

방화벽 NAT를 지원하는 새로운 다자간 화상회의 시스템의 설계 및 분석

Design and Analysis of a New Video Conference System Supporting the NAT of Firewall

정용득(Jung, Yong Deug)*, 김길준(Kim, Gil Choon)**, 전문석(Jeon Moon Seog)*

초 록

인터넷의 확산과 컴퓨터 기술의 발달로 웹을 기반으로 한 화상회의 시스템이 다양한 분야에서 활용되고 있다. 이러한 화상회의 시스템은 화이트보드의 공유와 파일의 공유를 위해서 공인 IP주소를 사용해야 하고 방화벽 내부사용자와 비공인 IP주소 사용자를 위한 처리가 어렵다는 문제가 있다. 본 논문에서는 방화벽내부 사용자나 비공인 IP주소 사용자를 위해 비공인 IP주소를 공인 IP주소로 변환시켜 주는 Application Level Gateway를 구현한다. 또한 네트워크 대역폭에 따라 화상과 음성 미디어를 동적으로 조절하는 Control Daemon을 제안한다. Control Daemon은 다자간 회의진행을 위한 회의실 개설과 종료, 회의참여 수락, 진행관리를 담당한다.

ABSTRACT

A video-conference system is being utilized in web based application services in various fields due to the widespread use of Internet and the progress of computer technologies. This system should use the public IP address for sharing file and white board and it is difficult to manage the internal network users of the firewall and non-public IP address users. In this paper, we propose an Application Level Gateway which transforms non-public IP address into public IP address. This mechanism is for the internal network users of the firewall or non-public IP address users over the Internet. We also propose a Control Daemon which manages video and audio media dynamically according to network bandwidth. This mechanism can start and terminate a video conference and manage the process of the video conference.

키워드 : 화상회의(Video Conference), Application Level Gateway, NAT(Network Address Translator), H.323, SIP(Session Initiation Protocol)

본 논문은 숭실대학교 교내지원비에 의한 것임.

* 숭실대학교 컴퓨터학부

** 성결대학교 전자상거래학부

1. 서 론

기업용 통신 인프라가 기존의 서킷교환방식에서 패킷망을 기반으로 한 IP 플랫폼 기반으로 빠르게 전환되면서, IP망을 활용한 화상회의 솔루션이 등장하고 있다[1,9]. ADSL 망을 활용한 PC에서의 화상회의 시스템은 초당 30프레임의 고화질 화상을 제공하며 PC상에서 비디오(카메라와 오디오(마이크/스피커))를 이용하여 실제 면대면(1:1) 회의 또는 다자간(1:N)회의와 같은 회의환경을 제공한다. E1, T1, T3 급의 인터넷 전용선을 이용한 화상회의에 필요한 단말측에 최소 대역폭인 300Kbps를 확보할 수 있고 안정된 대역폭이 보장 될 때에는 최상의 화질을 구현할 수 있다. 하지만, 대역폭이 낮은 네트워크나 PSTN을 통한 해외지역과 화상회의를 하는 경우 ISDN이나 CABLE을 통한 전이중 통신이 아니어서 사실상의 필요 대역폭 확보를 기대할 수 없는 문제점이 있다[10,11,12].

ISDN망이나 ATM 망에서는 다자간 화상회의를 지원하는 MCU(Multipoint Conferencing Unit)가 필요하다. MCU는 화상의 품질을 높여주는 장점이 있는 반면에 하드웨어적인 장비를 별도로 설치해야 한다. 본 논문에서는 다자간 회의를 지원하기 위해 MCU 장비를 사용하지 않고 소프트웨어적으로 해결하기 위해 H.323[9] 터미널과 호환할 수 있는 Control Daemon 서버를 사용하였다. H.323을 기반으로 하는 기존의 화상회의 시스템은 회의 참여자가 많으면 병렬성과 동기화 문제로 복잡성이 대두되어 문제가 발생하기도 한다[11]. 화상회의 서버에 부하를 최소

화 시키고 지대역폭 네트워크 환경에서 양방향 통신이 가능하기 위해서는 P2P(Peer-to-Peer) 통신 방식이 적합하다. 대부분 기업의 경우 신뢰할 수 없는 외부 네트워크로부터 내부 네트워크를 보호하기 위해 방화벽(Firewall)에서 네트워크 소켓 연결을 차단한다. 이러한 방화벽(Firewall) 사용 환경에서는 특정 포트로 접속하는 외부와의 세션이 실패하는 경우가 있다. 이를 해결하기 위해 여러 가지 기법들이 제안되고 있다[2,3,4].

이러한 문제의 해결을 위해 라우터 내부에 공인 IP주소를 가지고 방화벽에서는 80Port를 Open하여 NAT(Network Address Translator) 형태로 멀티미디어 데이터를 P2P(Peer-to-Peer)로 전달하도록 한다[13]. 방화벽(Firewall) 내부 사용자와 비공인(Non-Public) IP주소 사용자가 종단간 상호 연결하여 화상회의를 하기 위해서는 반드시 공인 IP로 변환되어야 한다[2,5].

주소변환을 위해 네트워크 계층의 목적지 주소 정보 뿐만 아니라 트랜스포트 계층의 포트정보를 이용해 IP주소 이용률을 극대화 시킨 네트워크 주소 변환 방법이 있지만 IP주소를 변환하기 위해 IP계층과 TCP/UDP 계층을 고려해야 하므로 처리가 복잡하고 처리 속도도 느린 단점이 있다[4].

이러한 단점을 해결하고자 본 논문에서는 화상회의 서버 내에 Application Level Gateway를 사용함으로써 비공인 IP 사용자가 화상회의 요청 시 공인 IP 주소로 변환시켜 주어 화상회의에 참여할 수 있도록 구현하고자 한다. 또한 앞에서 언급한 TCP 프로토콜 기반에서 다자간 회의시 발생할 수 있는 병렬성과 동기

화문제를 해결하기 위해 회의에 참여하는 클라이언트들의 정보를 관리하고 회의를 주관하도록 Control Daemon 모듈을 사용함으로써 회의실의 개설, 회의 참여자의 예약과 수락, 회의의 진행 등을 관장하는 기능을 새롭게 추가하였다. 이외에 Control Daemon 모듈은 네트워크 대역폭에 따라 종단간에 전송되는 미디어가 차지하는 네트워크 대역폭을 동적으로 조절하는 역할을 수행하도록 한다.

본 논문의 구성은 제2장에서는 화상회의 시스템의 종류와 화상회의 시스템을 설계하기 위한 고려사항을 언급하고 압축표준을 살펴본다. 제3장에서는 모델로 제시한 시스템을 설계하여 제4장에서는 3장에서 설계한 모델을 기준으로 구현하여 타 화상회의 시스템과 비교분석 평가하였으며, 마지막으로 제5장에서는 결론 및 향후 연구를 제시한다.

2. 관련연구

2.1 H.323과 SIP 표준

2.1.1 H.323

H.323[15]은 멀티미디어 화상회의 데이터를 TCP/IP와 같은 패킷교환 방식의 네트워크를 통해 전송하기 위한 ITU-T(International Telecommunication Union-Telecommunication Standardization Sector)의 표준이다. 패킷 네트워크에서 실시간 점대점 및 다지점 멀티미디어 통신을 제공하기 위한 구성 요소, 프로토콜 및 절차를 정의한 것으로, 구현을 위해서는 단말, 게이트웨이, 게이트키퍼,

MCU(Multipoint Control Unit)의 네 가지 구성요소가 필요하다. 이 서비스에 있어서 종단 요소 사이의 호 설정(Call Setup)과 접속해제를 위한 시그널링 프로토콜로 Q.931을 사용한다. H.323 영상회의 시스템 단말은 채널의 사용과 협상에 대한 능력을 제공하는 H.245 호 시그널링 및 설정을 위한 Q.931, 게이트키퍼와의 통신 프로토콜인 RAS(Registration /Admission /Status), 오디오와 비디오 패킷의 순서화를 담당하는 RTP/RTCP 등을 반드시 지원하여야 한다. 또한 선택적으로 비디오 코덱, T.120 데이터 회의 프로토콜, MCU 능력, 게이트웨이 등을 지원할 수 있다. 게이트웨이는 H.245와 Q.931 프로토콜을 사용하여 H.323 단말이나 LAN 상의 다른 게이트웨이와 WAN 상의 다른 ITU 단말간에 실시간 양방향 통신을 제공하는 종단 장치이다.

