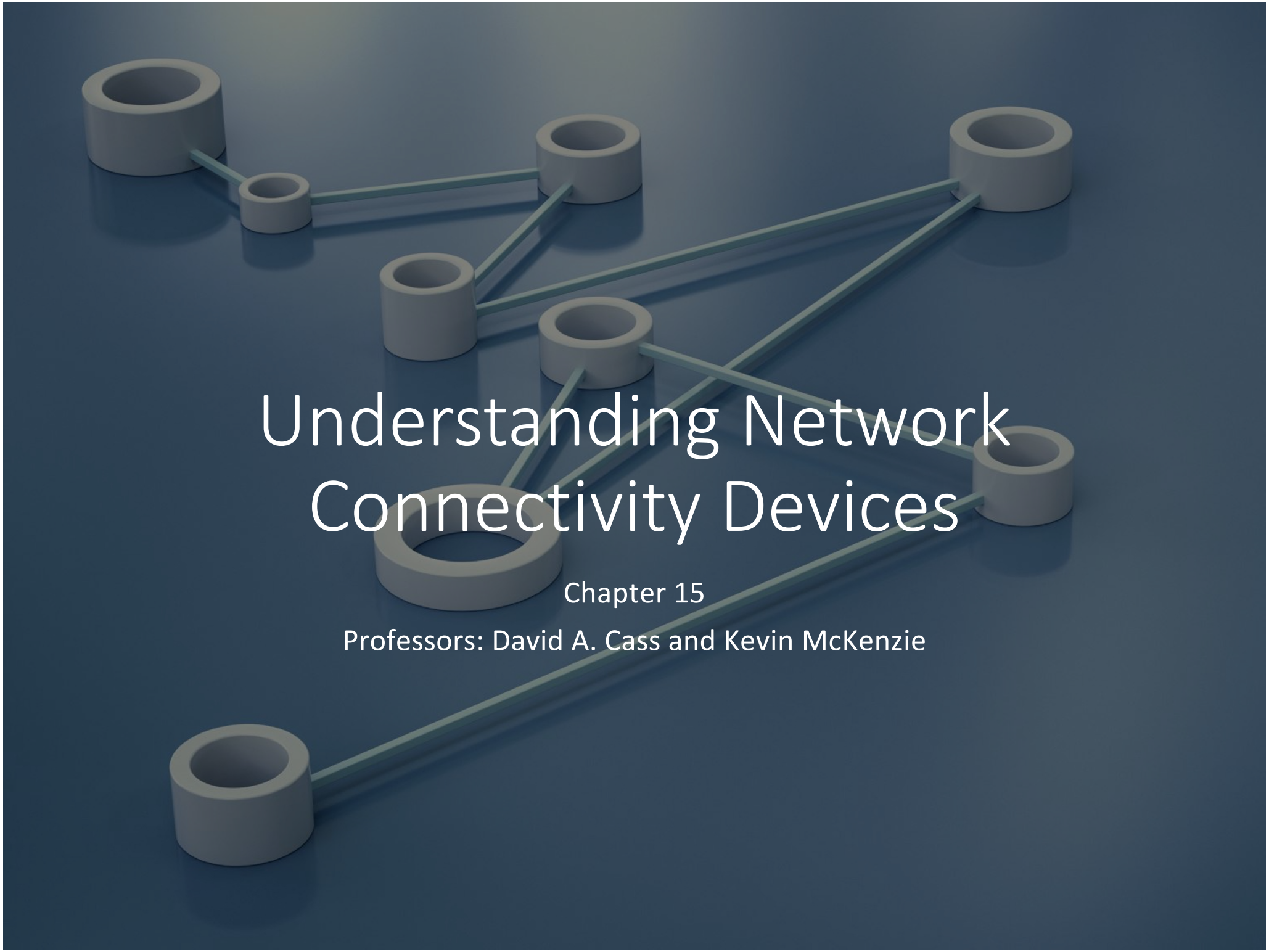


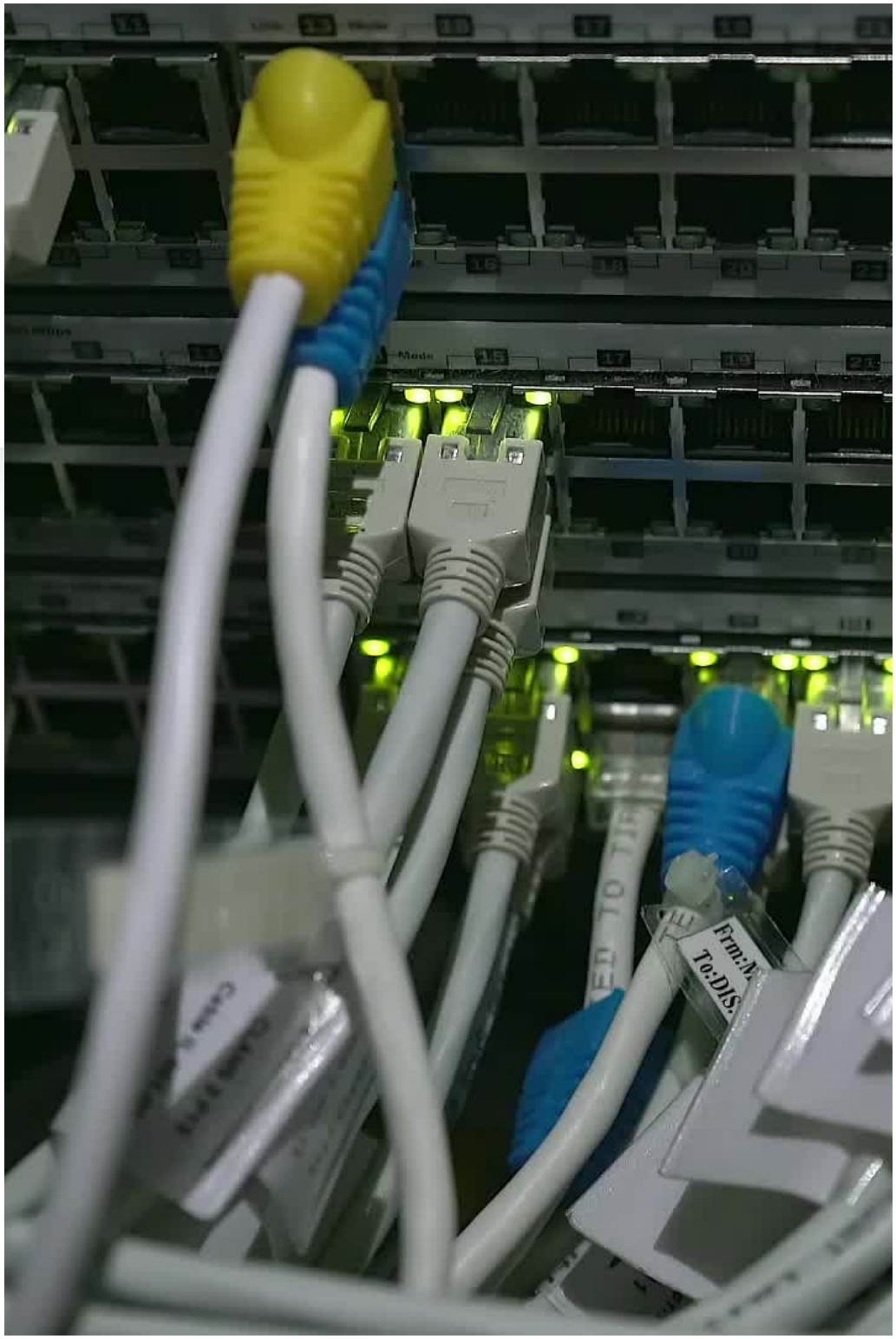
Understanding Network Connectivity Devices

