PLANNING A SUCCESSFUL WIRELESS NETWORK UPGRADE

federated®
SERVICE SOLUTIONS

Corporate Office
41100 Plymouth Road, Suite 165
Plymouth, Michigan 48170
(248) 539-9000

Introduction

We live in a globally connected world that requires tens of thousands cell towers, numerous satellites, and wireless networks that keep us all communicating with one another. This connectedness allows the conveniences we all enjoy: immediate access to texts, emails, the internet, and the ability to make and receive phone calls. It also allows businesses to continuously transmit large amounts of data necessary to keep their operations running.

Significant time and money is required to keep wireless networks secure, and ensure quick data upload and download speeds. IT departments have a massive responsibility to keep up with all the required security updates for both networks and their devices, as well as maintaining all of their network equipment.

Most Persistent Network Problems & Challenges

In our experience, some of the most persistent problems with wireless networks are:

- High traffic networks with slow transmission speeds (due to poor design)
- Security concerns (due to aging equipment)
- Dead zones, or areas in a building where the network cannot be accessed (due to a number of possible causes)

Making the decision to upgrade or replace a wireless network can be a long and challenging process and there are many factors to consider, including how equipment, employees, customers and guests will be impacted. An improved network needs to not only meet security and speed requirements, but must also be scalable for future growth. The time and money needed to upgrade the network is a capital expenditure, and every decision made before, during, and after the upgrade is critical to avoid rework and additional spending.

Network Challenges

Every industry faces its own unique challenges when planning an implementation.

Retail Stores

Strict security requirements, limited hours of installation, and long blackout periods to avoid implementation problems during busy holidays.

Medical Facilities

Have limited installation window, and require HIPPA certified technicians.

Commercial Buildings

Have both private and public networks, large amounts of traffic, and complex floor plans that may inhibit access to the network.

Distribution Centers

Are now more reliant on wireless technology that requires access to the network over a large area.

Each industry and type of business in that industry will face its own problems and challenges when designing a network that functions according to needs. They will also need a secure network that will easily adapt to business growth and advances in technology.

IT Managers must meticulously plan the implementation of the upgraded network, and how the installation of new network equipment will impact their company's day-to-day activities. They'll need to choose the right equipment, make sure that it meets their wireless network requirements, and submit a carefully-crafted budget.

The Costs of a Bad Network

What is the cost of a bad network? A slow internet, dropped calls and frustrated customers are just the beginning. Network downtimes could result in lost business and missed opportunities. One of the biggest concerns is that a network without adequate firewalls and the most recent security updates could allow a security breach and the theft of confidential company information and customer data. It's safe to say that the total cost of bad network is probably much higher than the cost of upgrading or replacing a network.

Information in the following chapters will help you get organized and plan a successful wireless network upgrade or replacement.

General Coverage Rules

Network requirements vary not just by the industry and business, but also the building type and layout. Many factors can impact not just wireless coverage but also traffic volume and network security.

After identifying the core requirements of your wireless network, as well as what your business needs to adapt to increasing mobility demands, you can begin to design a future-proofed and successful wireless network. Answer these questions:

How large of an area do you need to cover?

- How many employees need to connect wirelessly?
- Do you need outdoor coverage?
- Will you be offering guest internet access?

What is your budget?

For initial budgeting and planning purposes here are some rules to follow:

- Assume approximately 3,500-4,500 sq ft of coverage for each indoor access point, on a per floor basis
- Assume approximately 5,500-9,000 sq ft of coverage for each outdoor access point
- Assume each access point will provide connectivity to approximately 20-30 client devices

Chapter 2: General Coverage Rules

When considering your building keep in mind that any obstacles or partitions (walls, desks, cubicles, windows, etc) that the wireless signal (RF – Radio Frequency) needs to pass through will reduce signal strength. Construction materials affect wireless signals differently; a concrete wall is going to attenuate signal more than drywall, and a thick window is going to reflect signal more than a thin window.

Large environments, or buildings with a lot of obstructions, have different network requirements than smaller buildings with open office settings :

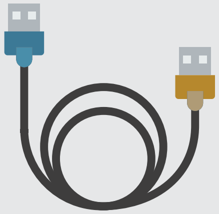
Large Buildings

- It's recommended that a predictive site survey be completed to help design the layout of your network.
- Whenever possible, have an installation professional complete a full site survey that will help you to design the layout of your network.

Small Buildings

- Network planning can usually be completed without additional software tools and/or a full survey.
- An installation professional is a great resource to help you to plan for a new network. This is especially true if you need to deploy an upgraded network in multiple locations.

