Réseaux informati

Nouvelle édition en français

Protocole SIP

Contexte VoIP, analyses avec Wireshark, protocole, et mise en oeuvre avec Asterisk

Protocole SIP

Le Protocole SIP, Session Initiation Protocol, Contexte VoIP, analyses avec Wireshark, protocole, et mise en oeuvre avec Asterisk. Support de formation sur le protocole SIP.

François-Emmanuel Goffinet

Ce livre est en vente à http://leanpub.com/protocole-sip

Version publiée le 2021-09-06

Aussi par François-Emmanuel Goffinet

Cisco CCNA 200-301 Volume 1

Cisco CCNA 200-301 Volume 2

Cisco CCNA 200-301 Volume 3

Cisco CCNA 200-301 Volume 4

Linux Administration Volume 1

Linux Administration Volume 2

Linux Administration Volume 3

Linux Administration Volume 4

Table des matières

Dédicace

À L., tendrement

Remerciements

Merci aux centaines de visiteurs quotidiens du site sip.goffinet.org.

Merci aux centres de formation et aux écoles qui m'accordent leur confiance et qui me permettent de rencontrer mon public en personne.

Avant-Propos

François-Emmanuel Goffinet est formateur IT et enseignant depuis 2002 en Belgique et en France. Outre Cisco CCNA, il couvre de nombreux domaines des infrastructures informatiques, du réseau à la virtualisation des systèmes, du nuage à la programmation d'infrastructures hétérogènes en ce y compris DevOps, Docker, K8s, chez AWS, GCP ou Azure, etc. avec une forte préférence et un profond respect pour l'Open Source, notamment pour Linux.

On trouvera ici un des résultats d'un projet d'autopublication en mode *agile* plus large lié au site web sip.goffinet.org.

Historique du document

Ce document trouve son origine dans l'expérience de l'auteur comme formateur dans plusieurs programmes de formations éprouvés dans des écoles et des centres de formation. En voici une liste non-exhaustive.

- CCNA Voice Primer (Cisco Academy)
- Base de Téléphonie IP, 40 p. (Communauté Wallonie Bruxelles)
- VOIP UC Open-Source : Architectures et Solutions, 4 j. (Evoliris)
- Formation Asterisk, 4 j. (Evoliris)
- CCNA Collaboration, 5 j. (Egilia)
- Formation SIP + Wireshark, 2 j. (Egilia)
- Formation Téléphonie IP Etat de l'Art, 2 j. (Egilia)
- Formation Asterisk, 3 j. (Egilia)
- Voix sur IP, les fondamentaux, 3 j. (AJC Formation)
- Protocole SIP, 3 j. (AJC Formation)
- Téléphonie IP, 1 j. (AJC Formation)

Public visé

Ce document s'adresse à des informaticiens en quête de savoir.

Logiciels et fichiers nécessaires

- Captures d'exemples

Introduction

Ce document intitulé “Le Protocole SIP, Session Initiation Protocol, Contexte VoIP, analyses avec Wireshark, protocole, et mise en oeuvre avec Asterisk” est un support de formation sur le protocole SIP.

Le support est composé de quatre parties : une introduction au contexte de la voix sur IP (VoIP) et des Communications Unifiées (UC), un propos sur l’analyse de trafic VoIP avec Wireshark, un guide complet de compréhension du protocole SIP et enfin des exercices de mise en oeuvre avec le logiciel populaire de téléphonie Asterisk.

La première partie est une sorte d’introduction générale porte sur le contexte de la voix sur IP (VoIP) et des Communications Unifiées (UC). On y trouve des concepts de la téléphonie du XXe siècle (POTS), une introduction générale des protocoles VoIP, une description des marchés de la VoIP, des considérations d’infrastructure, de conception et de migration. On y trouvera aussi un descriptif de matériel VoIP/SIP et des logiciels de téléphonie Open Source. Cette partie comporte deux exercices : l’un consiste à utiliser SIP nativement entre deux points qui se connectent en IP et une connexion externe au fournisseur de Téléphonie IP Anveo.

La seconde partie vous guidera dans une démarche d’analyse de trafic avec Wireshark avec des considérations sur le placement de la capture, et une attention particulière au trafic VoIP.

La troisième partie est un guide complet de compréhension du protocole SIP. On y aborde l’architetcure du protocole avec ses rôles et ses messages, un aperçu des opérations SIP mais aussi plus particulièrement la procédure INVITE, du diagnostic avec les codes de réponse, les études de cas Proxy SIP, Back-to-Back User Agent et Flux SIP Trapéziodal. Un chapitre est consacré aux extensions SIP et un autre à la sécurité du protocole. Enfin, en annexe, on trouvera une liste des RFCs relatives à SIP et une documentation pour manipuler des téléphones en ligne de commande.

La quatrième et dernière partie est une initiation pratique au logiciel Asterisk qui permet de mettre en oeuvre une solution de téléphonie IP en différentes étapes progressives. On fera dans un premier temps l’expérience FreePBX qui est une solution graphique aboutie basée sur Asterisk. Ensuite, on tentera de reproduire le service facilement avec FreePBX directement avec Asterisk Core, en ligne de commande et avec les fichiers de configuration des utilisateurs SIP et du plan d’appel (Dialplan). On trouvera trois niveaux d’exercice : base, intermédiaire et avancé.

Première partie Introduction au contexte VoIP et des communications unifiées

Introduction

Cette partie est une introduction générale aux parties qui suiavantes sur l'analyse VoIP avec Wireshark, sur le protocole SIP ou sur un logiciel de téléphonie comme Astersik.

Voici le sommaire de cette introduction :

1. POTS
2. Protocoles Multimédia
3. Marchés VoIP
4. Exercice de connexion SIP
5. Infrastructure VoIP
6. Migration VoIP
7. Conception VoIP
8. Aperçu des logiciels Open Source
9. Exemples de périphériques SIP
10. Exercices de mise en œuvre de l'infrastructure physique

1. POTS (Plain Old Telephony Systems)

Ce chapitre reprend un historique des télécoms et des problématiques propres aux réseaux de télécommunications :

- Téléphonie analogique
- Le PSTN opérateur
- L'arrivée du numérique (RNIS, BRI, PRI)
- L'adressage des points de terminaison sur les réseaux téléphoniques
- Les solutions "classiques" pour les entreprises
- Les PABX
- Les tie-trunks
- La fiabilité des réseaux PSTN (RTC ou RNIS)

1. POTS

POTS est un sigle anglais qui signifie Plain Old Telephone System que l'on peut traduire en français par "le bon vieux téléphone". Dans certains pays on parle de réseau fixe ou de téléphone fixe. Il s'agit en fait des services rendus par une ligne téléphonique analogique avant l'avènement des technologies ISDN, téléphone mobile, ADSL et VoIP.

Service POTS

Le service POTS existe depuis l'introduction du téléphone à la fin du XIXe siècle, sous une forme pratiquement inchangée pour l'utilisateur lambda malgré l'introduction de la numérotation par tonalité ou de la fibre optique en remplacement des fils de cuivre qui composaient les lignes. Outre la communication de la voix à travers le réseau RTC, on peut citer ces services communs comme :

1. Voicemail, service de boîte vocale
2. Caller ID, service d'identification de l'appelant
3. Call waiting, service de mise en attente
4. Speed dialing, composition rapide
5. Conference call (three-way calling), chambres de conférences
6. Enhanced 911, services d'urgences améliorés
7. Centrex, central téléphonique
8. Fac-simile (FAX), télécopie

9. Communications numériques

Le réseau RTC/PSTN utilise des technologies, des supports et des protocoles différents de ceux qui supportent TCP/IP.

Les principaux concepts utiles à retenir sont :

1. Communications numériques mais à commutation de circuit
2. Architecture : Boucle locale/Trunks
3. Compostion Pulse Dialing/DTMF
4. Trunks
5. Numérotation standard E.164
6. Signalisation SS7

Ils permettent de mieux comprendre les architectures de connexions d'accès aux téléphones des entreprises et des particuliers sur lignes fixes et mobiles. Des interfaces et des protocoles permettent de connecter les deux mondes RTC et VoIP.

2. Commutation de circuit

La commutation de circuit est un mode d'établissement d'une liaison de télécommunication pour laquelle :

- un chemin physique ou logique est établi entre deux équipements

et

- est bloqué pour toute la durée de la communication.

L'établissement de circuit est aujourd'hui exécutée de manière électronique.

Dans la commutation par circuit, il y a un risque de sous-utilisation du support en cas de "silence" pendant la communication.

RNIS (ISDN) est un exemple de technologie à commutation de circuit qui numérise (en format binaire par encodage) la voix en tant que service.

