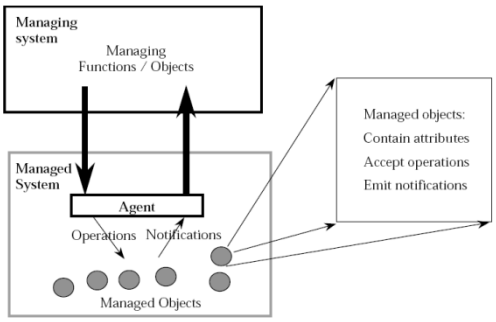
IP alapú hálózatok menedzsmentje – ZH tételsor (2007/2008 tavasz)

BEV: Mi a megfigyelés és a vezérlés közötti összefüggés? (2)

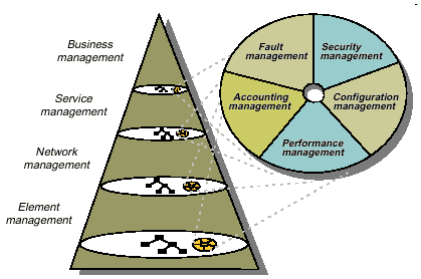
A menedzsment rendszer a megfigyelési pontok adatai alapján vélt állapot függvényében, a vezérlési pontokon keresztül képes a menedzselt hálózatot valamely kívánt állapotba hozni. A megfigyelés és vezérlés közti időbeli eltérést befolyásolja a lekérdezési intervallum, a protokoll- és kommunikációs költségek, valamint a feldolgozási idő.

BEV: Rajzolja le és magyarázza el a fundametális menedzsment modellt! (5)



A menedzsment rendszer ágenseken keresztül van kapcsolatban a menedzselt rendszer objektumaival. Ezen objektumok tulajdonságokkal bírnak, rajtuk az ágensen keresztül műveletek hajthatók végre, valamint bizonyos feltételek teljesülése esetén üzeneteket generálhatnak. A menedzsment rendszer feladatai: Operation, Administration, Maintenance, Provisioning

BEV: Ismertesse az OSI Network Management Model-t (piramis és területek, rajzoljon is). (5)



ISO 7498-4 (1978): a hálózatmenedzsment minden szintjén definiálja a menedzsmentfunkciókat (FCAPS):
Fault: hiba detektálása, javítása (reaktív, proaktív)
Configuration: MAC – moves, adds, changes
Accounting: számlázási információk, korlátok betartása
Performance: felhasználói igények kielégítése (policy-k), statisztikák, kapacitástervezés
Security: hitelesítés, titkosítás

BEV: Milyen komponensekből áll egy Network Management System architektúra? Hogyan kapcsolódnak ezek egymáshoz? (3)

Network control host (manager): NMA | NME, App | Comm | OS
server, workstation (agent): NME , App | Comm | OS
router (agent): NME |Comm | OS
NMA (Network Management Application): menedzsment alkalmazás felhasználó interfésszel
NME (Network Management Entity): statisztika gyűjtés, tárolás, vezérlőparancsok végrehajtása

BEV: Szoftveresen milyen fő komponensekből épül fel egy Network Management System architektúra? (3)

Három rétegből áll. A felső réteg *egységes felhasználói interfészt* biztosít az NMA-k felé. A középső rétegben helyezkednek egy a menedzsmentalkalmazások *(NMA)*, és az *NM adat transzport szolgáltatás*, melyen keresztül elérhető a *MIB hozzáférési modul*, valamint a hálózat elérését biztosító *kommunikációs protokoll stack*.

