Secure IP Video Door Phone
(TLS/SRTP Protocol)



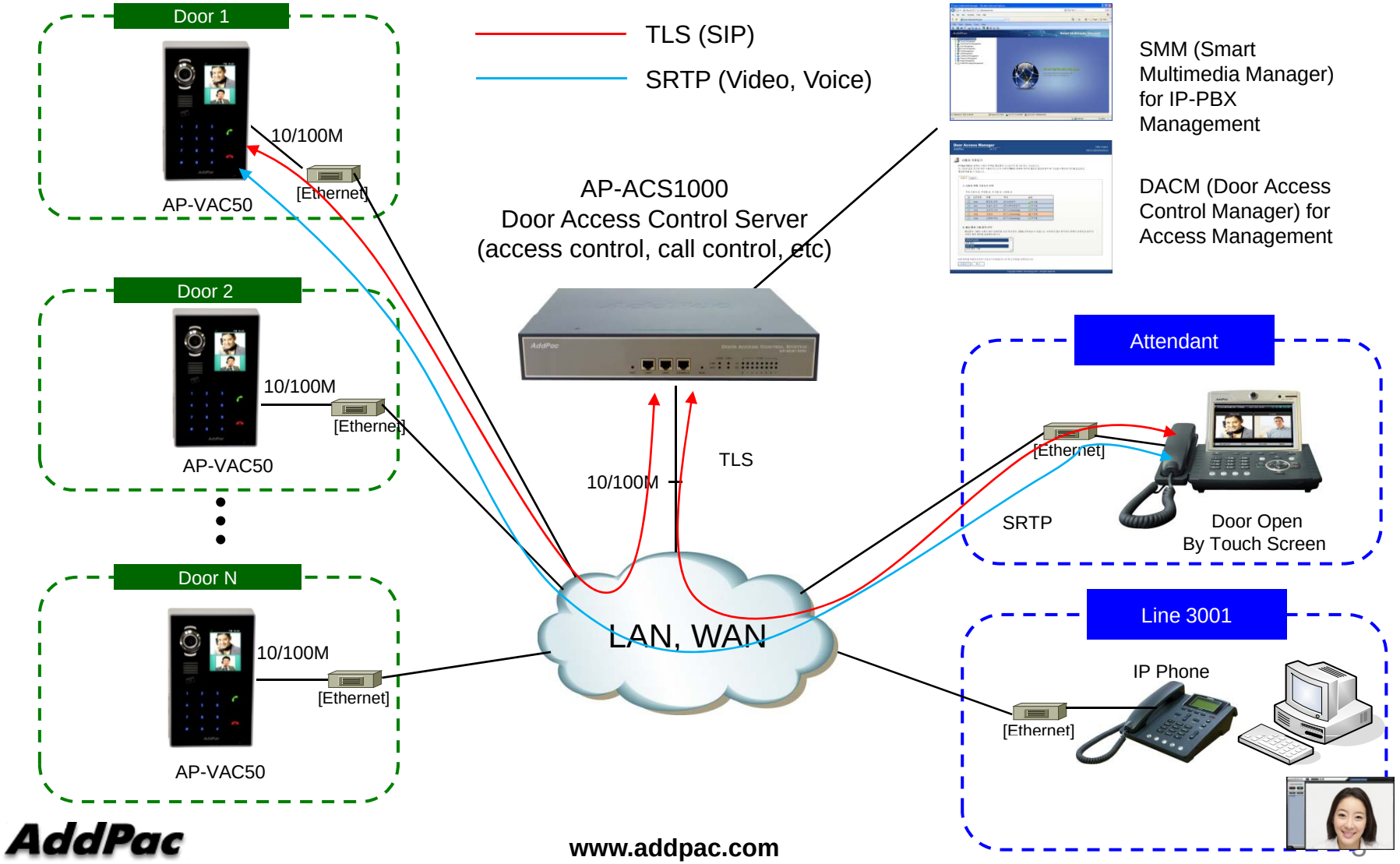
AddPac Technology

Sales and Marketing

Contents

- Secure IP Video Door Phone Service Diagram
- Secure VoIP Protocol & Algorithm (TLS & SRTP)
- AddPac Secure IP Video Door Phone Solution Components
  - Secure IP Video Door Phone Solution
  - Secure ACS (Access Control Server) Solution
  - Secure IP Video Phone Solution

