



Inspired Innovation

White Paper

Security Aspects in a Packet Data Network

February 2007

Spirent Communications, Inc.

1325 Borregas Avenue
Sunnyvale, CA 94089 USA

Email: sales-spirent@spirent.com

Web: <http://www.spirent.com>

Americas

T: +1 800.SPIRENT
+818 676.2683

Europe, Middle East, Africa

T: +33 1 6137.2250

Asia Pacific

T: +852 2511.3822

Copyright

© 2007 Spirent Communications, Inc. All Rights Reserved.

All of the company names and/or brand names and/or product names referred to in this document, in particular, the name “Spirent” and its logo device, are either registered trademarks or trademarks of Spirent plc and its subsidiaries, pending registration in accordance with relevant national laws. All other registered trademarks or trademarks are the property of their respective owners.

The information contained in this document is subject to change without notice and does not represent a commitment on the part of Spirent Communications. The information in this document is believed to be accurate and reliable; however, Spirent Communications assumes no responsibility or liability for any errors or inaccuracies that may appear in the document.

Security Aspects in a Packet Data Network

Contents

- Introduction4
 - Purpose and Scope.....4
- Overview4
- Security Solutions6
 - IPSec Gateways6
 - IMS Authentication and Key Agreement (AKA)7
 - L2TP8
 - AAA.....9
- Test Considerations10
 - IPSec Gateways11
 - IMS AKA.....13
 - L2TP14
 - AAA.....15
 - DoS16
- Acronyms18

Introduction

In today's world of thriving mobility and data centric applications – short messaging, e-mail, and web browsing – mobile network operators and enterprises face a growing threat of electronic attacks on their network elements. As the threats become more sophisticated, potential solutions become increasingly complex and costly. These costs are not only financial but impact the overall network performance as well. It has become vital to verify security solutions and validate network performance and reliability under a variety of conditions that may one day impede system performance or bring it down entirely.

Purpose and Scope

This document discusses security concepts in a packet data network (PDN) and offers testing considerations for the protection of networks. While several types of attacks are addressed, this paper does not attempt to define the threats nor does it propose specific solutions to such threats. It is an overview of how to test for threats and offers ways to determine if your network is vulnerable.

Overview

Malicious or even inadvertent attacks can be expensive. While loss of personal or credit information makes news headlines, other unpublicized consequences are just as costly. Recovery from system degradation, network failure, exhaustion of resources, and destroyed or altered data files are a time consuming and expensive undertaking.

This list of threats is by no means complete, but it does describe several common attacks that negatively impact packet data networks.

The following are discussed individually below:

- Viruses/Trojan Horses
- Denial of Service (DoS)
- Agent Spoofing
- Unauthorized Access
- Worm
- Replay Attack

Virus/Trojan Horses

A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a spreadsheet program. Each time the spreadsheet program runs, the virus also runs and has the chance to reproduce (by attaching to other programs) or wreak havoc. A Trojan horse is simply a computer program that claims to do one thing (it may claim to be a game) but instead does damage when you run it (erase your hard drive, for example). Trojan horses do not replicate automatically.

Denial of Service (DoS)

DoS is an attack that targets network resources with the intention of reserving resources and keeping legitimate users from gaining access. An example is a SYN attack. When a TCP/IP client initiates a session, the client transmits a SYN packet to the server. Upon receipt of the SYN, the server reserves resources for the anticipated session and responds back to the client seeking further identification. The client ignores the response from the server – thus reserving resources with no intention of using them. The real threat of this attack comes when a malicious client (or multiple clients) generates a large number of SYN requests. The server honors these requests and eventually runs out of resources for legitimate sessions.

Agent Spoofing

IP spoofing is accomplished when an outside hacker uses a discovered IP address to gain access to the trusted environment. In addition to IP spoofing, a malicious user can simulate network devices such as a SGSN and generate requests for service to peers (GGSNs in this example). DoS or hijacked sessions can result from agent spoofing.

