aruba
a Hewlett Packard Enterprise company

MIDSIZE BUSINESS SELECTION GUIDE

CHOOSING THE RIGHT ETHERNET SWITCH

As your business continues to grow, the need to hire more staff, support more customers, or expand into new ways of working grows along with it. This means more demand from devices, connections, and data sources is placed on your network infrastructure.

But is your wired network ready to handle the extra load?

While choosing the right Ethernet switch for your network can be challenging, knowing where to look and what variables to consider can make a daunting task much easier to manage.

Here are some helpful questions (and responses) to guide you along the way.

WHAT TYPE OF SWITCH DO YOU NEED?

There are three kinds of switches you may need for your network. What you choose and how many you will need will depend on your network size, your plan to scale, and the job you need them to perform to support your business goals.

Access switches

Access switches sit at the edge of the network, often where the most data originates. Their job is to connect users, wired client devices, and infrastructure equipment to the network. Some infrastructure equipment, like Wi-Fi access points, security cameras, and voice over IP phone systems, can receive data and power over an Ethernet cable to simplify deployment.

Aggregation switches

Aggregation switches connect access switches together, aggregate outbound traffic, and distribute data across the network edge and to the network core. To effectively manage traffic volume, these switches often have multi-gigabit ports, redundancy features, and deeper Layer 3 routing capabilities.

Core switches

Core switches sit at the heart of the network, typically connected to a router or gateway. They manage traffic coming to and from aggregation switches, the wide area network (WAN), and the internet. High availability, deep management capabilities, and fast throughput performance are required to ensure the smooth operation and integrity of the entire networking infrastructure.

HOW MANY PORTS DO YOU NEED?

Each switch has a maximum number of Ethernet ports, regardless of its type. Most switches support anywhere from eight to forty-eight wired connections. If you need more ports, you can connect multiple switches to form a stack, letting you manage connected switches as if they are a single, large switch.

When considering a set of access switches, you'll need to know the number of devices you plan to connect now and in the foreseeable future. It's always better to account for more capacity to have room to support growth.

In a larger network, you'll need enough Ethernet ports on a core switch to accommodate all your aggregation switches and enough ports on aggregation switches to support all your access switches connected downstream.

Another way to approach port density needs is with modular chassis switches, which offer the flexibility to physically slot in expansion modules to add more ports for higher switching capacity. Chassis switches often operate as core switches where high availability, redundancy, and scaling can prove mission-critical for ongoing business operations.

HOW MUCH PERFORMANCE IS ENOUGH?

After determining device count and port density needs, the next step is to understand how much bandwidth each part of your network should support.

Consider the types of software running on each device and the function of its user, then calculate the average volume of traffic each device will generate. You may already have these numbers with the help of your current networking equipment or a network analyzer tool. Be sure to consider how these numbers might change along with business and operational growth.

The maximum throughput requirements for each part of your network will determine how much total switching capacity is needed and how fast each Ethernet port should be for each switch in your deployment.

In addition to regular Ethernet access ports, switches of all kinds have uplink ports to help connect switches together, combining and passing traffic within and between the access, aggregation, and core network. For that reason, uplink ports usually support faster speeds than access ports on the same switch, ranging from 1 to 100 Gigabits per second (Gbps) or more in comparison to 1 to 10 Gbps.

Depending on your throughput calculations, you may need a higher-capacity switch for some parts of your access or aggregation network. You may also want to consider establishing service level expectations to keep client network demands within a resource budget, preventing a subset of devices from soaking up more than their fair share of bandwidth. Features like traffic prioritization, strict priority queuing, and rate-limiting are great ways to ensure each client receives an appropriate quality of service.

Wherever you draw the line on performance, look for switches that can support average traffic needs and foreseeable demand fluctuations while still having room for growth.

Consider the following as you build out your plan for network performance:

Expanding support for Wi-Fi 6

Wi-Fi 6 and 6E access points are more likely to be limited by a one Gigabit Ethernet port and may instead need a larger, 2.5 Gigabit backhaul connection to support unimpeded traffic flow for the client devices they're servicing.

Increased use of video conferencing

Zoom, Skype, Teams, and other video conferencing apps can put a sudden strain on network bandwidth availability. They are also latency-sensitive and need more network resources as more people join a call, resulting in jittery video and incomprehensible audio when supply does not meet demand.

Adopting Internet of Things devices

Smart locks, sensors, and other IoT devices may not need exceptional bandwidth, but their efficacy can be compromised because of latency issues and network congestion. This could translate into slower processing time, literally leaving employees waiting at the door.

DO YOU NEED POWER OVER ETHERNET?

Phone systems, access points, security cameras, and other connected devices can often accept both data and power through a connected Ethernet cable. Many switches support this use case through Power Over Ethernet (PoE), which can help simplify installation, deployment, and maintenance.

The first step is to know how much power you need to provide to each connected device. Wi-Fi 6E access points may need 30W of power or more whereas voice over IP phones, security cameras, or other powered devices (PD) may draw less than 15W. Finding this information can be as easy as looking at the specifications sheet for each PD on your network. Once you know each PD's power consumption, you can calculate the total power budget required and find a switch that can support your environment.

Keep in mind that switches with more power available on each port can supply power to PDs that need less. Conversely, an underpowered device may function poorly, if at all, so it's always a good idea to consider loss and overhead.

HOW CRITICAL IS NETWORK UPTIME?

Different parts of your network may have different requirements when it comes to availability and uptime. Understanding the business impact of unscheduled network downtime and maintenance can help as you think about redundancy needs.

Some switches, for example, can provide always-on power to connected PD's, keeping them running even during software updates. This can be useful for preventing blind spots in a deployed security camera system that monitors valuable assets and equipment.

