Internet Engineering Task Force
INTERNET DRAFT

G. Ruth, R. Yuan
GTE Laboratories
6 August 1996

Interworking Between CDPD and Mobile IP Networks
draft-ruth-cdpd-networks-00.txt

Abstract

Two protocols, CDPD (Cellular Digital Packet Data) and Mobile-IP have been developed by the CDPD Forum and IETF (Internet Engineering Task Force) respectively to address the issue of providing seamless network access to mobile data devices. In this memo a scheme is proposed for the two networks to interwork together and to support seamless migration of mobile data devices between the networks.

1. Introduction

Two protocols, CDPD and Mobile IP, have been developed in the past few years to address the issue of network layer mobility support for the general purpose data network. Both protocols enable a mobile terminal to migrate seamlessly from one local area network to another.

The CDPD (Cellular Digital Packet Data) standard was developed by the CDPD Forum (an industrial association of cellular carriers, equipment vendors and application developers) to provide packet data services through the cellular telephony network. It specifies a set of mobility enabling protocols for use in the CDPD networks.

CDPD networks is being deployed nationwide by the cellular carriers. The latest specification CDPD Specification, version 1.1 was published in January 1995 [1].

The Mobile-IP protocol has been developed by the IETF to provide mobility support in the current TCP/IP Internet. Mobile-IP is designed to support transparent host migration among a variety of IP subnetworks.

The concepts and principles for mobility management in both protocols are the same and many of mobility support functions are similar. However, while CDPD is designed to be a tariffed, carrier operated service with uniform link layer infrastructure (it has been widely deployed by many cellular carrier), Mobile IP is designed to support a variety of heterogeneous subnetworks. Thus, many differences exist between the two protocols. Currently, if a Mobile IP host migrates into a CDPD coverage area (or vice versa), its network connection will be terminated even with a CDPD wireless modem. This is because the network layer protocols for mobility support of the two networks cannot interoperable with each other. Therefore, to enable universal network connectivity for mobile hosts, it is necessary to provide methods for the two networks to internetwork with each other.

This memo compares the mobility management functions for CDPD and Mobile IP networks and suggests ways to support internetworking between the two networks.

2. Mobility Support in CDPD Networks

CDPD is designed to exploit the unused capacity of the cellular telephone network for packetized data delivery. It leverages the existing cellular infrastructure by adding CDPD specific equipment to the existing cell sites. The CDPD network architecture makes use of three distinctive devices:

- MES: Mobile End System -- A mobile terminal with a wireless modem that accesses the CDPD network through an airlink. Each MES may have one or more Network Entity Identifiers (NEIs) which are IP or CLNP addresses. The CDPD modem also has a 48-bit CDPD equipment identifier assigned by the manufacturer.

- MDBS: Mobile Data Base Station -- provides the mobile data link relay function for the MES over the radio channel. It performs part of the radio resource management function to ensure that the data user doesn't interfere with the regular voice users.

- MDIS: Mobile Data Intermediate System -- controls mobility,

performs registration, authentication and routing functions. It also controls the MDBS for radio resource management. The MDIS is a full-fledged network router.

Additionally, the CDPD architecture uses the term "Fixed End System" (FES) to denote an ordinary hardwired network end system.

The logical CDPD network architecture is shown in Figure 1:.

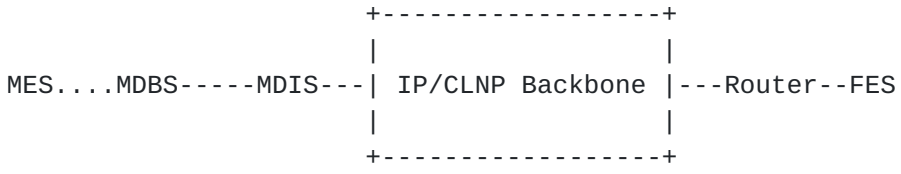


Figure 1: Logical CDPD Network Architecture

In a CDPD network, each wireless local network (termed as AREA) consists of one MDIS and up to 200 base stations (MDBSs). The mobile end system (MES) uses a multiple access scheme (Digital Sensing Multiple Access: DSMA) that gives packet data lower priority than voice traffic to access the cellular network. Because the MDBS is only involved in the data link relay function, the MES can roam transparently within the AREA using the different MDBSs for the data relay service, while maintaining the same data link connection between the MDIS and MES. Thus the AREA can be treated as a single network segment (e.g. Ethernet). Because there is one and only one MDIS within one AREA, the MDIS serves as the default gateway to/from the local network. It advertises the reachability of this network segment to other routers in the IP/CLNP backbone network.

