VoIP Fundamentals: Concepts, Protocols & Technologies

By ClearlyIP Published June 3, 2025 20 min read

VoIP Course 101

1. Introduction to VoIP

Voice over IP (VoIP) is the **real-time transmission of voice signals over IP networks** joehallock.com. Unlike traditional circuit-switched telephony, VoIP digitizes and packetizes audio for transport over data networks. Early research on ARPANET pioneered this idea: in 1973 Danny Cohen demonstrated "packet voice" (the Network Voice Protocol) on the ARPANET en.wikipedia.org, and by 1974 the first real-time voice call was achieved using speech compression en.wikipedia.org. With the advent of high-speed Internet and standards in the 1990s (e.g. ITU-T H.323) and 2000s (IETF

SIP), VoIP matured into a viable alternative to the PSTN. Modern VoIP is significant because it *unifies* voice and data networks: large organizations can carry voice on existing IP infrastructure joehallock.com, reducing costs (e.g. long-distance tolls joehallock.com) and enabling rich features (multimedia, mobility, integration with apps) that legacy telephony cannot support. Today virtually all enterprise voice systems and many consumer services (e.g. Skype, WhatsApp) run over VoIP.

2. Core Technologies

VoIP relies on several key Internet protocols and codecs:

- ** SIP (Session Initiation Protocol)** – the ubiquitous signaling/control protocol (RFC 3261). SIP runs at the application layer and uses text-based requests (INVITE, REGISTER, BYE, etc.) to **set up, modify, and terminate** voice (and multimedia) sessions ietf.org. It operates similarly to HTTP, using proxy servers to locate users and apply policies ietf.org. SIP can run over UDP, TCP or TLS; in fact, the *SIPS* URI scheme ensures encrypted signaling via TLS from caller to callee domain ietf.org. (E.g. a call to `sips:alice@example.com` mandates SIP over TLS ietf.org.) Proxies, registrars and user agents (softphones or IP phones) implement SIP to establish sessions.

- **RTP (Real-time Transport Protocol)** – the protocol for carrying the actual media (voice packets). RTP (RFC 3550) provides end-to-end transport functions for real-time data like audio and video datatracker.ietf.org. Each VoIP call's audio stream is sent in UDP packets with RTP headers that include payload type, sequence numbers, and timestamps datatracker.ietf.org. (RTCP, the RTP control protocol, periodically reports quality metrics.) RTP itself does *not* provide reliability or QoS – it simply delivers packetized audio.

- **Audio Codecs** – VoIP uses codecs to compress speech. Common standards include **G.711**, **G.729** and **Opus** among others. G.711 (µ-law/A-law PCM) is a legacy codec that samples at 8 kHz and outputs 64 kbps callfire.com. It's the default PSTN codec and offers toll-quality audio but uses significant bandwidth. G.729 is a low-bitrate codec (8 kbps) based on conjugate-structure CELP callfire.com, offering reasonable quality with heavy compression. Modern VoIP systems increasingly use **Opus** (RFC 6716): a versatile, open IETF codec that scales from ~6 kbps (narrowband speech) up to 510 kbps (fullband stereo) datatracker.ietf.org. For example, popular apps like WhatsApp use the LPC/MDCT-based Opus codec, and Skype uses its SILK codec en.wikipedia.org. Codecs may also implement packet-loss concealment (PLC) and silence suppression to optimize quality.

- **NAT Traversal** – Since many VoIP endpoints sit behind NAT/firewalls, protocols like **STUN**, **TURN**, and **ICE** are used to traverse these devices. (STUN [RFC5389] discovers a public IP/port; TURN relays media through a server; ICE [RFC8445] orchestrates candidates.) Without these, end-to-end RTP flows can fail. In practice, Session Border Controllers (see below) or specialized SIP ALG features help negotiate NAT traversal for both signaling and media.

- ** Quality of Service (QoS)** – VoIP is sensitive to delay (latency), jitter, and loss. Networks must prioritize voice traffic. Common QoS measures include assigning voice packets a high-priority DSCP class (usually Expedited Forwarding, DSCP 46 cisco.com) and placing them on a separate *voice VLAN*. Switches/routers use *priority queuing* so that voice packets are forwarded before regular data. On endpoints and gateways, **jitter buffers** smooth out delay variation: as Nextiva notes, jitter occurs when packet arrival times vary, and buffers compensate for this variability nextiva.com. Latency should ideally be kept below ~150 ms for conversational quality nextiva.com. Packet loss must be minimized: even a few percent loss causes audible gaps (loss >5% "significantly reduces" quality nextiva.com). Engineers also plan capacity: a G.711 call needs ~80 kbps (including IP/UDP/RTP headers), so a link's bandwidth and QoS must support the expected number of concurrent calls plus overhead.

