A Comprehensive

# Computer Network Strategy Guide for Small & Medium Businesses

FROM THE MANAGED SERVICES EXPERTS AT TPX

## Executive Summary

Every organization, including small and medium businesses (SMBs), depends on a network that connects computing devices that are used to communicate and collaborate with team members, customers, partners, suppliers and increasingly other machines. Optimizing that network for your business requires a knowledgeable IT staff or the guidance of networking experts from a proven managed services provider (MSP).

**In this Comprehensive Computer Network Strategy Guide for SMBs, we'll cover what your business can do to improve your overall network strategy.**

## Key Takeaways

### LANs & WANs Have Evolved

Today's local and wide area networks have evolved to support distributed, mobile, cloud-first organizations.

### A 'Good' Network Today is Always On, Fast & Secure

Your network needs to stay up, operate fast, have software and hardware redundancy and security.

### Networking & Cybersecurity are Blending

The lines between network and cybersecurity are blending as functionality merges in edge solutions.

### An Ideal Network is Built for the Future

Your network needs to be designed to adapt to your business needs tomorrow as well as today.

### An MSP Can Fill the Gaps

Leaning on a well-versed MSP like TPx can help your business improve network performance.

# Table of Contents

PART 1

# What is a Network?

Every organization uses networks to communicate and collaborate with key stakeholders — employees, customers, partners, suppliers and, increasingly, other machines.

Networks can be segmented into two major categories:

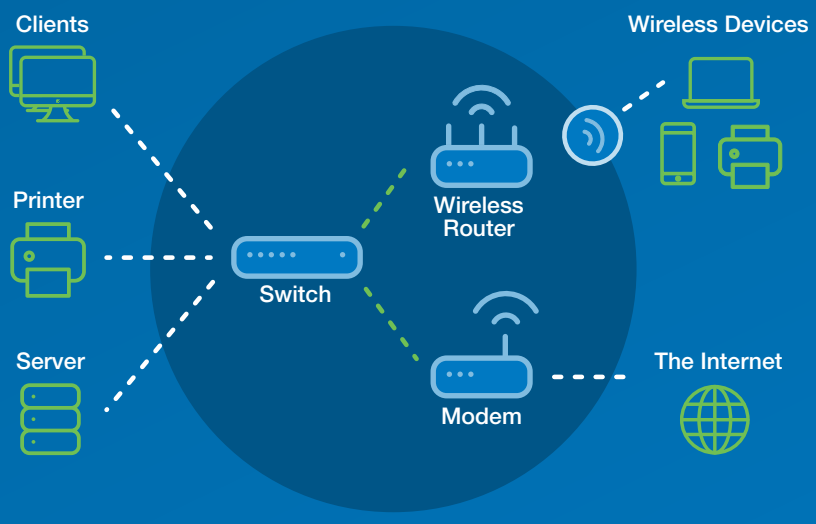
- **Local Area Networks (LANs)**
- **Wide Area Networks (WANs)**

Before we explain the differences, let's review what defines a network in general.

A network is a group of servers, mainframes, network devices and endpoints (like computers, laptops, tablets or smartphones) that are connected to allow sharing of data between all components of the network.

Components typically comprising a network include:

- Servers
- Mainframes
- Firewalls
- Switches
- Hubs
- Modems
- Routers
- Bridges
- Repeaters
- Consoles
- Endpoints (desktop computers, laptops, tablets, smartphones, webcams, etc.)



PART 2

# What is a Local Area Network?

A local area network, or LAN, is a computer network that connects devices in a limited area, such as a building, office, home and even campuses of adjacent buildings. In contrast, a wide area network (WAN) covers larger geographic areas (See Part 3 for information on WANs).

A LAN comprises switches, routers and other components that enable devices to connect to internal servers, web servers and even other LANs via WANs. The advantage of a LAN is that it enables your team to share files, printers, one internet connection and more.

Architecturally, a LAN can be set up in two ways:

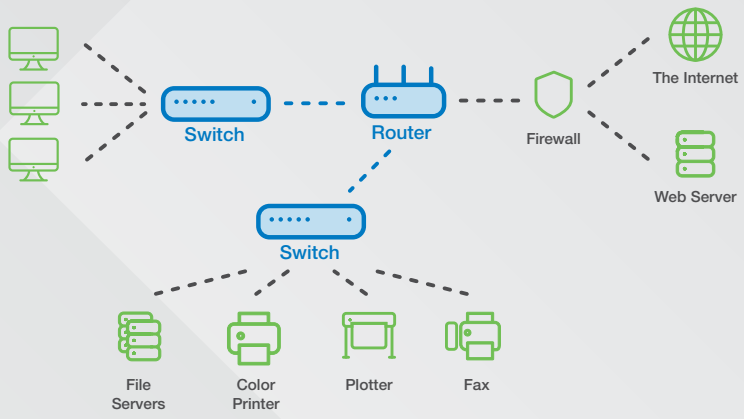
- **A peer-to-peer LAN** directly connects two devices.
- **A client-server LAN** is typical in business environments and includes multiple endpoints and servers connected to a LAN switch that directs communication among devices.

