

# Secure VoIP Gateway Solution (TLS/SRTP Protocol)



***AddPac***

**AddPac Technology**

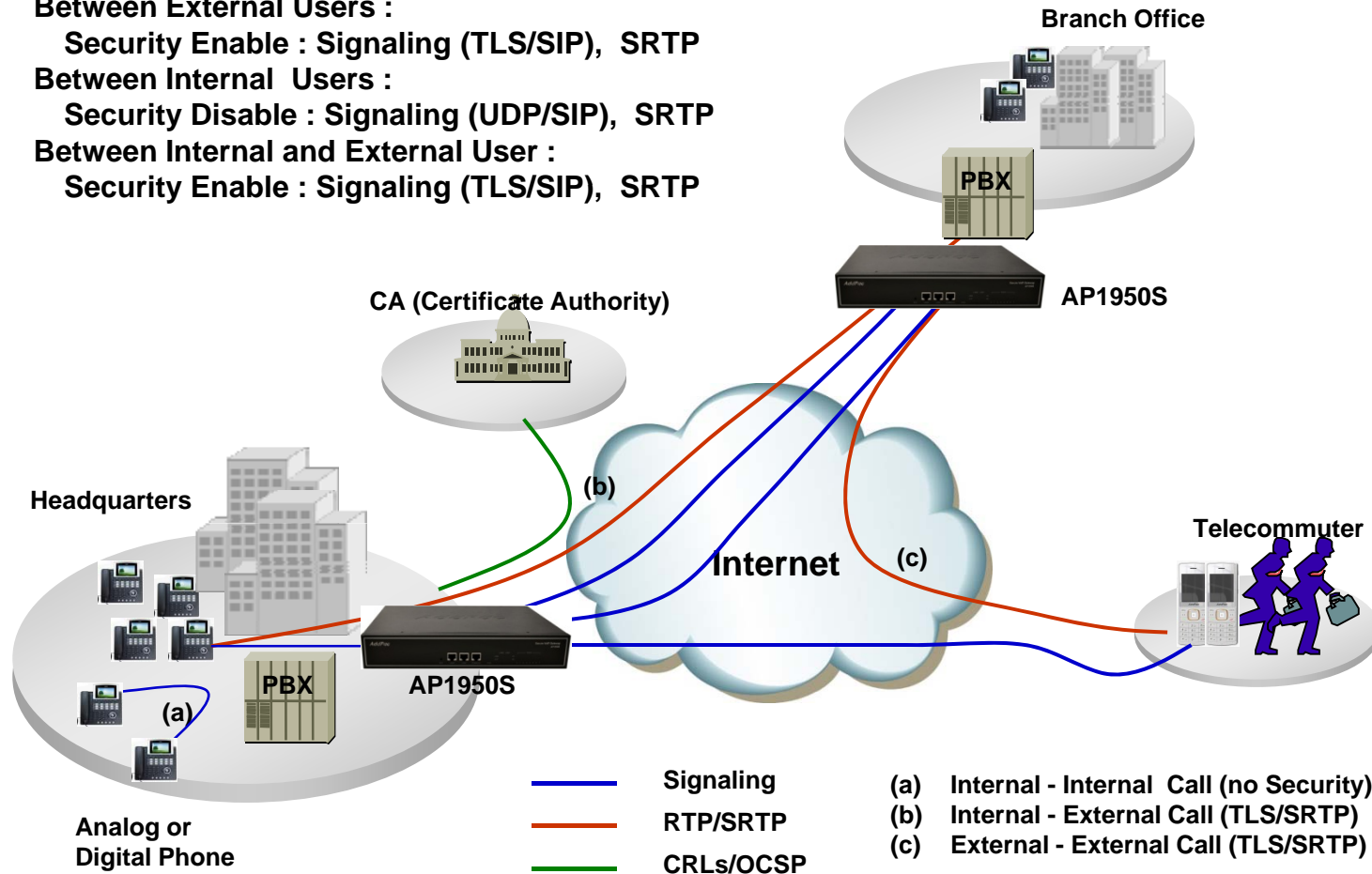
2011, Sales and Marketing

# Contents



- Secure VoIP Gateway Service Diagram
- Secure VoIP Gateway Comparison Table
  - Secure Analog VoIP Gateways
  - Secure Digital VoIP Gateways
- VoIP Modules for Rack Mountable Equipment
- VoIP Gateway Service Features
- Secure VoIP Gateway Service Features

