ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Problematika incident managementu v podniku

Vedoucí práce: Ing. David Buchtela Ph.D.

Autor práce: Bc. Martin Vašák

Praha, 2013

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačního inženýrství

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Vašák Martin

Informatika

Název práce

Problematika incident managementu v podniku

Anglický název

Problems of Incident Management in Company

Cíle práce

Práce má za cíl představit problematiku incident managementu a seznámit s jeho jednotlivými oblastmi. Hlavním výstupem práce je pak konkrétní návrh aplikace, participující na řešení potřeb zajištění služby (SA) u telekomunikačního operátora.

Metodika

Vytvoření teoretické (rešeršní) části diplomové práce bude založeno na studiu a analýze odborných informačních zdrojů týkajících se problematiky incident managementu u telekomunikačního operátora. V první části práce bude popsána problematika incident managementu. Na základě těchto soustředěných teoretických znalostí bude ve druhé, praktické části práce, navržena konkrétní aplikace splňující podmínky úvodního zadaní. Na základě syntézy teoretických poznatků a výsledků praktické části pak budou formulovány závěry práce.

Harmonogram zpracování

06/2012-08/2012 Upřesnění zadání práce a shromažďování literárních zdrojů
09/2012 Kontrola průběhu práce - 1.zápočet
09/2012-12/2012 Analýza informačních zdrojů a tvorba rešeršní části práce
01/2013 Kontrola průběhu práce - 2.zápočet
01/2013-02/2013 Vypracování praktické části práce
03/2013 Finalizace práce a odevzdání, 3.zápočet

Rozsah textové části

60 - 80 stran

Klíčová slova

incident management, fault management, telekomunikační síť, SNMP, MIB, RCA - root cause analysis, OSS - Operational Support System, BSS - Bussiness Support System

Doporučené zdroje informací

DINI, P, Pascal LORENZ a Jose´ Neuman de SOUZA. Service assurance with partial and intermittent resources: First International Workshop, SAPIR 2004, Fortaleza, Brazil, August 1-6, 2004 : proceedings. New York: Springer, c2004, 312 s. ISBN 35-402-2567-6.

STALLINGS, William. SNMP, SNMPv2, and CMIP : The Practical Guide to Network-Management Standards. Reading, Massachusetts : Addison Wesley, 1993. 625 s. ISBN 0-201-63331-0.

Vedoucí práce

Buchtela David, Ing., Ph.D.

Termín odevzdání

březen 2013

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.

Děkan fakulty

V Praze dne 8.10.2012

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem „Problematika incident managementu v podniku“ zpracoval samostatně za použití uvedené literatury a po odborných konzultacích s Ing. Davidem Buchtelou Ph. D.

V Praze dne 31. března 2013 _____

PODĚKOVÁNÍ

Děkuji tímto panu ing. Davidu Buchtelovi Ph.D. za odborné vedení a rady při zpracování této diplomové práce a hlavně za schovívavost, se kterou ke mně přistupoval.

Dále děkuji Mgr. Davidu Šebkovi za trpělivost, podporu a jazykovou korekturu a kolegům Bc. Jaroslavu Dudovi a Bc. Romanovi Brixí, bez jejichž tlaku by tato práce nikdy nevznikla.

Problematika incident managementu v podniku

Problems of Incident Management in Company

Souhrn

Práce se detailně věnuje problematice incident managementu jako důležité součásti tématu řízení sítí. V první části je nejprve pojem incident managementu vymezen. Následně je představen v souvislostech s platnými ISO standardy.
V pokračování rešeršní části jsou pak představeny jednotlivé funkční celky včetně vzájemných vazeb, které incident management zahrnuje. Součástí tohoto teoretického úvodu je i podrobný popis TMN modelu a korelačních metod používaných při zpracování alarmu. Ve druhé části práce je pak představena autorem vytvořená reálná aplikace řešící incident management u konkrétní zákaznické služby nabízené v rámci portfolia datových služeb telekomunikačního operátora.

Klíčová slova: Incident management, telekomunikační síť, SNMP, MIB, RCA – Root Cause Analysis, OSS – Operational Support System, BSS – Business Support System

Summary

This diploma thesis is dedicated to network management principles, mainly focused on incident management. It begins with a definition of incident management followed by an explanation in corresponding to ISO standards. Later in this theoretical prologue are introduced all functional elements of incident management including relations between them. Prologue also consists of detailed description of the TMN model and method of alarm correlation. The second, practical part of this thesis describes the author-developed real application which solves incident management issues connecting with one particular customer service, offered as a part of a portfolio of data services, provided by a telecommunication operator.

Keywords: incident management, telecommunications network, SNMP, MIB, RCA – Root Cause Analysis, OSS – Operational Support System, BSS – Business Support System

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V současné době si už málokdo z nás uvědomuje, jak silnou závislost má dnešní společnost na telekomunikačních službách. Ve většině případů tyto telekomunikační služby bereme jako samozřejmou součást moderního života a zcela automaticky předpokládáme jejich stálou dostupnost a plnění očekávaných funkcí na vysoké úrovni kvality. Například jakákoliv náhlá ztráta možnosti využití funkcionalit mobilního telefonu (ať už pro hlasový hovor nebo stále častěji pro datový přenos) v nás vyvolá prudké rozčarování, mnohdy i vztek nebo dokonce paniku. Opět jen malá část z nás si uvědomuje, jak rychlý vývoj služeb realizovaných prostřednictvím telekomunikačních sítí[1] v posledních letech probíhá. Například telekomunikační operátor Telefonica O2 [21] uvádí, že datový provoz ve fixní části sítě se za poslední dva roky zvýšil ve špičkách o 80 %; celkový objem dat přenesených fixní sítí tohoto operátora na území ČR byl v prosinci 2012 již 34500 TB dat. Velkou část tohoto provozu generují xDSL služby, kde sice počet zákazníků roste velmi pomalu, ale přístupová rychlost, kterou využívají, se zvyšuje skokově.

Nezvyšují se však jen nároky na přenosové kapacity. Prodej samotné přenosové kapacity totiž již dlouho není z pohledu operátorů zdrojem požadovaných příjmů. Nezbytné příjmy jsou v dnešní době generovány výhradně nabídkou ucelených služeb a komplexních řešení. Tyto požadavky však často vyvolávají potřebu velmi složitých řešení založených na nových - ne vždy dostatečně otestovaných - technologiích. Takto komplexně realizované služby je však nezbytné dodávat v požadované vysoké kvalitě. Silná konkurence na liberalizovaném telekomunikačním trhu žádná pochybení nepromíjí. Se vznikem každé nové služby je tak s předstihem potřeba řešit nejen otázky jejího technického zajištění, ale mnoho dalších oblastí, jakými jsou například plánování kapacit (přenosových, technologických a lidských) či sestavování procesů zřizovaní a provozování služby.

[1] Telekomunikační sítí bude v textu této práce chápána datová/hlasová síť včetně souboru všech prvků a přenosových cest, které zajišťují nebo podporují její činnost. Synonymem pro telekomunikační sít užívaným dále v textu budou slova „síť", „komunikační síť" nebo „network" [1].

Právě úkoly vyplývající z provozování služby zahrnují mimo jiné i vytvoření fungujícího a efektivního incident managementu, tedy oblasti, které se podrobně věnuje tato diplomová práce.

2 Cíl práce a použitá metodika

Cílem této diplomové práce je praktická realizace aplikace podporující incident management konkrétní datové služby telekomunikačního operátora. Tato aplikace musí splňovat předem stanovené zadání vyplývající z definice služby, maximálně využívat již dostupných informačních bází firmy, respektovat její technickou a procesní infrastrukturu a plnit očekávané přínosy.

Pro dosažení výše uvedeného cíle je nejprve v první části práce provedeno rešeršní zpracování problematiky incident managementu. Zdrojem pro tuto část je studium odborné literatury, souvisejících internetových zdrojů a produktových manuálů. Ve druhé, praktické části této diplomové práce je pak představeno konkrétní, v praxi realizované, autorovo řešení. Toto řešení vzniklo na základě rešerší získaných znalostí, několikaletých pracovních zkušeností autora v oblasti incident managementu a dodatečnými konzultacemi s dalšími odborníky.

3. Přehled problematiky incident managementu

Jak již bylo zmíněno v úvodu této práce, nedílnou součástí každé realizované služby by mělo být zajištění i oblasti incident managementu. Tato práce se bude věnovat procesům souvisejícím s telekomunikačními službami, které se mohou v detailech od jiných služeb lišit. Základní principy však zůstávají zachovány.

V práci bude v maximální míře používáno české názvosloví. Vzhledem ke zmíněné specializaci bude v případech, kdy by mohl být ohrožen významový smysl předkládané informace, použit originální anglický výraz s patřičným vysvětlením. Většina použitých přejatých vyobrazení je také prezentována v českém překladu. Výjimečně některá firemní vyobrazení byla ponechána v původní anglické verzi.

Následující text přináší rešerši problematiky incident managementu, která bude v praktické části využita při realizaci konkrétní aplikace.

3.1 ITIL

V následujících částech práce bude často odkazováno na ITIL. ITIL je zkratkou pro Information Technology Infrastructure Library. Jedná se o sadu doporučení, praktik pro poskytování ICT služeb. Jde o veřejně přístupný, ucelený rámec pokrývající komplexní životní cyklus ICT služby, který se skládá z pěti fází [10]:

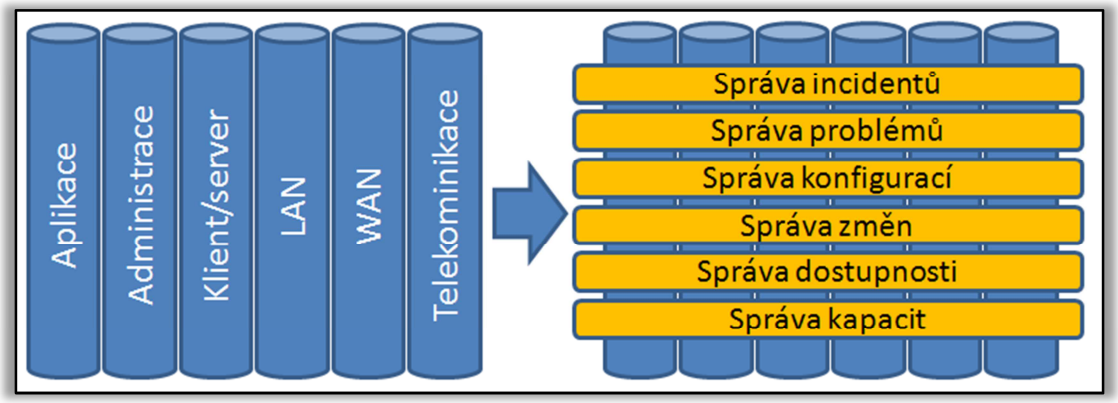
- Strategie služeb (service strategy);
- Návrh služeb (service design);
- Implementace služeb (service transition);
- Provoz služeb (service operation);
- Zlepšování služeb (continual service improvement).

Strategie služeb lze chápat jako návod, jak se navrhuje, vyvíjí a implementuje správa služeb. Service design nabízí návody pro návrh a vývoj služeb a procesů. *Návrh služeb* se stará o zavádění nových nebo pozměněných služeb do produkčního prostředí. *Provoz služeb* se zabývá činnostmi s ohledem na účinnost a efektivitu dodávky a provozu služby. *Zlepšování služeb* poskytuje nástroje a návody pro nepřetržité zlepšování služeb a všech předešle zmíněných aspektů jako je návrh, zavádění a provoz služby. Tyto jednotlivé fáze na sebe navazují a zároveň si předávají zpětnou vazbu. Tím

dochází k uzavření celého cyklu, který navazuje na životní cyklus obchodního procesu služby.

Díky šíři rozsahu ITIL svým záběrem zasahuje do firemní struktury, do firemních procesů a částečně i do samotných ICT technologií. Tvoří jakousi část pomyslné pyramidy, jejímiž základy jsou firemní procesy, nad tím postavené HP ITSM[2] a MS SMF[3] (jakožto technologické upřesnění), nad tím samotné ITIL (coby definované procesy). Předposlední patro tvoří ISO 20000-2 (jako doporučení ke zdokonalování) a samotnou špičku této pomyslné pyramidy pak ISO 20000-1 (jakožto souhrn požadavků) [11].

ITIL je veřejně dostupný rámec, což oproti proprietárním pracím a znalostem přináší například tu výhodu, že předkládaná doporučení jsou ověřena v různých prostředcích a situacích a neplatí tedy jen v omezené množině případů. V úvodu byl ITIL sbírkou více jak 40 knih o správě služeb. Jím tvořená knihovna nabízela nejobsáhlejší definici procesů ICT služeb. V průběhu let 1999 až 2004 byl ITIL modernizován (viz obrázek č. 1) a vydán v nové sadě knih jako ITIL v2. Další verze byla zveřejněna v roce 2007 pod názvem ITIL v3. Obsahovala hlavně aktualizaci obsahu a provázanost s dalšími doporučeními a normami. Poslední verze byla vydána v roce 2011 a je označena jako ITIL Edice 2011.



Obrázek č. 1 – Změna struktury ITIL od verze 2. /Překresleno z [9]./

[2] ITSM – IT Service Management (Hewlett Packard).
[3] SMF – Service Management Function (Microsoft).

3.2 Vymezení termínů

3.2.1 Služba

Služba je prostředek tvorby hodnot pro zákazníky. Poskytuje zákazníkům sjednané výsledky, aniž by tito museli nést zodpovědnost za specifické náklady a rizika spojená se službami. O službě hovoříme, že je zákaznicky orientovaná v případě, že přímo podporuje podnikové procesy jednoho či více zákazníků a má ve smlouvě a úrovni dodávané služby (SLA[4]) definovány jasné a měřitelné cíle její úrovně.

ITIL pro určení hodnoty služby tak, jak ji vnímá zákazník, používá dva úhly pohledu. První z nich ji stanovuje přes hodnotu *užitečnosti*, druhý pak přidává spolehlivost služby danou *zárukou*.

V rámci záruky se pak vyhodnocují tyto parametry:

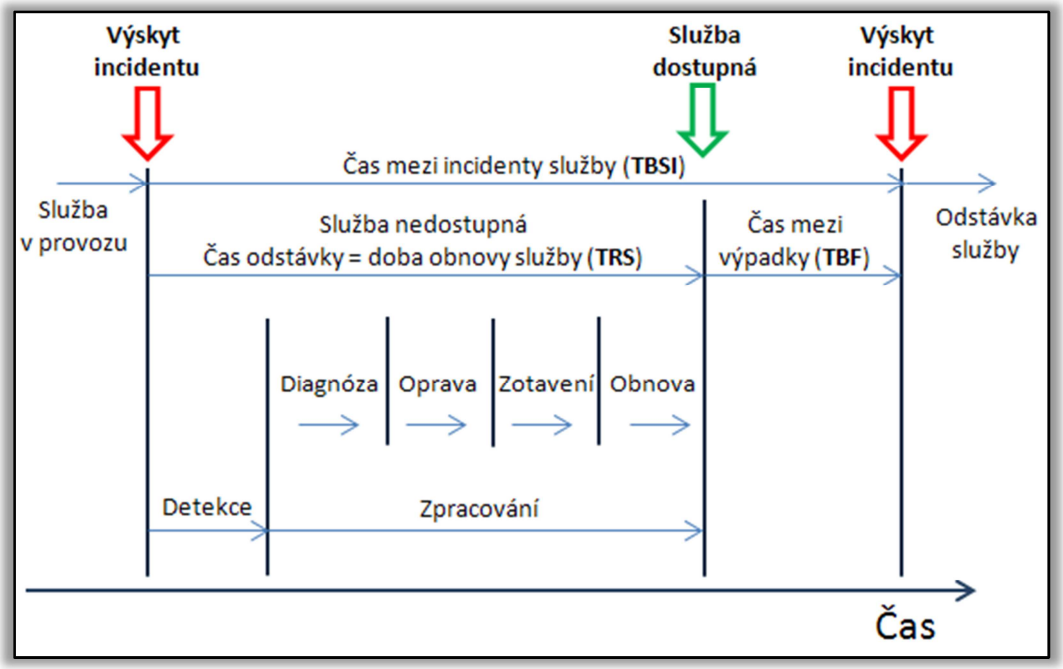
- Dostupnost – schopnost služby provést v případě potřeby očekávanou (smluvenou) funkci. Pro výpočet dostupnosti služby se používá následující vztah: $Dostupnost\ \% = \frac{Doba\ provozu\ služby - Doba\ výpadků}{Doba\ provozu\ služby} * 100$;
- Kapacita – maximální výkon, který je služba schopna poskytnout při dodržení cílů domluvené úrovně služby;
- Nepřetržitost – zajištění, že daná služba bude podporována v případě nějakého výjimečného stavu;
- Bezpečnost – zajištění ochrany firemních hodnot.

V souvislosti s *dostupností* služby se uvažuje i tzv. *udržitelnost*. Ta udává, jak rychle a efektivně je po výpadku možné službu obnovit. Obvykle se udává pomocí *střední doby obnovení služby* (MTRS[5]), která se určí ze vztahu:

$$MTRS\ (hod) = \frac{Celkový\ čas\ výpadku\ (hod)}{Počet\ přerušení\ služby} * 100\ .$$

Klíčové pojmy dostupnosti služby jsou patrné z obrázku č. 2.

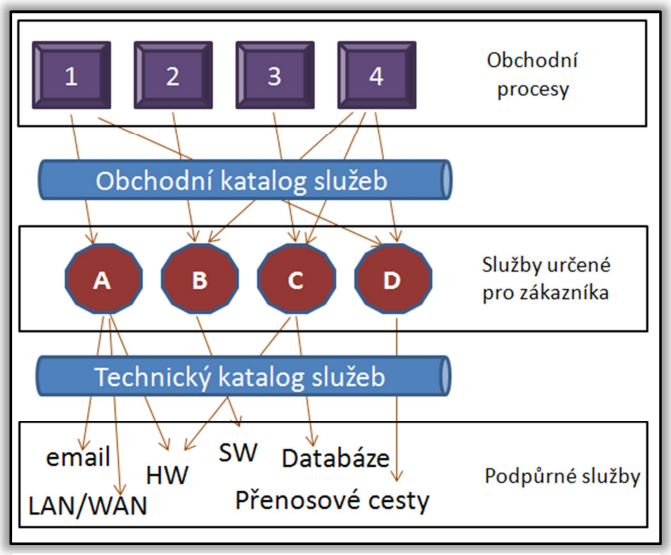
[4] SLA – Service Level Agreement.
[5] MTRS – Mean Time to Restore Service.



