POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Zabezpečení dat ve firemním prostředí

Diplomová práce

Data security in a corporate environment

Master thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Bc. Jan BEDEČ

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

Ve Slaném dne 14. 02. 2022

……

Bc. Jan BEDEČ

Poděkování

Chtěl bych poděkovat vedoucímu své diplomové práce RNDr. Václavu Hníkovi, CSc. za odborné vedení a vstřícnost při konzultacích. Dále bych chtěl poděkovat MV – GŘ HZS ČR za možnost využívat dostupné hardwarové vybavení pro potřeby diplomové práce.

ANOTACE
Diplomová práce popisuje ochranu dat ve firemním prostředí na několika úrovních. Počítačová bezpečnost, která se skládá ze zabezpečení počítače, mobilu, notebooku včetně povinností, které musí každý uživatel splňovat. Síťová bezpečnost, která chrání celistvost dat posílaných z jednoho zařízení na druhé a softwarová bezpečnost, která zajišťuje jednotné prostředí pro všechny firemní zaměstnance.

KLÍČOVÁ SLOVA
bezpečnostní protokoly * switch * router * Active Directory * Hyper-v * Group Policy * Cluster

ANNOTATION
The diploma thesis describes data protection in the corporate environment on several levels. Computer security, which consists of securing a desktop computer, mobile phone and laptop including the obligations that each user must fulfill. Network security, which protects the integrity of data sent from one device to another, and software security, which provides a unified environment for all corporate employees.

KEYWORDS
security protocols * switch * router * Active Directory * Hyper-V * Group Policy * Cluster

Obsah

Úvod

V dnešní době se s daty setkáváme na každém kroku, každý den a téměř kdekoliv na zemi. Rozmanitost technologií a obrovský potenciál dává vzniknout novým způsobům využití technologií pro přesun a ochranu dat.

Data můžeme vnímat jako informace v podobě jedniček a nul. Pro přenos těchto dat využíváme různé druhy přenosových sítí. Dnes má každá přenosová síť svůj hardware, software a pravidla, kterými se řídí. Jsou to sítě, které v dnešní době, přenáší data digitálně i analogově pomocí takzvaných datových rámců. Tyto rámce obsahují informace o zdroji a cíl, o cestě, kterou datový rámec musí absolvovat a kterými filtračními prvky projde.[1]

Důvodem, proč jsem si vybral téma diplomové práce „Zabezpečení dat ve firemním prostředí“, je vliv firemních dat jak na uživatele, tak na prostředí, ve kterém se firmy pohybují a kde interagují mezi sebou. Valná většina firemních zaměstnanců nepřikládá důraz na zabezpečení, protože si myslí, že se jich tato problematika netýká a že jsou jejich firemní data chráněná automaticky a k odcizení nebo zneužití nemůže dojít nebo jen velmi zřídka, a proč by to měl být zrovna ten nebo onen zaměstnanec. Ta šance je přeci velice nízká. Chyba.

Hackerské útoky se stávají stále větším strašákem. Firmy, které používají data jako každodenní prostředek komunikace a jako prostředek každodenního života zaměstnance jsou stále více v ohrožení z důvodu stále rychle se rozvíjejících technologií a možností proniknout zabezpečením firemních firewallů a ochran. Informace o hrozbách kyberterorismu nás obklopují ze všech stran a hrozba ztráty firemních dat se tak stává větší realitou než v dobách minulých. Bezpečné prostředí pro správu a přenos dat je jednou z největších priorit moderních firem.

[1] viz. str. 4, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. kapit. 1, ISBN 9781587143762.

1. Cíle a metodika práce

Cílem této diplomové práce je ukázat, jak komplexní je ochrana dat a jakou roli v ní hrají zaměstnanci, síťové prvky a softwarová řešení. V úvodu práce popíšu, co to vlastně data jsou a jakým způsobem se promítají do života běžných zaměstnanců a co pro ně představují. Pro pochopení, jak může uživatel přijít o firemní data, vysvětlím, jaké jsou doporučené postupy pro základní počítačovou bezpečnost, která se netýká pouze koncových stanic, jako jsou počítače nebo notebooky, ale také aktivní síťové prvky, které přenáší data uživatelů a je tedy potřeba mít bezpečnou firemní síť a rozumět činnosti jednotlivých zařízení a hlavně vědět, jaké možnosti správy tyto prvky mají. Na základní konfiguraci popíšu ochranu dat pomocí switchů a routerů. Dále se zaměřím na ochranu uživatelských dat pomocí nejčastěji využívaných nástrojů, jako je Active Directory, Group Policy a virtualizační platforma Hyper-V.

Každá část této diplomové práce bude obsahovat základní teorii i příklady, se kterými jsem se sám setkal nebo jej řešil v rámci své praxe. V každé z těchto kapitol budu používat a vysvětlovat technické termíny, které se běžně používají v prostředí informačních technologií.

K tomu, abych mohl vytvářet reálné simulace, budu využívat aktivní prvky firmy Cisco a hardware (dále jen HW), jehož vlastníkem je Generální ředitelství HZS ČR. K vysvětlení pojmů a mechanik využívám své vlastní znalosti a zkušenosti z praxe. Většina literatury, kterou při své práci cituji, pochází z certifikovaných kurzů Cisco a Microsoft. Jsou to tedy relevantní zdroje informací.[2] Bohužel není moc literatury, která se nabízí v českém jazyce, proto většina použité literatury pochází od zahraničních autorů.

Firmu Cisco jsem si vybral, protože je světovým leaderem na trhu se síťovými technologiemi a principiálně se firmy, které se síťovými technologiemi zabývají odlišují možnostmi správy, nikoliv základními funkcionalitami, které budu ve své diplomové práci rozebírat.

[2] Firma Cisco Technology Inc. je předním vývojářem a distributorem zařízení pro síťovou bezpečnost a komunikaci.

2. Data

Data se stala tak běžným slovem, že mnoho z nás pravděpodobně nikdy nepřemýšlelo o jejich přesné definici. První, co se lidem běžně vybaví, jsou s největší pravděpodobností tabulky nebo grafy, která obsahují čísla a znaky. Pokud někdo mluví o „*Big Data*“[3] stává se pojem ještě abstraktnější, protože ke správnému dešifrování je potřeba program, který veliké množství dat dešifruje. Pokud jsou to tedy stroje, kdo pracuje s daty, tak my pak vidíme pouze výsledek této činnosti. Nejčastěji jeho grafické znázornění.[4]

Pokud mluvíme o datech, tak na otázku „Co jsou data?“ můžeme odpovědět různými definicemi, z níž každá má z části pravdu. Podle společnosti Simplilearn, která je světovým leaderem v oblasti certifikovaných IT školení jsou data:

„*Data jsou různé typy informací, které jdou obvykle formátovány určitým způsobem. Veškerý software se pak rozděluje do dvou hlavních kategorií, a to jsou programy a data, kde programy jsou sbírkou instrukcí, které se používají k manipulaci s daty.“*[5]

Základní otázka tedy zní, jak citlivá data ve firemním prostředí jsou a jestli máme podchyceny všechny způsoby, díky kterým mohou být zcizena nebo zneužita. Únik dat může být způsobený omylem, například ztrátou flash disku nebo špatně zadanou e-mailovou adresou, ale i záměrným vynášením dat z firmy, a to například nespokojeným zaměstnancem. Všeobecně je známo, že největším nepřítelem firemních dat je samotný uživatel, a proto by měl být neustále vzděláván a prověřován, aby nedopatřením neohrožoval bezpečnost firmy.

[3] Big data jsou data z více zdrojů, ve velikém rozsahu, která protékají velikou rychlostí. Pozn. autora.
[4] SHEN, Stephanie. What is Data?: And why we need data management, data literacy and data analytics [online]. 29.11.2020 [cit. 10. 11. 2021]. Dostupné z: https://towardsdatascience.com/what-is-data-ade94b37204a
[5] SIMPLILEARN. What is Data: Types of Data, and How To Analyze Data? [online]. 10. 10. 2021 [cit. 10. 11. 2021]. Dostupné z: https://www.simplilearn.com/what-is-data-article#what_is_data

3. Počítačová bezpečnost

Zabezpečení přístupu uživatelů se týká kolektivních přístupů, pomocí kterých oprávnění uživatelé přistupují ke svému počítači, a neoprávněným uživatelům je v přístupu naopak zabráněno. Pro zpřesnění udávám, že zabránit přístupu uživatele omezuje i oprávněné uživatele na ty části systému, které mají výslovně povoleno používat. Není důvod k tomu, aby pracovník mzdové účtárny dostal povolení k přístupu na manažerská data. Ačkoliv má organizace právo chránit svá data prostřednictvím různých úrovní přístupu, uživatelé mají také svá práva. Je třeba vynaložit značné úsilí k informování všech firemních uživatelů o monitorování, logování systémů a sledování neoprávněných aktivit, které budou stíhány a prošetřovány. Je zde riziko, pokud organizace nebude informovat své zaměstnance anebo nezvaného útočníka, dopouští se tím narušení práva na soukromí každého, kdo se do systému dostane a nebude na tyto fakta upozorněn. Příkladem takové ochrany může být uvítací obrazovka, při přihlášení do systému, která varuje před neoprávněným vstupem. Pokud organizace takto přistupuje k ochraně svých dat, má to i další výhody:[6]

1) pomáhá chránit uživatelská data.
2) snižuje pravděpodobnost neoprávněného zveřejňování důležitých informací,
3) vzdělává uživatele o tom, co je v organizaci povoleno a co naopak zakázáno.

Zásady zabezpečení

Zabezpečení přístupu uživatelů vyžaduje, aby všechny osoby (nebo systémy), prokázaly, že jsou skutečně tím, za koho/co se vydávají. Uživatelé jsou následně omezení na přístup k těm souborům, které nezbytně potřebují k práci. Pro dosažení takového stavu je potřeba, aby bezpečnostní administrátoři vytvořili zásady zabezpečení napříč celou organizační strukturou pomocí uživatelských

[6] SZUBA, Tom, KING, Steve, ed. Safeguarding your Technology: Practical Guidelines for Electronic Education Information Sercurity. Washington, DC 20208-5574: U.S. Department of Education. National Center for Education Statistics., 1998, s. 86. Dostupné z: https://nces.ed.gov/pubs98/safetech/

účtů, Group Policy[7] (dále jen GPO), síťové bezpečnosti pomocí aktivních síťových prvků a mechanismů pro vzdálený přístup.[8]

3.1 Základní bezpečnostní opatření organizace

Národní úřad pro kybernetickou a informační bezpečnost vytvořil brožuru, jako doporučení pro bezpečné chování v kyberprostoru, a to bez ohledu na to, jestli se jedná o soukromý sektor nebo nikoliv. Materiál se zaměřuje především na management, ale i na zaměstnance, kteří svým chováním značně ovlivňují bezpečí organizace před kybernetickými útoky.

Obecná pravidla

„NEPOUŽÍVAT INFORMACE, KTERÉ JDOU NAD RÁMEC POTŘEBY AKTUÁLNÍ SITUACE.
Vše, co je obsahem komunikace, může být v budoucnu zneužito.“[9]

„MÍT NA PAMĚTI, ŽE NIC NENÍ ZADARMO.
Nabídky a on-line služby zdarma, které jsou jindy placené, je potřeba důkladně zvažovat.“[10]

„POKUD PROBÍHÁ KOMUNIKACE V ČASOVÉ TÍSNÍ, JE POTŘEBA O TO VÍCE UVAŽOVAT O JEJÍM OBSAHU A SDĚLOVÁNÍ POŽADOVANÝCH INFORMACÍ.
Útočníci rádi pracují s časovou tísní – teď je třeba něco vykonat, napravit, sdělit. Je potřeba to mít na paměti. Škoda z prodlení bývá menší než důsledky neuvážených činů.“[11]

[7] Skupinové politiky, které zakládají, mění nebo ruší předem daným skupinám oprávnění ve firemní síti. Pozn. autora
[8] SZUBA, Tom, KING, Steve, ed. Safeguarding your Technology: Practical Guidelines for Electronic Education Information Sercurity. Washington, DC 20208-5574: U.S. Department of Education. National Center for Education Statistics., 1998, s. 88. Dostupné z: https://nces.ed.gov/pubs98/safetech/
[9] viz str. 1, Národní úřad pro kybernetickou a informační bezpečnost. Základní bezpečnostní opatření pro vrcholové vedení [online]. 17. 9. 2021 [cit. 17. 09. 2021]. Dostupné z: https://www.nukib.cz/download/publikace/doporuceni/Zakladni_bezpecnostni_opatreni_pro_vrcholove_vedeni_brozura_barevna.pdf
[10] Ibid. str.1.
[11] Ibid. str.1.

3.2 Zabezpečení účtu

Firemní účty jsou pod dohledem organizace a není žádoucí je používat pro soukromé účely. Stejně tak soukromé účty, které nejsou spravované a nepodléhají bezpečnostním prvkům organizace, není moudré používat uvnitř firemního prostředí, například z důvodu infiltrace škodlivého kódu přes soukromý email, flash disk nebo mobilní zařízení. Základním prvkem bezpečnosti je uživatelské heslo pro přístup do firemního prostředí. Hesla k účtu musí být unikátní a pro každou službu rozdílná. V případě prolomení jednoho hesla může útočník toto heslo použít k prolomení dalších služeb. Heslo by nemělo být sdělováno nikomu, ani administrátorovi. Pro obnovení hesla není vhodná metoda kontrolních otázek. Informace z převážné většiny se dá dohledat na internetu.[12]

3.3 Práce s firemním zařízením

Základem bezpečnosti je použití pouze firemního, a tudíž organizací spravovaného hardware. Soukromá zařízení, která nespadají do bezpečnostní politiky, jsou zdrojem nebezpečí, protože nejsou pod dohledem. Taková zařízení neustále přenášejí data z a do zařízení, obsahují aplikace, které nejsou vhodná pro práci, a není vždy přesně patrné, co všechno dělají.

Jakékoliv firemní zařízení by nemělo být bez dohledu. Takové dává prostor útočníkovi k manipulaci s ním i jeho obsahem. Základními zásadami pro práci s firemním zařízením jsou:[13]

1) Nepřipojovat neznámé zařízení do firemní sítě. Taková zařízení, jako flash disk nebo externí disk, mohou obsahovat skrytý škodlivý kód, který se po připojení nahraje do systému a aktivuje.
2) Volit dlouhá hesla, která jsou zapamatovatelná, ale složitá.
3) Provádět aktualizace a vypínat stroj, pokud s ním nikdo nepracuje. Aktualizace se provádí na firemní úrovni a uživatel by o tom měl být srozuměn a mít dostatek času na ukončení a uložení veškeré činnosti.

[12] viz str. 2, NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Základní bezpečnostní opatření pro vrcholové vedení [.pdf]. 2020, [cit. 17. 11. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1630-zakladni-bezpecnostni-opatreni-pro-vrcholove-vedeni/

[13] Ibid str. 2.

4) Pravidelně zálohovat data. Vždy existuje riziko ztráty dat, např. při poruše disku počítače nebo cíleném útoku. Je proto důležité zálohovat data a mít je uložené jinde než v daném zařízení. Příkladem může být záloha na páskovou mechaniku, přičemž po provedení zálohy se páska odebere z mechaniky a uloží bezpečně do sejfu.
5) Věnovat pozornost odkazům, na které máme možnost kliknout. Vždy je potřeba ověřit identitu protistrany.
6) Kontrolovat obsah e-mailu. V případě podezření, kontaktovat IT oddělení.

4. Bezpečnostní protokoly

Pro ověření přístupu k uživatelskému účtu, firemnímu zařízení nebo aplikaci nacházejí uplatnění protokoly, které mohou být v rámci organizace nasazeny z důvodu bezpečnosti.

4.1 AAA protokoly

V oblasti bezpečnosti představují authentication, authorization a accounting. Protokoly AAA fungují tak, že se uživatel připojí na klienta AAA a požádá o přístup do sítě. AAA klient pošle žádost na server, který má na starosti ověření. Z pravidla to bývá doménový kontroler. Sever zpracuje požadavek a vrátí klientu kladnou nebo zápornou odpověď. AAA klient poté informuje uživatele o tom, jestli mu byl udělen přístup nebo nikoliv.[14]

4.1.1 Autentizace

Autentizovaný uživatel je takový uživatel, který má oprávnění požadovat služby pomoví síťových služeb. Autentizovat uživatele můžeme pomocí:[15]

- **Znalostí** – uživatel se prokáže znalostí uživatelského jména a hesla po případě pinu nebo odpovědí na vygenerovanou otázku.
- **Žadatele** – ten, kdo žádá o přístup, se ověřuje pomocí biometriky, jako je rozpoznání obličeje, otisk prstu, hlasové rozpoznání, rozpoznání duhovky.
- **Předmětu** – žadatel se prokáže pomocí předmětu, který je synchronizovaný se systémy na ověření identity (USB Token, RSA zařízení, služební průkaz apod.).

4.1.2 Autorizace

Autorizace poskytuje žadateli takovou službu, na kterou má nárok, pokud se autentizuje do systému. Autorizace omezuje uživatele například na síťových službách, času nebo fyzické polohy. Příkladem může být doba, po kterou je

[14] viz str. 14-15, MILFAJT, Jiří. Bezpečnostní protokoly v praxi: SECURITY PROTOCOLS IN PRACTICE. Brno, 2008, [cit. 20. 11. 2021] Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce Ing. Tomáš Pelka.
[15] viz str. 104, BURDA, Karel. Bezpečnost informačních systémů. [Skripta] VUT Brno: 2005. [cit. 20. 11. 2021].

žadatel vpuštěn do sítě nebo sekce, ve které se zrovna nachází. Dalším způsobem je filtrování IP adres, směrování nebo šifrování.

4.1.3 Accounting

Accounting je sledování využívání služeb, které uživatel po autorizaci využívá. Informace jsou využívány administrátory sítě. Administrátoři tak v reálném čase logují využívání síťových zdrojů, veškerou komunikaci nebo dobu přihlášení i odhlášení.

