BGP and Attacks

N12.1. Do a traceroute from your home and your school, and explain what you see.

N12.2. A BGP router knows 10 different paths to a network prefix, how many of these paths will this BGP router tell its peers?

N12.3. A BGP router X peers with BGP routers from five autonomous systems, A, B, C, D, and E. It receives an AS path announcement from A, and decides to forward this path to its peers. However, X only forwards the path to B, C, and D, not to E. Please name a reason why X decides not to forward the AS path to E.

N12.4. An autonomous systems A peers with its service provider B. A only uses B as a backup service provider, so normally, A does not use this link. (1) How does A conduct the configuration on its side, so the outgoing traffic will not pick this A-B link when other links are available? (2) How does A "tell" the outsider to avoid using the A-B link, so the incoming traffic will go to A's other links?

N12.5. The following is the content of a BGP UPDATE message, (1) Please explain what is covered in this message. (2) What autonomous system does the sender of this message belongs to? (3) What is the purpose of the `NEXT_HOP` attribute?

```
Border Gateway Protocol - UPDATE Message
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 4
    Withdrawn Routes
        10.151.0.0/24
    Total Path Attribute Length: 67
    Path attributes
        Path Attribute - AS_PATH: 3 12 164
        Path Attribute - NEXT_HOP: 10.100.0.3
    Network Layer Reachability Information (NLRI)
        10.164.0.0/24
            NLRI prefix length: 24
            NLRI prefix: 10.164.0.0
```

N12.6. Typically, the TTL field of the EBGP packets is set to 1. Please explain why.

N12.7. Some BGP routers set TTL of their BGP update packets to 255. What is the main purpose?

N12.8. Using the following diagram, please answer the following questions (assuming the length of AS path is the only criterion used in the path selection algorithm):

1. What does AS-11872 announce to its neighbor AS-30?
2. What is the AS path announced by AS-40 to AS-50 in terms of prefix 128.230.0.0/16?
3. What is the AS path announced by AS-50 to AS-60 in terms of prefix 128.230.0.0/16?

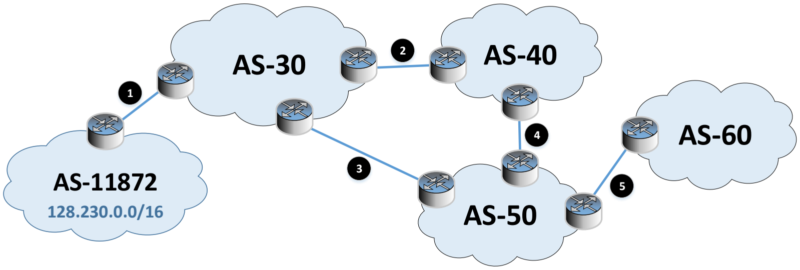

Figure 1: Diagram for Problem N12.8.

N12.9. Why is IP anycast not suitable for applications like `telnet`?

N12.10. Assume that an attacker has already compromised a BGP speaker on the Level 3 backbone located in Oklahoma City, his malicious goal is to prevent anybody from communicating with Bank32.com (130.219.96.0/19) over the Internet. In both questions, you do need to provide concrete IP addresses.

1. What can the attacker do to achieve the specified objective?
2. After the Bank32 finds out the attack, before Level 3 can stop the attack, the bank wants to resolve the problem by itself, please describe what the bank can do.