Obrázek č. 2 – Klíčové pojmy dostupnosti služby. /Překresleno z [9]./

3.2.2 Katalog služeb

V katalogu jsou popsané všechny provozované služby obvykle dle jejich hierarchie. Ta se může lišit z pohledu obchodu (tedy zákazníka) a z pohledu technologie (tedy providera služby). Tento rozdíl je v katalogu služby zohledněn jeho rozdělením na obchodní a technický katalog. Obchodní obsahuje všechny nabízené služby zákazníkům a tvoří propojení na obchodní procesy (oblast BSS[6] systémů).



Obrázek č. 3 - Schéma doporučované architektury servisního katalogu dle ITIL. /Upraveno z [9]./

Technický katalog pak obsahuje technické detaily ke všem

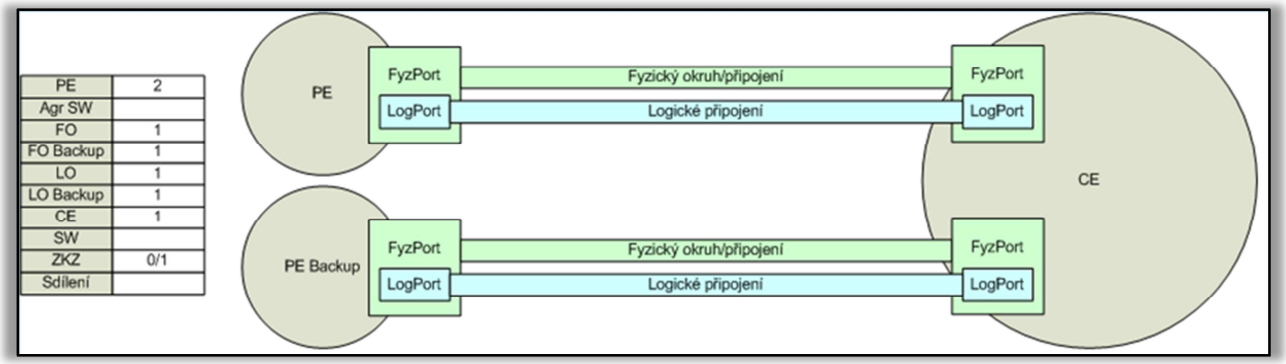
[6] BSS – Bussiness Support Systems.

službám a zajišťuje provázanost na systémy podpory provozu (OSS[7]). Tyto technické detaily musí jít na takovou úroveň, aby šla služba v reálně zřídit. Této úrovni obvykle vyhovuje dekompozice služby na jednotlivé konfigurační položky (CI[8]), které mohou reprezentovat například konkrétní port, logický nebo fyzický okruh nebo jinou službu. Schéma doporučované architektury servisního katalogu dle ITIL je na obrázku č. 3. Na obrázku č. 4 je pak zobrazen příklad služby zálohovaného připojení routeru zákazníka do sítě providera tak, jak je zachycen v technické části servisního katalogu. Jednotlivé konfigurační položky (CI) jsou odlišeny barevně a jejich celkový soupis je uveden v levé části obrázku. Katalog služeb je obvykle úzce provázán s databází konfigurace sítě (inventory databáze) a systémy podpory procesů zřizování služeb (workflow systémy).

3.2.3 Incident

Pojem incident má v praxi širokou škálu významů, proto je vždy třeba vymezit oblast, kde jej používáme, a konkretizovat pro tuto oblast jeho význam.

Ve smyslu normy *BS 25999-1:2006 Business continuity management – Part 1: Code of practice* je incidentem jakákoliv událost, která má za následek ztrátu či poškození aktiv společnosti.



Obrázek č. 4 - Příklad zachycení služby zálohovaného připojení routeru zákazníka v katalogu služeb.

[7] OSS – Operation Support Systems (viz kapitola 3.4).
[8] CI – Configuration item.

Ve smyslu normy ISO 20001 odst. 2.7 - je incidentem jakákoli událost, která není součástí běžného fungování služby a která způsobí nebo může způsobit přerušení dodávky nebo snížení kvality služby.

Výše citované normy jsou z oblasti bezpečnosti (Business continuity management) a z oblasti IT (ISO 20001).

Dle ITIL je incident (porucha) neplánovaným přerušením služby nebo snížením kvality služby (IT). I jakýkoliv výpadek komponenty služby, který nemá na službu jako celek vliv, je považován za incident. Jedná se totiž o událost nepatřící ke standardnímu provozu a tedy představující reálné nebo teoretické nebezpečí narušení nebo snížení kvality dodávané služby.

Další související pojmy jako bezpečnostní incident, provozní incident, globální incident, uživatelský incident a další konkrétně vymezují pojem incidentu pro daný konkrétní proces.

3.2.3.1 Problém

Související termín *problém* je dle ITIL definován jako příčina jednoho nebo více incidentů. Je-li tato příčina problému již známa, je možné, že už existuje také její řešení. To je důvodem, proč by měla být již použitá řešení vždy řádně dokumentována.

V této práci nebude na rozdíl mezi termíny incident a problém brán ohled kromě případů, kdy by záměnou mohlo dojít k ovlivnění významu předkládané informace.

3.2.4 Incident Management

Incident management je souhrnný název pro soubor postupů, procesů a nástrojů za účelem řešení incidentů existujících nebo potencionálních (viz kapitola 3.2.3).

ITIL definuje incident management jako správu incidentů, která je zaznamenává, zkoumá, kategorizuje, prioritizuje a sleduje tak, aby byly vyřešeny co nejdříve a s minimálními dopady na uživatele.

Hlavními cíli incident managementu jsou [22]:

- Efektivní a rychlý návrat stavu služby na úroveň domluvené nebo očekávané kvality;
- Minimalizování dopadů výpadku na uživatele;
- Příprava a implementace oprav a úprav služby, jsou-li vyžadovány;
- Minimalizace opakovaných incidentů.

V souvislosti s předešlými body je vhodné ještě uvést definici dvou následujících užitých pojmů.

3.2.4.1 Kvalita

Kvalita se dle normy ISO 402 chápe jako soubor vlastností a znaků konkrétního produktu/služby, který je důležitý pro splnění pevně daných nebo samozřejmých služeb. *Účinnost* naproti tomu staví na vyhodnocení poměru vstup--výstup, tedy na dosažení co možná nejvyšší výtěžnosti s pomocí daných prostředků, nebo dosažení definovaných výsledků s využitím minima zdrojů.

3.2.4.2 Efektivita

Efektivita vyjadřuje, jestli bylo dosaženo definovaného cíle, a vypovídá o tom, zda byly činěny správné kroky k jeho dosažení.

3.2.5 Service desk

Service desk je primárním kontaktním místem (často se používá i termín SPoC[9]), se kterým komunikuje zákazník v případě jakýchkoliv požadavků týkajících se jeho služeb. Rozhraní pro komunikaci se service deskem obvykle umožňují využít telefonické nebo emailové komunikace, často jsou však rozšířena i o webová rozhraní. Hlavním úkolem service desku je dohlížet službu zákazníka a dohlížet řešení jeho požadavků. Dle ITIL rozeznáváme následující typy service desku:

- Centrální service desk – jediné pracoviště obsluhující všechny zákazníky;
- Lokální service desk – existuje více specializovaných pracovišť dělených dle různých hledisek. Například podle typu obsluhovaných zákazníků (interní,

[9] SPoC – Single Point of Contact.

externí, externí korporace, externí retail apod.) nebo služeb (hlasové, datové, přenosové apod.);

- Virtuální service desk – service desk není fyzicky umístěn na jediném místě ale rozprostřen přes více lokalit. Zákazníkovi se však jeví jako jediné pracoviště;
- Service desk „následujícího slunce“ – zvláštní případ virtuálního service desku. Ten je geograficky rozmístěn v takových časových pásmech, aby zajistil potřebu být k dispozici v režimu 7x24.

Podle toho, jak k řešení incidentů a problémů Service desk přistupuje, označujeme jeho pracovní režim jako:

- Proaktivní – service desk se snaží problémům a incidentům zabránit a předcházet (například systematickým sledováním logů, zátěže apod.). Pokud incident ale nastane, je řešen okamžitě bez ohledu na to, zda ho uživatel služby oznámil;
- Reaktivní – vzniklé problémy a incidenty se řeší, až když nastanou a většinou až po té, když o jejich řešení požádá zákazník.

Poznámka: Proaktivní přístup je obvykle nabízen jako nadstavbová, vyšší úroveň služby. Z toho obvykle vyplývá vyšší celková cena služby ale taky některé povinnosti pro zákazníka. Mezi ně patří například povinnost nedegradovat dodávanou službu například odpojováním koncových zařízení (mimo stanovenou dobu, pokud je stanovena).

3.3 Proces incident managementu

Příloha 7.1 představuje proces incident managementu tak, jak ho ve svých doporučeních přináší ITIL. Obsahuje tyto základní aktivity:

3.3.1 Identifikace incidentu

Jedná se o začátek celého procesu. Některým z definovaných kanálů byl detekován incident. Tímto kanálem může být informace nebo požadavek od uživatele

služby, ale také informace, kterou dodá některý z dohledových nástrojů řízení sítě, jak bude představeno dále (kapitola 3.4).

3.3.2 Záznam incidentu

Každý příchozí incident je nutné zaevidovat ve formě *záznamu o incidentu*. Záznam následně slouží k evidenci všech provedených kroků v průběhu celého řešení. Je vždy základním zdrojem informací pro daného řešitele, kterých se může na řešení právě jednoho incidentu podílet postupně nebo zároveň více. Po jeho ukončení slouží záznamy k výpočtům kvalitativních údajů o službě, ale také jako zdroj informací pro vytváření postupů pro řešení podobných typů incidentu v budoucnosti nebo dokonce k předcházení těmto opakovaným incidentům.

3.3.3 Kategorizace

Kategorizace incidentů má zásadní vliv na další kroky a také na smysluplnost informací správy jakož i další vyhodnocení. Přidělenou kategorii je potřeba během životního cyklu incidentu kontrolovat a např. po uzavření poruchy opravit. Toto je zvlášť důležité pro bezpečnostní incidenty [9].

3.3.4 Přidělení priority

Priorita zohledňuje, jak rychlé se vyžaduje řešení (naléhavost) a jaký má dopad. Dopadem je například počet ovlivněných zákazníků. Priorita se během trvání incidentu také může měnit.

3.3.5 Úvodní diagnóza

Ve chvíli, kdy se incident dostane ke správě incidentů, zaměstnanec service desku zahajuje prvotní řešení, například dle doporučení vycházejících z řešení shodného typu incidentu dříve. Pokud se tato úvodní diagnóza nezdaří, dochází k eskalaci.
V tomto kroku neprobíhá žádné hlubší zkoumání příčin [9].

3.3.6 Zkoumání a diagnóza

V tomto kroku vyšší úrovně podpory se hledají řešení incidentu. Vše se stále dokumentuje v záznamu incidentu.

3.3.7 Řešení a obnova

Je-li nalezeno odpovídající řešení, je v tomto kroku implementováno. Součástí je jeho otestování.

3.3.8 Ukončení

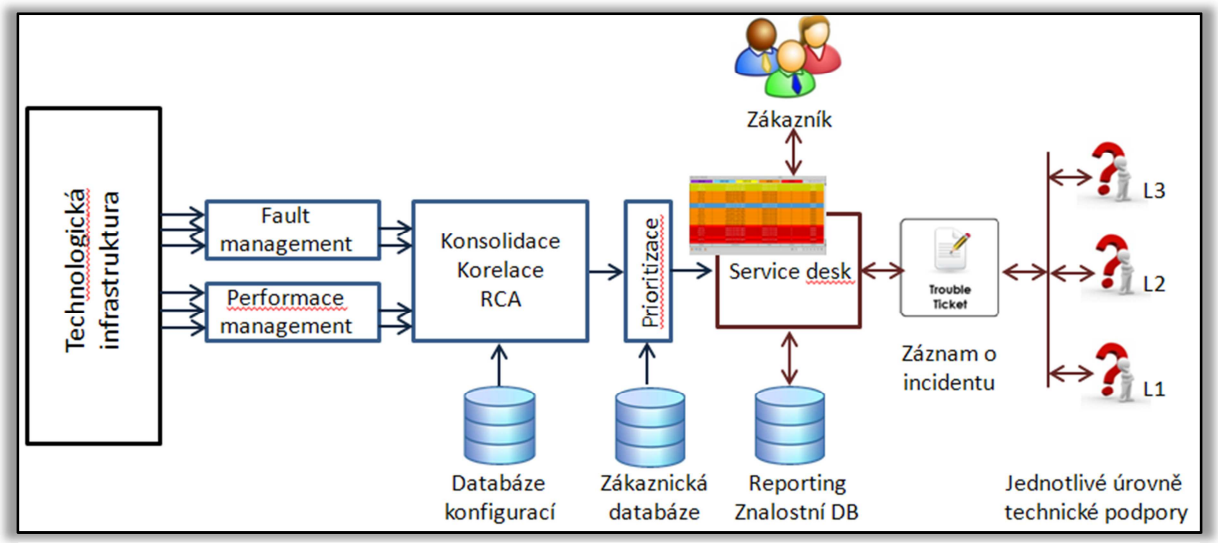
Pro ukončení incidentu si je třeba vyžádat souhlas zákazníka, pokud byl incident zákazníkem nahlašován, nebo pokud se se zákazníkem pracuje v proaktivním režimu. V případě, že incident vznikl na základě hlášení prostředků řízení sítě a neovlivnil obsluhovaného v proaktivním režimu, incident může být uzavřen po otestování.

3.4 Prostředky OSS podporující incident management

Systémy podporující provoz se často označují jako OSS, z anglického Operational Support Systems. Mezi úkoly těchto systémů patří:

- Pasivní dohled sítě (příjem událostí generovaných v síti, čtení logů apod.);
- Aktivní dohled sítě (aktivní zjišťování stavu jednotlivých komponent);
- Správa a konfigurace;
- Reporting.

Všechny tyto úkoly jsou vyžadovány i pro zajištění požadavků na incident management. Jedno z možných řešení, jak se procesů řešení incidentů účastní, je představeno na obrázku č. 5.



Obrázek č. 5 - Jeden z možných způsobů řešení incident managementu.

Levá část obrázku zahrnuje bloky fault a performance managementu včetně konsolidace, korelace a RCA alarmových vstupů. Tato část patří pod oblast řízení sítí,

podporuje procesy incident managementu a bude podrobně představena v následujících kapitolách věnovaných právě tématu řízení sítí.

3.5 Řízení sítě

3.5.1 Model TMN

Telekomunikační síť představuje složitý kybernetický stroj rozprostřený obvykle ve velké geografické oblasti. Aby bylo možné zvládnout úspěšně všechny procesy spojené s provozem sítě, je nutné síť systematicky rozčlenit na menší, logicky provázané celky. Vhodným prostředkem, dnes často používaným i v mnoha dalších technických oblastech, je princip vrstvené struktury [5].

Základní vrstvy telekomunikační sítě:

- Fyzická vrstva sítě je tvořena spojovacími a přenosovými zařízeními a přenosovými médii (včetně podpůrných systémů);
- Logickou (transportní) vrstvu tvoří přenosové cesty, ať už fyzické, nebo logické;
- Služební vrstva slouží pro řízení v reálném čase spojovacích procesů s uspokojováním potřeb jednotlivých okruhů a služeb (zahrnuje signalizační systémy);
- Řídicí vrstva sleduje činnost všech ostatních síťových vrstev a zajišťuje optimální přiřazení prostředků službám v globálním měřítku z hlediska maximální efektivnosti telekomunikační sítě. Funkce řídicí vrstvy vykonává tzv. řídicí síť telekomunikací, označovaná zkratkou TMN[10].

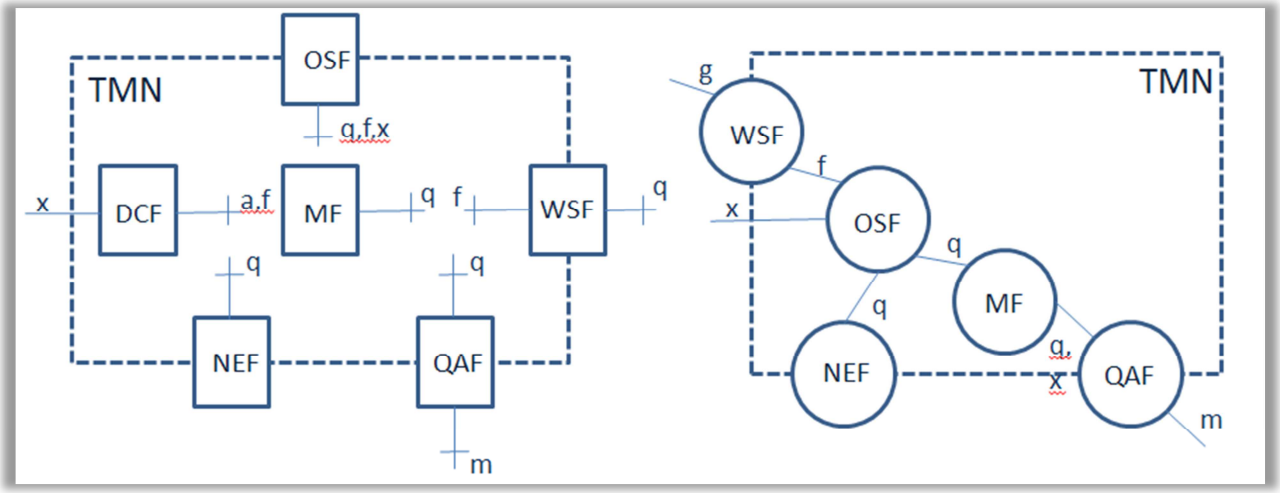
Problematikou TMN se začala zabývat již v polovině 80. let řada mezinárodních normalizačních institucí, například CCITT, EYSI, ANSI, ISO atd. Ještě do konce roku 1992 vniklo více jak 20 doporučení týkajících se TMN [5].

V rámci kompletního výkladu vlastností modelu TMN lze na tento model pohlížet v několika rovinách, které budou vysvětleny dále.

[10] TMN – Telecommunications Management Network.

