Contrôle d'accès en présence de changements topologiques : différentes stratégies

Marie-Mélisande Tromparent[(1)]

(1) Université technique de Munich – Département réseaux de communications, Munich, Allemagne.

Résumé

Contrôler l'accès à un réseau apparaît comme un moyen de fournir aux utilisateurs certaines garanties concernant la qualité de service. Dans cet article, nous nous intéressons au cas particulier d'un mécanisme de contrôle d'accès basé sur la connaissance topologique du réseau. Nous proposons différentes stratégies pouvant être employées pendant la courte période qui sépare l'intervention d'un changement dans le réseau (par exemple l'arrêt anormal d'un routeur) et le retour à la normale dans le réseau. Dans une telle situation, il est souhaitable que l'entité responsable du contrôle d'accès continue à prendre des décisions raisonnables dans la mesure du possible, bien qu'elle ne dispose plus d'une vue actuelle du réseau. Différentes stratégies sont présentées dans cet article, allant d'une approche simpliste consistant à rejeter (resp. accepter) systématiquement tous les appels à des approches plus sophistiquées basées sur la définition de zones.

Keywords: QoS, Contrôle d'accès (Admission Control)

1 Introduction

L'émergence de nouvelles applications aux exigences très strictes a entrainé l'évolution rapide de la recherche dans le domaine de la qualité de service ces dernières années. Entre autres choses, le contrôle d'accès à un réseau (CAC, Call Admission Control) a connu un développement marqué. On dit d'une entité qu'elle fournit un contrôle d'accès au réseau lorsque tout établissement d'une communication est soumis à son autorisation. Un telle entité sera désormais appelée Admission Controller, AC. La fonction de contrôle d'accès est naturellement essentielle dans le contexte des applications interactives telles que la téléphonie ou la vidéoconférence sur internet.

Dans cet article, on s'intéresse plus particulièrement au cas d'un contrôle d'accès basé sur la connaissance de la topologie, de la configuration et de l'occupation des ressources dans le réseau. Un tel mecanisme est utilisé dans l'architecture « Resource Management » brièvement décrite dans le chapitre 2. Lorsqu'un changement survient dans le réseau (comme par exemple l'arrêt anormal d'un routeur ou d'un lien), il faut un certain temps au réseau pour retrouver un état stable (entre autres choses, à cause du temps de convergence du protocol de routage). Il est néanmoins souhaitable que l'AC continue à prendre des décisions raisonnables. On désignera dans la suite par état transitoire la courte période séparant la défection d'un élément du réseau et le retour à la stabilité du réseau.

Cet article est divisé de la facon suivante : Le chapitre 2 décrit brièvement l'architecture « Resource Management » qui représente notre champ d'application pour les différents principes énoncés plus loin. Dans le chapitre 3, le problème de contrôle d'accès dans des conditions exceptionnelles est exposé de facon plus globale, délimitant ainsi clairement l'objet de cet article. Les chapitres 4 et 5 présentent des solutions concrètes au problème du contrôle d'accès en régime transitoire, élémentaires dans le chapitre 4, plus sophistiquées dans le chapitre 5. Enfin, le chapitre 6 reprend les idées principales développées dans les paragraphes précédents et conclut cet article.

2 L'architecture « Resource Management »

L'architecture « Resource Management » ([1], [2]) est une architecture destinée à fournir un certaine qualité de service aux utilisateurs de réseaux IP. Elle peut être couplée avec une architecture de service telle que H.323 [3] ou SIP [4]. Elle fournit différents niveaux de qualité (stricte ou statistique) dans le contexte de réseaux d'entreprises. De même que l'architecture DiffServ (Differentiated Services, [5]) développée par l'IETF, l'architecture « Resource Management » est basée sur le principe de l'aggregation de trafic en classes de service au niveau des couches 2-3 du modèle OSI. Les ressources du réseau (buffer des noeuds, et capacités des liens) sont assignées explicitement à chaque classe de service par configuration.

Les *Resource-Managers* (RMs) sont des serveurs particuliers de l'architecture « Resource Management », responsables de la gestion des ressources. Ils agissent au sein de domaines particuliers, appelés RM Domaines. Tout utilisateur souhaitant établir une communication doit avant tout s'adresser au RM dont il dépend. Celui-ci décide alors d'accepter ou non l'établissement de la communication (rôle d'Admission Controller). Chaque RM connaît complètement son domaine (topologie, configuration de chaque classe de service et occupation des ressources), de telle facon qu'il peut prendre les décisions nécessaires en fonction de la qualité désirée par l'utilisateur. Lorsqu'un RM accepte une communication, les ressources nécessaires pour celle-ci sont virtuellement réservées par le RM, ce qui rapproche l'architecture « Resource Management » d'IntServ (Integrated Services, [6]).

