Univerzita Karlova

Pedagogická fakulta

Katedra informačních technologií a technické výchovy

BAKALÁŘSKÁ PRÁCE

Diagnostika vybraných závad ve školní počítačové síti

Diagnostics of selected failures in school computer network

Tomáš Chabada

Vedoucí práce: PhDr. Martin Stejskal

Studijní program: Informační technologie se zaměřením na vzdělávání (B0114A140004)

2024

Odevzdáním této bakalářské práce na téma Diagnostika vybraných závad ve školní počítačové síti potvrzuji, že jsem ji vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Prohlašuji, že jsem při její tvorbě nepoužil nástrojů umělé inteligence jiným způsobem, než je uvedeno ve vyjádření, které je součástí textu práce. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Praha 28.11.2024

Rád bych poděkoval vedoucímu práce PhDr. Martinu Stejskalovi za vstřícnost při konzultování a za pro mě velmi cenné postřehy z praxe. Dále bych rád poděkoval Danielu Brůhovi za poskytnutí informací o struktuře a provozu skutečné školní počítačové sítě.

Anotace

Cílem mé bakalářské práce je poskytnout materiál pro správce školních počítačových sítí, který by jim pomohl při diagnostice závad, které se ve školních počítačových sítích mohou vyskytnout.

První část teoretické části práce bude zaměřena na diagnostické nástroje používané v oblasti počítačových sítí. Vybrané, často používané nástroje zde budou popsány (včetně principu fungování a jejich výstupů). Nejčastěji používané nástroje (PING a TRACEROUTE) budou popsány podrobněji.

Druhá část teoretické části práce se zaměří na popisy vybraných závad, které se v počítačových sítích běžně vyskytují. Při popisu závad bude kladen důraz zejména na vysvětlení souvislostí, tj. na zdůvodnění projevů daných závad a na diferenciální diagnostiku (odlišení závady od jiných závad s podobnými projevy).

Praktická část práce bude založena na praktickém postupu diagnostiky několika vybraných závad v síťovém emulátoru GNS3. Závady budou navozeny v emulované topologii, která bude vhodným způsobem napodobovat prostředí běžné školní počítačové sítě. Emulovaná topologie bude zadokumentována (fyzická topologie, logická topologie, adresní plán). U každé závady bude uveden způsob navození závady ve virtuální topologii, možný úvodní projev závady a zejména použití diagnostických nástrojů včetně jejich výstupů. Důraz bude kladen na zdůvodnění diagnostického procesu (myšlenkového pochodu při diagnostice) a interpretaci výstupů z ladicích nástrojů. Při tvorbě praktické části budou taktéž zohledněna omezení emulace (žádná emulace nedokáže zcela věrně napodobit prostředí skutečné počítačové sítě).

Klíčová slova

Diagnostika, závady, školní počítačová síť, PING

Annotation

The goal of my Bachelor thesis is to provide material for school computer network administrators, which would assist them in diagnostics of failures possibly occuring in such networks.

The first part of theoretical section focuses on diagnostic tools commonly used in computer networking. These tools will be described there, including the principle of their function and outputs. The most used tools (PING and TRACEROUTE) will be described in more detail.

Second part of theoretical section focuses on describing selected failures commonly occuring in computer networks. Description of each failure focuses mainly on explanation of context e.g. scrutinizing manifestations of given failures and performing differential diagnostics (distinguishing one failure from other failures with similar manifestations).

Practical section of the thesis is based on practical workflow of diagnostics of several selected failures in network emulator GNS3. Failures are to be triggered in emulated topology, which will simulate an environment of common school computer network in an appropriate manner. Emulated topology will be documented (physical topology, logical topology, address plan). Each failure entry will contain the way of triggering in virtual topology, possible initial manifestation of failure and mainly description of diagnostic tool usage including their outputs. Emphasis will be laid on explaining the diagnostics process (main thoughts during it) and interpretation of debugging tools' output. The limitations of emulation will also be taken into account over the course of practical section, as no emulation can perfectly faithfully simulate an environment of real computer network.

Keywords

Troubleshooting, fault, school computer network, PING

Obsah

1 Cíle práce

Hlavním cílem této práce je vytvoření postupu diagnostiky čtyřech vybraných závad, které se mohou vyskytnout ve školních počítačových sítích (mimo bezdrátových). Při tvorbě postupu bude kladen důraz na použití diagnostických nástrojů včetně interpretace jejich výstupů.

Práce má několik dílčích cílů. Prvním z nich je popis vybraných základních diagnostických nástrojů použitelných v oblasti školních počítačových sítí. U každého z takto popsaných nástrojů jsou uvedeny minimálně tyto informace:

- popis nástroje
- výstup nástroje (jakou informaci daný diagnostický nástroj dává)

Druhým dílčím cílem je popis vybraných závad, které se ve školních počítačových sítích mohou vyskytnout. Popis každé ze závad obsahuje:

- popis závady (co daný název znamená)
- příčiny závady (proč daná závada vzniká)
- projevy závady, včetně zdůvodnění, proč se daný projev u dané závady vyskytuje
- diferenciální diagnostika závady (kritéria, pomocí kterých lze odlišit danou závadu od jiných závad s podobnými projevy)

Třetím dílčím cílem je vytvoření virtuální síťové topologie vhodně reprezentující školní počítačovou síť. Takto vytvořená virtuální topologie umožní snadné navození závad a nasazování diagnostických nástrojů. Dokumentace postupu diagnostiky závad navozených v takovéto topologii umožňuje splnění hlavního cíle práce.

2 Diagnostické nástroje

2.1 PING

2.1.1 Popis

PING je základní diagnostický nástroj, který umožňuje otestovat obousměrné spojení mezi dvěma síťovými zařízeními. Pracuje na třetí vrstvě OSI/ISO modelu – testuje spojení na protokolech IPv4 nebo IPv6. Ke své funkci využívá pomocný protokol ICMP (Internet Control Message Protocol) [1]. Jeho vlastnosti (široká dostupnost, jednoduchost a rychlost použití) ho řadí mezi nejužitečnější nástroje při diagnostice.

Pro své fungování potřebuje nejméně jeden parametr – identifikátor zařízení, se kterým chceme otestovat spojení. Ten lze v běžných implementacích (OS Windows, OS Linux, Cisco IOS) zadat jako IPv4 adresu, jako IPv6 adresu, nebo jako FQDN (máme-li k dispozici DNS server). Spouštění nástroje probíhá obvykle přes rozhraní příkazové řádky.

2.1.2 Princip fungování

Vysílající stanice (tj. ta, ze které byl PING spuštěn) odešle cílové stanici ICMP Echo Request packet. Cílová stanice, je-li nastavena tak, aby na PINGy odpovídala, při přijetí ICMP Echo Request packetu odpoví jeho odesílateli zprávou ICMP Echo Reply. Přijetí odpovědi na PING je zobrazeno na výstupu programu (obvykle i s RTT latencí a TTL). [2] Podle implementace program může reagovat i na jiné packety, které mohl ICMP Echo Request vyvolat (typicky ICMP Destination Unreachable od mezilehlého routeru) a ty vhodným způsobem zobrazit.

2.1.3 Omezení

PING je nástroj s velmi širokou škálou použití, avšak má svá omezení. Mezi ně patří:

- Neověření propustnosti

Výchozí nastavení PINGu využívá pouze malých packetů vysílaných v relativně dlouhých časových intervalech. Kvůli tomu standardně není možné testovat chování trasy při vyšším vytížení. To znesnadňuje diagnostiku některých problémů, jako např. rozdílného duplexu (spoj při nízkém zatížení funguje, avšak při vyšším zatížení jeho propustnost dramaticky klesá). Omezení je možné obejít vhodným nastavením intervalu mezi jednotlivými PINGy a nastavením jejich velikosti.

- Nespojité testování

Relativně velký interval mezi vyslanými PINGy použitý při výchozím nastavení neumožňuje zachytit krátkodobě trvající problémy (jako např. elektromagnetické rušení metalických spojů). Ty se buďto neprojeví vůbec, nebo jen drobným zvýšením latence. Stejně jako u předchozího omezení je toto možné obejít změnou nastavení – zkrácením intervalu mezi vyslanými PINGy.

- Možnost nepřijetí žádné odpovědi

Síťové zařízení může být nakonfigurováno takovým způsobem, že vědomě neodesílá žádné odpovědi na přijaté zprávy ICMP Echo Request. V takovém případě vyslání PINGu skončí vypršením času (time-out) a nepřinese žádné informace (z nepřijetí žádné odpovědi nelze v žádném případě vyvodit závěr, a to ani o nefunkčnosti spojení).

- Možný rozpor mezi identifikátorem a zamýšleným zařízením.

Cíl PINGu je definován adresou cílového stroje (IPv4 nebo IPv6) nebo doménovým jménem. Skutečný příjemce PINGu se tak může lišit od zařízení původně zamýšleného obsluhou. Rozpor může být způsoben omylem, chybným nebo neaktuálním adresním plánem nebo také chybně nakonfigurovaným DNS (dojde k překladu doménového jména na IP adresu jiného, než zamýšleného zařízení).

2.1.4 Výstup

PING neposkytuje pouze dvoustavovou informaci typu „spojení funguje“ nebo „spojení nefunguje“. Možné výstupy PINGu jsou:

- Odpověď od cílového zařízení

Pokud spojení na třetí vrstvě mezi vysílající a cílovou stanicí funguje (a není zde jiný mechanismus, který by ICMP provoz zablokoval, např. firewall), PING tuto informaci zobrazí, obvykle spolu i s RTT latencí (round trip time, čas obrátky) a TTL.

- Odpověď od jiného, než cílového zařízení

Jestliže libovolné zařízení na trase mezi vysílající a cílovou stanicí nedokáže packet ICMP Echo Request předat dál, tento packet zahodí a pokud je nakonfigurován na zasílání ICMP Destination Unreachable zpráv, může touto zprávou odpovědět odesílateli zahozeného (nedoručitelného) PINGu. Vysílající stanice na tuto zprávu pak může reagovat – v případě PINGu může být název a druh této zprávy zobrazen spolu s IP adresou zařízení, které jej odeslalo.

- Žádná odpověď

Pokud do určitého času nedorazí žádná odpověď na ICMP Echo Reply, dojde k vypršení času (time-out). V takovém případě PING neposkytuje žádnou relevantní informaci k upřesnění příčiny problému a je tudíž třeba použít jiný nástroj.

2.2 TRACEROUTE

2.2.1 Popis

TRACEROUTE je nástroj, pomocí kterého lze zjistit cestu packetu sítí (resp. zjistit IP adresy rozhraní routerů, která packet přeposílala na jeho cestě k cíli). Stejně jako PING pracuje na třetí vrstvě OSI/ISO modelu a využívá zpráv protokolu ICMP – zde ICMP Time Exceeded. Oproti PINGu umožňuje přesnější lokalizaci problému (přímo lze zjistit, který router už packet dále zpracovat nedokázal). Jeho výhodou je velmi dobrá dostupnost a jednoduché použití (stejně jako u PINGu stačí znát jen identifikátor cílového zařízení – IPv4, IPv6 nebo FQDN).

2.2.2 Princip fungování

TRACEROUTE využívá hodnoty TTL pro IPv4 [3] nebo Hop Limit pro IPv6 [4] v hlavičce packetu. První vyslaná zpráva má toto číslo nastavené na 1. První router, který by měl packet předávat, ho sníží na 0. Tím životnost skončila a je-li nakonfigurován na zasílání ICMP zpráv, informuje o tomto odesílatele pomocí ICMP Time Exceeded zprávy. Přijetí této zprávy (spolu s jejím odesílatelem) TRACEROUTE zobrazí na výstup. Další zpráva vyslaná odesílatelem má TTL nebo Hop Limit nastavený na 2. První router jej sníží na 1 a provoz dále předá. Druhý router jej sníží na 0 a opět může následovat vyslání ICMP Time Exceeded.

TTL nebo Hop Limit se u každé další odeslané zprávy postupně zvyšují o 1, dokud buďto neodpoví cílová stanice, nebo dokud nedojde k překročení maximálního počtu hopů (liší se u každé implementace; lze nastavit parametrem příkazu). [5]

2.2.3 Omezení

Stejně jako PING má i TRACEROUTE svá omezení. Některá dědí od PINGu (propustnost, nespojitost testování, rozpor mezi zamýšleným a skutečným cílem), jiná jsou pro něj specifická. Mezi tato omezení patří:

- Neodeslání ICMP Time Exceeded zprávy

Jestliže router, u kterého došlo ke snížení životnosti na nulu, není nakonfigurován na odesílání Time Exceeded zpráv, TRACEROUTE tento skok na trase nedokáže zobrazit. Předávání

dalších zpráv (s vyšší životností) tím však není dotčeno, takže ostatní skoky mohou být zobrazeny.

- Dlouhá doba vykonávání příkazu

Výchozí nastavení příkazu mohou snadno způsobit dlouhé vykonávání příkazu. Nastavení ovlivňující dobu trvání jsou doba time-outu, počet opakování a případný reverzní překlad IP adresy odesílatele Time Exceeded zprávy. Dobu vykonávání mohou výrazně ovlivnit i spoje s vysokou latencí. Pokud navíc cílový stroj neodešle Time Exceeded zprávu, dojde k selhání i všech následujících pokusů s vyšším TTL, až do maxima daném nastavením příkazu. Omezení lze do značné míry obejít citlivým laděním parametrů vzhledem k odhadované délce trasy.

- Neschopnost ladit asymetrické směrování

TRACEROUTE z podstaty svého fungování dokáže odhalit pouze cestu packetu ve směru od odesílatele k cíli. Je-li cesta zpět od odesílatele k příjemci odlišná, TRACEROUTE tuto cestu zjistit nedokáže (není-li spuštěn z cílového stroje).

2.2.4 Výstup

Výstupem programu TRACEROUTE je posloupnost IP adres rozhraní routerů, která odesílaný provoz předávala cestou k cíli. Cesta provozu zpátky (od routerů nebo koncové stanice k vysílající) se nijak neřeší (nástroj se tedy nehodí pro diagnostiku závad v asymetrickém směrování). Výstup může obsahovat i latenci (stejně jako u PINGu ve formě RTT – času obrátky). Pokud některý router není nastaven na odesíláni ICMP Time Exceeded zpráv, jeho adresu TRACEROUTE zjistit nedokáže. Nezjistitelné zařízení je na výstupu TRACEROUTE obvykle indikováno pomocí symbolu hvězdičky (*).

2.3 Wireshark

2.3.1 Popis

Wireshark je aplikace, která umožňuje zachytávat a analyzovat síťový provoz. [6] Provoz lze zachytávat na libovolném síťovém rozhraní stroje, na kterém je Wireshark nainstalován, a to v obou směrech. Podporována jsou všechna běžná rozhraní (mj. Ethernet, 802.11, Bluetooth, sériové spoje). U zachycených zpráv Wireshark dokáže zobrazit data pro různé vrstvy (od linkové až po aplikační). Zachycený provoz lze filtrovat nebo uložit pro pozdější analýzu. Jeho vlastnosti (multiplatformnost, open-source, komunitní podpora vč. videokurzů) z něj činí velmi

užitečný a populární nástroj, a to nejen při diagnostice závad (dobře se uplatní i třeba ve vzdělávání).

2.3.2 Použití

Při diagnostice závady je vhodné spustit Wireshark na takovém stroji (a jeho síťovém rozhraní), kde předpokládáme provoz, jehož přítomnost potvrdí (anebo vyvrátí) zamýšlenou příčinu závady. Samotný proces použití Wiresharku je následovný:

1. Spuštění záznamu provozu
2. Zastavení záznamu provozu (po předpokládaném zaznamenání provozu, který by mohl být relevantní pro další diagnostiku)
3. Uložení a následné prohlédnutí (analýza) záznamu

S výhodou lze využít širokou škálu filtrů, které Wireshark nabízí (např. při diagnostice EIGRP si vyfiltrujeme pouze EIGRP zprávy). Jestliže na cílovém stroji není možné Wireshark nainstalovat spustit, lze provoz pro tento stroj na switchi zrcadlit na jiný port, do kterého je připojeno zařízení, na kterém Wireshark spustit lze. Toho lze docílit např. pomocí SPAN a od něj odvozených protokolů (např. RSPAN) [5].

2.3.3 Omezení

Mezi omezení použití Wiresharku (nebo jiného nástroje pro zachytávání provozu) patří například:

- Rozsáhlý výstup

Koncová i mezilehlá zařízení v běžné počítačové síti mohou zpracovávat značné množství provozu. Výstupy ze zachytávání provozu mohou být velmi rozsáhlé, což klade značné nároky na paměť zařízení. Ruční prohledávání rozsáhlých výstupů pak může být velmi zdlouhavé. Toto omezení lze odstranit vhodným použitím filtrů.

- Složitost interpretace výstupu

I přes použití dekodérů může být získání relevantní informace z výstupu zachytávání provozu obtížné. Obsluha provádějící analýzu výstupu musí mít odpovídající znalosti zachycených protokolů.

- Podpora na straně zařízení

Pokud potřebujeme zachytávat provoz přímo na síťovém zařízení, toto zařízení musí být vybaveno softwarem pro zachytávání provozu a dostatkem paměti pro uložení výstupu. Síťová

zařízení pro běžné domácí použití (SOHO) nemusí možnost zachytávání provozu podporovat. Omezení lze obejít zrcadlením provozu nebo připojením prostřednictvím hubu.

2.3.4 Výstup

Výstupem Wiresharku je zachycený provoz včetně jeho hlaviček. Interpretace takového výstupu vyžaduje určité zkušenosti a znalosti v oblasti počítačových sítí. Uživatelům s analýzou velmi pomáhají vestavěné dekodéry protokolů (odpovídající pole v obsahu či hlavičce zprávy jsou zobrazeny ve správném datovém formátu včetně popisu jejich významu).

2.4 Jednorázový výpis stavu zařízení (show)

2.4.1 Popis

Síťová zařízení, jsou-li spravovatelná („managed“), umožňují zobrazit stav jednotlivých funkcí zařízení. Možnosti zobrazování se značně odlišují dle typu zařízení (switch, router, AP, ...) i dle jeho účelu (firemní síťová zařízení obvykle nabídnou mnohem větší možnosti, než domácí). Stav lze vypsat přes CLI (připojení přes sériový port nebo vzdáleně přes Telnet nebo SSH), nebo GUI (webová rozhraní, pomocné aplikace), podle možností každého zařízení. Text výpisu může být možné i filtrovat. Použití tohoto nástroje klade určité nároky na znalost operačního systému daného zařízení (je zde nutnost znát příkazy a možnosti daného operačního systému), avšak u některých závad dokáže poskytnout velmi cenné informace, které rychle vedou k nalezení příčiny.

2.4.2 Výstup

Výstupem je výpis stavu daného procesu aktuálního zařízení podle zadaného příkazu. Formát výpisu se může lišit – může jít o textové formátování při spuštění příkazu z rozhraní příkazové řádky, XML nebo např. formátování pomocí HTML při spuštění příkazu z webového rozhraní pro správu.

2.4.3 Omezení

Zobrazení stavu zařízení je jednorázový úkon s daným výstupem. Z toho vyplývající omezení jsou například:

- Neschopnost reagovat na změny

Předpokládáme-li změnu stavu zařízení po vypsání stavu, je nutné tento výpis provést znovu. Výpis stavu nedokáže reagovat na změny. Jednorázovost je možné obejít vhodným použitím živého ladění (debug), pokud tuto možnost laděné zařízení podporuje.

- Nízká čitelnost výstupu

Výpis stavu spuštěný v rozhraní příkazové řádky je pro vyšší čitelnost textově formátován. Takovéto formátování předpokládá použití neproporcionálního fontu a pevně dané (nebo alespoň minimální) výšky a šířky terminálového okna. Není-li toto dodrženo, výpis nemusí být čitelný. Čitelnost výstupu může dále snížit použití zkratek a formulací. Čitelný výstup lze zajistit vhodným nastavením terminálového emulátoru a dobrou znalostí struktury výstupu obsluhou (výstupy často využívají zkratky a specifické formulace, typicky v anglickém jazyce).

- Nízká názornost výstupu

Formát a obsah výstupu je standardně napevno zvolen vývojáři operačního systému síťového zařízení při vývoji. Zejména u domácích síťových zařízení (kde se primárně nepředpokládá znalá obsluha) může mít výstup špatně čitelný formát (výstup je čitelný jen pro servisní techniky), nebo nemusí poskytovat relevantní informace, případně možnosti ladění nemusí být dobře zadokumentovány. Takovéto omezení prakticky obejít nelze – řešením je pořizovat síťová zařízení od renomovaných výrobců, u kterých lze předpokládat důraz na vývoj ladicích prostředků.

2.5 Ladění zařízení v reálném čase (debug)

2.5.1 Popis

Jednorázový výpis nedokáže reagovat na změny (pokud předpokládáme změnu, která by mohla ovlivnit výstup příkazu, je nutné ho spustit znovu). Potřebujeme-li sledovat nějaký proces v reálném čase, lze využít živého ladění. Živé ladění sleduje určitý proces zařízení (např. OSPF) a pokud v něm dojde k určité události (např. přijetí nové LSA nebo odpojení souseda), toto zobrazí na výstup. [7]

2.5.2 Výstup

Výstupem ladění je chronologická posloupnost událostí, ke kterým došlo v laděném procesu. Parametr příkazu určuje laděný proces a případně i druh událostí, které ladicí proces vypisuje.

2.5.3 Omezení

Při vhodném použití je živé ladění velice silný nástroj (schopný odhalit i nahodile vyskytující se závady), avšak jeho neuvážené spuštění může mít dalekosáhlé důsledky. Mezi jeho úskalí patří:

- Vysoká náročnost na prostředky

Živé ladění některých procesů (např. sledování IP provozu) může být značně náročné na prostředky, zejména na exponovaných produkčních zařízeních. Ladění potřebuje procesorový čas (pro sledování událostí a jejich zpracování) a pro případ odesílání ladicích zpráv na jiné zařízení potřebuje i šířku pásma. Neuvážené spuštění ladění může způsobit vysokou zátěž procesoru a přetížení sítě. Toto omezení nelze nijak odstranit, proto je při spouštění ladění v reálném čase vždy nutná obezřetnost obsluhy. [7]

- Udržování přesného času

Každá ladicí zpráva je běžně opatřena časovým razítkem. Časové razítko umožňuje sledovat chronologii událostí v síti (zvláště tehdy, pokud pro diagnostiku sbíráme události z více různých zařízení). Takovéto sledování však není možné, pokud všechna zařízení v topologii nemají k dispozici přesný a koordinovaný čas. Ten lze zajistit např. prostřednictvím služby NTP a pečlivým nastavením časového pásma včetně střídání letního a zimního času.

2.6 Logování zpráv

2.6.1 Popis

Pro sledování nahodilých událostí (např. odpojení kabelu ze síťového rozhraní) se nehodí ani výpis stavu (bylo by ho nutné spouštět neustále), ani živé ladění (zbytečně by zabíralo procesorový čas a většinu času by neposkytovalo přínosné informace). Vhodnějším nástrojem je generování systémových zpráv – proces při vzniku sledované události vygeneruje systémovou zprávu, přiřadí jí časové razítko, důležitost a popis a předá dalšímu procesu, který tyto systémové zprávy zpracovává. Ten s ní podle svého nastavení dále naloží (např. zobrazí ji na konzoli, uloží do RAM nebo odešle na vzdálený Syslog server). Tyto zprávy, jsou-li uloženy, lze zpětně prohlédnout a analyzovat.

