Távközlés-
Informatika
Laboratórium

IP alapú kommunikáció

11. Előadás – Hálózat Monitoring/Hálózat Manadgement

Kovács Ákos

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – Mire is kell??

- Mit is kell tudnia egy hálózatmenedzsmentnek?
- Konfiguráció Menedzsment
  - Folyamatosan figyelni, az eszközök beállításait és, hogy funkcionálnak
- Hiba Menedzsment
  - Problémák megoldása, vészhelyzetek elkerülése/kijavítása
- Performancia Menedzsment
  - Milyen a hálózat sebessége? Meg tud-e birkózni a jelenlegi terheléssel, mennyi tartalék van még?

Hálózat menedzsment – Mire is kell?? 2

- Security Menedzsment
  - Esetleges behatolás érzékelés / anomáliák feltárása
- Számlázás Menedzsment
  - Mérhető adatok, esetleges számlázás támogatás
- Leltár Menedzsment
  - Leltár, Inventory
- Tervezés Menedzsment
  - A későbbi bővítéshez szükséges tervezési folyamatok támogatása

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – Alapok

- Minden modern hálózat menedzsment alapja az SNMP
- Simple Network Management Protocol
- Első verzió 1991!!!!
- Az SNMP sztenderdizált megoldás (Routerek/switchek/szerverek) gyakorlatilag bármilyen eszköz monitorozása
- Több verzió is megjelent azóta a legfrissebb a V3

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – SNMP v1

- SNMP v1
  - UDP protokollt használ (UDP 161, 162-es port)
  - Nem IP alapú rendszerekben is használható pl.: IPX, Appletalk,
  - Semmilyen authentikációt nem használ (EZ is volt vele a legnagyobb baj)
  - ÚN. community stringet használ, általában: public (RO), secret (RW)
  - Ezeket plain text-ben küldözgeti a hálózaton
  - Nagy vizió : Nem csak monitorozásra, beavatkozásra is használható
  - Get/set paranccsokkal
  - Egyszerűsége miatt a hibáit VLAN-okkal hidalják át

