Security Protocol Overview for AddPac IoT Solution

AddPac Technology

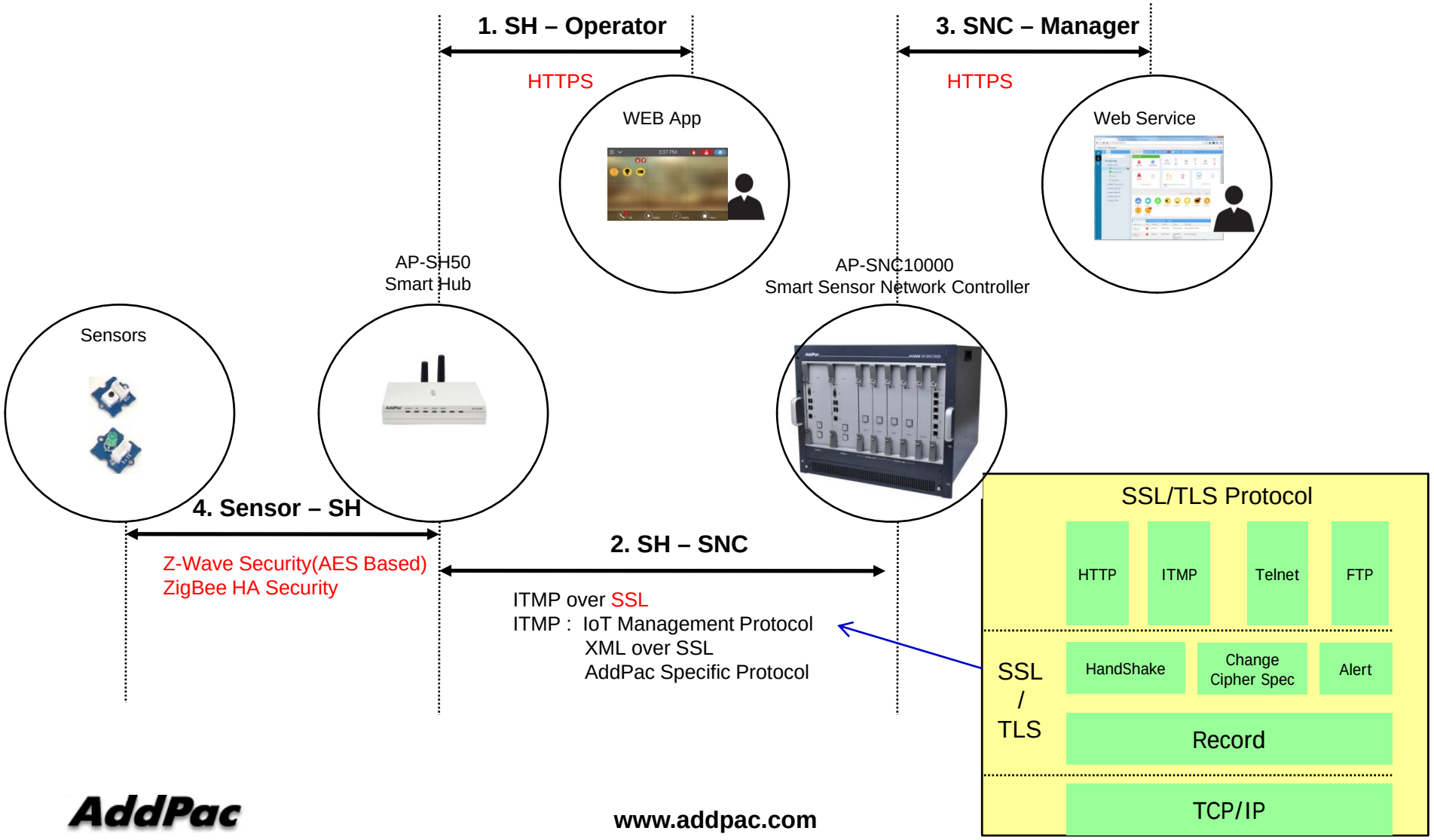
Sales and Marketing

www.addpac.com

Contents

- Security Protocol Network Diagram for AddPac IoT Solution
  - 1. Between Smart Hub and Web App.
  - 2. Between Smart Hub and Smart Sensor Network Controller
  - 3. Between Smart Sensor Network Controller and Web manager
  - 4. Between Zwave Sensor and Smart Hub
- SSL/TLS Secure Protocol Overview
- AddPac Smart IoT Solution Overview

