

Y36SPS

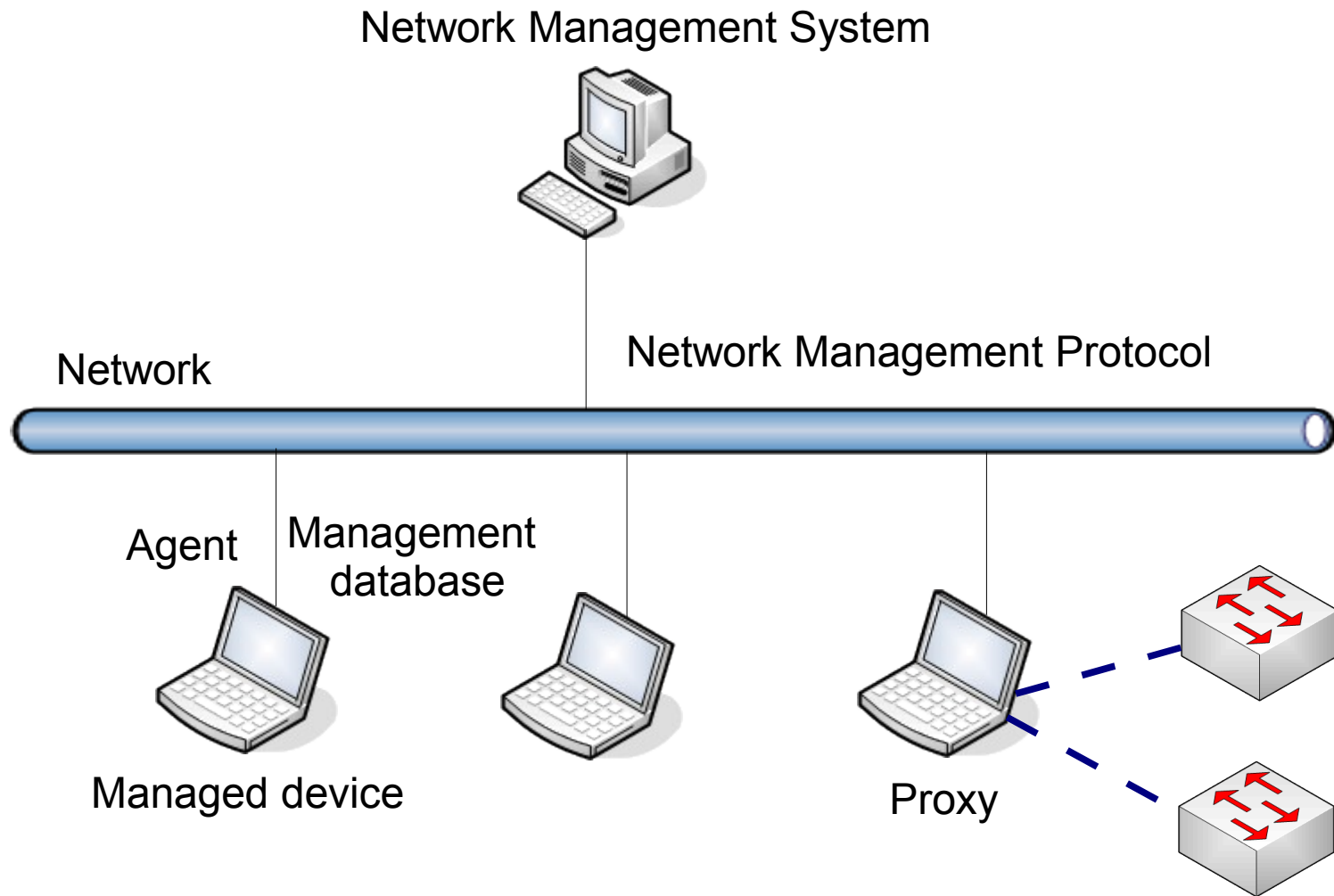
Správa síťových prvků protokoly



Sít'ová správa podle ISO

- správa výkonu (performance management)
 - reaktivní a proaktivní
 - měření výkonnosti a zatížení
- správa konfigurace (configuration management)
 - monitorování síťové konfigurace
- účetní správa (accounting management)
 - monitorování využití sítě
- správa poruch a chyb (fault management)
 - detekce chyb, logování a oznámení
- správa bezpečnosti (security management)
 - nastavení a monitorování přístupu