3. Network Architecture

The core components of a VoIP network include call controllers, gateways, and endpoints:

- **Softswitch / Media Gateway Controller** – A software-based call control element that handles signaling and call logic. Unlike old PBXs, a **softswitch** is software on generic hardware ribboncommunications.com. It establishes and tears down calls, applies routing rules, and interfaces to legacy networks. As Ribbon's architecture diagram shows, a typical softswitch *separates* the control and media planes ribboncommunications.com: the **Media Gateway Controller** (call agent) processes SIP/SS7 signaling, while separate **Media Gateways** handle the actual voice streams to/from the PSTN.

  Figure: Typical softswitch architecture. A Media Gateway Controller (call agent) handles call logic and signaling, controlling Media Gateways that convert between IP (RTP) and traditional PSTN circuits ribboncommunications.com.

- **VoIP Gateway** – Hardware or software that bridges between the IP network and legacy telephony (e.g. T1/E1 lines, analog trunks). A **media gateway** converts audio streams between formats (e.g. uncompressed VoIP ↔ PCM). It may support FXO/FXS ports for analog phones.

For instance, OnSIP describes a VoIP gateway as “hardware bridging PSTN analog to VoIP digital” onsip.com. Gateways also may perform codec transcodings between networks.

- **PBX (IP and Hybrid)** – A Private Branch Exchange is the internal switch for an organization's phones. An ** IP PBX** natively uses VoIP: all extensions are IP phones or softphones, and external trunks are SIP/T1s. As Asterisk notes, an IP PBX “acts as the central switching system” in a business, directing calls internally and to the outside world asterisk.org. A **hybrid PBX** is an older system upgraded to VoIP: for example, a legacy on-prem PBX may use SIP trunks for external calls without replacing existing wiring nextiva.com. In fact, hybrid systems let companies “keep [their] existing phone wiring” while gaining VoIP channels nextiva.com.

- **Session Border Controller (SBC)** – A network element placed at the edge (border) of a VoIP network to protect and manage call flows ribboncommunications.com. SBCs sit between domains (e.g. between a company and the ISP or Internet) and enforce security/policy. They handle NAT traversal for SIP and RTP, encrypt or re-sign signaling (SIP over TLS) and media (SRTP), and prevent attacks. As one definition states, SBCs “protect against denial-of-service attacks, toll fraud, and service theft, and provide media and signaling encryption” ribboncommunications.com. In summary, SBCs serve as a security and demarcation point, much like a firewall for SIP.

- **Endpoints** – The devices used by end-users. These include IP phones (desk phones with Ethernet/PoE), softphones (software on PCs or mobile devices), and analog telephone adapters (ATAs) for connecting old phones. Any device that sends/receives VoIP is an endpoint. For example, Cisco notes that “a VoIP endpoint could be a Cisco IP Phone, a PC using a software phone, or a communications client” certificationkits.com. Today many VoIP endpoints are “multimedia” (video phones, conferencing units) or mobile apps, but any SIP/RTP-capable device falls in this category.

4. Deployment Scenarios

VoIP is deployed in many settings:

- **Business VoIP (On-Premises IP PBX)** – Companies often deploy on-site IP PBXs or softswitches. Employees have IP phones on the LAN, and the PBX connects to outside lines via SIP trunks or T1/E1. On-prem VoIP offers feature-rich telephony (voicemail, conferencing, UC integration) under the company's control. However, it requires purchasing hardware and maintaining it. As one survey explains, premise-based systems “can be expensive” to set up (needing IP phones, SIP trunks, wiring, dedicated maintenance) nextiva.com.

Figure: Example multi-site business VoIP deployment. Branch offices and remote users connect over IP (VPN/Internet) to a central call system, enabling unified dialing and features across the organization.