MON: A menedzsment információ jellegét tekintve milyen típusokat különböztethetünk meg monitorozás szempontjából? Hogyan viszonyulnak ezek az osztályok egymáshoz? Mondjon példát az egyes osztályok elemeire! (5)

A menedzsment információ jellegét tekintve lehet *statikus, dinamikus, és statisztikus*. Statikus információ lehet egy konfigurációs paraméter (pl. Switch_Buffer) vagy egy szenzor állapota (pl. Status_Sensor), ami a berendezésben tárolódik/generálódik. Ezen szenzorok kiolvasásával, adatgyűjtéssel nyerhetjük a dinamikus információkat (pl. State_Variable), ezeket már általában a LAN többi tagja is láthatja. Majd feldolgozva, megfelelően absztrahálva kapjuk a statisztikákat (pl. Throughput).

MON: Milyen kétfajta alapvető módszert ismer monitorozásra? Melyiknek mi az előnye/hátránya? (3)

Polling (lekérdezés): a menedzser kérésére a kliens válaszol a MIB alapján (konfiguráció begyűjtése, kondíció periodikus lekérdezése).
Előnye: robosztus, hibatűrő. Hátránya: jelentős forgalmat generálhat, időkritikus.
Event reporting (jelentés): kliens által akár periodikusan, akár eseményhez kötve.
Előnye: az eseményhez kötődően azonnali jelzést kínál. Hátránya: a jelentés célba jutásáról vagy annak meg nem történtéről nem értesülünk (nem megbízható)

MON: Elsődlegesen milyen OSI menedzsment területeken monitorozunk? Mik ezen feladatok jellegzetességei? (6)

Teljesítménymonitorozás (Performance Monitoring): általa a teljesítménycsökkenést okozó hibákat javítani tudjuk, tervezhetővé válik a kapacitásbővítés
Teljesítmény indikátorok: szolgáltatás specifikus (availability, response time, accuracy), hatékonyság specifikus (throughput, utilization)
Hibamonitorozás (Fault Monitoring): hibák észlelése, jelentése, megelőzése (küszöbértékek megadása, figyelése), izoláció, diagnózis (kapcsolati-, adatintegritás-, protokollintegritás- és válaszidő tesztek)
Accounting Monitoring: hálózat használatáról információgyűjtés, korlátozás (kvóták), számlázás (eseti, havi és forgalomarányos díjak). Fejlett rendszerek képesek előrejelzéseket készíteni az erőforrások használatával, kvótákkal, számlázási költségekkel kapcsolatban.

VEZ: Elsődlegesen milyen OSI menedzsment területeket vezérlünk? Mik ezen feladatok jellegzetességei? (4)

Konfiguráció (Configuration mgmnt): objektumai konkrét fizikai erőforrások (pl. router) vagy alacsonyszintű logikai objektumok (pl. transzport réteg újraküldési számláló). Feladata meghatározni a konfigurációs információkat (erőforrások, attribútumok típusa és értékkészlete), majd a monitorozás vagy jelentés függvényében vezérelni (inicializálás/kikapcsolás, attribútumok módosítása, kapcsolatok megadása/módosítása), valamint szoftverek feltöltése (routing tábla, verzókezelés). A paraméter lehet: csak MIB (pl. adminisztratív bejegyzés módosítása), MIB + erőforrás (pl. port engedélyezés/tiltás), MIB + akció (pl. változó állítása általi inicializáció)
Biztonság (Security mgmnt): titoktartás (secrecy – csak a felhatalmazottak olvashatják), integritás (integrity – csak a felhatalmazottak módosíthatják), rendelkezésre állás (availability – hozzáférhető a felhatalmazottak számára)

Biztonsághoz kötődő információk kezelése (eseménynaplózás, biztonsági monitorozás, jelentések, backup), erőforrás hozzáférés vezérlése (authentication & authorization), titkosítási folyamatok vezérlése (titkosítási algoritmusok, a menedzser-ágens kommunikáció kódolása)

VEZ: Mi lehet a tárgya a biztonság menedzsmentnek? Milyen fenyegetésekkel találkozhatunk? Hogyan viszonyulnak a fenyegetések és védendő objektumok egymáshoz? (6)