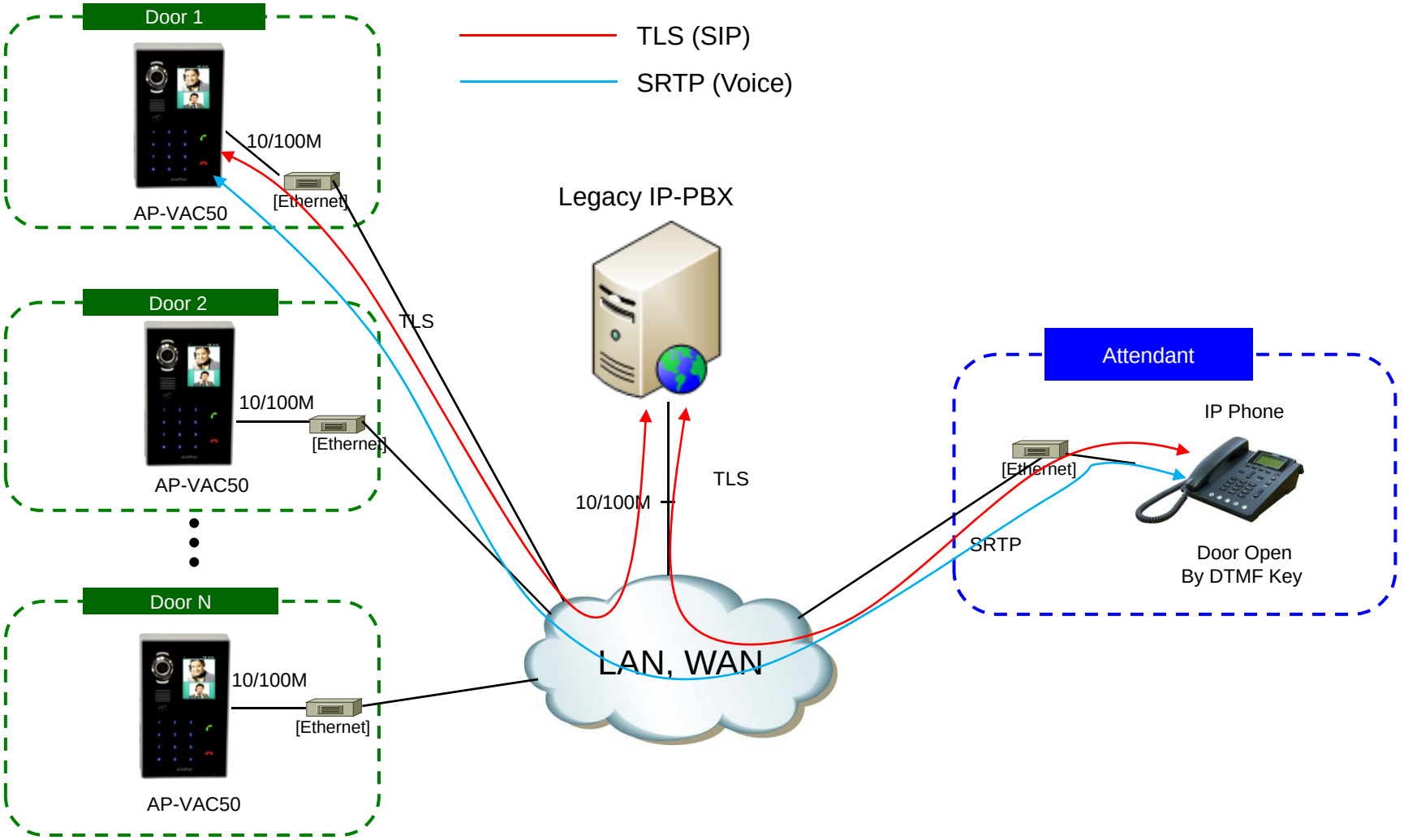
Secure IP Video Door Phone Service (AddPac Total Solution)



AddPac

www.addpac.com

Secure IP Door Phone Service (Voice Only)