2.1.2 SIP

SIP는 ITU-T의 H.323에 대응하는 프로토콜로서 멀티미디어 화상회의 서비스에서 단말간 또는 사용자들간에 호를 설정하는 프로토콜이다. SIP는 매우 간단한 텍스트 기반의 응용계층 제어 프로토콜로서, 한사람 이상의 참가자들이 함께 세션을 만들고, 수정하고 종료할 수 있게 한다. SIP는 텍스트 기반의 HTTP(Hypertext Transfer Protocol)를 응용하여 확장시켜 설계된 것으로 클라이언트가 호출을 시작하면 서버가 그 호출에 응답을 하는 클라이언트-서버 구조에 기반을 두고 있다. SIP는 이러한 기존의 텍스트 기반 인터넷 표준을 따름으로써, 고장수리와 네트워크 디버깅 등이 쉽다[14].

2.2 화상회의 시스템

2.2.1 화상회의 시스템의 고려사항

〈표 1〉에서와 같이 화상회의 시스템은 음성, 화상, 파일전송, 화면분할, 사용자편의성, 메신저, 녹화재생, 전송복구 지연처리, 운영, 화상회의 표준과의 호환성 등이 고려사항이다.

기업내부에서 사용하는 화상회의 시스템은 비즈니스에 주로 사용되므로 음성과 화상 전달에 끊어짐 현상이나 전송지연을 최소한으로 줄이기 위해서 음성이나 화상을 최대한 압축하여 전송시간을 최소한으로 줄여야 한다. 화상은 초당 프레임 전송율에 따라 화상의 질이 결정된다. 화상의 전송은 네트워크의 대역폭에 따라 전송지연이 불가피하므로 화상보다는 음성위주로 내용이 명확하게 전달될 필요가 있다. 1:1회의는 물론 다자간 회의가 가능해야 하며 화이트보드에서 멀티미디어의 파일을 서로 공유하여야 하고 전송지연에 따른 복구처리 기능이 필요하다.

2.2.2 화상회의 시스템의 표준과 호환성

본 논문에서는 ITU-T 화상회의 표준프로토콜인 H.323을 사용하는 Microsoft사의 NetMeeting에 접속하여 화상데이터를 송수신할 수 있도록 하였다. 이를 위하여 H.323 표준 규격에서 기본으로 사용하는 영상 코덱인 H.263의 해상도인 QCIF(176x144픽셀) CIF(352x288 픽셀) 해상도를 지원하도록 하였다. 또한, VoIP기반의 SIP 프로토콜의 User Agent와 Proxy Server와 음성데이터를 주고

받을 수 있도록 만들었다.

2.3 다자간 화상회의 운영 모듈

다자간 화상회의를 위해서는 ①회의실 참여자의 입장, 퇴장 관리와 회의실간에 충돌이 발생하지 않도록 관리하는 데몬의 기능, ②하나의 회의실에서 다수가 동시에 입장하여 다자간 화상회의를 할 수 있도록 오디오와 미디어 시그널의 처리와 미디어간의 동기화를 수행하는 프로세스들의 생성, 처리, 소멸의 관리는 물론 각 프로세스는 병렬처리와 실시간 처리가 가능하도록 처리, ③비공인 IP 사용자가 방화벽 내부의 Proxy기능의 수행을 통해 외부로 전달되는 공인 IP로의 변경을 통해 화상회의에 참여할 수 있도록 처리하는 Application Level Gateway의 기능, ④각 사용자의 상태를 모니터링하면서 회의실 정보의 관리기능 등이 필요하다. 이를 위해서 본 논문에서는 4개의 모듈을 사용하여 처리하도록 하였으며, 〈표 2〉는 본 논문에서 제안한 화상회의 시스템에서 사용하는 모듈로 Control Daemon, Gateway Daemon, Control Process, Gateway Control Process로 구성한다.

2.3.1 Control Daemon

현재 인터넷의 환경은 ADSL, 케이블 모뎀, 위성모뎀 형태로 통신을 이루고 있어서 유동 IP망 환경에서는 사용자의 IP주소가 매번 바뀌는 경우가 발생하므로 유동 IP주소를 고정 IP주소로 변환해 주는 기능이 필요하다. 이러한 기능은 Control Daemon Process가 미리 Control Process를 10개를 만들고 각 Control

〈표 1〉 다자간 화상회의 시스템 설계 고려사항

번호	기능	내용
1	음성전송	음성전송시 음성의 끊어짐이 일시적으로 발생하거나 음성 전송 지연
2	화상전송	화상전송시 화상의 끊어짐이 일시적으로 발생하거나 화상 전송 지연
3	화상회의실	1:1, 다자간 회의(1:2, 1:4, 1:9, 1:15) 화상회의에 필요한 회의공간
4	파일전송	멀티미디어 파일전송시 전송지연
5	팝업창 수용	화이트 보드에서 팝업창이 있는 웹사이트 로그인시 화상 끊어짐 현상
6	보안성	음성 및 화상코덱의 보안성 및 접근보안, 바이러스 침투에 대비한 보안성
7	사용자 편의성	사용자의 편의성을 위해 유저의 사용정도에 따른 User Interface 텍스트 입력, 텍스트모드 변경, 선택적 메시지 전송
8	메신지	회의요청시 쪽지보내기, 텍스트 채팅 중 1:L, 1:N 화상회의 요청
9	3D 그래픽 처리	웹공유시 Virtual Reality를 활용해 화상회의 중에 3D 카탈로그의 ZOOM IN-OUT 표현 가능
10	공유기능 동기화기능	웹페이지를 동시에 화이트보드에 띄워 놓고 화면을 공유하여 서로 대화할 수 있는 기능, 화상회의 화면과 음성을 녹화하고 캡처 3D 카탈로그의 Zoom in-out 할 때 동화상의 동기화
11	파일의 첨부 및 다운로드	멀티미디어 파일의 송,수신, 자료의 선택적 업로드와 다운로드, 견적서, 제품설명서, 매뉴얼, 카탈로그 등의 문서를 첨부하여 상대방에게 전송
12	뭉음처리	음성의 전송시 말을 안하고 있을 경우 음성데이터를 보내지 않고 뭉음 제거하여 처리
13	녹화 재생	화이트보드 상에 띄워 있는 판서내용을 정리하고 녹화하고 재생
14	전송지연 복구처리	네트워크 상태가 열악한 경우 화상과 음성을 분리하여 처리하여 음성이 전송되도록 처리
15	운영	회의실 입장, 퇴장, 제어권부여, 비디오세팅, 오디오세팅, 마이크 On/Off, 카메라 On/Off
16	화상회의 표준과 호환	H.323이나 SIP 등 IETF나 ITU-T의 표준과 호환성

Process는 Port 번호를 하나씩 부여한다. Port number는 회의를 할 때 데이터를 교환하기 위한 채널로 사용한다. 각 Control Process는 50개의 회의실을 생성, 관리하도록 하고 데이터를 빠르게 처리하도록 쓰레드를 사용한다. 회의 요청을 받으면 Control Daemon Process