Additionally, a LAN can be based on hard-wired Ethernet connections or wireless Wi-Fi connections, which we'll discuss in more detail on the next page.

# What is a Wired Local Area Network?

A wired LAN includes a switch that uses Ethernet cabling to connect to servers, workstations and other endpoints to the corporate network.

**Example of a Wired Local Area Network**

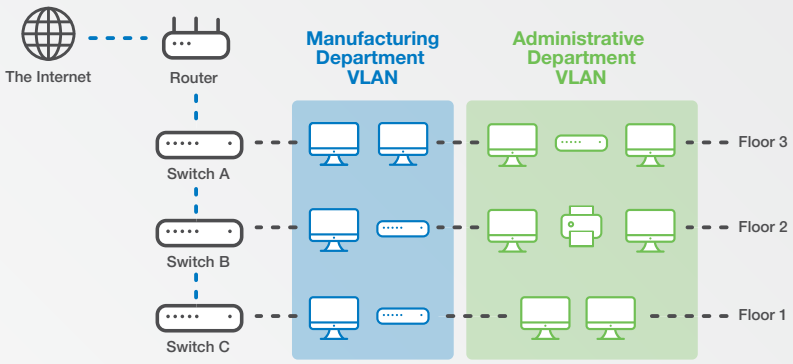



# What is a Virtual Local Area Network?

Smaller organizations with only a few devices can usually get by with a wired LAN, including one switch with Ethernet ports to interconnect all devices.

However, larger organizations with hundreds or thousands of devices require additional hardware, software and configuration to form multiple virtual LANs (VLANs). VLANs limit the amount of traffic individual devices experience, alleviating network congestion and bottlenecks that impact network performance.

**Example of a Virtual Local Area Network**



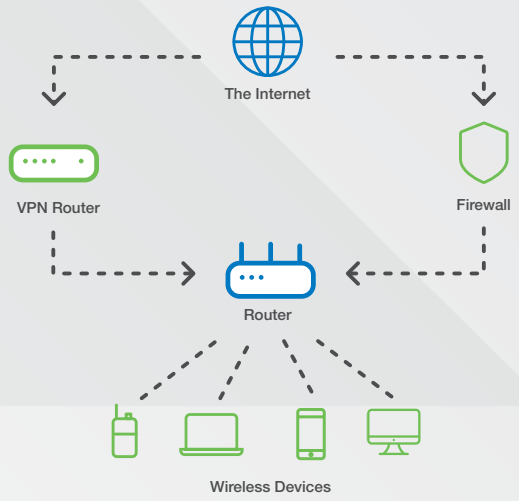
# What is a Wireless Local Area Network?

A wireless local area network (WLAN) is identical to a wired LAN except that the devices that make up the network are connected through radio transmissions, typically a Wi-Fi signal, instead of wired connections. An office or home Wi-Fi network is considered a WLAN.

A WLAN typically consists of a wireless router and endpoints, such as computers, mobile devices, printers, fax machines and other devices. The wireless router enables the devices to talk to each other and also connect to the Internet.

The ease of setup and management has made WLANs commonplace in offices that rely heavily on smartphones, tablets and other mobile devices. But it also has made it possible for other types of businesses, such as restaurants, coffee shops and stores, to have a WLAN. Wi-Fi also has expanded the types of connected devices beyond desktops and printers to include smart devices like lighting, thermostats, security cameras and more.

**Example of a Wireless Local Area Network**



PART 3

# Which LAN is Best for SMBs?

Now that you have a basic understanding of your options, let's discuss which LAN network is best suited for your SMB organization. Traditionally, companies with high security and bandwidth requirements have preferred wired LANs, while those that require mobility have chosen wireless options. With advances in wireless technologies, most organizations now use wireless LANs, at least in part. Here's why:

## Wired Vs. Wireless LANs

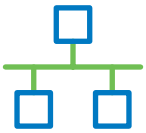
### Wireless LAN

Wireless LANs have these advantages over wired LANs:

**Convenience**
Wireless LANs are easier to set up when compared to wired LANs since they don't require cabling.

**Flexibility**
Endpoint devices like computers and printers only need to be in the wireless signal range and aren't tethered to the wire connection.

**Mobile Access**
Employees can connect to a wireless LAN through smartphones and tablets, which is impossible with wired LANs.



### Wired LAN

Wired LANs have these advantages over wireless LANs:

**Speed**
Wired LANs support greater bandwidth and have faster connection speeds.

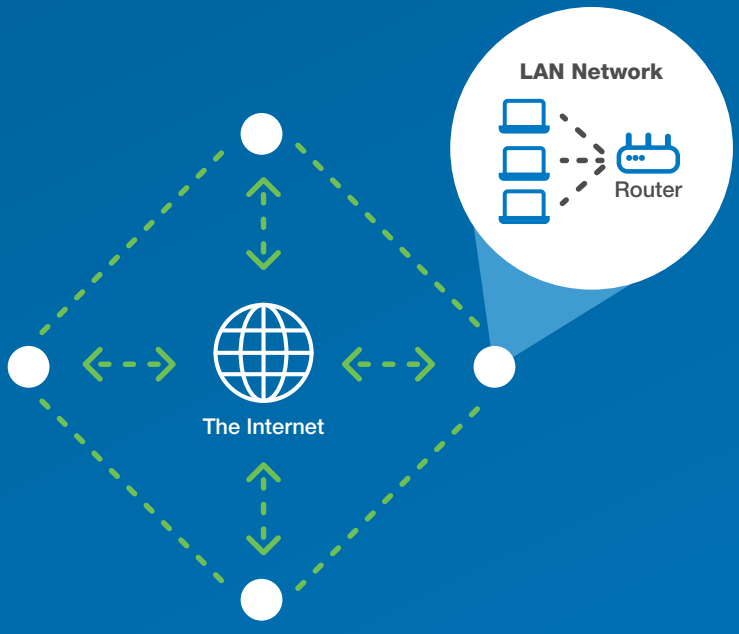
**Reliability**
Weak signal strength common with wireless LANs is not an issue with wired LANs.

**Greater Security**
To break into a wired LAN, the hacker must connect to a network switch, router or computer before accessing the network.

PART 4

# What is a Wide Area Network?

A wide area network, or WAN, is a computer network that spans over a large geographic area and connects multiple local area networks (LANs). In practice, a LAN serves a single office, store location or campus while a WAN connects LANs across cities, states, regions or countries. A WAN's primary purpose is to connect computers on one LAN to computers on another LAN or to computers located at a central data center located on-premises or hosted by a cloud service provider.




WANs have evolved and today are primarily based on a few technologies that can work over fiber, copper or even wireless connections:

- Multiprotocol Label Switching (MPLS)
- Carrier Ethernet
- Software-defined Wide Area Networks (SD-WAN)

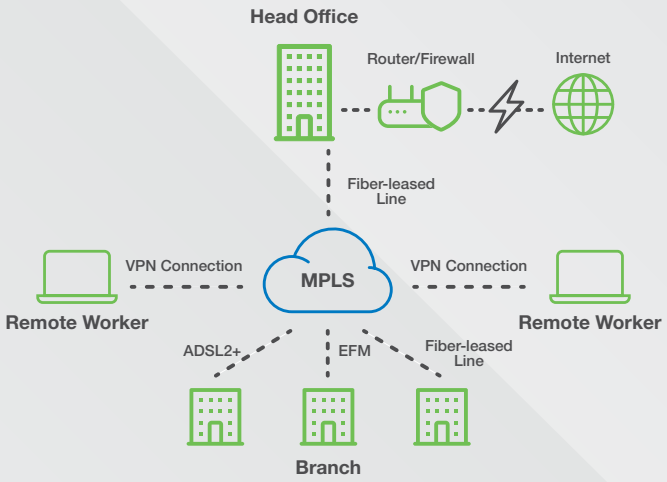
Let's look at each of these in turn.

# What is Multiprotocol Label Switching?

Multiprotocol Label Switching, or MPLS, has powered enterprise networks for more than two decades. An MPLS-based WAN is a virtual private network (VPN) that's built over the top of a carrier's MPLS network and sends data packets over Layer 2 (switching) or Layer 3 (routing), avoiding the public Internet.

MPLS supports classes of service (CoS) for different traffic types; traffic prioritization; scalability; control over latency, jitter and packet loss; and the ability to use multiple protocols (e.g., IP, Ethernet, SAN, FDDI) as the name implies. MPLS networks typically are deployed by geographically distributed organizations that need to connect their locations to a data center or headquarters.

**Example of an MPLS Network**




# What is Carrier Ethernet?

A more cost-effective alternative to MPLS, Carrier Ethernet extends Ethernet from the LAN to the WAN, enabling companies to connect their Ethernet LANs to carrier networks using the same Ethernet interface, bridging multiple LANs as if they were one network. Carrier Ethernet provides effortless scalability from 10Mbps to 100Gbps so that the network can grow with the business.

Carrier Ethernet operates at Layer 2, the data link layer, and can be configured in a few ways as defined by the Metro Ethernet Forum (MEF):

- **Ethernet Private Line (E-Line) — a point-to-point connection between two sites**
- **Ethernet LAN (E-LAN) — multipoint-to-multipoint, also known as "any-to-any" or "mesh," network**
- **Ethernet Tree (E-Tree) — point-to-multipoint, also known as "hub-and-spoke," network**

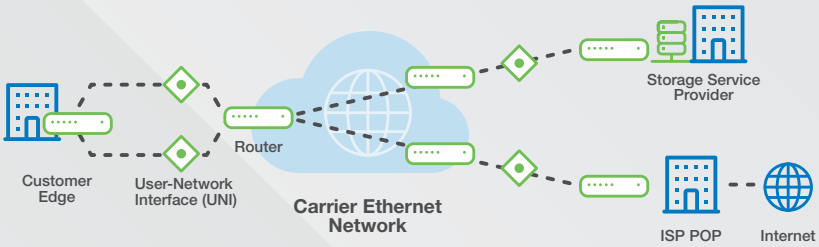
# Carrier Ethernet WANs Come in 3 Configurations

Let's review them one by one:

## E-Line

Ethernet Private Line (EPL) or Virtual Private Line (EVPL) services are used when businesses have high data traffic between a central hub location, like company headquarters, and a data center or storage service provider.