AddPac IoT - Security Protocol Network Diagram

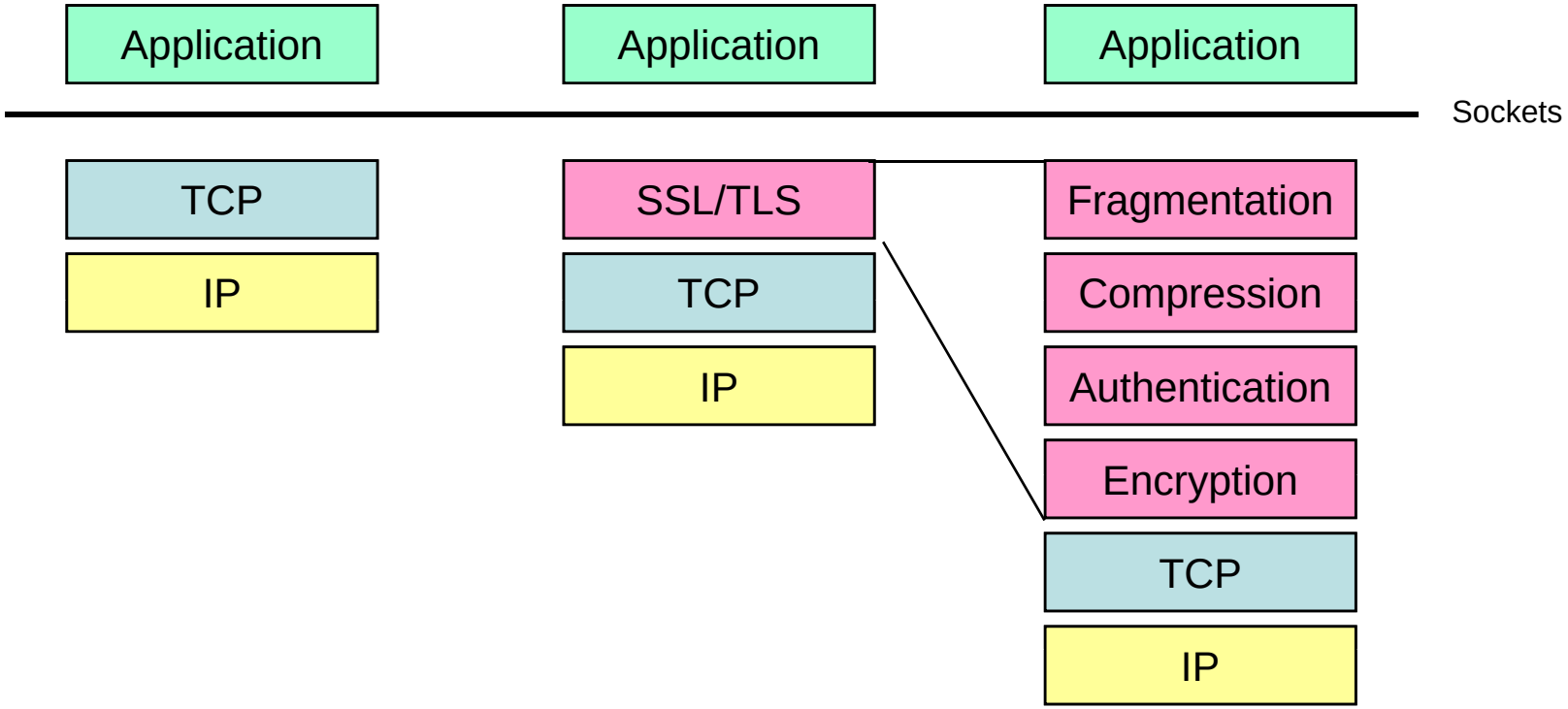


SSL/TLS
Secure Protocol Features

TLS Features for Secure VoIP Service

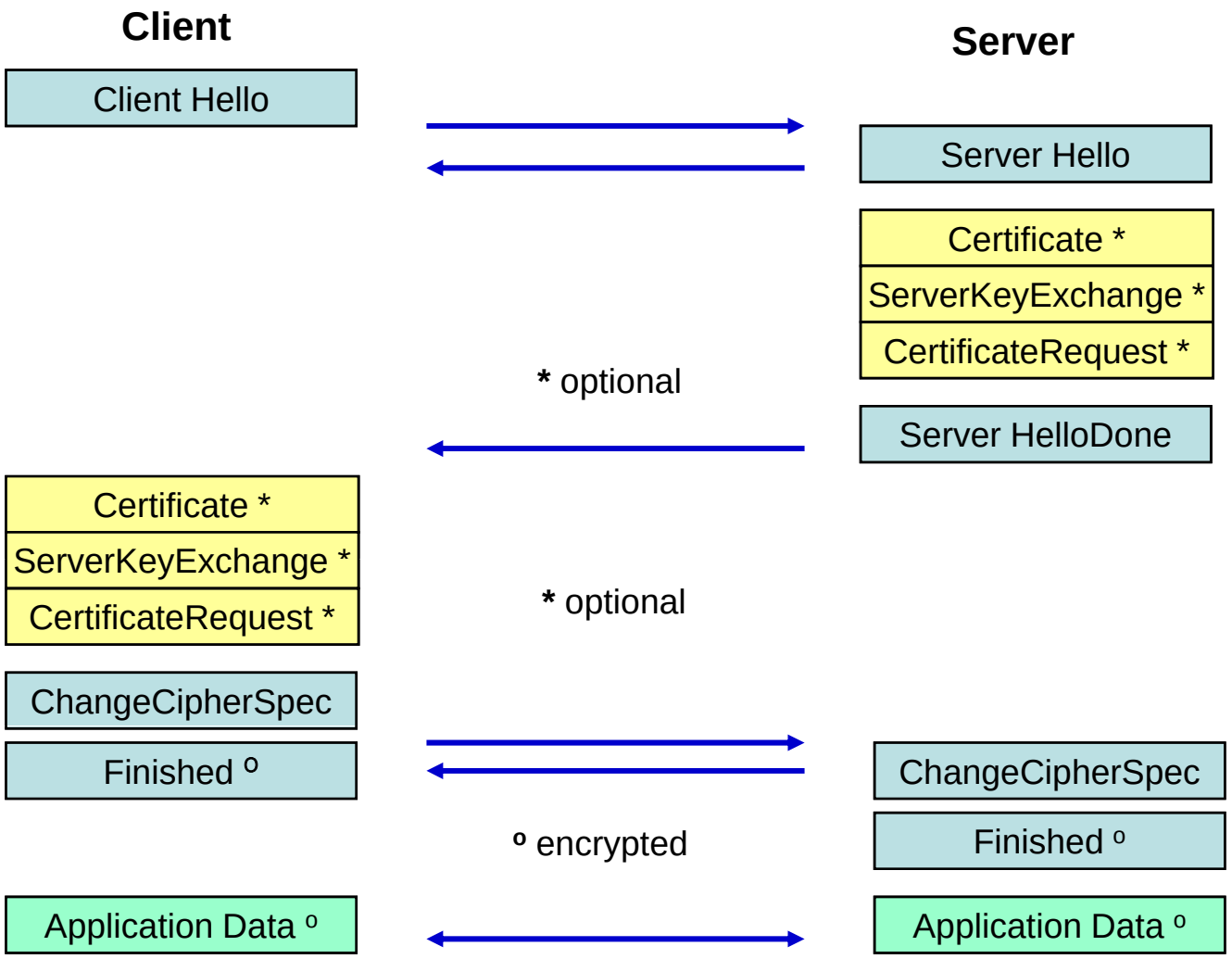
- Support for TLS 1.1, TLS 1.0 and SSL 3.0 protocols
- Since SSL 2.0 is insecure it is not supported.
- TLS 1.2 is supported but disabled by default.
- Support for TLS extensions: server name indication, max record size, opaque PRF input, etc.
- Support for authentication using the SRP protocol.
- Support for authentication using both **X.509 certificates** and OpenPGP keys.
- Support for TLS Pre-Shared-Keys (PSK) extension.
- Support for Inner Application (TLS/IA) extension.
- Support for X.509 and OpenPGP certificate handling.
- Support for X.509 Proxy Certificates (RFC 3820).
- Supports all the strong encryption algorithms (including SHA-256/384/512), including Camellia (RFC 4132).
- Supports compression (optional).
- CRLs
  - CRL (Certificate Revocation List)
  - OCSP (Online Certificate Status Protocol, RFC2560) (via HTTP)
- Hash Algorithm : SHA-1, MD5

SSL/TLS Protocol Layers



