ETSI GR NGP 009 V1.1.1 (2019-02)

Futurs Protocoles Génération (NGP); Un exemple d'une architecture de protocole de réseau non-IP basé sur des principes de conception RINA

Avertissement

Le présent document a été élaboré et approuvé par les Protocoles de génération (NGP) ETSI Industry Group specification (ISG) et représente les vues des membres qui ont participé à cette ISG. Il ne représente pas nécessairement l'opinion de l'ensemble des membres de l'ETSI.

Référence
DGR / NGP-009

Mots clés
API, architecture, Internet, méta-protocole,
réseau, le protocole de nouvelle génération, protocole

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel .: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N ° 348 623 562 00017 - NAF 742 C
Association à but non lucratif à la Enregistrée
Sous-Préfecture de Grasse (06) N ° 7803/88

Contenu

ETSI

Droits de propriété intellectuelle

brevets essentiels

DPI essentiels ou potentiellement essentiels aux produits livrables normatifs peuvent avoir été déclarés à l'ETSI. Les informations relatives à ces droits de propriété intellectuelle essentiels, le cas échéant, est accessible au public pour les membres et non-membres de l'ETSI et se trouve dans ETSI SR 000 314: « Droits de propriété intellectuelle (DPI), essentiels ou non essentiels, DPI notifiés à l'ETSI en ce qui concerne les normes ETSI », qui est disponible auprès du Secrétariat de l'ETSI. Dernières mises à jour sont disponibles sur le serveur Web de l'ETSI (https://ipr.etsi.org/).

Conformément à la politique des DPI ETSI, aucune enquête, y compris les recherches de DPI, a été réalisée par l'ETSI. Aucune garantie ne peut être donnée quant à l'existence d'autres DPI non mentionnés dans ETSI SR 000 314 (ou les mises à jour sur le serveur Web ETSI) qui sont, ou peuvent être, ou peuvent devenir, essentiels au présent document.

marques de commerce

Le présent document peut contenir des marques de commerce et / ou des appellations commerciales qui sont affirmées et / ou enregistrés par leurs propriétaires. ETSI ne revendique pas la propriété de ces sauf pour tout indiqués comme étant la propriété de l'ETSI, et transmet pas le droit d'utiliser ou de reproduire une marque de commerce et / ou nom commercial. La mention de ces marques dans le présent document ne constitue pas une approbation par l'ETSI des produits, des services ou des organismes associés à ces marques.

avant-propos

Ce rapport du groupe (GR) a été produit par le Groupe spécification de l'industrie (ISG) de l'ETSI et des futurs Génération de Protocoles (NGP).

terminologie verbes modaux

Dans le présent document « devrait », « ne devrait pas », « peut », « n'a pas besoin », « sera », « ne sera pas », « peut » et « ne peut pas » doivent être interprétés comme décrit à l'article 3.2 de laETSI Règles de rédaction (formes verbales pour exprimer des dispositions).

« Doit » et « ne doit pas » ne sont pas autorisés dans des documents ETSI, sauf lorsqu'ils sont utilisés dans la citation directe.

introduction

l'architecture de protocole réseau fournit un ensemble de modèles et la méthodologie qui guide réseau (protocole) les concepteurs dans l'accomplissement de leur tâche. Il capture les règles et les modèles qui sont invariantes par rapport aux besoins spécifiques de chaque réseau (cellulaire, centre de données, le capteur, l'accès, le noyau, l'entreprise, LAN, etc.). Aujourd'hui, l'architecture de protocole de réseau répandu (généralement appelé « suite de protocoles Internet »), vaguement basé sur OSI fournit des modèles trop peu et points communs et a des défauts de conception fondamentaux dans sa structure, de nommage et d'adressage, API service et de sécurité. Ces questions contribuent à une explosion du nombre des protocoles réseau nécessaires, à la fois pour couvrir les besoins de plusieurs cas d'utilisation et de travailler autour des principaux défauts de conception.

Le récursive InterNetwork Architecture (RINA) est un « retour aux sources » approche d'apprentissage de l'expérience avec TCP / IP et d'autres technologies dans le passé. Les résultats des recherches à ce jour ont montré que de nombreux problèmes de réseau de longue date peuvent par nature être résolus par la structure résultant de la théorie des réseaux. Par conséquent, des mécanismes supplémentaires ne sont pas nécessaires.

RINA fournit les outils nécessaires pour résoudre les problèmes de l'architecture Internet (complexité, l'évolutivité, la sécurité, la mobilité, la qualité du service ou de la direction pour ne nommer que quelques-uns). RINA est basé sur un seul type de couche, qui est répétée autant de fois que nécessaire par le concepteur du réseau. La couche est appelée une installation IPC distribué (DIF), qui est une application distribuée qui fournit des services de communication Inter Processus (IPC) sur un périmètre donné aux applications distribuées ci-dessus (qui peuvent être d'autres applications ou régulières DIF). Ces services IPC sont définis par l'API DIF, ce qui permet des instances d'autres applications DIFs-de recevoir des flux IPC avec certaines caractéristiques (telles que la perte, le retard, dans l'ordre de livraison) à d'autres instances de l'application. Par conséquent, une couche peut est un allocateur de ressource qui fournit et gère le service IPC four un champ donné (lien, réseau, interréseau, VPN, etc.). Il alloue des ressources (mémoire tampon, bande passante, la capacité de planification) aux flux concurrents.

Tous offrent les mêmes DIF services grâce à leur API et ont les mêmes composants et la structure. Chaque couche comporte deux ensembles de cadres de protocole: un pour le transfert de données (appelé EFCP, erreur et protocole de contrôle de flux), et un pour la gestion de la couche (CDAP, le protocole d'application Distributed Common). Cependant, tous les fonctionnent sur le DIF même portée et de l'environnement et ils ne doivent fournir le même niveau de service. Par conséquent, les parties invariantes (mécanismes) et des pièces de variantes (politiques) sont séparées en différents composants de la transmission des données et des cadres de protocole de gestion de couche. Cela permet de personnaliser le comportement d'un fonctionnement optimal DIF dans un certain environnement avec un ensemble de politiques pour cet environnement au lieu du traditionnel « taille unique »

Last but not least, RINA peut être déployé progressivement où il a les incitations et interopérer avec les technologies actuelles telles que l'IP, Ethernet, MPLS, WiFi, cellulaire ou autres.

1 Portée

Aujourd'hui, la plupart des protocoles de réseau suivent vaguement la structure en couches de l'architecture de réseau OSI. Les protocoles sont organisées en un nombre de couches statique, dans lequel chaque couche fournit une fonction différente de la couche ci-dessus. Les limites de cette structure ont conduit à une explosion du nombre de protocoles à chaque couche avec peu ou pas communs, les violations de la couche et la nécessité d'extensions ad hoc du nombre de couches où l'architecture ne peut pas modéliser les réseaux du monde réel avec suffisamment de fidélité (par exemple des couches de 2,5 ou 3,5, des réseaux virtuels, etc.). SDO développent indépendamment des protocoles pour les différentes couches de l'architecture de protocole, plusieurs fois répliquant le travail de chacun et conduisant à l'inefficacité au niveau du système. Cela se traduit par:

a) les réseaux qui sont très complexes à utiliser et à dépanner;

b) spécification et la mise en œuvre de nouveaux protocoles qui ajoutent peu de valeur à la base existante; et

c) un système en réseau global qui est loin d'un niveau d'intégration optimale du point de vue de la conception de systèmes.

Le présent document décrit les propriétés d'une architecture de réseau non-IP basé sur des principes de conception RINA. architecture réseau capture toutes les règles et les modèles qui sont indépendants des exigences adressées par des protocoles de réseau individuels. Il permet de résoudre les problèmes qui sont génériques à un réseau (par exemple la structure, le nommage et d'adressage, les modèles de sécurité ou QoS) au niveau de l'architecture, en évitant la nécessité de protocoles individuels pour résoudre ces problèmes par eux-mêmes. RINA a été conçu pour capturer les invariants de toutes les formes de mise en réseau, en fournissant SDO et concepteurs de réseaux avec un cadre commun et une méthodologie pour concevoir et construire des protocoles pour tout type de réseau. Ainsi, une architecture de protocole de réseau comme RINA encourage les réseaux avec moins de protocoles et plus communs,

2 Références

2.1 Références normatives

références normatives ne sont pas applicables dans le présent document.

2.2 références informatives

Les références sont soit spécifiques (identifiées par date de publication et / ou numéro d'édition ou numéro de version) ou non spécifique. Pour les références spécifiques, seule la version citée applique. Pour les références non spécifiques, la dernière version du document de référence (y compris les amendements).

REMARQUE: Bien que les liens hypertexte inclus dans cette clause étaient valides au moment de la publication, l'ETSI ne peut garantir leur validit à long termey.

Les documents de référence suivants ne sont pas nécessaires à l'application du présent document, mais ils aident l'utilisateur à l'égard d'un domaine particulier.

[I.1] IETF RFC 62: « Un système de communication inter-processus dans un réseau de partage des ressources », Août 1970, DC Walden.

REMARQUE: Disponible à https://tools.ietf.org/rfc/rfc62.txt.

[I.2] INWG-96 (1975): "Proposition de fin Protocole international pour mettre fin", V. Cerf, A. McKenzie, R. Scantleburie, H. Zimmerman.

REMARQUE: Disponible à http://dotat.at/tmp/INWG-96.pdf.

[I.3] IETF RFC 793: "Transmission Control Protocol", Septembre 1981, Université du Sud Californie.

REMARQUE: Disponible à https://tools.ietf.org/html/rfc793.

[I.4] ETSI GS NGP 007: "Suivant Protocoles génération (NGP), NGP modèle de référence".
REMARQUE: Disponible à https://www.etsi.org/deliver/etsi_gs/NGP/001_099/007/01.01.01_60/gs_NGP007v010101p.pdf.

[I.5] ISO / CEI 7498-1: 1994: « Technologies de l'information - interconnexion des systèmes ouverts - de base
Modèle de référence: Le modèle de base ».

[I.6] IETF draft-ietf-tap-arc-02: "Une architecture pour les services de transport", Janvier 2018, T. Pauly,
B. Trammell, A. Brunstrom, G. Fairhurst, C. Perkins, P. Tiesel, C. Wood.
REMARQUE: Disponible à https://datatracker.ietf.org/doc/draft-ietf-taps-arch/?include_text=1.

[I.7] PB Hansen: « Le noyau d'un système multi-programmation », Communications de l'ACM 13 (4): 238-241. Avril 1970.
REMARQUE: Disponible à https://dl.acm.org/citation.cfm?id=362278&dl=ACM&coll=GUIDE.

[I.8] Jour J.: "Patterns in Network Architecture: Un retour aux fondamentaux". Prentica Hall, 2008.

[I.9] R. Watson: « mécanisme basé retardateur dans la gestion de connexion de protocole de transport fiable »,
Computer Networks, 5: 47-56, 1981.

[I.10] G. Gursun, I. Matta et K. Mattar: « sur la performance et la robustesse de gestion fiable
Les liaisons de transport », 8e Atelier international sur PFLDNeT, Novembre de 2010.

[I.11] G. Boddapati, J. Day, I. Matta, L. Chitkushev: « Évaluation de la sécurité d'un Internet table rase architecture », 20e Conférence IEEE sur les protocoles de réseau 2012.

[I.12] E. Grasa, O. Rysavy, O. Lichtner, H. Asgari, Jour J., L. Chitkushev: « De la protection des protocoles à
couches de protection: la conception, la mise en œuvre et l'expérimentation de politiques de sécurité en RINA »,
ICC 2016 IEEE.

[I.13] IETF RFC 4291: "architecture d'adressage IPv6", Février 2006, R. Hinden, S. Deering.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc4291.

[I.14] IETF RFC 4192: « Les procédures de renumérotation un réseau IPv6 sans un jour de drapeau », Septembre 2005, F. Baker, E. Lear, et R. Droms.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc4192.

[I.15] IETF RFC 5887: "renumérotation a besoin encore du travail", mai 2010, B. Carpenter, R. Atkinson, et
H. Flinck.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc5887.

[I.16] D. Leroy et O. Bonaventure: "Préparation des configurations de réseau pour renumérotation IPv6," International Journal of Network Management, vol. 19, no. 5, pp. 415-426,
Septembre / Octobre 2009.

[I.17] J. Small: « L'analyse des menaces de l'architecture distribuée inter-réseaux récursive installations IPC »,
BU Rapport technique 2011.
REMARQUE: Disponible à http://pouzinsociety.org/research/publications.

[I.18] Eduard Grasa, Leonardo Bergesio, Miquel Tarzan, Diego Lopez, John Day et Lou Chitkushev: « Réseau sans couture Renumérotation dans RINA: Automatiser Changement d'adresse sans rupture
Flux! », EUCNC 2017.
REMARQUE: Disponible à https://zenodo.org/record/1013204#.WeTDrROCxTY.

[I.19] IETF RFC 5944: "aide à la mobilité IP pour IPv4, révisée", Novembre 2010, C. Perkins.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc5944.

[I.20] IETF RFC 6275: "Aide à la mobilité dans IPv6", Juillet 2011, JAC Perkins, D. Johnson.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc6275.

[I.21] IETF RFC 5213: "IPv6 mobile Proxy", Août 2008, S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury et B. Patil.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc5213.

[I.22] IETF RFC 6830: "Le protocole de séparation Locator / ID (LISP)", Janvier 2013, D. Meyer, D. Lewis, D. Farinacci, V. Fuller.

[I.23] Jour J. et E. Grasa: « La mobilité en toute simplicité ». PSOC papier Tutorial, mai 2016.
REMARQUE: Disponible à http://psoc.i2cat.net/sites/default/files/PSOC-tutorial-Mobility-made-simple.pdf? _ga = 2.45065702.356832367.1537337692-718608749.1512423093.

[I.24] V. Ishakian, J. Akinwumi, F. Esposito et I. Matta: « Le soutien à la mobilité et multihoming en architectures Internet récursives », Comput. Commun., vol. 35, n. 13, p. 1561-1573, Juillet de 2012.

[I.25] ETSI GS NGP 001 (V1.3.1): "Suivant Protocoles génération (NGP), les définitions du scénario".
REMARQUE: Disponible à https://www.etsi.org/deliver/etsi_gs/NGP/001_099/001/01.03.01_60/gs_NGP001v010301p.pdf.

[I.26] IETF RFC 1287: "Vers l'architecture Future Internet", December1991, D. Clark, L. Chapin, V. Cerf, R. Braden, R. Hobby.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc1287.

[I.27] J. Day: « Comment diable voulez-vous perdre une couche !? », Conférence internationale sur le réseau de la
Future 2011.

[I.28] Conseil de l'Atlantique, Frederik S. Pardee Center for International Futures, Zurich: « Le risque Nexus.
Vaincu par les risques Cyber? Les avantages économiques et les coûts des contrats à terme cyber autre », 2016.
REMARQUE: Disponible à http://publications.atlanticcouncil.org/cyberrisks//.

[I.29] IETF RFC 2535: "extensions de sécurité du système de noms de domaine", Mars 1999, D. Eastlake.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc2535.

[I.30] IETF RFC 2401: "l'architecture de sécurité pour le protocole IP", Décembre 2005, S. Kent, K. Seo.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc2401.

[I.31] IETF RFC 6863: « Analyse de la sécurité OSPF selon le clavetage et l'authentification pour protocoles de routage (KARP) lignes directrices de conception », Mars 2013, S. Hartman, D. Zhang.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc6863.

[I.32] IETF RFC 8205: "Spécification du protocole BGPsec", Septembre 2017, M. Lepinski, K. Sriram.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc8205.

[I.33] IETF RFC 5246: "La couche de transport Protocole de sécurité, version 1.2", Août 2008, T. Diersk, R.
Escola.
REMARQUE: Disponible à https://tools.ietf.org/html/rfc5246.

[I.34] J. Petit: « Modèles dans la sécurité du réseau: Une analyse de la complexité architecturale dans la sécurisation RINA
réseaux », l'Université de Boston Département Informatique, Mémoire de maîtrise, 2012.
REMARQUE: Disponible à https://open.bu.edu/handle/2144/17155.

[I.35] IETF draft-ietf-tsvwg-natsupp: « Adresse réseau Stream Control Transmission Protocol traduction », Juillet 2017, R. Stewart, M. Tuexen, I. Rengeler.

[I.36] R. Lytchev, S. Goldberg et M. Schapira: « BGE sécurité dans le déploiement partiel: Est la valeur de jus
la pression? », ACM SIGCOMM 2013.

[I.37] M. Bari, R. Boutaba, R. Esteves, L. Granville, M. Podlesny, M. Rabbani, Q. Zhang et M. Zhani: « La virtualisation de réseau de centres de données: une enquête », Enquêtes et tutoriels IEEE Communications,
vol. 15, no. 2, 2013.

[I.38] B. Schneier: « Un plaidoyer pour la simplicité: Vous ne pouvez pas sécuriser ce que vous ne comprenez pas », l'information
Sécurité, 1999.
REMARQUE: Disponible à https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

[I.39] J. Mirkovic et P. Reiher: "Une taxonomie des attaques DDoS et les mécanismes de défense DDoS", ACM
SIGCOMM Communications Computer Review, vol. 34, no. 2, pages 39-53, 2004.

[I.40] 802.1aq IEEE™: « Standard pour les réseaux locaux et métropolitains: ponté local virtuel Area Networks - Amendement 8: Shortest Path Bridging, 802.1aq », avril 2012.
REMARQUE: Disponible à https://standards.ieee.org/standard/802_1aq-2012.html.

[I.41] E. Grasa, B. Gastón, S. van der Meer, M. Crotty et MA Puente: « Simplifying multi-couche Gestion de réseau RINA », Actes de la conférence CNC 2016.
REMARQUE: Disponible à https://tnc16.geant.org/core/presentation/667.

[I.42] Jour J.: « Comment est Distribués Distributed Management Ou peut trop de cuisiniers gâtent la sauce? »,
Pouzin Société de blog.
REMARQUE: Disponible à http://pouzinsociety.org/node/55.

[I.43] Consortium VIERGE: « système de gestion D5.4 cultés consolidée », livrable VIERGE D5.4, Juillet ici 2016.
REMARQUE: Disponible à http://ict-pristine.eu/wp-content/uploads/2018/05/pristine-d54-consolidated-network-gestion system_v1_0.pdf.

[I.44] consortium ARCFIRE, livrable D3.1: « Le logiciel intégré prêt pour les expériences: RINA pile, Système de gestion et d'un cadre de mesure », H2020 ARCFIRE, Décembre ici 2016.
REMARQUE: Disponible à http://ict-arcfire.eu/wp-content/uploads/2017/10/arcfire_d31-final.pdf.

[I.45] V. Maffione: "Port du client ssh dropbear / serveur pour rina", Décembre ici 2016.
REMARQUE: Disponible à https://github.com/vmaffione/rina-dropbear.

[I.46] M. Williams: "émulateur sockets Prototype pour rina", Septembre 2017.
REMARQUE: Disponible à https://github.com/rlite/rina-dropbear.

[I.47] S. Vrijders, E. Trouva, Jour J., E. Grasa, D. Staessens, D. Colle, M. Pickavet et L. Chitkushev: "Unreliable communication inter-processus dans Ethernet: la migration vers RINA avec le DIF shim", en
5e Atelier international sur les réseaux fiables Conception et modélisation (RNDM-2013), 2013, pp. 97-102.

[I.48] IRATI Consortium: « IRATI Deliverable D2.4, troisième cas d'utilisation de phase, spécification RINA mise à jour
et l'architecture logicielle de haut niveau », le site web IRATI, Décembre ici 2014.
REMARQUE: Disponible à http://irati.eu/wp-content/uploads/2012/07/IRATI-D2.4-bundle.zip.

[I.49] IRATI Consortium: « Irati Deliverable D3.3, deuxième prototype rina intégré de phase pour les hyperviseurs
pour OS Aunix-like », Juin ici 2014.
REMARQUE: Disponible à http://irati.eu/wp-content/uploads/2012/07/IRATI-D3.3-bundle.zip.

[I.50] V. Maffione: "la mise en œuvre de la passerelle Rina-tcp", Septembre ici 2016.

REMAR
QUE: Disponible à https://github.com/rlite/rlite#71-rina-gw.

[I.51] S. Vrijders, V. Maffione, D. Staessens, F. Salvestrini, M. Biancani, E. Grasa, D. Colle, M. Pickavet, J. Barron, Jour J. et L. Chitkushev: « La réduction de la complexité de la machine virtuelle
réseau », IEEE Communications Magazine, vol. 54, no. 4, p. 152-158, Avril ici 2016.

[I.52] P. Teymoori, M. Welzl, S. Gjessing, E. Grasa, R. Riggio, K. Rausch et D. Siracussa: "Contrôle de congestion dans l'architecture interréseau récursif (RINA)", ICC IEEE 2016, Next Génération réseau et Internet Symposium 2016.

[I.53] S. León, J. Perello, D. Careglio, E. Grasa, D. Lopez et PA Aranda: « Avantages de programmable les politiques de routage topologiques dans RINA permis datacentres à grande échelle », Globecom IEEE 2016, Next
Symposium Generation Networks, Décembre ici 2016.

[I.54] V. Maffione: "Prototype RINA a permis la mise en œuvre de VRF", mai 2018.
REMARQUE: Disponible à https://github.com/rlite/rlite#72-iporinad.

[I.55] consortium ARCFIRE, D4.3 livrable: « Conception de scénarios expérimentaux, la sélection de mesures
et KPIs », H2020 ARCFIRE, Janvier 2017.
REMARQUE: Disponible à http://ict-arcfire.eu.

[I.56] IEEE 802.11 ™: « standard IEEE pour la technologie de l'information - Télécommunications et l'échange d'informations entre les systèmes réseaux locaux et métropolitains - spécifique exigences - Partie 11: LAN sans fil d'accès au support (MAC) et la couche physique (PHY) Caractéristiques".

3 Définition des termes, symboles et abréviations

3.1 termes

Aux fins du présent document, les termes suivants sont applicables:

Procédé d'application (AP): instanciation d'un programme d'exécution dans un système de traitement destiné à accomplir un but

REMARQUE: La définition du processus d'application vise à être tout à fait abstraite et applicable à une large gamme de matériels et logiciels (processeurs, FPGA, ASICs et d'autres plates-formes). Voir la définition de « système de traitement » ci-dessous.

Protocole d'application distribuée commun (CDAP): le composant de protocole d'application d'un qui peut être utilisé facilité d'application distribuée (DAF) pour construire des applications distribuées arbitraires, dont le DIF est un exemple

REMARQUE: CDAP permet aux applications distribuées d'échanger et de faire fonctionner objets de données structurés, plutôt que de forcer les applications à traiter explicitement sérialisation et opérations d'entrée / sortie.

Control Protocol Transfert de données (DTCP): une partie facultative de EFCP qui fournit les mécanismes liés de manière lâche

REMARQUE: Chaque instance DTCP est associé à une instance DTP pour contrôler le flux, en fonction de ses politiques et le contenu du vecteur d'état partagé.

Protocole de transfert de données (DTP): une partie de transfert de données requis de EFCP constitué de mécanismes étroitement liés présents dans tous les DIF, à peu près équivalent à IP et UDP

REMARQUE: Lorsque DTP nécessaire coordonne par un vecteur d'état avec une instance du protocole de contrôle de transfert de données. Il est une instance de DTP pour chaque flux.

Facilité d'applications distribuées (DAF): collecte de deux coopérants ou plusieurs processus d'application dans un ou plusieurs systèmes de traitement, qui échangent des informations en utilisant les services fournis par un IPC DIF et maintiennent l'état partagé

REMARQUE: Dans certains Distribuée Les demandes, tous les membres seront les mêmes, à savoir un DAF homogène, ou peuvent être différents, un DAF hétérogène.

couche Facility IPC distribuée (DIF): collection de deux ou plusieurs procédés d'application coopérant pour fournir une communication interprocessus (IPC)

REMARQUE: Un DAF est un DIF qui fait IPC. Le DIF fournit des services IPC aux applications via un ensemble de primitives API qui sont utilisés pour échanger des informations avec le Applicatile pairs sur.

Erreur et protocole de contrôle de flux (de EFCP): protocole de transfert de données nécessaire pour maintenir une instance d'un service de communication au sein d'un DIF

REMARQUE: Les fonctions de ce protocole garantissent la fiabilité, l'ordre et le contrôle de flux selon les besoins. Ilest constitué par des instances distinctes de DTP et éventuellement DTCP, qui coordonnent par l'intermédiaire d'un vecteur d'état.

couler: service fourni par un EFCP instance à un processus d'application

REMARQUE: La liaison entre une EFCP instance et le processus d'application qui l'utilise est appelé un port.

Flux Allocataire (FA): le composant de gestion de couche du processus IPC qui répond aux demandes d'allocation de processus d'application

REMARQUE: est créé pour chaque Allouer Demande de flux Allocataire instance (FAI). Le FAI est responsable de:

1) trouver l'adresse de l'IPC-processus avec accès à la destination application demandée;
2) déterminer si le processus de demande demandant un accès au processus d'application demandé;
3) le choix des politiques à utiliser sur le flux;
4) le contrôle de l'écoulement; et
5) la gestion du flux pendant toute sa durée.

Communication entre processus (IPC): service fourni par un à deux ou DIF plusieurs instances de processus d'application, ce qui leur permet d'échanger des informations

Procédé IPC (IPCP): Processus de demande, qui est membre d'un DIF et met en œuvre localement la fonctionnalité pour soutenir et gérer IPC en utilisant plusieurs sous-tâches

couche: ensemble de machines de protocole de partage État sous une certaine portée

REMARQUE: Dans le cadre de RINA, une couche est une installation IPC distribuée.

(N) -DIF: nomenclature pour indiquer le rang d'un DIF, comme base pour décrire sa relation avec DIF dans les rangs ci-dessus ((N + 1) -DIF)) et au-dessous ((N-1) -DIF)

peer IPCP: IPCP dans le même DIF qui est un saut de distance, sans nécessiter une autre IPCP d'agir comme un relais

REMARQUE: En général, PCIP par les pairs devraient avoir en commun un DIF N-1.

Système de traitement: matériel et logiciel capable d'exécuter des programmes instanciés comme processus d'application qui peuvent coordonner avec l'équivalent d'un « test et de définir » l'instruction, à savoir les tâches peuvent tous faire référence atomiquement la même mémoire

Protocole unité de données (PDU): chaîne d'octets échangés entre les machines (Protocole __gVirt_NP_NN_NNPS<__ PM)

REMARQUE: Deux parties contiennent PDUs. Le (information sur le contrôle protocole) PCI, qui est compris et interprété parle DIF et l'utilisateur des données, qui est incompréhensible pour ce PM et est passé à son utilisateur.