는 10개의 Control Process 중에서 회의에 사용되지 않는 Control Process를 선택하여 회의에 할당한다. Control Daemon Process는 네트워크 대역폭의 조절과 회의 신청에 대한 승락과 거절, 회의를 요청한 Client에 대한 IP 주소, Port번호, Data의 길이, Data 정보 등

〈표 2〉 각 모듈의 역할 및 기능

모듈명	모듈의 역할 및 기능
Control Daemon	회의실을 총괄 관리하고 통제한다.
Down_Server	OCX를 통해 회의 프로그램 다운로드 한다.
Gateway_Daemon	화상회의 서버에 기반한 화상회의 시 비공인 IP 사용자를 판별하여 공인IP로 변환해 주는 역할을 수행한다. Gateway Control (Gateway_Daemon) Process를 생성한다.
Data_Down_Server	화상회의 사용자의 데이터를 PC에 다운로드 하는 모듈
Web_Conn	회의실에 입장, 퇴장 상태를 웹 서버로 전달한다.
Control_27003~27012	회의실을 운영하며 사용자의 회의실 정보를 관리하기 위해 포트번호를 27003~27012까지 설정하여 Peer-to-Peer 기반 화상회의시 사용한다.
Gateway_Control_Process	비공인 IP사용자를 위해 화상회의 서버에 기반한 화상회의를 지원하는 모듈로 Gateway_Daemon을 자동으로 생성해 준다.

을 회의관리를 위해 저장한다.

2.3.2 Gateway Daemon

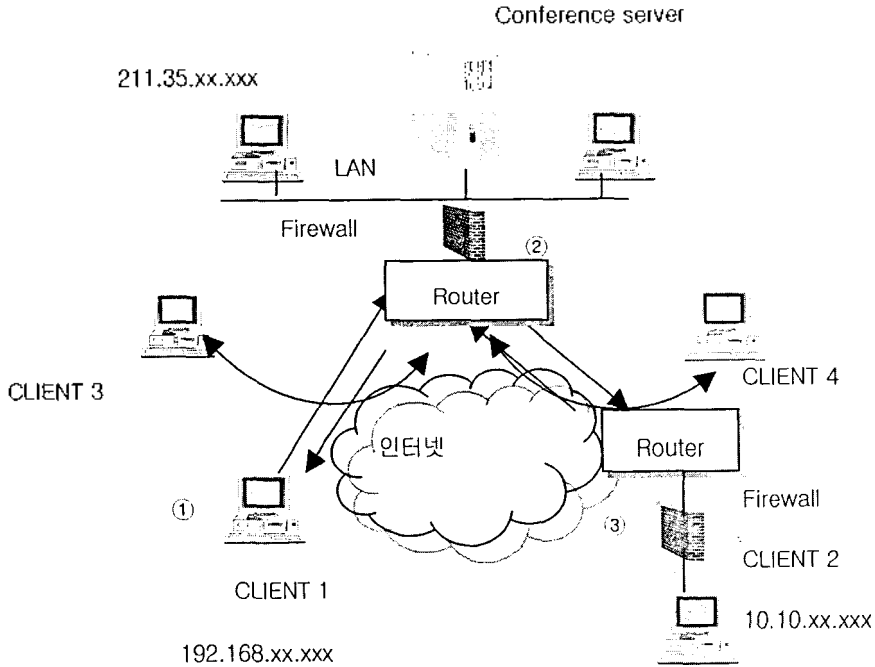
개설자가 비공인 IP주소를 사용하는 경우 회의실 개설이 불가능하다. 이를 해결하기 위해 Gateway Daemon은 비공인 IP주소를 공인 IP로 변환해 주어 회의실 개설을 할 수 있도록 한다. 비공인 IP 사용자는 화상회의 Server를 기반으로 하여 참여자와 회의를 진행할 수 있으며, 데이터의 교환도 가능하다.

2.3.3 Control Process

회의실을 만들기 위한 프로세스로 각각의 프로세스는 Port번호를 별도로 부여하여 데이터 교환을 위한 채널로 사용한다. Control Process는 Control Daemon의 하위모듈로 Peer-to-Peer 기반 화상회의시 사용할 수 있도록 지원한다.

2.3.4 Gateway Control Process

Gateway Daemon 이 데이터의 교환을 위한 채널로 Gateway Control Process를 통해 프로세스를 생성하여 사용하도록 한다. 회의실이 이미 만들어져 있는 경우에는 개설된 회의실에 참여할 수 있게 하고 회의실이 만들어지지 않은 경우에는 회의실을 만들고 사용자 식별을 위해 회의실 예약시 별도로 고유번호를 부여하여 이 고유번호로 로그인한 사용자에게 미리 알려준다. 회의실 개설자인 경우에는 개설자가 방화벽 사용자 인지를 검사하거나 로컬 IP와 서버에서의 IP를 비교하여 서로 다른 경우에 방화벽 사용자로 판단하고 Gateway Damon과 접속하여 Gateway Control Process를 생성하게 하고 Control Process Port 번호는 미리 설정하여 방화벽 사용자와 비공인 IP사용자를 따로 구분하여 처리하도록 한



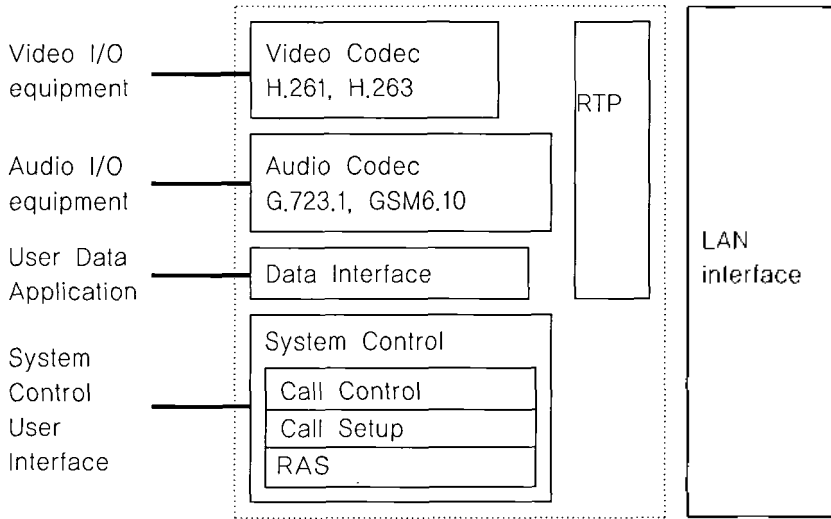
〈그림 1〉 화상회의 시스템의 구성도

다. 생성된 포트를 회의실에 참여한 모든 사용자에게 알려 Gateway Control Process와 접속을 하여 데이터를 주고 받을 수 있게 한다. 〈그림 1〉은 비공인 IP와 방화벽 사용자가 화상회의에 참여하는 형태로 ①은 비공인 IP주소를 사용하는 Client1의 상태 ②는 방화벽 내부에 위치한 화상회의 서버의 네트워크 구조 ③ 방화벽을 사용한 Client2의 상태를 나타낸다. 방화벽내부 사용자와 비공인 IP주소 사용자를 위한 화상회의의 절차는 다음과 같다. 현재 회의실에 있는 모든 사람에게 사용자 리스트를 보고 사용자 ID, 사용자 명, IP주소, 방화벽 사용여부, Gateway Control Process IP, Gateway Control Process PORT를 전송하여 회의실에 참여했음을 알려준다.