# SRTP/TLS Network Diagram



- **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



# Secure Analog VoIP Gateways (~32 Port)


Product	AP2330S	AP2340S
		
Available Modules	AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4	AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4
Analog Ports	Up to 24	Up to 32
Signaling	SIP, H.323	SIP, H.323
TLS/SRTP Support	Yes	Yes
Module Slots	3	4
Module Slot	Three(3)	Four(4)
LAN Port	2	2
Console	1	1
Power	Single PSU	Single PSU

# Secure Digital VoIP Gateways (1~2 E1/T1)

Product	AP1900S	AP1950S
		
Available Modules	AP-N1-E1 AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4	AP-N1-E1 AP-N1-2E1 AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4
VoIP Signaling	SIP, H.323	SIP, H.323
Digital E1/T1	Up to 1E1	Up to 2E1
Digital Signaling	ISDN PRI, R2	ISDN PRI, R2
TLS/SRTP Support	Yes	Yes
Module Slot	Two(2)	Two(2)
LAN Port	2	2
Console	1	1
Power	Single PSU	Single PSU








# VoIP Modules



Target :  
AP1900S, AP1950S,  
AP2330S, AP2340S

# VoIP Modules

DSP

Target	VoIP Modules	Module Features	Module Picture
AP19x0S AP2330S AP2340S	<b>AP-N1-FXS8</b>	8-Port FXS Module	
AP19x0S AP2330S AP2340S	<b>AP-N1-FXO8</b>	8-Port FXO Module	
AP1800 AP2330S AP2340S	<b>AP-N1-FXS4O4</b>	4-Port FXS&4-Port FXO Module	
AP1900S AP1950S	<b>AP-N1-E1</b>	1-Port Digital E1/T1 Module	
AP1950S	<b>AP-N1-2E1</b>	2-Port Digital E1/T1 Module	