Tárgyai: (pl. számlázási, előfizetői, piaci, mérnöki) információ, számítógép, hálózat.
Fenyegetések:
megszakítás (interruption) > availability: megsemmisít, hozzáférhetetlen vagy használhatatlan
elfogás (interception) > secrecy: jogosulatlan hozzáférés
megváltoztatás (modification)> integrity: jogosulatlan hozzáférés + meghamisítás
létrehozás (fabrication) >integrity: hamis információk létrehozása

SNM: Mit ad meg az Internetes Simple Network Management keretrendszer? Milyen alapvető dokumentumok (ezek témája) alkotja ezt a keretrendszert? (3)

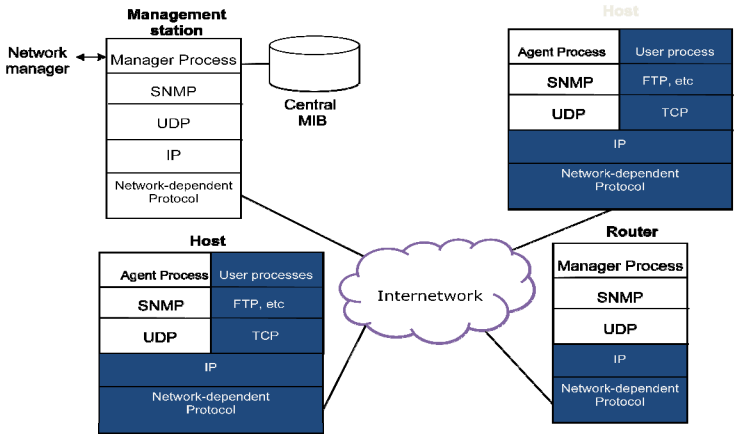
RFC 1155: Structure and Identification for Information for TCP/IP-based Networks
RFC 1157: Simple Network Management Protocol
RFC 1213: Management Information Base for Network Management of TCP/IP-based Internet: MIB-II
A keretrendszer elemei:
Structure of Management Information (SMI): a különböző eszközök együttműködése érdekében az adatok egységes struktúráját, szintaxisát, karakterisztikáját határozza meg.
Management Information Bases (MIBs): egy adott eszközre vonatkozó menedzselt változók halmaza.
Simple Network Management Protocol (SNMP): a protokoll, ami leírja az ágensek és menedzser állomások közti információcsere módját
Security and Administration: a három fő komponens számára biztonsági és adminisztratív képességek.

SNM: TCP/IP hálózatokra, milyen komponensekből áll a Network Management architektúra? Milyen funkciókat látnak el ezek a komponensek? (4)

menedzser állomás (MS): alkalmazások az adatok analizálására és hibamenedzsmentre, felhasználói interfész nyújtása a monitorozáshoz és vezérléshez, MIB-ből nyert adatbázis az összes menedzselt eszközre, a felhasználó (menedzser) „követelményeinek” átfordítása monitorozási és vezérlési cselekvésekké.
menedzsment ágens: az MS általi vezérlés végrehajtása, aszinkron üzenetek küldése
menedzsment információs alapok (MIB): hozzáférési pont a menedzser számára, az erőforrások objektumként (nézőpont) való reprezentálása
hálózatmenedzsment protokoll: összeköti a menedzsert és az ágenst (SNMP: get, set, trap)

SNM: Rajzoljon le és röviden magyarázzon egy SNMP protokoll architektúrát (menedzser, ágens, MIB, hoszt, router)! (4)

A management station-ön futó menedzseralkalmazás (folyamat) karban tartja a központi MIB-et, és az SNMP alkalmazási rétegbeli protokoll segítségével UDP felett kommunikál a hálózaton keresztül a menedzselt eszközökkel. A routerek és hosztok ugyanezen protokoll-architektúrán keresztül kapcsolódnak a hálózathoz.



SNM: Mi az a SNMP proxy? Mi a feladata? (2)

Az SNMP proxy egy olyan ágens, amely képes az SNMP protokoll-architektúráját egy más architektúrájú eszközhöz illeszteni (nem-IP alapú hálózat, SNMPv1 és SNMPv2 együttműködés).

