3GPP2 TSG-P
Wireless Packet Data Networking

TITLE:

TSG-P Meeting Summary, Meeting #20

SOURCE:

Chair, 3GPP2 TSG-P

Samsung Telecommunications America
1130 E. Arapaho Road
Richardson, TX 75081

Haeng S. Koo
(972)761-7755
hskoo@sta.samsung.com

ABSTRACT:

This document contains the summary of the twentieth TSG-P meeting, which was held on December 4 - 8, 2000 in Kauai, HI.

RECOMMENDATION:

Review for accuracy and amend as needed.

Notice

1 **3GPP2 TSG-P**
2 **Wireless Packet Data Networking**
3 **Meeting Report, Meeting #20**
4
5

Date:	December 4 - 8, 2000
Location:	Hyatt Regency Kauai Resort & Spa
	Kauai, HI
Chair:	Haeng S. Koo, Samsung Electronics
Phone:	972.761.7755
E-mail:	hskoo@sta.samsung.com

6

7 Quorum Members, Attendees, and Attendance Status
8

Organization	Attendee of this meeting	Last 4 Meetings Attended	Quorum Member
3Com	Ed Campbell	#17 #18 #19 #20	Yes
Cisco	Rajesh Bhalla	#17 #18 #19 #20	Yes
Ericsson	Lila Madour	#17 #18 #19 #20	Yes
Hyundai Electronics	Dong Hyun Lee	#17 #18 #20	Yes
ETRI	Jae Young Ahn	#17 #18 #20	Yes
Fujitsu	Mamoru Higuchi	#18 #19 #20	Yes
Hitachi		#18 #19	Yes
KDDI	Takuo Seki	#19 #20	Yes
LG Electronics	Ki0Youbg Kim	#17 #18 #20	Yes
Lucent Technologies	Tom Hiller	#17 #18 #19 #20	Yes
Lucent Technologies (TTC delegate)	Hajime Shiino	#17 #19 #20	Yes
Motorola	Sebastian Thalanany	#17 #19 #20	Yes
NEC		#17 #19	Yes
Nortel Networks	Neville Rego	#17 #18 #20	Yes
Qualcomm Inc.	Raymond Hsu	#17 #18 #19 #20	Yes
Samsung Electronics	Haeng S. Koo	#17 #18 #19 #20	Yes
Sprint PCS	David Collins	#17 #18 #19 #20	Yes

9

10 **Others Present**
11

Organization	Attendee
Alcatel USA	Tom Tansil
Certicom Corp	Dorothy Gellert
Cisco	Murtaza Chiba
Converse Network System	Shoji Matsushita
CWTS/RITT	Hua Ye
Ericsson	Mohammed Sammoor
France Telecom	Josep Sole Tresserres
Hyundai Electronics	Shin Hyun Yang
Lucent Technologies	Mike McPheters
Mitsubishi Electric	Daqing Gu
Motorola	Anda Farcasanu
Motorola	Wayne Bowen
Nextel	David Zufall
Nextel	H. Hussan Patrovi
Nokia	Thin Nguyenphu
Nokia	Anna Sillanpaa
Nortel Networks	Neville Rego

Nortel Networks	Kuntal Chowdhury
Qualcomm	Nish Abrol
Samsung Electronics	Jae Hyuk Do
Samsung Electronics	Junhyuk Song
Samsung Electronics	Rick Phung
Sprint PCS	Iris Zeng
SK Telecom	Sung Kim
SK Telecom	Dongkie Lee
Sun Microsystems	Pat Calhoun
Telcordia Technologies	Scott English
Verizon Wireless	Steve Rados

1. Call To Order and Opening Remarks

The meeting was called to order at 8:35 AM on December 4, 2000 at Hyatt Regency Kauai Resort & Spa in Kauai, HI.

2. Attendance Registration

The attendance roster was circulated, and the names and organizations of the present are reflected above. The quorum list stood at 17 member companies. With 15 member companies present, a quorum was declared.

3. Review and Adoption of Agenda

The Chair introduced 3GPP2-P00-20001204-001 as the proposed agenda, which was approved with the addition of agenda item, "9B. 1xEV-DO."

4. Contributions Assignment to Agenda Items

The following 26 contributions were submitted, numbered and assigned to the agenda:

Number	Title	Source	Agenda Item
3GPP2-P00-20001204-001	Proposed Agenda	Haeng Koo, Chair, Samsung	3
3GPP2-P00-20001204-002	Meeting Summary, Meeting #19	Haeng Koo, Chair, Samsung	5
3GPP2-P00-20001204-003	Correspondence	Haeng Koo, Chair, Samsung	6
3GPP2-P00-20001204-004	Comparisons of Low Interruption Deferred Handoff Approaches 6	Lucent , Tom Hiller, Pete McCann	8B2
3GPP2-P00-20001204-005	Solution for Collocated COA Mobiles on Carrier-Based Home Agents	Lucent , Tom Hiller, Pete McCann	8B6
3GPP2-P00-20001204-006	Multiple RLP and QoS	Lucent , Tom Hiller, Pete McCann	8B1
3GPP2-P00-20001204-007	RFC 2507 and RFC 2508 Header Compression with Retransmitting RLP	Lucent , Tom Hiller, Pete McCann	8B2
3GPP2-P00-20001204-008	Changes for Airlink Record Encoding	Motorola, Sebastian Thalanany	8B8
3GPP2-P00-20001204-009	Clarifications to IS–835 and Proposed Text Changes	Cisco Systems, Murtaza Chiba, Rajesh Bhalla, Gopal Dommety	8A
3GPP2-P00-20001204-010	Fast Handoff in cdma2000 Wireless IP Networks	Cisco Systems, Murtaza Chiba, Rajesh Bhalla, Gopal Dommety	8B2
3GPP2-P00-20001204-011	PPP Resource Management at the PDSN	Cisco Systems, Murtaza Chiba, Rajesh Bhalla,	8B4