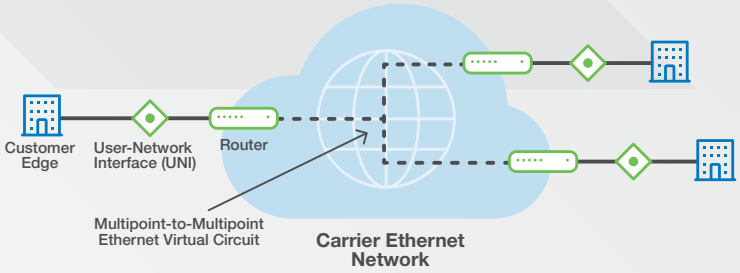
**Example of an Ethernet Virtual Private Line**




## Ethernet LAN

E-LAN provides multipoint-to-multipoint connectivity. E-LANs are used when businesses need to connect branch locations or data centers cost-effectively.

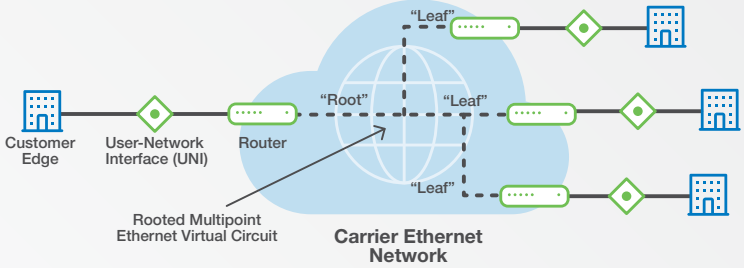
**Example of an Ethernet LAN Network**




## E-Tree

An E-Tree provides hub-and-spoke multipoint connectivity and is often used to connect a headquarters or data center to branch offices.

**Example of an Ethernet Tree Network**



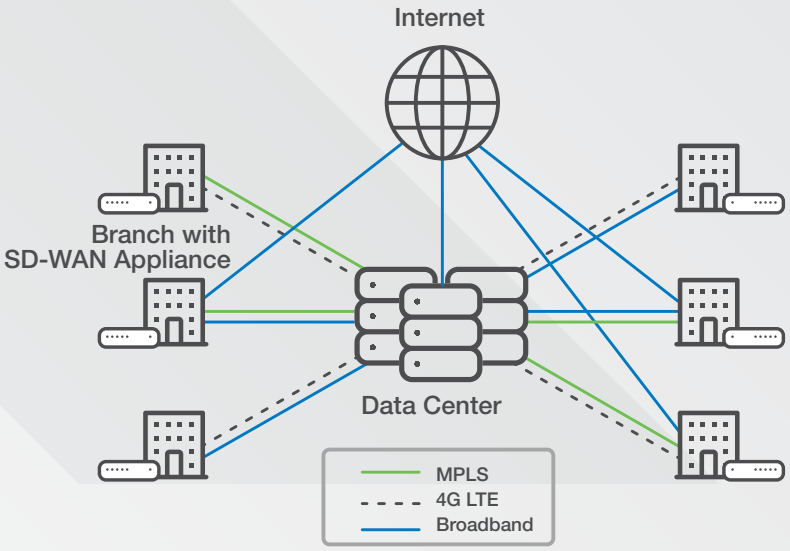
# What is a Software-defined Wide Area Network?

A software-defined WAN, or SD-WAN, is a more recent addition to the WAN lineup that is groundbreaking in that it leverages low-cost broadband connectivity options and also can replace or integrate with an existing MPLS network.

SD-WAN uses software-defined networking to abstract the control capabilities of underlying hardware on the network into a virtual environment where the network is then managed. Through software, SD-WAN unifies and manages network traffic between the different points on the WAN, including remote branches, data centers and cloud applications.

SD-WAN is ideal for connecting branch offices economically but also can be deployed to affordably provide diverse and redundant low-cost broadband connections at every location.

**Example of an SD-WAN Architecture**



PART 5

# Which WAN is Best for SMBs?

Now that you have a basic understanding of your options, let's discuss which WAN is best suited for your SMB organization.

## MPLS Benefits

MPLS-based WANs are known for their scalability, performance, efficient bandwidth utilization, reduced network congestion and quality of service (QoS). Because it's deployed as a VPN, partitioned from the public Internet, it's also considered a secure transport mode.

That said, MPLS was designed for organizations with geographically dispersed branch offices needing access to enterprise data centers. Today, much of enterprise networking traffic has shifted to cloud providers making MPLS's hub-and-spoke model less efficient.

For this reason, MPLS is considered a legacy WAN solution and may be displaced or augmented when new IT management pushes for newer network technologies to save the organization money. Larger enterprises, for example, may keep their MPLS networks for legacy apps that run on their enterprise network while offloading Internet traffic and access to cloud apps to a more modern SD-WAN.

Companies in vertical industries like finance may still rely on MPLS to ensure compliance with regulations like Sarbanes-Oxley Act of 2002[1] and are not eager to replace existing equipment that works.

SMB organizations are more likely to find a better fit with lower-cost Ethernet or SD-WAN options. And those companies that are using an all-cloud IT model are best served by SD-WAN's all broadband network.