The CDPD Forum has obtained several Class B IP addresses with prefix 166 from IANA. Thus, all the CDPD network AREAs use 166 as the network prefix.

If the MES roams from one AREA to another, the MES recognizes that it is in a new AREA during the cell transfer by listening to the channel identification message broadcasted from the base station during the channel acquisition time. It then initiates a new registration process using the MNRP (Mobile Network Registration Protocol) with the new MDIS. The serving MDIS handles the registration for the MES. It also communicate with the home MDIS of the MES so that appropriate authentication can be performed, and an appropriate routing entry can be set up at the home MDIS to forward packets destined to the mobile end system to the new foreign area. Figure 2 depicts the information flow for such an inter-AREA migration

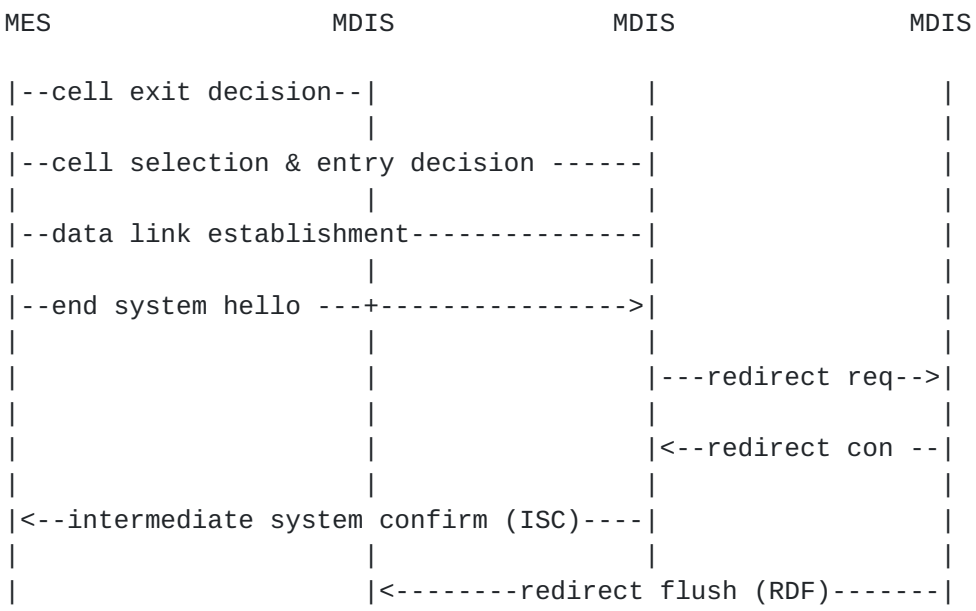
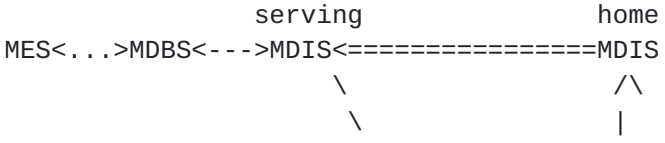


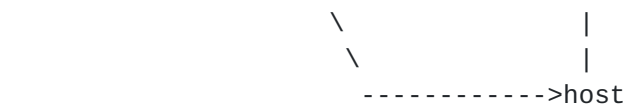
Figure 2: Information Flow for Inter-AREA Migration

One key aspect of an MES migrating into a new area is the associated authentication to verify the identity of the MES. In the CDPD network, airlink security is accomplished by exchanging secret keys between the serving MDIS and the visiting MES using a Diffie-Hellman key exchange scheme. After the MES obtains the key from the MDIS, it sends the authentication information tuple <NEI, ARN, ASN> (where ARN = Authentication Sequence Number and ASN = Authentication Sequence Number) to the serving MDIS in the End System Hello message. This information is relayed to the home MDIS for authentication in cleartext through the wired network.

