení. Na rozdíl od sítě se switchem, kde je síťový analyzátor schopen zachytit pouze

data zařízení, na kterém je nainstalován. Tento rozdíl je zapříčiněn filozofií jednotlivých zařízení. Zatímco hub pracuje na první vrstvě modelu OSI a přeposílá přijatou informaci na všechny své zbývající porty bez jakéhokoliv ohledu, switch pracuje na druhé vrstvě OSI a dělá rozhodovací proces založený na zdrojové a cílové MAC adrese, tudíž minimalizuje provoz v síti a doručuje informaci pouze zamýšleným příjemcům.

2.4 Metody připojení síťového analyzátoru do sítě

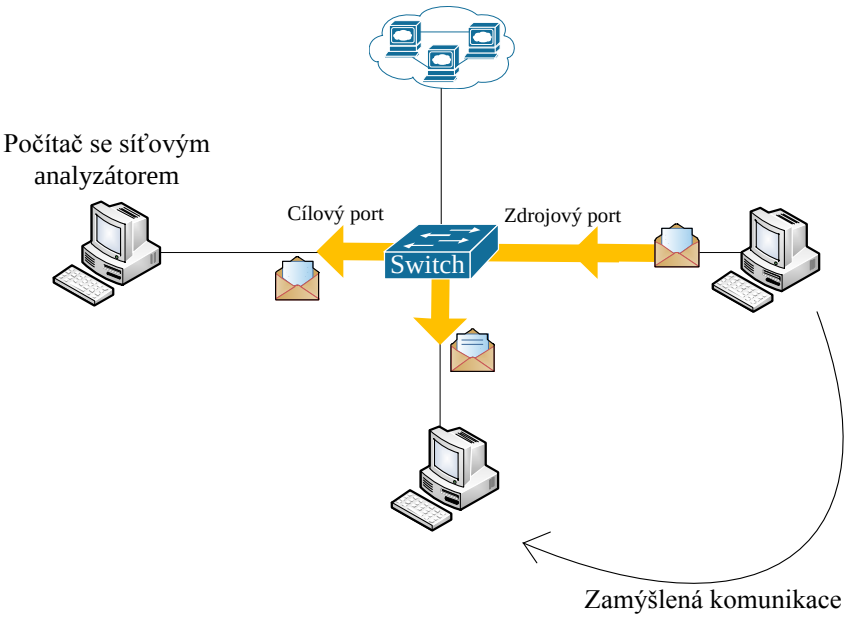
2.4.1 Instalace síťového analyzátoru na konkrétní problémové zařízení

Tato metoda je obvykle nejjednodušší, ale především nejméně vhodná hned z několika důvodů:

- Zařízení nemusí mít podporovaný operační systém, nemusí se vždy jednat o počítač.
- Zařízení nemusí být fyzicky ani vzdáleně přístupné.
- Instalace síťového analyzátoru na koncová zařízení může být v rozporu s firemní politikou.
- Nemusí být vhodné, aby o síťovém analyzátoru věděl uživatel.
- Instalace, popřípadě odinstalace analyzátoru může být časově náročná.

2.4.2 Zrcadlení portů (port mirroring)

Většina dnešních switchů a routerů podporuje funkci zrcadlení portů, která má za úkol umožnit například analýzu dat na zařízeních určitých portů, na částech sítě nebo třeba i na všech zařízeních zároveň. Zrcadlení portů probíhá v rámci jednoho i více switchů, kdy se jeden zdrojový port, více portů nebo celý provoz sítě zrcadlí na cílový port (3). Na tomto cílovém portu lze následně spustit analýzu dat přes síťový analyzátor.



Obrázek 5 – Průběh přenosu informace přes switch se zapnutou funkcí zrcadlení portu

Tato technologie je u zařízení značky Cisco označována jako SPAN pro zrcadlení portů na jednom zařízení. Pokud se data shromažďují z více zařízení zároveň, je tato technologie nazvána RSPAN. V následující tabulce (Tabulka 2) jsou podrobně znázorněny série zařízení firmy Cisco a jejich podpora těchto dvou protokolů.

Tabulka 2 – Přehled podpory protokolů SPAN a RSPAN

Catalyst Switche	SPAN	RSPAN
Catalyst Express 500 / 520	Ano	Ne
Catalyst 6500/6000	Ano	Ano
Catalyst 5500/5000	Ano	Ne
Catalyst 4900	Ano	Ano
Catalyst 4500/4000	Ano	Ano
Catalyst 3750 Metro	Ano	Ano
Catalyst 3750 / 3750E	Ano	Ano
Catalyst 3560 / 3560E	Ano	Ano
Catalyst 3550	Ano	Ano
Catalyst 3500 XL	Ano	Ne
Catalyst 2970	Ano	Ano
Catalyst 2960	Ano	Ano
Catalyst 2955	Ano	Ano
Catalyst 2950	Ano	Ano
Catalyst 2940	Ano	Ne
Catalyst 2948G-L3	Ne	Ne
Catalyst 2948G-L2	Ano	Ano
Catalyst 2900XL	Ano	Ne
Catalyst 1900	Ano	Ne

2.4.2.1 Konfigurace SPAN na zařízeních značky Cisco

Při konfiguraci je nutno vytvořit monitorovací session. Pro SPAN se jedná o jednu session, která obsahuje samotné propojení cílového portu se zdrojovým nebo zdrojovou VLAN. Číslo session, které je nutné zadat, může být 1 až 66. Jako zdroj může být zadáno rozhraní nebo VLAN, případně několik portů či VLAN. Jako cíl lze zadat port nebo skupinu portů. (3)

```
SWITCH(config)#monitor session 1 source interface g1/0/10
SWITCH(config)#monitor session 1 destination interface g2/0/1
```

Standardně se nemonitorují L2 protokoly, jako CDP, VTP, DTP, STP, PAgP. Pakety se také posílají bez informace o zařazení do VLAN. Přeposílání včetně těchto informací lze provést pomocí následujícího příkazu.

```
SWITCH(config)#monitor session 2 destination interface g1/0/5
encapsulation replicate
```

Pokud se sleduje provoz pouze na některých portech, lze jej ještě omezit na určité VLAN následujícím příkazem.

```
SWITCH(config)#monitor session 1 filter vlan 100, 150
```

2.4.2.2 Konfigurace RSPAN na zařízeních značky Cisco

Pro RSPAN je nutné nakonfigurovat jednu RSPAN zdrojovou session, která spojuje zdrojové porty nebo zdrojové VLAN s RSPAN VLAN. A jednu RSPAN cílovou session, která je na jiném switchi a spojuje RSPAN VLAN s cílovým portem.

Nejprve je nutné vytvořit RSPAN VLAN na všech switchích, které se budou účastnit RSPAN. Pro konfiguraci můžeme využít VTP.

```
SWITCH(config)#vlan 999
SWITCH(config-vlan)#name monitoring-rspan
SWITCH(config-vlan)#remote span
```

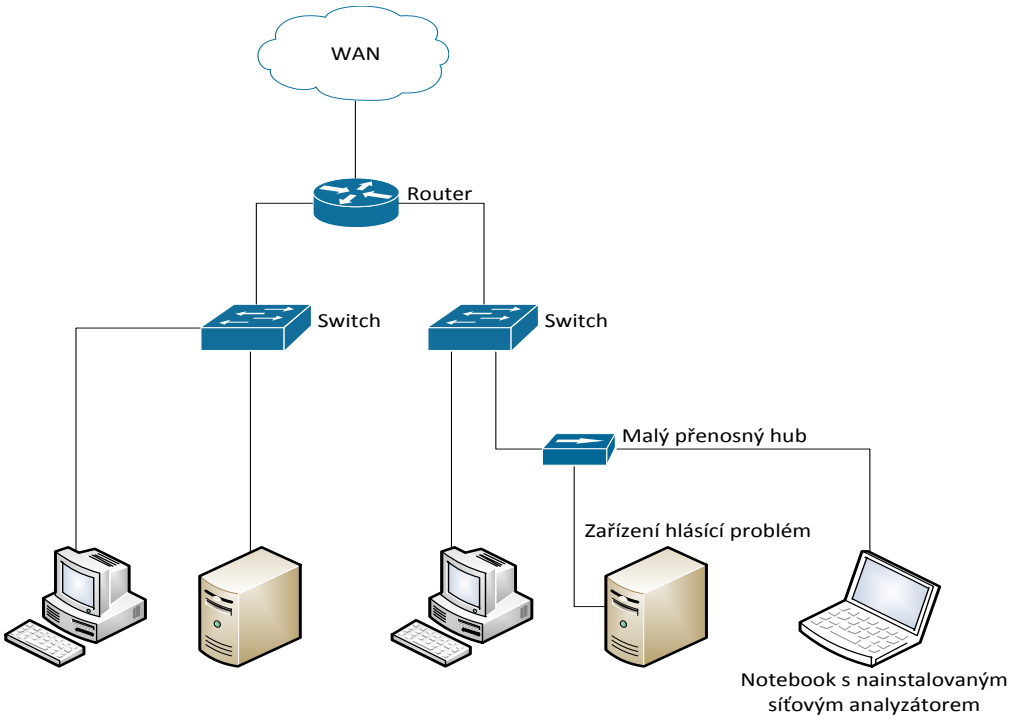
Následně je nutné vytvořit zdrojovou session na zdrojových switchích a cílovou session na cílovém.

```
SWITCH1(config)#monitor session 1 source interface g1/0/10,g1/0/20
SWITCH1(config)#monitor session 1 destination remote vlan 999
SWITCH2(config)#monitor session 2 source remote vlan 999
SWITCH2(config)#monitor session 2 destination interface g1/0/1
```

2.4.3 Přídavný hub jako pomůcka při řešení problémů

Jedna z dalších metod, jak dostávat informace ze sítě, pokud již nějaký problém existuje je s využitím malého hubu. Hub se zapojí mezi zařízení hlásící problém a nejbližší další síťový prvek a do hubu se následně zapojí diagnostická stanice (kvůli mobilitě nejlépe notebook se síťovým analyzátorem), tím se rozšíří kolizní doména a data jsou doručována do všech zařízení připojených do hubu. Umístění hubu a zařízení se síťovým analyzátorem by vždy mělo být co nejblíže k zařízení hlásící problém, aby vyplynul problém z jeho perspektivy. Fyzická vzdálenost v tomto případě není důležitá, jedná se o vzdálenost logickou, neboli síťovou.