## Carrier Ethernet Benefits

While MPLS networks have been the top-of-the-line for decades, Carrier Ethernet offers a more cost-effective alternative, especially for SMBs that want to upgrade their networks for improved communications systems, data storage and more.

Carrier Ethernet offers several advantages, including:

### Scalability

As your business bandwidth requirements grow, Carrier Ethernet can scale easily without the need for additional onsite equipment.

### High Speed

With bandwidth of 10Gbps+ over fiber links, Carrier Ethernet is ideal for businesses looking for high-speed services to connect data centers.

### Security

Carrier Ethernet operates at Layer 2 and its in-band control channel cannot be accessed via a Layer 3 network, i.e., the Internet, which is in contrast to MPLS routers that can be accessed remotely via the Internet.

### QoS

Carrier Ethernet VLANs are easily created to separate traffic types, reducing network congestion and latency.

**MPLS vs. Ethernet for the WAN**

| | MPLS | Ethernet |
|---|---|---|
| **Cost** | MPLS typically costs more than Ethernet but less than T1 lines. | Ethernet is typically more affordable than MPLS. |
| **Scalability** | MPLS can scale to thousands of sites. | Ethernet can scale to hundreds of sites. However, it's much easier to scale without the addition of equipment. |
| **WAN Routing** | MPLS allows businesses to leave WAN routing to the service provider and keep fewer WAN engineers on staff. | Ethernet gives WAN engineers control and responsibility over routing. |
| **Quality of Service** | MPLS has quality of service (QoS) options to enable preferential treatment of latency-sensitive traffic like VoIP. | Network engineers can bypass QoS complexity by hooking switches directly to Ethernet pipes. |
| **Service Level Agreements** | MPLS services come with service level agreements (SLAs) that include delivery guarantees, unlike consumer broadband. | IT professionals should either ask for an SLA for their Ethernet service or take WAN application delivery into their own hands. |
| **WAN Management** | Using MPLS for WAN connectivity requires that all network devices and management tools be compatible with both MPLS and Ethernet | Because LANs use Ethernet, using Ethernet for the WAN gives organizations an all-Ethernet infrastructure, simplifying network management. |
| **Availability** | Service providers offer MPLS services in many metropolitan areas but not everywhere. | Ethernet exchanges have made Ethernet WAN services available in more locations. |

Source: SearchEnterpriseWAN

## SD-WAN Advantages

SD-WAN is different from traditional WANs in the way it's deployed and managed. As its name implies, SD-WAN is a software-driven technology that's deployed as an overlay or virtualized network. While there are some differences in features depending on the SD-WAN provider, SMBs can expect the following benefits from SD-WAN:

### Business Continuity

One of the most valuable benefits of SD-WAN is its ability to deliver network redundancy. SD-WAN can direct traffic on multiple connections, whether the configuration is active-active or active-passive. This routing ability means that businesses often can avoid network downtime — with their users remaining online and active — even if there is an outage with one or more connections.

### Improved Data Security

Often, SD-WAN can support network security by virtualizing a firewall that encrypts public Internet traffic. Some basic security capabilities are inherent with SD-WAN, such as denying or limiting traffic from specific sites. *Note: SD-WAN is not a comprehensive security solution on its own and should be paired with other security solutions.*

### Enhanced Quality of Service (QoS)

SD-WAN steers business-critical traffic and applications through the most reliable, highest-performing connections. The net impact is a reduction in data packet loss and latency, which improves user experience and productivity.

### Bandwidth Elasticity

SD-WAN can manage multiple network connections to increase bandwidth by removing network congestion and creating better application response time.

### Cost Savings

Businesses can save money with SD-WAN. First, it can replace expensive private MPLS connections with more cost-efficient broadband connections. It also can remove the need for expensive routing hardware since those are now controlled with software. Since administrative control functions are now virtual, there are no physical configuration requirements onsite. Instead, IT can access and manage the control plane conveniently off-site, reducing the need for onsite IT personnel.

PART 6

# What Defines a 'Good' Network Today?

Networking technologies have evolved, enabling transformation for businesses of all sizes. In short, today's hyperconnected businesses are hyperdependent on their network connections — not only to communicate and share information but often to deliver their products and services.

So, as you're evaluating what's a "good" network for your SMB organization, consider these five must-have requirements.

## 1 Uptime

Whether LAN or WAN, the most critical attribute is uptime. If your business is like most, you rely on endpoint devices connecting to your network and/or the Internet to access a range of critical applications, such as:

- Email applications
- Phone systems
- Unified communications and collaboration applications
- Websites
- E-commerce applications
- Customer and partner admin portals
- Contact center software
- Office productivity applications (e.g., Microsoft Office or G-Suite)
- File sharing applications
- Accounting software
- Customer relationship management (CRM) applications
- Human resources (HR) files and employee records
- Accounting and billing systems
- Enterprise resource planning (ERP)
- Supply chain management (SCM)
- Payroll systems

Network downtime renders all these applications and systems inoperable, costing your organization in many ways, such as:

- Lost productivity
- Lost sales
- Lost customers
- Damaged reputation

## Security

Security goes hand in hand with uptime as cyberattacks often cause network issues and business disruptions. Cybersecurity is a priority for businesses of all sizes, especially since the COVID-19 pandemic expanded network vulnerabilities to remote workers and increased cybercrime reports by 400 percent to 4,000 complaints per day, according to the FBI[2].