Le temps passé est facturé.

3. Commutation de paquet

La commutation de circuits s'oppose au principe de la commutation de paquets qui optimise le canal de transmission laissant le soin à des commutateurs intermédiaires d'acheminer les paquets (Ethernet, Wi-Fi, IP) ou en établissant des Circuits Virtuels (ATM, Frame-Relay).

Ces technologies sont facturées par quantité de données échangées.

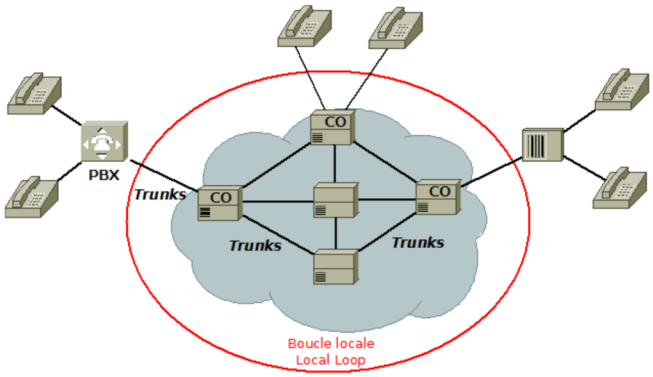
Le protocole MPLS permet de construire des réseaux IP cohérents sur ces architectures préexistantes avec une forme de confidentialité et de la gestion de qualité de service.

4. Boucle locale

Le réseau téléphonique commuté (RTC ou PSTN) peut transporter la voix mais aussi des données. Il utilise le principe de la commutation de circuit qui est celui de l'établissement d'un circuit dédié pour une communication.

Les téléphones sont connectés à des commutateurs téléphoniques (manuels, automatiques, électroniques) qui constitue des points d'échange téléphonique.

Ils sont situés chez l'opérateur au **central office (CO)** ou dans l'entreprise (en tant que Private Branch Exchange, PBX).



Boucle locale

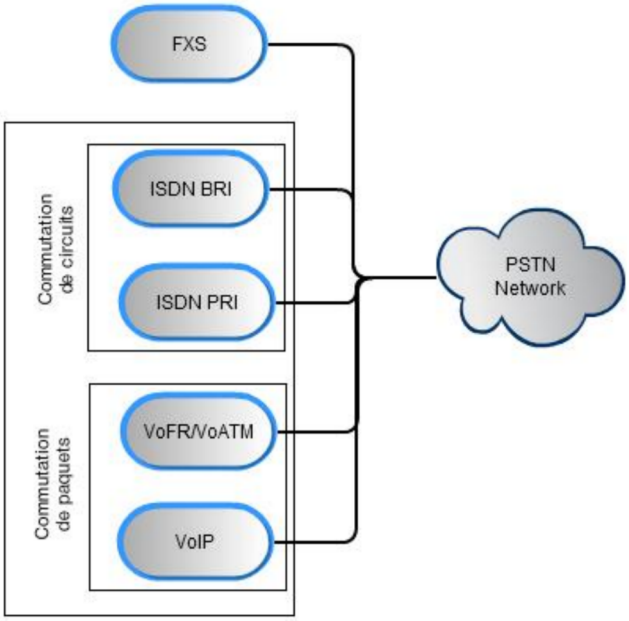
Ces commutateurs s'interconnectent entre eux via des **Trunks numériques ou analogiques**.

Si le nuage opérateur fonctionne entièrement en technologies numériques, du client à l'opérateur il reste souvent une connexion analogique avec des fréquences audibles pour transmettre la voix et la signalisation (Dial Tone Multi Frequency, DTMF). Cette zone est appelée **boucle locale** du CO de l'opérateur au bâtiment du client par une paire (téléphonique) de fils en cuivre.

5. Trunk

Un trunk est une liaison spéciale vers le réseau PSTN. Les opérateurs proposent des services numériques sur la boucle locale analogique et parmi ceux-ci le transport de la voix :

- sur ISDN
- mais ausssi sur TCP/IP supporté par des technologies d'accès plus intéressantes telles que xDSL, DOCSIS (câble/Fibre), Metro Ethernet, etc.



Chaque communication vocale numérisée prend 64 Kbps de bande passante.

Sur une technologie à commutation de circuits comme ISDN cette bande passante est monopolisée (même le silence est codé).

Sur une technologie à commutation de paquets, comme TCP/IP cette bande passante est optimisée en fonction de l'occupation.

6. Signalisation dual-tone multi-frequency signaling (DTMF)

La signalisation **Dual-tone multi-frequency signaling (DTMF)** est celle qui est utilisée "in band", c'est-à-dire dans le canal de communication, pour établir les destinations des appels auprès d'un central téléphonie privé ou public. DTMF est utilisé sur les claviers alphanumériques téléphoniques qui ont peu à peu remplacé les cadran à disque. Chaque touche correspond à deux fréquences audibles qui sont jouées simultanément.

Fréquences de touches DTMF :

	1209 Hz	**1336 Hz**	**1477 Hz**	**1633 Hz**
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

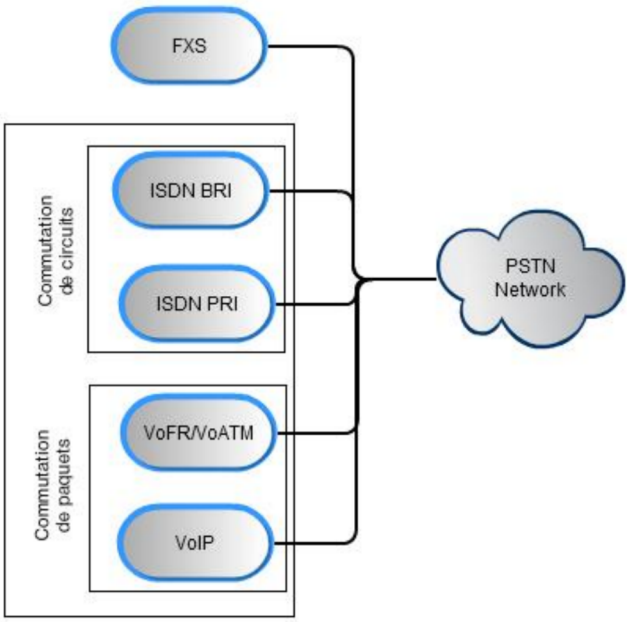
Certaines fréquences audibles sont réservées, en Belgique :

	Fréquence en Hz	Cadences en secondes
Busy tone	425	0.5 on 0.5 off
Congestion tone	425	0.167 on 0.167 off
Dial tone	425	continuous
Special dial tone	425	1.0 on 0.25 off
Holding tone	1400	0.4 on 15.0 off
Ringing tone	425	1.0 on 3.0 off
Special information tone	900/1400/1800	3x0.33 on 1.0 off
Call waiting tone	1400	0.175 on 0.175 off 0.175 on 3.50 off

7. FXO/FXS

En téléphonie, un **Foreign eXchange Station ou FXS** est une interface téléphonique qui **fournit la tonalité**, le courant de charge et la tension électrique nécessaire pour faire fonctionner la sonnerie.

Un périphérique qui connecte un FXS est une interface FXO qu'elle soit un téléphone analogique ou l'interface d'un PBX pour recevoir des appels. L'interface **Foreign eXchange Office** est le port qui reçoit la ligne analogique.



8. ISDN/RNIS

8.1. Définition

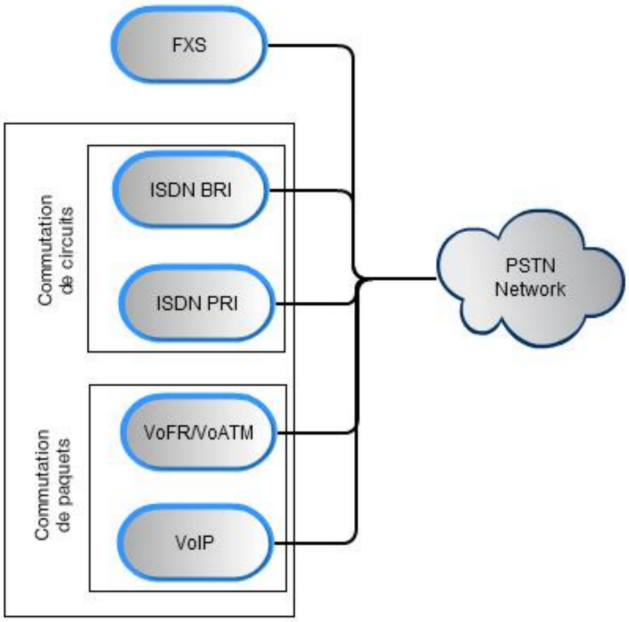
ISDN (Integrated Services Digital Network), RNIS en français, est une technologie qui utilise la boucle locale pour fournir divers services de transmission numériques de la voix, de la vidéo et des sonnées. ISDN permet de se connecter au réseau PSTN, à Internet, à des sites distants.