SSL/TLS Handshake

AP1950S Secure VoIP Gateway



TLS Comparison with OpenSSL

- **Protocol Support**

	SSLv2.0	SSLv3.0	TLSv1.0	TLSv1.1	TLSv1.2
AddPac	No	Yes	Yes	Yes	Yes
OpenSSL	Yes	Yes	Yes	No	No

- **Key Exchange Algorithms**

	Anon-RSA	RSA	RSA Export	DHE-RSA	DHE-DSS	SRP-DSS	SRP-RSA	SRP	PSK	ECC
AddPac	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
OpenSSL	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes

- **Encryption Algorithms**

(*1) **40-bit encryption is insecure**

	AES-256-CBC	AES-128-CBC	3DES CBC	DES CBC	RC4-128-CBC	RC4-40(*1)	RC2-40(*1)	Camellia	SEED	ARIA
AddPac	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenSSL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

AddPac
IoT Equipment

Smart IoT Equipment Table

Smart Enterprise Products	Description	Model
	Smart Hub for ZigBee/ZWave Sensors	AP-SH50, AP-SH50ZW, AP-SH70, AP-SHD100
	Smart Hub Cloud for ZWave Sensors	AP-SH20, AP-SH20W
	Enterprise Smart Hub	AP-SH1000
	Site based Smart Sensor Network Controller	AP-SNC2000
	Center based Multi-Site Smart Sensor Network Controller	AP-SNC10000