2.6.2 Výstup

Systémové zprávy obsahují zdroj (tj. jaký proces onu zprávu vyvolal), důležitost (v osmi úrovních očíslovaných podle závažnosti sestupně od 0 až po 7), časové razítko a detailnější

popis. Díky těmto údajům lze uložené zprávy účinně filtrovat a nalézt ty, které mohou nalézt příčinu aktuálně probíhající závady. Pro účinné použití při diagnostice (zejm. pokud na server posílá zprávy více síťových zařízení) je velmi důležité používat na zařízeních přesný a koordinovaný čas (např. pomocí NTP protokolu). [8]

2.6.3 Omezení

Podobně jako u živého ladění jsou zprávy opatřeny časovým razítkem, tudíž je nutné na zařízeních udržovat koordinovaný přesný čas (obzvláště pro sledování nahodilých, zřídka se vyskytujících událostí). Další omezení je např.:

- Omezení množství zpráv v čase

Síťová zařízení omezují množství vygenerovaných zpráv v čase. Příliš mnoho zpráv (vygenerovaných např. četně se opakujícím připojením a odpojením kabelu s chybně zajištěným konektorem) by mohlo zahltit úložiště zpráv, a navíc by samo o sobě bylo možností pro kybernetický útok (útočník by mohl záměrně vyvolávat události, které by vyvolávaly zprávy, jejichž další zpracování by přetěžovalo zařízení a síť). Řešením je vhodné nastavení maximálního počtu zpráv za jednotku času podle účelu a vytížení daného zařízení.

2.7 Světelné indikátory

2.7.1 Popis

Běžnou výbavou síťových zařízení jsou LED indikátory. Ty se mohou vztahovat buďto k celému zařízení, nebo se mohou vztahovat k jednotlivým portům. Indikátory společné pro celé zařízení mohou mít název např. „Power“ (pak obvykle poskytují informaci o napájení zařízení) nebo „System“ (obvykle poskytuje informaci o tom, zda řádně proběhl boot operačního systému zařízení).

Indikátory pro porty obvykle poskytují informaci o stavu (zda port přeposílá data, tj. je zapnutý z hlediska první a druhé vrstvy OSI/ISO modelu), duplexu, vytížení a rychlosti. V případě switchů vybavených PoE lze ze světelných indikátorů získat navíc informaci o tom, zda je k portu připojeno zařízení odebírající PoE výkon.

2.7.2 Výstup

Informaci o stavu zařízení nebo portu světelný indikátor předává prostřednictvím zhasnutí, trvalého svitu, blikání nebo barvy. Význam jednotlivých světelných a barevných kódů je nutno dohledat v dokumentaci každého zařízení. U některých switchů je pro každý port pouze jeden

indikátor a jejich kontext (tj. zda zobrazují stav, rychlost, duplex, ...) se přepíná stiskem fyzického tlačítka na zařízení. [9]

3 Závady

3.1 Přerušená kabeláž

3.1.1 Popis

Přerušená kabeláž je závada na první vrstvě OSI/ISO modelu. Přerušení způsobí nemožnost předávat signály mezi zařízeními, která jsou spojena poškozeným kabelem. Nemusí jít pouze o přímé poškození elektrických vodičů nebo optického vlákna – stejným způsobem se projeví i poškození konektoru nebo patch panelu.

3.1.2 Příčiny

Příčiny poškození mohou být velmi různorodé a mohou se zakládat na různých fyzikálních principech. Mezi některé z nich patří:

- Mechanické poškození kabeláže

K poškození kabeláže uložené ve zdi může snadno dojít při stavebních pracích. Kabely umístěné v zemi jsou náchylné na poškození při výkopových pracích (zejm. při špatné dokumentaci). Při takových poškozeních dochází ke škodám na celých souběžných svazcích kabelů, což rozšiřuje okruh zařízení a sítí, na kterých se závada projeví, čímž zvyšuje pravděpodobnost jejího dřívějšího nalezení.

- Únavové poškození kabeláže

Při opakovaných ohybech dochází k únavovým trhlinám v materiálu, které časem vyústí ve zlom. Takové zlomy mohou snadno vzniknout u patch kabelů používaných uživateli k připojení např. vlastního notebooku. Pravděpodobnost selhání snižuje použití licny (lépe se ohýbá a méně se láme) namísto drátu.

- Oxidace kontaktů

Nepozlacené kontaktní plošky konektorů mohou působením vzdušné vlhkosti zoxidovat, což může vést ke zhoršení vodivosti a selhání spoje.

- Zlomení kabelu

Optické kabely mají předepsaný minimální poloměr ohybu. Pokud dojde k jeho překročení, tak spoj přestane vést signály (vyslaný optický signál se od zlomu odrazí zpátky) nebo dojde k mechanickému poškození. K poškození při přílišném ohybu může dojít i u metalické kabeláže, zejména u kabelů s vodiči větších průřezů (Cat6A a vyšší).

- Zkrat mezi žilami

Při poškození izolace žil metalického vedení může dojít ke zkratu (vodivému spojení různých žil s různými potenciály). Izolace se může porušit průrazem příliš vysokým napětím (např. při úderu blesku), nebo i mechanicky. Zkratovaný spoj nedokáže vést žádný signál, a proto se projeví stejně jako přerušení.

3.1.3 Projevy

Přes zcela poškozenou kabeláž není možné vést elektrické nebo optické signály. Díky tomu je vyloučena veškerá komunikace přes tuto kabeláž. To se projeví nemožností dosáhnout vzdálený segment sítě po jakékoliv vrstvě přes postižený spoj (v případě použití redundantních spojů může být provoz příslušnými protokoly přesměrován přes fungující spoje, díky čemuž může být vzdálený segment stále dosažitelný). Výpis stavu ethernetového rozhraní se při připojení zcela přerušeného kabelu tváří, jako kdyby do rozhraní nebyl připojen žádný kabel (pouze v případě zapnuté detekce přítomnosti zařízení na vzdáleném konci, tzv. „keepalive“). Je-li kabel poškozený jen pro jeden směr, pak signály ze vzdáleného konce přicházet mohou a takový spoj se na jednom konci může tvářit jako fungující.

3.1.4 Diferenciální diagnostika

Charakteristickým projevem přerušené kabeláže je neschopnost přenášet informace na všech vrstvách OSI/ISO modelu. Tuto vlastnost sdílí několik dalších závad, které svými projevy mohou právě přerušenou kabeláž napodobovat.

Další možné závady s podobnými příznaky mohou být:

- Špatný kontakt

V případě špatného kontaktu (mezi vodiči a konektorem nebo i mezi dvěma konektory) může závada vypadat jako přerušení, které se ovšem vyskytuje jen za určitých podmínek (např. při určitém ohybu kabelu). Od skutečného přerušení kabeláže se liší přítomností projevů v čase.

- Rozdílná rychlost mezi konci ethernetového spoje

Pokud dojde k nastavení rozdílné rychlosti na obou koncích ethernetového spoje, tento spoj taktéž nepřenáší data na žádné vrstvě OSI/ISO modelu. Různé rychlosti ethernetu používají různé kódování a symbolovou rychlost. K tomu může dojít buďto chybnou manuální konfigurací rychlosti, nebo selháním autokonfigurace. Od přerušení kabeláže toto lze odlišit buďto kontrolou stavu (nastavené či domluvené rychlosti) na obou zařízeních postiženého

spoje, nebo změnou kabeláže za jinou, prokazatelně fungující (v případě přerušené kabeláže při náhradě postiženého segmentu spoj začne fungovat, v případě rozdílné rychlosti fungovat nezačne).

- Chybné použití kříženého, resp. přímého kabelu

Pokud propojíme síťová zařízení nesprávným typem kabelu (ve smyslu kříženého nebo přímého kabelu) a zároveň žádné z těchto zařízení nemá možnost detekce typu kabelu (např. auto-MDIX pro ethernet), vysílač jednoho zařízení je spojen s vysílačem druhého (a analogicky přijímač jednoho je propojen s přijímačem druhého). Takový spoj nedokáže přenést žádné informace na žádné vrstvě OSI/ISO modelu, a proto projevy této závady jsou stejné, jako u odpojeného nebo zcela přerušeného kabelu. Od přerušení tento problém odlišíme pokusem s jiným typem kabelu (při použití opačného typu spoj začne fungovat).

- Vypnutí rozhraní

Jestliže je alespoň jedno rozhraní daného spoje vypnuté, příslušný spoj opět nedokáže přenášet žádné informace. Od závady na kabeláži problém odlišíme kontrolou konfigurace nebo stavu rozhraní. Pokud je vypnuté jen jedno rozhraní spoje, problém odhalí kontrola zařízení právě na straně vypnutého rozhraní – kontrola na straně zařízení se zapnutým rozhraním nepřinese žádné bližší informace, protože ono zařízení nemá, jak zjistit, že protější rozhraní je vypnuté.

3.2 Rozdílný duplex

3.2.1 Popis

Pomalejší verze Ethernetu s rychlostmi 10 Mbps a 100 Mbps při použití dvou párů kroucené dvoulinky umožňují jak poloduplexní provoz (tj. vysílání je možné provádět oběma směry, ale v daném čase může vysílat pouze jedno zařízení), tak i plně duplexní provoz (vysílat lze oběma směry, a to i najednou). Podporuje-li koncové zařízení oba režimy duplexu, duplex je možné nastavit (ručně nebo automaticky). [10] Protože lze režim duplexu nastavit, může dojít k rozdílnému nastavení na obou koncích jednoho Ethernetového spoje – jedno zařízení je nakonfigurované pro plně duplexní provoz, druhé je nakonfigurováno pro poloduplexní provoz. Jestliže spoj mezi takovýmito zařízeními umožňuje plně duplexní provoz, dojde ke vzniku projevů této závady.

3.2.2 Příčiny

Režim duplexu lze na síťových zařízeních nastavit ručně, nebo automaticky. Obě možnosti mohou způsobit rozdíl v konfiguraci:

- Chybná manuální konfigurace

Jestliže je na jedné straně spoje nastavený poloduplexní režim a na druhé straně je nastavený plně duplexní režim, dojde ke vzniku rozdílného duplexu.

- Selhání automatické konfigurace

Automatická konfigurace by měla zajistit optimální nastavení (pokud je to možné, tak nastaví plně duplexní režim, jestliže to možné není, tak nastaví poloduplexní režim). V praxi může selhat, což taktéž povede ke vzniku rozdílného duplexu.

3.2.3 Projevy

Plně duplexní strana může vysílat i přijímat data v jeden okamžik. Jestliže k této situaci dojde (což je při i mírně vyšším vytížení sítě prakticky jisté – i zdánlivě jednosměrný provoz jako např. stream videa ve skutečnosti využívá i provozu opačného směru), poloduplexní strana musela nutně zaznamenat kolizi. Na tu poloduplexní strana zareaguje standardně podle algoritmu CSMA/CD – je vyslán tzv. jam signál (informace ostatním stanicím na kolizní doméně ohledně vzniklé kolize) a následuje čekání, po kterém dojde k retransmisi. [11] Protože plně duplexní strana kolize nijak neřeší, k této situaci dochází na postiženém segmentu relativně často a plynou z ní typické projevy této závady:

- Výrazný pokles výkonu spoje při zatížení

Je-li vytížení postiženého segmentu velmi nízké (např. při použití PINGu při ověřování funkčnosti segmentu nebo při základní diagnostice), závada se výrazněji neprojeví (provoz je v jeden čas prakticky výhradně jednosměrný). Při zvýšení vytížení dojde k výraznému nárůstu počtu kolizí, což razantně sníží propustnost postiženého spoje.

- Příjem poškozených rámců na plně duplexní straně

Plně duplexní strana přijímá rámce od poloduplexní strany, která implementuje CSMA/CD. Ten v případě detekované kolize (krom dalšího) zastaví vysílání aktuálně vysílaného rámce. To se na plně duplexní straně projeví jako příjem poškozeného rámce – nemusí souhlasit CRC kontrolní součet v patičce rámce nebo rámec může být příliš malý, pokud k detekci kolize došlo relativně brzy po zahájení vysílání rámce (tzv. runt frames – trpasličí rámce).

- Kolize a pozdní kolize na poloduplexní straně

Protože plně duplexní strana neimplementuje žádný algoritmus pro detekci nebo vyhnutí se kolizi, na poloduplexní straně dochází k relativně značnému množství kolizí. Dochází jak k běžným kolizím, tak i k pozdním (tzv. late collision, kolize, při které došlo k souběžnému vysílání po 64. bajtu rámce). K těm by za normálních podmínek v soudobých počítačových sítích docházet nemělo – mohlo by k nim dojít např. při použití příliš dlouhého kabelu nebo při nesprávném návrhu topologie v sítích s rozbočovači. Přítomnost pozdních kolizí je typický projev rozdílného duplexu. [12]

3.2.4 Diferenciální diagnostika

Dramatický pokles propustnosti postiženého spoje při zatížení je hlavním projevem, který je nutné odlišit od ostatních problémů. Možnými závadami, které mohou napodobovat projevy rozdílného duplexu jsou:

- Nízký přenosový výkon spoje

Postižený spoj má nízký přenosový výkon, čímž může napodobovat projevy vysokého vytížení sítě. Jakákoliv snaha o vyřešení samotného vysokého vytížení nepovede k vyřešení problému. Prosté přetížení od rozdílného duplexu odlišíme nejsnáze pomocí prohlédnutí statistik rozhraní (vysoké počty kolizí).

- Problém na fyzické vrstvě

Prohlédnutí statistik rozhraní postiženého spoje (CRC chyby, kolize, ...) může napovídat o možném problému na fyzické vrstvě (poškozená nebo příliš dlouhá kabeláž). Závadu na fyzické vrstvě od neshody duplexu odlišíme kontrolou konfigurace rozhraní. Rozdíl v ručně nastavených hodnotách je zde viditelný ihned; je-li nastavena automatická konfigurace duplexu, v takovém případě je nutné zkontrolovat ještě aktuální stavy rozhraní (tj. výsledek autokonfigurace).

3.3 Vysoké vytížení

3.3.1 Popis

Každý úsek (spoj nebo segment) počítačové sítě má svoji přenosovou kapacitu (množství informace, které je schopen přenést za jednotku času), udávanou obvykle v megabitech nebo gigabitech za sekundu. Toto číslo je značně závislé na použité technologii (stovky kilobitů za sekundu pro dlouhé ADSL smyčky, stovky gigabitů za sekundu u optických spojů), použitých

zařízeních i použitém médiu a jeho parametrech (zejména u bezdrátových sítí ovlivňuje přenosovou kapacitu vzdálenost mezi uzly a okolní rušení). Přenosovou kapacitu dále ovlivňují i použitá síťová zařízení a jejich výkon (např. routery, u kterých přenosový výkon závisí na počtu běžících služeb). Je-li požadavek na přenosový výkon segmentu sítě větší, než je jeho přenosová kapacita, část provozu nemůže zákonitě být předána (a musí být zahozena), z čehož plynou projevy této závady.

3.3.2 Příčiny

Základní příčinou přetížení sítě je překročení maximální přenosové kapacity sítě aktuálním požadavkem na přenosový výkon. To může být způsobeno buďto snížením přenosové kapacity, nebo náhlým zvýšením požadavku na přenosový výkon. Mezi možné příčiny těchto jevů patří:

- Náhlé zvýšení požadavku na přenosový výkon

Jestliže je přenosový výkon sítě nebo jejího segmentu dimenzován na určité množství provozu, jeho náhlé zvýšení může způsobit přetížení sítě, zejm. pokud je rezerva v přenosovém výkonu malá. Příčinou zvýšení množství provozu může být prostý vyšší požadavek na služby poskytované danou sítí, nebo třeba i DDoS útok. [13]

- Vysoké vytížení síťových zařízení

Přenosová kapacita spoje je dána nejen typem a vlastnostmi média, ale i schopností koncových zařízení spoje vysílat, resp. přijímat data. Dojde-li ke zvýšení vytížení některého ze zařízení, přenosový výkon spoje může poklesnout.

- Změna vlastností a stavu přenosového média

Přenosový výkon sítí je značně závislý na vlastnostech přenosového média. U optických spojů se vlastnosti (relevantní pro přenos dat) prakticky nemění, u metalických spojů se měnit už mohou (např. vnější elektromagnetické rušení, přeslechy mezi souběžnými vodiči), avšak u bezdrátových sítí se mění zcela běžně, a to i velmi výrazně. Změnit se může vzdálenost mezi vysílačem a přijímačem (zvýšení vzdálenosti vede ke snížení přenosového výkonu), změnit se může míra rušení (snížení odstupu signálu od šumu taktéž vede ke snížení rychlosti) a v případě venkovních bezdrátových spojů mohou hrát roli i fyzikální překážky v cestě bezdrátového signálu (déšť, mlha, sníh). Poklesne-li přenosový výkon pod úroveň požadavku na přenosovou kapacitu, dojde k přetížení sítě, i když před poklesem kapacity síť přetížena nebyla.

3.3.3 Projevy

Překročení přenosové kapacity nutně vede k tomu, že segment nebo spoj nedokáže ihned přeposlat veškerý provoz. Drobné, krátkodobě trvající přetížení dokážou vyrovnat buffery; u delšího přetížení dojde k jejich přetečení a k zahození části provozu. Z využití bufferů a ze zahazování provozu vychází projevy přetížení sítě:

- Vysoká latence

Jestliže zpráva nemůže být odeslána ihned, může se dostat do bufferu. Tam čeká, než bude příslušným rozhraním odeslána dále. V případě velkých bufferů a/nebo rozhraní s nízkou přenosovou kapacitou může čekání trvat relativně dlouho, zejm. pokud není využito žádné prioritizace provozu (QoS). Množství provozu taktéž do jisté míry zatěžuje procesor zařízení – v případě přetížení sítě je i využití procesoru vyšší, což latenci může taktéž zvýšit.

- Vysoké kolísání latence (jitter)

I v případě přetížení sítě není množství provozu za jednotku času konstantní. Zprávy uložené v bufferu se zpracovávají postupně, obvykle v pořadí, v jakém do bufferu byly uloženy (není-li použito nastavení QoS). Zpráva, která se do bufferu dostala v době, kdy byl téměř prázdný, bude odeslána dříve (tedy s nižší latencí), než zpráva, která se dostala až na samotný konec bufferu. Rozdíl mezi těmito dvěma časy je ona hodnota, o kterou latence kolísá.

- Zahazování provozu (packet loss)

Pokud aktuální přetížení nedokážou vyrovnat ani buffery (zprávu už není možné zařadit do bufferu, protože je plný), je provoz zahozen. Je-li použito TCP, dojde ke snížení velikosti okna a opakovanému odeslání zahozeného provozu (retransmisi); v případě UDP je provoz zahozen nenávratně.

- Nízká přenosová rychlost spojení

Provoz v přetíženém segmentu sítě se dělí o přenosovou kapacitu s ostatním provozem. Jestliže je požadavek na šířku pásma větší, než dokáže přetížený segment poskytnout, dojde k jeho omezení (u TCP změnou velikosti okna, u protokolů bez implementovaného řízení toku toto musí řešit jiná, vyšší vrstva).

3.3.4 Diferenciální diagnostika

Při řešení možného přetížení sítě je vhodné se zaměřit na to, které z výše uvedených projevů se vyskytují současně. Přítomnost pouze jednoho nebo dvou projevů příliš nesvědčí pro přetížení, avšak i většinu nebo všechny z těchto projevů mohou být přítomny u některých dalších závad:

- DoS nebo DDoS útok

Cílem útoku DoS (Denial of Service) nebo DDoS (Distributed Denial of Service) je zamezení přístupu oprávněných uživatelů k službě sítě. Jedním z možných nástrojů těchto útoků je právě využití přetížení sítě (cílem útočníka je vytížit síť nebo síťová zařízení natolik, aby výkon pro legitimní uživatele byl tak nízký, že službu nebude možné použít). K odlišení od jiných příčin přetížení (těch, která nejsou spojena s kybernetickým útokem) pomůže sledování charakteru provozu.

- Smyčka na druhé vrstvě OSI/ISO modelu

V případě, že dojde ke vzniku smyčky na druhé vrstvě OSI/ISO modelu, v postiženém síťovém segmentu dojde ke zvýšenému vytížení (které je způsobeno zejm. zmnožením provozu a broadcastovými rámci, které smyčkou cestují neustále, dokud není rozpojena). Prostřednictvím vysokého vytížení procesorů zařízení na postiženém segmentu se závada může propagovat i do dalších segmentů, ve kterých tato zařízení figurují. Od prostého přetížení sítě odlišíme smyčku sledováním charakteru provozu (velké množství broadcastových rámců, opakované kopie jednoho rámce), kontrolou MAC tabulek switchů na postiženém segmentu (rychlé přepínání MAC adres mezi porty, tzv. „flapping“), případně opticky (viditelná smyčka např. na switchi nebo na patch panelu). Rozpojení smyčky (případně kombinované s restartem switchů) tento problém vyřeší, v případě přetížení budou projevy nadále pokračovat.

- Rozdílný duplex

Rozdílný duplex mezi konci jednoho ethernetového spoje vede k poklesu přenosového výkonu takového spoje (při zvýšení množství provozu dojde ke zvýšení počtu kolizí, které daný spoj zpomalují). Snížený přenosový výkon spoje může svými projevy napodobovat vysoké vytížení sítě.

3.4 L2 smyčka

3.4.1 Popis

Ethernetový rámec nemá ve své hlavičce žádné pole, pomocí kterého by bylo možné určit jeho stáří nebo životnost. Rámec s pro switch neznámou cílovou MAC adresou (tj. adresou, pro kterou neexistuje záznam v tabulce MAC adres) nebo s broadcastovou MAC adresou je vyplaven na všechna rozhraní vyjma rozhraní příchozího (u nespravovatelných switchů; u spravovatelných je vyplaven na všechna rozhraní v konkrétní VLAN). Jestliže dojde ke vzniku smyčky v ethernetové topologii, vyplavený rámec v ní může cestovat donekonečna (není zde žádný mechanismus, který by cirkulující rámec dokázal odstranit). Obsahuje-li smyčka navíc redundantní cesty, dochází k množení vyplaveného provozu.

3.4.2 Příčiny

Příčinou vzniku smyčky v ethernetové topologii je samotný návrh fyzické topologie (existence redundantních cest), nebo nevhodné zapojení kabeláže (typicky zapojení patch kabelu uživatelem do sousední RJ-45 zdířky ve zdi, např. v domnění, že jde o slepou zásuvku). Pokud switche v topologii používají STP (Spanning Tree Protocol) či jinou odvozenou verzi (např. Rapid STP), mělo by i v takovém případě dojít k logickému rozpojení smyčky a zachování plné funkčnosti sítě. [14] V takovém případě je možné bez problému použít redundantní spoje a projevy závady objeví pouze v případě, že STP byl špatně nakonfigurován nebo implementován.

3.4.3 Projevy

Projevy smyčky vychází z chování switchů v případě přijetí rámce s broadcastovou, nebo pro switch neznámou unicastovou cílovou MAC adresou. Takovýto rámec je vyplaven na všechna rozhraní, kromě toho rozhraní, na kterém byl rámec přijat (v případě spravovatelných switchů je toho vyplavení omezeno jen na tu VLAN, ve které bylo rozhraní, na kterém byl rámec přijat). Nachází-li se v topologii sítě smyčka, dojde k cirkulaci rámce. Pokud by v hlavičce rámce bylo pole, pomocí kterého by bylo možno určit stáří nebo životnost rámce (jako TTL na IPv4, nebo Hop Limit na IPv6), bylo by možné ho ze sítě po nějaké době odstranit, jenže ethernet žádné takové pole nemá. Cirkulující rámec tedy nic (kromě rozpojení smyčky) nedokáže odstranit. Z této vlastnosti plynou hlavní projevy smyčky:

- Vysoké vytížení celého segmentu se smyčkou

Cirkulující rámce smyčkou velmi rychle vytíží celý segment na maximum. Takto způsobené vysoké vytížení blokuje veškerý užitečný provoz, včetně provozu určeného pro správu zařízení (může být velmi obtížné až nemožné se připojit do některého ze switchů přes např. Telnet nebo SSH a smyčku rozpojit na dálku vzdáleným přístupem).

- Množení provozu (duplicitní kopie)

Je-li rámec určen k vyplavení (zejm. broadcast), dostane se do každého uzlu daného segmentu. Pokud je znovu vyplaven do switche, který ho už jednou vyplavoval (což indikuje přítomnost smyčky), je opět vyplaven do každého uzlu. Zařízení na postiženém segmentu opakovaně zpracovávají kopie stejného rámce.