SNM: Mi az a trap-directed polling? (2)

Nagyszámú menedzselt ágens és objektum esetén jelentősen terhelné a hálózatot és a CPU-t ha a menedzser folyamatosan lekérdezné az összes objektumadatot. Ehelyett csak inicializáláskor és ritkán kérdezzük le az ágensek kulcsadatait. Ha valami rendkívüli esemény következik be (pl. reboot, linkhiba, küszöbérték átlépése) az ágens trap üzenet által értesíti a management stationt, ami ezután lekérdezi az ágenstől (és esetleg környezettől) a szükséges adatokat (polling), valamint a kivételnek megfelelő akciókat hajthat végre.

ASN: Mi az ASN.1-BER koncepció? Hol (milyen interfészeken) és mire/miért használjuk? (3)

Az ASN.1 (Abstract Syntax Notation One) egy, az alkalmazási rétegbeli protokollok egyértelmű és megvalósítás-független leírására használt, absztrakt leírónyelv. A BER (Basic Encoding Rules) egy kódolási specifikáció, mely megadja a fizikai octet stringek kódolását minden absztrakt ASN.1 adattípusra. Az SNMP-ben a MIB-ekben tárolt adatok megadása, és az alkalmazási rétegbeli reprezentáció ASN.1-ben történik, az adatátvitel (az UDP csomagokban) ennek alapján BER által, binárisan van kódolva.

ASN: Mire használja a TAG-eket az ASN.1? (3)

Minden ASN.1 adattípusnak (kivéve CHOICE és ANY) van hozzárendelt TAG-je, mely az osztály nevéből (class name, 2 bit), a formátumból (3. bit: egyszerű vagy összetett) és a típusazonosítóból (alsó 5 bit) áll, így egyértelműen beazonosítja a hivatkozott típust.
Osztályok: UNIVERSAL, APPLICATION, CONTEXT-SPECIFIC, PRIVATE

ASN: Mi az a BER? Hogyan működik? Miért jó ez a struktúra? (3)

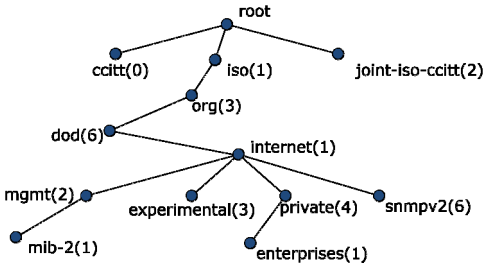
A BER az ASN.1 egyik kódolási specifikációja, minden ASN.1 típusra megadja annak octet stringre való kódolását. TLV (type-length-value) struktúrát használ rekurzívan (minden érték további TLV-t tartalmazhat). Előnye tömörségéből fakad, így kevés overheadet jelent az átvitel/tárolás során.

SMI: Mi az a SMI? Milyen más szabványt használ? (2)

Az SMI (Structure of Management Information) az SNMP MIB definíciós keretrendszere, mely megadja, hogy hogyan definiálhatók a menedzselt objektumok (MO) a MIB-ben, valamint az MO-k adattípusát, neveit, lehetséges értékeit. Az ASN.1 részhalmaza, csak egyszerű adattípusokat támogat (skaláris változók, 2-dimenziós skaláris táblázatok – SEQUENCE OF).

