Network Monitoring Fundamentals and Standards

Edmund Wong. ywong@cis.ohio-state.edu

Network monitoring is the information collection function of network management. First, this paper gives some background information on SMIv2, MIB-II, SNMPv2 to provide a basis for understanding network monitoring standards. Then it goes into detail discussion on remote monitoring standards RMON, RMON2 and ATM-RMON. Finally, it discusses monitoring issues on the internet as a whole.

[Other Reports on Recent Advances in Networking](#)
[Back to Raj Jain's Home Page](#)

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

Table of contents:

Introduction

Network monitoring provides the information necessary for network management. It is important to find network trends and locate network problems quickly. In this paper, the fundamentals of network monitoring are discussed at the beginning to set the background for subsequent sections on single network monitoring and internet monitoring. In the single network monitoring, there are three standards being discussed: RMON, RMON2 and ATM-RMON. RMON is the remote monitoring standard created by IETF, Internet Engineering Task Force. It is implemented in commercial network monitoring environment. SMIv2, MIB-II, and SNMPv2 are mentioned to provide a background in understanding RMON. RMON2 is the upgrade to RMON. It adds new functionalities to enhance what RMON can do. SMON is mentioned because it is an extension to RMON2 for switched networks. ATM-RMON is the ATM, Asychronous Transfer Mode, equivalent for RMON. ATM is a newer technology and remote monitoring is new to it. Finally, in the internet monitoring situation, difficulties in monitoring are discussed. Then a new idea of objective-driven monitoring is mentioned because it can possibly help monitor the internet in the future.

[Back to Table of Content]

Fundamentals of Network Monitoring

Network monitoring is the information collection function of network management. Network monitoring applications are created to collect data for network management applications. The purpose of network monitoring is the collecting of useful information from various parts of the network so that the network can be managed and controlled using the collected information. Most of the network devices are located in remote locations. These devices do not usually have directly connected terminals so that network management application cannot monitor their statuses easily. Thus, network monitoring techniques are developed to allow network management applications to check the states of their network devices. As more and more network devices are used to build bigger networks, network monitoring techiques are expanded to monitoring networks as a whole.

As more people communicate using networks, networks have become bigger and more complex. The proliferation of the internet has increased the pace of network expansions. At this age of big and complex networks, network monitoring applications need to use effective ways of checking the status of their networks so that network management applications can fully control their network and provide economical, and high-quality networking services to the users. It is very important to know what are the goals to achieve in network monitoring. By knowing the goals of network monitoring, network monitoring application can choose among network monitoring techniques that will best help them monitor their networks.

There are generally three basic goals for network monitoring[Stallings Book]:

- Performance monitoring

- Fault monitoring
- Account monitoring

These goals are three of the five functional areas of network management proposed by OSI, Open Systems Interconnect. The other two functional areas are not related to network monitoring. They are configuration management and security management.[Performance Management]

Performance monitoring deals with measuring the performance of the network. There are three important issues in performance monitoring. First, performance monitoring information is usually used to plan future network expansion and locate current network usage problems. Second, the time frame of performance monitoring must be long enough to establish a network behavior model. Third, choosing what to measure is important. There are too many measureable things in a network. But the list of items to be measured should be meaningful and cost effective. This list of items to be measured is called network indicators because they indicate attributes of the network. Here is an example list of network indicators[Checklist] in Table 1.

Table 1: A list of network indicators.

Network indicators	Description
Circuit Availability	The actual time that a user can dial up to a network and the network connection is available for the user
Node Availability	The actual time that a user can use network nodes, multiplexers and routers without having error.
Blocking Factor	The number of user who cannot access the network because of busy signal in theory.
Response Time	The time to transmit a signal and receive a response for the signal.

Fault monitoring deals with measuring the problems in the network. There are two important issues in fault monitoring. First, fault monitoring deals with various layers of the network. When a problem occurs, it can be at different layers of the network. Thus it is important to know which layer is having problem. Second, fault monitoring requires establishing a normal characteristics of the network in an extended period of time. There are always errors in the network but when there are errors, it does not mean the network is having persistent problems. Some of these errors are expected to occur. For example, noise in a network link can cause transmission errors. The network only has problem when the number of errors has suddenly increased above its normal behavior. Thus, a record of normal behavior is important.

Account monitoring deals with how users use the network. The network keeps a record of what devices of the network are used by users and how often they are used. This type of information is used for billing user for network usage, and for predicting future network usage.