		Gopal Dommety	
3GPP2-P00-20001204-012	0-byte Header Compression for cdma2000	Ericsson, Mohammed Sammour, Francis Lupien, Ulises Olvera-Hernandez, Lila Madour	8B8
3GPP2-P00-20001204-013	Diameter protocol requirements for release B	Ericsson, Lila Madour	8B5
3GPP2-P00-20001204-014	Fast-handoff and ROHC Header Compression	Ericsson, Lila Madour	8B2
3GPP2-P00-20001204-015	Clarification on differentiation between Simple IP and Mobile IP	SK Telecom, Dongkie Lee, Sung Kim	8A/8B8
3GPP2-P00-20001204-016	Comment on authentication Method for HDR-based subscriber	SK Telecom, Dongkie Lee, Sung Kim	9B
3GPP2-P00-20001204-017	Accounting Trigger for PDSN	SK Telecom, HyaeKyeung Lee, Sung Kim	8A
3GPP2-P00-20001204-018	Data Octet Count specification for the PDSN Accounting	SK Telecom, HyaeKyeung Lee, Sung Kim	8A
3GPP2-P00-20001204-019	Proxy DNS Update by Home Agent for Mobile Node	SK Telecom, Dongkie Lee, Sung Kim	8B8
3GPP2-P00-20001204-020	The Problems with CISCO key distribution by SNMP	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong	8A
3GPP2-P00-20001204-021	Replacement text for Section 6.2.4, 6.3.2, and 6.4 in IS-835 addendum with SAMSUNG's IKE security key distribution method	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong	8A
3GPP2-P00-20001204-022	Priority of work items for Release B	KDDI, Takuo Seki	8B8
3GPP2-P00-20001204-023	Handover support in 1xEV-DO: impacts on PCN resources and accounting.	Ericsson, Lila Madour	9B
3GPP2-P00-20001204-024	Leading role for 1xEV-DO network specifications	Ericsson, Lila Madour	9B
3GPP2-P00-20001204-025	The clarification for P00-20001204-Samsung-Key distribution	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong	9B
3GPP2-P00-20001204-026	'S' Fetching Protocol	Sun Microsystems, Pat Calhoun	8A

5. Review of Meeting Reports

The Chair introduced "3GPP2-P00-20001204-002, Meeting Summary, Meeting #19," and the contribution was accepted as presented.

6. Correspondence

The Chair presented the correspondence from Steven Dennett, Chair, 3GPP2 Steering Committee, regarding TSG leadership election. The Chair announced that the election of Chair and Vice Chairs would be held at the January meeting as requested by the correspondence.

7. Reports

Tom Hiller made a report on the IETF activities.

8. Old Business

A.   V&V of Addendum to P.S0001-A

Annex A lists the V&V comments for Addendum to P.S001-A. All the comments were reviewed and incorporated based on review discussion. The updated document that includes the results of the V&V resolution is in file P.S0001-A-R4.doc.

The following table shows the contributions and their resolutions related to the V&V comments:

Number	Title	Source	Resolution
3GPP2-P00-20001204-009	Clarifications to IS–835 and Proposed Text Changes	Cisco Systems, Murtaza Chiba, Rajesh Bhalla, Gopal Dommety	Rejected.
3GPP2-P00-20001204-015	Clarification on differentiation between Simple IP and Mobile IP	SK Telecom, Dongkie Lee, Sung Kim	Implementation Issue.
3GPP2-P00-20001204-017	Accounting Trigger for PDSN	SK Telecom, HyaeKyeung Lee, Sung Kim	Accepted. Use F1 and F2.
3GPP2-P00-20001204-018	Data Octet Count specification for the PDSN Accounting	SK Telecom, HyaeKyeung Lee, Sung Kim	Accepted. Added G15 and G16.
3GPP2-P00-20001204-020	The Problems with CISCO key distribution by SNMP	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong	Accepted with modifications proposed by Pat Calhoun.
3GPP2-P00-20001204-021	Replacement text for Section 6.2.4, 6.3.2, and 6.4 in IS-835 addendum with SAMSUNG's IKE security key distribution method	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong	Accepted with modifications.
3GPP2-P00-20001204-026	'S' Fetching Protocol	Sun Microsystems, Pat Calhoun	Rejected.

There were several V&V resolutions, especially on accounting parameters, that would impact IOS V4.0. Rajesh Bhalla volunteered to bring them to TSG-A as ballot comments of IOS V4.0.

B. 3G Packet Data Technical Standard (Rel B)

1. QoS

Tom Hiller presented 3GPP2-P00-20001204-006, Multiple RLP and QoS. This contribution proposes support of multiple RLP with PPP. Since there was no QoS framework that can be used for making a decision, this contribution was left open for further discussion.

2. Support of multimedia services

Tom Hiller presented 3GPP2-P00-20001204-007, RFC 2507 and RFC 2508 Header Compression with Retransmitting RLP. This contribution proposes adopting RFC 2507, 2508 and 2509 as mandatory for the PDSN and optional for the mobile station. This contribution was left open for further discussion.

Mohammed Sammour presented 3GPP2-P00-20001204-012, 0-byte Header Compression for cdma2000. This contribution extends ROHC (Robust Header Compression) for cdma2000 application. Again, this contribution was left open for further discussion.