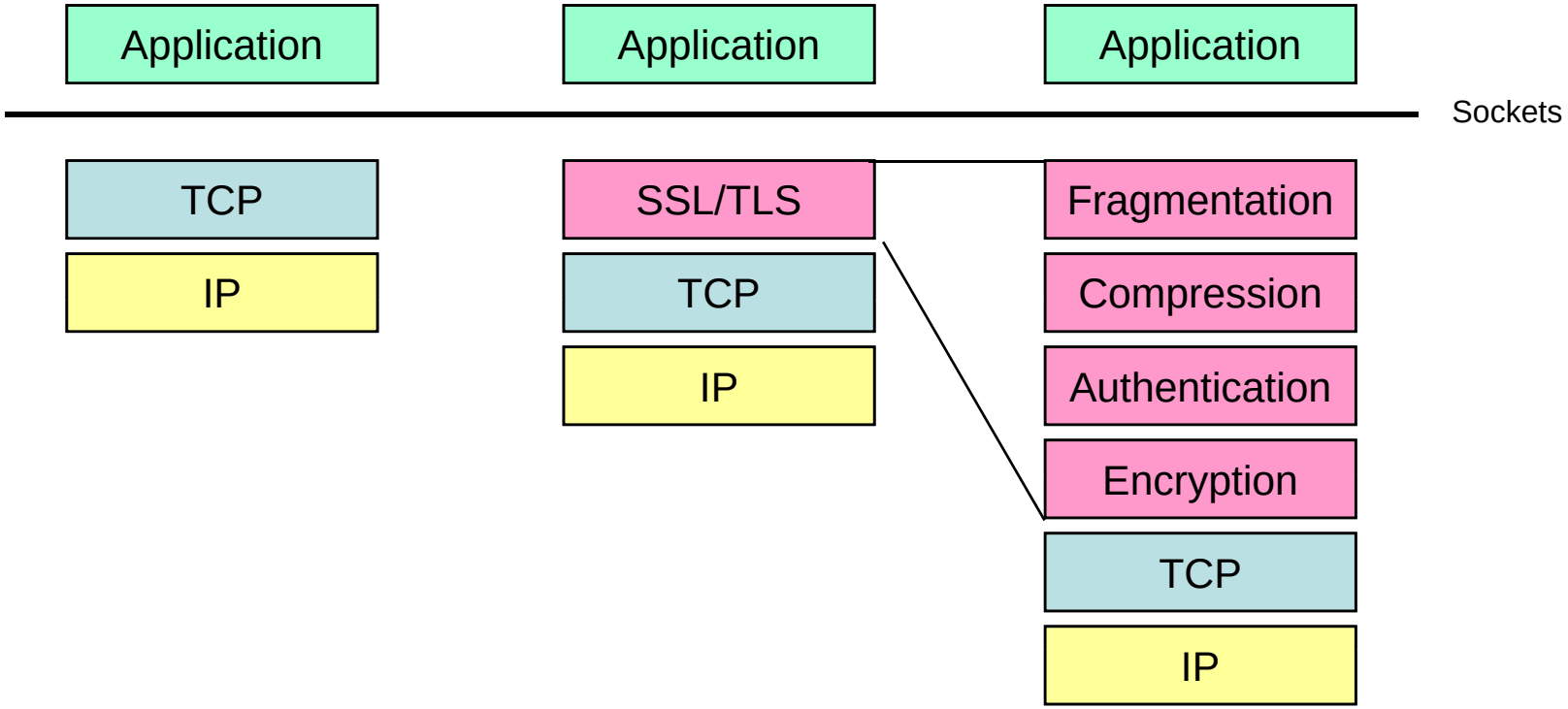


Secure IP Video Door Phone Service Features

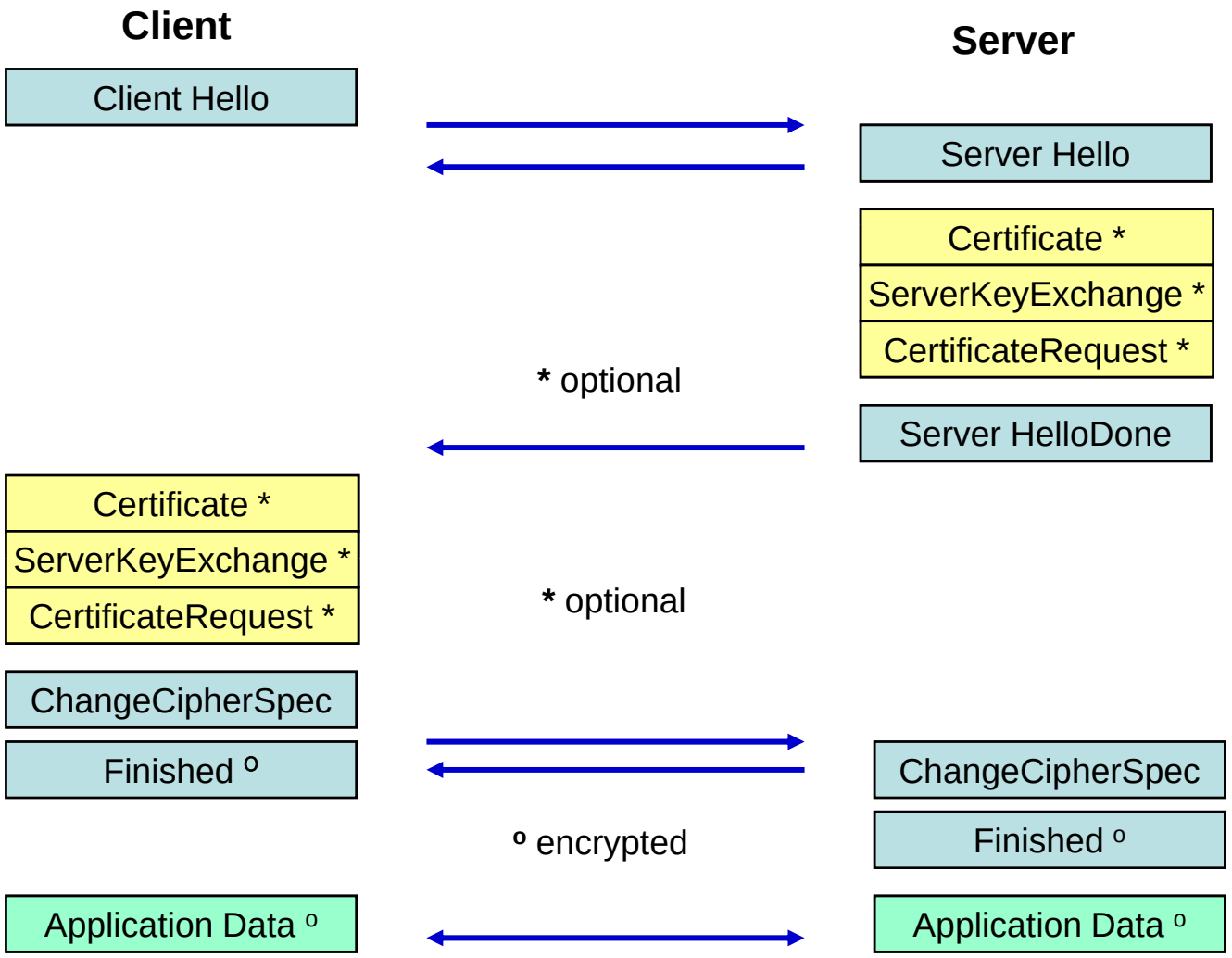
TLS Features for Secure VoIP Service

- 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



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

SRTP (Secure Real-time Transport Protocol) Features

- RFC4568, Standards Track, Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 3711, Proposed Standard, The Secure Real-time Transport Protocol (SRTP)
- RFC 3551, Standard 65, RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3550, Standard 64, RTP: A Transport Protocol for Real-Time Applications
- RFC 2104, Informational, HMAC: Keyed-Hashing for Message Authentication
- Cipher Algorithm : ARIA, SEED, AES, DES(*), 3DES(*)