[Back to Table of Content]

RMON/RMON2

In network monitoring using SNMP, monitored information is seen as a set of managed objects. MIB defines the set of objects being monitored. MIB is written in OSI's Abstract Syntax Notation One (ASN.1). SMI, Structure of Management Information, is the adapted set of ASN.1 used to describe and name objects in MIB. In order to understand RMON, a basic knowledge of SMI, MIB, and SNMP is required. The latest version 2 will be discussed: SMIv2, MIB-II and SNMPv2.

SMIv2

SMI is originally used with SNMP to describe and name MIB objects. In January 1996, RFC 1902 has updated SMI to be used with SNMPv2. In many literature, this updated SMI is referred SMIv2. SMIv2 is important because it is also used by RMON2, the latest remote monitoring standard.

SMIv2 is composed of three definitions: module definitions, object definitions, and notification definitions.
Module definition describes the information module. An information module is an ASN.1 module defined for monitoring. There are three kinds of information modules:

- MIB modules, a set of related managed objects
- Compliance statements for MIB modules, the minimum set of rules used to implement an MIB
- Capability statements, a set of conceptual capability the MIB should be allowed

Object definition describes the set of managed objects contained in the MIB. Notification definition describes unsolicited exchange of management information.

MIB-II

MIB, Management Information Base, is a set of inter-related managed objects. The attributes of these objects should have network monitoring values. MIB is originally used in SNMP. SMI is the mechanisem in describing MIB's. MIB may contain several nodes, with which a processing entity called agent can access management instrumentation; and at least one management station, from where a network manager can collect statistics; and a management protocol to exchange information between agents and the management station.

SNMPv2 is updated on January 1996 in RFC 1902. SNMPv2 has added the new exchange of management information between the agents and the management stations. Since new capabilities are added, new MIB's are added for SNMPv2. The new set of MIB's is referred as MIB-II.

MIB-II are divided into several groups: system, object resource information, SNMP, information for notifications, well-known traps, set, conformation information, compliance statement and unit of conformance.

The system group contains objects common to all managed systems. Object resource information contains objects which describe the SNMPv2 entity's support of various MIB modules. The SNMP group is a set of objects which provide basic control of an SNMP entity. The information for notification group defines the set of objects to generate SNMPv2-Trap-PDU's. The well-known traps group defines the set

of well-known boots-traps. The set group is a collection of objects which allow cooperative use of SNMPv2 set operation.

The conformation information group is a set of objects for basic requirements. The compliance statement group contains the minimum set of objects used to implement an MIB. The unit of conformance group contains units used in conformation information group or things being measured. Here is a list of objects defined for these groups in table 2.

Table 2: Objects defined for SNMPv2 MIB-II

SNMPv2 Groups	Objects
System	sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, sysServices
Object resource information	sysORLastChange, sysORTable, sysOREntry, SysOREntry, sysORIndex, sysORID, sysORDescr, sysORUpTime
SNMP	snmp, snmpInPkts, snmpInBadVersions, snmpInBadCommunityNames, snmpInBadCommunityUses, snmpInASNParseErrs, snmpEnableAuthenTraps, snmpSilentDrops, snmpProxyDrops
Information for notification	snmpTrap, snmpTrapOID
Well-know traps	snmpTraps , coldStart, warmStart, authenticationFailure
Set	snmpSet, snmpSetSerialNo
Conformation Information	snmpMIBConformance, snmpMIBCompliances, snmpMIBGroups
Compliance Statement	snmpBasicCompliance
Unit of conformance	snmpGroup, snmpCommunityGroup, snmpSetGroup, systemGroup, snmpBasicNotificationsGroup, snmpOutPkts, snmpInTooBigs, snmpInNoSuchNames, snmpInBadValues, snmpInReadOnlys, snmpInGenErr, snmpInTotalReqVars, snmpInTotalSetVars, snmpInGetRequests, snmpInGetNexts, snmpInSetRequests, snmpInGetResponses, snmpInTraps, snmpOutTooBigs, snmpOutNoSuchNames, snmpOutBadValues, snmpOutGenErrs, snmpOutGetRequests, snmpOutGetNexts, snmpOutSetRequests, snmpOutGetResponses, snmpOutTraps, snmpObsoleteGroup

SNMPv2

SNMP, Simple Network Management Protocol, is the internet standardized protocol on network management. It is used extensively for network monitoring functions such as collection errors and user statistics. In January 1996, it has been updated to version 2 and is referred to SNMPv2.

SNMPv2 is created in the object-oriented world. Thus, SNMPv2 is discussed in terms of entities.

