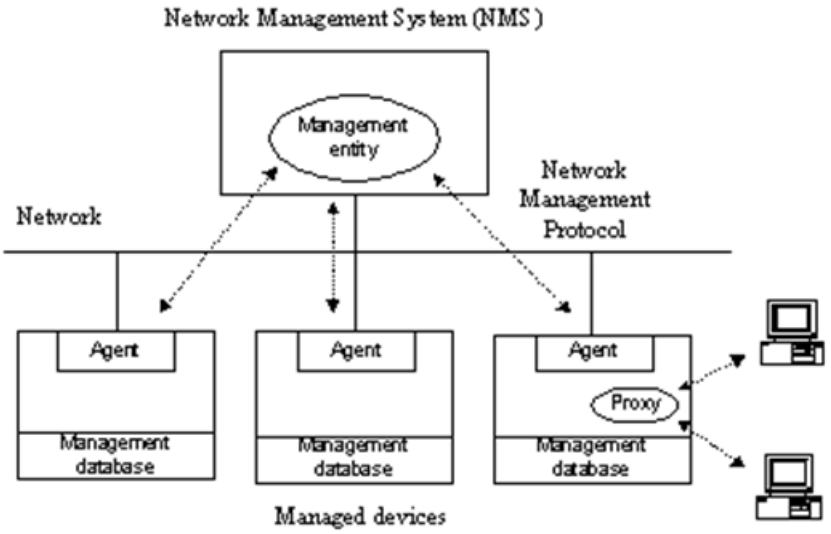
# Správa sítí

## Architektura síťové správy

Většina systémů síťové správy používá obecnou architekturu podpory koncových zařízení založenou na modelu Manager - Agent. **Agenti jsou na koncových zařízeních. Manager je instalován centrálně a je realizován management softwarem** (např. NMS - Network Management System).

### Model Manager-Agent

Agent je malý program, reprezentující dané zařízení, který neustále monitoruje a sbírá informace o všech dostupných funkcích a stavech daného zařízení a ukládá je do management database (MIB – management information database).




Manager získává informace o stavu zařízení na základě vyslaného požadavku **(pooling).** Pooling se většinou provádí v určitých časových intervalech.

Informace mohou být vyslány agentem bez vyžádání managerem a to v případě, že agent detekuje např. hardwarovou poruchu **(trap)**. Na trap pak reagují entity management systému a je tím zajištěna rychlá odezva na nestandardní stav zařízení.

Kombinace trap agenta a pooling managera zvyšují efektivitu správy zařízení.

## Model správy ISO

Stejně tak jako při tvorbě síťového modelu ISO/OSI sehrála ISO roli i při standardizaci managementu IS (informačního systému). **Model ISO/OSI Management Framework se skládá z 5 částí,** které odpovídají základním funkcím managementu IS.

- Správa výkonu- performance management
- Správa konfigurace- configuration management
- Účetní a evidenční správa - accounting management
- Správa poruch a chyb - fault management
- Správa bezpečnosti- security management

## Správa výkonu- performance management

Smyslem správy výkonu (performance management) je měření výkonnosti a zatížení jednotlivých částí a komponent IS. Jedná se o parametry jako např. zatížení operačního systému, využití šířky přenosového pásma, čas odezvy aplikací apod.

Správu parametrů lze provádět 2 způsoby:

- **Reaktivní management.** Při nastavení prahových úrovní je možné při kontinuálním monitorování zvolených parametrů **reagovat na překročení těchto parametrů odpovídající akcí. Vždy alespoň varovnou zprávou** pro správce systému nebo i pro uživatele.
- **Proaktivní management.** Pomocí **simulací lze plánovat potřebné změny,** případný růst IS a vliv těchto změn na výkonnost sítě. Jde především o metodu "what if" např. když se provede tato topologická změna, jak to ovlivní zatížení tohoto segmentu atd.

