



AP1950S

Secure VoIP Gateway

High Performance Secure VoIP Gateway Solution

Product Overview



AddPac

AddPac Technology

Sales and Marketing

www.addpac.com

Contents

- Product Overview
- Hardware Specification
- APOS Technology
- VoIP (Voice over IP) service
- TLS/SRTP Secure VoIP Service
- Advanced QoS Features
- Network Protocols
- Network Management
- Security Management
- Application Service
- Ordering Information

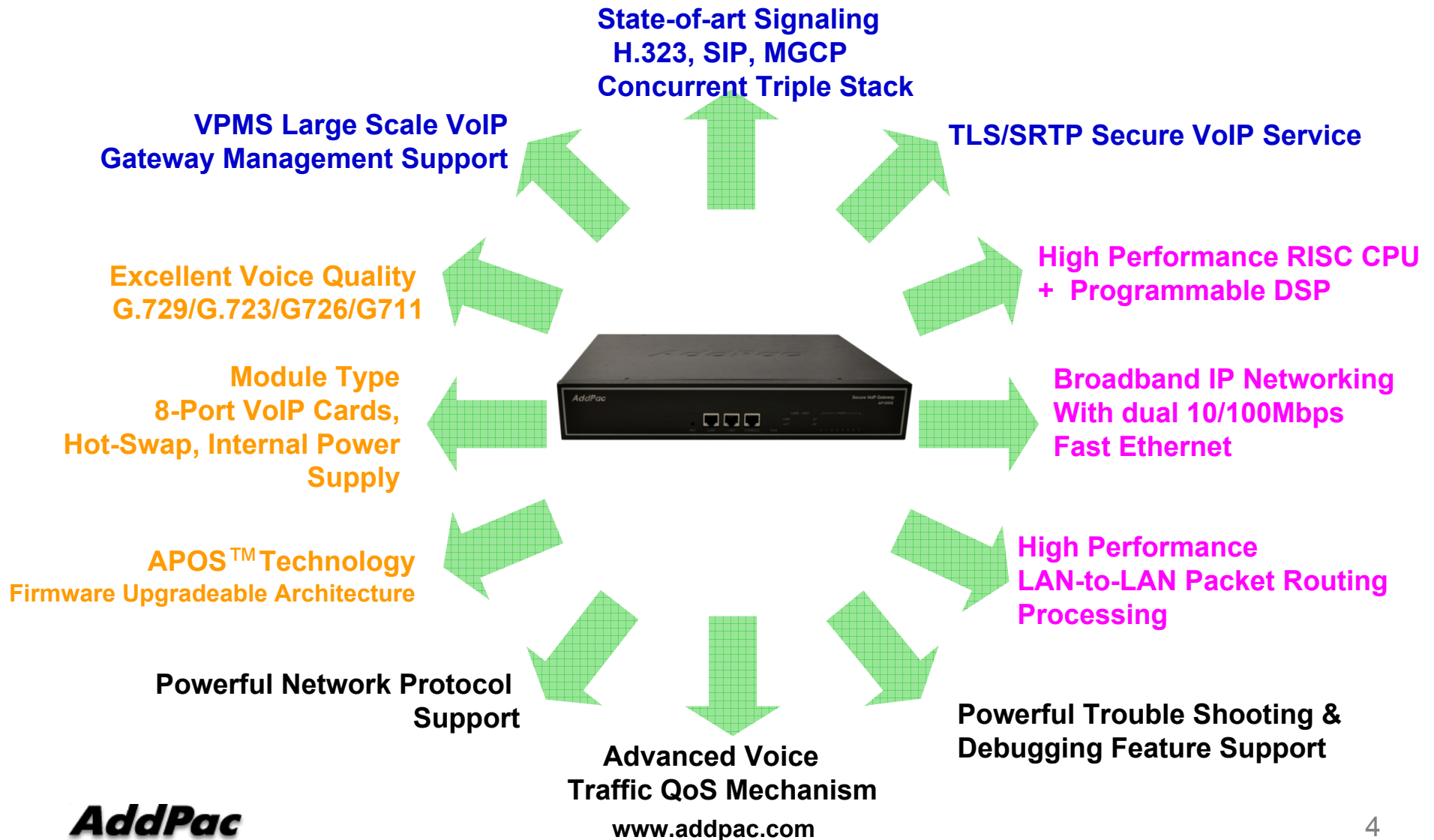
Product Overview

AP1950S Secure VoIP Gateway

- H.323/SIP/MGCP Triple Concurrent Stack Embedded
- High Performance RISC & Programmable DSP Architecture
- Secure VoIP Service (SRTP, TLS, etc)
- Up to 2E1/T1 Secure VoIP Performance
- Two(2) 10/100Mbps Fast Ethernet (IP Share ,etc)
- High Performance LAN-to-LAN Routing Capability
- G.711/G.726/G.723/G.729, T.38 Fax , VAD, etc
- Powerful Network Protocols (PPPoE, DHCP, Static Routing, etc)
- Firmware Upgradeable Architecture
- VPMS (VoIP Plug&Play Management System) for Large Scale Deployment
- Advanced Voice QoS Mechanism
- Light and Compact Design with Internal Power Supply
- Two(2) VoIP Module Slot