ISDN fournit plusieurs type de canaux numériques :

1. Canaux B de 64 Kbps pour la voix et les données (1 canal B = un canal voix)
2. Canal D de 16 Kbps pour la signalisation.

8.2. Accès de base BRI

L'accès de base ou Basic Rate Interface (BRI ou T0) comprend deux canaux B et un canal D. Soit un total de deux canaux voix simultanés ou 128 Kbps de bande passante.



8.3. Accès primaire PRI

L'accès primaire (PRA) ou Primary Rate Interface (PRI ou T2) propose trente canaux B et un canal D. Soit un total de 30 canaux voix simultanés ou 2 Mbps de bande passante. Ce type de ligne à 2 Mbps se vend aussi comme ligne dite E1.

9. Numérotation standard E.164

E.164 est une recommandation ITU-T qui définit le plan de numérotation international utilisé dans le réseau PSTN. Il définit aussi le format des numéros de téléphone de maximum 15 chiffres et habituellement écrits avec un sigle + en préfixe.

10. Signalisation SS7

Signaling System #7 (SS7) ou système de signalisation #7 est un ensemble de protocoles de signalisation téléphonique qui sont utilisés dans la grande majorité des réseaux téléphoniques mondiaux. SS7 fournit, dans le réseau téléphonique, une structure universelle pour :

1. la signalisation,
2. l'envoi de messages,

3. l'interconnexion et la maintenance réseau.

Il gère

1. l'établissement d'appels,
2. l'échange d'informations utilisateur,
3. le routage d'appels, la facturation et
4. supporte les services du réseau intelligent (en anglais Intelligent Network (IN))

L'utilisation principale de SS7 est de délivrer un appel téléphonique à travers le RTC. L'appel peut avoir à traverser plusieurs réseaux de différents opérateurs téléphoniques. (Par exemple sur un appel international ou s'il y a plusieurs opérateurs nationaux…). À chaque étape sur le chemin de l'appel les commutateurs téléphoniques ont besoin de savoir d'où vient l'appel (quelle ligne téléphonique, quel canal ou quel circuit) et vers où il va. Cela nécessite beaucoup de coordination. ISUP (ou ISDN User Part signaling) est un type de communication SS7 qui s'occupe de l'établissement d'un appel tout au long de ces différents liens. Les messages ISUP sont passés de commutateur en commutateur et à chaque point du circuit l'appel est étendu un peu plus jusqu'à l'aboutissement de l'appel (établissement de bout en bout).

Remarque : En VoIP, à l'échelle des communications globales, le protocole IETF SIP a l'ambition de remplacer SS7.

11. DSP : Digital Signal Processor

Les DSP (Digital Signal Processor) sont des puces optimisées dans le traitement numérique du signal notamment sonore et vidéo.

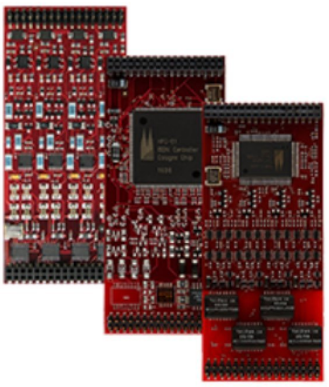
On retrouve ces puces dans des matériels divers et notamment les téléphones IP, les smartphones, etc.

Les interfaces qui connectent le monde IP aux technologies externes utilisent ces puces pour traiter le trafic VoIP. Ce matériel pourrait être utile dans la traduction de codec ou dans des oeuvres de transcodage.

12. Cartes et passerelles vocales

Pour interconnecter le réseau PSTN, des technologies numériques ou transcoder de la voix, on utilisera une passerelle vocale ou des cartes spéciales à insérer dans une passerelle. On citera le matériel fourni par :

- Digium : https ://www.digium.com/products/telephony-cards
- Beronet : http ://www.beronet.com/products/voip-gateways/
- Patton : https ://www.patton.com/voip-gateway/
- Cisco Systems



Deuxième partie Capture et Analyse de paquets avec Wireshark

Programme de formation Wireshark

L'objectif de ce chapitre est de fournir une aide aux utilisateurs qui veulent capturer et analyser des communications L2 et TCP/IP avec Wireshark.

Ce contenu est toujours en cours de conception.

En voici le sommaire :

2. Analyseurs de paquets

1. Définition

Un analyseur de paquets peut aussi être appelé en anglais : *packet analyzer*, *network analyzer*, *protocol analyzer* ou encore *packet sniffer*.

Wireshark est certainement le plus connu mais il en existe bien d'autres.

On citera en logiciels Open Source : `tcpdump`, `ngrep`, `WinDump` ,`tshark`, `dumpcap`, `rawshark`, `ipgrab`, ...

Par ailleurs, on remarquera le logiciel et le service en ligne CloudShark qui permet de présenter des captures en version Web (partages, commentaires, wireshark-like). Celui-ci ne remplit pas la fonction de capture qui est laissée à des logiciels de bas niveau.

2. Utilité

Analyser des paquets permet :

- de comprendre et d'apprendre les protocoles
- de reproduire leur comportement et de valider ces comportements
- de réaliser un audit de performance du réseau, d'identifier des problèmes dans une phase de diagnostic, d'implémenter du QoS *dans le cadre de la gestion de la bande passante*
- en cybersécurité, dans une *phase de reconnaissance passive* ou *active*, le *sniffing* permet d'interpréter les résultats d'une *prise d'empreinte par le réseau*
- dans un cadre plus défensif, les pots de miel (honeypots) et les systèmes de détection/prévention d'intrusions (IDS/IPS) utilisent la capture de trafic à des fins de journalisation ou de prise de décision
- En téléphonie, la capture de paquets aide à surveiller et à recomposer les conversations (dans un cadre légal strict : salles de marchés, services de centre d'appels, enquête légale, ...)

3. Compétences à developper

Les compétences à développer sont :

- L'identification précise des hôtes et des utilisateurs d'une conversation plongée au sein d'un trafic dense.
- Faire inter-agir les conversations accessoires pour comprendre une conversation utile.
- Etre capable d'identifier la charge d'un conversation voire la restituer.

Troisième partie Protocole SIP

3. Programme de formation SIP

Au préalable de ce chapitre sur le protocole SIP, il est conseillé de lire la partie “Contexte VoIP” où on retrouvera des généralités autour de SIP : le transport RTP, le support du NAT, les enregistrements DNS SRV et d’autres éléments opérationnels de téléphonie d’entreprise.

Sommaire

Programme de formation

Le canevas de ce support de formation est le suivant.

Architecture de SIP

Rappel sur la téléphonie classique

- Le réseau PSTN
- Les composants d’un réseau VoIP
- Les clients
- Les passerelles voix

La signalisation

- Comparaison à H.323
- Les serveurs d’application
- Les composants spécifiques au protocole SIP
- Les UA
  - UAC
  - UAS
- Les proxy

- Les registrar

Les méthodes SIP

- INVITE
- REGISTER
- ACK
- BYE
- CANCEL
- UPDATE

Les codes de statuts

- Codes provisionnels
- Codes de réussite
- Codes de redirection
- Code d'échec client
- Code d'échec serveur
- Code d'échec global

Le protocole SDP

La qualité de service

Processus d'enregistrement

- Enregistrement basique
- Messages de notification
- Les WMI
- Configuration du registrar
- Configuration des clients
- Validation de l'enregistrement

Session SIP

- Initiation du dialogue
- Requête client
- Réponse du serveur
- Routage de l'appel
- Perte du routage
- Routage strict
- Modification de la session SIP
- Terminaison de la session SIP
- Utilisation d'un proxy
- Connexion au réseau PSTN
- Gestion de la présence

Les extensions SIP

- Principe et rôles des extensions
- INFO
- COMET
- SUBSCRIBE
- PUBLISH
- NOTIFY
- MESSAGE
- REFER
- PRACK

SIP et la sécurité

- Support du NAT
- Utilisation de pare-feu (Firewalls)
- Les types d'attaques sur les réseaux convergents
- Le hijacking
- Déni de service
- Amplification
- Bots
- Les mesures de sécurité
- Contrôle des accès
- Cryptage
- Authentification
- Gestion des autorisations
- Systèmes de détection d'intrusion

4. Architecture SIP

Dans cette section, on trouvera une description du Protocole SIP comme boîte-à-outils. On décrira le concept d'AOR mais aussi on donnera une idée des rôles (UA, proxies, B2BUA), des requêtes (méthodes), des réponses et des messages du protocole SIP. Enfin, on envisagera quelques scénarios classiques à étudier.