Once you have the key questions answered and you have completed the coverage planning stage, you can also employ the services of an installation professional. They can help you work through the integration phase and verify the coverage of the network before you begin deploying. If you need cabling installed to each access



Cabling should be installed in accordance with NEC, LAHJ. It is highly recommended that best practices and industry standards be followed for optimal network performance.

point, keep in mind that cabling installation will require copper cables to be run from the network head-end to each AP location.

An installation professional can then assist you with the configuration of your network hardware (switches, routers, APs, firewalls) and can help to verify the network coverage upon completion. Configurations range in complexity based on network requirements and the current setup/configuration in place, if any. Coverage verification will then ensure that all clients that need access to the wireless network are within range. Functionality verification will confirm that all services that need to be reached wirelessly are accessible and that these services perform appropriately.

You also might want to test your deployment immediately, and then again within the first 30 days after the initial launch. Keep an eye on the performance of the network while encouraging feedback from the intended users of your wireless network to make sure that your expectations have been met. This will ensure that all of the required functionality is working properly and help to identify areas where improvements can be made in the rest of the deployments.

Chapter 3

Guest WiFi and Marketing Capabilities

Guest Internet access is in high demand and is a basic expectation in any customer-facing business environment. Providing a guest WiFi is a great perk for customers and can be used as an excellent way to incorporate marketing capabilities into your day-to-day customer base by sending them real time information on sales and special offerings. The good news is, the cost to deploy WiFi technology that increases customer satisfaction is minimal.

Deploying a Guest network is relatively simple.

By deploying the correct captive portal/splash page to login to your guest network, you are able to:

- Record information about your customers to utilize for a target list later on.
- Customize requirements to include things like Facebook authentication, that asks users to “check-in” to your location.
- Or ask for email address, phone number, name, etc.

You can also utilize these authentication methods to enable options to push sales flyers, special offers, and other sales/marketing content.

Cloud vs. Controller-Based

There are many options available today when designing a wireless network. One of the most important things to consider, and typically the first decision, is whether to use a **Cloud-Based Solution** or an **On-Premise/Controller-Based Solution**. It's important to understand where each makes the most sense and there are many use cases for either deployment method.

Cloud-Based Wireless Network

Cloud-based solutions bring benefits such as increased and simpler scalability, ease of deployment with multi-location businesses and businesses with remote staff. They also limit the need for a large in-house IT team that needs to spend their time managing your wireless network. A cloud-based solution eliminates the requirement of maintaining the controller of your network because the software is the responsibility of the supplier. This eliminates the need for your team to have to handle software patches and updates. You also won't have to worry about upgrading your wireless network hardware when your device count increases because everything is cloud-based. And unlike an on-premise solution, your cloud-based solution will not be limited in the amount of access points it can support.

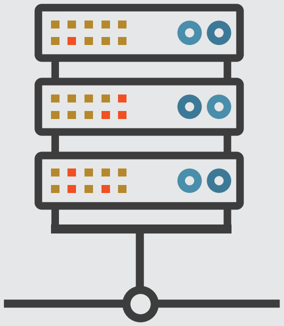
Lastly, deploying services to multiple buildings/states/regions is much simpler with a cloud-based solution as all of your network configuration lives in the cloud and typically is easily replicated to additional devices and/or networks. These devices are plug-n-play!

Controller-Based Wireless Network

The biggest advantages you will see with an on-premise wireless controller is increased control and customization. A controller-based solution is preferred when you are not able to rely 100% on your Internet. Because cloud-based solutions require that the Internet be connected for the devices to communicate with their controller, Internet reliability is a huge factor.

Controller-based solutions are also preferable for most large Enterprise networks, as these will typically have more policies in place, require in-depth control of the entire network, and the hardware available for controller-based solutions still has more variety/options. Be sure to keep in mind that with a controller-based solution, you will need a properly scaled IT team as the management of these networks will take more time, skill, knowledge, and effort.

Cloud-Based
Vs.
Controller-Based



Wireless Meshing

A mesh is the interconnection of devices or nodes. In networking, the term "mesh" can mean more than one thing and is differentiated by how the devices are organized in the network. Determining how the devices are meshed can have a significant impact on the speed of traffic flow in the network.

