In-Stat White Paper

The Organizational NOS (Network Operating System)

Bryan.vandussen@reedbusiness.com
November 2008

The Organizational NOS

Executive Summary

Network operating systems (operating systems designed and developed for networking devices such as routers and switches [NOSs]) have traditionally been designed to meet the needs of their hardware and innovative new network-based applications. However, the expected explosion in network video traffic driven by mobility, business Internet, consumer Internet, and consumer IPTV/CATV services have drastically changed the complexity of network architectures and have changed how NOSs are designed and used. Instead of a single NOS generically designed for all devices, the new NOS is designed for the position the devices occupy in the network (access, core, data center, customer premise) and people and organizations that use and manage them. The result is a more customized network operating system made for operational groups and individuals – the organizational NOS.

Unlike an overarching single NOS that attempts to meet all the requirements of all devices, in all areas of the network, for all services, and every group that operates and manages them, organizational NOSs are tailored to meet the unique requirements of the people and processes that operate and manage a variety of service provider, enterprise, and consumer networks. Organizational NOSs also provide a common language that enables organizations and their networks to seamlessly communicate and interoperate. The organizational NOS's ability to satisfy the diverse operational requirements of a variety of groups and individuals while preserving and enhancing the interaction between them, enables networks to be used in new ways. Organizational NOS's help operators of all sizes, capability, and levels of expertise deliver new services at unprecedented speed with unmatched availability.

This paper argues that a single NOS may not be the most efficient approach. Instead, NOSs should be designed not only for the place in the network occupied by the devices, but also to meet the needs of the people and processes that use them.

Organizational NOSs – One Size Does Not Fit All

NOSs have been used in a wide variety of devices by a wide variety of organizations for decades. Dating back to the first non-mechanical telephone switch and including many of today's routers, switches, security appliances, voice, video, application optimizers, storage appliances, and other network devices; NOSs have been used as the platform for delivering not only basic network transmission, switching, and routing, but also for a wide range of enhanced voice, video, and data services. These devices have also been used in a number of places in networks by a variety of organizations, groups, and individuals that range from the largest network service provider and corporate enterprise to the individual operating a home wired or wireless network.

The networking devices, although sized or configured to meet a variety of positions or functions in the network – service provider core and edge, the data center, branch office access, small and medium-sized business access, and home networking – may use an operating system that is not tailored to its

place in the network nor to the people and processes that employ it. For example: service provider personnel might discover that the NOS in their core routers include enterprise features such as SNA or AppleTalk support. Or, an enterprise or small business IT group might find that an access router NOS includes support for MPLS or integration with a service provider-oriented back office system.

Organizations or individuals using networking devices that have too many – or too few – NOS capabilities can impact not only the efficiency of the organization and people using the devices, but also create:

- *"Bloated" NOS's that use large amounts of RAM, yet still deliver poor performance*: Anyone who has attempted to upgrade a personal computer that has limited CPU and RAM capacity with a new OS that has a larger image with more functionality, knows that a big OS can slow things down or force the user to invest in hardware upgrades. In the network, the same scenario holds true. Too much OS functionality in a small device can result in poor performance and additional cost.
- *Complex integration with service provider and enterprise security, management, provisioning, and billing systems*: Service providers invest millions of dollars in their management, provisioning, and billing systems. A NOS that includes features and functions that may be well suited for enterprise networks or include access features in core network devices, can add complexity to the task of tying the device to back office systems. This can result in increased software development and maintenance costs, as well as longer lead times to develop and launch new network-based services.
- *Lengthy timelines to perform software maintenance*: Any NOS that increases software complexity by including non-essential features and functions can also make it more difficult for network operators to update software to accommodate bug fixes and other software changes. Operators can face extra regression and interoperability testing to ensure compatibility for features that are not used in specific network areas or devices. In some cases, bug fix might even require not just a software reload, but also a visit by a technician to perform the hardware upgrade.
- *Increased training and re-training costs*: Even though an organization may not use a specific feature or function in a NOS, users of that NOS must nevertheless understand the features and be familiar with configuration options for them.
- *Higher cost to operate and maintain networks*: Larger software images, increased software complexity, and more difficult integration with network management and back office systems increases operations and maintenance costs. NOSs that are not tailored to meet the needs of the organizations that use them increase the number of people required to support them as well.

A NOS, customized to meet the needs of the place in the network it occupies and the organization that operates it, is simpler, more cost effective, and easier to integrate with management and back office systems. Let's examine the people who use NOSs and their needs and how the organizational NOS has been developed to meet those needs.