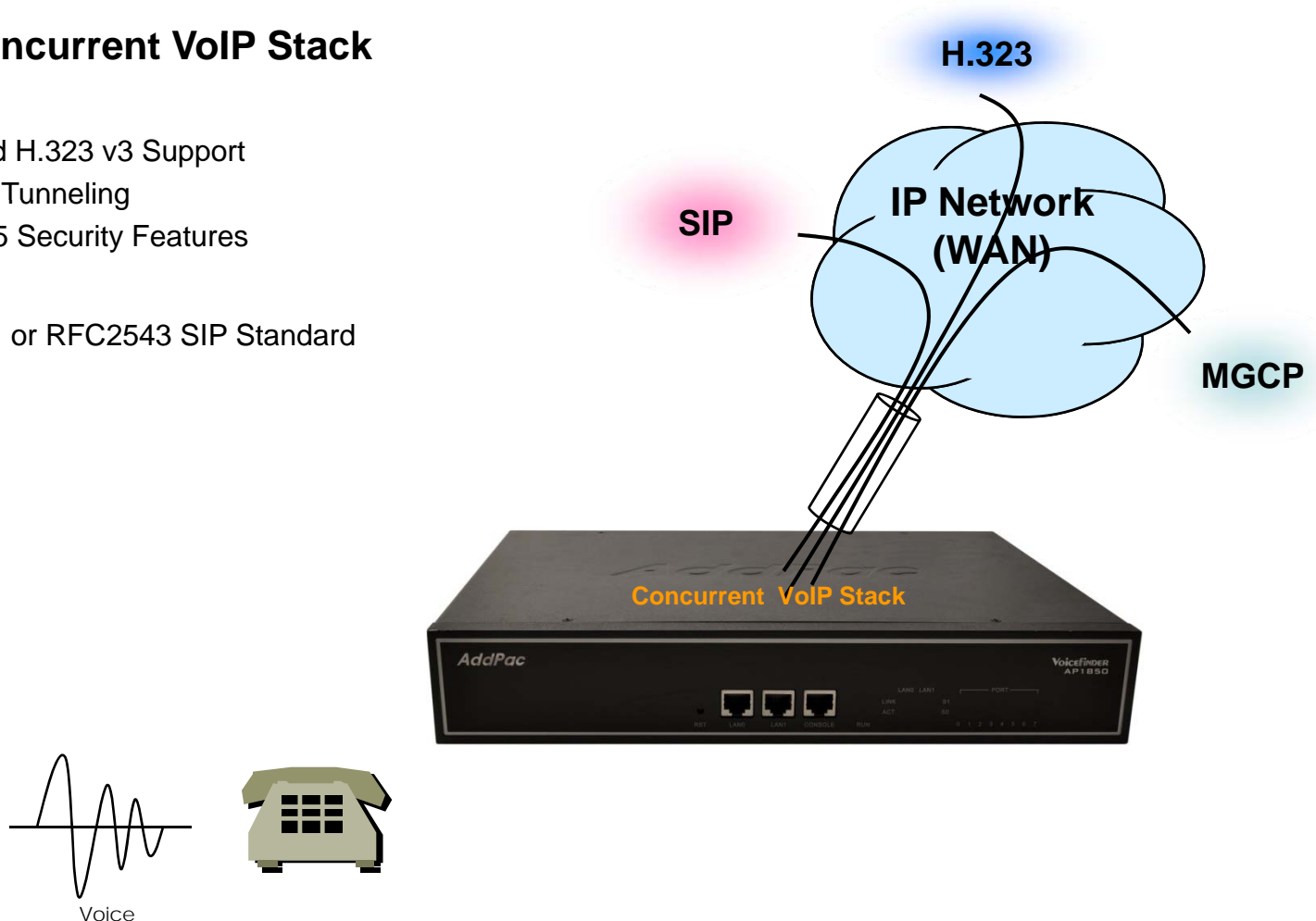




# VoIP Gateway Service Features

# VoIP (Voice over IP) Service

- **H.323, SIP Concurrent VoIP 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



# VoIP (Voice over IP) Service

- **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

# VoIP (Voice over IP) Service

- **Voice Codec**

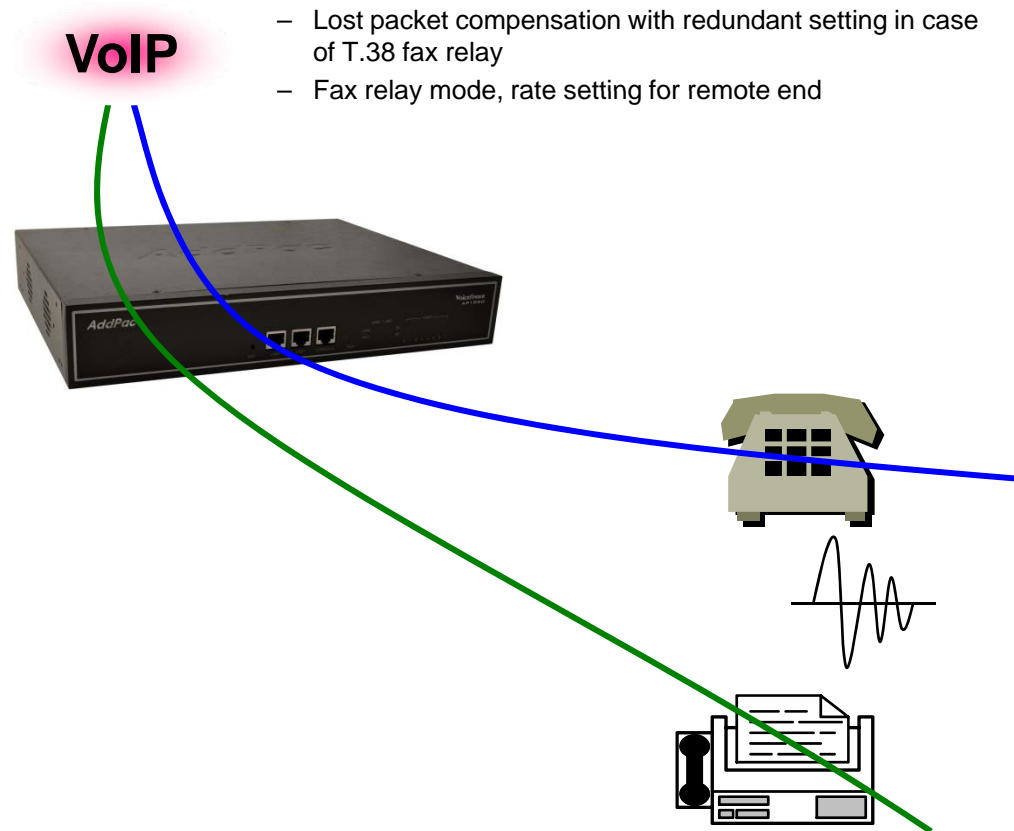
- G.711 A-Law, G.711 U-Law
- G.726 r16, G.726 r32
- G.729A
- G.723.1 r63, G.723.1 r53
- VAD (Voice Activity Detection) function support
- DTMF relay support (H.323, SIP, MGCP common) based on RFC2833