Unauthorized Access

Unauthorized access occurs when malicious user gain access to the network or services for which they have not subscribed. In the simplest scenario, a hacker uses the ID (and password) of an unsuspecting, valid user and gains access.

Worms

A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine with that specific security hole. The worm copies itself to the new machine using the security hole and replicates from there as well.

Replay Attacks

A replay attack occurs when a hacker intercepts a communication between two parties and replays the message. For instance, a hacker might intercept a credit card transaction between a consumer and a Web site. The hacker then replays the transaction multiple times resulting in multiple debits to the consumer's credit account.

Security Solutions

The security options facing a service provider or network operator are many and complex. Some current security solutions focus on data integrity and data confidentiality, user authentication and authorization, and point of entry control.

Internet Protocol Security (IPSec) protects traffic between two peers by authenticating the end points, ensuring the integrity of the packets and encrypting packets that are sent to a peer. A peer is any network element with IPSec capability: a security gateway, Home Agent or GGSN. Two peers negotiate one or more Security Associations (SA) consisting of keys that allow the peers to tunnel traffic over IPv4 or IPv6.

AAA servers, whether Radius- or Diameter-protocol based, authenticate the user (ensuring users are who they claim to be); authorize the user (allowed access); and provide accounting services.

Firewalls provide point of entry control. A firewall lets “valid” traffic pass while discarding “invalid” traffic. The system administrator defines what valid traffic is and what is not. All external traffic to and from the network passes through the firewall. For the purpose of this white paper, firewalls and security gateways are equivalent.

Combinations of solutions are becoming increasingly popular. For example, a user requesting service may have to encrypt a request and send it to a security gateway using a specific port combination. The security gateway either decrypts the request and forwards it to an AAA server or determines that the rules for traffic forwarding were not met and discards the packet. The AAA server may in turn challenge the user – forcing the user to prove identity before access is granted. Once service is granted, subsequent data traffic may or may not be examined by the security gateway depending on security configurations set by the administrator.

IPSec Gateways

A security gateway is a private network’s gatekeeper. This type of gateway provides security against unauthorized access to information on the inside. It can consist of routers, firewalls, VPN hardware and/or software.

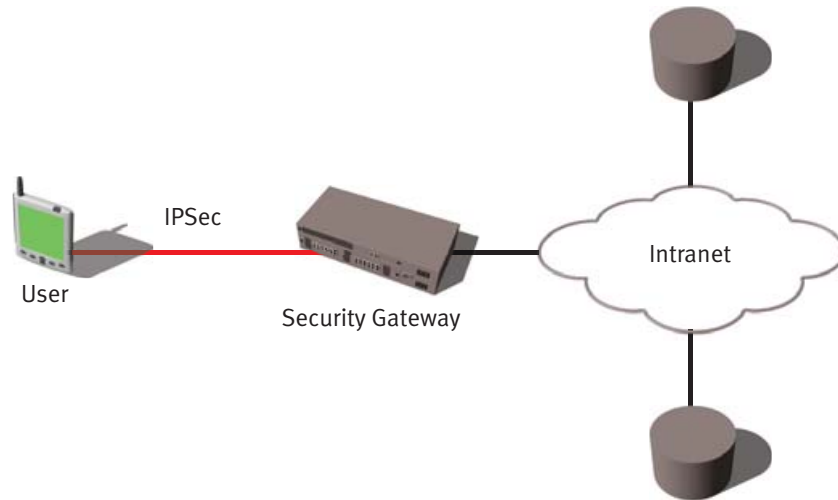


Figure 1: IP Security Gateway

IPSec is a Layer 3 security protocol defined by the IETF that provides authentication and/or encryption of IP traffic across the Internet. IPSec provides the ability to authenticate and/or encrypt data at the packet level. IPSec is built around standardized cryptographic technologies and includes encryption, authentication, usage of keys and management of those keys.

IMS Authentication and Key Agreement (AKA)

IMS is a proliferating technology in the communications industry. The 3G organizations (3GPP and 3GPP2) defined a security solution aimed at mutual authentication that uses IPSec and the Session Initiation Protocol (SIP) protocol.