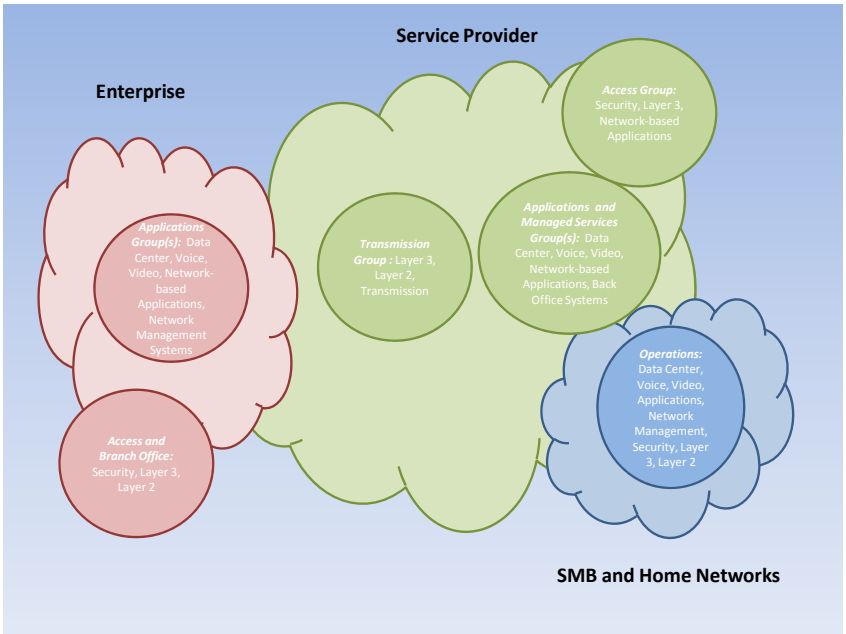
The Right NOS for the Right Organization

There are several discrete organizations and individuals that use network operating systems. In some cases, their needs and the tasks they perform overlap, however, in general each organization has specific operational requirements that make a customized NOS essential. In general, NOS organizations fall into eight categories that in general map to specific places devices occupy in the network (access, core, data center, customer premise):

- Service Providers
    - *Transmission Group*: Responsible for Layer 1, 2, and some Layer 3 services and the processes and interfaces to back office systems that support them.
    - *Access Group*: Responsible for Layer 3 services, network quality of service, and some network-based applications services (for example security) as well as the processes and interfaces to back office systems that support them.
    - *Applications Groups*: Responsible for data center, voice, video, network-based applications services and back office systems. There are often multiple application groups within large service providers.
    - *Managed Services*: Responsible for customer premise equipment and "cloud" computing as well as the back office systems that support them.
- Large Enterprise
    - *Access and Branch Office Group*: Responsible for Layer 2 and 3 services, as well as basic network-based capabilities such as Security. This group is also responsible for the network management systems that support the services they provide.
    - *Applications Groups*: Responsible for data center, voice, video, network-based applications services and back office systems. There are often multiple application groups within large enterprises.
- Small and Medium Sized Businesses and Home Network Owners
    - *Small and Medium Sized Businesses:* Often have limited capital budgets and personnel dedicated to networking forcing network devices and managers to “do it all” at a low cost.
    - *Home Network Owners:* Often implement Layer 2 and 3 and security services.

Figure 1 illustrates the organizations that use NOSs and the applications and services that they support.

Figure 1: Who Operates the Network? (Source: In-Stat)



In Table 1, the NOS needs of the organizations outlined above are examined. For service providers and large enterprises, flexibility, integration with network management and back office systems, and an expert interface are key attributes. For SMB's and home users, simplicity, ease of use, and a GUI are critical.

Table 1: What Do Network Operators Need from the NOS? (Source: In-Stat)

Attribute	Service Provider			Enterprise		SMB, Home Network
	Trans-mission	Access	Applications and Managed Services	Access	Applications	
User Interface	*Expert, CLI*	*Expert, CLI*	*Expert, CLI*	*Expert, CLI*	*Expert, CLI*	*Web-based GUI*
Layer_1,_2	*Carrier Ethernet,*	*Carrier Ethernet,*	*Limited*	*Ethernet, Optical,*	*Limited*	*Cable, DSL,*

Functions	*VPN, Optical, ATM, Frame Relay, TCP*	*VPN, Optical, Frame Relay, Cable, DSL, TCP*		*VPN, Frame Relay, Wireless, TCP*		*FTTH, Wireless, TCP*
Layer_3 Functions	*IP Routing, MPLS VPN, QoS, Multicast*	*IP Routing, QoS, Multicast, IPSec VPN, NAC*	*QoS, VoIP, Video, Multicast, Firewall, DDoS Prevention, Intrusion Detection*	*IP Routing, QoS, Multicast, IPSec VPN, NAC*	*QoS, VoIP, Video, Multicast, Firewall, DDoS Prevention, Intrusion Detection*	*IP Routing, QoS, IPSec VPN, Limited NAC*
Application Functions	*Links to Back Office Systems*	*Links to Back Office Systems*	*Firewall, DDoS Prevention, Intrusion Prevention, Managed Services, Web Hosting, Storage, Mail, Voice, Video, Back Office System Management*		*Firewall, DDoS Prevention, Intrusion Prevention, Managed Services, Web Hosting, Storage, Mail, Voice, Video, Network Management Systems*	*Firewall, DDoS Prevention*
Network Management Interface	*SNMP, TMN, XML*	*SNMP, XML*	*SNMP, APIs, XML*	*SNMP, XML*	*SNMP, APIs, XML*	*SNMP, Web-based GUI*
Provisioning and Billing	*CORBA, XML, APIs*	*CORBA, XML, APIs*	*CORBA, XML, APIs*	*XML, APIs*	*XML, APIs*	*Not Applicable*
High Availability	*In Service Software Upgrades, Process*	*In Service Software Upgrades, Process Re-*	*In Service Soft-ware*	*In Service Software Upgrade*	*Not Applicable*	*Not Applicable*