After authenticating the MES, the home MDIS returns a success message and assigns a new <authentication random number, authentication sequence number> to the serving MDIS in the Redirect Confirm message; the information is relayed to the MES and can be used for authentication in the next registration.

The data packet forwarding from the home MDIS to the serving MDIS is done by encapsulating each IP/CLNP packet into a new CLNP packet. The destination address of the new CLNP packet is the serving MDIS. When the serving MDIS receives the encapsulated CLNP packet, it decapsulates the packet and delivers to the MES using the established data link channel. This triangular routing scheme (shown in Figure 3) is similar to Mobile IP triangular routing. As with Mobile IP, the CDPD MES keeps its IP address at all times.





=== indicates an encapsulated flow

Figure 3: Packet Forwarding in a CDPD Network

3. Mobility Support in Mobile IP networks

Mobile IP is designed to support host mobility in the current Internet Protocol (IPv4). Therefore, any internet host with an arbitrary IP address can be a mobile host migrating into a foreign network. In addition, a local network segment may have multiple routers attached, so that the routing path to/from the local network is not unique. To address these issues, the basic architecture of Mobile IP defines two entities: Home Agent (HA) and Foreign Agent (FA). The FA is located in the serving (foreign) network and provides direct network access to the mobile host (MH) when needed. The HA is responsible for intercepting IP packets destined to the mobile host and forwarding them to the serving FA of the mobile host. Because the mobile host may not be able to detect a subnet change through the link layer protocol, the FA/HA explicitly advertise their presence using Agent Advertisement messages (an extension of the ICMP router advertisement message, a network layer service).

When a mobile host migrates into a new local area it recognizes the new network from the Agent Advertisement message broadcasted periodically from the FA. The network layer broadcast of the agent advertisement message is necessary because there may not be a data link layer mechanism to detect the network segment change. The Agent Advertisement message includes one or more Care-of-Addresses (COAs) from the FA, encapsulation type(s) supported by the FA, registration lifetime and advertisement sequence number. The MH then initiates a registration process with the home agent using UDP messages with destination port 434. The registration message is relayed through the serving FA in the foreign network. The registration process enables the HA to update its mobility binding <MH, COA, last message ID, registration lifetime> for the migrated mobile host so that packets can be forwarded to the new location (COA).

To address the authentication and security concerns, Mobile IP defines flexible authentication extensions that can be added to the registration message using keyed-MD5. Both mobile-HA and mobile-FA authenticators can be attached to the registration message for proper authentication. While different authentication schemes can be employed by the MH, FA and HA through service agreement in advance, the Mobile IP standard specifies a default authentication method using the MD5 algorithm (RFC 1321). The

algorithm computes a one-way hash function that produces a 128-bit "message digest" for an arbitrary long registration message. The shared secret key is pre-configured for the MH - HA authentication. For MH-FA authentication, the key can either be distributed manually, or using public key. The information flow of the registration messages is depicted in Figure 4.

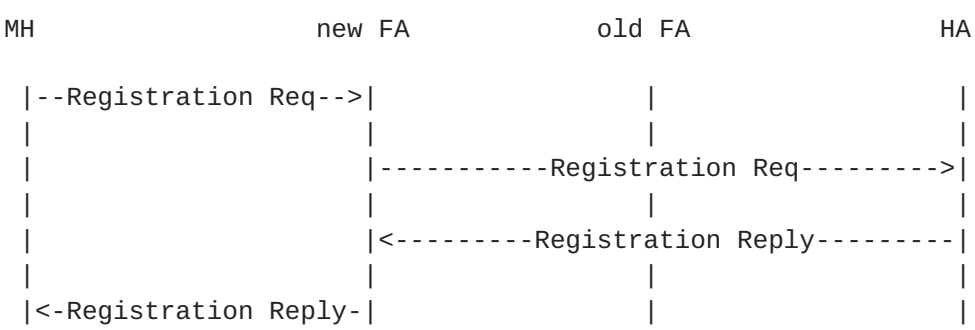


Figure 4: Information Flow for MobileIP Registration Messages

The Mobile IP protocol also defines an option for the MH to act as its own FA, if the foreign network has no FA and the MH can obtain a local address from the DHCP server (e.g. using anycast mechanism). In this case, the Care-of-Address is the newly obtained the local IP address from DHCP server.

