광대역통합망(BcN) 주요장비에 대한 정보보호 가이드(V1.0)

2006. 12

정보통신부
KISA 한국정보보호진흥원
Korea Information Security Agency

발 간 사

BcN Security Guide

언제 어디서나 정보 접근이 가능한 유비쿼터스 사회 실현을 위하여, 정부는 지난 '06년 3월, 제26차 정보화추진위원회에서 「광대역통합망 구축 기본계획 II(안)」을 확정하고, 이 기본계획에 따라 2단계('06~'07년) BcN 구축사업을 통한 차세대 정보인프라 구축에 더욱 박차를 가하고 있습니다.

하지만, BcN 환경에서는 PSTN, WiBro, 인터넷, WCDMA 등 다양한 이기종 망이 통합되어 IP기반에서 서비스를 제공하므로 IP망이 가지는 전통적인 보안 취약점 상속, 단일망의 침해사고로 인한 피해가 타 망으로의 급속한 확산 가능성 등이 새로운 문제로 대두되고 있습니다.

이에 따라 BcN 기반의 안전한 서비스 제공을 위해서는 다양한 이기종 망들이 통합되는 BcN 환경의 구축단계에서부터 운영 및 활성화 단계에 이르기까지 발생 가능한 다양한 보안위협을 식별하고 이에 대한 대응책을 마련하는 것이 선결조건이라 하겠습니다.

이를 위해 개발한 BcN 환경의 주요 정보보호 위협과 대응방법을 제시하는 『BcN 주요장비에 대한 정보보호 가이드(V1.0)』를 통해서 BcN 사업자, 서비스 및 장비 개발자 등이 안전한 BcN 환경을 구축하고, 이를 기반으로 사용자에게 다양한 서비스를 제공하여 사업 확대 및 BcN 활성화의 전기를 마련할 수 있기를 기대합니다.

부디 본 가이드가 안전한 BcN 환경을 구축하고, 안전한 유비쿼터스 사회를 실현하는데 큰 역할을 할 수 있기를 바라며, 가이드 발간을 위해 노력을 아끼지 않으신 관계자 여러분의 노고에 감사 드립니다.

2006년 12월
한국정보보호진흥원장 이 흥 서

목 차

contents

제 1 장 서 론 ····· **2**

제 1 절 개 요 ····· 2

제 2 절 가이드 목적 및 범위 ····· 5

제 3 절 가이드 구성 및 활용방법 ····· 6

제 2 장 BcN 정보보호 표준화 추진현황 ····· **7**

제 1 절 BcN 표준화 개요 ····· 7

제 2 절 국외 NGN 보안 표준화 동향 ····· 9

1. NGN 표준 ····· 9

2. NGN 보안 위협 ····· 9

3. 보안표준 추진내용 ····· 10

4. 보안표준 기술 및 향후추진 계획 ····· 12

제 3 절 국내 BcN 보안표준화 동향 ····· 14

1. BcN 표준모델 개요 ····· 14

2. BcN 표준모델 II(안) 구조 ····· 14

3. BcN 표준모델 II(안) 보안요구 사항 ····· 15

4. BcN 구축단계별 보안목표 및 고려사항 ····· 16

제 3 장 BcN 정보보호 영역 및 대상 ····· **18**

제 1 절 BcN 시범사업 추진현황 ····· 18

1. 시범사업추진 개요 ····· 18

2. 옥타브 컨소시엄 ····· 19

3. 광개토 컨소시엄 ····· 22

4. 유비넷 컨소시엄 ····· 24

5. 케이블 컨소시엄 ····· 27

제 2 절 BcN 정보보호 영역 ····· 30
1. BcN 연동개념 및 아키텍처 ····· 30
2. BcN 연동구간 도출 및 분석 ····· 32
제 3 절 BcN 정보보호 대상 ····· 36
1. 가입자망 연동구조 분석 ····· 36
2. 보호대상 식별 ····· 40

제 4 장 BcN 연동구간 보안위협 ····· 42
제 1 절 BcN 연동구간 보안위협 개요 ····· 42
제 2 절 서비스 거부공격 ····· 44
1. 시스템 자원고갈 ····· 44
2. 비정상 메시지 전송 ····· 44
3. 네트워크 경로자원 고갈 ····· 48
제 3 절 서비스품질(QoS) 저하 ····· 51
1. QoS가 조작된 패킷 인입 ····· 53
2. DiffServ 자원절도 ····· 54
3. 잡음 삽입 ····· 55
제 4 절 시스템 해킹 ····· 57
1. 시스템 설정 오류 ····· 57
2. 원격접속 프로토콜 취약점 ····· 58
3. 운영체제 및 어플리케이션 취약점 ····· 59
제 5 절 도청 ····· 63
1. 연동장비 해킹을 통한 도청 ····· 63
2. 전송패킷 분석을 통한 도청 ····· 64
3. 세션 가로채기를 통한 도청 ····· 66
4. Fake DHCP 운영을 통한 도청 ····· 67
제 6 절 메시지 위·변조 ····· 69
1. 사용자 등록 메시지 위·변조 ····· 69

목 차 contents

2. 가입자 정보 위·변조 ····· 70
3. 세션 연결 메시지 위·변조 ····· 72
4. 라우팅 메시지 위·변조 ····· 74

제 5 장 BcN 연동구간 정보보호 대책 ····· 76
제 1 절 BcN 위협별 보안대책 ····· 76
제 2 절 서비스 거부공격 ····· 80
1. 시스템 자원고갈 ····· 80
2. 비정상 메시지 전송 ····· 83
3. 네트워크 경로자원 고갈 ····· 86
제 3 절 서비스품질(QoS) 저하 ····· 88
1. QoS가 조작된 패킷 인입 ····· 88
2. DiffServ 자원절도 ····· 88
3. 잡음 삽입 ····· 89
제 4 절 시스템 해킹 ····· 91
1. 시스템 설정 오류 ····· 91
2. 원격접속 프로토콜 취약점 ····· 91
3. 운영체제 및 어플리케이션 취약점 ····· 92
제 5 절 도청 ····· 94
1. 연동장비 해킹을 통한 도청 ····· 94
2. 전송패킷 분석을 통한 도청 ····· 95
3. 세션 가로채기를 통한 도청 ····· 99
4. Fake DHCP 운영을 통한 도청 ····· 100
제 6 절 메시지 위·변조 ····· 101
1. 사용자 등록 메시지 위·변조 ····· 101

2. 가입자 정보 위·변조 ····· 102
3. 세션 연결 메시지 위·변조 ····· 103
4. 라우팅 메시지 위·변조 ····· 104

제 6 장 안전한 BcN 구축을 위한 전략 ····· 106
제 1 절 사업자간 정보보호 수준의 일관성 유지 ····· 106
제 2 절 지속적·체계적 정보보호를 위한 법·제도 활용 ····· 108
1. 정보보호시스템 평가·인증 제도 ····· 108
2. 주요정보통신기반시설 지정 제도 ····· 109
3. 정보보호관리체계(ISMS) 인증 ····· 111
제 3 절 BcN 구축단계를 고려한 정보보호 ····· 113
1. BcN 서비스의 안전성 사전검증 ····· 113
2. 망 구축 단계별 정보보호 ····· 114

제 7 장 결 론 ····· 119

참고문헌 ····· 120

약 어 ····· 122

용어설명 ····· 126

부록1 BcN 인프라 주요장비 기능 분석 ····· 130

부록2 BcN 시스템 운영체제별 시스템 해킹 위협 및 보호대책 ····· 174

부록3 BcN 주요장비별 정보보호 체크리스트 ····· 181

표목차

[표 1-1] BcN 정의 및 특성 ····· 2
[표 1-2] 가이드 적용 범위 ····· 5
[표 3-1] BcN 시범사업 컨소시엄 구성 ····· 19
[표 3-2] 옥타브 컨소시엄 서비스 목록 ····· 20
[표 3-3] 광개토 컨소시엄 서비스 목록 ····· 23
[표 3-4] 유비넷 컨소시엄 서비스 목록 ····· 25
[표 3-5] 케이블 컨소시엄 서비스 목록 ····· 28
[표 3-6] BcN 가입자망 연동 Case ····· 33
[표 3-7] 연동구간의 보호대상 ····· 41
[표 4-1] BcN 연동구간 보안위협별 공격대상 분석표 ····· 42
[표 5-1] BcN 위협별 보안대책 ····· 76
[표 6-1] BcN 망 구축단계별 주요 차이점 ····· 114
[표 6-2] 보안 위협의 예상변화 ····· 117
[표 부록1-1] BcN 주요장비 선정결과표 ····· 131
[표 부록1-2] Cable Modem 표준별 특성 비교 ····· 137
[표 부록1-3] DOCSIS 프로토콜 계층 ····· 138
[표 부록3-1] BcN 장비별 위협에 대한 보호대책(안) ····· 181

그림목차

(그림 1-1) 광대역통합망(BcN) 계층 ····· 3
(그림 2-1) BcN 표준모델 구조도 ····· 15
(그림 3-1) BcN 연동 개념도 ····· 31
(그림 3-2) BcN 아키텍처 및 연동 개념도 ····· 32
(그림 3-3) PSTN ↔ PSTN 연동 개념도 ····· 33
(그림 3-4) PSTN ↔ 인터넷망 연동 개념도 ····· 34
(그림 3-5) PSTN ↔ WCDMA 연동 구조도 ····· 36
(그림 3-6) 인터넷 ↔ WiBro 연동 구조도 ····· 38
(그림 3-7) 인터넷 ↔ 유선 방송망 연동 구조도 ····· 39
(그림 4-1) 대량 SIP INVITE 메시지 전송 위협 ····· 44
(그림 4-2) 대량의 DHCP Request 메시지 전송 위협 ····· 46
(그림 4-3) 대량의 IP 패킷 전송 위협 ····· 47
(그림 4-4) 연결 해제 및 종료 메시지 전송 위협 ····· 49
(그림 4-5) 비정상 등록 메시지 전송 위협 ····· 50
(그림 4-6) 네트워크 경로자원 고갈 위협 ····· 52
(그림 4-7) QoS가 조작된 패킷 인입 위협 ····· 53

(그림 4-8) DiffServ 자원절도 위협 ····· 55
(그림 4-9) 잡음 삽입 위협 ····· 56
(그림 4-10) 시스템 설정 오류 위협 ····· 57
(그림 4-11) 원격접속 프로토콜 문제점 악용 위협 ····· 59
(그림 4-12) 운영체제 및 어플리케이션 취약점 악용 위협 ····· 60
(그림 4-13) 연동장비 해킹을 통한 도청 위협 ····· 63
(그림 4-14) 전송패킷 분석을 통한 데이터 도청 위협 ····· 65
(그림 4-15) 세션 가로채기를 통한 도청 위협 ····· 66
(그림 4-16) Fake DHCP 서버 운영을 통한 도청 위협 ····· 68
(그림 4-17) 사용자 등록 메시지 위·변조 위협 ····· 69
(그림 4-18) 가입자 정보 위·변조 위협 ····· 71
(그림 4-19) 세션 연결 메시지 위·변조 위협 ····· 72
(그림 4-20) 라우팅 메시지 위·변조 위협 ····· 74
(그림 5-1) VPN 유형 ····· 96
(그림 부록1-1) BcN 주요 연동 장비 ····· 130
(그림 부록1-2) 소프트스위치의 위치 ····· 132
(그림 부록1-3) 소프트스위치 시스템 구성 ····· 134
(그림 부록1-4) CMTS의 위치 ····· 135
(그림 부록1-5) DOCSIS 참조모델 기반의 CMTS 동작구조 ····· 139
(그림 부록1-6) CMTS 주파수 대역폭 ····· 140
(그림 부록1-7) CMTS와 CM(Cable Modem)간 통신 절차도 ····· 141
(그림 부록1-8) SIP 서버 위치 ····· 142
(그림 부록1-9) Proxy 서버 동작절차 ····· 144
(그림 부록1-10) Redirect 서버 동작절차 ····· 145
(그림 부록1-11) Signaling Gateway의 위치 ····· 146
(그림 부록1-12) 시그널링 게이트웨이 시스템 구조 ····· 147
(그림 부록1-13) STP, SG, MGC간의 메시지 흐름도 ····· 149
(그림 부록1-14) SIGTRAN 프로토콜 스택 ····· 150
(그림 부록1-15) SG내에서 NIF, M3UA, SCTP 계층간 메시지 흐름도 ····· 152
(그림 부록1-16) 미디어 게이트웨이의 위치 ····· 153
(그림 부록1-17) 미디어 게이트웨이 프로토콜 구조 ····· 154
(그림 부록1-18) IP Phone → PSTN 전화연결 ····· 155
(그림 부록1-19) PSTN Phone → IP Phone ····· 156
(그림 부록1-20) MPLS 라우터 위치 ····· 158
(그림 부록1-21) MPLS 라우터 구조 예시 (Netron Systems의 IronWare OS) ····· 160
(그림 부록1-22) MPLS 라우더 동작절차(1) ····· 162
(그림 부록1-23) MPLS 라우더 동작절차(2) ····· 164
(그림 부록1-24) DHCP 동작개념도 ····· 166
(그림 부록1-25) Cisco CNR 설정개념도 ····· 167
(그림 부록1-26) DHCP 패킷의 포맷 ····· 168
(그림 부록1-27) DHCP 동작절차 ····· 169
(그림 부록1-28) DHCP 메시지 교환 순서도 ····· 170

제1장 서 론

제1절 개 요

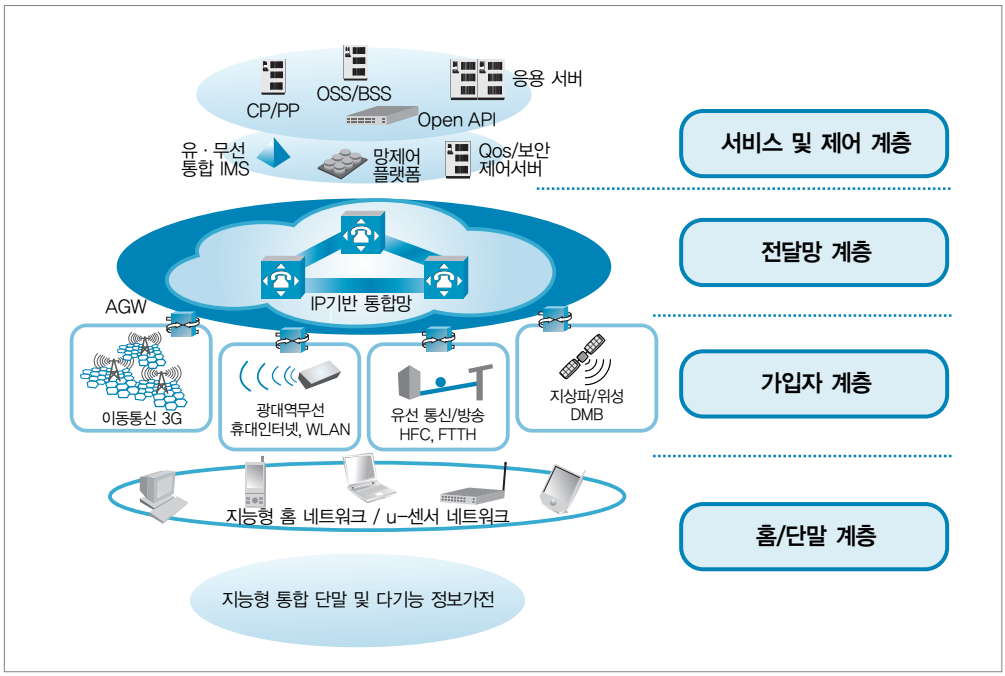
광대역통합망(BcN: Broadband Convergence Network)은 IT839전략의 3대 인프라의 하나로서 통신 · 방송 · 인터넷이 통합되어 언제 어디서나 고품질의 원하는 서비스를 제공하기 위한 차세대 통합 네트워크이다.

'BcN 구축 기본계획' 에서는 BcN에 대해 다음과 같이 정의하고 있다.

[표 1-1] BcN 정의 및 특성

정의	통신 · 방송 · 인터넷이 통합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김없이 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크
특성	① 음성 · 데이터, 유 · 무선, 통신 · 방송 융합형 멀티미디어 서비스를 언제 어디서나 편리하게 이용할 수 있는 서비스 통합망 ② 다양한 서비스를 용이하게 개발 · 제공할 수 있는 개방형 플랫폼(Open API) 기반의 통신망 ③ 보안(Security), 품질보장(QoS), IPv6가 지원되는 통신망 ④ 네트워크, 단말 등에 구애받지 않고 다양한 서비스를 끊김없이(Seamless) 이용할 수 있는 유비쿼터스 서비스 환경을 지원하는 통신망

(그림 1-1) 광대역통합망(BcN) 계층



다양한 융합형 서비스를 제공하기 위해 BcN망을 아래 그림과 같이 계층별로 구분한다.

BcN 망의 계층은 개방형 서비스와 차별화된 서비스 품질 제어, 가입자 및 전달망 자원을 제어하고 서비스 사용자 인증기능을 제공하는 서비스 및 제어 계층, 가입자망 접속에 대한 통합과 품질보장형 Service Edge Node 및 Label Switch 중심의 BcN Core 망으로 차별화된 품질 제공 및 세분화된 보안성을 제공하는 전달망 계층, 통신·방송 통합 및 단대단 품질 보장을 위한 FTTH, HFC 고도화와 Common Access Node를 통한 가입자망을 통합하고 있는 가입자망 계층, 지능형 홈서버와 유비쿼터스 단일망의 홈 네트워크 서비를 제공하는 홈 및 단말 계층으로 이루진다.

정부에서는 2010년까지 BcN 구축 완료를 목표로 국내 주요 통신사업자와 장비 업체들이 참여하여 BcN 시범사업 추진을 통해 단계별로 망 구축 추진 및 음성·영상전화 서비스, TV포탈, 실시간 방송, u-Work 등의 다수의 통합 서비스를 준비 중에 있다. 'BcN 구축 기본계획'에서는 2010년까지 1단계('04~'05) 유·무선 연동 및 통신·방송 서비스 기반 구축, 2단계('06~'07) 유·무선 통합 및 통신·방송 융합 서비스 제공, 3단계('08~'10)에서 광대역 통

신 · 방송 · 인터넷 통합망 완성을 목표로 BcN 망 구축을 진행하고 있다.

이러한 음성 · 데이터 · 영상 · 멀티미디어 등 다양한 형태의 정보가 여러 이기종 망을 경유하여 광대역으로 통합 서비스되는 BcN 환경에서, 안전한 서비스 제공을 위해서는 BcN 인프라에 대한 보호가 우선적으로 선행되어야 할 필수 조건이다.

이중에서도 BcN은 PSTN, WiBro, 인터넷, WCDMA 등 다양한 이기종 망이 통합되어 IP기반에서 서비스를 제공하므로 가입자망 연동에 따라 각기 다른 가입자망이 갖는 내부 취약점이 타 가입자망에서 접속하는 서비스 사용자에게도 노출될 수 있고, 다양한 가입자망 연동 및 초고속 · 광대역화로 인한 침해사고가 타 망으로의 급속한 확산에 따른 피해 및 파급효과 또한 매우 크고 심각하게 된다. 또한, BcN 망에서는 IP망이 가지는 전통적인 보안 취약점을 상속하므로 이로인한 보안문제도 여전히 존재하게 된다. 따라서 BcN 정보보호를 위해서는 이러한 BcN 인프라 정보보호가 우선적으로 다루어져야 할 필요가 있다.

이를 위해 정보통신부, KT, 하나로 텔레콤, SKT, 데이콤 등의 BcN 시범사업자, ETRI, TTA 등 유관기관 등이 참여하는 BcN 정보보호 연구반을 구성하여 BcN 인프라 보호를 위해 BcN 연동구간 중심의 정보보호 위협과 보안 대책을 도출하여 본 가이드를 개발하였다.

제2절 가이드 목적 및 범위

본 가이드는 통신사업자, 시스템 개발자 등이 안전한 BcN 환경 구축에 참조할 수 있도록 BcN 인프라 및 망간 연동시의 정보보호 문제점에 대한 기술적, 관리적, 정책적 정보보호 권고사항들을 제시하기 위한 목적으로 개발되었다. 본 가이드에서 다루고 있는 BcN의 범위는 다음 표와 같다.

[표 1-2] 가이드 적용 범위

분류	적용범위
BcN 계층 측면	• 전달망 및 가입자망 계층 • 서비스 및 제어 계층 일부
BcN 구현 측면	• 적용 구간 – 전달망 내부 및 전달망과 가입자망이 연결되는 구간 (연동구간) • 적용 장비 – Gateway 등 전달망 및 가입자망 연동구간에서 연동기능을 담당하는 주요장비 – 소프트스위치 등 전달망 및 가입자망 계층에서 서비스 및 제어를 담당하는 주요장비 – DNS 등 IP 망에서 기반 서비스를 제공하는 장비

본 가이드에서 제외된 서비스와 홈 · 단말 경우에는 적용되는 기술이 다양하여 각 서비스별로 차별화된 접근이 필요하며, 망 내부에 종속적이거나 단순 전송을 담당하는 장비의 경우에는 공격자가 접근이 어렵거나 기존의 기술들을 활용할 수 있기 때문에 제외하였다.

제3절 가이드 구성 및 활용방법

안전한 BcN 인프라 구축을 위해 제시된 본 가이드는 총 7장과 부록으로 구성되어 있다. 각 장의 구성과 내용을 살펴보면 다음과 같다.

우선, 제2장에서는 NGN 보안표준 추진동향을 ITU-T의 보안 표준화를 중심으로 설명하고 있고, 국내 BcN 포럼에서 추진하고 있는 BcN 표준모델 II(안)을 중심으로 BcN 망에서의 보안 요구사항 등을 설명하고 있다. 제3장에서는 BcN 시범사업 현황을 기반으로 BcN 아키텍처를 구성하고, 연동구간 및 연동 Case를 분석하여 주요 연동장비를 식별하여 본 가이드에서 다룰 보호대상으로 선정하였다. 제4장에서는 3장에서 제시한 BcN 아키텍처와 보호대상 장비를 중심으로 서비스 거부, 품질 저하 등 BcN 연동구간에서 발생 가능한 보안 위협을 상세히 설명하였다. 제5장에서는 4장에서 설명한 BcN 보호대상에 대한 보안위협별로 사용자 인증, 암호화 적용 등의 보호대책을 상세하게 설명하고 있다. 제6장에서는 BcN을 지속적 · 체계적으로 보호하기 위해 사업자가 활용할 수 있는 기존의 제도, 서비스 제공 및 망구축 단계에 따라 사업자가 고려해야할 내용 등의 정보보호 전략을 제시하고 있다.

또한, 안전한 BcN 인프라 구축을 위하여 [부록1]에서는 3장에서 도출한 보호대상 장비에 대한 기능을 분석하여 설명하고 있고, [부록2]에서는 각 장비의 운영체제인 윈도우와 유닉스가 갖는 공통적인 시스템 해킹 위협과 대책을 제시하고 있다. 마지막으로 [부록3]에서는 사업자가 쉽게 보호대책을 점검해 볼 수 있도록 5장에서 설명한 보안대책을 장비별로 매핑하여 보호대책 체크리스트를 제시하고 있다. 보호대책 체크리스트는 BcN 사업자, 학계, 유관기관 등의 검토를 통해 산정한 대책의 중요도를 포함하고 있다.

제 2 장 BcN 정보보호 표준화 추진현황

제1절 BcN 표준화 개요

유선망, 무선망, 방송망 등 액세스 기술 영역별로 네트워크 표준화가 진행되어 왔으나, 통합화 · 융합화가 진행됨에 따라 광대역통합망으로서 차세대 네트워크가 가져야할 요구사항 및 속성을 종합적으로 도출하고 새로운 네트워크 아키텍처를 설계하는 BcN 표준화 작업이 필요하게 되었다. 이에 따라 각 표준화 단체에서는 다음과 같은 BcN 망의 기능적 목표를 도출하였다. BcN망은 IP를 기반으로 하는 네트워크이지만 현재의 IP가 갖는 기능적 한계를 넘어 다음과 같은 속성들을 요구하고 있다.

① 응용 서비스에서 요구하는 수준의 전송대역폭을 제공하고, 단대단 QoS를 보장하여야 한다.
② 무선과 유선, 다양한 무선 네트워크 사이에 연결이 끊기지 않도록, 이동하면서 각 네트워크 사이의 연동이 이루어져야 한다.
③ 사고 또는 고의적인 망 훼손에 대해 망의 견고성이 보장되어야 한다.
④ 웜, 바이러스 등에 의한 비정상적인 트래픽 증가에 능동적으로 대처함으로써, 망의 생존성이 보장되어야 한다.
⑤ SLA에 따라 사용자별로 차별화된 서비스를 제공할 수 있어야 한다.
⑥ 방송형 서비스, 공동 작업형 서비스를 위한 멀티캐스트, 다자간 통신 메커니즘을 지원할 수 있어야 한다.

⑦ 서로 다른 사업자간의 연동이 이루어져야 하며, 이를 위해 필요한 관리정보가 공유되어야 한다.

⑧ IPv4망으로부터 순조롭게 IPv6망으로 전환되어야 한다.

⑨ 다양한 유 · 무선 액세스 망을 수용하여야 한다.

⑩ 공익형 서비스를 지원하여야 한다. 예를 들어, E112, E119 등에서 위치정보를 제공하고, 긴급통신을 우선적으로 처리할 수 있어야 한다.

BcN 표준화에서는 네트워크 관점에서 기능적 요구사항, 네트워크 아키텍처 및 프로토콜과 서비스 관점에서 각 각의 네트워크 하부구조에 의존적으로 제공되던 서비스를 BcN이라는 통합된 하부구조에서 끊김없이 제공하기 위한 서비스 아키텍처, 서비스 처리 절차, 서비스 연동 등을 다룬다.

제2절 국외 NGN 보안 표준화 동향

1. NGN 표준

NGN(Next Generation Network)은 패킷 기반의 통신 서비스를 제공하기 위한 네트워크로서, 광대역 고속 통신이 가능하고, 처리능력 및 전송 지연 등의 서비스 품질이 보장되며, 전달기술과 서비스 기술이 독립적이며, 완전한 이동성을 지원하는 ITU-T가 개발중인 차세대 통신망이다. NGN은 그림 1과 같이 트래픽 전달 측면에서 코어 전달 기능과 액세스 전달 기능으로 구성되며, 자원 및 서비스 제공 측면에서 사용자에게 종단간 연결을 위한 전달 계층(Transport Stratum)과 타 망과의 연결과 멀티미디어 서비스 제공을 포함한 응용 서비스를 다루고 있는 서비스 계층(Service Stratum)으로 구분할 수 있다. NGN은 기존의 별개 망으로 운영되는 유선망과 무선망이 하나로 통합된 액세스 망과 코어 전달망을 통하여 인터넷 전화 서비스(VoIP, Voice over IP), 방송 서비스 등의 다양한 멀티미디어 서비스까지를 제공할 수 있는 컨버전스 망이라고 할 수 있다. 따라서 음성 서비스는 물론 멀티미디어 서비스와 인터넷 서비스가 동시에 제공될 수 있다. 현재 ITU-T에서는 NGN을 위한 기술과 표준을 개발하고 있으며, NGN 보안 표준은 여러 SG들이 협력하여 개발하고 있다.

2. NGN 보안 위협

NGN에서의 보안 위협은 크게 (1) 사용자 관점에서 메시지의 도청, 패스워드 등의 중요 기밀정보의 도난 및 손실, 원하지 않은 스팸, 아이디 도용, 바이러스/웜/스파이웨어로부터의 단말 오염, 사용자에 대한 프라이버시 손실, 서비스 가용성 부재, 그리고 공격자에 의한 과도한 트래픽 집중을 통한 단말에 대한 트래픽 플러딩(flooding) 공격 등이 있으며, (2) 서비스 제공자 관점에서 서비스의 도용, 서비스 거부 공격 등 망에 대한 사이버 공격, 네트워크 구조의 인가되지 않은 공개, 그리고 비인가된 네트워크 설정 및 구조 변경 등이 있다.

이외에 정확히 위협이라고는 할 수 없으나 멀티미디어 서비스를 제공하기 위한 방화벽 등의 망설비의 설정 변경 등이 요구되고 있다. NGN 보안은 이러한 위협을 제거하는 여러 가지 대책이 강구될 것이다.

3. 보안표준 추진내용

현재 ITU-T에서 NGN을 위한 보안 표준은 NGN 보안표준을 주도하는 SG13, 보안 활동을 주도하고 있는 SG17, 그리고 망관리 측면의 보안 문제를 다루는 SG4, 신호 방식과 신호채널에 대한 보안을 표준화하고 있는 SG11, 그리고 멀티미디어 보안을 개발하고 있는 SG16에서 분산적이고 협력적으로 개발되고 있다. SG4에서는 연구과제 7에서 통신망 관리에 대한 인터페이스에 대한 보안 요구사항을 정의하고 있고, SG11에서는 연구과제 7을 중심으로 신호 방식을 위한 액세스 보안을 정의하고 있으며, SG13에서는 연구과제 15를 중심으로 보안 일반 및 인증 요구사항과 보안 가이드라인을 정의하고 있으며, SG16에서는 연구과제 25을 중심으로 인터넷 컨퍼런스를 위한 ID 인증관리 구조인 ID 페더레이션 등에 대한 표준을 정의하고 있다. SG17에서는 연구과제 5, 6, 7, 9를 중심으로 NGN을 위한 인증 및 키관리 프레임워크에 대한 표준화, 사이버 보안 가이드라인, 정보보호 관리 체계, 그리고 안전한 패스워드 인증 가이드라인 등에 대한 표준을 각각 추진하고 있다.

NGN을 개발하기 위하여 ITU-T 외부 표준화 기구는 ETSI, IETF, ATIS, ISO/IEC SC27, 3GPP, 3GPP2 등 대부분의 국제 표준화 단체가 협력하여 NGN을 개발하고 있다. 특히 ETSI의 TISPAN(Telecommunication and Internet converged Services and Protocols for Advanced Networking)에서는 위험 분석 등의 보안 표준이 개발되었으며, 이의 수용 여부가 주목되고 있다.

현재 ITU-T가 개발 중인 대표적인 NGN 보안 표준은 지난 2004년 6월에 시작하여 2005년 11월에 활동을 종료한 포커스그룹 NGN(Focus Group NGN)의 결과 문서로 현재 SG13으로 이전하여 보완 개발 중인 NGN 보안 요구사항 문서와 NGN 보안 가이드라인 문서가 있다. 보안 요구사항에서는 NGN 이 가져야 할 기본 보안 요구사항을 제시하고 있으며, 구체적으로 키 관리 기능이 제공되어야 한다는 일반 보안 원칙 등을 기술한 일반 보안 요구사항, 확장 가능한 보안 구조를 가져야 한다는 일반 보안 목표, 기본적으로 요구되는 보안 서비스를 정의한 보안 서비스 정의, 전달 계층의 보안 요구사항, 서비스 계층의 보안 요구사항을 다루고 있다.

먼저 서비스 계층의 경우, (1) 멀티미디어 서비스를 제공하는데 필요한 IMS(IP Multimedia Service) 코어 망 보안구조, (2) 보안 구조에서 인터페이스에 대한 보안 요구사항을 다룬 IMS

보안 구조 인터페이스 요구사항, (3) 서비스 및 자원 제어 서브시스템간에 보안 문제를 다룬 코어 네트워크의 전달 영역 보안, (4) 자원에 대한 응용 요구에 응답하기 이전에 접근제어 및 인증의 문제를 다루는 응용 보안, (5) NGN을 통한 인터넷 전화(VoIP, Voice over IP) 트래픽에 대한 기밀성과 사용자 ID 보호 등의 문제를 다루는 VoIP 보안, (6) 재난 상황에 대비한 위기 통신망 서비스와 재난복구 통신망 보안, (7) 공개 서비스 플랫폼 및 부가가치 서비스 간에 보안 등의 보안 요구사항 등을 다루고 있다.

전달 계층의 경우, 보안 요구사항은 (1) 가입자 장치와 가입자 게이트웨이 간에 가입자 댁내 보안, (2) NGN 액세스 망인 IP-CAN(IP-Connectivity Access Network) 자원 요구를 위하여 필요한 인증 및 접근제어 등의 보안 기능 요구사항을 제시한 가입자 망과 IP-CAN간에 인터페이스 보안, (3) 네트워크 장치와 신호 장치에 대한 보안 요구사항에 대한 코어 전달망 보안, (4) 원격 가입자의 홈 게이트웨이로의 원격 인증과 인가에 대한 원격 NGN 가입자 보안 등에 대한 보안 요구사항을 다루고 있다.

안전한 NGN을 구축하기 위한 일반 보안 원칙과 세부 보안 가이드라인에 대하여 기술하는 NGN 보안을 위한 가이드라인은 (1) NGN 보안 위협과 보안 대책, (2) 응용, 서비스, 패킷,그리고 링크 계층으로 구성되는 4 계층 기반 보안 모델과 보안 연관, 그리고 (3) 구성 서브 시스템에 대한 보안 등에 대한 기본 가이드라인을 기술하고 있다.

구성 서브시스템 보안의 경우, (1) 트래픽의 전달과 신호 전달을 담당하는 IP-CAN 서브시스템에 대한 네트워크 계층 보안, 링크 계층 보안, 그리고 확장 가능한 인증방식에 대하여 기술하고 있는 IP-CAN 서브시스템 보안 가이드라인, (2) IMS 데이터와 신호에 대한 보안, 베어러 서비스를 보호하기 위한 안전한 실시간 전달 프로토콜(SRTP, Secure Real Time Protocol) 사용, 로밍 서비스를 지원하기 위한 사용자 인증 데이터의 활용, 종단계층 보안 프로토콜인 TLS(Transport Layer Security) 프로토콜, IETF 망계층 보안 프로토콜인 IPSec 프로토콜의 사용을 권하는 IMS 네트워크 영역 및 IMS와 비-IMS간에 보안 가이드라인, (3) IMS 사용자 인증, IMS 보안 구조 하에서 각 구성 서브시스템 간에 보안 가이드라인을 기술하는 IMS 접근 보안 가이드라인, (4) 부가가치 서비스와 공개된 플랫폼 간에 제공되어야 할 보안 서비스를 정의하고 있는 공개 플랫폼 보안 가이드라인, (5) 긴급 통신망 서비스와 재난관리 통신망을 위한 가이드라인, (6) IMS 트래픽의 기존 NAT나 방화벽을 통과하는 문제를 다루는 NAT/방화벽 통과를 위한 가이드라인으로 구성되어 있다.

4. 보안표준 기술 및 향후추진 계획

ITU-T NGN SG13의 연구과제 15에서는 보안 요구사항, 인증 요구사항, AAA 요구사항, 보안 가이드라인, 그리고 기타 세부 보안 기술을 표준화할 것이고, SG17의 연구과제 5에서는 NGN을 위한 인증 및 키관리 프레임워크를 개발할 것이며, SG11에서는 신호 방식을 위한 액세스 보안표준을 개발할 예정이다. 현재까지의 표준화 실적을 근거로 NGN을 위하여 향후에 개발되어야 할 주요 표준화 항목은 다음과 같이 도출될 수 있다.

- NGN에 적용 가능한 암호 알고리즘 슈트(타원곡선 암호 알고리즘 슈트 포함)
- 확장 가능한 인증방법, AAA(Authentication, Authorization and Accounting) 프로토콜, 기타 요소 암호 프로토콜 등에 대한 기본 암호 프리미티브
- 최종 사용자와 네트워크 요소에 대한 사용자 친화적인 키 분배 및 관리
- 터미널 이동성과 네트워크 이동성을 위한 공개키 기반구조를 포함한 인증 기반구조
- NGN을 통하여 사용자 및 기기의 위치 추적을 막기 위한 사용자 및 네트워크 프라이버시 보호
- 멀티미디어 서비스를 위한 IMS 솔루션에 대한 보안 가이드라인
- NGN 코어 네트워크 보호하기 위한 능동적인 침입 탐지 및 차단을 포함한 보안 가이드라인
- IETF에서 표준화한 IPSec, TLS, SRTP 등의 기존 보안 프로토콜의 적용 및 구현을 위한 가이드라인
- DSL(Digital Subscriber Loop), WLAN(Wireless LAN), 케이블 접근 망 시나리오를 위한 액세스 망을 위한 보안
- NGN을 통하여 등급화된 보안 서비스를 제공하기 위한 보안 정책 가이드라인
- 인터넷 멀티미디어 응용 세션 개시 프로토콜을 위한 홉대홉 및 종단간 SIP(Session Initiation Protocol) 보안
- NGN 재난복구와 위기 관리를 위한 가이드라인
- NGN을 통한 N-RFID(Networked Radio Frequency ID) 보안
- 실시간 응용을 위한 NAT/방화벽 통과 문제

향후에는 상기와 같은 도출된 내용을 중심으로 각 SG들간의 적절한 역할 분배를 통하여 NGN 보안 표준이 개발될 것으로 예측되며, ETSI의 TISPAN과 IETF 등의 국제 표준화 기구 간의 협조 하에 추진될 것이며, 특히, SG13에서는 보안 요구사항 및 가이드라인을 중심으로, SG17에서는 세부 보안 핵심 기술을 중심으로, SG11에서는 신호 방식 보안을 중심으로 수행될 예정이다.

제3절 국내 BcN 보안표준화 동향

1. BcN 표준모델 개요

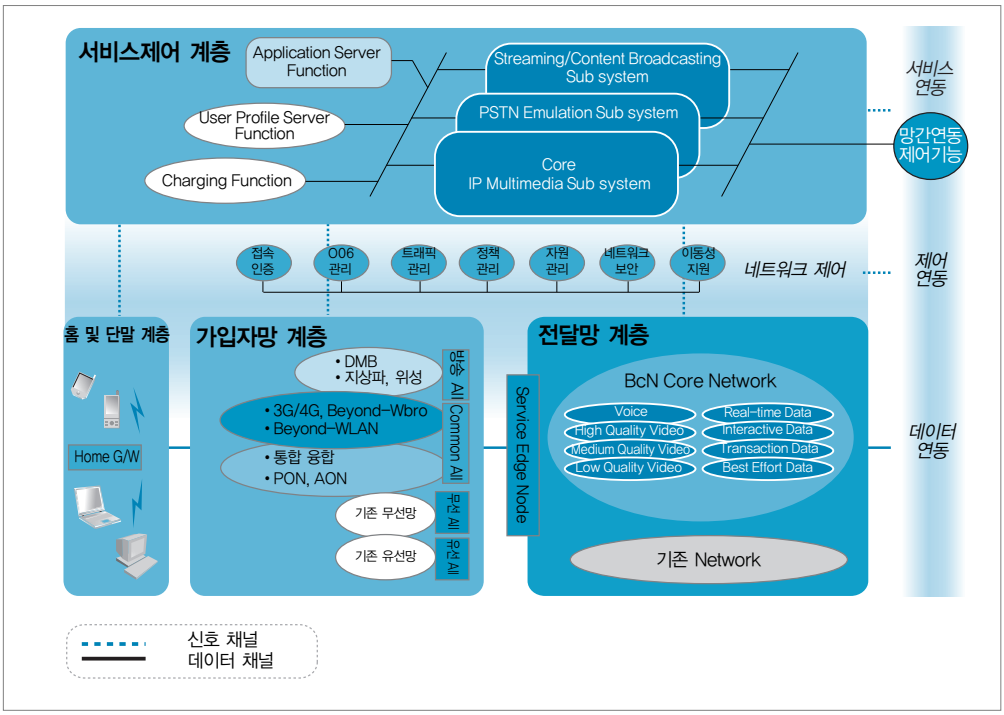
BcN 표준모델은 BcN 구축 목표를 실현하기 위한 망 구조, 기술 및 서비스 제공기준에 대한 가이드라인으로 논리적 기능 모델이 아닌 네트워크의 구축에 초점을 둔 실현 중심의 네트워크 모델이다. 표준모델은 음성/데이터/유무선/통신 · 방송의 서비스 수용이 가능한 네트워크 모델을 수립하고 BcN 구축 및 서비스 분야의 표준화 선도를 위해 필요하며 이는 각 사업자에 의해 선택적으로 활용될 수 있을 것으로 기대하고 있다. BcN 표준모델에서는 최종적으로 가입자에게 QoS가 보장되며 서비스 측면에서 음성/데이터/유무선/통신 · 방송의 어떤 조합이라도 수용 가능한 네트워크 모델을 제시하는 것을 목표로 하고 있다.

2. BcN 표준모델 II(안) 구조

BcN 표준모델 II(안)에서 제시하는 BcN 구조의 개념도는 옆과 같다.
BcN 표준모델 II(안)에서 제시하는 각 계층별 특징을 정리하면 다음과 같다.

① 서비스 제어 계층 : 신규서비스 도입에 용이한 개방형 서비스와 차별화된 서비스 품질 제어/서비스 사용 인증 기능 제공
② 네트워크 제어 : 요청된 서비스에 따른 가입자 및 전달망 자원의 제어와 가입자 접속 인증 기능 제공
③ 전달망 계층 : 다양한 가입자망 접속에 대한 통합과 품질보장형 Service Edge Node 및 Label Switch 중심의 BcN Core 망으로 차별화된 품질 제공 및 세분화된 보안성 제공
④ 가입자망 계층 : 통 · 방 통합 및 단대단 품질 보장을 위한 FTTH, HFC 고도화와 Common Access Node을 통한 가입자망 통합
⑤ 홈 및 단말 계층 : 지능형 홈서버와 유비쿼터스 단일망의 홈네트워크
⑥ 연동 : 연동은 크게 전달망 연동, 망 제어 연동, 서비스 연동으로 나눌 수 있음. 전말망 연동은 물리적인 측면에서 네트워크 기술간의 연동을 말하며 망 제어 연동은 네트워크 자원에 대한 제어와 트래픽에 대한 인증, 보안, 사용자 정책 등을 관리하며 서비스 연동은

(그림 2-1) BcN 표준모델 구조도



여러 서비스 제공 서버들을 활용하여 사용자에게 끊김없는 서비스를 보장한다.

3. BcN 표준모델 II(안) 보안요구 사항

BcN 표준모델 II(안)에서는 다음과 같은 보안기능을 요구하고 있다.

- 전달망에서 보안기능은 능동적 침해대응 체계 구축과 유해 트래픽의 침입 차단이 가능해야 한다.
- 망 통합 및 연동에 따른 보안피해의 확산 방지를 고려해야 한다.
- 이종망간의 상호연동에 따른 접근통제 및 인증이 고려되어야 한다.
- SEN에서 인증된 가입자 정보는 전달망에 해당정보를 알려 줄 수 있어야 하며, 이에 따른 자원의 예약이나 Traffic제어 기능을 수행 할 수 있어야 한다.
- 요금 및 정산을 위해 망사업자의 관문 백본의 경우 해당정보를 기록할 수 있어야 하며, 마

찬가지로 과금 및 정산서버에 해당 정보를 알려 주어야 한다.

- 다양한 접속 방식 및 융합서비스 환경에서 이동체 (단말, 사용자, 네트워크 등)의 서비스에 대한 연속성을 보장할 수 있는 인증/권한 기술, 위치 관리 기술, 핸드오버 기술 등의 개발이 필요하다.
- 전달망의 경우 타망과의 연동 시 요금 및 정산을 위해 해당정보를 기록할 수 있어야 하며, 마찬가지로 과금 및 정산서버에 해당 정보를 알려 주어야 한다.

4. BcN 구축단계별 보안목표 및 고려사항

BcN 표준모델 II(안)에서는 BcN 구축단계별 네트워크 보안 목표 및 고려사항을 아래와 같은 사항을 논의하고 있다.

- 1단계 보안목표
  - 네트워크 안정성 확보를 위하여 DDoS 및 Worm 등의 해킹공격에 대응능력을 갖는 보안시스템 확보
  - 국가적인 차원의 통합보안체계 마련 및 주요 사업자의 통합관제센터 구축

- 2단계 보안목표
  - 서비스/제어망, 전달망 및 가입자망에서 유해 트래픽을 실시간으로 감시하고 차단할 수 있는 수준의 고성능 보안시스템의 구축
  - 사업자별 네트워크 통합형 보안관리 시스템 구축 및 망 연동을 위한 상호 인증체계 마련

- 3단계 보안목표
  - 능동적으로 위험요소를 찾아 차단 및 추적할 수 있는 보안시스템 구축
  - 통신, 방송, 신규서비스(USN, RFID, 홈네트워크 등)에 대한 통합보안관리 시스템 및 통합인증 체계 구축

이러한 보안 목표를 달성하기 위한 주요 고려사항은 다음과 같다.

- BcN 전달망에서 네트워크 보안 방안 마련
- BcN 인프라 대비 네트워크 보안장비의 성능저하에 따른 보안 취약점 해결방안 적용
- 망 통합 및 연동에 따른 피해확산 방지
- 유무선, 방송환경에서의 도감청 및 데이터 위 · 변조 방지
- 이종망간의 상호연동에 따른 접근통제 및 인증 관련 취약성 고려
- IPv4와 IPv6의 병행사용에서의 End-to-End 보안 확보 방안 등 이다.

BcN 표준모델 II(안)에서는 위와 같은 보안 목표와 고려사항을 적용하기 위해, 사업자의 보안관리체계 수립 및 통합보안관리센터 구축 의무화, 네트워크 보안장비의 필수기능에 대한 인증제, 사업자 및 Service Provider에 대한 보안평가 등급제 실시 등의 정책적으로 보안에 대한 준수 기준을 마련하고, 장비의 상호호환성 확보를 위하여 규격 및 보안기술의 인터페이스 표준 추진, BcN의 통합서비스 제공이 가능할 수 있도록 통합인증 표준 마련 등 보안 표준 추진화의 정책적 추진방안을 제시하고 있고, 이에 대한 포럼 차원의 활발한 논의가 일어나고 있다.

제 3 장 BcN 정보보호 영역 및 대상

제1절 BcN 시범사업 추진현황

1. 시범사업추진 개요

지난 2004년 2월, 제22차 정보화추진위원회의 심의를 거쳐 "BcN 구축 기본계획"을 확정하고, 동 기본계획에 따라 1단계('04~'05년) BcN 구축 사업을 통한 차세대 정보인프라 구축을 본격 추진하였다. 이후, 정보통신부는 정보화촉진기본법 제26조 규정에 의거하여 u-Korea 실현을 위한 핵심인프라인 광대역 통합 정보통신기반을 조기에 구축하고, 공공 및 민간분야에서의 BcN 서비스 이용을 활성화 할 수 있도록 2006 ~2010년까지 추진할 "BcN 구축 기본계획 II"을 제시하고 있고, 이에 따라 한국정보사회진흥원(구 한국전산원) 주관으로 BcN 시범사업을 추진하고 있다.

한국정보사회진흥원 주관으로 2004년부터 2005년까지 수행된 1단계 BcN 시범사업은 다양한 초기 BcN 서비스를 발굴하고, 이와 관련된 기술 검증을 통한 시범 서비스 이용 활성화를 위한 것으로, 4개 컨소시엄, 220여개 업체(통신방송사, 제조업체, 연구소 등)가 참여하였으며, 영상전화 등 40여개 초기 BcN 서비스 모델을 발굴하였고, 컨소시엄별 BcN 시범망을 구축하여 수도권 외 6개 지역에서 총 2,076 가구를 대상으로 시범서비스를 제공하였다. 각 컨소시엄별 주관사 및 시범지역은 아래 [표3-1]과 같다.

[표 3-1] BcN 시범사업 컨소시엄 구성

컨소시엄	주관사 (참여사 수)	총투자예상 (정부/민간)	시범지역 (이용가구수)
Octave	KT (14개사)	145.5억원 (28.5억/117억)	서울, 대구, 광주 (426여 가구)
광개토	데이콤 (13개사)	166억원 (31억/135억)	서울, 경기, 울산 (350여 가구)
UbiNet	SKT/하나로텔레콤 (20개사)	172억원 (27억/145억)	서울, 경기, 대전, 부산 (600여 가구)
케이블 BcN	(주)한국케이블TV수원방송 (178개사)	65억원 (– /65억)	서울, 경기, 대구, 제주 등 (700여 가구)

※ 출처 : 한국전산원, 2005년도 BcN 시범사업 수행 결과, 2005.

2. 옥타브 컨소시엄

(1) 개요

KT가 주관하는 옥타브 컨소시엄은 KTF, 다이렉트미디어, 헤리트, 신지소프트, 캐럿코리아, 헬스피아, 유엔젤, 삼성전자, 코어세스, 코어커뮤니케이션, 아이크로스테크, C&S, 욱성전자, KTI 등 총 15개 회사로 컨소시엄을 구성하여 시범사업을 추진하였다. 총 459가입자를 대상으로 BcN 초기 서비스를 시범적용 하였다. 그리고 시범 서비스 제공을 위하여 음성 · 데이터 콘텐츠는 오락 및 교육용 32종을 확보하고 통신 · 방송 융합을 위한 콘텐츠는 HD급 VoD 콘텐츠는 6 종, 양방향 e-learning 서비스 3종을 확보하여 시범 가구에 제공하였다.

(2) 시범서비스 제공현황

옥타브 컨소시엄에서 제공하는 서비스는 다음 표와 같다.

[표 3-2] 옥타브 컨소시엄 서비스 목록

분 야	중분류	소분류	특징	시범서비스 지역 및 규모	시범 서비스 시기
음성 · 데이터 통합 분야	BcN 음성전화		고품질 영상단말 기반 영상통화 및 멀티미디어 응용서비스 Ethernet, xDSL 망 기반	• 서울 150 가구 (홈네트워크 시범가구 30가입자 포함) • 대구 150 가구 • 대전 100 가구 (POTS 가입자에 국한)	2005.9 ~ 2005.10
	BcN 영상 전화	멀티미디어 CID 서비스			
		멀티미디어 링백 서비스			
		맞춤음성다이얼 서비스			
		통화관리 서비스			
		멀티미디어 메시징 서비스			
		영상콘텐츠 서비스			
		프레즌스통화 서비스			
	B-Learning 서비스				
	B-게임 서비스				
	B-헬스케어 서비스				
	홈시큐어 서비스				
	개방형 서비스	단말상태기반 콘텐츠 서비스			
	멀티미디어 센트릭스 서비스			KT 연구소	
	IP-PBX			한국전산원	
통신 · 방송 통합 분야	양방향 데이터방송 전송서비스	TV-PoII 서비스	기존 초고속 접속 인프라 기반의 서비스 제공	• 서울 30 가입자	2005.9 ~ 2005.10
		T-Commerce 서비스			
		Infotainment			
	네트워크 PVR 서비스		FTTH 인프라 기반의 서비스 제공	• 광주 26 가입자	2004.12 ~ 2005.2
	고품질 실시간 VoD 서비스				
	양방향 e-learning 서비스				

분 야	중분류	소분류	특징	시범서비스 지역 및 규모	시범 서비스 시기
유·무선 통합 분야	유·무선 영상통화 연동 서비스	BcN 영상단말 가입자와 W-CDMA 이동단말 가입자 간 영상통화		• 수도권 100 가입자	2005.9 ~ 2005.10
기타 분야	RFID /USN 서비스	SOHO, 중소기업용 RFID/ USN 호스팅 솔루션 서비스		• 서울소재 물류업체 1개	2005.9 ~ 2005.10
	IPv6 응용서비스	기업 고객 대상 고품질 영상 회의 서비스 제공		• 우면동 연구소 • 분당 본사	

※ 출처 : 한국전산원, 2005년도 BcN 시범사업 수행 결과, 2005.