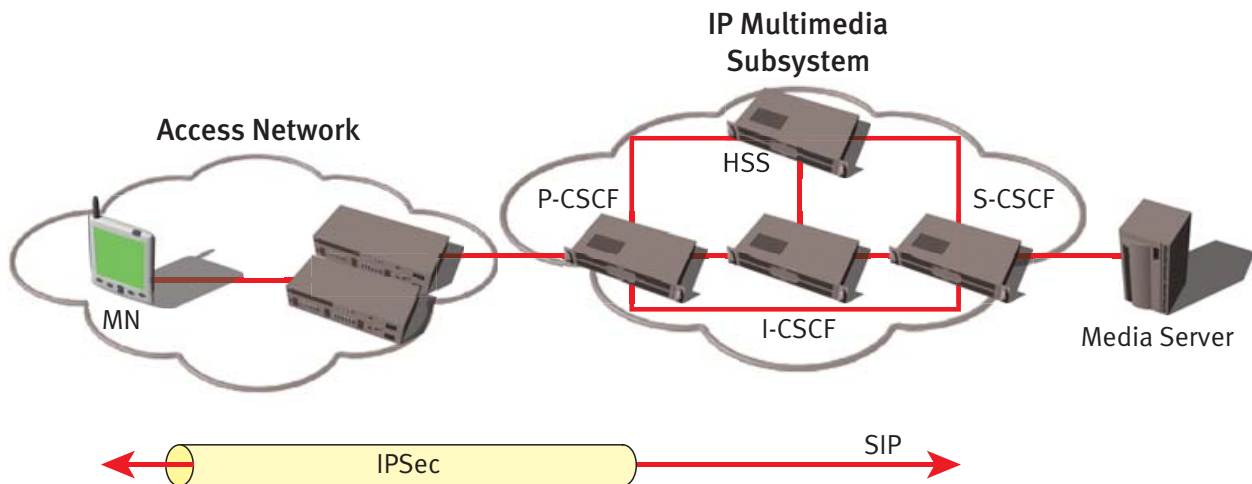


Figure 2: IMS AKA with IPSec

IMS is a separate and distinct system from the access network. Once a mobile Node (MN) obtains network access, it can initiate and participate in IMS activities. The access network and the IMS have interfaces for communicating information about the MN and network resources.

Once connected, the MN can register with the IMS. After registering, it can establish and participate in IMS sessions. The specified protocol for the MN IMS control signaling is SIP (with extensions to support IMS). The bearer for the IMS media flow varies upon the service being provided. The Session Description Protocol (SDP) is used with SIP signaling to identify and possibly negotiate the bearer resources.

The initial SIP messaging (Register and associated response) is carried in the clear (i.e. not encrypted). The response to the first Register message contains a challenge for the user and key information for the Proxy-CSCF. The P-CSCF removes the key information before forwarding the response to the user. The user calculates a response to the challenge and uses this calculated information to encrypt all future SIP control messages. The user sends a new register request encrypted, including the challenge response.¹ The P-CSCF uses the key information to decrypt the message and forward it in the clear toward the Serving-CSCF. The S-CSCF examines the response to authenticate the user. In the downstream direction, the P-CSCF uses the keys to encrypt the SIP messages before forwarding them to the user.

L2TP

Layer Two Tunneling Protocol (L2TP) can be used to tunnel PPP packets between two L2TP peers, in this case an L2TP Access Concentrator (LAC) and a L2TP Network Server (LNS), across the Internet or other IP network.