It is also noted that there is no registration cancellation message sent to the old FA when registration at the new FA becomes active. Because IP provides best effort datagram delivery, the packets in transit will simply be dropped and the old registration will expire after the validation period.

Similar to the CDPD approach, the packet forwarding in Mobile IP is carried out using encapsulation/decapsulation. The HA intercepts each packet destined to the MH and then encapsulate the packet using the COA in the mobility binding of the MH. Upon receiving the encapsulated packet, the FA decapsulates the packet and sends it directly to the MH using its own link layer protocol. Figure 5 shows the packet forwarding in Mobile IP.

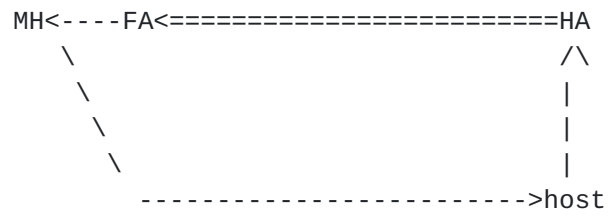


Figure 5: Packet Forwarding in a Mobile IP Network

Two encapsulation methods are defined in the Mobile IP standard: Minimum encapsulation and IP within IP (IPIP). IPIP encapsulation

is the recommended encapsulation method. The IPIP method handles packet fragmentation easily but adds more overhead to the encapsulated packet.

4. Comparison between CDPD and Mobile IP

CDPD and Mobile IP are designed to support general purpose network layer mobility for packet data networks. In particular, both are designed to support network layer mobility in the IP network, thus enabling mobile host migration in the Internet. The basic mobility management functions for CDPD and Mobile IP networks are based on the same concepts and principles (e.g. packet encapsulation and forwarding).

Although many of the mobility management concepts and functions in CDPD and Mobile IP are similar, the detailed message formats differs from each other. In addition, there are several notable difference in the protocol:

- In CDPD, the MES can detect the network segment change from the link layer support, while in mobile IP, the explicit Agent Advertisement message is necessary for the mobile host to detect network change.

- In CDPD, the registration process is separated into two stages. First, the MES registers with the serving MDIS using the MNRP, where no authentication is required. Second, the serving MDIS uses a separate protocol, MNLP, to update the location information to the home MDIS and forward the authentication information from the MES to the home MDIS for authorization. In Mobile IP, the mobile host registers directly with the HA, while the FA provides the relay service to the registration services.

- In CDPD, the home MDIS informs the previous serving MDIS to flush the MES's registration record, while in Mobile IP, multiple simultaneous registration records with different FAs for a mobile host are permitted.

- Because of the uniqueness of the MDIS, it is guaranteed that the home MDIS can intercept the packet destined to the MES, while in mobile IP, the HA needs to use the proxy ARP protocol to advertise the mobile host reachability in order to intercept the packet.

- CDPD defines a single encapsulation method between the home MDIS and the serving MDIS. All the packets forwarded to the serving MDIS are encapsulated using a CLNP packet with minimum encapsulation header to increase efficiency. In Mobile IP, two encapsulation methods are defined with

IP within IP as the recommended method.

The protocol architecture for registration in CDPD and Mobile IP differ as follows. The CDPD registration procedure is separated into two phases (MNRP and MNLP), different from the one phase approach of Mobile IP. In addition, the CDPD's MNLP defines several message to allow the MDISs to exchange location update information without the involvement of MES. Furthermore, the registration message contents of CDPD and Mobile IP is different. The information fields contained in these messages are listed in Table 1.