1. Protocole SIP

Session Initiation Protocol (SIP) est un protocole TCP/IP de couche application normalisé et standardisé par l'IETF (RFC 3261). Il a été conçu pour établir, modifier et terminer des sessions multimédia. Il prend en charge l'authentification et la localisation de multiples participants. S'il se charge de la négociation des médias, il laisse le soin à d'autres protocoles de transporter du texte, de la voix ou de la vidéo.

SIP fonctionne aussi bien avec IPv4 qu'avec IPv6. SIP est supporté par TCP ou UDP sur le port 5060 par défaut. La version sécurisée SIP-TLS utilise par défaut le port TCP 5061.

SIP prend en charge cinq facettes de l'établissement et de la terminaison de communications multimédia :

- **Localisation de l'utilisateur** : détermination du système terminal à utiliser pour la communication ;
- **Disponibilité de l'utilisateur** : détermination de la volonté de l'appelé à s'engager dans une communication ;
- **Capacités de l'utilisateur** : détermination du support et des paramètres de support à utiliser ;
- **Etablissement de session** : "sonnerie", établissement des paramètres de session à la fois chez l'appelant et l'appelé ;
- **Gestion de session** : y compris le transfert et la terminaison des sessions, la modification des paramètres de session, et l'invocation des services.

SIP n'est pas un système de communications intégré verticalement. SIP est plutôt un composant qui peut être utilisé avec d'autres protocoles de l'IETF pour construire une architecture multimédia complète.

SIP ne fournit pas de services. Plus justement, SIP fournit des primitives qui peuvent être utilisées pour mettre en œuvre différents services. Par exemple, SIP peut localiser un utilisateur et livrer un objet opaque à l'endroit où il se trouve. Une seule primitive est normalement utilisée pour fournir plusieurs services différents.

La nature des services fournis rend la sécurité particulièrement importante. A cette fin, SIP fournit une série de services de sécurité, qui comporte la prévention du déni de service, l'authentification (à la fois d'usager à usager et de mandataire à usager), la protection de l'intégrité, et de services de chiffrement et de confidentialité.

2. La boîte-à-outils SIP

SIP est donc un protocole de l'IETF (il aura la préférence du marché) qui est une véritable boîte-à-outils (primitives SIP) pour établir des communications à travers l'Internet. Ses illustrations les plus immédiates sont celles de la téléphonie IP, de la voix sur IP et puis des systèmes de messageries tels que Skype, WhatsApp, etc. Mais on peut y trouver d'autres cas d'usage où des communications vocales ou vidéos peuvent intervenir dans le cadre de services de support, de fourniture de connectivité ou encore dans l'IoT ou la domotique.

Une expérience SIP pleinement vécue ne se passe pas d'autres protocoles TCP/IP, de logiciels et de leurs librairies qui le mettent en oeuvre. Aussi, SIP n'est plus nécessairement le seul protocole ou l'élément central des solutions commerciales qui nous sont offertes sur le marché.

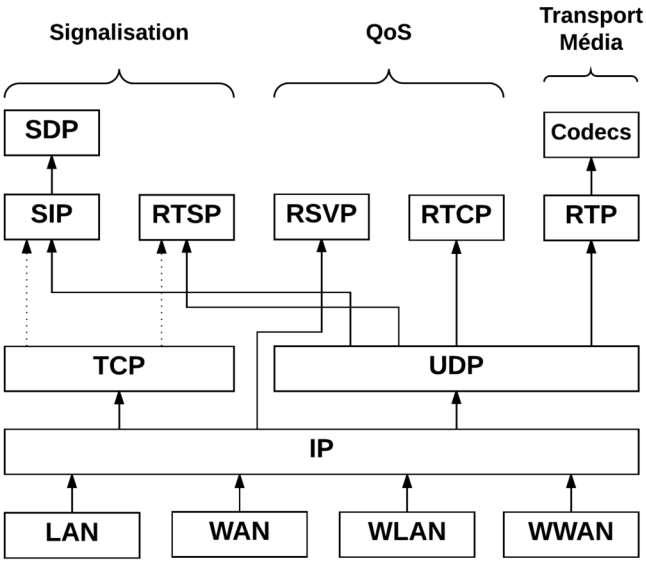


Figure : Protocoles VoIP

A cet égard, la mise en oeuvre du protocole peut provoquer des difficultés d'interconnexion entre des périphériques non supportés entre eux ; les passerelles Cisco Systems ont la faveur du marché et des opérateurs pour éviter cet écueil. Egalement, on prendra garde de ne pas confondre le message SIP rendu par l'application et l'erreur de l'application qui génère le message d'erreur. Enfin, comme boîte-à-outils, SIP aura notre préférence dans ses implémentations en "open source".

Comme protocole IETF, SIP est normalisé et standardisé IETF. Le document RFCs SIP reprend les principales RFCs relatives à SIP (il y en a plusieurs centaines) dont voici un exemple de nomenclature :

- Core SIP Documents
- SDP-Related Documents
- RTP-Related Documents
- HTTP-Related Documents
- MIME-Related Documents
- SIP Standards Track Documents (Options, Extensions, etc.)
- SIP Informational RFCs and BCP Documents
- SIP-Related Documents
- Directory Services Documents

3. AOR

Adresse d'enregistrement (AOR, Address-of-Record).

Une adresse d'enregistrement est un URI SIP ou SIPS qui pointe sur un domaine avec un service de localisation qui peut transposer l'URI en un autre URI où l'utilisateur pourrait être disponible. Normalement, le service de localisation est rempli au moyen des enregistrements. Un AOR est fréquemment vu comme l'"adresse publique" de l'utilisateur.

4. Rôles SIP

On trouvera différents rôles logiques en SIP.

4.1. User Agents (UA)

UA qui caractérisent les points d'extrémités de la communication ou un B2BUA.

- **UAC** : Un Agent Utilisateur Client est tout élément de réseau qui envoie une requête SIP et reçoit des réponses SIP. Les clients peuvent ou non interagir directement avec un utilisateur humain. Les clients et proxys d'UA sont des clients.
- **UAS** : Un Agent Utilisateur Serveur est une entité logique qui génère une réponse à une requête SIP. La réponse accepte, rejette, ou redirige la requête. Ce rôle ne dure que pendant le temps de cette transaction. En d'autres termes, si un logiciel répond à une requête, il agit comme UAS pour la durée de cette transaction. Si il génère plus tard une requête, il assume le rôle d'un UAC pour le traitement de cette transaction.

4.2. Proxy - serveur mandataire

Serveur Proxy (serveur mandataire) : Entité intermédiaire qui agit à la fois comme un serveur et comme un client pour les besoins de l'élaboration de requêtes au nom des autres clients.

Un serveur proxy joue principalement un rôle d'acheminement, de routage, ce qui signifie que sa tâche est de s'assurer qu'une requête est envoyée à une autre entité "plus proche" de l'utilisateur cible. En cela il est comparable au routeur IP qui transfère le trafic en fonction de l'adresse IP de destination.

Les proxys sont aussi utiles pour mettre en application la politique de routage des appels (par exemple, s'assurer qu'un utilisateur est autorisé à effectuer un appel).

Un proxy interprète et, si cela est nécessaire, réécrit des parties spécifiques d'un message de requête avant de le retransmettre.

Outbound Proxy : Proxy qui reçoit des requêtes de la part d'un client, même si il peut ne pas être le serveur donné par la résolution de l'URI demandée. Normalement un UA est configuré manuellement avec un mandataire de sortie, ou il peut en acquérir la connaissance au moyen de protocoles d'autoconfiguration.

Les notions de **Stateful Proxy** et et de **Stateless Proxy** se distinguent par le maintien d'un état des transactions. Alors que le proxy Stateless ne maintient aucun état, le proxy stateful peut accomplir des tâches plus complexes telles que la duplication les transactions, l'absorption des transactions ou d'autres telles que le transfert d'appel.

4.3. Serveur de redirection

Un serveur de redirection est un agent d'utilisateur serveur (UAS) qui génère des réponses 3xx (Redirection) aux requêtes qu'il reçoit, amenant le client à contacter un ensemble d'URI de remplacement.

4.4. B2BUA - Back-to-Back User Agent

B2BUA, **Back-to-Back User Agent** : Un B2BUA est une entité logique entre des UA qui reçoit une requête et la traite comme UAS. Afin de déterminer comment il devrait répondre à la requête, il agit comme un UAC vers l'UAS final et génère lui-même des requêtes. A la différence d'un serveur mandataire (proxy), il maintient l'état du dialogue et doit participer à toutes les requêtes envoyées dans les dialogues qu'il a établi. Comme c'est un enchaînement d'UAC et d'UAS, aucune définition explicite n'est nécessaire pour son comportement.