* Support at AddPac Specific SRTP

Secure IP Video Door Phone Solution (TLS/SRTP Protocol)

IP Video Door Phone Comparison Table

Model Service Features	AP-VAC100 	AP-VAC50 
Duplex (Voice)	Full Duplex	Full Duplex
Key Pad	3x4 Key Support	3x4 Key Support
LCD	3.5 Inch	2inch LCD
RF Card	Support	Support
Camera Sensor	SD(VGA)	SD(VGA)
Video Codec	SD, H.264/MPEG4	SD, H.264/MPEG4
Voice Codec	G.711	G.711
Signaling	H.323/SIP	H.323/SIP
Secure VoIP Service (TLS,SRTP)	Support	Support
MIC & Speaker Phone	Support	Support
LAN Port	1	1
PoE(Option)	Support	Support

AP-VAC50 IP Video Door Phone
(Secure Service Enabled)



Product Overview

AP-VAC50 IP Video Door Phone

- High Performance IP Video Door Phone Solution
- Video Camera, 3x4 Key, TFT Color LCD, Internal MIC & Speaker
- High Quality 2.4 Inch LCD, 320 x 240 Video Resolution
- SIP VoIP Signaling Stack Embedded
- TLS, SRTP Protocol Support for Secure IP Video Door Phone Service
- High-performance Video/Voice Codec Support
  - H.264/MPEG4, G.711, etc
- One(1) 10/100Mbps Fast Ethernet
- PoE(Power over Ethernet) Support
- High Quality Speaker Phone Features
- Powerful Acoustic Echo Canceller Chip Embedded
- Powerful Network Protocols (PPPoE, DHCP, Static Routing, etc)
- Firmware Upgradeable Architecture
- Advanced Voice QoS Mechanism

Hardware Specification

AP-VAC50 IP Video Door Phone

RISC CPU

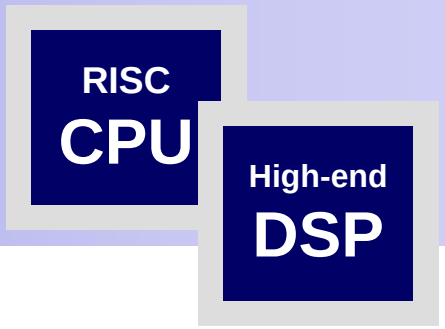
High-end DSP

- RISC+DSP Microprocessor Computing Power
- Audio and Voice Interface
  - Internal MIC
  - Internal Speaker
  - 3 x 4 key PAD
- Video Camera Interface
- TFT Color LCD Interface
  - 2.4 Inch LCD, 320 x 240 Video Resolution
- Network Interface
  - One(1) 10/100Mbps Fast Ethernet
- RF Card Interface
- Alarm & Relay Out Interface (door open, etc)
- RS232/RS485 Interface
- External RCA Audio Line Out and MIC In (back side)
- Power Supply
  - Power over Ethernet (Option)
  - External Power Supply



Hardware Specification

AP-VAC50 IP Video Door Phone



- LCD Controller
  - One-Chip Solution for amorphous TFT-LCD
  - Support resolution up to 240xRGBx320
  - Built-in 172800 bytes internal RAM
  - 6,8,16, and 18-bit RGB Interface
  - Resize Function (x ½, x ¼)
  - On-Chip Power Management System

- Camera
  - High Sensitivity for low-light operation
  - Output support for Raw RGB, RGB, and YCrCb format
  - Image Size : VGA, QVGA, and any size scaling down from CIF to 40x30
  - Support AEC, AGC,AWB, ABF, ABLC
  - Saturation Level, Edge Enhancement Level, De-noise level Auto adjust

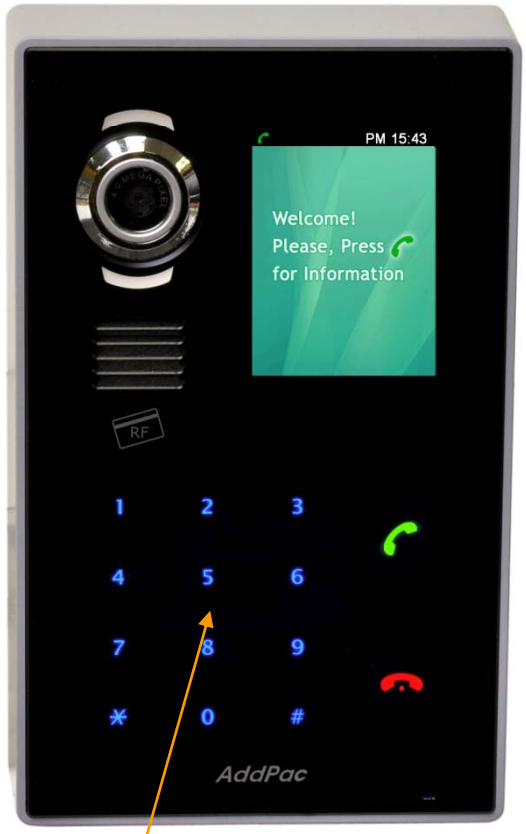
Hardware Specification

AP-VAC50 IP Video Door Phone

RISC CPU

High-end DSP

- RF Card Sensor
  - Protocol Supported
    - ISO14443A/B all bit rates
    - > 106,212,424 and 848 kbps
    - Compatible to MiFare Classic
    - ISO15693 all modes
    - > 1.65/6.6 & 26.5 kbps
    - > Uplink 1 & 2 sub-carrier
  - Receiver
    - Rx Sensitivity down to 1mVrms
    - Rx Automatic Gain Control
    - Accept external baseband signal from external circuitry for frame level processing
    - Integrated signal strength indicator (SSI)
    - On-Chip Framing handler for supported standard
  - Transmitter
    - Typical proximity operating distance up to 100mm.
    - Software configurable modulation index
    - Maximum driving current up to 200 mA/PIN @ 5V
    - Accept external baseband signal for RF modulation
    - Wide Transmitter driver supply range from 2.7~7.0V



