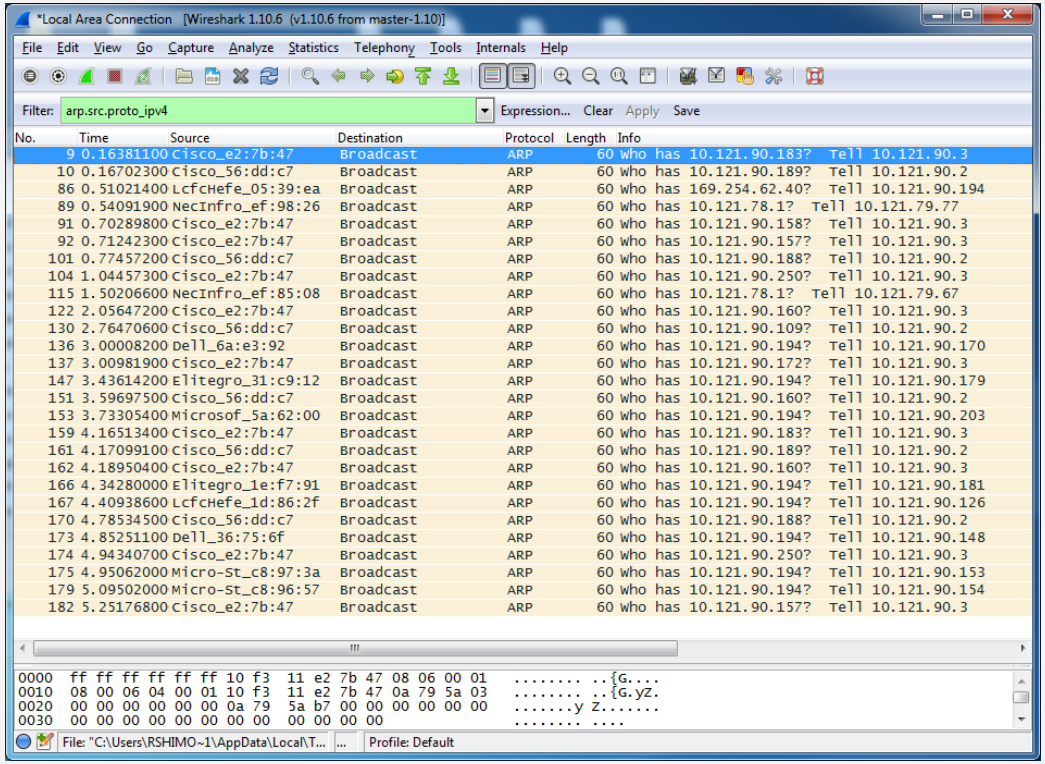
Network Layers & the OSI Model

Understanding Networking Concepts

- Fundamental network knowledge needed to use Wireshark
- How data traverses a network
  - Traffic flow concepts from source to destination
- OSI model
  - 7 layers and mapping of different protocol stacks
  - Understanding of encapsulation of data and the protocol stack (headers)

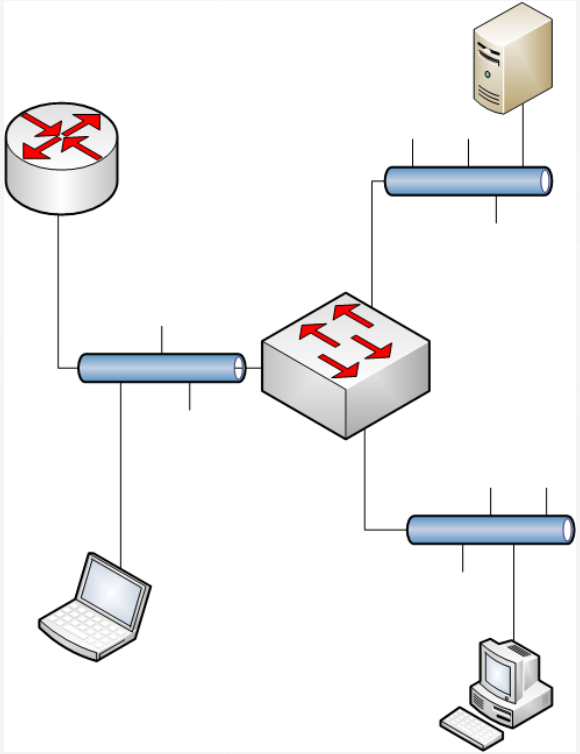
Wireshark & Protocols



Network Lab

- Simple network with Layer 2 and Layer 3, multiple segments and common scenarios
- How to capture traffic
  - Port mirroring
  - Endpoints
- Troubleshooting problems
  - Use Wireshark to capture traffic
  - Review traffic to analyze network, protocols, and traffic flow

