第 V 部

ネットワーク管理とセキュリティ

第 5 部
ネットワーク管理とセキュリティ

第 1 章 Introduction

The Netman Working Group has been carrying out research and development to make the Internet more manageable and secure. This has basically involved designing, developing and implementing MIBs for new protocols like Mobile IPv6 (MIP6) protocol, Network Mobility (NEMO) protocols and for existing protocols like the syslog protocol. In this report chapter 2 we describe the detail of NEMO-MIB.

On another track research and development is continuing on event detection, event notification and event diagnosis. For more detail about "event", please refer to `wide-memo-netman-event-00.pdf` published in last year. We have worked to expand the scope of event based management from the local domain to the open Internet. Event information may be shared over the Internet using a standard protocol and event format. That opens up a new area of research of correlating events that are happening across the Internet. For example, the spread of a virus, a large-scale concerted attack, a massive network failure etc. Each of these may cause incidents at globally dispersed regions. But, when correlated and connected the picture of the growth of the potentially snowballing incident may be constructed and the future course may be predicted. This facility will go a long way in securing the network and society.

第 2 章 NEMO-MIB: A MIB module for Network Mobility

2.1 Introduction

The growing demand for mobile and ubiquitous Internet access requires standard protocols that support node and network mobility for continuous network connection and services. Mobile IPv6 (MIPv6)[78] specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. Network Mobility Basic Support (NEMO)[31] is an extension to the Mobile IPv6 protocol which supports the movement of an entire network.

The open nature of the Internet, its protocols and the wide variety of its implementations makes it mandatory to standardize the management framework for deploying and operating these new technologies. A detailed overview of the documents that describe the current Internet-Standard Management Framework, are given in RFC 3410[23]. Management is carried out by referring to or setting the value the "Managed object" which is an abstract representation of the desired facet of the managed device. Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). The MIB module for MIPv6 entities, the MIPv6-MIB has been designed and is now a proposed standard[84]. This document describes the NEMO-MIB, a set of managed objects (MOs) that can be used to monitor and control NEMO entities.

2.2 Need of NEMO management

Management framework for traditional Internet has developed at a rapid pace. SNMP has been deployed as the standard protocol for monitoring and controlling Internet entities, routers, switches and servers. Entities connected to the Internet in general service MIB modules that have been defined to allow monitoring and configuration of the entity.

The *Mobile router* introduced by NEMO is a new entity in the Internet. It is basically a router with the additional functionality for mobility support that traditional routers don't have. This is the first case that the SNMP-based framework is applied to a mobile network environment.

The mobility of the target network and or router introduces some new aspects to network management particularly the mobility related status, parameters and metrics. The NEMO-MIB is designed to service these requirements.

2.3 Overview of NEMO-MIB

NEMO is a simple extension of MIPv6. The MIPv6 framework is described in terms of 3 types of entities — the mobile node (MN), correspondent node (CN) and home agent (HA). The NEMO framework has one entity called mobile router (MR) added to basic MIPv6. One of the key points of NEMO-MIB is to provide MOs to manage mobile router.

Typically mobile routers implement NEMO functionality for achieving network mobility. However, a mobile router may also function as a mobile node.

We are developing NEMO-MIB based on proposed standard MIPv6-MIB. There are 2 major parts in NEMO-MIB. The NEMO specific part and the MIPv6-MIB extension part.

NEMO-MIB comprises of the following major groups:

- nemoNotifications
- nemoSystem
- nemoConfiguration
- nemoStats
- nemoConformance

NEMO specific MOs are defined in these groups.

The nemoNotifications group defines the notifications generated by the NEMO entity in response to the operationally interesting state changes in the NEMO protocol. The nemoSystem group provides the general information of the NEMO entity. The objects in this group cover the current home registration state. The nemoConfiguration group contains information relevant to the implementation and operation of the NEMO protocol. The nemoStats group defines the statistics related to the NEMO protocol operations. The nemoConformance group identifies the managed objects that need to be implemented for conforming to this draft.

The MIPv6-MIB extension part comprises of the following groups:

- nemoBindings
- nemoMr
- nemoCn
- nemoHa

The nemoBindings group defines MOs that correspond to the extensions to the binding cache related information defined in MIPv6-MIB. The nemoMr group corresponds to Mobile Router (Mobile Node that supports NEMO). The nemoHa group corresponds to Home Agent that supports NEMO. Now nemoCn group is empty. Some MOs may be added the need arises.

2.4 Development of NEMO-MIB

2.4.1 Usefulness of NEMO-MIB

As mentioned above, NEMO-MIB can provide information about roaming status of a mobile router. One example of a useful application is, controlling the quality of streaming to a node that is connected to the mobile router. If the mobile router connects to a narrow bandwidth link, the streaming quality is affected. In this case, it is difficult for a node that receives a stream to notice changes upstream. NEMO-MIB can be utilized to monitor when and where the mobile router roams.

Of course the mobile router can provide upper link status, and traffic information of a receiver node. It makes it easy to control the streaming quality based on the situation of a receiver node. There are many researches about controlling QoS in a mobile environment. NEMO-MIB will provide the framework for the development of useful tools for these works.

2.4.2 Implementation and Security Issues

NEMO-MIB focuses on the management of a NEMO entity. The MIPv6-MIB[84] defines the managed objects for a mobile node. Implementations supporting both the mobile node and NEMO functionality SHOULD implement the managed objects defined for the NEMO entities and mobile nodes from both the MIPv6-MIB and NEMO-MIB.

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. Some of the readable objects in this MIB module may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

It is recommended that implementers consider the security features as provided by the SNMPv3 framework[23], including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy). It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

2.5 Conclusion

This document describes an overview of NEMO-MIB for the new mobility protocol, NEMO. It also considers about some implemention issues.

第 3 章 Conclusion and Future Works

In the area of plain and simple network management, new areas are emerging. E.g. the area of management of wireless LANs. Wireless LANs are getting deployed at a quickening pace. Yet the issues of management specific to wireless LANs are not well understood or addressed. From the management and security point of view, it should always be possible to track down the source of traffic in a network. However, in a wireless environment the source itself maybe on the move. This will mean, by the time a suspicious traffic has been noticed and tracking of the traffic is attempted the source may have moved. This can make it very difficult to track the location of the physical source of network traffic. This will require detecting and recording the connections of terminals, an area that has not been explored in detail. Concepts of connection, disconnection and reconnection will need to be reviewed and revised. These will determine the rate at which the connection history will grow and how effective the connection history will be in linking a terminal to its activities.

In this area we are starting wireless network monitoring on an operational wireless campus network. We will investigate the issues during the period 2008-01–03 and then attempt to address the issues.