NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Feature Brief

Precision Traffic Segmentation with VLAN Tagging

In today's multi-tenant and cloud-integrated networks, efficient traffic segmentation is essential for security, performance, and compliance. VLAN (Virtual Local Area Network) Tagging enables organizations to logically partition network traffic without physical separation, ensuring optimal bandwidth allocation, enhanced security, and simplified network management. At NEOX, we understand that VLAN Tagging is not just about isolation—it's about intelligent traffic steering, ensuring the right data reaches the right tools with zero compromise on performance.

What is VLAN Tagging

VLAN Tagging is a networking technique that assigns a unique identifier (VLAN ID) to Ethernet frames, allowing switches, routers, and network visibility tools to distinguish and route traffic based on logical segmentation rather than physical ports. Unlike traditional VLANs, which rely on static port assignments, VLAN Tagging enables dynamic traffic classification, supporting multi-VLAN environments, cloud workloads, and virtualized infrastructures.

Two of the most widely used VLAN Tagging standards are:

IEEE 802.1Q Standard VLAN Tagging: The foundational IEEE 802.1Q protocol enables VLAN identification by inserting a 4-byte tag into Ethernet frames. This universal standard supports up to 4,094 VLANs per network, ensuring interoperability across vendors while maintaining traffic segmentation for security and QoS prioritization.

Q-in-Q 802.1ad Provider Bridging: An extension of 802.1Q, Q-in-Q (or Stacked VLANs) adds a second VLAN tag for service provider environments. This allows nested VLAN segmentation (up to 16 million unique IDs), enabling carriers to preserve customer VLANs while applying their own service-tier identifiers across shared infrastructure.

Why VLAN Tagging Matters

NEOX's VLAN Tagging capabilities empower enterprises to streamline network visibility, enhance security, and optimize monitoring efficiency. Here's why it's critical:

1. **Granular Traffic Segmentation**
   VLAN Tagging enables organizations to isolate sensitive workloads—such as those in finance, healthcare, and IoT environments—while still ensuring full visibility for security monitoring tools. By logically segmenting traffic, it prevents unauthorized cross-VLAN communication, effectively minimizing the risk of lateral movement by potential attackers within the network. This enhances both security and compliance by keeping critical data flows separate and controlled, without sacrificing the ability to monitor and analyze traffic for threats.

2. **Optimized Monitoring & Tool Efficiency**
   VLAN Tagging significantly enhances monitoring and tool efficiency by ensuring that only relevant, VLAN-tagged traffic is filtered and forwarded to security and monitoring tools—dramatically reducing overhead and processing strain. By intelligently excluding non-critical VLANs from analysis, organizations can eliminate unnecessary data processing, allowing their security infrastructure to focus on high-priority traffic. This optimization not only improves tool performance but also streamlines threat detection, ensuring faster response times and more efficient resource utilization.

3. **Compliance & Data Privacy Alignment**
   VLAN Tagging plays a critical role in compliance and data privacy alignment by enforcing strict traffic segmentation to meet regulatory standards such as PCI DSS, HIPAA, and GDPR. By restricting monitoring tools to only access permitted VLANs, organizations can minimize legal exposure while maintaining necessary visibility for security and auditing purposes. This granular control ensures sensitive data remains isolated, reducing the risk of unauthorized access and helping enterprises adhere to stringent compliance frameworks without compromising operational efficiency.