Architektura



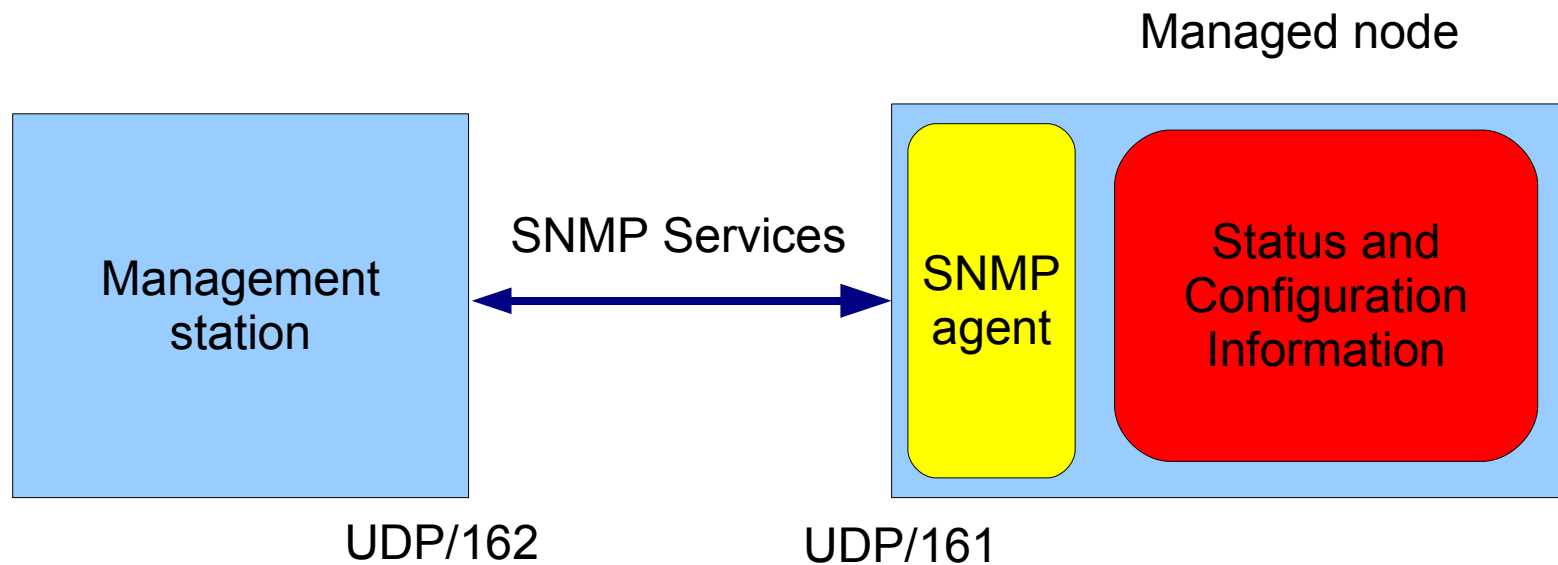
Protokoly

- Simple Network Management Protocol (SNMP)
- Remote Network Monitoring (RMON)
- Common Management Information Protocol (CMIP)
- Web-Based Enterprise Management (WBEM)
- Windows Management Instrumentation (WMI)
- Desktop Management Interface (DMI)
- Common Information Model (CIM)

