

Bluetooth Protocol Stack

임영희

시코드 연구소장



1. 서론

최근 들어 이동통신기와 IMT2000의 등장은 무선인터넷의 보급을 가속화시켰다. 일상생활에서 인터넷을 사용하는 것은 그리 어려운 일이 아니다. 또한 통신기능이 내장되어 있지 않은 디바이스들 간의 무선 네트워크를 구축할 수 있는 필요성이 대두되었고, 이러한 필요성에 따라 전력선 통신, 소형 인터넷 접속기기, 무선 LAN, IrDA 등이 등장하게 되었다. 그러나 최근 등장한 블루투스(Bluetooth)¹⁾는 앞에서 언급한 다른 어떠한 통신방식보다 통신기능이 내장되어 있지 않은 디바이스들 간의 무선 네트워크를 쉽고, 값싸게 구현할 수 있도록 도와주고 있다. 즉 블루투스는 휴대폰, PDA, PC, 심지어 TV, 냉장고와 같은 모든 가전기기의 네트워크 시대를 열어줄 기술로서 정보통신시장에 새로운 활력을 불어일으킬 주역으로 관심을 모으고 있다.

블루투스는 94년 에릭슨(Ericsson)이라는 이동통신그룹이 휴대폰과 주변기기 사이의 소비전력이 낮고 저가격의 무선통신 인터페이스를 연구하기시작하면서 태동되었다. 96년 2월에 에릭슨, 노키아, IBM, 도시바, 인텔로 구성된 블루투

스 SIG(Special Interest Group, <http://www.bluetooth.com>)를 결성하였으며, 지금은 9개의 기업(Microsoft, Lucent, 3Com, Motorola)으로 확장되었다. 지금 활동하고 있는 어댑터 그룹은 2491개인 것으로 알려져 있다.

블루투스 기술은 저가격대(칩 가격기준으로 5달러), 적은 소모전력(100mW)으로 휴대폰, PDA, 휴대용 노트북 등과 같은 휴대용장치들 간의 작은 반경(10m 또는 100m)내에서 2.4Ghz의 ISM(Industrial, Scientific, and Medicao) 밴드 주파수대역을 사용하여 무선 네트워크를 구성하는 기술이다. 이 때 사용되는 출력은 10m용에서는 0dBm, 100용에서는 +20dBm의 출력이 가능한 전력증폭기를 사용한다. 블루투스 네트워크에서는 1대 1 통신, 1대 n 통신연결을 지원하고 있다. 하나의 서버를 중심으로 주위의 디바이스들과 네트워크를 구성하게 되는데 이것을 피코넷(Piconet)이라 한다. 또한 피코넷 주위로 다른 피코넷을 형성할 수 있고, 이러한 피코넷 사이에는 항상 중개역할을 하는 디바이스가 존재하게 된다. 즉 하나의 피코넷을 중심으로 여러 피코넷이 형성되어진다. 이러한 피코넷의 모임을 스캐터넷(Scatternet)이라 한다. 이러한

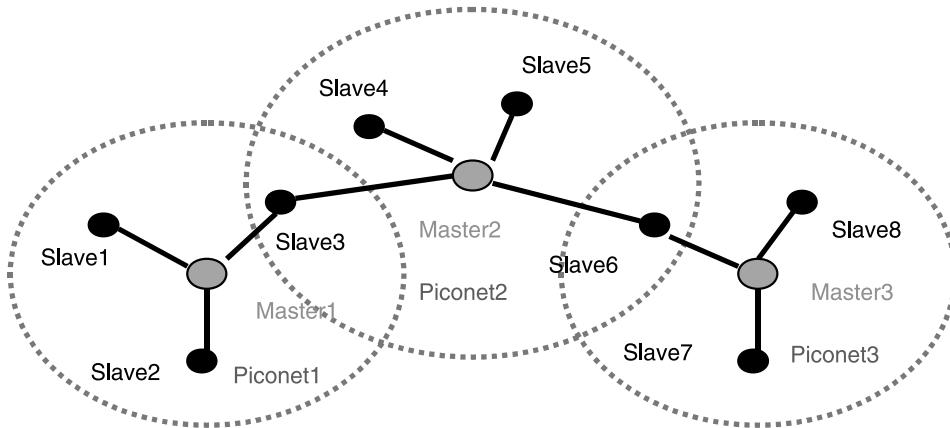


그림 1. Bluetooth Piconet Example

에는 그림 1과 같다²⁾.