The following three contributions were presented regarding fast or low interruption handoff:
• Rajesh Bhalla - 3GPP2-P00-20001204-010, Fast Handoff in cdma2000 Wireless IP Networks,

- Tom Hiller - 3GPP2-P00-20001204-004, Comparisons of Low Interruption Deferred Handoff Approaches,
- Lila Madour - 3GPP2-P00-20001204-014, Fast-handoff and ROHC Header Compression.

After reviewing the three proposals, the TSG selected Phase 1 of the proposal presented by Rajesh Bhalla. The future phases are for further study.

3. Broadcast/Multicast

There was no contribution on this topic.

4. Mobile IP enhancements

Rajesh Bhalla presented 3GPP2-P00-20001204-011, PPP Resource Management at the PDSN. This contribution proposes release of idle/unused PPP sessions at the PDSN as soon as possible. It was carried over to the next meeting.

5. AAA V2 requirements on the current architecture

Lila Madour presented 3GPP2-P00-20001204-013, Diameter protocol requirements for release B. This contribution proposes the required DIAMETER extensions for Release B to be prioritised and communicated to the AAA working group within IETF. Ericsson and Sun will communicate the priority list to IETF.

6. Ipv6

Tom Hiller presented 3GPP2-P00-20001204-005, Solution for Collocated COA Mobiles on Carrier-Based Home Agents. The proposed solution is to distribute a PDSN address prefix to the HA and require that the HA verify the collocated COA is contained within the given prefix of the PDSN. The TSG decided to move on with the proposed solution.

7. Link layer protocol

There was no contribution on this topic.

8. Other Release B work items

Sebastian Thalanany presented 3GPP2-P00-20001204-008, Changes for Airlink Record Encoding. This contribution proposes the transfer of Airlink Records without the use of an accounting specific protocol encoding. The basic idea was accepted, and details need to be worked out including backward compatibility issue.

Dongkie Lee resubmitted 3GPP2-P00-20001204-015R2, Clarification on differentiation between Simple IP and Mobile IP, for Release B. Dongkie Lee also presented 3GPP2-P00-20001204-019, Proxy DNS Update by Home Agent for Mobile Node. Takuo Seki presented 3GPP2-P00-20001204-022, Priority of work items for Release B. These three contributions were carried over to the next meeting due to lack of time to discuss in depth.

9. New Business

A. TSG Working Group Organization

The TSG decided to have two working groups within TSG-P: Release B and All IP. Working group chairs will be elected in the January meeting. The meetings will be run serially, until parallel sessions deem necessary.

B. 1xEV-DO

The following three contributions were remanded to TSG-A/C/P joint meeting on 1xEV-DO:

Number	Title	Source
3GPP2-P00-20001204-023	Handover support in 1xEV-DO:	Ericsson, Lila Madour

	impacts on PCN resources and accounting.	
3GPP2-P00-20001204-024	Leading role for 1xEV-DO network specifications	Ericsson, Lila Madour
3GPP2-P00-20001204-025	The clarification for P00-20001204-Samsung-Key distribution	Samsung, Jun Hyuk Song, Rick Phung, Sang Yong Moon, Chae Yong Chong

Dongkie Lee presented 3GPP2-P00-20001204-016, Comment on authentication Method for HDR-based subscriber.
This contribution proposes a solution to escape NAI construction in the absence of CHAP for HDR-based subscribers.
However, the proposed solution was found an implementation issue.

The TSG discussed leading role for 1xEV-DO network specifications and decided that TSG-A should have the leading role.
However, AAA and Billing should belong to TSG-P.

10. Workplan Review

The workplan for Addendum is as follows:
- ▪ Contributions: September, 2000
- ▪ Baseline: October, 2000
- ▪ V&V   December, 2000

The workplan for Release B was updated as follows:
- ▪ Contributions: June, 2001
- ▪ Baseline: July, 2001
- ▪ V&V   September, 2001

11. Review Assignments

The assignments from the meeting were reviewed.

12. Future Meeting Schedule

Week	Location
January 15 – 19, 2001	San Diego
February 12-16, 2001	Phoenix
March 12-16, 2001	Mauai
April 9 - 12, 2001	Atlanta
May 7 – 11, 2001	China
June 11 – 15, 2001	Vancouver
July 9 - 13, 2001	Montreal
August 13 – 17, 2001	Calgary
September 17 – 21, 2001	Japan
October 15 - 19, 2001	Korea
November 5 - 9, 2001	Tucson
December 3 – 7, 2001	Mauai

13. Open Discussion

Tom Hiller volunteered to present the QoS standard status of TSG-P and IETF at the QoS JEM.

14. Adjournment

The meeting was adjourned at 4:00 PM local time on December 7, 2000.