3.5.1.1 Funkční model TMN

Funkční model TMN představuje rozložení funkcionalit TMN za využití funkčních bloků (OSF). Tyto funkční bloky jsou navržené tak, aby se jejich kombinací dal poskládat libovolně složitý TMN model. Jednotlivé funkční bloky se stýkají v tzv. referenčním bodě neboli interface. Dva různé pohledy na základní funkční bloky a referenční body TMN modelu jsou zobrazeny na obrázku č. 6. Levá část obrázku je zpracována dle [5], pravá pak dle [6]. Rozdíl spočívá v integraci bloku DCF do



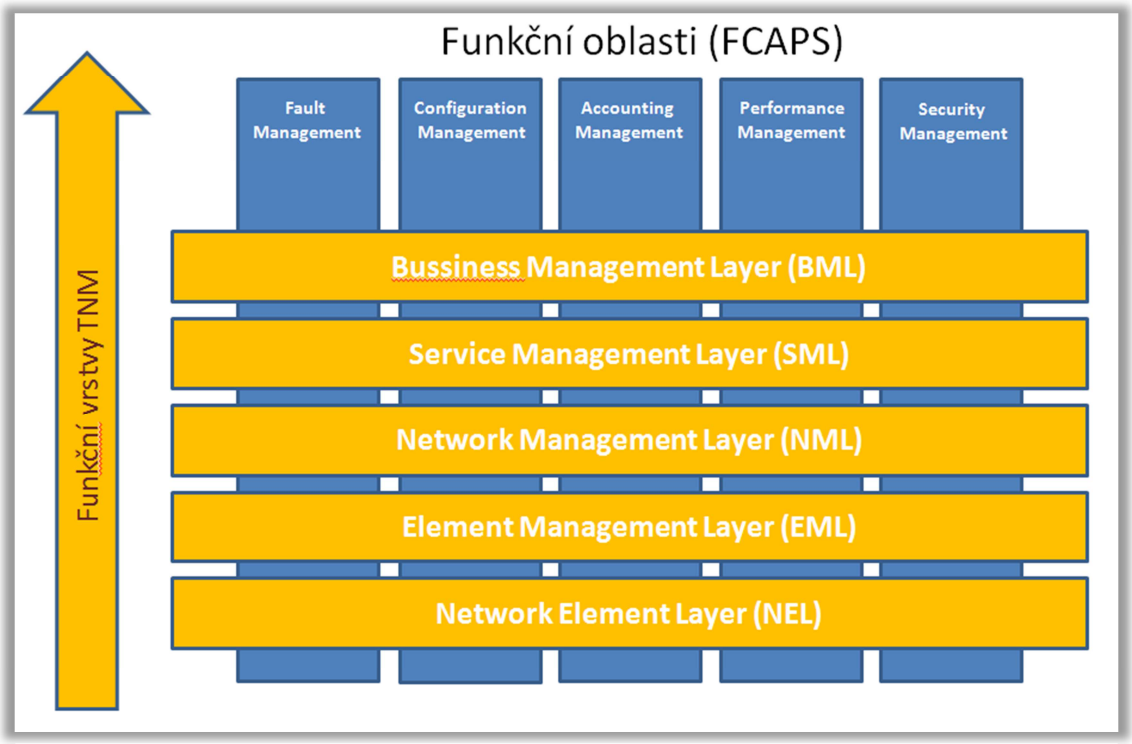
Obrázek č. 6 - Dva různé pohledy na základní funkční bloky a referenční body TMN modelu. /Zdroj: autor podle [5] a [6]./

Význam jednotlivých bloků vyznačených v modelu je následující:

- NEF (funkční blok síťového prvku). Blok je pod přímým řízením OSF. Obsahuje jak řídicí funkce přímo související s telekomunikačním procesem (přenos, spojování), tak podpůrné funkce (například účtování);
- MF (blok zprostředkovacích – mediačních funkcí). Ovlivňuje komunikaci mezi OSF a NEF (nebo QAF) za účelem standardizace této komunikace do jednotného formátu;
- WSF (funkční blok pracovní stanice). Jedná se o blok tvořící interface mezi TMN a člověkem;
- QAF (funkční blok Q-adaptér). Tento blok slouží jako rozhraní pro propojení a úspěšnou komunikaci TMN entit s entitami, které TMN přímo nebo vůbec nepodporují.

- DCF (funkce přenosu dat). Podpůrný blok, v jehož kompetenci je zajištění přenosu informací mezi ostatními bloky TMN. Obsahuje jak přenosový a směrovací mechanismus (zajištění síťové role), tak přístupový mechanismus pro připojení MCF[11].

Funkčních bloků (OSF) existuje mnoho typů. Jedna z jejich možných kategorizací je dle míry abstrakce. Tento způsob vede na jinou formu prezentace funkčního modelu, na tzv. vrstvový model (viz obrázek č. 7).



Obrázek č. 7 – Vrstvový model jako jiný způsob prezentace funkčního modelu.

Jednotlivé funkční vrstvy modelu (v obrázku vyznačeny modře) zajišťují následující funkcionality:

- Vrstva sítě (Network Element Layer – NEL) představuje vlastní síťové prvky a zařízení tvořící přenosovou část telekomunikační sítě. Prvky jsou na této úrovni řízeny zcela nezávisle na ostatních prvcích sítě;

[11] MCF – funkce přenosu zprávy. Obsahují ji všechny funkční bloky s fyzickým rozhraním, slouží pro výměnu řídicích informací subjektů ležících na shodné úrovni.

- Vrstva řízení síťových prvků (Element Management Layer – EML) obsahuje řídicí rozhraní do jednotlivých prvků sítě. V této úrovni se prvky sítě řídí již po skupinách, které obvykle tvoří funkční či doménové celky;
- Vrstva řízení sítě (Network Management Layer – NML). V této úrovni je již síť řízena jako celek (systémem end-to-end). Síťový management zde zajišťuje celkovou integritu sítě;
- Vrstva řízení služeb (Service Management Layer – SML) se na síť dívá již jako na zdroj služeb pro koncové uživatele. Řízení je tedy v úrovni služeb. Patří sem již workflow objednávek, řešení stížností, zpoplatňování (billing) nebo i například sledování kvality a dostupnosti služeb;
- Vrstva řízení obchodních aktivit (Bussiness Management Layer – BML). Tato vrstva je vrcholem abstrakce a řeší obchodní stránky provozování sítě - jako je například plánování a řízení finančních zdrojů, sledování rozpočtů, vytváření rozvojových strategií a podobně.

Dále jsou v tomto funkčním modelu definované funkční vlastnosti řídicích aplikací TNM. Tyto vlastnosti jsou dle doporučení TMN (M.3400) organizace ITU-T rozděleny do pěti řídicích oblastí, často souhrnně označovaných zkratkou FCAPS – Fault, Configuration, Accounting, Performance, Security Management. Mezi úkoly, které tyto řídicí oblasti zahrnují, patří například plánování, instalace, správa a obsluha telekomunikačních sítí a služeb. Stručný popis těchto jednotlivých řídicích oblastí:

- Fault Management (řízení poruch) je funkcí, jejímž hlavním cílem je odhalení (detection), izolace (isolation) a náprava (correction) výjimečného provozního stavu telekomunikační sítě. V předcházející bakalářské práci [1] byly zmíněny tyto hlavní úkoly fault managementu [3]:
  - Informovat o nastalém výjimečném stavu (chybě, výpadku) ihned v čase jeho výskytu a klasifikovat jeho závažnost (severity),
  - rychle a správně identifikovat místo, kde k chybě došlo,
  - izolovat zbytek sítě tak, aby chyba neovlivňovala funkční část sítě,
  - zahájit nápravu za účelem minimalizace dopadů závady,
  - odstranit závadu pro návrat provozu do původního stavu.

- Configuration management (řízení konfigurací) zajišťuje konfiguraci sítě tak, aby stav konfigurace jednotlivých prvků podporoval zajištění požadovaných služeb.
- Accounting Management (řízení účtování) obsahuje sadu funkcí pro sběr dat o zdrojích, jenž se podílí na poskytování služby. Souvisejícím úkolem accounting managementu je na základě těchto získaných dat následné generování účtů (kalkulace na základě objemu přenesených dat, délky přenosů, plnění SLA[12] apod.)
- Performance Management (Řízení výkonnosti)[13] sestává z řady funkcí monitorujících prvky sítě a jejich parametry využití a získané hodnoty dále zpracovávají a následně archivují.
- Security Management (řízení zabezpečení) sestává z řady funkcionalit pro zabezpečení síťových komponent a přenášených dat. Řeší například přidělování odpovídajících práv uživatelům či uživatelským skupinám, provádí autentikaci a autorizaci uživatelů, zajišťuje šifrování tam, kde je vyžadováno.

3.5.1.2 Informační model TMN

Informační model vytváří pohled do řídicích procesů. Je založen na objektově orientovaném přístupu, mapuje řídicí principy OSI do prostředí TMN a podle potřeb ho rozšiřuje. Řízené objekty chápe jako logické moduly fyzických prostředků, topologických struktur a fyzikálních procesů, které existují a mohou být řízeny proto, aby podporovaly řídicí funkce telekomunikačního procesu (např. konfiguraci sítě, zaznamenávání běhu událostí atd.). Řízený objekt je abstrakcí prostředku, který představuje jeho vlastnosti, tak jak se jeví z pohledu řízení [5].

Řízený objekt je dle [5] definován:

- atributy, tj. kvantitativními nebo kvalitativními parametry pozorovatelnými na svých hranicích,
- řídicími povely, které na něj mohou být z vnějšku aplikovány,

[12] SLA – Service Level Agreement. Dohodnutá záruka o měřitelné kvalitě poskytované služby.
[13] Performance management – aplikování řídicích přístupů s cílem zajistit plnění požadovaných výkonnostních parametrů [4].

- chováním, které vykazuje jako odezvu na řídicí povely nebo jako reakci na vnitřní systémové podněty,
- hlášeními, kterými podává informace o svém stavu.

3.5.1.3 Fyzický model TMN

Fyzická architektura TMN popisuje využitá rozhraní a jednotlivé fyzické bloky TMN. Realizace těchto fyzických bloků se může lišit, každý může implementovat jednu nebo více funkcí vyplývajících z funkčního modelu. Mezi tyto fyzické bloky patří:

- operační systém (OS),
- síťový prvek (NE),
- zprostředkovací (mediační) zařízení (MD),
- Q adaptér (QA) – slouží pro připojení řešení nekompatibilních s TMN,
- datová komunikační síť (DCN),
- pracovní stanice (WS).

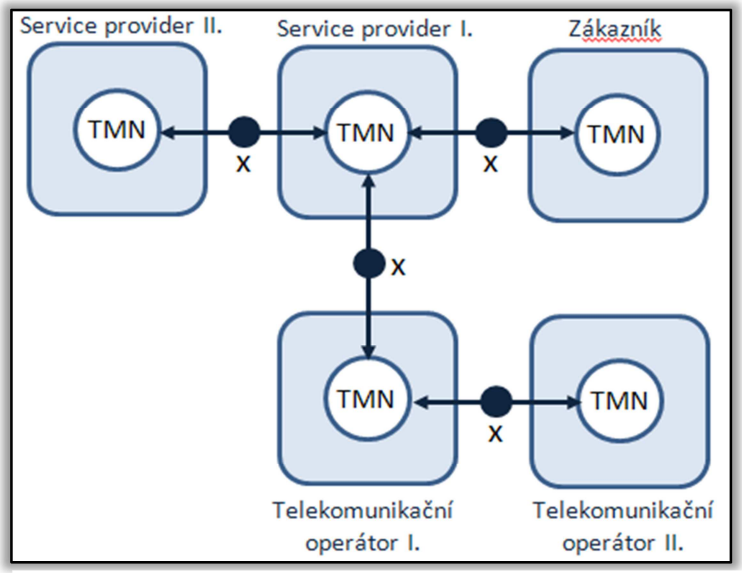
Tabulka č. 1 pak zobrazuje, které funkční bloky jsou ve kterých fyzických blocích (zařízeních) implementovány povinně (M) a které volitelně (O). Z tohoto přiřazení vyplývají funkce jednotlivých fyzických bloků.

	NEF	MF	QAF	OSF	WSF	DSF
NE	povinné	volitelné	volitelné	volitelné	volitelné	
MD		povinné	volitelné	volitelné	volitelné	
QA			povinné			
OS		volitelné	volitelné	povinné	volitelné	
WS					povinné	
DCN						povinné

Tabulka č. 1 – Povinně a volitelně implementované bloky fyzického TMN modelu podle [5].

3.5.1.4 Interoperabilita TMN

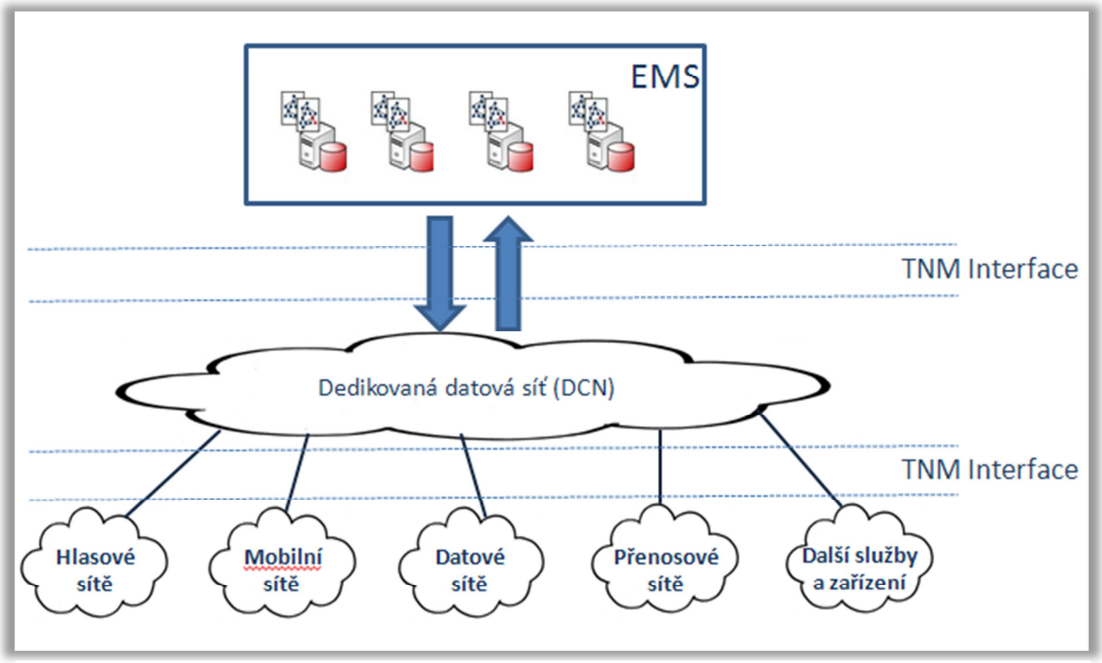
V modelu TMN je zohledněna i skutečnost, že telekomunikační sítě obvykle neexistují jako samostatné a oddělené entity. Naopak jejich předností je schopnost jejich vzájemného propojování. Za účelem propojení více různých sítí i na vrstvě řízení je v TMN modelu definováno rozhraní pojmenované x. Příklad propojení řídicí vrstvy více oddělených sítí je vidět na obrázku č. 8. Příklad popisuje například situaci, kdy zákazník využívá služeb lokálního service providera (poskytovatel služeb), který dále využívá síťovou infrastrukturu telekomunikačního operátora, jehož síť je propojena s dalšími operátory telekomunikačních služeb. Samotný servisní provider navíc sdílí část svých služeb s jiným servisním providerem.



Obrázek č. 8 - Příklad propojení řídicí vrstvy více oddělených sítí. /Zdroj: autor podle [7]./

3.6 Systém řízení poruch

Systémy řízení poruch, ve většině případů označované jako Fault management, zajišťují sběr informací o aktuálním stavu dohlížené telekomunikační sítě a jejich vyhodnocování. Základní představa vychází z již představeného TMN modelu a je zobrazena na obrázku č. 9.



Obrázek č. 9 – Systém řízení poruch vycházející z TNM modelu. /Zdroj: autor./

Jednotlivé technologické domény jsou řízeny separátními prostředky, tzv. element manažery (EMS). Pro vzájemnou komunikaci dohlížených prvků sítě s prostředky jejich řízení se dle doporučení vycházejícího z TMN modelu obvykle využívá zvláštní, od ostatní komunikace oddělená (dedikovaná) datová síť (DCN). Vrstva EMS obsahuje prostředky, umožňující řízení prvků a služeb sítě v rozsahu již zmíněného TMN modelu FCAPS. Jedná se tedy o prostředky řízení poruch, konfigurace, výkonosti, účtování a zabezpečení (fault, performance, configuration, accounting a security managementu).

Pro komunikaci element manažerů s prvky sítě se v rámci TMN interface používá kromě proprietárních řešení několika různých standardních síťových protokolů. Mezi nejrozšířenější a nejuniversálnější patří protokol SNMP[14], který byl speciálně pro tyto účely vytvořen. Pomocí stylu komunikace agent – manažer je s jeho pomocí možná obousměrná komunikace se síťovými prvky. Toho se využívá pro konfigurační, fault i performance management. Dalším protokolem vyvinutým pro účely řízení sítí je

[14] SNMP – Simple Network Management Protocol.

protokol CMIP[15], podporující služby definované standardem CMIS[16]. Mezi další rozšířené protokoly využívané pro řízení sítí objektově orientovaný protokol CORBA[17] definovaný organizací OMG[18] a MML[19] protokol realizovaný přes TL1[20] rozhraní. Těmto jednotlivým protokolům a způsobům jejich užití v rámci fault managementu se podrobně věnovala předcházející bakalářská práce (1), jejich bližší popis nebude tedy součástí této práce. Naopak tato práce v následující kapitole rozšíří téma fault managementu o problematiku korelací alarmů.

3.6.1 Korelace alarmů

Jak již bylo uvedeno v úvodu této práce, pro skutečně účinný incident management je zcela nezbytné mít v každý okamžik přesnou znalost o stavu dohlížené telekomunikační sítě a služeb, které poskytuje. Podstatnou část těchto informací poskytují právě v předchozí kapitole zmíněné prostředky fault a performance managementu. Ty ve formě událostí (častěji označovaných jako alarmy) informují o všech nestandardních stavech dohlížené sítě.

Problém však nastává při interpretaci těchto alarmů. V současné době, vzhledem ke stále rostoucí rozlehlosti a složitostí sítí, dostává řídicí systém obrovské množství alarmových událostí. Není žádnou výjimkou, že příchozí počet událostí převyšuje hodnoty stovek za sekundu. Obtížnost interpretace zvyšuje i skutečnost, že dnešní telekomunikační síť je tvořena více různými technologickými doménami, navíc obvykle dodávanými různými výrobci (vendory). Z těchto předpokladů jednoznačně vyplývá, že služby poskytované v takovéto telekomunikační síti jsou realizovány na více různých síťových prostředcích, které mají oddělený systém řízení poruch.

V takovýchto situacích je nezbytné využívat prostředků tzv. Integrovaného fault managementu (1). Jeho přínosem je konsolidace alarmů z mnoha různých technologických platforem do jednoho místa a v jednom standardizovaném formátu. Pořád ale zůstává problém s interpretací získaných alarmových hlášení (zpráv). Je zcela

[15] CMIP – Common Management Information Protocol.
[16] CMIS – Common Management Information Services.
[17] CORBA – Common Object Request Broker Architecture.
[18] OMG – Object Management Group.
[19] MML – Man-Machine Language (vyvinuto v laboratořích Bellcore).
[20] TL1 – Transaction Language.

nebytné, alarmy dále před jejich dalším využitím (interpretováním) zpracovat. Jednou ze základních forem tohoto zpracování je korelování alarmů.

