

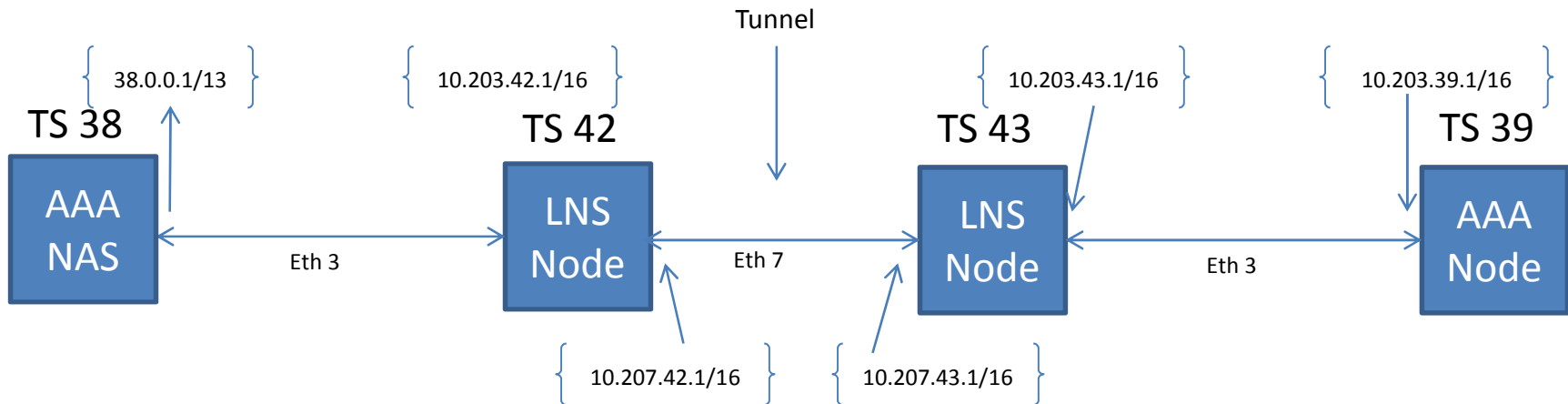
Landslide L2TP/IPsec

Spirent Global Services



PROPRIETARY AND CONFIDENTIAL

Landslide L2TP IPsec



| Test Server | SUT (System Under Test) | Physical | Ethernet Port |
|-------------|--|--|---------------|
| TS 38: | Accounting (10.203.39.1) Authentication (10.203.39.1) | 38.0.0.1 (Next-hop 10.203.42.1) | Eth3 |
| TS 42: | 10.207.43.1 | 10.207.42.1 Remote Network Host = 10.203.39.1 | Eth 7 |
| TS 43: | 10.207.42.1 | 10.207.43.1 IP Address Pool (38.0.0.1) | Eth 7 |
| TS 39 | NA | 10.203.39.1 (Next-hop 10.203.43.1) | Eth 3 |

LNS Nodal



LNS Nodal Configuration (Test Configuration)

Test Case - [LNS Nodal] / 0 / ts0:tc0

Name: Extra Phys:

Test Case Diagram

The diagram illustrates the network topology for the test case. It shows a sequence of components: Ext Data (green box) connects to UE (blue box). UE connects to LAC (blue box). LAC connects to LNS (green box). LNS connects to a protocol stack (blue box) containing PPP, L2TP, IPsec, L1-2, L2TP, L3-7, LL, PL, and IP. The IP layer connects to a Sec GW (grey box) and a Ntwk Host (green box). The LAC, LNS, and the protocol stack are grouped within a larger orange box.

