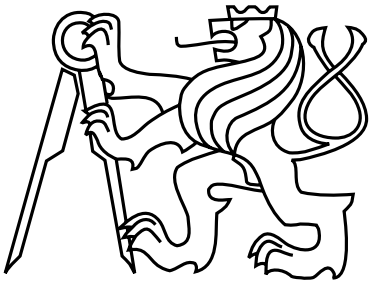
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra počítačů



Diplomová práce

SNMP/XML brána

Bc. Tomáš Hroch

Vedoucí práce: Ing. Peter Macejko

Studijní program: Elektrotechnika a informatika, strukturovaný, Navazující magisterský

Obor: Výpočetní technika

9. února 2009

Poděkování

Zde můžete napsat své poděkování, pokud chcete a máte komu děkovat.

Prohlášení

Prohlašuji, že jsem práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.
Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kořenovicích nad Bečvárkou dne 15. 5. 2008 .....

Abstract

Translation of Czech abstract into English.

Abstrakt

Abstrakt práce by měl velmi stručně vystihovat její podstatu. Tedy čím se práce zabývá a co je jejím výsledkem/přínosem.
Očekávají se cca 1 – 2 odstavce, maximálně půl stránky.

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Správa velkých počítačových sítí je v dnešní době naprosto samozřejmým úkolem většiny administrátorů. Velké množství spravovaných sítí se neomezuje pouze na lokální prostředí dané firmy či instituce. Může být naopak rozprostřena v rámci jednoho města, státu či dokonce několika států najednou. Efektivní spravování takovéto komunikační infrastruktury je úkolem velice náročným.

Jedním z protokolů, který takovouto vzdálenou správu umožňuje, je SNMP. Na jeho základě bylo vybudováno bezpočet aplikací, které mají za úkol sledovat provoz na síti, zatížení určitého systému a v neposlední řadě umožnit administrátorovi vzdálenou správu daného přepínače, routeru či pracovní stanice.

Protokol SNMP byl navržen v dřívějších dobách a nemusí plně vyhovovat dnešním požadavkům, až už na bezpečnost nebo efektivní využití přenosových médií. Pan Ing. Peter Macejko se ve své diplomové práci ([1]) zaobíral použitím technologií XML a návrhu protokolu, který by umožňoval minimálně stejnou funkcionalitu jako protokol SNMP a tento zefektivnil.

Tato práce se zaobírá vytvořením protokolové brány, která by umožnila použít navržený XML protokol ke správě strojů, které stále používají protokol SNMP. Cílem je vytvořit softwarový produkt, který bude plnit úkol prostředníka mezi správcem a spravovaným strojem. Hlavními problémy jsou implementace navrženého XML protokolu a spojení jej s několika verzemi protokolu SNMP.

V kapitole 2 je podrobně popsán protokol SNMP.

Kapitola 2

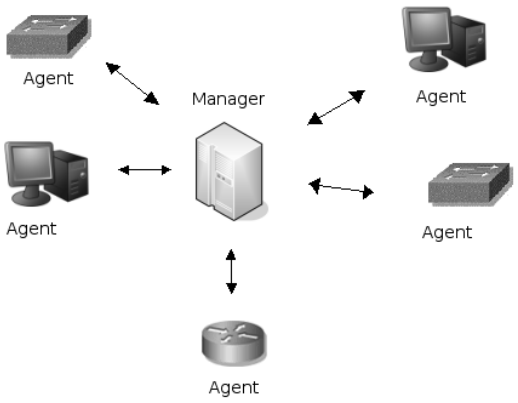
SNMP

SNMP, nebo-li Simple Network Management Protocol, je v dnešní době jeden z nejrozšířenějších protokolů na správu počítačové sítě. Je to aplikační protokol, který je součástí TCP/IP rodiny protokolů. Byl vyvinut skupinout IETF (Internet Engineering Task Force) a přijat jako standard v roce 1989. Umožňuje sledovat síťový provoz, hledat a řešit problémy, které se při provozu vyskytnou.

