Les longueurs de chemin d'objet de liaison physique, de nom de domaine et de nom d'hôte sont inconnues avant d'émettre la demande de service Get_Attributes_All. Les implémenteurs doivent se préparer à accepter une réponse contenant les tailles maximales de chemin d'objet de liaison physique (6 UINT), de nom de domaine (48 USINT) et de nom d'hôte (64 USINT).

7.5.5.3 Demande Set_Attributes_All

La demande Set_Attributes_All de l'instance doit contenir l'attribut Contrôle de configuration, suivi de l'attribut de configuration d'interface.

7.5.6 Services spécifiques à la classe

7.5.6.1 Généralités

L'objet Interface TCP/IP doit prendre en charge les services communs tel que spécifié dans le Tableau 64.

Tableau 64 – Services communs de l'objet d'interface TCP/IP

Service code	Nécessité dans la mise en œuvre		Nom du service	Description du service
	Classe	Instance		
0x4C	N/A	Sous condition [a]	Set_Port_Admin_State	Configure l'état (ouvert/fermé) des ports IANA qui peuvent être commandés.
0x4D	N/A	Sous condition [b]	Set_Protocol_Admin_State	Configure l'état (activé/désactivé) des protocoles IANA qui peuvent être commandés.

[a] Exigé si l'attribut d'instance #14 (IANA Port Admin) est pris en charge et au moins une entrée de port a le bit Configurable à un dans le membre Admin Capability.

[b] Exigé si l'attribut d'instance #15 (IANA Protocol Admin) est pris en charge et au moins une entrée de protocole a le bit Configurable à un dans le membre Admin Capability.

7.5.6.2 Service Set_Port_Admin_State

Le service Set_Port_Admin_State est utilisé pour configurer l'état (ouvert/fermé) pour les ports de l'attribut #14 (IANA Port Admin) qui a le bit Configurable à un dans le membre Admin Capability.

Si l'appareil exige une réinitialisation pour que la nouvelle configuration prenne effet (bit Reset Required à un dans le membre Admin Capability), l'appareil doit alors mettre à un le bit IANA Port State Change Pending (bit 8 de l'attribut Status). Si l'appareil n'exige pas une réinitialisation (bit Reset Required dans le membre Admin Capability supprimé) afin que la nouvelle configuration prenne effet, les modifications doivent prendre effet immédiatement après l'envoi de la réponse.

Si l'une des configurations de port demandées échoue, aucune des configurations demandées ne doit être appliquée et les valeurs précédentes doivent être conservées.

Les paramètres de demande sont définis dans le Tableau 65.

Tableau 65 – Paramètres de la demande de service Set_Port_Admin_State

Nom	Type de données	Description du paramètre
Port Count	USINT	Nombre de ports inclus dans la demande
Port Array	MATRICE de STRUCT	Matrice de ports à configurer
Port Number	UINT	Numéro de port IANA
Protocole	USINT	6 = TCP 17 = UDP
Etat Admin	BOOL	0 = fermé 1 = ouvert

7.5.6.3 Service Set Protocol_Admin_State

Le service Set_Protocol_Admin_State est utilisé pour configurer l'état (activé/désactivé) du protocole dans l'attribut #15 (IANA Protocol Admin) dont le bit Configurable est à un dans le membre Admin Capability.

Si l'appareil exige une réinitialisation pour que la nouvelle configuration prenne effet (bit Reset Required à un dans le membre Admin Capability), l'appareil doit alors mettre à un le bit IANA Protocol State Change Pending (bit 9 de l'attribut Status). Si l'appareil n'exige pas une réinitialisation (bit Reset Required dans le membre Admin Capability supprimé) afin que la nouvelle configuration prenne effet, les modifications doivent prendre effet immédiatement après l'envoi de la réponse.

Si l'une des configurations de protocole échoue, alors aucune des configurations demandées ne doit être appliquée et les valeurs précédentes doivent être conservées.

Les paramètres de demande sont définis dans le Tableau 66.