- **Cloud-based VoIP (Hosted PBX / UCaaS)** – Instead of on-site equipment, many businesses use hosted VoIP or Unified Communications as a Service (UCaaS). In this model, the provider hosts the PBX in the cloud. Companies connect via the Internet: typically only IP phones or apps on-premise. Cloud VoIP is often cheaper to start (no large hardware purchases) and scales easily. Calls from any office or home user route through the provider's data center. For example, hosted systems eliminate heavy telco fees; the connection "runs on the Internet" so there are "no … stacked fees from telco companies" onsip.com, just flat service charges.

- **Hybrid Deployments** – Some organizations mix on-prem and cloud. For instance, a company may keep certain analog lines or local gateways on-site but use a SIP trunk provider for most voice. Or they may use on-site PBX for internal calls and fall back to a cloud service for overflow or remote branches. A hybrid PBX (as above) lets a firm add VoIP channels without scrapping their existing system nextiva.com. Hybrid setups can ease migration: legacy hardware remains while VoIP features are gradually added.

- **Mobile VoIP (mVoIP)** – Mobile devices increasingly use VoIP. Softphone apps on smartphones/tablets can place VoIP calls over Wi-Fi or cellular data. Many messaging apps (WhatsApp, Skype, etc.) rely on VoIP to connect voice calls. VoLTE and VoNR are carrier-grade examples: 4G LTE's voice service (VoLTE) and 5G's voice-over-new-radio (VoNR) both use VoIP principles in the mobile core. In general, *mVoIP* allows users to be reachable via their "SIP address" on any device. As one VoIP guide notes, unlike wired phones that "stop ringing" when you leave the office, VoIP calls "go to your SIP address" so "any device logged in will ring" onsip.com.

- **Residential VoIP** – Home users often adopt VoIP through consumer services (e.g. Vonage, Ooma, etc.) over broadband. A typical home VoIP setup uses an Analog Telephone Adapter (ATA) or VoIP-capable router: the ATA converts the analog home phone's audio to IP packets. This gateway "bridges the PSTN and VoIP networks" by digitizing analog signals onsip.com. Law regulators distinguish "interconnected VoIP" (which provides service like a phone line) from "over-the-top" services. In either case, the user's broadband connection carries calls, and emergency location (E911) is handled via registered address (see below).

5. Security in VoIP

VoIP introduces new security considerations:

- **Threat Models:** Attackers exploit VoIP in various ways. Common threats include eavesdropping on calls (listening to RTP streams), toll fraud (unauthorized call origination), denial-of-service (flooding SIP servers or trunks), and **SPIT** (Spam over IP Telephony) or *vishing* (voice phishing). Malware can target VoIP endpoints or PBXs, and exploits like the "VOMIT" attack can capture VoIP traffic for later analysis. A security review lists malware, DDoS, VoIP eavesdropping, SPIT, and voice phishing as key threats gammagroup.co.

- **Encryption:** To counter eavesdropping, VoIP uses encryption. **SRTP** (Secure RTP, RFC 3711) encrypts and authenticates the media stream datatracker.ietf.org. SRTP applies AES encryption and anti-replay protection to RTP payloads, securing the call audio. Signaling can be encrypted using **TLS**: SIP over TLS (often called SIPS) encrypts SIP messages on the transport layer ietf.org. (For WebRTC and similar, DTLS-SRTP is also used.) Encryption adds overhead and latency nvlpubs.nist.gov, but is essential for confidentiality. Session Border Controllers often enforce SRTP and TLS: for instance, Ribbon notes SBCs "provide media and signaling encryption" to protect calls ribboncommunications.com.

- **Firewalls and NAT:** Firewalls must be VoIP-aware. A simple firewall can block VoIP traffic, so enterprises typically allow SIP and RTP ports (or use an SBC). Many routers have **SIP ALG** features (automatic helpers) – but these often introduce problems (it's usually safer to disable broken SIP-ALG and let an SBC or STUN/ICE handle NAT). The SBC or proxy also often performs topology hiding and deep packet inspection.

- **Anti-Fraud Measures:** Providers implement controls to prevent toll fraud: e.g. strict authentication on call origination, blacklists of suspicious call destinations (high-cost countries), and rate limits. Monitoring CDRs (Call Detail Records) for unusual calling patterns is common. As noted, SBCs can "safeguard against toll fraud and service theft" by enforcing call permissions ribboncommunications.com. VoIP systems also log calls and can audit for unauthorized use.