Test Case Settings

Test Configuration | Network Devices | L2TP | L3-7

Test Options

Test Activity: Capacity Test

Data Traffic External Data

Data IPsec L2TP IPsec

Mobile Subscribers

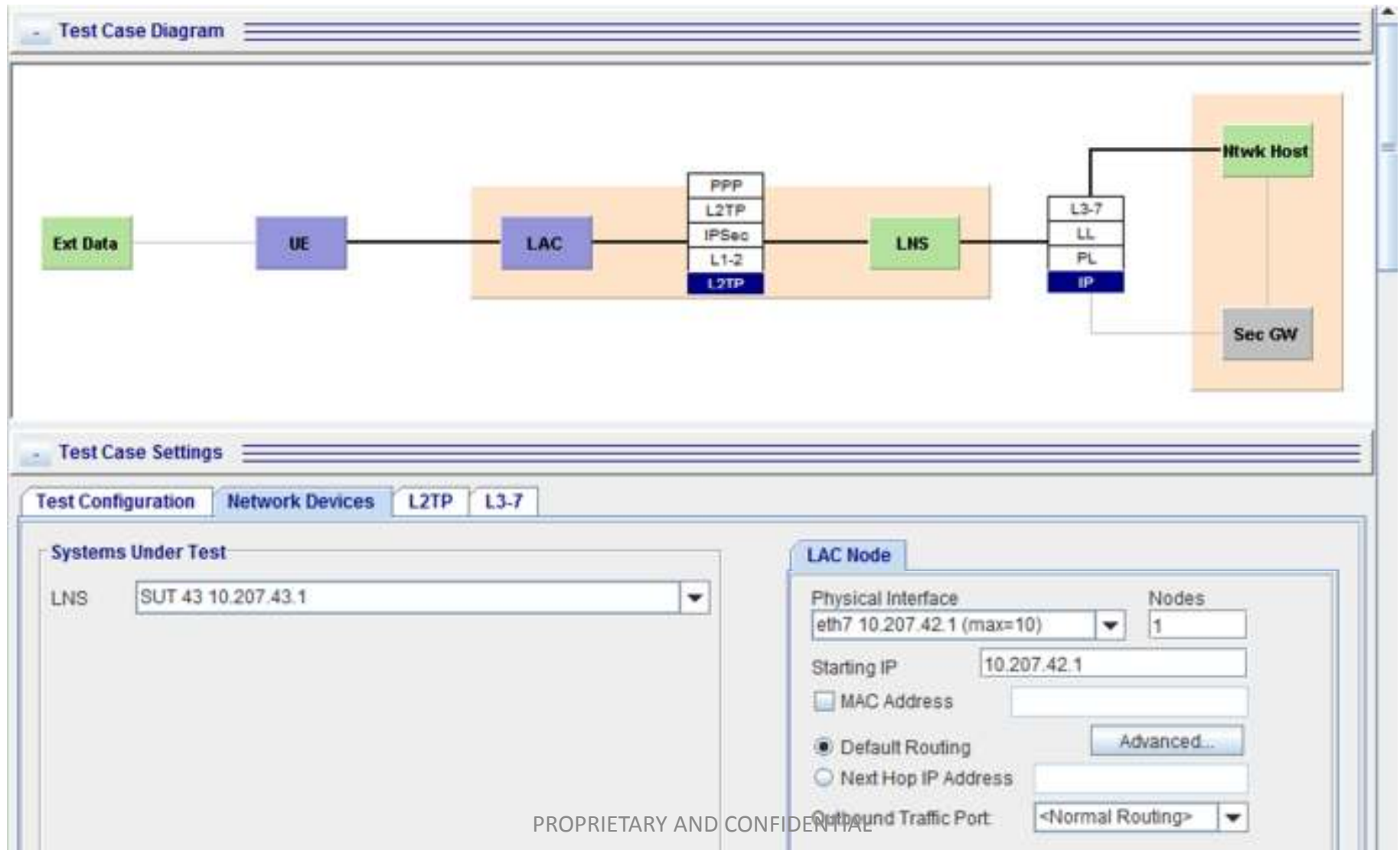
Number of Subscribers:

Activation Rate (sessions/sec):

Deactivation Rate (sessions/sec):

PROPRIETARY AND CONFIDENTIAL

LNS Nodal Configuration (Network Devices)



LNS Nodal Configuration (L2TP: L2TP IPsec)