Správné zapojení zařízení znázorňuje následující obrázek (Obrázek 6).



Obrázek 6 – Vložení hubu do sítě za účelem rozšíření kolizní domény

Toto řešení je pouze dočasné vzhledem ke snížení výkonnosti sítě a nutnosti síť přepojovat. Mělo by se tedy využívat pouze k řešení konkrétních nebo kritických problémů. Pro místa v síti, která jsou dlouhodobě kritická nebo jiným způsobem často problémová se používají vhodnější zařízení typu TAP. Tyto zařízení jsou v síti umístěné dlouhodobě a jsou konstruované přímo pro účely analýzy dat.

2.4.4 Další metody

Tyto metody nejsou jediné, jak získat přístup k datům zařízení z jiných částí sítě. Existují metody, které nevedou „oficiální“ cestou. Mohou být signálem k napadení sítě a je dobré je znát. Některé z nich jsou popsány dále v kapitole Návrh metodiky zjišťování topologie, nastavení a zabezpečení sítě s využitím Wiresharku.

3 Wireshark

3.1 Vlastnosti, parametry

Wireshark je především díky své podpoře napříč operačními systémy (OS založené na Unixu, Mac OS X, MS Windows) jedním z nejrozšířenějších a nejobsáhlejších síťových analyzátorů vůbec. (4)

- Je šířen jako svobodný software vydaný pod GNU General Public License.
- Obsahuje podporu více než 750 síťových protokolů.
- Umí zachytávat data z médií Ethernet, Token-Ring, 802.11 bezdrátových sítí, apod.
- Umí číst soubory z 25 různých produktů.
- Obsahuje konzolovou verzi zvanou TShark.
- Umí pracovat v promiskuitním i nepromiskuitním módu.

3.2 Instalace

Samotný software je možné stáhnout zdarma díky své licenci přímo na stránkách vývojového týmu[1], kde jsou v nabídce ke stažení verze pro jednotlivé OS.

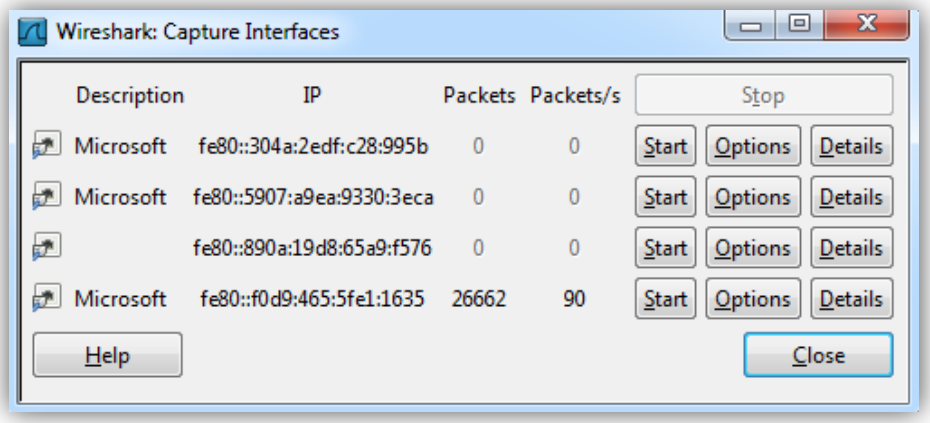
Instalace pod MS Windows probíhá standardně, tedy po stažení instalátoru a spuštění se instalační proces o všechno postará a výstupem se stává funkční program. Na stránkách programu je možné také stáhnout portable verzi, která se nemusí instalovat a lze ji nosit např. na USB klíčence.

Instalace pod Unixem může být provedena například pomocí repozitářů, kde průběh instalace je velice jednoduchý, podobně jako u MS Windows.

3.3 Spuštění

Po spuštění programu je nutné vybrat síťové rozhraní, na kterém bude probíhat analýza dat. Tento úkon se provede buď hned z úvodní obrazovky, nebo přes menu. Zobrazované IP adresy jsou standardně zobrazované ve formátu IPv6, nicméně po kliknutí na nápis se tato adresa zobrazí v čitelnější formě IPv4. Výběr správného síťového rozhraní se dá určit podle názvu, podle IP adresy nebo podle aktivity. Každé síťové rozhraní má ve svém řádku počet právě procházejících a celkový počet obdržených paketů. Samotný dialog výběru rozhraní je zobrazen na Obrázek 7.

[1] Dostupné na: http://www.wireshark.org/download.html

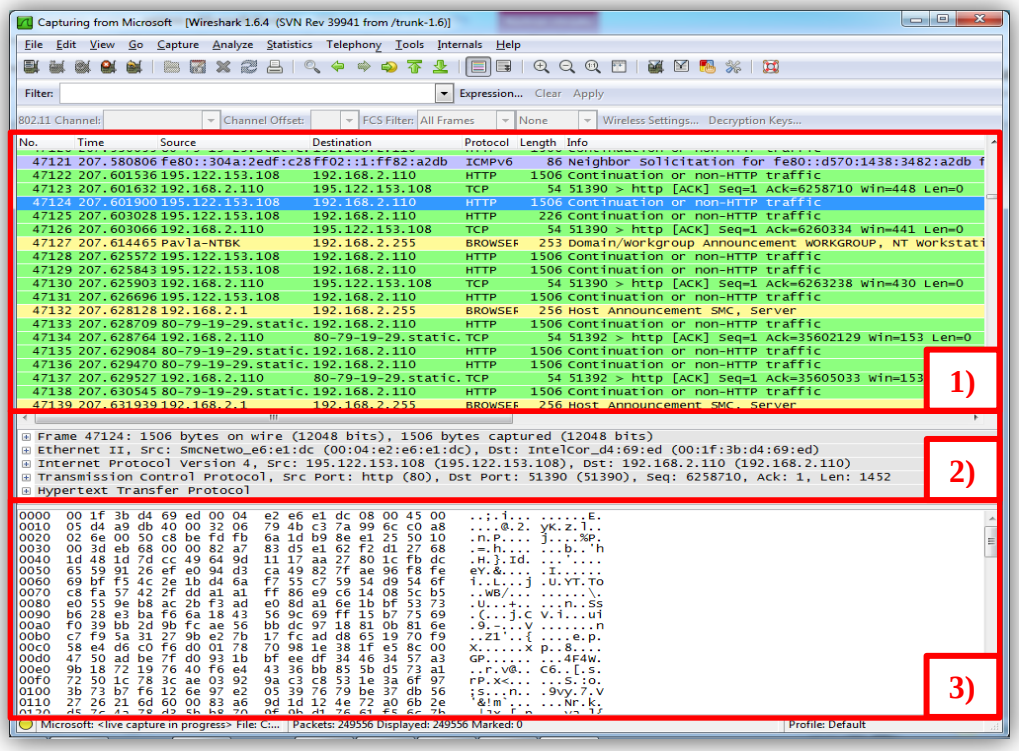


Obrázek 7 – Výběr síťového rozhraní pro analýzu dat

3.4 Grafické prostředí

Grafické prostředí Wiresharku se nijak zvlášť neliší od jiných grafických aplikací, je tedy velice intuitivní a snadno použitelné. Je založeno na třech hlavních sekcích (znázorněno na Obrázek 8):

1) Přehled jednotlivých paketů.
2) Detail vybraného paketu.
3) Dekódovaná data vybraného paketu.



Obrázek 8 – Základní rozložení ovládacích prvků programu Wireshark v MS Windows

Struktura a ovládání těchto tří sekcí programu je stromovitá. V závislosti na výběru jednotlivého paketu v sekci 1 se zobrazí seznam zachycených protokolů v sekci 2. V závislosti na výběru daného protokolu v sekci 2 se zvýrazní příslušná dekódovaná data v sekci 3.

V horní části je ještě klasické menu s velkým množstvím voleb, pod ním se nachází upravitelný panel nástrojů, pole pro zápis zobrazovacího filtru a úplně dole je stavový řádek obsahující informace o zvoleném rozhraní, počtu zachycených paketů a o použitém profilu.

3.4.1 Přehled jednotlivých paketů

Část označená na Obrázek 8 jako „1)“. Zde lze nalézt seznam zachycených paketů. Jeden řádek se rovná jednomu paketu. Ve sloupcích jsou údaje jako: číslo zachyceného paketu, čas zachycení, zdrojová IP adresa, cílová IP adresa, použitý protokol, délka zachycené informace a podrobný popis paketu. Seznam lze třídit podle kteréhokoliv údaje. Tyto sloupce jsou plně přizpůsobitelné a lze je přes nástroje v menu přidávat, odebírat, modifikovat jejich funkci, či měnit jejich pořadí.