Machine Protocole (PM): la mise en oeuvre de la logique de protocole qui échangent des informations d'état avec un PM de pairs par l'insertion des informations de commande de protocole en une PDU sur un côté (émetteur), et l'entrelacement de l'autre côté (récepteur)

Relayer / Multiplexing-tâches (RMT): RMT effectue la programmation en temps réel de l'envoi des PDU sur le lieu (N-1) -Ports des (N-1) -DIFs disponibles pour le RMT

REMARQUE: Cette tâche est un élément de la fonction de transfert de données d'un DIF. Logiquement, il se trouve entre le EFCP et SDU Protection.

Ressources Allocataire (RA): composante du DIF qui gère l'allocation des ressources et surveille les ressources du DIF en partageant des informations avec d'autres processus IPC et le DIF performance de soutien DIF

Base de données sur les ressources (RIB): représentation logique du référentiel local des objets à exposer l'état visible de l'extérieur d'un processus de demande

REMARQUE: Chaque membre du DAF maintient un RIB. Une application distribuée peut définir un RIB pour être sa représentation locale de son point de vue de l'application distribuée.

RIB Daemon: le composant de gestion de couche du processus IPC qui optimise les demandes d'information provenant des autres tâches de gestion de couche du IPCP

REMARQUE: Chaque processus de demande locale participant à une application distribuée peut avoir plusieurs sous-tâches ou threads. Chacun d'entre eux peutont des exigences d'information des autres participants à l'application distribuée sur une base périodique ou un événement conduit.

Service-Data-Unit (SDU): quantité de données transmises à travers l'interface de -DIF (N) devant être transféré dans le processus d'application de destination

REMARQUE: L'intégrité d'un SDU est maintenu par le (N) -DIF. Un SDU peut être fragmenté ou combiné avec d'autres SDU pour l'envoi comme une ou plusieurs PDUs.

3.2 symboles

Vide.

3.3 Les abréviations

Aux fins du présent document, les abréviations suivantes:

ACL	Access Control List
ADDR	Adresse
AP	Processus de demande
API	Interface de programmation d'applications
COMME	Système autonome
ASIC	Application-Specific Integrated Circuit
ASN	Notation de syntaxe abstraite
BGE	Border Gateway Protocol
BS	Station de base
BSS	Basic Service Set
CACEP	Connexion d'application commune de la phase d'établissement
CDAP	Protocole d'application distribuée commun
CEPID	Connexion EndPoint IDentifier
CMIP	Protocole de gestion commune
CPU	Central Processing Unit
CRC	Contrôle de redondance cyclique
CSP	Fournisseur de services de communication
DAF	Facilité d'applications distribuées
DC	Centre de données
DCCP	Datagram Protocol Congestion Control
DDoS	Déni de service distribué
DIF	Facilité IPC distribué
DMM	Gestion de la mobilité distribuée
DNS	Système de noms de domaines
DNSSEC	sécurité DNS
DSCP	Services de différentiel Code Point
DST	Destination
DTCP	Protocole de contrôle de transfert de données
DTP	Protocole de transfert de données
ECN	Explicit Congestion Notification
EFCP	Erreur et protocole de contrôle de flux

EPS	Système Evolved Packet
FA	flux Allocataire
FAI	Flux Allocataire instance
FPGA	Field Programmable Gate Array
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
IP	protocole Internet
IPC	Communication interprocessus
IPCP	Procédé IPC
IPsec	Internet Protocol Security
IRATI	RINA enquête comme alternative à TCP / IP
IS-IS	Système intermédiaire à système intermédiaire
LAN	Réseau local
ZÉZAYER	Locator Identifier Protocole de séparation
LTE	évolution à long terme
MAC	Medium Access Control
MH	hôte mobile
MIPv4	IPv4 mobile
MIPv6	mobile IPv6
MPLS	Multi-Protocol Label Switching
MP-TCP	Multi-Path Transmission Control Protocol
NAT	Network Address Translation
NMS	Système de gestion de réseau
NSM	namespace Responsable
NVGRE	La virtualisation réseau à l'aide Generic Routing Encapsulation
OS	Système opérateur
OSI	L'interconnexion des systèmes ouverts
OSPF	Ouvrez le chemin le plus court en premier
PBB	Provider Backbone Bridging
PCI	Protocole de contrôle de l'information
PPPC	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PE	Provider Edge
DYNAMIS ME	Amélioration de la performance Proxy
PMIPv6	Proxy mobile IPv6
Posix	Portable Operating System Interface
QoS	Qualité de service
RA	Allocateur de ressources
NERVURE	Base de données sur les ressources
RINA	Récursive InterNetwork architecture
DÉCHIRUR E	Routing Information Protocol
RLC	Radio Link Control
RMT	Relayer et multiplexer Tâche
SCTP	Stream Control Transmission Protocol
NRS	Software Defined Networking
SDO	Normes en développement Organisation
SDU	Service Data Unit
SD-WAN	Logiciel large réseau de la zone définie
SID	Les informations partagées et modèle de données
SLA	Service Level Agreement
SMI	Structure de gestion de l'information
SNMP	Protocole de gestion de réseau simple
SRC	La source
SSH	Enveloppe de protection
TAPS	Services de transport
TCP	Transmission Control Protocol
TLS	Sécurité Transport Layer
UDP	User Datagram Protocol
UE	Équipement de l'utilisateur
URL	Localisateur universel de resources
VLAN	Réseau virtuel local
VM	Machine virtuelle

VPLS	Virtual Private LAN Service de
VPN	Réseau privé virtuel
VRF	Routage et renvoi virtuel
VXLAN	eXtensible Virtual Local Area Network
BLÊME	Réseau sans fil Zone

4 Présentation et motivation

4.1 Qu'est-ce que le présent document signifie par « l'architecture de protocole réseau »?

L'architecture est le style de la conception et la méthode de construction des bâtiments et des structures physiques. Architecture fournit un ensemble de modèles et la méthodologie qui guide la construction concepteurs dans l'accomplissement de leur tâche. La même architecture permet de concevoir de nombreux bâtiments différents avec des exigences différentes: l'architecture capture les règles et les modèles qui sont invariantes par rapport aux besoins spécifiques de chaque bâtiment.

Pour illustrer l'explication du paragraphe ci-dessus avec un exemple, considérons le style de l'architecture gothique. Il dispose d'un ensemble d'éléments structurels communs qui sont communs à plusieurs bâtiments avec des exigences différentes. Parmi ces éléments communs peuvent être trouvés:

a) grandes, les dessins de grande taille qui ont balayé vers le haut avec la hauteur et grâce;

b) boutants;

c) arcs en ogive;

d) voûtes;

e) légers, aérés intérieurs; ou

f) l'accent mis sur le style décoratif et orné.

Avec ces éléments architectes ont conçu une myriade de bâtiments comme des cathédrales, des mairies, des palais, des marchés de poissons ou portes de la ville. Architectes adaptés les éléments de l'architecture au programme requis par les bâtiments qu'ils conçoivent.

Cependant, les concepteurs de protocole de réseau de tâches sont concernés par ne sont pas liés à la construction de structures physiques, mais de concevoir des protocoles qui prennent en charge les réseaux de dispositifs informatiques. Le terme « calcul » est ici utilisé au sens large du terme: des dispositifs qui produisent une sorte de calcul ou équivalent. Par conséquent cette catégorie comprend des capteurs, smartphones, tablettes, ordinateurs portables, les ordinateurs personnels, les serveurs haut de gamme, routeurs, commutateurs, etc.

Mise en réseau informatique est un catalyseur pour le calcul distribué. Il fournit des services de communication aux instances de processus d'application distribués (encore une fois, les processus d'application distribués utilisés de manière lâche, peuvent être des processus d'application OS, ou capteurs, actionneurs, etc.). Le service que le réseau informatique fournit aux applications est celui des services de réplication de données à distance imparfaits. Les réseaux peuvent être caractérisés comme des données distribuées photocopieuses de capacité finie, qui entraînerait des retards et des pertes dans l'exercice de leur tâche. En d'autres termes, la mise en réseau informatique peut être considérée comme IPC réparties (Inter Process Communication), une vue qui a été prise par les pionniers dans le domaine[I.1], [i.2], [i.3]; et est également compatible avec le modèle de protocole générique décrit dans ETSI GS 007 NGP [I.4].

Par conséquent, l'architecture de protocole de réseau fournit un ensemble de modèles et la méthodologie qui guide réseau (protocole) les concepteurs dans l'accomplissement de leur tâche. Il capture les règles et les modèles qui sont invariantes par rapport aux besoins spécifiques de chaque réseau (cellulaire, centre de données, le capteur, l'accès, le noyau, l'entreprise, LAN, etc.). Par conséquent, aux fins du présent document, l'architecture de protocole de réseau est défini comme les règles et les tendances générales de fournir des services distribués IPC à tout type d'application sur tout type de support physique.

4.2 Quelle est l'architecture actuelle du protocole de réseau?

Une partie des problèmes actuels réseaux informatiques sont en raison du manque de précision et de cohérence dans la définition des éléments des réseaux informatiques et de leur interaction. Il est difficile de raisonner logiquement sur les concepts vaguement définis, car il laisse trop de place à l'ambiguïté et des interprétations erronées. l'architecture de protocole de réseau est un bon exemple de ce problème, car il n'y a aucune spécification formelle de ce qui est l'architecture de protocole de réseau utilisé aujourd'hui (ou même s'il n'y a qu'un seul ou plusieurs).

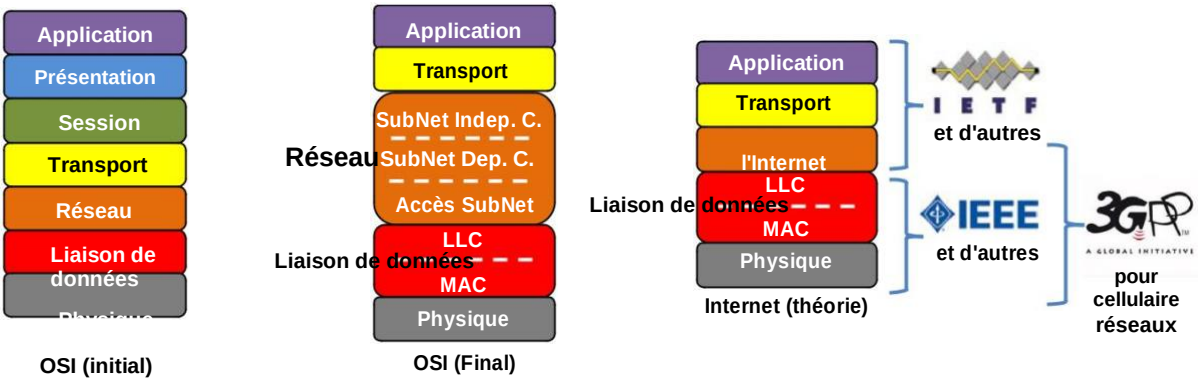


Figure 1: Modèles d'architecture OSI initiale et finale (gauche, centre) et le modèle de la suite de protocole Internet (à droite)

Il y a un consensus approximatif que l'architecture de protocole de réseau est vaguement basé sur OSI [I.5], l'effort d'interconnexion des systèmes ouverts. La partie gauche deFigure 1 montre les sept couches de la version la plus connue de l'architecture OSI. Bien que populaire, ce n'est pas la version finale de l'architecture OSI, qui figure dans la partie centrale deFigure 1. On a constaté que les trois couches supérieures étaient en réalité un seul (la couche d'application), et la couche de réseau a été divisé en trois sous-couches indépendantes:

a) couche d'accès au sous-réseau avec des adresses dépendant du réseau, qui effectue le relais et les fonctions de multiplexage dans un réseau;

b) couche de convergence dépendant du sous-réseau, qui fournit un contrôle d'erreur et le débit sur un réseau unique; et

c) sous-réseau indépendant couche de convergence, avec des adresses de réseau indépendant, qui effectue des fonctions de relayage et de multiplexage sur les réseaux.

Enfin, la partie droite de Figure 1 illustre les couches de ce qui pourrait être décrit comme l'architecture réseau / Internet actuel. Les couches inférieures (physique et liaison de données), sont les mêmes que dans l'architecture OSI. En plus de la couche de liaison de données il y a la couche « réseau » ou « Internet » (selon les sources, il est appelé d'une manière ou l'autre) avec des adresses, et sur le dessus de celui-ci une couche de transport de bout en bout fournissant fin pour mettre fin à l'erreur et le débit des services de contrôle de la couche d'application (avec des protocoles qui exécutent des tâches spécifiques à l'application). La plupart des protocoles dans la liaison de données et les couches physiques sont normalisées par l'IEEE (notamment Ethernet avec toutes ses variantes), alors que les protocoles de l'Internet, des couches de transport et d'application sont normalisés par l'IETF. D'autres organismes de normalisation se concentrent sur des types spécifiques de réseaux,

4.3 Résumé des questions d'actualité au niveau de l'architecture de protocole réseau

4.3.1 Structure

Couches comme unités de modularité. les architectures de réseau dans l'utilisation aujourd'hui sont principalement basées sur le paradigme de stratification fonctionnelle, dans laquelle différentes couches remplissent des fonctions différentes. Le modèle théorique décrit typique 4 couches (physique, liaison de données, réseau et transport) avec les protocoles d'application sur le dessus. Les couches sont considérés comme une unité de modularité. Les fonctions de chaque couche sont réalisées par différents protocoles, qui sont conçus indépendamment les uns des autres. Ce modèle de conception provoque beaucoup de frais généraux et la répétition (couche 2 protocoles ont de nombreuses fonctions en commun avec protocoles de couche 4, par exemple).

Les fonctions dans les différentes couches ne sont pas indépendantes. La répartition actuelle des fonctions dans différentes couches est avérée être problématique: la fragmentation IP ne fonctionne pas parce que pour faire fonctionner correctement des besoins d'information que TCP a, mais IP doit fonctionner indépendamment de celui-ci (car il est dans une autre couche).

Un nombre fixe de couches limite le nombre de champs d'application. Les couches permettent l'isolement de l'état des différents champs d'application: il est leur propriété fondamentale. L'architecture théorique a juste la place pour deux champs: liaison de données et réseau; à savoir l'ensemble d'Internet. En Internetworks réels, cela est nettement insuffisant - les fournisseurs de réseau veulent isoler leur allocation des ressources internes, les politiques de routage et expédition du reste de l'Internet, par exemple. Cela a provoqué la prolifération de nouveaux protocoles qui appartiennent à des couches 2,5 - telles que MPLS -, des couches virtuelles au-dessus du transport - comme VXLAN - tunnels - tels que GRE - ou encapsulations récursives - comme MAC-in-MAC. Ces protocoles ont évolué sans organisation pour résoudre des cas d'utilisation individuels comme ils sont apparus, invalidant le modèle architectural d'origine et l'augmentation de la complexité des réseaux, comme on le voit dansFigure 2.

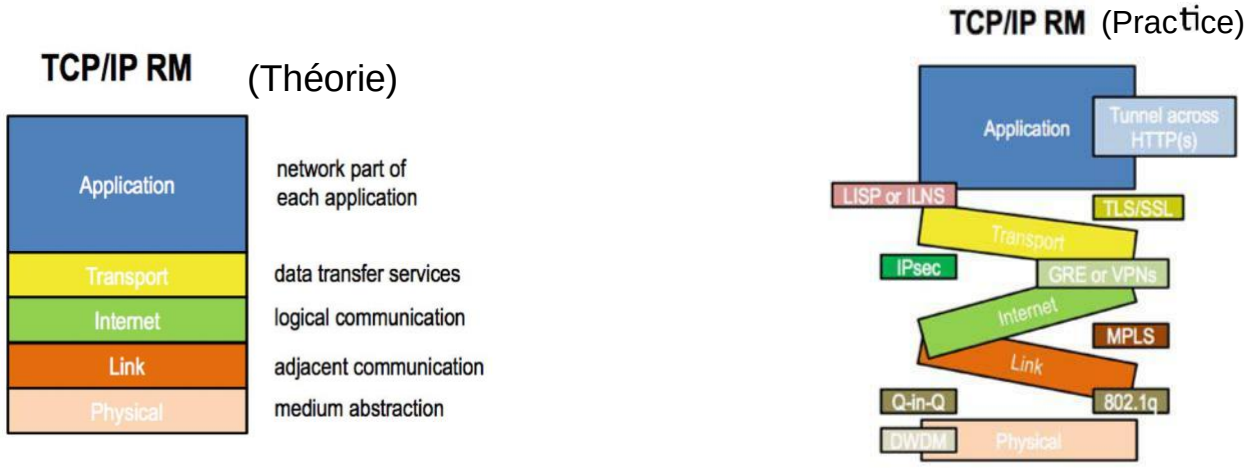


Figure 2: modèle d'architecture Internet est constamment étendu pour supporter de nouveaux cas d'utilisation

API de couche incomplète et / ou manquants. La plupart des couches ne sont pas une API standard qui fait abstraction du service que la couche fournit donc tous les utilisateurs d'une couche besoin de connaître les détails sur les protocoles spécifiques mettant en œuvre la fonctionnalité de couche. La couche seulement qui a une API standard (de facto) est la couche de transport avec l'API de sockets. Cependant Sockets ne cachent pas les détails de mise en œuvre de la couche de transport et des protocoles de transport exposer individuels aux applications. Par conséquent, les applications doivent être conscients du choix des protocoles de transport disponibles, et prendre une décision savvy en fonction de ses besoins. Ce fait rend non seulement les applications en réseau plus complexe, mais rend également le déploiement de nouveaux protocoles de transport très difficile[I.6].

4.3.2 la conception du protocole

Plusieurs protocoles par couche. Même avec l'approche de stratification fonctionnelle - dans lequel chaque couche remplit une fonction différente - aujourd'hui il y a plusieurs protocoles qui peuvent être utilisés dans chaque couche. Cela est dû au fait que les protocoles actuels sont fabriqués à la main pour résoudre un cas d'utilisation particulier ou pour couvrir une petite gamme d'exigences. Lorsque ces conditions ne peuvent être remplies d'un nouveau protocole est conçu à partir de zéro. La couche de transport est un bon exemple de cette approche, dans laquelle différents protocoles comme TCP, UDP, SCTP ou DCCP diffèrent surtout dans la façon dont ils ne coulent et le contrôle de la retransmission. Une stratégie de conception de protocole qui a identifié les principaux traits communs à travers des protocoles et a essayé de faire un design générique adaptable à des environnements différents réduirait considérablement le nombre de protocoles requis dans un réseau.

Protocoles conçus indépendamment les uns des autres.Étroitement lié au dernier point, la plupart des protocoles aujourd'hui sont conçus de manière isolée les unes des autres, ce qui maximise le travail de spécification et la mise en œuvre en raison de fonctions répétées qui sont réinventées par chaque protocole. Par exemple, tous les protocoles de routage utilisés aujourd'hui (OSPF, IS-IS, BGP, RIP, etc.) sont de maintenir une base de données partiellement réparties sur les noeuds du réseau, puis en appliquant des algorithmes différents pour calculer localement des tables expédition. Quels sont les changements de protocole à protocole est la stratégie utilisée pour la réplication, les informations échangées et les algorithmes locaux; mais les mécanismes utilisés pour coder les informations - syntaxes abstraites et concrètes - et de communiquer des mises à jour peuvent être communs à tous. Refonte groupes de protocoles avec des objectifs communs afin de maximiser les points communs entre simplifieraient la conception, le déploiement,

4.3.3 Nommage, d'adressage et de routage

Le manque de noms d'applications. Une architecture de réseau bien formé a besoin des noms d'application qui sont indépendants de la localisation, de sorte que les applications connectés au réseau peuvent maintenir leur identité, peu importe où ils sont. Dans l'URL Internet peuvent sembler jouer ce rôle, mais une inspection minutieuse révèle que ce n'est pas juste. L'URL est une concaténation d'un nom de domaine, un port de couche de transport et une chaîne qui est significative à l'application. Les noms de domaine sont des synonymes d'adresses IP (ils sont résolus à des adresses IP par DNS, qui est un service d'annuaire externe au réseau). Lorsqu'une application demande un service de transport à l'API sockets passe l'adresse où l'application de destination est fixée: le réseau ne connaît pas les noms. Si l'application change de point de rattachement au réseau, ses changements d'adresse IP et toutes les connexions de transport à cette application sont brisées. En outre, les règles de contrôle d'accès (par exemple, les règles de pare-feu) sont rédigées en termes d'adresses IP et les ports de transport; ce qui signifie qu'ils doivent être mis à jour chaque fois qu'une application modifie son attachement au réseau.

Nommer l'interface à la place du nœud. Au sein d'une couche d'un noeud est la machine de protocole qui retire l'en-tête de ce protocole dans cette couche. Par conséquent protocole dans PDUs une couche sont adressées aux nœuds. Cependant, dans les adresses de la suite de protocole TCP / IP sont attribués aux interfaces (points de fixation à la couche ci-dessous), et non pas des noeuds. Ce fait rend impossible de réel support multi-homing (parce que le réseau ne sait pas que deux adresses d'interface atteignent le même noeud), fabrique des tables d'acheminement de routeur 3/4 fois plus grande et complique grandement la mobilité.

Aucun nom pour les couches, aucun répertoire de couche. Bien que certaines couches ont des noms (BSS-id dans le cas des réseaux WLAN ou VLAN-ids dans le cas de VLANs), les couches supérieures proches des applications ne les ont pas. Ce fait, ainsi que l'absence de noms d'application, provoquer des applications soient disponibles par le biais d'une seule couche à la fois (habituellement le plus haut une) ou à plusieurs couches si l'application est fixé à des interfaces de plusieurs couches supérieures (par exemple, une interface appartenant à l'Internet, une autre interface appartenant à un réseau IP privé). L'absence de répertoires de couche permet de découvrir quelle est la meilleure couche pour atteindre une application impossible: cette information doit être configuré de manière statique dans les applications clientes.

4.3.4 Mobilité et multi-homing

Nécessité de protocoles spécialisés pour soutenir multi-homing. Plusieurs approches ont été proposées pour atteindre multi-homing dans les réseaux actuels. Musique classique (ou vrai) multi-homing nécessite adresses fournisseur indépendant - qui ne peuvent pas être regroupés dans la table globale de routage Internet - un protocole de routage dynamique (généralement BGE) et au moins deux liens: chacun à un autre fournisseur. Lorsque l'un des liens vers un fournisseur échoue BGP recalculera le chemin AS afin que l'autre fournisseur est sélectionné. Cependant, cela ne permet multi-homing au niveau AS. multi-homing hôte prend en charge partielle par l'intermédiaire de protocoles qui exploitent l'utilisation de plusieurs interfaces IP (tels que SCTP, MP-TCP ou SHIM6). Cependant, dans cette approche des paquets qui sont déjà en route vers une adresse IP appartenant à une interface qui est en panne sera perdue (par conséquent, que le support multi-homing partielle est atteint).

Nécessité de protocoles et d'objets spécialisés pour réaliser la mobilité. Ce soutien à la mobilité - qui peut être tout considéré comme multi-homing dynamique - est lourd devrait arriver à une surprise. L'absence de noms d'applications et adresses de nœuds nécessitent l'utilisation de protocoles spéciaux et des objets pour soutenir un certain degré de mobilité d'accueil. La plupart des solutions de mobilité actuelles nécessitent la mise en place des tunnels à travers des protocoles spécialisés. La gestion de ces tunnels résultats dans les frais généraux importants, car ils doivent être mis à jour chaque fois que l'hôte mobile change son point d'attache au réseau. Différents types de réseaux mobiles avec différents soutien à la mobilité hôte nécessitent différents protocoles (par exemple WiFi vs cellulaire). Les solutions de mobilité tunnel moins vrai sur la base multi-homing tel que celui réalisé par BGE ont été étudiés mais prouvé trop lent,

4.3.5 Qualité de service, l'allocation des ressources, le contrôle de la congestion

L'absence d'un modèle de qualité de service cohérente à travers les couches. L'absence d'un modèle clair, cohérent pour communiquer les exigences de performance à travers les couches rendent difficile de gérer les performances d'un réseau multi-couches afin qu'il offre une expérience de service cohérente à ses clients. Comme il n'y a pas de mécanismes abstraits pour la communication des exigences de performance entre les couches, cette communication doit être conçue sur un cas d'utilisation par base de cas d'utilisation, impliquant généralement le système de gestion de réseau. La couche doit également identifier les flux appartenant à différents groupes de qualité de service, qui dépend également de la technologie utilisée: le code DSCP marquage peut être utilisé dans le cas de la propriété intellectuelle, l'ingénierie du trafic MPLS basé sur les valeurs des étiquettes MPLS, les étiquettes VLAN pour Ethernet ou I-SID (les identificateurs de service) dans le cas de PBB.

Seuls de bout en bout (trop long) boucles de contrôle de congestion. Faire face à la congestion dans la couche de transport maximise seulement la longueur de la boucle de commande de congestion, ce qui maximise également le temps de réagir à l'encombrement et sa variance (oscillations). Par conséquent, les expéditeurs TCP peuvent être réagir à la congestion qui ne sont plus là; ou au moment où l'expéditeur TCP réagit le réseau est déjà dans un état très encombré. Ceci est un problème particulier sur les réseaux cellulaires, où la puissance du signal très variable connu par un hôte mobile peut provoquer l'allocation du réseau de ressources radio pour cet hôte pouvant varier de trois ordres de grandeur dans un temps beaucoup moins que la fin To- fin aller-retour. Si la congestion a été géré au niveau de chaque réseau individuel, des boucles de contrôle plus courts et plus efficaces seraient possibles.

Prédatrices (implicite) de contrôle de congestion. L'utilisation de paquets perdus ou en double comme un signal de la congestion, TCP interpréter la perte de paquets en raison de lier les défaillances de la congestion (ce qui est habituel dans les scénarios TCP-sur-sans fil). En conséquence TCP overreacts à la congestion inexistante, ce qui dégrade le débit et le retard subi par les applications. Explicit Notifications Congestion (ECN) de signalisation par les routeurs dans le chemin parcouru par les PDUs appartenant à la connexion TCP fournit un meilleur signal de rétroaction pour réagir à la congestion, mais cela nécessite encore un aller-retour de bout en bout pour déclencher une réaction, plutôt que traitée au point de congestion.

