2

ARCHITECTING AND SEGMENTING YOUR NETWORK

The way you architect and segment your network can provide the most significant security improvement for the least amount of time, effort, and money. A good network segmentation plan allows you to separate high- and low-risk devices and user types, which informs where you implement other security controls in your environment.

For example, your internet of things (IoT) devices are, in all likelihood, less tested, updated, and maintained than your Windows operating system, simply because the technology is newer and less widely adopted. This fact makes them inherently more vulnerable and less secure than other, more widely used technologies. By putting these vulnerable endpoints onto a logically or physically separate network, you lower the risk of an adversary exploiting them and moving laterally across your network to your computer. Once you've separated your devices, you can consider additional controls—such as an intrusion detection or prevention system—or other network security monitoring and alerting solutions, which we'll cover in **Chapter 10**.

In this chapter, we'll discuss types of network hardware used to segment networks, their strengths and weaknesses, and some recommended solutions and configurations for physically or logically segmenting your network and separating devices utilizing both Ethernet and wireless network devices and settings.

Network Devices

Hubs, switches, and routers can be used to segment a network. Some of these provide more features or are inherently more capable and secure by design. Depending on your needs, you might choose to use one, some, or all of these devices.

Hubs

A *network hub* is the most basic type of device that enables multiple computers to communicate with each another. A hub can be used in small networks relatively safely, whereas in larger networks they would likely cause significant issues. When host A, connected to a hub, communicates with host B, connected to the same hub, the data (packets represented as Ethernet frames) travel from host A to a port on the hub, and the hub then broadcasts that data out through all of its other ports. This means every other endpoint on the network receives the data destined for host B, which isn't very secure. Additionally, because hubs aren't intelligent, all ports are part of the same *collision domain*. This means that if two or more devices attempt to communicate at the same time, the traffic collides, causing network performance problems. When a collision occurs, the sending devices have to stop communicating and wait a randomized amount of time before attempting to communicate again, ideally without causing a second collision, resulting in a further delay.

Because of their limited functionality, hubs are typically cheap to buy and deploy, but they aren't scalable. If you have more than a handful of devices needing to communicate, you're better off getting a switch.

Switches

In contrast to hubs, *switches* forward traffic through a network using the physical hardware (MAC) addresses of the endpoints connected to them. When a host connected to a switch communicates with another host in the network, the data travels from the sender to a port on the switch, and the switch then uses the MAC address for which the data is destined to determine to which port it should forward that data. Switches keep a MAC address table in memory, so they know where each endpoint is located on the network. Each port on a switch has its own distinct collision domain, meaning that if two hosts communicate simultaneously, there won't be a collision—the packets won't meet each other during transmission. This also means that data isn't broadcast to every device on a network, which makes a switch inherently more secure than a hub.

Switches can be used in networks of any size. Small networks rarely need more than a single switch, depending on the number of endpoints.

Routers

A *router* is primarily used for transmitting data between networks or network segments. For example, your local intranet, where all of your endpoints are connected, is a private network. The internet, a very large, publicly accessible computer network, is separate from your private network. A router is the conduit between these two networks, enabling you to access one from the other and browse the internet. Where a switch uses MAC addresses, a router is primarily concerned with IP addresses. All internet-connected networks use a router of some type. In a small network, the border router that connects your network to your internet service provider is likely the only router you'll need.

Creating Trust Zones

Network segmentation is the practice of dividing a network into smaller parts, known as *subnets*, to increase the overall performance and security of that network. You can segment your network by separating devices either physically or logically.

Physical Segmentation

Arguably the simplest way to segment your network is to separate devices using physically discrete hardware (*physical segmentation*). For example, you can use one wireless router for your computers and another for your mobile devices. Or you might use the first router for all your personal devices and the second for all your IoT devices.

Separating your devices and users into classes or categories puts them into *trust zones*, which keep your most critical data and assets separate from more vulnerable devices. Separating devices that require more security and monitoring from those that require less security, and therefore less overhead to maintain, allows you to spend more time focusing on the assets that matter and less time managing those that don’t.

By keeping devices of different types separate, your network’s security increases, as an attack focusing on one type’s vulnerability doesn’t allow the attacker to move to other segments of your network. This is becoming more important as household appliances are gradually turning into smart devices.

Physical network segmentation is harder for an attacker to overcome than logical segmentation. The drawbacks associated with physical segmentation are increased administrative overhead, hardware cost, and other infrastructure costs, as you might need a separate internet connection for each physical network.