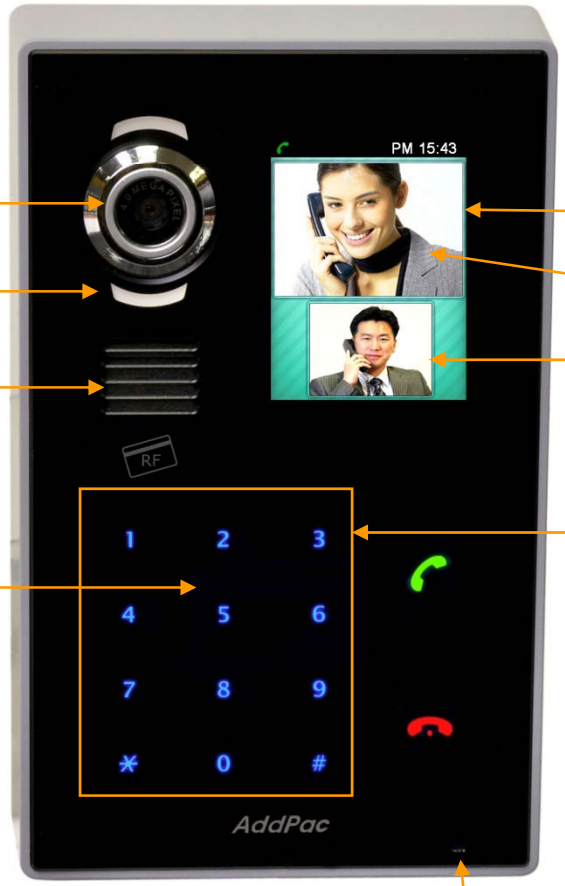
Hardware Specification

AP-VAC50 IP Video Door Phone

RISC CPU

High-end DSP

Front Side



Video Camera

LED Side Light

Internal Speaker

RF Card Sensor

TFT LCD Display

Remote Image Size : 240x160

Local Image Size : 160x120

3 x 4 Dial Key

Internal MIC Input

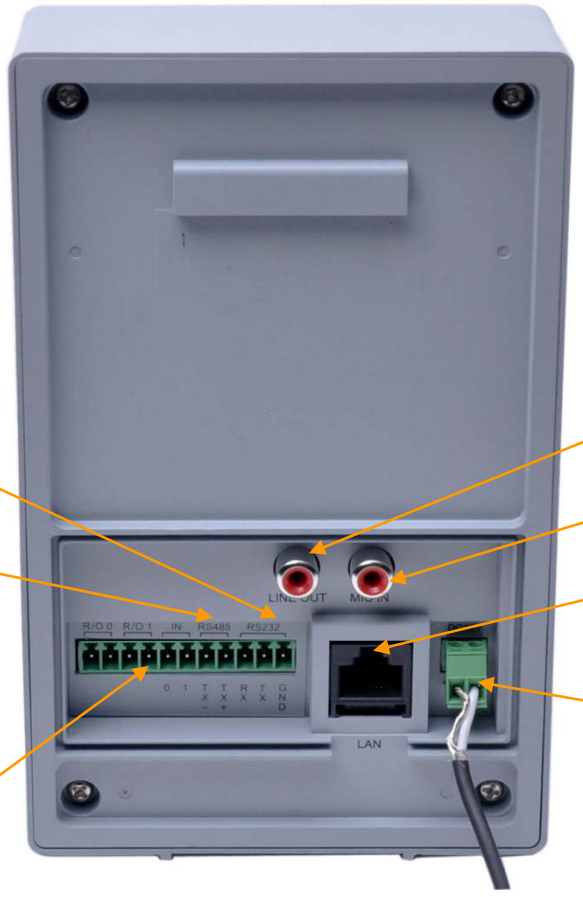
Hardware Specification

AP-VAC50 IP Video Door Phone

RISC CPU

High-end DSP

Back Side



RS485

RS232

2 Alarm,2 Relay Out

Option : Line Out

Option : MIC In

LAN Port

Power Input : Terminal Block
12V 1A

Secure ACS(Access Control System) Solution (TLS/SRTP Protocol)

Door Access Control Server Comparison Table

Model / Service Features		AP-ACS1500 	AP-ACS1000 
Registration User Number		200	100
Concurrent Call User Number		50	30
VoIP Signaling	Internal	SIP	SIP
	External	H.323/SIP	H.323/SIP
Powerful IVR, UMS, Media Service, User Presence Service		Support	Support
RTP Proxy Service (IPv6, Private IP)		Support	Support
System Duplication		Internal	External
Power Supply Duplication		Dual Power	Single Power
Secure IP Telephony Service (TLS, SRTP)		Support	Support
LAN Port		2	2
VoIP Module Slots for PSTN		N/A	2 Slots
VoIP Interface		N/A	FXS,FXO,E1/T1
Video Door Phone Control (RF card, etc)		Support	Support
Time & Attendance Management		Support(option)	Support(option)