SNMPv2 entities have two roles: agent or manager. Agent is a process which uses the network monitoring instruments. Manager is the process which gets the information collected by the agent. It is an agent when it performs management operations in response to notifications or when it sends trap notification. It is a manager when it initiates the management notifications or when it performs management requests. An SNMPv2 entity may act in either role or in both roles.

There are three types of access methods provided by SNMPv2. They are manager-request to manager-response, manager-request to agent-response, or unsolicited agent response. In the first method, two entities both are acting as managers. One entitiy sends a requestion to the other. Then a response is generated. In the second method, one entity is the manager and the other is the agent. The manager issues a request and the agent acts according to the request. In the third method, two entities are required. One is the agent and the other is the manager. The agent sends a message to the manager without receiving any request. In this case, no additional response is generated by the manager. See Fig 1. for three different access methods.
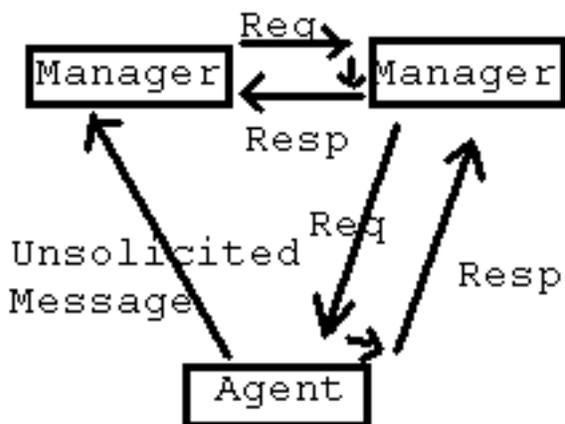

Fig 1.   SNMPv2 Access

SNMPv2 uses message to communicate between all entities. Message size should be maximized when a message is sent. This message can contain network monitoring statistics. The message size is maximized so that fewer messages are needed to be sent. This allows fewer fragmentations.

[Back to Table of Content]

RMON Standard

Remote network monitoring (RMON) is the standard of how to monitor internet traffic. This is a standard that is supposedly implemented by internet device vendors so that a network using RMON-compliant devices can be monitored using RMON-compliant software.

RMON is originally standardized by RFC 1271 in November 1991, but it is updated by RFC 1757 in February 1995. RFC 1757 has become the standard which talks about the implementation of RMON. [RFC1757]

The overall goal for RMON is to allow RMON-compliant network monitoring devices to be constructed. These devices are usually, referred to as monitors or probes, which measure specific aspects of the network without interfering normal operations. These devices are usually stand-alone devices and located in remote part of the network or even across network boundaries. The RMON standard allows these devices to communicate over the network they are monitoring. Usually, RMON is defined so that it can be implemented in a generic network. But some specification is created for monitoring Ethernet

networks, since it is one of the most popular network used in the internet. The following is a list of goals for RMON in table 3.

Table 3: List of RMON goals and explanation.

RMON Goal	Explanation
Offline Operation	RMON-compliant devices can be located in remote location. The RMON-compliant devices should be standalone so that they can function and keep on collecting statistics when the network management is offline.
Proactive Monitoring	RMON-compliant devices should continuously run diagnostics and keep records of network statistics even if the network is not experiencing problems. This establishes the normal behavior of the network so that if the network goes down, the network manager can have a baseline of network behavior to compare to problem network behavior.
Problem Detection and Reporting	RMON-compliant devices should be able to detect problems in themselves. When a part of the device is malfunctioning, the RMON-compliant device should notify the network manager the problem.
Value Added Data	RMON-compliant devices should keep useful statistics about the network even though those statistics are not used for finding out network problems. For example, host traffic can be monitored to see which host is used most often. These statistics can be used to assist planning for future network expansion.
Multiple Managers	RMON-compliants devices can be controlled by and report to more than a single network manager. This allows redundance to guarantee network management at all times. Also, it allows information collected to be distributed to different locations.

RMON is an extension of SNMPv2 and is used extensively for network monitoring activities. RMON is extended by created a new MIB specific for collecting information about the network. This specific MIB is usually referred to RMON-MIB. Inside the RMON-MIB, network monitoring objects are defined and the objects are separated into ten groups. When one object in a group is implemented, all objects inside the same group must also be implemented. The objects are listed in table 4.

Table 4: List of RMON group and explanation.