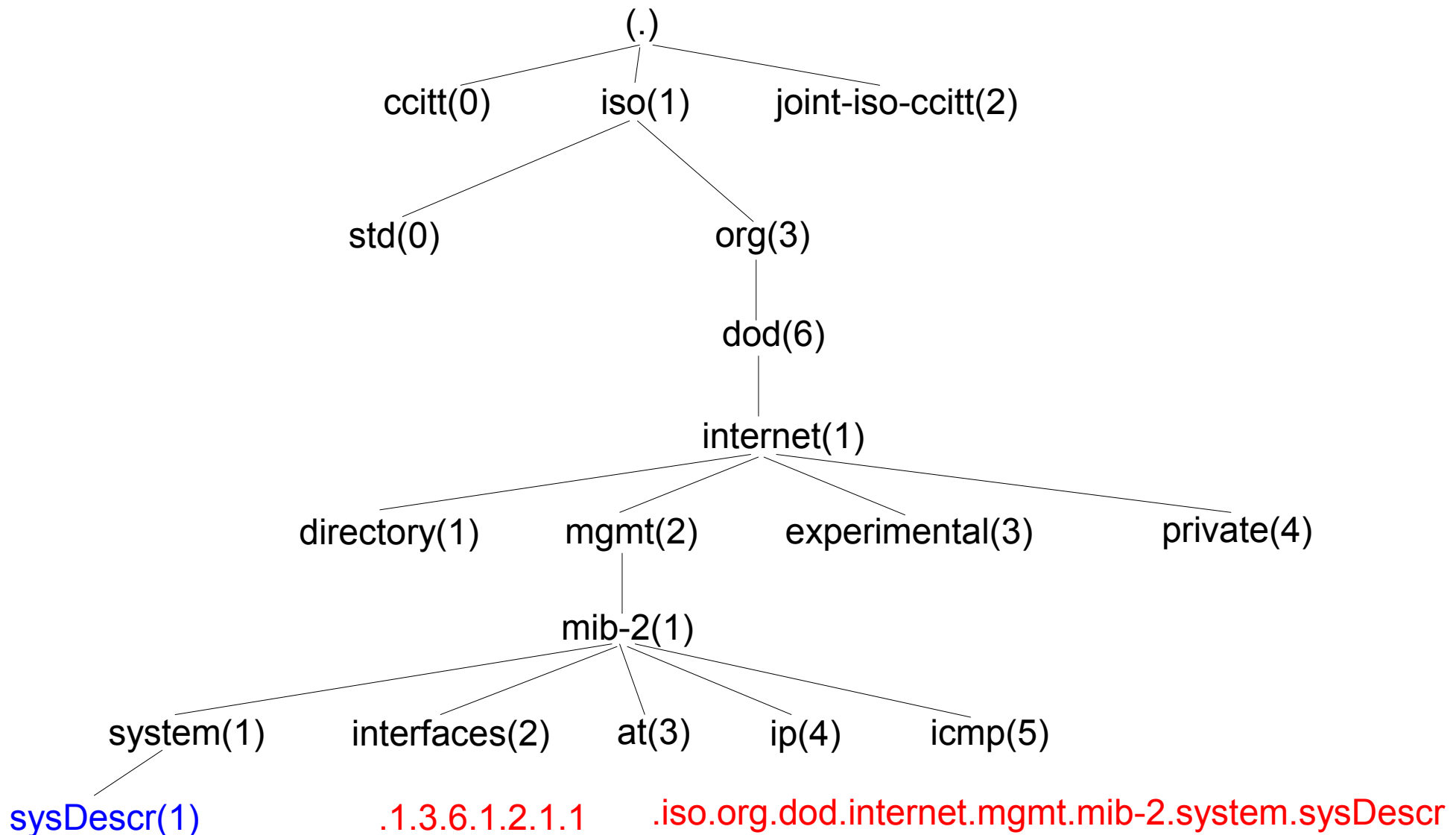
Network management protocol - SNMP

- Simple Network Management Protocol
- SNMPv1 – 1988
 - rfc1157
- SNMPv2 – 1993
 - rfc1441
 - rozšířená bezpečnost
 - další operace
- SNMPv2c – 1996
 - rfc1901
- SNMPv3 – 2002
 - rfc3411

