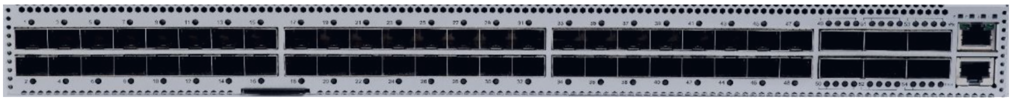
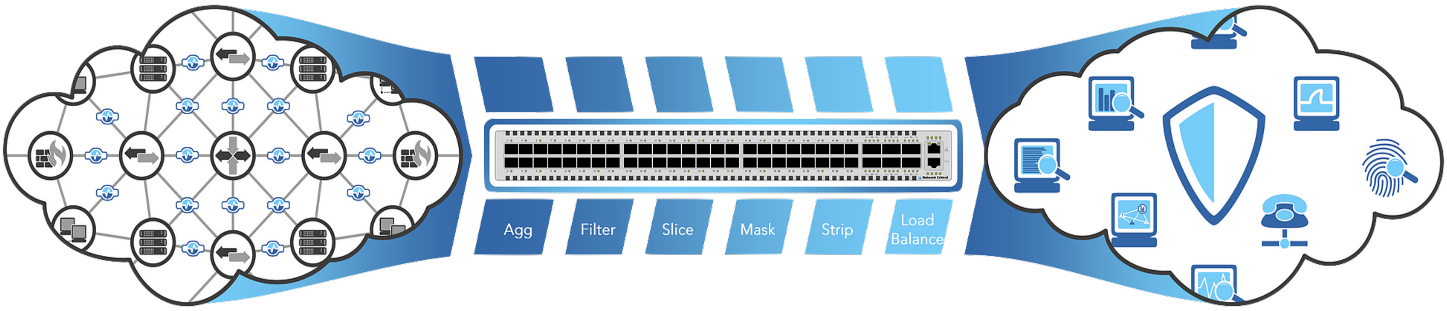


KARINCA

PACKET BROKER

Designing and operating your network is vital to provide the perfect flow to corporate applications. A network that is not designed to meet correct demands of a company and that requires big changes for each new requirement, would eventually cause a failure. This failure point, is usually comes with business shortages and cause service delivery problems, money loss and reputation erosion. Communication and application requirements change almost daily, and mandates your network runs on very high speeds. This is only sustainable, by implementing high performance devices, appropriate monitoring solutions and efficient security measures.
Life is usually not fair, so does IT budgets. Although all requirements are well set, the reality is, IT teams are expected to achieve the perfect environment with limited budgets together with users and customers that has no tolerance to any kind of communication problem.



Visibility

To keep everything visible, we need huge amount of data. Today, on the average only 70% of network is visible. Remaining 30% is the victim of, architectural complexities. To reach close to 100%, more significant high-resolution data collection point needed. But this returns with more complexities. On the other hand, troubleshooting times gets longer and capacity increase needed to evolve the network becomes more costly and painful. Last but not least, legal requirements and rules makes everything tangled.

To escape form this endless loop, we need creative solutions. The beauty of simplicity, not just makes operation simpler, also create easy access and solutions that you don’t need to sacrifice on anything. The result fewer blind spots, and saving from recurring costs and time.

Security

Security vendors creates extraordinary solutions for different needs. Firewalls, intrusion detection and prevention systems, malware detectors, data leakage protectors, APT analyzers etc. are all in the market to protect applications and users. Yet all requires only one thing to run correctly: Receiving right traffic

Packet Brokers are used to provide necessary environment for you to rule and secure your, now, very high-speed network, easier and effectively without any significant architectural changes.

Classification

Based on Angora Data Center packet switching technologies, smart packet classification algorithms combined with extremely easy user interface, we have created a protocol independent traffic distribution platform with very high capacity.
Packet duplication and delivery is the most important basic requirements but the magic is correct delivery. Since delivering every packet cause bottlenecks, and creates new blind spots, it also steals the performance of processing devices. With the help of smart classification and delivery filters, traffic from different ports can be classified independently.

Based on your network layered structure, selected traffic can be transferred to appropriate analysis and monitoring engine. Perfect isolation between ports allows the use of single packet broker to work for different segments of your network. L2/L7 packet analysis features, allows you to control from physical address to anything in the packet payload. This will help you with more detailed controls, and prevents any leaks. Very fast and correct classification clears the blind spots. They are losses caused by packet classification errors and result analysis errors and more importantly security implementation problems. Even a single malicious packet that is not correctly classified, would throw away all your security precautions. Packet Broker controls your traffic 100% and prevents any error on classification and delivery. Most important point is to give the right decision, you need to have the right idea.