4.2 Přenosové protokoly

Pro bezpečný přenos souborů jakéhokoliv druhu je dobré mít základní přehled o protokolech, díky kterým můžeme sdílet data bezpečně a bez obav.

Základní druhy přenosových protokolů jsou:[16]

FTP

File Transfer Protocol je původní protokol pro přenos souborů. Je to původní metoda přenosu souborů, která existuje již desítky let. FTP vyměňuje data pomocí dvou samostatných kanálů, kterým se říká příkazový kanál a datový kanál. Příkazový kanál slouží pro ověření identity uživatele a datový kanál slouží pro přenos souborů. U FTP jsou oba kanály nešifrované. Všechna data, která pošleme těmito kanály, jsou náchylná k jejich zneužití.

FTPS

File Transfer Protocol přes SSL/TLS je nadstavba klasického FTP přenosu. K ověření se používají klientské nebo serverové certifikáty a hesla.

SFTP

SFTP je zkratka pro FTP přes SSH. Je to zabezpečený FTP protokol určený jako alternativa k FTP nebo ručně psaným skriptům. SFTP vyměňuje data přes SSH spojení a poskytuje organizacím vysokou úroveň ochrany pro přenosy souborů sdílené mezi systémy nebo mezi systémy a zaměstnanci.

[16] HEATH, Kath. What Are the Top File Transfer Protocols [online]. 25. 03. 2020 [cit. 20. 11. 2021]. Dostupné z: https://www.goanywhere.com/blog/what-are-the-top-file-transfer-protocols

SCP

Secure Copy Protocol je starší síťový protokol, který podporuje přenosy souborů mezi hostiteli v počítačové síti. Rozdílem mezi FTP a SCP je ten, že SCP využívá funkce šifrování a ověřování.

HTTP a HTTPS

Hyper Text Transfer Protocol je páteří WWW (World Wide Web) jako základ datové komunikace. Definuje formát zpráv, prostřednictvím kterých webové prohlížeče a webové servery komunikují. HTTP používá TCP (Transmition Control Protocol) jako základní protokol pro přenos souborů.

HTTPS je zabezpečená verze HTTP protokolu, která komunikuje prostřednictvím certifikátu.

TCP/IP protokoly

Vznikly s cílem vytvořit sadu protokolů, u kterých bude možné udržet integritu dat. Více o sadě protokolů TCP/IP v kapitole 4.3.3.

4.3 Síťové protokoly

Základem síťové bezpečnosti je pochopení komunikace mezi dvěma zařízeními. Pro pochopení této komunikace je důležité znalost TCP/IP[17] protokolu.

4.3.1 Síťová komunikace

Zařízení v síti je buď odesílatelem, nebo příjemcem zprávy. Komunikace začíná tak, že jedno zařízení vysílá zprávu nebo informaci k druhému. Zpráva projde skrz přesně definovanou cestu v síti k cílovému zařízení. Pro úspěšný přenos zprávy slouží v síti veliké množství protokolů. Každý takový protokol má jasně nastavená pravidla komunikace. Popisují, co se má stát během komunikace. Síťové protokoly jsou součástí softwaru, který je nejčastěji dodán s hardwarem.[18]

O softwaru se bavíme jako o programovém vybavení, který je spojením mezi softwarem a hardwarem. Hardware je pak počítač samotný, ale i grafická a zvuková karta nebo tiskárna apod.[19]

---

[17] TCP/IP je sada protokolů, díky kterým stroje komunikují v síti.

[18] viz str. 48-49, LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 9788025123591.

[19] Správa-site.eu: Správa sítě – slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT [Online]. [Cit: 20. 11. 2021]. Dostupné z: https://www.sprava-site.eu/software/

Původní komunikace mezi zařízeními probíhala pouze, pokud měly počítače stejné aplikační vybavení. Každý vývojář spravoval pouze svou vlastní aplikaci a zabudovaný komunikační software. Tím pádem nemohly aplikace s rozdílnou komunikační sadou komunikovat mezi sebou. Tento problém byl z části odstraněn tím, že se oddělil software aplikační od software komunikačního. Díky tomu mohla mít aplikace více komunikačních technologií. Stále však byla závislá na jednom konkrétním výrobci. Revoluce přišla až s příchodem standardizovaného OSI modelu.[20]

4.3.2 OSI model

Standardizovaný OSI model popisuje, jakým způsobem prostupují data sítí. Byl vytvořen, aby spolu mohly komunikovat zařízení s rozdílným operačním systémem (windows, linux, android, IOS, OS X apod.). Jsou to zásady, které vývojáři dodržují, aby spolu mohly aplikace skrz internet komunikovat.[21]

Vrstvy referenčního modelu OSI (obrázek č.1)[22]:

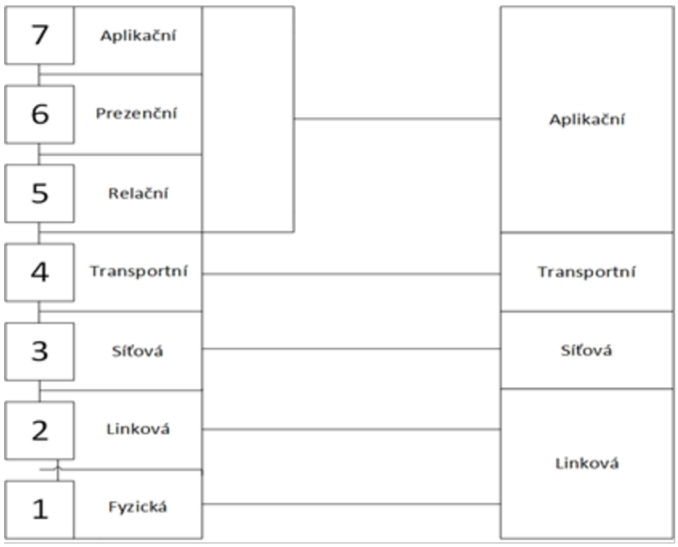
Obrázek 1 Vrstvy referenčního modelu OSI.

[20] viz kap. 1, str. 16, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.
[21] Ibid. kap. 1, str. 18.
[22] viz kap. 1, str. 18, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.

4.3.3 TCP/IP protokoly

Problémem této sady protokolů spočívá v tom, že vrstvy sdílí informace jenom s vrstvou nad sebou nebo pod sebou a zároveň musí být všechny vrstvy obsazeny. Protokoly TCP/IP vychází z OSI modelu, ale dokážou udržet integritu dat v komunikaci.[23]

Sada protokolů TCP/IP (obrázek č. 2) [24] je nejpoužívanější sadou protokolů pro komunikaci Host – Host. Tyto protokoly popisují, jak jsou data adresována, formátována anebo směrována v síti.



Obrázek 2 Model TCP/IP vs. ISO/OSI.

Funkce sady protoklů TCP/IP jsou rozděleny na čtyři vrstvy. To je rozdíl oproti OSI modelu, který má vrstev sedm.[25]

- **Linková vrstva** zastává ty samé funkce, jako linková a fyzická vrstva OSI modelu. Udává formátování dat a popisuje fyzické vlastnosti.
- **Síťová vrstva** směřuje datové rámce od zdroje dat k cílovému hostiteli. Informace o cestě paketu a o způsobu cesty je v datovém rámci zapsaná. Přesun jednoho paketu ze síťové do transportní vrstvy je nazýváno jako

[23] viz str. 103, LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 9788025123591.
[24] SOCHA, Łukasz. Grandmetric: tcp-model-vs-iso-osi-model [online]. 2019 [cit. 20.11. 2021]. Dostupné z: https://www.grandmetric.com/topic/network-layers-and-devices-operation/tcp-model-vs-iso-osi-model/
[25] viz kap. 1, str. 20, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.

směrování paketů. Jakmile se paket přesune, probíhá jeho fragmentace nebo defragmentace podle účelu cesty a typu komunikace.

- **Transportní vrstva** – je středem TCP/IP protokolů. Pomocí aplikačních procesů komunikuje s objekty, které se nachází v síti.
- **Aplikační vrstva** – tato vrstva slouží pro přenos souborů a případný troubleshooting.[26] Tato vrstva také umožňuje, poskytnutí komunikačních služeb mezi aplikacemi různých operačních systémů.

4.3.4 IP – Internet Protocol

Internet Protocol (dále jen IP) je obsažen v sadě protokolů TCP/IP a směruje pakety podle cílových adres. IP má několik funkcí:[27]

a) Je obsažen na třetí vrstvě modelu OSI a na druhé vrstvě protokolů TCP/IP.
b) Jako protokol je považován za „*connectionless*“.[28] To znamená, že pokud jsou data přenášena, tento protokol se nezabývá tím, kolik bylo paketů na začátku přenosu a kolik jich dorazilo do cíle.
c) Pakety nechodí po stejných trasách, protože jsou zpracovávány každý zvlášť.
d) Neposkytuje kontrolu při posílání paketů sítí.
e) Neopravuje poškozené pakety.
f) IP existuje ve dvou variantách, a to IPv4 a IPv6.

4.3.4.1 Praktický příklad fungování IP v síti

Posíláte 10 balíků z České republiky do Itálie. Každý balíček obsahuje jednu část stavebnice. Přepravní služba balíky sice doručí, ale nikdy nezaručí, že balíky dopraví do cíle stejný dopravce, ve správném pořadí a že bude všech deset balíků v pořádku předáno.

[26] Troubleshooting je termín pro hledání problému.
[27] viz kap. 2, str. 4, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.
[28] Ibid.

5. Zabezpečení pomocí aktivních síťových prvků

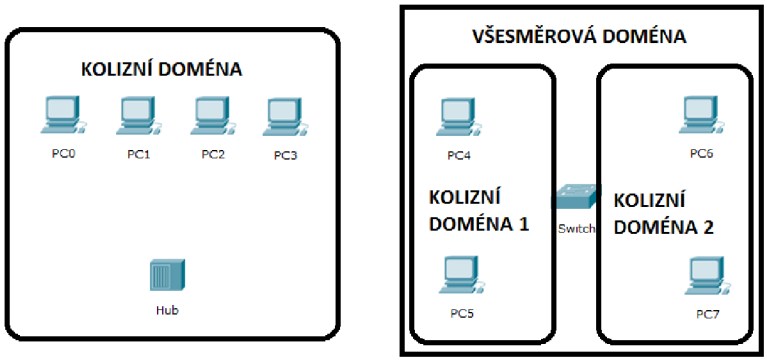
Mezi základní aktivní síťové prvky patří switche a routery (směrovače). Na těchto zařízení můžeme směrovat a předávat pakety v jedné síti, ale i mezi sítěmi navzájem. Tyto prvky představují celou plejádu možností, jak zabezpečit data proti ztrátě, poškození nebo zneužití.

5.1 Switche

Switch je takové zařízení, které poskytuje propojení mezi prvky na linkové vrstvě TCP/IP modelu. Pokud propojíme několik počítačů nebo serverů mezi sebou, potřebujeme právě switch k tomu, aby třídil komunikaci.

V minulosti fungovala komunikace objektů v síti mezi sebou pouze pro jedno zařízení v síti v určitou dobu. Propojeny byly tzv. opakovačem neboli HUB zařízením. Toto zařízení odesílá pakety na všechna připojená zařízení v dané síti kromě toho, které zprávu odeslalo. Síť, která má takto zapojená zařízení do opakovače signálu, označujeme jako kolizní doménu. V dnešní době se ve firemním prostředí tato zařízení nenachází. Jejich místa nahradily switche.[29]

Kolizní a všesměrová doména (obrázek č. 3)[30]:



Obrázek 3 Rozdíl mezi kolizní a všesměrovou doménou.

Switch oproti zařízení typu HUB dokáže rámce filtrovat. Užívá k tomu MAC adresy.[31] Předává tedy informace z jednoho portu na port cílového uzlu. Pro přenos využívá celou šířku pásma. To se vztahuje pouze na jeden rámec. Switch si pro sebe udržuje a aktualizuje tabulku s MAC adresami. V této tabulce se

[29] BROUŠKA, Petr. CSMA/CD, kolizní doména, duplex. [Online]. 2005. [Cit: 25. 11. 2021]. Dostupné z: https://bit.ly/3oYLF9S
[30] BEDEČ, Jan. Rozdíl mezi kolizní a všesměrovou doménou. Slaný. [cit. 25. 11. 2021].
[31] MAC adresa – jednoznačný identifikátor hardwaru

nachází informace o tom, za jakým portem se daná MAC adresa nachází. V hlavičce každého rámce je cílová MAC adresa, ta je porovnána s tabulkou, kterou má switch uložený v paměti. Podle toho se rozhodne, kam rámec pošle a v případě nesouladu rámec zahodí.[32]

Základní charakteristika

Základní výhody switchů v organizaci.[33]

- **Počet portů** – nabízí se varianty od 4 portů až po 48 portová zařízení. Střední a velké firmy využívají i možnost zapojit switche do tzv. STACK[34] modu. Maximální počet je tedy teoreticky neomezený. Z pravidla bývají omezené pouze finance, které jsou firmy ochotny vynaložit.
- **Rychlost portů** – rychlost sítě je vždy omezována nejpomalejším zařízením v síti/doméně. Některé switche umožňují modulárně měnit porty a tím získat vyšší propustnost. Některé firmy dokonce omezují rychlost portů pomocí zakoupených licencí.
- **Nízké náklady** – díky relativně nízkým nákladům na jeden port je i pro menší firmy možné si segmentovat síť a využívat řadu bezpečnostních benefitů, které switche nabízí.

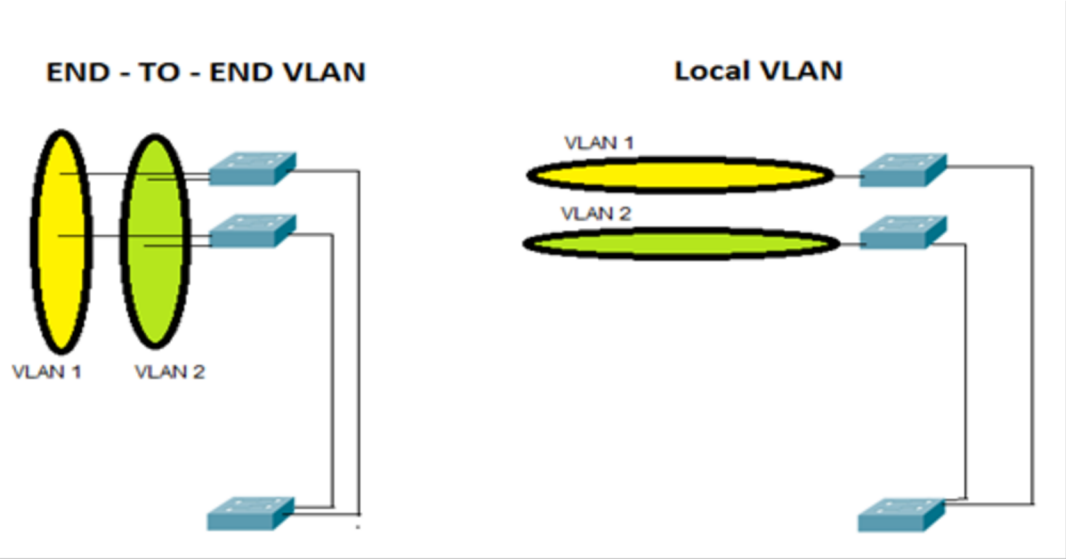
5.1.1 VLAN

VLAN je značení pro Virtuální LAN. To znamená, že každá VLAN představuje jednu logickou síť. Použitím těchto logických sítí můžeme firemní prostředí segmentovat na menší sítě a tím přehledněji spravovat zařízení a vytvářet bezpečnější prostředí. Komunikaci mezi VLAN probíhá pomocí trunk[35] portů. V organizaci se nejčastěji setkáme se dvěma různými druhy integrace VLAN. Prvních z nich jsou **end-to-end** VLAN, kdy jedna VLANa je konfigurována na více switchů a každý tento jeden switch je propojen jedním centrálním switchem. Takto vytvořené prostředí musí být propojeno mezi switche přes trunk

[32] viz kap. 1, str. 30, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.
[33] Ibid. str. 31.
[34] Pokud jsou zařízení ve STACKU, tak se v managementu tváří, jako jedno zařízení.
[35] TRUNK je port, který komunikuje skrz více VLAN. Pozn. autora

porty. Tyto porty poté směřují provoz skrz definované VLANy. Druhou variantou jsou tzv. **lokální VLANy**. Tato varianta je preferovaná firmou Cisco. VLANy jsou od sebe v této variantě odděleny i hardwarově. Z bezpečnostního hlediska je to nesporná výhoda, bohužel velice nákladná. Nevýhodou této varianty jsou tedy zvýšené náklady na pořízení hardwaru, a hlavně fyzicky limitovaní uživatelé, kteří se například z jiného patra než z toho, kde je VLANa definována, nepřipojí. Příkladem může být několikapatrový dům, kde patro reprezentuje určitou sekci nebo oddělení.[36]

Možnosti integrace VLAN (obrázek č. 4)[37]:



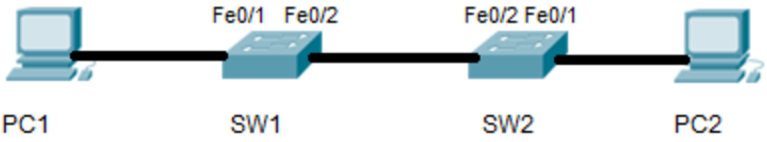
Obrázek 4 Grafické znázornění END – TO – END a local VLAN.

5.1.1.1 VLAN – praktická ukázka

V praktické ukázce představím základní nastavení VLAN a ověření jejich funkce vůči dvěma počítačům a dvěma switchům. V první fázi budou počítače zapojené do stejné VLANy. V druhé fázi bude každý počítač v jiné VLANě. Tím ověřím, kdy si spolu mohou klienti vyměňovat data (packety), a kdy ne.

VLAN – praktická ukázka (obrázek č. 5)[38]:

[36] viz kap. 2, str. 4, FROOM, Richard, SIVASUBRAMANIAN, Balaji and FRAHIM, Erum. Implementing Cisco IP switched networks (SWITCH). 1st ed. Indianapolis: Cisco Press, 2010. ISBN 9781587058844.
[37] BEDEČ, Jan. Grafické znázornění END – TO – END a local VLAN. Slaný. [cit. 26. 11. 2021].
[38] BEDEČ, Jan. Vlan: Schéma zapojení. Slaný. [cit. 26. 11. 2021].



