The 1st UMTS FemtoCell Plugfest;
Sophia Antipolis, France;
22-26 March 2010

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute yyyy.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

1 Executive Summary

The 1st UMTS FemtoCell Plugfest event was held from 22 to 26 March 2010 in Sophia Antipolis (France).

This event, which was co-organized by ETSI and the Femto Forum, aimed to test the interoperability between residential equipment and network components for the FemtoCell (or Home Node B) protocols.

This event required a very detailed preparation in order to allow the communication between network component located at remote sites, and the vendor implementations operating in the Plugfest premises.

22 companies participated in this event executing more than 1000 interoperability tests.

Despite the fact that some vendor's implementations did not support all mandatory features, more than 65 % of the tests were successful. This result shows the high level of maturity of the FemtoCell technology.

2 Introduction

This Plugfest event aimed to verify the interoperability between FemtoCell products from different vendors.

The FemtoCell technology is using several different components. This Plugfest event focused on the following types of equipment:

- Femto access points (FAP), also named interchangeably Home Node B (HNB),
- Security Gateways (SeGW),
- Femto Gateways (FGW), also named interchangeably Home Node B Gateways (HNB-GW)

All HNBs were provided by vendors at the Plugfest premises, in Sophia Antipolis. But the Gateways (either SeGW or HNB-GW) were partly located at vendor's premises. This fact had to be taken into account during the event preparation.

3 Abbreviations

FAP:	Femto Access Point
FGW:	Femto GateWay
HNB:	Home Node B
HNB-GW:	Home Node B GateWay
NO:	Test is recorded as NOT successfully passed.
NA:	Test is not applicable.
OK:	Test is recorded as successfully passed.
OT:	Test is recorded as not being executed due to lack of time.
SeGW:	Security GateWay
Test Session:	A paring of vendors that test together during a given time slot.
TSR:	Test Session Report. Report created during a test session.

5 Event preparation

5.1 Testbed setup

The first task of the event preparation consisted of deploying a testbed that should allow a seamless and secured communication between on-site and remote components.

To ensure secure IP communications between remote and on-site components, it was decided to allow the participants to use a VPN tunnel. This was achieved by using the HIVE (HUB for Interoperability and Validation at ETSI). The vendors, who intended to use the HIVE VPN network, were asked to provide technical information about their remote IP addresses. The HIVE documentation is described in the Annex A.

Furthermore, participants operated their local equipment in dedicated IP subnets, allowing to monitor the IP traffic and to isolate their component from the other vendor's ones.

This was realized by creating an IP subnet for each participating company and allowing communication between these subnets.

The figure **1** below shows the resulting network topology with the VPN routes and the IP subnet allocated to the vendors.

Two physical accesses were granted during the Plugfest:

- One SDSL 4Mb, to support the IP traffic between remote sites and the local component, this IP traffic was distributed over switches and Ethernet connections
- One ADSL 8Mb/1Mb to allow all participants to access internet, without disturbing the IP traffic dedicated to the testing.

Furthermore, domain names were created for each vendor's device, which require connection with other vendors.

The resulting physical network is as described in the figure 2 below.

