트래픽 폭주 공격 유형 분석 및 대응 방법에 관한 연구

박원주, 서동일*
*한국전자통신연구원 정보보호연구본부 네트워크보안연구부

The Attack types and Respond mechanisms of Traffic Congestion

*Wonjoo PARK, Dongil SEO**
**Information Security Technology Division, ETRI*
E-mail : [wjpark,bluesea]@etri.re.kr

요 약

최근들어 네트워크 트래픽 폭주 공격에 의한 피해 사례가 속출하고 있다. 지난해 7월, 전세계적으로 많은 피해를 일으켰던 코드레드(CodeRed)공격뿐만 아니라 지난 1월 전국의 인터넷망을 마비시켰던 1.25대란 역시 트래픽 폭주 공격으로 국가적인 차원에서 많은 손실을 일으켰던 대표적인 사례이다. 흔히 인터넷 대란이라고 일컬어지는 트래픽 폭주 공격 및 웜해킹은 갈수록 경제적인 손실 및 피해규모가 커지고 기법도 다양해지도 있어, 트래픽 유형 분석 및 대응에 관한 연구가 필요하다.

본 고는 이러한 트래픽 폭주 공격의 개념을 정의하고 유형별로 분석하고자 한다. 또한 소규모 망에서 기존의 네트워크 장비 및 서버를 이용하여 이 공격들을 대응할 수 있는 방법을 제시하고자 한다.

키워드
트래픽 폭주, DoS, DDoS, 웜해킹, 트래픽 수집, 트래픽 분석

1. 서 론

최근 들어 대학과 연구소, 기업들이 인터넷의 열풍 속에 대부분의 업무들을 인터넷에 크게 의존하고 있다. 전자 우편 서비스뿐만 아니라, 분산 업무처리방식이 도입으로 네트워크를 이용한 업무가 증가함에 따라 대형화 및 복잡화되었고, 이에 따른 보안의 위협도 날로 커지고 있다. 그중에서도 최근들어 가장 빈번하고 심각한 보안의 위협 사례가 네트워크 트래픽 폭주 공격에 의한 피해이다. 지난해 7월, 전세계적으로 많은 피해를 일으켰던 코드레드(CodeRed)공격뿐만 아니라 지난 1월 전국의 인터넷망을 마비시켰던 1.25대란 역시 트래픽 폭주 공격으로 국가적인 차원에서 많은 손실을 일으켰던 대표적인 사례이다. 흔히 인터넷 대란이라고 일컬어지는 트래픽 폭주 공격 및 웜해킹은 갈수록 경제적인 손실 및 피해규모가 커지고 기법도 다양해지도 있어, 트래픽 유형 분석 및 대응에 관한 연구가 필요하다.[1]

본 고는 이러한 트래픽 폭주 공격의 개념을 정의하고 유형별로 분석하고자 한다. 또한 소규모 망에서 기존의 네트워크 장비 및 서버를 이용하여 이 공격들을 대응할 수 있는 시스템을 제시하고자 한다.

2. 트래픽 폭주 공격

2.1 트래픽 폭주 공격의 개념

최근의 해킹 방법은 1988년 인터넷 웜 사건을 이후로 버퍼 오버플로우 공격과 1990년대 DoS 공격 그리고 2000년대의 DDos공격, 웜 해킹 등 그 방법이 다양화되고 더욱 위험성이 증가하고 있다. [표 1]은 해킹 방법의 변천을 보여주고 있다.[1]

[표 1. 해킹 기법의 변화]

연 도	공 격 유 형
1980년대 초	패스워드추측, 웜 바이러스
1985년	패스워드 크랙
1980년대	후반 시스템의 취약점 공격
1980년대 말	백도어

1990년대	스니핑,세션하이제킹,스푸핑
1995년 이후	CGI-attack, 버퍼 오버플로우
1997년	트로이 목마
1990년대 말	DoS 공격

최근의 네트워크 보안의 주류는 [표 1]에서 보듯이 DDoS 공격과 슬래머 웜과 같은 웜에 의한 트래픽 폭주 공격이다. DoS 공격은 공격자의 컴퓨터로부터 대상 시스템과 그 시스템이 속한 네트워크에 과다한 패킷을 보냄으로써 시스템과 네트워크의 성능을 급격히 저하시켜 시스템에서 제공하는 서비스들을 인터넷 사용자들이 이용하지 못하게 하는 기법이다. 이를 발전시킨 DDoS 공격이란 많은 수의 호스트들에 패킷을 범람시킬 수 있는 DoS 공격용 프로그램을 분산 설치하여 이들이 서로 통합된 형태로 어느 대상 시스템에 대하여 일제히 패킷을 범람시킴으로써 시스템 및 네트워크의 성능저하 또는 시스템을 마비시키는 기법을 말한다.