1 **Annex A: V&V Comments**

2

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
3Com	1	2	Cover	E	Change document number to P.S0001-A-1 (global comment).
KDDI	6		2.1	O	SDB in acronyms SNMP in acronyms
3Com	9	33	2.2	E	Line up indent with other definitions on same page.
TTC	10			E	Page 10; Delete line 27 and 28 (two blank lines)
NEC	10	19	3.1	E	Delete ']' after RFC 2794
KDDI	11		3.7	O	SNMP RFC number 'Case, Fedor, Schoffstall, & Davin, A Simple Network Management Protocol (SNMP), RFC 1157, May 1990. '
QC	11	33	3.7	O	Replase A.S0001 reference as follows: TIA/EIA/IS-2001-A, Inter-Operability Specification (IOS) for CDMA 2000 Access Network Interfaces. Reason: Section 10 (R-P Interface) has referenced to TIA/EIA/IS-2001-A (a.k.a. IOS V4.1).
KDDI	12		3.8	O	X.509 in reference 'ITU-T recommendation X.509, Public-key and attribute certificate frameworks'
NEC	13	7	4	E	Replace MTO with MT0
3Com	13	10	4	E	Delete space between "-" and "2".
3Com	18	6	5	E	Add period after second "PDSN".
3Com	18	33	5.2.1.1	E	Delete comma after "mapping".
QC	18	37	5.2.1.2	E	Change "RP-session" to "R-P session".
NEC	18	37	5.2.1.2	E	Replace RP-session with R-P session
TTC	19			E	Page 19, line 13; 5.2.2_1_ should be 5.2.2.1
3Com	19	13	5.2.1.3	E	Delete space between "." and "1".
QC	19	13	5.2.1.3	E	Remove extra spacing in "5.2.2. 1 ."
Cisco	20	5	5.2.2	T	User-Name (1) = NAI User-password(2) = password (if PAP) CHAP-Password (3) = CHAP ID and CHAP-response (if CHAP) NAS-IP-Address (4) = IP address of PDSN CHAP-Challenge (60)= challenge value issued by PDSN (if CHAP)[1]Correlation ID (defined in Annex C) = An ID that correlates all accounting sessions authorized for this NAI by this access request Add Footnote: If the CHAP Challenge value is 16 octets long, it MAY be placed in the Request Authenticator field instead of using this attribute. Note: Per REC 2138, if the CHAP Challenge is 16 bits long it may be placed in Request Authenticator.
Ericsson	20	6	5.2.2	E	Remove "defined in Annex C" Replace with "Table 6: Accounting parameter attribute RADIUS definition"
3Com	20	20	5.2.2	E	Add word "may" after "server".
Ericsson	20	22	5.2.2.1	O	Add "and PAP" to title of section so that it reads:

[1]

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					"NAI Construction in the Absence of CHAP and PAP".
NEC	20	46	5.2.2.1	E	Add d after base
NEC	22	16-17	5.3	E	ditto
NEC	22	13	5.3	E	Delete 2nd comma (,) and add comma(,) after support
3Com	22	13 & 16	5.3	E	Delete comma after "should".
NEC	23	11	5.4.1.1	E	Add a period (.) at the end of sentence
TTC	25			E	Page 25; Delete line 14 (blank line)
NEC	25	39	6.2.1.2	E	Replace RP-session with R-P session
3Com	25	39	6.2.1.2	E	Change "RP-session" to "R-P session".
QC	25	39	6.2.1.2	E	Change "RP-session" to "R-P session".
Ericsson	25	42	6.2.1.2	T	**Old text**: If the PDSN receives a failure code other than 133 or 136 in the RRP. **New text**: If the PDSN receives a failure code in the RRP where repair is not permitted
SK Telecom	26	22	6.2.1.4	T	Conflict with Simple IP NAI construction PDSN is supposed to do NAI construction in the absence of CHAP for accounting purpose for Simple IP. And IS-835 also recommends that "The mobile station should not use CHAP for Mobile IP." That means if MS does not want to authenticate, it could mean Simple IP NAI construction case or Mobile IP case. After LCP negotiation phase, PDSN does not know whether MS use Simple IP or Mobile IP if MS does not want to authenticate it's user due to the above mentioned reasoning. So if MS using Mobile IP Service tries to reject CHAP, PDSN could recognize this as Simple IP NAI construction case, and do NAI construction at this time. And some vendors implemented to put MSID-realm mapping table for NAI construction in RADIUS server, and get that MSID-realm information using Access Request/Accept with username like 'IMSI-707123'. That's because RADIUS server has much more storage than PDSN, so they put that information in RADIUS server. If it is true for a lot of vendors, that's contrary to the initial concept of avoiding longer initial setup time due to PPP authentication. Although most vendors put MSID-realm mapping table in PDSN itself, anyway at PPP authentication stage PDSN internally prepares to do NAI construction and if MS is proven to use Mobile IP, PDSN clears the prepared NAI construction information. So to solve the above mentioned problem, Do not allow no authentication and NAI construction for Simple IP, and recognize no authentication as an indication for Mobile IP Mandates PPP authentication for Mobile IP, and recognize no authentication as as indication for a sort of Simple IP See uploaded document "P00-20001204-015R1-SKTelecom-Clarification.doc"
QC	27	44-46	6.2.2.5	O	If the home RADIUS server sends a Reverse Tunnel Specification attribute in the RADIUS Access-Accept indicating that reverse tunneling is required, and the mobile station did not indicate reverse tunneling in the RRQ, the PDSN shall reject the registration with an error code of 75.

