XipACE – AI/ML Assisted Application Aware SD-WAN & Optimization

Advanced Traffic Steering, Link Balancing and Bonding, Quality of Service, Analytics

INTRODUCTION

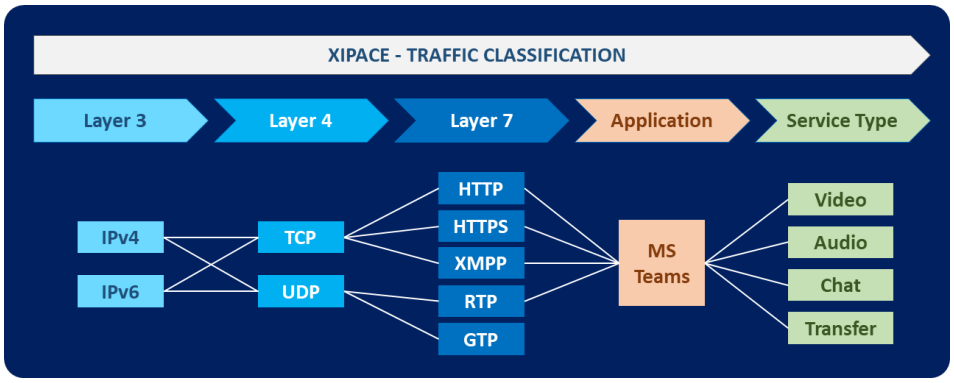
This document highlights the advantages of XipACE (XipLink Application Classification Engine), an AI/ML powered deep packet inspection, featuring XipLink SD-WAN solution proven over satellite and constrained networks. XipACE is tightly integrated with XipLink's advanced multi-orbit SD-WAN's traffic performance enhancement system with functions such as **Link Balancing/Bonding, Traffic Steering, Adaptive QoS and Application Priority**, **Selective Stream Duplication**, **Data Analytics**, and **Basic Firewall.**

XipACE Capabilities

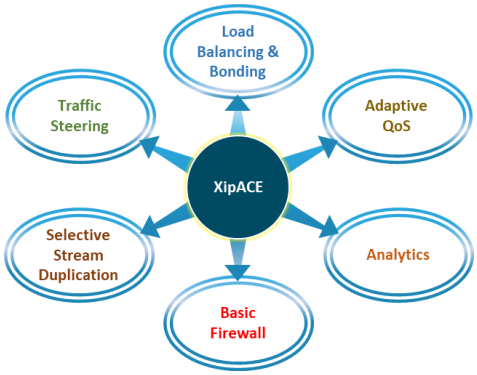
- Application **visibility up to Layer 7** (including service types)
- **Tightly integrated** with XipOS QoS, Link balancing/bonding, Traffic Steering, Failover/Overflow, Firewall
- Application and Usage **Analytics**
- **AI/ML assisted** enhanced classification speed and accuracy
- **7,727 signatures**, 2,085 apps, 471 protocols and 127 attributes, including metadata
- Close to 1**00% classification accuracy**; very low false negatives or false positives

NEXT-GEN PACKET CLASSIFICATION

XipLink's XipACE technology is an industry leading advanced protocol and application classification engine with metadata extraction for application-aware networking. XipACE provides real-time IP network traffic visibility up to layer 7 and beyond. XipACE, based on R&S PACE 2 technology, can identify and classify thousands of applications and protocols and extract metadata in real time, even if traffic is encrypted or obfuscated. R&S PACE 2 uses **Machine learning (ML) & deep learning (DL)** capabilities to enhance classification accuracy and provide **weekly signature updates** resulting in the best application detection capability.

