Automatic Remote Firmware Upgrade Algorithm through Internet for DOCSIS Cable Modems

Hong-Ik Kim[1] and Sung-Kwon Park[2]
[1] Department of Electronic and Communications Engineering, Hanyang University,
17 Hangdang-Dong, Sungdong-Gu, Seoul, Korea
Tel. +82-2-2294-0366, Fax.: +82-2-2281-9912
[2] Division of Electrical and Computer Engineering, Hanyang University,
17 Hangdang-Dong, Sungdong-Gu, Seoul, Korea
Tel. +82-2-2294-0366, Fax.: +82-2-2281-9912
e-mail : hongik@ihanyang.ac.kr, sp2996@hanyang.ac.kr

Abstract: This paper introduces a new web based method to remotely upgrade firmwares of Cable Modems (CM) which are integral part in providing high-speed Internet access through Hybrid Fiber Coaxial (HFC) networks. Also, it discusses various practical problems arising in the upgrading process. Traditional upgrade has been performed by modifying the CM configuration file. This paper shows a new web based CM firmware upgrade method using SNMP and MIB which greatly reduces upgrading time, cost and man-hour than traditional firmware upgrade methods. This method has been shown to be very efficient and practical. This method will make significant impact especially because tens of million cable modems are currently waiting to be upgraded soon to the next version from the current version.

1. Introduction

In the past few years, there has been so much advances in access networks to provide high speed internet to homes. ADSL (Asymmetric Digital Subscriber Line) modems and cable modems have been successful to provide additional paths to home without installing new cables. In Korea, about 5 millions of ADSL modems and 3 millions of cable modems have been deployed in the last several years.

Cable Modem (CM) technology is being developed to provide high-speed multimedia services to the subscribers' homes over the existing Hybrid Fiber Coax (HFC) infrastructure of cable TV networks.

A cable TV network consists of a headend, distribution center, fiber nodes, coaxial cable, and various transmission amplifiers. At the end near a home, there is a tap off to connect the coaxial network within the home. The headend receives information such as television signals, Internet packets, and streaming media, then delivers them home. Most modern cable networks already have fiber-optic backbones. CM's are able to receive up to 30Mbps in the downlink and 320Kbps to 10.24Mbps in the upstream link.

Currently, HFC networks are being considered as a most advanced access network technology without the need for any rewiring.

CM's performance is determined by the CM firmware version. Thus, CM cannot execute its fundamental functions with faulty firmware. For example, DOCSIS (data over cable service interface specification) 1.0 CM's can not provide toll quality VoIP (Voice over Internet Protocol) service while DOCSIS 1.1 CM's can. Most of CM manufacturers are now manually upgrading CM firmware. A CMTS manager usually reset all CMs after the CM configuration file is modified. This process poses some problems. First, this process can upgrade only one kind of CM at a time. It is improper in general especially when many kinds or a number of different types of CM's exist at the same time. Second, CM upgrade may frequently fail in the middle to process. This can take place when the upgrade is erroneously stopped due to packet loss and when some CM's may be inadvertently skipped by manager's operation mistakes. Therefore reliability in the firmware upgrade cannot be guaranteed. Third, the inactive (power off) CM cannot be upgraded. Hence the manger should keep trying upgrade many times. Fourth, this traditional upgrade process requires constant attention of the manager during the whole upgrading process. Fifth, the manger may make mistakes in operating CMTS. This may lead to some fatal errors in CMTS to cause crash of the whole HFC data network system.

In this paper, a new CM firmware upgrade process is suggested so that it can minimize the upgrade time, human interface and various errors including some fatal ones. In addition, many different kinds of CM firmwares can be simultaneously upgraded. Obviously, the reliability becomes high because the hardware (manufacture, model type, model version and so forth) classification information of CM's is detected through MIB (Management Information Base) in Simple Network Management Protocol (SNMP).

