# Networks Declassified:

## TCP/IP & Wireless Networking Survival Guide

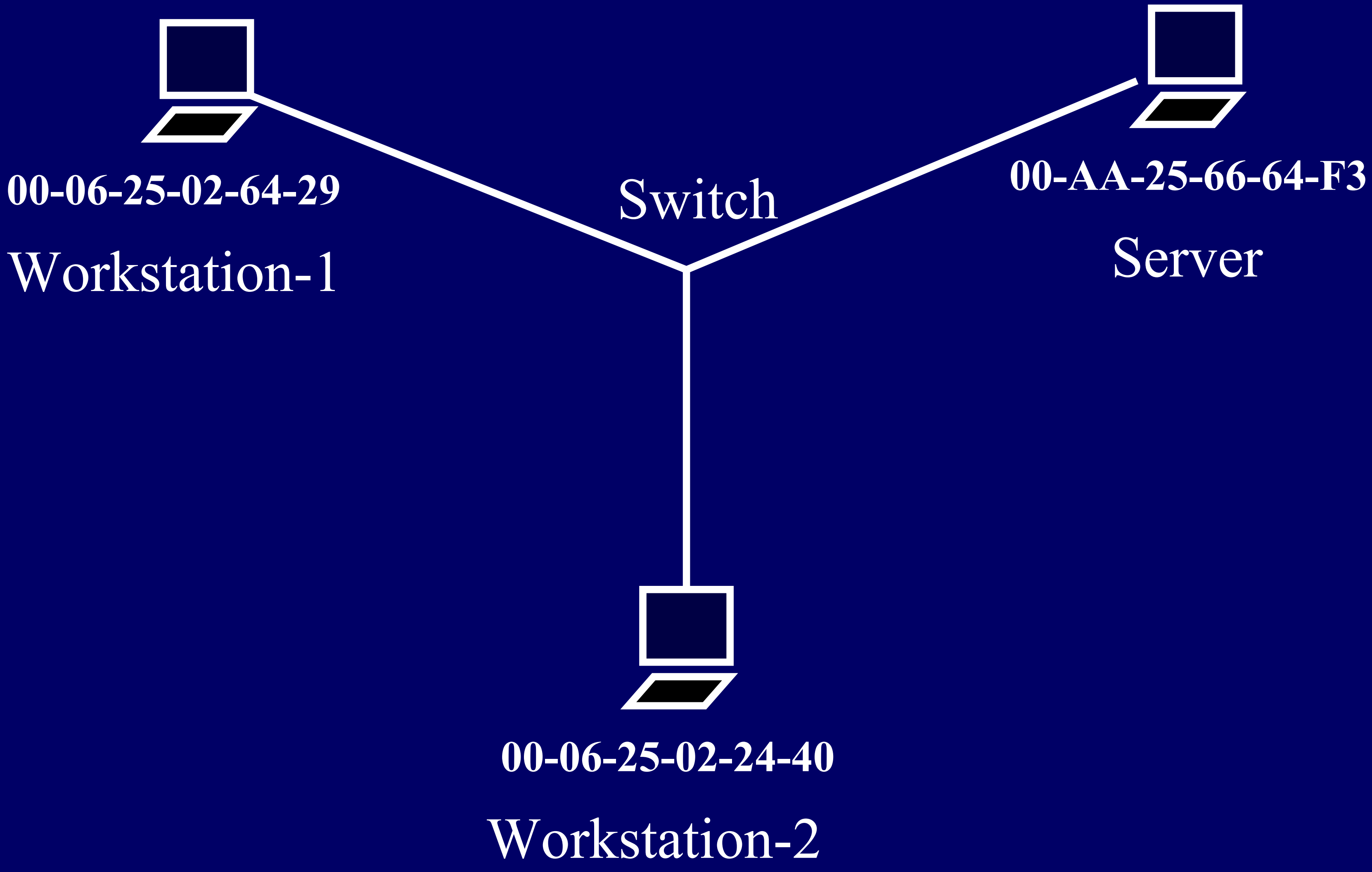
Steve Walker and Frank Fortner

# Seminar Overview

- Cable Media
- TCP/IP Protocol
- Packet Structure
- Addressing & Routing
- Wireless Fundamentals
- Realistic Wireless Surveys
- Wireless Pitfalls
- Wireless Security
- Stories From The Road

# Simple Network Diagram

## (demonstrates a “star” topology)



# The OSI 7 Layer Model

## The Secret “Geek” Sauce

| | |
|---|---|
| 7. Application | FTP - Telnet – LPR – WWW |
| 6. Presentation | Data is packaged and unpackaged for the app. |
| 5. Session | Establishes, manages and terminates connections among cooperating apps. (unused) |
| 4. Transport | TCP (guarantees reliable data stream) |
| 3. Network | IP or IPX (routing occurs here) |
| 2. Data Link | Ethernet - Token Ring –Arcnet |
| 1. Physical | Cable - wire – medium – Network cards |

# “Media” is at the Physical Level

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| **1. Physical** | Cable - wire – medium – Network cards |

# ETHERNET

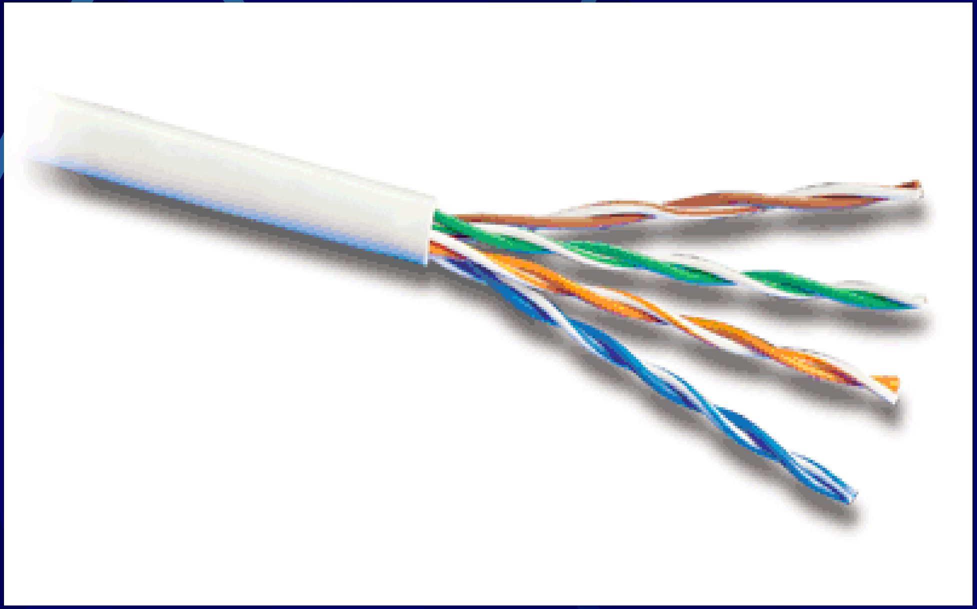
## The Road Most Traveled

- 10/100/1000 million bits/second
- data is encapsulated in packets
- packets are “addressed”
- Hardware is “addressed”
- Supports a variety of media

# UTP (Unshielded Twisted Pair)

## The "Plumbing" of Networking

- Essentially 8-wire telephone line
- Minimum Category 3 or above
- Maximum of 100 meters in length
- Maximum of 2 connections / segment
- EMI Sensitive



(Cat-5 cable w/ jacket removed)

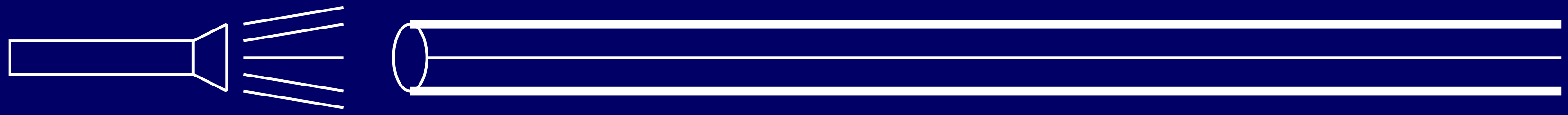
# UTP (continued)

- Gigabit Ethernet
  - Cat 5e & Cat 6 required as a minimum
- 10Gigabit Ethernet
  - High-end Cat 5e possible
  - Cat 6 better suited
  - Fiber required for long distances(+100M)

