
ERICSSON
SD-WAN 2.0
Bonding, slicing, and zero trust in a 5G world

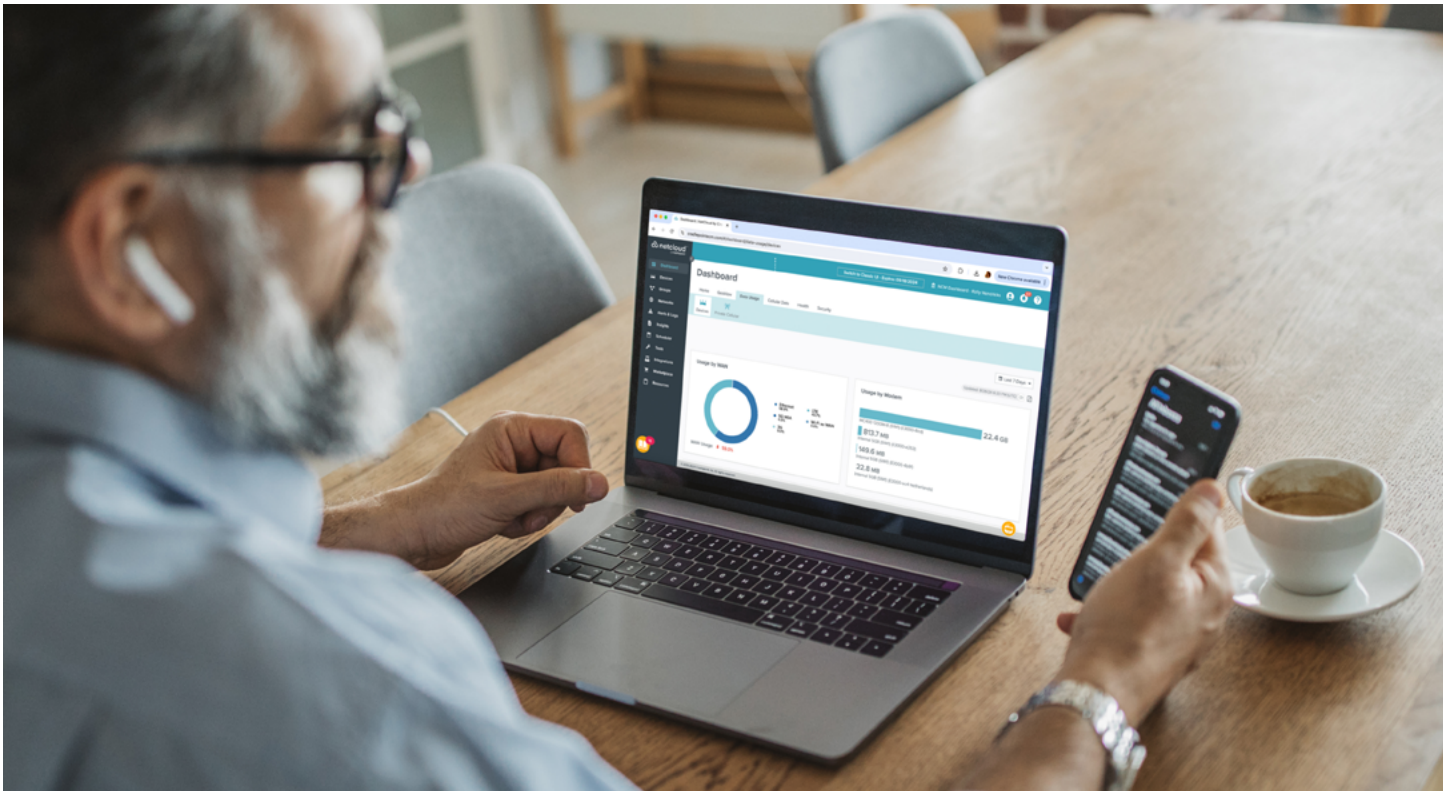
Overview

Table of Contents

How modern SD-WAN solutions complement cellular and hybrid WAN architectures to improve performance and secure networks

5G and LTE have enabled expansive digital transformation and growth across industries. Simultaneously, enterprise businesses struggle to keep up with the explosion of IoT devices and "work from anywhere" employees, which continue to pressure outdated security models and rigid network management tools. To improve network performance, enhance security, and simplify management, many companies have piecemeal solutions that ultimately don't meet the needs of the business.