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					Reason: To clarify the intend of this sentence for the scenario where reverse tunneling is required but the mobile station did not indicate reverse tunneling in the RRQ:
TTC	28			E	Page 28; Delete line 26 and 27 (two blank lines)
3Com	28	26-27	6.2.3	E	Delete these blank lines.
3Com	28	6	6.2.3	E	Add space between "RFC" and "2138".
Cisco	28	14	6.2.3	T	CHAP-Challenge $(60)^2$ = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed by the least-order 237 bytes of the Challenge Field in the MN-FA Challenge Extension. The MD5 checksum is computed over the MIP RRQ data preceding the MN-AAA Extension and the Type, Length, SPI fields of the MN-AAA Extension. Note: Per REC 2138, if the CHAP Challenge is 16 bits long it may be placed in Request Authenticator. In order to be compliant with RFC 2138, we do not want to mandate inclusion of the CHAP-Challenge attribute. Add Footnote: If the CHAP Challenge value is 16 octets long, it MAY be placed in the Request Authenticator field instead of using this attribute. Note: Per REC 2138, if the CHAP Challenge is 16 bits long it may be placed in Request Authenticator.
Ericsson	28	21	6.2.3	E	Remove "defined in Annex C" Replace with "Table 6: Accounting parameter attribute RADIUS definition"
TTC	29			E	Page 29; Delete line 23 and 24 (two blank lines). Delete lines 34 and 35 (two blank lines).
3Com	29	23-24 & 34-35	6.2.4	E	Delete these blank lines.
3Com	29	13	6.2.4	E	Add word "these" after "of".
Samsung	29	25	6.2.4	E	Rationale: Clear description Old Text: The appropriate *3GPP2 Security Level* attribute included in the Access-Accept message allows the home RADIUS server to verify whether IP security service should be provided to the user by the PDSN towards the HA. In the event the service should be provided to the user, the home RADIUS authorizes the PDSN to either use an existing security association with the corresponding HA or to establish a new security association if no prior SA exists. The home RADIUS server indicates to the PDSN if IP security should be applied on registration messages and/or tunneled data, or not to use IPsec at all. This implies that mobile stations in a given PDSN and belonging to the same HA will receive the same security service between the PDSN and HA.

[2]

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					New Text: The appropriate *3GPP2 Security Level* attribute included in the Access-Accept message allows the home RADIUS server to indicate whether IP security should be applied on registration messages and/or tunneled data from PDSN to HA, or not to use IPsec at all. The mobile stations in a given PDSN and belonging to the same HA will receive the same security service between PDSN and HA. In the event the service should be provided to the user, the home RADIUS authorizes the PDSN to either use an existing security association with the corresponding HA or to establish a new security association if no prior SA exists.
QC	29	31	6.2.4	O	This implies that mobile stations ~~in~~ served by a given PDSN and belonging to the same HA will receive the same security service between the PDSN and HA. Reason: To clarify that these mobile stations are served by a same PDSN.
Samsung	29	39	6.2.4	T	Rationale: SNMP is not necessary Old Text: Simultaneously, the Home RADIUS server shall send the Pre-Shared-Secret and KeyID attributes to the HA using SNMP event notification procedures. New Text: The pre-shared key is generated by key generator in the RADIUS server by input of RADIUS server IP address, PDSN IP address, and secret key 'S'. The 'S' shall be random number having lifetime to be periodically refreshed.
Ericsson	30	8	6.2.4	O	Emphasize that IPsec is authorized per PDSN-HA pair, not per mobile. The line should read: "The PDSN shall not delete existing IPsec security associations to a HA if the home RADIUS server does not authorize security for the mobile. This is because IPsec should be authorized per PDSN-HA pair and thus other mobiles may be using the same IPsec security association."
Samsung	30	21	6.2.4	O	Rationale: This paragraph should be placed in Radius requirements or somewhere else Old Text: The home RADIUS server will hide shared secrets using a method based on the RSA Message Digest Algorithm MD5 [RSA] as described in Section 5.2 of RFC 2138 [RADIUS]. This shared secret is associated with the next hop RADIUS server.
3Com	30	27	6.2.4	E	Change "an security" to "a security".
QC	30	39	6.3	O	Change "must" to "shall". Reason: To use "shall" consistently in Section 6.3 for mandatory requirements of HA.
QC	30	41	6.3	O	Change "must" to "shall". Reason: To use "shall" consistently in Section 6.3 for mandatory requirements of HA.
Nortel Networks	31	4	6.3.1	O	Comment: The statement is obvious as we do it anyway. Therefore, it could be ms-interpreted. *Preference is to strike this line out or expand it to clear that we already support static or dynamic address assignments for multiple registrations for different NAIs.*

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
Ericsson	31	7	6.3.2	O	Change "are required" to "may be authorized", "and" to "and/or". The sentence should read: "Security associations may be authorized for MIP control and/or payload tunnels".
Ericsson	31	7	6.3.2	O	Change "IKE" to "IPsec", and "or" to "and/or". The sentence should read: "Also, IPsec requires that all mobile stations on a given PDSN belonging to the same HA receive the same security between the PDSN and HA for registration messages and/or tunneled data".
Samsung	31	11	6.3.2	T	Rationale : SNMP is not necessary Old Text: The Home Agent will receive the *Pre-Shared-Secret* and the *KeyID* from the RADIUS server via SNMP event notification. The Home RADIUS and HA are assumed to be in the same administrative domain. Therefore, a secure communication path for SNMP is assured. New Text: HA shall have a table that may have 'S' key received from home RADIUS servers. Each key in the table shall also have lifetime set by home RADIUS server. Upon receipt of IKE handshake request from PDSN, HA shall make the pre-shared key by KeyID (Annext C), and 'S' key. HA shall check the 'S' key table indexed by Home RADIUS server IP address. If it wasn't listed in the table, Home RADIUS server shall request a secret key 'S' from the home RADIUS server in an Access Request by using a concatenation of the PDSN's care of address and home agent address placed in the user name attribute. The security of the Home Agent and Radius server is outside the scope of this standard.

Motorola	31	19	6.3.4	T	Current text:
					
					User-Name (1) = MN-NAI field in the MN-NAI Extension
					CHAP-Password (3) = High-order byte of the Challenge Field in the MN-FA Challenge Extension, followed by the Authenticator field from the MN-AAA Extension
					CHAP-Challenge (60) = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed by the least-order 237 bytes of the Challenge Field in the MN-FA Challenge Extension. The MD5 checksum is computed over the MIP RRQ data preceding the MN-AAA Extension and the Type, Length, SPI fields of the MN-AAA Extension.
					
