



Caractéristiques techniques

- [Protocoles réseau, à la page 1](#)
- [Interaction avec un réseau VLAN, à la page 5](#)
- [Informations port USB, à la page 5](#)
- [Configuration de SIP et de NAT, à la page 7](#)
- [Protocole CDP \(Cisco Discovery Protocol\), on page 13](#)
- [LLDP-MED, on page 13](#)
- [Résolution finale de stratégie réseau et QoS, à la page 18](#)

Protocoles réseau

Le téléphone IP Cisco série 8800 prend en charge plusieurs protocoles réseaux Cisco et métier requis pour la communication vocale. Le tableau suivant présente les protocoles réseaux pris en charge par ces téléphones.

Tableau 1 : Protocoles réseaux pris en charge par le téléphone IP Cisco série 8800

Protocole réseau	Rôle	Notes sur l'utilisation
Bluetooth	Bluetooth est un protocole de réseau personnel sans fil (WPAN) qui spécifie la méthode de communication entre appareils sur de courtes distances.	Les Téléphones IP Cisco 8845, 8865 et 8851 prennent en charge Bluetooth 4.1. Les Téléphones IP Cisco 8861 prennent en charge Bluetooth 4.0. Les téléphones IP Cisco 8811 et 8841 ne prennent pas en charge Bluetooth.
Protocole de démarrage (BootP)	BootP permet à un appareil réseau, comme un téléphone IP Cisco, de détecter certaines informations de démarrage, comme l'adresse IP.	-

Protocole réseau	Rôle	Notes sur l'utilisation
Cisco Discovery Protocol (CDP)	<p>CDP est un protocole de détection de périphériques qui est intégré à tous les équipements fabriqués par Cisco.</p> <p>Grâce au protocole CDP, un périphérique peut annoncer sa présence à d'autres périphériques et recevoir des informations sur d'autres périphériques du réseau.</p>	Les téléphones IP Cisco utilisent CDP pour communiquer des informations comme l'ID VLAN auxiliaire, les détails du power management pour chaque port ainsi que les informations de configuration de la qualité de service (QoS) grâce au commutateur Catalyst Cisco.
Protocole DHCP (Dynamic Host Configuration Protocol)	<p>Le protocole DHCP alloue dynamiquement une adresse IP qu'il affecte aux périphériques réseau.</p> <p>Le protocole DHCP vous permet de connecter un téléphone IP au réseau et de le rendre opérationnel sans avoir besoin d'attribuer manuellement une adresse IP ni de configurer des paramètres réseau supplémentaires.</p>	<p>Le protocole DHCP est activé par défaut. S'il est désactivé, vous devez configurer manuellement et localement l'adresse IP, le masque de sous-réseau et la passerelle sur chaque téléphone.</p> <p>Remarque Le paramètre Option DHCP à utiliser a une valeur par défaut de 66,160,159,150,60,43,125. Cette valeur indique l'ordre dans lequel le téléphone utilise l'adresse IP fournie par le serveur DHCP.</p>
Protocole HTTP (HyperText Transfer Protocol)	Le protocole HTTP est la méthode standard de transmission des informations et de déplacement de documents via Internet et le web.	Les téléphones IP Cisco utilisent le protocole HTTP pour les services XML, la mise à disposition du téléphone, la mise à niveau du téléphone et le dépannage.
Protocole HTTPS (Hypertext Transfer Protocol Secure)	Le protocole HTTPS (Hypertext Transfer Protocol Secure) est une combinaison du protocole de transfert hypertexte (HTTP) et du protocole SSL/TLS, qui permet le chiffrement et l'identification sécurisée des serveurs.	Certaines applications web prennent en charge les protocoles HTTP et HTTPS. Les téléphones IP Cisco qui prennent en charge HTTPS utilisent l'URL HTTPS.
IEEE 802.1x	<p>La norme IEEE 802.1x définit un contrôle d'accès de type client-serveur et un protocole d'authentification qui empêche les clients non autorisés de se connecter à un réseau LAN via des ports accessibles publiquement.</p> <p>Tant que le client n'est pas authentifié, le contrôle d'accès 802.1X autorise uniquement le protocole EAPOL (Extensible Authentication Protocol over LAN) sur le trafic via le port auquel le client est connecté. Une fois l'authentification réussie, le trafic normal peut traverser le port.</p>	<p>Le téléphone IP Cisco implémente la norme IEEE 802.1x en prenant en charge les méthodes d'authentification suivantes : EAP-FAST et EAP-TLS.</p> <p>Lorsque l'authentification 802.1x est activée sur le téléphone, il est recommandé de désactiver le port PC et le VLAN voix.</p>

Protocole réseau	Rôle	Notes sur l'utilisation
IEEE 802.11n/802.11ac	<p>La norme IEEE 802.11 spécifie la méthode de communication entre appareils via un réseau local sans fil (WLAN).</p> <p>802.11n fonctionne sur la bande des 2,4 GHz et celle des 5 GHz. 802.11ac fonctionne sur la bande des 5 GHz.</p>	<p>L'interface 802.11 est une option de déploiement pour les situations dans lesquelles le câblage Ethernet est impossible ou indésirable.</p> <p>Seuls les Téléphones IP Cisco 8861 et 8865 prennent en charge WLAN.</p>
Protocole IP	Le protocole IP est un protocole de messagerie qui adresse et envoie des paquets sur le réseau.	<p>Pour communiquer via IP, les périphériques réseau doivent se voir attribuer une adresse IP, un sous-réseau ainsi qu'une passerelle.</p> <p>Les adresses IP, les sous-réseaux et les passerelles sont attribués automatiquement si vous utilisez un téléphone IP Cisco avec le protocole DHCP (Dynamic Host Configuration Protocol). Si vous n'utilisez pas DHCP, vous devez affecter manuellement ces propriétés à chaque téléphone, localement.</p>
Protocole LLDP (Link Layer Discovery Protocol)	LLDP est un protocole standardisé de détection de réseau (similaire au protocole CDP) qui est pris en charge par certains périphériques Cisco et de fabricants tiers.	LLDP est pris en charge sur le port PC des téléphones IP Cisco.
LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED est une extension de la norme LLDP pour les produits de communication vocale.	<p>LLDP-MED est pris en charge sur le port de commutation des téléphones IP Cisco, pour communiquer des informations telles que :</p> <ul style="list-style-type: none"> • La configuration du VLAN • La détection de périphériques • La gestion de l'alimentation • La gestion de l'inventaire <p>Pour plus d'informations sur la prise en charge de LLDP-MED, consultez le livre blanc LLDP-MED and Cisco Discovery Protocol :</p> <p>http://www.cisco.com/1/13/65/06/136506.html</p>
Protocole RTP (Real-Time Transport Protocol)	RTP est un protocole standard pour le transfert de données en temps réel via des réseaux de données, comme la voix interactive.	Les téléphones IP Cisco utilisent le protocole RTP pour envoyer et recevoir le trafic audio en temps réel provenant d'autres téléphones et passerelles.