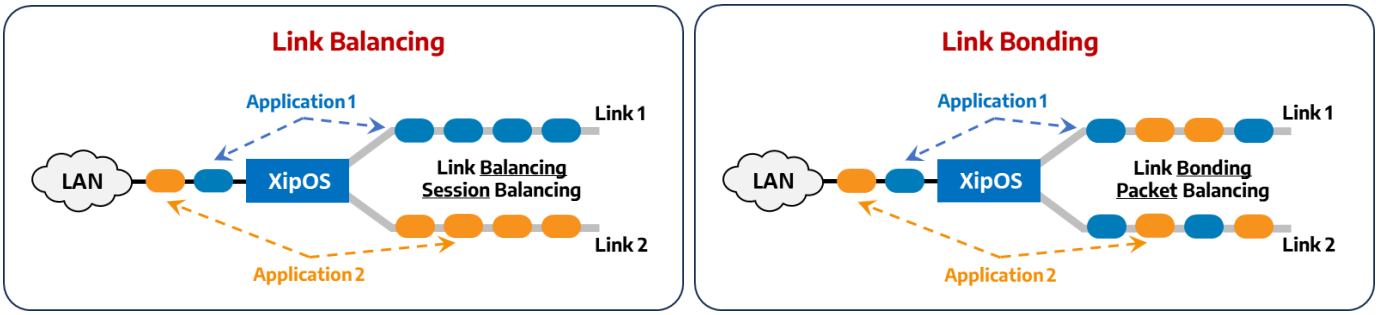


XipACE not only provides a complete view of the applications running on a network, but it also enhances the overall XipLink solution dramatically enhancing other XipOS functions shown in the drawing below.



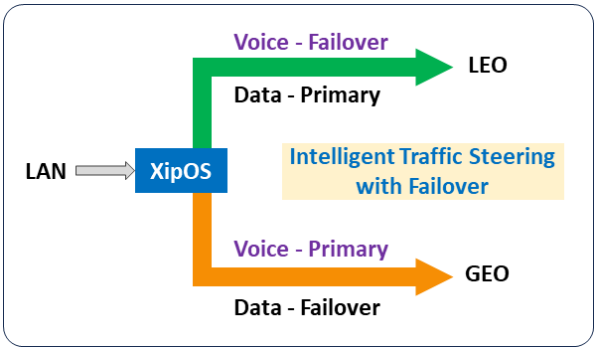
APPLICATION AWARE LINK BALANCING AND BONDING

XipACE significantly enhances the capabilities of XipOS Link bonding and balancing by providing more granular control over how applications are distributed across available links. This allows users to prioritize mission-critical applications while enabling service providers to utilize the links more efficiently and define more focused service level agreements (SLAs).



INTELLIGENT TRAFFIC STEERING AND APPLICATION FAILOVER

XipOS Traffic Steering provides the capability to select specific traffic types or applications and differentially steer those across appropriate links, depending upon the status and health of those links. Building upon XipLink's powerful, hierarchical QoS architecture, users can now define filter rules based on XipACE application classification up to Layer 7 (and beyond).



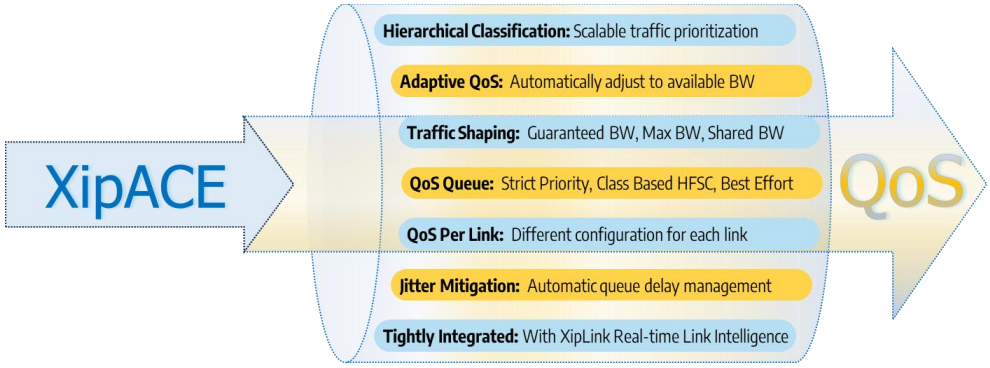
Steering rules can be based on Applications, Service Types, IP, port, protocol, DSCP, VLAN ID, VLAN priority or combinations of these fields to select specific traffic to be processed. Each such group of selected traffic may be configured with specific steering rules, in addition to the chosen acceleration and optimization policies.

XipOS supports advanced SD-WAN link failover that is seamless, integrated with link-specific QoS and ensures uninterrupted sessions. XipACE enhances this functionality by allowing users to define failover rules based on classifications, extending to application service types. This enables users to failover specific applications - rather than the entire link - when predefined criteria are met.

ADAPTIVE QUALITY OF SERVICE (QOS) AND APPLICATION PRIORITY

XipLink XipOS offers a highly flexible and configurable Quality of Service (QoS) solution that adapts to available bandwidth, ensuring optimal traffic and memory management. This is ideal for mission-critical or performance-sensitive TCP applications that require guaranteed bandwidth. Some of the key QoS features include:

Application Priority Fair Access Policy: One of the key benefits of XipOS QoS is its ability to prioritize applications over Low Earth Orbit (LEO) services. Typical LEO services treat all applications equally, which can lead to performance issues with critical traffic, such as voice signaling and control, especially during congestion or service degradation. In contrast, XipOS' can bypass LEO service provider's FAP and give control to XipOS' QoS to prioritize critical traffic, ensuring consistent application performance even in a consumer grade network service.



