VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2017 Bc. Michal Vaclík

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

SPRÁVA PODNIKOVÝCH DATOVÝCH SÍTÍ
ENTERPRISE NETWORK MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Michal Vaclík

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. Vít Novotný, Ph.D.

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Michal Vaclík ***ID:*** 154225
Ročník: 2 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Správa podnikových datových sítí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s hlavními službami nezbytnými v podnikových datových sítích menšího rozsahu, jako jsou zajištění konektivity prostřednictvím přepínačů a směrovačů, serverů se službami DHCP, DNS, správa pracovních stanic a jejich aplikací. Aplikujte získané poznatky na návrh síťové infrastruktury laboratoře zaměřené na výuku síťových technologií, navrhněte a realizujte řešení zasíťování laboratoře integrující i laboratorní pracoviště s úlohami zaměřenými na síťovou komunikaci. Implementujte i základní bezpečnostní mechanizmy a zajistěte logické oddělení jednotlivých laboratorních pracovišť.

DOPORUČENÁ LITERATURA:

[1] MINASI, Mark, Kevin GREENE, Christian BOOTH, Robert BUTLER, John MCCABE, Robert PANEK, Michael RICE a Stefan ROTH. Mastering Windows Server 2012 R2. Indianapolis: Sybex, 2014. ISBN 978-1-118-28942-6.

[2] FINN, Aidan, Darril GIBSON a Kenneth VAN SURKSUM. Mastering Windows 7 deployment. Indianapolis, Ind.: Wiley, ISBN 978-0-470-60031-3, 2011.

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 24.5.2017

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultant:

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

ABSTRAKT

Diplomová práce se věnuje návrhu a realizaci infrastruktury datové sítě pro laboratoř zaměřenou na výuku síťových technologií na UTKO. Práce popisuje návrh a implementaci VLAN sítí, zavedení serverových komponent a metod pro sledování sítě.

KLÍČOVÁ SLOVA

správa sítě, podnikové sítě, active directory, virtualizace, tcp/ip, vlan, hyper-v, zabbix

ABSTRACT

Master's thesis discusses the design and implementation of network infrastructure for computer laboratory in Department of Communications. Thesis focuses on VLAN definitions and deployment of server virtualization, including network monitoring station.

KEYWORDS

network management, enterprise data networks, microsoft active directory, virtualization, tcp/ip, vlan, hyper-v, zabbix

VACLÍK, Michal *Správa podnikových datových sítí*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Rok. 78 s. Vedoucí práce byl doc. Ing. Vít Novotný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Správa podnikových datových sítí“ jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Vítu Novotnému, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

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

PODĚKOVÁNÍ

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

Brno . . . . . .

. . . . . .

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Datové sítě dnes poskytují základ pro nasazení moderních forem komunikace. V závislosti na jejím účelu a komplexnosti je její realizace jednodušší či složitější, sítě jsou sofistikovanější a mohou garantovat jinou úroveň kvality služby, nabízet větší míru redundance či toleranci vůči chybám. Spolehlivost samotné sítě je pak rozhodujícím faktorem pro nasazování služeb koncovým uživatelům. Ve své diplomové práci se věnuji popisu, návrhu a implementaci optimalizací pro laboratorní síť se zaměřením na výuku síťových technologií.

První část diplomové práce se věnuje rozboru a zhodnocení možností pro realizaci datové sítě v laboratorním prostředí Ústavu telekomunikací. Následnou analýzu sítě začínám popisem aktuálního stavu z pohledu uživatele i správce takové sítě. Dále popisuji možnosti realizace této sítě s využitím technik dělení virtuálních sítí, segmentování podsítí a jejich zabezpečení a implementací podpůrných prvků, které zajišťují nejen chod samotné infrastruktury, ale i provoz zařízení vyžadovaných pro realizaci laboratorních úloh.

Realizace nové infrastruktury probíhá paralelně za chodu stávající sítě popsané v první části. Tuto „novou“ síť konfiguruji dle požadavků a možností popsaných v první části. V laboratoři je provozováno velké množství zařízení odlišných typů zařízení od výrobců Cisco, HP, Mikrotik a dalších. Konfigurace jednotlivých zařízení tedy využívá standardizovaných protokolů, čímž je zajištěna přenositelnost konfigurace a provoz infrastruktury na jiných produktech stejného typu.

Společně s restrukturalizací laboratorní sítě probíhá i nasazení nových služeb serverové infrastruktury. Zároveň dochází k migraci v současnosti nasazených služeb na nově instalovaný hardware. Výstupem práce je pak přepracovaný koncept síťové infrastruktury a to včetně její části dedikované pro práci se zařízeními v rámci výuky předmětu Architektura sítí. Tento síťový celek je následně uveden do provozu a od zimního semestru 2017 bude tvořit zázemí pro další výuku. Práce poslouží mj. i jako popis praktik, které vedly k uvedení dané sítě do provozu a poslouží budoucímu správci sítě k orientaci při správě a údržbě této infrastruktury.

1 PODNIKOVÉ DATOVÉ SÍTĚ

Podniková síť představuje prostředí pro implementaci základních služeb datové sítě a dalších pokročilých typických pro firemní prostředí. Tato síť bez ohledu na její rozměr a komplexnost musí zaručit jistou míru spolehlivosti, zabezpečení, dostupnost služeb a v neposlední řadě i možnosti pro její efektivní správu. S rostoucím počtem garantovaných služeb rostou i nároky na její návrh a správu. Pro podnikové prostředí je taktéž typický požadavek na vzájemnou integraci služeb a jejich propojení přes jednotný prvek řízení přístupu.

Podniková síť je pak zpravidla pod správou jedné organizace. Pokud je nutno datovou síť realizovat mezi geograficky oddělenými lokacemi (např. hlavní kancelář a vzdálená pobočka), pro potřeby propojení a zajištění bezpečného přenosu dat mezi těmito sítěmi bývá časté nasazení např. IP tunelů. Ty mohou tyto vzdálené sítě propojovat do jedné větší, zdánlivě „místní“ sítě. Pro účely této práce se však omezme pouze na jednu geograficky vyčleněnou síť, která je realizována v jedné lokalitě.

Strukturu libovolné místní sítě můžeme členit do určitých vrstev dle vlastností, které daná vrstva a její síťové prvky implementují. Tento strukturovaný model zavádí vrstvu jádra sítě, vrstvu distribuční a vrstvu přístupovou. Přestože jde o obecně uznávanou praktiku, implementace jednotlivých funkcí pro každou vrstvu není nijak striktní. V menších sítích, mezi které spadá i naše, může být úloha distribuční vrstvy rozdělena mezi vrstvu přístupovou a vrstvu jádra sítě a samotná síť tak nemusí obsahovat dedikovaný hardware pro realizaci dané vrstvy. Taková topologie je označována za tzv. zkolabovanou hierarchii. Vrstvový přístup je výhodný i z hlediska modularity celé architektury a možnosti členění síťového hardwaru dle požadovaných funkcí, které nabízí (např. PoE na přepínači tvořícím jádro sítě nenabízí žádný benefit a zbytečně zvyšuje cenu daného prvku).

Přístupová vrstva nabízí hraniční funkce mezi sítí a koncovými zařízeními jako jsou počítače, telefony, kamery apod. Zařízení učená pro tuto vrstvu zpravidla nabízí větší počet síťových rozhraní pro přípojení koncových zařízení a obsahují např. bezpečnostní funkce pro komunikující uzly (ARP inspection, DHCP snooping, funkce standardu IEEE 802.1X), bezpečnostní funkce pro síťovou infrastrukturu (STP, filtrace BPDU rámců) či PoE pro usnadnění nasazení koncových uzlů (telefonní přístroje, kamerové jednotky apod.).

Distribuční vrstva tvoří agregační bod síťové komunikace mezi přístupovými směrovači a jádrem sítě, ve kterém se většinou nachází klíčové služby zajišťující chod síťové infrastruktury. Častou vlastnstní je i redundance a agregace linek a s tím související zabezpečení proti výpadku jednotlivých spojů. Taktéž zde může docházet k směrování mezi virtuálními sítěmi, čímž je možno zajistit oddělení provozu mezi

logickými topologiemi realizovanými na druhé vrstvě RM ISO/OSI. Přínosem implementace distribuční vrstvy pomocí dalšího hardwaru v síťové topologii je především vysoká dostupnost síťových služeb a modularita návrhu.

Vrstva jádra sítě je tvořena výkonnými přepínači a směrovači, které zajišťují propojení s vnějšími sítěmi a přístupy do sítě internet. Jádro sítě je agregačním bodem velké části síťové komunikace, tudíž je zde požadavek nejen na maximální dostupnost, redundanci, ale i vysokou rychlost síťových prvků. Většina spojů je tedy redundantních a zálohovaných jinými síťovými prvky, fyzické spoje jsou rozprostřeny mezi větší množství aktivních prvků a propoje seskupovány do logických spojů o rychlostech v řádech až desítek gigabitů za sekundu.

1.1 Oddělování datových sítí

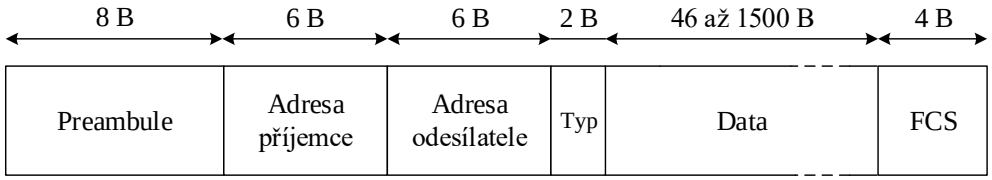
V datových sítích všech velikostí se zpravidla setkáváme s aktivními prvky, které zajišťují vzájemné propojení komunikujících stanic, a to na úrovni fyzické i logické. Mezi prvky zajišťující fyzickou konektivitu lze zařadit převážně přepínače a přístupové body pro bezdrátové sítě. Tyto prvky pracují převážně s adresami linkové vrstvy a dochází zde tedy pouze k přepínání datových jednotek. Propojování logických sítí je zajištěno pomocí směrovačů, jejichž rozhraní většinou náleží do těchto propojovaných sítí, mezi kterými dochází ke směrování paketů na síťové vrstvě, v současnosti vesměs výhradně na IP vrstvě protokolové sady TCP/IP.

Velmi často užívanou metodou pro oddělování datových sítí dle jejich účelu je jejich vzájemná izolace na úrovni linkové vrstvy. Dochází tím k podstatné redukci domény všesměrového vysílání a taktéž k žádoucí nutnosti zavedení směrování na úrovni síťové vrstvy. Možnosti vzájemného směrování mezi sítěmi bývají selektivně omezovány pomocí metod filtrace síťového provozu. Následující dvě kapitoly popisují principy dělení fyzické topologie pomocí značkování rámců a implementace oddělených podsítí v nově vzniklých virtuálních sítí. Tyto techniky jsou základním předpokladem pro oddělování jednotlivých typů zařízení (servery, pracovní stanice, VoIP zařízení) a pro případnou implementaci QoS mechanismů.

1.1.1 Dělení fyzické topologie pomocí VLAN

Přepínače odstraňují nedostatky rozbočovačů nasazením procesorů či obvodů zajišťující přepínání na základě informace obsažené v záhlaví přepínaných rámců. Záhlaví každého rámce obsahuje mj. adresu odesílatele a adresu příjemce, čímž je zajištěna možnost adresování přepínaných jednotek mezi dvěma komunikujícími stanicemi. V místních sítích je velmi časté i přepínání rámců jednoho odesílatele k více příjemcům.

Dnes se v místních sítích realizujících vícebodové spoje setkáváme s datovými jednotkami (rámci) typu Ethernet II. Ze struktury tohoto rámce, jež je znázorněna na obr. 1.1, je patrné mj. i pole určující délku či typ přenášeného protokolu. Do pole indikující typ přenášeného protokolu může být vkládáno záhlaví protokolu 802.1Q, jež je primárně použito pro specifikaci příslušnosti rámce k dané VLAN. Ze záhlaví 802.1Q může přepínač detekovat mj. i definice QoS parametrů na linkové vrstvě. Pokud rámec tuto hodnotu neobsahuje, může ji přepínač na základě předem stanovených pravidel doplnit, rámce přeznačit či značku zcela odebrat. Nastavení



Obr. 1.1: Struktura rámce Ethernet II

příslušnosti zařízení do jednotlivých VLAN sítí se v nejjednodušším případě nastavuje na daném portu přepínače[1]. Pokud je rozhraní použito pro přístup pouze do jedné virtuální sítě, je označováno jako přístupový (z angl. Access) port a naopak pokud lze přes toto rozhraní přenášet rámce náležících do více VLAN, bývá toto rozhraní označeno jako tzv. trunk port.

V případě použití identifikátoru VLAN v rámcích hovoříme o tzv. značkovaných rámcích (z angl. tagged frame). Se značkovanými rámci se většinou na rozhraní koncové stanice nesetkáme, neboť dané identifikátory se používají spíše na rozhraních propojující síťové prvky. Většina ovladačů síťových karet podporuje přidání VLAN identifikátoru přímo v procesoru síťové karty, nicméně přepínače s nastaveným přístupovým portem na svém vstupu očekávají spíše neznačkované rámce a stejně tak ze značeného rámce před odesláním koncové stanici VLAN identifikátor odstraní. Reakce přepínače na „neočekávaný“ značkovaný rámec na svém vstupu lze na některých typech přepínačů ovlivnit – přepínač může značený rámec přijmout, přeznačit či zahodit.

Pole záhlaví protokolu 802.1Q je dále rozděleno na dvě položky – prvních 16 bitů náleží TPID (Tag protocol identifier) identifikátoru a spodních 16 bitů TCI (Tag control information) informačním polím. Hodnota TPID je předem nastavena na hodnotu 0x8100. Protože je na tomto místě (bity pole TPID odpovídají pozici bitů polí EtherType v neznačkovaných rámcích) označení typu rámce, je touto hodnotou signalizováno použití značkovacího protokolu.

[1] Alternativně lze využít např. začlenění dle zdrojové MAC adresy či dalších mechanismů.

Zbylých 16 bitů přepínači signalizuje tři informace o způsobu práce s rámcem. Tři bity slouží jako tzv. identifikátor priorit PCP (z angl. Priority code point) a primárně slouží pro zajištění kvality služeb na linkové vrstvě. Hodnota pole může nabývat až 8 hodnot, které definují priority datové jednotky s tím, že hodnota 0 indikuje nejnižší prioritu (best effort) a hodnota 7 indikuje prioritu nejvyšší – většinou řídící provoz sítě. Čtvrtý bit nastavuje hodnotu DEI identifikátoru (z angl. Drop eligible indicator), na základě čehož přepínač v případě vyčerpání přepínacích kapacit může rozhodnout o zahození rámce jako prevence proti zahlcení sítě. Zbylých 12 bitů v TCI poli reprezentuje VLAN ID (z angl. VLAN identifier), čímž je určena příslušnost rámce do dané virtuální sítě linkové vrstvy [11].

1.1.2 Segmentování na síťové vrstvě

Pro adresování komunikace na internetové vrstvě TCP/IP jsou použity logické adresy protokolu IP. Protože po segmentaci na úrovni spojové vrstvy zařízení nejsou členy jedné L2 domény, musí docházet ke směrování. Přestože jsou pro větší sítě dnes zcela standardně nasazovány L3 přepínače, které jsou schopny rámce směrovat na základě údajů v IP paketu, v menších sítích je nutno využít směrovače. Práce s datovými jednotkami síťové vrstvy opět nabízí několik možností selektivní filtrace datového toku, překlad logických adres či implementace mechanismů pro zajištění kvality služeb.

Pro logicky segmentované L2 sítě je vhodné zavést adresní schéma s efektivním využitím adresního prostoru. Pokud do těchto podsítí bude směrován datový provoz z externích sítí bez překladu adres, je vhodné adresní prostor segmentovat s ohledem na možnost zpětného sloučení (tzv. supernetting) podsítí do jedné větší sítě. Tím dojde k redukci záznamů ve směrovacích tabulkách externích směrovačů pro zajištění směrování do vnitřních podsítí a potenciální úspoře výpočetního kapacity směrovače.

1.2 Vybrané služby v LAN

Následující kapitola se věnuje popisu základních služeb, které jsou nasazovány v místních datových sítích. Jedná se zejména o služby DHCP a DNS, jež zajišťují funkce pro komunikaci pomocí internetového protokolu IP verze 4 a verze 6. V podnikových sítích se běžně nasazují i funkce NAT a mechanismy pro ochranu účastníků na hraničních prvcích i koncových stanicích. Princip funkce překladu adres a filtrace datového provozu je nad rámec tohoto textu.

1.2.1 Vlastnosti protokolu DHCP

Protokol DHCP vychází z RFC 1531 a je považován za nástupce protokolu BOOTP. DHCP komunikace vychází z modelu server – klient, tedy server klientům odpovídá na požadavky o zaslání konfiguračních parametrů sítě. Nejčastěji jde o parametr IP adresy pro žádající uzel, masku sítě, adresu výchozí brány této sítě a IP adresy serverů DNS pro překlad názvů. DHCP protokol však nabízí i pokročilejší funkce, zejména předávání informací o síti stanici a naopak. Tyto informace jsou předávány pomocí zpráv DHCP Options, tedy jednotlivých parametrů, které lze pomocí DHCP protokolu nastavit. Přehled základních a dalších vybraných voleb je uveden v tab. 1.1 [16].

Mimo základní parametry pro realizaci síťové komunikace lze klientům zasílát i parametry pro zavaděč operačního systému ze síťového umístění. Tato funkce je nezbytná pro později implementovanou Službu pro nasazení systému Windows, pomocí které lze provést bezobslužnou instalaci a konfiguraci obrazu operačního systému na pracovních stanicích [1]. Kromě výše popsaných je možno pomocí DHCP protokolu konfigurovat i spoustu dalších funkcí síťových zařízení, např. adresy WINS, IRC, SMTP apod. Někteří výrobci specifického HW (VoIP/SIP zařízení) poskytují seznam jimi používaných DHCP parametrů, pro hromadné předávání řídících informací (adresy TFTP pro stažení firmware, adresy SIP registrátorů).

Tab. 1.1: Vybraná sada parametrů DHCP Options

DHCP volba	**ID**	**Popis**
Směrovač	003	IP adresa výchozí brány
Časový server	004	IP adresa NTP serveru
Servery DNS	006	IP adresa DNS serveru
Název domény DNS	015	přípona domény pro vyhledávání
Název spouštěcího serveru	066	Jméno nebo adresa spouštěcího serveru
Název souboru spuštění	067	Cesta k spouštěcímu souboru na PXE serveru

Protože jsou IP adresy a další parametry „zapůjčeny“ jen na předem stanovenou dobu, je nutno během komunikace ošetřit i stav, kdy se platnost zápůjčky blíží ke konci. Klientská stanice proto většinou pracuje s časovači T1 a T2. Po uplynutí poloviny času platnosti [16] zápůjčky (čas T1) se DHCP klient zasláním zprávy DHCP Request původnímu DHCP serveru, který zápůjčku poskytl, snaží o obnovu. Pokud je klient neúspěšný, po uplynutí $87,5$ % doby zápůjčky (čas T2) opět posílá žádost o prodloužení zápůjčky. Tato zpráva je již adresována všesměrově a pokud kterýkoli DHCP server žádost zamítne (klient obdrží zprávu DHCP Nack), klient musí okamžitě danou adresu přestat používat a proces síťové konfigurace začít znovu [3] [16].

Při dotazování jsou některé zprávy adresovány všem příjemcům (broadcast pakety). Všesměrové zprávy jsou nutné zejména pro nalezení DHCP serveru na síti, z čehož je patrné, že pokud se DHCP server a klient nachází v odlišných doménách všesměrového vysílání, je nutno použít další prvek, který komunikaci na rozhraní domény všesměrového vysílání zachytí a přepošle na adresu DHCP serveru.

V první fázi klient vyhledá DHCP servery zasláním zprávy DHCP Discover na všesměrovou adresu. Všechny dostupné DHCP servery v této L2 doméně na žádost reagují, avšak pouze v případě, že jejich databáze obsahuje volnou adresu pro zapůjčení klientovi. Přestože klient v tento okamžik nemá přiřazenu žádnou logickou adresu, je tato zpráva adresována všesměrově. DHCP klient může obdržet nabídek více, proto si dle preference vybere nejvhodnější server a na všesměrovou adresu pošle zprávu DHCP Request. Tuto zprávu opět zachytí všechny DHCP servery – jediný zvolený server, který se ztotožní s požadavkem, pak zápůjčku potvrdí zprávou DHCP Ack, pro ostatní servery je DHCP Request indikací, že klient zvolil jiný server. Po úspěšném nastavení konfigurace jsou u klienta spuštěny časovače T1 a T2 [16].

Pokud je síťový subsystém klienta restartován (restart OS, odpojení a opětovné připojení k síti) a zápůjčka je dle časovače klienta stále platná, klient může IP adresu používat bez nutnosti opakování procesu automatické konfigurace. Tato situace většinou nenastane při plánovaném opuštění sítě (softwarové vypnutí OS) – v tomto případě DHCP klient většinou zašle zprávu DHCP Release, čímž klient informuje server, že danou zápůjčku již nechce používat.

1.2.2 Vlastnosti systému DNS

Systém DNS má v dnešních místních i veřejných sítích zcela neodmyslitelné místo. Udržovat kompletní databázi síťových uzlů v jejich přirozené, tedy číselné podobě je dnes prakticky nemožné. Komunikace v počítačových sítích však probíhá výhradně pomocí IP adres, tedy 32-bitových, resp. 128-bitových číselných identifikátorů, a proto systém DNS z pohledu uživatele slouží spíše jako pomůcka, jak síťovým uzlům přiřadit snadno zapamatovatelný název.

DNS je aplikační protokol využívající transportních protokolů UDP 53 i TCP 53 na straně serveru. Využívá komunikačních modelů klient-server i server-server. Pro „běžné překlady“ požadavků klientů je využit transportní protokol UDP, a to zejména z důvodu rychlé odezvy. Spolehlivost přenosu zde většinou není vyžadována, možnou chybu při přenosu DNS klient většinou kompenzuje odesláním několika dotazů více DNS serverům ve velmi krátké době. Spojově orientovaná komunikace pomocí protokolu TCP je naopak vyžadována při tzv. přenosu zón, tedy přenosu a synchronizaci informační báze mezi samotnými DNS servery, kde je naopak žádoucí spolehlivost přenosu před rychlostí přenosu [15]. Protože je detailní rozbor komuni-

kace DNS serveru s klienty nad rámec tohoto textu, níže uvádím pouze nejčastěji používané typy DNS záznamů. Jedná se o záznamy typů:

- A, resp. AAAA – záznam mapuje název na IPv4, resp. IPv6 adresu,
- CNAME – kanonické jméno (tzv. alias) odkazující na jiný záznam,
- MX – záznam odkazující na IP poštovního serveru pro danou doménu,
- PTR – záznam mapující IP adresu na doménové jméno (reverzní vyhledávání).