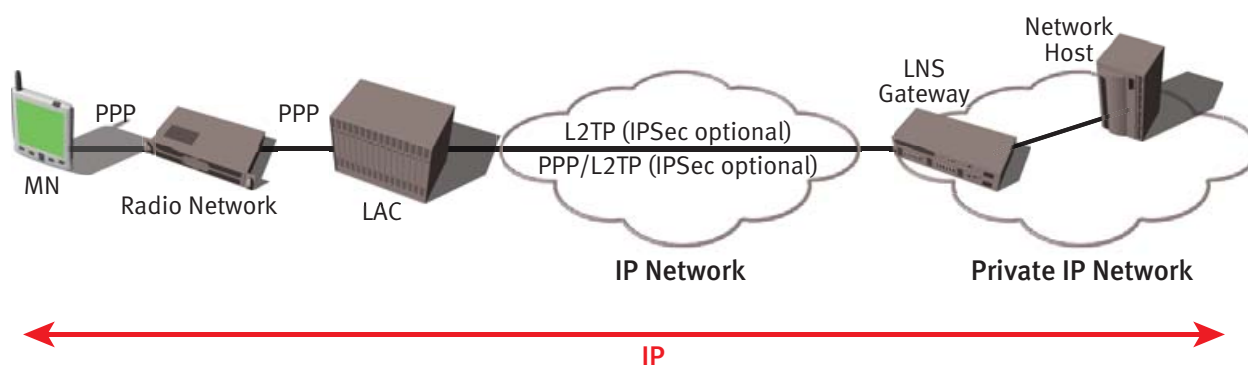


Figure 3: L2TP/LNS Gateway

¹ There may be IPSec tunnels between the P-CSCF and S-CSCF, especially if the S-CSCF is in a different realm than the P-CSCF.

The LAC and the LNS exchange messages to negotiate an L2TP tunnel and establish individual MN PPP sessions within the tunnel, resulting in PPP connectivity between the MN and the LNS. IPSec may be used to encrypt L2TP control plane traffic between the LAC and the LNS. IPSec may also be used to encrypt the bearer plane traffic between the MN and the LNS or another IPSec peer on the private network side of the LNS. A two-way CHAP challenge-response may be used to authenticate the L2TP peers during tunnel establishment. The LNS may authenticate an MN using an external device such as an AAA server.

AAA

Network Access Server (NAS) and AAA servers exchange messages necessary to negotiate mobile user connection requests, authenticate the mobile user, assign an IP address to the mobile user, determine the service that will be supplied to the mobile user and maintain accounting information. A general AAA access model is shown in the diagram below.

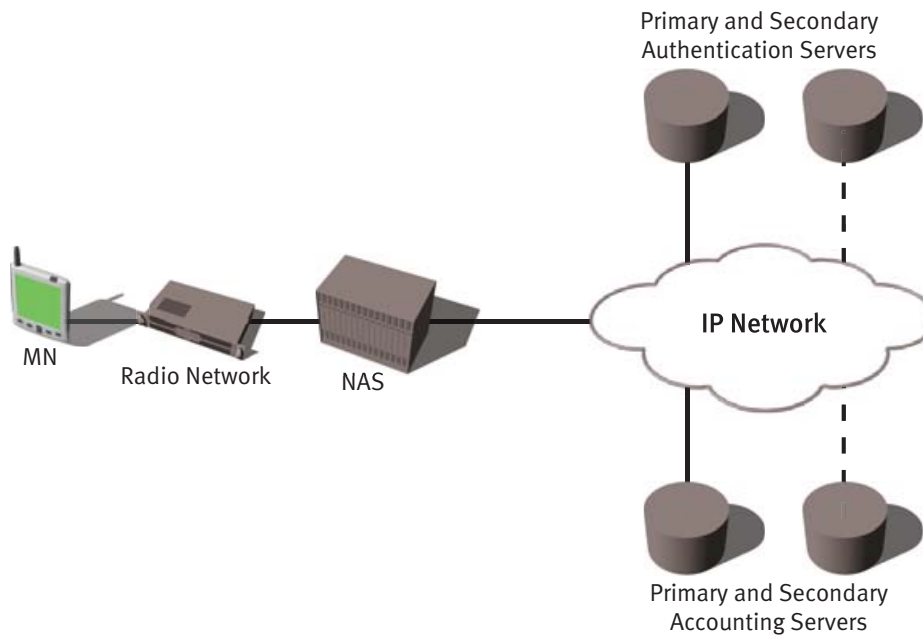


Figure 4: AAA Model

The Radius protocol was originally developed as the AAA protocol of choice but recently the Diameter protocol has become increasingly popular. For user authentication, a variety of authentication methods are supported. These may include but are not necessarily limited to:

- PAP
- CHAP
- MD5 (EAP)
- EAP-SIM
- EAP-AKA
- EAP-TLS
- EAP-TTLS

Test Considerations

With so many different security solutions and options available, a complex test bed is required to thoroughly test an operator's security implementation. The focus of testing extends beyond simple connectivity; the service provider needs to verify, measure and quantify performance of the security devices as well as the impact of those devices on the core data packet elements.

Tests for capacity capability, connectivity rates, stability and data throughput are important and should be available in the test system. Security (IPSec) support in a multitude of traffic models, scenarios, combinations and configurations is required. Lastly, it is essential to test network elements, including security gateways, by themselves (standalone) as well as the entire network (end-to-end).

To benchmark the performance of a node or network, it is imperative that a comprehensive set of data be captured in the test system and be made available to the user. A wide range of measurements including, but not limited to, the following is crucial:

- attempted connect/disconnect rate
- actual connect/disconnect rate
- average control traffic latency
- number of successful connect/disconnect attempts
- number of failed connect/disconnect attempts
- error codes when failures encountered

- average time to connect/disconnect sessions
- various IPSec measurements (when IPSec is enabled)
- a multitude of data throughput measurements when data is used.

The reports must be available in real time so the user can determine the maximum number of simultaneous subscribers that can be attached and determine thresholds of the device under test at various loading levels (e.g. measure latency with various numbers of subscribers attached and with various activation rates). When network failures occur, the test system must provide indications, both in reports generated and log files, to assist with problem identification and resolution. Ideally, measurements should be available on a per-connection (or range of connections) basis to further characterize performance or isolate issues.

IPSec Gateways

The Landslide 2700 Dynamic IPSec Option provides the ability to perform lab tests for performance and accuracy of IPSec transactions.

The Dynamic IPSec Option can be used with any of Landslide's wireless packet data test applications, including Landslide UMTS, Landslide GPRS, Landslide CDMA, Landslide Mobility, Landslide Data, Landslide LNS, Landslide AAA Diameter and Landslide DCCA. IPSec tunnels are established when the emulated mobile node sessions are activated, and they are torn down as the emulated mobile node sessions are deactivated.

Key Capabilities

- IKE Versions
 - IKEv1 (main and aggressive)
 - IKEv2
- Authentication options
 - IKE with pre-shared key
 - IKE with RSA
 - Pre-provisioned
- Authentication types
 - HMAC96-MD5
 - HMAC96-SHA1

- Encryption key types
 - 3DES
 - AES128
- RSA keys supported
 - Private RSA
 - Public RSA
 - 509 certificate
- EAP Authentication
 - EAP-MD5
 - EAP-SIM
 - EAP-AKA
 - EAP-TLS
 - EAP-TTLS

Performance

- Phase 2 tunnels
 - Up to 4 per mobile node
- Security associations per second
 - Pre-shared key = 200
 - RSA = 150 (Assumes 768-bit keys)
- Maximum tunnels
 - 200,000 without per session certificates
 - 100,000 with per session certificates

Landslide generates a full set of reports including IPSec tunnel establishment measurements and data measurements from both the mobile node and network host perspectives. Among the data measurements available in Landslide are number of packets and bytes sent and received, the number of packets per second, the number of bits per second, latency (one way and round trip), and error indicators. The user will be able to determine the performance, thresholds, and data throughput of the IPSec gateway at various loading levels and under different traffic models. When used in combination with other Landslide applications such as CDMA or GPRS, the user will be able to determine performance of the gateway and the entire network architecture

IMS AKA

The IP Multimedia Subsystem (IMS) allows service providers to securely deliver IP multimedia services to their subscribers while maintaining full control over access to those services. The Landslide IMS Security Testing feature, in conjunction with the Advanced Data and Dynamic IPsec features, provides the necessary functionality to test network elements responsible for controlling access to the IMS.