블루투스에서는 비동기적인 데이터채널과 동기식 데이터음성채널이 존재하게 된다. 음성 채널은 64Kbps의 동기화 링크를 지원하며 3개까지 한꺼번에 확보할 수 있다. 비동기식 채널에서 다운 링크는 최대 721Kbps, 업 링크는 57Kbps를 제공하며, 대칭전송시 432.6Kbps의 동기식 링크를 제공하고 있다²⁾.

블루투스에서 사용되는 전력모드는 총 7가지를 지원하고 있다. 7가지 전력모드는 Standby Mode, Inquiry Mode, Page Mode, Active Mode, Park Mode, Hold Mode, Sniff Mode이다²⁾.

앞에서는 무선 네트워크를 구성할 수 있는 블루투스 기술에 대한 전반적인 소개를 하였다. 본 글에서는 블루투스 기술의 핵심이 될 수 있는 프로토콜 스택에 대한 구성 및 내용을 간단히 소개하도록 하겠다. 이 글이 블루투스의 상용화를 앞당길 수 있는 바탕이 되었으면 한다.

2. 블루투스¹⁾, 무선 LAN³⁾, HomeRF⁴⁾의 비교

근거리 무선데이터 통신에 사용되는 대표적인 기술은 블루투스를 비롯해 IEEE802.11 (Wireless LAN), 홈 RF, IrDA⁵⁾등이 있으나 특히 블루투스가 가장 주목을 받고 있다. 블루투스는 비교적 간단한 통신방식을 채용하고 있고, 세계적인 칩 메이커와 휴대전화 메이커들의 참여에 따라 저가격, 대량생산을 기대할 수 있다. 또한 그 응용분야의 다양화로 시장점유도가 매우 높을것으로 기대되어지고 있다. 블루투스에서 사용되고 있는 주파수 대역이 ISM 밴드로 거의 전세계 공통으로 사용하고 있으므로 제품의 판매대상이 전세계가 될 수 있다는 장점도 가지고 있다. 이렇듯 다른 경쟁방식들에 비교하여 블루투스는 많은 장점을 가지고 있으며 앞으로 근거리 무선데이터 통신에서 가장 주목받는 통신규약으로 발전할 것이다. 근거리 무선데이터 통신기술들에 대한 기술규격 비교는 표 1과 같다.

표 1. 근거리 무선데이터 통신규약의 비교

		블루투스	홈 RF	IEEE 802.11
주요 참여업체		Ericsson, Intel, IBM, Nokia, Thosiba	Microsoft, Intel, IBM, HP, Compact	Harris, 3COM, Lucent, Symbol, Aironet
표준	버전	SIG 1.1	SWAP 1.11	IEEE 802.11 RevD10
	기술	RF 2.4GHz, FHSS	RF 2.4GHz, FHSS	RF 2.4Ghz, FHSS, DSSS, irDA
	Power	0 ~20dBm	<20dBm	<20dBm
	전송속도	1 MS/s	0.8/1.6 MS/s	11MS/s
	통신거리	10m, 100m	50/100m	30m
	Topology	8piconet, point-to-multi	128 CSMA	128 CSMA
	보안	Authentication Encryption	optional	Optional
	주파수 호핑	79ch, 1600hop/sec	79ch, 50hop/sec	79ch, 2.5hop/sec
	Protocol	Link Manager, L2CAP	Ethernet	Ethernet
응용분야		Mobile Phone, Mobile Computer	Home WLAN	WLAN