2.1 Správní struktura

SNMP je tvořen sadou standardů, které popisují správu sítě, zahrnující samotný komunikační protokol, definici databázové struktury (SMI) a datové objekty (MIB).

Základním funkčním principem je model Klient - Server. Struktura spravované sítě se tak dělí na tři klíčové elementy - spravované zařízení, agenta a manažera (viz obrázek 2.1).



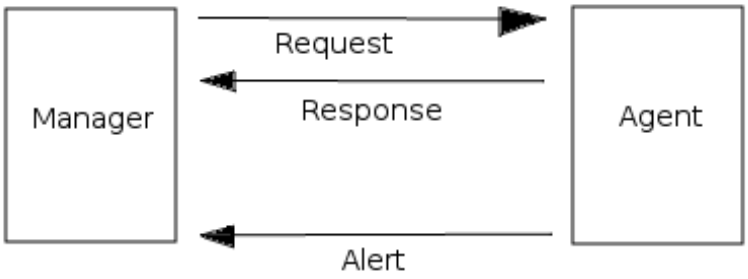
Obrázek 2.1: Základní princip fungování SNMP spravované sítě

- **Spravovaný systém** - je zařízení (přepínač, router, atd.), na kterém je spuštěn SNMP agent. Toto zařízení shromažďuje sledované informace a pak je dává k dispozici manažerovi pomocí SNMP protokolu.

- **Agent** - je software určený pro pro správný překlad požadavků manažera a jejích vykonání na sledovaném systému. Navíc může při sledování posílat manažerovi upozornění, že něco není se systémem v pořádku.

- **Manažer** (NMS - Network Managemet System) - je aplikace, která sleduje a spravuje všechny systémy na sledované síti. Tento systém získává od agentů data, zpracovává je do vizuální podoby, čímž dává možnost administrátorovi mít přehled o celé síti. Zároveň umožňuje měnit sledované parametry přímo u agenta.

Komunikace můžeme rozdělit do dvou kategorií dle toho, kdo jí započal. Základní schéma je vyjádřeno na obrázku 2.2.



Obrázek 2.2: Komunikace mezi SNMP manažerem a agentem

V první části schématu je vyobrazeno standardní chování managera, který posílá dotazy agentovi, který mu odpovídá. Přesný výpis příkazů a zpráv, které si mohou tyto dva systémy mezi sebou vyměňovat, bude diskutován dále v této kapitole.

Druhá část schématu popisuje moment, kdy na sledovaném systému nastala nějaká extrémní situace (např. zatížení síťového spoje se blíží k maximu) a agent informuje manažera pomocí zprávi Alert (v SNMP jsou to zprávy TRAP či INFORM, obě budoudiskutovány dále).

Je nutné zmínit, že SNMP protokol pracuje nad transportním protokolem UDP, který je nepotvrzovaný. Není tedy zaručeno, že bude komunikace probíhat bezchybně. Je možné, že některé dotazy a příkazy vůbec nedojdou ke svému cíli, o čemž se druhá strana nikdy nedozví. Tento fakt může být překážkou při správě rozsáhlých sítí, kde jsou špatné síťové spoje.

2.2 SMI, MIB standardy

Jak již bylo zmíněno dříve, SNMP je sada standardů, která kromě komunikačního protokolu musí definovat i strukturu sledované databáze a samotná data. Tyto informace byly definovány ve standardech SMI a MIB.

SMI

SMI je zkratkou pro Structure and Identification of Management Information for TCP/IP-based Internets. Tento standard ([?]) popisuje a definuje základní datové struktury a typy, které protokol využívá. Jednotlivé objekty jsou pojmenovány a organizovány, aby bylo možné k těmto datům logicky přistupovat. Dle standardu musí mít každý objekt jméno, syntaxi a kódování. Jméno jednoznačně identifikuje objekt. Datový typ (číslo, řetězec) je určen syntaxí. Kódování zajišťuje správnou serializaci dat při přenosu mezi systémy.