					Proposed change:
					
					User-Name (1) = MN-NAI field in the MN-NAI Extension
					CHAP-Password (3) =
					   CHAP Ident field = High-order byte of the Challenge Field in the MN-FA Challenge Extension
					   String field = Authenticator field from the MN-AAA Extension
					CHAP-Challenge (60) = MD5 (Preceding MIP RRQ, Type, Length, SPI), followed by the least-order 237 bytes of the Challenge Field in the MN-FA Challenge Extension. The MD5 checksum is computed over the MIP RRQ data preceding the MN-AAA Extension and the Type, Length, SPI fields of the MN-AAA Extension.
					.

Samsung	31	33	6.4	T	Rationale: SNMP is not necessary.

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					Old Text: The Home RADIUS server shall also support sending of the *Pre-Shared-Secret* and the *KeyID* to the HA using the SNMP event notification procedures. New Text: The Home RADIUS server shall also support sending of the secret 'S' key and its lifetime to the HA using the RADIUS Access Accept message.
3Com	31	37	6.4	E	Delete comma after "support".
QC	33	28	6.5.2.3	O	Need an RFC number for [FAC].
QC	33	32	6.5.2.3	O	Because advertisements are rarely sent to save air resources, the mobile station should use the challenge value contained in the ~~most recent~~ last received RRP in the case of re-registrations as described in [FAC]. Reason: The wording "most recent" is ambiguous.
Ericsson	34	48-49	7.3	T	Add a bullet between line 48 and 49: authentication by the RADIUS infrastructure
3Com	34	8 & 13	7.2	E	Add word "the" prior to "PPP session".
3Com	35	7	8.1	E	Delete comma after "support".
TTC	37			E	Page 37; Add a blank line between line 29 and 30.
3Com	37		Figure 8	E	Add comma after "i.e.".
Ericsson	37	25	9.1	E	**Old text**: Table 5 in section 9.4 **New Text**: Table 5 in section 9.3
FUJITSU	37	25	9.1	E	Section 9.4 should be Section 9.3
Ericsson	38		9.2.1 9.2.2 9.2.3 9.2.4	T	1. All the detailed specifications of airlink records should be removed since IOSV4.1 has included all the detailed accounting specifications required as per TSG-P request. The changes brought up to the addendum should be liaised to TSG-A.
Nortel Networks	38		9.2.2	O	Table 2: Delete rows for f3 and f4. These rows correspond to rate set. Rate set is now a subset of RC which contained in f9 and f10. f3 and f4 are therefore redundant.
3Com	38	3	9.2	E	Delete underline under period.
Ericsson	38	22	9.2	T	Add the following: Details specification of airlink records are found in IOSV4.1 (section 6.2.2.166 of IOS V4.1)
3Com	38	2, 6, & 29	9.2	E	"R-P session ID" should be "R-P Session ID".
Nortel Networks	39		9.2.2	T	Table 2: Add row f14 with parameter "DCCH Frame Size (0/5/20 ms)", length=4, format=integer. In cdma2000, **either or both** the fundamental and/or DCCH may be present. Either one may be 5 or 20 ms frame size. By adding f14 and using in conjunction with f8, the accounting record can reflect whether fundamental and/or DCCH was present and which had 5 or 20 ms frames. Without f14, the accounting record is incomplete.
3Com	39	Item A1	Table 5	E	Add comma after "e.g.".
Nortel Networks	40		9.3	O	Delete rows F3 and F4. These rows correspond to rate set. Rate set is now a subset of RC which contained in F9 and F10. F3 and F4 are therefore redundant.

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
Nortel Networks	40		9.3	T	Add row F14 with parameter "DCCH Frame Size" and description "The dedicated signaling channel has the choice of 5 or 20 ms size. The 5ms frame size allows fast response from short signaling messages (short frame can be decoded quickly). However, depending on the configuration, the DCCH may not be present." In cdma2000, **either or both** the fundamental and/or DCCH may be present. Either one may be 5 or 20 ms frame size. By adding F14 and using in conjunction with F8, the accounting record can reflect whether fundamental and/or DCCH was present and which had 5 or 20 ms frames. Without F14, the accounting record is incomplete.
QC	40	D4	9.3	O	In the third column, replace "base ID" with "Base Station ID".
QC	40	G14	9.3	O	Clarify the second column as follows: Number of HDLC-layer bytes received
SK Telecom	40		9.3	O	Add text after G1 with "This includes PPP bytes without HDLC-like framing. (Exclude flags, Address, Control, FCS fields, Control Escaping Characters) Excludes PPP Control Messages. (LCP, Authentication, IPCP) Other Control Messages (Agent Advertisement, Mobile IP Registration Reply) Add text after G2 with This includes PPP bytes without HDLC-like framing. (Exclude flags, Address, Control, FCS fields, Control Escaping Characters) Excludes PPP Control Messages. (LCP, Authentication, IPCP) Other Control Messages (Agent Solicitation, Mobile IP Registration Request) See uploaded document "P00-20001204-018R1-SKTelecom-OctetCount.doc"
Samsung	40		9.3 Table 5 G1	T	Rationale: It caused lots of confusion for carriers. Old Text: total # of octets sent to the user. This includes the bytes between HDLC flags before escaping New Text: total # of IP packet octets sent to the user. This excludes HDLC flags, Address, Control , Protocol, FCS fields, escape characters, and the LCP and NCP packets
Samsung	40		9.3 Table 5 G2	T	Rationale: It caused lots of confusion for carriers Old Text: total # of octets sent to the user. This includes the bytes between HDLC flags before escaping New Text: total # of IP packet octets sent to the user. This excludes HDLC flags, Address, Control , Protocol, FCS fields, escape characters, and the LCP and NCP packets
NEC	40		Table 5		In descriptions of G1, G2 and G3 '#' could be changed to 'number' for keeping consistency with others (G9 – G13)

Nortel Networks	40
	
	42
		24
		
		5
			9.3
			
			9.4
				T
				
				T
					Add C3 in table 5
					Item Parameter Description
					C3 Session Continue This attribute when set to 'true' means it is not the end of a
					
					                                               Session and an Accounting Stop is immediately followed
					
					                                               By a start Record. 'False' means end of a session.
					