Smart IoT Equipment Table

Smart Enterprise Products	Description	Model
	Smart Hub + Wall PAD	AP-SHC300
	Sensor Control Wall PAD	AP-SWP100
	Smart Phone and Tab/Pad Appl.	AP-ASH100, AP-ISH100
	Enterprise IoT Manager Appl.	AP-ASM1000

Sensor Network Controller Comparison Table

Sensor Network Controller / Specification	AP-SNC10000	AP-SNC3000	AP-SNC2000
			
Capacity Level	Large Scale	Medium Scale	Small & Medium
Processor	Intel	RISC	RISC
Operating System	Linux	Embedded Linux	Embedded Linux
System Duplication for Fault Tolerant	Support	Support	Support
Power Duplication (module type)	Support	Support	N/A

Large-Scale
Smart Sensor Network Controller
AP-SNC10000

Product Overview

AP-SNC10000 Smart Sensor Network Controller

- Large-Scale Sensor Network Control Service
- Support Large-Scale Smart Hub Devices for Zigbee/Zwave sensors
- One(1) System Dual Sensor Network Controller Architecture
  One(1) Gigabit Ethernet Interface, Two(2) Hard Disk / a CPU Board
  Default : Single Smart Sensor Network Controller
  Option A : Dual Smart Sensor Network Controller
  Option B : One(1) Smart Sensor Network Controller
  + One(1) Smart Sensor Network Manager
- Fault Tolerant and Scalability Architecture
- Powerful Management and User Friendly Features
- Firmware Upgradeable Architecture
- Linux Operation System
- Dual Redundancy Power Module

Hardware Specification

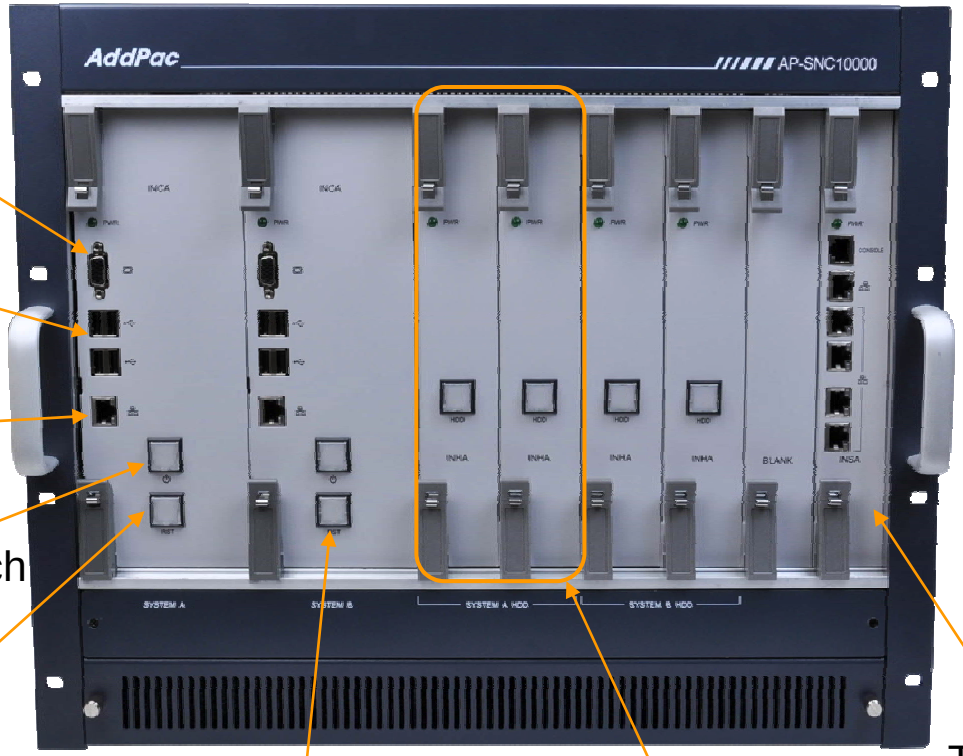
AP-SNC10000 Smart Sensor Network Controller

- High-End Computing Power
- Main Chassis
  - Dual Redundancy CPU Boards for System Fault Tolerant
    - One(1) 10/100/1000Mbps Gigabit Ethernet
    - Four(4) USB Interface Port
    - VGA Interface Port for External Video Monitor
    - Two(2) 3.5 Inch Hard Disk Interface Slot (RAID 1)
  - Dual Redundancy Power Supply Module
  - Hot-Swap Features
  - Right most two(2) slots is reserved for Switch Board,, etc

Hardware Specification

AP-SNC10000 Smart Sensor Network Controller

AP-SNC10000 Front Side



VGA Connector

USB Interface

Gigabit Ethernet Port

Power On/Off Switch for System

CPU Board A (Hot-Swap)

CPU Board B (Hot-Swap)