3. 블루투스 프로토콜 스택의 구성²⁾

6), 7)

프로토콜의 구성은 크게 3가지로 구분되어진 다. 첫번째로 블루투스 하드웨어와 밀접한 관계를 가지고 있으며 또한 펌웨어(Firmware) 형태로 제공되어지는 Link Manager, HCI(Host Controller Interface) 등이 있다. 이것들은 베이스밴드(Baseband) 소프트웨어라고 한다. 이것은 보통 칩 제조업체에서 제공하고 있으며 그 구성은 아래와 같다.

- 베이스밴드 소프트웨어
- Link Manager
- Link Manager Protocol
- HCI 호스트 컨트롤러 부분
- UART 인터페이스 소프트웨어
- USB 인터페이스 소프트웨어

두 번째로 호스트에 존재하게 되는 프로토콜 스택은 PC나 PDA와 같은 운영체제가 존재하는 곳에 설치되는 소프트웨어로 그 구성은 아래와 같다.

- HCI 호스트 인터페이스
- L2CAP(Logical Link Control and Adaptation Protocol)
- SDP(Service Discovery Protocol)
- RFCOMM(RS-232 포트 시뮬레이션)
- TCS(Telephony Control Protocol)
- OBEX(Object Exchange Protocol)⁸⁾

마지막으로 블루투스의 사용·응용분야에 따른 내용을 규정한 프로파일로 그 구성은 아래와 같다.

- GAP(Generic Access Profile)
- SDAP(Service Discovery Application Profile)
- TCS(TCS-Binary based Profile)
- CTP(Cordless Telephony Profile)
- IP(Intercom Profile)
- SPP(Serial Port Profile)
- DUN(Dial-up Networking Profile)
- FAX Profile
- Headset Profile
- LAN Access Profile

- GOEP(Generic Object Exchange Profile)
- File Transfer Profile
- Object Push Profile
- Synchronization Profile
- 피코넷 관리
 - 슬레이브(Slave)의 연결과 단절 관리
 - 마스터(master)와 슬레이브 역할의 전환
 - ACL(Asynchronous Connectionless) and