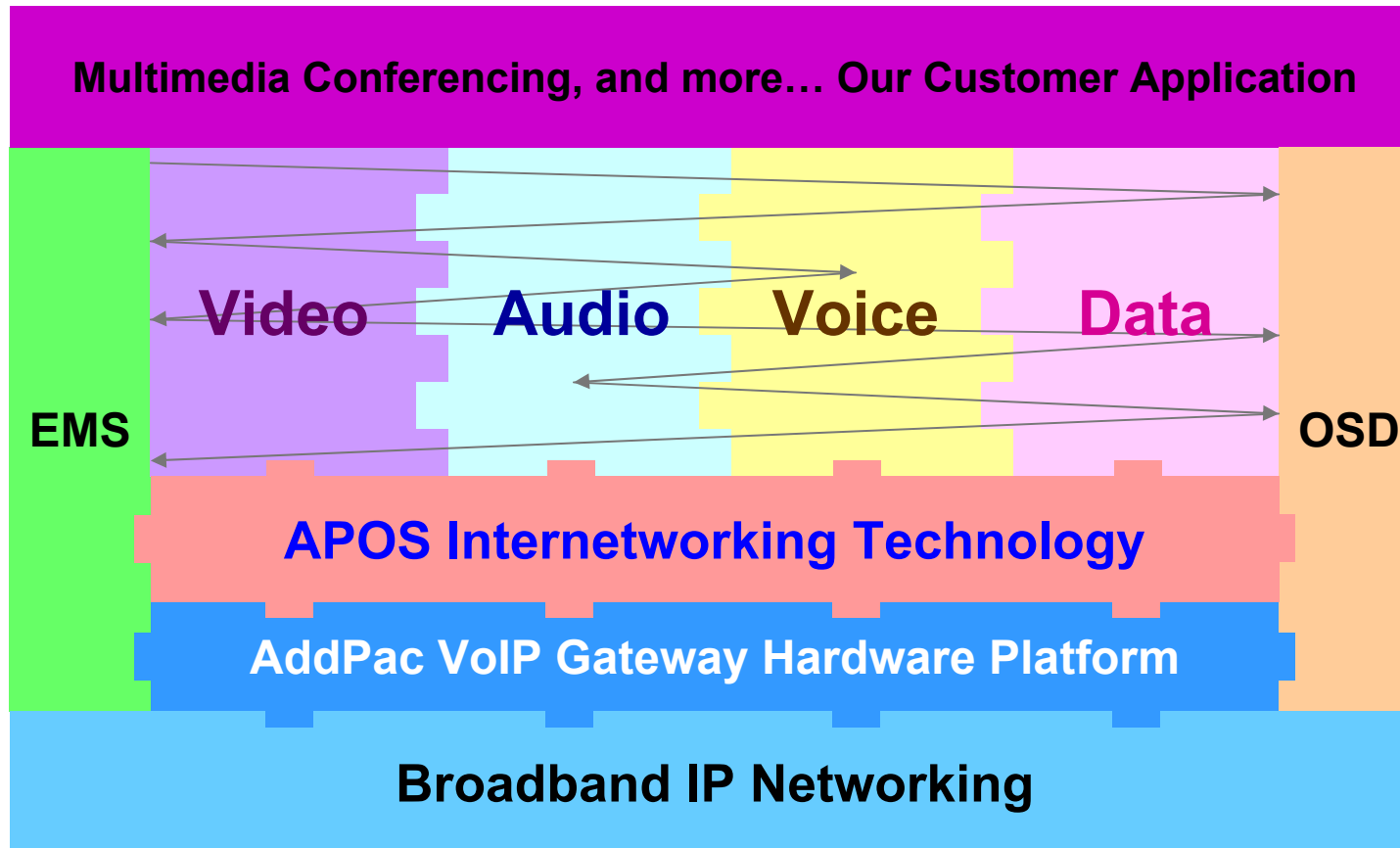
Product Highlights

AP1950S Secure VoIP Gateway



APOS Technology

AP1950S Secure VoIP Gateway



- APOS : AddPac Internetworking Operating System
- OSD : On- Screen Display
- EMS : Element Management System

Hardware Specification

AP1950S Secure VoIP Gateway

RISC
CPU

High-end
DSP

- **RISC Microprocessor Computing Power**
- **Up to 16 Port Analog VoIP Gateway**
- **Two(2) VoIP Module Slots (Hot-Swap)**
 - 8-Port FXS Card, 8-Port FXO Card, 4-Port FXS 4-Port FXO Card, 1-Port Digital E1/T1 Card, 2-Port Digital E1/T1 Card
- **Network Interface**
 - Two(2) 10/100Mbps Fast Ethernet (RJ45)
- **RS232C Console Interface**
- **Run LED, LAN LED, Port LEDs**
- **Internal Power Supply**

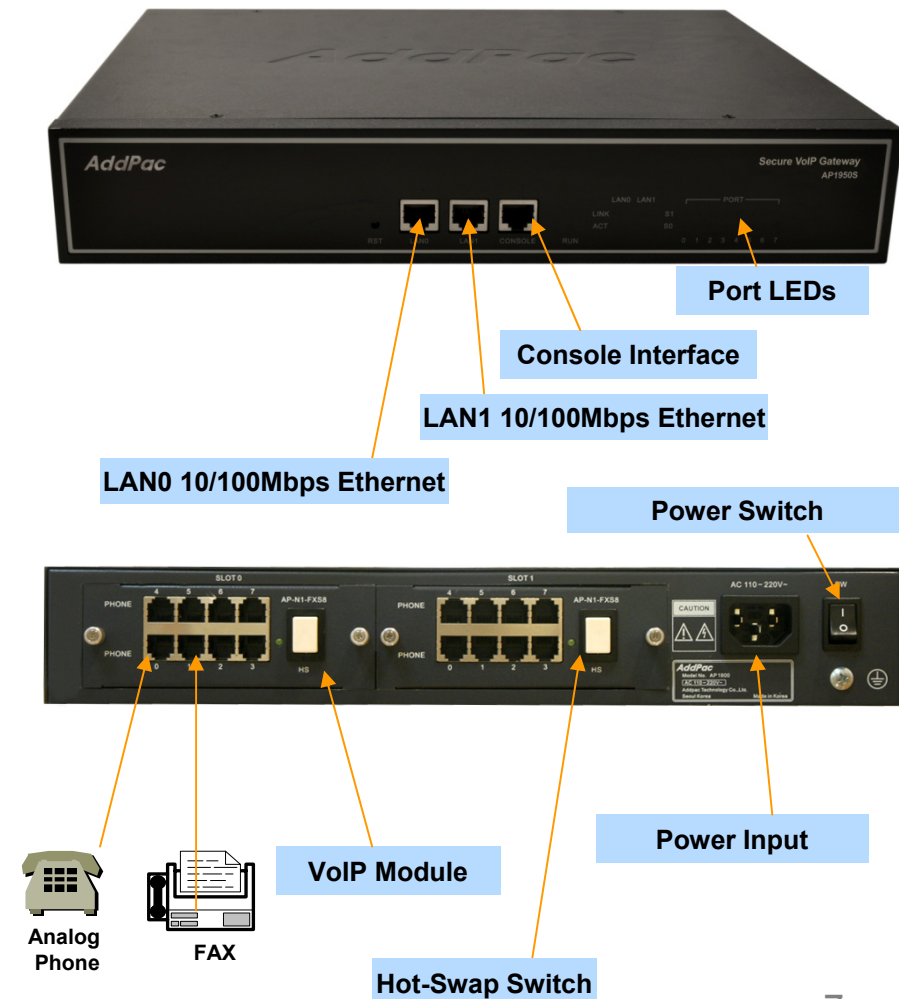
Hardware Specification

AP1950S Secure VoIP Gateway

Hardware Specifications

AP1950S VoIP Series	Basic Specifications
Voice Interface	Two(2) VoIP Module Slots AP-N1-FXS8, AP-N1-FXO8, AP-N1-FXS4O4, AP-N1-E1, AP-N1-2E1
Ethernet Interface	2-Ports 10/100Mbps Ethernet Interface(RJ-45)
Flash Memory	128 Mbyte High-speed Flash Memory
Base Memory	128 Mbyte High-speed DDR Memory
Power Requirement	Power Supply Adaptor / VAC 110~220V, 50/60Hz, 40Watt
Operating Temperature	0°C ~ 45°C (32 °F ~ 122°F)
Storage Temperature	-40°C ~ 85°C (-40°C ~ 185°F)
Relative Humidity	5% ~ 95% (Non-condensing)