SNMP model



Management Information Base



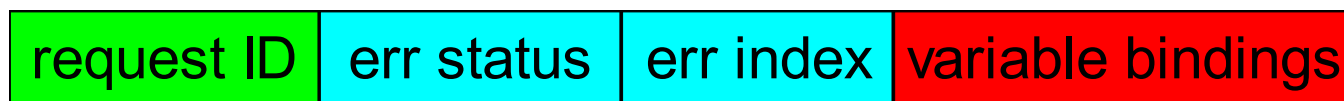
SNMP services

- snmpset
 - snmpget
 - snmpgetnext
 - snmpgetbulk – v2
 - trap
 - inform – v2
-
- skalární a tabulkové hodnoty – instance

SNMP



get, getnext
getresponse, set



trap



Bezpečnost SNMP

| verze | úroveň | způsob autentizace | šifrování | popis |
|-------|--------------|--------------------|-----------|---|
| v1 | noAuthNoPriv | Community String | ne | shoda community string |
| v2c | noAuthNoPriv | Community String | ne | shoda community string |
| v3 | noAuthNoPriv | Username | ne | shoda username |
| v3 | AuthNoPriv | MD5, SHA | ne | autentizace pomocí HMAC-MD5, HMAC-SHA |
| v3 | AuthPriv | MD5, SHA | ano | autentizace pomocí HMAC-MD5, HMAC-SHA; šifrování pomocí DES 56b |

- možnost omezení
 - přístupu do podstromu
 - čtení zápis
 - IP adresa

SNMP Agent

location: Kdesi v budove.
contact: Jan Kubr
sys-descr: HP-UX testsys

get-community-name: globalget
default-mibVIEW: system
get-community-name: sysget IP: 15.2.2.1 15.2.2.3
set-community-name: sysset IP: 15.2.2.1

default-mibVIEW

get-community-name: monitor IP: 15.3.2.1 15.4.23.1 VIEW: system \
interfaces at ip snmp

get-community-name: public IP: 0.0.0.0 VIEW: system
set-community-name: admin IP: 15.3.2.1 15.4.23.1 VIEW: internet -private
set-community-name: root IP: 15.3.2.1 VIEW: internet

trap-dest: 15.2.1.45 trap-dest: 15.3.2.1 trap-dest: 15.4.23.1

Define MIB - ASN.1

```
RFC1213-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    mgmt, NetworkAddress, IpAddress, Counter, Gauge,  
        TimeTicks
```

```
    FROM RFC1155-SMI
```

```
OBJECT-TYPE
```

```
    FROM RFC-1212;
```

```
-- This MIB module uses the extended OBJECT-TYPE macro as defined in [14];
```

```
-- MIB-II (same prefix as MIB-I)
```

```
mib-2    OBJECT IDENTIFIER ::= { mgmt 1 }
```

```
DisplayString ::=
```

```
    OCTET STRING
```

```
-- This data type is used to model textual information taken from the NVT ASCII
```

```
-- character set. By convention, objects with this syntax are declared as having SIZE (0..255)
```

```
PhysAddress ::=
```

```
    OCTET STRING
```

```
-- This data type is used to model media addresses. For many types of media, this will
```

```
-- be in a binary representation. For example, an ethernet address would be represented
```

```
-- as a string of 6 octets.
```