Hálózat menedzsment – SNMP v1

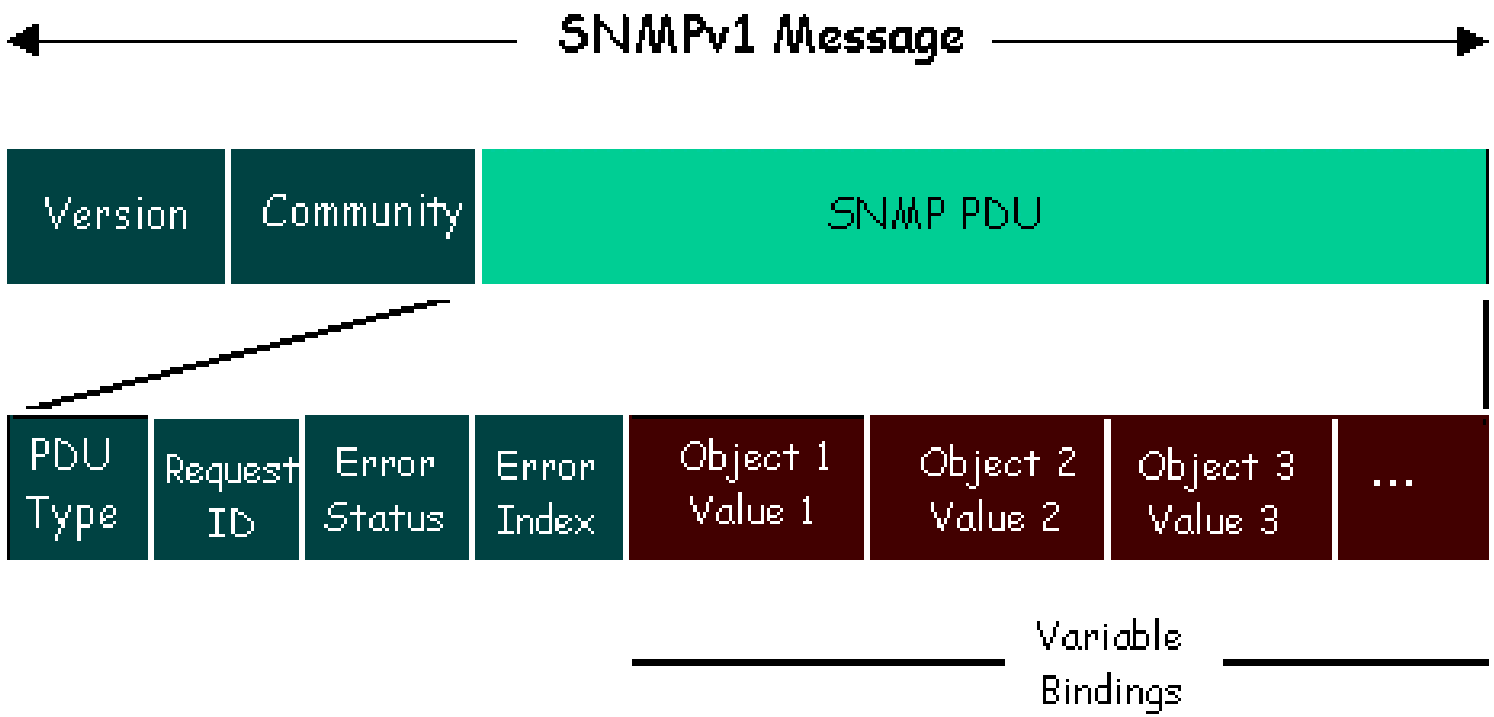


Figure 2: SNMPv1 Message Format

Hálózat menedzsment – SNMP v2

- SNMP v2
  - A v1 újra gondolt verziója
  - Fejődött a sebesség, biztonság
  - Bemutatták a GetBulkRequest üzenetet
  - Nagy mennyiségű adat egyszeri lekérésre
  - Mégsem lett nagy siker
  - Egy Community verzió is született: v2c néven
  - Ez a v2 előnyeit a v1 community rendszerével ötvözve jelenleg is a legelterjedtebb verzió

Hálózat menedzsment – SNMP v3

- SNMP v3
  - Csak kriptográfiai újítások
  - Titkosítás: titkosított üzenetek elolvashatatlanok más számára
  - Integritás védelem: CRC ellenőrzéssel biztosított, hogy a csomag nem változatlanul halad át a hálózaton
  - Authentikáció: biztosított a küldő kiléte
  - Minden egyes eszközhöz hozhatunk létre felhasználónév/jelszó párost

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – SNMP

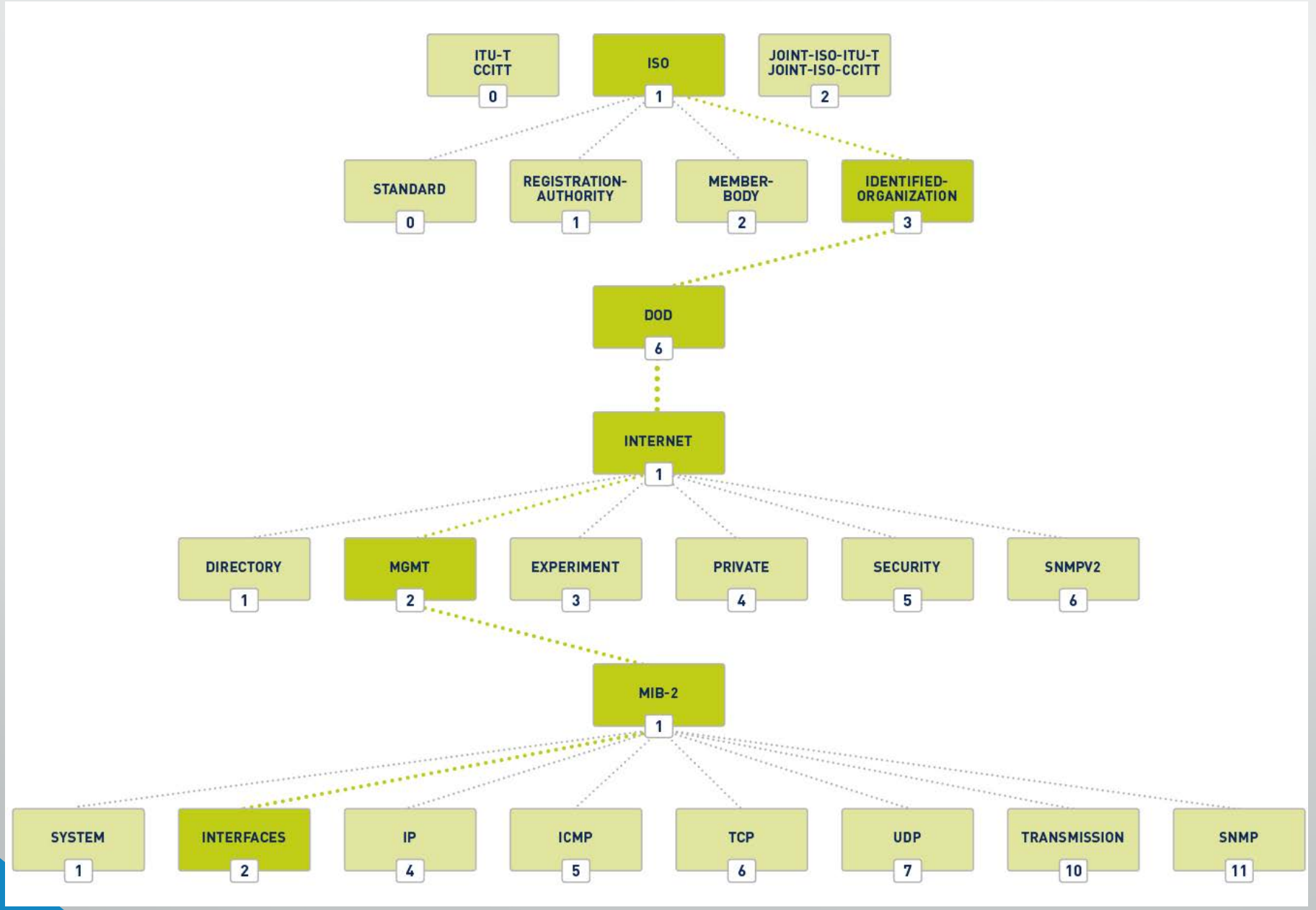
- Két féle működési mód:
- Normál és esemény vezérelt
  - A szerver megadott időközönként kéri a paramétereket a kliensektől, a szerver oldal feladata, hogy feldolgozza és felismerje az esetleges anomáliákat
  - A kliens egy speciális esemény hatására küld üzenetet a szervernek, ezzel felhívva a figyelmét az anomáliára