3.4.2 Detail vybraného paketu

Část označená na Obrázek 8 jako „2)“. Obsahuje rozbalovací seznam zachycených protokolů daného paketu. Ke každému protokolu jsou po rozbalení zobrazeny všechny zachycené detaily a dostupná data včetně seřazeného seznamu jednotlivých protokolů, jak se v síti vyskytují podle modelu OSI.

3.4.3 Dekódovaná data vybraného paketu

Část označená na Obrázek 8 jako „3)“. Zobrazuje čistě zachycená data bez ohledu na protokol, pokud není kliknuto na daný protokol v sekci se seznamem protokolů. Pokud je kliknuto na protokol v této sekci se zvýrazní část dat, která vybranému protokolu náleží. V levé části této sekce jsou hodnoty vyjádřené hexadecimálně, v pravé jsou převedeny do ASCII.

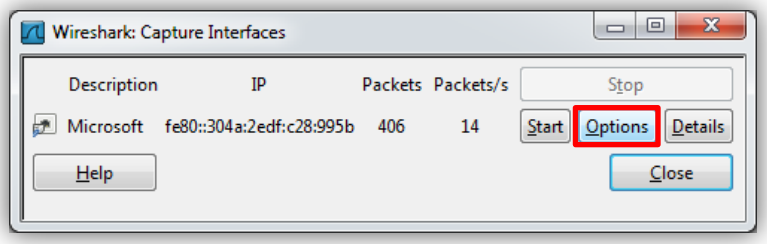
3.5 Filtry

Standardním chováním Wiresharku je zachytávat a zobrazovat veškerá data, která na síťové rozhraní dorazí. Pokud bude analyzátor spuštěný na lehce vytížené domácí síti, nebude pravděpodobně problém s přehledností. Ovšem pokud se vezme v potaz vysoce vytížená páteřní síť, zde bude orientace velice obtížná, ne-li nemožná. Ať už vzhledem k množství paketů, protokolů nebo i k samotné náročnosti na systém. Pro lepší orientaci jsou ve Wiresharku zavedeny dva filtry, pomocí kterých může být síťový provoz redukován. Je jím externí/zachytávací a interní/zobrazovací filtr.

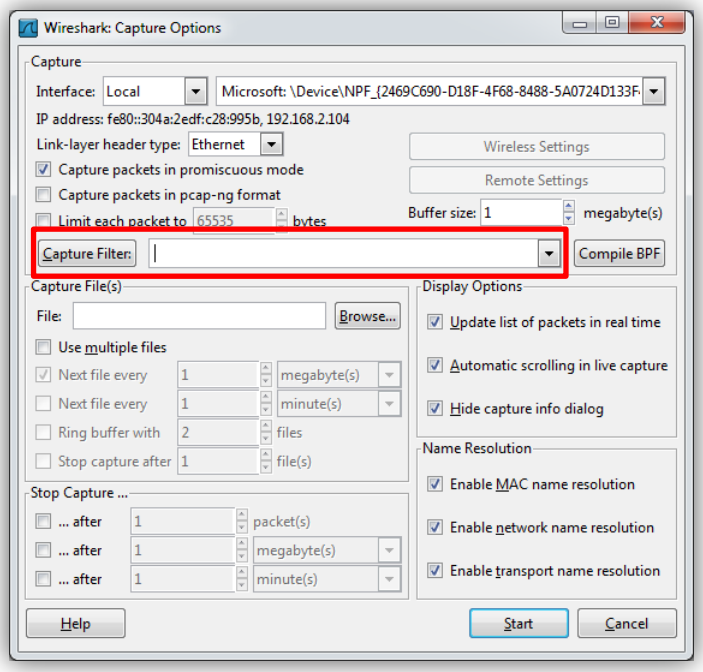
3.5.1 Externí/zachytávací filtr

Externí filtr slouží k omezení množství zachycených dat již na vstupu, to znamená, do aplikace již vyloučená data nedorazí. Tudíž se následně pracuje pouze s touto podmnožinou dat a nelze tedy zpětně pracovat se všemi daty, které byly v danou dobu k

dispozici. Díky tomuto filtru nemusí docházet k takové zátěži na systém a veškerá práce s programem je tím pádem výrazně rychlejší. Tento filtr se definuje v nastavení síťového rozhraní, jak je znázorněno na Obrázek 9 a Obrázek 10.



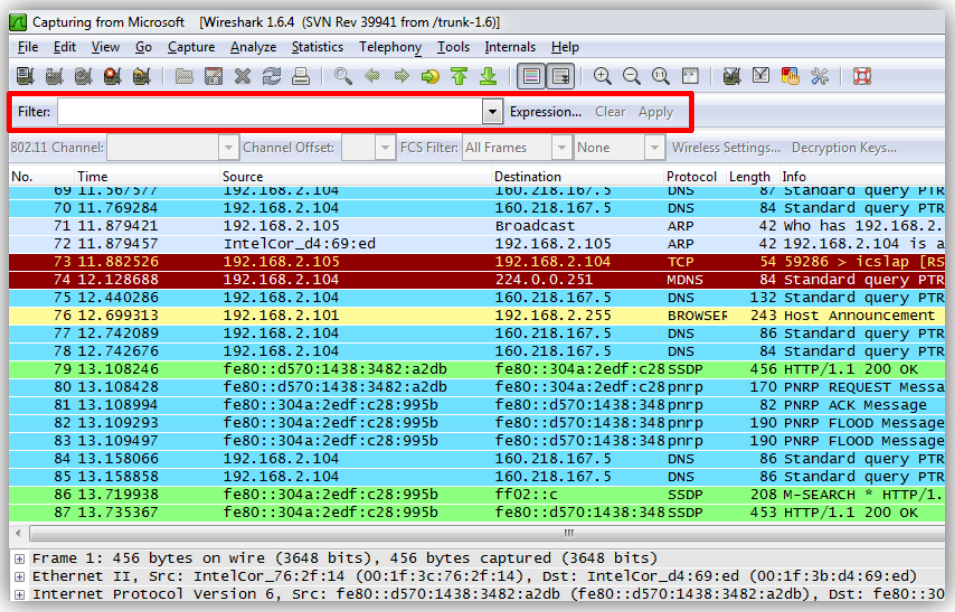
Obrázek 9 – Přístup k externímu filtru



Obrázek 10 – Definice externího filtru

3.5.2 Interní/zobrazovací filtr

Interní filtr slouží k omezení již zachycených dat. K dispozici jsou tedy všechna data, která byla zachycena nebo omezena externím filtrem a na nich lze filtrovat požadované výsledky.



Obrázek 11 – Definice interního filtru

3.5.3 Příklady zápisu interního filtru

Zobrazení všech záznamů se zdrojovou IP adresou 192.168.2.100:

```
ip.addr == 192.168.2.100
```

Zobrazení všech záznamů, které nemají zdrojovou IP adresu 192.168.1.1 a zároveň jsou protokolem SMTP:

```
!ip.addr == 192.168.1.1 && smtp
```

Filtry jsou velice důležitou součástí Wiresharku, kde výrazně zlepšují orientaci v zachycených datech a zrychlují práci s programem samotným. Je tedy dobré jich maximálně využívat.

Důvody, které mohou vést k používání právě Wiresharku:

- je zcela intuitivní,
- přehledný,
- lehce přístupný,
- přenositelný, ale i dostatečně podrobný a v široké škále využitelný.

Dále je výhodou široká podpora síťových protokolů a operačních systémů.

4 Sítě LAN

4.1 Zásady tvorby bezproblémových sítí LAN

Aby počítačová síť byla plně funkční, stabilní a bezproblémová, je nutné dodržovat různé zásady a pravidla již od jejího základu, tedy od jejího budování. Kvůli jednotnosti, vzájemné kompatibilitě i jednoduchosti implementace existují standardy, které říkají, jak mají sítě, všechny jejich prvky a zařízení vypadat, jaké mají splňovat parametry a jak mají být nastaveny. Nezanedbatelnou součástí funkční datové sítě je také její údržba a důsledné sledování.

4.1.1 Návrh

„*Jakýkoliv návrh sítě by měl být standardizovaný proces, který splní alespoň ta nejnižší kritéria na výkon sítě, dá se snadno realizovat i udržovat a počítá s rozumným budoucím rozšiřováním a růstem sítě.*“ (1)

Síťový návrhář navrhující počítačovou síť musí brát v potaz spousty požadavků, kritérií, možných problémů, aby výsledná síť byla funkční a měla všechny náležitosti, které má mít.

Co by si měl síťový návrhář především uvědomit při návrhu bezproblémové počítačové sítě?

4.1.1.1 Rozsáhlost sítě

Rozsáhlost sítě je jedna ze základních informací. Kolik bude potřeba připojit koncových stanic i s rezervou pro budoucnost?

4.1.1.2 Topologie

Zvolení správné topologie je nezbytný krok pro vytvoření silné a stabilní sítě. Implementace záložních spojení, redundancí. Ucelené úvahy nad logickou i fyzickou topologií jsou ve fázi návrhu nezbytné.

4.1.1.3 Rychlost sítě

Rychlost sítě je vlastnost související především s očekávaným druhem využití a rozsáhlostí sítě, popřípadě částí sítě. Zde je nezbytné uvažovat i o aktivních a pasivních prvcích sítě vzhledem k jejich výkonu a šířce pásma.

4.1.1.4 Objekt fyzického umístění sítě

Je nutné zvážit, zda se jedná o nový, či již existující objekt. V obou případech je nutností vlastnit nebo mít přístup k plánům objektu, rozvodům elektřiny apod., a tomu uzpůsobit návrh sítě.