Securing your network is no small task, as bad actors can attack your network at any point, not just in one place. The best defense is a layered approach, including:

- Next-Generation Firewalls
- Backup & Data Recovery
- Password Management
- Multi-Factor Authentication
- Patch Management
- Managed Detection & Response (MDR)
- DNS Protection
- Security Awareness Training
- Email Security

## High Speed

Speed refers to the maximum rate of transmitting data, typically measured as megabits per second (Mbps). Network speed is essential to both employee and customer experience. For example, storefront retail organizations need credit cards processed at an acceptable rate to complete the transaction so that customers aren't upset at the hassle of trying to pay for their products.

## High Bandwidth

Bandwidth refers to the maximum amount of data your connection can handle at any moment, also measured as Mbps (and increasingly Gbps, for gigabyte connections). Adequate bandwidth is required to ensure that all of your applications can function simultaneously.

## High Availability

Technically speaking, a "high availability" network has built-in failover at the hardware level. You might have multiple circuits connected to an SD-WAN edge device so that if one circuit goes down, another circuit will be up. However, if the SD-WAN device fails, it no longer matters there are two circuits; the entire network will go down. A network that has "high availability" addresses this by incorporating redundant hardware.

PART 7

# What Are Common Network Trends Today?

Corporate networks have evolved to accommodate distributed and mobile workforces, cloud-based computing and communications, and a rise in security threats. Common trends in networks today include:

## Secure Networks

The need to secure networks (WAN or LAN) is of utmost importance today.

Cyberattacks like ransomware are the most common cyberthreat SMBs face, with 60 percent of MSPs reporting that their SMB clients have been hit as of the third quarter of 2020[3], Datto reveals.

Ransomware has been around since the late 1980s, but the number of attacks has skyrocketed within the past two years. In fact, according to the FBI, cybercrime reports surged 400 percent during the pandemic[4], to 4,000 complaints per day.

The network security risk profile has changed at such a rapid pace over the past year that SMBs need to upgrade their networks by implementing comprehensive cybersecurity solutions.

## Blending Networking & Cybersecurity

Over time, networking technology has become mixed with cybersecurity technology.

A network firewall began as a straightforward solution that performed a narrow scope of functions, including blocking unsolicited incoming network traffic and validating access by assessing traffic for malware, hackers, etc. Today, a next-generation network firewall has multiple security appliances in one device, performing functions of a traditional firewall but boosting protection through heuristics (ie. analysis using rules, estimates and educated guesses for prediction) or artificial intelligence (AI). Next-generation protection also delivers unified threat management (UTM), which includes:

- Antivirus software
- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)
- Deep Packet Inspection (DPI) of SSL traffic
- Safelisting/blocklisting software

Similarly, when looking at a first-generation SD-WAN solution, the edge device is essentially a router and a load balancer[5] combined into one. Today, SD-WAN and security functionality are being bundled together as a "secure SD-WAN" appliance that keeps your business connected, guarantees redundancy and increases security.

Consolidation of networking and functionality under a single management plane increases management complexity — an area where an MSP like TPx can help.

## Remote Network Access

While it's a tired statement, the pandemic has dramatically changed the way every company does business. According to Upwork's Future Workforce Pulse Report[6], 22 percent of the workforce (36.2 million Americans) will be working remotely by 2025.

This trend has resulted in a need to identify top applications that need priority, like video calling, which is where the majority of sales are taking place today. Businesses literally can't afford for the connection to be poor. In addition, streaming applications like Hulu and Netflix needs to be deprioritized so that critical applications like CRMs, PRMs, PMS, file-sharing systems, accounting systems and communications aren't affected.

Additionally, remote workers need to securely connect to the business network from home, so VPNs and home-based SD-WAN deployments have become more commonplace.

## Secure Access Service Edge

Secure Access Service Edge (SASE) moves away from data center-oriented security. It unifies your network and security tools into a single service delivered via the cloud, providing edge-to-edge protection for remote users and data centers.

SASE is an upcoming player potentially and the market is still determining hype or whether it's adopted. MSPs like TPx are assessing the value of SASE for delivery to SMB customers. It's worth noting that there is nothing new about SASE technology except that it's packaged and consolidated onto a single platform.

## Managed Switching

Switching is often overlooked, but TPx sees growth in the managed switching market. Managed switches offer a range of features that can be configured by IT professionals to optimize network performance, availability and security.

Managed switches are a must for networks where reliability and security are critical, such as those used by government agencies, universities and healthcare organizations.

However, with their additional functionality, managed switches require more expertise to provision and manage, which entails having greater skills or the assistance of a knowledgeable MSP like TPx.

## Wi-Fi 6

Today, business Wi-Fi networks are struggling to keep up with the dramatic increase in the number of wireless devices and high-bandwidth multimedia applications — not to mention the influx of 8K video, virtual reality and 5G network traffic. WLANs need to handle higher density and higher throughput requirements as well as issues associated with radio interference and security.