A mesh network topology indicates that all devices within the network are interconnected to one another. However, in a wireless network, meshing (2) or more access points is slightly different. When (2) or more access points are meshed, there is a master unit and repeater unit(s). The master unit acts as your Gateway, or main connection, to the Internet/network. The repeater unit simply connects to the master unit wirelessly, similar to the way your phone or computer would connect to an access point. However, with a successful mesh connection the "repeater" unit acts as an extension of the master unit and the wireless network.

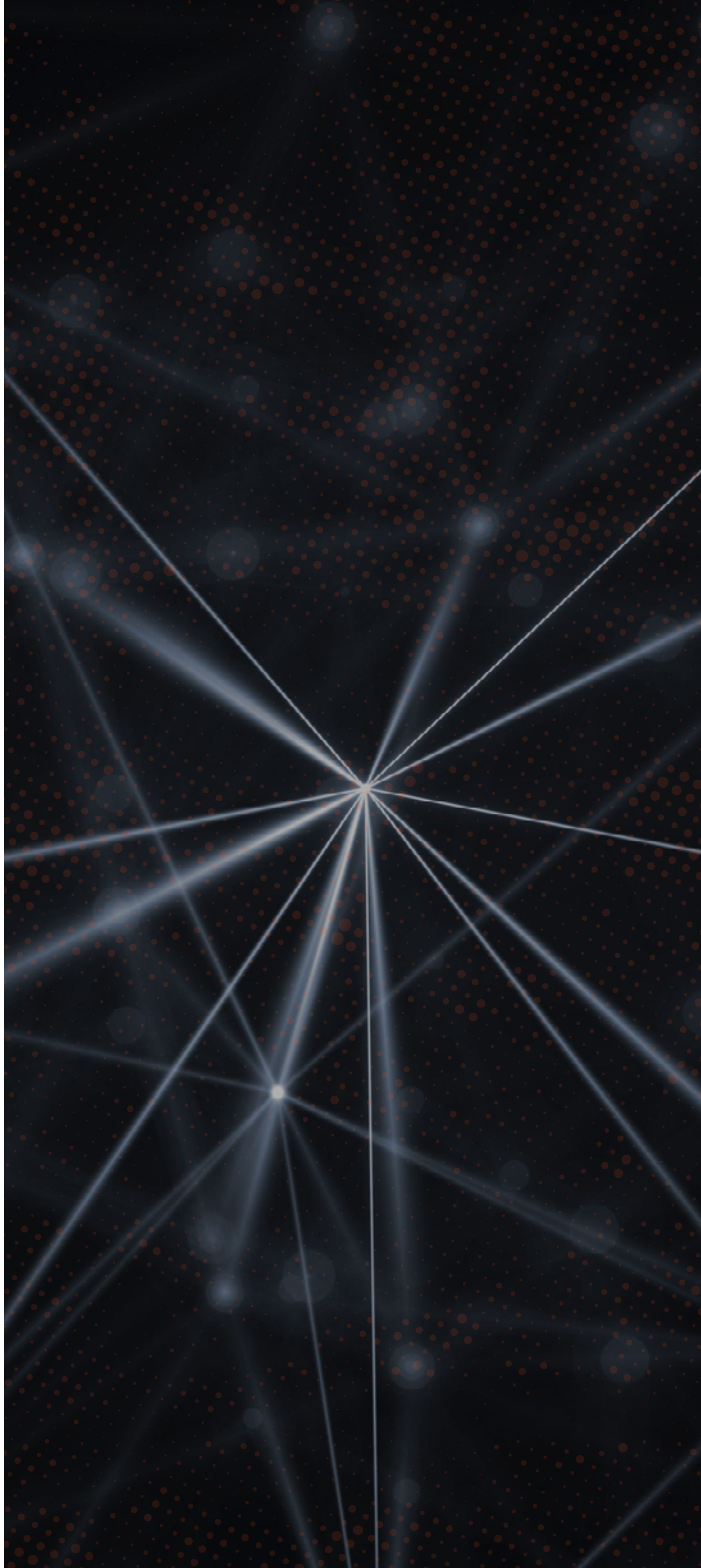
There are pros and cons to this setup. The pros are the ease of deployment and costs associated with the deployment. When you mesh access points, you do not need cabling installed to the 2nd, 3rd, etc access points because their connection to the network will be wireless. You simply need power for the devices and they will be ready to go.

However, each time you "mesh" access points you are cutting the throughput of these devices in half. If you run an organization with heavy wireless utilization and a lot of client devices, it usually is not a good idea to mesh your access points. The other con of meshing access points is that if your main unit loses connectivity to the Internet/ network, all devices will lose connectivity until the main unit is restored.