Správnost a aktuálnost informace poskytované DNS serverem je jedním z předpokladů pro chod podnikové sítě na bázi služeb Active Directory[2] [3]. Servery DNS mohou být mj. konfigurovány i pro zajištění vyrovnávání zátěže na žádané stanici či serveru. Na dotaz klienta o „překlad“ názvu na IP adresu může být vybíráno z více uzlů dosažitelných pod tentýž jménem. Ve své práci pro identifikaci stanic využívám výhradně jmenné názvy. Hlubší popis DNS systému je nad rámec této práce. Více o systému DNS a službách Active Directory dostupné v [1] a [15].

1.3 Bezpečnost a spolehlivost v LAN

V moderních instalacích datových sítí se lze dnes setkat zcela běžně s vícenásobným propojováním dvou síťových entit, tedy technikou, kdy více fyzických spojů vytváří jeden logický. Stejně tak se dnes zcela běžně implementují bezpečnostní mechanismy pro ochranu datové sítě a jejích účastníků. Následující kapitola slouží jako stručný popis metody pro agregaci fyzických linek a popisu vybraných metod pro zajištění bezpečnosti logické topologie sítě. Protože je popis dalších dostupných mechanismů nad rámec tohoto textu, uvádím zde jen stručný seznam těch, jejichž konfigurace je v diplomové práci upřednostňována. Jde zejména o funkce konfigurované na přístupových přepínačích. Jedná se o funkce ochrany proti útoku přetečením, ochrana před paděláním záznamů ARP tabulek účastníků sítě a filtrace zpráv nepovoleného DHCP serveru v síti. Příklady konfigurace a značení jednotlivých funkcí se může lišit v závislosti na výrobci zařízení, příklady konfigurace uvádím pro zařízení společnosti Cisco s operačním systémem Cisco IOS.

1.3.1 Agregace spojů dle IEEE 802.1AX

Agregace rozhraní se stala běžnou praktikou pro efektivní zužitkování více dostupných spojů mezi dvěma body v síti. Přestože je tato technika využívána spíše mezi síťovými prvky tvořící infrastrukturu sítě, dnes je princip sdružování několika síťových rozhraní nasazován i na koncových zařízeních datové sítě, zpravidla pak serverech vyžadující vyšší přenosovou kapacitu při přístupu k datové síti. Pro agregaci

[2] Adresářové služby jsou nasazeny ve stávající i nové infrastruktuře

více dostupných rozhraní je do moderních operačních systémů integrována funkce tzv. „NIC Teaming“, která často dokáže agregovat spoje i bez přímé podpory na straně přepínače. Ve své práci však využívám výhradně „přepínačem asistované“ agregace pomocí protokolu Link Aggregation Control Protocol.

Tento protokol byl původně definován v doporučení IEEE 802.3ad, nicméně dnes je součástí revidovaného souboru doporučení IEEE 802.1AX. Na rozdíl od proprietárních protokolů jednotlivých výrobců – příkladem může být PAgP společnosti Cisco či Aggregated Ethernet společnosti Juniper – jde o IEEE standard implementovaný nezávisle na výrobci zařízení, a to i na aktivních prvcích výrobců, které nabízí proprietární řešení agregace [14]. Z tohoto důvodu je jeho užití vhodné v prostředí, kde je nasazeno více zařízení odlišných výrobců.

Uvažujme přepínače SW1 a SW2, nechť každý je schopen přiřadit dva fyzické spoje s rychlostí 1 Gbit/s do agregovaného kanálu. Maximální teoreticky dosažitelná propustnost V výsledného spoje je tedy $V = 2$ Gbit/s, neboť

$$V = n \times v, \tag{1.1}$$

kde n je počet fyzických portů daného kanálu a v je rychlost každého samostatného portu. Počet n sdružovaných portů bývá obvykle 1 až 8 a rychlost jednotlivých rozhraní je nutno zachovat stejnou pro všechny účastníky logického kanálu [14]. Tato technika zároveň zajišťuje i jistou míru tolerance vůči výpadku spoje, neboť v případě výpadku některého z rozhraní podílejících se v logickém kanálu lze agregovaný spoj dále provozovat i pokud je složen z jediného fyzického spoje.

LACP je na síťovém zařízení konfigurován zpravidla v aktivním či pasivním režimu. Pokud je dílčí rozhraní konfigurováno jako aktivní, dané zařízení opakovaně vysílá LACPDU rámce a aktivně vyzývá protistranu s žádostí o sjednání logického kanálu. Opakem aktivního režimu je pasivní režim – v tom režimu zařízení pouze přijímá LACP řídicí rámce a ke sjednání logického kanálu dojde pouze v případě, že je přijata výzva od zařízení vysílajícího v aktivním režimu[14]. Během detekční periody, tedy doby, kdy na daném rozhraní není sjednán žádný logický kanál, jsou LACP rámce vysílány s periodou 1 sekundy a dále jsou vysílány tzv. „udržovací“ rámce s periodou 30 sekund pro zachování logického kanálu.

Více o principu agregace spojů pomocí protokolu LACP dostupné z [14].

1.3.2 Prevence proti útoku přetečením

Přepínače si v závislosti na přijatých rámcích tvoří tabulky vazby MAC adresy a příslušnost k dané VLAN pro zařízení připojená k portům přepínače. Tím je možné

adresovat rámce pouze určeným stanicím. Útok přetečením zneužívá konečné kapacity paměti přepínače vysláním velkého množství rámců s padělanými MAC adresami zdroje, které si přepínač postupně zapisuje do svojí přepojovací tabulky [6]. Tyto záznamy jsou ukládány na omezenou dobu – většinou na 300 sekund. Po uplynutí této doby či po restartu přepínače je tato informace odstraněna. V momentě, kdy je paměť přepínače vyčerpána a není tedy možné uložit do tabulky MAC adres další záznam, přepínač přejde do stavu úplného přeposílání, kdy se svojí funkcí blíží rozbočovači. Aby nedošlo k přerušení komunikace, přepínač posílá rámce i na rozhraní, kde se cílové zařízení nenachází. Tímto způsobem se ke stanici útočníka přeposílají rámce, které jsou adresovány jinému uzlu sítě[3]. Ochrana proti tomuto typu útoku spočívá v nastavení limitu aktivních MAC adres, které mohou být registrovány k jednomu rozhraní přepínače či přímou specifikací hodnot MAC adres, které mohou být v přepojovací tabulce registrovány k danému rozhraní. Příklad konfigurace přístupového rozhraní Fa0/1 přepínače SW1, která zamezí výskytu více než 2 MAC adres přidružených k tomuto rozhraní a v případě narušení této zásady rozhraní deaktivuje, je:

```
SW1(config)#interface fa0/1
SW1(config-if)#switchport port-security maximum 2
SW1(config-if)#switchport port-security violation shutdown
```

Volitelně lze specifikovat i zdrojové MAC adresy, jež budou v případě výskytu na daném rozhraní zavedeny do přepojovací databáze přepínače. Zbylé či nespecifikované adresy budou do přepojovací databáze doplněny za předpokladu, že nedojde k porušení výše konfigurovaného limitu aktivních MAC adres na daném rozhraní [6]. Tato funkce je vhodná např. pro zapojení telefonního přístroje a počítače na jedno rozhraní přepínače, případně ji lze použít k zamezení možnosti připojení např. nezabezpečené virtuální stanice s přemostěným síťovým rozhraním.

1.3.3 Kontrola validity datových jednotek ARP protokolu

Aby bylo možno v místních ethernetových sítích zajistit komunikaci dvou účastníků na základě jejich IP adres, je nutno nasadit mechanismy mapování fyzické adresy (MAC adresa rozhraní) k logickým adresám síťové vrstvy (IP adresy). Aby tato tabulka vazeb nemusela být na každé stanici a síťovém prvku konfigurována ručně, především v rozsáhlých datových sítích se spoléhá na podpůrné protokoly ARP či ICMPv6 (Neigbour Discovery). ARP je bezstavový protokol definovaný v RFC 826 a zajišťuje „překlad“ IP adresy stanice na její MAC adresu [5].

[3]Cílová stanice tyto rámce zpravidla zničí

Stanice běžně registruje a zpracuje ARP odpovědi i pokud sama nevyslala ARP dotaz [5]. Tím lze do tabulky vazeb linkové a síťové adresy na stanici oběti řízeně zavést nelegitimní (falešné) informace. Komunikace oběti v dané ethernetové síti je následně přepínána na rozhraní přepínače, jež má přidruženu MAC adresu cílové stanice[4] [9].

Metodou ochrany proti tomuto typu útoku je funkce síťového prvku, která vytváří tabulku vazby pouze skutečné, tedy legitimní IP adresy a legitimní MAC adresy. Tuto funkci zajišťuje mechanismus označovaný jako Dynamic ARP Inspection, zkráceně často označováno jako DAI. Veškeré rámce, jež obsahují ARP dotaz či odpověď, jsou zachyceny a analyzovány řídící jednotkou přepínače. Zejména jde o kontrolu informace obsažené v datové jednotce ARP protokolu. Tuto kontrolu provádí přepínač proti vlastní důvěryhodné databázi, kterou dynamicky naplnil informacemi (vychází z činnosti mechanismu DHCP Snooping) nebo do které správce daného síťového prvku zanesl statické údaje [10]. Metoda zanášení statických údajů je vhodná zejména pokud se v dané síti vyskytují prvky se statickou konfigurací IP protokolu. U těchto stanic zpravidla neprobíhá DHCP konfigurace a přepínač by tuto vazbu linkové a síťové adresy nebyl schopen zachytit pomocí funkcí DHCP Snooping.

Pokud přepínač informaci v datových jednotkách ARP protokolu vyhodnotí jako validní, využije ji k aktualizaci vlastní přepojovací tabulky a následně rámec předá na patřičné výstupní rozhraní. V opačném případě je rámec nesoucí jednotky ARP protokolu zničen. Příklad konfigurace DAI na přepínači SW1 pro kontrolu ARP paketů šířených ve VLAN s VID 10 je uveden níže.

```
SW1#configure terminal
SW1(config)#ip arp inspection vlan 10

SW1(config)#interface gigabitEthernet 0/1
SW1(config)#ip arp inspection trust
```

Výše uvedená konfigurace nastaví kontrolu validity šířených ARP informací globálně pro VLAN 10. Následně je pro rozhraní *GigabitEthernet 0/1* nastavena důvěra[5], na tomto rozhraní tedy kontrola datových jednotek ARP protokolu neprobíhá.

1.3.4 Kontrola validity DHCP serveru

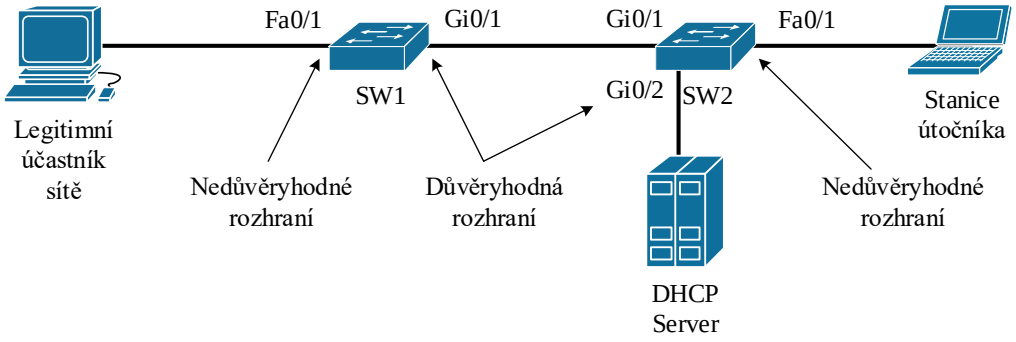
V podnikových sítích bývá nejen privátní adresní prostor centrálně spravován. Zároveň je nutno znemožnit připojení neautorizovaného DHCP serveru do počítačové sítě, aby nedocházelo k distribuci nevalidních či konfliktních IP adres klientům dané

[4]Tento typ útoku je většinou zneužíván při útoku typu mužem uprostřed

[5]Pouze v rámci DAI, nikoli DHCP Snooping

sítě. K tomuto účelu se zejména na přístupových přepínačích zavádí funkce pro limitaci šíření určitých typů DHCP zpráv. Funkce, která řídí, resp. omezuje šíření DHCP zpráv dle zdrojového rozhraní bývá na moderních síťových prvcích souhrnně označována jako DHCP Snooping.

Správce síťového prvku určí porty přepínače, na kterých se může v rámci ethernetové sítě (lze specifikovat odlišně pro konkrétní VLAN) šířit paket se zprávou DHCP Offer. Zjednodušeně lze opět říci, že zpráva DHCP Offer neautorizovaného DHCP serveru je zahozena na vstupním portu přepínače a nikdy se nepřepíná až na výstupní rozhraní ke stanici jež vygenerovala zprávu DHCP Discover. Příklad nastavení úrovní důvěry portů přepínače je znázorněno na obr. 1.2.



Obr. 1.2: Označení rozhraní přepínačů pro DHCP Snooping

Nechť rozhraní Fa0/1 přepínačů SW1 a SW2 jsou přístupová rozhraní pro pracovní stanice v dané síti. Tato rozhraní jsou správcem přepínačů konfigurována jako nedůvěryhodná. Naopak rozhraní, na které je připojen autorizovaný DHCP server, resp. rozhraní, která přes mezilehlý prvek připojují tento DHCP server, jsou označena jako důvěryhodná. Pokud falešný DHCP server na stanici útočníka zachytí všesměrovou zprávu DHCP Discover a vygeneruje odpověď DHCP Offer, přepínač SW2 podnikne konfigurovanou akci na rozhraní Fa0/1, např. odpojení (vypnutí) daného rozhraní přepínače. Příklad konfigurace přepínače SW2, jež aktivuje funkci DHCP Snooping globálně – tedy na všechna rozhraní a virtuální sítě je:

```
SW2#configure terminal
SW2(config)#ip dhcp snooping
```

Následně je nutno povolit šíření nabídky zápůjčky (viz. 1.2.1) na rozhraní Gi0/2:

```
SW2(config)#interface gigabitEthernet 0/2
SW2(config-if)#ip dhcp snooping trust
```

Korektní konfigurace mechanismu DHCP Snooping na přístupových přepínačích je základním předpokladem pro efektivní ochranu pomocí mechanismů Dynamic ARP Inspection. Tyto funkce jsou typicky konfigurovány na přístupových rozhraních přepínače, na jehož porty se připojují koncová zařízení klientů.

1.3.5 Filtrace datových jednotek pomocí ACL seznamů

Velmi často v datových sítích vzniká požadavek na řízení provozu mezi definovanými IP podsítěmi. V případě laboratorní sítě je např. velmi nežádoucí přístup do sítě, ve které se nachází administrativní rozhraní ze stanic na studentských pracovištích. Z tohoto důvodu moderní síťové prvky, např. přepínače[6] a směrovače umožňují tvorbu tzv. „seznamů pro řízení přístupu“, které v tom nejjednodušším případě definují zdrojovou síť, cílovou síť (případně i protokoly transportní vrstvy) a pravidlo podle kterého s danými jednotkami zařízení zachází. V případě naší datové sítě jde o ta nejjednodušší pravidla povolení či zamítnutí přístupu, tedy zda bude paket na rozhraní přijat a směrován nebo bude zničen [7].

Na zařízeních se systémy Cisco IOS[7] lze vytvořit zpravidla dva typy ACL seznamů, tedy standardní a rozšířený. Standardní ACL uvažuje pouze adresu zdrojové stanice a provádí definovanou akci. Naopak tzv. Extended ACL lze použít pro „konkrétnější“ určení datových jednotek, tedy např. zamezení přenosu na konkrétních transportních adresách a další. Seznamy pro řízení přístupu jsou aplikovány na konkrétní rozhraní a v konkrétním směru (vstup či výstup), jejich pravidla jsou procházena sekvenčně od prvního k poslednímu a posledním pravidlem každého ACL je pravidlo pro zničení provozu, který nebyl povolen či zničen na základě žádného předchozího pravidla [7].

1.4 Serverové a síťové služby Microsoft

Následující kapitoly jsou věnovány popisu vybraných technologií a serverových služeb společnosti Microsoft, které jsou v současnosti implementovány v prostředí laboratoře. Produkty této firmy jsou zvoleny zejména kvůli jejich spolehlivosti, výkonu a možnostem administrace. Existují i alternativy pro jednotlivé produkty, např. pro serverovou virtualizaci se nabízí produkty z řady vSphere konkurenční společnosti VMware. Taktéž adresářové služby lze implementovat pomocí zdarma dostupných alternativ jako je např. OpenLDAP server.

[6] Moderní přepínače dokáží filtrovat i jednotky vyšších vrstev TCP/IP

[7] Předpokladem je dostupnost patřičné funkcionality, např. balík *ipservices*

1.4.1 Serverová virutualizace Hyper-V

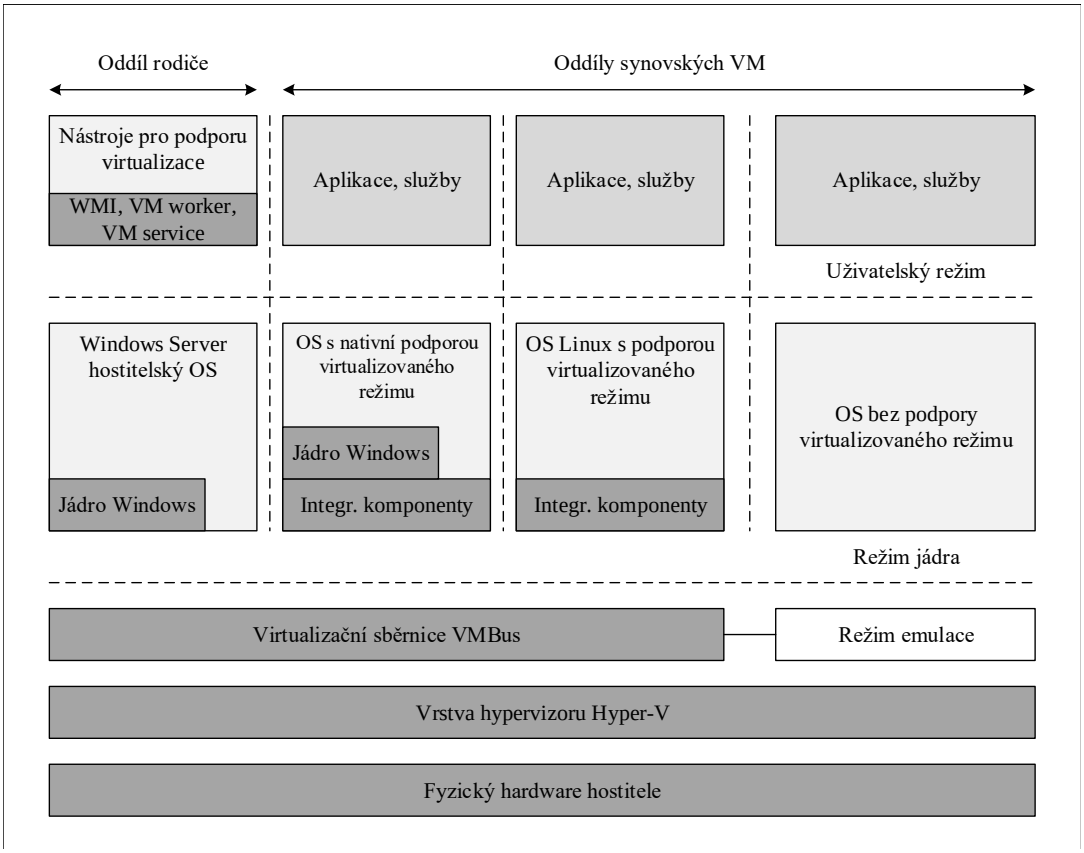
Hyper-V je role[8] operačního systému Windows Server ve verzi 2008 R2 a novějších. Tato role nabízí možnost provozu několika virtuálních systémů na jednom fyzickém serveru, který je označován jako virtualizační hostitel (z angl. host)[9]. Hardware hostitelského serveru je většinou plně dedikován pro provoz pouze virtualizační role a není zde nasazena žádná jiná role. Účelem serverové virtualizace bývá často vytvořit vrstvu nabízející určitou abstrakci hardwaru, na kterém je provozován virtuální stroj (zkráceně VM z angl. Virtual Machine) a jeho operační systém, který zprostředkovává požadovanou službu – např. doménový kontrolér, webový server apod. Fyzický server se tak de facto stává víceúčelovým zařízením, na kterém může být provozován server zprostředkující síťové služby, webové stránky či služby souborového serveru. Přestože by tyto role bylo možno provozovat i v jedné instanci operačního systému, separace těchto rolí je doporučeným postupem jak z hlediska výkonu, tak zabezpečení serverové infrastruktury [3].

Po instalaci Hyper-V role je na fyzickém serveru implementována architektura jež je znázorněna na obr. 1.3. Z diagramu virtualizační architektury je patrné nasazení vrstvy hypervizoru přímo na fyzický hardware a její propojení přes virtualizační sběrnici VMBus, která zprostředkovává přístup operačních systémů k hardwaru hostitele. Tento princip je podobný obecné vrstvové architektuře operačních systémů. Operační systém, jež provozuje roli Hyper-V serveru, se stane poskytovatelem všech nutných provozních procesů a služeb pro provoz virtuálních strojů (poskytovatel WMI objektů, spouštěč procesů a služeb) a stane se tzv. rodičovským oddílem [3]. Jednotlivé virtuální stroje jsou poté instalovány do tzv. synovských oddílů. V závislosti na schopnosti provozu virtualizovaného operačního systému ve virtualizovaném režimu se liší přístup a komunikace jednotlivých VM po virtualizační sběrnici VMBus. Přístup k této sběrnici je zpravidla zajištěn Integračními komponentami Hyper-V, které jsou dostupné pro většinu moderních operačních systémů.

Před instalací Hyper-V serveru je potřeba zohlednit nejen nároky samotného operačního systému, ale i nároky v něm provozovaných virtuálních systémů. Z vrstvového modelu je patrné, že o prostředky fyzického serveru soupeří i v něm provozované virtuální stroje a pro optimální běh je nutno zajistit vyhrazený přístup k fyzickým prostředkům. Toho je nejen v Hyper-V možno dosáhnout pomocí rezervace CPU jader, zajištění minimální a maximální paměti dostupné pro VM a možností rozprostírat diskové kontejnery napříč více fyzických disků či diskovým polem. Kromě

[8] v tomto kontextu jde o serverovou roli, přestože od Windows verze 8 je možné Hyper-V instalovat i na klientské počítače

[9] Je třeba dbát zvýšené opatrnosti při práci s anglickou a českou literaturou – angl. označení host znamená „hostitel“ a naopak angl. označení „guest“, či „guest VM“ znamená v češtině host (provozovaný virtuální stroj), nikoli však fyzický hostitel či virtualizační server



Obr. 1.3: Vrstvová architektura Hyper-V hostitele

obecných nároků operačního systému (v našem případě Windows Server 2016) [1] [3] je vyžadována podpora 64-bitových instrukcí procesoru, podpora virtualizační technologie Intel VT či AMD-V a podpora ochrany datového segmentu ve strojovém kódu, tedy Data Execution Prevention implementovaná pomocí technologií Intel XD bit či AMD NX bit.