Tableau 66 – Paramètres de la demande de service Set_Protocol_Admin_State

Nom	Type de données	Description du paramètre
Protocol Count	USINT	Nombre de protocoles inclus dans la demande
Protocol Array	MATRICE de STRUCT	Matrice de protocoles à configurer
Protocol Number	USINT	Numéro de port IANA
Etat Admin	BOOL	0 = Désactivé 1 = activation

7.5.6.4 Codes d'erreur

Les services spécifiques à la classe Set_Port_Admin_State et Set_Protocol_Admin_State doivent prendre en charge les codes d'erreur présentés dans le Tableau 67, en complément des codes d'erreur répertoriés dans l'IEC 61158-6-2, 4.1.11.2.1.

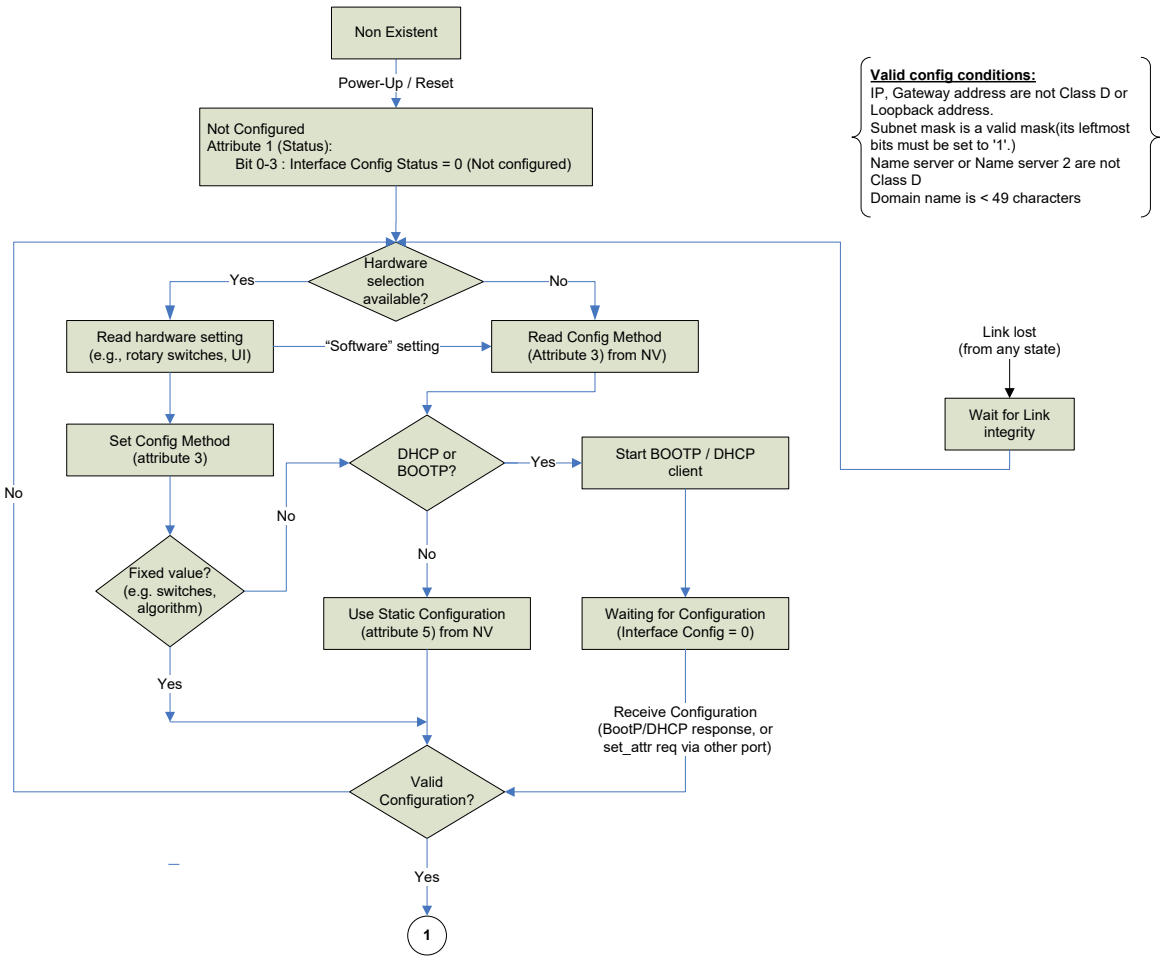
Tableau 67 – Codes d'erreur spécifiques à la classe