4.1.1.5 Rozpočet

Rozpočet je další z nosných informací, která je předem daná a s kterou se musí síťový návrhář vypořádat. Rozpočet bývá stanoven předem a měl by být dodržen.

4.1.1.6 Technologie

Zvolení správné síťové technologie je stěžejním faktorem, který by měl vyplynout z výše uvedených kritérií. Ve výsledku by tedy mělo být snahou, aby síť splňovala všechny požadované vlastnosti a parametry, nebo je překonávala.

4.1.1.7 Snadnost instalace a údržby

Snadnost instalace má vliv mimo jiné i na celkové náklady na vybudování sítě, snadnost údržby pak na náklady provozu sítě. Obecně tedy platí, že čím je instalace síťových komponent a zařízení snazší, tím je snazší i jejich údržba.

4.1.1.8 Návrh s ohledem do budoucna

Vzhledem k rychlosti vývoje síťových technologií je nutností plánovat síť s ohledem na budoucnost. Potom v rámci pozdějšího upgradu sítě není výměna síťového zařízení takový problém jako případná výměna kompletní kabeláže, která je zabudovaná v podhledech, zdech apod. Z toho důvodu je vhodné kabeláž naddimenzovat, vzhledem k životnosti místa, pro které se síť navrhuje.

4.1.1.9 Výběr komponent a materiálů

Při použití vhodných součástek a správných pracovních postupů síť splní výkonnostní parametry, které se od jejího typu očekávají. (1) Ve spoustě případů výběr komponent ulehčí norma upravující, jak by prvky sítě měly vypadat, jaké parametry by měly splňovat a jak by se měly instalovat.

4.1.2 Zapojení

Počítačová síť se skládá z mnoha prvků a síťové kabely jsou základ, na kterém všechno stojí. Bez správného fyzického zapojení měděných drátů, skleněných optických vláken, konektorů, propojek, propojovacích panelů a různých typů kabelů nebude síť fungovat spolehlivě. (1)

4.1.3 Testování

Žádný návrh ani návrhář není dokonalý. I když při samotné instalaci sítě nedojde k žádnému problému, tak to neznamená, že je vše funkční. Testování a závěrečná validace sítě, je jedním z nejdůležitějších kroků v celém procesu. Je naprostou nezbytností prověřit úplnou funkcionalitu nové sítě a zabezpečit tak bezproblémový start. Testování se může zhostit instalátor, lze jej provést při určité úrovni znalostí svépomocí, dále existují specializované společnosti na testování sítí nebo je možné provést kombinaci předešlých možností. Při samotném testování je často využíváno přístrojů, které jsou schopné mimo jiné měřit např. síťovou propustnost, chybovost, stabilitu nebo zpoždění. Některé přístroje nabízí rozšířené možnosti při samotném odstraňování problémů a chyb. Jedním z nich je testovací, validační a diagnostický nástroj Fluke Networks ES2 EtherScope™ Series II Network Assistant.

Obrázek 12 – Diagnostický nástroj Fluke Networks ES2 EtherScope™ Series II Network Assistant

Zdroj: (5)

4.1.4 Dokumentace

Další fází tvorby bezproblémové sítě je její dokumentace. Nutnost tvorby dokumentace se vyskytuje především u větších a komplexnějších sítí, kde v případě problému není jednoduché dohledat problémový uzel nebo zařízení. Dokumentuje se a zaznamenává úplně každý prvek, který se v síti vyskytuje. Běžnou praktikou je přidělování jednoznačného kódu, který posléze pomáhá s orientací.

4.1.5 Sledování a údržba

Avšak úspěšným zprovozněním sítě a dokumentací práce nekončí, spíše naopak. Síť stejně jako jakýkoliv jiný stroj, systém, či zařízení potřebuje pravidelnou údržbu. Existují spousty automatických činností pro sledování provozu sítě, které dokáží včas odhalit problémy, ke kterým se schyluje. Popřípadě zpětně poskytnout data, pomocí kterých lze vyčíst např. příčiny již vyskytlého problému a předejít tak jeho vzniku v budoucnu. Sledování sítě je doporučeno i z hlediska bezpečnosti. Může tak dojít k odhalení různých druhů útoků, pokusů o útok a dalším podezřelým aktivitám na síti.

5 Návrh metodiky zjišťování topologie, nastavení a zabezpečení sítě s využitím Wiresharku

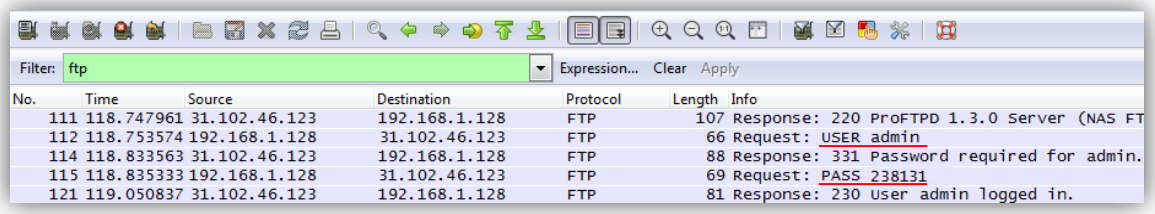
Vezme-li se v potaz již existující síť, nejde zpravidla jen o to ji udržovat funkční, ale jistě také o bezpečnost, kompatibilitu a do jisté míry i prevenci. Pokud je člověk postaven před již existující síť a dokumentace je neúplná, chybná nebo neexistuje vůbec je zapotřebí zjistit o síti co možná nejvíce informací. Dalším důvodem ke shromažďování informací o síti může být například ověřování správnosti již existující konfigurace.

5.1 Zjišťování topologie sítě

Obecná snaha při umisťování síťového analyzátoru za účelem zjištění topologie by měla směřovat k centrálním prvkům sítě. Samozřejmě pokud není známa ani přibližná topologie nejde určit nejlepší začátek. V takovém případě musí být začátek vybrán náhodně. Po spuštění síťového analyzátoru by mělo být zřejmé, v jak velkém síťovém segmentu se analyzátor nachází. Po zaznamenání zachycených informací by měl další krok směřovat k prvnímu centrálnímu prvku. Pokud je zde použit např. hub veškeré informace síťový analyzátor již zachytil. Pokud je použit switch, nejlepším následujícím krokem je nastavení zrcadlení veškerého datového provozu na port, kde je zapnutý analyzátor. Tímto způsobem se získají informace o dalších uzlech sítě. Lze takto pokračovat prvek po prvku a zjišťovat veškeré informace o síti, nebo lze, pokud to zařízení podporují, nakonfigurovat vzdálené zrcadlení portů. U zařízení Cisco se tato technologie jmenuje RSPAN. Za pomocí speciální VLAN si zařízení vzájemně předávají „zrcadlená“ data, tyto data jsou pak předány na jeden či více portů. Zde by měl běžet síťový analyzátor zachytávající veškerý provoz.

5.2 Zjišťování zabezpečení a nastavení sítě

Síťová bezpečnost je jedním z hlavních pilířů správně fungující sítě. Za pomocí Wiresharku lze poměrně snadným způsobem zjistit úroveň zabezpečení sítě jako takové. V dobře zabezpečené síti by nemělo být možné zachytit síťovým analyzátorem jakákoliv data, která by byla jednoduše čitelná. V případě protokolů, které přenášejí informace jako prostý text je možné s Wiresharkem zachytit data včetně hesel a jiných citlivých informací. Z těchto důvodů by se tyto protokoly měly používat pouze k přenosu dat, která nebude moci potenciální útočník zneužít. Jedním z nezabezpečených protokolů je například FTP. Přihlášení do FTP ve Wiresharku je zobrazeno na Obrázek 13 – Zobrazení protokolu FTP ve Wiresharku.



Obrázek 13 – Zobrazení protokolu FTP ve Wiresharku

Další nezabezpečené protokoly například jsou:

- Telnet,
- RFB,
- POP3 (může být zabezpečen),
- SMTP (může být zabezpečen),
- HTTP,
- IRC.

Existují i zabezpečené protokoly, jako například:

- SSH (SFTP),
- SSL/TLS (HTTPS),
- IPSec,
- OpenVPN.

Hlavní pointou síťové bezpečnosti tedy je:

1. Nedovolit útočníkovi se do sítě vůbec dostat.
2. Pokud se do sítě dostane, poskytovat mu pouze šifrovaná data, která není schopen „přečíst".
3. Co nejdříve si útočníka všimnout a podniknout patřičné kroky k jeho odstranění.
4. Poučit se z nastalé situace a zamezit jejímu opakování.
5. Zdokumentovat vzniklou situaci pro pozdější užití.

