Konfigurace aktivních síťových prvků finanční instituce

Configuration of active network elements for a financial institution

Bc. Jiří Klimeš

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jiří KLIMEŠ**
Osobní číslo:	**A10424**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Konfigurace aktivních síťových prvků finanční instituce**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Navrhněte topologii sítě finanční instituce s ohledem na požadavek stálé dostupnosti serverové aplikace.**
3. **Zdůvodněte výběr použité technologie WAN, navrhněte alternativy.**
4. **Vypracujte návrh kompletní konfigurace aktivních síťových prvků Cisco se zaměřením na AAA, HSRP, SNMP, TACACS a ACL.**
5. **Analyzujte bezpečnostní rizika uvedeného řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ODOM, Wendell. CCNP route: 642-902 Official Certification Guide. Indianapolis: Cisco Press, 2010. ISBN 978-1587202537.**
2. **TRULOVE, James. Site LAN. Praha: Grada Publishing, 2009. ISBN 978-8024720982.**
3. **HUCABY, David. CCNP switch: 642-813 Official Certification Guide. Indianapolis: Cisco Press, 2010. ISBN 978-1587202438.**
4. **WALLACE, Kevin. CCNP tshoot: 642-832 Official Certification Guide. Indianapolis: Cisco Press, 2010. ISBN 978-1587058448.**
5. **LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.**

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá návrhem konfigurace aktivních síťových prvků společnosti Cisco s důrazem na zabezpečení a dostupnost serverové aplikace finanční instituce. V teoretické části práce jsou popsány protokoly TACACS, HSRP a SNMP pro zajištění bezpečnosti a dostupnosti. Další prostor je věnován možným WAN řešením pro přístupové linky ke směrovačům.

Praktická část rozvíjí teoretický popis a uvádí konkrétní příkazy pro konfiguraci s ohledem na zadání práce. Mimo protokoly a technologie uvedené v části I je zde pro úplnost navržena konfigurace směrování s využitím protokolů BGP verze 4 a EIGRP.

Klíčová slova: zabezpečení, dostupnost, Cisco, AAA, SNMP, TACACS, HSRP, BGPv4, SSH, OOB

ABSTRACT

This thesis deals with the configuration of active network elements from Cisco systems, with emphasis on a security and availability of a server application used by a financial institution. Theoretical part describes various protocols such as TACACS, HSRP and SNMP ensuring availability and security. Another space is devoted to possible solutions for WAN access links to the routers.

The practical part develops a theoretical description and provides specific commands for a configuration with respect to the assignment of work. In addition to protocols and technologies listed in part I, there is design proposal for routing using BGP version 4 and EIGRP.

Keywords: security, availability, Cisco, AAA, SNMP, TACACS, HSRP, BGPv4, SSH, OOB

Tímto bych chtěl vyjádřit poděkování pro Ing. Miroslava Matýska, Ph.D. za odborné rady a vedení při tvorbě práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Již od počátku 90. let dochází k prudkému rozvoji komunikačních technologií. Tento trend byl nejvíce zřetelný zejména v oblasti bezdrátových komunikací a to s rozvojem sítí NMT a později GSM. Pozadu nezůstávají ani klasické telekomunikační technologie, které jsou reprezentovány technologiemi ATM a ISDN.

Zároveň dochází k rozšíření osobních počítačů do oblastí, kde to dříve nebylo myslitelné nebo těžce realizovatelné. Miniaturizace, velkokapacitní výroba a nárůst výkonu vedly ke zvýšené poptávce nejenom z oblasti státního, ale i soukromého sektoru. Bylo to dáno i faktem, že společnost IBM zveřejnila architekturu svého osobního počítače a firma Microsoft zase uvolnila definici rozhraní pro uživatelské programy. Počítače již byly dostatečně výkonné na to, aby mohly zajistit požadavky uživatelů a přitom tak malé, že mohly být na stole v kanceláři.

Postupem času však vznikla potřeba sdílet jak informace, tak i periferní zařízení (např. tiskárny). Na trhu se tedy objevují první síťová řešení pro fyzické propojení počítačů. Jedná se o technologie Ethernet, ARCnet a Token Ring. Každá má svoje výhody a nevýhody, ale z hlediska dalšího vývoje a nasazení se ukázalo, že nejdůležitější bylo předání specifikace do rukou nezávislé standardizační instituce.

Síťové technologie se dnes používají prakticky ve všech odvětvích lidské činnosti a jsou na ně kladeny velké požadavky. Často jsou na nich závislé kritické aplikace. Tato práce má tedy za cíl popsat mechanismy a trendy, které jsou v současnosti používány pro zabezpečení aktivních prvků sítě. Zabývá se také návrhem redundantního řešení pro případ, kdy dojde k selhání hardwaru.

I. TEORETICKÁ ČÁST

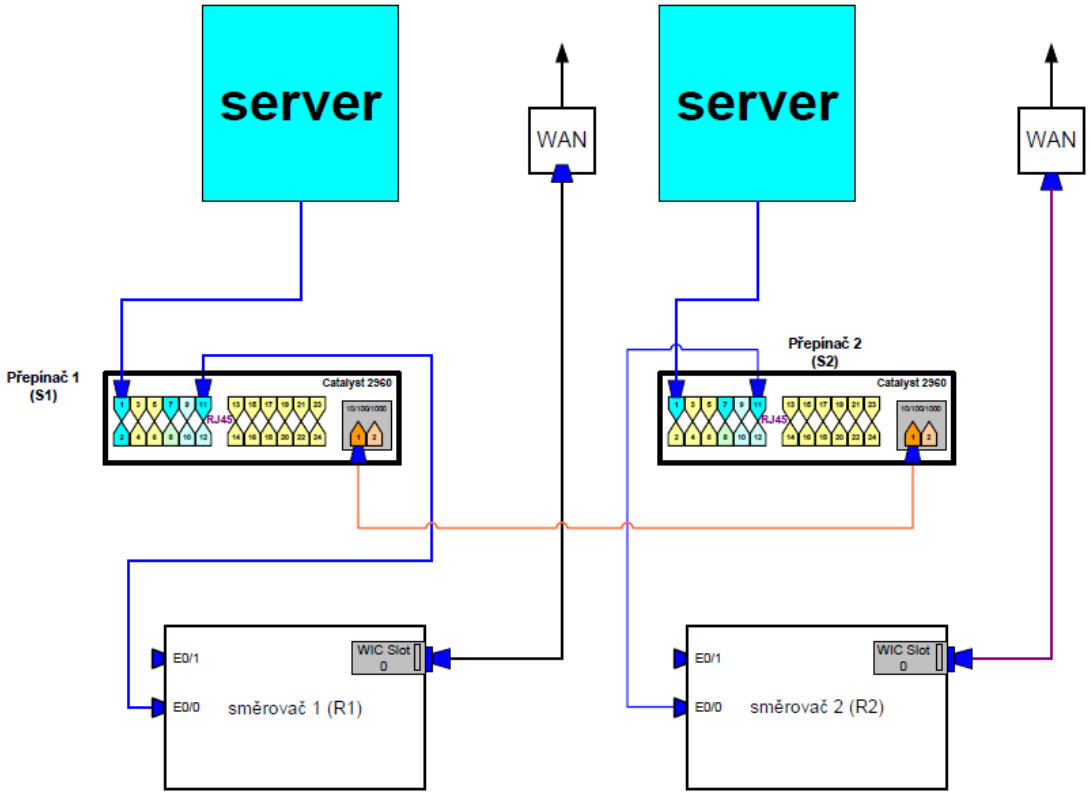
1 NÁVRH TOPOLOGIE A WAN TECHNOLOGIE

Při návrhu sítě pro nějakou instituci, ať už se jedná o školu nebo nadnárodní finanční korporaci, je třeba vždy vycházet z konkrétních požadavků zákazníka a řešení dodat tzv. na míru. Navržené řešení se také odvíjí od toho, jak moc zákazník chce nebo může investovat. Nelze požadovat nadstandardní zabezpečení s neustálou dostupností při minimálních nákladech. Vzhledem k tomu, že je téma práce zadáno pro finanční instituci, budeme uvažovat, že nejsme omezeni prostředky a návrh tedy nebude limitován.

1.1 Topologie sítě s využitím redundantních prvků

Výchozím zadáním je stálá dostupnost serverové aplikace, ke které se přistupuje z „venkovního prostředí“- např. MPLS (Multiprotocol Label Switching) sítě. Může se jednat o kritickou aplikaci, kde probíhají bankovní transakce. V tomto případě je tedy kladen požadavek na zabezpečení a zejména redundanci. Server je zapojený do přepínače a ten následně do směrovače. I přes sebelepší zabezpečení nejsme chráněni proti situaci, kdy dojde k selhání hardwarového vybavení (např. dojde k poškození větráku nebo zdroje). Z tohoto důvodu je tedy nutné, i přes zvýšené náklady, zařadit redundantní prvky. Vložená investice je řádově menší než případné škody, kdy dojde k selhání a nejsou k dispozici záložní prvky.

Z výše zmíněných důvodů byla navržena topologie, kdy budou servery zapojeny do dvou přepínačů a dvou směrovačů. Z velkého množství zařízení, která jsou na trhu dostupná jsem vybral Cisco Catalyst 2960 a Cisco 2811. Jedná se o zařízení, které byly uvedeny na trh již dříve a jsou odzkoušeny praxí. Pro názornost přikládám grafické znázornění návrhu topologie.



Obr. 1: Topologie sítě

Z přiloženého schématu vyplývá, že pokud dojde k výpadku přepínače 1 (nebo analogicky směrovače 1), tak uživatel může využít záložního serveru, který je připojený do přepínače 2. Může také nastat situace, kdy bude jedno z poskytovaných WAN (Wide Area Network) připojení nedostupné nebo nebude stabilní. V tom případě je důležité správně nakonfigurovat všechna zařízení tak, aby šla uživatelská data přes záložní linku připojenou ke směrovači 2.

1.2 Výběr WAN technologie

Z hlediska připojení do WAN je na výběr z několika možností. Každá má své výhody a nevýhody, někde je také výběr determinován finančními možnostmi popř. tím, zda je v místě připojení vybraná technologie dostupná.

1.2.1 ISDN

ISDN (Integrated Services Digital Network) je jednou z možností jak řešit připojení do WAN. Výhodou je poměrně velká dostupnost a velmi rychlé navazování spojení za 0,5 až 2 sekundy. Záleží, zda je hovor místní nebo mezinárodní [3]. Nevýhodou je jistá zastaralost technologie a nižší rychlosti. ISDN tudíž nelze považovat za kandidáta pro připojení hlavního směrovače, nicméně tato technologie je vhodná k připojení záložního směrovače.

Z hlediska poskytované rychlosti je důležité zmínit, že ISDN rozlišuje 2 základní typy přípojek:

- BRI (Basic Rate Interface), označována jako 2B + D;
- PRI (Primary Rate interface), označována jako 30B + D.

Přípojka 2B + D (základní přístup) znamená dva nezávislé B kanály („bearer“) o rychlosti 64 kbit/s určené pro přenos a jednoho D („delta“) kanálu o rychlosti 16 kbit/s určeného pro přenos signalizace. Přípojka 30B + D (primární přístup) znamená třicet nezávislých B kanálů o rychlosti 64 kbit/s a jeden D kanál také o rychlosti 64 kbit/s určený pro přenos signalizace. V USA a Japonsku je PRI omezeno na 23B +D [2]. Pro připojení ISDN linky do směrovače lze použít kartu HWIC-1B-U (Highspeed WAN interface Card). Doporučený kabel je RJ45 přímý (využívají se piny 3,4,5,6).