Network interface Configurations



Hardware Specification

AP1950S Secure VoIP Gateway

- **VoIP Interface Module**

AP-N1-FXS8 8-Port FXS Module



AP-N1-FXO8 8-Port FXO Module



AP-N1-FXS4O4 4-Port FXS&4-Port FXO Module



AP-N1-E1 1-Port Digital E1/T1 Module



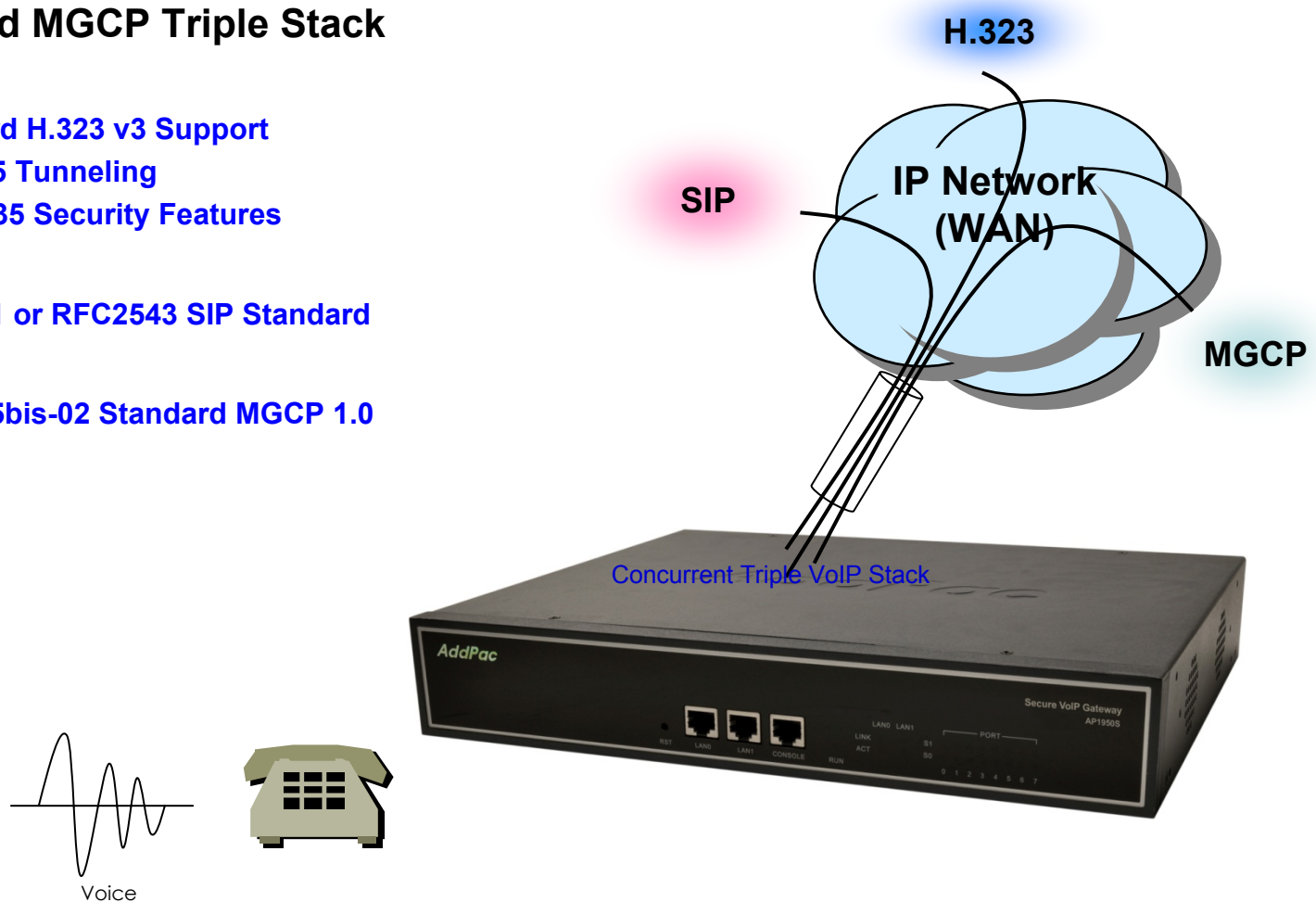
AP-N1-2E1 2-Port Digital E1/T1 Module



VoIP (Voice over IP) Service

AP1950S Secure VoIP Gateway

- **H.323, SIP, and MGCP Triple Stack**
- **H.323**
 - ITU-T Standard H.323 v3 Support
 - Support H.245 Tunneling
 - Including H.235 Security Features
- **SIP**
 - IETF RFC3261 or RFC2543 SIP Standard
- **MGCP**
 - IETF RFC2705bis-02 Standard MGCP 1.0



VoIP (Voice over IP) Service

AP1950S Secure VoIP Gateway

- **H.323**

- Fast connect, normal connect support
- H.245 tunneling support
- Q.931 response message setting for inbound VoIP calls
- H.245 logical channel open timing selection function
- Start H.245 procedure support
- DTMF / Hook flash relay with H.245 alphanumeric / signal
- Secondary gatekeeper support
- Gatekeeper assignment according to the domain name
- Gatekeeper discovery with multicast
- Lightweight RRQ support
- Signaling TCP port assignment
- Resource threshold setting with RAI
- H.235 clear-token, crypto-token support
- canMapAlias support
- Technical prefix (supported prefix) support
- Public IP assignment in NAT environment

- **SIP**

- Gateway-based / Endpoint-based registration support
- Secondary proxy-server assignment function
- SIP signaling port change function
- SIP proxy server assignment according to the domain name
- T.38 real-time fax relay support
- DTMF relay support with RFC2833 / OPTION message
- Re-INVITE support

- **MGCP**

- Secondary call agent assignment function
- Default package assignment
- Announcement Server Package, Generic Media Package, Handset Package, Line Package, Trunk Package support
- MGCP call agent assignment according to the domain name
- T.38 real-time fax relay support
- DTMF relay support based on RFC2833

VoIP (Voice over IP) Service

AP1950S Secure VoIP Gateway

- **Voice Codec**

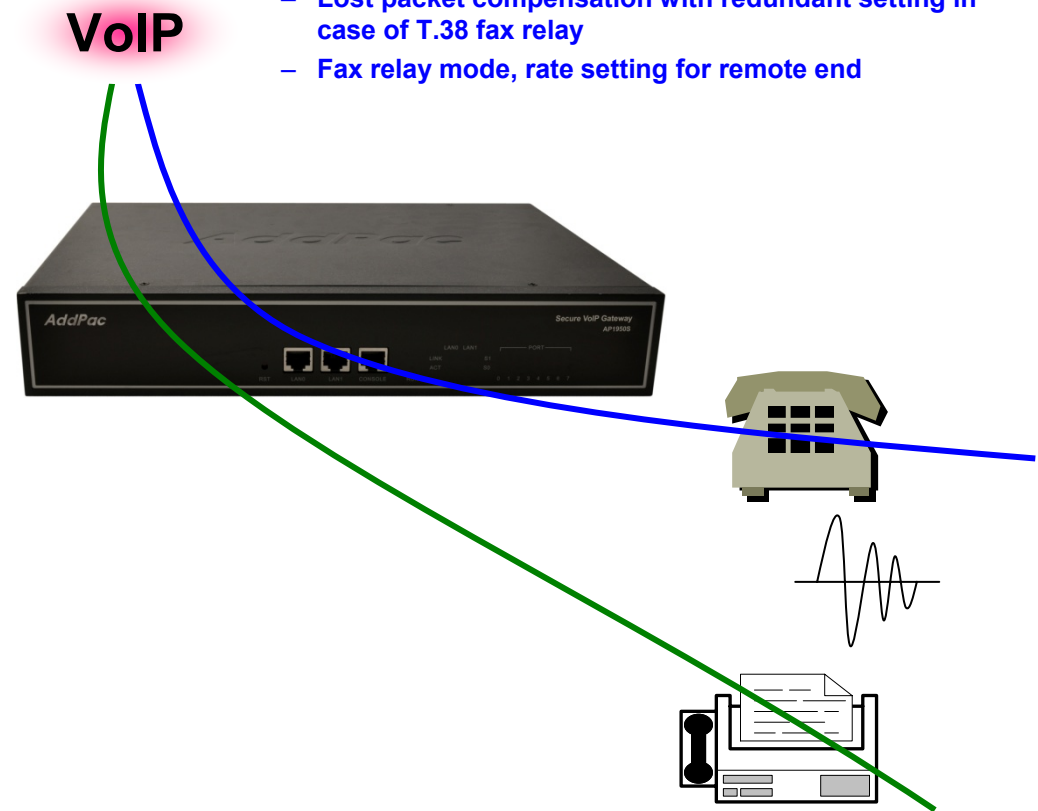
- G.711 A-Law, G.711 U-Law
- G.726 r16, G.726 r32
- G.729A
- G.723.1 r63, G.723.1 r53
- VAD (Voice Activity Detection) function support
- DTMF relay support (H.323, SIP, MGCP common) based on RFC2833

