



NetDevices ModuLive™ Operating System

A NetDevices Technical Note

This technical note describes the key features of NetDevices' ModuLive Operating System and how they enable enterprises to overcome the limitations of traditional solutions and fully deliver the benefits of integrating multiple services.

In today's globally connected marketplace, enterprises are rapidly becoming more decentralized and distributing more & more business applications to branch offices. Branch office networking requirements are changing significantly in order to support these business needs. Multiple networking services such as routing, security, firewall and VPN are required at most locations. With mission-critical applications being distributed to branch offices, the branch network infrastructure must be robust, scalable and remotely manageable, with easy extensibility to support new services & applications.

Being based on cascaded point devices, traditional branch office solutions are not able to satisfy these requirements -- due to disruptive addition of new devices to support new services, complex management, lack of remote management and unacceptable levels of downtime. Hence, enterprises need next-generation branch office solutions that enable them to fundamentally re-architect the way their branch office networks are built & managed.

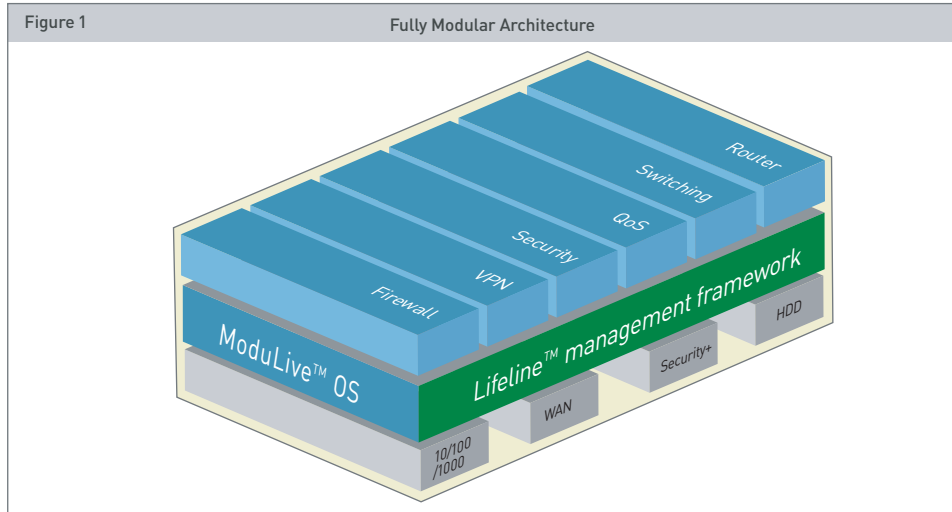
Converging multiple services on a single branch office platform appears to be an attractive option to overcome the limitations of traditional solutions. However, integrating multiple services on a single platform presents several significant challenges as outlined below:

- Risk of wide service outage as one service impacts others and services become frequently unavailable
- Constant service upgrades/ changes, impacting uptime for all services on the platform
- Ensuring efficient & effective management of all services
- Maintaining high performance while supporting multiple services
- Providing extensibility for future services

To fully & effectively address the branch office networking requirements of today's distributed enterprises, *a purpose-built solution that is based on a fully modular software & hardware architecture and has been architected from the ground up to provide unified operation & simplified management of multiple services* is required.

The NetDevices ModuLive™ Operating System

NetDevices unified services gateways are based on NetDevices' multi-patent-pending ModuLive operating system, which is a fully modular, always live software base that provides levels of availability and serviceability previously unavailable in enterprise branch office products. The key aspects of ModuLive and how they address the challenges outlined above are described in this document.