SD-WAN enables the optimization of applications across a diverse set of WAN links, including wired, cellular, and even satellite. When built on a foundation of zero trust security, this technology can also provide a modern converged networking and security solution for interconnecting distributed sites and vehicles.



The evolution of SD-WAN

Early SD-WAN iterations

As online imagery, video, and VoIP exploded in the late 2010s, networks became increasingly complex, and a need to replace deterministic routing and multiprotocol label switching (MPLS) emerged. SD-WAN technology entered the scene with the understanding that not all applications are the same, not all networks are equal, and the state of the network at any given time might be different. Armed with that knowledge and policies set forth by network administrators, SD-WAN uses multiple WAN links to establish a reliable, secure path for applications while improving quality of experience. It does this using:

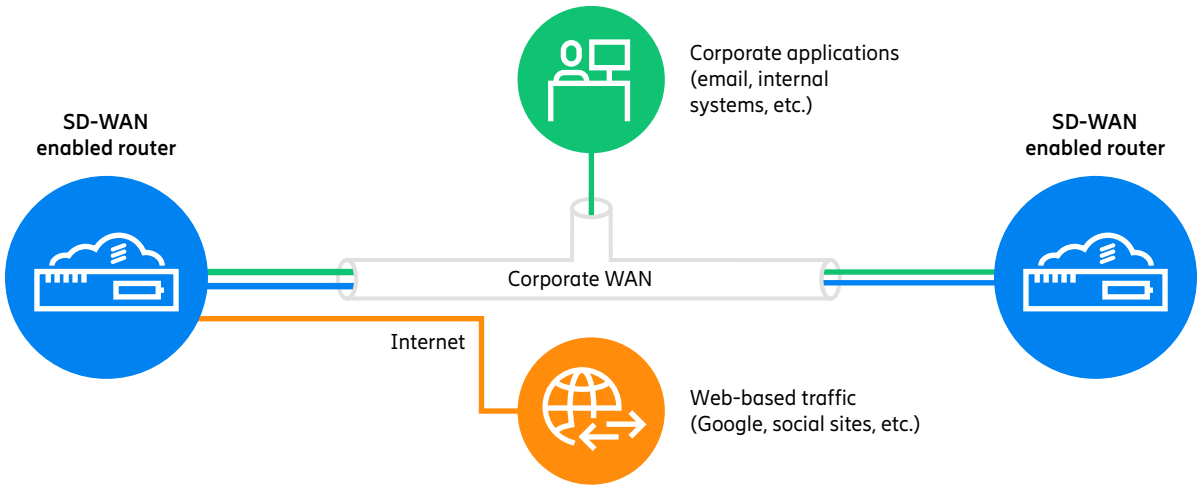
- Traffic steering features that match each application to the appropriate WAN interface based on performance criteria.
- Link bonding and active/active traffic handling to solve for insufficient link capacity.
- Tunnel-based systems to transport packets from one SD-WAN appliance to another.

Early SD-WAN technology also enhanced network performance and allowed sites to connect directly to the cloud rather than backhaul traffic to the data center first — an improvement that helped businesses transition from on-premises applications in the data center to cloud-based applications. However, besides being cumbersome to provision and manage, these traditional solutions relied on perimeter-based security and had limited mechanisms available to accommodate remote users or limit the blast radius of network breaches. Additionally, the first iterations of SD-WAN were built for wired connections only, which was challenging to reconcile with the popularity and growth of cellular in enterprise networking.