1.4.2 Doménové služby Active Directory

Doménové a adresářové služby bývají základem infrastruktury podniků všech velikostí. V našem případě se jedná o implementaci adresářových služeb firmou Microsoft, která vychází ze standardu X.500 a protokolu LDAP [1] [3]. Tato služba (z angl. Active Directory Domain Services, zkráceně AD DS) působí jako centralizované úložiště objektů, které jsou obsaženy v AD DS databázi. Tato databáze obsahuje informace o uživatelích, skupinách, počítačích, topologii sítě, ale i DNS záznamy a DHCP zápůjčky[10]. Základním účelem je však autentizace identit (uživatelů a počítačů), autorizace (řízení přístupu) k prostředkům a jejich vyhledávání.

[10]Informace z DHCP a DNS serverů jsou ve formě objektů dále replikovány mezi ostatní servery realizující stejnou službu [3]

Role AD DS nabízí základní doménové a adresářové služby, nicméně v rámci struktury Active Directory lze instalovat spoustu dalších rolí, které využívají struktury implementované rolí AD DS. Jde například o služby certifikační autority v prostředí AD, federačních služeb, služeb oprávnění a další. V našem případě však využijeme pouze „základní“ AD DS role, a to zejména pro uložení identit, správu objektů a sdílení prostředků.

Active Directory zavádí několik logických komponent v síťové infrastruktuře. Jedná se o domény, stromy, lesy, organizační jednotky a místa. Zjednodušeně lze tyto komponenty označit za oblasti s platností definovaných pravidel [1] [3]. Návrh doménové struktury vyžaduje značnou míru plánování, zejména pokud jde o definici zásad skupiny (hromadná a centralizovaná konfigurace OS Windows), přidělování členství v bezpečnostních skupinách (autorizace) ale i komplexnějších úloh jako je navazování tzv. vztahů důvěry s ostatními doménami.

Ve stávající datové síti jsou nasazeny doménové služby Active Directory včetně začlenění pracovních stanic do doménové struktury. Případný zásah do konfigurace pracovních stanic je mimo rozsah tohoto textu a návrh datové sítě jej nezohledňuje.

Podrobnější popis je nad rámec textu, v následujících kapitolách budou pouze popsány a odůvodněny konkrétní konfigurace.

1.4.3 Vzdálená správa OS Windows

Serverové verze OS Windows i verze určené pro osobní počítače standardně obsahují mnoho nástrojů a možností pro efektivní a vzdálenou správu[11]. Protože je od verze 2012 doporučováno využívat serverové verze bez GUI, je nutné na daném OS nasadit metody pro vzdálenou administraci operačního systému a jeho rolí. K tomuto účelu lze použít hned několik nástrojů pro připojení „terminálovou službou“, neboli pomocí funkce Vzdálené plochy (z angl. Remote Desktop). Na serverech, kde však grafické nástroje nejsou instalovány je správci nabídnut většinou jen příkazový interpret či prostředí Windows Powershell, čímž se Vzdálená plocha pro tyto potřeby stává relativně zbytečnou.

Z výše popsaného důvodu je OS Windows vybaven sadou nástrojů, které dohromady tvoří službu pro vzdálenou správu OS Windows (angl. WinRM). Základem těcho nástrojů je tzv. WS-Management Protocol. Tento textově orientovaný protokol vychází z implementace SOAP modelu pro přenos informací formátovaných do podoby XML dat. Na rozdíl od objektového typu jako je tomu např. při použití WMI. WS-Management Protocol může být využit i v aplikacích třetích stran, tedy nejen v nástrojích pro administraci, které jsou součástí OS Windows. Zdrojem jeho dat může být již zmíněný WMI poskytovatel, pomocí kterého lze zpřístupnit

[11] Některé zde uvedené informace jsou specifické pro edice Windows Pro nebo Windows Enterprise

řadu informací o samotném HW, a to např. verze BIOS, výrobní a sériová čísla a další informace [1]. Tato data jsou většinou sbírána případnými klienty dohledových systémů.

Z pohledu správce operačního systému Windows je však nejvhodnější metodou vzdálené správy schopnost vzdáleného připojení k sezení příkazového interpreta Windows Powershell. Toho je docíleno povolením funkce „Powershell Remoting“, která je automaticky povolena při zapnutí komponenty Windows Remote Management[12]. Tím je správci umožněno nejen adresování vzdálených operačních systémů v příkazech a skriptech prostředí Windows Powershell, ale i samotný přístup k instanci příkazového interpreta, který je spuštěn ve vzdáleném operačním systému [1] [3]. Správu všech serverů a pracovních stanic provádím výhradně pomocí nástrojů sady Microsoft Remote Server Administration Tools.

[12]Tato funkcionalita je od verze 2012 ve výchozím stavu povolena automaticky

2 PROSTŘEDÍ LABORATORNÍ SÍTĚ

Následující kapitola se věnuje popisu současné topologie a v ní zavedených zařízení. Taktéž jsou hodnoceny výhody a nevýhody logické struktury sítě a v ní provozovaných služeb. Laboratorní síť zajišťuje přenos datových jednotek v oddělených VLAN sítích specifických pro každé pracoviště. Tyto VLAN sítě jsou poté přivedeny na přepínač, který připojuje fyzická experimentální zařízení. Experimentální VLAN sítě s VID v rozsahu 330 – 360 jsou přenášeny pouze pomocí značkovaných rámců. Experimentální sítě tak tvoří zcela oddělenou část laboratorní sítě a jejich propojení je zpravidla nežádoucí. V těchto sítích se může nacházet velké množství nevhodně zabezpečených pracovních stanic, chybně konfigurovaných síťových zařízení a jejich vzájemným propojením by mohlo dojit k narušení provozu laboratorní sítě (např. nevhodně konfigurovaný STP). Tato tvrzení vychází ze znalosti obsahu a řešení laboratorních úloh popsaných v [12].

Protože přepínač v rozvaděči s experimentálním vybavením zajišťuje pouze přepojování rámců mezi prvky laboratorních úloh, jeho konfigurace musí zajistit zcela transparentní přenos bez jakéhokoli zásahu do přenášených dat. Nesmí zde tedy pracovat žádné mechanismy filtrace, QoS apod. Výkon experimentálních úloh a schopnost jejich realizace je hlavním požadavkem na nově navrhovanou datovou síť.

2.1 Infrastruktura laboratorní sítě

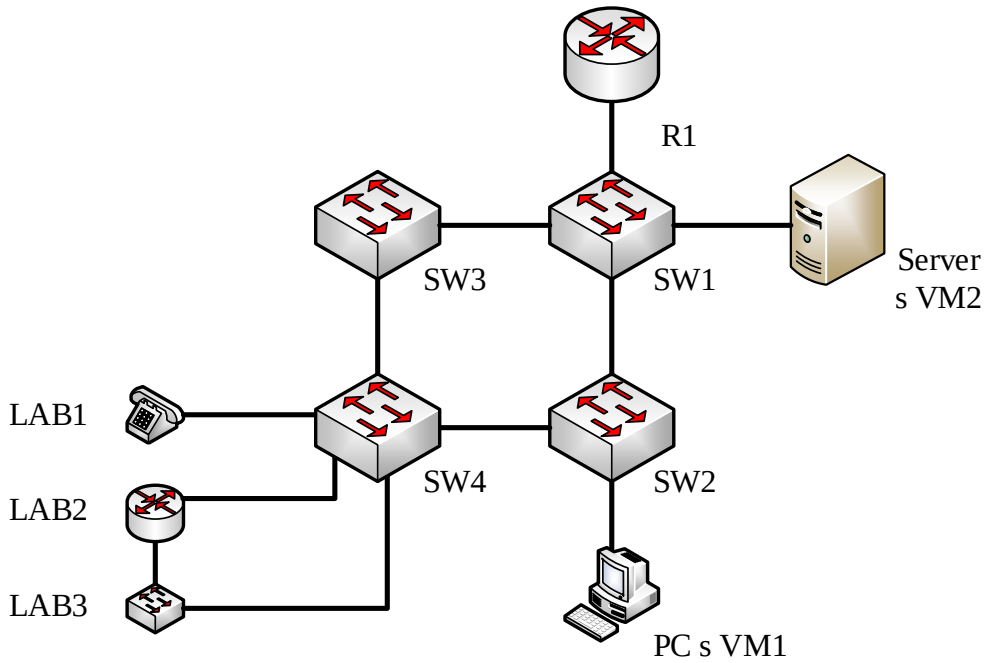
Aktuálně provozovaná datová síť využívá jednoho směrovače a čtyř přepínačů. Pro jednoduchost využijme symbolického značení síťových prvků a připojených fyzických a virtuálních stanic.

Nechť R1 tvoří hraniční směrovač laboratorní podsítě, provádí překlad adres síťové vrstvy a selektivní překlad adres transportní vrstvy. Na směrovači je definována pouze jedna LAN, která je pomocí neznačkovaných rámců šířena k prvnímu přepínači SW1. Na tomto přepínači jsou již definovány specifické virtuální sítě (VLAN), které jsou selektivně přiřazeny na jednotlivá rozhraní. Oddělení tzv. výukové VLAN od experimentálních, tj. virtuálních sítí, mezi kterými neprobíhá směrování a jsou vyhrazeny pro potřeby laboratorních úloh, zde však není realizováno zcela optimálně. Na SW1 je výchozí VLAN s VID 1 prakticky nevyužitá a veškerá zařízení, jež se připojují do laboratorní sítě (nikoli specifické experimentální) se připojují na rozhraní, které slouží jako přístupové pro VLAN s VID 310. Tato zařízení jsou pak členy stejné IP podsítě, jejíž adresovatelné rozhraní výchozí brány je na hraničním směrovači R1 členem výchozí ethernetové sítě s VLAN VID 1. Z tohoto důvodu je nutné z rámců přepínaných na odchozí rozhraní k R1 odebrat VLAN značku ze

záhlaví a ve zpětném směru, tedy při přenosu od R1 k SW1, všechny rámce označit dle 802.1Q a specifikovat pole VID s hodnotou 310.

K přepínači SW1 je přímo připojen další přepínač SW2. Rozhraní připojující druhý přepínač k SW1 je konfigurováno stejným způsobem jako linka mezi R1 a SW1. Rámce, které jsou na SW1 přiřazeny do VLAN s VID 310, jsou opět této značky zbaveny a odeslány na rozhraní připojující SW2, kde však již nejsou začleněny do žádné specifické VLAN sítě a zůstávají v nativní VLAN.

Vzhledem k této skutečnosti lze konstatovat[1], že jedna IP podsíť je jednak neefektivně rozprostřena mezi oddělené virtuální LAN sítě, navíc je definována na R1, SW1 a SW2 s nekonzistentními VLAN identifikátory. Pokud stanice připojená k přepínači SW2 vysílá rámec, jež je přepínán na rozhraní mezi SW2 a SW1 a následně k R1 (typicky pokud je zapouzdřený paket směrován mimo laboratorní podsíť), dochází ke trojímu značení rámce IEEE 802.1Q značkou. Relativně zbytečné přeznačení rámce způsobuje nutnost výpočtu nového kontrolního součtu v poli FCS daného rámce, čímž dochází k mrhání výpočetním výkonem všech zúčastněných přepínačů. Takto provozovaná IP podsíť je jedinou výukovou podsítí a zároveň slouží pro přístup na konfigurační rozhraní všech síťových prvků, KVM zařízení, vestavěných rozhraní pro správu serverů a dalších s využitím IP protokolu.



Obr. 2.1: Schématické znázornění fyzické topologie

[1]Toto tvrzení je dokázáno analýzou konfigurace zařízení

Kompletní symbolické schéma zapojení laboratorních prvků je znázorněno na obr. 2.1. Je zde patrné připojení i několika virtuálních pracovních stanic, které jsou virtualizovány jak na koncových pracovních stanicích, tak na dedikovaném virtualizačním serveru. Tyto virtuální stroje jsou začleněny téměř výhradně pouze do experimentálních VLAN. Pracovní stanice využívají pro přístup do experimentálních VLAN sítí kombinace značkovaného a neznačkovaného provozu akceptovaného na příslušném rozhraní přepínače. Neznačkované rámce jsou začleněny do výukové VLAN s VID 310, resp. VID 1, značkované pak přímo do dané VLAN, pro kterou na daném rozhraní přepínač očekává rámce.

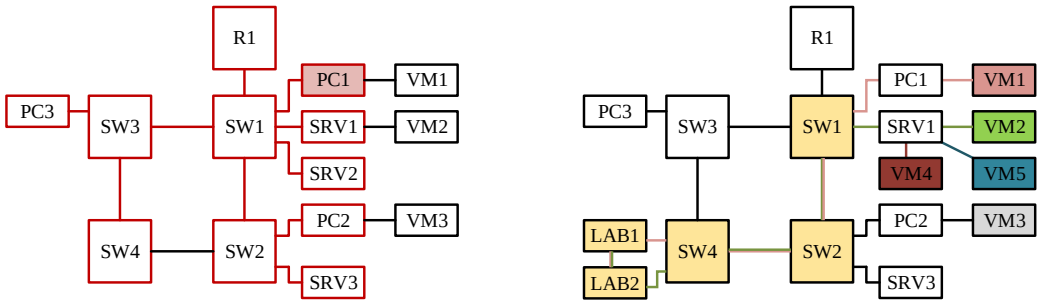
V případě virtualizace na vyhrazeném serveru je využito dedikované síťové karty, která je připojena k rozhraní na němž přepínač očekává značkované rámce pro dané VLAN sítě.

2.1.1 Dostupnost virtuálních sítí

Jak bylo uvedeno v předchozí kapitole, pracovní stanice umožňují mimo jiné přístup virtuálních strojů do experimentálních VLAN sítí, které jsou pomocí značkovaných rámců na trunk rozhraních vedeny k přepínači SW4. Ze schématu na obr. 2.1 je patrné cyklické propojení přepínačů SW1 – SW4, čímž vzniká riziko záplavového přepínaní rámců. K této situaci však nedochází z následujících důvodů:

- Mezi SW2 a SW4 se nešíří VLAN s VID 1,
- na spoji mezi SW1 a SW3 je šířena výuková VLAN s VID 310 a další experimentální VLAN pomocí značkovaných rámců,
- výuková VLAN je šířena pomocí neznačkovaných rámců na přístupové rozhraní mezi SW3 a SW4, kde má přidělenu platnou IP adresu
- mezi SW2 a SW4 jsou přenášeny jen experimentální VLAN sítě pomocí značkovaných rámců.

Zatímco výše popsané může být jednoduchým řešením pro odstranění smyčky v síti bez použití sofistikovaných řídících protokolů, přepínač SW3 ztrácí v topologii význam, neboť k němu nejsou připojena žádná experimentální zařízení a neslouží pro šíření experimentálních VLAN. Taktéž je nutno zohlednit případný tok rámců v síti pro jednotlivé VLAN sítě. Uvažujme dva scénáře, jež jsou zobrazeny na obr. 2.2a a obr. 2.2b. První scénář představuje šíření rámců sítí v případě, kdy stanice PC1 posílá rámce na všesměrovou adresu. Vzhledem k realizaci ethernetové sítě, může často docházet k zbytečnému či nežádoucímu šíření těchto rámců celou sítí. Se zvětšujícím se počtem zařízení v síti pak roste i procento zatížení sítě tokem rámců vysílaných na všesměrovou adresu. Dále lze předpokládat neoptimální využití výpočetních prostředků síťových zařízení, které dle specifických pravidel musí provádět přeznačení 802.1Q polí pro každý rámec výukové VLAN, který je šířen i mimo přepínač SW1.



(a) Všesměrové vysílání ve výukové VLAN

(b) Příklad šíření experimentální VLAN

Obr. 2.2: Šíření rámců dle příslušnosti do VLAN sítě

Obrázek 2.2b ilustruje komunikaci virtuální stanice s protějškem v experimentální VLAN síti. Tento scénář je přímo odvozen z topologie zapojení úlohy č. 2 předmětu Architektura sítí a znázorňuje fyzické zapojení prvků, které tvoří část topologie popisované v rámci laboratorní úlohy. Z obrázku je patrné neoptimální využití spojů i samotných přepínačů, neboť pro komunikaci mezi VM1 a VM2 jež je demonstrována s využitím směrovačů LAB1 a LAB2 v rámci úlohy dochází k zatížení dalších tří mezilehlých prvků fyzické topologie. Problematice násobného využití spojů a přepojovacích prvků je věnována kapitola 2.1.2.

2.1.2 Vlastnosti experimentálních topologií

V laboratorních úlohách se hojně využívá virtualizovaných stanic a serverů, které jsou často připojovány k fyzických prvkům, jež jsou předmětem laboratorních úloh. Připojení experimentálních zařízení laboratoře je zajištěno hlavním přepínačem v rozvaděči R3[2], který je dále připojen k přepínači zajišťující konektivitu fyzických pracovních stanic a serverů. Následující popis uvažuje příklad topologie pro úlohu předmětu Architektura sítí – Lab. 2: Zajištění kvalitativní podpory služeb v podnikových sítích.

V úloze prezentovaná topologie využívá pracovních stanic, IP telefonních přístrojů a serverů, které jsou připojeny k fyzickým síťovým prvkům. Popisovaná logická topologie je znázorněna pomocí zjednodušeného schématu se symbolickým značením na obr. 2.3a. Zobrazená topologie experimentálního pracoviště odpovídá fyzické topologii s využitím virtualizovaných stanic dle symbolického schématu jež je znázorněno na obr. 2.3b. Pro přehlednost schématu je zachováno symbolického značení[3] laboratorních prvků a celých produktových názvů využitých zařízení, jež tvoří

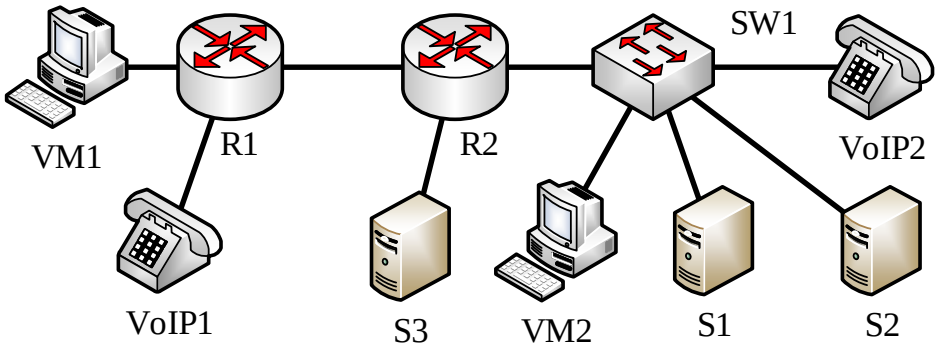
[2] Jedná se o prvky SW3 a SW4

[3] Značení prvků odpovídá značení v schématu na obr. 2.3a

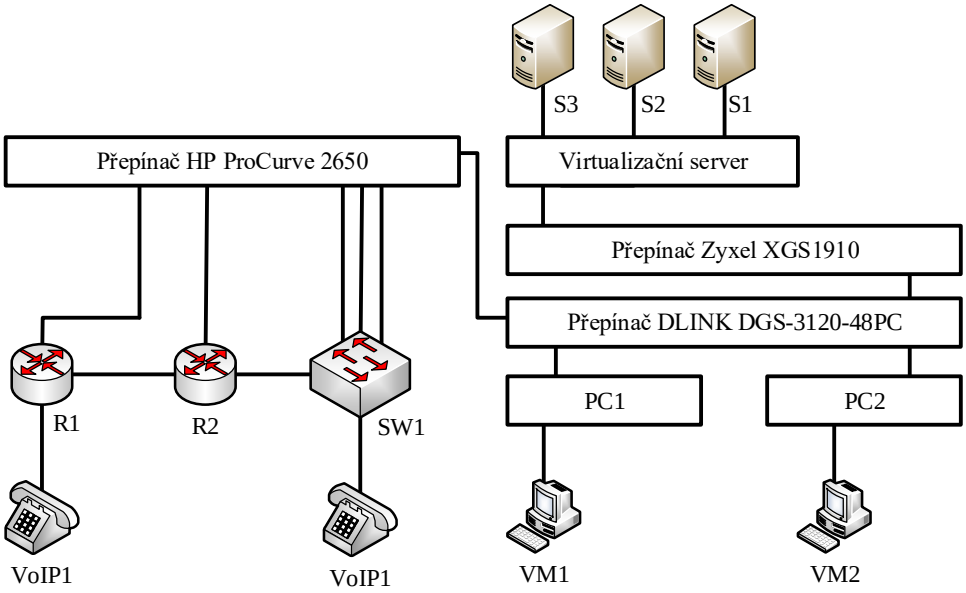
fyzickou topologii sítě. Je tedy patrné, že při komunikaci virtuálních počítačů s využitím fyzického vybavení laboratoře dochází k nadměrnému přenosu mezi prvky laboratoře a virtuálními počítači. K tomuto jevu dochází vzhledem k nevhodně zvolenému přípojnému bodu pro virtualizační server, a to i v případě, že spolu komunikují prvky VM2 a S1 či ostatní, tedy prvky, jež jsou v topologii laboratorní sítě zdánlivě připojeny k jedinému fyzickému přepínači.

Obr. 2.3: Srovnání fyzické a logické topologie pro úlohu BARS č. 2

(a) Logická topologie pro úlohu BARS lab. 2 [12]



(b) Skutečné zapojení zařízení pro úlohu BARS lab. 2



Tento nedostatek je vzhledem k charakteru laboratorních úloh odstranitelný vhodným připojením virtualizačního serveru přímo na rozhraní laboratorního pře-

pínače SW3 (HP ProCurve 2650). Tím dojde k zamezení nutnosti přenášet data po lince mezi přepínači SW1, SW2 a SW3 dvakrát pro zajištění jednosměrné komunikace.

Dále je nutno uvážit situaci, kdy v rámci laboratorní úlohy dochází ke komunikaci fyzické pracovní stanice s protistranou ve výukové VLAN. Tato situace je typická pro úlohu předmětu Architektura sítí - Lab. 8: Analýza SIP protokolu. V tomto případě se softwarový klient i hardwarový telefon připojují k softwarové IP PBX na virtuálním serveru. Všechna zařízení jsou však zařazena do stejné VLAN a nedochází zde k směrování mezi IP podsítěmi. Zde je problematické převážně připojení virtualizačního serveru, jež je realizováno pomocí stejného spoje typu trunk, který zajišťuje dostupnost ostatních experimentálních VLAN pro virtualizační server. Protože jsou k tomuto serveru připojeny všechny experimentální i výuková VLAN[4] pomocí jediného spoje, je velmi pravděpodobné, že vlivem nadměrného využití tohoto spoje a neaktivní podpoře QoS parametrů na přístupovém přepínači budou negativně ovlivněny výsledky laboratorní úlohy. Řešením tohoto nedostatku by bylo užití oddělených spojů mezi „serverovým“ přepínačem a virtualizačním hostitelem pro obsluhu experimentálních a výukové VLAN, případně přesun virtualizovaných serverů, které mají být připojeny do výukové VLAN na odlišný virtualizační server, který je užíván výhradně pro připojení zařízení ve výukové virtuální síti.