Homogène politiques de contrôle de la congestion pour les réseaux hétérogènes.des connexions de protocole de transport passent généralement par un certain nombre de différents réseaux et / ou des segments de réseau ayant des caractéristiques différentes (accès câblé / sans fil, l'agrégation, de base, d'interconnexion, centre de données, etc.). Essayer de trouver un seul contrôleur de congestion qui peut se comporter de manière optimale pour la fin de boucle composée de commande de boucle d'extrémité est tout simplement impossible: ce qui est optimal pour un certain segment n'est pas efficace pour l'autre. Là encore, si la congestion est gérée au niveau du segment de réseau ou d'un réseau - par le biais de multiples boucles de commande plus courtes - chaque boucle de commande peut être optimisé pour le segment de réseau qu'il contrôle.

4.3.6 Sécurité

La plupart des protocoles ont leur propre modèle de sécurité. Le modèle de sécurité suite de protocoles TCP / IP est généralement basée sur la construction des fonctions de sécurité pour chaque protocole. Par exemple, DNSSEC fournit l'intégrité des données et l'authentification résolveurs de sécurité au courant. IPsec est un cadre général pour les communications IP sécurisées, soutenant la confidentialité, l'intégrité, l'authentification ou la protection contre les attaques de relecture. Cependant, depuis IPsec fonctionne de bout en bout dans une couche, non plus ne protège que la charge utile IP (mode de transport) ou fait orienté connexion IP (mode tunnel), l'encapsulation d'un paquet IP protégé dans un paquet IP non protégé. Cela rend IPsec une solution partielle, sans répondre aux exigences des protocoles de plan de contrôle IP, qui doivent définir leurs propres fonctions de sécurité, telles que OSPF ou BGP. TLS, le protocole Transport Layer Security, spécifie un ensemble de fonctions de sécurité connexes pour permettre des communications sécurisées sur la couche de transport. Dans l'ensemble, cette approche se traduit par un surcoût élevé et la complexité sans bornes, étant donné que de nouveaux protocoles dans de nombreux cas exigent ses protocoles de sécurité compagnon.

Couplé fonctions d'allocation et de synchronisation du port; utilisation des ports bien connus.la couche transport protocoles surcharge le port-id être à la fois une poignée local (socket) et l'ID de connexion de point de terminaison (CEPID). En outre, l'absence de noms d'application surchargent port-ids avec la sémantique de l'application: paramètres d'application sont identifiés par une combinaison d'adresse IP et un bien connu port-id qui est attribué lorsque l'application se lie à une couche IP. les valeurs de port de destination identifiant statique doivent être connues par l'application source lors de la demande d'une connexion de transport. Par conséquent, un attaquant voulant intercepter une connexion de transport particulier n'a besoin que de deviner / usurper le port source-id.

Aucun nom d'application: Les adresses réseau sont exposées à des applications. Depuis la suite de protocoles TCP / IP ne pas les noms d'applications (DNS est un annuaire externe), les couches IP exposer les adresses aux applications. La divulgation de l'information facilite l'usurpation d'identité des adresses IP, et en combinaison avec l'utilisation d'outils de contrôle communs tels que traceroute ou ping permet aux pirates sur les hôtes finaux pour se renseigner sur les adresses des cibles potentielles dans une couche ainsi que le graphique de la connectivité réseau. Les pirates peuvent utiliser ces informations pour DDoS attaques de configuration en automatisant la découverte et l'infection des machines vulnérables, ou d'attaquer l'infrastructure réseau en prenant le contrôle sur les routeurs.

4.3.7 La gestion du réseau

Trop peu de points communs dans les protocoles de réseau. Les différentes couches remplissent des fonctions différentes qui nécessitent des protocoles différents. Même au sein de la même couche plusieurs protocoles sont nécessaires pour adapter la couche aux différentes exigences opérationnelles. Chaque protocole est livré avec sa propre définition de la machine de protocole, sa propre configuration et son propre modèle d'état. La gestion des réseaux conçus de cette façon est difficile et lourd, étant donné que les nouveaux États membres doit comprendre les modèles état, le fonctionnement et la configuration de tous les différents protocoles du réseau, ainsi que leurs interactions.

Aucun modèle bien défini pour l'interaction entre les couches. Pour gérer un réseau multi-couches, les besoins non seulement les nouveaux États membres à comprendre les protocoles individuels, mais aussi l'interaction entre les multiples couches de protocole. Comme il n'y a pas bien défini, API couche cohérente, chaque interaction de la couche doit être traitée au cas par cas, ce qui complique la configuration du réseau, la performance et la gestion de la sécurité.

Différents protocoles et modèles d'objets pour la gestion du réseau. Bien que NETCONF et YANG gagnent la traction comme protocole et le modèle objet pour la gestion de la configuration du réseau, ils sont encore loin de couvrir tous les segments du réseau et des technologies. CMIP et X.700, SNMP et SMI et SID (les informations partagées et modèle de données) sont encore répandues dans les différents domaines de mise en réseau. En tant que réseaux d'opérateurs conséquence convergé aujourd'hui sont susceptibles de nécessiter plusieurs protocoles et de l'objet des modèles de gestion, ce qui complique cette tâche encore plus.

Aucun ensemble d'API pour borné programmabilité réseau. SDN veut améliorer la programmabilité de dispositifs de réseau à travers la séparation des plans d'acheminement et de contrôle des données. Current SDN approche de mise au point sur la définition API et les protocoles pour les données d'expédition par l'intermédiaire de contrôleurs centralisés. Toutefois, étant donné NRS ne change pas l'organisation de protocoles réseau et des couches, et le nombre de protocoles réseau est sans bornes, l'ensemble des API nécessaires pour soutenir programmabilité réseau est sans bornes. Par conséquent programmabilité est atteint au prix d'une complexité accrue, ce qui rend difficile de convenir d'un ensemble d'API standard pour faciliter programmabilité des fonctions de réseau à travers un large éventail de fabricants d'appareils.

4.4 Objectifs pour une architecture de protocole de réseau générique

Une meilleure architecture réseau que l'on a besoin aujourd'hui en place pour fournir autant que invariants possible, de sorte que le nombre de protocoles nécessaires pour couvrir tous les cas d'utilisation en réseau peut être réduite au minimum et leurs points communs maximisée.

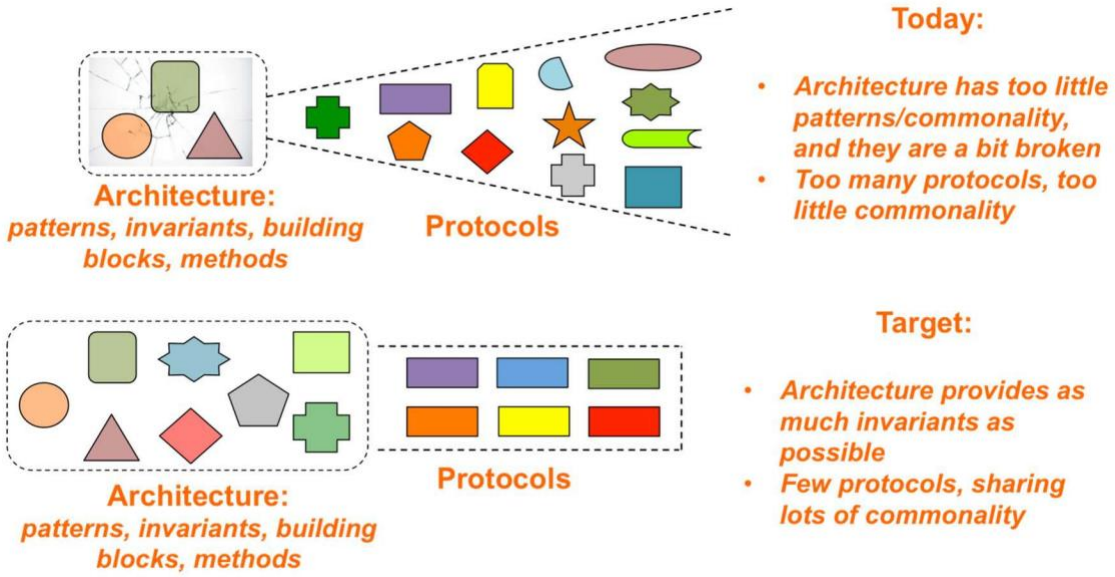


Figure 3: représentation abstraite de l'architecture actuelle du réseau et des protocoles par rapport à l'objectif recherché

Plus précisément, une architecture de protocole réseau amélioré par rapport à celui qui prévaut aujourd'hui devrait:

- Fournir un cadre pour faciliter la réutilisation des mécanismes à travers les couches, afin de pouvoir répéter les fonctions sans avoir à les repréciser.
- Évitez les violations de la couche: couches doivent être considérées comme des boîtes noires avec une API bien définie.
- Prévoir un nombre variable de champs d'application, qui peut être décidé en temps réel par les concepteurs du réseau. Évitez la nécessité d'introduire de nouveaux protocoles lorsque de nouveaux champs d'application sont nécessaires.
- Maximiser les points communs entre les différents niveaux, afin de simplifier sa structure autant que possible.
- Fournir une structure claire et la répartition des fonctions au sein de chaque couche, ce qui réduit le nombre de protocoles nécessaires pour le faire fonctionner.
- Fournir une dénomination complète et architecture d'adressage, avec prise en charge des noms d'application.

- mobilité et soutien multi-homing en raison des propriétés de la structure du réseau, sans exiger des protocoles spécialisés.
- Fournir un modèle uniforme de qualité de service à travers les couches, qui peuvent être appliquées à partir de l'application sur le fil physique.

- Fournir un soutien adéquat pour le contrôle de la congestion, y compris la détection de congestion explicite, ce qui réduit la longueur des boucles de contrôle et permettant leur personnalisation.
- Assurer la sécurité et la confidentialité par la conception, plutôt que comme extension (s).
- Fournir un modèle de sécurité cohérent au sein et à travers les couches, qui est indépendante des protocoles individuels.
- Minimiser la quantité d'état interne qui doit être exposée à l'extérieur d'une couche (telles que les adresses).
- Réduire au minimum le nombre de protocoles nécessaires à la gestion du réseau (idéalement un).
- Soutenir un ensemble limité et bien défini de points de programmabilité.

5 Structure

5.1 Une définition de service réseau

Comme présenté dans le paragraphe 4.1, le rôle des réseaux informatiques est de soutenir le calcul distribué; qui est: pour permettre aux instances d'applications distribuées à communiquer entre eux. D'où le réseau alloue des ressources pour soutenir les instances de communications entre les applications à distance. Le service fourni par le réseau peut être caractérisée comme Process Communication Inter distribué ou distribué IPC.

Selon les définitions de l'ETSI GS 007 NGP [I.4], le terme « flux » est utilisé pour décrire une instance individuelle d'un service de communication. D'où la demande d'applications circule vers le réseau afin d'échanger des informations avec d'autres applications. Lorsque les applications demandent un service de communication (flux), ils fournissent des informations sur ce que d'autres applications (s) ils aimeraient communiquer avec, et ce que (le cas échéant) devraient être les caractéristiques du service.

Par conséquent, il est nécessaire pour les noms qui identifient des instances d'applications (une instance spécifique, toute instance, un groupe d'instances, etc.), et la nécessité d'un mécanisme qui permet à l'application d'exprimer des contraintes sur les caractéristiques de l'écoulement. De telles contraintes peuvent être liées à la performance du service (Goodput, latence), sa fiabilité (taux de perte de paquets, a ordonné la livraison de données, etc.), la sécurité ou peut-être d'autres. Cependant, ces contraintes sont toujours liées à la définition du service, ils ne devraient jamais essayer de dicter les protocoles, les mécanismes ou les politiques que le réseau a en interne à utiliser pour répondre à la demande de débit: applications demandent ce que les caractéristiques du service qu'ils veulent, le réseau décide comment fournir le service.

Une fois que les ressources du flux sont alloués, les applications peuvent commencer à envoyer et recevoir des données à ses pairs par le biais du flux. Lorsque l'application se fait avec la communication, il peut informer le réseau que les ressources liées au flux peuvent être libérés.

Par conséquent, un service de réseau générique selon le mode RINA peut être défini comme suit, y compris un très haut niveau définition abstraite de l'API.

Les réseaux offrent distribués Inter Process Communication Services (IPC) aux instances d'applications distribuées. Les réseaux permettent plusieurs instances d'applications distribuées pour communiquer avec certaines caractéristiques. Chaque instance d'un service de communication est appelé « flux ». Les applications peuvent interagir avec le réseau via les primitives suivantes:

- **flow_handle allocate_flow**(Source_app_name, app_name de destination, liste des service_characteristics)
- **write_data_to_flow**(Flow_handle, données)
- **read_data_from_flow**(Flow_handle, données)
- **deallocate_flow**(Flow_handle)

5.2 Les réseaux et l'informatique distribuée

Avant d'essayer d'identifier les modèles génériques dans la structure des réseaux, il est important d'obtenir une meilleure compréhension de leur nature. Clause 5.1 soutient que les réseaux fournissent des services à des applications distribuées, afin de faciliter l'informatique distribuée. Mais quels sont les réseaux internes? La nature des réseaux très différent de celui des applications distribuées, ils prennent en charge?

Traditionnellement, les réseaux ont été vus comme quelque chose de spécial et distinct par ceux qui recherche, la conception et les bâtiments (sauf aux débuts de la recherche réseau, lorsque la vision était que le réseau était tout au sujet de l'informatique distribuée). Mais c'est le point de vue de l'observateur (l'homme à la recherche sur les réseaux), et non pas celui de l'organisme (réseaux). Regardons de plus près dans ce que les réseaux font:

- Ils fournissent des services distribués IPC à d'autres applications distribuées.
- Les fonctions réseau exécutent sous une forme d'entité Compute (processeurs génériques, FPGA, ASICs, etc.) dans une variété de plates-formes (PC, ordinateurs portables, routeurs, capteurs, smartphones, tablettes, commutateurs, etc.).
- Les instances de fonctions de réseau peuvent être mises en œuvre dans le logiciel, le matériel ou une combinaison.
- Fonctions réseau / machines de protocole ont des cas distribués par de nombreux systèmes, le partage de l'État et l'échange d'informations pour mener à bien une tâche de collaboration.

Tout comme le Web, les systèmes de distribution peer-to-peer, le courrier électronique, etc. D'où les réseaux sont juste une classe particulière d'applications distribuées, qui sont spécialisés pour effectuer leur tâche: fournir des services IPC aux instances d'autres applications distribuées (comme d'autres applications distribuées sont spécialisés pour mener à bien leurs propres tâches). Cette observation ne peut pas être NOVATRICE, mais il a deux conséquences qui sont importantes pour identifier les invariants, des modèles communs et de simplifier la façon dont les réseaux sont modélisés, conçus et construits:

- Si les réseaux sont distribués applications, il peut y avoir des motifs structuraux communs partagés par tous les types d'applications distribuées (qui sont également communs aux réseaux).
- Si les réseaux sont des applications distribuées, par définition de « réseaux » peuvent également être les utilisateurs de services distribués IPC (qui fait allusion à la structure récursive présentée à l'article 5.3).

5.3 Un motif structural répétitif: récursifs CIB Installations distribuées (DIF)

Le réseau est une application distribuée qui fournit des services IPC aux instances d'autres applications distribuées, appelées Distribuée Facility IPC (DIF). Mais une seule instance de ce courant dans tous les DIF les machines dans le monde et de soutenir toutes les applications dans le monde est pas très évolutive. Il est nécessaire d'isoler les étendues (lien, réseau, Internet, VPN, etc.) à la fois pour la sécurité, des raisons de performance et d'évolutivité.

La solution est d'avoir plusieurs instances du DIF, traitant de différents champs d'application et de fournir des services à l'autre (après tout, un est juste une DIF application distribuée). L'architecture de protocole réseau RINA dispose d'un seul type de couche (DIF) qui se répète autant de fois que nécessaire par le concepteur du réseau. Une couche est un allocateur de ressource qui fournit et gère le service IPC sur une certaine portée (lien, réseau, Internet, VPN, etc.). Une couche alloue des ressources (mémoire dans des mémoires tampons, la capacité de planification) à des flux en compétition, ce qui peut avoir différentes exigences de qualité en termes de taux de perte de données admissible, la latence, la gigue ou le débit.

Un exemple d'une telle structure répétitive est prévue dansFigure 4. La figure représente cinq systèmes: deux hôtes, deux routeurs de bordure et un routeur intérieur, reliés entre eux par quatre liaisons physiques point à point. IPC sur chaque lien physique est géré par une instance d'un DIF. Une autre DIF (en bleu) fournit des services IPC entre les applications dans les deux routeurs de bordure, cachant le routeur intérieur des hôtes. Enfin, un DIF « bout en bout » (en orange) fournit des services IPC entre les applications en cours d'exécution dans les hôtes.

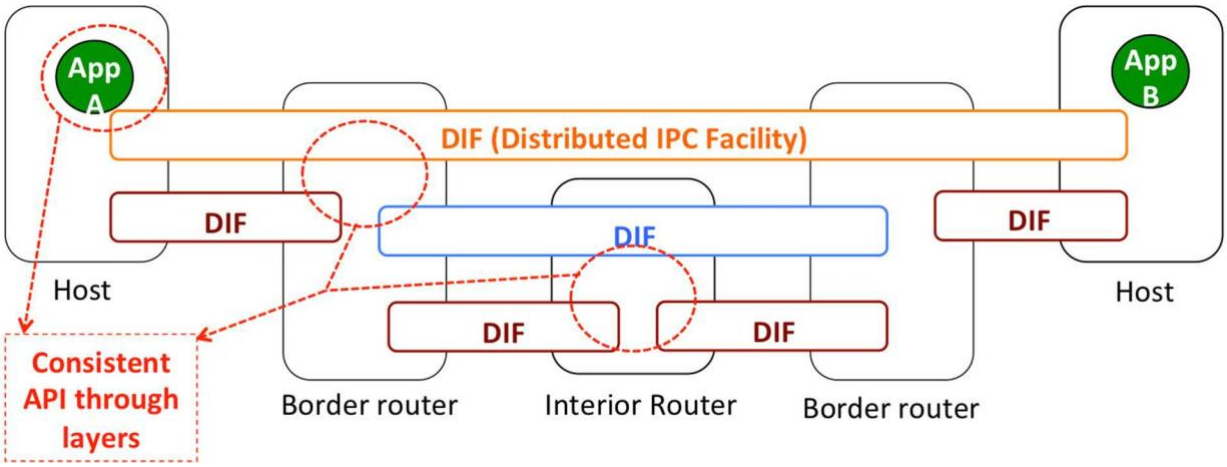


Figure 4: une couche de répétition (DIF) pour différents champs d'application est le motif structurel de base de RINA

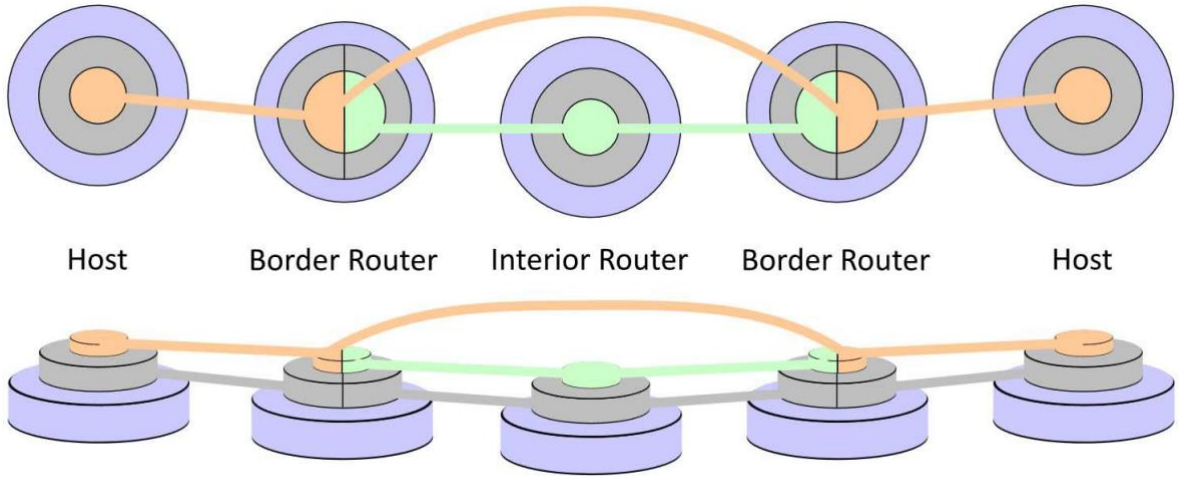


Figure 5: Illustrant pour montrer différents DIF portées

Le champ d'application de chaque couche (DIF) est configuré pour gérer une gamme donnée de largeur de bande, la qualité de service et de l'échelle; divisant ainsi le problème de l'allocation des ressources réseau mondial en parties traitables. Gérer les ressources sur DIF une plage donnée, par conséquent, les politiques de chaque couche seront sélectionnés pour optimiser cette gamme. Le nombre de requis dans un DIF réseau ou inter-réseau dépend de la plage de la bande passante, la qualité de service et de l'échelle. De plus, ce nombre peut changer dynamiquement et être différents dans différentes parties d'un réseau (l'accès, l'agrégation, noyau, etc). Ceci est une question de conception du réseau, pas une question d'architecture de protocole réseau.

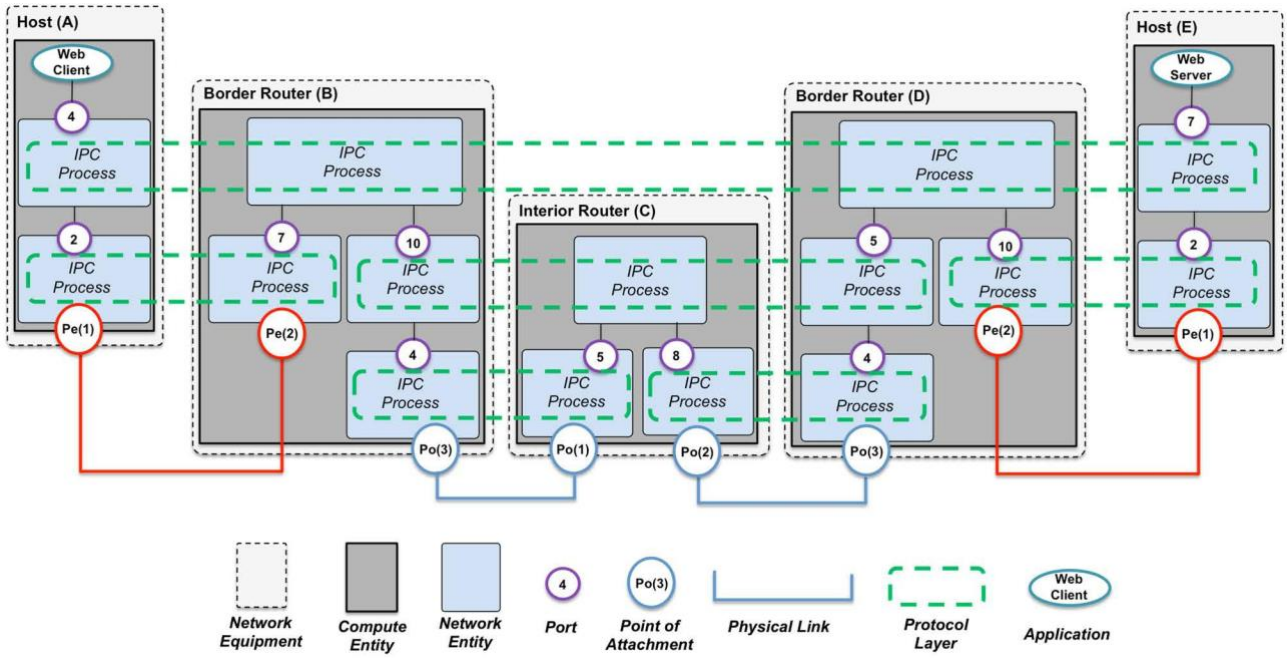


Figure 6: DIF décrites à l'aide du modèle de protocole ETSI GS 007 NGP [I.4]

La figure 6 illustre le scénario d'exemple présenté dans Figure 4, mais décrit à l'aide du modèle de protocole générique NGP introduit dans ETSI GS NGP 007 [I.4]. Chaque composé est par DIF un certain nombre de « processus CIB » (PCIP), qui collaborent ensemble pour fournir et gérer un service IPC sur une certaine portée. Chaque IPCP peut être considéré comme une instance d'une application distribuée, à l'intersection d'une couche de protocole et un équipement réseau.

Le IPCP fournit de multiples flux d'applications sur le dessus de celui-ci, chaque flux étant une instanciation d'un service IPC identifié par un orifice (cercles pourpres dans Figure 6). Les applications utilisant ces flux peuvent également être d'autres PCIP de couche supérieure, en formant ainsi une structure récursive. PCIP consomment les flux fournis par d'autres PCIP ci-dessous ou les points de fixation sur des liens physiques de différentes technologies (électrique, optique, radio, etc.).

Le travail d'un IPCP est de:

a) données multiplexées de flux « client » (les applications desservies par le IPCP) dans les flux fournis par DIF inférieur; et

b) transmettre des données à partir de différents ports DIF inférieurs.

PCIP utilisent un protocole de transfert de données commun pour effectuer cette tâche, qui sera introduit à l'article 6. Ce protocole de transfert de données commun peut être optimisé pour les exigences de chaque DIF par les politiques, en maximisant les points communs entre DIF mais permettant une certaine flexibilité où il fait vraiment différence.

Pour mener à bien ses tâches de transfert de données, le PCIP nécessite un certain nombre de fonctions de gestion de couche pour gérer l'allocation des flux, des ressources, la découverte d'applications, l'authentification, le contrôle d'accès, par les pairs découverte IPCP, etc. Depuis PCIP sont les mêmes pour chaque DIF , il faut un cadre de gestion de couche commune qui peut être adaptée à l'environnement opérationnel de chaque DIF. Un tel cadre est introduit à l'article 6.

5.4 Des exemples de configurations de DIF

5.4.0 introduction

Cette clause présente quelques exemples pour faciliter la compréhension comment peuvent être utilisés DIF dans les réseaux du monde réel.