Definice MIB - ASN.1

-- groups in MIB-II

```
system      OBJECT IDENTIFIER ::= { mib-2 1 }
interfaces  OBJECT IDENTIFIER ::= { mib-2 2 }
at          OBJECT IDENTIFIER ::= { mib-2 3 }
ip          OBJECT IDENTIFIER ::= { mib-2 4 }
icmp       OBJECT IDENTIFIER ::= { mib-2 5 }
tcp        OBJECT IDENTIFIER ::= { mib-2 6 }
udp        OBJECT IDENTIFIER ::= { mib-2 7 }
egp        OBJECT IDENTIFIER ::= { mib-2 8 }
```

-- historical (some say hysterical)

```
-- cmot     OBJECT IDENTIFIER ::= { mib-2 9 }
```

```
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
```

```
snmp       OBJECT IDENTIFIER ::= { mib-2 11 }
```

Definice MIB - ASN.1

sysObjectID OBJECT-TYPE

SYNTAX OBJECT IDENTIFIER

ACCESS read-only

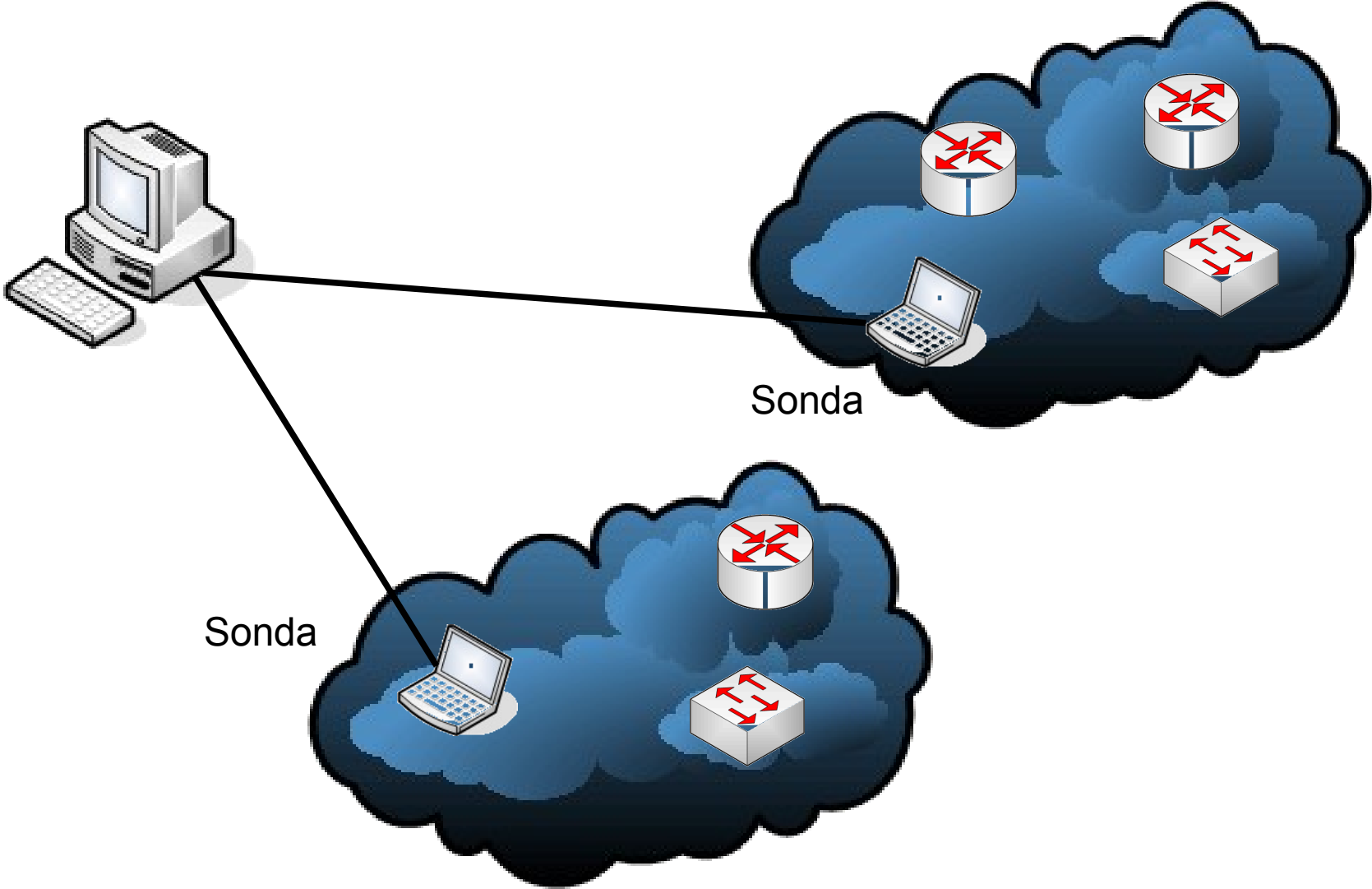
STATUS mandatory

DESCRIPTION

"The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router'."

::= { system 2 }

RMON



RMON

- vzdálený sběr informací o provozu pomocí sond
- nasbíraná data se přenáší pomocí SNMP
- monitorování toků
- RMON1
 - rfc2819
- RMON2
 - rfc2021

RMON1 skupiny

- rfc2819
- Statistic – okamžitý provoz (byte, kolize, chyby ...)
- History – dtto, ale historie
- Alarms – prahování měřených hodnot
- Hosts – přenosová statistika pro každý uzel
- Host Top N – setříděná předchozí statistika
- Traffic Matrix – vzájemná komunikace mezi uzly
- Filters – filtry pro následující skupinu
- Packet Capture – pakety pro další dekódování
- Events – záznamy událostí
- Token Ring – rozšíření pro Token Ring

