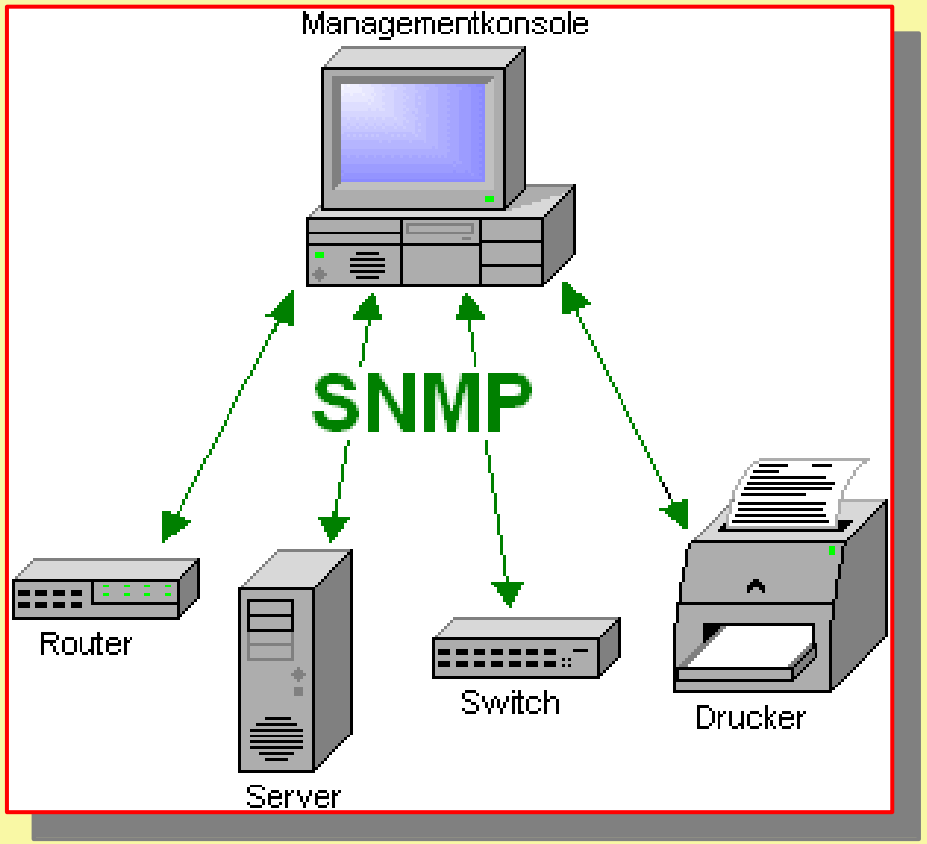
SNMP



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?***
  - Routerek, switche, nyomtatók… stb. menedzselése