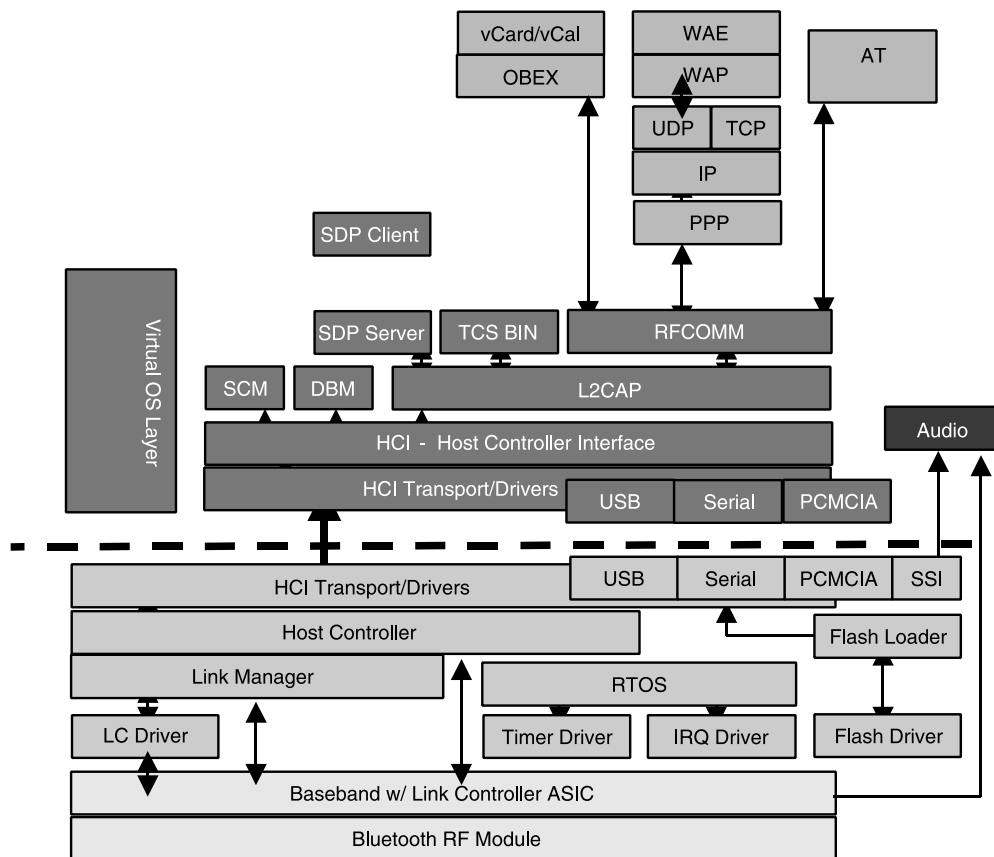


그림 2. 프로토콜 스택의 구성

3.1 Link Manager Protocol ^{2), 6), 7)}

LMP는 블루투스 하드웨어의 핵심이라 할 수 있는 베이스밴드 하드웨어를 직접 제어하는 펌웨어 레벨의 소프트웨어이다. LMP에는 피코넷 관리(Piconet management), 링크 관리(Link Configuration), 암호화 기능(Security Functions)의 3가지 기능으로 구성되어 있으며 각 세부 기능은 아래와 같다.

SCO(Synchronous Connection Orient)의 연결

- 전력모드 관리
- 링크 관리
 - Supported features
 - QoS
 - 전력 제어
- 암호화 기능
 - Authentication

- Encryption(key management 포함)

3.2 호스트 컨트롤러 인터페이스(HCI)^{2), 6), 7)}

HCI는 블루투스 프로토콜 스택에서 가장 기본이 되는 것으로 HCI에 대한 이해정도가 블루투스에 대한 이해정도라고 할 수 있을 것이다. HCI의 내용은 블루투스 스펙의 대부분을 차지하고 있으며, 즉 스택에서 중요한 부분을 차지하고 있다고 할 수 있다. HCI는 하드웨어 인터페이스 종류에 따라 UART, USB, PCMCIA로 나누어질 수 있으며, 각 하드웨어 인터페이스 종류에 따라 HCI의 송/수신 부분이 약간씩 달라져야 한다.

HCI는 호스트와 호스트 컨트롤러 사이에 명령어와 그 수행결과를 전달하고 또한 데이터를 전달할 목적으로 사용되어지고 있다. 즉 HCI는 명령어(Command), 이벤트(Event) 그리고 데이터(Data) 송/수신으로 크게 나눌 수 있으며 이것은 그림 3과 같다.

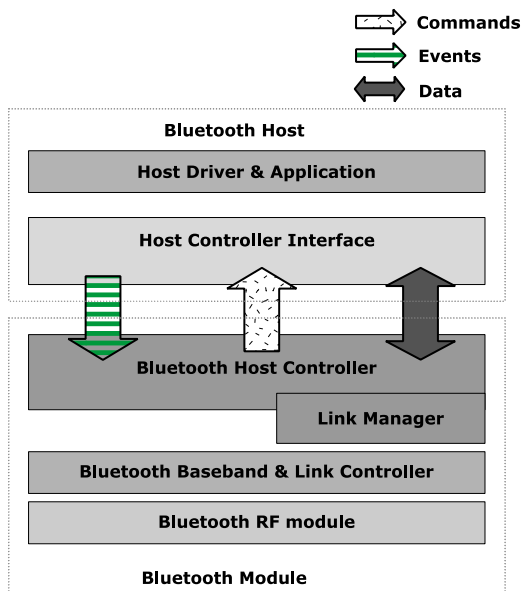


그림 3. HCI의 기능

HCI에서 하드웨어적인 인터페이스가 UART인 경우, 패킷의 포맷은 아래와 같다.