Protocole réseau	Rôle	Notes sur l'utilisation
Protocole RTCP (Real-Time Control Protocol)	Le protocole RTCP fonctionne en conjonction avec le protocole RTP pour fournir des données QoS (comme la gigue, la latence et le délai aller-retour) sur les flux RTP.	Le protocole RTCP est désactivé par défaut.
Protocole SDP (Session Description Protocol)	SDP est la partie du protocole SIP qui permet de déterminer quels paramètres sont disponibles pendant une connexion entre deux terminaux. Les conférences sont créées en utilisant uniquement les fonctionnalités SDP prises en charge par tous les terminaux dans la conférence.	Les fonctionnalités SDP, comme les types de codec, la détection DTMF et le bruit de confort, sont habituellement configurées à un niveau global par le système de contrôle d'appels tiers ou la passerelle multimédia en fonction. Certains terminaux SIP peuvent permettre la configuration de ces paramètres directement sur le terminal.
Protocole SIP (Session Initiation Protocol)	Le protocole SIP est la norme de groupe de travail (IETF, Internet Engineering Task Force) pour la conférence multimédia sur IP. SIP est un protocole ASCII de contrôle de couche application (défini dans la norme RFC 3261), qui peut être utilisé pour établir, gérer et interrompre des appels entre plusieurs terminaux.	Comme les autres protocoles VoIP, le protocole SIP se charge du signalement et de la gestion des sessions dans un réseau de téléphonie par paquets. Le signalement permet le transport des informations d'appel au-delà des limites d'un réseau. La gestion des sessions permet de contrôler les attributs d'un appel de bout en bout. Les téléphones IP Cisco prennent en charge le protocole SIP lorsqu'ils fonctionnent uniquement en IPv6, uniquement en IPv4 ou à la fois en IPv6 et IPv4.
Protocole TCP (Transmission Control Protocol)	Le protocole TCP est un protocole de transport orienté connexion.	Les téléphones IP Cisco utilisent TCP pour se connecter au système de contrôle des appels tiers et pour accéder aux services XML.
Transport Layer Security (Protocole TLS, Sécurité des couches de transport)	TLS est un protocole standard de sécurisation et d'authentification des communications.	Dès l'implémentation de la sécurité, les téléphones IP Cisco utilisent le protocole TLS lorsqu'ils s'enregistrent de manière sécurisée avec le système de contrôle des appels tiers.
Protocole TFTP (Trivial File Transfer Protocol)	Le protocole TFTP permet de transférer des fichiers sur le réseau. Sur un téléphone IP Cisco, le protocole TFTP vous permet d'obtenir un fichier de configuration propre au modèle du téléphone.	Le protocole TFTP nécessite la présence dans votre réseau d'un serveur TFTP que le serveur DHCP peut identifier automatiquement.

Protocole réseau	Rôle	Notes sur l'utilisation
Protocole UDP (Utilisateur Datagram Protocol)	Le protocole UDP est un protocole de communication sans connexion pour l'envoi des paquets de données.	Le protocole UDP est uniquement utilisé par les flux RTP. Le signalement SIP sur les téléphones ne prend pas en charge le protocole UDP.

Interaction avec un réseau VLAN

Le téléphone IP Cisco contient un commutateur Ethernet interne, qui permet la transmission de paquets au téléphone, au port PC et au port réseau situés à l'arrière du téléphone.

Si un ordinateur est connecté au port (d'accès au) PC, l'ordinateur et le téléphone partagent la même liaison physique au commutateur et le même port sur le commutateur. Ce lien physique commun présente les implications suivantes pour la configuration VLAN du réseau :

- Les VLAN actuels peuvent être configurés par sous-réseau IP. Toutefois, des adresses IP supplémentaires risquent de ne pas être disponibles pour affecter le téléphone au même sous-réseau que d'autres périphériques connectés au même port.
- Le trafic de données du réseau VLAN qui prend en charge les téléphones peut réduire la qualité du trafic VoIP.
- La sécurité du réseau peut indiquer qu'il est nécessaire d'isoler le trafic voix du trafic de données VLAN.

Pour résoudre ces problèmes, isolez le trafic voix en l'hébergeant sur un VLAN distinct. Le port de commutation auquel le téléphone est connecté doit être configuré pour des VLAN distincts pour transporter :

- Le trafic voix en direction et en provenance du téléphone IP (VLAN auxiliaire sur le téléphone Cisco Catalyst série 6000, par exemple)
- Le trafic voix en direction et en provenance de l'ordinateur qui est connecté à ce commutateur au moyen du port PC du téléphone IP (VLAN natif)

Le fait d'isoler les téléphones sur un VLAN auxiliaire distinct améliore la qualité du trafic voix et permet l'ajout d'un grand nombre de téléphones sur un réseau qui ne dispose pas de suffisamment d'adresses IP pour tous les téléphones.

Pour obtenir plus d'informations, reportez-vous à la documentation relative aux commutateurs Cisco. Vous pouvez également accéder aux informations relatives aux commutateurs à l'adresse suivante :

<http://cisco.com/en/US/products/hw/switches/index.html>

Informations port USB

Les téléphones IP Cisco 8851, 8861 et 8865 prennent en charge un maximum de cinq périphériques se connectant à chaque port USB. Chaque périphérique qui se connecte au téléphone est inclus dans le nombre maximum de périphériques. Par exemple, votre téléphone peut prendre en charge cinq périphériques USB sur le port latéral et cinq périphériques USB supplémentaires sur le port arrière. Un grand nombre de produits USB tiers peuvent compter comme plusieurs périphériques USB. Par exemple, un périphérique contenant un

concentrateur USB ainsi qu'un casque peut compter comme deux périphériques USB. Pour en savoir plus, reportez-vous à la documentation du périphérique USB.



