



Renouvellement des moyens téléphoniques à la DSI du CNRS

V. Chong-Wing

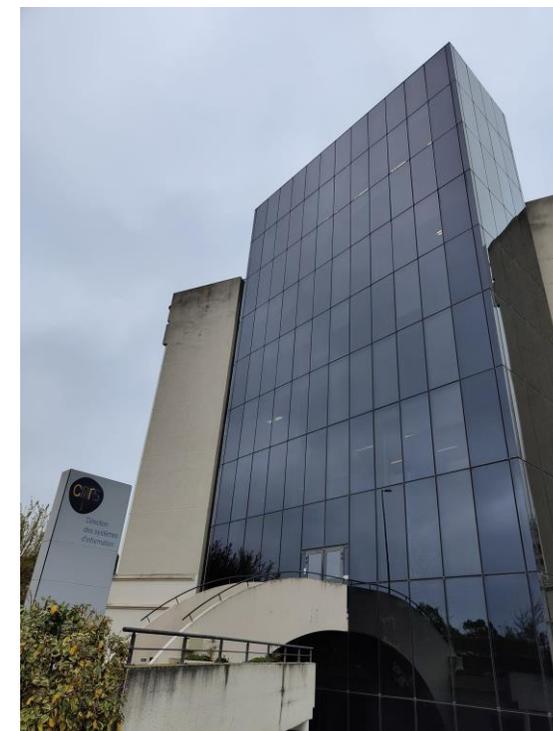
Session « ToIP » - capitoul.org

Avril 2022

Présentation générale

- **Direction des Systèmes d'Information**

- Mission : définir et mettre en œuvre les systèmes d'information de gestion et de pilotage des différentes activités du CNRS
- Périmètre : Siège (Paris), Délégations Régionales, Labos
- Organigramme :
 - Direction
 - Secrétariat général (RH, finances, logistique, ...)
 - Différents départements, dont
 - Dept Infrastructure SI
 - Equipe Ingénierie & Expertise des Infrastructures (IEI)
 - Equipe Postes de Travail (PDT)
 - Dept Sécurité SI
 - Dept Architecture Applicative
 - Equipe Assistance Utilisateurs
- Effectif 160 personnes



Contexte du projet

- **PABX historique :**

- Alcatel 4400
 - Obsolète
 - Limite de capacité des cartes numériques et analogiques
 - Difficulté pour trouver des pièces en cas de défaillance

⇒ **Risque d'interruption de service**

Service critique pour l'Assistance Utilisateurs

- **Décision lancement projet ToIP**

- Piloté par l'équipe PDT

Objectifs

Le projet vise à :

- Résorber l'obsolescence
- Disposer d'une architecture moderne, robuste et résiliente
- Augmenter la capacité du nombre de postes (200 à minima)
- Proposer de nouveaux services adaptés aux usages
 - Nomadisme
 - Télétravail

Expression du besoin

Fonctionnalités attendues

- Affichage de l'appelant
- Double appel, conférence à trois
- Renvoi d'appel (interne, externe)
- Transfert, interception
- Historique des appels (émis, reçus, manqués)
- Messagerie vocale
- ...

Expression du besoin

Fonctionnalités spécifiques

au groupement d'appel « Assistance Utilisateurs »

- SVI, Numéro unique
- Possibilité d'avoir 8 agents à minima
- Distribution séquentielle ou circulaire des appels
- Gestion simplifiée et rapide des messages du serveur vocal
- Entrée et sortie du groupement par simple touche
- Possibilité d'appeler un agent directement, indépendamment du groupement

- **Exigences d'intégration**

- Robustesse (redondance)
- Nombre limité d'éléments physiques (virtualisation)
- No Cloud !
- Déploiement en mode « greenfield » :
 - La nouvelle infrastructure ne partage aucun élément avec le PABX historique
 - Tests et recettes avant la migration
 - Réversibilité
- Conforme aux recommandations ANSSI
(https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_securiser_ToIP_NoteTech-v1.pdf)
 - Cloisonnement
 - Chiffrement
 - Contrôle d'accès au réseau
 - No Cloud !

Conformité du LAN

- Equipements réseau d'extrémité supportant :
 - PoE
 - LLDP-MED (auto-découverte du VLAN Voix)
 - Authentification 802.1x (contrôle d'accès au réseau)
- Câblage



Au choix :

- Appel d'offres
 - Procédure longue
 - Peu de ressources disponibles en interne
- Marché UGAP
 - Solution Alcatel
 - Titulaire : Resadia (national), Scopelec (régional)

Solution ToIP proposée

- **Alcatel Omni PCX Enterprise**

- Appliance virtuelle
- Support ESXi, Hyper-V, KVM

- **200 poste IP Alcatel 8028s**

- Protocole propriétaire NOE
- Micro-switch, 2x ports 1Gb/s

- **1 poste Alcatel 8058s**

- dédié POPC

- **Serveur d'administration OmniVista 8770**

- Serveur physique

- **Serveur vocal 4645**

- **Serveur OMS (**



Lien opérateur

- **Trunk SIP**

- Migration des 200 SDAs du T2 historique

- **Installation**

- Fibre optique
 - Cheminement simple
 - Surcoût important si double adduction
- Routeur