- **RTP**

- Redundant RTP packet transmission in case of severe packet loss
- Dynamic jitter buffer management and RTP packet jitter and loss compensation with heuristic & DSP error concealment
- Static jitter buffer setting support
- Voice frame per RTP packet number control for each codec
- In-band ring-back tone support
- Virtual ring-back tone support
- Tone parameter change support

- **FAX**

- Fax relay mode supporting T.38, inband-T.38, bypass mode
- Lost packet compensation with redundant setting in case of T.38 fax relay
- Fax relay mode, rate setting for remote end



VoIP (Voice over IP) Service

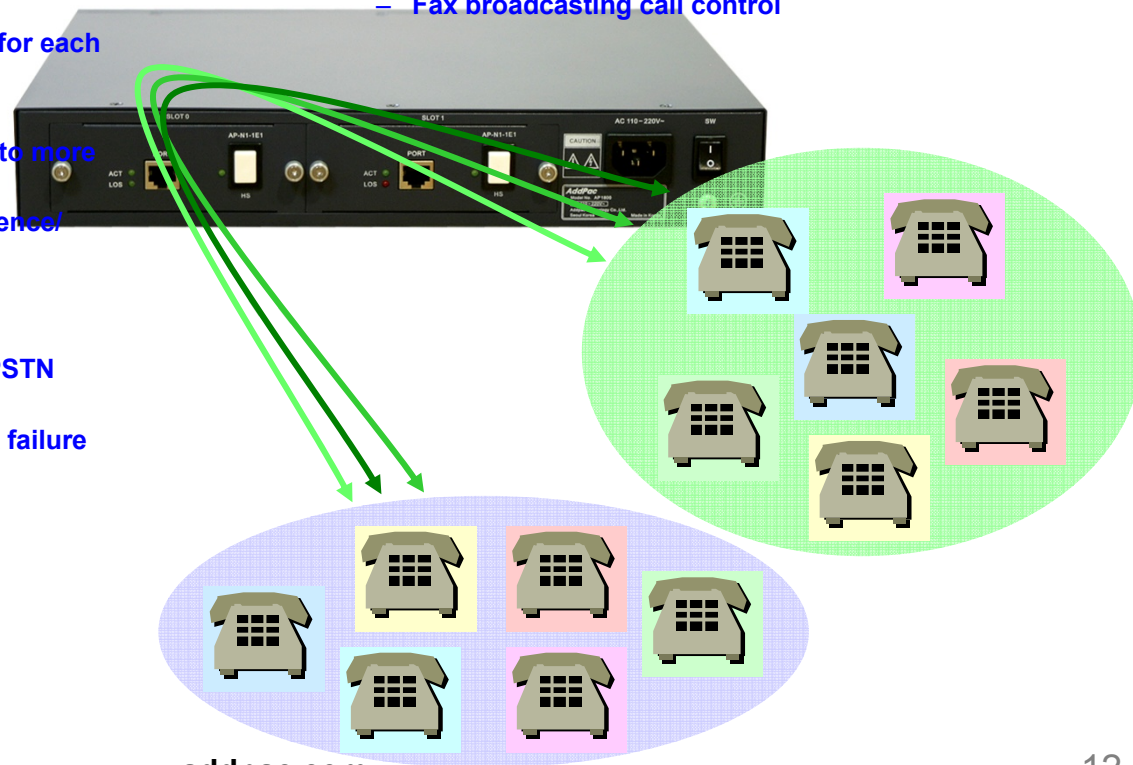
AP1950S Secure VoIP Gateway

• VoIP Call Controls

- Hot line connection function with PLAR (Private Line Auto Ring Down)
- Leased line emulation function
- Connection monitoring function
- Fault tolerant with Redundancy and Call Distribution among Gateways for load balancing
- Call attempt with IP address
- H.323, SIP, MGCP inbound call connection for each voice port
- Multiple E.164 setting for one voice port
- One E.164 or digit pattern can be assigned to more than one voice port
- Hunting with Longest match/ priority/ sequence/ random
- One stage call setup by Digit forwarding
- Call barring with specific digit patterns
- Calling and called number conversion for PSTN outbound calls
- PSTN rerouting in case of VoIP call attempt failure

• VoIP Call Controls (cont.)

- Call transfer for internal calls
- Call pickup for internal calls
- Calling and called number conversion for VoIP outbound calls
- Calling and called number conversion for VoIP inbound calls
- Fax broadcasting call control