(3) 시범망 구축현황

옥타브 컨소시엄에서는 차세대 통신망을 패킷 전달 및 미디어 변환을 수행하는 전달 계층, 호/연결 제어를 수행하는 제어계층, 다양한 차세대 통신 서비스를 제공하는 응용 계층으로 구분하고 있다. 특히, 제어신호망, 베어러 트래픽, 운용 관리망을 최대한 분리하여 구축함으로써 각 계층별 트래픽 품질 수준을 만족하고, 망 운영관리의 안정성과 생존성을 확보하고 있다.

소프트스위치는 제어 계층에 위치하며, 호/연결/세션 제어를 수행하는 장비로서 미디어서버 및 응용서버 등 각종 서버를 위한 표준 인터페이스를 제공하며, 액세스 게이트웨이, 트렁크게이트웨이, 시그널링 게이트웨이 등의 시스템과 연동을 주관한다. 지능망시스템(AIN)과 소프트스위치간 사이는 트렁크 게이트웨이와 시그널링 게이트웨이를 통하여 연동하고 있다.

옥타브 컨소시엄에서는 BcN 시범 전달망을 3개 시범지역(서울, 대전, 광주)에 신규 구축하고, 광대역통합연구개발망(KOREN)과의 연동 및 기존 인터넷망인 KORNET, WCDMA 등과 연동하고 있다. 가입자망은 품질 보장형 서비스 제공이 가능한 50M급 VDSL 공급지역 및 신축 아파트 등 Ntopia-E 시설이 공급된 지역, FTTH 시범망을 포함하여 구축하고 있으며, Wibro 망은 서울 및 수도권에 기 구축된 WiBro 시범망과 연동하고 있다.

3. 광개토 컨소시엄

(1) 개요

광개토 컨소시엄은 주관사인 데이콤을 비롯한 LG텔레콤, 파워콤 등의 3개 통신회사와 드림시티방송, 다음커뮤니케이션 등의 방송 및 인터넷회사 그리고 아크로메이트, 욱성전자, 유엔젤 등 제조회사 및 KIST 등 총 15개 회사로 구성되어 1단계 시범사업을 추진하였으며, 시범가구중에서 일반가입자는 서울 은평구, 경기도 부천시, 울산광역시 지역의 350가입자를 대상으로 HFC, 광랜, FTTH 유형의 시범을 실시하고 기관가입자는 광주광역시청, 동서대학교 및 KIST의 70가입자에게 무선가입자망 구축 및 유선영상전화 시범을 하여 총 420가입자를 대상으로 시범을 하였다.

그리고 시범을 위한 방송 콘텐츠는 케이블용 SD급 VoD 콘텐츠는 7편, 케이블용 HD급 VoD 콘텐츠는 다큐 및 교양등 70편을 확보하였으며, HD급 IP VoD 콘텐츠는 12편의 다큐, SD급 IP VoD 콘텐츠는 30편의 영화와 236강의에 달하는 수능강의를 확보하여 시범 가구에 제공하였다. 또한 데이터 방송 콘텐츠 8종, PPV 2종, VoD 6종에 달하는 부가서비스를 제공하고, T-Gov 콘텐츠는 2종의 서비스, TV포털 콘텐츠는 영화, 음악 등 12개 채널을 확보하였고 또한 T-book 콘텐츠는 어린이문고 27권 등 도합 101권에 해당하는 도서물 콘텐츠를 제공하였다.

(2) 시범서비스 제공현황

광개토컨소시엄은 MPLS 기반 품질보장형 상용망을 통해 다양한 통신 · 방송융합 서비스, 유무선 통합 서비스, 음성 · 데이터 통합서비스 등을 제공하는 것을 목표로 하고 있으며, BcN 환경에서의 서비스 모델 발굴, 장비 시험 · 검증, 서비스활성화, 홍보, 연구개발 및 그 성과의 상용화를 목적으로 한다. 특히 1단계 시범사업과는 달리 2단계에서는 통신사업자의 네트워크/서비스 진화 로드맵을 기준으로, 상용화 가능성이 가장 큰 서비스 모델을 시범서비스로 선정하여, 시범사업 기간중 서비스를 제공하고, 시범서비스 이후의 빠른 상용화를 최우선적으로 추진할 예정이다.

2단계에서는 FMC, IPTV를 포함하는 4개의 사업모델을 통해서 10개의 신규 서비스를 포함한 총 23개의 서비스를 개발하며, 이에 필요한 장비, 솔루션에 대해 32건의 시험검증을 거쳐, 600여 시범가구 및 5개 서비스 이용기관에 BcN 시범 서비스를 제공하는 것을 목표로 한다.

광개토 컨소시엄에서 제공하는 서비스는 아래 표와 같다.

[표 3-3] 광개토 컨소시엄 서비스 목록

분야	서비스명	세부 모델	서비스 지역 및 규모	시기
통신 · 방송 통합	DCATV	독립형 데이터방송	• 수도권(100) – HFC 기반 : 100가구 부천 50, 은평 50	• 2005년 7~12월 (HD급 VOD, T-Gov.는 10월부터 서비스 제공)
		T-Gov.		
		HD급 케이블 VOD		
	IP-TV	HD급 IP-VOD	• 울산 (30) – FTTH 기반 : 30가구	
		TV 포털		
유 · 무선 통합	IP BS 기반 유무선 연동	WPBX	• 무선 PDA 보급 – 부산 동서대 : 30가입자 – 광주 시청 : 30 가입자	
		영상전화연동		
음성 · 데이터 통합	BcN 음성전화	CID	• 수도권 (100) – HFC 기반 : 100가구 부천 50, 은평 50 • 울산 (30) – FTTH 기반 : 30가구	
		통화연결음 서비스		
		음성메일		
		통화관리		
		3자통화		
	BcN 영상전화	멀티미디어 CID 서비스	• 수도권 (100) – HFC 기반 : 100가구 부천 50, 은평 50 • 울산 (120) – HFC 기반 : 120가구 • 서울 KIST 영상단말기 : 10 가입자 • 부산 동서대 영상단말기 : 10 가입자 • 광주 시청 영상단말기 : 10 가입자	
		멀티미디어 링백톤		
		통화관리		
		영상메일		
		통화편의		
		영상회의		
	멀티 미디어 메신저	메신저	• 수도권 (100) – HFC 기반 : 100가구 부천 50, 은평 50 • 울산 (120) – HFC 기반 : 120가구 ※메신저 및 통화편의 서비스는 350 가구 제공	
		영상 소프트폰		
		통화편의		
	홈시큐어 서비스	홈지킴이 서비스	• 은평:15 가구 • 부천:15 가구	

분야	서비스명	세부 모델	서비스 지역 및 규모	시기
	개방형 서비스	클릭투콜 서비스	• 울산 (30) – FTTH 기반 : 30가구	• 2005년 7~12월 (HD급 VOD, T-Gov.는 10월부터 서비스 제공)
기타 서비스	IPv6 응용	IPv6 CDMA	– 부산 동서대 : 30 가입자 – 광주 시청 : 30 가입자	
	URC 로봇	감시 등	전산원 및 URC와 추후 협의에 따름	

※ 출처 : 한국전산원, 2005년도 BcN 시범사업 수행 결과, 2005.

(3) 시범망 구축현황

광개토 컨소시엄에서는 1단계 BcN 시범 사업 추진의 노하우를 바탕으로 데이콤이 보유한 사용망에 BcN 모델을 적용할 예정이다. 기존 상용망을 BcN이 요구하는 고기능의 전달망으로 진화시켜, 3단계의 BcN 서비스 상용화 진화에 대한 전략을 마련하고자 한다. 광개토컨소시엄의 BcN 계층별 망구성은 가입자망, 전달망, 서비스 및 제어망의 계층구조로 구성된다. 전달망은 MPLS망으로 된 상용망을 활용하여 구성하고 가입자망은 HFC(차세대HFC), 광랜(유사 FTTH)으로 구성된다. 서비스 및 제어망은 VoIP, MMoIP, IPTV, 인터넷, 이동통신망의 서비스망과 OSS, CSS, AAA, 빌링 등의 제어망으로 구성된다. 광개토 컨소시엄 망의 구성상 특이사항으로는 2단계 BcN 시범망은 데이콤이 보유하고 있는 상용망에 직접 서비스를 도입하는 형태로 추진할 예정이고, 기서비스 중인 상용 가입자에 영향없이 서비스를 도입하는 것을 전제로 하고 있다. 또한, IPv6는 기존망 및 기수용 가입자 보호를 위하여 우선 KOREAv6 별도 망과의 터널링 연동, NAT-PT 연동으로만 추진하고, 시범사업으로 인한 상용망의 영향을 최소화하기 위해 검증된 솔루션을 적용하고, 검증되지 않은 기술 및 솔루션은 가급적 지양하여 추진하고 있다.

4. 유비넷 컨소시엄

(1) 개요

유비넷 컨소시엄은 주관사인 SKT를 비롯하여 하나로텔레콤, (주)리젠, 미리넷, 엔텔스, SK C&C, 제너시스템즈, SK커뮤니케이션, 매일경제TV, 헤리트, 대한전선, 텔코웨어, 욱성전자, 휴림인터렉티브, 프리셋, 유엔젤, 한국디지털위성방송, SK건설, 삼성전자 등 17개 회사로 구

성되어 1단계 시범사업을 추진하였으며, 시범가구 중에서 일반가입자는 서울, 대전, 부산, 분당 지역의 600가입자를 대상으로 VDSL, DCATV, WCDMA, FTTH 유형의 시범을 실시하고 기관가입자는 서울대, 인하대 및 ICU에 유선영상단말 및 VoIP 단말을 제공하였고, 1개의 BcN 체험관을 구축 및 시범을 하였다. 그리고 시범을 위한 방송 콘텐츠는 SD급 DCATV 40개 채널, SD급 SCN 18개 채널, HD급 SCN 1개 채널, SD급 TV 포털 601편, HD급 TV 포털 601편을 확보하여 제공하였다.

BcN 2단계 시범사업의 2006년도는 1단계 수행결과를 기반으로 BcN 1단계 서비스 고도화 및 상용화를 추진하고, 테스트베드 구축을 통한 신규 서비스 기술검증 등을 목표로 한다. 2007년도는 BcN 서비스 개술개발 완료, 장비 및 솔루션, 시스템에 대한 개발, 시험 · 검증을 완료할 예정이다. 또한 700가구 이상에 BcN 시범 서비스를 제공하고 체험관 구축을 통한 홍보활동 등을 계획하고 있다.

(2) 시범서비스 제공현황

유비넷 컨소시엄은 다음 표와 같은 서비스에 대해 전체 700가구를 대상으로 시범 서비스 제공한다. BcN 시범 서비스에서 제공하는 서비스는 음성 · 데이터 통합, 유무선 연동 및 통합, 통방 융합 서비스 및 기타 서비스로 구분하고 있고, 유비넷 컨소시엄에서 제공하는 서비스는 아래 표와 같다.

[표 3-4] 유비넷 컨소시엄 서비스 목록

<table>
<tr><th>분야</th><th>서비스명</th><th>세부 모델</th><th>서비스 지역 및 규모</th></tr>
<tr><td rowspan="8">음성 · 데이터
통합 서비스</td><td rowspan="6">BcN영상전화</td><td>고품질 영상전화 서비스</td><td rowspan="8">〈분당〉
• 유선 영상단말(200)
• PDA(CDMA) (105)
• 영상Phone(120)

〈동작/성북〉
• 유선 영상단말 (50)
• PDA/CDMA (87)
• AP/무선랜카드 (50)

〈대전〉
• 유선 영상단말 (50)
• PDA/CDMA (30)
• AP/무선랜카드 (150)
• 유선전화기 (100)
• VoCM(100)</td></tr>
<tr><td>멀티미디어 컬러링 서비스</td></tr>
<tr><td>멀티미디어 레터링 서비스</td></tr>
<tr><td>대체 영상 제공 서비스</td></tr>
<tr><td>영상사서함 서비스</td></tr>
<tr><td>멀티미디어 컨퍼런스</td></tr>
<tr><td colspan="2">가입자 정보 기반 서비스</td></tr>
<tr><td colspan="2">통합 메시징 서비스</td></tr>
</table>

분야	서비스명	세부 모델	서비스 지역 및 규모
유무선 연동 및 통합 서비스	IMS(무선)와 Softswitch(유선) 연동 서비스		〈부산 (하나로)〉 • 유선 영상단말 (50) • PDA/CDMA (30) • AP/무선랜카드 (50)
	WCDMA 영상전화 연동 서비스		
	개방형 서비스(커뮤니티 서비스)		
통방융합	DCATV	디지털 다채널 방송 서비스	〈분당〉 • IP STB(150) • DMB단말(93) • 동작/성북 • IP STB(50) • SCN STB(50) • DMB단말 (6) 〈대전〉 • IP STB(50) • CABLE STB(100) • DMB단말 (22) 〈부산(하나로)〉 • IP STB(50) • DMB단말(22)
	SCN	디지털 다채널 방송 서비스	
		T-Banking	
	TV포털	HD/SD급 VOD (HD급 체험관수준)	
		T-Game	
		T-Communication	
	위성 DMB 서비스		
기타	IPv6 응용 서비스	영상전화	Test-bed or 분당 체험관(1)
	RFID/USN 서비스	정보제공 서비스	분당 체험관(1)
		영상 메시징 서비스	
	ZBPMS 응용 서비스	u-Zone Coupon/Info 서비스	
		Contents Push서비스 (뉴스, 날씨 등)	
		영상 메시징 서비스	
	URC 서비스		동작 (7), 동작 홍보관 (1)

※ 출처 : 한국전산원, 2005년도 BcN 시범사업 수행 결과, 2005.

(3) 유비넷 시범망 구축현황

유비넷 컨소시엄의 BcN 시범망 구축현황은 수도권(분당), 광주, 부산, 첨단 연구개발망을 활용하여 연구기관 및 공공기관에 BcN 시범 서비스를 제공하고 있다.

유비넷 컨소시엄에서 구축하고 있는 가입자망은 Ethernet, HFC, FTTH(DWDM-PON,AON)등의 유선가입자망, EV-DO, WCDMA, WiBro, WLAN, USN 등의 무선 가입자망, 위성 DMB, 지상파/위성방송(DTV), CATV 등의 방송망을 활용하여 서비스를 제공한다. 그리고 연구기관 및 공공기관에 BcN 서비스를 제공하기 위하여 첨단 연구개발망을 적극활용하고 있다. BcN 응용서비스 제공을 위한 서버군과 Test-Bed 및 제어망은 분당 및 동작에 설치하며, BcN 시범 사이트를 상호연결하기 위해 유선사업자의 전달망을 활용한다. IPv6의 경우 IPv6 lsland 형태로 Test-Bed와 일부 사이트에서 서비스를 제공하며, 보안을 강화하기 위하여 서비스를 제공하는 주요 시설에 보안 시스템을 구축한다.

5. 케이블 컨소시엄

(1) 개요

케이블 컨소시엄은 KDMC를 비롯한 4개 DMC(Digital Media Center)와 70여개의 SO가 연합하여 서울(강남, 서초, 양천, 도봉), 안양, 대구, 제주 지역의 700 가구를 대상으로 시범 서비스를 하였다.

그리고 시범 서비스를 위한 방송 콘텐츠는 민간 방송으로 영화 PP 방송 등 13개 채널로 212,260 시간을 확보하였으며, 공공 방송으로는 국정홍보 PP 방송 등 3개 채널 17,280 시간을 확보하고 VoD 콘텐츠는 MoD 등 1,200 편 1,360 시간이었고 HD 콘텐츠는 영화 및 스포츠 등 249편 232 시간을 확보하여 시범 가구에 제공하였다.

(2) 시범서비스 제공현황

케이블 컨소시엄이 제공한 서비스는 4개 분야 27개 서비스이다.

[표 3-5] 케이블 컨소시엄 서비스 목록

분야	세부 모델	내 용	서비스 시점
방송 · 통신 융합 서비스 ;TPS	디지털방송	720(h)× 480(v)(MP@ML) SD급의 표준해상도 화질 서비스 Dolby 5.1채널의 고음질 서비스 100 채널 이상의 다채널 24시간 서비스	2005년 상용
	초고속인터넷 (200M급 ISP)	DOCSIS 표준의 케이블 모뎀 기반 인터넷 서비스 최대 하향 속도 200Mbps	2005년 시범, 2006년 상용
	VoIP	광동축혼합망(HFC; Hybrid Fiber Coaxial)을 이용한 IP 기반의 인터넷 전화 내부 가입자간 통화, 시내/시외/국제전화 /이동전화와의 통화	2005년 시범 2006년 상용
		1920(h)× 1080(v)(MP@HL), 16:9 와이드 화면비의 HD급 고해상도 화질 서비스 Dolby 5.1채널의 고음질 서비스 7개 채널의 24시간 서비스	2006년 시범 및 상용
VoD 서비스	Real VoD Subscription VoD Near VoD Free On Demand	BcN HFC망을 이용한 고속의 Video on Demand 서비스 영화, 드라마, 교육, 스포츠, 성인물 등 다양한 종류의 콘텐츠 제공	2005년 상용
양방향 데이터 방송 서비스	T-Government	BcN HFC망과 디지털 케이블TV를 이용한 양방향 TV-전자정부 서비스 지자체의 대민 공공서비스, 여론조사 등	2006년 시범 및 상용
	T-Commerce	BcN HFC망과 디지털 케이블TV를 이용한 양방향 전자상거래 서비스 방송프로그램 연동형 서비스 및 독립형 서비스 데이터 방송 연동(증권, 일기예보, 뉴스 등)	2005년 상용
	T-Learning	BcN HFC망과 디지털 케이블TV를 이용한 양방향 교육 서비스 교육방송 및 지자체 수능방송과의 연계 서비스	2006년 시범 및 상용
	T-Banking	BcN HFC망과 디지털 케이블TV를 이용한 양방향 금융 서비스 예금 조회, 이체 등	2006년 시범 및 상용

분야	세부 모델	내 용	서비스 시점
	T-Book	U-Class 서비스 및 T-신문 서비스	2006년 시범, 및 상용
부가 서비스	케이블 홈네트 워크 서비스	BcN HFC망과 디지털 케이블TV를 이용한 디지털홈 서비스 USN 기반 홈어플라이언스, 방범/방재, 원격검침	2006년 시범, 2007년 상용

※ 출처 : 한국전산원, 2005년도 BcN 시범사업 수행 결과, 2005.

(3) 케이블 시범망 구축현황

BcN 서비스 제공을 위한 케이블 컨소시엄의 망 구성도는 기본적으로 각 DMC들을 연결하기 위한 Ring 형태의 전달망과 각 SO에서 가입자까지 연결하는 HFC 망으로 구성되어 있으며 Open API를 사용하여 ISP, 전화, 데이터 및 케이블 서비스를 연결하는 구조를 갖는다.

제2절 BcN 정보보호 영역

BcN 정보보호 영역은 BcN 구조의 4개 계층 전체에 해당할 수 있으나, BcN은 다양한 서비스를 제공하기 위해 다양한 이기종 망들이 통합된 광대역 인프라이므로, 시범사업의 시범망 및 인프라 구축현황을 바탕으로 이기종 망간 연동측면과 서비스 제공을 위한 기반 장비 측면에서 정보보호 영역을 설정한다.

1. BcN 연동개념 및 아키텍처

(1) BcN 연동개념

다양한 융·복합형 서비스가 제공되는 BcN망은 다수의 가입자망과 사업자간의 연결로 구성되고 있다. 다양한 가입자망의 연결로 구성된 네트워크 환경에서 전송 경로 확보, 네트워크 자원 확보 등에 관한 정보 교환이 필요하다. 다양한 가입자망에서 제어정보의 교환과 데이터 전송경로 확보, 네트워크 자원 확보를 통한 융·복합형 서비스를 제공하는 것을 BcN 망에서의 연동이라 볼 수 있다.

본 가이드에서는 BcN 망 연동을 아래와 같이 정의한다.

■ BcN 망에서의 연동

1. 다양한 가입자망 사이의 연동

: ①PSTN, ②인터넷, ③WiBro, ④WCDMA, ⑤유선 방송망 사이의 연동

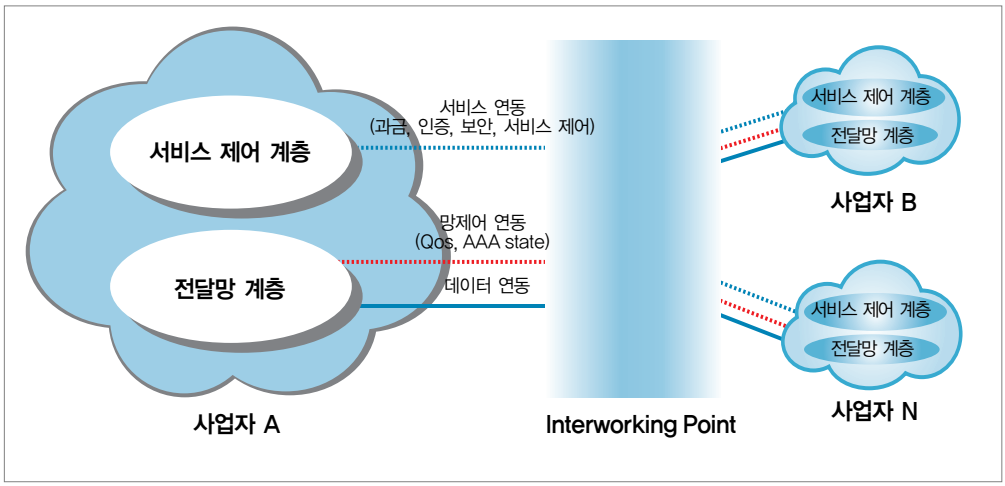
2. BcN 망 사업자 사이의 연동

: 동일 또는 이종의 가입자망 환경에서의 연동

BcN 망에서의 연동은, 다양한 서비스를 제공하기 위해, 연결설정 경로를 확보하기 위한 시그널링 메시지를 통한 서비스제어 계층의 과금, 인증, 보안 및 망 제어 정보 등의 교환이

필요하고, 연결이 허용된 서비스의 미디어 데이터 전송을 위한 전달망에서의 연동 단계가 필요하다.

(그림 3-1) BcN 연동 개념도



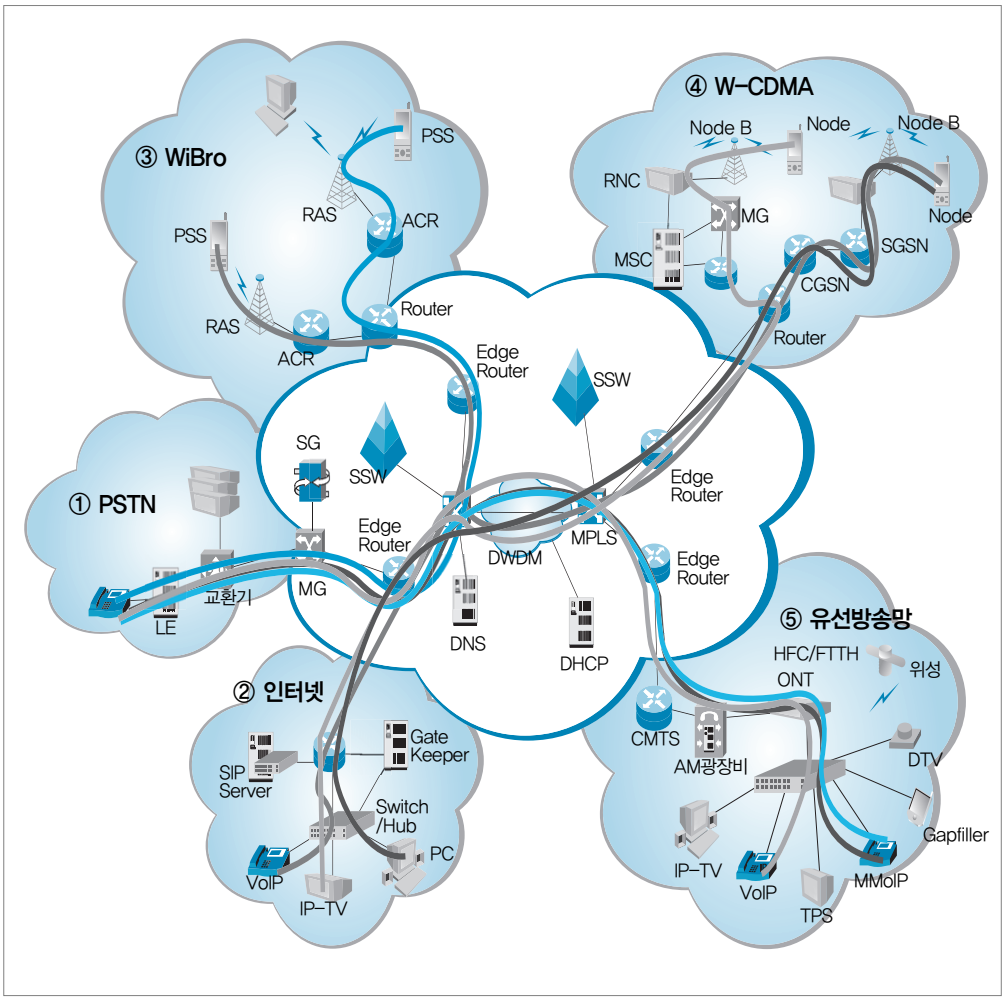
※ 출처 : BcN 표준모델 II(안)

- 서비스 · 제어계층의 연동 : 각 가입자망의 시그널 메시지로 변환 필요
- 전달망 계층의 연동 : 각 가입자망의 패킷구조로 변경 필요

(2) BcN 아키텍처

앞에서 언급한 바와 같이 BcN 망에서의 연동은 BcN 전달망과 다양한 가입자망 사이의 연동으로 표현할 수 있다. BcN 전달망과 가입자망의 연동 아키텍처 및 구조는 제2장에서 기술한 BcN 표준모델 구조와, 제3장에서 언급한 BcN 컨소시엄에서 추진하고 있는 네트워크 구조를 개념적으로 다음 그림과 같이 표현된다.

(그림 3-2) BcN 아키텍처 및 연동 개념도



2. BcN 연동구간 도출 및 분석

(1) 연동구간 도출

여기에서는 앞의 BcN 아키텍처를 기반으로 다양한 가입자망의 연동 Case를 설명한다. 앞에서도 언급한 바와 같이 BcN 망은 BcN 전달망을 중심으로 주요 가입자망인 ①PSTN, ②인터넷(유선), ③WiBro, ④WCDMA, ⑤유선방송망(HFC)의 연결로 이루어진다.

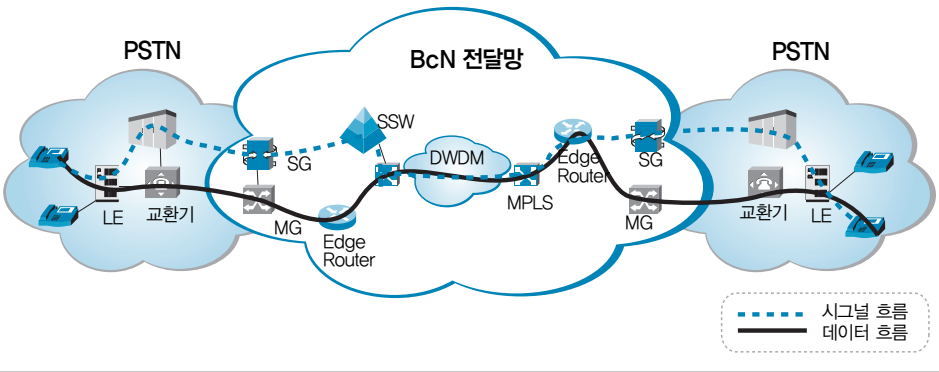
이 5가지 가입자 망과 전달망사이의 연동 Case를 도출하여 정리하면 아래 표와 같다.

[표 3-6] BcN 가입자망 연동 Case

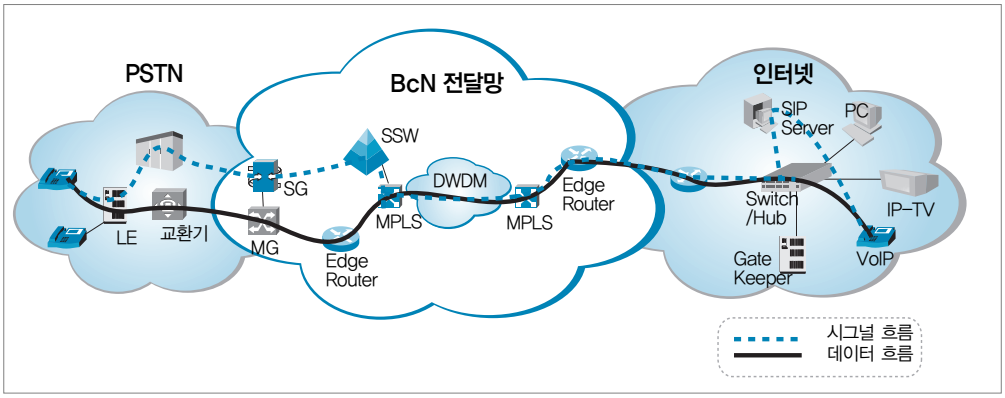
분류			적용범위		
구분	①PSTN	②인터넷	③WiBro	④WCDMA	⑤유선방송망
①PSTN	Case ①	Case ②	Case ③	Case ④	Case ⑤
②인터넷		Case ⑥	Case ⑦	Case ⑧	Case ⑨
③WiBro			Case ⑩	Case ⑪	Case ⑫
④WCDMA				Case ⑬	Case ⑭
⑤유선방송망					Case ⑮

위의 표의 이해를 돕기 위해, Case ①과 Case ②에 대해 보충 설명을 하면, Case ①의 경우는 아래 (그림 3-3)과 같이 BcN 전달망을 중심으로 PSTN 가입자망과 PSTN 가입자망의 연동으로 볼 수 있고, Case ②의 경우는 (그림 3-4)와 같이 BcN 전달망을 중심으로 PSTN과 인터넷망의 연동으로 볼 수 있다. 위의 표에서는 표기한 가입자망 사이에는 전달망이 위치하고 있다.

(그림 3-3) PSTN↔PSTN 연동 개념도



(그림 3-4) PSTN↔ 인터넷망 연동 개념도



(2) BcN 연동구간 도출결과 분석

앞에서 도출된 BcN 가입자망에서의 연동 가능 Case를 분석하면 아래와 같이 요약할 수 있다.

1. 음성 · 데이터 통합

- Circuit망에서 전송되는 음성신호를, packet망인 IP 데이터로 전송하기 위한 연동임
- Circuit망인 PTSN과 packet망인 인터넷, WiBro, WCDMA망 사이의 제어(시그널) 및 데이터 연동으로 볼 수 있음

2. 유선 · 무선 통합

- 유선 통신 기술을 기반으로 하는 유선망과 무선 통신 기술의 발전으로 새로이 생긴 무선망 사이의 연동임
- 유선 가입자망인 인터넷과 무선 가입자망인 WiBro, WCDMA망 사이의 제어(시그널) 및 데이터 연동으로 볼 수 있음

3. 통신 · 방송 통합

- 아나로그 신호를 전송하는 유선방송망(HFC)의 고도화에 따라, 방송망을 통한 IP 데이터를

송 · 수신하기 위한 연동임

- 양방향 통신기술과 CMTS 등 패킷망과의 연동 장비를 이용하여 VoIP, DTV 및 T-Banking 등의 서비스를 제공하고 있음

제3절 BcN 정보보호 대상

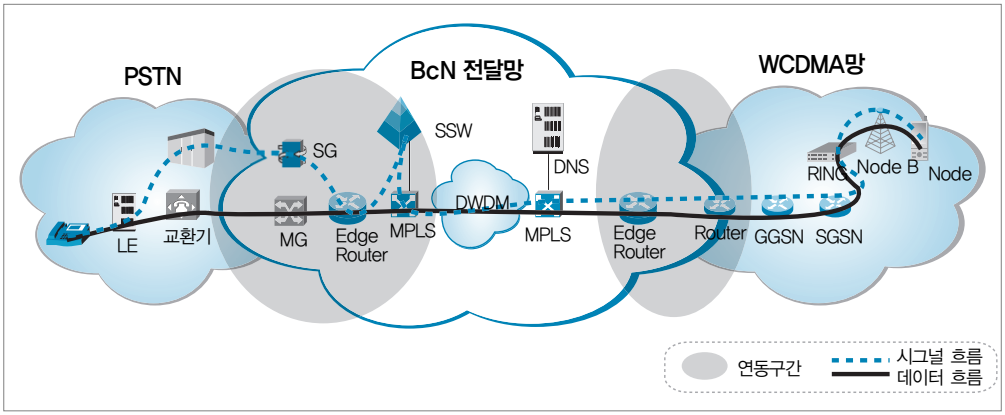
1. 가입자망 연동구조 분석

앞에서 BcN 가입자망 연동 Case를 분석한 결과, BcN 연동은 음성 · 데이터 통합, 유선 · 무선 통합, 통신 · 방송 통합의 3가지 연동 Case로 구분하여 볼 수 있다. 3가지 연동 Case 중 대표적인 연동 Case를 선정하여 각각의 연동 구조를 분석하고, 본 가이드에서 보호해야할 보호대상을 도출한다.

(1) 음성 · 데이터 연동 : PSTN ↔ WCDMA

음성 · 데이터 통합 서비스의 대표적인 구조인, 음성 가입자망인 PSTN망과 데이터망인 WCDMA망 사이의 연동으로 구조를 통해 살펴보기로 한다. 아래 그림은 PSTN망과 WCDMA망 사이의 연동의 개념을 나타내는 구조도로, 서비스 제어 정보인 시그널 메시지의 흐름과 사용자 데이터의 흐름을 나타내고 있다.

(그림 3-5) PSTN ↔ WCDMA 연동 구조도



위의 그림을 바탕으로 PSTN망의 서비스 이용자가 WCDMA망의 서비스 이용자와 통화할 경우, 통화 경로의 흐름을 살펴보면 다음과 같다.

■ Signal 정보흐름

구간	PSTN 망	연동구간	BcN 전달망	연동구간	WCDMA 망
Node	전화기 ↔ SG	↔ 소프트스위치 ↔	라우터 ↔ MPLS ↔라우터	↔ 라우터 ↔	GGSN↔SGSN ↔RNC↔ RAS↔PSS
주요 Protocol	DP, DTMF, SS7	SIGTRAN, MGCP, Megaco, H.323, SIP	SIP	SIP	SIP

■ Media 정보흐름

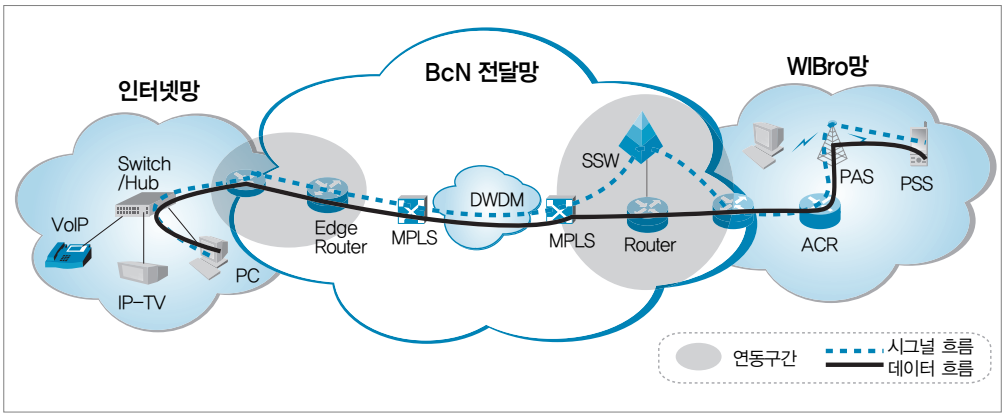
구간	PSTN 망	연동구간	BcN 전달망	연동구간	WCDMA 망
Node	전화기 ↔ Switch	↔ MG ↔	라우터↔ MPLS↔ 라우터	↔ 라우터 ↔	GGSN↔SGSN ↔RNC↔ RAS↔ PSS
주요 Protocol	–	UDP(RTP)	UDP(RTP)	UDP(RTP)	UDP(RTP)

BcN 전달망, PSTN망, WCDMA 망 내부는 각 사업자에 의해 관리되는 영역으로서 단일 목적의 서비스만을 제공하므로 연동구간에서 제외한다. 따라서, 연동구간은 End-to-End 서비스 제공을 위해 가입자 망과 BcN 전달망의 정합부분으로, 망간 호처리를 위해 상호 작용하는 시그널링 처리장비(예: 소프트스위치), DNS 서버 등을 포함한다.

(2) 유선 · 무선 연동 : 인터넷 ↔ WiBro

유선 · 무선 통합 서비스의 대표적인 형태로는 인터넷(유선) 가입자망과 WiBro망 사이의 연동 Case를 생각해 볼 수 있다. 두 가입자망의 연동 구조는 아래 그림과 같이 나타낼 수 있다.

(그림 3-6) 인터넷 ↔ WiBro 연동 구조도



인터넷망과 WiBro망 사이의 연동 구조도를 참조하여 인터넷망과 WiBro망 사이의 세션 연결 경로와 미디어 데이터 흐름을 분석해 보면 다음과 같이 나타낼 수 있다.

■ Signal 정보흐름

구간	인터넷	연동구간	BcN 전달망	연동구간	WiBro
Node	단말기 ↔ Router	↔ 소프트스위치 ↔	MPLS ↔DWDM ↔MPLS	↔ 소프트스위치 ↔	ACR↔ ↔RAS↔ PSS
주요 Protocol	SIP	SIP	SIP	SIP	SIP

■ Media 정보흐름

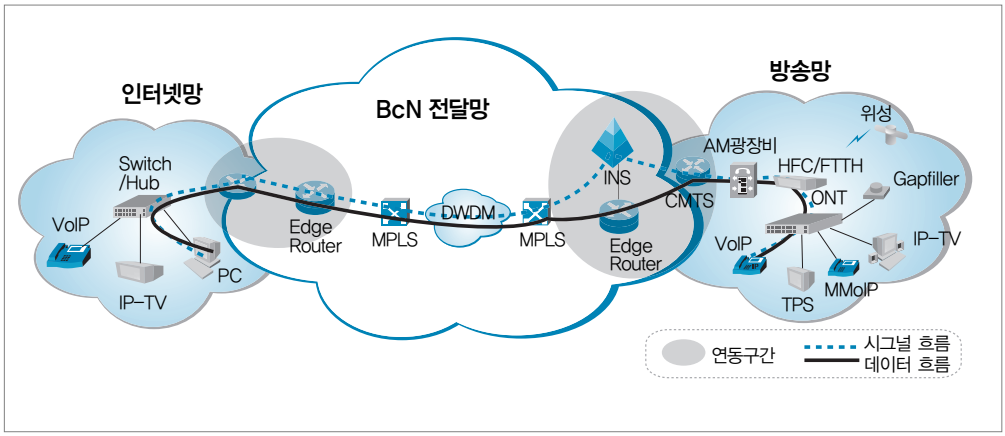
구간	인터넷	연동구간	BcN 전달망	연동구간	WiBro
Node	단말기 ↔ Router	↔ Router ↔	MPLS ↔DWDM ↔MPLS	↔ Router ↔	ACR↔ ↔RAS↔ PSS
주요 Protocol	UDP(RTP)	UDP(RTP)	UDP(RTP)	UDP(RTP)	UDP(RTP)

BcN 전달망, 인터넷망, WiBro망 내부는 각 사업자에 의해 관리되는 영역으로서 단일 목적의 서비스만을 제공하므로 연동구간에서 제외한다. 따라서, 연동구간은 End-to-End 서비스 제공을 위해 가입자 망과 BcN 전달망의 정합부분으로 볼 수 있다.

(3) 통신 · 방송 연동 : 인터넷 ↔ 유선 방송망(HFC)

BcN의 대표적인 통합 서비스로 통신 · 방송 통합 서비스에 대한 대표적인 연동 형태로는 인터넷(유선) 가입자망과 유선방송망(HFC) 사이의 연동 Case를 생각해 볼 수 있다. 인터넷망과 유선방송망의 연동구조도는 아래 그림과 같이 나타낼 수 있다.

(그림 3-7) 인터넷 ↔ 유선 방송망 연동 구조도



인터넷망과 HFC망 사이의 시그널링 흐름과, 미디어 데이터 흐름을 분석해 보면 다음 표와 같이 나타낼 수 있다.

■ Signal 정보흐름

구간	인터넷	연동구간	BcN 전달망	연동구간	유선방송망(HFC)
Node	단말기 ↔ Router	↔ 소프트스위치 ↔	MPLS ↔DWDM ↔MPLS	↔ 소프트스위치 ↔	CMTS↔ ↔STB↔ 단말기
주요 Protocol	SIP	SIP	SIP	SIP	SIP

■ Media 정보흐름

구간	인터넷	연동구간	BcN 전달망	연동구간	유선방송망(HFC)
Node	단말기 ↔ Router	↔ Router ↔	MPLS ↔DWDM ↔MPLS	↔ Router ↔	CMTS↔ ↔STB↔ 단말기
주요 Protocol	UDP(RTP)	UDP(RTP)	UDP(RTP)	UDP(RTP)	UDP(RTP)

BcN 전달망, 인터넷망, 유선 방송망 내부는 각 사업자에 의해 관리되는 영역으로서 단일 목적의 서비스만을 제공하므로 연동구간에서 제외한다. 따라서, 연동구간은 End-to-End 서비스 제공을 위해 가입자 망과 BcN 전달망의 정합부분으로 볼 수 있다.

2. 보호대상(장비) 식별

상기 연동구조 분석을 통해 이기종 망간 연동장비와 BcN 주요 서비스를 제공하기 위한 BcN 인프라 구성요소를 중심으로 보호대상을 선정하며, 선정기준은 다음과 같다.

① Gateway 등 전달망 및 가입자망 연동구간에서 연동기능을 담당하는 핵심장비
② 소프트스위치 등 전달망 및 가입자망 계층에서 서비스 및 제어를 담당하는 핵심장비
③ DNS 등 IP 망에서 기반 서비스를 제공하는 장비

※ 개별망 내부에 종속적이며 하위계층에서 단순전송을 담당하는 장비는 제외

선정기준에 의해 도출한 보호대상은 다음 표와 같다.

[표 3-7] 연동구간의 보호대상

보호대상		주요기능
소프트 스위치	CSC (Call Seesion Controller)	• 각 가입자망간의 호 연결, 세션제어 기능 수행 – 다양한 응용서버와 표준인터페이스로 연동하여 다양한 서비스 제공 – 인입호 관문, 가입자 인증 및 등록, 세션제어 및 서비스 라우팅, 등록 가입자 프로파일 관리, 번호 분석 및 변환, SIP/SDP 메시지 압축 및 해제기능 제공
	MGC (미디어 게이트웨이 Controller)	• 미디어 게이트웨이 제어 – 회선기반 PSTN망의 트래픽을 IP기반 SIP, H.323 등의 패킷트래픽으로 변환하도록 제어
CMTS(Cable modem Termination System)		• HFC망을 통한 초고속인터넷 서비스를 제공하기 위해 인터넷 IP 패킷 기반 신호를 RF 고주파 신호로 변환시켜 가입자에게 전송 • 가입자 단말에서 오는 RF 신호를 IP 패킷으로 변환 • 인터넷망의 스위치(라우터)와 H/E Combiner를 연결하는 Bridge 역할을 수행 • 양방향 방송을 위한 데이터를 Headend로 전달해 주는 리턴채널 기능 제공
SIP 서버	Register (Registra) Server	• REGISTER 메시지를 통해 사용자 등록 정보 저장 • 특정 사용자의 접속주소에 대한 정보 제공
	Proxy Server	• 연결 요청 메시지를 수신하면 연결설정 경로를 결정한 다음, 헤더 필드들의 일부를 수정한 후 직접 연결요청을 수행
	Redirect Server	• 다음 홉 서버의 주소를 포함하는 재방향 응답을 사용하여 클라이언트의 호설정 요청에 응답하여 세션연결을 처리
Gateway	SG(Signal Gateway)	• PSTN과 IP망사이의 미디어 전송의 연동을 담당하는 MG를 제어 • PSTN과 IP 망사이에서 회선기반의 신호(프로토콜)을 IP 기반의 SIP, H.323 패킷트래픽으로 또는 그 반대로 변환하여 전송
	MG(미디어 게이트웨이)	• PSTN과 IP 망사이에서 회선기반의 트래픽을 IP 기반 트래픽으로 변환하여 전송
MPLS Router		• BcN 전달망, 각 가입자망 경계에서 IP 데이터 전송
DHCP 서버		• 주요 단말 부팅시 IP 주소를 할당하는 기능
DNS 서버		• IP주소와 도메인 네임 번역 기능

제 4 장 BcN 연동구간 보안위협

제1절 BcN 연동구간 보안위협 개요

[표 4-1] BcN 연동구간 보안위협별 공격대상 분석표

위협		공격대상						
		소프트스위치	CMTS	SIP서버	Gateway	MPLS라우터	DHCP	DNS
서비스 거부공격	1. 시스템 자원고갈							
	(1) 대량 SIP INVITE 메시지 전송	●		●				
	(2) 대량의 DHCP Request 메시지 전송						●	
	(3) 대량의 IP 패킷 전송	●	●	●	●	●	●	●
	2. 비정상 메시지 전송							
	(1) 연결 해제 또는 종료 메시지 전송	●		●				
	(2) 비정상 등록 메시지 전송	●		●				
	(3) MPLS 라우팅 정보 변경					●		
	3. 네트워크 경로자원 고갈		●		●	●		
서비스품질 (QoS)저하	1. QoS가 조작된 패킷 인입		●	●	●	●		
	2. DiffServ 자원절도					●		
	3. 잡음 삽입				●	●		
시스템 해킹	1. 시스템 설정 오류	●	●	●	●	●	●	●
	2. 원격접속 프로토콜 취약점	●	●	●	●	●	●	●
	3. 운영체제 및 어플리케이션 취약점	●	●	●	●	●	●	●

위협		공격대상						
		소프트스위치	CM TS	SIP 서버	Gate way	MPLS 라우터	DH CP	DNS
도청	1. 연동장비 해킹을 통한 도청	●	●	●	●	●		
	2. 전송패킷 분석을 통한 도청	●	●	●	●	●		
	3. 세션 가로채기를 통한 도청	●	●	●	●			
	4. Fake DHCP 서버 운영을 통한 도청						●	
메시지 위 · 변조	1. 사용자 등록 메시지 위 · 변조	●		●				
	2. 가입자 정보 위 · 변조	●		●				
	3. 세션 연결 메시지 위 · 변조	●	●	●	●			
	4. 라우팅 메시지 위변조					●		

제2절 서비스 거부공격

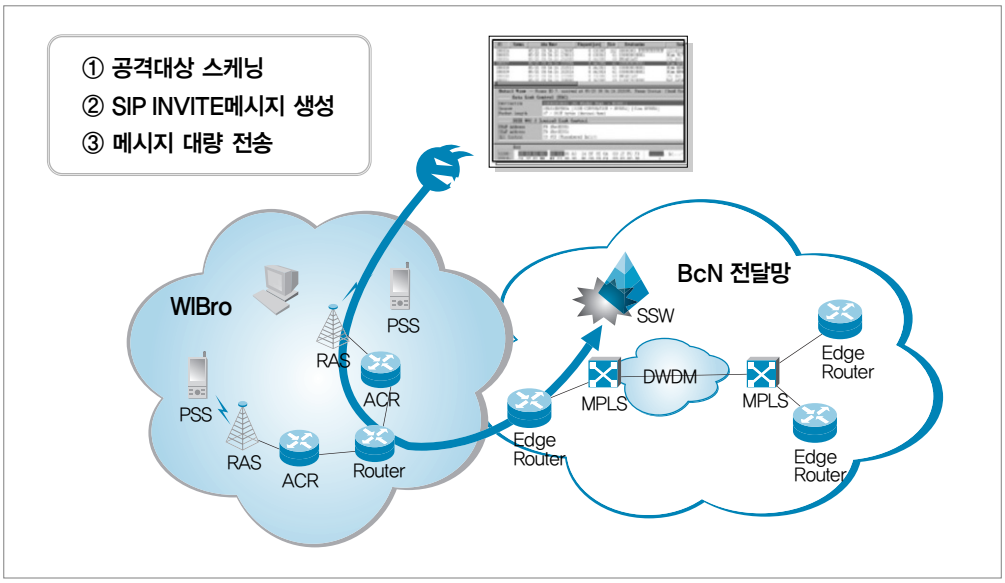
1. 시스템 자원고갈

BcN 연동구간의 주요 공격대상 시스템에 대량의 메시지와 IP 패킷의 전송으로 인해 시스템 자원이 고갈되어, 시스템의 정상적인 동작이 어려워질 수 있다. 시스템 자원 고갈의 원인이 되는 대량 메시지 전송과 대량의 IP 패킷 전송 등에 관한 위협의 상세 내용은 다음과 같다.

(1) 대량 SIP INVITE 메시지 전송

가. 위협 시나리오

(그림 4-1) 대량 SIP INVITE 메시지 전송 위협



① 공격자는 네트워크 스캐닝 도구를 사용하여 메시지 처리 장비(예: SSW, SIP 서버 등)의 IP 주소 등을 알아낸다.

② 공격자는 SIP 메시지 생성도구를 이용하여 SIP-INVITE 메시지를 생성한다.
③ 생성된 SIP INVITE 메시지를 BcN 메시지 처리장비인 소프트스위치, SIP 서버 등에 대량으로 전송하여 시스템 자원을 고갈시켜, 정상적인 연결설정을 방해한다.

나. 공격대상

- 소프트스위치, SIP 서버 등 BcN 메시지 처리장비

다. 예상피해

- 서비스를 제공하는 사업자에게는 연결메시지 처리장비의 자원고갈로 인해 서비스 장애, 서비스에 대한 품질 미보장 등이 발생할 수 있다.
- 사용자에게는 실시간 서비스에 대한 품질저하, 서비스 장애 등의 문제가 발생할 수 있다.

라. 고려사항

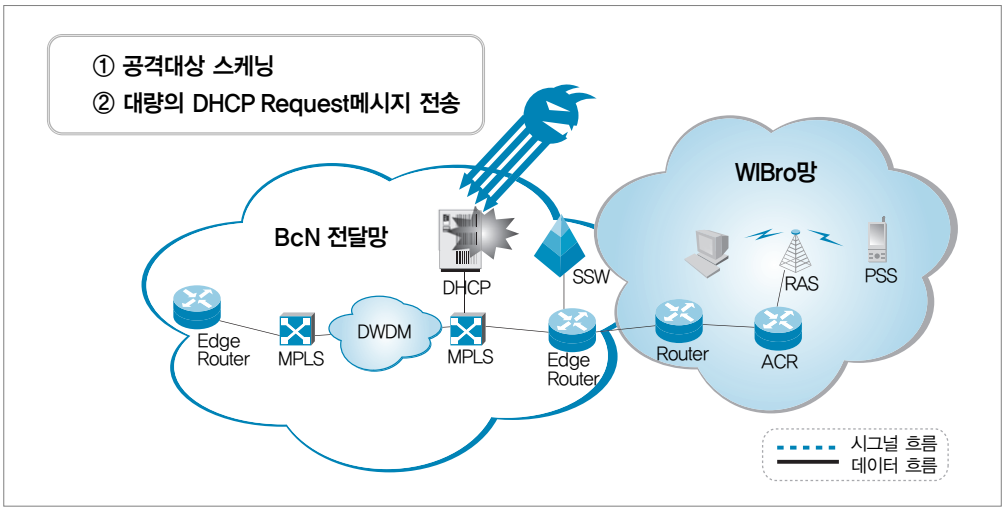
대량의 SIP INVITE 전송은 대규모 가입자에게 서비스를 제공하는 장비 운영 사업자에게는 피해가 크다. 또한 SIP 메시지 생성 도구 등을 이용하여 어렵지 않게 대량의 SIP 메시지를 발생할 수 있어 발생 가능성이 높은 편이다. 하지만, 연동구간에서 BcN 장비는 대부분 대용량 패킷을 처리할 수 있으며 이러한 이상징후는 모니터링하기가 쉬워 BcN 장비의 자원을 고갈시키는 일은 그리 쉬운 것은 아니다.

