infinera®

Infinera Converged Network Operating System (CNOS)

Disaggregate and Accelerate Network Innovation

TRANSFORMING NETWORK ELEMENT ARCHITECTURES

New emerging network concepts and applications – as in 5G networks – require fast technology innovation cycles. Yet traditional monolithic network element architectures restrict the flexibility for changes and increase the cost and complexity of the network. To accelerate innovation and prepare the network for new applications, the disaggregation of hardware and software components delivers the promise of easily adding and upgrading best-in-breed functions based on open network architectures. It adopts this principle by disaggregating the network operating system (NOS) from the routing hardware, which is an essential part of Infinera's Infinite Network vision. Infinera makes the disaggregated architecture a viable solution for service providers who are currently using traditional monolithic solutions.

INFINERA CONVERGED NOS IN CARRIER NETWORKS AND DATA CENTERS

BOOSTING FLEXIBILITY AND PERFORMANCE

In the expanding ecosystem of open white box switches, Infinera Converged NOS (CNOS) offers high-performance hardware-independent flexibility and disaggregated software components including a Linux operating system, hardware abstraction layer, IP stack and network protocol suite. Based on Open Compute Project elements, CNOS provides broad support for white box switches with Open Network Linux (ONL) running on open hardware and installed using Open Network Install Environment (ONIE). CNOS is designed from the ground up to meet the requirements of carrier networks where comprehensive IP/Multiprotocol Label Switching (MPLS) functionality complements high availability and resilience at multiple levels, ensuring accurate packet synchronization without compromising robustness. CNOS includes a sophisticated hardware abstraction layer that supports both standalone and multi-unit forwarding architectures, as well as protocols such as MPLS. CNOS relies on our field-proven IP/MPLS stack for applications requiring high performance, high scalability and high resiliency. The user space IP stack decouples the stack from the kernel, thereby supporting in-service software upgrades. CNOS is designed with open application programming interfaces (APIs) to simplify integration into existing environments and enable operators to reap the benefits of a programmable infrastructure.

BENEFITS OF INFINERA CONVERGED NOS ON OPEN NETWORKING PLATFORMS

■ **Provides a contemporary software architecture** leveraging open source, Linux and the proven Infinera IP/MPLS stack

■ **Offers a modular protocol suite** that enables customers to choose the right protocols for the application, e.g., Infinera IP/MPLS, open source or commercial protocol stacks

■ **Accelerates innovation cycles** with open APIs that guarantee interoperability with existing systems, allowing operators to focus on virtualizing and automating their infrastructure

■ **Promotes platform independence** to support the growing ecosystem of white box switches for carrier, cloud and enterprise applications

■ **Delivers hardware disaggregation**, enabling the Converged NOS to be purchased independently from white box switches

■ **Incorporates flexible and resilient deployment** from single nodes, multi-unit nodes and spine-and-leaf POD architectures

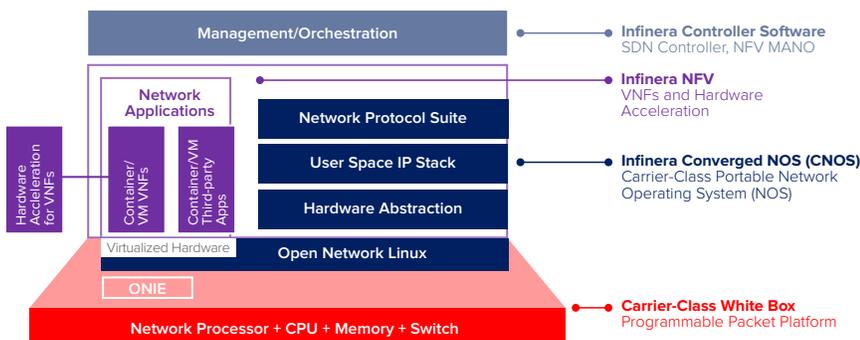■ **Supports standard provisioning tools** and ancillary applications and monitoring agents