Packet type	Information
패킷 종류	표시
Command Packet	0x01
ACL Data Packet	0x02
SCO Data Packet	0x03
Event Packet	0x04

HCI에서 명령어는 크기는 6가지로 나누어지고, 총 90여 개의 명령어로 구성되어 있다. 명령어 패킷은 아래와 같은 형식이며, 각 명령어 별로 상세한 내용은 스펙을 참고. 그리고 6가지 명령어 그룹은 아래와 같다.

OCF (10bits)	OGF (6bits)	Parameter Total Length (1byte)	Parameter 0 (1byte)	Parameter N (1byte)
--------------	-------------	--------------------------------	---------------------	-------	---------------------

- Link Control Commands
- Link Control Commands(OGF = 0x01)
- Link Policy Commands(0x02)
- Host Controller & Baseband Command (0x03)
- Information Parameters(0x04)
- Status Parameters(0x05)

HCI 이벤트 패킷의 구성은 아래와 같습니다. 이벤트는 각 명령어에 따라 올 수 있는 것이 정하여져 있다. 자세한 내용은 스펙을 참고.

Event Code	Parameter Total	Parameter 0	Parameter N
------------	-----------------	-------------	-------	-------------

HCI ACL Data 패킷의 구성은 아래와 같다. 12Bit의 connection Handle과 Packet Boundary, Broadcast bit로 구성되어 있으며 한번에 전송할 수 있는 데이터의 길이는 65K 정도이다.

Connection Handle(12bits)	PB (2bits)	BC (2bits)	Data Total Length (2bytes)	Data
---------------------------	------------	------------	----------------------------	------------

3.3 L2CAP 프로토콜

L2CAP(Logical Link Control and Adaptation Protocol)은 인터넷 프로토콜의 TCP레이어의 기능과 비슷하다. 이것은 HCI 계층위에 존재하고 논리적인 연결을 담당하고 있다. L2CAP은 HCI의 ACL 데이터구조를 이용하여 상호간에 데이터를 주고받으며 L2CAP과 L2CAP 사이에 데이터를 주고받을 수 있고, 또한 상위 레이어로 데이터를 주고받을 수 있다. L2CAP의 주요 기능은 아래와 같다.

- 프로토콜 멀티플렉싱
- SAR(Segmentation and Reassembly)
- QoS(Quality of Service)
- Group 관리

L2CAP에서 사용되는 패킷의 종류는 Connection Oriented Channel Packet과 Connectionless Packet으로 나눌 수 있으며 각각의 구성은 아래와 같다.

Length (2bytes)	Channel ID (2bytes)	Information (payload)
Channel ID		설명
0x0000		Null Identifier
0x0001		Signalling Channel
0x0002		Connectionless Reception Channel
0x0003 - 0x003F		예약
0x0040 - 0xFFFF		Dynamically allocated

Connection-Oriented Channel Packet

Length (2bytes)	Channel ID (2bytes)	PSM (2bytes)	Information (payload)
Protocol/Service Multiplexer(PSM)			설명
0x0001			SDP
0x0003			RFCOMM
0x0005			TCS
<0x1000			예약
0x1000 - 0xFFFF			Dynamically Assigned

Connectionless Packet

시그널링 패킷은 L2CAP 계층과 L2CAP 계층 사이에 데이터를 주고받는 패킷형태로 요구와 응답의 형태로 구성되어 있다. 패킷의 구성은 아래와 같다.

