

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Bakalářská práce

Využití síťového úložiště (NAS)

Jakub Fulín

© 2015 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jakub Fulín

Informatika

Název práce

Využití síťového úložiště (NAS)

Název anglicky

Using Network attached storage

Cíle práce

Cílem práce je rozbor obecné tematiky Síťových datových úložišť, nástin možností jejich použití a rozbor klíčových parametrů se zaměřením na dostupné funkce a poskytované služby. Rozbor komunikačních protokolů, možností zabezpečení dat proti poruše zařízení/komponent i odcizení nebo zneužití dat. Důležitou částí je i uvedení a rozbor doplňkových funkcí, jež nejsou původním účelem zařízení.

Metodika

Práce je založena na studiu odborné literatury, doplňkově pak internetových zdrojů. Hlavním cílem je analýza funkcí NAS a možné oblasti použití. Dílčími cíly práce jsou:

- analýza dostupných souborových systémů
- ochrana dat před výpadkem a zneužitím
- stanovení charakteristik těchto zařízení

Praktické ověření bude provedeno na vybraném zařízení. Z výsledků analýzy, studia literatury a praktických poznatků bude formulován závěr práce.

Doporučený rozsah práce

30 – 40 stran

Doporučené zdroje informací

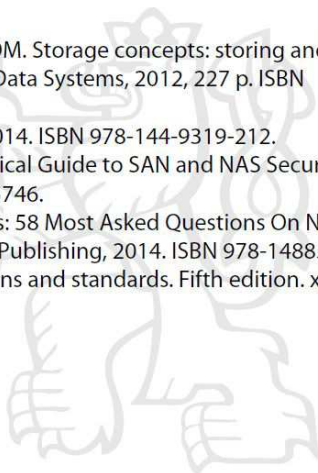
EDITED BY PETER MANIJAK, Martin Stewart a Nathan YOCOM. Storage concepts: storing and managing digital data. Santa Clara, Calif: HDS Academy, Hitachi Data Systems, 2012, 227 p. ISBN 06-156-5649-8.

HAGEN, Silvia. Ipv6 essentials. 3. Aufl. S.I.: O'Reilly Media, 2014. ISBN 978-144-9319-212.

HIMANSHU DWIVEDI, Himanshu. Securing Storage: A Practical Guide to SAN and NAS Security. Addison-Wesley Professional, 2012. ISBN 978-0321885746.

SNOW, Ruby. Network Attached Storage 58 Success Secrets: 58 Most Asked Questions On Network Attached Storage – What You Need To Know. Emereo Publishing, 2014. ISBN 978-1488529740.

STALLINGS, William. Network security essentials: applications and standards. Fifth edition. xvii,2013, 427 pages. ISBN 01-333-7043-7.



Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Alexandr Vasilenko

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 02. 03. 2015

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Využití síťového úložiště (NAS)" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2015

Jakub Fulín

Poděkování:

Rád bych touto cestou poděkoval panu Ing. Alexandru Vasilenkovi, za cenné rady a připomínky, za odborné vedení a vstřícnost při vypracování této bakalářské práce.

Využití síťového úložiště (NAS)

Using Network attached storage

Souhrn

Bakalářská práce se zabývá využitím síťového úložiště (Network attached storage – NAS) ve firmách a domácnostech. Teoretická část se věnuje vymezením základních pojmů, představením zařízení NAS, rozborem základní a rozšiřujících funkcí. Zaměřuje se především na analýzu dostupných souborových systémů, ochranou dat před výpadky energií, poruchám hardware a případným zneužitím dat. Část je věnována i zabezpečení bezdrátových sítí Wi-Fi, která s touto tematikou velmi úzce souvisí hlavně z hlediska zneužití dat. V praktické části je uveden detailní popis konkrétního zařízení. Další část se zabývá nastavením NAS a následným testováním na konkrétním zařízení.

Summary

Bachelor's work follows up the use of Network attached storage - NAS in companies and in households. Theoretical part is dedicated to demarcation of basic terms, introduction of NAS facility and analysis of basic and extending functions. It focuses primarily on analysis of available file systems, data protection against electricity failures, hardware malfunctions and possible data misuse. One part is dedicated even to Wi-Fi protection, which relates very closely with this topic mainly by easily misuseable datas. In practical part, the detailed description of certain device is presented. Another part is addressed to settings of NAS and the follow-up testing on concrete device.

Klíčová slova: NAS, Síťové datové úložiště, Systém souborů, Komunikační protokoly, RAID, Zabezpečení dat, Zálohování

Keywords: NAS, Network attached storage, File system, Communication protocols, RAID, Data security, Backup

Obsah

1	Úvod.....	3
2	Cíl práce a metodika	4
3	Teoretická část	5
3.1	Funkce.....	5
3.2	Komunikační protokoly	6
3.3	Souborový systém.....	9
3.4	Ochrana před výpadkem napájení - UPS	13
3.5	RAID (Redundant Array of Independent Disks)	13
3.6	Mechanické poškození harddisku	19
3.7	Ochrana dat před zneužitím	20
3.8	Zamezení přístupu přes Wi-Fi	22
3.9	Geografická redundance	25
3.10	Zálohování dat pomocí Cloud Station na zařízení Synology	28
4	Praktická část	30
4.1	Popis sítě a požadavků.....	30
4.2	Zapojení a nastavení NSLU2.....	31
4.3	Doplňkové služby a funkce.....	34
4.4	Přístup k NAS z prostředí Windows.....	34
4.5	Nastavení zabezpečení Wi-Fi	36
4.6	Testy rychlostí.....	37
4.7	Diskuze	40
5	Závěr	44
6	Seznam použitých zdrojů.....	45
7	Seznam obrázků.....	48
8	Seznam tabulek	49

1 Úvod

V dnešní moderní době se stále více setkáváme s přesunem dat do digitální podoby a ukládáním těchto dat na pevných discích počítačů. Tento trend je stále vzrůstající nejen díky rostoucím kapacitám pevných disků, ale i nízkým cenám diskového prostoru a komfortem, který tento způsob ukládání nabízí oproti konvenčním nosičům jako CD, DVD, magnetické pásky. Tradiční dokumenty na papíru s tištěným či psaným textem nahrazují dokumenty v podobě pdf dokumentů. Většinu klasických fotoaparátů nahradily digitální fotoaparáty. Videozáznamy se z DVD a VHS kazet přesunuly do PC, notebooku, media center nebo chytrých televizí. Stále více se i v oblasti zabezpečovací techniky setkáváme s IP kamerami s digitálním obrazem zaznamenávaným na lokální nebo vzdálené úložiště. To klade stále větší nároky na diskovou kapacitu a rychlost přenosu dat.

Dalším aspektem moderní doby je mohutný rozmach počítačových sítí nejen v průmyslu a firmách, ale i v běžných domácnostech. Většina dnešních domácností s přístupem k internetu vlastní alespoň levný Wi-Fi router, který vytváří jednoduchou počítačovou síť spojující většinu zařízení jako notebook, PC, tablet, chytrý telefon, smart TV, satelitní přijímač. Ne zřídka se také setkáváme s tzv. chytrými (smart) TV umožňujícími projekci filmů umístěných na externím HDD nebo na úložišti připojeném do počítačové sítě. Díky rozmachu sítí se hojně zavádí i zařízení NAS, o kterém tato práce pojednává. Díky němu je diskový prostor přístupný z celé sítě popřípadě i přes internet prakticky z celého světa.

2 Cíl práce a metodika

Cílem teoretické části práce je rozbor obecné tematiky NAS především v domácnostech a menších firmách. Rozbor funkcí a možností především sdílení dat a zálohování. Popis nejběžnějších komunikačních protokolů, dostupných systémů souborů, možností zabezpečení proti ztrátě a zneužití dat. Doplnkovým cílem je nástin problematiky zabezpečení wi-fi sítí, které je důležité pro ochranu před zneužitím či odcizením dat.

Cílem praktické části je popis konkrétního zařízení použitého pro ověření a aplikaci získaných vědomostí. Další důležitou částí je nastavení zařízení a následné testování s vyhodnocením a shrnutím výsledků testů.

Metodika práce je založena na studiu odborných publikací obsahově zaměřených na zařízení NAS a problematiku zabezpečení, komunikačních protokolů a systému souborů. Hlavním cílem je analýza funkcí a možné oblasti použití.

V praktické části bude ověření provedeno na vybraném zařízení. Z výsledků analýzy, studia literatury a doplňkových internetových zdrojů bude formulován závěr práce.

3 Teoretická část

NAS (network attached storage) v přesném překladu znamená: „k síti připojené úložiště“. NAS jsou aktivní zařízení zprostředkávající připojení pevných disků určených pro ukládání dat do počítačové sítě. Hlavní výhodou je trvalý neustálý provoz zařízení, které je přístupné pro všechna zařízení v celé síti. Pokud je síť připojena k internetu a správně nakonfigurována, je možné k datům přistupovat přes internet z celého světa. U starších NAS byla rychlost limitována především rychlostí síťového připojení, u moderních NAS s nástupem 1Gbps portů je zde limitující hlavně výpočetní rychlost CPU a rychlost pevných disků. Problematika rychlosti bude podrobněji popsána v praktické části na konkrétním zařízení. [2]

3.1 Funkce

- Centrální úložiště dat. Jedná se o hlavní funkci NAS. Uživateli je umožněn přístup k diskovému prostoru přes některý z podporovaných komunikačních protokolů. Hlavními z nich jsou CIFS, SMB, NFS, FTP, HTTP, DLNA. [1,4]
- Zálohovací server. Vybavenější NAS obsahují funkce automatického zálohování. Po nastavení časových intervalů zálohování a vybrání dat, která mají být zálohována, provede server automatickou zálohu dat. Tato funkce je velmi žádaná především při firemním nasazení. [4]
- Sdílení multimédií. Pokud NAS i televize/projektor/tablet podporuje DLNA protokol, je možné přehrávat pomocí tohoto protokolu filmy a hudbu bez použití multimediálních center nebo HTPC. [4]
- Server. NAS podporují spoustu doplňkových funkcí. Nejvýznamnějšími jsou FTP, e-mailový server a webový server. Největším omezením se zde stává použitý software a výpočetní výkon CPU. Na provoz osobních e-mailů a soukromých webových stránek servery většinou plně dostačují. Po instalaci doplňkových aplikací lze na NAS provozovat PHP nebo MySQL server. [3,4,5]
- Download centrum. Vybrané modely podporují přímé stahování ze serverů pro sdílení souborů (uloz.to) nebo přes torrenty bez nutnosti spuštěného PC. [4]

- HW rozšiřování pomocí USB portů. Pokud má NAS volné USB porty, lze je využít ke sdílení nejen diskového prostoru ve formě externích HDD nebo Flash pamětí, ale i pro připojení dalšího HW. Nejpoužívanější bývá připojení tiskáren, které nemají vlastní síťový port. Takto připojená tiskárna nabízí široké možnosti použití. Může být sdílena s uživateli nebo automaticky tisknout informace zaslané na vlastní e-mail přiřazený k tiskárně. [3,5]
- Sdílení a synchronizace kalendáře – zařízení s podporou funkce CalDAV. [3,5]

3.2 Komunikační protokoly

Podporované protokoly jsou jedním z nejdůležitějších parametrů NAS, určují k jakým zařízením je možno NAS připojit. Protokol je souhrn pravidel, podle kterých se řídí vzájemná komunikace mezi periferiemi. V konkrétním případě uživatele (notebook, tablet, TV) a NAS zařízení. Počet podporovaných protokolů do značné míry určuje kompatibilitu NAS s ostatními zařízeními. Důležité je sledovat podporované protokoly hlavně v případě pokud budeme k NAS přistupovat z různých platform, Windows, Unix, MacOS. [1]

CIFS

CIFS (Common Internet File System) je otevřená varianta protokolu SMB (Server Message Block) vyvinutého a používaného společností Microsoft ve svých operačních systémech. Známý je také pod pojmem Samba, což je jméno projektu, který přinesl svobodnou implementaci SMB protokolu. [7]

CIFS je síťový protokol pracující na aplikační vrstvě síťového modelu sloužící ke sdílenému přístupu k tiskárnám, souborům a sériovým portům. Je využíván především na platformě Windows. [6,7]

Protokol poskytuje:

- Přístup ke vzdáleným souborům umístěným na místní síti, nad kterými je schopen vykonávat operace čtení a zápis. [7]

- Současný přístup více klientů využívá k této činnosti odemýkání a zamykání zápisu nad soubory. Uzamčení souboru znemožní ostatním uživatelům zápis, aby během čtení souboru prvním uživatelem nedošlo ke změně dat ostatními uživateli. [7]
- Zabezpečený a anonymní přístup k souborům, který lze snadno spravovat.
- Umožňuje názvy souborů v unicode. Tabulka unicode obsahuje více než 110 000 znaků. Soubory mohou být téměř v jakékoliv znakové sadě. [7]

Princip komunikace probíhá na základě modelu klient-server. Klient zašle prvotní požadavek. Zasláním dojde ke specifikaci parametrů spojení mezi klientem a serverem. Sdílené prostředky jsou identifikovány pomocí síťové adresy UNC ve tvaru \\jméno_server\jméno_zdroje. Klient definuje požadavky na sdílené prostředky serveru. Server poté porovná přístupová práva a na základě přístupových práv zahájí požadovanou operaci (spuštění souboru, vytváření adresáře...). [6]

NFS

NFS (**N**etwork **F**ile **S**ystem) znamená v překladu síťový souborový systém. Byl vytvořen společností Sun Microsystems v roce 1984. Nyní se o jeho vývoj stará organizace Internet Engineering Force (EITF). Funguje hlavně nad protokolem UDP transportní vrstvy, od verze 3 lze provozovat i nad protokolem TCP.[8]

Hlavní myšlenkou bylo mezisystémové sdílení souborů mezi systémy Linux a Windows. Výhradně se však používá na unixových distribucích. Práce se soubory je velmi intuitivní a vyvolává dojem jako by uživatel pracoval se soubory lokálními. K připojení souborů dochází již při zavádění systému. [8]

V současné době je nejpoužívanějším protokolem z rodiny NFS verze 4. Na rozdíl od bezstavových předchůdců je stavový, což vykoupeno větší složitostí dává verzi 4 výhodu funkce zamykání souborů. Oproti verzi 3 se řeší přenos přístupových práv. Další podstatnou výhodou je potřeba pouze jednoho předem definovaného portu, na kterém komunikace probíhá. Usnadní se tak nastavování routerů a firewallů. Podporuje také využití bezpečnostního mechanismu Kerberos (autentizační protokol). [9]

FTP

FTP (**F**ile **T**ransfer **P**rotocol), v překladu protokol pro přenos souborů se na rozdíl od protokolů CIFS a NFS, které slouží především pro sdílení souborů na lokální síti, vyznačuje tím, že umožňuje sdílení a přenos dat přes veřejnou síť internet. Podmínkou je připojení lokální sítě, ve které je NAS zapojen k internetu. Z důvodu zabezpečení je tento protokol ve výchozím nastavení zablokovaný, lze jej však povolit v nastavení. [11]

Hlavní výhodou je nezávislost na platformě. Ke komunikaci s FTP serverem je zapotřebí FTP klient, který je běžně součástí webových prohlížečů, specializovaných programů na práci se soubory (FileZilla, Total Commander) nebo jednoúčelových FTP klientů. Vzhledem k faktu, že se jedná o velmi starý protokol (první specifiky byla sepsána v roce 1971), nastává zde problém se zabezpečením. Přihlašovací údaje jsou zasílány nešifrovaně v textové podobě. Tento problém řeší nadstavby s použitím SSL. [11]

Princip komunikace probíhá na dvou portech na protokolu TCP. První port číslo 21 zajišťuje přenos příkazů mezi serverem a klientem, kterými je řízena činnost serveru a druhý port číslo 20 zajišťuje vlastní přenos dat v textové nebo binární podobě. [11]

HTTP

HTTP (**H**yper**T**ext **T**ransfer **P**rotocol). Jedná se o internetový protokol pro výměnu hypertextových dokumentů. Jedná se o celkově nejpoužívanější protokol v oblasti internetu. Protokol je bezstavový, vybudovaný nad protokolem TCP. Podpora protokolu HTTP je podporována valnou většinou zařízení. U NAS se používá především pro administraci a nastavení. NAS nemá žádné zobrazovací zařízení jako monitor ani složitější vstupní zařízení jako např. klávesnici. Nastavování je prováděno pomocí webové administrace (ve výjimečných případech je možno provádět nastavení přes speciální aplikaci nebo úpravou konfiguračních souborů). Na NAS zařízení je spuštěn webový server umožňující připojení přes webový server na standardním portu TCP/80. Po připojení a přihlášení probíhá komunikace formou klient-server. Některé NAS podporují i stahování dat přes tuto administrativu, nejedná se však o rozšířené a používané řešení přístupu k datům. [11]

Nevýhodou protokolu HTTP bylo obdobně jako u FTP zabezpečení, jde také o velmi starý protokol. Z důvodu zvyšování bezpečnosti vznikla nadstavba HTTPS. Data jsou šifrována pomocí SSL a TLS protokolu. [11]

DLNA

Nejedná se o protokol, ale o organizaci **D**igital **L**iving **N**etwork **A**lliance. Vznikla v červnu 2003, byla založena firmou Sony. Hlavním úkolem bylo stanovení norem umožňujících sdílení digitálních video a audio záznamů mezi zařízeními různých výrobců. Jsou založeny na stávajících protokolech. Výsledné normy jsou soukromé, jsou ale volně k dispozici. Obsahují pouze omezené množství nejpoužívanějších multimediálních formátů (obrazové JPG, GIF, TIFF, PNG, audio MP3, WMA9, AC-3, AAC, ATRAC3plus, video formáty MPEG1, MPEG2, MPEG4, WMV9). DLNA používá technologii Universal Plug and Play (UPnP). Připojené zařízení samo prohledá síť a po nalezení DLNA serveru (nakonfigurovaného na NAS) automaticky naváže spojení. Organizace má v současné době přes 220 členů. [12,13]

3.3 Souborový systém

Oproti systémům SAN, které zprostředkovávají uživateli přístup přímo k pevným diskům a blokům, o souborový systém se musí postarat samotný uživatel. NAS zavádí i souborový systém. [14]

Souborový systém je v oblasti informačních technologií označení pro způsob organizace dat formou souborů a adresářů. Musí umožňovat snadný přístup k souborům a práci s nimi. Pro uživatele je mnohem snadnější práce s daty uspořádanými v hierarchické struktuře, než náročná práce s jednotlivými paměťovými buňkami či bloky disků. Souborový systém neuchovává pouze informace o cestě k souboru a jeho názvu, uchovává i některé důležité informace o souborech. Nejčastěji se jedná o datum a čas poslední změny souboru, dále spravuje informace o vlastních souborech a také přístupových právech, což je velmi důležité u systémů s více uživateli nebo při přístupu z počítačové sítě jako v případě NAS. [15]

Souborové systémy Windows (NTFS)

NTFS (New Technology File System) byl vyvinut na konci 80. let 20. stol. společností Microsoft jako nástupce systému FAT. Hlavní faktorem při vývoji byla bezpečnost dat. Oproti FAT obsahoval spoustu novinek: [17]

- Žurnálování – všechny akce na disku jsou zaznamenávány do speciálního souboru „žurnálu“. Pokud by při zápisu souboru došlo k pádu systému, je možné v žurnálu akci dohledat a rozpracované operace dokončit a uvést tím disk do konzistentního stavu. [17]
- Access Control List – sloužící k přidělování práv k souborům. [17]
- Komprese na úrovni souborového systému - uživatel pracuje se soubory jako s nekomprimovanými a o kompresi se nestarají externí programy, ale samotný souborový systém. [17]
- Kvóty na disku – umožňují přidělit každému uživateli maximální využitelné místo na disku. Při kvótování se nepočítají komprimované soubory, ale jejich reálná velikost. [17]
- Šifrování – probíhá na úrovni souborového systému. Data jsou chráněna před přístupem z jiného operačního systému. [17]

Další významnou novinkou je zavedení 11 souborů s metadaty. Jedná se o neviditelné soubory pro běžného uživatele. Obsahují důležité informace o organizaci dat na disku. [17]

Nejdůležitější soubory s metadaty:

- \$BADCLUS – soubor obsahuje informace o clusterech, u kterých došlo k problémům během čtení. Systém již nebude tento vadný cluster používat. [17]
- \$BITMAP – shromažďuje informace o prázdném místě na disku a předchází tak přílišné fragmentaci souborů. [17]
- \$MFT (Master File Table) – obdoba FAT tabulky. Úkolem je udržovat informace o rozložení dat na disku a vlastnosti souborů. Rychlost čtení tohoto souboru je rozhodujícím faktorem pro rychlost souborového systému. Aby nedocházelo k fragmentaci souboru \$MFT je v jeho okolí rezervován

dostatečně velký prostor pro rozšiřování záznamů. Ten je uvolněn až po plném obsazení disku. [17]

- \$Logfile – soubor žurnálování. [17]

Adresáře jsou reprezentovány jako speciální druh souborů používající odlišné atributy. Na disk jsou vloženy jako stromy se záznamy o jménech souborů a odkazy na jejich záznam v MFT. Velmi se tím urychluje procházení adresářů. [17]

Značnou nevýhodou je špatná kompatibilita s ostatními operačními systémy. Většina linuxových distribucí podporuje spolehlivě NTFS pouze pro čtení. [17]

Souborové systémy Linux (EXT3, EXT4)

Operační systém Linux je většinou distribuován jako Open Source (otevřený zdrojový kód), tudíž každý uživatel může vyvinout vlastní systém souborů. Nejpoužívanějšími jsou ext3 a ext4. V oblasti NAS se velmi často využívají jednoúčelově upravený systém Linux. [4,18]

EXT3

EXT3 je nástupcem EXT2. Podstatným vylepšením je zavedení žurnálování (viz NTFS). Mezi EXT3 a NTFS je zde podstatný rozdíl v jeho způsobu. U EXT3 jsou žurnálována pouze metadata obsahující informace o souboru, se kterým se pracuje. Metoda žurnálování metadat je podstatně rychlejší než metoda používaná u NTFS. Tento způsob je označován slovem „writeback“. Tato metoda nese i svá rizika. Jedním z nich je problém, který nastane např. při upravování souboru. Pokud dojde během úprav k výpadku mezi alokací datových bloků a zápisem dat, došlo by poté k zápisu náhodných dat do alokovaných bloků. Vznikla by nekonzistence mezi metadaty a samotnými daty. Problém je řešen metodou „ordered“, což znamená, že systém nejdříve zapíše data a až po zápisu dat provede záznam o akci do metadat. Zpětná kompatibilita s EXT2 je zajištěna při vypnutém žurnálování. [18]

Výhodou systému EXT 3 je velmi vysoká odolnost proti vzniku fragmentace. Ke fragmentaci začíná docházet až okolo zaplnění 80 procent disku. Existují sice dvě možnosti jak defragmentaci provést - první je převést systém na EXT2, provést defragmentaci a poté opět převést na EXT3. Druhý je využít externích aplikací na

defragmentaci, které fungují na principu kopírování a přesouvání souborů na volná místa disku. Vzhledem k velmi nízké náchylnosti ke vzniku fragmentace není prakticky nutno defragmentaci provádět. [18]

Další podstatný znak EXT3 je nemožnost obnovení smazaných souborů. Jediný způsob obnovení je potřeba znát první a poslední blok smazaných dat. EXT3 totiž maže při smazání souboru ukazatele v i-nodech. Tento aspekt může být považován za výhodu i nevýhodu zároveň. [18]

Velikost bloku	1kiB	2kiB	4kiB	8kiB
Max. velikost souboru	16GiB	256GiB	2TiB	2TiB
Max. velikost oddílu	2TiB	8TiB	16TiB	32TiB

Tabulka 1 - vliv velikosti bloku na max. velikost souboru a oddílu

EXT4

Vývoj souborového systému EXT4 byl zahájen v roce 2006 a první stabilní verze byla uvedena v roce 2008. EXT4 vznikl úpravami předešlého systému EXT3, opět podporuje žurnálování a je plně kompatibilní s EXT3. Hlavní úpravy spočívají v navýšení limitů, které měl jeho předchůdce. Maximální velikost oddílu byla navýšena na 1EB, max. velikost souboru na 16TB. Maximální počet souborů zůstal zachován na 4 mld. a maximální počet podadresářů byl zcela odstraněn. Podstatné je zvýšení výkonu souborového systému a přidání a doplnění několika nových funkcí: [18]

- Extent – jednotka nahrazující blok. Je to několik souvislých bloků a při velikosti bloku 4kB může mít jeden extent až 128MB. Na tento extent se poté poukazuje pouze jedním ukazatelem namísto velkým počtem v případě bloků, čímž dochází k znatelnému nárůstu výkonu. [18]
- Prelokace – metoda umožňující rezervaci místa pro budoucí rozšiřování souborů. Dříve se používal místo prelokace zápis nulových dat. Tuto funkci využívají především tvůrci databází, kde je potřeba zvětšování souborů největší. [18]

- Online defragmentace – defragmentace probíhá zcela automaticky na pozadí v době nečinnosti systému a odpadá tak plánování a spouštění defragmentace jako u systému Windows. [18]
- Zpožděná alokace – je mechanismus zabraňující přílišné fragmentaci. Spočívá v odkládání alokace a ukládání souboru po dobu zvětšování souboru, aby byl uložen až ve finální podobě. [18]

3.4 Ochrana před výpadkem napájení - UPS

Výpadky napájecích energií jsou co do počtu nejčastěji se vyskytujícími elementy způsobujícími poruchy a ztráty dat. Další nebezpečný element vyskytující se v napájecích sítích jsou přepětíové špičky a vlny. K ochraně zařízení slouží zařízení zvaná UPS (Uninterruptible Power Source) - v překladu nepřerušovaný zdroj napájení. Jedná se o zařízení obsahující akumulátor, měnič napětí a řídicí elektroniku. Nejčastěji používaným typem UPS je Off-line. Tento typ hlídá napětí sítě a při detekci podpětí nebo výpadku přepne svůj výstup na výstup měniče vytvářejícího z nízkého napětí akumulátoru síťové napětí 230V. Toto přepnutí trvá zpravidla mezi 20-30ms. Takto krátký výpadek je vykryt z kapacit kondenzátorů umístěných v napájecích jednotkách NAS či adaptérech. Doba chodu UPS je závislá na kapacitě a stáří akumulátoru. Součástí UPS bývají zpravidla i přepětíové ochrany třetího stupně zachycující napětíové špičky způsobené např. průmyslovými provozami nebo indukci atmosférického napětí do rozvodné sítě (bouřková aktivita). Plnohodnotné fungování přepětíových ochran je podmíněno instalací předcházejících stupňů ochran do domovní instalace. [20]

Některé NAS servery jsou schopné s vybranými UPS i datově komunikovat přes datový port (nejčastěji USB). Při detekci pak NAS spustí předem definovanou akci jako např. uložení všech neuložených dat a bezpečný přechod do stand-by režimu. Zařízení podporující komunikaci s NAS je např. „Netgear Ready NAS“. [20]

3.5 RAID (Redundant Array of Independent Disks)

V překladu znamená “vícenásobné pole nezávislých disků“. Dříve tato zkratka znamenala Redundant Array of Inexpensive Disks (vícenásobné pole levných disků) a používala se pro zvyšování spolehlivosti levných HDD. Jedná se o technologii spojování dvou a více

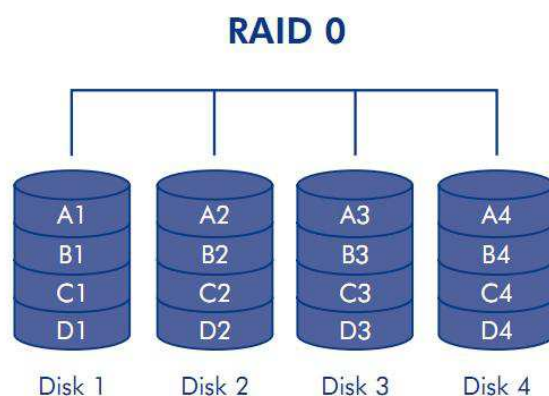
pevných disků za účelem zvyšování kapacit, rychlostí a především spolehlivosti a odolnosti proti ztrátě a poškození dat. Vzájemnou koordinaci disků řídí specializovaný RAID řadič, v tom případě mluvíme o HW řešení. Druhou možností je použití specializovaného SW. HW řešení je sice nákladnější, ale mnohem rychlejší a výkonnější než SW řešení. [21,22]

Pro využití této technologie musíme pečlivě vybírat NAS již při nákupu. Hlavním předpokladem je NAS podporující připojení dvou a více pevných disků. Dalším aspektem je podpora požadovaného typu RAID. Nejběžnější typy řazení RAID polí budou dále podrobněji rozebrány. [21,22]

RAID 0 – stripping

Není to klasický RAID, jelikož nedochází ke zvyšování spolehlivosti a k ochraně dat. Toto pole neobsahuje žádné redundantní (zdvojené) informace. V konfiguraci RAID 0 dochází ke spojení disků za účelem vytvoření logického disku s kapacitou rovnou součtu kapacit použitých disků. Spojení se provádí dvěma způsoby: [21,22]

- Zřetězení – po naplnění prvního disku se data začnou ukládat na druhý, třetí až do počtu použitých disků. Hlavní výhodou je snadné přidávání dalších jednotek, spolehlivost zůstává závislá na každém použitém disku zvlášť a data na různých discích jsou ukládána s různou úrovní spolehlivosti. [21,22]
- Prokládání – data se ukládají prokládaně (střídavě) na všechny použité disky. Výrazně se zvyšuje rychlost čtení i zápisu dat. Data se zapisují na všechny disky zároveň. Jeden soubor se tedy může nacházet fragmentován na všech discích. Spolehlivost pole silně klesá s počtem použitých disků. Postačí výpadek jednoho disku a dojde ke kompletní ztrátě dat (ztratí se pouze data z porouchaného disku, ale fragmenty souborů z ostatních disků jsou již většinou bezcenné). [21,22]



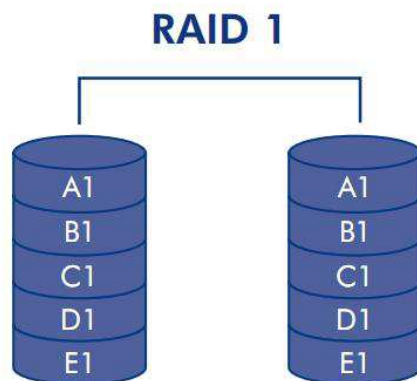
Obrázek 1 - Znázornění rozložení a struktury dat u metody RAID 0, zdroj:

<http://recuperacionraid.com/wp-content/uploads/2012/07/Recuperacion-de-datos-de-arreglo-RAID-0.jpg>

Nejčastější použití je při nárocích na vysokou propustnost dat a nízkou cenu řešení. Nemělo by být nasazováno v případech, kdy data nemohou být ztracena (je požadována spolehlivost). Typický příklad nasazení je střih videa, práce s obrazem a grafikou. [21,22]

RAID 1 – mirroring

Nejjednodušší, ale velmi efektivní způsob zvýšení ochrany dat. Princip funkce RAID 1 je zápis dat paralelně na více pevných disků. Při výpadku disku je možno okamžitě začít pracovat se zálohou a není nutné čekat na dopočítání a obnovu dat. Pokud by porucha nastala na řadiči a ne na pevném disku, lze použít dva samostatné řadiče. Tato metoda se nazývá „duplexing“. Výpadek řadiče neznamená nutně poškození dat, jen po dobu výměny řadiče nejsou data přístupná. Nevýhodou je potřeba minimálně dvojnásobného diskového prostoru. Používá se nejčastěji u aplikací s požadavky na vysokou spolehlivost uchování dat (bankovní účty a agendy). Výsledná kapacita je rovna kapacitě nejmenšího disku. [21,22]

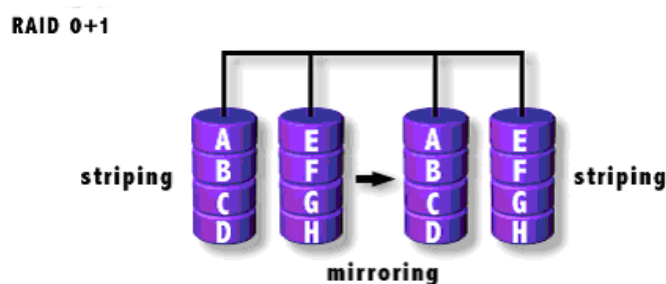


Obrázek 2 - Znáornění rozložení a struktury dat u metody RAID 1, zdroj:
http://recuperacionraid.com/wp-content/uploads/2012/07/4566967115_16846e9d58_o.jpg

RAID 0+1

Jedná se o kombinaci technologie prokládání a zrcadlení. Data se nejprve prokládají na dva disky a tato dvojice se poté zrcadlí. Rychlost může být vyšší než v případě RAID 1 díky použití technologie striping. Výsledkem jsou dva logické disky s redundantním obsahem. Je nutno použít min. 4 disky. [21,22]

Celková kapacita = $(n \cdot c) / 2$; n = počtu disků v poli a c = kapacita nejmenšího disku

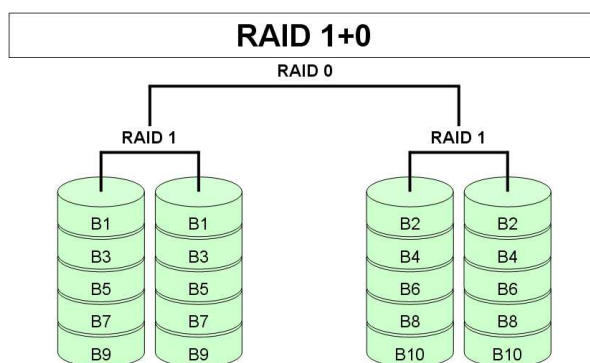


Obrázek 3 - Znáornění rozložení a struktury dat u metody RAID 0+1, zdroj:
<http://zive.v.mfstatic.cz/Files/Obrázky/2003/4/RAID/graf3.gif>

RAID1+0

Obdobně jako u RAID 0+1 se jedná o kombinaci pouze s prohozeným pořadím. Výsledkem jsou dva logické disky s prokládaným obsahem. Dosahovaná rychlost je vyšší než u RAID1, při stejné spolehlivosti. [21,22]

Celková kapacita = $(n \cdot c) / 2$; n = počtu disků v poli a c = kapacita nejmenšího disku

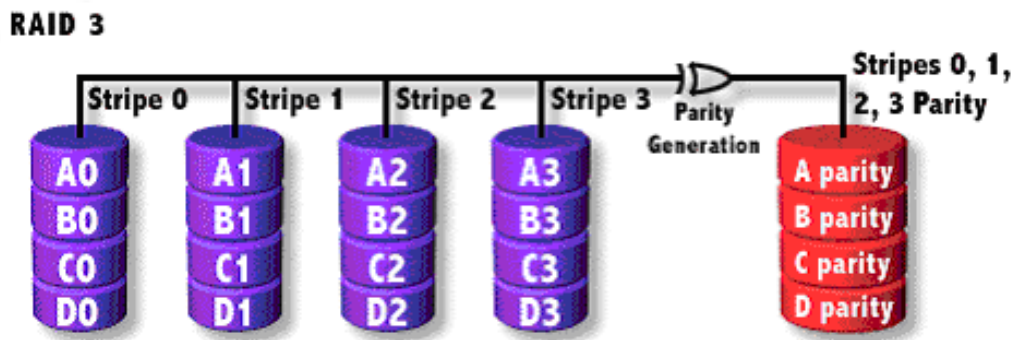


Obrázek 42 - Znárodnění rozložení a struktury dat u metody RAID 1+0, zdroj:
https://orlandoolguin.files.wordpress.com/2010/06/raid_1_0.jpg

RAID 3

V konfiguraci RAID 3 je použito $n+1$ disků. Na n -disků se ukládají data a na poslední neboli paritní disk je ukládána exkluzivní OR – XOR parita uložených dat. Při poruše paritního disku jsou data zachována a parita lze znovu obnovit. Při poruše disku s daty se obnova provede dopočítáním ztracených dat s použitím dat ze zachovalých disků a parity. Výhodou je nutnost použití jen jednoho disku navíc. Nevýhodou je přílišné zatížení paritního disku, je využívám pokaždé, pokud se zapisuje na libovolný datový disk. Vzhledem k vytížení lze předpokládat i rychlejší opotřebení a vzrůstající poruchovost tohoto disku. Konfigurace je odolná výpadku jednoho disku. [21,22]

Celková kapacita = $c \cdot (n-1)$; n = počtu disků v poli a c = kapacita nejmenšího disku

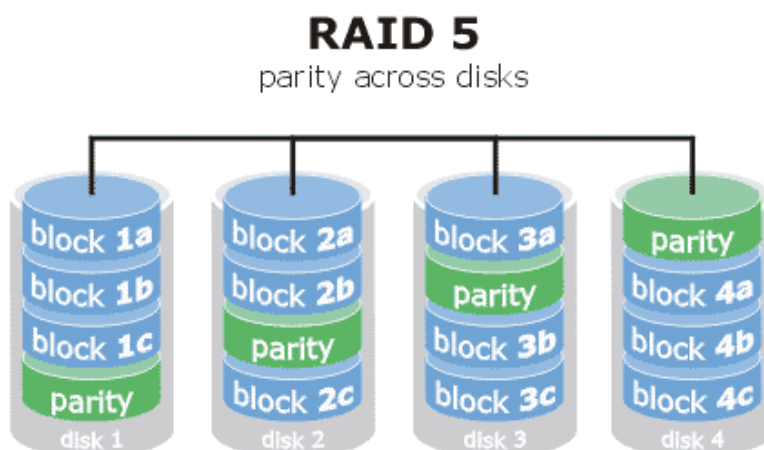


Obrázek 5 - Znázornění rozložení a struktury dat u metody RAID 3, zdroj:
<http://zive.v.mfstatic.cz/Files/Obrázky/2003/4/RAID/graf6.gif>

RAID 5

Je vylepšenou variantou RAID 3. Řeší přetížení paritního disku rozdělením paritních dat mezi všechny použité disky. Nevzniká zde nejslabší článek v podobě paritního disku. Obdobně jako u RAID 3 je RAID 5 odolný výpadku jednoho disku. [21,22]

Celková kapacita = $c \cdot (n-1)$; n = počtu disků v poli a c = kapacita nejmenšího disku



Obrázek 6 - Znázornění rozložení a struktury dat u metody RAID 5, zdroj:
<http://abeggi.altervista.org/blog/raid5.gif>

Porovnání rychlostí RAID polí

Zvyšování spolehlivosti není jediným účelem RAID polí. Dalším účelem je zvyšování rychlostí čtení i zápisu. Výsledek testu prováděného na Linux Software RAID s použitím 4 SATA disků s rychlostí čtení 60-80MB/s a rychlostí zápisu v rozmezí 12-13MB/s je shrnuta do přehledné tabulky. Při testu bylo využito 10GB oddílů a 40MB souborů. [16]

Typ pole	Čtení (MB/s)	Zápis (MB/s)	Výsledná velikost (GB)
Bez RAID (prům.)	70	12,5	10
RAID 0	106	37	20
RAID 1	60	19	10
RAID 5 (3 disky)	101	26	20
RAID 5 (4 disky)	137	38	30
RAID 1+0	90	34	20

Tabulka 2 - Vliv typu RAID pole na rychlost čtení a zápisu, zdroj:

<http://www.abclinuxu.cz/blog/MartinT/2007/9/software-raid-0-1-5-6-10-srovnani-rychlosti>

U všech testovaných konfigurací vyjma RAID 1 dochází ke zdatelnému nárůstu rychlostí oproti samostatným pevným diskům. Při použití RAID 0 dochází k nárůstu rychlostí přibližně o 50% při čtení a rychlost zápisu vzroste na trojnásobek. Spolehlivost je nižší, než u použití samotného disku. Cena řešení je poměrně nízká. RAID 0 je vhodný při požadavcích na běžnou spolehlivost, nízkou cenu a vysokou rychlost čtení a zápisu dat. Použitím RAID 5 je docíleno obdobných rychlostních nárůstů společně se zvýšením spolehlivosti. Nevýhodou je potřeba min. 3 disků. S rozšířením pole o další disky je docíleno dalšího nárůstu výkonu. [16]

3.6 Mechanické poškození harddisku

Mechanické poškození disků vzniká důsledkem selhání z rozličných příčin. Selhání komponent vlivem nekvalitní výroby či skryté výrobní vady nemůžeme ovlivnit. Dalším aspektem mechanického selhání mohou být nadměrné otřesy a nešetrné zacházení. Je důležité zvolit vhodné umístění NAS, kde k otřesům dochází minimálně a nehrozí zde riziko pádu a následného otřesu. Zvýšené opatrnosti je třeba dbát i při manipulaci se

zařízením, přenášením apod. Třetím faktorem ovlivňujícím životnost a spolehlivost disků je dodržení provozních teplot. Kvalitní chlazení a bezprašné prostředí je základní požadavkem pro dodržení tohoto parametru. V prostředí se zvýšenou prašností (technická místnost s kobercem) je nutno instalovat vzduchový filtr jako součást ventilace zařízení (NAS). Ten pravidelně čistit či vyměňovat. Maximální provozní teploty běžných HDD se pohybují okolo 50°C. Častý cyklus vypínání a zapínání disků též negativně ovlivňuje životnost pevných disků. Pro tyto účely je možné zakoupit úsporné HDD (řady green a eco) uzpůsobené pro časté zapínání a vypínání. [23]

3.7 Ochrana dat před zneužitím

Zabezpečení dat proti odcizení a zneužití je stejně důležité jako zabezpečení proti ztrátě, především u firemního nasazení může NAS obsahovat spoustu citlivých dat. Zpravidla platí, pokud se můžeme k datům dostat my, dostane se k nim i kdokoliv jiný. Rozhodující je, jak to pro útočníka bude obtížné. Ani umístění NAS na lokální síť jej nemusí plně ochránit před útoky z internetu. Větší rizika nastávají, pokud je na NAS provozován VPN nebo FTP server. Zabezpečení NAS je poměrně obsáhlý a komplexní problém, který se dá rozdělit do několika základních částí. [24]

Uživatelské účty, práva a hesla

První nejdůležitější účet NASu je účet administrátorský. Tento účet má ve výchozím stavu kompletní přístup k veškerému obsahu a administraci. Takovýto účet je nutno chránit dostatečně silným heslem. Nedoporučuje se používat snadno uhodnutelná hesla složená např. ze jména a data narození atd. Pro silné a snadno zapamatovatelné heslo odolávající slovníkovým útokům je možno použít kombinaci min. dvou slov a číslice. Administrátorský účet je vhodné používat výhradně pro administraci, pro běžnou práci s daty je vhodné vytvořit další uživatelský účet, který má omezená práva a umožňuje jen ty možnosti, které je potřeba aktivně používat. [25]

Pokud NAS neslouží jen jednomu uživateli, není vhodné ostatním uživatelům sdělovat (sdílet) heslo. Vhodný způsob je vytvořit každému uživateli (případně skupinám uživatelů) vlastní uživatelské účty. Je poté jednoduché jednotlivým uživatelům přidělovat a odebírat práva podle aktuální potřeby. Případně účet zablokovat. Při přidělování práv uživatelům

platí, zakázat vše a povolit jen to, co je potřebné. Nejkritičtější jsou aplikace a protokoly dostupné z internetu (VPN, FTP). [25]

Sdílení a oprávnění

Ne všechna data jsou vhodná pro sdílení se všemi uživateli. Některá data jako např. zálohy není vhodné sdílet vůbec, pouze v případě aktuální potřeby. Další skupinou dat jsou data zpřístupňovaná pouze některým skupinám uživatelům, do této skupiny spadají například dokumenty, účetní a skladové výkazy, materiály spojené s provozem firem atd. Třetí skupina dat je zcela bezpečná a může být sdílena téměř se všemi uživateli. Do této kategorie spadají např. multimediální soubory (hudba filmy) neobsahující citlivý obsah. [26]

Aktualizace NAS a aplikací

Aktualizování aplikací a systému neprobíhá jen kvůli doplnění nových funkcí, ale především z bezpečnostního hlediska. Nové verze firmware nejenže zlepší výkon, stabilitu a funkčnost, ale také zvýší bezpečnost opravením bezpečnostních děr. Kvalitnější NAS již poskytují možnost nastavení automatických aktualizací obdobně jako je tomu u PC. [27]

Důležité je též aktualizovat aplikace. Nejen aplikace nainstalované přímo do NAS, ale též aplikace, přes které k NAS přistupujeme. [27]

Šifrování disků

Šifrování obsahu disku je velmi užitečný nástroj pro ochranu přístupu k datům neoprávněnou osobou i při fyzickém odcizení disku. Probíhá nejčastěji šifrovacím standardem AES (Advanced Encryption Standard). Podrobněji vysvětlen v části Wi-Fi. [15]

U NAS Synology je šifrování disků implementováno přímo v aplikaci Disk Station Manager (DSM). Poskytuje 256 bitové šifrování. Data jsou na disk ukládána v šifrované podobě a bez znalosti klíče k nim nelze přistupovat ani z jiného zařízení. Proces výpočtu je poměrně náročný na výkon zařízení, v případě potřeby šifrování velkého obsahu dat

společnost Synology nabízí i NAS s podporou HW akcelerace AES, které sníží výkonnostní pokles při aktivaci šifrování. [15]

3.8 Zamezení přístupu přes Wi-Fi

Se stále se prodlužujícím dosahem Wi-Fi sítí je potřeba této tématice věnovat náležitou pozornost. Do NAS zařízení se po prolomení Wi-Fi útočník dostane již velmi snadno. Je tedy na místě tomuto předcházet. [28]

ACL založená na filtrování MAC adres

ACL (Access Control List) používající MAC adres zařízení pokoušejících se o připojení k bezdrátové síti je jedním ze základních způsobů, jak znemožnit přístup nechtěným zařízením. Nevýhodou je zde potřebná administrativa evidující seznam MAC adres různých zařízení. Tato evidence se musí aktualizovat při každé výměně zařízení nebo i jen samotného síťového adaptéru. Velké usnadnění přinese informační systém podporující automatické aktualizace MAC adres v přípojných bodech. Další nevýhodou je, že toto řešení nijak nezabezpečuje samotný přenos dat, pouze zamezuje připojení k bezdrátové síti. Z tohoto důvodu se jedná spíše o doplňkový nástroj, který se nehodí pro samostatné provozování. Vhodná je jeho kombinace s dalšími způsoby zabezpečení. Prolomení ACL pro zkušeného útočníka je otázkou několika málo minut. Stačí zjistit adresu zařízení s povoleným přístupem a tu emulovat na zařízení pokoušejícím se o útok. [28]

Skrytý přípojný bod (AP)

Další způsob zabezpečení je skrytí SSID. Pokud má síť skryté SSID (Service Set Identifier) není tak snadné síť identifikovat a zjistit, zda se jedná o síť, ve které se nachází potenciálně napadnutelné NAS. Problém bývá u některých systémů s vyhledáním takových sítí. Pro příklad Windows XP rovnou ve svém správci bezdrátových sítí automaticky filtruje a skrývá sítě, které mají skryté SSID. Použitím externích utilit ale tyto sítě není obtížné naleznout, je potřeba pamatovat i na méně zkušené uživatele. [28]

WEP

WEP (**W**ired **E**quivalent **P**rivacy) je protokol ke zvýšení bezpečnosti bezdrátových sítí. Základním úkolem bylo poskytnout obdobnou úroveň ochrany jako při použití metalických sítí. Hlavním rozdílem mezi metalickou a bezdrátovou sítí je používání sdíleného média u bezdrátových sítí. Odposlech radiové komunikace je mnohem jednodušší než fyzické napojování na metalický či optický kabel. Odposlouchávat komunikaci může každý potenciální útočník vlastníci přijímač naladěný na stejné pásmo, ve kterém probíhá komunikace. Takovým přijímačem je např. běžná bezdrátová karta v notebooku či mobilním telefonu s Wi-Fi modulem. [28]

WEP je možné používat pro autentifikaci i pro šifrování vlastní komunikace. Pro autentizaci slouží 40 bitový klíč sdílený všemi připojenými stanicemi. Významným bezpečnostním rizikem je samotná autentifikace. Probíhá ve třech krocích. [28]

- Stanice žádá AP o připojení
- AP odpoví a zašle nešifrovaně výzvu
- Stanice výzvu zašifruje a pošle zpět do AP

Jak bylo popsáno výše, není obtížné tuto komunikaci odposlouchávat a zjistit tak šifrovanou a nešifrovanou podobu výzvy. Používané šifrování je RC4. Jedná se o symetrické šifrování, což znamená, že zašifrování a rozšifrování probíhá stejným způsobem. Porovnáním zašifrované a nešifrované výzvy je nalezen šifrovací vektor a není obtížné zjistit i klíč. [28]

K prolomení WEP klíče je napsáno nespočet jednoúčelových utilit na základě odposlechu nebo s využitím Brutal Force. S těmito utilitami trvá prolomení klíče několik desítek minut, maximálně několik hodin a není tedy v současné době doporučován jako vhodné zabezpečení. AP podporující pouze zabezpečení WEP je vhodné vyměnit za novější bezpečnější zařízení. [28]

WPA

Jak vyplývá z části o zabezpečení s použitím WEP, toto zabezpečení neplnilo dostatečně svou funkci zabezpečení. I přesto se stále dosti hojně používá z důvodu nevědomosti uživatelů a částečně z důvodu nevole vyměnit starší HW za jiný podporující novější způsoby zabezpečení. [28]

Jako reakce na zmíněné nedostatky byl společností Wi-Fi aliance v roce 2002 vyvinut nový způsob nazvaný WPA (**Wi-Fi Protected Acces** – v překladu Wi-Fi chráněný přístup). Problémy vzniklé u WEP zde byly odstraněny použitím TKIP a 802.1.x. [28]

Šifrovací algoritmus je použit stejný jako u WEP a to RC4. Hlavním důvodem použití RC4 byl snadný přechod bez změn HW pouze aktualizací firmware (pokud byl aktualizovaný firmware výrobcem routerů a AP vydán). Bylo zde použito 128 bitového dynamického klíče a inicializační vektor měl délku 48 bitů. [28]

Další podstatnou výhodou WPA je možnost zabezpečení pomocí autentizačního serveru (nejčastější a nejznámější RADIUS), který je schopen zasílat každému uživateli rozdílný klíč. Této možnosti je využíváno především u podnikových nasazení. Pro domácí použití je zde možnost použití PSK (**Pre Shared Key**) – sdílený klíč. Každému uživateli je zaslán shodný sdílený klíč. Toto řešení se používá u malých firem a především v domácnostech. [28]

WPA byl navržen jako dočasné řešení později nahrazené WPA2. [28]

WPA2

Zatím nejspolehlivější běžně dostupné zabezpečení Wi-Fi. Pokud ho zařízení podporuje je jednoznačnou volbou. Mechanismus WPA2 jinak označovaný též jako IEEE802.11i, vznikl v roce 2004 jako standard podporující několik nových zabezpečovacích metod. Je zde používán protokol CCMP, který je nezbytnou částí pro plně bezpečnou síť. Zaručuje mnohem lepší šifrování díky použití AES (**Advanced Encryption Standard**). CCMP dokáže zajistit nejen zabezpečení, ale i integritu. [28]

AES je natolik dobrým šifrovacím algoritmem (na rozdíl od RC4 používaného u WEP a WPA), že je používán i pro vládní účely. Dříve u WPA a WEP stačilo útočnickovi odposlouchávat komunikaci a po nasbírání dostatečného množství dat klíč prolomit. U WPA2 probíhá automatická změna klíčů dostatečně rychle, aby jej útočník ze zachycených dat nemohl rozluštit. Obdobně jako WPA nabízí WPA2 možnost autentizace pomocí PSK nebo autentizačního serveru (802.1x). [28]

V současné době je dostupný na téměř všech současně prodávaných zařízeních a při volbě správného neuhodnutelného hesla a správného nastavení (použití AES místo TKIP) je velmi silným zabezpečovacím nástrojem. [28]

3.9 Geografická redundance

Nestává se to často, ale rizikový faktor živelných pohrom může ohrozit důležitá data. Kromě povodní, požárů a podobných katastrof je možné do této kategorie zařadit i krádež zařízení a disků. Není to ojedinělá situace, kdy záloha byla provedena na více discích metodou zrcadlení, ale všechny byly ve stejném domě na stejném místě. Zloděj odcizil všechny najednou. Obdobná situace může nastat i při vypuknutí požáru a podobných nehod. [23]

Těmto situacím zamezuje metoda zvaná geografická redundance. Data jsou uložena zrcadleně na dvou a více zařízeních umístěných na vzdálených místech (často desítky až stovky kilometrů). Geografická redundance řeší částečně problematiku přepětí vzniklé atmosférickou činností (bouřky) avšak vzhledem k nízkým cenám přepět'ových ochran se vyplatí nespolehat jen na geografickou redundanci a použít přepět'ových ochran na všech lokalitách. [23]

Metody zálohování

Standardní metody zálohování jsou rozděleny do tří základních skupin. V Unix systémech jsou označovány jako úrovně. [19]

- Plná záloha (Úroveň 0) – jedná se o metodu zálohování veškerých předem nadefinovaných vstupů. Za vstup může být brán soubor, složka nebo kompletní stav systému včetně veškerých dat a nastavení. To lze v některých případech využít pro obnovu tzv. „Bare metal recovery“ – obnova zálohy na nový počítač bez nainstalovaného systému. Tyto typy záloh jsou velmi dobře propracované u zálohovacích systémů společnosti Acronis. Se specializovanými nástroji lze obnovu provádět i na rozdílný HW od původního.
- Rozdílová záloha (Úroveň 1) – metoda bere v úvahu změnu dat vzhledem k poslednímu provedení zálohy plné. V Systémech Unix se zálohovací software řídí časovou značkou, kdežto u Windows podle nastavení archivačního bitu. Tento způsob zálohování šetří objem přenášených dat a je rychlejší než provádění plných záloh.
- Přírůstková záloha (Úroveň 2-9) – metoda používaná nejčastěji ve zvolených časových intervalech. Zálohování probíhá opět na základě archivačního bitu, který je pro provedení přírůstkové zálohy vynulován. U Unix systémů se provádí oproti předchozím verzím zálohy.

Zálohování serveru Synology pomocí rsync na geograficky odlehlý server

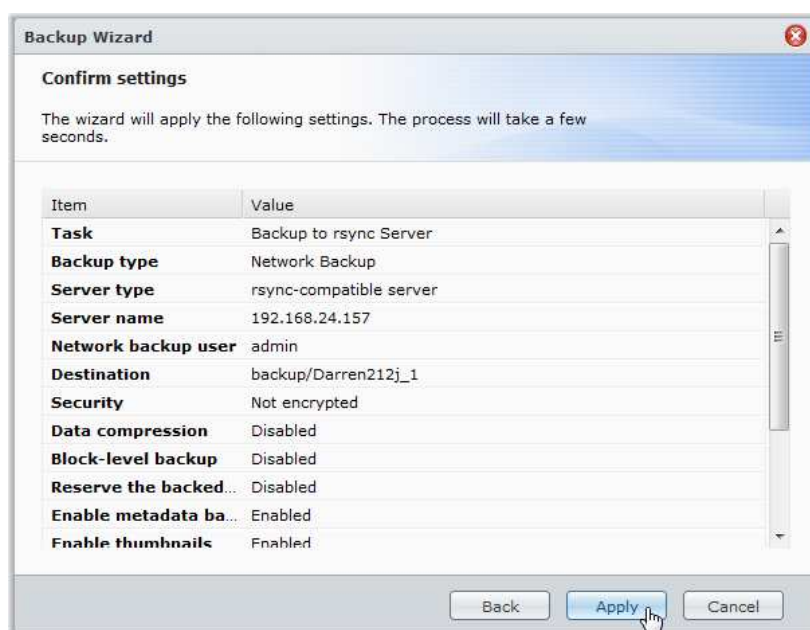
Síťová záloha umožňuje kopírování dat z jednoho Synology zařízení na další servery Synology DiskStation nebo na jiné servery kompatibilní s technologií rsync. Během přenosu dat je možno používat šifrování a zabezpečit tak bezpečný přenos dat. Zálohování je možno provádět i na úrovni bloků a kopírovat pouze bloky pozměněné. Dochází tím k úspoře množství přesouvaných dat. Tato metoda je vhodná pro zálohování přes internet. [10]

Prvním potřebným krokem je instalace HW NAS serveru, Dále instalace software pro systém Synology DiskStation Manager, vytvoření svazků a sdílených složek a v poslední

řadě místních uživatelů. Nyní lze přikročit k nastavení zálohování. Nastavení cílového serveru je provedeno vybráním zálohovacího režimu Synology v záložce Síťová záloha. Na cílovém serveru je nutno nastavit přístupová práva pro zálohování. V nastavení oprávnění aplikace pod záložkou Síťová záloha je nutno nastavit příslušná oprávnění. [10]

Nastavení zálohovaného serveru probíhá dle těchto kroků:

- Vytvoření úlohy zálohování a obnovení. [10]
- Nastavení typu cílového zařízení (Synology/rsync kompatibilní zařízení). [10]
- Zadání parametrů cílového zařízení (IP adresa, přihlašovací údaje, adresář cílové jednotky a zálohovací modul). Zde je možno povolit možnost šifrovaného přenosu dat. Pro úsporu přenesených dat lze aktivovat block-level backup. [10]
- Výběr složek a dat určených k zálohování. [10]
- Nastavení zálohovacího plánu (denní doba běhu zálohování). [10]
- Potvrzení a uložení vybraných možností. [10]



Obrázek 7 - Shrnutí a potvrzení nastavení záloh u NAS Synology, zdroj:

https://www.synology.com/img/knowledgebase/tutorials/backup_DiskStation_to_another_server/Snap7.png

3.10 Zálohování dat pomocí Cloud Station na zařízení Synology

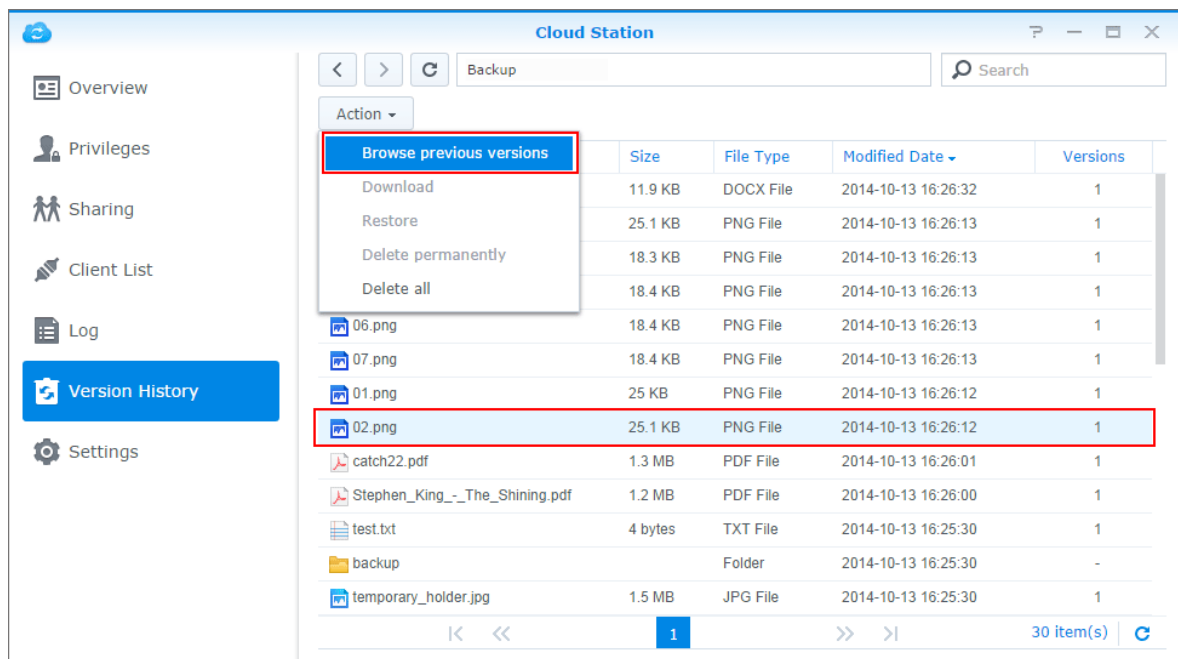
Možnosti Cloud Station jsou velmi rozsáhlé. Poskytuje nejen sdílení souborů napříč rozdílnými platformami, ale i sofistikovaný a propracovaný systém zálohování. Podporuje replikaci v reálném čase, okamžité obnovení dat, uchování až 32 verzí zálohovaných souborů, filtrování obsahu v rámci jedné složky. Výběr souborů je určen buď velikostí, nebo typem (příponou). [32]

K funkci je zapotřebí instalace aktuální verze systému DSM 4.0 (cit.10.3.2015). Druhou nedílnou částí je instalace balíčku Cloud Station. Po instalaci lze přikročit k samotnému nastavení zařízení NAS v následujících krocích: [32]

- Přihlášení pod administrátorským účtem, spuštění aplikace Cloud Station a povolení složky uživatele. [32]
- Nastavení oprávnění uživatelů k přístupu ke službě Cloud Station. [32]
- Vytvoření složky pro ukládání záloh, aktivace sdílení složky a přidělení oprávnění přístupu pro jednotlivé uživatele. [32]

Tím je dokončeno nastavování NAS. Druhou částí nezbytnou pro funkci zálohování je nastavení klientské aplikace. Aplikace lze stáhnout z webu nebo přímo z NAS pod záložkou Přehled – počítače. Po spuštění instalace je zobrazen průvodce obsahující jednoduché nastavení (adresa serveru, přihlašovací údaje, výběr složky synchronizované se zálohou). Přidání dalších složek je prováděno stejným způsobem - průvodcem obsaženým v klientské aplikaci. Pro zálohování dalších složek je nutno nejprve vytvořit cílovou složku na NAS. [32]

Obnovení nechtěně smazaného nebo pozměněného souboru ze zálohy lze provést přes aplikaci v PC otevřením volby „Open Cloud Station folder“. Po nalezení souboru se provede vyvolání seznamu předchozích verzí souboru tlačítkem „Browse previous version“ nacházejícím se v nabídce zobrazené po kliknutí pravým tlačítkem myši na obnovovaný soubor. Z otevřené nabídky souborů lze stáhnout libovolnou vybranou verzi. Postup záloh i obnovování u MAC je téměř totožný s PC. [32]



Obrázek 8 - otevření nabídky předchozích verzí souboru, zdroj: https://www.synology.com/img/knowledgebase/tutorials/backup_with_cloud/browseversions.png

4 Praktická část

V praktické části bude provedeno základní nastavení NAS serveru NSLU2 společnosti Linksys. Nastavení bude provedeno přes webové rozhraní a NAS bude zakomponován do domácí již zavedené počítačové sítě. Hlavním úkolem bude poskytování prostoru pro objemná data a dokumenty. Velkou výhodou bude přístup k datům prostřednictvím notebooku a mobilního telefonu zároveň a dostatečná kapacita úložného prostoru. Stávající kapacita pevného disku v notebooku byla již nedostačující. Jedna z kapitol teoretické části se věnuje nastavení zabezpečení Wi-Fi. To bude demonstrováno na přípojné bodu „Wireless – G Broadband Router, model WAP54G ver.3“ taktéž od společnosti Linksys. Závěrem bude provedeno několik testů rychlostí a vyhodnoceny výsledky.

4.1 Popis sítě a požadavků

Stávající domácí síť je postavena z těchto komponentů:

- Switch: FSD-803PE - Planet switch FSD-803PE, 8x10/100, 1x PoE 802.3af
- Wi-Fi: Wireless-G Access Point WAP54G ver. 3
- Připojení k internetu: Ubiquiti NanoBridge M5
- Tiskový server: HP JetDirect 200M
- 3x jednoduchá LAN zásuvka na kabeláži cat5e

Požadavky

Hlavním předpokladem použití NAS je uložení objemných dat (filmů, hudby, fotek) a dokumentů v domácím prostředí. Dalším důležitým požadavkem je využití stávajícího USB externího disku Western Digital Elements Desktop 3,5“ 2TB. K NAS se bude přistupovat výhradně z prostředí Windows popř. z mobilních telefonů s OS Android. Požadavky na rychlost jsou vzhledem k internetovému připojení 8Mbps a rychlosti Wi-Fi 54Mbps dosti nízké.

Klíčové parametry NAS NSLU2 znázorňuje následující tabulka.

Model	NSLU2
Standardy	IEEE 802.3, IEEE 802.3u, USB1.1, USB 2.0
Protokoly	SMB/CIFS over TCP/IP
Porty	1x 10/100Mbps RJ-45, Napájení, 2xUSB 2.0
Kabeláž	UTP cat 5 nebo lepší
Topologie	Hvězdicová
Indikace	LED: Ready/Status, Ethernet, Disk 2, Disk 1
Tlačítka	Zapínání, Reset

Tabulka 3 - základní specifikace NAS NSLU 2

4.2 Zapojení a nastavení NSLU2

Na použitém switch byl volný jeden port, pro připojení nebylo nutno instalovat další switch. K ochraně před přepětím a před výpadky byl použit UPS od společnosti APC model BK500. Do shodné UPS jsou zapojeny i pevné disky.

Zapojení a připojení k administraci

Po zapojení HW a stisknutím tlačítka power se spustí NAS. Prvním krokem je dočasné nastavení IP adresy na notebooku, aby bylo možno přistupovat do webové administrace. Výchozí adresa NAS je 192.168.1.77, pokud síť používá stejný rozsah, není nutno IP na notebooku měnit. Pokud síť používá jiný rozsah, dočasně nastavíme na notebooku adresu 192.168.1.1. Tím je zajištěn základní předpoklad pro komunikaci NAS a notebooku, ze kterého bude provedena administrace. Po otevření webového prohlížeče a načtení adresy 192.168.1.77 se zobrazí úvodní okno na záložce Home (umožňující přístup do soukromých složek jednotlivých uživatelských skupin nebo přístup na jednotlivé disky). [30]

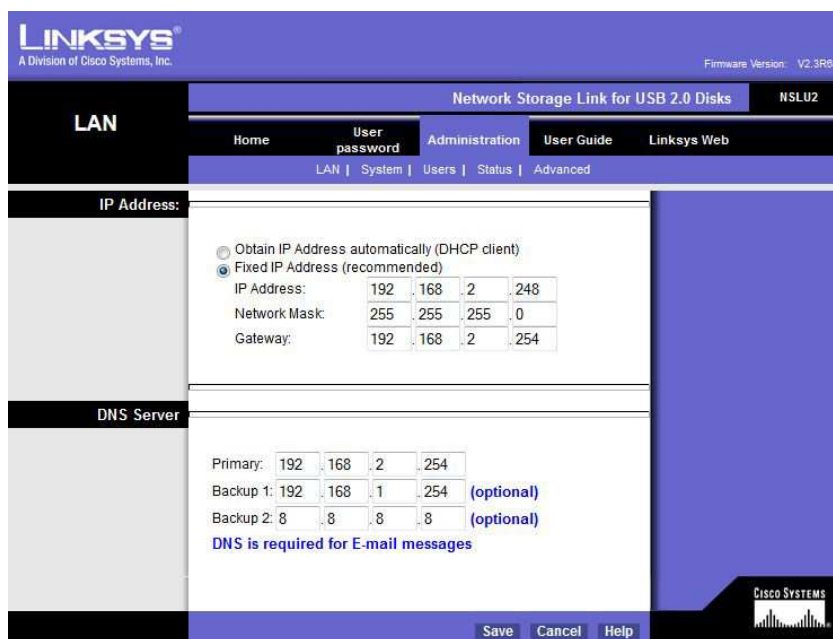
Účet administrátora

Na záložce “User password” lze měnit hesla všech uživatelů. Nejdůležitějším krokem je nyní změna administrátorského hesla z výchozího nastavení. Administrátorský účet má

uživatelské jméno: admin a výchozí heslo: admin. To okamžitě změním dle zásad tvorby silného hesla. [30]

Nastavení IP

Dalším důležitým krokem je síťové nastavení. NAS je nyní schopen komunikovat pouze s notebookem, ze kterého je prováděna administrace. Důležité je nastavit IP adresy dle rozsahů použitých v síti. Nastavení síťových parametrů je umístěno pod záložkou administrace a podzáložkou „LAN“. Pro přístup k této možnosti jsme dotázáni na uživatelské jméno a heslo. Do záložky administrace je přístup povolen pouze administrátorskému účtu. Po přihlášení administrátorským účtem je provedeno nastavení dle požadavků sítě. Pro jednoduchý přístup je zvolena statická adresa sítě - je zvolena z rozsahu, který používá celá síť, vzhledem k nemožnosti přístupu k nastavení DHCP na routeru, který je zaheslován poskytovatelem připojení k internetu. Adresa je nastavena mimo rozsah přidělováný pomocí DHCP běžícím na zařízení NanoBridge. Zde konkrétně 192.168.2.248. Pokud plánujeme používat funkce E-mail alert je nutno nastavit i adresy DNS serverů, konkrétně zde jsou shodné s výchozí bránou a jedná se o adresu routeru poskytujícího internetovou konektivitu 192.168.2.254, záložní DNS je nastaveno 8.8.8.8 – adresa Google DNS. [30]



Obrázek 9 - ukázka administrace přes web - nastavení IP

Nastavení systému

Nachází se pod záložkou administrace a podzáložkou „System“. Prvním důležitým prvkem je nastavení identifikace v síti. Zde je možno nastavit název zařízení a umístění do pracovní skupiny. Další důležitou částí je nastavení jazykové sady. Pro podporu českých znaků je zapotřebí nastavit znakovou sadu „Slavic/Latin 2 (852)“. V kategorii „Location“ je možno povolit účet host, FTP server nebo podporu UPnP. Pokud tyto funkce neplánujeme využívat, raději je z bezpečnostních důvodů necháme zakázané. [30]

Disky a diskové nástroje

Kliknutím na podzáložku „Advanced“ se přepne podnabídka do druhé části, zpět se vrátí stiskem „Setup“. V podnabídce „Advanced“ v sekci „Disk“ nalezneme nástroje pro formátování disků 1 a 2. Disky jsou schopny pracovat v systému souborů NTFS, ale po praktické zkušenosti s nefunkčností přidělování oprávnění a celkově nestandardním chováním celého NAS při použití NTFS, bych doporučoval nové disky naformátovat na výchozí systém souborů EXT3, se kterým zařízení pracuje zcela bezproblémově. NAS pracuje na upraveném systému Linux, i z tohoto hlediska je vhodnější použít EXT3. Výhody EXT3 jsou probrány v teoretické části v kapitole systémy souborů. V nabídce „Disk“ se nalézá i funkce „Scandisk“ pro nalezení a případnou opravu dat na discích. Lze také nastavit pravidelné spouštění tohoto nástroje v době, kdy je NAS nejméně využíván. Po dobu Scandisku nelze totiž na disk přistupovat. [30]

Tvorba skupin, uživatelů a přiřazení práv

K tvorbě uživatelských účtů slouží podzáložka „Users“. Při tvorbě uživatele lze kromě uživatelského jména a hesla doplnit ještě komentář. Další možností je povolení soukromé uživatelské složky a omezení maximálního množství dat v MB, která může uživatel nahrát na disk. [30]

K tvorbě skupin slouží podzáložka „Groups“. Po vytvoření skupiny do ní lze přidat/odebrat uživatele ze seznamu vytvořených uživatelů tlačítkem „Members“. [30]

Vytváření sdílených složek se nachází v podzáložce „Shares“. Seznam Složek obsahuje 4 základní nesmazatelné složky ADMIN1/2 a DISK1/2 reprezentující jednotlivé disky a

kompletní obsah přístupný pro administrátora přes administrátorský účet. Pro povolení přístupových práv ke složce slouží tlačítko „Access“. K jednotlivým složkám lze přiřadit jednotlivé skupiny uživatelů s právy Read nebo Read/Write. Tím je základní nastavení dokončeno. [30]

4.3 Doplnkové služby a funkce

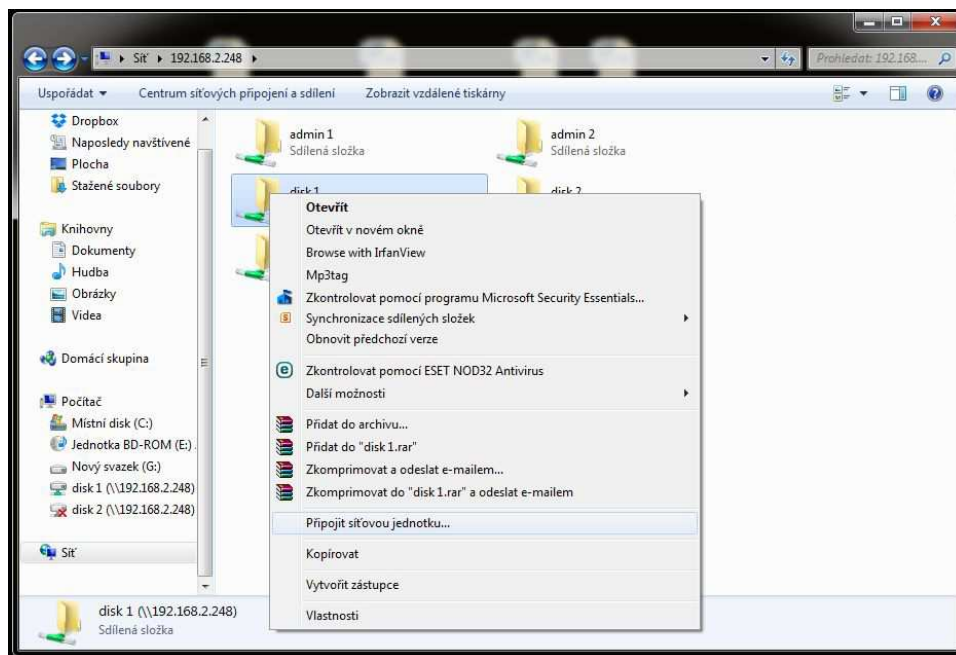
NSLU2 nepodporuje žádnou technologii RAID, částečně ji nahrazuje funkcí Drive Backup (nalezneme v podzáložce „Backup“) umožňující pravidelnou zálohu předem stanovených složek z Disku1 na Disk2. [30]

Další funkcí je možnost zálohování aktuálního nastavení a provádění aktualizací firmware. [30]

Užitečnou je i podzáložka „Status“ poskytující aktuální informace o stavu systému a zaplnění jednotlivých disků. Je zde možno plánovat pravidelný restart zařízení. Především u firemního nasazení se využije i možnost automatického zasílání informací o varování a chybách na dva nastavené e-maily. [30]

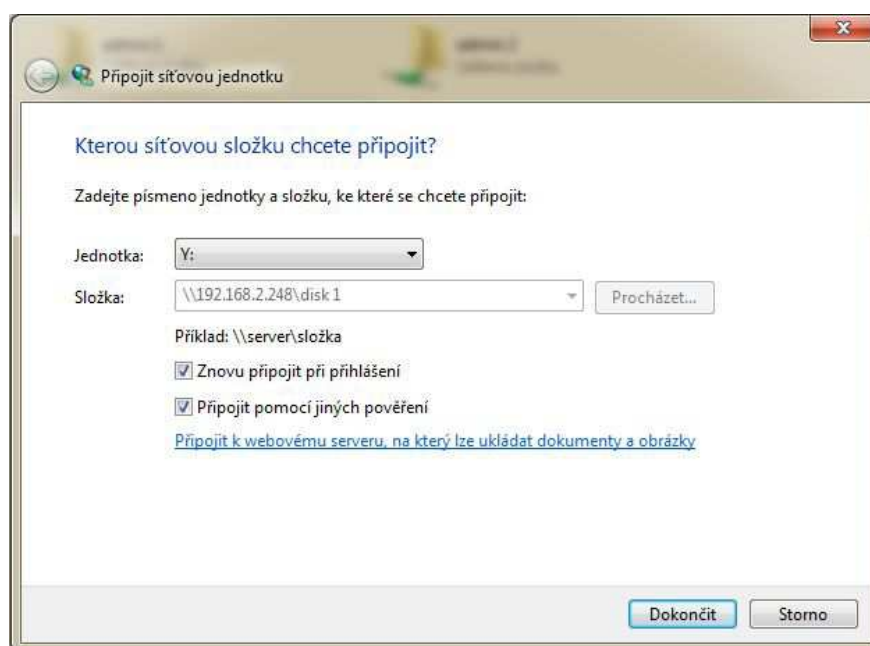
4.4 Přístup k NAS z prostředí Windows

Ke sdíleným datům se lze připojit třemi způsoby. Nejméně praktický je přístup přes webový prohlížeč po připojení na IP NASu. Tato možnost umožňuje pouze stahování a prohlížení dat. Samozřejmě je chráněna heslem. Druhou možností je přes průzkumník Windows vyhledáním NAS přes položku místa v síti. Zde se zobrazí pod svým jménem, které bylo nastaveno při úvodním nastavení. Třetí možností je přístup přímo přes IP adresu zadáním adresy do adresního řádku průzkumníku ve tvaru \\192.168.2.248. [30]



Obrázek 10 - připojení do Windows jako síťový disk

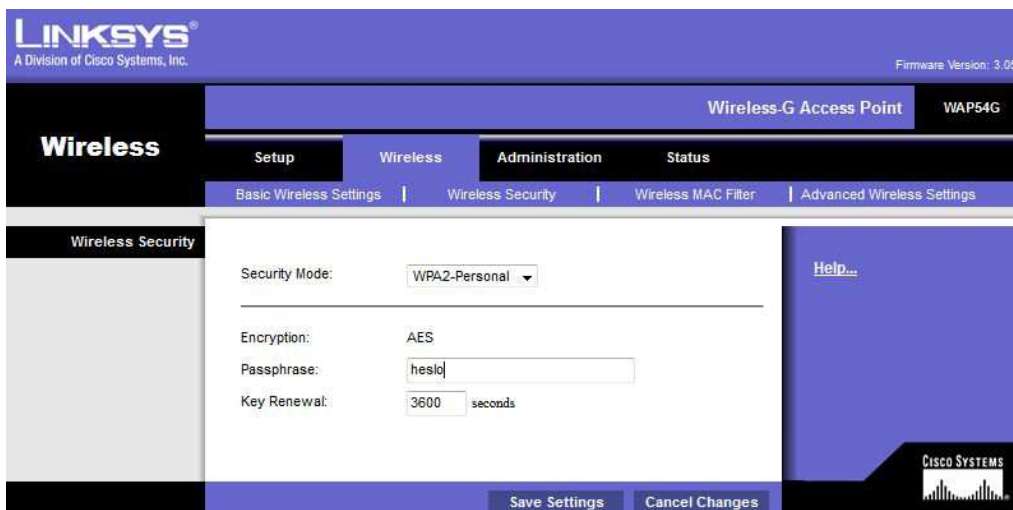
Pro trvalý přístup ke složce je možno ji připojit k PC jako síťový pevný disk možností „připojit síťovou jednotku“ vyvolané pravým kliknutím myši na složku určenou k připojení. Použití této funkce umožňuje uložení uživatelského jména a hesla a automatické připojení vždy, když je složka přístupná. [30]



Obrázek 11 - nastavení názvu disku

4.5 Nastavení zabezpečení Wi-Fi

Přihlášení do administrace Wi-Fi přípojného bodu je nejjednodušší přes webový prohlížeč přes IP zařízení (příklad: //192.168.2.249). Po přihlášení se objeví okno s přihlášením k administraci. Přihlášení je ve výchozím stavu bez uživatelského jména s heslem „admin“. V záložce „Administration“ okamžitě nastavíme nové heslo dle zásad bezpečného hesla probraných v teoretické části. Nastavení SSID, druhu sítě, IP přeskočím, to není předmětem této práce. Další krok je nastavení zabezpečení Wi-Fi. Zabezpečení se nachází v záložce „Wireless“ a podzáložce „Wireless Security“. V rozklikávacím boxu „Security mode“ je možno vybrat požadovaný způsob zabezpečení. Dle rozboru zabezpečení v praktické části je nejlepší volbou zabezpečení pro domácnost WPA2-Personal (používá pouze algoritmus AES). Do okénka „Passphrase“ vypíšeme klíč pro připojení, opět podle zásad tvorby silného hesla. [31]



Obrázek 12 - příklad administrace WAP54G - nastavení zabezpečení

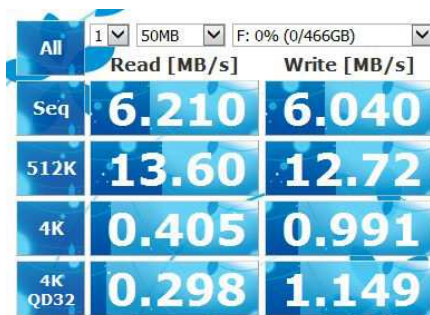
Vzhledem k velké síle šifrování AES se již při běžném použití nemá cenu zabývat doplňkovými metodami jako filtrování MAC atd. Filtrování MAC je dobré použít, například pokud je potřeba blokace jednotlivého uživatele bez změny přihlašovacího hesla. V tom případě v podzáložce „Wireless MAC Filter“ povolíme možnost na „Enable“, zaklikneme možnost „Prevent“ a vyplníme adresu blokováného uživatele. [31]

4.6 Testy rychlostí

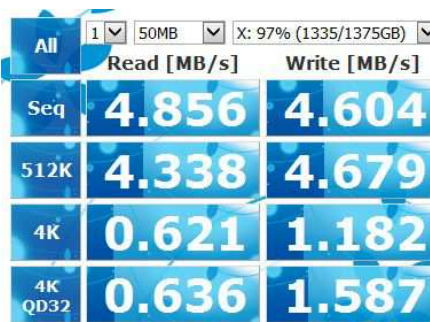
Testování rychlostí bylo prováděno programem CrystalDiskMark 3.0.3b. Aplikace provádí test zápisu a čtení pomocí 50MB souboru. Byl proveden celkem 4x. Poprvé byl prováděn přímo na HDD připojeném k PC přes sběrnici USB2.0, podruhé na HDD připojeném k NAS a připojení notebooku na LAN síť. Potřetí při připojení notebooku přes Wi-Fi se zabezpečením WPA2. Poslední je test HDD přímo v PC pro porovnání. Souhrn výsledků testu zobrazuje následující tabulka. Proveden bude také test vlivu zabezpečení bezdrátové sítě a vliv použitého komunikačního protokolu na rychlost přenosu.

Typ připojení	Čtení (MB/s)	Zápis (MB/s)
Interní disk	95,34	89,41
USB 2.0	6,210	6,040
LAN	4,856	4,604
Wi-Fi	1,095	1,243

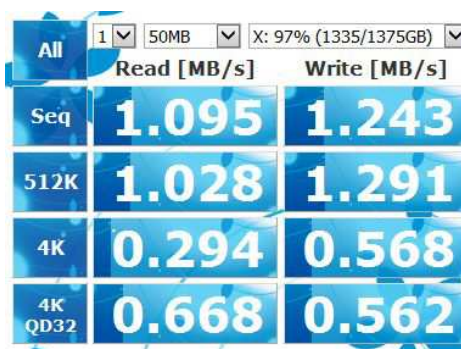
Tabulka 4 - srovnání klíčových rychlostí zápisu a čtení



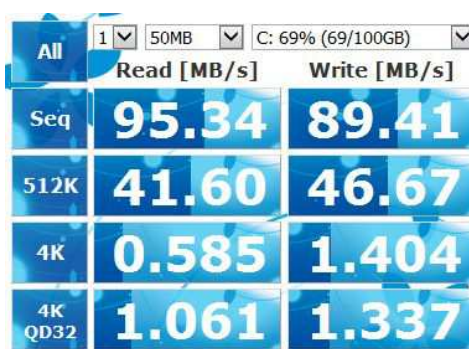
Obrázek 13- -Rychlost čtení a zápisu, připojení přes USB 2.0



Obrázek 14 - Rychlost čtení a zápisu, připojení přes LAN 100mbps



Obrázek 15 - Rychlost čtení a zápisu, připojení přes Wi-Fi 54mbps



Obrázek 16 - Rychlost čtení a zápisu, interní disk v notebooku

Vliv změny nastavení zabezpečení byl testován zápisem a čtením souboru přes průzkumník Windows. Síla signálu byla dle Windows ukazatele maximální (vzdálenost notebooku a AP cca 50cm). Vzhledem k velmi nízké přenosové rychlosti byla vyzkoušena komunikace i na jiných kanálech kvůli zarušení, dokonce na jiném AP stejného modelu. Opět se stejnými výsledky.

Zabezpečení:	Rychlost zápisu (MB/s)
Zakázáno	1,3
WEP 64 bit	1,25
WPA TKIP	1,2
WPA2 AES	1,1

Tabulka 5 - vliv zabezpečení Wi-Fi na rychlost komunikace s NAS

Použitý NAS NSLU2 podporuje pouze protokoly FTP, CIFS a HTTP (pouze čtení). Test proběhl s připojením přes 100mbps LAN a Wi-Fi 54mbps (šifrování WPA2 AES) zápisem a čtením 50MB souboru přes program Total Commander (x64) verze 8.01.

Protokol	Zápis (MB/s)	Čtení (MB/s)
FTP (LAN)	2,8	5,1
CIFS (LAN)	4,2	4,6
HTTP (LAN)	nepovoluje	4,7
FTP (Wi-Fi)	0,7	1,1
CIFS (Wi-Fi)	1,1	1,1
HTTP (Wi-Fi)	nepovoluje	0,9

Tabulka 6 - Vliv komunikačních protokolů na rychlosti zápisu/čtení

Porovnáním výsledků je zjištěn podstatný rozdíl mezi protokolem FTP a CIFS při zápisu dat s připojením jak na LAN tak na Wi-Fi. Při čtení dat nebyl mezi všemi testovanými protokoly výraznější rozdíl. Vliv připojení odpovídá i předchozím měřením vlivu připojení programem CrystalDiskMark.

Porovnáním výsledků testu zjistíme, že klíčovým hlediskem ovlivňujícím rychlost je způsob připojení klienta k síti, ve které se nachází NAS. Při srovnání s interním HDD je rychlost externích disků a testovaného NAS přibližně o jeden řád nižší. Samotný NAS při připojení USB disku komunikaci nijak výrazně neomezuje. Drobný rozdíl rychlostí je způsoben nízkým výpočetním výkonem použitého NAS (obsahuje procesor taktovaný pouze na 266MHz a RAM 32MB). Největším omezujícím faktorem bylo Wi-Fi připojení. Zkoumán byl i vliv změny vysílacího kanálu z důvodu případného omezování rychlosti vlivem zarušení. Změna kanálu, ani změna typu zabezpečení nepřinesla výraznou změnu rychlosti. Rychlostní omezení je pravděpodobně způsobeno nedostatečným výkonem samotného Wi-Fi routeru nebo chybou ovladače bezdrátové karty v notebooku HP probook 4525s, na kterém byly testy prováděny.

4.7 Diskuze

Instalace NAS zařízení přináší řadu výhod. Mezi hlavní z nich patří mobilní přístup k souborům a přístup z mnoha různých zařízení, bez kopírování dat, či přenášení a přepojování disků. Umístěním dat na discích stabilně uložených na bezpečném místě z hlediska mechanického poškození, se značně eliminuje riziko poškození případným úderem či pádem disku. Zvýší se také komfort s přenášením notebooku. Některé mobilní telefony sice podporují připojení externího paměťového média přes USB, NAS ale možnost přístupu k diskům rozšiřuje na mnohem širší spektrum modelů a zvyšuje mobilitu. Dalším nepřehlédnutelným aspektem je možnost zálohování dat nebo celých systémů včetně nastavení, sdílení kalendáře a poznámek. Zajištění bezpečnosti dat buď geografickou redundancí, nebo pomocí RAID pole. Možnost zálohování a zvýšení zabezpečení dat využijí především živnostníci a firmy.

Nevýhod použití NAS není mnoho. Mezi to málo z nich patří vyšší pořizovací cena oproti samotným diskům. Další nevýhodou je snazší napadnutí dat z internetu, které lze minimalizovat aplikací dostatečného zabezpečení a proškolením uživatelů. Posledním záporným faktorem je snížení rychlosti, kterému lze předejít vhodnou volbou zařízení NAS a konfigurací sítě.

Celkově lze hodnotit NAS jako obrovský přínos. Několik výše uvedených nevýhod je zcela převáženo spoustou výhod, které jednoznačně hovoří pro zavedení NAS jak v domácnosti, tak ve firemním prostředí.

Cenová kalkulace testovaného řešení a časová náročnost

Komponent:	Cena (Kč)
NAS NSLU (bazar)	450
Switch Planet 8 port (bazar)	350
AP WAP54G (bazar)	250
Kabel cat5e 60m	420
Drobný materiál	200
Disk WD Elements USB 2.0, 2TB	2700
Disk WD Elements USB 2.0 1,5TB	2200
UPS APS BK500 (bazar)	400
Akumulátor 7Ah/12V	490
Celková suma	7460

Tabulka 7 - Cenová kalkulace testované sestavy

Většina komponentů testované sestavy byla nakupována již použitá, z důvodu nízkého studentského rozpočtu. Pevné disky, switch a AP jsem vlastnil již před instalací NAS a tak samotná instalace NAS a zapojení pevných disků do sítě stála 1440Kč včetně zabezpečení proti výpadku energií pomocí UPS.

HW instalace trvala okolo jedné hodiny a spočívala v instalaci kabeláže mezi místností se switch a NAS, zapojení UPS, rozbočovacího kabelu napájení, připojení NAS a pevných disků. Nastavení trvalo zhruba půl hodiny. Nejvíce času zabralo formátování disků a přesun dat. Data musela být nejprve překopírována na zapůjčené disky. Provedeno formátování na EXT3 a poté data nahrána zpět na původní disky. Při objemu dat přes 2TB tato činnost probíhala několik dní.

Cenová kalkulace firemního NAS pro menší firmu

Komponent:	Cena (Kč)
Synology Disk Station DS214+	8990
2x Disk WD Red 2TB	2x2999
APC Back-UPS 400	1059
Kabeláž a drobný materiál	300
Celková suma	16347

Tabulka 8 - cenová kalkulace NAS pro menší až střední firmu

Zvolený NAS podporuje RAID 0/1, šifrování disků, sdílení dat, zálohování a nespočet dalších funkcí plně postačujících pro menší až střední firmu. Velikost pevných disků byla zvolena 2x2TB. Celková kapacita je tedy 1/4TB dle zvoleného režimu RAID.

Cenová kalkulace firemního NAS pro náročné použití

Komponent:	Cena (Kč)
Synology Disk Station DS2413+	35790
4x Disk WD Red 3TB	4x3749
APC Back-UPS 400	1059
Kabeláž a drobný materiál	300
Celková suma	52145

Tabulka 9 - cenová kalkulace NAS pro náročné použití u velké firmy

Toto řešení neplní pouze funkci NAS, ale kompletní serverové firemní řešení s vysokým nárokem na objemy dat. Plně nahrazuje podnikové servery. V základu pojme až 48TB dat (s rozšiřovací jednotkou až 96TB). Podporuje použití RAID 0,1,5,6,10. Pojme až 12 pevných disků o kapacitě 4TB. V kalkulaci je počítáno se čtyřmi 3TB disky. Je vybaveno duálním gigabitovým síťovým rozhraním. Díky podpoře iSCSI se jedná se o ideální alternativu SAN řešení i pro velké podniky. Podporuje také virtualizační nástroje Vmware vSphere 4, Microsoft Hyper-V, Citrix Ready.

Široká nabídka NAS pokrývá veškeré uživatelské potřeby od sdílení filmů v domácnosti až po složitá firemní řešení. Tomu odpovídá i cena pohybující se v rozmezí od několika tisíc korun až po řešení v řádu desítek až stovek tisíc.

5 Závěr

Cílem práce bylo teoreticky probrat a analyzovat zvolenou tematiku NAS se zaměřením na souborové systémy, komunikační protokoly, zabezpečení dat proti ztrátě, krádeži a využití pro zálohování dat. Možností, jak docílit spolehlivého a bezpečného provozu NAS splňujícího všechny uživatelské požadavky na funkčnost, je nespočet. Je důležité si předem důkladně promyslet, jaké funkce od zařízení budou požadovány a podle toho zvolit vhodný produkt. Z hlediska zabezpečení existuje mnoho účinných způsobů, avšak žádný není stoprocentní a nikdy není zabezpečení úplně dokonalé. Nejdůležitějším a nejrizikovějším bezpečnostním faktorem je doposud uživatel samotný.

Vzhledem k nepřebernému množství funkcí, které NAS podporují, napříč cenovým spektrem od těch nejlevnějších až po profesionální řešení, se NAS hodí jako vhodný způsob sdílení dat, zálohování a provoz doplňkových služeb.

Při tvorbě této práce jsem získal mnoho užitečných poznatků a zkušeností, především v oblasti systému souborů a komunikačních protokolů. Ačkoliv vlastním NAS již několik let, až nyní jsem zcela pochopil všechny možnosti a porozuměl jeho funkcím a možnostem nastavení. Věřím, že získané informace a zkušenosti uplatním při dalším vzdělávání i v profesním životě.

6 Seznam použitých zdrojů

1. PTÁČNÍK Jiří. Kam ukládat filmy, hudbu a fotky? Na datové úložiště NAS. *digilici.cz*. [online]. 4.4.2013 [cit. 2015-02-06]. Dostupné z: <http://www.digilidi.cz/datove-uloziste-nas>
2. JUNEK Pavel. Zálohování a archivace dat v podnikovém prostředí. *zalohovani.net*. [online]. 28.8.2013 [cit. 2015-02-06]. Dostupné z: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-4-dil-datova-uloziste/>
3. KEJDUŠ Radek. Úvod do NAS serverů – Váš domácí cloud. *pctuning*. [online]. 9.5.2011 [cit. 2015-02-06]. Dostupné z: <http://pctuning.tyden.cz/software/zalohovani-zachrana-dat/20780-uvod-do-nas-serveru-vas-domaci-cloud?start=3ziste/>
4. Velký průvodce výběrem NAS serveru. *CZC: rozumíme vám i elektronice*. [online]. 16.4.2013 [cit. 2015-02-06]. Dostupné z: <http://www.czc.cz/velky-pruvodce-vyberem-nas-serveru/clanek>
5. BEAL Vangie. NAS – Network Attached Storage. *Webopedia*. [online]. 12.9.2013 [cit. 2015-02-06]. Dostupné z: http://www.webopedia.com/TERM/N/network-attached_storage.html
6. KÁLLAY, Fedor. Počítačové sítě LAN/MAN/WAN a jejich aplikace. 2. aktualiz. vyd. Praha: Grada, 356 s. ISBN 80-247-0545-1
7. ROUSE Margaret. Common Internet File System (CIFS) definition. *TechTarget*. [online]. 2005 [cit. 2015-02-08]. Dostupné z: <http://searchstorage.techtarget.com/definition/Common-Internet-File-System-CIFS>
8. ROUSE Margaret. Network File System (NFS). *TechTarget*. [online]. 2005 [cit. 2015-02-08]. Dostupné z: <http://searchenterprisedesktop.techtarget.com/definition/Network-File-System>
9. MACHACKOVA Zuzana. NFS – Síťový souborový systém. *PIT*. [online]. 12.11.2001 [cit. 2015-02-08]. Dostupné z: <http://pit.wz.cz/nfs.php>
10. Zálohování dat z NAS serveru Synology na jiný server (DSM 4). *Synology: Znalostní databáze*. [online]. neznámé [cit. 2015-03-10]. Dostupné z: <https://www.synology.com/cs-cz/knowledgebase/tutorials/461>
11. JANOVSKEJ Dušan. HTTP protokol. *Jak Psát Web*. [online]. 4.5.2005 [cit. 2015-02-08]. Dostupné z: <http://www.jakpsatweb.cz/server/http-protokol.html>
12. GRABHAM Dan. DLNA: what it is and what you need to know. *techradar*. [online]. 22.3.2013 [cit. 2015-02-08]. Dostupné z:

<http://www.techradar.com/news/digital-home/home-networking/dlna-what-it-is-and-what-you-need-to-know-1079015>

13. BUCHTA Martin. DLNA pro začátečníky – jak doma sdílet videa, fotografie, hudbu. *AVmania*. [online]. 11.2.2013 [cit. 2015-02-08]. Dostupné z: <http://avmania.e15.cz/dlna-pro-zacatecniky-jak-doma-sdilet-video-fotografie-hudbu>
14. ROUSE Margaret. storage area network (SAN) definition. *TechTarget*. [online]. 2005 [cit. 2015-02-08]. Dostupné z: <http://searchstorage.techtarget.com/definition/storage-area-network-SAN>
15. Šifrování sdílených složek na NAS serverech Synology. *Synology: Znalostní databáze*. [online]. neznámé [cit. 2015-03-10]. Dostupné z: <https://www.synology.com/cs-cz/knowledgebase/tutorials/455>
16. Software-RAID 0,1,5,6,10 – srovnání rychlostí. *ABC Linuxu*. [online]. 12.9.2007 [cit. 2015-03-10]. Dostupné z: <http://www.abclinuxu.cz/blog/MartinT/2007/9/software-raid-0-1-5-6-10-srovnani-rychlosti>
17. NTFS — New Technology File System. *NTFS.com*. [online]. 2015 [cit. 2015-02-12]. Dostupné z: <http://www.ntfs.com/ntfs.htm>
18. MGR.MRÁZEK, L. Operační systémy. Systém souborů, koncepce souboru [online]. 2007 [cit. 2015-02-12]. Dostupné z: <http://homen.vsb.cz/~kod31/vyuka/opsys/os.html>
19. VESELÍK, Patrik. Data v suchu pro každého: obecné trendy v ukládání a zálohování dat. *Connect!* 12(12/12):12-13, 2007
20. GIANLUCA. UPS jako součást zálohování. *GTblog*. [online]. 10.3.2010 [cit. 2015-02-14]. Dostupné z: <http://blog.gtweb.cz/2010/hardware/ups-jako-soucast-zalohovani>
21. NATARAJAN Ramesh. RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams. *The Geek Stuff*. [online]. 10.8.2010 [cit. 2015-02-14]. Dostupné z: <http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/>
22. KOČMÁNEK Vít. Přehled všech režimů RAID. *Živě.cz*. [online]. 2.4.2003 [cit. 2015-03-09]. Dostupné z: <http://www.zive.cz/clanky/prehled-vsech-rezimu-raid-rychlejsi-a-bezpecnejsi-ukladani-dat/raid-0-1-01/sc-3-a-111138-ch-27725/default.aspx#articleStart>
23. Mechanicky poškozený harddisk (fyzické poškození). *My Blue Day*. [online]. 2008 [cit. 2015-02-14]. Dostupné z: <https://www.zachrana-harddisku.cz/cz/mechanicke-poskozeni-harddisku.asp>
24. TUHÝ Radan. NAS: Jak na firewall a zabezpečení? – Úvod, jednotlivé oblasti, na které se zaměříme. *Svět Hardware: vše ze světa počítačů*. [online]. 28.6.2013 [cit. 2015-02-14]. Dostupné z: <http://www.svethardware.cz/nas-jak-na-firewall-a-zabezpeceni/37842>
25. TUHÝ Radan. NAS: Jak na firewall a zabezpečení? – Uživatelské účty a práva, hesla. *Svět Hardware: vše ze světa počítačů*. [online]. 28.6.2013 [cit. 2015-02-

- 14]. Dostupné z: <http://www.svethardware.cz/nas-jak-na-firewall-a-zabezpeceni/37842-2>
26. TUHÝ Radan. NAS: Jak na firewall a zabezpečení? – Sdílení a pravidla oprávnění. *Svět Hardware: vše ze světa počítačů*. [online]. 28.6.2013 [cit. 2015-02-14]. Dostupné z: <http://www.svethardware.cz/nas-jak-na-firewall-a-zabezpeceni/37842-3>
27. TUHÝ Radan. NAS: Jak na firewall a zabezpečení? – Aktualizace firmware a aplikací. *Svět Hardware: vše ze světa počítačů*. [online]. 28.6.2013 [cit. 2015-02-14]. Dostupné z: <http://www.svethardware.cz/nas-jak-na-firewall-a-zabezpeceni/37842-4>
28. PATEJTL. Zabezpečení wifi sítí. *SOOM.cz: we make the internet better*. [online]. 26.12.2008 [cit. 2015-02-17]. Dostupné z: <http://www.soom.cz/clanky/1048-Zabezpeceni-wifi-siti>
29. PATEJTL. Zálohovací služby. *WA: web application*. [online]. 2007 [cit. 2015-02-17]. Dostupné z: <http://www.wa.cz/index.php?page=zaloha>
30. CISCO. USER GUIDE Network Storage Link for USB 2.0 Disk Drives. *CISCO*. [online]. 2007 [cit. 2015-02-19]. Dostupné z: http://downloads.linksys.com/downloads/userguide/NSLU2-EU_V10_UG_D-WEB.pdf
31. CISCO. USER GUIDE Wireless-G Access Point WAP54G. *CISCO*. [online]. 2005 [cit. 2015-02-19]. Dostupné z: http://downloads.linksys.com/downloads/userguide/1224638995107/WAP54G-EU-LA-UK_V3_user_guide_Rev_NC_web,0.pdf
32. Postup zálohování dat na počítači / Mac pomocí aplikace Cloud Station. *Synology: Znalostní databáze*. [online]. neznámé [cit. 2015-03-10]. Dostupné z: <https://www.synology.com/cs-cz/knowledgebase/tutorials/637>

7 Seznam obrázků

Obrázek 1 - Znázornění rozložení a struktury dat u metody RAID 0, zdroj: http://recuperacionraid.com/wp-content/uploads/2012/07/Recuperacion-de-datos-de-arreglo-RAID-0.jpg	15
Obrázek 2 - Znázornění rozložení a struktury dat u metody RAID 1, zdroj: http://recuperacionraid.com/wp-content/uploads/2012/07/4566967115_16846e9d58_o.jpg	16
Obrázek 3 - Znázornění rozložení a struktury dat u metody RAID 0+1, zdroj: http://zive.v.mfstatic.cz/Files/Obrazky/2003/4/RAID/graf3.gif	16
Obrázek 42 - Znázornění rozložení a struktury dat u metody RAID 1+0, zdroj: https://orlandoolguin.files.wordpress.com/2010/06/raid_1_0.jpg	17
Obrázek 5 - Znázornění rozložení a struktury dat u metody RAID 3, zdroj: http://zive.v.mfstatic.cz/Files/Obrazky/2003/4/RAID/graf6.gif	18
Obrázek 6 - Znázornění rozložení a struktury dat u metody RAID 5, zdroj: http://abeggi.altervista.org/blog/raid5.gif	18
Obrázek 7 - Shrnutí a potvrzení nastavení záloh u NAS Synology, zdroj: https://www.synology.com/img/knowledgebase/tutorials/backup_DiskStation_to_another_server/Snap7.png	27
Obrázek 8 - otevření nabídky předchozích verzí souboru, zdroj: https://www.synology.com/img/knowledgebase/tutorials/backup_with_cloud/browseversions.png	29
Obrázek 9 - ukázka administrace přes web - nastavení IP	32
Obrázek 10 - připojení do Windows jako síťový disk.....	35
Obrázek 11 - nastavení názvu disku	35
Obrázek 12 - příklad administrace WAP54G - nastavení zabezpečení.....	36
Obrázek 13- -Rychlost čtení a zápisu, připojení přes USB 2.0	37
Obrázek 14 - Rychlost čtení a zápisu, připojení přes LAN 100mbps.....	37
Obrázek 15 - Rychlost čtení a zápisu, připojení přes Wi-Fi 54mbps	38
Obrázek 16 - Rychlost čtení a zápisu, interní disk v notebooku.....	38

8 Seznam tabulek

Tabulka 1 - vliv velikosti bloku na max. velikost souboru a oddílu.....	12
Tabulka 2 - Vliv typu RAID pole na rychlost čtení a zápisu, zdroj: http://www.abclinuxu.cz/blog/MartinT/2007/9/software-raid-0-1-5-6-10-srovnani-rychlosti	19
Tabulka 3 - základní specifikace NAS NSLU 2.....	31
Tabulka 4 - srovnání klíčových rychlostí zápisu a čtení.....	37
Tabulka 5 - vliv zabezpečení Wi-Fi na rychlost komunikace s NAS.....	38
Tabulka 6 - Vliv komunikačních protokolů na rychlosti zápisu/čtení.....	39
Tabulka 7 - Cenová kalkulace testované sestavy.....	41
Tabulka 8 - cenová kalkulace NAS pro menší až střední firmu	42
Tabulka 9 - cenová kalkulace NAS pro náročné použití u velké firmy.....	43