SD-WAN 2.0

SD-WAN's abilities to monitor the network for degraded links, prioritize one type of traffic over the other, ensure application quality, compensate for network errors, and make decisions during outages have become critical to business continuity — and they are here to stay. However, like any technology, SD-WAN must adapt to changing business needs and technology landscapes. Modern SD-WAN, or SD-WAN 2.0, balances security and usability while incorporating future-facing features.

- Cellular optimization
- Zero trust foundation
- Thin network edge
- Deployment as a service
- Granular visibility



How 5G and LTE impact SD-WAN

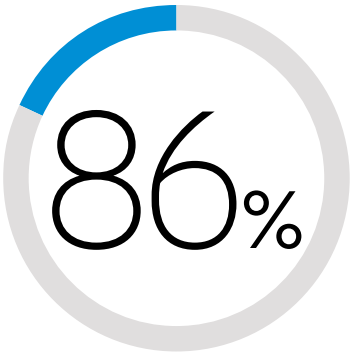
Cellular-optimized SD-WAN

Once considered a failover connection, cellular is now used for primary and secondary WAN connectivity due to its flexibility and time-to-service advantages. A study by EMA found that 86% of enterprise IT organizations use 5G or 4G to connect corporate sites to their WAN. Among them, 50% currently have plans to leverage cellular as their primary connection.

As 5G saturation among enterprise businesses grows, SD-WAN solutions must be optimized to work as efficiently over cellular connections than they do over wired ones. Because the main objectives of today's SD-WAN solutions are to enhance application QoE while improving connection resiliency, the success of modern SD-WAN technology teeters on its ability to support the scale and mobility of 5G networks. With this in mind, SD-WAN must:

- Consider cellular-centric attributes (i.e., bandwidth and data usage) to enable more cost-effective and reliable 5G networking when steering traffic.
- Preserve bandwidth using in-line traffic to calculate WAN performance metrics. This prevents impacts on data plans and eliminates the burden of manual data measurements.
- Ensures visibility and management of the cellular network by incorporating comprehensive cellular insights, including visibility into service providers, signal strength, and router and serving cell tower locations.

These attributes help organizations "cut the cord" and transition to more agile cellular WAN connectivity.



of enterprise IT organizations use 5G or 4G to connect corporate sites. (EMA)

Network slicing

Consider network slicing to better understand how cellular and SD-WAN solutions can work together to improve network performance. This essential capability of 5G standalone (SA) infrastructure can partition radio spectrum into virtual slices based on use cases and application styles. This enables the support of differentiated services across a single 5G connection and facilitates the deterministic transport of business-critical applications across 5G networks that service-level agreements (SLAs) can back. Network slices can be customized and divided based on unique bandwidth, signal strength, jitter, and latency needs.

SD-WAN provides the intelligence to recognize, classify, and create policies to steer the applications to their appropriate network slice. For example, an enterprise may designate Microsoft Teams to a slice with more bandwidth and lower latency if that is the company's primary mode of communication. The assigned SD-WAN policies will then recognize when an authorized user attempts to connect to Teams and steer that traffic to its designated slice. Although 5G SA networks are not yet widely available, this functionality is key for service providers validating how to roll out network slicing to their enterprise customers.

Enhanced Mobile Broadband (eMBB)

Reserved for use cases requiring high throughput and low latency such as mobile video streaming and broadcasting or social networking from user devices in dense areas.

Massive or Critical Machine Type Communications (mMTC or cMTC)

Dedicated to low-cost, long-life IoT devices that send or receive small amounts of data, such as meters, sensors, trackers or wearables.

Ultra-Reliable Low Latency Communications (URLLC)

Built with strict requirements for availability, reliability, and ultra-low latency to support autonomous vehicles, AR/VR, mobile robots, and remotecontrol applications.