Obrázek 5 Vlan: Schéma zapojení.

Vlastní konfigurace

PC1 (obrázek č. 6)[39] má nastavenou IP adresu 192.168.1.10. Maska je 255.255.255.0 (obrázek č. 6). V tomto případě nepotřebujeme nastavovat defaultní gateway.[40]

```
PC1>
     IP address.....................: 192.168.1.10
     Subnet Mask....................: 255.255.255.0
     Default Gateway................: 0.0.0.0

```

Obrázek 6 Výpis z terminálu na PC1.

PC2 (obrázek č. 7)[41] má IP 192.168.1.20 s maskou sítě 255.255.255.0.

```
PC2>
     IP address.....................: 192.168.1.20
     Subnet Mask....................: 255.255.255.0
     Default Gateway................: 0.0.0.0

```

Obrázek 7 Command Line výpis PC2.

Oba switche jsou nakonfigurovány tak, aby porty, které jsou směrem k počítačům, byly v modu access a zároveň porty, které spojují switche, byly mezi sebou propojeny porty v modu trunk (obrázek č. 8 a č. 9)[42]. Trunk porty zároveň nastavíme tak, aby o svém zařazení s nikým nevyjednávaly. Pokud tedy nastavíme vyjednávání na interface jednotlivých portů, musí se porty tvářit tak, jak jsou nastaveny. Nemohou se tedy svévolně přepnout do jiného režimu.

[39] BEDEČ, Jan. Výpis z terminálu na PC1. Slaný. [cit. 26. 11. 2021].
[40] Default Gateway je anglický název pro bránu, přes kterou zařízení komunikuje.
[41] BEDEČ, Jan. Command Line výpis PC2. Slaný. [cit. 26. 11. 2021].
[42] BEDEČ, Jan. Výpis portů na SW1 a SW2. Slaný. [cit. 26. 11. 2021].

```
SW1#
Interface FastEthernet0/1
 switchport mode access
 switchport access vlan 30
 switchport nonegotiate
!
Interface FastEthernet0/2
 switchport mode trunk
 switchport nonegotiate
```

Obrázek 8 Výpis portů na SW1.

```
SW2#
Interface FastEthernet0/1
 switchport mode access
 switchport access vlan 30
 switchport nonegotiate
!
Interface FastEthernet0/2
 switchport mode trunk
 switchport nonegotiate
```

Obrázek 9 Výpis portů na SW2.

Takto nastavené prvky propustí komunikaci mezi sebou. Ověřit, že tomu tak skutečně je můžeme pomocí příkazu „ping“, který spustíme v příkazovém řádku neboli Terminálu.

Test komunikace z PC 1 na PC2 pomocí terminálového příkazu PING. (obrázek č. 10 a č. 11)[43]

```
PC1>ping 192.168.1.20

Pinging 192.168.1.20 with 320bytes of data:

Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Obrázek 10 Test komunikace z PC1 na PC2.

[43] BEDEČ, Jan. Ping z PC1 na PC2 a z PC2 na PC1. Slaný. [cit. 26. 11. 2021].

```
PC2>ping 192.168.1.10

Pinging 192.168.1.10 with 320bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Obrázek 11 Test komunikace z PC2 na PC1.

Z obrázku č. 11 a č. 12 je zřejmé, že spolu PC1 a PC2 dokáží na síťové vrstvě komunikovat oběma směry. Na řádku jedenáct u obou obrázků je výpis nejdůležitějších informací, které říkají, kolik paketů bylo odesláno a kolik paketů bylo zpět přijmuto.

5.1.2 Port Security

Port Security utilita, umožňuje ochránit data před vstupem neautorizovaného zařízení do sítě. Zabezpečení přístupu probíhá na úrovní portů switche.[44]

Základem bezpečnosti u switche je zakázat access porty, které nejsou využívané. To znamená, že manuálně nastavíme port jako *„Administratively down“*[45]. Pokud se tedy do takto nastaveného portu někdo připojí, port se neaktivuje a zařízení do něj připojená žádná data nepřijme ani žádná neodešle. Pokud využíváme port security, musíme mít dokonalý přehled o tom, která zařízení do portu má vstupovat a do jaké části sítě se má zařízení komunikovat. Je to jeden ze způsobů, jak zabezpečit switch na úrovni portů a zabránit tak úniku dat.[46]

Správně nastavená port security omezí přístup pomocí zapsané MAC adresy, kterou má switch uloženou v tabulce ve své paměti. MAC adresy si switch načte buď dynamicky anebo je administrátor zadá v konzoli aktivního prvku.

---

[44] BROUŠKA, Petr. nastavení interface/portu - access, trunk, port security. [Online]. 2009, Cisco IOS 3. [Cit: 26. 11. 2021]. Dostupné z: https://bit.ly/3IRieyx

[45] Cisco IOS Router Basic Configuration: CCNA Routing & Switching ICND1 100-105 [online]. [cit. 27. 11. 2021]. Dostupné z: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/cisco-ios-router-basic-configuration

[46] Viz kap. 3, str. 18, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.

Port, který má nastavenou port security přijímá a odesílá data pouze, pokud je cíl za správnou MAC adresou.

Způsoby zadávání MAC adres pro port security jsou:[47]

- Dynamické – přesně specifikuje, jaké adresy může daný port používat. Nastavit můžeme časový horizont nebo platnost nově přistupující adresy.
- Statické – adresy se zadávají ručně do konzole switche. Switch pak na základě tabulky přijímá data v rámci povolených MAC adres.
- Dynamické + statické přiřazování adres – na switchi můžeme nastavit kombinaci dynamického a statického zapisování MAC adres do tabulky. V podstatě můžeme říct, jaké adresy jsou povolené a jaký počet adres má být povolen celkové. Pokud tedy určím, že na jeden konkrétní port může být povolen přístup pouze z 6 MAC adres a tři zadám staticky, tak pro dynamické přiřazení zbývají pouze 3 paměťové sloty v tabulce.

5.1.2.1 Port Security – praktická ukázka

Praktická ukázka bude probíhat mezi PC1 a PC2. Jako prostředník komunikace bude sloužit Cisco switch 2950 (obrázek. č. 12) [48].

- PC1: IP 192.168.1.10; maska 255.255.255.0; MAC adresa 0060.475B.EAD3
- PC2: IP 192.168.1.20; maska 255.255.255.0; MAC adresa 000C.85EB.8952
- Switch: VLAN10; PC1 na portu Fa0/1; PC2 na portu Fa0/2

Obrázek 12 Port Security: Schéma zapojení.

[47] Ibid. kap. 3, str. 21.
[48] BEDEČ, Jan. Port Security: Schéma zapojení. Slaný. [cit. 27. 11. 2021].

Postup konfigurace

Na obou počítačích nastavím IP adresu a pomocí ethernetového kabelu je připojím ke switchi. Na switchi nakonfiguruji VLAN10 na portech FastEthernet0/1 a 0/2. Díky takto nakonfigurovaným portům na switchi může mezi PC1 a PC2 probíhat komunikace. Pro ověření použiji ICMP příkaz v terminálovém řádku. (obrázek. č. 13)[49]

```
PC1>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=1ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
PC2>ping 192.168.1.10

Pinging 192.168.1.10 with 320bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Obrázek 13 Výpis příkazu „ping“ na PC1 a PC2.

Je více možností, jak nastavit Port Security na switchi. Můžeme ukládat MAC adresy staticky nebo dynamicky do paměti switche. Můžeme kombinovat mezi statickým a dynamickým ukládáním. Důležité je ale i to, co se stane s portem, který nesplňuje nastavená pravidla. Pokud na port switche přijde MAC adresa, která není v adresní tabulce zavedená, tak nastává jedna ze tří možností nastavení restrikcí:[50]

1. **Protect:** Pokud se se switchem na určitém portu komunikuje MAC adresa, která není povolená, komunikační data se zahazují, ale pro povolené adresy, které s portem komunikují, se nic nemění. Tam komunikace probíhá dál.
2. **Restrict:** Na dohledový server přijde zpráva o neautorizované komunikaci.
3. **Shutdown:** Pokud proběhne neschválená komunikace, switch převede port do error-disable stavu. Tím se veškerá komunikace na portu zablokuje.

Pro konkrétní příklad nastavím statickou Port Security tak, aby došlo k porušení pravidel a port se dostal do error-disabled stavu (obrázek. č. 14)[51].

[49] BEDEČ, Jan. Výpis příkazu „ping“ na PC1 a PC2. Slaný. [cit. 27. 11. 2021].
[50] BROUŠKA, Petr. Nastavení interface/portu - access, trunk, port security. [Online]. 2009, Cisco IOS 3. [Cit: 27. 11. 2021]. Dostupné z: https://bit.ly/3CUEuTS
[51] BEDEČ, Jan. Příkaz „Show running-config“ na SW1. Slaný. [cit. 27. 11. 2021].

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0060.2FAB.64B6
```

Obrázek 14 Příkaz „Show running-config“ na SW1.

Na výpisu je patrné, že security je nastavená pouze na jednom portu a pouze pro jednu MAC adresu (obrázek č. 15)[52].

```
SW1#show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address Type            Ports       Remaining Age
                                  (mins)
----    ----------- ----            -----       -------------
10  0060.2FAB.64B6  SecureConfigured    FastEthernet0/1
```

Obrázek 15 Ověření konfigurace Port Security na SW1 a portu FastEthernet0/1.

Pokud na takto nastavený port připojím zařízení s jinou MAC adresou, Port Security daný interface okamžitě vypne (obrázek č. 16)[53].

```
SW1#show port-security interface FastEthernet 0/1
    Port Security              : Disabled
    Port Status                : Secure-down
    Violation Mode             : Shutdown

```

Obrázek 16 Příklad vypnutého portu pomocí Port Security.

Konfigurovat Port Security není náročné, ale je dobré předem plánovat a dokumentovat, jak bude zabezpečení nastaveno a jakým způsobem se bude nasazovat do firemního prostředí.

5.1.3 EtherChannel

EtherChannel slouží pro spojování linek, dovoluje spojit více interface do jednoho logického portu. Používá se především mezi switchi navzájem anebo mezi switchem a serverem. Jednoduše tam, kde je potřeba zvětšit propustnost sítě.[54]

[52] BEDEČ, Jan. Ověření konfigurace Port Security na SW1 a portu FastEthernet0/1. Slaný. [cit. 28. 11. 2021].
[53] BEDEČ, Jan. Příklad vypnutého portu pomocí Port Security. Slaný. [cit. 28. 11. 2021].
[54] BROUŠKA, Petr. EtherChannel, Link Agregation, PAgP, LACP, NIC Teaming. [Online]. 2009, Cisco IOS 21. [Cit: 29. 11. 2021]. Dostupné z: https://bit.ly/3E3Bl5p

Výhody EtherChannelu:[55]

1. Základní výhodou je ta, že pro EtherChannel využíváme porty, které jsou již zakoupené, nebo na ně máme licenci. Není tedy potřeba dokupovat speciální licenci.
2. Samotná konfigurace se provádí na EtherChannelu, to znamená, že se nemusí každý port konfigurovat zvlášť a tím se předejde chybě v překlepu na jednotlivých portech, a to i v případě, že provádíme konfiguraci mezi dvěma switchi.
3. Logický port, který vytvoříme pomocí EtherChannelu dává výhodu toho, že pokud jedna část spojení na jedné straně vypadne, nedojde ke změně topologie sítě a konektivita zůstává, ačkoliv s každým dalším nefunkčním portem klesá propustnost.
4. Mezi stranami agregovaného spojení probíhá „load balancing“[56], který probíhá na každé straně. Podle použitého hardwaru můžeme implementovat několik metod rozložení zátěže. Buď podle zdrojové a cílové MAC adresy nebo IP adresy.

EtherChannel se vždy nasazuje ve fyzických párech. Spojení probíhá 1:1 a z toho důvodu může jeden redundantní spoj komunikovat s druhým, ale ne se třetím. Každý jeden EtherChannel má svůj interface, který se nazývá PortChannel. Konfigurace na PortChannelu ovlivní porty, které jsou k tomuto interface přiřazeni.[57]

Port Aggregation Protocol + Link Aggregation Control Protokol

Port Aggregation Protocol (dále jen PAgP), je Cisco proprietární protokol. To znamená, že ho lze nakonfigurovat pouze na zařízeních od firmy Cisco. V případě konfigurace logického EtherChannelu pomocí PAgP jsou data posílány portem k vyjednávání. Jakmile PAgP vyjedná linku, vytvoří spojení.

---

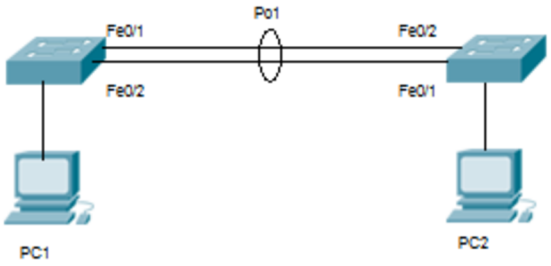
[55] Ibid.
[56] Load balancing v kontextu datových sítí znamená rozložení zátěže. Autor: BROUŠKA, Petr. EtherChannel, Link Agregation, PAgP, LACP, NIC Teaming. [Online]. 2009, Cisco IOS 21. [Cit: 29. 11. 2021]. Dostupné z: https://bit.ly/3E3Bl5p
[57] viz kap. 2, str. 56-58, FROOM, Richard, SIVASUBRAMANIAN, Balaji and FRAHIM, Erum. Implementing Cisco IP switched networks (SWITCH). 1st ed. Indianapolis : Cisco Press, 2010. ISBN 9781587058844.

Link Aggregation Control Protocol (dále jen LACP), je součástí normy pro propojování fyzických portů do logických. To je také důvod, proč LACP podporují i jiní výrobci než jenom firma Cisco.

5.1.3.1 EtherChannel – praktická ukázka

Praktická ukázka bude probíhat mezi dvěma switchi, kde ke každému bude připojen jeden počítač (obrázek č. 17). [58]

- Na SW1 bude nakonfigurovaný EtherChannel mezi porty Fa0/1 a 0/2.
- Na SW1 bude nakonfigurovaný EtherChannel mezi porty Fa0/1 a 0/2.
- PC1 má IP adresu 192.168.1.10, maska je 255.255.255.0.
- PC2 má IP adresu 192.168.1.20, maska je 255.255.255.0.



Obrázek 17 EtherChannel: Schéma zapojení.

Na začátku praktické ukázky nakonfiguruji EtherChannel mezi dvěma switchi. (obrázek č. 18)[59]. Na prvním z nich v módu desirable a na druhém v módu auto. Tím zajistím konektivitu mezi PC1 a PC2. (obrázek č. 19)[60].

```
SW1# show running-config
!
interface FastEthernet0/1
channel-protocol pagp
 channel-group 1 mode desirable
 switchport mode trunk
!
interface FastEthernet0/2
channel-protocol pagp
 channel-group 1 mode desirable
 switchport mode trunk
```

```
SW2# show running-config
!
interface FastEthernet0/1
channel-protocol pagp
 channel-group 1 mode auto
 switchport mode trunk
!
interface FastEthernet0/2
channel-protocol pagp
 channel-group 1 mode auto
 switchport mode trunk
```

Obrázek 18 Výpis z konfigurace SW1 a SW2.

[58] BEDEČ, Jan. EtherChannel: Schéma zapojení. Slaný. [cit. 29. 11. 2021].
[59] BEDEČ, Jan. Výpis z konfigurace SW1 a SW2. Slaný. [cit. 29. 11. 2021].
[60] BEDEČ, Jan. Výpis komunikace mezi PC1 a PC2. Slaný. [cit. 29. 11. 2021].

```
PC1>ping 10.1.1.20

Pinging 10.1.1.20 with 32 bytes of data:

Reply from 10.1.1.20: bytes=32 time=0ms TTL=128
Reply from 10.1.1.20: bytes=32 time=0ms TTL=128
Reply from 10.1.1.20: bytes=32 time=1ms TTL=128
Reply from 10.1.1.20: bytes=32 time=0ms TTL=128
```

```
PC2>ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time=1ms TTL=128
Reply from 10.1.1.10: bytes=32 time=0ms TTL=128
Reply from 10.1.1.10: bytes=32 time=0ms TTL=128
Reply from 10.1.1.10: bytes=32 time=0ms TTL=128
```

Obrázek 19 Výpis komunikace mezi PC1 a PC2.

Změnou na jedné straně PortChannelu bych změnil protokol z PAgP na LACP, a to nám switch nedovolí. Protokoly spolu neumí spolupracovat. Konfigurace LACP protokolu je velice podobná, pouze se musí při konfiguraci switche myslet na to, že mód Auto u PAgP je ekvivalentem Active u LACP a zároveň mód Desirable je ekvivalentem módu Pasive u protokolu LACP.

Ve většině případů se technologie EtherChannelu používá pro propojení sever⇔switch, kde switche z pravidla bývají osazeny 10 GB porty. Význam je především v prevenci ztráty komunikace mezi diskovým polem, na kterém jsou data uložena a serverem, který s daty pracuje.