Dual 3.5 Inch HDD Disks(RAID1) : Hot-Swap

Two(2) Slots is reserved for Switch Board, etc

Hardware Specification

AP-SNC10000 Smart Sensor Network Controller

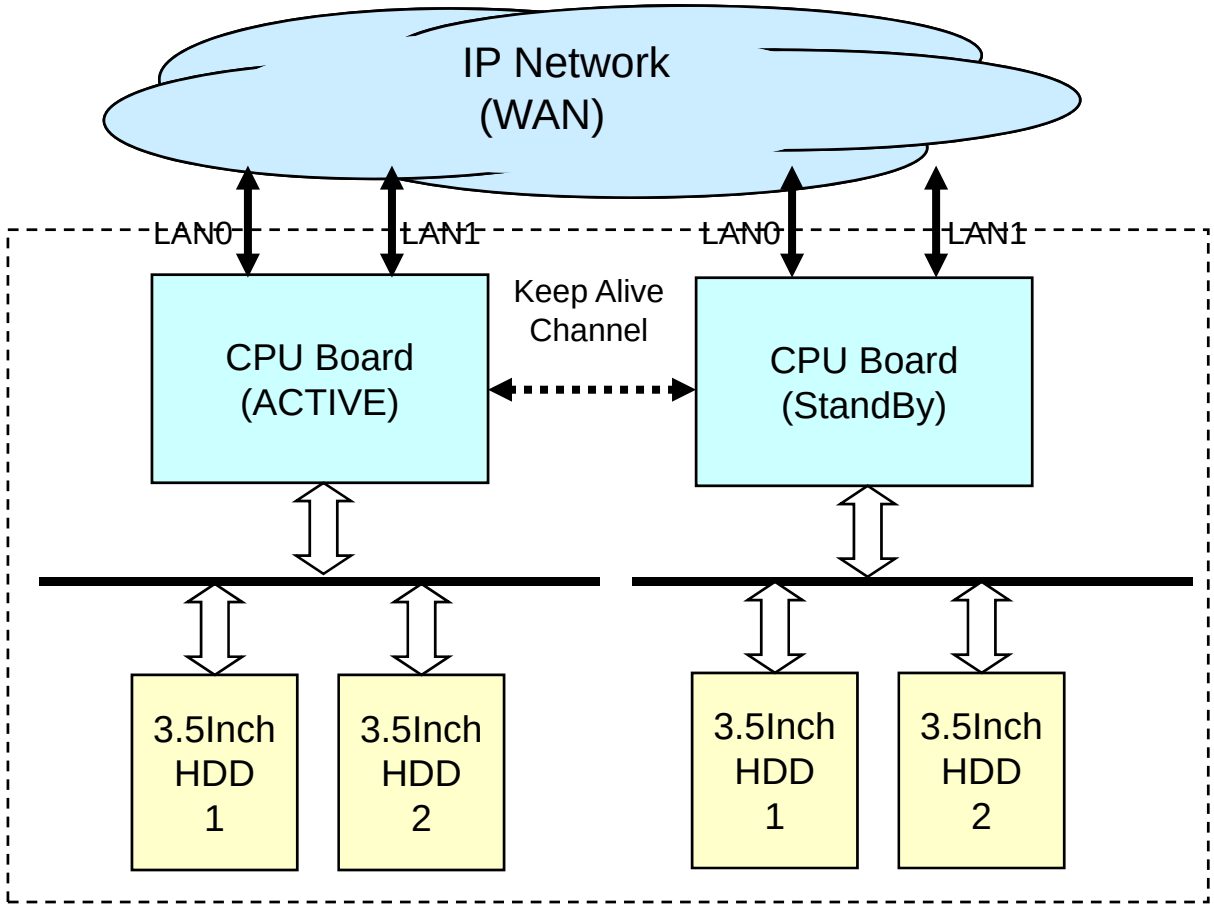
AP-SNC10000 Back Side



System Redundancy Features

AP-SNC10000 Smart Sensor Network Controller

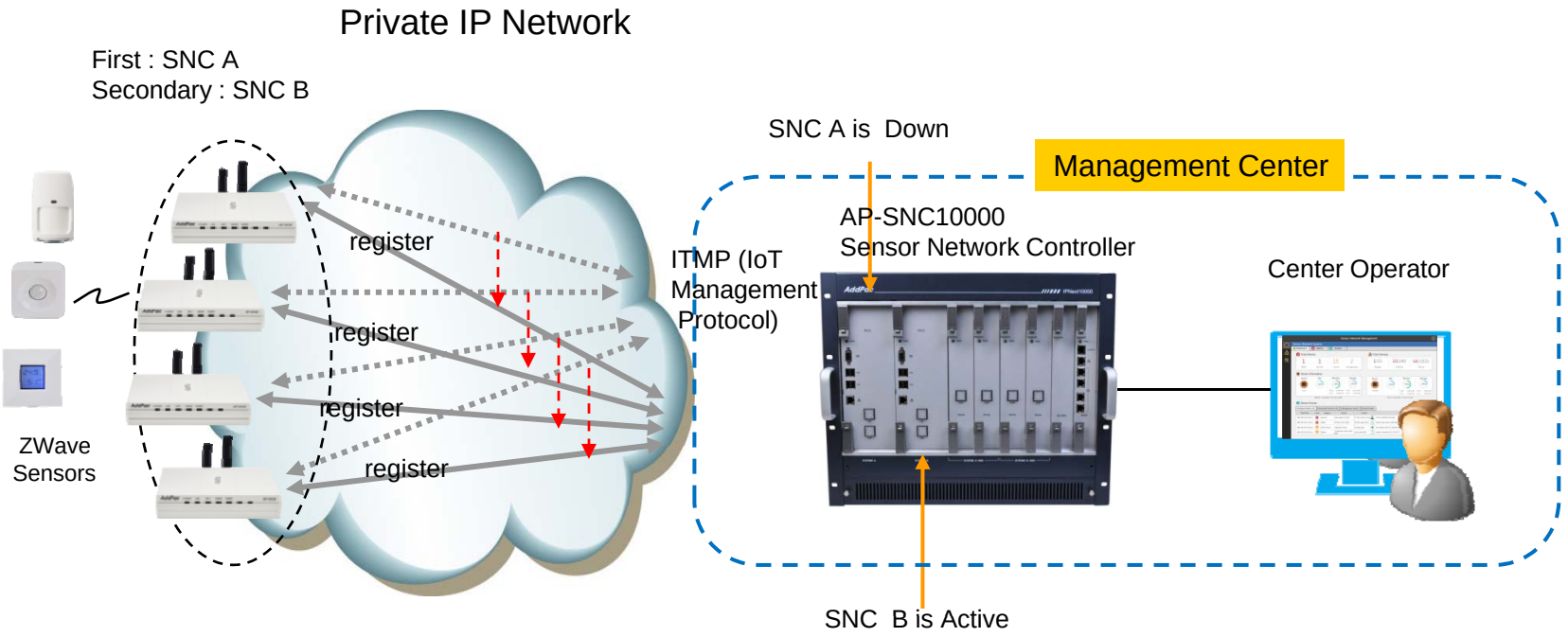
AP-SNC3000 System Block Diagram



System Redundancy Features

AP-SNC10000 Smart Sensor Network Controller

- Active– Active Duplication Scheme
- Active – Standby Duplication Scheme
- VRRP based Duplication Scheme



Active – Standby Duplication Scheme (example)

Smart Sensor Network Controller
AP-SNC3000

Product Overview

AP-SNC3000 Smart Sensor Network Controller

- Embedded H/W Platform with Dual CPU Module Slots
- Fault Tolerant and Reliability Service
- Support Multiple Smart Hub for Zigbee/Zwave sensors
- Support RTSP based Network Video Encoder (Video Codec, IP Camera, etc) Control
- Support RTP based Video Door Phone Control
- Mini Call Manager Function Support for Smart Phone, Tab/PAD registration
- Load Balance using RTSP Redirect Service
- Web based Smart Sensor Network Control Management Software

Benefits and Features

AP-SNC3000 Smart Sensor Network Controller

- Multiple Smart Hub Support for Zigbee/Zwave sensors
- RTP based Video Door Phone Support
- RTSP based Network Video Encoder Support
- TCP/UDP Transport Protocol Support
- Two(2) Module Slots for Embedded Sensor Control Service Module
- Fault Tolerant and High Reliability Service using Dual CPU Module
- Load Balance and Hot-Swap Service
- Compact Size and Low Power Consumption compare with Commercial Server
- IP based Network Protocol Support
- Web based Smart Sensor Network Control Management Software
- Smart Tab, Smart Phone Appl. Support for Sensor Control, Network Camera, Video Door Phones.
- Mini Call Manager Support for Standard SIP based Smart Phone Application Services

Hardware Specification

AP-SNC3000 Smart Sensor Network Controller

High-end RISC

AP-SNC3000 Front Side



Power On/Off Switch for System

CPU Board (Hot-Swap)

Dual Power Supply Modules (Hot-Swap)