Remarque

- Les concentrateurs non alimentés ne sont pas pris en charge et les concentrateurs alimentés disposant de plus de quatre ports ne sont pas pris en charge.
- Les casques USB se connectant au téléphone via un concentrateur USB ne sont pas pris en charge.

Chaque module d'extension de touches qui est raccordé au téléphone compte comme un périphérique USB. Si trois modules d'extension de touches sont raccordés au téléphone, ils comptent comme trois périphériques USB.

Désactiver le port USB

Si vous ne permettez pas aux utilisateurs d'utiliser un ou tous les ports USB à certaines fins, vous pouvez désactiver l'arrière ou le côté, ou les deux ports USB du téléphone. Le port USB désactivé ne fournit aucune fonction. Par exemple, il ne reconnaît pas le casque USB et le Key Expansion Module (KEM). De même, il ne charge aucun périphérique connecté.

Le téléphone IP Cisco 8851 comprend un seul port USB, le port USB latéral. Les téléphones IP Cisco 8861 et 8865 contiennent deux ports USB, un port USB latéral et un port USB arrière.

Avant de commencer

Accéder à la page Web d'administration du téléphone. Reportez-vous à [Accéder à l'interface Web du téléphone](#).

Procédure

Étape 1

Sélectionnez **Voix > Système**.

Étape 2

Dans la section **Power Settings** (Paramètres d'alimentation), définissez le paramètre **Désactiver le port USB arrière** sur **Oui** pour désactiver le port USB arrière.

Vous pouvez également configurer ce paramètre dans le fichier de configuration XML du téléphone (cfg.xml) en entrant une chaîne au format suivant :

```
<Disable_Back_USB_Port ua="na">No</Disable_Back_USB_Port>
```

Options : Oui et Non

Par défaut : Non

Étape 3

Dans la section **Paramètres d'alimentation**, définissez le paramètre **Désactiver le port USB latéral** sur **Oui** pour désactiver le port USB latéral.

Vous pouvez également configurer ce paramètre dans le fichier de configuration XML du téléphone (cfg.xml) en entrant une chaîne au format suivant :

```
<Disable_Side_USB_Port ua="na">No</Disable_Side_USB_Port>
```

Options : Oui et Non

Par défaut : Non

Étape 4 Cliquez sur **Envoyer toutes les modifications**.

Configuration de SIP et de NAT

SIP et le téléphone IP Cisco

Le téléphone IP Cisco utilise le protocole d'initiation de session SIP, ce qui garantit son interfonctionnement avec tous les fournisseurs de service informatique prenant en charge SIP. Le protocole SIP est un protocole de signalisation IETF qui contrôle les sessions de communication vocale sur un réseau IP.

Le protocole SIP traite la signalisation et la gestion de session sur les réseaux de téléphonie par paquets. La *signalisation* permet la transmission des informations d'appel dans les limites du réseau. La *gestion de session* contrôle les attributs d'un appel de bout en bout.

Dans des déploiements commerciaux types de téléphonie IP, tous les appels transitent par un serveur proxy SIP. Le téléphone recevant la requête est appelé le serveur de l'agent utilisateur (UAS) SIP et le téléphone qui effectue la requête, le client de l'agent utilisateur (UAC).

Le routage des messages SIP est dynamique. Si un proxy SIP reçoit une requête de la part d'un UAS pour une connexion mais qu'il ne parvient pas à localiser l'UAC, il transfère le message à un autre proxy SIP du réseau. Lorsque l'UAC est localisé, la réponse est acheminée vers l'UAS et une session directe de pair-à-pair est alors établie entre les deux UA. Le trafic voix entre les UA est transmis sur les ports attribués de manière dynamique à l'aide du protocole RTP (Real-Time Protocol).

Le protocole RTP transmet les données audio et vidéo en temps réel ; cela ne garantit pas la transmission en temps réel des données. Le protocole RTP fournit des mécanismes d'envoi et de réception pour prendre en charge les données en continu. Généralement, le protocole RTP s'exécute sur UDP.

SIP sur TCP

Pour garantir des communications basées sur l'état, le téléphone IP Cisco peut utiliser le protocole de transport TCP pour SIP. Ce protocole permet une *remise garantie* qui assure la retransmission des paquets perdus. Le protocole TCP garantit aussi que les paquets SIP sont reçus dans l'ordre dans lequel ils ont été envoyés.

Le protocole TCP permet de surmonter le problème de blocage des ports UDP par les éventuels pare-feu d'entreprise. Avec le protocole TCP, il n'est pas nécessaire d'ouvrir de nouveaux ports ou d'abandonner des paquets, car TCP est déjà utilisé pour les activités de base, comme la navigation sur Internet ou le commerce électronique.

Redondance du proxy SIP

Un serveur proxy SIP moyen peut gérer des dizaines de milliers d'abonnés. Un serveur de sauvegarde permet à un serveur actif d'être temporairement inactivé pour permettre la maintenance. Les téléphones Cisco prennent en charge l'utilisation des serveurs de sauvegarde pour minimiser ou éliminer les interruptions de service.

Une méthode simple pour prendre en charge la redondance de proxy consiste à configurer un serveur proxy SIP dans le profil de configuration du téléphone. Le téléphone envoie une requête DNS NAPTR ou SRV au serveur DNS. S'il est configuré, le serveur DNS renvoie un enregistrement SRV qui contient la liste des serveurs du domaine, avec leurs noms d'hôtes, leur priorité, leurs ports d'écoute, etc. Le téléphone tente alors de contacter les hôtes par ordre de priorité. Le serveur doté d'un numéro inférieur a une priorité plus élevée. Jusqu'à six enregistrements NAPTR et ou douze enregistrements SRV sont pris en charge dans une requête.