Obr. 2: karta HWIC-1B-U

1.2.2 Pronajaté linky

Další možností pro připojení do WAN je pronájem linky. Jedná se o trvalé připojení až do 2.5 Gbps a cena je závislá na požadované šířce pásma a vzdálenosti. Nevýhodou je fakt, že se platí fixní poplatek nezávisle na tom, jak je linka využívána. Pro Evropu je to například E1 – první řád Evropské PDH (plesiochronní digitální hierarchie), který se skládá z 32 časových slotů po 64 kbps, celkově tedy 2,048 Mbps (je třeba si uvědomit, že tato šířka pásma zahrnuje i časové sloty pro signalizaci). V severní Americe se používá T1, která má šířku pásma 1,544 Mbps. Samozřejmostí jsou i vyšší standarty – např. E3 (34,064 Mbps) resp. T3 (44,736 Mbps) [2].

1.2.3 Frame Relay

Frame relay je velmi oblíbená a používaná technologie, která vychází z X.25. Charakteristické je přepínání paketů, absence kontroly chyb (přenechává vyšším vrstvám) a schopnost přizpůsobení šířky pásma. Jedná se o spojově orientovanou službu – pro komunikaci tedy musí být vytvořeny virtuální okruhy (PVC - Permanent Virtual Circuit nebo SVC - Switched Virtual Circuit). Hlavní rozdíl mez PVC a SVC spočívá v tom, že PVC je zřízen trvale zatímco SVC se formuje automaticky a dočasně. Tyto virtuální okruhy jsou mezi 2 zařízeními a jsou identifikované pomocí DLCI (Data Link Connection Identifier). DLCI má lokální význam (tzn. DLCI např. 202 může být použito na více místech v síti).

Výhodou je tedy sdílený charakter této technologie a fakt, že poskytovatel i tak garantuje jistou minimální šířku pásma - tzv. CIR (Committed Information Rate). Z hlediska zadání této práce se tato technologie jeví jako nejvýhodnější pro připojení hlavního směrovače. Není tak drahá jako pronajaté linky, ale nabízí garantovanou šířku pásma, kterou lze navíc dočasně překročit dle momentálních možností a vytížení. Pro řízení toku dat se využívají bity FECN (Forward Explicit Congestion Notification), BECN (Backward Explicit Congestion Notification) a DE (Discard Eligible) [2].

1.2.4 ATM

ATM (Asynchronous Transfer Mode) pracuje na principu přepojování paketů s užitím virtuálních okruhů. Používá buňky fixní velkosti 53B (48B data + 5B režijní informace) a zabezpečuje QoS (Quality of Service) což ji činí vhodnou zejména pro služby jako je přenos hlasu a videa. Ačkoliv měla tato technologie velké ambice a předpoklady, k většímu rozšíření nedošlo. Z důvodu univerzálnosti IP protokolu nebyl důvod implementovat ATM na linkové vrstvě. Rozvoj v technologii VoIP (Voice over IP) způsobil, že integrace hlasu a dat byla možná s využitím IP, čímž se opět odstranila nutnost všude zavádět ATM. Další nevýhodou je poměrně velká složitost. ATM má svoje místo u některých vysokorychlostních spojení, kde se poskytovatelé navzájem dohodli na použití existujících ATM sítí.

Pro účely této práce jsem se z výše uvedených důvodů rozhodl nevybrat technologii ATM. I tak je ale mnoho společností, které ATM používají [2].

1.2.5 Ostatní technologie

Do této kategorie jsem zařadil technologie jako např. DSL, kabelové připojení a bezdrátové připojení. Tyto technologie se používají - některé více, některé méně, ale pro účely této práce jsem se rozhodl je nevyužít z důvodů menší spolehlivosti, nedostupnosti nebo omezené rychlosti. Zajímavé je především bezdrátové připojení prostřednictvím karet HWIC-3G-GSM[1] a HWIC-3G-CDMA[2].

---

[1] Pracuje v pásmech 850/900/1800/1900 MHz pro EDGE (Enhanced Data GSM Environment) a GPRS (General Packet Radio Service). Pro UMTS (Universal Mobile Telecommunications System) a HSDPA v pásmech 850/1900/2100 MHz

[2] Určena pro pásma 800/1900 MHz. Společnost O_2 provozuje CDMA síť v pásmu 450 Mhz (pásmo, které bylo dříve využíváno analogovými telefony sítě NMT).

2 TECHNOLOGIE PRO ZABEZPEČENÍ A REDUNDANCI AKTIVNÍCH SÍŤOVÝCH PRVKŮ

V současné době se pro zajištění redundance a bezpečnosti aktivních síťových prvků[3] nejvíce využívají následující protokoly a technologie:

- ACL (Access Control List);
- TACACS (Terminal Access Controller Access-Control System);
- SNMP (Simple Network Management Protocol);
- HSRP (Hot Standby Router Protocol);
- AAA (Authentication, Authorization and Accounting).

2.1 ACL

ACL je součástí konfigurace téměř každého síťového prvku. Používají se nejenom z bezpečnostních důvodů, ale např. i pro tzv. „route filtering“, NAT (Network Address Translation) nebo QoS. Z hlediska této práce je důležité, že pomocí ACL je možné omezit vzdálenou správu směrovače jen pro určité adresy (v rámci konfigurace „*line vty*“). Důležité jsou i bezpečnostní politiky na jednotlivých portech – např. LAN, kde mají všichni uživatelé adresy začínající 192.168, tak na příslušném portu můžeme povolit pouze tyto a všechny ostatní jednoduše zakázat. Cisco ACL má několik důležitých vlastností a charakteristik:

- používá se tzv. wildcard mask (maska opačná k tradiční masce);
- rozlišujeme „standard“ (jednodušší, vyhodnocuje pouze zdrojové adresy) a „extended“ (rozšířené) ACL (složitější, umožňuje kontrolovat jak zdrojové, tak i cílové adresy, může kontrolovat také porty (protokoly);
- ACL můžeme identifikovat pomocí čísla nebo jména;
- nová pravidla se přidávají vždy na konec seznamu;

[3] firewallové implementace nejsou součástí této práce a svým rozsahem vyžadují samostatné zpracování, např. Cisco ASA/PIX

- na konci každého ACL je vždy pravidlo, které zakazuje vše („*deny any*“);
- ACL se prochází od prvního pravidla postupně k poslednímu, pokud dojde ke shodě, tak se dále nepokračuje;
- ACL se definuje jako odchozí (outbound) nebo příchozí (inbound).

Vždy je třeba dobře zvážit jakým způsobem ACL zkomponovat (více specifická pravidla na začátek a méně specifická na konec). Dále je důležité, kde v síti a v jakém směru (in nebo out) bude ACL implementován – obecně platí, že standardní ACL se použije na blokování provozu blízko cíle a rozšířený ACL na blokování blízko zdroje [2]. Může se také stát, že u rozsáhlých konfigurací není zřetelné, z jakého důvodu je ACL zaveden a co je jeho smyslem, proto je dobré používat poznámky s vysvětlivkami uvnitř ACL (příkaz „*remark*“). Při úpravě již existujícího ACL jsou dvě možnosti. Celý se odstraní a nakonfiguruje znova. Nebo odstraníme (přidáme) konkrétní pravidlo s využitím tzv. „line numbers“.

Příklad: na portu FastEthernet 0/0 je připojený server, na který můžou přistupovat pouze zaměstnanci ekonomického úseku, kteří mají na svých pracovních stanicích nastaveny IP adresy 192.168.10.X s maskou podsítě 255.255.255.0. ACL, který povolí pouze legitimní požadavky na server a zablokuje všechny ostatní, bude vypadat následovně:

- „*ip access-list 10 permit 192.168.10.0 0.0.0.255*“;
- „*interface fastethernet 0/0*“;
- „*ip access-group 10 out*“.

ACL číslo 10 bude mít jen dvě položky (označují se jako tzv. ACE – access list entries). První propustí všechny pakety, které mají zdrojovou adresu, kde jsou první tři oktety ve tvaru 192.168.10. Pakety, které toto pravidlo nesplňují, postupují ke druhému pravidlu, což je implicitní „*deny any*“ a budou zahozeny. Jedná se o jednoduchý příklad, který ale vysvětluje podstatu ACL. Pokud by byl požadavek filtrovat internetový provoz, tak by ACL vypadal následovně:

„*ip access-list 105 deny tcp any any eq www*“.

Tento konkrétní příklad již vyžaduje použití rozšířeného ACL, protože se požaduje filtrovat specifický protokol (www filtruje porty 80 a 443). Dvě slova „*any*“ v příkazu znamenají, že se vůbec nekontroluje zdrojová a cílová IP adresa, jde pouze o internetový provoz.

2.2 AAA

Cisco IOS (Internetwork Operating System) provádí autentizaci uživatele na základě „*line vty*“ hesla (pokud je vůbec nakonfigurováno). Další možností je nakonfigurovat jednotlivé přihlašovací jména („*username*“) a k nim příslušející hesla a oprávnění (privilege level). Samozřejmostí je konfigurace hesla pro přístup do tzv. „*enable*“ módu (bez enable hesla není možná vzdálená konfigurace přes telnet nebo ssh!). To je nevýhodné pro organizace, kde je potřeba více správců daného zařízení s různými oprávněními. Z hlediska řízení přístupu na zařízení by bylo jednodušší mít centralizovanou správu uživatelských účtů. Dále je poměrně běžný požadavek, aby bylo možné zpětně zjistit kdo, kdy a jak zařízení konfiguroval. To je důvod proč se zavádí AAA.

„AAA je zkratka označující autentizaci, autorizaci a účtování. Autentizace je ověření identity uživatele autentizační autoritou (např. TACACS serverem). Autorizací se rozumí přidělení přístupových práv uživateli, který úspěšně absolvoval proces autentizace, respektive nepřidělení těchto práv uživateli, který autentizačním požadavkům nevyhověl. Účtování je sběr provozních informací o autorizovaném uživateli, typicky se jedná o údaje o přeneseném množství dat, trvání připojení k síti a identifikaci přístupového bodu, ze kterého bylo k síti přistupováno [4].“ Mezi AAA protokoly patří:

- RADIUS (Remote Authentication Dial In User Service);
- Diameter;
- Kerberos;
- TACACS;
- TACACS+.

2.2.1 TACACS+

„Protokol TACACS+, je síťový autentizační, autorizační a účtovací (AAA) protokol navržený firmou Cisco umožňující řízení a kontrolu přístupu na síťové prvky. K tomu využívá jeden nebo více centralizovaných serverů. Kontrola přístupu tedy nemusí být soustředěna v každém síťovém zařízení, ale veškerá přístupová práva mohou být uložena právě na jednom centralizovaném serveru. Tento server také obsahuje kontrolu

přístupu pro mnoho dalších síťových zařízení, čímž se výrazně usnadňuje sledování a konfigurace přístupových práv pro všechna tato zařízení. (podmínkou je fakt, že jednotlivá zařízení TACACS+ podporují). Protokol TACACS+ navazuje na svého předchůdce protokol TACACS a vylepšuje jej. Na rozdíl od původního protokolu poskytuje detailnější účtovací informace, hesla přenáší s použitím otisku MD5 (Message-Digest Algorithm, version 5) a umožňuje šifrování komunikace (v původní specifikaci TACACS se veškeré informace přenášely v otevřené podobě). Před uvedením TACACS+ vznikla ještě verze XTACACS, bylo to však jen upravení původního protokolu s přidáním možnosti AAA přes více TACACS. TACACS+ obsahuje natolik významné změny, že není zpětně kompatibilní s původním TACACS protokolem ani s rozšířeným XTACACS“ [5]. TACACS+ používá TCP (Transmission Control Protocol) port 49 zatímco TACACS a XTACACS používaly také port 49, ale UDP (User Datagram Protocol). Samotná implementace se skládá ze dvou částí:

- konfigurace síťového prvku;
- instalace a konfigurace TACACS+ serveru (např. s využitím operačního systému Linux).