3. 새로운 다자간 화상회의 시스템의 설계

3.1 다자간 화상회의 시스템의 구성

멀티미디어 데이터 통신은 네트워크 부하량을 줄이고 미디어 전송률을 최소화시키기 위해 화상과 음성을 압축한다[6]. 본 논문에서 사용한 화상 압축코덱은 H.261, H.263을 채택[7,8]하며, 음성압축 코덱은 G.723.1, GSM6.10을 지원하도록 하고 자료공유는 웹공유, 파일업로드와 다운로드가 가능하도록 하고 화이트보드를 공유하도록 한다. 시스템제어를 위한 사용자 인터페이스는 화상회의 시작과 종료, 회의실 관리를 위한 호제어가 가능하도록 구성한다. 인터넷의 네트워크 환경에 따른 통신 대역폭이 수시로 변화하는 점을 감안하여



〈그림 2〉 H.323 표준 화상시스템 구성요소

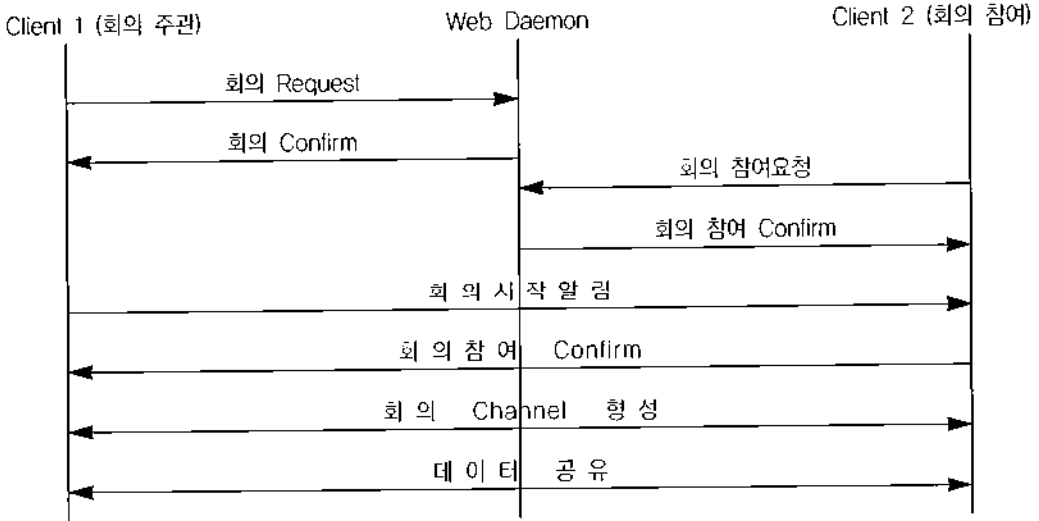
회의 참여자가 느끼는 네트워크의 부하를 최소화하도록 Client에서 대용량의 프로그램이 실행되도록 하였으며 과도한 네트워크 대역폭을 차지하는 멀티미디어 그래픽데이터를 패킷 단위로 분할하여 전송하도록 하였다 [10.11].

본 논문에서 제시한 모델은 TCP 프로토콜을 사용하여 화상회의 서버를 기반으로 한 통신방식과 화상서버에 부하를 주지 않는 P2P 기반 통신방식, 방화벽 내부 사용자와 비공인 IP주소 사용자가 공인 IP주소를 공유하여 화상회의에 참여하여 회의 참여자간에 웹공유, FTP, 파일을 공유하도록 모델을 설계하였다. 〈그림 2〉는 H.323 화상회의의 표준에 따라 본 논문에서 구현한 화상회의의 시스템의 구성도이다.

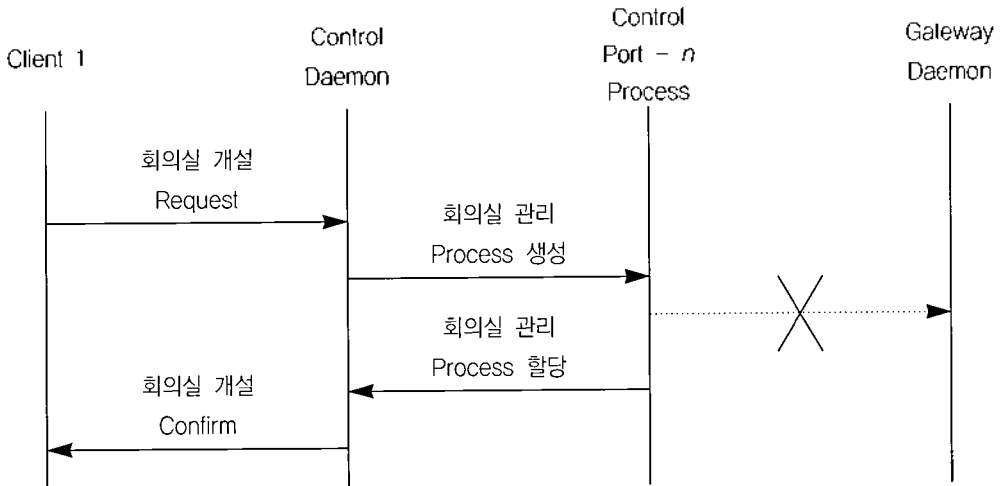
3.2 화상회의 시스템의 기본 모델

〈그림 3〉은 화상회의의 시스템의 기본 모델로 Client1과 Client2가 화상회의를 위해 Web 서버에게 화상회의를 요청하고 세션을 맺고 채널을 형성하여 멀티미디어 데이터를 공유하는 형태이다[10.11,12].

- ① 웹서버에 접속한 Client1이 화상 회의실 에 입장을 요청한다.
- ② 웹서버는 화상회의의 서버에게 URL로 Client1에 대한 정보를 Parameter로 전달한다.
- ③ 화상회의의 서버에서 Client1에 대한 시작 정보를 받아서 Client2에게 Active-X API 형태로 Client1에 대한 정보를 전달한다.
- ④ Client1과 client2가 Active-X API에 의해 화상회의를 실행한다.



〈그림 3〉 화상회의 시스템의 기본흐름도

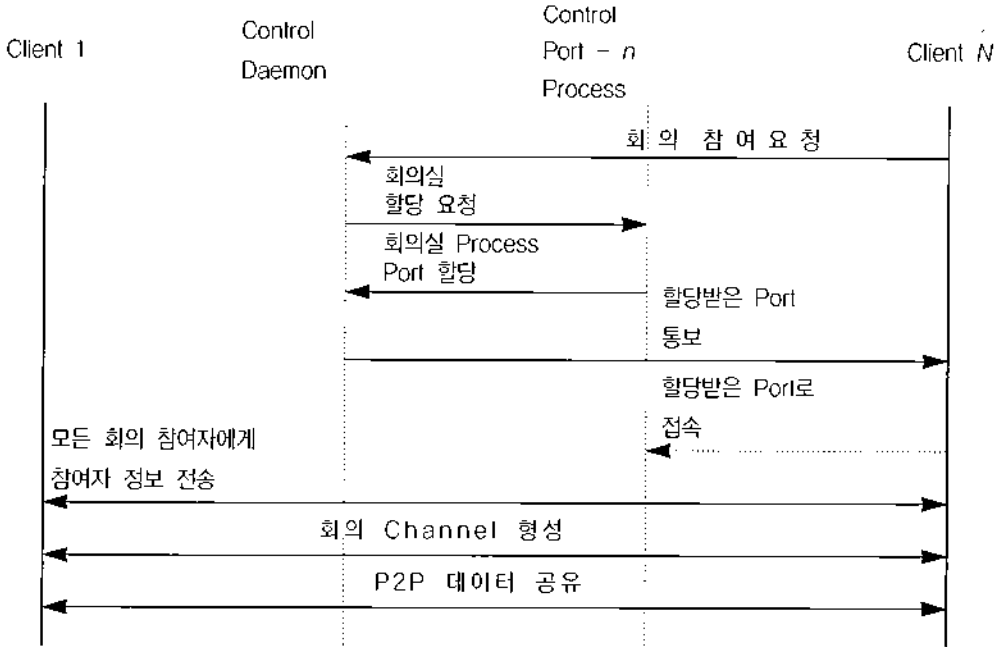


〈그림 4〉 공인 IP 사용자가 회의실을 개설할 때 화상회의 흐름도

3.3 공인 IP사용자의 회의실 개설형태

〈그림 4〉는 공인 IP 사용자가 회의실을 개설할 때 화상회의 흐름도로 Client 1이 화상회의를 개최하기 위해 웹에 접속하게 되면

Control Daemon은 회의실 개설 요청을 받는다. 회의실 키를 생성하기 위해 Control Process 중에서 접속자 수가 가장 적은 노드를 선택하여 Port를 Client 1에게 할당하여 Control Daemon에게 통보한다. Control Daemon은



〈그림 5〉 새로운 참여자 접속시 화상회의 흐름도

Control Process와의 접속을 끊고 새로 생성한 Control Process 포트와 접속을 하고 회의실 키를 생성하고 생성한 정보를 공유메모리에 저장한다. 이때 개설자가 공인IP주소를 가지고 있다면 Gateway Daemon에 접속하지 않는다.

