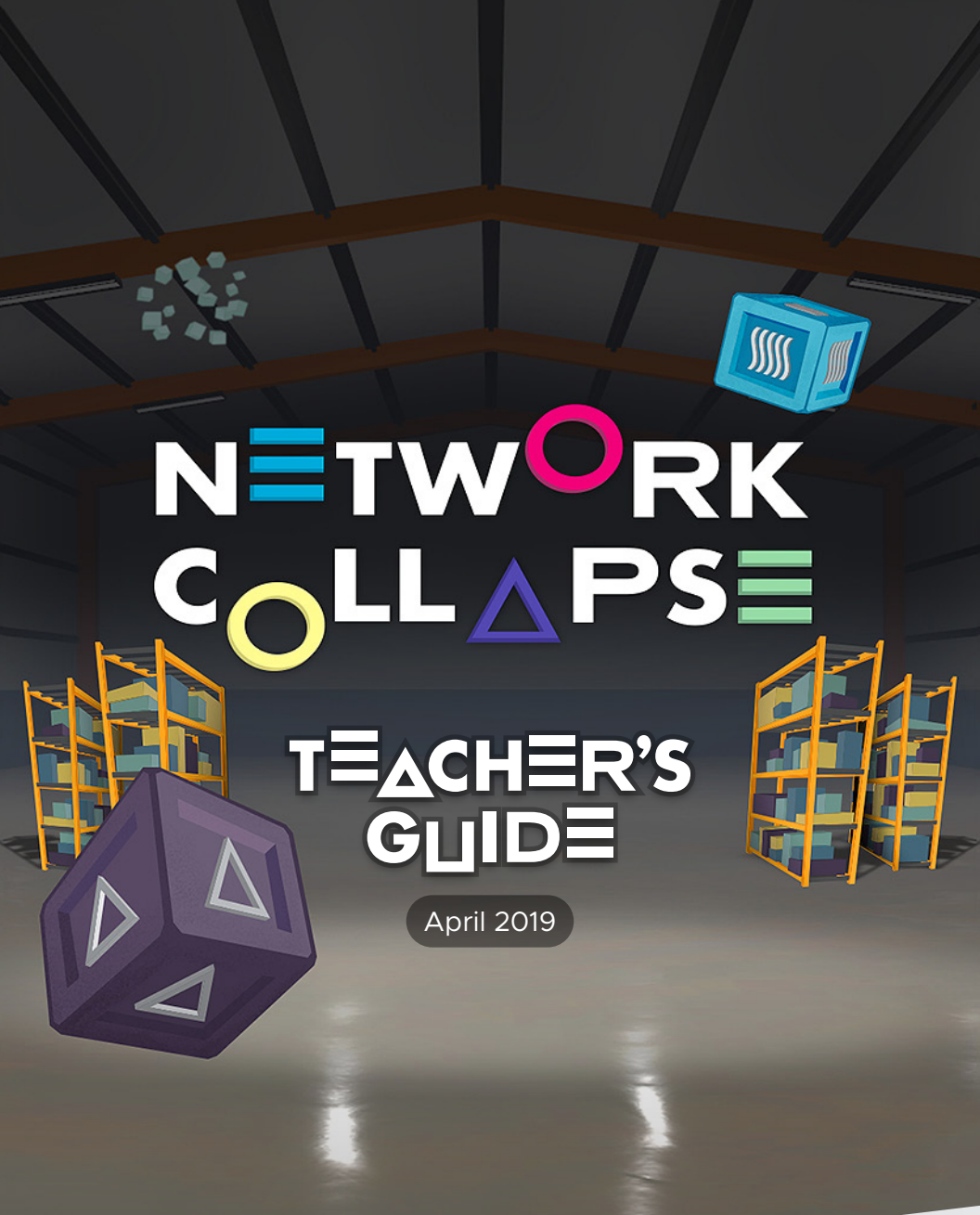

NETWORK COLLAPSE

TEACHER'S GUIDE

April 2019

EVERYONE
E
CONTENT RATED BY ESRB

Pacific Northwest
NATIONAL LABORATORY


FIRE
FIRE

Contents

Introduction 4

Targeted Standards 5

Script 6

Definitions of Vocabulary Terms 9

Resources for Lessons to Accompany App 12

Example Discussion Questions 13

Oculus Go 14

Pacific Northwest National Laboratory 15

Immersive Computing 15

Introduction

Network Collapse is a virtual reality experience designed to help teach concepts from the Computer Science Teachers Association K-12 Computer Science Standards. Because Network Collapse is designed as a game, it can be played beyond those levels designed for learning—Levels 1-6. The experience is optimized for the Oculus Go headset with a single controller. The Oculus Go headset tracks rotational motion of the head and the controller but not player movement through physical space. Players need space to rotate—ideally in a swivel chair or a space that allows them to safely turn while standing. Please refer to the section **"Tips and Tricks for Classroom Use"** for more notes on using the headsets