## Správa konfigurace- configuration management

Správa konfigurace znamená monitorování IS a jeho konfigurace z důvodů poznání vlivu jednotlivých elementů IS na jeho chod. Elementy IS jsou

- **fyzické** tj. servery, pracovní stanice, veškeré komunikační prvky (switche, směrovače, modemy, atd.), kabeláž a fyzická topologie sítě,
- **logické** tj. síťové operační systémy, operační systémy klientů, používané protokoly a aplikace.

Konfigurační subsystém ukládá veškeré konfigurační informace do databáze (MIB).

## Účetní a evidenční správa - accounting management

Cílem účetní a evidenční správy je monitorování parametrů využití IS jednotlivými uživateli. Tyto informace ve formě reportů umožní správci IS:

- účtovat uživatelům poplatky za využití jednotlivých zdrojů,
- plánovat potřebné změny a růst sítě
- případně regulovat přístup uživatelů k6 jednotlivým zdrojům a tak zajistit jejich co nejefektivnější a spravedlivé sdílení.

### Správa poruch a chyb - fault management

Cílem správy poruch a chyb je detekce chyb a poruch IS, jejich izolace a záznam do chybového souboru. Následuje buď pokus o jejich nápravu nebo alespoň upozornění **(alert)** uživatelům a správci IS o vzniku problému. Tato oblast managementu IS je nejrozšířenější, protože poruchy IS způsobují významné finanční ztráty.

### Správa bezpečnosti- security management

Správa bezpečnosti řídí přístup uživatelů do IS podle stanovených pravidel (bezpečnostních politik) tak, aby nemohlo dojít k neoprávněnému (úmyslnému nebo neúmyslnému) zničení nebo zneužití dat. Jeho součástí je

- **nastavení systému autorizace** (oprávněnosti přístupu) uživatelů k jednotlivým entitám IS
- **monitorování a detekování pokusů o neoprávněný přístup do IS** např. zadávání hesla a počet pokusů.

## Metriky IS

Metrikami se nazývají datové elementy, které indikují chování systému, subsystému nebo aplikace. **Správný výběr metrik** pro účely managementu (provozu IS) **je kritický** z hlediska úspěšného řízení IS.

Podle stavu spravovaného IS se budou lišit nároky na potřebné komponenty správy. V experimentálních nebo vývojových stadiích budou potřeba co největší objemy sesbíraných dat a jejich uchování pro pozdější analýzu (poznání chování systému). V této fázi ještě není jasné, které údaje jsou pro nás důležité. Jakmile je systém vyladěn není již nutné monitorovat a uchovávat tolik dat.

Pro řízení provozu IS je nezbytný management v reálném čase. Nutné je řešení problémů v krátkých časových intervalech a rychlá reakce na upozornění systému o porušení stanovených pravidel chování jednotlivými subsystémy nebo rychlá reakce na informace o zhoršení celkového stavu systému.

### Sady metrik

Pro optimální využití prostředků managementu je nutné stanovit odpovídající sady metrik. **Sady se většinou dělí do 3 skupin.** Každá sada je určena pro jinou oblast požadavků.

- **Skupina nejvyšší úrovně.** Malé množství metrik (1 - 10), poskytující pohled na systém z nejvyšší úrovně v reálném čase. Jedná se spíše jen o **indikátory stavu**, jejichž diskrétní hodnoty mají často odpovídající barevnou interpretaci.
    - **zelená** - v pořádku
    - **žlutá** - pozor, vzniká problém (alert)
    - **červená** - problém, je vyžadována okamžitá pozornost.

Ve většině případů tyto metriky nejsou konkrétními veličinami, ale spíše souhrnem více hodnot, indikujícím celkový stav nějakého systému, subsystému nebo aplikace. To předpokládá inteligenci agenta, který nepřetržitě monitoruje jednotlivé veličiny a předává informace na centrální místo v případě vzniku nějaké anomálie.

- **Skupina střední až vyšší úrovně.** V případě, že se vyskytne nějaký problém v systému (např. žlutý alert), potřebujeme větší počet metrik (až 30) na podrobnější prozkoumání označeného systému. Ideou je poskytnout **dostatečný počet metrik pro rozpoznání a pochopení problému a přitom nezahltit management agenta.** Tyto údaje je možné uchovávat pro pozdější analýzu.