5.4.1 Virtual Private LAN Service de (VPLS)

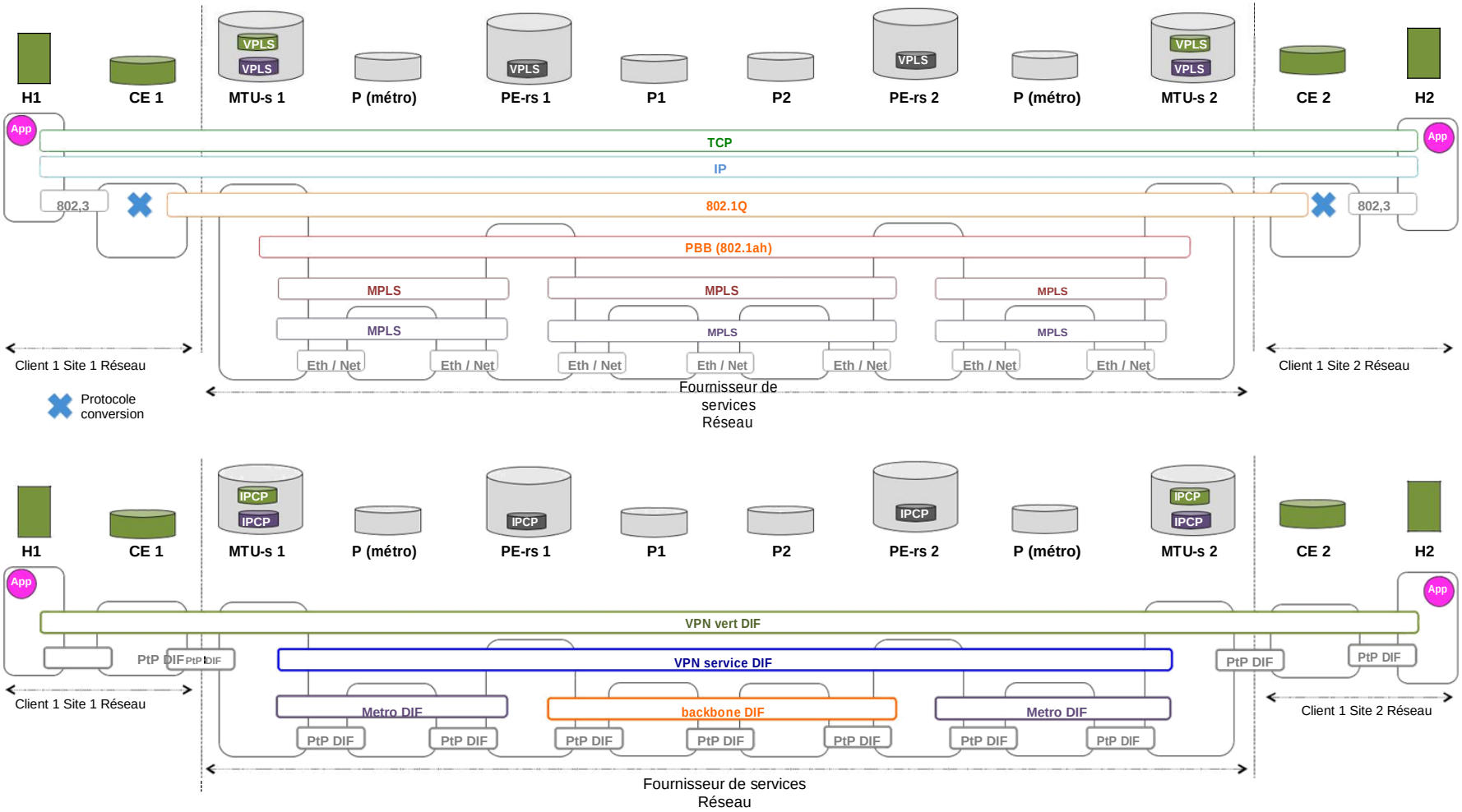


Figure 7: Exemple de réseau fournisseur offrant réseaux privés virtuels d'entreprise:
l'architecture actuelle de protocole (en haut) et RINA (en bas)

La partie supérieure de Figure 7 représente un opérateur fournissant un réseau local privé virtuel service (VPLS) pour interconnecter deux sites clients à la couche 2. Le fournisseur de services exécute le service VPN de couche 2 sur deux MPLS réseaux métropolitains et un noyau MPLS basé. Bridging Provider Backbone (PBB) est utilisé pour isoler le routage du service VPN sur le réseau du fournisseur de l'espace d'adressage du client. Un équivalent configuration RINA est représentée dans la partie inférieure de la figure 7. Point-to DIF point (PTP) fournissent des services IPC sur différents types de liaisons point à point. Metro fournissent IPC sur DIF réseaux d'agrégation de métro, le trafic multiplexage des différents types de services de l'opérateur fournit sur le segment métropolitain. Un DIF de squelette fournit IPC sur le segment de base du réseau, interconnexion POP dans différentes villes.

5.4.2 LTE Evolved Packet Système (EPS) Plan utilisateur

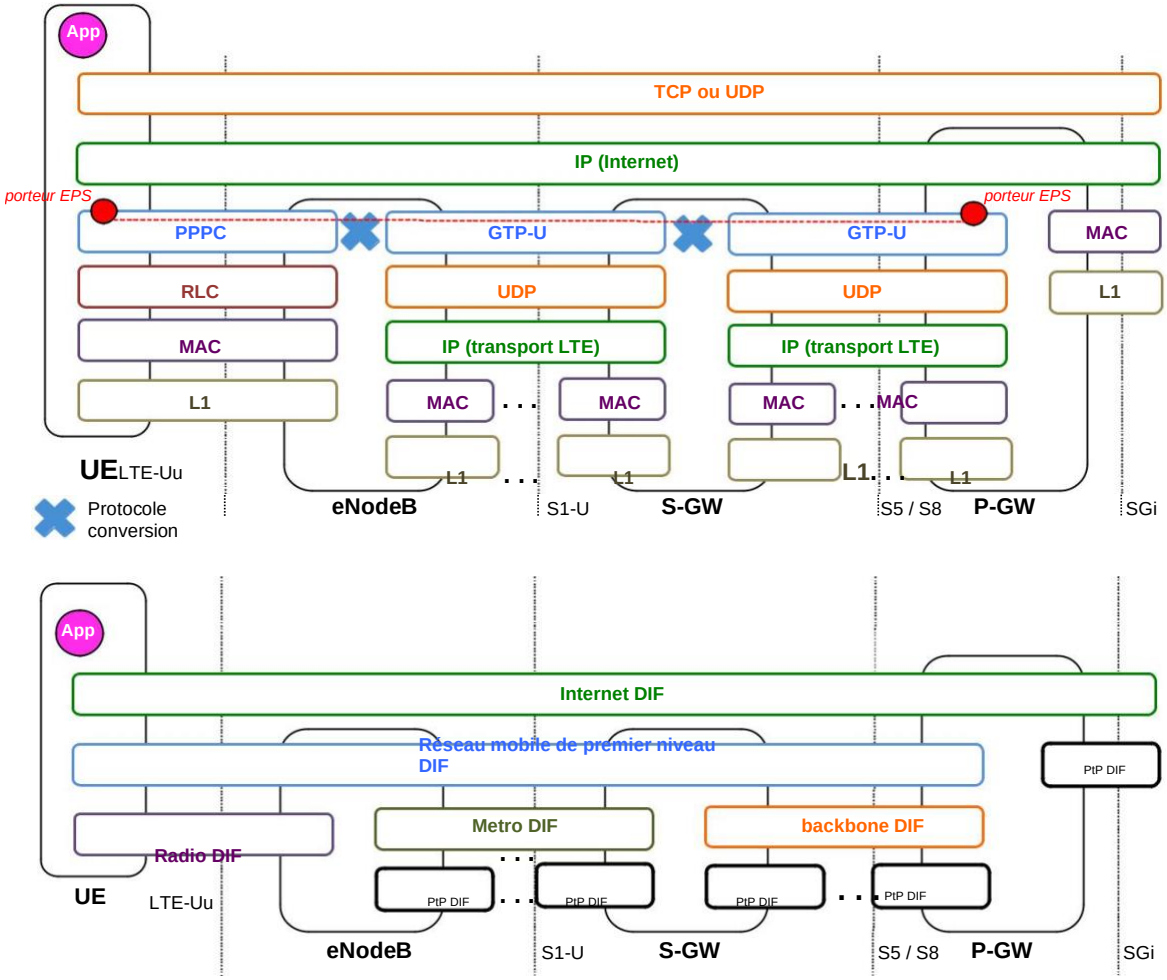


Figure 8: réseau d'accès cellulaire offrant des services Internet: pile de protocole LTE (up) et RINA (vers le bas)

Figure 8 montre la pile de protocoles de plan d'utilisateur d'un réseau LTE, avec i) des protocoles radio (RLC, MAC, L1), les protocoles de tunnellisation pour créer des porteurs (flux) sur le réseau mobile (PDCP et GTP) et le TCP de recouvrement, UDP et les couches IP de l'Internet public. tunnels GTP sont agrégées sur l'agrégation et les couches backbone IP du fournisseur, qui multiplexer les porteurs LTE avec d'autres types de trafic appartenant à d'autres services offerts par l'opérateur. Une structure équivalente peut être recréé en utilisant la stratification générique de RINA, comme indiqué dans la partie inférieure deFigure 7. Une radio multi-accès DIF gère l'allocation des ressources radio et IPC sur les médias sans fil. Un réseau mobile haut niveau fournit des flux sur DIF la portée du réseau mobile - les politiques de ce sont optimisés pour DIF Jongler avec des taux de mobilité d'équipement utilisateur (UE). Metro et Backbone multiplex et transport de DIF le trafic du haut de DIF niveau du réseau mobile et d'autres services en fournissant d'autres DIF sur les segments de métro et réseau de base. Enfin, l'Internet permet aux applications publiques DIF dans l'UE de se connecter à d'autres applications disponibles sur l'Internet (d'autres peuvent également demander DIF à ce niveau, par exemple une entreprise privée pour les utilisateurs autorisés DIF d'un réseau d'entreprise externe).

Notez que l'architecture LTE est logiquement comparable à l'architecture 5G pour le bien du présent document. Pour un résumé des différences entre les EPS LTE et 5G SBA (Based Service Architecture), s'il vous plaît voir ETSI GS NGP 001 (V1.3.1)[I.25] Annexe B (5G modèle de réseau mobile).

5.4.3 Multi-location Data Center

Finalement, Figure 9 montre un exemple d'un réseau Data Center supportant le multi-location. Dans ce cas, le protocole VXLAN est utilisé pour créer plusieurs réseaux virtuels de couche 2 sur une base partagée Centre IPv6 données Fabric. L'équivalent en configuration RINA est représenté au bas de la même figure, avec deux types de DIF: un Data Center Fabric DIF qui alloue les ressources dans le tissu de feuilles colonne vertébrale aux flux utilisés par la concurrence DIF des locataires, qui fournissent des domaines de réseaux isolés et personnalisés à différents locataires.

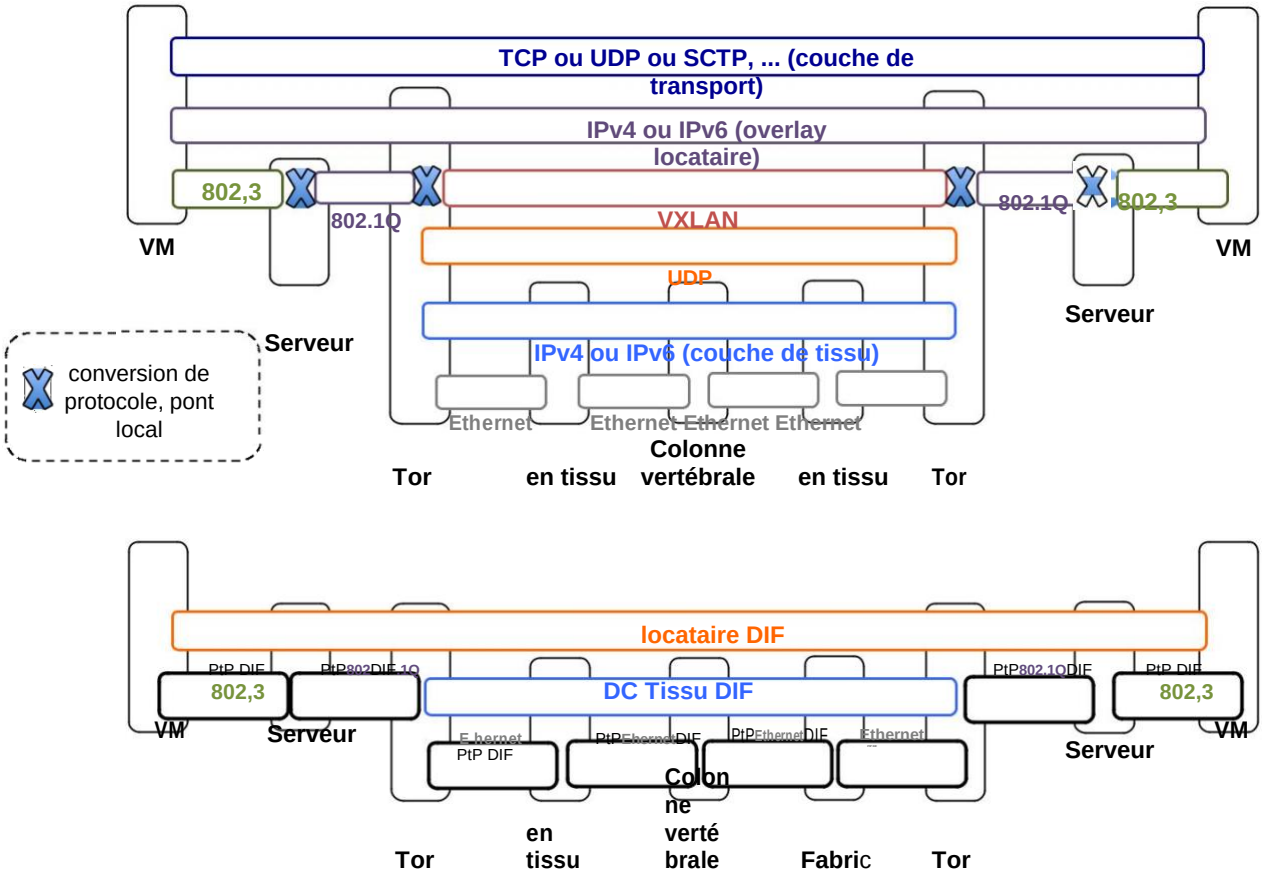


Figure 9: Multi-locataire centre de données: architecture de protocole courant (en haut), RINA (en bas)

5.5 Résumé des propriétés structurales RINA

Cette clause résume la façon dont RINA aborde les problèmes identifiés à l'article 4.3.1.

- **Les différentes couches, les mêmes fonctions mais différentes politiques.** Dans RINA toutes les couches remplissent les fonctions requises pour fournir des IPC distribués sur une certaine portée et l'étendue de la QoS. Les couches sont des unités d'allocation des ressources, et non pas des unités de modularité. Chaque couche gère un ensemble de ressources (tampons, la capacité de planification, la bande passante) à l'aide d'une structure invariante commune, quel que soit la couche qui gère un point à point, effectue l'agrégation sur un réseau métropolitain ou fournit un service VPN à une certaine application. Différentes politiques permettent à l'infrastructure de couche commune de fonctionner de manière optimale sur différents champs d'application et les gammes de QoS.

- **stratification stricte: les couches sont des boîtes noires.** Chaque couche RINA est indépendante de l'autre, un DIF ne peut utiliser que le DIF des services de couche inférieure de DIF en invoquant les opérations dans l'API inférieur DIF - donc aucune violation de la couche sont autorisés. Au sein d'une couche (toutes les fonctions de transfert de données, de commande de transfert de données et de gestion de couche) ont différents degrés de dépendance ou d'accouplement à l'autre. La conception des différents cadres de protocole au sein de RINA fait en sorte que le DIF de toutes les fonctions a suffisamment d'informations DIF disponible pour son bon fonctionnement.

- **nombre variable de couches, a décider au moment de la conception du fonctionnement.** L'architecture RINA n'est pas liée au nombre de couches qui se trouve dans un réseau. Chaque réseau doit utiliser le nombre de couches qui permettent de résoudre de manière optimale à ses besoins d'allocation des ressources et de sécurité: ni plus ni moins. Par conséquent, l'architecte du réseau a la liberté et une flexibilité considérable dans la conception du réseau, tout en limitant encore la complexité globale en raison de l'utilisation de l'infrastructure commune immuable à chaque couche - quel que soit son classement / positionnement. Cet environnement contraste avec le nombre « fixe et statique » des couches dans les architectures de réseau actuelles, où les concepts tels que le réseau de virtualisation, des tunnels et des superpositions doivent être introduites pour contourner cette limitation au prix d'une augmentation de la complexité globale du système.

- **API cohérente à travers les couches.** Puisque toutes les couches offrent le même service IPC, l'API offerte par toutes les couches est le même. Cette API permet des instances de points d'accès et d'allocation des flux de communication d'utilisation à d'autres applications, la définition d'un ensemble d'exigences pour la qualité du flux de communication. Depuis PCIP ne sont que comme toute autre application distribuée sous forme spécialisée de processus d'application, utiliser DIF sous-jacente ferait DIF.

6 cadres de protocole générique

6.1 La structure interne d'un processus IPC

L'un des principes de conception RINA clé a été de maximiser invariance et de minimiser les discontinuités. En d'autres termes, extraire le plus commun possible sans créer de cas particuliers. L'application du concept de systèmes d'exploitation de séparation mécanisme et de la politique[I.7], d'abord aux protocoles de transfert de données, puis à la machine de gestion de couche (généralement appelée au plan de contrôle), il se trouve que deux protocoles sont nécessaires dans un DIF [I.8]:

- Un cadre de protocole de transport de données unique qui prend en charge de multiples politiques et qui permet différentes syntaxes de béton (longueur des champs dans les PDU de protocole). Ce cadre de protocole est appelé EFCP - l'erreur et le protocole de contrôle de flux.

- Un protocole d'application commun qui fonctionne sur des objets distants utilisés par toutes les fonctions de gestion de couche (inscription, la gestion des espaces de noms, la répartition des flux, l'allocation des ressources, coordination de la sécurité). Ce protocole est appelé CDAP - le Protocole d'application distribuée commun. CDAP est accompagné d'un mécanisme de gestion de couche commune qui simplifie la spécification et le développement des fonctions de gestion de couche spécifique.

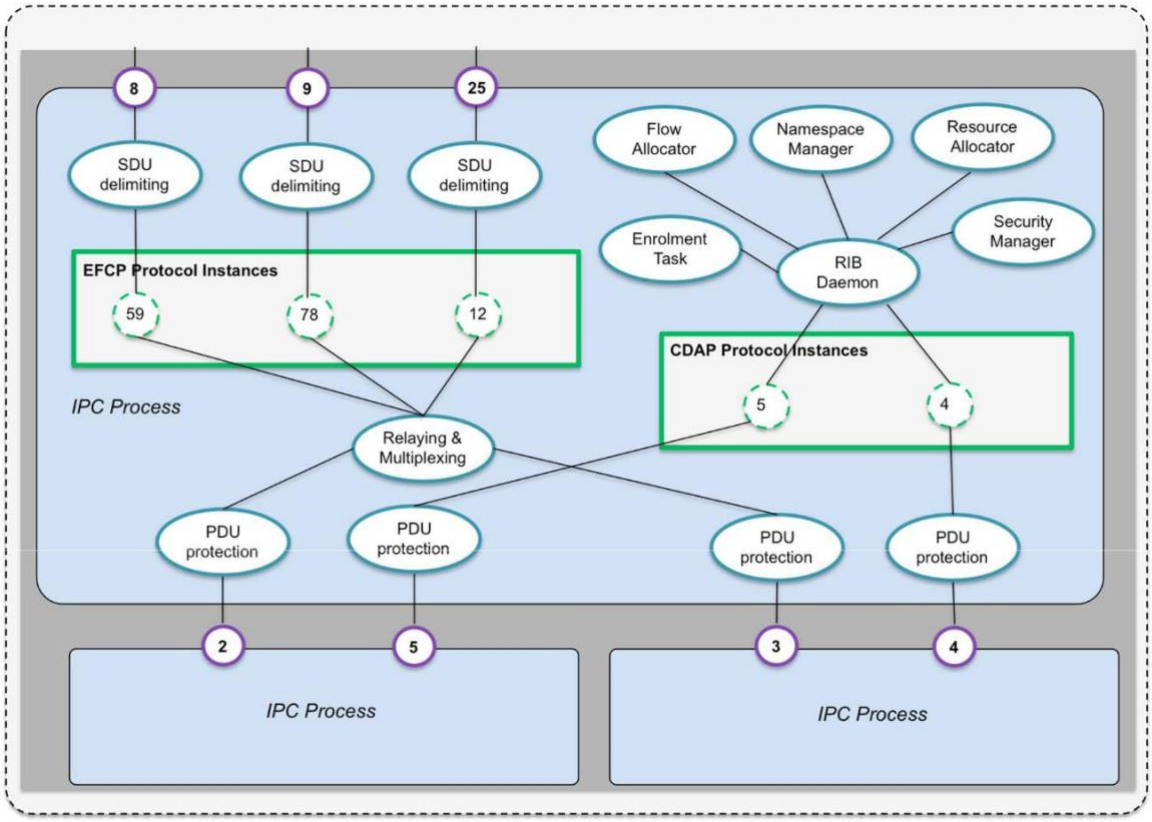


Figure 10: Internes d'un procédé CIP, décrit en utilisant le modèle de protocole ETSI GS 007 NGP [I.4]

La séparation du mécanisme et de la politique a également fourni de nouvelles informations sur la structure de ces fonctions au sein du processus IPC. Les principaux composants d'un IPCP sont présentés dans leFigure 10 et peut être divisé en trois catégories:

a) Transfert de données, découpler par un vecteur d'état de.

b) Contrôle de transfert de données, découplée par une base de données sur les ressources de.

c) Gestion de la couche. Ces trois lieux de traitement sont caractérisés par la diminution du temps de cycle et la complexité croissante de calcul (fonctions plus simples exécutent plus souvent que les complexes):

- *SDU Délimitation*. L'intégrité du SDU écrit à l'écoulement est conservé par l'intermédiaire d'une fonction DIF de délimitation. Délimitation adapte également la SDU à la taille maximale de PDU. Pour ce faire, comprend les mécanismes de délimitation de la fragmentation, réassemblage, concaténation et de séparation.

- *EFCP, l'erreur et le protocole de contrôle de flux*. Ce protocole est basé sur le travail de Richard Watson[I.9] et le mécanisme et la politique sépare. Il y a un exemple de l'état de protocole pour chaque débit en provenance ou à ce processus IPC. Le protocole naturellement clive dans le transfert de données (séquençage, perdus et en double détection, l'identification des connexions parallèles), qui met à jour un vecteur d'état; et transfert de données de contrôle, composé de contrôle de retransmission (ack) et le contrôle de flux.

- *RMT, le relayage et multiplexer Task*. Il prend une décision d'acheminement sur les PDU entrantes et multiplexe plusieurs flux sortants de PDU sur un ou plusieurs (N-1) circule. Il y a un processus RMT par IPC.

- *SDU protection*. Il fait la détection d'intégrité / erreur, par exemple CRC, le cryptage, la compression, etc. potentiellement il peut y avoir une politique différente SDU protection pour chaque flux (N-1).

L'état du processus IPC est modélisé comme un ensemble d'objets stockés dans la base d'informations de ressources (RIB) et accessible par le démon RIB. Le RIB impose un schéma sur les objets de modélisation de l'état IPCP, définissent quelles opérations CDAP sont disponibles sur chaque objet et quels seront leurs effets. Le Daemon RIB fournit toutes les fonctions de gestion de couche avec les moyens d'interagir avec les semi-rigides de PCIP par les pairs. La coordination au sein de la couche utilise le protocole d'application Distributed Common (CDAP).

6.2 Transfert de données: fonctions, protocoles et procédures

6.2.1 introduction

EFCP, l'erreur et le protocole de contrôle de flux, est le protocole de transfert de données unique d'un DIF. Afin de permettre son adaptation aux différents environnements d'exploitation, EFCP prend en charge plusieurs politiques et plusieurs syntaxes spécifiques. Pour ce faire, la spécification EFCP définit les crochets où les différentes politiques peuvent être enfichés - décrivant aussi le comportement des politiques par défaut - ainsi que la syntaxe abstraite de EFCP (types de PDU et ses champs, sans décrire son encodage). EFCP met à profit les résultats publiés par Richard Watson (et plus tard mis en œuvre dans le protocole delta-t). Watson a prouvé que bondissant trois minuteries est une condition nécessaire et suffisante pour la gestion des connexions de transport fiable; en d'autres termes: SNY et FinS ne sont pas nécessaires. Cela simplifie non seulement la mise en œuvre du protocole,[I.10] ou des attaques au niveau de transport [I.11].

EFCP comporte deux parties: DTP (protocole de transfert de données), qui porte sur les mécanismes étroitement couplées à des PDUs de transfert de données (telles que adressage ou séquençage) et DTCP (Data Transfer Control Protocol), qui traite des mécanismes couplés de manière lâche, tels que le contrôle de flux ou un contrôle de retransmission. DTP et DTCP sont assez indépendants et fonctionnent avec leurs propres PDUs, étant tout à couplage lâche via un vecteur d'état.

6.2.2 DTP PDU syntaxe abstraite

Figure 11 illustre la syntaxe abstraite du DTP EFCP PDUs. Notez que la longueur d'adresse, SGQ-id, CEPID, la longueur et le numéro de séquence des champs dépend de l'environnement DIF. Par exemple, pas de champs d'adresse source ou de destination sont nécessaires pour en liaisons point DIF à point.

VERS	DST ADDR	SRC ADDR	QoS ID	DST CEPID	SRC CEPID	PDU Type	drapeaux	Longueur	Seq. Nombre	Données d'utilisateur
1 octet	addr-octets	addr-octets	qos-octets	cepid-octets	cepid-octets	1 octet	1 octet	longueur-octets	seqnum-octets	n-octets

Figure 11: syntaxe abstraite de PDUs DTP

- **Version:** Version EFCP.
- **Src / adresse de destination:** Adresses des processus IPC qui hébergent les extrémités de cette connexion. EFCP
- **QoS-id:** Id du cube QoS où cette connexion EFCP appartient (voir l'article 8.1).
- **cepids Src / destination:** Les identifiants des instances de EFCP qui sont les extrémités de cette connexion. EFCP
- **Type PDU:** Code indiquant le type de PDU (dans ce cas, il est une unité PDU DTP).
- **drapeaux:** Indiquer les conditions qui peuvent affecter le traitement de la PDU et peut changer d'une PDU à l'autre.
- **Longueur:** La longueur totale de l'unité PDU, en octets.
- **Numéro de séquence:** Numéro de séquence de la PDU.
- **Données d'utilisateur:** Contient un ou plusieurs fragments de SDU et / ou un ou plusieurs complète SDU.

