Voip

Introduction et Contextualisation

La VoIP (Voice over Internet Protocol) a révolutionné les communications en permettant la transmission de la voix sur des réseaux IP tels qu'Internet. Cette technologie repose sur un ensemble de protocoles pour établir, maintenir et sécuriser les appels vocaux. Dans cette analyse, nous explorerons les protocoles clés, les solutions de sécurité telles que SSL, TLS et SRTP, ainsi que les codecs audio pour la compression et la qualité audio.

Présentation Fonctionnelle

La VoIP utilise des protocoles comme SIP (Session Initiation Protocol) et IAX (Inter-Asterisk eXchange) pour établir et gérer les sessions de communication, ainsi que RTP (Real-time Transport Protocol) pour le transport des données audio et vidéo. SIP est un protocole de signalisation largement utilisé pour l'initiation, la modification et la résiliation des sessions multimédias, tandis qu'IAX, spécifique à Asterisk, offre des fonctionnalités avancées et une gestion efficace de la bande passante.

Protocoles de Sécurité

- **SSL (Secure Sockets Layer) / TLS (Transport Layer Security)** : Ces protocoles sécurisent les communications en ligne en chiffrant les données échangées entre les clients et les serveurs. Ils sont utilisés pour sécuriser les échanges de signalisation SIP et IAX, ainsi que les flux de média avec SRTP.
- **SRTP (Secure Real-time Transport Protocol)** : SRTP est une extension de RTP qui ajoute des mécanismes de sécurité, tels que le chiffrement et l'authentification, pour protéger les flux de média en temps réel contre l'interception et la manipulation.
- **IPsec (Internet Protocol Security)** : IPsec fournit des fonctionnalités de sécurité au niveau du réseau en assurant l'authentification, l'intégrité et la confidentialité des données IP. Bien que moins couramment utilisé dans les déploiements VoIP grand public, IPsec peut être utilisé pour sécuriser les communications entre des réseaux VoIP distants.

Codecs Audio

Les codecs, ou codeurs-décodeurs, sont des algorithmes logiciels ou matériels qui compressent et décompressent les données audio et vidéo. Leur fonction principale est de réduire la taille des fichiers audio et vidéo afin de permettre un transfert plus efficace sur les réseaux de communication, tout en maintenant une qualité audiovisuelle acceptable.

Les codecs peuvent utiliser différentes techniques de compression, telles que la compression avec perte (lossy) ou la compression sans perte (lossless). Les codecs avec perte éliminent certaines données jugées moins importantes pour la perception humaine, tandis que les codecs sans perte préservent l'intégralité des données originales.

Dans le contexte de la VoIP, les codecs audio sont utilisés pour compresser la voix afin de réduire la bande passante nécessaire pour les transmissions vocales sur les réseaux IP. Certains des codecs audio les plus couramment utilisés dans les systèmes VoIP comprennent G.711, G.729 et Opus. Chaque codec a ses propres caractéristiques en termes de qualité audio, de débit binaire et de complexité de traitement, ce qui influence son choix en fonction des besoins spécifiques de l'application VoIP.

Certains des codecs les plus couramment utilisés dans les systèmes VoIP comprennent :

- **G.711** : Un codec standard qui offre une qualité audio haute fidélité mais utilise une bande passante plus importante.
- **G.729** : Un codec à débit binaire réduit qui offre une qualité audio acceptable tout en conservant une consommation de bande passante minimale.
- **Opus** : Un codec open source conçu pour la voix et l'audio en temps réel, offrant une qualité audio élevée avec une efficacité de bande passante optimale.

Conversion Analogique-Digitale

Les codecs convertissent un signal analogique en un signal numérique. Voici comment cela fonctionne généralement :

1. **Échantillonnage** : Le signal analogique, tel que la voix, est échantillonné à des intervalles réguliers dans le temps. À chaque intervalle, la valeur du signal est mesurée et enregistrée. Cette étape produit une série de points de données qui représentent le signal analogique.
2. **Quantification** : Les valeurs échantillonnées sont ensuite quantifiées, c'est-à-dire qu'elles sont arrondies à des valeurs discrètes. Par exemple, dans un signal audio numérique, chaque échantillon peut être représenté par un nombre entier correspondant à son amplitude.
3. **Codage** : Enfin, les valeurs quantifiées sont encodées numériquement pour former une représentation numérique du signal. Cette représentation peut être sous forme binaire (0 et 1) ou sous une autre forme, selon le codec utilisé.

Une fois que le signal analogique a été converti en signal numérique par le codec, il peut être transmis sur un réseau numérique, tel qu'Internet, et décodé à nouveau à destination pour être reproduit sous forme de signal analogique audible. Le processus inverse est utilisé pour convertir le signal numérique en signal analogique à destination, ce qui permet à la personne de recevoir le son original.