4.5. REGISTRAR Server et Location Server

Un **REGISTRAR Server** un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.

Un service de localisation est utilisé par un Redirect Server ou un serveur proxy pour obtenir des informations sur la ou les localisations possibles d'un appelé. Il contient une liste de liens de clés d'address-of-record pour aucune ou plusieurs adresses de contact. Les liens peuvent être créés et retirés de nombreuses façons.

Les URI SIPs sont très similaires dans leur forme à des adresses email : `sip :utilisateur@domaine.com`

Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.

4.6. SBC - Session Border Controller

Un **SBC (Session Border Controller)** est placé comme élément intermédiaire pour rendre des services entre les UA et les serveurs SIP en matière de sécurité, de camouflage de topologie, de filtrage ou d'assistance dans du NAT Traversal ou encore de chiffrement du trafic.

4.7. Gateways - Passerelles

Les **Gateways (passerelles)** sont des entités logiques qui sont capables d'établir des liaisons vers des destinations non-IP notamment les réseaux PSTN.

5. Requêtes (Méthodes) SIP

Le client envoie des requêtes au serveur ; serveur qui, en retour, lui renvoie une réponse. Les méthodes de base (RFC 3261) comprises dans ces requêtes sont :

- INVITE : permet à un client de demander une nouvelle session,
- ACK : confirme l'établissement de la session,
- CANCEL : annule un INVITE en suspens,
- BYE : termine une session en cours,
- OPTIONS : permet de récupérer les capacités de gestion des usagers, sans ouvrir de session,
- REGISTER : permet de s'enregistrer auprès d'un serveur d'enregistrement.

D'autres RFC sont venus compléter les capacités du protocole avec de nouvelles méthodes :

- PRACK : "Provisional acknowledgement" (RFC 3262)
- SUBSCRIBE : "Subscribes for an Event of Notification from the Notifier" (RFC 6665)
- NOTIFY : "Notify the subscriber of a new Event" (RFC 6665)
- PUBLISH : "Publishes an event to the Server" (RFC 3903)
- INFO : "Sends mid-session information that does not modify the session state" (RFC 6086)
- REFER : "Asks recipient to issue SIP request (call transfer.)" (RFC 3515)
- MESSAGE : "Transports instant messages using SIP" (RFC 3428)
- UPDATE : "Modifies the state of a session without changing the state of the dialog" (RFC 3311)

6. Réponses (Status Codes) SIP

Les réponses SIP sont présentées dans la page Réponses SIP.

Selon les contextes une réponse est attendue, les réponses possibles sont similaires aux réponses HTTP. Dans le meilleur des cas on obtient un 200 OK.

Une transaction SIP survient entre un client et un serveur et comprend tous les messages depuis la première requête envoyée du client au serveur jusqu'à la réponse finale (non-1xx) envoyée du serveur au client. Si la requête est INVITE et la réponse finale est un non-2xx, la transaction comporte aussi un ACK à la réponse. Le ACK pour une réponse 2xx à une requête INVITE est une transaction distincte.

Un dialogue est une relation SIP d'homologue à homologue qui persiste pendant un certain temps entre deux agents d'utilisateur. Un dialogue est établi par les messages SIP, comme une réponse 2xx à une requête INVITE.

> Un dialogue est identifié par un identifiant d'appel, une étiquette locale, et une étiquette distante.

- Provisional (1xx) : La requête est reçue et est en cours de traitement.
- Success (2xx) : L'action a été reçue, comprise et acceptée avec succès.
- Redirection (3xx) : Une action supplémentaire doit être prise (par l'appelant) pour compléter la requête.
- Client Error (4xx) : La requête comporte une mauvaise syntaxe et ne peut être prise en charge par le serveur.
- Server Error (5xx) : Le serveur a échoué remplir une requête apparement valide.
- Global Failure (6xx) : La requête ne peut être prise en charge par aucun serveur.

7. Messages SIP

Un message SIP est composé des éléments suivants :

1. Une ligne de départ (start-line) : `Message URI SIP/2.0`
2. Un ou plusieurs champs d'en-tête (header fields)
3. Une ligne vide indiquant la fin des champs d'en-tête.
4. Un corps de message optionnel (message body)

Un message SIP est notamment composé de champs d'en-têtes définis dans le RFC 3261 pour la signalisation et le routage des informations entre des entités SIP. SIP utilise le même format que celui qui définit un en-tête HTTP (RFC 2616). Chaque en-tête consiste en un nom de champ suivant d'un deux-points (:) et d'une valeur.

Les champs d'en-tête (header fields) peuvent être, entre autres :

1. **From** : Il indique l'identité de celui qui initié la requête SIP. Cette valeur est souvent valorisée par l'AOR de l'envoyeur. Il comprend un URI SIP ou SIPS voire un "display name" optionnel.
2. **To** : Cet en-tête indique le destinataire souhaité pour la requête SIP. Il utilise habituellement l'AOR du destinataire.
3. **Call-ID** : Il identifie un dialogue SIP de manière unique. Il est donc identique pour toutes les requêtes et les réponses SIP d'un même dialogue.
4. **Cseq** : Cet en-tête est composé d'une valeur de nombre entier et un nom de méthode. Il identifie, ordonne et séquence les requêtes SIP au sein d'un dialogue. Il permet de différencier les nouveaux messages et les retransmissions.
5. **Via** : Le champ Via indique le chemin pris par la requête et identifie où la réponse doit être envoyée. Il indique aussi le transport utilisé. Cet en-tête doit contenir un paramètre "branch" qui est utilisé pour identifier la transaction créée par la requête. Ce paramètre est utilisé aussi bien par le client que par le serveur. Il doit toujours commencer par un "magic cookie" d'une valeur de "z9hG4bK".
6. **Contact** : Cet en-tête identifie un URI SIP ou SIPS où l'UA veut adresser une nouvelle requête SIP. C'est ce champ qui permettra aux intervenant de communiquer directment entre eux.
7. **Allow** : Cet en-tête liste les méthodes supportée par l'UA qui génère le message.
8. **Supported** : Cet en-tête liste toutes extensions supportées par l'UA autre que celles définies dans le RFC 3261. Les extensions SIP sont représentées comme des étiquettes (tags) option.
9. **Require** : Identique au précédent "Supported" mais obligatoire pour aboutir la transaction.

10. **Content-Type** : Cet en-tête indique le type de corps de message (body)
11. **Content-Lenght** : Indique la longueur du corps du message en décimal. Il est obligatoire quand les messages SIP sont transportés sur TCP.

Les champs d'en-tête obligatoires dans toutes les requêtes SIP sont : `To`, `From`, `CSeq`, `Call-ID`, `Max-Forwards` et `Via`.

7.1. Exemple d'une transaction BYE-200 OK

Message	Structure
Méthodes	Nom de la méthode + URI du destinataire + Version SIP `BYE sip :201@10.33.6.101:5060 SIP/2.0`
Réponses	Version SIP + Status Code + Raison `SIP/2.0 200 OK`

Requête BYE

```
BYE sip:201@10.33.6.101:5060 SIP/2.0
Via: SIP/2.0/UDP 10.33.6.100;branch=z9hG4bKac795178845
Max-Forwards: 70
From: <sip:101@10.33.6.100;user=phone>;tag=1c782609321
To: <sip:201@10.33.6.101>;tag=1c1450530943
Call-ID: 145053037715220106222l@10.33.6.101
CSeq: 1 BYE
Supported: em,timer,replaces,path,resource-priority
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,U\
PDATE
User-Agent: IPP/v.6.20A.027.012
Reason: Q.850 ;cause=16 ;text="local"
Content-Length: 0
```