2. SNMP and DOCSIS Cable Device MIB

2.1 SNMP

The TCP/IP standard for network management uses the Simple Network Management Protocol (SNMP). SNMP was considered for the purpose of network management in IAB (Internet Activities Board). The protocol has evolved through its three generations. Consequently, the current version is known as SNMPv3. The changes have been minor – all versions use a similar general framework. Many features are backward compatible. [6]

SNMP consists of three services of [Get], [Set] and [Trap] messages. [Get] asks the system to send related information from an agent to a manager system and [Set] modifies information in the agent system if the manager system asks.

And [Get] and [Set] are made in the manager system and executed in the agent system, and [Trap] is made in the agent system and reported to the manager system. In this paper MIB object ID represents [ ] symbol, and MIB value represents ' ' symbol for convenience.

2.2 DOCSIS Cable Device MIB

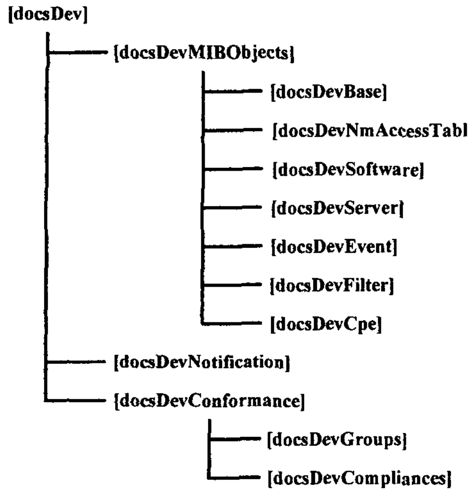

Figure 1. DOCSIS cable device MIB structure, [docsDev] contains various DOCSIS cable devices information.

Figure 1 shows the tree structure of DOCSIS cable device MIB. It is defined by IETF (Internet Engineering Task Force) and this provides device information on CM. This organizes [docsDevMIBObjects], [docsDevNotification], and [docsDevConformance] of CM device information. Among them this paper concentrates on [docsDevMIBObjects], because CM firmware upgrade is related with [docsDevMIBObjects]. [docsDevMIBObjects] consists of five object identifications. [docsDevMIBObjects] provides [docsDevBase], [docsDevNmAccessTable], [docsDevSoftware], [docsDevServer], [docsDevEvent], [docsDevFilter], and [docsDevCpe] of CM. In [docsDevBase], elementary hardware information such as time, serial number, device reset, and current role of device is provided. Device access IP, IP mask, community, and interface information can be found in [docsDevNmAccessTable], Firmware information is defined in [docsDevSoftware]. Information of TFTP (Trivial File Transfer Protocol) and DHCP (Dynamic Host Configuration Protocol) firmware server can be found in [docsDevServer]. Information of device event occurrence is in [docsDevEvent]. Information of CPE is found in [docsDevCpe]. In this paper, the newly suggested CM firmware algorithm uses [docsDevSoftware] among them. Following section gives a full explanation on [docsDevSoftware]. [3]

2.3 [docsDevSoftware]

[docsDevSoftware] consists of five objectID. They are [docsDevSwServer], [docsDevSwFilename], [docsDevSwAdminStatus], [docsDevSwOperStatus], and [docsDevSwCurrentVers]. The Figure 2 shows the structure of [docsDevSoftware] used for the CM firmware upgrade. [docsDevSwServer] indicates the IP address of TFTP server used for the CM firmware upgrade. [docsDevSwFilename] indicates the file name of the firmware to be loaded into CMs to be upgraded. [docsDevSwAdminStatus] gives the CM commands with respect to firmware upgrade.

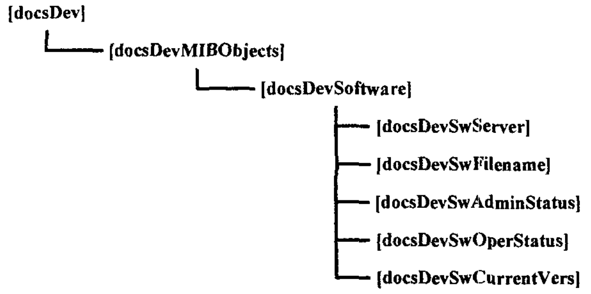

Figure 2. [docsDevSoftware] tree structure, [docsDevSoftware] composed five objectIDs.

