WIDS/WIPS White Paper

Copyright © 2026 TP-Link Systems Inc. All rights reserved.
No part of this document may be reproduced, copied, or transmitted in any form or by any means without the prior written permission of the company.

Contents

1 Overview 3
1.1 Introduction 3
1.2 Background 3
1.3 Purpose of This White Paper 4
2 Key Technologies 4
2.1 Basic Concepts 4
2.1.1 Detection Mechanism 4
2.1.2 Analysis Mechanism 5
2.1.3 Protection Mechanism 5
2.1.4 Advantages 5
2.2 Market Demand 5
3 Key Technical Principles 6
3.1 Protocol Analysis 6
3.1.1 Management Frames 6
3.1.2 Control Frames 6
3.1.3 Data Frames 6
3.2 Principle Analysis 7
3.2.1 Protocol Parsing 7
3.2.2 Behavior Analysis 7
3.2.3 Environment Awareness and Comparison 8
3.2.4 Feature Impact 8
3.2.5 Summary 8
3.3 Framework Analysis 8
4 Application Scenarios 11
4.1 Open Public Wi-Fi Scenarios 11
4.2 Enterprise Office Scenarios 12
4.3 High-Security and Sensitive Scenarios 12
4.4 High-Density, Controlled-Access Scenarios 13
5 Representative Models 14
6 Glossary 14

1 Overview

With the widespread adoption of wireless networks, Wi-Fi has become the primary means for enterprises and the public to access the internet. Compared with wired networks, wireless networks are more susceptible to various security threats due to their open nature and shared spectrum, including fake access points, disconnection attacks, hotspot spoofing, and resource exhaustion attacks.

As key components of the wireless security framework, WIDS (Wireless Intrusion Detection System) and WIPS (Wireless Intrusion Prevention System) enable threat identification and proactive defense by continuously sensing and analyzing the wireless air interface environment. This technology effectively addresses gaps in traditional network security on the wireless side, providing more comprehensive and real-time protection.

This chapter provides an overall introduction to WIDS/WIPS from three aspects: system overview, technical background, and the purpose of this white paper.

1.1 Introduction

WIDS and WIPS are core technology modules for securing wireless networks. By leveraging detection capabilities deployed on APs, WIDS continuously monitors the wireless air interface, identifies abnormal behaviors and unauthorized devices in the network, and generates security events. Building on WIDS, WIPS adds protection capabilities and intervenes in or blocks identified attacks through measures such as dynamic block lists and active disconnection (Deauthentication).

By relying on the existing wireless infrastructure, the system provides real-time awareness and security control of the wireless environment, forming a complete protection framework covering detection–analysis–response.

1.2 Background

As wireless networks continue to expand in scale, network boundaries have become increasingly blurred. Attackers can directly access the network environment through the wireless air interface, making wireless security issues more prominent. Common wireless attack types include:

- AP Spoofing / Rogue APs
- Deauthentication Attacks
- Flood Attacks
- Brute Force Attacks
- Hotspot Attacks
- Malformed Frames

Because traditional network security policies mainly operate on wired networks or higher-layer protocols, they cannot effectively detect attacks at the wireless air-interface layer. Therefore, it is necessary to establish dedicated detection and protection mechanisms at the 802.11 protocol layer to enhance overall wireless network security.

1.3 Purpose of This White Paper

This white paper aims to provide a systematic description of the WIDS/WIPS technology framework, including:

- Explaining wireless security threats and their detection models
- Introducing key technologies and system advantages
- Describing core functional modules and implementation mechanisms
- Analyzing system architecture and typical application scenarios

This white paper helps network administrators and system integrators fully understand the principles of wireless security protection and guides practical deployment and use.

2 Key Technologies

2.1 Basic Concepts

The core operating mechanism of a WIDS/WIPS system can be summarized into three interconnected stages: Detect, Analyze, and Protect. Through this closed loop, the system continuously identifies and controls security threats in the wireless environment.

2.1.1 Detection Mechanism

By listening to frames on the wireless air interface, the system detects devices and behaviors in the network and abstracts the findings into standardized security events.

