RMON
(Remote Monitoring)

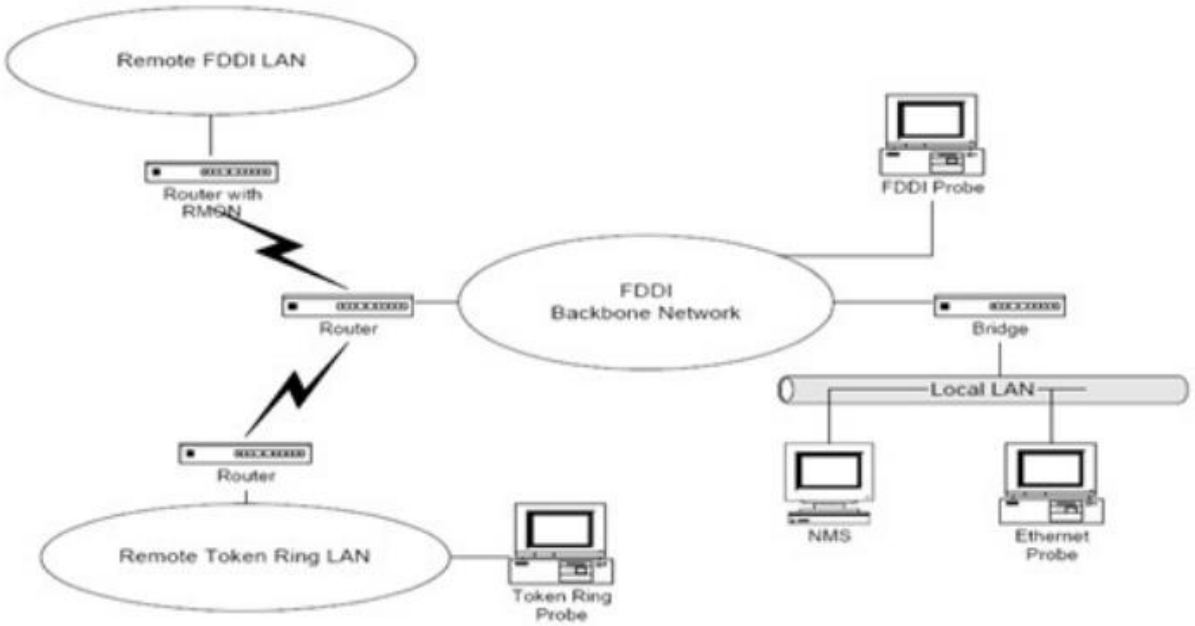
What is Remote Monitoring???

- SNMP messages going across a network between manager and agent.
  - Using a tool that sniff every packet going across a LAN,
    - Open it and analyze it.
    - It is a passive operation and does nothing to the packets, which continue on to their destinations.
    - This approach is called monitoring or probing the network and the device that performs that function is called a network monitor or probe.

Components of a Probe

- There are two components of a probe,
  - Physical object/Data Gatherer
    - Its is connected to the transmission medium.
  - Processor
    - That analyzes the data.
  - If both are at the same place geographically, the probe is called local.
    - The monitored information, gathered and analyzed locally, can be transmitted to a remote network management station.
    - In such a case, remotely monitoring the network with a probe is referred to as RMON (Remote Monitoring).

Illustration by an example



1. FDDI backbone network with a local Ethernet LAN.
    1. Two Remote LANs, one a token ring LAN and another is an FDDI LAN are connected to the backbone network.
    2. The NMS is on the local Ethernet LAN. Ethernet Probe monitoring the local LAN.
    3. The FDDI backbone is monitored by an FDDI probe via the bridge and Ethernet LAN.
    4. A token ring probe monitors the token ring LAN. It communicates with NMS via the routers, the WAN and the backbone networks.
    5. The remote FDDI is monitored by the built in probe on the router.
    6. The FDDI probe communicates with the NMS.
    7. All four probes that monitor the four LANs and communicate with the NMS are RMON Devices.

RMON Devices Advantages

- Each RMON device monitors the local network segment and does the necessary analysis.
  - It relays information in both solicited or unsolicited fashion to NMS.
  - Polling is local, the information is fairly reliable.
    - Local monitoring and reporting to a remote NMS significantly reduces SNMP traffic in the network.
- RMON reduces the need for agents in the network to be visible at all times to the NMS.

Cont…

- Monitoring packets, such as ICMP pings, may get lost in log distance communications.
  - Such losses may wrongly be interpreted by the NMS that the managed object is down.
  - RMON pings locally and hence has less chance of losing packets, thus increasing monitoring reliability.
- Individual segment can be monitored almost continuously with RMON.
  - This provides better statistics and control.
    - A fault can be diagnosed more quickly by the RMON and reported to the NMS.
      - A study report (CISCO/RMON) indicates significantly increased productivity for network administrators who use RMON in their

RMON SMI and MIB

- As the network components are made by different vendors and even the RMON devices may be from different vendors.
  - As in the comm. Of network management info, standards need to be established for common syntax and semantics for the use of RMON devices.
    - The syntax used in ASN.1 and the RMON SMI is similar to that of SMI-v2 in defining the object types.
    - RMON MIB, which define RMON groups has been developed in three stages.
      - The original RMON MIB, now referred to as RMON1 was developed for Ethernet LAN. (Nov, 1991, obsoleted in 1995).
      - Token Ring extension to RMON1 was established in sep 1993.

Cont…

- the use of RMON1 for remote monitoring was extremely beneficial, but RMON1 addressed parameters at the OSI layer 2 only.
- Hence the RMON2 [RFC 2021] was developed and released in January 1997:
  - It addressed the parameters associated with OSI layer 3-7.

RMON1 Textual Conventions

- Two new data types defined in the RMON1,
  - OwnerString
  - EntryStatus
    - Extremely useful in the operation of RMON devices, which are used by NMS to measure and produce statistics on network elements.
    - These functions involves setting up tables that control parameters to be monitored.
    - Typically a network has more than one NMS, which could be permitted to create, use and delete the control parameters in a table.
    - These operations can be done though human incharge of network.

Cont…

- For this purpose the owner identification is made part of the control table defined by the OwnerString data type.

— The EntryStatus is used to resolve conflicts that might arise between Management Systems in the manipulation of control tables.

Contents of the OwnerString

- The information content of OwnerString,
  - Info. About the owner
    - Such as IP address,
    - management station Name
    - Manager's Name
    - Location
    - Telephone Number.
  - If the agent itself is the owner,
    - The OwnerString is set to "Monitor".

EntryStatus Data Type

- For a table to be shared by multiple users,
  - A columnar object using EntryStatus(e.g. etherStatsStatus), is added to the table that contains the information on the row's status.
  - The EntryStatus data type can exist in one of four states.
    - Valid
    - createRequest
    - underCreation
    - Invalid

State	Enume-ration	Description
valid	1	Row exists and is active. It is fully configured and operational
createRequest	2	Create a new row by creating this object
underCreation	3	Row is not fully active
invalid	4	Delete the row by disassociating the mapping of this entry