Test Case Settings

Test Configuration Network Devices L2TP L3-7

PPP
L2TP
L2TP IPsec

IKE: IKE With Pre-Shared Keys

IKE Settings - Pre-Shared Key

| | | | |
|---|-------------------------------|--|------------------------------|
| IKE Version | V1 | IKE Phase 1 Type | Aggressive |
| Authentication Type | HMAC96-MD5 | Pre-Shared Key | 0 |
| Hash Type | HMAC-MD5 | <input type="checkbox"/> EAP Authorization | EAP Settings... |
| Encryption Key Type | 3DES | Identification Type | Local IP Address |
| Oakley Group Type | Group 768 | Distinguished Name | CN=MN#, DC=HomeAgent, DC=net |
| <input type="checkbox"/> Disable IKE Message Encryption | | Host/User Name | MN# |
| Retry interval (s) | 30 | Domain Name | HomeAgent.net |
| SA Lifetime Type | seconds | <input type="checkbox"/> Include Peer ID | Fully Qualified Domain Names |
| SA Lifetime | 28800 | Peer Host Name | PeerAgent |
| Initial Contact Notification | Following Phase 1 Negotiation | Peer Domain Name | spirent.net |
| <input type="checkbox"/> NAT Traversal | | <input type="checkbox"/> Extended Authentication (Xauth) | |
| Keepalive Interval (s) | 240 | Xauth User Name | |
| NAT Source Port | 4500 | Xauth Password | |

LNS Nodal Configuration (L3 – L7: Data Traffic)

The screenshot shows the 'Test Case - [LNS Nodal]/ 0 / ts0:tc0' window. The 'Test Case Settings' section is expanded to show 'Test Configuration', 'Network Devices', 'L2TP', and 'L3-7'. The 'Data Traffic' tab is selected, showing 'Network Host' and 'Client' settings.

Network Host

Host Type: Local Remote

| Index | IP |
|-------|-------------|
| 0 | 10.203.39.1 |

Buttons: Add, Delete

Reset Idle Host Traffic Session
Idle Time to Trigger Reset (s): 0.0

Client

Traffic Type: Continuous Perform Verification
Traffic Start: When All Sessions Established
Data Start Delay (ms): 1000 Auto Stop Control Layer
 Limit Ingress Link Speed (Kb/s): 16
 Limit Egress Link Speed (Kb/s): 16
Maximum Transmission Unit: 1400 Do Not Fragment
Error Injection...
 Apply Test Data File to User Side
Select

LNS Node



LNS Node Configuration (Emulator Configuration)

Test Case - [LNS Node] / 0 / ts1:tc0

Name: Extra Phys:

Test Case Diagram

```
graph LR; UE[UE] --- LAC[LAC]; subgraph LNS_Box [LNS]; direction TB; LNS_Protocol[PPP, L2TP, IPsec, L1-2, L2TP]; LNS[ ]; end; LAC --- LNS_Box; LNS_Box --- NtwkHost[Ntwk Host]; LNS_Box --- SecGW[Sec GW];
```

Test Case Settings

Emulator Configuration | Network Devices | L2TP

Emulator Options

- Data Traffic
- Data IPsec
- L2TP IPsec

Mobile Subscribers

| | |
|----------------------------------|---------------------------------------|
| Number of Subscribers | <input type="text" value="1"/> |
| Activation Rate (sessions/sec) | <input type="text" value="1.0"/> |
| Deactivation Rate (sessions/sec) | <input type="text" value="1.0"/> |
| IP Address Pool | <input type="text" value="38.0.0.1"/> |

PROPRIETARY AND CONFIDENTIAL

LNS Node Configuration (Network Devices)

The screenshot displays a network configuration interface for a test case titled "Test Case - [LNS Node] 0 / ts1:tc0". The interface is divided into several sections:

- Test Case Diagram:** A network diagram showing a UE (User Equipment) connected to a LAC (Local Access Client). The LAC is connected to an LNS (Local Network Server) node. The LNS node is associated with protocols: PPP, L2TP, IPsec, L1-2, and L2TP. The LNS is connected to a Sec GW (Secondary Gateway), which is further connected to a Ntwk Host (Network Host).
- Test Case Settings:** This section contains two main tabs: "Emulator Configuration" and "Network Devices". The "Network Devices" tab is active, showing the "L2TP" configuration for the "LNS Node".
- Systems Under Test:** A list of systems under test, including "LAC" with a SUT (System Under Test) value of "SUT 42 10.207.42.1".
- LNS Node Configuration:** This section is expanded to show the configuration for the "LNS Node". It includes:
 - Physical Interface:** eth7 10.207.43.1 (max=10)
 - Starting IP:** 10.207.43.1
 - MAC Address:** (checkbox unchecked)
 - Default Routing:** (radio selected)
 - Next Hop IP Address:** (radio unselected)
 - Outbound Traffic Port:** <Normal Routing>

PROPRIETARY AND CONFIDENTIAL

LNS Node Configuration (L2TP: L2TP IPsec)