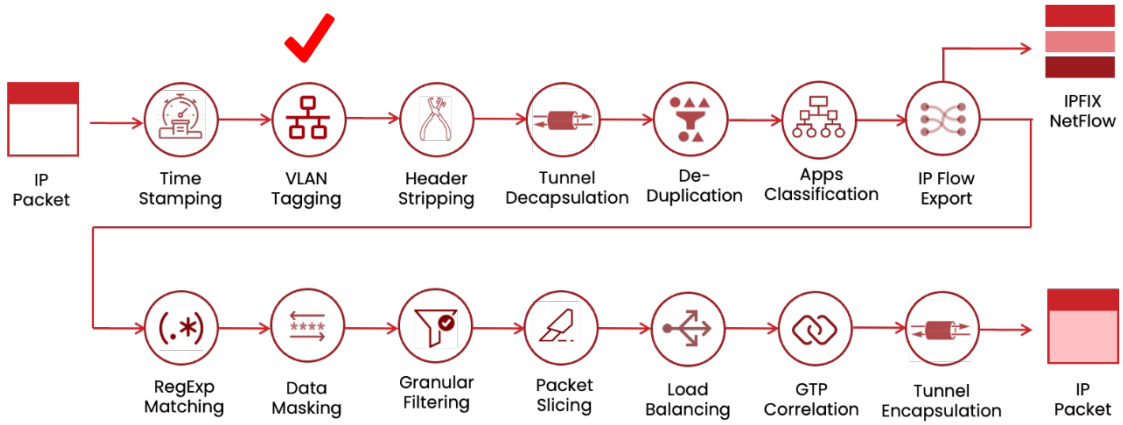
How NEOX Delivers Advanced VLAN Tagging

NEOX's PacketWolf, PacketLion, and PacketTiger series of Packet Brokers integrate hardware-accelerated VLAN Tagging to ensure zero-latency traffic classification and forwarding.

1. **Dynamic VLAN Assignment & Rewriting**
   Dynamic VLAN Tagging enables real-time network adaptability by allowing administrators to add, modify, or strip VLAN tags on-the-fly, ensuring seamless monitoring by the tools. This capability is particularly valuable in complex environments, as it supports Q-in-Q (802.1ad) tagging for service providers and multi-tenant architectures, enabling layered segmentation. By dynamically adjusting VLAN configurations, organizations can optimize traffic flow, enhance security policies, and maintain efficient network operations across diverse infrastructure deployments.

2. **VLAN-Aware Filtering & Forwarding**
   VLAN-Aware Filtering & Forwarding by Packet Brokers delivers intelligent traffic management by precisely routing specific VLANs to their designated monitoring and security tools—such as directing VoIP traffic to QoS analyzers or PCI-sensitive data to IDS. When combined with Deep Packet Inspection (DPI), this capability enables granular policy enforcement that goes beyond simple VLAN tagging, allowing network administrators to classify and control traffic based on actual application types and content. This approach ensures optimal tool performance while maintaining strict compliance with security policies and service-level requirements across the network infrastructure.

3. **Cloud & Virtual Network Integration**
   The PacketTigerVirtual solution extends advanced VLAN Tagging capabilities to cloud workloads, enabling organizations to maintain consistent network segmentation policies across both physical and virtual environments. By automating VLAN mapping between on-premises infrastructure and cloud deployments, it delivers seamless hybrid visibility while eliminating manual configuration errors. This intelligent integration ensures uniform security enforcement and monitoring across multi-cloud architectures, allowing enterprises to preserve their segmentation strategies while benefiting from cloud scalability - all without compromising compliance requirements.



Feature	PacketWolf	PacketLion	PacketTiger	PacketTigerVirtual
VLAN Tagging	✓	✓	✓	✓