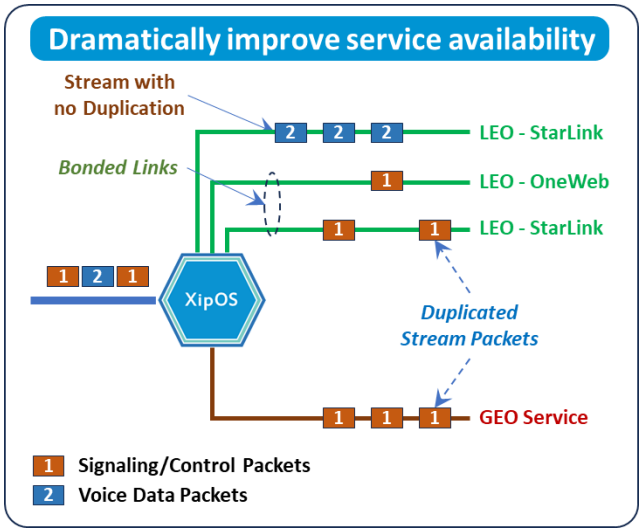
Multiple QoS Queue Support: XipOS supports various configurations, including Strict Priority, Class-Based, and Best Effort, allowing for tailored traffic management.

Multi-Path Network Capabilities: In a multi-path network, QoS configurations can be applied per link in each direction, enabling separate queues and bandwidth management options such as Guaranteed Bandwidth, Maximum Bandwidth, and Shared Bandwidth.

Advanced Queue Delay Management: XipLink's sophisticated delay management minimizes jitter, significantly enhancing the user experience for jitter-sensitive traffic.

SELECTIVE STREAM DUPLICATION

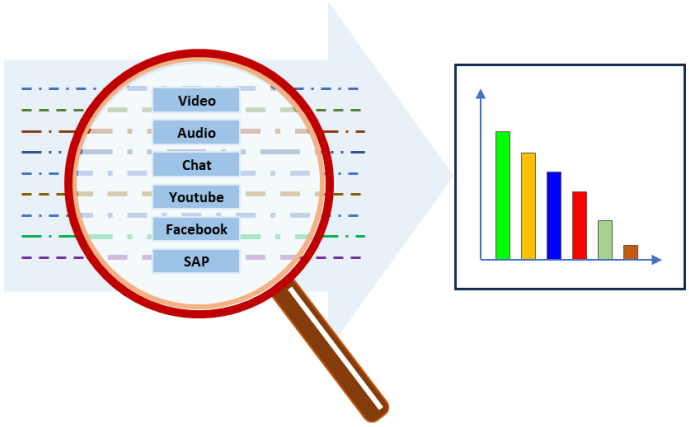
XipLink's selective stream duplication addresses the challenges of lossy or inconsistent links, by allowing the duplication of any high-value and/or impairment-sensitive streams, across one or more links, on an application-by-application basis. This feature is particularly valuable for ensuring the reliability of control plane traffic. By duplicating control plane packets, critical applications such as voice and video sessions can maintain their integrity even in the face of network disruptions. The combination of more robust GEO links with LEO links, when used for duplicating control-plane traffic, enhances overall service reliability. As a result, users experience significantly improved service quality and greater assurance of SLA compliance. XipACE enhances this feature by allowing a highly granular application classification and control.



Selective stream duplication is a powerful tool for enhancing availability of mission-critical traffic in single path or multi-path environments, increasing resiliency and availability of critical applications for end users. This functionality is ideal for ensuring resilience of signaling or control plane packets for high value voice/video real-time applications.

APPLICATION VISIBILITY (ANALYTICS)

XipACE inspects the data packets flowing through the network, identifying specific applications generating the traffic. This level of visibility allows network administrators to gain insights into how applications are behaving, even if the traffic is encrypted or obfuscated. This information enables network administrators to detect anomalies, performance issues, irregular patterns, make changes to any policies, update QoS rules or block certain applications based on security / business rules. XipACE based application visibility also allows for better management of network resources by prioritizing important traffic (e.g., VoIP, video conferencing) over less essential applications (e.g., file sharing).



BASIC FIREWALL

XipOS supports a basic firewall that allows or drops traffic based on packet identification by the built-in classification engine. XipACE application awareness enhances XipOS capability by adding the ability to classify packets up to layer 7 (including service types). This enables network administrators to control traffic that flows across the links.