THE SOFTWARE DISPERSED NETWORK

A fundamentally new approach
to software-defined networking

dispersive technologies™

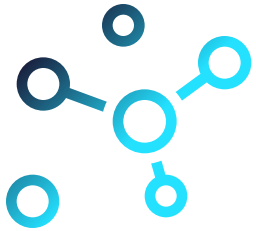
Introduction

NETWORKING IS IN TROUBLE

Traditional approaches to networking are struggling to contain the impact of multiple IT mega-trends.

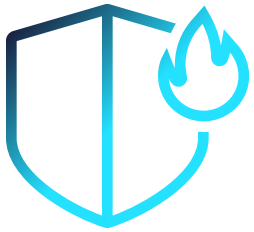
1

The distribution of mobile and Internet of Things devices has made the edge of the network more dynamic than ever, raising all sorts of new security challenges.



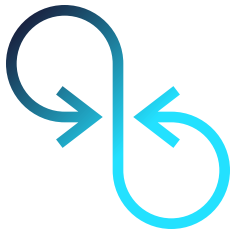
2

The proliferation of cloud applications means crucial systems and data now live outside the firewall.



3

The rise of big data and the consumerization of IT mean bandwidth has never been in more demand – or shorter supply.



Any one of these trends would be enough to change the way networks are managed. But put together, they're threatening even the most basic assumptions about how networks should be run.

To cope with all this change, IT and networking leaders have been forced to turn to a variety of band-aid solutions:

- In some cases they'll turn to solutions that use Border Gateway Protocol (BGP)tricks to control routing by making endpoints issue commands to the network
- In other cases they're using solutions for bandwidth bonding and orchestration
- But more often than not, they're just buying more private circuits or leasing new MPLS links

The trouble is, while these approaches do make life a little easier for network managers in the short term, none of them actually overcome the underlying restrictions of traditional networking. So they can't actually reduce the overall workload or size of investment required to maintain modern networks.

Most important: they don't actually raise network performance to the levels now required by users and consumers.

What's needed is a fundamentally new approach to software-defined networking. One that is built to address the new needs of the 'floating' edge of modern networks and release organizations from the bandwidth constraints that have held them back for so long.

Let's dive in.

Section 01

THE IMPACT OF NEW NETWORKING REALITIES

Before we detail what the ideal solution for modern networks should be, we need to take a closer look at how the collision of all these mega-trends is actually impacting organizations.

In practice, they impact organizations in five crucial ways.

1 User productivity

Across enterprises, just about every job role now relies on some form of connected software to get work done. So network congestion is no longer just a mild annoyance. It has a non-trivial impact on the everyday productivity of most employees. The slower the network, the slower the enterprise.

This issue only gets worse when it comes to remote and mobile users. Mobile devices may have encouraged more users to leave the confines of their desks, but poor connectivity to core enterprise systems still holds them back.

2 Quality of service

Voice and video applications are only becoming more important to collaboration.

But as long as enterprises have to rely on private networks to deliver these applications with the required quality of service, they'll always be forced into a false compromise between cost and quality. Either you pay more to keep your users happy or you pay less and suffer frequent end-user complaints. This compromise is unnecessary.

3 IT agility

Maintaining and managing networking hardware for multiple MPLS and broadband connections takes up enough time and effort as it is.

So it doesn't actually help when IT organizations get saddled with the added complexity of hard-coding and managing the policy-based routing mechanisms of most software-defined networking solutions.

Moreover, because of the lock-in caused by different vendors' proprietary hardware, most IT teams don't have the flexibility they need to upgrade their networks and give users the performance they need.

4 Security

The growth of cloud and mobile endpoints has dramatically increased the size of the potential attack surface available to hackers. The trouble is, VPNs remain a single point of failure for most organizations, becoming the easiest point of entry for hackers who want to gain access to the whole network and all its extended services. And if there's one thing hackers have proven, it's that current approaches to encryption don't stop them.

As a result, most security solutions today are bolted on to applications in a way that compromises user convenience. While too few security protocols actually protect the network itself. Security cannot be an afterthought.

5 Costs

Traditional approaches to networking directly cost organizations in two different ways. First, you have to pay the operating expenses needed to employ a staff that can manage and maintain multiple network connections.

Second, you have to make the capital expenditure necessary to buy new hardware for new private networks and segments.

As long as it costs you so much to provision more connectivity and deliver a higher quality of service, you'll always be forced into false compromises.

Section 02

WHY TRADITIONAL NETWORKING STRUGGLES

Standard approaches to networking all have one crucial flaw in common: they all use a single path for data transfers.