6.2.3 DTCP Formats PDU

Selon les politiques associées à une connexion EFCP particulière, l'instance DTCP peut être configuré pour exécuter des fonctions de contrôle débit et / ou la retransmission. Bien que la spécification définit EFCP 10 codes de fonctionnement définis pour DTCP, en réalité, il n'y a que trois types PDU:

a) Ack / Nack / flux;

b) Sélective Ack / Nack / flux; et

c) Contrôle Ack.

Chacune de ces unités PDU de commande porte les adresses, une connexion id, un numéro de séquence et de commande de retransmission et / ou des informations de contrôle de flux, etc. Les opcodes indiquent quels champs de l'unité PDU sont valides. Les champs obligatoires pour ces PDUs peuvent être prolongés par la définition des politiques.

6.2.4 Vue d'ensemble des procédures de transfert de données

Une vue d'ensemble de haut niveau des procédures de transfert de données sont fournies par Figure 12. Notez que ceci est un exemple de scénario montrant des fonctions logiques, en tout cas, ce qui suggère une stratégie est mise en œuvre particulière.

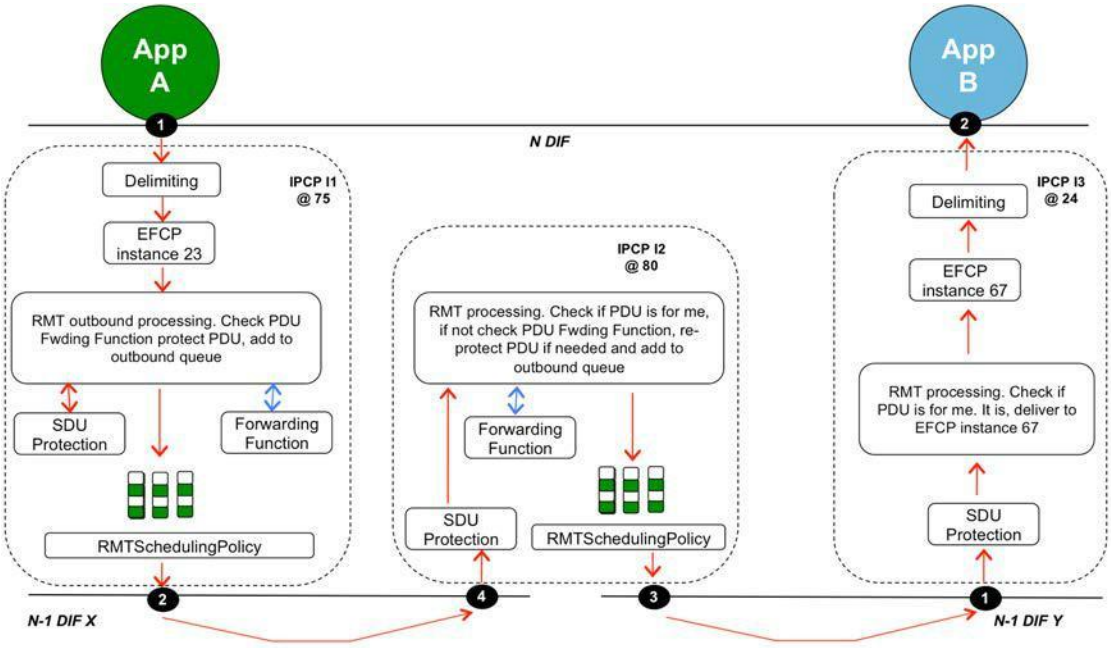


Figure 12: Exemple de procédures de transfert de données

Dans ce scénario exemple, le N fournit un DIF flux identifié par le port-id 1 entre les applications A et B. Application A écrit un SDU au port, invoquant l'API DIF. Le SDU est ensuite traité par la fonction de délimitation de IPCP I1, qui va créer un ou plusieurs champs de données d'utilisateur EFCP de la SDU, conformément à la politique de délimitation. EFCP champs de données utilisateur sont livrés à l'instance EFCP 23 - qui est actuellement lié au port-id 1 - ce qui crée une ou plusieurs unités PDU de transfert de données EFCP et les remet à la relayage et multiplexer Tâche (RMT).

Le RMT vérifie la fonction de transfert (une autre politique), qui renvoie le port-ids d'un ou plusieurs flux de N-1 à travers laquelle l'unité PDU doit être transmis pour atteindre le saut suivant (dans ce cas le IPCP avec l'adresse 80). En général, il y aura une ou plusieurs files d'attente devant chaque port N-1, et une politique d'ordonnancement triera sortants pour la transmission PDUs selon différents critères. Une fois que le port N-1 à laquelle la PDU sera transmise est connue, la politique de protection des SDU associée peut être appliquée à la PDU (ou il peut être appliqué lorsque EFCP crée la PDU s'il y a une politique de protection SDU commune pour tous les N- 1 ports).

Finalement IPCP I2 lit le PDU du port N-1 4. Il supprime la protection SDU nécessaire pour traiter l'en-tête de PDU et le RMT décide si elle est la destination finale de la PDU (en fonction de l'environnement de DIF, par exemple, la vérification de la destination champ d'adresse dans cet exemple). Dans ce cas, le IPCP est pas la destination finale, de sorte que le RMT vérifie la fonction de transfert, qui renvoie une ou plusieurs ports N-1 à travers lequel la PDU est transmise. La protection nouvelle demande RMT si nécessaire (politique de protection SDU peut être différent), et gère la PDU pour transmission à la politique de planification, qui écrit finalement la PDU au port N-1.

Enfin, le PDU atteint IPCP I3 via le port N-1 3. Protection SDU est supprimé, les contrôles RMT si elle est la destination finale de l'unité de distribution et, puisque dans ce cas, il est, il fournit le RMT à l'instance EFCP de destination (EFCP exemple 87 dans l'exemple) pour un traitement ultérieur. L'instance de EFCP met à jour son état interne et peut générer zéro ou plusieurs PDUs de contrôle. EFCP récupère le champ de données d'utilisateur de PDU, et fonctionne avec la fonction de délimitation en fonction des politiques configurées afin de récupérer SDU complète. Enfin, SDU sont lus à partir du port 2 par application B.

6.3 Gestion des calques: protocole, fonctions et procédures

6.3.1 introduction

Les différentes fonctions de gestion de la couche d'un effet de levier de processus IPC un des mécanismes communs d'échanger des informations avec leurs pairs. Tout le processus IPC externe état visible est modélisé comme des objets qui suivent un schéma logique appelé RIB, Base de données sur les ressources. La spécification du RIB définit la désignation de l'objet, les relations entre les objets (héritage, confinement, etc.), les attributs de l'objet et les opérations CDAP qui peuvent être appliquées sur eux. L'accès au RIB est médiatisée par le Daemon RIB. Le RIB Daemon d'un échange IPCP CDAP avec PDUs RIB Démons du voisin PCIP. Ces PDUs communiquent les opérations à distance sur les objets. Lorsqu'une tâche de gestion de couche souhaite communiquer une action à un pair (par exemple une mise à jour de routage), il demande au Daemon pour effectuer CÔTES une action sur un ou plusieurs objets d'un ou plusieurs voisins PCIP. Le démon RIB génère les PDU CDAP requis et les envoie sur les flux requis N-1 pour communiquer l'action de ses voisins. Lorsque le Daemon reçoit un RIB CDAP PDU, il décode, analyse les objets sont impliqués et en informe les fonctions de gestion de couche concernés (qui ont déjà souscrit à des objets de leur intérêt).

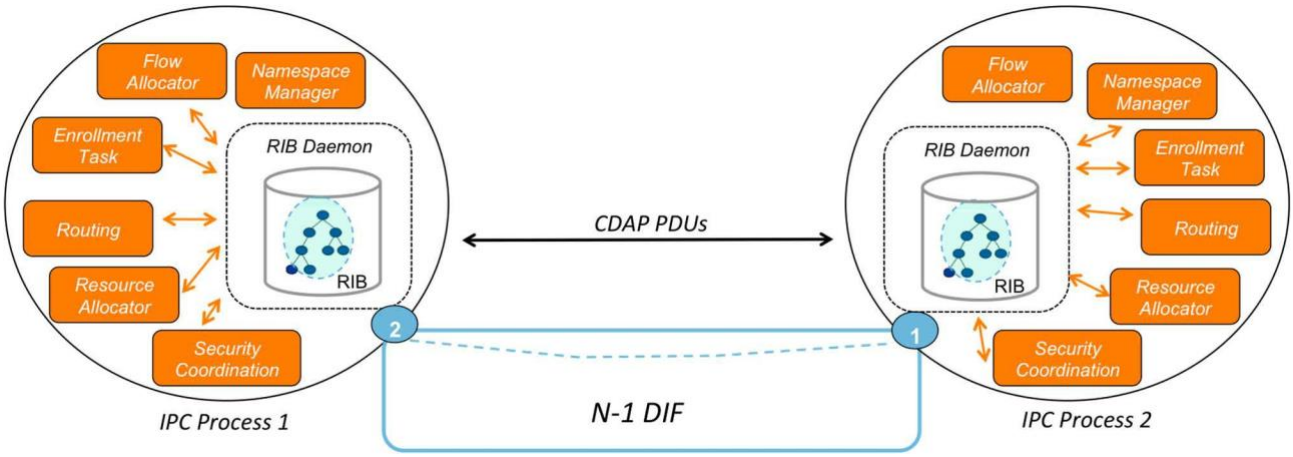


Figure 13: Machines de gestion de couche commune: semi-rigide, semi-rigide Daemon et CDAP

L'ensemble du processus est illustré à la Figure 13. Cette conception permet aux tâches de gestion de couche pour se concentrer uniquement dans les fonctions qu'ils fournissent et déléguer les tâches rutinary de PDUs générer et protocole d'analyse syntaxique au Daemon RIB (en fait, les tâches de gestion de couche ne sont même pas au courant de CDAP). Si nécessaire, de nouvelles fonctions de gestion de couche peuvent être ajoutés sans la nécessité de définir de nouveaux protocoles. De plus, le démon RIB peut coordonner et optimiser la génération d'unités PDU de protocole à partir de différentes tâches de gestion de couche; réduisant ainsi le trafic de gestion de couche entre PCIP pairs. La spécification définit CDAP une syntaxe abstraite qui décrit les différents types de CDAP et leurs PDUs champs. De multiples encodages en béton peuvent être pris en charge (il est juste une politique de DIF), tels que les différents encodages ASN.1, Google™ Protocol Buffers, etc.

Avant de pouvoir échanger des informations, deux PCIP pairs établissent une association entre eux. Cette association est appelée connexion d'application en termes RINA. Pendant la phase de connexion d'application de l'établissement, les informations de nommage échange PCIP, le cas échéant authentifie l'autre, et d'accord dans les syntaxes abstraites et concrètes de CDAP / RIB à utiliser dans la connexion, ainsi que dans la version du RIB. Cette information de version est importante, car les mises à jour du modèle RIB ne peuvent pas être appliquées de façon uniforme à l'ensemble du réseau à la fois. Par conséquent, il devrait être possible de permettre à plusieurs versions du RIB à utiliser, pour permettre des mises à niveau supplémentaires.

6.3.2 fonctions de gestion de couche: inscription

L'inscription est la procédure par laquelle un IPCP se joint à un existant et DIF initialisé avec suffisamment d'informations pour devenir membre pleinement opérationnel DIF. L'inscription commence après un IPC-processus établit une connexion d'application avec un autre IPCP, ce qui est un membre d'un DIF. Une fois la connexion d'application est établie cette procédure d'inscription peut procéder. La procédure d'inscription spécifique est une politique de chaque DIF, mais en général il implique des opérations similaires à celles de la politique par exemple décrit dans le paragraphe suivant.

Le IPCP membre lit l'adresse du Nouveau membre IPCP. Si nul ou expiré, il attribue une nouvelle adresse; autrement, suppose le nouveau membre a été très récemment un membre. Le nouveau membre se lit alors les informations qu'il n'a pas pris en compte la façon dont « nouveau » est. Ces paramètres caractérisent le fonctionnement de ce DIF et peuvent inclure des paramètres tels que la taille max PDU, différentes gammes de temporisation, gammes de politiques, etc. Une fois terminé, le nouveau membre est maintenant membre et cela déclenche une mise à jour normale RIB (pour obtenir la dernière des informations à jour sur le routage, le répertoire, l'allocation des ressources, etc.).

6.3.3 fonctions de gestion de couche: Gestion de l'espace de noms

La gestion d'un espace de noms dans un environnement distribué nécessite une coordination pour veiller à ce que les noms restent sans ambiguïté dans le champ droit et peuvent être résolus efficacement. Le nom Space Manager (NSM) intégré dans le DIF est responsable des noms d'applications de cartographie à des adresses de processus IPC - ce dernier étant l'espace de nom géré par le NSM DIF. des moyens spécifiques de réaliser cette cartographie sont basés sur les politiques et varient d'une DIF DIF. Pour les petits, les environnements distribués, cette gestion peut être assez résolution décentralisée et le nom peut être réalisé par une recherche exhaustive. Une fois trouvé l'emplacement de l'information qui a résolu le nom peut être mis en cache localement afin de réduire les recherches futures. Il est facile de voir comment que l'environnement distribué croît que ces caches seraient en utilisant plus souvent organisées des notes dans le nom lui-même, telles que l'affectation hiérarchique, à raccourcir les temps de recherche. Pour les grands environnements, bases de données distribuées peuvent être organisées avec la réplication complète ou partielle et les conventions de dénomination, à savoir la structure topologique, et les règles de recherche pour réduire la recherche, ce qui nécessite une gestion plus de l'espace de nom.

Les deux fonctions principales de la DIF NSM sont à attribuer des adresses valides aux processus CIB pour son fonctionnement dans le DIF et à résoudre dans lequel procédé IPC est enregistré une application spécifique. En d'autres termes, le NSM maintient une correspondance entre des noms d'applications externes et des procédés CIP où il y a le potentiel pour une liaison au sein du même système de traitement. Par conséquent, l'inscription, l'enregistrement de l'application et l'allocation des flux nécessitent les services du NSM.

6.3.4 fonctions de gestion de couche: répartition du débit

Le flux Allocataire est responsable de la création et la gestion d'une instance de l'IPC, soit un flux. L'IPC-API communique les demandes de l'application du DIF. Un Allouer-demande provoque une instance du flux Allocataire à créer. L'allocateur instance de débit (FAI) détermine quelles politiques seront utilisées pour fournir les caractéristiques demandées dans le Allouer. Il est important que la façon dont ces caractéristiques sont communiquées par l'application est découplée de la sélection des politiques. Cela donne la flexibilité importante dans l'utilisation de différentes DIF politiques, mais permet également de nouvelles politiques à incorporer. Le FAI crée l'instance de EFCP pour le flux demandé avant d'envoyer le flux CDAP Créer demande de trouver l'application de destination et de déterminer si le demandeur a accès.

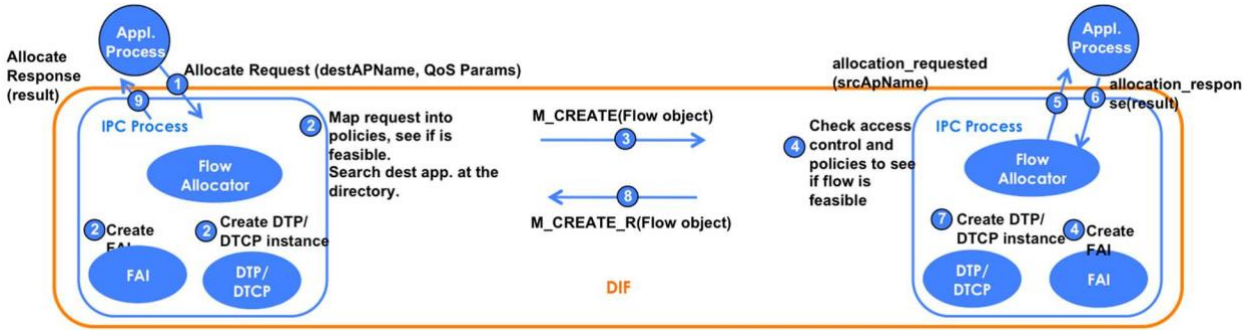


Figure 14: Illustration de la procédure d'allocation des flux

Une demande de création est envoyée à la source et les applications de destination, des informations de qualité de service, et les choix politiques, ainsi que les informations de contrôle d'accès nécessaires. Utilisation du composant NSM, la FAI recherche le IPCP dans le DIF qui réside sur le système de traitement qui a accès à l'application demandée. Cet échange accomplit trois fonctions:

- En suivant les règles de recherche en utilisant la fonction de gestion de l'espace nom pour trouver l'adresse d'un IPC-processus avec accès à l'application de destination.
- Déterminer si le processus de demande demandant un accès au processus d'application demandé et si oui ou non la destination IPC-processus peut prendre en charge la communication demandée.

- Instanciation du processus d'application demandée, le cas échéant, et l'attribution d'un FAI et un port-id dans la destination IPCP.

La réponse créer renvoie une indication de réussite ou d'échec. En cas de succès, l'adresse de destination et des informations-ID de connexion seront également retournés avec des choix politiques proposées. Cela donne les IPC-processus d'information suffisante pour lier ensuite le port-ids à une EFCP instance, à savoir une connexion, de sorte que le transfert de données peut procéder.

6.3.5 fonctions de gestion de couche: allocation des ressources

La ressource allocateur (RA) est l'intelligence de base du processus de classification. Il surveille le fonctionnement du processus IPC et fait des ajustements à son fonctionnement pour le maintenir dans la plage de fonctionnement spécifiée. Les fonctions de l'AR sont expliquées plus en détail à l'article 8.2.

6.3.6 fonctions de gestion de couche: routage

Une contribution majeure à la ressource allocateur est itinéraire. Routage effectue l'analyse de l'information maintenue par la nervure d'apporter une contribution de connectivité pour la création d'une fonction de transfert. L'article 8 aborde ce sujet plus en détail.
Le choix des algorithmes de routage dans un particulier est une question DIF de la politique.

6.3.7 fonctions de gestion de couche: coordination de la sécurité

Coordination de la sécurité est la composante du processus IPC responsable de la mise en œuvre d'un profil de sécurité cohérente pour le processus IPC, la coordination de toutes les fonctions liées à la sécurité (authentification, contrôle d'accès, la confidentialité, l'intégrité) et de l'exécution aussi certains d'entre eux (l'audit, la gestion des titres de compétences). La sophistication de cette fonction de gestion de couche est une question de politique.

6.4 Résumé des principes de conception du cadre du protocole RINA

Cette clause résume la façon dont RINA aborde les problèmes identifiés à l'article 4.3.2.

- **Une répartition claire des fonctions de chaque couche.** Chaque DIF remplit des fonctions de fournir IPC sur une certaine portée et l'étendue de la QoS (transfert de données et les fonctions de contrôle de transfert de données), ainsi que les fonctions pour gérer de façon autonome ce service IPC dans les (fonctions de gestion de couche) DIFF. fonctions de transfert de données sont faiblement couplés aux données des fonctions de commande de transfert via un vecteur d'état, et les transferts de données et les fonctions de contrôle de transfert de données sont faiblement couplés à la couche des fonctions de gestion via la base de l'information RINA (RIB). Il n'y a pas besoin de concepts tels que « données séparées et des plans de contrôle » avec des protocoles différents, toutes les fonctions d'un sont proprement séparés DIF entre les trois catégories mentionnées ci-dessus. Cette approche est également généralement suivie par des protocoles IEEE (tels que IEEE 802.11TM [I.56]), RINA généralise à toutes les couches.

- **Deux cadres de protocole par. DIF** Au sein d'une fonction de contrôle de transfert de données DIFF et le transfert de données sont réalisées par l'erreur et flux Control Protocol (EFCP). EFCP définit une syntaxe abstraite (définition des champs de transfert de données et de contrôle PDUs) et la fonctionnalité programmable commun pour réaliser le protocole de transfert de données spécifiques de chaque DIF. Pour ce faire, une syntaxe concrète (de codage pour l'en-tête PDU de transfert de données) et un ensemble de politiques de contrôle de flux, contrôle de la retransmission, la gestion de la congestion, la planification, la transmission et la protection SDU doit être défini. fonctions de gestion de couche (d'inscription, la répartition des flux, l'allocation des ressources, la gestion des espaces de noms, routage, authentification, contrôle d'accès, gestion de la sécurité) tirer parti de l'infrastructure de gestion de couche commune, qui prévoit:

  i) un protocole d'application pour faire fonctionner à distance sur les objets (CDAP);

  ii) un schéma pour modéliser l'état d'un processus de classification; et

  iii) un ensemble de politiques visant à distribuer les informations d'état IPCP tel que requis par chaque fonction de gestion de couche (sur demande, hiérarchiquement, sur certains événements, etc.).

  les fonctions de gestion de couche juste besoin de définir son modèle d'information d'objet et de préciser ce qui se passe lorsque les opérations CDAP sont invoquées sur les objets définis.

- **fonctions de couche communes sont invariantes, seules des politiques peuvent changer**. Un autre avantage de séparer les parties immuables (les cadres de protocole identifiés dans le premier point) de la partie variable à chaque DIF est que les politiques ne sont pas conçus de manière isolée. Chaque politique a une vision claire « point de branchement » dans l'infrastructure de chaque DIF, avec une fonction bien définie et API. Par conséquent, le nombre d'interactions entre les politiques individuelles et la commune, l'infrastructure immuable de est limitée par DIF conception, ce qui limite la complexité d'un DIF. De plus, étant donné que chaque a la même DIF infrastructure immuable, la même politique peut être utilisée dans tous les DIF, maximisant ainsi la réutilisabilité et l'applicabilité des politiques. Cette situation facilite le raisonnement sur le comportement du réseau et le dépanner.

sept Nommage et d'adressage

7.1 Les noms dans RINA et leurs propriétés

ETSI GS 007 NGP [I.4] fourni une description initiale des noms qui identifient les différents composants du modèle de protocole générique. Cette clause s'applique ce système à l'architecture RINA décrit dans les articles 5 et 6.

Figure 15 illustre les noms requis dans RINA, du point de vue de la N-DIF. Depuis l'architecture de protocole est récursive, le même schéma de nommage est appliqué à chaque DIF. PCIP fournissent des flux de demandes au DIF ci-dessus, qui à leur tour peuvent être d'autres PCIP. Ces applications desservies par le IPCP sont identifiés par un nom d'application, qui a les propriétés suivantes:

- ***Nom de l'application:*** Affecté aux applications, il est l'emplacement indépendant (ne change pas lorsque l'application attache à plusieurs réseaux ou DIF). Il identifie de manière unique l'application dans un espace de noms d'application. Dans les noms généraux iT un ensemble, qui peut avoir un seul membre. Par conséquent, dans les noms généraux peuvent identifier une collection d'instances de processus d'application, qui peut être « toutes les instances d'une application distribuée », un « sous-ensemble des instances d'une application distribuée », « toute instance d'une application distribuée » un « spécifique instance d'une application distribuée », etc.

Depuis PCIP sont également des applications, ils sont identifiés par un nom d'application. Cependant, ce nom d'application est généralement attribué à partir d'un espace de noms qui a une portée plus grande que la DIF où le IPCP appartient, et ne sont pas conçues pour faciliter le transfert et l'acheminement de paquets entre PCIP au sein de cette DIF. Il est donc utile d'affecter un ou plusieurs synonymes temporaires au IPCP, l'adresse (s):

- **Adresse:** synonyme dépendant de l'emplacement d'un nom d'application, attribué à un IPCP. Une adresse reflète l'emplacement du IPCP dans son DIF (emplacement défini comme étant une abstraction du graphe de connectivité DIF). Une adresse est temporaire, son champ d'application est le DIF et doit être changé quand il ne reflète plus correctement l'emplacement du IPCP dans le DIF (c.-à-n'est plus agrégeable).

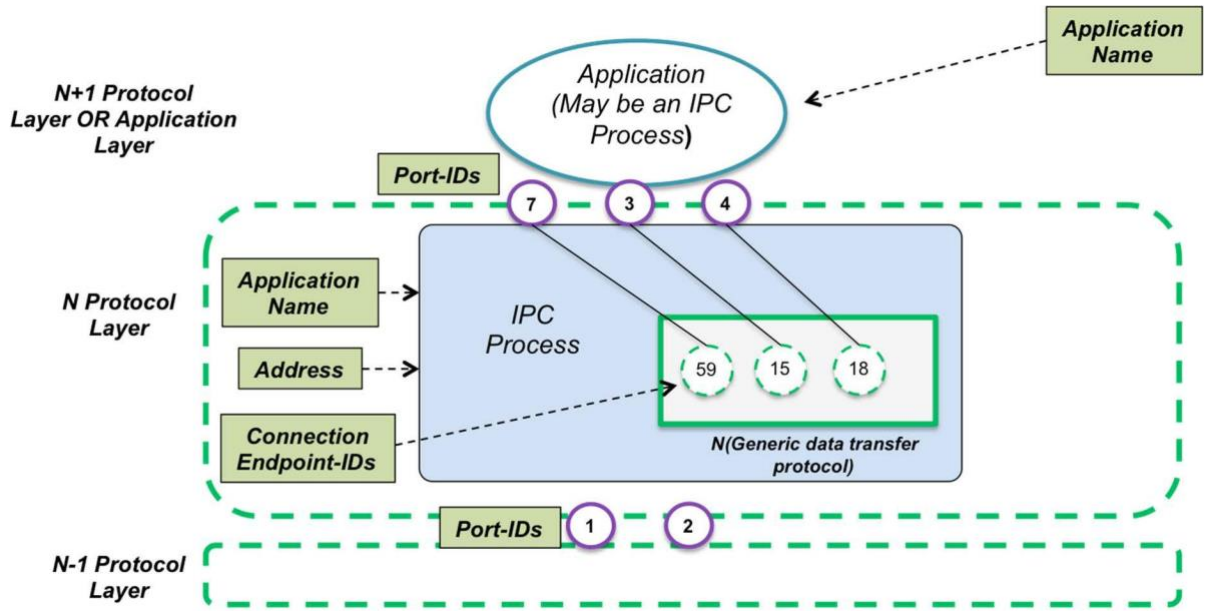


Figure 15: noms dans l'architecture RINA, du point de vue de la N-DIF

Les flux (services de communication fournis par PCIP aux applications) fournissent un service IPC entre deux ports. Ces ports sont utilisés par l'application pour envoyer et recevoir des données, ce qui permet l'application de traiter le service comme une boîte DIF noire. Comme indiqué dans l'ETSI GS 007 NGP[I.4], chaque port dans un équipement réseau est identifié par un port ID:

- **Port-ID:** Identifier la fin d'un flux à l'intérieur d'un équipement de réseau (la portée de ce nom est local à l'équipement de réseau).