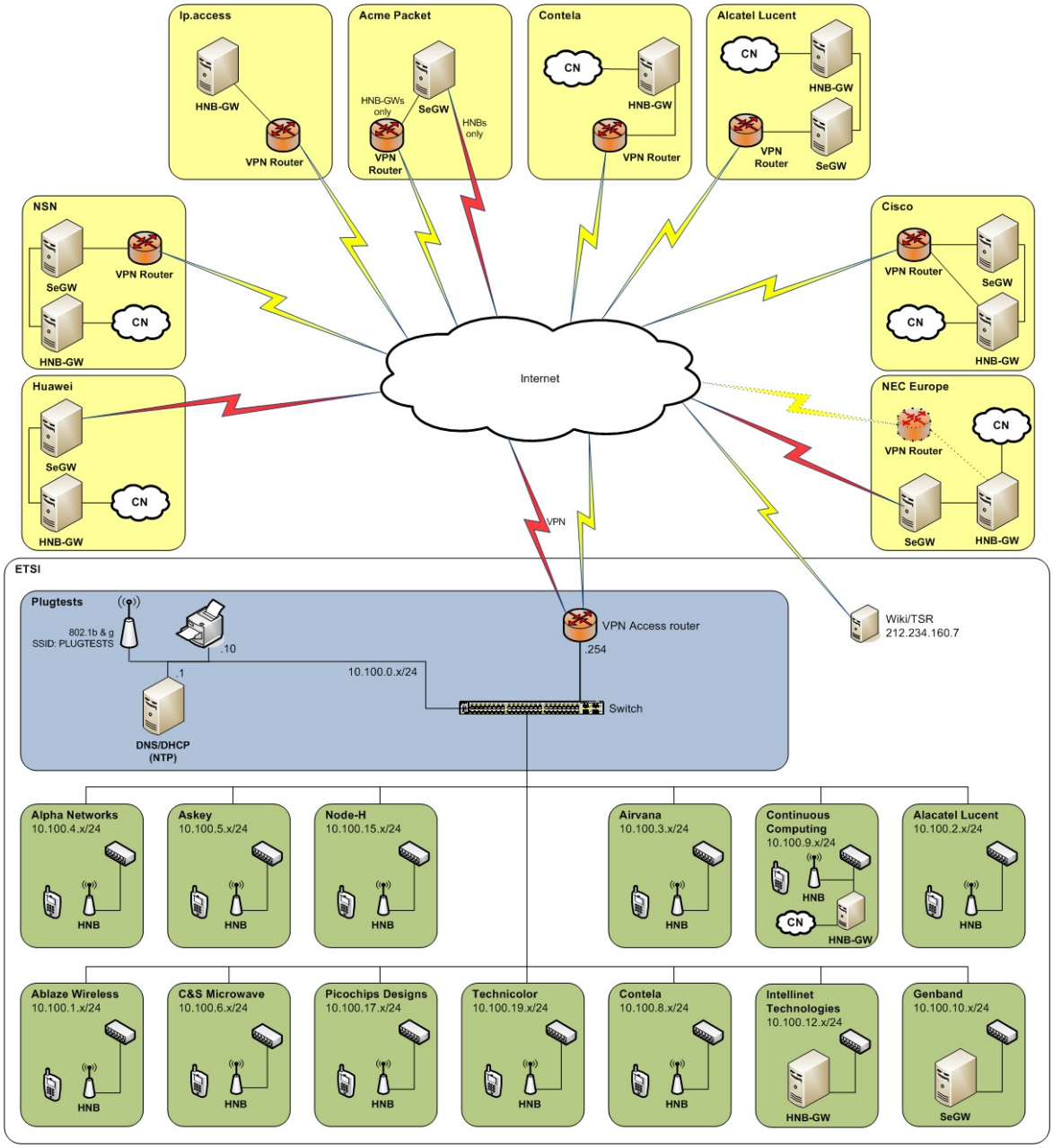

Figure1: the network topology

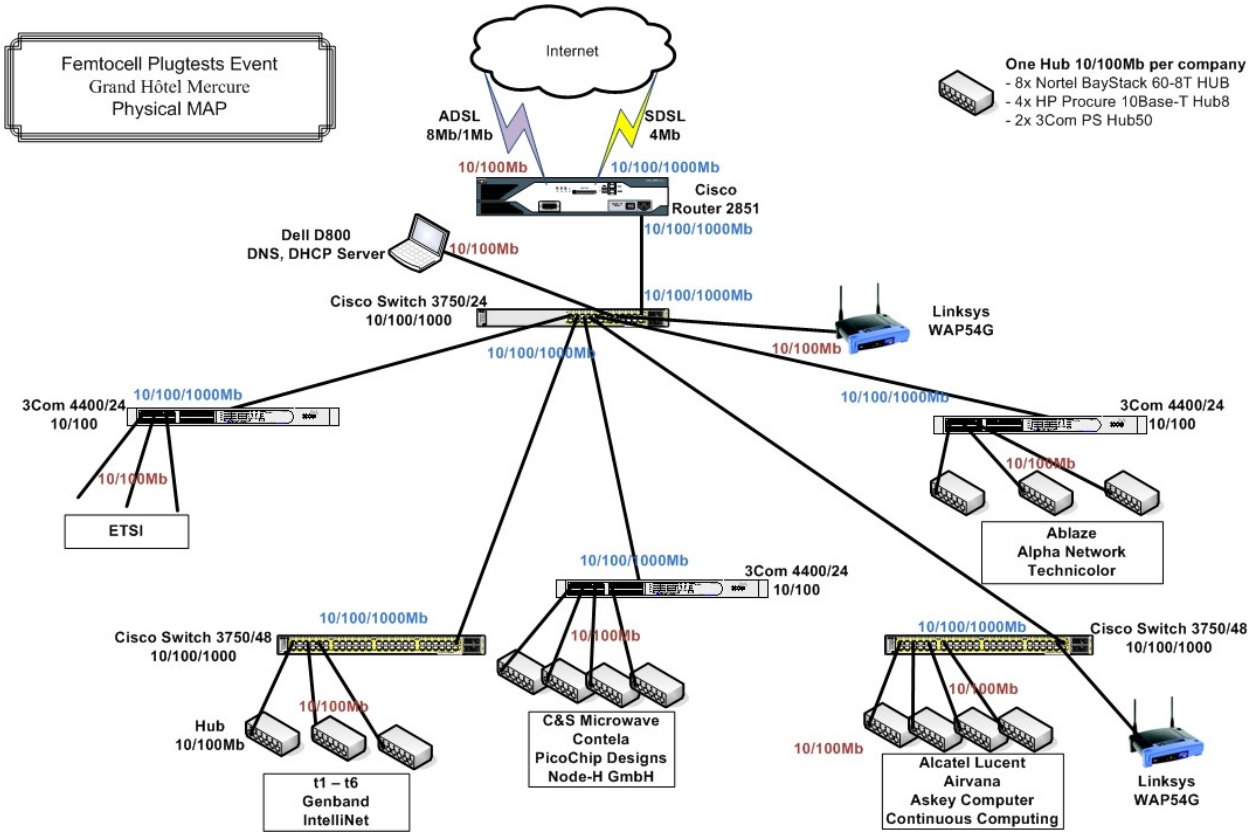

Figure2: the physical network

5.2 The test specifications

The test specification applying for this Plugfest event were the "Fa Interface Interoperability requirement", provided by the IOT working group (WG3) of the Femto Forum. The test cases were analyzed by ETSI/CTI and discussed during the conference calls dedicated to the event preparation.

The test specification contains test cases to test the interoperability of Femto systems, considering FAP (HNB), FGW (HNB-GW) and SeGW components. The release applying to the present plugfest event was the draft version 0.9, of March 2010. It contained 29 test cases, but only 26 test cases applied to the present plugfest event. The 3 other test cases were reserved for a phase 2 Interoperability event.

The table 1 below shows the test scenarios, grouped by protocol features, and indicates which types of equipment are involved in the test process:

Table 1: the test cases

Group	TD Identifier	Summary	HNB	SeGW	HNB-GW
HNB Registration	FIC/HNB/01	HNB Registration with HNB-GW	Y	Y	Y
	FIC/HNB/02	HNB Rejection from HNB-GW – Access Control	Y	Y	Y
	FIC/HNB/03	HNB Rejection from HNB GW – Overload Condition [Phase-2]	Y	Y	Y
	FIC/HNB/04	HNB-GW Redirection	Y	Y	Y
	FIC/HNB/05	HNB De-Registration – Initiated by HNB	Y	Y	Y