Etat général	Etat étendu	Condition d'erreur
0x20	0x0001	Port Count ou Protocol Count trop volumineux
0x20	0x0002	Port Number non valide
0x20	0x0003	Protocol non valide
0x20	0x0004	Combinaison Port Number/Protocol non valide
0x20	0x0005	Le port demandé ne peut pas être fermé
0x20	0x0006	Le protocole demandé ne peut pas être désactivé

7.5.7 Comportement

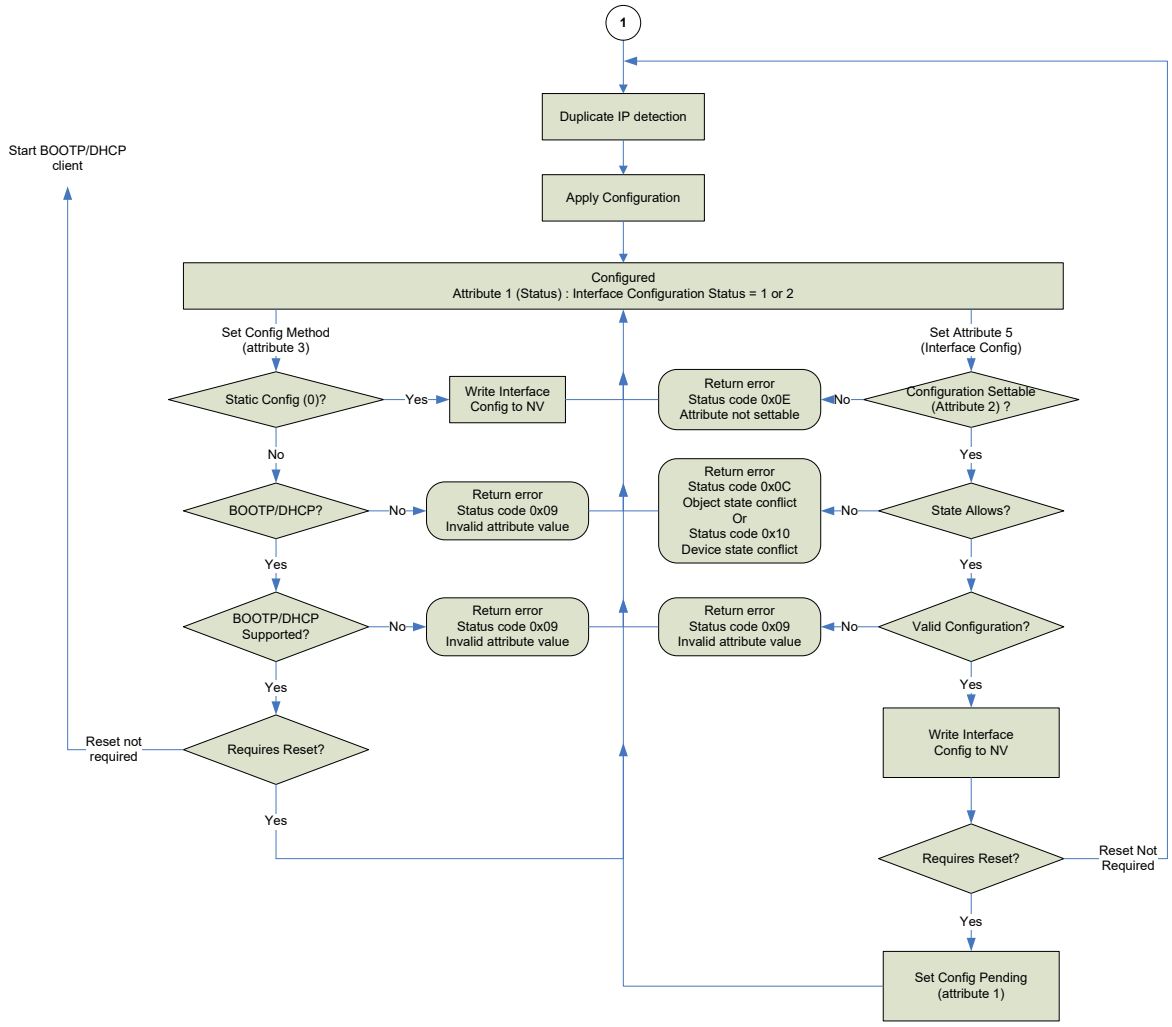
Le comportement de l'objet d'interface TCP/IP doit être tel qu'illustré dans le diagramme de transition d'états (voir Figure 21 et Figure 22).