RMON MIB Group	Explanations
ethernet statistics	Statistics on each monitored Ethernet interface on the RMON-compliant device.
history control	Periodic statistical samples of data.
ethernet history	Periodic statistical samples of data from an Ethernet. These statistics are reported when they are needed.
alarm	Network attributes. When the network attributes are above a certain value or threshold, an alarm event will be sent to the network manger.
host	Statistical data from all hosts on the network.

hostTopN	Reporting on a subset of hosts. The subset of hosts is determined by ordering the host statistics and the top of the list is used.
matrix	Connections between two addresses.
filter	Packets to be chosen by a filter equation. Chosen packets are recorded.
packet capture	Packets to be recorded when the packets go through a specific path.
event	Generates and receives events. Events are messages.

Here is part of an example object etherStatsTable defined in ethernet statistics.

```
etherStatsTable OBJECT-TYPE
        SYNTAX SEQUENCE OF EtherStatsEntry
        ACCESS not-accessible
        STATUS mandatory
        DESCRIPTION
        "A list of Ethernet statistics entries."
        ::= { statistics 1 }
```

RMON-compliant devices are controlled by modifying the RMON-MIB. Also, RMON-MIB contains statistical data collected by the device. The objects in RMON-MIB can be represented as tables. This is easy for human to understand and manipulate these information. These tables are divided into control tables and data tables. Control tables have read-write permission. Control tables are updated to set up new commands for the RMON-compliant device. Data tables have read permission. These tables contain statistical data.

Here is an example control and data tables in fig. 2.

Fig 2: Diagram of made-up control table and data table.

Control Table

Control Index	Control Parameter	Control Owner	Status Object
1	7	Manager station A	valid(1)
2	2	Manager station B	valid(1)
3	84	Monitor	valid(1)

The following data table changes according to parameters set in the control table above.

Data Table

DataControlIndex	DataIndex	DataValue
1	1	64
1	1	34
2	2	656
2	4	2
2	5	2
3	1	55

In table-form, RMON-MIB is usually modified by rows. A status object is defined for each row. This

concept is important because each row has a state at different time. There are three operations:addition, modification, and deletion. Addition means addng a new row to the table. Modification changes the content of a specific row. Deletion is the removal of a specific row of the table. When these operations are executed on the table, the status object for each row changes.

Row addition is done by a series of steps.

- An index is required to specify the row to be created. The row is created with a status object of createRequest(2).
- The status object's value is then changed to underCreation(3).
- Rows exist in the underCreation(3) status until it is created. Then the state object is changed to valid(1).
- If the row has already been created before the first step, an error is returned.

Row modification is done by two steps. First, the row is deleted, and then the new row is created using row addition. Row deletion is simple. A row is deleted when its state object is set to invalid.

Since RMON-MIB allows multiple network managers, resource sharing must be taken into account. There are many possible situations in which two resources will run into sharing problems. A list of sharing problems are listed in table 5.

Table 5: Sharing problems:

Two managers want to use the same resource and the requests have exceeded the device's capability.
A manager may use a resource for too long of a time. The resource is not available to the rest of the network.
A manager has forgotten to release an unused resource. The unused resource is not available to the rest of the network.

The solution to these sharing problems is to create a label identifying the owner of the resource. This allows the manager to recognize unused resources; so that the manager can choose to release the resources. Also, the label allows the manager to find another manager to negotiate who uses which resources. The label is called OwnerString. There is a special use for the OwnerString. If its value is set to "monitor",it means the object is intended to be used by the RMON-compliant device and modification by the network management application should probably not happen. [RFC 2021]

[Back to Table of Content]

RMON2 Standard

RMON2 is an extension of RMON that focuses on higher layers of traffic above the medium access-control(MAC) layer. RMON2 has an emphasis on IP traffic and application-level traffic. RMON2 allows network management applications to monitor packets on all network layers. This is difference from RMON which only allows network monitoring at MAC layer or below. RMON2 is intended to be used by network monitoring applications. It is not intended to be used by human. [RFC 2021]

Each monitored object must have a name, a syntax, an access-level, and an implementation-status. The name is used to identify the a monitored object. The name has an object type and an object instance. Usually, the name is a text string for human to read. The syntax is the structure defined using ASN.1 notation. This abstract structure helps the human to understand the monitored object. The access-level means whether the monitored object can be read, written or both. Implementation-status is the status of the actual object. There are four possible values:mandatory, optional, obsolete, or deprecated.

RMON2 objects are divided into the following 10 groups: protocol directory,protocol distribution,address mapping, network layer host,network layer matrix,application layer host,application layer matrix,user history, probeConfig, rmonConformance. These groups are addition to existing groups in RMON.