6. Performance Optimization

Maintaining call quality involves active network management:

- **Latency and Jitter:** Use low-latency links. Keep **one-way delay** under ~150 ms nextiva.com; latency beyond ~250 ms causes poor interactivity. Minimize jitter with proper queuing and jitter buffers nextiva.com; a jitter buffer holds arriving packets briefly to smooth delay variations. Configure voice VLANs and trust DSCP markings (Expedited Forwarding, DSCP 46) so that switches schedule voice frames first cisco.com.

- **Packet Loss:** Strive for near-zero packet loss. Even a few percent loss can cause choppy audio. (Statistically, Nextiva warns that loss >5% "significantly reduces" quality nextiva.com.) Use reliable Ethernet (no collisions), QoS (to avoid buffer overflows), and consider FEC (forward error correction) or PLC in codecs.

- **Bandwidth and Capacity Planning:** Calculate required bandwidth (e.g. ~80 kbps per G.711 call, ~24 kbps per G.729 call including overhead). Overprovision lines (allow ~20–30% headroom) and implement Call Admission Control if needed. Monitor usage trends: as one best practice recommends, watch for traffic spikes or saturated links, since spikes can "negatively impact calls" nextiva.com.

- **Network Monitoring:** Use SNMP and VoIP-specific tools. Monitor metrics like Mean Opinion Score (MOS), RTP packet loss, jitter and latency end-to-end. As Nextiva suggests, collect call-quality statistics and logs from all devices nextiva.com. Set up alerts for rising loss/jitter or trunk failures. Regularly sample test calls from different locations and times to detect emerging problems nextiva.com.

- **VLANs and QoS Configuration:** Put all IP phones on a dedicated **voice VLAN**. Configure switches to trust and prioritize the CoS/DSCP of voice packets. On wireless segments, enable Wi-Fi Multimedia (WMM) or similar for voice priority. Finally, ensure Power over Ethernet (PoE) for phones so they stay up during power issues.

7. Regulatory and Legal Considerations

- **E911 (Enhanced 911)**: VoIP providers in many countries must support emergency calling by conveying caller location to dispatchers. In the U.S., FCC rules mandate that *interconnected VoIP* providers deliver the caller's registered physical address (Automatic Location Information) to the PSAP when 911 is dialed telnyx.com. Users must supply/verify their location at registration, and calls must be routed to the correct local emergency center telnyx.com. Dynamic E911 solutions (particularly for nomadic VoIP) are evolving, but the core rule is "known location → correct PSAP" telnyx.comtelnyx.com.

- **CALEA (Lawful Intercept)**: In the U.S., the Communications Assistance for Law Enforcement Act was extended to VoIP in 2005. Providers of broadband and "interconnected VoIP" service are required to accommodate court-ordered wiretaps ndcac.fbi.gov. This means the VoIP network must have capabilities (often via an IMS core or SBC) to duplicate traffic (signaling and media) for law enforcement when legally authorized. Similar laws exist in other countries (e.g. Europe's intercept regulations, albeit more in telecom carriers).

- **Data Privacy (GDPR and others)**: Call metadata and recordings are subject to data protection laws. For example, the EU's GDPR requires that call recordings be handled with consent and legitimate interest. Companies must justify call recording: valid reasons include consent from participants, contractual need, or legal obligation voipstudio.com. Call detail records (CDRs) and personal data in call logs must be secured and often encrypted. Privacy laws may also mandate data retention limits and user access rights to their own data. Compliance often means implementing strong access controls, encryption of stored call data, and clear notification/consent procedures.

8. Troubleshooting and Maintenance

- **Common Issues:** Frequent VoIP problems include one-way audio (audio only heard in one direction), no dial tone (failed SIP registration), call drops, garbled audio, echo, and poor quality (choppiness). One-way audio is typically caused by NAT/firewall issues blocking the return RTP stream support.onsip.com; misconfigured SIP ALG or missing ports often cause it. Codec mismatches (unsupported codec between endpoints) can also cause call failure. High jitter or packet loss manifests as choppy or broken speech. Network issues (e.g. jitter spikes, intermittent connectivity) often underlie poor call quality.

- **Diagnostic Tools:** Packet capture (Wireshark) is essential: capture SIP and RTP flows to see registration exchanges, INVITEs, and RTP payload. Tools like *sngrep* (for SIP signaling traces) or RTP analysis software can help spot packet loss or reordering. SNMP or network probes can measure jitter, latency, and loss on links. Ping and traceroute can reveal routing problems. On endpoints, enable SIP debug logging and capture phone/system logs.