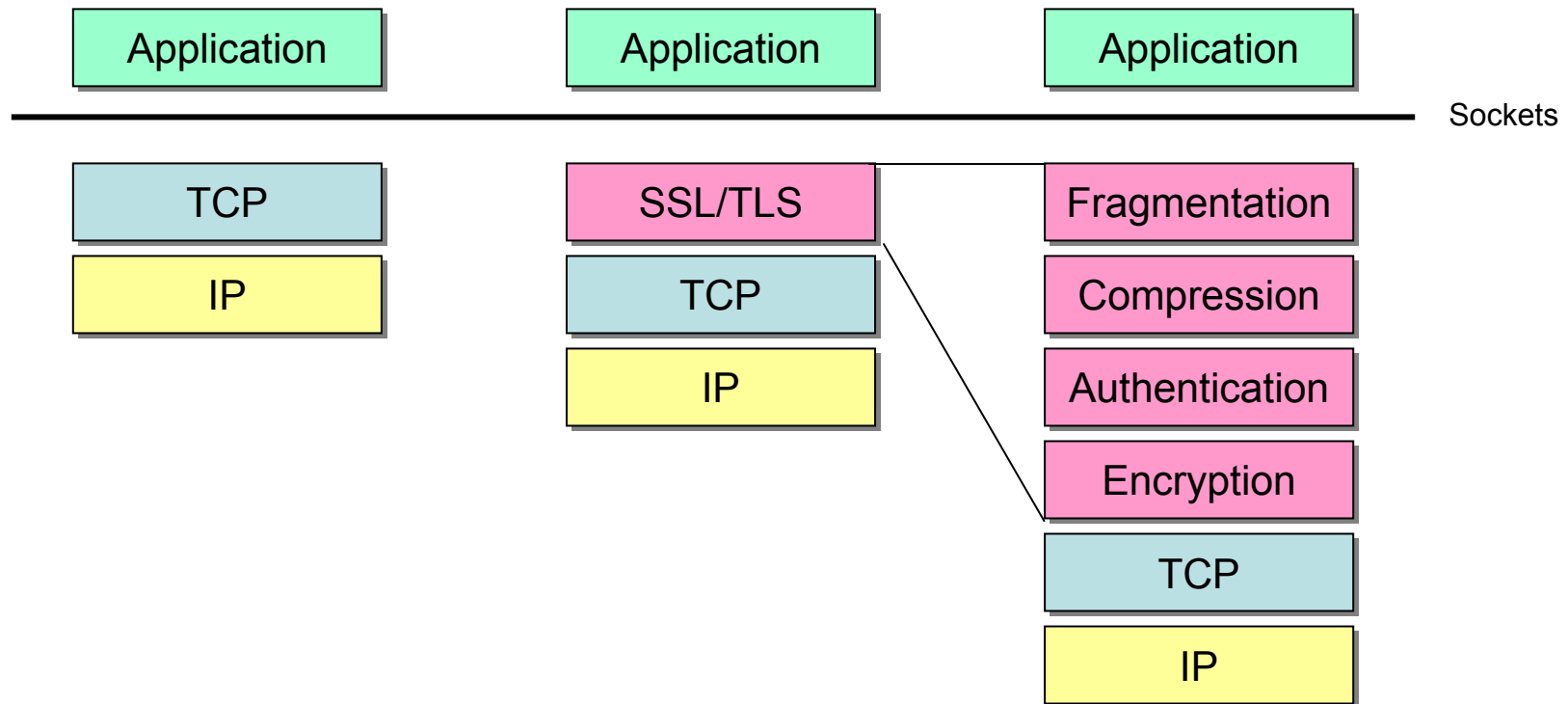
TLS Features for Secure VoIP Service

AP1950S Secure VoIP Gateway

- 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

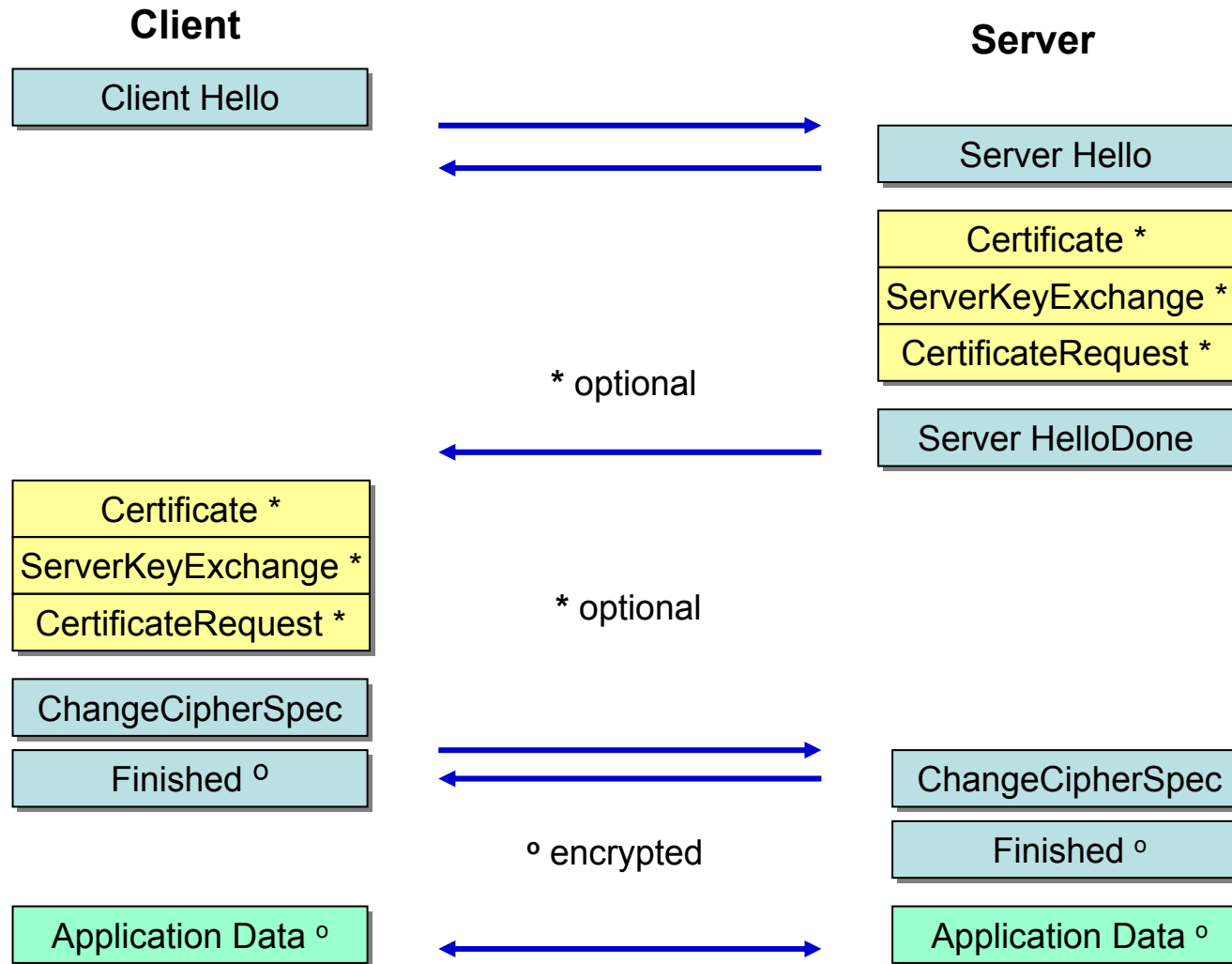
SSL/TLS Protocol Layers

AP1950S Secure VoIP Gateway



SSL/TLS Handshake

AP1950S Secure VoIP Gateway



TLS Comparison with OpenSSL

AP1950S Secure VoIP Gateway

• 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

AP1950S Secure VoIP Gateway

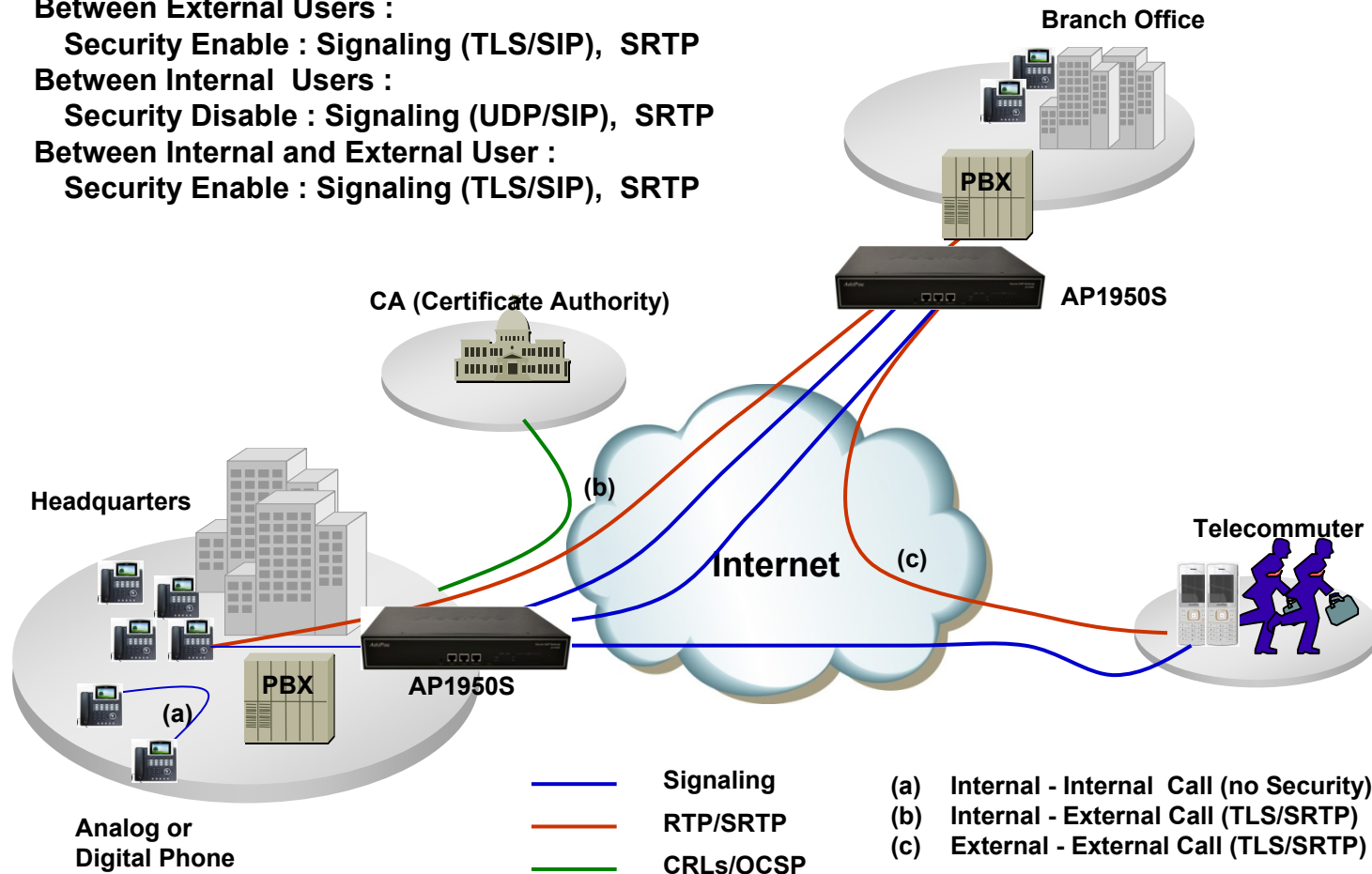
- [RFC4568](#), Standards Track, Session Description Protocol (SDP) Security Descriptions for Media Streams
- [RFC 3711](#), Proposed Standard, The Secure Real-time Transport Protocol (SRTP)
- [RFC 3551](#), Standard 65, RTP Profile for Audio and Video Conferences with Minimal Control
- [RFC 3550](#), 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