(2) 대량의 DHCP Request 메시지 전송

가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 사용하여 DHCP의 IP 주소 등 공격에 필요한 정보를 수집한다.
② DHCP 서버에 대량의 DHCP Request 메시지를 생성하여 전송한다.
③ DHCP 서버의 IP 주소자원을 모두 고갈시켜, 정상적인 단말기에 IP 주소를 부여하지 못하도록 한다.

(그림 4-2) 대량의 DHCP Request 메시지 전송 위협



나. 공격대상

• DHCP 서버, DHCP 서버에서 관리하는 IP 주소자원

다. 예상피해

• DHCP에서 부여하는 IP 주소자원의 고갈로 정상적인 단말기에 IP 주소를 부여할 수 없어, 서비스 장애를 초래할 수 있다.

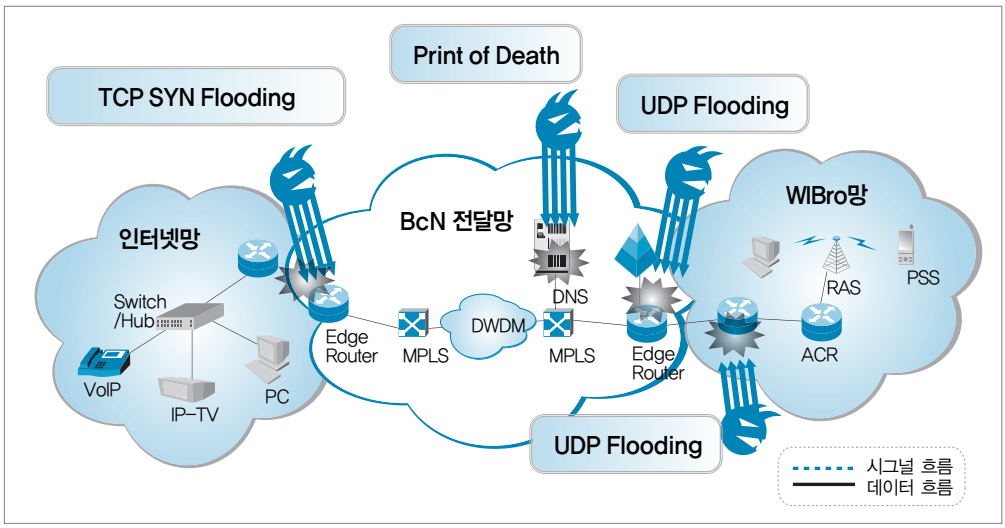
라. 고려사항

대량의 DHCP Request 메시지 전송 공격은 DHCP 서버에서 관리하는 IP 주소자원을 고갈시켜 정상적인 사용자 단말에 IP 주소 부여를 방해하는 공격으로 전통적인 인터넷 환경에서도 많이 발생하는 공격 방식이다. 즉, 많은 공격자에게 익숙한 공격방식으로 공격시도는 매우 많을 것으로 분석된다.

(3) 대량의 IP 패킷 전송

가. 위협 시나리오

(그림 4-3) 대량의 IP 패킷 전송 위협



① 공격자는 네트워크 스캐닝 도구를 사용하여 공격대상 시스템의 IP 주소, 포트 정보 등 공격에 필요한 정보를 수집한다.

② 공격자는 플러딩 공격도구를 사용하여 TCP SYN Flooding, ICMP Flooding, Ping of Death, UDP Flooding 등의 공격을 수행한다.

③ 공격대상 시스템의 자원을 고갈시켜, 정상적인 서비스 제공을 방해한다.

나. 공격대상

• CMTS, SIP 서버, Gateway, MPLS 라우터 등 IP 패킷을 처리하는 시스템

다. 예상피해

• CMTS, SIP 서버, Gateway, MPLS 라우터 등 IP 패킷을 전송하는 주요 시스템 자원의 고갈로 정상적인 서비스 제공이 어려워져, 서비스 장애, 품질 미 보장 문제 등이 발생할 수 있다.

• BcN 연동장비의 정상적인 서비스 제공이 어려워지면, BcN 망을 이용한 다양한 서비스와 많은 사용자에게 실시간 서비스에 대한 품질저하, 서비스 장애 등의 피해가 발생할 수 있다.

라. 고려사항

대량의 IP 패킷전송 위협은 TCP SYN Flooding, ICMP Flooding, Ping of Death, UDP Flooding 등의 공격 방식을 통해 이루어진다. 이러한 공격방식은 기존 인터넷망에서 행해지는 시스템 자원고갈 공격과 동일한 방식으로 공격자에겐 매우 익숙한 방식이며 공개된 공격도구 또한 매우 많고 대응이 어려워 공격 발생 가능성이 높다. 공격자는 친숙한 공격방식으로 인해 공격을 시도할 수 있지만, 연동구간에서 BcN 장비는 대부분 대용량 패킷을 처리할 수 있고 이상징후는 모니터링이 쉬워 BcN 장비의 자원을 고갈시키는 일은 그리 쉬운 것은 아니다.

2. 비정상 메시지 전송

비정상 메시지를 이용하여 공격자는 정상적인 연결을 해제, 종료시키고, 비인가 사용자를 등록하여 서비스를 이용, 비정상 라우팅 정보 삽입을 통한 네트워크 경로설정 오류 등을 발생시키는 공격을 말한다.

(1) 연결 해제 또는 종료 메시지 전송

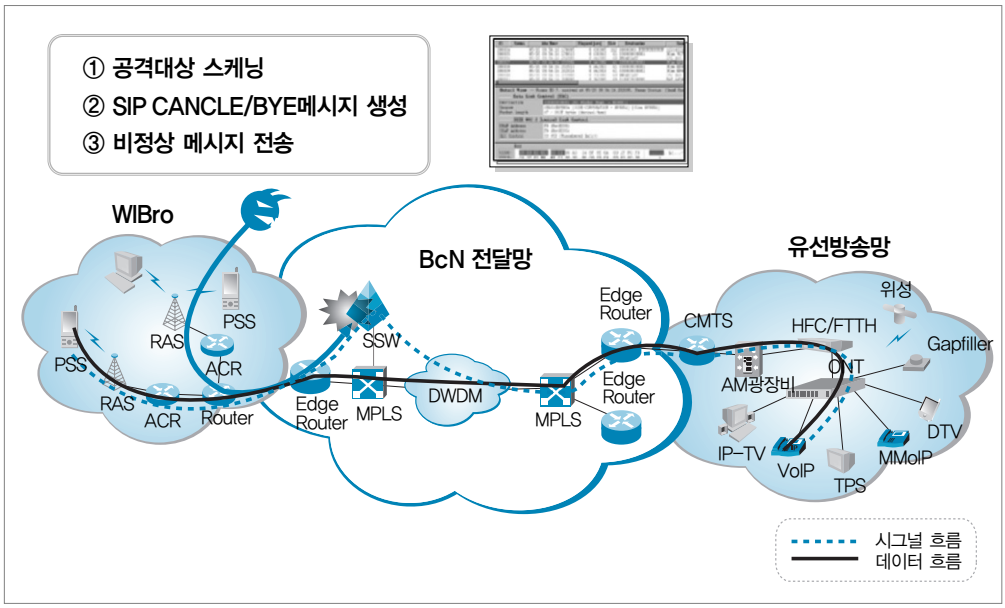
가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 사용하여, BcN망에서 메시지 처리 장비인 소프트스위치, SIP 서버 등의 공격대상 시스템의 IP 주소 등 공격에 필요한 정보를 수집한다.

② 공격자는 SIP 메시지 생성 도구를 이용하여 비정상 연결 해제, 종료 메시지인 SIP CANCEL, SIP BYE를 생성한다.

③ 공격자는 생성된 비정상 메시지를 소프트스위치, SIP 서버 등에 전송하여 사용중인 연결을 끊는다.

(그림 4-4) 연결 해제 및 종료 메시지 전송 위협



나. 공격대상

• 소프트스위치, SIP 서버 등 BcN 메시지 처리 시스템

다. 예상피해

• 비정상적인 연결 해제 및 종료 메시지 전송에 따라 서비스가 종료되거나, 지속적인 서비스 장애가 일어날 수 있다.

(2) 비정상 등록 메시지 전송

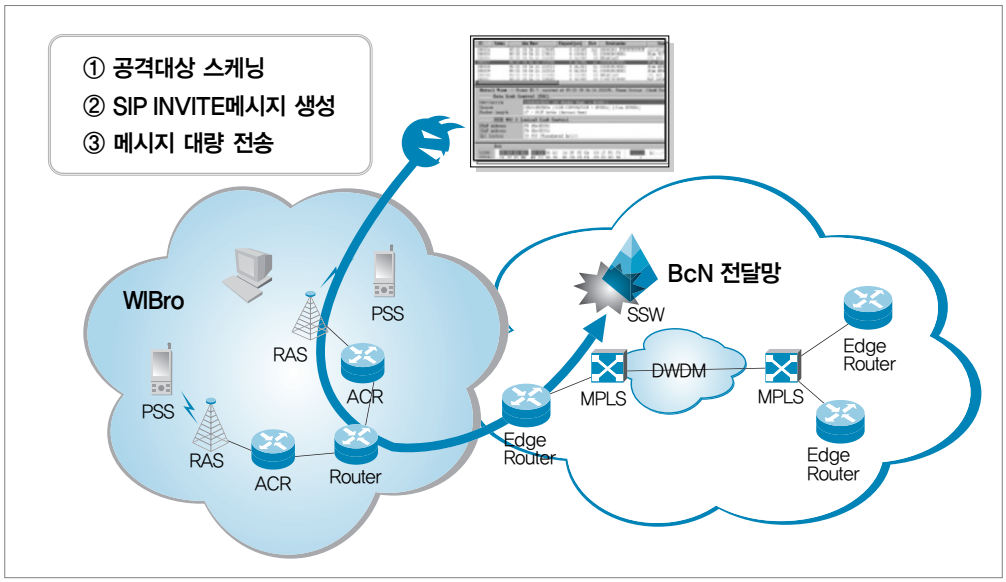
가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 사용하여, 사용자 등록 메시지를 처리하는 소프트스위치, SIP 서버 등의 공격대상 시스템의 IP 주소 등 공격에 필요한 정보를 수집한다.

② 공격자는 SIP 메시지 생성 도구를 이용하여 비정상 등록 메시지를 생성한다.

③ 공격자는 생성된 비정상 등록 메시지를 소프트스위치, SIP 서버 등에 전송하여 비인가자를 등록하여 서비스를 도용한다.

(그림 4-5) 비정상 등록 메시지 전송 위협



나. 공격대상

• 소프트스위치, SIP 서버 등 BcN 메시지 처리 시스템

다. 예상피해

• 비인가자의 등록으로 비인가자의 불법 서비스 사용으로 서비스 제공 비용, 컨텐츠 사용 비용 등 금전적 피해발생

(3) MPLS 라우팅 정보 변경

가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 사용하여, MPLS 라우터의 라우팅 정보를 교환하는 IP 주소 등 공격에 필요한 정보를 수집한다.

② 공격자는 MPLS 라우팅 메시지를 생성하여 공격대상 MPLS 라우터에 전송하여 MPLS 라우팅 테이블을 변경한다.

나. 공격대상

• MPLS 라우터의 라우팅 프로토콜 및 라우팅 테이블

다. 예상피해

• MPLS 라우팅 정보의 위조에 따라 네트워크 패킷 전송오류가 발생할 경우에는 특정 링크에 트래픽이 집중되어 네트워크 인터페이스가 마비 되거나, 특정 링크에 연결된 네트워크의 과부하로 네트워크 장애, 잘못 설정된 경로를 통해서 전송됨으로 종단간 서비스 장애 발생 등 그 피해 규모는 매우 클 수 있다.

라. 고려사항

백본망의 경계지점에 설치되어 있는 MPLS 라우터에 접근하고 라우팅 프로토콜을 위조하여 라우팅 경로를 변경하는 것은 일반적인 공격자로는 매우 힘든 일이다.

3. 네트워크 경로자원 고갈

네트워크 경로자원 고갈은 웜 · 바이러스 등에 의한 비정상 IP 트래픽 폭주와 DDoS 등의 해킹으로 인한 서비스 거부 공격으로 가용한 대역폭을 소진시키는 위협을 말한다.

가. 위협 시나리오

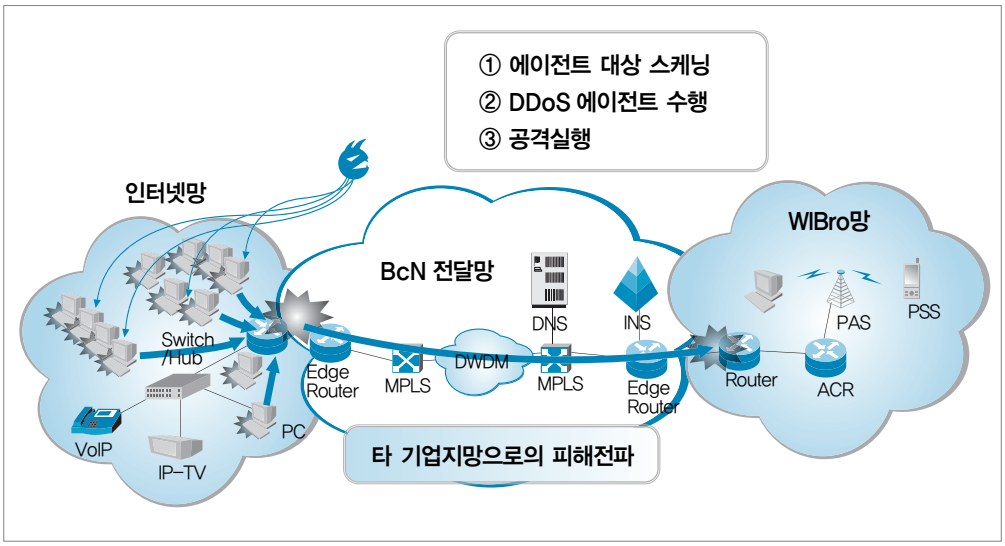
① 공격자는 DDoS 공격에 필요한 에이전트를 심기 위해 네트워크 스캐닝 작업을 수행한다.

② 취약한 시스템의 관리자 권한을 획득하여 DDoS 공격을 위한 에이전트를 수행한다.

③ DDoS 공격을 수행하기 위한 에이전트에 공격 명령을 전달하여 공격을 수행하여 특정 네트워크의 대역폭을 고갈시킨다.

※ DDoS 공격은 위의 해킹기법 이외에, 다수의 시스템에 웜 · 바이러스를 감염시킨 후, 감염된 다수의 시스템에서 특정 네트워크에 IP 트래픽을 폭주시켜 공격하는 방법도 있다.

(그림 4-6) 네트워크 경로자원 고갈 위협



나. 공격대상

• BcN 패킷 전송 경로 자원

다. 예상피해

• MPLS 라우터, Gateway 등 IP 패킷을 전송하는 주요 시스템 자원의 고갈로 정상적인 서비스 제공이 어려워져, 서비스 장애, 품질 미 보장 문제 등이 발생할 수 있다.
• 이 경우, 전송 경로 자원의 고갈로 새로운 경로를 찾아 패킷을 전송하는 경우 타 경로의 전송자원까지 고갈시켜 피해가 급속히 확산될 수 있다.
• BcN 연동장비의 정상적인 서비스 제공이 어려워지면, BcN 망을 이용한 다양한 서비스와 많은 사용자에게 실시간 서비스에 대한 품질저하, 서비스 장애 등의 피해가 발생할 수 있다.

라. 고려사항

현재 많은 사업자들이 이상 트래픽에 대한 관제 서비스를 제공하고 있어, 실제로 이상 트래픽 폭주로 인한 경로자원 고갈, 다른 전송경로로의 피해확산 등이 발생할 확률은 매우 낮다. 하지만, 앞에서도 언급했듯이 경로자원 고갈로 인한 피해는 연동망에서 연동 서비스를 마비시켜 그 피해가 매우 심각할 것이다.

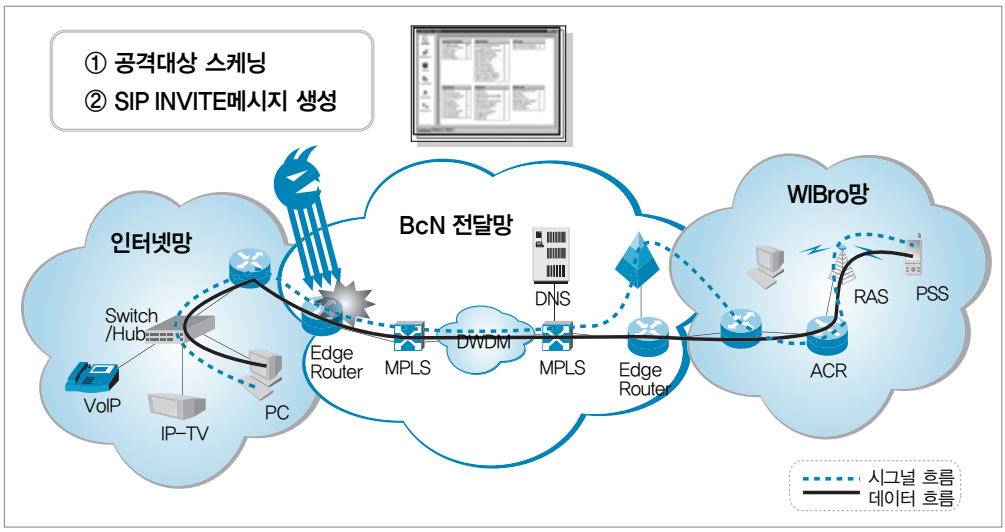
제3절 서비스품질(QoS) 저하

1. QoS가 조작된 패킷 인입

BcN은 QoS 보장을 위한 고도화된 망구조를 갖는다. 하지만, 공격자는 QoS 우선순위를 조작한 패킷을 네트워크에 대량으로 인입시켜, 서비스 품질을 저하시키는 공격을 시도 할 수 있다.

가. 위협시나리오

(그림 4-7) QoS가 조작된 패킷 인입 위협



① 공격자는 네트워크 스캐닝 도구를 이용하여 공격에 악용할 시스템을 선택한 후 IP 주소 등 필요한 정보를 수집한다.

② 공격자는 패킷 생성 도구를 이용하여 QoS가 조작된 패킷을 생성하고, 수집한 BcN 시스템의 주소 정보 등으로 근원지 주소 정보 등도 위장하여 패킷을 구성한다.

③ 공격자는 QoS와 근원지 주소 등이 조작된 패킷을 네트워크에 대량으로 주입하여 서비스 품질저하를 유발한다.

나. 공격대상

• MPLS 라우터 등 BcN 망에서 QoS 관련 패킷을 처리하는 시스템

다. 예상피해

• 공격자가 높은 순위를 갖는 QoS 패킷을 네트워크에 대량으로 주입하여, 낮은 순위를 갖는 서비스 패킷은 혼잡구간에서 삭제되어, 낮은 순위를 갖는 서비스의 품질이 현저하게 저하된다.
• 또한, 높은 순위를 갖는 패킷의 폭주가 발생하여 높은 우선 순위를 갖는 서비스 품질 또한 저하된다.

라. 고려사항

앞에서 설명한 것처럼 QoS 순위를 조작하는 공격은 QoS가 낮은 순위를 갖는 서비스의 품질을 현저하게 저하시키고, 높은 순위를 갖는 서비스 패킷의 전송에도 영향을 미치는 등 단순한 서비스 거부공격보다 더욱 다양하고, 많은 피해를 야기할 수 있다.

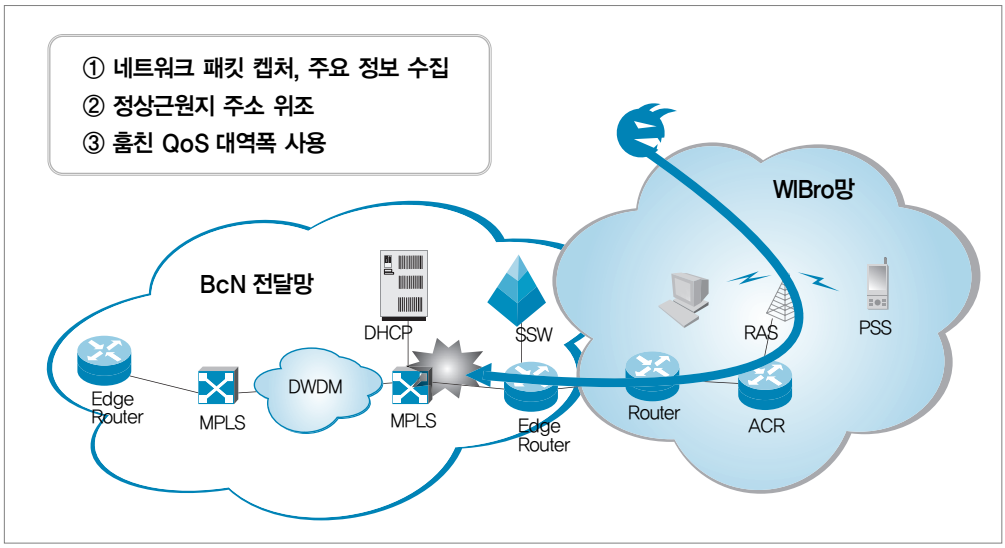
2. DiffServ 자원절도

BcN 망에서 QoS 보장을 위해 DiffServ(Differentiated Service)를 적용하는 경우가 많다. 공격자는 이러한 DiffServ 방식의 취약점을 이용하여 네트워크 자원을 훔쳐내어 사용함으로써 정상적인 서비스 품질을 저하시킬 수 있다.

가. 위협시나리오

① 공격자는 네트워크 스캐닝 도구를 이용하여, 높은 우선 순위의 QoS를 갖는 패킷을 분석하여 근원지 주소 등 공격에 필요한 정보를 수집한다.
② 공격자는 자신의 패킷을 수집한 근원지 주소로 위조하여 패킷을 전송하여, MPLS 라우터를 속인다.
③ MPLS 라우터에서는 높은 우선 순위를 갖는 패킷으로 여기고, 높은 서비스 품질로 패킷을 전송한다.

(그림 4-8) DiffServ 자원절도 위협



나. 공격대상

• DiffServ를 적용하고 있는 MPLS 라우터

다. 예상피해

• 높은 우선 순위의 QoS로 변경한 공격자의 패킷으로 고품질 서비스 사용자의 서비스 장애 및 사용자와 체결한 SLA에 위반에 따른 분쟁 등이 발생할 수 있다.

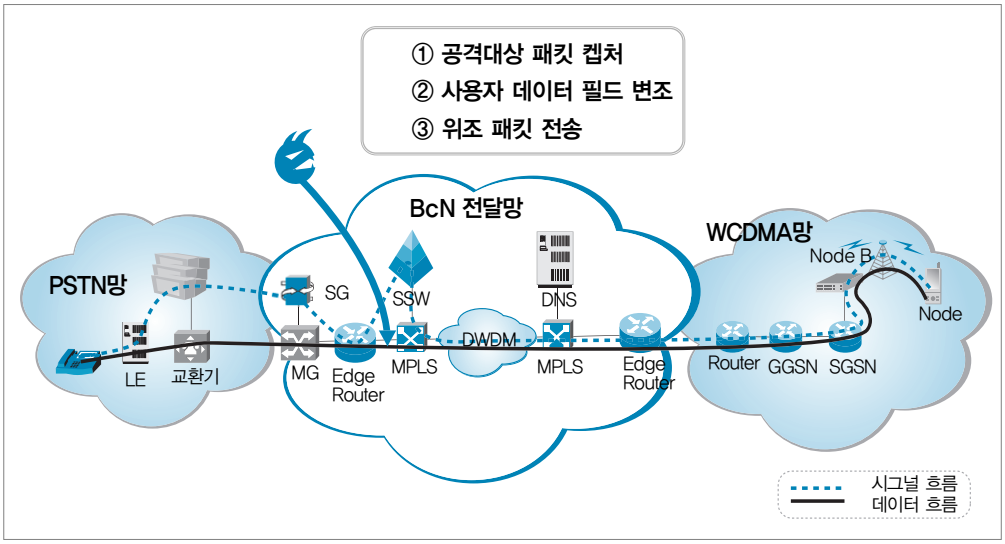
3. 잡음 삽입

BcN 연동구간에서 전송되는 대용량의 멀티미디어 데이터나 실시간 전송을 하여야하는 음성전화 패킷의 사용자 데이터 필드를 변조하여 불필요한 데이터를 삽입하는 공격을 말한다. 이 공격의 성공시 사용자는 멀티미디어 서비스와 전화 서비스에 잡음이 끼는 듯한 현상을 느낄 수 있다.

가. 위협 시나리오

① 공격자는 패킷분석 도구를 이용, IP 패킷을 수집 분석한 후, 멀티미디어 데이터 혹은 음성전화 데이터가 전송되는 패킷을 식별해 낸다.

(그림 4-9) 잡음 삽입 위협



② 공격자는 멀티미디어 데이터, 음성전화 데이터 등을 가로채, 데이터 필드를 손상하여 전송한다.

나. 공격대상

- BcN 연동구간에서 멀티미디어 데이터, 음성전화 데이터 등을 전송하는 Gateway, 라우터 등

다. 예상피해

- 실시간 고속 전송을 필요로하는 멀티미디어, 음성전화 데이터 등의 중간 정보를 손상시켜, 서비스 품질을 저하시킨다.
- 이러한 유형의 서비스 품질 저하 공격은 사용자와 체결한 SLA에 위배되면, 막대한 규모의 금전적인 피해도 동반할 수 있다.

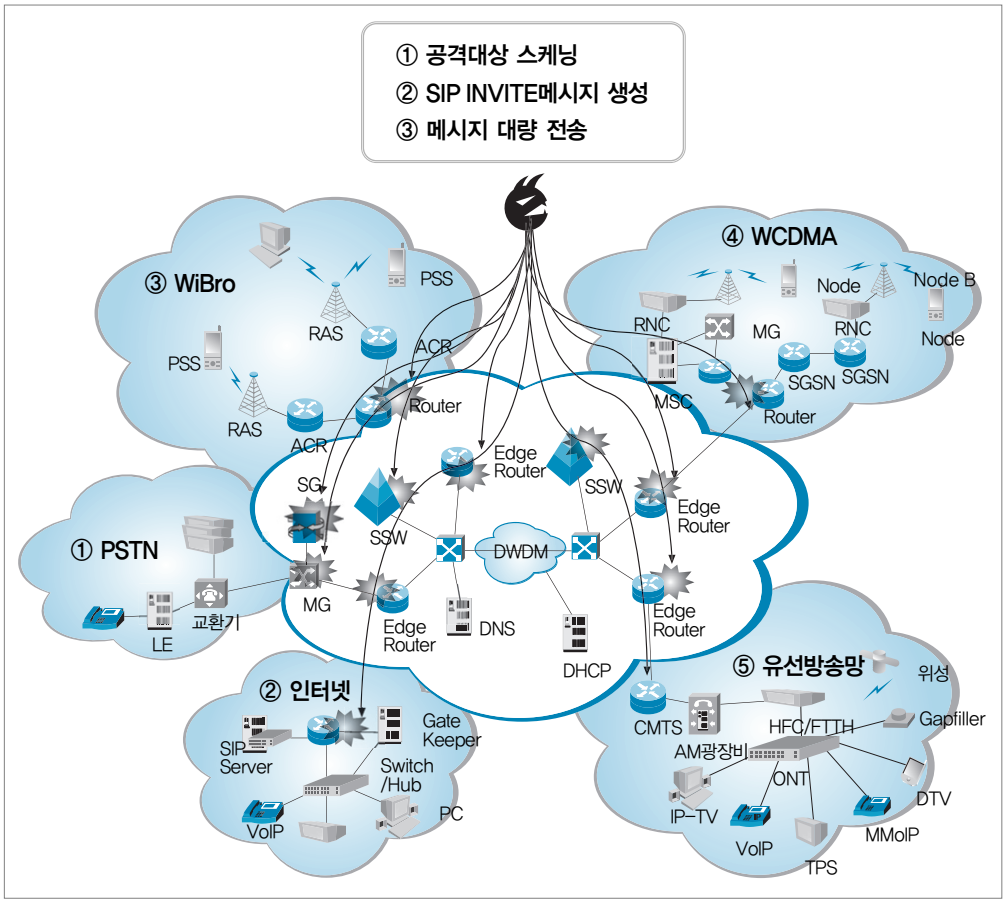
제4절 시스템 해킹

1. 시스템 설정 오류

시스템 해킹의 가장 기본적인 공격방식으로 BcN 주요장비의 모델명과 운영체제 등을 알아내어, 장비별 관리자 모드 접속 암호의 초기 값을 이용하여 접속을 시도하는 공격이다.

가. 위협 시나리오

(그림 4-10) 시스템 설정 오류 위협



① 공격자는 네트워크 스캐닝 도구를 이용하여 공격하고자 하는 시스템명, 제조업체, 모델명 등을 알아낸다.
② 공격자는 알아낸 시스템 모델별로 알려진 변경되지 않은 초기설정값(예: 관리자 모드 초기암호)을 악용하여 접속을 시도한다.

나. 공격대상

- BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

다. 예상피해

- 공격자가 BcN 주요 연동 시스템에 관리자 모드 접속을 통한 해킹을 성공하면, 시스템의 설정을 변경할 수 있게 된다. 즉, 공격자는 시스템 설정변경을 통해, 서비스 거부, 서비스 품질저하, 도청, 주요 정보 위변조 등 다양한 형태의 피해를 야기시킬 수 있다.
- BcN 주요 연동 장비 해킹에 의한 피해 규모와 형태 또한 다양할 것이다.

라. 고려사항

시스템 설정 오류로 인한 공격은, 주요 연동 장비가 네트워크 상에 노출되었을 경우에는 알려진 공격기법들이 많아 생각보다 쉽게 공격이 시도될 수 있으나, 주요장비를 사설망 및 가상 네트워크 등을 이용하여 Hiding하였을 경우에는 공격자가 주요시스템에 접근하기 위한 네트워크 경로 설정 매우 어려워 공격을 현실화하기가 어렵다.

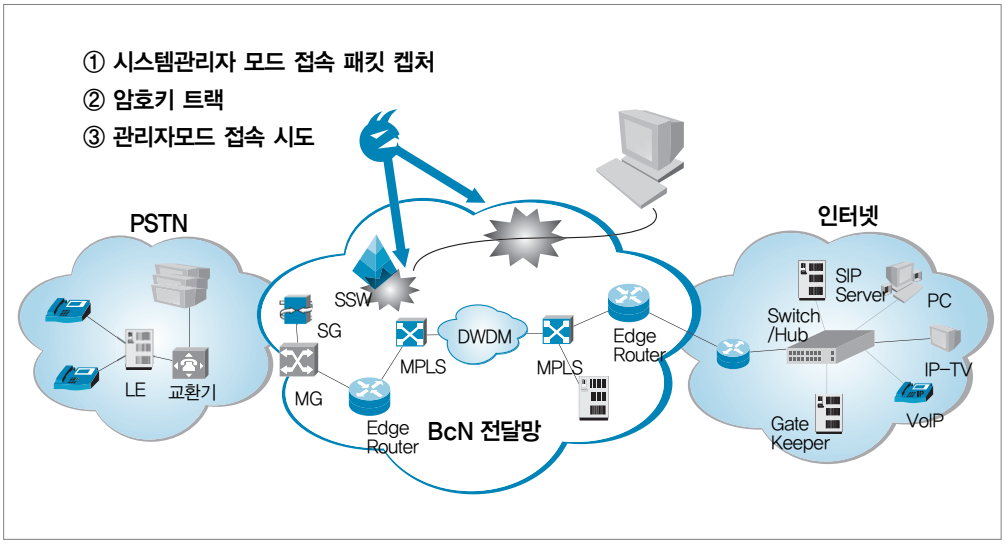
2. 원격접속 프로토콜 취약점

원격접속 프로토콜의 취약점을 이용하는 시스템 해킹방식은 공격자가 원격지에서 접속하는 SNMP, HTTP 등의 관리 프로토콜 취약점을 악용하여 관리자 권한을 획득하는 공격이다.

가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 이용하여, SNMP, HTTP 등의 관리 프로토콜에서 주요시스템 관리자 모드 접속 패킷을 수집한다.

(그림 4-11) 원격접속 프로토콜 문제점 악용 위협



② 수집한 패킷을 분석하여, 관리자 모드 접속 암호를 크랙한다.

③ 공격자는 크랙한 관리자 모드 접속 암호를 이용하여 접속한다.

나. 공격대상

• BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

다. 예상피해

• 앞의 '시스템 설정 오류' 로 인한 피해와 동일하다.

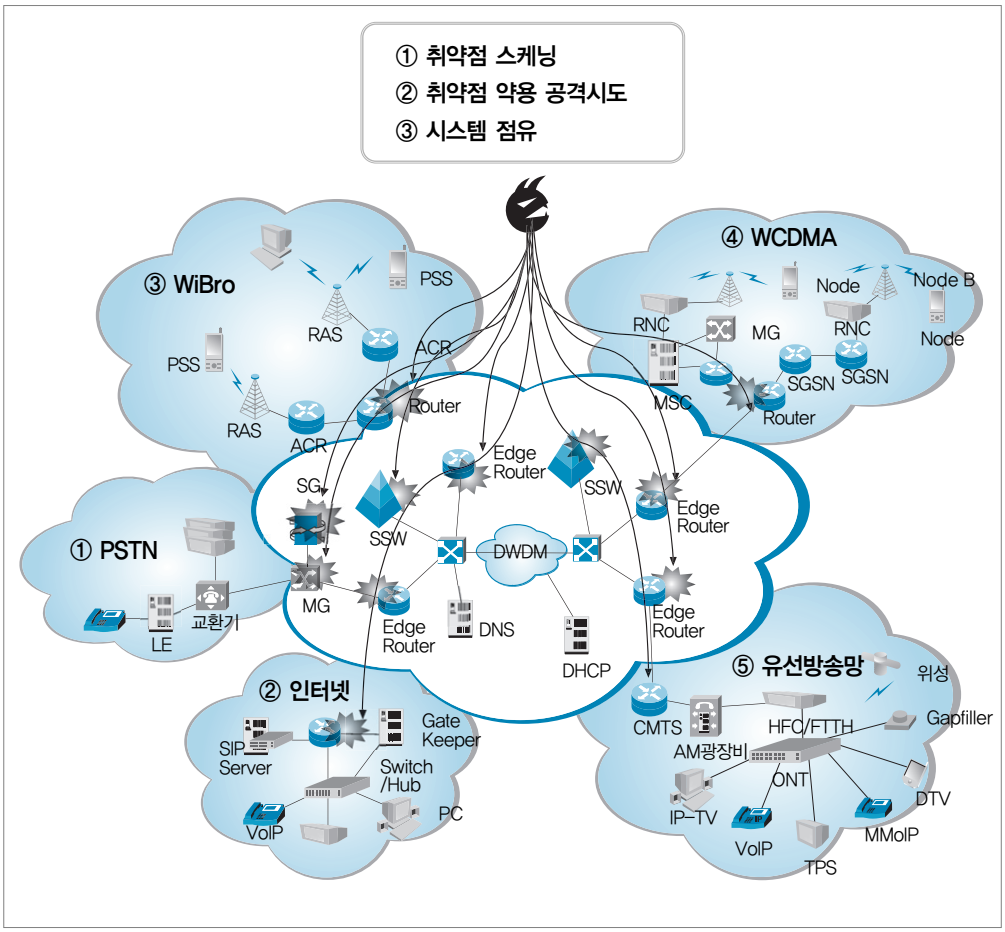
3. 운영체제 및 어플리케이션 취약점

BcN 주요 장비의 시스템에 탑재된 각종 운영체제 및 응용 서비스 프로그램의 구현, 설정, 프로토콜 등과 관련된 취약점을 이용하여 해킹을 시도하는 경우이다.

가. 위협 시나리오

① 공격자는 네트워크 스캐닝 도구를 이용하여, 주요시스템 운영체제, 어플리케이션 정보

(그림 4-12) 운영체제 및 어플리케이션 취약점 악용 위협



등을 알아낸다. 이때, 네트워크 취약점 점검 도구를 사용하여 공격대상 시스템의 취약점을 알아내기도 한다.

② 알아낸 운영체제와 어플리케이션에 존재하는 취약점을 악용하여 시스템 접속을 시도한다.

나. 공격대상

- BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

다. 예상피해

• 앞의 '시스템 설정 오류'로 인한 피해와 동일하다.

라. 참고사항

즉, BcN 주요 장비도 일반적인 시스템 보안 취약점 분석도구 이용하면 시스템이 갖고 있는 취약점을 쉽게 발견할 수 있고, 이러한 시스템 해킹은 특별한 해킹 수행 코드 없이도 간단한 해킹도구를 이용하여 공격이 성공할 가능성이 높은 편이며, 잘 알려진 공격 기법은 다음과 같다.

■운영체제 취약점을 이용한 공격기법

① 버퍼 오버플로우(buffer overflow) 공격

② 포맷 스트링(format string) 취약점 공격

③ 스크립트(script)의 취약점 공격

④ 경쟁 조건을 이용하는 공격

※ 이러한 취약점들은 프로그램 자체에 있기 때문에, 일반적으로 시스템에 설치된 보안 시스템들이 쉽게 대처를 하지 못하는 경우가 많다.

⑤ TCP/IP 등 각종 인터넷 프로토콜(ICMP, ARP, RARP, UDP 등)의 설계상 취약점을 이용한 공격

※ 예: ICMP Connection Reset 공격으로, Reset packet을 전송하게 되면 실제 연결이 끊길 수 있다.

⑥ IP spoofing

※ 전송되는 패킷의 헤더 부분의 IP 주소를 변경해서 보내는 것으로, 제3자를 사칭하여 다른 시스템에 접속하여 공격

⑦ ARP를 이용한 MAC address 조작하는 공격

⑧ 패스워드 크랙킹 등

■응용프로그램 취약점을 이용한 공격기법

① IIS(Internet Information Services) 웹서버 취약점 공격

② SQL Injection 등의 SQL 서버 공격

※ SQL Injection 공격: 조작된 SQL 쿼리문을 보내 Database의 등록정보 추출, 변경, 삭제 등을 수행하는 공격

③ 웹브라우져(Internet Explorer)의 ActiveX Control 취약점 공격

④ sendmail buffer overflow 공격

※ 조작된 e-mail 메시지를 보내 공격 대상 관리자 권한 등을 획득하는 공격

⑤ RPC(Remote Procedure Call) 서비스 buffer overflow 공격 등

※ RPC 프로그램의 불충분한 오류검사 또는 입력 미확인에 의한 buffer overflow를 통해 관리자 권한을 획득하는 공격

이외에도, BcN 주요 운영체제인 유닉스와 윈도우즈관련 시스템 해킹에 악용되는 취약점과 대응방안은 "[부록2] BcN 시스템 운영체제별 해킹 위협 및 대응방안"을 참고하도록 한다.

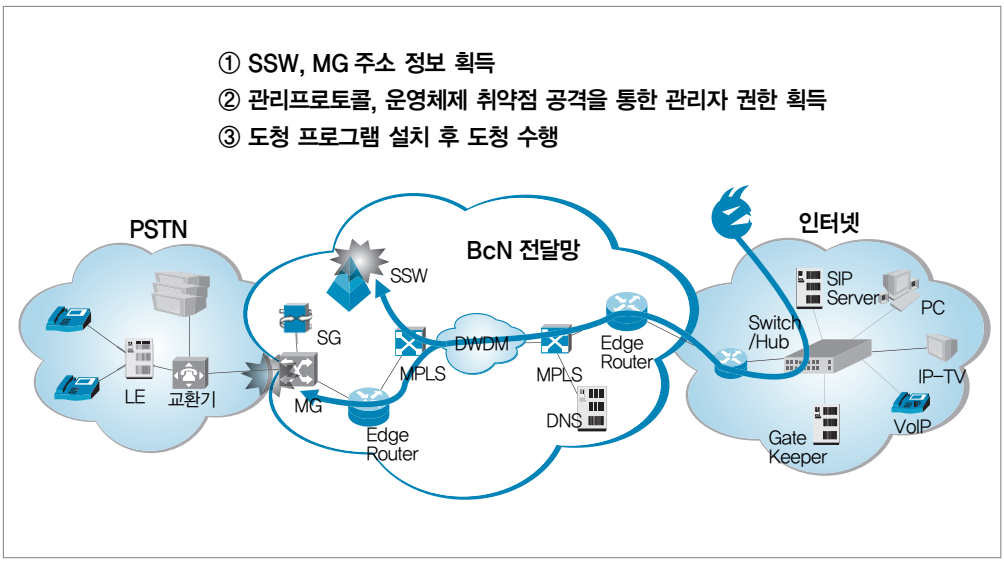
제5절 도청

1. 연동장비 해킹을 통한 도청

연동장비 해킹을 통한 도청 위협은 공격자가 불법적인 서비스 콘텐츠 및 사용자정보 획득, 2차 공격을 위한 자료수집 등을 목적으로 서비스 제공을 위한 연동장비에서 시그널, 미디어 등의 메시지를 도청하는 것을 말한다.

가. 위협 시나리오

(그림 4-13) 연동장비 해킹을 통한 도청 위협



① 공격자는 네트워크 및 시스템 스캐닝 도구를 사용하여 연동장비(예: Gateway, SSW, SIP 서버 등)에 대한 주소정보를 획득한다.

② 공격자는 연동장비의 운영체제 취약점, 관리 프로토콜(SNMP, HTTP 등) 취약점 등을 악용하여 시스템을 해킹하여 관리자 권한을 획득한다.

③ 공격자는 연동장비 내에서 시그널링 메시지, 음성통화, 금융거래 및 사용자 인증정보, 방

송컨텐츠 등의 데이터를 모니터링하거나, 연동장비에 모니터링 프로그램 등을 설치 후 원격에서 이들 데이터를 모니터링한다.

나. 공격대상

- 시그널 게이트웨이, 미디어 게이트웨이, 소프트스위치, SIP 서버, 라우터, CMTS 등의 연동장비

다. 예상피해

- 서비스를 제공하는 사업자에게는 가입자정보 누출, 사용자의 서비스 사용내역 누출 등에 따른 개인정보 침해에 대한 분쟁, 시스템 및 네트워크 구성정보 누출에 따른 대처비용 등이 발생할 수 있다.
- 사용자에게는 공격자에게 서비스 사용 내역, 개인정보 등의 콘텐츠 누출 등의 문제가 발생할 수 있다.

라. 고려사항

연동장비 해킹을 통한 도청 위협은 발생시 사업자 및 사용자 모두에게 피해가 크다. 연동장비 접근을 막는 대처수단이 없을 경우 운영체제 취약점, 관리에 사용되는 SNMP/HTTP 등의 프로토콜 취약점 등은 많이 알려진 공격기법들이 있어 해킹이 비교적 용이하다. 특히 서비스를 제공하는 연동장비는 사업자가 얻는 피해가 크고 얻는 정보량이 많다는 측면에서 공격 발생 가능성도 높다.

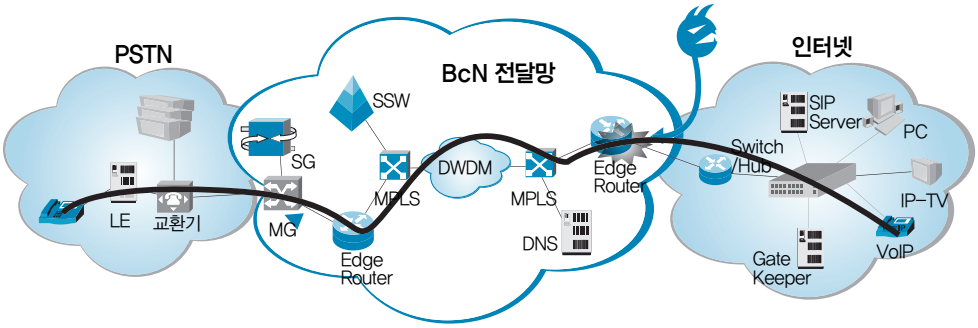
2. 전송패킷 분석을 통한 도청

전송패킷 분석을 통한 도청은 공격자가 LAN 네트워크 구간에서 불법적인 서비스 콘텐츠 및 사용자 정보 획득, 2차 공격을 위한 자료수집 등을 목적으로 시그널, 미디어 등의 메시지를 도청하는 것을 말한다.

가. 위협 시나리오

① 공격자는 스니핑 도구를 탑재한 컴퓨터를 LAN 등의 네트워크 공유 구간에 연결

(그림 4-14) 전송패킷 분석을 통한 데이터 도청 위협



② 공격자는 스니핑 도구를 이용해 전송패킷을 분석하여, 네트워크 공유 구간에서의 음성 통화내용, 방송 콘텐츠, 금융거래 정보 등을 도청한다.

나. 공격대상

- 가입자 망의 회선공유 구간에 있는 시그널 게이트웨이, 미디어 게이트웨이, 소프트스위치, SIP 서버 등의 서비스 제공 장비

다. 예상피해

- 서비스를 제공하는 사업자에게는 가입자정보 누출, 사용자의 서비스 사용내역 누출 등에 따른 개인정보 침해에 대한 분쟁 등이 발생할 수 있다.
- 사용자에게는 공격자에게 서비스 사용 내역, 개인정보 등의 콘텐츠 누출 등의 문제가 발생할 수 있다.

라. 고려사항

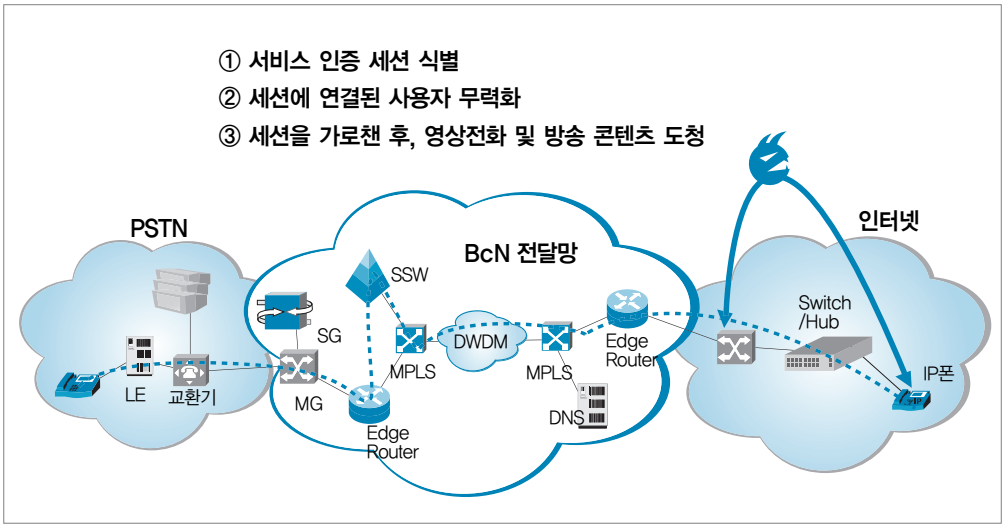
전송패킷 분석을 통한 도청 위협은 발생시 피해범위가 한정되어 사업자에게는 피해가 크지 않으나 개개의 사용자에게는 피해가 크다. LAN 등의 네트워크 공유구간에서 스니핑은 고도의 지식이나 특별한 장비를 요구하지 않는 비교적 손쉬운 해킹기법이므로 공격 발생 가능성도 높다.

3. 세션 가로채기를 통한 도청

세션 가로채기를 통한 도청 위협은 공격자가 불법적인 서비스 콘텐츠 및 사용자 정보 획득 등을 목적으로 서비스가 진행되는 세션에 개입하여 시그널, 미디어 등의 메시지를 도청하는 것을 말한다.

가. 위협 시나리오

(그림 4-15) 세션 가로채기를 통한 도청 위협



① 공격자는 스캐닝 도구를 사용하여 진행중인 음성통화, 방송 등의 서비스 세션을 찾는다.

② 공격자는 DoS 공격 등을 통해 세션에 연결된 사용자의 시스템을 무력화 시킨 후, 정상 사용자처럼 위장한다.

③ 공격자는 서비스 세션 연결에 필요한 정보를 스푸핑하여 서비스 세션을 가로챈다

④ 공격자는 서비스 제공장비(예: 소프트스위치, SIP 서버, 방송서버 등)에 접속하여 정상 사용자에게 제공되는 서비스 내용을 도청한다.

나. 공격대상

- 소프트스위치, SIP 서버, 방송서버 등의 서비스 제공 장비 및 사용자 시스템

다. 예상피해

- 서비스를 제공하는 사업자에게는 과금되지 않는 불법 서비스 사용에 따른 금전적 피해 등이 발생할 수 있다.
- 사용자에게는 부당한 서비스 이용 금액 지출, 개인정보 누출 등의 문제가 발생할 수 있다.

라. 고려사항

세션 가로채기를 통한 도청 위협은 발생시 피해범위가 한정되어 피해가 크지 않고 이를 성공하기 위해서는 응용 서비스 계층에 대한 고도의 지식과 공격기술을 필요로 하기 때문에 공격 발생 가능성은 낮으나, 공격 발생시 세션을 암호화 하지 않으면 마땅한 대응이 어려운 문제점이 있다.

4. Fake DHCP 서버 운영을 통한 도청

Fake DHCP 서버 운영을 통한 도청 위협은 공격자가 불법적인 서비스 콘텐츠 및 사용자 정보 획득 등을 목적으로 위조된 DHCP 서버를 운영하여 이 위조된 DHCP 서버가 클라이언트 시스템으로 하여금 공격자의 시스템에 접속하도록 유도하여 공격자의 시스템에서 시그널, 미디어 등의 메시지를 도청하는 것을 말한다.

가. 위협 시나리오

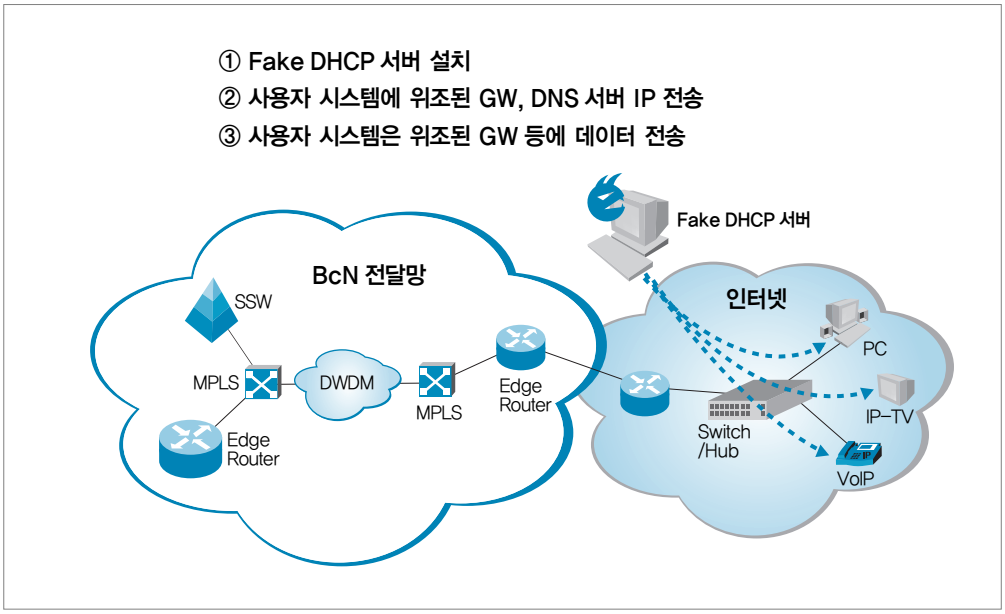
① 공격자는 네트워크에 위조된 Fake DHCP 서버를 연결한다.