This causes a number of issues:

- Transfers are restricted to the path they're on, even if it's degraded, so packet loss is inevitable
- If the path is congested – as it often is – the data can't be re-routed mid-transfer
- Latency sensitive applications like voice and video that are crucial to enterprise communication and collaboration inevitably suffer
- Hackers only need to beat a single layer of encryption to gain access to data

Additionally, traditional networking approaches are almost always reliant on expensive hardware and rigid logic that takes ages to customize and deploy.

This slows IT teams down and restricts their ability to make the most of all their available bandwidth.

The rise of SD-WAN solutions has looked like a blessing for network administrators. They make networks easier to deploy, easier to manage and rely on less equipment so they're actually cheaper than the previous paradigm of hardware-centric networking.

But while SD-WAN solutions make basic bandwidth bonding and orchestration capabilities a little easier, they don't actually do anything innovative or new. Instead, they simply repackage the technologies you already have.

Which means they still have to comply with the restrictions and compromises of the underlying architectures they work with.

- They still rely on a single path for data transfers. So all the issues stemming from this approach – packet loss, congestion, vulnerability to threats – don't go away
- They don't actually address any of the issues faced by mobile and remote users
- They do provide interfaces and tools that make policy-based routing easier, but creating and managing all those policies is still a burden on IT
- Their policy-based routing mechanisms are still constrained by the bandwidth inefficiencies of existing networking connections
- They're too rigid and inflexible to adapt to the changing conditions of multiple WAN connections
- They still rely on private networks for low-latency applications like voice and video – so you've still got to pay more if you want faster speeds

Put simply: SD-WAN solutions get a lot right. But they don't actually solve the bandwidth inefficiencies or underlying architectural issues that make networking hard.

So they don't sustainably improve the speed, security or reliability of your network or give your end users the experience and performance they need.

Close, but no cigar.

Why SD-WAN comes close but not close enough

Software-defined wide area networks (SD-WAN) are a specific application of software-defined networking (SDN) technology applied to WAN connections, which are used to connect enterprise networks over large geographic distances.

They automate the ongoing configuration of WAN edge routers, running traffic over a hybrid of public broadband, private MPLS links, and other WAN links such as LTE.

SDX central

Section 03

THE SOFTWARE DISPERSED NETWORK

When TCP was invented, memory was expensive. Now that it's not, you can use software to remove all the compromises of traditional networking approaches, while still running over the public Internet.

Software Dispersed Networking is a fundamentally new approach to networking. It uses software to move control and intelligence to the edges of your network.

Instead of relying on a single path for data transfers it relies on multiple. And instead of being restricted by the bandwidth inefficiencies of your underlying connections, it maximizes utilization of all your available bandwidth.

Here's how it works:

1. The software aggregates all your available IP connections (broadband, cellular, WiFi, and satellite).
2. This creates a single, virtual pipe that makes your combined bandwidth available to every session.
3. Then, the software splits the packet data into several, independent packet streams that can be transferred in parallel, down multiple, individually encrypted paths.
4. The software dynamically rolls these independent paths based on:

- Bandwidth availability (across all your IP connections)
- Line quality
- Measured time delay on each path
- Any other factors that are important to you

5. Finally, it reassembles the data at the receiving device.

Why bandwidth aggregation is smarter than bandwidth bonding

WAN optimization and SD-WAN solutions use link bonding to leverage multiple physical connections. They also use policy-based routing to steer high-priority traffic across high bandwidth links and low-priority traffic over slower links.

The trouble is, policy-based routing forces your network administrators to program routing behaviors based on complicated provisioning rules for every single service on the network. So neither bandwidth utilization nor performance is actually optimized.

With dispersed, virtualized networks, all your combined bandwidth is made available to every session. Instead of policy-based routing, it dynamically optimizes path selection for you. All you need is a simple web interface to easily manage the network from one central location.

Because of this fundamentally different approach, some important things become possible for the first time:

Order-of-magnitude improvements in throughput
By sending packet data down multiple paths in parallel, data transfer speeds improve by a factor of 10 – while running over the public Internet.

Maximum utilization of bandwidth
By treating all your available physical network connections as one logical pipe, you efficiently leverage all your available bandwidth efficiently – without changing your network configuration.

Security for data-in-motion
By using a different encryption key for every independent path used in a data transfer, it exponentially increases the amount of security available to all network traffic.

Support mobile endpoints
By using a distribution of cloud-hosted endpoints called deflects to influence routing, it ensures that your mobile and remote users get an 'in-office' experience wherever they are.

Dynamic path selection
By monitoring the performance of any given path in real time, it can spot potential packet loss and then dynamically select a better path to complete the transfer before it reaches the application.