[4]V popisované úloze je použita výkouvá VLAN

3 NOVÁ ARCHITEKTURA DATOVÉ SÍTĚ

Datová síť popisovaná v této práci by měla sloužit jako základ pro realizaci velkého množství laboratorních úloh v rámci výuky síťových technologií, současně by však měla umožnit přístup do zbytku univerzitní sítě a internetu, měla by zajistit přístup k některým pokročilejším službám, které se běžně uplatňují v podnikovém prostředí a zároveň garantovat jistou míru spolehlivosti. Protože je k dispozici několik aktivních síťových prvků a pokročilé serverové technologie, práce zohledňuje i možnost zakomponování těchto prvků do výsledného návrhu.

Bohužel však nejsou k dispozici žádná data, která by potvrdila případné přetěžování spojů ať již vlivem popsaných nedostatků topologie sítě, či volbou nedostatečně výkonných přepínačů. Tato data budou pro další analýzu[1] zprostředkována především dohledovým systémem, jehož implementace je popsána v kapitole 5.1.

Nový model datové sítě vzniká v průběhu letního semestru paralelně s výukou v laboratoři. Z tohoto důvodu je zde použito zcela odděleného přepínače Cisco WS-3750X-48P, který je konfigurován pro účely hlavního přepínače formujícího jádro sítě. K dispozici je zde mj. 48 rozhraní 1000BASE-T, kterými je připojen nejen hraniční směrovač, ale i ostatní přístupové přepínače. Instalovaná verze operačního systému Cisco IOS obsahuje mj. balík *ipservices*, díky kterému je přepínač vhodný pro zajištění základních služeb na bázi protokolu IP (L3 přepínání, tvorba a aplikace ACL, DHCP Relay agent apod.).

Použitím L3 přepínače v jádru sítě se daná topologie stává velmi flexibilní a tvoří základ pro novou datovou síť s následujícími požadavky:

- konektivita pracovních stanic pomocí ethernetové sítě,
- konektivita laboratorního vybavení pomocí ethernetové sítě,
- chráněný přístup do univerzitní sítě a internetu pro PC,
- izolovaná L2/L3 konektivita pro laboratorní pracoviště,
- zálohovaná konektivita s využitím agregovaných spojů,
- odstranění nedostatků popsaných v předchozí kapitole.

V datové síti, která bude provozována v laboratoři pro realizaci výuky, bude potřeba zajistit přístup do sítě pro 24 pracovních stanic, které tvoří základ každého pracoviště v laboratoři. Každá pracovní stanice je vybavena síťovým rozhraním, které je použito pro přístup do místní sítě a pro realizaci experimentálního síťového prostředí, které zajišťuje spoj s experimentálními prvky laboratoře. Většina pracovních stanic využívá přístupu do experimentálních sítí pomocí značkování rámců a ostatní (neznačkované) hostitelský operační systém řadí do výchozí VLAN, která je na přístupovém přepínači definována jako VLAN s VID 10. Stejným způsobem je

[1] Například během výuky v zimním semestru

zajištěna konektivita v serverové části, avšak v oddělené VLAN s VID 20. Zvláštním případem je šíření VLAN s VID 90, která slouží výhradně pro správu a na přístupové přepínače je přivedena pouze kvůli realizaci virtuálního L3 rozhraní pro správu daného prvku. Do této VLAN sítě nikdy nebude zapojena koncová stanice či server[2], avšak mezi zařízeními (virtuální L3 rozhraní síťových prvků) bude k dispozici směrování a L3 přepínání. VLAN síť pro správu je šířena na všechny aktivní prvky síťové infrastruktury. Pro nově navrženou topologii zavádím i nové názvosloví

Tab. 3.1: Nové názvy pro aktivní síťové prkvy

Výrobce, model	**Hostname**	**IP adresa, VLAN 90**
Mikrotik RB800	RB-R2-CORE-01	10.10.90.2
Cisco WS-3750X-48P	SW-R2-CORE-01	10.10.90.1
Zyxel XGS1910	SW-R2-SRV-01	10.10.90.3
D-Link DGS-3120-48P	SW-R2-KLI-01	10.10.90.4
HP ProCurve 2650	SW-R3-LAB-01	10.10.90.5
HP ProCurve 2626	SW-R3-LAB-02	10.10.90.6

pro síťové prvky. Jejich názvy odpovídají vazbám dle tab. 3.1, které je mj. možno překládat pomocí DNS a to jak v případě A záznamů, tak i PTR.

Názvy aktivních prvků jsou voleny dle předem sjednané dohody, která si klade za cíl usnadnit správu daných zařízení (např. při vzdáleném přístupu pomocí emulovaného terminálu). První dvojice písmen je volena dle účelu daného zařízení, tedy

- **RB**: RouterBoard[3] – zařízení je směrovač,
- **SW**: Switch – zařízení je přepínač,
- **FW**: Firewall – zařízení je filtrační prvek,

R2 či **R3** značí umístění zařízení v technické místnosti (číslo racku), dále

- **CORE**: jde o zařízení tvořící jádro sítě,
- **SRV**: jde o zařízení serverového segmentu,
- **KLI**: jde o zařízení uživatelského segmentu,
- **LAB**: jde o zařízení připojující experimentální prvky.

Číslo ve jmenném schématu značí pořadí prvku daného typu v datové síti. Schématické zobrazení nově navržené datové sítě je patrné ze schématu na obr. A.1.

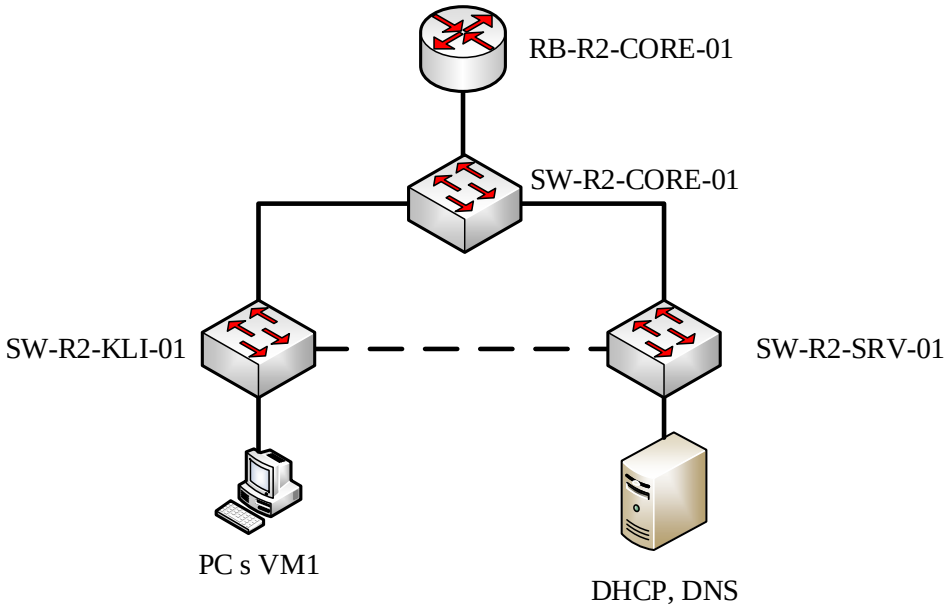
[2]Výjimkou jsou zařízení vyhrazena pro správu, tedy KVM přepínač, řídící jednotka PoN apod.

[3]RouterBoard je produktovým názvem pro směrovače značky Mikrotik. Vzhledem k jejich četnému zastoupení v technické místnosti je toto značení zvoleno záměrně namísto značení obecného (např. RO: Router).

3.1 Základní konektivita uživatelů sítě

Jak již bylo zmíněno, použitý přepínač Cisco WS-3750X nabízí funkcionalitu L3 přepínání a v novém návrhu bude použit jako přepínač jádra sítě. V sítích menšího rozsahu, mezi které patří i tato, je velmi časté splynutí distribuční vrstvy a vrstvy jádra sítě. Nově vytvořená topologie je uvedena na obr. 3.1.

Ze schématu datové sítě je patrná realizace uživatelského a služebního fragmentu pouze pomocí dvou přepínačů. Ty jsou následně připojeny k „centrálnímu“ L3 přepínači, na jehož rozhraní dochází mj. k směrování IP paketů mezi jednotlivými VLAN sítěmi. Z tohoto zapojení vyplývá nárok na dostupnost dílčích spojů s přepínačem v jádru sítě, proto jsou tvořeny agregovaným kanálem, který v případě výpadku jednoho z páru tvořící logický kanál zajistí konektivitu pro daný fragment. Přístupová



Obr. 3.1: Infrastruktura datové sítě bez experimentálních topologií

vrstva je jak pro uživatelský, tak i služební fragment tvořena dvěma vzájemné propojenými přepínači. V případě užití jednoho přepínače pro pracovní stanice a druhého pouze pro serverová zařízení se značně zjednoduší konfigurace obou přístupových přepínačů. Taktéž je možno „globálně“, tedy s rozsahem platnosti na všechna rozhraní serverového přepínače aplikovat jiný stupeň zabezpečení než v případě přepínače, který slouží pro připojení pracovních stanic studentů a jehož rozhraní jsou vyvedena na jednotlivá pracoviště. Tato realizace však zavádí do datové sítě zvýšené nároky na dostupnost serverové infrastruktury. V případě, že serverový segment bude pro pracovní stanice nedostupný, pracovní stanice ztratí přístup ke službám DHCP,

DNS i doménovým službám Active Directory. Nedostupnost těchto služeb znemožní veškerou práci uživatelů pracovních stanic, neboť v případě nedostupnosti doménového kontroléru nebude možno autentizovat uživatelské účty v databázi AD[4] [1].

Z tohoto důvodu je pomocí rozhraní typu trunk přivedena serverová VLAN s VID 20 i na přístupový přepínač klientů. Na tomto přepínači je vyčleněno rozhraní č. 41 pro připojení ADC, sekundárního DNS server a sekundárního DHCP serveru. Tím je zajištěna dostupnost základních síťových služeb a možnost užití pracovních stanic i v případě, že všechna zařízení vč. samotného přepínače serverového segmentu budou odpojena.

Pro každou podsíť je na přepínači v jádru sítě vytvořeno virtuální L3 rozhraní, kterému je přiřazena první použitelná adresa daného segmentu, tedy např. 10.10.10.1 z rozsahu adres 10.10.10.0/24. Obdobné adresní schéma platí pro podsíť vyhrazenou pro serverová zařízení a podsíť určenou pro správu síťových prvků, tedy IP podsítě ve VLAN sítích s VID 20 a 90. Dále je na přepínači v jádru sítě vytvořená další VLAN s VID 100, která je přenášena pouze mezi přepínačem a hraničním směrovačem. V této VLAN je nasazena IP podsíť z rozsahu 10.10.0.0/24, která zajišťuje dvoubodový spoj pro přenos datových jednotek k výchozímu (hraničnímu) směrovači. Tím je zajištěna konektivita do univerzitní sítě a internetu pro všechna zařízení v laboratorních podsítích s výjimkou experimentálních zařízení, resp. podsítí definovaných v experimentálních VLAN sítích.

3.1.1 Konfigurace přepínače Cisco WS-3750X-48P

Přepínač Cisco WS-3750X-48P je v datové síti agregačním prvkem pro komunikaci mezi VLAN s VID 10, 20 a 90. Pro tento prvek bylo zvoleno jméno SW-R2-CORE-01. Zařízení tvoří tzv. jádro sítě a nabízí funkci L3 přepínaní, tedy směrování mezi VLAN sítěmi, které jsou zpravidla definovány na přístupových přepínačích. Pro každou takovou VLAN je na tomto přepínači vytvořeno virtuální L3 rozhraní s první platnou adresou dané IP podsítě. Spoje k oběma přístupovým přepínačům jsou tvořeny agregovaným kanálem s využitím dvou fyzických linek. Maximální teoretická dostupná kapacita je tedy dle rov. 1.1 rovna $C = 2$ Gbit/s. Redundantní spoj je zde zvolen z důvodu zajištění konektivity v případě selhání jedné z linek, nikoli s cílem zajistit vyšší přenosovou kapacitu mezi přístupovou částí a částí jádra sítě.

Přenos rámců mezi přístupovými přepínači i hraničním směrovačem probíhá výhradně pomocí značkovaných rámců. Specifikem této konfigurace je nastavení výchozí VLAN, pro všechna rozhraní na neexistující VLAN s VID 3 a zamezení šíření VLAN s VID 1. Tím je zamezeno přenosu rámců, které nepatří do předem definované VLAN sítě. Na tomto přepínači jsou vyhrazena rozhraní pro přístup do VLAN

[4] V krajním případě dojde k odepření přístupu k pracovní stanici

s VID 90, kam může pouze správce (rozhraní nejsou vyvedena na přepojovací panel a přivedena na LAN zásuvky na pracovištích laboratoře) připojit zařízení, jejichž účelem je správa síťové infrastruktury. Zpravidla jde o zařízení přepínače KVM, Power over Net, UPS a další. Pro tato zařízení je zvoleno připojení k prvku sítě u kterého se předpokládá maximální dostupnost – např. vlivem ztráty konektivity na přepínači SW-R2-SRV-01 tak nedojde k možnosti vzdáleného řízení serverů pomocí KVM.

Přestože na přepínači nejsou konfigurovány funkce ARP Inspection, Port Security apod., režim provozu přepínače lze označit za provoz s zvýšenou bezpečnostní úrovní pro zajištění konzistence topologie datové sítě. Tomu odpovídá i nasazení ochranných mechanismů PortFast a BPDU Guard. Dále je na rozhraní, která tvoří logický spoj s přístupovými směrovači nastaven limit přenosu rámců zaslaných na všesměrovou adresu pomocí funkce Storm Control. Tato funkce pro dané rozhraní definuje úroveň vztaženou k dostupné přenosové kapacitě rozhraní, které může dosahovat v daném intervalu určitý typ provozu [8]. Interval je volen s délkou trvání jedné sekundy a úroveň v případě všesměrových zpráv volím $L = 0{,}125$. Pro konfiguraci na rozhraní, jehož teoretická maximální propustnost je 2 Gbit/s způsobí konfigurace

```
interface port-channel 10
sotrm-control broadcast level 0.125
```

omezení kapacity na rozhraní `port-channel 10` pro šíření rámců zaslaných na všesměrovou adresu na hodnotu 250 Mbit/s. Pro podsíť klientských zařízení zavádím omezení komunikace pracovních stanic s prvky v síti VLAN s VID 90, tedy IP podsítě 10.10.90.0/24, jež je určena pouze pro správu a konfiguraci těchto zařízení. V podsíti 10.10.10.0/24 je vyhrazena jedna pracovní stanice (PC lektora s DHCP rezervací), které jediné je umožněn plný přístup do zmíněné podsítě. K filtrování datových jednotek používám rozšířených seznamů pro řízení přístupu a aplikuji jej pouze v příchozím směru na virtuální rozhraní pro VLAN 10, tedy:

```
acc-li 100 permit ip host 10.10.10.50 10.10.90.0 0.0.0.255
acc-li 100 deny ip 10.10.10.0 0.0.0.255 10.10.90.0 0.0.0.255
acc-li 100 permit ip any any

interface Vlan10
  description %Client VLAN interface%
  ip address 10.10.10.1 255.255.255.0
  ip access-group 100 in
```

Výše popsané zajistí požadovanou bezpečnost a znemožní směrování L3 přepínačem pro všechny pracovní stanice v této podsíti s výjimkou lektorského PC, kde je

naopak žádoucí dostupnost všech prvků v dané podsíti. Kromě výše popsané konfigurace přidávám všechny experimentální VLAN sítě na vyhrazený spoj typu trunk na rozhraní mezi SW-R3-LAB-01 a SW-R2-LAB-01 pro zajištění alternativní cesty v datové síti pro šíření experimentálních VLAN, viz 3.3. Dále konfiguruji obecná nastavení, IP adresy SNTP serverů, přístup pomocí SNMP s oprávnění pro čtení a zasílání zpráv SNMP Trap na centrální dohledový prvek. Zbytek konfigurace zařízení je nad rámec textu a je dostupný na přiloženém DVD.

3.1.2 Konfigurace přepínače DLINK 3120-48PC

Přepínač DLINK 3120-48PC s odpovídajícím názvem SW-R2-KLI-01 nabízí 48 rozhraní pracujících rychlostí až 1 Gbit/s a 4 šachty pro připojení SFP+ modulů. Přístup na konfigurační rozhraní je možný přes virtuální L3 rozhraní, kterému je ve výchozím stavu přiřazena adresa DHCP serverem. Konfigurace přepínače je možná pomocí webového rozhraní, protokolů Telnet a SSH pro terminálový přístup a pomocí sériového rozhraní RS-232. Na přepínači je konfigurace, která umožňuje provoz datové sítě popsané v kapitole 2.1. V této konfiguraci provádím změny, které umožňují provoz dle výše popsaného konceptu. Výsledná konfigurace je k dispozici v textové podobě a je přiložena na disku DVD. Tato kapitola slouží jako komentovaný rozbor relevantních částí konfigurace.

Nový model datové sítě zohledňuje dostupnost virtuálních VLAN s VID 10, 20 a 90. Prvním krokem je konfigurace VLAN dedikované pro správu daného prvku, tedy VLAN s VID 90, která je šířena na trunk rozhraní připojující nadřazený přepínač v jádru sítě. Jde o rozhraní 1:47 a 1:48 (zatím nejsou přiřazeny do LACP kanálu). Následně je tato VLAN určena jako VLAN pro správu, dojde tedy k vytvoření virtuálního L3 rozhraní, kterému je následně možno přiřadit IP adresu z rozsahu 10.10.90.0/24.

```
# VLAN
create vlan Management tag 90
config vlan Management add tagged 1:47-1:48
  advertisement disable

# IP
config ipif System ipaddress 10.10.90.4/24 vlan Management
  advertisement disable
disable autoconfig
```

Obdobným způsobem jsou na přepínači vytvořeny všechny VLAN sítě, avšak není jim přiřazena žádná IP adresa. Z výše uvedeného vyplývá konfigurace rozhraní jako

typ trunk, neboť jsou zde akceptovány značkované rámce. Příklad definice VLAN s VID 10 a přístupových rozhraní 1:01 – 1:42, je pak analogicky:

```
# VLAN
create vlan Klienti tag 10
config vlan Klienti add tagged 1:47-1:48
config vlan Klienti add untagged 1:1-1:42
```

Opět je tato VLAN šířena i na trunk rozhraní nadřazeného přepínače v jádru sítě, konkrétně pomocí portů č. 47 a 48. Rozhraní, které přenáší pouze značkované rámce[5], tedy mj. rozhraní spoje mezi SW-R2-KLI-01 a SW-R3-LAB-01 je pak konfigurováno dle[6]:

```
# VLAN
create vlan Exp320 tag 320
config vlan Exp320 add tagged 1:1,1:46-48
  advertisement disable
create vlan Exp321 tag 321
config vlan Exp321 add tagged 1:2,1:46-48
  advertisement disable
create vlan Exp322 tag 322
config vlan Exp322 add tagged 1:3,1:46-48
  advertisement disable

# -- výstup zkrácen --
```

V této fázi jsou nastavena jednotlivá rozhraní přepínače pro potřeby šíření experimentálních VLAN sítí a pro přístup do VLAN sítě pracovních stanic pomocí neznačených rámců, tedy VLAN s VID 10. Oddělení jednotlivých pracovišť je zde realizováno nastavením konkrétních VLAN sítí, pro které přístupový přepínač na daném rozhraní akceptuje patřičně značkované rámce. Následuje konfigurace zmíněného logického kanálu složeného ze dvou fyzických spojů s přepínačem v jádru sítě. K tomu jsou použita rozhraní č. 47 – 48 a následující direktiva:

```
# LACP
config link_aggregation algorithm mac_source
create link_aggregation group_id 10 type lacp
config link_aggregation group_id 10
  master_port 1:48 ports 1:47-1:48 state enable
config lacp_port 1:1-1:48 mode passive
```

[5]V této ukázce jde o porty 1:45-48

[6]Nutnost šíření specifických experimentálních VLAN sítí vychází ze znalosti obsahu a řešení lab. úloh popsaných v [12]

Z výše uvedeného je patrné přiřazení portů 47 a 48 do logického kanálu s ID 10. Přestože je primárním účelem zajištění redundance mezi dvěma přpínači, LACP protokol definuje i algoritmy pro rozkládání zátěže mezi fyzickými linkami. Všechna rozhraní jsou nastavena v pasivním režimu, iniciaci agregovaného kanálu provádí nadřazený přepínač.

Podstatnou částí konfigurace je i zavedení bezpečnostních mechanismů popsaných v kap. 1.3.2 až 1.3.4. Jde o konfigurace souhrnně označované jako Port Security, ARP Spoofing Prevention a DHCP Server Screening.

```
# PORT_SECURITY
config port_security system max_learning_addr no_limit
config port_security vlan vlanid 10 max_learning_addr 40
config port_security ports 1:1-1:40 admin_state enable
  max_learning_addr 3 lock_address_mode deleteontimeout

# ARPSpoofingPrevention
config arp_spoofing_prevention add  gateway_ip 10.10.10.1
  gateway_mac 70-CA-9B-80-F1-41 ports 1:47-1:48

# DhcpServerScreening
config filter dhcp_server ports all state disable
config filter dhcp_server
  illegal_server_log_suppress_duration 5min
config filter dhcp_server
  add permit server_ip 10.10.20.15 ports 1:47-1:48
config filter dhcp_server trap_log disable
```

Z výše uvedené konfigurace je v případě funkce kontroly validity ARP nastavena jediná MAC adresa, která může být obsažena v datových jednotkách ARP Reply při hledání MAC adresy odpovídající IP adrese výchozí brány sítě, v tomto případě tedy 10.10.10.1. Dále zavádím limity aktivních MAC adres na přístupových rozhraních, jež jsou určena pro pracní stanice, na maximální možný počet 3 MAC adres registrovaných k jednomu portu, celkem pak 40 MAC adres pro přístupová rozhraní[7] pro VLAN s VID 10 (1 MAC adresa pro každé rozhraní).

Poslední, avšak velmi významnou částí, je nastavení SNTP klienta a sad informací, které budou zpřístupněny pomocí SNMP OID a zasílány na centrální monitorovací systém (Zabbix server, IP 10.10.20.20). SNTP klient používá časových informací získaných z obou doménových kontrolérů. Tato konfigurace je velice užitečná pro případ dohledávání událostí a jejich porovnávání s událostmi na dalších prvcích

[7]Jde tedy o porty 1:1-40

sítě. Synchronní časová informace je také velmi podstatná pro záznam událostí s časovou značkou.

```
# SNTP
enable sntp
config time_zone operator + hour 1 min 0
config sntp primary 10.10.20.2
  secondary 10.10.20.15 poll-interval 720
config dst annual s_date 29 s_mth 4 s_time 0:0
  e_date 12 e_mth 10 e_time 0:0 offset 60
config dst repeating s_week last s_day sun s_mth 3 s_time
  2:0 e_week last e_day sun e_mth 10 e_time 3:0 offset 60

# MANAGEMENT
enable snmp
enable snmp traps
enable snmp linkchange_traps
config snmp system_name SW-R2-KLI-01
config snmp system_location SC5-32-R2
config snmp system_contact novotnyv@feec.vutbr.cz
config snmp linkchange_traps ports 1:1-1:48 enable
create snmp community public view CommunityView read_only
# -- výstup zkrácen --
```

Výpis kompletní konfigurace v textovém formátu je dostupný na přiloženém DVD. Záměrně jsou zde vynechány pasáže, které by mohly kompromitovat bezpečnost daného prvku (definice uživatelských účtů, metody autentizace, přístupové metody apod.). Taktéž nastavení SNMP komunit pro potřeby práce záměrně nechávám ve výchozím stavu a jako komunitu s oprávněním pro čtení hodnot nechávám výchozí s názvem *public*. V praxi se tato komunita většinou z bezpečnostních důvodů nepoužívá a případný budoucí správce datové sítě musí zajistit patřičnou úpravu tohoto nastavení[8].