Network Lab



Connectivity & the OSI Model

- Layer 1
  - Cabling and electrical signals
  - Wireless
- Layers 2–7
  - As data flows from endpoints on a network, it changes while traversing different layer devices
  - Data is encapsulated and addresses are changed
- Ports, sockets, etc.
  - Higher-layer protocols use other functionality to establish connections

Hardware Connectivity

- **Network interfaces**
  - NIC card
  - Ports
  - Probes
- **Other hardware**
  - Switches, routers, firewalls, IPS units, load balancers, and other hardware change way data is captured and interpreted

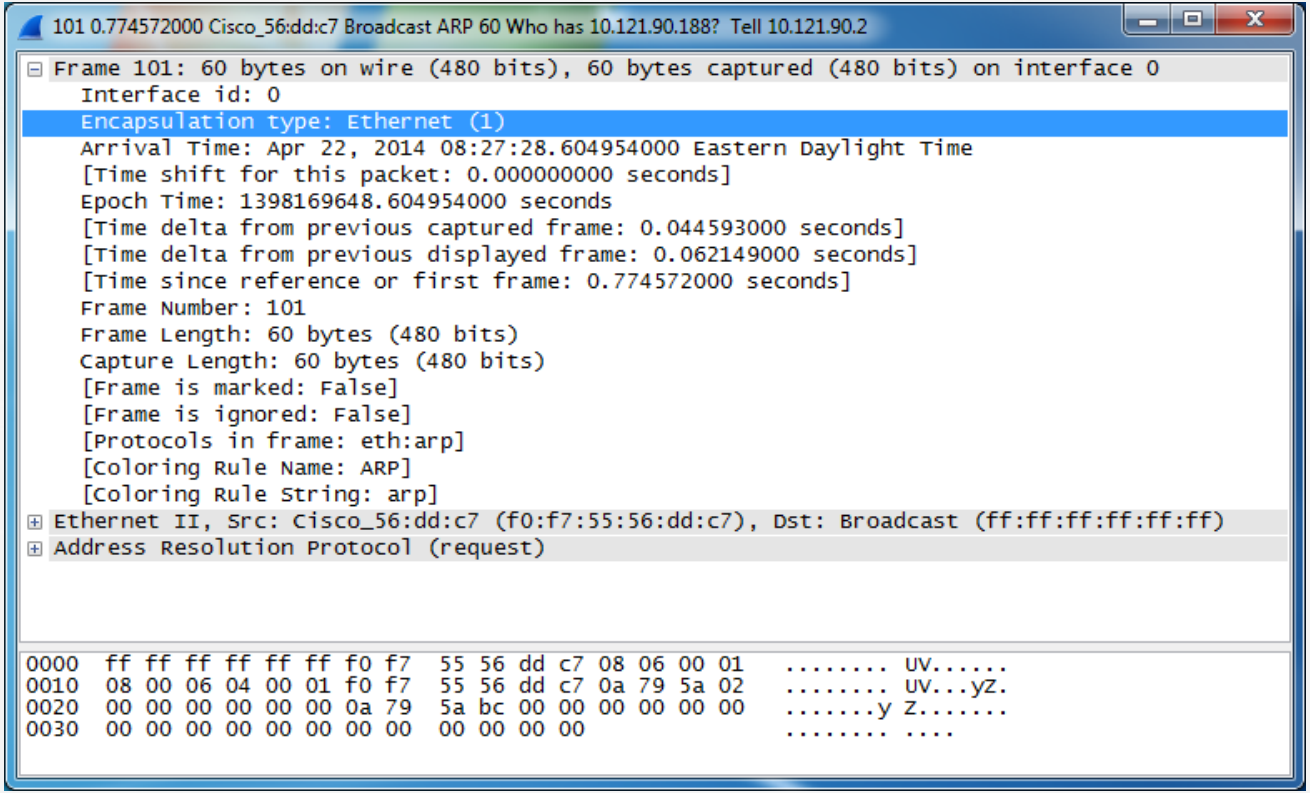
Traffic Flow Analysis

- Data captured for analysis can reveal many issues
  - Bandwidth
  - Corruption
  - Incorrect path
  - Latency
  - Many others
- Source to destination
  - Data is commonly captured and analyzed from a source computer to a destination computer
  - Data is analyzed to isolate and find root cause of a known or unknown problem

Encapsulation

- Traffic flow and the OSI model
- Data encapsulation
  - Headers
  - Protocol analysis of traffic flow
- Protocol decode and inspection
  - When data is captured, it can be analyzed at all applicable layers to show the “under the hood” details needed to solve problems

Network Lab



Capturing Protocol Data

- Captured protocol data 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 bandwidth, latency, and other network issues