② 위조된 Fake DHCP 서버는 서비스 사용 시스템(Gateway, 단말기 등)에 공격자의 시스템 IP를 Default Gateway, DNS 서버 값으로 설정하여 서비스 사용 시스템에 제공한다.

③ 서비스 사용 시스템은 공격자의 IP를 Dafault Gateway, DNS 서버로 설정한다.

※ 이후, 서비스 사용 시스템의 모든 데이터는 공격자의 시스템을 경유하게되어 공격자가 데이터를 모니터링할 수 있다.

(그림 4-16) Fake DHCP 서버 운영을 통한 도청 위협



나. 공격대상

• Gateway, 사용자 시스템 등의 DHCP 주소를 사용하도록 설정된 시스템

다. 예상피해

• 서비스를 제공하는 사업자에게는 사용자의 서비스 사용내역 누출 등에 따른 개인정보 침해에 대한 분쟁 등이 발생할 수 있다.
• 사용자에게는 공격자에게 서비스 사용 내역, 통화내역, 개인정보 등의 콘텐츠 누출 등의 문제가 발생할 수 있다.

라. 고려사항

Fake DHCP 서버 운영을 통한 도청 위협은 발생시 DHCP 프로토콜을 사용하는 다수의 시스템 사용자에 피해가 발생할 수 있으며, 위조 DHCP 서버 설치가 용이하고 사용자가 Fake DHCP 서버 조사가 어려우므로 네트워크 관리를 강화하지 않으면 공격 발생 가능성이 높다.

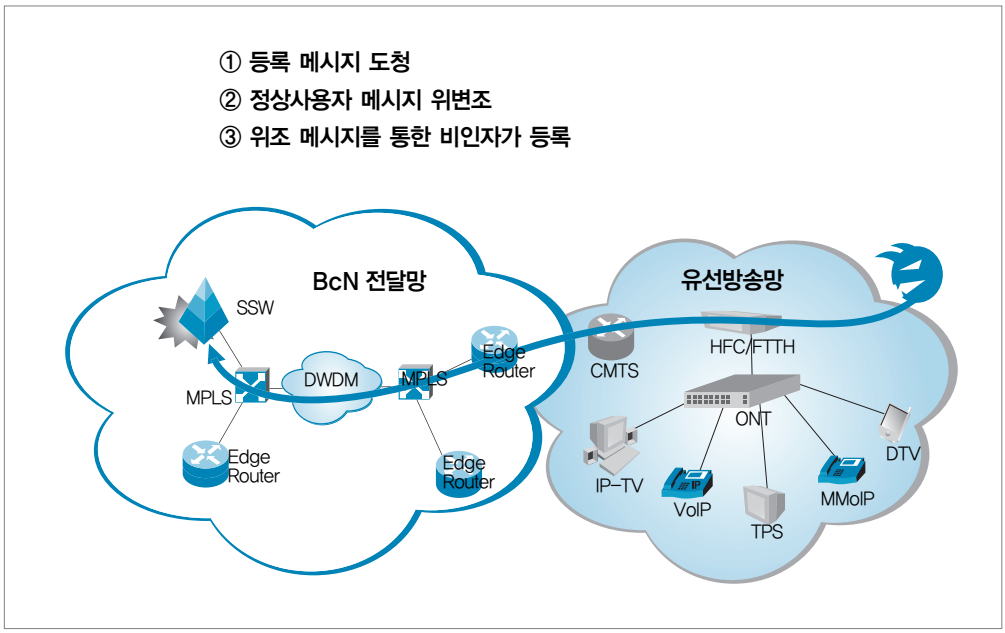
제6절 메시지 위 · 변조

1. 사용자 등록 메시지 위 · 변조

사용자 등록 메시지 위 · 변조 위협은 공격자가 불법적인 서비스 사용 등을 목적으로 서비스를 제공하는 주요 장비에 대한 사용자 등록과정의 메시지를 위조 또는 변조하여 정상 사용자인 것처럼 위장하는 것을 말한다.

가. 위협 시나리오

(그림 4-17) 사용자 등록 메시지 위 · 변조 위협



① 공격자는 네트워크 스캐닝 도구를 사용하여 특정 서비스 제공 장비(예: SSW, SIP 서버 등) 또는 LAN 구간 등에서 해당 프로토콜, 포트 등에 대해 스니핑을 통해 사용자 등록정보를 도청한다.

② 공격자는 세션 하이재킹 도구를 사용하여 등록메시지 세션을 가로챈 후, 인증정보 또는 주소 정보 등을 공격자의 데이터로 조작하여 해당 서버에 전송한다.

③ 서비스 제공 장비는 위 · 변조 데이터를 정상적으로 처리하여 저장한다.

※ 이후, 서비스 제공 장비는 공격자에게 정상 서비스 제공, 공격자가 의도한 위치로 서비스 제공 등의 문제를 가지게 된다.

나. 공격대상

- 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 사용자 등록 서비스를 제공하는 장비에 대한 사용자 등록 메시지

다. 예상피해

- 서비스를 제공하는 사업자에게는 과금되지 않는 불법 서비스 사용에 따른 금전적 피해 및 이로 인한 개인정보 침해에 대한 분쟁 등이 발생할 수 있다.
- 사용자에게는 부당한 서비스 이용 금액 지출, 공격자에게 서비스 사용 기록 및 통화내용 등의 콘텐츠 누설 등의 문제가 발생할 수 있다.

라. 고려사항

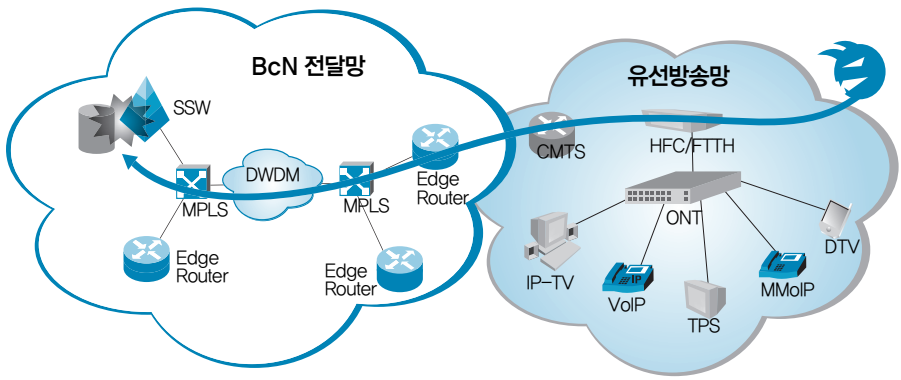
사용자 등록 메시지 위 · 변조 위협은 발생시 피해의 정도는 크다고 할 수 있으나, 사용자 등록과정이 자주 일어나지 않고 응용서비스 및 공격기법에 대한 충분한 이해를 필요로 하며 피해범위가 제한되어 있다는 점에서 공격의 발생의 가능성은 낮은 편이다.

2. 가입자 정보 위 · 변조

가입자 정보 위 · 변조 위협은 공격자가 불법적인 서비스 사용 또는 서비스 방해 등을 목적으로 서비스를 제공하는 주요 장비에 저장된 가입자 정보를 위조 또는 변조하는 것을 말한다.

가. 위협 시나리오

(그림 4-18) 가입자 정보 위 · 변조 위협



① 공격자는 음성 · 영상 또는 방송 등 서비스 가입자를 관리하는 서버(예: SSW, SIP 서버 등)의 IP 주소를 획득하고, 해당 서버의 운영체제 취약점, SNMP 및 HTTP 등의 관리 프로토콜 취약점 등을 악용해 해킹한 후, 가입자 정보가 저장된 Database에 접근한다.

② 공격자는 Database의 관리자 권한을 획득한 후 Database에 저장된 가입자의 인증정보, 과금정보 등을 위조 또는 변조한다.

나. 공격대상

- 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 가입자 정보를 관리 또는 저장하는 서버

다. 예상피해

- 서비스를 제공하는 사업자에게는 과금정보 유실 또는 변경에 따른 금전적 피해, 가입자 정보 재구축을 위한 비용 손실, 서비스 제공 불능, 가입자 정보 누출로 인한 개인정보 침해에 대한 분쟁 등이 발생할 수 있다.
- 사용자에게는 가입자 등록시 제공한 개인정보의 누출, 부당한 서비스 이용 금액 지출, 서비스 이용 불능 등의 문제가 발생할 수 있다.

라. 고려사항

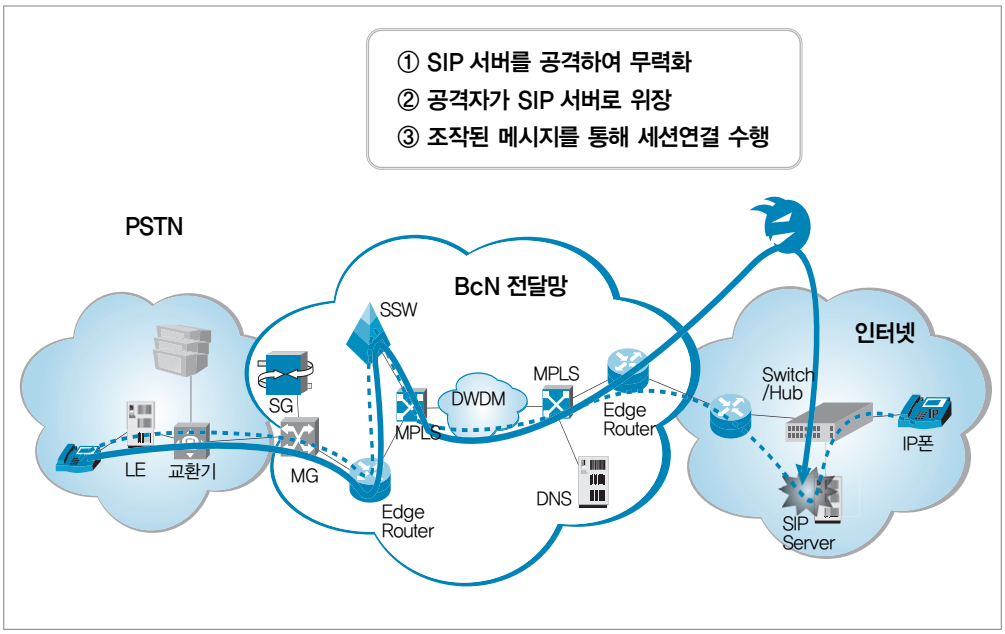
가입자 정보 위 · 변조 위협은 발생시 대량의 가입자 정보에 피해가 미치므로 그 정도가 매우 심각하다. 해당 서버에 접근이 허용될 경우 알려진 공격기법들이 많아 공격 발생 가능성도 비교적 높다.

3. 세션 연결 메시지 위 · 변조

세션 연결 메시지 위 · 변조 위협은 공격자가 불법적인 서비스 제어권한 획득, 잘못된 정보 전달, 불법적인 정보획득 등을 목적으로 서비스를 제공하는 주요 장비와 서비스 요청 장비간에 세션에 개입하여 메시지를 위조 또는 변조하는 것을 말한다.

가. 위협 시나리오

(그림 4-19) 세션 연결 메시지 위 · 변조 위협



① 공격자는 네트워크 스캐닝 도구를 사용하여 특정 서비스를 제공하는 장비(예: SSW, SIP 서버 등)의 IP 주소를 획득한다.

② 공격자는 스푸핑 등을 통해 서비스 제공 장비를 무력화 시킨 후, 메시지 조작을 통해 서비스 제공 장비로 위장한다.

※ 서비스 제공 장비가 활성화되지 않은 경우 스푸핑 등의 과정없이 위장 가능

③ 공격자는 서비스 제공 장비로 위 · 변조된 메시지를 사용해 응답하여 서비스 요청 장비와 정상적인 세션을 수립한다.

※ 이후, 공격자는 서비스 사용장비에서 전송하는 모든 메시지를 획득하거나, 서비스 사용장비에 잘못된 정보를 주입할 수 있다.

나. 공격대상

- 소프트스위치, SIP 서버, 방송센터 서버, 시그널링 및 미디어 게이트웨이, DNS 서버, DHCP 서버 등 서비스를 제공하는 서버

다. 예상피해

- 소프트스위치 등을 운영하는 서비스 제공 사업자 및 DNS 서버 등을 운영하는 망 운영 사업자에게는 서비스 제공 불능 등을 초래할 수 있다.
- 사용자에게는 공격자에게 서비스 사용 기록, 통화내용 및 금융정보 등의 콘텐츠 노출, 개인정보의 누출 등의 문제가 발생할 수 있다.

라. 고려사항

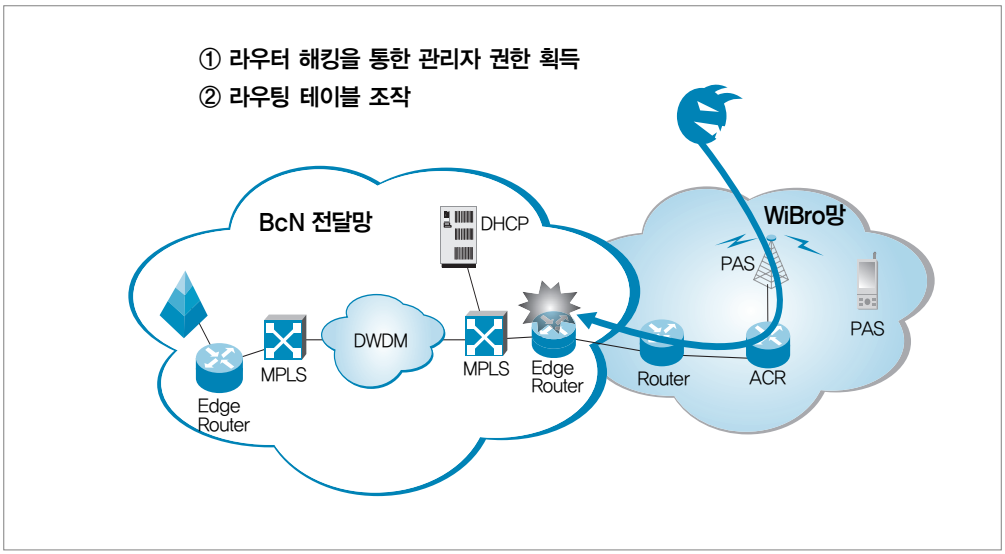
세션 연결 메시지 위 · 변조 위협은 발생시 다수의 서비스 이용자에게 피해를 미칠 수 있으나, 이를 성공하기 위해서는 응용 서비스 계층에 대한 고도의 지식과 공격기술, 위조 서비스 시스템 자원이 필요하며, 사업자가 서비스 제공 시스템이 무력화된 상황을 발견하기 쉽다는 점에서 공격 발생 가능성은 낮은 편이다.

4. 라우팅 메시지 위 · 변조

라우팅 메시지 위 · 변조는 공격자가 특정 네트워크 마비, 데이터 전송 경로 변경, 서비스 방해 등을 목적으로 라우팅을 제공하는 주요 장비의 라우팅 정보 변경, 위 · 변조된 라우팅 메시지를 주입하는 것을 말한다.

가. 위협 시나리오

(그림 4-20) 라우팅 메시지 위 · 변조 위협



① 공격자는 라우터의 운영체제 취약점, 관리적 취약점 등을 악용하여 관리자 권한을 획득한다.

② 공격자는 라우팅 테이블을 조작하여 공격하고자 하는 네트워크로 라우팅 트래픽이 집중되도록 설정한다.

※ 공격자는 라우팅 테이블 조작없이, 소스 라우팅으로 전송 트래픽에 라우팅 경로를 지정하여 공격할 수도 있음

※ 이후, 해당 라우터에 도착하는 트래픽은 공격자가 설정한 링크로 전송된다.

나. 공격대상

• 라우팅 기능을 제공하는 일반 라우터, MPLS 라우터

다. 예상피해

• 망 운영 사업자에게는 라우터의 특정 네트워크 인터페이스 차단, 특정 링크에 트래픽 집중 또는 잘못된 경로의 패킷 전달로 네트워크 마비를 초래할 수 있다.

라. 고려사항

라우팅 메시지 위·변조 위협은 망 운영자에게 피해를 미칠 수 있으나, 직접적으로 사용자에게 미치는 피해가 적고 라우팅 이상은 탐지가능성이 높다는 점에서 공격 발생 가능성은 낮은 편이다.

제 5 장 BcN 연동구간 정보보호 대책

제1절 BcN 위협별 보안대책

[표 5-1] BcN 위협별 보안대책

위협	정보보호 대책
■ 서비스 거부공격	
• 시스템 자원고갈	
대량 SIP INVITE 메시지 전송	• 단위 시간당 INVITE 메시지 처리량 제한 • 외부에서 메시지 처리장비에 직접 접근할 수 없도록 하거나, 접근을 통제할 수 있는 네트워크 구조 운영 • 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 • 사용자 인증 및 기기인증 메커니즘 적용 • 통합 모니터링 및 보안관제를 수행하여 대량의 INVITE 패킷 폭주시, 패킷 전송 근원지 차단
대량의 DHCP Request 메시지 전송	• 사용자 인증 및 기기인증 메커니즘 적용 • 단시간 대량의 DHCP Request 메시지를 요청하는 시스템 차단
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 • 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입시 차단 • 시스템 자원 및 트래픽 모니터링 및 이상 트래픽 통제 • uRPF 기능을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는

위협	정보보호 대책
대량의 IP 패킷 전송	대량 패킷 차단 • 보안패치 및 업그레이드 • 시스템의 Backlog Queue 사이즈 늘림
연결 해제 또는 종료 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 • 사용자 인증 및 기기인증 메커니즘 적용 • 메시지 전송채널 보호 • S/MIME 등 메시지 암호화 적용
비정상 등록 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 • 사용자 인증 및 기기인증 메커니즘 적용 • 메시지 전송채널 보호 또는 S/MIME 등 메시지 암호화 적용
MPLS 라우팅 정보 변경	• 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 및 시스템 침입탐지 • 사용자 인증 및 기기인증 메커니즘 적용 • MPLS 라우팅 정보 교환 프로토콜인 LDP(Label Distribution Protocol)에 보안 메커니즘 적용 • uRPF 기능을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷 차단
• 네트워크 경로자원 고갈	• ACL 적용운영, 스캐닝 공격 탐지 및 시스템 침입탐지 • 웜 · 바이러스 및 유해트래픽 자동차단 • 네트워크 자원 모니터링 및 자원 사용량 통제 • 단위시간당 패킷 전송량 제한 • 전송 경로 이중화 및 우회경로 확보 • 통합 모니터링 및 보안 관제 • 백업 및 장애대응 절차 수립 • 보안패치 및 업그레이드 • 사용자 인증 및 기기인증 메커니즘 적용 • uRPF 기능을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷 차단
■ 서비스품질 (QoS) 저하	
• QoS가 조작된 패킷 인입	• ACL 설정 운영 및 스캐닝 공격 탐지 • 메시지 전송채널 보호 • 네트워크 자원 모니터링 및 사용량 통제 • 서비스별, 사용자별 단위시간당 전송 패킷 제한

위협	정보보호 대책
• QoS가 조작된 패킷 인입	• 전송 경로 이중화 및 우회경로 확보 • 통합 모니터링 및 보안 관제 • 보안패치 및 업그레이드
• DiffServ 자원절도	• ACL 설정 운영, 스캐닝 공격 탐지 및 시스템 침입탐지 • 메시지 전송채널 보호 • 사용자 인증 및 기기인증 메커니즘 적용 • 네트워크 자원 모니터링 및 사용량 통제 • 서비스별, 사용자별 단위시간당 전송 패킷 제한 • 전송 경로 이중화 및 우회경로 확보 • 통합 모니터링 및 보안 관제 • 보안패치 및 업그레이드
• 잡음 삽입	• 공격대상 선정을 위한 스캐닝 공격 탐지 • ACL 설정 운영 및 시스템 침입탐지 • 사용자 인증 및 기기인증 메커니즘 적용 • 미디어 데이터 전송 채널 보호 • 미디어 데이터 암호화 적용
■ 시스템 해킹	
• 시스템 설정 오류	• 시스템 설치시 기본설정값 변경 • 시스템 설치후, 최신 업데이트 및 보안패치 • 주요시스템 관리자 모드 설정 암호 변경 • ACL, 스캐닝 공격 탐지 및 시스템 침입탐지 • 웜 · 바이러스 차단 • 비인가 프로세스 감사
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터 암호화 적용 • ACL 설정 운영 • 사용자 인증 및 기기인증 메커니즘 적용 • 보안이 강화된 원격접속 프로토콜 사용
• 운영체제 및 어플리케이션 취약점	• ACL 설정운영, 스캐닝 공격 탐지 및 시스템 침입탐지 • 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드 • 불필요한 서비스 제거 • 비인가 프로세스 감사 • 웜 · 바이러스 및 유해트래픽 자동차단 • 통합 모니터링 및 보안 관제 • 사용자 인증 및 기기인증 메커니즘 적용 • 주기적인 취약점 점검

위협	정보보호 대책
■ 도청	
• 연동장비 해킹을 통한 도청	• 연동장비의 IP 주소, 포트 등에 대한 접근제한 • 비인가 프로세스 제거 • 공격자의 도청행위 방지를 위한 정보접근 영역 분리
• 전송패킷 분석을 통한 도청	• 제어 데이터, 미디어 및 사용자 데이터 암호화 • 네트워크 공유 구간에서 정기적인 스니핑 도구 동작 검사 • 스니핑 방지 네트워크 환경 구성
• 세션 가로채기를 통한 도청	• 메시지 무결성 검증 가능한 서비스 프로토콜 사용 • 제어 데이터, 미디어 및 사용자 데이터 암호화 • 세션 가로채기 방지 네트워크 환경 구성 • 스니핑 및 과도 트래픽 유발 시스템 모니터링 및 조치
• Fake DHCP 서버 운영을 통한 도청	• DHCP 트래픽 모니터링을 통한 Fake DHCP 서버 제거 • 네트워크 장비에서 DHCP 인가(Trust) 포트 설정운영 • 비인가 DHCP 서버의 네트워크 접속 차단
■ 메시지 위 · 변조	
• 사용자 등록 메시지 위 · 변조	• 서비스 등록 메시지 암호화 • 서비스 등록에 대한 상호인증 적용
• 가입자 정보 위 · 변조	• 연동장비에 대한 해킹 차단 • 연동장비의 IP 주소, 포트 등에 대한 접근제한 • 서비스 제공과 가입자 정보 관리간 기능영역 분리 운영 • 가입자 정보 저장데이터에 대한 무결성 검사 • 가입자 정보 보호를 위한 관련 법규, 지침 및 절차 등의 준수
• 세션 연결 메시지 위 · 변조	• 메시지 무결성 검증 가능한 서비스 프로토콜 사용 • 제어 데이터, 미디어 및 사용자 데이터 암호화 • 세션 가로채기 방지 네트워크 환경 구성 • 스니핑 및 과도 트래픽 유발 시스템 모니터링 및 조치
• 라우팅 메시지 위 · 변조	• 라우터에 대한 해킹 차단 • 라우터의 보안기능 활성화 • 라우터에 접근하는 IP 주소, 포트 등에 대한 접근제한 • 라우터 내의 비인가 프로세스 제거 • 라우팅 테이블에 대한 무결성 검사

제2절 서비스 거부공격

1. 시스템 자원고갈

(1) 대량 SIP INVITE 메시지 전송

가. 위협 개요

연결설정 메시지인 SIP INVITE 메시지를 대량으로 전송하여 메시지 처리 장비의 자원을 고갈시키는 공격으로 정상적인 서비스 제공을 방해하는 공격위협이다.

나. 보호대상

- 소프트스위치, SIP 서버 등 BcN 메시지 처리장비

다. 보호대책

- 단시간 대량의 INVITE 메시지 처리량 제한 운영
  ※ 예: 단위시간당 INVITE 처리량, 단일 host의 INVITE 요청 수 설정 등
- 외부에서 메시지 처리장비에 직접 접근할 수 없도록 하거나, 접근을 통제할 수 있는 네트워크 구조 운영

■ 네트워크 구조 운영 예제

- 사설망 구성 등을 통해 네트워크 구조를 감추고, 사설망 내부에서 소프트스위치, SIP 서버 등의 메시지 처리 장비를 운영
- SSW, SIP 서버 등의 메시지 처리 장비 앞단에 서비스 콘텐츠를 이해하는 Proxy 방식의 침입차단시스템(예: Application Level Gateway, Session Border Controller)을 운영하여 비인가 또는 과도한 INVITE 메시지 등을 필터링

• 공격 대상 선정을 위한 스캐닝 공격 탐지

■스캐닝 공격 탐지 방식 예제

• 로그 파일 점검

– 스캐너가 일정 시간동안 많은 포트에 접속하여 서비스를 요구함으로, 시스템 로그 파일을 분석하여 스캔 공격 탐지 가능

• 네트워크 트래픽 감시

– tcpdump, snoop, netlog 등의 도구를 이용하여 실시간 또는 로그를 남겨 스캔 공격 탐지

※ 로그가 매우 많을 수 있으므로 주기적인 감시필요

• 스캐닝 공격탐지 도구 적용

– courtney, gabriel, Natas, iplog, sentry 등

• ACL 설정 운영

– 메시지 처리 장비 내에 ACL(Access Control List)을 구성하여 연동장비에 접근하는 비인가된 IP 주소, 프로토콜 및 포트에 대한 접근 차단

■ACL 구성 방법 예제

• UNIX, Linux 계열의 운영체제를 사용하는 연동장비의 경우, host.deny, host.allow 등에 차단/허용 IP 주소를 설정하거나, IPChains, TCP Wrappers, IP Filter 등의 프로그램을 설치하여 접근차단

• Cisco, Juniper 라우터의 경우 access-list 명령어, firewall-filter 등을 설정하여 접근차단

• 사용자 인증 및 기기인증 메커니즘 적용

※ 예: 사용자 또는 기기(단말, Gateway 등)를 인증하여 정당한 사용자인 경우에만 INVITE 메시지 처리

• 통합 모니터링 및 보안관제를 수행하여 대량의 INVITE 패킷 폭주시, 패킷 전송 근원지 차단

(2) 대량의 DHCP Request 메시지 전송

가. 위협 개요

사용자 단말에 IP를 부여하는 DHCP 서버에 대량의 DHCP Request 메시지를 전송하여 DHCP가 관리하는 IP 주소자원을 고갈시키는 공격 위협을 말한다.

나. 보호대상

- DHCP서버, DHCP의 IP 주소자원

다. 보호대책

- 사용자 인증 및 기기인증 메커니즘 적용
- 단시간 대량의 DHCP Request 메시지를 요청하는 시스템 차단

(3) 대량의 IP 패킷 전송

가. 위협 개요

공격자가 플러딩 공격도구를 사용하여 TCP SYN Flooding, ICMP Flooding, Ping of Death, UDP Flooding 등의 공격을 수행하여 주요 시스템의 네트워크 연결설정을 위한 자원을 고갈시키는 공격이다.

나. 보호대상

- CMTS, SIP 서버, Gateway, MPLS 라우터 등 BcN 망에서 IP 패킷을 처리하는 시스템

다. 보호대책

- 공격대상 선정을 위한 스캐닝 공격 탐지
- ACL 설정 운영
- 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입시 차단
- 시스템 자원 및 트래픽 모니터링 및 이상 트래픽 통제

※ 예: 보안관제 등을 통해 이상 트래픽 모니터링 및 통제

• uRPF 기능을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷 차단
• 보안패치 및 업그레이드
• 시스템의 Backlog Queue 사이즈 늘림

■Backlog Queue
• 시스템에서 3Way Handshake로 TCP 세션 연결시, 세션연결이 완료되기까지의 세션 요청 상태를 저장하는 공간

■예제 : 유닉스/리눅스 시스템 Backlog Queue 사이즈 늘림
• FreeBSD : net.inet.tcp.syncache.cachelimit 값을 올림
• 리눅스 : sysctl 명령으로 net.ipv4.tcp_max_syn_ backlog 값을 늘림

2. 비정상 메시지 전송

(1) 연결 해제 또는 종료 메시지 전송

가. 위협 개요

공격자가 연결해제/종료 메시지인 SIP CANCEL, SIP BYE 메시지를 생성하여 정상적인 연결을 끊는 공격 위협을 말한다.

나. 보호대상
• 소프트스위치, SIP 서버 등 BcN 메시지 처리 시스템

다. 보호대책
• 공격대상 선정을 위한 스캐닝 공격 탐지
• ACL 설정 운영
• 사용자 인증 및 기기인증 메커니즘 적용
• 메시지 전송채널 보호 또는 S/MIME 등 메시지 암호화 적용

■SIP 메시지 보호방식

• HTTP Digest Authentication
  – SIP에서는 호(call)의 성립시 사용자 인증을 위해 적용
  – 사용자 등록시 nonce 값, ID/PW 등의 값들을 MD5 checksum으로 전송하여 패스워드가 평문으로 전송되어 노출되는 것을 방지
• S/MIME(Security Services for MIME)
  – SIP 프로토콜을 통하여 전송되는 SIP 메시지는 MIME 형태로 전송됨
  – MIME에서는 MIME 데이터의 integrity와 confidentiality를 보장
  – S/MIME을 적용하여 공개키 분배, 인증, 무결성, 시그널 메시지의 기밀성 제공 가능
    ※ S/MIME은 메시지 양이 크기 때문에 UDP보다 TCP상에서 전송 권장함
• TLS(Transport Layer Security)
  – SIP 메시지의 무결성, 기밀성 제공과 재생(replay)공격 방지
  – Hop-by-Hop에서만 전송가능하며 TCP에서만 사용
• IPSec(IP Security Protocol)
  – 네트워크 레이어(L3)의 IP 패킷 단위의 암호화 수행
  – UDP/TCP에 모두 적용가능하며, 메시지 암호화 적용
  – 인증, 무결성, 기밀성 등을 제공하며, hop-by-hop, end-to-end 보안 모두 제공

⑵ 비정상 등록 메시지 전송

가. 위협 개요

비정상 등록 메시지 전송 위협은 공격자가 소프트스위치, SIP 서버 등 시그널 처리 장비에 비정상 등록 메시지를 이용하여 비인가자를 정상 사용자처럼 등록하여 서비스를 도용하는 공격 위협이다.

나. 보호대상

• 소프트스위치, SIP 서버 등 BcN 메시지 처리 시스템

다. 보호대책

- 공격대상 선정을 위한 스캐닝 공격 탐지
- ACL 설정 운영
  - 메시지 처리 장비에 접속 가능한 IP 대역폭을 설정하여 비인가자의 접속시도 방지
- 사용자 인증 및 기기인증 메커니즘 적용
- 메시지 전송채널 보호 또는 S/MIME 등 메시지 암호화 적용

(3) MPLS 라우팅 정보 변경

가. 위협 개요

MPLS 라우팅 정보 변경 위협은 공격자가 MPLS 라우터에 비정상적인 MPLS 라우팅 메시지를 전달하여 MPLS 라우터의 라우팅 테이블을 변경하는 공격의 위협으로, 네트워크 트래픽 경로 변경에 따라 서비스 품질저하, 서비스 거부 등 대규모 피해 발생이 예상되는 위협이다.

나. 보호대상

- MPLS 라우터의 라우팅 프로토콜 및 라우팅 테이블

다. 보호대책

- 공격대상 선정을 위한 스캐닝 공격 탐지
- ACL 설정 운영 및 시스템 침입탐지
- 사용자 인증 및 기기인증 메커니즘 적용

  ※ 예: MPLS와 연결되는 가입자망의 라우터에 대해 VPN 기술 등을 사용하여 인증
- MPLS 라우팅 정보 교환 프로토콜인 LDP(Label Distribution Protocol)에 보안 메커니즘 적용

■MPLS LDP 보호

• LDP에 TCP MD5 옵션 적용

– MPLS 에지라우터가 피어 라우터와 정보교환을 위해 사용하는 TCP에 MD5 알고리즘 적용

3. 네트워크 경로자원 고갈

가. 위협 개요

공격자가 웜 · 바이러스를 유포 시키거나, DDoS 공격, 패킷 생성 도구 등을 이용하여 대량의 패킷을 생성하여 비정상 IP 트래픽을 증가시키는 공격의 위협으로 네트워크 경로자원 고갈로 인한 서비스 거부 공격의 피해는 대규모이고, 피해금액도 매우 크다.

나. 보호대상

• MPLS 라우터, Gateway 등의 연동구간 전송경로의 자원

다. 보호대책

• ACL 설정 운영, 스캐닝 공격 탐지 및 시스템 침입탐지
• 비인가 프로세스 검사
• 이상 트래픽 탐지 및 차단

※ 예: 침입방지시스템(IPS), 싱크홀 및 블랙홀 라우터 기술 적용

• 웜 · 바이러스 및 유해트래픽 자동차단
• 네트워크 자원 모니터링 및 자원 사용량 통제
• 단위시간당 패킷 전송량 제한
• 전송 경로 이중화 및 우회경로 확보
• 통합 모니터링 및 보안 관제
• 백업 및 장애대응 절차 수립 · 운영
• 보안패치 및 업그레이드

• uRPF 기능을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷 차단

■uRPF(Unicast Reverse Path Forwarding)

• 변조된 근원지 IP를 갖고 공격 목적지로 전달되는 패킷을 검사해 FIB-포워딩 테이블에 정의된 실제 소스 IP인지 점검한다. 이 테이블에 없는 IP일 경우 네트워크 장비는 이 패킷을 변조된 IP로 판단하고 폐기하는데, 이 방식을 uRPF라 한다.

• 이 방식은 굳이 ACL를 적용해 패킷 필터링 기술을 적용시키는 것이 아니기 때문에, 네트워크 장비의 자원을 효율적으로 사용할 수 있다.

제3절 서비스품질(QoS) 저하

1. QoS가 조작된 패킷 인입

가. 위협 개요

QoS가 조작된 패킷 인입 위협은 공격자가 패킷 필드의 QoS 우선순위를 조작한 후, 네트워크에 대량으로 인입시켜 서비스 품질을 저하시키는 공격의 위협이다.

나. 보호대상

- CMTS, SIP 서버, Gateway, MPLS 라우터 등 BcN 망에서 IP 패킷 처리하는 시스템

다. 보호대책

- ACL 설정 운영 및 스캐닝 공격 탐지
- 메시지 전송채널 보호

  ※ 예: MPLS라우터 등 하부구조에서 IPSec 등을 사용하는 VPN 기술 적용
- 네트워크 자원 모니터링 및 사용량 통제

  ※ 예: 특정 QoS 클래스별 대역폭 사용량 모니터링
- 서비스별, 사용자별 단위시간당 전송 패킷 제한
- 전송 경로 이중화 및 우회경로 확보
- 통합 모니터링 및 보안 관제
- 보안패치 및 업그레이드

2. DiffServ 자원절도

가. 위협 개요

DiffServ 자원절도 위협은 공격자가 정상사용자 근원지 주소를 도용하여 높은 우선 순위의 패킷을 생성하여 자신의 패킷을 전송시키는 방식으로, 결과적으로는 네트워크 자원을 무단으

로 절도하여 사용하는 효과를 얻는 QoS 관련 공격의 위협이다.

나. 공격대상

• DiffServ를 적용하고 있는 MPLS 라우터 및 IP 패킷

다. 보호대책

• ACL 설정 운영, 스캐닝 공격 탐지 및 시스템 침입탐지
• 메시지 전송채널 보호
※ 예: MPLS라우터 등 하부구조에서 IPSec 등을 사용하는 VPN 기술 적용
• 사용자 인증 및 기기인증 메커니즘 적용
• 네트워크 자원 모니터링 및 사용량 통제
※ 예: 특정 QoS 클래스별 대역폭 사용량 모니터링
• 서비스별, 사용자별 단위시간당 전송 패킷 제한
• 전송 경로 이중화 및 우회경로 확보
• 통합 모니터링 및 보안 관제
• 보안패치 및 업그레이드

3. 잡음 삽입

가. 위협 개요

잡음 삽입 위협은 BcN 연동구간에서 전송되는 대용량의 멀티미이더 데이터나 실시간 전송을 하여야하는 음성이나 영상 패킷의 사용자 데이터 필드를 변조하는 공격의 위협을 말한다.

나. 보호대상

• BcN 연동구간에서 전송되는 멀티미디어 데이터, 음성전화 데이터 등

다. 보호대책

• 공격대상 선정을 위한 스캐닝 공격 탐지
• ACL 설정 운영 및 시스템 침입탐지

• 사용자 인증 및 기기인증 메커니즘 적용
• 미디어 데이터 전송 채널 보호
• 미디어 데이터 암호화 적용

■미디어 데이터 보호방식(예제)

• CAS(Conditional Access System)
  – 단방향 방송망에 적합한 구조로 다양한 디지털 미디어 전송에 적용 가능
  – 전송 콘텐츠 경로에 대한 접근 제어를 수행
  – IP 환경에서 콘텐츠 유출 가능성 보완
    ※ 콘텐츠 불법 복제 방지 위한 메커니즘 부재
• SRTP(Secure Real Time Protocol)
  – 음성전화 서비스의 미디어 트래픽 암호화에 적용
• DRM(Digital Right Management)
  – 불법 컨텐츠 복사 방지를 위해 컨텐츠를 암호화

제4절 시스템 해킹

1. 시스템 설정 오류

가. 위협 개요

시스템 설정 오류 위협은 시스템 해킹의 가장 초보적인 공격방식으로 장비의 설정후 변경되지 않은 기본값(관리자 암호, 불필요한 서비스 등) 을 이용하여 접속을 시도하는 공격의 위협이다.

나. 보호대상

- BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

다. 보호대책

- 시스템 설치시 기본설정값 변경
- 시스템 설치후, 최신 업데이트 및 보안패치
- 주요시스템 관리자 모드 설정 암호 변경
- ACL 설정 운영, 스캐닝 공격 탐지 및 시스템 침입탐지

  ※ ACL 설정 운영은 자체시스템 또는 Firewall 등을 활용할 수 있음
- 웜 · 바이러스 차단
- 비인가 프로세스 감사

2. 원격접속 프로토콜 취약점

가. 위협 개요

원격접속 프로토콜의 취약점을 이용하는 시스템 해킹방식은 공격자가 원격지에서 접속하는 시스템 관리자의 패킷을 분석하여 암호를 알아내어 관리자 모드로 접속하는 공격의 위협이다.

나. 보호대상

- BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

다. 보호대책

- 관리자 모드 전송 데이터 암호화 적용
- ACL 설정 운영

※ 관리를 수행하는 IP 주소에 대해서만 접근을 허용

- 사용자 인증 및 기기인증 메커니즘 적용

※ 상호인증 메커니즘을 사용한 사용자 인증 수행

- 보안이 강화된 원격접속 프로토콜 사용

※ 예: 신뢰된 구간에서 원격접속을 하지 않는 경우에 SNMP의 경우 SNMPv3, HTTP의 경우 SSL, TFTP의 경우 Secure TFTP 사용 등

■SSL 개요

- HTTP 계층 아래의 SSL 서브 계층에서 사용자 데이터 암호화
- TCP/IP에서 HTTP 포트 80 대신에 포트 443 사용
- SSL은 RC4 스트림 암호 알고리듬용으로 40비트 키 사용
- 브라우저에서 https://URL로 페이지를 지정하면 HTTPS는 그것을 암호화하고, 도착된 https://URL은 HTTPS 서브 계층에서 복호화하는 방식으로 동작
- HTTPS와 SSL은 사용자의 송신자 인증을 위해 서버로부터 X.509 디지털 인증서 사용 지원

3. 운영체제 및 어플리케이션 취약점

가. 위협 개요

BcN 주요 장비의 시스템 및 시스템에서 제공하는 각종 운영체제 서비스의 설정과 관련된 취약점을 이용하여 해킹을 시도 공격의 위협이다.

나. 공격대상

- BcN 주요 연동 장비인 소프트스위치, CMTS, SIP 서버, Gateway, MPLS 라우터, DHCP서버, DNS 서버

나. 보호대책

- ACL 설정운영, 스캐닝 공격 탐지 및 시스템 침입탐지
- 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드
- 불필요한 서비스 제거
- 비인가 프로세스 감사
- 웜 · 바이러스 및 유해트래픽 자동차단
- 통합 모니터링 및 보안 관제
- 사용자 인증 및 기기인증 메커니즘 적용
- 주기적인 취약점 점검

이외에도, BcN 주요 운영체제인 유닉스와 윈도우즈관련 시스템 해킹에 악용되는 취약점과 대응방안은 "[부록2] BcN 시스템 운영체제별 해킹 위협 및 대응방안"을 참고하도록 한다.

제5절 도청

1. 연동장비 해킹을 통한 도청

가. 위협개요

소프트스위치, 시그널링 및 미디어 게이트웨이 등의 연동장비 해킹을 통해 시그널링 메시지, 음성통화, 금융거래 및 사용자 인증정보, 방송 컨텐츠 등을 도청하는 위협이다.

나. 보호대상

- 시그널 게이트웨이, 미디어 게이트웨이, 소프트스위치, SIP 서버, 라우터, CMTS 등의 연동장비

다. 보호대책

- 연동장비에 대한 해킹 차단

  ※ '제4절 시스템 해킹'의 대책에 따라 조치

- 연동장비의 IP 주소, 포트 등에 대한 접근제한

  – 외부에서 연동장비에 직접 접근할 수 없도록 하거나, 접근을 통제할 수 있는 네트워크 구조 운영

■네트워크 구조 운영 예제

- 사설망을 구성하고, 사설망 내에서 SSW, SIP 서버 등 운영
- SSW, SIP 서버 등의 연동장비 앞단에 서비스를 이해하는 상태기반의 침입차단시스템(예: Application Level Gateway, Session Border Controller)을 운영하여 비인가 접근을 차단

– 연동장비 내에 ACL(Access Control List)을 구성하여 연동장비에 접근하는 비인가된 IP 주소, 프로토콜 및 포트에 대한 접근 차단

■ACL 구성 방법 예제

- UNIX, Linux 계열의 운영체제를 사용하는 연동장비의 경우, host.deny, host.allow 등에 차단/허용 IP 주소를 설정하거나, IPChains, TCP Wrappers, IP Filter 등의 프로그램을 설치하여 접근차단
- Cisco, Juniper 라우터의 경우 access-list 명령어, firewall-filter 등을 설정하여 접근차단

• 비인가 프로세스 제거

– 백신 프로그램, 연동장비에서 제공하는 프로세스 검사 도구를 사용하여 주기적으로 도청을 위한 웜 · 바이러스, 백도어 프로그램, 루트킷 등 제거

• 공격자의 도청행위 방지를 위한 정보접근 영역 분리

– 연동장비 내에서 사용자의 역할에 따라 접근 가능한 영역을 분리 운영

※ 이를 통해, 공격자가 해킹에 성공한 이후에도, 연동장비 내에 도청 프로그램 설치, 모니터링 행위 등을 제한

■관련기술

- 참조 모니터링과 다중 등급의 강제적인 접근통제 기능으로 사용자의 객체(파일, 디바이스 등) 사용을 엄격하게 통제하는 보안운영체제(Secure OS) 기술이 있음

※ 이 대책은 연동장비가 제공하여야 하는 기본기능 구현에 복잡성을 가중시킬 수 있으므로, 다른 대책들이 우선적으로 고려되어야 한다.

2. 전송패킷 분석을 통한 도청

가. 위협개요

공격자가 LAN 등의 네트워크 공유 구간에서 스니핑 도구 등을 사용해 공유구간 사용자의

시그널링 메시지, 음성통화 및 방송 컨텐츠 등의 미디어 메시지, 금융거래 및 사용자 인증정보 등의 사용자 메시지를 도청하는 위협이다.

나. 보호대상

- 가입자 망의 네트워크 공유 구간에 있는 시그널 게이트웨이, 미디어 게이트웨이, 소프트스위치, SIP 서버 등의 서비스 제공 장비

다. 보호대책

- 제어 데이터, 미디어 및 사용자 데이터 암호화
  - 서비스 제공 장비(UAS, 예: SIP 서버, 미디어 게이트웨이, 방송서버 등)와 서비스 사용 장비(UAC, 예: 단말기 등) 구간에서 흐르는 제어/미디어/사용자 데이터에 대해 암호화 적용

■암호화 기술 적용방법 예제

- IPSec 보안 프로토콜을 사용하는 VPN 기술을 사용하여 UAS와 UAC간 네트워크 계층에서 암호화 (시그널, 미디어 및 사용자 메시지)

(그림 5-1) VPN 유형

다양한 VPN 유형들			
VPN 유형	**애플리케이션**	**속성**	**프로비전 주체**
VGP/MPLS IP VPN (RFC4364/RFC 2547bis)	사이트 대 사이트 ; 멀티 포인트	레이어 3 ; 보통 풀 메시 접속성 지원(허브 앤 스포크, 부분 메시, 엑스트라넷 접속성도 또한 프로비전 가능하다).	통신서비스 사업자
마티니 표준(AToM)	사이트 대 사이트 ; 포인트 투 포인트	레이어 2 ; MPLS 백본에서 레이어 2 트래픽의 포인트 투 포인트 전송 허용. 통신사업자는 레거시 인프라와 IP/MPLS 네트워크 인프라를 통합할 수 있다.	통신서비스 사업자
VPLS/IPLS	사이트 대 사이트 ; 멀티 포인트	레이어 2(이더넷이나 IP전용)전송 ; 풀메시 접속성 지원	통신서비스 사업자
GRE	사이트 대 사이트 ; 포인트 투 포인트	레이어 3 ; IP백본에서 레거시 프로토콜과 IP전송	통신서비스 사업자나 기업
IEEE 802.Q터널링 (Q-in-Q)	사이트 대 사이트	레이어 2 ; 이더넷 VLAN 헤더 시작 부분에 별도의 802.Q태그를 추가함으로써 고객 이더넷 트래픽을 분리	통신서비스 사업자
IPsec	사이트 대 사이트나 원격 엑세스 ; 포인트 투 포인트 터널 ; 언제나 공중 인터넷에서 사용됨	레이어 3 ; 보안게이트웨이나 호스트간에 IP트래픽을 암호화 혹은 인증	통신서비스 사업자나 기업
L2TPv2(Layer 2 Tunneling Version 2)	원격 엑세스	레이어 2 ; IP백본에서 PPP(Point-to-Point Protocol)를 캡슐화 및 터널링	통신서비스 사업자나 기업

VPN 유형	애플리케이션	속성	프로비전 주체
L2TPv3	원격 엑세스 ; 사이트 대 사이트	레이어 2 ; 포인트 투 포인트 IP 접속에서 레이어 2 프로토콜 캡슐화	통신서비스 사업자
SSL VPN(WebVPN)	원격 엑세스	레이어 4-7 ; 필요한 클라이언트 소프트웨어가 없기 때문에 사용자가 역동적으로 배치 할 수 있다	통신서비스 사업자나 기업

※ 출처 : Cisco.com

- TLS/SSL 등의 보안 프로토콜을 사용한 UAS와 UAC간 응용 계층에서 암호화 (시그널, 사용자 메시지)
- STRP, SRTCP 등의 보안 프로토콜, CAS(Conditional Access System), DRM(Digital Right Management) 등 컨텐츠 보안 기술을 사용한 UAS와 UAC간 응용 계층에서 암호화 (미디어, 사용자 메시지)

• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작 검사

– 네트워크 공유 구간의 시스템들에 대해 직접 또는 원격에서 스니핑 하는 시스템을 찾아 조치

■스니핑 여부 검사 방법 예제

- 리눅스의 경우, ifconfig 명령어를 사용하여 시스템의 인터페이스가 PROMISC가 설정되었는지 검사 (PROMISC 설정시 스니핑이 가능)
- 원격에서 특성 시스템의 스니핑 여부를 검사할 수 있는 Sentinel, AntiSniff, ARPWatch 등의 프로그램 활용

• 스니핑 방지 네트워크 환경 구성

– 네트워크 공유 구간에서 패킷을 broadcast 하는 장비(예: Dummy Hub) 대신에 스위치 장비로 네트워크를 구성

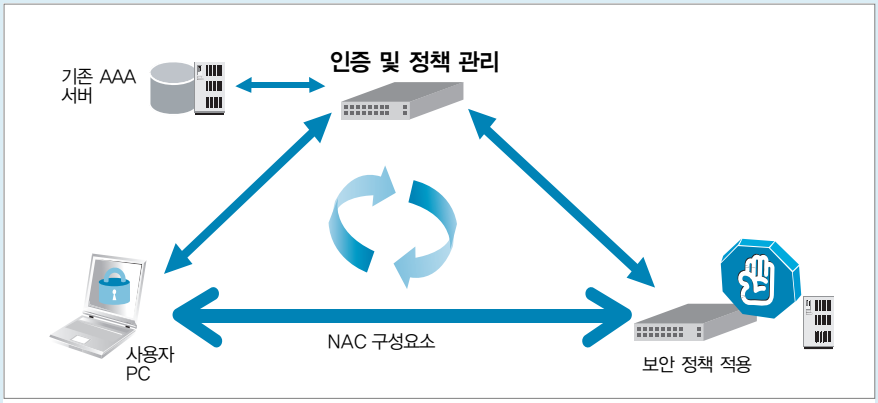
※ 스위치는 패킷을 해당 포트로만 전송하므로 스니핑이 어려움

– 이동식 장치를 포함하여 인가된 장비만 네트워크 공유 구간에서 네트워크에 연결할 수 있도록 관리하고, 네트워크에 연결된 비인가된 장비를 제거

■비인가 장비의 네트워크 접속 방지를 위한 관련기술

• NAC(Network Access Control) 기술

NAC 구성요소



※ 출처 : 주니퍼 네트웍스

– 사용자 단말기(PC 등)가 내부 네트워크에 접근하기 전에 사전에 정의해 놓은 보안정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 기술임

– 참조 사이트

- 마이크로소프트 NAP(Network Access Protection), http://www.microsoft.com/
- 시만텍, SEP(Sygate Enterprise Protection), http://www.symantec.com/
- 시스코시스템즈, NAC(Network Admission Control), http://www.cisco.com/
- 쓰리콤, TippingPoint Quarantine Protection, http://www.3com.com/
- 주니퍼네트웍스, UAC(Unified Access Control), http://www.kr.juniper.net/

3. 세션 가로채기를 통한 도청

가. 위협개요

공격자가 음성통화, 방송 서비스 등 진행중인 BcN 서비스 세션에 개입하여 정상 사용자 시스템에 대한 스푸핑 등을 통해 사용자의 음성통화 및 방송 컨텐츠 등의 미디어 메시지, 금융거래 및 사용자 인증정보 등의 사용자 메시지를 도청하는 위협이다.