Mise en conformité du LAN

- **Existant :**

- Equipements réseaux disparates, vieillissants et obsolètes
 - Cisco C2950, 2970, 3550, ...
- Injecteurs PoE pour bornes Wi-Fi

- **Nouveaux switches :**

- Catalyst C9200L-48P-4X
 - 48 ports full PoE+, 4x 1/10G fixed uplinks, StackWise-80, 80 Gbps
 - Alimentation redondante
- Stacks de 2 ou 3 membres
 - Double attachement au cœur de réseau

Mesures de sécurisation

- **Cloisonnement**

- Isolation de l'infrastructure ToIP par rapport aux réseaux de données existants
- Séparation des flux voix et data

- **Chiffrement**

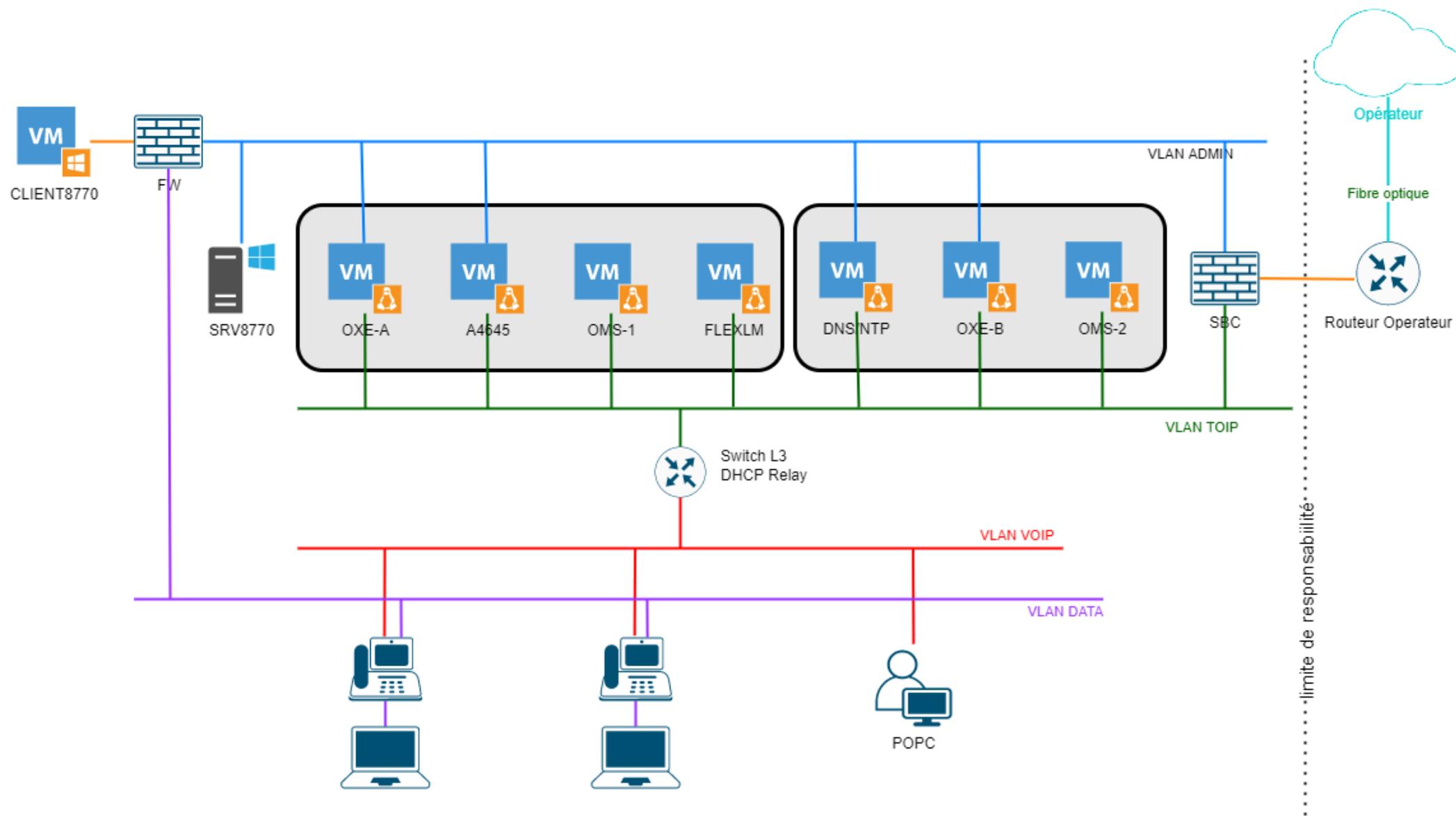
- Voix et Signalisation
- dTLS

- **Authentification**

- Contrôle d'accès au réseau (802.1x)
- Méthode eap-tls (certificat)

- **Sécurisation du trunk SIP**

- Mise en place de SBC (Session Border Controller)
 - Mécanisme de normalisation et de routage SIP
 - Amélioration de la défense du périmètre contre les attaques DoS
 - Monitoring avancés pour analyser et optimiser les services VoIP
 - Haute disponibilité (2x boîtiers Mediant 800)



- **Répartition des coûts**

- 20% Licences & matériels
- 40% Prestations:
 - Ingénierie,
 - Intégration,
 - Transfert de compétences
- 40% Maintenance, support logiciel et matériel sur 5 ans

Questions ???