Objekty, identifikovány svým jménem (OID), jsou seřazeny do hierarchické struktury. K identifikaci je použito Abstract Syntax Notation One (ASN.1). Každý OID identifikátor je složen ze skupiny přirozených čísel, které vyjadřují jeho pozici v pomyslném stromu. Strom má kořen, který je spojen hranami s očíslovanými uzly. Každý uzel může mít vlastní děti, čímž tvoří vlastní podstrom. Takto je možno pokračovat dále do značné hloubky stromu. Tento standard též specifikuje, jaké identifikátory jsou přiřazeny počátku správní databáze.

MIB

MIB je zkratka pro Management Information Base. Je to soubor definicí, které popisují parametry a vlastnosti sledovaného zařízení. Existuje více než 100 různých MIB, které popisují různá zařízení. Každý takovýto soubor definic musí splňovat předpisy SMI, aby bylo zaručena správná interpretace objektů. Každý objekt (někdy také nazýván MIB objekt) je unikátně identifikován svým OID a všechny dohromady jsou uspořádány do stromové struktury tak, jak to bylo popsáno v minulém odstavci.

Objekty v dané databázi se dělí na *skalární* a *tabelární*. Skalární objekty reprezentují jeden parametr sledovaného zařízení (např. počet ethernetových karet v přepínači), kdežto tabelární objekty jsou spojením několika spřízněných objektů (např. routovací tabulka je spojením jednotlivých záznamů, coby řádků dané tabulky).

V rámci hierarchického uspořádání jsou vyhrazeny vyšší úrovně stromu (blíže kořenu) jednotlivým standardizujícím organizacím, nižší úrovně jsou poté zadány jednotlivými společnostmi. Každý výrobce si může definovat svojí privátní větev, do které umístí specifické informace daného zařízení.

MIB, které nebyly standardizovány a oficiálně schváleny, jsou umístěny do větve experimentální.

2.3 Verze SNMP protokolu

Celkem byly doposud standardizovány tři verze protokolu SNMP. Každá z nich definuje svoje specifické datové typy a používané datové rámce pro komunikaci.

SNMPv1

V první verzi protokolu byly definovány dvě skupiny datových typů:

- Základní datové typy (Simple data types)
- Aplikační typy

Základní typy jsou definovány v SNMPv1 SMI a definují základní používané hodnoty:

- **INTEGER** - celá čísla od -2^{31} do $2^{31} - 1$
- **OCTET STRING**
- **OBJECT IDENTIFIER** - identifikace jednotlivých objektů v rámci normy ASN.1

Aplikační specifické typy pak jsou:

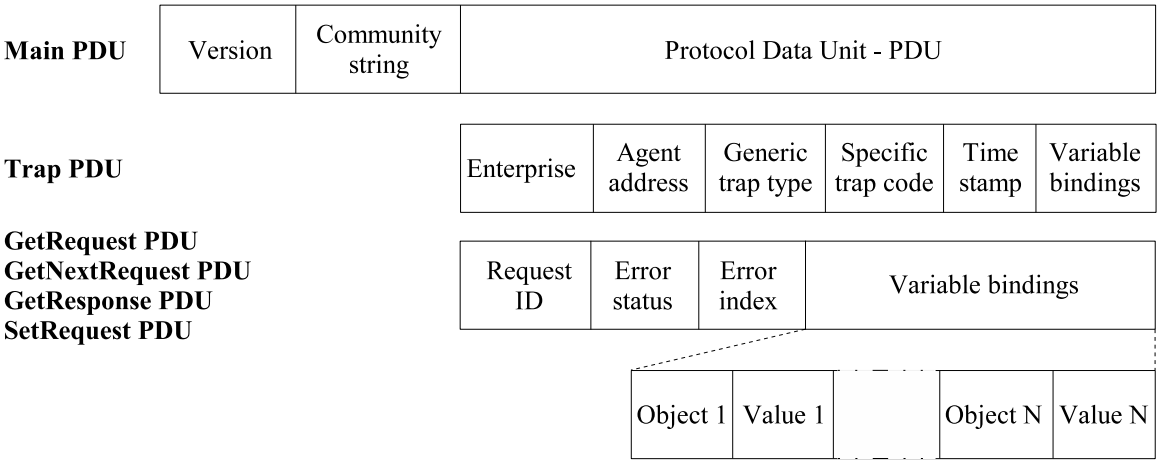
- **Network Address** - obecná síťová adresa pro podporu mnoha rodin protokolů.
- **IpAddress** - přímo definovaný typ pro IP adresu. SMIv1 podporuje pouze 32 bitovou adresu (IPv4)
- **Counter** - čítač, vyjádřen celým číslem bez znaménka; Jeho hodnota se pouze zvyšuje a to až do maxima a pak se vrací zpět na nulu
- **Gauge** - je definována jako nezáporné celé číslo. Může hodnotu zvyšovat i snižovat a to v definovaných mezích minima a maxima
- **Time Ticks** - počet hodinových tiků od nějaké události, měřeno v setinách vteřiny
- **Opaque** - typ dovolující přenášet libovolná data v kódování ASN.1. Tato data jsou zakódována jako OCTET STRING a následně přenesena médiem.
- **Integers** - celočíselný typ, který předefinovává specifikaci v SMI
- **Unsigned Integer** - celočíselný typ bez znaménka, který stejně jako předchozí předefinovává specifikaci.

Komunikační mechanismus mezi manažerem a agentem je definován pomocí datových rámců, které je možné v rámci SNMPv1 přenášet. Tyto jsou:

- **Get Request** - získání hodnoty uzlu identifikovaného OID (zpráva od manažera agentovi)

- **Get Next Request** - žádost o hodnotu uzlu následujícího po zaslaném OID (od manažera k agentovi)
- **Set Request** - Nastavení hodnoty uzlu specifikovaném OID (od manažera k agentovi)
- **Get Response** - odpověď agenta manažerovi na Get a Set zprávy. Obsahují požadovanou hodnotu
- **Trap** - zpráva od agenta manažerovi, která upozorňuje na nastálé situace na monitorovaném systému.

Strukturu jednotlivých SNMP paketů zobrazuje obrázek 2.3. Pro pochopení významu jednotlivých polí se obraťte na [**?**].



Obrázek 2.3: Schéma datových paketů protokolu SNMPv1 a v2

Bezpečnost v této verzi protokolu je založena pouze na takzvaném *community string*u, který vystupuje jako heslo. Existují pouze dvě úrovně zabezpečení přístupu a to - pouze pro čtení (read only) a čtení-zápis (read-write access). Je patrné, že se používají pouze dvě hesla, každé pro jednu úroveň. Je to velice slabé zabezpečení, vezmeme-li v úvahu, že toto heslo se posílá nezašifrované a každý, kdo dokáže odchytit jednotlivé pakety, si může tento řetězec přečíst. Tento nedostatek se pokoušejí odstranit až další verze protokolu.

SNMPv2

Druhá verze protokolu SNMP byla zaměřena na odstranění nedostatků verze první. Bohužel bylo vydáno několik soupeřících specifikací, označované názvy SNMPv2c, SNMPv2u, SNMPv2*, které byly vzájemně nekompatibilní. Nicméně zlepšení oproti první verzi bylo několik. Byly definovány nové datové typy, nové zprávy a zlepšená práce s chybami.

Nové datové typy zahrnují rozšíření podpory z 32-bitových čísel na 64-bitová (Integer32, Integer64, Counter32, ...).

Přidané zprávy jsou:

- **Get Bulk** - tento operátor se snaží efektivněji využít přenosovou kapacitu kanálu tím, že od agenta si vyžádá sérii informací pomocí jediného dotazu.
- **Inform** - stejná funkcionalita jako zpráva Trap ve verzi 1, ale nutné je potvrzení od manažera, že zprávu přijal (Response paket)
- **Response** - odpověď na předcházející Inform zprávu (od manažera k agentovi)

Ostatní zprávy SNMPv2 přebírá z předchozí verze a zachovává jejich strukturu. Stejně tak je to i s bezpečností, kde je stále použito heslo ve smyslu community stringu.

SNMPv3

Třetí verze protokolu SNMP je definována sadou standardů, které nepostihují celkovou funkčnost protokolu jako takového, ale dodávají do systému chybějící prvky, hlavně bezpečnosti. Přímo v jednom ze standardů [**?**] je řečeno, že tato verze může být chápána jako SNMPv2 s dodatečnými administrativními a bezpečnostními schopnostmi.

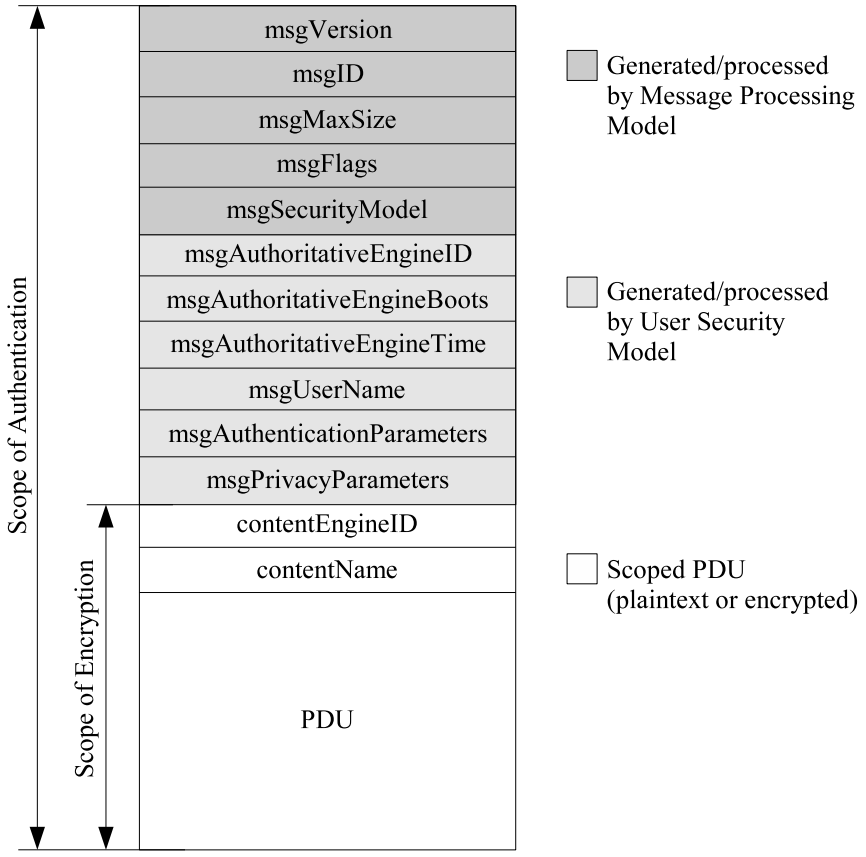
SNMPv3 definuje tři základní služby:

- *Autentifikaci* - datový přenos od manažera k agentovi může být autentifikován, aby se zajistilo ověření identity odesílajícího.
- *Soukromí* - šifrování přenášených zpráv.
- *Přístupová práva* - agent může definovat přístupová práva, omezovat přístup manažerům k pouze některým akcím a částem dat.

Základním principem SNMPv3 je modularita. Každá SNMP entita je tvořena SNMP řídícím systémem a vlastní aplikací. Řídící systém má za úkol přijímat, odesílat, šifrovat, dešifrovat všechny zprávy a dále spravuje a kontroluje monitorované objekty. Tyto funkce jsou poté k dispozici jedné či více aplikací.

Stejně jako předchozí verze, je SNMPv3 založena primárně na transportním protokolu UDP, ale není na něj vázána. Pro přenos dat tak může být použit i jiný protokol. Vlastní aplikační protokol SNMP je rozdělen do dvou úrovní. První zpracovává datové pakety (PDU processing layer) a druhá zpracovává zprávy (message processing layer). Nejvyšší úroveň - PDU processing layer - se stará o zpracování příkazů (Get, Get Next, ...), které přijdou v daném paketu. Zpracovaný paket pak předá nižší úrovni - message processing layer - která tomuto paketu dodá hlavičku, kde jsou uložena bezpečnostní data.

Na obrázku 2.4 je vyobrazen formát SNMPv3 zprávy. První část je tvořena systémem zpracování zpráv. Nese informace ohledně verzi protokolu, identifikaci zprávy, maximální délce zprávy a nastavení bezpečnostího modelu. Druhá část je generována bezpečnostním systémem a obsahuje informace o kódování a autorizaci. Třetí část obsahuje samotná data.



Obrázek 2.4: Schéma datového paketu protokolu SNMPv3

Důležitou součástí nového standardu je i systém přístupových práv (VACM - View-Based Access Control Model). Tento model umožňuje nakonfigurovat agenta tak, že specifickému manažerovi bude umožněn přístup pouze k části MIB. Je možné omezit manažera pro přístup pouze k části databáze monitorovaných dat a zároveň ještě omezit operace, které nad touto množinou může provádět. Omezení přístupu se provádí pro definované skupiny, kde součástí jedné skupiny může být více manažerů.

Kapitola 3

XML protokol

Zde bude doplnen seznam funkci, struktura a pozadavky vyplyvajici z prace p. Macejka = všechno o XML protokolu.

3.1 Trasformace SNMP do XML

3.2 Struktura protokolu

3.3 Zprávy

Kapitola 4

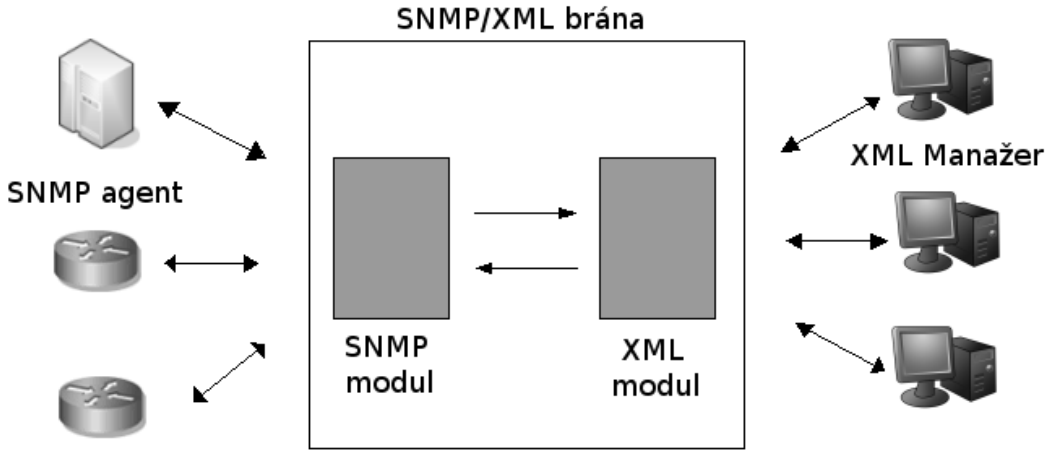
Návrh systému

V předchozích dvou kapitolách byla rozebrána teoretická část problému. V této kapitole shrneme požadavky vyplývající z teorie, které je nutno zakomponovat do výsledného systému. Nejprve bude schématicky vyjádřena obecná funkcionalita systému, která se následně bude rozebírat detailněji.

4.1 Teoretické požadavky

Nároky na systém, které vyplývají z teorie můžeme rozdělit do třech částí - implementace SNMP protokolu, implementace navrženého XML protokolu a propojení těchto dvou protokolů dohromady.

Hlavním požadavkem, který vyplývá i ze zadání práce, je vytvořit modulární systém, který bude nejenom spojovat současné verze protokolů, ale bude počítat i s potenciálním rozšířením do budoucna. Obecné schéma navrhovaného systému zobrazuje obrázek 4.1.



Obrázek 4.1: Schéma navrhovahého systému

Zde je vidět, že oba dva protokolové moduly jsou na sobě nezávislé a jejich interakce spočívá v předávání si zpráv. Nyní přejděme k detailnějším požadavkům na výše zmíněné části systému.

V rámci *SNMP protokolu* je požadováno

- implementace komunikačních struktur protokolů SNMPv1 a SNMPv2
- převzetí bezpečnostního schématu z tohoto protokolu

XML orientovaná část programu má za úkol

- implementovat komunikační struktury navrženého protokolu
- navrhnout efektivní správu XML struktur v paměti
- poskytnout XML manažerům transparentní získání dat z monitorovaných zařízení
- mapovat rozšířenou množinu funkcí v rámci XML protokolu do SNMP
- s manažery komunikovat pouze přes HTTP/HTTPS protokol

Spojením protokolů je myšlen přechod od databázových struktur jednoho protokolu k druhému. V našem případě je to transformace SNMP MIB do XML, jak bylo vysvětleno v kapitole 3.

4.1.1 XML

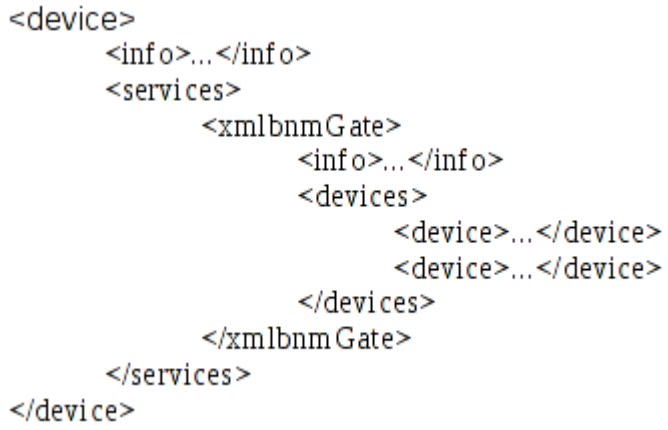
Nejprve se zaměříme na reprezentaci dat, které budou v rámci XML popisovat jak bránu, tak monitorované zařízení. Z předchozích kapitol vyplynulo, že bude použito částečně objektového přístupu a přímého mapování MIB. Strukturu dat bude popisovat XML dokument, strom, který má strukturu vyjádřenou na obrázku 4.2.

Kořenový uzel specifikuje celé zařízení vystupující jako protokolová brána, obsahuje tyto elementy:

- **info** - tento element obsahuje text, kterým je popsáno dané zařízení.
- **services** - element vymezující poskytované služby (při širší implementaci může obsahovat služby DNS, DHCP, apod.)
- **xmlbnmGate** - naše služba poskytující spojení XML a SNMP protokolu
- **device** - je podelementem **xmlbnmGate** a vymezuje jedno monitorované zařízení

Prvky **device** jsou do XML dokumentu přidávány na základě informací v konfiguračním souboru (viz kapitola 4.2).

Strukturu elementu **device** popisuje obrázek **??**. Každý takovýto element bude obsahovat následující informace:



Obrázek 4.2: Obecná struktura XML dokumentu

- **info** - stejně jako kořenový element popisuje dané zařízení
- **notifications** - obsahuje elementy a typy upozornění (TRAP zprávy v rámci SNMP), na které manažer čeká
- **subscriptions** - obsahuje informace o datech, které si nechává manažer posílat v pravidelných intervalech (více v popisu komunikace)
- **data** - sem jsou mapována veškerá data přímo z MIB.

Samotný element má atribut *id*, což je jeho identifikace v rámci xml dokumentu. Dle tohoto unikátního čísla je pak možné v sadě dotazů rozpoznat, ke kterému zařízení se dotaz vztahuje.

Element **info** obsahuje elementy, které specifikují jméno a popis zařízení (viz obrázek **??**).

Jednotlivé podelementy uzlu **subscriptions** musí z podstaty věci obsahovat informace, které určují, jaké objekty chce manažer pravidelně sledovat, identifikovat manažera, aby mu mohly být data doručena a specifikovat časový interval, tj. frekvenci sledování příslušné veličiny.

Děti uzlu **notifications** určují, které typy událostí jsou sledovány u daného zařízení. V rámci konfigurace systému je nezbytné, aby pro každé zařízení bylo jasně definováno, kam mají být příslušné zprávy o událostech zasílány. Tudíž v rámci typu události je nutné uvést příjemce, který bude zprávy očekávat. Přesná specifikace jednotlivých uzlů dokumentu je v příloze

Mapování dat z MIB bylo obecně popsáno v kapitole 3 a přesný algoritmus bude specifikován v následující kapitole. Pro adresaci jednotlivých objektů je, jak bylo již nastíněno v předchozí kapitole, použito mechanismů XPath či XQuery. Dotaz na položku z MIB může vypadat následovně

```
/device/services/xmlbnmgate/device[id=1]/data/...
```

Zprávy

Zprávy, které budou posílány mezi manažerem a bránou, mají formu XML dokumentu. Schématicky je znázorněna a popsána v kapitole 3, obrázek .

Kořenový element message obaluje veškerá posílaná data. Může obsahovat několik dílčích dotazů, nastavení a ostatních informací, které budou vykonávány postupně jedna po druhé. V rámci teorie byla nastíněna možnost použití několika různých front, které by byly specifikovány identifikátorem a zaručovaly by různou prioritu zpracování. Navrhovaný systém bude podporovat pouze jednu frontu zpracování zpráv, čímž budou jednotlivé dotazy zpracovány postupně. Bude tak zaručena integrita dat a předejde se různým extrémním situacím.

Komunikace mezi manažerem a bránou je na XML úrovni omezena na zprávy

- GET
- SET
- DISCOVERY
- PUBLICATION
- SUBSCRIPTION
- DISTRIBUTION
- EVENT

Přesná struktura a popis funkce jednotlivých zpráv byla popsána v předchozí kapitole.

Komunikační protokol

Od protokolu SNMP se XML část komunikace liší taky tím, že bude probíhat na spolehlivém a potvrzovaném protokolu - HTTP. Každá zpráva, která je poslána, musí mít potvrzeno doručení, což tento aplikační protokol, využívající transportního protokolu TCP, nabízí.

Informace budou posílány ve formátu HTTP POST zprávy. Strukturu dotazu a odpovědi zobrazuje obrázek **??**.

Otázka bezpečného přenosu dat byla řešena v předchozí kapitole a byl zvolen protokol HTTPS. Zajištění distribuce a zpracování certifikátů bude diskutováno dále v této kapitole.

4.1.2 SNMP

Druhou část komunikace tvoří SNMP protokol. Z kapitoly **??** vychází seznam zpráv, které je nutné implementovat:

- Get
- Set
- Response
- GetNext
- Trap

V rámci komunikace se v naší práci budeme zaobírat verzemi SNMPv1 a SNMPv2. Samotná implementace a mapování SNMP zpráv na XML dotazy bude diskutována až v kapitole 5.

Bezpečnost se v SNMP omezuje pouze na komunitní heslo, které je zasíláno jako součást XML zprávy a bude pouze přepsáno do SNMP paketu. Je tedy zřejmé, že ponecháváme bezpečnost takovou, jak je standardizována v SNMP protokolu.

4.2 Struktura programu

4.3 Manager

Kapitola 5

Implementace

Literatura

[1] I. P. Macejko. *XML SNMP protocol*, volume 1. CVUT, Oval Road, London, UK, 4th edition, 2006.