Good use cases for meshing your wireless access points are:

- temporary deployments
- retrofitting a building/area where cabling is not feasible
- residential installs or installs that do not require high throughput

It is typically recommended to hardwire each access point in a network to guarantee maximum throughput and reliability.



WLAN Types

WLAN is of course the initialized name for Wireless Local Area Network. It utilizes Wireless Medium, that includes radio wave, microwave, and so on. As there are several types of WLANs selecting the best one to fit the needs of your business is a critical decision. Each WLAN provides different areas of coverage and has different standards and applications.

WLAN access points or routers are a commonly utilized device, which convert LAN to WLAN, so that various devices that utilize WiFi can communicate with the pre-established LAN. Most routers have the capability to perform both functions, and many other devices offer the ability to broadcast to these WiFi devices, as well, whether they be USB dongles, or other similar devices.

WLAN operates on radio frequency of 2.5GHz or 5GHz. The main data rates of WLAN are 11a, 11b, 11g, 11n, 11ac, and 11ad. These all are colloquially known as the IEEE Standards, which define PHY and MAC layers of the above data rates.

Below is a brief breakdown of each type of WLAN:

- IEEE 802.11a supports the OFDM physical layer, and performs at 5GHz RF center frequency.
- IEEE 802.11b supports the DSSS/CCK physical layer.
- IEEE 802.11g supports both 11a and 11b, at RF center frequencies of 2.4GHz and 5GHz.
- IEEE 802.11n supports OFDM and MIMO, and enables 40MHz bandwidth.
- IEEE 802.11ac greatly increases MIMO antennas and data rates compared to 11n.
- IEEE 802.11ad enables devices operating in 60GHz band.

Directional vs. Omnidirectional Antennae

Another consideration to be made when deploying access points is which antenna to use in which area, and which scenario. WAPs (Wireless Access Points) generally utilize either a Directional antenna, or an Omnidirectional (Omni) antenna. Each has a purpose, range, and use case depending on location of cell towers, line of sight to the towers and distance from the cell towers to the building.

Omni Antennae

Omni antennae, when installed on an access point, broadcast in a generally spherical-shaped signal. The ideal usage for an Omni antenna would be for individual rooms, or vehicles. Degradation of the signal will take place nearly at the same distance of the full diameter of the signal being broadcast by the WAP, given perfect conditions. Obstructions such as walls, doors, windows, furniture, and certain electronic devices can cause changes in attenuation and weaken the signal. Being prepared for the arrangement of WAPs to provide full, strong coverage is key.

Directional Antennae

The Directional antenna has a much stronger focus on range and distance than the Omni antenna, but sacrifices full coverage surrounding the WAP itself. The Directional antenna broadcasts in a cone, intensifying the signal in a certain area. These antennae are aimed in a particular direction and can target an area with far more distance than the Omni. The best use case for Directional antennae are for larger, outdoor areas, where physical connectivity is more difficult to achieve. Large areas can be covered with multiple Directional antennae, as well as the capability to serve as point-to-point connections.

Chapter 8

WIPS Density

WIPS stands for Wireless Intrusion Prevention System. A WIPS device has a radio dedicated to scanning the airwaves for rogue access points and other nefarious devices or tools. A WIPS device also has the capability to automatically contain these threats and alert system administrators to their presence. The **PCI Security Standards Council** recommends the use of WIPS to automate the ability to scan the network and detect rogue access points and other threats to the network.

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. Learn More

WIPS devices can be sensors dedicated to WIPS alone or built into access points. Most enterprise-class access points have WIPS capabilities. Access points can function as both a WIPS sensor that also serves clients, or function solely as a WIPS sensor without serving clients. Some access points that can serve clients and function as a sensor may do so in a limited fashion, while others have a radio dedicated solely for WIPS.

Dedicated WIPS devices are generally deployed in a 1:4 or 1:5 ratio which can change depending on type of environment and actual AP density. APs with a dedicated 2.4GHz and 5GHz radio (on a single radio) should be deployed in a 2:5 ratio due to the additional scanning time needed since there are more channels to scan. APs that can both serve clients and function as a WIPS sensor can be deployed in a 1:1 ratio.

Chapter 9

Bluetooth Capabilities

Bluetooth technology was first invented in 1994. Over the last 24 years it has become the cornerstone of **Internet of Things** (IoT) and enables us to connect wirelessly to our phones, computers, vehicles, appliances and even our homes and businesses. It has also become an integral component of all wireless networks.