- **Skupina detailní úrovně.** Pro vyřešení zbývajících problémových případů musíme použít všechny metriky, které je nám systém schopen poskytnout. Stejně tak použijeme tuto detailní sadu při jemném ladění a optimalizaci systému. Protože **zatížení systému při tomto detailním monitorování může být dosti vysoké, je nutné jej používat jen po nezbytně nutnou dobu.**

Management nástroje by měly umožňovat výběr metrik, které chceme monitorovat, tak abychom měli informace odpovídající úrovně a nezatěžovali zbytečně celý systém.

## ITIL - IT Infrastructure Library

doplnit

## Integrovaná správa IS

Integrovaná správa IS - produkty, pokrývající v jednom, nezávislém a otevřeném řešení všechny potřeby managementu IS - sítí, serverů, klientských stanic, síťových zařízení a aplikací.

Tyto nástroje umožňují správcům systému detekovat aktuální nebo zatím jen potenciální problémy (bez ohledu na jejich původ) a pomáhají určit optimální řešení problémů.

Společnými rysy integrované správy je:

- síťová konzole pro monitorování síťových zařízení (dohledové aplikace – např. OpenView
- síťový a systémový agenti pro monitorování aplikací (např. AVO s centrální konzolí)
- nástroje pro konfigurování a monitorování síťových klientů (např. vzdálené převzetí obrazovky a aplikace pro distribuce SW – např. HP Radia, MS SMS)
- management a administrativní nástroje pro lokální i vzdálené servery (síťová administrace pomocí ActiveDir nebo serverové dohledové aplikace)
- nástroje pro inventarizaci zdrojů a generování reportů (např. Service Desk , Siebel)

# SNMP- Simple Network Management Protocol

SNMP je jednoduchý protokol pro správu sítě. Je to **standard používaný pro správu sítí. Pracuje nad IP protokolem a je založen na modelu agent- manager.**

Síťový manager, vytváří spojení se SNMP agentem, který běží na sledovaném síťovém zařízení. Agent monitoruje stav zařízení a poskytuje o něm informace manageru (např. počet zpracovaných paketů za sec, počet chybových paketů, atd.). Informace, poskytované agentem, jsou uspořádány podle databáze MIB ( Management Information Base ). Ta svojí strukturou odpovídá danému zařízení.

**SNMP je protokolem aplikační vrstvy.** Nejběžnější je **podpora protokolu TCP/IP**. Některá zařízení a správcovské systémy umožňují i přenos po jiných síťových protokolech, např. IPX/SPX.

## Vznik a vývoj SNMP a CMIP

**Protokol SNMP vznikl pro správu směrovačů Internetu.** Vyvinul se jako jedna varianta protokolu SGMP (Simple Gateway Monitoring Protocol), který byl navržen pro výměnu informací mezi směrovači a branami. Druhou variantou protokolu SGMP vytvořenou organizací ISO (www.iso.ch) je protokol CMIP (Common Management Information Protocol). Na počátku byla snaha o společný vývoj obou verzí. Řešení se ale ukázalo nepraktické a další vývoj probíhal nezávisle. Důvodem byla hlavně objektová orientace CMIP na rozdíl od SNMP. CMIP byl pokusem vytvořit standard s podporou protokolů a služeb s definovanou databázovou strukturou pro přenos pomocí protokolu TCP/IP. Pokus nenašel podporu u výrobců ani uživatelů a nedočkal se významnějšího rozšíření.

SNMP protokol prokázal velkou životaschopnost. Relativní jednoduchost implementace jej rychle učinila velice populárním, protože přesně splňoval požadavky na vzrůstající potřeby síťového správy. **Od roku 1989 se stal standardem pro správu sítí založených na protokolu TCP/IP.**

Má tři verze: druhá obsahuje autentizaci a třetí šifrování. Nejvíce zařízení podporuje druhou verzi.