Lorsque le téléphone ne parvient pas à communiquer avec le serveur principal, il peut basculer vers un serveur à faible priorité. S'il est configuré, le téléphone peut rétablir la connexion principale. La prise en charge du basculement et de la restauration bascule entre des serveurs dotés de protocoles de transport SIP différents. Le téléphone n'effectue pas de retour arrière vers le serveur principal lors d'un appel actif tant que l'appel n'est pas terminé et que les conditions de restauration ne sont pas réunies.

Exemple d'enregistrements de ressource du serveur DNS

```
aslbsoft      3600      IN NAPTR 50 50 "s" "SIPS+D2T"      "" _sips._tcp.tlstest
              3600      IN NAPTR 90 50 "s" "SIP+D2T"      "" _sip._tcp.tcptest
              3600      IN NAPTR 100 50 "s" "SIP+D2U"      "" _sip._udp.udptest

_sips._tcp.tlstest SRV 1 10 5061 srv1.sipurash.com.
                  SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest  SRV 1 10 5061 srv3.sipurash.com.
                  SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest  SRV 1 10 5061 srv5.sipurash.com.
                  SRV 2 10 5060 srv6.sipurash.com.

srv1      3600      IN      A      1.1.1.1
srv2      3600      IN      A      2.2.2.2
srv3      3600      IN      A      3.3.3.3
srv4      3600      IN      A      4.4.4.4
srv5      3600      IN      A      5.5.5.5
srv6      3600      IN      A      6.6.6.6
```

L'exemple suivant montre la priorité des serveurs du point de vue du téléphone.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	TLS	UP
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

Le téléphone envoie toujours les messages SIP à l'adresse disponible ayant la priorité la plus haute et l'état EN FONCTIONNEMENT de la liste. Dans l'exemple, le téléphone envoie tous les messages SIP à l'adresse 1.1.1.1. Si l'adresse 1.1.1.1 dans la liste est marquée comme EN PANNE, le téléphone communique avec l'adresse 2.2.2.2 à la place. Le téléphone peut rétablir la connexion à l'adresse 1.1.1.1 lorsque les conditions de restauration spécifiées sont remplies. Pour plus d'informations sur le basculement et la restauration automatique, voir [Basculement du proxy SIP, à la page 8](#) et [Proxy SIP de secours, à la page 9](#).

Basculement du proxy SIP

Le téléphone effectue un basculement dans l'un des cas suivants :

- Le téléphone envoie des messages SIP et n'obtient aucune réponse du serveur.
- Le serveur répond à l'aide d'un code correspondant au code spécifié dans **Essayer la sauvegarde RSC**.
- Le téléphone reçoit une demande de déconnexion TCP.

Il est vivement recommandé de configurer l'**enregistrement automatique lors du basculement** sur **Oui** lorsque le **Transport SIP** est défini sur **Auto**.

Vous pouvez également configurer le paramètre spécifique au numéro de poste dans le fichier de configuration du téléphone (cfg.xml).


```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
<Auto_Register_When_Failover_n_ ua="na">Yes</Auto_Register_When_Failover_n_>
```

Où *n* correspond au numéro de poste.

Comportement du téléphone en cas de basculement

Lorsque le téléphone ne parvient pas à communiquer avec le serveur actuellement connecté, il actualise l'état de la liste de serveurs. Le serveur non disponible est marqué avec l'état EN PANNE dans la liste des serveurs. Le téléphone tente de se connecter au serveur de niveau supérieur dont l'état est EN FONCTIONNEMENT dans la liste.

Dans l'exemple suivant, les adresses 1.1.1.1 et 2.2.2.2 ne sont pas disponibles. Le téléphone envoie des messages SIP à l'adresse 3.3.3.3, qui a la priorité la plus haute parmi les serveurs dont l'état est EN FONCTIONNEMENT.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

Dans l'exemple suivant, il y a deux enregistrements SRV provenant de la réponse DNS NAPTR. Pour chaque enregistrement SRV, il existe trois enregistrements A (adresses IP).

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

Supposons que le téléphone n'a pas réussi à se connecter à 1.1.1.1 et qu'il soit enregistré dans 1.1.1.2. Lorsque 1.1.1.2 tombe en panne, le comportement du téléphone dépend de la valeur du paramètre **Proxy Fallback intvl**.

- Lorsque **Proxy Fallback intvl** est défini sur **0**, le téléphone tente de se connecter aux adresses dans l'ordre suivant : 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- Lorsque **Proxy Fallback intvl** est défini sur une valeur autre que zéro, le téléphone tente de se connecter aux adresses dans l'ordre suivant : 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

Proxy SIP de secours

Le proxy de secours nécessite d'indiquer une valeur différente de zéro dans le champ **Proxy Fallback intvl** de l'onglet **Poste (n)** de l'interface Web du téléphone. Si vous définissez ce champ sur 0, la fonction de restauration automatique du proxy SIP est désactivée. Vous pouvez également configurer le paramètre spécifique au numéro de poste dans le fichier de configuration du téléphone (cfg.xml).