„Cisco Systems poskytuje aktuální verze TACACS+ serveru pouze ve svém softwarovém balíku Cisco Secure ACS, který je ovšem licencovaný a není zdarma. Starší verze TACACS+ serveru, kdy ještě nebyly součástí CSACS, jsou volně k dispozici včetně zdrojových kódů, a tak existuje mnoho jejich modifikací“ [5]. Charakteristickým prvkem TACACS+ je fakt, že tento software má jeden konfigurační soubor (tac_plus.conf). Jeho umístění není důležité, protože cesta k tomuto souboru se předává jako parametr při spouštění serveru. Samotný konfigurační soubor má přímočarou a srozumitelnou podobu:

- pokud je nutné, aby byla komunikace mezi směrovačem a serverem šifrována, musíme v konfiguračním souboru nastavit heslo příkazem:
  key= secret ()[4];
- v případě požadavku na ukládání účtovacích informací je třeba definovat cestu k souboru, do kterého se budou účtovací informace ukládat:
  accounting file = /home/acc/tac.log;

[4] stejné heslo je třeba nastavit i na směrovači

- je možné, že se při spuštění TACACAS+ serveru výše uvedený účtovací soubor nevytvoří a je tedy nutné jej vytvořit pomocí známých příkazů „*touch*“ a „*chmod*“:
  touch /home/acc/tac.log
  chmod 666 /home/acc/tac.log;
- kontrola přihlašování správců na směrovač funguje na základě definování uživatelů a skupin v konfiguračním souboru;
- příklad definice skupiny „spravcove“, která má nejvyšší oprávnění a její heslo vyprší 31. 12. 2012:
  group = spravcove {
  login = cleartext "heslo" ()[5]
  expires = "Dec 31 2012"
  service = exec { priv-lvl = 15 }
  };
- výchozí úrovně pro tzv. „privilege levels“ jsou následující:
  - *privilege level 0* - zahrnuje příkazy *disable*, *enable*, *exit*, *help* a *logout*,
  - *privilege level 1*- výchozí úroveň pro telnet, která zahrnuje všechny dostupné příkazy v módu *router>*,
  - *privilege level 15* - zahrnuje všechny dostupné příkazy v módu *router#* (tzv. privileged EXEC mode);
- Jednotlivé uživatele přiřazujeme skupinám následujícím způsobem:
  user = jklimes {
  member = spravcove
  };
- ne vždy se musí využít definic pomocí skupin a jednotlivé uživatele lze definovat i samostatně. Pro jejich specifikaci se používají stejné příkazy jako v definici skupin:
  user = admin {
  default service = permit
  login = cleartext "adminheslo"
  };

[5] tato skupina má heslo „heslo“ uloženo v nezašifrované podobě, heslo lze uložit i šifrovaně a to příkazem „*login = des heslo*“

- takto vytvořený uživatel „admin“ má povoleny všechny možné příkazy na konkrétním zařízení. Toho bylo dosaženo použitím příkazu „*default service = permit*“. Pokud má takto uživatel všechny příkazy povoleny, lze je nyní jednotlivě zakazovat příkazem „*deny*“, který se zapisuje úplně stejně jako příkaz „*permit*“ [5].;
- pokud je požadavek na zakázání např. všech příkazů „*show*“, tak bude použita následující konfigurace:
  cmd = show {
  deny .*.

Dalším krokem je spuštění služby (daemona) TACACS+. Spuštění je doporučeno ověřit kontrolou logu a také prohledáním seznamu spuštěných procesů. Další nezbytnou podmínkou je funkční konektivita mezi aktivními síťovými prvky a jedním nebo více TACACS servery. V případě, že je použita složitější topologie je třeba dbát na správné nastavení směrování – např. statické definice s použitím příkazu „*ip route*“. Samotnou konfigurací aktivního síťového prvku se zabývá praktická část.

2.3 SNMP

SNMP je jedním ze základních nástrojů při správě sítě. Je součástí určitého standardu pro správu sítí, který je znám jako tzv. FCAPS (Fault, Configuration, Accounting, Performance, Security) model, jenž obsahuje pět oblastí správy:

- správa poruch a chyb (Fault Management);
- správa konfigurace (Configuration Management);
- účetní a evidenční správa (Accounting Management);
- správa výkonu (Performance Management);
- správa bezpečnosti (Security Management).

Obr. 3: FCAPS model

SNMP je nástroj, který umožňuje sledování a monitorování aktivních síťových prvků. Správce získá lepší představu o vznikajících problémech okamžitě (mnohem dříve než by uživatelé reportovali např. nedostupnost nějaké služby). Slouží také ke konfiguraci síťových zařízení.

SNMP funguje na principu komunikace typu klient – server. Dotazy jsou odesílány klientem na server, který provádí jejich vyhodnocení a odpověď posílá zpět. Tento protokol používá své vlastní označení pro komunikující strany:

- agent – hraje roli serveru;
- správce (manager) – stává se klientem serveru.

Jako „manager“ vystupují tzv. NMS (Network Management System). NMS je možné obecně nazvat jako stanice správy sítě. „SNMP agent je malý program implementovaný v síťovém zařízení, který má určenou databázi objektů MIB (Management Information Base) daného zařízení, o kterých může poskytovat informace. Čeká na příjem dotazu obsahující jméno objektu a vrací jeho současnou hodnotu. Mezitím monitoruje tyto objekty a sbírá informace o nich. Při příchodu dotazu na objekt, prochází celou stromovou strukturu databáze, až narazí na požadovaný objekt. Teprve pak je schopen interpretovat jeho hodnotu.

SNMP správce je složitější program, který se pravidelně ptá jednotlivých zařízení na pro něj zajímavé objekty a díky běžícímu agentovi obdrží jejich hodnoty. To vše provádí za účelem získaní a shromáždění co nejvíce informací o všech zařízeních v síti. Tyto data by si měl ukládat, aby je mohl prezentovat síťovému správci. S pravidelným dotazováním neboli „pollingem“ se v případě SNMP musí zacházet opatrně, protože ve vyšší míře může způsobit zbytečné zatížení sítě. Převážná část komunikace probíhá formou dotazu a odpovědi, ale existuje i výjimka. Jedná se o asynchronní automaticky generovanou zprávu na straně zařízení. Této zprávě se říká trap a je odeslána, pokud nastanou určité (administrátorem specifikované) podmínky. Těmi může být například hardwarový problém, ale i situace kdy ztratíme BGP (Border Gateway Protocol) „peering“ nebo jde nějaký z portů do stavu up/ down nebo down/ down [6].“

Jednou z nejdůležitějších záležitostí při správě sítě pomocí SNMP je MIB. Je nezbytný jak na straně agenta tak i na straně správce. Je to databáze objektů, které je možno sledovat a spravovat v závislosti na jejich přístupových oprávněních. Agent tuto strukturu používá k monitoringu vlastností zařízení. Následně tak může informovat dotazující se stranu. Z hlediska správce představuje množinu objektů, na které se můžeme dotazovat [7]. S MIB je možno provádět různorodé operace. SNMP nabízí dvě základní operace pro práci s objekty v databázi MIB:

- GET - tímto příkazem načítá stanice NMS od agenta požadovanou instanci objektu;
- SET - změní hodnotu v instanci objektu.

Koncepce SNMP byla nastavena tak, aby byly zprávy nezávislé na transportním protokolu. Může se tedy využít jak TCP a UDP, tak i např. SPX. Nejčastější je implementace se síťovým protokolem IP a protokolem 4. vrstvy UDP. Pro příjem zpráv se na straně agenta používá port 161. Správce používá port 162.

SNMP zpráva se skládá ze dvou hlavních částí:

- hlavička (header);
- datová jednotka PDU (Protocol Data Unit).

Hlavička obsahuje informaci o verzi použitého protokolu a tzv. „community string“, který má funkci přístupového hesla[6].

verze	community	PDU typ	Request ID	Error status	Error index	Variable bindings

Obr. 4: Struktura SNMP

Struktura datové jednotky je ve všech typech zpráv kromě zprávy typu "trap" následující:

- Request ID – pořadové číslo dotazu. Díky tomuto poli je možné zjistit duplikované zprávy a správné pořadí zpráv. Důležité je také to, že se číslo dotazu i odpovědi na dotaz shoduje, čímž je možná jednoznačná identifikace;
- Error status – informuje o typu chyby;
- Error index – identifikuje proměnnou v poli Variable bindings, u které chyba nastala;
- Variable bindings – pole struktur, ze kterých je možno zjistit hodnoty dotazovaných objektů [6].

Zpráva Trap má svoji vlastní strukturu PDU:

- Enterprise – zde je uveden typ objektu, kde je identifikován druh zařízení, které vygenerovalo danou zprávu;
- Agent Address – obsahuje adresu zařízení, kterého se týká obdržená zpráva;
- Generic trap type, Specific trap code – identifikuje typ a kód zprávy;
- Time stamp – časová informace;
- Variable bindings – seznam proměnných a jejich hodnot, které jsou relevantní pro danou zprávu.

Původním a tudíž i nejstarším protokolem je SNMP verze 1. Existují ovšem i další, novější verze, které zavádějí několik vylepšení. V roce 1993 byl publikován SNMPv2, který je popsán v dokumentech RFC (Request for Comments) 1441 – 1452. Ten odstraňuje

[6]u verze 1 je přenášený v otevřené formě, takže SNMP v této podobě není příliš bezpečné

bezpečnostní nedostatky první verze (např. otevřený přenos "community string"). U druhé verze vzniklo několik specifikací založených na technologiích různých výrobců, což je chápáno jako jistý nedostatek [6]:

- SNMPv2p - „party–based security“;
- SNMPv2c - „community–based security“;
- SNMPv2u - „user–based security“;
- SNMPv2* - kombinace první a třetí varianty.

Poslední verzí je SNMPv3. Verze 3 si bere ty lepší vlastnosti předchozích verzí, vylepšuje bezpečnost a možnosti vzdálené konfigurace, zavádí kontrolu integrity a ověření zdroje dotazu. SNMPv3 je definovaný v RFC 3411 - 3418 vydaných v roce 2004 [6].

2.4 HSRP

HSRP je zkratkou pro Hot Standby Router Protocol a jedná se o proprietární řešení společnosti Cisco Systems. Detailní popis je uveden v RFC 2281. Patří do skupiny tzv. First Hop Redundancy Protocols (FHRP), což jsou protokoly, které nabízí řešení pro situace, kdy v síti používáme redundantní prvky. Uživatelé LAN sítí obdrží IP adresu, masku podsítě a výchozí bránu (default gateway). Toho může být docíleno pomocí manuální konfigurace u každého uživatele. Nicméně tato varianta je velmi pracná a z toho důvodu se používá protokol DHCP (Dynamic Host Configuration Protocol), který celý proces zautomatizuje. Jednotlivé uživatelské stanice ovšem nemají představu o tom, jakým způsobem funguje směrování. V případě, kdy selže směrovač (nebo tzv. „multilayer switch“), na který výchozí brána odkazuje, a v síti jsou redundantní prvky, které jsou schopny výpadek nahradit, by muselo dojít ke změně nastavení u všech uživatelských stanic tak, aby výchozí brána odkazovala na záložní prvek. Toto řešení je velmi pracné a ne moc elegantní. Z tohoto důvodu byl vyvinut protokol HSRP a následně protokoly VRRP (Virtual Router Redundancy Protocol) a GLBP (Gateway Load Balancing Protocol).

