Packet Data Roaming

4/18/2005
Andrew Hunter
ahunter@qualcomm.com
Contents

• CDMA2000 Packet Data Overview

• Review of CDMA2000 Architecture and Protocols

• Packet Data Roaming Challenges

• Packet Data Roaming Network Configurations

• Packet Data Roaming Billing

• Packet Data CRX for Interconnection and Settlement
Packet Data Applications

• Internet access
  – Web access
  – VPN connections to home office

• Packet data service required for many new features
  – Access to WAP/JAVA/BREW servers while roaming
  – Location services
  – Network games
  – Multimedia messaging
  – VoIP/Push-to-Talk
  – Multimedia conferencing
CDMA2000 Packet Data Overview

• CDMA2000 1x provides data speeds up to 150 kbps
  – CDMA Channel hosts both voice and data users
  – Dynamic configuration
  – Capacity shared between voice and data
  – Average speeds of 50 kbps

• CDMA2000 1xEV-DO is the fastest high-speed wireless data technology commercially deployed today with data speeds up to 2.4 Mbps
  – CDMA Channel is dedicated to data services
  – Average speeds of 400-600 kbps
CDMA2000 Architecture

- CDMA2000 architecture defined by 3GPP2 standards

- IS-835 defines the 1xRTT network architecture
  - Latest published version is IS-835D (QoS and MobileIPv6)

- CDMA Data protocols are primarily based on IETF RFCs, for example IP, PPP, Mobile IP, etc
CDMA2000 Packet Data - Infrastructure Overview

MS = Mobile Station
RAN = Radio Access Network
AAA = Authorization, Authentication, Accounting
PCF = Packet Control Function
PDSN = Packet Data Serving Node
HA/FA = Home/Foreign Agent (Mobile IP only)
CDMA Data Roaming Implementation Challenges:

• There are no *standards* for implementing CDMA data roaming
  – Connectivity and protocols are left open for the operators to define

• The CDG provides *recommendations* for implementations:
  – Reference Document #79: Wireless Data Roaming Requirements and Implementation
  – Reference Document #94: CDMA Packet Data Roaming eXchange Guidelines

• Data roaming implementation decisions are relevant to both 1xRTT and EV-DO
Fundamental Step: Interconnection

- Interconnection can be established via direct, leased line or VPN
- Most implementations use an IPSec VPN over the Internet
- Provides security of user data and authentication information
Access Authentication Overview

- Roaming MS requests access on the visited operator’s network
- Visited AAA acts a proxy to the home AAA
- Home AAA remotely authenticates, and MS is authorized to visited network
Network Address Identifier (NAI)

- NAI allows visited systems to contact the Home system for authentication and billing data exchange.
- Must use a fully qualified NAI for roaming:
  - NAI is constructed based on the MSID of the Mobile in the form `<MSID>@<realm>`
  - Where MSID can be an IMSI, MIN, or IRM
  - And ‘realm’ is the internet domain name of the home network that owns the mobile (need to use workarounds if home domain is not available.)

- Example: 0199123456@cdmacarrier.com
Data Services Common Issues

• Shortage of IPv4 addresses
  – Network Address Translation
  – Could use IPv6 internally and roam on IPv4

• Security of IP networks
  – Firewalls

• Performance uncertainty
  – Routing latency and end-to-end service quality not always under operator control
Network Architecture Options

- Three network options for implementing data roaming:
  - Simple IP: Access to public network at serving system
  - L2TP: Subscriber’s traffic is routed via home network
  - Mobile IP: Subscriber accesses public network at home system. Subscriber maintains same address across networks.

- There are advantages and disadvantages to each approach

- Different operators have different needs, so implementations vary
Implementing Roaming with Simple IP

- Visited operator assigns roaming MS its IP address
- If visited operator assigns private IP address, NAT required
- MS may directly access public Internet from visited operator’s network
- Must traverse public Internet via VPN to access home application servers
Implementing Roaming with L2TP

- Home operator LNS assigns roaming MS its IP address. L2TP tunnel is created between visited PDSN/LAC and LNS.
- Must tunnel back to home network to access public Internet
- Can directly access application servers in home network without NAT
Implementing Roaming with Mobile IP

- Home operator HA assigns roaming MS its IP address. Visited operator provides COA. Mobile IP tunnel created between visited PDSN/FA and HA.
- Must tunnel back to home network to access public Internet
- Can directly access application servers in home network without NAT
Packet Billing and Roaming

- PDSN collects data records (e.g. packet/byte counts, IP addresses, etc.)
- PDSN sends to AAA the usage data records (UDRs)
- Visited AAA forwards copies of usage records to home AAA.
- AAA is an accounting collection point for the billing system
- The home operator uses the UDRs to bill the subscriber for the roaming data session
- The home and visited operators use the UDRs to determine the amount owed by own operator to another
- Operators will typically aggregate UDR data and settle on a monthly basis.
CRX – Interconnection Made Easy

• CDG Document #94 provides guidelines for CDMA2000 packet data Roaming eXchange (CRX).