Avantages et Inconvénients

Avantages :

- Réduction des coûts de communication.
- Flexibilité et portabilité des appels.

- Intégration avec d'autres applications et services.
- Fonctionnalités avancées telles que la messagerie vocale et la vidéoconférence.

Inconvénients :

- Dépendance à Internet.
- Risques de sécurité, notamment l'interception et la fraude.
- Qualité de service variable en fonction de la bande passante et de la congestion du réseau.

Solutions Existantes sur le Marché (Open Source/Payantes)

- **Open Source** : Des solutions telles qu'Asterisk, FreeSWITCH et Kamailio offrent une flexibilité et une personnalisation élevées, ainsi que des options de sécurité telles que SRTP et l'utilisation de protocoles SSL/TLS.
- **Payantes** : Les entreprises comme Cisco, Avaya et Microsoft proposent des solutions VoIP intégrées avec des fonctionnalités avancées et un support professionnel, y compris des protocoles de sécurité comme SSL/TLS et SRTP.

Exemples d'Implémentation

- Une petite entreprise utilise Asterisk avec le protocole IAX pour ses communications internes et externes, avec le codec G.729 pour une utilisation efficace de la bande passante.
- Une organisation gouvernementale déploie un système de téléphonie VoIP sécurisé en utilisant Asterisk avec SSL/TLS pour chiffrer les communications SIP et IAX, ainsi que SRTP pour sécuriser les flux de média, avec le codec Opus pour une qualité audio optimale.
- Un centre d'appels utilise une solution VoIP basée sur le cloud, avec une architecture basée sur SIP pour la gestion des appels entrants et sortants, et IAX pour la connexion aux serveurs Asterisk distants, avec le codec G.711 pour une qualité audio haute fidélité.

***installation d’Asterisk**

Commande	Description
`apt update && apt upgrade -y`	Met à jour la liste des paquets disponibles (**`apt update`**) puis procède à la mise à niveau de tous les paquets installés sur le système (**`apt upgrade -y`**). Le **`-y`** indique que toutes les questions de confirmation seront répondues automatiquement par "oui".
`cd /usr/src`	Change le répertoire de travail actuel vers **`/usr/src`**. Cela est souvent utilisé pour la compilation et l'installation de logiciels à partir des sources.
`wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz`	Télécharge le fichier source compressé pour Asterisk version 18 depuis le site officiel d'Asterisk.
`wget https://downloads.asterisk.org/pub/telephony/libpri/libpri-current.tar.gz`	Télécharge le fichier source compressé pour la bibliothèque libpri depuis le site officiel d'Asterisk.
`wget https://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz`	Télécharge le fichier source compressé pour le pilote DAHDI depuis le site officiel d'Asterisk.
`apt install build-essential wget libssl-dev libncurses5-dev libnewt-dev libxml2-dev linux-headers-$(uname -r) libsqlite3-dev uuid-dev libjansson-dev git subversion -y`	Installe divers outils et bibliothèques nécessaires à la compilation de logiciels, y compris les en-têtes Linux, les outils de développement, Git, Subversion, etc.
`tar -xvf asterisk-*.tar.gz && tar -xvf libpri-*.tar.gz && tar -xvf dahdi-linux-complete-*.tar.gz`	Extrait les fichiers des archives compressées téléchargées pour Asterisk, libpri et DAHDI. Les commandes **`tar -xvf`** sont utilisées pour extraire (**`x`**) les fichiers d'une archive, en affichant les détails de l'extraction (**`v`**) et en spécifiant le fichier d'archive à extraire (**`f`**).
`cd /usr/src && cd dahdi-linux-complete-* && make && make install && make config`	Change le répertoire de travail vers celui contenant les sources DAHDI, puis compile (**`make`**), installe (**`make install`**) et configure (**`make config`**) le pilote DAHDI. Les commandes **`make`**, **`make install`** et **`make config`** sont des étapes courantes de la compilation et de l'installation de logiciels à partir des sources.
`cd /usr/src && cd libpri-* && make && make install`	Change le répertoire de travail vers celui contenant les sources libpri, puis compile (**`make`**) et installe (**`make install`**) la bibliothèque libpri.
`cd /usr/src && cd asterisk-* && contrib/scripts/get_mp3_source.sh && contrib/scripts/install_prereq install && ./configure && make menuselect && make && make install && make samples && make config && ldconfig`	Change le répertoire de travail vers celui contenant les sources Asterisk, exécute des scripts pour configurer les dépendances, puis configure, compile, installe, configure les échantillons et met à jour les liens de bibliothèque dynamique pour Asterisk.
`groupadd asterisk && useradd -d /var/lib/asterisk -g asterisk asterisk`	Crée un groupe système nommé "asterisk" et un utilisateur nommé "asterisk" avec un répertoire personnel défini sur **`/var/lib/asterisk`** et ajouté au groupe "asterisk".
`sed -i 's/#AST_USER="asterisk"/AST_USER="asterisk"/g' /etc/default/asterisk && sed -i 's/#AST_GROUP="asterisk"/AST_GROUP="asterisk"/g' /etc/default/asterisk`	Modifie le fichier de configuration **`/etc/default/asterisk`** pour définir l'utilisateur (**`AST_USER`**) et le groupe (**`AST_GROUP`**) d'Asterisk comme "asterisk".
`sed -i 's/;runuser = asterisk/runuser = asterisk/g' /etc/asterisk/asterisk.conf && sed -i 's/;rungroup = asterisk/rungroup = asterisk/g' /etc/asterisk/asterisk.conf`	Modifie le fichier de configuration d'Asterisk (**`/etc/asterisk/asterisk.conf`**) pour spécifier l'utilisateur (**`runuser`**) et le groupe (**`rungroup`**) d'exécution comme "asterisk".
`chown -R asterisk:asterisk /var/spool/asterisk /var/run/asterisk /etc/asterisk /var/{lib,log,spool}/asterisk /usr/lib/asterisk`	Attribue récursivement la propriété de tous les répertoires et fichiers pertinents d'Asterisk à l'utilisateur et au groupe "asterisk".
`systemctl start asterisk`	Démarre le service Asterisk.
`asterisk -rvvv`	Lance l'interface de commande d'Asterisk en mode verbeux pour effectuer des opérations de débogage et surveiller le système en temps réel.