5.1.4 Spanning Tree Protokol

Pokud je v síti více aktivních spojení, můžou na switchi i mezi nimi vznikat datové smyčky. Tím, že vznikne v síti smyčka, paket se dubluje a tím dokáže zahltit celý switch a znemožnit komunikaci v síti. Takovým situacím lze předejít pomocí Spanning Tree Protokolu, který paketům určí nejkratší cestu k cíli. Data tak doputují tam, kam mají v celku a ve správném pořadí.[61]

Spanning Tree Protokol (dále jen STP), chrání před smyčkami v síti, kde se nachází redundantní spoje. Druhy STP jsou:[62]

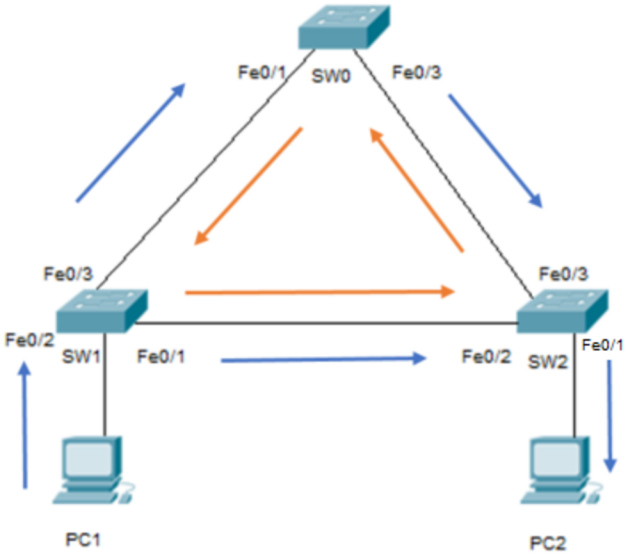
- STP, který využívá pro celou síť pouze jednu úroveň Spanning Tree bez ohledu na to, jaké jsou v síti VLANy.
- Per vlan STP je vylepšená verze klasického STP, kterou má na svědomí firma Cisco. Tento typ poskytuje instanci ke každé VLANě, která se v síti nachází.

[61] viz kap. 3, str. 3, FROOM, Richard, SIVASUBRAMANIAN, Balaji and FRAHIM, Erum. Implementing Cisco IP switched networks (SWITCH). 1st ed. Indianapolis : Cisco Press, 2010. ISBN 9781587058844.
[62] Ibid. str. 4.

- Multiple STP umožňuje propojení více VLAN do jedné instance nebo do vícer instancí, které se v síti nachází.
- Rapid STP má nejrychlejší konvergenční čas.
- Per VLAN Rapid STP+ je nadstavba od firmy Cisco, která reprezentuje výhody předchozích modelů STP.

Vznik smyčky, a tudíž nebezpečí, které představuje, ukážu na příkladu. Použiji k tomu tři switche, na kterých nebude nastavená žádná instance STP a které jsou propojené FastEthernetem mezi sebou. Dva switche budou mít přes ethernetový kabel připojený stolní počítače. Komunikace probíhá tak, že datový rámec přijme packet, který je směřovaný na prozatím neznámé zařízení. Datový rámec přepošle na všechny komunikační porty s výjimkou toho, ze kterého rámec přijal. Do paměti si uloží MAC adresu a data o portu, ze kterého data přijal.[63]

Průběh komunikace probíhá z PC1. (obrázek č. 20)[64]:



Obrázek 20 Spanning Tree Protocol: Všesměrová bouře v síti.

- PC1 pošle na SW1 datový rámec.
- SW1 rámec přijme na portu Fe0/1 a zapíše si MAC adresu do paměťové tabulky.

[63] BROUŠKA, Petr. Spanning Tree Protocol. [Online]. 2007, Cisco IOS 9. [Cit: 30. 11. 2020]. Dostupné z: https://bit.ly/3paRMqp
[64] BEDEČ, Jan. Spanning Tree Protocol: Všesměrová bouře v síti. Slaný. [cit. 30. 11. 2021].

- SW0 přijme datový rámec na Fe0/1 a odešle ho portem Fe0/3. Stejně jako SW1 si zapíše MAC adresu a port ze kterého data přišla.
- SW2 přijme data na Fe0/3 a odešle je na porty Fe0/ a 0/2. Zapíše si MAC adresu a data o příchozím portu do paměti.
- PC2 získává data z PC1, ale switch nemá, jak se dozvědět, že PC2 zprávu obdržel, a navíc dostává zprávu ze SW1 přes jeho port Fe01/ na port Fe0/2.
- Tím že tyto data od SW1 přijal, přepsal si již zapsaná data ve své paměti a odešle je portem Fe0/3 na SW0, zároveň také portem Fe0/1 na PC2. PC2 datový rámec znovu nepřijme, a tak ho zahazuje.
- SW0 datový rámec přijme, přepíše tabulku a pokračuje v odesílání.

Tímto způsobem se proces neustále opakuje a v případě více aktivních prvků se i data více množí.

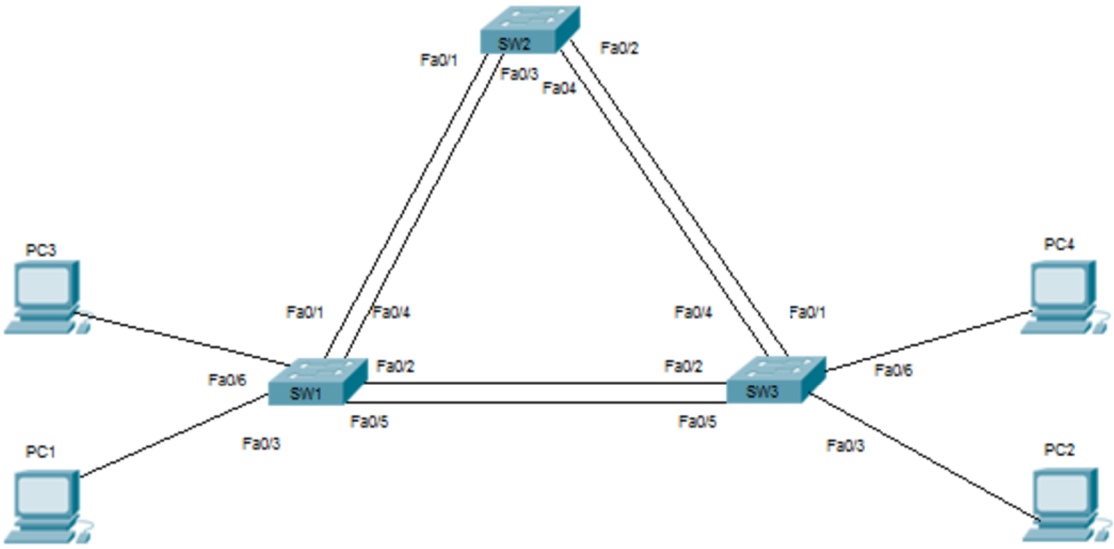
5.1.4.1 Spanning Tree Protocol – praktická ukázka

Praktická ukázka bude v konfiguraci STP ve verzi PVST (obrázek č. 21)[65].

Prvky použité v praktické ukázce + schéma:

- **PC1:** IP 192.168.1.10/24.
- **PC2:** IP 192.168.1.20/24.
- **PC3:** IP 192.168.2.10/24.
- **PC4:** IP 192.168.2.20/24
- **SW1, SW2, SW3:** VLAN10, 20.

[65] BEDEČ, Jan. Spanning Tree Protocol: Topologie zapojení PVST. Slaný. [cit. 30. 11. 2021].



Obrázek 21 Spanning Tree Protocol: Topologie zapojení PVST.

Postup konfigurace

V první fázi mezi sebou propojím switche do VLAN. Pro každou VLANu vytvořím samostatný okruh.

- **VLAN10** obsahuje porty **Fe0/1, 0/2 a 0/3** na **SW1** a **SW3**. Na **SW2** nastavím VLANu na porty **Fe0/1 a 0/2**.
- **VLAN20** obsahuje porty **Fe0/4, 0/5 a 0/9** na **SW1** a **SW3**. Na **SW2** nastavím VLANu na porty **Fe0/3 a 0/4**.

Pomocí příkazu „Show vlan“, ověřím, zda jsou správné porty ve správných VLANách (obrázek č. 22)[66].

[66] BEDEČ, Jan. Výpis VLAN na switchi 1,2 a 3. Slaný. [cit. 30. 11. 2021].

```
SW1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   VLAN10                            active    Fa0/1, Fa0/2, Fa0/3
20   VLAN20                            active    Fa0/4, Fa0/5, Fa0/6
```

```
SW2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN10                            active    Fa0/1, Fa0/2
20   VLAN20                            active    Fa0/3, Fa0/4
```

```
SW3#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   VLAN10                            active    Fa0/1, Fa0/2, Fa0/3
20   VLAN20                            active    Fa0/4, Fa0/5, Fa0/6
```

Obrázek 22 Výpis VLAN na switchi 1,2 a 3.

Automatická konfigurace STP nastaví na nenakonfigurovaných switchích PVST mód. Je tedy dobré nastavit STP cíleně a nenechat automatiku, aby si nastavovala STP podle okolních switchů, a to z důvodu toho, že porty v základní konfiguraci spolu komunikují skrz VLAN1. Pokud připojíme třetí a následně další aktivní prvek, STP přepočítá cesty a bude se v síti určovat novou topologii. Doba přepočítání u Per Vlan SPT probíhá v řádově během jedné minuty. Pokud jsou switche nakonfigurované dle požadavku správně, zapsaly si novou topologii do paměti a nedojde tak k všesměrovým bouřím.[67]

Ve vytvořeném síťovém prostředí je switch s nejnižší prioritou označen jako „root bridge“. Rootovský switch je vztažen vždy k některé z propagovaných VLAN. Následně switch určí porty, které jsou ve stavu designated anebo ve stavu forward. Takové porty odesílají a přijímají data skrze danou VLANu. V této topologii se stal SW3 root bridgem pro VLAN10 (obrázek č. 23)[68].

[67] BROUŠKA, Petr. Spanning Tree Protocol. [Online]. 2007, Cisco IOS 9. [Cit: 30. 11. 2020]. Dostupné z: https://bit.ly/3paRMqp
[68] BEDEČ, Jan. SW3 – STP konfigurace u VLAN10. Slaný. [cit. 30. 11. 2021].

```
SW3#Show spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    12298
             Address     0002.1655.CCC6
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    20490  (priority 20480 sys-id-ext 10)
             Address     0002.1655.CCC6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Obrázek 23 SW3 – STP konfigurace u VLAN10.

Na třetím switchi jsou porty 1, 2 a 3 ve stavu Desg FWD. To znamená, že SW3 je root bridgem pro VLAN10.

Ověření root bridge pro SW1 na VLAN20. (obrázek č. 24)[69].

```
SW1#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0001.646E.EE9C
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0001.646E.EE9C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

Obrázek 24 SW1 – STP konfigurace u VLAN20.

Na třetím switchi jsou stejně jako na prvním switchi porty nastavené ve stavu Desg FWD. Každý switch může mít prioritu nastavenou manuálně. Takto se dá nastavit, který switch se má stát root bridge. Čím nižší je priorita, tím pravděpodobněji se switch stane root bridge.

Tímto způsobem lze nastavit SW 2 (obrázek č. 25)[70] jako root bridge nebo jako následující, pokud by primární switch nefungoval.

[69] BEDEČ, Jan. Ověření konfigurace STP pro VLAN20 na SW1. Slaný. [cit. 30. 11. 2021].
[70] BEDEČ, Jan. Možnosti manuálního nastavení priority switche pro STP. Slaný. [cit. 30. 11. 2021].

```
SW2(config)#spanning-tree vlan 10 priority 1
SW2(config)#spanning-tree vlan 10 root primary
SW2(config)#spanning-tree vlan 10 root secondary
```

Obrázek 25 Možnosti manuálního nastavení priority switche pro STP.

V této praktické ukázce není pro VLAN10 ani VLAN20 root bridge SW2. Tento switch je k SW1 a SW3 připojen vždy dvěma porty. Na jedné straně patří do VLAN10 a na straně druhé je přiřazen k VLAN20.

Z obrázků (obrázek č. 26 a 27)[71] je patrné, že pro VLAN10 má Fa0/2 pozici root bridge a porty ve stavu FWD. Port Fa0/2 je root bridge pro ostatní prvky ve VLAN10 a port F0/1 je pouze odkazování na další prvek v síťové topologii.

```
SW2#show spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    12298
             Address     0002.1655.CCC6
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    16394  (priority 16384 sys-id-ext 10)
             Address     00D0.BAE6.1AA9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

Obrázek 26 SW2 – STP VLAN20.

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0001.646E.EE9C
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     00D0.BAE6.1AA9
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/3            Root FWD 19        128.3    P2p
```

Obrázek 27 SW2 – STP VLAN10.

Port Fa0/3 je root bridge a Fa0/4 je pro komunikaci ve VLAN 20 zablokovaný. Pro VLAN20 je tedy root bridge za portem Fa0/3. Z výpisu konfigurace je patrné, který switch je root bridge pro VLAN10 a VLAN20. Mezi SW1, SW2 a SW3 existuje vždy jenom jediná cesta k PC.

[71] BEDEČ, Jan. SW2 – STP VLAN10 a 20. Slaný. [cit. 30. 11. 2021].

Z důvodu použití pouze dvou VLAN, se vyplatilo nechat klasický Per Vlan STP protokol. Při síťové topologii, která by obsahovala více VLAN, by bylo vhodnější konfigurovat Multiple STP.

5.2 Routery

Druhý, nejčastěji se vyskytující aktivní prvek, který dokáže propojit sítě je zařízení, kterému se říká router. Toto zařízení přijme datový rámec, ze kterého odstraní obsah hlavičky a vloží do ní informace o tom, které zařízení má tento datový rámec obdržet. Nejčastěji se mění IP adresa, která je v hlavičce obsažena, protože všechny dostupné IP adresy v síti jsou uložené v routovací tabulce, která směruje provoz díky nastavenému routovacímu protokolu.[72]

Správně nastavený routovací protokol zajistí bezproblémovou komunikaci mezi sítěmi, to se mimo jiné hodí i v případě privátního cloudového úložiště, které je geograficky vzdálené. Bez správně nastaveného směrování se k datům firemní pracovník nedostane.

Směrovací (routovací) protokoly jsou převážně procesy, algoritmy a data, sloužící k výměně informací, které se následně plní do směrovací tabulky. Tím může router rozhodnout o nejvýhodnější cestě. Ne vždy je totiž nejkratší cesta tou nejrychlejší.[73] Předávání těchto pravidel směrování probíhá dynamicky mezi routery. To znamená, že jakákoliv změna na prvku způsobí změnu ve směrovací tabulce. Router pak o této změně informuje okolní zařízení, které provedou vlastní aktualizaci směrovací tabulky. Cílem každého směrovacího protokolu je učit se o vzdálených sítích a přizpůsobit se tak nové topologii.[74]

Pro praktické příklady routovacích protokolů jsem zvolil jeden proprietární protokol a jeden, který lze konfigurovat napříč výrobci směrovacích zařízení.

---

[72] BROUŠKA, Petr. Router Switching metody a související termíny – CAM, FIB, CEF. [Online]. 2009, Cisco. [Cit: 1. 12. 2021]. Dostupné z: https://bit.ly/2ZMp6vc
[73] Ibid.
[74] viz. kap. 4, str. 23, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 2 (ICND2) foundation learning guide. 2th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 97324501.

5.2.1 Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (dále jen EIGRP) je jedním z proprietárních protokolů od firmy Cisco. Jak jsem psal výše, proprietární protokoly podporují pouze zařízení daného výrobce. EIGRP pro komunikaci využívá „Hello“ pakety, které slouží k nalezení a komunikaci s dalšími směrovači. Hello pakety se posílají opakovaně. Rychlost opakování je závislá na propustnosti linek.

5.2.1.1 EIGRP – praktická ukázka

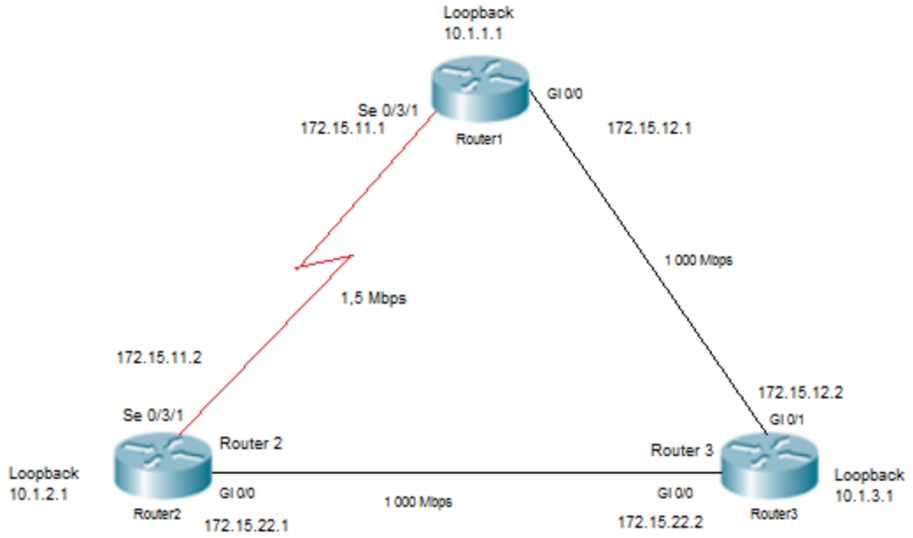
EIGRP je složité na počítání metriky. Z toho důvodu využiji jednoduchou topologii, která se liší propustností linek (obrázek č. 28) [75].

Nastavení IP rozsahů (tabulka č.1.)[76]:

	PORT	IP	NETMASK
Router 1	Se 0/3/1	173.20.11.1	255.255.255.0
	GI 0/0	173.20.12.1	255.255.255.0
	Lo1	10.0.1.1	255.255.0.0
Router 2	Se 0/3/1	173.20.11.2	255.255.255.0
	GI 0/0	173.20.22.1	255.255.255.0
	Lo1	10.0.2.1	255.255.0.0
Router 3	GI 0/0	173.20.22.2	255.255.255.0
	GI 0/1	173.20.15.2	255.255.255.0
	Lo1	10.0.3.1	255.255.0.0

Tabulka 1 Nastavení IP R1, R2 a R3.

[75] BEDEČ, Jan. EIGRP: Schéma zapojení pro praktickou ukázku EIGRP. Slaný. [cit. 01. 12. 2021].
[76] BEDEČ, Jan. Nastavení IP R1, R2 a R3. Slaný. [cit. 01. 12. 2021].



Obrázek 28 EIGRP: Schéma zapojení pro praktickou ukázku EIGRP.

