Lab 10: Understanding BGP

10 points

Due: Before class on 4/27/2022

Objectives of this lab:

1. Learn about aspects of BGP by analyzing a PCAP file with wireshark
2. Research aspects of BGP

PCAP

For the following questions open the file **bgp.cap** from the D2L lab. This is a PCAP showing a BGP session between 2 routers: 19.168.0..15 and 192.168.0.33.

1. What protocol does BGP use to communicate (UDP or TCP)? [1 point]
   TCP
2. What version of BGP are these routers running (this can be found in either of the OPEN messages)? [1 point]
   4
3. There are 3 important pieces of information in a BGP UPDATE message: the AS_PATH, the NEXT_HOP, and the Network Layer Reachability Information (NLRI). These 3 aspects tell the other router what AS's the new path travels through, the next hop to send traffic through to get there, and the network prefix being advertised. For this question look at packet #16 (the packet with a KEEPALIVE and UPDATE portion in the same packet). [6 points]

   a. What are the AS numbers from the AS_PATH section that the updated route will travel through (these are labelled AS2 in the pcap and one of the numbers is listed twice)?
      500 and 65211
   b. What is the IP address of the NEXT_HOP for this update?
      192.168.0.15

c. What network prefix is being advertised with this update (found in the NLRI section)?
/16

Research

4. We discussed in class the dangers of BGP Hijacking. One proposed solution to this problem is a security extension to BGP called BGPSec. What does BGPSec add to BGP and how does it work to stop BGP Hijacking attacks? [2 points]
   Adds a cryptographic signature to the AS path updates. It makes sure the updates are going where they're supposed to and not to a third party.