Targeted Standards

Networks and the Internet

- Model how information is broken down into smaller pieces, transmitted as packets through multiple devices over networks and the internet, and reassembled at the destination.
- Explain how physical and digital security measures protect electronic information.
- Evaluate the scalability and reliability of networks by describing the relationship between routers, switches, topology, and addressing.
- Illustrate how sensitive data can be affected by malware and other attacks.

Script (with bolded vocabulary terms)

Introduction

- Welcome to **Network** Collapse. Here, you will take on the role of various types of **networking hardware** used every day in the real world; your job is to move information from a source to a destination.
- **Information** passed along a network needs a physical or wireless path to travel to be sent and received. Information is broken into smaller pieces called **packets** that are sent individually and reassembled at the destination.
- As you progress, the amount of packets and number of sources and destinations will increase. Additionally, you will become more prone to **common attacks** such as a **denial-of-service (DoS)** or **viruses**, which you will need to protect your network against.
- See how long you can last before the network collapses. Good luck!

Level 1 – Home Switch/Router

- You are a simple home **router** or **switch** that allows one **computer** to communicate with another. You need to get transmitted and received messages from one color to the other.
- To do this, first point at a **data packet** and click (squeeze the trigger) to pick it up. Find the matching color conveyor belt, then point and click to send.

Level 2 – Small Office/Home Router

- You will now act as a simple office or home **router** that allows multiple computers to communicate with one another. Expect to see more connections appearing around you as you progress.

TIP **Your Data Packet Vacuum Gun can hold multiple packets at once—up to five total packets! The packets can be any mix of colors. The display on the left side of your Vacuum Gun will show you what you are currently holding.**

Level 3 – Router with Wi-Fi

- You are now a home router with **Wi-Fi** capabilities. Data packets will now arrive both through wires (conveyors) and Wi-Fi antennas (through the air) over each conveyor belt.
- To transfer the Wi-Fi packets, point and click at arriving packets like usual, then point at the matching color Wi-Fi antenna and click to launch.

TIP **Your Data Packet Vacuum Gun CANNOT hold Ethernet and Wi-Fi packets at the same time.**

Level 4 – Router with Wi-Fi

- Repeats Level 3, with an additional connection (lane).

Script (continued)

Level 5 – Public Wi-Fi Router

- Public **Wi-Fi** routers allow computers to send and receive information in public locations. Public networks are more susceptible to **attacks**, such as a **denial-of-service (DoS)** or **viruses**. If you see an attack happening, deploy a **firewall** or **antivirus** before it's too late.

TIP **Viruses are disguised as regular packets, but they are not grabbable. If you see a packet you can't grab, it is a virus! Quickly deploy your antivirus to quarantine the threat.**

TIP **DoS attacks will rapidly flood you with packets. Deploy your firewall to prevent them from collapsing the network!**

Level 6 – Public Wi-Fi Router (2)

- Repeats Level 5, with more difficulty.

Definitions of Vocabulary Terms

Antivirus – a type of software program designed and developed to protect computers from threats such as *known* viruses, that may harm the computer or the information it holds.

Attacks (aka cyberattacks) – any attempt, in a computer or computer network, with digital information or resources, to expose, alter, disable, destroy, steal, access, or use without permission.

Common Attacks – categories of ways that an attempt to harm, expose, access, steal, or use digital information or resources are most likely to be used currently. This includes denial-of-service attacks and various kinds of malicious software (aka malware), such as viruses.

Computer Network Data Packet (or packet) – small pieces of information created from larger pieces of information so that they can be sent digitally to another computer through a network.

NOTE: Data encapsulation is heavily simplified for this game, referring to it only as "packets." Advanced students may search online about network "segments," "packets," and "frames." Students ready for even more information should study the OSI layer.

Denial-of-Service (DoS) – an attack on computer systems or networks, where the attacker sends more data (aka traffic) than the system or network is designed to handle (aka flooding the network) in order to make it difficult or impossible for legitimate users to gain access, or an attempt to forcefully break past/through security systems.

Definitions (continued)

Ethernet – technology connecting wired local area networks so that devices can communicate with one another. The reference in the experience is to an Ethernet cable, which is the physical, encased wiring that the packets travel inside as small, but fast, electrical signals.