					Add C3 in table 6

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
	45	50	9.5.1	T	**Item Parameter Type Maximum Format Field Special Values** ** Payload Length** C3 Session Continue 26/46 4 integer 3GPP2 0=False, 1=True
	46	19	9.5.3	T	_Session_cont
	46	45	9.5.5	T	Or, <u>add a Session Continue attribute in the UDR with the value set to 1 (True).</u> Send a RADIUS Accounting-Request Stop record based on the current UDR.
	47	33	9.5.9	T	<u>Add a Session Continue attribute in the UDR with the value set to 0 (False).</u> Send a RADIUS Accounting-Request Stop record based on the current UDR.
	47	46	9.5.10	T	Or, <u>add a Session Continue attribute in the UDR with the value set to 1 (True).</u> Send a RADIUS Accounting-Request Stop record based on the current UDR. When the Stop Record Trigger initiates, the PDSN shall <u>add a Session Continue attribute in the UDR with the value set to 1 (True). Then the PDSN shall</u> send a RADIUS Accounting-Request Stop record based on the current UDR. Or, <u>add a Session Continue attribute in the UDR with the value set to 1 (True).</u> Send a RADIUS Accounting-Request Stop record based on the current UDR.
FUJITSU	41 44 48	 3, 5	Table 5, I4 Table 6, I4	E	TIA document numbering should be 3GPP2 document numbering to keep consistency with others
Ericsson	41	5	9.4	T	Remove the following line: RN parameters transmitted across the RP interface shall follow the RADIUS format.
Nortel Networks	42		9.4	O	Delete rows F3 and F4. These rows correspond to rate set. Rate set is now a subset of RC which contained in F9 and F10. F3 and F4 are therefore redundant.
QC	42	D4	9.4	O	In the last column, replace "base ID" with "Base Station ID".
Nortel Networks	43		9.4	T	Add row F14 with parameter "DCCH Frame Size", type=26/14, length=4, format=integer, field=3GPP2_DCCHSIZE, Special values "0=no DCCH, 1=5 msec frame, 2=20 msec frame" In cdma2000, **either or both** the fundamental and/or DCCH may be present. Either one may be 5 or 20 ms frame size. By adding F14 and using in conjunction with F8, the accounting record can reflect whether fundamental and/or DCCH was present and which had 5 or 20 ms frames. Without F14, the accounting record is incomplete.
Nortel Networks	43		9.4	O	Row H1 special values should be "currently undefined"
Cisco	43	??	9.4	T	Parameter: F13 -- Release Indicator

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment

					Clarification needed for Values:
					  3=PPP protocol failure
					  4=PPP abnormal release
					
					Note: Under what conditions the above mentioned values would be used is not clear. Recommend removing these two values.

QC	43	G14	9.4	O	Clarify the second column as follows: Number of HDLC-layer bytes received
Nortel Networks	44		9.4	O	Row I2 special values should be "currently undefined"
TTC	45			E	Page 45; Add a blank line between line 2 and 3.
3Com	45	15	9.5	E	Change "pairs" to "pair".
3Com	45	18	9.5	E	Change "correlation" to "Correlation".
3Com	45	20	9.5	E	Change "Accounting session ID" to "Account Session ID".
3Com	45	22	9.5	E	Change "RP session ID" to "R-P Session ID".
3Com	45	37	9.5	E	Change "Correlation Session" to "Correlation".
3Com	45	23, 26, & 27	9.5	E	Change "R-P session ID" to "R-P Session ID".
3Com	46	31	9.5.4	E	Add period at end of line.
Cisco	46	31	9.5.4	T	Increment G14 by the number of octets received at the PPP HDLC layer
KDDI	46	31	9.5.4	E	PPP replaced with HDLC
SK Telecom	46	40	9.5.5	T	Replace with "Otherwise, if airlink record indicates parameters E1, or I4 have changed," by "Otherwise, if airlink record indicates parameters E1, F1, F2 or I4 have changed," See uploaded contribution "P00-20001204-017-SKTelecom-MuxOption.doc"
3Com	46	50	9.5.5	E	Change "Accounting" to "Account".
3Com	47	7	9.5.7	E	Change period to colon at end of line.
3Com	47	25	9.5.9	E	Change "records" to "record".
3Com	47	35 & 49	9.5.9 & 9.5.10	E	Change "Accounting" to "Account".
3Com	48	6 & 7	10	E	Add comma after "i.e." and "e.g.", respectively.
QC	49	34	11.1	O	Replace "A.S0001" by "TIA/EIA/IS-2001-A".
Ericsson	51	18	Annex A	O	Add Main Mode as an option for the ISAKMP fixed header of Phase 1. The sentence should read: "The ISAKMP Fixed Header may indicate a Main Mode or Aggressive Mode exchange for Phase 1 ISAKMP, Quick Mode for all Phase 2 exchanges, or an Informational exchange to pass notification regarding security lifetimes.
HITACHI	51 52	22 30 3	Annex A	E	Delete colon(:) after subtitle to keep consistency others subtitles
Ericsson	51	26	Annex A	E	Add underscore so that "SIT IDENTITY ONLY" becomes "SIT_IDENTITY_ONLY".
NEC	51	28	Annex A	E	Standards -> standards
Ericsson	51	34	Annex A	O	Remove mention of using ESP for the ISAKMP SA created in Phase 1. The following sentence should be removed:

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					"Service provider owned HAs will support IPsec ESP (using 3DES) for the ISAKMP SA."
Ericsson	51	51	Annex A	T	If the Home RADIUS indicates a request for no security on the IP-in-IP tunnelled packets, do not delete existing SAs. The sentence should read: "If the Home RADIUS indicates a request for no security on the IP-in-IP tunnelled packets, the PDSN shall not delete existing IPsec security associations to the HA. This is because IPsec should be authorized per PDSN-HA pair and thus other mobiles may be using those IPsec security associations."
TTC	52			E	Page 52; Add a blank line between line 20 and 21.
Ericsson	52	4	Annex A	O	Add a sentence which reads: "For Phase 1, the PDSN shall use KEY_IKE as the transform identifier."
Ericsson	52	5	Annex A	O	Specify that this paragraph applies to Phase 2. The sentence should read: "For Phase 2 Quick Mode exchange, the PDSN shall minimally support the ESP_3DES transform identifier within a Transform Payload for IPsec ESP Proposal Payload. It must also support both HMAC-MD5 and HMAC-SHA as transform identifiers within a Transform payload for IPsec AH Proposal Payload."
Ericsson	52	10	Annex A	O	There are 3 messages used in the Quick Mode exchange, mention that Main Mode uses 6 messages: The sentence should read: "The PDSN and HA IP security negotiations should complete within six messages for a Main Mode exchange and three messages for Aggressive Mode and Quick Mode exchanges."
3Com	52	20	Annex A	E	Add <CR> at end of line.
Ericsson	52	26	Annex A	O	This section should be re-written as follows: "For Phase 1 negotiation, the PDSN must set the Protocol-Id field to zero or UDP. The port number must be set to zero or 500. If the HA receives any other values for these two fields in the Identification Payload, IKE negotiation must be aborted. For IKE authentication using preshared key, the PDSN and HA shall minimally support ID_IPV4_ADDR in the ID Type field. For IKE authentication using Revised Public Key Encryption with RSA using X.509 certificates, the PDSN and HA shall minimally support ID_DER_ASN1_DN in the ID Type field. For Phase 2 (Quick Mode), both the PDSN and HA may include the client identifiers in the form of optional Client Identification Payloads as specified in IKE (ie. IDci and IDcr). Two separate Quick Mode negotiations must be performed to establish two different types of IPsec security associations between the PDSN and HA to protect mobile IP control messages and tunnelled user data.

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
					For IPsec security for MobileIP control packets, the PDSN and HA shall exchange IDci and IDcr. The protocol field shall be set to UDP and port number to 434 for both IDci and IDcr. For IPsec on the user's tunnelled data, the PDSN and the HA exchange client identification identifying a tunnel protocol type that matches the encapsulation type requested by the mobile station's RRQ.
Ericsson	52	26	Annex A	O	This section should be re-written as follows: "For Phase 1 negotiation, the PDSN must set the Protocol-Id field to zero or UDP. The port number must be set to zero or 500. If the HA receives any other values for these two fields in the Identification Payload, IKE negotiation must be aborted. For IKE authentication using preshared key, the PDSN and HA shall minimally support ID_KEY_ID in the ID Type field. For IKE authentication using Revised Public Key Encryption with RSA using X.509 certificates, the PDSN and HA shall minimally support ID_DER_ASN1_DN in the ID Type field. For Phase 2 (Quick Mode), two separate Quick Mode negotiations must be performed to establish two different types of IPsec security associations between the PDSN and HA to protect mobile IP control messages and tunnelled user data. Both the PDSN and HA shall include the client identifiers in the form of optional Client Identification Payloads as specified in IKE (ie. IDci and IDcr). For IPsec security for MobileIP control packets, the PDSN and HA shall exchange IDci and IDcr. The protocol field shall be set to UDP and port number to 434 for both IDci and IDcr. IDCi: Protocol field=UDP,Port=434,Idtype=ID_KEY_ID, Identification_data=PDSN_IPV4_ADDR IDCr: Protocol field=UDP,Port=434,Idtype=ID_KEY_ID, Identification_data=HA_IPV4_ADDR For IPsec on the user's tunnelled data, the PDSN and the HA exchange client identification identifying a tunnel protocol type that matches the encapsulation type requested by the mobile station's RRQ. Example of IDCi and IDCr values when IP-IP tunnel is used are: IDCi: Protocol field=IP-IP,Idtype=ID_KEY_ID, Identification_data=PDSN_IPV4_ADDR IDCr: Protocol field=IP-IP,Idtype=ID_KEY_ID, Identification_data=HA_IPV4_ADDR
TTC	54			E	Page 54, lines 21 and 22; HA or PDSN -> PDSN or HA, HA and PDSN -> PDSN and HA
NEC	55	12	Annex B	E	Replace carrier CA with service provider CA
NEC	55	17	Annex B	E	Add s after provider
NEC	58			E	2 formats should keep consistency with the format shown in page 56. Accounting container is shown by octal.
3Com	59	1	Annex	E	Add <CR> after "RADIUS Accounting" and make line Heading 1

2. Source (Company Name)	3. Page	4. Line	5. Section	6. Type	8. Comment
			D		format.

1
2