White Paper

# Best Practices for Your Next Network Refresh

## An Investment in Optimizing IT Infrastructure

# INTRODUCTION

Your network is the backbone of your IT infrastructure. But as business operations evolve, so do the requirements for the speed, reliability, and security of your network and all its components.

There are several components of the network including the hardware, software, protocols, and the connection mediums. Two key hardware components of the network are the switches and the wireless access points which connect devices to the network and to each other. Whether you are considering a network expansion, a replacement of EOL/EOSL equipment, or a full upgrade, this White Paper will address considerations for selecting network switches and wireless access points and best practices for your next network refresh in today's hybrid work environment.

# CONSIDERATIONS FOR SELECTING THE RIGHT DEVICES

## Switches

Not all switches are the same. The cost of the switch often directly correlates to the functionality and quality of the switch. Switches vary based on the network speed that they offer and their capabilities. It is important to consider the requirements and user demands on the network when selecting a switch for your organization.

A poor-quality or malfunctioning switch can cause problems on the network beyond just the cost and time of fixing the switch. It can create unrelated problems on the network which can cause productivity loss for both your IT team and your end-users. Higher quality switches are less likely to fail and come with tools that help administrators troubleshoot problems that may arise.

Your budget will always be a factor in selecting the right switch for your network, but there are other considerations such as performance, configuration, and scalability that come into play.

**Performance:** Each switch comes with a connection speed and processor which manages the data flowing through the switch. The latency of the switch is the time it takes for a user to request access and see a result. As latency increases, employee productivity decreases and the odds of employee frustration increases. A switch that minimizes latency-based problems is ideal.

**Configuration:** Switches vary by their flexibility for configuration and features. For instance, ***Modular Switches*** offer the greatest flexibility and are best for addressing changing network requirements but come at a higher cost. ***Fixed-Configuration Switches*** include low-cost *unmanaged switches* which are designed to be plug and play (no configuration needed), *smart switches* which offer some management, segmentation and security capabilities, and *managed switches* which have advanced capabilities and features for control and management of the network, security, and scalability.

**Scalability:** As your business grows, your requirements for your network may grow or change. Adding switches to the network could negatively affect the bandwidth of the network, so it is important to design a network and select switches that allow for multiple switches to be configured together, such as a switch stacking solution.

## Wireless Access Points

There are also important considerations and parameters for selecting new wireless access points or choosing to refresh what is currently in place.

**Range:** The range is the coverage area of the access point. Selecting an access point that can cover a larger area could have cost benefits for an organization, but consideration for the number of access points should be balanced with the risk of devices trying to connect and getting a bad signal.

**Guest Access:** Modern access points can apply corporate security policies ensuring that your network is protected from unsafe devices.

**No Hardware Controllers:** New access points use software-based controls within the network and don't require external controllers, which also reduces the possibility of hardware-related failure.

**Cloud Management:** Today's access points allow for system administration through the cloud, allowing them to be accessed and managed from anywhere.

**Wi-Fi Technology:** Select your access point technology based on your business need. Mesh technology can provide a cost-effective alternative to connecting the WLAN via ethernet. MIMO technology increases the number of simultaneous users a single access point can support and is a major part of Wi-Fi 6 (802.11ax) protocol. Power over Ethernet (PoE) technology should be considered for every network refresh. Not only does it help to reduce infrastructure costs by removing the need for an independent power supply, it has also become standard for enterprise wireless networks using Wi-Fi 5 and Wi-Fi 6 access points which require more than 30 watts of power to support applications and devices such as HD/4K video displays, point-tilt-zoom cameras, POS systems, and numerous other IoT devices.

As Wi-Fi standards continue to evolve, adoption of Wi-Fi 6 will improve high density performance and provide faster throughput speeds designed for newer technologies such as IoT connections. It will also provide backward-compatibility with earlier Wi-Fi standards.

The Wi-Fi 6E extension supports Wi-Fi 6E devices. Wi-Fi 6E devices will communicate in the 6-GHz band, which offers more than twice the bandwidth of the 5-GHz band, resulting in faster speeds and less interference for an optimized experience. To take advantage of Wi-Fi 6E and its higher speeds, IT teams would need to upgrade routers, switches, access points, and other critical elements.

**Gain Antenna:** The antenna directly impacts the signal strength and transmission range of a wireless access point. Consider choosing one that contains a booster antenna if your environment requires coverage in spaces such as large warehouses, outdoors, or stadiums.

**Speed:** The rate at which information travels. Wireless access point speeds can range from 450Mbps to 2.3Gbps in older Wi-Fi bands and up to 9.6Gbps in Wi-Fi 6 and Wi-Fi 6E.

## BENEFITS OF A NETWORK REFRESH

A network refresh is designed to make sure that all your networking equipment is updated, supported, and maintained. The refresh allows the company to plan on regular replacements whether the older tech is still working or not. Although companies may consider replacing equipment that still works as an avoidable expense and ultimately put off the project, adhering to a network refresh has some financial benefits and helps to avoid risk.

***When is it optimal to update your networking equipment?*** In relation to switches, the typical refresh cycle is 5-7 years, although some firms may choose the *"if it isn't broke, don't fix it"* refresh strategy and may keep network switches for at least 10 years. In general, wireless access points can last 3-5 years, but recent trends have shown firms outgrowing the devices more quickly due to a need for better coverage, more bandwidth, or more devices accessing the network.

