TELECOM PROFESSIONALS

"YOUR LINK TO QUALITY COMMUNICATION"

The Global Connectivity Challenge

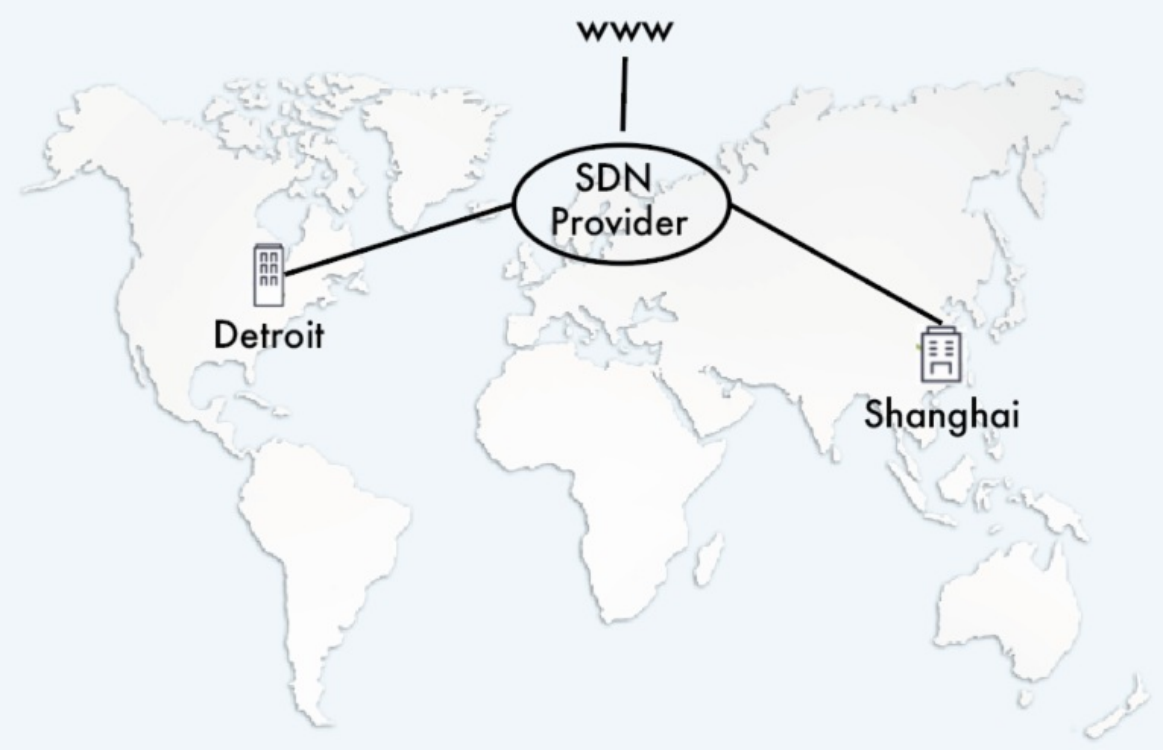
How to Connect China and Other Bandwidth Challenged Countries to the US

Whether you're a manufacturing, engineering, or retail firm, global enterprises are aggressively expanding worldwide. International locations need reliable and optimized connectivity to global resources. Typical business requirements include high quality WAN connectivity to the datacenter for voice, ERP and remote desktop applications, and optimized internet access to cloud resources such as Office 365, Amazon Web Services, and Microsoft Azure.

If you are used to the reliable and affordable connectivity of North America and Western Europe, extending your network globally could prove challenging. Here is what you need to consider. The connectivity challenge in developing countries is twofold: the quality of last mile infrastructure to remote locations and the high latency of global connectivity.

Internet last mile connections are often less reliable due to poor physical infrastructure or an oversubscribed connection shared by many businesses (such as with cable or ADSL). The situation is improving with countries worldwide upgrading their infrastructure.

When delivering applications across long distances, latency and packet loss will determine application performance. This established fact becomes critical for worldwide connectivity. The long distance and poor internet peering in more remote locations throughout the rest of the world exacerbate latency. In addition, due to regulatory oversight, traffic leaving countries such as China, must be inspected by a central firewall (also known as the "Great Firewall of China"). The firewall enforces Chinese regulations regarding the use of internet and cloud services. As a result, global internet-based connectivity from China exhibits high packet loss and high latency.



What are the options for business-grade connectivity outside of the US?

Internet VPNs Are Not Always an Option

Recent changes in the regulatory environment in China tightened the controls around the use of encrypted links (i.e, site-to-site VPN tunnels) crossing the central firewall. **SD-WAN edge solutions** that rely on public internet VPNs to establish datacenter or cloud connectivity, can be disrupted or perform poorly at any given time.

Private Lines

MPLS private lines are an expensive option, which can work well for WAN connectivity, assuming the MPLS provider can effectively peer with the enterprise data center MPLS provider. This option is sub-optimal for access to cloud resources due to the need to backhaul the traffic to a secure internet exit.

Software-Defined Backbone

Software-Defined Backbone providers, such as Telstra, use private links via authorized carriers to exit traffic from China to Hong Kong. The strategy is to route the traffic globally over a SLA-backed backbone applying multiple traffic acceleration and packet loss mitigation techniques. WAN traffic is specifically optimized to reach the Point of Presence (PoP) closest to the datacenter, and cloud traffic egress near the cloud instances used by the enterprise.

We Want to Hear From You!

If you are the 10th person to respond to this Newsletter or like our Facebook page, we will send you a pair of Detroit Lions tickets to the game of your choice. Good luck!

DETROIT LIONS

1-855-567-5000 www.telecomprofessionals.us

FOLLOW US