- **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



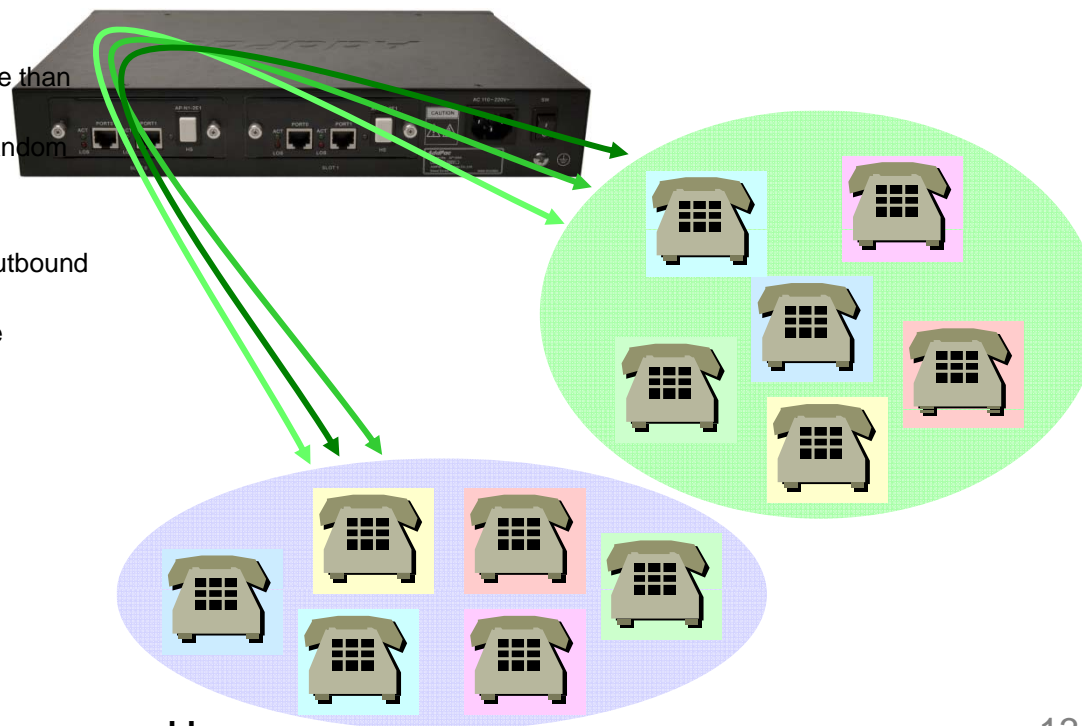
# VoIP (Voice over IP) Service

## • 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



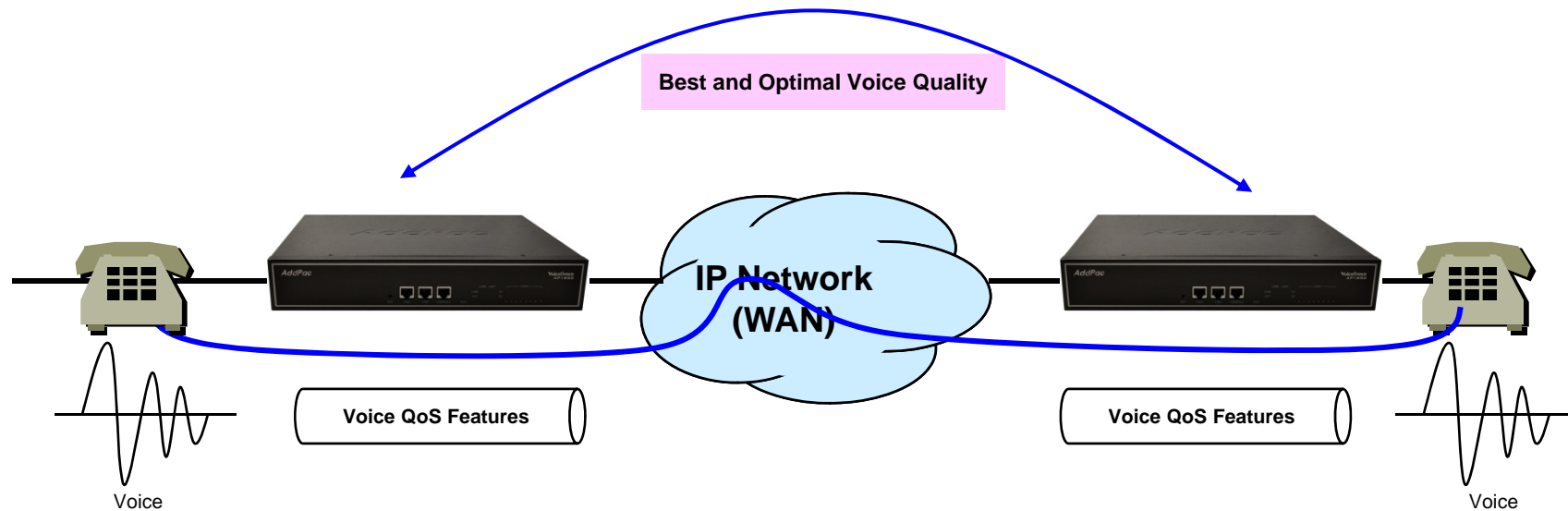
# Advanced QoS Features

- **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