5.3 Detekce síťového analyzátoru na síti

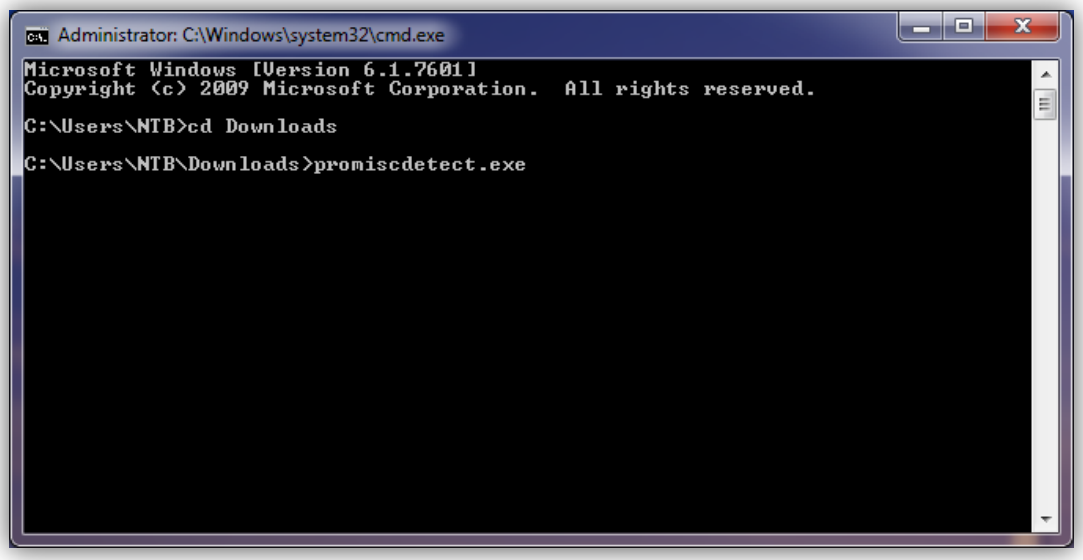
Pokud má síťový administrátor podezření, že je jím spravovaná síť „odposlouchávána" cizím analyzátorem, tudíž že na některém ze zařízení běží síťový analyzátor nebo jiný software ilegálně sbírající data o síti, tak existuje několik způsobů odhalení takovéto činnosti. Je potřeba si uvědomit, že analýza je pouze pasivní činnost. Síťový analyzátor není navržen, aby měnil, či jinak upravoval přenášená data. Je tedy jeho jedinou činností zaznamenávání informací, a to ho činí hůře odhalitelným.

5.3.1 Promiskuitní mód

První a nejjednodušší metoda je ověření síťového rozhraní podezřelého zařízení. Jedním ze základních jevů běžících analyzátorů je, že přepínají síťový adaptér do promiskuitního módu. Tato skutečnost se dá zjistit v Unixu za pomocí příkazu ifconfig.

```
[root@localhost root]# ifconfig -a
eth0 Link encap:Ethernet HWaddr 00:02:B3:06:5F:5A
inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
RX packets:204 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:46113 (45.0 Kb) TX bytes:5836 (5.6 Kb)
Interrupt:11 Base address:0x1800 Memory:e8120000-e8120038
```

MS Windows v základu žádnou funkcionalitu pro zjišťování stavu adaptéru neobsahují, je tedy nutné použít dodatečný program. Například konzolovou aplikaci PromiscDetect[2]. Aplikace je distribuovaná jako freeware a k používání není nutná instalace. Spouští se přímo v příkazovém řádku zadáním cesty ke staženému souboru. Spuštění je znázorněno na následujícím Obrázek 14.



Obrázek 14 – Spuštění aplikace PromiscDetect

Po spuštění této aplikace se na obrazovce okamžitě objevuje, v jakém módu běží síťová karta.

```
C:\Users\NTB\Downloads>promiscdetect.exe
PromiscDetect 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/promiscdetect/
Adapter name:
- Intel(R) PRO/100 SP Mobile Combo Adapter
Active filter for the adapter:
- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a
member of)
- Broadcast (capture broadcast packets)
- Promiscuous (capture all packets on the network)
WARNING: Since this adapter is in promiscuous mode there could be a
sniffer running on this computer!
```

Nicméně některé analyzátory jsou schopné skrytím příznaku o promiskuitě utajovat svoji přítomnost. Další z možností skrývání analyzátoru může být nahrazení příkazu na výpis podrobností o síťových adaptérech (ifconfig, iwconfig) tak, že bude zobrazovat útočníkem chtěný výstup namísto skutečného (1).

[2] Ke stažení na: http://ntsecurity.nu/toolbox/promiscdetect/

5.3.2 Monitoring DNS a ICMP

Další metoda je založena na principu funkce analyzátoru. Pokud je analyzátor nastaven tak, aby překládal IP adresy na DNS jména, bude se pravděpodobně dost často dotazovat na velké množství IP adres DNS serveru. Stejně tak je podezřelá aktivita, kdy je při odhalování topologie používán příkaz ping na celý rozsah příslušné podsítě. Tyto činnosti lze monitorovat a být tak včas upozorněn.

5.3.3 Sledování prostředků

Pokud je síť větších rozměrů nebo je hojně využívaná, zaznamenávání veškerých dat bude náročné nejen na výkon procesoru, ale bude také vyžadovat spoustu místa na místním úložišti. Sledováním těchto prostředků lze tedy také vysledovat nežádoucí analyzátor.

5.3.4 Reset paket u promiskuitního módu

Za normálních okolností síťový adaptér filtruje pakety, které neodpovídají MAC adrese přístroje. V promiskuitním módu některé systémy odpovídají na takový paket reset paketem. Za pomocí velkého množství těchto reset paketů pak lze usoudit, že se pravděpodobně jedná o nežádoucí analyzátor.

5.4 Získávání přístupu přes switch

Každý port switche znamená jednu kolizní doménu. To zlepšuje nejen propustnost, ale především i bezpečnost sítě samotné. Existují techniky, které umožňují přístup do jiných částí sítě přes switch i bez technologie jako je například zrcadlení portů. Tyto techniky jsou zneužitelné potenciálními útočníky, je tedy velmi vhodné je znát a rychle tak umět určit zda se jedná o cílený útok, či nikoliv.

5.4.1 Zahlcení switche

Tato technika využívá vlastnosti některých switchů při jejich zaplnění adresní tabulky. Toho je docíleno posláním velkého množství podvrhnutých MAC adres útočníkem. Po úplném zaplnění adresní tabulky se switch začíná chovat jako hub a útočník se tak dostává ke všem částem sítě. (4)

5.4.2 Podvrhnutí MAC adresy

Pokud se útočníkovi podaří zjistit MAC adresu nějakého zařízení připojeného do stejného switche, je schopný předstírat, že on je dané zařízení. Změnou MAC adresy zajistí, aby switch vložil tuto informaci do své adresové tabulky a začal přeposílat informace určené jinému zařízení útočníkovi. Původní zařízení lze vyřadit například DoS útokem, či podobnými. Tuto záležitost lze vyřešit pevným přiřazením MAC adres k portům switchů. Nevýhodou tohoto řešení je především následné omezení přenositelnosti zařízení v síti. Administrátor je tak často nucen udělat určitý kompromis a volit kombinaci těchto možností. (4)

5.4.3 ICMP oznámení

Tyto oznámení říkají počítačům, které routery mají využívat pro jejich komunikaci. Útočník je schopen poslat podobné oznámení tvrdící, že on je daný router. Díky tomuto

činu veškerá komunikace, která za normálních okolností směřuje za pomoci routeru ze sítě ven, je nyní přesměrována na útočníka. (4)

5.4.4 ARP přesměrování

Pokud počítače snažící se o vzájemnou komunikaci nemají ve svých adresových tabulkách adresy svých protějšků je před komunikací zapotřebí obdržet MAC adresu druhé strany. Stane se tak posláním ARP dotazu. Tato žádost je všesměrová, tzn., obdrží ji všichni, kteří jsou připojeni do stejného switche. Útočník v tomto případě využívá tohoto ARP dotazu, při kterém se vydává za místní router nebo jinou entitu v síti, jež by mohla obdržet cenná data. Po této události se pokusí všechny ovlivněné počítače odeslat svoje informace přímo na zařízení útočníka. (4)

6 Metody řešení síťových problémů

Celkový model řešení jakéhokoliv problému se obecně skládá ze tří základních částí. A to:

- Nahlášení, popř. zjištění problému.
- Diagnóza problému.
- Odstranění problému.

V případě komplexních systémů, rozsáhlých sítí nebo složitých konfigurací bývá velmi náročnou složkou právě diagnóza a odhalení problému způsobující potíže. Následující metody diagnózy lze aplikovat na téměř jakýkoliv problém. Nicméně nelze obecně říci, která z metod je nejlepší. Velmi důležitou roli při výběru vhodné metody zde hrají zkušenosti člověka řešící problém. Při nevhodně zvolené metodě se může řešení celého problému až několikanásobně protáhnout.

Výhodou dodržování těchto postupů je jejich systematičnost. V případě dlouhého pátrání po problému je jasné, co už bylo zkoušeno a co nebylo. V případě více lidí hledající jeden problém, je snazší koordinace a rozdělování úkolů mezi nimi (5).

6.1 Přístup „odshora dolů“

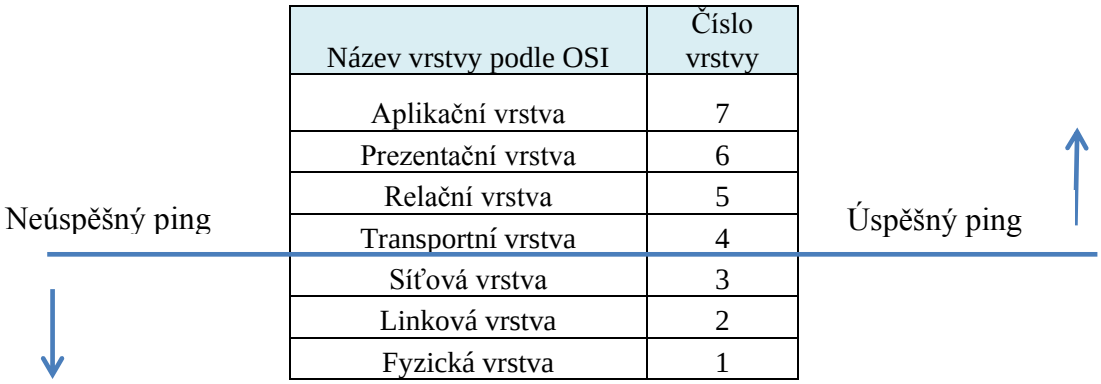
Tento přístup je založen na modelu OSI. Jak název sám napovídá, začíná se s nejvyšší vrstvou modelu a postupuje se směrem k nižším vrstvám, dokud se nenarazí na problém. Příklad řešení může být od kontroly nastavení aplikace hlásící nefunkčnost až po analýzu Ethernetového rámce ve Wiresharku nebo fyzickou kontrolu zapojení, kabelů a jiných prvků počítačové sítě.

