

# BGP 及其攻击

版权所有 © 2022 作者：杜文亮，保留所有权利。

允许个人使用。利用这些问题只有当作者的书被采用作为该课程的教科书时，该课程才被授予。所有其他用途必须征得作者同意。

- N12.1. 分别从家中和学校执行 traceroute，并解释观察到的路径差异。
- N12.2. 某 BGP 路由器学到了到同一网络前缀的 10 条不同路径。它通常会向一个对等体通告其中多少条？
- N12.3. BGP 路由器 X 与自治系统 A、B、C、D、E 的路由器建立了对等关系。X 收到 A 的 AS 路径通告后，将其转发给 B、C、D，却没有转发给 E。可能有哪些原因？
- N12.4. 自治系统 A 与提供商 B 相连，但只把 A-B 链路作为备份。(1) A 应如何配置，使出站流量在其他链路可用时不选择 A-B？(2) A 如何降低外部网络通过 A-B 向 A 发送进站流量的可能性？
- N12.5. 以下是 BGP UPDATE 消息的内容，(1) 请解释本消息的内容。(2) 该消息的发送者属于哪个自治系统？(3) NEXT\_HOP 属性的用途是什么？

## 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Withdrawn Routes Length: 4
Withdrawn Routes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. 通常，EBGP 数据包的 TTL 字段设置为 1。请解释原因。
- N12.7. 一些 BGP 路由器把 BGP 更新报文的 TTL 设为 255，主要目的是什么？
- N12.8. 请根据下图回答问题，假设路径选择只比较 AS\_PATH 长度：

1. AS-11872 向其邻居 AS-30 宣布什么？

2. 根据前缀 128.230.0.0/16, AS-40 到 AS-50 宣布的 AS 路径是什么?
3. 根据前缀 128.230.0.0/16, AS-50 到 AS-60 宣布的 AS 路径是什么?

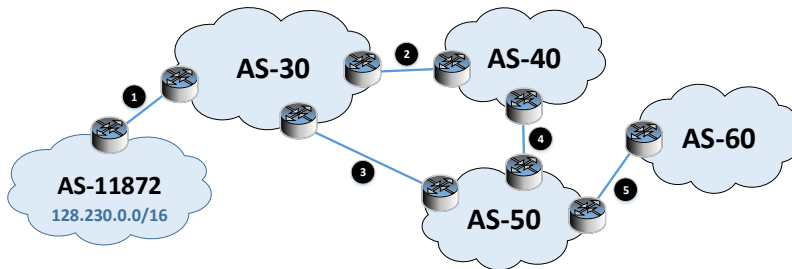


图 1: 问题 N12.8. 的网络拓扑

N12.9. 为什么 IP anycast 不适合 telnet 这类应用?

N12.10. 假设攻击者控制了 Level 3 位于 Oklahoma City 的一台 BGP 路由器, 目标是阻止互联网用户访问 Bank32.com 的前缀 130.219.96.0/19。以下两问都要给出具体 IP 前缀。

1. 攻击者可以做什么来达到指定的目标?
2. Bank32 发现攻击后, 希望在 Level 3 处理之前先自行恢复可达性。银行可采取什么措施?