PCIP soutenir le fonctionnement d'un écoulement par l'intermédiaire d'une connexion de transfert de données. Tous les PCIP impliqués dans la fourniture d'un flux (peut être deux ou plus) créer une instance d'un protocole de transfert de données pour soutenir l'échange de données écrites et lues à ce flux. Les instances de protocole de transfert de données sont identifiés par des identifiants de connexion en point final (ou CEPIDs). CEPIDs sont les identifiants portés dans des paquets de données, utilisées pour démultiplexer les paquets appartenant à une connexion spécifique une fois qu'ils atteignent la destination IPCP. PCIP créer une liaison locale entre le port-ID et son CEPID support. Ce découplage permet une plus grande sécurité et une flexibilité au DIF[I.12]:

- **Connexion-point d'extrémité ID:** Identifier les instances de protocole de transfert de données qui sont les extrémités d'une connexion. Son champ d'application est locale à l'IPCP, qui stocke également une liaison locale à un port-ID.

Figure 16 montre comment ces noms sont utilisés pour faire fonctionner un DIF et quelles relations existent entre eux, du point de vue d'un DIF (depuis les récursivement d'architecture, le même type de relations et les concepts sont valables pour chaque DIF). Les applications qui souhaitent être accessible par l'intermédiaire d'un certain registre à ce DIF via son nom DIF d'application. Le IPCP à ce système crée une correspondance entre le nom de l'application et l'adresse IPCP. La collection de ces correspondances pour un répertoire est appelé DIF. répertoires distribués DIF peuvent être conçus et mis en œuvre de multiples façons (entièrement répliqués, hiérarchique, via des tables de hachage distribuées, partiellement répliquées, centralisée, basées sur la recherche, etc.), et le choix spécifique pour chaque DIF dépendra de la portée du DIF et ses besoins opérationnels.

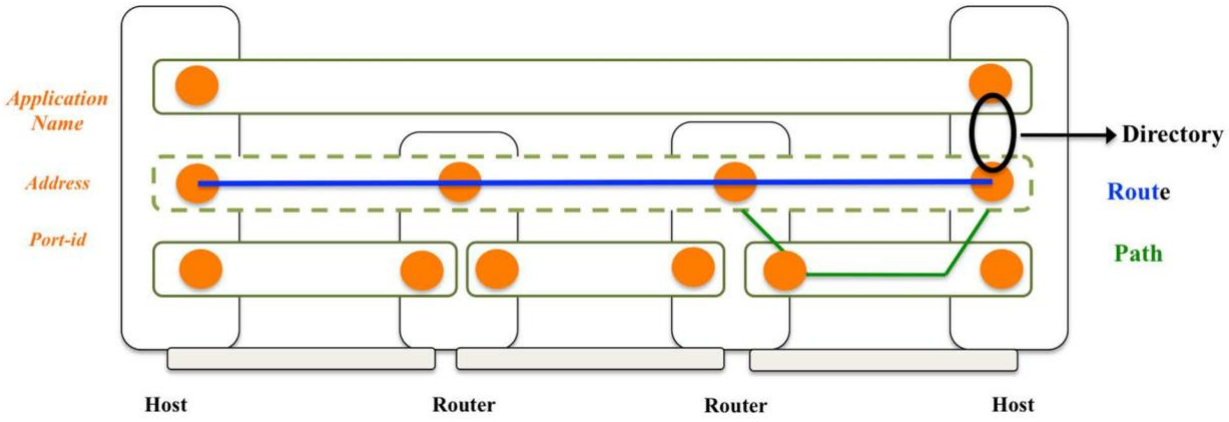


Figure 16: Répertoires, routes et chemins de la perspective d'un N-DIF (rectangle en pointillés)

L'utilisation de répertoires permet de cacher les DIF adresses de PCIP qui sont membres du DIF des applications qui l'utilisent. Applications demandent juste flux à un nom de l'application de destination (qui peut se résoudre à une seule instance ou plusieurs instances d'un processus d'application), et il est le SNDIF celui qui utilise en interne le répertoire pour effectuer la cartographie du nom de l'application de destination aux adresses (s) du IPCP (s) par l'intermédiaire duquel l'instance de l'application cible (s) sont accessibles.

routes sont des séquences d'adresses IPCP. algorithmes de routage calculent un ensemble d'adresses de saut suivant pour chaque adresse de destination (il est important de noter que l'algorithme de routage peut retourner plus d'un saut suivant pour la même adresse de destination, avec des coûts égaux ou différents). Cette procédure génère la table d'adresses suivante-hop. Chaque IPCP puis cartes localement l'adresse suivante-hop au port-ID d'un flux N-1 à travers lequel transmettra les paquets qui voyagent vers cette adresse de destination (le chemin vers le prochain saut). Cette procédure génère la table de transfert. Notez que les deux procédures (calculé prochaine houblon, puis dériver des flux N-1) sont découplées et peuvent exécuter à différentes échelles de temps.

7.2 Implications pour les multi-homing

Compte tenu du schéma de nommage présenté à l'article 7.1 et les propriétés présentées par ses noms, multi-homing est réalisée sans l'ajout d'un protocole dédié. Multi-homing est la capacité d'un noeud de réseau à exploiter la connectivité par l'intermédiaire de multiples points de fixation (à savoir, les données peuvent quitter et entrer dans le noeud par l'intermédiaire des interfaces multiples sous-jacents), qui peuvent ou peuvent ne pas être attachés au même

réseau. Traduire le problème dans l'environnement d'architecture RINA, un processus IPC multiconnecté devrait être en mesure d'envoyer et de recevoir des données via plusieurs ports N-1.

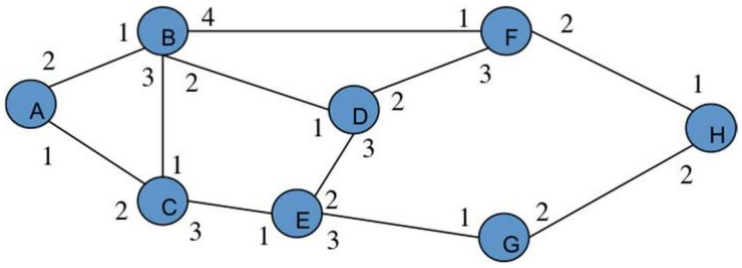


Figure 17: graphique de connectivité d'un DIF, formé par des entités de réseau génériques IPC

Figure 17 montre le graphique de la connectivité d'un exemple DIF. Les cercles bleus représentent PCIP, reliés entre eux par l'intermédiaire des flux N-1 (traits pleins). Chaque cercle bleu est marqué avec l'adresse de la IPCP (A, B, C, etc.), et chaque ligne locale solide avec le port-ID du débit N-1.Figure 18 montre le tableau suivant-hop calculé par chaque IPCP, en supposant qu'un algorithme simple-chemin le plus court est utilisé (pour garder l'exemple simple). Chaque colonne indique le tableau suivant-hop pour une entité de réseau IPC générique spécifique (la première colonne indique le tableau suivant hop pour « A », la seconde la prochaine table hop pour « B », etc.)

Using Next Hop

Destination Address	A	B	C	D	E	F	G	H
A	-	A	A	B	C	D	E	F
B	B	-	B	B	C	D	E	F
C	C	C	-	B	C	D	E	F
D	B	D	B	-	D	D	E	F
E	B	D	E	E	-	D	E	F
F	B	D	B	F	D	-	E	F
G	B	D	E	E	E	D	-	G
H	B	D	B	F	D	H	H	-

Figure 18: tableau suivant-hop pour chaque entité de réseau générique IPC

Si le IPCP « A » envoie des paquets à « H », les paquets contiendra « H » comme adresse de destination. Le IPCP "H" a 2 N-1 flux, une à "F" (avec port-ID "1"), et une à "G" (avec port-ID "2"). Si le débit entre N-1 « F » et « H » échoue, « F » et « H » peut le détecter et émettre une mise à jour de routage qui rejette le flux entre N-1 « F » et « H ». Ensuite, chaque IPCP recalculera la prochaine table de saut et une table de transfert PDU prenant en compte que ce flux N-1 est plus disponible. Packets qui étaient en transit peuvent être réacheminés parce qu'ils sont adressés à « H », quel que soit le chemin qu'ils suivent pour atteindre « H ». IPCP A n'a pas besoin de changer l'adresse de destination du paquet,

Avaient-adresses été affectées aux ports N-1 au lieu des entités de réseau génériques IPC (situation équivalente à celle prônée par l'architecture d'adressage IPv6[I.13]) la situation serait plus complexe, comme le montre Figure 19.Ici, les étiquettes attribuées aux processus IPC (« A », « B », etc.) ne sont que pour les identifier dans les colonnes du tableau suivant-hop, mais pas utilisé pour le routage ou le renvoi. ports N-1 sont affectées des adresses qui sont uniques dans le DIF, qui sont utilisés pour calculer la table de saut suivant représenté sur laFigure 20.

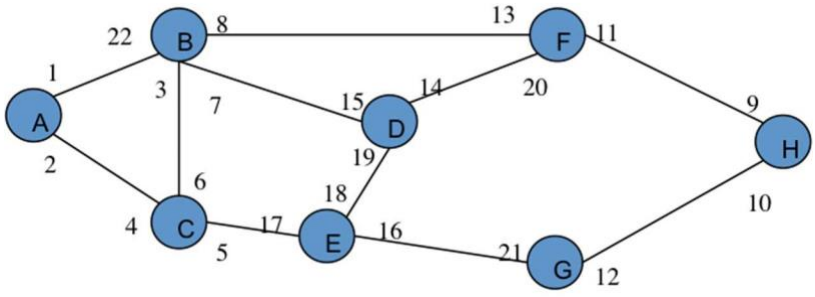


Figure 19: graphe de connectivité d'un DIF, avec des adresses affectées aux ports N-1

La première différence notable est que les tables N-hop sont beaucoup plus grandes, car il y a beaucoup plus d'adresses (un pour chaque port N-1 au lieu d'un par IPCP). Cela en soi est un problème, mais pas le plus grand. Si « A » envoie des paquets à « H », les paquets du réseau ne reflètent pas la situation plus. adresses source et de destination dans les paquets transporteront l'adresse d'un des ports N-1 des PCIP sources / destination; cet exemple suppose qu'il est « 1 » et « 9 ». Si le lien entre « 1 » et « 9 » échoue (comme avant), « F » et « H » détectera cette situation et d'émettre une mise à jour de routage, ce qui provoquera la prochaine hop et tables expédition à recalculée. Mais les paquets qui étaient en transit sont adressées à « 9 », ce qui est plus disponible. hop suivant et tables expédition ne sont pas suffisamment d'informations pour savoir que l'adresse « 10 » apporte des paquets au même endroit que l'adresse « 9 », donc les paquets seront supprimés, même si il y a un chemin viable pour ipcp « H ». Qui plus est, le nœud « A » doit être informé que l'adresse de destination « 9 » n'est plus accessible, et qu'il devrait être en utilisant l'adresse « 10 » comme adresse de destination au lieu.

Il est important de noter tous les problèmes qu'un tel petit changement a créé, ce qui nécessite 3 à 4 fois plus d'adresses, next-hop plus grand et tables transitaires, des protocoles supplémentaires pour détecter les adresses échouées de PCIP multirésidents et utiliser les alternatives, et plus taux de perte de paquets en cas de défaillance dans PCIP multirésidents se produisent.

	Next Hop							
Destination Address	A	B	C	D	E	F	G	H
1	-	1	3	7	19	14	16	11
2	-	1	2	18	17	14	16	12
3	22	-	3	18	17	14	16	12
4	4	1	-	7	19	14	10	11
5	4	6	-	18	17	14	16	12
6	22	6	-	18	7	14	10	11
7	4	-	17	7	7	14	16	11
8	4	-	3	14	19	13	10	11
9	22	15	17	14	19	9	16	-
10	4	6	17	18	21	14	10	-
11	4	6	17	18	21	-	10	11
12	22	6	17	14	19	9	-	12
13	22	15	17	7	17	-	16	12
14	22	13	17	-	21	14	10	11
15	22	15	3	-	17	14	16	11
16	4	15	17	14	-	9	16	12
17	4	6	17	7	-	14	10	11
18	4	15	2	18	-	9	10	11
19	4	6	17	-	19	9	16	12
20	22	15	17	20	19	-	16	12
21	4	6	17	18	21	14	-	11
22	22	-	2	18	17	14	16	12

Figure 20: Tableau suivant-hop (adresses affectées aux ports N-1)

7.3 Conséquences pour renumérotation

La plupart des réseaux réels doivent être éventuellement renuméroté [I.14]: un sous-ensemble ou toutes les adresses attribuées à des entités du réseau doivent être mis à jour. Il peut arriver que le réseau a augmenté au point que son plan d'adressage actuel est plus efficace ou n'échelle. Ou peut-être le réseau est en train de changer les fournisseurs en amont et en a besoin d'obtenir de nouvelles adresses du nouveau fournisseur (adresses basé sur le fournisseur sont la norme dans l'Internet actuel), ou il y a eu une fusion d'entreprise de deux fournisseurs de réseau (et donc leurs réseaux) Quels que soient la raison, la renumérotation dans les réseaux IP est une procédure complexe impliquant un certain nombre d'étapes: les adresses IP doivent être attribuées aux interfaces des commutateurs et des routeurs, des informations de routage doit se propager, d'entrée et de filtres évacuation doivent être mis à jour - ainsi que les pare-feu et les listes de contrôle d'accès, les hôtes obtenir de nouvelles adresses et les entrées DNS doivent être mis à jour.

Une vue d'ensemble des problèmes liés à la renumérotation des réseaux IP est fournie dans [I.15]. Étant donné que les connexions TCP et UDP sont étroitement liés à une paire d'adresses IP, en changeant l'un d'eux détruira le flux. Étant donné que DNS est un annuaire externe - ne fait pas partie des couches de réseau - le processus de renumérotation conduit généralement à des entrées DNS obsolètes pointant vers les adresses désapprouvées. Pire encore, les applications peuvent fonctionner grâce à l'utilisation directe des adresses IP, ce qui nécessitera une mise à jour du code d'application, sa configuration ou les deux. Router renumérotation nécessite généralement une procédure manuelle exhaustive et sujette aux erreurs de mise à jour plan de contrôle des listes de contrôle d'accès ou des règles de pare-feu. De plus, les adresses IP statiques sont généralement intégrés dans de nombreux fichiers de configuration et les bases de données de gestion de réseau[I.16].

La plupart, sinon tous les problèmes décrits sont enracinés dans la désignation incomplète et architecture d'adressage des réseaux IP. Contrairement au schéma présenté à l'article 7.1, dans le monde IP, il n'y a pas de noms d'applications - noms de domaine sont des synonymes pour les adresses IP résolues en dehors de la couche réseau - et de bout en bout des flux de communication sont créés entre les extrémités de la couche de transport identifiés par une adresse IP adresse et un numéro de port de transport. Si les demandes de débit au réseau étaient basés sur les noms d'application et le réseau interne résolu ces noms aux adresses réseau renumérotation alors serait complètement transparent pour les applications.

Les problèmes de pare-feu, et ACLs qui utilisent des règles basées sur les adresses IP, ont une origine similaire. Depuis l'adresse IP est à la fois l'identité des machines de protocole (nœuds) dans la couche IP et aussi le nom utilisé pour la transmission des paquets IP, il y a un problème si le réseau est renuméroté: ACL et des règles de pare-feu doivent être mis à jour pour refléter la nouvelle attribution d'adresse. Parer le fait que dans les architectures bien formés pare-feu ne sont pas nécessaires[I.17], le problème peut être généralisé à celui de la définition des règles de contrôle d'accès dans la couche IP. Il y a clairement un besoin d'un nom stable, indépendant du lieu qui identifie le noeud (machine de protocole) dans la couche, et un autre nom en fonction de l'emplacement qui est utilisé pour la transmission des paquets entre les machines de protocole (les adresses). Dans ces règles de contrôle d'accès des scénarios peuvent être écrits en fonction des noms indépendants LOCATION-; si les adresses changent les règles de contrôle d'accès ne doivent pas être mis à jour. Des considérations similaires sont applicables aux problèmes liés à la gestion: si le système géré est identifié par un emplacement nom de l'application indépendante (gestion), tous les problèmes liés à Ståle adresses dans les fichiers de configuration et les bases de données de gestion de réseau sont tout simplement éviter.

Les paragraphes suivants analysent si renumérotation peut causer des problèmes dans un réseau qui est conforme à l'architecture RINA.Figure 21 illustre la procédure d'enregistrement de l'application et de répartition de flux réalisés par un DIF formé par des procédés CIP (cercles oranges).

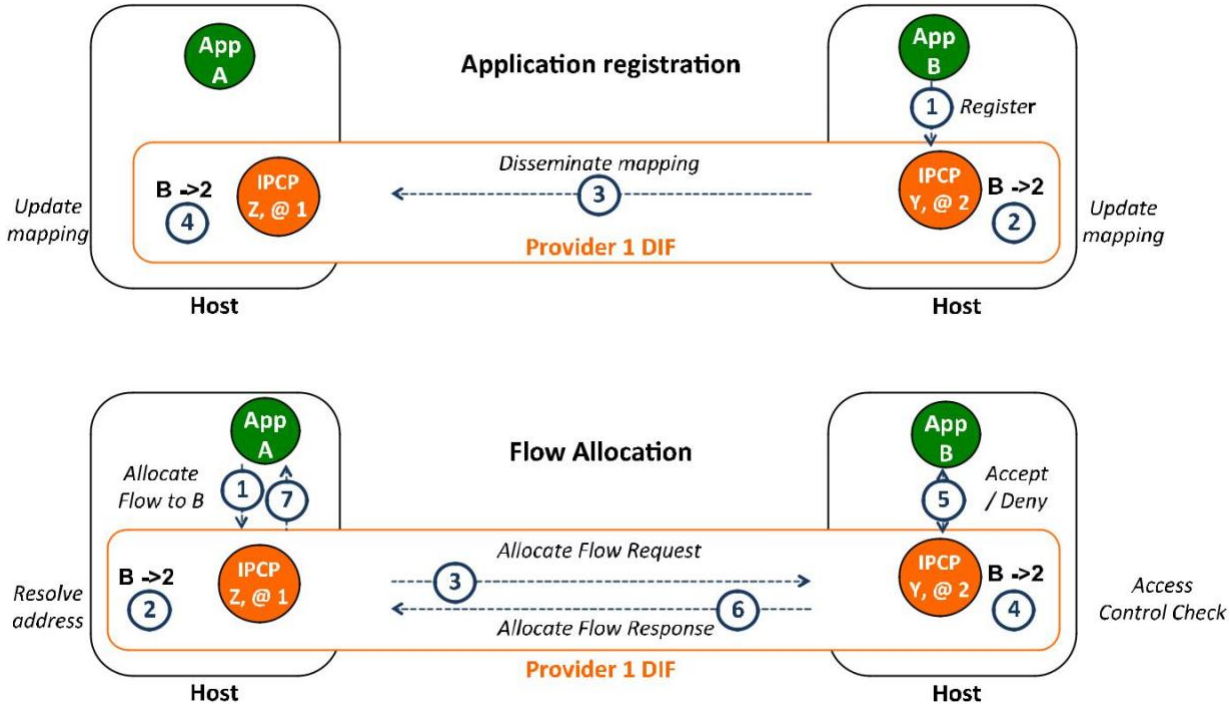


Figure 21: Enregistrement de l'application et le flux des procédures d'attribution

Processus de demande (AP) nommé "B" enregistre au DIF orange. Procédé IPC « Y » est le représentant DIF au niveau du système où AP « B » est en cours d'exécution. Dès réception de la demande d'enregistrement du IPCP met à jour sa carte d'annuaire interne et diffuse les nouvelles informations d'inscription par le DIF. Finalement IPCP « Z » apprend cette information et met à jour sa carte d'annuaire interne. Notez que les procédures de maintenance du répertoire distribué dans le sont une politique DIF: ils changent de DIF DIF, en fonction de son environnement opérationnel (celui illustré dans cet exemple est gardé très simple pour un souci de clarté).

Lorsqu'un AP veut communiquer à un autre, il demande l'attribution d'un flux de communication à l'AP de destination, juste fournir son nom. Le IPCP local qui traite la demande interroge le répertoire pour résoudre le DIF adresse du IPCP par lequel la destination AP est accessible, et transmet la demande d'allocation de débit au IPCP résolu. Le IPCP destination effectue une vérification de contrôle d'accès et informe l'AP local, qui a le dernier mot pour accepter ou rejeter le flux. Un exemple de cette procédure est montré dans la partie inférieure deFigure 21.

Notez que dans toute cette procédure, les adresses des IPCP ne sont jamais exposés en dehors du DIF, par conséquent, si les adresses changent la possibilité de créer de nouveaux flux ne soit pas compromise et l'identité des flux anciens ne sont pas perdues. De plus, étant donné que les applications sont également DIF distribués - et PCIP ne sont que des processus d'application - les problèmes de nommage de PCIP à chaque sont également résolus DIF. PCIP ont un nom AP emplacement stable et indépendant qui utilisent leur identité, alors qu'ils ont également un ou plusieurs synonymes temporaires en fonction de la localisation (adresses) qui sont utilisés pour la transmission des paquets de protocole de transfert de données générique du DIF. Les adresses sont temporaires par la conception, donc renumérotation est seulement une partie du cycle de vie normal du DIF.

La gestion du réseau est une application distribuée, avec des instances de processus d'application jouant le rôle de « gestionnaires » et d'autres instances d'application qui jouent le rôle des « agents de gestion ». A ce titre, ils ont tous les noms d'applications emplacement indépendant, qui sont ceux utilisés pour établir les flux entre les gestionnaires et les agents (ou entre les agents de gestion) de gestion. Par conséquent, étant donné que les adresses de PCIP ne sont jamais utilisés pour communiquer avec un système géré, renumérotation ne peut causer des problèmes.[I.18] discute la procédure renumérotation en RINA en profondeur, fournissant des résultats expérimentaux sur la renumérotation de plusieurs DIF en même temps.

7.4 Conséquences pour la mobilité

Quel est le problème fondamental de la gestion de la mobilité? Les applications dans les appareils mobiles doivent être en mesure de continuer à envoyer et recevoir des données à travers le réseau, même si elles ne cessent de changer leurs points d'attache au réseau comme ils se déplacent (l'exigence de continuité de service). La dégradation de la qualité du service (perte de paquets, retard) perçue par l'application alors que le dispositif mobile change son point de connexion physique (la procédure de transfert) devrait également être réduite au minimum.

Une bonne solution de gestion de la mobilité nécessite au moins deux ensembles d'identifiants:

a) Les noms d'application qui ne changent pas les mouvements hôtes mobiles, de sorte que les paramètres de communication ont des identités stables, quel que soit leur emplacement; et

b) les adresses qui changent que l'hôte se déplace, pour tenir compte de la position du dispositif dans le réseau et permettent le routage à l'échelle.

Le problème fondamental de la gestion de la mobilité dans l'Internet est que le seul identifiant attribué à une entité dans un hôte mobile (MH) qui a une portée plus grande que le système lui-même est l'adresse IP. Par conséquent, il y a un conflit: un identifiant unique ne peut pas satisfaire à la fois les propriétés en même temps.

Il n'y a pas de noms d'application emplacement indépendant dans l'architecture Internet actuelle. paramètres de communication sont identifiés par la concaténation de l'adresse IP et un port de transport local. Si l'adresse IP change, l'identité du point de terminaison de communication est perdue et les ruptures de flux de communication. Les noms de domaine sont des macros pour les adresses IP.
Les noms de domaine ne sont pas utilisés pour le routage, et ne satisfont pas aux propriétés énoncées au paragraphe précédent que les modifications au nom DNS ne le font pas (et ne peuvent pas en général) se propagent aux utilisateurs d'une adresse IP si le mappage DNS est modifié pour faire référence à un une adresse IP différente.

Par conséquent, l'adresse IP ne peut pas changer, mais l'emplacement de l'appareil ne; Par conséquent, l'infrastructure de routage doit être conscient des adresses IP qui sont mobiles. Si rien n'a été fait, alors chaque routeur qui pourrait voir une adresse MH devrait avoir une entrée de table de routage distincte pour cette adresse, car il ne serait pas agrégeable une fois que le MH quitte la zone de la maison où l'adresse a été assignée. En outre, les mises à jour de routage devraient être assez souvent et propagée à travers l'ensemble de l'infrastructure de routage IP plus rapide que le taux de variation des points de fixation. Cela n'échelle et plusieurs solutions ont été proposées pour atténuer ce problème. De telles solutions de gestion de la mobilité ont été classés en deux groupes:

a) des solutions qui fonctionnent à la couche IP;

b) solutions qui masquent la mobilité de la couche IP.

solutions de type II gérer la mobilité à couches inférieures entre l'appareil mobile et une passerelle mobile, créant essentiellement un grand sous-réseau IP qui ressemble à une couche fixe du point de la couche IP de vue. Les systèmes cellulaires tels que LTE (Long Term Evolution), gérer la mobilité par la mise en place et au démontage des tunnels entre le MH (appelé équipement de l'utilisateur en termes cellulaires) et les passerelles mobiles qui fournissent la connectivité à Internet ou à des réseaux IP privés. Les tunnels doivent être recréée chaque fois que le MH attache à un point d'accès différent, encourir les frais généraux importants. Si le MH passe d'un fournisseur de réseau mobile à l'autre, la continuité du service est perdue (puisque le MH se voit attribuer une adresse IP d'un autre fournisseur).

Type I solutions, solutions de mobilité IP étiquetés, fournissent le degré de soutien différent à la mobilité via des protocoles qui fonctionnent à la couche IP. Il existe trois principales approches pour faire la Mobilité IP: Mobile IPv4 (MIPv4)[I.19], Mobile IPv6 (MIPv6)[I.20], et Proxy Mobile IPv6 (MIPv6) [I.21]. ZÉZAYER [I.22], le protocole de séparation identificateur de localisation, a été récemment proposé comme solution de mobilité IP. Vous trouverez une analyse de ces protocoles[I.23].