AP-ACS1500
Door Access Control Server



Main Features

AP-ACS1500 DACS (Door Access Control System)

- Door Access Control Application System + Call Manager
- SIP Application Server, Proxy, Registrar and Location Server
- TLS, SRTP Protocol Support for Secure Call Manager Service
- Multiple ITSP Trunk with SIP & H.323 Accounts Support
- High Performance RISC Architecture
- Smart Multimedia Manager for Call Manager
- DACM(Door Access Control Manager) for IP Door Phone Control (RF Card, Fingerprint Module, etc)
- IPv4/IPv6 based Dual Network Protocol Support
- Fault Tolerant and Scalability Architecture
- Firmware Upgradeable Architecture
- Dual System Redundancy Architecture
  - Two(2) Fast Ethernet Interface / System
- Dual Redundancy Power

Hardware Features

AP-ACS1500 DACS (Door Access Control System)

- High-End Microprocessor Computing Power
- Main Chassis
  - Dual Redundancy CPU Boards for System Fault Tolerant
    - Two(2) 10/100Mbps Fast Ethernet
    - One(1) RS-232C Console (RJ45)
  - Dual Redundancy Power Supply
  - Hot-Swap Features

Hardware Specification

AP-ACS1500 DACS (Door Access Control System)

AP-ACS1500 Front Side



Hardware Specification

AP-ACS1500 DACS (Door Access Control System)