A noter que l'obtention d'une image exécutable initiale par l'intermédiaire de BOOTP/TFTP ne doit pas être considérée dans le cadre du comportement de l'objet d'interface TCP/IP. Les appareils sont libres de mettre en œuvre ce type de comportement. Toutefois, il doit être considéré comme s'étant produit à l'état “inexistant”.



Anglais	Français
Non-existent	Non existant
Powerup/reset	Mise sous tension/réinitialisation
Not configured	Non configuré
Attribute 1 (Status):	Attribut 1 (statut):
Bit 0-3: Interface Config Status = 0 (Not configured)	Bit 0-3: statut de configuration d'interface = 0 (non configuré)
Hardware selection available?	Sélection du matériel disponible?
Yes / No	Oui / Non
Read hardware setting (e.g. rotary switches, UI)	Lecture des paramètres matériels (ex: commutateurs rotatifs, interface utilisateur)
“Software” setting	Paramétrage “logiciel”
Read Config Method (Attribute 3) from NV	Lecture méthode configuration (attribut 3) de NV
Set Config Method (attribute 3)	Lecture méthode configuration (attribut 3)
DHCP or BOOTP?	DHCP ou BOOTP?
Start BOOTP / DHCP client	Démarrer le client BOOTP / DHCP
Link lost (from any state)	Liaison perdue (tout état)
Wait for Link Integrity	Attendre l'intégrité de la liaison
Fixed values?(e.g. switches, algorithm)	Valeurs fixes? (commutateurs, algorithme)
Use static configuration (attribute 5) from NV	Utiliser configuration statique (attribut 5) de NV
Waiting for configuration (Interface Config = 0)	Attente de la configuration (config. Interface = 0)
Receive configuration (BOOTP/DHCP response, or set_attr req via other port)	Réception de la configuration (réponse BOOTP/DHCP ou demande set_attr via un autre port)
Valid configuration?	Configuration valide?
Valid config conditions:	Conditions de configuration valide:
IP, Gateway address are not Class D or Loopback address.	Les adresses IP et de la passerelle ne sont pas de la classe D ou ne sont pas des adresses en boucle.
Subnet mask is a valid mask (its leftmost bits must be set to 1)	Le masque de sous-réseau est un masque valide (ses bits de gauche doivent être définis sur 1)
Name server or name server 2 are not class D Domain name is < 49 characters	Serveur de noms et serveur de noms 2 ne sont pas de classe D Nom de domaine < 49 caractères

Figure 21 – Diagramme de transition d'états de l'objet d'interface TCP/IP



Anglais	Français
Duplicate IP detection	Dupliquer la détection IP
Start BOOTP / HDCP client	Démarrer le client BOOTP / HDCP
Apply Configuration	Appliquer la configuration
Configured Attribute 1 (Status): Interface Configuration Status = 1 or 2	Configuré Attribut 1 (Status): Interface Configuration Status = 1 ou 2
Set config method (attribute 3)	Définir méthode de configuration (attribut 3)
Set Attribute 5 (interface config)	Définir attribut 5 (configuration d'interface)
Static Config (0)?	Configuration statique (0)?
Yes / No	Oui / Non
Write interface config to VN	Ecrire la configuration d'interface dans le NV
Return error Status code 0x0E Attribute not settable	Erreur de retour Code statut 0x0E Attribut non définissable
Configuration settable (attribute 2)?	Configuration définissable (attribut 2)?
Return error Status code 0x09 Invalid attribute value	Erreur de retour Code statut 0x09 Valeur d'attribut non valide
Return error	Erreur de retour

Anglais	Français
Status code 0x0C Object state conflict or Status Code 0x10 Device state conflict	Code statut 0x0C Conflit d'état d'objet ou Code statut 0x10 Conflit d'état d'appareil
State allows?	Autorisation par l'état?
BOOTP/DHCP supported?	Prise en charge BOOTP/DHCP?
Valid configuration?	Configuration valide?
Reset not required	Réinitialisation non requise
Requires reset?	Réinitialisation requise?
Set config pending (attribute 1)	Définition de la configuration en attente (attribut 1)

Figure 22 – Diagramme de transition d'états de l'objet d'interface TCP/IP

7.5.8 Détection de conflit d'adresses (ACD)

7.5.8.1 Généralités

7.5.8.1.1 Exigences ACD pour les appareils de type 2

La détection de conflit d'adresses (ACD) est un mécanisme que peuvent utiliser les appareils pour détecter et agir sur les conflits d'adresses IPv4.