For example if [docsDevSwAdminStatus] is set to 'upgradeFromMgt(1)', the device will initiate a TFTP software image download using [docsDevSwFilename]. After successfully receiving an image, the device will set its state to 'ignoreProvisioningUpgrade(3)' and reboot. If download process is interrupted by a reset or power failure, the device will load the previous image. After re-initialization, it continues to attempt to load the image specified in [docsDevSwFilename]. If [docsDevSwAdminStatus] is set to 'allowProvisioningUpgrade(2)', the device will use the software version information supplied by the provisioning server until the next rebooting (this does not cause a reboot). When [docsDevSwAdminStatus] is set to 'ignoreProvisioningUpgrade(3)', the device will disregard software image upgrade information from the provisioning server. Note that reading this object can return 'upgradeFromMgt(1)'. This indicates that a software download is currently in progress and that the device will reboot after successfully receiving an image. At initial startup, this object has the default value of 'allowProvisioningUpgrade(2)'.

[docsDevSwOperStatus] indicates the progress of a CM firmware in upgrading. 'InProgress(1)' indicates that a TFTP download is underway, either as a result of a version mismatch at provisioning or as a result of a 'upgradeFromMgt(1)' request. 'CompleteFromProvisioning(2)' indicates that the last software upgrade was a result of version mismatch at provisioning. 'CompleteFromMgt(3)' indicates that the last software upgrade was a result of setting [docsDevSwAdminStatus] to 'upgradeFromMgt(1)'. 'Failed(4)' indicates that the last attempted download failed ordinarily due to TFTP timeout.

[docsDevSwCurrentVers] indicates the firmware version currently operating in CM. This object should be in the syntax used by the individual vendor to identify software versions. [3]

3. Cable Modem Firmware Upgrade

CM firmware is upgraded through [docsDevSoftware] information by SNMP [Set] order. During firmware upgrade procedure, CM manufacturer and model is classified. CM firmware state is inspected after CM firmware upgrade. If CM firmware state is abnormal, SNMP retry upgrade procedure.

3.1 Cable Modem firmware upgrade algorithm

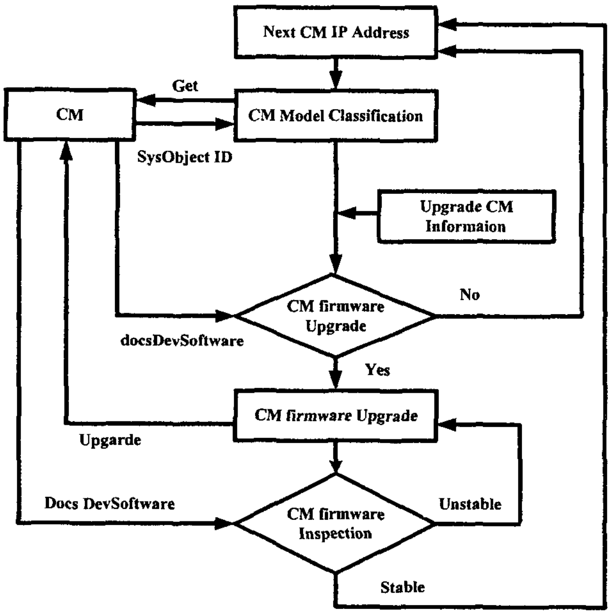

Figure 3. Cable Modem firmware upgrade algorithm

The Figure 3 shows a block diagram of the CM firmware upgrade algorithm. The Figure 3 represents that CM firmware upgrade IP range decided. CM's within the IP address range are first found, and then the manufacturer and the model of the CM are identified. And proper MIB should be applied according to a corresponding model, and the firmware should be upgraded if necessary after CM firmware information is identified. After the firmware is upgraded, the state of the upgrade firmware should be checked and if errors are found, the upgrade should be executed again. If the upgrade procedure is completed, the next CM within the IP address range is found.