Korelace alarmů je proces, kdy na základě předdefinovaných pravidel systém vytváří logické závislosti mezi jednotlivými alarmy nebo mezi celými skupinami alarmů. Na základě těchto závislostí lze pak obvykle výrazně redukovat počet alarmů jen na ty se skutečnou vypovídající hodnotou a tím ulehčit a zrychlit jejich zpracování v dalších krocích incident managementu.

Příklady situací, kdy je vhodné uplatnit korelaci alarmů:

- komponenta s poruchou generuje více než jeden alarmový stav
- dochází k časté změně stavu nějaké síťové komponenty
- jedna porucha ovlivní zprostředkovaně více síťových komponent
- porucha jedné síťové komponenty je duplicitně oznamována z více komponent zároveň

Korelace se uplatňují ve všech již dříve zmíněných pěti funkčních oblastech TMN modelu (FCAPS). V reálném prostředí se však jejich použití zužuje jen na oblast fault a performance managementu. Zvláště pak v oblasti fault managementu je provádění korelací prakticky zcela nezbytné.

Samotný proces korelací alarmů není jednoduchou záležitostí. Systém, který korelaci provádí, musí obsahovat mnoho přesných algoritmů (pravidel), jak korelaci provádět. Mnohá z těchto pravidel se navíc neobejdou bez detailních znalostí o aktuální topologii sítě a konfiguraci prvků v této síti. Jen zajištění tohoto předpokladu je často velmi složitý úkol, v některých případech, při požadavku 100% akurátnosti získaných dat, dokonce neřešitelný. V těchto případech i korelace alarmů poskytuje ne zcela dokonalé výsledky, s čímž je třeba počítat při dalším jejich zpracování.

Asi nejčastějším příkladem korelace je logické provázání alarmů, které oznamují začátek poruchy s alarmy, které tuto poruchu ukončují. Standardním požadavkem na dohledový systém je to, že bude zobrazovat aktuální stav sítě, a to pokud možno v reálném čase. Předpokládá se, že alarm oznamující nějaký abnormální stav v síti (*Problem*), bude v budoucnu doplněn o další alarm, který naopak informuje o

ukončení tohoto abnormálního stavu (*Resolution*). Tato dvojice alarmů musí být následně v dohledovém systému automaticky detekována, označena jako související a následně i z pohledu na aktuální stav sítě odstraněna. Příklad takto korelovaného alarmu je na obrázku č. 10.

Node	Summary	Count	LastOccurrence	First Occurrence
102230PHPRIB051032	Node Down: 102230PHPRIB051032 (This incident indicates that	4	03/26/13 18:28:34	03/26/13 18:27:14
102230PHPRIB051032	Node Down: 102230PHPRIB051032 (Incident closed)	2	03/26/13 18:33:25	03/26/13 18:33:25

Obrázek č. 10 – Příklad korelace Problem/Resolution.

Dle způsobu použití korelací při zpracovávání alarmů rozeznáváme několik dalších základních typů prováděných korelací. Jejich výčet, tak jak jej uvádí [18], se stručným popisem je uveden v následujících odstavcích. Pro překlad názvu jednotlivých položek výčtu, bylo použito [17].

Poznámka: Každá alarmová událost netvoří pár *Problem*/*Resolution*. Některé události jsou pouze informativní. Příkladem je například informace o reloadu síťového prvku, špatně zadaném heslu uživatele a podobně. Tento typ událostí se v literatuře někdy označuje jako *transient event*. Příklad takovéto události je na obrázku č. 11.

Node	Summary	Count	LastOccurrence	First Occurrence
102490JIJIXX010198	Cold start - power-on	4	03/26/13 13:49:35	03/26/13 13:49:35

Obrázek č. 11 – Příklad události typu *transient.*

3.6.1.1 Deduplikace (compresion)

Deduplikace spočívá v detekci shodných alarmů v rámci daného časového intervalu. Alarmy se za shodné obvykle považují, splňují-li následující 2 podmínky:

- jsou vztaženy k právě jedné síťové komponentě (nebo službě),
- souhlasně informují o právě jednom stavu (například CRC[21] chyba).

Typickým výsledkem tohoto typu korelace je sloučení korelovaných alarmů v jeden, ze kterého je kromě popisu alarmového stavu a identifikace místa v síti, kde k němu došlo, patrné, že se jedná o opakovaný problém (často se přímo uvádí počet jednotlivých signalizací tohoto problému), kdy byl problém signalizován prvně a kdy

[21] CRC – Cyclic Redundance Check. Chyba při přenosu datových paketů sítí.

naposledy. Příklad takto korelovaného alarmu je vidět na obrázku č. 12. Pole *Count* zobrazuje počet výskytu konkrétního typu alarmu (pole *Summary*) souvisejícím s prvkem (*Node*) v časovém intervalu daném časy *First Occurrence* a *Last Occurrence*.

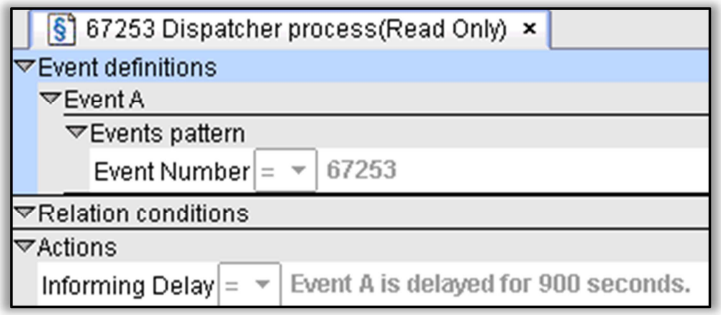
Node	Summary	Count	LastOccurrence	First Occurrence
ism	pppd: Connect script failed	4	03/26/13 16:44:53	03/26/13 16:38:53

Obrázek č. 12 – Příklad deduplikovaného alarmu.

3.6.1.2 Sčítání (counting)

V rámci tohoto typu korelace se vytváří nový alarm vždy v okamžiku, kdy počet příchodů daného typy alarmy překročí za určitý čas předem dany počet. Původní alarm je zároveň potlačen. Velmi často se v souvislosti s aplikací tohoto pravidla zároveň zvyšuje závažnost[22] alarmu (někdy se tato akce nazývá eskalace alarmu).

3.6.1.3 Potlačení (selective suppression)



Obrázek č. 13 – Příklad manuálně konfigurovaného pravidla.

Potlačením alarmů v rámci korelace je myšleno jejich dočasné skrytí, na základě jasně daných pravidel a souvisejícího s aktuálním stavem v síti, například dočasné skrytí alarmů s nižší závažností, pokud zároveň existují alarmy se závažností vyšší. Jiným příkladem využití tohoto typu korelace je stav, kdy v síti přestane odpovídat dohledovému systému konkrétní síťový prvek (například switch). Dohledový systém jej označí za nedostupný (typ alarmu NodeDown). Zároveň ale jsou ale nedostupné i jednotlivé monitorované části tohoto zařízení. V rámci aplikování pravidel potlačení, jsou ale alarmy na nedostupnost těchto jednotlivých částí potlačeny po celou dobu existence závažnějšího alarmu, informujícímu o nedostupnosti celého zařízení. V příkladu zobrazeném na obrázku č. 13 je vidět manuálně konfigurované pravidlo, na jehož základě se konkrétní typ alarmu (67253) zobrazí k dalšímu zpracování až v případě, že doba jeho trvání překročí nastavenou časovou hranici (15 min).

[22] Závažnost (severity) alarmu je příznak, kterým se dle standardů vyjadřuje stupeň důležitosti tohoto alarmu. Více v předcházející bakalářské práci [1].

3.6.1.4 Filtrace (filtering)

Filtrace je potlačení některých alarmů dle vybraných parametrů. Tímto způsobem se k dalšímu zpracování mohou dostat jen například alarmy, přímo související s konkrétní službou, zákazníkem, technologií nebo lokalitou.

3.6.1.5 Dočasný vztah (temporal relationship)

Tato korelace se provádí na základě pořadí v čase, ve kterém byly korelované alarmy generovány nebo přijaty. V korelačním mechanizmu se následně využijí závislosti dané vztahy: před, poté, předchůdce, následník, během, na začátku, na konci, ve shodě a zároveň.

3.6.1.6 Zobecnění (generalization)

V tomto typu korelace se nahrazuje alarm jiným alarmem, který má vyšší úroveň závažnosti. Například pokud skupina alarmů indikuje přerušení všech vláken jednoho optického kabelu, jsou tyto alarmy nahrazeny jedním alarmem indikujícím přerušení kabelu jako celku.

3.6.1.7 Specializace (specialization)

Specializace je opakem zobecnění. Dochází tedy při něm naopak k rozpadu alarmu vrstvy vyšší na (obvykle) více alarmů vrstvy nižší. Tyto nově generované alarmy nepřinášejí přímo žádnou novou informaci – mohou být ale využity při následném hledání příčin indikovaného problému.

3.6.1.8 Sdružování (clustering)

Výstupem tohoto typu korelace je nový alarm, vytvořený na základě pravidel (šablon) aplikovaných na přicházející alarmy. Velmi často slouží jako vstupy výstupy z předešle aplikovaných korelačních pravidel.

3.6.2 Analýza prvotní (kořenové) příčiny

Dalším způsobem, jakým lze docílit efektivnějšího způsobu využití došlých alarmových stavů je analýza prvotní příčiny, většinou označovaná jako RCA z anglického root cause analysis. Tento mechanismus třídí aktivní alarmy na symptomy problému a příčiny problému. Například pokud dojde k nedostupnosti celé interní sítě na jedné pobočce zákazníka, je cílem RCA najít příčinu této nedostupnosti (pravděpodobně se jedná o přerušení přístupové konektivity pro celou tuto pobočku), tuto příčinu zvýraznit a ostatní související alarmy současně potlačit. Specialista nebo systém řešící tento incident bude pak rovnou informován o hlavním problému (tedy

přerušení konektivity na pobočku) a nebude zdržován v danou chvíli nepodstatnými alarmy signalizujícími výpadky jednotlivých zařízení této pobočky.

RCA se obvykle neřadí přímo mezi korelace, i když se jedná také o velmi účinný způsob předzpracování alarmů. V případě korelací se spojují symptomy, které se velmi pravděpodobně týkají právě jedné kořenové příčiny. Tato příčina se však na rozdíl od RCA přímo nehledá. Cílem korelace je hlavně filtrace a redukce množství přicházejících informací. Teprve až takto upravené informace jsou následně podrobovány RCA pro nalezení zdrojové příčiny nastalého problému.

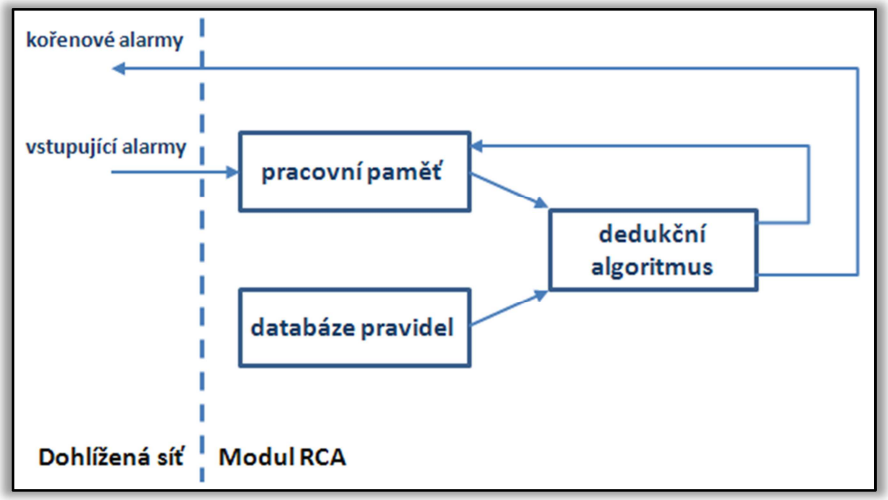
V následujících odstavcích jsou uvedeny některé postupy využívané při RCA tak, jak je uvádí [17] a [19].

3.6.2.1 Metoda Rule Based Reasoning

Metoda Rule Based Reasoning (RBR) je rozšířenou metodou řešení RSA v mnoha komerčních aplikacích. Je založena na reprezentaci znalostí sítě sadou pevných pravidel. Aktuální stav sítě se pak s těmito pravidly v nekonečném cyklu porovnává. Hlavními součástmi systému RBR jsou:

- pracovní paměť,
- databáze pravidel,
- dedukční algoritmus.

V pracovní paměti je udržován aktuální stav dohlížené sítě. Jednotlivá pravidla jsou uložena v databázi pravidel. Zpracovávání přicházejících alarmů ze sítě je realizováno dedukčním algoritmem (viz obrázek č. 14).



Obrázek č. 14 – Zpracování alarmu dedukčním algoritmem. /Zdroj: autor podle [17]./

Metoda RBR má možnost zpracovávat alarmy dvěma způsoby:

- dopředným řetězením,
- zpětným řetězením.

V případě dopředného řetězení se položky z pracovní paměti porovnávají s databází pravidel s cílem nalezení příslušného kořenového problému. Ve chvíli, kdy se tímto způsobem správné pravidlo nalezne, je jeho aplikací ihned upraven stav pracovní paměti. Tímto způsobem lze výstupy tohoto kroku využít při zpracovávání dalších přicházejících událostí. V pracovní paměti jsou všechny přijaté alarmy a algoritmem je hledána jejich příčina.

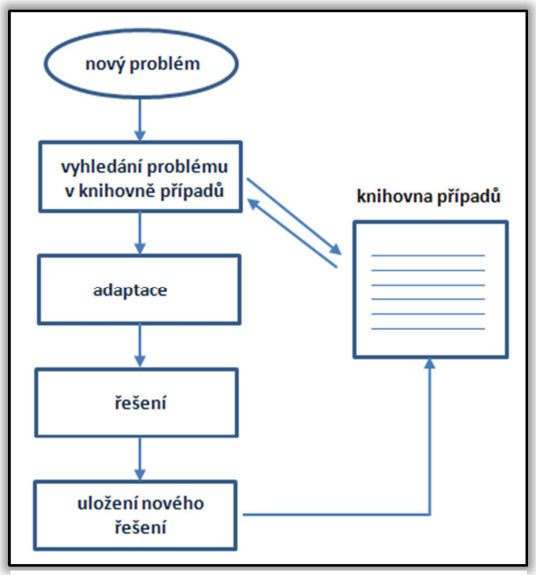
Druhý způsob, někdy také nazývaný metoda dedukce, postupuje tak, že hledá pravidla nejlépe odpovídající řešení problému. Podmínky těchto pravidel se následně porovnají s obsahem pracovní paměti. Podmínka je splněna tehdy, pokud se naleznou odpovídající data v paměti nebo i vyhledáním dalších pravidel (splňujících danou podmínku). Při tomto způsobu jsou v pracovní paměti uloženy všechny možné problémy a cílem hledání je nalézt podmínku, kterou splňují všechny došlé alarmy.

V obou popsaných režimech metody RBR se aplikuje shodná sada pravidel.

Důvodem časté implementace této metody je poměrně snadno sestavitelná logika zpracování alarmů. Problémy ale nastávají v rozsáhlejších sítích, kde složitost výpočtu využití metody omezuje. Metoda také nevyužívá vyhodnocení, která již učinila. Ve všech příchozích situacích se vždy musí použít vyhledávácí algoritmus v plném rozsahu, a to i na často opakující se stejný stav.

3.6.2.2 Metoda Case Based Reasoning

Metoda, která odstraňuje některé nedostatky metody předešlé, se nazývá metoda Case Based Reasoning (CBR). Tato metoda si postupy řešení včetně jeho výsledků ukládá do tzv. *případů*. Tyto *případy* jsou pak součástí tzv. *knihovny případů*, která tak obsahuje všechny již řešené předchozí *případy*. Postup hledání touto metodou je zobrazen na obrázku č. 15.



Obrázek č. 15 - Schéma metody Case Based Reasoning (CBR). /Zdroj: autor podle [17]./

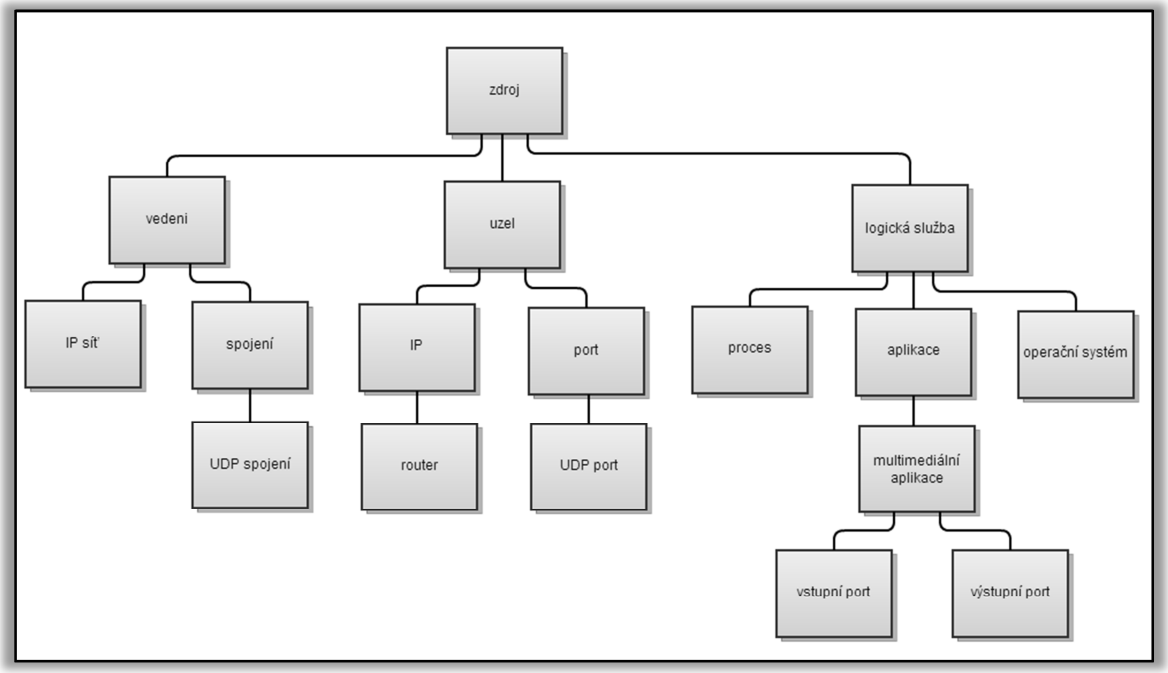
Každý nový řešený problém se v prvním kroku porovná s již řešenými případy. Je-li nalezena shoda, postupuje se dále dle řešení nalezeného případu. Pokud k žádné shodě nedojde, musí být uplatněn některý ze způsobů adaptace postupů uložených v knihovně případů. Po takto provedené adaptaci případ rozšíří stávající knihovnu. Metoda CBR tedy využívá výsledků získaných během předchozích cyklů.