- SNMPv1 (1988) - autentizace pomocí nešifrovanáho řetězce
- SNMPv2 (1993) - zrychlení, zvýšení bezpečnosti, důvernosti a zlepšení komunikace mezi řídícími stroji
- SNMPv3 (1999) - pouze přidání kryptografických prvků

## SNMP protokol

SNMP protokolu se využívá ke správě jednotlivých zařízení připojených zpravidla do TCP/IP sítě. Lze ho využít i v sítích IPX, AppleTalk, OSI a dalších.

Jeho činnost zajišťují 3 části:

- **SMI Structure and Identification of Management.** Definuje podobu přenášených dat.
- **MIB Management Information Base** je databáze s definicí přenášených objektů.
- **SNMP Simple Network Management Protocol** popisuje protokol, kterým probíhá řízení těchto objektů.

Model je klient-manager. Manager může číst a nastavovat hodnoty objektů agenta. Činnost těchto proměnných si můžeme představit jako vlastnosti (property) známé z programovacích jazyků (Java atd.). Tyto objekty jsou popsány v MIB databázi.

**Agent může managera upozornit "nevyžádanou zprávou" (trap),** že došlo k nějaké významné události.

## SMI

Typ dat, které je možno předávat mezi managerem a agentem pomocí SNMP protokolu popisuje **Structure and Identification of Management (SMI)**.

### Primitivní datové typy

K popisu předávaných objektů **používá SMI datový jazyk ASN.1** (Abstract Syntax Notation One) což je jeden ze standardů ISO. Tento jazyk je ale příliš obsáhlý a proto se přistoupilo k jeho zjednodušení. K jediným dovoleným primitivním typům patří:

- INTEGER
- OCTET STRING
- OBJECT IDENTIFIER
- NULL

**INTEGER slouží k předávání číselných hodnot**, ale není definován jako typ s pevnou délkou, což umožňuje různým aplikacím stanovit si jeho rozsah dle svých možností.

**OCTET STRING přenáší binární řetězce** (objekty s binárními daty). Dále byl zaveden typ DisplayString pro textové řetězce. Některé realizace nemusí podporovat řetězce delší než 255 znaků.

**OBJECT IDENTIFIER určuje jednoznačné jméno objektu.** Vytváří se hierarchicky průchodem stromu, do něhož jsou všechny objekty mapovány. Libovolný uzel ve stromu má své jméno, složené z textového popisu a celého čísla (mimo kořene, který je bezejmenný). Je to posloupnost celočíselných hodnot oddělených tečkou, popisujících cestu od kořene stromu až k danému objektu.

### Příklad

Identifikátor proměnné s popisem sledovaného zařízení:

.1.3.6.1.2.1.1.1.0

Posloupnost čísel označuje pojmenování proměnné sysDescr a v textovém popisu vyjadřuje

.iso(1).org(3).dot(6).Internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1).

NULL lze využít k označení objektu bez jakékoliv informace.

Výčtový typ se nahrazuje použitím typu INTEGER, přičemž se v seznamu výčtových hodnot nesmí objevit nula.

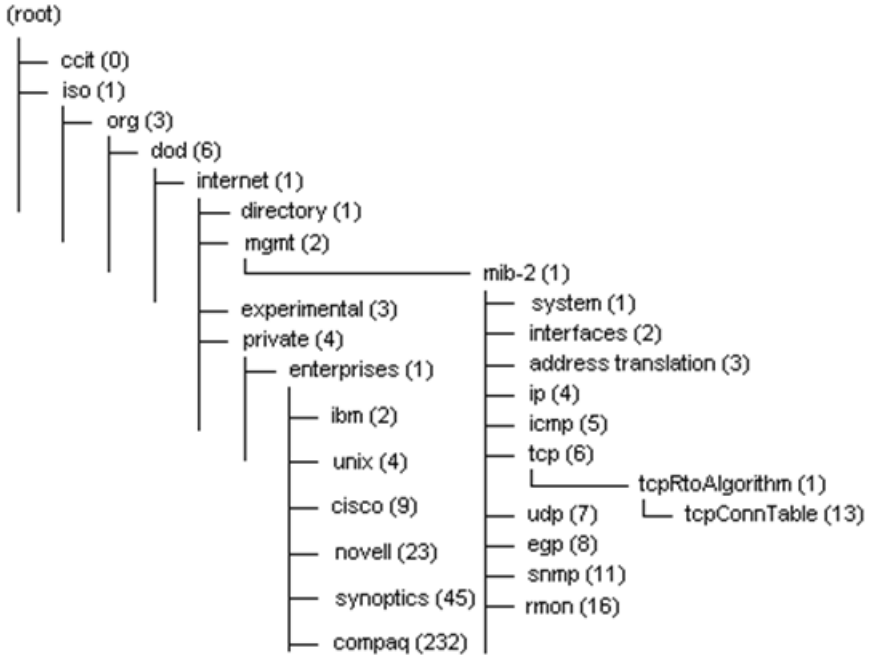
## MIB (Management Information Base)