Chapter 15

Professors: David A. Cass and Kevin McKenzie

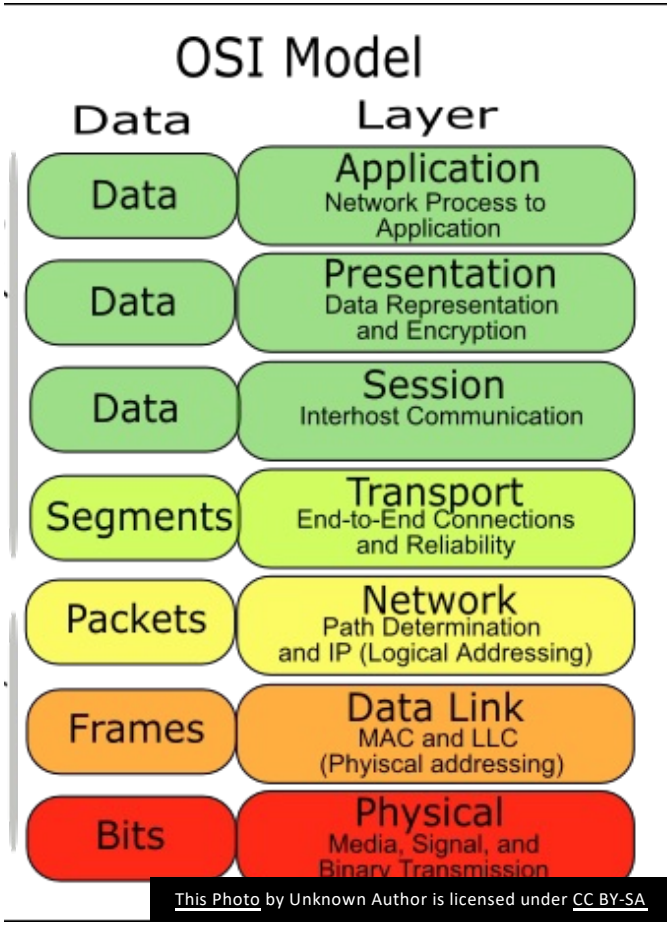
In this chapter, you'll learn to:

- Understand network switches
- Understand routers
- Understand gateways
- Understand network bridges
- Understand network connectivity