Zero-touch provisioning
By managing all your network connections centrally, it gives you the ability to easily create new segments and provision new connections and services in seconds.

Security for the network layer
Since both sides of any given communication call out to an isolated deflect (rather than receiving connections at the end points) it moves the attack surface away from where work happens. More important: it uses a cloud-hosted 'soft switch' to authenticate and authorize both devices and users before granting them access.

What's a 'deflect'?

To create dispersed, virtualized networks, we use a global distribution of separate, cloud-hosted appliances to influence routing decisions and move the attack surface away from where your users work. We call these appliances 'deflects'.

Section 04

THE IMPACT OF SOFTWARE DISPERSED NETWORKING

Now that you've seen how this approach removes the restrictions and compromises of traditional approaches to networking, let's take a look at how that impacts organizations.

1 User productivity

With order-of-magnitude improvements in throughput, the applications your users rely on work faster. With applications now protected against packet loss, your users get the benefits of more resilient transfers.

Your mobile and remote users get an in-office experience when they connect to the core enterprise systems they need to work.

2 Quality of service

Voice and video applications are only Low-latency applications for voice and video can be delivered without loss or the extra costs of separate private networks. Which means your users can use rely on existing applications for voice and video like telepresence without hassle.

But it also means you can power new applications like HD remote monitoring in a way you couldn't do it before – over public broadband.

3 IT agility

With dynamic routing based on the rulesyou care about, you don't need to manage the complexity of policy-based routing.

Even better, since you can manage your combined bandwidth like it's software, you can rapidly provision new services whenever you need to – without having to manage or maintain any hardware.

4 Security

As an approach, Software Dispersed Networking mitigates against DoS, DDoS and man-in-the-middle attacks.

It also multiplies the amount of authentication and encryption used to protect your users, your data and your network – without compromising the convenience of any user's experience.

5 Costs

It lowers your operational expenses by simplifying network deployment, making network management zero-touch and maximizing your bandwidth utilization.

At the same time, it lowers your capital expenditure by giving you the freedom to use off-the-shelf commodity hardware instead of proprietary devices. You can even deploy it as virtual machine.

Use cases:

High-definition video monitoring over a low-bandwidth connection

An Oil and Gas company set up high-definition cameras to monitor tampering and protect its mission-critical 'block valves' against vandalism. But bandwidth constraints in the valves' remote locations meant the team had to choose between a slow VPN and unsecured lines to their Texas office.

By switching to dispersed, virtualized networks, they could transmit the high-definition video efficiently and securely over the low-bandwidth connection.

Smarter disaster recovery

A major computer consulting and service hosting company was concerned about its disaster recovery capabilities. Specifically, they worried about their ability to push client data to their cloud fast enough.

By turning to dispersed, virtualized networks, they were able to improve their throughput in two crucial ways. First, they could run multiple transfers of large amounts of data without any latency or packet loss. And second, they were able to handle big data transfers throughout the day without bogging down their normal traffic.

Who else benefits from Software Dispersed Networking?

Different organizations use their networks in different ways. But invariably, dispersed, virtualized networks give them the ability to do things they previously couldn't.

Content delivery networks can use it to stand up Points of Presence in faster, more agile ways. **Carriers** can use it to extend their global footprint faster than ever with cloud-based 'deflects'. **Banks** can use it to centralize network management, aggregate all their available bandwidth and even use 4G LTE as backup.

Conclusion

THE FUTURE OF NETWORKING IS DISPERSED

The collision of the cloud, mobile, the Internet of Things and the consumerization of IT have had a seismic impact on the way companies get work done.

But as long as enterprises have to rely on old-school approaches to networking (or new software-defined approaches that rely on old architectures), they'll continue to be victims to the restrictions and compromises of old.

Software Dispersed Networking is a fundamentally new approach at a time when a fundamentally new way is needed most.

- It empowers all users – remote, mobile or in-office – to use the applications and big data they need
- It makes IT's life easier, delivering more control, flexibility and security than private networks
- And it lowers the costs of networking while simultaneously improving the speed, security and reliability of the network

This is big

It's been clear for some time now that the future of networking is software. But it's only with Software Dispersed Networking that we can finally see the full potential of virtualized networking.

Which begs the question: what would you do with total control over all your available bandwidth?

We're Dispersive™

And we believe enterprises need a faster, more secure and more reliable approach to networking. It's why we invented Dispersive™ Virtualized Networks. So if you're looking for an entirely new way to manage your network, we should talk.

Let's talk.
1-844-403-5850
www.dispersivetechnologies.com