3.1.3 Konfigurace přepínače Zyxel XGS1910

Stejně jako v případě přístupového přepínače SW-R2-KLI-01 se v této kapitole věnuji rozboru nastavení přepínače SW-R2-SRV-01 zajišťujícího konektivitu serverového segmentu. Bohužel je exportovaná konfigurace uložena do XML souboru, jehož pasáže nejsou do textu práce. Z tohoto důvodu je tato kapitola pouhým komentovaným rozborem a neobsahuje ukázky konfigurace.

[8]Konkrétní nastavení není z bezpečnostních důvodů v textu práce zveřejněno

Jak již bylo zmíněno, přepínač serverového segmentu je vyhrazen pouze pro potřeby konektivity serverových zařízení. Z tohoto důvodu jsou odstraněny některé konfigurace v oblasti bezpečnosti. Základním předpokladem je, že žádný uživatel nemá fyzicky přístup k rozhraní tohoto přepínače. Stejně tak nejsou zásuvky tohoto přepínače připojeny na přepojovací panel a na studentská pracoviště. Jsou zde také připojeny virtualizační servery, které poskytují konektivitu mnoha virtuálním stanicím. Konfigurace limitu MAC adres na takové rozhraní je velmi kontraproduktivní (hodnoty se mohou dynamicky měnit v rámci migrace za provozu), efektivní fungování mechanismů ARP Inspection je zde limitováno převážně z důvodu staticky přiřazovaných adres.

Přepínač Zyxel XGS1910 disponuje celkem 48 porty standardu 1000BASE-T a osmi šachtami pro připojení SFP+ modulů. Tyto šachty však nejsou využity a pro připojení k nadřazenému přepínači v jádru sítě je použito metalického kabelu. Správa zařízení je možná pouze pomocí webového rozhraní nebo připojením na fyzické rozhraní konzole. Protože většina zde připojených zařízení obsahuje více rozhraní či síťových karet, je zde ve velké míře konfigurována agregace fyzických linek a to i v případě připojování koncových zařízení (serverů). Tím je zajištěna jednak větší spolehlivost připojení, ale i lepší rozkládání zátěže mezi více spojů. Pro serverový segment je typická velmi častá vzájemná komunikace serverů v rámci lokální sítě (VLAN 20). Příkladem této komunikace je migrace virtuálních strojů mezi Hyper-V hostiteli. Jedná se zejména o přenos virtuálních pevných disků, které jsou k jednotlivým serverům připojeny ze sdíleného síťového úložiště či přenos SCSI příkazů s užitím IP protokolu pomocí iSCSI.

Základní konfigurace zahrnuje opět tvorbu všech VLAN sítí a jejich přiřazení dle portů. Dále je zde vytvořeno virtuální L3 rozhraní pro správu zařízení, které je opět přiřazeno do VLAN s VID 90 a IP adresou z odpovídajícího rozsahu dle tab. 3.1. Dále při konfiguraci obecných nastavení vždy uvádím validní informace do polí Contact, Name a Location – tyto informace jsou přenášeny v OID objektech informační báze pomocí SNMP protokolu a usnadňují identifikaci a inventarizaci pomocí centrálního dohledového prvku.

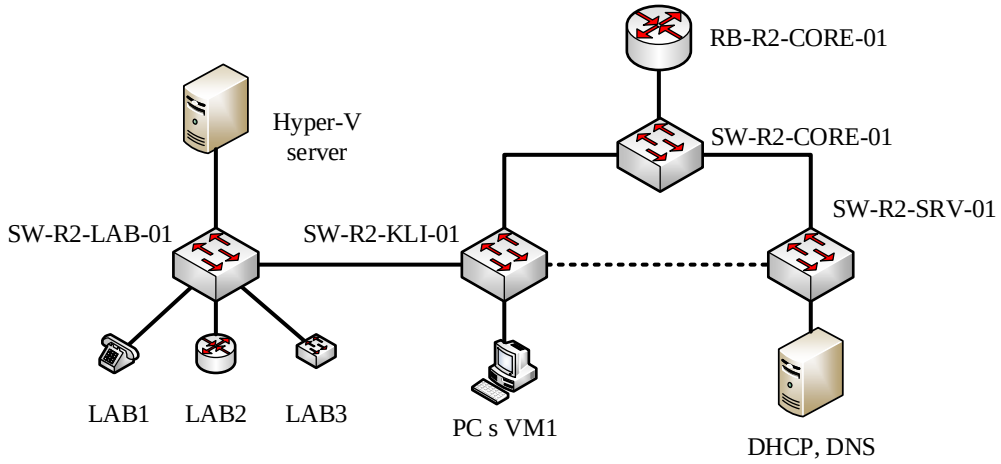
Podstatnou odlišností v konfiguraci ve srovnání se SW-R2-KLI-01 je mnohonásobné připojování serverových zařízení na více rozhraní jednoho přepínače. Virtualizační servery disponují 4 – 6 rozhraními a zpravidla dvěma síťovými kartami. Z tohoto důvodu je vhodné využít agregaci a vyčlenění specifických VLAN sítí, které se na daném kanále mohou šířit. Pro server, na kterém jsou provozovány kritické komponenty sítě, konfigurace těchto rozhraní umožní přenos rámců s VID 10 a 20.

Protože je k tomuto přepínači připojeno mj. úložné zařízení Lenovo px6-300, které slouží jako centralizované úložiště pro laboratorní síť i jako sdílené úložiště pro virtualizační cluster, obě jeho rozhraní taktéž konfiguruji do agregovaného kanálu.

Předností této konfigurace je mj. odstranění všech experimentálních VLAN sítí z konfigurace tohoto přepínače. Mezi SW-R2-SRV-01 a SW-R2-KLI-01 se již experimentální sítě nebudou přenášet, resp. na tomto přepínači již nebude připojeno trunk rozhraní k virtualizačnímu serveru. Není tedy vhodné, aby se mezi těmito prvky dále přenášely a všesměrovým vysíláním využívaly kapacitu spoje. VLAN sítě jsou jednotlivým rozhraním přiřazena vždy staticky. Kompletní tabulka přiřazení a výpis konfigurace přepínače je dostupný na přiloženém DVD.

3.2 Připojení experimentálních sítí

Dosud popsaná topologie neuvažuje konektivitu ostatních zařízení, převážně pak experimentálních síťových prvků, jejichž konfigurace bývá obsahem laboratorních cvičení. Původní návrh zajišťuje dostupnost experimentálních zařízení pomocí přepínače HP ProCurve 2650, na jehož rozhraní se mezi přepínači SW-R2-KLI-01, SW-R2-SRV-01 a SW-R3-LAB-01 přenáší značkované rámce experimentálních VLAN sítí. Tato realizace vzhledem k charakteru laboratorních úloh velmi nevhodná. Použitý virtualizační server nabízí dostatečný počet rozhraní, která je možno připojit dle potřeby na přístupové přepínače tak, aby byla zajištěna nejkratší možná cesta sítí mezi dvěma přímo komunikujícími stanicemi. Bohužel jsou na přepínači SW-R3-



Obr. 3.2: Komunikace mezi komponentami laboratorní úlohy

LAB-01 (model HP ProCurve 2650) dostupná pouze dvě rozhraní typu 1000BASE-T. Z tohoto důvodu bude jedno rozhraní dedikováno pro přenos značkovaných rámců mezi přepínačem SW-R2-KLI-01 připojující pracovní stanice studentů a druhé rozhraní pro přímé připojení virtualizačního serveru. Pomocí značkovaných rámců jsou mezi dvěma přepínači přenášeny rámce doplněné patřičnou značkou dle příslušnosti

stanice k dané laboratorní úloze. Zapojení aktivních prvků a zúčastněných stanic pro komunikaci dle potřeb laboratorních úloh je znázorněno na obr. 3.2.

Ze schématu upravené topologie je patrné zapojení virtualizačního hostitele k přepínači SW-R3-LAB-01. Hlavní předností je podstatná redukce počtu prvků, které se podílí na šíření experimentálních VLAN sítí. Druhou výhodou je snížení nutnosti komunikace na rozhraní typu trunk mezi přepínačem připojující pracovní stanice a laboratorní prvky. Nevýhodou tohoto relativně jednoduchého zapojení je však opět značné omezení provozu v případě výpadku jednoho ze spojů mezi prvky experimentální části a prvky studentských pracovišť. Riziko naprostého selhání lze částečně snížit připojením dalšího spoje, který zajistí dostupnost experimentálních VLAN sítí i v případě selhání spoje mezi SW-R3-LAB-01 a SW-R2-KLI-01. Zde je konfigurováno šíření experimentálních VLAN sítí z klientského přepínače i přes prvek jádra (SW-R2-CORE-01) a následně k přepínači SW-R3-LAB-01. Toto propojení zajistí přijatelnou míru redundance a ochranu proti selhání spoje mezi zmíněnými přepínači, avšak záložní linka bude realizována pouze spojem typu 100BASE-TX, resp. s rychlostí dle rov. 1.1 v případě agregovaného kanálu. Dále bude potřeba pomocí řídícího protokolu využívajícího algoritmu hledání kostry grafu zajistit odstranění smyček v síti.

3.2.1 Konfigurace přepínače HP ProCurve 2650

Hlavním přepínačem v rozvaděči pro připojení experimentálních prvků je přepínač HP ProCurve 2650 s názvem SW-R3-LAB-01. Toto zařízení zajišťuje konektivitu mezi experimentálními prvky laboratorních úloh a virtualizovanými pracovními stanicemi, resp. virtuálními servery. Přestože zařízení nabízí až 50 portů, pouze dva jsou schopné práce v režimu dle 1000BASE-T. To je podstatnou limitací hlavně pro implementaci alternativních tras experimentálních topologií. Obě tato rozhraní jsou využita – rozhraní č. 49 připojuje přepínač SW-R2-KLI-01 a přenáší všechny experimentální a dedikovanou management VLAN. Druhé rozhraní je vyhrazeno pro zajištění zmíněné konektivity virtualizačního hostitele, tedy pro přístup do experimentálních sítí pomocí značkovaných rámců pro 10 virtualizovaných serverů.

Je tedy patrné, že pro komunikaci virtualizované stanice na pracovních stanicích studentů s virtuálním serverem provozovaným na virtualizačním hostiteli je nutné zajistit dostupnost patřičných VLAN sítí na obou portech přepínače. Konfigurace specifických VLAN sítí je realizována na základě analýzy VLAN sítí konfigurovaných na virtualizačním serveru, resp. jejich přiřazení virtuálním stanicím[9]. Přepínač SW-R3-LAB-01 pro žádnou z experimentálních sítí nenabízí funkce síťové vrstvy, na jeho rozhraní tedy nedochází ke směrování, filtraci, ani zajištění kvality služby.

[9]Realizováno mimo text práce

Na přepínači je na rozhraní s přepínačem SW-R2-KLI-01 šířena i VLAN s VID 90, jejíž účel je vyhrazen pro správu síťových prvků. Dále je pro tuto VLAN síť vytvořeno virtuální IP rozhraní s IP adresou 10.10.90.5 z odpovídajícího rozsahu. Přípojení k tomuto přepínači je možné mj. konzolovým kabelem či protokolu Telnet pro realizaci virtuálního terminálu.

Konfigurace tohoto přepínače byla před realizací nového řešení laboratorní sítě zanechána ve velmi nevyhovujícím stavu. Největším nedostatkem je samotné šíření VLAN, která je užita pro správu (byla zde použita výuková VLAN 310 a přivedena pomocí neznačkovaných rámců na přístupové rozhraní z přepínače SW3 (viz 2.1). Z tohoto důvodu nově definuji VLAN s VID 90 a mapuji ji na rozhraní připojující přepínač SW-R2-KLI-01. Spoj k přepínači HP ProCurve 2626 (ve schématu 2.1 jde o spoj mezi SW3 a SW4) bude zcela zrušen a jako alternativní způsob šíření jednotlivých VLAN bude v případě výpadku spoje mezi SW-R2-KLI-01 a SW-R3-LAB-01 použit přepínač SW-R2-CORE-01.

Při konfiguraci doplňuji zcela chybějící obecné informace o zařízení – tedy umístění, informace pro kontaktování správce a nastavuji synchronizaci časových údajů pomocí SNTP protokolu s dvěma doménovými kontroléry[10]. Dále nastavuji možnost sběru dat pomocí SNMP protokolu a zasílání SNMP „upozornění“ (SNMP Traps) na dohledový server s IP 10.10.20.20. Kompletní konfigurace je k dispozici na přiloženém DVD.

3.2.2 Konfigurace přepínače HP ProCurve 2626

S přechodem na nový koncept datové sítě zůstal přepínač HP 2626 nevyužitý. Jeho účelem bylo šíření výukové VLAN na rozhraní přepínače HP 2650 a – jak je patrné z obsažené konfigurace – některých experimentálních. Protože tyto požadavky v nové struktuře datové sítě zanikají, dle dohody tento přepínač konfiguruji pro budoucí rozšíření laboratorní sítě, tedy šíření VLAN s VID 10, 20 a 90. Jeho konfigurace je typově obdobná jako v případě přístupového přepínače klientů, avšak nejsou zde aktivovány bezpečnostní funkce typické pro přístupový přepínač SW-R2-KLI-01. Fyzicky se tento přepínač nachází v rozvaděči R3, kde z technických důvodu již není možné realizovat další spoj k rozvaděči R2. Zařízení, která by bylo nutno připojit k přepínačům SW-R2-KLI-01 a SW-R2-SRV-01 a jež nevyžadují použití rozhraní standardu 1000BASE-T, je možno připojit až na 24 rozhraní tohoto přepínače. Typicky jde o bezdrátové přístupové body či zařízení Serial over Net.

Konfiguraci provádím pomocí virtuálního terminálu realizovaným protokolem Telnet. Nastavuji základní konfiguraci[11] – název zařízení SW-R3-LAB-01, IP adresy

[10] Tato obecná konfigurace je aplikována i na zbylé prvky datové sítě

[11] Typicky shodnou pro všechna zařízení popsaná v předchozích kapitolách

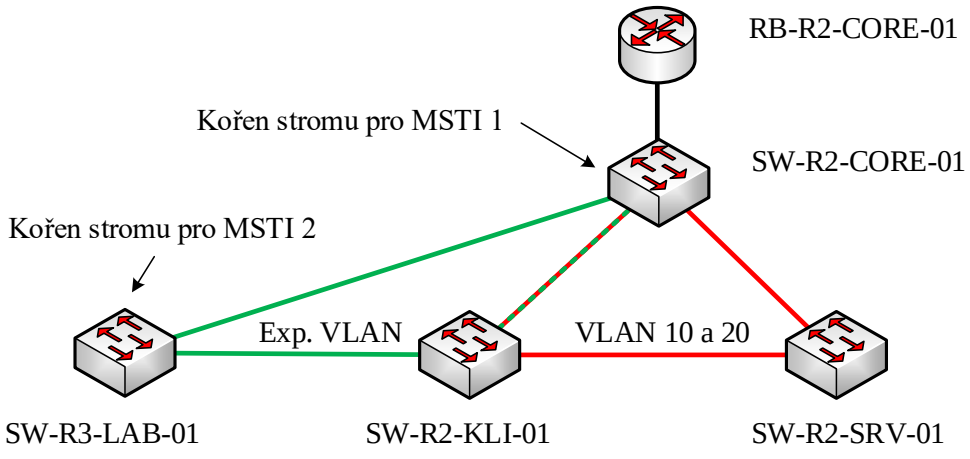
SNTP serverů, konfiguraci pro realizaci dohledu pomocí SNMP a další. Kompletní konfigurace je k dispozici na přiloženém DVD.

3.3 Odstranění smyček pomocí MSTP

Z výše popsané konfigurace je patrné zavádění smyčkové topologie z důvodu zajištění redundance mezi celky datové sítě. Obecně tuto síť dělím na dvě samostatné části, každá s odlišnými požadavky na dostupnost a výkon topologie.

- **Produkční infrastruktura** – červené vyznačená část, tedy segment datové sítě, který pomocí základních síťových služeb zajišťuje provoz pracovních stanic (DNS, DHCP, AD DC),
- **experimentální infrastruktura** – zeleně vyznačená část, tedy segment datové sítě, který zajišťuje realizaci experimentálních topologií a zpracování laboratorních úloh.

Toto hrubé rozdělení vyplývá z obrázku 3.2. Na základě této skutečnosti realizuji první smyčkové zapojení mezi přepínači SW-R2-CORE-01, SW-R2-KLI-01 a SW-R2-SRV-01. Jde tedy o dvě VLAN sítě, které je v rámci MSTP protokolu vhodné mapovat do samostatné instance – v případě změny topologie vlivem výpadku budou tyto VLAN sítě postiženy stejnou mírou, neboť se z jádra sítě šíří současně na stejné přepínače. Tyto VLAN sítě přiřazuji do první instance MSTP protokolu, tedy MSTI 1. Experimentální infrastruktura tvoří samostatný celek, který koexistuje



Obr. 3.3: Infrastruktura datové sítě bez experimentálních topologií

s produkční infrastrukturou a do jisté míry na něm závisí (šíření VLAN s VID 90).

Pro experimentální sítě je specifické jejich šíření mezi prvky SW-R2-KLI-01, SW-R3-LAB-01 a SW-R2-CORE-01. Přepínač v jádru sítě je jako alternativní prvek zvolen záměrně z důvodu dostatečné přepínací kapacity a množství neobsazených portů. Pro veškeré experimentální sítě, které se šíří mezi dvěma primárními přepínači (SW-R2-KLI-01 a SW-R2-LAB-01) a záložním přepínačem v jádru sítě volím další instanci MSTP protokolu – MSTI 2. Opět zde platí, že v případě potřeby hledání alternativní kostry grafu vlivem nedostupnosti primárního spoje bude potřeba přes záložní přepínač šířit všechny experimentální VLAN sítě.

Smyčková topologie obou částí infrastruktury je patrná ze schématu na obr. 3.3. Ze schématu jsou patrné i preferované volby kořenů stromů pro obě instance. Pro produkční infrastrukturu je nejvhodnější volbou přepínač v jádru sítě, a to zejména kvůli redundantním propojům, rychlosti a charakteru šíření VLAN sítí s VID 10 a 20. Naopak pro experimentální topologie je vhodné za kořen stromu zvolit přepínač SW-R3-LAB-01 a úpravou priorit daného rozhraní zajistit preferovanou komunikaci s využitím primárního spoje, a to z následujících důvodů :

- Spoj mezi SW-R2-KLI-01 a SW-R3-LAB-01 představuje nejkratší cestu šíření rámců v experimentálních VLAN,
- k SW-R3-LAB-01 mohou být v budoucnu připojeny další přepínače pro šíření experimentální infrastruktury,
- mezi SW-R3-LAB-01 a SW-R2-CORE-01 je dostupný spoj 100BASE-TX.

Volba kořene stromu podléhá mj. i nastaveným prioritám a platí, že nižší hodnota priority (udávaná zpravidla v násobcích 4096 [13] [11])[12] indikuje vhodnější přepínač pro kořen stromu. Pro případ zajištění role kořene pro přepínač SW-R2-CORE-01 je v konfiguračním režimu pro danou MSTI použita hodnota prioritiy 8192:

```
SW-R2-CORE-01(config)#spanning-tree mst configuration
SW-R2-CORE-01(config-mst)#revision 1
SW-R2-CORE-01(config-mst)#instance 1 vlan 10, 20
SW-R2-CORE-01(config)#spanning-tree mst 1 priority 8192
```

Po konvergenci MSTP protokolu je možno ověřit výběr kořene dle:

```
SW-R2-CORE-01#show spanning-tree mst
-- výstup zkrácen --

##### MST1    vlans mapped:   10,20
Bridge        address 70ca.9b80.f100  priority  8193
Root          this switch for MST1
-- výstup zkrácen --
```

[12]Do procesu hledání vhodného kořene vstupuje více parametrů [13]

Dále záměrně snižuji prioritu výběru[13] u rozhraní realizující záložní linku mezi SW-R2-SRV-01 a SW-R2-KLI-01, tak aby pro připojení k nadřazenému přepínači byl zvolen agregovaný kanál. Testováním scénáře přerušení primárního spoje mezi prvky SW-R2-CORE-01 a přístupového přepínače serverového, resp. uživatelského segmentu byla změřena doba obnovy spojení, tedy rychlost konvergence MSTP protokolu pro instanci MSTI 1, v rozmezí 1 – 3 sekund. Výpadek takového spoje uživatel při běžné práci v rámci výuky nepostřehne, pro interaktivní aplikace náročné na zpoždění (VoIP, online hry) tuto dobu považuji za přijatelnou.

Stejným způsobem je zajištěno vhodného výběru kořene pro druhou instanci MSTP protokolu, která zajišťuje odstranění smyčky v případě experimentálních VLAN sítí. Opět záměrně volím hodnotu 8192 pro nastavení priority na přepínači SW-R3-LAB-01 a adekvátní prioritu preferovaného rozhraní. Přepínače SW-R2-CORE-01 a SW-R2-KLI-01 pro MSTI 2 musí mít zvolenu prioritu nižší, aby nedošlo k jejich nežádoucímu zvolení za kořen stromu. Virtuální síť s VID 90 záměrně nechávám součástí výchozí instance MSTI 0. Výběr kořene pro tuto instanci není příliš podstatný, většinu datového provozu přenášeného v této VLAN tvoří pouze datové jednotky SNMP protokolu, případně data protokolů Telnet a SSH při připojení na konfigurační rozhraní síťových prvků. Výjimkou může být práce s KVM. Zde se však předpokládá, že administrátorské operace provádí správce připojený vzdáleně pouze v případě potřeby, a to zpravidla pomocí VPN. Tyto pakety nejsou nikdy šířeny mimo přepínač jádra sítě a hraniční směrovač. Zařízení pro správu jsou připojena na porty přepínače v jádru sítě. Výběr vhodného kořene stromu žádným výrazným způsobem neovlivní potřebu zajištění dostupnosti zařízení v IP podsíti 10.10.90.0/24.

Soubory s konfigurací pro konfigurované přepínače jsou dostupné na přiloženém DVD.