**Management Information Base (MIB) popisuje sadu objektů, které jsou předmětem správy.** Spravované zařízení může implementovat jednu nebo více MIB, v závislosti na jeho funkci. Tyto MIB databáze jsou velmi podobné standardním databázím v tom smyslu, že popisují jak strukturu, tak formát dat.

MIB jsou napsány podle pravidel Structure of Management Information (SMI) a rozděleny do pěti oblastí dle OSI Management Framework (viz. model správy):

- Správa výkonu- performance management
- Správa konfigurace- configuration management
- Účetní a evidenční správa - accounting management
- Správa poruch a chyb - fault management
- Správa bezpečnosti- security management

MIB je datová hierarchická stromová struktura, která odpovídá danému konkrétnímu zařízení a je objektově **orientována jako sada SNMP objektů, relací a operací na/mezi objekty**.



## SNMP Global Naming Tree

**Každý SNMP objekt zařízení musí mít jedinečné jméno, aby se dalo na něj odkazovat při SNMP operacích.** Protože jedno zařízení může obsahovat objekty, definované nezávisle několika různými výrobci, schéma pro pojmenování těchto objektů muselo být navrženo tak, aby nemohlo dojít k záměně - **koncepce hierarchického stromu SNMP Global Naming Tree,** vyvinutého ISO.

**Standardní MIB struktura odpovídá SNMP Global Naming Tree,** který se skládá z objektů

- Root
- Subtree
- Leaf

Každá část stromu má označení složené ze dvou částí - textového popisu a číselného integeru. Kořenový uzel (root) je bez popisu, ale **pod ním jsou přinejmenším tři uzly**:

- **iso(1)** - spravován organizací ISO
- **ccitt(0)** - spravován organizací ITU-T (bývalé CCITT)
- **joint-iso-ccitt(2)** - společně spravováno ISO a ITU-T

Jednotlivým výrobcům zařízení jsou přidělovány subtree - jsou jmenováni jeho výkonnými autoritami - a mohou si tak vytvářet do šířky a hloubky neomezenou vlastní strukturu. Takto vzniklé privátní (proprietary) MIB popisují vlastnosti konkrétního zařízení. Většinou jsou výrobci zveřejňovány, právě z důvodu umožnění správy těchto prvků i aplikacemi jiných výrobců.

Jméno uzlu ( OBJECT IDENTIFIER) je tak tvořeno sekvencí těchto číselných integerů na cestě z root přes subtree až k danému objektu typu leaf. Tato decimální notace reprezentuje tedy cestu ke každé z funkcí nebo schopností daného zařízení. **Jde o podobný systém jako při specifikacích plných cest k souborům v systémech UNIX a WIN.** Textový popis slouží jen k naší snadnější orientaci v této struktuře.