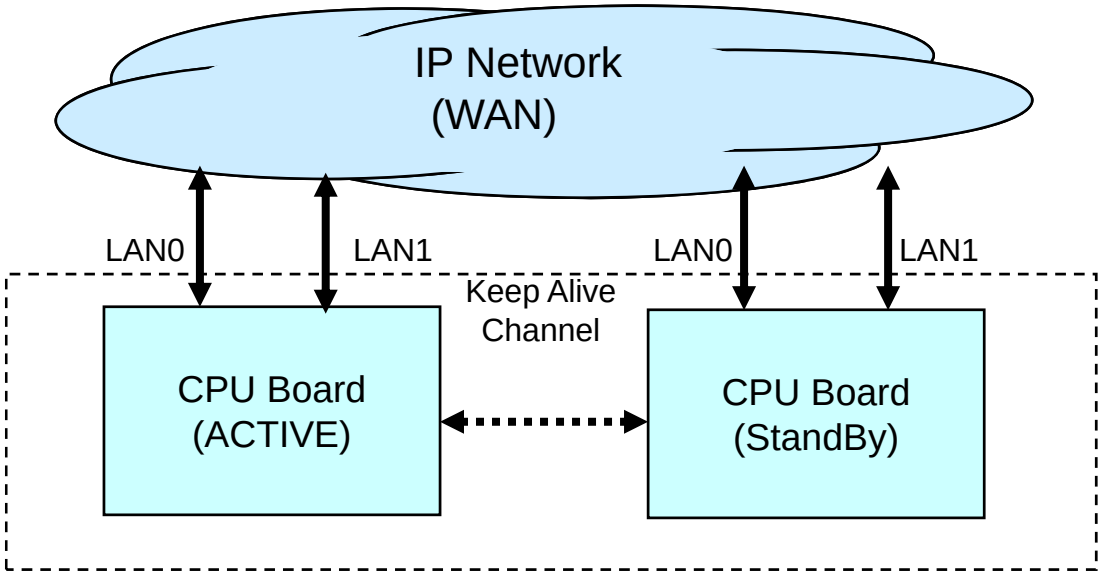
AP-ACS1500 Back Side



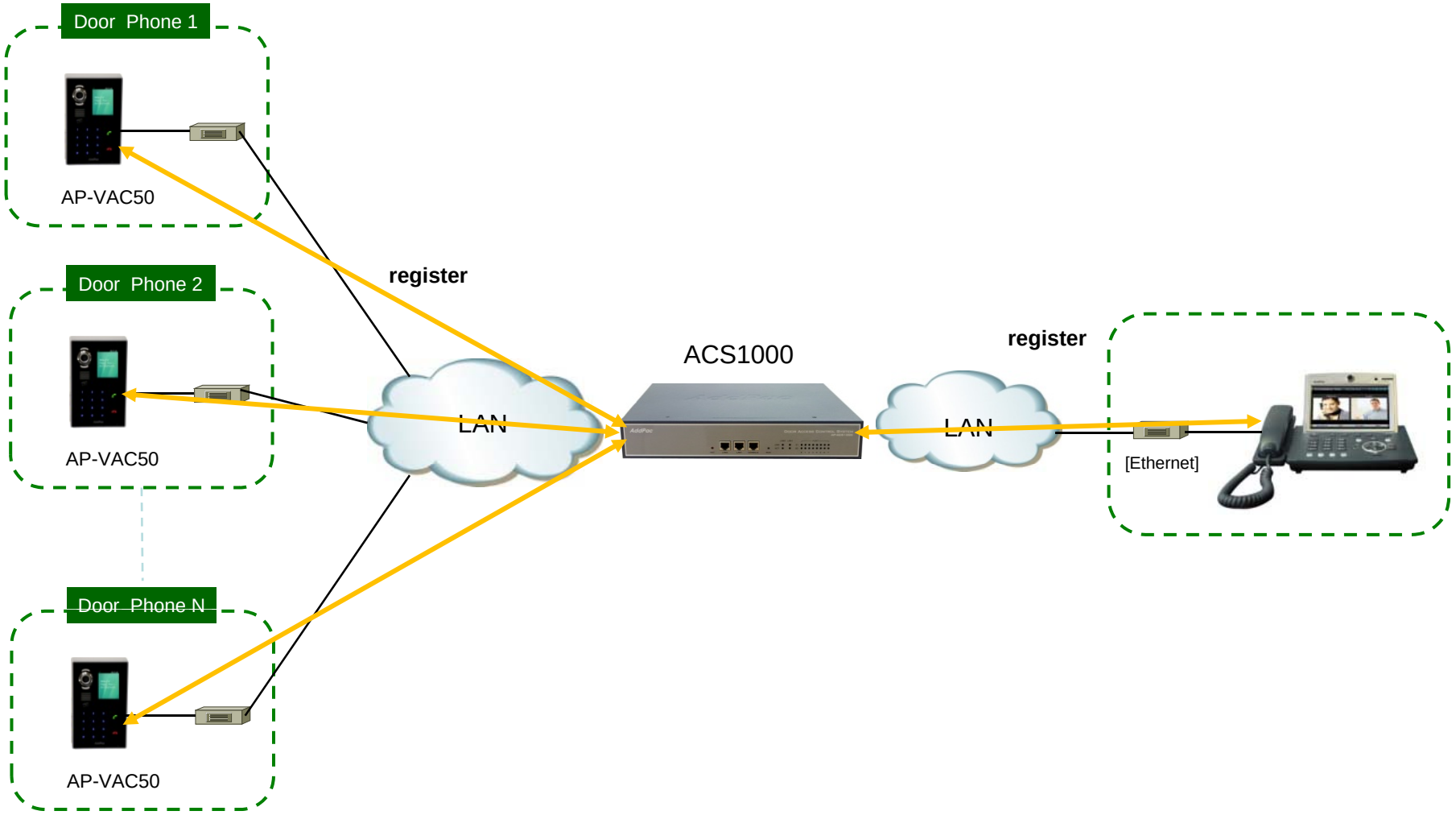
System Redundancy Features

AP-ACS1500 DACS (Door Access Control System)