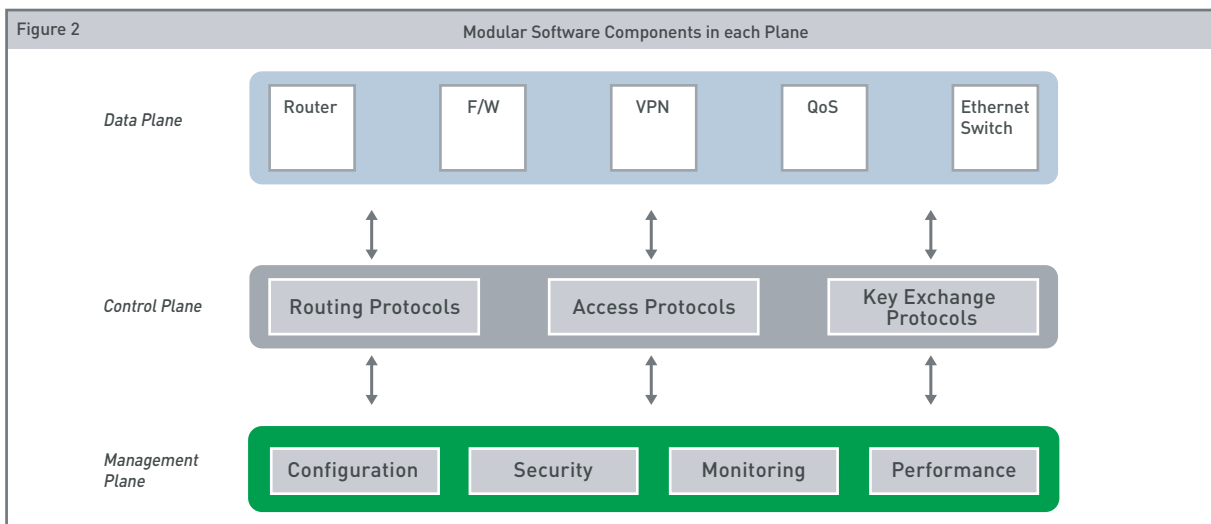


Modular Software Design

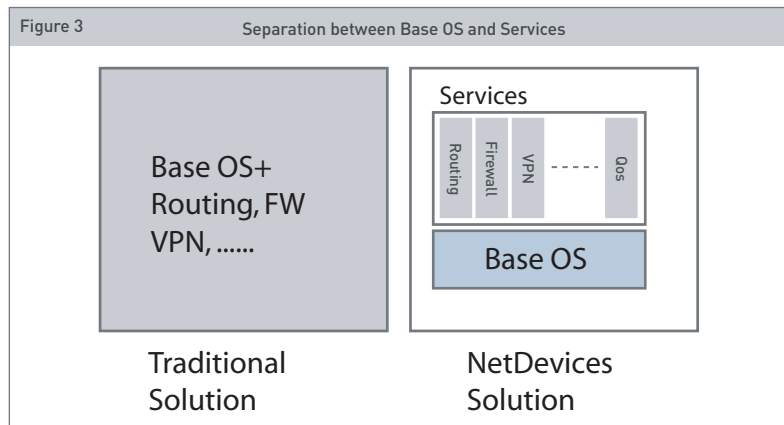
The fully modular software architecture of the NetDevices ModuLive OS supports modularity along multiple dimensions, which plays a critical role in maximizing serviceability and service availability.

Separation between different planes: The services and management functions of the NetDevices system are separated into three different planes – data, control and management planes. This enables insulation of failures from one plane to another. For instance, if the data plane or control plane is unavailable, the management plane is unaffected and full management access & functionality continues to be available.

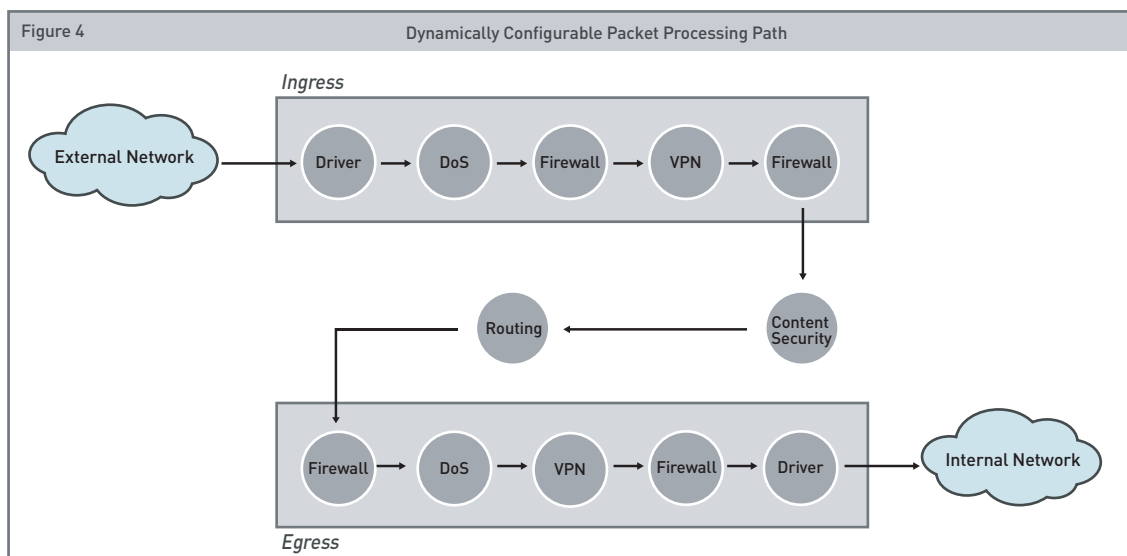
Modular software components within each plane: The functions and services within each plane are delivered through modular software components, as illustrated in Figure 2 below. Each service can be enabled, disabled, upgraded or re-configured without impacting other services. A failure in one service causes minimal or no disruption to other services. The serviceability is further enhanced by the ModuLive Service Manager, which supports comprehensive revision control and tracking of each service module with the ability to roll back to an older version if required.



