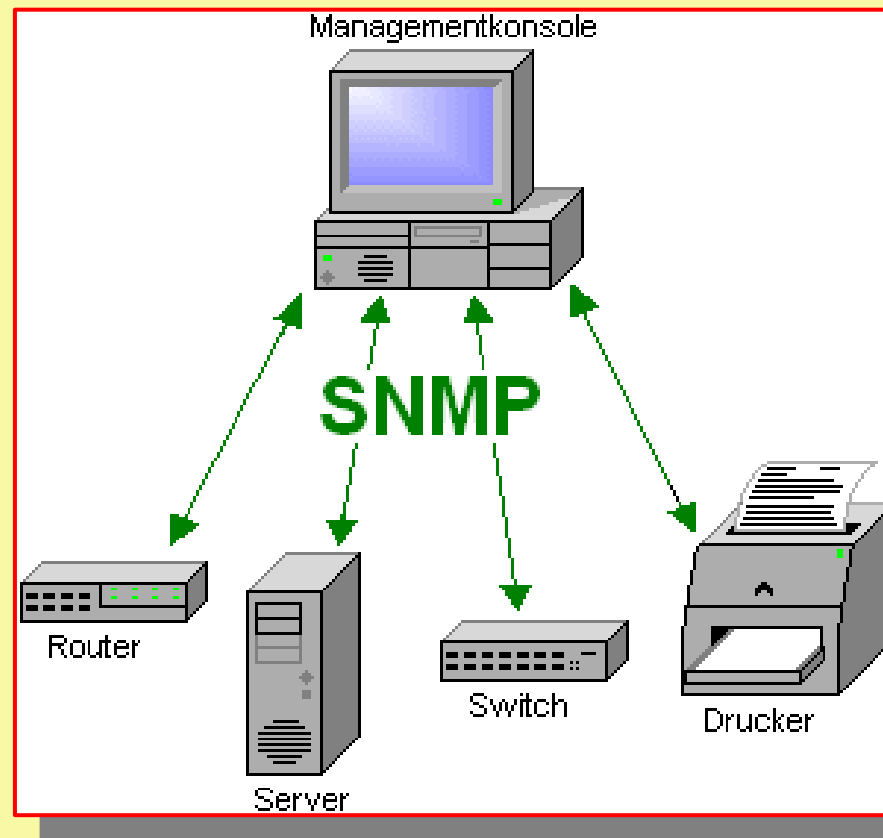


SNMP



Forrás:

<http://szabilinux.hu/snmp/index.html>

https://hu.wikipedia.org/wiki/Simple_Network_Management_Protocol

<https://wiki.hup.hu/index.php/SNMP>

<http://www.net-snmp.org>

SNMP

- ***Mi az SNMP?***

- Simple Network Management Protocol (SNMP)
 - Egyszerű Hálózat Menedzsment Protokoll
- A 80-as évek közepén fejlesztették ki
- Egyre jelentősebb problémát jelentett a növekvő hálózat menedzselése

- ***Mi az SNMP feladata?***

- Routers, switches, nyomtatók... stb. menedzselése

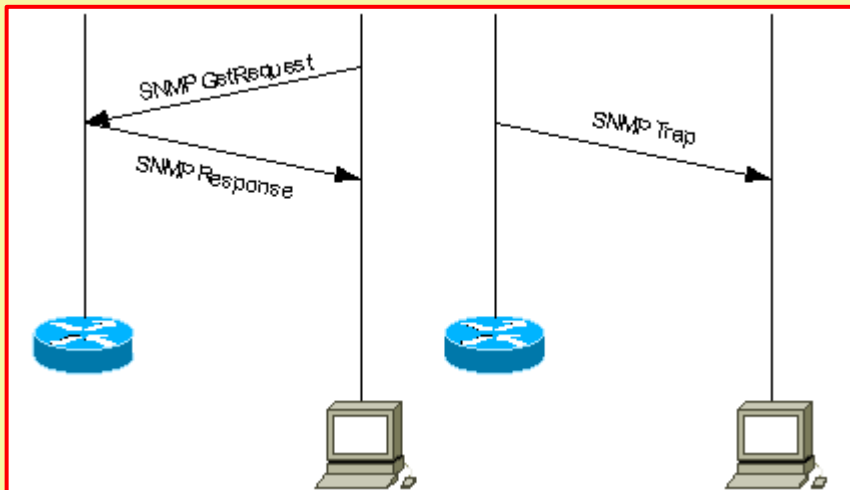
SNMP

- **Az SNMP protokollverziók**
 - SNMPv1 (RFC: 1988)
 - SNMPv2, SNMPv2c, SNMPv2u (RFC: 1993-)
 - SNMPv3 (RFC: 2002)
- Mindegyik verzió az előzőnél jóval fejlettebb biztonsági megoldásokat tartalmaz, értelemszerűen jelenleg a v3 javasolt.