Code (1byte)	Identifier (1byte)	Length (2bytes)	Data
Code		설명	
0x00		Reserved	
0x01		Command Reject	
0x02		Connection Request	
0x03		Connection Response	
0x04		Configure Request	
0x05		Configure Response	
0x06		Disconnection Request	
0x07		Disconnection Response	
0x08		Echo Request	
0x09		Echo Response	
0x0A		Information Request	
0x0B		Information Response	

Signalling Packet

3.4 SDP(Service Discovery Protocol)^{2), 6), 7)}

SDP는 블루투스 디바이스가 제공하는 서비스를 찾고 응답하기 위한 프로토콜이다. SDP는 서버와 클라이언트로 나누어지며, PSM 코드는 0x0001번에 해당한다. SDP 클라이언트에서 서버측으로의 패킷전송은 L2CAP 패킷의 데이터 부분에 SDP에서 사용되는 패킷을 넣어 보내게 되고, 이 패킷은 L2CAP의 위쪽 계층에 있는 SDP로 전달되어진다. SDP 서버는 전달된 데이터를 분석한 후 적당한 응답을 되돌려주게 된다. 패킷의 구성은 아래와 같다.

PDU ID (1byte)	Transaction ID (2bytes)	Parameter Length (2bytes)	Parameters (payload)
Code		설명	
0x01		SDP Error Response	
0x02		SDP Service Search Request	
0x03		SDP Service Search Response	

Code	설명
0x04	SDP Service Attribute Request
0x05	SDP Service Attribute Response
0x06	SDP Service Search Attribute Request
0x07	SDP Service Search Attribute Response

SDP Packet

SDP에서 요구하는 질문은 서비스의 존재 유무와 특정한 속성값에 해당하는 값을 요구하는 것이 대부분이다. 서비스에 대한 질문은 SDP__ServiceSearchRequest 함수로 요구하게 되고, 속성에 대한 질문은 SDP__ServiceAttributeRequest, SDP__ServiceSearchAttributeRequest 함수로 요구하게 된다. 응답은 각각 SDP__ServiceSearchResponse, SDP__ServiceAttributeResponse, SDP__ServiceSearchAttributeResponse 함수로 응답하게 된다.

3.5 RFCOMM^{2), 6), 7)}

RFCOMM은 RS-232 시리얼 포트를 이물레이션하기 위한 프로토콜이다. 블루투스에서는 TS 07.10 9)에 있는 규격을 대부분 그대로 따르고 있다. 다른 점은 Server Channel에 D라는 비트가 하나 더 존재하는 것만이 다르다. RFCOMM은 시리얼 포트를 이물레이션하는 Type I과 물리적인 시리얼 포트와 디바이스를 직접 연결하는 Type II를 제공하고 있다.

RFCOMM의 프레임 형태는 5가지로 구분되어진다. 자세한 내용은 TS07.10을 참고.

- SAMB(Start Asynchronous Balanced Mode)
- UA(Unnumbered Acknowledgement)
- DISC(Disconnect)
- DM(Disconnected Mode)
- UIH(Unnumbered Information with Header check)

RFCOMM의 기능중의 하나인 멀티플렉싱 기능은 RFCOMM의 UIH 프레임을 이용하여 전

송하게 된다. 이 때 사용되는 DLCI는 control 채널인 0번을 사용한다. 이러한 멀티플렉싱 프레임은 다음과 같다.

- PN - DLC 파라미터 조정
- Test - 통신 Link 체크
- Fcon/Fcoff - 모든 연결의 흐름제어를 제어
- MSC - 한 연결에서 모뎀의 상태나 흐름제어를 제어한다.
- RPN - Remote Port Negotiation
- RLS - Remote Line Status
- NSC - Non Supported Command


4. 결론

국제적으로 블루투스를 발전시키기 위한 모임들이 많이 있으며, 또한 전세계의 기술을 한 곳으로 모으는 장이 있는데 이것은 Unplug Test라고 합니다. 블루투스 SIG는 자주 Unplug Test를 개최하여 블루투스 기술에 대한 호환성 테스트 및 기술의 문제점을 도출하고 보완하는데 많은 시간을 소비하고 있습니다. 그러나 국내에서는 아직 기술개발의 미비로 이러한 모임이 많지 않은 실정이며 블루투스 시장을 확대하기 위해서는 세미나나 Unplug Test와 같은 만남의 장이 많이 있어야 할 것 같다. 또한 국가적인 지원정책도 있어야 블루투스 기술을 세계적인 경쟁력 있는 기술로 발전시킬 수 있는 원동력이 될 것이라고 생각한다.