Le mécanisme ACD spécifié dans le présent Paragraphe 7.5.8 est conforme à l'IETF RFC 5227. Les exigences spécifiées dans l'IETF RFC 5227 sont incluses par référence, sauf en cas de remplacement par des exigences normatives en 7.5.8. Le présent Paragraphe 7.5.8 spécifie des exigences supplémentaires pour les appareils de type 2 relatifs au mécanisme ACD IPv4.

Les exigences ACD suivantes s'appliquent aux appareils de type 2:

- ACD est recommandé;
- un appareil mettant en œuvre l'ACD doit être conforme au mécanisme ACD spécifié dans l'IETF RFC 5227, sauf en cas de remplacement par des exigences normatives dans la présente Annexe;
- un appareil exécutant l'ACD doit exécuter le mécanisme ACD indépendamment de la méthode employée par l'appareil pour l'obtention de ses paramètres IP;
- un appareil exécutant l'ACD, et n'exécutant pas l'algorithme QuickConnect, doit exécuter le mécanisme ACD avant d'utiliser un ensemble de paramètres IP;
- les appareils doivent répondre aux sondes ARP.

7.5.8.1.2 Aperçu du mécanisme ACD dans l'IETF RFC 5227

Le mécanisme IPv4 ACD décrit dans l'IETF RFC 5227 implique les activités suivantes:

- échantillonnage d'adresse initiale et détection de conflit – avant d'utiliser une adresse IP, l'appareil émet des sondes ARP pour détecter si l'adresse est utilisée par un autre appareil;
- annonce de l'adresse – un paquet de demande ARP est envoyé après avoir déterminé qu'il n'existe aucun autre conflit d'adresse IP;
- détection de conflit continue – processus continu en vigueur tant que l'appareil utilise une adresse IP;
- défense d'adresse – procédure utilisée pour résoudre un conflit d'adresses.

7.5.8.2 Comportement ACD

Les principes de fonctionnement du mécanisme ACD sont spécifiés dans l'IETF RFC 5227.

En particulier, l'IETF RFC 5227, 2.1, exige qu'"un hôte mettant en œuvre la présente spécification doit effectuer des tests afin de vérifier si l'adresse est déjà utilisée lorsqu'une modification de l'état d'une liaison signale qu'un câble Ethernet a été connecté".

Par ailleurs, le présent Paragraphe 7.5.8 détaille davantage encore le comportement ACD comme suit.

– Les activités de l'ACD sont regroupées en régions, notamment:
  - la phase active;
  - la phase passive;
  - la phase semi-active.
– Un ensemble plus complet de transitions link_up est inclus dans le diagramme.
– Les appareils à port simple et à ports multiples sont compatibles.

Un appareil doit mettre en œuvre le mécanisme ACD avec le comportement spécifié dans la Figure 23.