Dual 3.5 Inch HDD Disks(RAID1) : Hot-Swap

Hardware Specification

AP-SNC3000 Smart Sensor Network Controller

High-end RISC

AP-SNC3000 Back Side



LAN0 for Active CPU

LAN1 for Active CPU

FANs for Air Cooling

LAN0 for Standby CPU

LAN1 for Standby CPU

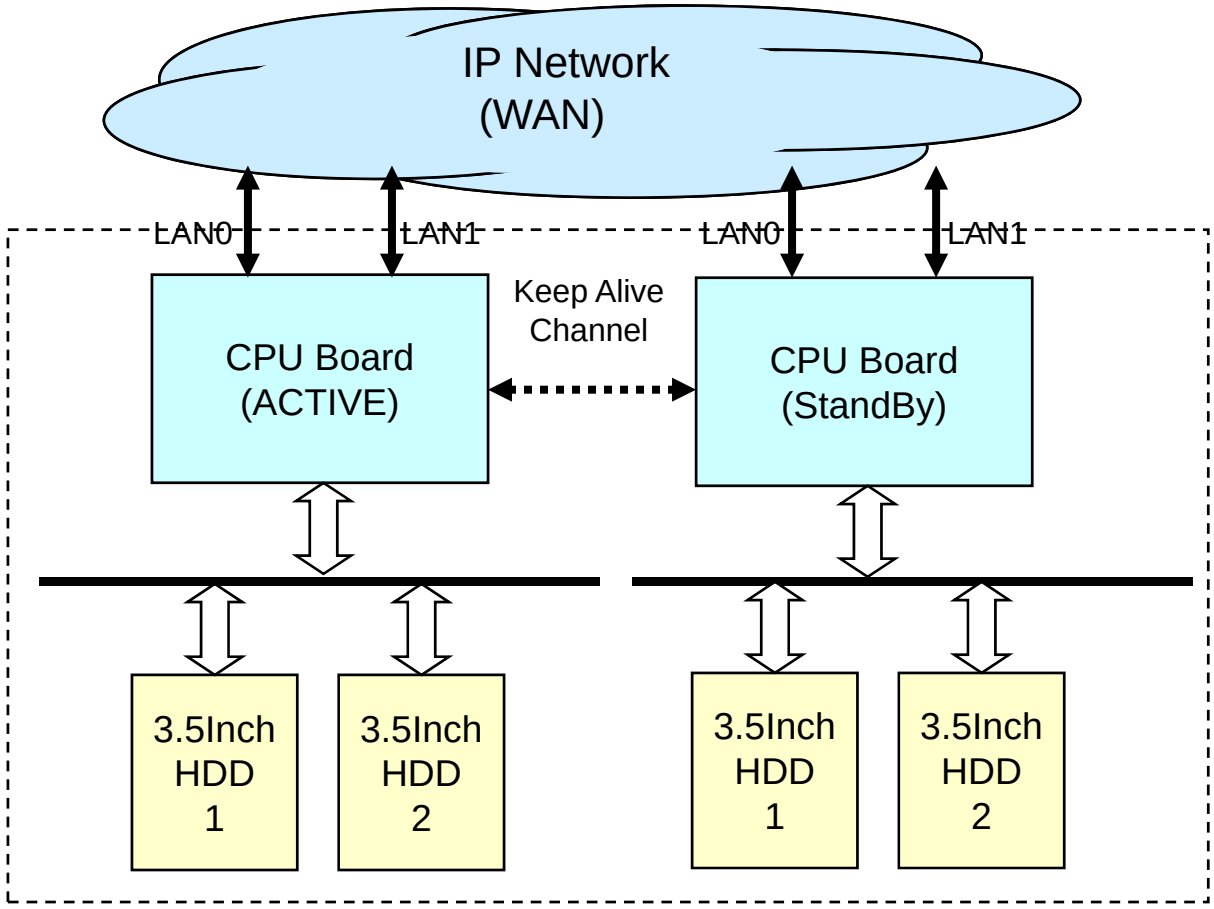
Plug for PSU Module B

Plug for PSU Module A

System Redundancy Features

AP-SNC3000 Smart Sensor Network Controller

AP-SNC3000 System Block Diagram



Smart Sensor Network Controller
AP-SNC2000

Product Overview

AP-SNC2000 Smart Sensor Network Controller

- Embedded H/W Platform with Dual CPU Module Slots
- Fault Tolerant and Reliability Service
- Support Multiple Smart Hub for Zigbee/Zwave sensors
- Support RTSP based Network Video Encoder (Video Codec, IP Camera, etc) Control
- Support RTP based Video Door Phone Control
- Mini Call Manager Function Support for Smart Phone, Tab/PAD registration
- Load Balance using RTSP Redirect Service
- Web Server Function for Smart Tab, Smart Phone Appl.

