e·santé Occitanie
Connecter pour mieux soigner

Prérequis pour l'usage de la visioconférence

TABLE DES MATIÈRES

Contact : pastel@esante-occitanie.fr

1 - Lieu de l'activité de Télémédecine

La salle ou le bureau choisi pour l'activité télémédecine doit être propice au secret médical et adapté aux personnes à mobilité réduite.
L'espace doit être suffisant pour accueillir tous les participants et intervenants. Vous devez avoir la possibilité d'occulter les ouvertures (portes, fenêtres...).
Du mobilier de bureau doit être installé, des prises électriques ainsi qu'une prise réseau, dédiées doivent être disponibles à portée de l'endroit où vous souhaitez installer le système.

2 - Poste de travail configuration bureau

2.1 Recommandation matérielle

CPU Intel Core i5, 2.5GHz ou supérieur (jusqu'à 720p 30 images seconde en émission et 1080p 30 images seconde en réception)
RAM : 4 Go / Mémoire vidéo minimum 256 Mb
Ecran 24 pouce, 16/9, 1920 x 1080. Minimum 1280 x 720

2.2 Système d'exploitation

Windows 7, W8, W8.1, W10 - 32/64 bit
Mac OS X Yosemile 10.10, El Capitan 10.11, Sierra 10.12

3 – Réseau

Nous vous présentons ci-après les différents prérequis pour la mise en place d'une solution de Vidéoconférence sur IP ainsi que les mécanismes de Qualité de Service à mettre en œuvre.
Le bon fonctionnement de la vidéoconférence IP dépend de plusieurs paramètres :

- La qualité de la **connexion physique**
- La priorisation des **flux Vidéoconférence** (qualité de service QoS)
- La disponibilité des **réseaux LAN & WAN**

3.1 Prérequis LAN/WAN/Sécurité

3.1.1 Connexion physique

Pour assurer une bonne connexion au réseau local, il est nécessaire de remplir les conditions suivantes :

- Câblage de catégorie 5 (minimum)
- Connexion 100 Mbps Full Duplex directe sur un commutateur (switch d'extrémité) sachant gérer la QoS.

La connexion sur un câble de catégorie inférieure peut engendrer des erreurs physiques et entraîner des pertes de paquets voix/image, donc de dégrader la qualité de la voix et de l'image.
Pour assurer une bonne transmission de la vidéoconférence, le réseau doit remplir les conditions suivantes :

- Réseau commuté 100 Mbits/s
- Pas d'utilisation de hub comme concentrateur (chaque composant sur un port séparé d commutateur)
- Tous les composants réseaux concernés par le projet doivent supporter au minimum la norme802.1d (couche 2)
- Tous les composants réseaux concernés par le projet doivent être conformes aux standards RFC 2474 (DiffServ) et RFC 791 (Type of Service ToS).

3.1.2 Gestion de la qualité de service QoS

Les éléments actifs du réseau doivent permettre une **priorisation des flux vidéoconférence par rapport aux flux Données** et respecter le standard IEEE 802.1p.
Ce mécanisme de gestion de la QoS est un service de bout en bout implémenté au niveau 2 c'est- à-dire que l'indication sur la priorité d'un flux se situe dans l'en-tête de la trame Ethernet.

Les 3 paramètres de performance réseau impactant sur la QoS de la vidéoconférence sur IP sont :

- Le temps de latence : délai de réponse du réseau
- La gigue : variation du temps de latence
- Le taux de perte de paquets : chaque paquet perdu fait disparaître un ou plusieurs échantillons du flux vidéoconférence.

Afin de conserver une bonne qualité lors du transport de la vidéoconférence sur IP :

- Le temps de latence doit être **inférieur à 60 ms**
- La gigue **ne doit pas dépasser 20 ms**
- Le taux de perte de paquets doit être inférieur ou égal à 1%

3.1.3 Bande passante sur le WAN

Le déploiement de la vidéoconférence sur IP entre sites distants interconnectés par un réseau étendu (WAN) nécessite de préférence une **adresse IP privé par site**.
Pour effectuer un appel point à point, audio et vidéo, tout en diffusant un document ou une présentation électronique, un minimum **de 512 kbps** de bande passante est préférable pour la bonne tenue d'une réunion (résolution de type DVD), **et** jusqu'à **1 MB** pour une réunion en Haute définition, voire **1,7 MB** pour une réunion en Full HD.

3.2 Configuration du pare feu (firewall)

Certains firewalls et routeurs disposent de fonctionnalités SIP et H.323 ALG. Cela permet au firewall ou au routeur d'identifier, d'inspecter et parfois de modifier les messages liés au trafic SIP et H.323 lorsqu'ils traversent le firewall ou le routeur.
ATTENTION : Si votre firewall a une fonction qui autorise à intercepter et altérer les messages SIP ou H.323, vous devez désactiver ces services. Si ce n'est pas le cas ; ce service peut provoquer des échecs d'appels.

Il est à noter que les standards SIP et H.323 sont en développement constant. Il est donc important de disposer des dernières versions logicielles sur les firewalls ou routeurs.