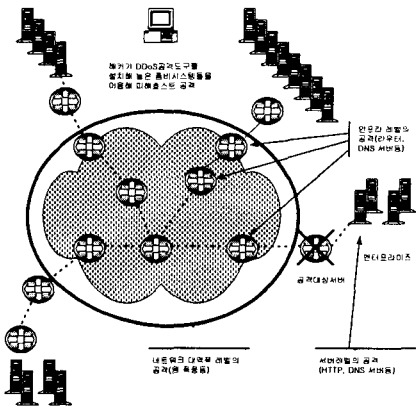
과거의 공격이 서버 시스템에 침투해서 정보를 가져오는 형태를 띄었다면 최근의 공격은 전 세계적으로 연결되어 있는 네트워크를 통해서 불특정 다수의 시스템 및 네트워크에 트래픽을 전송하여 시스템의 기능을 상실시키는 DDoS 공격이 주를 이루고 있다. 2000년 초 야후, 아마존과 같은 대규모 서비스 공급 시스템이 DDoS 공격에 의해 공격당하고, 2002년 말경에도 전 세계의 최상위 네임서버가 DDoS 공격을 당하는 등 DDoS 공격에 의한 피해가 속출되고 있다. DDoS 공격은 이전의 DoS 공격보다 단시간 내에 많은 트래픽을 발생시키며, 공격툴 또한 누구나 쉽게 인터넷상에서 접할 수 있고 사용하기가 쉬워 그 피해가 점점 늘어가고 있는 실정이다. 또한, 인터넷에 연결된 수많은 Slave들에 의해 공격이 행해지며 공격자는 자신의 근원지 IP 주소를 속여서 피해호스트로 패킷을 전송함으로써 공격자를 찾아내어 대비하기는 더욱 어렵다.

이와 더불어 웜에 의한 공격은 1990년대부터 인터넷이 보급화 되면서 대두되기 시작하였다. 바이러스나 다른 공격툴과는 달리 다른 파일을 감염시키지 않으므로 알아내기가 쉽지 않으며 이메일과 같은 손쉽게 접하는 매체를 통해서 전파되므로 최근에는 웜에 의한 피해가 속출하고 있다. 다른 해킹방법과 달리 인터넷상에 연결되어 있으면 어느 곳이나 쉽게 침투하여 빠른 감염 속도로 전파되어 단시간 내에 전 세계적으로 감염되며, 공격기법도 지능적이 되어 가고 있다.

2003년 인터넷 대란을 일으킨 슬래머 웜은 10분만에 전 세계로 전파되어 서버를 다운시킨 기록을 가지고 있다.

이렇듯 최근의 해킹 방법은 DDoS나 웜 공격에 의한 트래픽 폭주 공격이 주를 이루고 있으며, 시스템 내의 정보를 빼어가는 소극적인 형태에서 시스템 자체의 기능을 마비시키는 적극적인 방법으로 발전하고 있으며, 공격 방법도 지능적이고 악독해지면서 그 해결방법이 어렵고 아직까지 이런 공격들을 사전에 대비할 방법이 없는 실정이다.[2]

[그림 1]은 트래픽 폭주 공격의 일반적인 동작원리 및 공격 형태를 보여주고 있다.



[그림 4. 트래픽 폭주 공격의 일반적인 동작원리 및 공격형태]

2.1 트래픽 폭주 공격의 유형

2.1.1 DDoS 공격의 유형

DoS 공격은 대역폭, 프로세스 처리능력, 기타 시스템 자원을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격의 형태이다. 이 공격 방법은 IP 헤더의 근원지 IP 주소를 공격하고자 하는 대상 IP 주소로 변경한 다음 IP 헤더 뒤에 ICMP 메시지를 붙여서 ICMP echo_request를 전송하는 smurf 공격이 대표적이다.