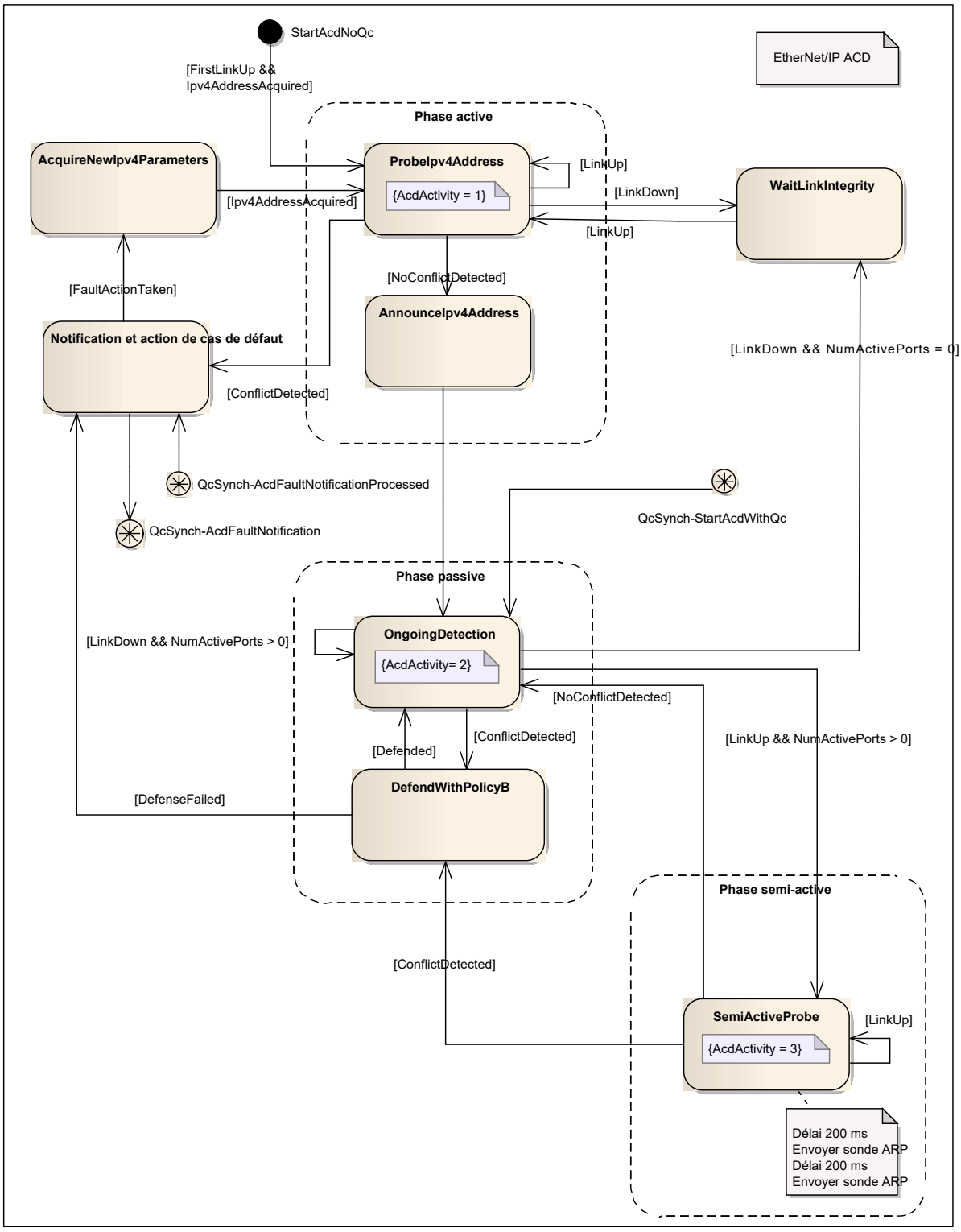


Figure 23 – Comportement ACD

7.5.8.3 Détails ACD

7.5.8.3.1 Contraintes temporelles IPv4 ACD

L'IETF RFC 5227, 1.1 spécifie un nombre de contraintes temporelles. Certaines de ces contraintes ne sont pas optimales pour les applications et réseaux de type 2. Plus particulièrement, les délais de démarrage causés par les intervalles des sondes ARP seraient inacceptables dans un contexte industriel. L'adaptation des valeurs alternatives spécifiées est cohérente avec l'IETF RFC 5227, 1.3 concernant l'applicabilité.

Les appareils dotés de l'ACD doivent mettre en œuvre les valeurs alternatives suivantes pour les paramètres définis dans l'IETF RFC 5227, 1.1.

- PROBE_WAIT: 200 ms (délai aléatoire initial)
- PROBE_NUM: 4 (nombre de paquets de sondes)
- PROBE_MIN: 200 ms (délai minimal jusqu'à la sonde répétée)
- PROBE_MAX: 200 ms (délai minimal jusqu'à la sonde répétée)
- ANNOUNCE_WAIT: 200 ms (délai avant annonce)
- ANNOUNCE_INTERVAL: 2 s (délai entre les paquets d'annonce)
- DEFEND_INTERVAL: 2 s (intervalle minimal entre les ARP défensives)

Les appareils doivent se conformer à la temporisation indiquée dans l'IETF RFC 5227 telle que modifiée ci-dessus à ±10 %. Noter que les paramètres PROBE_MIN et PROBE_MAX définis sur la même valeur illustrent la recommandation CPF 2 visant à utiliser un intervalle fixe entre les sondes plutôt que la recommandation de l'IETF RFC 5227, 2.1.1 (Détails des sondes) selon laquelle les sondes ultérieures après la sonde initiale sont rendues aléatoires entre les valeurs PROBE_MIN et PROBE_MAX.