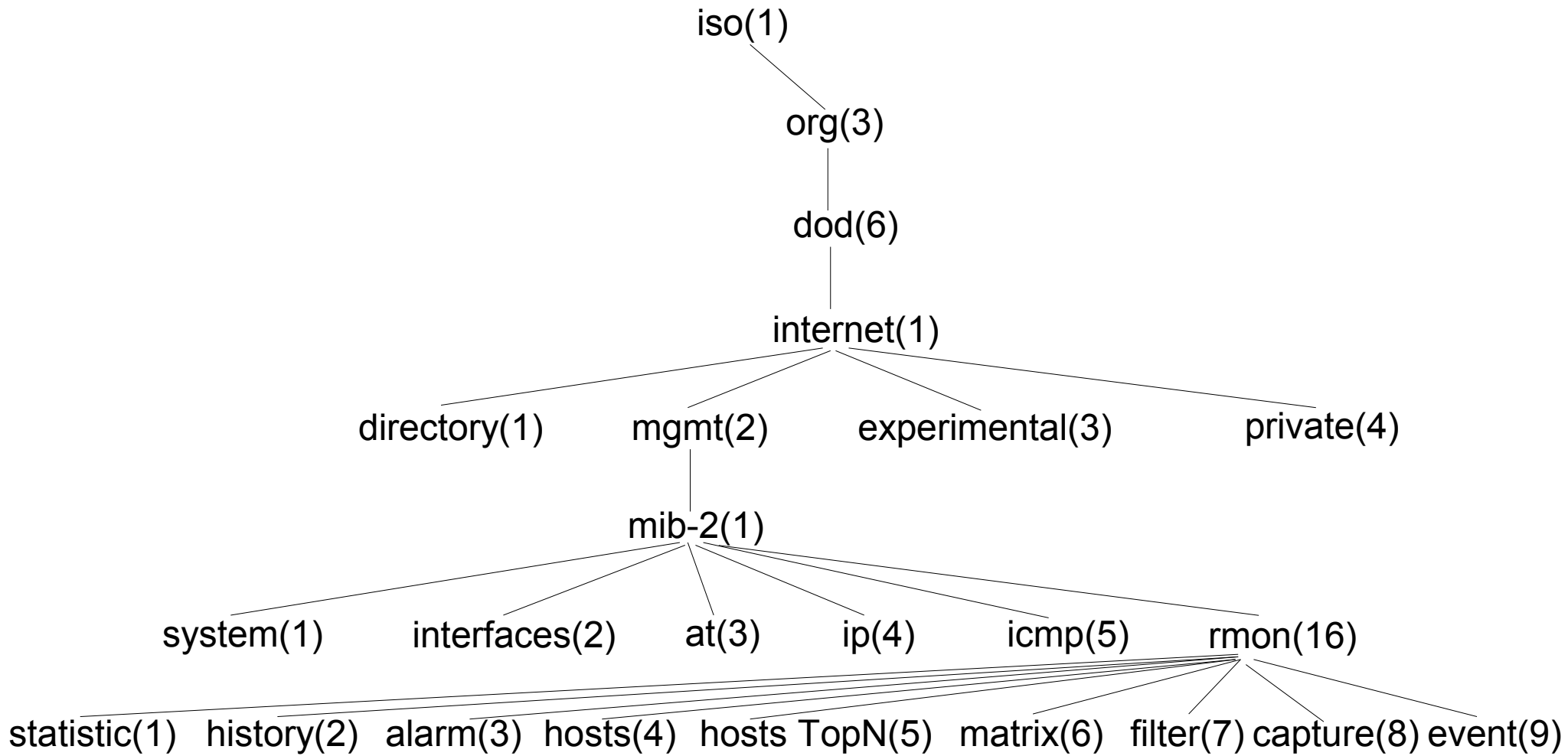
RMON2 skupiny

- rfc2021
- Protocol Directory – monitorovatelné protokoly
- Protocol Distribution – statistiky pro protokol
- Address Map – mapování IP-MAC adres
- Network-Layer Host – net statistiky pro uzly
- Network-Layer Matrix – net statistiky pro dvojice uzlů
- Application-Layer Host – appl statistiky pro uzly
- Application-Layer Matrix – appl statistiky pro dvojice uzlů

RMON2 skupiny

- User History – pravidelné vzorky uživatelsky definovaných proměnných
- Probe Configuration – vzdálená konfigurace sondy
- RMON Conformance – požadavky pro souhlas s RMON2

RMON MIB



Problémy RMON

- RMON zařízení nemusí implementovat všechny skupiny ale má podporu RMON
 - důkladné prostudování popisu zařízení
- výkonnost procesoru při monitorování více skupin
- velikost paměti pro ukládání vzorků

Common Management Information Protocol (CMIP)

- definován v ISO/OSI modelu správy
- používá ISO/OSI komunikační protokoly
- CMIP over TCP/IP – CMOT
 - rfc1189
- oproti SNMP umí spouštět akce
- oproti SNMP lepší bezpečnost
- datový model založen na objektech
- příliš složitý