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
```

Où *n* correspond au numéro de poste.

L'heure à laquelle le téléphone déclenche une restauration dépend de la configuration du téléphone et des protocoles de transport SIP utilisés.

Pour permettre au téléphone d'effectuer une restauration entre différents protocoles de transport SIP, paramétrez le **transport SIP** sur **Auto** dans l'onglet **Poste(n)** de l'interface Web du téléphone. Vous pouvez également configurer ce paramètre spécifique au poste dans le fichier de configuration à l'aide de la chaîne XML suivante :

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

Où *n* correspond au numéro de poste.

Restauration à partir d'une connexion UDP

La restauration à partir d'une connexion UDP est déclenchée par les messages SIP. Dans l'exemple suivant, le téléphone n'a pas pu s'enregistrer pour la première fois sur 1.1.1.1 (TLS) à l'heure T1, car il n'y a pas de réponse du serveur. Lorsque le temporisateur F SIP expire, le téléphone s'enregistre sur 2.2.2.2 (UDP) à l'heure T2 (T2 = T1 + temporisateur SIP F). La connexion en cours est active sur 2.2.2.2 via UDP.

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	TLS	DOWN	T1 (Down time)
2nd	2.2.2.2	UDP	UP	
3rd	3.3.3.3	TCP	UP	

La configuration du téléphone est la suivante :

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

Où *n* correspond au numéro de poste.

Le téléphone actualise l'enregistrement à l'heure T2 (T2 = (3600-16) * 78 %). Le téléphone vérifie la liste d'adresses pour déterminer la disponibilité des adresses IP et de l'heure de fin. Si T2-T1 >= 60, le serveur défaillant 1.1.1.1 est restauré en EN FONCTIONNEMENT et la liste est mise à jour comme suit. Le téléphone envoie des messages SIP à 1.1.1.1.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	UDP	UP
3rd	3.3.3.3	TCP	UP

Restauration à partir d'une connexion TCP ou TLS

La restauration d'une connexion TCP ou TLS est déclenchée par le paramètre **Proxy Fallback intvl**. Dans l'exemple suivant, le téléphone n'a pas pu être enregistré sur 1.1.1.1 (UDP) à l'heure T1 et de ce fait a été enregistré sur 2.2.2.2 (TCP). La connexion en cours est sur 2.2.2.2 via TCP.

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	UDP	DOWN	T1 (Down time)
2nd	2.2.2.2	TCP	UP	
3rd	3.3.3.3	TLS	UP	

La configuration du téléphone est la suivante :

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

Où n correspond au numéro de poste.

L'intervalle de secours du proxy (60 secondes) est décompté à partir de T1. Le téléphone déclenche la restauration du proxy à l'heure T1 + 60. Si vous définissez l'intervalle de secours du proxy sur 0 dans cet exemple, le téléphone conserve la connexion sur 2.2.2.2.

Enregistrement double

Le téléphone est toujours enregistré auprès du proxy principal (ou sortant principal) et du proxy secondaire (ou sortant secondaire). Après l'enregistrement, le téléphone envoie des messages SIP Invite et Non-Invite en passant d'abord par le proxy principal. S'il n'y a pas de réponse au nouveau message INVITE du proxy principal, après temporisation, le téléphone tente de se connecter au proxy secondaire. Si le téléphone ne parvient pas à s'enregistrer auprès du proxy principal, il envoie un message INVITE au proxy secondaire sans solliciter le proxy principal.

L'enregistrement double est pris en charge ligne par ligne. Trois paramètres supplémentaires peuvent être configurés par le biais de l'interface utilisateur Web et de la mise à disposition à distance :

- Proxy secondaire : ce champ est vide par défaut.
- Proxy sortant secondaire : ce champ est vide par défaut.
- Enregistrement double : la valeur par défaut est Non (désactivé).

Après avoir configuré les paramètres, redémarrez le téléphone pour que la fonctionnalité prenne effet.



Note Indiquez une valeur pour le proxy principal (ou proxy sortant principal) et pour le proxy secondaire (ou proxy sortant secondaire) afin que la fonctionnalité soit opérationnelle.

Enregistrement double et limites de DNS SRV

- Lorsque l'enregistrement double est activé, le basculement ou la récupération du proxy DNS SRV doivent être désactivés.
- N'utilisez pas l'enregistrement double avec d'autres mécanismes de récupération ou de basculement. Par exemple : mécanisme BroadSoft.
- Il n'y a aucun mécanisme de récupération pour la requête de fonctionnalité. Toutefois, l'administrateur peut modifier l'heure de réenregistrement pour une mise à jour rapide de l'état d'enregistrement des proxys principal et secondaire.

Enregistrement double et proxy alternatif

Lorsque le paramètre Dual Register est défini sur **Non**, le proxy secondaire est ignoré.

Enregistrement du basculement et de la récupération

- Failover : le téléphone effectue un basculement en cas d'échec/de temporisation du transport ou d'échec de connexion TCP, si les valeurs des champs Try Backup RSC et Retry Reg RSC sont renseignées.
- Recovery : le téléphone tente de se réenregistrer auprès du proxy principal lorsqu'il est enregistré ou activement connecté au proxy secondaire.

Le paramètre Enregistrement automatique en cas de basculement contrôle le comportement de basculement en cas d'erreur. Lorsque ce paramètre est défini sur Oui, le téléphone se réenregistre après basculement ou récupération.

Comportement du basculement

Le basculement se produit à l'expiration de l'enregistrement actuel ou au déclenchement de l'intervalle de basculement du proxy.

Si l'intervalle de basculement du proxy est dépassé, tous les nouveaux messages SIP sont transmis au proxy principal.

Par exemple, lorsque la valeur de l'option Register Expires est 3 600 secondes et que celle de l'option Proxy Fallback Intvl est 600 secondes, le basculement est déclenché 600 secondes plus tard.

Lorsque la valeur de l'option Register Expires est 800 secondes et que celle de l'option Proxy Fallback Intvl est 1000 secondes, le basculement est déclenché à 800 secondes.

Après le réenregistrement auprès du serveur principal, tous les messages SIP sont transmis au serveur principal.

RFC3311

Le téléphone IP Cisco prend en charge la norme RFC-3311, la méthode SIP UPDATE.

Service SIP NOTIFY XML

Le téléphone IP Cisco prend en charge l'événement de service XML SIP NOTIFY. Après réception d'un message SIP NOTIFY avec un événement de service XML, le téléphone teste le message NOTIFY avec une réponse 401 si le message ne contient pas les informations d'identification correctes. Le client doit fournir les informations d'identification correctes en utilisant le MD5 digest avec le mot de passe du compte SIP pour la ligne correspondante sur le téléphone IP.

Le corps du message peut contenir le message d'événement XML. Par exemple :

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentification :

```
challenge = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

Mappage NAT avec un contrôleur de limites de session

Il est recommandé de choisir un fournisseur de service prenant en charge le mappage NAT via un contrôleur de limites de session. Si votre fournisseur de service prend en charge le mappage NAT, vous disposez d'un plus grand choix pour la sélection d'un routeur.

Mappage NAT avec un routeur SIP-ALG

Le mappage NAT peut être effectué à l'aide d'un routeur équipé d'une passerelle de couche d'application (ALG) SIP. En utilisant un routeur SIP-ALG, vous disposez d'un plus grand choix pour la sélection de votre fournisseur de service.