- **Basic Network Protocols**

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

- **Routing Protocol**

- IPv4 : Static

- **Service Protocol**

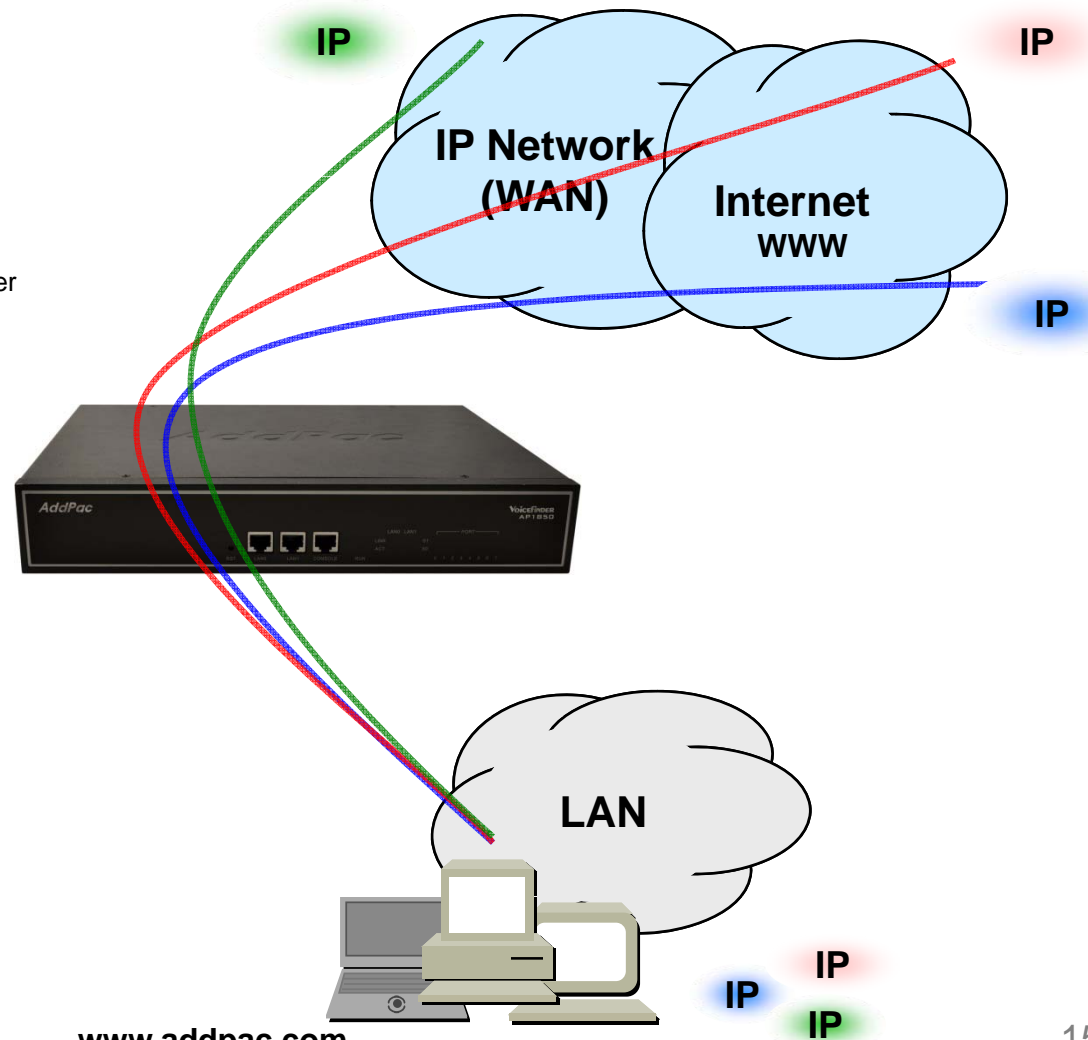
- FTP, Telnet, TFTP, DHCP Server/Relay, SNMP Server
- CDP (Cisco Discovery Protocol)
- DNS Resolver , DDNS(nsupdate)
- Bridge
- Syslog