# Ethernet Media
## Fiber Optics

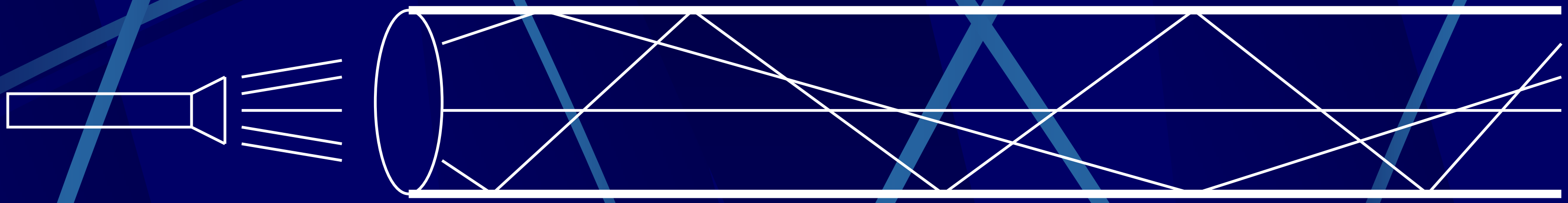
- Pairs of hair-like glass strands (TX & RX)
- Two propagation modes
  - Single Mode
  - Multimode
- Typically used for backbone connectivity

# Singlemode



- Extremely low signal loss, great for long distances
  - 70-100km possible
  - 10-20km typical
- High capacity

# Multimode



- Least costly
- Higher signal loss = shorter distances
  - Depending on fiber diameter and wavelength, ~1Km maximum distance
  - Special (Mode-Conditioning) patch cord required for distances over 300m

# Patch Cords
## Plugging It In!

- Standard Fiber Patch Cord
  - $10-20/foot
  - Limited to multi or single fiber only

- Mode Conditioning Fiber Patch Cord
  - $30-50/foot
  - Allows you to use cheaper multimode fiber with single mode equipment

# Building Bigger Networks at the Physical Layer

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| **1. Physical** | Cable - wire – medium – Network cards |

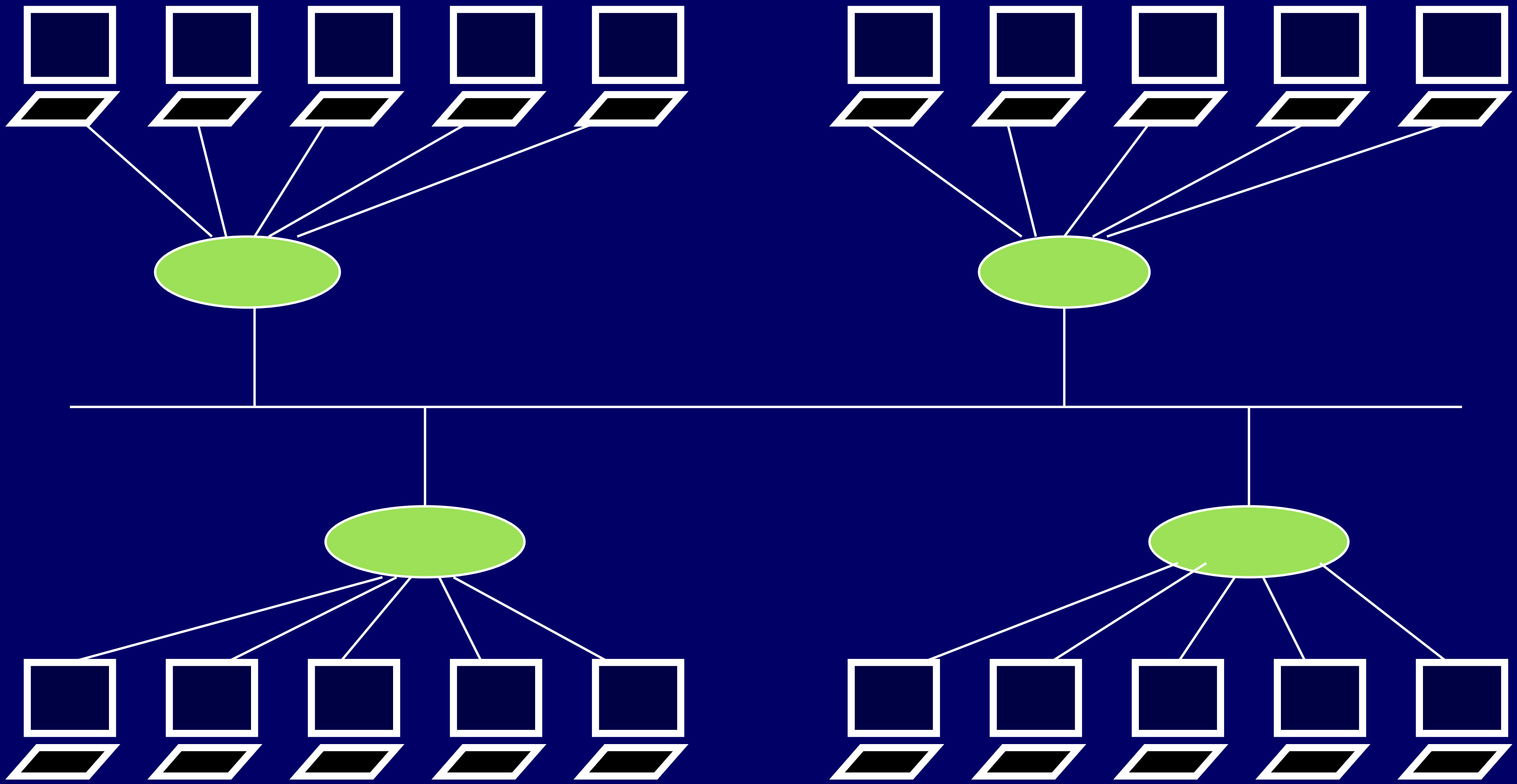
# Building Bigger Networks at the Physical Layer

- Mult-Segment networks (Lan to Lan)
  - Allows you to exceed cable restrictions
  - Allows growth
  - Isolates workgroup traffic
- Wide Area Networks (WAN)
  - Connects multiple facilities
  - Transparent to users

# HUB
## (Connecting Legacy Networks)

- Allows connection of multiple like segments
- Re-times, repeats and boosts signal
- Limit of 2 hubs between any 2 nodes
- Limit of 4 hubs on any 1 segment
- Works at physical layer (1) of OSI model
- Allows devices to be physically cabled as a “star” but functions as a “bus”
- Also called “Concentrator” or “Repeater”

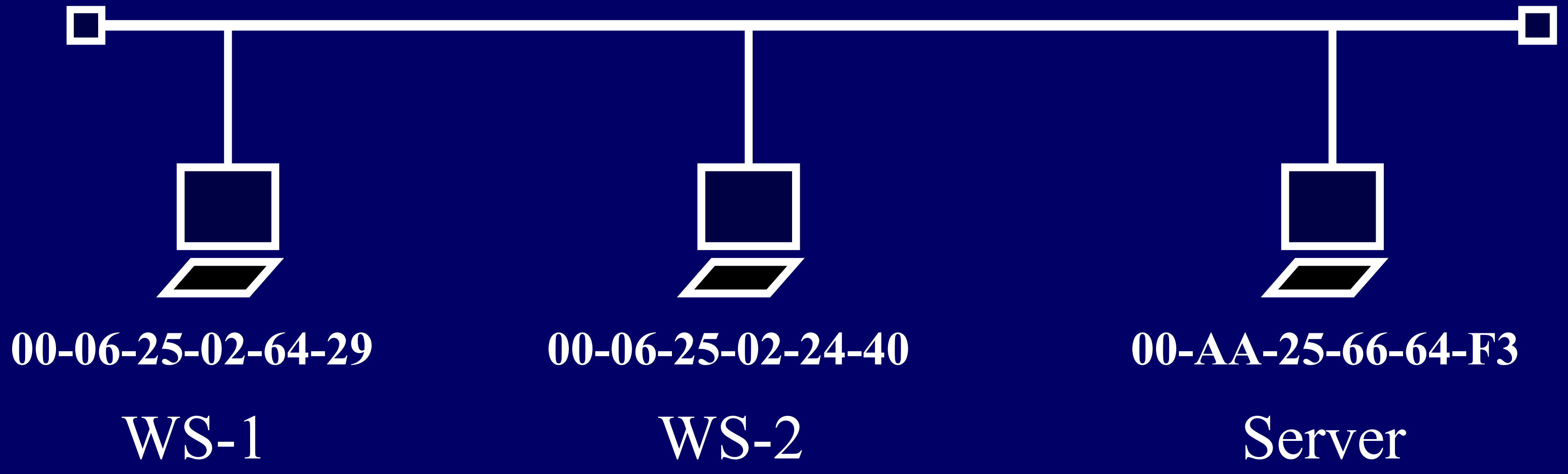
# Network built with hubs



# Building bigger networks at the Data Link Layer

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| **2. Data Link** | Ethernet - Token Ring –Arcnet - Packets |
| **1. Physical** | Cable - wire – medium – Network cards |