- **Logging:** Enable verbose SIP and call logs on servers, IP PBXs, and SBCs. Keep Call Detail Records (CDRs) with timestamps, durations, and endpoints to trace calls. Monitor system logs for SIP errors (403/480 responses, timeouts). Use syslog or centralized log servers for correlation. As a best practice, Nextiva suggests a **layered monitoring approach**: gather metrics, device logs, infrastructure health and even customer feedback in concert nextiva.com. For example, if users report static or echo, check network error logs and core dumps on the VoIP gateway.

- **Problem Isolation:** When troubleshooting, correlate symptoms: frequent SIP "408 Timeout" might indicate packet loss on the LAN or trunk. No registration (401 challenge repeatedly) indicates authentication/misconfig. One-way audio usually means RTP path blockage support.onsip.com. Echo usually comes from bad analog interfaces or double-talk. Test with different codecs or direct calls to isolate if it's a network vs endpoint issue. Regular maintenance includes updating firmware (fixing SIP bugs), patching security holes, and checking certification of TLS certificates for SIP.

9. Future Trends

- **5G and VoIP:** Mobile networks are shifting to all-IP architectures. 4G LTE introduced VoLTE (Voice over LTE), which is essentially VoIP over the LTE core. 5G will continue this trend: "Voice over NR" (VoNR) is the native 5G voice service. 5G's ultra-low latency and high reliability will further improve mobile call quality (smaller codecs, HD voice, low-latency conference). Also, network slicing in 5G may dedicate resources for critical voice (e.g. enterprise or emergency networks) ietf.org.

- **AI and Voice Analytics:** AI is rapidly entering VoIP applications. Call centers use AI-driven features like speech-to-text transcription, sentiment analysis, and real-time agent coaching. For example, modern VoIP call-center systems can do **predictive call routing**, virtual assistants, speech analytics and sentiment analysis to improve service voicespin.com. Machine learning can also enhance network management (predictive QoS tuning) and security (detect anomalies in calling patterns). Even on endpoints, AI noise-cancellation and voice quality optimization are emerging.

- **WebRTC:** Web Real-Time Communications (WebRTC) is a W3C/IETF standard that brings VoIP into web browsers and apps without plugins ietf.org. WebRTC defines JavaScript APIs and protocols to send/receive RTP in browsers, enabling web-based voice/video apps. As of 2021, WebRTC is an official standard "bringing audio and video communications anywhere on the Web" ietf.org. In practice, WebRTC is widely used for click-to-call, video conferencing (e.g. browser-based meetings), and VoIP clients integrated into web services.

- **UCaaS (Unified Communications as a Service):** VoIP is now often delivered as part of a broader cloud communications platform. UCaaS bundles VoIP telephony with messaging, video conferencing, presence, and collaboration tools techtarget.comtechtarget.com. In UCaaS, the entire stack (softswitch, PBX features, apps) is hosted by the provider. Businesses migrate from hardware phones to software clients and cloud phones, gaining unified calendaring, mobility, and integrations (CRM, email) at the platform level. The trend is towards fully hosted communication suites where VoIP is one component of an integrated service techtarget.com.

10. Case Studies and Real-World Applications

- **Enterprise Deployments:** Many large organizations have moved to VoIP for cost and feature benefits. For instance, global companies often replace multiple legacy PBXs with a single SIP-based network, unifying voice across offices worldwide. An example is the UK's upcoming PSTN shutdown: telecom carriers are urging businesses to migrate their phone systems off PSTN by 2025 business.bt.com. This reflects the broad trend: *all-IP* telephony. Compared to legacy copper telephones, VoIP is substantially cheaper and more flexible. OnSIP notes that VoIP requires only an internet connection (no expensive copper wiring) and avoids "stacked" telco fees onsip.com. In practice, enterprises report cutting phone bills by 30–50% while gaining features like softphones, mobile integration and unified messaging.

- **VoIP in Call Centers:** Contact centers are a natural fit for VoIP/UC. VoIP enables advanced call routing (IVR/ACD), distributed agents (work-from-home), and easy call recording and monitoring. Modern call centers integrate VoIP with CRM and workforce management. For example, AI-enhanced VoIP platforms now provide live speech analytics: calls are transcribed and sentiment is detected in real time, helping supervisors intervene. VoiceSpin highlights that AI-driven VoIP can auto-transcribe, route calls predictively, and offer virtual assistants – features unheard of in analog systems voicespin.com. The scalability of VoIP also allows centers to burst capacity or use cloud bursts for peak loads.