***configuration des Endpoint dans Asterisk**

-**fichier pjsip.conf**

Configuration définissent différents aspects de la configuration d'un endpoint SIP dans Asterisk, y compris l'authentification, l'adresse de ressource originale (AOR), les paramètres de l'endpoint et les options de médias.

Ligne	Description
[167]	Cette ligne indique le début d'une section de configuration pour l'identifiant "167". Les paramètres qui suivent seront appliqués à

	cet identifiant.
auth_type=userpass	Définit le type d'authentification utilisé comme "userpass", ce qui signifie que l'authentification se fera à l'aide d'un nom d'utilisateur et d'un mot de passe.
type=auth	Indique que cette section de configuration est une définition d'authentification.
username=167	Spécifie le nom d'utilisateur associé à cette authentification, qui est "167" dans ce cas.
password=123456	Définit le mot de passe associé à l'utilisateur "167".
[167]	Cette ligne indique une nouvelle section de configuration pour l'identifiant "167", mais cette fois-ci pour une adresse de ressource originale (AOR).
type=aor	Indique que cette section de configuration est une définition d'adresse de ressource originale (AOR).
qualify_frequency=60	Spécifie la fréquence (en secondes) à laquelle cette adresse AOR doit être contrôlée pour vérifier si elle est toujours disponible.
max_contacts=1	Définit le nombre maximal de contacts autorisés pour cette adresse AOR.
remove_existing=yes	Indique si les contacts existants doivent être supprimés lorsqu'un nouveau contact est enregistré pour cette adresse AOR.
qualify_timeout=3.0	Spécifie le temps d'attente maximal (en secondes) pour une réponse lors de la vérification de la disponibilité d'un contact.
authenticate_qualify=no	Détermine si la vérification de la disponibilité doit également être utilisée pour l'authentification. Dans ce cas, elle est désactivée.
[167]	Une autre section pour l'identifiant "167", cette fois-ci pour la configuration de l'endpoint.
context=internal	Spécifie le contexte dans lequel les appels entrants seront dirigés lorsqu'ils sont destinés à cet identifiant.
auth=167	Référence à l'identifiant d'authentification utilisé pour valider les appels entrants.
aors=167	Référence à l'adresse AOR associée à cet identifiant d'extrémité.
type=endpoint	Indique que cette section de configuration définit un point de terminaison (endpoint).