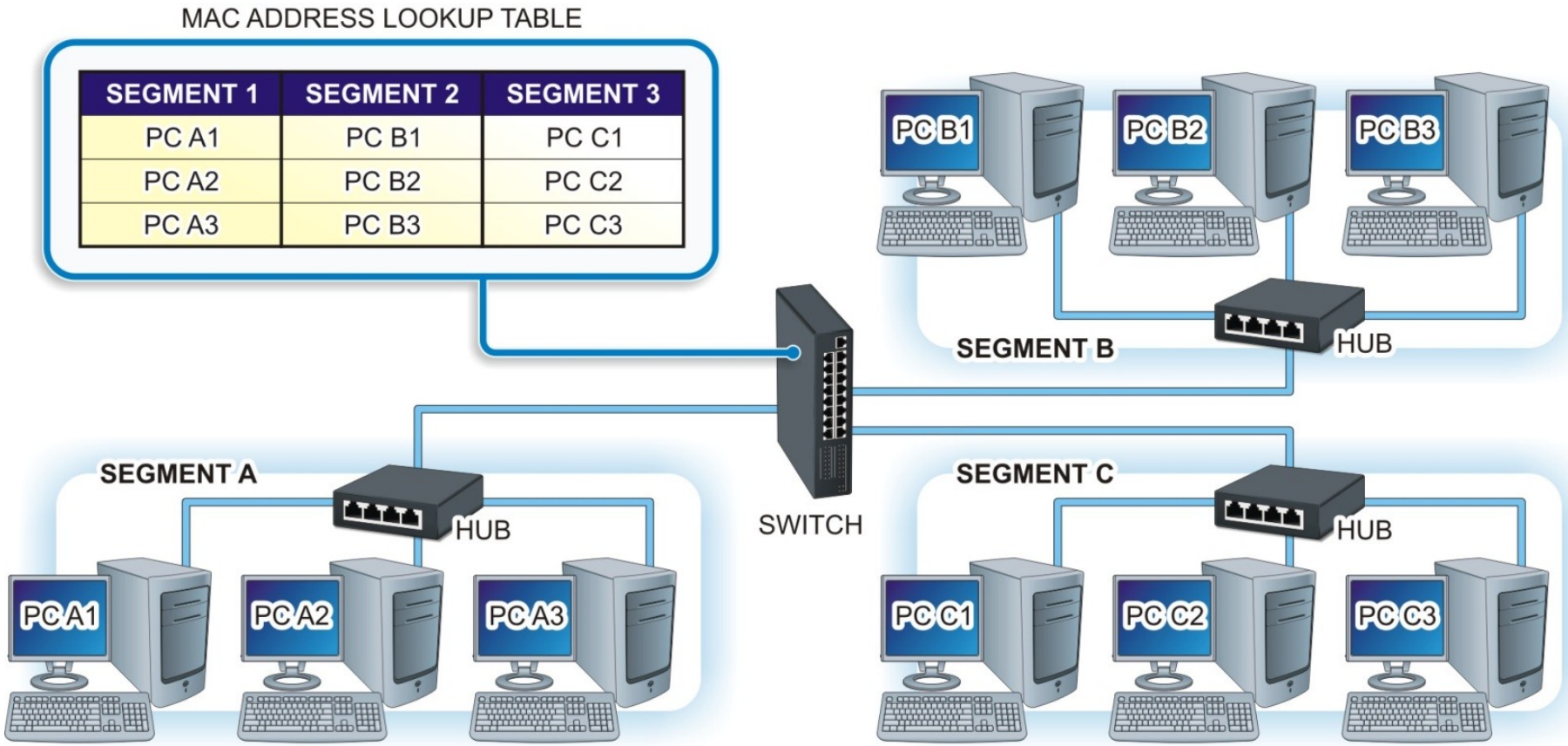


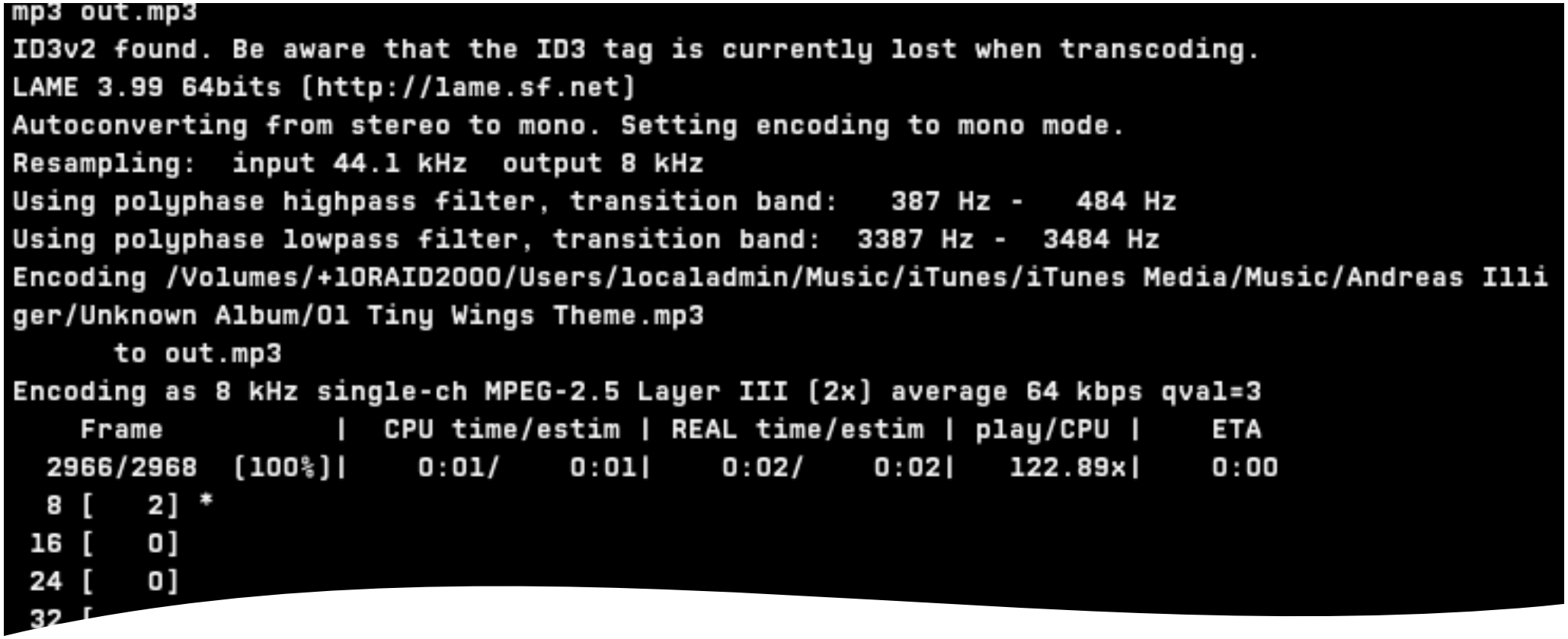
A Word About Network Switches

- Primarily, switches are Layer 2 devices that function at the OSI data link layer. However, there are also Layer 3 switches that act similarly to *brouters* (devices that have the functional capabilities of both routers and bridges covered in the upcoming sections), Layer 4 switches that include Network Address Translation (NAT) capabilities, and Layer 7 (content) switches that distribute content based on server loading factors.