나. 보호대상

• 소프트스위치, SIP 서버, 방송서버 등의 서비스 제공 장비 및 사용자 시스템

다. 보호대책

• 메시지 무결성 검증 가능한 서비스 프로토콜 사용

– 서비스 제공 장비(UAS)와 서비스 사용 장비(UAC)간의 메시지 교환에 메시지 조작 여부 판별이 가능한 전송 메시지 무결성 지원 서비스 프로토콜을 사용해 공격자의 세션 개입을 차단

※ 무결성 값 자체도 조작할 수 있으므로, UAS와 UAC간 공유된 비밀정보를 활용하여 전송 메시지 무결성을 제공이 필요

• 제어 데이터, 미디어 및 사용자 데이터 암호화

– 서비스 제공 장비(UAS)와 서비스 사용 장비(UAC)간의 메시지 교환에 무결성을 제공하는 암호화 프로토콜을 적용하여 공격자의 개입을 원천적으로 차단

※ 앞 단락, '2. 전송패킷 분석을 통한 도청'의 '제어 데이터, 미디어 및 사용자 데이터 암호화'와 동일하게 조치

• 세션 가로채기 방지 네트워크 환경 구성

– 세션 가로채기를 위한 사전조사 공격(스니핑)을 방지할 수 있도록 네트워크를 구성

※ 앞 단락, '2. 전송패킷 분석을 통한 도청'의 '스니핑 방지 네트워크 환경 구성'과 동일하게 조치

• 스니핑 및 과도 트래픽 유발 시스템 모니터링 및 조치

– 정기적인 스니핑 도구 동작 여부 조사

※ 앞 단락, '2. 전송패킷 분석을 통한 도청'의 '네트워크 공유 구간에서 정기적인 스니핑 도구 동작 검사'과 동일하게 조치

– 특정 정상 단말로 집중되는 이상 트래픽을 모니터링하여 트래픽 발신자에 대한 조치

4. Fake DHCP 서버 운영을 통한 도청

가. 위협개요

공격자가 위조된 DHCP 서버를 운영하여 위조된 GW, DNS 서버 등의 IP 주소를 클라이언트 제공하여, 클라이언트가 공격자의 시스템에 접속하도록 유도하여 공격자의 시스템에서 시그널, 미디어 등의 메시지를 도청하는 위협이다.

나. 보호대상

- Gateway, 사용자 시스템 등의 DHCP 주소를 사용하도록 설정된 시스템

다. 보호대책

- DHCP 트래픽 모니터링을 통한 Fake DHCP 서버 제거
  - 정기적으로 DHCP 트래픽 모니터링을 통해 지정되지 않은 서버에서 DHCP OFFER/ACK 브로드캐스트 메시지를 발송하는 서버를 찾아 제거
- 네트워크 장비에서 DHCP 인가(Trust) 포트 설정운영
  - 네트워크 장비에서 DHCP 인가(Truste) 포트를 정의하여 DHCP가 연결된 물리적 포트에만 DHCP IP Request 패킷을 허용하고, 다른 비인가(Untrust) 포트에는 DHCP IP Request 패킷을 포워딩하지 않도록 설정
- 비인가 DHCP 서버의 네트워크 접속 차단
  - 네트워크에 DHCP 서버 등의 시스템 연결시 관리자가 허가한 장비만 연결할 수 있도록 관리하고, 네트워크에 연결된 비인가된 장비를 제거

제6절 메시지 위 · 변조

1. 사용자 등록 메시지 위 · 변조

가. 위협개요

공격자가 음성통화, 방송, 금융거래 등의 서비스를 받기위한 사용자의 서비스 등록과정에 개입하여 정상 사용자인것처럼 등록 메시지를 위조 또는 변조하여 불법적으로 서비스를 이용하는 위협이다.

나. 보호대상

• 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 사용자 등록 서비스를 제공하는 장비에 대한 사용자 등록 메시지

다. 보호대책

• 서비스 등록 메시지 암호화

– 서비스 제공 장비(UAS)와 서비스 사용 장비(UAC)간의 등록 메시지 교환에 암호화 프로토콜 적용

※ 앞 단락, '2. 전송패킷 분석을 통한 도청'의 '제어 데이터, 미디어 및 사용자 데이터 암호화'와 동일하게 조치

• 서비스 등록에 대한 상호인증 적용

– 서비스 제공 장비(UAS)와 서비스 사용 장비(UAC)간의 등록 메시지 교환에 사용자 및 기기를 서비스 수준에서 상호인증할 수 있는 프로토콜을 적용

■관련기술 예제

• VoIP 서비스

– H.235 프로토콜을 사용한 RAS(Registration, Admission, Status) 수행

- SIP HTTP Digest 인증기술을 사용한 인증 수행

• 무선랜

- CHAP(Challenge Handshake Authentication Protocol), EAP(Extensible Authentication Protocol) 등을 사용한 인증

2. 가입자 정보 위 · 변조

가. 위협개요

공격자가 음성통화, 방송, 금융거래 등의 불법적인 서비스를 사용 또는 가입자 정보 훼손을 위해 서비스 제공장비 해킹을 통해 관리하는 가입자 정보를 위조 또는 변조하는 위협이다.

나. 보호대상

• 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 가입자 정보를 관리 또는 저장하는 서버

다. 보호대책

• 연동장비에 대한 해킹 차단

- 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 가입자 정보를 관리 또는 저장하는 서버에 대한 해킹 차단

※ '제4절 시스템 해킹'의 대책에 따라 조치

• 연동장비의 IP 주소, 포트 등에 대한 접근제한

- 소프트스위치, SIP 서버, 방송센터의 가입자 관리서버 등 가입자 정보를 관리 또는 저장하는 서버에 대한 비인가자의 IP 주소, 포트 등에 대한 접근제한

※ '제5절 도청'의 '1. 시스템 해킹을 통한 도청'의 '연동장비의 IP 주소, 포트 등에 대한 접근제한'과 동일하게 조치

• 서비스 제공과 가입자 정보 관리간 기능영역 분리 운영

- 소프트스위치, SIP 서버, 방송센터 등의 사용자 접속 서버와 가입자 정보를 저장 · 관리

하는 Database 서버를 분리하여 운영

※ 이를 통해, 공격자가 서비스 제공장비를 해킹에 성공한 이후에 가입자 정보 위·변조 행위를 제한

■서비스 제공과 가입자 정보 관리간 기능영역 분리 예제

- 서비스 제공장비(소프트스위치, SIP 서버, 방송 서버 등)와 가입자 정보를 저장·관리하는 Database 서버는 개별시스템에서 별도로 운영
  - 가입자 정보를 저장·관리하는 Database 서버는 사설망 등에 위치시키고 서비스 제공장비와 Dedicated 회선을 이용해 상호인증 및 암호화 메커니즘을 사용하여 연결
- 동일한 시스템에 서비스 제공기능과 가입자 정보 관리기능이 존재하는 경우, 보안운영체제(Secure OS) 등을 사용하여 서비스 기능에 따라 접근 가능한 영역을 분리 운영

- 가입자 정보 저장데이터에 대한 무결성 검사
  - 가입자 정보의 위·변조 여부를 확인할 수 있도록 Database 등에 대한 무결성 값을 생성(예: 암호키와 HASH 알고리즘을 사용하여 무결성값 생성) 하고 주기적으로 검사
- 가입자 정보 보호를 위한 관련 법규, 지침 및 절차 등의 준수
  - 개인정보의 경우, '개인정보보호지침' 및 동 해설서를 참조하여 가입자 정보를 관리

    ※ 개인정보보호지침해설서: http://www.kisa.or.kr/kisa/privacy/down/law_4_14.pdf 참조
  - 위치정보의 경우, '위치정보의 보호 및 이용 등에 관한 법률 해설서' 등을 참조하여 가입자 정보를 관리

    ※ 위치정보의 보호 및 이용 등에 관한 법률 해설서: http://jeju.koreapost.go.kr/ n_post/bbs/download.jsp·mask=1151621329986 참조

3. 세션 연결 메시지 위·변조

가. 위협개요

공격자가 음성통화, 방송 서비스 등 진행중인 BcN 서비스 세션에 개입하여 정상 사용자 시스템에 대한 스푸핑 등을 통해 사용자의 음성통화 및 방송 컨텐츠 등의 미디어 메시지, 금융거래 및 사용자 인증정보 등의 사용자 메시지를 위·변조하는 위협이다.

나. 보호대상

• 소프트스위치, SIP 서버, 방송센터 서버, 시그널링 및 미디어 게이트웨이, DNS 서버, DHCP 서버 등 서비스를 제공하는 서버

다. 보호대책

세션 연결 메시지 위·변조에 대한 대책은 공격방식이 세션 가로채기를 통한 도청과 동일하므로, '제4절 도청'의 '3. 세션 가로채기'의 대책과 동일하게 적용한다.

• 메시지 무결성 검증 가능한 서비스 프로토콜 사용
• 제어 데이터, 미디어 및 사용자 데이터 암호화
• 세션 가로채기 방지 네트워크 환경 구성
• 스니핑 및 과도 트래픽 유발 시스템 모니터링 및 조치

4. 라우팅 메시지 위·변조

가. 위협개요

공격자가 라우터 해킹 등을 통해 라우팅 테이블을 조작하여 특정 네트워크 마비, 데이터 전송 경로 변경, 서비스 방해 등을 초래하는 위협이다.

나. 보호대상

• 라우팅 기능을 제공하는 일반 라우터, MPLS 라우터

다. 보호대책

• 라우터에 대한 해킹 차단

※ '제4절 시스템 해킹'의 대책에 따라 조치

■라우터 보안을 위한 참조자료

• 라우터 보안관리 가이드

http://www.kisa.or.kr/ → 정보통신기반보호 → 자료실 → 라우터보안관리가이드.zip

• 라우터를 활용한 네트워크 보안설정
  http://www.sis.or.kr/se/pdf2005/200505security_router.pdf
• Cisco IOS Security
  http://www.cisco.com/global/kr → 제품&솔루션(라우터&라우팅 시스템) → Cisco IOS Security
• 주니퍼 네트웍스 보안센터
  http://www.juniper.net/support/security

• 라우터의 보안기능 활성화
– 위 · 변조된 라우팅 테이블에 기반한 잘못된 라우팅 방지를 위한 보안기능(예: 소스 라우팅 차단, uRPF)을 활성화
• 라우터에 접근하는 IP 주소, 포트 등에 대한 접근제한
※ '제5절 도청'의 '1. 시스템 해킹을 통한 도청'의 '연동장비의 IP 주소, 포트 등에 대한 접근제한'과 동일하게 조치
• 라우터 내의 비인가 프로세스 제거
※ '제5절 도청'의 '1. 시스템 해킹을 통한 도청'의 '비인가 프로세스 제거'와 동일하게 조치
• 라우팅 테이블에 대한 무결성 검사
– 라우팅 테이블 변경여부를 확인할 수 있도록 무결성 메커니즘을 적용하여 테이블을 저장하고, 주기적으로 테이블의 비인가된 변경여부 검사

제 6 장 안전한 BcN 구축을 위한 전략

제5장에서는 BcN에서 당면하고 있는 각각의 위협들에 대한 보호대책을 제시하였다. 이렇게 제시된 보호대책은 기술적, 관리적, 정책적인 대책을 포함하고는 있으나, BcN 전체 망 통합과 연동을 고려하여 이러한 대책들이 종합적이며 지속적 · 체계적으로 유지되기 위해서는 다음과 같은 또 다른 접근들이 필요하다.

제1절 사업자간 정보보호 수준의 일관성 유지

가. 필요성

VoIP 등과 같이 서비스가 여러 사업자를 경유하는 경우 사업자마다 적용하는 보안정책과 수준이 다를 수 있으며, 이 경우 서비스 보안수준은 가장 취약한 부분의 보안수준에 의존하게 된다. 이는 여러 사업자중 어느 한 사업자가 보안수준을 높이더라도 약한 보안을 적용하는 사업자에 의해 종단(End-to-End)간에서 해당 서비스가 의도하는 보안수준 유지가 어려울 수 있음을 의미한다.

나. 대응방안

- BcN 인프라, 서비스 보호를 위한 지침, 가이드라인, 규정 등을 전체 BcN 사업자가 공통적으로 준수

  ※ 예: 전체 사업자가 'BcN 정보보호 가이드', 'VoIP 정보보호 가이드라인' 등을 준수하여 동일하게 조치

- 인프라 및 서비스 연동시 정보보호를 위한 정책, 기술 등의 세부규격에 대한 사업자간 표준화 또는 합의된 규격을 작성하고, 정기적으로 합의된 규격에 대해 사업자 공동 점검

- 사업자간 연동되는 서비스의 경우 정보보호 침해사고에 따르는 역할, 법적인 책임 및 의무 관계 등을 명확히 정의 및 적용

제2절 지속적 · 체계적 정보보호를 위한 법 · 제도 활용

사업자는 BcN 환경의 정보보호를 위해 자체적으로 많은 비용과 노력을 기울이고 있으나, 국가에서 제공하고 있는 관련 법 · 제도, 정책 등을 활용할 경우 보다 지속적 · 체계적이며 비용 효과적인 정보보호를 수행할 수 있다.

1. 정보보호시스템 평가 · 인증 제도

가. 개요

정보보호시스템 평가 · 인증 제도는 국제적으로 인정되는 보안성 평가기준인 공통평가기준(CC: Common Criteria)과 및 평가방법론(CEM: Common Evaluation Methodology)에 의해 IT 제품의 안전 · 신뢰성을 검증하는 보안성 평가제도이다.

나. 필요성

BcN 사업자는 BcN 인프라 구축 및 서비스 장비 도입시, 자체적인 보호대책 강구에 소요되는 비용투자를 최소화 하기 위해 국제적인 기준과 방법에 의해 해당 장비의 보안성이 검증된 제품을 도입함으로써 이러한 노력을 최소화 할 수 있다.

※ 정보시스템의 정보보호 취약성 수정에 소요되는 비용은 설계단계를 기준으로 구현단계는 6.5배, 테스트 단계는 15배, 운영단계에서는 60~100배가 증가 (출처: IBM)

다. 주요내용

보안성 평가는 네트워크 정보보호 제품군, 정보보호 기반제품군 및 컴퓨팅 정보보호 제품군에 속한 다양한 정보보호제품의 안전. 신뢰성을 공통평가기준(CC)와 공통평가기준 평가방법론(CEM)에 의해 평가하여 보안성을 평가한다. 제품의 전체 윤곽인 보안목표명세서(ST), 설계내용, 기능동작, 동작시험, 취약성 분석 및 시험, 개발과정관리, 제품 설명서 등에 대해 평가를 수행한다. EAL(Evaluation Assurance Level) 1 ~ 7까지의 평가등급을 두고 있으며 EAL7 등급으로 갈수록 제공하는 기능에 대해 더 높은 보증수준을 요구한다.

■보증수준별 평가방법

- EAL1 : 기능시험
- EAL2 : 구조시험
- EAL3 : 방법론적 시험과 점검
- EAL4 : 방법론적 설계, 시험 및 검토
- EAL5 ~7 : 준정형적 설계 및 시험, 정형적 검증

※ 국제적으로 인정되는 등급은 EAL4까지임

■참조 사이트

- 보안성 평가에 대한 상세한 내용은 한국정보보호진흥원 보안성평가센터 (http://www.kisa.or.kr/→ 보안성평가)를 참조

라. 활용방법

CC기반의 보안성을 획득한 제품은 보안목표명세서(ST: Security Target)를 통해 제품의 기능 및 보안기능, 보증수준 등을 제시하므로 사업자는 이를 참조하여 BcN 환경 구축시 자신의 환경에 맞는 제품을 선택하여 사용할 수 있다.

또한 사업자는 필요시 자신의 환경에 맞는 보증수준, 보안기능 등을 요구하는 보호프로파일(PP: Protection Profile)을 개발하여, 개발자로 하여금 이에 따라 평가등급을 획득한 제품들만 납품하도록 요청할 수도 있다.

2. 주요정보통신기반시설 지정 제도

가. 개요

주요정보통신기반시설 지정 제도는 국가 주요정보통신기반시설을 해킹 등의 침해사고 위협으로부터 보호할 수 있도록 정기적으로 취약점 분석·평가, 보호대책 수립 등을 통해 기반시설의 안정적인 운영 도모하는 제도이다.

나. 필요성

BcN은 다양한 사업자, 이기종 망들을 경유하여 대규모의 가입자들에 대한 서비스를 제공하므로 침해사고 발생시 사업자 독자적인 대응이 어려울뿐 아니라 그 악영향에 대한 파급효과 또한 매우 크다. 이를 방지하기 위해 자체적인 정보보호 대책 운영 · 관리 소홀에 따른 문제점을 보완하고, 침해사고 발생시 국가차원의 지원을 받기 위해서는 주요정보통신기반시설 지정 제도를 활용하는 것도 하나의 대책이 될 수 있다.

다. 주요내용

주요정보통신기반시설 지정 제도에서는 기반시설의 안정적 운영을 위해 동 시설에 내장된 중요 정보에 대해 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협요인을 파악하고, 취약성 평가방법론을 통해 침해시 파급효과 및 대책을 식별 · 분석 · 평가하고 보호계획을 수립하게 된다.

이러한 과정은 정보보호컨설팅전문업체, 한국정보보호진흥원, 정보공유분석센터 등의 정보보호 전문기관을 통해 수행하며, 취약점 분석 · 평가를 수행을 통해 수립된 보호계획은 국무총리산하의 기반보호위원회에 보고하여 관리 · 감독을 받는다.

라. 활용방법

주요정보통신기반시설 지정은 중앙행정기관의 장이 지정하며, 동 기관의 장이 소관분야의 정보통신기반시설중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정한다.

사업자가 자체적으로 BcN 중요 서비스 시설에 대해 주요정보통신기반시설로 지정할 수는 없으나, 이에 대한 이슈는 한국정보보호진흥원을 통해 제기할 수 있다. 주요정보통신기반시설 지정을 위한 세부 내용, 절차 및 방법은 지원기관인 한국정보보호진흥원에 문의한다.

■주요정보통신기반시설 지정 제도 문의처

• 한국정보보호진흥원: Tel:02-405-5555, 이메일: ciip@kisa.or.kr

■주요정보통신기반시설 지정 제도 참조 사이트

• 한국정보보호진흥원 (http://www.kisa.or.kr/→ 정보통신기반보호) 참조

마. 유사제도

주요정보통신기반시설 지정 제도와 비슷하게 법에 기반을 두고 운영되는 제도로 정보보호 안전진단 제도가 있다. 동 제도는 주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 관리적 · 기술적 · 물리적 정보보호지침(안전진단기준)를 이행하고, 안전진단수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다.

■정보보호안전진단 제도 문의처

• 한국정보보호진흥원: Tel:02-405-5233, 이메일: securitycheck@kisa.or.kr

■정보보호안전진단 제도 참조 사이트

• 한국정보보호진흥원 (http://www.kisa.or.kr/ → 정보보호안전진단지원) 참조

3. 정보보호관리체계(ISMS) 인증

가. 개요

정보보호관리체계(ISMS: Information Security Management System) 인증제도는 ISO 9001(품질경영시스템)과 같이 품질 보증을 위한 기업 내 일련의 활동에 대한 인증과 유사한 개념으로, 정보보호를 위한 기업 내의 일련의 활동들에 대해 제3자의 인증기관(한국정보보호진흥원)이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도이다. 이와 유사한 인증체계로는 BS7799 등이 있다.

나. 필요성

다양한 사업자, 이기종 망이 통합되는 BcN 특성상 일회성, 단편적, 부분적 정보보호는 침해사고의 가능성을 매우 높게 만들 수 있으므로 사업자는 전반적인 정보보호 활동 평가를 통해 종합적, 체계적, 지속적인 정보보호 수행이 필요하다. 정보보호관리체계 인증은 사업자의 이러한 노력을 지원하며, 이를 통해 기업의 대 고객 신뢰제고, 정보통신망의 안전성 강화 및 정보보호관리능력 향상을 이룰 수 있다.

다. 주요내용

정보보호관리체계 인증은 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리 절차와 과정이 체계적으로 수립、문서화되고 정보보호 대책들이 유기적으로 통합되어 있는지를 평가한다. 심사 기준은 정보통신부 고시(제2002-32호)에 의해 필수사항인 관리과정 14개 항목, 문서화 요구사항 3개 항목과 선택사항인 정보보호대책 120개 항목 등 총 137개 항목으로 구성되어 있다.

정보보호관리체계 인증은 사업자의 필요에 따라 자율적으로 신청하여 인증을 획득할 수 있으며 강제사항이 아니다.

라. 활용방법

사업자는 조직의 보안강화를 위해 자체적인 필요에 따라 정보보호관리체계 인증을 신청할 수 있다. 정보보호관리체계 인증 신청을 위해서는 신청서 양식을 작성하여 한국정보보호진흥원에 신청한다.

■문의처

- 한국정보보호진흥원: Tel:02-405-5547
- 한국정보보호진흥원 (http://www.kisa.or.kr/→ 정보보호관리체계인증) 참조

제3절 BcN 구축단계를 고려한 정보보호

1. BcN 서비스의 안전성 사전검증

가. 필요성

대부분의 위험관리 방법론이 정보시스템 구축 이후에 보호대책을 수립하도록 구성되어 있어 정보보호의 비용 효과성 및 서비스 안전 · 신뢰성 확보에 제한이 있다. BcN 기반의 서비스는 다양한 사업자, 망을 경유하여 대규모 사용자에게 영향을 미치므로 서비스 개시후 침해사고 발생시 시스템 복구, 타 사업자 및 사용자와의 법적분쟁 등에 따르는 비용 손실, 고객의 신뢰 상실 등의 커다란 문제점에 직면하게 될 수 있다. 따라서 사후조치에 다른 비용손실을 최소화 하기위해 서비스 개시전에 미리 서비스의 안전성 확보가 필요하다.

나. 추진방법

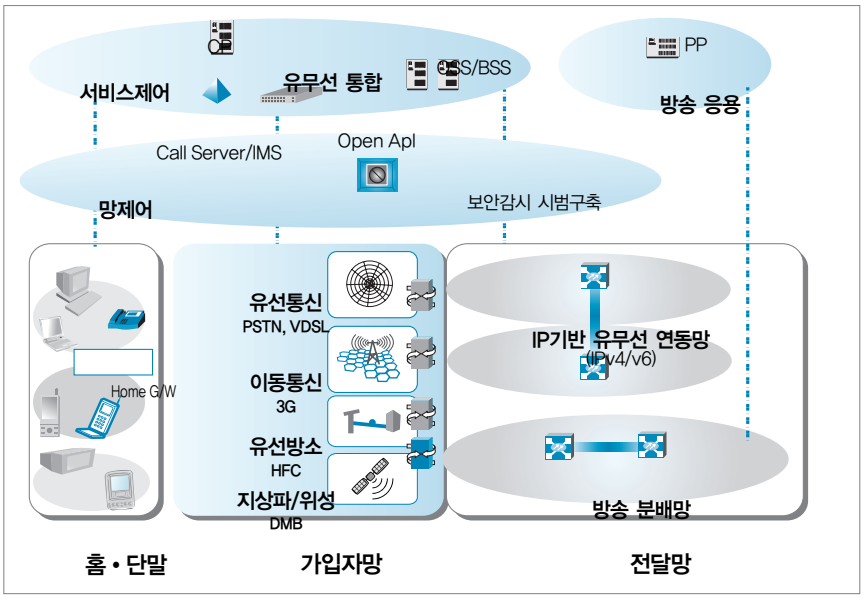
신규 서비스 개발 후, 서비스 아키텍쳐 및 운영환경 분석, 위험분석, 취약성 평가 등을 통해 해당 서비스에 대한 보호대책을 구현하고 이에 대해 검증한다.

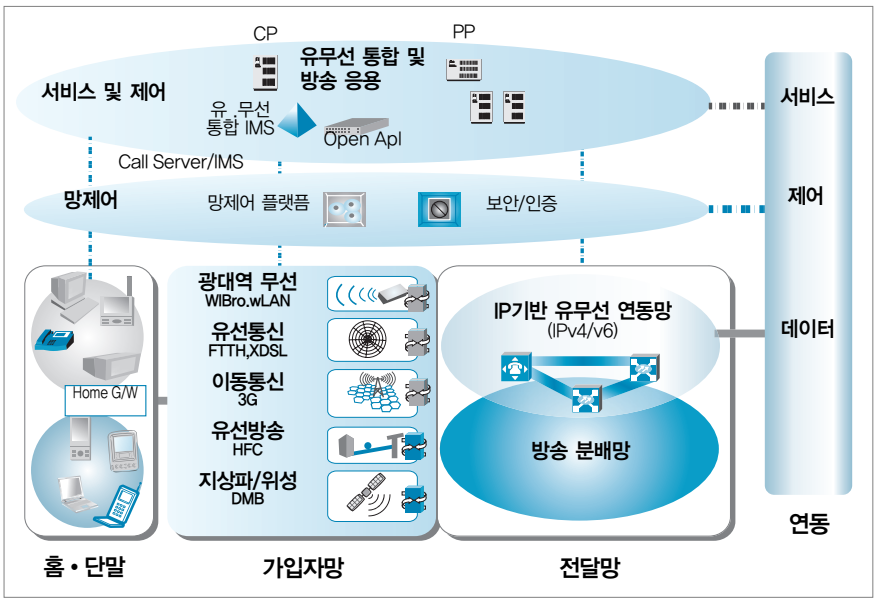
※ 한국정보보호진흥원에서 서비스 사전평가에 활용할 수 있는 'IT서비스 정보보호 사전진단 방법론'에 대해 국내 표준화를 추진중에 있음

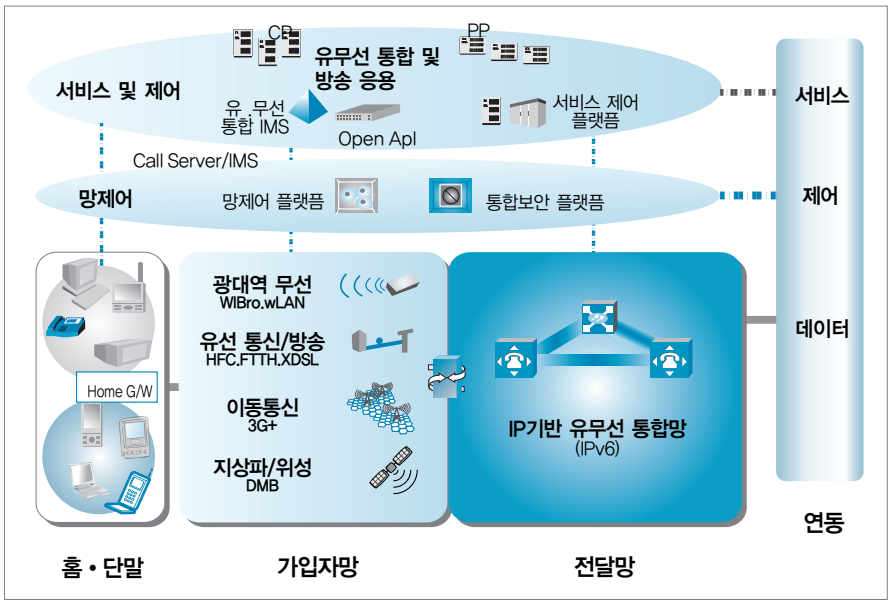
2. 망 구축 단계별 정보보호

가. BcN 망 구축단계별 주요 차이점

[표 6-1] BcN 망 구축단계별 주요 차이점

	1단계 ('04년~'05년)
목표	유 · 무선 연동 및 통신 · 방송 서비스 기반 구축
망 개념도	
주요	• 유 · 무선 연동 – 가입자망의 개별적 존재 • VoIP, 영상전화 등의 통신 · 방송 초기 통합 서비스 제공 • 전달망의 QoS기능(IP–DiffServ, MPLS– DiffServ) 시범도입 • 유 · 무선망별 Open API G/W 도입

	1단계 ('06년~'07년)
목표	유 · 무선 통합 및 통신 · 방송 통합 서비스 제공
망 개념도	
주요	• 유 · 무선 통합 – 유비쿼터스 센서 네트워크 도입 • IPTV, u-Work 및 통신 · 방송 통합 서비스 본격 제공 • BcN Core 망 및 MPLS 적용 확대, 50~ 100Mbps급 서비스 제공을 위한 망 고도화 • 웹 서비스 기반의 유 · 무선 통합 Open API G/W 도입

	3단계 ('08년~'10년)
목표	광대역 통신 · 방송 · 인터넷 통합망 완성
망 개념도	
주요	• 광대역 통합망 완성 – 통신/방송/인터넷 전달망 통합 및 IPv4/IPv6 전면지원 • 고품질 영상전화, HD급 품질보장형 멀티미디어 서비스 제공 • 유 · 무선 간 주요 서비스의 End-to-End QoS 보장 • 통신 · 방송 통합 Open API G/W 도입

※ 참조: BcN 구축 기본계획 II

나. 보안 위협의 예상변화

BcN 망 구축단계별 주요 차이점을 고려할 때, 주요 보안 위협은 다음과 같은 방향으로 중요하게 부각될 것으로 예상된다.

[표 6-2] 보안 위협의 예상변화

	1단계 ('04~'05년)	2단계 ('06~'07년)	3단계 ('08~'10년)
주요 위협 변화	• BcN 개별망에 대한 위협 – 유선인터넷, 유선방송망, WCDMA 등 망 자체의 취약점 악용 • BcN 인프라에 대한 위협 – SSW, 방송서버 등에서 IPv4, OS 등에 대한 전통적인 취약점 악용 ※ DoS, DDoS, 해킹 등 • BcN 연동구간에 대한 위협 – Access GW, Open API GW 등에 대한 프로토콜 및 OS의 전통적인 취약점 악용	• 통합망 기반 신규 서비스에 대한 위협 – VoIP, IPTV, u-Work 등에 대한 취약점 악용 • 전송망에서 품질 보장에 대한 위협 • 망 통합, 고속화에 따른 침해사고 확산 위협 • 신규 가입자망, 단말에 대한 위협 – BcN에 통합되는 RFID/USN, 다양한 단말의 취약점 악용 및 이를 통한 확산	• All-IP 통합망 생존성 보장에 대한 위협 – IPv6 프로토콜, 망구성 요소 등에 대한 취약점 악용 및 단일화된 IP에 기인한 급속한 침해확산 • 다양한 서비스의 품질 보장에 대한 위협 – 종단(End-toEnd)간 품질보장 프로토콜, 기술 등의 취약점 악용 • 다양한 서비스를 사용하는 대규모 사용자의 개인정보 침해에 대한 위협

※ 2단계는 1단계를 포함하고, 3단계는 2단계를 포함

다. 보안대책 고려사항

• 1단계 보안대책

– BcN 개별망(유선인터넷, 유선 방송망, WiBro, WCDMA, 등) 및 서비스 단말의 위협에 대한 보호대책 수립 · 운영

– BcN 주요 서비스 장비(SSW, 방송서버 등)와 연동장비(Signaling 및 Media GW, Open API GW 등)의 위협에 대한 보호대책 수립 · 운영

• 2단계 보안대책

– BcN 인프라 및 네트워크에 대한 통합보안관리 및 위험수준에 따른 망 분리 대책 운영

– 서비스/제어망, 전달망에서 유해 트래픽을 실시간으로 감시하고 차단할 수 있는 수준의 고성능 보안시스템 구축

– 신규 서비스 개발시, 상용화전 사전평가를 통해 안전성 검증

– 신규 가입자망(USN 등) 및 서비스 단말의 위협에 대한 보호대책 수립 · 운영

※ 1단계 보안대책을 포함

• 3단계 보안대책

– 사업자간 침해사고 통합 모니터링 및 대응을 위한 체계 구축 · 운영

– IPv6기반 인프라 및 네트워크에 대한 대책 수립 · 운영

– 서비스/제어망, 전달망 및 가입자망에서 유해 트래픽을 실시간으로 감시하고 차단할 수 있는 수준의 고성능 보안시스템 구축

– 통신, 방송, 신규서비스(USN, RFID, 홈네트워크 등)에 대한 통합보안관리 시스템 및 통합인증 체계 구축

– 개인정보보호 처리 · 저장 · 관리 등의 시스템(사용자 Database 등)에 대한 강화된 보호대책 수립 · 운영

– 능동적으로 위험요소를 찾아 차단 및 추적할 수 있는 네트워크 기술 운영 및 보안시스템 구축

※ 2단계 보안대책을 포함

제7장 결 론

BcN 정보보호를 위해 본 가이드에서는 BcN 연동구간을 중심으로 발생 가능한 서비스 거부, 품질저하, 해킹, 도청 등의 보안 위협을 분석하고, 이에 대한 기술적 보호대책과 정책적 정보보호 권고사항들을 제시하였다.

특히, 가이드의 제3장에서 제시하고 있는 BcN 아키텍처와 연동구간은 BcN 사업자가 추진하고 있는 시범사업의 BcN 망을 반영하여 구성하였고, 제3장의 BcN 정보보호 대상 선정과 제4장의 BcN 연동구간에서 발생 가능한 보안 위협의 도출, 제5장에서 제시한 각 위협에 대한 보호대책과 [부록3]에서 제시하고 있는 주요장비별 정보보호 체크리스트 등은 BcN 사업자와 유관기관, 정보보호 업체 등으로 이루어진 "BcN 정보보호 연구반"을 통해서 도출된 결과이다.

본 가이드는 BcN 연동구간 인프라를 중심으로 발생 가능한 위협을 도출하고 이에 대한 보호대책을 제시하고 있다. 그러나 새로이 개발되는 신규 BcN 서비스 등에 대한 보호대책을 제시하기에는 부족한 면이 있다. 하지만, 음성 · 데이터 · 영상 · 멀티미디어 등 다양한 형태의 정보가 이기종의 가입자 망을 경유하여 광대역으로 통합 서비스되는 BcN 환경에서 BcN 인프라에 대한 보호는 서비스의 안전성 확보를 위한 우선적인 필수 조건이다. 따라서 정보보호 대책을 제시하고 있는 본 가이드는 안전한 BcN 환경을 구축하기 위한 선행조건으로 매우 큰 의미가 있다.

향후, 본 가이드가 좀더 실효성을 확보하기 위해서는 새로이 도입되는 BcN 서비스에 대한 정보보호 대책들이 추가되고, BcN망 구축의 진행과 더불어 새로이 개발되는 인프라 장비에 대한 대책 및 정보보호 체크리스트의 추가 개발이 지속적으로 진행되어야 한다.

참고문헌

[1] BcN 구축 기본계획 II(안), 정보통신부, 2006.3

[2] BcN 표준모델, TTA, 2005. 12. 21

[3] BcN 정보보호 기술개발 현황, 한국인터넷정보학회, 2005. 9

[4] BcN 인프라 정보보호, 정보보호학회, 2005. 6

[5] u-KOREA 기본계획(2006~2010)(안), 정보통신부, 2006. 3

[6] BcN 정보보호 기술개발 현황, ETRI, 2005. 9

[7] IT839 8대 서비스의 공통보안 프레임워크 연구, KISA, 2005. 10

[8] 광대역 통합 네트워크 서비스, 전자신문사, 2006. 3

[9] 인터넷 전화, 전자신문사, 2004. 9

[10] BcN 정보보호프레임워크 개발, KISA, 2005. 12

[11] IPTV 보안기술, 디지캡 보안기술연구소 오성흔, 2006. 6

[12] IPTV 서비스 기술, TTA Journal no. 104, 2006. 4

[13] 인터넷망 기반 IPTV 기술, KT, 2005. 11

[14] VoIP 서비스 개요, www.lsfurion.com, 2006. 4

[15] 인터넷전화(VoIP) 구축시 보안 고려사항(SP 800-58), NIST, 2005. 1

[16] Telecommunication System Engineering, Roger L. Freeman, Wiley-Interscience

[17] VoIP Security and Privacy Threat Taxonomy, VoIPSA, 2005. 10

[18] IP TELEPHONY & VOICE OVER PROTOCOL
(SECURITY TECHNICAL IMPLEMENTATION) Version 2, Release 0, DISA, 2004. 12

[19] Next Generation Networks and Security an Introduction, voipsecurity.org, 2005. 4

[20] TISPAN NGN Security (NGN_SEC) Requirements NGN Release 1
(draft ETSI TS 187 001), 2005. 10

[21] 남기성, "광대역통합전달망 제어기술", http://anf.ne.kr/events/manw2004/ data/nam8.pdf

[22] 정일영, "BcN 서비스 방향", http://kidbs.itfind.or.kr/WZIN/jugidong/1159/115903.htm

[23] ITU-T FGNGN, http://www.itu.int/ITU-T/ngn/fgngn/

[24] Parlay Group, http://www.parlay.org

[25] 한국정보통신기술협회, http://www.tta.or.kr

[26] European Telecommunications Standard Institute, http://www.etsi.org

[27] 한국정보보호진흥원, http://www.kisa.or.kr

[28] 한국정보사회진흥원 BcN, http://www.bcn.ne.kr

[29] BcN 포럼, http://www.bcnforum.or.kr

[30] VoIP Security Alliance, http://www.voipsa.org

[31] GoDaddy.com, http://www.vopsecurity.org

[32] The SANS™ Institute, http://www.sans.org

[33] National Vulnerability Database, NIST, http://nvd.nist.gov

[34] 인터넷침해사고대응지원센터, http://www.krcert.or.kr

[35] VoicePulse Inc., https://connect.voicepulse.com

[36] NuFone Inc., http://www.nufone.net

[37] EnderUNIX project, http://www.enderunix.org/voipong/

[38] Open Communications Architecture Forum (OCAF) Focus Group, http://www.itu.int/[38] ITU-T/ocaf/index.html

[39] The Session Initiation Protocol (SIP) : http://www.cs.columbia.edu/ ~hgs/ teaching/ais/slides/sip_long.pdf

[40] SIP and the new network communications model : http://www.webtorials. com/main/resource/papers/nortel/paper19.htm

[41] Cisco Systems Inc., http://www.cisco.com

[42] Juniper Networks, http://www.juniper.net/

[43] 3Com Corporation, http://www.3com.com

[44] Ethereal Inc., http://www.ethereal.com

[45] Packetwatch Research, http://www.packetwatch.net

[46] C. Kaufman, R. Perlman and B. Sommerfeld, "DoS Protection for UDP- Based Protocols,"Conf. on Computer and Comm. Security, Proc. of the 10th ACM Conf. on Computer and Comm.security, Washington DC, 2003, pp. 2-7.

[47] "Advanced Networking Management Lab (ANML) Distributed Denial of ServiceAttacks(DDoS) Resources," Pervasive technology labs, Indiana Univ., 2001; http://www.anml.iu.edu/ddos/types.html

[48] SiVuS User Guide, VoIP Security Forum, 2004; http://vopsecurity. org/index.php · module=dpDocs&func=display&mid=4

약 어

A

AAA	Authentication, Authorization, and Accounting
AAP	Alternative Approval Process
ACIF	Australian Construction Industry Forum
ACK	Acknowledge
ACL	Access Control List
ACR	Access Control Router
AN	Access Node
AON	Active Optical Network
ARP	Address Resolution Protocol
ATIS	Alliance for telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode

B

BcN	Broadband Convergence Network
BS7799	British Standard 7799
BSS	Business Support System

C

CC	Common Ceteria
CCS	Common Channel Signaling
CDR	Call Detail Record
CEM	Common Evaluation Methodology
CEO	Chief Executive Officer
CM	Cable Modem
CMTS	Cable Modem Termination System
CP	Contents Provider
CPE	Customer Premises Equipment
CSS	Cascading Style Sheets
CTO	Chief Technology Officer

D

DB	Database
DDoS	Distributed Denial of Service
DECT	Digital European Cordless Telephone
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DMB	Digital Multimedia Broadcasting
DMC	Digital Media Center
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSG	Digital Settop Gateway
DTV	Digital TeleVision
DVB	Digital Video Broadcasting
DWDM	Dense Wavelength Division Multiplexer

E
F
G
H
I

EAL	Evaluation Assurance Level
EMS	Element Management System
ETSI	European Telecommunications Standard Institute
FTTH	Fiber To The Home
GGSN	Gateway GPRS Supporting Node
GSM	Global System for Mobile communication
GW	Gateway
HDTV	High Definition TeleVision
HFC	Hybrid Fiber Coaxial
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	The Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IOS	Internetwork Operating System
IP	Internet Protocol
IPTV	Internet Protocol TV
IPv6	Internet Protocol version 6
ISDN	Integrate Service Digital Network
ISP	Internet Service Provider
IT	Information Technology
ITU-T	International Telecommunications Union Telecommunication Standardization Sector
IWF	Interworking Function

K
L
M

KISA	Korea Information Security Agency
LAN	Local Area Network
LDP	Label Distribution Protocol
LSR	Label Switch Router
M3UA	MTP3 Adaption Layer
MAC	Meduim Access Control
Megaco	Media Gateway Control
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MMoIP	Multimedia Mail over Internet Protocol

약어

N

MoD	Music on Demand
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part
NAT	Network Address Translation
NAT-PT	Network Address Translation - Protocol Translation
NCP	Network Control Protocol
NGN	Next Generation Network
N-RFID	Networked Radio Frequency ID

O

OAM&P	Operation, Adminstration, Maintenance and Provisioning
ODR	Original Dependent Routing
Open API	Open Application Programming Interface
OSS	Operation Support System

P

PG	Project Group
PLC	Power Line Communication
PON	Passive Optical Network
PP	Protection Profile
PSS	Potable Subscriber System
PSTN	Public Switched Telephone Network

Q

QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
QSS	Quality Security Service

R

RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RFC	Request For Comments
RFID	Radio Frequency Identification
RGW	Residential Gateway
RIB	Routing Inforation Base
RNC	Radio Network Controller
RR	Resource Record
RSVP	Resource Reservation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-Time Transport Protocol

S

SCN	Switched Circuit Network
SCTP	Stream Control Transport Protocol
SDP	Session Description Protocol
SEN	Service Edge Node

SG	Signaling Gateway
SGSN	Serving GPRS Supporting Node
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Network
SS7	Signaling System 7
SSW	SoftSwitch
ST	Security Target
STP	Signaling Transfer Point
SYN	Synchronous

T

TAP	Traditional Approval Process
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TDR	Time Dependent Routing
TFTP	Trivial File Transfer Protocol
TG	Trunk Gateway
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TPS	Triple Play Service
TSACC	Telecommunications Standards Advisory Council of Canada
TTA	Telecommunication Technology Association

U

UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource locators
uRPF	unicast Reverse Path Forwarding

V

VoCM	Voice over Cable Modem
VDSL	Very high speed Digital Subscriber Line
VoD	Video on Demand
VoIP	Voice of IP

W

WCDMA	Wideband Code Division Multiple Access
WDM-PON	Wavelength Division Multiplexer Passive Optical Network
WiBro	Wireless Broadband
WLAN	Wireless Local Area Network

Z

ZBPMS	Zone Based Personalized Multimedia Service

용어설명

AAA(Authentication, Authorization, and Accounting)

인증, 권한부여, 과금, 인증이란 어떤 사람이나 사물이 실제로 신고된 바로 그사람(또는 바로 그것)인지를 판단하는 과정이다. 개별 또는 인터넷을 포함한 공공 네트워크에서의 인증은 대개 로그온시 암호의 사용을 통해 이루어진다.

AGW(Access Gateway)

일반전화, xDSL, 전용회선 등 다양한 가입자 서비스를 단일 플랫폼에 수용하는 통합 액세스 장비이다. 소프트스위치와 연동하여 음성 패킷 트래픽을 패킷망으로 전달하는 기능을 제공하며, 패킷 기반의 신규 가입자 수용을 위한 확장성을 보장하고 기존 운용 관리 시스템과 연동하며, 기존 서비스를 QoS가 보장된 형태로 제공한다. 엑세스 게이트웨이의 호/연결 제어는 소프트스위치가 담당한다.

BcN (Broadband Convergence Network)

광대역 통합망으로 통신、방송、인터넷이 통합된 품질 보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김없이 광대역으로 이용할 수 있는 차세대 통합 네트워크이다.

CDR(Call Detail Record)

호 상세 레코드는 전화 서비스에 대해 과금할 목적으로, 특정 내선번호나 가입자 그룹에 대한 통화 내역 데이터를 수집하고 기록하는 서비스 기능이다.

DHCP(Dynamic Host Configuration Protocol)

네트워크 관리자들이 조직 내의 네트워크 상에서 IP 주소를 중앙에서 관리하고 할당해 줄 수 있도록 해주는 프로토콜이다. DHCP는 주어진 IP 주소가 일정한 시간 동안만 그 컴퓨터에 유효하도록 하는 "임대" 개념을 사용한다.

FTTH(Fiber To The Home)

영상 전송 등 각종 멀티미디어 서비스를 실현하기 위해 데이터 센터에서 각 가정까지 광케이블을 연결하는 네트워크 형태이다.

GK(GateKeeper)

게이트 키퍼는 H.323를 이용한 화상회의에서 사용자의 이름을 물리적인 주소로 바꾸어주는 서버이다. 이것은 호출 허가나 계정 정보를 제공하는데 사용되기도 한다.

HTTP(Hyper Text Transfer Protocol)

웹상에서 파일(텍스트, 그래픽 이미지, 사운드, 비디오 그리고 기타 멀티미디어 파일)을 주고 받는데 필요한 프로토콜로서 TCP/IP와 관련된 하나의 응용 프로토콜이다.

IP(Internet Protocol)

TCP/IP 스택에서 비연결성 연결 네트워크 서비스를 제공하는 네트워크 계층 프로토콜, IP는 주소지정, 서비스 타입 규격, 분해와 합성, 보안 등의 기능을 지니고 있다.

IPv6(Internet Protocol version 6)

현재 버전의 IP(버전4)를 대치하는 것으로 IPv6는 패킷 헤더 안에 플로우를 구분하는데 사용할 수 있는 플로우 ID를 넣을 수 있다. IPv6는 128비트(16비트)로써 IP할당이 가능하다.

ISDN(Integrate Service Digital Network)

다른 매체는 물론, 평범한 구리 전화선 위에서도 디지털 전송을 할 수 있게 하기 위한 일련의 CCITT/ITU 표준들이다. 모뎀대신에 ISDN 어댑터를 설치한 가정이나 회사의 사용자들은 최고 128Kbps까지의 데이터 서비스를 제공 받을 수 있다.

ISP(Internet Service Provider)
개인이나 회사들에게 인터넷 접속서비스, 웹사이트 건설 및 웹호스팅 서비스 등을 제공하는 회사들을 말한다.

MG(Media Gateway)
TDM 트래픽을 IP나 ATM 패킷으로 변환해 주는 장치로서, 액세스 게이트웨이와 트렁크 게이트웨이가 있다. 이 미디어 게이트웨이는 호제어를 위해 소프트스위치와 제어 프로토콜로 연동된다.

MPLS(Multi Protocol Label Switching)
MPLS는 주어진 패킷 열에 대하여 특정 경로를 설정하는 것에 관여하는데, 각 패킷 내에는 라벨이 있어서 라우터 입장에서는 그 패킷을 전달해야 할 노드의 주소를 보는데 소요되는 시간을 절약할 수 있다. MPLS는 멀티프로토콜이라 불리는데 IP, ATM 및 프레임 릴레이 네트워크 프로토콜 등과 함께 동작하기 때문이다. MPLS는 네트워크의 OSI 표준 참조모델과 관련하여, 3계층(라우팅)이 아닌, 스위칭을 하는 2계층에서 대부분의 패킷이 전달될 수 있게 한다.

NAT(Network Address Translation)
NAT는 외부 네트워크에 알려진 것과 다른 IP 주소를 사용하는 내부 네트워크에서, IP 주소를 변환하는 것이다. 일반적으로, 한회사는 자신의 내부 네트워크 주소를 하나 또는 그 이상의 공인 IP 주소로 사상한다. 그리고 들어오는 패킷들 상의 공인 IP 주소를 다시 사설 IP 주소로 변환한다. 이렇게 함으로써 나가거나 들어오는 각 요구들은 주소 변환 과정을 반드시 거쳐야 하기 때문에, 보안 문제를 확실하게 하는데 도움이 되며, 또한 요구를 제한하거나 인증하고, 또 이전의 요구와 일치시키는 기회를 제공한다. NAT는 또한 회사에서 필요한 공인 IP 주소의 수를 보존하며, 회사가 외부 네트워크와의 통신에서 단 하나의 공인 IP 주소를 사용할 수 있게 한다.

NGN(Next Generation Network)
회선망과 패킷망을 하나로 통합해 다양한 멀티미디어 서비스를 제공하는 차세대 네트워크이다.

Open API(Open Application Programming Interface)
사업자의 서비스 개발 및 실행을 위해 소프트스위치 및 OSA/Parlay 게이트웨이에서 제공하는 소프트웨어 플랫폼이다.

OSS(Operation Support System)
통신회사의 네트워크와 장비를 관리하기 위한 표준으로 각기 다른 통신회사간 장비의 연동과 호환성을 보장하는 역할도 담당한다. OSS는 TMN과 함께 네트워크 감시와 관리, 요금 청구, 네트워크 시험, QoS 감시, 장비 제고 파악, 콜 계정관리, 경고 등 다양한 기능을 처리한다.

PON(Passive Optical Network)
광케이블망을 통해 최종 사용자에게 신호를 전달하는 시스템이다. 이 시스템은 PON이 어느 위치에서 종단처리되느냐에 따라 FTTC, FTTB 또는 FTTH 등으로 나뉘어 진다.

PSTN(Public Switched Telephone Network)
전세계적으로 사용되는 다양한 전화 네트워크와 서비스를 가리키는 일반적인 용어이다.

QoS(Quality of Service)
전송 품질과 서비스 가용성을 알려주는 전송 시스템의 수행 성능 척도를 의미한다.

RAS(Remote Access Service)
원격접속서버는 원격지에서 네트워크에 접속을 원하는 사용자들을 관리하도록 설정된 컴퓨터와 관련 소프트웨어이다. 통신 서버라고도 불리는 원격접속서버는 보통 보안문제를 보장하기 위한 방화벽 서버, 원격접속 요구를 회사 네트워크의 다른 부분으로 전달하기 위한 라우터 등을 포함하거나 연계된다.

용어설명

RGW(Residential Gateway)
가입자 댁내 등에 위치하여 수용된 가입자 트래픽의 미디어 변환 기능을 수행하는 시스템이다. 레지덴셜 게이트웨이의 호/연결 제어는 소프트스위치가 담당한다.

RTP(Real-Time Transport Protocol)
오디오와 비디오와 같은 실시간 데이터를 전송하기 위한 인터넷 프로토콜이다. RTP 그자체가 데이터의 실시간 전송을 보장하지는 않지만, 송수신 응용 프로그램들이 스트리밍 데이터를 지원하기 위한 장치를 제공한다. RTP는 일반적으로 UDP 프로토콜 상에서 실행된다.

SG(Signaling Gateway)
PSTN의 No.7 신호를 소프트스위치가 처리할 수 있도록 메시지 변환 또는 프로토콜 변환 기능을 수행하는 시스템이다.

SIGTRAN(Signaling Transport)
SS7 엑세스 포인트와 소프트스위치(미디어 게이트웨이 콘트롤러)를 상호 연결하여 시그널링의 전달을 담당하며 이를 통해 소프트스위치(미디어 게이트웨이 콘트롤러)에서 ISUP 및 TCAP 등을 구현할 수 있게 한다.

SIP(Session Initiation Protocol)
SIP은 매우 간단한 텍스트 기반의 응용계층 제어 프로토콜로서, 하나 이상의 참가자들이 함께 세션을 만들고, 수정하고 종료할 수 있게 한다. 이러한 세션들에는 인터넷을 이용한 원격회의, 전화, 면회, 이벤트 통지, 인스턴트 메시징 등이 포함된다. SIP는 하위에 있는 패킷 프로토콜(TCP, UDP, ATM, X.25)에 독립적이다.

SNMP(Simple Network Management Network)
SNMP는 네트워크 관리 및 네트워크 장치에 대해 그들의 동작을 감시, 설정 등을 수행하는데 사용되는 프로토콜이다.