	FIC/HNB/06	HNB De-Registration – Initiated by HNB-GW due to Overload [Phase-2]	Y	Y	Y
	FIC/HNB/07	HNB Re-Registration – Loss of IP Connectivity	Y	Y	Y
	FIC/UET/01	UE Registration with HNB-GW (non-CSG)	Y	Y	Y
UE Registration	FIC/UET/02	UE Registration Rejection from HNB-GW(non-CSG)	Y	Y	Y
	FIC/UET/03	UE De-Registration with HNB-GW, UE Power Off (non-CSG)	Y	Y	Y
	FIC/UET/04	UE De-Registration with HNB-GW, Periodic Timer Expiry (non-CSG)	Y	Y	Y
	FIC/UET/05	UE De-Registration from HNB-GW (non-CSG)	Y	Y	Y
	FIC/UET/06	UE Re-Registration with HNB-GW (non-CSG)	Y	Y	Y
Iuh Disconnect	FIC/IUH/01	Iu Release	Y	Y	Y
Services	SVC/CSO/01	CS - Mobile Originating (non-CSG)	Y	Y	Y
	SVC/CSO/02	CS - Mobile Terminating (non-CSG)	Y	Y	Y
	SVC/PSO/01	PS - Mobile Originating (non-CSG)	Y	Y	Y
	SVC/CPS/01	CS+PS - Mobile Originating (non-CSG)	Y	Y	Y
	SVC/EMG/01	Emergency Call - Unauthorised UE (non-CSG)	Y	Y	Y
	SVC/EMG/02	Emergency Call - (U)SIM-less UE (non-CSG)	Y	Y	Y
	SVC/SMS/01	SMS - UE Originating (non-CSG)	Y	Y	Y
Mobility	MOB/CSO/01	CS Handout to Macro Layer [Phase-2]	Y	Y	Y
Security	SEC/FSG/01	FAP – SeGW Crypto Profile Configuration and Basic Tunnel Establishment	Y	Y	
	SEC/FSG/02	Use of NAT-T	Y	Y	
	SEC/FSG/03	Use of NAT-T – Dynamic Address Change	Y	Y	
	SEC/FSG/04	DPDs	Y	Y	

Annex A: HIVE documentation

A.1 Introduction

Paperwork for establishing a request to get remote access to the HIVE (Hub for Interoperability and validation at ETSI).