Wi-Fi 6, also known as High-Efficiency WLAN, is the answer. Wi-Fi 6 lays the groundwork for the growing use of internet-connected hardware and devices as well as applications like collaborative high-definition (HD) video streaming, augmented reality and virtual reality.

Wi-Fi 6 not only triples the maximum throughput of Wi-Fi 5 but delivers better indoor signal penetration and supports greater device density. Wi-Fi 6 has enhanced capabilities to effectively handle increasing traffic demands, capacity, coverage and network intelligence.

PART 8

# What Are Common Network Pain Points for SMBs?

SMBs typically need to address common network pain points, which can be solved by outsourcing to an MSP like TPx. These include:

## Filling Technology & Training Skills Gaps

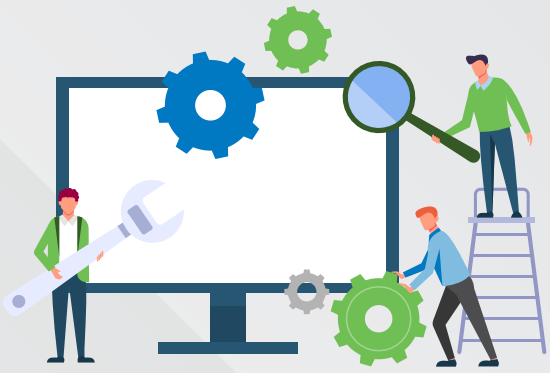
As the complexity of IT has ratcheted up, SMBs often don't have the necessary IT resources available to handle the specialization that networks require. In many cases, SMBs with an in-house IT department rely on an IT generalist, or they've assigned IT responsibilities to an employee whose core job is not IT-related. An MSP like TPx can help fill these gaps with IT specialists in a range of areas.

## Sourcing Highly-Paid Specialized Network Engineers

Even when an SMB is fortunate enough to have an IT team, in-house specialization for their network often doesn't make financial sense. Outsourcing to an MSP like TPx is more cost-effective than hiring a full-time engineer. Plus, specialists will execute more quickly and efficiently, reducing total costs.

## Managing Networks & Security

If your SMB doesn't have networking experts on staff, managing your network is a big pain point. Even if some members of your IT staff are networking experts, they're unlikely to be security experts. Today's networks require a dozen security solutions to be layered over the top. And best practice is 24/7 monitoring and remediation by analysts in a security operations center (SOC). Few, if any, SMBs have this capability; an MSP like TPx provides expertise in both networking and security with round-the-clock management.



## Gaining Network Visibility

The growing volume and variety of data traversing your enterprise network have complicated network monitoring. Visibility is critical for understanding traffic behavior and ensuring efficiency, security and performance. An MSP like TPx has invested in state-of-the-art networking monitoring tools as well as the experts who can act on the data to improve your network.

## Preventing & Responding to Problems

IT teams are constantly putting out multiple fires and can't proactively prevent issues. An MSP like TPx has access to technical information and live feeds to stop problems before the customer knows they exist.

## Retaining Existing IT Staff

Your IT team has opted into a 24/7 on-call gig and may need to put out fires at odd hours, including overnight and on the weekends. But even they have boundaries. If members of your IT team need to be giving up nights and weekends to solve issues, they may burn out and leave. With in-demand skills, your hard-to-source engineers will simply move on. This turnover is commonplace and can cripple your company's operations. An MSP can alleviate the pressure on your IT specialists and give your team a better work-life balance.

PART 9

# Where Should SMBs' Network Strategies Start?

Are you looking to get a handle on your network strategy? Start by identifying your network needs, assessing your current network capabilities and planning for the future.

## Identify Your Network Needs

- What do you need to accomplish through your network?
- What problems are you trying to solve with your network?
- Do you have critical applications that require 100 percent uptime?
- What are your current network resources?
- What existing network resources are on-premises?
- What existing network resources are in the cloud?
- What systems does your business need to function? Typically, this includes communications, project and task management programs, customer databases and credit card processing required for your business to operate.
- What systems does your business not need to function? Non-critical applications might include a random file server on your network, which you might not want to lose, but won't impede your ability to operate.

In TPx's experience, some businesses, especially SMBs, don't know the answers to these clarifying questions because they don't have visibility into their networks. In these situations, a trusted resource like TPx can assess the company's needs and engineer solutions around them.

## Use Network Assessment Tools

Using network monitoring and assessment tools, TPx can identify existing parameters and characteristics of your business network and present options to optimize it for security and redundancy.

TPx offers a Cyber Threat Assessment Program (CTAP), a free network assessment that doesn't affect the network and simply observes and audits for possible problems concerning both network traffic and security. After the evaluation is complete, TPx takes the information and makes recommendations for how to resolve any issues.

For example, TPx might discover that a significant portion of your bandwidth is being used by employees who are streaming video services. In response, you could buy more bandwidth to handle streaming traffic, or limit, throttle or block it altogether.

Problems that may be uncovered could include mundane issues like excessive streaming traffic or more severe concerns like a botnet that presents a security threat.