To effectively describe complex wireless environments, the system breaks network behaviors down into multiple categories of detection events, covering the following typical security scenarios:

- **Abnormal control behavior detection**
  Includes abnormal disconnection behaviors such as broadcast deauthentication and broadcast disassociation.
- **Access point spoofing and identity impersonation detection**
  Includes AP spoofing, AP impersonation, and SSID hijacking.
- **Abnormal network topology detection**
  Includes unauthorized ad-hoc networks and other unauthorized network formation behaviors.
- **Protocol anomaly detection**
  Includes abnormal information elements, abnormal HT parameters, and abnormal control fields.
- **Abnormal communication behavior detection**
  Includes flood attacks and abnormal request behaviors.
- **Authentication security detection**
  Includes brute-force attacks and anomalies during the authentication process.

With this event framework, the system converts complex wireless air-interface behaviors into structured security events, providing a foundation for subsequent analysis.

2.1.2 Analysis Mechanism

After relevant events are detected, the system evaluates them through multi-dimensional analysis to determine whether they constitute actual security threats.

The analysis process mainly uses the following methods:

- **Protocol rule validation:** Determines whether frames comply with standard protocol specifications.
- **Behavioral statistical analysis:** Analyzes whether device behavior exhibits abnormal patterns.
- **Environment comparison analysis:** Determines whether a device or network matches normal deployment characteristics.

Through these mechanisms, the system can differentiate normal communication behavior from potential attack behavior, improving detection accuracy.

2.1.3 Protection Mechanism

When the system confirms a security threat, it triggers corresponding protection policies to intervene in the attack.

The main protection methods supported include:

- **Dynamic block list mechanism:** Isolates abnormal devices and blocks their communications.
- **Deauthentication countermeasure:** Forces clients to disconnect from unauthorized connections.

Protection is executed locally on the wireless access point, enabling fast response while minimizing impact on overall network performance.

2.1.4 Advantages

- Provides protocol-level detection for fine-grained identification of wireless attacks.
- Supports real-time local protection with rapid response.
- Integrates detection and protection into a closed-loop control system.
- Supports flexible policy configuration to fit different scenarios.
- Leverages existing wireless devices, resulting in low deployment cost.

2.2 Market Demand

With the widespread use of wireless networks in enterprise and public environments, demand for wireless security has increased significantly, mainly due to:

- Increasing security compliance requirements
- Higher security risks in public wireless environments
- Escalating threats driven by the proliferation of attack tools
- Wireless access becoming the mainstream networking method

Wireless security capabilities have shifted from an optional feature to a foundational infrastructure requirement.

3 Key Technical Principles

3.1 Protocol Analysis

The WIDS/WIPS system operates based on the IEEE 802.11 protocol. By parsing 802.11 wireless frames, it identifies and analyzes device behavior in a wireless network. Wireless frames are typically categorized as management frames, control frames, and data frames. Each frame type carries different functional information and serves as a key foundation for security detection.

3.1.1 Management Frames

Management frames are used to establish and maintain a wireless network, including Beacon, Probe Request/Response, Authentication, and Association.

Specifically:

- Beacon frames broadcast basic network information (e.g., SSID, capability parameters, etc.).
- Probe frames support device scanning and network discovery.
- Authentication/Association frames are used during the connection establishment process.

Management frames are often transmitted without encryption and are easy to spoof or tamper with, so they are vulnerable to wireless attacks. For example, rogue AP and hotspot deception attacks typically spoof legitimate Beacon information.

3.1.2 Control Frames

Control frames coordinate channel access, such as RTS, CTS, and ACK. By analyzing key fields in control frames (e.g., Duration), the system can identify abnormal channel-occupancy behavior. For example, an attacker can craft an abnormal Duration value to keep the channel occupied for an extended period, disrupting normal communications and causing a denial-of-service (DoS) attack.

3.1.3 Data Frames

Data frames carry actual user traffic on the wireless network. They can also reflect client behavior during access authentication and device interactions. While management frames primarily describe network structure, data frames more directly reflect behavior patterns during communication, which makes them important for detecting sophisticated attacks.