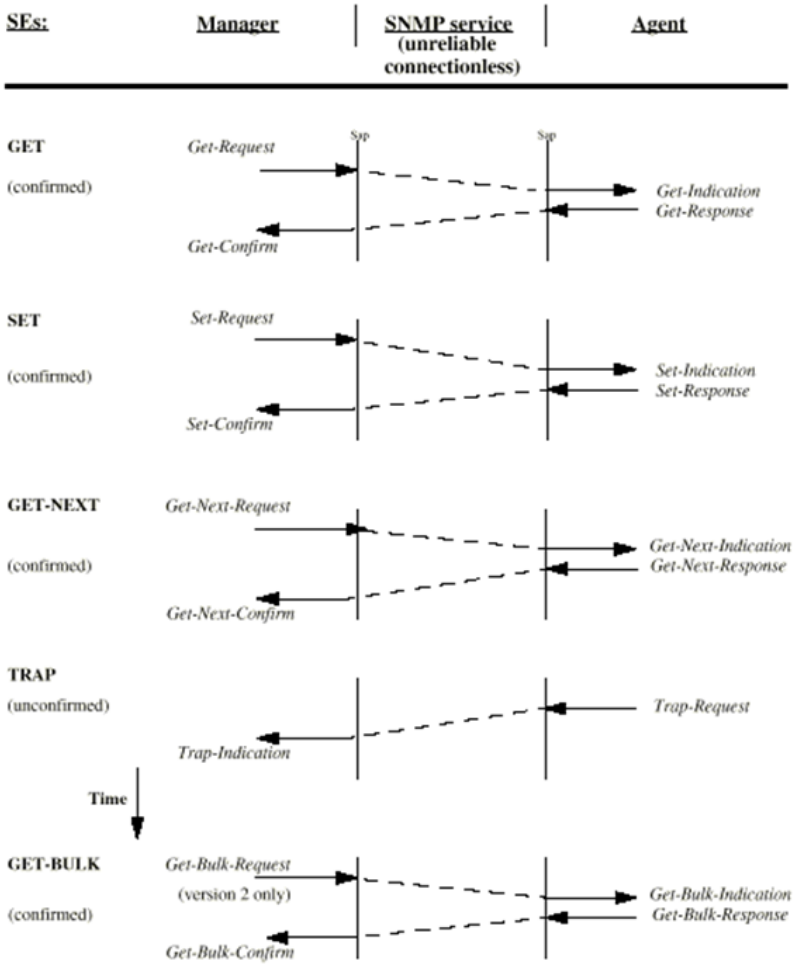
Ve větvi internet(1) jsou vytvořeny tři logické skupiny:

- **Management Branch** - ty standardní MIB, které byly vytvořeny orgánem IETF (www.ietf.org), jsou umístěny v části (... internet(1)mgmt(2)) hierarchické struktury MIB a obsahují definované objekty pro některé běžné síťové zařízení a protokoly. Tuto skupinu podporují zařízení většiny výrobců a tak umožňují jejich nezávislou správu.
- **Experimental Branch** - tato větev zahrnuje MIB, které jsou zatím ve vývoji.
- **Private Branch** - privátní MIB jednotlivých výrobců jsou lokalizovány v části (iso(1)org(3)dod(6)internet(1)private(4)enterprises(1)). Tato větev tak umožňuje jednotlivým výrobcům vytvářet MIB pro svá vlastní zařízení, jimž nedostačují standardní MIB. Tak např. object identifier 1.3.6.1.4.1.45 reprezentuje cestu k objektům firmy SynOptics, 1.3.6.1.4.1.23 cestu k objektům Novell, 1.3.6.1.4.1.9 cestu k objektům Cisco, atd.

# SNMP Simple Network Management Protocol

**SNMP je asynchronní protokol typu požadavek/odpověď.** SNMP v1 definuje služby GET, SET, GET-NEXT and TRAP. SNMP v2 přidává GET-BULK a **INFORM (umožňuje komunikaci dvou managerů mezi sebou).**

