802.11 Wireless Security

The Protocol Analysis Perspective

Joe Bardwell

VP of Professional Services
WildPackets, Inc.

www.wildpackets.com

What Is Protocol Analysis ?

- Capture packets using a protocol analyzer tool
  - The packets go into the analyzer’s buffer
  - The analyzer software decodes the packets
  - Statistics, problem reports, and packet contents are assessed
- Device-to-device behavior is disclosed
  - You can directly observe the interactions between machines
  - You see where packets came from, and where they went
  - You identify appropriate and inappropriate behavior

How Are Conversations Analyzed ?

- The features of your analyzer are used to manipulate packets and extract relevant conversations
- Determine whether the observed behavior is consistent with your expectation for “correct” behavior

Using a protocol analyzer is not exceptionally difficult.

The challenge is to understand the technology, engineering, and networking concepts that make communication possible.

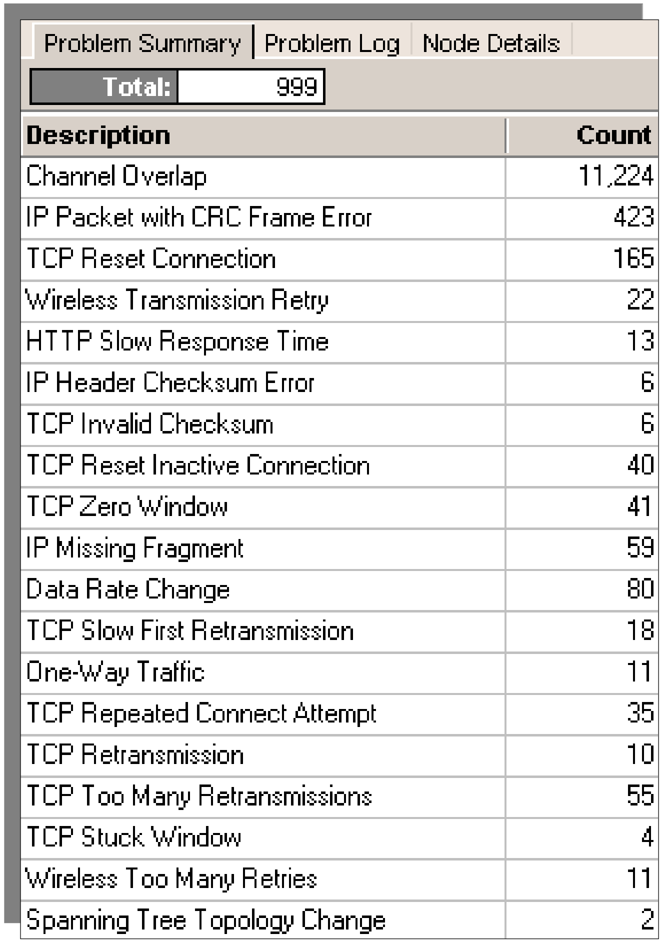
Protocol Analysis Is Not Magic !

"When you know what the magician knows...

It's not magic anymore !"

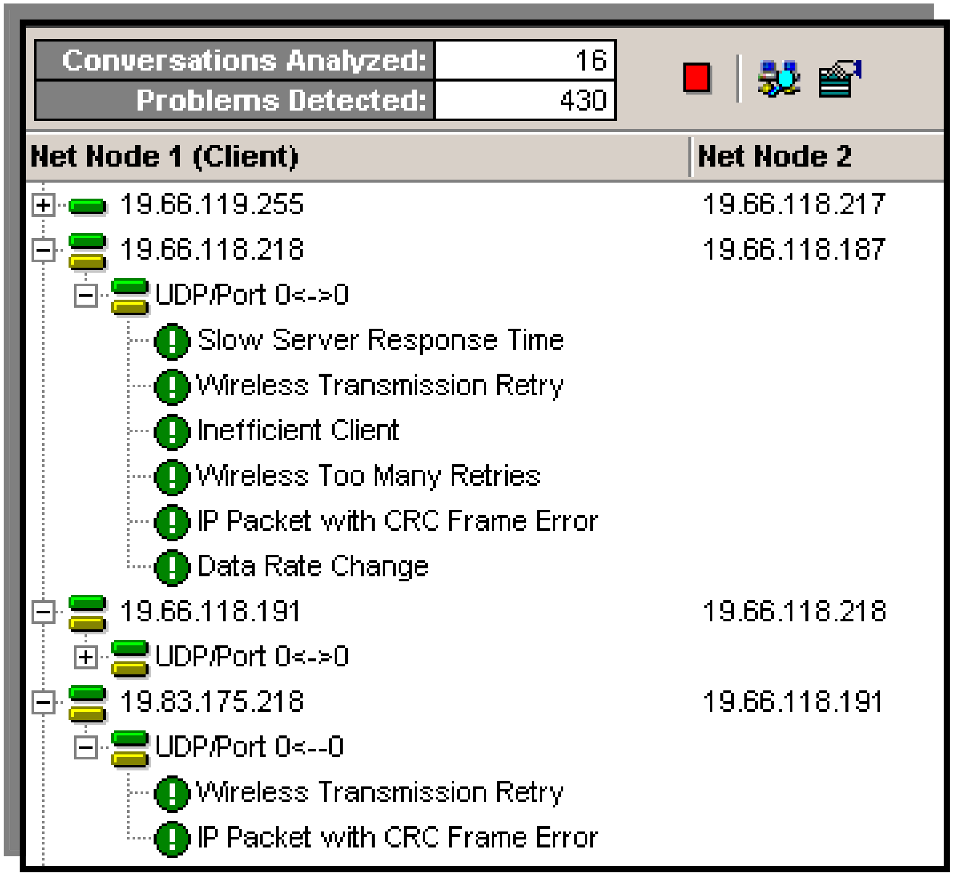
WildPackets

Disclosing The Behavior Of The Wireless Network



Total: 999

Description	Count
Channel Overlap	11,224
IP Packet with CRC Frame Error	423
TCP Reset Connection	165
Wireless Transmission Retry	22
HTTP Slow Response Time	13
IP Header Checksum Error	6
TCP Invalid Checksum	6
TCP Reset Inactive Connection	40
TCP Zero Window	41
IP Missing Fragment	59
Data Rate Change	80
TCP Slow First Retransmission	18
One-Way Traffic	11
TCP Repeated Connect Attempt	35
TCP Retransmission	10
TCP Too Many Retransmissions	55
TCP Stuck Window	4
Wireless Too Many Retries	11
Spanning Tree Topology Change	2

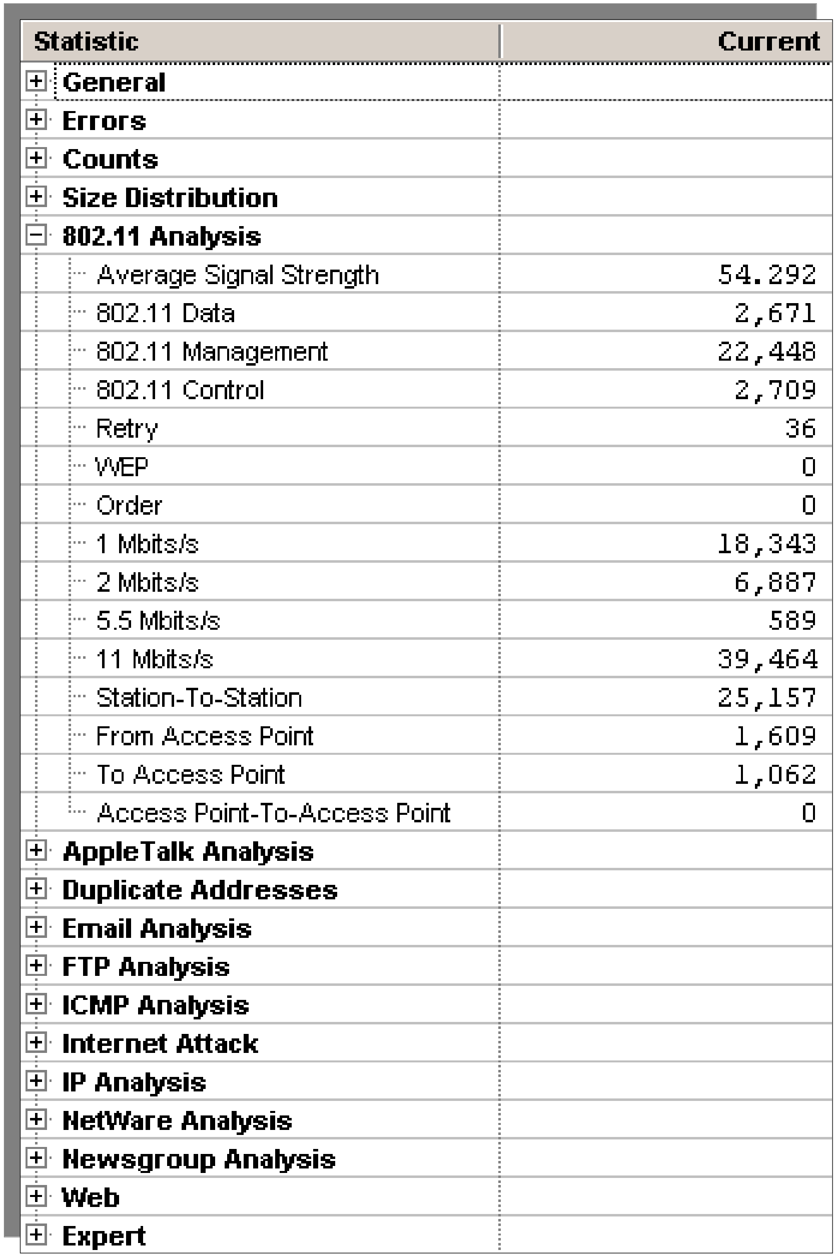


Conversations Analyzed: 16
Problems Detected: 430

Net Node 1 (Client)	Net Node 2
19.66.119.255	19.66.118.217
19.66.118.218	19.66.118.187
UDP/Port 0<->0	
Slow Server Response Time	
Wireless Transmission Retry	
Inefficient Client	
Wireless Too Many Retries	
IP Packet with CRC Frame Error	
Data Rate Change	
19.66.118.191	19.66.118.218
UDP/Port 0<->0	
19.83.175.218	19.66.118.191
UDP/Port 0<--0	
Wireless Transmission Retry	
IP Packet with CRC Frame Error	

Expert System Analysis Exposes Both Problem Issues And Potential Security Exposures

Start By Assessing The Physical Environment



Statistic	Current
General	
Errors	
Counts	
Size Distribution	
802.11 Analysis	
Average Signal Strength	54.292
802.11 Data	2,671
802.11 Management	22,448
802.11 Control	2,709
Retry	36
WEP	0
Order	0
1 Mbits/s	18,343
2 Mbits/s	6,887
5.5 Mbits/s	589
11 Mbits/s	39,464
Station-To-Station	25,157
From Access Point	1,609
To Access Point	1,062
Access Point-To-Access Point	0
AppleTalk Analysis	
Duplicate Addresses	
Email Analysis	
FTP Analysis	
ICMP Analysis	
Internet Attack	
IP Analysis	
NetWare Analysis	
Newsgroup Analysis	
Web	
Expert	

Responsibilities Of the 802.11 MAC Layer

- Addressing
  - Address the frame to allow proper delivery
- Handling BSS Membership
  - Become a member of a BSS through association
  - Leave a BSS through disassociation
- Authentication (Optional)
  - If authentication is enabled, the MAC Layer will have to authenticate itself before it will be allowed to associate with a BSS
- Fragmentation
  - Fragment upper-layer data units for transmission on the WLAN
  - Acknowledge fragments and retransmit lost fragments
- Arbitration
  - Determine when it is legal to transmit data

Frames Used To Get The Job Done

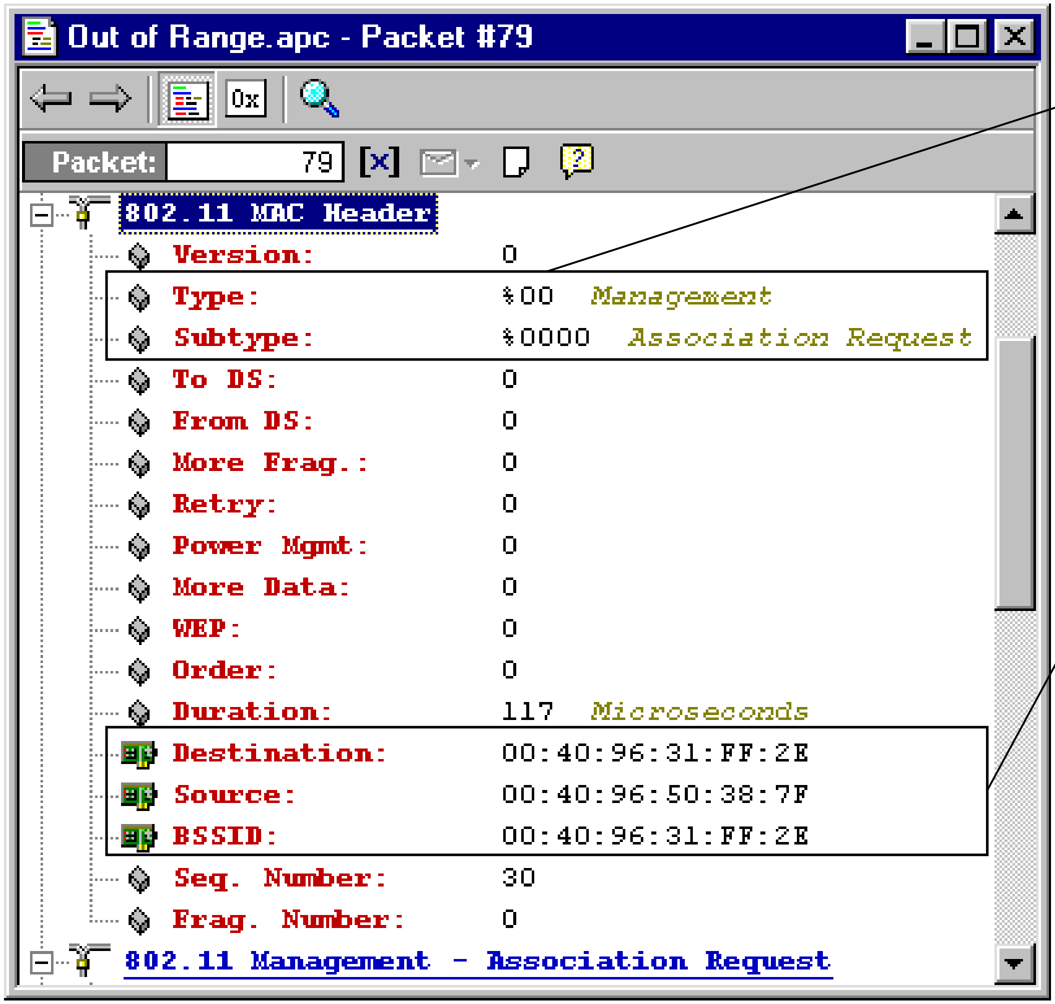
- The 802.11 MAC layer uses three types of frames to carry out its responsibilities
  - **Management frames** are used for managing membership to the BSS
    - Joining and leaving the BSS
    - Finding Access Points
  - **Control frames** are used for lower-layer MAC functions
    - Determining if it is okay to transmit data
    - Acknowledging frames
  - **Data frames** carry user data

Initialization Behavior Exposes Security Issues

Association

- To deliver a message within a distribution system, the DS needs to know which access point in the DS is capable of reaching the destination station
- The concept of **association** provides this information
  - A station discovers that an AP is within its coverage area
  - The station sends an **Association Request** frame to the AP
    - Contains the MAC address of the station
    - Contains the MAC address of the AP
    - Contains the ID of the ESS being joined
  - The AP determines whether the station may join the BSS and sends an **Association Response**
    - Contains the result of the requested association (successful or unsuccessful)
- Association is sufficient to ensure communication in all cases where stations remain within a single BSS

Analysis of Association Request (MAC)

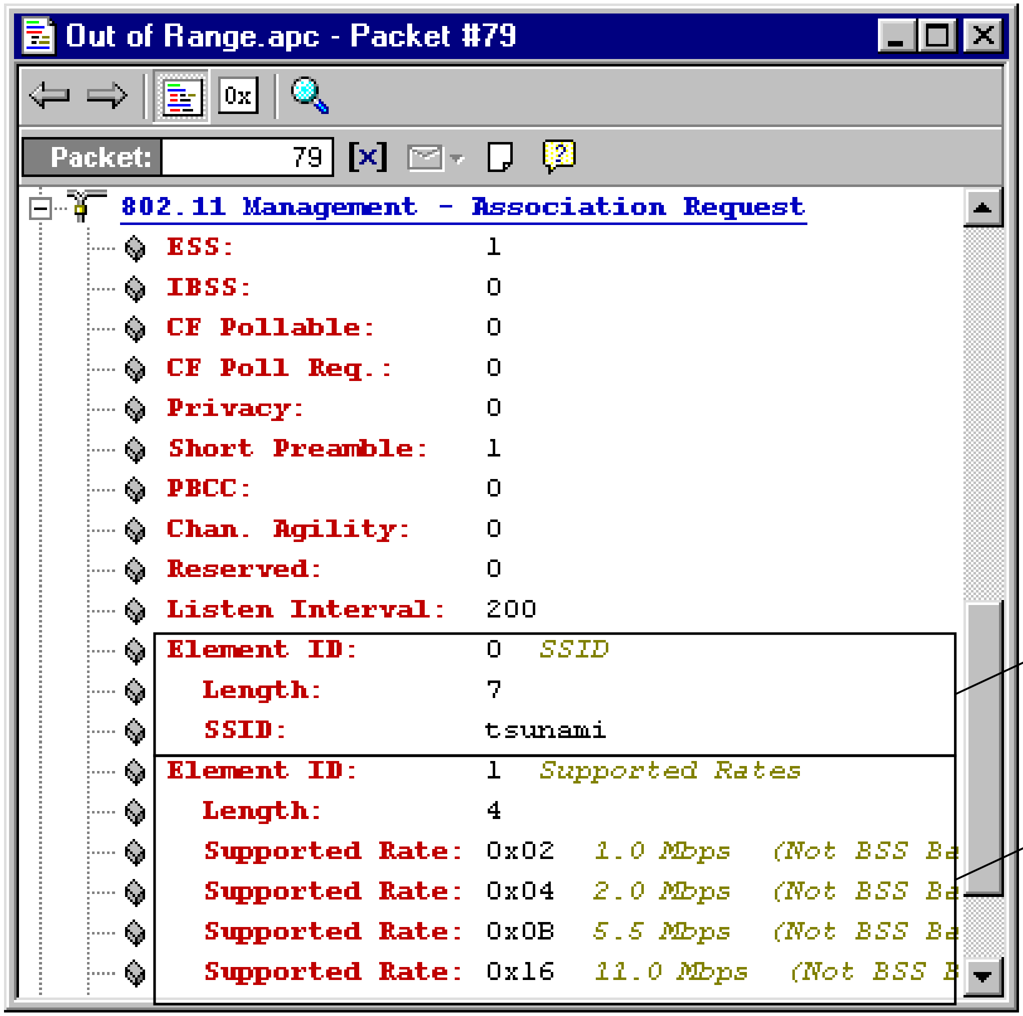


```
802.11 MAC Header
    Version:          0
    Type:             $00    Management
    Subtype:          $0000  Association Request
    To DS:            0
    From DS:          0
    More Frag.:       0
    Retry:            0
    Power Mgmt:       0
    More Data:        0
    WEP:              0
    Order:            0
    Duration:         117    Microseconds
    Destination:      00:40:96:31:FF:2E
    Source:           00:40:96:50:38:7F
    BSSID:            00:40:96:31:FF:2E
    Seq. Number:      30
    Frag. Number:     0
802.11 Management - Association Request
```

Frame type is Management; **subtype** Association Request

Destination address represents the AP with which the station is associating. **Source** address represents the station which initiated the association. **BSSID** represents the ID of the BSS being joined (should be the same as the Destination Address.

Analysis of Association Request (Body)



```
802.11 Management - Association Request
    ESS:                1
    IBSS:               0
    CF Pollable:        0
    CF Poll Req.:       0
    Privacy:            0
    Short Preamble:     1
    PBCC:               0
    Chan. Agility:      0
    Reserved:           0
    Listen Interval:    200
    Element ID:         0   SSID
       Length:          7
       SSID:            tsunami
    Element ID:         1   Supported Rates
       Length:          4
       Supported Rate:  0x02   1.0 Mbps   (Not BSS Ba
       Supported Rate:  0x04   2.0 Mbps   (Not BSS Ba
       Supported Rate:  0x0B   5.5 Mbps   (Not BSS Ba
       Supported Rate:  0x16   11.0 Mbps   (Not BSS B
```

SSID shows the ID of the ESS being joined

Supported Rates shows the data rates supported by the station initiating the association

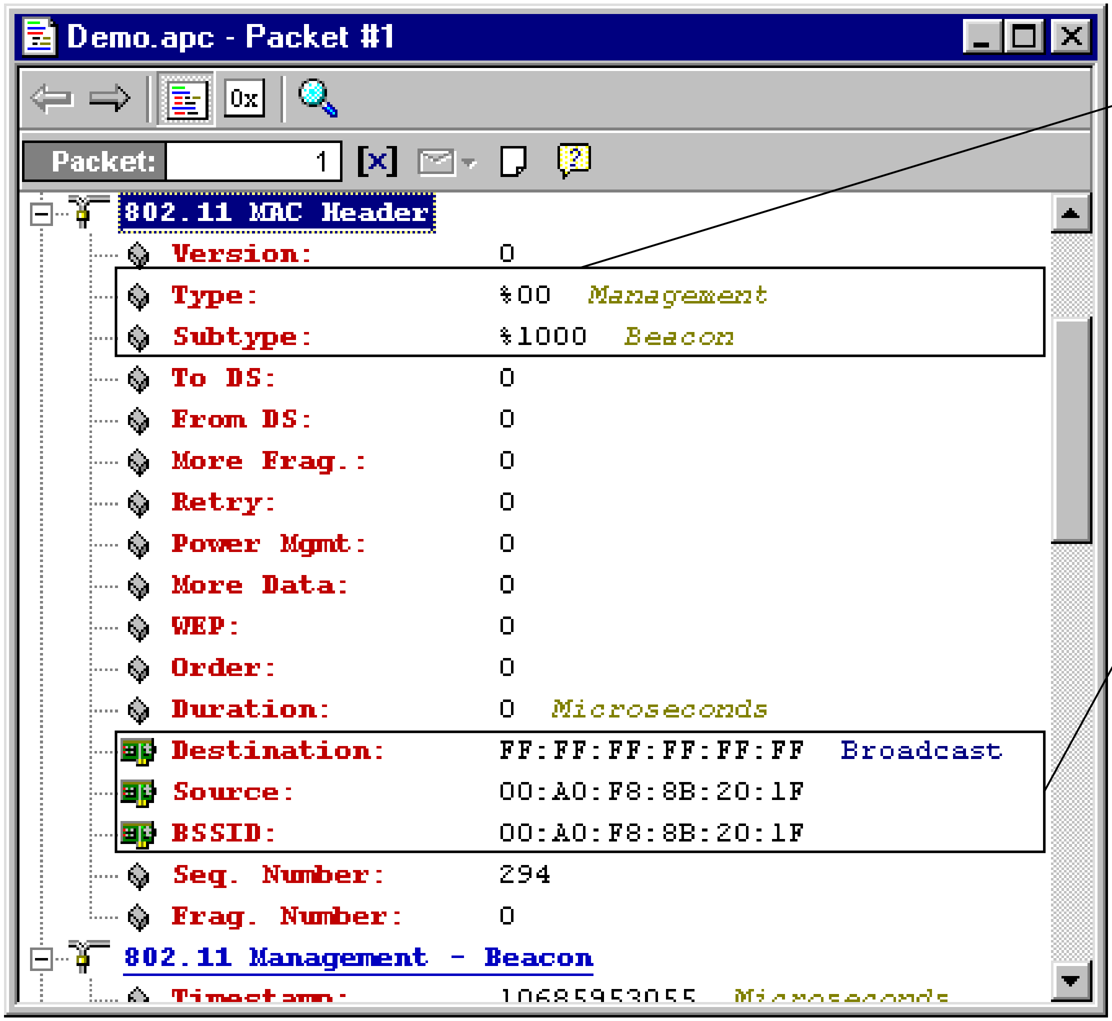
Association/Disassociation Analysis

- In general, association will succeed
- If association does not succeed, the Association Response frame will contain a code that explains the reason why
  - AiroPeek decodes these codes
  - The most common reasons for association to fail is that the device is not authenticated or that the device is prohibited from associating by a MAC access list
  - Another common reason for failure is incompatible data rates
    - Association frames are sent at 1 Mbps so all stations can hear them
    - The station may not support the proper data rates to actually send and receive data
    - Examine the Supported Data Rates element in the frame
- Disassociation frames will contain a code explaining the reason why the station is disassociating or being disassociated
  - Station idle too long; AP is overloaded; station going out of range…

Finding a BSS

- Before a station can join a BSS, it must learn that one exists
- Passive method: Listen for beacons
  - Access points periodically send **Beacon** frames
    - Contain the AP's SSID
    - Contain other information as well
  - If the station hears a beacon frame with an SSID matching its configured SSID, it may issue a Join Request to the AP sending the beacon
- Active method: Send a probe
  - Station sends **Probe Request** frames
    - Contain the SSID that has been configured in the station
  - Any AP that hears the Probe Request and that has the same SSID as the SSID in the Probe Request sends a **Probe Response** back
  - The station may set the SSID to all F's (known as the broadcast SSID) to indicate that all Access Points should respond

Analysis of Beacon Frame (MAC Header)

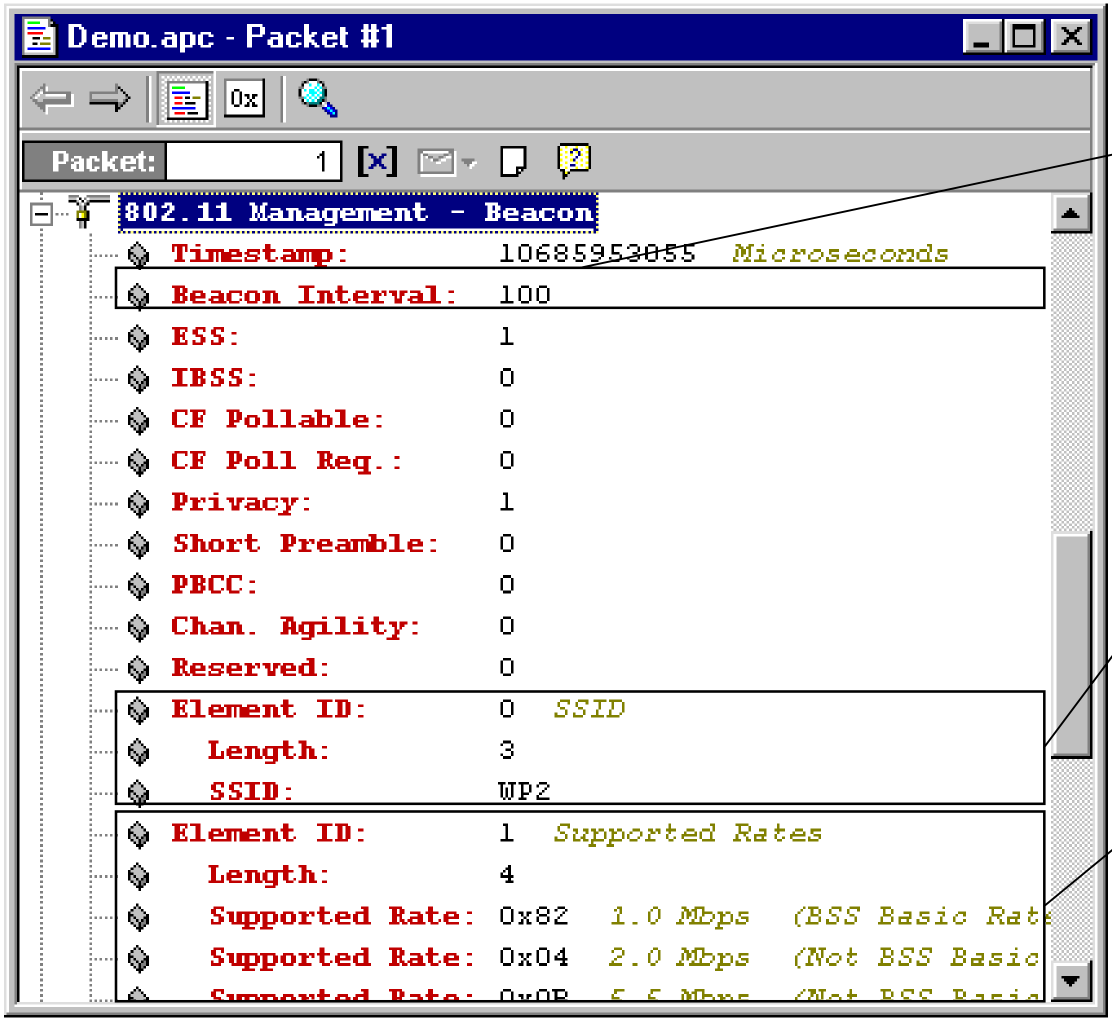


```
802.11 MAC Header
   Version:           0
   Type:              $00   Management
   Subtype:           $1000   Beacon
   To DS:             0
   From DS:           0
   More Frag.:        0
   Retry:             0
   Power Mgmt:        0
   More Data:         0
   WEP:               0
   Order:             0
   Duration:          0  Microseconds
   Destination:       FF:FF:FF:FF:FF:FF  Broadcast
   Source:            00:A0:F8:8B:20:1F
   BSSID:             00:A0:F8:8B:20:1F
   Seq. Number:       294
   Frag. Number:      0
802.11 Management - Beacon
   Timestamp:         10685953055  Microseconds
```

Frame type is Management; **subtype** is Beacon

Destination is always broadcast; **Source** is the Access Point sending the beacon; **BSSID** should match Source

Analysis of Beacon Frame (Body)



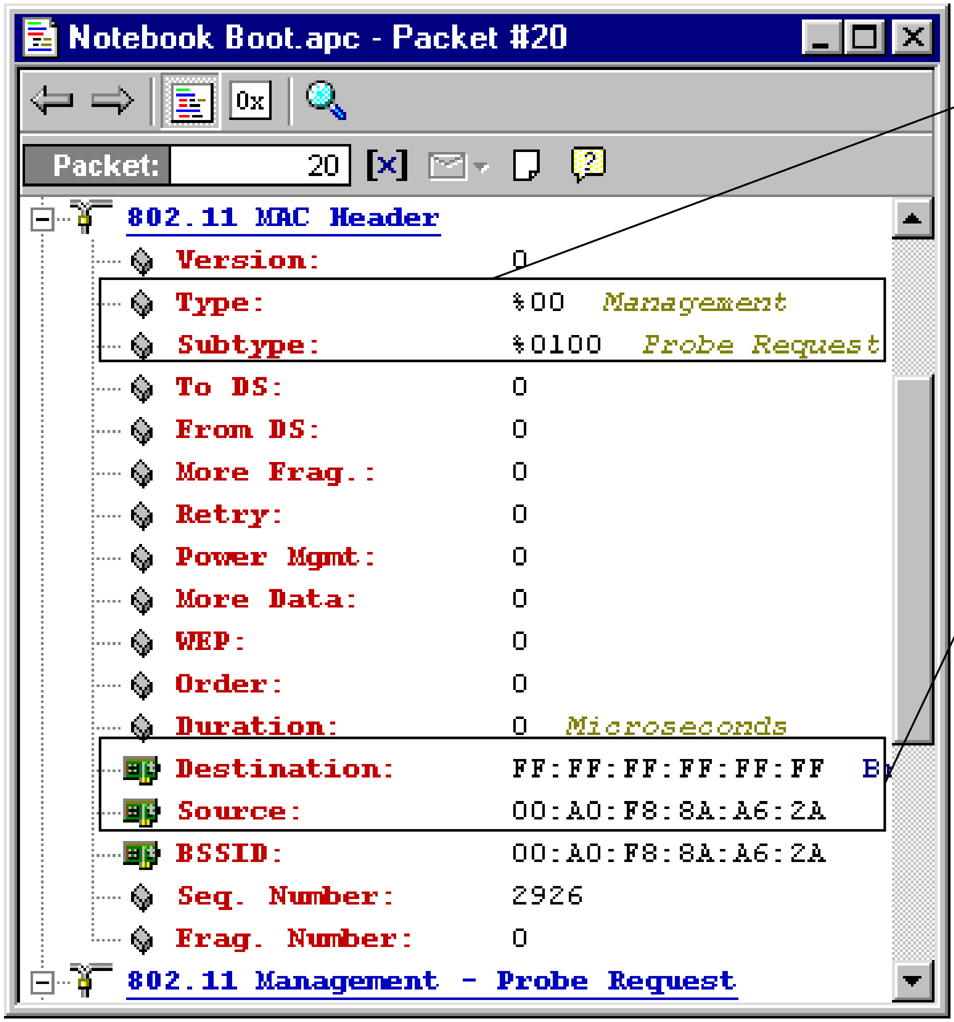
```
802.11 Management - Beacon
    Timestamp:          10685953055  Microseconds
    Beacon Interval:    100
    ESS:                1
    IBSS:               0
    CF Pollable:        0
    CF Poll Req.:       0
    Privacy:            1
    Short Preamble:     0
    PBCC:               0
    Chan. Agility:      0
    Reserved:           0
    Element ID:         0   SSID
      Length:           3
      SSID:             WP2
    Element ID:         1   Supported Rates
      Length:           4
      Supported Rate:   0x82   1.0 Mbps   (BSS Basic Rat
      Supported Rate:   0x04   2.0 Mbps   (Not BSS Basic
      Supported Rate:   0x0B   5.5 Mbps   (Not BSS Basic
```

Beacon interval shows how often beacon frames will be sent, in ms (the 100 ms interval seen here is common)

SSID element shows the **ESSID** to which the AP belongs

Supported Rates element shows data rates supported by the Access Point

Analysis of Probe Request (MAC Header)

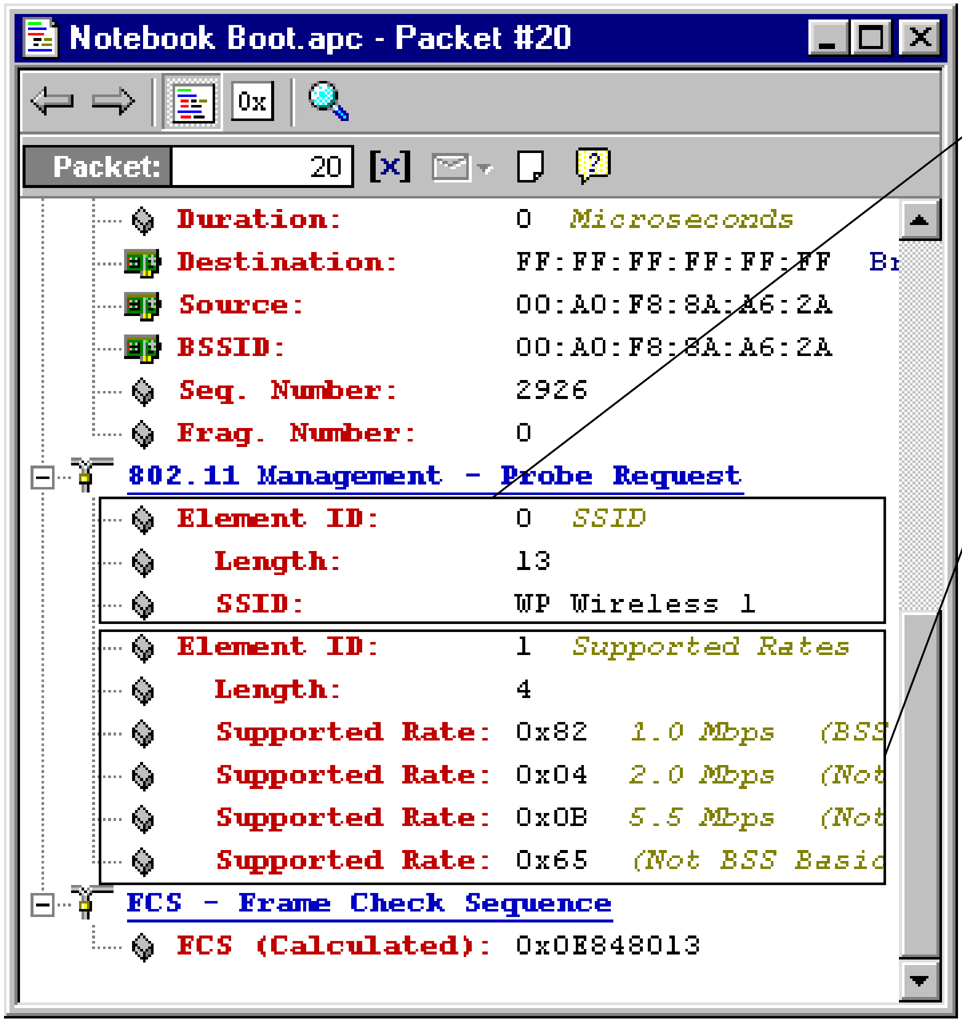


```
Packet: 20
802.11 MAC Header
    Version:          0
    Type:             $00     Management
    Subtype:          $0100   Probe Request
    To DS:            0
    From DS:          0
    More Frag.:       0
    Retry:            0
    Power Mgmt:       0
    More Data:        0
    WEP:              0
    Order:            0
    Duration:         0    Microseconds
    Destination:      FF:FF:FF:FF:FF:FF   B
    Source:           00:A0:F8:8A:A6:2A
    BSSID:            00:A0:F8:8A:A6:2A
    Seq. Number:      2926
    Frag. Number:     0
802.11 Management - Probe Request
```

Frame Type is Management; **Subtype** is Probe request.

Destination is the broadcast address. **Source** is the MAC address of the Probing station.

Analysis of Probe Request (Body)



```
Packet: 20

Duration:            0   Microseconds
Destination:         FF:FF:FF:FF:FF:FF   Br
Source:              00:A0:F8:8A:A6:2A
BSSID:               00:A0:F8:8A:A6:2A
Seq. Number:         2926
Frag. Number:        0
802.11 Management - Probe Request
Element ID:          0   SSID
   Length:           13
   SSID:             WP Wireless 1
Element ID:          1   Supported Rates
   Length:           4
   Supported Rate:   0x82   1.0 Mbps   (BSS
   Supported Rate:   0x04   2.0 Mbps   (Not
   Supported Rate:   0x0B   5.5 Mbps   (Not
   Supported Rate:   0x65   (Not BSS Basic
FCS - Frame Check Sequence
FCS (Calculated):    0x0E848013
```

SSID element contains the ID of the ESS that the station has been configured to join.

Supported Rates element contains the data rates supported by the Probing station. Notice that this station does not support the 11 Mbps rate.

WildPackets

Probe/Beacon Analysis

- If stations are receiving beacons or probe responses, the next logical step is to attempt to Associate with one of the Access Points sending the beacons or probe responses
  - SSID in the station must match SSID in the AP
    - Station may be configured with a “null” SSID, meaning that it will associate with any AP
    - Some Access Points will be configured to reject stations with the null SSID
  - Other vendor-specific factors may dictate whether the station will attempt to associate or not
- Stations often periodically send Probe requests even after they have associated
  - May be used to find new APs
  - May be used to confirm that the current AP is still the best
- Use Beacon/Probe Response frames to find “rogue” APs

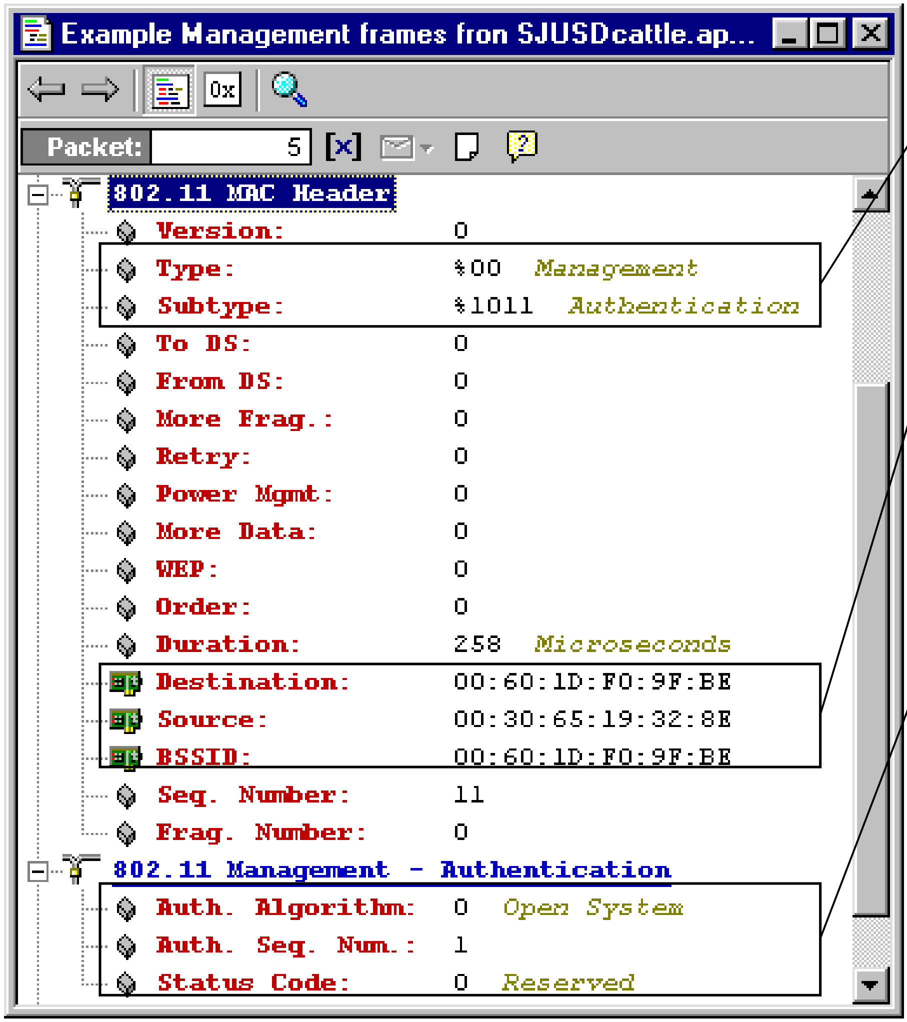
MAC Layer Security

- In wired LANs, physical security can be used to prevent unauthorized access to network resources
- This is not the case in wireless networks, since their signal is extremely difficult to contain
- The 802.11 MAC layer provides mechanisms to authenticate stations and prevent unauthenticated stations from gaining access to network resources and data
    - Specifics will be provided in a later section
- If an Access Point is configured to require authentication, it will not allow unauthenticated stations to associate with it
    - These stations normally cannot send and receive data
    - They can capture data (AiroPeek does not need to be associated)
- Stations can also authenticate directly with other stations (e.g. in an ad-hoc network)

Authentication

- The concept of **authentication** ensures that only authorized stations gain access to network resources and prevents unauthorized stations from viewing network data
  - A station realizes that authentication is required
  - It sends an **Authentication** frame to the station with which it is authenticating
    - This frame is always sent unencrypted
    - Identifies the authentication algorithm being used
    - Contains the identity of the station being authenticated
    - Contains information specific to the algorithm being used
  - A sequence of Authentication frames is exchanged
    - The specifics will vary depending on the specifics of the authentication algorithm in use
    - These frames may or may not be encrypted
    - The final frame contains the result of the authentication (successful or unsuccessful)

Analysis of Authentication Frame (1 of 2)



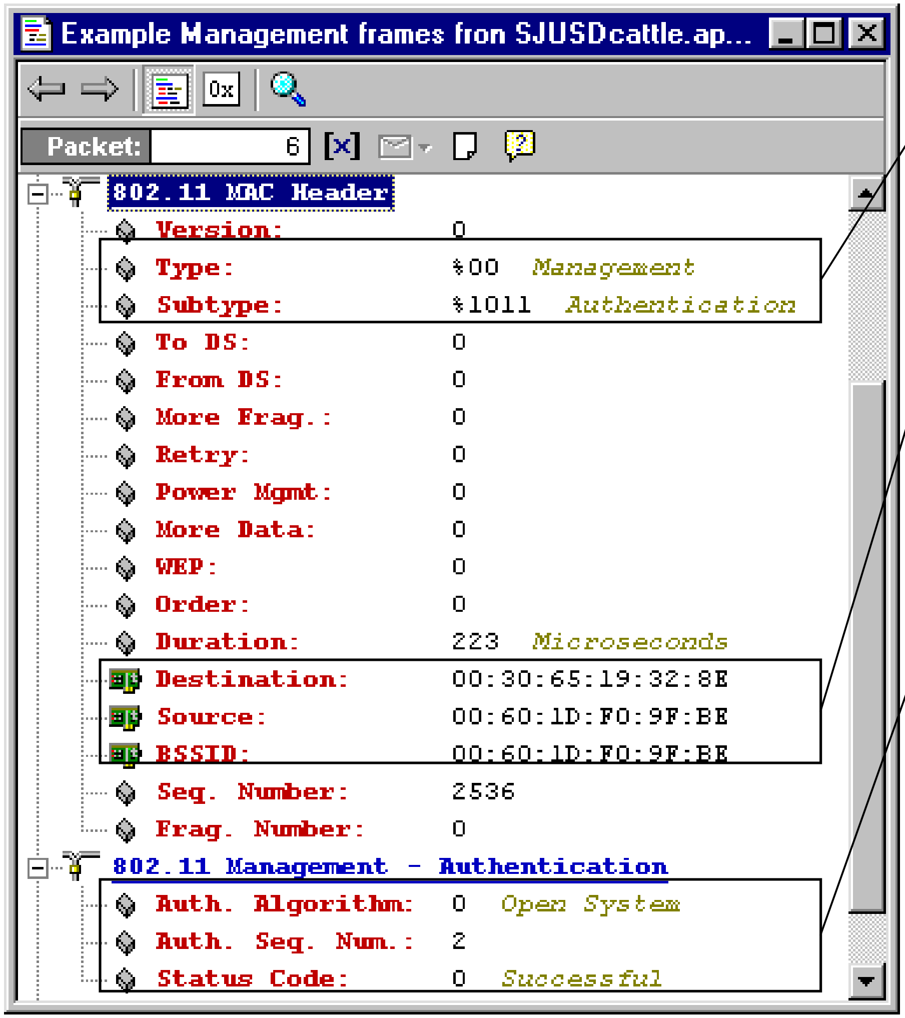
```
802.11 MAC Header
  Version:          0
  Type:             %00     Management
  Subtype:          %1011   Authentication
  To DS:            0
  From DS:          0
  More Frag.:       0
  Retry:            0
  Power Mgmt:       0
  More Data:        0
  WEP:              0
  Order:            0
  Duration:         258   Microseconds
  Destination:      00:60:1D:F0:9F:BE
  Source:           00:30:65:19:32:8E
  BSSID:            00:60:1D:F0:9F:BE
  Seq. Number:      11
  Frag. Number:     0
802.11 Management - Authentication
  Auth. Algorithm:  0  Open System
  Auth. Seq. Num.:  1
  Status Code:      0  Reserved
```

Frame Type is Management; **subtype** is Authentication

Source is the station being authenticated; **Destination** is the Access Point with which the station is authenticating; **BSSID** should match Destination.

Authentication Algorithm is Open System, indicating that no authentication is in use. **Authentication Sequence Number** is used to sequence frames of the authentication. **Status Code** will eventually indicate success or failure.

Analysis of Authentication Frame (2 of 2)



```
802.11 MAC Header
  Version:              0
  Type:                 %00    Management
  Subtype:              %1011  Authentication
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             223  Microseconds
  Destination:          00:30:65:19:32:8E
  Source:               00:60:1D:F0:9F:BE
  BSSID:                00:60:1D:F0:9F:BE
  Seq. Number:          2536
  Frag. Number:         0
802.11 Management - Authentication
  Auth. Algorithm:      0  Open System
  Auth. Seq. Num.:      2
  Status Code:          0  Successful
```

Frame Type is Management; **subtype** is Authentication

Destination is the station being authenticated; **Source** is the Access Point with which the station is authenticating; **BSSID** should match Source

Authorization Algorithm is Open System. **Authorization Sequence Number** has increased by one. **Status Code** indicates success (which should always be the case in an Open System).

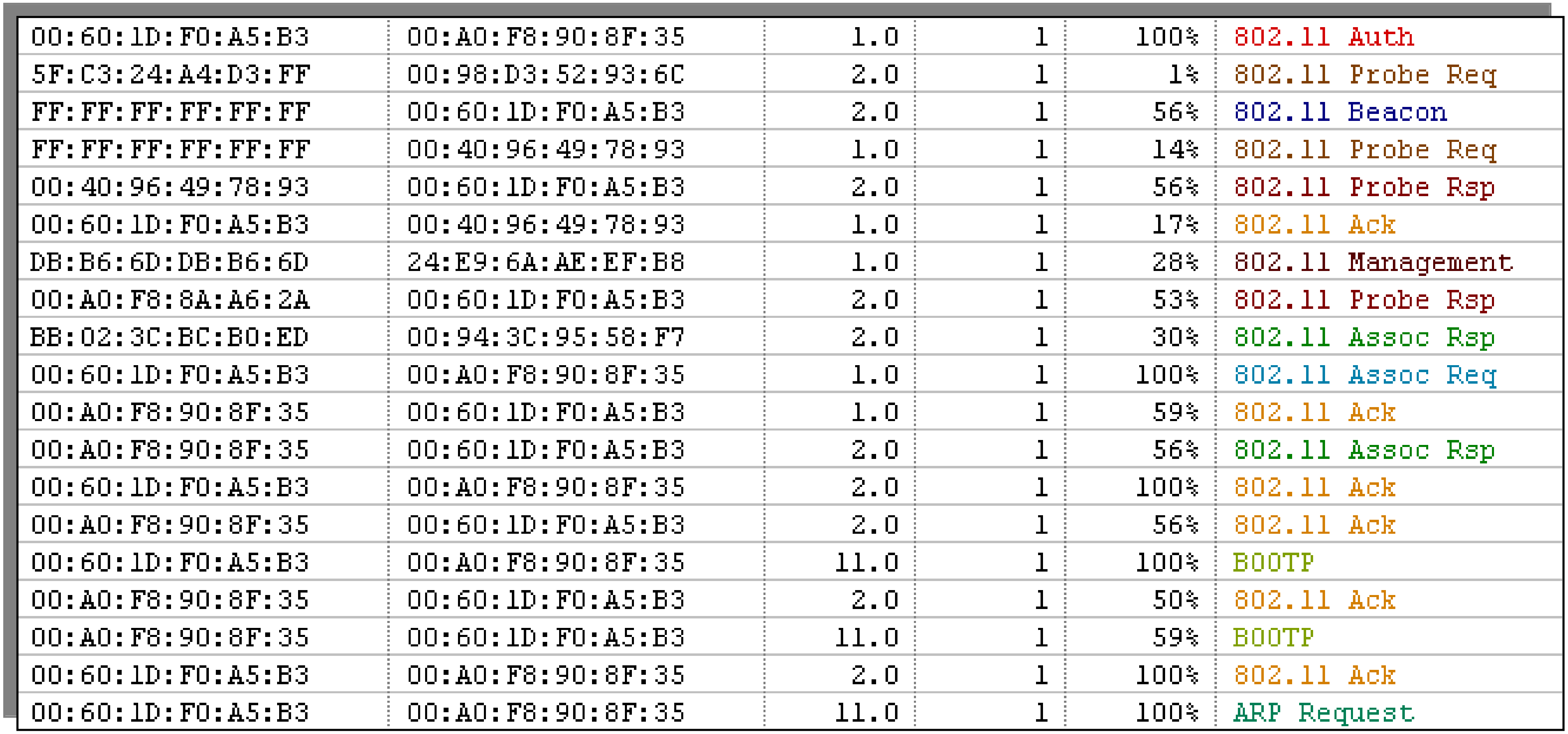
Authentication Analysis

- If you have an Open System, authentication should never fail
  - In Open systems, the authentication process typically involves two frames
    - Open System Authentication to AP
    - Successful response from AP
- If you are using WEP authentication, then confirm that Open Systems are being rejected
  - WEP authentication typically involves four frames
    - Shared Key Authentication to AP
    - Challenge from AP
    - Challenge response to AP
    - Successful response from AP
- If WEP authentication fails, check the WEP key(s) in the station
  - The last frame will contain an response code, which can be interpreted to see the reason why the station was rejected

Expected Frames at Startup

- When a wireless station starts up or first joins a BSS, these frames will usually be seen in this order
  - Probes / Probe Responses
    - Optional, since a station may just listen for Beacons
    - Station will listen for Probe Responses and choose an AP
  - Authentication
    - The station authenticates with the AP
    - This will occur even in Open Systems, which don’t use authentication
  - Association / Association Response
    - The station associates with the AP
  - Data
  - Disassociation
    - This frame may not be seen, depending on how the station leaves
  - Deauthentication
    - This frame may not be seen, depending on how the station leaves

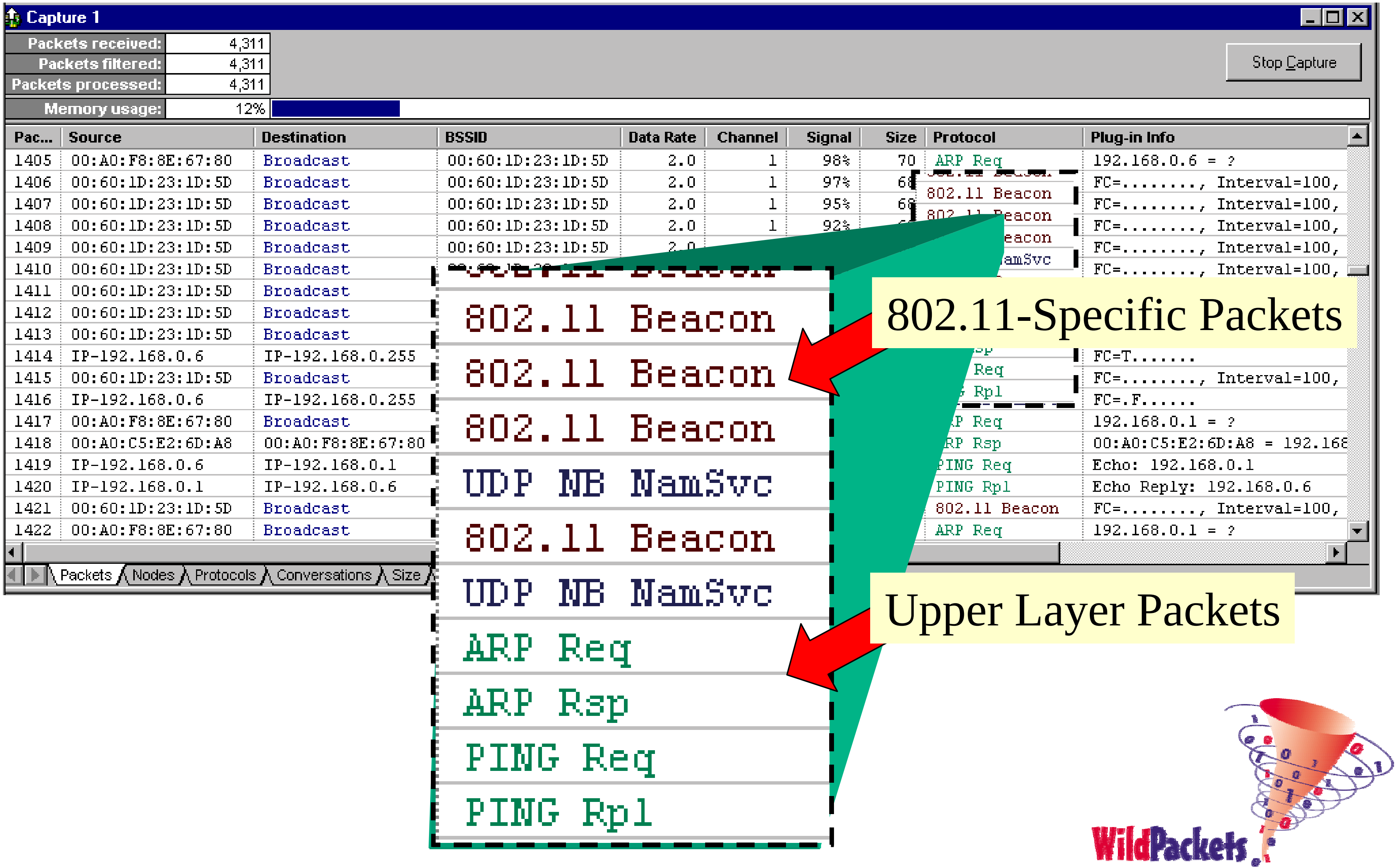
Station Startup Packet Analysis



00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	1.0	1	100%	802.11 Auth
5F:C3:24:A4:D3:FF	00:98:D3:52:93:6C	2.0	1	1%	802.11 Probe Req
FF:FF:FF:FF:FF:FF	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Beacon
FF:FF:FF:FF:FF:FF	00:40:96:49:78:93	1.0	1	14%	802.11 Probe Req
00:40:96:49:78:93	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Probe Rsp
00:60:1D:F0:A5:B3	00:40:96:49:78:93	1.0	1	17%	802.11 Ack
DB:B6:6D:DB:B6:6D	24:E9:6A:AE:EF:B8	1.0	1	28%	802.11 Management
00:A0:F8:8A:A6:2A	00:60:1D:F0:A5:B3	2.0	1	53%	802.11 Probe Rsp
BB:02:3C:BC:B0:ED	00:94:3C:95:58:F7	2.0	1	30%	802.11 Assoc Rsp
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	1.0	1	100%	802.11 Assoc Req
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	1.0	1	59%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Assoc Rsp
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	2.0	1	100%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Ack
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	11.0	1	100%	BOOTP
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	50%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	11.0	1	59%	BOOTP
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	2.0	1	100%	802.11 Ack
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	11.0	1	100%	ARP Request

WildPackets

Viewing The WLAN Conversations



Packets received: 4,311
Packets filtered: 4,311
Packets processed: 4,311
Memory usage: 12%

Pac...	Source	Destination	BSSID	Data Rate	Channel	Signal	Size	Protocol	Plug-in Info
1405	00:A0:F8:8E:67:80	Broadcast	00:60:1D:23:1D:5D	2.0	1	98%	70	ARP Req	192.168.0.6 = ?
1406	00:60:1D:23:1D:5D	Broadcast	00:60:1D:23:1D:5D	2.0	1	97%	68		FC=........, Interval=100,
1407	00:60:1D:23:1D:5D	Broadcast	00:60:1D:23:1D:5D	2.0	1	95%	68	802.11 Beacon	FC=........, Interval=100,
1408	00:60:1D:23:1D:5D	Broadcast	00:60:1D:23:1D:5D	2.0	1	92%		802.11 Beacon	FC=........, Interval=100,
1409	00:60:1D:23:1D:5D	Broadcast	00:60:1D:23:1D:5D	2.0				eacon	FC=........, Interval=100,
1410	00:60:1D:23:1D:5D	Broadcast						amSvc	FC=........, Interval=100,
1411	00:60:1D:23:1D:5D	Broadcast							
1412	00:60:1D:23:1D:5D	Broadcast							
1413	00:60:1D:23:1D:5D	Broadcast							
1414	IP-192.168.0.6	IP-192.168.0.255						sp	FC=T.......
1415	00:60:1D:23:1D:5D	Broadcast						Req	FC=........, Interval=100,
1416	IP-192.168.0.6	IP-192.168.0.255						Rpl	FC=.F......
1417	00:A0:F8:8E:67:80	Broadcast						P Req	192.168.0.1 = ?
1418	00:A0:C5:E2:6D:A8	00:A0:F8:8E:67:80						RP Rsp	00:A0:C5:E2:6D:A8 = 192.168
1419	IP-192.168.0.6	IP-192.168.0.1						PING Req	Echo: 192.168.0.1
1420	IP-192.168.0.1	IP-192.168.0.6						PING Rpl	Echo Reply: 192.168.0.6
1421	00:60:1D:23:1D:5D	Broadcast						802.11 Beacon	FC=........, Interval=100,
1422	00:A0:F8:8E:67:80	Broadcast						ARP Req	192.168.0.1 = ?

802.11 Beacon
802.11 Beacon
802.11 Beacon
UDP NB NamSvc
802.11 Beacon
UDP NB NamSvc
ARP Req
ARP Rsp
PING Req
PING Rpl

802.11-Specific Packets

Upper Layer Packets

WildPackets

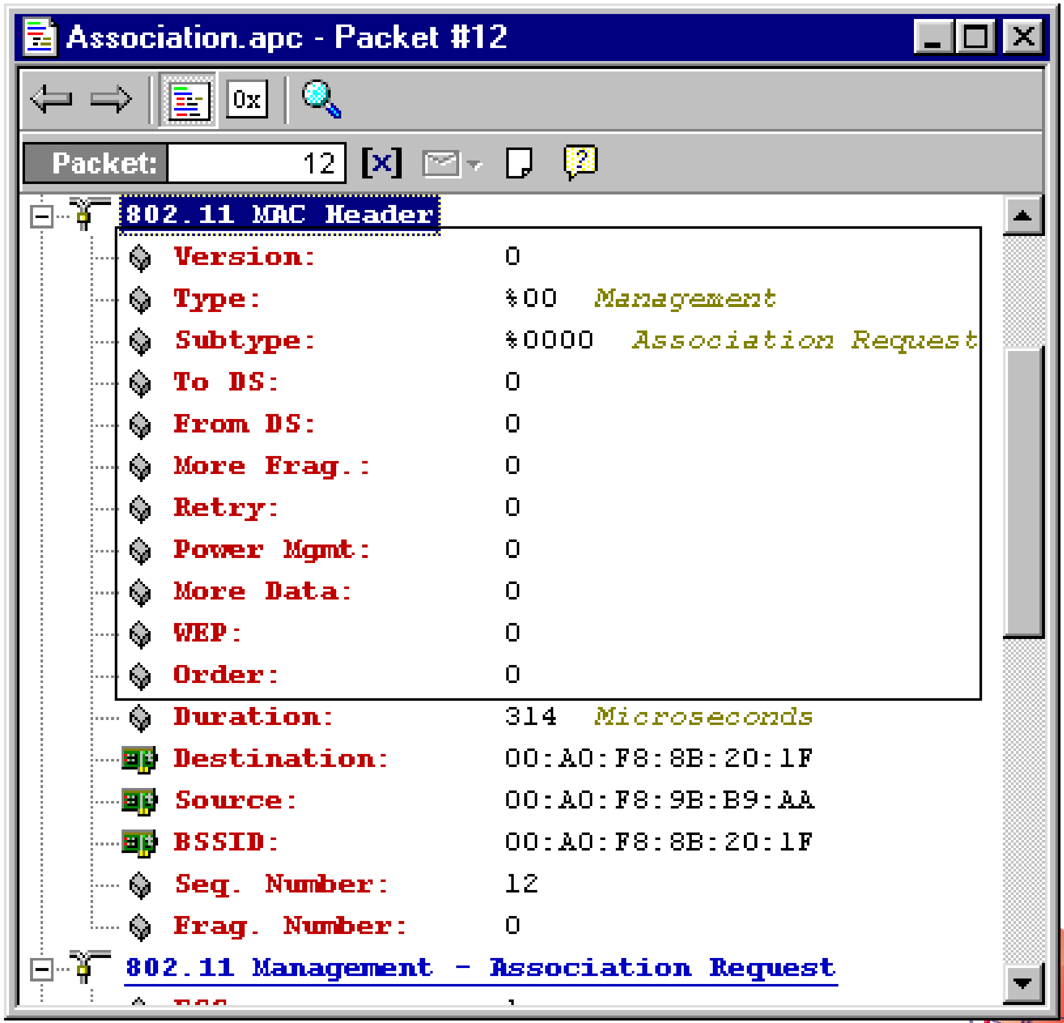
Analysis of Other MAC Fields

These fields are collectively known as the **Frame Control** (FC) field.

The **To DS** bit is set to 1 in frames that are going into the DS. The **From DS** bit is set to 1 in frames that are coming out of the DS.

The **Retry** bit is set to 1 in any frame that is being retransmitted.

The **WEP** bit is set to 1 in any frame that uses WEP encryption. Note that this does not indicate whether WEP is actually required by the AP, only whether this frame was encrypted with WEP.



```
802.11 MAC Header
    Version:          0
    Type:             %00   Management
    Subtype:          %0000   Association Request
    To DS:            0
    From DS:          0
    More Frag.:       0
    Retry:            0
    Power Mgmt:       0
    More Data:        0
    WEP:              0
    Order:            0
    Duration:         314   Microseconds
    Destination:      00:A0:F8:8B:20:1F
    Source:           00:A0:F8:9B:B9:AA
    BSSID:            00:A0:F8:8B:20:1F
    Seq. Number:      12
    Frag. Number:     0
802.11 Management - Association Request
```

Your 802.11 Network Has No Clothes

Who was the first WLAN Security Analyst?

WLAN Security
And Intrusion Detection Issues

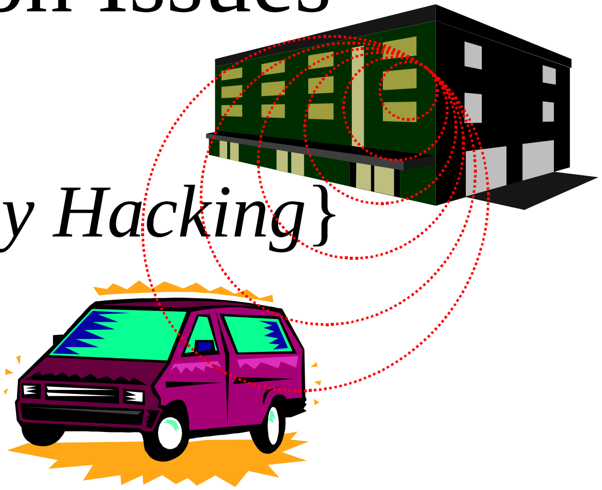
- Unauthorized access to network resources
  - Internet connections are a common target
  - Hacking
- Hostile disruption of network service
  - Denial of service
  - Virus deployment
- Exposure of confidential information
  - No physical security
  - Data is accessible without physical network attachment

WLAN Security
And Intrusion Detection Issues

- The “Invisible Client” attack

  - Install access points outside your firewall
  - Carefully implement DHCP for wireless clients
  - Confirm proper server and resource permissions
  - Use AiroPeek to determine who’s on your network
  - Implement access lists at your access points

WLAN Security
And Intrusion Detection Issues



- The “Invisible Client” attack
- The “Parking Lot” attack {*Drive-By Hacking*}
    - Survey accessibility from outside the building using AiroPeek
    - Don’t forget that RF propagates in all directions
    - Make your security personnel aware of the potential for wireless intrusion

WLAN Security
And Intrusion Detection Issues

- The “Invisible Client” attack
- The “Parking Lot” attack
- The “Rogue Resource” attack

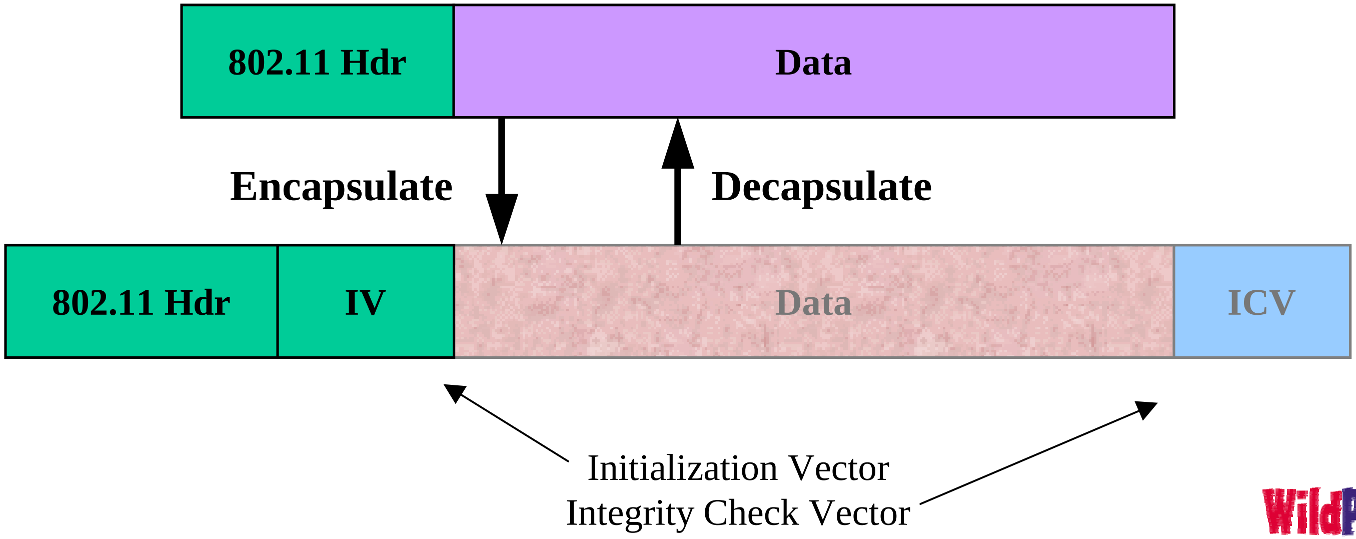
  - A rogue DHCP server can wreak havoc on your network
  - A rogue Ethernet address can spoof the target address for a valid resource
  - Use AiroPeek to confirm proper data exchange between communicating devices

WLAN Security
And Intrusion Detection Issues

- The “Invisible Client” attack
- The “Parking Lot” attack
- The “Rogue Resource” attack
- Defeating WEP encryption
  - Wireless Equivalent Privacy (WEP) encrypts the 802.11 packets
  - It’s fairly straightforward to break WEP encryption and determine your secret keys

Wired Equivalent Privacy (WEP)

- A link-layer security protocol defined by 802.11
  - Simulate physical access control by denying access at the Data Link layer
- An encryption key is shared between communicators
  - “Shared Key” as opposed to “Open System”
- The shared key is distributed “out of band”
  - You type it in to both communicators



802.11 Hdr | **Data**

Encapsulate

Decapsulate

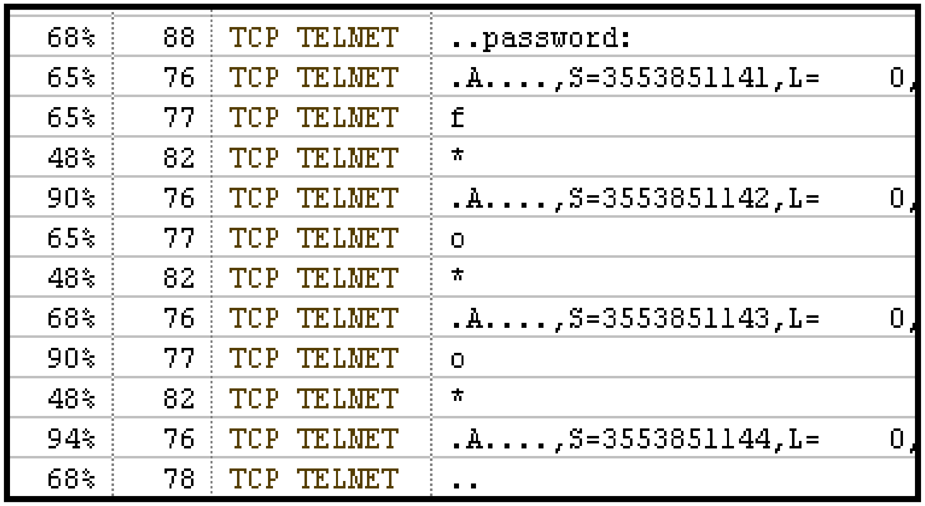
802.11 Hdr | **IV** | **Data** | **ICV**

Initialization Vector

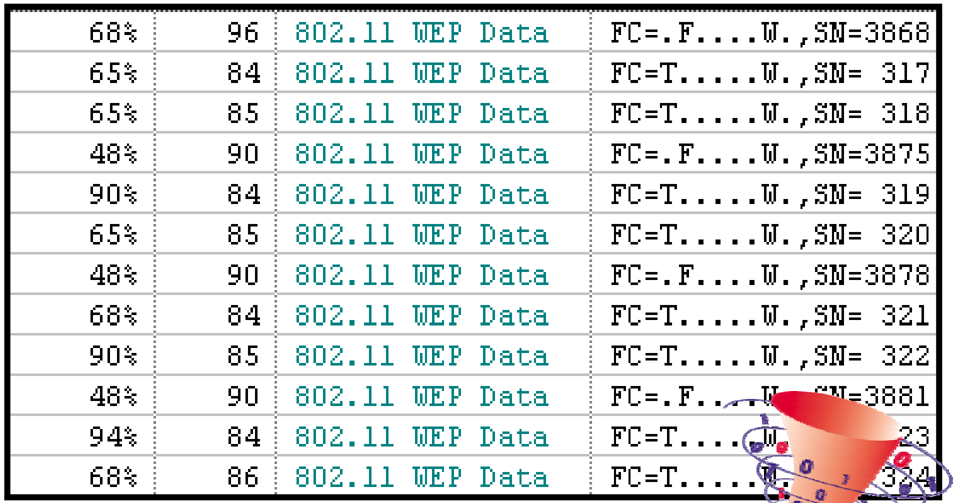
Integrity Check Vector

Facts And Myths About WEP

- Without the proper WEP keys there is no current protocol analysis tool on the market that can decrypt the traffic
  - This may change as more motivated hackers place freeware on the Internet
- A casual intruder will be appropriately thwarted by WEP
  - A serious intrusion attempt will bypass WEP



```
68%   88  TCP TELNET  ..password:
65%   76  TCP TELNET  .A....,S=3553851141,L=     0,
65%   77  TCP TELNET  f
48%   82  TCP TELNET  *
90%   76  TCP TELNET  .A....,S=3553851142,L=     0,
65%   77  TCP TELNET  o
48%   82  TCP TELNET  *
68%   76  TCP TELNET  .A....,S=3553851143,L=     0,
90%   77  TCP TELNET  o
48%   82  TCP TELNET  *
94%   76  TCP TELNET  .A....,S=3553851144,L=     0,
68%   78  TCP TELNET  ..
```



```
68%   96  802.11 WEP Data   FC=.F....W.,SN=3868
65%   84  802.11 WEP Data   FC=T.....W.,SN= 317
65%   85  802.11 WEP Data   FC=T.....W.,SN= 318
48%   90  802.11 WEP Data   FC=.F....W.,SN=3875
90%   84  802.11 WEP Data   FC=T.....W.,SN= 319
65%   85  802.11 WEP Data   FC=T.....W.,SN= 320
48%   90  802.11 WEP Data   FC=.F....W.,SN=3878
68%   84  802.11 WEP Data   FC=T.....W.,SN= 321
90%   85  802.11 WEP Data   FC=T.....W.,SN= 322
48%   90  802.11 WEP Data   FC=.F..  W   N=3881
94%   84  802.11 WEP Data   FC=T....W        23
68%   86  802.11 WEP Data   FC=T....W.      324
```

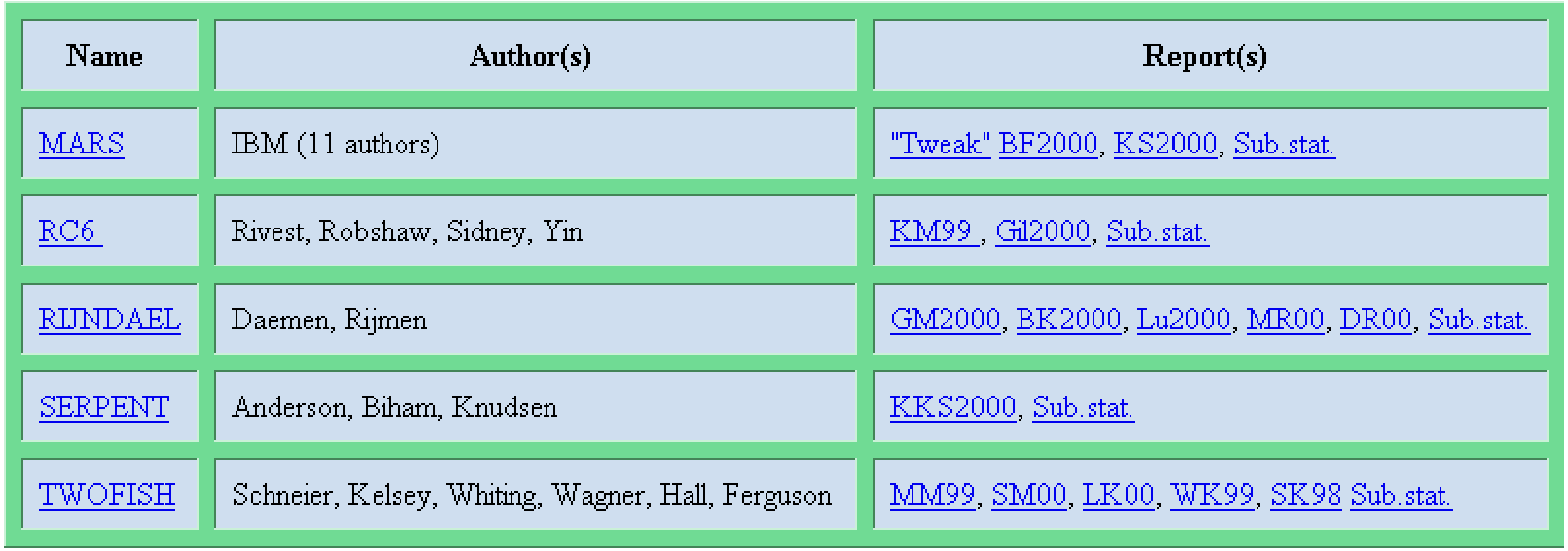
The Discovery Of The WEP Flaws

- January 2001
  - UC Berkely releases paper with their findings
- August 2001
  - Scott Fluhrer, Itsik Mantin, and Adi Shamir find a flaw in the RC4 key setup algorithm which results in a total recovery of the secret key. Implementing the attack requires the collection of traffic passively.
- Today
  - You can download instructions and helpful utilities from the Internet that will allow WEP keys to be recovered
  - Most utilities are Linux-based
  - Extracting a WEP key is non-trivial but well within the technical capabilities of a bright high-school student

Alternatives To WEP Encryption

- Implementation of Virtual Private Networks or other tunneling protocol approaches
- Offset Codebook (OCB) encryption using Advanced Encryption Standard (AES) 128- 192- and 256-bit keys
  - Proposals are being reviewed by the National Institute of Standards and Technology (NIST)
- Kerberos authentication
  - RFC 1510
- Extensible Authentication Protocol (EAP) in 802.1X
  - RFC 2284
  - Used in Transport Layer Security (TLS) in Windows 2000
  - Integrates with Kerberos
  - Cisco has introduced “Lightweight EAP” (LEAP)

Five Final Proposals Are Under Review



Name	Author(s)	Report(s)
MARS	IBM (11 authors)	"Tweak" BF2000, KS2000, Sub.stat.
RC6	Rivest, Robshaw, Sidney, Yin	KM99 , Gil2000, Sub.stat.
RIJNDAEL	Daemen, Rijmen	GM2000, BK2000, Lu2000, MR00, DR00, Sub.stat.
SERPENT	Anderson, Biham, Knudsen	KKS2000, Sub.stat.
TWOFISH	Schneier, Kelsey, Whiting, Wagner, Hall, Ferguson	MM99, SM00, LK00, WK99, SK98 Sub.stat.

- Selected from a field of 15 final submissions
- See http://www.ii.uib.no/~larsr/aes.html

What You Need To Do

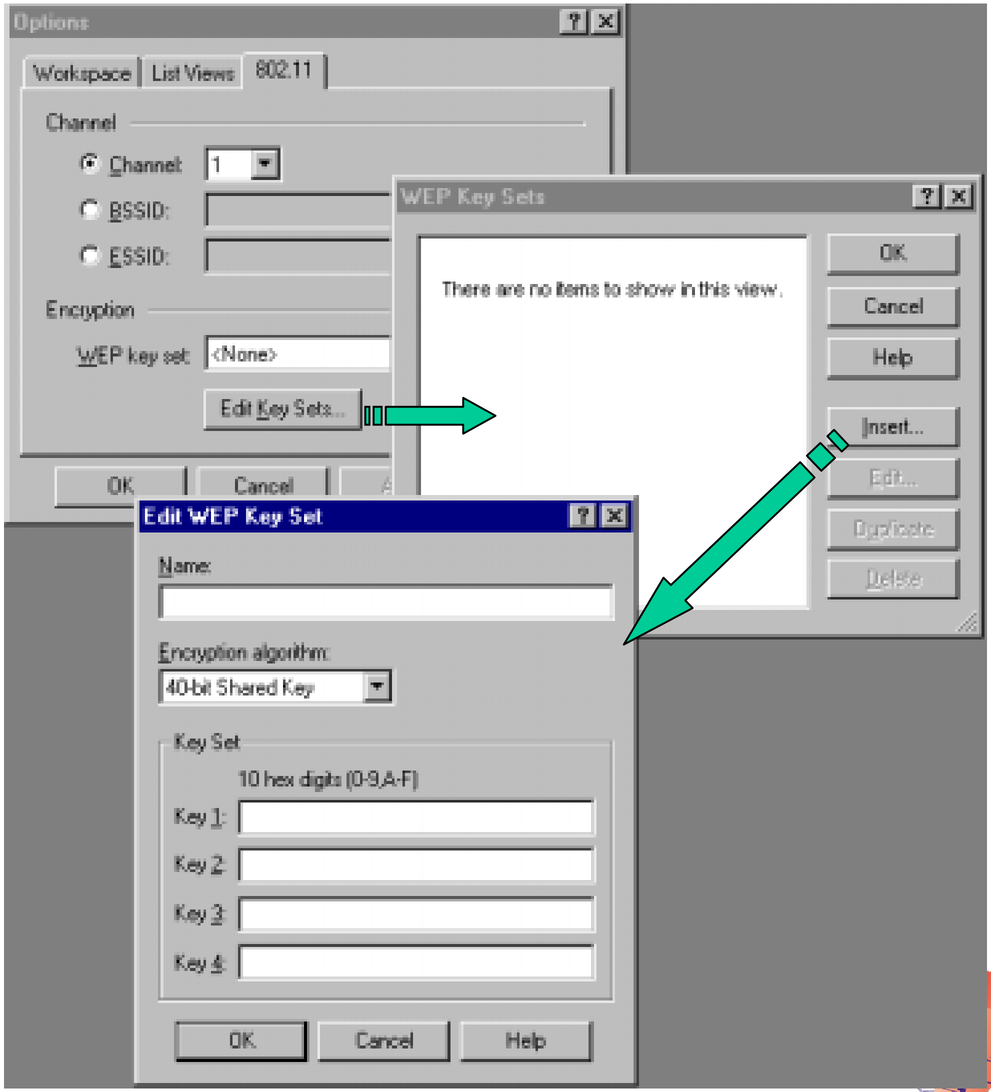
- ✍🙚🙛⑤⓿⓪🙝❺ 🙘⑥⑤🙝⓪🙚🙛⑤⓿⓪🙙③ ⓪⑤🙝⑥⑨④🙙⓿⓪⑥⑤
- ⊗⑩🙛 🙙⑦⑦③⓪🙘🙙⓿⓪⑥⑤🗏③🙛❷🙛③ 🙛⑤🙘⑨❺⑦⓿⓪⑥⑤ ❸🙞🙛⑤ 🙙⑦⑦⑨⑥⑦⑨⓪🙙⓿🙛
  - ☒🙞⓪⑩ 🙙⑦⑦③⓪🙛⑩ ⓿⑥ ⓿🙞🙛 ❸⓪⑨🙛🙚 ✍⑤⓿🙛⑨⑤🙛⓿ ⓿⑥⑥✎
- ✍④⑦③🙛④🙛⑤⓿ ⑩🙛🙘❶⑨🙛 ❶⑦⑦🙛⑨🗏③🙙❺🙛⑨ ⑦⑨⑥⓿⑥🙘⑥③⑩
  - ☒☒✌🗎 ✌☒☒✓☒🗎 ✍✓☒☛☞
- ✍④⑦③🙛④🙛⑤⓿ 🙙 🙚🙙⓿🙙🗏③⓪⑤② 🙛⑤🙘⑨❺⑦⓿⓪⑥⑤ ④🙛⓿🙞⑥🙚
  - ⦸☛✓🗎 ☝☛☛✓🗎 ☑☛☛✍⦸
- ☒☛☒☒ 🙰×⊗☑ ✍✌✓☝☛✌☛✋☒☛☒✍×✋
  - ⊗⑩🙛 ☛⓪⑨⑥✓🙛🙛② ⓿⑥ 🙘⑥⑤🙝⓪⑨④ ⓿🙞🙙⓿ ❸🙞🙙⓿ ⑩🙞⑥❶③🙚 ⑤⑥⓿ 🙟🙛 ❷⓪⑩⓪🙟③🙛 ⓪⑩🗎 ⓪⑤ 🙝🙙🙘⓿🗎 ⑤⑥⓿ ❷⓪⑩⓪🙟③🙛✎

What You Need To Do

- Identify confidential information
- Implement access control lists where possible
  - Connect access points outside your firewall
- Use application-level encryption when appropriate
  - This applies to the wired Internet too!
- Implement secure upper-layer protocols
  - SSH, HTTPS, IPSEC
- Implement a data-link encryption method
  - WEP, LEAP
- TEST YOUR IMPLEMENTATION
  - Use AiroPeek to confirm that what should not be visible is, in fact, not visible!

WEP And The Protocol Analysis Process

- WEP keys are entered in the appropriate configuration dialog boxes
- Trace files can be "unweped" after capture using a supplied utility



● Channel: 1

WEP key set: <None>

There are no items to show in this view.

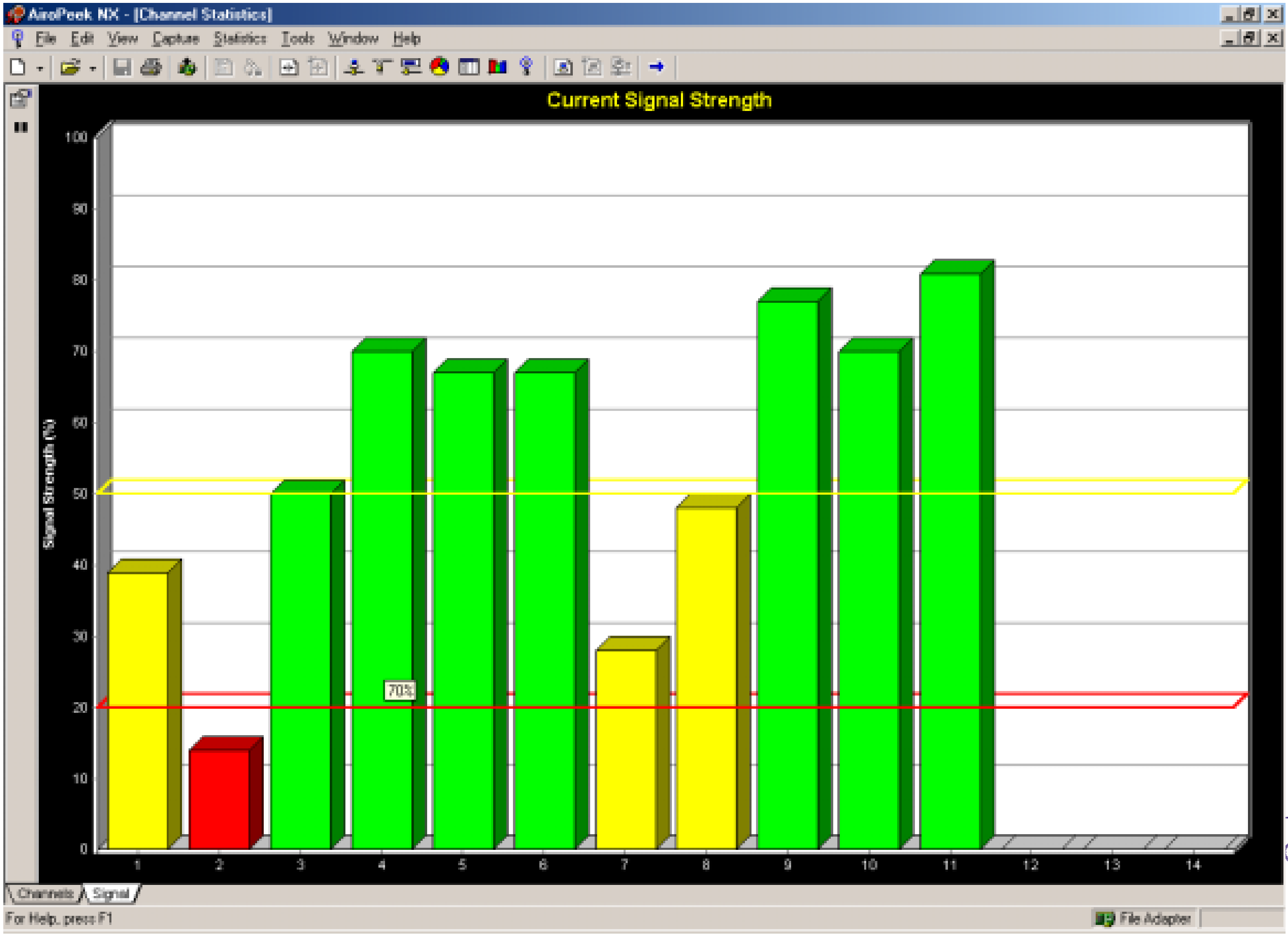
Encryption algorithm: 40-bit Shared Key

10 hex digits (0-9,A-F)

Use AiroPeekNX to Evaluate Security

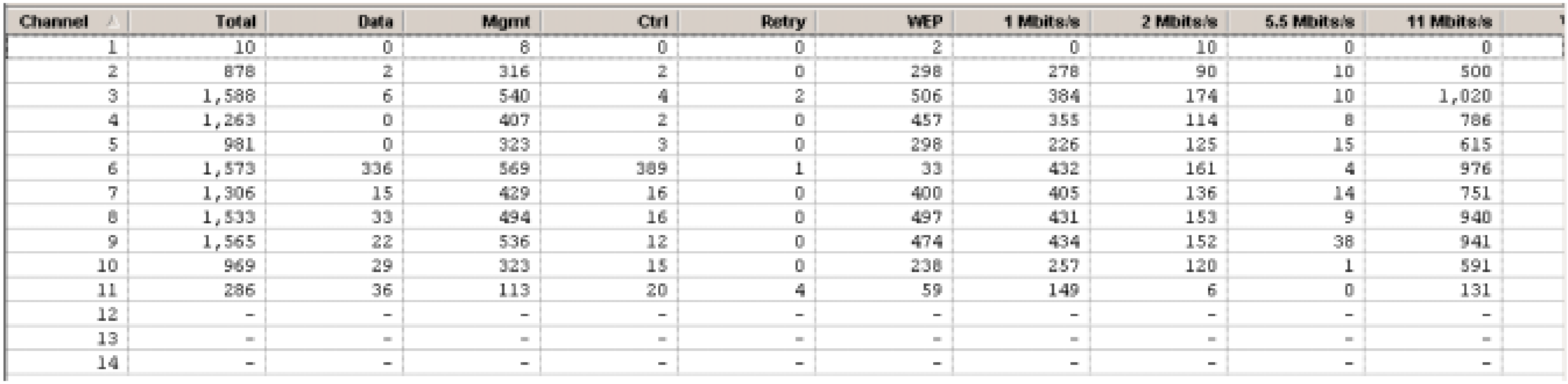
- Determine whether WEP is or is not in use by stations and Access Points
- Determine whether SSID is being broadcast by Access Points or not
- Determine signal strength available at different locations
  - Parking lot
  - Hallways outside of your office
- If upper layer encryption technologies (IPsec, etc…) are in use, confirm that data is not visible
- Use Node statistics to look for unexpected stations
  - Build up a Name Table of known stations
  - Any station without a name is unexpected
    - Add new stations if they are legitimate users
    - Investigate if not

Determining Which Channels Are Being Used



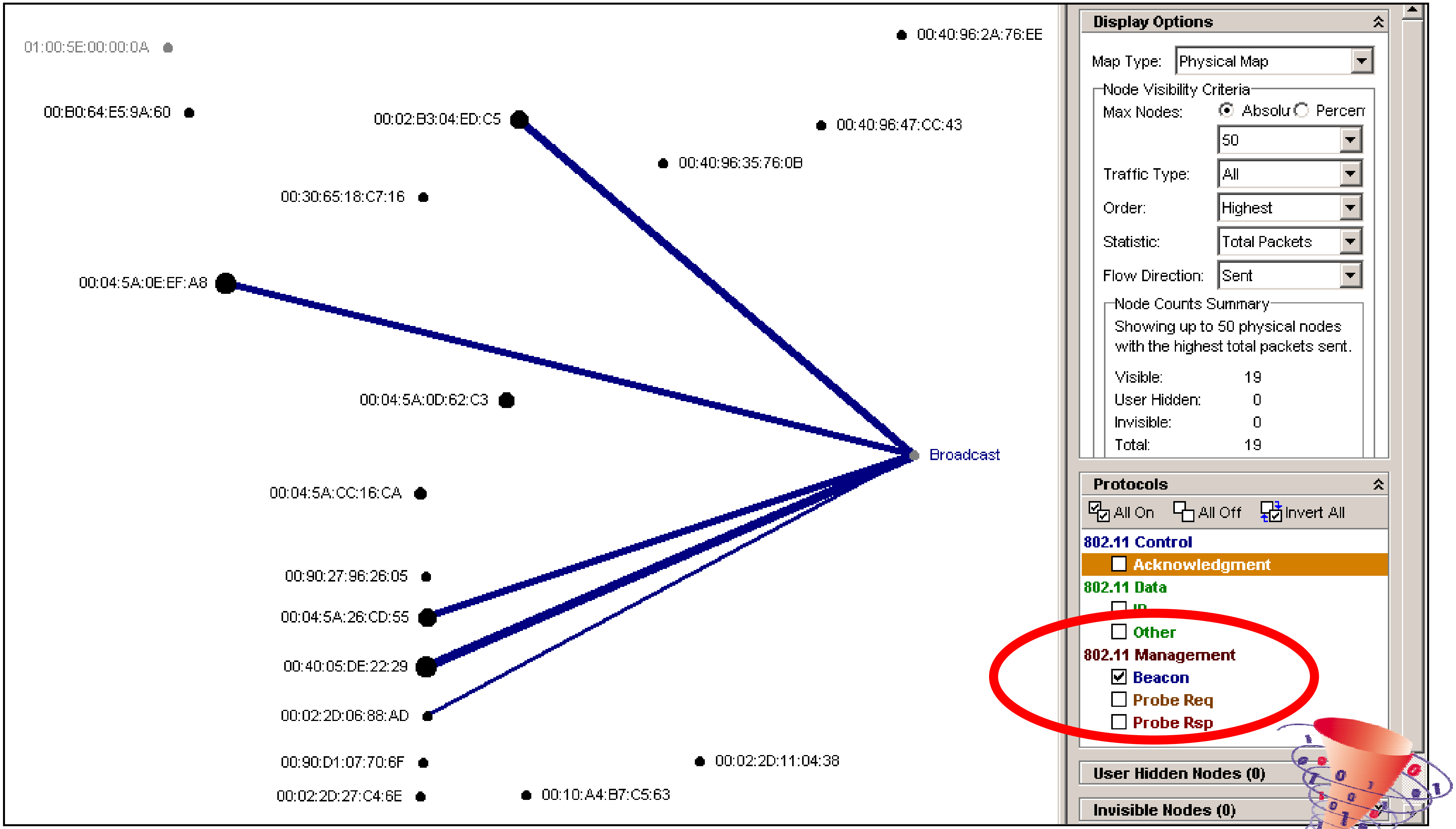
WildPackets

Scanning Shows How Each Channel Is Used



Channel	Total	Data	Mgmt	Ctrl	Retry	WEP	1 Mbits/s	2 Mbits/s	5.5 Mbits/s	11 Mbits/s
1	10	0	8	0	0	2	0	10	0	0
2	878	2	316	2	0	298	278	90	10	500
3	1,588	6	540	4	2	506	384	174	10	1,020
4	1,263	0	407	2	0	457	355	114	8	786
5	981	0	323	3	0	298	226	125	15	615
6	1,573	336	569	389	1	33	432	161	4	976
7	1,306	15	429	16	0	400	405	136	14	751
8	1,533	33	494	16	0	497	431	153	9	940
9	1,565	22	536	12	0	474	434	152	38	941
10	969	29	323	15	0	238	257	120	1	591
11	286	36	113	20	4	59	149	6	0	131
12	–	–	–	–	–	–	–	–	–	–
13	–	–	–	–	–	–	–	–	–	–
14	–	–	–	–	–	–	–	–	–	–

Locating Rogue Access Points



Display Options

Map Type: Physical Map

Node Visibility Criteria

Max Nodes: ● Absolu ○ Percen

50

Traffic Type: All

Order: Highest

Statistic: Total Packets

Flow Direction: Sent

Node Counts Summary

Showing up to 50 physical nodes with the highest total packets sent.

Visible:	19
User Hidden:	0
Invisible:	0
Total:	19

Protocols

802.11 Control
- ☐ Acknowledgment

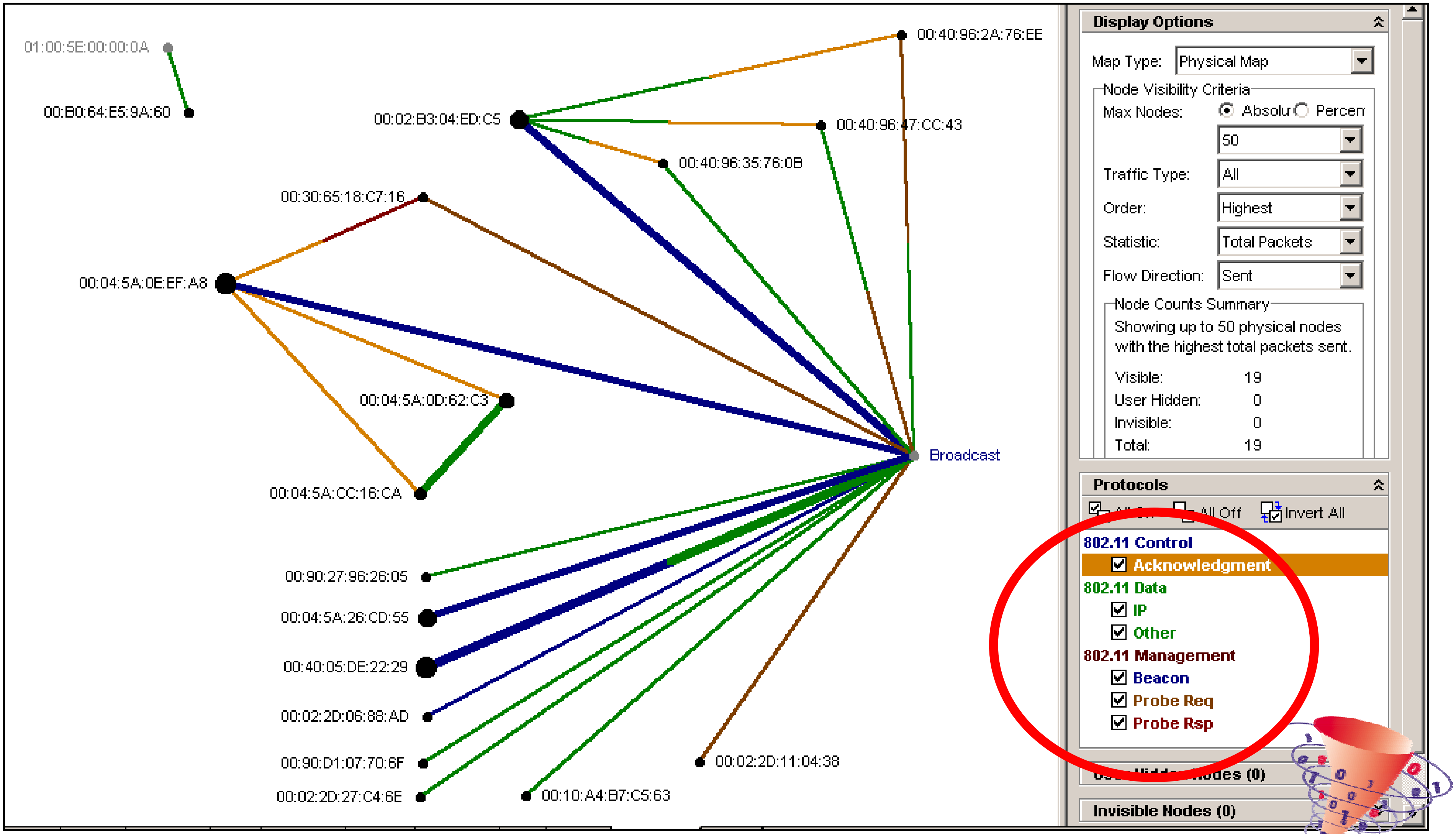
802.11 Data
- ☐ IP
- ☐ Other

802.11 Management
- ☑ Beacon
- ☐ Probe Req
- ☐ Probe Rsp

User Hidden Nodes (0)

Invisible Nodes (0)

Identifying Unusual Traffic Patterns



Display Options

Map Type: Physical Map

Node Visibility Criteria

Max Nodes: ● Absolu ○ Percen

50

Traffic Type: All

Order: Highest

Statistic: Total Packets

Flow Direction: Sent

Node Counts Summary

Showing up to 50 physical nodes with the highest total packets sent.

Visible: 19
User Hidden: 0
Invisible: 0
Total: 19

Protocols

802.11 Control
- ☑ Acknowledgment

802.11 Data
- ☑ IP
- ☑ Other

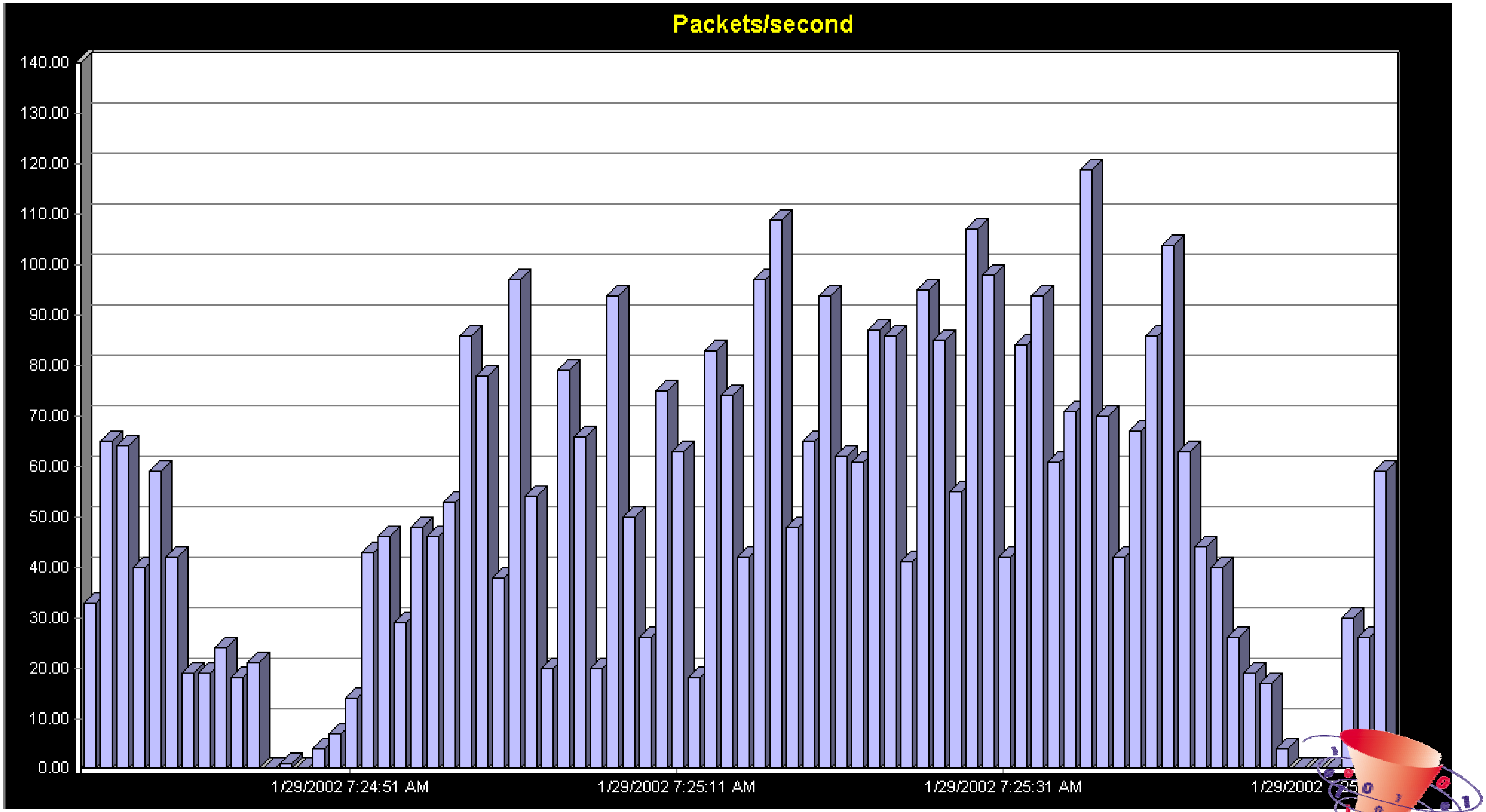
802.11 Management
- ☑ Beacon
- ☑ Probe Req
- ☑ Probe Rsp

U... Hidden Nodes (0)

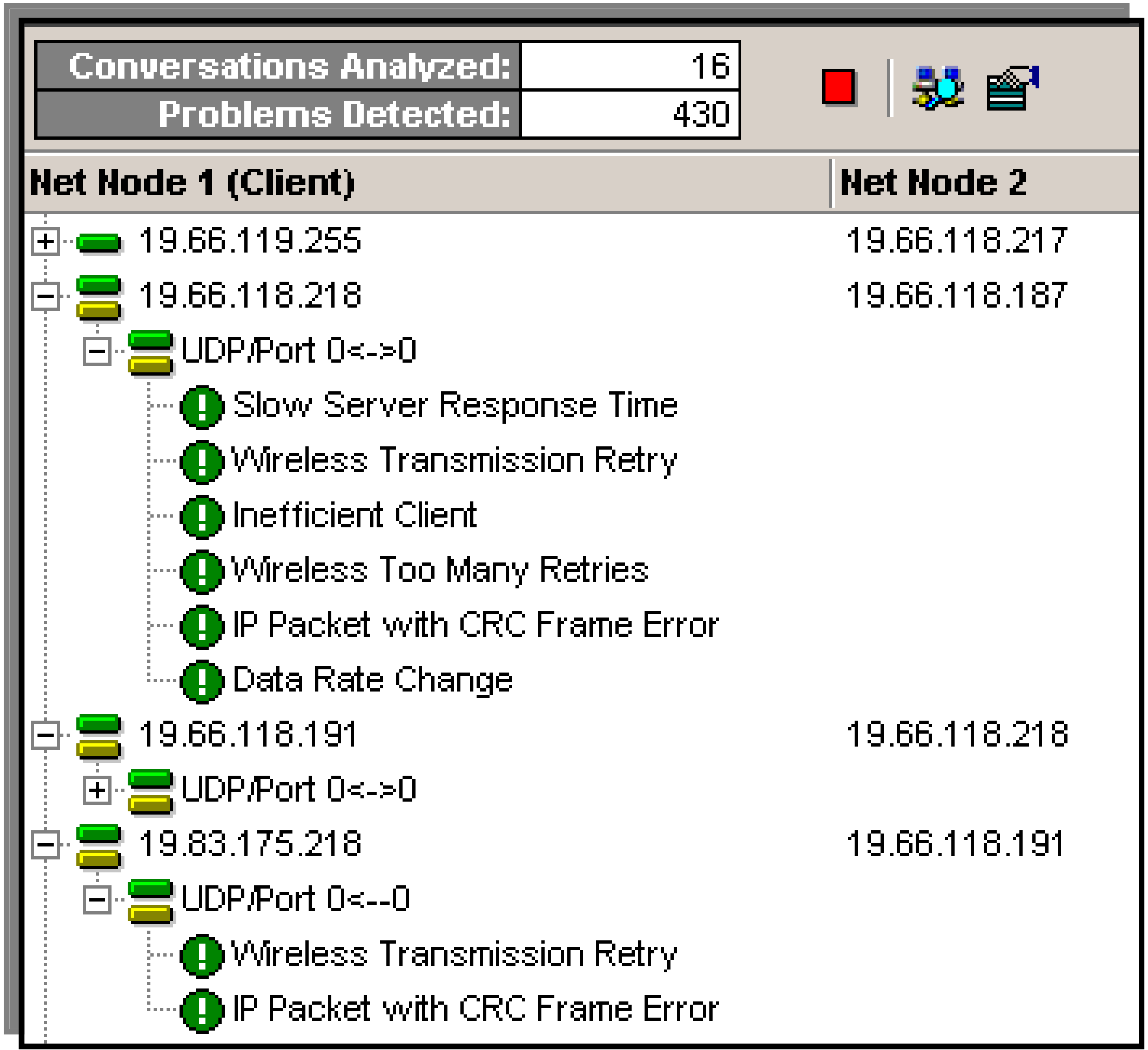
Invisible Nodes (0)

WildPackets

Assessing Band Saturation With AiroPeek NX



Applying Expert System Analysis Techniques

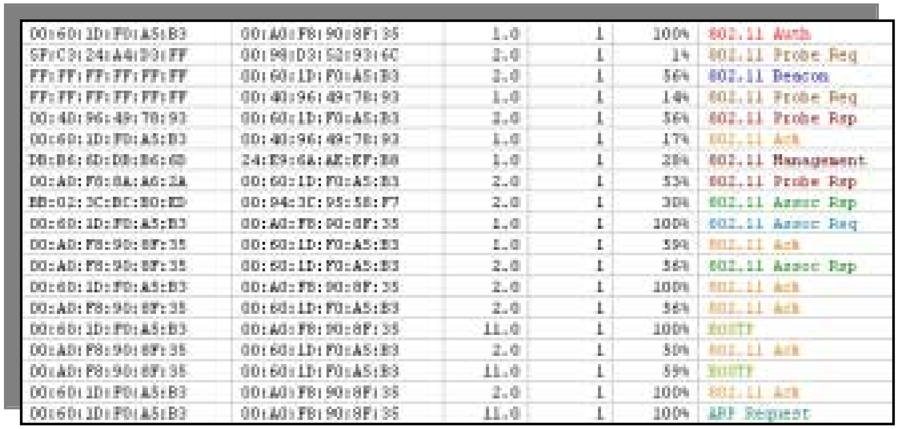


Conversations Analyzed: 16
Problems Detected: 430

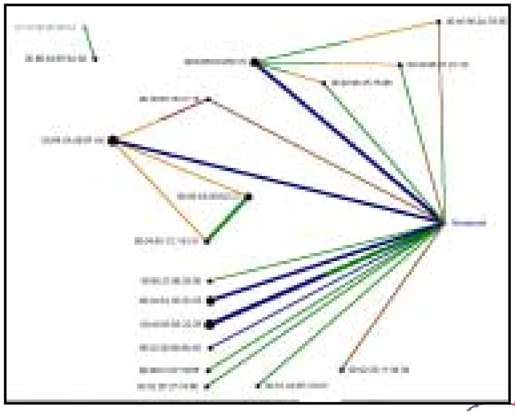
Net Node 1 (Client)	Net Node 2
19.66.119.255	19.66.118.217
19.66.118.218	19.66.118.187
UDP/Port 0<->0	
Slow Server Response Time	
Wireless Transmission Retry	
Inefficient Client	
Wireless Too Many Retries	
IP Packet with CRC Frame Error	
Data Rate Change	
19.66.118.191	19.66.118.218
UDP/Port 0<->0	
19.83.175.218	19.66.118.191
UDP/Port 0<--0	
Wireless Transmission Retry	
IP Packet with CRC Frame Error	

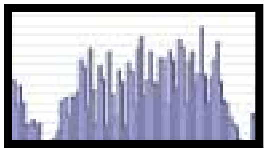
Protocol Analysis In The 802.11 Wireless Environment

- Understand how the protocols work
- Capture from your wireless environment
- Evaluate problem reports, statistics, and individual conversations
- Isolate and describe inappropriate behavior
- Perform a site survey to assess the overall characteristics of your wireless environment



00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	1.0	1	100%	802.11 Auth
5F:C3:24:A4:D3:FF	00:98:D3:52:93:6C	2.0	1	1%	802.11 Probe Req
FF:FF:FF:FF:FF:FF	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Beacon
FF:FF:FF:FF:FF:FF	00:40:96:49:78:93	1.0	1	14%	802.11 Probe Req
00:40:96:49:78:93	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Probe Rsp
00:60:1D:F0:A5:B3	00:40:96:49:78:93	1.0	1	17%	802.11 Ack
D0:B6:6D:D8:B6:6D	24:E9:6A:AE:EF:B8	1.0	1	28%	802.11 Management
00:A0:F8:8A:A6:2A	00:60:1D:F0:A5:B3	2.0	1	53%	802.11 Probe Rsp
8B:02:3C:BC:B0:ED	00:94:3C:95:58:F7	2.0	1	30%	802.11 Assoc Rsp
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	1.0	1	100%	802.11 Assoc Req
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	1.0	1	59%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Assoc Rsp
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	2.0	1	100%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	56%	802.11 Ack
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	11.0	1	100%	BOOTP
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	2.0	1	50%	802.11 Ack
00:A0:F8:90:8F:35	00:60:1D:F0:A5:B3	11.0	1	59%	BOOTP
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	2.0	1	100%	802.11 Ack
00:60:1D:F0:A5:B3	00:A0:F8:90:8F:35	11.0	1	100%	ARP Request





WildPackets

Thank You !

Joe Bardwell
VP of Professional Services
WildPackets, Inc.

www.wildpackets.com