## Plan for the Future

To create an optimal network strategy, plan for the future by building in scalability. Build a network that will serve your needs two years down the road to prevent your business from quickly exceeding the capacity and capabilities of your WAN infrastructure.

To design a network built for the future, your team, preferably with the aid of an experienced MSP, should consider:

- Sizing WAN infrastructure properly beyond current needs
- Acquiring a new switch with higher capacity
- Incorporating Wi-Fi 6 or other next-generation Wi-Fi technology that has greater capacity so more devices can access the business Wi-Fi connection at once

Additionally, choose a network services provider with scalable technologies and the infrastructure (i.e., people and systems) to manage the network effectively and keep tabs on developments in network technology that can make your business more productive.

**Case in point:** SD-WAN wasn't on the radar six years ago; now, it's a standardized solution for most networks. The average SMB IT staff doesn't have the bandwidth or expertise to keep up with trends in the marketplace, whereas a large MSP like TPx is tapped into industry resources to stay on the pulse of emerging tech.

PART 10

# How Can SMBs Improve Their Network Performance?

Figuring out how to improve your corporate network can be a tall order, so we recommend leaning on a well-versed MSP like TPx to guide your business through the process from end to end.

## 5 Steps to Improve Network Performance

STEP 1

### Gain Network Visibility

Through network management tools, gain insight into your network to assess current status and resources.

STEP 2

### Assess Network Needs

Network requirements change over time, so network configurations must be assessed and revised to meet evolving needs.

STEP 3

### Monitor Network Performance

Observe your network over time to discover what's working well and what should be improved.

STEP 4

### Patch Firmware

Sometimes improving a network simply means keeping firmware up to date. Since network technology is all software-based, an MSP working on your behalf can patch the applications remotely.

STEP 5

### Upgrade Gear

Finally, depending on your network structure, you may elect to acquire new and improved network technology such as Wi-Fi 6 access points or upgrade to new hardware components like edge devices or switches.

**Ultimately, decisions must be made that balance network performance and cost. A qualified MSP like TPx can help your company navigate these decisions.**

PART 11

# Why Should SMBs Choose TPx for Network Services?

TPx offers end-to-end management of your network infrastructure, helping you increase productivity, lower costs and remove the complexity of running your vital connections on your own.

## Why Choose TPx?

We solve the biggest IT issues, including cybersecurity, connectivity, communications and collaboration, all under one umbrella.

We have the IT solutions, staff and experience to deliver cybersecurity effectively and within budget. We use our buying power to pass on the savings to your clients.

We have 120+ certifications across 60+ categories from well-known vendors and associations, including Microsoft, CompTIA, SilverPeak, Cisco, Fortinet, AWS, SMC and more.

We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.

With 23,000 clients in 50,000+ locations, we're big enough to get the job done and small enough to be agile.

We mix and match solutions and deliver a variety of service levels customized to meet your needs.

## TPx Knows Networks

The expert managed networking division at TPx can easily turn on new network services for your business using our thorough pre-install analysis and planning process backed by our proven track record. Our team has deployed 15,000+ devices and have network engineers on staff who have experience with SD-WAN, MPLS and traffic routing.

### Third-Party Circuit Support

Use our superior network or run over-the-top (OTT) of any carrier network — all with guaranteed performance through our delivery management.

### Continuity Options

We offer three-circuit active deployment scenarios using TPx or OTT carriers, 4G LTE and inbound IP for VPNs and web servers.

### 4G LTE Service Options

Take advantage of our 4G LTE deployment models:

- Failover— Active/Passive
- Secondary— Active/Active with primary circuit
- Primary— Active/Active

# TPx: Your One-Stop-Shop for Managed Networking Services

### SD-WAN

Deliver guaranteed performance over the cloud without headaches like multiple provider footprints, complex routing, high expenses and connectivity or redundancy limitations. Simplify management and operation of network connections between different sites and improve application performance.

### Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your business from Internet-based threats. Firewalls block today's advanced threats while also providing secure access, visibility and control to help your business be more productive.

### Network Switches

TPx uses the latest switch technologies with advanced troubleshooting and reporting capabilities, along with redundant power and stackable features. Through network switch tech made for modern business, you'll gain the fastest and most reliable network possible.

### Wi-Fi 6

TPx Wi-Fi 6 service delivers higher performance and greater efficiency to your wireless LAN even as the bandwidth-intensive media content and the number of devices connecting to Wi-Fi grows.

### Wireless LAN

A new or updated managed wireless LAN solution from TPx can help increase productivity by allowing your employees to work more freely and on more wireless devices while providing security and control.

### Internet Access

TPx offers a wide array of access options for your business from dedicated internet access (DIA), broadband (e.g., cable and DSL), wireless 4G LTE, MPLS and more.

**Sources**


1 https://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act

2 https://apnews.com/press-release/newswire/d50cabdf813c59e4c1ffe046009b41b6

3 https://www.helpnetsecurity.com/2020/11/18/ransomware-cyber-threat-smbs/

4 https://apnews.com/press-release/newswire/d50cabdf813c59e4c1ffe046009b41b6

5 https://www.techtarget.com/searchnetworking/definition/load-balancing

6 https://www.upwork.com/press/releases/economist-report-future-workforce