A Network Switch Connection



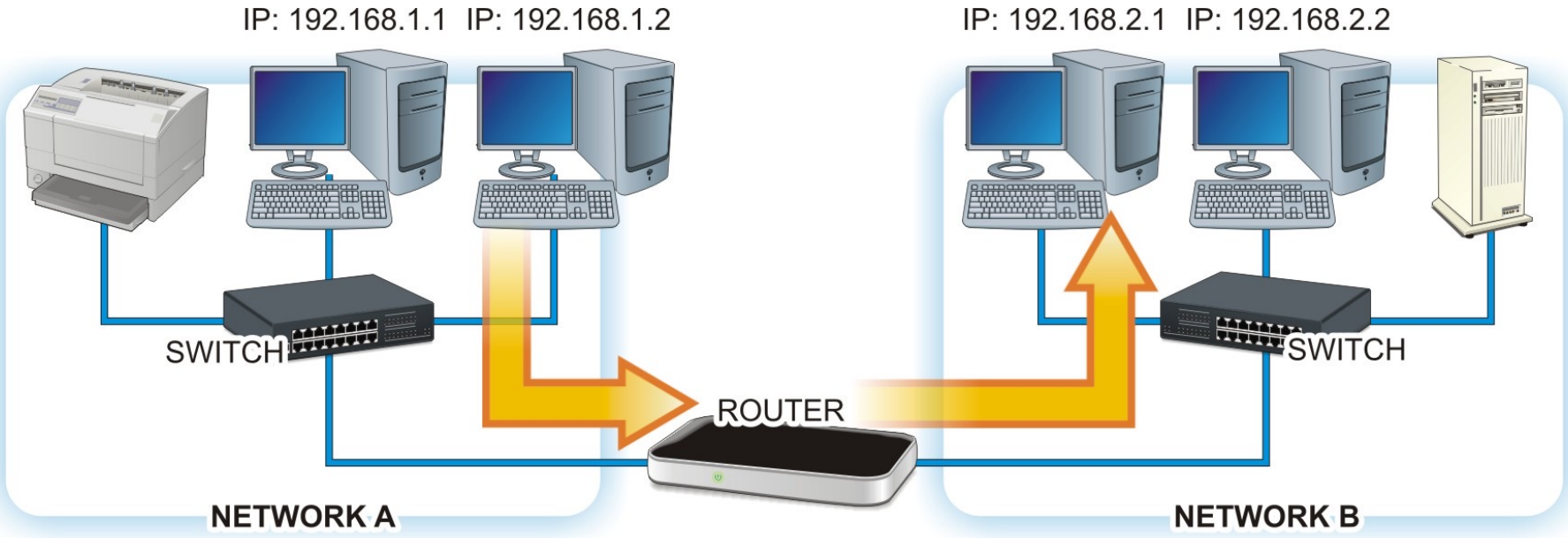


Command-Line Programming

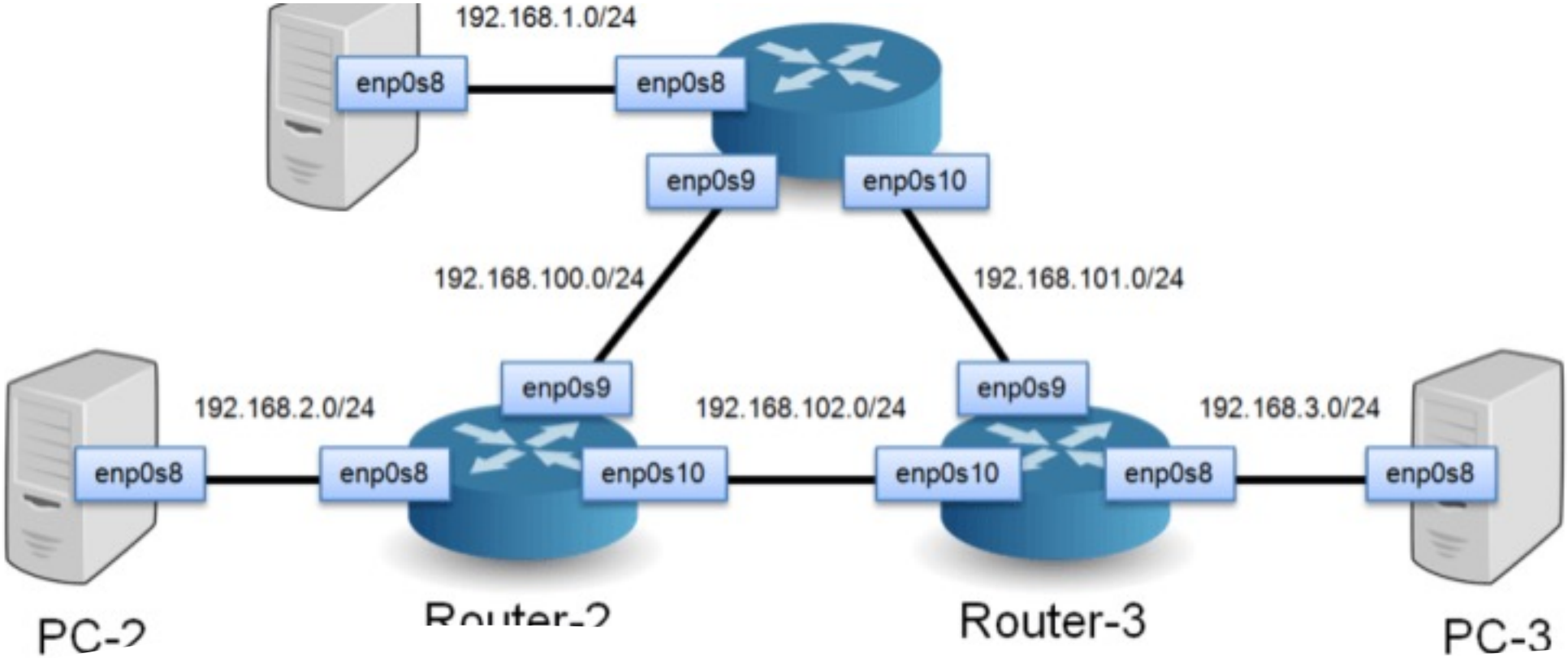
- This format provides a very efficient and direct text-based method of programming the switch's settings. Command-line programming requires the administrator to be aware of the instruction set and parameter variables available for setting the different parameters.

Web Browser-Based Interfaces

- These interfaces provide a more graphical, menu-driven tool for setting key switch parameters. A Simple Network Management Protocol (SNMP) tool is used to permit the administrator to access the switch's parameters through a remote client using its web browser.

