Networking

Networking Fundamentals

1.4.1 - Public and Private Networks

What are public and private networks and how do they differ from each other?

Overview

Given a scenario, the student will configure a subnet and use appropriate IP addressing schemes

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 1.4

- Given a scenario, configure a subnet and use appropriate IP addressing schemes
    - Public vs. Private
        - RFC1918
        - Network address translation (NAT)
        - Port address translation (PAT)
    - Virtual IP (VIP)
    - Subinterfaces

Public and Private Networks

Public IP Addresses

A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). The terms public, global, and external may all be used interchangeably, although public is the most common. All servers and sites on the Internet use public IP addresses. All public IP addresses on the Internet are unique to their host or server and cannot be duplicated.

Private IP Addresses

When dealing with IPv4 addresses, there are specific addresses that are stored for private (local, internal) networks. These addresses cannot be accessed by a machine outside of a private network. For example, the IP address 1.1.1.1 will always take a user to Cloudflare's website since it's their IPv4 address from any device that is connected to the internet. However, the IP address 10.17.45.136 will not take a user to a website unless a device on their private network has this IP address. ***RFC1918*** sets the addresses, and they are the following IPv4 addresses:

IP Address Range	CIDR Notation	Number of Addresses
10.0.0.0 – 10.255.255.255	10.0.0.0/8	16,777,216
172.16.0.0 – 172.31.255.255	172.16.0.0/12	1,048,576
192.168.0.0 – 192.168.255.255	192.168.0.0/16	65,536

Teacher Notes:

Why are these addresses set aside for private networks? The reasoning was because people realized that there were too many devices for the set number of IPv4 addresses. This number being slightly above 4 billion addresses, with people having multiple computers, phones, tablets, etc…, these addresses quickly fill up. Thus, the RFC1918 addresses are reused in private networks and allow for IPv4 to still be used where devices use the same IP addresses on private networks.

NATs and PATs

There is a problem with RFC1918, how does a device on a public network talk to a device on a private network? This is solved in using a ***NAT, or network address translation.*** NATs translate a private IP address to a public IP address where a machine on a private network can still be accessed by a machine on a public network. It does this by only using the public IP address, and not the private IP, thus adding an extra layer of security to the device on the private network. Similar to NAT is ***PAT, or port address translation***, where private IP addresses can be translated to the public network, but here they use a port number. The private network can then map that port number to a specific device on the private network.

VIP

A ***virtual IP (VIP)*** address is an IP address that does not contain the actual network interface numbers. For example, if your school's IP address is 136.15.4.5 where 136.15 is the network, a device on the school's network could be 192.168.45.31. This IP address does not actually correspond with the network's IP. This is able to be done with a NAT, network address translation that will be able to make a device with a VIP still be connected to the WAN and have network access.

Subinterfaces

Subinterfaces happen on Layer 3 of the OSI Model. This occurs when a physical interface is split up into many interfaces. This is common when one router wants to have two different networks on the same device, so the router will create the two networks and still have a way for those two communicate with each other while keeping them separate. Thus, routers are able to control multiple networks instead of having multiple devices for each separate network.