- Vysoké vytížení procesorů zařízení

Samotné předávání provozu síťovým zařízením probíhá s použitím hardwarových akcelerátorů (např. ASIC u switchů), avšak některé úkony jsou stále prováděny pomocí softwaru (tj. s použitím procesoru zařízení). Mezi tyto úkony může patřit ARP, u kterého je úvodní zpráva předávána prostřednictvím broadcastu (a v případě existence smyčky tedy dochází k množení). Nutnost zpracovávat velké množství zpráv vyžadujících pozornost procesoru zvyšuje vytížení procesoru a může způsobit, že se závada izolovaná na jednu danou VLAN začne propagovat i do jiných VLAN (nepostižených smyčkou).

- MAC flapping

Algoritmus zpětného učení u switchů využívá v nejjednodušší podobě tabulky uspořádaných dvojic MAC adresy a portu (rozhraní). Jestliže z nějakého rozhraní přijde rámec, tak dojde k prohledání tabulky MAC adres switche. Pokud je v ní záznam pro toto dané rozhraní a zdrojovou MAC adresu, neděje se nic. Nachází-li se v ní záznam pro jiné rozhraní a tuto zdrojovou adresu, dojde k aktualizaci (záznam pro jiné rozhraní je odstraněn a je vložen nový pro nově příchozí rozhraní). Nenachází-li se zdrojová MAC adresa v žádném záznamu, je vytvořen záznam zcela nový. Při vzniku smyčky a množení provozu dochází k velmi častým aktualizacím v tabulce MAC adres – v nejjednodušší situaci stejný rámec dorazí jednou od odesílatele a pak znovu přes smyčku. Časté aktualizace tabulky MAC adres zatěžují switche, avšak mohou být cenným vodítkem pro diagnostiku (jedná se o zcela typický příznak smyčky).

3.4.4 Diferenciální diagnostika

Dominantním projevem smyčky na druhé vrstvě je vysoké vytížení sítě. Jeho přítomnost může chybně napovědět o možné příčině závady (banální vysoké vytížení, DoS, DDoS, ...), avšak

v takovém případě pokus o řešení nepovede k odstranění závady. Možné závady, které mohou smyčku svými projevy napodobovat, jsou:

- Vysoké vytížení sítě

V případě smyčky na druhé vrstvě je vysoké vytížení přítomné, náhle vzniklé. Nejde ovšem o závadu jako takovou, ale pouze o následek (projev) smyčky. Žádný pokus o odstranění vysokého vytížení (implementace QoS, výměna zařízení za novější a rychlejší, EtherChannel, snížení vytížení) nepovede k řešení, protože smyčka vždy vytíží příslušný ethernetový segment na maximum (resp. alespoň jeho nejužší hrdlo – nejpomalejší spoje). Přítomnost smyčky odlišíme od prostého přetížení pomocí přítomnosti dalších projevů smyčky.

- Vysoké vytížení procesorů zařízení

Obdobně jako u diagnostiky vysokého vytížení sítě je u smyčky vysoké vytížení procesorů síťových zařízení přítomné, avšak je pouhým projevem smyčky, a tudíž jakákoliv snaha o jeho řešení (vypnutí nadbytečných služeb, výměna hardware za novější, ...) nepovede k odstranění projevů. Diagnostika je taktéž stejná, založená na zjištění přítomnosti dalších projevů smyčky.

- Nedostupný vzdálený management síťových zařízení

Při zjištění projevů závady je obecně správným krokem snaha zjistit dostupné informace od mezilehlých síťových zařízení. V případě přítomnosti smyčky může pokus o připojení se k zařízení (např. Telnetem nebo SSH) skončit neúspěšně (kvůli vysokému vytížení sítě i procesoru). Vypršení času pro připojení (time-out) může napodobovat jiné problémy, jako např. přítomnost firewallového pravidla zahazující provoz). V takovém případě smyčku identifikujeme nejsnáze pomocí LED diod pro porty switche ve smyčce, nebo pomocí postupného odpojování připojených kabelů (po rozpojení smyčky dojde ke snížení vytížení).

3.5 L3 (routovací) smyčka

3.5.1 Popis

Předávání packetů mezi sítěmi zajišťují routery pomocí směrování (procesu, při kterém se podle různých kritérií – nejčastěji cílové IP adresy – rozhodne, kterému dalšímu zařízení je daný packet předán). Směrování je prakticky výhradně deterministický proces – jestliže router obdrží stejný packet podruhé, naloží s ním úplně stejným způsobem, jako když ho obdržel poprvé (není-li nastaveno vyvažování zátěže, tzv. loadbalancing). Jestliže je směrování nastaveno tak, že router předá packet routeru, který ho již zpracovával, dojde ke vzniku smyčky.

Na síťové vrstvě prakticky nedochází k množení nebo duplikování provozu (výjimkou je směrovaný broadcast), navíc v hlavičce každého IP packetu je pole, pomocí kterého lze zjistit jeho stáří (Time to Live pro IPv4, Hop Limit pro IPv6). Cirkulující packet ve smyčce tedy na rozdíl od smyčky na druhé vrstvě nezpůsobí výrazný pokles výkonu sítě, protože nedochází k množení a packet je po určité době odstraněn.

3.5.2 Příčiny

Směrování v počítačových sítích probíhá buďto staticky (ruční konfigurací administrátorem), anebo dynamicky. Oba tyto mechanismy mohou způsobit vznik směrovací smyčky.

- Chybná manuální konfigurace směrování

Jestliže při nastavování směrování vytvoříme cestu, při které je následující router (tzv. „next hop“) některým z routerů, který packet již zpracovával, dojde ke vzniku smyčky – do smyčky spadne veškerý provoz, který je zpracováván routerem, kterému je provoz následně opět předán.

- Nesprávná implementace směrovacích protokolů

Protokoly pro dynamické směrování implementují mechanismy, které vzniku smyček účinně zabraňují (např. mechanismus „split horizon“ pro RIPv2 [15]). Je-li výrobcem použitá implementace nesprávná, může dojít ke vzniku smyčky i při použití dynamického směrování.

3.5.3 Projevy

Směrovací smyčka způsobuje ztráty packetů a vytváří neúčinný tok packetů. Z toho plynou hlavní projevy směrovací smyčky, kterými jsou:

- Část sítí nebo všechny sítě jsou nedostupné

Pokud cesta packetu sítí obsahuje smyčku, každý packet, který je do ní nasměrován, nemůže být cílovému stroji nikdy doručen, protože ve smyčce nutně skončí jeho životnost (pole Time to Live nebo Hop Limit v hlavičce skončí na nule). Router, který životnost snížil na nulu (a packet zahodil), může odesílatele upozornit pomocí ICMP Time Exceeded. Přijetí této zprávy (spolu se ztrátou packetu) je typickým projevem routovací smyčky.

- Vyšší vytížení sítě

Životnost packetu může dosahovat hodnoty až 255. Packet tedy ve smyčce může cirkulovat relativně dlouho, což (zbytečně) zatěžuje postižený segment a zařízení v něm. Jsou-li routery

nakonfigurovány na zasílání Time Exceeded zpráv, generování a zasílání většího počtu těchto zpráv může způsobit vyšší vytížení procesorů routerů ve smyčce.

3.5.4 Diferenciální diagnostika

Specifickým projevem směrovací smyčky je výskyt Time Exceeded zpráv. Pokud se tyto zprávy při diagnostice nepodaří zachytit, nejvýraznějším projevem smyčky zůstane nedostupnost určitého síťového segmentu. Ta může mít řadu příčin, jako např.:

- Chybná konfigurace směrování (chybějící routovací záznamy)

Všechny packety, které jsou nasměrovány do smyčky, se nikdy nepodaří doručit. Nedostupnost sítí při vzniku L3 smyčky napodobuje celkově chybnou konfiguraci směrování (např. chybějící routy při ručním nastavování). Od smyčky tento problém odlišíme pomocí přítomnosti ICMP Time Exceeded zpráv (prostá nepřítomnost routovacích záznamů se projeví spíše pomocí přítomnosti ICMP Destination Unreachable zpráv).

- Přerušená kabeláž nebo vypnuté rozhraní

Vypnuté rozhraní nebo přerušený kabel nedokáže přenášet data. Veškerý provoz, který by měl procházet postiženým kabelem nebo rozhraním je zahozen a pokud není k dispozici redundantní cesta, segment za takto postiženým spojem nebude dostupný.

3.6 Duplicitní IPv4 adresa

3.6.1 Popis

V každém ethernetovém segmentu (resp. v každé broadcastové doméně) musí být IP adresy všech zařízení jedinečné. V případě IPv4 může zařízení adresu získat buďto prostřednictvím manuální konfigurace, nebo prostřednictvím DHCP (alternativně ještě pomocí APIPA [16], ale tento mechanismus není na IPv4 běžně používán). Kterýkoliv z těchto mechanismů může vést ke vzniku duplicity. V případě IPv6 je použit mechanismus DAD (Duplicate Address Detection) [17], který by měl duplicitám účinně zabránit; IPv4 nic takového nemá a detekce duplicitních adres je záležitostí koncových zařízení a DHCP serverů.

3.6.2 Příčiny

Kterýkoliv mechanismus přidělení adresy může selhat a tím vést ke vzniku duplicitní adresy. Možné příčiny jsou:

- Chybná manuální konfigurace

Jestliže manuálně nastavíme dvěma zařízením na stejném segmentu stejnou adresu, dojde ke vzniku duplicity. K tomu může dojít např. nepozorností při konfiguraci nebo použitím nesprávného adresního plánu.

- Duplicitní přidělení adresy DHCP serverem

DHCP servery mají několik mechanismů, kterými zajišťují, aby k přidělení duplicitní adresy nedošlo. Jsou to např:

1. Databáze přidělených adres (server si udržuje přehled o tom, které adresy již sám přidělil, a ty už nepřiděluje, pokud nedošlo k jejich uvolnění)
2. PING na IP adresu, kterou se server chystá přidělit (při řádné odpovědi se adresa považuje za přidělenou)
3. ARP dotaz na adresu, kterou se server chystá přidělit (při přijetí ARP odpovědi se adresa považuje za přidělenou)

Nachází-li se DHCP server ve stejné podsíti, jako zařízení, kterému se chystá přidělit adresu, může použít všechny tyto mechanismy. Pokud je server v jiné podsíti (např. centrální DHCP server pro celou organizaci), nemůže použít ARP, který funguje na druhé vrstvě. Protože ne každé zařízení je nastaveno, aby odpovídalo na PINGy (obzvláště na ty, které jsou vyslány z jiných sítí), může snadno dojít ke kolizi (přidělení duplicitní adresy).

- Duplicitní DHCP server

Chybné spuštění nadbytečného DHCP serveru v síti může způsobit vznik duplicitních adres v síti. Nadbytečný DHCP server lze v síti omylem spustit např. při testování síťového zařízení nebo při připojení zařízení se zapnutým sdíleným připojením. Jestliže takto nadbytečně spuštěný server přiděluje adresy ze stejného rozsahu, jako je původní rozsah sítě, může dojít ke vzniku duplicitních adres a problémům s bránou (podle aktuálně použité brány dojde k výpadku služeb školní sítě). Jestliže přiděluje adresy z jiného rozsahu, než je původní rozsah sítě, dojde k výpadku služeb školní sítě vzniklého přesměrováním provozu na fungující bránu přidělenou nadbytečným DHCP serverem. Vzniku této situace snadno zabrání řádná konfigurace mechanismu na switchi, který zablokuje DHCP provoz z nedůvěryhodných zdrojů (DHCP snooping).

- Útočící duplicitní DHCP server

Útočník v síti může snadno spustit svůj vlastní DHCP server. Protože odpovědi DHCP serverů standardně nejsou žádným způsobem autentifikovány (tj. neověřuje se totožnost ani

důvěryhodnost serveru, který na DHCP dotaz odpovídá), zařízení kontaktující DHCP server vybere ten, který odpoví jako první (rychlejší odpověď útočníkova DHCP serveru lze snadno zařídit zatížením hlavního DHCP serveru). Útočníkův DHCP server může přidělovat duplicitní adresy, ale také může přidělit vlastní výchozí bránu; je-li tato také ovládána útočníkem, může zde docházet k zahazování provozu (DoS útok) nebo v případě nezašifrovaného provozu může docházet i k jeho sledování a úpravě před předáním skutečné bráně (man-in-the-middle útok).

3.6.3 Projevy

Projevy duplicitní adresy jsou dány zejména fungováním ARP protokolu. Zařízení, které chce komunikovat s jiným zařízením ve stejné podsíti, potřebuje při znalosti IP adresy znát i MAC adresu – tu získá vysláním ARP dotazu. ARP dotaz je vyslán broadcastem, tj. obdrží ho všechna zařízení v dané podsíti (tedy nutně i všechna zařízení sdílející duplicitní IP adresu). Z přijetí ARP dotazu více zařízeními plynou projevy této závady:

- Duplicitní ARP odpovědi

Jestliže se zařízení pomocí ARP dotáže na duplicitní IP adresu, dostane ARP odpověď od každého zařízení, které tuto duplicitní IP adresu sdílí. Vícenásobná ARP odpověď je typickým projevem této závady.

- Schopnost komunikace jen pro jedno zařízení sdílející duplicitní adresu

ARP tabulka zařízení neumožňuje uložit více MAC adres pro jednu IP adresu. Zařízení si tedy uloží pouze jednu z odpovědí. Veškerý unicastový provoz na duplicitní IP adresu je předán pouze tomuto jednomu zařízení. Každé zařízení, které s duplicitní IP adresou komunikuje, může mít jiný ARP záznam pro tuto adresu (tj. bude komunikovat s jiným zařízením sdílejícím duplicitní IP adresu).

- Změna komunikujícího zařízení v čase

Dynamicky vytvořené ARP záznamy jsou ukládány do RAM paměti síťových zařízení. Při restartu tedy dojde k jejich smazání; stejně tak může dojít ke smazání po určitém čase (záznam může mít přidělenou životnost). Vznikne-li potřeba komunikace s duplicitní IP adresou znovu, zařízení znovu vyšle ARP dotaz. Přijetí odpovědí v jiném než původním pořadí před restartem nebo smazáním způsobí změnu zařízení, se kterým se bude komunikovat. Proměnlivost projevů v čase (a proměnlivost ARP záznamů mezi zařízeními, která s duplicitní adresou komunikují) značně znesnadňuje diagnostiku problému.

3.6.4 Diferenciální diagnostika

Hlavním projevem duplicitní IP adresy je neschopnost komunikace některého ze zařízení, které duplicitní adresu sdílí. Tento projev sám o sobě může nabádat k některým možným příčinám, jako např.:

- Chybná konfigurace výchozí brány

Jestliže diagnostiku problému zahájíme na zařízení, které zrovna není v ARP záznamu brány pro duplicitní IP adresu, zjistíme neschopnost komunikovat s veškerými sítěmi mimo podsíť, ve které se postižený stroj nachází. To může vést k úvahám o chybném nastavení brány. Tento problém vyloučíme kontrolou adresního plánu, nebo lépe kontrolou ARP záznamů brány – z něho lze najít záznam pro jiný stroj, což přímo vede ke správné diagnostice závady, navíc ze záznamu lze vyčíst MAC adresu jednoho dalšího zařízení, které sdílí duplicitní adresu.

- Chybějící směrovací záznamy brány

Neschopnost komunikace s vnějšími sítěmi může napodobovat projev závady ve směrování (např. chybějící default routa nebo chybné nastavení dynamického směrování). Problém vyloučíme buďto kontrolou směrovacích tabulek na bráně, nebo pokusem na jiném zařízení v síti (nepostiženém duplicitní IP adresou).

- Problém fyzické vrstvy

Proměnlivost projevů v čase může nabádat k podezření na problém s kabeláží (poškozený konektor, rušení, ...) kdekoliv mezi postiženým zařízením a cílovým strojem, se kterým se snažíme komunikovat. Tuto příčinu nejsnáze odlišíme komunikací z jiného stroje v síti s duplicitní adresou. Jestliže je bezproblémová (a zároveň komunikace z postiženého zařízení je stále neúspěšná), problém na fyzické vrstvě není pravděpodobný (nebo se týká pouze spoje od postiženého zařízení k nejbližšímu síťovému prvku).

- Vysoké vytížení

Neschopnost komunikace měnící se v čase je jedním z projevů vysokého vytížení (pokud vysoké vytížení není konstantní, v časech nižšího vytížení může komunikace bez problémů fungovat, v časech vyššího vytížení nemusí fungovat vůbec). Od duplicitní adresy tuto závadu odlišíme kontrolou vytížení (rozhraní nebo síťových prvků) - problém bude přetrvávat i tehdy, je-li vytížení nízké.

3.7 Excesivní fragmentace

3.7.1 Popis

Z pohledu vrstev vyšších než fyzické, počítačové sítě standardně přenášejí data po určitých blocích (rámce pro Ethernet a 802.11, packety pro IPv4 a IPv6). Tyto bloky mají obvykle variabilní délku (např. nemělo by smysl posílat celých 1500 bajtů pro jeden znak odeslaný z terminálového emulátoru pomocí Telnetu nebo SSH). Každý spoj (fyzický i virtuální) má ovšem omezenou maximální délku tohoto bloku omezenou - tzv. MTU (Maximum Transmission Unit).

Jestliže je přijatý blok větší než MTU rozhraní, přes které má být dále odeslán, dojde buďto k jeho zahození, nebo k fragmentaci (rozdělení bloku na dva či více menších bloků), které mají délku nižší než MTU). Jednotlivé fragmenty se postupně přenesou a u příjemce dojde k jejich seskládání zpět do původního bloku. Fragmentace zvyšuje zátěž zařízení i sítě a dává prostor ke kybernetickým útokům (útočník posílá fragmenty velkých bloků ve snaze vyčerpat paměť zařízení, které si ji rezervuje na zbylé fragmenty, které nikdy nedorazí). [18]

3.7.2 Příčiny

Nadměrná fragmentace vznikne, pokud se na trase mezi odesílatelem a příjemcem nachází úsek s menším MTU, než 1500 bajtů. Mezi takové úseky patří:

- DSL spoje využívající PPPoE protokol s osmibajtovou hlavičkou (tj. typické MTU takového spoje je 1492 bajtů) [19]
- GRE tunely (hlavička GRE má 24 bajtů) [20]
- Šifrované tunely (VPN)

Pokud dojde k selhání mechanismu pro zjišťování MTU cesty (PMTUD) např. kvůli firewallu zahazujícímu ICMP provoz a pokud není přítomné jiné nastavení (např. omezení maximální hodnoty TCP segmentu, tzv. TCP MSS clamping), dojde ke vzniku projevů závady. [21]

3.7.3 Projevy

Projevy jsou dány zejména fungováním TCP protokolu při neúspěšném doručení segmentu. Pokud segment není doručen (bez ohledu na příčinu), dojde po jeho nepotvrzení příjemcem k opakovanému zaslání segmentu odesílatelem, tzv. retransmisi. Při retransmisi se nemění velikost segmentu, takže pokud byl původní segment příliš velký a zároveň nedošlo k upozornění odesílatele prostřednictvím ICMP zprávy, přenos je několikrát opakován, pokaždé

se stejným, neúspěšným výsledkem. [22] Po nějaké době vyprší čas spojení (time-out) a spojení je ukončeno. Mezi projevy tedy patří:

- Neschopnost přenést větší bloky dat

Navázání spojení přes TCP (handshake) je možné i přes úsek s malým MTU, protože využívá pouze malé bloky dat. Úvodní komunikace většinou taktéž zahrnuje pouze menší bloky, tudíž spojení po krátký čas zdánlivě funguje. Jakmile je přes spojení vyslán segment větší velikosti, dojde k jeho zahození (na routeru, který ho měl předat na úsek s malým MTU) a pokud nedojde k upozornění odesílatele, celé spojení uvázne na mrtvém bodě (jediná reakce odesílatele na nepotvrzení segmentu příjemcem je opakované odeslání, velikost segmentu se při retransmisi nemění). Praktickým projevem je tedy např. přenos pouze textu webové stránky (hlavičky a HTML se přenesou, spojení uvázne až na prvním větším obrázku) nebo uváznutí terminálového spojení při zadání příkazu s obsáhlejším výstupem (prompt se přenese, znaky z terminálu taktéž, ale rozsáhlejší výstup – jako např. log – už nikoliv).

- ICMP zpráva Fragmentation needed and DF set

Packet může být zaslán s příznakem DF (Don't Fragment). Pokud packet s tímto příznakem dorazí routeru, který jej má předat na trasu s menším MTU, než má tento packet, dojde k jeho zahození a zároveň může dojít k informování odesílatele packetu pomocí zprávy ICMP Fragmentation needed and DF set. Přijetí této ICMP zprávy zcela jasně ukazuje na problém s malým MTU (zdrojová IP adresa této zprávy navíc jasně identifikuje router, na kterém došlo k tomuto problému), avšak generování těchto zpráv může být zakázáno v konfiguraci routeru (jde o podtyp zprávy ICMP Destination Unreachable, které se běžně zakazují z důvodu bezpečnosti). Pokud odesílatel příliš velkého datagramu přijme tuto zprávu, může následující komunikaci upravit tak, aby k chybě již nedošlo (využitím mechanismu objevování MTU cesty – Path MTU Discovery, PMTUD).

- Nízký přenosový výkon a vysoká zátěž zařízení

Četné fragmentace zatěžují procesory routerů, které tuto fragmentaci provádějí. Seskládání fragmentů zabírá hardwarové prostředky příjemce (obzvláště tehdy, dochází-li ke ztrátám fragmentů). Fragmentace navíc činí přenos velmi náchylným na nahodilé chyby – ztráta i jednoho fragmentu vede k nutnosti poslat celou zprávu znovu (a tedy i k nutnosti opětovně fragmentovat a skládat). Retransmise po zahození velkého segmentu zatěžují síťový segment, kterým procházejí. Je-li nastavené MTU postiženého segmentu velmi nízké, lze po něm přenášet jen malé bloky dat, čímž narůstá režie protokolů nižších vrstev. Všechny tyto události

vedou k (potenciálně výraznému) poklesu přenosového výkonu okrsku sítě s postiženým spojem.

3.7.4 Diferenciální diagnostika

Při znalosti typického projevu příliš malého MTU (uváznutí TCP spojení při vyslání většího segmentu) je diagnostika problému snadná. Bez této znalosti však závada může napodobovat mnoho jiných problémů, jako např.:

- Přetížení sítě

Nízký přenosový výkon sítě může velmi věrně napodobovat vysoké vytížení sítě. Vysoká zátěž síťových zařízení způsobená fragmentací ve spojení s částečným fungováním sítě jsou typické projevy právě přetížení. Příliš malé MTU od přetížení odlišíme kontrolou vytížení spojů (přes spoje neteče velké množství dat) a nepřítomností dalších projevů přetížení (nedochází ke kolísání latence a problémy se spojením jsou nezávislé na čase – pokus o přijetí nebo odeslání většího segmentu skončí vždy uváznutím spojení).

- Chybějící routa, úplná neschopnost přenést data

Jestliže diagnostikujeme problém pomocí vysílání velkých packetů s DF příznakem (které jsou na úseku s malým MTU zahozeny), spojení nebude fungovat vůbec. V takovém případě může problém imitovat neschopnost úseku s malým MTU přenést libovolná data (tj. problém fyzické vrstvy, chybějící směrovací záznam, ...). Tyto problémy od nadměrné fragmentace odlišíme pokusem s menším blokem dat (např. PING výchozí velikosti na běžných operačních systémech) – skončí-li takový diagnostický pokus úspěšně, segment je schopen přenosu dat. Dobrým vodítkem pro diagnostiku je i odpověď routeru, který packet zahazuje (pokud odpovídá pomocí ICMP Fragmentation needed and DF set, jde o jasnou indikaci malého MTU, pokud odpovídá např. pomocí ICMP Destination Network Unreachable, problém s MTU není pravděpodobný).

4 Praktická část

4.1 Metodika praktické části

Aby bylo možné závady ukázat v kontextu školních počítačových sítí, bude nejprve nutné vytvořit topologii, která bude odpovídat prostředí školních počítačových sítí. Při návrhu topologie bude nutné zohlednit několik různých aspektů – topologie nesmí být příliš jednoduchá (na příliš jednoduché topologii by některé závady nebylo možné navodit), ani příliš složitá (příliš složitou topologii by bylo velmi pracné nastavit a její emulace by byla značně hardwarově náročná). Zároveň bude nutné respektovat prostředí školních sítí (rozdělení na počítačové učebny, počítače učitelů v kabinetech, jedna konektivita ven do internetu).