Based on the system's current detection capabilities, data-frame security analysis can be summarized in the following typical scenarios:

- **Authentication security behavior detection**

  During Wi-Fi access, a client establishes a connection through authentication and key negotiation. This process is completed through data frame exchanges.

  By analyzing authentication-phase interactions, the system can detect risks, such as:

  - Abnormal authentication attempts (e.g., frequent failures)
  - Unauthorized or abnormal key negotiation behavior

This category helps detect password attacks and authentication anomalies, such as brute-force attempts.

- **Abnormal communication behavior detection**

Data frames directly reflect a client's communication behavior. By analyzing transmission patterns and communication frequency, the system detects abnormal behavior patterns, such as:

- Sending a large volume of request traffic in a short time
- Abnormal interaction frequency or patterns

These behaviors often indicate abnormal resource consumption and are typical DoS attack indicators.

- **Power-saving mechanism anomaly detection**

In wireless communications, clients can use power-saving mechanisms to reduce power consumption, and related behavior is also reflected in data frames. By analyzing changes in these behaviors, the system detects abnormal activity that abuses power-saving mechanisms, such as:

- Abnormal connection states
- Abnormal growth in buffered data

These anomalies can disrupt normal communication and, in specific scenarios, represent interference or resource-consumption behavior.

3.2 Principle Analysis

The WIDS/WIPS system continuously collects and analyzes over-the-air wireless data to build comprehensive awareness of the wireless environment. From a technical perspective, it relies on coordinated mechanisms in three areas—protocol parsing, behavior analysis, and environment awareness—to accurately identify abnormal activity.

3.2.1 Protocol Parsing

Protocol parsing is the foundation of the system's detection capabilities. WIDS/WIPS parses wireless frame structures and fields to determine whether they comply with IEEE 802.11 specifications.

In standard 802.11 frames, field structures are well-defined. Abnormal values in key fields typically indicate that the traffic deviates from normal communication patterns. Examples include:

- Abnormal Information Element (IE) length
- Authentication parameters that do not conform to the spec
- Abnormal Duration values in control frames

By identifying these anomalies, the system can detect potential security risks early in the communication process.

3.2.2 Behavior Analysis

In complex wireless environments, a single frame often cannot fully represent device

behavior. The system therefore uses behavioral statistics to analyze device behavior over a defined time window.

This mechanism focuses on identifying event frequency and behavior patterns. For example:

- An abnormal increase in request frames per unit time may indicate a flooding attack.
- A sustained increase in authentication failures may indicate brute-force behavior.

Behavior analysis improves detection accuracy by identifying anomalies at the pattern level and helps reduce false positives.

3.2.3 Environment Awareness and Comparison

Because wireless networks operate across multiple channels, information from a single channel cannot represent the full environment. To address this, the system scans channels to collect wireless information and build a complete view of the environment.

Based on environmental data, the system can perform comparative analysis, such as:

- Determining whether the same SSID is being broadcast simultaneously by multiple unauthorized devices
- Determining whether device identifiers (e.g., BSSID or MAC address) show abnormal inconsistencies

If the system detects that the source of the same SSID is inconsistent and does not match normal deployment characteristics, it can indicate a rogue AP or hotspot deception attack.

3.2.4 Feature Impact

When you enable WIDS, the AP periodically scans the surrounding wireless environment, which may have a slight impact on peak wireless performance.

For most APs that do not have a dedicated radio for scanning, the scan uses the service radio. WIDS performs a single-channel scan every 20 seconds, with a maximum channel dwell time of 60 ms. The impact depends on the environment and traffic load. Evaluate before enabling WIDS in high-density deployments.

3.2.5 Summary

By combining protocol parsing, behavior analysis, and environment awareness, the WIDS/WIPS system accurately identifies abnormal activity in the wireless environment and provides a reliable basis for follow-up protection, enabling proactive wireless security.