Test Case Settings

Emulator Configuration | Network Devices | **L2TP**

PPP
L2TP
L2TP IPsec

IKE IKE With Pre-Shared Keys

IKE Settings - Pre-Shared Key

| | | | |
|---|-------------------------------|--|------------------------------|
| IKE Version | V1 | IKE Phase 1 Type | Aggressive |
| Authentication Type | HMAC96-MD5 | Pre-Shared Key | 0 |
| Hash Type | HMAC-MD5 | <input type="checkbox"/> EAP Authorization | EAP Settings... |
| Encryption Key Type | 3DES | Identification Type | Local IP Address |
| Oakley Group Type | Group 768 | Distinguished Name | CN=MN#, DC=HomeAgent, DC=net |
| <input type="checkbox"/> Disable IKE Message Encryption | | Host/User Name | MN# |
| Retry Interval (s) | 30 | Domain Name | HomeAgent.net |
| SA Lifetime Type | seconds | <input type="checkbox"/> Extended Authentication (Xauth) | |
| SA Lifetime | 28800 | Xauth User Name | |
| Initial Contact Notification | Following Phase 1 Negotiation | Xauth Password | |
| <input type="checkbox"/> NAT Traversal | | <input type="checkbox"/> Inspect Rekey Packets | |
| Keepalive Interval (s) | 240 | | |
| NAT Source Port | 4500 | | |
| NAT Destination Port | 4500 | | |

PROPRIETARY AND CONFIDENTIAL

Appendix – AAA Node/Nodal Configuration

AAA NAS



AAA NAS (Test Configuration)

r Nodalj/ 0 / ts1:tc0

Extra

The diagram illustrates the AAA NAS configuration. A central AAA server is connected to AN NAS and NAS. The AAA server is configured with RADIUS (UDP, IP) and DIA (TCP, IP, IPsec). It is connected to Au AAA and Ac AAA servers, which are in turn connected to mobile subscribers.

| | |
|--------|-------|
| RADIUS | DIA |
| UDP | TCP |
| IP | IP |
| | IPSec |
| AAA | |

Test Case Settings

Test Configuration Network Devices AAA

Test Options

Test Activity: Capacity Test [Settings...]

AAA Protocol: RADIUS Diameter

Alternate Node Authentication Diameter IPsec

Mobile Subscribers

Number of Subscribers: 1

Activation Rate (sessions/sec): 1.0

Deactivation Rate (sessions/sec): 1.0

PROPRIETARY AND CONFIDENTIAL

AAA NAS (Network Devices)

Set the name of this instance

| | |
|--------|-----|
| RADIUS | DIA |
| UDP | TCP |
| IP | IP |
| IPsec | |
| AAA | |

Test Case Settings

Test Configuration Network Devices AAA

Systems Under Test

AAA SUT Distribution Mode Dedicated Round Robin

Authentication Secondary Auth Accounting Secondary Acct

SUT TS39 10.203.39.1

NAS Node Alternate NAS Node Target NAS Node

Physical Interface lo 38.0.0.1 (max=400001) # of Nodes 1

Starting IP 38.0.0.1

MAC Address

Default Routing

Next Hop IP Address 10.203.42.1

Advanced...

PROPRIETARY AND CONFIDENTIAL

AAA Node



AAA Node (Emulator Configuration)

The diagram illustrates the AAA Node configuration. It shows a central AAA node (blue box) with a table of protocols and their transport methods. The protocols are RADIUS, DIA, UDP, TCP, IP, and IPsec. The transport methods are UDP, TCP, IP, and IPsec. The AAA node is connected to HAS (green box), HA (grey box), and AAA (blue circle). The connections are as follows: HAS is connected to the central AAA node; HA is connected to the central AAA node; and the central AAA node is connected to the AAA node.

| | |
|--------|-------|
| RADIUS | DIA |
| UDP | TCP |
| IP | IP |
| | IPsec |
| AAA | |

Test Case Settings

Emulator Configuration | Network Devices | AAA

Emulator Options

AAA Protocol RADIUS Diameter

IP Address Allocation

Address Pool Selection Method:

CoA Simulation Disconnect Simulation

Diameter IPsec

Mobile Subscribers

Number of Authentication Sessions:

Number of Accounting Sessions:

Deactivation Rate (sessions/sec):

PROPRIETARY AND CONFIDENTIAL

AAA Node (Network Devices)

Test Case Diagram

The diagram shows a network topology within an orange box. On the left is a green box labeled 'HAS'. In the center is a blue box labeled 'AAA' with a table of protocols: RADIUS, DIA, UDP, TCP, IP, IP, and IPsec. On the right is a purple circle labeled 'AAA'. A grey box labeled 'HA' is at the top. Lines connect HAS to the central AAA node, the central AAA node to the right AAA node, and HA to both HAS and the right AAA node.