	Restartability	*startability*	*Up-grades, Process Re-startabili ty*	*s*		
Programmabilit y	*XML*	*XML*	*XML*	*XML*	*Not Applicable*	*Not Applicable*

The people that operate networks have different needs often based on the devices and area of the network they manage. Therefore, NOSs must be tailored to meet the requirements of each group and network area. But even by tailoring the NOS to the needs of the network place and operator, it is important to not lose sight of a final critical requirement for organizational NOSs – interoperability.

Keeping the Lines of Communication Open

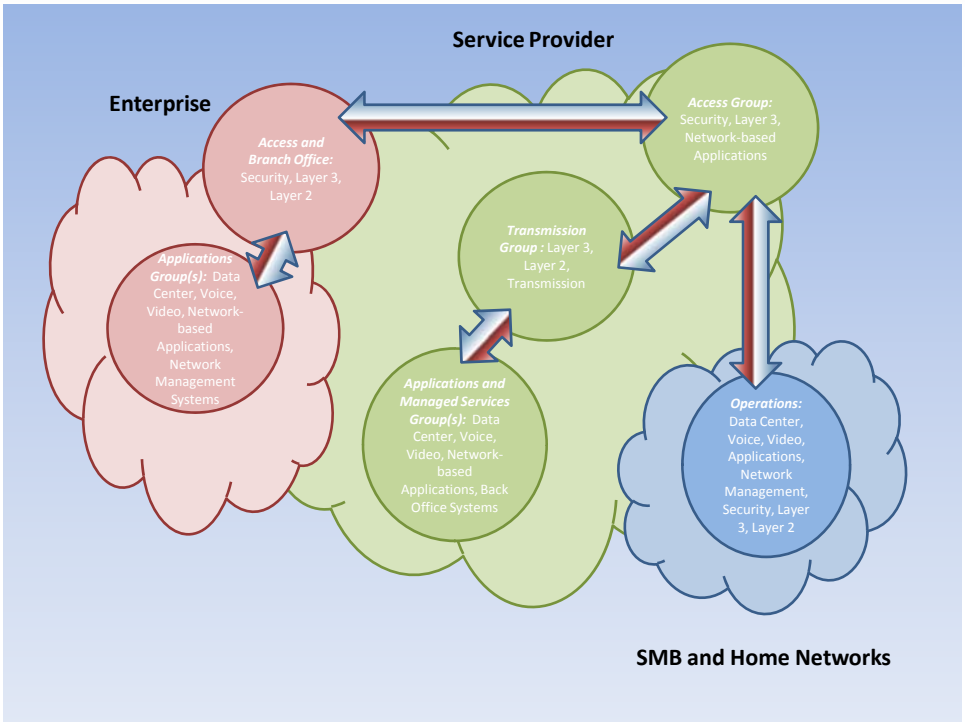
Although service providers, enterprises, SMBs and home businesses may use separate NOSs designed specifically for those environments, organizational NOSs must also provide a common, interoperable language between those groups and their networks. The common language used by each organizational NOS includes several areas where "translations" are not necessary and networks and groups can communicate quickly and easily.

- *Communications protocols: IP and IP routing protocols such as OSPF, RIP, MPLS and others*
- *Management protocols: SNMP*
- *Programming interfaces: APIs, CORBA, XML*
- *Command Line and web-based management interfaces*

Combined, each organizational NOS's common communications and management protocols, programming, command-line interface (CLI) and Web-based management interfaces provide diverse groups with simple, yet powerful ways to seamlessly operate networks across organizational and network boundaries. This enables organizational NOSs to meet the unique needs of each operational group and area in the network without sacrificing the ability to add new functions, services, and capabilities that cross network and organizational boundaries.

Organizational NOSs make it possible for service providers with complex, high capacity networks to provide data, voice, video, and application services to the business owner operating a simple, home-based network. Organizational NOS's keep the lines of communication open while making it possible for organizations to simply and cost-effectively implement, manage, and maintain their networks – and develop and consume innovative, network-based service offerings.

Figure 2: Lines of Communication (Source: In-Stat)



Conclusion: The Organizational NOS

A single NOS might appear to be the most efficient solution for every network device, every place in the network, and every network owner. However, upon closer examination, a NOS that is customized to meet the unique needs of the devices, their position in the network and the people and processes that use them is more efficient and cost-effective.

The organizational NOS is customized to not only help make managing network devices simpler and more efficient, it also helps make operators, managers, business users, and consumers more productive and keeps network costs down by ensuring that software images are not weighed down by extraneous features and functions. Organizational NOSs help keep maintenance costs low, network availability high, and addition of new services and capabilities fast and easy. And, organizational NOSs do this while ensuring that lines of communication between organizations remain open and networks interoperable by "speaking" a common language of industry standard network protocols, management, and programming interfaces.