Switch stacking builds resiliency into your deployment. Stackable switches behave like a single physical switch with a single IP, simplifying network configuration, administration, and system monitoring. If one switch goes down, another switch can take over to keep data flowing through the stack.

Planning to include hot-swappable hardware components is another way to build resiliency in your deployment. Redundant power supplies and management modules help minimize downtime by making it a snap to fix without having to replace the entire switch.

HOW IMPORTANT IS NETWORK SECURITY?

As companies adopt technology to address business needs, they continuously face new security challenges. From personnel-owned mobile phones to connected cameras and autonomous IoT equipment, allowing new devices onto the network can change and increase the attack surface, requiring IT professionals to re-think risk mitigation plans.

When combined with malicious intent, common network threats like unauthorized access to data and leaks of privileged information can be damaging and even catastrophic to business operations. Despite the significant degree of human error involved in security breaches, your switches can support risk mitigation efforts.

The myriad of methods to help prevent unauthorized access include an Access Control List (ACL) and Terminal Access Controller Access-Control System (TACACS+). An ACL lets you create rules for filtering traffic based on identity markers like source IP address, destination IP address, and subnet, whereas TACACS+ provides a way to authenticate and authorize remote users.

Another common way to mitigate risk is through Layer 2 and Layer 3 segmentation strategies like creating subnets and private VLANs. Separating guest traffic from IoT device traffic and both from your production network can significantly reduce attack surfaces in the event of a breach.

In larger network deployments with limited IT support, the above strategies may become too complex to manage. This is where embracing adjacent hardware and integrated services like dynamic segmentation can be a big help, streamlining the ability to centralize, segment, and enforce role-based policy while reducing manual workload.

The right switch for your deployment should support company security stances, give the right degree of control over network privileges and policies, and deliver the right amount of access for your people to be productive while mitigating the most risk.

HOW DO YOU PLAN TO MANAGE THE NETWORK?

No matter the switch, its management interface is where most IT staff will spend their time when it comes to deploying and configuring new hardware, onboarding and assigning policy, and implementing changes as a result of data-informed insights and troubleshooting.

For many, management can be a question of preference and habit. Command Line Interface (CLI) used to be the clear winner for IT professionals. However, as networks, deployments, and commands become increasingly complex, network operators can face a significant time investment along with the greater risk and consequences of human error. Embedded web UI reduces the dependence on CLI while maintaining localized control and simplifying configuration to point-and-click.

Modern networking equipment offers on-premise and cloud-based management solutions with centralized control for switches, access points, and other hardware. Simplicity and usability are often maintained or further improved with the transition from web UI to software and apps. This includes the added value of having better scalability, convenience, and analytics, reducing IT troubleshooting workload, improving real-time reporting, and accelerating insights at the cost of a subscription.

ARUBA SWITCHING FOR MIDSIZE BUSINESSES

With Aruba, you can put your network to work for you, using smart, scalable, secure switches that keep your business in the fast lane.

Aruba switching solutions range from entry-level access to speedy aggregation and resilient core switches that are easy to deploy, scale, and manage through a single pane of glass without disrupting your day-to-day workflow.

Resolve issues faster and free up IT resources to support business growth of any kind, whether that's digital, multi-site, hybrid, or automation. All while keeping your people, data, and customers safe with best-in-class security.

Network switches aren't one size fits all. Whether you're expanding your edge, aggregation, core, or all the above, Aruba has you covered with expertly engineered equipment backed by industry-leading limited lifetime warranty, and global support services with no switch software licensing needed.

Want to learn more? Visit the Aruba website.

Aruba CX Switching		CX 6000	CX 6100	CX 6200	CX 6300	CX 6400
Platform and network services	**Deployment type**	Access	Access	Access	Core, aggregation, access, DC ToR (1 GbE)	Core, aggregation, access, DC EoR/ MoR
	Routing	Layer 2	Layer 2	Layer 3	Layer 3	Layer 3
Scale, performance, flexibility	**Uplink speeds**[1]	1G	1/10G	1/10G	1/10/25/50G	Variable 1/10/25/40/100G
	Gigabit access port count	12, 24, 48	12, 24, 48	24, 48	24, 48	Variable
	Form factor	Compact 1U models	Compact 1U models	Compact 1U models with stacking (8)	Compact 1U models with stacking (10)	Modular chassis: high performance 5 slot (7 RU) and 10 slot (12 RU)
	Smart rate: Multi-gigabit ethernet				●	●
High availability	**Wi-Fi 6 ready with Always On PoE**[2] (PoE per port / Max PoE)	● Up to 30W / 370W	● Up to 30W / 370W	● Up to 30W / 740W	● Up to 60W / 2880W	● Up to 60W / 8760W
	Stacking (VSF), virtualization (VSX)			● 8 (VSF)	● 10 (VSF)	● 2 (VSX)
	Hot-swappable, redundant power supplies				●	●
	VSX live upgrade					●
Security with segmentation	**VLANs, ACLs**	●	●	●	●	●
	Dynamic segmentation			●	●	●
	VXLAN				●	●
Management, automation, analytics	**Flexible management:** Aruba Central[3] (Cloud & On-Prem), Aruba NetEdit, CLI, Web UI	●	●	●	●	●
	REST APIs, Python scripting	●	●	●	●	●
	Onboard analytics (NAE)			●	●	●

1. 50G connectivity with 50GbE DACs
2. Always On PoE not supported: CX 6000, CX 6100
3. Aruba Central support planned for future release: CX 6000

SLTG_SMB_RVK_110521 a00106898enw EM