Základem protokolu HSRP je forma sdílení virtuální IP adresy. Uživatelská stanice má nastavenou výchozí bránu a odešle tedy „ARP request“ (Address Resolution Protocol) pro danou IP adresu a následně obdrží „ARP reply“ zprávu s MAC (Media Access Control) adresou zařízení, které vystupuje jako výchozí brána. Princip HSRP spočívá v tom, že se uživatelská stanice dotazuje na virtuální IP adresu a obratem dostane odpověď s MAC adresou, která je také virtuální. Pro HSRP jsou MAC adresy definovány ve tvaru 0000.0c07.acXX, kde XX reprezentuje číslo HSRP skupiny v hexadecimální podobě. Jednoduchým testem může každý čitatel této práce zjistit, pracuje-li v organizaci, kde se používá HSRP. Do příkazového řádku je třeba zadat „arp -a“. Pokud je pro IP adresu, kterou požíváme jako výchozí bránu, přiřazena MAC adresa v HSRP formátu, tak organizace HSRP používá. HSRP skupina může nabývat hodnot 0-255. Pro skupinu 1 bude obdržená MAC adresa ve tvaru 0000.0c07.ac01.

O této dvojici virtuální IP a MAC adresy ví všechny směrovače v dané HSRP skupině. Ale jen jeden směrovač může být působit jako hlavní a umožňovat tak tok uživatelských dat. Tento směrovač je označovaný jako „active“. Dále máme jeden směrovač, který má statut „standby“ a je schopen téměř okamžitě převzít úlohu aktivního směrovače. Všechny ostatní směrovače v dané skupině jsou ve stavu „listen“. Směrovač, který je „active“, je do své role zvolen na základě HSRP priority. Hodnota je dána v rozmezí 0-255 a čím vyšší, tím větší váha. Výchozí hodnota je nastavena na 100 a v případě shody rozhoduje vyšší MAC adresa. Rychlost s jakou je schopen záložní směrovač převzít úlohu aktivního směrovače se odvíjí od specifikace tzv. „hello“ a „hold“ časovačů. Výchozí hodnota pro „hello“ je nastavena na 3 sekundy, pro „hold“ na 10 sekund. „Hello“ zprávy se posílají na „multicast“ adresu 224.0.0.2 (všechny směrovače). V případě, že po dobu „hold“ časovače neobdržím žádnou „hello“ zprávu od aktivního HSRP směrovače, tak je považován za nedostupného a jeho úlohu přebírá záložní. Pokud se po odmlce opět ozve a začne posílat „hello“ zprávy, tak se nestane znovu aktivním i přesto, že má vyšší prioritu.[7]

Výše uvedené řešení sice napomáhá k zajištění vysoké dostupnosti v síti, ale neřeší případy, kdy dojde k výpadku linky k poskytovateli připojení. Je to např. situace, kdy má směrovač A (HSRP aktivní) všechny uživatele připojeny na port FastEhernet 0/0 (na něm

[7] k tomu je třeba nakonfigurovat tzv. „*preempt*“

je virtuální IP adresa, pro uživatele je to výchozí brána) a linka k poskytovateli (např. Serial 0/0) jde do stavu up/ down nebo down/ down. V tomto případě půjdou všechny požadavky uživatelů na aktivní směrovač A, který je ale z důvodu nefunkčnosti linky nebude schopen obsloužit. Záložní směrovač B, která má funkční linku, by byl schopen tyto požadavky obsloužit. Jeho stav ale bude pořád „standby“, protože stále dostává „hello“ zprávy od aktivního směrovače. Pro tyto případy je nezbytné nakonfigurovat tzv. „tracking“ na port Serial 0/0. „Tracking“ nedělá nic jiného než, že neustále sleduje stav portu a v případě, kdy dojde ke změně z up/ up na up/ down nebo down/ down, tak okamžitě sníží prioritu o předem určenou hodnotu. Modelová situace bude vypadat následovně:

- směrovač A má nastavenou prioritu na 105 (je aktivní), „tracking“ na port Serial 0/0 je nakonfigurovaný tak, že v případě změny stavu na jiný než up/ up sníží prioritu o 10;
- směrovač B má prioritu ponechanou na výchozí hodnotě 100, je ve stavu „standby“;
- poskytovatel linky pro směrovač A má poruchu;
- HSRP priorita se u směrovače A okamžitě sníží na 95 a prostřednictvím „hello“ zprávy o tom informuje všechny směrovače v dané skupině;
- v tento moment má směrovač B nejvyšší prioritu a stává se aktivním (musí mít ovšem nakonfigurovaný „preempt“), směrovač B si bere do správy virtuální IP a MAC adresu a obsluhuje uživatelské požadavky (uživatelé zaznamenají jen minimální nebo vůbec žádný výpadek).

Výše uvedený příklad ilustruje důležité vlastnosti a především jednoduchou implementaci protokolu HSRP pro zajištění vysoké dostupnosti. Mohou nastat i situace, kdy je linka k poskytovateli ve stavu up/ up, ale i přesto je nefunkční (např. pro optické spoje, nebo DSL připojení). I na tuto situaci je HSRP připraveno a „tracking“ se nastaví na nějaký jiný objekt – může to být například konkrétní adresu sítě ve směrovací tabulce, který přichází od BGP peera (souseda).

Do skupiny FHRP patří i dva další protokoly:

- VRRP;
- GLBP.

VRRP je téměř totožné s HSRP, ale je definováno jako IETF standard v RFC 2338 [8]. Hlavní rozdíly jsou následující:

- časovače jsou nastaveny pro „hello“ na 1 sekundu, pro „hold“ na 3 sekundy[8];
- „preempt“ je výchozí a nemusí se nastavovat;
- aktivní směrovač je pojmenovaný jako „master“ a záložní jako „backup“;
- virtuální MAC adresa je ve tvaru 0000.5e00.01XX.

GLBP pracuje na podobném principu jako HSRP a VRRP, ale přináší tzv. „load balancing“[9], kdy je možné rozložit uživatelské požadavky i na směrovače, které zrovna nejsou aktivní. Zavádí koncept AVG (Active Virtual Gateway) a AVF (Active Virtual Forwarder). Vtip řešení spočívá v tom, že směrovač, který je na základě priority zvolen jako AVG přiřazuje příchozím ARP dotazům od uživatelských stanic různé virtuální MAC adresy, které pak dává směrovačům, které jsou označeny jako AVF. Uživatelská data jdou pak přes více směrovačů a zátěž je tím pádem rozložena.

2.5 OSTATNÍ BEZPEČNOSTNÍ DOPORUČENÍ

Existuje celá řada bezpečnostních doporučení pro Cisco zařízení, z nichž se některé sice staly součástí téměř každé konfigurace, ale jiné bývají opomíjeny. Je důležité mít na paměti zejména následující:

- vždy používat příkaz „*service-password encryption*“. IOS následně zašifruje hesla použitá v celé konfiguraci;
- vždy zabezpečit fyzický přístup k danému zařízení, zejména pak dát pozor na „console“ port;
- někdy se také doporučuje zakázat proces obnovení hesla tzv. „password recovery“ pomocí příkazu „*no service password-recovery*“ Tuto možnost je ale třeba velmi

[8] důvodem nižších hodnot je fakt, že VRRP bylo definováno až 5 roků po HSRP

[9] „load balancing“ je možný i u HSRP a VRRP, nicméně jeho konfigurace není tak elegantní jak u GLBP a musí se vytvořit více skupin pod každým portem, část uživatelských stanic pak má jinou výchozí bránu než ostatní

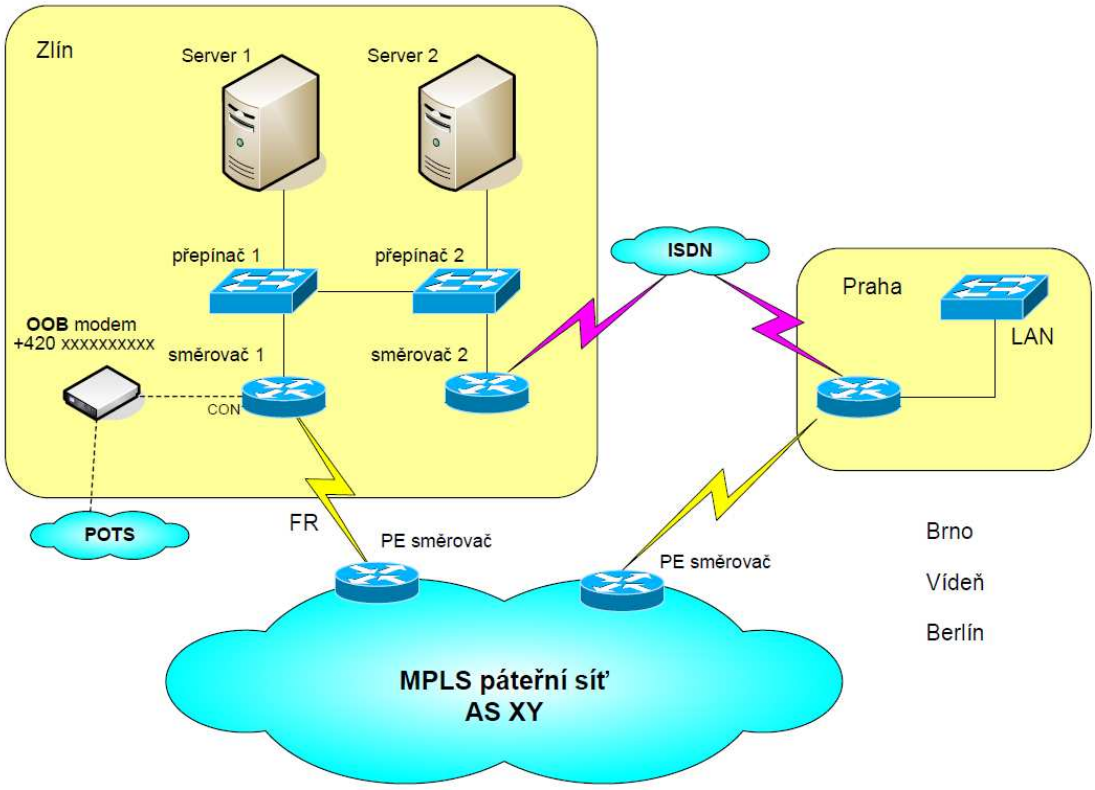
důsledně zvážit. V budoucnu může způsobit velké problémy, zejména v případě kdy není uložena záložní konfigurace;

- zakázat služby, které jsou ve výchozím nastavení povoleny, ale nepoužívají se. Nejčastěji (a společností Cisco doporučenými) se jedná o příkazy:
    - *no ip domain-lookup,*
    - *no ip finger,*
    - *no service tcp-small-servers,*
    - *no service udp-small-servers,*
    - *no service pad,*
    - *no ip http server,*
    - *no ip http secure-server,*
    - *no service config,*
    - *no cdp run*;
- používat tzv. „management interface“ (nadefinovat logický port „*Loopback1*“);
- vždy používat ssh místo telnetu;
- zařízení musí být vždy umístěna ve vhodném prostředí např. v racku. V místnosti je třeba udržovat předepsanou teplotu a vlhkost, tak aby se minimalizovalo riziko poškození hardwarového vybavení;
- používat tzv. „nepřerušitelné zdroje energie“ - UPS (Uninterruptible Power Supply), které jsou dimenzovány pro výkonové požadavky všech síťových prvků a dobou, po kterou chceme mít nahrazen výpadek stálé elektrické sítě;
- používat NTP (Network Time Protocol) protokol;
- používat hesla pro směrovací protokoly;
- pokud je využit modem pro OOB (Out of Band) připojení, tak nastavit heslo i na něm [8].

II. PRAKTICKÁ ČÁST

3 KONFIGURACE AAA

Pro názornost jsou v praktické části práce přiloženy důležité „*show*“ příkazy. Jsou stáhnuty z webu společnost Cisco a upraveny tak, aby reflektovaly navrženou konfiguraci. Všude tam, kde to bylo technicky možné, byla využita pracovní laboratoř. Konfigurace je navržena pro fiktivní pobočku Zlín, kde je důležitá serverová aplikace, k níž přistupují uživatelé ostatních poboček.