Architecture

While distributing the traffic, you can choose sending the traffic from one port to a single port or to multiple ports, so you can both process the traffic and keep a copy on different devices at once.

Load balancing options, allows using multiple low performance devices that are responsible with same tasks. This is a very cost-effective way to protect your time and budget without the need for long-term, unsure investments. For example, you would not need an unnecessarily high capacity security analysis device, to keep your network simple for the future. You only need to buy what you need now, and Packet Broker would help you adding another same function device by simply plugging it another port. You will keep your architecture simple, and also your money, saving against any unpredictable traffic increase.

Hardware

All are possible with very powerful and high capacity ASIC architecture coupled with latest x86 CPUs. End result is a very efficient software running on higher capacities than server based hardware.

Current hardware architecture supports up to 1Tbps traffic distribution on 48x25Gbps and 6x100Gbps ports. With the fabric extender options for data center architecture, up to 192 ports of 25G interface would be available under a single management space, you can meet current requirements today, and simplify your operation without any architectural change in case you need to provision new applications or security measures, resulting easier control on your IT budget and on demand modular expansion.

Packet Broker eliminates any loss while classifying and distributing traffic. Switching rates will be higher than other architecture-based routing options. End solution prevents the complexity due to Layer3 routing and delays caused by multiple hops. Also by sending only significant traffic to right device directly, you would conserve resources on the devices that lays between traffic entry point and processing engine. As a result, all devices would be responsible with traffic they are excelled to process with.

Lawful Intercept

Packet broker is most useful on lawful intercept applications, especially for internet service providers that are legally responsible. In case laws mandate copying traffic, with very easy operation, traffic can be transferred to legal authorities. The most critical requirements in front of service provisioning can be cleared very easily.

User Interface

Everything is possible with a couple of drag and drop actions. All you have to do, is to define the ports exchanging traffic and rules to classify this traffic. That's all. No CLI commands or complex, nonsense and error prone regex games needed. Always possible to configure with simple clicks and drags. The rest will be handled by the backend operating system resulting error free configuration and smooth operation.

Karinca - Non-Stop Delivery

Correct data, right decision principle is the key to success for network administrators. This way, applying more efficient security policies and protecting application and user data more firmly becomes possible. High resolution network visibility, prevents errors and decrease troubleshooting times. Detailed analysis and decision tools help you easily and quickly create traffic flows. Once things are getting easier, it is more comfortable to deal with limited budget and resources. Time to return on investment for security products gets shorter. So, efficiency or cost index becomes higher.

Role of Packet Broker

No more deduplication: Once you collect copy of packets from different points, security and analysis devices process the same data more than once. This affects the performance and use of highly precious resources.

SSL encryption/decryption: By distributing the SSL packets to algorithm processing solutions, Packet Brokers allows decrypted packets to be transferred in the security chain. After inspection packet are redirected to SSL devices for re-encryption. All these adventures run without any significant delay.

Application control and analysis: User defined application data control of first 128 byte, enough to distinguish the application. Karinca also provides exceptional integrations with DPI softwares for deep data learning

Function	Description
Traffic Distribution/Filtering	L2 Mac Addresses, VLAN ID, MPLS tag, Ethertype L3 IPv4&IPv6 addresses, DSCP, protocol numbers L4 TCP/UDP port numbers
Port Selection	One to one One to many Many to one Many to many
Load Balancing	From one port to destination group From many port to destination group
Traffic Flow	100% packet delivery.No interruption or latency Analysis , aggregation, regeneration and filtering for traffic from more than one TAP modules
Other Controls	Tunnel termination, ERSPAN, GRE, VxLAN, Paket slicing, Port tagging protocol header manipulation
Yönetim	SNMP alarm management Easy Drag&Drop Web UI Single management interface
Hardware	
1/10/25Gb Ports	48
100 Gb Ports	6
Packet processor	Marvell
Flash - RAM	16GB - 8GB
Traffic Limit	1.9 Tbps
Power Supply	1+1 redundant, 220V, 650W
Fan	4+1 redundant
Dimensions	1U, 440x470x44 mm
Ordering Information	
ANW-NPB-ANT-601 / Karınca Packet Broker - 48x25G and6x100G ports	