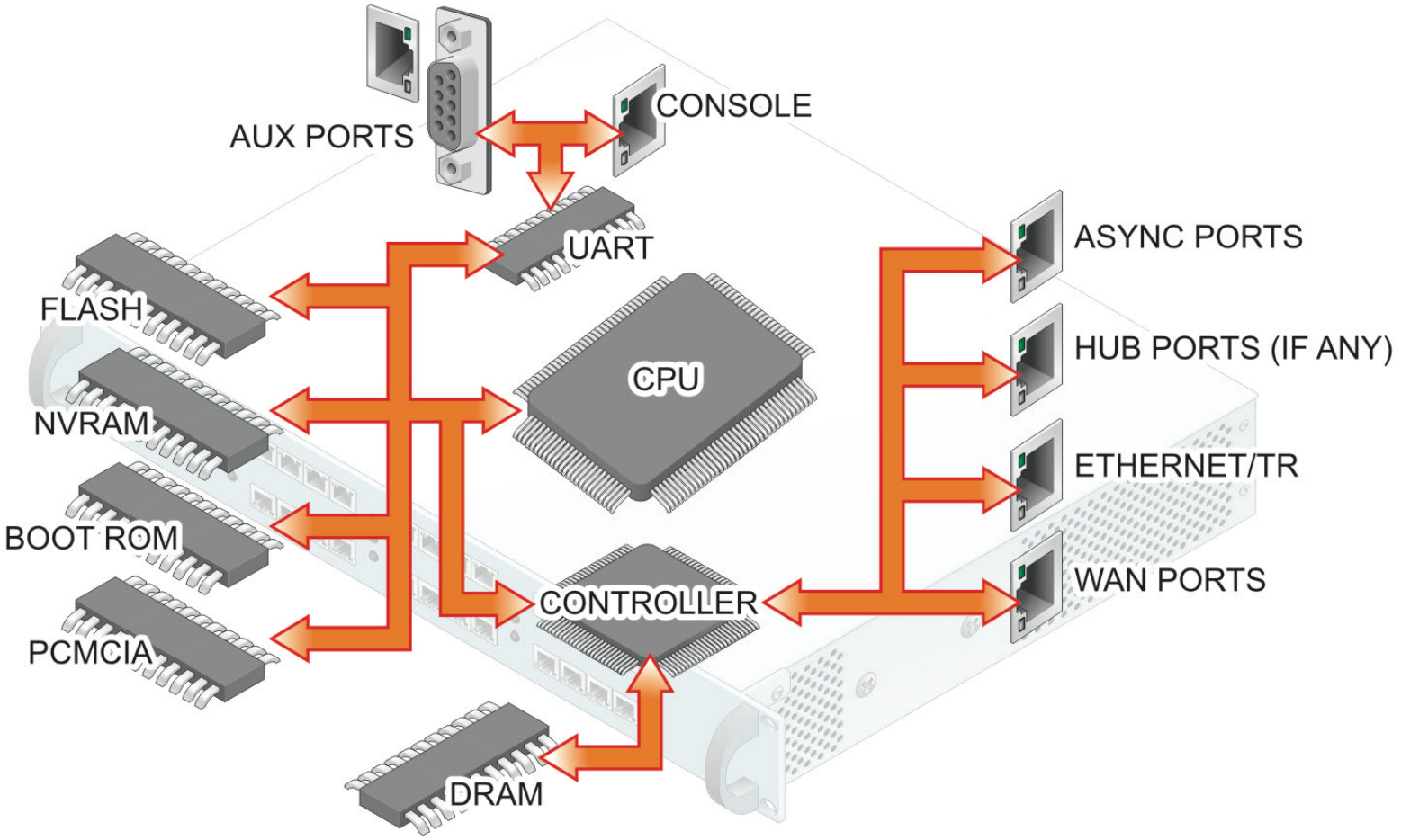


A Network Router



A Word About Routers

- Routers operate from their own operating systems. The most widely recognized router/switch operating system is Cisco System's Internetwork Operating System (IOS). However, many other Linux/Unix-based router OS distributions are available for use.