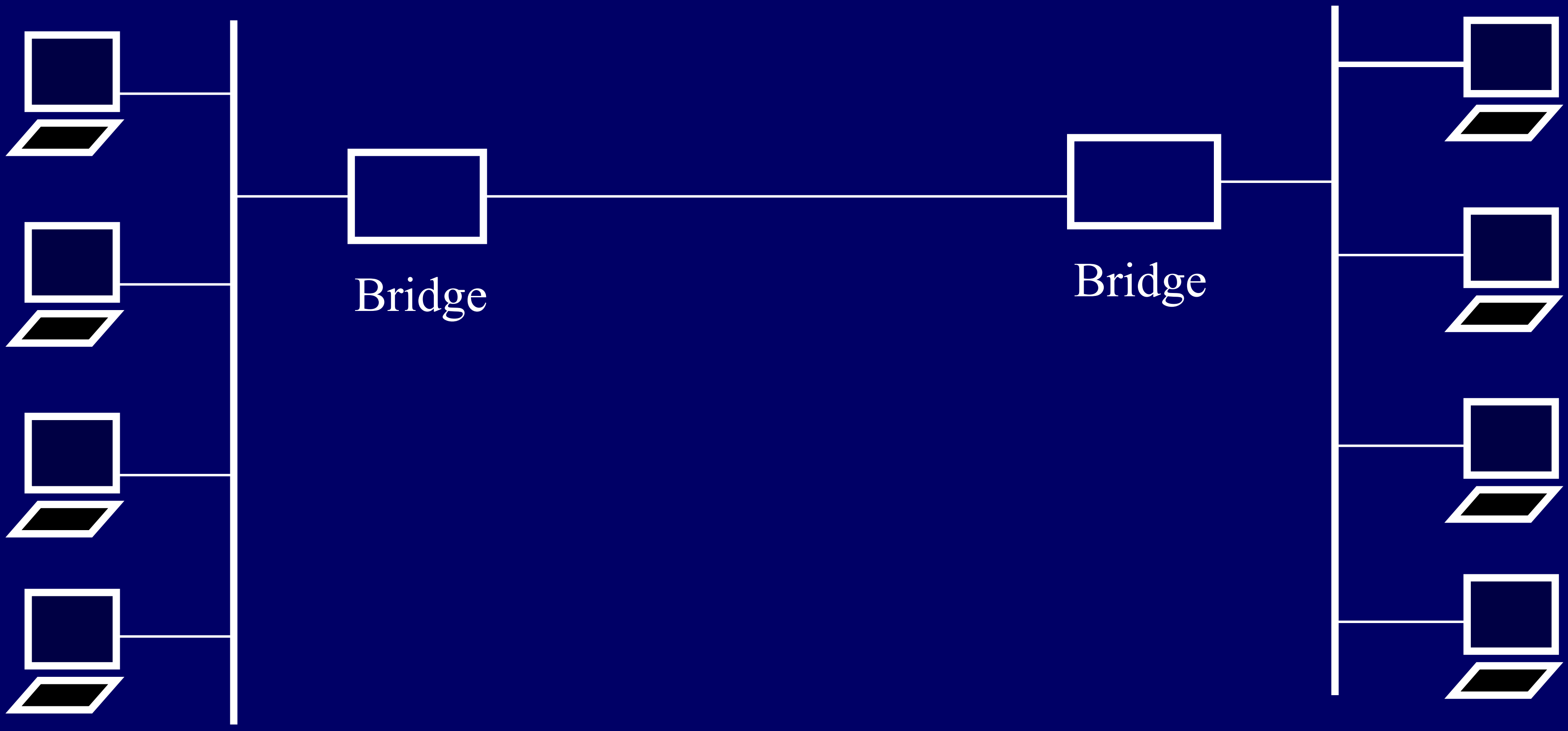
# “Logical” Network Diagram



# Bridges
# Networking's Border Patrol

- Allows connection of two like segments
- "Intelligent" device
- Only forwards packets if needed
- Provides MAC layer traffic management
- Functions at "Data Link" (2) layer of OSI model
- Maximum 7 bridges between any 2 nodes

# Typical Bridge Application



# Switches
# A Box of Bridges

- Designed for high speed networks
- Often performs both bridging and routing
- Switches high speed network traffic to multiple 10/100/1000 Mbps segments.
- Performs traffic management to reduce network bottlenecks.

# Switched Blades and Fabric

- Fabric
  - Combination of hardware and software
  - Devices connected to each other via switches
  - Creates multiple paths to reduce failure

- Blades
  - Fixed capacity of blades, but multiple options for each blade configuration
  - Easily scalable

Example:

Blade Server

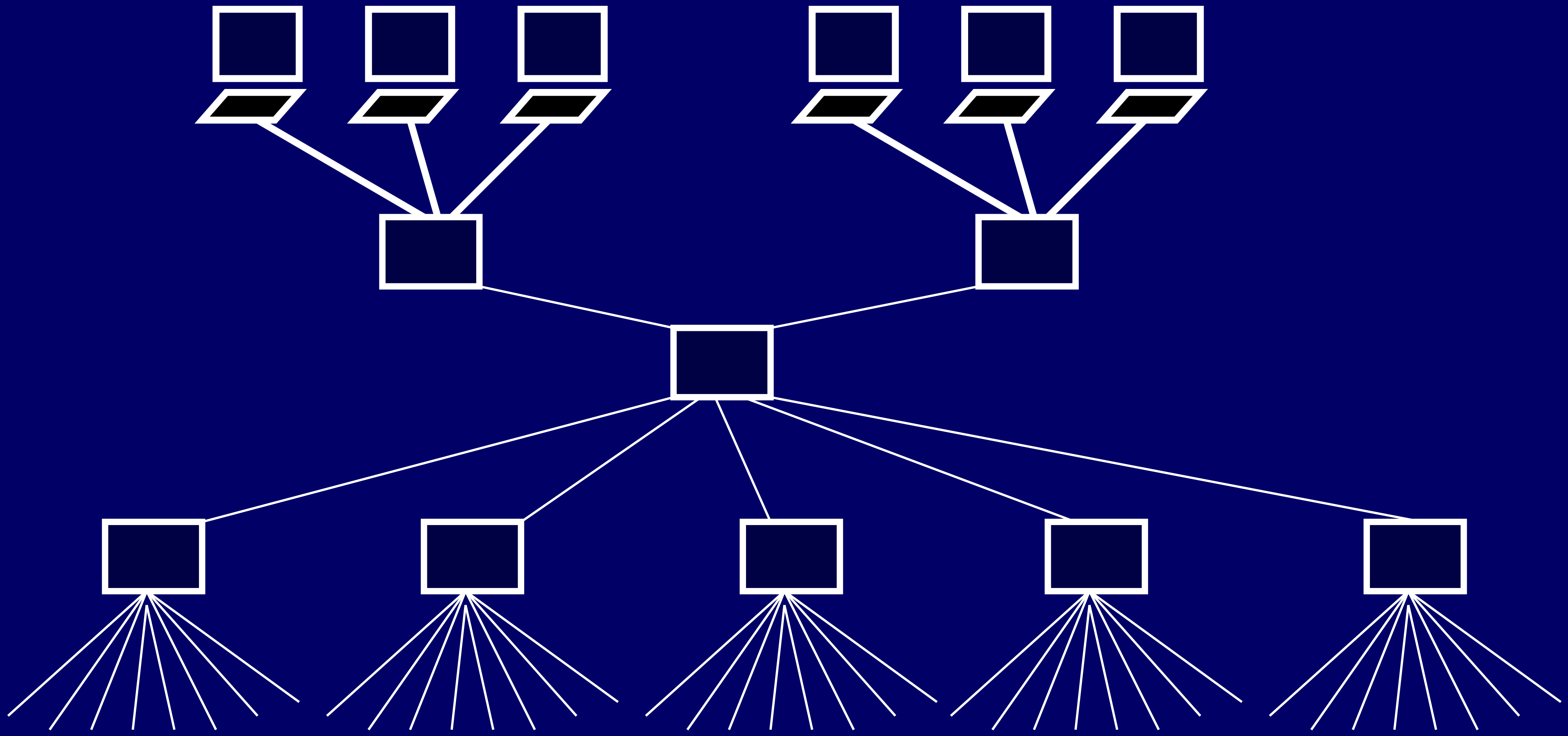
Blade 1: Fiber link

Blade 2: Ethernet switch link

Blade 3: Token Ring link

Blade 4: Fiber Channel SAN link

# Network built with switches



# Packet Structure *

| | | | |
|---|---|---|---|
| 802.3 | | | |
| destination | source | length | data |
| 6 bytes | 6 bytes | 2 bytes | 46-1500 |