7.5.8.3.2 ProbeIpv4Address

Voir l'IETF RFC 5227, 2.1 et 2.1.1.

Outre les exigences spécifiées dans l'IETF RFC 5227, seules les sondes ARP envoyées à l'adresse de diffusion Ethernet doivent être prises en compte pour la détection de conflit. Les messages ARP dirigés (envoyés à l'adresse MAC Ethernet de l'appareil) avec l'adresse IP de l'expéditeur de 0.0.0.0 ne doivent pas être traités comme un conflit.

NOTE Cette exigence n'est pas en contradiction avec l'IETF RFC 5227, qui définit les sondes ARP comme étant diffusées sur la liaison locale.

7.5.8.3.3 AnnounceIpv4Address

Voir l'IETF RFC 5227, 2.3.

Une fois que l'appareil a envoyé sa première annonce ARP, il doit passer à l'état OngoingDetection.

NOTE La phase OngoingDetection se produit en même temps que la phase AnnounceIPv4Address.

7.5.8.3.4 WaitLinkIntegrity

L'activité WaitLinkIntegrity attend l'occurrence d'un événement LinkUp depuis un port Ethernet.

Cette activité est initiée dans deux scénarios:

- premièrement lorsqu'un événement LinkDown se produit sur un appareil à port unique;
- deuxièmement, lorsqu'un événement LinkDown se produit sur un appareil à ports multiples et que tous ses autres ports Ethernet sont également inutilisables.

Lorsqu'un événement LinkUp se produit, l'activité ProbeIpv4Address est initiée.

Lorsqu'un appareil détecte que l'intégrité de la liaison Ethernet a été perdue puis retrouvée (par exemple, le câble réseau a été retiré puis remis), l'appareil doit redémarrer l'activité ProbeIpv4Address initiale.

7.5.8.3.5 Notification et action de cas de défaut

Voir l'IETF RFC 5227, Article 1.

Outre le comportement de l'IETF RFC 5227, lorsqu'un conflit d'adresses est détecté, les appareils de type 2 doivent prendre les actions de cas de défaut suivantes:

- définir l'état de l'appareil sur Recoverable Fault (défaut récupérable) (voyant d'état du module rouge clignotant);
- définir le voyant d'état du réseau sur rouge fixe.

Il existe 2 transitions de synchronisation entre l'activité ACD Notification & FaultAction et le diagramme de comportement de QuickConnect.

QcSynch-AcdFaultNotification est une transition de synchronisation vers le diagramme de comportement de QuickConnect qui se produit lorsque le mécanisme ACD contient un défaut ConflictDetected provenant de l'activité ProbeIpAddress ou un défaut DefenseFailed provenant de l'activité DefendWithPolicyB.

QcSynch-AcdFaultNotificationProcessed est une transition de synchronisation du diagramme de comportement QuickConnect vers l'activité Notification & FaultAction qui se produit après que QuickConnect a traité la précédente AcdFaultNotification.

7.5.8.3.6 AcquireNewIpv4Parameters

Voir l'IETF RFC 5227, Article 1.

Après notification de la détection d'un conflit d'adresses IPv4, l'appareil peut être conçu pour obtenir ou utiliser une adresse IPv4 alternative. La conception de cette méthode et la sélection qui en résulte pour les paramètres IPv4 sont propres au fournisseur.

Si un événement LinkDown se produit sur le dernier port actif alors que l'activité est AcquireNewIpv4Parameter, le processus ACD illustré dans la Figure 23 (Comportement ACD) doit s'achever. Le processus ACD doit être redémarré après qu'au moins une liaison ait été rétablie et qu'une configuration IPv4 valide ait été acquise conformément à la Figure 21 et la Figure 22 qui illustrent le comportement de l'objet TCP/IP.