Na vytvořené topologii následně bude nutné navodit závady. To se provede prostou změnou konfigurace zařízení (např. vypnutím protokolu STP pro simulaci smyčky na druhé vrstvě OSI/ISO modelu) nebo změnou topologie (např. odpojením spoje pro simulaci přerušené kabeláže).

Po navození závady bude nutné vhodným způsobem nasadit diagnostické nástroje a zobrazit jejich výstup. Diagnostické nástroje lze spouštět z konzolového rozhraní síťových zařízení nebo z grafického rozhraní koncových zařízení. V obou případech lze výstup snadno zobrazit a vložit jej do praktické části práce.

4.2 Zkušební topologie

4.2.1 Předpoklady

Pro účely praktické části práce bude nutné vytvořit síťovou topologii, která by svým charakterem odpovídala topologii školní počítačové sítě. Topologie bude postavena na následujících pilířích, vycházejících z minimálních možností školních sítí:

- Jedna konektivita do internetu
- Připojení počítačů a koncových zařízení pomocí switchů
- Použití VLAN, oddělené VLAN pro jednotlivé segmenty sítě (učebny, učitelské počítače, DMZ, …)
- Směrování mezi VLAN prostřednictvím jednoho routeru, který je zároveň branou školní sítě
- NAT (dynamický překlad mezi vnitřními soukromými adresami a jednou nebo několika málo vnějšími, veřejnými adresami)

- IPv4

Předpoklady vycházejí z ekonomických, technických i personálních možností menších škol. Redundantní spoje ve starých školních budovách nemusí být vybudované. Zdvojená konektivita nemusí být dostupná a její správná implementace a nastavení klade nároky na obsluhující personál. Běžná škola nemá k dispozici dostatečně velký blok veřejných IPv4 adres, aby každý stroj mohl mít svojí veřejnou adresu bez potřeby NAT. Vhodným řešením by bylo nasazení IPv6, avšak IPv6 nemusí být na starších síťových zařízeních podporována, nemusí být podporována ani poskytovatelem připojení a navíc klade vyšší nároky na znalosti obsluhy a údržby sítě.

4.2.2 Omezení topologie

Topologie pro účely praktické části práce bude vytvořena v síťovém emulátoru GNS3. Protože síťová zařízení budou emulována, nebude možné vytvořit zcela přesnou repliku běžné školní sítě. Další omezení plynou z cílů této práce. Mezi zásadní omezení emulace pro účely této práce patří:

- Nutnost omezit počet zařízení (zejm. v učebnách)

Emulace několika počítačových učeben s mnoha počítači by byla extrémně náročná na hardwarové prostředky, navíc konfigurace mnoha zařízení by trvala velmi dlouho a byla by náchylná na vznik chyb obsluhy při konfiguraci. Vysoký počet koncových zařízení by pro účely práce nebyl prakticky nijak přínosný, proto dojde k jeho razantnímu omezení (na několik málo počítačů v každé oblasti).

- Absence emulace fyzické vrstvy

Síťový emulátor nedokáže emulovat síť až na úroveň fyzické vrstvy (tj. na úroveň elektrických, elektromagnetických nebo optických signálů). Kvůli tomu nebude možné při diagnostice použít diagnostické nástroje fyzické vrstvy, jako např. reflektometrie nebo LED diody na portech. Nelze se spolehnout ani na ukazatele stavů rozhraní.

- Absence bezdrátové části sítě

Ve školních počítačových sítích se zcela běžně vyskytuje možnost bezdrátového připojení klientů. Tato práce se však bezdrátovými technologiemi a jejich diagnostikou nezabývá (mj. proto, že je nelze emulovat) a proto bezdrátová část topologie nebude brána na zřetel. Zahrnutí popisu a diagnostiky závad v bezdrátové části sítě by navíc vedlo k razantnímu překročení rozsahu práce.

4.2.3 Topologie

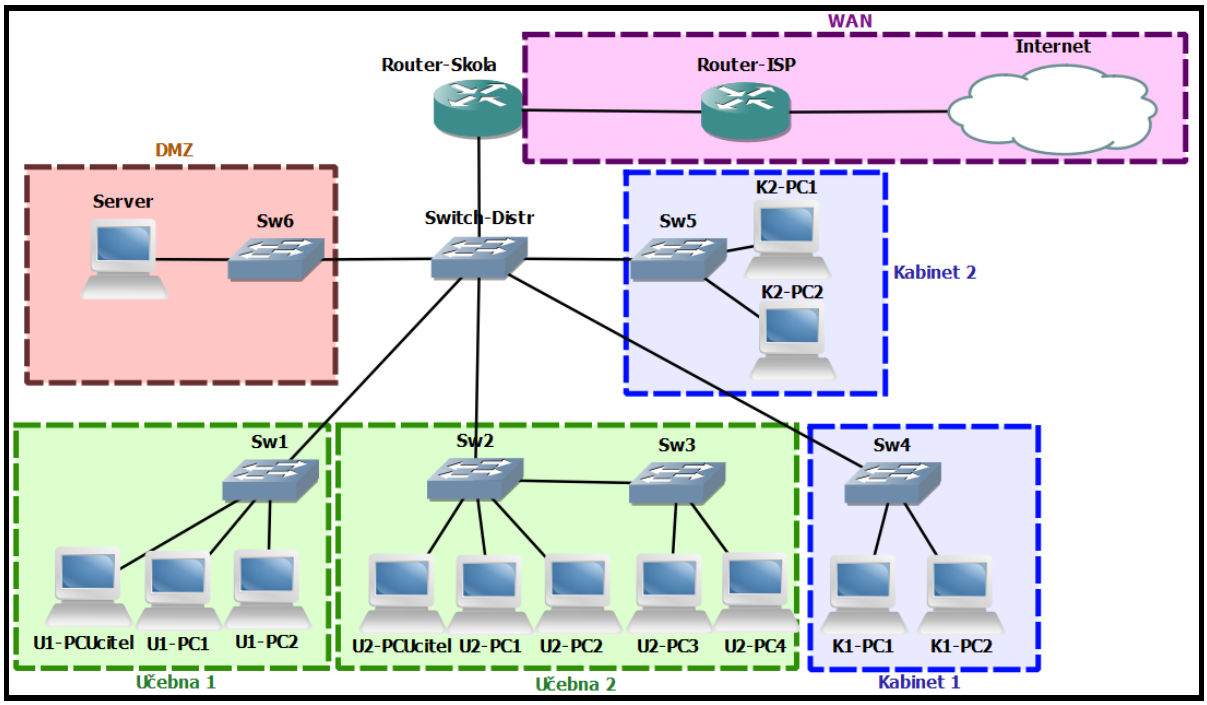
Po zpracování všech požadavků a omezení byla vytvořena topologie, která co nejvěrohodněji reprezentuje školní síť. Jádro sítě obsahuje jeden router (který směruje provoz mezi VLAN a zároveň je branou do internetu) a jeden distribuční switch, ke kterému jsou připojeny další switche. Tyto další switche připojují koncová zařízení (počítače a server) ve vyznačených oblastech, které se ve školních sítích budou vyskytovat. Všechny switche mají přístupná svá rozhraní pro správu ve VLAN 255.

Oblasti DMZ, Kabinet 1 a Kabinet 2 jsou připojené jedním switchem a obsahují všechna svá koncová zařízení v jedné VLAN (VLAN 100 pro oblast DMZ a VLAN 50 pro oblasti Kabinet 1 a Kabinet 2).

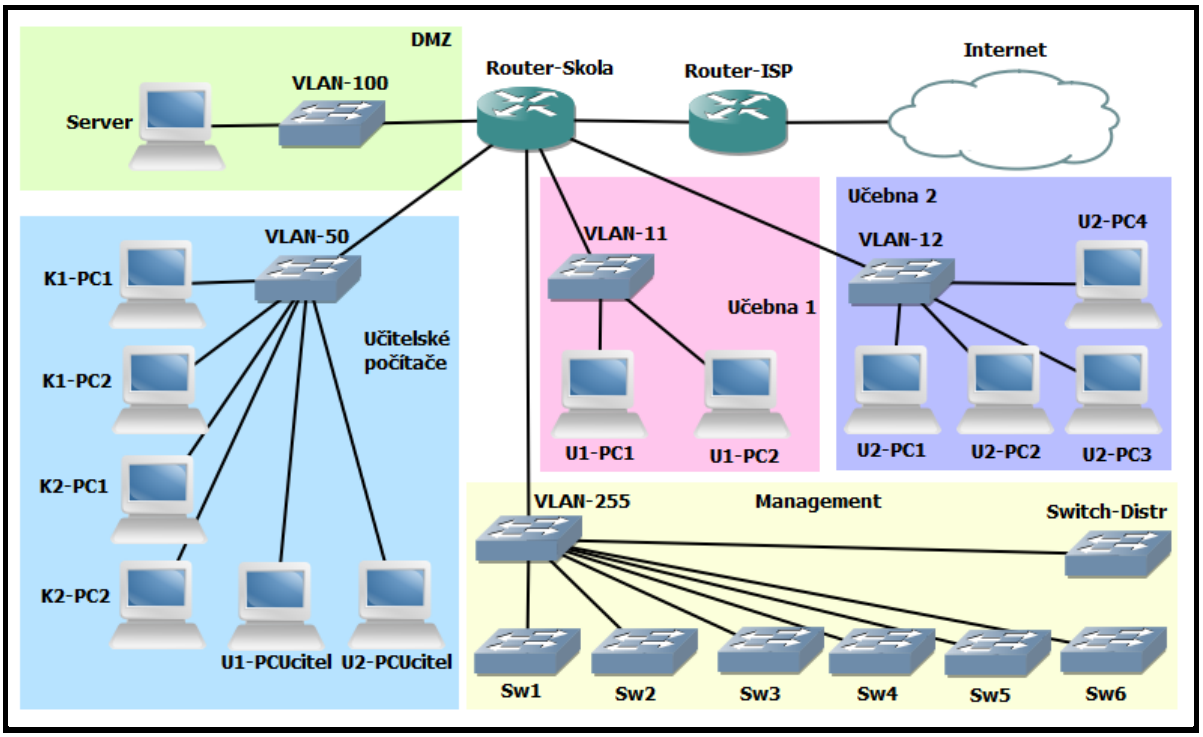
Oblast Učebna 1 je připojena jedním switchem, avšak koncová zařízení se nacházejí ve dvou různých VLAN (učitelský počítač se nachází ve VLAN 50, studentské počítače se nachází ve VLAN 11). Oblast Učebna 2 je připojena dvěma switchi Sw2 a Sw3. Switch Sw2 je připojen přímo do distribučního switche a připojuje koncová zařízení do VLAN 12 (studentské počítače) a VLAN 50 (učitelský počítač). Switch Sw3 je připojen jako podružný do switche Sw2 a sám připojuje studentské počítače do VLAN 12.

Switche, které připojují počítače pouze do jedné VLAN, by mohly být nespravovatelné. Pro účely práce však bylo zvoleno použití spravovatelných switchů všude, i tam, kde by nebyly potřeba. Nespravovatelný switch v GNS3 nedokáže poskytnout naprosto žádné informace o stavu rozhraní.

Zbývající oblast WAN už nespadá do správy školy (vyjma vnějšího rozhraní routeru Router-Skola). V topologii je přítomná pouze pro účely emulace – pro navození závad, které vyžadují úpravu nastavení vnějšího rozhraní školního routeru (např. zmenšení MTU). Bez přítomnosti tohoto routeru by bylo nutné pro navození změny MTU upravovat parametry fyzické produkční sítě, ve které se nachází server, na kterém běží GNS3. Přidání jednoho routeru toto umožňuje bez potřeby provádět jakékoliv změny v produkční síti – postačí prostá úprava konfigurace na onom přidaném routeru.



Obrázek 1 – Fyzická topologie



Obrázek 2 – Logická topologie

4.2.4 Adresní plán

Všechna zařízení mají svá L3 rozhraní nakonfigurována pouze na IPv4. Ve skutečné školní síti by k přiřazení adres počítačům docházelo použitím DHCP, avšak pro účely práce postačí (a bude výrazně vhodnější) statické nastavení adres. Pro vnitřní adresaci jsou použity soukromé

adresy třídy C dle RFC 1918 [23]. Třetí oktet adresy odpovídá číslu VLAN, čtvrtý oktet svým formátem napovídá, o jaké zařízení jde (první adresu má vždy brána, číslo počítače je uloženo v poslední číslici čtvrtého oktetu). Pro vnější adresaci (spoj mezi Router-Skola a Router-ISP) jsou použity soukromé adresy z rozsahu 100.64.0.0/10 definovaném v RFC 6598 [24]. Vnější adresa Routeru-ISP je přidělená DHCP serverem fyzické sítě.

Síť	Adresa sítě	VLAN
Učebna 1	192.168.11.0/24	11
Učebna 2	192.168.12.0/24	12
Kabinet 1	192.168.50.0/24	50
Kabinet 2		
Učitelské počítače		
DMZ	192.168.100.0/24	100
Management síť. zař.	192.168.255.0/24	255
WAN (Vnější síť)	100.64.12.0/30	

Tabulka 1 – Adresní plán sítí a jejich přiřazení do VLAN

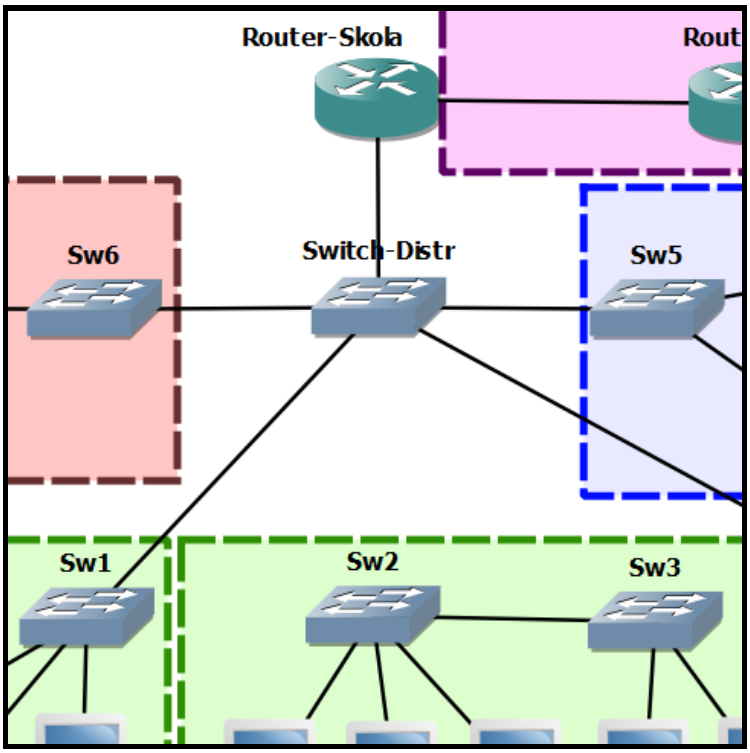
Zařízení	Síťové rozhraní zařízení	Adresa zařízení
Router-Skola	Eth0/0 (k Router-ISP)	100.64.12.1/30
Router-Skola	Eth0/1 ve VLAN 11	192.168.11.1/24
Router-Skola	Eth0/1 ve VLAN 12	192.168.12.1/24
Router-Skola	Eth0/1 ve VLAN 50	192.168.50.1/24
Router-Skola	Eth0/1 ve VLAN 100	192.168.100.1/24
Router-Skola	Eth0/1 ve VLAN 255	192.168.255.1/24
Switch-Distr	VLAN 255 SVI	192.168.255.10/24
Sw1	VLAN 255 SVI	192.168.255.11/24
Sw2	VLAN 255 SVI	192.168.255.12/24
Sw3	VLAN 255 SVI	192.168.255.13/24
Sw4	VLAN 255 SVI	192.168.255.14/24
Sw5	VLAN 255 SVI	192.168.255.15/24
Sw6	VLAN 255 SVI	192.168.255.16/24
Server		192.168.100.100/24
U1-PC1		192.168.11.11/24
U1-PC2		192.168.11.12/24
U2-PC1		192.168.12.11/24
U2-PC2		192.168.12.12/24
U2-PC3		192.168.12.13/24
U2-PC4		192.168.12.14/24
U1-PCUcitel		192.168.50.31/24
U2-PCUcitel		192.168.50.32/24
K1-PC1		192.168.50.11/24
K1-PC2		192.168.50.12/24
K2-PC1		192.168.50.21/24
K2-PC2		192.168.50.22/24

Tabulka 2 – Adresní plán koncových a mezilehlých zařízení

4.3 Diagnostika přerušené kabeláže

4.3.1 Navození závady

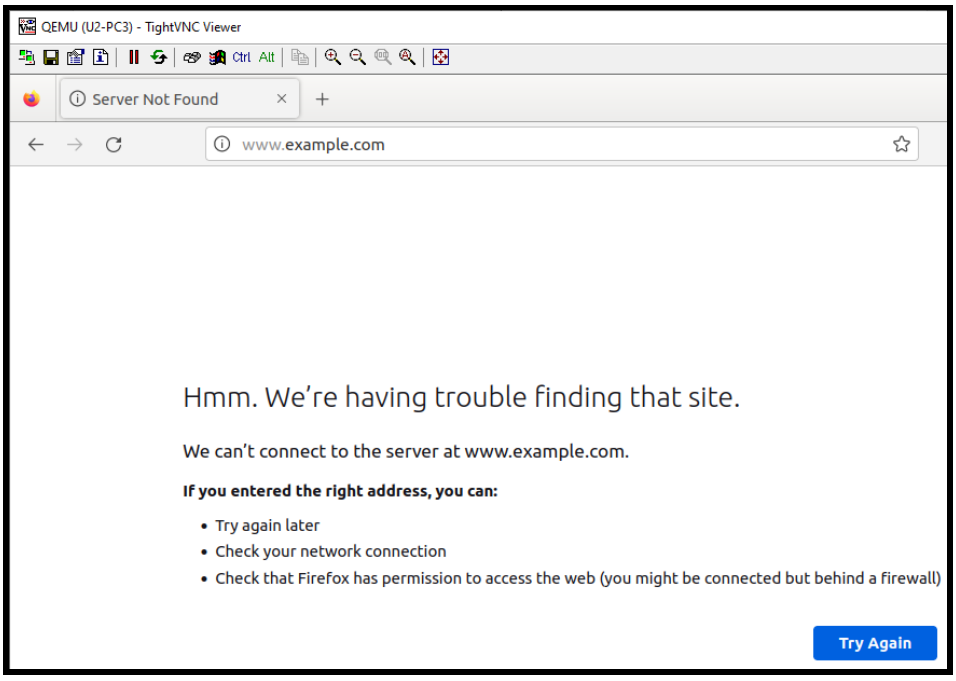
Přerušenou kabeláž navodíme prostým odpojením spoje, který chceme přerušit. Další možností by bylo vypnutí jednoho z rozhraní spoje, avšak pro účely práce je vhodnější odpojení spoje (odpojení spoje vyvolá změnu v topologii). Pro účely navození závady odpojíme spoj mezi Switch-Distr a Sw2.



Obrázek 3 – Změna topologie po odpojení kabelu

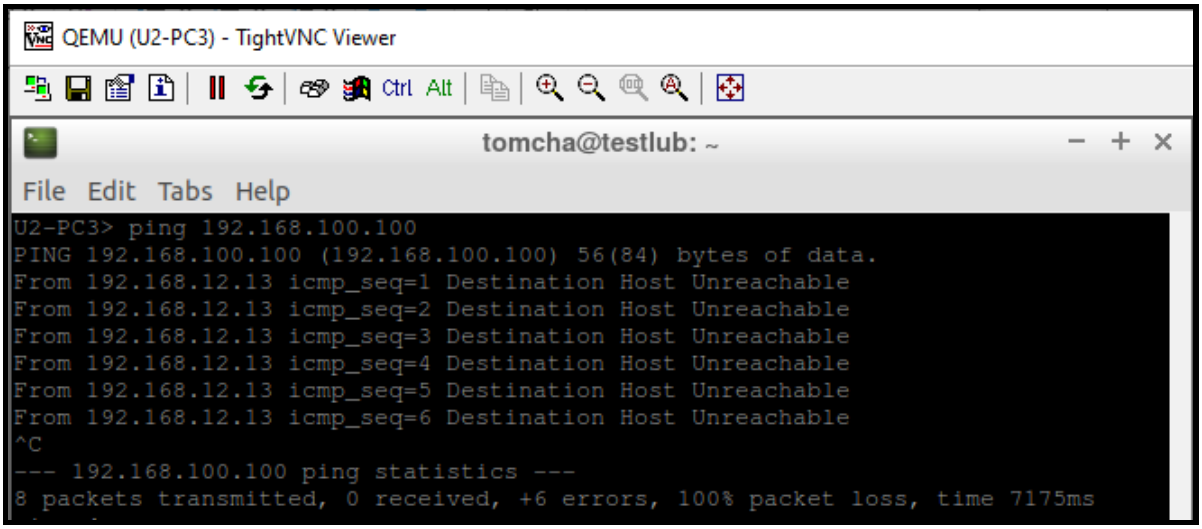
4.3.2 Úvodní projev

Úvodním projevem této závady ve školní síti bude pravděpodobně neschopnost připojení k jakékoliv internetové službě ze všech počítačů v Učebně 2 (obecně se závada projeví na všech zařízeních za přerušením).



Obrázek 4 – Neschopnost prohlížení webové stránky na U2-PC3

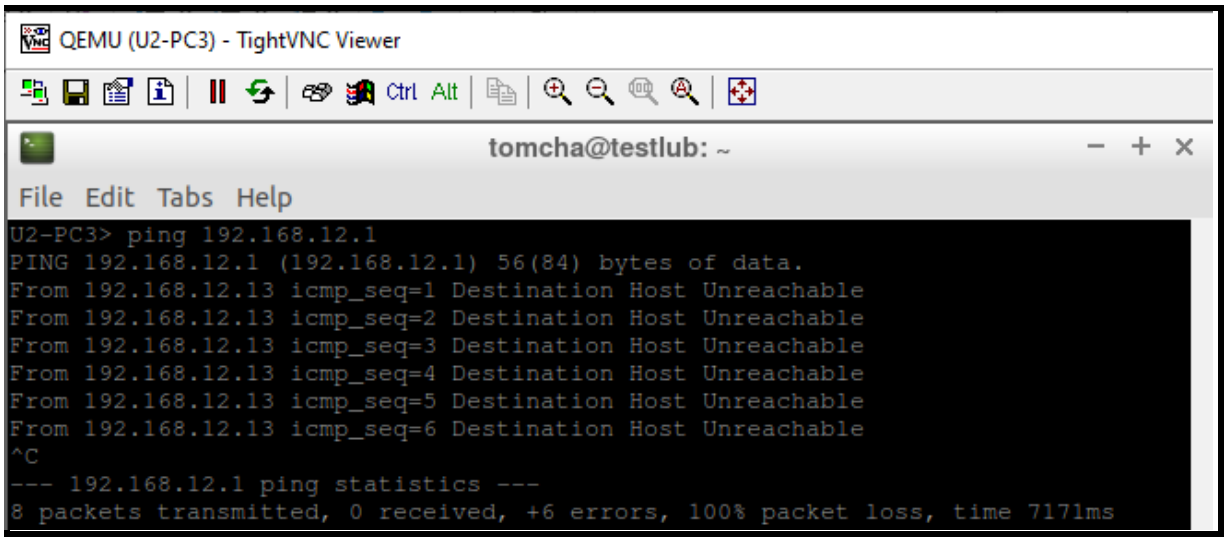
Souběžným projevem bude neschopnost dosáhnout vnitřního serveru školy v DMZ – nebude fungovat přístup ke školním diskům nebo k výukovým aplikacím (obecně nebude fungovat přístup ke zdrojům za přerušením).



Obrázek 5 – Neschopnost připojení k vnitřnímu serveru z U2-PC3

4.3.3 Diagnostika

Diagnostiku závady zahájíme zkouškou dostupnosti výchozí brány sítě, ve které se nachází postižený počítač. K tomuto účelu nejsnáze poslouží PING.