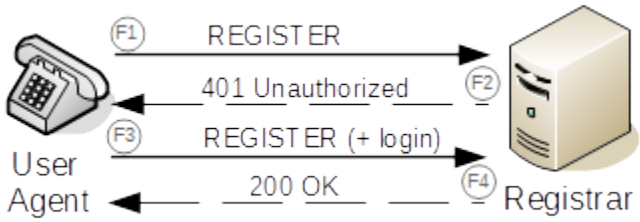
Réponse 200 OK

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.6.100;branch=z9hG4bKac795178845
From: <sip:101@10.33.6.100;user=phone>;tag=1c782609321
To: <sip:201@10.33.6.101>;tag=1c1450530943
Call-ID: 145053037715220106222l@10.33.6.101
CSeq: 1 BYE
Contact: <sip:201@10.33.6.101:5060>
Supported: em,timer,replaces,path,resource-priority
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,U\
PDATE
Server: GW/v.6.20A.027.012
Content-Length: 0
```

8. Scénarios SIP

Selon le contexte d'exécution on trouvera probablement plusieurs intervenants dans une session SIP.

8.1. Processus d'enregistrement

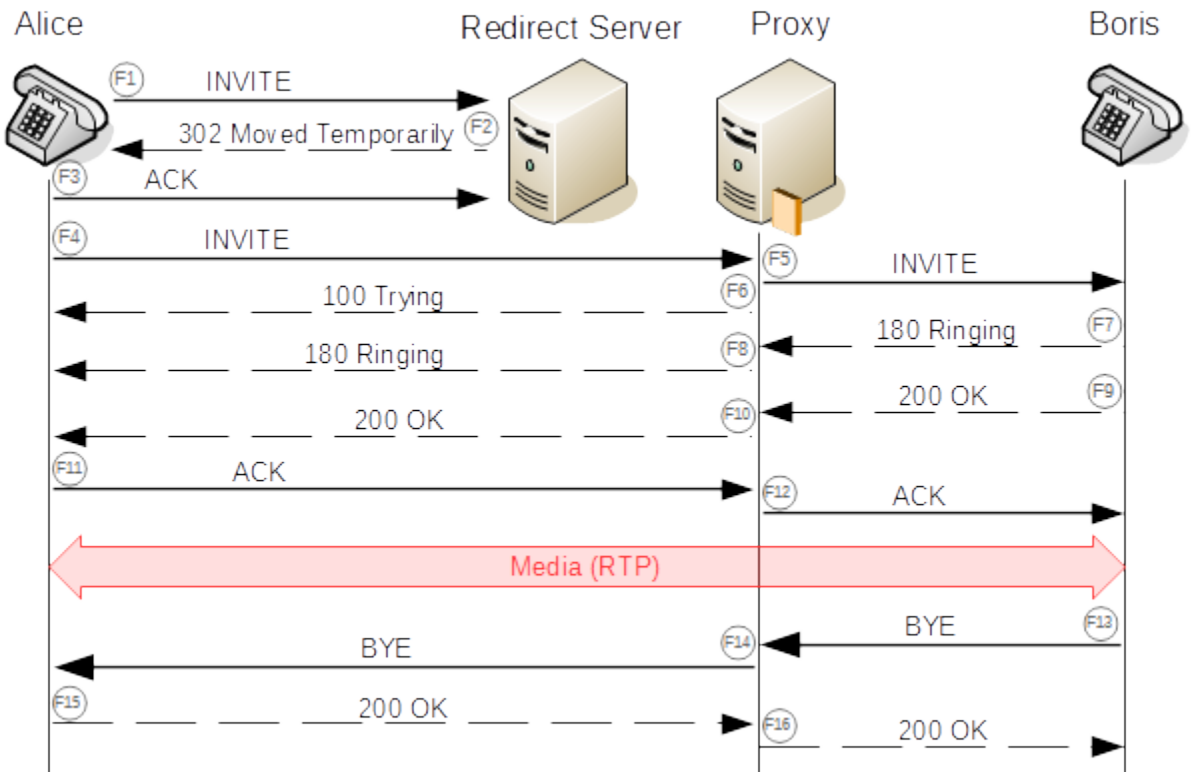


Processus d'enregistrement

Source de l'image

- F1 - demande d'enregistrement initial auprès du SIP User Agent avec ses informations d'adresse (AOR)
- F2 - réponse du SIP Registrar avec les informations sur le login nécessaire
- F3 - nouvelle demande d'enregistrement avec login
- F4 - confirmation de l'enregistrement réussi sur le SIP Registrar

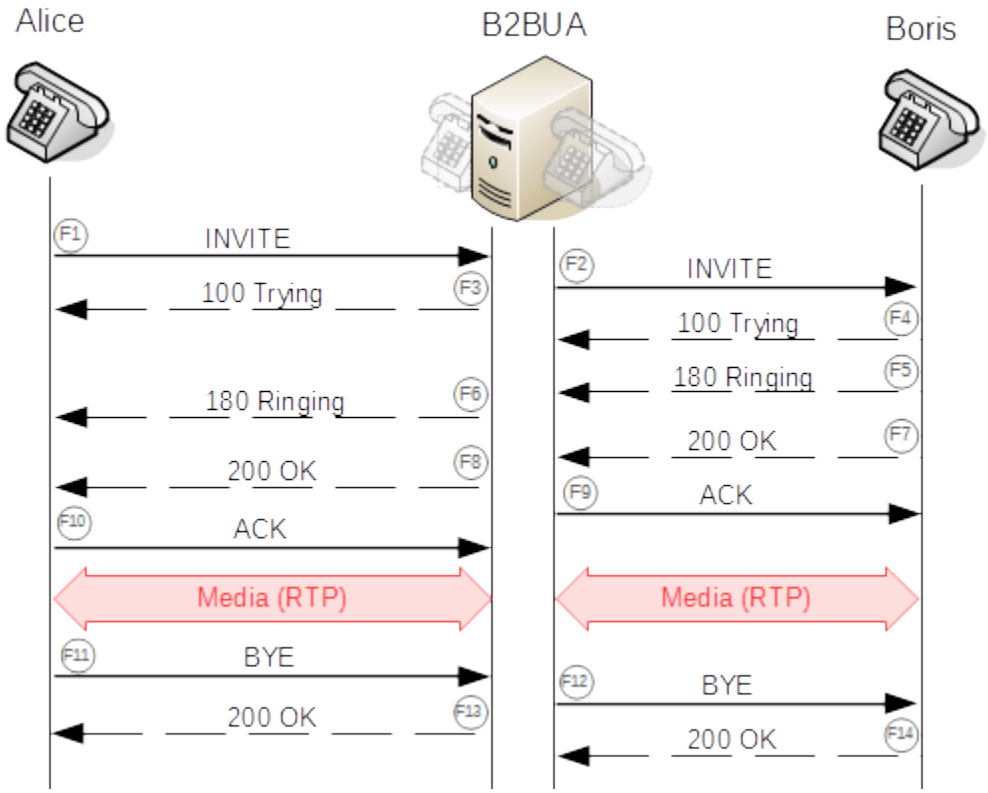
8.2. Flux d'appel SIP entre UA et serveurs de redirection entre proxys et UAs



Flux d'appel SIP entre UA et serveurs de redirection entre proxys et UAs

Source de l'image

8.3. Flux d'appel B2BUA



Flux d'appel B2BUA

Source de l'image

9. Terminologie SIP

9.1. Transaction SIP

Une transaction se compose d'une demande, de toutes les réponses non définitives (1xx) reçues et d'une réponse finale (2xx, 3xx, 4xx, 5xx ou 6xx), ainsi que des accusés de réception des réponses (ACK ou PRACK), sauf les ACK aux 2xx réponses.

> Fondamentalement, une transaction SIP est un seul échange demande / réponse finale complet.

9.2. Dialogue SIP

Un dialogue n'est qu'une série de transactions entre deux pairs SIP.

Le but d'un dialogue est de configurer, éventuellement de modifier, puis de démonter une session. D'où le nom de Session Initiation Protocol.

Comme il peut y avoir de nombreux dialogues en cours entre deux pairs SIP à tout moment (par exemple, il peut y avoir de nombreux appels simultanés en cours entre deux serveurs SIP), les dialogues sont identifiés par les champs `From`, `To` et `Call-ID` dans l'en-tête. Ainsi, si le pair SIP A reçoit deux requêtes BYE en même temps, il peut examiner ces champs pour déterminer à quel dialogue ils appartiennent.

> Fondamentalement, les dialogues sont identifiés par les champs `From`, `To` et `Call-ID` des messages SIP.

Parce qu'il peut y avoir plusieurs dialogues en cours à la fois entre deux pairs (par exemple, plusieurs appels en cours entre deux serveurs SIP), des balises ("*tags*") servent simplement à identifier à quel dialogue une requête ou réponse particulière appartient.

9.3. Session Média

Une session n'est qu'un flux média (par exemple audio ou vidéo) circulant entre pairs, généralement constitué de paquets RTP (et éventuellement RTCP).

Par exemple, si le protocole SIP est utilisé pour passer un appel vocal, la session est la donnée vocale qui est envoyée entre les terminaux.

> Les transactions et dialogues SIP sont nécessaires pour créer des sessions (des flux média entre deux pairs), une "session" étant l'objectif principal du protocole SIP.

9.4. Domaine SIP

Un domaine est un nom de domaine qui identifie les ressources SIP.

Un service DNS robuste est recommandé pour identifier les ressources SIP.

> Un domaine est un nom de domaine qui identifie les ressources SIP notamment grâce à un service DNS robuste.

Quatrième partie Asterisk PBX

Programme de formation Asterisk

On trouvera dans cette partie une suite d'exercices de mises en oeuvre du protocole SIP avec le logiciel Asterisk.

En voici le sommaire :

1. Solution FreePBX
2. Asterisk Core PABX
3. Asterisk Base
4. Asterisk Intermédiaire
5. Asterisk Avancé

5. Solution FreePBX

On propose ici un exercice d'installation et de configuration d'un IP-PBX avec Astersik/FreePBX dans le but d'illustrer le déploiement VoIP dans une PME. Plus il y a d'utilisateurs et de périphériques, plus le lab est représentatif.

1. Introduction

Source : https ://en.wikipedia.org/wiki/FreePBX

FreePBX est un GUI basé Web qui gère le serveur de téléphonie Asterisk. FreePBX est sous licence GNU General Public License version 3.

FreePBX a été acquis par Schmooze.com au début 2013 qui a été acquis par Sangoma Technologies Corporation au début 2015.

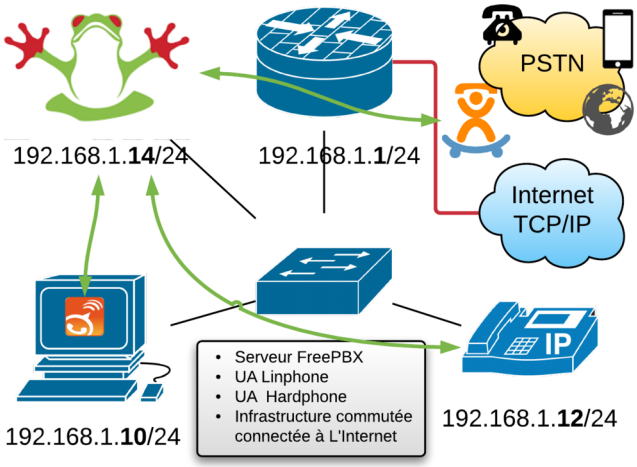
FreePBX peut être exploité :

- A partir d'une installation native combiné au logiciel Asterisk et à une base donnée.
- A partir d'une distribution FreePBX (FreePBX Distro), il existe des variantes comme AsteriskNow, Elastix ou Trixbox, FreePBX même.
- A partir d'un matériel dédié et soutenu par les auteurs du projet, en proposant des appliances : https ://www.freepbx.org/st appliances/, ce qui donne une idée du dimensionnement physique.

1.1. Fonctionnalités

PBX IP graphique complet et à usage avancé.

1.2. Topologie



Topologie

- Serveur FreePBX/AsteriskNow (2-4Go RAM, 1-2 CPU)
- UA Linphone
- UA Hardphone
- Infrastructure commutée connectée à L'Internet

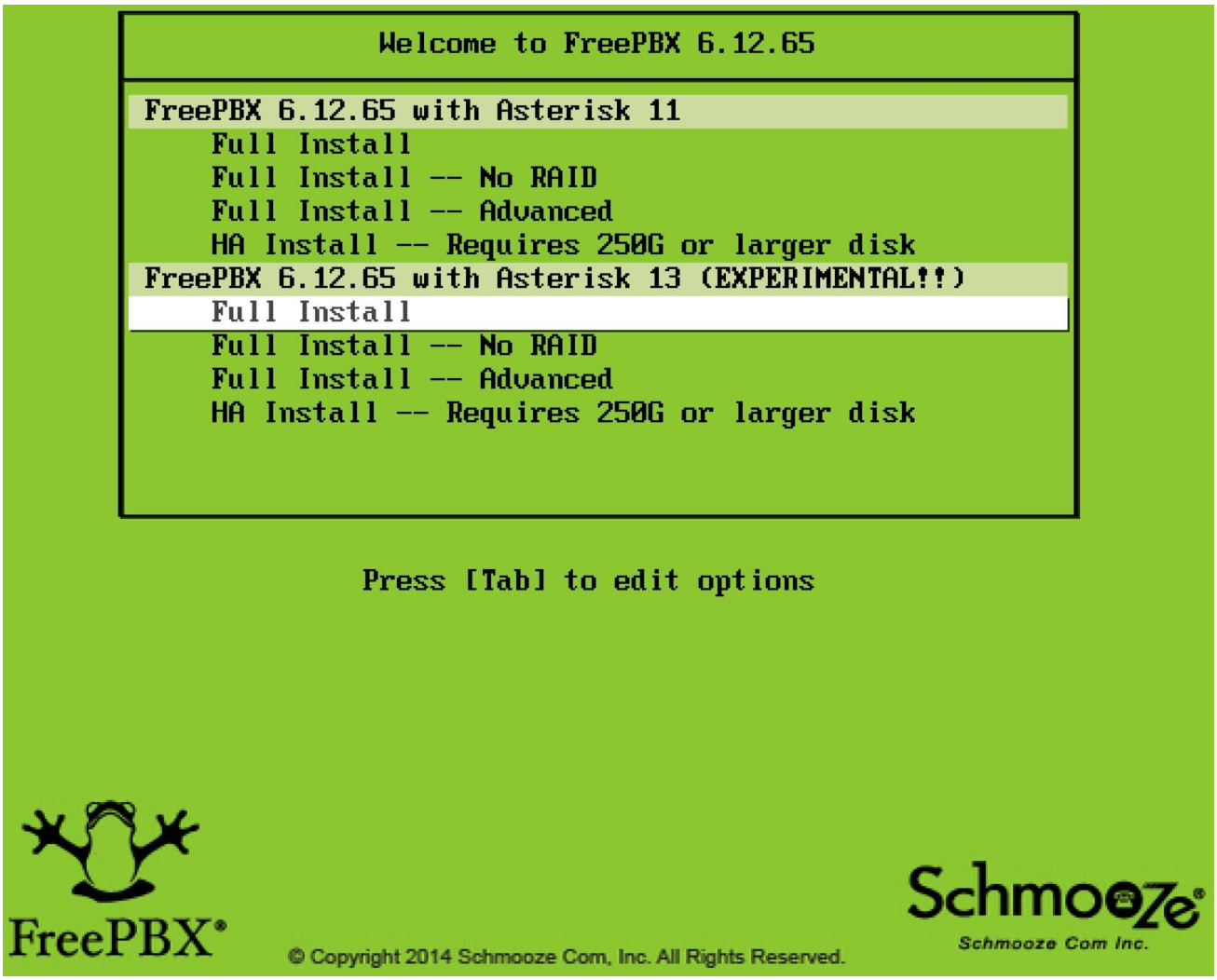
2. Installation

2.1. Procédure d'installation