3.4 공인 IP 사용자의 화상회의

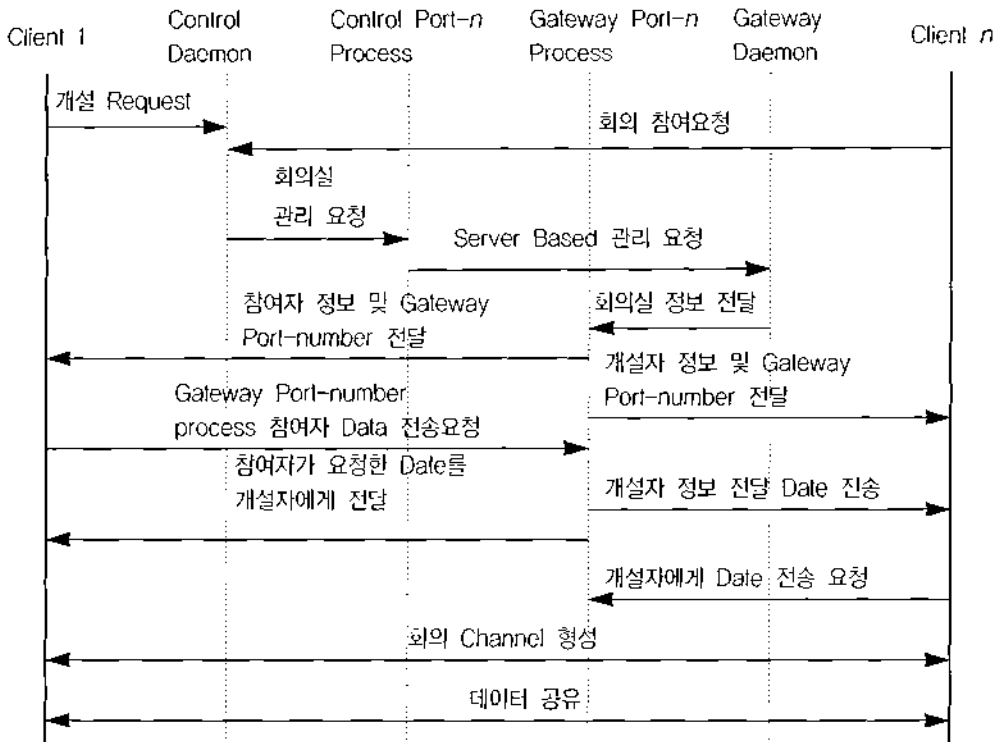
〈그림 5〉는 새로운 참여자가 접속 시 화상회의 흐름도이다. 공인 IP주소를 소유한 사용자 Client n 이 화상회의에 참여하기 위해 웹에 접속을 시도한다.

Control Daemon은 회의실 키에 해당하는 포트번호를 Client n에게 할당한다. Client n은Control Daemon 과의 접속을 끊고 새로 할

당 받은 Control Process Port번호와 접속한다. Control Process Port번호는 회의실 키로 같은 Port번호를 할당받은 모든 참여자에게 Client n 이 회의실에 참여하였음을 알려 준다. 회의실 개설자인 Client 1이 Client n 에게 참여자 정보인 공인 IP와 할당 받은 Port번호를 통해 접속하게 되고 이후 데이터를 Control Daemon을 거치지 않고 직접 P2P로 주고 받을 수 있게 된다.

3.5 방화벽 사용자가 비공인 IP 사용 시 화상회의 모델

〈그림 6〉은 개설자가 방화벽 사용 시 화상회의 흐름도이다. Client 1이 화상회의를 위해 회의실 개설을 Control Daemon 서버에게 요



〈그림 6〉 개설자가 방화벽 사용시 화상회의 흐름도

청하면 Control Port-*n* process를 생성한다. Control Port-*n* Process는 현재 회의실 키에 해당하는 회의실이 생성 되어 있지 않으므로 Control Port-*n* Process 중에서 접속자 수가 가장 적은 PORT를 Client1에게 할당한다.

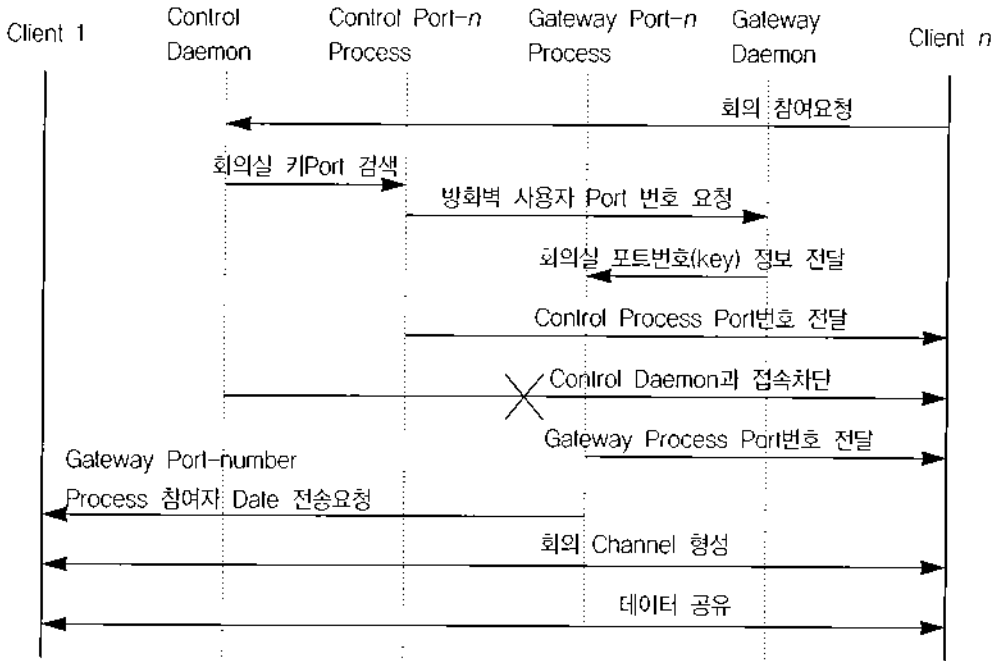
Client 1은 Control Daemon과 접속을 끊고 할당 받은 포트번호로 Control Port-*n* Process와 접속을 하고 Control Port-*n* Process를 회의실 키에 해당하는 회의실을 생성한다. 이때 생성한 정보는 공유메모리에 저장하고 개설자가 방화벽 사용자이므로 중간에 Gateway Daemon Server가 공인 IP로 전환해 주는 역할을 수행한다.