language=en	Définit la langue par défaut pour les appels passant par cet endpoint comme l'anglais ("en").
deny=0.0.0.0/0.0.0.0	Indique les adresses IP ou les sous-réseaux qui sont explicitement refusés pour les appels entrants. Dans ce cas, aucun n'est spécifié, ce qui signifie qu'aucun appel n'est refusé.
trust_id_inbound=yes	Détermine si l'identifiant de l'appelant (caller ID) entrant doit être accepté comme étant fiable.
send_rpid=no	Indique si l'identifiant de l'appelant (caller ID) doit être envoyé avec les appels sortants. Dans ce cas, il est désactivé.
transport=tcp_transport	Spécifie le transport utilisé pour les communications SIP, qui est le protocole TCP dans ce cas.
rtcp_mux=no	Indique si le multiplexage RTCP (Real-time Transport Control Protocol) doit être activé. Dans ce cas, il est désactivé.
call_group=	Définit le groupe d'appel auquel cet endpoint appartient.
pickup_group=	Définit le groupe de prise d'appel auquel cet endpoint appartient.
disallow=all	Indique que tous les codecs sont désactivés par défaut pour les appels passant par cet endpoint.
allow=ulaw,alaw,gsm	Active les codecs µ-law, A-law et GSM pour les appels passant par cet endpoint.
mailboxes=300	Spécifie la boîte vocale associée à cet endpoint.
permit=0.0.0.0/0.0.0.0	Indique les adresses IP ou les sous-réseaux qui sont explicitement autorisés pour les appels entrants. Dans ce cas, toutes les adresses sont autorisées.
ice_support=no	Indique si le support ICE (Interactive Connectivity Establishment) est activé pour cet endpoint. Dans ce cas, il est désactivé.
use_avpf=no	Indique si AVPF (Audio-Visual Profile with Feedback) doit être utilisé pour cet endpoint. Dans ce cas, il est désactivé.
dtls_cert_file=	Spécifie le chemin du fichier de certificat DTLS (Datagram Transport Layer Security) pour cet endpoint. Dans ce cas, aucun n'est spécifié.
dtls_private_key=	Spécifie le chemin de la clé privée DTLS pour cet endpoint. Dans ce cas, aucun n'est spécifié.
dtls_ca_file=	Spécifie le chemin du fichier CA DTLS pour cet endpoint. Dans ce cas, aucun n'est spécifié.
dtls_setup=actpass	Définit la méthode d'établissement DTLS comme "actpass" pour cet

	endpoint.
dtls_verify=no	Indique si la vérification du certificat DTLS est activée pour cet endpoint. Dans ce cas, elle est désactivée.
media_encryption=no	Indique si le chiffrement des médias est activé pour cet endpoint. Dans ce cas, il est désactivé.
message_context=	Spécifie le contexte pour les messages SIP. Dans ce cas, aucun n'est spécifié.
subscribe_context=	Spécifie le contexte pour les abonnements SIP. Dans ce cas, aucun n'est spécifié.
allow_subscribe=yes	Indique si les abonnements SIP sont autorisés pour cet endpoint. Dans ce cas, ils sont autorisés.
rtp_symmetric=yes	Indique si la symétrie RTP (Real-time Transport Protocol) est activée pour cet endpoint. Dans ce cas, elle est activée.
force_rport=yes	Indique si le comportement de l'attribut "rport" dans les en-têtes SIP est forcé pour cet endpoint. Dans ce cas, il est activé.
rewrite_contact=yes	Indique si l'en-tête "Contact" des messages SIP doit être réécrit pour refléter les informations de routage correctes. Dans ce cas, il est activé.
direct_media=no	Indique si le support des médias directs est activé pour cet endpoint. Dans ce cas, il est désactivé.
media_use_received_transport=no	Indique si le transport reçu doit être utilisé pour les médias. Dans ce cas, il est désactivé.
callerid="linuxhelp" <167>	Définit l'identifiant de l'appelant (caller ID) sortant pour cet endpoint comme "linuxhelp" avec le numéro 167.

-**fichier extensions.conf**

configuration d'extensions.conf définissent deux règles d'extension pour le contexte "internal". Lorsque les utilisateurs composent les numéros 167 ou 168, les appels sont acheminés vers les identifiants PJSIP correspondants.

Ligne	**Description**
[internal]	Cette ligne indique le début d'une section de configuration pour le contexte "internal". Les extensions et les règles qui suivent seront applicables à ce contexte.
exten => 167,1,Dial(PJSIP/167)	Cette ligne définit une extension pour le numéro 167. Lorsque le numéro 167 est composé, l'appel est acheminé vers l'application Dial, qui compose l'identifiant PJSIP 167. Le "1" indique la priorité de cette règle.
exten => 168,2,Dial(PJSIP/168)	Cette ligne définit une autre extension pour le numéro 168. Lorsque le numéro 168 est composé, l'appel est acheminé vers l'application Dial, qui compose l'identifiant PJSIP 168. Le "2" indique la priorité de cette règle.

Conclusion

La VoIP offre une gamme de protocoles, de codecs et de solutions pour répondre aux besoins divers des utilisateurs, offrant des avantages significatifs en termes de coûts, de flexibilité et de fonctionnalités. Cependant, la sécurité et la qualité audio restent des préoccupations majeures, nécessitant l'utilisation de protocoles de sécurité comme SSL/TLS et SRTP, ainsi que le choix judicieux de codecs pour optimiser l'efficacité de la bande passante tout en préservant une qualité audio satisfaisante.