Používané metody adaptace [17]:

- Parametrická adaptace – pracuje s matematickou funkcí, která popisuje vztah mezi proměnnými popisujícími problém a proměnnými, jež charakterizují odpovídající řešení;
- Adaptace substitucí = pokud vztah nelze vyjádřit matematickou funkcí, ale pouze sekvencí určitých kroků, provede se adaptace nahrazením původní hodnoty proměnné hodnotou novou;
- Adaptace critic-based. Jedná se o úpravu knihovny případů zásahem uživatele systému. Předcházející případ adaptace se může doplnit například o zprávu zaslanou před provedením restartu serveru a podobně.

3.6.2.3 Metoda Model Based Reasoning

Principy této metody již zasahují i do oblasti umělé inteligence. Každý prvek sítě je nahrazen modelem, mezi těmito modely dochází k vyměňování a sdílení informací. Tyto informace zahrnují nejenom popis síťových prvků a vztahů mezi nimi, ale i úplnou topologii sítě. Model může popisovat fyzickou nebo logickou vrstvu. Nese tři typy informací: Atribut (např. IP adresu), typ vztahu k jiným modelům (je částí,



Obrázek č. 16 - Jednotlivé prvky modelu multimediální služby. /Zdroj: autor podle [17]./

spojený s, závislý na …) a chování modelovaného prvku. Na obrázku č. 16 jsou zobrazeny jednotlivé prvky modelu multimediální služby.

3.6.2.4 Metoda kódování alarmů (Code Based Systems)

Metoda kódování alarmů (CBS) vychází z předpokladu, že každý problém vyvolá specifickou množinu symptomů (alarmů), které tento problém identifikují. Číselná reprezentace těchto symptomů se nazývá kód. Sestavený kód jednoznačně identifikuje prvotní příčinu poruchy, proces korelace alarmů je tedy způsob dekódování přijímaných alarmů. Optimalizovaný soubor kódů je nazýván kódovou knihou a podobně jako u metod RBR a CBR je popisem znalostní databáze – souboru definovaných problémů, které se mohou v analyzované síti vyskytovat.

Technika kódování se skládá ze dvou fází. V první je definován soubor událostí, jenž je třeba monitorovat. Tím vzniká korelační matice, následně pak její optimalizací kódová kniha. Obojí, kódová kniha i korelační matice se zapisují jako matice, ve které každý řádek odpovídá jednomu symptomu (příznaku, alarmu) a každý sloupec pak představuje jeden problém.

V další fázi, takzvaném dekódování, se kód příchozích alarmů označujících určitý problém porovnává s kódy uloženými v kódové knize a hledá se nejvyšší shoda. Systém CBS je chráněn speciálním algoritmem, který řeší ztráty symptomu respektive přijetí falešného alarmu. Tyto situace se souborně označují jako šum. Systém musí být vůči určité hladině šumu odolný.

Systémy využívající metod CBS patří k nejsilnějším v určení kořenové příčiny poruchy. Součástí této práce je i představení komerčního produktu SMARTS, který navíc kromě metody CBS využívá vlastního modelu popisujícího jednotlivé prvky sítě a to včetně jejich chování. Součástí modelu jsou i vztahy mezi definovanými alarmy. Kombinace tohoto vlastního modelu s metodou CBS umožňuje aplikaci SMARTS reagovat na změny topologie v reálném čase bez dodatečných zásahů do nastavení.

3.6.2.5 Distribuovaná korelace

V případě rozsáhlejších sítí je vhodné dělit působnost řídícího systémů mezi více řízených domén. Toto aplikování distribuované architektury usnadní použití scénářů stanovování příčiny poruchy. Telekomunikační síť je rozdělena na více separátních částí (domén), kde každá z těchto domén je řízena odděleně – samostatným řídicím centrem. Tato od sebe oddělená centra mají omezený přehled o stavu domén, které nejsou pod jejich přímým řízením. Během řešení problémů však spolupracují a alarmové informace si vzájemně vyměňují.

Algoritmus lokalizace poruchy pracuje s pravděpodobností poruchy v doméně alarmů. Nejpravděpodobnější příčina je identifikována jako maximální hodnota pravděpodobnosti souboru řízených objektů. Vedle atributu pravděpodobnosti poruchy se zavádí ještě informační hodnota, definovaná jako záporný logaritmus pravděpodobnosti poruchy. Potom lze očekávat, že nejpravděpodobnější příčina

poruchy bude charakterizována minimální hodnotou souboru řízených objektů. Při lokalizaci lze využít třech rozdílných přístupů:

- Centralizovaná lokalizace. Centrální řídicí systém s působností nad celou sítí řeší přímo každý problém, který zasahuje do více řízených domén;
- Decentralizovaná lokalizace. Problém ovlivňující více domén se řeší spoluprací centrálního řídicího systému s řídicími systémy postižených domén;
- Distribuovaná lokalizace se snaží nalézt příčinu poruchy bez spolupráce s centrálním řídicím systémem.

3.6.3 Příklady produktů řešících korelace a hledání kořenové příčiny

V předcházející kapitole 3.6.2 byly popsány různé metody používané pro RCA událostí přicházejících z dohledované sítě. V této kapitole budou představeny konkrétní softwarové produkty/balíky, které ve svých funkcionalitách některým z popsaných způsobů korelaci událostí provádějí.

Do výběru následujících představovaných produktů byly zahrnuty ty, které se pro oblast síťového managementu staly určitými standardy [2]. Jako součást představení každého z těchto produktů je kromě základního popisu uveden i mechanismus, jakým způsobem je korelace a RCA událostí v jeho konkrétním případě řešena. Největší prostor je vyčleněn pro produkt HP Network Node Manager, protože je důležitou součástí řešení praktické části této práce.

3.6.3.1 HP Network Node Manager

Softwarový produkt HP Network Node Manager je součástí produktové řady HP OpenView, vyvíjené společností Hewlett Packard. Do této produktové řady patří více než 30 jednotlivých separátních produktů, které jsou určeny pro následující oblasti (v závorkách jsou uvedeny příklady zástupců produktů spadajících do dané oblasti):

- správa sítí a internetu (Network Node Manager, Performance Insight for Networks, OV Problem Diagnosis, OV Internet Services),
- správa zálohování a SAN[23] (OV OmniBack, OV SAN),
- správa systémů a aplikací (OV Operation, OV Performance),
- správa procesů (OV ServiceDesk, OV Reporter, OV Service Information Portal).

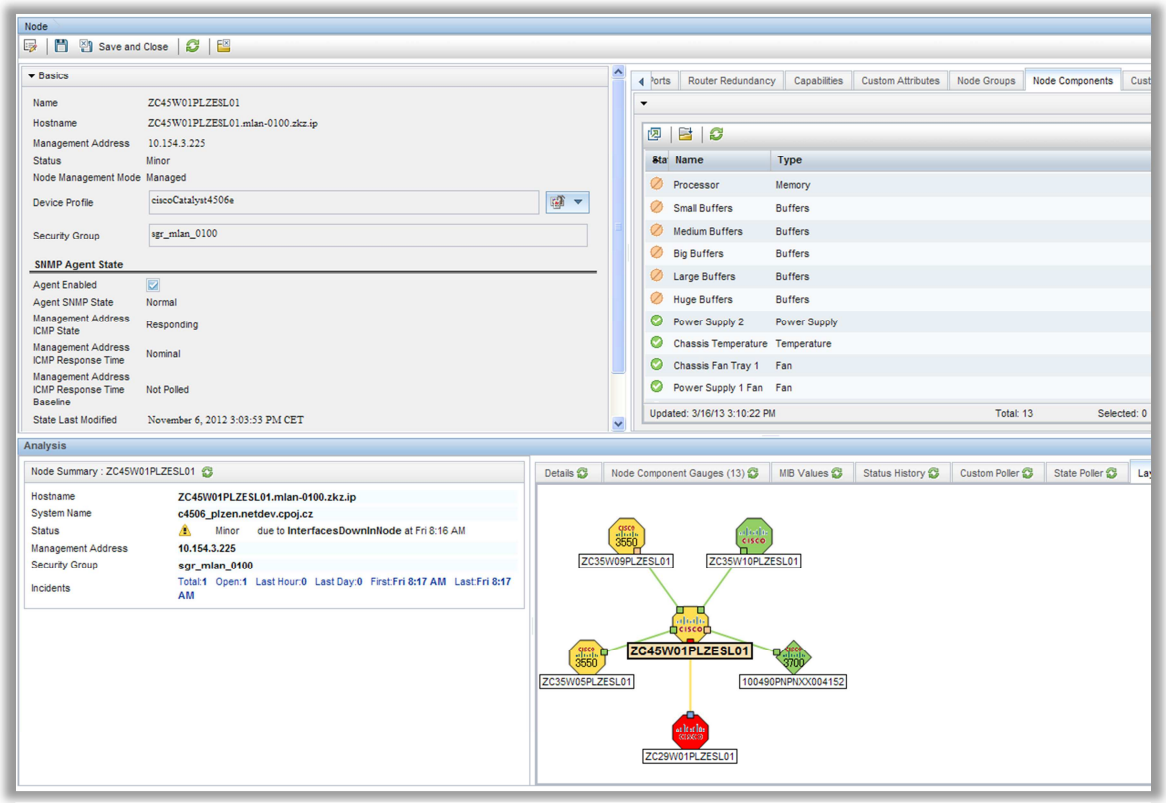
Network Node Manager (NNM) byl už zmíněn a krátce popsán v předešlé bakalářské práci [1]. Jedná se asi o jeden z nejznámějších komerčních nástrojů pro síťový management. Za tento fakt vděčí mimo jiné téměř neomezené škálovatelnosti, robustní architektuře a širokým možnostem integrace jak směrem k dohlížené síťové infrastruktuře, tak směrem k dalším managementovým nástrojům. Nejnovější verze 9.20 se dodává s řadou užitečných „plug-in“ modulů specializujících se na různé speciální

[23] SAN – storage area network. Dedikovaná síť obvykle určená pro přímý přístup serverů k datovým uložištím (diskovým polím, páskovým knihovnám apod.).

typy sítí či prvků. Jedná se například o plug-in pro MPLS[24] sítě, IP telefonii, IP multicastové služby a podobně. Společně s dalšími prvky produktové řady tvoří kompletní sadu nástrojů pro podporu incident managementu dle doporučení ITIL v3.

Pro komunikaci s dohlíženou síťovou infrastrukturou používá Network Node Manager SNMP protokol [3], je tedy primárně určen pro síťové prvky podporující toto rozhraní. Předností je i vestavěná funkce autodiscovery, která umožňuje získat obraz architektury sítě bez nutnosti použití separátních inventory databází. Naopak tyto databáze je schopen do určité míry substituovat, a to nejenom pro svoje vnitřní potřeby, jak bude ukázáno dále při popisu korelačních postupů, které NNM využívá.

Administrátorské i uživatelské rozhraní je v posledních verzích NNM realizováno pomocí web interface. Příklad jednoho z možných pohledů je zobrazen na obrázku č. 17.



Obrázek č. 17 – Web interface nástroje NNM.

[24] MPLS – Multiprotokol Label Switch network.

V případě tohoto pohledu jsou v jednotlivých kvadrantech zobrazeny následující informace:

- základní údaje o monitorovaném prvku/zařízení jako jsou hostname a dohledová adresa + aktuální stav SNMP agenta na tomto zařízení,
- seznam komponent tohoto zařízení (získaných funkcí autodiscovery),
- hierarchické zobrazení okolních prvků, jejich propojení a aktuálních stavů (vyjádřeno v barevném kódování),
- aktuální stav zobrazeného prvku.

Network Node Manager zahrnuje i funkcionalitu korelací získaných událostí. Její popis je obsahem následujících dvou kapitol.

Vestavěný korelační modul

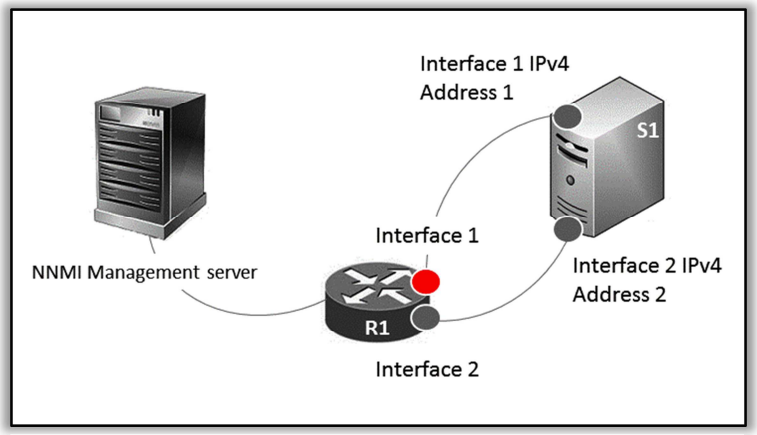
NNM verze 9.20 ve svém základu obsahuje a využívá modul pro korelaci událostí. Je automaticky využíván při zpracování a zobrazování událostí/stavů přicházejících ze sítě (a to jak v případě událostí získaných aktivním poolováním síťových prvků a jejich součástí, tak pro případ spontánně přicházejících SNMP trapů). Korelace využívá faktu, že NNM má k dispozici aktuální stav topologie sítě (viz funkce autodiscovery v předešlém textu). Z tohoto důvodu má odvozeně NNM také k dispozici informace o vzájemných závislostech jednotlivých síťových prvků a jejich částí. Na základě znalostí těchto vztahů je pak využitím MINCAUSE algoritmu [12] aplikována RCA[25] za účelem zjištění prvotní příčiny problému v dohlížené síti. Na základě provedené analýzy pak NNM provede některou z těchto akcí (nebo jejich kombinací):

- generovaní nové události,
- logické propojení událostí,
- potlačení událostí,
- smazání události,
- změna statusu[26] souvisejících objektů.

[25] RCA – Root Cause Analysis - analýza příčiny a následků.
[26] Status nabývá těchto hodnot: Unknown, Disabled, Critical, Major, Minor, Warning, Normal, No status.

Některé z těchto prováděných akcí budou použity v následujících modelových scénářích.

Scénář č. 1: Síťová IP adresa neodpovídá na ICMP



Obrázek č. 18 – Scénář č. 1.

V tomto případě (viz obrázek č. 18) je adresa 1 monitorovaného serveru S1 nedostupná na ICMP. Stav obou interface na routeru R1 je *operational*. Server S1 je dostupný přes interface 2. Po vyhodnocení tohoto stavu v korelačním modulu NNM bude vygenerována událost *AddressNotResponding* se statusem *Critical*, status dohlíženého serveru S1 se změní na *Minor*.

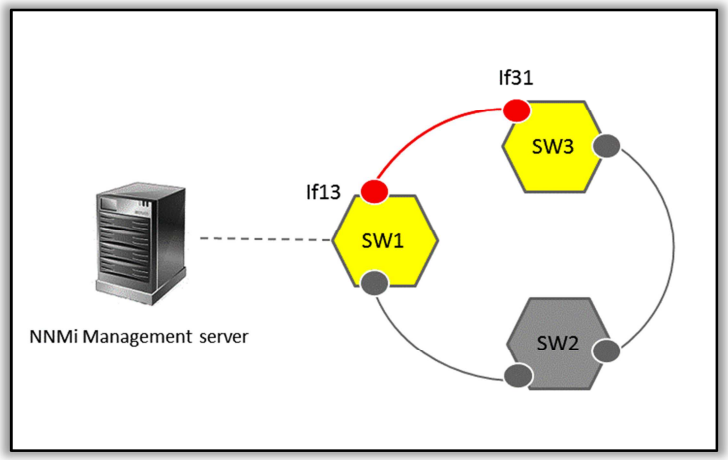
Scénář č. 2: Interface je ve stavu *Operationally Down*

Scénář opět vychází ze síťové topologie zachycené na obrázku č. 18. V tomto případě je však interface 1 ve stavu *operationally down* a zároveň ve stavu *administratively up* (tedy požaduje se jeho funkčnost, ale funkční aktuálně není). Router R1 je dostupný, server S1 je dostupný přes interface 2. Interface 1 je opět jako v předešlém případě a nedostupný na ICMP. Na základě pádu propojení R1 – S1 je routerem automaticky generována událost *LinkDown*. V tomto případě NNM jako kořenovou příčinu vyhodnotí pád interface 1, vygeneruje na tento interface událost *InterfaceDown* se statusem *Critical*. Událost *LinkDown* s touto generovanou událostí koreluje a ze zobrazení ji dočasně potlačí. Status serveru S1 bude změněn na *Minor*.

Scénář č. 3: Interface je ve stavu Administratively Down

Scénář představuje shodnou situaci jako předešlý scénář číslo 2. Změna je ve stavu interface 1 na hodnotu *Administratively Down*. Server S1 je i nyní dostupný přes interface 2. Událost *LinkDown* není routerem generována. NNM v tomto případě negeneruje žádnou událost, pouze status interface 1 změní na *Disabled*.

Scénář č. 4: Nedostupné spojení mezi dvěma přepínači (switch)

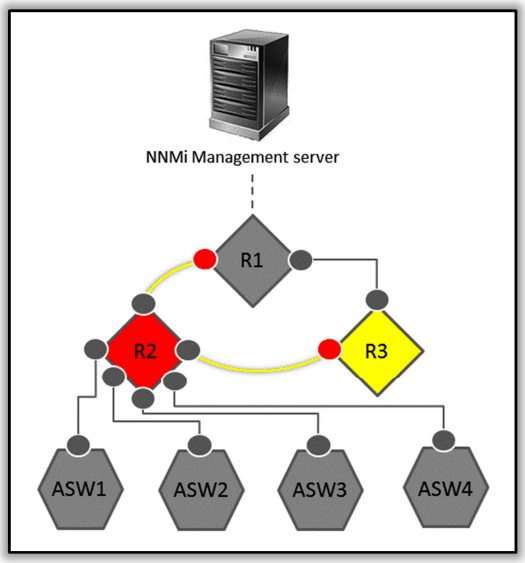


Obrázek č. 19 - Scénář č. 4.