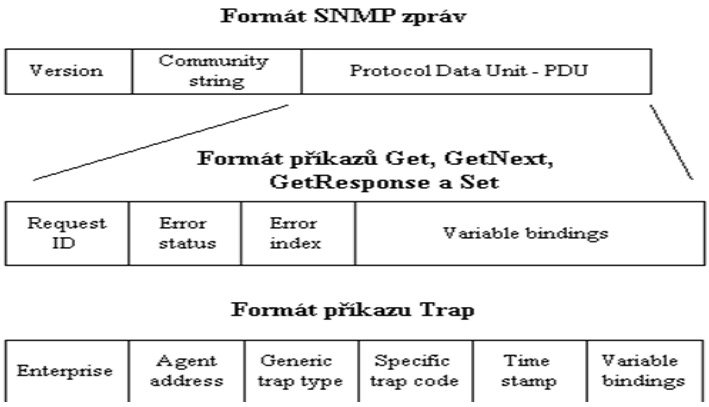
- **GET** - slouží pro čtení jedné nebo více hodnot objektů z MIB.
- **SET** - slouží pro zápis jedné nebo více hodnot objektů v MIB.
- **GET-NEXT** - slouží pro sekvenční čtení hodnot z MIB (např. po přečtení prvního řádku tabulky pomocí GET, lze zbytek tabulky přečíst pomocí GET-NEXT).
- **TRAP** - vysílá agent jako oznámení o významné události (jako např. výpadek proudu, větráku, překročení mezních údajů, objevení nového zařízení).
- **GET-BULK** - slouží pro získání velkého množství informací najednou (např. celé tabulky) místo použití GET a GET-NEXT.



## Formát SNMP zpráv

**SNMP zpráva sestává ze dvou částí**

- **Hlavička zprávy** - obsahuje číslo verze protokolu a tzv. Community String (funguje jako kombinace uživatelského jména a hesla – zadává se při prvním nastavení obou stran, více v části bezpečnost přístupu).
- **PDU (Protocol Data Unit) -** obsahuje jeden ze SNMP příkazů a příslušný operand (položku objektu, která je předmětem transakce). Všechny pole mohou mít proměnnou délku.




Jednotlivá pole mají následující význam:

- **Request ID** - přiřazuje požadavky s odpověďmi.
- **Error status** - určuje, zda požadavek uspěl - indikuje chybu a její typ (pouze odpovědi nastavují tuto položku).
- **Error index** - přiřazuje chybu dané proměnné z pole variable bindings (pouze odpovědi nastavují tuto položku).
- **Variable bindings** - obsahuje vlastní data SNMP PDU, přiřazuje daným proměnným jejich aktuální hodnoty (proměnná:hodnota).

SNMP PDU typu trap se liší a obsahuje tyto pole:

- **Enterprise** - identifikuje typ objektu, který vygeneroval trap.
- **Agent address** - je adresa objektu, který vygeneroval trap.
- **Generic trap type, Specific trap code** - identifikují typ a kód trapu.
- **Time stamp** - čas mezi poslední reinicializací sítě a vygenerováním trapu.
- **Variable bindings** - seznam proměnných, které obsahují relevantní informace k danému trapu.

SNMP v2 PDU typu GetBulk obsahuje:

- **PDU type** - určuje typ PDU - GetBulk.
- **Request ID** - přiřazuje požadavky s odpověďmi.
- **Non repeaters** - určuje počet objektů v listu proměnných(variable bindings), které se neopakují.
- **Max repetitions** - počet opakujících se řádků v tabulce proměnných.
- **Variable bindings** - list proměnných.

## Bezpečnost přístupu

**Součástí SNMP komunikace je zabezpečení přístupu k objektům.** Jedná se o definování přístupových práv k jednomu SNMP Agentu z různých SNMP Managerů. Každý příkaz obsahuje v sobě i tzv. **Community String,** který funguje jako kombinace uživatelského jména a hesla. Správce zařízení definuje jeden Community String pro read-write přístup k objektům uvnitř zařízení a druhý Community String pro pouze omezený read-only přístup. Jestliže Community String obsažený v SNMP příkazu souhlasí s jedním nebo druhým, definovaným pro zařízení, přístup k zařízení je umožněn s odpovídající úrovní přístupu. Nesouhlasí-li, požadavek je odmítnut.

Nejpoužívanější "default" Community String u SNMP zařízení je "public" pro read-only přístup a "private" pro read-write přístup. Je třeba jen dávat pozor na to, že tyto hesla rozlišují velká a malá písmena, což je trochu nezvyklé.

Struktura činností v rámci SNMP: