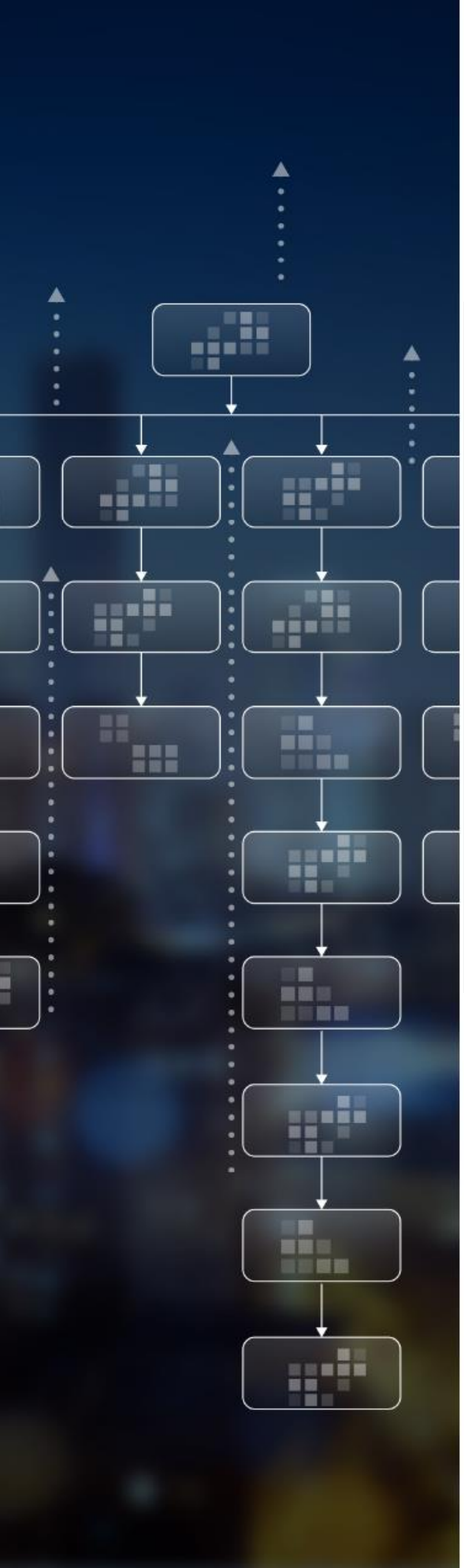


# What is network virtualization? Everything you need to know

**In this guide:**

Network virtualization doesn't require admins to manually configure hardware to instantiate the virtual networks, so teams can spin up logical networks more quickly in response to business requirements. This flexibility enables faster service delivery, operational efficiency and improved control.

These factors and more have spurred the adoption of network virtualization within enterprise and carrier networks. Explore more about the associated benefits and challenges of network virtualization, how it works and the different types.

# What is network virtualization? Everything you need to know

*JENNIFER ENGLISH, SENIOR SITE EDITOR*

Network virtualization is a method of combining the available resources in a network to consolidate multiple physical networks, divide a network into segments or create software networks between VMs.

IT teams can use network virtualization to create multiple isolated virtual networks that share the same underlying physical infrastructure. Teams can add and scale these virtual networks without making any changes to the physical hardware.

Because network virtualization doesn't require admins to manually configure hardware to instantiate the virtual networks, teams can spin up logical networks more quickly in response to business requirements. This flexibility enables faster service delivery, operational efficiency and improved control.

These factors and more have spurred the adoption of network virtualization within enterprise and carrier networks. Explore more about the associated benefits and challenges of network virtualization, how it works and the different types.

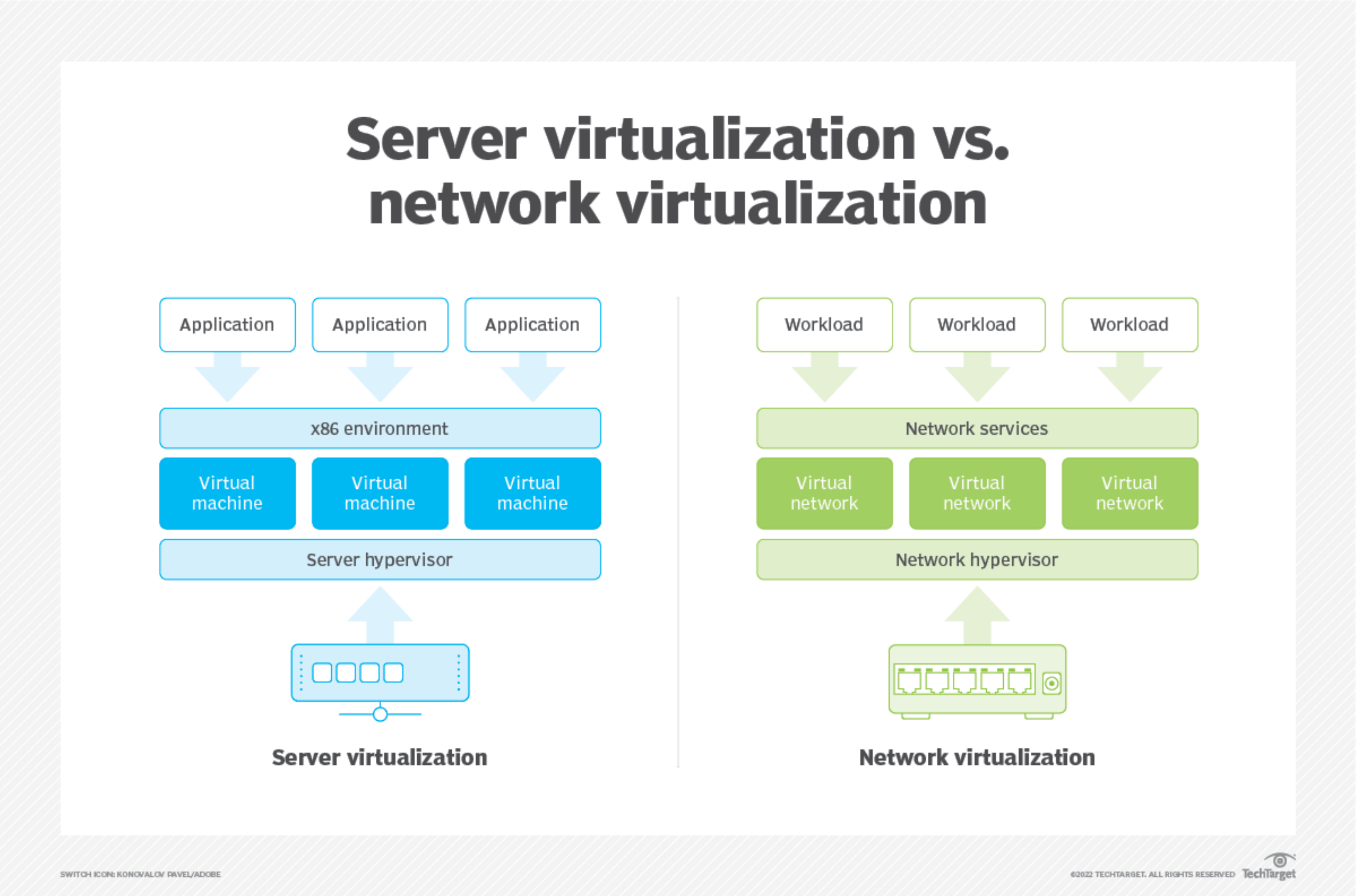
## HOW DOES NETWORK VIRTUALIZATION WORK?

Network virtualization abstracts network services from the physical hardware and infrastructure. To do this, a network hypervisor creates an abstraction layer that hosts and supports different virtual networks, according to Stephen J. Bigelow, senior technology editor at TechTarget.

The abstraction layer provides a simplified representation of the nodes and links making up the virtual networks. The hypervisor is not only responsible for abstraction, but also controls the resources, bandwidth and capacity for each logical network. While the virtual networks share the hypervisor platform, they remain independent of each other and have their own security rules.

Elements within a virtual network -- such as VM workloads -- can communicate with each other and with nodes on a separate virtual network using encapsulated host protocols, virtual switches and virtual routers. The messages do not travel through the physical networking devices, which helps reduce latency.

**In this guide:**



Server virtualization vs. network virtualization

SWITCH ICON: KONOVALOV PAVEL/ADOBE

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

In this guide:

Network administrators can migrate a workload from one host to another in real time, with the associated security policies and networking requirements moving with it. The virtualization platform also applies security policies to new workloads automatically.

Network virtualization typically encompasses the following components:

- a network hypervisor;
- controller software;
- host protocols, such as Virtual Extensible LAN (VXLAN);
- virtual switching and routing; and
- management tools.

## WHY IS NETWORK VIRTUALIZATION IMPORTANT?

Virtualization has been around for years, present as server virtualization, virtual LANs (VLANs) and overlay networks. As enterprises sought more control over their networks, they started applying virtualization principles to their data centers and eventually to the WAN and LAN.

By introducing concepts like abstraction, programmability and microsegmentation, enterprises could scale their networks, add centralized control and apply specific security policies to workloads and traffic types -- all of which help the network deliver applications and services more quickly and, ultimately, meet business initiatives.

Some of the most common network virtualization use cases include performance management and security and risk management, according to John Burke, CTO and analyst at Nemertes Research. For example, network virtualization helps network teams allocate appropriate bandwidth for specific resources, while also specifying and enforcing security policies to meet auditing requirements.

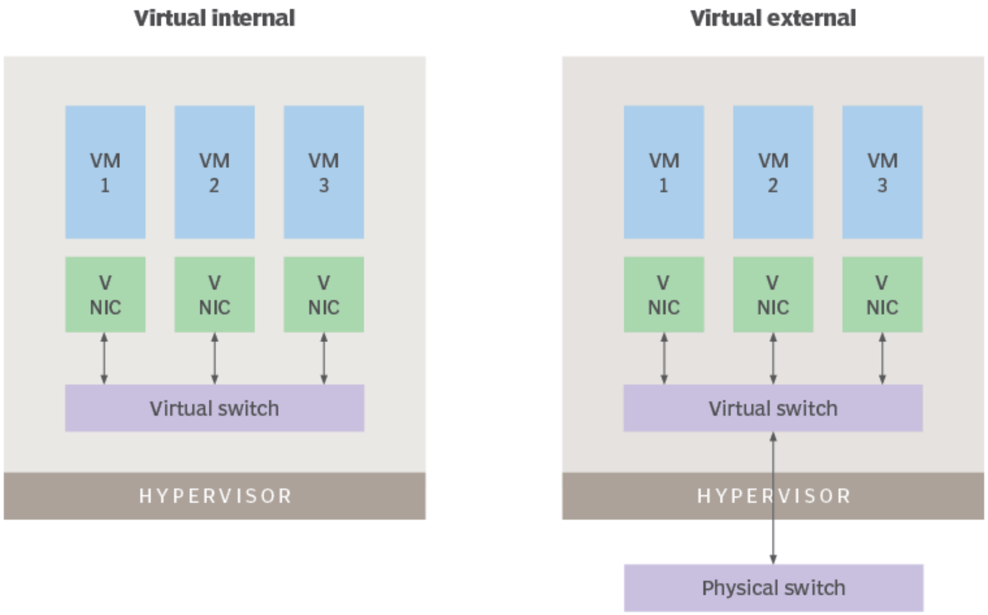
## TYPES OF NETWORK VIRTUALIZATION

Traditionally, virtual networks exist in two forms: external and internal. Both terms refer to their location in relation to the server. External virtualization uses switches, adapters or networks to combine one or more networks into virtual units. Internal virtualization uses network-like functionality in software containers on a single network server, enabling VMs to exchange data on a host without using an external network.

**In this guide:**

## Internal and external virtual networks

A hypervisor can create an internal virtual network that enables communication only to VMs local to the hypervisor or an external virtual network that enables communication to the rest of the network.



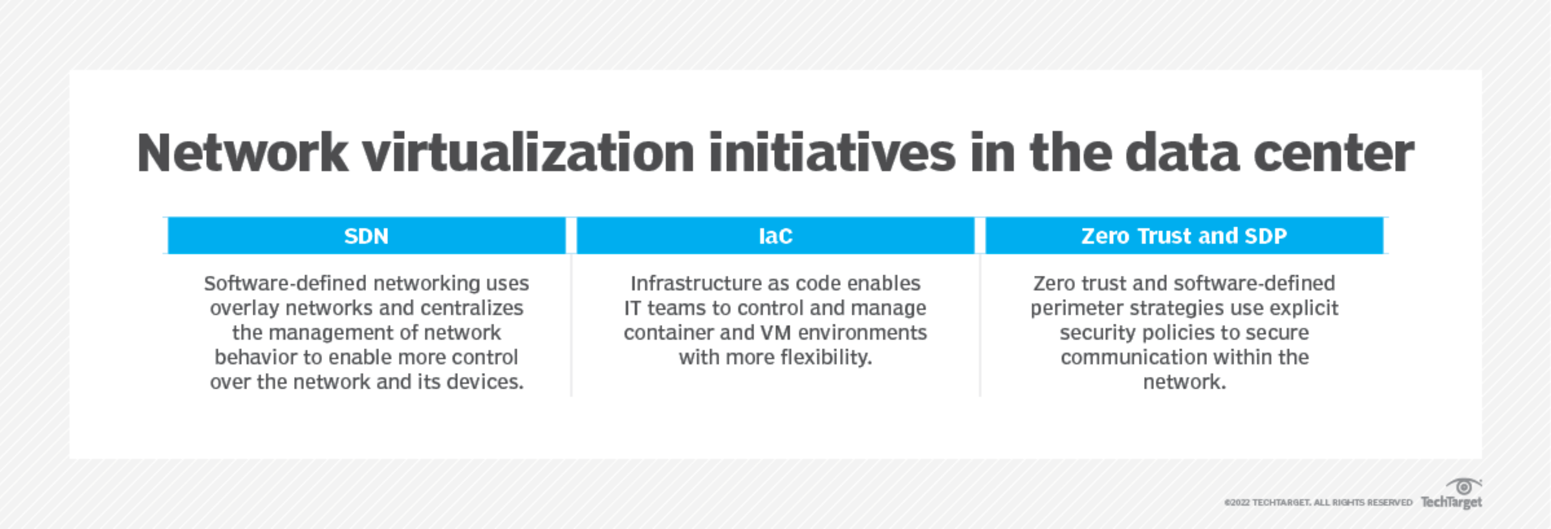
Network virtualization initiatives are typically identified by their uses within different segments of the network, such as the data center, WAN and LAN. Software-defined networking (SDN) drove the evolution of data center network virtualization, while the emergence of software-defined WAN (SD-WAN) revolutionized WAN virtualization. Meanwhile, LAN virtualization has been stimulated by enterprises implementing software-defined LAN (SD-LAN) to improve operations.

These segments are often managed by different teams and focus on different use cases. As networking evolves, however, enterprises may need to consider how to consolidate these individual initiatives to attain an end-to-end network virtualization strategy with embedded zero-trust security.

### NETWORK VIRTUALIZATION IN THE DATA CENTER

Virtual networking has long been prevalent within data centers, in the form of VLANs, VPNs and MPLS. As networks and network threats advanced, enterprises looked for ways to increase network security while also adding more control, according to Burke. SDN was one response to these requirements, as it enables centralized control and supports more policy-driven designs.

Virtualization in the data center has also evolved to include concepts like *infrastructure as code* -- which uses software code instead of manual processes to configure and manage resources -- and zero trust in the form of software-defined perimeter. SDP relies on identity controls to permit access to resources and creates a virtual boundary around the network.



## Network virtualization initiatives in the data center

| SDN | IaC | Zero Trust and SDP |
|---|---|---|
| Software-defined networking uses overlay networks and centralizes the management of network behavior to enable more control over the network and its devices. | Infrastructure as code enables IT teams to control and manage container and VM environments with more flexibility. | Zero trust and software-defined perimeter strategies use explicit security policies to secure communication within the network. |

### NETWORK VIRTUALIZATION IN THE WAN

The WAN was one of the last segments of the network to embrace virtualization, until the rise of SD-WAN revolutionized it. Using SD-WAN, enterprises can abstract the various physical connections within their WANs, as well as allocate bandwidth and capacity more appropriately for application and business needs.

One of the most important elements of WAN virtualization, according to Burke, is the management of the underlay infrastructure. Without properly assessing which providers they're using and where, network teams can quickly fall into the trap of provider sprawl. Other considerations include billing, contract management and troubleshooting.

Zero trust and SDP have also worked their way into WAN virtualization. SD-WAN can use zero-trust concepts to carry only sanctioned traffic and create security partitions that adhere to security policies. An additional factor is how WAN virtualization extends to cloud environments, where enterprises increasingly host resources and workloads.

### NETWORK VIRTUALIZATION IN THE LAN

LANs have commonly used VLANs to segment network traffic and create isolated virtual networks. But, just as in the data center and WAN, the LAN is also experiencing virtualization changes that stem from SDN, according to Burke.

