SOLUTION BRIEF

Network segmentation

Network segmentation is the practice of dividing an enterprise network into smaller subnetworks. It has the effect of isolating users/devices or groups of users/devices from one another. This may be accomplished using several technologies, including hardware-based approaches, software-defined networking (SDN), VLANs, and VXLANs. Because firewalls or SDN approaches can introduce unwanted complexity into the network environment, many IT organizations are turning to VLANs or VXLANs.

VLANs and VXLANs—two approaches to virtualized networks

A VLAN, or virtual local area network, is an approach to network segmentation that separates users and devices into logical network segments without the need for purpose-built hardware. This approach is effective and fairly simple to implement but comes with scalability limitations—only 4,094 VLANs can exist on the network. This limitation is not RUCKUS®-specific but rather part of the IEEE 802.1Q standard. It is also difficult to extend VLANs across geographical areas and physical network segments.

A VXLAN (virtual extensible local area network) is a more advanced alternative to a VLAN, leveraging overlay network architectures and network virtualization to separate users and devices into logical network segments. This approach scales to up to 16 million VXLANs and can span multiple physical network segments and geographical areas. Traditionally this approach has been confined to the data center due to the relative complexity of implementing it. Newer approaches simplify implementation by automating most of the tasks associated with deploying VXLANs as a method of network segmentation. VXLANs are therefore emerging as a practical approach to segmentation across the broader enterprise network.

Benefits

- Improves security by preventing lateral propagation of attacks within the network
- Increases network performance by putting mission-critical devices on their own network
- Delivers a better user experience by giving users a personalized network
- Supports audit and compliance requirements

Use cases—why segment the enterprise network?

Following are several reasons why enterprise organizations use network segmentation:

Security—Organizations can use network segmentation to isolate devices and groups of devices from one another to improve the organization's IT security posture. If they were to rely only on perimeter defenses, once an attack penetrates the perimeter it would be free to move about the network laterally and jeopardize users, devices and data. Organizations can increase security by segmenting the network to prevent an attack from spreading. For example, they can put IoT devices, or groups of IoT devices, on their own virtual network. This separates them from other vulnerable computing resources such as PCs and servers. Since they are effectively on a different network, this approach prevents attacks from propagating.

User experience—Organizations can use network segmentation to provide a better, more personalized user experience. This is often useful in specific verticals that have a single physical network but in which users don't need to interact with one another. An example of this is in the multi-dwelling unit sector—apartments, college residences, military barracks and similar communal living situations. Network segmentation lets IT put each user on their own virtualized personal network. At this level of granularity, a hardware-based approach would be impractical—but VLANs and, with recent technological advances, VXLANs are very practical. Each user can see their own devices, but not those of other users. Users maintain connectivity as they move about the environment just as they would in a non-segmented network. These capabilities create a better user experience for residents. Unlike VLANs, VXLANs also provide the flexibility to extend across geographical areas and physical network segments.

Guest networks—Guest users can be placed on a separate VLAN or VXLAN from other users—one that grants them internet access only rather than the higher level of access granted to employees. This also has performance benefits—the network segment that supports business-critical data traffic can be separated from that associated with non-business activities generated by visitors accessing applications like streaming video.

Performance/QoS—Network segmentation is used to ensure performance (bandwidth) for a group or groups of devices by eliminating congestion/interference.

Audit and compliance—Some enterprises deploy network segmentation to isolate users and devices that are subject to stringent compliance requirements. This way, they can limit the resources required to achieve compliance. For example, they might put all devices subject to PCI-DSS on a separate virtual network. Auditors need audit only those users/devices to sign off on compliance requirements.

RUCKUS products and technologies that enable network segmentation

The RUCKUS product line and its underlying technologies support network segmentation using virtual networks both for organizations that have an end-to-end RUCKUS network and those that run a wired and wireless network from other vendors.

- Cloudpath® Enrollment System works with networks from any standards-based vendor to enable network segmentation using VLANs.
- Cloudpath, SmartZone™ and SmartZone Data Plane combine to enable network segmentation using VXLANs. This removes the scalability limitations of VLANs and allows the virtual network to extend across physical network segments. Recent enhancements to the SmartZone control and management platform also remove the complexity traditionally associated with VXLANs. It does this by automating many of the tasks associated with VXLAN implementation. IT teams can now get the best of both worlds—the flexibility of VXLANs with simple deployment. This is one advantage of choosing RUCKUS products for an organization's networking needs.
- Dynamic PSKs™ (DPSKs) are a CommScope-patented technology that helps enable network segmentation. A DPSK works the same as a conventional Pre-Shared Key (PSK) from an end-user perspective but is much more secure because every user gets a unique key. Each DPSK can be assigned to a different VLAN or VXLAN. While DPSK technology is available in all RUCKUS control and management architectures, Cloudpath offers the most advanced implementation of this technology.

Summary

Network segmentation is the practice of dividing the enterprise network into smaller subnetworks. This can be accomplished by a variety of approaches with different capabilities and different levels of complexity. Many organizations have favored VLANs as an approach to network segmentation because of their simplicity. VXLANs have historically been more complex to implement than VLANs. Newer approaches to VXLAN technology, such as those found in RUCKUS products, simplify VXLAN deployment so that their use is no longer confined to the data center. This is accomplished by automating implementation tasks that formerly had to be performed manually. As a result, VXLANs are a very practical approach to network segmentation for organizations deploying RUCKUS networks.

About Ruckus Networks

Ruckus Networks builds and delivers purpose-driven networks that perform in the demanding environments of the industries we serve. Together with our network of trusted go-to-market partners, we empower our customers to deliver exceptional experiences to the guests, students, residents, citizens and employees who count on them.

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

CO-116379.1-EN (09/22)

RUCKUS®
COMMSCOPE