The Landslide IMS Security Testing feature can be used with any data-capable test case. When used with a CDMA2000, GPRS, or UMTS test case, for example, you can test access network elements and IMS network elements. When the security testing feature is used with the IP Application Node test case, you can isolate IMS network elements such as the P-CSCF.

In an end-to-end configuration, Landslide emulates the MNs. The MNs generate SIP traffic towards the IMS. The traffic traverses the IMS network elements with the Landslide MNs accepting and processing the associated responses.

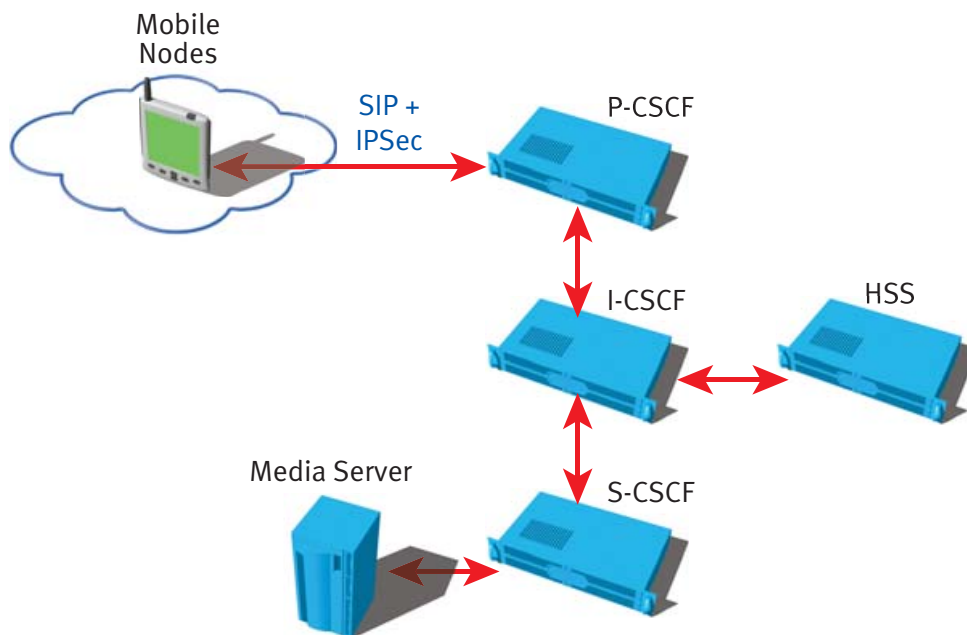


Figure 5: IMS AKA End to End

In a nodal configuration, the P-CSCF is isolated for testing. The Landslide emulates the MNs, S-CSCF and the Media Server.

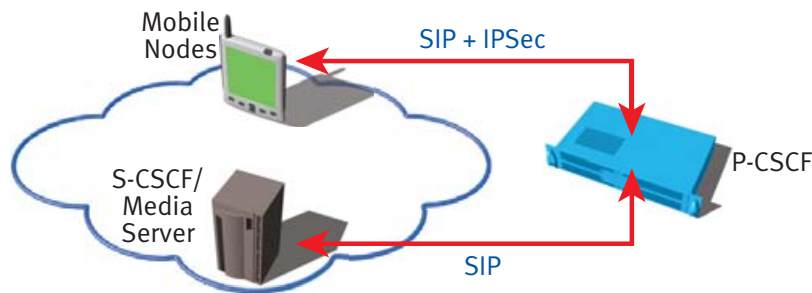


Figure 6: IMS AKA P-CSCF Nodal

For an MN to successfully register with an IMS, it must be able to participate in IMS AKA and dynamically respond to authentication challenges as well as establish an IPsec SA with the P-CSCF. Landslide Data Message Flow and Message Editor windows enable the user to quickly and easily construct a SIP DMF that can correctly respond, on both the client and server sides, during the registration process. Additional flexibility allows the user to define the MNs' private key, digest URI and nonce information. Landslide Message Flow Controls can trigger the calculation of a challenge response and the initiation of an IPsec connection. Lastly, the user has the ability to capture and insert dynamic information specific to IMS as well as IP address and port information.