SRTP/TLS Network Diagram

AP1950S Secure VoIP Gateway

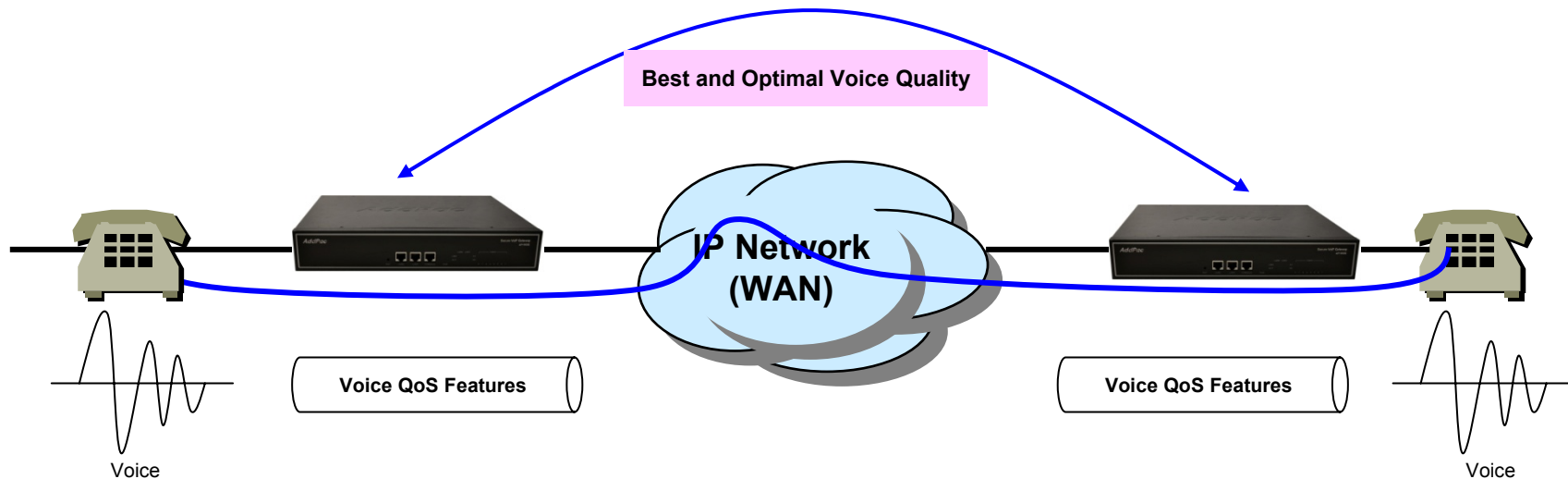
- **Between External Users :**
Security Enable : Signaling (TLS/SIP), SRTP
- **Between Internal Users :**
Security Disable : Signaling (UDP/SIP), SRTP
- **Between Internal and External User :**
Security Enable : Signaling (TLS/SIP), SRTP



Advanced QoS Features

AP1950S Secure VoIP Gateway

- Enhances **Transmit** Voice QoS Features
 - Voice Traffic Priority Queuing
 - QoS Service Profiling
 - Providing Virtual Network Transmit Algorithm
 - Real-time Voice Traffic QoS Support
 - RTP Packet Transmit Interval Control
 - Supporting RTP Packet Redundancy Scheme
 - IP Header Control such as ToS, Diffserv
- Enhances **Receive** Voice QoS Features
 - Dynamic Jitter Buffer Management
 - Error Concealment
 - Support T.38 FAX Data Error Recovery Scheme