Postup konfigurace

Porty routerů nastavím podle zadání (obrázek č. 29, 30, 31)[77]. Pro lepší názornost jsem router 1 a 2 propojil tak, aby kabel simuloval sériovou linkou, která se dnes již nevyužívá. Nevýhoda sériových linek je v jejich propustnosti, která je na současné poměry velice malá. Pro účely praktické ukázky bude sériová linka vyhovující.

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     173.20.12.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            unassigned      YES unset  administratively down down
Serial0/3/1            173.20.11.1     YES manual up                    up
Loopback1              10.0.1.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down

```

Obrázek 29 Výpis R1 interface.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     173.20.22.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            unassigned      YES unset  administratively down down
Serial0/3/1            173.20.11.2     YES manual up                    up
Loopback1              10.0.2.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Obrázek 30 Výpis R2 interface.

[77] BEDEČ, Jan. Výpis R1, R2, R3 interface. Slaný. [cit. 01. 12. 2021].

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     173.20.22.2     YES manual up                    up
GigabitEthernet0/1     173.20.12.2     YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            unassigned      YES unset  administratively down down
Serial0/3/1            unassigned      YES unset  administratively down down
Loopback1              10.0.3.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Obrázek 31 Výpis R3 interface.

Po nastavení příslušných adres na interface routerů spolu zařízení komunikují (obrázek č. 32, 33, 34)[78]. Nicméně nemají nastavený protokol, který určí nejefektivnější cestu. Z toho důvodu nastavím na každém routeru EIGRP instanci pro vytvořené sítě. Metrika EIGRP se počítá v závislosti na propustnosti linek a jejich zpoždění.[79] Z toho důvody jsem dva routery propojil sériovou linkou. Pokud bude mít router lepší cestu, vždy se vyhne méně efektivní trase. To vše řídí metrika EIGRP.

```
R1#show running-config | begin router
router eigrp 100
 network 10.0.0.0 0.0.255.255
 network 173.20.11.0 0.0.0.255
 network 173.20.12.0 0.0.0.255
```

Obrázek 32 Výpis z routeru 1. Konfigurace EIGRP.

```
R2#show running-config | begin router
router eigrp 100
 network 173.20.11.0 0.0.0.255
 network 173.20.22.0 0.0.0.255
 network 10.0.0.0 0.0.255.255
```

Obrázek 33 Výpis z routeru 2. Konfigurace EIGRP.

```
R2#show running-config | begin router
router eigrp 100
 network 173.20.22.0 0.0.0.255
 network 173.20.12.0 0.0.0.255
 network 10.0.0.0 0.0.255.255
```

Obrázek 34 Výpis z routeru 3. Konfigurace EIGRP.

[78] BEDEČ. Jan. Výpis konfigurace R1, R2, R3. Slaný. [cit. 01. 12. 2021].
[79] viz kap. 4, str. 58-59, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 2 (ICND2) foundation learning guide. 2th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 97324501.

Routovací protokoly používají inverzní masky, které mají přesně opačné značení od klasické síťové masky.[80]

Z výpisu (obrázek č. 35)[81] je patrné, jaká cesta bude zvolena k jednotlivým sítím, do kterých router R1 vidí. Značení FD označuje nejlepší metriku pro danou síť. Tato metrika platí, dokud se v síti něco nezmění. Pokud je hodnota za lomítkem v závorce menší než FD, považuje se cesta za primární. V opačném případě slouží jako záložní cesta v případě ztráty primárního spojení. To je konkrétní příklad sériové linky, která má větší metriku než nejkratší nalezená cesta.

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 128256
         via Summary (128256/0), Null0
P 10.0.0.0/16, 1 successors, FD is 128256
         via Connected, Loopback1
P 173.20.0.0/16, 1 successors, FD is 2816
         via Summary (2816/0), Null0
P 173.20.11.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/3/1
P 173.20.12.0/24, 1 successors, FD is 2816
         via Connected, GigabitEthernet0/0
P 173.20.22.0/24, 1 successors, FD is 3072
         via 173.20.12.2 (3072/2816), GigabitEthernet0/0
         via 173.20.11.2 (2170112/2816), Serial0/3/1
```

Obrázek 35 Topologie EIGRP na routeru 1.

Nevýhody EIGRP jsou v první řadě omezenost na produkty firmy Cisco, problémové párování na ostatní komunikační protokoly a oproti konkurenci složitá konfigurace.

5.2.2 Open Shortest Path First

Oproti EIGRP není Open Shortest Path First (dále jen OSPF), proprietární protokol, to znamená, že může být nasazen na zařízení od různých výrobců. Samozřejmě, zařízení musí být s tímto protokolem kompatibilní. OSPF protokol funguje na principu stromové struktury. Nejprve vytvoří topologii prvků v síti, zařadí

[80] viz kap. 2, str. 124, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.
[81] BEDEČ, Jan. Topologie EIGRP na routeru 1. Slaný. [cit. 01. 12. 2021].

je do stromové struktury a poté si do směrovací tabulky zapíše cesty k jednotlivým prvkům.[82]

Principem fungování jsou oblasti. Oblasti zkracují dobu konvergence. Oproti EIGRP je ale konfigurace poněkud složitější. Mezi jednotlivými oblastmi musí být ASBR[83] routery.[84]

5.2.2.1 OSPF – praktická ukázka

V praktické ukázce propojím dvě oblasti. Ukážu postup konfigurace oblastí OSPF a základní troubleshooting.

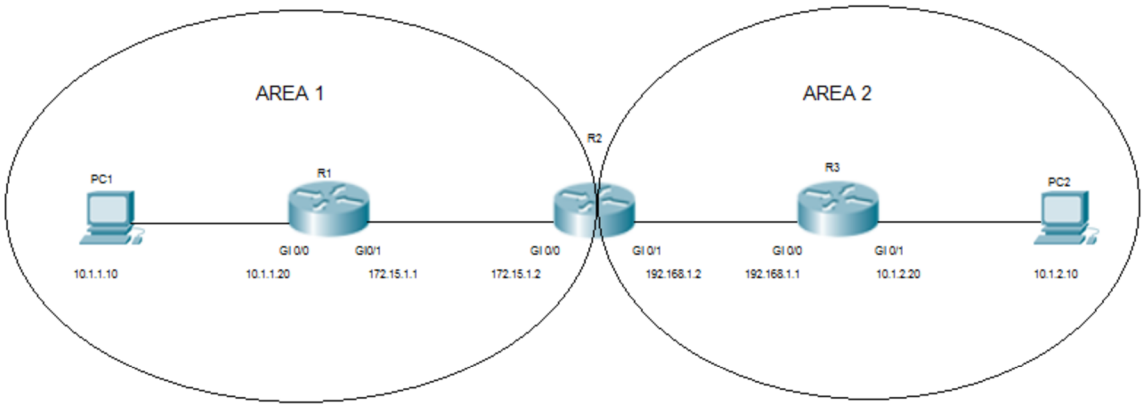
Zařízení:

- **PC1**
  - IP 10.10.1.10/24
- **PC2**
  - IP 10.10.2.10/24
- **R1**
  - Gi 0/0 s IP 10.10.1.20/24
  - Gi 0/1 s IP 173.150.1.1/24
  - Router-id 1.1.1.1
- **R2**
  - Gi 0/0 s IP 173.150.1.2/24
  - Gi 0/0 s IP 10.90.1.2/24
  - Router-id 2.2.2.2
- **R3**
  - Gi 0/0 s IP 10.90.1.1/24
  - Gi 0/0 s IP 10.10.2.20/24
  - Router-id 3.3.3.3

Schéma zapojení (obrázek č. 36) [85]:

[82] viz str. 446, LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 9788025123591.
[83] Hraniční routery „Autonomous Systém Boundary Router“
[84] viz str. 448, LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010, ISBN 9788025123591.

[85] BEDEČ, Jan. OSPF: Schéma zapojeni. Slaný. [cit. 01. 12. 2021].



Obrázek 36 OSPF: Schéma zapojeni.

Konfigurace:

Na každém routeru je nutné nejprve aktivovat protokol, se kterým chceme pracovat. Po zapnutí funkce protokolu OSPF je potřeba nastavit sítě, které na router doléhají a přidělit jim oblast tzv. areu. Jsou-li nastavené sítě přiřazené k oblastem, zbývá nastavit ID routeru.

ID má podobu IP adresy (obrázek č. 37, 38, 39)[86].

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#log-adjacency-changes
R1(config-router)#network 10.10.1.0 0.0.0.255 area 1
R1(config-router)#network 173.150.1.0 0.0.0.255 area 1
```

Obrázek 37 Výpis konfigurace OSPF na routeru R1.

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)# log-adjacency-changes
R2(config-router)#network 173.150.1.0 0.0.0.255 area 1
R2(config-router)#network 10.90.1.0 0.0.0.255 area 2
```

Obrázek 38 Výpis konfigurace OSPF na routeru R2.

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#log-adjacency-changes
R3(config-router)#network 10.90.1.0 0.0.0.255 area 2
R3(config-router)#network 10.10.2.0 0.0.0.255 area 2
```

Obrázek 39 Výpis konfigurace OSPF na routeru R3.

[86] BEDEČ, Jan. Výpis konfigurace OSPF na routeru R1, R2, R3. Slaný. [cit. 01. 12. 2021].

Routery mají povolený protokol OSPF a nastaveny sítě. V tuto chvíli tedy každý router v síti vidí svého souseda. Výsledek se dá ověřit pomocí příkazu „*Show ip ospf neighbor*“[87] (obrázek č. 40, 41, 42)[88].

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:34    173.150.1.2     GigabitEthernet0/1
```

Obrázek 40 Výpis sousedících routerů s routerem R1.

Na výpisu z konfigurace R1 je patrné, že jediným sousedem router R1 je router R2, který má ID 2.2.2.2 a k sousednímu routeru je připojen pomocí GgabitEthernetu0/1. Označení „*FULL/DR*“[89] značí, že pro oblast 1 je tento router hlavní.

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DR         00:00:32    173.150.1.1     GigabitEthernet0/0
3.3.3.3           1   FULL/BDR        00:00:37    10.90.1.1       GigabitEthernet0/1
```

Obrázek 41 Výpis sousedících routerů s routerem R2.

Hraničním routerem je router R2. To je důvod, proč vidí do oblasti 1 a oblasti 2. Vidí tedy routery R2 a R3 (obrázek č. 42)[90].