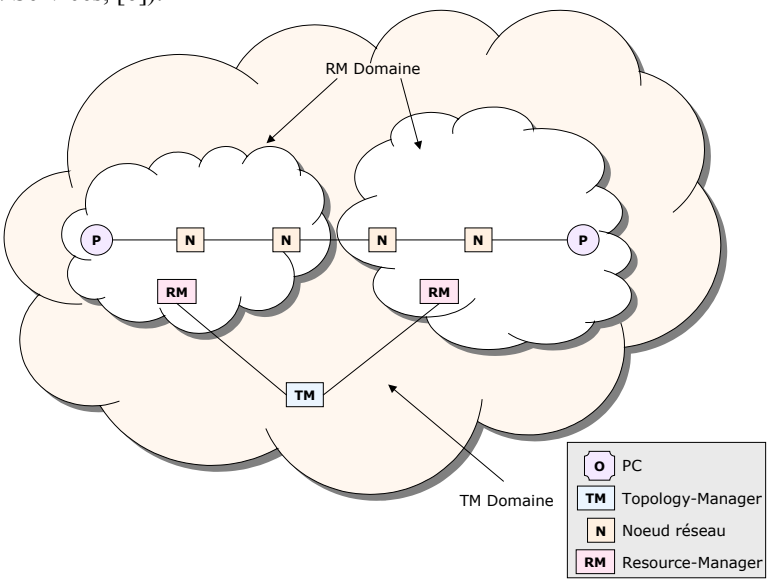

Figure 1 *Vue d'ensemble de l'architecture "Resource Management"*

Etant données la topologie et la configuration du réseau, le RM est capable de maintenir une carte de la charge du réseaux, l'actualisant à chaque fois qu'une communication est acceptée ou terminée. Cependant, il doit recevoir la topologie et la configuration d'une autre entité . Ces entités particulières de l'architecture « Resource Management » s'appellent « Topology-Managers » [7] (TMs). De même que les RMs, les TMs sont responsables de domaines limités appelés TM domaines. Pour des raisons de scalabilité et de flexibilité, un TM domaine peut comprendre plusieurs RM domaines. Le TM acquiert sa connaissance de la topologie du réseau grace à une procédure automatique décrite dans [7], basée sur les protocoles SNMP [8] et ICMP [9]. RM et TM ont été implémentés dans le cadre de cette recherche.

Bien que le contexte de cet article soit l'architecture « Resource Management », les différentes stratégies décrites dans la suite sont applicables dans beaucoup d'autre contextes, où le contrôle d'accès est réalisé grâce à la connaissance du réseau sous-jacent.

3 Vue d'ensemble du procédé

La figure 2 décrit les différents modes de fonctionnenemnt d'un Admission Controller, tel que le Resource-Manager par exemple. Au démarrage, l'AC procède à un certain nombre d'initialisations, avant d'entrer en mode normal. En mode normal, il est capable de traiter des requêtes, d'effectuer des réservations de ressources et de répondre en conséquence. Si un changement dans le réseau survient, celui-ci doit être détecté au plus vite (par le Topology-Manager dans le cas de l'architecture « Resource Management »), et transmis à l'AC. À ce stade, l'AC sait qu'un changement est intervenu, mais ne sais pas exactement lequel. De plus, le réseau est en phase transitoire de convergence, si bien qu'il est impossible pour l'AC de connaître la topologie instantanée du réseau. Malgré cela, il doit continuer de remplir sa fonction. Ce mode particulier de fonctionnement est appelé mode exceptionnel ou régime transitoire. Au bout d'un certain temps (dépendant essentiellement du temps de convergence du protocole de routage utilisé), le réseau converge, et la topologie est à nouveau fixe. A ce moment-là, l'AC doit réévaluer toutes ses réservations de ressources, afin de déterminer si la nouvelle topologie offre les ressources suffisantes pour les autoriser toutes. Si tel n'est pas le cas, l'AC interrompra éventuellement certaines des communications actives.