Network Protocols

AP1950S Secure VoIP Gateway

Basic Network Protocols

- ARP, IPv4, TCP, UDP, ICMP, SCTP, IGMP, MLD

Routing Protocol

- IPv4 : Static

Service Protocol

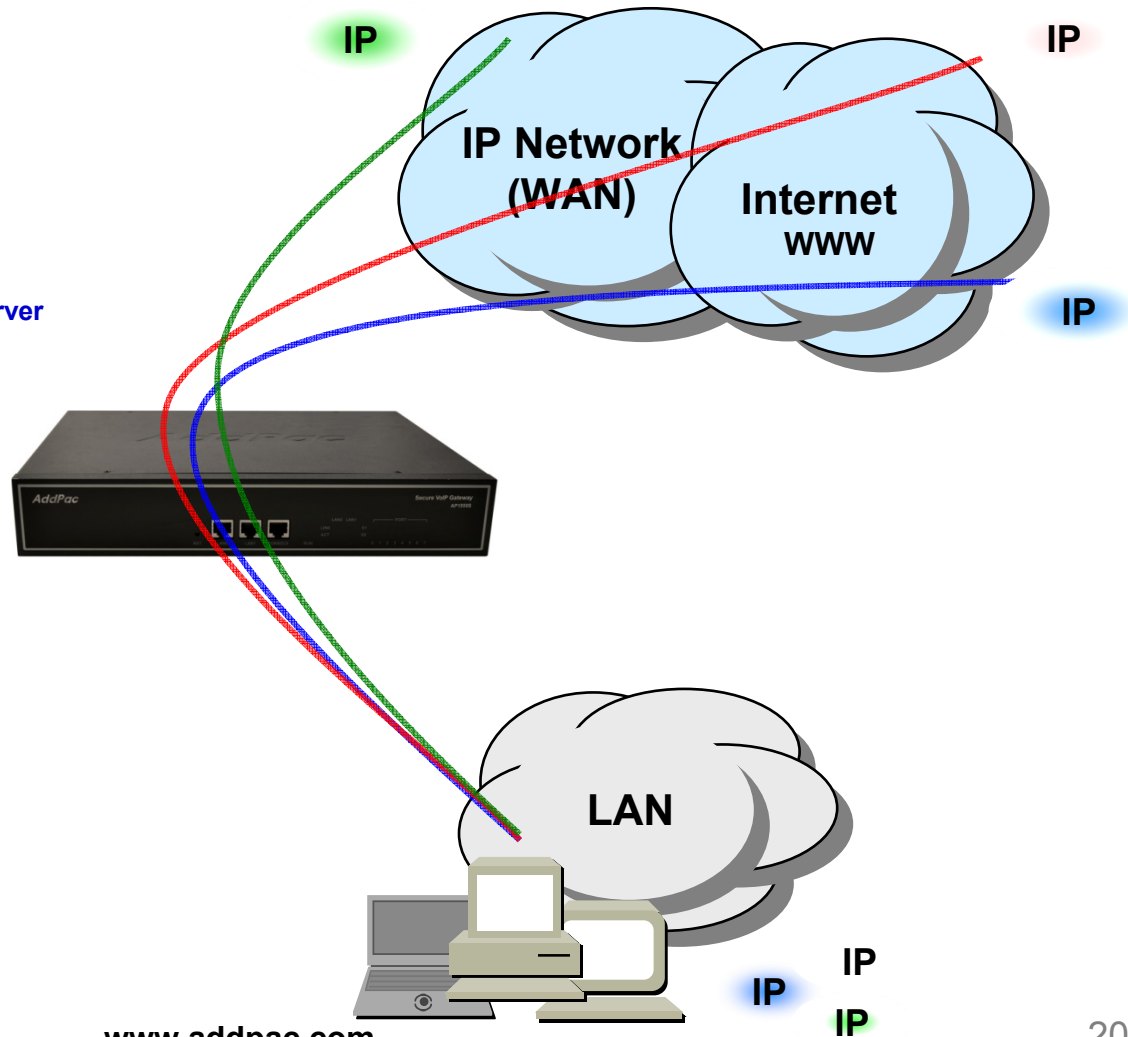
- FTP, Telnet, TFTP, DHCP Server/Relay, SNMP Server
- CDP (Cisco Discovery Protocol)
- DNS Resolver , DDNS(nsupdate)
- Bridge
- Syslog

IPv4 Address Configuration

- Fixed (Static)
- DHCP
- PPPoE

Miscellaneous

- Cisco Style CLI
- Standard & Extended IPv4 Access List
- Multi-level User Account Management
- IP accounting
- STUN Client



Network Management

AP1950S Secure VoIP Gateway

- **SNMP**

- Standard Simple Network Management Protocol(SNMP) Agent support
- MIB v1 and v2 Support

- **Web-based Management**

- Smart Easy Setup
- Standard Voice Interface
- Standard PSTN Back-up Interface

- **Watch-dog Function**

- Hardware, Software watch-dog services

- **Remote Management**

- Telnet
- Rlogin

- **Auto Upgrade Service**

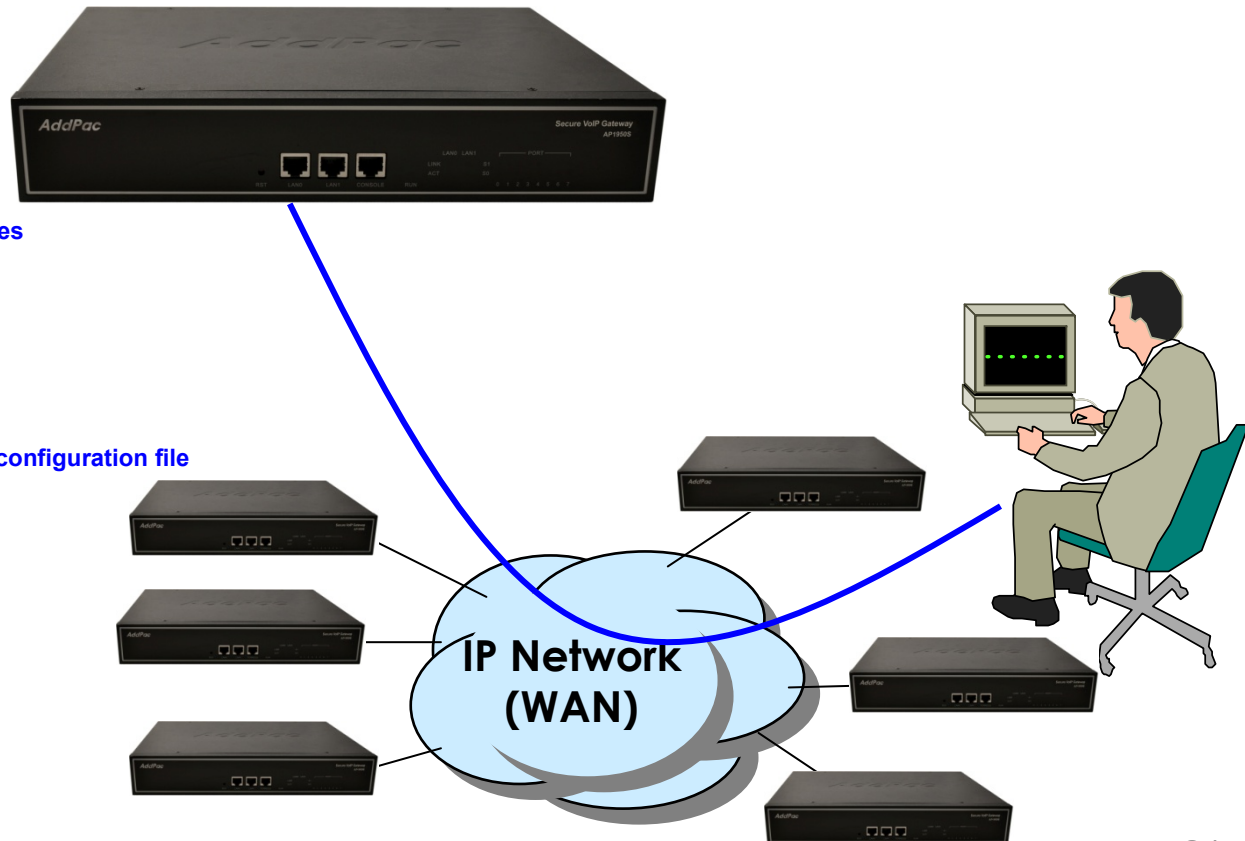
- HTTP server based APOS image and configuration file auto-upgrade support

