Nile's layer 3 only network: Transcending VLANS

Introduction

Since the introduction of VLANs (802.1q), networks have become increasingly complex. Cloud adoption, IoT proliferation, and heightened security threats have exposed the limitations of the traditional Layer 2 approach, driving the need for more robust access controls and secure network architectures.

VLANs were primarily invented to mitigate broadcast storms, but their use for security-driven network segmentation was a later development. However, broadcast domain limitations, complex management overhead, and insufficient security boundaries hindered scalability, agility, and the ability to enforce granular access controls. Using VLANs for segmentation also left networks vulnerable to attacks within shared broadcast domains and introduced complexity in managing segmentation across multiple devices and vendors.

This document explores how dynamic, policy-driven Layer 3 segments, a foundational innovation of the Nile Access Service (NaaS), addresses these challenges. Nile's approach, grounded in zero-trust principles and microsegmentation, enables organizations to build secure, dynamic, and future-proof networks aligned with modern security best practices and scalability requirements.

Why a Layer 3 only network?

Nile's Layer 3 Network Architecture represents a significant advancement in network design, addressing the limitations of traditional VLAN-based segmentation. By operating entirely at the network layer (Layer 3) of the OSI model, Nile's architecture leverages technologies like network virtualization, overlay networks, and routing protocols to create secure, isolated network segments that span multiple physical locations.

Nile's Layer 3 segments are logical constructs that define network access and security policies based on user identities, device attributes, and application requirements, rather than relying on IP addresses or physical network boundaries. Hybrid cloud technologies, dedicated Nile Access Service hardware, and OSPF routing create logical segments that can span across multiple physical networks and locations. Layer 3 segmentation also solves the inherent complexity of managing and

securing traditional VLANs, as segments are created in the Nile Customer Portal and applied to devices and users wherever they connect.

At the core of Nile's approach is the principle of zero trust, which assumes that no user, device, or application should be implicitly trusted. Instead, granular access controls and continuous authentication and authorization are enforced through a combination of network segmentation, security policies, and identity-based access management.

Key features and benefits of Nile's Layer 3 Network Architecture include:

1. **Granular Segmentation**: Nile's architecture allows for the creation of fine-grained segments based on various criteria, such as user roles, device types, or application requirements. This level of granularity enables precise access controls and reduces the attack surface.
2. **Centralized Policy Management**: Network access policies and security controls are managed centrally through Nile's intuitive management interface. This simplifies the configuration and enforcement of consistent policies across multiple locations and eliminates the complexity associated with traditional VLAN configurations.
3. **Scalability and Flexibility**: Nile's architecture can easily scale to accommodate a large number of segments and can adapt to changing business requirements. New segments can be created, modified, or removed without the need for extensive network reconfiguration or hardware changes.
4. **Enhanced Security**: By enforcing zero trust principles and micro segmentation, Nile's architecture significantly enhances network security. By default, each segment, device and user is isolated from all others, mitigating the spread of threats and reducing the attack surface.
5. **Campus Zero Trust by default**: Unknown devices accessing the network are isolated by default, mitigating any threat of malware entering the domain.
6. **Seamless Integration**: Nile's Layer 3 Network Architecture seamlessly integrates with existing network infrastructure and security solutions. It leverages standard routing protocols like OSPF to enable efficient communication between segments and can integrate with leading security appliances and cloud platforms.

Jas >> regarding the Centralized Policy Management, with Nile's Access Engine, we are just controlling access policies, when I as a user is reading security controls, the first thing that comes to my mind is IDS/IPS, DDoS and other security related things that a firewall typically controls. Nile's Access Engine is not a security center but instead it is just a policy center. Before we had Access Engine, our story to the customers has always been about Centralized Policy Management through the firewall: By default Nile will forward all the traffic to the firewall upstream, where the customer will be able to take care of adding all the security and access policies and they would have a single management plane where they can troubleshoot and add/delete any new policy. We want to promote the use of Nile's Access Engine but at the same time also show a note to the customers that if they want security policies to be applied, they still need to use the firewall to control those aspects.

Layer 3 segmentation in the Nile Service Block operates at the network layer by leveraging OSPF to facilitate communication between segments. Each segment functions as a separate logical network, with upstream security appliances or routers handling inter-segment traffic. The Nile Access Service integrates closely with security vendors like Palo Alto, Fortinet and zScaler, ensuring policies are consistently applied to all traffic.

Nile's Layer 3 Network Architecture represents a significant step forward in network design, providing organizations with a scalable, flexible, and secure foundation for building modern, zero-trust networks. By eliminating the complexities associated with traditional VLAN-based segmentation and enabling granular access controls, Nile empowers organizations to protect their critical assets, streamline network management, and adapt to the ever-evolving demands of the digital landscape as we enter this period of AI powered innovation.

Layer 2 vs Layer 3

Characteristic	VLAN (Layer 2)	Nile's Layer 3 Architecture
Scope of Segmentation	Confined to the broadcast domain	Creates logical segments isolated at the network layer
Role of Routing	Requires external routers for inter-VLAN communication	Inherently leverages routing for inter-segment traffic
Configuration Complexity	Configuration maintenance and control across multiple devices and vendors is highly complex and prone to human error.	Centralized management and simplified configuration through the Nile Customer Portal
Security Approach	Limited isolation within shared broadcast domains and susceptible to physical port vulnerabilities	Zero trust principles with granular access controls and default isolation between segments, users, and devices
Redundant Connectivity	Implementing redundant links is cumbersome	OSPF routing enables optimized path selection and redundancy
Broadcast Domain Issues	Prone to broadcast storms and performance degradation in large networks	Significantly reduces broadcast traffic, enhancing performance
Connectivity Approach	Often tied to physical location or switch port	Policy-based connectivity based on user identity, device attributes, and application requirements

The comparison between traditional VLANs and Nile's Layer 3 Network Architecture highlights the significant advancements and benefits of Nile's approach in terms of segmentation, management simplicity, security, performance, and connectivity. These advantages position Nile's Layer 3 Network Architecture as a powerful enabler of zero-trust security models and a foundation for building modern, agile, and secure networks.

Nile Layer 3 Architecture: Customer Use Cases

Now that we've covered the theory, how are Nile Access Service customers benefiting from our Layer 3 only approach today?

Healthcare

One of our customers in the healthcare industry faced a critical security challenge when the manufacturer of their 50 x-ray imaging machines suddenly announced the discontinuation of security and OS updates. The customer was advised to replace all the machines, many of which were not fully depreciated, leading to a financial impact of several million dollars.

With Nile's Layer 3 segmentation, the customer was able to swiftly create firewall rules to isolate the vulnerable x-ray machines from the rest of their network. Through the Nile Customer Portal, they centrally configured and deployed the segmentation policies across all affected sites, without the need for physical reconfiguration or on-site visits.

By leveraging Nile's architecture, the customer avoided the premature replacement of the x-ray machines, saving them millions in replacement costs and lost productivity. Moreover, the segmentation approach ensured the customer maintained compliance with HIPAA regulations and protected sensitive patient data, despite the vulnerabilities in the x-ray machines.

Read Next

Building a Zero Trust Campus: Zero Trust Access, Nile Service Block Hardware

Revision #17
Created 13 March 2024 19:16:06 by JR
Updated 28 March 2024 21:55:09 by JR