	CDPD		MobileIP	
Parameter	Field Name	M/O	Field Name	M/O
Permanent addr. of mobile	Source addr	M	Home addr	M
Registration seq. control	Regist. seq Count	M	Registration identification	M
Authentication (home-mobile)	Authentication parameter	M	Mobile-home auth. extension	M
Home agent id	NR		Home Agent	M
Registration lifetime	NR		Lifetime	M
Forwarding address	Forwarding net address	M	Care-of-Address	M
Multiple regist. req.	NR		Code	M
Authentication (foreign-mobile)	NR		Mobile-foreign auth. extension	O
Encapsulation method	NR		Minimum encaps. extension	O
Carrier identi-fication	Location info	O	NR	

M=Mandatory, O=Optional, NR=Not Relevant

Table 1: Information fields in registration messages

In a CDPD network, no authentication is required between the MES and the serving MDIS. although an encryption key is exchanged

between the two entities using Diffie-Hellman algorithm. The MES then authenticates itself within its home MDIS using the <NEI, <ARN, ASN>> tuple; the serving MDIS will only issue an ISC message to the MES if proper authorization from the home MDIS is obtained. In a Mobile IP network, the registration message from the mobile host can contain the FA-mobile host authentication extension to allow the FA and the MH to authenticate each other.

When the mobile host/end system is roaming, the home network should forward the packets to the serving/foreign network. In CDPD, this task is being performed by the home MDIS. Since all packets destined into the MES's home network go through the MDIS, there is no need for the MDIS to make extra efforts to intercept the packets. In Mobile IP, a subnet may have multiple paths for packets to be routed to/from the subnet, and the mobile host's HA may not be the gateway router. Thus the HA uses gratuitous ARP to advertise the reachability of the mobile host once it receives the mobile's registration from a foreign network (impersonating the mobile host). When the MH returns to the home network and deregisters from the HA, the normal packet delivery is resumed.

5. Internetworking between CDPD and Mobile IP

Due to the differences mentioned in Section 3, CDPD and Mobile IP cannot interwork without any modifications. However, since many of the mobility management concepts and functions are derived from the same principles, CDPD and Mobile IP can support each other's operation without major modification of the specification. This section discusses how a CDPD network can support a Mobile IP user through the use of middleware software that interfaces the CDPD and Mobile IP networks. (A similar method can be used to enable CDPD terminal support from a Mobile IP network.)

Suppose a Mobile IP host enters a CDPD domain and wants to establish network access through the CDPD network. The MH can use a CDPD docking station and/or a CDPD modem to access the CDPD network. Following the CDPD network operation convention, the CDPD modem must have a valid network address (IP address) registered with the network operator. The CDPD network address uses prefix **166 and is different from the original IP address of the mobile** host.

To obtain network service from the CDPD network and maintain a Mobile IP connection, the MH must register with both the CDPD network and its HA. Following the CDPD protocol, the CDPD modem performs the CDPD registration with the serving MDIS using its CDPD recognized IP address with prefix 166. From the CDPD network's perspective, the MH is a valid CDPD MES with a valid CDPD address, thus the Mobile IP aspect of the MH is completely transparent from the CDPD network. The MH can then use the

standard Mobile IP protocol to register with its HA, using the CDPD network address as the COA. In this case, the FA and the MH are collocated and MH acts as its own agent. The CDPD network address (NEI) is easily accessible from the modem memory/registers using the standard AT command.

Upon completion of the registration process, the MH can continue to send out IP packets to the network using the serving MDIS as its default router. The CDPD network treats the MH as a conventional MES with a valid CDPD address. The packets destined to the MH will be encapsulated by the HA and forwarded to the MH using the CDPD network address as the COA. The scenario is the same as an IP-based FES communicating with an MES. The routing scenario is depicted below in Figure 6. (The CDPD network encapsulation is not shown.)