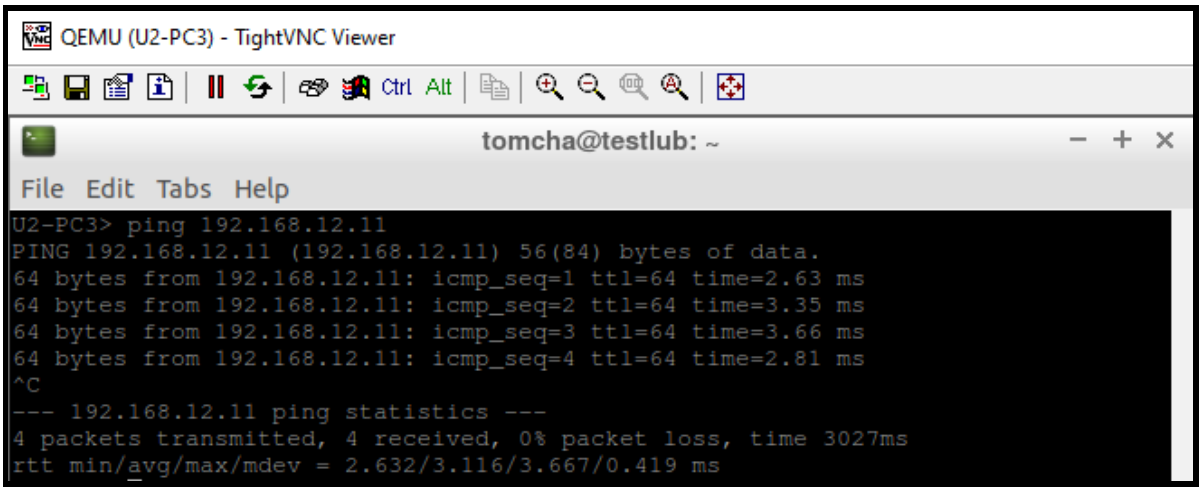
Obrázek 6 – PING z U2-PC3 na vnitřní rozhraní Router-Skola

Odpovědí na PING je ICMP Destination Host Unreachable od sebe samotného (počítače U2-PC3). Taková odpověď ukazuje na neschopnost počítače získat MAC adresu výchozí brány sítě prostřednictvím ARP. Touto odpovědí získáváme podezření na ztrátu konektivity mezi:

- Počítačem U2-PC3 a přístupovým switchem Sw3
- Přístupovým switchem Sw3 a přístupovým switchem Sw2

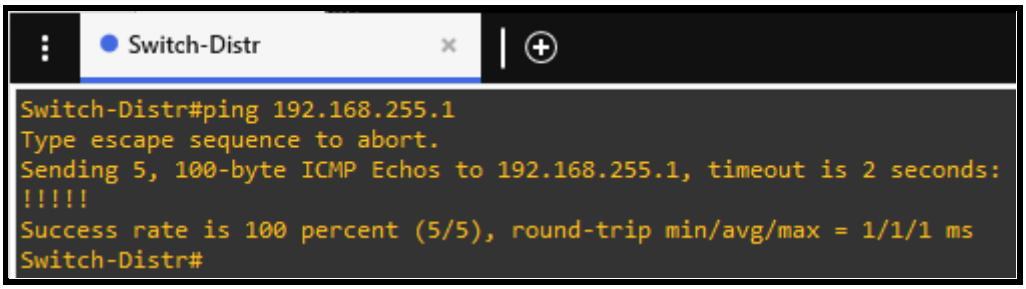
- Přístupovým switchem Sw2 a distribučním switchem Switch-Distr
- Distribučním switchem Switch-Distr a routerem Router-Skola

Konektivitu mezi přístupovým switchem a počítačem snadno ověříme PINGem mezi počítači U2-PC3 a U2-PC1. Tímto diagnostickým pokusem navíc ověříme i konektivitu mezi oběma přístupovými switchi Sw2 a Sw3 – oba počítače jsou připojené do různých switchů, tudíž jestliže funguje konektivita mezi počítači, musí nutně fungovat i konektivita mezi switchi.



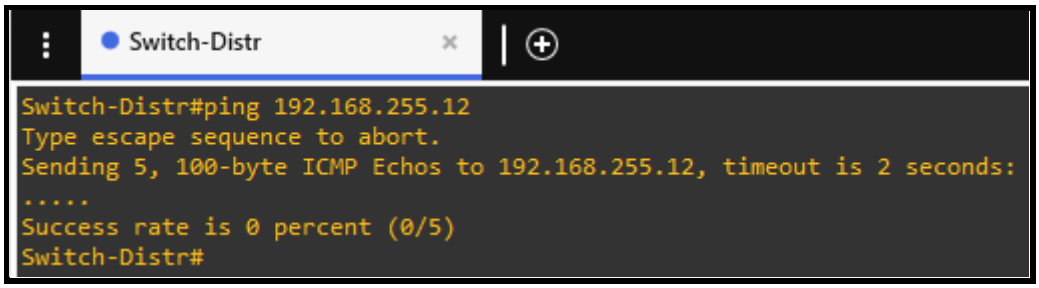
Obrázek 7 – PING mezi počítači v Učebně 2

Podobně snadno můžeme vyloučit ztrátu spojení mezi distribučním switchem a routerem prostřednictvím PINGu ze Switch-Distr na vnitřní rozhraní Router-Skola.



Obrázek 8 – PING ze Switch-Distr na vnitřní rozhraní Router-Skola

Podobně jako v předchozím případě PING řádně prošel, tudíž problém se s velkou pravděpodobností nachází mezi switchem Sw2 a distribučním switchem Switch-Distr. Problém finálně potvrdíme a izolujeme pokusným PINGem mezi rozhraními pro správu switchů Sw2 a Switch-Distr.



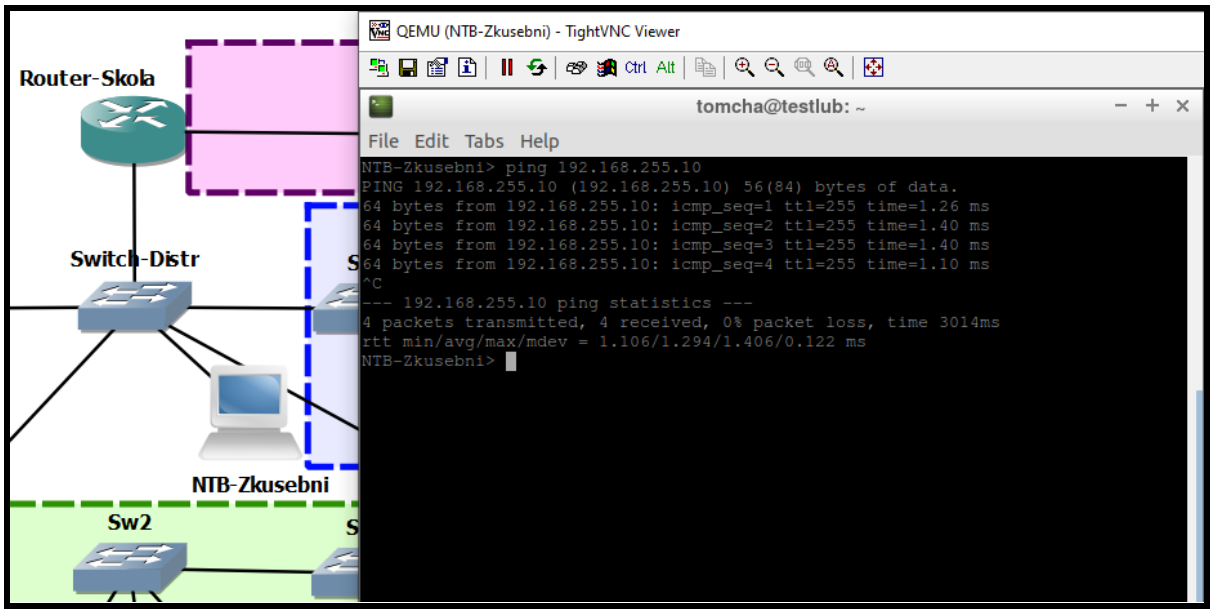
Obrázek 9 – PING ze Switch-Distr na rozhraní pro správu switche Sw2

Neúspěšný výsledek potvrzuje teorii o závadě na spoji. Vhodným nástrojem pro kontrolu spojení by byl ukazatel stavů fyzické vrstvy (informaci bychom získali buďto výstupem z rozhraní pro správu, nebo pohledem na LED diody na portech). Ukazatele fyzické vrstvy však v emulovaném prostředí nefungují (stejně tak by nemusely fungovat v případě jednosměrného optického spoje), proto se na ně nelze spolehnout.

Obrázek 10 – Výpis stavů rozhraní switche Sw2

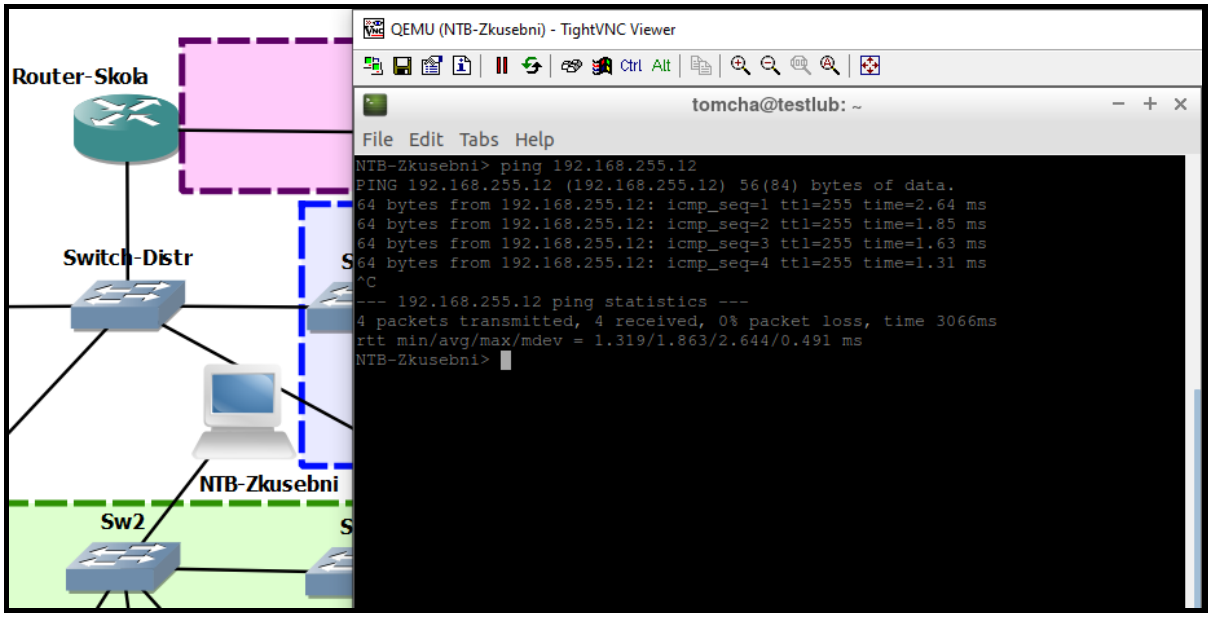
Přítomnost závady na spoji definitivně potvrdíme použitím jiného zařízení (např. notebooku), které připojíme postupně na jeden a druhý konec a nakonfigurujeme na IP adresu příslušného rozhraní. Oba switche Sw3 a Switch-Distr mají své rozhraní pro správu (virtuální síťová karta pro VLAN 255) ve VLAN 255, která je na všech trunk portech nastavená jako nativní (tj. přenáší se bez VLAN tagu). Díky tomuto nastavení není nutné na zkušebním zařízení nastavovat VLAN tag.

Při prvním diagnostickém pokusu nastavíme zkušební zařízení na IP adresu switche Sw2 (192.168.255.12) a připojíme ho do stejného portu distribučního switche Switch-Distr, do kterého byl připojen Sw2. Následně ze zkušebního zařízení vyšleme PING na adresu management rozhraní distribučního switche (192.168.255.10).



Obrázek 11 – PING ze zkušebního zařízení na rozhraní pro správu switche Switch-Distr

PING řádně prošel. Závada však může být ještě na portu switche Sw2, a proto pro druhý pokus situaci obrátíme – zkušební zařízení nastavíme na IP adresu rozhraní pro správu Switch-Distr a připojíme ho do portu Sw2, do kterého byl předtím připojen Switch-Distr. Opět vyzkoušíme PING.



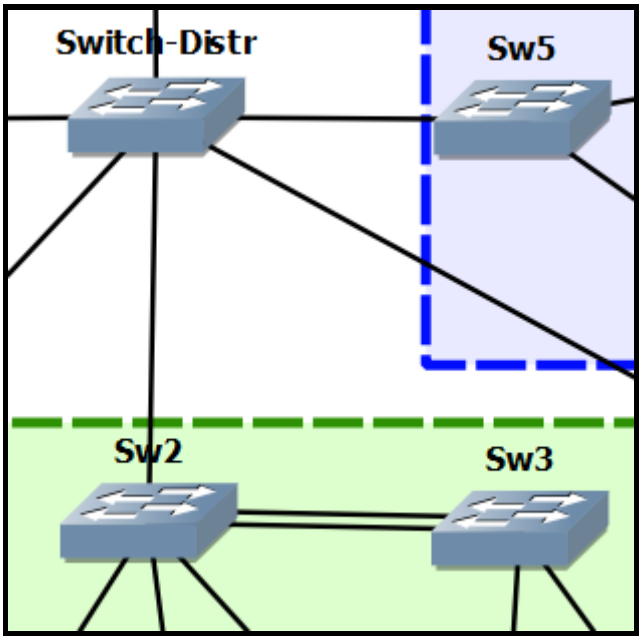
Obrázek 12 – PING ze zkušebního zařízení na rozhraní pro správu switche Sw2

Úspěšný výsledek obou PINGů potvrzuje závadu na spoji mezi Sw2 a Switch-Distr.

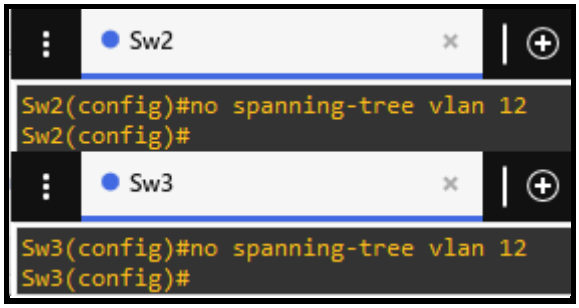
4.4 Diagnostika L2 smyčky

4.4.1 Navození závady

Smyčku na druhé vrstvě navodíme propojením switchů Sw2 a Sw3 nacházejících se ve stejné VLAN 12. Z praktického hlediska by bylo vhodnější propojení dvou portů v rámci jedné VLAN jednoho switche (taková situace by v praxi odpovídala propojení dvou sousedních zdířek ve zdi např. při úklidu), avšak použitý emulátor GNS3 toto neumožňuje. Projevy však budou v obou případech velmi podobné. Výchozí nastavení virtuálních switchů použitých v topologii obsahuje zapnutý STP, a proto je nutné jeho ruční vypnutí.



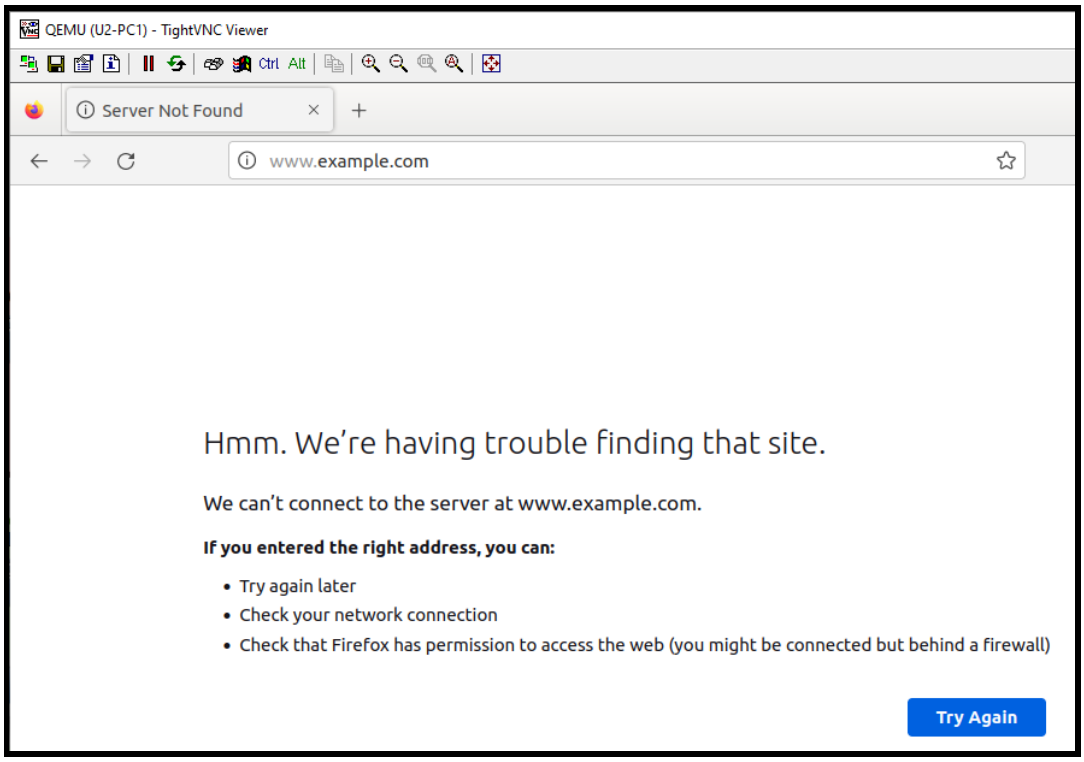
Obrázek 13 – Přidání nadbytečného spoje mezi Sw2 a Sw3



Obrázek 14 – Vypnutí STP na switchích Sw2 a Sw3

4.4.2 Úvodní projev

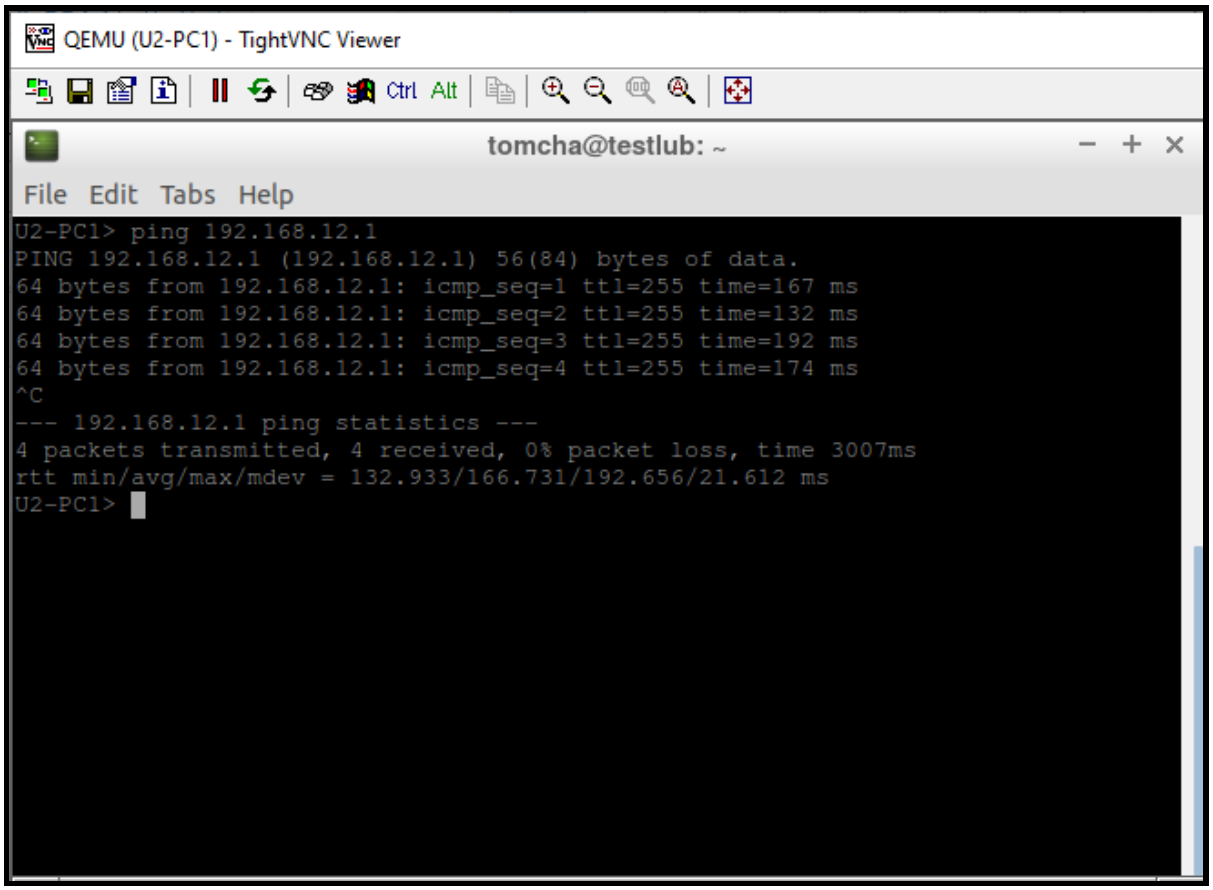
Prvním projevem závady bude zřejmě nedostupnost (nebo velmi omezená dostupnost) služeb internetu na postiženém segmentu. Kvůli vysokému vytížení procesorů switchů se závada může propagovat i do ostatních, smyčkou nepostižených segmentů. V takovém případě může dojít i k nedostupnosti vnitřních zdrojů.



Obrázek 15 – Neschopnost prohlížení webové stránky na U2-PC1

4.4.3 Diagnostika

Stejně jako u jiné nedostupnosti vzdálené sítě začneme diagnostiku PINGem na výchozí bránu sítě postiženého stroje.