3.3 Framework Analysis

In the Omada Controller, go to the **Site** view, then go to **Network Config** > **Security** > **Wireless IDS/IPS**. On this page, you can:

- Configure Wireless IDS and Wireless IPS
- View Wireless IDS detected events and Dynamic Block List entries for a selected time range

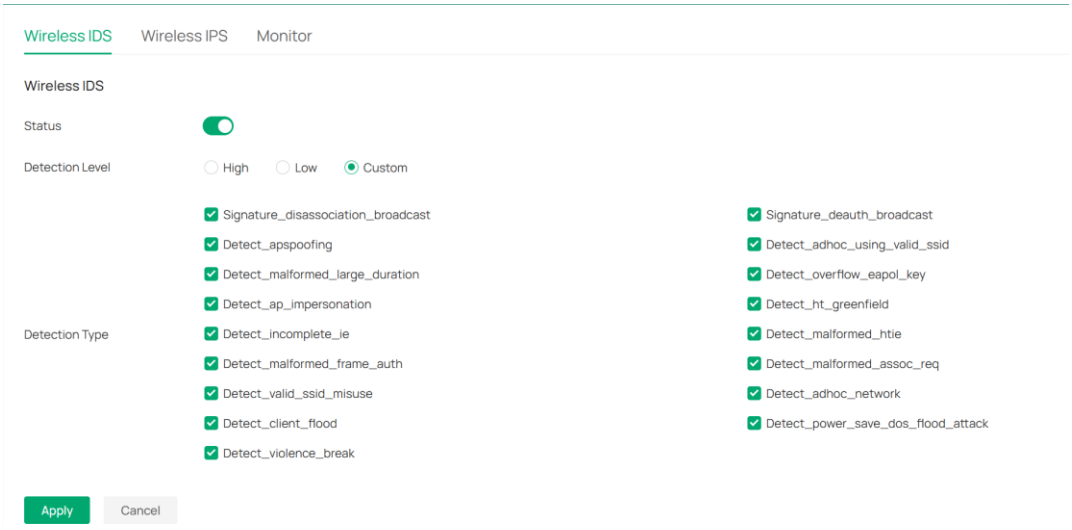


Figure 3-1: Wireless IDS configuration page

Status: Global toggle

Detection Level: Controls which Wireless IDS event types are enabled.

- **High:** Selects all event options.
- **Low:** Selects Detect_apspoofing, Detect_malformed_large_duration, Detect_ap_impersonation, Detect_valid_ssid_misuse, Detect_client_flood, and Detect_violence_break.
- **Custom:** Allows you to select specific event options.