Test Case Settings

Emulator Configuration | Network Devices | AAA

Systems Under Test

NAS: < Choose a SUT >

Port: 3799

HSS: < Choose a SUT >

Host: HSSServer.Sprint.com

Realm: Sprint.com

AAA Server Node | HA Node

Physical Interface: eth3 10.203.39.1 (max=201)

IP Address: 10.203.39.1

MAC Address

Default Routing

Next Hop IP Address: 10.203.43.1

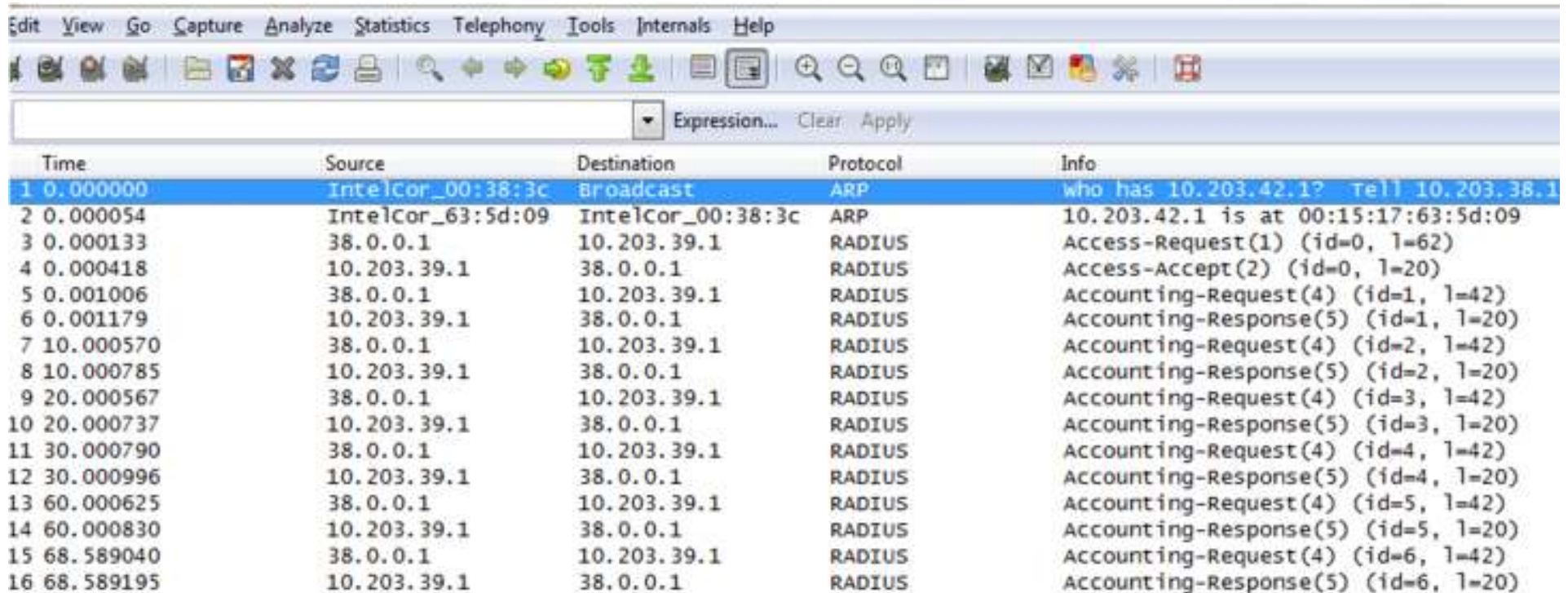
Advanced...