새롭게 할당 받은 Control Port-*n* process는

Gateway Daemon과 접속을 한다. 새로운 Gateway Port-*n* process를 생성하고 PORT 번호를 Client1에게 넘겨준다. Client1은 데이터를 전송하기 위해 Gateway Port-*n* process와 접속을 하고 화상회의를 진행한다.

3.6 새로운 참여자가 방화벽 사용시 화상회의 모델

방화벽 내부에 있는 사용자인 Client *n*이 화상회의에 참여하기 위해 화상회의에 접속할 때 Control Daemon은 회의실의 종류와 제목을 키로 하여 회의실 포트를 Client *n*에게 할당한다. Client *n*은 Control Daemon과의 접



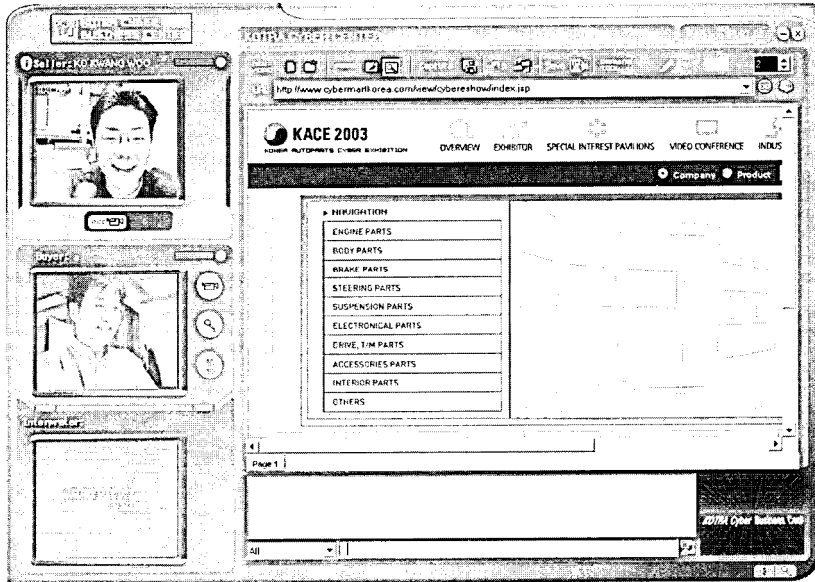
〈그림 7〉 새로운 참여자가 방화벽 사용시 화상회의 흐름도

속을 끊고 할당 받은 Control Process 포트번호와 접속한다. Control Process Port를 참조하여 회의실 키에 접속된 모든 참여자에게 Client n 이 접속했음을 알려준다. 개설자는 Control Daemon으로부터 사용자 정보를 받고 새로운 참여자인 Client n 이 방화벽 내부 사용자임을 알게 되고 개설자가 방화벽으로 접속했으므로 사용자 리스트를 통해 해당된 포트번호에 접속을 하고 Gateway control process를 통해 데이터를 주고 받을 수 있게 한다. 〈그림 7〉은 새로운 참여자가 방화벽을 사용할 때의 화상회의 흐름도이다.

4. 화상회의 시스템의 구현

4.1 화상회의 시스템의 구현환경

화상회의 시스템은 클라이언트의 환경은 Windows XP, Pentium IV, 2.3Ghz로 사용하였고, 화상회의 서버는 Linux Pentium VI 2CPU, 2.3Ghz를 사용한다. 화상압축은 ITU-U 압축 표준인 H.261, H.263 코덱을 사용하여 화상프레임을 초당 8kbyte로 전송하도록 하였으며, 음성 압축 코덱으로는 유럽 ETSI(European Telecommunications Standards Institute)의 표준인 G723.1과 GSM6.10을 사용하였다. 본 논문에서 구현한 화상회의 시스템은 기존의 화상회의 시스템이 1:1이나 음성위주인 단점을 해결하기 위해 〈그림 8〉



〈그림 8〉 제안한 화상회의 시스템

과 같이 다자간 회의 기능과 화이트보드 공유를 통한 컨설팅이 가능하도록 구현하였다. 미디어 데이터의 전송을 위해 멀티미디어 대용량 자료의 전송이 가능하도록 문서를 전달할 때 페이지 단위로 분할하여 전달한다. 상대방이 페이지를 열어 봤을 경우 새로운 페이지를 보내준다. 계속하여 한 페이지씩 분리하여 전송대역폭을 감안하여 자료를 보내주도록 설계하였으며, 가상의 공유메모리 관리를 통해 멀티미디어 데이터의 송수신을 자유롭게 하였고, 회의실을 개설한 경우 1개의 회의실에는 동시사용자 수가 최대 16명까지 최대 50개의 회의실을 개설할 수 있도록 설계하였다.

4.2 각 모듈의 패킷 구조

4.2.1 Daemon Server Packet

회의실 키를 서버에 보내 회의실이 개설된 경우에는 개설된 서버의 포트 번호를, 개설되지 않은 경우에는 Control 서버 중에서 노드가 적은 Control 서버의 포트 번호를 할당해서 그 서버로 접속할 수 있도록 Packet을 구성한다.

4.2.2 Control Server Packet

회의실의 개설 및 입장, 참여, 연결된 사용자 정보, 채팅 등을 위한 서버와의 연결을 위한 Packet, 접속한 회의실 참여자의 리스트 정보를 갖고 회의 진행의 제어권을 변경한다.

Command	Flag	Data length	Data
---------	------	-------------	------

〈그림 9〉 Control Server Packet 구조

〈표 3〉 기존 화상회의 시스템과 비교 분석

기 능	A사	B사	논 문
음성압축	8~22Kbps	8Kbps(8KHz)	8~12Kbps
화상압축	60kbps~100kbps	50kbps~80kbps	8~12Kbps
비공인IP지원	지원하지 않음	지원하지 않음	지원
방화벽 지원	지원하지 않음	지원하지 않음	방화벽 통과를 위한 포트 지원
다자간회의 화면분할	최대 8명 화면분할	최대 10명 화면분할	최대 16명 화면분할
네트워크방식	화상 전용(80port 지원) 5~8개 port 지원	화상회의 전용서버 (80port 지원)	화상회의 전용서버 (80port 지원)
서버 네트워크	T1(1.5Mbps)/10명	T1(1.5Mbps)/30명	T1(1.5Mbps)/50명
부가기능	이미지캡처, 전자철판, 웹공유, 파일공유	이미지캡처, 전자철판, 웹공유, 파일공유	이미지캡처, 전자철판, 웹공유, 파일공유, Media 공유
표준	지원하지 않음	H.263/30Fps	H.323(GSM6.10/G.723지원)
운영방식	Server Based	P2P	Server Based와 P2P 동시 지원

4.2.3 Gateway Server Packet

Gateway가 내부 LAN의 비공인 IP Network 주소인 192.164.xxx.xxx 정보를 외부로 전달하지 않으면 라우터는 공인 IP Network 주소 정보만 전달하게 되어 인터넷에 문제를 야기시키지 않게 된다. Gateway는 내부 LAN에 있는 시스템으로부터의 요청을 받아 인터넷으로 전달하고 인터넷으로부터 결과를 받아 내부 LAN에 있는 시스템으로 전달해 주는 대리자 역할을 한다. 요청은 내부시스템 주소인 192.164.68.1 에서 발생 했지만 Gateway가 자신의 공인 IP 주소 203.128.25.0으로 대체하여 요청한다. 그리고 해당 데이터가 오면 그것을 받아 192.164.xxx.xxx 시스템에게 전달한

다. Gateway가 Proxy 기능을 하기 위해서는 Proxy Server 프로그램을 Gateway 시스템에 설치한다. 경우에 따라서는 Gateway에 인터넷 Mail Server를 설치하여 외부에서 오는 메일을 받고 내부에서 발생한 메일을 외부로 전달해 주는 역할을 담당한다.