3.2 Identification of Cable Manufacturer and Model

In order to properly upgrade the CM firmware, the manufacturer and the model of the CM must first be identified. If CM's are not classified correctly following the firmware upgrade requirement, it is impossible to upgrade properly CM firmware simultaneous. Thus it is very important to correctly classify the manufacturer and the model of the CM.

This information can be obtained from [sysObjectID] and provides a very important clue to identify the manufacturer and the model of the CM.

For example, once the manufacturer and the model of the CM are obtained by [sysObjectID] using SNMP. A response such as ".iso.org.dod.internet.private.enterprises.-236.100.1.1.1.206.1" is returned and a manufacturer is identified according to the numbers following ".iso.org.-dod.internet.private.enterprises".

CM [sysObjectID]	Description
.iso.org.dod.internet.private .enterprises.236.100.1.1.1. 206.1	Manufacture: 236 (Samsung) Model : 100 (SCM100) Hardware version : 1.1 Software version : 1.206.1

Table 1. Samsung CM [sysObjectID] description

The Table 1 introduces CM model identification method. Samsung CM [sysObjectID] information is presented in the form of .org.dod.internet.private.enterprises.236.*αα.ββ.ββ.-ηη.ηη.ηη*". Number *αα* indicates CM model. *ββ* is use for CM hardware version. *ηη* is for CM firmware version.

3.2 Cable Modem firmware upgrade

The CM firmware state information is obtained through [docsDevSoftware]. Particularly, [docsDevSwFilename] indicates the CM firmware filename, and [docsDevSw-OperStatus] indicates CM firmware condition. So the CM [docsDevSoftware] information is checked prior to CM firmware upgrade. This procedure finds whether [docsDevSwFilename] is the file name to be upgraded and then whether [docsDevSwOperStatus] is set to be 'completeFromMgt(3)' or not. 'completeFromMgt(3)' indicates that the last attempted download is successful.

When this information is different from the wanted firmware file name and download success information, the CM is registered to be an object to be upgraded and upgrade is realized in accordance with the procedures.

[docsDevSwServer], [docsDevSwAdminStatus] and [docs-DevSwFilename] are set to be the TFTP server IP Address, 'upgradeFromMgt(1)' and a wanted upgrade firmware file name, and then the CM starts to download the firmware from the TFTP server. [4][5]

Unless upgrading is completed as wanted, upgrade should be retried. When this procedure is finished, the CM with the next IP address in the range is upgraded.

4. Experiment Setup

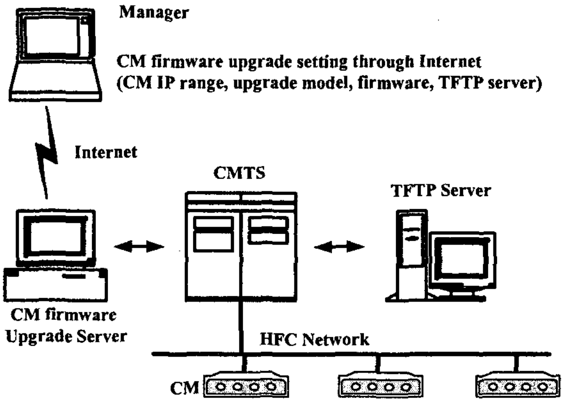
Manager
CM firmware upgrade setting through Internet
(CM IP range, upgrade model, firmware, TFTP server)
Internet
CMTS
TFTP Server
CM firmware Upgrade Server
HFC Network
CM

Figure 4. CM firmware upgrade algorithm test environment

The Figure 4 shows experimental field setup. Manager controls the firmware upgrade server through Internet using a web browser. In this test, Miscrosoft Ineternet Explorer Version 5 was used. The firmware upgrade server performs the proposed CM firmware upgrade algorithm in this paper, and the upgrade server gateway IP address is set as the router IP address. The CMTS was Cisco 7200 series router. All server systems were running Windows 2000. The number of CM's connected was about 2400. The exact number was not known because the number of the available CM's under CMTS varied frequently. The various models of CM's were under the CMTS. The HFC network was in the normal state during the experiment.

The proposed CM firmware upgrade algorithm was compared with a traditional firmware upgrade method in the experiment environment.