System Block Diagram

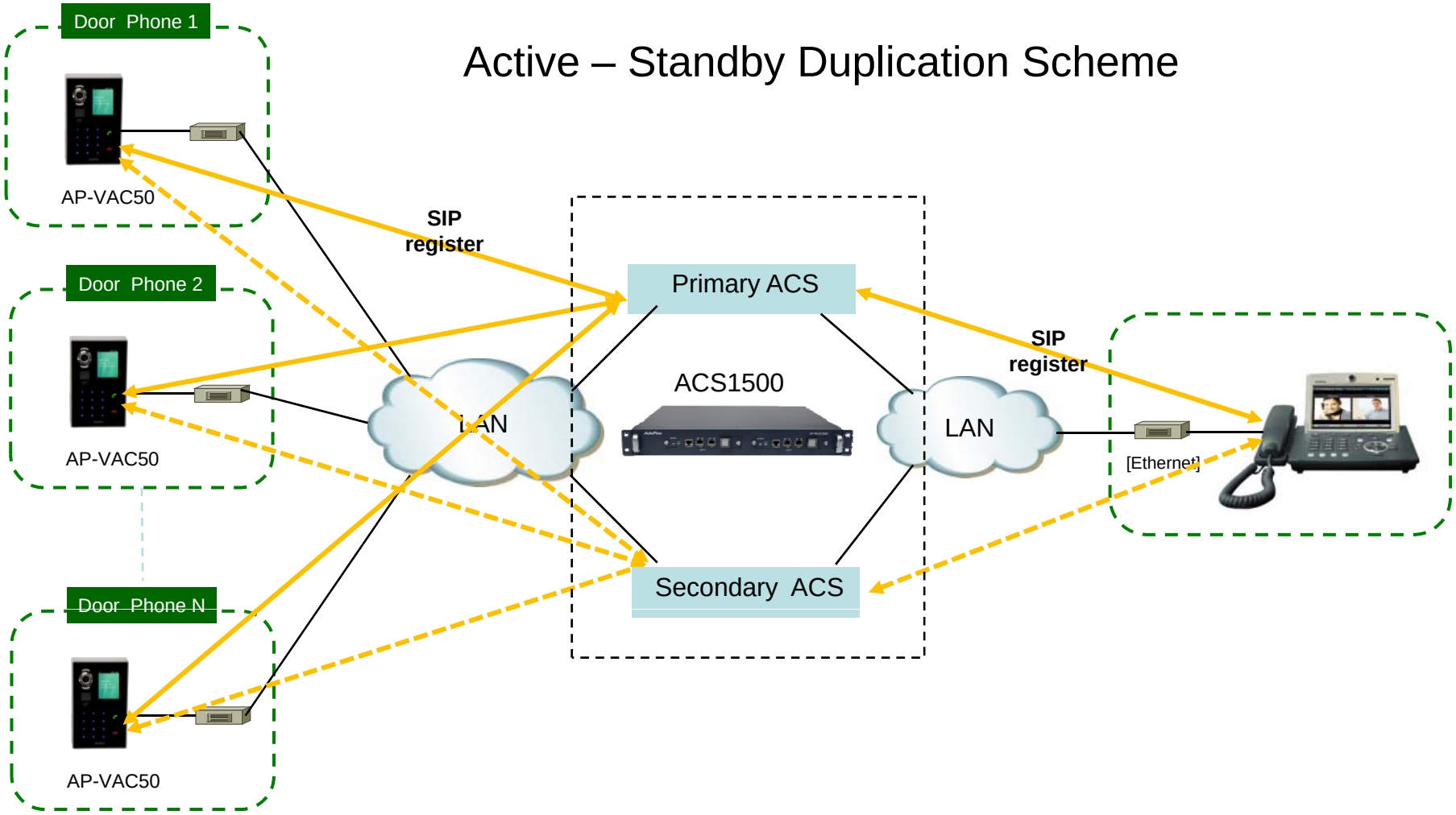


ACS Network Diagram



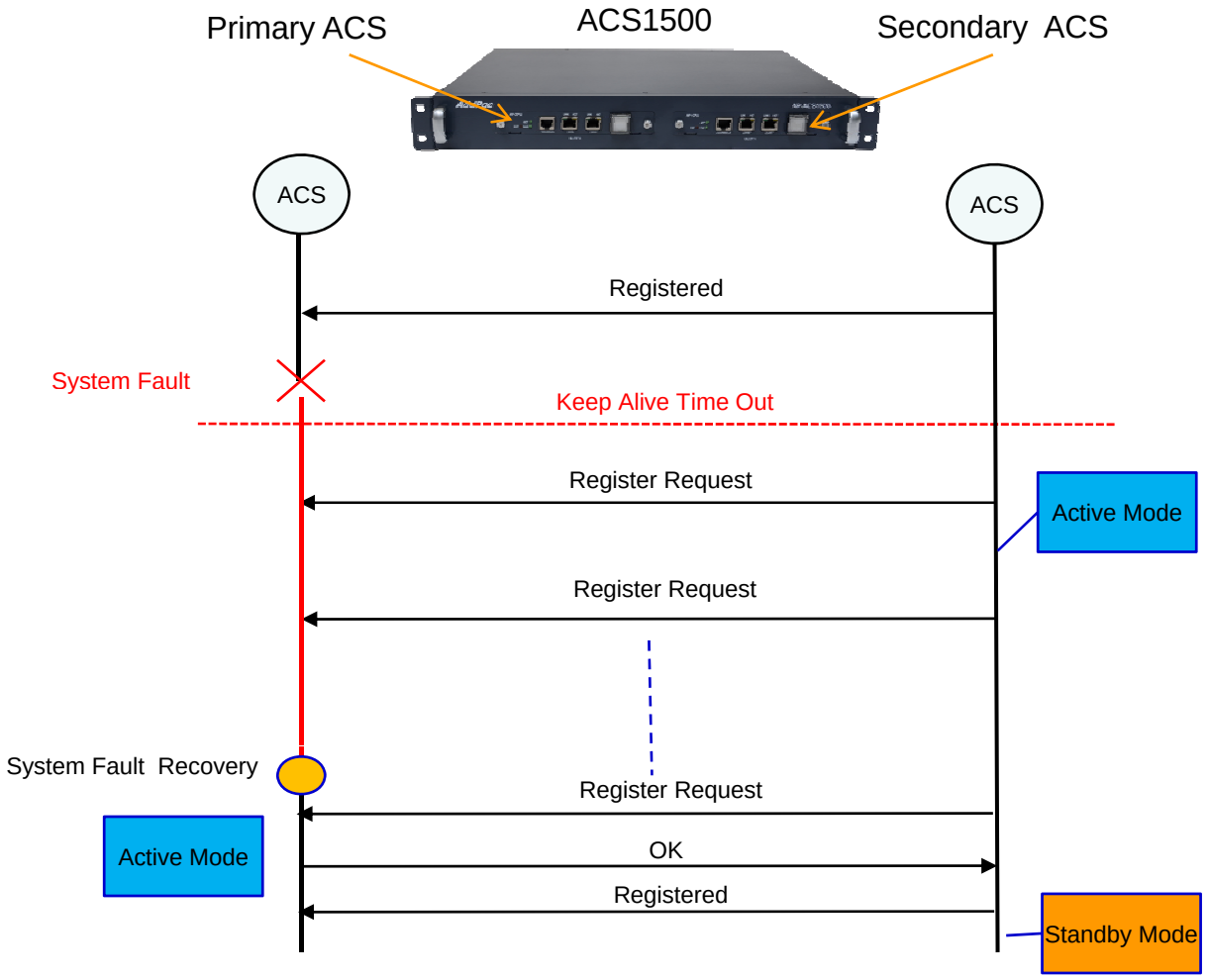
ACS Redundancy Scheme Network Diagram

- Call Manager Function



ACS Redundancy Scheme Network Diagram

- Door Access Control Function



Secure IP Video Phone Solution (TLS/SRTP Protocol)

Secure IP Video Phone Comparison Table

	AP-VP700	AP-VP500	AP-VP300N	AP-VP280
				
LCD Size	12.1 Inch Touch Screen	12.1 Inch Touch Screen	7Inch Touch Screen	7Inch Touch Screen
Camera	HD CCD	HD CCD	CCD	CMOS
Video Codec Resolution	HD	SD	SD	SD
Video Codec	H.263 MPEG4 H.264	H.263 MPEG4 H.264	H.263 MPEG4 H.264	H.263 MPEG4 H.264
Signaling	H.323/SIP	H.323/SIP	H.323/SIP	H.323/SIP
Security Protocol	TLS/SRTP	TLS/SRTP	TLS/SRTP	TLS/SRTP
Voice MCU	3-Party	3-Party	3-Party	3-Party
LAN Port	2 (GE)	2 (FE)	2 (FE)	2 (FE)
PoE	N/A	N/A	Support	Support

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