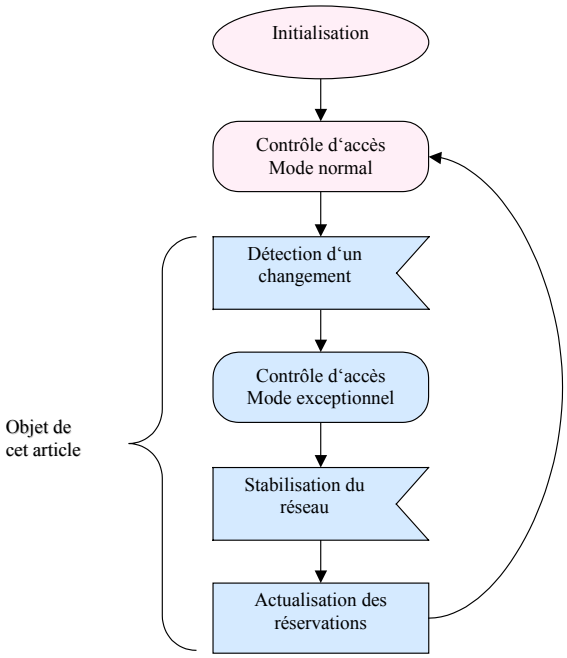

Figure 2 *Diagramme d'état de l'Admission Controller*

Cet article traite uniquement de l'état « contrôle d'accès en mode exceptionnel ». Quelques détails supplémentaires sont fournis sur les autres états dans [10].

4 Contrôle d'accès pendant le régime transitoire : approches extrêmes

À ce stade, l'AC sait qu'un changement s'est produit dans le réseau, mais n'en connaît pas les conséquences sur la topologie, car le réseau n'a pas encore convergé. Il continue cependant à recevoir des requêtes d'utilisateurs souhaitant établir des communications, et doit leur fournir une réponse malgré tout. Nous proposons ici différentes stratégies sur la manière de prendre la décision d'accepter ou non une communication étant donné cette situation particulière que représente le régime transitoire.

4.1 Approche simpliste

Une facon très simple de résoudre ce problème consiste à ne rien changer, c'est-à-dire que l'AC continue à utiliser les mêmes règles de contrôle d'accès qu'en régime normal. Cette solution basique peut donner des résultats satisfaisants dans le cas d'un réseau bien concu et bien dimensionné ou bien dans le cas où le lien (resp. noeud) défectueux est inutilisé. Cette approche a l'avantage évident d'être facile à implémenter !

4.2 Approche pessimiste

Une autre facon très simple de réagir dans ce contexte consiste à refuser tous les appels entrants pendant le régime transitoire. Cette approche est la plus fidèle à l'esprit de l'architecture « Resource Management » dans la mesure où aucune communication n'est acceptée, dont on ne puisse garantir la qualité percue par l'utilisateur. Cependant, puisque l'on ne connaît pas les conséquences du changement survenu dans le réseau sur la topologie, il est de toutes facons impossible de fournir quelque garantie que ce soit. Par ailleurs, cette approche n'est pas intéressante du point de vue du fournisseur de service qui souhaite maximiser ses profits, c'est-à-dire le nombre de communications actives.

4.3 Approche optimiste

Cette approche au contraire de la précédente consiste à accepter toutes les communications entrantes. Avantages et inconvénients sont diamétralement opposés à ceux du cas précédent : les communications initiées pendant le régime transitoire sont systématiquement acceptées. Du point de vue du fournisseur de service, cette solution est avantageuse, puisqu'elle maximise le nombre de communications actives, et donc le profit. Cependant, accepter un certains nombre de communications sans garantie peut entraîner la dégradation de la qualité de communications établies qui n'étaient pas concernées jusqu'à présent. Cette approche a donc tendance à négliger les intérêts de l'utilisateur aux dépens de ceux du fournisseur de service.

4 Contrôle d'accès pendant le régime transitoire : approches intermédiaires

Les différentes approches présentées chapitre 4 sont naturellement trop extrêmes pour être appliquées en l'état. C'est pourquoi nous décrivons dans ce nouveau chapitre un certain nombre de variantes intermédiaires permettant d'apporter une réponse au problème du contrôle d'accès pendant le régime transitoire.

5.1 Approche locale

Cette approche concerne le cas particulier où l'AC sait exactement quel changement dans le réseau s'est produit. Considérons dans un premier temps qu'il s'agit d'une panne de routeur. Nous proposons dans ce cas de définir une zone Z autour de ce routeur et d'appliquer la règle suivante : Toute communication entrant pendant le régime transitoire et dont la route à travers le réseau coupe la zone Z est systématiquement refusée. Pour toute autre communication, les règles de contrôle d'accès du mode normal sont appliquées. Conceptuellement, la zone Z représente la zone qui a le plus de chance statistiquement d'être touchée par le changement. Il est intéressant de remarquer que si Z est vide, cette approche correspond à l'approche optimiste. Si au contraire Z équivaut au domaine géré par l'AC, cette approche correspond exactement à l'approche caractérisée de simpliste dans le chapitre 4. Cette approche locale est évidemment applicable dans le cas où au lieu d'un routeur, c'est un lien qui tombe en panne. Tout le problème qu'il reste désormais à résoudre concerne la facon de définir cette zone Z. Les paragraphes suivants proposent quelques solutions possible.