SNMP

- Az SNMP felépítése

- Kliens-szerver architektúra
 - Menedzselt eszközön fut az agent
 - Központi (hálózati) menedzsment rendszer



The screenshot shows the 'SNMP Testing Module' interface. The title bar indicates the module name and IP address: 'SNMP Testing Module - none - 192.168.1.1:161'. The interface includes a toolbar with buttons for 'Run', 'Test', 'Add MIBs', 'Build Test', 'Load Test', 'Save Test', 'Collapse Tests', and 'MIB Info'. Below the toolbar is a table displaying test results for various SNMP objects. The table has columns for Status, Object Name, OID, Index, Value, Test Type, and MIB. The status column uses color coding: red for FAIL, orange for WARNING, and green for PASS. The bottom of the interface shows a summary: 'Tests finished. PASS 650 WARN 1 FAIL 1 SNMP'.

Status	Object Name	OID	Index	Value	Test Type	MIB
FAIL	incomingPortEnd	1.3.6.1.4.1.3955.3.4.1.48.1.6			GETNEXT	LINKSYS-MODEL-MIB
no values returned when trying for next leaf						
WARNING	ipRouteAge	1.3.6.1.2.1.4.21.1.10			SYNTAX_INTEGER	OLD-RFC1213-SUPPL-MIB
PASS	sysDescr	1.3.6.1.2.1.1.1			GETNEXT	SNMPv2-MIB
PASS	sysDescr	1.3.6.1.2.1.1.1			GET	SNMPv2-MIB
PASS	mgmtBootStatus	1.3.6.1.4.1.3955.3.1.4			GET	LINKSYS-MODEL-MIB
PASS	mgmtBootStatus	1.3.6.1.4.1.3955.3.1.4			SYNTAX_INTEGER	LINKSYS-MODEL-MIB
PASS	sysUpTime	1.3.6.1.2.1.1.3			GET	SNMPv2-MIB
PASS	sysObjectID	1.3.6.1.2.1.1.2			GETNEXT	SNMPv2-MIB
PASS	sysUpTime	1.3.6.1.2.1.1.3			SYNTAX_TIMETICKS	SNMPv2-MIB
PASS	sysContact	1.3.6.1.2.1.1.4			SYNTAX_DISPLAYST...	SNMPv2-MIB
PASS	sysContact	1.3.6.1.2.1.1.4			GETNEXT	SNMPv2-MIB
PASS	sysContact	1.3.6.1.2.1.1.4			GET	SNMPv2-MIB
PASS	sysName	1.3.6.1.2.1.1.5			SYNTAX_DISPLAYST...	SNMPv2-MIB
PASS	sysName	1.3.6.1.2.1.1.5			GET	SNMPv2-MIB
PASS	sysName	1.3.6.1.2.1.1.5			GETNEXT	SNMPv2-MIB
PASS	sysLocation	1.3.6.1.2.1.1.6			GET	SNMPv2-MIB
PASS	sysLocation	1.3.6.1.2.1.1.6			GETNEXT	SNMPv2-MIB

SNMP

- **Az SNMP komponensek**

- SNMP topológia három komponensből áll:
 - Menedzselt eszközök (managed/slave device)
 - Eszközökön futó kliens (agent) szoftverek
 - Adatokat gyűjtő monitorozó rendszer (NMS – network monitoring system)
- Milyen portokat használ?
 - 161/UDP (request/response)
 - 162/UDP (trap, notification)

SNMP

- **SNMP üzenettípusok**
 - **GET REQUEST:** egy bizonyos információ lekérése
 - **GETNEXT REQUEST:** a következő információ lekérése: ennek segítségével végig lehet lépkedni az információkon
 - **GET RESPONSE:** a válasz üzenet
 - **SET:** egy objektumnak értékadás (SNMPv1-es protokoll esetében biztonsági megfontolások miatt a legtöbb gyártó kihagyta ezt a protokoll-műveletet)
 - **TRAP:** egy speciális üzenet, akkor jön létre, ha a menedzselt eszközt figyelmeztetés küldésére állították be (például a forgalomszámláló elér egy bizonyos értéket, meghibásodás lépett fel stb.)
 - **GETBULK:** több adat lekérdezése