또한 ICMP 메시지를 직접 대상 시스템으로 대량의 패킷을 발생시키는 ICMP flood 공격, 대량의 UDP 패킷을 대상 시스템으로 보내는 UDP flood 공격 또는 대량의 TCP 패킷을 대상 시스템으로 보내는 TCP flood 공격 등이 있다. 이러한 공격들은 프로세스 처리 능력과 시스템 자원을 고갈을 목표로 하는 공격이나 혹은 비정상적인 패킷 사이즈를 통한 방법이 있다. 최근에는 이런 방법들이 여러 개의 에이전트를 이용하여 분산 환경에서 공격하는 형태를 보이고 있으며 이는 기존의 DoS 공격보다 많은 트래픽을 유발시켜 그 피해정도가 심각하다. [표 2]는 대표적인 DDoS 공격툴의 비교를 나타낸 것으로서, DDoS 공격은 기본적으로 마스터 시스템 내에 핸들러 프로그램이 작동하며, 핸들러는 공격자로부터의 명령을 받아서 자신이 관리하는 에이전트에 공격을 지시하면, 에이전트 시스템 내에 데몬 프로그램을 작동한다. 데몬 프로그램은 각각 핸들러로부터 받은 공격명령에 따라서 대상 시

[표 2. 대표적인 DDoS 공격툴의 비교]

종류 / 항목	Trinoo	TFN	Stacheldraht	Shaft	TFN2K	Mstream
공격방법	UDP floods	UDP/SYN /ICMP floods,Smurf	UDP/SYN/ICMP floods, Smurf	UDP/SYN/ICMP floods(혼합가능)	UDP/SYN /ICMP floods, Smurf	TCP ACK floods
통신암호화 기능	X	X	O	X	O	X
Attacker↔Master	27665/TCP	Telnet등의 방법	16660/TCP (암호화)	20432/TCP	Telnet등의 방법	6723/TCP 15104/TCP
Master ↔Agent	27444/UDP	ICMP echo reply	ICMP echo reply, 65000/TCP	18753/UDP	UDP/TCP/ICMP 랜덤(암호화)	7983/UDP 10498/TCP
Agent ↔Master	31335/UDP	ICMP echo reply	ICMP echo reply	20433/UDP	없음	9325/UDP 6838/UDP
IP spoofing 기능	X	O	O	X	O	O
발견시기	1999년 이전	1999년 이전	1999년 8월	1999년 11월	1999년 11월	2000년 3월
Process Name변경	X	O	O	?	O	X

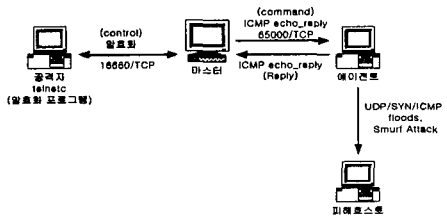
스템에게 공격을 가한다.

Trinoo는 많은 소스로부터 통합된 UDP flood 공격을 유발하는데 사용되는 도구이다. 몇 개의 마스터와 많은 수의 에이전트들로 이루어져있어공격자는 trinoo 마스터에 접근하여 마스터에게 하나 또는 여러 개의 IP 주소를 공격하도록 마스터와 통신을 한다. 에이전트내의 데몬 프로그램은 하나 이상의 마스터 IP 주소를 가지고 있으며 데몬 프로그램이 실행되면 "*HELLO*"라는 스트링을 포함한 UDP 패킷을 마스터에게 보냄으로써 실행 가능함을 알린다. 마스터는 실행가능 하다고 확인된 모든 데몬들에게 브로드캐스트 주소로 ICMP echo_request를 명령하고 데몬들은 "PON G"이라는 스트링을 포함하는 UDP 패킷을 마스터에게 보내어 응답한다. 이런 과정을 거쳐 공격자가 마스터에 공격 명령을 내림으로써 공격이 시작된다.

TFN은 trinoo와 거의 유사한 분산도구로 많은 소스에서 하나이상의 대상 시스템에 대해 서비스 거부 공격을 수행한다. 그러나 trinoo와는 달리 공격자가 마스터로 접속하기 위한 별도의 포트가 준비되어 있지 않다. 따라서 공격자가 마스터로 접근하기 위해서는 telnet등의 프로그램을 사용해서 마스터내에서 핸들러를 직접 실행해야 한다.