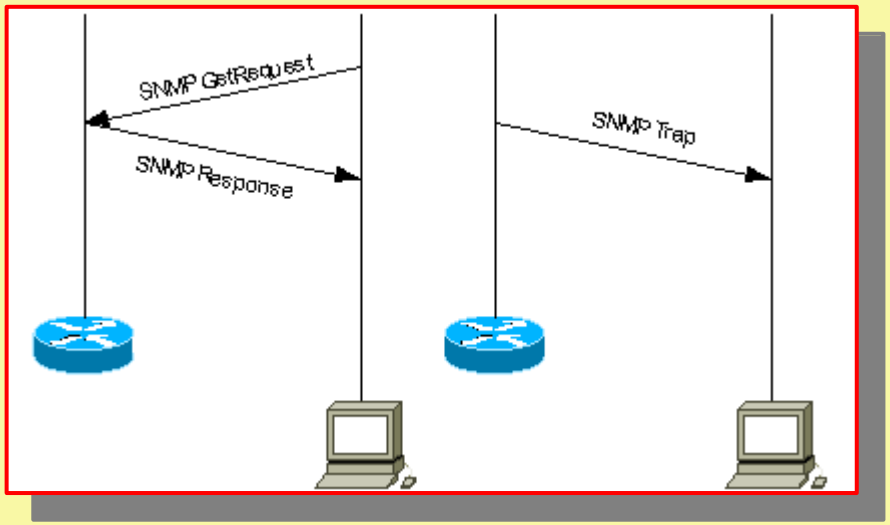
SNMP

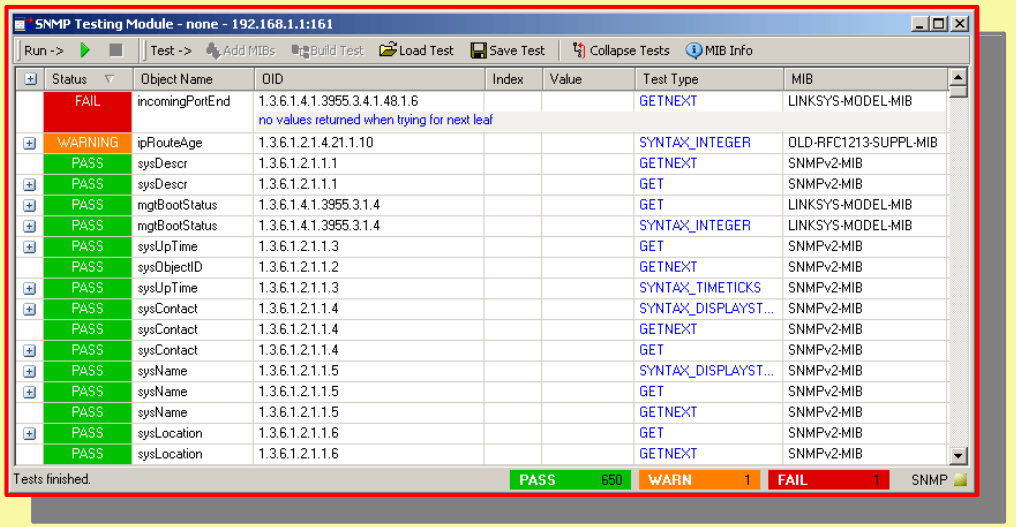
- ***Az SNMP protokollverziók***
  - SNMPv1 (RFC: 1988)
  - SNMPv2, SNMPv2c, SNMPv2u (RFC: 1993-)
  - SNMPv3 (RFC: 2002)

  - 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





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***

SNMP csomag felépítése (nem Trap üzenet esetén)

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 törzs hossza Byte	PDU-Body	
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

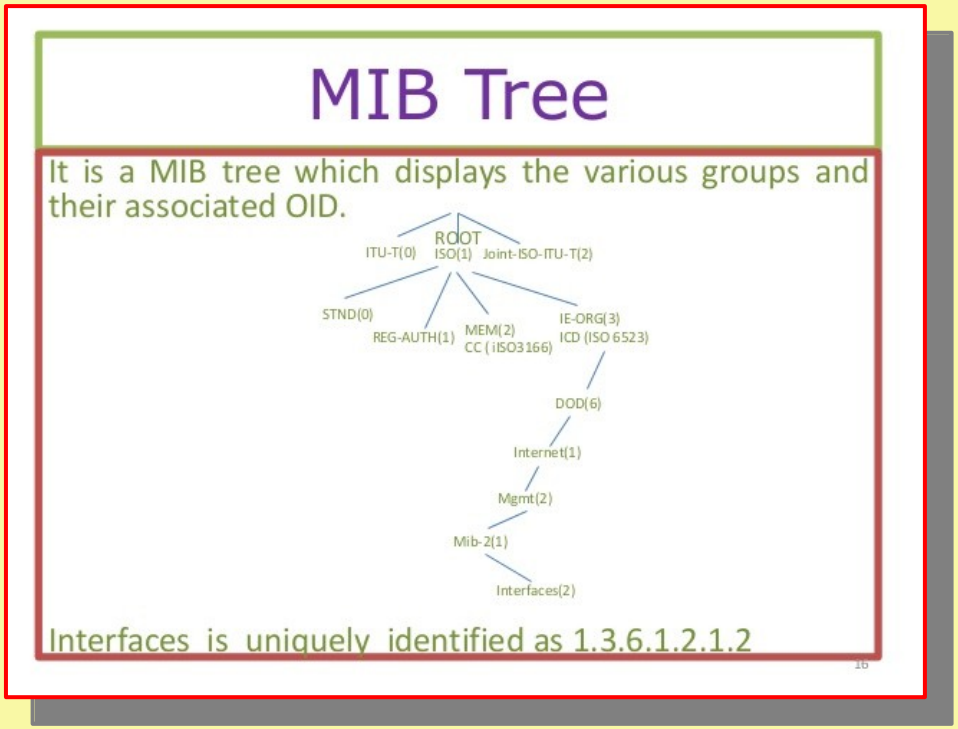
- ***SNMP verziók***
  - ***SNMP Version 2***
    - ***Javított biztonság***
    - ***Jobb teljesítmény***
    - ***GETBULK üzenet létrehozása → több adatot egyszerre lehet lekérdezni, ez sokat javít a v1 hatékonyságán***
    - ***Nem annyira elterjedt a vitatott biztonsági javítások miatt***
      - ***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***

