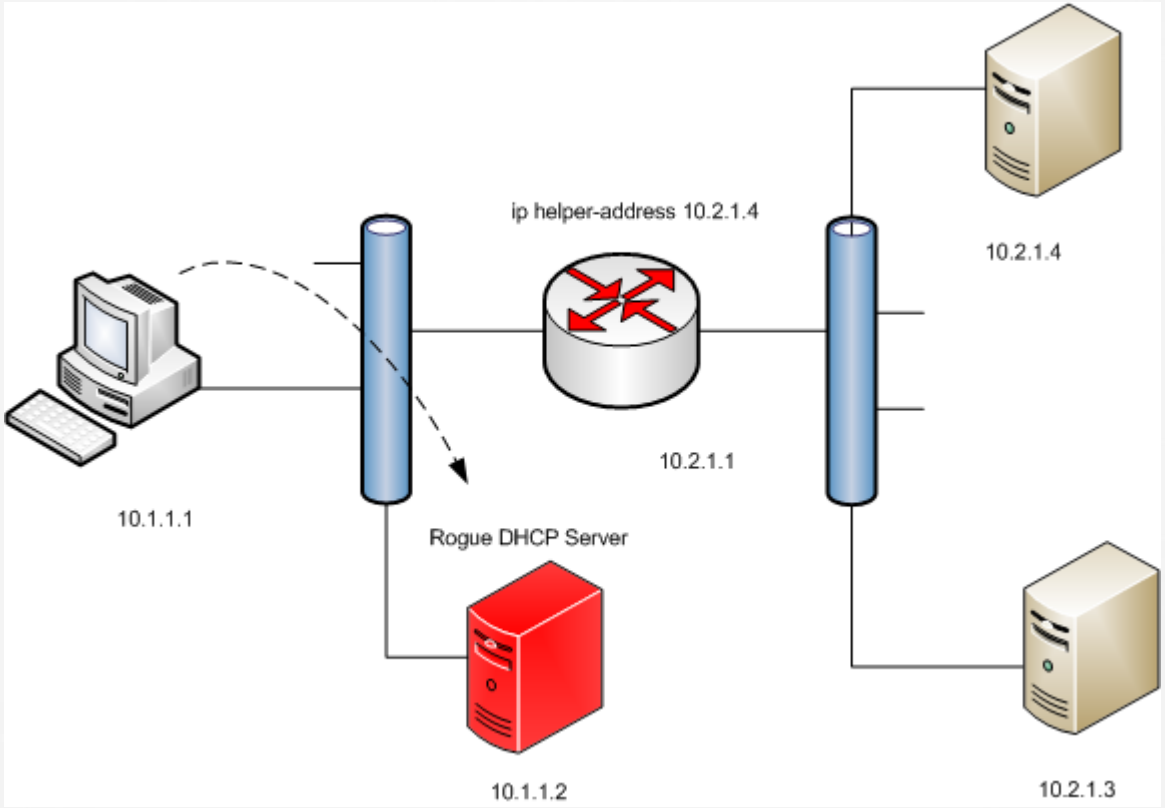
Analyzing DHCP

Analyzing DHCP

- What is a rogue DHCP server?
- Why is it an issue?
  - Breaks the appropriate logical addressing scheme on your subnet
  - Causes disconnections
  - Can be a security violation

Analyzing DHCP



Analyzing DHCP

- **Wireshark analysis of rogue DHCP**
  - In DORA you will find inaccurate and unexpected responses from DHCP server(s)
- **DHCP snooping**
  - Configure protection on your Cisco switch
  - Router(config)# ip dhcp snooping

Analyzing DHCP

```
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 328
    Identification: 0x0445 (1093)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.10 (192.168.0.10)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
  ⊞ Checksum: 0x2233 [validation disabled]
```

Questions?