- **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

- **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**

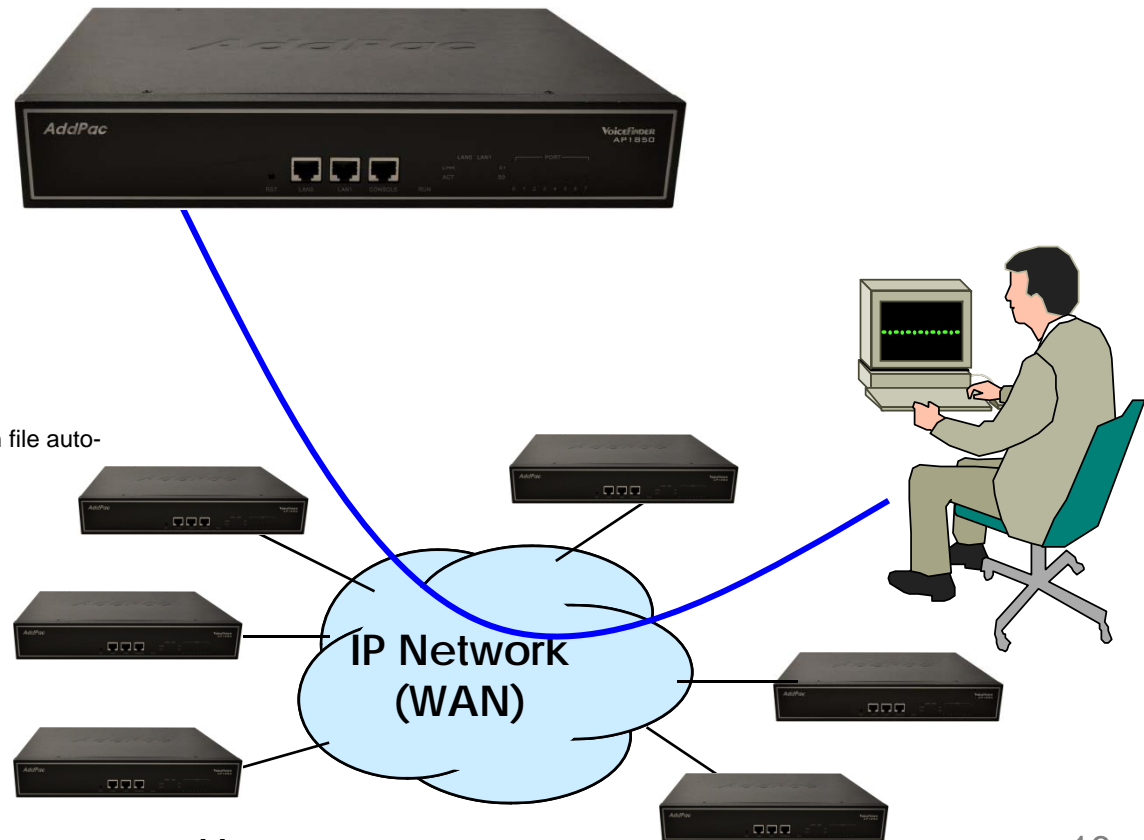
- HTTP server based APOS image and configuration file auto-upgrade support

- **Batch Job Function**

- Text based script downloading

- **Interoperable with AP-VPMS Service**

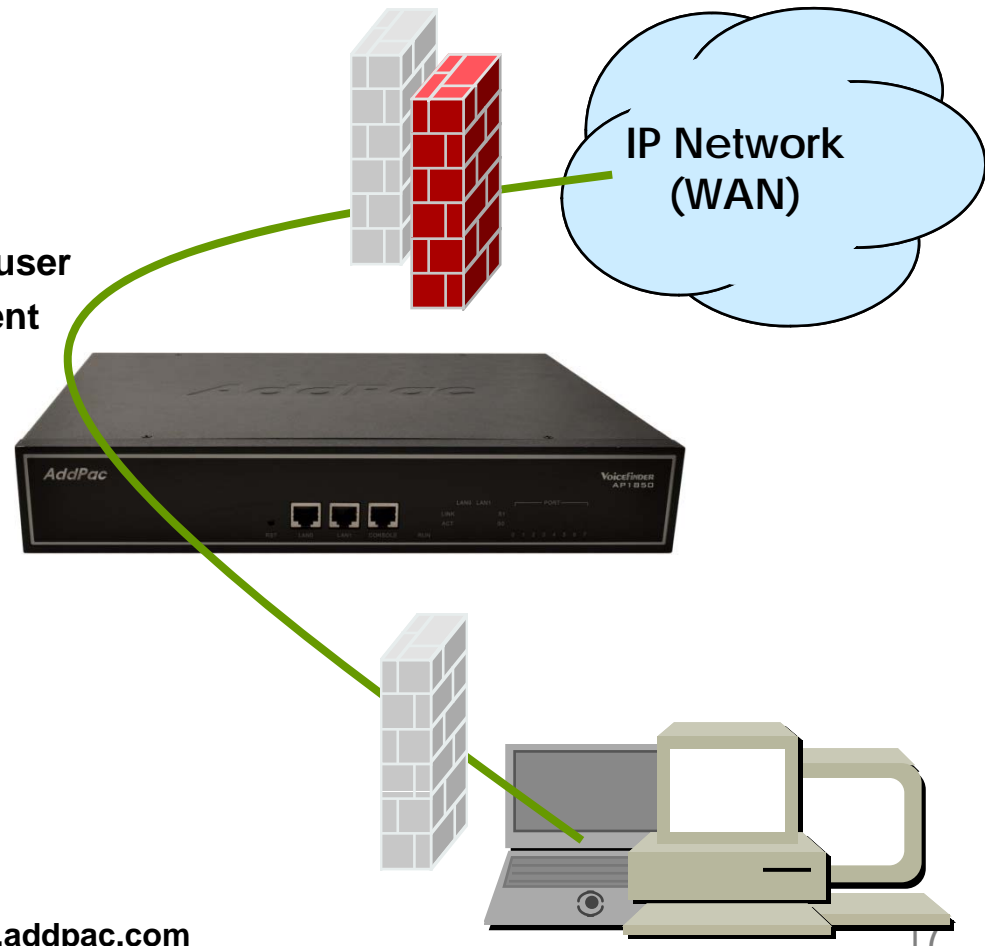
- AddPac VoIP Plug & Play Management System (AP-VPMS)





