Access Point
Configuration Guide

All Software versions

Document revision 3
Revision date: 2009-08-21

Contents

INTRODUCTION **3**

INTRODUCTION 3
ACCESS POINT / ROUTER FUNCTIONS 3

RECOMMENDED CONFIGURATION **7**

DETAILED RECOMMENDED CONFIGURATIONS 8
Cisco *8*
D-Link *10*
Linksys *11*
Netgear *12*

Introduction

1

Introduction

This document describes how to configure popular commercial 802.11 Access Points to work with Aginova WiFi Sentinel Sensors.

Access Point / Router functions

The IEEE 802.11 suite of standards, often known by the trade name Wi-Fi®, are the basis for most wireless local-area networks. Aginova Sentinel Sensors use an 802.11-compliant wireless link to communicate with a host computer. In Infrastructure mode, an 802.11 Access Point (AP) does the work of managing wireless communications with the Sentinel Sensor and other stations, and forwarding packets between the wireless link and a larger (typically wired) network.

Many AP's also act as TCP/IP routers, providing DHCP service (to give each wireless station that requests it an IP address), and then routing network-layer packets. Network Address Translation (NAT) functions may also be supported. As a consequence, an AP may provide a variety of services, both in managing the wireless links for its client stations, and in configuring the network-layer interface between the stations and the wired network.

Radio PHY and MAC Configuration

Most commercial AP's today support a number of 802.11-related protocols:

- 802.11g: 2.4 GHz band, orthogonal frequency-division multiplexing (OFDM), to 54 Mbps
- 802.11b: 2.4 GHz band, complementary-code-keying (CCK), to 11 Mbps
- 802.11 classic: 2.4 GHz band, Barker code, 1 or 2 Mbps

However, the Sentinel Sensors support only the classic data rates. The more advanced protocols are backward-compatible to varying extents. For example, 802.11b uses classic 1 Mbps long preambles, or optional 2 Mbps short preambles, so that a classic station can detect the preamble and consider the channel as in use even if it cannot decode the data portion of the message. The higher-rate 802.11g packets are invisible to an 802.11 classic or 802.11b radio, but 802.11g

stations can use older 802.11b preambles, or transmit request-to-send (RTC) and clear-to-send (CTS) packets, to ensure that other stations defer during a transmission. These reverse-compatible modes reduce peak rate and may not normally be used if all stations are expected to be 802.11g-capable (typically known as g-only mode), but they are necessary for smooth operation of Sentinel Sensors, which are limited to classic rates.

In order to identify themselves, AP's periodically send out beacon packets, containing their Service Set Identification (SSID, a human-readable name), and some information about the rates they support. A Sentinel Sensor will only associate with an AP with the proper SSID. A list of three SSID's, in order of preference, is pre-configured, and stored in flash memory. The SSID's need to correspond to the SSID names of the AP's you wish to be candidates for association with the node.

AP's transmit within a given radio channel (frequency sub-band) within the 2.4-2.483 GHz US Industrial Scientific and Medical (ISM) band, or on slightly different channels in other jurisdictions. The standard defines 14 channels, spaced 5 MHz apart. However, the classic / 802.11b signals are about 16-20 MHz wide (depending on how you choose to measure the width), and OFDM signals are slightly wider, so in practice there are only 3 non-overlapping channels for US operation: 1, 6, and 11. The channel to be used for each AP can also be configured, or modified, typically using wireless configuration.

Packets can be unicast (addressed to a specific station) or broadcast/multicast (sent to many stations). Unicast packets are always acknowledged by the receiving station; the receipt of the ACK packet tells the transmitting station the message arrived. If no ACK is received, a message can be retransmitted; most stations will also reduce data rate if messages to a specific station are not being acknowledged. Thus as long as an AP is allowed to operate in b/classic mode, a unicast packet directed to a Sentinel Sensor will eventually be transmitted at a classic rate it can understand. On the other hand, broadcast packets are not acknowledged, and so rate backoff cannot be relied upon to ensure that they are sent at a rate the Sentinel Sensor can follow. Many AP's default to sending broadcast packets at the lowest basic rate available, typically 1 Mbps, but certain AP's instead send them at the highest basic rate available; if this is not a classic rate, the nodes will not hear broadcast packets. When those packets contain information the node needs – for example, a DHCP offer of an address (see next section), the node will not be able to join a network.

Beacons play an important role in 802.11's power-save mode, which is used by Sentinel Sensors to save power. If a station is in power-save mode, any multicast frames (frames addressed to all stations in associated with the AP) will be buffered and transmitted with every Delivery Traffic Identification Message (DTIM) beacon. Stations that are asleep need to awaken to hear the DTIM beacon. The DTIM interval – the number of beacons between multicast deliveries – can be set to a small value (1, 2, or 3) for high performance, or to a large value for best endurance. For example, some AP's transmit DHCP acknowledgements to the broadcast address; when the node is in power-save mode, the AP will hold such a packet for DTIM beacon periods. This delay can cause the DHCP routine to time out, so that the node can't get an IP address. AP's also buffer frames that are addressed to a station that is in power-save mode. Each beacon contains of map

indicating buffered frame status for each associated station; a station can wake up and send a power-save poll message to obtain its buffered frames.

WiFi Security

Wireless messages are intrinsically insecure, in that any station in range can listen to transmitted packets. Packets can be encrypted to keep messages private despite such interception. There are a number of differing secure modes of operation, normally configured by the AP:

- **Open authentication**: no authentication or encryption. Any compatible station can associate with an AP, and packets are sent in the clear (unencrypted). This mode is supported by all compliant WiFi stations, including the Sentinel Sensors.
- **Wired Equivalent Privacy (WEP)**: Packets are encrypted using a simple stream cipher; the AP authenticates stations by verifying that they can decrypt a packet. WEP has a number of security flaws rendering it easy to extract the "secret" key. Sentinel Sensors support WEP at different key lengths.
- **WPA/WPA2/802.11i**: Packets are encrypted using either an elaborate version of the WEP cipher with rotating keys (TKIP), or the more sophisticated Advanced Encryption Standard (AES). There are two separate approaches to configuring security in this case. In the first, a passphrase or a 32-byte Pre-Shared Key (PSK) [check] is pre-configured in the node and the AP; knowledge of the secret key is used to authenticate both sides, and encrypt the data. This is often known as the Personal mode. The more sophisticated approach, often referred to as Enterprise mode, uses a Radius authentication server on the AP side, according to the IEEE 802.11i standard; a Protected Access Credential (PAC) must be configured in the sensor, and may be reprovisioned during operation. The Sentinel Sensor supports WPA/TKIP or WPA2/AES using either PSK or 802.11i/Radius.

The security approach in use must be specified at the AP, and the Sentinel Sensor must be appropriately configured according to that approach.

Network Configuration

The Sentinel Sensor uses Simple Network Management Protocol (SNMP) packets to maintain association with the AP, and to allow the node to be configured remotely while in use. The reference User Application sends data packets to a data sink. Data in both cases is encapsulated in Internet Protocol (IP) packets. In order to send and receive these packets, a series of actions must take place:

- The Sentinel Sensor must have an IP address. It normally receives this address using Dynamic Host Configuration Protocol (DHCP). AP's often contain a DHCP server for this purpose; AP's with a DHCP function are often labeled as Wireless Routers. An Access Point without a DHCP server can be used, but only if a DHCP server is available on the same subnet as the AP. Using DHCP allows multiple nodes to flexibly associate with a single AP.

It is also possible to configure a sensor with a fixed (static) IP address. In this case, no DHCP server is needed.

- The Sentinel Sensor needs to send IP packets to a router that can forward those packets over the network. The IP address of the router must be pre-configured in the node. Commercial AP's often contain an embedded router; its IP address may be set to that expected by the sensor.
- Sentinel sensors need to know the IP address of the WiBox server. The Wibox server will normally reside on a host computer accessible to the AP. The address is normally pre-configured, but can optionally be provided by a specialized WiBox server.
- The reference User Application sends data packets to a data sink. The data sink will generally be on a host computer, and need not be configured at the AP, so long as the IP address is accessible from the AP's network connection.

Recommended configuration

2

Recommended configuration for popular APs and Routers

Commercial APs are generally equipped with an embedded web server, allowing them to be configured using any standard web browser. The AP documentation will provide the web address, user name, and password to be used to access the configuration pages. AP's may also incorporate an SNMP Agent, for remote automated configuration.

Generic Configuration Instructions

Most access points will work with the Sentinel Sensors "out of the box", once a few simple configuration settings are made.

- Set the SSID to the one specified in your user guide.
- Set the IP address of the AP to the one specified in your user guide.

Table 1: Summary of configuration requirements for common AP's.

Vendor	*Model*	*Generic Config OK?*	*Remarks*
Cisco	AP1231G-A-K9	-	Set basic rate to 1-2 Mbps. DHCP server configuration required.
D-Link	DWL-6730AP	4	Set backside switch to AP.
Linksys	WRT54G v 2.1	4	
	WRT54GS v 8	4	
Motorola	AP 5131	4	
Netgear	WG602	-	No DHCP server; custom configuration required.
	WPN824	4	

Note that the settings given above correspond to the default configuration for a Sentinel Sensor.

Detailed Recommended Configurations

Configuration details for a number of common commercial access points are provided in the following tables. Note that different terminology may be used by different vendors for the same or similar parameter. Recommended parameter values or ranges have been verified to support communication with a Sentinel Sensor. Disparaged settings work poorly or not at all.

Cisco

The Cisco AP1200 can provide DHCP service to its wireless clients, but the DHCP service is not enabled by default. There are three approaches to configuring the AP1200 to communicate with a Sentinel Sensor:

- Connect the AP1200 to an Ethernet switch or router with a DHCP server. The Sentinel Sensor DHCP request will be forwarded through the AP1200 to the server, which will then assign the node an address. The Cisco AP can be configured with a fixed IP address in the same subnet, or can accept an address from the same remote DHCP server.
- Configure the Sensor with a fixed IP address, in the same subnet as the fixed IP addresses of the AP and SNMP Manager.
- Enable the AP's local DHCP server. This requires a serial connection to the AP, using an RJ45-to-serial adaptor or cable plugged into the Console port on the AP1200. A host serial communications utility such as Hyperterminal can be used to communicate over the serial port; the required settings are 9600 baud, 8 bits, 1 stop bit, no parity. Commands you type are shown in **bold**.

```
ap>enable
ap>password  (enter Cisco unless you have changed the passsword)
ap#conf t
(Enter configuration commands, one per line.  End with CNTL/Z.)
ap(config)#ip dhcp pool 3-network
ap(dhcp-config)#network 192.168.0.0 255.255.255.0
ap#sh run
```

The detailed configuration recommendations for the Cisco radio interface are summarized in Table 2.

Table 2: Configuration details, Cisco AP1231G-A-K9

Parameter	Recommended	Disparaged	Remarks
EXPRESS SECURITY			
SSID	Any		Must correspond to one of the preferred SSID's configured in the Sentinel Sensor.
Broadcast SSID in Beacon	Checked		If the Sensor is configured for passive scanning, SSID broadcast must be enabled. Sensors configured for active scanning work with or without SSID Broadcast (default value).
EXPRESS SET-UP			
Configuration server protocol	Static IP		The method the AP gets its address (NOT the way it distributes addresses to wireless clients). DHCP can be selected if the Ethernet port of the AP is connected to a DHCP server.
Role in Radio Network	Access Point		
Optimize Radio Network for:	Custom or Range	Default	See NETWORK INTERFACES below.
Aironet Extensions	Enable		Disable can be used.
NETWORK INTERFACES: Radio(x)-802.11G: SETTINGS			
Enable Radio	Enabled	Disabled	Note the radio cannot be enabled until an SSID is entered.
Role in Radio Network	Access Point		
Data Rates	Best Range	Best Throughput, Default	
Data Rates, custom settings	Require 1 Mbps and/or 2 Mbps	Require > 2 Mbps (only)	Note: higher rates can be Enabled as desired. OK: 2Mbps required, 5.5Mbps required **WRONG**: 5.5Mbps required, all other enabled
CCK Transmitter Power	Any		Transmitter power depends on range, interference, and propagation conditions.
OFDM Transmitter Power	Any		
Client Power Local	Enable, Disable		
Limit Client Power	Any		
Default Radio Channel	1,6,11 (US)		Must correspond to one of the preferred SSID channels configured in the sensor.
World-mode multi-domain	NA		

World Mode	Any		
Radio Preamble	Short, Long		
Receive Antenna	Diversity		Selection of a specific antenna may be appropriate if the antenna configuration differs from the default dipole pair.
Transmit Antenna	Diversity		
Traffic Stream Metrics	Enable, Disable		
Aironet Extensions	Enable, Disable		
Ethernet Encapsulation	Either		
Reliable Multicast to Workgroup Bridges	Enable, Disable		
Public Secure Packet Forwarding	Enable, Disable		
Short slot-time	Enable, Disable		
Beacon Privacy Guest Mode	Enable, Disable		
Beacon Period	20-1000	>1000	
DTIM Interval	1-25	>50	Assumes beacon interval = 100
Max Data Retries	Any		
Max RTS Retries	Any		
Fragmentation Threshold	2346		Values to 256 can be used.
RTS Threshold	2347		Values to 0 can be used.
Root Parent Settings	NA		

D-Link

Table 3: Configuration details, D-Link DWL-G730AP.

Parameter	Recommended	Disparaged	Remarks
HOME - WIRELESS			
SSID	Any		Must correspond to one of the preferred SSID's configured in the Sensor.
Channel	1,6,11 (US)		Must correspond to one of the preferred SSID channels configured in the Sensor.
SSID Broadcast	Enabled		If the Sensor is configured for passive scanning, SSID broadcast must be enabled. Sensors configured for active scanning work with or without SSID Broadcast (default value).
Security	Disable, WEP, WPA-PSK,		

	WPA2-PSK		
HOME – DHCP			
DHCP Server	Enabled	Disabled	The Sensor requires a DHCP server be available unless it is configured with a fixed IP address. Starting and ending IP addresses can be any subnet-compliant address allowing access to the desired services.
ADVANCED-PERFORMANCE			
Beacon Interval	100		Values up to 1000 can be used.
RTS Threshold	2432		Values down to 256 can be used.
Fragmentation	2346		Values down to 256 can be used.
DTIM Interval	1-3	>50	Assumes beacon interval = 100 ms.
TX Rates	Auto	1, 2, 5.5 and above	
Mode Setting	Mix Mode	G Mode	
Preamble	Short, Long		
Antenna Transmit Power	Any		Transmit power depends on range, interference, and propagation conditions.

Note that the configuration switch on the back of the unit should be set to the AP position. The DWL-6730 contains two internal antennas, orthogonal to one another but both polarized in the plane of the circuit board. The circuit board should be aligned with the polarization of the Sensor antenna.

Linksys

Table 4: Configuration details, Linksys WRT54G v8.

Parameter	Recommended	Disparaged	Remarks
BASIC SETUP			
DHCP Server	Automatic Configuration-DHCP		The node requires a DHCP server be available unless it is configured with a fixed IP address. Starting and ending IP addresses can be any subnet-compliant address allowing access to the desired services.
BASIC WIRELESS SETTINGS			
Wireless Network Mode	B-only		G-only, Mixed also work.
Channel	1,6,11 (US)		Must correspond to one of the preferred SSID channels configured in the Sensor.
SSID Broadcast	Enabled		If the Sensor is configured for passive scanning, SSID broadcast must be enabled. Sensors configured for active scanning work with or without SSID Broadcast (default value).

ADVANCED WIRELESS SETTINGS			
Authentication Type	Auto	Shared Key	
Basic Rate	1-2 Mbps	Default, Auto	
Transmission Rate	Auto, 1 Mbps, 2 Mbps	5.5 and above	Lower data rates provide longer range but are more susceptible to interference.
CTS Protection Mode	Disable		Auto also works.
Frame Burst	Disable		
Beacon Interval	100-1000	5000 and above	
DTIM Interval	1-255		Choice depends on tradeoff between performance and power consumption.
Fragmentation Threshold	2346		Values down to 256 can be used.
RTS Threshold	2347		Values down to 0 can be used.
AP Isolation	Off		On can be used.
Secure Easy Setup	Disable		Enable can be used.
WIRELESS SECURITY			
Security Mode	Disabled, WPA Personal TKIP, WPA2 Personal TKIP+AES, WEP, WPA Personal AES, WPA2 Personal AES, WPA2 Enterprise		

The WRT54G is equipped with external dipole-type antennas. At least one of these antennas should be generally aligned along the polarization direction of the Sensor antenna.

Netgear

Table 5: Configuration details, Netgear WPN824 v3.

Parameter	Recommended	Disparaged	Remarks
LAN IP Setup			
DHCP Server	Use Router as DHCP Server		The node requires a DHCP server be available unless it is configured with a fixed IP address. Starting and ending IP addresses can be any subnet-compliant address allowing access to the desired services.
WIRELESS SETTINGS			
Channel	1,6,11 (US)		Must correspond to one of the preferred SSID channels configured in the node.

Mode	b-only, b and g	g-only	Auto-108 Mbps requires that the node be configured for operation on channel 6.
Security Options	None, WPA2-PSK (AES), WPA-PSK (TKIP), WPA-PSK (TKIP)+WPA2-PSK (AES)		
ADVANCED WIRELESS SETTINGS			
Enable Wireless Router Radio	Enabled		Required for the unit's radio to operate.
SSID Broadcast	Enabled		If the Sensor is configured for passive scanning, SSID broadcast must be enabled. Sensors configured for active scanning work with or without SSID Broadcast (default value).
Fragmentation Length	2346		Values down to 256 can be used.
CTS/RTS Threshold	2347		Values down to 1 can be used.
Preamble Mode	Short, Long		
Advanced 108 Mbps Features	Disabled		Enabled also works (but see above).
eXtended Range Features.	Disable, Enabled.		

The WPN824 is equipped with a number of internal antennas, all in the plane of the circuit board. The circuit board should be generally aligned with the polarization direction of the Sensor antenna.

Document source: Gainspan Corp.