V tomto případě (viz obrázek č. 19) nastalo přerušení síťového spojení mezi interface if13 a if31. Oba tyto interface generují událost *InterfaceDown*. Korelační modul NNM potlačí obě události InterfaceDown a vytvoří novou jednu událost *ConnectionDown* se statusem *Critical*. Status switchů SW1 a SW2 se změní na *Minor*.

Scénář č. 5: Výpadek routeru připojujícího skupinu přístupových přepínačů

V rámci tohoto vybraného případu dojde k závadě na routeru R2 takové, že se stane nedostupný (viz obrázek č. 20). Do NNM přichází události *InterfaceDown* na všechny interface dotčené nedostupností tohoto routeru. Korelační modul vyhodnotí jako kořenovou příčinu nedostupnost routeru R2 a vygeneruje událost *NodeDown* se statusem *Critical*. S touto událostí koreluje všechny související *InterfaceDown* události. Zároveň NNM změní status všech k routeru R2 připojených switchů na *Unknown*.



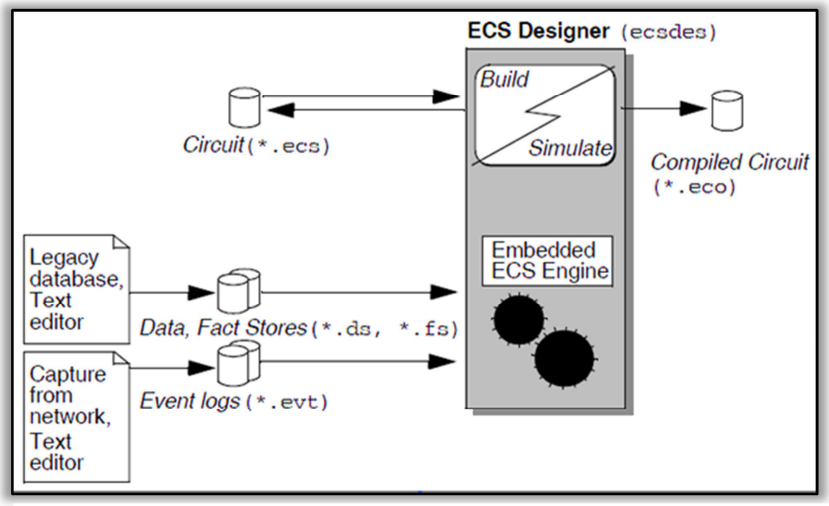
Obrázek č. 20 - Scénář č. 5.

Poznámka: Chování korelačního obvodu, kdy označil status switchů stavem Unknown, může přinášet v určitých případech i problém (i když je logicky správný). Více o tomto případě bude zmíněno v následné praktické části této diplomové práce.

Korelační obvody (ECS)

HP OpenView Event Correlation Services (ECS) je nadstavbová část produktů Network Node Manager a OpenView Operation (produkt pro dohled serverů a aplikací). Jejím cílem je umožnit rozšíření vestavěných korelačních mechanismů o další - dle požadavků konkrétního nasazení systému. ECS se skládá z následujících dvou částí:

1. ECS designer



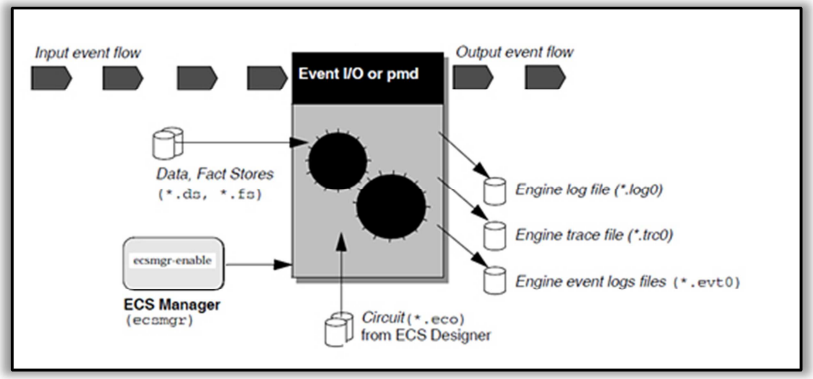
Obrázek č. 21 – Blokové schéma ECS designeru. /Zdroj: [13]./

Nástroj ECS designer umožňuje vytváření nových korelačních pravidel. Jedná se o grafické prostředí, jehož pomocí se modelují vzájemné závislosti jednotlivých objektů (například síťových prvků).

Těmto vzájemným vazbám se říká korelační obvody (correlation circuit). ECS designer umožňuje dále načíst externí data, pokud jsou součástí korelačního obvodu (figurují jako proměnné v rozhodovacích blocích). Po sestavení obvodu Designer pomoci otisku reálných dat přicházejících ze sítě nasimuluje chování a výstupy takto nově vytvořeného korelačního obvodu. Pokud výsledek odpovídá očekávání, Designer konfiguraci zkompiluje do univerzálního souboru, což umožní následnou snadnou přenositelnost mezi jednotlivými instalacemi. Blokové schéma ECS designeru je na obrázku č. 21.

Příkladem korelačního obvodu může být například sestavení obvodu sledující dvojici událostí PowerOn a PowerOff. Nastavení pak může udávat, že se uživatelům zobrazí pouze ta událost PowerOff, po které během následných 5 sekund nenásledovala událost PowerOn.

2. ECS engine



Obrázek č. 22: Schéma ECS engine. /Zdroj: [13]./

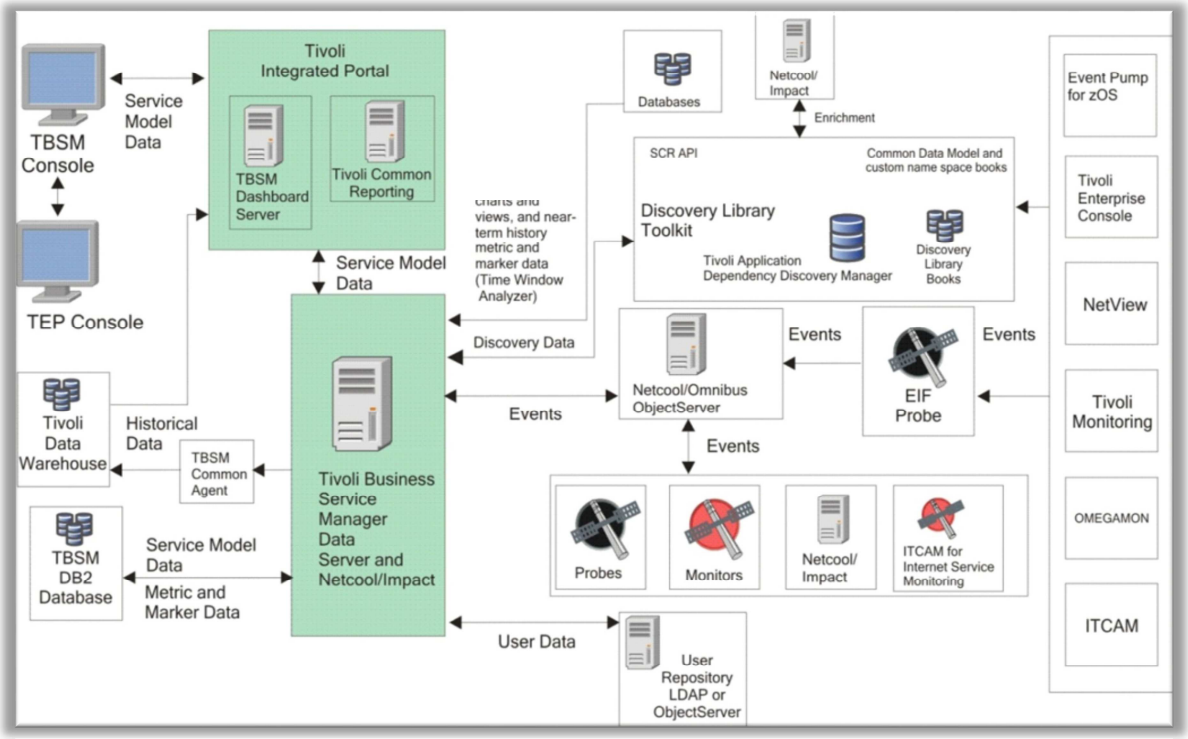
ESC engine je součástí produktu Network Node Manager a OpenView Operational (OVO). Jeho aktivace jej začlení do toku zpracovávaných událostí přicházejících z dohlížené sítě (či její části) nebo z dohlížených serverů a aplikací. Na základě definovaných korelačních obvodů, předem vytvořených v ECS Designeru a přenesených v kompilovaném tvaru, pak engine provádí samotné korelace, viz schematický obrázek č. 22.

3.6.3.2 Tivoli Bussiness Service Monitor

Tivoli Bussiness Service Monitor (TBSM) je produktem firmy IBM. Je jedním z mnoha produktů tvořících řadu pojmenovanou souhrnným názvem IBM Tivoli. Tato řada zahrnuje kompletní portfolio softwarových nástrojů pro dohled sítí a služeb.

TBSM na základě vytvořených stromů služeb (servisní model), ke kterým mapuje přicházející incidenty ze sítě, zobrazuje aktuální stav jednotlivých provozovaných bussiness služeb, umožňuje sledování SLA pro tyto služby a usnadňuje hledání závislostí mezi síťovou událostí a související degradovanou službou.

Produkt TBSM nelze provozovat samostatně. Pro svoji činnost vyžaduje instalaci několika dalších komponent z rodiny produktů IBM Tivoli. Příklad, jak by mohla vypadat architektura podporující dohled služeb využívající korelaci událostí, je vidět na obrázku č. 23.

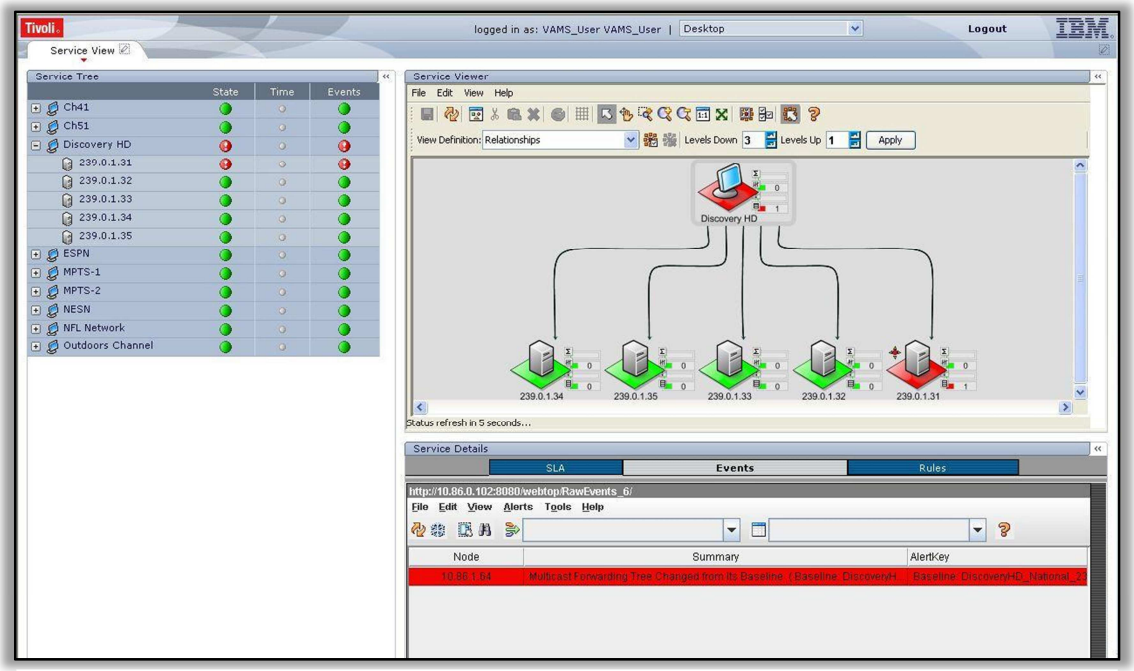


Obrázek č. 23 - Architektura podporující dohled služeb využívající korelaci událostí. /Zdroj: [14]./

Zvýrazněný zeleně je samotný TBSM a Tivoli Integrated Portal (TIP). Tato komponenta umožňuje uživatelský přístup jak za účelem administrace, tak pro přístup k výstupům jednotlivých Tivoli komponent nebo jejich spojení. Přístup je realizovaný prostřednictvím web rozhraní. Komunikace mezi TIP a TBSM je přímá pro účely konfigurace a zobrazování on-line událostí nebo prostřednictvím komponenty Tivoli Data Warehouse, která slouží k ukládání událostí do databáze pro jejich pozdější (off-line) zobrazení. TBSM pro ukládání vytvořeného servisního modelu (bude podrobněji zmíněn následně) využívá datové uložiště (v obrázku označeno jako TBSM DB2 Databáze). Vstupní události, které TBSM vyhodnocuje, jsou obsahem další komponenty – Netcool/Omnibus ObjectServer. Jedná se o databázi událostí, které jsou aktuálně v dohlížené části sítě, serverech a aplikacích. Způsob jejich získávání byl blíže popsán v předešlé bakalářské práci [1] a bude zmíněn v praktické části této práce. Za zmínku stojí komponenta Netcool/Impact, kterou je možno na základě sestavených politik

upravovat přicházející události. Příkladem těchto úprav může být doplňování zákaznických identifikátorů k souvisejícím událostem nebo generování nové události na základě splnění dané podmínky. Poslední samostatnou komponentou tohoto příkladu využití TBSM je komponenta Discovery Library Toolkit, která pomáhá vytvářet servisní model nutný pro správnou činnost TBSM. Tato komponenta se skládá ze dvou částí. První část tvoří knihovna předpřipravených závislostí vhodných pro použití v servisním modelu. Druhou, podstatnější částí je pak Tivoli Application Dependency Discovery Manager (TADDM), který je schopen mapovat síťovou infrastrukturu a služby, které jsou jejím prostřednictvím realizovány. Toto jsou hlavní podklady pro sestavování potřebného servisního modelu užitého následně v TBSM.

Na základě sestaveného servisního modelu (stromu služby) lze pak v TBSM zobrazit jednotlivé komponenty této služby, jejich aktuální stav, stav služby jako celku a číselné údaje související s plněním SLA vázané k této službě. Příklad takového



Obrázek č. 24 – Strom služby zobrazený v TBSM. /Zdroj: [16]./

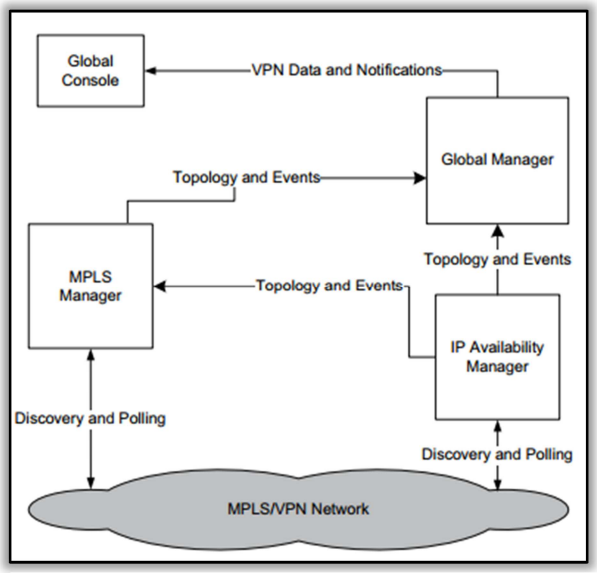
3.6.3.3 EMC Smarts

Smarts je softwarové řešení, aktuálně vyvíjené a dodávané společností EMC Corporation. Jedná se opět o portfolio složené z více produktů, z nichž některé mohou pracovat samostatně, některé pouze při spolupráci s dalšími. Řešení jako celek opět pokrývá požadavky úkolů řízení sítí a služeb.

Portfolio Smarts inCharge se skládá z těchto jednotlivých produktů:

- Smarts Application Connectivity Monitor,
- Smarts Global Manager,
- Smarts IP Availability Manager,
- Smarts MPLS Manager,
- Smarts Global Console,
- a dalších, viz (15).

Příklad doporučené architektury EMC Smarts pro dohled MPLS sítí je uveden na obrázku č. 25.



Obrázek č. 25 - Příklad doporučené architektury EMC Smart pro dohled MPLS sítí. /Zdroj: [16]./

Většina produktů portfolia pracuje s modulem RCA, který je řešený patentovanou technologií.

Systém využívá metody kódování alarmů, blíže popsané v kapitole 3.6.2.4. Základní filozofií této RCA metod je předpoklad, že každý problém v sítí má svoji jednoznačnou identifikaci. Tato identifikace je určena jednotlivými symptomy. Symptomy mohou být například události přicházející ze sítě. Zahrnují tedy jak události z postižené komponenty či služby, tak z následně ovlivněných komponent nebo služeb. Symptomy různých problémů se mohou

překrývat, ale unikátní kombinace symptomů charakterizuje právě jeden problém. Smarts sbírá tyto unikátní kombinace symptomů a jejich vazeb na problém a ukládá je v rozsáhlé tabulce nazvané kódová kniha (Codebook). Tu si je možné představit jako tabulku (matici), kde na jednotlivých osách jsou uvedeny symptomy a problémy. Existuje-li v této tabulce vazba mezi problémem a aktuálně existujícími symptomy, kořenový (root) problém je jednoznačně identifikován [2].

Porovnání vybraných produktů

Na závěr představení několika vybraných komerčních řešení určených pro řízení sítí a služeb, jejichž součástí je nějakým způsobem integrovaná funkcionalita korelace událostí, je v následující tabulce uvedeno krátké porovnání těchto produktů. Porovnání vychází z aktualizovaných výsledků uvedených v disertační práci [17].

	HP NNM	IBM Tivoli TBSM	EMC SMARTS
Deduplikace alarmů	ano	ano	ano
Určení prvotní příčiny poruchy	ano, závislé na bázi dodaných pravidel (od verze 9.x je součástí modul již obsahující základní sadu pravidel)	ano, závislé na bázi dodaných pravidel (možné využití nástrojů, při jejich specifikaci)	ano, vyhodnoceno dekódováním příchozích alarmů, závisí na správném modelu síťové domény
Statistická analýza	počítadlo výskytu stejných alarmů	počítadlo výskytu stejných alarmů	zobrazuje se pouze alarm příčiny poruchy
Korelace přes více vrstev	ano	ano dle dodaných pravidel	ano
Korelace na více doménách	omezeno na zařízení podporující SNMP protokol nebo na servery a aplikace	ano	pouze po úpravách
Citlivost na ztracené nebo falešné alarmy	ne	ne	ano, dle vstupních parametrů korelací, kde lze udat i pravděpodobnost výskytu
Rychlost korelace	ve větších doménách je pro zachování dostatečné rychlosti využito distribuovaného modelu	ve větších doménách pomalé	rychlý a efektivní proces

Tabulka č. 2 – Porovnání jednotlivých produktů řešících korelace a hledání kořenových příčin.