Public safety

Intended for government and public safety agencies who need reliable, high- band-width connectivity to support push- to-talk, IoT, and remote monitoring feeds.

The intersection of SD-WAN and zero trust security

Benefits of a zero trust foundation

Traditional SD-WAN uses encryption and site-based VPN technology to secure traffic over multiple WAN connections. This perimeter-based foundation for SD-WAN is inadequate in today's hybrid work environment, where applications and users can reside anywhere, and cybersecurity threats are increasing in frequency and sophistication. When combined with the "never trust; always verify" principles of zero trust security, SD-WAN provides benefits over and above traditional setups.

- Obscures public IP addresses, rendering IP scans ineffective and preventing lateral movement and discovery of critical assets.
- Requires new applications and devices to be defined before they can be seen or accessed on the network.
- Restricts access and policies using a "deny all by default" approach until policies are in place to define access.
- Provides containment of breaches and malware by restricting east west traffic and blocking incoming connections by default.
- Enables continuous inspection of traffic to detect and prevent malicious activity.

Managing expansive networks

Provisioning traditional SD-WAN solutions is cumbersome. Traditional devices are heavy in terms of routing protocols and security features, and require configuring the VPN underlay, VLANs and routing protocols, traffic steering policies, and firewall rules. Organizations that have recently undergone a merger or acquisition may have the additional burden of re-addressing network devices and integrating different routing domains. This complexity can lead to human error during configuration and slow network expansion.

To reduce complexity, an emerging trend simpler SD-WAN appliances, with more of the advanced routing and security features being moved to the cloud. Often referred to as a thin edge, it enables the following key benefits:

- Reduced device-based configuration
- Simplified routing protocol configuration leveraging DNS and name-based routing
- Support for overlapping IP addresses