The term "Internet of Things" refers to devices that collect and transmit data via the internet. This includes devices such as cellphones, coffee makers, washing machines, assembly line robotics and almost anything else you can think of!

Learn More

Bluetooth technology sends and receives radio waves in a band of 79 different frequencies centered on 2.45 Ghz. Bluetooth devices have the ability to automatically detect and connect to each other and can pair up with up to 7 other devices and communicate with each of them at the same time. Bluetooth devices can also select channels randomly when two devices want to communicate, a technique known as spread-spectrum frequency hopping. To minimize any chance of interference from other devices, paired devices can shift the frequency that they are using. They are even capable of shifting frequencies thousands of times per second. A group of paired devices may also share information with each other and can form a mini network called a piconet. Devices can join or leave the piconet at any time.

Chapter 9: Bluetooth Capabilities

Enterprise-class access points may feature Bluetooth Low Energy radios and antennas to function as beacons in high-density AP deployments. Bluetooth LE is designed to consume very little power while sharing tiny packets of data to smart phones, tablets, fitness bands, and other similar devices. Its primary use case on access points is for location analytics.

Bluetooths are used to connect computers and electronics devices on the fly to share small amounts of data over short distances. Whereas WiFi is used to transmit large amounts of data between computers and the over longer distances. Bluetooth's capability to connect and communicate with numerous devices makes it easier for those devices to work together without needing to communicate via WiFi which would dramatically increase the volume of traffic on the network.

Bluetooth technology does not compete with WiFi. It is complementary to WiFi technology.

Chapter 10

RF Optimization

Radio frequency optimization is a process that is used to improve not just the coverage area of a network but also the quality of signal. Measuring and testing network equipment during the design and test deployment is a critical component of the network design process.

WiFi communications use the 2.4GHz and 5GHz radio bands with each band divided into multiple channels (allowable channel usage is regulated by country). The 2.4GHz band has a much larger range than 5GHz and is much better at penetrating walls. However, it is highly susceptible to interference due to only having three non-overlapping channels. The 5GHz band is less congested because it has more usable channels to work with but these are reduced by channel bonding required for higher throughput technologies.

This is less of an issue in urban areas or high-density AP deployments because of the reduced range. Some of the 5GHz channels are designated as dynamic frequency selection or DFS channels, requiring devices to use dynamic frequency selection and transmit power control to avoid interference with weather radar systems. These restrictions have changed over time and are evolving.

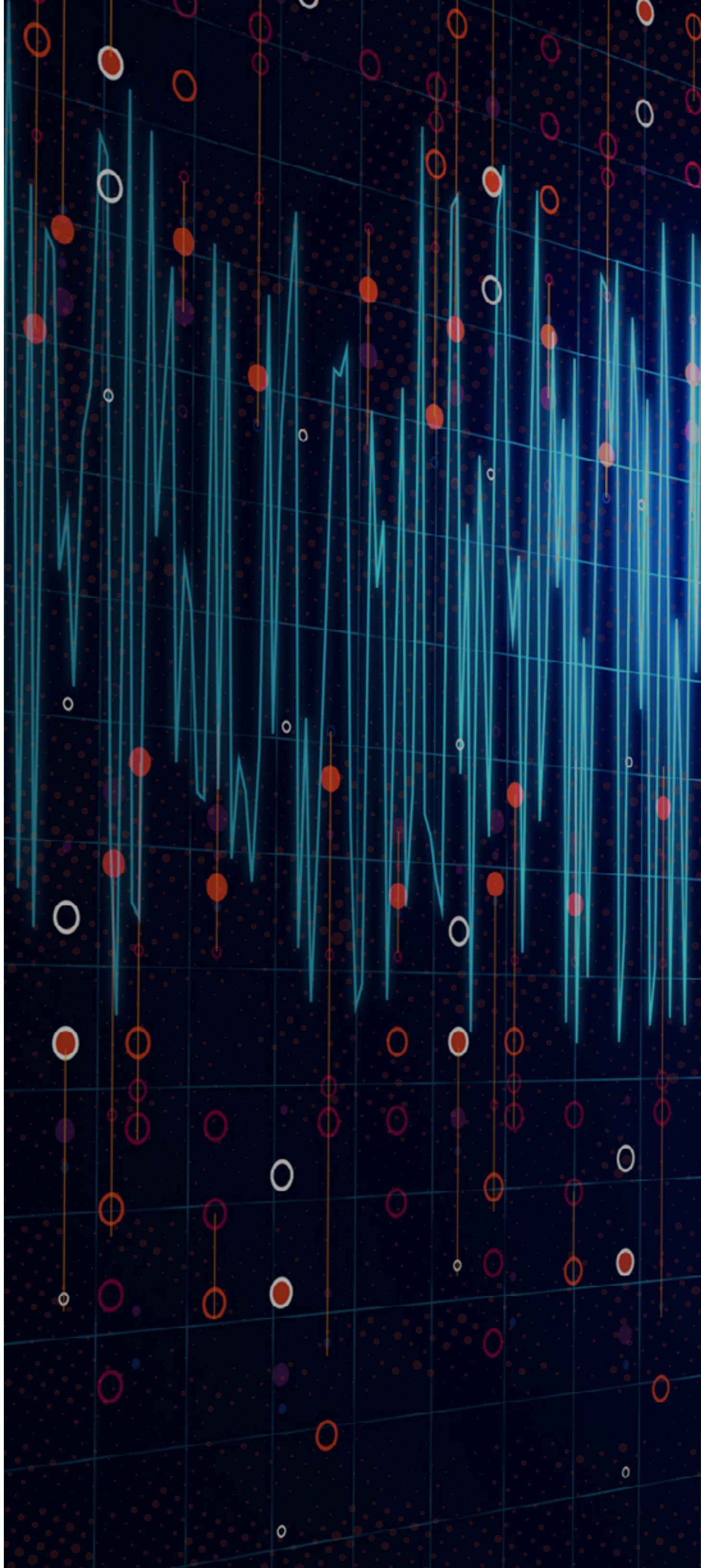
All modern enterprise-class access points feature some form of RF optimization capabilities, often with dedicated radios for scanning the environment. These APs will usually ship with automatic channel and power adjustment turned on by default. The AP will dynamically adjust its power output and channel to minimize interference. Channels and power may need to be manually set in some environments.