Benefits and Features

AP-SNC2000 Smart Sensor Network Controller

- Multiple Smart Hub Support for Zigbee/Zwave sensors
- RTP based Video Door Phone Support
- RTSP based Network Video Encoder Support
- TCP/UDP Transport Protocol Support
- Two(2) Module Slots for Embedded Sensor Control Service Module
- Fault Tolerant and High Reliability Service using Dual CPU Module
- Load Balance and Hot-Swap Service
- Compact Size and Low Power Consumption compare with Commercial Server
- IP based Network Protocol Support
- Smart Tab, Smart Phone Appl. Support for Sensor Control, Network Camera, Video Door Phones.
- Mini Call Manager Support for Standard SIP based Smart Phone Application Services

Hardware Specification

AP-SNC2000 Smart Sensor Network Controller

High-end RISC

- High-end Programmable RISC Hardware Architecture
- Two(2) Module Slots for Redundancy and Load Balance
- Smart Sensor Network Control Module (AP-SNCM)
  - Network Interface
    - Two(2) 10/100/1000Mbps Gigabit Ethernet
    - One(1) Console Port



Hardware Specification

AP-SNC2000 Smart Sensor Network Controller

High-end
RISC

AP-SNC2000 Front View



Sensor Network Controller Module

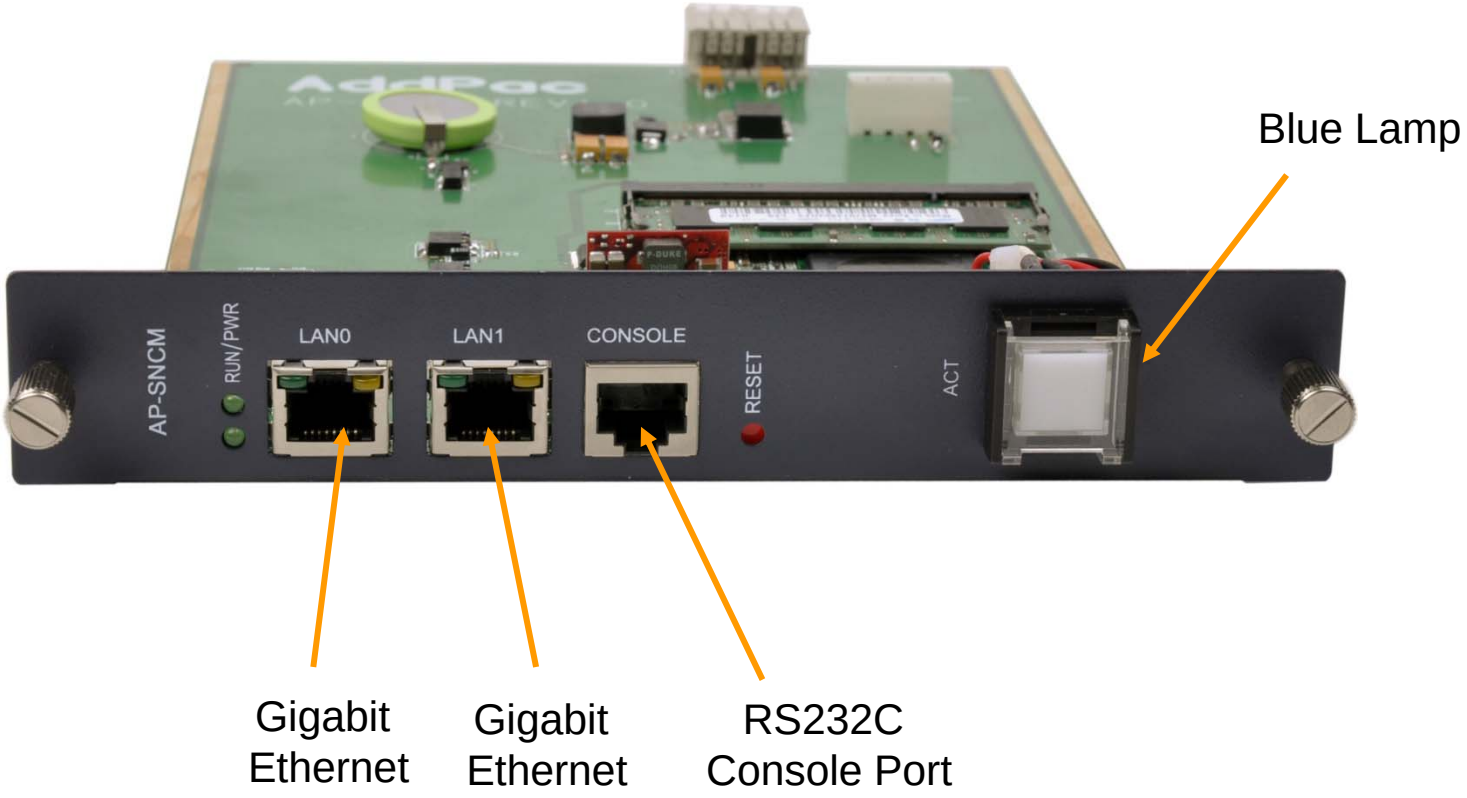


Hardware Specification

AP-SNC2000 Smart Sensor Network Controller

High-end RISC

AP-SNCM Sensor Network Control Module



Thank you!

AddPac Technology Co., Ltd.
Sales and Marketing

Phone +82.2.568.3848 (KOREA)
FAX +82.2.568.3847 (KOREA)
E-mail sales@addpac.com