Top 6 Benefits of a Network Refresh

1. Improved security
2. Better uptime/less chance of failure
3. Greater user productivity
4. Scalability for future growth
5. Support cloud-based networks
6. Budget predictability

Outdated network technology increases the chances of security risk, risk of downtime due to outages, and are less capable of supporting today's hybrid workforce and new IoT devices. These risks help to highlight the importance of maintaining or even accelerating one's network refresh schedule.

### Improve Security

Obviously the older your network components are, the more vulnerable your network is to a security breach. Outdated and unsupported components expose network vulnerabilities that can bring down the network and negatively impact your business. When considering new devices such as switches and access points, make sure they meet your requirements for maintenance, support, and updates for greater assurance of your network's security.

### Reduce Outages and Chances of Failure

Outdated components have a greater chance of failure. This causes IT teams to focus more time on fixes and maintenance and less time on strategic IT projects. Additionally, an outage could affect part or even the entire network. Not only does this impact your business operations, but ultimately it can impact your bottom line and your business credibility.

### Increase User Productivity

Today's hybrid workforce has brought new challenges to IT networking. Remote work has become the new normal. It is predicted that remote work will increase by 87% by 2025 compared to pre-pandemic levels[1]. Remote work and the applications needed for communication and collaboration will continue to have a growing impact on the network traffic loads for VPNs and the bandwidth speeds of the wireless access points at the network edge.

Prior to today's hybrid work model, users accessed the network through firm issued devices. Now many users access the network with their own devices and often use a variety of different devices from personal laptops, phones, tablets, and even smart watches. As employees "return to work" or continue to work remotely, they need the flexibility and speed to do their jobs on whatever device they are using and regardless of where they are connecting. But older wireless network equipment and configurations with network switches may not be equipped to fully support newer devices and demand. Any resulting delays and lags on the network can cause frustration and decreased productivity.

### Scalability

As industry standards change and new devices and technology enter the network, older hardware may not be able to support them efficiently or eventually at all. For instance, the growth of IoT devices has brought new challenges to the security and scalability of the network. IoT device technology is expected to grow to 14.4 billion active connections in 2022 and to 27 billion connections by 2027[2]. But these devices may lack strong built-in security or may not have robust authentication, making them greater targets for attacks. And because IoT devices are often located in public areas they are more susceptible to probing, manipulation, and network breaches. Planned network refreshes make it easier to scale to meet increasing demands on the network, support modern applications, and take advantage of the benefits of the cloud and IoT technology.

### Supporting Cloud-based Networks

Both hybrid cloud and multi-cloud environments rely on switches to support connectivity to and from the cloud and within each cloud. Migration to cloud networking offers several benefits including broader visibility and control of all devices and users on the network regardless of location, simpler configuration, and regular vendor updates and enhancements. With any network refresh it is important to consider the benefits of the cloud and centralized cloud management tools to manage and control wired and wireless LANs through a single pane of glass.

### Budget Predictability

Instead of not being ready for an unexpected expenditure, a regular technology refresh cycle prepares companies to plan purchases in advance and adds stability to long-term budgets. It also ensures a smoother process and selection based on informed choices rather than urgency.

## CONSIDERATIONS FOR NETWORK AS A SERVICE

Network as a Service (NaaS) offers companies an option to operate their own networks efficiently without having to internally maintain their network infrastructure. Maintaining internal WANs require regular maintenance and upgrades to aging network hardware. NaaS allows enterprises to consume and optionally outsource the full lifecycle of their enterprise network deployment, with all hardware, software, licenses, and services delivered in a flexible consumption or subscription-based offering. Benefits include:

**Lower Cost:** A NaaS solution reduces capital expenses related to infrastructure hardware, software, and operations. The monthly consumption model also creates more predictability for the IT budget.

**Proactive Network Monitoring:** NaaS solutions provide insight and visibility into the network and can predict network issues early on using proactive monitoring. This eliminates your IT team from spending time troubleshooting the network.

**Optimize Performance:** NaaS solutions can ensure your network traffic is operating efficiently. It can be designed to prioritize and route network traffic as appropriate for optimized performance.

**Improve Security:** A NaaS solution can provide best practices for IT security utilizing hardware and software platforms and policies tailored to the needs of your organization.

## SELECT VANDIS FOR YOUR NETWORK REFRESH PROJECT

Because a network refresh is a complex undertaking that can bog down internal IT teams, it is critical that your investment in your network refresh project get the time and expertise it needs to be successful. Vandis' team of experts will help to minimize the risk and downtime that is often associated with network refresh projects. The Vandis' professional services team will take a security-first approach to your project and will advise on the right technology, plan and design your network, and incorporate the new solutions in line with best practices.

Alternatively, Vandis' managed services team can provide a NaaS solution to free up the costs associated with maintaining your own IT infrastructure; allowing your existing IT team to concentrate on your organization's strategic goals and business growth.

For nearly four decades, Vandis has been a trusted partner to our clients. We offer Managed Services and IT Solutions that optimize the security and performance of network infrastructures, both on-prem and in the cloud. Leveraging deep subject matter expertise, we design IT solutions to meet each organization's unique needs and goals.

To learn more about how Vandis can assist your organization visit
www.vandis.com/services/naas/ or call (800) 397-3146!

Source:

1. Flexjobs: Remote Work Statistics
2. IOT Analytics: Number of Connected IOT Devices

VANDIS