# Network Management & Security (CS 330)
# RMON

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

November 08, 2013

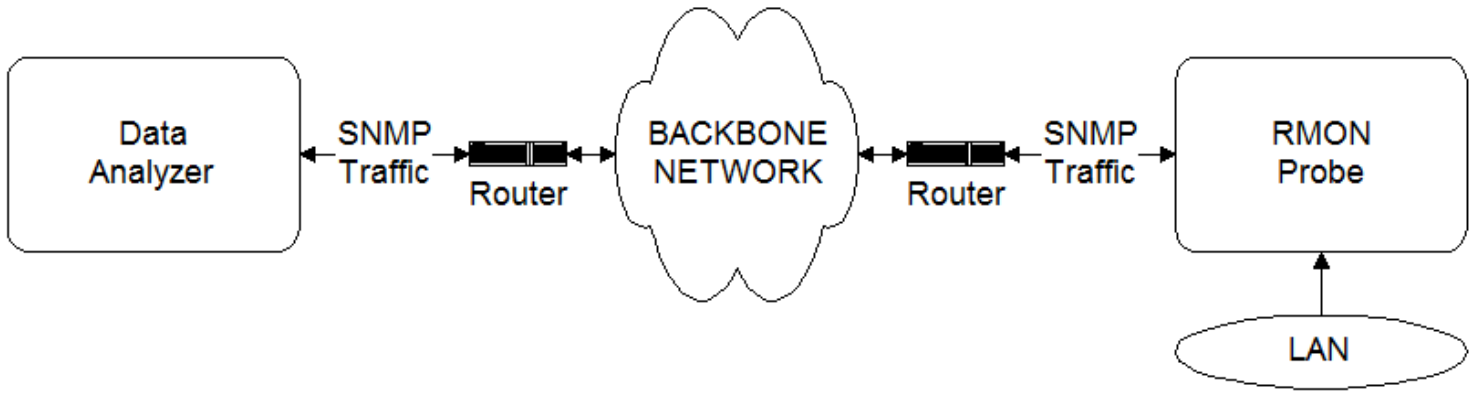
# Outline

# Remote Network Monitoring

- The most important addition to the basic set of SNMP standards, (RFC 1271)
- A major step forward in internetwork management
- Defines a remote-monitoring MIB that supplements MIB-II
- RMON1 focused on OSI Layer 1 and Layer 2 information in Ethernet and Token Ring networks
- Extended by RMON2 which adds support for Network and Application-layer monitoring

# RMON implementation

- Monitoring devices (probes) contain RMON software agents that collect information and analyze packets
- These probes act as servers and the Network Management applications that communicate with them act as clients
- Information is only transmitted to the management application when required



# RMON1

- The RMON1 MIB provides:
  - Current and historical traffic statistics for a network segment, for a specific host on a segment, and between hosts (matrix).
  - A versatile alarm and event mechanism for setting thresholds and notifying the network manager of changes in network behavior
  - A powerful, flexible filter and packet capture facility that can be used to deliver a complete, distributed protocol analyzer

# RMON1

The RMON1 MIB consists of 10 groups:

- Statistics: real-time LAN statistics, e.g., utilization, collisions, CRC errors
- History: history of selected statistics
- Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds
- Hosts: host specific LAN statistics, e.g., bytes sent/received, frames sent/received
- Hosts top N: record of N most active connections over a given time period
- Matrix: the sent-received traffic matrix between systems
- Filter: defines packet data patterns of interest, e.g., MAC address or TCP port
- Capture: collect and forward packets matching the Filter
- Event: send alerts (SNMP traps) for the Alarm group
- Token Ring: extensions specific to Token Ring

# RMON1 capabilities

- Without leaving the office, a network manager can watch the traffic on a LAN segment
- The network manager can identify trends, bottlenecks, and hotspots
- RMON1 also includes a powerful protocol analyzer so the network manager has distributed troubleshooting tools immediately
- RMON1 device is permanently attached to the network segment, it already collects and analyzes data; and is ready to transmit it to the central management system whenever required
- Deploying network management staff resources more efficiently

# RMON2

- To go up the protocol stack and provide statistics on network- and application-layer traffic
- By monitoring at the higher protocol layers, RMON2 provides the information that network managers need to see beyond the segment and get an internetwork or enterprise view of network traffic

# RMON2

The RMON2 MIB adds 10 more groups:

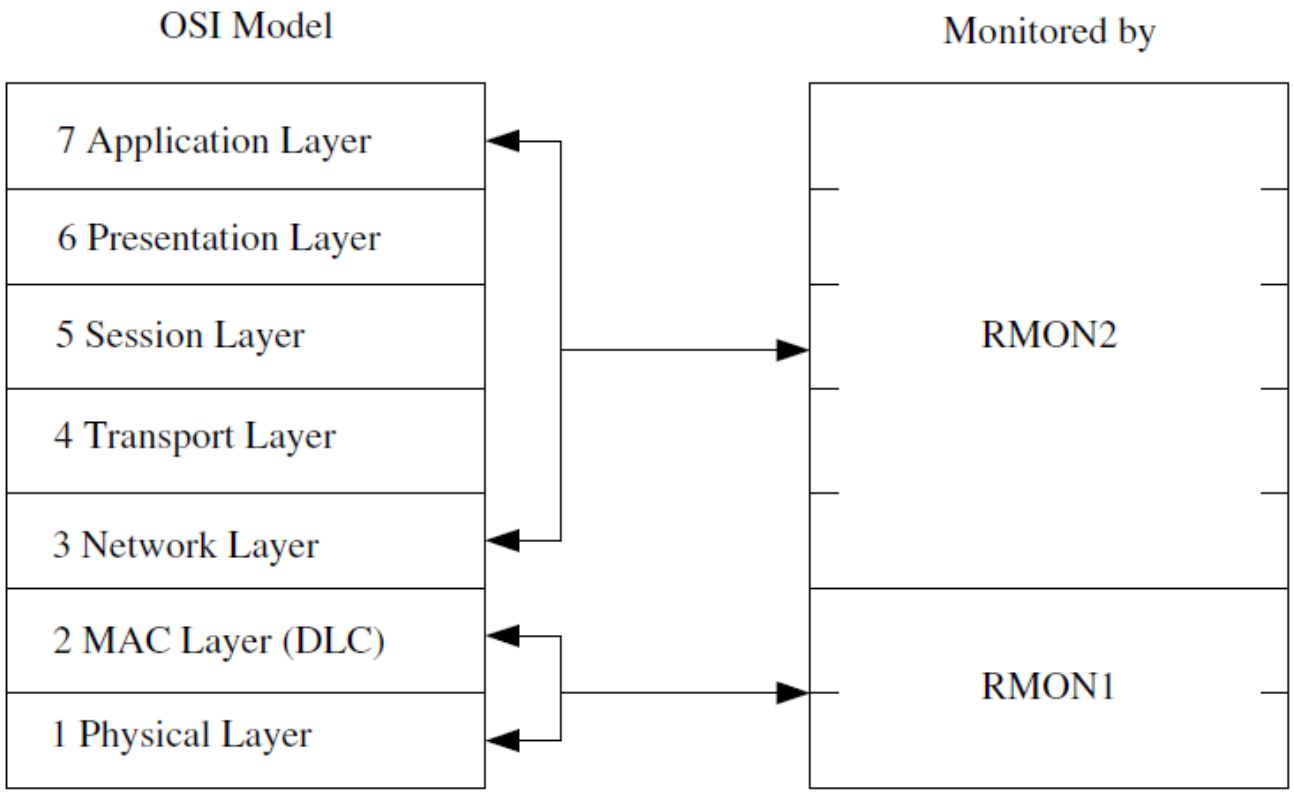
- Protocol Directory: list of protocols the probe can monitor
- Protocol Distribution: traffic statistics for each protocol
- Address Map: maps network-layer (IP) to MAC-layer addresses
- Network-Layer Host: layer 3 traffic statistics, per each host
- Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts
- Application-Layer Host: traffic statistics by application protocol, per host
- Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts
- User History: periodic samples of user-specified variables
- Probe Configuration: remote configuration of probes
- RMON Conformance: requirements for RMON2 MIB conformance

# RMON2

The RMON2 MIB adds 10 more groups:

- Protocol Directory: list of protocols the probe can monitor
- Protocol Distribution: traffic statistics for each protocol
- Address Map: maps network-layer (IP) to MAC-layer addresses
- Network-Layer Host: layer 3 traffic statistics, per each host
- Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts
- Application-Layer Host: traffic statistics by application protocol, per host
- Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts
- User History: periodic samples of user-specified variables
- Probe Configuration: remote configuration of probes
- RMON Conformance: requirements for RMON2 MIB conformance

# RMON reference layers



# RMON2 capabilities

- The most visible capability in RMON2 is monitoring above the MAC layer, which supports protocol distribution and provides a view of the whole network rather than a single segment
- Higher Layer Statistics. Traffic statistics, host, matrix, and matrix topN tables at the network layer, and the application layer enables the network manager to have a clear view of the network and resources could be better placed
- Translation between the network and MAC addresses that also adds the feature of duplicate IP address detection
- User-Defined History: specific history on a particular file server or a router-to-router connection

# RMON2 capabilities

- Improved Filtering: Additional filters to support the higher layer protocol capabilities
- Probe Configuration: With RMON2, one vendor's RMON application will be able to remotely configure another vendor's RMON probe
- Currently, each vendor provides a proprietary means of setting up and controlling their probes
- The probe configuration specification is based on the Aspen MIB which was jointly developed by AXON and Hewlett-Packard
- The Aspen MIB provides probe device configuration, trap administration, etc.