3 enhancements are made to RMON so that RMON2 and RMON work well together. DroppedFrames and LastCreateTime are added back to all tables in RMON MIB. New function is added the RMON filter table to filter based on a header offset for any type of protocol even if the protocol header has variable length. Bits 6-9 are newly defined in the filter and capture groups to support WAN and generic media. Enhancements are added to instruments which implements both RMON and RMON2. They are not backward implemented in RMON-compliant only instruments.

Like RMON, there are two kinds of tables in RMON2: control tables and data tables. Control tables are used for configuration and for control of the data tables. Data tables are used for storing statistical data. Since the control tables control the data table, the control tables can only be modified if the entry modified is not active. Entries are modified by a sequence of actions: de-activate an entry, make changes, and then re-activate the entry. RMON2 objects can carry out actions based on the status of their status when the control tables are modified.

Resources are usually allocated when a new row is added to the control table. It is not a requirement, but it is recommended the device to find a row to share before creating new rows in the control table. So that new rows are created at a minimum and resources are not allocated unnecessarily.

In the same group, each object should be unique. When an attempt to create an existing object, an error is returned. When two management applications attempt to create the same object. The first object will be created and the second management application will receive an error.

RMON2 can monitor all network layers. It is not limited to MAC or network layer. It can understand and parse packets from a set of protocol types. The protocol directory keeps track of the set of protocol packets being monitored. The protocol directory can be modified dynamically. The methods of parsing different protocol types are pre-defined. The protocol directory is modified to select a subset of it. Since

it has been expanded into higher network layers, RMON2 focuses on packet level monitoring, and link-level errors are not monitored.

ATM traffic can be counted in RMON2. ATM AAL-5 cell size is used as the frame size to count ATM traffic. But RMON2 has not considered how to capture ATM traffic in the packet capture group. [Internet Draft RMONPROT]

There is a hierarachial layer structure in protocol identifiers. The layers are as follows: base Layer encapsulation Layer and network Layer.

Base layer deals with the hardware dependent aspect of monitoring. RMON2 can support up to 255 kinds of base layer encapsulation. Right now, only 5 base layers are defined. They are Ethernet-II, Logical Link Layer, Sub-Network Access Protocol (SNAP), virtual SNAP packets, and one for non-classified protocol. But this list can be easily expanded by assigning a new base layer value for each new protocol. See table 5. [Internet Draft RMONPROT]

Table 5:Base Layer Encoding Values.

Base Layer	ID
Ether2(Ethernet-II)	1
LLC(Logical Link Layer)	2
SNAP(Sub-Network Access Protocol)	3
Virtual SNAP Packets	4
ianaAssigned(Non-classifed protocol)	5

The next layer is encapsulation layer. It is created specifically for VLAN, Virtual Local Area Network, (IEEE 802.1Q). The final layer is network layer. This layer includes anything from transport protocol to application protocols. These are some example network layers currently defined: TCP/IP, ARP, IP, ICMP, IGMP, GGP, IPIP4, ST, TCP, UCL, EGP, IGP, BBN, NVP2, PUP, ARGUS, EMCON, XNET, UDP, MUX, DCN-MEAS, ...etc. [Internet Draft RMONPROT]

RMON2 has been designed for existing networks. But future networks will have higher capacity. As a result, more information will be collected. RMON2 is currently being extended to support high capacity network. But the proposed standard is still being discussed. The new standard shares a similar format as other RMON2 related standards. Groups are added for new functionalities.

There are 15 new groups defined for high capacity network: mediaIndependentGroup, etherStatsHighCapacityGroup, etherHistoryHighCapacityGroup, hostHighCapacityGroup, hostTopNHighCapacityGroup, matrixHighCapacityGroup, captureBufferHighCapacityGroup, protocolDistributionHighCapacityGroup, nlHostHighCapacityGroup, nlMatrixHighCapacityGroup, nlMatrixTopNHighCapacityGroup, alHostHighCapacityGroup, alMatrixHighCapacityGroup, alMatrixTopNHighCapacityGroup, usrHistoryHighCapacityGroup. These groups are similar to previous group defined in RMON2, but they can process more infomration for high capacity networks. [Internet Draft HCRMON]

RMON and RMON2 are useful standards. There are already companies providing network monitoring solutions using RMON and RMON2 standards. Here is a list of major corporations providing RMON and

RMON2 solutions in table 6.