6.2 Přístup „odspoda nahoru“

Tato metoda je přesným opakem předcházející. Tudíž se začíná na nejnižší vrstvě modelu OSI a pokračuje se směrem vzhůru.

6.3 Přístup „rozdělit a dobýt“

Přístup „rozdělit a dobýt“ je založen na rozpůlení modelu OSI a pokračování směrem, ve kterém se vyskytuje problém (5). V případě neznalosti přibližné lokace problému s ohledem na model OSI, je tato metoda z hlediska času řešení problému vhodnější než předešlé metody. Jako příklad lze uvést test za pomocí příkazu ping. Pakliže je ping, využívající protokol ICMP na třetí vrstvě modelu OSI v pořádku, je zjevné, že se problém nachází ve vyšších vrstvách, tedy 4-7. V opačném případě je nutné hledat příčinu problému ve vrstvách 3-1.



Název vrstvy podle OSI	Číslo vrstvy
Aplikační vrstva	7
Prezentační vrstva	6
Relační vrstva	5
Transportní vrstva	4
Síťová vrstva	3
Linková vrstva	2
Fyzická vrstva	1

Obrázek 15 – Příklad použití metody „rozdělit a dobýt"

6.4 Přístup „následování cesty dat“

Další z metod funguje na principu následování cesty dat způsobujících problémy. Tato metoda je dobře uplatnitelná např. při problémech v síti, kdy se testuje komunikace mezi jednotlivými zařízeními. Jde se tedy po směru toku dat a zjišťuje se kam až je spojení v pořádku. Vyřazovací metodou se poté určí vadný prvek.

6.5 Přístup „porovnávání konfigurací“

Metoda porovnávání konfigurací je založena na porovnávání funkčních částí prvků sítě s identickými protějšky. Pokud existují například dva identické routery, jeden vykazuje problémy a druhý funguje spolehlivě, jedna z možností odstraňování problémů je porovnání jejich konfigurace a vyvození patřičných závěrů.

6.6 Přístup „záměny komponent“

Přístup záměny komponent pracuje s myšlenkou postupné výměny jednotlivých prvků systémů. Lze tedy výměnou jednotlivých kompatibilních prvků sledovat, zda problém ustal, či nikoliv. Příkladem může být výměna síťového kabelu za jiný.

7 Časté chyby v sítích LAN a řešení za pomocí síťového analyzátoru Wireshark

S pomocí Wiresharku lze řešit mnoho rozmanitých problémů. V této části práce je demonstrativně vybráno několik běžných situací, ve kterých bude provedena identifikace problému a návrh řešení za pomocí síťového analyzátoru Wireshark. Některé problémy lze řešit i jinými způsoby, nebo dokonce i bez Wiresharku. Hlavní výhoda při řešení pomocí analyzátoru však spočívá v pochopení problému, proč a kde k němu dochází, v jakém protokolu, kdy ho lze očekávat a podobně. Je tedy pochopena i podstata problému, nejen pouhý fakt.

7.1 Problém č. 1

Situace:

Existují 2 počítače. Jsou propojené na přímo, bez centrálního prvku. Propojovacím kabelem je kroucená dvojlinka. Kabel je koncipovaný jako křížený. Wireshark po filtraci na protokol ARP zobrazuje víceméně stále stejný záznam.

119	24.008288	Dell_5d:11:f4	Broadcast	ARP	42 Who has 169.254.102.214? Tell 0.0.0.0
122	25.008353	Dell_5d:11:f4	Broadcast	ARP	42 Who has 169.254.102.214? Tell 0.0.0.0
126	26.008401	Dell_5d:11:f4	Broadcast	ARP	42 Who has 169.254.102.214? Tell 0.0.0.0
168	27.293285	Dell_81:e2:c9	Broadcast	ARP	60 Who has 169.254.238.215? Tell 0.0.0.0
182	28.291665	Dell_81:e2:c9	Broadcast	ARP	60 Who has 169.254.238.215? Tell 0.0.0.0
191	29.290103	Dell_81:e2:c9	Broadcast	ARP	60 Who has 169.254.238.215? Tell 0.0.0.0

Obrázek 16 – Výstup z Wiresharku

Problém:

Nefunguje vzájemná komunikace. Počítače se navzájem nevyhledají.

Příčina:

Ačkoliv pro tuto komunikaci není nutný protokol IP, jeho špatná konfigurace může působit problémy. V tomto případě je zapnuta volba automatického obdržení adresy ze serveru DHCP, který v této síti neexistuje. Lze si všimnout, že na Obrázek 16 je IP a všesměrová adresa z implicitního rozsahu, ty jsou nastavovány systémem v případě nemožnosti obdržet správná data ze serveru DHCP. Z výstupu poskytnutého Wiresharkem je vidět, že počítače ani nejsou schopné vytvořit základní vzájemnou komunikaci mezi sebou založenou na protokolu ARP.

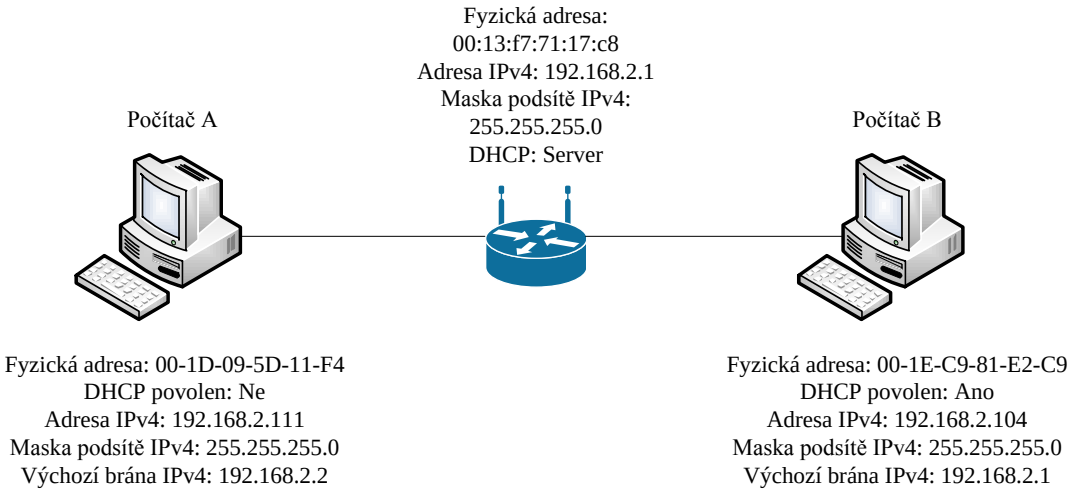
Řešení:

Řešením je tedy manuální nastavení správných IP adres ze správných podsítí, nebo vypnutí protokolu IP.

7.2 Problém č. 2

Situace:

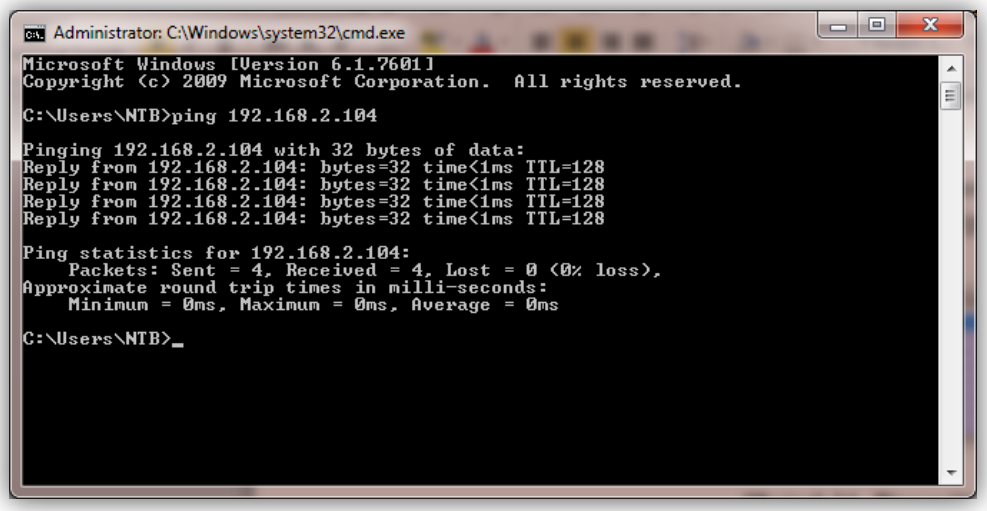
Existuje počítač A a počítač B. Jsou vzájemně propojené skrze router. Oba počítače jsou připojené do routeru kroucenou dvojlinkou, která koncipována jako nekřížená. Oba počítače při dotazu ping na router dostanou odpověď. Schéma zapojení včetně konfigurace je zobrazeno na Obrázek 17.