Logical Segmentation

Logical segmentation is more common than physical segmentation and often less expensive to implement because it doesn't require separate pieces of physical hardware for each network segment. Logical segmentation is usually achieved using *virtual local area networks (VLANs)*: groups of systems that appear to be on the same local area network but are logically separated from systems on other VLANs. Switches capable of creating and managing VLANs are called *managed switches*. Each VLAN acts like a virtual switch that exists within your physical switch. Assigning a physical port on your switch to a particular VLAN is equivalent to plugging a cable into a specific switch.

For example, you can place a switch, like an eight-port Netgear GS308E (or similar), behind your broadband router, allowing the endpoints connected to the switch access to the internet. Then, on the switch itself, you can create VLANs with different purposes, such as a management or administration VLAN, a business or personal VLAN for your primary endpoints, and a guest VLAN for less-secure device types such as mobile and IoT devices.

With the VLANs created, you can specify which of the eight ports on the switch are capable of communicating on each of these VLANs, keeping each of the VLANs and their respective devices logically separated with just one physical device. Of course, this approach works best for networks with more Ethernet or hardwired devices than wireless devices, unless you plan to use multiple wireless access points.

#11: Segmenting Your Network

The recommended approach for network segmentation in small networks is to categorize your endpoints into trust zones based on the type of access and level of security and monitoring they require.

For example, your primary network segment should include your primary devices, which contain or have access to your private data such as your email, contacts, messages, and data stored in cloud services like Google Drive or Dropbox. This network segment is designed to be the most secure, with the strictest security requirements and the most monitoring and detection in place.

Your secondary network segment is for those endpoints that don't need to talk to your primary devices or access the same data, such as your IoT and other connected devices—smart lights, printers, casting devices such as Google Chromecast, and so on. All of those devices should be separated in their own segments because they're inherently less secure than your primary devices; this mitigates the risk of an adversary using them as a stepping-stone into your network. This network segment can afford to have less strict security controls, because it doesn't contain any critical data or information.

Next, you might have one or more tertiary network segments where all other endpoints live, such as your guest network. Again, this segment can have less strict security controls and less monitoring than your primary network segment.

Finally, depending on the types of devices you have in your network (or plan to have), you might want a network segment that has very strict access rules. This network could be for devices that you do not want to connect to the internet under any circumstances, including CCTV or security cameras. With tight network segmentation like this, other considerations need to be made, such as how devices within this network segment will receive updates.

There are various ways to segment your network. Let's go into more detail about how to achieve effective network segmentation, first by using separate wireless networks and then by using Ethernet segmentation with VLANs. It's possible to combine these approaches if your network calls for it.

Ethernet Segmentation

You can use an Ethernet switch capable of assigning specific Ethernet ports to VLANs to logically segment your network and its devices. An inexpensive managed switch such as the Netgear GS308E provides this functionality, and installing it in your small network is quick and easy. This is the device we'll use for the following example network configuration. You can purchase the GS308E directly from Netgear or other online retailers, or second-hand from marketplaces like eBay. Alternatively, I recommend researching the Ubiquiti range of networking equipment, which, while more expensive, is user friendly and highly capable.

VLANs are used for separating trust zones. Ideally, this is done in larger networks by using two different physical switches. If your switch is misconfigured, the higher and lower security networks and devices might be able to communicate, but if two switches are physically separate, this is less likely. However, in small networks, we usually don't have the luxury of buying multiple devices; it's cost prohibitive. So, we do the next best thing and use VLANs to keep our networks virtually separate.

NOTE *Purchasing two unmanaged switches without advanced functionality like VLANs could be cheaper than a single managed switch with VLAN capability. Taking this route will result in two or more physically separate networks, each with one switch. If both networks require internet access, you'll need separate internet connections for each network, or a gateway device capable of keeping the switched networks logically separate. In this case, you'd be better off investing in the slightly more expensive managed switch in the first place. The use of unmanaged switches is not covered in this book because they are plug-and-play with little additional setup required and will result in a less secure architecture than a managed switch.*