[13]Hodnota priority rozhraní se tedy zvyšuje

4 SERVEROVÁ INFRASTRUKTURA

Hlavním prvkem nově navržené infrastruktury serverového segmentu je přepínač Zyxel XGS1910, který zajišťuje přístup k síti všech fyzických i virtuálních serverů. Jde o přepínač, jehož účel je záměrně vyhrazen pouze pro připojení serverových zařízení jež komunikuji v nově vzniklé VLAN s VID 20. Tato realizace je zvolena s ohledem na vyšší nároky na datové přenosy mezi servery (např. zálohování na sdílené úložiště, použití sdíleného úložiště virtualizačním clusterem). V takto definované serverové podsíti operují mj. následující servery:

- Dva uzly virtualizačního clusteru,
- fyzický řadič domény, DHCP a primární DNS server,
- sdílené úložiště,
- nevyužitý server.

Jelikož byly ve značné míře nasazeny služby a serverové systémy Microsoft Windows Server ve starší verzi 2008 R2, s přechodem na nový koncept probíhá aktualizace (přechod) na aktuální verzi Windows server 2016. Hlavním cílem je efektivnější rozložení serverových služeb mezi dostupné servery a zajištění tolerance vůči výpadku serveru poskytující základní služby typické pro podnikové sítě. Z tohoto důvodu pomocí dvou serverů tvořím virtualizační cluster, ve kterém je provozován mj. záložní doménový kontrolér a dedikovaná stanice pro správu síťové infrastruktury. Oba uzly virtualizačního clusteru zajišťují vysokou dostupnost (tzv. High Availability) pro virtuální server, který je schopen zajistit provoz služeb AD, DNS a DHCP. Veškeré virtuální stanice pro provoz laboratorních úloh zajišťuje pouze jeden uzel a tyto VM nejsou zálohovány funkcí HA.

Přehled všech instalovaných serverů je k dispozici v přílohách práce a na přiloženém DVD. Popis instalace SVN serveru, TFTP serveru i stanice vyhrazené pro management je nad rámec této práce – pro správu je využito základních systémových nástrojů z balíku MS Remote Server Admnistration Toolkit. Tento způsob je vhodný vzhledem k již konfigurovaným zásadám skupiny Active Directory a bezpečnostních oprávnění[1].

4.1 Prostory úložišť

V laboratoři je dostupné úložné zařízení s připojením k datové síti. Jedná se o zařízení LenovoEMC™PX6-300d. Tato jednotka disponuje šesti interními šachtami pro připojení pevných disků s rozhraním SATA 6Gbps a USB3.0 konektory pro připojení externích zařízení. Pevné disky lze konfigurovat pro použití v diskových polích typu

[1] Rozbor této konfigurace je nad rámec textu.

RAID 0, 1 a 5. Zařízení dále disponuje dvěma síťovými rozhraními s podporou maximálních rychlostí až 1 Gbit/s a která lze agregovat do logického kanálu. Pro lepší přístup k zařízení a jeho snadnou identifikaci v doménové struktuře tomuto zařízení přiřazuji název SC5-32-NAS01 s IP adresou 10.10.20.3 z rozsahu 10.10.20.0/24. Dále je úložiště zařazeno do doménové struktury Active Directory.

V současnosti jsou v úložném zařízení osazeny čtyři pevné disky Western Digital WD20EFRX s kapacitou 2 TB. Jedná se o pevné disky, které jsou výrobcem určeny pro použití v úložných zařízení pro „domácí“použití, nikoli v zařízení, kde je prioritou vysoký výkon a rychlá odezva. Na tomto zařízení jsou všechny disky přiřazeny do pole typu RAID 5. Pro svůj návrh provádím restrukturalizaci diskového pole, kde jsou celkem 4 disky rozděleny do dvojic po 2 pevných discích. Každá dvojice tvoří pole typu RAID 1. Toto uspořádání vychází z požadavku jednotlivých aplikací na diskový subsystém. Každé diskové pole tvoří prostor úložišť jehož celková kapacita je odvozena dle rov. 4.1.

$$C_{\text{RAID1}} = \frac{n}{2}, \tag{4.1}$$

kde n je součet kapacit všech pevných disků v diskovém poli typu RAID 1. Konfigurace těchto polí poté odpovídá tab. 4.1. Začlenění disků na lichých a sudých pozicí do dvou diskových polí vede ke snížení vibrací a vyzařovaného tepla vlivem aktivity daných disků. Prostor disků s označením `drive_pool_1-3` je dále použit pro tvorbu svazků, které jsou připojovány přes iSCSI protokol jako úložiště virtuálních počítačů. Lze tedy předpokládat, že tyto disky budou neustále v provozu, zatímco disky s ID 2 a 4 tvořící prostor disků s označením `dirve_pool_2-4` tvoří prostor pro tvorbu sdílených složek. Zde lze předpokládat častější zastavování pevných disků, neboť disky v tomto poli se roztočí pouze v případě přístupu na sdílenou jednotku, jež diskový prostor nabízí.

Tab. 4.1: Rozvržení pevných disků v úložném zařízení

ID prostoru	**Název**	**Ochrana**	**ID použitých disků**
A	drive_pool_1-3	RAID 1	1 a 3
B	drive_pool_2-4	RAID 1	2 a 4

Každý diskový prostor pak nabízí celkem 1.802 TiB úložné kapacity. Její rozdělení bude podřízeno budoucím potřebám. Pro tvorbu virtualizačního clusteru v prostoru `drive_pool_1-3` vytvářím nový svazek `iscsi-5-cluster` s kapacitou 300 GB a který je možné připojit pomocí iSCSI protokolu a bude použit jako sdílené úložiště všemi uzly clusteru. Tomuto svazku je automaticky přiřazen IQN identifikátor

`iqn.2012-07.com.lenovoemc:storage.SC5-32-NAS01.iscsi-5-cluster`.

Připojení k takto vytvořenému svazku ze serverového zařízení je popsáno v následující kapitole.

4.1.1 Připojení ke svazku pomocí iSCSI

Pomocí IQN identifikátoru lze jednoznačně určit svazek úložného zařízení, který má být připojen pomocí iSCSI protokolu na koncové stanici či serveru. K tomuto účelu je v OS Windows, jež je použit na obou uzlech clusteru, dostupný nástroj *iSCSI Initiator*. Tento nástroj je možné obsluhovat i z rozhraní interpreta Windows Powershell. Prvním krokem na cílovém serveru je spuštění služby iSCSI, která mj. zajistí automatické připojení ke svazku na síťovém úložišti i po restartu OS.

```
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
PS C:\> Start-Service msiscsi
```

Následuje vyhledání tzv. *iSCSI Target Portal*, tedy serveru, který zprostředkovává spojení k diskovým jednotkám označovaných jako tzv. iSCSI Target. Konkrétní diskové jednotky jsou identifikovány IQN řetězcem, který je taktéž označován jako `NodeAddress`. Připojení ke svazku vytvořenému v předchozí kapitole je tedy možné pomocí:

```
PS C:\> New-IscsiTargetPortal
  -TargetPortalAddress sc5-32-nas01
PS C:\> Connect-IscsiTarget -NodeAddress
iqn.2012-07.com.lenovoemc:storage.SC5-32-NAS01.iscsi-5-cluster
```

Přístup k diskovým svazkům lze řídit serverem RADIUS, lze autentizovat iniciátora i cílový server a přenos samotných příkazů zabezpečit pomocí protokolu IPSec. Tohoto však v práci není využíváno. Na takto připojeném virtuálním disku lze nyní vytvořit MBR záznam, diskové oddíly a jejich souborové systémy. Pro realizaci clusterem sdíleného úložiště (tzv. Cluster Shared Storage) pomocí základních nástrojů vytvářím nový diskový oddíl s písmenem `R` a souborovým systémem NTFS. Takto vytvořený diskový oddíl je nyní dostupný pro ukládání dat v rámci OS. Aby bylo možné tento postup reprodukovat i na druhém uzlu clusteru, je nutné připojený disk na prvním uzlu odpojit (převést do režimu offline)[2]. iSCSI svazek může zůstat připojen, diskový oddíl však nesmí být aktivní ve více uzlech.

[2]Souborový systém NTFS neumožňuje současnou práci s diskovou jednotkou na více zařízeních

4.2 Virtualizační infrastruktura

Z důvodu zachování zvyklostí a jednoduché integrace do stávajícího prostředí bude infrastruktura laboratoře rozšířena o zcela nový uzel virtualizačního clusteru realizovaný službou Hyper-V. Jako hostitelský operační systém je zde zvolen OS Microsoft Windows Server 2016 Datacenter. Jedním z kritérií výběru je zde požadavek na jednoduchou správu virtualizační platformy a bezproblémovou integraci ve stávájícím prostředí, které využívá doménových služeb Active Directory společnosti Microsoft.

Aktualizace operačního systému virtualizačních serverů přináší značené výhody[3], z nichž nejpodstatnější jsou nové režimy dynamické paměti VM, nové síťové služby VM (QoS, umístění na sdílený disk) a v neposlední řadě možnost správy virtuálního počítače z prostředí Windows Powershell[4].

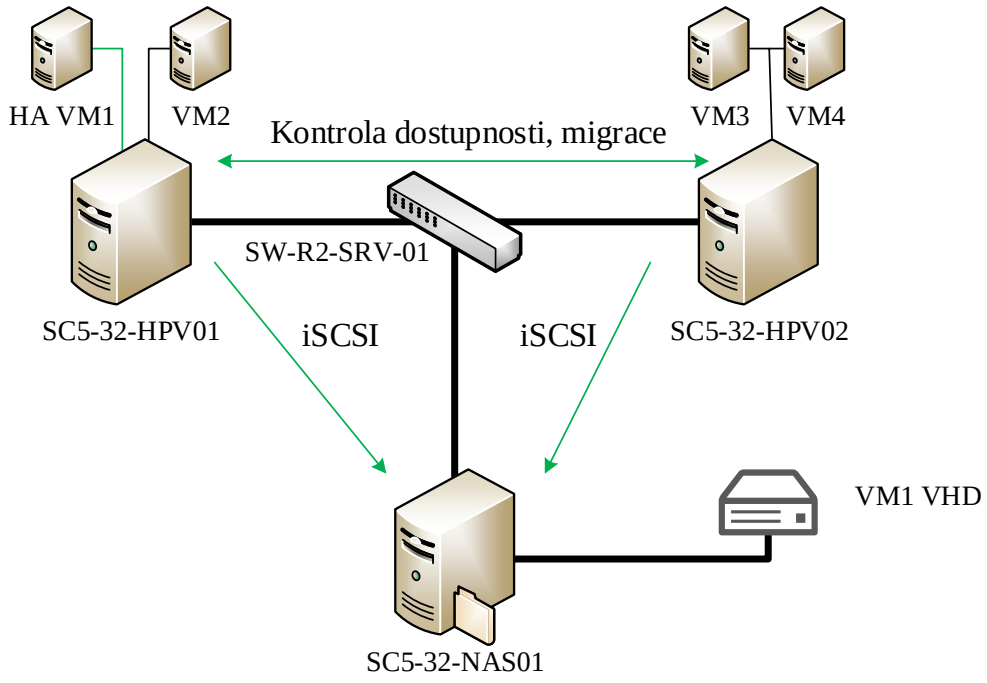
S přechodem na novější verzi hypervizoru se nabízí možnost efektivněji přidělovat prostředky fyzického hostitele virtuálním stanicím. Toho je mj. docíleno pokročilejší integrací mezi rodičovským a synovským oddílem a možností dynamicky alokovat prostředky dané virtuální stanici za jejího chodu [1]. Kompletní virtualizací serverové infrastruktury nevyhnutelně dochází k zavedení kritického místa, kterým je spolehlivý běh fyzického hostitele. Nároky na jeho nepřetržitou dostupnost se zvyšují s počtem na něm provozovaných VM, jejichž role je v rámci sítě nenahraditelná. Zatímco funkce doménového řadiče a DNS serveru může v případě výpadku jednoho z hostitelů zajistit ADC, servery, které nejsou součástí distribuovaného prostředí je nutno zabezpečit pomocí funkce zálohování v clusteru. Tímto mechanismem lze zabezpečit i jiné služby či servery, např. souborový server, SQL server a mnohé další [1].

Přínosem virtualizačního clusteru je nejen možnost migrace virtuálních strojů mezi jednotlivými hostiteli v clusteru, ale i jejich spuštění na jiném hostiteli v případě výpadku virtualizačního serveru, na kterém byl virtuální stroj provozován. V závislosti na sofistikovanosti zálohovacího mechanismu lze hovořit o zálohování bez nutnosti restartu stroje či zálohování spuštěním na odlišném hostiteli. V případě zálohování bez nutnosti restartu je virtuální počítač spuštěn současně na dvou a více hostitelích v clusteru, obsah jejich operačních pamětí se synchronizuje a v případě selhání serveru, na kterém je VM aktuálně aktivní, se automatickou rekonfigurací síťového subsystému obnoví spojení s „záložním“ virtuálním strojem.

Efektivnějším využitím prostředků laboratoře je provoz clusteru se zálohováním virtuálních strojů s případným restartem na jiném hostiteli. Toto řešení je vhodným kompromisem pro zajištění vysoké dostupnosti virtuálních počítačů a efektivním využitím výpočetní kapacity jednotlivých hostitelů. Tato metoda je zvolena i s ohle-

[3]Popis funkcí nové verze Hyper-V dostupný z: `https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/what-s-new-in-hyper-v-on-windows`

[4]Platné již od verze 2012



Obr. 4.1: Provoz HA VM ve virtualizační infrastruktuře

dem na vlastnosti virtualizované infrastruktury – některé virtuální servery jsou součástí distribuované architektury (řadiče služby Active Directory, DNS servery), která funkcionalitu při výpadku jednoho z serverů zajišťuje na úrovni aplikací či rolí OS.

Nezbytnou komponentou virtualizačního clusteru je sdílené úložiště, a to nejen pro zajištění dostupnosti virtuálních strojů a jejich konfigurací, ale i pro zápis a čtení řídících operací, které jsou použity pro udržení koordinace mezi členy clusteru [3]. Funkční schéma virtualizačního clusteru s externím sdíleným úložištěm je zobrazeno na obr. 4.1. Pokud má daný VM nastavenu možnost spuštění na alternativním hostiteli, je tento stroj označen jako tzv. Highly Available VM, tedy stroj s vysokou dostupností.

Z obr. 4.1 je patrné, že v clusteru nemusí být provozovány všechny virtuální počítače. Dále je nutno zvážit rezervace výpočetní kapacity pro stroje, které by v případě selhání jednoho z členů clusteru musely být restartovány na alternativním hostiteli. Pro řešení této problematiky se v praxi zavádí rezervace a priority jednotlivých VM tak, aby v případě výpadku byla možnost zajistit provoz infrastruktury, a to i za předpokladu, že hostitel nebude mít k dispozici prostředky pro provoz daného VM. Tímto mechanismem je vhodné zabezpečit alespoň jeden řadič domény, jeden DNS server a DHCP server. V laboratorní síti je však k dispozici dedikovaný fyzický server, který poskytuje shodné služby, proto rezervace zdrojů není užito.

4.2.1 Základní konfigurace hostitele Hyper-V

Popisovaný cluster bude složen ze dvou fyzických uzlů (hostitelů). Tato kapitola se věnuje instalaci prvního hostitele a popisuje přidání Hyper-V role, její konfiguraci a přípravě na provoz v režimu clusteru. Nezbytným předpokladem pro efektivní chod virtualizačního clusteru je shodná konfigurace síťových rozhraní všech členů daného clusteru a dostupnost sdíleného úložiště. Příprava úložného zařízení je popsána v kapitole 4.1.1. Vytvořený LUN je do jednotlivých uzlů clusteru připojen pomoci iSCSI protokolu. Pro operační systém hostitele se takto připojený virtuální disk jeví jako fyzicky dostupné úložiště ve kterém je možno vytvořit tabulku oddílů, definovat diskové oddíly a jejich souborové systémy.

Následující kapitoly předpokládají alespoň základní znalosti práce se systémem Windows Server 2016. Vycházím z předpokladu dokončené instalace OS fyzického serveru, jeho základní konfigurace (název, síťová rozhraní, začlenění do AD domény). Pokud je to možné, pro zachování jednoduchosti popisu instalačních a konfiguračních procesů používám vždy tzv. cmdlet v prostředí Windows Powershell či jejich vzájemné řetězení.

```
PS C:\> Install-WindowsFeature -Name Hyper-V
  -IncludeManagementTools
```

Instalaci je nutno zakončit restartem fyzického serveru. Po opětovném spuštění OS hostitele je možno začít přidávat virtuální počítače. K tomu lze použít nově instalovaný nástroj Správce technologie Hyper-V nebo nově dostupné cmdlety v prostředí Windows Powershell. Před vytvořením prvního VM je však vhodné rozhodnout, kde budou virtuální počítače a jejich disky uloženy, zda bude využito externího úložiště, např. diskové pole připojené pomocí iSCSI či technologie FibreChannel. Zde nastavuji pouze lokální úložiště[5] a to v umístění na místním disku `D`, ve složce `hpv` a ve vnořených složkách `vhd` a `vm` pro umístění disků, resp. konfiguračních souborů daných VM.

Dále je nutné vytvořit virtuální přepínače, které umožňují připojení do učených VLAN sítí. Pokud má být virtualizační hostitel součástí clusteru, musí být zajištěna dostupnost stejných síťových rozhraní (virtuálních přepínačů) na všech uzlech daného clusteru a to vč. shodného názvosloví [17]. Na každém hostiteli tedy vytvářím dva virtuální přepínače s přístupem do externí sítě (typ External). Pokud je pro připojení externího přepínače použito agregovaného rozhraní – tzv. NIC Team, je nutno zvolit tento agregovaný propoj, nikoli jeho dílčí rozhraní.

```
PS C:\> New-VMSwitch -name vSwitchPROD
```

[5] Hyper-V server bude provozovat i VM mimo cluster

```
  -NetAdapterName NICTeam1-2 -AllowManagementOS $false
PS C:\> New-VMSwitch -name vSwitchLAB
  -NetAdapterName NICTeam3-4 -AllowManagementOS $false
```

Při vytváření přepínače s přístupem k fyzickému adaptéru hostitele používám parametr `-AllowManagementOS $false`, čímž je pro OS Hyper-V serveru odepřena možnost užití daného přepínače pro vlastní přístup k síti. Tím dojde k vyhrazení dané kapacity pouze pro virtuální počítače, které mají nastaveno připojení pomocí externího virtuálního přepínače. Parametr `-NetAdapterName` v tomto kontextu specifikuje rozhraní, které bude použito pro připojení virtuálního přepínače k přepínači fyzickému. Pokud pro tyto účely není použit agregovaný kanál, je možno použít i jediného síťového rozhraní v serveru hostitele.

Tímto je dokončena základní instalace hypervizoru, instalaci druhého virtualizačního serveru provádím stejným způsobem. Virtuální počítače, které jsou užity při výkonu laboratorních cvičení importuji pouze na druhý uzel, jejich provoz není zálohován funkcí clusteru. Virtuální počítače je možno tvořit již nyní a do režimu zálohování clusterem je zavést později. Instalaci a konfiguraci samotného clusteru popisuje následující kapitola.

4.2.2 Hyper-V cluster s převzetím služeb při selhání

Před tvorbou virtualizačního clusteru je nutné začlenit oba virtualizační hostitele do jedné doménové struktury, čím dojde k možnosti automatické vzájemné autentizace nejen samotného správce clusteru, ale navázání tzv. vztahů důvěry mezi členy clusteru samotnými. Funkce clusteru je možno využít pro zajištění dostupnosti více služeb, nikoli jen samotných virtuálních počítačů. Proto je tato funkce obecně označována jako *Failover Clustering*, resp. *Cluster s podporou převzetí služeb při selhání*. Provoz virtuálních počítačů s vysokou dostupností je jen jednou z mnoha funkcí, které obecný cluster může zajišťovat. Lze tedy např. zálohovat funkcionalitu pouze dílčích rolí DHCP, DNS, WINS a dalších [1] [3].

Instalaci opět na obou uzlech provádím z prostředí skriptovacího interpreta Windows Powershell.

```
PS C:\> Install-WindowsFeature -Name Failover-Clustering
  -IncludeManagementTools -ComputerName sc5-32-hpv01
PS C:\> Install-WindowsFeature -Name Failover-Clustering
  -IncludeManagementTools -ComputerName sc5-32-hpv02
```

Tvorba clusteru pokračuje provedením následujícího na jakémkoli uzlu clusteru. Tím dojde k vytvoření nového účtu počítače v doménové struktuře Active Directory [3] [17] a zaregistrování záznamu typu A a PTR do systému DNS, kde název clusteru odpovídá uvedené IP adrese.

```
PS C:\> New-Cluster -name SC5-32-CLS01
  -Node sc5-32-hpv01,sc5-32-hpv02 -StaticAddress 10.10.20.50
```

Po vytvoření nového clusteru je nutné provést jeho validaci. Proces validace se skládá z několika dílčích částí, které testují konfiguraci OS, Hyper-V role, fyzického HW, síťové konfigurace a konfigurace sdíleného úložiště. Proces validace je spuštěn pomocí cmdletu

```
PS C:\> Test-Cluster -Node sc5-32-hpv01,sc5-32-hpv02
```

a po jeho dokončení dochází k vyhodnocení výsledků. Způsobilost uzlu pro provoz cluster je interpretována dle následujících pravidel:

- **Prospěl:** Konfigurace dané části splňuje podmínky pro nasazení v režimu clusteru
- **Prospěl s upozorněním:** Konfigurace dané části splňuje podmínky pro nasazeni v režimu clusteru, avšak není garantována plná funkcionalita[6]. Upozornění není považováno za chybu, je však vhodné zvážit, zda je tato konfigurace optimální.
- **Neprospěl:** Konfigurace dané části nevyhovuje podmínkám pro nasazení v režimu clusteru a je nutno ji opravit[7].
- **Ukončeno:** Test validity byl předběžně ukončen [17].

Pokud je v některé z kategorií test ohodnocen hodnocením „neprospěl“, je daný cluster považován za nevhodný pro provoz virtuálních počítačů. Takto vyhodnocená konfigurace není ze strany výrobce podporována. Pokud je konfigurace označena za validní, avšak vyskytují se upozornění, cluster je celkově vyhodnocen jako validní [17]. Námi vytvořený cluster lze použít pro provoz virtuálních strojů za předpokladu, že je v daném VM povoleno zachovaní zpětné kompatibility ve vlastnostech procesoru. To je způsobeno mezigeneračním rozdílem mezi použitými procesory Intel Xeon v uzlech clusteru. Výsledky validačních testů jsou dostupné na přiloženém DVD.

[6]Typickým příkladem může být upozornění na neshodu generace daného hardware, např. generace CPU apod.