Figure 1: Infinera Converged NOS (CNOS) Architecture

FLEXIBLE DEPLOYMENT MODELS

Hardware abstraction, open APIs and the modular NOS software structure define the framework for building network elements, from single unit pizza boxes to innovative, fully resilient multi-unit node configurations or versatile, data center-like spine-and-leaf POD architectures. This broad set of innovative deployment options provides flexibility in moving from one deployment type to another when networking needs change. These components enable seamless scaling capacity and capabilities such as network functions virtualization (NFV), as required for multi-access edge computing (MEC) and provider edge (PE) router applications.
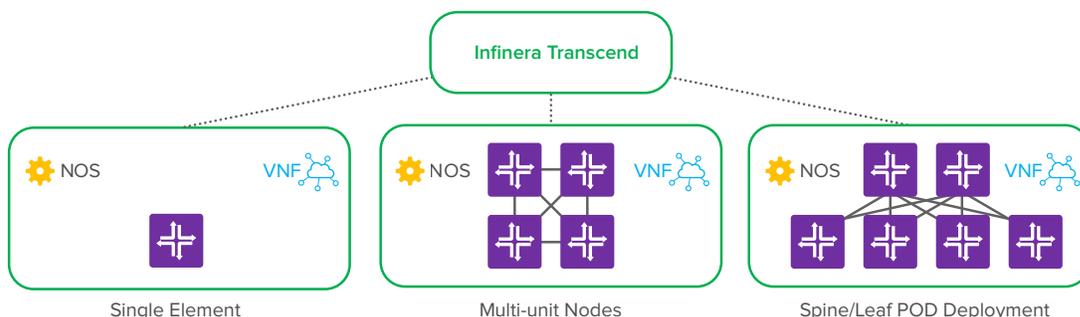

Figure 2: Highly Scalable Network Element Architecture Options

CNOS APPLICATIONS IN CARRIER, CLOUD AND ENTERPRISE NETWORKS

CNOS capabilities, including hardware platform independence and unique deployment options, are ideal for a broad range of use cases in carrier and data center applications.

CARRIER APPLICATIONS

CNOS is built for robust carrier-class network operations characterized by sophisticated packet processing and forwarding mechanisms along with a high degree of service availability. CNOS software is a single software image that ports to multiple white boxes and thus secures smooth interworking between elements as well as simplified operations and maintenance. CNOS is built to meet the requirements of networks where fiber deep architectures are in focus — such as 5G networks and Distributed Access Architectures. CNOS, together with the right set of white box elements, meets these application requirements, including capacity scale and growth, accurate synchronization, low latency and future scalability. Multi-unit configurations contain multiple similar white boxes connected together to form a fully resilient and high-capacity node, which is managed as a single element. The carrier-class control and management plane empowers self-healing and graceful recovery from exceptions and outages. Open APIs guarantee interoperability for newly purchased software and simplified integration of subcomponents with new functionality. The Infinera disaggregated router with CNOS, together with the advanced, multi-vendor Infinera Transcend software-defined networking (SDN) controller, enables new flexibility to extend router capabilities to multiple use cases and manage network evolution in multi-vendor environments. By leveraging best-in-class NFV solutions running as part of the router setup, the Infinera solution addresses various applications, such as PE router applications where virtual Broadband Network Gateway (vBNG) or virtual carrier-grade network address translation (vCGNAT) are required, as well as MEC use cases.

DATA CENTER INTERCONNECT

For cloud applications that require high capacity, high port count and high scalability, cloud fabrics can be built using standard data center-centric white boxes running simple interior gateway protocols (IGPs). Layer 2 services requiring protocols such as Virtual Private LAN Service (VPLS), Virtual Extensible LAN {VXLAN) and Ethernet Virtual Private Network (EVPN) interconnect these data centers. Gateway nodes typically connect data centers to other data centers or to end-users/customers via IP backbones, IP transit networks and peering exchanges. Devices used in these applications require support for large forwarding tables, large packet buffers and protocols such as IP/MPLS or segment routing. These capabilities are emerging on white box hardware today, and CNOS enables these capabilities in cloud provider networks.