# Typical Ethernet Packet

## (Hex dump)

```
00 CA 00 14 40 48 00 AA 00 37 EF 40 08

00 A5 00 00 29 01 A3 00 00 FF C6 E2 B4

C7 F2 A3 90 C7 F2 A4 01 04 ED AC ED 01

00 E8 18 0F EE D7 89 50 18 07 FF BC A4

00 00 41 00 00 00 00 00
```

# Typical Ethernet Packet

## (Hex dump)

```
00 AA 00 14 40 48   00 AA 00 37 0F 40   08
  Destination MAC Address   Source Mac Address   Type
00 45 00 00 29 01 A3 00 00 FF 06 E2 B4
Type
C7 F2 A3 90 C7 F2 A4 01 04 0A 00 17 01

00 8E 18 00 EE 77 89 50 18 07 FF BC A4

00 00 41 00 00 00 00 00
```

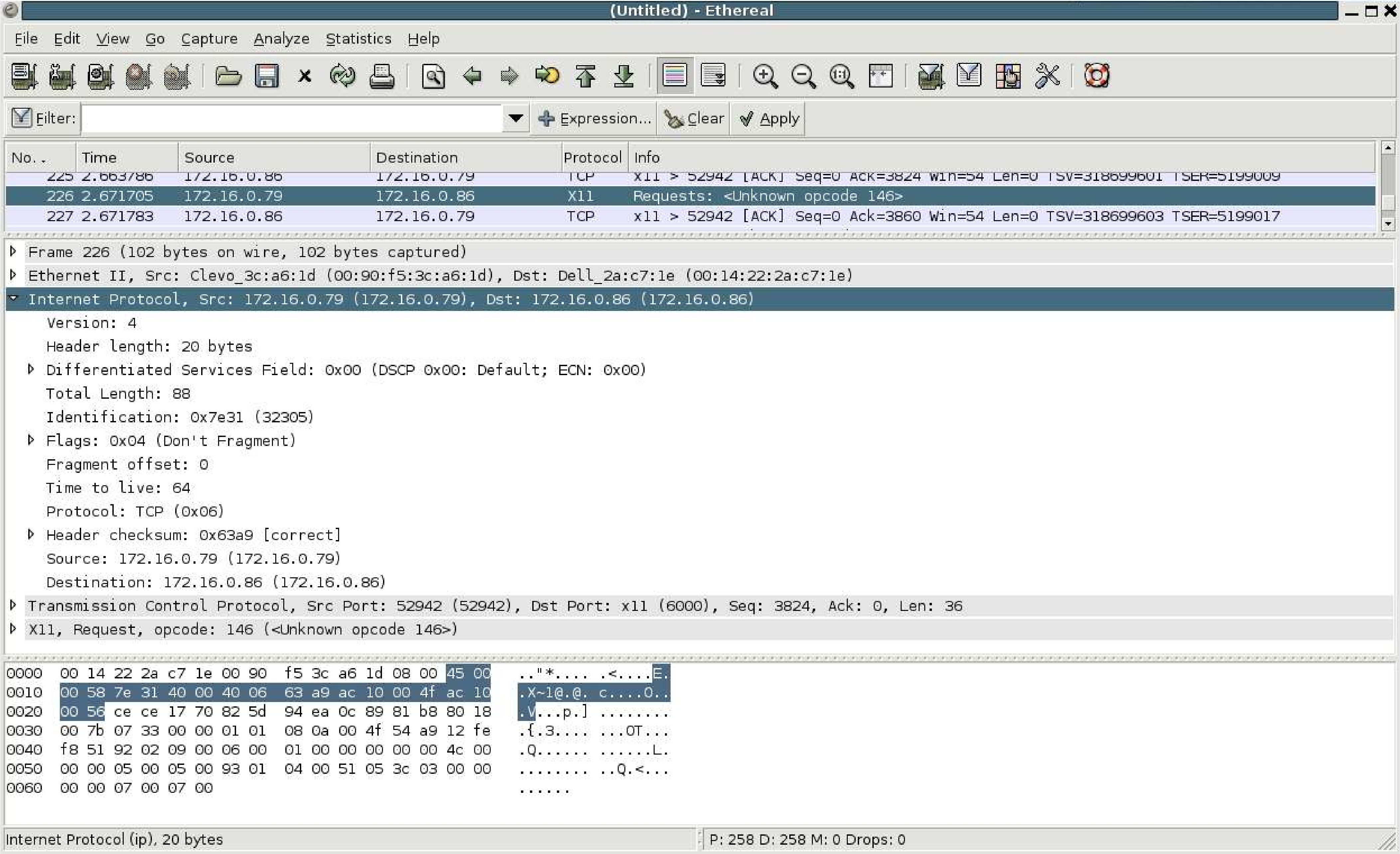
# Capturing Packets
## Network "Eavesdropping"

- A piece of software called a **Packet Sniffer** is used to capture packets.

Examples:

- Ethereal (Now WireShark) It's Free!
- Sniffer
- WildPackets
- EtherSnoop

# Ethereal



```
No. .  Time      Source        Destination   Protocol Info
  225 2.663786  172.16.0.86   172.16.0.79   TCP      x11 > 52942 [ACK] Seq=0 Ack=3824 Win=54 Len=0 TSV=318699601 TSER=5199009
  226 2.671705  172.16.0.79   172.16.0.86   X11      Requests: <Unknown opcode 146>
  227 2.671783  172.16.0.86   172.16.0.79   TCP      x11 > 52942 [ACK] Seq=0 Ack=3860 Win=54 Len=0 TSV=318699603 TSER=5199017
```

```
▷ Frame 226 (102 bytes on wire, 102 bytes captured)
▷ Ethernet II, Src: Clevo_3c:a6:1d (00:90:f5:3c:a6:1d), Dst: Dell_2a:c7:1e (00:14:22:2a:c7:1e)
▽ Internet Protocol, Src: 172.16.0.79 (172.16.0.79), Dst: 172.16.0.86 (172.16.0.86)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 88
    Identification: 0x7e31 (32305)
  ▷ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
  ▷ Header checksum: 0x63a9 [correct]
    Source: 172.16.0.79 (172.16.0.79)
    Destination: 172.16.0.86 (172.16.0.86)
▷ Transmission Control Protocol, Src Port: 52942 (52942), Dst Port: x11 (6000), Seq: 3824, Ack: 0, Len: 36
▷ X11, Request, opcode: 146 (<Unknown opcode 146>)
```

```
0000  00 14 22 2a c7 1e 00 90  f5 3c a6 1d 08 00 45 00   .."*.... .<....E.
0010  00 58 7e 31 40 00 40 06  63 a9 ac 10 00 4f ac 10   .X~1@.@. c....O..
0020  00 56 ce ce 17 70 82 5d  94 ea 0c 89 81 b8 80 18   .V...p.] ........
0030  00 7b 07 33 00 00 01 01  08 0a 00 4f 54 a9 12 fe   .{.3.... ...OT...
0040  f8 51 92 02 09 00 06 00  01 00 00 00 00 00 4c 00   .Q...... ......L.
0050  00 00 05 00 05 00 93 01  04 00 51 05 3c 03 00 00   ........ ..Q.<...
0060  00 00 07 00 07 00                                  ......
```

Internet Protocol (ip), 20 bytes

P: 258 D: 258 M: 0 Drops: 0

# Building bigger networks at the Network level

| | |
|---|---|
| | |
| | |
| | |
| | |
| **3. Network** | The “IP” of TCP/IP is here |
| **2. Data Link** | Ethernet - Token Ring –Arcnet |
| **1. Physical** | Cable - wire – medium – Network cards |