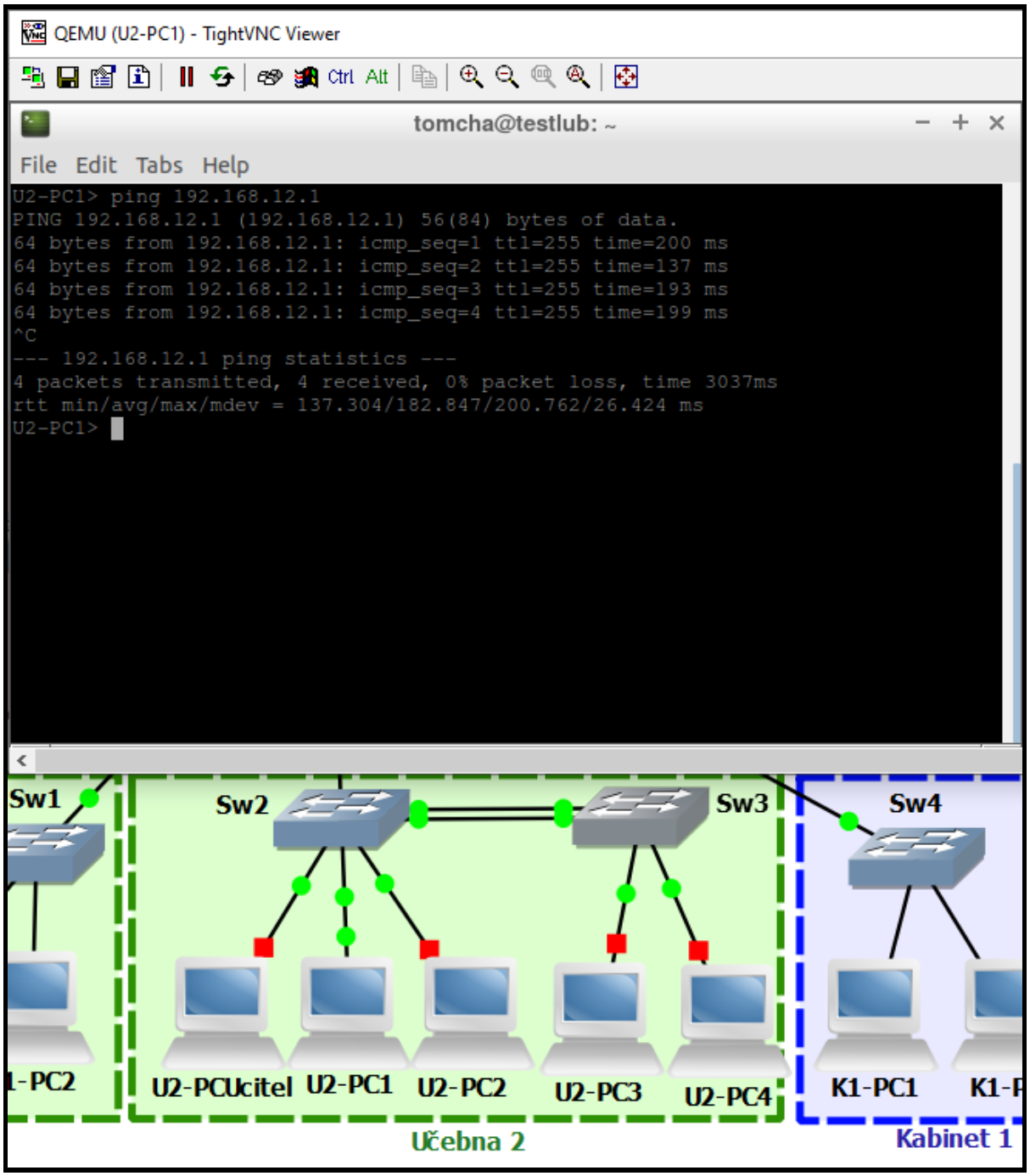


Obrázek 16 – PING z U2-PC1 na vnitřní rozhraní Router-Skola

Extrémně vysoká latence a její kolísání jasně poukazuje na vysoké vytížení sítě nebo její části. Vysoké vytížení v takové situaci může mít několik příčin. Mezi ty nejpravděpodobnější patří např.:

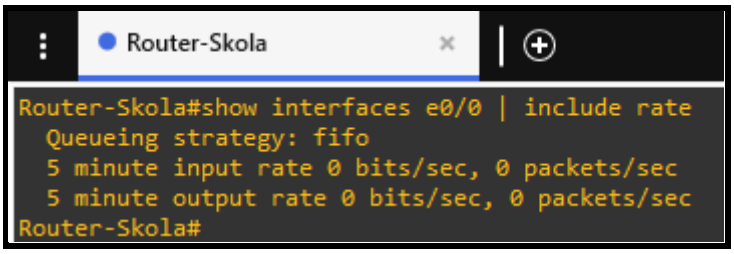
- Prosté přetížení
- DDoS útok (z vnějšku sítě)
- Plná tabulka MAC adres na switchi
- L2 smyčka

Přetížení snadno vyloučíme vypnutím všech počítačů v učebně kromě jednoho, ze kterého opět provedeme PING na bránu.



Obrázek 17 – PING z U2-PC1 na vnitřní rozhraní Router-Skola po vypnutí ostatních PC

Protože problém nadále přetrvává, prosté přetížení pravděpodobně není příčinou problému. Jako další možnost diagnostiky lze vyloučit kybernetický útok z vnějšku sítě. To lze nedisruptivně (tj. bez přerušení provozu zbývající funkční části sítě) provést kontrolou příchozího provozu na vnější rozhraní brány Router-Skola.

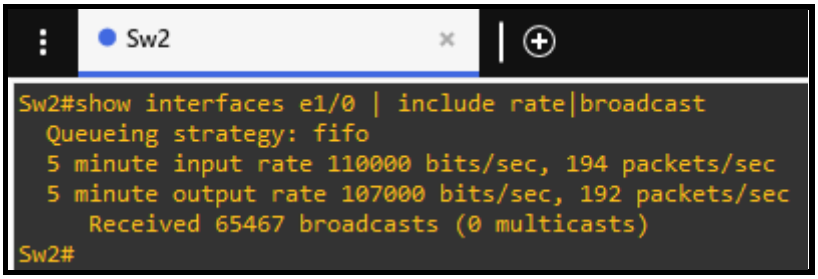


Obrázek 18 – Výpis množství provozu z vnějšího rozhraní Router-Skola

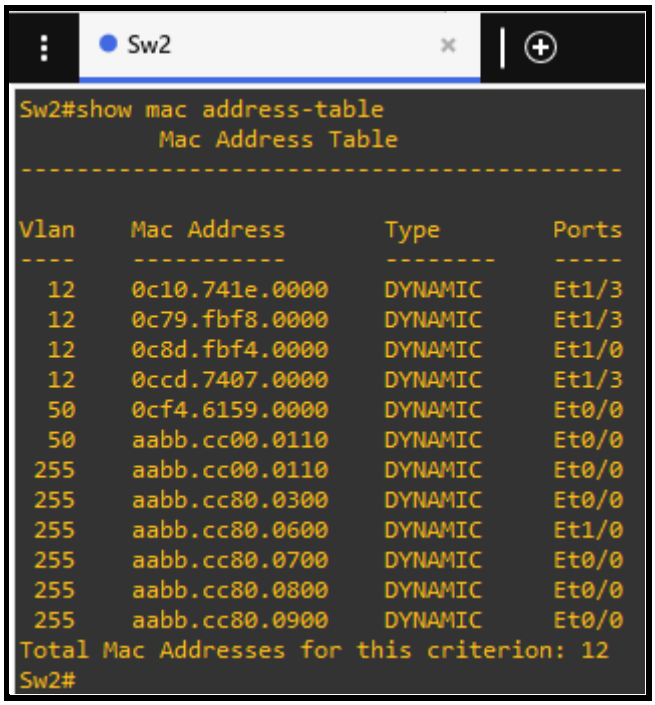
Disruptivně lze toto ověření provést dočasným odpojením spoje mezi Routerem-Skola a Routerem-ISP nebo Routerem-Skola a distribučním switchem Switch-Distr. V obou případech se útok z vnějšku nepotvrdí (množství příchozího i odchozího provozu vnějšího rozhraní brány je v běžných hodnotách a odpojení sítě od vnějšku nevede k vyřešení závady).

Přetížení by mohlo být následkem také přeplnění tabulky MAC adres na některém ze switchů. V takovém případě by se switch začal chovat jako hub, tj. unicastový příchozí provoz by začal být vyplavován na všechny porty, kromě příchozího portu. Toto vyplavování by mohlo způsobit projevy závady. U nespravovatelného switche není možné tabulku MAC adres nijak zobrazit – jedinou možností je tedy takovýto switch restartovat. U spravovatelného switche si můžeme tabulku zobrazit a zkontrolovat počet záznamů, zda odpovídá očekávané hodnotě.

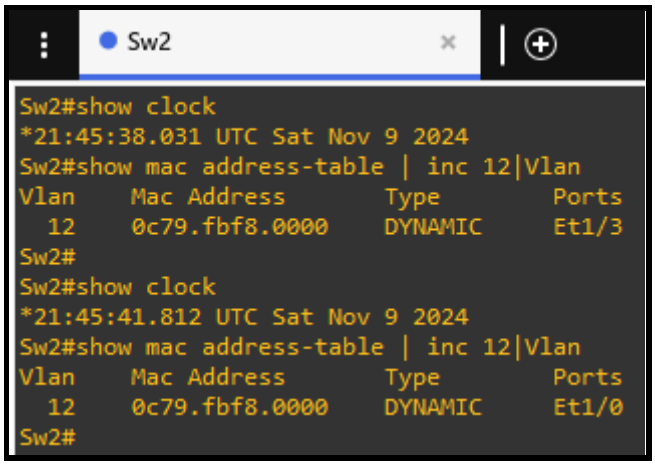
Jako další pravděpodobná možnost se nabízí smyčka na druhé vrstvě. Máme-li přístup ke správě některého ze switchů, který se nachází v postiženém segmentu, lze tuto příčinu problémů potvrdit snadno. Vhodně poslouží zobrazení vytížení portů nebo zobrazení tabulky MAC adres v různých časech.



Obrázek 19 – Výpis množství provozu z rozhraní switche Sw2, kterým je připojen postižený počítač U2-PC1

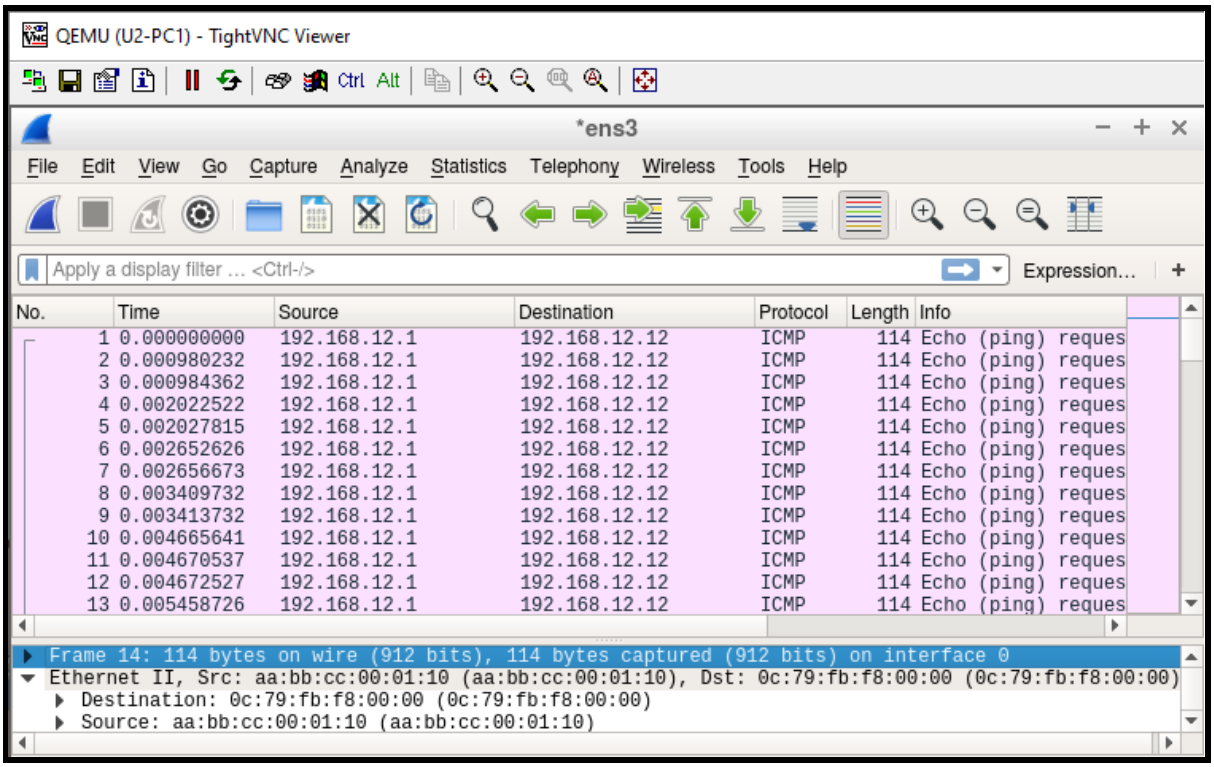


Obrázek 20 – Výpis tabulky MAC adres switche Sw2



Obrázek 21 – Výpis změn tabulky MAC adres switche Sw2 v čase

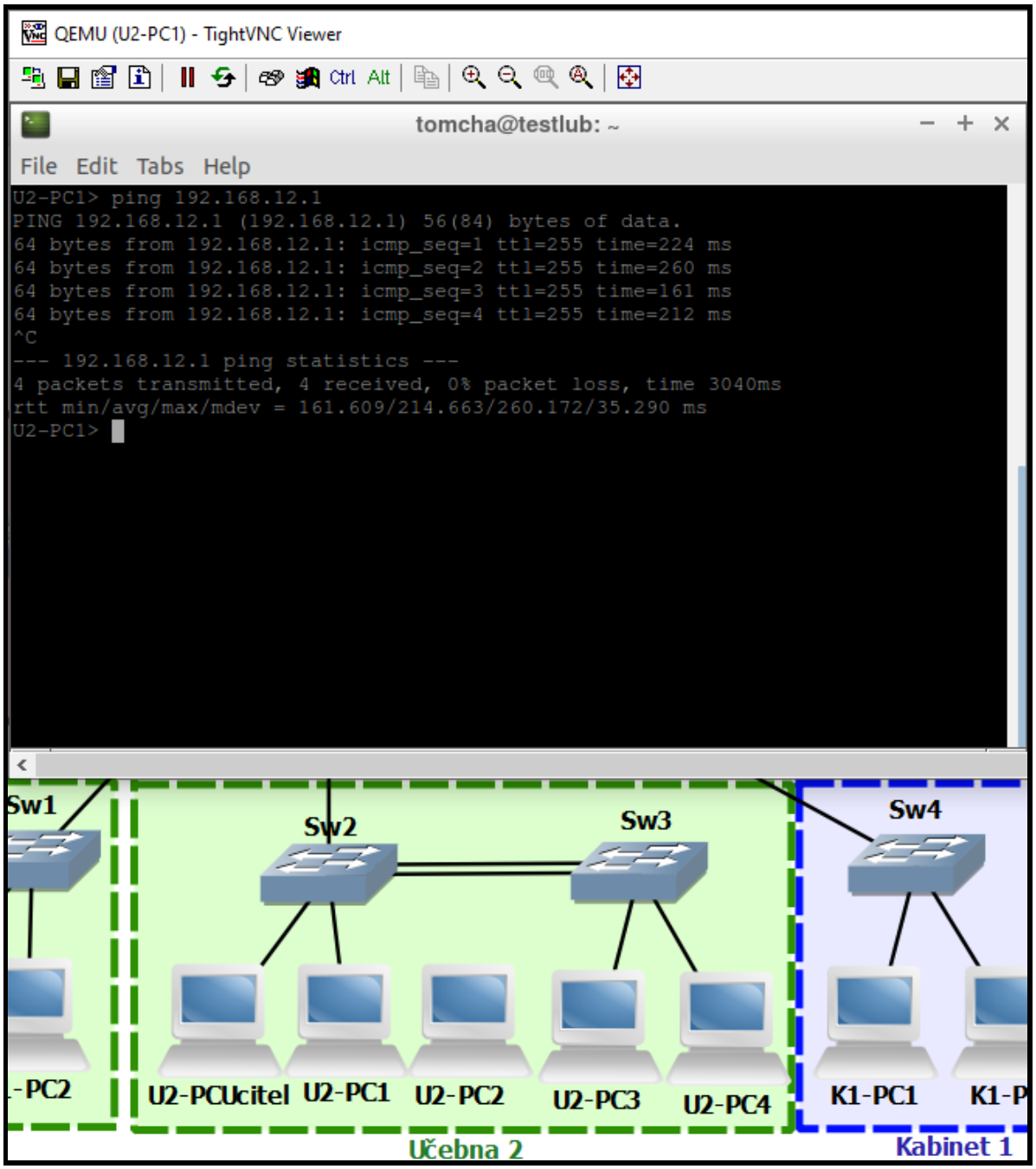
Změna záznamů v tabulce adres v krátkém čase (tzv. MAC flapping) a vysoké vytížení portů s vysokým počtem broadcastů potvrzují příčinu závady jako smyčku na druhé vrstvě. Počet záznamů je v rámci očekávaných hodnot, a proto přetečení tabulky tohoto switche není pravděpodobnou příčinou závady. Nemáme-li k dispozici připojení ke správě žádného ze switchů v postiženém úseku sítě, lze spustit Wireshark na libovolném počítači v postiženém úseku.



Obrázek 22 – Výpis zachyceného duplicitního provozu pomocí Wiresharku na U2-PC1

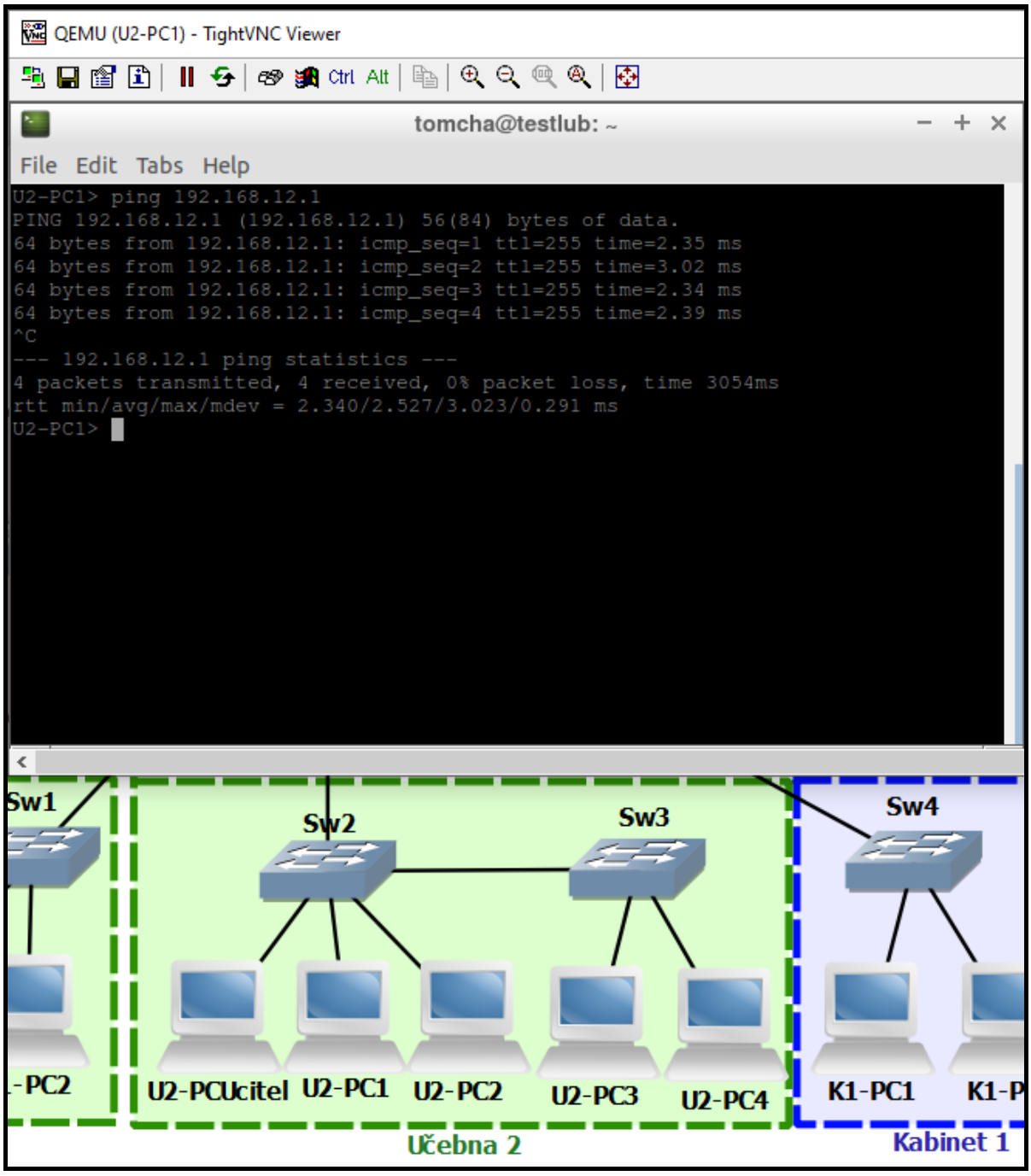
Velké množství duplicitního provozu (zde vícenásobné kopie jednoho ICMP Echo Request packetu přijaté ve velmi krátkém časovém úseku) ve výpisu provozu potvrzuje příčinu závady jako L2 smyčku. Pokud jsou ve výpise vidět vícenásobné kopie stejných rámců, L2 smyčka je prakticky s jistotou potvrzena.

Závadu lze odhalit i bez použití nástrojů (a zároveň jí tím i odstranit) postupným odpojováním kabelů ze switche v postiženém úseku. Odpojení kabelu, který není součástí smyčky nepovede k odstranění projevů závady.



Obrázek 23 – PING z U2-PC1 na vnitřní rozhraní Router-Skola po odpojení chybného kabelu

Odpojení kabelu, který tvoří smyčku, v ideálním případě vede k odstranění závady.



Obrázek 24 – PING z U2-PC1 na vnitřní rozhraní Router-Skola po odpojení kabelu tvořícího smyčku

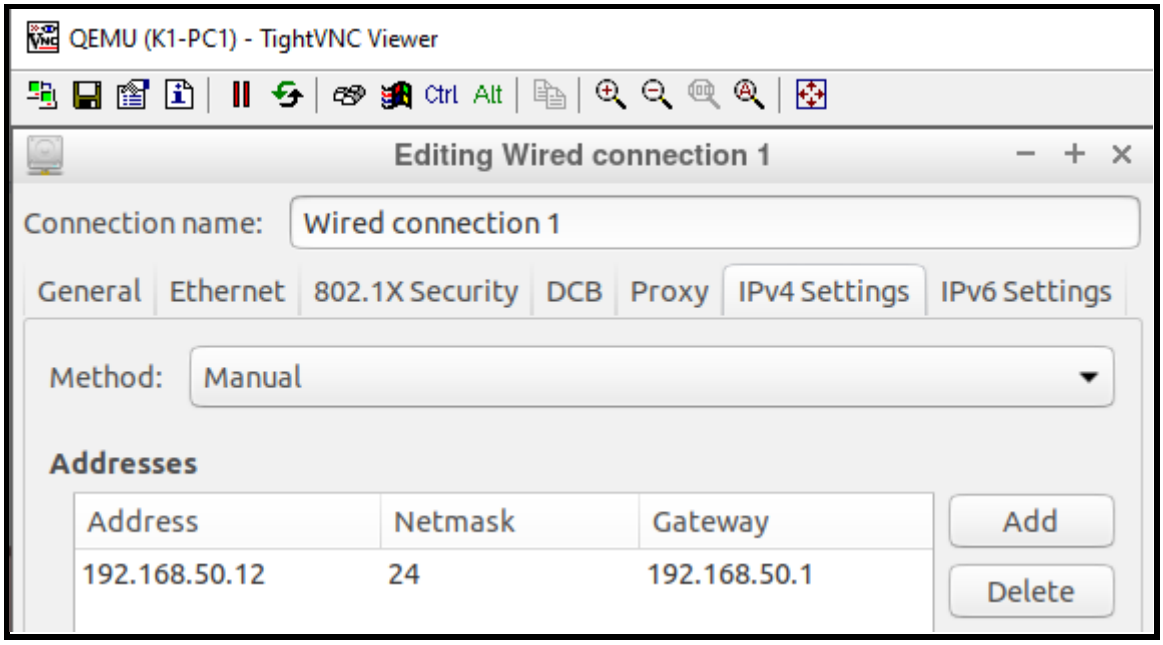
Rozpojením smyčky projevy závady vymizí. V praxi může být vhodné restartovat zařízení ve smyčkou postiženém úseku (vlivem extrémního množství provozu mohlo dojít k softwarové chybě, zejm. u levnějších zařízení nerenomovaných výrobců).