Protocole CDP (Cisco Discovery Protocol)

Le protocole CDP (Cisco Discovery Protocol) est un protocole basé sur la négociation qui détermine le réseau local virtuel (VLAN) qui héberge le téléphone IP Cisco. Si vous utilisez un commutateur Cisco, le protocole CDP est disponible et activé par défaut. Le protocole CDP possède les attributs suivants :

- Il obtient les adresses de protocole des périphériques voisins et détecte la plateforme de ces périphériques.
- Il indique les informations relatives aux interfaces utilisées par votre routeur.
- Il est indépendant du support et du protocole.

Si vous utilisez un VLAN sans CDP, vous devez saisir un identifiant de VLAN pour le téléphone IP Cisco.

LLDP-MED

Le téléphone IP Cisco prend en charge le protocole LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) pour le déploiement avec des périphériques de connectivité réseau Cisco ou de fabricants tiers qui utilisent un mécanisme de détection automatique de couche 2. La mise en œuvre du protocole LLDP-MED est effectuée conformément à la spécification IEEE 802.1AB (LLDP) de mai 2005 et à la norme ANSI TIA-1057 d'avril 2006.

Le téléphone IP Cisco fonctionne comme un terminal multimédia LLDP-MED de classe III avec des liaisons LLDP-MED directes à des périphériques de connectivité réseau, conformément à la définition et au modèle de référence de détection de terminaux multimédia (ANSI TIA-1057 Section 6).

Le téléphone IP Cisco prend uniquement en charge les TLV suivants en tant que terminaux multimédia LLDP-MED de classe III :

- ID du châssis TLV
- ID du port TLV
- Temps de vie TLV
- Description du port TLV
- Nom du système TLV
- Fonctionnalités du système TLV
- TLV de configuration/état MAC/PHY selon IEEE 802.3 (pour réseaux câblés seulement)
- TLV de capacités LLDP-MED
- Politique de réseau TLV LLDP-MED (pour le type d'application = voix uniquement)
- Alimentation étendue-Via-MDI TLV LLDP-MED (pour les réseaux câblés seulement)

- Révision du micrologiciel TLV LLDP-MED
- Fin du LLDPDU TLV

Le LLDPDU sortant contient tous les TLV précédents, le cas échéant. Pour le LLDPDU entrant, le LLDPDU est éliminé si l'un des TLV suivants est absent. Tous les autres TLV ne sont pas validés et sont ignorés.

- ID du châssis TLV
- ID du port TLV
- Temps de vie TLV
- TLV de capacités LLDP-MED
- Politique de réseau TLV LLDP-MED (pour le type d'application = voix uniquement)
- Fin du LLDPDU TLV

Le téléphone IP Cisco envoie le LLDPDU d'arrêt, le cas échéant. La trame LLDPDU contient les TLV suivants :

- ID du châssis TLV
- ID du port TLV
- Temps de vie TLV
- Fin du LLDPDU TLV

Certaines restrictions s'appliquent à la mise en œuvre de LLDP-MED sur les téléphones IP Cisco :

- Le stockage et la récupération des informations sur le voisin ne sont pas pris en charge.
- SNMP et les MIB correspondants ne sont pas pris en charge.
- L'enregistrement et la récupération des compteurs de statistiques ne sont pas pris en charge.
- La validation complète de tous les TLV n'est pas effectuée ; les TLV qui ne s'appliquent pas aux téléphones sont ignorés.
- Les machines d'état de protocole définies dans les normes ne sont utilisées qu'à titre de référence.

ID du châssis TLV

Pour le LLDPDU sortant, le TLV prend en charge le sous-type subtype=5 (Adresse réseau). Lorsque l'adresse IP est connue, la valeur de l'ID de châssis est un octet du numéro de la famille d'adresses INAN suivi de la chaîne d'octet de l'adresse IPv4 utilisée pour les communications vocale. Si l'adresse IP est inconnue, la valeur de l'ID de châssis est 0.0.0.0. La seule famille d'adresses INAN prise en charge est IPv4. Actuellement, l'adresse IPv6 n'est pas prise en charge pour l'ID de châssis.

Pour le LLDPDU entrant, l'ID de châssis est traité comme une valeur opaque pour former l'identifiant MSAP. La valeur n'est pas validée par rapport à ce sous-type.

Le TLV Chassis ID est obligatoire en tant que premier TLV. Seul un TLV Chassis ID est autorisé pour les LLDPDU entrant et sortant.

ID du port TLV

Pour le LLDPDU sortant, le TLV prend en charge le sous-type subtype=3 (Adresse MAC). L'adresse MAC à 6 octets du port Ethernet est utilisée pour la valeur de l'ID de port.

Pour le LLDPDU entrant, le TLV d'ID de port est traité comme une valeur opaque pour former l'identifiant MSAP. La valeur n'est pas validée par rapport à ce sous-type.

Le TLV d'ID de port est obligatoire en tant que deuxième TLV. Seul un TLV d'ID de port est autorisé pour les LLDPDU entrant et sortant.

TLV Time to Live

Pour le LLDPDU sortant, la durée de vie est de 180 secondes. Cela diffère de la valeur de 120 secondes recommandée par la norme. Pour le LLDPDU d'arrêt, la durée de vie est toujours égale à 0.

Le TLV de durée de vie en tant que troisième TLV. Seul un TLV de durée de vie est autorisé pour les LLDPDU entrant et sortant.

Fin du LLDPDU TLV

La valeur par défaut est 2 octets de zéros. Ce TLV est obligatoire et seul un TLV est autorisé pour les LLDPDU entrantes et sortantes.

Description du port TLV

Pour le LLDPDU sortant, dans le TLV de description du port, la valeur de la description du port est la même que le TLV Port ID de CDP. Pour le LLDPDU entrant, le TLV de description du port est ignoré et n'est pas validé. Seul un TLV de description du port est autorisé pour les LLDPDU entrant et sortant.

Nom du système TLV

Pour le téléphone IP Cisco, la valeur est SEP+adresse MAC.

Exemple : SEPAC44F211B1D0

Pour le LLDPDU entrant, le TLV de nom du système est ignoré et n'est pas validé. Seul un TLV de nom du système est autorisé pour les LLDPDU entrant et sortant.