이상과 같이 블루투스 스택에 대하여 개괄적인 내용을 살펴보았습니다. 지면상 내용이 불충분하지만 스택에 관심을 가지고 있는 사람에게 많은 도움이 되었으면 한다.

참고문헌

1. Bluetooth Homepage, <http://www.>

- bluetooth.com
2. "Specification of the Bluetooth System, Specification, Profiles", Version 1.1, 2001
 3. 802.11 Architecture presentation(Ref:IEEE P802.11-94/49B), IEEE Std 802.11-1997, IEEE 802.11-1999, IEEE 802.11a-1999 and IEEE 802.11b - 1999 march 1996.(all available from <http://grouper.ieee.org/groups/802/11>)
 4. HomeRF Working Group, Home Networking Technologies, Comdex November, 1999.
 5. Infrared Data Association, "IrDA Specification", (<http://www.irda.org>)
 6. RiKu Mettala, "Bluetooth Protocol Architecture", A bluetooth SIG White Paper, Revision, 0.95, July, 1999.
 7. S. Kambhatla, "Bluetooth PC Software Architecture", A Bluetooth SIG White Paper, Intel Corporation, Version 0.30 October, 1998.
 8. P. Megowan, D. Suvak, and D. Kogan, "Infrared Data Association, IrDA Object Exchange Protocol(OBEX)", Version 1.2 April, 1999.
 9. European Telecommunications Standard Institute(ETSI), "Digital Cellular Telecommunications system (Phase 2+):Terminal Equipment to Mobile Station(TE-MS) multiplexer protocol(GSM 07.10 version 6.3.0)", 1999. 

정통부, 중국 로드쇼서 6180만달러 계약체결

정보통신부는 지난 5월 19일부터 26일까지 중국 베이징, 상하이, 선전 등 3개 도시에서 CDMA(코드분할다중접속) 로드쇼를 개최한 결과 5건에 총 6180만 달러 규모의 계약이 체결됐다고 5월 27일 밝혔다. 정통부에 따르면 국내 중계기 업체인 KNC가 무한통신 및 베이징 경고통신과 3000만 달러, 중앙시스템이 중국 대당전신과 1100만 달러의 CDMA 중계기 수출계약을 각각 베이징에서 체결했다. 상하이에서는 중계기업체인 위다스가 중국의 신신전자와 1040만 달러, 에어로텔레콤이 중국의 DNG와 900만 달러의 계약을 맺었고, 선전에서는 신지소프트가 중국의 CEC와 휴대폰 탑재용 게임 소프트웨어 140만 달러 어치를 수출하기로 계약했다. 또 정통부는 로드쇼 기간동안 총 1904건, 8억8000만 달러 규모의 수출상담이 이뤄짐으로써 앞으로 한국기업의 중국 진출이 크게 증가할 것으로 기대된다고 밝혔다. 김동선 차관은 "이번 로드쇼를 통해 10억달러 규모로 추정되는 중국 중계기 시장에 한국기업이 본격적으로 진출하는 계기가 마련됐다"고 평가했다. 김 차관은 지난 5월 25일 중국 통신장비업체인 중흥통신, 과건 등을 방문해 장비 및 단말기 분야에서의 협력방안을 논의했다. 정통부는 중국 CDMA시장에서의 국내기업의 점유율을 높이고 단말기, 이동통신 칩, 표준분야 협력을 강화하기 위해 다양한 대책을 수립, 추진할 계획이다.