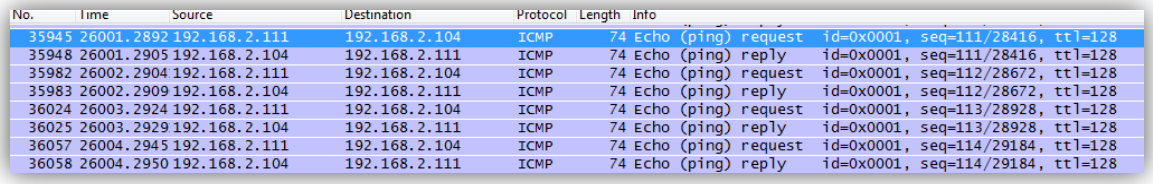
Obrázek 17 – Síťový diagram – zapojení sítě

Problém:

Počítač A dostane odpověď od počítače B na požadavek ping, nicméně počítač B nedostane odpověď od počítače A.

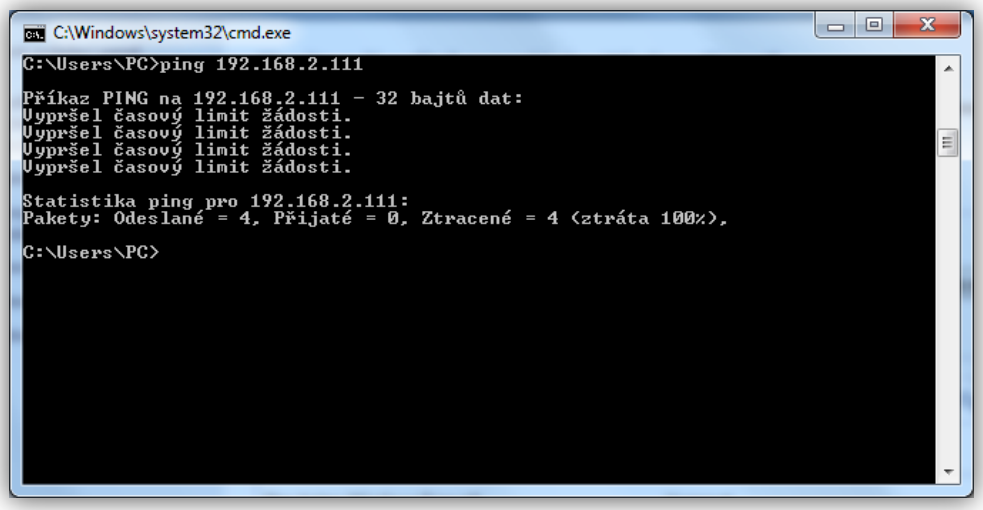


Obrázek 18 – Úspěšný ping počítač A > Počítač B – příkazový řádek

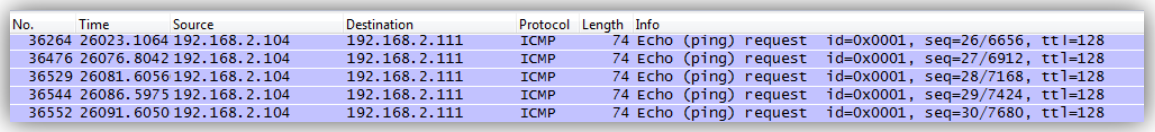


No.	Time	Source	Destination	Protocol	Length	Info
35945	26001.2892	192.168.2.111	192.168.2.104	ICMP	74	Echo (ping) request id=0x0001, seq=111/28416, ttl=128
35948	26001.2905	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) reply id=0x0001, seq=111/28416, ttl=128
35982	26002.2904	192.168.2.111	192.168.2.104	ICMP	74	Echo (ping) request id=0x0001, seq=112/28672, ttl=128
35983	26002.2909	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) reply id=0x0001, seq=112/28672, ttl=128
36024	26003.2924	192.168.2.111	192.168.2.104	ICMP	74	Echo (ping) request id=0x0001, seq=113/28928, ttl=128
36025	26003.2929	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) reply id=0x0001, seq=113/28928, ttl=128
36057	26004.2945	192.168.2.111	192.168.2.104	ICMP	74	Echo (ping) request id=0x0001, seq=114/29184, ttl=128
36058	26004.2950	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) reply id=0x0001, seq=114/29184, ttl=128

Obrázek 19 – Úspěšný ping počítač A > počítač B – Wireshark



Obrázek 20 – Neúspěšný ping počítač B > počítač A – příkazový řádek



No.	Time	Source	Destination	Protocol	Length	Info
36264	26023.1064	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
36476	26076.8042	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128
36529	26081.6056	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128
36544	26086.5975	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128
36552	26091.6050	192.168.2.104	192.168.2.111	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128

Obrázek 21 – Neúspěšný ping počítač B > počítač A – Wireshark

Příčina:

K tomuto chování dochází, protože počítač A má špatně nakonfigurovanou výchozí bránu. Každý příkaz ping se skládá z požadavku a z odpovědi. V případě pingu z počítače A na počítač B se odezva zobrazí, protože počítač B má správně nastavenou výchozí bránu a odpověď se tedy zašle na správnou adresu. Pokud je ovšem ping z počítače B na počítač A, požadavek dorazí na počítač A (jak je vidět na Obrázek 21), ale již není známa cesta zpět, respektive je špatná, proto počítač B nezobrazí žádný výsledek.

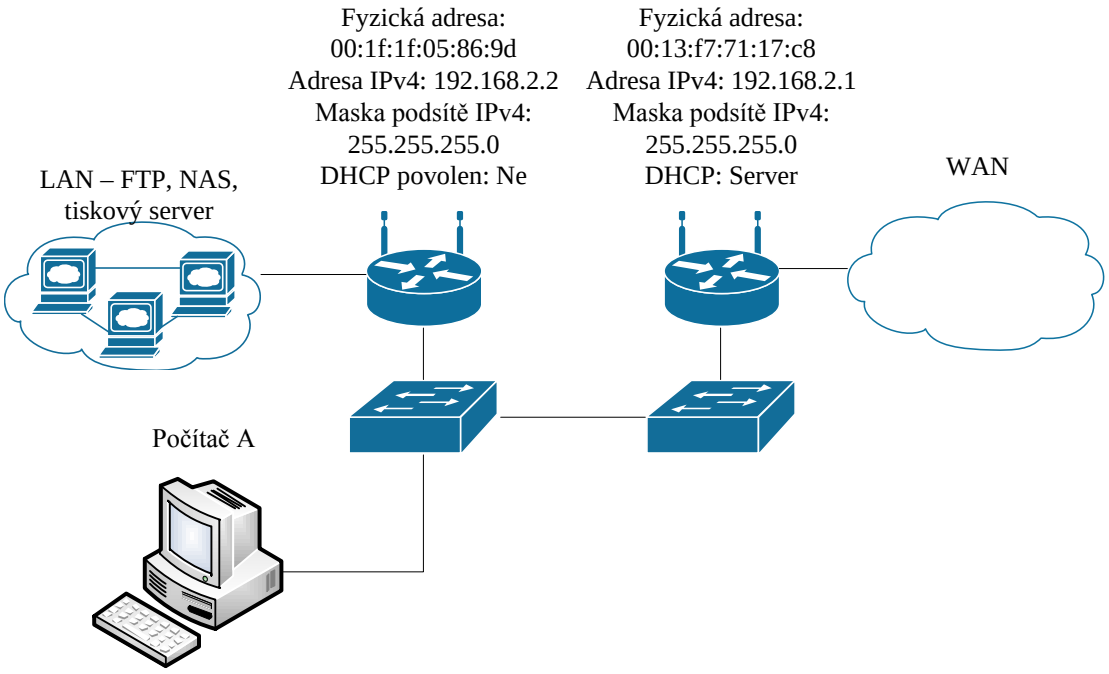
Řešení:

Konfigurace výchozí brány počítače A na hodnotu 192.168.2.1.

7.3 Problém č. 3

Situace:

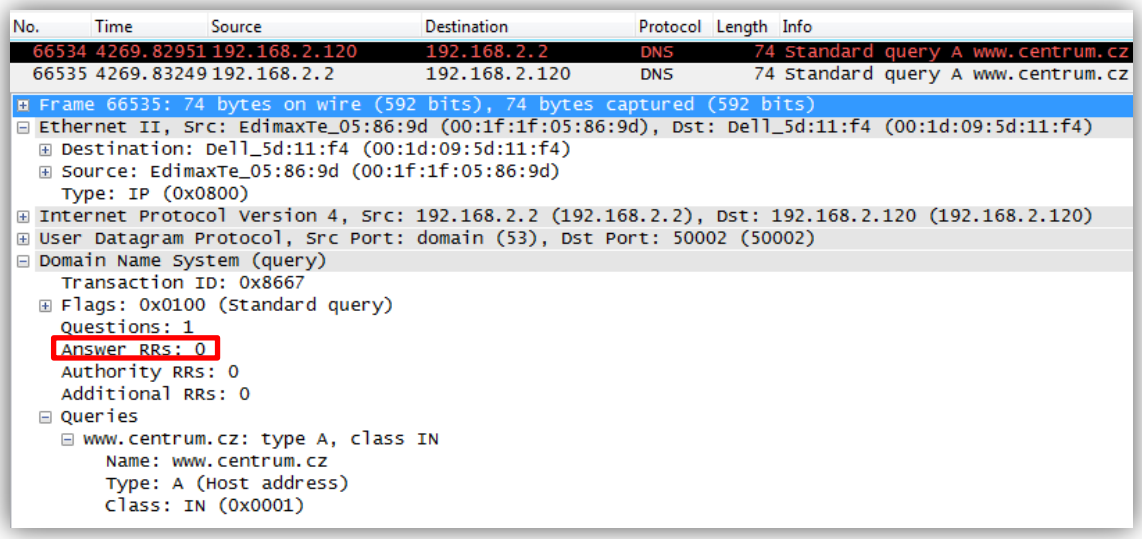
Existuje počítač připojený do existující sítě. Propojovacím kabelem je kroucená dvojlinka. Kabel je koncipovaný jako nekřížený.