SNMP

- SNMP csomagformátum

Üzenethossz Byte		SNMP-csomag Header
Verziószám		
Community Name		
Csomagtípus (Get, GetNext, ...)	PDU-fejléc	PDU (Protocol Data Unit)
PDU hossz Byte		
RequestID		
Hibakód		
Hiba-Index	PDU-Body	
PDU törzs hossza Byte		
Variable Binding 1		
Variable Binding 2		
...		
Variable Binding n		

SNMP

- ***SNMP verziók***
 - ***SNMP Version 1***
 - ***Gyenge biztonság***
 - ***Nem titkosított üzenetcsere***
 - ***jelszó helyett pedig a Community stringeket használja***
 - ***így könnyen támadható***

SNMP

- **SNMP verziók**
 - **SNMP Version 2**
 - **Javított biztonság**
 - **Jobb teljesítmény**
 - **GETBULK üzenet létrehozása → több adatot egyszerre lehet lekérdezni, ez sokat javít a v1 hatékonyságán**
 - **Nem annyira elterjedt a vitatott biztonsági javítások miatt**
 - **Több módosítás is készült: v2c, v2u**
 - **A v2c terjedt el**

SNMP

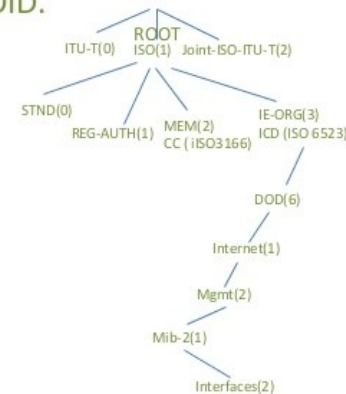
- ***SNMP verziók***
 - ***SNMP Version 3***
 - ***Javított verzió a v2-höz képest***
 - ***SNMP hivatalos szabványa***

SNMP

- Mi a MIB?
 - *Management Information Base*
 - *Menedzsment Információs Bázis*
 - *Fastruktúra-szerű osztályozás*
 - *Bővíthetőre tervezték*

MIB Tree

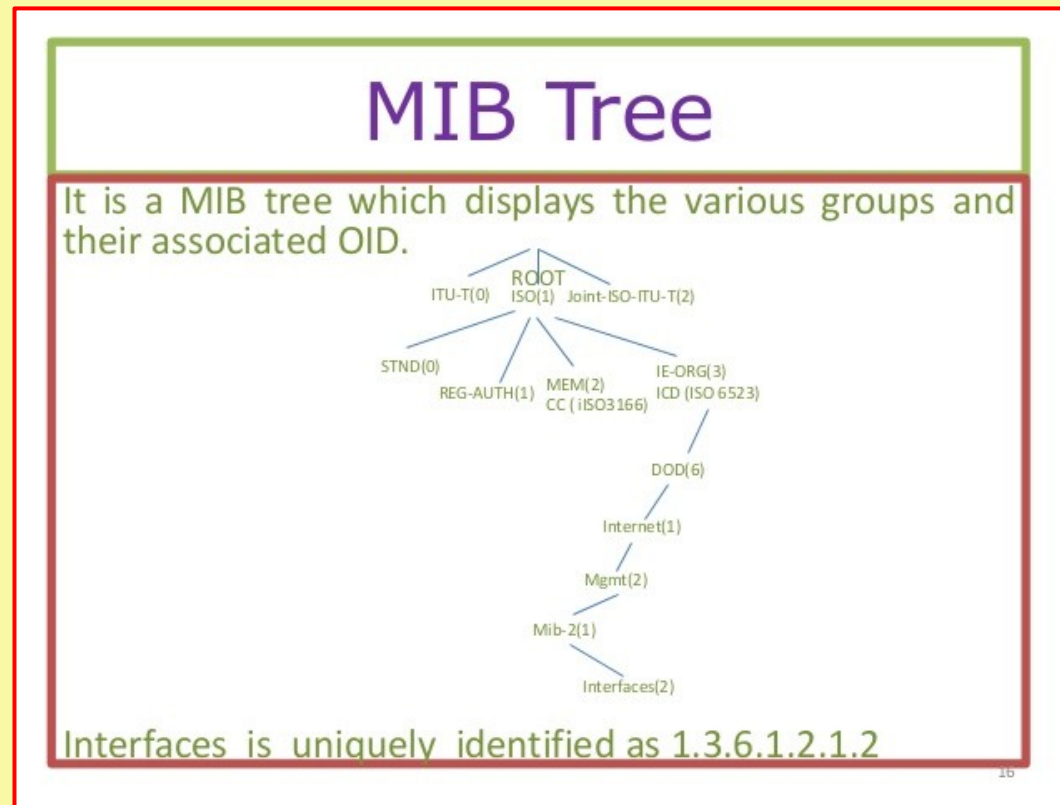
It is a MIB tree which displays the various groups and their associated OID.