SD-LAN applies the same principles of SDN, specifically for the LAN. While VLANs depend on Ethernet and other Layer 2 protocols, SD-LAN extends virtualization to the entire LAN, so the system can look at access, visibility, users, device identity, IP addresses and time of day -- all of which enable more granular management for applying policies to what is on the LAN, Burke said.

SD-LAN works well with zero-trust strategies, which results in a more comprehensive security design that can keep up with modern advances like IoT. The combination also helps improve LAN operations and monitor network state via automation. But challenges remain, Burke added, such as working with legacy infrastructure, upgrade expenses and staff upskilling.

## NETWORK VIRTUALIZATION SECURITY

Security has become an intrinsic part of any network design. But with different areas of the network typically isolated from each other, it can be difficult for network teams to create -- and enforce -- security policies across the whole network.

Zero trust can unify those network segments and their associated virtualization initiatives, according to Burke. The zero-trust framework relies on user and device authentication throughout the network. If users on a LAN want to access data center resources, they must receive authentication to do so.

A zero-trust environment combined with network virtualization provides the secure connectivity needed for endpoints to converse securely. Virtual networks can be spun up or down to support these interactions, while maintaining the necessary level of traffic segmentation.

An important factor in this process is specifying access policies that detail which devices can talk to each other and where. For example, if a device is permitted to reach a data center resource, the policy must be understood at the WAN and campus levels as well. This is one of the biggest challenges for network teams, as it can be difficult for teams to determine which entities need to converse, Burke said.

An additional challenge is getting teams to work together. Network and security teams will need to discuss security policies, network requirements and infrastructure upgrades.