# Routers
# Networking's "Mailman"

- Adds layer of responsibility
- Allows connection of same or different types of segments
- Routes packets based on network protocol
- Functions at "Network" (3) layer of OSI model
- Must specifically support protocol(s)
- Virtually "unlimited" routers allowed between any 2 nodes.
- Slower, 10-200 microseconds latency compared to switches at 200-300 nanoseconds; not very noticeable

# Routers

- Core Routers
  - Higher end routers
  - Able to move large amounts of data internal to your network

- Edge Routers
  - High end routers
  - Best suited for placement at the “edge” of your network.
  - Able to move large amounts of data

# Routing vs. Switching

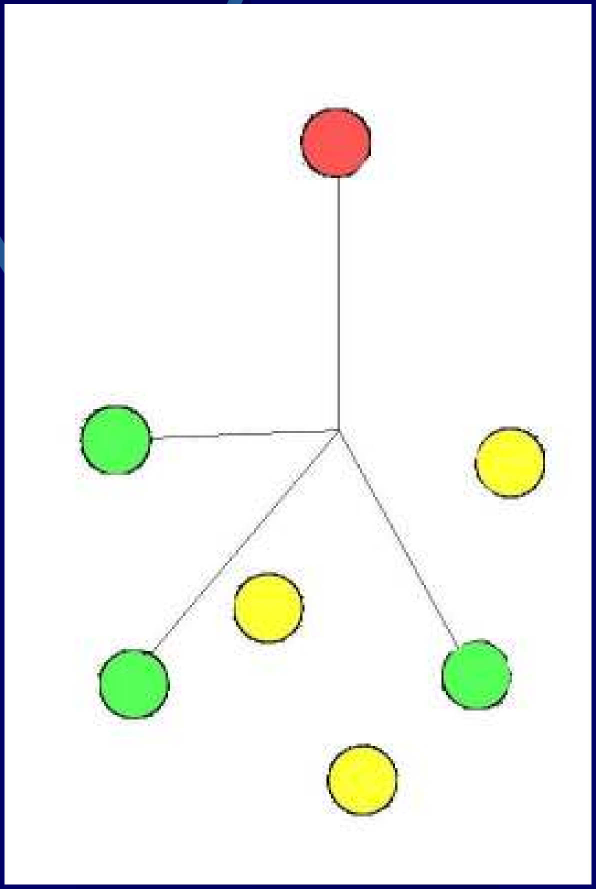
- Search based
- Fast
- Able to dynamically change paths
- Layer 3
- Best for joining two or more networks
- More expensive
- Limit broadcast domains

- Routing software in every switch in the network
- Index based
- Fast
- Layer 2, layer 3 possible.
- Layer 3 switches function much like routers
- Cheap

# Multicast Communication

## Networking's "Party Line" via Routers

- Send one copy and the subscribers all receive it
- Allows for an unknown number of receivers
- Sender only initiates one stream of data, the router controls where the data is going next
- More efficient than unicasting (sending each recipient requires another copy/transmission)
- Excellent for video conferences



# The “IP” of TCP/IP

## (Transmission Control Protocol / Internet Protocol)

- A protocol that routes data
- Not responsible for logical errors
- Common Protocol for Novell, Meditech, VAX and many other systems
- The Internet’s protocol
- Designed for easy routing

# Typical Ethernet Packet

## (Hex dump)

```
00    AA    00    14    40    48    00    AA    00    37    0F    40    08
      Destination MAC Address          Source Mac Address              Type

00    45    00    00    29    01    A3    00    00    FF    06    E2    B4
Type  V H   flags length      Ident       flag/offset TTL   prot  hdr chksum

C7    F2    A3    90    C7    F2    A4    01    04    0A    00    17    01
src(199.242.163.144)    dest(199.242.164.1)

00    8E    18    00    EE    77    89    50    18    07    FF    BC    A4

00    00    41    00    00    00    00    00
```

# “TCP” of TCP/IP is at the Transport level

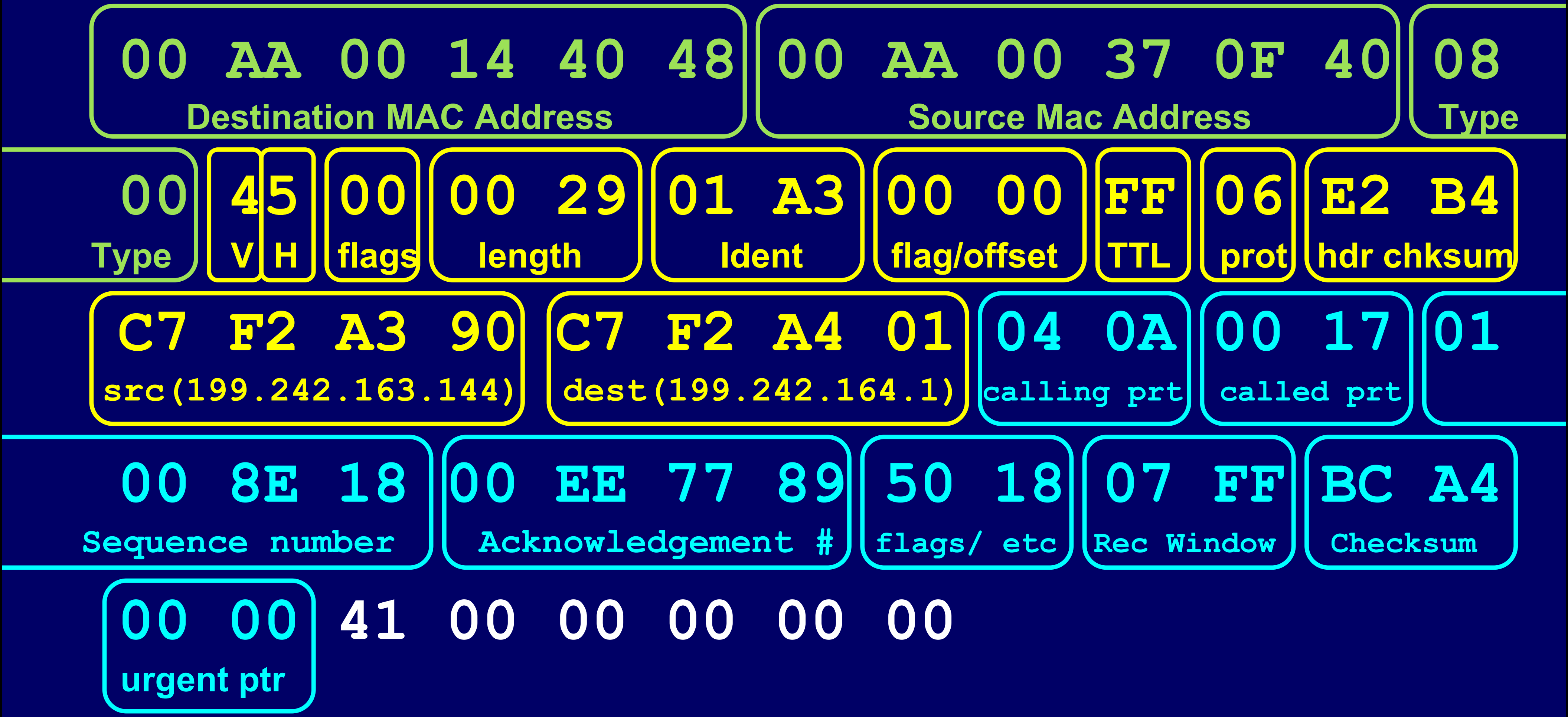
| | |
|---|---|
| | |
| | |
| | |
| **4. Transport** | TCP (guarantees reliable data stream) |
| **3. Network** | IP or IPX (routing occurs here) |
| **2. Data Link** | Ethernet - Token Ring –Arcnet |
| **1. Physical** | Cable - wire – medium – Network cards |

# The “TCP” of TCP/IP

- Operates at Transport Layer (layer 4)
- TCP - Transmission Control Protocol
- Guarantees reliable transmission of data stream over IP between two computers
- Some error checking built in

# Typical Ethernet Packet

## (Hex dump)



```
  00 AA 00 14 40 48         00 AA 00 37 0F 40      08
   Destination MAC Address   Source Mac Address    Type
  00   45   00     00 29   01 A3     00 00      FF  06    E2 B4
 Type  V H  flags  length  Ident   flag/offset  TTL prot  hdr chksum
  C7 F2 A3 90            C7 F2 A4 01          04 0A        00 17       01
 src(199.242.163.144)   dest(199.242.164.1)   calling prt  called prt
  00 8E 18          00 EE 77 89         50 18        07 FF        BC A4
 Sequence number    Acknowledgement #   flags/ etc   Rec Window   Checksum
  00 00    41 00 00 00 00 00
 urgent ptr
```