PROPRIETARY AND CONFIDENTIAL

Wireshark Traces

PROPRIETARY AND CONFIDENTIAL

Eth3 Interface (Radius): TS 38 – TS 42



The image shows a Wireshark network traffic capture window. The menu bar includes Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, navigation, and analysis. Below the toolbar is a filter expression field with a dropdown arrow, the text "Expression...", and buttons for "Clear" and "Apply". The main display area shows a list of captured packets with the following columns: Time, Source, Destination, Protocol, and Info.

| Time | Source | Destination | Protocol | Info |
|--------------|-------------------|-------------------|----------|---------------------------------------|
| 1 0.000000 | IntelCor_00:38:3c | Broadcast | ARP | who has 10.203.42.1? Tell 10.203.38.1 |
| 2 0.000054 | IntelCor_63:5d:09 | IntelCor_00:38:3c | ARP | 10.203.42.1 is at 00:15:17:63:5d:09 |
| 3 0.000133 | 38.0.0.1 | 10.203.39.1 | RADIUS | Access-Request(1) (id=0, l=62) |
| 4 0.000418 | 10.203.39.1 | 38.0.0.1 | RADIUS | Access-Accept(2) (id=0, l=20) |
| 5 0.001006 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=1, l=42) |
| 6 0.001179 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=1, l=20) |
| 7 10.000570 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=2, l=42) |
| 8 10.000785 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=2, l=20) |
| 9 20.000567 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=3, l=42) |
| 10 20.000737 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=3, l=20) |
| 11 30.000790 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=4, l=42) |
| 12 30.000996 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=4, l=20) |
| 13 60.000625 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=5, l=42) |
| 14 60.000830 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=5, l=20) |
| 15 68.589040 | 38.0.0.1 | 10.203.39.1 | RADIUS | Accounting-Request(4) (id=6, l=42) |
| 16 68.589195 | 10.203.39.1 | 38.0.0.1 | RADIUS | Accounting-Response(5) (id=6, l=20) |

Eth7 Interface (L2TP IPsec): TS 42 – TS 43

09_05.12.22.AM_TS-TS43_eth7_capture[1].pcap

Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Go forward in packet history

Expression... Clear Apply

| Time | Source | Destination | Protocol | Info |
|-------------|-------------------|-------------------|----------|---------------------------------------|
| 1 0.000000 | IntelCor_55:07:38 | Broadcast | ARP | who has 10.207.43.1? Tell 10.207.42.1 |
| 2 0.000019 | IntelCor_55:07:50 | IntelCor_55:07:38 | ARP | 10.207.43.1 is at 00:15:17:55:07:50 |
| 3 0.000081 | 10.207.42.1 | 10.207.43.1 | ISAKMP | Aggressive |
| 4 0.001401 | 10.207.43.1 | 10.207.42.1 | ISAKMP | Aggressive |
| 5 0.002120 | 10.207.42.1 | 10.207.43.1 | ISAKMP | Aggressive |
| 6 0.002122 | 10.207.42.1 | 10.207.43.1 | ISAKMP | Informational |
| 7 0.002773 | 10.207.42.1 | 10.207.43.1 | ISAKMP | Quick Mode |
| 8 0.004097 | 10.207.43.1 | 10.207.42.1 | ISAKMP | Quick Mode |
| 9 0.004833 | 10.207.42.1 | 10.207.43.1 | ISAKMP | Quick Mode |
| 10 0.004866 | 10.207.42.1 | 10.207.43.1 | ESP | ESP (SPI=0x00000000) |
| 11 0.004935 | 10.207.43.1 | 10.207.42.1 | ESP | ESP (SPI=0x00000000) |
| 12 0.005125 | 10.207.42.1 | 10.207.43.1 | ESP | ESP (SPI=0x00000000) |
| 13 0.005247 | 10.207.43.1 | 10.207.42.1 | ESP | ESP (SPI=0x00000000) |
| 14 1.004338 | 10.207.42.1 | 10.207.43.1 | ESP | ESP (SPI=0x00000000) |
| 15 1.004392 | 10.207.43.1 | 10.207.42.1 | ESP | ESP (SPI=0x00000000) |
| 16 1.004485 | 10.207.42.1 | 10.207.43.1 | ESP | ESP (SPI=0x00000000) |
| 17 1.004487 | 10.207.42.1 | 10.207.43.1 | ESP | ESP (SPI=0x00000000) |
| 18 1.004552 | 10.207.43.1 | 10.207.42.1 | ESP | ESP (SPI=0x00000000) |
| 19 1.004568 | 10.207.43.1 | 10.207.42.1 | ESP | ESP (SPI=0x00000000) |

Landslide L2TP/IPsec

Spirent Global Services



PROPRIETARY AND CONFIDENTIAL