Best Practices for VLAN Tagging with NEOX

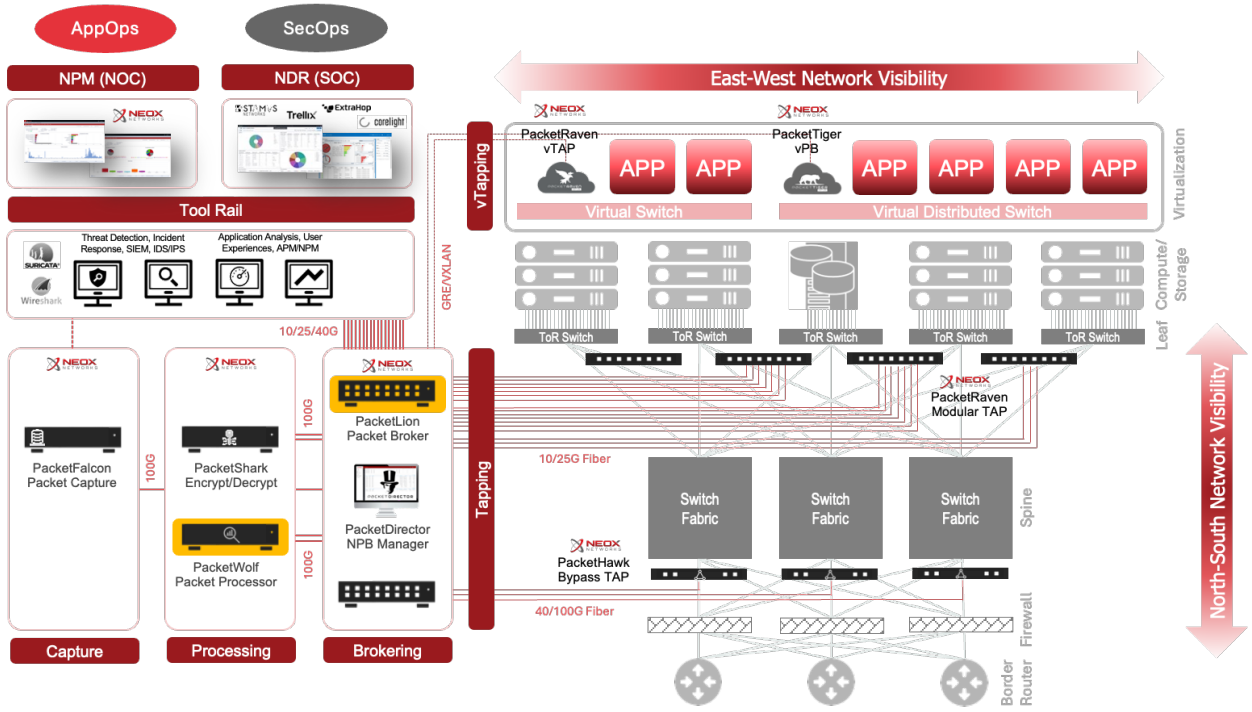
To maximize security and efficiency, we recommend:

- ✓ Enforce VLAN policies at the Packet Broker to filter traffic before it reaches monitoring tools.
- ✓ Enable hierarchical VLAN segmentation in multi-tenant/service provider environments.
- ✓ Preserve customer VLAN tags while adding service provider identifiers for end-to-end traffic isolation.
- ✓ Enforce granular policies—segment by VLAN and inspect content for application/behavioral threats.

To help you get the most out of your network, we recommend the following best practices to funnel, consolidate, and process all network traffic to be monitored through one of the two NEOX Packet Broker approaches:

- For better hardware performance, lower latency network, or for a future-proofed scalable visibility approach, deploy a **two-tier visibility architecture**. Use NEOX PacketLion Packet Broker for high-density TAP and tool aggregation, and use NEOX PacketWolf Packet Broker for faster VLAN Tagging and other packet services operations.

- For a lighter or software-driven approach, consolidate all network traffic to be monitored through a NEOX PacketTiger, and then from there to the tool rail. Same can be achieved in the cloud with PacketTigerVirtual before forwarding traffic to cloud-native monitoring or security tools.



The Future of Network Traffic Brokering Starts Here

As networks grow in complexity and speed, the importance of VLAN Tagging will only continue to rise. At NEOX we're committed to helping you stay ahead of the curve with innovative solutions that deliver precision, reliability, and performance.

Ready to Transform Your Network?

Discover how NEOX can elevate your Network Traffic Brokering with advanced VLAN Tagging technology. Contact Us today or Request a Demo to learn more about our solutions and take the first step toward a smarter, faster, and more secure network.

NEOX – Precision. Performance. Perfected.

About NEOX Networks

NEOX Networks provides Next Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity, by integrating the network intelligence and real-time data-in-motion. Learn more at neoxnetworks.com