Définitions :

IP address of external client: Adresse IP publique de la station visioconférence

RPAD system public IP address: Adresse IP du serveur d'approvisionnement (91.247.75.148)

SIP Signaling :

SRC IP	SRC Port	Protocol	DST IP	DST Port	Description
IP address of external SIP client	>1023	TCP	RPAD system public signaling IP address	5060[1]	SIP (TCP 5060) connection from the WAN to the RPAD system
IP address of external SIP client	>1023	UDP	RPAD system public signaling IP address	5060	SIP connection from the WAN to the RPAD system
IP address of external SIP client	>1023	TCP	RPAD system public signaling IP address	5061[2]	SIP TLS (TCP 5061) connection from the WAN to the RPAD system
RPAD external signaling IP address	13001–15000	TCP	Public signaling IP address of the other SIP system	>1023[3]	Outbound SIP call from the RPAD system to another system
RPAD external signaling IP address	5060[1]	UDP	IP address of remote user SIP client	>1023	Outbound SIP call from the RPAD system to the remote user's SIP client

[1] 5060 is the default SIP external listening port on the RealPresence Access Director system. If you change this external port or add other SIP external listening ports on the RealPresence Access Director system, the ports must also be changed or added on the firewall.

[2] 5061 is the encrypted (TLS) SIP external listening port on the RealPresence Access Director system.

[3] Outbound calls normally resolve to TCP or UDP 5060 or TCP 5061 but DNS SRV queries may indicate any TCP or UDP port >1023.

H.323 Signaling :

SRC IP	SRC Port	Protocol	DST IP	DST Port	Description
IP address of external H.323 device	>1023	UDP	RPAD system public signaling IP address[1]	1719[2]	H.225 registration request from a remote endpoint to the RPAD system
Public signaling IP address of the other enterprise system	>1023	UDP	RPAD system public signaling IP address	1719	Inbound H.225 Location ReQuest (LRQ) to the RPAD system (suggested)
IP address of external H.323 device	>1023	TCP	RPAD system public signaling IP address	1720[3]	H.225 connection from the WAN to the RPAD system
IP address of external H.323 device	>1023	TCP	RPAD system public signaling IP address	10001–13000	H.245 connection from the WAN to the RPAD system
RPAD external signaling IP address	10001–13000	TCP	IP address of external H.323 device	1720	H.225 connection from the RPAD system to the WAN
RPAD external signaling IP address	10001–13000	TCP	IP address of external H.323 device	>1023	H.245 connection from the RPAD system to the WAN

[1] The RealPresence Access Director system public signaling IP address refers to the public IP address for signaling mapped on the firewall located between the WAN and the RealPresence Access Director system.

[2] 1719 is the default listening port on the RealPresence Access Director system used by remote H.323 endpoints to request registration.

[3] 1720 is the default H.225 TCP port in the RealPresence Access Director system. If you change the port in the RealPresence Access Director system, you must also change it accordingly on the firewall.

Access Proxy:

SRC IP	SRC Port	Protocol	DST IP	DST Port	Description
IP address of external client	>1023	TCP	Public IP address of the RPAD system	443[1]	HTTPS connection from the WAN to the RPAD system to sign in for provisioning
IP address of external client	>1023	TCP	Public IP address of the RPAD system	389[1]	TLS-encrypted or unencrypted encrypted (TCP) LDAP connection from the WAN to the RPAD system[2]
IP address of external client	>1023	TCP	Public IP address of the RPAD system	5222	XMPP connection from the WAN to the RPAD system
IP address of RealPresence Mobile client using an HTTP tunnel proxy	>1023	TCP	Public IP address of the RPAD system's external access proxy IP address	443	HTTPS tunnel proxy connection from the WAN to the RPAD system. The RPAD system terminates the tunnel and proxies the traffic to the internal systems.

[1] The RealPresence Access Director system automatically redirects inbound access proxy traffic on ports 443 and 389 to the internal ports 65100–65130 reserved on the system's loopback interface private IP address. The CentOS operating system does not allow processes without root ownership to listen on ports <1024. Redirecting access proxy traffic on ports <1024 to the internal ports 65100–65130 enables the access proxy process to function correctly.

[2] The RealPresence Access Director system denies all unencrypted LDAP requests if you enable Enforce TLS for LDAP connection in the web user interface (Admin > Security Settings).

Media Ports :

SRC IP	SRC Port	Protocol	DST IP	DST Port	Description
IP address of external device	>1023	UDP	RPAD system public media IP address[1]	20002–30001	Inbound media (RTP) traffic from the WAN to the RPAD system
RPAD system public media IP address	20002–30001	UDP	Public media IP address of the external device	>1023	Outbound media traffic from the RPAD system to the to WAN[2]

[1] The RealPresence Access Director system public media IP address refers to the public IP address for media mapped on the firewall located between the WAN and the RealPresence Access Director system.

[2] Most firewalls do not require a specific policy for the outbound media port range. The port range is the same for both inbound and outbound media traffic. The port information is included here for reference.

Les firewalls doivent permettre le trafic entrant et sortant sur les ports TCP et UDP qui ont été ouverts vers l'adresse ip : 91.247.75.148

Les ports réseaux (physiques) des équipements doivent être configurés en 100 Mbit/s Full Duplex.

4 - SI Télémédecine SYNAPSES

4.1 Recommandations matérielles

CPU Intel Core i5, 2.5GHz ou supérieur

Mémoire RAM : 4 Go

Ecran 24 pouce, 16/9 - 1920 x 1080, 4/3 – 1280 x 720

4.2 Recommandations pour la mobilité

Si un usage en mobilité est envisagé (tablette), il est nécessaire d'utiliser une connexion wifi ou un réseau 3G/4G.

4.3 Navigateur internet

Firefox

Chrome

Internet Explorer – Non recommandé

Edge – Non recommandé

4.4 Adresse du site Synapses

Accessible depuis tout poste informatique doté d'une connexion internet à l'adresse :

https://synapses.esante-occitanie.fr

e·santé Occitanie
Connecter pour mieux soigner

Groupement d'Intérêt Public e-santé Occitanie

Siège social : 10, ch. du Raisin · 31200 Toulouse · 05 67 20 74 00
www.esante-occitanie.fr