[7]Typickým příkladem je neshoda dvou procesorových výrobců (CPU značky Intel a CPU značky AMD, nedostupnost síťových rozhraní na jednom z uzlů clusteru a další

Nyní je vytvořen adresovatelný cluster, který však nemá k dispozici žádný úložný prostor. Ten je nutno opět přidat ve správci clusteru, popř. pomocí následujících cmdletů. Nutnou prerekvizitou je dostupnost svazku na obou uzlech a to pod stejným identifikátorem. Zobrazení dostupného disku, který je možno přiřadit jako úložiště clusteru, a jeho následné přidání je provedeno zřetězením výstupu a vstupu dvou cmdletů[8]. Následně je na nově vytvořeném disku potřeba vytvořit souborový systém typu CSVFS.

```
PS C:\> Get-ClusterAvailableDisk | Add-ClusterDisk
PS C:\> Add-ClusterSharedVolume -Name 'Cluster-Disk-1'
```

Souborový systém CSVFS je nyní přístupný všem členům clusteru pro současné čtení a zápis dat. Nově vytvořený svazek se systémem souborů CSVFS je ve výchozím nastavení připojen do adresáře ClusterStorage na systémovém oddílu a dále dle jednotlivých CSVFS svazků do vnořených adresářů. Nově vytvářené virtuální stroje, které jsou předurčeny pro provoz v režimu vysoké dostupnosti je nutné ukládat do tohoto umístění. Fyzicky se tak daný VM nachází na pevném disku na úložném zařízení SC5-32-NAS01. Práce s takto uloženými virtuálními počítači je pomalejší než při jejím provozu na lokálním úložišti daného hostitele. Tento nedostatek je však vzhledem k povaze takto provozovaných VM zcela akceptovatelný. V režimu HA provozuji virtuální počítač SC5-32-DC03v a SC5-32-MNG01. Jejich tvorba probíhá standardním způsobem, avšak jako místo pro ukládání dat virtuálního počítače (jeho pevný disk, konfigurace i kontrolní body) musí být zvoleno umístění `Cluster-Disk-1`. Dále je vzhledem k specifickým odlišnostem fyzického hardware obou uzlu nutno zachovat zpětnou kompatibilitu označením jejich procesorové konfigurace jako „omezené pro zachování kompatibility při migraci“ [17].

4.2.3 Provoz AD, DNS a DHCP s vysokou dostupností

S migrací na nový koncept datové sítě a oddělení rolí instalovaných na dostupných serverech zanikla i role alternativního doménového kontroléru, který byl provozován neoptimálně na virtualizačním serveru (nikoli ve VM). Protože je v rámci ochrany doménové struktury doporučováno provozovat alespoň dva synchronizované doménové kontroléry s funkcí globálního katalogu [1], instaluji nový virtuální počítač SC5-32-DC03v s operačním systémem MS Windows Server 2016 Datacenter. VM ukládám do místa připojeného CSV svazku a po instalaci jej přidávám jako roli[9] clusteru.

[8] V tomto případě bude zobrazen pouze jeden dostupný disk, při dostupnosti více disků je toto zřetězení nevhodné

[9] V tomto kontextu znamená provoz VM v režimu HA přidání role danému clusteru

```
PS C:\> Add-ClusterVirtualMachineRole
  -VirtualMachine SC5-32-DC03v
```

Primárním hostitelem je server SC5-32-HPV01, avšak v rámci migrace a v případě výpadku je možné VM přesunout i na druhý virtualizační uzel. Předpokladem je, že v případě selhání fyzického doménového kontroléru bude možno nadále využívat služeb Active Directory, DNS a DHCP serverů – tyto služby bude v případě potřeby zajišťovat nově instalovaný virtuální server.

S přidáním role doménového řadiče probíhá automaticky i instalace DNS serveru. Zóny tohoto DNS serveru jsou integrovány v databázi Active Directory a její data vč. DNS záznamů jsou automaticky replikována a synchronizována na ostatní řadiče domény v předem stanoveném intervalu 15 minut [1] [3].

V průběhu migrace na nový koncept datové sítě je tento doménový kontrolér zároveň jediným DHCP serverem v laboratorní síti. Obsluhuje definované adresní prostory pro VLAN 10, 20 a 90. Pro VLAN 20 a 90 je k dispozici odpovídající rozsah se záměrně omezeným počtem – adresy z těchto rozsahů jsou přiřazeny zpravidla staticky a dynamická konfigurace je zde pouze z důvodu usnadnění přechodu z původní datové sítě na nový koncept. Tím je zajištěno adresování a přístup k síťovému zařízení, které ještě nebylo patřičně přenastaveno. Dále je zde definován rozsah IP adres pro přidělení klientům z VLAN 12, která je vyhrazena pro uživatele bezdrátových přístupových bodů v laboratoři. DHCP žádosti jsou k DHCP serveru přeposílány zpravidla DHCP Relay agentem, který je konfigurován na přepínači v jádru sítě s výjimkou VLAN 12 a 20.

Konfigurace obou DHCP serverů předpokládá předchozí přidání stejných adresních prostorů a jejich shodnou konfiguraci – např. rezervace adres, výjimky z rozsahů a další. Proces nastavení „zálohování provozu“ DHCP serveru zajišťuje navázání partnerství obou DHCP serverů a určení procentuálního podílu pro každý rozsah, který daný DHCP server obsluhuje. Toto partnerství lze provozovat v režimech Hot Standby a Load Balancing[10]. Vytvoření nového partnerství pro servery s názvy SC5-32-DC03v a MERCURY lze provést pomocí cmdletu:

```
PS C:\> Add-DhcpServerv4Failover -ComputerName sc5-32-dc03v
  -PartnerServer mercury -Name DHCP-LB -ScopeID 10.10.10.0
  -LoadBalancePercent 50 -SharedSecret heslo
```

Činnost páru spočívá v řízené obsluze žádosti klienta na základě hodnoty jeho MAC adresy. Ta je spočítána speciální hashovací funkcí, jejíž výstup nabývá hodnot od 1 do 256 [1] [3]. Pokud je poměr rozdělení nastaven na 50 procent, první server

[10]Vzhledem k vlastnostem režimu Load Balancing je tento provoz preferovanou volbou [1]

reaguje na žádosti klientů s hodnotou hashe od 1 do 128, druhý server na žádosti s hodnotou hashe od 129 do 256. Dostupné adresy, které mají být v adresním prostoru zapůjčeny jsou také rozděleny ve stejném poměru mezi oba DHCP servery. Pokud je vlivem výstupních hodnot hašovací funkce jedna polovina rozsahu čerpána větší mírou než polovina druhá, jsou každých 5 minut volné adresy přidruženy do nového podprostoru, který je opakovaně rozdělen mezi partnerské DHCP servery. Pokud jeden ze serverů není v provozu, přidělování zápůjček převezme partnerský server nezávisle na hodnotě hash pro danou MAC adresu klienta [1].

Po korektní konfiguraci obou DHCP serverů je potřeba patřičně upravit nastavení zařízení realizující funkci DHCP Relay. Tato zařízení mohou požadavky patřičně přeposílat na adresu všesměrového vysílání v IP podsíti, kde se DHCP servery nachází. Alternativně lze specifikovat pouze adresy těchto DHCP serverů. V nové datové síti využívám cíleného zasílání na IP adresy DHCP serverů. Toto nastavení je provedeno na virtuálním L3 rozhraní přepínače v jádru sítě, a to pro VLAN s VID 10, 20 a 90. Příklad konfigurace pro VLAN s VID 10 je:

```
interface Vlan10
 description %Client VLAN interface%
 ip address 10.10.10.1 255.255.255.0
 ip access-group 100 in
 ip hleper-address 10.10.20.2
 ip helper-address 10.10.20.15
```

Protože je na partnerském DHCP serveru instalován OS Windows Server 2008 R2, je v průběhu psaní práce funkce zálohování DHCP serveru a vyrovnávání zátěže nedostupná. Funkčnost této metody jsem ověřil v experimentálním prostředí a její nasazení v produkční infrastruktuře proběhne až po vyřazení aktuální instalace OS na primárním doménovém kontroléru, který je zároveň partnerským DHCP serverem.

5 DOHLEDOVÝ SYSTÉM A ZÁLOHOVÁNÍ

Poslední část práce se zabývá návrhem a implementací monitorovacího systému v datové síti laboratoře. Dále jsou nasazeny možnosti zálohování konfigurací síťových prvků jejichž okamžitá dostupnost poslouží správci pro sledování změn a přehlednější orientaci v jejich nastavení. Společně s možností sledování aktuálního stavu vybavení laboratoře tak tvoří velmi přínosné zdroje informací a to nejen v případě řešení chybových stavů.

5.1 Monitoring systémem Zabbix

Systém Zabbix je dostupný ke stažení pro většinu běžně používaných distribucí OS s jádrem Linux[1]. Nasazení systému je možné stažením a importem tzv. appliance, tedy virtuálního disku s předem připravenou instalací OS a SW Zabbix. Tvorba VM pak probíhá stejným způsobem (nejde o VM s vysokou dostupností), avšak namísto vytvoření nového virtuálního disku připojuji již stažený a extrahovaný pevný disk s instalací OS Linux a plně instalovaným systémem[2] Zabbix ve verzi 3.4.

Zabbix je v práci zvolen zejména z důvodu jednoduché správy a užívání systému. Cílem nasazení dohledového systému je především možnost sledování základních provozních informací (dostupnost, vytížení, využití fyzických prostředků), inventarizace a případně zajištění základních metodik pro lokalizaci případných problémů.

Virtuální počítač, který zajišťuje provoz dohledového systému, provozuji na virtualizačním serveru SC5-32-HPV01. Pro tento VM záměrně nevyužívám funkce zálohování clusterem (je však možno selektivně iniciovat přesun mezi hostiteli). Daný VM využívá agregovaného fyzického spoje a je připojen do serverové VLAN 20. Pro jeho IP adresu 10.10.20.20 do DNS databáze zanáším záznam typu A, PTR[3] a záznam typu CNAME s hodnotou „monitoring“ pro usnadnění přístupu do systému z webového prohlížeče.

Bližší popis systému Zabbix proběhl v rámci semestrálního projektu a je nad rámec tohoto textu. Následující podkapitoly se věnují popisu implementace metod sledování a testování dostupnosti s užitím protokolu ICMP, SNMP a s využitím Zabbix agenta.

[1]Seznam podporovaných distribucí s jádrem OS Linux dostupný z `http://www.zabbix.com`

[2]Postup instsalace OS a dohledového systému je nad rámec tohoto textu, je však zdokumentovaný a dostupný na oficiálních stránkách výrobce systému Zabbix

[3]OS není členem provozované domény AD a nelze použít dynamických aktualizací DNS záznamů

5.1.1 Sledování pomocí SNMP a Zabbix agenta

Systém Zabbix nabízí hned několik způsobů sledování a sběru dat z cílového zařízení. Prvním hojně nasazovaným je sběr a přenos dat pomocí SNMP protokolu. Tento způsob je velmi vhodný zejména na aktivních prvcích sítě (přepínače a směrovače). Informace o síťovém prvku zprostředkovává tzv. SNMP agent, který generuje SNMP zprávy a zasílá je na předem konfigurovanou adresu dohledového prvku [18]. Tato nastavení byla provedena v rámci konfigurace síťových prvků popsaných v kapitolách 3.1.1 – 3.1.3 a 3.2.1 – 3.2.2. Následuje přidání zařízení (hostitele) do seznamu sledovaných zařízení. Toto nastavení je dostupné na záložce Configuration/Hosts.

Pro přidání cílového prvku uvádím jeho popisný název a specifikuji komunikační rozhraní. Rozhraní určuje vždy alespoň IP adresu či DNS záznam pro daný prvek. Pokud sběr dat probíhá pomocí SNMP protokolu, přidávám tzv. SNMP Interface, pokud s asistencí Zabbix agenta, přidávám patřičnou informaci do pole Agent Interface. Pro přehlednost je vhodné dle typu zařízení přidané položky zařadit do odpovídajících skupin.

Dále pro každé zařízení přiřazuji konfigurační šablonu, která obsahuje definici služeb a parametrů, které jsou na daném zařízení sledovány. V případě zařízení s využitím SNMP jde zpravidla o tabulku definující OID, hodnoty a jejich interpretaci. Tato šablona specifikuje i tzv. spouštěče událostí, kterým může být např. limitní úroveň zatížení linky či využití RAM a další.

Předem připravené šablony lze dále řetězit. Šablona může definovat i využití systémové aplikace pro provedení akce a následnou interpretaci těchto výsledků. Příkladem takové šablony je kontrola dostupnosti pomocí systémového nástroje `ping`. Šablony lze libovolně vytvářet[4], lze jim přiřadit akci i způsob interpretace výsledků. Dále lze definovat i místo zpracování, tedy např. kontrola aktualizací na sledovaném stroji.

Pro zařízení konfigurovaná v této práci přiřazuji vždy šablony SNMP Device a ICMP Ping. Tím je zajištěna kontrola dostupnosti zařízení[5] i sledování stavu zařízení (obecné informace – název, kontakt na správce, umístění) a aktuálního využití[6]. Experimentálním testováním však bylo ověřeno, že hodnota zprostředkovaná SNMP agentem vykazuje odchylku hodnot v rozmezí 10 až 15 procent. Informaci o zatížení linky lze tedy považovat pouze za orientační[7].

Alternativou k sledování pomocí SNMP agenta je využití softwarového klienta Zabbix Agent, který je instalován v operačním systému sledované stanice. Přestože lze pomocí SNMP sledovat i počítače s OS Linux či Windows, využití softwarového

[4]Popis tvorby je nad rámec textu

[5]Za předpokladu, že zařízení přijímá a reaguje na zprávy ICMP Echo Request

[6]Použitá instalace SW Zabbix již obsahuje MIB tabulky pro interpretaci získaných hodnot

[7]Měření provedeno s použitím nástrojů *iperf*

klienta je flexibilnější. Pro potřeby sledování základních informací o stavu koncových stanic záměrně nechávám nastavení ve výchozím stavu. Softwarového klienta je na počítači s OS Windows nutno nainstalovat jako službu, zajistit její automatické spuštění a povolit komunikaci této aplikace na portu TCP 10050. Konfiguračního souboru agenta pro všechna konfigurovaná zařízení je dostupný v příloze. Softwarového klienta instaluji na všechny servery s OS Windows Server. Nasazení agenta na pracovních stanicích není realizováno, avšak lze jej efektivně provést instalací pomocí objektů zásad skupiny.

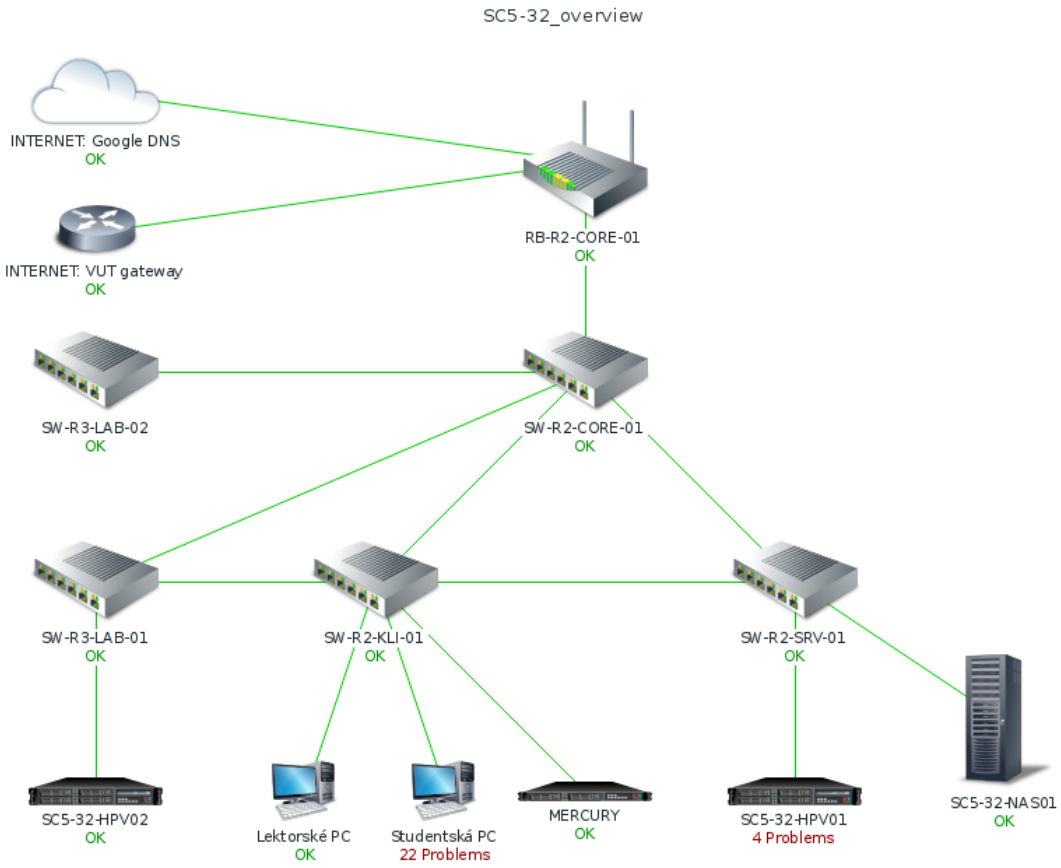
5.1.2 Detekce zařízení v datové síti

Pro potřeby sledování dostupnosti přidávám do sledovacího systému položky pro servery v internetu, které nejsou monitorovány, avšak je testována jejich dostupnost. Jedná se o server (zařízení), které je výchozí bránou univerzitní sítě v přiděleném IP rozsahu a veřejný DNS server společnosti Google. Lze předpokládat, že pokud jsou obě tato zařízení nedostupná, pro laboratorní síť není k dispozici konektivita do univerzitní sítě a internetu.

Pro sledování připojených zařízení v daném IP rozsahu nasazuji funkci Discovery. Zabbix server v konfigurované IP podsíti (zavádím pro sítě 10.10.20.0/24 a 10.10.10.0/24) periodicky odesílá zprávy ICMP Echo Request na všechny definované adresy (v tomto případě všechny IP adresy dané podsítě) a vyhodnocuje přijaté odpovědi. V mém případě kontrolu provádím volím periodu 60 sekund. Tato doba je zvolena s ohledem na využití výpočetních prostředků a množství generovaného provozu. Tato metoda je nejvhodnější vzhledem k faktu, že doménová politika aplikovaná na všechny validní stanice definuje nutnost zpracování dotazů ze všech síti. Na základě těchto informací lze sledovat výskyt stanic v síti a případně detekovat nežádoucí zařízení.

5.1.3 Reprezentace datové sítě mapou

Velmi užitečnou funkcí je grafické znázornění zařízení v topologii sítě pomocí map. Tyto mapy je možno vytvářet pouze staticky, tedy bez interakce s danou položkou, ale i s interaktivním zobrazením zařízení, a to včetně jejich stavu. Tato mapa může sloužit pro rychlou lokalizaci problémů. Ve své práci vytvářím základní mapu, která zobrazuje síťové prvky včetně vzájemných propojů, vyhodnocuje stav jejich rozhraní na základě dat přijatých od SNMP agentů a následně kontroluje dostupnost těchto zařízení v síti, tedy zda zařízení odpovídá na periodické zasílání zpráv ICMP Echo Request.



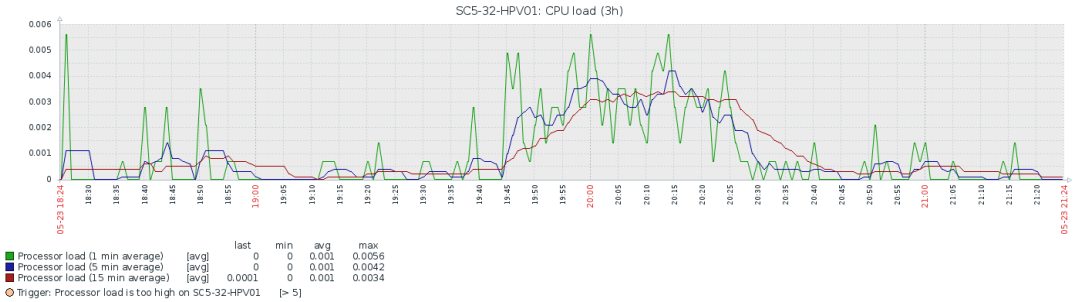
Obr. 5.1: Přehledová mapa datové sítě

Příklad takové mapy je zobrazen na obr. 5.1. Mapa obsahuje některá zařízení, jejichž monitoring byl nakonfigurován dle postupu v předchozí kapitole. Samotný stav zařízení (informace `OK`) nastavuje tzv. spouštěč. Pro ICMP jsou nasazeny spouštěče dle příjmu ICMP Echo Reply, spouštěč vyhodnocující ztrátovost paketů ICMP Echo Reply a spouštěč vyhodnocující zpoždění, tedy dobu definovanou jako interval od vyslání paketu ICMP Echo Request a příjmem paketu ICMP Echo Reply. Mapa dále zobrazuje i aktuální problémy, tedy stavy, které jsou na základě přiřazené šablony označeny jako problémové. V případě skupiny *Studentská PC* je spouštěčem stav rozhraní přepínače SW-R2-KLI-01, jehož stav je reportován SNMP zprávou Trap.

5.1.4 Vizualizace dat a inventarizace

Často užívanou funkcí dohledového systému bývá grafická reprezentace dat a jejich vizualizace v reálném čase. Hodnoty, které jsou sbírány agentem či zasílány v paketech SNMP protokolu lze v závislosti na přiřazené šabloně graficky reprezentovat. Opět zde pro jednoduchost využívám již předem připravených grafů (šablony obsahují ty nejpoužívanější), je však možné grafy libovolně upravovat, vytvářet

či mazat. Příklady grafu zobrazující historii využití CPU virtualizačního hostitele SC5-32-HPV01 je zobrazen na obr. 5.2. Tato data jsou sbírána s využitím agenta instalovaného na sledované stanici (serveru).



Obr. 5.2: Příklad sledování využití CPU pro VM

Grafy jsou generovány a dynamicky aktualizovány v intervalech s dobou trvání 30 sekund. Se stejnou periodou probíhá příjem dat z SW agenta. Data jsou uchována po dobu až 30 dnů (lze ovlivnit v nastavení systému Zabbix). V závislosti na požadované přesnosti lze chování Zabbix agenta patřičně upravit, aby k dotazování a sběru dat docházelo s menším vzorkovacím intervalem. Častější dotazování agentem generuje větší zatížení sledovaného systému. Protože jsou pro potřeby práce sbíraná data pouze orientační a není nutné jejich přesné zobrazení v reálném čase, záměrně volím dotazovací interval 30 sekund.

Sbíraná data lze kromě zobrazení v grafu použít i k inventarizaci. Pro všechna síťová zařízení jsem v práci vyplnil základní informace (zpřístupněné pomocí známých OID objektů), tedy informace o názvu zařízení, jeho umístění a kontaktu na správce daného zařízení. Tato data jsou poté obsažena v SNMP objektech a zpracována dohledovým prvkem. Obdobně lze stejná data získat i pomocí Zabbix agenta na pracovních stanicích a serverech. Dohledový systém z těchto informací poté generuje přehlednou databázi prvků a informací, do které lze manuálně vkládat další hodnoty. Tento způsob automatického plnění tabulek databáze pak užívám jako jednoduchý systém pro správu a přehled o vybavení laboratoře.

5.2 Zálohování konfigurací prvků sítě

Většina operačních systémů, které jsou nasazeny na síťových prvcích, dnes implementuje i metody pro zálohování a přenos konfiguračních souborů pomocí protokolů TFTP, FTP apod. Zálohování a přenos konfigurací pomocí instalovaného TFTP klienta je i vzhledem k horším bezpečnostním vlastnostem protokolu TFTP stále preferovanou volbou, a to zejména pro svoji jednoduchost. Síťové prvky, které nabízí grafické rozhraní pak většinou nabízí možnost danou konfiguraci stáhnout či obnovit

s přenosem pomocí protokolu HTTP. Nevýhodou ukládání konfigurací z prostředí webového prohlížeče jsou však horší možnosti automatizace dané úlohy. V následujících kapitolách je popsán princip automatizované zálohování konfigurací přepínačů jak s použitím terminálového přístupu, tak i pomocí zasílání specifických žádostí pomocí protokolu HTTP.