Presque toutes les solutions de gestion de la mobilité IP nécessitent l'utilisation de tunnels pour gérer la mobilité. Les tunnels nécessitent l'ajout d'entrées de la table de transfert dédiées par hôte mobile, ainsi qu'un protocole pour signaler leur création, la modification et la destruction. ancres de mobilité centralisée comme dans PMIPv6 provoquent des points uniques de défaillance et nécessitent des ressources importantes au niveau des noeuds d'ancrage, étant donné que beaucoup de trafic doit être transmis à travers eux. LISP n'est pas capable de faire face à la mobilité des hôtes à la superposition couche IP, et engage des frais généraux plus importants pour faire face à la mobilité que les réseaux basés sur RINA faire[I.24].

La solution analysée dans une [I.23] qui ne nécessite pas des tunnels pour faire face à la mobilité (entièrement mis en déroute par BGP) a deux problèmes principaux:

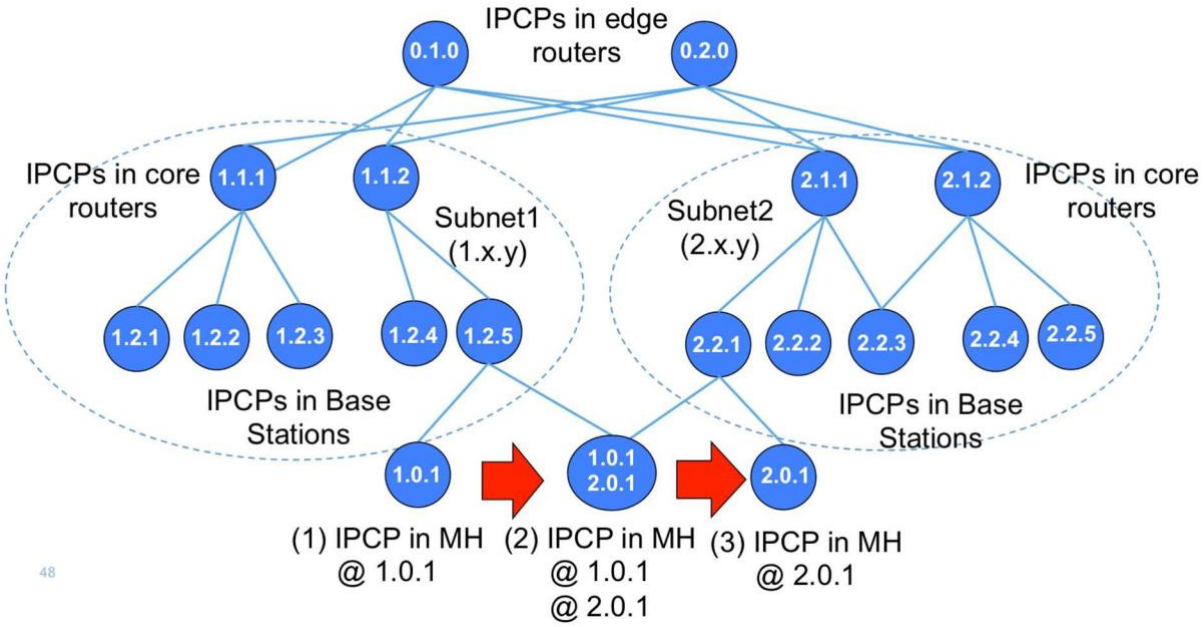
a) puisque la portée de la couche réseau est la convergence globale de routage est trop lent; et

b) étant donné que l'adresse IP de l'hôte mobile ne change pas, en tête de routage est élevée et contribue à de nouvelles augmentations de la taille des tables d'acheminement de suivi des nœuds mobiles.

La gestion fondamentale de la mobilité de la raison est si complexe est l'absence d'un ensemble complet d'adressage. Il n'y a rien à tenir, mais l'adresse IP. Un autre problème avec toutes ces propositions est qu'elles traitent simplement la mobilité des cas d'utilisation spécifiques. Ils ont besoin de mécanismes supplémentaires considérables et les protocoles qui nécessitent des mécanismes de sécurité supplémentaires, et ont pas d'autres avantages.

En revanche, pour un réseau qui utilise la dénomination et schéma d'adressage proposé à l'article 7.1, la mobilité est rien de plus que multihoming où les points de fixation changent un peu plus souvent. Article 7.2 décrit comment le soutien pour multihoming ne nécessite pas de protocoles spéciaux, il est réalisé en raison de la structure de nommage. Les paragraphes qui suivent une brève analyse de la façon dont la mobilité est réalisée dans les réseaux intégrés à l'architecture RINA.

Adresses localiser l'hôte mobile (MH). Au sein d'un DIF, chaque IPCP se voit attribuer une adresse qui est l'emplacement dépendant, structuré de manière à refléter l'emplacement du IPCP par rapport aux autres entités de son DIF. Si le MH, qui contient ce IPCP, se déplace trop loin (par exemple attache à une station de base dans un autre sous-réseau) l'adresse ne sera plus agrégeable entraînant une augmentation de la taille de la table de routage routeur et potentiellement moins efficace. Cela signifie que l'adresse IPCP dans le MH doit changer pour maintenir la taille de la table de routeur gérable et efficace (ces changements d'adresse ne se produira pas à chaque changement de station de base, que lorsque le MH entre un sous-réseau différent au sein du DIF).



REMARQUE: Le MH IPCP obtient une nouvelle adresse lorsque attache à la BS IPCP. Pendant une brève période de temps, le MH IPCP est multihébergement deux BS PCIP.

Figure 22: PCIP dans un MH faisant un transfert entre les stations de base (BS) de différents sous-réseaux

La procédure de mise à jour des adresses en RINA DIF est discuté dans l'article précédent, montrant que cela peut être fait en temps réel, sans impact sur les flux fournis par le DIF (continuité du service et la qualité de service sont conservés). Par conséquent, lorsqu'un IPCP dans un MH attache à une entité d'une nouvelle station de base dans un autre sous-réseau - comme cela est représenté dansFigure 22, il obtiendra une nouvelle adresse - et l'ancien cessera d'être annoncé et disparaître. La nouvelle adresse sera diffusée via le système de routage, et les mises à jour du répertoire modifiera les noms d'applications de couche supérieure nécessaires pour répondre consolidations. Toutes ces procédures font déjà partie de l'architecture et ne nécessitent aucun ajout pour gérer des scénarios de mobilité.

La sensibilité au changement de l'emplacement.Étant donné que les changements d'adresse déclenchent le routage et parfois des mises à jour de l'annuaire (uniquement si le IPCP qui a changé les adresses a des applications de serveur enregistrées), ces mises à jour doivent être assez rapide (par rapport au taux et le nombre d'événements de transfert) pour permettre au DIF de converger et atteindre un état de fonctionnement stable. Cela met une limite sur la portée et la taille du DIF, qui doit être correctement conçu pour fonctionner efficacement. Ceci est un problème similaire à celui connu par la gestion de la mobilité distribuée (DMM) solution entièrement routé, avec la différence essentielle que les concepteurs de réseau RINA peuvent décider du nombre et la portée de réseau dans le DIF.

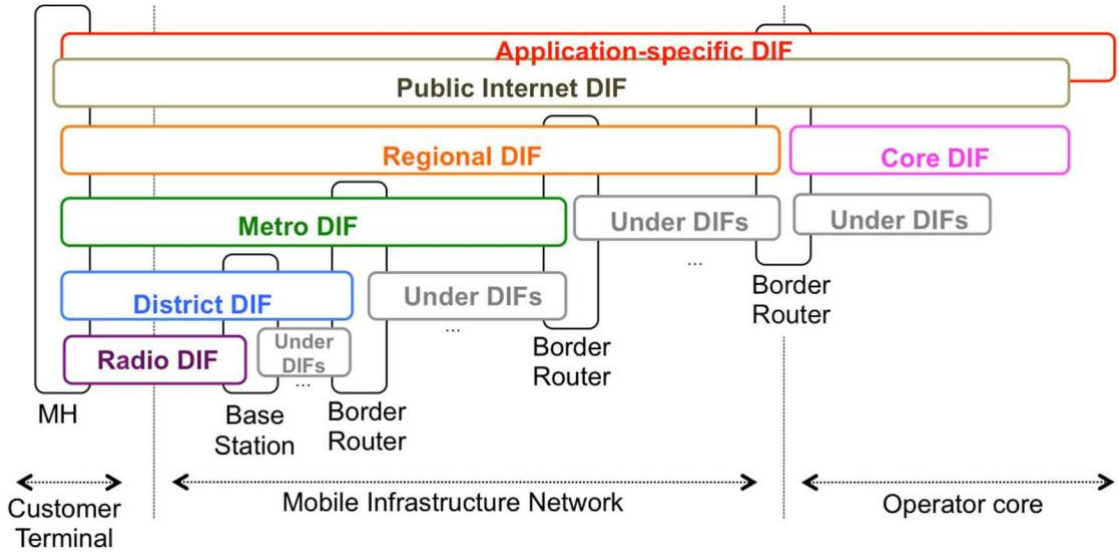


Figure 23: Réseau mobile partitionné en plusieurs DIFS de portée de plus en plus

Comme on le voit dans Figure 23, les réseaux mobiles peuvent avoir de multiples possibilités de plus en plus DIF. La baisse géreront les événements DIF de mobilité fréquentes pour un nombre plus faible d'hôtes mobiles, sur une portée réduite (par exemple, un quartier dans une ville). La hausse ne sera DIF au courant des transferts entre les points d'accès appartenant à des plus bas DIF, ils devront donc faire face aux événements de mobilité moins fréquents et peuvent avoir une plus grande portée. Cette structure peut être mise à profit par le concepteur du réseau à l'échelle le réseau et limiter la taille des tables de routage et taux d'événements de mobilité à chaque DIF.

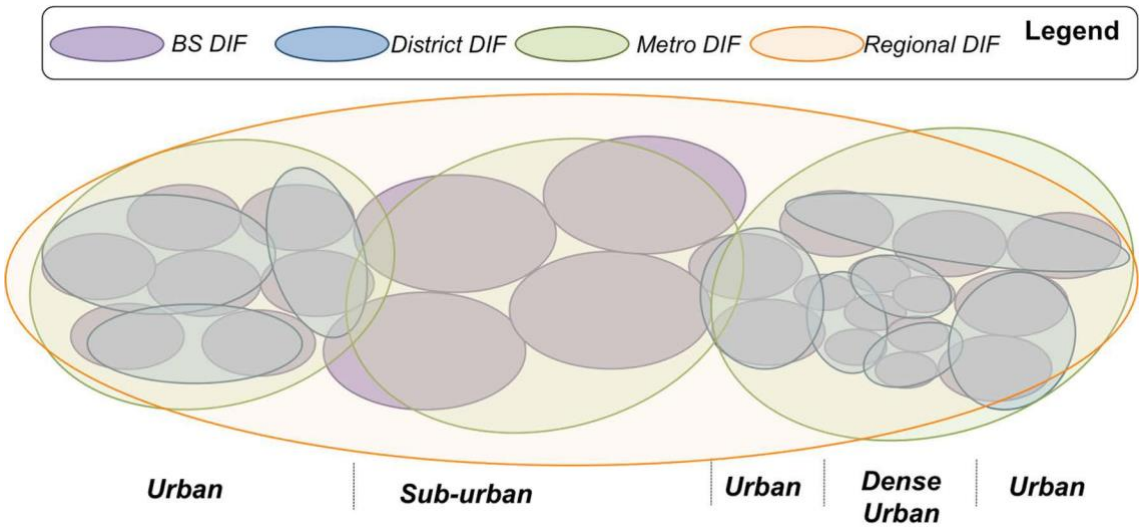


Figure 24: Réseau mobile en vue de dessus, avec DIF représentés par des cercles

De plus, le nombre de DIF n'a pas besoin d'être la même dans l'ensemble du réseau. Par exemple, les zones urbaines à forte densité d'utilisateurs bénéficieront d'un plus grand nombre de ceux que rurales DIF, comme le montreFigure 24. Last but not least, l'opérateur peut créer de façon dynamique DIF plus ou moins dans les différentes régions du réseau en fonction de ses besoins et de la demande pour les ressources réseau: par exemple, il peut créer une structure ad hoc du DIF à regrouper tous les hôtes mobiles des personnes présentes un concert, pour fournir une capacité suffisante et cacher leurs événements de mobilité d'autres parties du réseau.

Ajouter plus de DIF augmente le surdébit d'en-tête, mais puisque chaque DIF a les mêmes protocoles et la présence et la longueur des champs d'en-tête de protocole (par exemple les adresses) peut être adapté aux exigences de chaque DIF, la surcharge de l'ajout d'un DIF peut être minimisé par rapport à la situation actuelle dans laquelle toutes les couches sont différentes. En outre, la mise à une seule couche horizontalement introduit également en tête (longueur des champs d'en-tête de protocole sera plus grande, les mécanismes de protocole deviennent plus complexes) et rend plus difficile à l'échelle (comme le montre l'exemple de solution entièrement routé DMM).

***la continuité et la dégradation QoS service*.**Les mêmes flux sont en place à travers toute la durée de la connexion de l'application, les événements de mobilité ne perturbent pas les flux existants puisque les noms d'application sont stables et l'emplacement indépendant. Il n'y a pas de tunnels pour mettre en place et le démontage. La qualité de service expérimenté par les applications ne se dégradent par le retard de transfert, la perte de paquets ne peut se produire s'il n'y avait pas de communication physique avec le réseau.

***gérabilité*.**Les noms d'applications ne changent jamais. Le mappage du nom de l'application à adresse (N) et de (N) - Adresses à (N-1) -Adresses est assurée par l'ingénierie de la portée des DIF pour garantir le temps de mise à jour est faible par rapport à la vitesse de variation de (N-1) -Adresses. Gestion de la mobilité ne nécessite pas de procédures supplémentaires qui ne sont pas déjà présentes dans d'autres types de réseaux (inscription, routage, répertoires, mises à jour d'adresses).

***évolutivité*.**Les concepteurs de réseau ne sont pas limités à l'utilisation d'un seul DIF, ils peuvent évoluer son réseau à la fois horizontalement (en créant de plus grandes DIF) et verticalement (en créant plus en plus DIF de l'autre). Le nombre de DIF dans un réseau mobile devient une question de conception de réseau - pas décidé et gelé dans les normes - donc il peut être adapté et optimisé de façon dynamique alors que le réseau est en cours d'exécution.

7.5 Résumé des propriétés architecturales RINA pertinentes pour le nommage, l'adressage et le routage

Cette clause résume la façon dont RINA aborde les questions identifiées dans les clauses 4.3.3 et 4.3.4:

- **dénomination complète et architecture d'adressage.** RINA utilise une dénomination complète et le traitement complémentaire. Les processus d'application ont des noms indépendants de l'emplacement, qui les identifient de manière unique dans un certain espace de noms. Les points d'accès peuvent également avoir des synonymes qui facilitent certaines tâches dans les applications distribuées dont ils sont membres. Au sein d'un DIF, les processus (IPC qui sont juste une forme de points d'accès) obtenir des adresses affectées, qui sont des noms en fonction de l'emplacement qui facilitent la transmission PDUs. Les adresses ne sont jamais exposées à l'extérieur d'un DIF, sa gestion est maintenue complètement interne au DIF. Lorsqu'un registres d'application à un DIF, un répertoire cartes son nom de l'application à l'adresse du processus CIB, il est attaché. Si l'application change de point de fixation au DIF, la cartographie (qui est interne au DIF) est mis à jour, mais le nom de l'application ne change pas. Le routage au sein d'un DIF est un processus en deux étapes: tout d'abord une voie en termes d'adresses de processus IPC est calculé; puis, pour chaque adresse de saut suivant, un chemin d'accès approprié pour le saut suivant est choisi (le chemin d'accès est identifié par le port-id de l'écoulement N-1 vers le processus IPC). Le choix de la voie peut être tirée par l'allocation des ressources (par exemple d'équilibrage de charge), la résilience ou d'autres exigences.

- **Adresses attribuées à des noeuds à chaque DIF.** Le noeud dans une couche est la machine de protocole qui retire l'en-tête de ce protocole dans cette couche. Les processus IPC sont les nœuds du DIF, et par conséquent les entités abordées (par opposition aux « points de fixation aux couches de niveau inférieur comme recommandé par l'architecture d'adressage IPv6[I.13]). Cette règle simple permet un processus IPC d'avoir une adresse unique quelle que soit la façon de l'atteindre (les adresses sont voie indépendante), ce qui rend multi-homing trivial et réduisant au minimum le nombre d'adresses présentes dans la table de transfert.

- **Les réseaux peuvent être en toute transparence renumérotés.**Les adresses ne sont que temporaires synonymes de processus internes IPC à chaque DIF, les processus IPC peuvent être dynamiquement et automatiquement renumérotés sans impact sur les services qu'ils offrent aux supérieurs DIF. renumérotation dynamique transparente peut être réalisé parce que l'adresse d'un processus IPC ne tient pas compte de son identité, et aussi parce que les adresses ne sont pas exposée à l'extérieur d'un DIF. Cette fonction facilite non seulement la gestion du cycle de vie d'un réseau (plan d'adressage de chacun peut évoluer en DIF les besoins

du changement de DIF), mais réduit également la taille des tables expédition dans les réseaux où se déplacent les processus IPC.

- **Attribution de noms permet la découverte de DIF application sur DIF.** Non seulement chaque processus d'application ont des noms, mais aussi la pleine application distribuée. Étant donné que les applications ne sont que DIF distribués, ils ont des noms attribués également. Il est donc possible de suivre les applications disponibles par le biais qui sur un ensemble DIF de interfonctionnement des réseaux RINA. La fonction qui gère dynamiquement cette cartographie est appelée DIF allocateur, et permet à un processus de découverte DIF autonome. Les applications peuvent être disponibles via plusieurs DIF, le DIF Allocataire permet la découverte dynamique du DIF optimale pour atteindre une application de destination (où optimale peut être une fonction de la latence, la fiabilité, etc.), au cas par cas.

- **Multi-homing réalisée en raison de la structure.** Multi-homing est pris en charge au niveau du processus IPC sans avoir besoin de protocoles spécialisés, comme une conséquence de la désignation d'un schéma d'adressage. Depuis PCIP sont assignés des adresses lieu-dépendante et indépendante de la route, la liaison de destination l'adresse du processus IPC à l'écoulement du N-1 est une décision de transmission qui est prise par les voisins les plus proches de l'IPCP. Si un certain chemin (N-1 flux) à un IPCP échoue, cette cartographie doit être recalculée voisins les plus proches (soit par re-routage, ou par le passage à un autre chemin si multiples sont disponibles, etc.) L'adresse de destination le IPCP avec le chemin échoué ne change donc pas PDUs en vol peut être réacheminé et ne sont pas perdus.

- **Mobilité atteint en raison de la structure.**La mobilité dans RINA peut être vu multi-homing comme dynamique des défaillances attendues. Lorsqu'un processus IPC dans un bouge DIFF, il obtient de nouveaux points d'attachement et laisse tomber sans plus les valides. Tant que l'adresse IPCP est toujours valide (représente correctement l'emplacement du IPCP dans une abstraction du graphique du DIF), la mobilité déclenche simplement des mises à jour de routage: aucun tunnel doivent être mis en place. Si le IPCP a déménagé loin, il est renuméroté en suivant les procédures normales. Dans tous les résultats dans une approche beaucoup plus simple et générique de la mobilité, qui maintient constante quelle que soit la couche et la technologie sous-jacente utilisée.

8 QoS, allocation des ressources et le contrôle de la congestion

8.1 modèle cohérent de QoS dans les couches

Même si tous fournissent le même DIF type de service, les caractéristiques du service offert varie entre DIF. Chaque DIF définit un ensemble de cubes de qualité de service pris en charge, à savoir les classes de qualité de service pour les flux fournissant des limites statistiques sur les indicateurs tels que le taux de données, la latence, pertes, etc. Compte tenu de ces QoS cubes, les applications et DIF supérieures peuvent demander des flux avec des besoins spécifiques, et le DIF, puis fournit un flux avec la QoS Cube qui correspond à ces exigences, en utilisant les politiques (planification, routage, etc.) le mieux adapté à son but. Étant donné que tous DIF offrent la même interface de service, RINA dispose d'un modèle cohérent de qualité de service de l'application vers le bas pour les couches physiques, dont les exigences de qualité de service font partie des méta-données transmises au DIF dans chaque demande d'allocation de flux, comme illustré dansFigure 25. Niveau supérieur DIF demande flux avec une certaine qualité de service à bas niveau DIF, jusqu'à ce que le support physique soit atteinte.

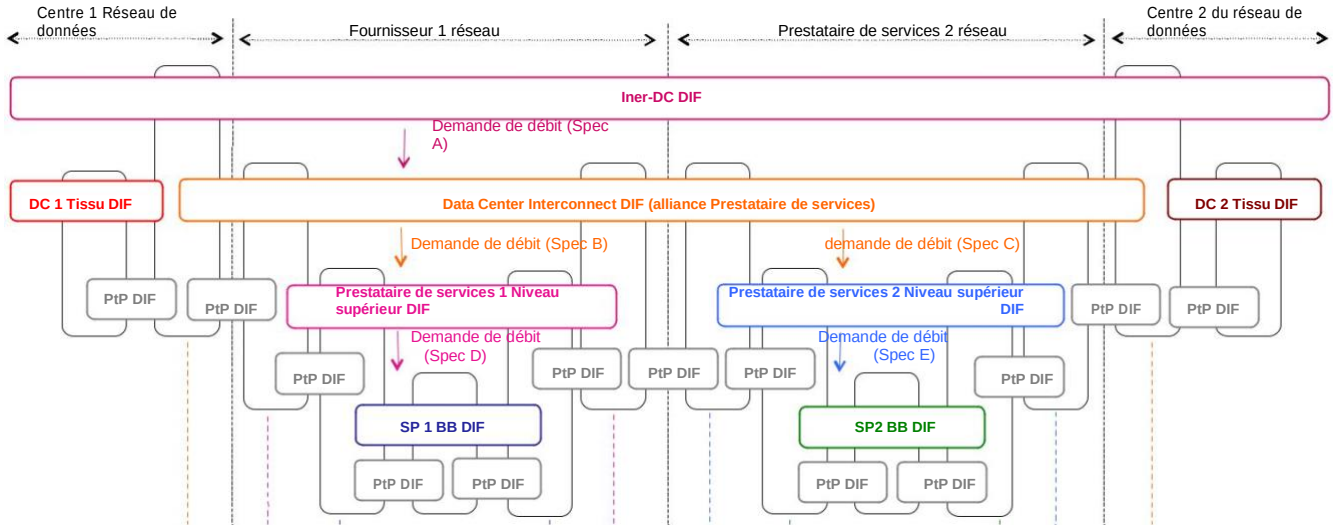


Figure 25: Modèle de QoS Conformément à l'application vers le bas aux couches physiques

Par conséquent, l'une des principales tâches lors de la conception d'un DIF est de décider quel cubes de qualité de service, il soutiendra. Le terme cube de QoS provient de la modélisation de l'espace de représentation comme un ensemble de N paramètres indépendants dont les valeurs peuvent varier entre certaines limites. En utilisant plusieurs axes, un espace de représentation à N dimensions peut être définie. cubes de qualité de service définissent une région dans l'espace de représentation, supportant un sous-ensemble spécifique de paramètres à une gamme limitée. Voici quelques exemples de cubes de qualité de service pourraient être les suivantes:

- Pas de perte avec dans l'ordre de livraison des données, pas de limites sur le retard, pas de limites sur la charge acceptée (équivalent à TCP dans l'Internet).
- Aucune limite sur le retard, la perte et la charge acceptée (équivalent à UDP dans l'Internet).
- 5 ms retard et 0,00001 probabilité de perte de 95% des paquets, 15 ms retard et 0,0001 probabilité de perte de paquets de 99,999%, pour une charge maximale admise de 10 Mbps.

Lorsqu'un reçoit la demande DIF d'allocation de débit, il vérifiez les paramètres de qualité de service dans la demande flux allouer et mappe le flux à l'un des cubes de qualité de service disponible dans le DIF. Chaque cube de QoS a un ensemble de politiques associées qui ont été conçus pour respecter les gammes supportées par le cube. Ces politiques portent principalement sur le contrôle de flux, le routage, la transmission, la planification et la gestion de la congestion.

Tous les PDUs EFCP qui transportent des données du flux sont marqués avec l'identificateur de cube de QoS, de sorte que les processus intermédiaires IPC peuvent correctement identifier et traiter le trafic de chaque cube de QoS. cubes de qualité de service sont des normes dans un DIF: tous les participants prennent en charge les mêmes DIFF identificateurs de cube de QoS et exécuter un ensemble cohérent de politiques visant à fournir un bout en bout cohérente (au DIF) une expérience de qualité de service.

REMARQUE: En général à flux DIF de couche inférieure (N-1) DIFS agrégées de multiples flux de DIF couche supérieure (N-DIFS), d'où l'une des tâches de la DIF est de cartographier la classe de QoS supporté par le N-écoulement dans l'une des classes de qualité de service offerts par des flux N-1.

Ce modèle QoS applique récursive à chaque DIF. Lorsqu'un IPCP dans un DIF demande une allocation de flux à un autre IPCP, il utilise la même abstraite API de service IPC comme toute autre application, il indique donc un niveau inférieur DIF quel est le nom de l'application, il veut communiquer avec et quels sont les exigences de qualité pour le flux (perte, retard dans la livraison des commandes, etc.). Le niveau inférieur DIF ne sait pas si la requête dans le flux est un DIF ou tout autre type d'application. Il qu'élaborer la demande de débit à l'un des cubes de qualité de service de la N-1 DIF et répartir le flux. Par conséquent cubes QoS définitions sont internes à un DIF, mais la sémantique des paramètres passés à la demande d'écoulement doivent être allouer standard à travers DIF (de sorte que par différents DIF ils sont tous interprétés de la même façon).

8.2 Allocation des ressources

Le problème de l'allocation des ressources dans un DIF consiste à allouer des ressources aux différents flux d'une manière conforme aux exigences des applications et permet également une utilisation efficace des ressources du DIF. Les principales ressources d'un processus IPC qui doivent être affectés aux différents flux sont espace tampon et de la capacité d'ordonnancement. Le DIF repose également sur les ressources allouées aux flux N-1 fournis par d'autres DIF.