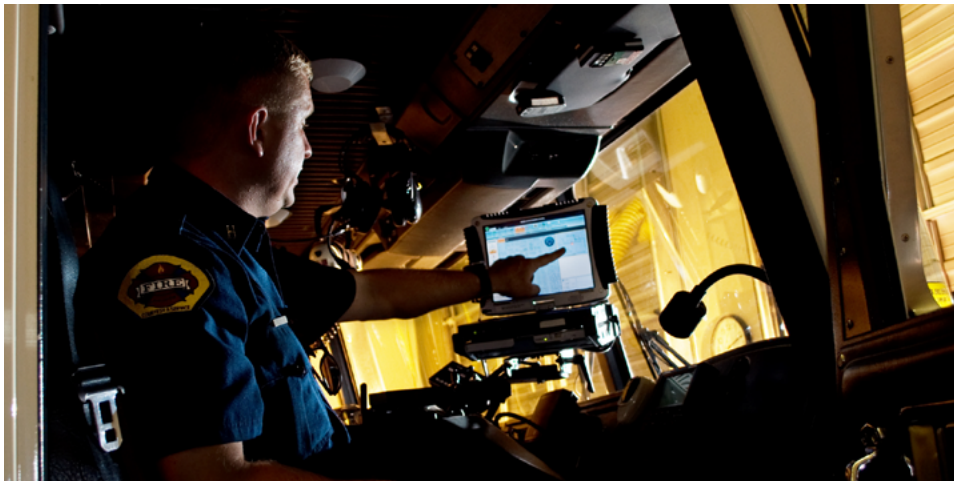
SD-WAN and increased resiliency

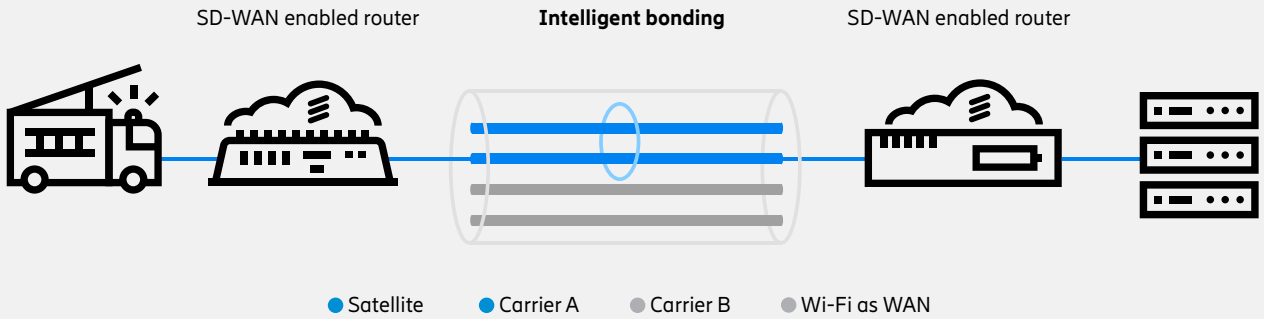
Since its inception, companies have adopted SD-WAN to maximize throughput and optimize application performance. In the past, this was accomplished through techniques such as active/active traffic handling, compression, and more. Today, enterprise networks can harness a zero-loss WAN connection for business-critical applications through intelligent bonding and forward error correction (FEC).

Intelligent bonding

Intelligent bonding combines multiple WAN connections — wired, cellular, satellite, or Wi-Fi-as-WAN — into a single virtual connection to improve network performance, efficiency, and resilience. Intelligent bonding consists of three different features:

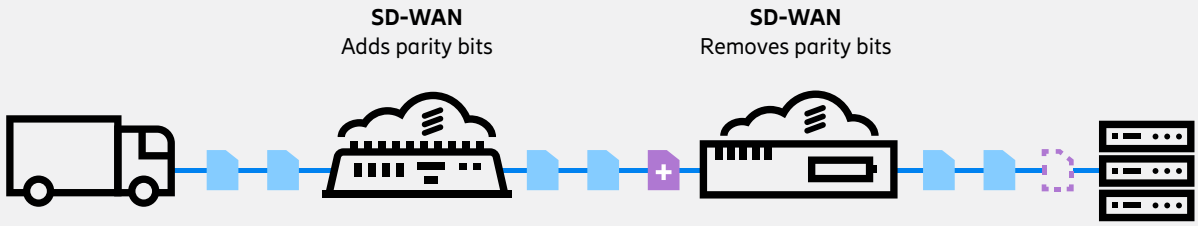
- Flow duplication duplicates mission-critical traffic across two or more WAN connections. Duplication ensures that if there is any congestion on one of the links, there is no packet loss or impact to the application.
- Weighted flow balancing distributes application traffic across diverse WAN links according to user-defined priorities. This feature is most useful when there are WAN connections with different cost profiles (i.e., a mix of metered and unmetered links) and allows for advanced control over traffic for improved cost savings.
- Bandwidth aggregation increases bandwidth and network performance by combining multiple connections into a single, logical link to create a fatter pipe.