4.2.4 Gateway Control Process Data Packet

화상회의 참여자가 음성, 화상, 화이트보드, 첨부파일 등을 송신하기 위한 Packet 구조로 송신측의 ID와 수신측의 ID, 송신데이터 형식인 화상, 음성, 화이트보드 Data와 특정한 회의실 참여자에게 송신할 수 있도록 구성되어 있다. 파일 전송시 데이터를 보내는 도중

```

4:25pm up 150 days, 5:12, 4 users, load average: 0.00, 0.00, 0.00
109 processes: 108 sleeping, 1 running, 0 zombie, 0 stopped
CPU0 states: 5.0% user, 2.1% system, 0.0% nice, 92.2% idle
CPU1 states: 0.2% user, 0.0% system, 0.0% nice, 99.3% idle
CPU2 states: 0.0% user, 0.0% system, 0.0% nice, 100.0% idle
CPU3 states: 0.0% user, 0.0% system, 0.0% nice, 100.0% idle
Mem: 3939616K av, 509252K used, 3430364K free, 0K shrd, 116952K buff
Swap: 2096440K av, 0K used, 2096440K free, 203648K cached

  PID USER   PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
 1161 root     15   0 15856 15M 12220 S    1.9  0.4 138:57 kdeinit
   999 root     15   0 34068 25M  5300 S    1.1  0.6 12497n N
 1157 root     15   0 15892 15M 13956 S    1.1  0.4 223:05 kdeinit
 1127 root     15   0 10336 10M  9492 S    0.9  0.2 703:45 kdeinit
15428 root     15   0 23820 23M 16600 S    0.9  0.6  0:15 kdeinit
 1175 root     15   0 3724 3724 3012 S    0.3  0.0 40:00 antsd
15936 root     15   0 1100 1100  860 R    0.3  0.0  0:19 top
   953 root     15   0 4540 4540  876 S    0.1  0.1  3:57 kotra_control
   954 root     15   0 4616 4616  860 S    0.1  0.1  3:26 kotra_control
   955 root     15   0 4520 4520  852 S    0.1  0.1  3:35 kotra_control
   960 root     15   0 4332 4332  768 S    0.1  0.1  4:05 kotra_control
     1 root     15   0 480 480  420 S    0.0  0.0  1:51 init
     2 root     15   0  0  0  0 SW    0.0  0.0  0:00 keventd
     3 root     34  19  0  0  0 SWN   0.0  0.0  0:00 ksoftirqd_CPU0
     4 root     34  19  0  0  0 SWN   0.0  0.0  0:00 ksoftirqd_CPU1
     5 root     34  19  0  0  0 SWN   0.0  0.0  0:00 ksoftirqd_CPU2
     6 root     34  19  0  0  0 SWN   0.0  0.0  0:00 ksoftirqd_CPU3
     7 root     15   0  0  0  0 SW    0.0  0.0  1:07 kswapd
     8 root     25   0  0  0  0 SV    0.0  0.0  0:00 bdflush
     9 root     15   0  0  0  0 SV    0.0  0.0  0:47 kupdated
    10 root     25   0  0  0  0 SV    0.0  0.0  0:00 mdrecoveryd
    16 root     25   0  0  0  0 SV    0.0  0.0  0:00 sccs_ch_0
    17 root     25   0  0  0  0 SW    0.0  0.0  0:00 sccs_ch_1
    21 root     15   0  0  0  0 SW    0.0  0.0  0:00 kjournald
    96 root     16   0  0  0  0 SW    0.0  0.0  0:00 khubd
   191 root     15   0  0  0  0 SW    0.0  0.0  0:00 kjournald
   192 root     15   0  0  0  0 SW    0.0  0.0  0:00 kjournald
   193 root     15   0  0  0  0 SV    0.0  0.0  0:00 kjournald
   194 root     15   0  0  0  0 SW    0.0  0.0  2:21 kjournald
   195 root     15   0  0  0  0 SW    0.0  0.0  0:00 kjournald
   196 root     15   0  0  0  0 SW    0.0  0.0  0:00 kjournald
   635 root     15   0 500 500  500 S    0.0  0.0  0:10 syslogd
   640 root     15   0 444 444  384 S    0.0  0.0  0:00 klogd
    
```

〈그림 10〉 Gateway Control Daemon의 CPU 사용량

에 계속 보낼 경우 처리와 파일의 이름과 크기, 데이터의 끝을 명시한 정보를 포함하고 있고 데이터전송의 승낙과 취소에 대한 처리를 하도록 한다.

4.3 비교 분석

본 논문에서 제안한 시스템과 타 시스템을 비교 평가하기 위해 2개의 유사한 시스템을 비교하였다. <표 3>은 화상회의 시스템의 기본적인 기능을 비교한 표이다. 비공인 IP사용

자로 접속하였을 경우 Gateway Control Daemon이 공인IP로 변환시켜주는지와 이때 어플리케이션의 응답시간을 측정하였다. 네트워크 지연시간, 서버응답시간의 지연, 사용자 시스템의 응답지연시간으로 구분하여 실험하였다. 실험환경은 클라이언트는 Windows XP, Pentium IV, 2.3Ghz로 사용하였다. 통신환경은 E1급 2회선을 사용하였다. 네트워크 평균 대역폭으로는 음성은 1.4kb, 화상은 4kb~2kb 기타 1kb로 전송 대역폭을 설정한 후 대역폭에 따라 화상프레임의 대역폭

을 조절하면서 데이터를 송신하도록 구성하였다. 네트워크의 환경에 따라 전송되는 대역폭의 변화가 있을 경우 프로토콜을 변경하여 사용한다.

4.3.1 대역폭 조절 알고리즘

다자간 화상회의에서는 오디오와 비디오를 네트워크를 통해 전송할 때 각각의 프레임에 따라 동적인 중복성을 제거하기 위해 버퍼를 사용한다. 미디어의 전송을 네트워크의 상태에 따라 전송율을 동적으로 변화시켜 줄 필요가 있다. <그림 11>은 본 논문에서 적용한 대역폭 조절 알고리즘이다.

```

if  $\alpha \neq \text{DECREASE}$  then  $b_a = \max\{b_r * u, b_{\min}\}$ 
else if  $\alpha \neq \text{INCREASE}$  THEN  $b_a = \max\{b_r + v, b_{\max}\}$ 
    
```

<그림 11> 대역폭 조절 알고리즘

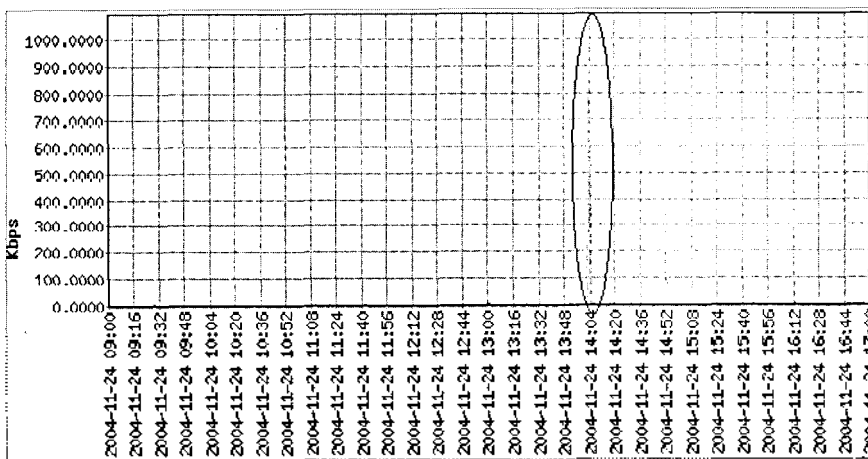
대역폭 조절 알고리즘은 전송상태의 값이 Increase로 설정되면 v의 값을 더해주기 때문에 선형적으로 증가하고, 전송상태의 값이

Decrease로 설정되면 u의 값을 곱해주기 때문에 지수적으로 감소한다. 최대 대역폭을 b_{\max} 로 설정하고, 최소대역폭을 b_{\min} 으로 설정하며, b_a 은 결정된 대역폭의 값을 나타내고 있다.