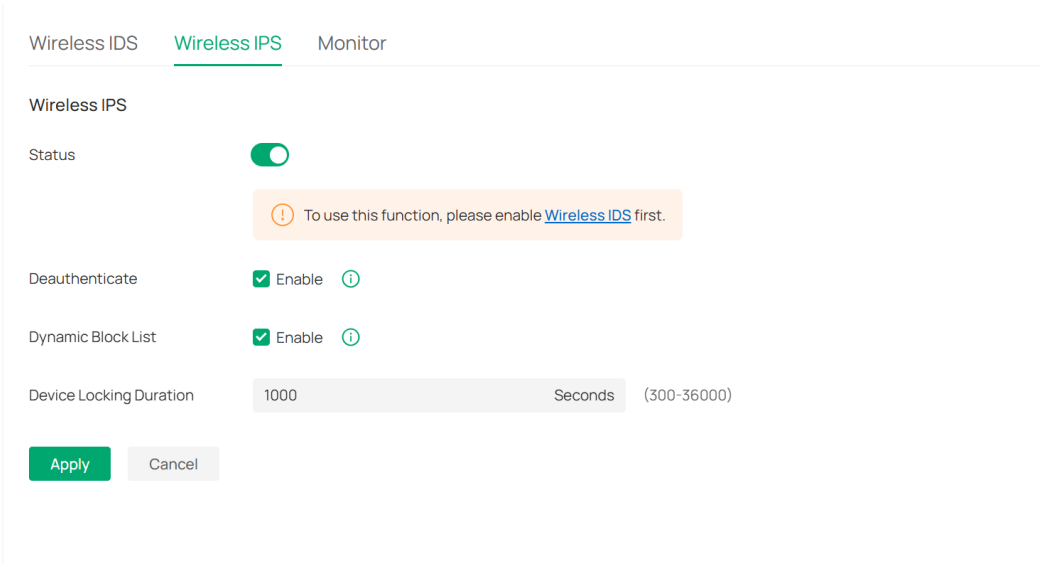


Figure 3-2: Wireless IPS configuration page

Status: Global toggle

Deauthenticate: When enabled, the Omada AP actively mitigates detected malicious APs by disconnecting clients from those APs. To use this feature, make sure you have enabled Detect_adhoc_using_valid_ssid and Detect_valid_ssid_misuse. Otherwise, this setting has no effect.

Dynamic Block List: When enabled, if an AP detects malicious activity such as brute-force attacks, it adds the attacker to the block list and ignores that attacker's packets for a period of time. To use this feature, make sure you've enabled Detect_client_flood, Detect_violence_break, and Detect_power_save_dos_flood_attack. Otherwise, this setting has no effect.

Device Locking Duration: Specifies how long an attacker remains on the dynamic block list. Valid range: 300 seconds to 36,000 seconds. If you do not have specific requirements, use the default value (1,000 seconds).

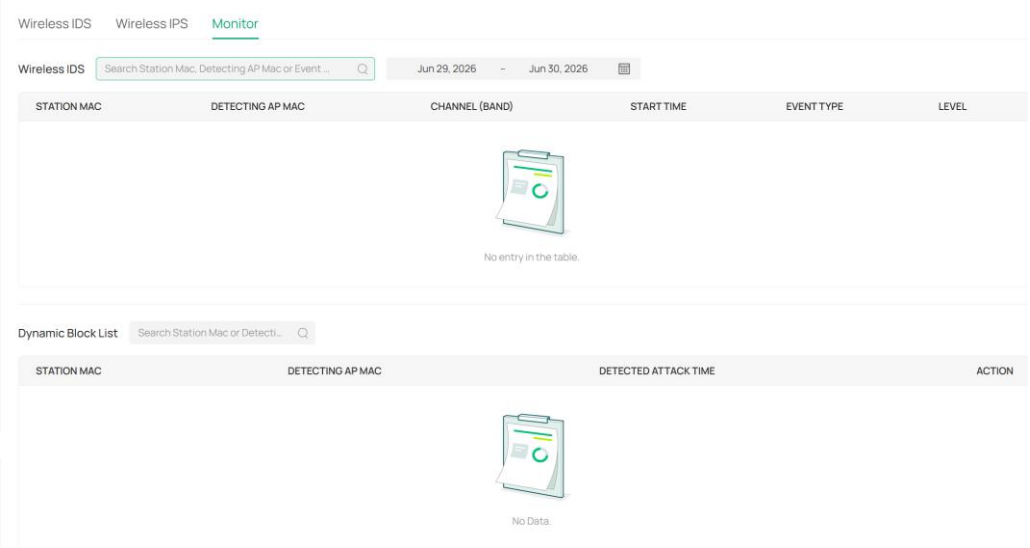


Figure 3-3: Monitor page

Omada currently supports 17 WIDS events. The following table describes each event:

Event Type	Detection Criteria	Detection Level	WIPS Mitigation
Signature_disassociation_broadcast	Broadcast Disassociation frames are present in the wireless environment.	High	-
Signature_deauth_broadcast	Broadcast Deauthentication frames are present in the wireless environment.	High	-
Detect_apspoofing	There are management frames with the same MAC address as the current AP.	Low	-
Detect_adhoc_using_valid_ssid	There is an ad hoc network that uses the same SSID as the current AP.	High	Deauthenticate
Detect_malformed_large_duration	Wireless frames have abnormal Duration values.	Low	-
Detect_overflow_eapol_key	EAPOL frame KeyLength is invalid.	High	-
Detect_ap_impersonation	Beacon frame count is abnormal.	Low	-