# Layer 4 Switching
## Playing Favorites

- Uses TCP port information to enhance routing decisions
- Can give traffic priority based on the port
- Prioritizing certain ports can alleviate painful network congestion

# The OSI 7 Layer Model

## Closing the Loop

| | |
|---|---|
| **7. Application** | FTP - Telnet – LPR – WWW |
| **6. Presentation** | Data is packaged and unpackaged for the app. |
| **5. Session** | Establishes, manages and terminates connections among cooperating apps. (unused) |
| **4. Transport** | TCP (guarantees reliable data stream) |
| **3. Network** | IP or IPX (routing occurs here) |
| **2. Data Link** | Ethernet - Token Ring –Arcnet |
| **1. Physical** | Cable - wire – medium – Network cards |

# Protocols on Your MEDITECH System

- Telnet
- LPR/LPD
- FTP

# How does TCP/IP work

- Every network has an address “space”
- Every computer has a specific IP address
- The IP protocol routes packets from the transmitting machine to the receiving machine
- The TCP protocol breaks “message” to manageable packets
- The TCP protocol ensures an accurate stream of data packets

# Address Format

- All addresses are considered to be in two parts
- First part is “Network Address”
  - Assigned by the NIC
  - Determines size of net
- Last part is “Local Address”
  - Administered by network owner
- Addresses are Classified A,B,C,D,E

# Subnetting Example

- Class B address subnetted into 254 class C addresses.

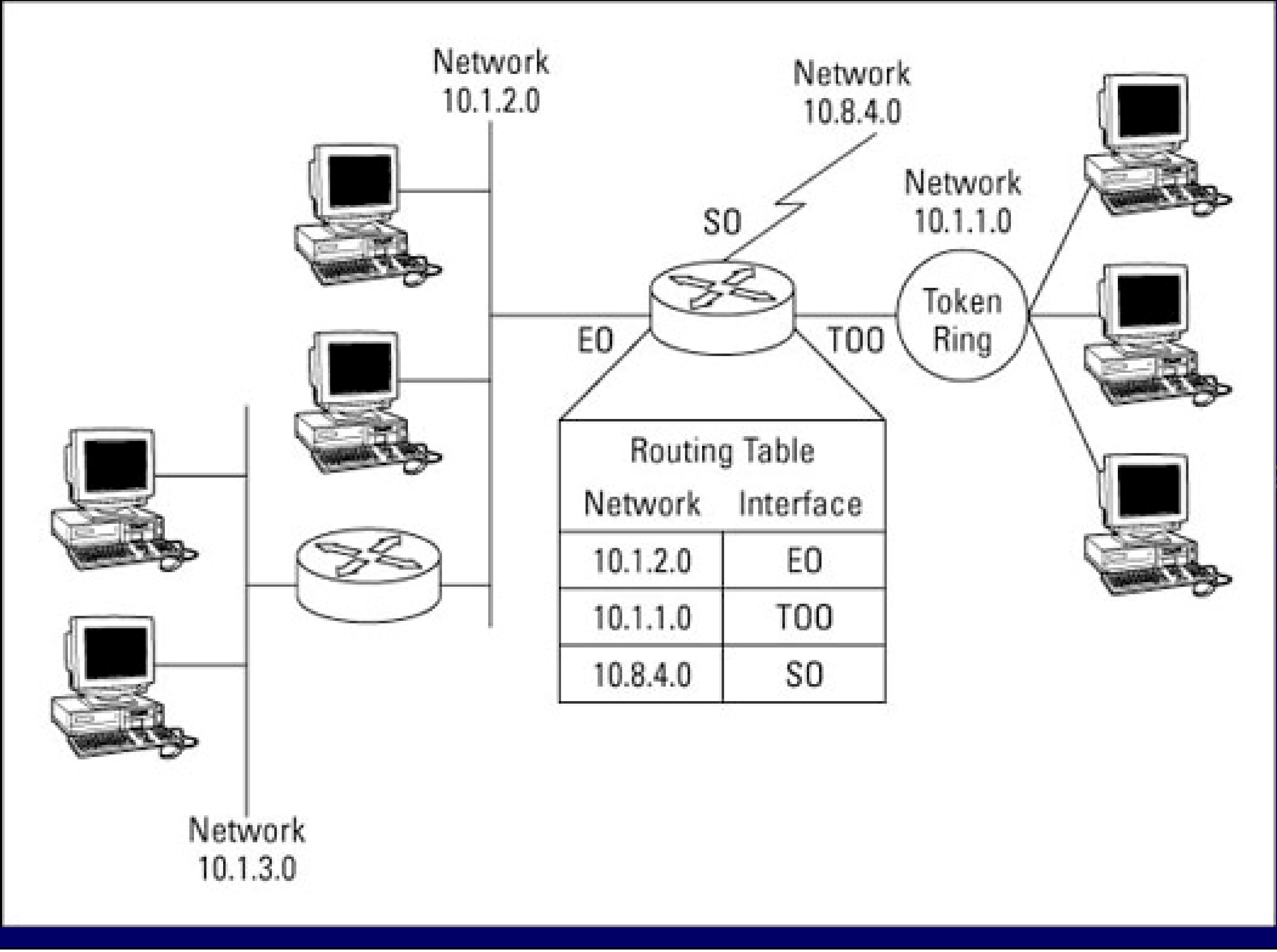
| | | |
|---|---|---|
| 130 192 | 200 | 182 |
| network | sub<br>net | host |

| | | | | | |
|---|---|---|---|---|---|
| addr | 1000 1100 | 1100 0000 | 1100 1000 | 1011 0110 | (130.192.200.182) |
| mask | 1111 1111 | 1111 1111 | 1111 1111 | 0000 0000 | (255.255.255.0) |

# IP Routing

- Transmission of datagram from one node to another on the same or different network
- Two Types -
  - Local - destination on same network
  - Remote - destination on different network
- Net Mask is used to determine if destination is on the same net.

# Routing on Class A Network



Routing Table

| Network | Interface |
|---|---|
| 10.1.2.0 | EO |
| 10.1.1.0 | TOO |
| 10.8.4.0 | SO |

# Wireless Networking
## Can you hear me now?

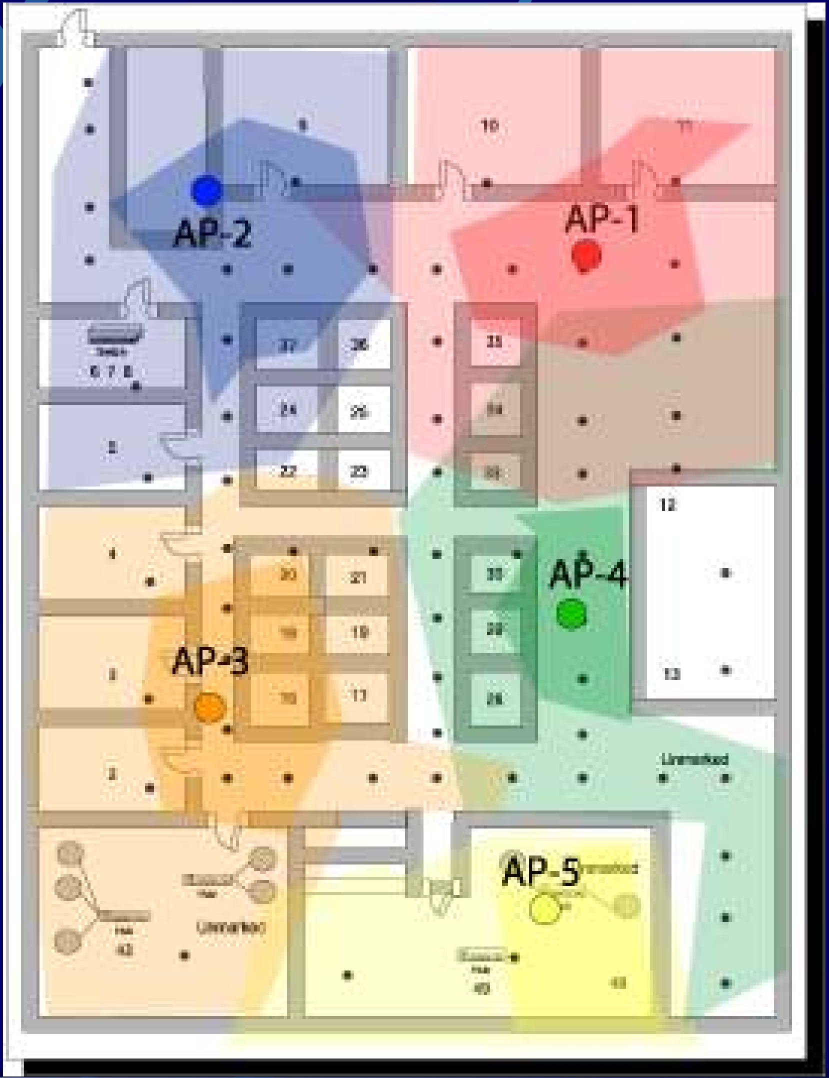
- Most common is 802.11b/g (2.4Ghz)
- Less common is 802.11a (5.8Ghz)
- 11/54 Megabits in theory
- EMI Sensitive (Very)
- Usually implemented with an "Access Point"
- Very insecure "out of the box"