SSW(SoftSwitch)
소프트스위치는 패킷전달망에 접속, 단대단 통신을 위한 호 또는 세션제어를 담당하는 시스템이다. 단대단 통신제어를 위해서 표준화된 프로토콜 또는 API를 이용하여 통신망 계위 상으로 하부의 각종 게이트웨이 및 단말을 제어하고, 상위의 응용 서비스 제공 및 관리를 위한 응용 서버와 연동하며, 타 소프트스위치와 연동한다.

STP(Signaling Transfer Point)
SP간의 신호 트래픽만을 중계해 주는 패킷 스위치로서 SS7 메시지내의 라우팅 정보를 기반으로 수신메시지를 송신측으로 라우팅한다.

TCP(Transmission Control Protocol)
TCP는 인터넷 상의 컴퓨터들 사이에서 데이터를 메시지의 형태로 보내기 위해 IP와 함께 사용되는 프로토콜이다.

TDMA(Time Division Multiple Access)
하나의 통신회선이나 채널을 이용하여 송신하기 위해 다수의 신호들이 결합되는 방식으로서, 각 신호는 매우 짧은 지속시간을 갖는 여러 개의 세그먼트들로 나뉘어 진다.

TG(Trunk Gateway)
가입자망 시설정보, 고객 서비스 정보관리스시템, 즉 전화, ADSL Access Domain, FLC, ISDN 구성관리시스템으로서 주요기능은 고객 Service Order 분석, 고객에 적합한 장비 및 네트워크 자동 선정, 교환기 또는 가입자 망 장비 관리시스템(EMS)과 연동하여 망 자동 활성화 등의 기능이 있다.

TPS(Triple Play Service)

단일 사업자가 전화(음성), 초고속인터넷(데이터), 방송(영상)의 3가지 독립된 서비스들을 한데 묶어 고객에게 패키지 형태로 제공하는 결합 서비스의 일종을 말한다.

URL(Uniform Resource Locator)

인터넷에서 접근 가능한 자원의 주소를 일관되게 표현할 수 있는 형식을 말한다.

VDSL(Very high speed Digital Subscriber Line)

비교적 가까운 거리에서 더 빠른 속도를 보장하는 초고속 데이터 서비스 방식중의 하나이다(300m 정도의 길이에서 51~55Mbps 가량의 속도를 낸다).

VoD(Video on Demand)

개인들이 TV나 컴퓨터 화면을 통해 중앙의 서버로부터 비디오를 선택해 볼 수 있도록 하는 것을 공동의 목표로 삼고 있는 회사들과 관련된 일련의 기술들을 일컫는 광범위한 용어이다.

VoIP(Voice over IP)

IP를 사용하여 음성정보를 전달하는 일련의 설비들을 위한 IP 전화기술을 지칭하는 용어이다. 일반적으로 이것은 공중 교환전화망인 PSTN처럼 회선에 근거한 전통적인 프로토콜들이 아니라, 불연속적인 패킷들 내에 디지털 형태로 음성정보를 보낸다는 것을 의미한다.

WiBro(Wireless Broadband)

휴대폰처럼 언제 어디서나 이동하면서 초고속인터넷을 이용할 수 있는 서비스로, 휴대폰과 무선랜의 중간 영역에 있다. 시속 60㎞ 이내로 이동하면서 초고속인터넷을 이용할 수 있다. 주파수 대역은 2.3㎓, 인터넷 속도(서비스 대역폭)는 1Mbps 정도이다.

WLAN(Wireless Local Area Network)

무선 전파 도달거리는 50~200m 정도이며 전송속도가 4~11Mbps로 대용량의 멀티미디어 정보도 주고받을 수 있다. 복잡한 백화점이나 병원 · 박물관 등과 전시회 · 세미나 · 건설현장 등 일시적으로 네트워크를 설치하는 데에 매우 유용하다.

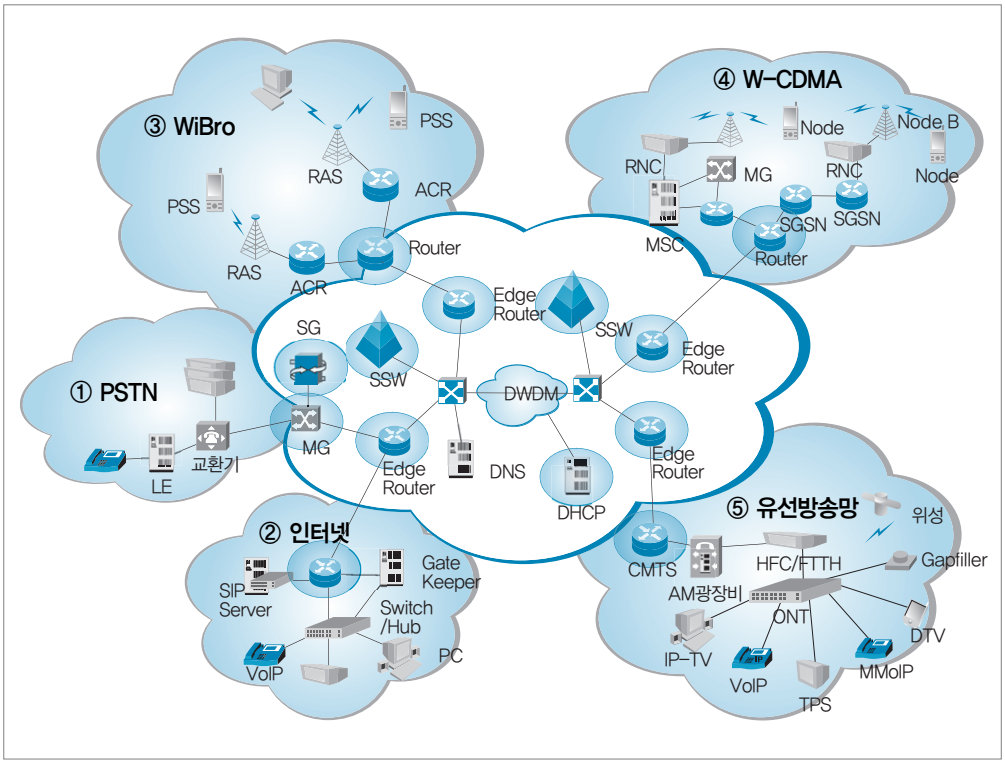
부록 1 BcN 인프라 주요장비 기능 분석

1. 개요

(1) BcN 연동구간 주요장비 선정

BcN 연동구간 주요 장비는 다음의 망 구조도를 중심으로 선정한다.

(그림 부록 1-1) BcN 주요 연동 장비



BcN 주요장비 선정기준은 아래와 같다.

① Gateway 등 전달망 및 가입자망 연동구간에서 연동기능을 담당하는 핵심장비

② 소프트스위치 등 전달망 및 가입자망 계층에서 서비스 및 제어를 담당하는 핵심장비

③ DNS 등 IP 망에서 기반 서비스를 제공하는 장비

※ 개별망 내부에 종속적이며 하위계층에서 단순전송을 담당하는 장비는 제외

(2) BcN 주요장비 선정결과

[표 부록 1-1] BcN 주요장비 선정결과표

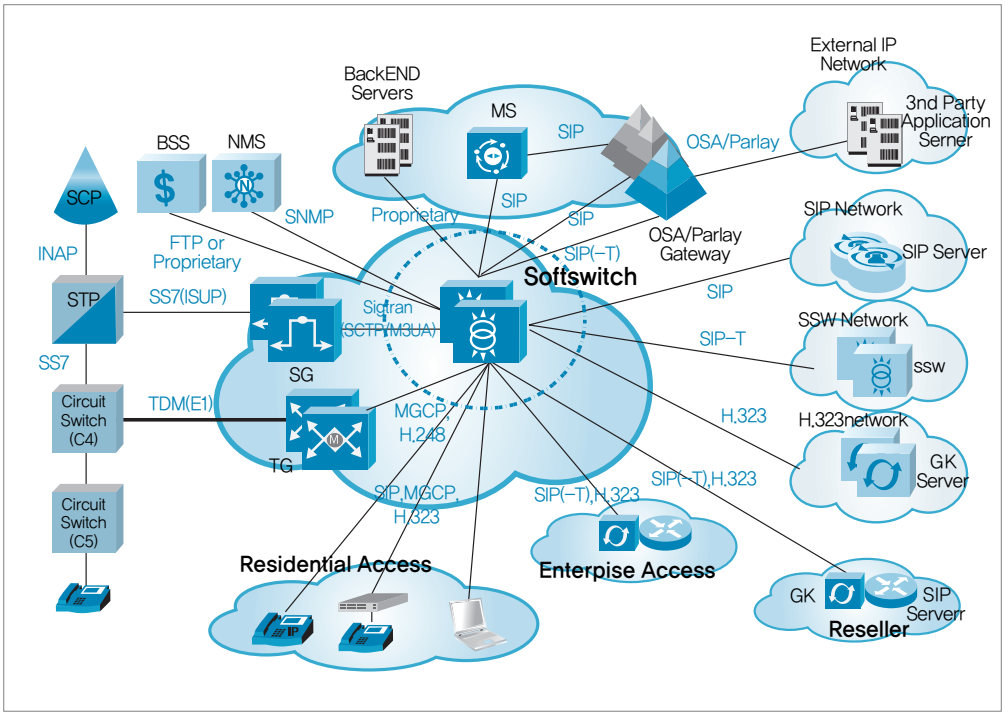
장비명	주요기능
시그널링 게이트웨이	• PSTN과 IP망사이의 미디어 전송의 연동을 담당하는 미디어 게이트웨이를 제어 • PSTN과 IP 망사이에서 회선기반의 트래픽을 IP 기반의 SIP, H.323 패킷 트래픽으로 또는 그 반대로 변환
미디어 게이트웨이	• PSTN과 IP망 사이에서 회선기반의 미디어트래픽을 IP 기반 미디어 트래픽으로 변환
소프트스위치	• 각 가입자망간의 호 연결, 세션제어 기능 수행 – 다양한 응용서버와 표준인터페이스로 연동하여 다양한 서비스 제공 – 인입호 관문, 가입자 인증 및 등록, 세션제어 및 서비스 라우팅, 등록 가입자 프로파일 관리, 번호 분석 및 변환, SIP/SDP 메시지 압축 및 해제기능 제공 • 미디어 게이트웨이 제어기능 – 회선기반 PSTN망의 트래픽을 IP기반 SIP, H.323 등의 패킷 트래픽으로 변환하도록 제어
SIP 서버	• SIP 서버는 IP 프로토콜 기반에서 SIP 프로토콜을 사용하여 인터넷 기반의 음성 · 영상 통화 서비스 제공 • 메시지 교환, 사용자 위치 정보 관리, 라우팅, 보안 정책 운영, 사용자 인증 기능 제공 ※ Proxy Server, Register Server, Redirect Server
CMTS	• HFC망을 통한 초고속인터넷 서비스를 제공하기 위해 인터넷 IP 패킷 기반 신호를 RF 고주파 신호로 변환 시켜 가입자에게 전송 • 가입자 단말에서 오는 RF 신호를 IP 패킷으로 변환 • 인터넷망의 스위치(라우터)와 H/E Combiner를 연결하는 Bridge 역할을 수행 • 양방향 방송을 위한 데이터를 Headend로 전달해 주는 리턴채널 기능제공
MPLS 라우터	• BcN 전달망, 각 가입자망 경계에서 IP 데이터 전송
DHCP 서버	• 가입자 단말기 등에 유동 IP를 부여하는 등 IP 자원관리
DNS 서버	• 주요 전송 시스템의 IP 주소 변환 기능

2. 소프트스위치

(1) 개요

소프트스위치(SSW: SoftSwitch)는 호처리 서비스를 제공하기 위해 IP기반 망에서 H.323, SIP(SIP-T), MGCP, Megaco, ISUP(No.7), SIGTRAN 등의 프로토콜 처리 및 변환, 번호번역 및 라우팅, Media Gateway 제어, 가입자 관리, 가입자 부가서비스, 운용관리 기능 등을 제공하며, PSTN과 IP망 또는 IP망 상호간, PSTN 상호간의 연동 호처리 서비스를 제공하는 시스템이다.

(그림 부록 1-2) 소프트스위치의 위치



⑵ 주요기능

- 호처리와 접속제어 기능 : 소프트스위치가 처리하는 호의 유형은 MGCP 또는 MEGACO를 통해서 미디어 게이트웨이와 소프트스위치 사이에 발생하는 호, H.323 또는 SIP를 통해서 IP 기반의 가입자와 소프트스위치 사이에 발생하는 호, SS7 망 사이에 발생되는 호, 응용 서버와의 사이에서 발생하는 호, 그리고 SIP-T를 통해서 소프트스위치 사이에서 발생하는 호 등으로 분류할 수 있다.

- 미디어 게이트웨이 제어와 관리기능 : 소프트스위치와 미디어 게이트웨이는 주로 MGCP 또는 MEGACO/ H.248 프로토콜을 사용하여 제어가 이루어진다. 이러한 프로토콜은 접속과 제어에 사용되며 게이트웨이의 세부적인 자원관리와 유지보수 기능은 EMS(Element Management System)에서 이루어진다. 소프트스위치는 명령 메시지를 통하여 특정 그룹의 가용성, 호처리 상태 자원을 관리하며, 미디어 게이트웨이가 가지는 인터페이스의 종류에 독립적으로 모든 호에 대한 접속과 제어를 수행한다.

- 주소번역과 라우팅 기능 : 차세대 통신망에서는 전화뿐만 아니라 멀티미디어의 호접속을 위해서 ITU-T E.164 주소체계 뿐만 아니라 IP 주소, URL(Uniform Resource locators) 주소 등 다양한 주소 체계가 사용될 수 있다. 소프트스위치는 이러한 다양한 주소의 상호 변환을 수행하고 번역할 수 있는 기능을 갖추어야 한다. 주소 번역이 완료되면 베어러 채널의 목적지가 정해지게 되며 목적지에 따라 베어러 채널을 네트워크에 연결하는 기능을 수행한다. 향상된 라우팅 서비스를 위해서 TDR(Time Dependent Routing), ODR(Original Dependent Routing) 등의 방법과 루트의 트래픽 상태에 따라 적절한 루트를 선택하는 기능도 제공된다.

- 과금관리 기능 : 소프트스위치에서는 연결된 호에 대해서는 CDR(Call Detail Record)가 생성되며, 이 데이터는 과금관리와 분석을 위해 과금 서버로 전송된다. 호 설정후 연결 정보를 과금서버에 제공하여 사용자의 과금을 관리할 수 있는 기능을 제공한다.

- OAM&P (Operation, Adminstration, Maintenance and Provisioning) 기능 : 장애관

리, 성능관리, 형상관리, 시험 및 프로비저닝 기능을 제공하고, 사용자와의 인터페이스와 타 시스템과의 인터페이스도 제공한다. ESM으로는 SNMP 또는 다른 프로토콜을 사용하여 시스템 내·외부에서 미디어 게이트웨이와 함께 통합해서 운영·관리 할 수 있도록 지원하고 있다.

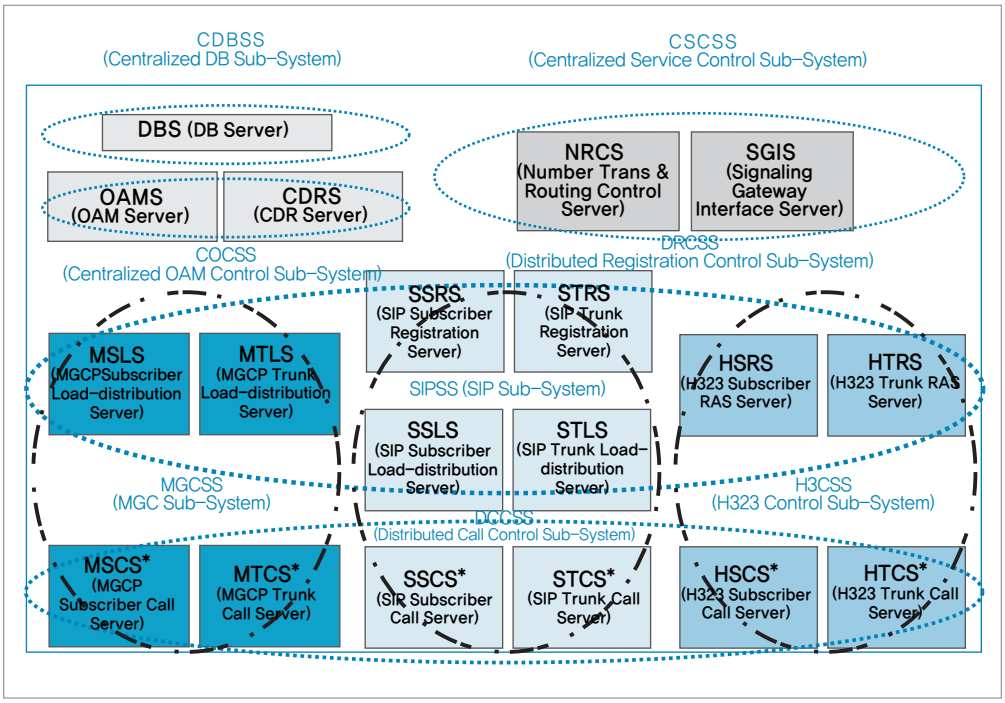
- 다중프로토콜 지원 : 소프트스위치는 다양한 장비와 연결되어 있고, 각 장비들과의 통신을 위해서, MGCP, MEGACO, SIP, SS7 등 다양한 프로토콜을 지원하고 있다.

(3) 동작구조

가. 시스템 구조

소프트스위치는 DB, OAM, Service Control, 그리고 각 Protocol별로 Registration 및 호를 처리하는 Subsystem으로 구성되어진다.

(그림 부록 1-3) 소프트스위치 시스템 구성



나. 동작방식

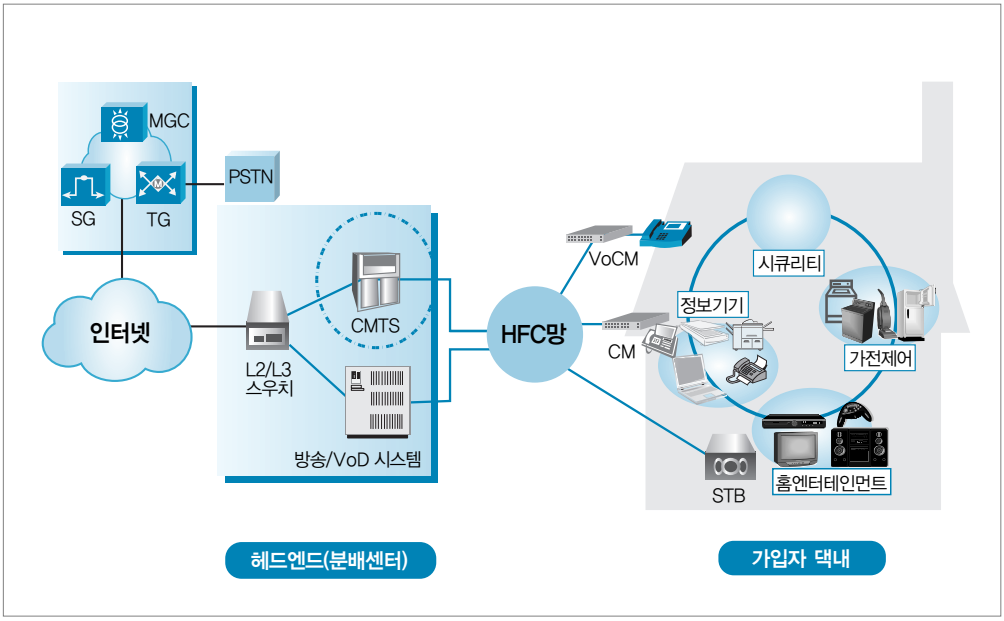
SSW는 Megaco, Sigtran 등의 제어 프로토콜을 사용하여 TG(Trunk Gateway)제어와 SG(Signaling Gateway) 제어 및 연동을 호처리 서비스를 제공하고, SIP, SIP-T, H.323 프로토콜을 통해 타망의 SSW 또는 타 호처리망과 연동기능을 수행한다. 또한 가입자 호처리 서비스를 제공하기 위해 Residential GW 및 IP terminal를 관리하여 H.323, SIP 가입자들에게 등록 및 호 처리 기능을 제공 한다.

SSW 동작의 대부분은 시그널링 게이트웨이 및 미디어 게이트웨이 제어를 통해 호처리 서비스를 제공하는 것으로, 세부 동작방식은 앞서 언급된 시그널링 게이트웨이 및 미디어 게이트웨이 처리절차에서 SSW의 역할을 참조하면 된다.

3. CMTS (Cable Modem Termination System)

(1) 개요

(그림 부록 1-4) CMTS의 위치



※ 출처 : 하나로텔레콤

CMTS는 HFC 망에서 가입자단 케이블 모뎀 (Cable Modem)과 Head-End의 백본 라우터 사이에 위치하여, 케이블 모뎀과의 상호작용을 통해 DOCSIS (Data Over Cable Service Interface Specification) 신호를 인터넷 데이터 패킷으로 바꾸어 백본 네트워크로 전달하여 광대역 인터넷 액세스 서비스를 고객에게 제공하는 장비로써, DSG(Digital Settop Gateway), VoIP 단말장비와 연동하여 Digital CATV, 인터넷 전화 등 TPS(Triple Play Service)를 제공할 수 있게 해주는 장비이다.

(2) 주요기능

- 패킷변환 및 전송 기능 : 인터넷 IP 패킷을 Cable Modem 표준인 DOCSIS 형태로 바꾸어 HFC 분배망을 통해 다수의 Cable Modem(가입자)에게 전송 또는 그 반대의 기능 수행
- Routing 기능 : IP protocol routing을 수행

(3) 동작구조

CMTS는 인터넷을 통해 전송된 IP 패킷을 Cable Modem 표준인 DOCSIS 형태로 바꾸어 HFC 분배망을 통해 다수의 가입자에게 전송하는 기능을 수행하므로, CMTS를 이해하기 위해 먼저 Cable Modem 표준에 대해 살펴본다.

가. 관련 표준 (DOCSIS)

Cable Modem을 위한 표준은 IEEE 802.14, DOCSIS(Data Over Cable Service Interface Specification), Euro-DOCSIS, DVB-RC 등이 있으나, 국내에서 주로 사용되는 DOCSIS 표준에 대해서 먼저 살펴본다.

DOCSIS는 CableLabs에서 개발되어 1998년 3월 ITU에서 비준한 표준으로 케이블 서비스 인터페이스를 통한 데이터 사양에 대해 정의하며, 케이블 모뎀과 지원 장비에 대한 인터페이스 표준으로 사용된다.

[표 부록 1-2] Cable Modem 표준별 특성 비교

Features	Docsis 1.x	Euro-Docsis	DVB-RC
Downstream Rates	64-QAM : 27Mbps 256-QAM : 42Mbps ITU J83 Annex B FEC 6MHz Channelization	64-QAM : 38Mbps 256-QAM : 52Mbps ITU J83 Annex A FEC 8MHz Channelization	64-QAM : 38Mbps 256-QAM : 52Mbps ITU J83 Annex A FEC 8MHz Channelization OOB
Upstream Rates	QPSK : 0.32, 0.64, 1.28, 2.56, 5.12Mbps 16-QAM : 0.64, 1.28, 2.56, 5.12, 10.24Mbps 5-42MHz	QPSK : 0.32, 0.64, 1.28, 2.56, 5.12, 10.24Mbps 16-QAM : 0.64, 1.28, 2.56, 5.12, 10.24Mbps 5-65MHz	0.256, 1.544, 3.088Mbps Differential QPSK 5-65MHz
Services	Internet Access. Interactive set-top Box. Voice over IP	Internet Access. Interactive set-top Box. Voice over IP	Internet Access. Interactive set-top Box.
Basic Protocol	Variable Length. Native IP with QoS	Variable Length. Native IP with QoS	ATM Cell transport. with IP Adaptation layer translation
Security	Baseline Privacy/Plus 56bit DES CBC	Baseline Privacy/Plus 56bit DES CBC	None/latest draft

• DOCSIS 1.0

- CMTS(Cable Modem Termination System)에 의해서 조절되는 대역폭 할당
- 상향에서의 미니슬롯 스트림
- 예약방식과 경쟁방식이 동적으로 혼합된 상향전송
- 가변길이 패킷의 지원을 통한 대역폭의 효율성
- ATM과 다른 데이터 PDU를 수용할 수 있는 확장성
- 폭넓은 데이터 속도의 지원

• DOCSIS 2.0

- 음성, 영상 및 데이터 서비스를 통합하는 수렴형 네트워크
- 잡음에 대한 Robustness가 요구됨에 따라 DOCSIS 2.0 규격은 물리계층의 변복조방식

을 개선

- IP기반 데이터 서비스를 위한 전달구조
- Advanced S-CDMA 및 A-TDMA 도입예정
- Upstream/Downstream Symmetry Service
- Upstream Band-Width Channel 용량 증가와 Noise Immunity 실현
- Upstream Band-Width 확대를 통한 Upstream 전송 속도 향상
- Cell당 가입자의 수용증가

• DOCSIS 프로토콜 계층

물리계층의 HFC를 기반으로 DOCSIS에서 규정된 Cable을 위한 MAC 프레임을 기반으로 기존의 IP, TCP 또는 UDP가 탑재되며, IP와 동일한 계층에서 DOCSIS 제어를 위한 메시지가 동작한다.

[표 부록 1-3] DOCSIS 프로토콜 계층

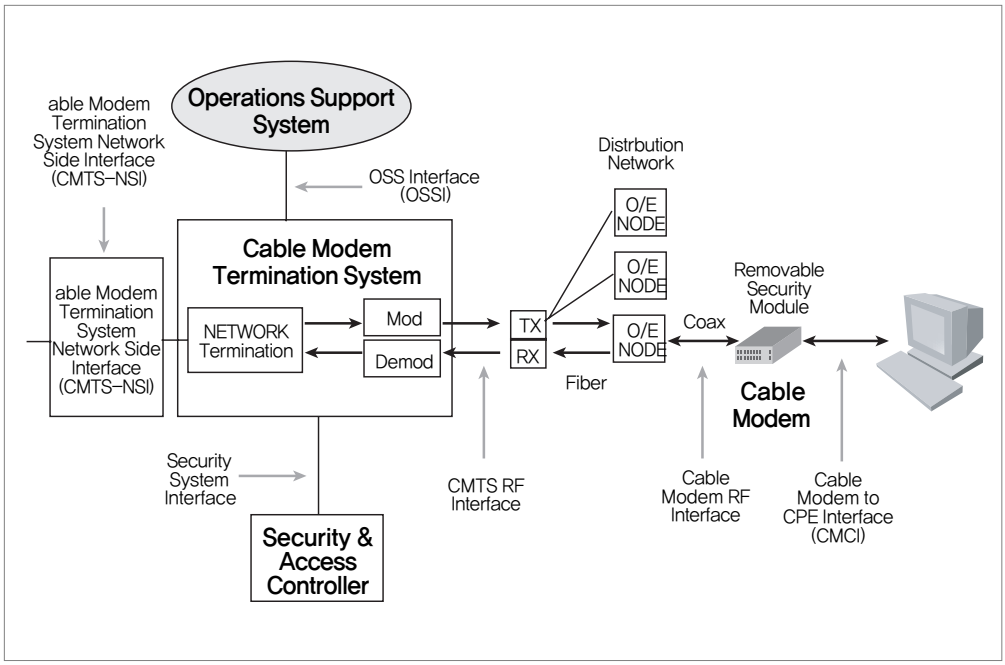
<table>
<tr><th>OSI</th><th colspan="3">DOCSIS Data Over Cable</th></tr>
<tr><td>Higher Layers</td><td colspan="2">Applications</td><td rowspan="3">DOCSIS
Control
Messages</td></tr>
<tr><td>Transport</td><td colspan="2">TCP or UDP</td></tr>
<tr><td>Network</td><td colspan="2">IP, ICMP, ARP</td></tr>
<tr><td rowspan="2">Data Link</td><td colspan="3">IEEE 802.2(14byte)</td></tr>
<tr><td colspan="3">DOCSIS MAC (9byte)</td></tr>
<tr><td rowspan="3">Physical</td><td>UP Stream
TDMA(mini-slot)</td><td colspan="2">Down Stream
TDMA(mini-slot)</td></tr>
<tr><td>5-50/54 MHz</td><td colspan="2">6 MHz</td></tr>
<tr><td colspan="3">HFC</td></tr>
</table>

나. CMTS 동작구조

CMTS 동작구조는 DOCSIS 참조모델을 중심으로 설명한다. CMTS는 인터넷과 연결되는

Network Side 인터페이스(CMTS-NSI: Cable Modem Termination System Network Side Interface)와 Cable 모뎀과 연결하기 위한 DOCSIS 기반의 CMTS RF 인터페이스로 구성된다. 또한 CMTS 관리를 위해 OSS(Operations Support System)와 연결되는 인터페이스를 가지며 보안을 위해 보안시스템 인터페이스를 가진다.

(그림 부록 1-5) DOCSIS 참조모델 기반의 CMTS 동작구조

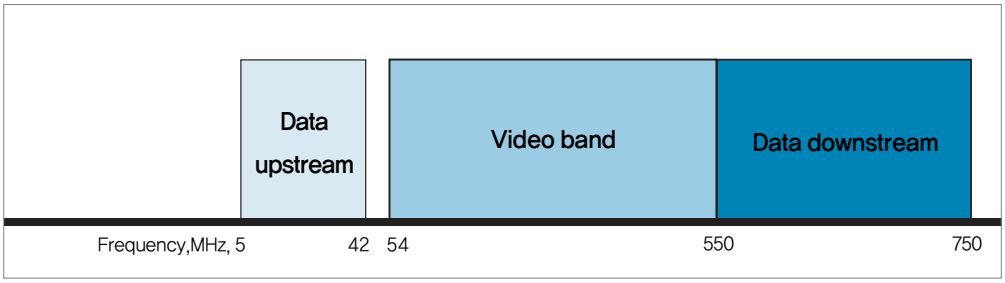


CMTS는 인터넷과 연결되는 CMTS-NSI와 Cable 모뎀과 연결하기 위한 DOCSIS 기반의 CMTS RF 인터페이스는 데이터링크 계층까지는 서로 다른 기술을 사용하지만, 네트워크 계층에서는 양쪽 인터페이스 모두 IP를 사용한다.

1) 물리계층의 동작

- HFC 망에서 동축케이블에 사용되는 네트워크 주파수 대역은 5~750MHz의 주파수 대역폭을 가짐
  - 동영상, 하방향(downstream) 데이터, 상방향(upstream) 데이터로 나뉨

(그림 부록 1-6) CMTS 주파수 대역폭



- 동영상(아날로그 방송) 대역 : 54~550MHz의 주파수, 80개 이상의 채널을 담을 수 있음
- 하방향 데이터 대역 : 550~750MHz의 주파수, 6MHz 채널들로 나뉘어 있으며, 64-QAM 변조 기술을 사용하며 채널당 데이터 전송률은 30Mbps (5비트/Hz x 6MHz)
- 상방향 데이터 영역 : 5~42MHz의 주파수, 6MHz 채널로 나뉘어 있으며, QPSK 변조 기술을 사용하고 채널당 데이터 전송률은 12Mbps(2 비트/Hz x 6MHz)

• HFC망에서 여러개의 Cable 모뎀이 데이터를 전송하는 경우에 medium에 대한 공유가 필요

- 상방향 공유 : 상방향은 6개의 채널(대역폭(37MHz) / 채널(6MHz) = 6 채널)이 있으며, 상방향으로 데이터를 전송시 하나의 채널을 사용한다. 많은 가입자 있을 경우에는 이를 해결하기 위해 시간공유(time sharing), 채널이 빌 때까지 기다리는 contention 기법 등을 사용
- 하방향 공유 : 하방향은 33개의 6MHz 채널이 있으며, 다중 방송(multicasting) 방식을 통해 각 가입자에게 데이터가 채널로 전달됨

2) CMTS와 CM(Cable Modem)간 통신 절차

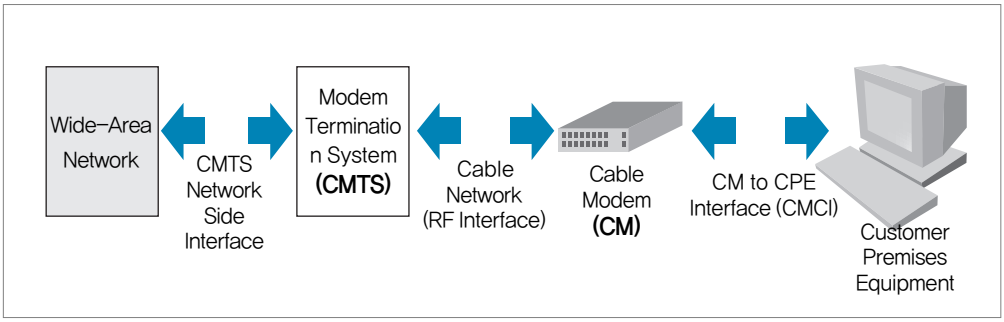
• 상향 스트림(Upstream) : CM → CMTS

① CPE(가입자 컴퓨터)로부터 IP 트래픽을 Ethernet으로 받아 Cable MAC Frame으로 Framing

② 필요시 암호화

③ QPSK 또는 16-QAM으로 디지털변조

(그림 부록 1-7) CMTS와 CM(Cable Modem)간 통신 절차도



④ 5~65MHz에서 CMTS로 전송

※ CMTS로 데이터 전송을 위해, 먼저 CMTS가 CM에 패킷을 보내 상/하방향 채널을 할당하고, CM은 할당된 상방향 채널에 시간공유 또는 경쟁방식을 통해 슬롯을 할당 받은 후에 데이터를 전송

• 하향 스트림(Downstream) : CMTS → CM

① CMTS에서 전송되는 선택한 Downstream Channel로부터 RF 신호를 수신

※ CMTS는 할당된 하방향 채널을 사용하여 수신 CM의 주소와 함께 패킷을 보냄

② 64/256-QAM Digital 변조된 신호 복조

③ MPEG 패킷을 추출

④ CM 자신 또는 CPE로 향하는 MPEG 패킷으로 MAC frame 추출

⑤ 암호화된 경우 원 Data로 복구

⑥ CM으로 향하는 Message 처리

⑦ CPE로 향하는 Data는 Ethernet으로 전송

3) CMTS와 인터넷간 통신절차

CMTS는 Network Side 인터페이스를 통해 인터넷을 위한 L2/L3스위치 또는 라우터 등과 연결된다. 일부 CMTS는 자체적으로 OSPF, RIP 등의 라우팅 프로토콜을 탑재한 라우팅, 멀티캐스트 지원을 위한 IGMP 프로토콜 지원 기능도 수행한다. 인터넷 연결을 위한 라우터 또는 스위치와 CMTS간 동작 절차는 일반 인터넷 연결 구조와 동일하므로 별도의 설명은 생략한다.

4) CMTS 관리 기능

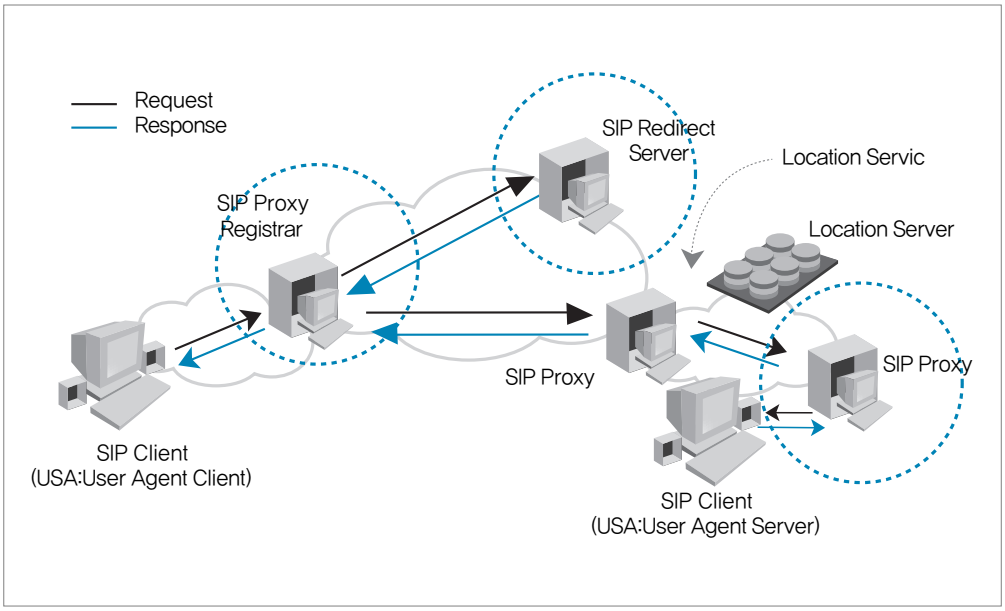
CMTS는 Cisco, 주니퍼네트웍스, Terayon 등에서 개발하고 있으며 자체적인 운영체제(예: Cisco의 경우 Cisco IOS)를 탑재하고, DNS 지원, SNMP/Telnet 프로토콜을 통한 원격관리 등을 지원하고 있다.

4. SIP 서버

(1) 개요

SIP 서버는 IP 프로토콜 기반에서 SIP 프로토콜을 사용하여 인터넷 기반의 음성 · 영상 통화 서비스를 제공하는 장비이다. SIP Server는 SIP 단말들이 메시지 교환, 사용자 위치 등록으로 네트워크를 이동하여 사용할 수 있도록 해주며, 사업자로 하여금 라우팅, 보안 정책 운영, 사용자 인증, 사용자 위치를 관리하도록 한다. SIP Server 는 여러 응용 형태로 표현될 수 있으나, 일반적으로 SIP Standard에서는 Proxy Server, Register (Registra) Server, Redirect Server의 3가지 형태로 표현된다.

(그림 부록 1-8) SIP 서버 위치



⑵ 주요 기능

가. Proxy Server 기능

- UAC에서 SIP 호처리 메시지 수신하여 상대편 UAC 또는 Proxy Server에 호를 연결해주며 요청 메시지에 대한 수용, 거절 또는 Redirect 등의 기능을 수행
- 메시지 처리를 위해 UAC, UAS[1]로써 동작하며, 수신한 SIP 요청 메시지에 대한 응답 메시지를 생성하며, 경우에 따라 수신메시지 수정

나. Redirect Server 기능

- Proxy 등에 사용자 위치정보를 제공
- 요청 메시지에 3xx 응답을 생성하여 클라이언트 접속 주소를 가리키는 대체 URI 전송

다. Registrar Server 기능

- REGISTER 메시지를 통해 호 서비스 송수신을 위한 사용자 접속정보 저장
- 특정 사용자의 접속주소에 대한 정보 제공

⑶ 동작구조

가. Proxy 동작

Proxy Server는 UAC로부터 호 연결 요청을 받게 되면, 수신자의 위치정보를 제공 해주는 Registrar 서버에게 연결하여 수신자의 정보를 얻게 된다. Proxy 서버는 수신자의 위치정보를 가지고 UAC가 보낸 INVITE 메시지를 재조립한 다음 파악된 위치정보 상의 서버에게 전달한다.

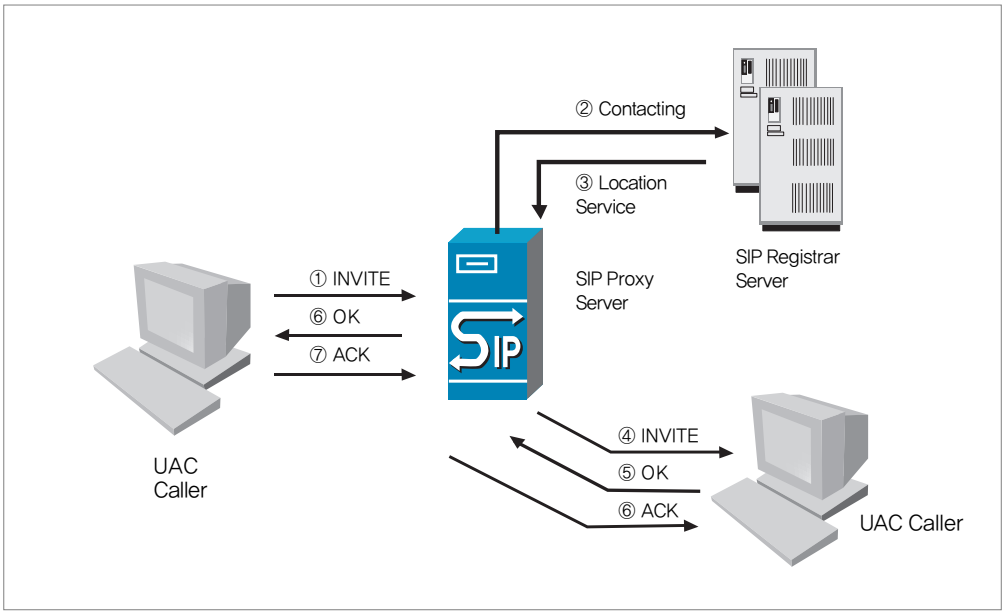
Proxy Server는 동작방식에 따라 Stateful과 Stateless 방식으로 나뉘며, Stateful은 각각 유입된 호에 대한 정보를 기억하며 이것으로 호를 생성하고 처리하는 반면 Stateless은 각 호를 처리하지만 호에 대한 상태 정보를 기억하지 않는다.

---

1) UAC와 UAS의 차이 : SIP request를 요청하는 측은 UAC(User Agent Client), 이에 응답하는 측은 UAS(User Agent Server)로서 SIP 단말기, Proxy 서버 등도 역할에 따라 UAS, UAC로 동작

Proxy 서버의 동작절차는 다음과 같다.

(그림 부록 1-9) Proxy 서버 동작절차



① Proxy서버는 INVITE 메시지를 수신

② Request의 어드레스를 확인후 Registrar 서버에게 contact

③ Registrar 서버로부터 callee의 정확한 위치 정보를 수신

④ Proxy 서버는 Registrar 서버에게 받은 수신자 주소로 SIP Request를 송신

⑤ Proxy 서버에게 메시지를 잘 받았다는 응답 송신

⑥ Proxy 서버는 UAC 에게 OK 응답을 송신하면서, caller에게 OK 응답을 송신

⑦ UAC 는 Proxy 서버에게 ACK 메시지를 포워딩함으로써 메시지 전송이 성공적으로 이루어짐을 알리게 되고 호 설정 완료

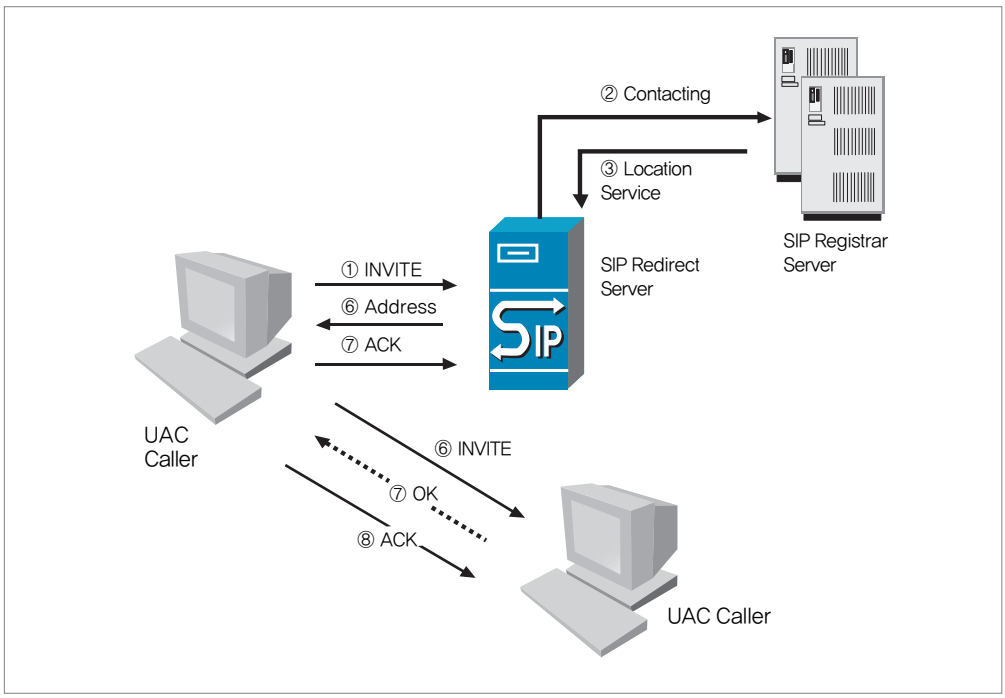
나. Redirect 동작

Redirect 서버는 UAC의 SIP 요청메시지를 수신하면 상대방 UAS와 연결하기 위한 서버의 주소를 UAC에게 알려줌으로써 UAC가 직접 다음 서버에 요청메시지를 보낼 수 있도록 한다. 즉 Redirect 서버는 사용자의 요청에 대한 응답 기능만을 수행할 뿐 스스로 요청 메시지를 생

성하지 않는다.

Redirect 서버의 동작절차는 다음과 같다.

(그림 부록 1-10) Redirect 서버 동작절차



① Redirect 서버는 INVITE 메시지를 수신

② Redirect 서버는 INVITE의 어드레스를 보고 Registrar 서버를 contact 하여 callee의 정확한 위치 정보수신

③ Redirect 서버는 새로 얻어진 Callee의 주소를 UAC에게 송신

④ UAC는 Redirect 서버에게 되돌려 받은 Callee의 주소로 새로운 Request를 송신

⑤ 호 요청이 성공적으로 이루어지면 UAC와 UAS는 ACK를 주고 받음으로써 호 설정 완료

다. Registration 동작절차

Registration 동작 절차는 앞의 Proxy 서버 동작절차도와 Redirect 서버의 동작절차도를

참고하도록 한다. Registration 서버는 아래와 같이 기능을 수행한다.

① UAC는 Registra 서버에게 자신의 contact 주소를 전송하여 등록요청

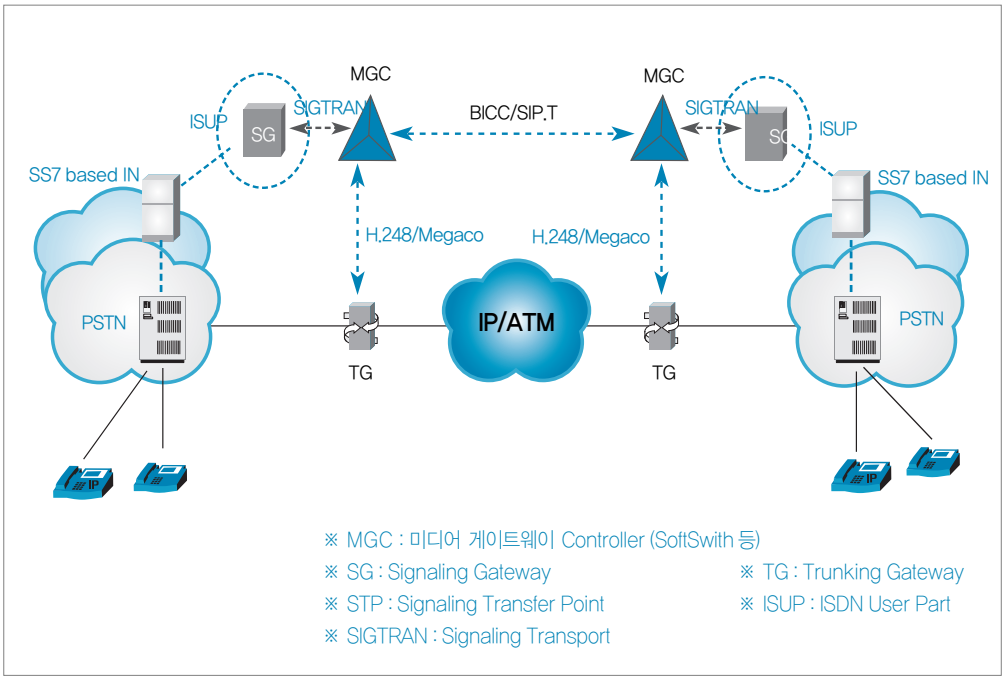
② Registra 서버는 200 OK 메시지로 응답하여 UAC에 등록을 알림

5. 시그널링 게이트웨이

(1) 개요

시그널링 게이트웨이(SG: Signaling Gateway) 시스템은 PSTN 망과 인터넷 망 사이에서 No.7 신호 메시지를 IP Core 망에 필요한 SIGTRAN 프로토콜 형태로 변환하여 MGC(미디어 게이트웨이 Controller)에 전달하는 기능을 수행한다.

(그림 부록 1-11) Signaling Gateway의 위치



⑵ 주요기능

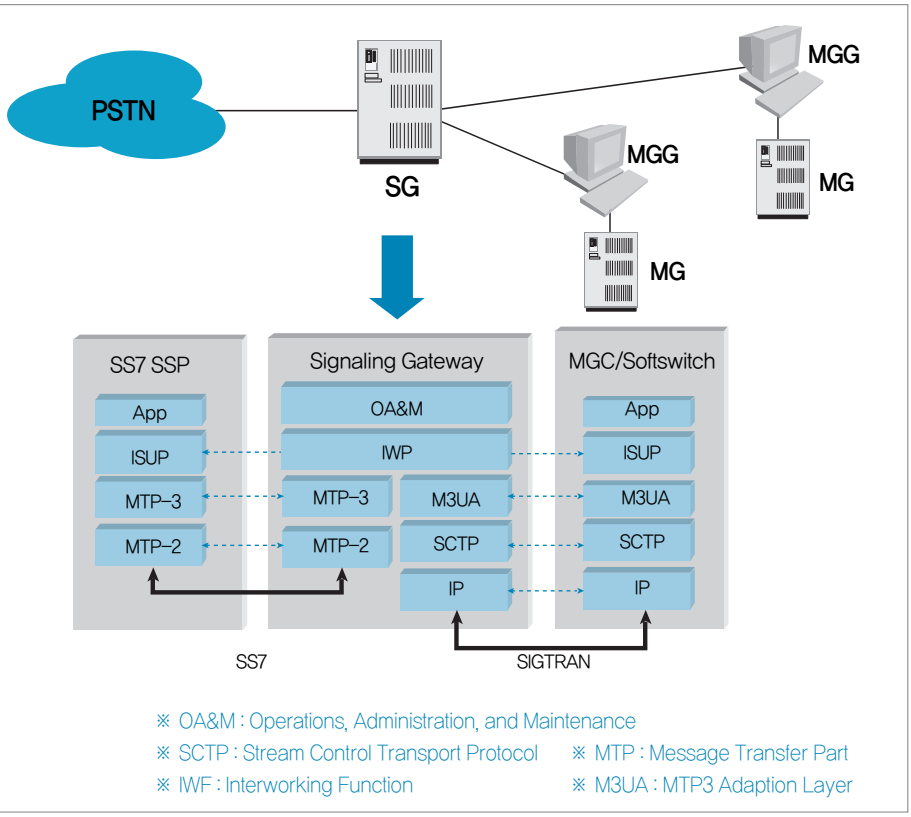
• PSTN망의 SS7/ISUP 시그널과 IP망의 SIGTRAN 프로토콜을 상호변환하여 STP 또는 MGC로 전송하는 기능

⑶ 동작구조

가. 시스템 구조

시그널링 게이트웨이 내부 구성요소는 신호처리를 위한 DSP, 내부 운영체제 및 응용프로그램 운영을 위한 Micro Processor, 시그널링 변환을 위한 Network protocol, Signaling 변환 및 네트워크 관리 등을 위한 소프트웨어 등으로 구성된다.