L2TP

The Landslide L2TP VPN Gateway test application provides comprehensive L2TP Network Server testing in a 3G environment using the L2TP protocol. With this application, the Landslide emulates L2TP LACs to measure the performance of an LNS Gateway.

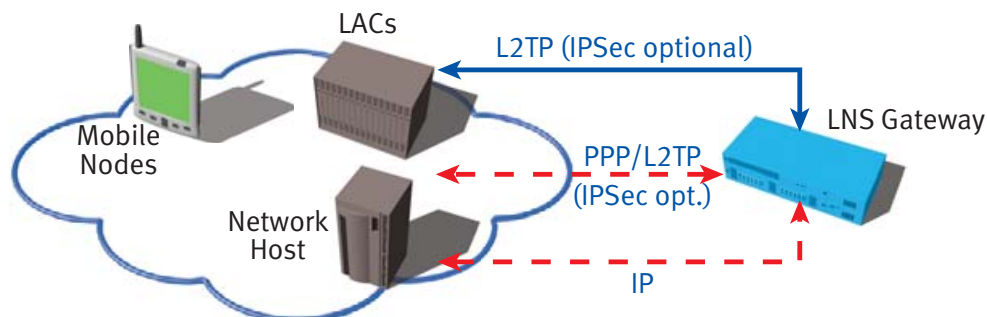


Figure 7: LNS Gateway Testing

This application provides the ability to test an L2TP Network Server (LNS) using the L2TP, IPsec and PPP protocols. The test system emulates one or more L2TP Access Concentrators (LAC) establishing L2TP tunnels and sessions with the LNS while listening for and responding to L2TP control messages from the LNS.

Measurements collected for these test cases include:

- Counters that record the number and types of messages sent and received
- Average response times for the different types of messages received from an SUT
- Errors encountered during the test
- Session state and rates
- Tunnel state and rates

An optional virtual LNS feature supports test operations driven by another test system or tool. You can use the virtual LNS to support L2TP testing that is driven by test devices external to this test system. The virtual server includes Network Host functionality and supports both control and bearer plane testing as shown in the diagram below. It will respond to any LAC that presents valid credentials. The L2TP Secure Network Server feature provides a virtual server with IPsec support.

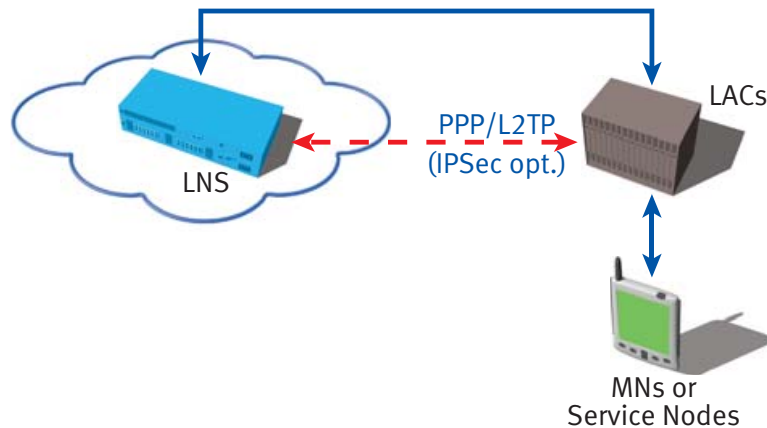


Figure 8: LNS Server Emulation

AAA

The Landslide AAA test applications provide comprehensive Authentication, Authorization, and Accounting (AAA) testing in a 3G environment using either the Radius or Diameter protocol. The Landslide AAA applications enable you to test both an AAA server and a NAS. The AAA server test case tests an AAA server by generating traffic from an emulated NAS towards the AAA server, and listening for and interpreting the responses.