4.5 Diagnostika duplicitní IP adresy

4.5.1 Navození závady

Duplicitní IP adresu v místní síti navodíme snadno statickým nastavením adresy některého z počítačů na jinou IP adresu, která je v daném L2 segmentu již použitá. Pro účely navození

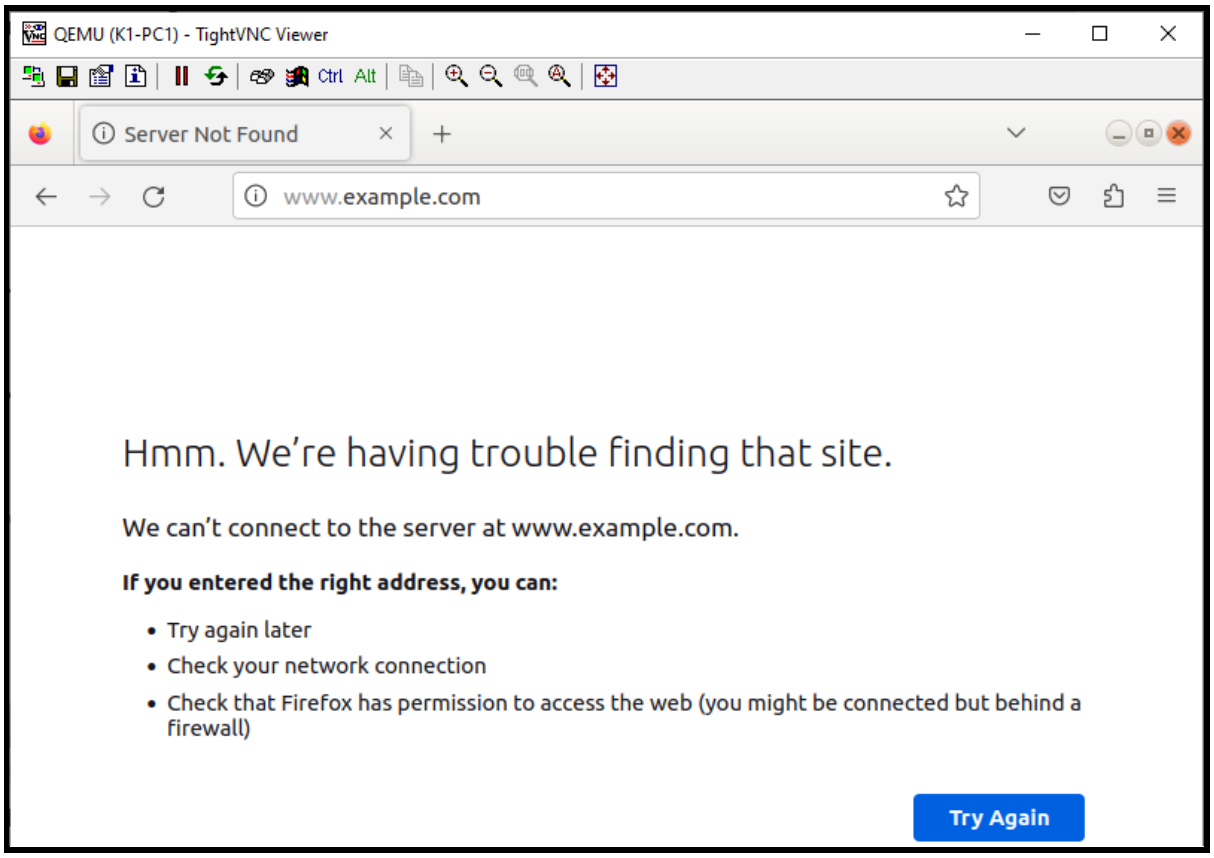
této závady nastavíme IP adresu počítače K1-PC1 na již použitou adresu počítače K1-PC2 (192.168.50.12/24).



Obrázek 25 – Nastavení duplicitní IP adresy počítače K1-PC1

4.5.2 Úvodní projev

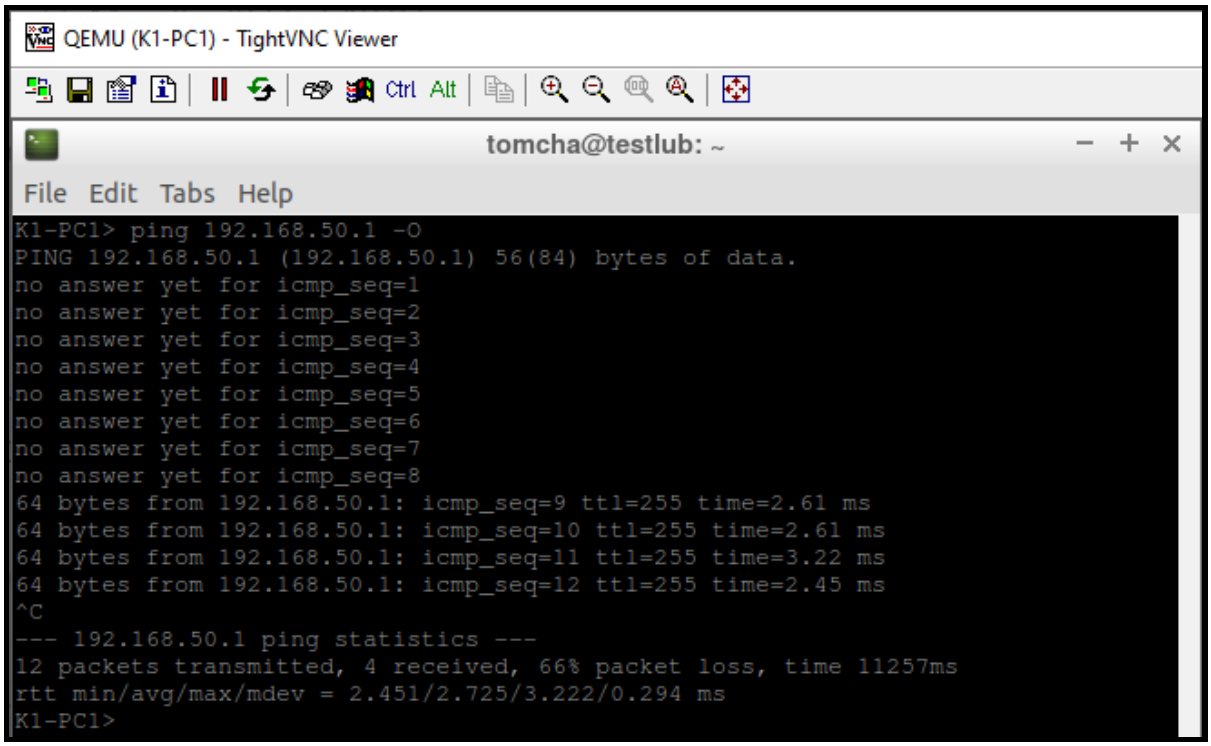
Nejpravděpodobnějším prvním projevem duplicitní IP adresy bude úplná neschopnost jednoho z počítačů komunikovat s vnějšími sítěmi. Jediný počítač sdílející duplicitní IP adresu schopný komunikovat ven bude ten počítač, jehož MAC adresa (resp. MAC adresa jeho síťové karty) bude v danou chvíli v ARP záznamu Routeru-Skola pro danou duplicitní adresu. Všechny ostatní počítače sdílející duplicitní adresu nebudou schopny komunikovat ven.



Obrázek 26 – Neschopnost prohlížení webové stránky na K1-PC1

4.5.3 Diagnostika

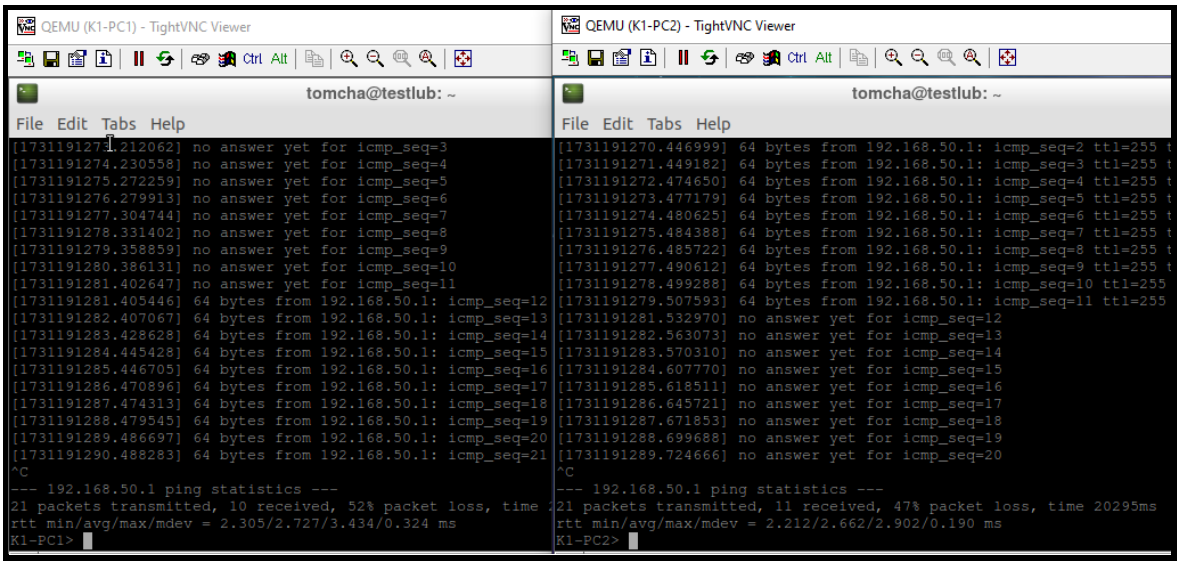
Protože nelze komunikovat s vnějšími sítěmi, vhodným úvodním diagnostickým pokusem bude PING na výchozí bránu, tj. na adresu 192.168.50.1.



Obrázek 27 – PING z K2-PC1 na vnitřní rozhraní Router-Skola

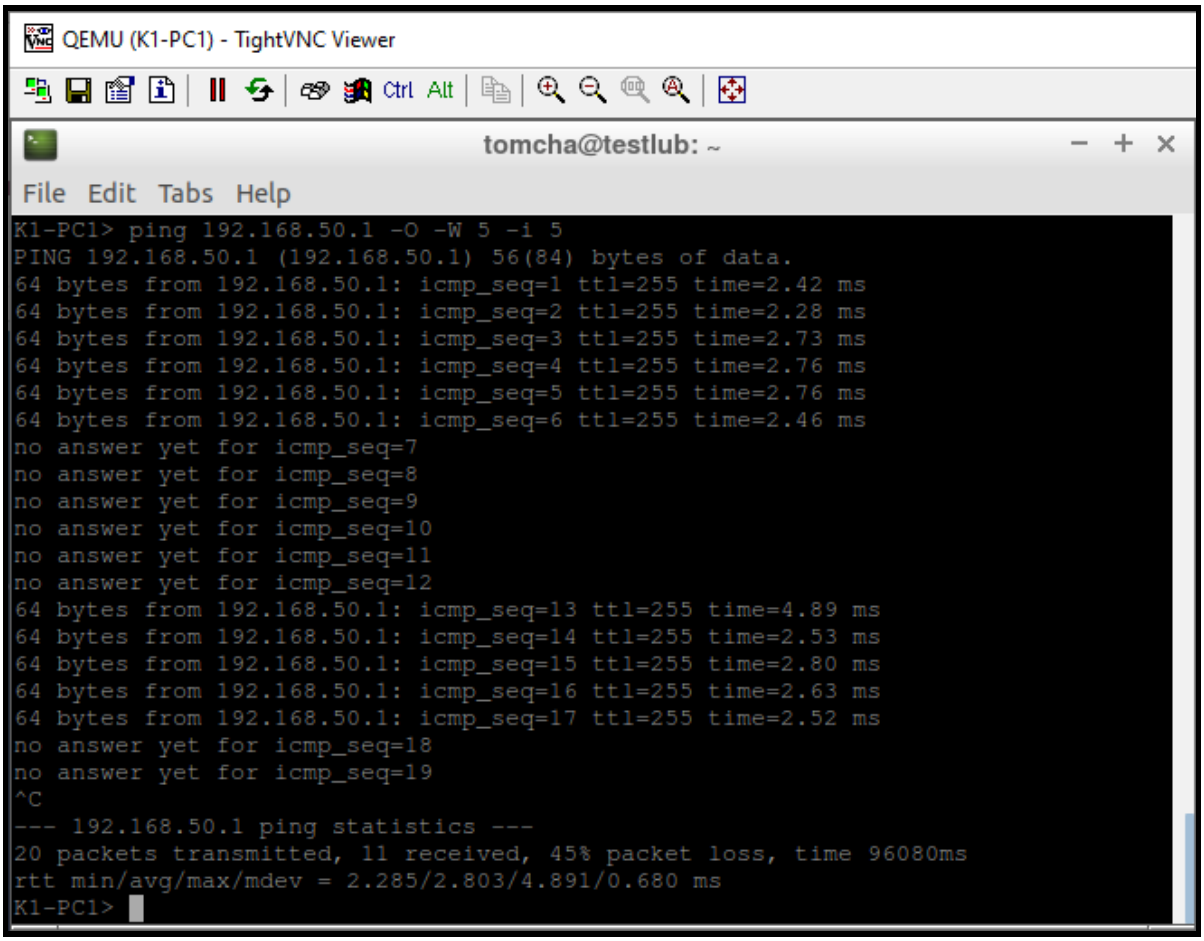
Několik prvních packetů bylo ztraceno, avšak po chvíli začalo spojení fungovat řádně. Vysoká míra ztráty packetů může svědčit pro možné přetížení sítě. Přetížení je však spojeno i s vysokou kolísající latencí, což zde není přítomné. Tyto projevy jsou pro přetížení typické a jejich nepřítomnost jej prakticky vylučuje.

V čase, ve kterém spojení z K1-PC1 funguje, přestane fungovat spojení na druhém počítači sdílejícím duplicitní adresu, zde K1-PC2. Takováto proměnlivost projevů v čase zcela typicky svědčí pro duplicitní IP adresu (není-li pro ni v daném kontextu jiné zřejmé vysvětlení).



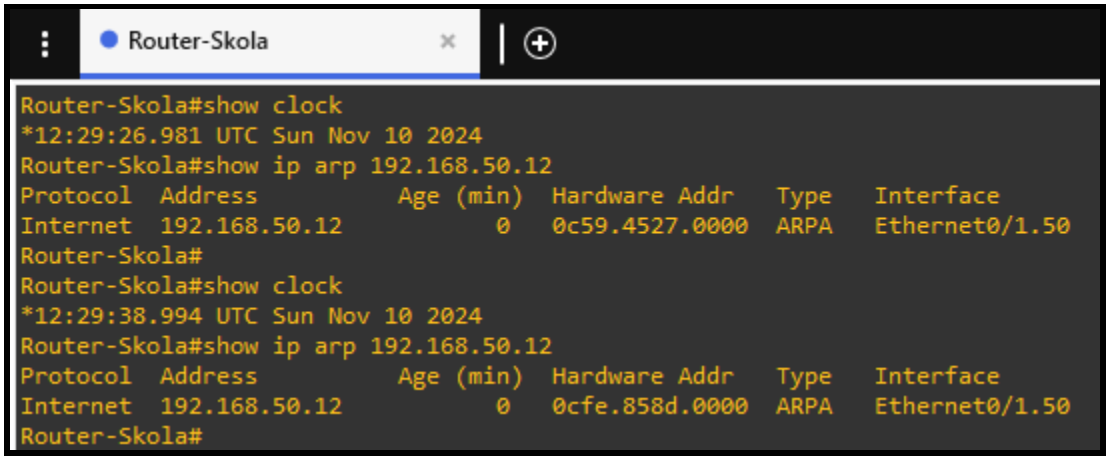
Obrázek 28 – Změna komunikujícího zařízení v čase

Necháme-li PING na libovolném počítači sdílejícím duplicitní IP adresu běžet delší dobu, uvidíme zde periody, během kterých spojení funguje dobře, střídané periodami, během kterých spojení nefunguje.



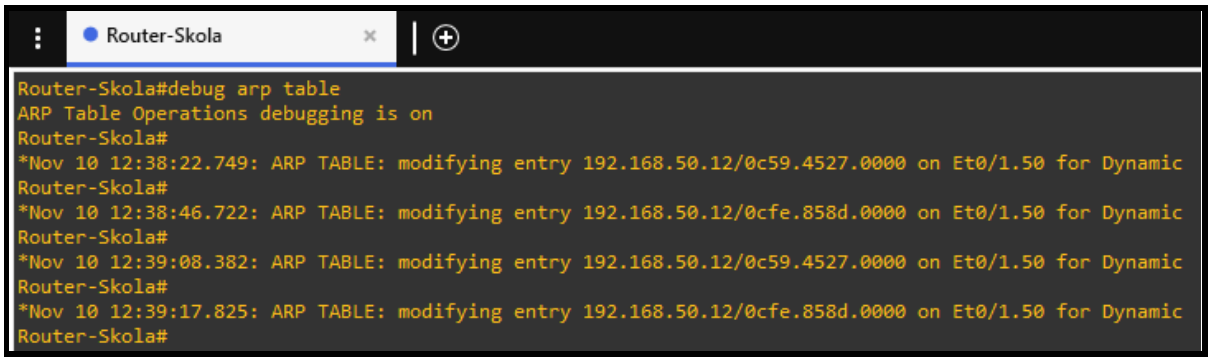
Obrázek 29 – Proměnlivost projevů v čase

Použitím pokročilejších nástrojů lze závadu diagnostikovat přesněji. Vhodně poslouží zobrazení ARP tabulky Routeru-Skola, konkrétně záznamů pro IP adresu, u které předpokládáme, že ji sdílí více zařízení. Opakované výpisy v různých časech mohou prokázat změny MAC adresy pro daný záznam.



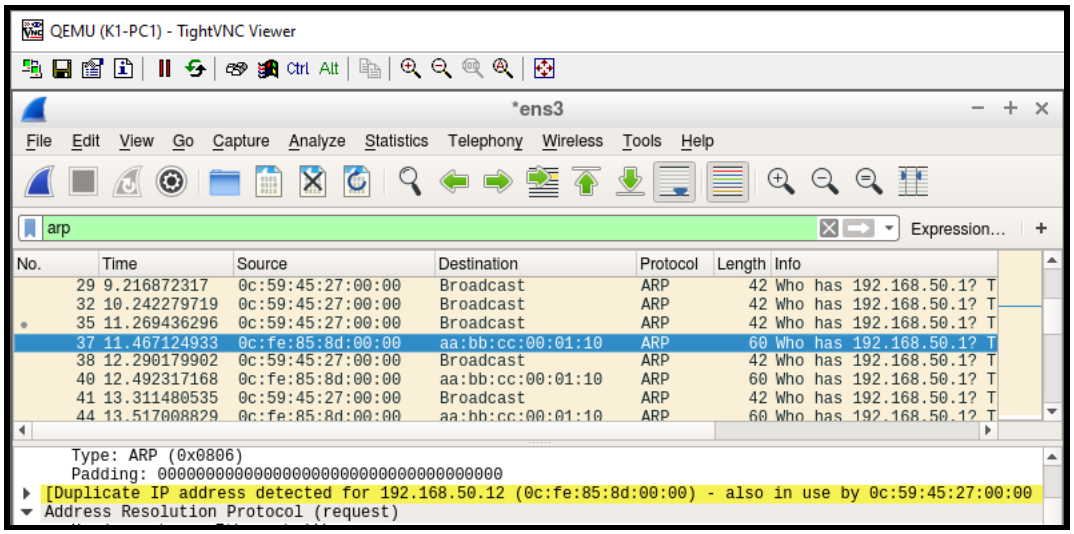
Obrázek 30 – Změny ARP záznamů Router-Skola pro duplicitní IP adresu v čase

Závadu pomůže upřesnit i živé ladění na Routeru-Skola – uvidíme v něm opakované změny ARP tabulky pro danou IP adresu. Výpis příhodně poskytuje i MAC adresy, které pomohou odhalit stroje sdílející duplicitní adresu.



Obrázek 31 – Ladění změn ARP tabulky routeru Router-Skola

Finálně lze závadu potvrdit sledováním provozu na síti prostřednictvím např. Wiresharku. Vhodným filtrováním ARP dotazů a odpovědí lze duplicitní adresu snadno odhalit.

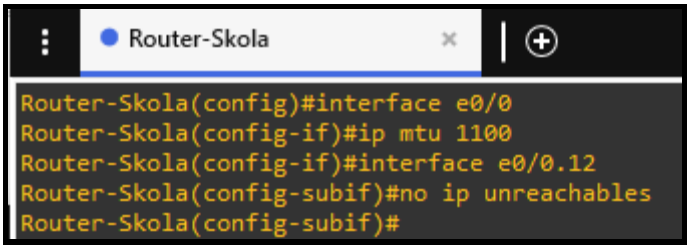


Obrázek 32 – Odhalení duplicitní IP adresy pomocí Wiresharku

4.6 Diagnostika excesivní fragmentace

4.6.1 Navození závady

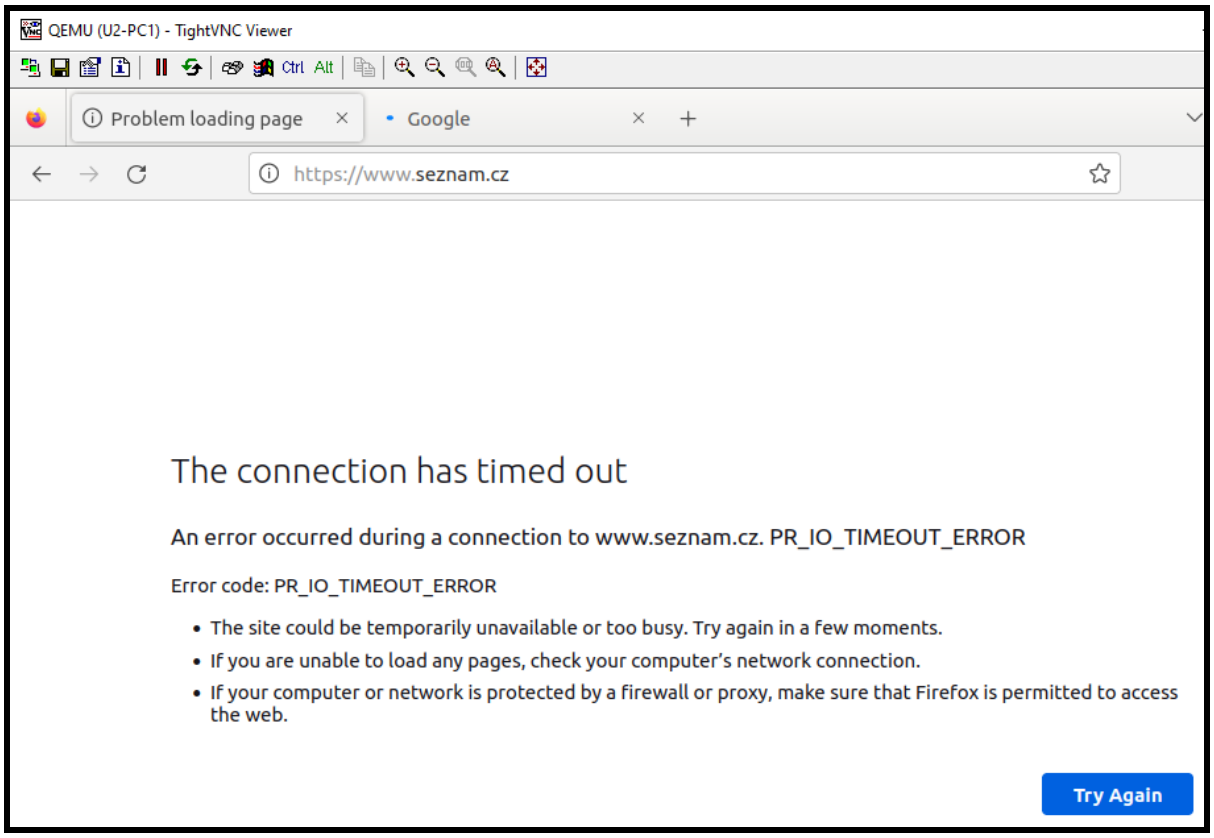
Závadu navodíme fixním nastavením MTU pro IP protokol na obou rozhraních spoje mezi Router-Skola a Router-ISP. Pro vyšší názornost zvolíme relativně nízkou hodnotu, zde 1100 bajtů. Za účelem vypnutí mechanizmu pro zjišťování MTU cesty vypneme zasílání zpráv ICMP Destination Unreachable na rozhraní Routeru-Skola, ke kterému je připojen zkušební počítač, ze kterého budeme provádět diagnostiku (U2-PC1).