# Security Management

- 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



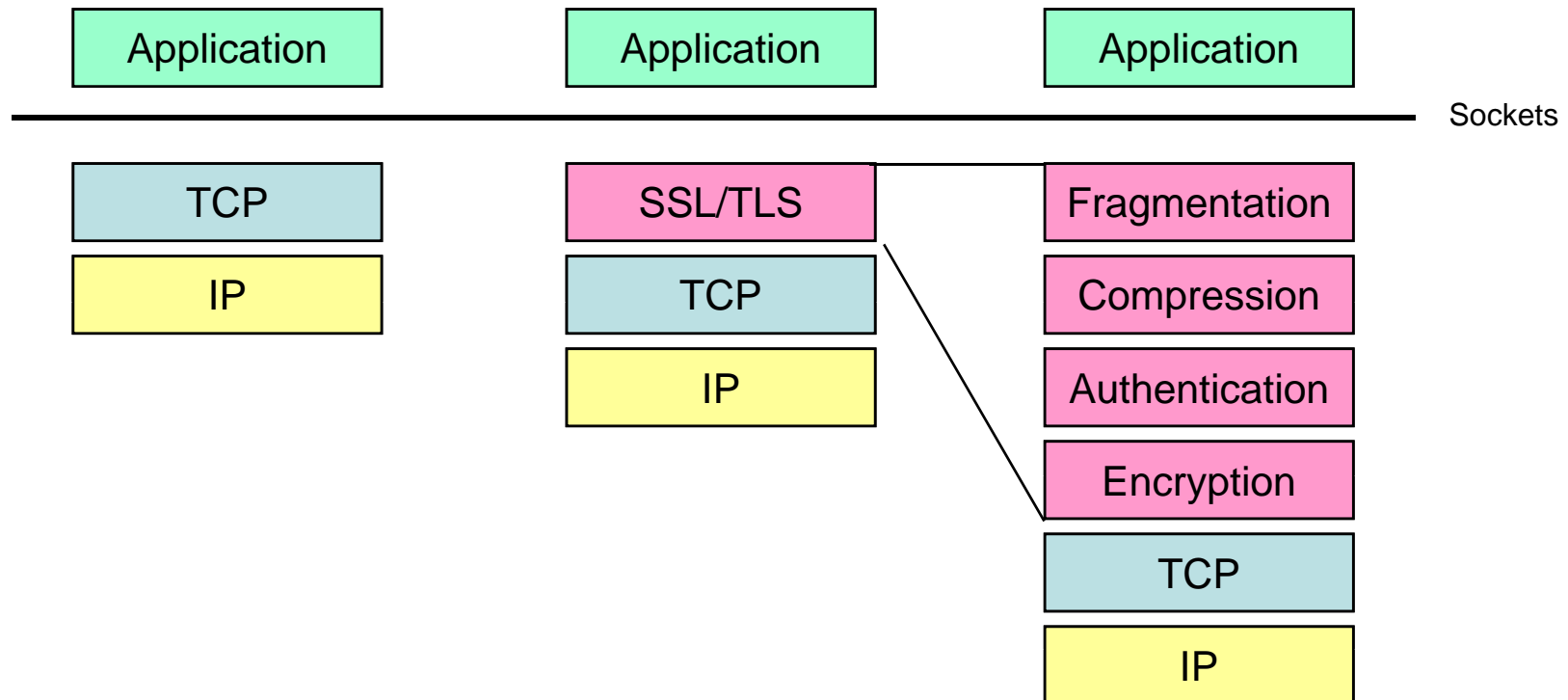


# Secure VoIP Gateway Service Features

# TLS Features for Secure VoIP Service

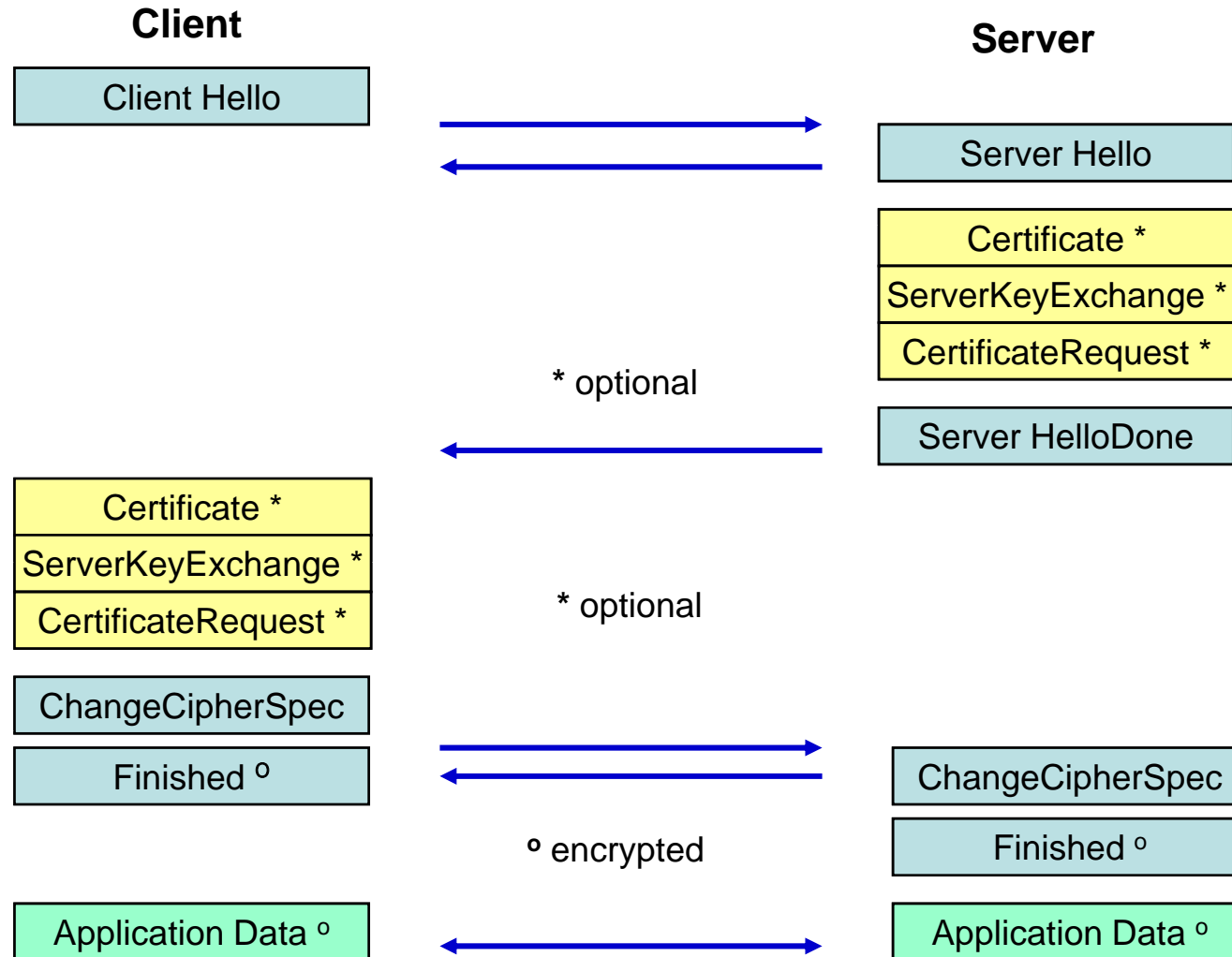
- Support for TLS 1.1, TLS 1.0 and SSL 3.0 protocols
- Since SSL 2.0 is insecure it is not supported.
- TLS 1.2 is supported but disabled by default.
- Support for TLS extensions: server name indication, max record size, opaque PRF input, etc.
- Support for authentication using the SRP protocol.
- Support 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

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

# 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



# 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](mailto:sales@addpac.com)