또한 trinoo와는 달리 실행에 필요한 별도의 암호가 없지만, 마스터와 에이전트 모두 ICMP를 사용하므로 root권한을 필요로 한다. TFN의 공격방법은 매우 다양하여 UDP flood 공격을 할 수 있을 뿐만 아니라 TCP/SYN flood 공격, ICMP echo_request공격, ICMP 브로드캐스트 공격(smurf)을 할 수도 있다. 마스터와 에이전트의 통신에는 ICMP echo_reply 메시지를 사용하므로 별도의 포트를 열어둘 필요가 없으므로 쉽게 탐지되지 않는다.

Stacheldraht는 이것의 모태에 해당하는 trinoo의 네트워크 구조와 TFN의 다양한 공격방법을 포함한다. 이것은 공격자 시스템과 자동적으로 업데이트되는 에이전트 데몬과의 통신을 위하여 암호화 기능이 추가된 DDoS 공격도구이다. 암호화를 위해서 공격자가 직접 사용하는 telnet과 비슷한 프로그램인 telnetc를 제공하는데 이 프로그램을 사용하여 공격자와 마스터간의 암호화된 통신이 가능하다. 따라서, 공격자와 마스터간의 통신에 대해서는 네트워크 패킷을 분석한다고 하더라도 Stacheldraht의 여부를 판단하기 쉽지 않다. 그림 2-5는 Stacheldraht의 기본적인 구조를 나타낸 것이다.



[그림 5.Stacheldraht의 구조]

Stacheldraht는 TFN이나 TFN2K 처럼 ICMP flood, SYN flood, UDP flood와 smurf등의 공격에 의해서 DDoS 공격을 할 수 있는 기능을 가지고 있다. 공격은 Intrusion 및 에이전트에 데몬 프로그램을 설치하는 단계와 공격자 시스템에서 마스터 시스템과의 암호통신용 프로그램을 실행시켜서 마스터를 통해 에이전트의 데몬으로 하여금 대상 시스

템에 DDoS 공격을 가하는 부분으로 나눌 수 있다. 데몬은 실행될 때 자신의 마스터에게 ICMP echo_reply 패킷의 ID필드와 데이터 필드를 넣어서 보내고, 이 패킷을 받은 마스터의 핸들러 프로그램은 다시, ICMP echo_reply 패킷의 ID필드와 데이터 필드를 넣어서 보낸다. 이러한 과정을 통해서 마스터와 에이전트간의 서로의 존재를 인식한다. 공격방법은 공격자가 사용하는 telnetc 프로그램을 실행하면 인증과정이 시작되고 이 과정을 통과해야만 진행할 수 있다. Stacheldraht 또한 trinoo처럼 여러 개의 command를 가지고 있으며 공격자의 명령들을 핸들러가 받아서 다시 에이전트로 해당 명령을 변환해서 보내게 되며, 그때 사용되는 것이 ICMP echo_reply 패킷이다. 이것은 TFN과 동일한 방식이며, ICMP echo_reply 패킷의 ID필드에 command를, 데이터 필드에 argument를 넣어서 에이전트로 보내면 에이전트들은 표적 시스템을 공격하게 된다.

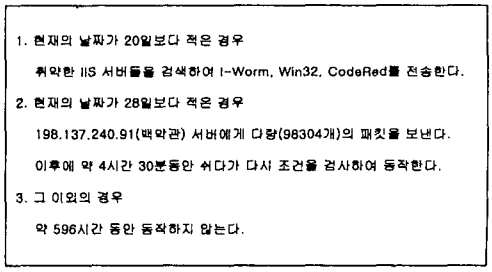
이외에 TFN의 발전된 형태인 TFN2K 및 TCP ACK 공격을 사용하는 Mstream, 핸들러와 데몬 사이의 연결을 trinoo에 기초하여 기초적인 암호화 기능이 포함된 Shaft등이 있다.[3]

2.1.2 웜해킹의 유형

웜은 바이러스와는 달리 다른 파일을 감염시키지 않고 자신을 복제하는 능력을 가진 프로그램을 말한다. 1980년대 이전까지는 웜에 대해서 관심을 가지지 않았었지만, 최근의 공격형태가 시스템내의 정보를 알아내기보다는 시스템 자체의 기능을 상실토록 하는 추세로 가면서 웜의 확산성을 이용한 공격이 나타나기 시작하였다. 가장 최근의 2003년 1월 슬래머 웜에 의한 대규모 인터넷 대란에서 웜은 단시간 안에 전 세계로 확산되어 SQL 서버를 다운시키는 무서운 괴력을 보여주었다.