SMI: Hogyan néz ki a MIB struktúra (rajzoljon is)? Hogyan azonosítjuk az objektumokat? Mely objektumok mögött van erőforrás? (3)

Az objektumok hierarchikus struktúrába vannak rendezve, minden MO rendelkezik egy objektum azonosítóval (OID). A fa levelei reprezentálják a valós erőforrásokat.
Pl.: 1.3.6.1.2.1.6.13 = {iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) tcp(6) tcpConnTable(13)

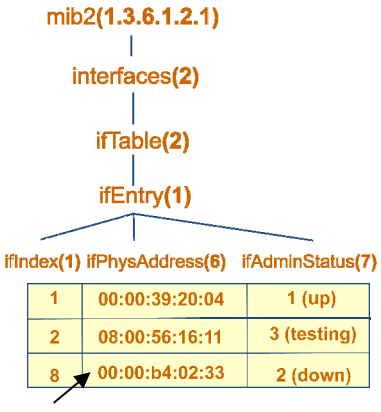


MIB-Mod: Milyen modellezési lépéseket és feladatokat célszerű alkalmazni MIB létrehozására? (5)

1. MIB objektum-osztályok meghatározása (Components, Attributes, Actions, Statistics, State)
2. modellezés és MIBre fordítás: objektummodell a komponensekről és azok számosságáról, attribútumairól, statisztikákról, állapotokról, majd ezt fordítsuk le a MIB szintaxisára. Az alkomponensek nullánál nagyobb számossággal táblázatot kell alkossanak. A statisztikák típusának meghatározása (monoton emelkedik – Counter, küszöbérték – Integer, diszkrét érékek (FSM) esetén – enumeratedInteger, fluktuál – Gauge), az objektumok adatai Octet String (felhasználó által olvasható vagy bináris adat), vagy Integer (mérhető).

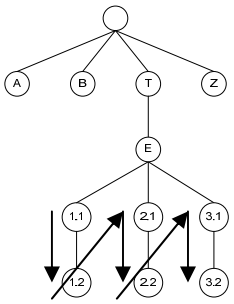
MIB-1: Hogyan épülnek fel a táblázatok a MIB-ben? Milyen ASN.1 típusként vannak definiálva? Mi a MIB konvenció? Hogyan férhetünk hozzá egy meghatározott táblázat elemhez? Rajzoljon és magyarázza! (6)

Kétdimenziós táblákat hozunk létre, melyek nem tartalmazhatnak beágyazott táblázatokat. Az elemek egyértelmű azonosításáért egy vagy több index elem felelős. A táblázat sorai SEQUENCE típusként vannak definiálva, a táblázat pedig ezen sorokból alkotott SEQUENCE OF típusból áll össze. Egyszerű objektumok példányaihoz az <objektum azonosító>.0 azonosítóval, a táblázat példányaihoz pedig a <táblázat azonosító>.<oszlop>.<indexérték> azonosítóval.
pl. az ábrán 1.3.6.1.2.1.2.2.1.6.8

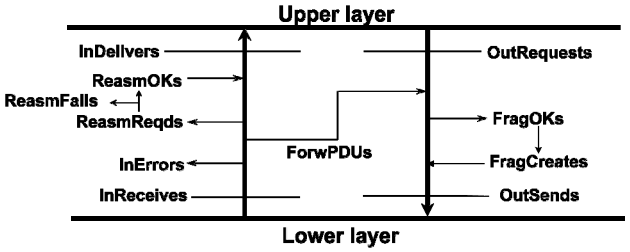


MIB-1: Ismertesse a lexicographikus sorrendezést! Rajzoljon is! Mire és hol használják? (3)

Mivel az objektumok attribútumait lexikografikus rendezésben tároljuk (mint pl. a szótárakban a szavakat), a táblázatok adatainak lekérdezése jelentősen egyszerűsödik a GetNextRequest kérés által, ami így az egész táblázatot oszlopfolytonosan adja vissza, mint egy (preorder) mélységi bejárás (ld. ábra).



MIB-1: Ismertesse a CASE diagram koncepciót! Rajzoljon egy mintapéldát illusztrálásra, értelmezze a számlálókat! (3)



Jeffrey Case (1989), jól használható eszköz a MIB-ek fejlesztésénél, protokoll-rétegenkénti forgalmi összetétel számlálására.

