COMPARISON SHEET
PROS AND CONS OF MPLS

Frontier
BUSINESS

UNDERSTANDING THE CONCEPTS:

Multiprotocol Label Switching (MPLS) is a way of transferring data between two or more locations. It was designed to speed up and shape traffic across enterprise-wide networks. MPLS isn't a type of internet connection, but instead can be described as a 'technique' that prioritizes your data packets based on their class of service—like your IP phone, video or Skype data. SD-WAN, on the other hand, is software-defined networking in a WAN (Wide Area Network) environment. It's a technology that sits on top of virtually any kind of link and enables you to prioritize network traffic. It simplifies the management and operation of your WAN connection by binding multiple pathways together to provide a single, logical, virtualized route that can adapt to network conditions and automatically choose the best path.

Both MPLS and SD-WAN enable you to prioritize network traffic.

Which option works best for you?

MPLS	
Pros	Cons
• You can prioritize the most important services for your business. Never have a voice call interrupted or let another app monopolize the network again. • MPLS is reliable, predictable and manageable—everything you want in a network.	• It's expensive. And because it's so expensive, most enterprises haven't been able to implement or scale it across their organization. • MPLS networks don't offer built-in data protection. You need to purchase extra hardware and software.

SD-WAN	
Pros	Cons
• SD-WAN is flexible, allowing you to scale up or down with demand. • It's reliable, cost effective AND secure. • Unlike MPLS, SD-WAN comes with no bandwidth penalties, leaving you with 100% of usable bandwidth and enabling you to upgrade easily by adding new links, with no changes to the network overall.	• Sadly, nobody's perfect. SD-WAN typically sits on top of an internet link (even though the underlying technology is transport-independent), so it might not be the best possible solution in every scenario. But it's very often the best option!

UNDERSTANDING THE CONCEPTS:

A Virtual Private Network (VPN) lets users send and receive data across a shared or public network, as if their computing devices were directly connected to that private network. IP VPN goes one step further, combining a VPN with MPLS technology, prioritizing internet traffic and avoiding public gateways to increase security. Because of this, it is considered 'layer 2'.

IP VPN	
Pros	Cons
• It's cheap! • You can back up your data and even access your critical sites via another internet circuit when the primary connection fails. • Easily upgrade your features by just introducing a new router operating system. Easy as 1, 2, 3. • It's adaptable to your needs. WAN engineers have total control over the VPN tunnel created between sites.	• There's no quality of service associated with IP VPN (this means you cannot prioritize traffic). • Higher packet loss and latency, which means downgraded performance when using interactive applications, videos and voice connections over long geographic distances. • Your data is more vulnerable when using IP VPN because you are exposed to the internet. This can lead to unforeseen costs when looking to improve it. • A direct internet connection comes with its own risks, like exposure to potentially damaging denial of service (DoS) attacks.

SD-WAN	
Pros	Cons
• SD-WAN keeps your network's performance consistently high, allowing it to deal with each and every workload. • Networks can be configured easily through a centralized portal, making it flexible to you and your businesses' needs.	• It may come with a higher upfront price point. However, there are no hidden costs, unlike the additional security associated with IP VPN.

Although VPN has been around for decades, SD-WAN should be thought of as the next major evolutionary step for the technology. Say 'hello' to the Future of Networking!

Frontier
BUSINESS

UNDERSTANDING THE CONCEPTS:

Metro Ethernet Multi-Site Deployment combines the power of ethernet with a fiber line, across a Wide Area Network (WAN) to provide low-cost, scalable and secure bandwidth. Metro Ethernet Multi-Site Deployment is already widely available across businesses and homes and lets you transfer file data, access the internet and store your data off site.

METRO ETHERNET MULTI-SITE DEPLOYMENTS	
Pros	Cons
• It's cheap, scalable AND secure. • Ethernet is everywhere—across the LAN and WAN, making it pretty easy to connect. • It has its own new technology, replicating the benefits of other services like MPLS to give you the best of both worlds.	• Even though it's relatively secure, prevention of IP address theft, MAC address limiting, DHCP snooping and DDOS can be difficult. • Quality of service can be somewhat limited. • Site deployments can be complicated.

SD-WAN	
Pros	Cons
• It's EVEN cheaper! • It performs even better! • SD-WAN is able to pick the best path for your data out of many, including the ethernet fiber. Ethernet is limited to just your fiber connection. More is better!	• SD-WAN doesn't fix every problem. If a given cloud application is not performing well over the internet, the user experience will suffer as well.