- **Batch Job Function**

- Text based script downloading

- **Interoperable with AP-VPMS Service**

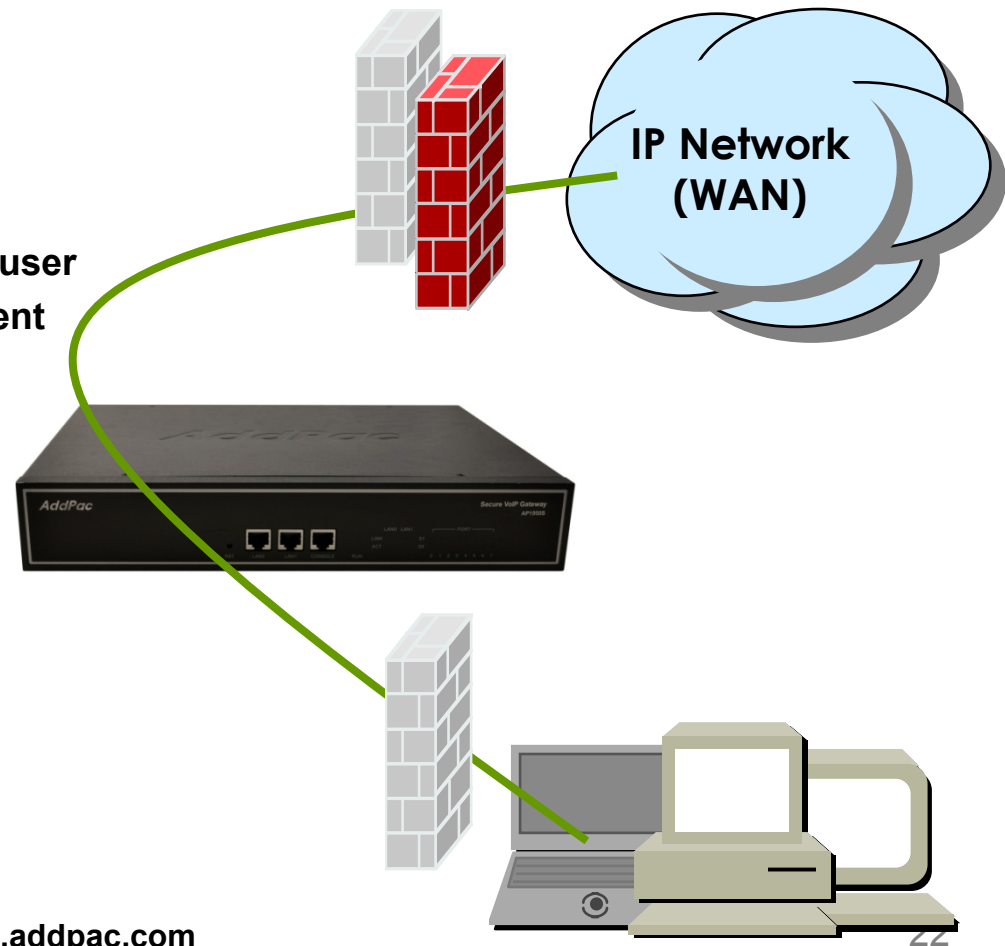
- AddPac VoIP Plug & Play Management System (AP-VPMS)



Security Management

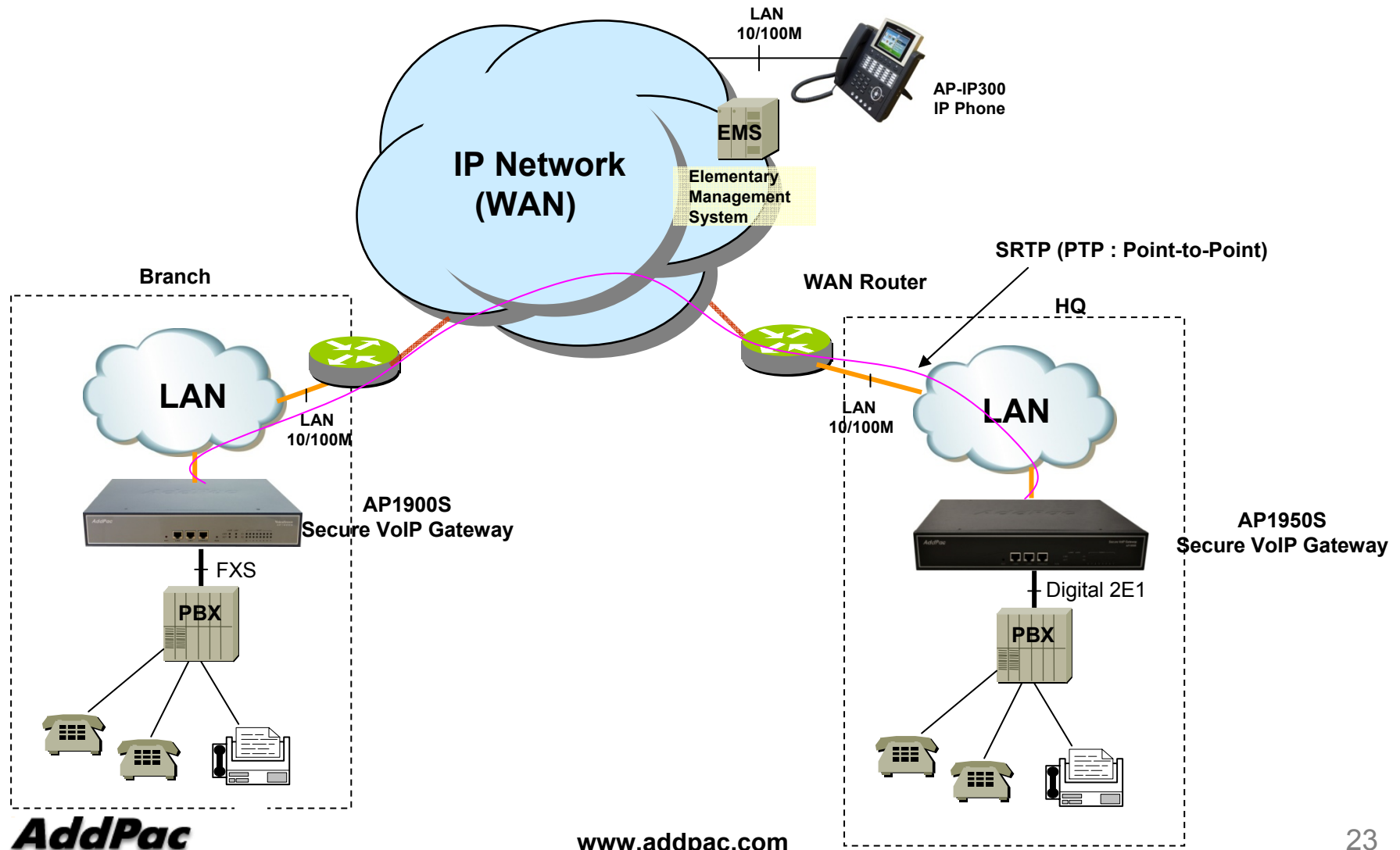
AP1950S Secure VoIP Gateway

- IP packet filtering
- IP access list
- User authentication function
 - Password Authentication Protocol (PAP)
 - Challenge Handshake Authentication Protocol (CHAP)
- Enable/Disable specific protocols
- Auto-square connect of Telnet session
- Account Management function for multi-level user
- SNMP/TELNET/FTP/HTTP/TFTP port assignment function
- SNMP/TELNET/FTP access list management
- Boot mode security checking function



Standard Application

AP1950S Secure VoIP Gateway



Ordering Information

- **AP1950S Secure VoIP Gateway Hardware**
 - AP1900S Secure VoIP Gateway Main Body
 - RISC Microprocessor with High-end Programmable DSP Architecture
 - 2-ports 10/100Mbps Fast Ethernet(RJ45)
 - Option Module: AP-N1-FXS8, AP-N1-FXO8, AP-N1-FXS4O4, AP-N1-E1, AP-N1-2E1etc
 - Including Network Cable & Internal Power Supply, etc.
- **Built-in APOS Internetworking Software for AP1950S**
- **Including 1 Year Hardware Warranty**
- **Product Documents**
 - Install and Operation Guide (PDF)
- **Pricing**
 - AddPac Technology Regional Sales Manager
 - Authorized Sales and Marketing Representatives
 - Please Contact www.addpac.com

Secure VoIP Gateway Series

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