Elemei: fő áram (az upper és lower rétegek közötti folyam), horizontális vonal (számláló), kifele mutató nyíl (feltétel és számláló a fő folyam elhagyásához), befelé mutató nyíl (számláló, új PDU-k belépési pontja).

pl.: InReceives (az alsó rétegből érkezett csomagok), InErrors (hibás csomagok, eldobva), ReasmReqds, ReasmFails, ReasmOK (újracsomagolt csomagok, hibás/eldobva, OK), InDelivers (a felsőbb réteg számára kézbesített csomagok), ForwPDUs (az alsóbb réteg felé vissza), stb.

MIB-1: Válasszon 3 objektumot a MIB-II alatt és röviden ismertesse, hogy milyen menedzsment információkat szolgáltat az alatta lévő fa. (4)

MIB-II: 10 csoportban, 171 objektum. Ebből három példa (RFC 1158 alapján):

interfaces(2): fizikai vagy virtuális interfészekről általános információk (konfiguráció, ált. stat.).

ifNumber(1): az interfészek száma (állapotuktól függetlenül)

ifTable(2) -> ifEntry(1)

ifIndex(1): az interfész egyedi azonosítója

ifType(3): az interfész alsó két rétegnek megfelelő típusa (pl. 6 – Ethernet)

ifMtu(4): a legnagyobb datagram (octetben), amit küldeni/fogadni képes

ifSpeed(5): az interfész aktuális becsült sebessége (b/s)

ip(4): IP konfigurációk (pl. TTL), statisztikák (forgalom és hiba), táblák

ipInReceives(3): fogadott datagramok száma, beleértve a hibásakat is

ipRouteTable(20): az útvonalválasztó táblát tartalmazza, valamint a hozzá tartozó metrikákat

icmp(5): az ICMP csomagokkal kapcsolatos adatok

icmpInDestUnreachs(3): érkezett ICMP Destination Unreachable csomagok száma

MIB-1: Miért van szükség táblázatok indexelésére? (2)

Mert az indexek azonosítják a táblázat sorait, elemei ezek segítségével érhetők el.

RMON: Mi az RMON koncepció? Milyen előnyökkel jár(hat) a távoli monitorozás? (4)

A dedikált (vagy egyéb funkciókat is ellátó) RMON eszközök (monitorok vagy probe-ok) a menedzser és az ágensek tehermentesítése érdekében promiscuous módban figyelik az adott alhálózat forgalmát, csomag(részleteket) gyűjtve, analizálva (proaktív monitorozás). Így nem csak az egyedi eszközökre, hanem az adott LAN-ra vonatkozóan is gyűjthetünk információkat. Csökkenti az SNMP forgalmat, több menedzserrel is együttműködhet (növekszik a megbízhatóság), az aktív analízisek alapján gyorsabb diagnosztika és jelentés az NMS felé, valamint lehetőség van offline monitorozásra is (ha a menedzser épp nem elérhető).

RMON: Hogyan vezérelhetjük a távoli monitorozást? Mik ennek jellegzetes problémái? Hogyan kezelik ezt az SNMP keretben? (5)

Az RMON MIB-ben kerültek meghatározásra a vezérlési funkciók (Configuration Control, Action Invocation), ezek funkcionális csoportokba vannak rendezve, csoportonként kontrol- és adattáblákkal (utóbbiak csak olvashatók). A kontrol táblában határozzuk meg az adatgyűjtés paramétereit (forrás, adat típusa, gyűjtés időtartama), az adattáblákból pedig kiolvashatjuk az összegyűjtött adatokat.

A kontrol táblában néhány paramétert csak úgy módosíthatunk, hogy invaliddá tesszük (ezzel töröljük a hozzá tartozó adattábla bejegyzéseket is), majd a módosított paraméterekkel újra létrehozunk egy bejegyzést.