5.1.1 Définition de la zone Z par un nombre de hops

Dans ce premier cas, nous proposons d'utiliser un nombre de hops pour définir la zone Z (cf figure 3). Plus le nombre de hop est élevé, moins il existe de communications ne traversant pas la zone Z, et donc plus une communication entrant pendant le régime transitoire a de chances d'être refusée. Cette approche est justifiée par le fait que les routes qui risquent d'être influencées par le changement survenu dans le réseau sont celles qui passent le plus près (en terme de nombre de hops) de l'élément défectueux.

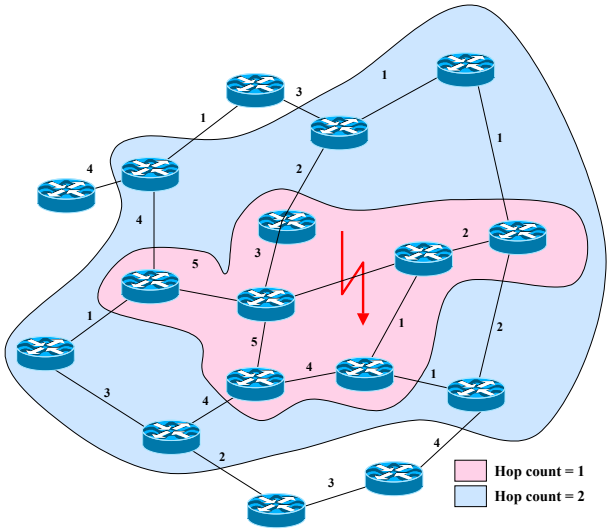

Figure 3 *Définition de la zone Z par un nombre de hops*

5.1.2 Définition de la zone Z par une distance

Une autre possibilité pour définir la zone Z consiste à utiliser la distance à l'élément défectueux (on peut pour cela utiliser les même métriques que le protocole de routage). Figure 4 montre sur le même réseau que précédemment ce à quoi correspond un zone définie par une distance à l'élément défectueux inférieure ou égale à 5 (resp. 3).

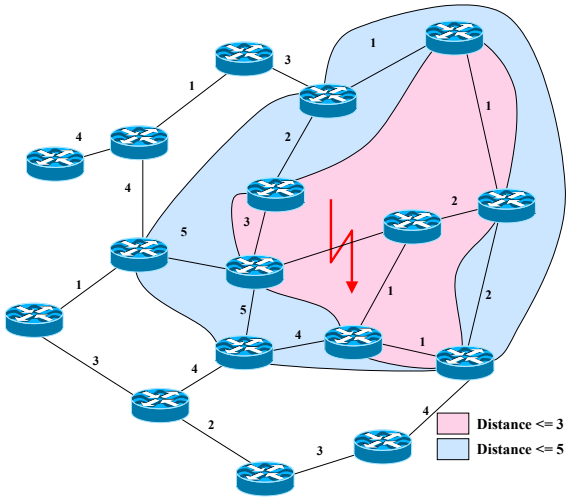

Figure 4 *Définition de la zone Z par une distance*

Le choix de la zone est décisif quant à l'efficacité de la méthode. Il est cependant impossible de dire de facon inconditionnelle qu'une approche est meilleure qu'une autre. Le choix de la zone dépend entièrement du type de

réseau sous-jacent. Pour un réseau pourvu de mécanismes de protection, il est suffisant de définir Z comme la zone « nombre de hop = 1 ». Au contraire pour un réseau faiblement protégé contre les pannes, il est indispensable de définir une zone plus large (soit par un nombre de hop plus important, soit par une distance plus grande).

Il est intéressant de remarquer que dans le cas où le protocole de routage utilisé est RIP (Routing Information Protocol, [11]), les deux méthodes précédentes se confondent puisque RIP utilise le nombre de hops comme métrique.

5.2 Approche locale améliorée

Cette dernière approche est similaire à la précédente en ce sens que l'on définit une zone Z autour de l'élément défectueux, zone ayant statistiquement une plus grande probabilité d'être touchée par le changement. Pour toute communication active au moment où le changement se produit dans le réseau, on réserve virtuellement les ressources nécessaires à cette communication sur tous les liens et nœuds de la zone Z (avant même de traiter d'éventuelles demandes d'établissement de communications entrantes). Cela revient en somme à tenter de prévoir le reroutage effectué par le réseau. Autrement dit, on suppose dans cette méthode que toute communication passant par l'élément défectueux sera après la convergence du réseau reroutée à l'intérieur de la zone Z. Après avoir effectué ces réservations virtuelles, l'AC peut poursuivre son contrôle d'accès de même qu'en régime normal, avec un traitement particulier pour les communications traversant l'élément défectueux (refus systématique, réservation sur tous les liens et nœuds de la zone Z, etc.).