2003년 1월 전 세계적으로 인터넷 대란을 일으킨 SQL 슬래머 웜은 엄청난 전파속도와 파괴력으로 전 세계 인터넷 서버와 기업의 네트워크를 파괴시켰다. '슬래머'는 '문간'이라는 뜻으로 SQL 서버를 위하여 사용되는 포트나 UDP 1431포트가 외부에서 내부로 접속하기 위한 관문을 대상으로 한 공격으로 슬래머 웜은 MSDE/SQL 서버 2000의 보안상의 약점을 이용하여 원격 권한을 얻어낸 뒤 시스템을 감염시켰다. 시스템을 감염시킨 후, 임의의 IP 주소로 무한의 복제 웜을 발송해 빠른 속도로 다른 시스템까지 감염시켰다. 슬래머 웜은 자체적으로는 파괴적 실행코드를 가지고 있지 않지만, 대신 엄청난 네트워크 트래픽을 발생시켜 피해를 주었다. 대상 시스템 및 네트워크의 대역폭을 목표로 한 공격이었다.

CodeRed 웜은 2001년 6월 18일에 발견된 마이크로소프트사의 Security MS01-033인 "Unchecked Buffer in Index Sever ISAPI Extension"의 취약점을 이용한 것이다. 따라서 이 웜은 IIS를 구동하고 있는 윈도우 서버급을 목표로 하고 있다. 이 웜은 메모리에만 존재하며, 일반적으로 파일의 형태로 존재하지 않는다. 즉, 80 포트로 들어온 패킷을 제대로 해석하지 못한 IIS가 버퍼오버플로어 되면서 악성코드로 유입된 웜을 수행하게 되는 것이다.



[그림 6. CodeRed 웜의 동작방법]

ColdBule 웜은 IIS 4.0과 IIS 5.0의 MS00-078 (Web Server Folger Traversal)보안 취약점을 이용하는 공격으로서 그 동안 알려졌던 CodeRed의 공격 대상이 되는 취약점과는 다른 취약점을 이용하여 공격하고 감염시킨다. 특징적인 증상은 오전 10시와 11시에 중국에 할당되어 있는 서버에 DoS 공격을 시도하며, 100개 이상의 쓰레드를 생성함으로서 시스템 속도가 현저하게 떨어지고 랜덤한 IP 주소 대역으로도 공격을 시도하므로 네트워크 트래픽이 증가하게 된다.

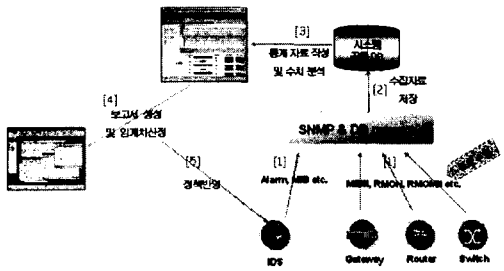
I-worm.FreeBSD.Scalper 아파치 웹 서버의 문제점을 이용하여 감염되는 웜으로서 감염된 시스템은 80포트를 이용하여 다른 아파치 서버를 찾고, 찾은 서버에서 아파치 웹 서버 chunk handling 문제점을 발견하면 감염되는 동작을 반복하면서 확산된다. 감염된 시스템에서 이메일 주소를 얻어와 스팸메일 형식으로 메일을 발송하며, 특정 웹 주소로 접속하게 되어있어 DoS 공격을 일으킨다. 감염된 시스템은 80번 포트를 사용하여 인터넷상의 존재하는 또 다른 아파치 서버를 찾는 조건을 계속 진행하기 때문에 인터넷 속도가 저하될 수 있다. 또한, UDP 포트 2001번을 통하여 시스템을 제어할 수 있게 한다.

이외에 Yaha의 변형인 **I-worm.Win32, Yaha.28672**와 **Worm.Win32.Netspree, Linux.Slapper.worm, Linux/Slapper.worm** 등이 있다. [4]

3. 트래픽 정보 수집 및 분석

기존의 일반적인 네트워크 트래픽 정보의 수집 및 분석방법은 네트워크 서비스를 향상시키기 위한 일환으로 주로 사용되었다. 네트워크 트래픽 정보를 통한 네트워크의 병목현상이나 네트워크 장애를 판단하여 트래픽 흐름을 조절하는 것이다. 트래픽 폭주 공격은 네트워크에 수많은 트래픽을 유발시켜 네트워크 자원을 고갈시키거나 종단 호스

트의 기능을 마비시켜서 정상적인 서비스를 하지 못하도록 하는 공격 방법이다. 트래픽 폭주 공격으로부터 네트워크 자원과 시스템을 보호하기 위한 방법들 중 하나의 방법이 네트워크에 흐르는 트래픽의 정보를 수집하고 분석하여 트래픽 폭주 공격에 대응하는 방법이다.