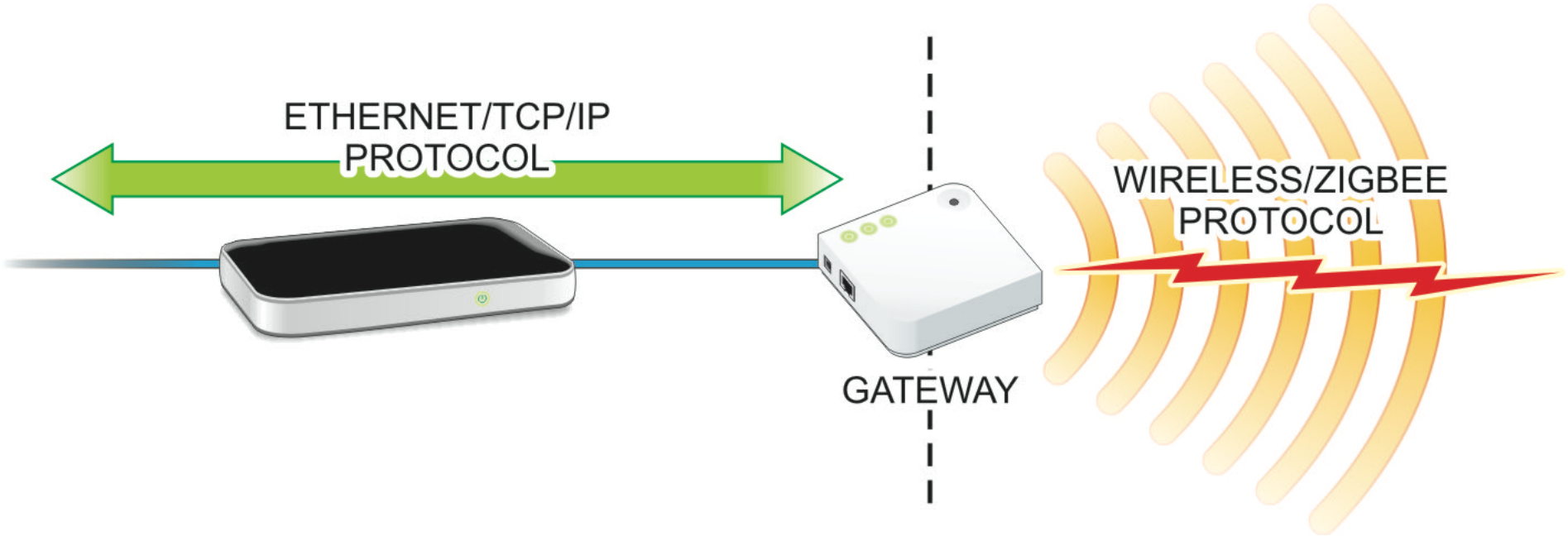


Internal Structure of a Network Router

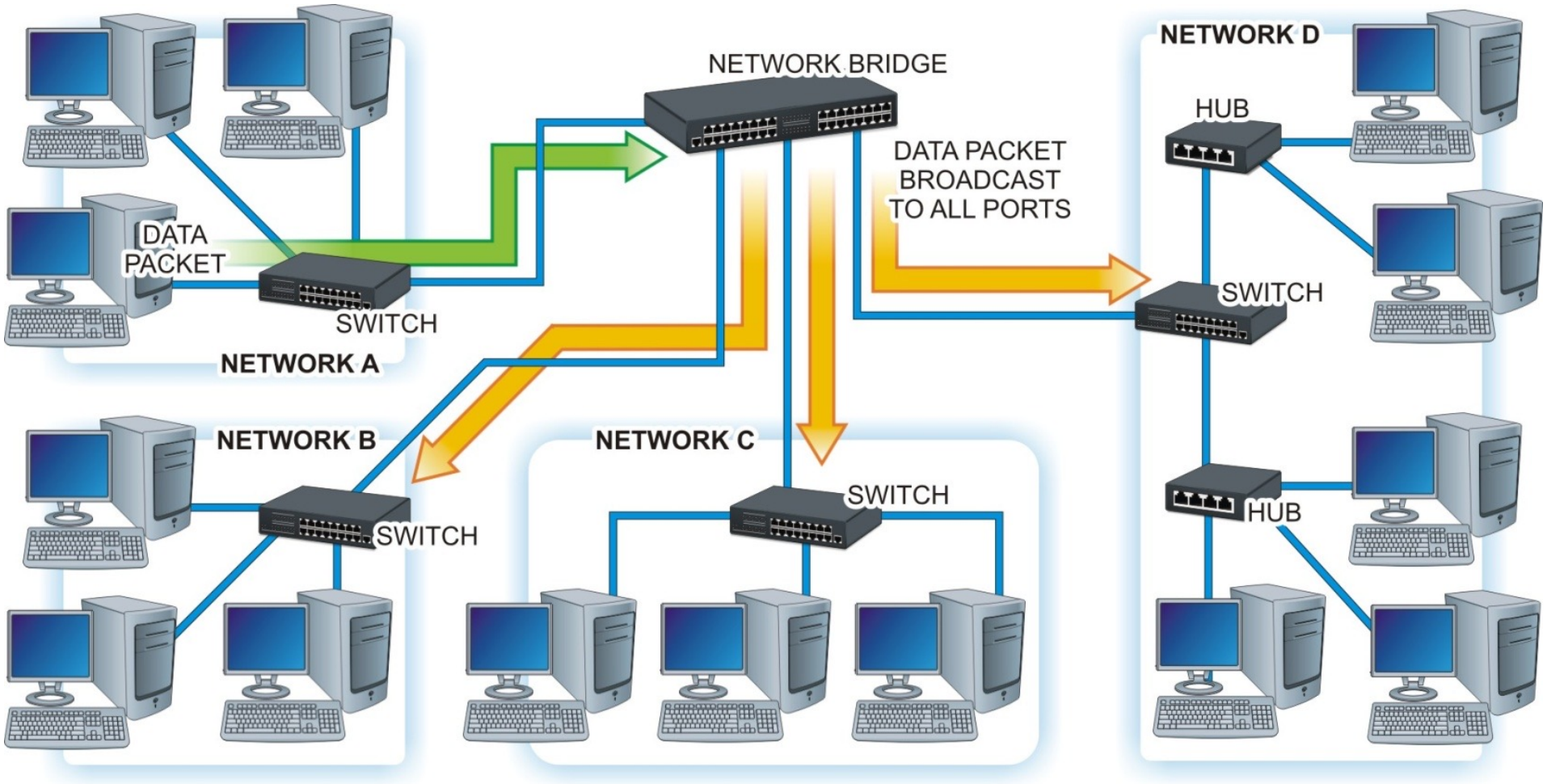
Clearing Up Connectivity Device Confusion

- There is often confusion about connectivity devices because of the way they are marketed. For example, switch and router functions are sometimes built into the same piece of equipment and marketed as a multi port router. Routers may be labeled by the function they perform. For example, a router connecting a network to the Internet may be referred to as an *edge router*, while a pair of routers simply connecting two network segments together are called *core routers*.

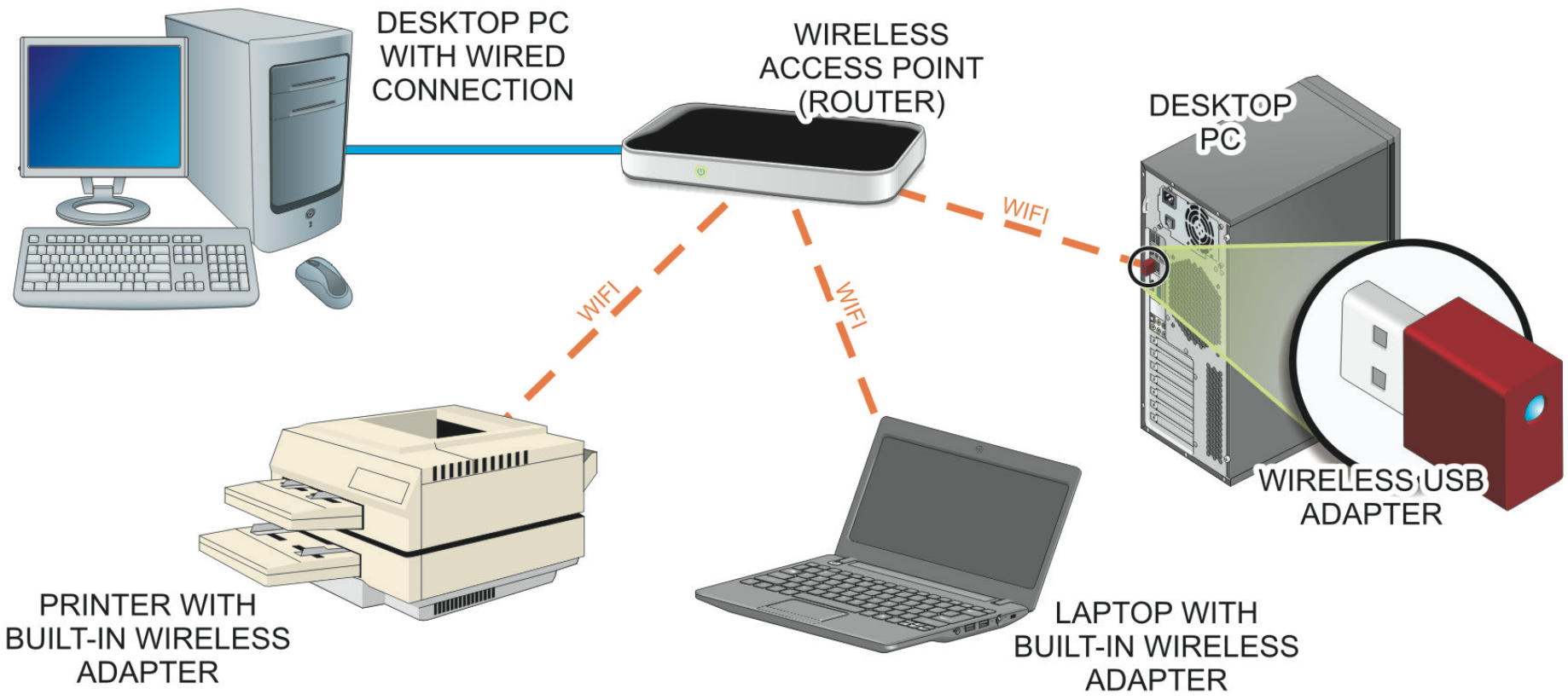
Gateway Operations



A Network Bridge Arrangement



A Wireless Access Point



Protecting Network Connectivity Devices

- Placing connectivity devices in secure wall cabinets or locating them within the security of the server room to provide physical protection.

Protecting Network Connectivity Devices

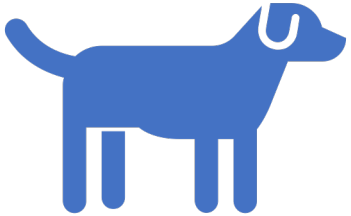
- Configuring device management settings so that required features are as secure as necessary to provide the performance level needed. Disabling any management features that are not needed.