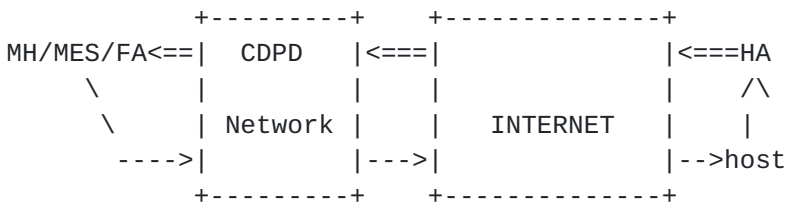


Figure 6: Supporting Mobile IP host in a CDPD Network: One-directional Encapsulation Approach

Refinement

The one directional encapsulation approach described above may create an accounting problem for the CDPD network. As dictated by some CDPD network operators, any packet originated from the CDPD network must have a valid CDPD network address (with prefix 166) as its source address. Such networks use the source to create accounting data for billing purposes. The one way encapsulation approach allows a packet originating from the MH to use its home address as the source address, which cannot be properly accounted by the account meter in the MDIS. Therefore, for accounting purposes, every packet originating from the MH should be encapsulated using the CDPD network address as the source address. However, this creates another problem for the corresponding host for the MH, since the corresponding host may not have the capability to decapsulate the packet.

A bidirectional encapsulation approach is proposed to solve the accounting problem and keep the corresponding host transparent at the same time. The MH encapsulates outgoing packets using the HA's address as the destination address and the CDPD NEI as the source address. Upon receiving the encapsulated packets, the HA decapsulates and forwards them to the correct destination.

Therefore, to support the migration of a mobile host into a CDPD network, the HA must also provide a decapsulation function. This is relatively simple because the HA already has the encapsulation capability. The bidirectional encapsulation tunnel established between the MH and HA serves as a virtual private network (VPN) connection for the MH and its home network.

The bidirectional encapsulation method is depicted in Figure 7.

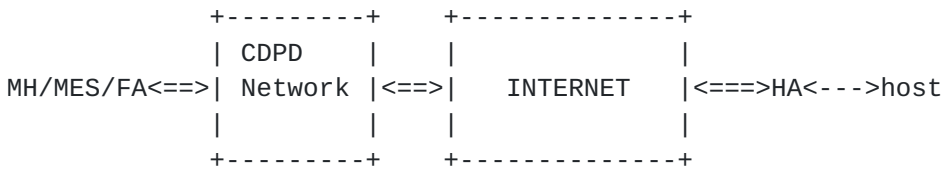


Figure 7: Supporting Mobile IP host in a CDPD Network: Bi-directional Encapsulation Approach

Note that in the initial approach, the only interaction between the Mobile IP software and the CDPD network is for the Mobile IP software to retrieve the CDPD network address associated with the CDPD modem. No modification on the part of CDPD network infrastructure is needed. For the one directional encapsulation approach, no change on the Mobile IP HA is required. On the other hand, for the VPN approach, the Mobile IP software on the MH and its HA should be enhanced so that a bidirectional encapsulation tunnel can be established between the two entities.

If the MH/MES roams into a new serving MDIS, both the registration and packet forwarding will be performed by the CDPD network without impact on the Mobile IP protocol.

6. Summary

This memo has investigated the mobility management functions for the two prominent technologies being developed and deployed in the communication industry: CDPD and Mobile IP. While these two are based on the same principles and concepts, they can not interwork with each other due to the differences in their approaches in the registration protocol, encapsulation method, and security extensions. Historically, the two protocols have different design goals in terms of uniformity/heterogeneity, tariff and security concerns.

An approach was identified for interworking between CDPD and Mobile IP networks while keeping the existing protocols unchanged. The scheme calls for adding relative simple middleware to the mobile host software to enable its usage of CDPD network as a

Mobile IP subnet.

With a large deployed base of CDPD networks and the ubiquity of the IP based Internet it is important to explore schemes that allow the two networks to interconnect with each other and provide mobility services to the ever increasing population of mobile computing devices.

7. Security Considerations

Security considerations are not discussed in this memo.

8. References

[1] CDPD Forum, "Cellular Digital Packet Data System Specification", Release 1.1, January 19, 1995.

[2] IETF Mobile IP working group, "IP Mobility Support - Draft-IETF-Mobileip-Protocol-17", May 31, 1996.

9. Authors' Addresses

Greg Ruth
GTE Laboratories, Inc.
40 Sylvan Street
Waltham, MA 02254
gruth@gte.com
617 466 2448

Ruixi Yuan
GTE Laboratories, Inc.
40 Sylvan Street
Waltham, MA 02254
ry00@gte.com
617 466 2050