The objective is to give participants technical elements about the HIVE platform and gather mandatory pieces of information for ETSI to implement VPN tunnel between the local site and the participant's sites.

A.2 to be filled by the Requester

Table 2: Form to provide business information

Concern	Value	Description
Company		Your Company name
Name		Your name
Phone number		Your phone number
Email	mailto:gboue@streamwide.com	Your Email address
Mailing Address	Address: Country:	Your mailing address within the company
Project		Specify project / event name
Project Manager's name		Project Manager's name within your company accountable for your request
Project Manager's e-mail		Project Manager's email address within your company accountable for your request
Technical contact's name		Contact name of technical person responsible for implementation at requestor side.
Technical contact's e-mail		Email address of technical person responsible for implementation at requestor side.
Date of request	/ /	Date of request (dd/mm/yyyy) at least 15 days before deadline
Deadline	/ /	Deadline to establish VPN connectivity (dd/mm/yyyy)
End date	/ /	End date of the project / event (dd/mm/yyyy)
Business Reason of Connection		

Table 3: Form to provide service data

Concern	Value	Description
Service Description	IPSec GRE	
Remote IPs/Subnets	**Error! Bookmark not defined.**	Specify IP addresses / IP address range – (x.x.x.x – x.x.x.x/yy)
Remote Gateway		Public IP Address of company's Firewall or router
Remote Gateway equipment	mailto:gboue@streamwide.com	Model of the equipment use to establish VPN tunnel to HIVE. Good to know in case of troubleshooting

A.3 Technical Specifications Summary

Table 4: applicable security procedures

	Type	Policy 1	Policy 2
IKE Phase 1 (ISAKMP SA)	Encryption	AES 256 bits	AES 128 bits
	Authentication	Pre Shared Key	Pre Shared Key
	Hash Algorithm	SHA-1	SHA-1
	Lifetime	14400 sec	14400 sec
	Diffie Hellman	Group 5	Group 2

IKE Phase 2 (IPSec SA)	Protocol	ESP
	Mode	Tunnel
	Encryption	AES 128 bits
	Hash Algorithm	SHA-1 and/or MD5
	Lifetime	86400 sec
	PFS (Perfect Forward Secrecy)	No
	Replay Detection	Disabled
	Diffie Hellman	Group 1 (default)

VPN Gateway	ETSI Side	212.234.160.1	This IP may change accord to the event location
	Model	Cisco 2851	

HIVE networks	ETSI Side	10.100.0.0/16 and 212.234.160.1/24	This IP may change accord to the event location
Routing protocol	Dynamic routing	OSPF	Manage ACL on your equipment to limit access via your tunnel
		Area 0	

Pre-Shared key and **Tunnel IP address** will be communicated directly to the Technical contact indentified in the Business information table above.