Separation between base operating system (OS) and services: In the NetDevices ModuLive software architecture, the individual services are separated from the base operating system. As a result, individual services can be upgraded or new services added, without having to re-start the base operating system. This is in contrast to traditional solutions that are based on a monolithic software base with no separation between the base OS and services. This distinction is illustrated in Figure 3 below. With the traditional approach, upgrade of any service will require a re-start of the base OS, thereby impacting all services in the system.

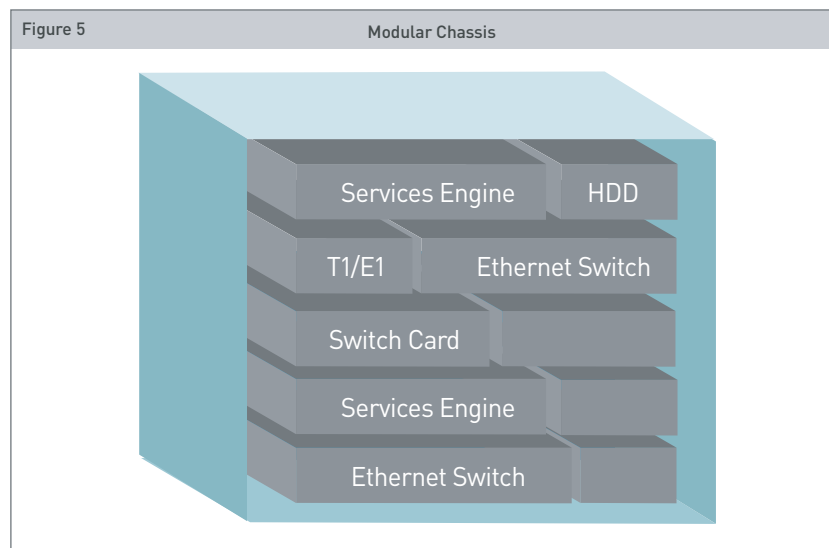


Dynamic configurability of packet processing path: Another key aspect of modularity in the NetDevices ModuLive architecture is the ability to dynamically configure the service functions in the packet processing path for each interface. An example of such a packet processing path is depicted in the figure below. Inclusion or exclusion of specific services from the processing path and changing the order of services in the path can be done dynamically. This capability plays a critical role in enabling upgrades of each individual service without impacting other services. For instance, in the example below, if the VPN service needs to be upgraded, the packet processing path is first modified to exclude the VPN node. Packet processing through other services continues uninterrupted. After the VPN service is upgraded, it can be re-inserted back into the processing path.



Modular Hardware Design

The NetDevices ModuLive OS runs on a modular hardware chassis with separate slots for different line interface cards, Ethernet switch cards, the switching fabric and the Services Engine (which is the packet processing core of the system). The chassis design, illustrated in Figure 5 below, allows wide flexibility to customize the number and mix of cards used based on the enterprise's requirements. Furthermore, the modular design allows the addition of optional hardware components such as the Hard Disk Drive (HDD) card when required.



The NetDevices system supports online insertion and removal of cards (i.e. live “plug & play”). The ModuLive Chassis Manager supports dynamic detection of new hardware modules and configuration changes, thereby enabling seamless service continuity during hardware upgrades.

