Tech Info Library

SNMP Technical Introduction, Part 1 of 3

Revised: 11/24/92
Security: Everyone

SNMP Technical Introduction, Part 1 of 3

==========

Article Created: 10 November 1992

TOPIC ----------

This is the first of three articles that introduce SNMP (Simple Network Management Protocol). This article describes the evolution of management and troubleshooting tools used by network administrators, and describes network management for the Macintosh.

DISCUSSION ----------

Introduction

Since the early days of data communications, network administrators have been searching for ways to increase the availability, usefulness, and performance of their networks.

The networking environment has also changed. Data communications has become much more complex since the days of point-to-point low-speed serial connections. Today's networks consist of not only traditional point-to-point connections, but include LANs (Local-Area Networks) serving distributed databases, network servers, and other services. The ability to centrally administer services, configure network devices, detect and diagnose problems, and plan for future growth has become critical to the successful operation of any large network.

Packet Analyzers

One of the first tools developed was the packet analyzer. Early packet analyzers consisted of dedicated hardware and software, such as the Hewlett-Packard Datascope, or (more recently) Network General's Sniffer.

These devices capture and analyze network packets. They must be physically connected to the cable segment being monitored in order to see all the traffic. Packet Analyzers operate at the Physical and Data Link layers of

the OSI model. To decode and analyze the captured packets, the packet analyzer must understand the various protocols on the cable. Furthermore, to monitor connection-oriented protocols, the packet analyzer must maintain the state of the connection so it can understand the actions of the entities involved.

Interpreting and analyzing network packets usually requires technical knowledge of the protocols, so packet analyzers are used mainly by experienced network administrators.

Recently, various vendors have developed lower cost, lower performance packet analyzers which run on desktop computers. For example, the AG Group's EtherPeek and LocalPeek, and Neon Software's NetMinder Ethernet and NetMinder LocalTalk products run on the Macintosh.

Network Monitors

The second type of passive network management tool is the Network Monitor. A monitor observes network traffic to keep track of various services and other important network information. These products typically issue a warning if a service suddenly disappears, or if there is something odd about the traffic originating from a particular node. Network monitors rely on the traffic output by various services on the network, so are very useful in environments where services advertise themselves, such as AppleTalk.

Monitoring at the Transport and Network layers of the OSI model provide further advantage.

A number of Network Monitor tools have emerged for AppleTalk environments, including NetWatchman and TrafficWatch II. While network monitors are more useful in managing networks than packet analyzers, they still do not allow control of the network.

Pro-Active Network Management

The third class of tools involve pro-active network management. These tools can manage network routers, bridges, gateways, nodes, servers and other devices on the network. In multi-vendor networking environments, this is still a developing field. Perhaps the biggest risk of pro-active management is the security scheme implemented to prevent unauthorized manipulation of the network and its resources. And of course, everyone on the network must agree on the management protocol in order for this to be successful on a multi-vendor network.

Historically, the software to manage a particular networking device has been provided by the vendor of that device. Because no standards existed until recently, a specific vendor's console usually could not manage other vendors' devices, unless it was specifically designed to do so. As networks grew, customers often found themselves connecting networks with products from different vendors, and trying to manage their networks using different, and incompatible, management software. Consequently, managing large networks was, and still is, fairly difficult.

Pro-active network management requires access to all seven layers of the OSI model, as services such as file servers and print spoolers require management at the application layer.

SNMP is a good example of a tool with good pro-active management potential. SNMP has a number of advantages over proprietary management schemes, and these will be discussed in detail later.

Network Management and AppleTalk

AppleTalk networks are really no different from others in regards to troubleshooting, monitoring, and active management.

Many of Apple's customers, especially large customers, have been asking for tools to manage Macintosh computers and AppleTalk networks for a number of years.

Tools such as Apple's Inter•pol, and products like Status•Mac from Pharos Technologies and GraceLAN from Technology Works, Inc. have attempted to address this need through proprietary protocol implementations using AppleTalk as transport.

Recently, this demand has risen dramatically, as customers increasingly interconnected their networks and as network management solutions standards, like Simple Network Management Protocol (SNMP), started emerging. MacIS (a Macintosh users group consisting of Management Information Systems professionals) has put network management from Apple near the top of their wish list for two years (1990-91). In 1991, they further specified that this solution should be SNMP-based.

Recently, Apple had embarked on a strategy to implement yet another proprietary network management scheme utilizing new AppleTalk protocols, AppleTalk Management Protocol. In the process of creating this product, feedback from our customers, field support and sales staff, as well as internal project participants leads to a decision to change the direction of our network management strategy.

Instead of inventing a new protocol, the team decided to adopt an open industry-standard implementation leveraging off existing management and transport equipment and software -- a direction strongly supported by our customers, field support, sales staff, and organizations such as MacIS.

Besides addressing a major customer need with SNMP based network management products, Apple has an opportunity to have a major impact on the Internet-standard Network Management framework definitions, particularly those that address the AppleTalk environment. Further, this enhances the ability of Apple and third parties to develop unique and state of the art tools to aid in the design, setup, management and growth of new existing AppleTalk based devices in a multi-vendor, multi-protocol, environment.

Tech Info Library Article Number:11015