4. Návrh aplikace pro zajištění požadovaných funkcionalit incident managementu

V následujících kapitolách praktické části této diplomové práce bude postupně představena aplikace řešící konkrétní zadání vyplývající z požadavku zajištění úkolů incident managementu ke konkrétní službě obsažené v nabídce telekomunikačního operátora (dále jen Operátora).

Zadání vychází z konkrétního případu, kdy se stávající Operátor rozhodl na základě průzkumů trhu rozšířit portfolio nabízených služeb o nadstavbové služby zajišťující vyšší úroveň servisu pro zákazníky. Vzhledem ke skutečnosti, že se jednalo o zcela nový typ služeb, bylo nutné nastavit mnoho nových procesů, včetně procesů souvisejících se zajištěním incident managementu. Právě na tuto část zavádění nové služby se soustředí praktická část této práce.

Nejprve bude představena nová služba tak, jak ji definoval product management Operátora. Popis služby bude zestručněn v oblastech, které se nebudou týkat řešeného problému. Naopak části popisu služby, které přímo ovlivňují zadání pro představované řešení, budou publikovány v detailnějším rozsahu. Na základě takto představené služby bude následně sestaveno konkrétní zadání k řešení.

Druhá část praktické části práce bude rozdělena do dvou hlavních celků. První se bude věnovat popisu stávající situace OSS prvků Operátora jako výchozí roviny pro řešení sestaveného zadání. Ve druhé pak bude toto řešení v detailu představeno.

Vzhledem k tomu, že - jak již bylo v úvodu řečeno - se jedná o popis řešení reálné služby, budou některé informace zobecněny. V případě, že se bude jednat o konkrétní zákaznické údaje, budou tyto informace z důvodu ochrany obchodního tajemství zobrazeny ilustrativním způsobem. V případě, že v textu bude uvedeno slovo SLUŽBA, jedná se o obchodní název představované služby.

4.1 Popis služby

Popis služby bude rozdělen do dvou částí. První bude obsahovat obecný popis služby, ve druhé pak budou představeny ty součásti služby (proaktivita, service desk), které se týkají požadovaného řešení.

4.1.1 Obecný popis služby

Popis služby tak, jak ho představil product management:

SLUŽBA nabízí úplnou správu provozu lokálních, národních a mezinárodních datových sítí včetně proaktivního řešení incidentů, konzultace se systémovými architekty týkající se rozvoje datové sítě či analytickou činnost související s přípravou implementace nových technologií (VoIP, bezpečnostní politika, nasazení systémů náchylných na výpadky apod.). Součástí produktu je rovněž vytvoření a průběžná aktualizace podrobné technické dokumentace WAN/LAN sítě zákazníka.

SLUŽBA je komplexní outsourcingová služba, která sestává z monitoringu, dohledu, správy, řízení, plánování a údržby všech funkcí týkajících se infrastruktury a komponent rozsáhlých komunikačních sítí WAN a LAN.

SLUŽBA umožňuje zákazníkům využívat nezbytných materiálních a lidských zdrojů Operátora pro zvýšení dostupnosti svých síťových služeb a tím i produktivity jejich činností a aktivit.

SLUŽBA je nabízena v několika různých úrovních, které jsou vždy dohlíženy a spravovány zákazníkem, což umožňuje využití služby jako fundamentálního přístupu k rozsáhlým outsourcingovým projektům. Jako základní jsou nabízeny dvě různé úrovně v závislosti na požadavcích supervize a správy určené zákazníkem.

4.1.2 Podrobný popis služby

SLUŽBA je v základu koncipována tak, že k již poskytovaným službám IP datových přenosů přidává novou hodnotu v možnosti až kompletního outsourcingu těchto služeb (v závislosti na vybrané konfiguraci). Ilustrační schéma oblastí, kterých se SLUŽBA týká, je představeno později v kapitole 4.1.2.3.

4.1.2.1 Proaktivní dohled

Jednou z hlavních součástí SLUŽBY je nabídka zajištění proaktivního dohledu zákazníkovi dodávaných IP přenosových služeb. Proaktivní dohled umožňuje zákazníkovi zajištění dohledu jeho sítě v proaktivním režimu (viz kapitola 3.2.5) a založení záznamu o případném incidentu bez nutnosti jeho inicializace zákazníkem. Tento parametr je jedním z hlavních výhod SLUŽBY. Proaktivní dohled je dostupný pro vybrané úrovně SLA jako volitelný parametr. Na webovém portále Operátora je možné následně získat informaci o tzv. proaktivity indexu, který udává poměr incidentů založených proaktivně vůči celkovému počtu založených incidentů.

4.1.2.2 Service desk

Každý zákazník využívající SLUŽBU získá přístup na dedikovaný Service desk. Úkolem Service desku je řešit nebo koordinovat řešení všech založených incidentů zákazníkem. V případě varianty SLUŽBY s proaktivitou pak navíc i proaktivně předcházet a řešit incidenty související s využívanými službami zákazníkem.

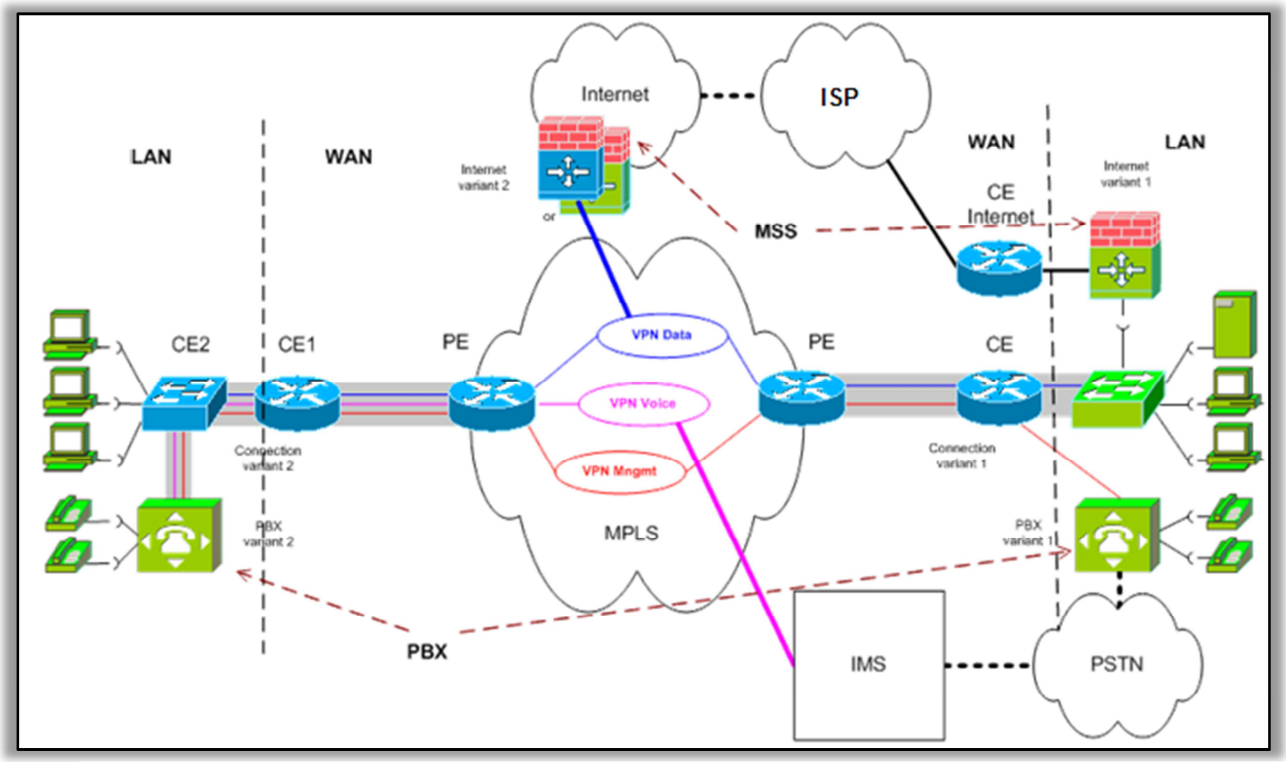
Z pohledu Service desku (SD) dává SLUŽBA na výběr ze dvou variant (viz tabulka č. 3). Jednotlivé úrovně odlišují rozsah podpory Service desku (sdílený nebo vyhrazený právě pro jednoho zákazníka), jeho dostupnost a fyzické umístění.

Typ service desku	Varianta 1	Varianta 2
Rozsah podpory SD	sdílený	vyhrazený
Dostupnost SD	24x7, 12x7 nebo 8x5	24x7
Místo provozování SD	prostory Operátora	prostory Operátora, volitelně prostory zákazníka

Tabulka č. 3 – Dvě nabízené varianty úrovně aktivit Service desku.

4.1.2.3 Ovlivněné stávající služby

Jak již bylo zmíněno, SLUŽBA rozšiřuje IP přenosové služby, které jsou již v nabídkovém portfoliu Operátora. Tyto služby jsou schematicky zobrazeny na obrázku č. 26.



Obrázek č. 26 – Schéma služeb v nabídce operátora.

Ve středu obrázku je umístěna MPLS[27] síť Operátora. Jejím prostřednictvím jsou realizovány veškeré datové přenosy související se SLUŽBOU. Obrázek zachycuje následující skupiny dodávaných služeb.

4.1.2.4 WAN konektivita

WAN konektivita je realizována propojením jednotlivých lokalit zákazníka pomocí MPLS sítě. U zákazníka je umístěn CE[28] router (v obrázku označeno jako CE a CE1), které je přenosovou technologií propojeno s MPLS sítí zajišťující funkci páteřní přenosové sítě. Jako přenosová technologie může být použito CDMA, xDSL nebo dedikovaný pronajatý okruh požadované rychlosti.

[27] MPLS – Multiprotocol Label Switching Network.
[28] CE – Customer Edge Router.

4.1.2.5 LAN konektivita

LAN konektivita zajišťuje jak realizaci LAN sítí v prostorách zákazníka, tak propojení těchto sítí mezi lokalitami zákazníka. Odpovědnost Operátora za LAN službu začíná na zákaznickém portu routeru nebo switche.

4.1.2.6 Přístup k internetu

Dodávané služby také zahrnují možnost propojení do internetu. Toto propojení může být realizováno jak v rámci již popsané WAN konektivity, tak dedikovaným připojením.

4.1.2.7 Hlasové služby

Součástí nabízených služeb je nabídka realizace hlasových přenosů, a to propojením pobočkových hlasových ústředen (PBX) přes IP síť.

4.2 Zadání k řešení

Z popisu služby uvedeného v předchozích odstavcích, vyplynulo i následující zadání pro oblast incident managementu.

4.2.1 Nástroj proaktivního dohledu

Vzhledem k faktu, že součástí SLUŽBY je i nově zřizované pracoviště Service desku, které bude v reaktivním nebo proaktivním režimu dohlížet datové služby zákazníka, je potřeba toto pracoviště vybavit dostatečně vhodným nástrojem, který tento požadovaný dohled bude umožňovat. Tento nástroj by měl být snadno obsluhovatelný a musí umožňovat interpretaci předkládaných informací i pracovišti Service desku, tedy pracovišti s předpokládanou pouze základní znalostí dohlížené části telekomunikační sítě, ve které jsou služby realizovány.

Požadovaný nástroj proaktivního dohledu musí obsahovat minimálně tyto vlastnosti:

- Uživatelské přístupy realizované výhradně přes webové rozhraní;
- Uživatele rozdělovat do dvou rolí – uživatelské a administrátorské;
- Intuitivní a přehledné ovládání;

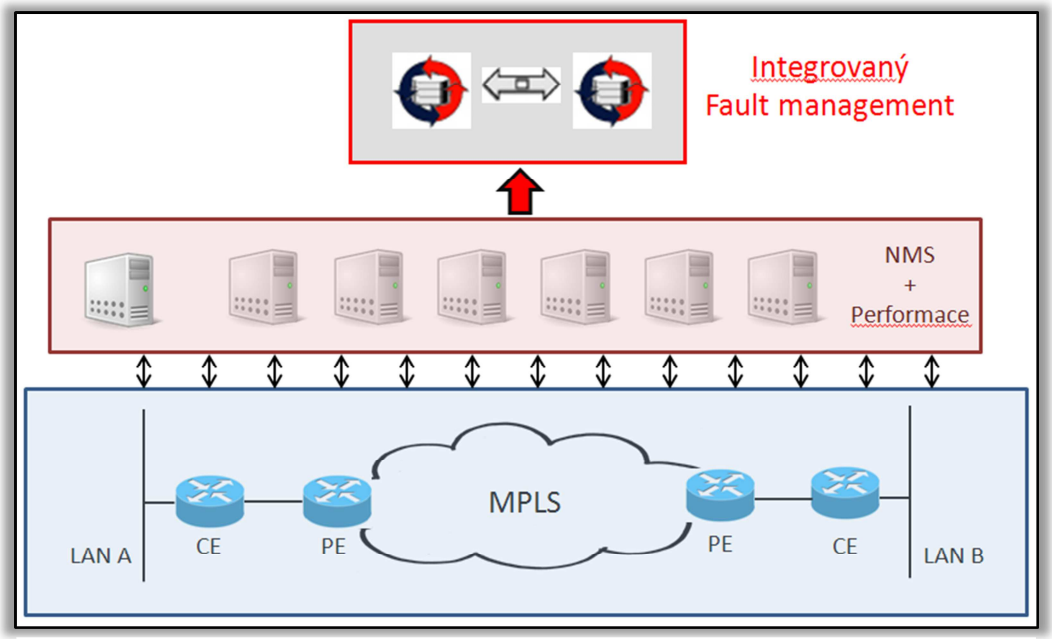
- Zálohované řešení;
- Spolupráce s již existujícími OSS systémy;
- Automatická konfigurace obsahu dle workflow a inventory databází;
- Automatická kontrola stavu zavedení služby v systémech fault managementu;
- Zobrazování sestav o aktuálních uživatelích (zákaznících) SLUŽBY;
- Možnost exportu těchto sestav pro účely dalšího zpracování;
- Zobrazování aktuálních stavů služby v reálném čase;
- Možnost základních testů dostupnosti služby;
- Možnost ruční aktivace/deaktivace proaktivního dohledu celého zákazníka nebo konkrétní služby;
- Možnost přímého zakládání incidentů ve stávajícím trouble ticketingovém systému Operátora;
- Historický reporting stavů služeb;
- Reporting pracovních aktivit Service desku.

4.3 Výchozí stav

Jak již bylo zmíněno v zadání řešení (kapitola 4.2), jednou z nezbytných podmínek, které realizované řešení musí splňovat, je jeho integrace s již existujícími OSS systémy. Tato kapitola se bude věnovat krátkému popisu právě těchto OSS systémů. Zvláštní důraz bude kladen na rozhraní (interface), která tyto systémy pro přístup okolí nabízejí.

4.3.1 Fault management

Realizace fault managementu odpovídá doporučením představeným v kapitole 3.6. Jednotlivé technologické domény, které se na zajištění služby podílejí, jsou řízeny příslušnými network management systémy (NMS) (viz obrázek 27).



Obrázek č. 27 – Stávající stav realizace fault a performance managementu u Operátora.

Alarmové výstupy těchto EMS systémů se sdružují v takzvaném integrovaném fault systému (IFM). V něm tedy dochází ke konsolidaci alarmových hlášek ze všech integrovaných NMS systémů. Na takto konsolidované alarmy jsou aplikovány některé z korelačních postupů zmíněných v kapitole 3.6.1. Více o integrovaném fault managementu lze nalézt v předcházející bakalářské práci [1].

V případě technologické domény IP sítí, je jako NMS systém použito řešení NNM od firmy Hewlett Packard (viz kapitola 3.6.3.1). Z tohoto důvodu je některá forma korelace a RCA realizována již v tomto prostředí a do IFM jsou již předávány výstupy z těchto postupů.

V prostředí Operátora je do integrovaného fault managementu zahrnut i výstup z performance monitoringu. To umožní získávat výstupy z obou oblastí řízení sítí na jednom místě.

V případě našeho řešení je nutné pro pokrytí celé služby uvažovat o zpracování alarmových stavů z celkem šesti technologických domén plus jeden zdroj generovaný performance monitoringem. Seznam těchto technologických domén je v tabulce č. 4.

Technologická doména	NMS	Rozhraní na IFM	Oblast
přístupová síť xDSL (1)	Alcatel SC	TL1	fault mng.
přístupová síť xDSL (2)	Huawei U2000	SNMP	fault mng.
přístupová síť LL	Alcatel 5620	logfile	fault mng.
přístupová síť SDH (1)	Lucent OMC	TIM	fault mng.
přístupová síť SDH (2)	Marconi MV38	CORBA	fault mng.
přístupová síť SDH + xWDM	Huawei U2000	CORBA	fault mng.
IP síť	NNM	SNMP	fault mng.
IP síť	Infovista	SNMP	performace mng.

Tabulka č. 4 – Seznam technologických domén.

Integrovaný fault management Operátora je realizován na produktech Tivoli od firmy IBM. Ty jako možné rozhraní k uloženým alarmům nabízí databázový interface do databáze Sybase.

4.3.2 Performace management

V našem případě je performance management již součástí integrovaného fault managementu (viz předcházející kapitola 4.3.1).

4.3.3 Inventory databáze

Jak již bylo zmíněno v rešeršní části této práce, obsahem inventory databáze je aktuální stav konfigurace v síti. Tato databáze musí dávat přesné odpovědi na dotazy o reálném a aktuálním stavu síťových konfigurací, například z pohledu jednotlivých provozovaných služeb.

V případě našeho řešení je potřeba zajistit spolupráci s jednou inventory databází, která v sobě obsahuje informace právě o datových službách, které jsou součástí SLUŽBY (viz kapitoly 4.4.2.3-7).

Inventory systém nabízí rozhraní k datům v něm uloženým ve formě databázových pohledů, a to pouze v režimu pro čtení (read-only). To ale vzhledem k potřebám připravovaného řešení není omezujícím faktorem.

4.3.4 Systém pro realizaci služby

Součástí procesů realizace služby je i systémová podpora jejich pracovních postupů (tzv. workflow). Tyto systémy obvykle ve spojení s katalogem služeb (kapitola 3.2.2) a inventory databází podporují procesy zřizování, modifikace a rušení služeb.

V případě představovaného řešení se jedná o právě jeden workflow systém, který nabízí read-only přístup k datům přes databázové rozhraní.