# Wireless Survey
## Save yourself some pain!

- Initial Survey
  - Establish location of AP’s
  - Evaluate network coverage
  - Evaluate user needs/security
- Periodic surveys
  - Discover rogue wireless devices
  - Evaluate network coverage
    - Weak areas for signal increase
    - Strong areas for signal decrease to prevent unwanted coverage
  - Test security measures

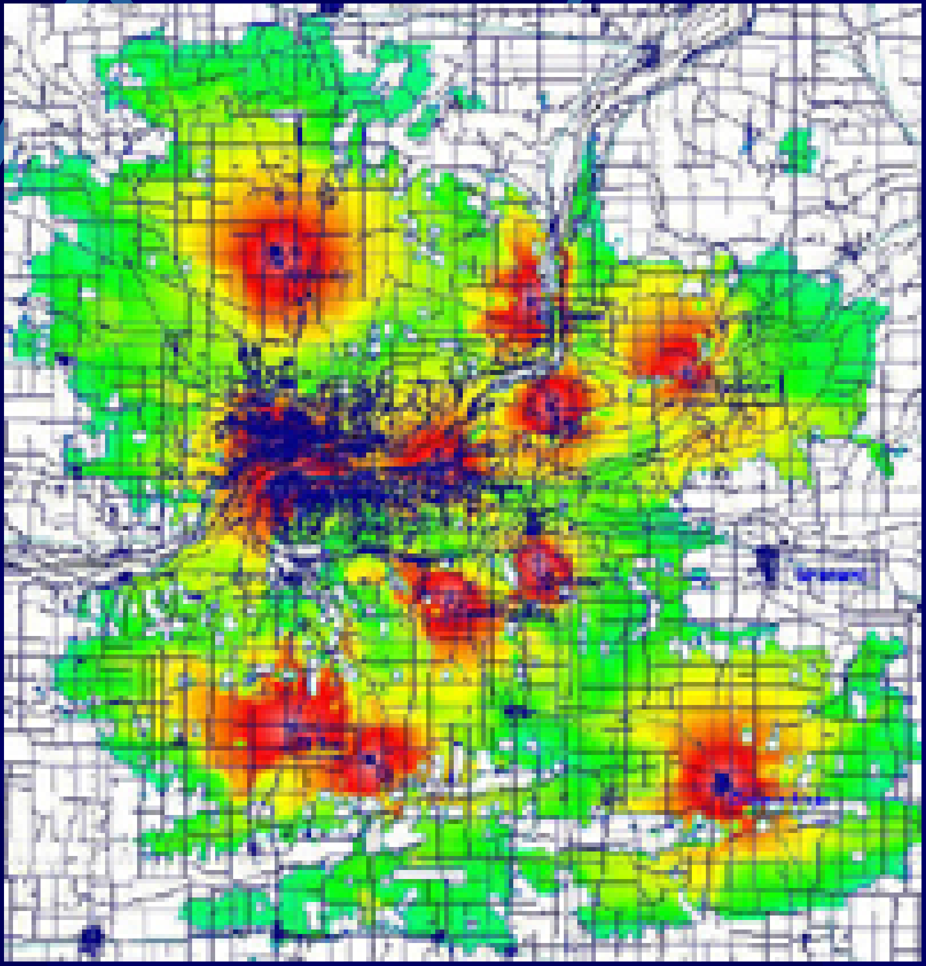
# Wireless Survey (continued)

Your individual survey will show your weak and strong areas. Walls, doors, pipes, ducts, windows, any large object can have an effect on your wireless coverage.

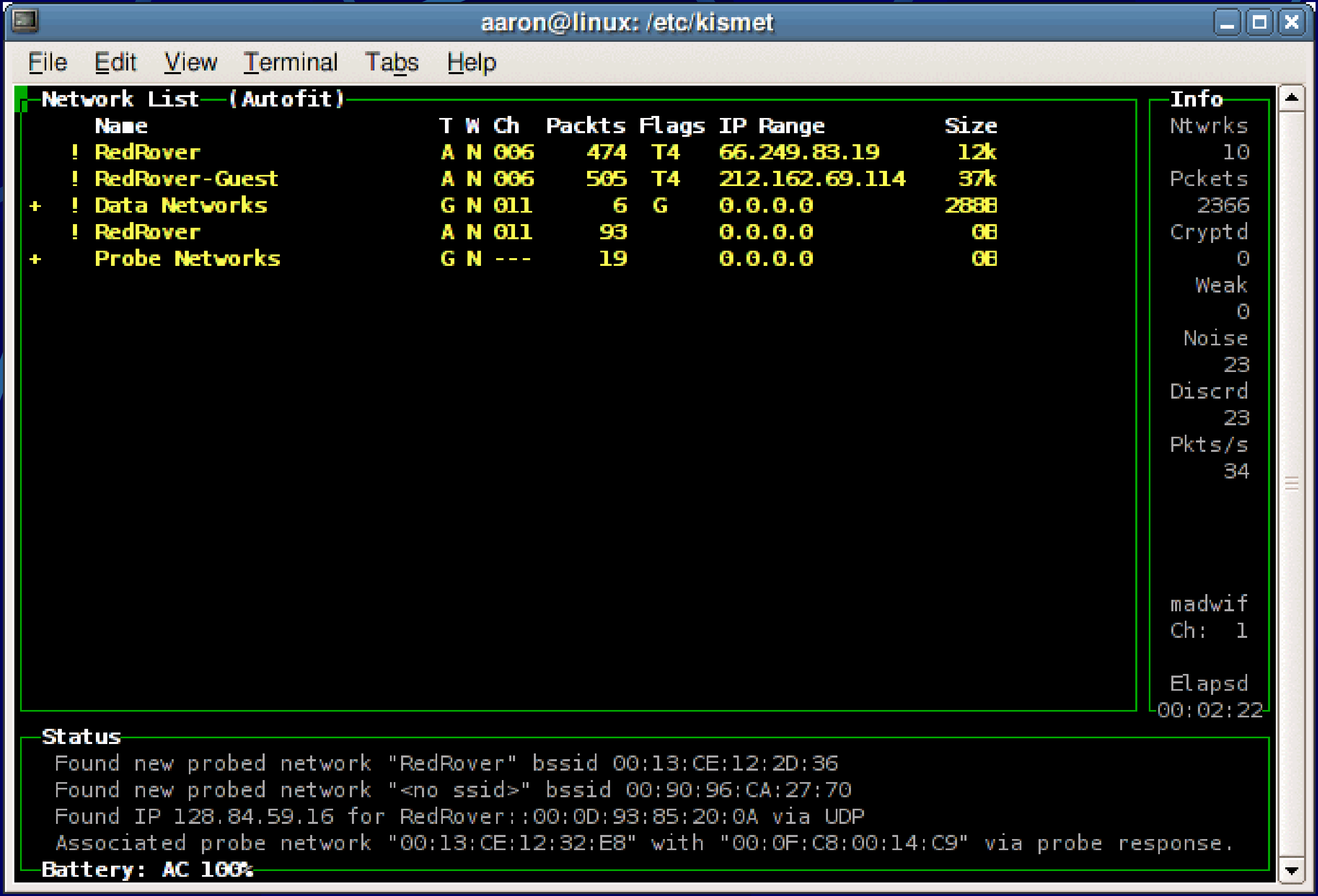


# Wireless Survey (continued)

It may look like a weather map, but this is the result of two pieces of software: Kismet and GPS visualizer.