Firewall – a security system for a network that monitors traffic from and to that network using a defined set of security rules to, for example, allow authorized packets, reject/block unauthorized packets from trusted systems, and drop unauthorized packets from unknown/untrusted systems.

Information (computer-specific) – data that has been processed, organized, structured, or presented in a way that makes it useful.

Malware – software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Network – a group of two or more devices that can communicate.

Networking Hardware – the physical devices needed for communication and interaction between any devices on a computer network.

Public Wi-Fi Router – a wireless networking device with access freely provided for public use. Security is never guaranteed while using public Wi-Fi routers.

Router – a networking device that forwards data packets between computer network switches.

Definitions (continued)

Server – computers that function only to provide things for other devices or systems.

Switch – a device used to connect network devices to computer systems, centralizing communications among the multiple computer systems connected in one small area.

Virus (computer-specific) – a piece of code capable of copying itself and that typically has a detrimental effect, such as corrupting the system or destroying data.

NOTE: For simplicity, the game only presents viruses. Viruses are common, but are only one of many types of malware. For extra reading, search online for information about "computer trojans," "computer worms," and "ransomware."

Wi-Fi – a wireless method that uses radio waves to send information.

Resources
for Lessons to Accompany the Experience

Examples of Related Unplugged Lessons/Activities:

- Information Hiding
- Cryptographic Protocols
- Routing and Deadlock
- Network Protocols
- Public Key Encryption
- Computer Science-in-a-Box – pp. 113-122

Code.org Related Lessons:

- The Internet
- Internet Simulator
- CS Principles – Unit 1, Lesson 11 as well as other lesson

Other Lessons:

- Wi-Fi safety video
- Video of game play (link TBD)

These resources can be easily accessed via the live hyperlinks (above) in the electronic version of this document. If you're viewing the Network Collapse Teacher's Guide in printed form, visit **http://www.pnnl.gov/STEM/** to download a free copy of the interactive .PDF.

Example Discussion Questions

- Thinking about the game you played, what did you learn?
- How do you think information moves in a network? How might this be similar to information moving over the Internet?
- What role were you playing in the game?

  Answer: A router or switch
- What does a switch do? What does a router do?

  Answer: Both move data packets, but the switch does so among devices in a local network and a router moves packets between computer network switches—see ***vocabulary terms***
- What are data packets?
- How did you protect the data? What other ways can data be protected?
- How do we know that we received all of the information that was sent to us?
- What can happen if there is too much traffic coming through the router or switch?

Oculus Go

Set Up and Help

Tips and tricks for classroom use:

- Screen Cast can be used to see live student game play.
- Students can take a video or screenshot while in the game. These can be downloaded from the headset as evidence of student progress.
- Have students working on other tasks while they take turns with the experience. After all students have played the game, have a full classroom discussion with reinforcing activities or a formative assessment.
- A small subset of students may experience nausea or have trouble seeing clearly.
- Glasses can be worn while using the headset.
- Make sure students put the controller safety strap on their wrists to prevent the controller from falling.
- This game drains the controller batteries quickly—rechargeable batteries are suggested.

Pacific Northwest National Laboratory

PNNL advances the frontiers of knowledge, taking on some of the world's greatest science and technology challenges. Distinctive strengths in chemistry, Earth sciences, and data analytics are the heart of our science mission, laying a foundation for innovations that improve America's energy resiliency and enhance our national security.

Immersive Computing

At PNNL, we create novel immersive experiences that work with a variety of devices and platforms. We apply and develop emerging user-interface technologies to create more engaging experiences and seamless workflows. Our researchers develop multi-sensory interfaces that support collaboration, where users can immerse themselves in their data to explore, discover, and analyze.

As a multidisciplinary national laboratory, we assemble customized teams of software developers, user experience designers, and subject matter experts from dozens of science and technology fields. Working with instructional designers, we conduct extensive user research to understand and document specific needs, so that users come away with the desired knowledge and understanding.

NETWORK COLLAPSE

This Teacher's Guide is provided as an instructional companion to the Network Collapse virtual reality game, developed by computer scientists at Pacific Northwest National Laboratory. An interactive .PDF version of the Teacher's Guide is needed to access the additional information available from the hyperlinks inside, and can be freely downloaded from:

http://www.pnnl.gov/STEM/

oculus

Network Collapse can be downloaded for FREE — find it under the Education category within the Oculus App.

Pacific Northwest NATIONAL LABORATORY

Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy

BATTELLE

U.S. DEPARTMENT OF ENERGY

PNNL-SA-143694