Routers & Switches

Switching (Layer 2)

- Fundamental network knowledge needed to use Wireshark
- How data traverses a network
  - Traffic flow concepts from source to destination
- Switching concepts
  - What is switching?
  - What can go wrong

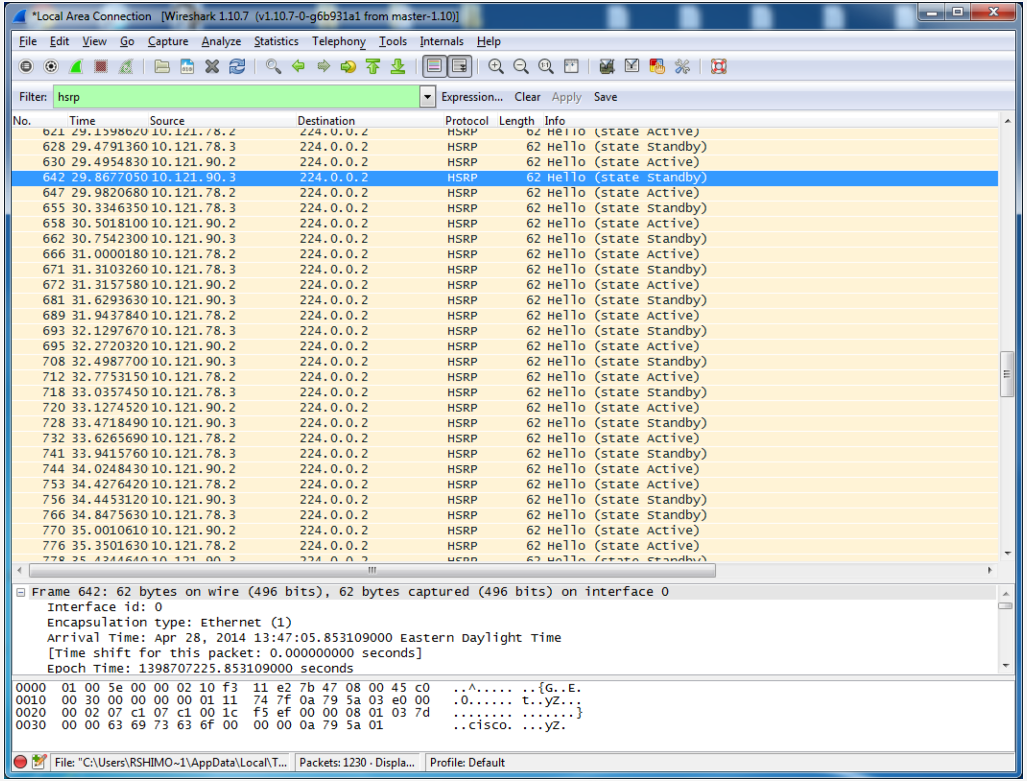
Copyright © www.ine.com

Routing (Layer 3)

- How data traverses a network
  - Traffic flow concepts from source to destination
- Routing concepts
  - What is routing?
  - What can go wrong
  - What is HSRP?

Copyright © www.ine.com

Wireshark & Routing



*Local Area Connection [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: hsrp

```
No.    Time         Source        Destination    Protocol  Length  Info
   621 29.1598620 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   628 29.4791360 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   630 29.4954830 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   642 29.8677050 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   647 29.9820680 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   655 30.3346350 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   658 30.5018100 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   662 30.7542300 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   666 31.0000180 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   671 31.3103260 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   672 31.3157580 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   681 31.6293630 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   689 31.9437840 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   693 32.1297670 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   695 32.2720320 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   708 32.4987700 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   712 32.7753150 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   718 33.0357450 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   720 33.1274520 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   728 33.4718490 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   732 33.6265690 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   741 33.9415760 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   744 34.0248430 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   753 34.4276420 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   756 34.4453120 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
   766 34.8475630 10.121.78.3    224.0.0.2      HSRP      62 Hello (state Standby)
   770 35.0010610 10.121.90.2    224.0.0.2      HSRP      62 Hello (state Active)
   776 35.3501630 10.121.78.2    224.0.0.2      HSRP      62 Hello (state Active)
   778 35.4344640 10.121.90.3    224.0.0.2      HSRP      62 Hello (state Standby)
```

```
⊟ Frame 642: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 28, 2014 13:47:05.853109000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1398707225.853109000 seconds
```

```
0000  01 00 5e 00 00 02 10 f3  11 e2 7b 47 08 00 45 c0   ..^..... ..{G..E.
0010  00 30 00 00 00 00 01 11  74 7f 0a 79 5a 03 e0 00   .0...... t..yZ...
0020  00 02 07 c1 07 c1 00 1c  f5 ef 00 00 08 01 03 7d   ........ .......}
0030  00 00 63 69 73 63 6f 00  00 00 0a 79 5a 01         ..cisco. ...yZ.
```

File: "C:\Users\RSHIMO~1\AppData\Local\T... | Packets: 1230 · Displa... | Profile: Default