Protecting Network Connectivity Devices

- Establishing port security through MAC address filtering (manually entering static MAC addresses into the CAM), or by specifying the maximum number of devices allowed on a port. By entering static ARP entries, this removes the possibility of attackers being able to replace them with forged ARP replies.

Network Connectivity Devices Attacks

Unauthorized accesses



Packet sniffing attacks

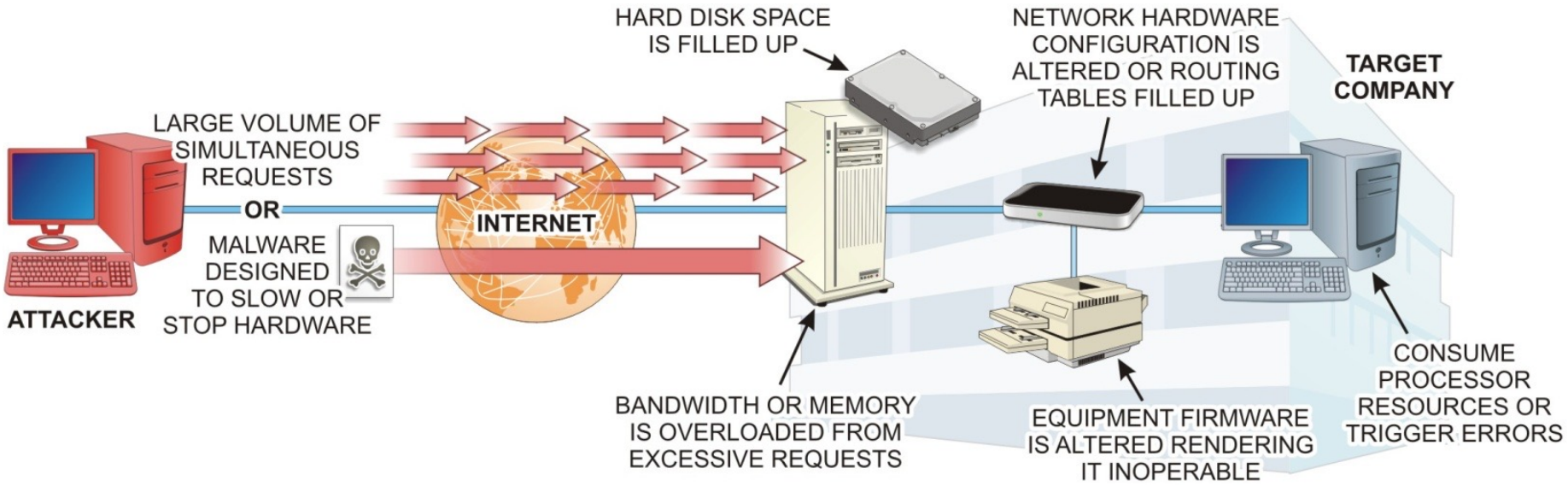
Packet Sniffing Attacks

- Address Resolution Protocol (ARP) Spoofing Attacks
- MAC Flooding
- Router Flood Attacks
- MAC Duplicating (or Cloning) Attacks
- Switch Port Stealing
- Denial of Service (DoS) Attacks

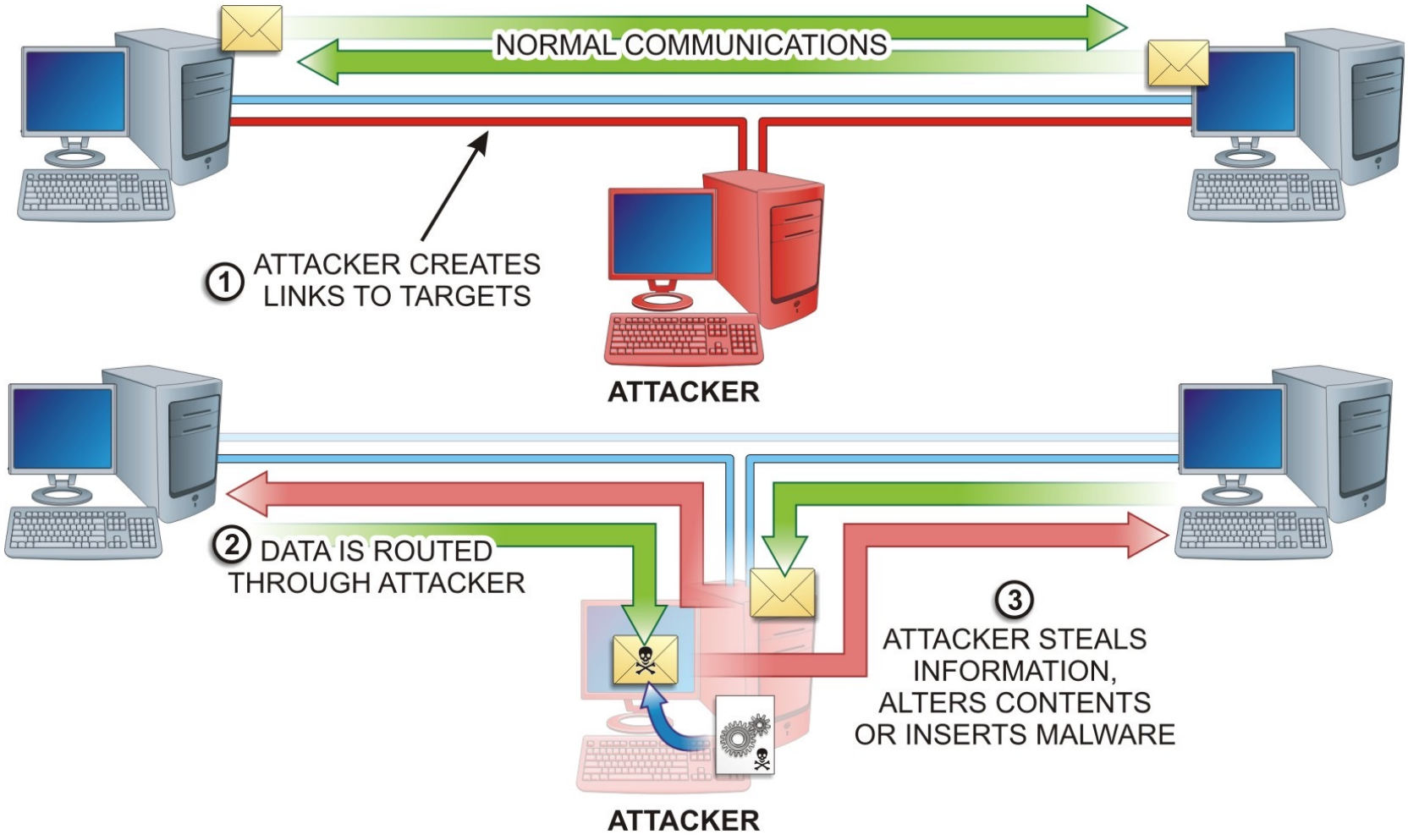
Packet Sniffing Attacks

- Spoofing Attacks
- Man-in-the-Middle (MITM) Attacks
- Session Replay Attacks
- Rerouting Attacks
- Masquerade Attacks

