

Instructional Scenario

The Startup Security Audit



Course/Duty Area: Cybersecurity Fundamentals/Examining Computer Networks as a Foundational Element of Cybersecurity

Scenario:

Vertex Innovations, a local tech startup, has just moved into a two-story office. They have inherited old hardware, unorganized networking equipment, and a lack of security protocols. You have been hired to perform a ground-up audit. You must identify their physical assets, design a secure local area network (LAN), and ensure their data transmissions are encrypted and reliable.

Big Question:

How do physical computer components and networking protocols work together to create a secure, interoperable global communication system?

Focused Questions:

- What are the essential internal components of a computer, and how do their roles differ in data processing and storage?
- What is the difference between a LAN and a WAN, and why are international standards critical for interoperability?
- How do wired and wireless networks compare in terms of speed, reliability, and security risks?
- Which protocols (TCP vs. UDP) and services (DNS, DHCP, HTTPS) are necessary to ensure a network is both functional and secure?

Student Project or Outcome:

Students will act as consultants to produce the Vertex Network Blueprint and Audit Report, a comprehensive digital or physical portfolio that includes

- hardware inventory, a labeled diagram or photo set of a disassembled PC identifying the case, motherboard, CPU, RAM, hard drive, power supply, and ports
- network map, a visual schematic of the office's local area network (LAN) showing the placement of the switch, router, wireless access points, and firewall
- protocol manual for the startup's IT staff, explaining when to use TCP vs. UDP, why SFTP is required over FTP, and the importance of HTTPS for their web traffic.

Project-Based Assessment:

Students will be evaluated on a security presentation in which they must defend their infrastructure choices. (Teachers could also invite local IT/cybersecurity professionals to hear the presentation and offer mentorship and feedback to students.)

Criteria	Proficient Performance
Component ID	Correctly identifies all seven internal/external hardware components and their functions.
Network Design	Differentiates between LAN and WAN; correctly places NICs, switches, and routers.

Criteria	Proficient Performance
Security Logic	Justifies the use of wired connections for sensitive data and wireless for convenience.
Protocol Application	Accurately explains the roles of DNS, DHCP, and the necessity of TLS/SSL in HTTPS.
Troubleshooting	Uses a ping (ICMP) test scenario to diagnose a connectivity issue within the blueprint.

Teacher Resources:

- Hardware: old desktop towers for disassembly, anti-static mats, and screwdrivers
- Simulation Software: tools like Cisco Packet Tracer or LucidChart for network mapping
- Protocol Analysis: Wireshark (to demonstrate the difference between plain-text HTTP and encrypted HTTPS traffic)
- Virginia Cyber Range: access to virtual environments that include Cisco Packet Tracer and Wireshark

Scenario submitted by Chris Starke, Briar Woods High School, Loudoun County Public Schools