- **Legacy vs. Modern:** In comparing VoIP to legacy telephony, the differences are striking. VoIP offers *versatility* beyond voice. Landlines were single-purpose, whereas VoIP endpoints can carry voice, video, and data simultaneously. Remote and mobile users are inherently supported (calls follow the user over IP), unlike old PBXs. As OnSIP points out, VoIP calls "go to your SIP address" so any registered device (desktop, laptop, mobile) rings onsip.com. This flexibility, along with flat-fee pricing, has led many to abandon aging PBXs.

- **Regulatory/Market Examples:** Aside from the PSTN cutover, regulators are actively shaping VoIP. For instance, California law SB 460 (2017) requires VoIP providers to integrate dispatchable location for 911 calls. Globally, countries are harmonizing VoIP E911 rules (often following FCC-like mandates) so that internet-based calls have reliable emergency support. Meanwhile, operators (like AT&T's IP Voice or BT's One Voice) illustrate commercial VoIP trunks replacing traditional lines. These real-world cases show that VoIP is no longer experimental – it is the mainstream telephony platform for enterprises, call centers, and even home users worldwide business.bt.comonsip.com.

Sources: Authoritative telecom standards (RFCs, ITU-T); industry whitepapers; vendor documentation; and technical references en.wikipedia.orgietf.org datatracker.ietf.orgcallfire.com callfire.comdatatracker.ietf.org nextiva.comribboncommunications.com cisco.comnextiva.com nextiva.comnextiva.com telnyx.comndcac.fbi.gov voipstudio.comsupport.onsip.com nextiva.comvoicespin.com ietf.orgtechtarget.com business.bt.comonsip.com.

Tags: voip, voice over ip, sip protocol, ip networks, real-time communication, data networks, telecommunications, networking, digital voice

About ClearlyIP

ClearlyIP Inc. — Company Profile (June 2025)

1. Who they are

ClearlyIP is a privately-held unified-communications (UC) vendor headquartered in Appleton, Wisconsin, with additional offices in Canada and a globally distributed workforce. Founded in 2019 by veteran FreePBX/Asterisk contributors, the firm follows a "build-and-buy" growth strategy, combining in-house R&D with targeted acquisitions (e.g., the 2023 purchase of Voneto's EPlatform UCaaS). Its mission is to "design and develop the world's most respected VoIP brand" by delivering secure, modern, cloud-first communications that reduce cost and boost collaboration, while its vision focuses on unlocking the full potential of open-source VoIP for organisations of every size. The leadership team collectively brings more than 300 years of telecom experience.

2. Product portfolio

- **Cloud Solutions** – Including *Clearly Cloud* (flagship UCaaS), **SIP Trunking**, **SendFax.to** cloud fax, **ClusterPBX OEM**, **Business Connect** managed cloud PBX, and **EPlatform** multitenant UCaaS. These provide fully hosted voice, video, chat and collaboration with 100+ features, per-seat licensing, geo-redundant PoPs, built-in call-recording and mobile/desktop apps.
- **On-Site Phone Systems** – Including CIP PBX appliances (FreePBX pre-installed), ClusterPBX Enterprise, and Business Connect (on-prem variant). These offer local survivability for compliance-sensitive sites; appliances start at 25 extensions and scale into HA clusters.
- **IP Phones & Softphones** – Including CIP SIP Desk-phone Series (CIP-25x/27x/28x), fully white-label branding kit, and *Clearly Anywhere* softphone (iOS, Android, desktop). Features zero-touch provisioning via Cloud Device Manager or FreePBX "Clearly Devices" module; Opus, HD-voice, BLF-rich colour LCDs.
- **VoIP Gateways** – Including Analog FXS/FXO models, VoIP Fail-Over Gateway, POTS Replacement (for copper sun-set), and 2-port T1/E1 digital gateway. These bridge legacy endpoints or PSTN circuits to SIP; fail-over models keep 911 active during WAN outages.
- **Emergency Alert Systems** – Including **CodeX** room-status dashboard, **Panic Button**, and **Silent Intercom**. This K-12-focused mass-notification suite integrates with CIP PBX or third-party FreePBX for Alyssa's-Law compliance.
- **Hospitality** – Including **ComXchange** PBX plus PMS integrations, hardware & software assurance plans. Replaces aging Mitel/NEC hotel PBXs; supports guest-room phones, 911 localisation, check-in/out APIs.
- **Device & System Management** – Including **Cloud Device Manager** and **Update Control (Mirror)**. Provides multi-vendor auto-provisioning, firmware management, and secure FreePBX mirror updates.
- **XCast Suite** – Including Hosted PBX, SIP trunking, carrier/call-centre solutions, SOHO plans, and XCL mobile app. Delivers value-oriented, high-volume VoIP from ClearlyIP's carrier network.