• CRX provider is a 3rd-party hub to exchange roaming traffic:
  – User traffic
  – Signaling traffic
  – AAA traffic
  – Billing records
CRX Providers

• CDMA Packet Data Roaming eXchange (CRX) Providers are in the business of facilitating CDMA data roaming for operators

• Similar function to GPRS Roaming Exchange (GRX) providers

• Allows an operator to only create a single data connection with the CRX provider and implement roaming with multiple operators

• CRX providers typically perform financial settlement between operators

• CRX providers are required to interconnect, so operators serviced by different CRX providers should still be able to implement roaming
Functions of a CRX Provider

- Provides a secure backbone for operator interconnection

- Provides a proxy AAA so operators always send AAA transactions to same place

- Interfaces with operator billing system to perform settlement function
CRX Reference Model
Xd Interface

- Xd is the interface between the border gateways of a carrier and CRX provider.
  - Exchange Mobile IP and L2TP roaming traffic (user & signaling).
  - Exchange AAA traffic between AAA servers.
  - Support secure connectivity:
    - Private connections (e.g., dedicated lines), or
    - IPsec tunnels over public Internet.
  - Support static routing or BGP-4 routing protocol.
  - Network QoS specifications (e.g., network availability, latency, packet loss rate)
Xa Interface

• Xa is the interface between the AAA servers of a operator and CRX provider.
  – Exchange authentication, authorization, and accounting information.
  – Support RADIUS protocols and attributes defined in IS-835-A.
  – Proxy RADIUS messages to the AAA server in a home carrier or another CRX provider.
  – Respond to the AAA server in a visited carrier if RADIUS messages cannot be routed (e.g., destination unreachable or unrecognized).
  – Duplicate accounting information for the data clearing system.
Data Clearing System

• Collect the Usage Data Record (UDR) (i.e., accounting information) from the CRX’s AAA server.
• Check the UDR formats for correctness.
  – E.g., checks if the length of each UDR attribute is within the allowable range.
• Determine roaming partner pair from UDR attributes.
  – E.g., Base Station ID (BSID) attribute contains System ID (SID) that identifies a visited carrier.
  – E.g., Username attribute contains user’s NAI whose realm identifies the user’s home carrier.
• Support rating function to generate financial information from the UDR.
  – E.g., rating unit is in U. S. Dollars per 1 Kbytes.
CRX Inter-Connectivity

- Visited & home carriers may choose different CRX providers.

- Two CRX providers inter-connect through
  - Central peering point managed by an independent provider, or
  - Direct connectivity under bilateral agreement.

- Inter-connection between visited & home carriers must not traverse more than two CRX providers.
Central Peering Reference Model

CDMA2000 Packet Data System A

CRX A

BG
Proxy AAA

LNS
HA
AAA

CRX C

BG
Proxy AAA

CDMA2000 Packet Data System B

CRX B

BG
Proxy AAA

BG
AAA
HA
LNS

CDMA2000 Packet Data System C

BG
AAA

Central Peering
CDMA2000/GPRS Inter-Standard Roaming

• Support roaming MS to access servers in its home CDMA2000 system from a visited GPRS/GSM system.
• From the perspective of the visited GPRS/GSM system, the CRX provider acts as a home GPRS/GSM system that
  – Supports GGSN functions,
  – Inter-connects with the visited GPRS/GSM system via a GRX provider.
• From the perspective of the home CDMA2000 system, the CRX provider acts as a visited CDMA 2000 system that
  – Supports FA and LAC functions,
  – Inter-connects with the home CDMA2000 system via Xd interface.
CDMA2000/GPRS Inter-Standard Roaming
Thank You

ahunter@qualcomm.com
Simple IP Roaming Pros/Cons

Advantages:

- The roaming MS may directly access the public Internet without tunneling to the home operator’s network.
- The roaming MS may directly access application servers in the visited network without tunneling to the home operator’s network.

Disadvantages:

- The visited operator must assign the roaming MS its IP address
- The roaming MS may not be assigned a static IP address
- If the MS is provisioned with private, hard coded DNS server addresses, it will not be able to access DNS services while roaming
- If the MS is assigned a private IP address by the visited operator, NAT must be employed for the MS to access applications servers in the home network
- The IP addresses of application servers must be made visible to the visited network
- Security is compromised since other inbound roamers in the visited operator’s network will be able to access the home operator’s network. To avoid this, the visited operator may need to maintain separate IP address pools for each roaming partner.
Mobile IP Roaming Pros/Con

Advantages:

• The home operator assigns the roaming MS its IP address
• The home operator may assign a static IP address to the roaming MS
• The home operator may assign a private IP address to the roaming MS without the need to employing NAT for home network access.
• The roaming MS may transparently access servers in the home network.
• Security is improved since other inbound roamer s in the visited operator’s network will not be able to access the home operator’s network.
• The use of Mobile IP allows for network layer mobility across PDSNs.

Disadvantages:

• There is a performance overhead for Mobile IP
• When the roaming MS is accessing the public Internet, tunneling back to the home network is not efficient
• If the roaming MS requires access to an application server in the visited network, it will be required to tunnel back to the home operator and then route back to the visited operator