Obr. 6: Topologie sítě

Kapitola č. 3 se věnuje AAA. Jednou z výhod konfigurace AAA je to, že je stejná pro všechny aktivní síťové prvky, které v rámci organizace spravujeme. Příkazy jsou členěny do tří logických celků a to:

- autentizaci (ověření totožnosti);
- autorizaci (stanovení oprávnění);

- účtování (sběr informací).

Základním příkazem, který povolí činnost AAA je „*aaa new-model*“ a musí být vždy implementován. Bez něj není možná další konfigurace:

```
R1(config)#aaa ?
  new-model  Enable NEW access control commands and functions.(Disables OLD
             commands.)

R1(config)#aaa new-model
R1(config)#aaa ?
  accounting      Accounting configurations parameters.
  attribute       AAA attribute definitions
  authentication  Authentication configurations parameters.
  authorization   Authorization configurations parameters.
  cache           AAA cache definitions
  configuration   Authorization configuration parameters.
  dnis            Associate certain AAA parameters to a specific DNIS number
  group           AAA group definitions
  local           AAA Local method options
  max-sessions    Adjust initial hash size for estimated max sessions
  memory          AAA memory parameters
  nas             NAS specific configuration
  new-model       Enable NEW access control commands and functions.(Disables
                  OLD commands.)
  pod             POD processing
  policy          AAA policy parameters
  route           Static route downloading
  server          Local AAA server
  session-id      AAA Session ID
  session-mib     AAA session MIB options
  traceback       Traceback recording
  user            AAA user definitions

R1(config)#aaa
```

Obr. 6: Použití příkazu aaa new-model

Pro všechna zařízení v topologii byla navržena následující konfigurace:

„aaa authentication login default group tacacs+ enable“ - nastavuje autentizaci uživatelů pro přihlášení na aktivní síťový prvek („*login*“) na všechny rozhraní a jako výchozí metodu („*default*“) s tím, že údaje pro přihlášení jsou uloženy na serveru („*group*“ – znamená server group). Příkaz tacacs+ dále specifikuje, že používáme tatacs+ a ne radius.

„aaa authentication enable default group tacacs+ enable“ - definuje metodu pro přihlášení do tzv. „*enable*“ módu. Používáme opět stejný přístup jako v předchozím případě. Důležitý je příkaz „*enable*“ na konci, který udává, jakým způsobem dojde k autentizaci uživatele v případě, kdy nebude TACACS server dostupný (např. při špatném

nastavení směrování). V tom případě uživatel použije heslo, které je nastaveno pomocí příkazu „*enable secret*“.

„aaa authorization config-commands“ - autorizaci podléhají všechny příkazy v konfiguračním módu.

„aaa authorization exec default group tacacs+ if-authenticated“ - uživatel musí být autorizován.

„aaa authorization commands 0 default group tacacs+ none“ - tento a následující dva příkazy umožňují rozlišit mezi uživateli tři úrovně přístupu tak, aby jen určení mohli dané zařízení konfigurovat.

„aaa authorization commands 1 default group tacacs+ none“ - viz výše.

„aaa authorization commands 15 default group tacacs+ none“ - viz výše.

„aaa accounting exec default start-stop group tacacs+“ - účtování (accounting, jedná se o logování příkazů) pro všechny příkazy v „user exec“ módu. Příkaz „*start-stop*“ znamená okamžité ukládání. Další možností je „*stop-only*“, který ukládá po ukončení připojení.

„aaa accounting commands 1 default start-stop group tacacs+“ - účtování probíhá již od nejnižší možné úrovně. Výsledkem je velké množství dat, ale také jistota že zpětně můžeme dohledat veškerou činnost na směrovači. Pokud je třeba omezit množství dat a bude se logovat pouze činnost správců, tak bude nastavena úroveň 15.

„aaa accounting network default start-stop group tacacs+“ - účtování pro PPP (Point-to-Point Protocol) nebo SLIP (Serial Line Internet Protocol) protokoly.

„aaa accounting connection default start-stop group tacacs+“ - pro odchozí telnet spojení.

„aaa accounting system default start-stop group tacacs+“ - pro systémové události, např. reload.

Dále je nezbytné nastavit adresu TACACS serveru a heslo (klíč):

„tacacs-server host A.B.C.D“ - kde A.B.C.D je IP adresa hlavního TACACS serveru.

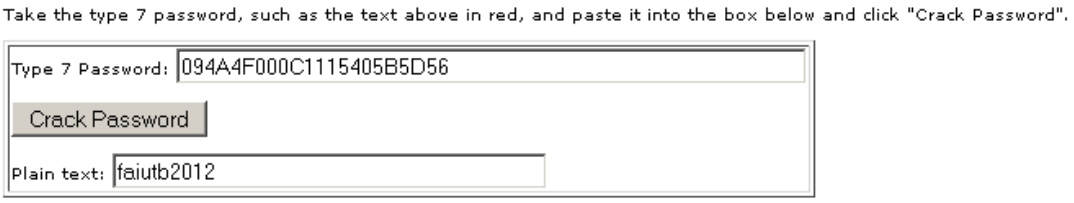
„tacacs-server host A.B.C.D“ - kde A.B.C.D je IP adresa záložního TACACS serveru.

„tacacs-server key faiutb2012“ - heslo musí být stejné na serveru i aktivním síťovém prvku.

Samozřejmostí je dostupnost TACACS serveru (ověřit pomocí příkazu ping). Je tedy třeba správně nastavit směrování. Všechny příkazy zkontrolovat jestli jsou v aktuální konfiguraci („*show running-config*“). „*Tacacs-server key*“ bude uložen jako otisk:

tacacs-server key 7 094A4F000C1115405B5D56.

Číslovka 7 znamená, že nebyl použit algoritmus md5, ale slabší, společností Cisco označován jako typ 7. Prolomení takového hesla je velmi snadné. Lze použít několik aplikací a pro názornost je přiložena ukázka ze stránek http://www.ifm.net.nz/ cookbooks/passwordcracker.html:



Obr. 7: Prolomení hesla typu 7

Dnes už je téměř samozřejmostí použití příkazu ***„ip tacacs source-interface Loopback1“***. „Loopback1“ je logický port, který je vždy ve stavu up/ up. Záznamy na TACACS serveru tak mají jako zdrojovou adresu IP adresu portu „Loopback1“ a ne IP adresu portu „Serial0/0/0.111“, což je činí přehlednějšími. Port „Loopback1“ se používá také pro správu a jednoznačnou identifikaci zařízení.

3.1 Ověření funkčnosti AAA

Pokud je AAA správně nakonfigurováno, tak se každý uživatel přihlásí se svými údaji. Nejdůležitějším „*show*“ příkazem pro ověření je „*show tacacs*“. Pokud je vše v pořádku, tak je očekáván následující výstup:

```
R1#show tacacs

Tacacs+ Server            : A.B.C.D/49
              Socket opens:      16092
             Socket closes:      15738
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:      17468
        Total Packets Recv:      17438


Tacacs+ Server            : A.B.C.D/49
              Socket opens:         34
             Socket closes:         34
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:         35
        Total Packets Recv:         27
```

Obr. 8: Příkaz show tacacs

Číslo 49 za IP adresou TACACS serverů je výchozí číslo portu pro TACACS. Dalším způsobem pro ověření funkčnosti je spustit tzv. „*debug*“. Pro AAA jsou možnosti:

R1#debug tacacs ?

accounting	TACACS+ protocol accounting
authentication	TACACS+ protocol authentication
authorization	TACACS+ protocol authorization
events	TACACS+ protocol events
packet	TACACS+ packets

Pokud má uživatel pochybnosti o své úrovni přístupu, tak je může ověřit pomocí příkazu „*show privilege*“. Pro správce je očekáván následující výstup:

```
R1#show privilege
Current privilege level is 15.
```

4 KONFIGURACE SNMP

Konfigurace SNMP je poměrně přímočará a lze ji rozdělit do několika logických kroků:

- vytvoření SNMP „community“;
- specifikace SNMP serveru;
- konfigurace množiny „trapů“ (zpráv).

SNMP „community“ slouží pro vytvoření vazby mezi správcem a agentem. Pro potřeby této práce bylo navrženo vytvořit dvě – jednu pro čtení (r – read) a druhou pro čtení i zápis (rw – read write). Bude využito následujících příkazů:

- ***„snmp-server community heslo1 RO 5“***;
- ***„snmp-server community heslo2 RW 6“.***

Čísla 5 a 6 se odvolávají na standardní ACL, který slouží pro omezení přístupu. Pokud nedojde k nakonfigurování ACL 5 a 6, tak SNMP nebude fungovat. Výchozí verze pro SNMP je v2c.

Pro specifikaci serveru slouží tyto příkazy:

- ***„snmp-server host A.B.C.D heslo1“***;
- ***„snmp-server host A.B.C.D heslo2“***.

Kde A.B.C.D je IP adresa SNMP serveru. Dále byla navržena následující konfigurace SNMP trapů pro směrovač (je třeba respektovat konkrétní konfigurace - např. použité WAN technologie):

- ***„snmp-server enable traps snmp linkdown linkup coldstart warmstart“*** - pošle trap pokud jde port do stavu down nebo zpět do up, nebo v případě, kdy dojde k restartování směrovače.
- ***„snmp-server enable traps envmon“*** - SNMP trapy pro situace, kdy dojde k překročení povolené teploty nebo napětí (popř. aktuální hodnota je mimo výrobcem stanovený rozsah). Taktéž informuje při poruše větráku nebo zdroje (pokud máme redundantní). Všechny uvedené informace ověříme pomocí příkazu „*show environment*“.

```
R1# show environment all
SYSTEM POWER SUPPLY STATUS
==========================
 Internal Power Supply Type: AC
 Internal Power Supply 12V Output Status: Normal

 External Redundant Power Supply is absent or powered off

SYSTEM FAN STATUS
=================
 Fan 1 OK, Low speed setting
 Fan 2 OK, Low speed setting
 Fan 3 OK, Low speed setting
 Fan 4 OK, Low speed setting

SYSTEM TEMPERATURE STATUS
=========================
 Intake Left(Bezel) temperature: 15 Celsius, Normal
 Intake Left temperature: 17 Celsius, Normal
 Exhaust Right(Bezel) temperature: 21 Celsius, Normal
 Exhaust Right temperature: 19 Celsius, Normal
 CPU temperature: 50 Celsius, Normal
 Power Supply Unit temperature: 20 Celsius, Normal

REAL TIME CLOCK BATTERY STATUS
==============================
 Battery OK (checked at power up)

SYSTEM POWER
===============
 Motherboard Components Power consumption = 44.1 W
 Total System Power consumption is: 44.1 W

 Environmental information last updated 00:00:00 ago
```

Obr. 9: Příkaz show environment

- ***„snmp-server enable traps isdn call-information“*** - informace o ISDN voláních.
- ***„snmp-server enable traps isdn layer2“*** - pro ISDN trapy na 2. vrstvě.
- ***„snmp-server enable traps isdn chan-not-avail“*** - pro nedostupný ISDN kanál, lze konfigurovat pouze u BRI.
- ***„snmp-server enable traps bgp“*** - jako směrovací protokol se na R1 využívá BGP, daný příkaz povolí trapy pro jakoukoliv změnu stavu u BGP souseda (např. stav jde z požadovaného *„estabilished“* do *„active“* nebo *„idle“*). Sleduje se také počet přijatých prefixů a pokud dojde k dosažení limitu, tak se odešle trap.
- ***„snmp-server enable traps config“*** - hlášení, pokud dojde ke změně konfigurace.
- ***„snmp-server enable traps frame-relay“*** - pro monitorování frame-relay (pokud jde PVC z požadovaného stavu *„active“* do *„inactive“* nebo *„deleted“*).