(그림 부록 1-12) 시그널링 게이트웨이 시스템 구조



• PSTN망의 STP(Signaling Transfer Point)에서 SS7, ISUP 프로토콜을 사용하여 호 설정 Signal이 입력되면, SG는 MGC로 Signal을 전송하기 위해 SIGTRAN 프로토콜 형태로 변환하여 전송

• OA&M 계층에서는 SNMP 등의 프로토콜 등을 사용하여 SG 설정변경, 모니터링 등의 관리기능을 제공할 수 있도록 GUI, Command Line 등 인터페이스 기능 제공

• MTP(Message Transfer Part) 계층은 소스에서 메시지를 받아 목적지로 전송하는 역할을 담당하며, MTP-1은 노드간 물리적 연결을 담당하며 MTP-2는 SS7 메시지의 오류 검출/정정 및 순서화된 전달을 제공하고, MTP-3는 SS7 네트워크의 signaling 지점간 메시지 라우팅, signaling 네트워크 관리, 링크 오류시 트래픽 rerouting, contestion 제어 등을 담당

• IWF는 SS7 네트워크와 IP 네트워크 사이에서 ISUP 시그널링 신호를 SIGTRAN 프로토콜 형태로 변환하여 연결하는 기능을 담당

나. SS7/ISUP 프로토콜 동작

스위치간에 발생하는 전화호의 설정/해제를 담당하는 프로토콜로서 SG에서는 MTP-1, 2, 3와 같은 하위계층 프로토콜에 encapsulation되어 전달되며, 다음과 같은 메시지들을 포함한다.

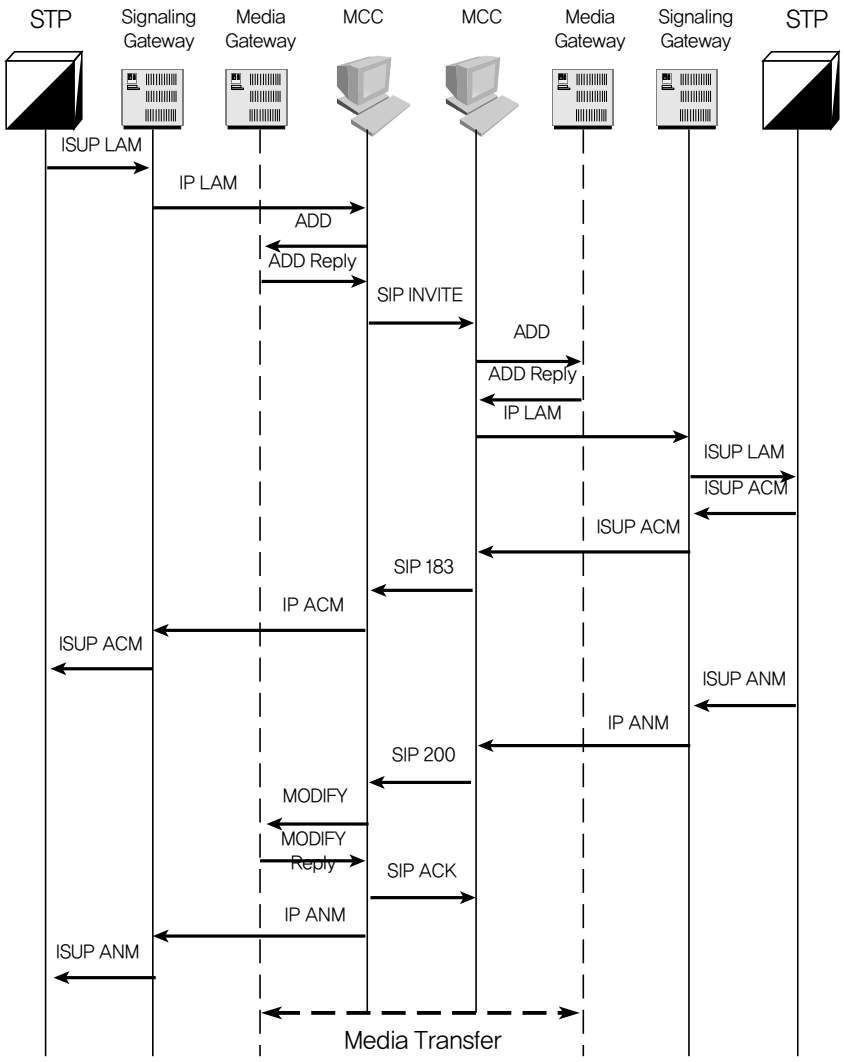
• Initial Address Message (IAM)
 - 스위치간 호 초기화
• Address Complete Message (ACM) - Optinal
 - 수신지로부터 발신지 스위치까지 단방향 오디오 경로가 개설되었음을 알림 (발신자가 Ringback 톤을 들을 수 있음)
• Call Progress Message (CPG) - Optional
 - 호 처리 관련하여 발신지 스위치에 추가적인 정보 제공
• Answer Message (ANM)
 - 수신지(called party)에 의해 호가 수락되었음을 알림

• Release Message (REL)

– 호 해제 초기화

STP ↔ SG 사이의 ISUP 시그널링 메시지가 SG ↔ MGC 사이의 메시지로 변환되는 메시지 흐름의 예는 다음과 같다.

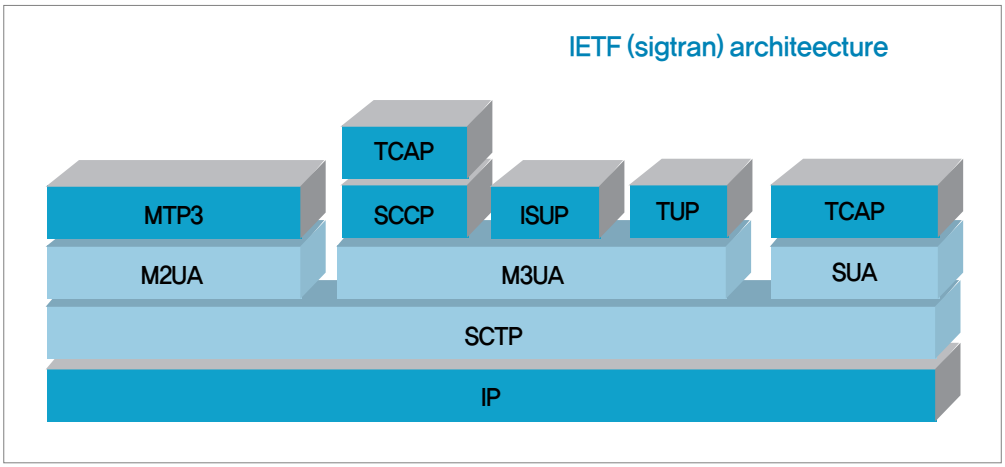
(그림 부록 1-13) STP, SG, MGC간의 메시지 흐름도



다. SIGTARN 프로토콜 동작

SIGTRAN(Signaling Transport)은 IP 망에서 SCN(Switched Circuit Network)의 Signaling을 전송하고 캡슐화하기 위한 메시지 기반의 프로토콜이다. 구조적으로는 시그널링 게이트웨이와 미디어 게이트웨이 Controller 사이에 Signaling 정보를 주고받는데 사용된다. SCN protocol의 번역은 Signaling 종단에서 일어나기 때문에 SIGTRAN은 단순히 캡슐화된 정보를 전송하는 기능을 수행한다.

(그림 부록 1-14) SIGTRAN 프로토콜 스택



SIGTRAN은 시그날링 게이트웨이에 필요한 두 종류의 상이한 표준으로 구성된다. SCN 신호패킷이 인터넷을 통과해서 다른 시그날링 게이트웨이로 전달되기 위해서는 인터넷에서 처리할 수 있는 패킷 형태로 바뀌어야 하는데 SS7과 ISDN Q.921 관련된 "SCN Adaptation Module" 부분과, 변환된 패킷을 인터넷을 통해서 상대방 시그날링 게이트웨이에 올바르게 전송하기 위한 "Common Signaling Transport" 관련 부분이며 이를 위해 새로운 전송 프로토콜인 SCTP (Stream Control Transmission Protocol)가 제정되었다.

- 시그날링 전송 프로토콜 : SCTP
  - SIGTRAN 프로토콜의 일부로, SS7 신호를 IP 네트워크에 전송해야 하며 SS7 Gateway가 PSTN 신호를 IP 패킷으로 변환하기 위한 표준이다.

- SCTP는 IP 프로토콜(IP 프로토콜 번호: 132) 기반에서 동작하며, IP 패킷내에 encapsulation되어 신뢰된 데이터 전송을 지원한다(RFC 2960).
- SCTP 프로토콜 포맷

MAC header	IP header	SCTP header	Data :::

- SCTP 프로토콜 헤더

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source port	Destination port
Verification tag	
Checksum	
Chunk [1.. n] :::	

- Chunk는 INIT, DATA, SACK, SHUTDOWN, ECNE, ERROR, ABORT 등의 Type을 정의하여 SCTP 프로토콜의 초기화, 재전송, 종료, Congestion Notification 등의 기능을 제공한다.
- SCTP 프로토콜은 연결형 스트림을 제공하며(필요시 비연결형 스트림 전달 제공), 손실/손상된 패킷에 대한 선택적인 재전송 및 중복 패킷 검출, 체크섬, 검증 tag를 이용한 패킷 무결성 등을 제공하여 신뢰된 패킷 전달 기능을 제공하며, TCP와 유사한 흐름제어 및 congestion 회피, 네트워크 MTU에 맞는 긴 패킷 프래그먼테이션 등의 기능을 제공한다.

• M3UA (MTP3 User Adaptation Layer)

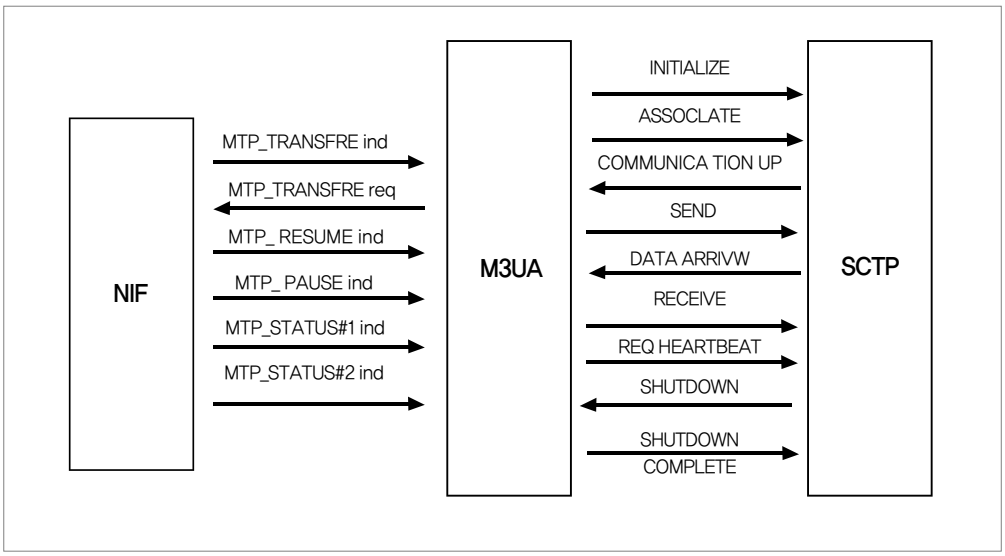
- M3UA는 SG에서 SCN 시그널링 프로토콜을 MGC 또는 IP 기반의 데이터베이스 등에 전달하는 역할을 수행한다.
- MGC에서 ISUP 메시지를 아래 계층으로 데이터 전송 명령 및 요청하면 M3UA가 이를 처리하며 SG에서 MTP3의 하위 인터페이스에 제공한다. SS7 네트워크로부터의 시그널링 메시지 착신 표시를 하고, 착신 데이터 메시지는 SG에서 MTP3로부터 상위로 전달되며 M3UA에 의해 MGC의 ISUP 하위 인터페이스로 전달된다. (〈시그널링 게이트웨이 내부 구조〉 그림 참조)

- M3UA는 포트 2905를 사용하여 TCP/SCTP 프로토콜에 포함되어 전송된다. (프로토콜 세부내용은 RFC 3332 참조)
- M3UA 프로토콜 포맷

MAC header	IP header	TCP header	M3UA header	Data :::
MAC header	IP header	SCTP header	M3UA header	Data :::

- SG내에서 NIF, M3UA, SCTP 계층간 메시지 흐름은 다음과 같다.

(그림 부록 1-15) SG내에서 NIF, M3UA, SCTP 계층간 메시지 흐름도



6. 미디어 게이트웨이

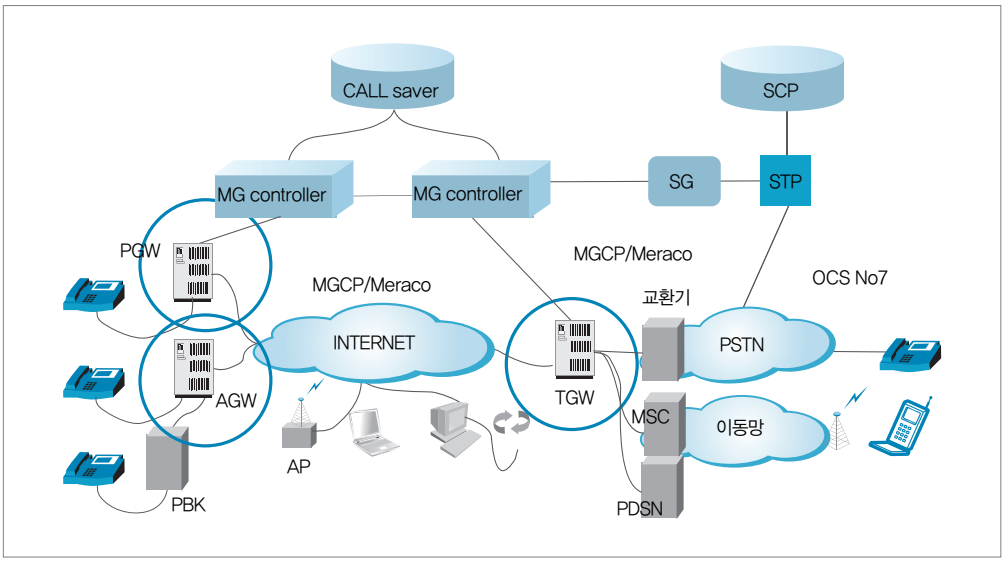
(1) 개요

통신망에 따라 트래픽 포맷의 형식을 변환하는 장비로서 주로 차세대 패킷 음성 전달망에서 서킷망의 TDM 트래픽을 패킷망의 ATM 혹은 IP 트래픽 변환으로 사용되는 관문 역할을 수행한다. 이때 통화 호 제어를 위해 소프트스위치와 제어 프로토콜(예: MGCP, Megaco 등)로 연

동하여 트래픽 흐름 경로를 결정한다. 게이트웨이들간의 정보 전달은 IP 방식인 경우 RTP(Real-time Transport Protocol)를 이용하며, ATM 방식인 경우 영구 가상 연결(PVC) 혹은 교환 가상 연결(SVC)을 이용한다.

MGW(미디어 게이트웨이)는 RGW(Residential Gateway), AGW(Access Gateway), TGW(Trunk Gateway)를 통칭하는 용어이며, MGC(미디어 게이트웨이 Controller)는 MGCP, Megaco 등의 제어 프로토콜을 사용하여 MGW를 제어하는 역할을 한다.

(그림 부록 1-16) 미디어 게이트웨이의 위치



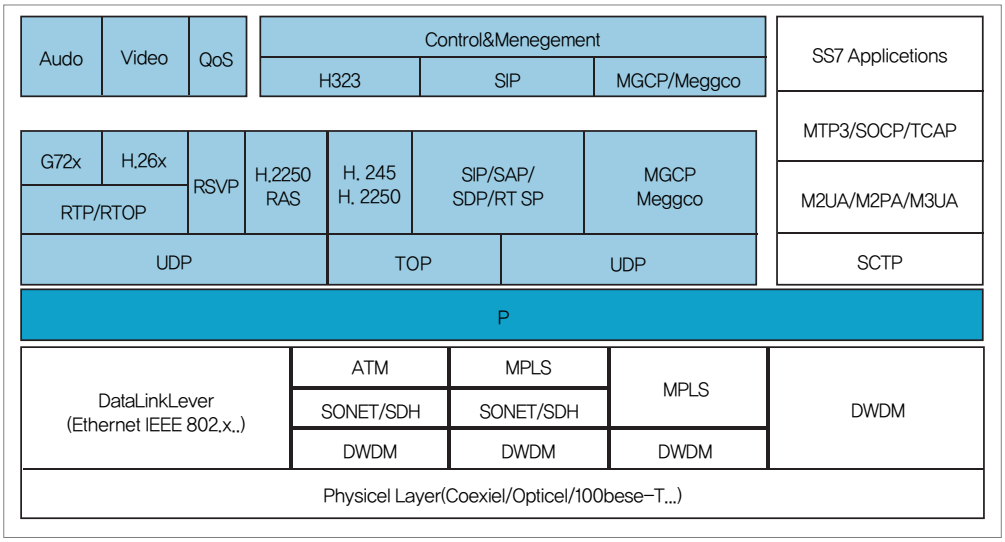
(2) 주요기능

- 단 대 단(Peer to peer) 연결 제어 기능 (회선망과 패킷망간)
- 미디어 연결 및 전송 기능 : Audio, Video, Data
- VoIP Protocol Control : H.323, SIP(Session Initiation Protocol), SDP(Session Description Protocol) 처리
- 사업자간 호 제어 연결 관리 및 처리
- 보안기능 및 QoS 기능 제공

(3) 동작구조

가. 프로토콜 구조

(그림 부록 1-17) 미디어 게이트웨이 프로토콜 구조



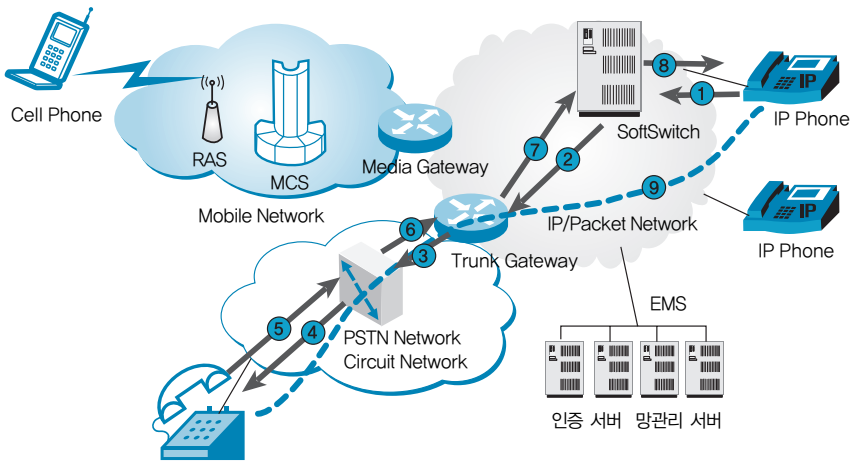
- 데이터링크 계층은 이더넷, ATM, MPLS, DWDM 등을 사용하며 네트워크 계층에서는 IP 프로토콜을 사용하여 IP기반의 데이터와 음성 서비스 모두를 제공
- 인터넷 프로토콜 상위 기반으로는 회선 교환망과 연동하기 위한 CCS(Common Channel Signaling) No.7 신호 호 처리 프로토콜 부분인 SCTP(Stream Control Transmission Protocol), MTP3(Message Transfer Part Level 3), M2PA(SS7 MTP2-User Peer-to-Peer Adaptation Layer), M2UA(SS7 MTP2-User Adaptation Layer), M3UA(SS7 MTP3-User Adaptation Layer), SCCP(Signaling Connection Control Part), TCAP(Transaction Capabilities Application Part)으로 구성
- IP 기반 망으로 호 설정 프로토콜과 음성 데이터를 전달하는 프로토콜로 TCP(Transmission Control Protocol)와 UDP(User Datagram Protocol) 사용
- 호 제어 및 관리를 위하여 H.323, SIP, Megaco를 사용
- 음성 데이터는 G시리즈로 전달하고, 화상데이터는 H시리즈로 전송하며, 이들 데이터는

RTP(Realtime Transport Protocol)/ RTCP(RTP Control Protocol) 프로토콜을 이용하여 실시간으로 전송

나. 동작 절차

• IP Phone에서 전화를 걸어 PSTN 전화기에서 수신하는 경우

(그림 부록 1-18) IP Phone→ PSTN 전화연결



① IP Phone → 소프트스위치 : INVITE (SDP 포함) 메시지를 전달한다. 소프트스위치는 수신자의 전화번호를 보고 Trunk Gateway 방향으로 연결되어 있다는 것을 알 수 있다. 이러한 사용자의 위치 정보는 Trunk Gateway를 통해 PSTN Phone 사용자를 미리 등록시킬 수도 있으며 사업자가 네트워크 구성시에 해당 전화번호 프리픽스를 보고 라우팅 경로를 설정할 수도 있다.

② 소프트스위치는 Trunk Gateway 쪽으로 콜을 호출하는 INVITE 메시지(SDP 포함)를 전송한다.

③ 트렁크 게이트웨이는 자신이 속해 있는 PSTN Network 교환기쪽으로 SS No.7 (IAM) 메시지를 전달함으로써 해당 콜을 요청한다.

④ PSTN 교환기는 자신이 관장하는 PSTN 폰에 벨이 울리도록Ringing Voltage를 송신한다. 동시에 Trunk Gateway 쪽으로 SS No.7(ACK) 메시지를 전달한다. 이때 이미

IP Phone과 PSTN 교환기 간에는 SDP 메시지의 협상과 함께 RTP 루트가 성립된다.

⑤ PSTN Phone이 응답하면 PSTN 교환기 쪽으로 Answer 메시지를 송신한다.

⑥ PSTN 교환기는 트렁크 게이트웨이에게 ANM 메시지를 송신하면서 호가 성립하였음을 통지한다.

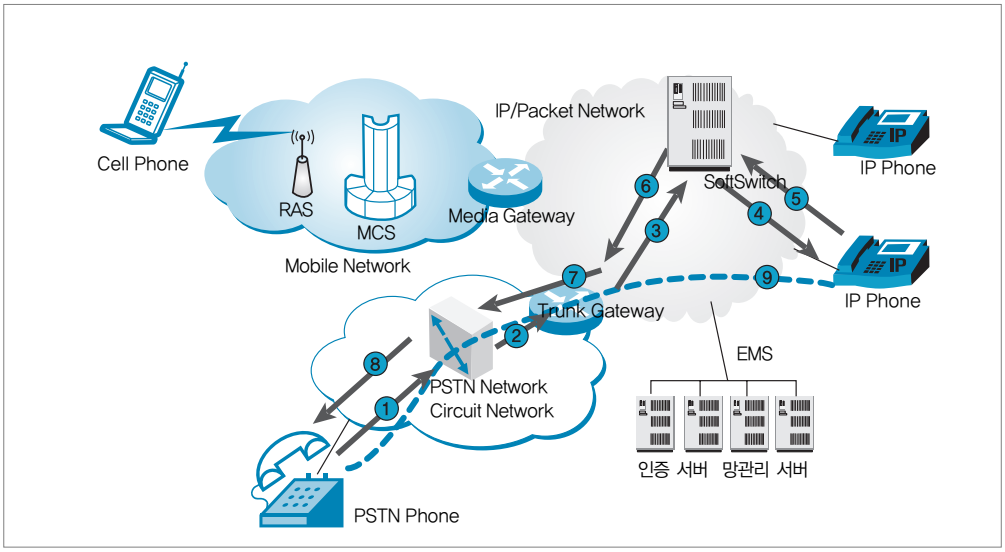
⑦ 트렁크 게이트웨이는 SIP 메시지 200으로 소프트스위치에 응답한다.

⑧ 소프트스위치는 IP 폰에게 200 메시지를 전달하고 그에 대한 응답으로 ACK 메시지를 수신한다.

⑨ 앞의 ⑧번까지의 모든 과정이 호처리 과정이며 이를 통해 End-to-End 통신을 위한 RTP 경로가 9번과 같이 설정된다. RTP 연결시 소프트스위치는 경로에서 빠지게 되며 트렁크 게이트웨이가 미디어에 대한 변환 기능을 담당한다.

• PSTN Phone에서 전화를 걸어 IP Phone에서 수신하는 경우

(그림 부록 1-19) PSTN Phone→ IP Phone



① PSTN Phone에서 IP Phone No2로 발신을 시작한다. 이 경우 발신자의 SETUP 메시지는 PSTN 교환기로 일차적으로 보내어진다.

② PSTN 단말에서 받은 SETUP 메시지를 트렁크 게이트웨이 쪽으로 보낸다.

③ PSTN 게이트웨이는 PSTN 단말에서 올라온 정보를 보고 INVITE 메시지를 생성해서 소프트스위치 쪽으로 전달한다. 이 때 코덱 관련 정보도 함께 생성하여 전달한다.

④ 소프트스위치는 그림에는 나타나 있지 않지만 별도로 구성될 수 있는 데이터베이스에서 목적지 주소의 위치정보를 획득하고 획득한 정보에 의해 SIP Phone No.2 로 INVITE 메시지를 전송한다.

⑤ IP Phone은 180 Ringing 메시지를 먼저 보내서 통화 시도중이라는 메시지를 전달할 수도 있다. 현재 이 그림에서는 IP Phone이 곧바로 수화기를 들어 응답했다는 가정으로 IP Phone이 응답을 하게 되면 200 메시지가 소프트스위치로 보내어진다.

⑥ 소프트스위치는 트렁크 게이트웨이 쪽으로 200 메시지(SDP 포함)를 전송한다.

⑦ 트렁크 게이트웨이는 자신이 속해 있는 PSTN 교환기쪽으로 SS No.7 (Alerting과 상대방 응답시 Connect) 메시지를 전달함으로써 통화 성립을 통보한다. 그림에는 표시되지 않았지만 동시에 ACK 메시지를 IP Phone에 전송한다.

⑧ PSTN 교환기는 Alerting 메시지를 받아서 PSTN Phone에 전달하고, Connect 메시지를 받음으로써 End-to-End RTP 통신을 시작하기 위한 준비 단계에 들어간다.

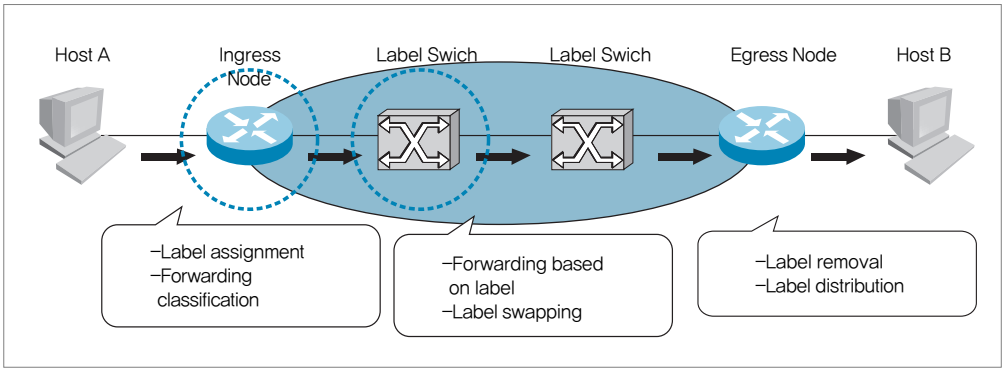
⑨ PSTN Phone과 IP Phone No.2는 협상된 코덱 정보를 가지고 RTP 채널을 만들고 통신을 시작한다. RTP 연결시 소프트스위치는 경로에서 빠지게 되며 트렁크 게이트웨이가 미디어에 대한 변환 기능을 담당한다

7. MPLS 라우터

(1) 개요

MPLS 라우터는 MPLS(Multiprotocol Label Switching) 기능을 제공하는 라우터를 의미하며, RFC 3031[1]에서는 "Label Switching Router" 또는 LSR이라고 정의한다. MPLS는 네트웍 트래픽 흐름의 속도를 높이고 관리하기 쉽게 하기 위한 기술로, 각 패킷에 라벨을 붙여 이에 따라 라우팅을 수행한다. MPLS는 또한 IP, ATM 및 프레임 릴레이 등 다양한 네트워크 프로토콜 등과 함께 동작하며 OSI의 네트워크 계층(라우팅)이 아닌, 스위칭을 하는 데이터링크 계층에서 대부분의 패킷이 전달될 수 있게 한다. MPLS는 트래픽을 전반적으로 빠르게 움직이게 하는 것 외에도, 라벨에 따른 QoS 관리를 쉽게 해준다.

(그림 부록 1-20) MPLS 라우터 위치



MPLS 라우터는 MPLS 도메인에서의 위치에 따라 다음과 같이 구분하고 있다.

- MPLS ingress node: MPLS 도메인으로 들어가는 트래픽을 다루는 MPLS 에지 노드
- MPLS egress node: MPLS 도메인을 떠나는 트래픽을 다루는 MPLS 에지 노드
- MPLS intermediate node: MPLS 도메인에 속하는 MPLS 라우터 중에서 에지 라우터를 제외한 중간에서 동작하는 MPLS 라우터

모든 MPLS 라우터는 역할에 따라 달리 사용될 수 있으므로 이 기능들을 모두 포함하고 있어야 한다. MPLS 라우터는 실제 망에서 사용될 때에는 MPLS 기능만을 제공하는 네트워크 장비보다는 기존의 IP 포워딩 기능(IP 라우팅)과 MPLS 스위칭 기능을 모두 제공하는 네트워크 장비로 구현된다.

(2) 주요기능

가. IP 포워팅 기능

- IP 라우팅 테이블(RIB) 생성 기능 : IP 패킷의 L3 포워딩을 위한 판단의 근거가 되는 정보 테이블로, 관리자에 의한 정적(static) 생성 또는 라우팅 프로토콜을 통한 동적(dynamic) 생성
- IP 포워딩 기능 : 목적지 IP 주소를 기반으로 한 IP 라우팅

나. MPLS Ingress 에지 노드 기능

- MPLS 정보테이블(LIB) 생성 기능 : unlabeled 패킷에 레이블을 할당하기 위해 필요한 LIB 테이블을 생성하는 기능
- MPLS 신호 프로토콜 운영 : LIB 생성에 필요한 정보를 얻기 위해 MPLS 신호 프로토콜을 운영하는데, 관리자의 정적 관리와 MPLS 신호 프로토콜을 통한 동적 관리가 가능
- FEC 정의 기능 : unlabeled 패킷을 받은 후에, FEC를 정의할 수 있는 기능
- labeled 패킷 생성 기능 : unlabeled 패킷의 FEC 정의 후 LIB에서 해당하는 레이블 값을 찾아서 패킷을 MPLS 패킷으로 만드는 기능
- labeled 패킷 전달 기능 : labeled 패킷을 해당하는 출력 포트로 출력하는 기능

다. MPLS Egress 에지 노드 기능

- MPLS 정보 테이블(LIB) 생성 기능: labeled 패킷에서 레이블을 제거하기 위해 필요한 정보를 담고 있는 LIB 테이블을 생성하는 기능
- MPLS 신호 프로토콜 운영: LIB 생성에 필요한 정보를 얻기 위해 MPLS 신호 프로토콜을 운영하는데, 관리자의 정적 관리와 MPLS 신호 프로토콜을 통한 동적 관리가 가능
- unlabeled 패킷 생성 기능: labeled 패킷에서 레이블을 제거하여 unlabeled 패킷(IP 패킷)으로 만드는 기능
- unlabeled 패킷 전달 기능: unlabeled 패킷을 해당하는 출력 포트로 출력하는 기능으로 결국 IP 포워딩 기능

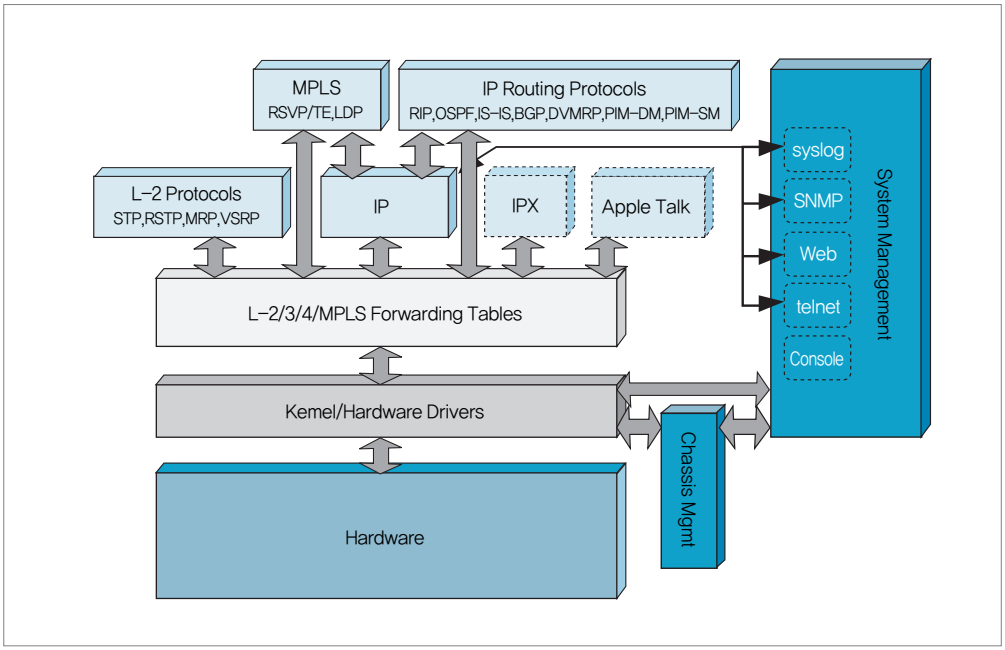
라. MPLS 중간 노드 기능 (MPLS 스위칭 기능)

- MPLS 정보 테이블(LIB) 생성 기능: labeled 패킷에서 레이블을 제거하기 위해 필요한 정보를 담고 있는 LIB 테이블을 생성하는 기능
- MPLS 신호 프로토콜 운영: LIB 생성에 필요한 정보를 얻기 위해 MPLS 신호 프로토콜을 운영하는데, 관리자의 정적 관리와 MPLS 신호 프로토콜을 통한 동적 관리가 가능
- labeled 패킷 스위칭 기능: 입력 labeled 패킷을 받아서 LIB에서 검색한 정보를 기반으로 레이블을 교체하고 출력 인터페이스로 전달하는 기능

(3) 동작구조

가. 시스템 구조

(그림 부록 1-21) MPLS 라우터 구조 예시 (Netron Systems의 IronWare OS)



일반적으로 대형 라우터들은 제어 보드(control board)와 패킷 처리 보드(packet processing board)가 통합되어 있지 않고 분리되어 있는 구조로 개발된다. 이렇게 함으로써 제어 보드의 이중화를 통한 시스템의 안전성 보장과 하나 이상의 패킷 처리 보드의 구성으로 그 용량 및 성능을 향상시킬 수 있고, 다양한 사양의 패킷 처리 보드와의 구성이 가능하여 융통적인 시스템의 구성이 가능하기 때문이다.

제어 보드에는 IP와 MPLS 처리를 위해서 라우팅, MPLS 시그널링, 그리고 그 외의 응용 소프트웨어가 탑재된다. 패킷 처리 보드에서는 실제 IP 패킷과 MPLS 패킷을 수신하고 패킷에 따라 전달 방식을 결정하고 그 결과에 기반하여 전달하는 과정을 수행하게 되는데, ingress와 egress의 양방향 패킷 처리가 모두 가능하다. 그리고 요즘은 네트워크 프로세서(Network

Processor)를 도입하여 ASIC과 유사한 처리 능력을 제공하면서도 기능의 구현과 수정이 용이하여 융통성 있고 효율적인 시스템을 구현하고 있다.

나. MPLS 라우터 동작절차

MPLS 라우터의 동작방식을 살펴보면 크게 두 단계로 구분할 수 있다. 첫 번째 단계는 레이블 분배가 일어나는 단계 즉, LSP가 설정되는 단계이고, 두 번째 단계는 실제 사용자 데이터가 설정된 LSP를 따라 전달되는 단계이다. 이 단계는 레이블 할당을 언제 어떻게 하는가에 따라서 각 과정의 수행 순서에 차이가 있다.

레이블의 할당 방식은 다음과 같이 크게 제어 트래픽 기반 레이블 할당과 데이터 트래픽 기반 레이블 할당으로 구분해 볼 수 있다.

1) 제어 트래픽 기반 레이블 할당

- 패킷 전송 전에 라우팅 또는 토폴로지 정보를 이용하여 레이블을 할당하는 방식
- 토폴로지 기반 레이블 할당
  - 네트워크 토폴로지 정보를 이용하여 레이블을 할당
  - 여러 경로를 하나의 레이블로 통합 가능
- 요구 기반 레이블 할당
  - 요구 제어 트래픽을 통해 레이블을 할당
  - RSVP, CR-LDP 프로토콜 사용

2) 데이터 트래픽 기반 레이블 할당

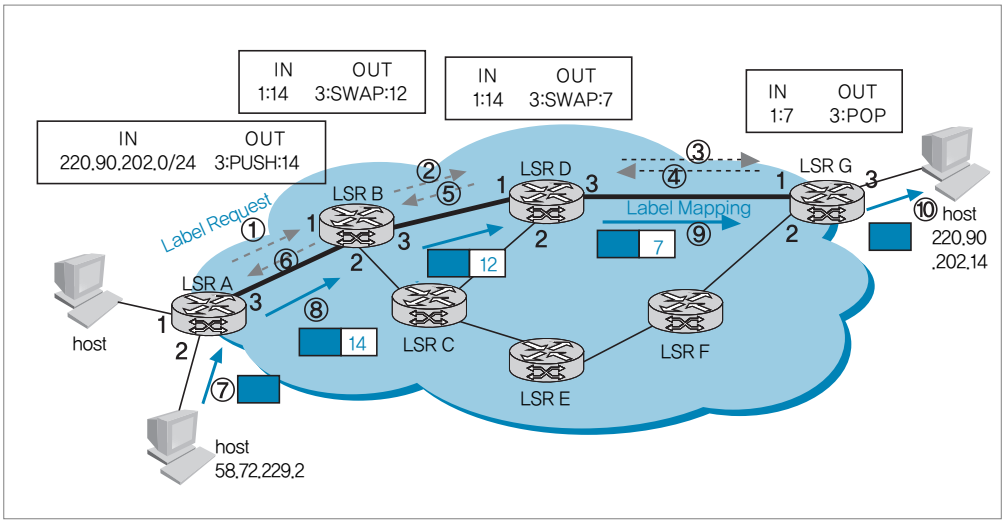
- FEC에 속한 데이터가 도착하는 시점에서 플로우마다 레이블을 할당하는 방식
- 많은 레이블을 필요로 하기 때문에 확장성 문제 발생

레이블 할당 요청('Label Request' 메시지 수신)을 받은 MPLS 라우터는 egress 에지 라우터인 경우를 제외하고는 하위 스트림 MPLS 라우터에게 'Label Request' 메시지를 전송하여 해당 FEC에 대한 레이블을 요청하게 되는데, 이 때 하위 스트림 MPLS 라우터로부터 요청한 레이블을 할당받은 후에 상위 스트림 MPLS 라우터에게 레이블을 할당(Ordered control

mapping mode)할 수도 있고, 레이블을 할당받기 전에 상위 스트림 MPLS 라우터에게 레이블을 할당(Independent control mapping mode)할 수도 있다. 전자의 경우에는 ingres MPLS 라우터에서 egress MPLS 라우터까지 레이블 할당 요청이 전달된 후에 egress MPLS 라우터에서부터 요청된 FEC에 대한 레이블을 할당받아 오는 것이므로 ingress MPLS 라우터에 레이블 할당이 메시지('Label Mapping' 메시지)가 수신되면, 요청한 FEC에 대해서 단대단으로 LSP가 제대로 설정되었다는 것을 보장할 수 있다. 이것은 일정 대역폭의 할당 등의 조건이 만족되어야 하는 LSP 설정에 적용하면 단대단 품질 만족을 위한 LSP 설정이 가능하다는 장점을 얻을 수 있다. LDP에서는 두 가지 모드를 모두 지원하고 있다.

다음은 Ordered control mapping mode로 동작한다고 가정하고 수행한다.

(그림 부록 1-22) MPLS 라우더 동작절차(1)



① 라우팅 프로토콜이 생성한 라우팅 정보를 이용하여 220.90.202.0/24 네트워크를 하나의 FEC로 정의하고 이에 대한 레이블 할당을 위해, LSR A는 LSR B에게 'Label Request' 메시지를 전송하여 레이블을 요청한다.

② '220.90.202.0/24' 네트워크에 대한 'Label Request' 메시지를 받은 LSR B는 해당 네트워크로 데이터를 전달하기 위한 하위 스트림 MPLS 라우터인 LSR D에게 'Label Request' 메시지를 전송하여 레이블을 요청한다.

③ LSR D는 'Label Request'를 수신한 후에 하위 스트림 MPLS 라우터인 LSR G에게 'Label Request' 메시지를 전송한다.

④ LSR G는 220.90.202.0/24 네트워크에 대한 'Label Request'를 수신한 후, 이 네트워크가 자신의 하위에 연결되어 있는 로컬 네트워크임을 인식하고 egress로 동작하게 된다. 그래서 7번 레이블을 할당하여 LIB 테이블에 엔트리를 추가하고, 'Label Mapping' 메시지를 LSR D에게 전송한다.

⑤ LSR D는 LSR G로부터 할당받은 레이블 값 7을 LIB의 출력 정보에 기입하고, LSR B에게 레이블 12를 할당하여 LIB 입력 정보에 기입하고 'Label Mapping' 메시지를 LSR B에게 전송한다.

⑥ LSR B는 LSR D로부터 레이블 12값을 포함한 'Label Mapping' 메시지를 받아 LIB의 출력 정보를 추가하고, 레이블 14를 할당하여 LIB의 입력 정보에 등록한 후 LSR A에게 'Label Mapping' 메시지를 전송한다.

⑦ 호스트 58.72.229.2에서 220.90.202.14로 데이터 패킷을 전송한다.

⑧ MPLS 도메인의 ingress 에지 라우터인 LSR A는 호스트로부터 unlabeled 패킷을 수신하여 FEC를 정의한 후, LIB에서 해당되는 정보를 검색하여 대응되는 엔트리대로 패킷을 처리한다. 예에서는 출력 레이블에 14를 PUSH하고 3번 인터페이스로 전달한다. 이 때, 출력 인터페이스의 링크 계층이 이더넷이라면 심헤더로 캡슐화하여 전송한다.

⑨ LSR A부터 LSR G까지 각각의 MPLS 라우터들은 labeled 패킷을 수신하여, LIB에서 입력 인터페이스와 입력 레이블 값을 키로 하여 해당되는 엔트리를 검색하고 대응되는 엔트리가 있는 경우에는 지정된 레이블 연산을 수행한다. 예에서는 각각 출력 레이블로 SWAP를 수행하여 다음 홉으로 전송하였다.

⑩ egress 에지 라우터로 동작하는 LSR G는 labeled 패킷을 수신한 후, LIB에서 대응되는 엔트리의 정보대로 레이블을 POP하고 내부의 IP 패킷 헤더의 목적지 주소를 보고 IP 라우팅을 수행한다.

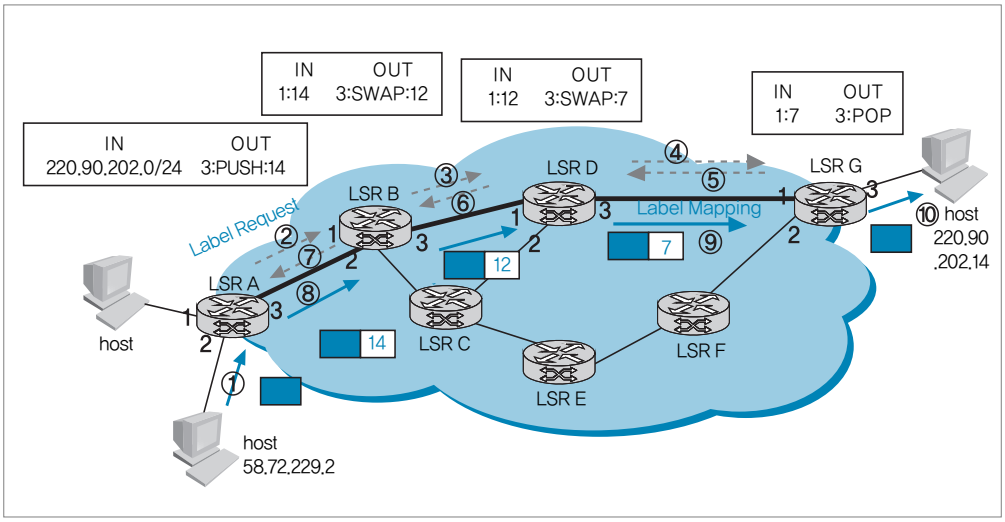
다음의 그림은 데이터 트래픽 기반 레이블 할당을 나타낸 것이다. 이 방식은 사용자 데이터가 ingress 에지 라우터에 도착하는 시점에 FEC를 정의하고 플로우마다 레이블을 할당하는 방식으로, 플로우마다 레이블을 할당하기 때문에 제어 트래픽 기반 레이블 할당 방식보다 많은 레이블을 필요로 하여 확장성에 문제가 발생할 수 있다. 하지만, 사용자마다 또는 응용마다

LSP를 설정해야 하는 경우에는 유용하게 사용할 수 있는 방식이다.

전송할 데이터가 ingress 에지 라우터에 도착하였을 때 레이블 할당이 시작되기 때문에 전체적으로 LSP가 설정될 때까지는 사용자 데이터가 LSP를 통해 전송될 수 없다. 그래서 LSP가 설정되는 시간 동안 데이터 전송을 지연시키거나, 폐기하거나, IP 라우팅으로 수행하는 방법 중 선택해서 적용할 수 있다.

다음의 그림도 레이블 요청과 할당의 순서를 'Ordered control mapping' 모드로 동작하며, LSR 사이의 피어 발견은 이미 수행되었다고 가정한다.

(그림 부록 1-23) MPLS 라우더 동작절차(2)



① 호스트 58.72.229.2에서 220.90.202.14로 데이터 패킷을 전송한다.

② LSR A는 unlabeled 패킷을 받은 후, 220.90.202.0/24 네트워크를 하나의 FEC로 정의하고 이에 대한 레이블 할당을 위해 LSR B에게 'Label Request' 메시지를 전송하여 레이블을 요청한다.

③ '220.90.202.0/24' 네트워크에 대한 'Label Request' 메시지를 받은 LSR B는 해당 네트워크로 데이터를 전달하기 위한 하위 스트림 MPLS 라우터인 LSR D에게 'Label Request' 메시지를 전송하여 레이블을 요청한다.

④ LSR D는 'Label Request'를 수신한 후에 하위 스트림 MPLS 라우터인 LSR G에게 'Label Request' 메시지를 전송한다.

⑤ LSR G는 220.90.202.0/24 네트워크에 대한 'Label Request'를 수신한 후, 이 네트워크가 자신의 하위에 연결되어 있는 로컬 네트워크임을 인식하고 egress로 동작하게 된다. 그래서 7번 레이블을 할당하여 LIB 테이블에 엔트리를 추가하고, 'Label Mapping' 메시지를 LSR D에게 전송한다.

⑥ LSR D는 LSR G로부터 할당받은 레이블 값 7을 LIB의 출력 정보에 기입하고, LSR B에게 레이블 12를 할당하여 LIB 입력 정보에 기입하고 'Label Mapping' 메시지를 LSR B에게 전송한다.

⑦ LSR B는 LSR D로부터 레이블 12값을 포함한 'Label Mapping' 메시지를 받아 LIB의 출력 정보를 추가하고, 레이블 14를 할당하여 LIB의 입력 정보에 등록한 후 LSR A에게 'Label Mapping' 메시지를 전송한다.

⑧ LSR A는 호스트로부터 LSR B로부터 레이블 매핑을 받은 후 LIB의 출력 정보에 14번 레이블 값과 출력 인터페이스 3을 등록하고서 전송할 사용자 데이터에 레이블을 추가하여 전송한다. 이 때, 출력 인터페이스의 링크 계층이 이더넷이라면 심헤더로 캡슐화하여 전송한다.

⑨ LSR A부터 LSR G까지 각각의 MPLS 라우터들은 labeled 패킷을 수신하여, LIB에서 입력 인터페이스와 입력 레이블 값을 키로 하여 해당되는 엔트리를 검색하고 대응되는 엔트리가 있는 경우에는 지정된 레이블 연산을 수행한다. 예에서는 각각 출력 레이블로 SWAP를 수행하여 다음 홉으로 전송하였다.

⑩ egress 에지 라우터로 동작하는 LSR G는 labeled 패킷을 수신한 후, LIB에서 대응되는 엔트리의 정보대로 레이블을 POP하고 내부의 IP 패킷 헤더의 목적지 주소를 보고 IP 라우팅을 수행한다.

앞의 두 그림에서 살펴본 레이블의 할당과 데이터 전송을 위한 MPLS 라우터의 동작은 단방향에만 적용되므로, 송신 호스트와 수신 호스트 사이의 데이터 통신을 위해서는 레이블 할당이 양방향으로 각각 수행되어야만 한다. 이렇게 각 방향에 따라 레이블을 할당하여 LSP를 설정하는 과정에서 라우팅 정보와 토폴로지 정보에 따라 순방향과 역방향의 LSP가 서로 일치하지 않을 수도 있다.

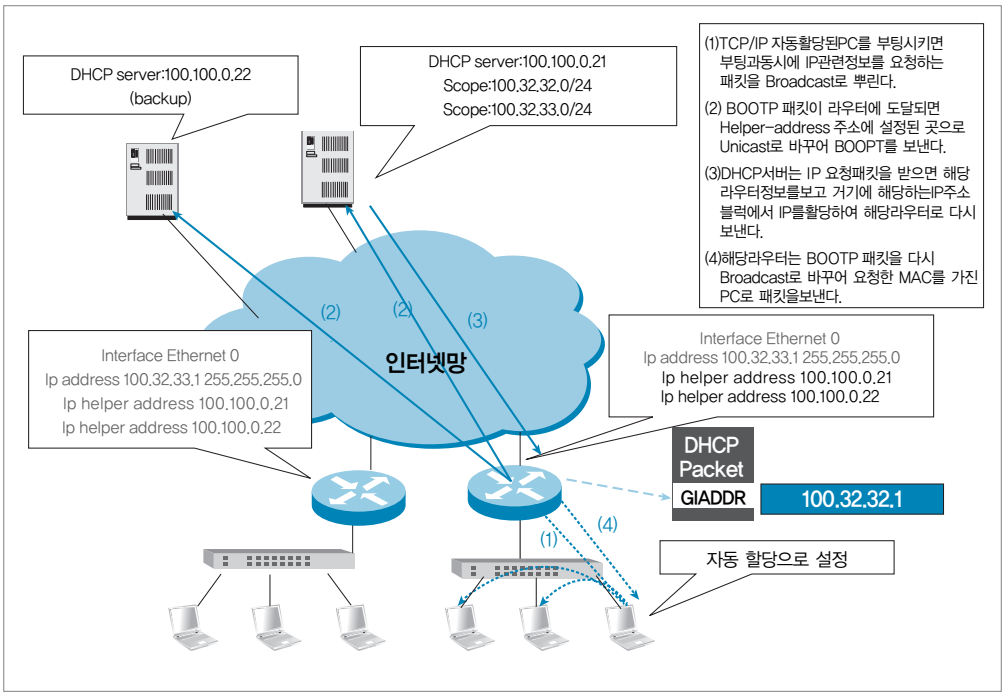
8. DHCP 서버

(1) 개요

DHCP (Dynamic Host Configuration Protocol)은 시스템이 IP정보를 서버에 요청하게 되면 DHCP서버에서 미리 지정된 IP블럭 내에서 적절한 IP를 부여하여 인터넷을 사용할 수 있도록 지원해주는 기능을 하며, 부주의한 사용자에 의한 IP 설정 오류 및 IP 주소 충돌에 의한 장애를 방지해주며, 유한한 IP자원의 효율적 사용 및 관리의 편의성을 제공해준다. DHCP 서버는 실제 서비스하고 있는 사용자의 수보다 적은 IP수로 서비스를 가능하게 해주는 기능들을 가진다.