Fonctionnalités du système TLV

Pour le LLDPDU sortant, dans le TLV System Capabilities, les valeurs d'octet des champs de fonctionnalités système à 2 octets doivent être définies pour Bit 2 (passerelle) et Bit 5 (téléphone) pour un téléphone doté d'un port PC. Si le téléphone n'est pas doté d'un port PC, seule la valeur de Bit 5 doit être définie. La même valeur de fonctionnalité système doit être définie pour le champ relatif à la fonctionnalité activée.

Pour le LLDPDU entrant, le TLV de fonctionnalités système est ignoré. Le TLV n'est pas validé de manière sémantique par rapport au type de périphérique MED.

Le TLV de fonctionnalités système est obligatoire pour les LLDPDU sortants. Un seul TLV de fonctionnalités système est autorisé.

TLV Management Address

Le TLV identifie une adresse associée à l'agent LLDP local (qui peut être utilisé pour joindre des entités de couche supérieure) pour aider à la détection par la gestion du réseau. Le TLV permet l'inclusion du numéro de l'interface système et d'un identifiant d'objet (OID) qui sont associés à cette adresse de gestion, s'ils sont connus.

- TLV information string length : ce champ contient la longueur (en octets) de tous les champs de la chaîne d'informations TLV.
- Management address string length : ce champ contient la longueur (en octets) des champs Management address subtype et Management address.

TLV System Description

Le TLV permet à l'administration du réseau de publier la description du système.

- TLV information string length : ce champ indique la longueur exacte (en octets) de la description du système.
- System description : ce champ contient une chaîne alphanumérique qui est la description textuelle de l'entité réseau. La description du système inclut le nom complet du système et l'identification de la version du matériel, du logiciel, du système d'exploitation et du logiciel de mise en réseau du système. Si les implémentations prennent en charge la norme IETF RFC 3418, l'objet sysDescr doit être utilisé pour ce champ.

TLV de configuration/état MAC/PHY selon IEEE 802.3

Le TLV n'est pas utilisé pour la négociation automatique, mais pour la résolution de problème. Pour le LLDPDU entrant, le TLV est ignoré et n'est pas validé. Pour le LLDPDU sortant, pour le TLV, la valeur de l'octet de l'état ou la prise en charge de la négociation automatique doit être :

- Bit 0 : défini sur 1 pour indiquer que la négociation automatique est prise en charge.
- Bit 1 : défini sur 1 pour indiquer que l'état de la négociation automatique est activé.
- Bit 2-7 : défini sur 0.

Les valeurs du champ à 2 octets relatif à la fonctionnalité publiée de négociation automatique doivent être définies sur :

- Bit 13 : 10BASE-T mode semi duplex
- Bit 14 : 10BASE-T mode duplex intégral
- Bit 11 : 100BASE-TX mode semi duplex
- Bit 10 : 100BASE-TX mode duplex intégral
- Bit 15 : inconnu

Les bits 10, 11, 13 et 14 doivent être définis.

La valeur du type MAU opérationnel à 2 octets doit être définie de manière à refléter le type réel de MAU opérationnel :

- 16 : 100BASE-TX duplex intégral
- 15 : 100BASE-TX semi duplex
- 11 : 10BASE-T duplex intégral
- 10 : 10BASE-T semi duplex

Par exemple, le téléphone est généralement défini sur 100BASE-TX duplex intégral. La valeur 16 doit alors être définie. Le TLV est facultatif pour les réseaux câblés et ne s'applique pas aux réseaux sans fil. Le téléphone n'envoie ce TLV que lorsqu'il est en mode filaire. Si le téléphone n'est pas configuré pour la négociation automatique, mais pour une vitesse ou un duplex spécifique, pour le TLV LLDPDU sortant, le bit 1 de la valeur d'octet de prise en charge/d'état de la négociation automatique doit être effacé (0) pour indiquer que la négociation automatique est désactivée. Le champ à 2 octets relatif à la fonctionnalité publiée de négociation automatique PMD doit être défini sur 0x8000 pour indiquer la valeur Inconnu.

TLV de capacités LLDP-MED

Pour le LLDPDU sortant, le TLV doit comprendre le type de périphérique 3 (terminal de classe III), les bits suivants étant définis pour le champ à 2 bits relatif à la fonctionnalité :

Position du bit	Capacité
0	Fonctionnalités LLDP-MED
1	Stratégie réseau
4	Alimentation étendue via MDI-PD
5	Inventaire

Pour le TLV entrant, si le TLV LLDP-MED n'est pas présent, le LLDPDU est supprimé. Le TLV de capacités LLDP-MED est obligatoire et seul un TLV est autorisé pour les LLDPDU entrant et sortant. Tous les autres TLV LLDP-MED seront ignorés s'ils sont présentés avant le TLV de capacités LLDP-MED.

TLV de stratégie réseau

Dans le TLV pour le LLDPDU sortant, avant que le VLAN ou le DSCP ne soit déterminé, le drapeau de politique inconnue (U) est défini à 1. Si le paramètre VLAN ou DSCP est connu, la valeur est définie à 0. Lorsque la politique est inconnue, toutes les autres valeurs sont définies à 0. Avant que le VLAN ne soit déterminé ou utilisé, le drapeau balisé (T) est défini à 0. Si le VLAN balisé (VLAN ID > 1) est utilisé pour le téléphone, le drapeau balisé (T) est défini à 1. Réserve (X) est toujours défini à 0. Si le VLAN est utilisé, l'ID VLAN et la priorité L2 correspondants seront définis en conséquence. Les valeurs valides du champ VLAN ID sont comprises dans la plage 1 à 4094. Toutefois, VLAN ID=1 ne sera jamais utilisé (limitation). Si DSCP est utilisé, la plage de valeurs de 0 à 63 est définie en conséquence.

Dans le TLV du LLDPDU entrant, des TLV de stratégie réseau multiples sont autorisés pour plusieurs types d'application.

TLV LLDP-MED Extended Power-Via-MDI

Dans le TLV du LLDPDU sortant, la valeur binaire du champ Power Type est définie sur « 0 1 » pour indiquer que le type d'alimentation du téléphone est PD Device. La source d'alimentation du téléphone est définie sur « PSE and local » avec la valeur binaire « 1 1 ». Le champ Power Priority est défini sur la valeur binaire « 0 0 0 0 » pour indiquer une priorité inconnue lorsque le champ Power Value est défini sur la valeur d'alimentation maximale. La valeur d'alimentation du téléphone IP Cisco est 12900mW.