Detect_ht_greenfield	An AP with Green Field enabled exists in the environment.	High	-
Detect_incomplete_ie	Management frame length is abnormal.	High	-
Detect_malformed_htie	Beacon frame HT Capabilities are abnormal.	High	-
Detect_malformed_frame_auth	Authentication frame is abnormal.	High	-
Detect_malformed_assoc_req	Association Request frame is abnormal.	High	-
Detect_valid_ssid_misuse	An unauthorized AP uses the same SSID as the current AP.	Low	Deauthenticate
Detect_adhoc_network	An ad hoc network is detected.	High	-
Detect_client_flood	A client is performing a management-frame flooding attack.	Low	Dynamic Block List
Detect_power_save_dos_flood_attack	A client is performing a flooding attack using Null Data frames.	High	Dynamic Block List
Detect_violence_break	A client is performing a brute-force attack.	Low	Dynamic Block List

4 Application Scenarios

4.1 Open Public Wi-Fi Scenarios

In open public Wi-Fi environments, user sources are diverse, and the surrounding wireless environment is uncontrollable. Risks such as rogue APs, phishing Wi-Fi, and look-alike SSID impersonation are common. These scenarios require continuous visibility into the wireless environment, rapid threat identification and localization, and the ability to coordinate alerts with response/countermeasure actions. WIDS/WIPS can be used to:

- Scan in real time and identify rogue APs, fake APs, and phishing hotspots using the same SSID
- Monitor and alert on abnormal access and suspicious communication behaviors
- Classify legitimacy and trace the source based on SSID/MAC/location and other attributes
- Trigger response actions in coordination (e.g., alerting, isolation, blocking/countermeasures) to enable visualization and centralized management of wireless security

In high-traffic, high-mobility environments, such as airports and train stations, access is highly concurrent, and clients frequently connect and disconnect. Users may mistakenly connect to a fake official Wi-Fi, leading to phishing or man-in-the-middle attacks. WIDS/WIPS can scan for and identify look-alike rogue APs and alert/block abnormal access.

In complex environments, such as shopping malls and commercial complexes, SSIDs are numerous, and self-deployed marketing Wi-Fi networks are mixed together. Unauthorized APs and spoofed hotspots can easily appear, introducing data leakage and control risks. WIDS/WIPS can perform unified scanning, classification, and visual risk labeling to support

centralized governance.

In open service venues, such as hotels and cafés, users stay for long periods and often conduct payments or office work, making them targets of persistent rogue AP and man-in-the-middle attacks. WIDS/WIPS can continuously monitor spoofed hotspots and abnormal communications, issue alerts, and proactively block suspicious connections.

4.2 Enterprise Office Scenarios

In enterprise office networks, internal data is sensitive. Employee-deployed hotspots or unauthorized routers can create uncontrolled entry points such as rogue APs, increasing the risk of brute-force attacks and various other wireless attacks. These scenarios require wireless visibility, rogue AP identification and location tracking, abnormal behavior monitoring and alerting, and policy-based response (isolation/blocking). WIDS/WIPS can be used to:

- Discover and classify rogue APs, employee-deployed hotspots, and unauthorized wireless devices, and assist in locating and tracing them
- Analyze client behavior to identify and alert on abnormal access and abnormal association/authentication behavior
- Monitor and detect common wireless attacks, generating security event records and visualization
- Enforce response policies for illegal devices/high-risk connections: isolation, blocking/disconnection, or alert-driven handling

In core business departments, such as R&D offices, data is highly valuable, and unauthorized access or wireless attacks can easily cause leaks. WIDS/WIPS can focus on detecting fake APs, man-in-the-middle attacks, and abnormal traffic, and proactively block high-risk connections.

In small offices and branch sites, limited IT resources may allow unauthorized APs or misconfigurations to go unnoticed for extended periods. WIDS/WIPS enables centralized monitoring of branch wireless environments, automatically discovering rogue APs, abnormal clients, and attack behaviors, and sending alerts to headquarters.

In headquarters and other centralized office locations with dense personnel and heavy business loads, employee hotspots or unknown APs can easily become uncontrolled entry points. WIDS/WIPS can continuously monitor and identify unauthorized hotspots/unknown APs, and eliminate risks in time through alerts or policy actions.