(2) 주요기능

(그림 부록 1-24) DHCP 동작개념도



가. 기본기능

- IP할당 : 단말이 부팅할 때 DHCP서버로부터 IP를 할당 받는다
- Subnet Mask설정 : 단말에 Subnet Mask를 자동으로 할당해준다.
- 게이트웨이 주소 설정 : 단말의 Default 게이트웨이를 자동으로 할당해준다.
- DNS 서버 주소 할당 : 단말의 DNS 서버를 자동으로 할당해준다.

나. 선택기능

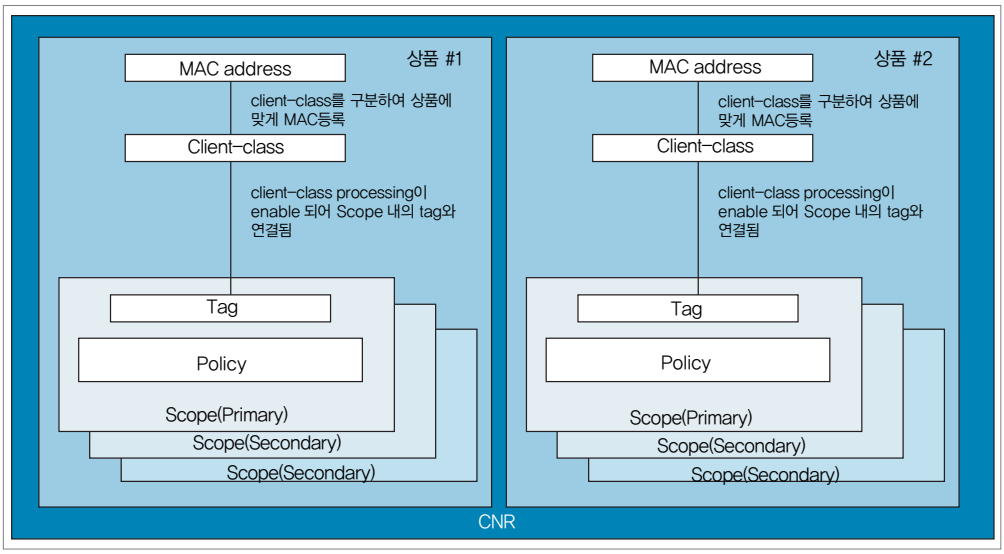
- TFTP서버 설정 : VoIP단말설정에 필요한 TFTP서버를 자동으로 설정해준다.
- Configuration 화일 자동 설정 : VoIP단말의 통화에 필요한 Configuration 파일을 자동으로 설정해준다.

(3) 동작구조

가. 시스템 개요

Cisco의 CNR의 경우 Scope에 ISP에 맞는 Tag가 설정되어 있어 Policy의 Option에 정의된 규정에 따라 Scope의 네트워크 IP블록을 할당 받는다. 다음은 Cisco의 CNR의 동작개념도

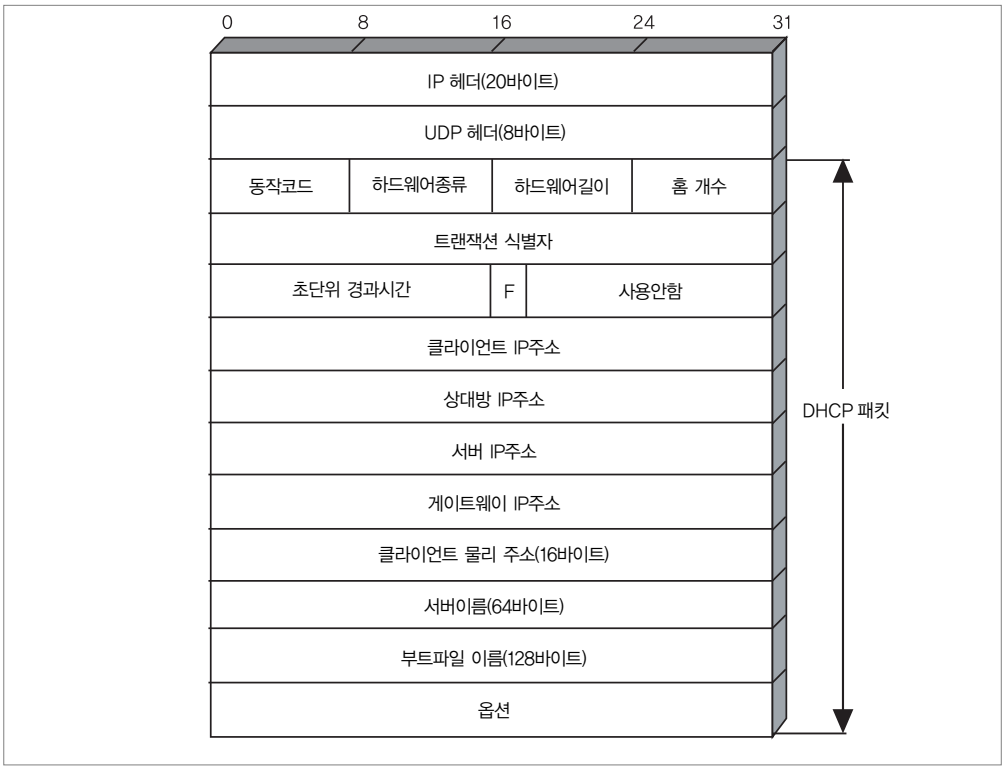
(그림 부록 1-25) Cisco CNR 설정개념도



이다. CNR은 서비스 제공자를 위해 전세계적으로 가능한 자체 운영시스템 기반으로 개발되어 있다.

나. DHCP 패킷 포맷

(그림 부록 1-26) DHCP 패킷의 포맷



다. DHCP 동작절차

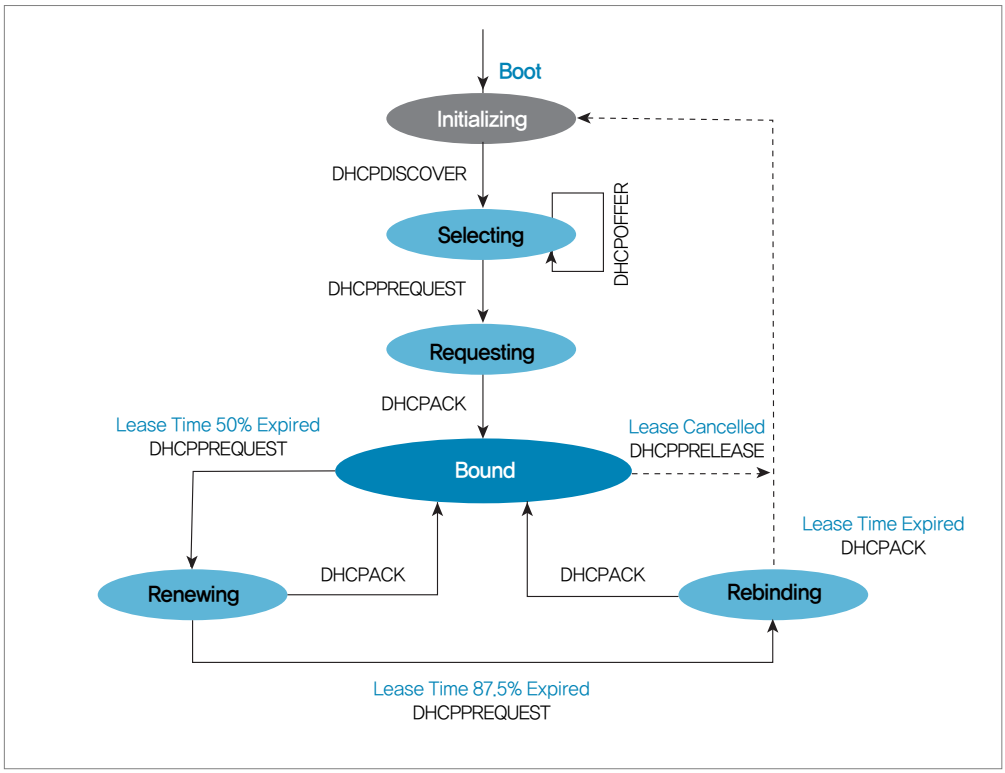
네트워크 상에서 DHCP 패킷은 위 포맷과 같이 만들어지며 클라이언트와 서버간 IP임대 요청, IP임대 제공, IP임대 선택, IP임대 확인, IP임대 갱신, IP임대 제거 등의 과정을 거쳐 동작된다.

DHCP의 IP할당 전체에 대한 매커니즘은 아래의 순서대로 진행된다.

① IP임대 요청 (DHCP Discover)

- 단말에서 서버측으로 IP임대를 요청한다.

(그림 부록 1-27) DHCP 동작절차



- Mac 주소와 호스트 이름 포함

② IP임대 제공 (DHCP Offer)

- 서버가 제공할 수 있는 IP주소, 서비넷마스크, 임대기간, DHCP 서버주소(서버 식별자)를 브로드 캐스팅으로 전송한다.

③ IP임대 선택 (DHCP Request)

- 가장 먼저 도착한 DHCP Offer메시지에 Request 메시지로 응답한다.

④ IP임대 확인 (DHCP ACK)

- 서버에서 단말측으로 IP임대를 최종 확인한다.
- NACK를 전송하면 클라이언트는 처음과정부터 다시 시도한다.

⑤ IP임대 갱신 (IP Lease Renewal)

- 단말측에서 IP address단말 대여기간이 끝나기 전에 이미 사용중인 IP address사용기간을 갱신한다.

– 유효 대여 기간의 50% 남았을 때 처음 갱신 시도

– 총 대여 기간의 87.5%에 달했을 때 다시 한번 갱신 시도

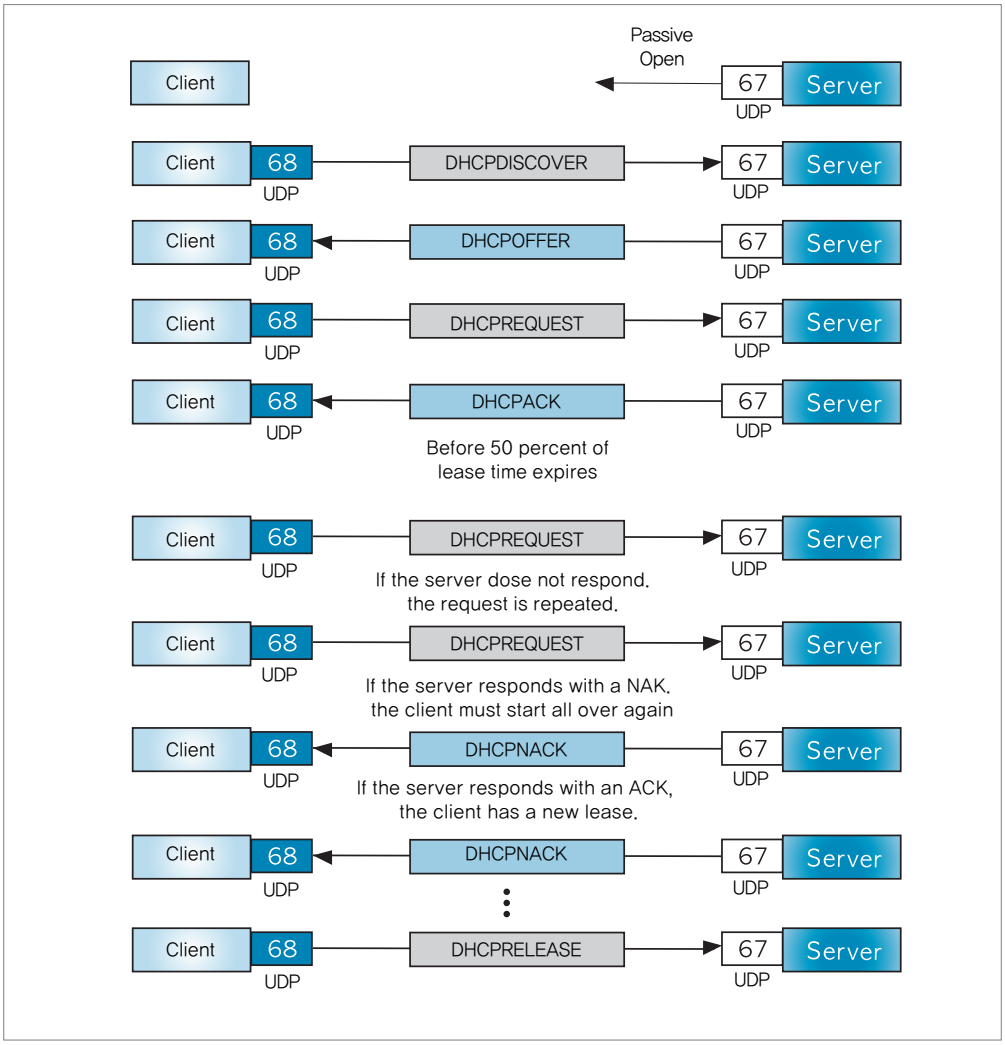
⑥ IP임대 제거 (DHCP Release)

– 단말에서 서버측으로 임대기간 이전에 임대를 종료하려면 Release 메시지 전송

다. DHCP 메시지 교환 순서

다음은 DHCP 서버와 클라이언트간 메시지 교환순서도이다.

(그림 부록 1-28) DHCP 메시지 교환 순서도



9. DNS 서버

(1) 개요

DNS는 IP와 도메인 이름간 번역 서비스를 제공하는 트리(Tree)형의 분산 데이터베이스이다. 클라이언트와서버 패러다임으로 구성되어 있으며 트리의 루트노드는 "."으로 표시한다. 각 노드는 서브트리의 루트 역할을 하며 위임을 통해 권한을 얻은 루트로부터 그권한이 영향을 미치는 노드들의 영역을 도메인(domain)이라 하고 각 도메인은 최소한 1개 이상의 네임서버(name server)를 가져야 한다.

(2) 주요기능

• IP주소와 도메인 이름(예: www.kisa.or.kr)간 번역 서비스 제공

(3) 동작구조

가. DNS 구성요소

DNS는 크게 리졸버(resolver)와 네임서버로 구성되며 이를 이용해 존과 도메인에 관한 정보를 표현한다.

1) 존(Zone)

존이란 네임서버에 의해 구분되는 데이터베이스 영역을 말하며 서브트리를 구성하는 자원레코드(RR : Resource Record)의 집합이라고 할 수 있다. 존에서는 표현할 데이터를 여러 RR 을 통해 구성하는데 여기서는 대표적으로 SOA RR, NS RR, A RR을 사용하여 구역 내의 모든 노드에 대한 신뢰성 있는 데이터, 구역의 상단 노드를 정의하는 데이터, 위임된 하위 존을 설명하는 데이터, 하위 존의 네임서버들에 대한 접근을 허용하는 데이터가 포함된다.

2) 도메인(Domain)

도메인이란 관리의 대상이 되는 개체들의 추상적인 영역을 말한다. DNS 에서는 하나의 서

브트리가 하나의 도메인을 이루며 트리 내에서의 등급에 의한 구분과, 위임에 따른 도메인 절단에 의한 구분이 가능하다.

3) 리졸버(Resolver)

리졸버란 호스트 명을 IP 주소로 전환하기 위한 일종의 모듈로서, 명칭 그대로 해결자 역할을 한다. DNS에서 발생하는 질의는 리졸버가 사용자 응용프로그램으로부터 받아들여 네임서버로 전송되고, 이에 대한 응답이 리졸버로 수신되면 사용자 응용프로그램으로 전송하게 된다.

4) 네임서버(Name Server)

도메인 데이터베이스를 구성하는 정보의 저장소로써, DNS 요청을 수신하게 되면 동작방식에 따라 결과를 리졸버에 돌려주는 역할을 한다. 네임서버에서 사용하는 동작방식으로는 비순환식과 순환식이 있다.

나. DNS 동작방식

DNS는 리졸버와 네임서버를 기본으로 하여 캐쉬(Cashe) 공유 데이터베이스와 외부의 DNS체계들로 구성된다. 여기서 외부의 DNS 체계는 DNS 동작에 필요한 요소들이며 내부와 외부의 체계는 연계 통해 존 트랜스퍼(zone trasnfer)나 외부로의 요청 및 응답관계가 성립된다.

리졸버는 지역네임서버와 데이터베이스를 공유하며 캐쉬된 정보의 내용을 얻거나 캐쉬정보를 추가하고 지역 네임 서버는 이 데이터베이스를 이용하여 외부로 보낸 질의에 대한 정보를 캐쉬할 수 있다.

사용자 응용프로그램이 도메인 명을 IP 주소로 전환하기 위한 질의(query)를 리졸버에 전송하면 리졸버는 이 정보를 질의 형식으로 바꾸어 처리를 시작한다. 만약 기존에도 같은 질의가 이루어져 캐쉬 정보가 공유 데이터베이스 내에 저장되어 있다면 리졸버는 사용자 응용프로그램에 바로 응답한후 처리가 끝나며, 그렇지 않을 경우 외부에 있는 네임서버에 이에 대한 질의를 보낸다. 외부의 네임서버는 전송 받은 질의에 대해 위에서 설명했던 네임 서버의 동작방식에 따라 처리를 한다. 비 순환식 동작에서는 해당 네임 서버 내에 응답할 수있는 데이터가 있

을 경우 리졸버에 응답을 보내며 그렇지 않을 경우 참조할 수 있는 다른 네임 서버의 주소를 알려 리졸버로부터 재전송된 질의를 통해 최종 응답을 보낸다. 순환식 동작 방식에서는 질의를 받은 네임서버가 다른 네임 서버들로부터 정보를 수집하여 최종 응답을 얻은 후에 리졸버에 그 응답을 보낸다.

네임 서버는 다른 네임 서버들과 정보의 동기화를 위해 유지관리가 필요하다. 여기서 주 네임서버와 부 네임서버의 구분이 이루어지며 SOA RR내에 명시되어 있는 필드들의 값을 이용하여 주기적으로 폴링(polling) 후 주 네임 서버로부터 존파일(zone file)을 전송받는다.

부록 2 BcN 시스템 운영체제별 시스템 해킹 위협 및 보호대책

1. 유닉스(리눅스) 운영체제 시스템 해킹 위협 및 보호대책

유닉스(리눅스) 시스템 해킹 위협	보호대책
• 미사용(퇴직, 휴직, 계약 해지자, guest, test 계정) 등이 삭제되지 않았을 경우, 이를 이용한 시스템 침투 위협 존재	• 퇴직, 전배, 휴직, 계약 해지자, guest, test 계정 등의 더 이상 사용되지 않는 계정 삭제 ※ userdel [사용되지 않는 계정]
• 디폴트 계정을 이용하여 시스템 침투할 위협 – OS, Package 설치시 디폴트로 생성되는 계정 (bin, deamon, adm, uucp, lp, nuucp) 등이 삭제되지 않았을 경우, 이를 이용하여 시스템 침투	• OS 및 설치시에 디폴트로 설정된 계정 삭제 혹은 lock ※ userdel [lp | uucp | nuucp | 의심스러운 특이한 계정]
• UID가 중복되어 관리자 권한으로 침투할 위협 – root (UID = 0)와 UID가 중복이 되어있으면 관리자 권한을 다른 사용자가 사용할 수 있으며, 사용자 간 UID 중복 시에 사용자 감사 추적이 어렵고, 사용자 권한이 중복되는 위협 존재	• UID/GID가 0인 일반계정 삭제, 적절한 UID/GID를 부여, root그룹에 속한 일반계정은 적절한 권한의 그룹에 등록
• Shell 제한이 안되어 관리자 권한으로 침투할 위협 – 접근이 필요하지 않은 사용자들의 계정을 이용하여 비인가자가 관리자 권한 획득	• 로그인이 필요하지 않는 계정에 /bin/false 쉘을 부여
• 취약한 패스워드를 이용하여 시스템 침투할 위협 – 패스워드가 없거나 계정과 동일한 패스워드를 사용하는 경우, 공격자가 시스템에 쉽게 접근 가능 – 쉬운 패스워드를 사용할 경우에도, 패스워드 추측 공격이나 해킹 도구에 의한 Cracking으로 시스템 접속 가능	• 패스워드 없는 계정의 로그인을 금지합니다. "/etc/default/login" 파일에 PASSREQ=YES 설정 • 계정과 동일, 유사하지 않은 6자 이상의 영문, 숫자, 특수문자의 조합으로 패스워드 재설정

유닉스(리눅스) 시스템 해킹 위협	보호대책
• 취약한 패스워드 정책으로 패스워드 크랙위협	• 패스워드 최소길이, 최대 사용기간, 최소 사용기간 설정
• 패스워드 파일 설정오류를 이용한 시스템 침입 – "/etc/passwd"파일이나 "/etc/shadow" 파일의 설정 상 문제점이나, 파일 권한(permission)의 설정 오류를 이용한 침입	• 패스워드 설정파일은 root만이 접근하도록 설정
• NFS 취약성을 이용한 시스템 해킹 위협	• 사용하지 않는다면 NFS 서비스는 제거 [서비스 제거 방법의 예] 1. "/etc/dfs/dfstab"나 "/etc/exports" 모든 공유를 제거 2. NFS 데몬(nfsd, statd, mountd)를 KILL하고 시동 스크립트인 "/etc/rc3.d/S · · nfs.server"와 "/etc/rc2.d/S · · nfs.client"를 제거
• 취약한 R-Command 서비스를 이용한 침투 위협	• 특별한 용도로 사용하지 않는다면 아래의 서비스를 제거 – shell(514), login(513), exec(512)
• 불필요한 서비스 포트 OPEN으로 인한 해킹 위협	• 사용하지 않는다면, 아래 서비스 제거 – echo(7), discard(9), daytime(13), chargen(19), time(37), tftp(69), finger(79), sftp(115), uucp-path(117), nntp(119), ntp(123), netbios_ns(137), netbios_dgm(138), netbios_ssn(139), bftp(152), ldap(389), printer(515), talk(517), ntalk(518), uucp(540), pcserver(600), ldaps(636), ingreslock(1524), www-ldap-gw(1760), nfsd(2049)-NFS미사용시, dtspcd(6112)
• root 원격 접근 허용으로 인한 스니핑 공격 위협	• CONSOLE 옵션 수정을 통해 root는 시스템 콘솔을 통해서만 접속할 수 있도록 설정 • 부득이한 경우, 일반 사용자로 접근하여 "su" 명령을를 통해 root권한으로 접속할 수 있도록 설정

유닉스(리눅스) 시스템 해킹 위협	보호대책
• 취약한 SetUID, SetGID를 통한 관리자 권한 획득 위협	• 보안에 취약한 root 소유의 SetUID 파일들의 경우, /usr/bin/passwd 파일과 같이 꼭 SetUID Bit을 가지고 있어야만 하는 파일도 있으므로 벤더와 협의 후 단계적으로 setui bit/setgi bit를 제거 ※ chmod –s file–name • 반드시 사용이 필요한 Setuid 파일의 경우에는 특정 그룹에서만 사용하도록 제한 **〈특정그룹 사용을 제한하는 예〉** ※ /usr/bin/chgrp 〈Group_Name〉 〈Setuid_File_Name〉 ※ /usr/bin/chmod 4750 〈Setuid_File_Name〉
• FTP 서비스의 오용으로 인한 관리자 권한 획득 위협	• /etc/ftpusers 파일에 ftp 서비스 접근 불가계정 등록 – 주로 아래의 계정들은 FTP 서비스를 제한할 것을 권고 ⇒ root, daemon, bin, sys, adm, lp, smtp, uucp, nuucp, listen, nobody, noaccess, nobody4
• Anonymous FTP 서비스의 오용으로 인한 중요 정보 유출 위협	• 익명 사용자의 ftp 접근 제한 ※/etc/passwd 파일에 ftp 계정이 삭제
• SNMP 설정 오류로 인한 시스템 정보의 유출	• SNMP 서비스 제거 ※ ps –ef | grep snmp ※ kill · 9 247 ※ cd /etc/rc3.d ※ mv S76snmpdx /rc–mv • snmpd.conf 파일에서 community string 변경
• Sendmail 취약성으로 인한 관리자 권한획득 및 주요정보 유출 위협	• Sendmail 서비스 제거 • 취약점 패치된 Sendmail 버전 유지하고, 취약점 패치 발표시 바로 적용

유닉스(리눅스) 시스템 해킹 위협	보호대책
• Bind 취약성으로 인한 관리자 권한 획득 및 시스템 주요정보 유출 위협	• 시스템 초기 설치 후, 불필요한 DNS서비스 제거 [DNS 서비스 제거 방법 예] ※ ps –ef | grep named ※ kill –9 279 ※ cd /etc/rc3.d ※ mv S79named /rc–mv
• 백도어를 통한 시스템 침입 위협	• 자주 사용되고 있는 백도어 포트를 확인하며 백도어로 의심되는 파일이 발견될 경우, 파일이 언제 누구에 의해 생성되었는지 ls –asl, ls –aslc 명령으로 점검한 뒤, 파일 삭제 • 백도어 예방, 탐지를 위한 대책 1) 시스템 및 네트워크 침입차단시스템 2) 네트워크 침입방지시스템 3) 무결성 점검 시스템 적용 4) 주기적인 취약점 점검
• Trojan을 통해 침입흔적을 숨기거나, 관리자 권한을 획득할 위협	• Trojan 프로그램(백도어 포함)에 대한 대책으로는 주기적인 무결성 점검이 중요함 – 무결성 점검을 위해서는 TripWire 등의 도구를 활용할 수 있으며, 대부분의 상용 취약성 점검 Scanner에는 이러한 기능이 탑재되어 있으므로 이를 활용하여 주기적으로 점검 수행 **[점검 대상 루트킷]** – Adore LKM(Loadable Kernel Module) – Knark LKM(Loadable Kernel Module) – T0rn 루트킷 – T0rn v8 루트킷 – Monkit 루트킷 – HiDrootkit 루트킷 – RSHA 루트킷 – RH–Shaper 루트킷 – Ark 루트킷 – LPD 루트킷 – Maniac 루트킷 – RK17 루트킷 – Ducoci 루트킷 – 의심스러운 LKM(Loadable Kernel Module) – Renzo 루트킷 등
• 보안패치 미적용으로 침해 및 장애 위협 존재	• 시스템의 보안성 및 안전성을 위하여 주기적으로 패치를 적용

2. 원도우 운영체제 시스템 해킹 위협 및 보호대책

윈도우 시스템 해킹 위협	보호대책
• 미사용(퇴직자 등) 계정을 이용 시스템 침투할 위험	• 퇴직, 전배, 휴직, 계약 해지자, guest, test 계정 등의 더 이상 사용되지 않는 계정 삭제, Administrator 계정은 다른 이름의 계정 사용 **[Guest 계정에 대한 사용 제한 설정]** – 설정〉제어판〉관리도구〉컴퓨터관리〉로컬 사용자 및 그룹〉사용자 선택하여 Guest 계정 등록정보에서 사용제한 설정
• 관리자권한을 이용 시스템 침투 위협	• 서버담당자(2~3명)만 접근 제한
• 취약한 패스워드를 이용하여 시스템 침투할 위험	• 패스워드 없는 계정의 로그인 금지 • 자신의 계정과 동일하거나 유사하지 않은 8자 이상의 영문, 숫자, 특수문자 조합으로 암호 설정 **[피해야 할 암호설정]** – Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자성명, 대표업무명, "root", "rootroot", "root123", "123root", "admin", "admin123" 등
• 취약한 패스워드 정책으로 패스워드 Cracking을 용이하게 할 위험	• 암호정책 설정 **[예제]** – 최대 암호 사용 기간 30~90일 – 최소 암호 사용 기간 1일 – 최소 암호 길이 6 문자 – 암호 유일성 12개 암호 기억 등
• Brute force 공격이나 패스워드 크랙공격에 노출될 위험	• 계정잠금 정책 설정 – 5번 잘못된 로그온 시도후 계정잠금 – 횟수 다시 설정 60분 후 – 잠금 유지 시간 60분 등
• 불필요한 서비스 포트 OPEN으로 인한 해킹 위협	• Netstat –an 명령을 통해 열려진 포트 조사하여 불필요한 포트 막음
• 불필요 서비스 운영으로 인한 해킹 위험	• 업무에 부합되는 서비스가 아닌 기타 디폴트 서비스를 사용하지 않음

윈도우 시스템 해킹 위협	보호대책
• 배너설정 오류로 인한 시스템 정보 유출 위험 – 시스템에 일반적인 서비스(HTTP, FTP, SMTP 등)의 접근시 출력되는 배너(Banner)를 통해 서비스 버전 정보 등 시스템 주요 정보 유출 가능	• 배너정보를 제거하여 시스템 정보 등의 유출 방지
• 널 세션접근 획득 위협 – Windows NT/W2K는 비인가된 사용자가 Null Session을 통해 사용자 인증을 거치지 않고 서버에 접근, 시스템 내부로의 접근 가능	• 인증된 사용자만 접속허용 1. 시작〉실행〉regedit 를 실행 2. HKLM\SYSTEM\CurrentControlSet\Control\LSA 레지스트리를 검색. 3. 오른쪽 버튼을 눌러 새로만들기|DWORD값을 선택. 4. RestrictAnonymous 를 입력. 이때 값은 Default 값인 0 을 다음 값으로 변경. (Windows 2000 = 2, Win NT = 1, Windows XP = 1) • 방화벽과 라우터에서 135~139(TCP, UDP)포트의 차단을 통해 외부로부터의 위협을 차단하도록 함. • 원천적으로 봉쇄. – 네트워크 및 전화 접속〉연결〉로컬영역〉등록정보〉고급〉고급설정〉Microsoft네트워크파일 및 프린트공유 해제
• 터미널 서비스를 이용한 해킹 위험	• 불필요한 터미널 서비스 중지 • 터미널 서비스 제공시, – 관리자 이외의 일반 사용자의 터미널 서비스 접속을 허용하지 않음. 방화벽에서 터미널 서비스 포트(3389)의 사용을 관리자 컴퓨터의 IP로 제한. – 다수의 계정이 필요한 경우 엄격한 ACL(Access Control List)을 적용.
• Idle Time을 이용한 세션 하이젝킹 위험	• 일정시간후 연결 자동 끊김 설정
• 레지스트리 편집기를 이용해 원격 접속하여 수정 위험	• Remote Registry Service 비활성화

윈도우 시스템 해킹 위협	보호대책
• Autologon 기능을 이용한 비허가자에 의한 시스템 정보 유출 위험	• Autologon 기능중지 1. 시작〉실행〉regedt32를 실행 2. HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon 3. AutoAdminLogon 값을 0으로 세팅. 4. DefaultPassword 엔트리가 존재한다면 삭제
• 시스템의 물리적 셧다운 위험	• 로그온 박스의 시스템 종료 버튼 삭제 **[예제]** HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon Name : ShutdownWithoutLogon Data Type : REG_SZ Value :0
• 사용자 계정정보 노출 위험	• 제어판〉관리도구〉로컬 보안 정책〉보안 설정〉로컬 정책 〉보안 옵션〉로그온 스크린〉 마지막 사용자 이름 표시 안함
• 잠김 미설정시 자리 이탈시 시스템 정보 유출 위험	• 스크린 세이버 적용
• FTP 서비스의 오용으로 인한 관리자 권한 획득 위험	• FTP 서비스 제공시 보안설정 **[예제-절차]** 1. Default 설정으로 되어 있는 익명연결 허용 금지 2. FTP 를 위한 계정을 따로 만들어서 사용합니다. 3. Password 복잡도 높이고, 권한제한 4. Home Directory는 Default로 설정하지 말고, 임의의 폴더를 생성 금지
• SNMP 설정 오류로 인한 시스템 정보의 유출 위험	• 불필요한 SNMP 서비스 제거 • SNMP 서비스 사용시 보안조치 – 디폴트 커뮤니티스트링(public, private) 변경합니다. **[예제]** 제어판〉관리도구〉서비스〉SNMP Servies〉 등록정보〉보안탭〉커뮤니티 이름 편집
• Telnet 통신 정보 유출 위험	• SSH, IPsec 등을 이용한 암호화 통신 권장

부록 3 BcN 주요장비별 정보보호 체크리스트

[표 부록 3-1] BcN 장비별 위협에 대한 보호대책(안)

위협		공격대상						
		소프트 스위치	CM TS	SIP 서버	Gate way	MPLS 라우터	DH CP	DNS
서비스 거부공격	1. 시스템 자원고갈							
	(1) 대량 SIP INVITE 메시지 전송	●		●				
	(2) 대량의 DHCP Request 메시지 전송						●	
	(3) 대량의 IP 패킷 전송	●	●	●	●	●	●	●
	2. 비정상 메시지 전송							
	(1) 연결 해제 또는 종료 메시지 전송	●		●				
	(2) 비정상 등록 메시지 전송	●		●				
	(3) MPLS 라우팅 정보 변경					●		
	3. 네트워크 경로자원 고갈		●		●	●		
서비스품질 (QoS)저하	1. QoS가 조작된 패킷 인입		●	●	●	●		
	2. DiffServ 자원절도					●		
	3. 잡음 삽입				●	●		
시스템 해킹	1. 시스템 설정 오류	●	●	●	●	●	●	●
	2. 원격접속 프로토콜 취약점	●	●	●	●	●	●	●
	3. 운영체제 및 어플리케이션 취약점	●	●	●	●	●	●	●

위협		공격대상						
		소프트스위치	CMTS	SIP서버	Gateway	MPLS라우터	DHCP	DNS
도청	1. 연동장비 해킹을 통한 도청	●	●	●	●	●		
	2. 전송패킷 분석을 통한 도청	●	●	●	●	●		
	3. 세션 가로채기를 통한 도청	●	●	●	●			
	4. Fake DHCP 서버 운영을 통한 도청						●	
메시지 위·변조	1. 사용자 등록 메시지 위·변조	●		●				
	2. 가입자 정보 위·변조	●		●				
	3. 세션 연결 메시지 위·변조	●	●	●	●			
	4. 라우팅 메시지 위변조					●		

1.소프트스위치

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량 SIP INVITE 메시지 전송	• SSW에 대한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 단위 시간당 INVITE 메시지 처리량을 제한하고 있는가?	상	
	• 통합 모니터링 및 보안관제를 수행하여 대량의 INVITE 패킷 폭주시, 패킷 전송 근원지 차단을 실시하고 있는가?	중	
	• 외부에서 메시지 처리장비에 직접 접근할 수 없도록 하거나, 접근을 통제할 수 있는 네트워크 구조 운영하고 있는가?	상	
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
대량의 IP 패킷 전송	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	상	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	하	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
연결 해제 또는 종료 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 메시지 전송채널 보호 또는 S/MIME 암호화 등을 사용하여 메시지를 보호하고 있는가?	중	
비정상 등록 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 메시지 전송채널 보호 또는 S/MIME 암호화 등을 사용하여 메시지를 보호하고 있는가?	중	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	상	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	상	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
• 시스템 설정 오류	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 시스템의 웜 · 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	상	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	상	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	상	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	상	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
■ 도청			
• 연동장비 해킹을 통한 도청	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	상	
	• 시스템 내에서 사용자 역할에 따라 접근영역을 분리하여 운영하고 있는가?	하	
• 전송패킷 분석을 통한 도청	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 회선공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 스니핑 방지를 위한 네트워크 환경을 구성하여 운영하고 있는가?	하	
• 세션 가로채기를 통한 도청	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	
■ 메시지 위 · 변조			
• 사용자 등록 메시지 위 · 변조	• 암호화 등을 사용하여 서비스 등록 메시지를 보호하고 있는가?	중	
	• 서비스 등록 과정에서 상호인증 메커니즘을 적용하고 있는가?	상	
• 가입자 정보 위 · 변조	• 시스템에 대한 해킹 차단을 위한 적절한 대책을 수립운영하고 있는가? ※ 해킹위협 점검결과를 반영	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
• 가입자 정보 위·변조	• 서비스 제공 기능(서버)과 가입자 정보(Database)간 기능영역을 분리하여 운영하고 있는가?	중	
	• 가입자 정보 저장데이터에 대한 무결성 검사를 주기적으로 실시하고 있는가?	중	
	• 가입자 정보 보호를 위한 관련 법규, 지침 및 절차 등의 준수하고 있는가?	중	
• 세션 연결 메시지 위·변조	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	

2. CMTS

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
대량의 IP 패킷 전송	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
• 네트워크 경로자원 고갈	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 네트워크 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• 단위시간당 일정량 이상인 트래픽 유입을 차단하고 있는가?	중	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템 및 네트워크에 대한 백업 및 장애대응 절차를 수립 · 운영하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
■ 서비스 품질(QoS) 저하			
• QoS 가 조작된 패킷 인입	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 암호화 등을 사용해 메시지 전송채널을 보호하고 있는가?	중	
	• 네트워크 QoS 자원 모니터링 및 QoS 자원 사용량을 통제하고 있는가?	중	
	• 서비스별, 사용자별 단위시간당 전송 패킷량을 제한하고 있는가?	중	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	

위협	정보보호 체크리스트	중요도	적용여부
• QoS 가 조작된 패킷 인입	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	중	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	중	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 시스템의 웜 · 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 운영체제 및 어플리케이션 취약점	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	하	
■ 도청			
• 연동장비 해킹을 통한 도청	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 시스템 내에서 사용자 역할에 따라 접근영역을 분리하여 운영하고 있는가?	하	
• 전송패킷 분석을 통한 도청	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 스니핑 방지를 위한 네트워크 환경을 구성하여 운영하고 있는가?	하	
• 세션 가로채기를 통한 도청	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	하	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	

위협	정보보호 체크리스트	중요도	적용여부
■ 메시지 위·변조			
• 세션 연결 메시지 위·변조	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	

3. SIP 서버

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량 SIP INVITE 메시지 전송	• 시스템 대한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 단위 시간당 INVITE 메시지 처리량을 제한하고 있는가?	상	
	• 통합 모니터링 및 보안관제를 수행하여 대량의 INVITE 패킷 폭주시, 패킷 전송 근원지 차단을 실시하고 있는가?	중	
	• 외부에서 메시지 처리장비에 직접 접근할 수 없도록 하거나, 접근을 통제할 수 있는 네트워크 구조 운영하고 있는가?	상	
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
대량의 IP 패킷 전송	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	하	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
연결 해제 또는 종료 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 메시지 전송채널 보호 또는 S/MIME 암호화 등을 사용하여 메시지를 보호하고 있는가?	상	
비정상 등록 메시지 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 서비스 사용자 및 기기에 대해 인증 메커니즘 을 적용하고 있는가?	상	
	• 메시지 전송채널 보호 또는 S/MIME 암호화 등을 사용하여 메시지를 보호하고 있는가?	상	
■ 서비스품질 (QoS) 저하			
• QoS가 조작된 패킷 인입	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 암호화 등을 사용해 메시지 전송채널을 보호하고 있는가?	상	
	• 네트워크 QoS 자원 모니터링 및 QoS 자원 사용량을 통제하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• QoS가 조작된 패킷 인입	• 서비스별, 사용자별 단위시간당 전송 패킷량을 제한하고 있는가?	중	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	상	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	상	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	상	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 시스템의 웜? 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
• 운영체제 및 어플리케이션 취약점	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	하	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜?바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	상	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	
■ 도청			
• 연동장비 해킹을 통한 도청			
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 시스템 내에서 사용자 역할에 따라 접근영역을 분리하여 운영하고 있는가?	하	
• 전송패킷 분석을 통한 도청	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	상	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 스니핑 방지를 위한 네트워크 환경을 구성하여 운영하고 있는가?	하	
• 세션 가로채기를 통한 도청	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
• 세션 가로채기를 통한 도청	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	
■ 메시지 위 · 변조			
• 사용자 등록 메시지 위 · 변조	• 암호화 등을 사용하여 서비스 등록 메시지를 보호하고 있는가?	상	
	• 서비스 등록 과정에서 상호인증 메커니즘을 적용하고 있는가?	상	
• 가입자 정보 위 · 변조	• 시스템에 대한 해킹 차단을 위한 적절한 대책을 수립운영하고 있는가? ※ 해킹위협 점검결과를 반영	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 서비스 제공 기능(서버)과 가입자 정보(Database)간 기능영역을 분리하여 운영하고 있는가?	중	
	• 가입자 정보 저장데이터에 대한 무결성 검사를 주기적으로 실시하고 있는가?	중	
	• 가입자 정보 보호를 위한 관련 법규, 지침 및 절차 등의 준수하고 있는가?	중	
• 세션 연결 메시지 위 · 변조	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	상	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	

4. 게이트웨이

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	상	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
• 네트워크 경로자원 고갈	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 네트워크 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	상	
	• 단위시간당 일정량 이상인 트래픽 유입을 차단하고 있는가?	상	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템 및 네트워크에 대한 백업 및 장애대응 절차를 수립 · 운영하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 네트워크 경로자원 고갈	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
■ 서비스품질 (QoS) 저하			
• QoS가 조작된 패킷 인입	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 암호화 등을 사용해 메시지 전송채널을 보호하고 있는가?	중	
	• 네트워크 QoS 자원 모니터링 및 QoS 자원 사용량을 통제하고 있는가?	중	
	• 서비스별, 사용자별 단위시간당 전송 패킷량을 제한하고 있는가?	중	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
• 잡음 삽입	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 서비스를 제공받는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 암호화 등을 사용해 미디어 전송채널을 보호하고 있는가?	중	
	• 컨텐츠 보호를 위해 미디어 데이터에 암호화 등을 적용하고 있는가?	중	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	상	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 시스템 설정 오류	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 시스템의 웜 · 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	
■ 도청			
• 연동장비 해킹을 통한 도청	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	상	
	• 시스템 내에서 사용자 역할에 따라 접근영역을 분리하여 운영하고 있는가?	하	
• 전송패킷 분석을 통한 도청	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 스니핑 방지를 위한 네트워크 환경을 구성하여 운영하고 있는가?	하	
• 세션 가로채기를 통한 도청	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	
■ 메시지 위 · 변조			
• 세션 연결 메시지 위 · 변조	• 메시지 무결성 검증이 가능한 서비스 프로토콜을 사용하고 있는가?	중	
	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 세션 가로채기를 방지할 수 있도록 네트워크 환경을 구성하여 운영하고 있는가?	하	

위협	정보보호 체크리스트	중요도	적용여부
• 세션 연결 메시지 위·변조	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를 점검하여 조치하고 있는가?	중	
	• 특정 시스템에 집중되는 과도 트래픽 유발 시스템을 모니터링하여 조치하고 있는가?	하	

5. MPLS 라우터

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	상	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
MPLS 라우팅 정보 변경	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 라우팅 정보를 관리하는 서비스 사용자 및 관리를 위해 접근하는 시스템에 대해 인증 메커니즘 을 적용하고 있는가?	중	
	• MPLS 라우팅 정보 교환 프로토콜에 보안 메커니즘을 적용하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 네트워크 경로자원 고갈	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 웜?바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 네트워크 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• 단위시간당 일정량 이상인 트래픽 유입을 차단하고 있는가?	중	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템 및 네트워크에 대한 백업 및 장애대응 절차를 수립 · 운영하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
■ 서비스품질 (QoS) 저하			
• QoS가 조작된 패킷 인입	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 암호화 등을 사용해 메시지 전송채널을 보호하고 있는가?	중	
	• 네트워크 QoS 자원 모니터링 및 QoS 자원 사용량을 통제하고 있는가?	중	
	• 서비스별, 사용자별 단위시간당 전송 패킷량을 제한하고 있는가?	상	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• DiffServ 자원절도	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 암호화 등을 사용해 메시지 전송채널을 보호하고 있는가?	중	
	• QoS 서비스를 제공받는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 네트워크 QoS 자원 모니터링 및 QoS 자원 사용량을 통제하고 있는가?	중	
	• 서비스별, 사용자별 단위시간당 전송 패킷량을 제한하고 있는가?	상	
	• 전송 경로 이중화 및 우회경로를 확보하고 있는가?	하	
	• 시스템 및 네트워크 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 실시하고 있는가?	중	
• 잡음 삽입	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 서비스를 제공받는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 암호화 등을 사용해 미디어 전송채널을 보호하고 있는가?	중	
	• 컨텐츠 보호를 위해 미디어 데이터에 암호화 등을 적용하고 있는가?	중	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	중	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	중	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	

위협	정보보호 체크리스트	중요도	적용여부
• 시스템 설정 오류	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 시스템의 웜 · 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	중	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
■ 도청			
• 연동장비 해킹을 통한 도청	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 시스템 내에서 사용자 역할에 따라 접근영역을 분리하여 운영하고 있는가?	하	
• 전송패킷 분석을 통한 도청	• 암호화 등을 사용해 제어/미디어/사용자 데이터를 보호하고 있는가?	중	
	• 네트워크 공유 구간에서 정기적인 스니핑 도구 동작여부를		
	점검하여 조치하고 있는가?	중	
	• 스니핑 방지를 위한 네트워크 환경을 구성하여 운영하고 있는가?	하	
■ 메시지 위 · 변조			
• 라우팅 메시지 위 · 변조	• 시스템에 대한 해킹 차단을 위한 적절한 대책을 수립운영하고 있는가? ※ 해킹위협 점검결과를 반영	상	
	• uRPF 등 라우터의 보안기능을 활성화하여 운영하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 라우팅테이블에 대한 무결성 검사를 주기적으로 실시하고 있는가?	중	

6. DHCP 서버

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량의 DHCP Request 메시지 전송	• DHCP Request 요청 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 단시간 대량의 DHCP Request 메시지를 요청하는 시스템 차단 대책을 마련하고 있는가?	상	
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	상	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	상	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	상	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	

위협	정보보호 체크리스트	중요도	적용여부
• 시스템 설정 오류	• 시스템의 웜? 바이러스를 주기적으로 차단하고 있는가?	상	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	상	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	상	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	중	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	상	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	
■ 도청			
• Fake DHCP 서버 운영을 통한 도청	• DHCP 트래픽 모니터링을 통해 비인가된 DHCP 서버운영을		

위협	정보보호 체크리스트	중요도	적용여부
• Fake DHCP 서버 운영을 통한 도청	감시하여 조치하고 있는가?	상	
	• 네트워크 장비에서 DHCP 인가(Trust) 포트 설정하여 운영하고 있는가?	하	
	• 비인가 DHCP 서버의 네트워크 접속을 차단할 수 있도록 관리활동을 수행하고 있는가?	중	

7. DNS 서버

위협	정보보호 체크리스트	중요도	적용여부
■ 서비스 거부공격			
• 시스템 자원고갈			
대량의 IP 패킷 전송	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 인입 패킷의 Rate-Limit 기술을 적용하여 단위시간당 일정량의 패킷이상으로 트래픽 유입을 차단하고 있는가?	중	
	• 시스템 자원 및 트래픽에 대한 모니터링 및 이상 트래픽을 통제하고 있는가?	중	
	• uRPF 기능 등을 적용하여 가입자 단에서 IP 주소를 위조하여 인입되는 대량 패킷을 차단하고 있는가?	중	
	• 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템의 Backlog Queue 사이즈를 늘려서 운영하고 있는가?	하	
■ 시스템 해킹			
• 시스템 설정 오류	• 시스템 설치시 또는 설치 후 기본설정값을 적절하게 변경하였는가?	상	
	• 시스템 설치후, 최신 업데이트 및 보안패치를 실시하였는가?	상	
	• 시스템 설치 후, 주요시스템 관리자 암호를 영문/숫자/특수문자 등을 사용하여 8자 이상으로 변경하였는가?	상	
	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한		

위협	정보보호 체크리스트	중요도	적용여부
• 시스템 설정 오류	ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	상	
	• 시스템의 웜 · 바이러스를 주기적으로 차단하고 있는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
• 원격접속 프로토콜 취약점	• 관리자 모드 전송 데이터에 암호화를 적용하고 있는가?	중	
	• 시스템에 접근하는 원격접속 시스템의 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 시스템 관리를 위한 원격 관리자 및 시스템에 대한 인증 메커니즘을 적용하고 있는가?	상	
	• 관리를 위한 원격접속 시 보안이 강화된 원격접속 프로토콜을 사용하고 있는가?	상	
• 운영체제 및 어플리케이션 취약점	• 시스템에 접근하는 비인가 IP주소, 프로토콜 접속 차단 등을 위한 ACL 설정 또는 Firewall 등을 운영하고 있는가?	중	
	• 공격대상 선정을 위한 스캐닝 공격 탐지를 수행하고 있는가?	중	
	• 시스템 공격을 위한 침입시도를 탐지하고 있는가?	상	
	• 운영체제 및 응용 프로그램 최신 보안패치 및 업그레이드를 주기적으로 수행하고 있는가?	상	
	• 시스템에서 불필요한 서비스를 제거하였는가?	중	
	• 시스템 내의 비인가 프로세스를 주기적으로 검사하여 조치하고 있는가?	중	
	• 웜 · 바이러스 및 유해트래픽에 대한 자동차단을 실시하고 있는가?	중	
	• 시스템에 대한 통합 모니터링 및 보안 관제를 실시하고 있는가?	중	
	• 시스템에 접근하는 사용자 및 장비에 대해 인증 메커니즘을 적용하고 있는가?	중	
	• 주기적으로 시스템에 대한 취약점 점검 및 조치를 실시하고 있는가?	중	

광대역통합망(BcN) 주요장비에 대한 정보보호가이드(V1.0) 개발을 위해 다음과 같은 분들께서 수고 하셨습니다.

2006년 12월

총괄 책임자	**정보통신부 정보보호정책팀**	**팀 장 서 석 진**
	한국정보보호진흥원 IT기반보호단	**단 장 이 재 일**
사업 참여자	정보통신부 정보보호정책팀	사 무 관 우 영 규
	한국정보보호진흥원 IT기반기획팀	팀 장 이 강 신
	한국정보보호진흥원 IT기반기획팀	수석연구원 김 호 성
	한국정보보호진흥원 IT기반기획팀	주임연구원 신 동 훈
	한국정보보호진흥원 IT기반기획팀	주임연구원 허 준
검 토	데이콤	부 장 정 내 준
(가나다 순)	데이콤	과 장 구 자 현
	순천향대학교	교 수 염 흥 렬
	숭실대학교	교 수 정 수 환
	숭실대학교	최 재 덕
	하나로텔레콤	부 장 반 총 섭
	하나로텔레콤	과 장 김 영 민
	한국외국어대학교	교 수 정 일 영
	한국정보사회진흥원(NIA)	팀 장 하 상 용
	한국정보사회진흥원(NIA)	선임연구원 조 일 권
	ETRI	책임연구원 강 성 수
	KT	부 장 정 창 성
	KT	과 장 허 원
	SKT	부 장 박 선 호
	SKT	차 장 이 채 헌
	TTA	팀 장 김 선

광대역통합망(BcN) 주요장비에 대한 정보보호가이드(V1.0)

2006년 12월 인쇄
2006년 12월 발행

발행처 : **정보통신부 · 한국정보보호진흥원**

서울특별시 종로구 세종로 100번지
통신센터빌딩 정보통신부
Tel: (02) 750-2114

서울특별시 송파구 가락동 78번지
IT벤처타워(서관) 한국정보보호진흥원
Tel: (02) 405-5114

인쇄처 : 한올
Tel : (02) 2279-8494