Table 6: List of major corporations and their RMON-compliant products

Corporation	Product	Implements
3COM	Transcend Enterprise Monitors	RMON, RMON2
Cisco	SwitchProbes	RMON
HP	NetMatrix	RMON2
DEC	clearVISN	RMON

[Back to Table of Content]

Proposed SMON

Traditionally, RMON2 is used to monitor frame-based networks such as Ethernet. As switched networks such as ATM and switched LAN are expanding. RMON2 is being extended to monitor switched networks.This extension is called SMON, Switched network monitoring. This name is not standardized yet. [Internet Draft SMON]

There are several issues in monitoring switched networks that are different from monitoring frame-based networks. First, data in switched networks are connection oriented and a single monitor cannot capture data by listening to broadcasts as in frame-based networks. Second, monitoring end-to-end in a switched network requires many resources. There must be some ways to aggregate the data determined by the management applications. Third, virtual switched networks must also be considered such as VLAN. Fourth, packet prioritization exists in swtiched network. Fifth, SMON focuses on packet monitoring in high layer of the network instead of cells in lower layer.

SMON sees three different kinds of data sources: RMON data source, VLAN data source, and physical data source. RMON data source is defined to be compatible with RMON, VLAN data source is defined to include virtual data source created by VLAN. All other data sources are grouped into physical data source.

A new copy-port feature is addedin SMON to allow traffic from one switched port to be copied to another port. This allow traffic to be monitored on different ports. Copy-port feature can be done in three ways. It can be port-to-port, multiport-to-pot or multiport-to-multiport.

Four bits are added to RMON probeCapabilities bitmask by SMON. These four bits, bit 33-36, are smonVlanStats, smonPrioStats, dataSource and portCopy. smonVlanStats is for VLAN. smonPrioStats allows uses for the user priority in VLAN header. dataSource allows all new data source types to be specified. portCopy allows copy-port functionality.

[Back to Table of Content]

ATM-RMON Standard

ATM-RMON is the remote monitoring standard created for ATM networks. ATM network is more recent technology and its connection oriented feature requires a different set of standards to be developed. ATM-RMON is developed by the ATM forum and is approved as a standard in the middle of 1997. It is the equivalent of RMON and RMON2 developed by IETF.

ATM-RMON is designed based on RMON because of several reasons. First, it is compatible with RMON so that existing RMON applications can run on ATM and reduces the cost of developing new monitoring applications. Second, many protocols currently monitored by RMON are emulated over ATM, and RMON is already used to monitor those data. Third, RMON2 has been added to upgrade RMON and ATM should anticipate compatiblity issues wtih RMON2. [ATM-RMON]

There are several issues being addressed since the beginning of ATM-RMON's development. First, it must provide compatible functions with existing RMON. Second, new functions specific for ATM networks are added. Third, data collection from source is taken into account. Fourth, resource allocation should be flexible. Fifth, data reduction mechanism is incorporated. These issues are addressed in order to make ATM-RMON a more powerful and yet compatible network monitoring standard. As a result, the basic MIB for ATM-RMON is created and it is called ATOM MIB(Please note it is not ATM MIB).

One difference between ATM-RMON and RMON is that ATM-RMON does not implement the hostTopN function and instead, a matrixTopN is implemented. The matrixTopN is a collection of hostTopN in a table. Thus ATM-RMON is more complex in this function. Another difference between ATM-RMON and RMON is that ATM-RMON does not use data source index to identify data source. Instead, it uses global tables to define circuit selection groups.

Even though ATM-RMON is based on RMON, it has incorporated many new features in RMON2 to stay compatible in the future. For example, it has included new TopN functions such as 'last-create-time'; counters are used instead of table size; and ProtocolDirectory selects which protocol to monitor is also included.

ATM-RMON has added basic statistics non-existant in RMON to monitoring ATM specific statistics such as cells-sent count, cells-received count, number of successful call setups, number of attempted call setups, and total connection time.

ATM-RMON has just been standardized. There are still many insufficiencies in this version. First, ATM network is designed to carry data traffic, voice, video and other traffic. But only frame-base traffic is monitored by ATM-RMON. Second, no cell filter nor capture group is specified in ATM-RMON. This is a design decision to hurry the standardization of ATM-RMON.

No standard exists for monitoring cells. Thus monitoring guideline has been suggested to vendors and let the vendors to choose which way to implement. This will allow future standardization easier. There are two options which can vary. The RMON device can be either internal or external. Also, it can allow copy function to copy traffic to another port or disallow it. By the combincation of these two options, four methods are suggested to vendors for implementation.

[Back to Table of Content]

Monitoring Internet

Internet is a network of many networks. Each individual network is owned and operated by different organizations. Monitoring the internet is different from monitoring a single network because in a single network, all components are usually under the control of a single network management, but in the case of internet, each individual network has different base layer platform and is managed by different network management.