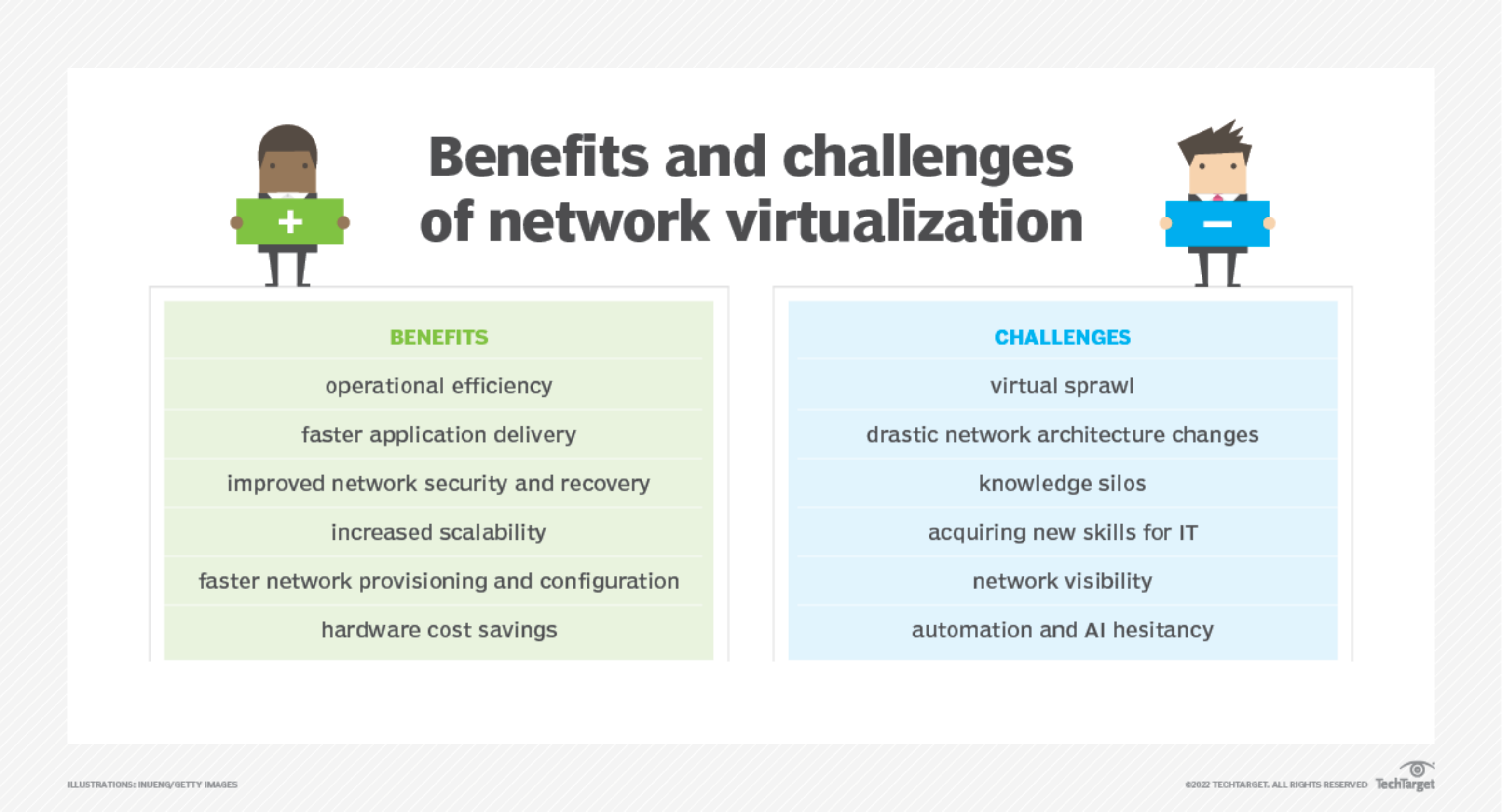
## BENEFITS OF NETWORK VIRTUALIZATION

The benefits of network virtualization vary based on business requirements and where enterprises implement virtualization within their networks, said Andrew Froehlich, president of West Gate Networks and founder of InfraMomentum. For example, virtualization within the data center can enhance security through microsegmentation and support scalability. WAN virtualization, on the other hand, focuses more on improving application performance and policy enforcement.

Overall, common advantages of network virtualization include the following:

- operational efficiency;
- faster application delivery;
- improved network security and disaster recovery;
- faster network provisioning and configuration; and
- hardware cost savings.

In this guide:



Benefits and challenges of network virtualization

| BENEFITS | CHALLENGES |
|---|---|
| operational efficiency | virtual sprawl |
| faster application delivery | drastic network architecture changes |
| improved network security and recovery | knowledge silos |
| increased scalability | acquiring new skills for IT |
| faster network provisioning and configuration | network visibility |
| hardware cost savings | automation and AI hesitancy |

ILLUSTRATIONS: INUENG/GETTY IMAGES

TechTarget

## CHALLENGES OF NETWORK VIRTUALIZATION

While network virtualization helps enterprises improve overall performance, scalability and security, it introduces some challenges as well. One such challenge is virtual sprawl, which frequently occurs as a result of the ease at which network administrators can create virtual networks. Virtual sprawl often results in excess resource consumption and network complexity.

Other challenges with network virtualization include the following cultural and technical obstacles, according to Froehlich:

- **Network architecture changes.** As enterprises migrate from reliance on physical appliances to virtual networking, they need to calculate how the new architecture might affect their resource consumption -- such as CPU and storage -- as well as resilience and security considerations.

- **Knowledge silos.** Traditional IT teams are usually siloed into different departments, such as security, networking and servers. The evolution of enterprise technologies and the spread of virtualization throughout various parts of the network, however, call for increased collaboration among these separate departments.

- **New skills for IT.** Because of traditional IT and network silos, staff can expect a learning curve as they acquire the necessary skills to configure, manage and operate various network virtualization technologies.

- **Network visibility.** As network virtualization adds more logical layers that work together, traditional monitoring tools can lose visibility into the abstracted layers, Froehlich said. Network teams may respond by adopting network visibility tools, further adding to the tool sprawl common among enterprise networks.