```
R3#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:38    10.90.1.2       GigabitEthernet0/0
R3#
```

Obrázek 42 Výpis sousedících routerů s routerem R3.

Za svou praxi jsem se nesetkal s firmou, která by měla nasazený protokol EIGRP. Malé a střední podniky si většinou nemohou dovolit mít síť poskládanou pouze z prvků firmy Cisco. OSPF je proto schůdná, ačkoliv na konfiguraci náročnější varianta neproprietárního routovacího protokolu. Nevýhodou se jeví fakt, že routery, které jsou zařazené do OSPF routingu musí znát topologii celé sítě.

---

[87] viz kap. 4, str. 77, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 2 (ICND2) foundation learning guide. 2th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 97324501.
[88] BEDEČ, Jan. Výpis sousedících routerů s routerem R1, R2, R3. 2021.
[89] viz kap. 4, str. 77, SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 2 (ICND2) foundation learning guide. 2th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 97324501.
[90] BEDEČ, Jan. Výpis sousedících routerů s routerem R3. Slaný 2021.

6. Softwarová bezpečnost

Každá organizace, která chce navenek i prostřednictvím internetu jednat vlastním jménem, musí mít i svou vlastní doménu. Tím je ve skutečnosti myšleno doménové jméno, které je součástí například i e-mailové adresy. Hlavní funkcí je nahrazení IP adresy jménem, které se pamatuje lépe než změť čísel, které tvoří odkaz.[91]

Základním softwarem, kterým je spravována doména organizace je Active Directory, které slouží ke správě jak jednotlivých stanic, uživatelů a skupin tak tisícovky objektů, které se řídí doménovou politikou. Zásady se v prostředí domény tvoří pomocí nástroje, který se jmenuje Group Policy. Tento nástroj je součástí řešení Active Directory.

6.1 Active Directory

Služba Active Directory umožňuje správcům efektivně spravovat celopodnikové informace z centrálního úložiště, které lze globálně distribuovat. Jakmile jsou informace o uživatelích, skupinách, počítačích, tiskárnách, aplikacích a službách přidány do služby Active Directory, lze je zpřístupnit napříč celým podnikem pro všechny nebo jen vybrané uživatele. Organizační struktura může odpovídat struktuře organizace. Uživatelé se mohou v prostředí domény dotazovat na umístění tiskárny nebo na e-mailovou adresu kolegy. Správa může být delegována na jednotlivý objekt i na celou doménu.[92] Tím je zajištěna víceúrovňová bezpečnost.

Active Directory je základní bezpečnostní komponenta v síti. Jedním z klíčových bezpečnostních protokolů je Kerberos, který je bezpečný a flexibilní ověřovací protokol.

[91] Co to je doména?. Domény.cz. Domény – dostupnost, převod, ceník. Domény.cz [online]. Copyright © 2021 ACTIVE 24, s.r.o. [cit. 22.12.2021]. Dostupné z: https://domeny.cz/jak-na-to/co-to-je-domena-7/

[92] viz str. 1, DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, c2013. ISBN 1449320023.

6.1.1 Kerberos

Jedním ze základních pilířů každé sítě, která je postavena na Active Directory, je bezpečnostní protokol Kerberos. Kerberos poskytuje mechanismus ověřování, který umožňuje přihlašování uživatelů, přístup k aplikacím a komunikaci mezi řadiči domény (mimo jiné). K zahájení používání Kerberos není potřeba prakticky žádná konfigurace. Ve skutečnosti, pokud si aplikace nežádá speciální konfiguraci, tak se Kerberos nakonfiguruje poměrně snadno.[93]

Hlavní výhodou bezpečnostního protokolu Kerberos je schopnost uživatele bezpečně prokázat svou identitu a poté dosáhnout jednotného přihlášení k jiným službám. Ve skutečnosti s Kerberosem hesla nikdy neprocházejí sítí v prostém textu nebo v zašifrovaném formátu. Místo toho jsou generovány klíče specifické pro danou relaci.[94]

6.1.1.1 Přihlášení uživatele

První věc, kterou uživatel provede poté co zasedne k pracovnímu stolu a zapne počítač je přihlášení do firemní sítě. Proces přihlášení má na starost Kerberos.

Základní výhodou protokolu Kerberos je jednotné přihlášení. Proces přihlášení probíhá v následujících krocích:[95]

1) Získání tiketu pro udělování tiketů (TGT).[96]
2) Po přihlášení uživatele si systém uloží tiket do mezipaměti.
3) Pokud je vyžadováno ověření k doménové službě, tiket uložený v mezipaměti se použije k získání tiketu chtěné služby bez nutnosti opětovného zadávání přihlašovacích údajů.

Prvním krokem autentizace je předložení požadavku na předběžné ověřování v paketu AS_REQ (žádost o autentizační službu). AS_REQ (obrázek

[93] Ibid. str. 261.
[94] Ibid. str. 261-262.
[95] viz str. 262, DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, c2013. ISBN 1449320023.
[96] TGT = Ticket Granting Ticket

č. 43)[97] obsahuje podrobnosti nezbytné k prokázání uživatele, že je tím, za koho se vydává. Tyto podrobnosti jsou:[98]

1) Jméno klienta, kterým se rozumí přihlašovací jméno.
2) Název služby, která je přiřazena k doméně.
3) Časové razítko klienta, kterým se rozumí aktuální čas, zašifrovaný heslem uživatele. Řadič domény pak dešifruje takové pole hodnotou, kterou má uloženou v databázi Active Directory. Časové razítko je poté zkontrolováno, aby bylo zajištěno zabezpečení proti útokům na opakované přehrávání časového razítka.

Obrázek 43 Požadavek na ověření služby.

Protokol Kerberos pomáhá ověřit identitu služby napříč celou sítí. Operační systémy nejnovější verze operačního systému Windows Server implementují ověřovací protokol Kerberos ve verzi 5 a rozšíření pro ověřování pomocí veřejného klíče, přenosu autorizačních dat a delegování.

6.1.2 Group Policy

Active Directory Group Policy je technologie, která firemním správcům umožňuje provádět změny na zařízeních bez nutnosti fyzického zásahu.

[97] BEDEČ, Jan. Požadavek na ověření služby. Slaný. [cit. 22. 12. 2021].
[98] viz str. 262, DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, c2013. ISBN 1449320023.

Technologie Group Policy pomáhá centrálně spravovat konfigurace uživatelů, počítačů a serverů.

Podnik může nasazením skupiny zásad:

- Vynutit bezpečné heslo (délku, speciální znaky apod.) a zásady účtu.
- Zajistit přístup k síťovým zdrojům.
- Zabezpečit síťovou a bezdrátovou komunikaci.
- Dodržovat vládní a průmyslová nařízení a mnoho dalších.

Firmy využívají tuto technologii, ale vědí, že provádění změn v objektech, které jsou v rámci sítě živé, může být riskantní a může mít nezamýšlené a nákladné důsledky. Použití Group Policy (dále jen GPO), může pomoci zabezpečit a sjednotit podnikové operace. GPO mohou pomoci splnit cíle dodržování předpisů, vyžadující dokumentaci přístupů, které ovlivňují zabezpečení sítě nebo přístup k citlivým souborům, jako jsou finanční nebo personální údaje.[99]

Zásady skupiny jsou velmi jednoduché na pochopení, ale jejich použití může být poměrně složité. Každý objekt GPO se může skládat ze dvou částí. První, která se vztahuje na počítač (např. spouštění skriptů nebo změna systémové části registru) a druhá část, která se vztahuje na uživatele (například odhlašovací skript nebo změna uživatelské části registru). GPO Může používat zásady pro uživatele, počítače nebo kombinaci obou.[100]

Jakýkoli objekt GPO je zpočátku vytvořen jako samostatný objekt ve službě Active Directory. Objekt lze poté jednou nebo vícekrát propojit se třemi různými typy umístění: weby, domény a organizačními jednotkami. Primárním nástrojem, který se používá pro práci s GPO, je konzole pro správu zásad skupiny (obrázek č. 44)[101], která poskytuje rozhraní pro zobrazení a úpravu zásad a pochopení, kde jsou zásady v organizaci uplatňovány.[102]

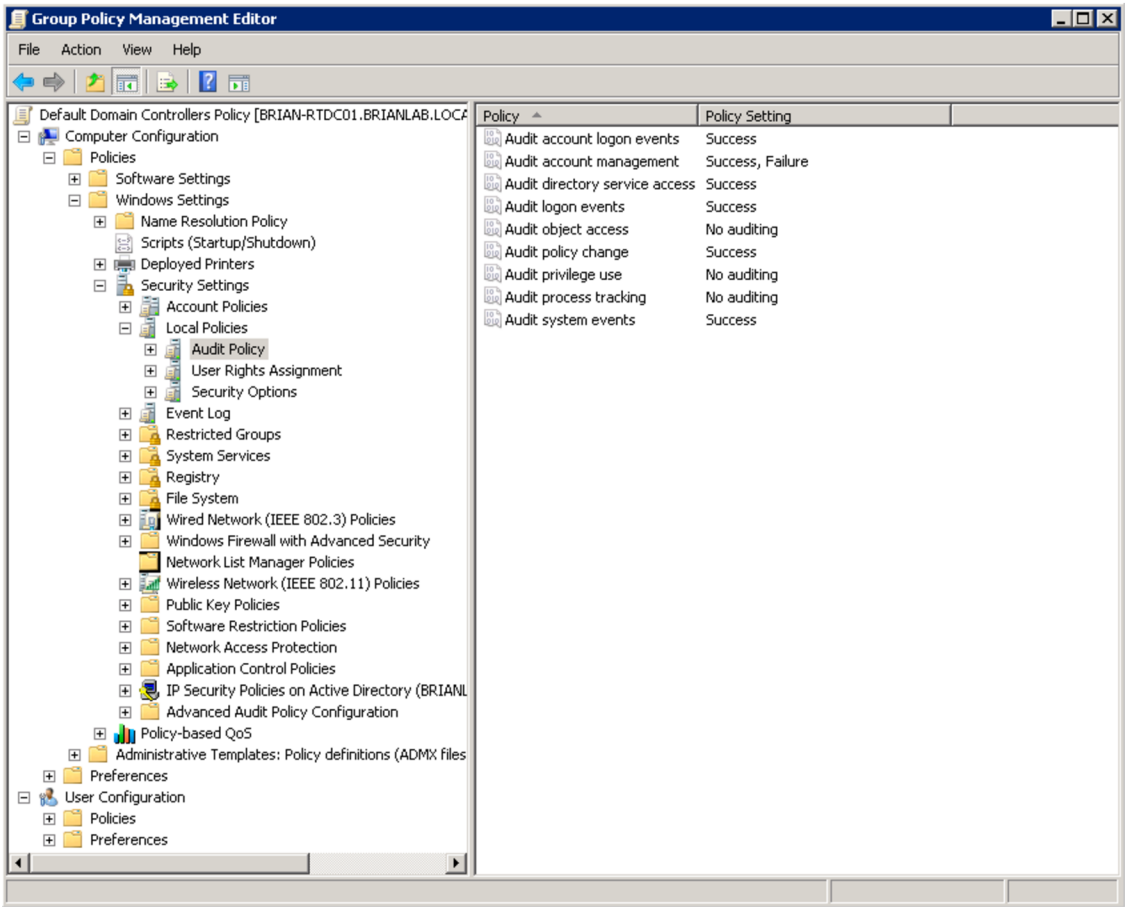
---

[99] viz str. 15, NETIQ CORPORATION. Group Policy Administrator™: User Guide [pdf]. online, 2019. [cit. 23. 12.2021]. Dostupné z: https://www.netiq.com/documentation/group-policy-administrator-67/pdfdoc/grouppolicyadministratoruserguide/grouppolicyadministratoruserguide.pdf

[100] viz str. 289, DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 1449320023.

[101] Ibid. str. 312.

[102] viz str. 308, DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 1449320023.



Obrázek 44 Group Policy Management Console.

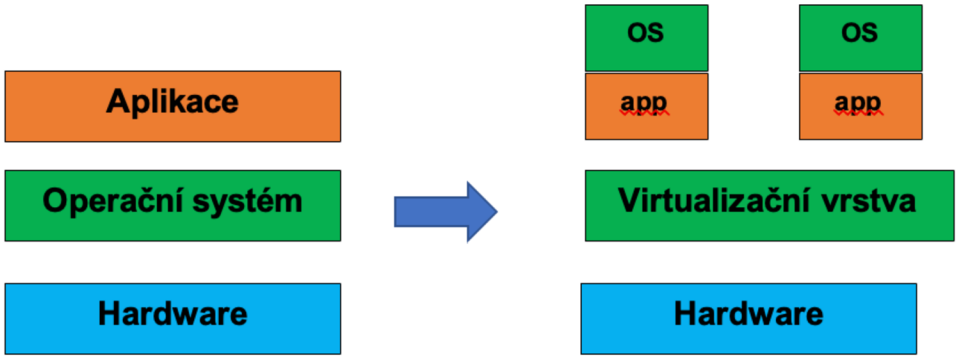
Group Policy je efektivní nástroj, kterým za předpokladu správné konfigurace může administrátor zajistit jednotné prostředí, které se snadno spravuje a není náchylné na zásahy samotných uživatelů. Přes GPO se dají snadno instalovat i aplikace, které se po připojení firemního prostředí automaticky nainstalují a tím opět šetří čas jak zaměstnanci, který může během pár minut začít pracovat, tak administrátorovi, který nemusí nad instalací jednoho PC trávit hodiny.

6.1.3 Hyper-V virtualizace

Mezi trendy v oblasti hardwarové bezpečnosti patří bezesporu virtualizace prostředí. Existuje několik společností, které se zabývají hardwarovou virtualizací. Mezi nejznámější patří Hyper-V od firmy Microsoft nebo VMware, který je dceřinou společností firmy Dell. V neposlední řadě XEN od firmy Citrix.

Hyper-V je role, která je k dispozici v systému Windows Server od verze 2008 a slouží k virtualizaci hardwaru. Virtualizace hardwaru umožňuje rozdělit kapacitu hardwaru jednoho fyzického serveru a přidělit ji více virtuálním strojům. Každý

virtuální stroj má operační systém, který běží nezávisle na hostiteli Hyper-V a dalších virtuálních strojích (obrázek č. 45)[103]. Při instalaci Hyper-V se do zaváděcího procesu vloží softwarová vrstva známá jako hypervizor. Hypervizor je zodpovědný za řízení přístupu k fyzickému hardwaru. Ovladače hardwaru se instalují pouze do hostitelského operačního systému. Všechny virtuální stroje komunikují pouze s virtualizovaným hardwarem.[104]



Obrázek 45 Tradiční architektura hardware oproti virtualizační technologii.

V nedávné historii bylo běžné, že pro jednu aplikaci byl připraven jeden nebo více serverů. To je nákladné na správu zařízení, místo, i finanční prostředky. Každý z těchto serverů vykazoval riziko poškození komponenty, která posléze zapříčiní ztrátu dat nebo odstavení aplikace či služby od užívání. Virtualizační technologie mají za úkol tyto druhy problémů eliminovat. Hypervizory rozdělují zátěž na jednotlivé fyzické servery tak, aby v případě výpadku jednoho fyzického serveru běžely virtuální stroje bez výpadku na ostatních hypervizorech, které spolu sdílejí virtualizační službu.

[103] BEDEČ, Jan. Tradiční architektura hardware oproti virtualizační technologii. Slaný. [cit. 22. 12. 2021].
[104] viz str. 13, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

Servery, které spolu úzce komunikují a jsou schopny mezi sebou migrovat virtuální stroje jsou ve spojení, kterému se říká cluster.[105] Díky tomuto spojení můžou virtuální stroje migrovat jak za pomoci administrátora, tak automaticky pokud dojde k výpadku některé části clusteru.

[105] viz str. 68, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

7. Případová studie – nasazení Hyper-V

7.1 Cíle a požadavky

Cílem této případové studie je nasazení Hyper-V virtualizace a možné varianty konfigurace ve firemním prostředí. Na konkrétních příkladech ukážu postup nasazení řešení. Nejprve nakonfiguruji servery a poté provedu nasazení role Hyper-V Failover Cluster.

Možností, jak nastavit virtualizaci je mnoho. Vždy záleží na konkrétní prostředí a dostupných zdrojů. Nicméně, jsou doporučené postupy, kterých se budu držet.

Předpokladem je, že jsou ve firemním prostředí nasazené a nakonfigurované síťové prvky, diskové pole, doménové prostředí. Firma je tedy plně připravena pro integraci Hyper-V.

Požadavky pro nasazení Hyper-V:

1) Diskové pole o dostatečné kapacitě.
2) Fiber Channel[106] switch pro propojení diskového pole a serverů pomocí optických kabelů.
3) Dva servery, které obsahují:
    a. Nainstalovaný operační systém ve verzi Datacenter.
    b. Připojení k firemní doméně.
    c. Propoj mezi síťovými prvky, diskovým polem a servery.

Licence Windows server se z pravidla prodávají ve verzi Standard, kde je zákazník omezen provozováním pouze dvou virtuálních strojů a každý z nich může mít přiřazené pouze dvě jádra. Windows server ve verzi Datacenter může provozovat neomezené množství virtuálních serverů. To ve výsledku znamená, že stačí koupit jedinou Datacenter licenci a můžu provozovat na jednom fyzickém serveru neomezené množství virtuálních serverů, na které nemusím kupovat licenci a omezené jsou pouze výkonem nodů[107] a velikostí diskového prostoru.[108]

---

[106] Fiber Channel je vysoce výkonná technologie, která pomocí optických vláken dokáže propojit servery, disková pole a mnoho dalších. Pozn. autora.
[107] NODY jsou servery, na kterých běží role Hyper-V Failover Claster. Pozn. autora.
[108] viz str. 246, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

7.2 Konfigurace serverů Hyper-V

Instalace a nastavení rolí je pro servery Hyper-V, kterým se říká „nody“ totožná, kromě přidělovaní IP adres.

Potřebné role, které je potřeba doinstalovat na čistě nainstalovaný Microsoft Windows server se instalují přes aplikaci Server Manager. Vše je samozřejmě možné nastavovat pomocí příkazového řádku, ale grafická nadstavba je pohodlnější.

Potřebné role a služby jsou:

File and Storage services

Obsahují funkce, díky kterým se spravují připojená úložiště. Navíc dovoluje uživatelům získat přístup k souborům na severu i sdílených discích.

Hyper-V

Role dovoluje řídit a vytvářet virtuální servery a organizovat zdroje. Dovoluje tak vytvářet velké množství instancí s rozdílnými typy operačních systémů, které jsou od sebe logicky oddělené.

Failover Clustering

Dovoluje více serverům pracovat spolu pro řízení vysoké dostupnosti provozovaných rolí. Využívá se pro práci se soubory, virtuálními stroji, databázemi a mailovými aplikacemi.

MPIO

Povoluje využívání souborových služeb výrobců třetích stran a umožňuje vícecestné propojení na diskových polích a serverech.

Toto je minimální výčet rolí, které jsou potřeba pro plnohodnotné využívání virtualizačního prostředí.

7.2.1 Síťové prostředí

Pro vlastní konfiguraci role Hyper-V je zapotřebí přiřadit jednotlivým síťovým interfacům jejich funkce. Minimálně musí být jeden interface pro management serverů. Management by se měl provádět z vnitřní intranetové sítě za použití patřičných administrátorských přístupů. Další síťové prostředky budou použity pro migraci virtuálních serverů a tzv. HeartBeat, který slouží k zjišťování konektivity mezi jednotlivými nody. Poslední interface, který je třeba přiřadit je propoj mezi

VLANy firemního prostředí tak, aby virtuální stroje mohly mít adresy z rozsahu, který je pro tuto část vyhrazen. K tomuto účelu slouží aplikace, která se jmenuje Hyper-V Manager.

Výše zmíněný výčet síťových interfaců je minimum pro řádný běh Hyper-V na windows serverech.

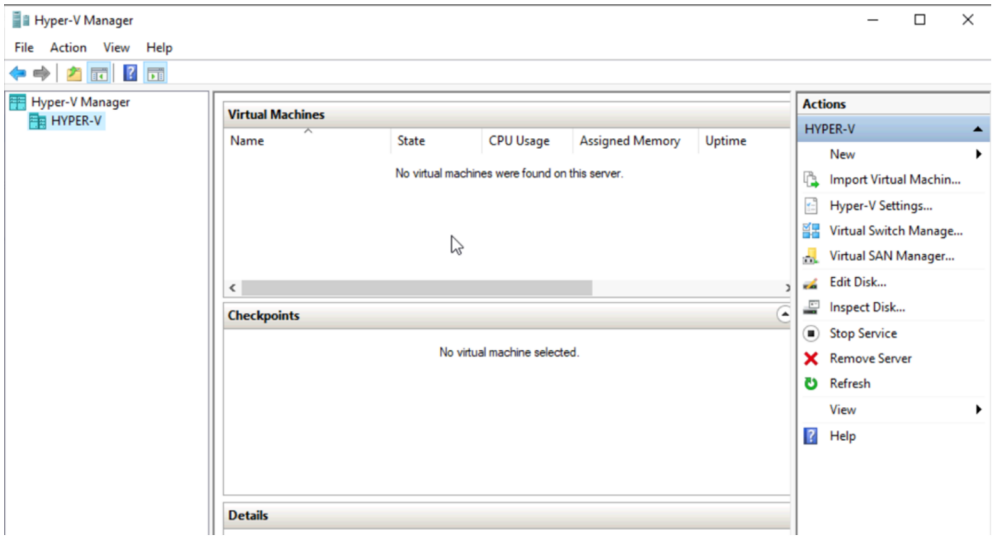
7.2.2 Hyper-V Manager