Monitoring difficulties

The internet is getting more and more difficult to monitor because more and more users are added to it everyday, and there is a lack of measurements of the quality for the internet as a whole. There is no standardized metric being used in measuring the internet. But usually host response time, time delay, and loss rate are being measured by individual network. The users of the internet has to measure aspects of the internet which tell them the performance of their network applications.

There is no standardized monitoring tool for monitoring the internet. Different people use different tools in monitoring the internet. The most common internet monitoring tools are public domain softwares because they are available for the internet at extremely low cost and also these public domain softwares can be easily customized. Several common public domain softwares used in network monitoring are ping, ftp, and traceroute. [Tutorial] Ping sends a packet of user data to a specific node and the packet is echoed back. This allows the measurement of response time and the percentage of packet loss. Ftp transfers a file from one host to another. This allows the measurement of the data transfer rate. Traceroute sends packets of ICMP,Internet Control Message Protocol, messages to the host. This allows the measurement of number of hops to another host and the performance of the route. There are many other public domain softwares for internet monitoring. For example, arpwatch, nslookup and so on. [Tools List]

Right now, there is no standardized effort in monitoring the internet as a whole and none is being researched and developed. The only way to monitoring the internet now is to use existing public softwares and extend their functionalities. There are couple problems with this approach. First, these public softwares are not intended for monitoring. Their usage eats up network capacity; thus allowing only a small amount of monitoring activities. Second, monitoring the internet is difficult and not many people are doing it. As a result, problems are not often reported and consequently solved infrequently. As a result, the internet performance is degrading. This phenomenon created by the lack of monitoring is referred to "gridlock".[Monitor LAN/WAN]

Objective-driven monitoring

Objective-driven monitoring is a new idea which can be useful to monitor the internet. The basic idea is to use knowledge base to control a large number of sensors installed on the network. These large numbers of sensors can be installed on different parts of network and work together to monitor the

network as a whole. Currently, there is no practical implementation for objective driven monitoring. But it can possibly be applied to internet in the future.

Objective-driven monitoring is designed for monitoring a distributed computing environment which carries a diversed classes of traffic and traffic patterns. Tradition network monitoring uses log files to record the events or states of the network. In objective-driven monitoring, many sensors are installed on the network, but they are not always turned on as in the traditional network monitoring strategies. The number and topology of them to be turned on is determined by a set of rules. A knowledge base is set up to apply the rules and gives instructions on which sensors to be turned on. Then the readings from the sensors can be recorded and analyzed to provide specific answers to questions on network monitoring. For example, the time delay of a packet can be measured by adding up the time delay in the switch buffer, link and the switch fabric.

The conceptual design of the objective-driven monitoring system is simple. The basic unit for the monitoring system is the a system of sensors, a knowledge base, an inference engine. [OD Monitoring]

The locations for installation are studied by the engineers to gather useful information about the network. The sensors are not always activiated. But when they are used, they can monitor real-time and non-real-time traffic. These sensors are basically divided into three types: status sensor, event sensor and derived status sensor. Status sensor records the internal states of the network devices. Event sensor records the actions carried out by the network devices. Derived status sensor manipulates the recorded information and stores it in the form of states.

The knowledge base is a database that serves two purpose. It contains the rules specified how to turn on the sensors and how the data are analyzed.

The inference engine is designed for reasoning on the database. The inference engine consists of the deductive inference processor and the statistical inference processor. The deductive inference processor mainly allows the inference engine to use the rules in the database to deduce which sensors should be turned on. It deals with analyzing the logical rules. The statistical inference processor mainly handles the data collected. It also uses the rules from the knowledge base to analyze the data using mathematical inferences.

[Back to Table of Content]

Summary

Network monitoring is an important funtion in network management because it helps achieve three of the five goals in network management: performance monitoring, fault monitoring, and account monitoring.

SMIv2 is the naming structure used for naming monitored objects. MIB-II defines how the set of objects monitored can be defined. SNMPv2 provides the information exchange and backbone for network monitoring. By adding up SMIv2, MIB-II, and SNMPv2, RMON is born. RMON is the first standard in providing remote monitoring. Bascially, RMON-compliant devices are created to check the status of the network. In RMON, 10 groups are defined. Each of these groups has its own functions in monitoring.

RMON2 is the upgrade to RMON. It adds new functionalities to extend RMON into higher network layer. RMON2 is still being worked on. But extensions of RMON2 are being proposed. One of the more important proposal is SMON, which provides network monitoring to switched networks.

ATM-RMON is designed for ATM networks. This is a new standard based on RMON-like features. There are still many insufficienies, but it is a good start in providing remote monitoring in ATM networks.