Source : https ://wiki.asterisk.org/wiki/display/AST/Installing+AsteriskNOW

Télécharger le fichier `AsteriskNOW-612-current-64.iso` sur https ://www.asterisk.org/downloads/asterisknow.

Le choix se porte aujourd'hui sur une installation standard de FreePBX 6.12.65 avec Asterisk 13.



2.2 Post-installation

Après redémarrage,

- Prendre connaissance de l'adresse IP du serveur.
- Sur un autre ordinateur, aller à l'adresse http du serveur PBX.
- Remplir le formulaire de création de compte admin

Source de l'image

Le menu principal offre quatre options :

Source de l'image

1. **FreePBX Administration**
2. **User Control Panel**
3. **Operator Panel**
4. **Get Support**

Dans la suite, veuillez accomplir les actions suivantes :

- Choisir le menu **FreePBX Administration**
- Passer les étapes d'activation, firewall et SIPStation
- S'attarder sur les offres

2.3. Configuration du PBX

https ://wiki.freepbx.org/display/PPS/FreePBX+Distro+First+Steps+After+Installation

2.4. Configuration des modules

https ://wiki.freepbx.org/display/FPG/Standard+Modules

1. ~~Mise à jour des modules~~
2. Installation de nouveaux modules :
3. ~~Languages (voir plus haut)~~
4. Endpoint Manager
5. Time Conditions
6. ~~Ring Groups~~

Paramètres avancés et paramètres SIP

https ://wiki.freepbx.org/display/FPG/Advanced+Settings

- Adresse : Static
- Adresse IP publique
- Réseau local

https ://wiki.freepbx.org/display/FPG/Asterisk+SIP+Settings et https ://wiki.freepbx.org/display/FPG/NAT+Configuration+Fre

Changer éventuellement "Strong Passwords"

3. Connectivité

3.1. Ajout des extensions

Softphones SIP/IAX

- Zoiper
- Linphone
- Ekiga
- Jitsi
- Yate
- 3CX Phone
- SJPhone
- Voir https ://fr.wikipedia.org/wiki/Liste_des_logiciels_SIP#Clients_SIP

Matériel VoIP

- Polycom SoundPoint IP 321 (3)
- Cisco SPA508G (3)
- Cisco SPA504G (2)
- Cisco SPA922 (6)
- ATA Cisco PAP2T (2)
- Power and Network Devices
- PoE FS108P (4)
- Cisco PoE SF300-24P (1)

Nomenclature des numéros internes

Nom de serveur	Extensions
pbx01	2101, 2102, 2103, 2104
pbx02	2201, 2202, 2203, 2204
pbx03	2301, 2302, 2303, 2304
pbx04	2401, 2402, 2403, 2404
pbx05	2501, 2502, 2503, 2504
pbx06	2601, 2602, 2603, 2604
pbx07	2701, 2702, 2703, 2704
pbx08	2801, 2802, 2803, 2804
pbx09	2901, 2902, 2903, 2904
pbx0a	3001, 3002, 3003, 3004
pbx0b	3101, 3102, 3103, 3104
pbx0c	3201, 3202, 3203, 3204
pbx0d	3301, 3302, 3303, 3304
pbx0e	3401, 3402, 3403, 3404
pbx0f	3501, 3502, 3503, 3504

https ://wiki.freepbx.org/display/FPG/Extensions+Module+-+SIP+Extension

- Application / Extension / Add a SIP Extension
- User Extension
- Display Name
- Devices Options / Secret
- Voicemail : Enabled ...

3.2. Configuration du compte Anveo

Numéros de téléphone en format `322XXXXXXX`

https ://www.anveo.com/faq.asp ?code=sip_freepbx

- `Localized`
- `32 Belgium`
- `00`

3.3. Configuration du Trunk SIP

1. Menu “Connectivity” / “Trunks” / “Add A SIP Trunk”
   - Trunk name : “Anveo”
   - Outbound CallerID : “32XXXXXXXX”
2. Onglet “SIP Settings”
   - Trunk name : “Anveo”
   - “Outgoing Settings” -> “PEER Details”, remplacer par le **numéro de compte** et le **mot de passe** : `ini type=friend host=sip.de.anveo.com port=5010 username=ACCOUNT_NUMBER secret=SIP_PASSWORD insecure=port,invite disallow=all allow=ulaw context=from-trunk`
   - Enfin, dans “Incoming Settings” :
     - “Register String” : `ACCOUNT_NUMBER :SIP_PASSWORD@sip.de.anveo.com :5010`
     - “Submit” / “Apply”

3.4. Route sortante

Pour les numéros fixes et cellulaires :

1. “Connectivity” / “Outbound Routes”
2. “Route Name” : “Anveo”
3. “Dial patterns” : “‘ 0XXXXXXXX
   0XXXXXXXXX “‘
4. “Trunk Sequence for Matched Routes” : “Anveo”
5. “Submit” / “Apply”

3.5. Route entrante

Par numéro de téléphone routé sur le PBX :

1. “Connectivity” / “Inbound Routes”
2. “DID Number” : “32XXXXXXXX”
3. “Set Destinations” : p. ex. Extensions/numéro
4. “Submit” / “Apply”

5. Francisation

A partir de la version 13, de FreePBX, un module se charge des fichiers de langues nécessaires.

Version FreePBX 13 minimum.

1. Admin/Sound Languages
2. Filtrer selon “French”
3. Ajouter les packs de langues FR (alaw)
4. Aller dans “View Custom Languages”
5. Action/edit sur “language fr”
6. Ajouter “French” dans la description et valider
7. Revenir dans Admin/Sound Languages
8. Aller dans change “Global Sound Language”
9. Choisir French et valider

Avec les versions précédentes, 12 et inférieures, il sera nécessaire de placer soi-même les fichiers de langues FR au bon endroit.

On devrait trouver au minimum dans le dossier `/var/lib/asterisk/sounds/fr` le contenu décompressé des fichiers suivants :

- https ://downloads.asterisk.org/pub/telephony/sounds/asterisk-core-sounds-fr-alaw-current.tar.gz
- https ://downloads.asterisk.org/pub/telephony/sounds/asterisk-extra-sounds-fr-alaw-current.tar.gz
- https ://downloads.asterisk.org/pub/telephony/sounds/asterisk-moh-opsound-alaw-current.tar.gz

Plusieurs méthodes sont envisageables pour placer ces fichiers sur le PBX. Le plus facile est de se connecter sur la console du PBX et d’exécuter le script disponible à cette adresse https ://gist.github.com/goffinet/7835fb38aa1ce29544acc079ecfd

Soit, on peut l’exécuter directement dans la console Linux :