Nastavit roli Hyper-V lze z příkazového řádku (PowerShell), nebo z grafického rozhraní, který je součástí instalované role. Z důvodu přehlednosti preferuji grafické rozhraní.

Hyper-V Manager (obrázek č. 46) [109] se skládá z několika částí. V první části je zobrazen hypervizor, na kterém lze vytvářet virtuální stroje. Je zde možnost přiřadit další hypervizory, aniž by mezi sebou mely nějakou vazbu. Jedná se čistě o správu daného hypervizoru.

V druhé části jsou zobrazeny virtuální stroje, které jsou na jednotlivých hypervizorech.

Třetí část obsahuje nabídky možností konfigurace jak hypervizoru, tak virtuálního stroje.



Obrázek 46 Generální ředitelství HZS ČR. Hyper-V Manager.

[109] BEDEČ, Jan. Generální ředitelství HZS ČR. Hyper-V Manager. Slaný. [cit. 22. 12. 2021].

Před samotným vytvořením virtuálního stroje je zapotřebí upřesnit obecné nastavení.

7.2.2.1 Hyper-V Settings

Tlačítko „Hyper-V Settings…“ dovoluje specifikovat domovský adresář, kam se budou ukládat informace o virtuálním stroji a stejně tak virtuální disk, který se vytvoří při zakládání virtuálního stroje. Virtuální disk může být uložen do předem zvoleného úložiště. Nastavení Live Migration[110] (dále jen LM), dovoluje migrovat mezi nody i úložišti bez výpadku. Můžeme nastavit povolení migrace skrz celý síťový rozsah nebo specifikovat povolené nody pomocí konkrétního výčtu IP adres. Z dalších funkcí, které je dobré nastavit je vytváření replik na vzdálený server.

Při vytváření politiky LM je třeba zvolit variantu ověřování tak, aby byl přenos virtuálního stroje bezpečný. Zvolit můžeme mezi variantou CreedSSP nebo Kerberos, na který jsem poukazoval v kapitole 6.1.1.

CredSSP

Credential Security Support Provider (dále jen CredSSP) znamená, že mezi hostiteli, na kterém je spuštěn proces živé migrace, musí být administrátor přihlášen. CredSSP je výchozí nastavení. Ve skutečnosti není potřeba žádná konfigurace, aby vše fungovalo. Nevýhoda používání CredSSP spočívá v tom, že umožňuje přenos pouze na jeden skok, jako například ze zdrojového hostitele Hyper-V do cílového hostitele Hyper-V, ale ne dále. Vyžaduje také aktivní přihlášení na hypervizoru, ze kterého má být migrace provedena.[111]

Kerberos

Výhodou ověřovacího protokolu Kerberos je, že není omezen počtem přenosů na přihlašovacích údajích. To může být považováno za bezpečnostní riziko. Řešením je konfigurace omezeného delegování. Omezuje možnosti, k čemu lze přihlašovací údaje účtu použít. Omezení delegování protokolu Kerberos na určité služby se nastavuje v managementu Active

[110] Live Migration můžeme přeložit jako migraci stroje za provozu. Pozn. autora
[111] viz str. 79, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

Directory. Nastavení musí být na všech požadovaných serverech stejné, jinak není zaručena konzistentnost přenosu.[112]

Používání CredSSP je mnohem jednodušší, ale má určitá omezení, z nichž hlavním je přenos pouze na jeden skok. Použití protokolu Kerberos by nemělo být příliš obtížné, protože hypervizory jsou již členy domény Active Directory.

7.2.2.2 Virtual Switch Manager

Další nastavení, které musí administrátor provést po instalaci role Hyper-V Server, je konfigurace přepínače virtuální sítě.

Při vytváření nebo konfiguraci virtuálního přepínače Hyper-V (obrázek č. 47)[113] se můžeme rozhodnout mezi třemi různými typy:[114] Interní, Externí nebo Privátní.

Interní

Tento typ přepínače umožňuje síťová připojení mezi všemi virtuálními stroji na konkrétních hostitelích a samotným fyzickým serverem. Připojení k jiným fyzickým počítačům v síti nebo virtuálním počítačům na jiném hostiteli není možné.

Externí

Tento typ přepínače umožňuje síťově propojit všechny virtuální stroje napříč síťovou infrastrukturou a také propojení mezi fyzickými hostiteli a virtuálními stroji na různých hypervizorech.

Privátní

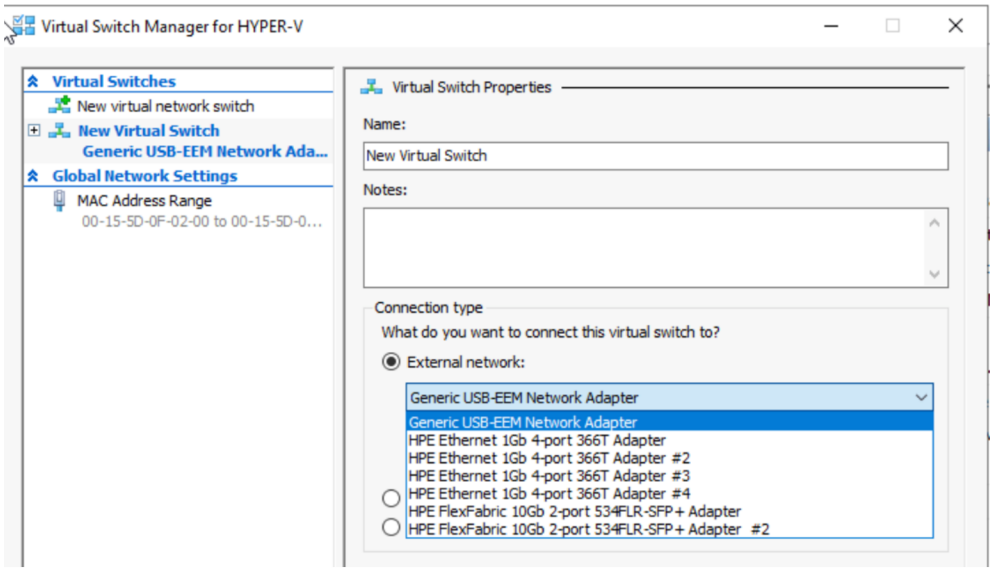
Typ privátního přepínače umožňuje pouze síťovou komunikaci mezi virtuálními stroji na konkrétním hypervizoru, nikoli však s fyzickým hostitelem samotným.

V praxi jsem se setkal pouze s externím nastavením síťového přepínače. Hlavním důvodem je segmentace síťových interfaců, které mohou být nastaveny pouze pro určité vlany a není žádoucí, aby virtuální stroje, které slouží pro zabezpečení provozu (monitorovací systémy, DHCP, DNS apod.), posílaly data

---

[112] Ibid. str. 80-81.
[113] BEDEČ, Jan. Virtual Switch Manager. Slaný. [cit. 22. 12. 2021].
[114] viz str. 53, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

skrz stejné rozhraní, jako provozní databázové servery. Například personální systémy nebo databázové systémy.



Obrázek 47 Virtual Switch Manager.

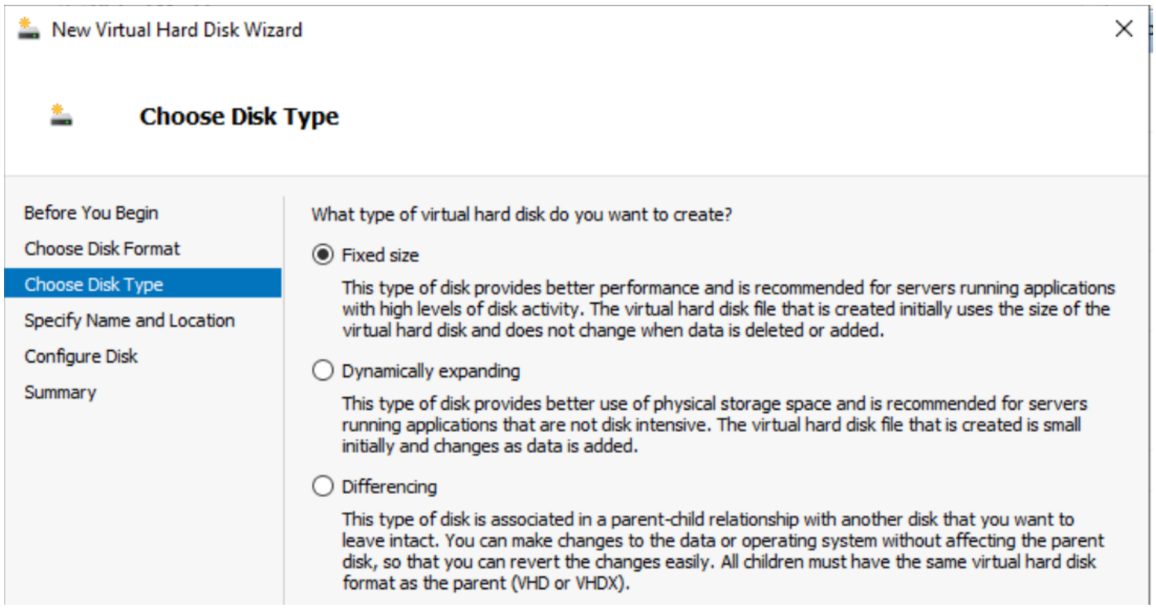
7.2.2.3 Vytváření virtuálního stroje

Vytvoření virtuálního stroje (dále jen VM), je po úvodním nastavením jednoduchá věc, která nezabere víc než pár minut. Avšak i při procesu vytváření VM musí administrátor přesně vědět, jaký typ VM chce vytvořit.

Průvodce pro vytváření VM nabízí vždy jenom několik variant, ale ne všechny. Z toho důvodu je dobré vytvořit nejdříve virtuální disk a ten poté připojit k VM při jeho vytváření. Průvodce pro vytváření VM (obrázek č. 48)[115] administrátorovi povolí připojit již existující virtuální disk (preferovaná volba), vytvořit nový virtuální disk (dovolí upravit pouze velikost a cílové umístění), nebo možnost připojit virtuální disk později.

Osobně preferuji variantu nejprve vytvořit virtuální disk. Tím získám větší paletu možností správy virtuálního disku.

[115] BEDEČ, Jan. Virtual Hard Drive Disk Wizard. Slaný. [cit. 22. 12. 2021].



Obrázek 48 Virtual Hard Drive Disk Wizard.

Nejdůležitější volbou je vybrat typ virtuálního disku:[116] Fixed size disk, Dynamically expanding disk a Differencing disk.

Fixed size

Virtuální disk (dále jen VHD) s pevnou velikostí zabere celý prostor, který je mu přidělen při vytváření. Velikost VHD se při vytváření nebo mazání dat nemění. Pokud je například vytvořen VHD s pevnou velikostí 127 GB, znamená to, že 127 GB místa na disku hostitelského úložiště (například diskového pole), bude vyhrazeno pouze pro tento VHD. [117]

Disk s danou velikostí se při vytvoření vynuluje. To vede k vyššímu výkonu, protože Hyper-V nemusí provádět operaci vynulování při prvním zápisu na disk. Disky jsou vynulovány jako bezpečnostní opatření, aby k jakýmkoli podkladovým datům na diskovém poli neměl přístup nástroj pro skenování disků ve virtuálním počítači.[118]

Výhody

- Nejrychlejší z typů VHD.

[116] viz str. 15, 51, 52, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. SBN 9781782176077.
[117] VEMBU Backup & Disaster Recovery: Hyper-V Disks : Fixed size, dynamically expanding, and differencing disks [online]. 2019 [cit. 10. 01. 2022]. Dostupné z: https://www.vembu.com/blog/hyper-v-disk-types-fixed-size-dynamically-expanding-and-differencing-disks/
[118] Ibid.

- Lepší výkon disků.
- Není náchylný k fragmentaci disku.

Nevýhody

- Vytvoření pevného disku je časově náročnější proces.
- Disky nemají dynamický růst.
- Pokud je vytvořený VHD příliš velký, neexistuje způsob, jak přerozdělit jeho zdroje.

Ve většině případů se doporučuje používat pevný disk, protože má ve srovnání s ostatními typy disků lepší odolnost a výkon.

Dynamically expanding

Tento typ disku se rozšiřuje do takové velikosti, jak veliká jsou na něj zapisována data. Soubor VHD, který se vytvoří jako první, je malý a roste úměrně tomu, jak jsou do něj přidávána data. Tato volba je také výchozí volbou, pokud se VHD vytváří přes průvodce vytváření virtuálního stroje.[119]

VHD se zprvu tváří jako malý soubor s přednastavenou maximální velikostí. Tato velikost souboru roste úměrně tomu, jak rychle a kolik dat do něj přidáváme. Soubor se přestane zvětšovat, když je dosaženo přednastavené maximální velikosti. Při vytváření dynamického svazku musí být vždy zadána počáteční velikost disku, ale využití hostitelského disku závisí na tom, kolik dat je na tomto svazku skutečně uloženo.[120]

Pokud například zpočátku vytvoříte 127 GB VHD, ale virtuální počítač vyžaduje pouze 40 GB, pak bude z hostitelského fyzického disku (například diskové pole), spotřebováno pouze 40 GB.

U dynamicky se rozšiřujících disků se místo na disku mění pouze tehdy, když jsou na něj zapisována data. Tyto disky také vyžadují hodně plánování a monitorování, protože místo na disku by mohlo snadno zaplnit datové úložiště a nečekaně odpojit produkční zařízení. Ačkoli se zdá, že zřejmým problémem dynamických disků je postupný nárůst dat, skutečný problém spočívá v rychlosti

[119] VEMBU Backup & Disaster Recovery: Hyper-V Disks : Fixed size, dynamically expanding, and differencing disks [online]. 2019 [cit. 10. 01. 2022]. Dostupné z: https://www.vembu.com/blog/hyper-v-disk-types-fixed-size-dynamically-expanding-and-differencing-disks/

[120] Ibid.

čtení. Příkladem může být 20 malých dynamických virtuálních pevných disků u kterých na stejném svazku roste každý disk samostatně. Způsobují fragmentaci mezi svazky. To ovlivňuje čtení, protože musí diskové pole trávit čas poskakováním z jednoho bloku do druhého v rámci svazku, aby načetl požadovaná data.

Klady

- Lepší využití fyzického úložného prostoru.
- Snadné kopírování souborů virtuálního disku mezi počítači.

Nevýhody

- Možnost zaplnění místa na disku datového úložiště.
- Pomalejší rychlost čtení.
- Sklon k fragmentaci disku.

Typy dynamických disků se doporučují pro případy, kdy je úložiště hlavním problémem, protože nabízí kromě úspory místa také vyšší odolnost proti ztrátě dat.

Diferenční disk

Diferenční neboli rozdílový disk je v podstatě dynamickým svazkem, připojeným k nadřazenému VHD. Lze je nakonfigurovat pomocí vztahu rodič-dítě a vytvořit tak hierarchii VHD.

Rozdílový disk obsahuje data na úrovni bloků, která představují změny nadřazeného VHD. Každý rozdílový disk může mít pouze jednoho rodiče a rodičem může být buď pevný, dynamický, nebo jiný rozdílový disk. Hyper-V může sloučit všechny rozdílové disky zpět k rodičovskému, čímž vymaže všechny podřízené disky.[121]

Podřízené disky jsou obvykle malé, mohou však narůst až do velikosti rodičovského disku. Rozdílový disk připojený k dynamickému rodiči jej může přerůst, pokud dynamický disk není plně rozšířen.[122]

---

[121] VEMBU Backup & Disaster Recovery: Hyper-V Disks : Fixed size, dynamically expanding, and differencing disks [online]. 2019 [cit. 11. 01. 2022]. Dostupné z: https://www.vembu.com/blog/hyper-v-disk-types-fixed-size-dynamically-expanding-and-differencing-disks/

[122] Ibid.

Tento typ VHD je obvykle určen pro virtuální počítače, které budou mít krátkou životnost. Například testovací server, aplikace, databáze. Lze také vytvořit jeden nadřazený disk VHD s operačním systémem a pomocí odlišných disků VHD lze zajistit chod více virtuálních strojů. Tyto virtuální stroje pak používají ke spuštění sdílený operační systém z rodičovského disku. Rozdílové disky VHD začínají jako malé a rostou s tím, jak se na ně přidávají data. Rozdílové disky se obvykle vytvářejí během zálohování a po dokončení zálohování se okamžitě odstraní. [123]

Při dlouhodobém používání a nárůstu rozdílových disků vzniká stálý pokles výkonu a problémy s úložištěm, proto není ideální pro použití v produkčních systémech.

Výhody

- Pomáhá udržovat konzistenci základních dat.
- Vysoký výkon pro krátkodobě nasazené stroje.
- Možnost izolovat změny na nadřazeném disku.
- Užitečné pro řešení problémů a analýzu.

Nevýhody

- Nevhodné pro produkční systémy.
- Možnost nadměrného poskytování úložiště hostitelského VHD.
- Přemístění nadřazeného disku je složité.

Virtual Machine Wizard

Samotný průvodce pro vytvoření virtuálního stroje už nenabízí žádnou možnost, která by se později nedala upravit kromě jedné, a to je výběr generace VM. Pokud je tedy nastavená dostatečná kapacita paměti RAM, přidělen správný typ disku, průvodce nabídne volbu, která je zásadní pro samotný operační systém. Tou volbou je generace VM. Druhá generace oproti první využívá UEFI BIOS a je v základu o 20% výkonnější a hlavně Generation 2 už může bootovat z virtuálního

[123] VEMBU Backup & Disaster Recovery: Hyper-V Disks : Fixed size, dynamically expanding, and differencing disks [online]. 2019 [cit. 11. 01. 2022]. Dostupné z: https://www.vembu.com/blog/hyper-v-disk-types-fixed-size-dynamically-expanding-and-differencing-disks/

ISO souboru. Rozdíl nastává u operačních systémů. Ne každý operační systém může být provozován na Generaci 1 nebo Generaci 2.[124]

Rozdíly mezi generací 1 a generací 2.

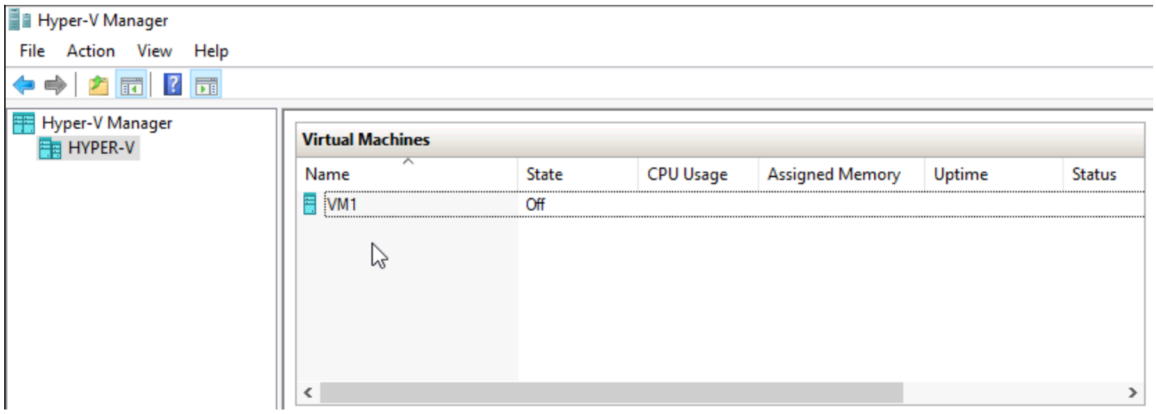
Z tabulky (tabulka č. 2)[125] je patrné, že zastaralé verze operačních systémů na novějších generacích nefungují. Ostatně krom testovacího prostředí k tomu není z bezpečnostního hlediska žádný důvod.

Operační systém	Generation 1	Generation 2
Windows Server 2008 R2	✓	✗
Windows Server 2008	✓	✗
Windows 7	✓	✗
Windows 32-bit	✓	✗
CentOS 5.x series	✓	✗
Debian 7.x series	✓	✗
FreeBSD 8.4-10.3	✓	✗
Oracle Linux 6.x series	✓	✗
Open SUSE 12.3	✓	✗
Ubuntu 12.4	✓	✗

Tabulka 2 Rozdíly mezi Generací 1 a Generací 2 u operačních systémů.

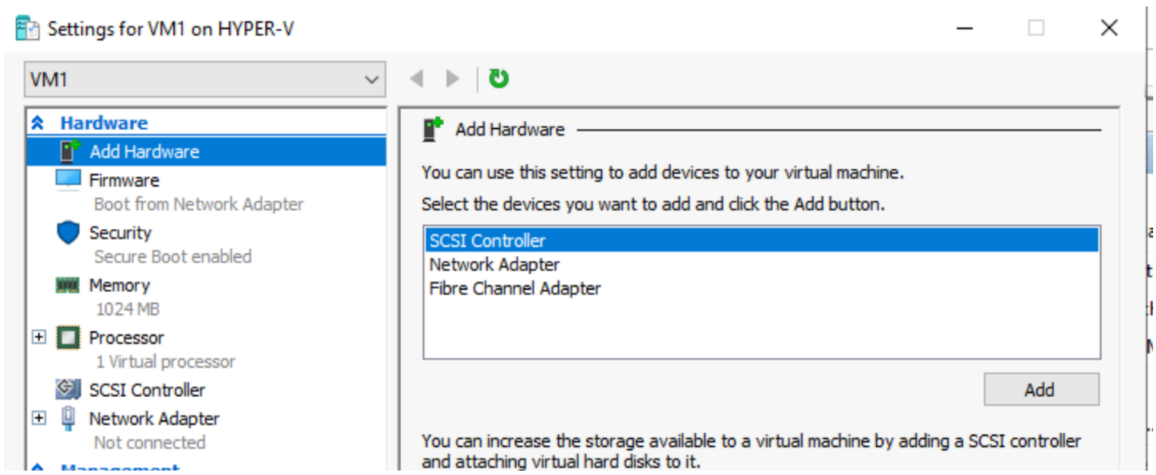
Vytvořený virtuální stroj se zobrazí v Hyper-V Manageru (obrázek č. 49) [126].

[124] Microsoft: Should I create a generation 1 or 2 virtual machine in Hyper-V? [online]. 2021 [cit. 11. 01. 2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v
[125] BEDEČ, Jan. Rozdíly mezi Generací 1 a Generací 2 u operačních systémů. Slaný. [cit. 11. 01. 2022].
[126] BEDEČ, Jan. Vytvořený VM s názvem VM1. Slaný. [cit. 11. 01. 2022].



Obrázek 49 Vytvořený VM s názvem VM1.

U takto vytvořeného „VM1“ je zobrazený status, který říká, v jaké stavu se daný stroj nachází. VM1 je momentálně vypnutý (state = OFF). S vytvořeným a vypnutým virtuálním strojem se dají provádět operace, které za spuštěného stavu nelze vykonat (obrázek č. 50)[127]. Příkladem je změna počtu přiřazených procesorů, změna paměti nebo přiřazení DVD mechaniky a síťového adaptéru. Vypnutý VM může být velice snadno migrován mezi úložišti i mezi hostitelskými nody.



Obrázek 50 Nastavení VM1 v Hyper-V Manageru.

7.2.3 Hyper-V Cluster

Failover[128] clustering je spojení několika serverů, které mezi sebou převezmou službu v případě, že jeden server nefunguje správně. Používá se pro aplikace, které jsou omezeny na jednu sadu dat, například databázi.

[127] BEDEČ, Jan. Nastavení VM1 v Hyper-V Manageru. Slaný. [cit. 11. 01. 2022].
[128] Failover se dá přeložit jako převzetí služeb při selhání. Pozn. autora

Hyper-V cluster se používá pouze pro protokoly založené na IP. Podporovány jsou protokoly IP verze 4 (dále jen IPv4) i IP verze 6 (dále jen IPv6). Umožňuje klientovi po převzetí spadlé služby automaticky obnovit připojení.

Při plánování Hyper-V Failover clustering se musí brát v potaz:

- Konfigurace distribuce VM z uzlu[129], který selhal. Při selhání nodu by se měly VM, které jsou v HA[130] selhaného uzlu rozdělit mezi zbývající servery, aby nedošlo k přetížení jediného serveru.
- Dostatečná kapacita každého uzlu pro obsluhu HA. Tato kapacita by měla představovat dostatečnou rezervu, aby nedocházelo k tomu, že uzly po výpadku poběží téměř na plný výkon. Špatné plánování odpovídajícího využití prostředků může mít za následek snížení výkonu po selhání nodu, po případě výpadek služeb, které se kvůli chybějícím zdrojům nespustí.
- Hardware by měl být od stejného výrobce, tím se předejde problémům s kompatibilitou při převzetí služeb a VM mohou být rovnoměrně distribuovány podle zátěže jednotlivých NODŮ.

7.2.3.1 Úložiště Hyper-V Clusteru

Failover Cluster vyžaduje sdílené úložiště, které poskytuje data konzistentně a nepřetržitě i poté, co dojde k převzetí služeb.

Hyper-V Cluster dovoluje pět možností sdíleného úložiště:[131]

- Sdílené sériové rozhraní SCSI (dále jen SAS). Sdílený SAS je nejlevnější variantou. Není však příliš flexibilní, protože dva uzly clusteru musí být fyzicky blízko sebe. Sdílená úložná zařízení podporující SAS mají navíc omezený počet hypervizorů, které k nim mohou v jednu chvíli přistupovat.
- iSCSI je typ sítě SAN (storage area network), která přenáší příkazy SCSI přes protokol IP. Výkonově se jedná o variantu, která přes 10 GB interface funguje pro většinu scénářů spolehlivě a rychle. Implementace tohoto typu

[129] Uzlem v Hyper-V clusteru je server, který má roli Hyper-V a je v clusteru (NOD). Pozn. autora
[130] High Availability (HA) je v překladu vysoká dostupnost. Pozn. autora.
[131] viz str. 110-115, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

sítě SAN je levná, protože nevyžaduje žádný specializovaný síťový hardware. Tato možnost je dostupná od verze Windows Server 2012.

- Sítě Fiber Channel SAN mají obvykle vyšší výkon než sítě iSCSI SAN, ale jsou výrazně dražší. Kromě toho vyžadují specializované znalosti a hardware pro implementaci.
- Sdílený virtuální pevný disk. V systému Windows Server 2012 R2 a novějších verzích může být sdílený virtuální pevný disk použit jako úložiště pro VM v clusteru.
- V systému Windows Server 2012 R2 a novějším lze jako sdílené úložiště pro některé role Failover clusteru, konkrétně pro SQL Server, použít sdílené úložiště SMB (Server Message Block). Hypervizory, které jsou hostiteli SQL databází, pak nemusí mít místní úložiště. Veškerá data se ukládají prostřednictvím SMB 3.0 na serveru.

Dle mého názoru je nejvýhodnější varianta propojit Fiber Channel (otická vlákna) s diskovým polem a příslušnými hypervizory v clusteru. Díky tomu mohou být servery geograficky rozmístěny na větší vzdálenost bez ztráty propustnosti.

Doporučení pro sdílené úložiště Failover clusteru:

1. Pokud se pro failover nepoužívá externí diskové úložiště, jako například NAS nebo SAN, doporučuji nepoužívat dynamicky expandovatelné nastavení disků.
2. Doporučeným formátem pro souborový systém je NTFS. Například ReFS není podporován pro databázové systémy (SQL).
3. Pokud je použit víc jak jeden Hyper-V Failover cluster ve firemním prostředí, musí mít rozdílné úložiště nebo alespoň oddělené sekvence na diskových polích.
4. Doporučuji používat aplikaci MPIO, která je součástí každé instance Windows server. MPIO poskytuje nejvyšší stupeň redundance a dostupnosti. Někteří výrobci diskových polí např. Huawei, dodávají svůj vlastní software pro vysokou dostupnost. Tento software musí být nainstalovaný na všech hypervizorech v clusteru.

7.2.3.2 Síťové požadavky Hyper-V Failover cluster

Před implementací Failover clusteru je třeba zajistit, aby síťové komponenty splňovaly konkrétní požadavky.[132]

1. Síťové adaptéry každého uzlu by měly být identické a měly by mít stejnou verzi protokolu IP i propustnost.
2. Sítě a síťová zařízení, ke kterým jsou nody připojeny, by měly být redundantní, aby v případě jedné poruchy mohly nody pokračovat v komunikaci. Redundanci jedné sítě můžeme zajistit pomocí týmového propojení[133] síťových adaptérů. Po případě můžeme jeden, např. 10 GB adaptér rozdělit na dva virtuální interface. Jeden může být přiřazen pro migraci VM a druhý pro HeartBeat. Doporučuji použít více sítí, abyste mohli zajistit více komunikačních cest mezi nody.
3. Síťové adaptéry v clusteru by měly mít stejnou metodu přidělování IP adres, což znamená, že všechny používají buď statické IP adresy nebo protokol DHCP (Dynamic Host Configuration Protocol), který automaticky adresy přiděluje.
4. Nastavení sítě a IP adres by se mělo shodovat. Pokud síť používá shodné síťové adaptéry, měly by se shodovat také v nastavení komunikace, jako je rychlost, režim, typ média, ke kterému přistupují. Kromě toho je dobré porovnat nastavení síťového adaptéru, přepínače a ujistit se, že nedochází ke konfliktům. Mohlo by dojít k zahlcení sítě nebo ztrátě datových rámců, což by mohlo negativně ovlivnit způsob komunikace mezi nody v clusteru.
5. Vyhýbat se smyčkám. Každá síť, která nemá přístup do intranetu, ale je používaná pro provoz clusteru, by měla mít specifický rozsah, který se jinde v síti nepoužívá. Předejde se tím konfliktu na aktivních prvcích sítě.

---

[132] viz str. 103, TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

[133] Funkce se v originálu jmenuje NIC Teaming. Pozn. autora.

7.2.3.3 Quorum

Quorum určuje kolektivní stav celého clusteru. Ověřuje stav clusteru v provozu a zjišťuje, zda má cluster ještě dostatečnou rezervu s dostatečným počtem nodů pro podporu Hyper-V clusteru. Ve základním nastavení má každý nod jeden hlas. V případě rovnosti hlasů se započítává i hlas svědka (může jít o sdílené úložiště nebo disk). Různé režimy quora určují, který hlas se započítá.

Typy quora jsou následující:

- Nod má prioritu: Každý nod v clusteru, který běží a má síťové připojení, může použít svůj hlas. Neexistuje žádný svědek a quorum má většinový hlas.
- Prioritu má nod a sdílené úložiště nebo disk jako svědek: Svědek i nody v clusteru mají hlas. Kvorum má většinový hlas plus hlas svědka.
- Nody nemají hlas: Žádný z nodů nemá hlas. Hlas se má pouze svědek. (Toto nastavení není doporučeno, protože svědek představuje jediný bod, který může selhat).

Dynamic Quorum

V systému Windows Server 2012 R2 byl zaveden nový režim, který byl nazvaný dynamické quorum, které označuje dynamickou úpravu hlasů quora na základě počtu online serverů v clusteru. Pro příklad budu mít Hyper-V cluster s pěti nody. Dva z nich uvedu do stavu offline a jeden zhavaruje. Ve starších verzích by cluster nemohl dosáhnout výsledku quora a celý cluster by přešel do offline stavu. Dynamické quorum by však upravilo hlasování clusteru. V době, kdy první dva servery přejdou do režimu offline, quorum by vyžadovalo dva a nikoli tři hlasy. Výhodou je, že cluster s dynamickým quorem zůstává online.

U quora je opět velice důležité propočítat si zátěž, která může přejít na jednotlivé nody v clusteru a podle toho naddimenzovat jednotlivé servery.

7.3 Shrnutí

Nasazení virtualizace Hyper-V je dle mého názoru nejjednodušší možná varianta z dostupných nabízených řešení. Z pohledu administrátora, který se zabývá správou a nasazením Windows severů je řešení Hyper-V nejpodobnější

variantou, na kterou může administrátor narazit. Bez řádného školení je ale veliké riziko konfigurovat produkční prostředí na míru jakéhokoliv firmě.

Hyper-V nabízí veliké množství variant nasazení. Tyto varianty lze různě modifikovat a provázat mezi sebou. Platforma se nebrání ani programovatelné nadstavbě ani monitorovacím systémům. Jako jedna z nejrozšířenějších variant se těší veliké podpoře po celém světě. Výhodou synchronizace s Active Directory je i bezpečnost Hyper-V Clusteru možné řešit na úrovni domény.

Závěr

Cílem diplomové práce nebylo naučit čtenáře konfigurovat základní síťové prvky, ani z nich udělat bezpečnostní správce nebo správce domény. Cílem práce bylo ukázat, že bezpečnost informačních technologií potažmo dat, se kterými zaměstnanci pracují, se pohybuje na několika vrstvách. Každá vrstva má svá zranitelná místa a je potřeba jim věnovat řádnou pozornost a nedoufat, že se zrovna nám nic stát nemůže.

V části zaměřené na uživatelskou bezpečnost jsem se rozhodl vypsat takové problémy, ve kterých se každý uživatel najde a je schopen si své pracovní prostředí poměřit s příslušnými řádky mé práce.

Aktivní síťové prvky jsou kapitolou samy o sobě. Jenom o problematice Cisco směrovačů a přepínačů mám 15 publikací. Vybral jsem tedy taková témata, která jsou pro běh sítě zásadní a zároveň jsem se cíleně vyhnul problematice firewallu, která by byla na samostatnou diplomovou práci.

Softwarovou bezpečnost ochrany dat ve firemním prostředí jsem cíleně vedl k případové studii, kde jsem podrobně popsal možné varianty nastavení.

Za cíl případové studie jsem si vzal Hyper-V virtualizaci, protože s touto virtualizační platformou mám bohaté zkušenosti a absolvoval jsem nejedno certifikované školení. Hlavním problémem u této práce se ukázala literatura. Všechny knihy, které se při školení od Microsoftu dostávají, nejsou tištěné, ale jsou v elektronické verzi, a ačkoliv mám na všechny publikace přístup, nelze z nich citovat pro nedostatek údajů. Naštěstí knihovna Generálního ředitelství HZS poskytla celou řadu publikací, o která jsem se mohl opřít.

Práci jsem se snažil psát tak, abych vysvětlil maximum odborných termínů, které jsem při psaní použil.

Seznam použitých zkratek

AAA	Autentizace Autorizace Accounting
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
FTPS	File Transfer Protocol s podporou TLS
GPMC	Group Policy Management Console
GPO	Group Policy Object
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IP	Internet Protocol
iSCSi	Internet Small Computer System Interface
LACP	Link Aggregation Control Protocol
LM	Live Migration
MAC	Media Access Control
MPIO	Multipath I/O
MST	Multiple Spanning Tree
PAgP	Port Aggregation Protocol
PVST	Per VLAN Spanning Tree
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SFTP	Secure File Transfer Protocol
SMB	Server Message Block
SSH	Secure Shell Protocol
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VLAN	Virtual LAN
VM	Virtual Machine

Seznam obrázků a tabulek

Seznam použité literatury

Monografie

[1] BURDA, Karel. Bezpečnost informačních systémů. [Skripta] VUT Brno: 2005. s. 104. [cit. 20. 11. 2021]

[2] DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. Active Directory. 5th edition. Sebastopol: O'Reilly Media, c2013. ISBN 1449320023.

[3] FROOM, Richard, SIVASUBRAMANIAN, Balaji and FRAHIM, Erum. Implementing Cisco IP switched networks (SWITCH). 1st ed. Indianapolis: Cisco Press, 2010. ISBN 9781587058844.

[4] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Brno: Computer Press, 2010. ISBN 9788025123591.

[5] MILFAJT, Jiří. Bezpečnostní protokoly v praxi: SECURITY PROTOCOLS IN PRACTICE. Brno, 2008, s 14-15. [cit. 20. 11. 2021] Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce Ing. Tomáš Pelka.

[6] SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 1 (ICND1) foundation learning guide. 4th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 9781587143762.

[7] SEQUEIRA, Anthony. Interconnecting Cisco Network devices, part 2 (ICND2) foundation learning guide. 2th Ed. Indianapolis, IN: Cisco Press, 2013. ISBN 97324501.

[8] TENDER, Peter De. Mastering Hyper-V: Learn to design, build, and manage a virtualized data center using Microsoft Hyper-V. Livery Place 35 Livery Street Birmingham B3 2PB, UK.: Packt Publishing, 2015. ISBN 9781782176077.

Webové stránky a elektronické zdroje

[9] BROUŠKA, Petr. CSMA/CD, kolizní doména, duplex. [Online]. 2005. [Cit: 25. 11. 2021]. Dostupné z: https://bit.ly/3oYLF9S

[10] BROUŠKA, Petr. nastavení interface/portu - access, trunk, port security. [Online]. 2009, Cisco IOS 3. [Cit: 26. 11. 2021]. Dostupné z: https://bit.ly/3IRieyx

[11] BROUŠKA, Petr. EtherChannel, Link Agregation, PAgP, LACP, NIC Teaming. [Online]. 2009, Cisco IOS 21. [Cit: 29. 11. 2021]. Dostupné z: https://bit.ly/3E3Bl5p

[12] BROUŠKA, Petr. Spanning Tree Protocol. [Online]. 2007, Cisco IOS 9. [Cit: 30. 11. 2020]. Dostupné z: https://bit.ly/3paRMqp

[13] BROUŠKA, Petr. Router Switching metody a související termíny - CAM, FIB, CEF. [Online]. 2009, Cisco. [Cit: 1. 12. 2021]. Dostupné z: https://bit.ly/2ZMp6vc

[14] CISCO IOS Router Basic Configuration: CCNA Routing & Switching ICND1 100-105 [online]. [cit. 27. 11. 2021]. Dostupné z: https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/cisco-ios-router-basic-configuration

[15] HEATH, Kath. What Are the Top File Transfer Protocols [online]. 25. 03. 2020 [cit. 30. 11. 2021]. Dostupné z: https://www.goanywhere.com/blog/what-are-the-top-file-transfer-protocols
[16] MICROSOFT: Should I create a generation 1 or 2 virtual machine in Hyper-V? [online]. 2021 [cit. 11. 01. 2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v
[17] NETIQ CORPORATION. Group Policy Administrator™: User Guide [pdf]. online, 2019. s. 15. [cit. 23. 12.2021]. Dostupné z: https://www.netiq.com/documentation/group-policy-administrator-67/pdfdoc/grouppolicyadministratoruserguide/grouppolicyadministratoruserguide.pdf
[18] Národní úřad pro kybernetickou a informační bezpečnost. Základní bezpečnostní opatření pro vrcholové vedení [online]. 17. 9. 2021 [cit. 17. 09. 2021]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1630-zakladni-bezpecnostni-opatreni-pro-vrcholove-vedeni/
[19] SHEN, Stephanie. What is Data?: And why we need data management, data literacy and data analytics [online]. 29.11.2020 [cit. 10. 11. 2021]. Dostupné z: https://towardsdatascience.com/what-is-data-ade94b37204a
[20] SOCHA, Łukasz. Grandmetric: tcp-model-vs-iso-osi-model [online]. 2019 [cit. 20.11. 2021]. Dostupné z: https://www.grandmetric.com/topic/network-layers-and-devices-operation/tcp-model-vs-iso-osi-model/
[21] SIMPLILEARN. What is Data: Types of Data, and How To Analyze Data? [online]. 10. 10. 2021 [cit. 10. 11. 2021]. Dostupné z: https://www.simplilearn.com/what-is-data-article#what_is_data
[22] SPRAVA-SITE.EU: Správa sítě – slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT [Online]. [Cit: 20. 11. 2021]. Dostupné z: https://www.sprava-site.eu/software/
[23] SZUBA, Tom, KING, Steve, ed. Safeguarding your Technology: Practical Guidelines for Electronic Education Information Sercurity. Washington, DC 20208-5574: U.S. Department of Education. National Center for Education Statistics., 1998. Dostupné z: https://nces.ed.gov/pubs98/safetech/
[24] VEMBU Backup & Disaster Recovery: Hyper-V Disks : Fixed size, dynamically expanding, and differencing disks [online]. 2019 [cit. 10. 01. 2022]. Dostupné z: https://www.vembu.com/blog/hyper-v-disk-types-fixed-size-dynamically-expanding-and-differencing-disks/