Obrázek 22 – Síťový diagram – zapojení sítě

Problém:

Počítač A dostane odpověď na dotaz ping od všech prvků sítě, má vzájemnou konektivitu s místními zařízeními. Přístup na Internet však nemá.



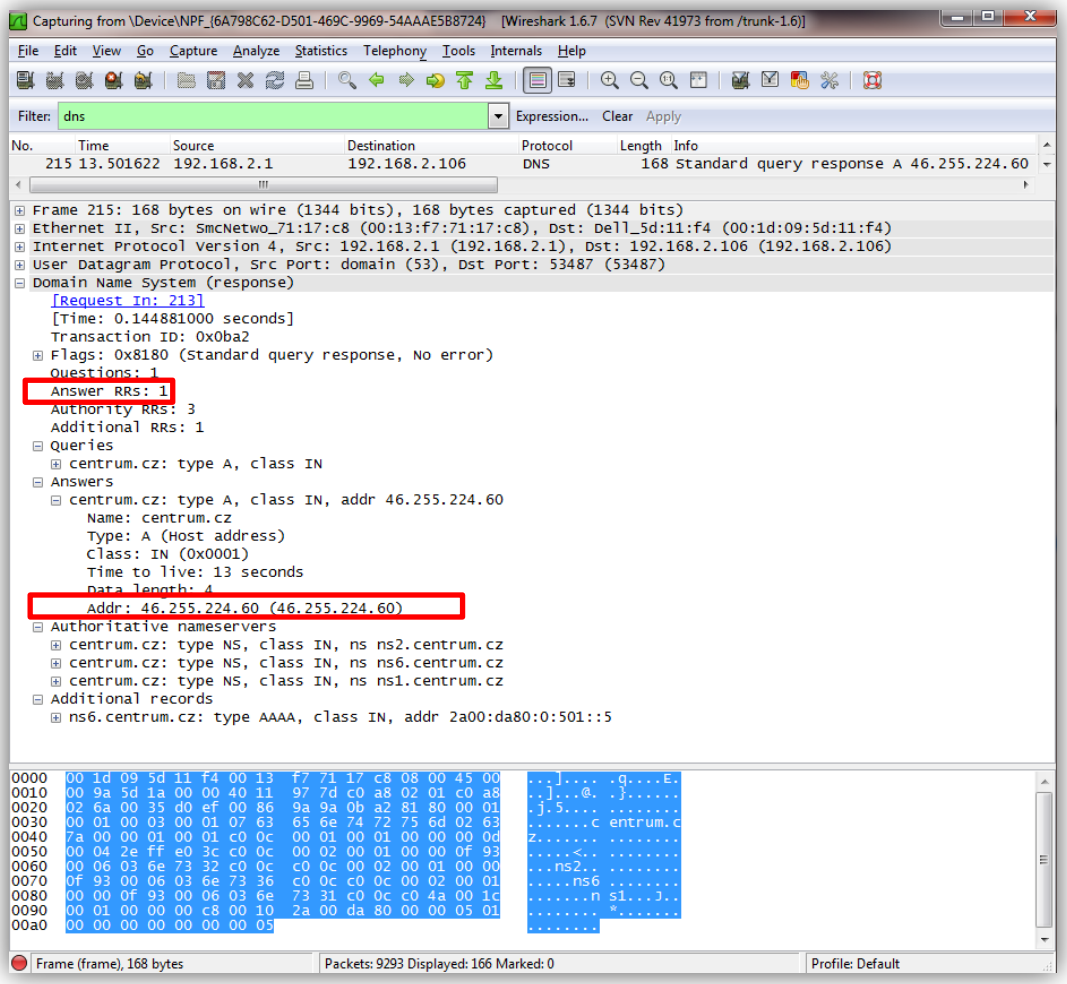
Obrázek 23 – Výstup z Wiresharku

Příčina:

Jedním možným problémem může být chyba v DNS záznamu. Výstup z Wiresharku to potvrzuje. Počítač A sice dostane odpověď na dotaz DNS, nicméně odpověď je prázdná, resp. neobsahuje překlad na adresu IP. To je důvod proč prohlížeč nemůže zobrazit webové stránky zadané jménem.

Řešení:

Správná konfigurace DNS serveru na routeru 192.168.2.2, nebo konfigurace IP adresy primárního DNS počítače A na router obsahující funkční DNS server, tedy na 192.168.2.1. Prevencí může být automatická konfigurace DNS ze serveru DHCP. Následující obrázek (Obrázek 24) ukazuje, jak by měla vypadat správná odezva ze serveru DNS.



Obrázek 24 – Jak by měla vypadat odezva z DNS

Závěr

Síťové analyzátory jsou velice silnou pomůckou administrátorů, správců sítí a síťových návrhářů při řešení rozmanitých problémů napříč různými typy sítí. Jejich funkcionalita dovoluje uživateli kontrolu nad daty procházející skrze monitorovaný port, switch, či jinou část počítačové sítě. Dále například možnost ukládání zaznamenaných dat pro pozdější analýzu, může být zároveň bezpečnostním prvkem každé sítě, a v neposlední řadě je velice účinnou a názornou pomůckou při studiu síťových protokolů. V této práci byl vysvětlen základní princip a součásti fungování síťových analyzátorů včetně metod výběru vhodného umístění.

Stejně jako je síťový analyzátor silnou pomůckou v rukou administrátorů, je stejně silnou zbraní v rukou útočníků. Nejen z tohoto důvodu je důležité mít na mysli závažnost síťové, potažmo počítačové kriminality a dopady z toho plynoucí vzhledem především k navrhované, stavěné nebo spravované síti. A ačkoli síťový analyzátor jedná a v síti vystupuje jako ryze pasivní zařízení, lze jej pomocí metod nastíněných v této práci v síti vypátrat a určit jeho lokaci.

Z práce by rovněž měly být zřejmé základní principy tvorby a návrhu bezproblémových, moderních a bezpečných místních sítí LAN. Tyto principy by měly obecně platit pro jakýkoliv typ sítě. Stejně tak bylo v práci rozebráno, jakým způsobem a za pomocí jakých metod se dají řešit již vzniklé síťové potíže. Probrané metody lze prohlásit za systematické, tudíž velmi vhodné a doporučované.

Wireshark, jakožto jeden z nejrozšířenějších a nejrozsáhlejších freeware síťových analyzátorů byl v práci popsán od instalace až po praktické používání. Byl zde představen včetně popisu grafického prostředí a logického uspořádání programu. Za pomocí tohoto softwaru byla vyzkoušena jeho funkčnost na praktických experimentech, respektive na simulaci běžných problémů vyskytujících se v počítačových sítích. Bylo zjištěno, že za pomoci Wiresharku, zkušeností a určitého stupně znalostí síťových protokolů se tento síťový analyzátor stává poměrně rychlou a efektivní pomocí v případě nejasného chování síťových zařízení nebo síťových problémů.

Při pohledu do budoucna vidím v užívání síťových analyzátorů stále stejně silnou pomůcku zastávající stále stejnou funkci. S vývojem síťových protokolů bude zcela jistě docházet i k vývoji síťových analyzátorů pro zajištění maximální možné podpory při řešení různorodých problémů.

Literatura

1. **Trulove, James.** *Sítě LAN.* [překl.] Tomáš Znamenáček. Praha 7 : Grada Publishing, a.s., 2009. ISBN: 978-80-247-2098-2.

2. **Sportack, Mark A.** *Směrovaní v sítích IP.* [editor] Libor Pácl. [překl.] David Krásenský. Brno : Vydavatelství a nakladatelství Computer Press, 2004. ISBN: 80-251-0127-4.

3. **Bouška, Petr.** Cisco IOS 22 - monitoring/kontrola/zrcadlení provozu - SPAN a RSPAN. *Samuraj.* [Online] Petr Bouška, 15. červen 2009. [Citace: 8. Duben 2012.] http://www.samuraj-cz.com/clanek/cisco-ios-22-monitoringkontrolazrcadleni-provozu-span-a-rspan/.

4. **Orebaugh, Angela, et al., et al.** *Wireshark & Ethereal Network Protocol Analyzer Toolkit.* s.l. : Syngress Publishing, Inc., 2007. ISBN-10: 1-59749-073-3, ISBN-13: 978-1-59749-073-3.

5. **Wallace, Kevin.** *CCNP TSHOOT 642-832 - Official Certification Guide.* [ed.] Paul Boger. Indianapolis : Cisco Press, 2010. ISBN-10: 978-1-58705-844-8, ISBN-13: 1-58705-844-8.

6. **Chappell, Laura.** *Laura's lab kit.* [DVD]. San Jose : Chappell University, 2011. v10.

7. **BIGELOW, Stephen J.** *Mistrovství v počítačových sítích - správa, konfigurace, diagnostika a řešení problémů.* Brno : Computer Press, 2004. ISBN 80-251-0178-9.

8. **Cisco.** Catalyst Switched Port Analyzer (SPAN) Configuration Example. *Cisco Homepage.* [Online] Cisco Systems, Červenec 16, 2007. [Cited: Březen 20, 2012.] http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml. Document ID: 10570.

9. **Fluke Networks.** EtherScope™ Series II Network Assistant. *Web Fluke Corporation.* [Online] Fluke Corporation. [Citace: 6. Březen 2012.] http://www.flukenetworks.com/enterprise-network/network-testing/EtherScope-Series-II-Network-Assistant.