```
# wget -qO- https://gist.githubusercontent.com/goffinet/7835fb38aa1ce29544acc079e\
cfdbe6d/raw/55513cb8ac796ee8abb3ab133d3b397c619a4f31/astpbx_fr.sh | sh
```

Source du script :

```
#!/bin/sh
##1. Dans le GUI :
##Modules Administration/Download and install Languages/Apply Config
##Asterisk SIP Settings/Advanced General Settings/Language = fr/Apply config
##2. En console :
##amportal restart
##3. Téléchargement des fichiers
REP=https://downloads.asterisk.org/pub/telephony/sounds
DIR=/var/lib/asterisk/sounds/fr
mkdir $DIR
cd $DIR
wget $REP/asterisk-core-sounds-fr-alaw-current.tar.gz
wget $REP/asterisk-extra-sounds-fr-alaw-current.tar.gz
wget $REP/asterisk-moh-opsound-alaw-current.tar.gz
```

```
gunzip *.gz
tar xfv asterisk-core-sounds-fr-alaw-current.tar
tar xfv asterisk-extra-sounds-fr-alaw-current.tar
tar xfv asterisk-moh-opsound-alaw-current.tar
rm asterisk-*
```

Ensuite, on pourra définir la langue par défaut ou la langue des utilisateurs

- Modules Administration/Download and install Languages/Apply Config
- Asterisk SIP Settings/Advanced General Settings/Language = fr/Apply

6. Boîtes vocales

Au minimum, on se souciera de la livraison du courrier électronique (messages vocaux).

Sous Debian/Ubuntu :

```
apt-get -y remove exim4
```

```
apt-get -y install postfix
```

Choisir installation satellite ou Internet smarhost : serveur SMTP par exemple, **smtp.colt.net**, **relay.skynet.be**

Par exemple sous Centos 6 (AsteriskNow), une installation de type smarthost (relay SMTP) :

```
echo "relayhost = smtp.colt.net" >> /etc/postfix/main.cf
service postfix reload
```

On ira consulter la documentation officielle pour la configuration des boîtes vocales.

https ://wiki.freepbx.org/display/FPG/Voicemail

7. IVR

Admin / Feature Codes

https ://wiki.freepbx.org/display/FPG/System+Recordings+Module

https ://wiki.freepbx.org/display/FPG/IVR+Module

8. Trunk IAX2 intersites

Inter-Asterisk eXchange (IAX) est un protocole de couche application natif au logiciel PBX. Il est supporté par quelques autres produits de type systèmes PBX ou téléphones orientés OSS. Le protocole existe aujourd'hui dans sa version 2 et a été formalisé en 2010 dans le RFC 5456 de type *informational (non-standards-track)*. Il remplit aussi bien les fonctions de signalisation que de transport des medias (voix/vidéo). Il utilise un seul port UDP 4569.

IAX remplit les objectifs suivants :

- Réduction de la bande passante utilisée sur les liaisons inter-sites

- Chiffrement AES-128 inclus
- Traversée aisée des routeurs NAT et pare-feux

La documentation ci-dessous suggère une solution fonctionnelle à travers les pare-feux de connexion entre deux PBX distants. Les adresses IP publiques des systèmes téléphoniques doivent être connus.

https ://wiki.freepbx.org/pages/viewpage.action ?pageId=4161588

9. Sécurité

Activité sous Windows

https ://www.oxid.it/cain.html

1. Capture et crack de mot de passe SIP.
2. Mise en place d'une Attaque MitM ARP Poison Routing entre un PBX et deux téléphones.
3. Capture et reconstitution d'un appel.

10. Fail2ban

Dans AsteriskNow, on peut constater que la prison "pbx-gui" vérifie les logs de sécurité d'Asterisk (`/var/log/asterisk/freep`
`security.log`)

```
# fail2ban-client status
Status
|- Number of jail:       7
`- Jail list:              apache-tcpwrapper, recidive, pbx-gui, apache-badbots, ssh-iptables\
, asterisk-iptables, vsftpd-iptables
```

11. Support du Fax

...

Révisions

Page vide.