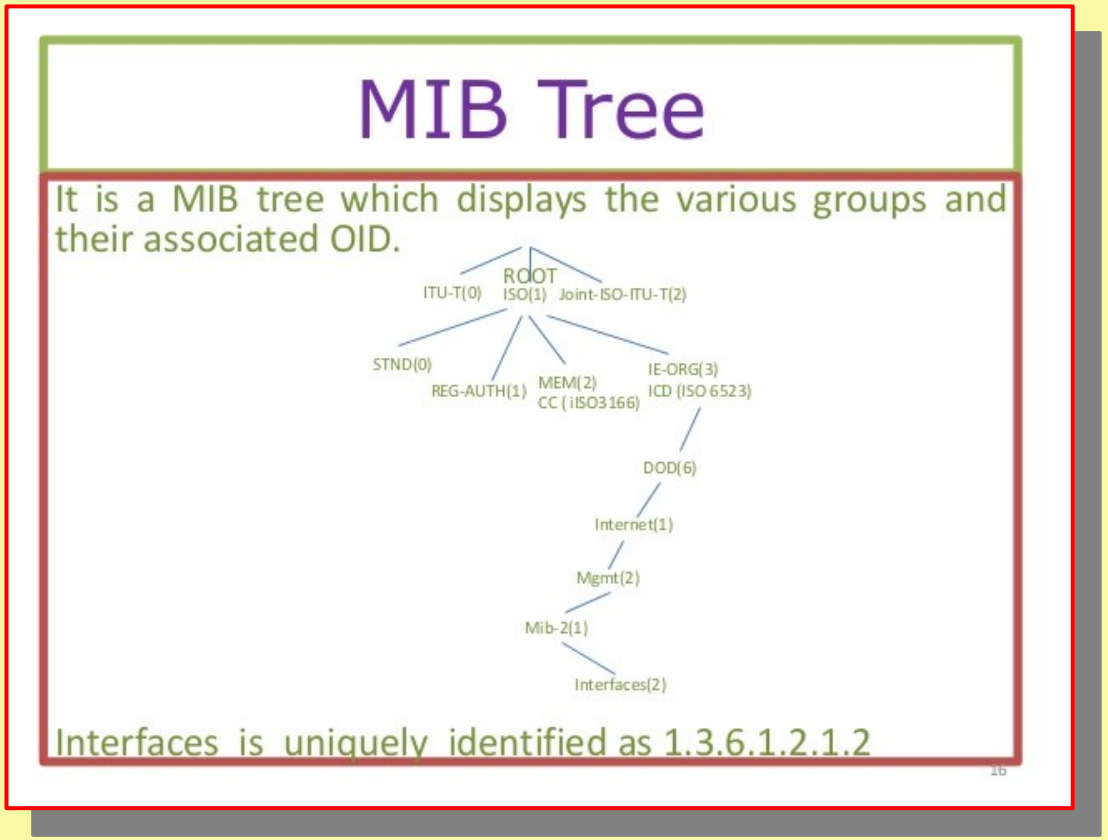
SNMP

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



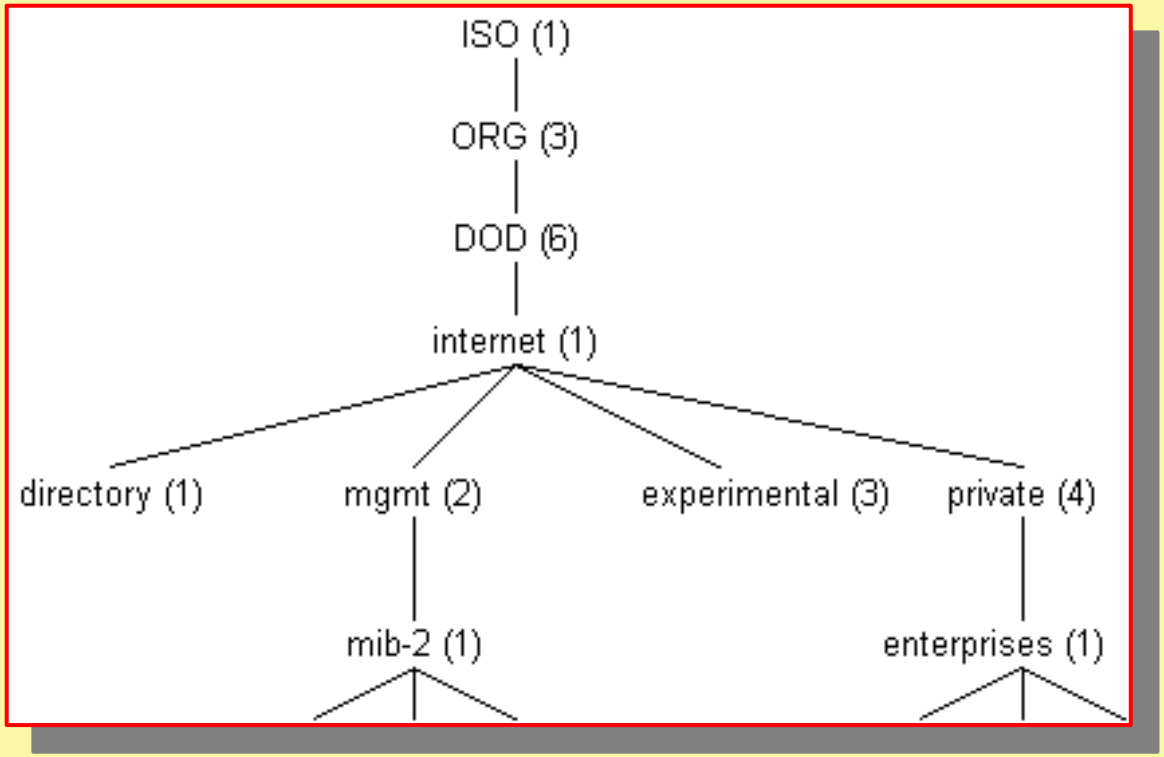
SNMP

- ***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!