High Performance

NetDevices Unified Services Gateways ensure high performance as multiple services are added onto the platform through several different aspects of its hardware and software design. The management plane and data/control planes are powered by separate, dedicated processors. This ensures that the processing load required by system management functions do not have any impact on service performance for all services supported on the system.

Modular software processes that are part of a truly unified system also play a critical role in enhancing overall system performance. In NetDevices' “Common Classification” approach, each packet is classified at the system ingress point and the packet traverses through the rest of the system with all aspects categorized. As a result, each additional service in the packet processing path does not consume any processor cycles for the CPU-intensive categorization process. A similar approach is used to optimize performance when a service needs to perform additional packet inspection (e.g. URL extraction and normalization by the IDS service). In such a scenario,

the output from this additional packet inspection is stored in a buffer, so that any additional service that needs this information does not need to repeat the CPU-intensive process. These architectural elements clearly illustrate the contrast between NetDevices' unified services approach and an approach based on point products or "semi-integrated" platforms with no real unification of services.

Unified Management

The NetDevices system enables efficient management of all services by providing a comprehensive, unified, web-based management system to remotely manage all branch office services. All services are managed via a common interface with granular, detailed instrumentation and control provided for all components and modules in the system.

In a platform supporting multiple services, it is possible to have inadvertent conflicts between different services. For instance, the firewall access control policies may conflict with the routing policies. Since the NetDevices management system has full visibility over all services and built-in knowledge of the interactions between services, it supports an application-aware configuration process. A wizard-based approach is used to drive towards the right configuration for each service and automatically detect & resolve configuration conflicts.

By leveraging its fully modular system design, the NetDevices unified services gateways can support functional, role-based partitioning of management. The management of services and physical components can be partitioned among different administration groups based on their roles. Conflicts between groups can be avoided through the use of clearly defined access rights, priorities and over-ride privileges for each group.

Extensibility for future services

As noted in earlier sections, the modular software and hardware design of the NetDevices unified services gateways enables quick and non-disruptive addition of new services. New services can be added via a remote software upgrade without impacting other services in operation. Due to the dynamic configurability of the packet processing path, the new service can be seamlessly inserted into the processing path for specific interfaces.

If additional cards have to be added to support new services, the modular chassis design of the NetDevices hardware allows hot-swappable insertion of these cards into the system. For instance, due to the addition of new services, if one Services Engine card is not adequate to meet the required processing capacity, a second Services Engine card can be added to support the new services.

In contrast, with traditional solutions, adding a new service often requires the disruptive addition of a new device, impacts all other services and substantially adds to overall system downtime.

Key Benefits

The following table summarizes the key benefits offered by the NetDevices ModuLive architecture and the features that deliver these benefits:

Key Benefits	Derived From:
Maximum availability	<ul style="list-style-type: none"> • Non-disruptive service upgrades & configuration changes • Online insertion & removal of cards • Quick & easy addition of new services • Minimal or no disruption caused by failure of one service on other services
Lower OpEx	<ul style="list-style-type: none"> • Efficient service upgrades • Total remote management • Efficient use of centralized IT resources
Lower CapEx	<ul style="list-style-type: none"> • Unification of services on one platform • High availability without need for dedicated failover devices • High performance with multiple services
Enhanced IT staff productivity	<ul style="list-style-type: none"> • Less time spent on upgrades & routine maintenance • Efficient use of centralized IT resources
Investment protection	<ul style="list-style-type: none"> • Easy extensibility for new services • New service additions via remote software upgrades • Hot-swappable addition of new hardware cards

Summary

Branch office networking requirements are changing at a rapid pace in order to support the enterprise need for distributed applications. Traditional solutions, based on multiple point devices, are unable to satisfy the new requirements. A unified branch office services platform is required to overcome these challenges. To provide unified operation & simplified management of multiple services, such a platform has to be based on a fully modular software and hardware architecture. The NetDevices Unified Services Gateways, based on the NetDevices ModuLive operating system, are purpose-built solutions designed from the ground up to overcome the limitations of traditional point products and fully deliver the benefits of integrating multiple services.



NetDevices Inc.
 1296 Lawrence Station Road
 Sunnyvale, CA 94089
 T +1.866.YES.NETD
 F +1.408.734.5401
 E info@netd.com
 W www.netd.com