

## 軟體式可視化系統

### Software Based Network Visibility System

Zenya's Software Based Network Visibility System optimizes cyber security and performance monitoring applications by delivering the required data in the right volume and the correct format. Cyber and monitoring tools are required to handle incoming traffic from multiple visibility devices including TAPs, SPAN ports and NPB (Network Packet Broker) appliances. The volume and diversity in the types of traffic can be overwhelming to these tools. Duplicated packets may cause applications to be stretched to the limits of their processing power whereas packets with multiple headers (e.g. MPLS, VLAN tags, ERSPAN etc.) are often unrecognized by these tools and are typically dropped. The Software Packet Broker supports ports on the PC of 1/10/25/40/100Gb, plus additional configurable monitoring/Tap ports. This flexibility lets you configure the system with multi-purpose bypass segments, or with I/O packet broker ports, or any combination of bypass segments and packet broker ports.

#### Main Features:

Mapping traffic flow relationships between source and destination ports:

- Aggregate traffic to single port
- Replicate **same** traffic to multiple ports
- Sophisticated filtering - L2-L4, User Defined Byte (UDB)
- GRE Tunnelling
- VLAN support for filtering, stripping and modifying
- User configurable packet heartbeat (ns resolution)
- Ingress and egress filters
- AND/OR/NOT Operators
- Inner Tunnel Filtering

#### Advanced Features:

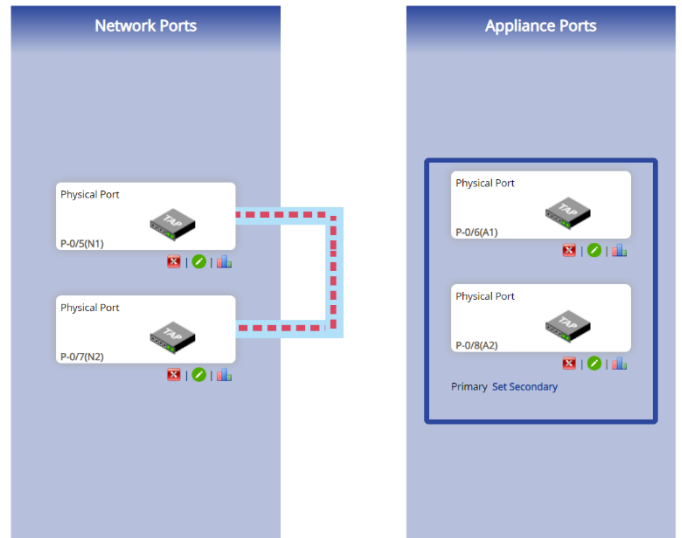
- User defined virtual bypass segments
- Layer-7 Filtering (Perform DPI and identify thousands of layer 7 protocols)
- Regex Filtering (Identify and filter traffic that includes specific strings)
- Session Tracking (Track the entire session once the desired pattern has been identified)
- Weighted Load Balancing (Distribute traffic across multiple tools and prevent over-subscription)
- Header Stripping (Modify MAC, VLAN and IP header)
- Header Editing (Modify MAC, VLAN and IP headers)
- Deduplication, Data Masking, Packet Slicing
- Time Stamping

Sample Screenshot:

```

root@zenya-System-Product-Name: ~
root@zenya-System-Product-Name:~#
root@zenya-System-Product-Name:~# rdiffctl
Usage: rdiffctl <command> [parameters]
  Commands List:
set_cfg - set the device to predefined configuration
get_dev_num - get total number of rdi devices.
get_port_info <port> | if_name |bus:slot.fn> - get port & switch info.
set_sw_remain <val> - enable/disable (1/0) remain switch configuration after rdi
f stop
get_sw_remain
get_cfg - get current configuration mode
get_port_link <port> - get link status
get_port_speed <port> - get port speed
set_port_parser <port> <val> - set parser level (2,3,4)
get_port_parser <port> - get parser level
set_rframe_update <port> <val> - set bitmask indicating the fields
that will be updated on a routed frame
dnac - bit 0, smac - bit 1, vlan - bit 2
get_rframe_update <port> - get routed frame fields that will be updated
set_ttl_update <port> <val> - enable/disable (1/0) decrement TTL field on routed
frames
get_ttl_update <port>
temp_write <addr> <length (1)> <reg>
temp_read <addr> <length>
temp1_write <addr> <length (1)> <reg> - use only for 0x4c address
temp1_read <addr> <length> - use only for 0x4c address
dir - add the rule of a port with direction matching packets to another port
lb - add the rule of a port with send matching packets to load balance group
(LBG)
drop - drop matching packets
permit - permit matching packets
mir - copy matching frame to mirror_port (mirror must be created previously,
see mir_create)
set_prio - set switch priority for the packet
set_vlan vlan_act <vlan_act> - set vlani rule
add_vlan_promisc <port> - add the port to all 2...4095 VLANs
rem_vlan_promisc <port> - remove the port from all 2...4095 VLANs
get_power port <port> - get SFP/QSFP TX/RX power
stat port <port> - get statistic for specific port (port is mandatory)
prio_stat port <port> - get priority statistic for specific port (port is manda
tory)
reset_stat port <port> - reset statistic for specific port (port is mandatory)

```



Edit IPv4 Session List	
IP Session	Direction
192.168.0.0/24	source
192.168.0.0/24	source

Filter filters/2

Filter Attributes

Name: test2

Description: test2

Admin:  Enable  Disable

Action:  Drop  Redirect  Copy

Input-ports: 1

Output-ports: 3

Output-LB-group:

Logical operation:  AND  OR

L2 Filter Parameters

L3 Filter Parameters

Fragments:  None Or First  Not First

DSCP:

IP protocol number:

IPv4 address: 192.168.0.1/32 NOT Source: 172.16.0.0/24

IPv4 session: (No sessions)