Noter également que les appareils CP 2/2 doivent limiter la fréquence à laquelle ils sondent de nouvelles adresses candidates en utilisant les paramètres MAX_CONFLICTS et RATE_LIMIT_INTERVAL comme défini dans l'IETF RFC 5227, 2.1.1.

7.5.8.3.7 OngoingDetection

Voir l'IETF RFC 5227, 2.4.

L'IETF RFC 5227, 2.4 déclare que “la détection de conflit d'adresses ne se limite pas uniquement au moment de la configuration d'interface initiale, lorsqu'un hôte envoie des sondes ARP. La détection de conflit d'adresses est un processus continu en vigueur tant qu'un hôte utilise une adresse.

Après sondage réussi et utilisation d'une adresse IP, un appareil doit effectuer une détection de conflit et une défense continues, conformément à l'IETF RFC 5227.

QcSynch-StartAcdWithQc est une transition de synchronisation avec le diagramme de comportement de QuickConnect. Si QuickConnect est activé sur l'appareil, l'activité de l'ACD démarre à ce stade.

Le mécanisme ACD tel que spécifié dans l'IETF RFC 5227, 2.1 déclare qu'"un hôte ne doit pas effectuer cette vérification périodiquement", indiquant qu'il n'est pas nécessaire que les sondes ARP périodiques soient envoyées dans le cadre de la détection continue. Toutefois, il a été observé que les sondes ARP périodiques permettent au module de détecter des conflits avec des appareils qui peuvent ne pas avoir été connectés au réseau lors du sondage initial, ou lorsque les commutateurs ont perdu les sondes ARP initiales en raison du délai de transmission initial. Par conséquent, il convient que les appareils de type 2 qui fournissent l'algorithme ACD émettent des sondes ARP périodiques durant la détection continue.

Les appareils de type 2 prenant en charge les sondes ARP périodiques doivent utiliser un délai de transmission dans la plage comprise entre ONGOING_PROBE_MIN et ONGOING_PROBE_MAX selon les valeurs ci-dessous:

- ONGOING_PROBE_MIN: 90 s (intervalle minimal pour les sondes continues);
- ONGOING_PROBE_MAX: 150 s (intervalle maximal pour les sondes continues).

Ces valeurs ne sont pas définies dans l'IETF RFC 5227. Les appareils ne doivent pas dépasser cette plage spécifiée de plus de 10 % aux deux extrémités.

Il est recommandé que le délai de transmission initial pour la première sonde ARP périodique ait une valeur pseudo-aléatoire dans la plage de ONGOING_PROBE_MIN et ONGOING_PROBE_MAX. (rendue "aléatoire" à l'aide de l'adresse MAC Ethernet comme cela est montré par exemple en 7.5.8.3.9). Le délai de transmission pour les sondes ARP périodiques ultérieures peut ne pas être rendu aléatoire et peut, par exemple, sélectionner la valeur centrale (120 s).

7.5.8.3.8 DefendWithPolicyB

Voir l'IETF RFC 5227, 2.4.

En cas de détection d'un conflit d'adresses, l'appareil doit défendre son adresse conformément à l'alternative (b) indiquée dans l'IETF RFC 5227, 2.4.

Si un conflit persiste (tel que défini par l'IETF RFC 5227), l'appareil doit immédiatement cesser d'utiliser cette adresse et exécuter les actions de notification et de défaut spécifiées en 7.5.8.3.5.

7.5.8.3.9 SemiActiveProbe

L'activité SemiActiveProbe est initiée lorsqu'un appareil à ports multiples reçoit un événement LinkUp pendant que les autres ports sont toujours actifs.

L'activité SemiActiveProbe consiste en une activité de sondage modifiée dans laquelle seules deux sondes ARP sont envoyées à l'aide de délais de sondage de 200 ms.

L'activité SemiActiveProbe est définie pour réduire le volume de trafic de diffusion ARP qui sera initié depuis l'activité LinkUp sur les appareils à ports multiples.

7.5.8.3.10 Exemple d'algorithme de délai pseudo-aléatoire (informative)

NOTE L'algorithme Xorshift Random Number Generator suivant est fondé sur le travail de George Marsaglia de la Florida State University.