Interfaces is uniquely identified as 1.3.6.1.2.1.2

SNMP

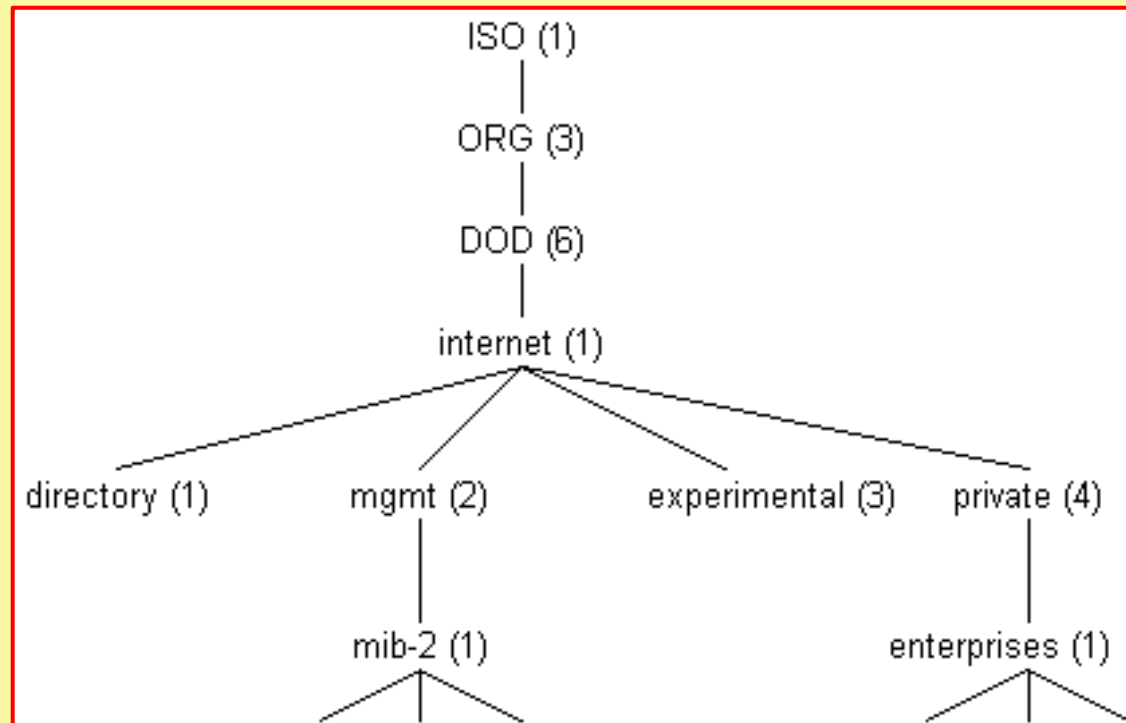
- Mi az OID?
 - OBJECT ID
 - Egy adott paraméter a MIB tree-n belül



SNMP

- A MIB felépítése

- *Abstract Syntax Notation One (ASN.1) alapján történik*



SNMP

- **A MIB felépítése**

- **Objektum definíciója (OBJECT)**

- **OBJECT: objektum neve (szöveges), OBJECT DESCRIPTOR zárja**
- **SYNTAX: objektum típusát határozza meg (pl. INTEGER, OCTET STRING)**
- **ACCESS: hozzáférés jogai (read-only, read-write, write-only, not-accessible)**
- **STATUS: kötelező (mandatory), opcionális (optional), nem használt (obsolete)**

SNMP

- **A MIB felépítése**

- **Objektum példa**

sysUpTime OBJECT-TYPE

SYNTAX TimeTicks

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

::= { system 3 }

SNMP

- ***Az SNMP implementáció***
 - Nyílt forráskódú implementáció: net-snmp
 - Kliens szoftvere: snmpget, snmpwalk
 - SNMP szoftverek:
 - Nagios
 - Icinga
 - Cacti
 - ...stb.

SNMP

Köszönöm a figyelmet!