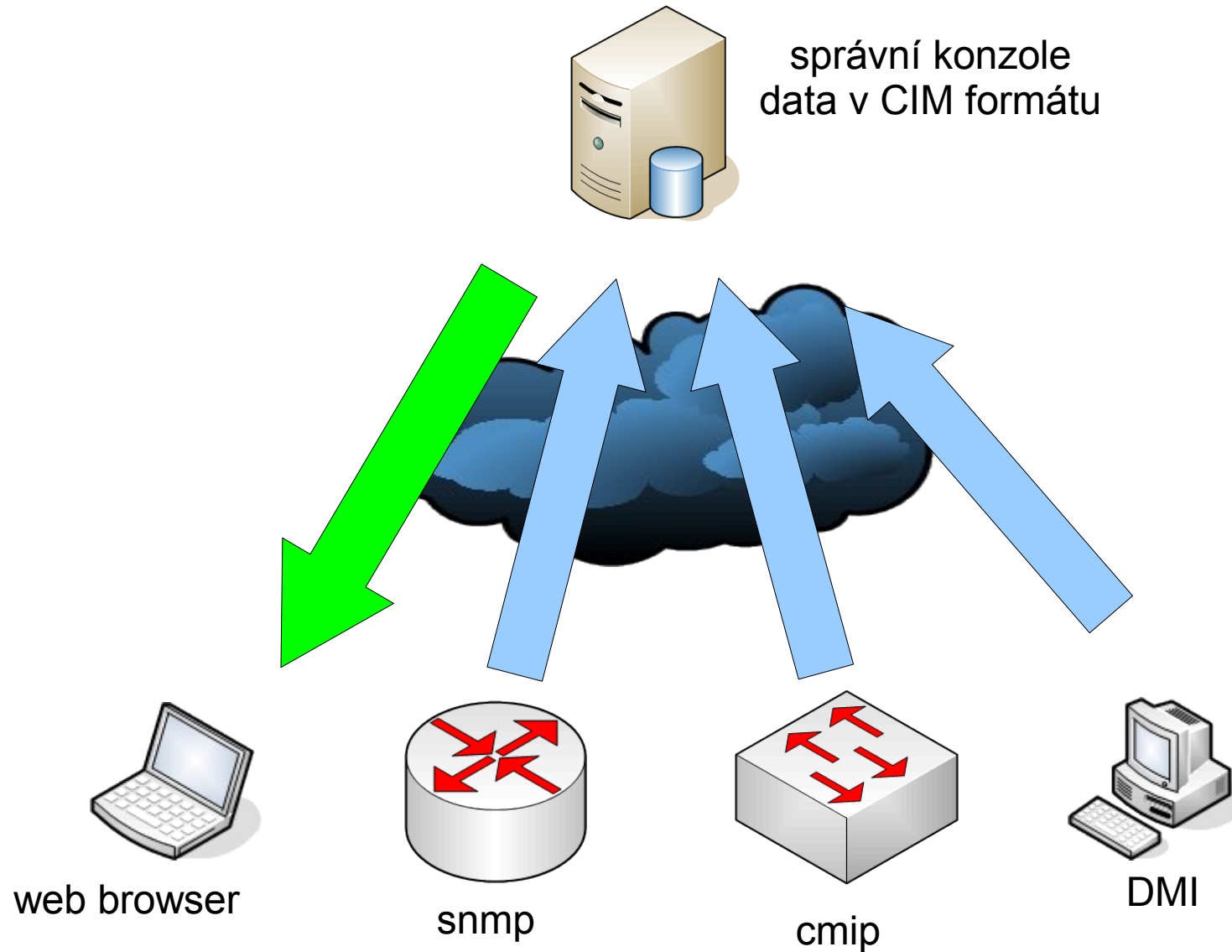
Desktop Management Interface (DMI)

- standard pro správu pracovních stanic
- DMTF ukončilo podporu k 31.3.2005
- <http://www.dmtf.org/standards/dmi/>
- MIF – management information format
 - obdoba SNMP MIB

Web-Based Enterprise Management (WBEM)

- CIM schema
- xmlCIM
- CIM over http
- www.dmtf.org/wbem/

WBEM



Windows Management Instrumentation (WMI)

- MS implementace WBEM
- jednotné rozhraní pro získávání informací o systému
- [http://msdn2.microsoft.com/en-us/library/aa394582\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa394582(VS.85).aspx)

Literatura

- MIB-II
 - rfc1213
- SNMPv3
 - http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html
- DMI
 - <http://www.dmtf.org/standards/dmi/>
 - <http://pc.toshiba-asia.com/product/doc/dmi.pdf>
- WBEM
 - <http://www.dmtf.org/wbem/>
 - <http://openwbem.sourceforge.net/>
-

DMI
WebManagement
formát SNMP paketů
SNMPv3 bezpečnost

...