Výše uvedená konfigurace je pro oba dva směrovače. Pro přepínače postačí příkaz ***„snmp server enable traps snmp linkdown linkup coldstart warmstart“.*** Dále je doporučováno doplnit konfiguraci o následující příkazy:

- ***„snmp-server ifindex persist“*** - slouží k jednoznačné identifikaci portů, které jsou na zařízení použity. Důležité je zejména to, že zůstává konstantní i po restartování.
- ***„snmp-server trap-source Loopback1“*** - používání tzv. „management interfaces“ je v současnosti běžně doporučováno. Zdrojová IP adresa bude IP adresa logického rozhraní „*Loopback1*“.
- ***„snmp-server location“*** - pro upřesnění fyzického umístění aktivního síťového prvku, slouží pro lepší přehlednost.
- ***„snmp-server contact“*** - opět pro lepší přehlednost, zde se např. uvádí kontakt na správce.

4.1 Ověření funkčnosti SNMP

Pro test funkčnosti SNMP se používají tři hlavní nástroje:

- použití tzv. snmpwalk[10] - jedná se o příkaz, který postupně vypíše „uptime“, verzi použitého IOSu, údaje z „*snmp-server contact*“, „*snmp-server-location* a všechny podporované MIB proměnné:

```
/users/jk >>snmpwalk -v2c  -c "heslo1" "IP adresa loopbacku"
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, 2800 Software (C2800NM-SPSERVICESK9-M)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 03-Sep-10 06:26 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.576
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (27267660) 3 days, 3:44:36.60
SNMPv2-MIB::sysContact.0 = STRING: Petr Novotny +420604245357
SNMPv2-MIB::sysLocation.0 = STRING: R1, Zlin, Czech Republic
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::enterprises.9.7.129
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-SMI::enterprises.9.7.115
SNMPv2-MIB::sysORID.3 = OID: SNMPv2-SMI::enterprises.9.7.265
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-SMI::enterprises.9.7.112
SNMPv2-MIB::sysORID.5 = OID: SNMPv2-SMI::enterprises.9.7.106
```

Obr. 10: Příkaz snmpwalk

[10] často se využívá utilita „*snmpset*“, která umožňuje konfiguraci přes SNMP v případě, kdy ztratíme přístup – např. při nevhodné implementaci restriktivního ACL v rámci „line vty“

- ověřovací příkaz „*show snmp*“, který nám vypíše hlavní charakteristiky a statistiky:

```
R1#show snmp
Chassis: FOC1431V3RH
Contact: Petr Novotny +420604245357
Location: R1, Zlin, Czech Republic
2554080 SNMP packets input
    0 Bad SNMP version errors
    759 Unknown community name
    0 Illegal operation for community name supplied
    25 Encoding errors
    12061408 Number of requested variables
    2399 Number of altered variables
    1083521 Get-request PDUs
    969343 Get-next PDUs
    994 Set-request PDUs
2557136 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    1569 No such name errors
    0 Bad values errors
    306 General errors
    2553296 Response PDUs
    3840 Trap PDUs
SNMP global trap: enabled
```

Obr. 11: Příkaz show snmp

- manuální test, při kterém se fyzicky odpojí přístupová frame-relay linka. Následkem toho půjde port „Serial0/0/0“ do stavu down/ down. Při tomto testu je nezbytné, aby došlo ke generování snmp trapu jeho odeslání (pokud je cesta v síti) správci. Lze samozřejmě ověřovat i jiné trapy (BGP není ve stavu „*estabilished*“ atd.).

5 KONFIGURACE WAN ROZHRANÍ

Konfigurace WAN rozhraní (interfaces) nepatří mezi hlavní témata této práce, ale jedná se o jednu ze stěžejních částí konfigurace směrovačů. V teoretické části byla vybrána technologie frame-relay pro hlavní linku a ISDN pro záložní.

5.1 Konfigurace frame-relay

Do směrovače je vhodná a také velmi často používaná karta WIC-2T, která má rozhraní „smart serial“ a nemá integrované CSU/ DSU. Pro připojení se používá kabel s rozhraním V.35. V případě použití novější karty - např. VWIC-2MFT-E1 s integrovaným CSU/ DSU a rozhraním RJ48 je třeba nakonfigurovat „*card type*“, „*framing*“ a „*linecode*“. Pro WIC-2T a frame-relay je třeba následující konfigurace (pro R1):

- ***„interface Serial0/0/0“***;
- ***„description linka cislo 123456, poskytovatel XY“*** - pro přehlednost;
- ***„no ip address“*** - nakonfiguruje se až pro dílčí rozhraní;
- ***„no ip redirects“*** - bezpečnostní doporučení společnosti Cisco;
- ***„no ip proxy-arp“*** - bezpečnostní doporučení společnosti Cisco;
- ***„encapsulation frame-relay“*** - typ zapouzdření. Na výběr je „cisco“ (výchozí) nebo „ietf“;
- ***„load-interval 30“*** - určení časové periody pro statistiky rozhraní „*Serial0/0/0*“;
- ***„frame-relay traffic-shaping“*** - pro QoS (volitelné);
- ***„interface Serial0/0/0.111 point-to-point“*** - vytvoření dílčího rozhraní;
- ***„description pripojeni do site BT (AS 22222)“***;
- ***„ip address A.B.C.D 255.255.255.252“*** - specifikace IP adresy, maska se většinou používá /30;
- ***„no ip redirects“*** - bezpečnostní doporučení společnosti Cisco;
- ***„no ip proxy-arp“*** - bezpečnostní doporučení společnosti Cisco;
- ***„snmp trap link-status“*** - z důvodu použití dílčího rozhraní;

- ***„no arp frame-relay“*** - není třeba povolit;
- ***„frame-relay interface-dlci 111“*** - k dílčímu rozhraní přiřadí číslo DLCI 111, umožňuje také změnit typ zapouzdření pro dílčí rozhraní (ietf, cisco - výchozí);
- ***„class FR-QoS“*** - pro QoS, název třídy (volitelné).

V konfiguraci není typ LMI (Local Management Interface). Je tedy ponechán výchozí – cisco. V případě že frame-relay switch používá jiný typ (jsou celkem tři – q933a, cisco a ansi) by mělo dojít k vyjednání toho správného a směrovač následně změní svůj typ. Obecně lze doporučit řádně se informovat u poskytovatele a následně LMI typ nakonfigurovat. Pokud by LMI nebylo správné tak bude fyzické rozhraní up/ down a logické down/ down.

Mezi nejdůležitější ověřovací příkazy pro frame-relay patří:

- „*show frame-relay pvc*“ – musí být „*active*“. V ostatních případech, kdy je „*deleted*“ nebo „*inactive*“ řešit s poskytovatelem. Očekávaný výstup je následující:

```
R1#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

                Active     Inactive      Deleted       Static
  Local            1            0            0            0
  Switched         0            0            0            0
  Unused           0            0            0            0

DLCI = 111, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.111

  input pkts 14555146      output pkts 13617097     in bytes 2906991773
  out bytes 1970799473     dropped pkts 0           in pkts dropped 0
  out pkts dropped 1488              out bytes dropped 493346
  late-dropped out pkts 1488         late-dropped out bytes 493346
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 181682    out bcast bytes 62498608
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
  pvc create time 1y10w, last time pvc status changed 9w3d
```

Obr. 12: Příkaz show frame-relay pvc

- „*show frame-relay lmi*“ – zde jsou uvedeny informace a statistiky pro LMI. Hlavní je aby „*Num Status Enq. Sent*“ byl stejný jako „*Num Status msgs Rcvd*“.

V následujícím případě tomu tak není a rozdíl je v kolonce „*Num Status Timeouts*“. Správná funkce je také indikována stejným časovým údajem v posledním řádku:

```
R1#show frame-relay lmi

LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 1090561          Num Status msgs Rcvd 1090108
  Num Update Status Rcvd 0              Num Status Timeouts 453
  Last Full Status Req 00:00:46         Last Full Status Rcvd 00:00:46
```

Obr. 13: Příkaz show frame-relay lmi

- „*show frame-relay map*“ – zobrazí položky mapovaní IP/ DLCI.

5.2 Konfigurace ISDN

V teoretické části byla pro záložní připojení vybrána technologie ISDN. Funkční koncept je takový, že dochází k neustálému sledovaní specifické adresy sítě ve směrovací tabulce, která je přijímána po primární lince a následně jde přes přepínače do R2. V případě, že R2 nevidí tuto adresu sítě, tak dojde k aktivaci ISDN.

Pro ISDN BRI připojení je na výběr z několika karet. Mezi nejpoužívanější patří WIC-1B-S/T-V3. Pro konfiguraci ISDN je nezbytná znalost tzv. „*isdn switch-type*“. Existuje několik druhů podle lokality:

- basic-ts013 – používaný v Austrálii;
- basic-1tr6 – Německo;
- basic-net3 – Evropa, Nový Zéland;
- vn3 – Francie;
- ntt – Japonsko;
- další – např. basic-ni, basic-5ess.

Dále je třeba vybrat způsob jak ISDN nakonfigurovat. V této práci byla zvolena metoda pomocí tzv. „dialerů“ a DDR (dial-on-demand routing). „*Dialer*“ je logické

rozhraní, které nám umožňuje oddělit konfiguraci od rozhraní, které přijímá nebo iniciuje volání. Tento přístup umožňuje mnohem větší variabilitu konfigurací. Výsledné příkazy jsou následující:

- ***„interface BRI0/0/0“***;
- ***„description ISDN zaloha“***;
- ***„no ip address“***;
- ***„no ip redirects“***;
- ***„no ip proxy-arp“***;
- ***„encapsulation ppp“*** - použije se PPP zapouzdření;
- ***„dialer pool-member 1“*** - stěžejní příkaz, který tvoří vazbu mezi fyzickým (BRI) a logickým rozhraním („*Dialer0*“, konfigurace následuje);
- ***„isdn switch-type basic-net3“*** - upřesnění typu ISDN zařízení, je třeba mít na paměti, že stejný příkaz musí být i v globálním konfiguračním módu a ne jen pod BRI rozhraním;
- ***„ppp multilink“*** - stejný příkaz musí být i pod rozhraním „*Dialer0*“, vysvětlení níže;
- ***„interface Dialer0“***;
- ***„description zaloha na smerovac Praha“***;
- ***„ip address A.B.C.D“***;
- ***„no ip redirects“***;
- ***„no ip proxy-arp“***
- ***„encapsulation ppp“*** - použije se PPP zapouzdření;
- ***„no ip mroute-cache“*** - obecné doporučení společnosti Cisco, které zakazuje „fast switching“ pro „multicast“;
- ***„dialer pool 1“*** - vazba s fyzickým portem, v našem případě BRI0/0/0;
- ***„dialer idle-timeout 90“*** - čas v sekundách, po kterém dojde k odpojení při nečinnosti;
- ***„dialer wait-for-carrier-time 180“*** - čas v sekundách, který stanovuje jak dlouho se čeká na zařízení poskytovatele pro úspěšné sestavení hovoru. Výchozí hodnota je 30 sekund, ale v některých zemích je doporučeno tuto hodnotu navýšit;
- ***„dialer string 0042018262355“*** - telefonní číslo;
- ***„dialer hold-queue 50“*** - počet paketů, které mohou čekat ve frontě než se sestaví ISDN hovor (výchozí nastavení zakazuje tvorbu front);