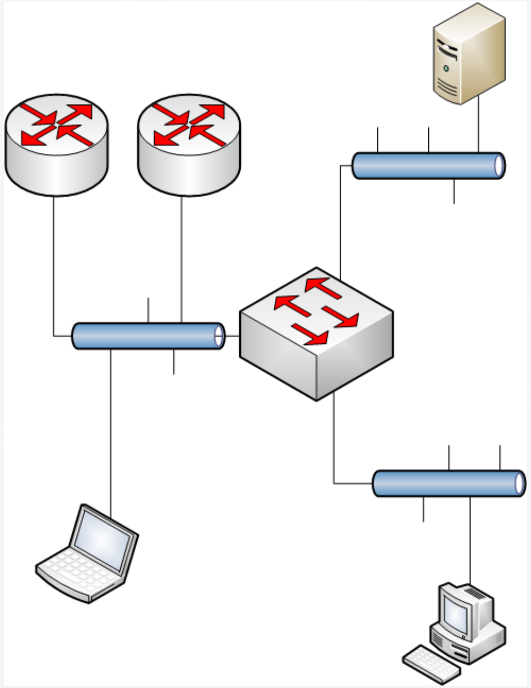
Copyright © www.ine.com

Capturing HSRP

- Hot Standby Routing Protocol (HSRP)
- How to capture traffic
  - Capturing router traffic
- Troubleshooting problems
  - Use Wireshark to capture traffic
  - Review traffic to analyze network, protocols, and traffic flow

Copyright © www.ine.com

Network Lab



Copyright © www.ine.com

Traffic Flow Analysis

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

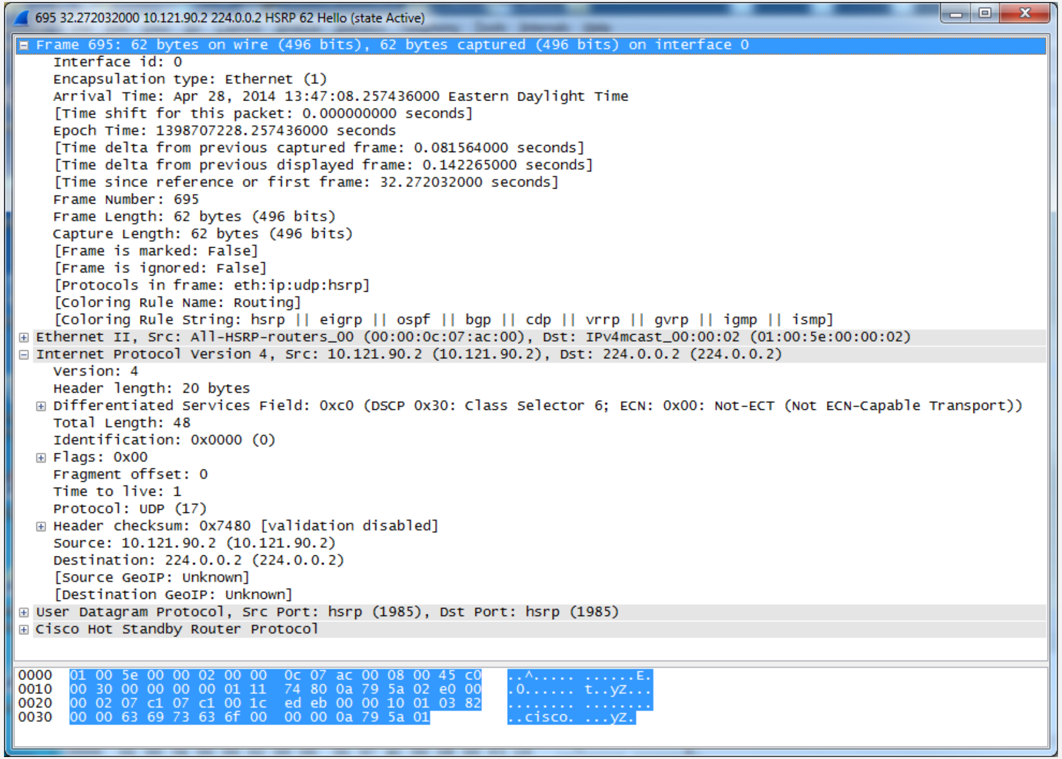
Copyright © www.ine.com

Encapsulation

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

Copyright © www.ine.com

Network Lab



695 32.272032000 10.121.90.2 224.0.0.2 HSRP 62 Hello (state Active)

```
⊟ Frame 695: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 28, 2014 13:47:08.257436000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1398707228.257436000 seconds
    [Time delta from previous captured frame: 0.081564000 seconds]
    [Time delta from previous displayed frame: 0.142265000 seconds]
    [Time since reference or first frame: 32.272032000 seconds]
    Frame Number: 695
    Frame Length: 62 bytes (496 bits)
    Capture Length: 62 bytes (496 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:hsrp]
    [Coloring Rule Name: Routing]
    [Coloring Rule String: hsrp || eigrp || ospf || bgp || cdp || vrrp || gvrp || igmp || ismp]
⊞ Ethernet II, Src: All-HSRP-routers_00 (00:00:0c:07:ac:00), Dst: IPv4mcast_00:00:02 (01:00:5e:00:00:02)
⊟ Internet Protocol Version 4, Src: 10.121.90.2 (10.121.90.2), Dst: 224.0.0.2 (224.0.0.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 48
    Identification: 0x0000 (0)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
  ⊞ Header checksum: 0x7480 [validation disabled]
    Source: 10.121.90.2 (10.121.90.2)
    Destination: 224.0.0.2 (224.0.0.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ User Datagram Protocol, Src Port: hsrp (1985), Dst Port: hsrp (1985)
⊞ Cisco Hot Standby Router Protocol

0000  01 00 5e 00 00 02 00 00  0c 07 ac 00 08 00 45 c0   ..^..... ......E.
0010  00 30 00 00 00 00 01 11  74 80 0a 79 5a 02 e0 00   .0...... t..yZ...
0020  00 02 07 c1 07 c1 00 1c  ed eb 00 00 10 01 03 82   ........ ........
0030  00 00 63 69 73 63 6f 00  00 00 0a 79 5a 01         ..cisco. ...yZ.
```

Copyright © www.ine.com

Capturing Protocol Data

- Captured protocol data can be inspected for issues
- Protocol analysis
  - Opens 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

Copyright © www.ine.com