Cette méthode à l'avantage de limiter l'impact du changement sur les communications actives au moment où il s'est produit. Par ailleurs, elle offre un compromis entre les approches extrêmes présentées au chapitre 4, ce qui signifie également un compromis entre le profit réalisé par le fournisseur de service et la qualité ressentie par les utilisateurs. Cette méthode est particulièrement efficace dans les réseaux faiblement protégés ou dimensionnés de facon économe.

6 Conclusion

Contrôler l'accès à un réseau apparaît comme un moyen de fournir aux utilisateurs certaines garanties concernant la qualité de service. Dans cet article, nous nous intéressons au cas particulier d'un mécanisme de contrôle d'accès basé sur la connaissance topologique du réseau. Nous proposons différentes stratégies pouvant être employées pendant la courte période qui sépare l'intervention d' un changement dans le réseau (par exemple l'arrêt anormal d'un routeur) et le retour à la normale dans le réseau.

La méthode la plus simple est évidemment de ne rien changer, c'est-à-dire d'appliquer les mêmes règles lors du fonctionnement normal et pendant le régime transitoire. On peut aussi choisir d'accepter systématiquement (resp. refuser systématiquement) toute appel entrant pendant le régime transitoire. Ces approches étant quelque peu simplistes, nous avons imaginé des approches plus complexes basées sur la définition d'une zone « plus probablement concernée par le changement ». Il est alors possible de prendre des décisions différentes selon les appels entrants : On peut supposer qu'un appel entrant ne traversant pas la zone déterminée ne sera pas concerné par le changement, et prendre de ce fait la même décision qu'en mode normal. Pour un appel entrant traversant la zone critique, plusieurs possibilités se présentent : accepter (resp. refuser) systématiquement l'appel ; réserver plus de capacité que nécessaire ; réserver les ressources nécessaires sur différents chemins susceptible d'être empruntés après reroutage.

Dans les prochains mois, nous prévoyons de complèter ces travaux par une implémentation des divers procédés, ainsi qu'une évaluation précise des différentes stratégies en fonction du type de réseaux.

7 Remerciements

Les travaux présentés ici sont issus d'un projet appelé CoRiMM (Control of Resources in Multidomain Multiservice networks) financé par Siemens. C'est pourquoi nous souhaitons remercier messieurs Totzke, Mueller et Glasmann ainsi que le reviewers anonymes pour leurs précieux commentaires.

Références

[1] C. Prehofer, H. Müller, J. Glasmann, Scalable Resource Management Architecture for VoIP, Proc. of PROMS 2000, Cracow, Oct. 2000.
[2] J. Glasmann, H. Müller, Resource Management Architecture for RealtimeTraffic in Intranets, Networks 2002, Joint IEEE International Conferences ICN and ICWLHN, Atlanta, USA, August 2002.
[3] ITU-T Rec. H.323, Packet-Based Multimedia Communications Systems, Geneva, Switzerland, Nov. 2000; http://www.itu.int/itudoc/itu-t/rec/h (link to substandards)
[4] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, SIP: Session Initiation Protocol. IETF RFC 2543, March 1999.
[5] K. Nichols, V. Jacobson, L. Zhang, A Two-bit Differentiated Services Architecture for the Internet, Internet RFC 2638, July 1999.
[6] R. Braden, D. Clark, S. Shenker, Integrated Services in the Internet Architecture: an Overview, Internet RFC 1633, Jun. 1994.
[7] J. Glasmann, M. Tromparent, Topology Discovery in the Context of Resource Management in IP-Networks, SoftCOM'02, Split, Croatia, Oct. 2002.
[8] J. Case, M. Fedor, M. Schostall, J. Davin, A Simple Network Management Protocol (SNMP), RFC 1157, Mai 1990.
[9] J. Postel, Internet Control Message Protocol (ICMP), RFC 792, September 1981.
[10] M. Tromparent, J. Glasmann, H. Mueller, J. Totzke, Admission Control Strategies in Transient Network States, ICT'2003, Papeete, French Polynesia, Fevrier 2003
[11] G. Malkin, RIP Version 2, Internet RFC 2453, November 1998