

### 4.5.2.a APPENDIX 2: Gedetailleerd overzicht van de RMON2 MIB

RMON version 2 is een uitbreiding van de RMON-standard en richt zich op het monitoren van de hogere protocol lagen. RMON2 is beschreven in RFC 2021 en heeft de status van proposed standard. Een aantal van de RMON2-groepen wordt hieronder beschreven:

1. Protocol Directory-groep (*protocolDir*)  
 Bevat informatie over de protocollen die de RMON2 probe kan herkennen. De groep bestaat uit een scalair object, *protocolDirLastChange*, en een tabel, *protocolDirTable*. De *protocolDirTable* omvat een element voor elk ondersteund protocol (voor de datalink layer, network layer, en application layer). Elk element omvat onder andere de protocol identifier, protocol parameters, protocol description, enzovoort. De *protocolDirLastChange* bevat de tijd waarop de *protocolDirTable* voor het laatst werd gewijzigd.
2. Protocol Distribution-groep (*protocolDist*)  
 Bevat het aantal bytes en packets verzonden onder elk van de ondersteunde protocollen. Deze groep bevat een data-tabel, *protocolDistStatsTable* en een controletabel, *protocolDistControlTable*. De werkelijke data wordt door de *protocolDistStatsTable* bijgehouden; voor elk protocol waaronder minstens één packet is verzonden wordt het aantal packets alsmede het aantal octets geteld. De *protocolDistControlTable* bestuurt per protocol het verzamelen van de data. Elk tabel element beschrijft onder andere welk sub-netwerk gemonitord moet worden, het aantal gemiste packets, de waarde van *sysUpTime* toen deze sturing werd geactiveerd, enzovoort.
3. Address Map-groep (*addressMap*)  
 Beeldt ieder netwerkadres af op een datalink-adres. Deze groep bestaat uit twee tabellen (*addressMapTable* en *addressMapControlTable*) en drie scalaire objecten (*addressMapInserts*, *addressMapDeletes*, en *addressMapMaxDesiredEntries*). De *addressMapTable* bevat de afbeelding (mapping) tussen netwerk en datalink-adres. De probe vult deze tabel door ieder foutvrij ontvangen packet te analyseren. Ieder element in de tabel bevat een netwerkadres, data link adres, tijd, en de laatste interface poort waarop een packet met het betreffende netwerk-adres is gesignaleerd. De *addressMapControlTable* bestuurt het verzamelen van informatie en beschrijft onder andere de bron

van de data, het aantal packets dat niet verwerkt kon worden, enzovoort.

De *addressMapInserts* bevat het aantal malen dat een element is toegevoegd aan de *addressMapTable*; de *addressMapDeletes* bevat het aantal malen dat een element is verwijderd en de *addressMapMaxDesiredEntries* beschrijft het gewenste maximum aantal elementen in de *addressMapTable*.

#### 4. Network Layer Host-groep (*nlHost*)

Maakt het mogelijk packets te analyseren op basis van hun network layer-adressen. Bestaat uit twee tabellen: *nlHostControlTable* en *nlHostTable*.

Deze groep lijkt veel op de *host*-groep. Het verschil is dat deze groep informatie verzamelt op basis van het network layer-adres, terwijl de *host*-groep informatie verzameld op basis van het datalink-adres.

#### 5. Network layer Matrix-groep (*nlMatrix*)

Maakt het mogelijk het verkeer te analyseren tussen twee hosts op basis van hun network layer adressen. Bestaat uit vijf tabellen: *nlMatrixControlTable*, *nlMatrixSDTable*, *nlMatrixDSTable*, *nlMatrixTopNControlTable*, en *nlMatrixTopNTable*.

De gegevens in de *nlMatrixControlTable*, *nlMatrixSDTable*, en *nlMatrixDSTable* komen overeen met die in de *matrix*-groep, maar zijn gebaseerd op het network layer-adres in plaats van het datalink-adres.

De gegevens in de *nlMatrixTopNControlTable* en *nlMatrixTopNTable* komen overeen met die in de *hostTopN* groep, maar zijn gebaseerd op het network layer adres in plaats van het datalink-adres.

#### 6. Application Layer Host-groep (*alHost*)

Maakt het mogelijk de packets te analyseren op basis van hun application layer-adressen. Bestaat uit één tabel, *alHostTable* die bestuurd wordt via de *nlHostControlTable*. Deze groep komt overeen met de *host*-groep, maar de informatie wordt verzameld op basis van de application layers-adressen in plaats van de datalink-adressen.

#### 7. Application Layer Matrix-groep (*alMatrix*)

Maakt het mogelijk het verkeer te analyseren tussen twee hosts, op basis van hun application layer-adressen. Bestaat uit vier tabellen: *alMatrixSDTable*, *alMatrixDSTable*, *alMatrixTopNControlTable*, en *alMatrixTopNTable*.

De *alMatrixSDTable* en *alMatrixDSTable* worden bestuurd via de *nlMatrixControlTable*. Ze verzamelen vergelijkbare informatie als de *matrix*-groep maar op basis van application layer-adressen in plaats van datalink-adressen.

De gegevens in de *alMatrixTopNControlTable* en *alMatrixTopNTable* komen overeen met de gegevens in de *hostTopN* groep, maar de informatie wordt verzameld op basis van de application layer-adressen in plaats van de datalink-adressen.

8. User History Collection-groep (*usrHistory*)  
Verzamelt periodieke monsters (samples) van MIB variabelen op basis van door de gebruiker gedefinieerde parameters. In tegenstelling tot de *history*-groep van RMON1, kan in principe iedere variabele in iedere door de probe ondersteunde MIB be-monsterd worden. Vanwege de vele mogelijkheden is het gebruik van deze groep complex. Er zijn drie tabellen op drie niveaus. De tabel op het hoogste niveau is *usrHistoryControlTable* die één of meer exemplaren 'bevat' van de *usrHistoryObjectTable*. Elke *usrHistoryObjectTable* 'bevat' wederom één of meer exemplaren van de *usrHistoryTable*.
9. Probe Configuration-groep (*probeConfig*)  
Dient om het gemengd gebruik (interoperabiliteit) van RMON-probes en managers van verschillende leveranciers te ondersteunen. Bevat informatie over de configuratie van de probe. Bestaat uit tien scalaire objecten en vier tabellen.  
De scalaire objecten bevatten onder meer informatie over de ondersteunde RMON-groepen, softwareversie, hardwareversie, huidige datum en tijd van de probe, reset control, enzovoort. De tabellen zijn *serialConfigTable* (bevat één element voor elke seriële interface van de probe), *netConfigTable* (bevat één element voor elke netwerk interface van de probe), *trapDestTable* (bevat het doeladres van de trap berichten), en *serialConnectionTable* (bevat de benodigde parameters voor de initialisatie van een Serial Line Interface Protocol verbinding met een management station).