A Denial of Service Attack



Man-in-the-Middle Attack



Network Hardening

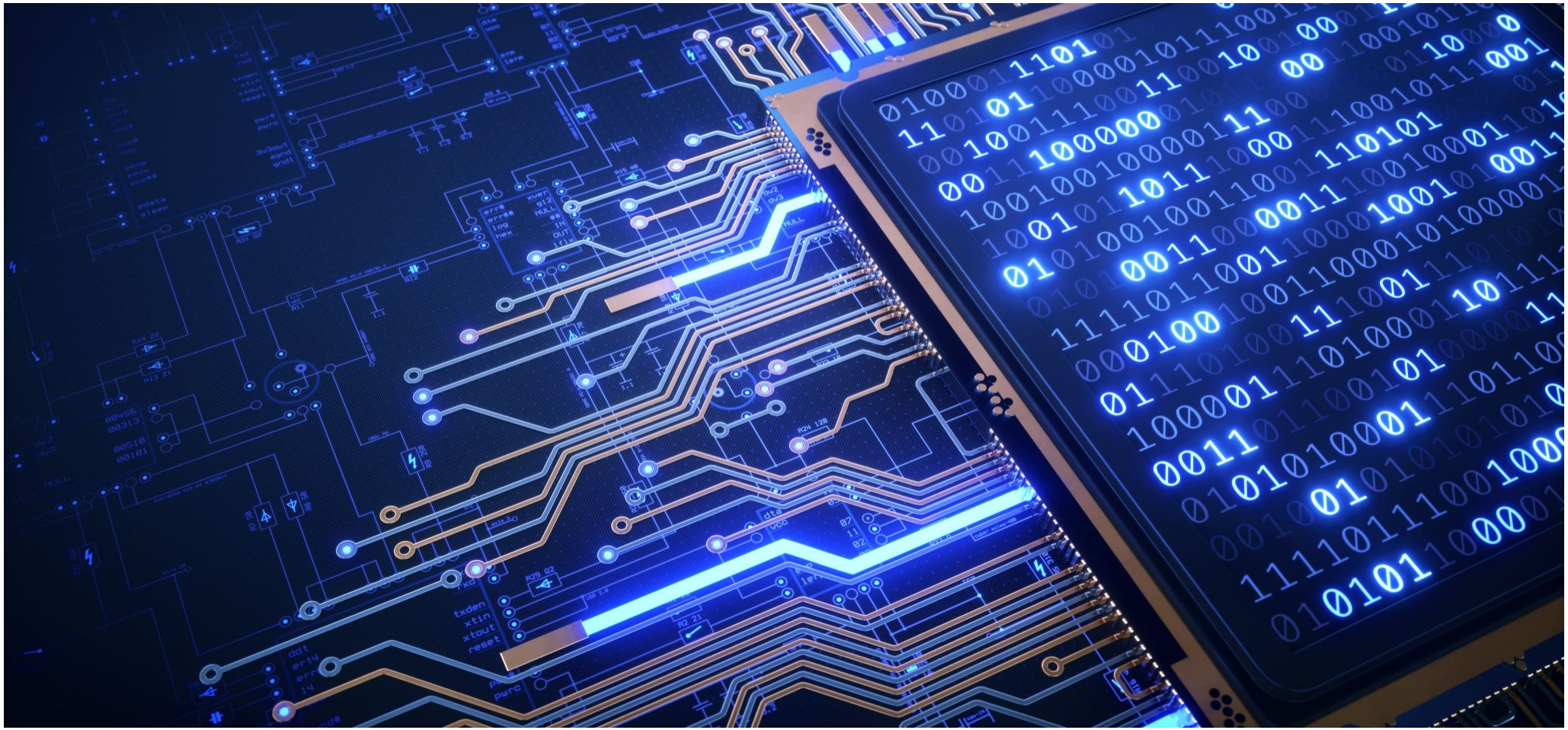
- Secure the system's servers to the degree called for in the organization's security policies. If possible, place them in a monitored, centralized server room that has a double locking door.

Network Hardening

- Check to determine if there are any network devices whose specifications fail to meet current security goals and therefore represent easy access points to the network.

Network Hardening

- Verify that the network is configured to perform its communication functions and still provide the security levels called for by the organization's security policies. Make certain that devices such as switches, firewalls, and routers are not still set to their default configuration settings.



Network Hardening

- Evaluate the cybersecurity plan to make sure that critical devices such as production servers are installed in the correct network segment, security zone or subnet.

	Page/Namespace	User/Group	Permissions[1)]
#1	*	@ALL	○ None ○ Read ○ Edit ◉ Create ○ Upload ○ Delete
#2	*	bigboss	○ None ○ Read ○ Edit ○ Create ○ Upload ◉ Delete
#3	devel:*	@ALL	◉ None ○ Read ○ Edit ○ Create ○ Upload ○ Delete
#4	devel:*	@devel	○ None ○ Read ○ Edit ○ Create ◉ Upload ○ Delete
#5	devel:*	bigboss	○ None ○ Read ○ Edit ○ Create ○ Upload ◉ Delete
#6	devel:*	@marketing	○ None ◉ Read ○ Edit ○ Create ○ Upload ○ Delete
#7	devel:funstuff	bigboss	◉ None ○ Read ○ Edit ○ Create ○ Upload ○ Delete
#8	devel:marketing	@marketing	○ None ○ Read ◉ Edit ○ Create ○ Upload ○ Delete
#9	marketing:*	@marketing	○ None ○ Read ○ Edit ○ Create ◉ Upload ○ Delete
#10	start	@ALL	○ None ◉ Read ○

- Establish and configure ACLs on network connectivity devices to limit or restrict access to assets as required by the organization's security policies.

Network Hardening

Network Hardening

Evaluate the roles and responsibilities of personnel against the servers they commonly access.

Network Hardening

- Access residual risks that remain in the network and monitor for changes that may need to be made in the future.

Questions?