Pro práci se zálohami využívám virtualizované pracovní stanice SC5-32-MNG01v a virtuálního serveru SC5-32-SRV01vx. Zmíněný server s OS Linux v distribuci Ubuntu 16.04 poskytuje funkci TFTP serveru, na který jsou ukládány zálohy konfiguračních souborů a zároveň slouží jako interpret skriptovacího jazyka Expect. Z bezpečnostních důvodů pomocí softwarového programu *iptables* přidávám konfiguraci paketového filteru daného OS, které znemožní příjem TFTP datagramů ze všech IP podsítí s výjimkou IP podsítě používané pro správu, serverové podsítě a stanice s IP 10.10.10.50 (PC lektora):

```
iptables -A INPUT -s 10.10.90.0/24 -p udp --dport 69 -j ACCEPT
iptables -A INPUT -s 10.10.20.0/24 -p udp --dport 69 -j ACCEPT
iptables -A INPUT -s 10.10.10.50 -p udp --dport 69 -j ACCEPT
iptables -A INPUT -p udp --dport 69 -j DROP
```

5.2.1 Automatické zálohovaní virtuálním terminálem

Přestože některé novější operační systémy síťových zařízení nabízí možnost zálohovací úlohy plánovat a automaticky spouštět, starší operační systémy nabízí možnost pouze správcem iniciovaného stažení konfigurace. V této kapitole popsaná metoda využívá automatizace interakce se síťovým prvkem. K tomu je použito interpreta skriptovacího jazyka Expect, který je navržen pro interakci s počítačovým systémem. Spuštění zálohovacích skriptů na serveru SC5-32-SRV01vx je pomocí programu Cron nastaveno na opakované spuštění každý den v 2:30 hodin[8].

Uvažujme sekvenci úloh, která vede k úspěšnému odeslání konfiguračního souboru na TFTP server ze zálohovaného prvku. Terminálový přístup je téměř vždy nutno autentizovat. Tato autentizace může probíhat např. zadáním hesla k použitému účtu či autentizace pomocí páru privátního a veřejného klíče. Pro jednoduchost a názornost používám metodu autentizace heslem. Po přihlášení k danému zařízení je nutný přechod do privilegovaného režimu. Poté je uživatel oprávněn číst aktuální konfigurace (často označované jako tzv. running-config, resp. startup-config). Ty lze dále odeslat pomocí zmíněného TFTP klienta. Po skončení zálohovacího procesu se správce odhlásí a ukončí spojení. Proces automatizace tohoto procesu pro zařízení s operačním systémem Cisco IOS je vykonán následující sekvencí příkazů:

[8]Popis tvorby plánovaných úloh je nad rámec textu

```
PS C:\> telnet sw-r2-core-01.lab427.utko.feec.vutbr.cz
This system is property of UTKO FEKT VUT Brno.
Unauthorized access to this device is prohibited!

User Access Verification

Password: --- zadání hesla ---
SW-R2-CORE-01>enable
Password: --- zadaní hesla ---

SW-R2-CORE-01#copy startup-config tftp://sc5-32-srv01vx

Address or name of remote host [sc5-32-srv01vx]?
Translating "sc5-32-srv01vx"...domain server (10.10.20.2)[OK]
Destination filename [sw-r2-core-01-confg]?

!!
8365 bytes copied in 0.058 secs (144224 bytes/sec)

SW-R2-CORE-01#logout
```

Od momentu navázání spojení je správce celkem dvakrát vyzván k zadání hesla. Po přechodu do privilegovaného režimu je zadán požadavek na odeslání konfigurace. Dále je potvrzen cíl zálohy (IP adresa či název TFTP serveru) a specifikuje se název souboru, do kterého bude konfigurace zapsána. Následuje potvrzení o přenosu a odhlášení od zařízení. Tyto interakce lze zcela automatizovat pomocí skriptů interpretovaných knihovnou Expect. Výše popsané pak přímo odpovídá následujícímu[9]:

```
#!/usr/bin/expect -f

#informace pro prihlaseni k SW-R2-CORE-01
set username "uzivatel"
set password "heslo"
set enable_pw "heslo"

# nastavit casove razitko zalohy
set date [exec date +%d-%m-%Y]

# otevrit nove spojeni
```

[9]Z typografických důvodů je struktura skriptu patřičně poupravena. Originál je dostupný na přiloženém DVD

```
spawn telnet sw-r2-core-01.lab427.utko.feec.vutbr.cz

# provest zalohovaci proceduru
expect "Password:" {
send "$password\n"
expect "SW-R2-CORE-01>" {
send "enable\n"
expect "Password:" {
send "$enable_pw\n"
sleep 1
expect "SW-R2-CORE-01#" {
send ‘copy startup-config tftp://sc5-32-srv01vx\n‘
sleep 1
expect "]?" {
send "\n"
sleep 1
expect "]?" {
send ’sw-r2-core-01-config_\$date\n’
sleep 1
expect "SW-R2-CORE-01#" {
send "logout\n"
}}}}}}
```

Užitá metodika je patrná z obsahu skriptu. V první fázi jsou definovány hodnoty proměnných, ve kterých jsou uloženy informace o uživatelském účtu. Následně je vytvořena relace pomocí protokolu Telnet. Interpret jazyka Expect načítá řetězec znaků zaslaný protistranou a dle vstupu zasílá danému prvku příkazy k provedení[10]. Tyto příkazy jsou formátovány jako jednotlivé znaky, kde ukončení řádku, tedy vykonání příkazu, odpovídá „odeslání“ klávesy Enter (znaku `\n`). Záměrně do skriptu zanáším prodlevy (v tomto případě 1 sekunda) z důvodu zajištění dostatečné doby pro reakci protistrany. Umělé prodlevy je vhodné vkládat za příkaz zaslání hesla, neboť autentizace může probíhat i s ověřováním serverem v síti, jehož odezva může být až jednotky či desítky milisekund. Následně je provedeno odeslání na server s názvem SC5-32-SRV01vx, potvrzena destinace, název souboru a po ukončení odesílání relace ukončena zasláním příkazu `logout`.

Princip zálohování ostatních prvků v síti je realizován obdobně. Pro každý prvek je nutno sekvenci zasílaných příkazů přizpůsobit dle řetězců zaslaných protistranou.

[10]Nejde o vzdálené volání funkcí

5.2.2 Přenos konfigurací pomocí HTTP (metoda POST)

Specifickým případem automatizace zálohovacích činností je nedostupnost terminálového přístupu. V prostředí realizované datové sítě jde zejména o přepínač Zyxel XGS1910. Daný přepínač nabízí možnost stažení aktuální konfigurace pouze v prostředí webového konfiguračního rozhraní.

Přístup do konfiguračního webového rozhraní je zabezpečen pomocí uživatelského jména a tajného hesla. Proces ověřování je realizován metodou HTTP Authentication[11]. Požadavek na stažení aktuální konfigurace přepínače je následně možno odeslat stisknutím tlačítka *Backup Configuration*. Analýzou přenášených aplikačních dat bylo zjištěno, že po stisknutí daného tlačítka dojde k nastavení hodnoty `save=0` na zobrazené stránce /config/conf_save.htm a jejího odeslání metodou POST na webový server. Server odpověď klienta zpracuje a zahájí přenos vyžádaného souboru s konfigurací. Konfigurační soubor je poté uložen ve formátu XML na místní disk počítače.

Tento proces lze zautomatizovat pomocí programu `curl`. Jde o program, který umožňuje vkládat a přenášet data v řetězcích URL. Vložením hodnoty `save=0` a jejím odesláním je na cílové stanici ze serveru uložen konfigurační soubor. Tuto akci realizuje následující skript v prostředí Bash, který je taktéž pomocí program Cron vykonáván periodicky každý den ve 2:30.

```
#!/bin/bash

# odeslat POST s zadosti o stazeni konfigurace v XML
curl -d "save=0" \
  http://uzivatel:heslo@sw-r2-srv-01/config/conf_save \
  > /srv/tftp/sw-r2-srv-01-config_$(date +%d-%m-%Y)
```

Veškeré skripty pro realizaci automatického zálohování jsou dostupné na přiloženém DVD.

[11] V případě použití této metody lze autentizační informaci zaslat jako součást URL

ZÁVĚR

Diplomová práce se věnuje návrhu a popisu realizace zcela nové datové sítě, která je realizována v jedné z laboratoří Ústavu telekomunikací. V této síti je kladen důraz na spolehlivost a efektivní využití datové sítě pro potřeby výuky předmětů se zaměřením na studium pokročilých síťových technologií. Svoji práci začínám teoretickým rozborem praktik, které jsou dnes při tvorbě datových sítí běžně užívány a hodnotím možnosti jejich zavedení a realizaci v datové síti laboratoře.

Při návrhu nové datové sítě vycházím především z poznatků uživatele (studenta) a následně z poznatků správce stávající infrastruktury. Tomuto rozboru je krátce věnována kapitola 2. Při návrhu se zaměřuji hlavně na nedostatky původní infrastruktury, za které považuji sníženou bezpečnost, strukturu datové sítě a její nečlenitost. Tyto poznatky mne vedou k přehodnocení možností správy takové sítě, dohledu nad samotnými prvky a zhodnocení efektivního využití vybavení laboratoře.

Z tohoto důvodu do infrastruktury sítě ve značné míře zavádím virtualizaci serverových prvků a přechod na vrstvový model uspořádání datové sítě. Cílem této restrukturalizace je zavést efektivnější využití jak v části tvořící serverovou infrastrukturu, tak i v části, která zajišťuje přístup k síti koncových stanic a jejich uživatelů. Protože je laboratorní síť užita k realizaci velkého množství experimentální výuky, snažím se infrastrukturu této sítě patřičně chránit zavedením pokročilejších bezpečnostních technik zejména v uživatelském fragmentu.

Původní datová síť bohužel vůbec nezohledňovala nároky na její spolehlivost, tedy sadu technických opatření vedoucích k odstranění případně vzniklých chybových stavů. Z tohoto důvodu se snažím datovou síť rozdělit na experimentální a produkční část s odlišnými metodami pro zajištění spolehlivosti obou částí sítě. Jedná se zejména o nasazení redundantních spojů mezi klíčovými zařízeními a tvorbu alternativních topologií, které zajistí, byť i za cenu snížené propustnosti části sítě, dostupnost všech zařízení v datové síti.

V poslední části zavádím systém pro sledování stavu prvků v síti i samotných koncových zařízení. Tento systém volím s ohledem na jeho jednoduchost jak z pohledu uživatele, tak i jeho správce. Tím je zajištěn dohled nad infrastrukturou v rámci laboratoře. V posledním kroku se věnuji zajištění záloh konfigurací všech prvků, jež tvoří funkční celek jak produkční infrastruktury, tak i experimentálních prvků. Na základě testování (zejména spolehlivosti a bezpečnosti) považuji novou strukturu sítě za funkční a spolehlivou. Od zimního semestru 2017 může být použita pro další výuku v laboratoři.

LITERATURA

[1] MINASI, M., GREENE, K., BOOTH C., BUTLER, R., MCCABE, J., PANEK, R., RICE, M., ROTH, S. *Mastering Windows Server 2012 R2*. Indianapolis: Sybex, 2014. ISBN 978-1-118-28942-6.

[2] FINN, A., GIBSON, D., SURKSUM, K. *Mastering Windows 7 deployment*. Indianapolis, Ind.: Wiley, 2011. ISBN 978-0-470-60031-3.

[3] PANEK, William. *MCSA Windows Server 2012 R2 Complete Study Guide*. Sybex, 2015. ISBN 978-1-118-85991-9.

[4] SIRON, Eric. *Microsoft Hyper-V Cluster Design: plan, design and maintain Microsoft Hyper-V Server 2012 and 2012 R2 clusters usign this essentail guide*. Birmingham: Packt Publishing, 2013. ISBN 178217768X.

[5] PLUMMER, David. *RFC 826: An Ethernet Address Resolution Protocol* [online]. [cit. 19. 4. 2017]. Dostupné z: <`https://tools.ietf.org/html/rfc826`>.

[6] *Unicast Flooding in Switched Campus Networks*. [online]. [cit. 19. 4. 2017]. Dostupné z: <`http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/23563-143.html`>.

[7] *Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S*. [online]. [cit. 2. 5. 2017]. Dostupné z: <`http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html`>.

[8] *Catalyst 6500 Release 12.2SX Software Configuration Guide*. [online]. [cit. 4. 5. 2017]. Dostupné z: <`http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html`>

[9] KIRAVUIO, T., SÄRELÄ Mikko, MANNER J. *A Survey of Thernet LAN Security*. [online]. [cit. 4. 4. 2017]. Dostupné z: <`http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6407456`>.

[10] BHAIJI, Yusuf. *Network security technologies and solutions*. Indianapolis, IN, Cisco Press, 2008. ISBN 978-1-58705-246-0.

[11] *IEEE 802.1: 802.1Q-2014 – Bridges and Bridged networks*. [online]. [cit. 11. 12. 2016]. Dostupné z: <`https://standards.ieee.org/findstds/standard/802.1Q-2014.html`>.

[12] NOVOTNÝ, V., KRKOŠ, R., NAGY, L. *Architektura sítí – laboratorní cvičení.* VUT v Brně, 2013. ISBN 978-80-214-4723-3.

[13] *Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches.* [online]. [cit. 15. 4. 2017]. Dostupné z: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html>.

[14] *802.1AX-2014 – IEEE Standard for Local and metropolitan area networks – Link Aggregation.* [online]. [cit. 15. 4. 2017]. Dostupné z: <http://standards.ieee.org/getieee802/download/802.1AX-2014.pdf>.

[15] MOCKAPETRIS, P. *Domain Names – Implementation and Specification.* [online]. [cit. 11. 10. 2016]. Dostupné z: <https://www.ietf.org/rfc/rfc1035.txt>.

[16] DROMS, R. *Dynamic Host Configuration Protocol.* [online]. [cit. 7. 10. 2016]. Dostupné z: <https://www.ietf.org/rfc/rfc2131.txt>.

[17] *Deploy a Hyper-V Cluster.* [online]. [cit. 5. 5. 2017]. Dostupné z: <https://technet.microsoft.com/en-us/library/jj863389(v=ws.11).aspx>.

[18] HARRINGTON, D., PRESUHN, R., WIJNEN, B. *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.* [online]. [cit. 1. 12. 2016]. Dostupné z: <https://www.ietf.org/rfc/rfc3411.txt>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ARP	Address Resolution Protocol – mechanismus zjištění MAC adresy na základě znalosti IP adresy
DHCP	Dynamic Host Configuration Protocol – protokol pro automatickou konfiguraci síťového rozhraní
IEEE	Institute of Electical and Electronics Engineers – asociace zabývající se vývojem v oblasti počítačových věd
SOAP	Simple Access Protocol – protol pro výměnu zpráv formátovaných do XML
UDP	Nespojově orientovaný protokol transportní vrstvy
TCP	Spojově orientovaný protokol transportní vrstvy
DNS	Systém jmenných názvů
STP	Spanning Tree Protocol – protokol pro převod obecné topologie na stromovou (odstranění smyček v síti)
BPDU	Bridge Protocol Data Unit – datová jednotka STP protokolů
ISO/OSI	Referenční model ISO/OSI – referenční vrstvový model pro zajištění komunikace v síti
QoS	Quality of Service – mechanismy pro garanci kvality služby
NAT	Network Address Translation – překlad adres síťové a/nebo transportní vrstvy
SIP	Session Initiation Protocol – signalizační protokol v IP sítích
WMI	Windows Management Instrumentation – struktura obsahující data a operace pro správu OS Windows
Intel VT-x	Funkce procesoru zajišťující podporu běhu virtuálních počítačů
AMD-V	Funkce procesoru zajišťující podporu běhu virtuálních počítačů
Intel XD	Execute Disable Bit – ochrana procesoru před spuštěním kódu v datovém segmentu programu
AMD NX	No-Execute Bit – ochrana procesoru před spuštěním kódu v datovém segmentu programu

LDAP	Lightweight Directory Access Protocol – protokol pro přístup a přenos informací v adresářové struktuře
AD DS	Active Directory Domain Services – Doménové služby Active Directory (implementace adresářových služeb firmou MS)
PXE	Preboot Execution Environment – metoda pro boot (start) počítače z počítačové sítě
WDS	Windows Deployment Services – Služba pro nasazení OS Windows
GUI	Graphical User Interface – grafické uživatelské rozhraní
GUID	Globally Unique Identifier – 128-bitový identifikátor objektu (unikátní)
ICMP	Internet Control Message Protocol – protokol pro přenos řídících zpráv na síťové vrstvě
IPMI	Intelligent Platform Management Interface – rozhraní pro správu HW bez závislosti na provozu OS
PoE	Power over Ethernet – přenos napájecího napětí po datovém vodiči
PoN	Power over Net – zdroj napětí říditelný pomocí IP protokolu
IOS	Operační systém zařízení spoelčnosti Cisco
VID	Identifikátor příslušnosti rámce k dané VLAN
ADC	Alternative Domain Controller – řadič domény Active Directory
ACL	Access Control List – Seznam pro řízení přístupu
DAI	Dynamic ARP Inspection – mechanismus kontroly jednotek ARP protokolu
MBR	Master Boot Record – Hlavní spouštěcí záznam na pevném disku

SEZNAM PŘÍLOH

A PŘÍLOHY

A.1 Seznam síťových prvků

Následující tabulka uvádí všechna instalovaná zařízení v nově vzniklé datové síti. Přístupové údaje jsou předány bezpečnou formou vedoucímu prace a nejsou součástí

Tab. A.1: Seznam použitých zařízení a přístupové údaje

Název hostitele	**Výrobce a model**	**IP adresa**	**Účel**
SW-R2-CORE-01	Cisco WS-3750X-48P	10.10.90.1	Přepínač jádra sítě
RB-R2-CORE-01	Mikrotik RB800	10.10.90.2	Hraniční směrovač
SW-R2-SRV-01	Zyxel XGS1910	10.10.90.3	Přepínač servr. segmentu
SW-R2-KLI-01	DLINK DGS3120	10.10.90.4	Přepínač klient. segmentu
SW-R3-LAB-01	HP ProCurve 2650	10.10.90.5	Přepínač s exp. zařízeními
SW-R3-LAB-02	HP ProCurve 2626	10.10.90.6	Nevyužitý přepínač

příloh.

A.2 Seznam provozovaných serverů

Následující tabulka uvádí všechny servery provozované v nově vzniklé datové síti. Přístupové údaje jsou předány bezpečnou formou vedoucímu práce a nejsou sou-

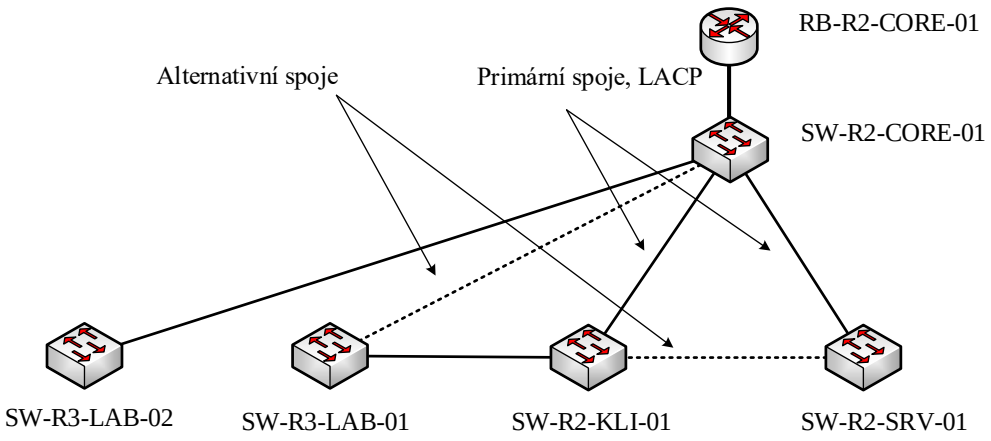
Tab. A.2: Seznam konfigurovaných serverů

Název hostitele	**Zařízení**	**IP adresa**	**Účel serveru**
sc5-32-dc01	AutoCont Mercury	10.10.20.2	AD, DNS, DHCP
sc5-32-hpv01	Cisco UCS210-M2	10.10.20.10	Virtualizace
sc5-32-hpv02	HP DL180G6	10.10.20.5	Virtualizace pro BARS
sc5-32-dc03v	Hyper-V HA VM	10.10.20.15	AD, DNS, DHCP
sc5-32-svn01v	Hyper-V VM	10.10.20.16	SVN služba
sc5-32-srv01vx	Hyper-V VM	10.10.20.17	TFTP server a zálohování
sc5-32-mng01v	Hyper-V HA VM	10.10.20.18	Správa stanic a serverů
sc5-32-mon01vxa	Hyper-V VM	10.10.20.18	Dohledový systém Zabbix

částí příloh.

A.3 Struktura navržené datové sítě

Architektura nově navržené datové sítě bez připojení koncových zařízení je zobrazena na obr. A.1.



Obr. A.1: Výsledná struktura nové datové sítě

A.4 Obsah přiloženého DVD

Na přiloženém DVD jsou konfigurační soubory všech zařízení, jejichž nastavení bylo měněno v průběhu práce. Na DVD jsou k dispozici i konfigurační soubory, dle kterých je nastaveno sledování agentem dohledového systému. Dále přikládám tabulku s využitím adresních prostorů a obsazení portů přepínačů pro užití jako podkladů pro provozní dokumentaci.

- `/konfigurace_zarizeni/rb-r2-lab-01-config_24-05-2017`
- `/konfigurace_zarizeni/sw-r2-core-01-config_24-05-2017`
- `/konfigurace_zarizeni/sw-r2-srv-01-config_24-05-2017`
- `/konfigurace_zarizeni/sw-r2-kli-01-config_24-05-2017`
- `/konfigurace_zarizeni/sw-r3-lab-01-config_24-05-2017`
- `/konfigurace_zarizeni/sw-r3-lab-02-config_24-05-2017`

Seznam zálohovacích skriptů:

- `/skripty_zalohovani/backup_sw-r2-core-01.sh`
- `/skripty_zalohovani/backup_sw-r2-srv-01.sh`
- `/skripty_zalohovani/backup_sw-r2-kli-01.sh`
- `/skripty_zalohovani/backup_sw-r3-lab-01.sh`
- `/skripty_zalohovani/backup_sw-r3-lab-02.sh`

Výsledky testů validity clusteru jsou uloženy v souborech `Create Cluster.htm` a `Failover Cluster Validation Report.htm`.

- `/Create Cluster.htm`
- `/Failover Cluster Validation Report.htm`
- `/xvacli00_mmst.pdf`

Tato konfigurace je konečná a platná k datu odevzdání práce. Obsah DVD obsahuje mj. i elektronickou kopii práce a odpovídá datové struktuře popsané výše.