Ethernet

Understanding Ethernet

- Ethernet, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet
- What is Ethernet and why is it important?
  - The most commonly used Layer 2 standard in use today

Wireshark & Ethernet

```
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1399232307.066541000 seconds
    [Time delta from previous captured frame: 0.523380000 seconds]
    [Time delta from previous displayed frame: 0.523380000 seconds]
    [Time since reference or first frame: 26.890111000 seconds]
    Frame Number: 40
    Frame Length: 1474 bytes (11792 bits)
    Capture Length: 1474 bytes (11792 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:data]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
⊟ Ethernet II, Src: ArrisGro_7f:f2:81 (00:19:a6:7f:f2:81), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ⊞ Source: ArrisGro_7f:f2:81 (00:19:a6:7f:f2:81)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 169.254.1.143 (169.254.1.143), Dst: 255.255.255.255 (255.255.255.255)
⊞ Data (1440 bytes)
```

Why Analyze Ethernet?

- **Troubleshooting problems**
  - Use Wireshark to capture traffic
  - Review traffic to analyze network, protocols, and traffic flow
- **Common issues include**
  - Layer 2 encapsulation
  - Incorrect frame type
  - Media problems
  - Mismatches

Capturing Protocol Data

- Protocol data captured can be inspected for issues
- Protocol analysis
  - Opens up the data for inspection
  - Helps find problems you cannot see without capturing data for inspection
- Traffic analysis
  - Used to find collisions, degraded signals, and corruption