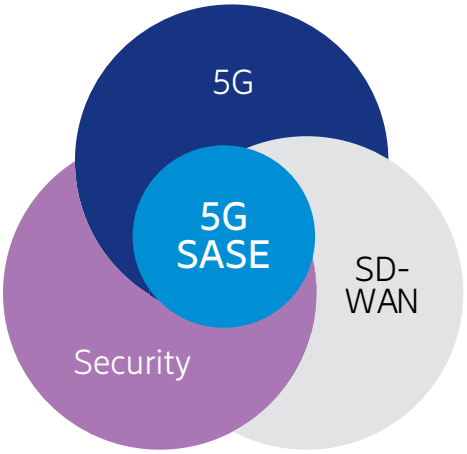
Forward error correction

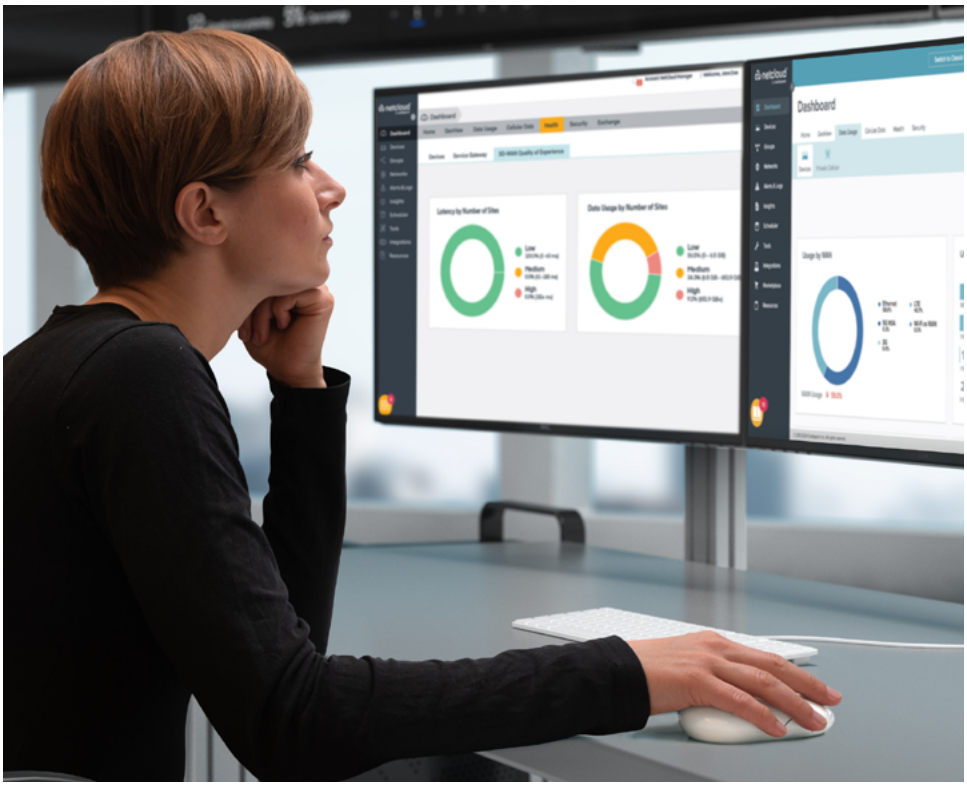
Forward error correction ensures enterprise WANs deliver maximum throughput to applications for optimal performance. To do this, the transmitter sends redundant data bits in the bitstream to safeguard against loss or corruption. The receiver removes the redundant bits to decode the transmission, extract the original data, and correct errors. By adding redundancies, FEC prevents retries when connections are "lossy," allowing enterprises to quickly recover from packet loss in the service provider's network. This feature is essential when using a cellular WAN link where burst packet loss is prevalent.



SD-WAN: Part of a complete SASE solution

SASE eliminates the complexity of managing separate network and security policies by combining them under one policy engine. 5G SASE solutions are replacing standalone SD-WAN to address the challenges of distributed enterprises. Instead of deploying SD-WAN independently, enterprises can implement a secure, scalable SD-WAN solution integrated as a core component within a SASE platform.





A single-stack approach to networking

Multi-vendor SASE solutions are complex and often lead to inconsistencies and potential security gaps. IDC reports that the average cost to a business for a failed SASE implementation is $300K. This is further compounded by the cost of network downtime, which can be upwards of $10K per minute.

An alternative approach for lean IT teams is a full-stack, single-vendor solution. A single, cloud-based policy engine with SASE can govern network traffic management and security. This simplifies policy creation for an improved user experience, reduces the risk of human error, improves performance with only one policy look-up, and ensures consistent enforcement across the entire network.