Hálózat menedzsment – SNMP

- Adatok azonosítása:
- OID Object Identifier az SNMP alapköve, egy ID mely az egyes eszközök egyes paramétereit azonosítja
- MIB Management Information Base – az OID-k adatbázisa
- Minden eszközgyártó az általános MIB-ek mellett sajátot is gyárt az eszközeihez (pl. az, hogy hány ventilátor fordulatszámát kell lekérdezni csak a gyártó tudja)

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – OID



tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – OID

- OID egymás utáni számok az előbbi fa struktúra alapján
- Pl.: .1.3.6.1.2.1.1.5.0 vagy sysName.0
- Ez valamilyen adatot ad vissza, pl.: integer, string
- A MIB szükséges ahhoz, hogy a számokhoz valamilyen nevet is hozzárendeljünk

tilb
Távközlés-
Informatika
Laboratórium

Hálózat menedzsment – SNMP

- SNMP implementációk:
  - Gyakorlatilag bármiben amiben van RJ45 port létezik hozzá SNMP implementáció is
  - Legelterjedtebb hálózat menedzsment alkalmazások:
  - Open-Source: Zabbix, Nagios, Cacti, OpenNMS és forkjai
  - Soknak saját agent-je van az SNMP mellett, mely a SNMP-nél nagyobb funkcionalitást eredményez Pl.: Zabbix fájl checksum ellenőrzés a passwd fájlra
  - Fontos, Ezek az implementációk folyamatosan gyűjtenek adatot, óriási adatmennyiség egy idő után kontollálhatatlan

Hálózat menedzsment – SNMP

- **snmpwalk -On -c mycommunity -v 1 remotehost**
- .1.3.6.1.2.1.1.1.0 = STRING: AIX remotehost 3 5 0000DEADBEEF
- .1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.8072.3.2.15
- .1.3.6.1.2.1.1.3.0 = Timeticks: (63151778) 7 days, 7:25:17.78
- .1.3.6.1.2.1.1.4.0 = STRING: Sysadmin (root@localhost)
- .1.3.6.1.2.1.1.5.0 = STRING: remotehost
- .1.3.6.1.2.1.1.6.0 = STRING: Server Room
- .1.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
- **$ snmpwalk -Os -c mycommunity -v 1 remotehost**
- sysDescr.0 = STRING: AIX remotehost 3 5 0000DEADBEEF
- sysObjectID.0 = OID: netSnmpAgentOIDs.15
- sysUpTimeInstance = Timeticks: (63164986) 7 days, 7:27:29.86
- sysContact.0 = STRING: Sysadmin (root@localhost)
- sysName.0 = STRING: remotehost
- sysLocation.0 = STRING: Server Room
- sysORLastChange.0 = Timeticks: (0) 0:00:00.00

Hálózat menedzsment – SNMP

- **Bemutató:**

- `snmpwalk -c public -v 3 10.9.0.194 -u public -l noAuthNoPriv  1.3.6.1.4.1.34774.4.1 -m all`
- `snmpwalk -c public -v 2c 10.9.0.30 .1.3.6.1.4.1.343.2.19.1.2.10 -m all`
- Zabbix / grafana