[그림 3. 트래픽 정보 수집]

본 고는 네트워크의 트래픽을 수집하기 위하여 기존의 대부분의 네트워크 장비에서 지원하고 있는 MIB II의 트래픽 정보, RMON1, RMON2 에서 제공하는 프로토콜 정보, 시스코 장비의 netflow를 활용한 플로우 정보, SNORT에서 제공하는 침입탐지정보 등을 활용하여 트래픽을 수집하고 활용하고자 한다.[4-10]

이는 기존의 네트워크 인프라에 구성된 라우터 및 스위치, 게이트웨이에서 지원하고 있는 SNMP agent를 활용하여 시스템의 인터페이스 레벨 및 시스템, 프로토콜 레벨로 패킷 및 옥텟의 송수신률, 에러률, 손실률을 측정하여 트래픽 공격이 일어나지 않는 상태에서의 트래픽 정보를 계속해서 수집하다. 수집된 정보는 시스템의 공통 DB에 저장되어져 공격되지 않은 상태에서의 시스템 및 네트워크 트래픽 율이 측정되어 시스템의 공통 DB에 저장되어진다.

현재 대부분 소규모의 LAN환경의 기본인 Ethern et 환경에서 100Mbps 네트워크를 기본으로 할 때 최소 프레임의 크기는 84bytes이고 이때 발생가능한 트래픽은 148,800 frames/sec이다. 또한 최대 프레임의 크기는 최대 데이터 프레임이 1518bytes일 때, 최대 프레임의 크기는 1538 bytes이고 이때 발생 가능한 트래픽은 8.127 frames/sec이다. 이때 패킷의 크기가 매우 작은 프레임이 비정상적으로 폭주되면 시스템의 CPU가 과부하상태가 되고, 서비스 품질이 떨어질 수 있다. 또한 최대 프레임 사이즈의 패킷이 비정상적으로 폭주되면 시스템의 메모리의 오버플로우 및 대역폭 점유, 네트워크 속도 등의 저하로 폭주 공격을 예측할 수 있다. 이와 같이 시스템의 임계치가 산정되면 공격 탐지 시스템의 새로운 정책으로 반영시킬 수 있다. 비정상적인 트래픽이 폭주가 감지되면 자동 감지 알람이 매니저에게 통보되어 네트워크 장비 및 어플리케이션을 보호할 수 있도록 한다.

4. 결론 및 고찰

본 고는 트래픽 폭주 공격의 개념을 정의하고 유형별로 분석하였다. DDoS 공격 및 Worm 해킹 공격의 유형을 분석하고 최근들어 계속 발달하고 있는 공격 방법에 대해서 살펴 보았다. 또한 소규모 망에서 기존의 네트워크 장비 및 서버를 이용하여 이 공격들을 대응할 수 있는 시스템을 제시하였다.

본 시스템은 설계 단계로서 MIBII, RMON, RMON2 정보 및 meter MIB 정보, 시스코 장비의 netflow 정보를 활용하여 트래픽 공격을 탐지할 수 있는 정보의 흐름의 추이를 파악하여 공격을 탐지하고자 한다.

5. 참고 문헌

[1] http://www.certcc.or.kr/
[2] http://www.certcc.or.kr/paper/tr1999/1999 10/tr1999010.html
[3] http://www.securitymap.net/sdm/sdm_ddos .html
[4] K. McCloghrie, M. Rose, "Management Information Base for Network MAnagement of TCP/IP-based internet:MIB-II",RFC-1213, 1991
[5] N. Brownlee, "Traffic Flow Measurement : Meter MIB", RFC2064, 1997
[6] S. Waldbusser, "Remote Network Monitoring Management Information Base",RFC1271,1991
[7] S. Waldbusser, "Remote Network Monitoring Management Information Base", RFC1757, 1995
[8] S. Waldbusser, "Token Ring Extensions to the Remote Network Monitoring MIB", RFC1513, 1993
[9] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)", RFC1157, 1990
[10] K . McCloghire, F. Kastenholz, "The Interface group MIB", IETF RFC2863, 2000