- ***„dialer watch-disable 30“*** - údaj v sekundách, který stanovuje jak dlouho bude pokračovat ISDN hovor poté, co dojde ke zprovoznění hlavní linky;
- ***„ppp authentication chap“*** - pro autentizaci je použit protokol CHAP (Challenge-Handshake Authentication Protocol);
- ***„dialer load-threshold 127 either“*** - pokud překročí vytížení 50% (to lze ověřit pomocí příkazu „*show interface dialer0*“, rozmezí je 0-255), tak se využije i druhý BRI kanál. Příkaz „*either*“ stanovuje, že k využití druhého ISDN kanálu dojde při překročení limitu buď u příchozích dat (incoming) nebo odchozích (outgoing):

```
R2#show interfaces dialer 0
Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Description: zaloha na Router Praha
  Internet address will be negotiated using IPCP
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Obr. 14: Statistika vytížení portu

- ***„dialer watch-group 5“*** - důležitý příkaz povolující tzv. DDR. Jedná se o „sledování“ konkrétní adresy sítě a v případě, kdy není ve směrovací tabulce, tak dojde k inicializaci ISDN volání;
- ***„ppp multilink“*** - souvisí s příkazem „*dialer load-threshold 127 either*“. „*Multilink ppp*“ je použit z důvodu rozložení zátěže na oba dva BRI kanály a musí být nakonfigurován jak pod fyzickým rozhraním, tak pod rozhraní „*Dialer0*“.

Výše uvedené příkazy jsou dostačující pro konfiguraci rozhraní „*Dialer0*“ a „*BRI0/0/0*“. Zbývá ještě konfigurace sledovaného objektu (adresa sítě) a CHAP konfigurace:

- ***„username R2 password heslo“*** - stejné heslo musí být použito i na druhé straně[11];
- ***„dialer watch-list 5 ip A.B.C.D“*** - adresa sítě, která je sledována;

[11] samozřejmostí je kontrola aktuální konfigurace druhé strany, nicméně lze také použít „*debug ppp authentication*“

- ***„dialer watch-list 5 delay disconnect 30“*** - časový údaj v sekundách, který stanovuje, jak dlouho se počká, než dojde k odpojení záložní linky (poté, co se ve směrovací tabulce znovu objeví sledovaný prefix[12]).

Funkčnost ISDN linky lze ověřit následujícími způsoby:

- port BRI je ve stavu up/ up;
- „*show isdn status*“ ukazuje na první vrstvě stav „*active*“ a na druhé „*multiple frame established*“;
- „*show isdn active*“ ukazuje aktivní hovor (jen v případě výpadku primární linky) [8].

```
R2#sh isdn status
Global ISDN Switchtype = basic-net3
ISDN BRI0/0/0 interface
        dsl 0, interface ISDN Switchtype = basic-net3
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 67, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

Obr. 15: ISDN status

[12] jedná se o adresu sítě, který dostává R1 od PE („provider edge“) směrovače

6 KONFIGURACE HSRP

Pro HSRP stačí v rámci dané topologie jedna skupina - např. 1. R1 má primární frame-relay linku a bude tedy HSRP „*active*“ s následující konfigurací „*FastEthernet0/0*“:

- ***„standby 1 ip A.B.C.D“*** - virtuální IP adresa;
- ***„standby 1 preempt delay minimum 60“*** - zdržení o 60 sekund v případě preempce (pro kalkulaci BGP);
- ***„standby 1 track Serial0/0/0.111 50“*** - HSRP sleduje stav primární linky a v případě, kdy není up/ up dojde ke snížení priority o 50.

Konfiguraci ověříme pomocí příkazu „*show standby brief*“:

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       1    100 P Active  local           A.B.C.D           E.F.G.H
```

Obr. 16: Ověření HSRP pro R1

Konfigurace záložního směrovače R2 bude obdobná (opět pro „*FastEthernet0/0*“):

- ***„standby 1 ip A.B.C.D“*** - virtuální IP adresa;
- ***„standby 1 priority 60“*** - můžeme zvolit cokoliv mezi 51 a 99;
- ***„standby 1 preempt“*** - R2 používá EIGRP a „delay“ tedy nevolíme.

Konfiguraci ověříme pomocí příkazu „*show standby brief*“:

```
R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       1    60  P Standby A.B.C.D         local             E.F.G.H
```

Obr. 17: Ověření HSRP pro R2

Funkčnost se ověří pomocí intruzivního testu:

- fyzicky se odpojí hlavní linka vedoucí do portu „*Serial0/0/0*“ na R1 (nebo pomocí příkazu „*shutdown*“);
- HSRP priorita R1 klesne na 50;
- R2 má prioritu 60 a stává se „*active*“;
- R2 nedostává specifickou adresu sítě, která je kontrolována DDR;
- dojde k inicializaci ISDN hovoru a serverové aplikace jsou opět dostupné;
- při zapojení hlavní linky vzroste HSRP priorita R1 na 100;
- R2 zjistí, že je ve stejné HSRP skupině směrovač s vyšší prioritou. Od té chvíle přesně za 60 sekund půjde R2 ze stavu „*active*“ do stavu „*standby*“;
- dojde k ukončení ISDN hovoru a uživatelský provoz jde opět přes R1.

7 KONFIGURACE OOB, SMĚROVÁNÍ A OSTATNÍCH BEZPEČNOSTNÍCH PRVKŮ

Tato kapitola popíše další možnosti jak zvýšit bezpečnost a dostupnost aktivních síťových prvků. Jedná se o OOB, ACL a SSH. Bude také nastíněn princip směrování.

7.1 Konfigurace OOB

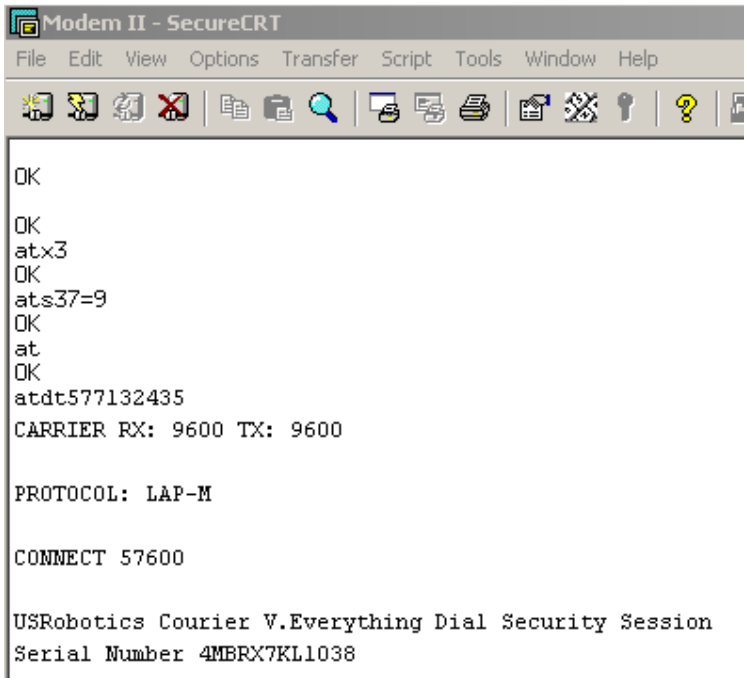
Konfigurace OOB neboli out-of-band je užitečná v případech, kdy dojde k selhání hlavní i záložní linky a správce nemá možnost vzdáleně ověřit stav na aktivních síťových prvcích.

Pro OOB jsou nutné pouze dvě věci - klasická analogová telefonní linka a vhodný modem. Telefonní linka se zapojí do modemu a modem přes rozhraní DB25 do „console“ portu R1. Toto spojení je pak využíváno v kritických situacích s využitím tzv. „dialout“ serverů nebo integrovaného modemu v notebooku. Mezi nejčastěji používané modemy patří zařízení společností US Robotics a Multitech. Tyto modemy pak musí být náležitě nakonfigurovány. Pro US Robotics se nastavují tzv. DIP přepínače na spodní straně modemu. Pro Multitech modem je nutná následující konfigurace[13]:

- AT#Sxxxxx - kde xxxxx je zvolené heslo o délce 1-8 znaků (výchozí je MTSMODEM);
- AT%R1&W0 - nastaví několik dílčích provozních detailů pro správnou funkci OOB (např. 9600 baudů) a uloží (&W0).

[13] pro konfiguraci je možné využít nástroj Microsoft Windows - Hyperterminal

Správná funkce je indikována vypsáním zprávy „*OK Connecting*“ po zadání hesla do modemu. Následně bude uživatel vyzván k zadání svého TACACS jména a hesla (v případě výpadku obou linek jenom „*enable*“ hesla). Výhodou je téměř stálá dostupnost a finanční nenáročnost. OOB nevyžaduje konfiguraci přepínače.



Obr. 18: Připojení přes OOB

7.2 SSH

V současné době je protokol telnet z bezpečnostního hlediska nevyhovující a pro vzdálenou správu se tedy doporučuje používat ssh. Konfigurace je přímočará a může být použita na všechny zařízení (je ale třeba dávat pozor na verzi IOSu, ne všechny podporují SSH – v názvu musí být obsaženo „*k9*“). Konfigurace je následující:

- ***„ip domain-name ABC“*** - specifikace domény;
- ***„aaa new-model“*** - nutné pro SSH s přihlašovacím jménem a heslem, již nakonfigurováno z předchozích kapitol;
- ***„ip ssh version 2“*** - verze 2;
- ***„crypto key generate rsa“*** - je třeba vygenerovat klíče, 512, 1024, ...;

- ***„ip ssh source-interface Loopback1“*** - zdrojová adresa paketu bude IP adresa logického rozhraní „*Loopback1*“ a ne portu „*Serial0/0/0*“, nutné v případech ssh připojení na další zařízení, kde je restriktivní ACL v rámci „*line vty*“;
- ***„transport input ssh“*** - povolení ssh v rámci „*line vty 0 15*“ (nebo „*line vty 0 4*“) [9].

7.3 Nastavení směrování

Pro směrování byly vybrány dva protokoly – BGP pro primární linku na R1 a EIGRP pro záložní linku na R2. BGP je specifické tím, že soused není hledán pomocí příkazu „*network*“, tak jak je tomu u EIGRP nebo OSPF, ale je explicitně nakonfigurován pomocí příkazu „*neighbor*“. Rozdílů je nespočet a BGP samo o sobě vydá na samostatnou práci. V této podkapitole jsou pro ilustraci uvedeny soukromé IP adresy. Pro LAN je dostatečná maska /24 a z bloku 10.0.0.0 byla vybrána podsíť 10.10.44.x. Konfigurace směrování na R1 bude vypadat následovně:

- ***„router bgp MOJE_AS“*** - druhá strana (PE) to má nastaveno jako „*remote-as*“;
- ***„neighbor 10.10.253.82 remote-as AS_SOUSEDA“*** - je třeba ověřit dostupnost souseda pomocí příkazu „*ping*“. V případě špatného nastavení sousedova AS budeme upozorněni výpisem „terminal monitoru“ a správné číslo AS lze zjistit převodem hexadecimálního čísla;
- ***„neighbor 10.10.253.82 soft-reconfiguration inbound“*** - pro povolení tzv. „*soft clear*“ (BGP „peering“ je zachován, vhodné při filtrování adres sítí);
- ***„neighbor 10.10.253.82 distribute-list 30 in“*** - pro filtrování adres sítí, bylo povoleno např. jen 10.0.0.0/8 pro celou firmu;
- ***„network 10.10.44.0 mask 255.255.255.0“*** - pro LAN;
- ***„network 10.10.250.6 mask 255.255.255.255“*** - IP adresa rozhraní „Loopback1“ na směrovači R1;
- ***„network 10.10.250.7 mask 255.255.255.255“*** - IP adresa rozhraní „Loopback1“ na směrovači R2;

Všechny adresy sítí s danou maskou, které jsou uvedeny v „*network*“ příkazech, musí být ve směrovací tabulce R1 jinak tento koncept nebude fungovat. Ve směrovací tabulce R1 chybí adresa sítě „*Loopback1*“ R2 a proto je třeba mezi R1 a R2 (FastEthernet0/0 na obou směrovačích) nastavit EIGRP (EIGRP je také vhodnější pro ISDN DDR, mezi oběma směrovacími protokoly se zároveň nastaví redistribuce z BGP do EIGRP). Konfigurace pro R1:

- ***„router eigrp 130“***;
- ***„redistribute bgp MOJE_AS metric 1536 2000 255 1 1500“*** - bez tzv. „metric values“ by redistribuce nefungovala. R2 tedy dostává „celofiremní“ prefix 10.0.0.0/8, který použije pro ISDN DDR;
- ***„passive-interface Serial/0/0.111“*** - zde je BGP a není nutné posílat EIGRP „*hello*“;
- ***„network 10.0.0.0“*** - povolí EIGRP pro všechny porty na směrovači R1;
- ***„no auto-summary“.***

Konfigurace pro R2:

- ***„router eigrp 130“***;
- ***„network 10.0.0.0“*** - povolí EIGRP pro všechny porty na směrovači R1;;
- ***„distribute-list 57 out Dialer0“*** – analogicky jako u BGP bude ACL 57 obsahovat příkazy povolující pouze adresy sítí pro LAN, „*Loopback*“ R1 a R2 („*access-list 57 permit 10.10.44.0“, „access-list 57 permit 10.10.250.7“, „access-list 57 permit 10.10.250.6“*);
- ***„no auto-summary“.***

Na obou přepínačích (S1 a S2) se musí nastavit „*ip default-gateway A.B.C.D*“ kde A.B.C.D je virtuální IP adresa HSRP skupiny (např. 10.10.44.1).

7.4 Zabezpečení pomocí ACL

V dnešní době je už nutnost používat pouze povolené rozsahy IP adres - tzn. je třeba nadefinovat rozsahy, ze kterých bude povolena konfigurace. Následuje vytvoření konkrétních ACL a jejich implementace v rámci „*line vty 0 4*“ (nebo 15) pomocí příkazu „*access-class XY in*“, kde XY je číslo ACL. Obdobné ACL je třeba nastavit také pod porty FastEthernet0/0 (s použitím příkazu „*access-group XY in*“) na obou směrovačích. V tomto ACL budou mimo jiné povoleny IP adresy serverové aplikace a Vlan1 (SVI sloužící pro management přepínačů S1 a S2). Při implementaci je třeba obezřetnost, protože pokud dojde ke konfiguraci „*access-class*“ s číslem ACL, který neexistuje, tak se stane zařízení nedostupným pro vzdálenou konfiguraci.

7.5 Bezpečnostní rizika

Vzhledem k využití zabezpečovacích prvků v podobě ACL a TACACS spočívá největší riziko v samotném fyzickém zabezpečení aktivních síťových prvků a serveru. Nezbytností je uzamykatelná řádně zabezpečená místnost s UPS, stálou teplotou a vlhkostí. V případě volného přístupu k zařízením hrozí, že útočník provede tzv. obnovení hesla[14] (password recovery) a získá tak plný přístup a kontrolu nad zařízeními.

Proces obnovení hesla je pro přepínač Cisco 2811 následující:

- připojit se do „console“ portu;
- restartovat přepínač;
- stisknout tzv. „break sequence“ (nejčastěji se jedná o klávesu „break“, popř. kombinaci kláves „ctrl“ + „break“ nebo „ctrl“ + „F6“ + „break“);
- následuje systémové hlášení:
  „**** System received an abort due to Break Key ****“;

[14] Proces je nazýván „password recovery“ a volný překlad je obnovení hesla. Tento překlad je však zavádějící. Jedná se o vytvoření nového hesla pro přístup k zařízení bez ztráty konfigurace.

- další konfigurace probíhá v ROMmon módu;
- změnit hodnotu konfiguračního registru na 2142 (= nebude použita konfigurace uložená v NVRAM, tzn. „*startup-config*“):
  „*rommon 1 > confreg 0x2142*“;
- následuje další restart pomocí příkazu „reset“:
  „*rommon 2 > reset*“;
- směrovač nabootuje s prázdnou konfigurací a následuje dotaz na zadání „*initial configuration*“:
  „*Would you like to enter the initial configuration dialog? [yes/no]:*“;
- konfiguraci není důležitá, odpovíme „n“ pro odmítnutí;
- v „*enable*“ módu následuje příkaz:
  „*copy startup-config running-config*“;
- dojde ke zkopírování funkční („*startup-config*“) konfigurace do současné („*running-config*“);
- potenciální útočník zde může vytvořit nový uživatelský účet nebo změnit hesla:
  „*router(config)#username utocnik privilege 15 password ejlncGK*“;
- posledním krokem je změna konfiguračního registru zpět na obvyklou hodnotu 2102 a restart směrovače:
  „*Router(config)#config-register 0x2102*“ [10].

Útočník tak získá přehled o konfiguraci a plnou kontrolu nad zařízením. Pro přepínače je procedura obdobná. Pro „break„ sekvenci se ale využívá tlačítko „mode“ na přední straně přepínače [10]. Správce má možnost proces obnovy hesla úplně zakázat pomocí příkazu „*no service password-recovery*“. Uvedené opatření je ale nutné pečlivě zvážit.

ZÁVĚR

Tato práce se zabývá návrhem konfigurace aktivních síťových prvků společnosti Cisco s důrazem na zabezpečení a dostupnost serverové aplikace finanční instituce. Navržená konfigurace je jednou z možných variant jak danou situaci řešit. Zatímco použití protokolů TACACS a HSRP (popř. VRRP nebo GLBP) je téměř nevyhnutelné, tak konfigurace pro směrování a výběr WAN technologií skýtají celou řadu více či méně náročných variant řešení. Vždy je třeba splnit kriteria zadání a řešení koncipovat na míru s ohledem na finanční možnosti zákazníka.

Dalším faktorem, který je třeba zohlednit je riziko. Rizikem je myšlena pravděpodobnost, že nastane situace (jedna či více), kdy bude serverová aplikace nedostupná. V práci je navržena redundantní topologie se dvěma přepínači a dvěma směrovači. Tento fakt umožňuje lépe čelit situacím, kdy dojde k poškození technického vybavení (jeden přepínač nebo jeden směrovač bude nefunkční) nebo výpadku linky. Je také doporučeno používat rozdílné poskytovatele pro hlavní a záložní připojení.

Jako hlavní připojení bylo doporučeno použití frame-relay linky vedoucí do páteřní MPLS sítě některého z velkých poskytovatelů nabízejících své služby celosvětově (např. British Telecom, Verizon). Frame-relay sice není nejnovější, nicméně stále se těší velké oblibě pro svou flexibilitu a jednoduchost.

Pro záložní linku bylo doporučeno ISDN z důvodu nízkých provozních nákladů (platí se jen paušální poplatek a poplatky za hovory při výpadku frame-relay). Jako alternativu lze uvažovat použití např. DSL místního poskytovatele s veřejnou IP adresou. Součástí by byl i firewall a na směrovači by se nakonfiguroval IPsec tunel.

CONCLUSION

This thesis deals with the configuration of active network elements from Cisco systems, with emphasis on a security and availability of a server application used by financial institution. The proposed configuration is one of the possible options how to solve this situation. While the use of TACACS and HSRP (or VRRP or GLBP) is almost inevitable, routing configuration and selection of WAN technologies offer a range of more or less challenging options. It is always necessary to meet the criteria and to design tailored solutions with regard to the financial possibilities of the customer.

Another factor to take into account is the risk. The risk is represented by a probability of a situation (one or more) when the server application is unavailable. A redundant topology with two switches and two routers was proposed. This fact makes it easier to deal with situations where there is a damage to the hardware (either a switch or router will not work) or access link is out of order. It is also recommended to use different providers for primary and backup connections.

As the main connection was recommended to use frame-relay link leading into the MPLS backbone of one of the major providers offering their services worldwide (eg British Telecom, Verizon). Frame-relay is not recent, but is still popular because of its flexibility and simplicity.

ISDN line was recommended as a backup link because of low running costs (there is only a flat fee plus charges for calls during frame-relay outage). DSL link with a public IP address installed by a local provider could be an alternative solution. This scenario needs a firewall and IPsec tunnel interface configured on the router.

SEZNAM POUŽITÉ LITERATURY

[1] BALÁŽ, M. *Úvod do počítačových sítí*. Brno, 2009. Bakalářská práce. Masarykova Univerzita.

[2] LAMMLE, T. CCNA*: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.

[3] HADÁČEK, P. *ISDN a videokonference*. České Budějovice, 2001. Absolventská práce. Soukromá vyšší odborná škola a obchodní akademie, s.r.o.

[4] STANKUŠ, M. *Autentizace, autorizace a accounting v prostředí IEEE 802.1X / RADIUS*. Ostrava, 2007. Ročníkový projekt. Vysoká škola báňská.

[5] WALDER, L. a T. SZKANDERA. *TACACS+*: *Instalace a konfigurace pro spolupráci s Cisco síťovými prvky*. Ostrava, 2007. Ročníkový projekt. Vysoká škola báňská.

[6] MALÍK, J. *Správa různorodých síťových zařízení pomocí SNMP protokolu*. Brno, 2011. Diplomoviá práce. Masarykova Univerzita.

[7] WALLACE, Kevin. *CCNP tshoot: 642-832 Official Certification Guide.* Indianapolis: Cisco Press, 2010. ISBN 978-1587058448.

[8] HUCABY, David. *CCNP switch: 642-813 Official Certification Guide.* Indianapolis: Cisco Press, 2010. ISBN 978-1587202438.

[8] Configuring ISDN DDR with Dialer Profiles. *Cisco Systems, Inc* [online]. [cit. 2012-05-01]. Dostupné z: http://www.cisco.com/en/US/tech/tk801/tk133/technologies_configuration_example09186a0080093c2e.shtml

[9] Configuring Secure Shell on Routers and Switches Running Cisco IOS. *Cisco Systems, Inc* [online]. [cit. 2012-05-01]. Dostupné z: http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

[10] Password Recovery Procedure for the Cisco 2600 and 2800 Series Routers. *Cisco Systems, Inc* [online]. [cit. 2012-05-01]. Dostupné z: http://www.cisco.com/en/US/products/hw/routers/ps259/products_password_recovery09186a0080094675.shtml

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization and Accounting
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CDMA	Code Division Multiple Access
CHAP	Challenge-Handshake Authentication Protocol
CIR	Committed Information Rate
DDR	Dial-on-Demand Routing
DE	Discard Eligible
DHCP	Dynamic Host Configuration Protocol
DLCI	Data link Connection Identifier
EDGE	Enhanced Data GSM Environment
FECN	Forward Explicit Congestion Notification
FHRP	First Hop Redundancy Protocols
HSDPA	High-Speed Downlink Packet Access
IBM	International Business Machines
ISDN	Integrated Services Digital Network

GLBP	Gateway Load Balancing Protocol
GNS	Graphical Network Simulator
GPRS	General Packet Radios Service
GSM	Global System for Mobile
HSRP	Hot Standby Router Protocol
HWIC	Highspeed WAN Interface Card
IOS	Internetwork Operating System
IP	Internet Protocol
LMI	Local Management Interface
MAC	Media Access Control
MD5	Message-Digest Algorithm, version 5
MIB	Management Information Base
NAT	Network Address Translation
NMS	Network Management System
NMT	Nordic Mobile Telephone
NTP	Network Time Protocol
OOB	Out of Band
PDU	Protocol data Unit
PDH	Plesiochronous Digital Hierarchy
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PVC	Permanent Virtual Circuit
RADIUS	Remote Authentication Dial In User Service
QoS	Quality of Service
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Management Protocol

SSH	Secure Shell
SVC	Switched Virtual Circuit
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
VoIP	Voice over IP
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

SEZNAM OBRÁZKŮ