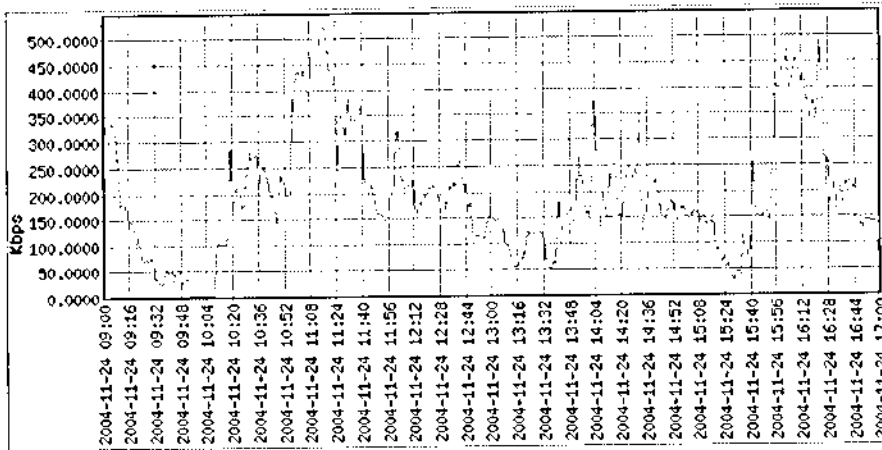
4.3.2 미디어 대역폭 소모량

화상회의를 위한 미디어 대역폭 소모량은 표준 JPEG을 사용하여 측정된 결과 예상대로 <그림 12>에 나타난바와 같이 Peer-to-Peer 기반의 화상회의를 위하여 화상회의 서버에 접속할 때만 네트워크의 부하를 차지할 뿐, Peer-to-Peer로 접속한 이후로는 거의 네트워크의 부하를 차지하지 않는 것으로 나타났다.

반면에, 표준 JPEG을 사용한 같은 실험환경에서 <그림 13>과 같이 기존의 화상회의 시스템은 화상회의 도중에도 계속하여 일정하게 네트워크의 부하량을 차지하는 것을 알 수 있다.



<그림 12> 제한 시스템의 네트워크 부하량



〈그림 13〉 기존 시스템의 네트워크 부하량

5. 결 론

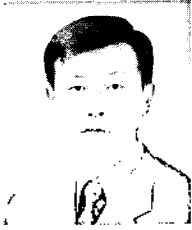
본 논문에서는 웹 환경에서 방화벽 사용자나 비공인 IP사용자가 Application Layer Gateway의 구현을 통해 비공인IP주소 사용자와 공인IP주소 사용자간에 화상회의가 가능함을 실험을 통해 증명하였다. 네트워크의 대역폭에 따라 음성과 화상의 속도를 동적으로 조절하여 미디어 지연시간을 최소화 하여 지연이나 끊어짐이 발생하지 않도록 하였다. 다자간 회의가 가능하도록 회의실 개설과 입장, 퇴장을 제어하는 Control 프로세스 서버를 사용하였다. Control 프로세스의 개수는 최대 200개로 각 회의실 참여자의 수를 50명까지 확보하여 사용할 수 있도록 하였으며, 인터넷상에서 서버의 부하를 최소화 하기 위해서 P2P로 대용량의 멀티미디어 데이터를 전송함으로써 쌍방향 통신이 가능하도록 하였다. 이를 위해 사설 IP에서는 NAT를 사용하여 공인 IP 주소를 갖는 사용자의 패킷 정보

를 패킷의 헤더에 실어 상대방에게 보내주어 미디어의 용량을 최소화 하여 화상회의가 가능하도록 구성하였다. 이러한 방법을 사용하면 네트워크의 대역폭에 따라 500명까지 동시에 화상회의를 할 수 있다. 향후 연구과제로 다자간 회의시 회의내용의 기밀성, 무결성, 보안성을 강화하기 위해 PKI를 통한 사용자 인증과 미디어스트림의 암호화를 통해 화상회의의 안전성을 보장할 수 있을 것이다.

참 고 문 헌

- [1] H.Schulzrinne(Feb 1996). "Simple Conference Invitation Protocol", Internet Draft, IETF.
- [2] P.Srisuresh, M.Holdrege(1999). "IP Network Address Translator(NAT) Terminology and Considerations" IETF, RFC2663.
- [3] N.Freed(Oct,2000). "Behavior of and Requirements for Internet Firewalls." IETF.
- [4] D.C.Hyde(Jan.2002). "How New Peer to Peer Developments May Effect Collaborative Systems." Department of Computer Science Bucknell University.
- [5] R.Braden, Ed., L. Zhang, S.Berson, S.Herzog, and S.Jamin(September 1997). "Resource ReSerVation Protocol(RSVP)", RFC2205, .
- [6] L.Berc, W. Fenner, R.Frederick, S.McCann(October 1996). "RTP Payload Format for JPEG-compressed Video", RFC 2035.
- [7] International Telecommunication Union(ITU), Online(URL:http://www.itu.int).
- [8] The Internet Engineering Task Force, Online (URL:http://www.ietf.org).
- [9] Ismail Dalgic, Hanlin Fang(Sep.1999). "Comparision of H.323 and SIP or IP Telephony Signaling", Proc. of Photonics East.
- [10] H.Schulzrinne, S.Casner, R.Fredrick, and V.Jacobson(Jan.1996). "RTP : a transport protocol for real-time applications", RFC 1889, IETF.
- [11] K.Kelly and J.Mark(Mar.2000). "Distributed multipoint conferences using SIP" Internet Draft, Internet Engineering Task Force.
- [12] NetMeeting, Online http://www.microsoft.com/windows/NetMeeting/default.ASP.
- [13] 김영진, 김문정, 엄영익(2002). "순수P2P 네트워크환경에서 프락시서버 할당을 위한 동적 피어 선정기법", 2002년도 한국정보과학회 가을 학술발표논문집 Vol.29.No2.
- [14] M.Handley, H.Schulzrinne, E.Schooler, J.Rosenberg, "SIP : Session Initiation Protocol," RFC 2543, March 1999.
- [15] ITU-T, "Recommendation H.323 : Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-guaranteed Quality of Service," 1996.

저 자 소 개



정용득 (E-mail : jungyd@kotra.or.kr)
 1988. 목포대학교 전산통제학과(학사)
 1990. 숭실대학교 전자계산학과(석사)
 2001. 숭실대학교 컴퓨터학부 박사과정 수료
 1990 ~ 현재 대한무역투자진흥공사 차장
 관심 분야 암호학, 멀티미디어정보통신, PKI



김길준 (E-mail : kimid@sungkyul.edu)
 1975. 숭실대학교 전자계산학과(학사)
 1984. 숭실대학교 대학원 전산과(석사)
 1991. 숭실대학교 대학원 전산과 박사
 1995 ~ 현재 성결대학교 전자상거래학부 부교수
 관심 분야 전자상거래, 인터넷비즈니스, PKI



전문석 (E-mail : mjun@comp.ssu.ac.kr)
 1980. 숭실대학교 전자계산학과(학사)
 1996. University of Maryland 전산과(석사)
 1989. University of Maryland 전산과(박사)
 1989. Morgan State University 전산수학과 조교수
 1989 ~ 1991. New Mexico state University 부설 Physical Science Lab.
 책임 연구원
 1991 ~ 현재 숭실대학교 정보과학대학 부교수
 관심 분야 암호학, 침입차단 시스템, PKI