In monitoring the internet, simple public domain softwares are used. But there are many problems because these softwares are not originally intended for monitoring. The lack of monitoring on the internet has led to the "gridlock" problem in which the performance of the internet is degrading. Also, a new idea of objective-oriented monitoring is introduced and the idea is to use knowledge base combined with many sensors to determine the status of the network.

Network monitoring is important and network service providers should pay more attention to it.

[Back to Table of Content]

Abbreviation

- ASN.1 --Abstract Syntax Notation One
- ATM -- Asychronous Transfer Mode
- ATM-RMON -- Asychronous Transfer Mode Remote Monitoring
- ATOM-MIB -- The basic MIB for ATM-RMON
- ICMP -- Internet Control Message Protocol
- IETF -- Internet Engineering Task Force
- LAN -- Local area network
- OSI -- Open Systems Interconnect
- MAC -- medium access-control layer
- MIB -- Management Information Base
- MIB-II -- Version 2 of Management Information Base
- RMON -- Remote Monitoring
- RMON2 -- Version 2 of Remote Monitoring
- SMI -- Structure of Management Information
- SMIv2 -- Version 2 of Structure of Management Information
- SMON -- Switch Network Monitoring
- SNMP -- Simple Network Management Protocol
- VLAN -- Virtual Local Area Network
- WAN -- Wide Area Network

Reference

Here is a list of reference listed in categories and then in order of usefulness:

RMON

- [Stallings Book] William Stallings "SNMP, SNMPv2, and RMON Practical Network Management, Second Edition" Addison-Wesley Professional Computing and Engineering 1996. A good general reference in basics of RMON.
- [RFC 1757] S. Waldbusser "Remote Network Monitoring Management Information Base" http://www.cis.ohio-state.edu/htbin/rfc/rfc1757.html Technical specification for RMON
- [RMON device] Jeff Huges "Characterizing Network Behavior Using Remote Monitoring Devices" Telecommunications v29 n3 Mar 1995 p43-44

RMON2

- [RFC 2021] S. Waldbusser "Remote Network Monitoring Management Information Base Version 2 using SMIv2" http://www.cis.ohio-state.edu/htbin/rfc/rfc2021.html Technical specification for RMON2.
- [Internet Draft RMONPROT] Andy Bierman, Chris Bucci, Robin Iddon "Remote Network Monitoring MIB Protocol Identifiers"Proposed technical specification for RMON2 protocol identifiers.
- [Internet Draft HCRMON] S. Waldbusser "Remote Network Monitoring Management Base for High Capacity Network" Proposed tehnical specification for RMON of high capacity network.

SMON

- [Internet Draft SMON] Richard Waterman, Bill Lahaye, Dan Romascanu, Steve Waldbusser "Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0" Proposed technical specification for RMON of swtiched networks.

ATM-RMON

- [ATM-RMON] The ATM Forum Technical Committee "Remote Monitoring MIB Extensions for ATM Networks" ftp://ftp.atmforum.com/pub/approved-specs/af-nm-test-0080.000.pdf Technical specifiation for ATM-RMON.

Monitoring Internet and Network in general

- [OD Monitoring] Subrata Mazumdar and Aurel A. Lazar "Objective-Driven Monitoring For Broadband Networks" IEEE Transactions on Knowledge and Data Engineering v 8 n 3 Jun 1996. p 391-402 A research paper on objective oriented monitoring.

- [Tutorial] Les Cottrell and Connie Logg, SLAC "Tutorial on WAN Monitoring at SLAC" http://www.slace.stanford.edu/comp/net/wan-mon-tutorial.html A tutorial paper on monitoring on Wide Area Network including the internet.

- [Tools List] Les Cottrell "Network Monitoring Tools" http://www.slac.stanford.edu/~cottrell/tcom/nmtf_tools.html A good list of network monitoring tools.

- [Monitor LAN/WAN] Less Cottrell and Connie Logg, SLAC "Network Monitoring for the LAN and WAN" http://www.slac.stanford.edu/grp/scs/net/talk/ornl-96/ornl.html A tutorial paper on internet monitoring in general

- [Performance Management] Theodore K. Apostolopoulos and Victoria C. Daskalou "On the Implementation of a Prototype for Performance Management Services" IEEE symposium on computers and communications 1995 p57-63. A research paper on a prototype for management services.

- [Checklist] Frank A. LeFavi "Network Quality Assurance: A Checklist" Telecommunications July 1995 p.56-60. An article discussing what to look for in network monitoring.

[Back to Table of Content]

Last modified Aug 14th, 1997