4.3 High-Security and Sensitive Scenarios

In highly security-sensitive scenarios, there are strict compliance and audit requirements, and the environment is more likely to face targeted attacks such as Evil Twins, wireless eavesdropping, and man-in-the-middle attacks. These scenarios require continuous full-band monitoring, accurate attack identification, traceable log retention, and proactive defense and response capabilities. WIDS/WIPS can be used to:

- Perform continuous full-band scanning and long-term wireless security monitoring
- Detect advanced attack behaviors (e.g., signal/identity spoofing) and trigger alerts
- Generate detailed logs and event records to support auditing and compliance evidence
- In WIPS mode, proactively handle high-risk connections (e.g., forced disconnection/blocking)

In government agencies and administrative offices, information and systems are highly sensitive, and wireless compromise via rogue APs or man-in-the-middle attacks poses extremely high risk. WIDS/WIPS can continuously monitor for illegal APs, spoofed SSIDs, and abnormal behaviors, and coordinate alerts and blocking of high-risk connections to keep wireless operation under control.

Financial institutions, such as banks and securities firms, carry transactions and customer data, and are common targets for wireless eavesdropping and hijacking attacks, potentially leading to security incidents involving funds and information. WIDS/WIPS can identify phishing hotspots and high-risk behaviors such as man-in-the-middle attacks, and prevent illegal access through monitoring, alerts, and WIPS countermeasures.

In research institutions such as laboratories, data and research outputs require strong confidentiality. Rogue APs or wireless eavesdropping can leak sensitive information. WIDS/WIPS can monitor research areas and detect unknown APs, abnormal clients, and suspicious communications, retaining audit records to support rapid investigation and stronger protection.

4.4 High-Density, Controlled-Access Scenarios

In high-density, controlled-access scenarios, the number of clients is large, and the wireless environment is complex. Self-deployed hotspots/APs are common, making it difficult to distinguish legitimate devices from unauthorized ones. Interference and security issues compound and affect network stability, and administrators cannot quickly troubleshoot manually. These scenarios require unified wireless visibility, automatic identification and differentiation of abnormal APs/clients, rapid localization and tracing, and alert-driven response. WIDS/WIPS can be used to:

- Scan the wireless environment in a unified way to discover abnormal clients and abnormal APs
- Identify and locate unauthorized/illegal APs (including self-deployed hotspots) and classify them
- Monitor and alert on abnormal access and suspicious wireless behaviors to help quickly locate root causes
- Trigger coordinated response policies (e.g., alert/isolate/block) to reduce the impact of abnormal devices on the network

In university campuses with teaching buildings and dormitories, there are many

endpoints, wide coverage, dense AP deployments, and frequent self-deployed hotspots and external AP access, which can easily cause environmental disorder and security risks. WIDS/WIPS can scan and identify self-deployed hotspots/unauthorized APs centrally and assist rapid response through alerts.

In large venues such as convention and exhibition centers, short-term high-concurrency access and dense AP deployments are common. Exhibitors' self-deployed wireless devices further complicate the environment and increase management difficulty. WIDS/WIPS can identify illegal APs/abnormal devices, distinguish official networks from third-party networks, and assist rapid troubleshooting.

In large office areas such as industrial parks, networks are large-scale and complex. Department-deployed APs or non-standard configurations can easily lead to loss of wireless control. WIDS/WIPS can monitor the environment as a whole, detect unauthorized APs and abnormal access, and improve centralized management efficiency with unified alerts.

5 Representative Models

Category	Models
Pro AP	AP9635 1.0, AP9635 2.0, AP8635-I 1.0, AP8635-E 1.0, etc.
EAP	EAP772 2.0, EAP772-Outdoor 1.0, EAP787 1.0, etc.

Note: EAP models support WIDS/WIPS only after they are updated to firmware that is compatible with Controller v6.3 or later.

6 Glossary

Term	Explanation
AP	Access Point
Ad-Hoc	Ad hoc network
HT	High Throughput
RTS	Request to Send
CTS	Clear to Send
ACK	Acknowledgement