A.4 VPN network architecture

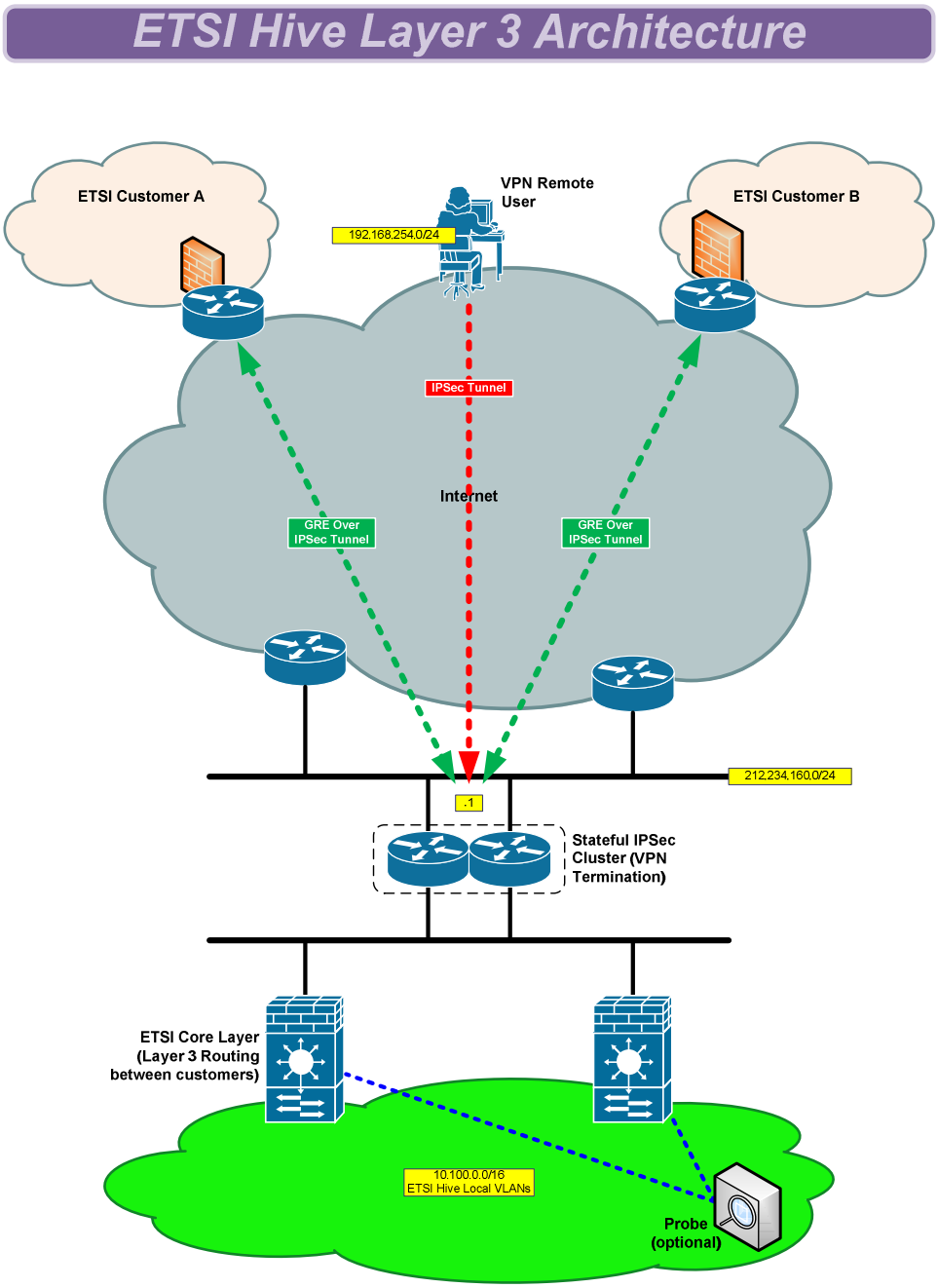

Figure 3: HIVE architecture

A.5 IPSec Protocol Reminder

ETSI has chosen to use Router platforms in order to provide a site-to-site WAN connectivity with his customers or partners. The solution is based on IPSec standards, IKE and ESP.

A.5.1 IPSec Protocol

A.5.1.1 Phase 1

The basic purpose of ***IKE Phase 1*** is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. IKE Phase 1 occurs in two modes: main mode and aggressive mode.

The main mode has three two-way exchanges between the initiator and receiver:

- First exchange: the algorithms and hashes used to secure the IKE communications are negotiated and agreed upon between peers.
- Second exchange: this exchange uses a DH exchange to generate shared secret keys and pass nonces, which are random numbers, sent to the other party, signed, and returned to prove their identity. The shared secret key is used to generate all the other encryption and authentication keys.
- Third exchange: this exchange verifies the other side's identity. It is used to authenticate the remote peer. The main outcome of main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, you might establish a secure communication channel with a hacker who could be stealing all your sensitive material.

The main outcome of the main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, it is possible that you might establish a secure communication channel with a hacker who will steal your sensitive material.

In the aggressive mode, fewer exchanges are done and with fewer packets. The first exchange covers almost all of the steps: the IKE policy set negotiation; the DH public key generation; a nonce, which the other party signs; and an identity packet, which can be used to verify the identity of the other party via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange.

A.1.5.1.2 Phase 2

The purpose of ***IKE Phase 2*** is to negotiate the IPSec security parameters used to secure the IPSec tunnel. These functions are performed in IKE Phase 2:

- Negotiation of IPSec security parameters and IPSec transform sets
- Establishment of IPSec SAs
- Periodic renegotiation of IPSec SAs to ensure security
- Optionally, performance of an additional Diffie-Hellmann exchange

IKE Phase 2 has one mode, called Quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. Quick mode negotiates a shared IPSec transform, derives shared secret keying material used for the IPSec security algorithms, and establishes IPsec SAs. Quick mode exchanges nonces that are used to generate new shared secret key material and to prevent replay attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires. Quick mode is used to refresh the keying material used to create the shared secret key based on the keying material derived from the Diffie-Hellmann exchange in Phase 1.