Accelerating network repairs with AI

Organizations need SD-WAN solutions that provide excellent visibility and management of their enterprise network — including users, applications, and devices. If IT teams can view every flow across the WAN, they can quickly determine where problems exist and how to fix them. Today's SD-WAN management and orchestration platforms leverage the power of AI to do this.

AI insights simplify IT management by providing real-time fault detection and isolation, as well as proposing remediation tactics to dramatically improve the average time to repair. Virtual experts based on large language models can assist administrators with everyday queries about their network and make recommendations to troubleshoot issues and fine-tune performance. AI can also effectively baseline typical WAN traffic patterns so anomalies can be immediately flagged and remediated. These capabilities allow lean IT organizations to deliver enhanced uptime while increasing efficiency.

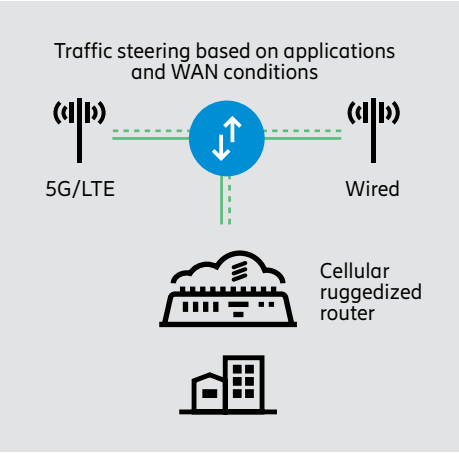
How SD-WAN enhances connectivity for sites and vehicles

One key reason organizations deploy SD-WAN is to provide high availability across diverse WAN connections and service providers. Traditionally, this service has been limited to stationary sites. Today, the benefits of SD-WAN also extend to vehicles, providing resiliency and reliability for applications on the move.

Hybrid WAN for sites

Hybrid WAN combines multiple types of connections, such as wired broadband, cellular, and even satellite, into a single network architecture. It allows organizations to achieve network redundancy, load balancing, and improved network performance by leveraging different types of connections for applications or locations.

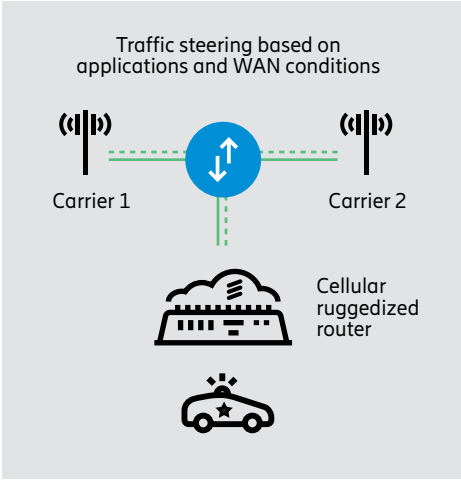
In these hybrid environments, SD-WAN solutions provide the agility, flexibility, and control necessary to optimize WAN performance, ensure reliability, and simplify management. It does so by allowing network administrators to prioritize network traffic to match the needs of the business through increased control over traffic, forward error correction, and intelligent link bonding.



Dual modems for vehicles

Network administrators and fleet managers can address mobility challenges and satisfy vehicle bandwidth demands by installing ruggedized dual-modem routers. These devices facilitate automatic, application-based traffic steering between carriers based on signal strength, latency, jitter, and data usage. If performance degrades beyond the pre-defined thresholds, traffic is dynamically steered to a better-performing connection.

As fleet technologies become more complex, using 5G SD-WAN in vehicles will become more common, particularly when coupled with WAN bonding features such as flow duplication and bandwidth aggregation. Bonding ensures mission-critical traffic gets through and can deliver higher aggregate bandwidth for video uploads.



Enhancing end-user quality of experience is the critical driver behind SD-WAN deployments at the office, on the road, and everywhere in between. Combining zero trust with SD-WAN as part of a 5G SASE solution ensures organizations can switch between links, segregate specific traffic types, or open a new business location effortlessly.

Learn more at cradlepoint.com