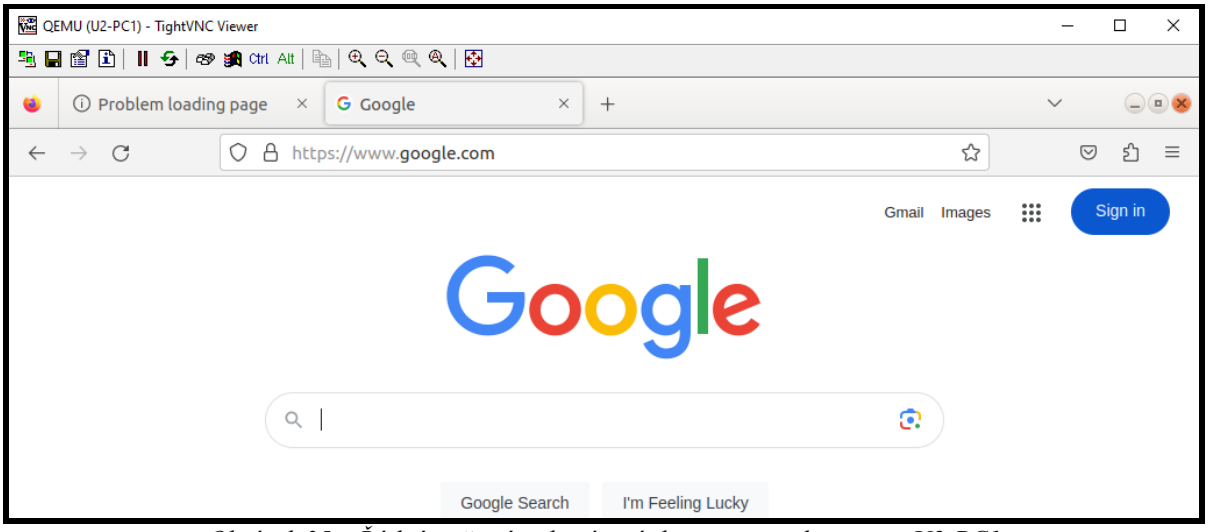
Obrázek 33 – Změna MTU a vypnutí zasílání ICMP Destination Unreachable zpráv na routeru Router-Skola

4.6.2 Úvodní projev

Prvním projevem této závady bude pravděpodobně omezená funkčnost webových stránek hostovaných mimo školní síť. Načtení některých webů bude fungovat, avšak pomaleji (kvůli fragmentaci). Jiné weby nebudou fungovat vůbec (spojení ihned uvázne zasláním velkého packetu a po nějaké době skončí vypršením času).



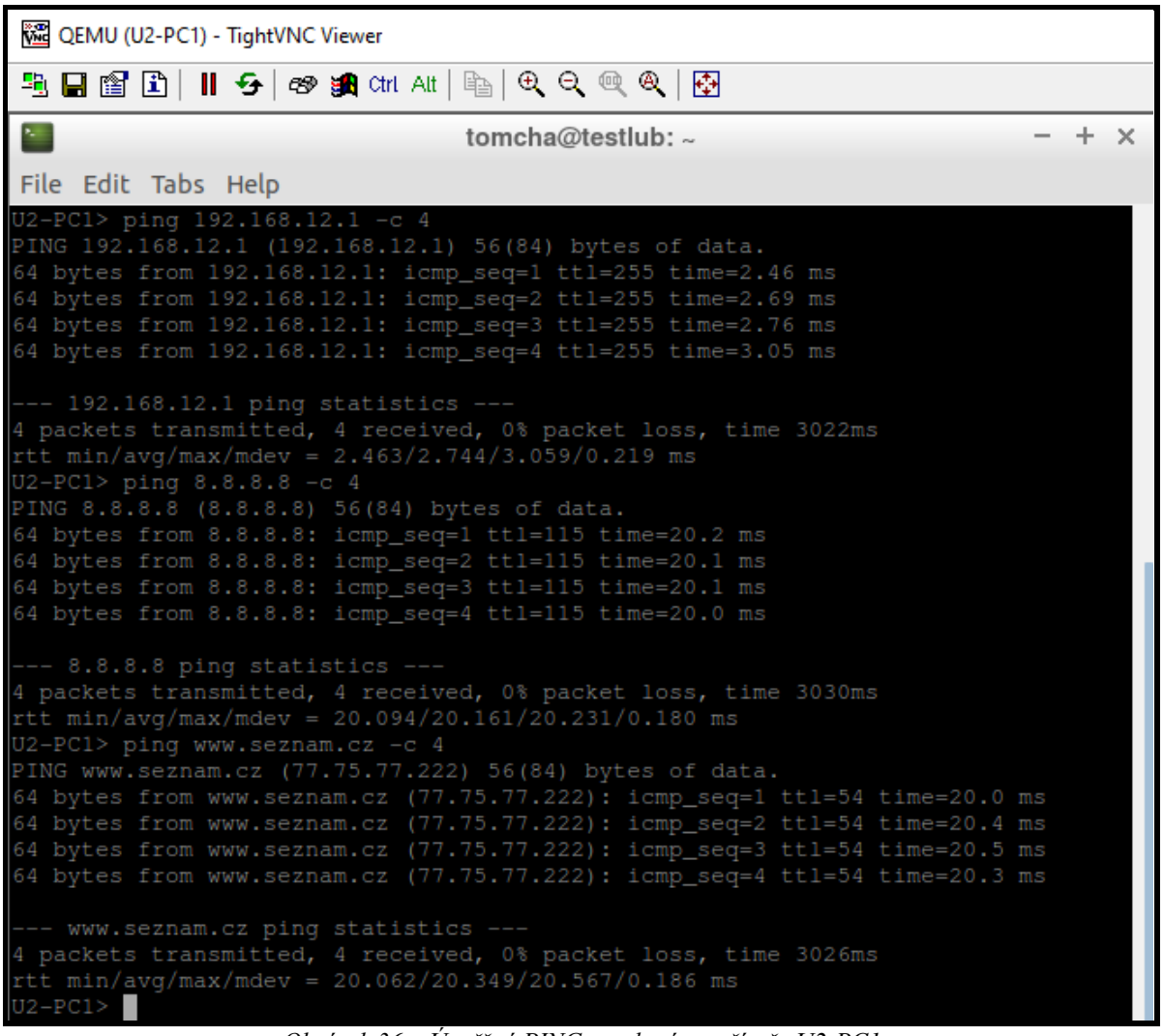
Obrázek 34 – Neschopnost prohlížení webové stránky www.seznam.cz na U2-PC1



Obrázek 35 – Řádné načtení webové stránky www.google.com na U2-PC1

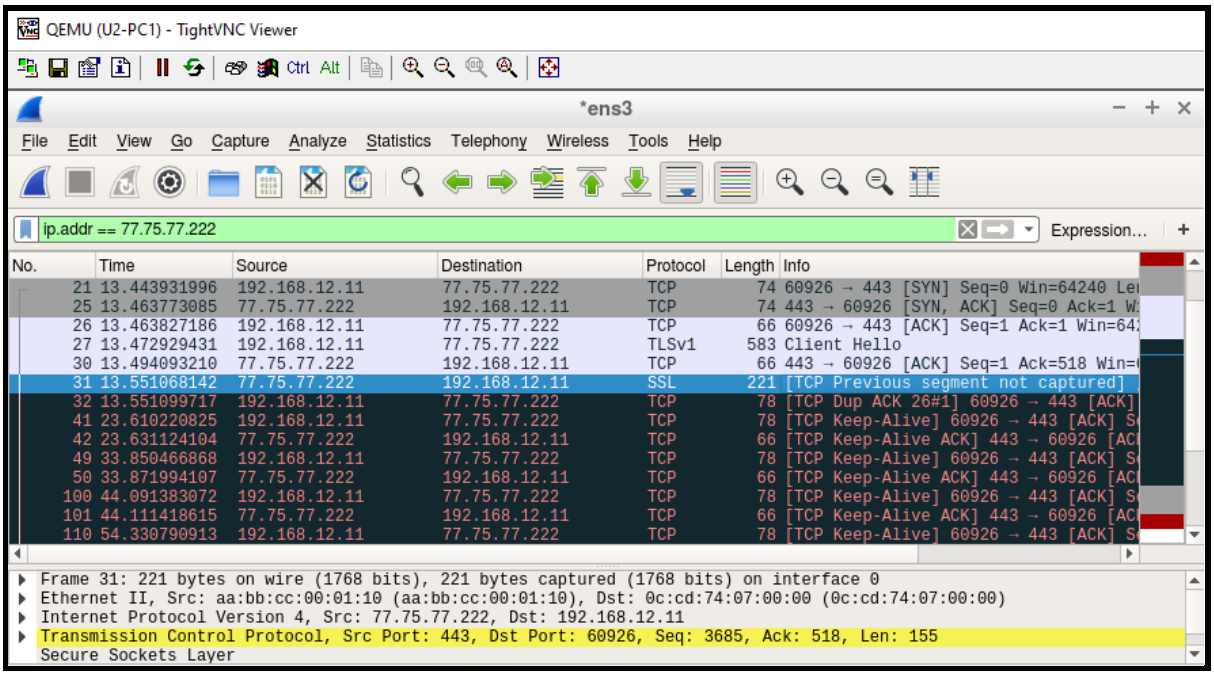
4.6.3 Diagnostika

Jestliže jedinou informací o závadě bude nefunkčnost webové stránky (tj. nedojde ke zjištění funkčnosti alespoň některých stránek nebo služeb), může být diagnostika této závady značně problematická. PING ve výchozím nastavení odesílá příliš malé packety ICMP Echo Request na to, aby se závada projevila. Zkušební PING na bránu bez potíží projde (zde by se ani závada nemohla projevit, týká se až vnějšího rozhraní), stejně jako PING na vzdálený server v internetu nebo i PING na adresu nefungující webové stránky (pokud je server nastaven tak, aby na PINGy odpovídal).



Obrázek 36 – Úspěšné PINGy vyslané z počítače U2-PC1

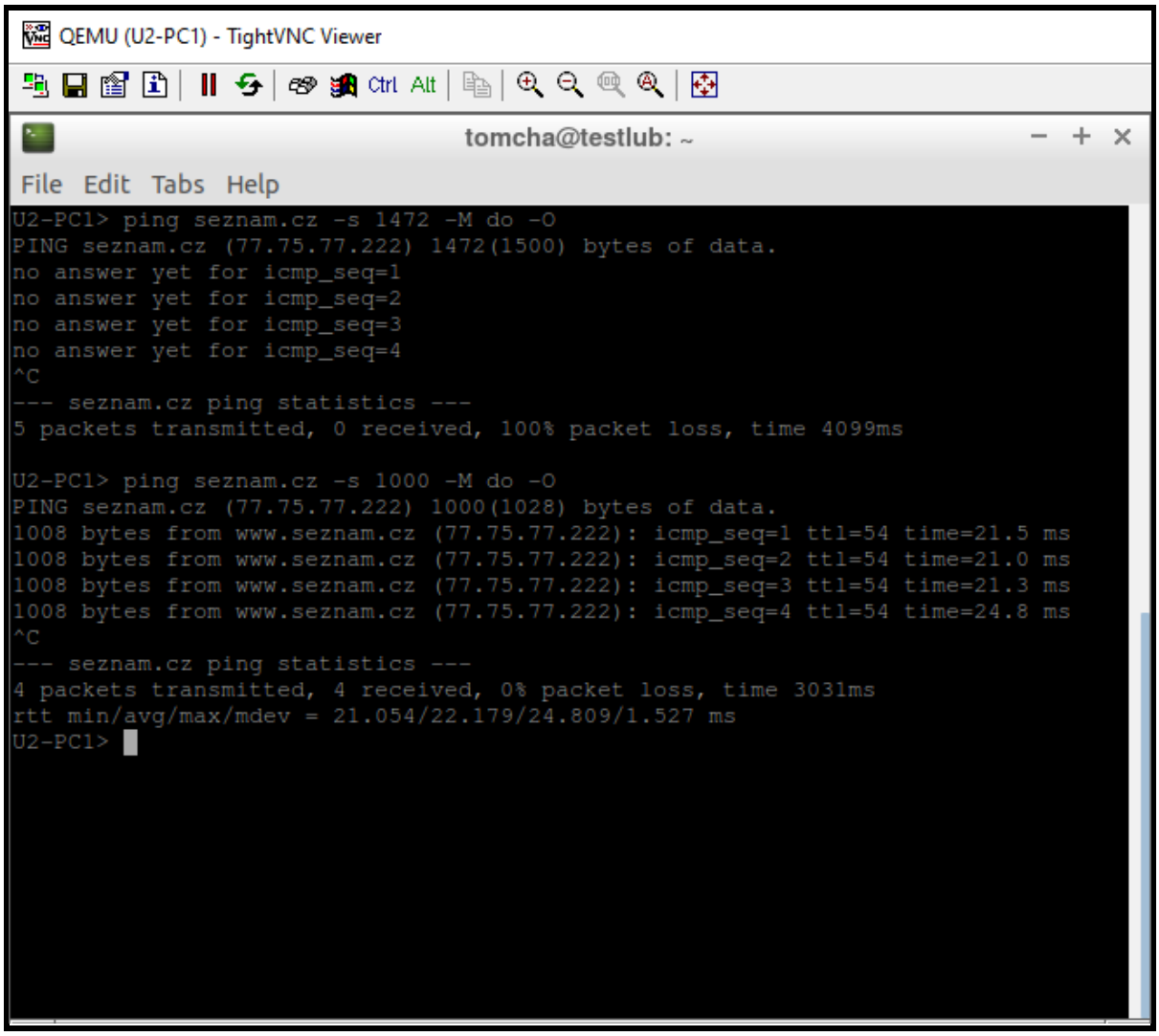
Vzdálený server nefungující stránky je dostupný. Vhodnou možností, jak odhalit příčinu závady, může být použití Wiresharku.



Obrázek 37 – Výpis TCP provozu z počítače U2-PC1 pomocí Wiresharku

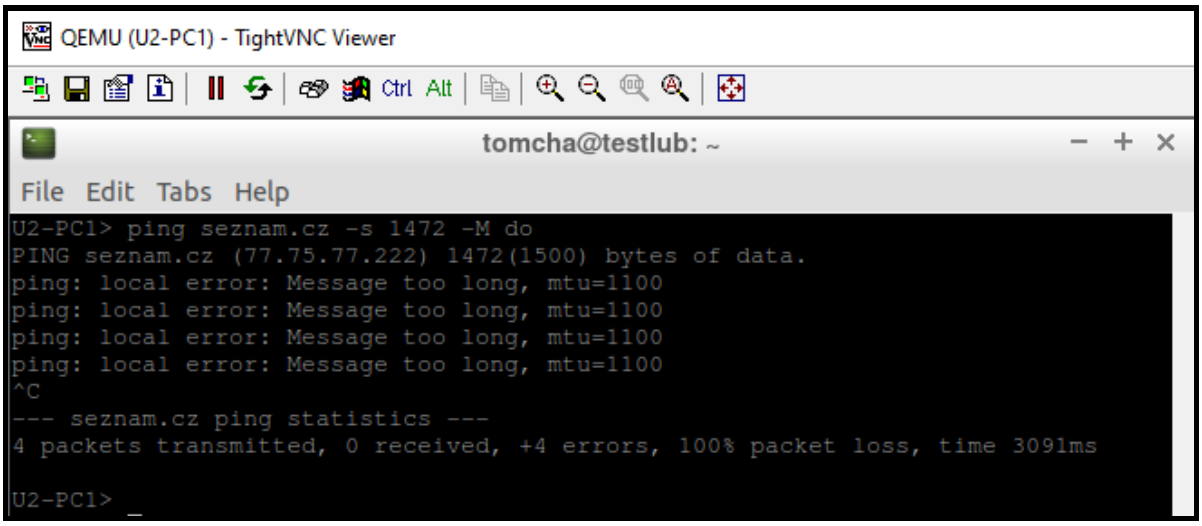
Pečlivým pročtením výstupu je možné odhalit uváznutí TCP spojení s vzdáleným serverem. Uváznutí spojení nasvědčuje řádné otevření spojení (SYN – SYN/ACK – ACK) a jeho řádné fungování (důkazem funkčnosti spojení jsou potvrzené keep-alive zprávy). Na výstupu je vidět i datová komunikace přes spojení (navázání TLS). Tato komunikace používání nižší velikost packetu, než nastavené MTU, a tudíž řádně prošla. Po ní následoval již větší segment, který přes úsek s nízkým MTU neprošel, a proto spojení uvázlo.

Po úvaze o nízkém MTU je již diagnostika jednoduchá. Ověření hypotézy provedeme pomocí dostatečně velkého PINGu se zakázanou fragmentací na server nefungující webové stránky.



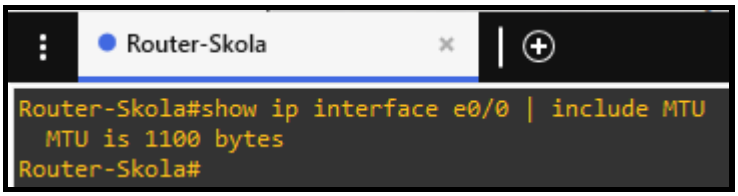
Obrázek 38 – Vysílání PINGů různých velikostí z U2-PC1

Velký PING s nákladem 1472 bajtů (tj. velikostí 1500 bajtů) kvůli malému MTU trasy neprošel. Menší PING prošel řádně. Pokud by Router-Skola byl nakonfigurován na zasílání ICMP zpráv, odpovědí na tento PING by byla zpráva ICMP Destination Unreachable, podtyp Fragmentation needed and DF set (spolu s nejvyšší hodnotou MTU, která by byla přípustná, aniž by došlo k fragmentaci) od Routeru-Skola.



Obrázek 39 – Vysílání PINGů různých velikostí z U2-PC1 při fungujícím PMTUD

Pokud router takto nastavený není, PING skončí vypršením času a rozhraní s nízkým MTU bude nutné najít ručně. Rozhraní WAN Routeru-Skola je nejpravděpodobnějším místem vzniku této závady, a prostá kontrola MTU vede k odhalení příčiny závady.



Obrázek 40 – Výpis MTU vnějšího rozhraní routeru Router-Skola

4.7 Závěr a diskuze

Výše uvedené ukázky jsou možné postupy pro diagnostiku a potvrzení čtyř nejpravděpodobnějších závad, které se mohou vyskytnout ve školních sítích. Při zjišťování příčin závad bylo pokaždé vhodné použít několik nástrojů, kde každý z nich pomohl dále zúžit možný rozsah příčin.

Jako nejuniverzálnější diagnostický se jednoznačně ukázal PING, který byl použit při diagnostice každé závady, u některých závad i vícekrát. Použití v praxi potvrdilo jeho výhody (zejm. velmi široká dostupnost), avšak značně zjednodušené prostředí emulace neodhalilo jeho úskalí (zahazování PINGů firewallem či prosté neodpovídání na PINGy). Pro většinu účelů zcela postačovalo výchozí nastavení, avšak při diagnostice excesivní fragmentace bylo nutné použít další rozšiřující parametry, jako např. velikost.

Pro diagnostiku L2 smyčky, duplicitní adresy a excesivní fragmentace byl použit Wireshark. Informace z něj dokážou závadu odhalit okamžitě (duplicitní kopie rámců, vícenásobné ARP dotazy a odpovědi, uvázlé TCP spojení), avšak jen tehdy, pokud se příslušný projev podaří zahlédnout. Jeho výstup je ve zkušební, omezené topologii velmi přehledný a orientace ve

výstupu je jednoduchá. Pro jeho účinné použití v praxi (zejm. na exponovaných zařízeních) je nutná znalost použití filtrů, které zpřehlední výstup. V případě diagnostiky uváznutého TCP spojení je nutná i vyšší kvalifikace obsluhy.

Výstupy ze spravovatelných zařízení (výpisy stavů a živé ladění) pomohly s určitostí potvrdit některé závady. Nejednalo se však o vyloženě kritické výstupy, bez kterých by diagnostiku nebylo možné dokončit (spíše šlo o závěrečné potvrzení příčiny obtíží). Jako primární diagnostický nástroj se tyto výstupy hodí zejména při tvorbě a úpravě konfigurace.

V praktické části nebyl ani jednou použitý TRACEROUTE. Stejně jako PING jde o velmi silný nástroj, který se však hodí spíše pro ladění problémů souvisejících se směrováním. Vzhledem k velikosti a struktuře topologie (přepínaná síť s jedním centrálním routerem) TRACEROUTE nemohl poskytnout příliš užitečné informace o závadách, které vznikly ve školní síti. V praxi by pomohl izolovat možnou závadu (tj. rozhodnout, zda příčina je „uvnitř“ ve školní síti, nebo „vně“, v síti poskytovatele připojení a dále).

Při diagnostice nebylo použito ani logování zpráv. Logování by mohlo být v praxi užitečné u diagnostiky přerušené kabeláže (pokud by došlo k úplnému přerušení spoje, došlo by k vygenerování patřičné zprávy). Emulované prostředí však nedokáže emulovat parametry fyzické vrstvy (i po odpojení spoje je příslušné rozhraní zapnuté), a proto ke generování žádných zpráv nedošlo.

Seznam použitých informačních zdrojů

1) *INTERNET CONTROL MESSAGE PROTOCOL*. Online. 1981. Dostupné z: https://datatracker.ietf.org/doc/html/rfc792. [cit. 2024-10-28].
2) *Ping (networking utility)*. Online. Dostupné z: https://en.wikipedia.org/wiki/Ping_(networking_utility). [cit. 2024-10-28].
3) *INTERNET PROTOCOL*. Online. 1981. Dostupné z: https://datatracker.ietf.org/doc/html/rfc791. [cit. 2024-10-28].
4) *Internet Protocol, Version 6 (IPv6) Specification*. Online. 2017. Dostupné z: https://datatracker.ietf.org/doc/html/rfc8200. [cit. 2024-10-28].
5) *How to Use TRACERT to Troubleshoot TCP/IP Problems in Windows*. Online. Dostupné z: https://support.microsoft.com/en-us/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e. [cit. 2024-10-28].
6) *About Wireshark*. Online. Dostupné z: https://www.wireshark.org/about.html. [cit. 2024-10-28].
7) *Understand Important Information on Debug Commands*. Online. Dostupné z: https://www.cisco.com/c/en/us/support/docs/dial-access/integrated-services-digital-networks-isdn-channel-associated-signaling-cas/10374-debug.html. [cit. 2024-10-28].
8) *The Syslog Protocol*. Online. 2009. Dostupné z: https://datatracker.ietf.org/doc/html/rfc5424. [cit. 2024-10-28].
9) *Cisco Catalyst 9200 Series Switches Hardware Installation Guide (Chapter: Switch LEDs)*. Online. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/hardware/install/b-c9200-hig/leds.htmldoc/html/rfc5424. [cit. 2024-10-28].
10) *Configure and Verify Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation*. Online. Dostupné z: https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html#toc-hId-313951887. [cit. 2024-10-28].
11) PETERKA, Jiří. *CSMA/CD*. Online. 1993. Dostupné z: https://www.earchiv.cz/a93/a333c120.php3. [cit. 2024-10-29].
12) *Duplex mismatch*. Online. Dostupné z: https://en.wikipedia.org/wiki/Duplex_mismatch. [cit. 2024-10-28].
13) *What is a DDoS attack?* Online. Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [cit. 2024-10-28].

14) *Spanning Tree Protocol (STP) Overview*. Online. Dostupné z: https://documentation.meraki.com/MS/Port_and_VLAN_Configuration/Spanning_Tree_Protocol_(STP)_Overview. [cit. 2024-10-29].
15) *RIP Version 2*. Online. 1998. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2453. [cit. 2024-10-31].
16) *Dynamic Configuration of IPv4 Link-Local Addresses*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc3927. [cit. 2024-10-29].
17) *Enhanced Duplicate Address Detection*. Online. Dostupné z: https://www.rfc-editor.org/rfc/rfc7527. [cit. 2024-10-29].
18) *IP fragmentation attack*. Online. Dostupné z: https://en.wikipedia.org/wiki/IP_fragmentation_attack. [cit. 2024-10-29].
19) *A Method for Transmitting PPP Over Ethernet (PPPoE)*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2516. [cit. 2024-10-29].
20) *Generic Routing Encapsulation (GRE)*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2784. [cit. 2024-10-29].
21) *Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec*. Online. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html. [cit. 2024-10-29].
22) *Transmission Control Protocol (TCP)*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc9293. [cit. 2024-10-29].
23) *Address Allocation for Private Internets*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc1918. [cit. 2024-10-29].
24) *IANA-Reserved IPv4 Prefix for Shared Address Space*. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc6598. [cit. 2024-10-29].

Vyjádření k využití nástrojů umělé inteligence

Umělá inteligence byla využita pro kontrolu pravopisu.

Seznam použitých obrázků

Seznam použitých tabulek