With the Landslide AAA Server emulator, you can include an emulated AAA server in a test session with a test case from another application (such as GPRS) in order to test a NAS SUT. The AAA emulator provides authentication services for the NAS, including optional IP address allocation, and responds to accounting messages sent from the NAS.

The Landslide AAA applications give you total control over the optional Radius, Diameter, vendor-specific, and application-specific attributes included in the various messages. In addition to the attributes defined on the tabs of a test case, you can configure and explicitly define the optional attributes required by your SUT.

Whenever a test includes Radius or IPSec with IKEv2, you can optionally use the Extensible Authentication Protocol (EAP) to authenticate the MN with an AAA server. EAP provides a framework that supports many authentication methods over various transport protocols between the NAS and the MN. The NAS performs a screening function, validating the message composition of responses from the MN and forwarding the MN's credentials on to an AAA server for final authentication and authorization. EAP messages can be carried in the payload of Radius messages. Since EAP devices can support different authentication methods, a negotiation mechanism enables the MN and the AAA server to agree upon the authentication method to be used when the two devices support at least one common method.

The following authentication methods are supported by the test system:

- MD5
- EAP-SIM
- EAP-AKA
- EAP-TLS
- EAP-TTLS

A comprehensive set of AAA measurements is provided by the Landslide. Depending on protocol (Radius or Diameter), the set of measurements includes counts for the number of messages sent and received, authentication requests sent, responses received, average response times to various requests and a list of error indications received. When EAP is used, an additional set of measurements is available including counts of general EAP messages exchanged for full and fast authentication processes, and measurements for the specific authentication method selected: MD5, EAP-SIM, EAP-AKA and EAP-TLS.

DoS

Denial of service attacks are a real threat in today's networks. Malicious users can execute coordinated attacks from vulnerable points in the networks to cause a loss of services due to bandwidth over-consumption. Hackers can overload network resources or completely crash a network element. The Landslide Distributed Denial of Service (DDoS) Test Suite performs lab tests that simulate these attacks for testing the ability of a network or a network element to combat these attacks.

The DDoS Test Suite can be used with many of Spirent's wireless packet data test applications, including Landslide UMTS, Landslide GPRS, Landslide CDMA, Landslide Mobility and Landslide IP Data. With the Landslide's Advanced Data Option, the user has access to a comprehensive suite of DDOS attack messages that can be used to test the security and vulnerability of your network or network equipment.

Other DDOS attacks are specific to particular access networks. Landslide is equipped to support these attacks as well. In addition to the DDOS attacks generated using the Advanced Data Option, the DDOS Test Suite also provides access-specific DDOS attack tests. For a GPRS/UMTS network, the Landslide can generate a high volume of non-authentic PDP context messages (create, update, delete) to flood a network with invalid/erroneous control messages. Similar types of tests are available for all of the Landslide applications.

The DDOS Test Suite contains a spate of DDOS attack messages. Here is a sample of the types of DDOS attacks available:

- ICMP Message Flooding
- PING of Death
- Erroneously checksummed messages
- MN spoofing
- MN attacks
- IP flooding
- DNS attacks
- DHCP attacks
- Unauthorized access
- Control Message Flooding
- Malformed packets
- Fragmented packets
- SYN Flooding
- Invalid HTTP requests

Each Landslide 2700 test server can generate tens of thousands DDOS packets per second, ensuring a thorough test of your network prior to or after "going live."

Acronyms

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
CSCF	Call Session Control Function
DoS	Denial of Service
GGSN	Gateway GPRS Support Node
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IPSec	IP Security
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Controller
LNS	L2TP Network Server
MN	Mobile Node
NAS	Network Access Server
P-CSCF	Proxy-CSCF
PDN	Packet Data Network
PPP	Point to Point Protocol
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module (GSM)
SUT	System Under Test
VPN	Virtual Private Network



Inspired Innovation