RMON: Hogyan valósítja meg az RMON probe az erőforrások hatékony megosztását? Mire kell figyelnie a menedzsereknek? (3)

Minden monitorozási funkcióhoz tulajdonost rendel (owner, aki létrehozta), így a menedzser felismerheti saját foglalásait (ha nincs már rá szüksége, felszabadíthatja). Egyeztetés és megfelelő jogok birtokában más erőforrását is felszabadíthatjuk (pl. ha a foglalást birtokló menedzser időközben összeomlott). A monitor rendelkezik saját funkciókkal is, ezekben a legnagyobb a bizalma. Egy funkció kérés beérkeztekor a kontrol tábla végigpásztázása hasonló, már kért funkció után.

RMON: Hogyan kezeli az RMON probe a konkurens vezérlő tábla sor hozzáadást? Mi az RMON polka? (3)

RMON polka:

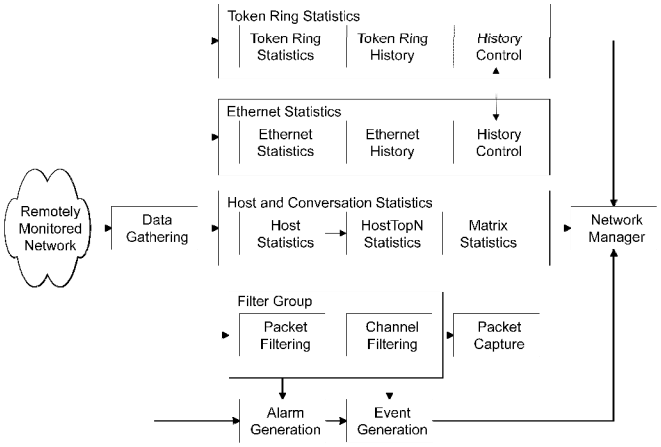
1. menedzser sor létrehozása createRequest(2) EntryStatus mezőértékkel
2. ha az ágens végrehajtotta a műveletet, akkor a sor státuszt underCreation(3) értékre állítja (mindaddig ez az értéke, amíg a menedzser az összes sorát be nem állítja)
3. ha a menedzser kész az összes sorával, azok státuszát valid(1) értékre állítja
4. ha a sor már létezik, vagy createRequest végrehajtása alatt van, akkor hibával tér vissza

RMON: Mi az általános kapcsolat az adat és a vezérlési táblák között? (2)

A vezérlési tábla indexei (pl. rm1ControlIndex) segítségével az adattáblában azonosíthatjuk az azonos bejegyzéshez tartozó adatsorokat, mivel a saját indexükön kívül tartalmazzák a hozzájuk tartozó kontroltábla-bejegyzés indexét is (pl. rm1DataControlIndex).

RMON: Hogyan épül egymásra az RMON adat és statisztika gyűjtés? Milyen kapcsolódó csoportok vannak? (3)

Az RMON az adatokból vett minta alapján statisztikákat generál, majd ezen statisztikák periodikus mintavétele alapján top- és táblázatos historykat készít.



RMON: Milyen információt szolgáltat az RMON statistic csoport? (2)

MAC (alhálózat) szintű kihasználtság és hiba statisztika.
R/W objektumok: etherStatsSource, etherStatsOwner, etherStatsStatus
counterek: packets, octets, broadcasts, multicasts, collisions, errors, csomagméret eloszlások

RMON: Milyen információt szolgáltat az RMON history csoport? (2)

Periodikus statisztikus minták a statistics csoportra. (kivétel a csomagvesztés-eolszlás)
Körkörös puffert (bucket) használ, melynek méretét a menedzser igényli.
Vezérlés: historyControlTable (melyik szegmensre, milyen mintavétellel – javaslat: 30mp és 30p)
Adatok: etherHistoryTable

RMON: Milyen információt szolgáltnak az RMON host csoportok? (4)

Hoszt-forgalmak az adott alhálózaton. Ki-/bemenő csomagok, oktettek, kimenő multicast, broadcast üzenetek, hibák. A táblázat indexelhető MAC cím (hostTable), létrehozási idő (hostTimetable) vagy valamely paraméter (hostTopN) alapján.