# Kismet

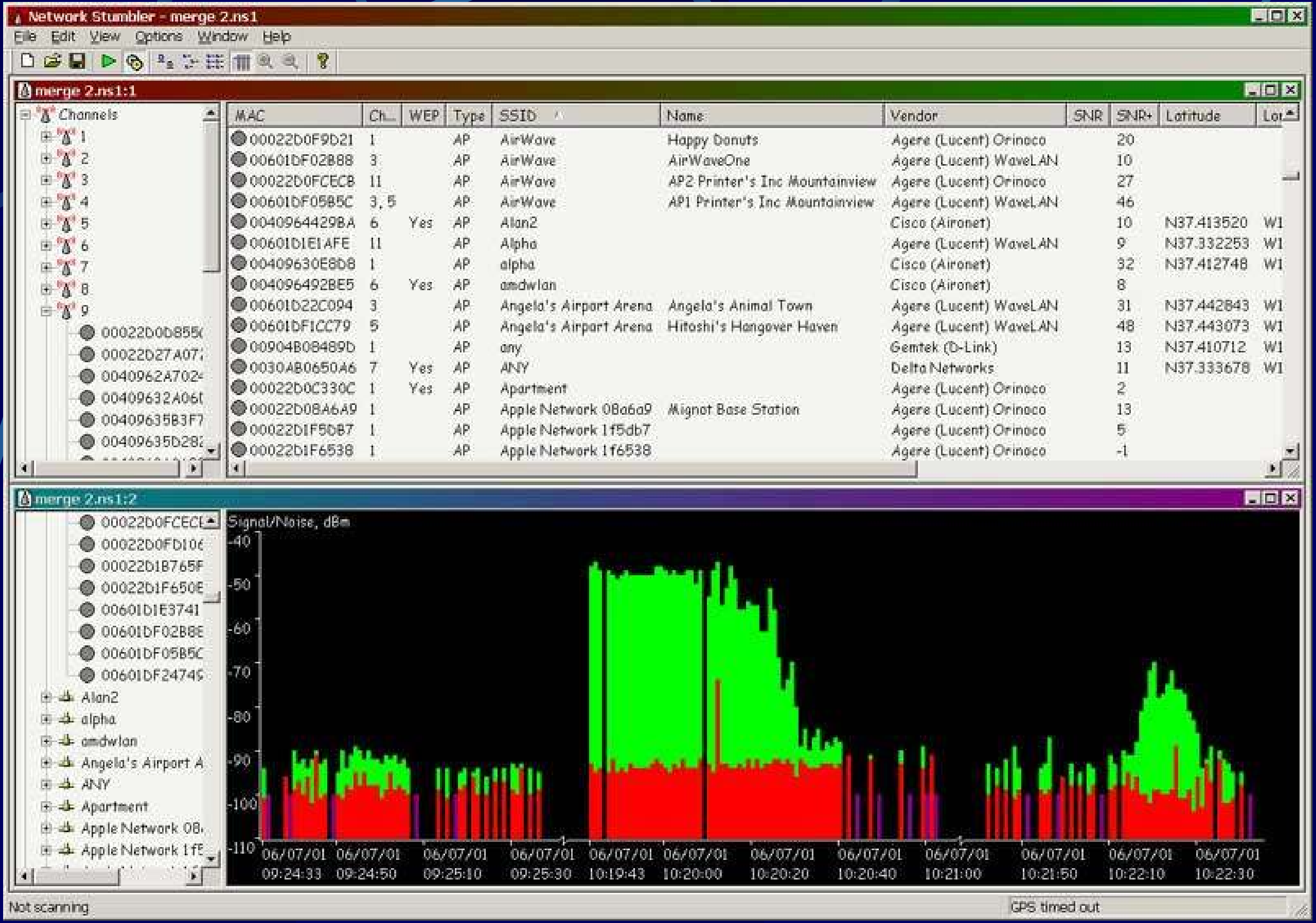


```
Network List—(Autofit)                                                                  Info
     Name                       T W Ch  Packts Flags IP Range        Size   Ntwrks
   ! RedRover                   A N 006   474  T4    66.249.83.19     12k      10
   ! RedRover-Guest             A N 006   505  T4    212.162.69.114   37k   Pckets
 + ! Data Networks              G N 011     6  G     0.0.0.0         288B     2366
   ! RedRover                   A N 011    93        0.0.0.0           0B   Cryptd
 +   Probe Networks             G N ---    19        0.0.0.0           0B        0
                                                                              Weak
                                                                                 0
                                                                             Noise
                                                                                23
                                                                            Discrd
                                                                                23
                                                                            Pkts/s
                                                                                34

                                                                            madwif
                                                                            Ch:  1

                                                                            Elapsd
                                                                          00:02:22
Status
  Found new probed network "RedRover" bssid 00:13:CE:12:2D:36
  Found new probed network "<no ssid>" bssid 00:90:96:CA:27:70
  Found IP 128.84.59.16 for RedRover::00:0D:93:85:20:0A via UDP
  Associated probe network "00:13:CE:12:32:E8" with "00:0F:C8:00:14:C9" via probe response.
Battery: AC 100%
```

# Netstumbler



Network Stumbler - merge 2.ns1

merge 2.ns1:1

| MAC | Ch... | WEP | Type | SSID | Name | Vendor | SNR | SNR+ | Latitude | Lo |
|---|---|---|---|---|---|---|---|---|---|---|
| 00022D0F9D21 | 1 | | AP | AirWave | Happy Donuts | Agere (Lucent) Orinoco | | 20 | | |
| 00601DF02B88 | 3 | | AP | AirWave | AirWaveOne | Agere (Lucent) WaveLAN | | 10 | | |
| 00022D0FCECB | 11 | | AP | AirWave | AP2 Printer's Inc Mountainview | Agere (Lucent) Orinoco | | 27 | | |
| 00601DF05B5C | 3, 5 | | AP | AirWave | AP1 Printer's Inc Mountainview | Agere (Lucent) WaveLAN | | 46 | | |
| 0040964429BA | 6 | Yes | AP | Alan2 | | Cisco (Aironet) | | 10 | N37.413520 | W1 |
| 00601D1E1AFE | 11 | | AP | Alpha | | Agere (Lucent) WaveLAN | | 9 | N37.332253 | W1 |
| 00409630E8D8 | 1 | | AP | alpha | | Cisco (Aironet) | | 32 | N37.412748 | W1 |
| 004096492BE5 | 6 | Yes | AP | amdwlan | | Cisco (Aironet) | | 8 | | |
| 00601D22C094 | 3 | | AP | Angela's Airport Arena | Angela's Animal Town | Agere (Lucent) WaveLAN | | 31 | N37.442843 | W1 |
| 00601DF1CC79 | 5 | | AP | Angela's Airport Arena | Hitoshi's Hangover Haven | Agere (Lucent) WaveLAN | | 48 | N37.443073 | W1 |
| 00904B08489D | 1 | | AP | any | | Gemtek (D-Link) | | 13 | N37.410712 | W1 |
| 0030AB0650A6 | 7 | Yes | AP | ANY | | Delta Networks | | 11 | N37.333678 | W1 |
| 00022D0C330C | 1 | Yes | AP | Apartment | | Agere (Lucent) Orinoco | | 2 | | |
| 00022D08A6A9 | 1 | | AP | Apple Network 08a6a9 | Mignot Base Station | Agere (Lucent) Orinoco | | 13 | | |
| 00022D1F5DB7 | 1 | | AP | Apple Network 1f5db7 | | Agere (Lucent) Orinoco | | 5 | | |
| 00022D1F6538 | 1 | | AP | Apple Network 1f6538 | | Agere (Lucent) Orinoco | | -1 | | |

merge 2.ns1:2

Not scanning

GPS timed out

# Wireless Pitfalls

- No barrier to entry (no wall jack to find)
- Inclement weather causes signal degradation
- 802.11b/g fair range, relatively cheap, many devices at same frequency
  - (microwave ovens, cordless phones, security radios/monitors)
- 802.11a shorter range, higher cost, fewer devices at same frequency

# Wireless Security

- WEP, Wired Equivalent Privacy
  - RC4 Algorithm
  - Easily compromised, suitable for home networks
- WPA, Wi-Fi Protected Access
  - RC4 Algorithm
  - Pre-shared Key or 802.1x authentication
  - Much more secure when Radius is used
- WPA2, Wi-Fi Protected Access 2
  - AES-based algorithm
  - Pre-shared Key or 802.1x authentication
  - Much more secure when Radius is used

# Stories

## from the

# Road