4. Result

In this experiment, the CM firmware upgrade error rate, the number of operator interventions and the number of successfully upgraded CM's for one time operator intervention were measured. These results of CM firmware upgrade methods are compared. The CM firmware upgrade error rate is defined as the percentage of CM's failed in the upgrade process.

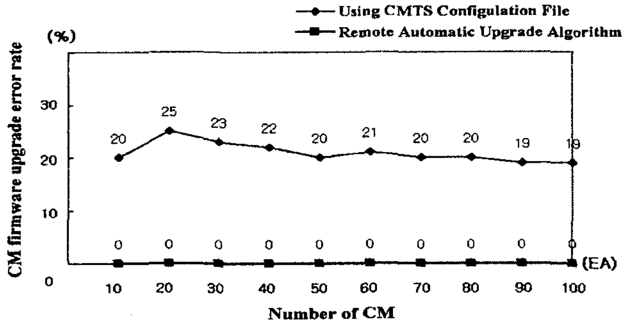

Figure 5. CM firmware upgrade error rate: The traditional upgrade method error rate is higher than the proposed automatic firmware upgrade algorithm.

CM firmware upgrade error rate is shown in Figure 5. This graph shows that the error rate by the traditional upgrade method was on the average 20%. The error rate of the newly suggested firmware upgrade algorithm was 0%. The CM firmware state inspection procedure after upgrade reduces the error rate. Therefore the proposed algorithm greatly improved the reliability of the firmware upgrade.

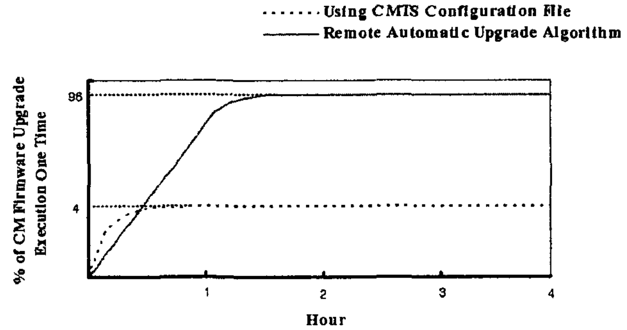

Figure 6. The number of CM's successfully upgraded for one time upgrade. In this experiment, 200 CM's were under a CMTS. Traditional upgrade method can upgrade for only one CM model. However, the newly suggested automatic upgrade algorithm simultaneously upgrade many different models of CM's.

The percentage of successful CM firmware upgrades per one time operation is shown in Figure 6. This graph show that traditional upgrade method was approximately 4% while the proposed algorithm was approximately 96%. The rest of 4% failed because these CM's were deactivated for a long time. The CM identification was possible for many different kinds of CM models.

6. Conclusion

This paper has suggested a remote CM firmware upgrade algorithm through the web. The test result shows clearly the algorithm resolve many problems of traditional upgrade methods. It greatly reduces the upgrading time, operator's intervention, and cost. Beside, many different types of CM models can be upgraded simultaneously from a remote place through the web.

In addition, the upgrade reliability has been increased because the manufacturer and the model information of a CM is detected through the MIB information. Hence the firmware upgrade can be done independent with the hardware. The details of the algorithm and the results out of a field test were included in this paper.

References

[1] K. McCloghrie, M. Rose, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, IETF RFC 1213, March. 1991.

[2] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing SNMP Management Frameworks," IETF RFC 2271, January. 1998.

[3] M. St. Johns, DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, IETF RFC 2669, August. 1999.

[4] *Data-Over-Cable Service Interface Specifications : Radio Frequency Interface Specification SP-RFIv1.1-107-010829* DOCSIS, August 2001.

[5] *Data-Over-Cable Service Interface Specifications : Baseline Privacy Plus Interface Specification SP-BPI+-I07-010829* DOCSIS, August 2001.

[6] Douglas E. Comer, *Internetworking With TCP/IP*, Prentice Hall, 2000

[7] http://www.docsis.org

[8] http://www.cablelabs.com

[9] http://java.sun.com