Pour le LLDPDU entrant, le TLV est ignoré et n'est pas validé. Seul un TLV est autorisé dans les LLDPDU entrant et sortant. Le téléphone n'enverra le TLV que pour le réseau câblé.

À l'origine, la norme LLDP-MED standard a été conçue pour Ethernet. Des discussions sont en cours pour appliquer LLDP-MED aux réseaux sans fil. Voir ANSI-TIA 1057, Annexe C, C.3 TLV applicable pour VoWLAN, tableau 24. Il est recommandé que la TLV ne soit pas applicable dans le contexte du réseau sans fil. Ce TLV est destiné à être utilisé dans le cadre de PoE et d'Ethernet. S'il est ajouté, le TLV ne fournira aucune valeur pour la gestion du réseau ou pour la modification de la stratégie d'alimentation sur le commutateur.

TLV de gestion des stocks LLDP-MED

Ce TLV est facultatif pour les périphériques de classe III. Pour le LLDPDU sortant, seul le TLV de révision du micrologiciel est pris en charge. La valeur du champ Firmware Revision est la version du micrologiciel du téléphone. Pour le LLDPDU entrant, les TLV sont ignorés et ne sont pas validés. Seul un TLV de révision du micrologiciel est autorisé pour les LLDPDU entrant et sortant.

Résolution finale de stratégie réseau et QoS

VLAN spéciaux

VLAN=0, VLAN=1 et VLAN=4095 sont traités de la même manière qu'un VLAN non balisé. Comme le VLAN n'est pas balisé, la classe de service (CoS) ne s'applique pas.

Mode QoS pour SIP par défaut

Si aucune stratégie réseau n'est définie dans CDP ou LLDP-MED, la stratégie par défaut est utilisée. La classe de service (CoS) est basée sur la configuration du poste spécifique. Il est applicable uniquement si le VLAN manuel est activé et si l'ID VLAN manuel n'est pas égal à 0, 1 ou 4095. Le type de service (ToS) est basé sur la configuration pour le numéro de poste spécifique.

Résolution de QoS pour CDP

S'il existe une stratégie réseau valide provenant de CDP :

- Si le VLAN=0, 1 ou 4095, le VLAN ne sera pas défini, ou le VLAN n'est pas balisé. La CoS ne s'applique pas, mais DSCP s'applique. Le ToS est basé sur la valeur par défaut, comme décrit précédemment.
- Si VLAN > 1 et VLAN < 4095, la valeur VLAN est définie en conséquence. La CoS et le ToS sont basés sur la valeur par défaut, comme décrit précédemment. DSCP s'applique.

- Le téléphone est réamorcé et redémarre la séquence de démarrage rapide.

Résolution de QoS pour LLDP-MED

Si la CoS s'applique et si CoS=0, la valeur par défaut est utilisée pour le poste spécifique, comme décrit précédemment. Mais la valeur indiquée dans L2 Priority for TLV pour les LLDPDU sortants est basée sur la valeur utilisée pour le numéro de poste 1. Si CoS est applicable et si CoS != 0, CoS est utilisé pour tous les numéros de poste.

Si DSCP (mappé sur le ToS) s'applique et si DSCP=0, la valeur par défaut est utilisée pour le poste spécifique, comme décrit précédemment. Mais la valeur indiquée sur DSCP pour TLV pour LLDPDU sortant est basée sur la valeur utilisée pour le numéro de poste 1. Si DSCP est applicable et si DSCP != 0, DSCP est utilisé pour tous les numéros de poste.

Si VLAN > 1 et VLAN < 4095, la valeur VLAN est définie en conséquence. La CoS et le ToS sont basés sur la valeur par défaut, comme décrit précédemment. DSCP s'applique.

S'il existe une stratégie réseau valide pour l'application voix du PDU LLDP-MED et si l'indicateur de balisage est défini, les champs VLAN, L2 Priority (CoS) et DSCP (mappé sur le ToS) s'appliquent tous.

S'il existe une stratégie réseau valide pour l'application voix du PDU LLDP-MED et si l'indicateur de balisage n'est pas défini, seul le DSCP (mappé sur le ToS) s'applique.

Le téléphone IP Cisco est réamorcé et redémarre la séquence de démarrage rapide.

Coexistence avec le protocole CDP

Si CDP et LLDP-MED sont activés, la stratégie réseau du réseau VLAN détermine la dernière stratégie définie ou modifiée par l'un des modes de détection. Si LLDP-MED et CDP sont activés, lors du démarrage, le téléphone envoie simultanément des PDU CDP et LLDP-MED.

Une configuration et un comportement sans cohérence des modes CDP et LLDP-MED sur les périphériques de connectivité réseau risquent d'entraîner un comportement instable lors du redémarrage du téléphone, car les périphériques basculent alors entre plusieurs VLAN.

Si le VLAN n'est pas défini par CDP et LLDP-MED, l'ID du VLAN qui est manuellement configuré est utilisé. Si l'ID du VLAN n'est configuré manuellement, aucun VLAN n'est pris en charge. DSCP est utilisé et le cas échéant, la stratégie réseau détermine LLDP-MED.

LLDP-MED et plusieurs périphériques réseau

Si le même type d'application est utilisé pour la stratégie réseau, mais que les téléphones reçoivent des stratégies réseau QoS de couche 2 ou 3 provenant de plusieurs périphériques de connectivité réseau, la dernière stratégie réseau valide est appliquée. Pour assurer le caractère déterministe et cohérent de la stratégie réseau, plusieurs périphériques de connectivité réseau ne doivent pas envoyer des stratégies réseau conflictuelles pour le même type d'application.

LLDP-MED et IEEE 802.X

Le téléphone IP Cisco n'est pas compatible IEEE 802.X et ne fonctionne pas dans les environnements 802.1X câblés. Toutefois, les protocoles IEEE 802.1X ou Spanning Tree sur les périphériques réseau peuvent entraîner un retard de la réponse de démarrage rapide provenant des commutateurs.