---

3. Services

- **Telecom Consulting & Custom Development** – FreePBX/Asterisk architecture reviews, mergers & acquisitions diligence, bespoke application builds and Tier-3 support.
- **Regulatory Compliance** – E911 planning plus **Kari's Law**, **Ray Baum's Act** and **Alyssa's Law** solutions; automated dispatchable location tagging.
- **STIR/SHAKEN Certificate Management** – Signing services for Originating Service Providers, helping customers combat robocalling and maintain full attestation.
- **Attestation Lookup Tool** – Free web utility to identify a telephone number's service-provider code and SHAKEN attestation rating.
- **FreePBX® Training** – Three-day administrator boot camps (remote or on-site) covering installation, security hardening and troubleshooting.

- **Partner & OEM Programs** – Wholesale SIP trunk bundles, white-label device programs, and ClusterPBX OEM licensing.

---

4. Executive management (June 2025)

- **CEO & Co-Founder: Tony Lewis** – Former CEO of Schmooze Com (FreePBX sponsor); drives vision, acquisitions and channel network.
- **CFO & Co-Founder: Luke Duquaine** – Ex-Sangoma software engineer; oversees finance, international operations and supply-chain.
- **CTO & Co-Founder: Bryan Walters** – Long-time Asterisk contributor; leads product security and cloud architecture.
- **Chief Revenue Officer: Preston McNair** – 25+ years in channel development at Sangoma & Hargray; owns sales, marketing and partner success.
- **Chief Hospitality Strategist: Doug Schwartz** – Former 360 Networks CEO; guides hotel vertical strategy and PMS integrations.
- **Chief Business Development Officer: Bob Webb** – 30+ years telco experience (Nsight/Cellcom); cultivates ILEC/CLEC alliances for Clearly Cloud.
- **Chief Product Officer: Corey McFadden** – Founder of Voneto; architect of EPlatform UCaaS, now shapes ClearlyIP product roadmap.
- **VP Support Services: Lorne Gaetz** (appointed Jul 2024) – Former Sangoma FreePBX lead; builds 24×7 global support organisation.
- **VP Channel Sales: Tracy Liu** (appointed Jun 2024) – Channel-program veteran; expands MSP/VAR ecosystem worldwide.

---

5. Differentiators

- **Open-Source DNA:** Deep roots in the FreePBX/Asterisk community allow rapid feature releases and robust interoperability.
- **White-Label Flexibility:** Brandable phones and ClusterPBX OEM let carriers and MSPs present a fully bespoke UCaaS stack.
- **End-to-End Stack:** From hardware endpoints to cloud, gateways and compliance services, ClearlyIP owns every layer, simplifying procurement and support.
- **Education & Safety Focus:** Panic Button, CodeX and e911 tool-sets position the firm strongly in K-12 and public-sector markets.

In summary

ClearlyIP delivers a comprehensive, modular UC ecosystem—cloud, on-prem and hybrid—backed by a management team with decades of open-source telephony pedigree. Its blend of carrier-grade infrastructure, white-label flexibility and vertical-specific solutions (hospitality, education, emergency-compliance) makes it a compelling option for ITSPs, MSPs and multi-site enterprises seeking modern, secure and cost-effective communications.

DISCLAIMER

This document is provided for informational purposes only. No representations or warranties are made regarding the accuracy, completeness, or reliability of its contents. Any use of this information is at your own risk. ClearlyIP shall not be liable for any damages arising from the use of this document. This content may include material generated with assistance from artificial intelligence tools, which may contain errors or inaccuracies. Readers should verify critical information independently. All product names, trademarks, and registered trademarks mentioned are property of their respective owners and are used for identification purposes only. Use of these names does not imply endorsement. This document does not constitute professional or legal advice. For specific guidance related to your needs, please consult qualified professionals.