Success Strategies for Channel Planning

Channel planning can also be included with an AP deployment design.

Here are a few tips:

- Perform a wireless site survey prior to designing a predictive access point layout.
- Access points should be appropriately laid out with overlapping coverage cells, but they should not be located too closely together.
- Each AP's coverage cell should be on a different channel from the one it overlaps while also taking in the RF environment results from the site survey.
- Some devices, such as WiFi phones, are very sensitive to environments with RF interference and often require channels and power output to be set manually.
- DFS channels and high throughput modes may need to be disabled as well.



Chapter 11

VPN and SD-WAN Capabilities

The choice between a VPN (Virtual Private Network) and SD-WAN (Software-Defined Wide Area Network) is an important decision and one that is not necessarily based on cost. Factors to consider should include network performance, network type, and whether the network is managed in-house or outsourced.

VPNs provide many different things. Primarily, they offer individuals and corporate entities a means with which to create a privatized, selective network, for the purposes of communication, connectivity, sharing and accessing data, and multiple security features. Utilizing a VPN can provide encryption during data transmission, which protects sensitive data from nefarious sources. VPNs can also provide users access to localized services, allowing remote employees to interface with resources usually only available locally. Beyond the capabilities of security, the extra layer, or possibly layers, of authentication, a VPN is incredibly flexible in its use-case.

SD-WAN is a large portion of SDN (Software Defined Networking), and is the evolution of the VPN. Its main focus is to connect large networks together, regardless of distance. The approach is a cloud-based solution, and while it carries all the benefits of traditional VPNs, it isn't burdened with some necessary hardware and routing solutions. It can handle a variety of connection types including legacy and even mobile connection integration. With major security features and virtualization, SD-WAN is far easier to deploy on a large scale. Whether it's being used as an internal resource, or as infrastructure to provision for a customer, SD-WAN has a far broader scope than past methods of wide-ranging connectivity.

In Summary

The needs and requirements of every network are different, and a cookie-cutter solution is not a good choice for most companies. You will want to choose tools and technologies that best match your goals and objectives for your network. It may even help to consult with network engineers who have designed and deployed networks for environments similar to yours. We can help by taking a look at your network and making recommendations that are customized for you.

federated®
SERVICE SOLUTIONS

Whether it's advanced network design, hardware upgrades or low voltage cabling, we follow the same, proven process on every project to establish consistency and provide a seamless customer experience. Our proven process has ensured success for our clients, from small businesses to global corporations. At FSS, we work with you to identify and prioritize your needs at every stage of your project, so we can achieve success together.

Ready to get down to work? Contact us:

(248) 539-9000 | networkheroes@federatedservice.com