4.3.5 Systém pro práci se záznamy o incidentech

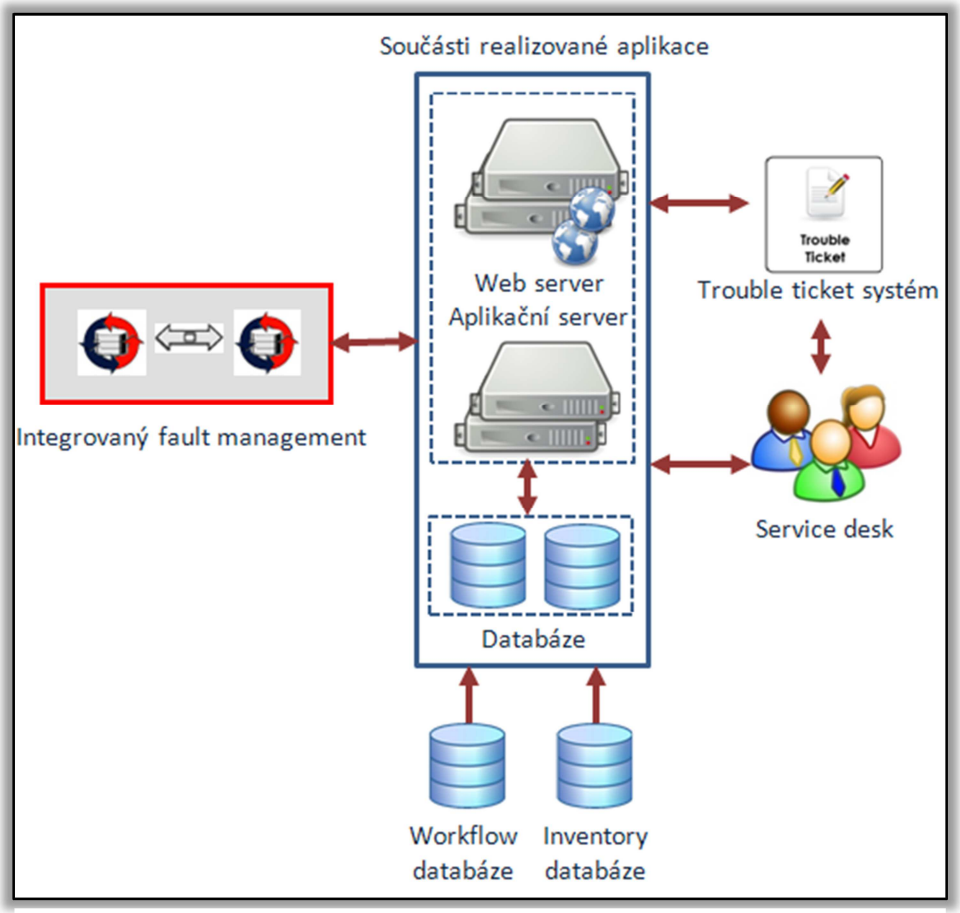
Systém pro práci se záznamy o incidentech, často nazývaný trouble ticket systém (TTS), je základní součástí technických prostředků podporujících incident management. V některých zdrojích je dokonce za incident management považován právě jenom trouble ticket systém, což ale není přesné (viz definice v kapitole 3.2.4).

V případě Operátora se využívá v případě zákaznických služeb jednotný TT systém. Ten bude také využit pracovištěm Service desku. Z podmínek zadání jednoznačně vyplývá, že tento TT systém bude zahrnut i v připravovaném řešení.

Využívaný TT systém nabízí jako interface pro okolní systémy databázové rozhraní. To je realizováno v prostředí databáze Oracle. Vzájemná komunikace TTS a okolních systémů je pak voláním uložených procedur (pro vkládání a modifikaci dat) nebo read-only přístupem do vytvořených databázových view.

4.4 Popis realizovaného řešení

Výstupem realizovaného řešení je samostatná aplikace. Je navržena v třívrstvé architektuře[29]. Základní schéma řešené aplikace je na obrázku č. 28.



Obrázek č. 28 - Základní schéma řešené aplikace.

V centrální části obrázku jsou vidět jednotlivé součásti vytvořené aplikace, v jejich okolí jsou pak vyobrazeny okolní systémy, na které má aplikace potřebná rozhraní. Samotná aplikace je fyzicky umístěna na páru redundantních aplikačních serverů, které zároveň plní funkci i webserverů. Databáze, kterou aplikace používá jako pracovní, je umístěna na separátním hardware.

[29] Vrstvy architektury:
Prezentační vrstva - je viditelná pro uživatele, zajišťuje vstup požadavků a prezentaci výsledků.
Aplikační vrstva - prostřední vrstva modelu zajišťující výpočty a operace prováděné mezi vstupně-výstupními požadavky a daty.
Datová vrstva - nejnižší vrstva modelu, zajišťuje práci s daty.

4.4.1 Datová vrstva

Datová vrstva aplikace je tvořena strukturou realizovanou v prostředí relační databáze Oracle verze 11.2. Databáze je z důvodu požadavku na redundantní řešení fyzicky realizována ve dvou paralelně běžících instancích umístěných na dvou oddělených serverech, kde synchronizace dat mezi instancemi je zajištěna pomocí služby Oracle Streams.

V databázi byly v dedikovaném schématu vytvořeny následující tabulky:

MS_ACK_EXPIRE	Tabulka acknowledged alarmů, na které byl ACK proveden pouze dočasně.
MS_ACTION_LOG	Logování akcí, které operátoři service desku provedli nad alarmy.
MS_ALARMS	Tabulka aktivních alarmů SLUŽBY.
MS_ALARMS_STATECHANGE	Čas posledního zpracovaného alarmu SLUŽBY.
MS_ALARM_LOG	Seznam historických alarmů SLUŽBY pro rychlé prohlížení a sestavu reportu.
MS_ATRIBUTY	Tabulka atributů pro technické zajištění dohledu SLUŽBY.
MS_CUST_ID_LIST	Tabulka obsahující všechny aktuální CUST_ID s počty souvisejících IP zařízení a alarmů. Slouží jako agregace pro urychlení zobrazení titulní stránky dohledu SLUŽBY.
MS_ENTITY	Základní tabulka se seznamem aktuálních entit zákazníků.
MS_ENTITYGROUP_NAME	Seznam EntityGroup (seskupování vybraných služeb) pro každého zákazníka.
MS_FIRMA	Nepovinné doplňující údaje k jednotlivým zákazníkům.
MS_CHECK_CONFIG	Výstup denní kontroly konfigurací všech nakonfigurovaných služeb
MS_JOURNAL	Nepovinný komentář k jednotlivým službám doplněný Service deskem.
MS_MLAN_DETAILS	Tabulka WAN CE routerů jednotlivých LAN lokalit.
MS_OUTAGE_STATISTIC	Tabulka s počty výpadků za daný den pro konkrétní službu zákazníka.
MS_USERDATA	Doplňující informace k jednotlivým přípojkám.
MS_UTILIZATION_STATISTICS	Tabulka s denní statistikou překročení prahových hodnot utilizace konkrétní služby zákazníka.

Tabulka č. 5 – Tabulky vytvořené v databázi v dedikovaném schématu.

Jednotlivé tabulky jsou vybaveny kombinací primárních a cizích klíčů tak, aby odpovídaly požadavkům datové normalizace. Pro urychlení práce s daty je v některých případech použito indexování.

4.4.2 Aplikační vrstva

Aplikační vrstva je řešena soustavou skriptů vytvořených v jazyce PHP. Jejich seznam a činnosti budou uvedeny v následujících odstavcích. Aktuálně využívaná verze PHP je 5.3.0 kompilovaného s rozhraními na použité typy databází.

Skripty jsou umístěny paralelně na dvou oddělených aplikačních serverech, funkční jsou v jednu chvíli právě na jednom z nich – druhý slouží jako standby záloha.

4.4.2.1 Skript create_lookup_file.php

Tento skript spouštěn jednou denně na základě poskládání dat z inventory a workflow databáze vytvoří seznam zákazníků a jejich služeb, kterých se SLUŽBA týká. Tyto výsledky jsou uloženy v tabulce *ms_entity* lokální databáze aplikace (viz kapitola 4.4.1). Součástí běhu tohoto skriptu je i kontrola všech nalezených služeb zda jsou v evidenci a tedy dohledu fault managementu pro IP síť. Pokud ne, jsou patřičně označeny a eskalovány na příslušné pracoviště servisních manažerů k dořešení.

4.4.2.2 Skript ms_enrichment_A.php

Skript *ms_enrichment_A.php* v nekonečném cyklu provádí monitorování alarmů uložených v databázi integrovaného fault managemntu a jejich následné zpracování. Využitím tabulky *ms_entity* skript kontroluje, zda daný alarm nesouvisí se SLUŽBOU. Pokud ano, doplní alarm o identifikátor zákazníka (CUST_ID v poli alarmu MS_Customer) a zapíše tento alarm do tabulky *ms_alarmlog* sloužící jako log příchozích alarmů SLUŽBY.

4.4.2.3 Skript ms_enrichment_B.php

Dalším nezávisle v nekonečném cyklu pracujícím skriptem je skript ms_enrichment_B.php. Jeho úkolem je zajistit synchronizaci označených alarmů v IFM s lokální databázovou tabulkou *ms_alarms*. Tato tabulka tedy obsahuje všechny aktuální alarmy SLUŽBY a přistupují k ní uživatelé z řad Service desku a servisní manažeři. Hlavním důvodem její existence je oddělení zátěže přicházející od uživatelů od

databáze IFM. Druhým důvodem je fakt, že alarmy v ní uložené už obsahují mnoho dalších atributů, které v IFM uloženy nejsou. Tyto atributy jsou doplněny také tímto skriptem na základě porovnání dat s tabulkou *ms_entity*.

4.4.2.4 Skript ms_enrichment_C.php

Skript *ms_enrichment_C.php* pravidelně prochází tabulku aktivních alarmů SLUŽBY *ms_alarms* a kontroluje platnost obsahu atributu *alarm_active*. Tento příznak určuje, zda je alarm aktivní v čase, kdy si na něj zákazník přál proaktivní reakci ze strany Operátora. Tato funkcionalita odpovídá požadavku na zohlednění více možných variant SLUŽBY.

4.4.2.5 Skript ms_enrichment_D.php

Skript *ms_enrichment_D.php* pravidelně kontroluje, zda u některého ze se SLUŽBOU souvisejících alarmů s příznakem *acknowledge*[30] (ACK), již neuplynula doba, po kterou bylo ACK platné. Pokud ano, provede odznačení tohoto příznaku.

4.4.3 Prezentační vrstva

Prezentační vrstva je vytvořena soustavou dynamicky generovaných stránek. Použito bylo prostředí web serveru Apache s podporou PHP. Jak již bylo uvedeno, web server je umístěn také na aplikačních serverech. Seznam jednotlivých stránek tvořící prezentační vrstvu řešení, je uveden v tabulce č. 6.

ack.php	Autorizovaným uživatelům umožňuje označovat alarmy SLUŽBY jako zpracované (ACK).
alarm_log.php	Rozhraní pro prohledávání historických alarmů na SLUŽBU.
alarmy.php	Zobrazení alarmů a souvisejících informací k vybranému zákazníkovi.
control_panel.php	Zobrazení alarmů a souvisejících informací k vybrané skupině zákazníků. Primární stránka pro Service desk.
csid.php	Doplnění nepovinných poznámek ke konkrétní službě.
diagnostika.php	Stránka pro základní, on-line diagnostiku vybrané služby.

[30] Pomocí příznaku tzv. Acknowledge si pracovníci Service desku označují alarmy, na které již není potřeba reagovat. Tato poznámka může mít někdy omezenou časovou platnost.

export_csv.php	Rozhraní pro export dat z aplikace ve formátu txt nebo csv.
firma.php	Doplnění nepovinných poznámek ke konkrétnímu zákazníkovi.
index.php	Titulní strana aplikace. Rychlý náhled na aktuální stav služeb jednotlivých zákazníků.
journal.php	Doplnění dodatečných informací k vybranému aktivnímu alarmu.
lan.php	Zobrazení detailu LAN lokality zákazníka.
search_record.php	Prohledávání databáze zákazníků a jejich služeb.
showOutageStatistics.php	Rozhraní pro zobrazování statistik výpadků. Slouží pro service managery.
showUtilizationStatistics.php	Rozhraní pro zobrazování statistik vytížených linek. Slouží pro service managery.
show_activity_reports.php	Rozhraní pro zobrazování aktivit jednotlivých pracovníků Sevice desku. Slouží pro managera Service desku.
tts.php	Rozhraní pro zakládání záznamu o incidentu nad konkrétním alarmem.

Tabulka č. 6 – Seznam dynamicky generovaných stránek prezentační vrstvy řešení.

5 Závěr

V úvodu této práce byla zmíněna naše závislost na telekomunikačních sítích a službách, které jsou jejich prostřednictvím realizovány. V podobném tempu, jakým se zmíněná závislost zvyšuje, se zvyšují i naše nároky na spolehlivost těchto služeb a související servis. V závěru předchozí bakalářské práce bylo vysloveno tvrzení, že funkčnosti a spolehlivosti těchto služeb lze dosáhnout propracovaným network managementem. Tato práce toto tvrzení rozšiřuje i na oblast incident managementu, který se týká nejenom oblasti zajištění spolehlivosti a dostupnosti služby, ale jak z této práce vyplývá, týká se i zákaznické zkušenosti.

V první části práce byly postupně definovány jednotlivé termíny související s problematikou incident managementu z pohledu standardů a doporučení ITIL. Následně byl představen koncept TMN modelu pro doménu řízení sítí se zvláštním důrazem na oblast fault managementu. Ta byla následně rozšířena o shromážděné poznatky o postupech korelací alarmů a hledání jejich kořenových příčin.

Ve druhé části je nejprve popsána vybraná zákaznická služba z portfolia služeb telekomunikačního operátora. Pro zavedení této služby do reálného světa bylo nutné vyřešit i úkoly související právě s tématem incident managementu. Definovanou část těchto úkolů řeší autorem vytvořená aplikace, která je představena v této části práce.

Návrh reálné a funkční aplikace tak, jak byla představena v praktické části, plní cíle této diplomové práce. Reálnost aplikace je dána jejím skutečným nasazením v prostředí telekomunikačního operátora a funkčnost skutečností, že aplikace již druhým rokem pokrývá definovanou oblast incident managementu komerčně úspěšné služby, využívané hlavně velkými korporacemi.

6 Seznam použité literatury

[1] VAŠÁK, Martin. Návrh fault managementu ve vybraném podniku. Praha, 2011. Bakalářská práce. Česká zemědělská univerzita v Praze. Vedoucí práce Ing. David Buchtela, Ph.D.

[2] DINI, P, Pascal LORENZ a José Neuman de SOUZA. *Service assurance with partial and intermittent resources: First International Workshop, SAPIR 2004, Fortaleza, Brazil, August 1-6, 2004 : proceedings*. New York: Springer, c2004, xi, 312 p. ISBN 35-402-2567-6.

[3] STALLINGS, William. *SNMP, SNMPv2, and CMIP: the practical guide to network-management standards*. Reading, Mass.: Addison-Wesley Pub. Co., c1993, xvii, 625 p. ISBN 02-016-3331-0.

[4] ROWE, Stanford H. *Business telecommunications*. Chicago: Science Research Associates, c1988, xx, 529 p. ISBN 05-741-8690-5.

[5] MENINGER, Milan. *Digitální telekomunikační technika: Postgraduální studium*. 1. vyd. Praha: ČVUT, 1993, II, 45 s. ISBN 80-010-0892-4.

[6] TSCHICHHOLZ, Michael. *Design of a TMN based inter domain management environment for the open service market: an ODP based modelling approach*. München [u.a.]: Oldenbourg, 1996. ISBN 34-862-4092-7.

[7] HALL, Jane. *Management of telecommunication systems and services: modelling and implementing TMN-based multi-domain management*. New York: Springer, c1996, xxi, 229 p. ISBN 35-406-1578-4.

[8] HEWLETT PACKARD. *Causal Analysis White Paper: Software Version 9.00*. Palo Alto, CA, 2012. Dostupné z: http://support.openview.hp.com/selfsolve/document/KM869731/binary/nnmi_causal_analy_whitepaper_9.20.pdf

[9] *ITIL 2011*. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.

[10] VITOUŠ, Martin. Výzvy v řízení IT: K čemu jsou ITIL, CobiT, CMMI, Lean, Six Sigma. Connect!. 2010, roč. 15, č. 2, s. 8-10. DOI: 1211-3085.

[11] ZAHRADNÍK, Pavel. Jak je důležité míti nejen Filipa: Aneb kterak být za draho I(n)TIL. 2010, roč. 15, č. 2, s. 11. DOI: 1211-3085.

[12] HASAN, Masum, Binay SUGLA a VISWANATHAN. *A Conceptual Framework for Network Management Event Correlation and Filtering Systems* [online]. 2006 [cit. 2013-03-06]. Dostupné z:

http://users.encs.concordia.ca/~assi/courses/network%20management%20material/a-conceptual-framework-for.pdf

[13] HEWLETT PACKARD. *HP OpenView Communications Event Correlation Services Administrator's Guide*. Palo Alto CA, 2009. Dostupné z: http://support.openview.hp.com/selfsolve/document

[14] IBM. *Technical overview of TBSM*. Armonk, New York, 2010. Dostupné z: http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/index.jsp

[15] *EMC* [online]. 2012 [cit. 2013-03-10]. Dostupné z: http://www.emc.com

[16] *CISCO* [online]. 2013 [cit. 2013-03-10]. Dostupné z: www.cisco.com

[17] VONDRÁČEK, Petr. *Metody dohledu telekomunikačních služeb*. Praha, 2005. Disertační práce. ČVUT, Fakulta elektrotechnická, KTT. Vedoucí práce Doc. Ing. Boris Šimák, Csc.

[18] MEIRA, Dilmar Malheiros. *A model for alarm correlation in telecommunication networks*. Belo Horizonte, 1997. Disertační práce. Federal University of Minas Gerails, Brasil.

[19] LEWIS, Lundy. *Service level management for enterprise networks*. Boston: Artech House, c1999, xiii, 307 p. ISBN 15-805-3016-8.

[20] BIRTOVÁ, Ivana a Petr SODOMKA. Řízení pracovních toků prostřednictvím workflow. *Computerworld*. Praha: IDG Czech, a.s, 2012, XXII, č. 7. ISSN 1210-9924.

[21] DOLEJŠ, Radan. S rychlostí roste chuť. *Computerworld*. Praha: IDG Czech, a.s, 2013, XXII, č. 3. ISSN 1210-9924.

[22] ADDY, Rob. *Effective IT service management to ITIL and beyond!*. Online-Ausg. Berlin: Springer, 2007. ISBN 978-354-0731-986.

7 Přílohy

Příloha 7.1 – Diagram /zdroj [9]/