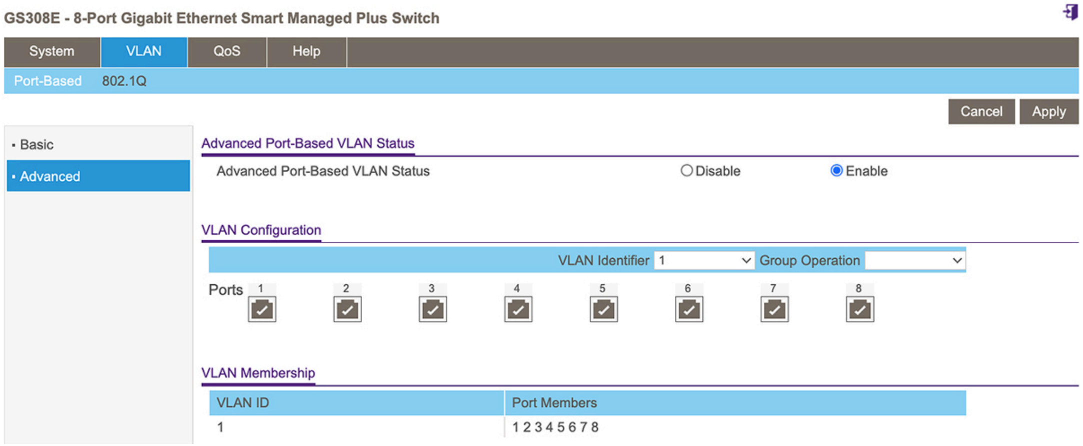
Once you have your switch, initial configuration is usually straightforward:

1. Unbox and plug the switch into power.
2. Connect an Ethernet cable from your modem/router (or whichever device provides your internet connection, like the pfSense device we'll cover in **Chapter 3**).
3. 3. You can find the IP address of the switch in three ways:
    a. The switch will accept an IP address from whichever device in your network provides DHCP. You can find its IP address in your router or other DHCP provider by following the steps in **Chapter 1**.
    b. Netgear (and most network equipment manufacturers) provides an application to discover its switches on your network. You can download the Netgear Switch Discovery Tool (NSDT) from ***https://www.netgear.com/support/product/netgear-switch-discovery-tool.aspx***. Download, install, and run the tool to identify the switch in your network.
    c. The switch is configured with the IP address 192.168.0.239 by default. If either previous method doesn't work, you can use this default IP address to connect to your switch's web interface for configuration.
4. Once you've discovered or configured the IP address for your switch, browse to that IP address in a web browser and log in using the default password (supplied in the switch manual).
5. You'll be prompted to change the admin password. I recommend you do, as default passwords are insecure.

At this point you'll be presented with a summary page that provides the switch information, such as the name, serial number, MAC address, and so on. Add this information to your asset list and network map.

With that done, you're ready to configure the VLANs. The switch will accept and pass through the internet connection to the devices you connect to the switch. Configuring and utilizing VLANs on a Netgear switch is a simple operation, and the method should be similar on any other managed switch:

6. Log in to the switch as an administrator.
7. Along the top of the web interface, locate the VLAN tab, as shown in **Figure 2-1**.
8. In the menu on the left, click **Advanced** to view the Advanced VLAN options.
9. Toggle Advanced Port-Based VLAN Status from Disable to Enable, as shown in **Figure 2-1**.



GS308E - 8-Port Gigabit Ethernet Smart Managed Plus Switch

Advanced Port-Based VLAN Status

Advanced Port-Based VLAN Status ○ Disable ● Enable

VLAN Configuration

VLAN Identifier 1 Group Operation

Ports	1	2	3	4	5	6	7	8
	☑	☑	☑	☑	☑	☑	☑	☑

VLAN Membership

VLAN ID	Port Members
1	1 2 3 4 5 6 7 8

Figure 2-1*: VLAN configuration*

Next, you need to assign the physical Ethernet ports on the switch to specific VLANs. Configure one VLAN for each trust zone you want in your network. If you want a primary network for your most secure devices, a secondary network for your guest devices, and a tertiary network for your IoT devices, you should configure three separate VLANs. If configuring a new VLAN is equivalent to creating a new physical local network, with a new switch or router, assigning a port to a VLAN is the same as plugging a device into that physical switch. If you think about VLANs as separate networks, assigning each port to a VLAN tells the switch to which logical network that port belongs, and only the ports and endpoints within the same VLAN will be able to communicate.

10. In the VLAN Identifier drop-down menu, select the ID of the VLAN you want to configure.

2. 11. For each physical port you want to add to this VLAN, ensure the port is ticked. Untick the ports that will not be allowed to communicate on this VLAN. Click Apply.

When you plug devices into these ports, which now have a VLAN assignment, those devices will communicate only within that VLAN.

312. To remove those same ports from VLAN 1 (the default VLAN), select **VLAN 1** from the drop-down menu. Click the relevant ports until their displays are blank. Click **Apply**.

To test your VLAN configuration, connect an endpoint to one of the assigned ports on the switch, and connect another endpoint to any port that still has the default configuration or another VLAN configured. If you're unable to ping between these devices, your VLANs have been correctly configured.

Summary

In this chapter, you've identified and created trust zones for your devices. By doing so, you've been able to segment your network to keep devices of high trust and security separate from those with lower trust. You can create as many or as few network segments as you like by using a switch in this way, helping to keep your network and your users more secure.