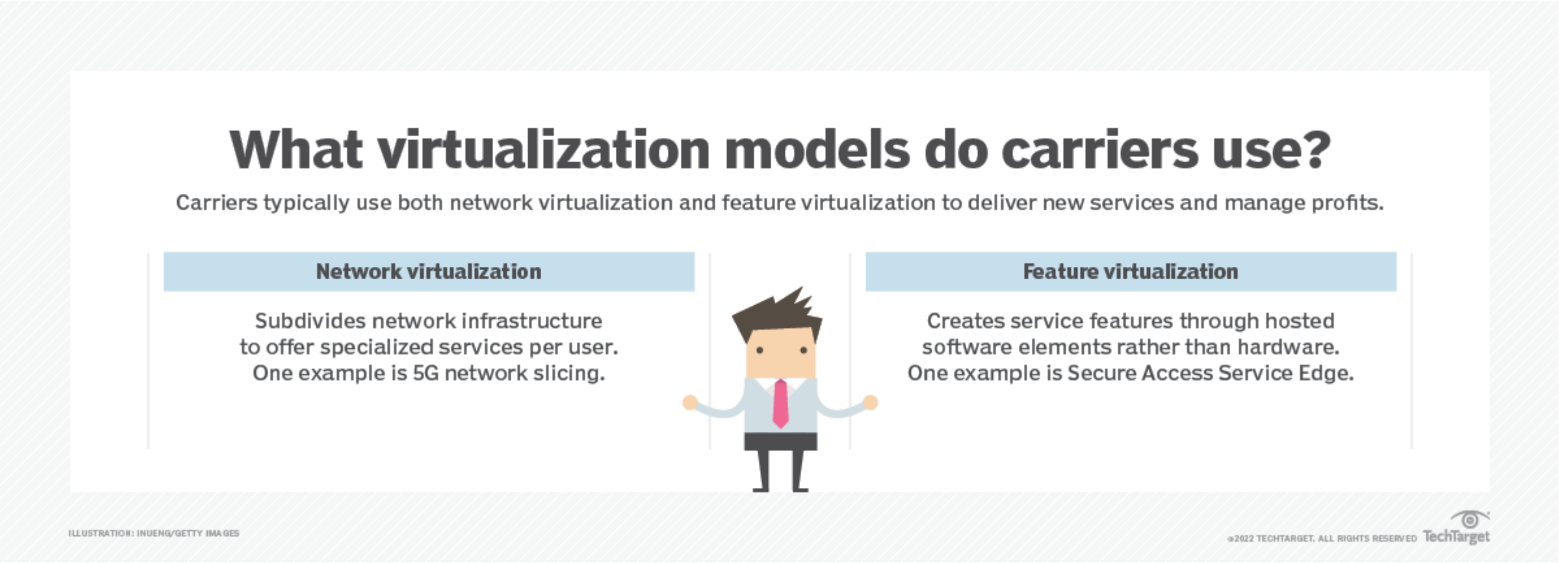
- **Automation and AI.** Network virtualization can also introduce automation and AI tools to the network. These tools improve network management, but they also require new standards and processes that need to be documented, Froehlich said. Network teams must ensure that automation and AI strategies align with each other. Additionally, automation and AI may reveal cultural barriers that need to change.

## EXAMPLES OF NETWORK VIRTUALIZATION

Some of the first forms of network virtualization were VLANs and VPNs. As virtualization use cases extended throughout the network, enterprises eventually adopted SDN principles in their data centers, WANs and LANs.

Meanwhile, carriers use feature virtualization and network virtualization to deliver services efficiently to enterprise customers, according to Tom Nolle, president of CIMI Corp.

**In this guide:**



What virtualization models do carriers use?

Carriers typically use both network virtualization and feature virtualization to deliver new services and manage profits.

**Network virtualization**

Subdivides network infrastructure to offer specialized services per user. One example is 5G network slicing.

**Feature virtualization**

Creates service features through hosted software elements rather than hardware. One example is Secure Access Service Edge.

ILLUSTRATION: INUENG/GETTY IMAGES

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

A carrier strategy for feature virtualization focuses on network functions virtualization (NFV) architecture. NFV removes individual functions -- like load balancing, routing and firewalling -- from dedicated hardware devices and hosts them on virtual appliances or commodity hardware. This capability enables carriers to load specific feature software onto general purpose equipment, delivering the services as virtual network functions (VNFs). If carriers want to expand their portfolios, they can develop new software instead of having to buy specialized hardware and then determine how to use it at scale.

Carriers are also looking at new network virtualization technologies, such as 5G network slicing, cloud computing and edge computing, Nolle said. With network slicing, carriers can divvy up their physical infrastructure into multiple private networks for different customers -- each with its own features and security requirements. Edge computing and cloud computing are efficient and flexible alternatives to on-premises strategies, hosting and delivering the various features and services customers need closer to where they use them.

Network virtualization will continue to be an important element in both enterprise and carrier network designs. Moving forward, network virtualization initiatives will inherently include zero trust, automation, and edge and cloud computing.

▼ **CONTINUED READING**

- 5 network virtualization challenges and how to solve them
- Network virtualization benefits in the LAN, WAN and data center
- How network virtualization works