Plusieurs stratégies d'allocation des ressources s'inscrivent dans ce cadre: les ressources peuvent être allouées aux connexions EFCP individuels au moment de l'établissement du flux (émulant une approche de circuit virtuel), ou peuvent être partagées entre plusieurs connexions EFCP appartenant au même cube de QoS (QoS basée sur les classes), ou peut être même partagé entre toutes les connexions EFCP aussi (pas de différenciation de la qualité de service, une approche purement connexion).

Le modèle permet également hors ligne par rapport à l'allocation des ressources en ligne. Dans l'allocation des ressources hors-ligne a la connaissance DIF du trafic, il doit prendre en charge, et les ressources sont à l'avance. En matière de ressources d'allocation des ressources en ligne sont attribués à la volée, comme de nouveaux flux sont alloués et désallouées par les applications utilisant le DIF. Une combinaison des deux approches est également possible - et sera probablement le cas le plus courant. En utilisant une combinaison des approches du DIF peut effectuer une allocation initiale des ressources en ligne, puis adapter aux conditions en temps réel à l'aide d'exploitation l'allocation des ressources en ligne.

La ressource Allocataire (RA) est la tâche de gestion de couche chargée de la coordination et l'ajustement des politiques d'allocation des ressources au sein du DIF. Il surveille le fonctionnement du processus IPC et fait des ajustements à son fonctionnement pour le maintenir dans la plage de fonctionnement spécifiée. La mesure dans laquelle le fonctionnement de la RA est distribué et réalisé en collaboration avec les autres AR dans les membres du DIF et la mesure dans laquelle la RA recueille simplement et communique des informations à un système de gestion de réseau (NMS), qui détermine la réponse est une question de conception et de recherche de DIF. Le premier cas peut être appelé système nerveux autonome, alors que ce dernier cas est plus l'approche traditionnelle de la gestion du réseau. Les deux approches ont leurs cas d'utilisation et les domaines d'application. L'approche traditionnelle est appropriée lorsque les ressources des membres du DIF sont étroitement limitées, alors que l'approche autonome est plus appropriée lorsque les temps de réaction rapide sont nécessaires. La norme sera quelque part entre les deux et il y a un certain nombre d'architectures intéressantes à explorer. La RA est responsable d'assurer que l'opération de transfert de données au sein du processus IPC reste à l'intérieur (et satisfait) ses besoins opérationnels. Au sein d'une IPCP, la RA a accès aux compteurs suivants et peut régler les cadrans suivants. La RA est responsable d'assurer que l'opération de transfert de données au sein du processus IPC reste à l'intérieur (et satisfait) ses besoins opérationnels. Au sein d'une IPCP, la RA a accès aux compteurs suivants et peut régler les cadrans suivants. La RA est responsable d'assurer que l'opération de transfert de données au sein du processus IPC reste à l'intérieur (et satisfait) ses besoins opérationnels. Au sein d'une IPCP, la RA a accès aux compteurs suivants et peut régler les cadrans suivants.

Il existe essentiellement trois séries d'informations disponibles au processus IPC pour prendre ses décisions:

- Les caractéristiques de la circulation de trafic à destination de l'utilisateur du DIF, à savoir l'application ou le (N + 1) -DIF.
- Les caractéristiques de trafic du trafic arrivant et étant envoyés sur le (N-1), de flux.
- Informations autres membres du DIF sur ce qu'ils observent (cette dernière catégorie pourrait être limitée à seulement voisins les plus proches ou d'un autre sous-ensemble - tous les deux ou trois voisins de houblon - ou les tous les membres du DIF).

Les deux premières catégories seraient généralement des mesures qui sont facilement tirées de l'observation du trafic: la bande passante, le retard, la gigue, PDUs endommagés, etc. Les données partagées pourraient envisager le statut interne des autres processus IPC tels que la longueur de la file d'attente, l'utilisation de la mémoire tampon, et d'autres.

La ressource Allocataire a plusieurs « leviers » et « cadrans » qui peut changer d'influer sur la façon dont le trafic est géré:

- **Création / Suppression de QoS Classes.** Les demandes d'allocations de flux spécifient la QoS-cube le trafic nécessite, qui est mis en correspondance avec une qualité de service de classe. La RA peut créer ou supprimer des classes de qualité de service en réponse aux conditions changeantes. (Il convient de noter que les paramètres manipulés sont relativement insensibles et définir des plages plus de points dans l'espace).
- **QoS de transfert de données Définit.** Lorsqu'une demande Allouer certains paramètres de qualité de service, ceux-ci sont convertis en une qualité de service de classe qui à son tour se traduit par un ensemble de politiques de transfert de données, une qualité de service de classe ensemble. Le RA peut modifier la qualité de service de classe utilisé ensemble. Par exemple, on pourrait imaginer un autre ensemble de politiques pour la même classe de qualité de service dans différentes conditions de charge.
- **Modification de transfert de données des paramètres politiques.** On suppose que certaines politiques de transfert de données peuvent permettre à certains paramètres à modifier sans modifier la politique en vigueur. Un exemple trivial pourrait changer la politique de contrôle de retransmission de Acking chaque seconde PDU à Acking chaque troisième PDU.
- **Création / Suppression de Queues RMT.** Les flux de transfert de données sont mappés sur les files d'attente relais et de multiplexage pour envoyer au (N-1) -DIF. Le RA peut contrôler ces files d'attente ainsi que les classes de qualité de service sont mis en correspondance avec les files d'attente. (La décision ne doit pas exclusivement en fonction de la qualité de service de classe, mais peut aussi dépendre des adresses ou courant de charge, etc.).
- **Modifier RMT File d'attente d'entretien.** La PR peut changer la discipline utilisée pour les files d'attente RMT.
- **Création / Suppression de (N-1), de flux.** La RA est responsable de la gestion des flux distincts de différentes QS-classes avec les (N-1) -DIF. Étant donné que le multiplexage se produit dans un DIF ne serait pas attendre les (N) -QoS classes à exactement les mêmes que les (N-1) -QoS classes. La PR peut demander la création et la suppression des flux N-1 avec les plus proches voisins, en fonction de la charge de trafic offert au processus IPC et d'autres conditions du DIF.

8.3 Contrôle de congestion

La façon RINA contrôle la congestion est une généralisation de la façon dont cela est fait dans l'Internet: s'il n'y a qu'un seul contrôle de la faire DIF la congestion dans le réseau, il fonctionne de manière de bout en bout. Si deux ou plusieurs contrôle de congestion DIF sont concaténés, la boucle de commande de bout en bout est divisé en boucles plus courtes. Contrôle de congestion dans RINA « naturellement » présente des propriétés de diverses améliorations qui ont été apportées (ou au moins proposé pour) Internet sans hériter des problèmes qui viennent d'imposer ces mécanismes sur une architecture qui n'a pas été fait pour eux (tous les problèmes que la performance Améliorer proxies (PEP) ont)[I.52].

PEP cassent généralement des connexions de bout en bout en plusieurs connexions en boucle fermée; à chaque connexion, un système de contrôle de la congestion qui tient compte des caractéristiques de liaison locale peut être exploitée. Internet PEPs présentent plusieurs inconvénients. En plus du problème de la fiabilité (ils cassent la sémantique de bout en bout de la connexion de transport), la complexité en utilisant IPSec et TLS surviennent parce que la sécurité est une fonction de bout en bout dans ces cas. PEPs aussi n'échelle pas bien avec le nombre de flux et l'exécution d'une instance de TCP séparé pour chaque flux est coûteux en termes de délai de traitement.

L'architecture en couches de RINA n'a pas ces problèmes de PEPs Internet parce que:

1) la sécurité est une fonction par-DIF: PDUs sont protégés comme ils traversent les frontières DIFF, et parce que chaque a sa propre DIF contrôle de la congestion, les connexions cryptées ne ont pas besoin d'être divisé; et

2) flux vers chaque prochain bond sont agrégées au DIF amoindris, ce qui signifie qu'il y a beaucoup moins de l'état d'entretien.

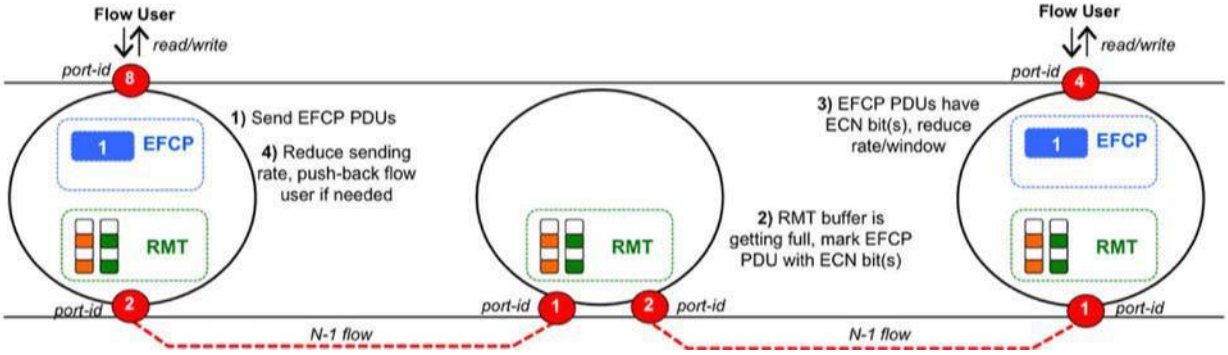


Figure 26: Un exemple illustratif de la façon dont la congestion est gérée dans un DIF

Quand un récepteur d'une connexion EFCP voit une PDU EFCP avec la marque de ECN, il calcule un nouveau taux (réduit) pour l'expéditeur, et signaler cette nouvelle vitesse de la machine à protocole de EFCP envoi en utilisant le mécanisme de commande d'écoulement de la connexion EFCP (Alternativement, il peut l'écho des informations à l'expéditeur de EFCP, qui fera le calcul du nouveau taux / fenêtre). L'envoi de la machine protocole EFCP réduira le débit d'émission, ce qui provoque également repoussage sur l'utilisateur du flux. Si nécessaire, cette repoussage peut être fait en bloquant l'utilisateur du flux ou de signalisation d'une condition d'erreur lorsqu'un appel API d'écriture est faite.

Une différence importante avec l'Internet est que la congestion peut être géré sur une base de cube QoS par; l'a suffisamment d'informations DIF à adopter différentes politiques de gestion de la congestion pour les différentes clases de qualité de service. Par exemple, en présence de « faible encombrement » seulement le trafic meilleur effort peut être repoussé; si la congestion continue de soulever tout le trafic sauf celui à faible latence est repoussé; etc.

8.4 Résumé des principes de conception RINA pertinents pour la qualité de service, Allocation des ressources et le contrôle de la congestion

Cette clause résume la façon dont RINA aborde les problèmes identifiés à l'article 4.3.5:

- **modèle de QoS cohérente à travers les couches.** Un modèle de service abstrait qui est API indépendant de la technologie et un service cohérent à travers toutes les couches sont les principales propriétés qui permettent RINA de fournir un modèle cohérent de qualité de service à travers DIF. Le rôle de tous est de fournir DIF flux de communication avec des caractéristiques de qualité de service sur une certaine portée. Ces caractéristiques de qualité de service - le service de flux Level Agreement, SLA - liés aux propriétés statistiques du flux, tels que la perte de paquets, le retard, la capacité ainsi que d'autres propriétés comme la livraison des données dans l'ordre. Chaque mappe les exigences DIF de flux à l'une des catégories de services (niveaux de qualité de service), il fournit. Chaque marque les PDUs DIF appartenant à un certain débit avec une qualité de service-id, de sorte que les politiques à chaque IPCP peuvent traiter appartenant à la PDUs même classe de manière cohérente. Les fournisseurs peuvent signaler les exigences de qualité de service à l'autre,

- **boucles de contrôle de congestion à l'aide de ECN à proximité de l'endroit où la congestion se produit.** Chaque a la capacité DIF d'identifier et de gérer la congestion. Un concepteur de réseau peut utiliser cette capacité à réduire le temps de réponse à la congestion et sa variance (ce qui est la clé de réagir contre les échelles de temps appropriées), et limiter les effets de la congestion au DIF (s) où il se produit et aux flux qui en sont la cause. Utilisation des informations ECN dans les en-têtes EFCP PDU assure que les boucles de contrôle réagissent vraiment à la congestion et non à d'autres phénomènes tels que la perte de paquets - « car il peut se produire avec la détection de la congestion implicite des approches largement utilisées aujourd'hui dans l'Internet ».

- **personnalisé par-politiques de contrôle DIF de congestion pour les réseaux hétérogènes.** Étant donné que chaque peut gérer la congestion DIF dans ses propres ressources, les politiques de gestion de la congestion peuvent être adaptés à l'environnement DIF. Le contrôleur utilisé dans un réseau sans fil sera DIF différente de celle d'un réseau à faible niveau ou à celui DIF d'un VPN DIF. réseaux hétérogènes peuvent avoir une gestion plus efficace des ressources que de nos jours en utilisant hétérogènes politiques de gestion de la congestion, au lieu de compter sur un seul contrôleur d'encombrement de bout en bout qui n'a pas la visibilité de toutes les retransmissions de couche inférieure ou contention des ressources. Les contrôleurs chaînées permettent la personnalisation de segment par-réseau, tandis que les contrôleurs empilés réduisent le nombre de boucles de commande en compétition et d'augmenter la stabilité du comportement global du réseau[I.52].

9 Sécurité

9.1 introduction

la sécurité Internet actuelle est complexe, coûteux et inefficace. Les attaques sur les applications utilisant l'Internet et sur l'infrastructure fournissant grandir chaque année, malgré les protocoles sans cesse croissants liés à la sécurité, des systèmes et des dispositifs déployés dans le filet. L'une des explications habituelles est que la suite de protocoles TCP / IP n'a pas été conçu avec la sécurité à l'esprit. Les mécanismes de sécurité ont été ajoutés comme add-ons ou des protocoles distincts. Cependant, deux décennies après avoir reconnu ce problème[I.26], les niveaux de sécurité Internet ne sont pas encore suffisantes pour une infrastructure critique. On peut faire valoir que l'une des causes principales des problèmes de sécurité de l'Internet sont les défauts fondamentaux et les limites de la conception de la suite de protocole TCP / IP[I.27].

L'absence d'une approche structurée pour la conception provoque une prolifération des protocoles, dont chacun doit être protégé individuellement. interactions inattendues entre le protocole de base sans cesse croissante, l'inefficacité du nombre de mécanismes de sécurité répétées, une couche de réseau plat et d'exposer les adresses aux applications Internet font pratiquement impossible d'assurer à un coût abordable[I.28]. En revanche RINA offre un cadre architectural avec un bloc de construction bien défini - la diffé - qui récursif autant de fois que nécessaire. Fonctions de sécurité appartiennent au DIF, et non aux protocoles individuels au sein du DIF. Les interactions et le modèle de confiance entre sont bien compris DIF, ce qui permet des architectes du réseau de raisonner sur la sécurité d'un réseau, comprendre les menaces auxquelles il est exposé et concevoir les politiques plus adéquates pour protéger ses DIF.

Les clauses suivantes fournissent des informations détaillées sur les propriétés de sécurité RINA.

9.2 Sécurisation des protocoles au lieu DIF individuels

Sont le bloc DIF de construction composable de RINA, l'outil disponible pour les concepteurs de réseau pour créer des réseaux. Et non DIF protocoles individuels, sont l'élément à fixer dans l'architecture RINA. La structure récursive de RINA permet un modèle de sécurité clair dans lequel les relations de confiance entre et entre les DIF membres d'un seul sont bien compris DIF.Figure 27 illustre ces limites de confiance, ce qui facilite la mise en place des différentes fonctions de sécurité.

Les utilisateurs d'un besoin d'avoir DIF peu de confiance du DIF qu'ils utilisent: seulement que le DIF tentera de fournir des unités de service de données (SDU) à un processus. Les applications utilisant un DIF sont responsables d'assurer la confidentialité et l'intégrité du SDU qu'ils passent au DIF. Par conséquent, les mécanismes de protection appropriés SDU (telles que le cryptage) doivent être mis en place.

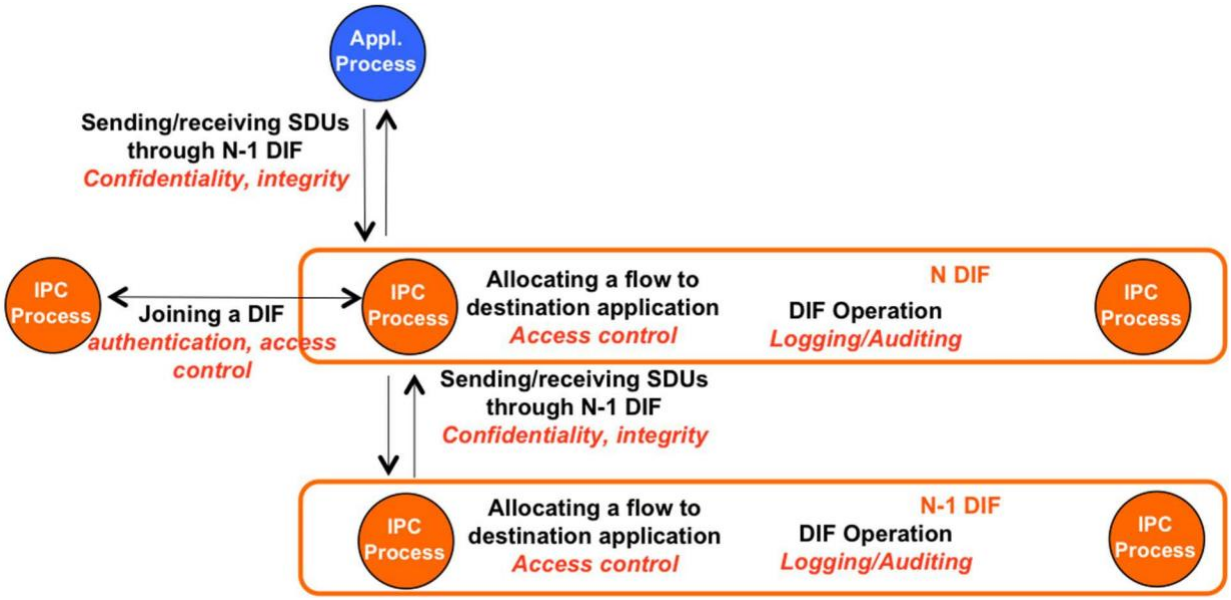


Figure 27: Mise en place de fonctions de sécurité RINA

Lorsqu'un nouveau IPCP veut se joindre à un premier besoin, il DIF d'allouer un flux à un autre IPCP qui est déjà membre d'une part par le DIF en commun N-1 deux processus DIF. Ici, le contrôle d'accès est utilisé pour déterminer si l'application demande est autorisé à parler à l'application demandée. Si le flux au membre existant est acceptée, l'étape suivante consiste à passer par une phase d'authentification, dont la force peut varier de pas d'authentification aux systèmes de chiffrement. Dans le cas d'une authentification réussie, le membre décidera si DIF le nouveau IPCP est admis au DIF, l'exécution d'une politique de contrôle d'accès spécifique.

Les opérations à distance sur PCIP par les pairs sont un autre domaine où le contrôle d'accès est d'une importance capitale. Toutes les fonctions de gestion de la couche d'un IPCP utilisent une infrastructure commune pour échanger des informations avec ses pairs: la Base de données sur les ressources (RIB) et CDAP. CDAP définit un protocole pour effectuer six opérations à distance sur un ensemble d'objets distribués, qui sont utilisés pour modéliser les informations de chaque tâche de gestion de couche spécifique. Le RIB impose un schéma (nom et ensemble de relations) sur les objets DIFF. A la granularité la plus fine, il est possible de prendre une décision de contrôle d'accès pour autoriser l'accès à chaque objet dans le schéma de RIB pour chacune des opérations CDAP (permettant différentes tâches de définir leurs propres restrictions de contrôle d'accès).

Petit et al. effectuer une analyse de la menace de RINA au niveau de l'architecture[I.17], concluant que lorsque l'authentification correcte, les politiques de contrôle de la protection et l'accès SDU sont mis en place, un conteneur est un DIF sécurisable: une structure utilisée pour maintenir ou transport de données qui peuvent être faites non soumis à la menace. En revanche, le modèle de sécurité suite de protocoles TCP / IP est généralement basée sur la construction des fonctions de sécurité pour chaque protocole.

Par exemple, DNSSEC [I.29] fournit l'intégrité des données et l'authentification résolveurs de sécurité au courant. IPsec[I.30] est un cadre général pour les communications IP sécurisées, soutenant la confidentialité, l'intégrité, l'authentification ou la protection contre les attaques de relecture. Cependant, étant donné que IPsec fonctionne de bout en bout dans une couche IP, soit il ne protège que la charge utile IP (mode de transport) ou fait orienté connexion IP (mode tunnel), l'encapsulation d'un paquet IP protégé dans un paquet IP non protégé. Cela rend IPsec une solution partielle, sans répondre aux exigences des protocoles de plan de contrôle IP, qui doivent définir leurs propres fonctions de sécurité, telles que OSPF[I.31] ou BGE [I.32]. TLS, la couche de protocole de transport de sécurité [I.33], spécifie un ensemble de fonctions de sécurité connexes pour permettre des communications sécurisées sur la couche de transport.

Dans l'ensemble, cette approche donne lieu à plus de frais généraux et de la complexité par rapport à la sécurisation DIF. Dans[I.34] Petit exécute une première comparaison entre RINA et l'Internet actuel, la mesure des débits, les protocoles et les mécanismes nécessaires pour fixer chaque architecture. Petit conclut que les réseaux RINA peut fournir des exigences de sécurité avec moins de complexité que est actuellement possible en utilisant la suite de protocoles Internet.

9.3 La récursivité permet une isolation et des couches de portée inférieure

L'un des principaux défis de la sécurité Internet actuelle est celle de son champ d'application. La surface d'attaque d'une couche augmente avec sa taille: plus une couche est la plus grande sera le nombre d'attaquants potentiels et des vulnérabilités exploitables telles que missconfigurations, l'utilisation des pouvoirs faibles, etc. La portée du public couche IP Internets est énorme ; assez grand pour épuiser 32 bits d'IPv4 de l'espace d'adressage, et il continuera de croître avec IPv6.

Non seulement ce fait faire des nœuds dans l'Internet public plus sujettes aux attaques, mais contrecarre également le déploiement de nouveaux protocoles pour deux raisons: soit les nouveaux protocoles doivent assumer un certain niveau de confiance dans leurs pairs qui ne peuvent pas être garantis dans la nature réseau public; ou des millions de mécanismes de défense standard tels que les pare-feu doivent être mis à jour pour tenir compte des particularités du nouveau protocole, qui est difficile à faire dans la pratique (par exemple, le déploiement SCTP[I.35]). Les protocoles existants sont également difficiles à mettre à jour, même si les mises à jour sont essentielles à la sécurité de l'Internet, comme le cas pour les extensions de sécurité BGP[I.36].

L'avènement de la virtualisation du réseau et son déploiement à grande échelle dans les centres de données (PED) a fourni aux concepteurs de réseaux DC avec un outil pour créer DIF de moindre ampleur offrent une meilleure isolation, de minimiser l'impact des menaces de sécurité et permettre la personnalisation des politiques de sécurité à différents des profils d'utilisateurs[I.37].structure récursive de virtualisation RINA généralise réseau, ce qui permet des architectes du réseau de composer des politiques de DIF taille arbitraires et personnalisées dans un réseau avec un modèle de sécurité clair.

Figure 28 montre un exemple du réseau d'un fournisseur de services, connecté à un réseau de clients (à gauche) et d'échange de trafic avec un autre réseau de fournisseurs (à droite). Fournisseur 1 ne partage que l'accès et DIF DIF multi-fournisseur avec d'autres réseaux, les internes du DIF fournisseur - Difs régionaux et la colonne vertébrale - ne sont pas visibles à l'extérieur du réseau de fournisseurs. Cette conception réduit la surface d'attaque des réseaux, ce qui limite les dégâts qu'un attaquant externe peut effectuer: la plupart des fonctions de routage et d'allocation des ressources du fournisseur sont exécutées dans les internes DIF. Compromettre les compromettre physiquement exige DIF les actifs des fournisseurs, donc le fournisseur peut concentrer ses ressources sur la protection du périmètre de son réseau avec les politiques de protection et d'authentification forte SDU.

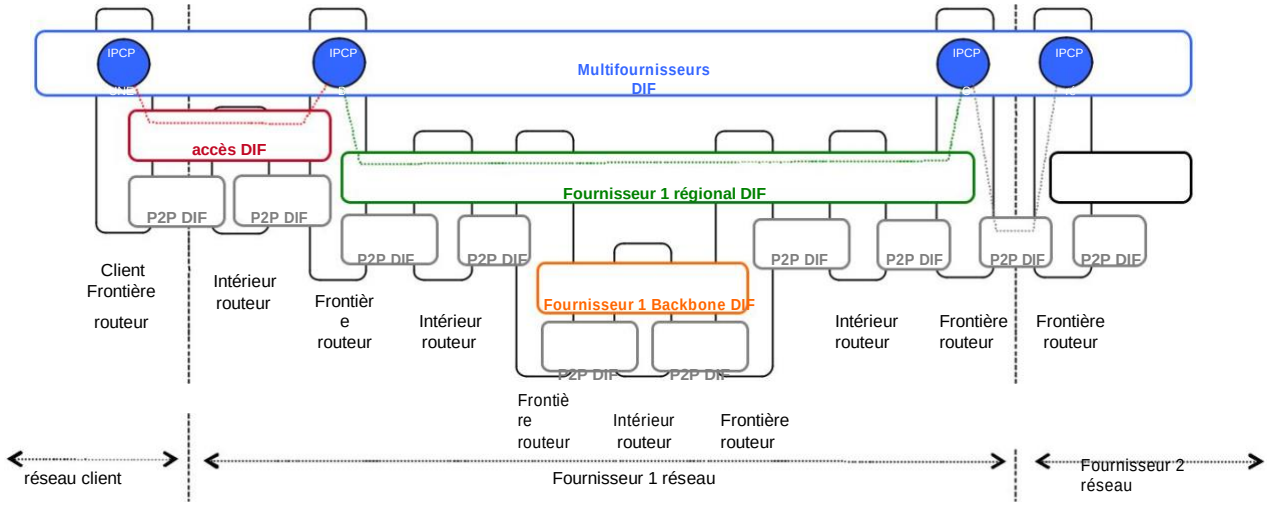


Figure 28: Utilisation Rinas structure récursive pour cacher les internes d'un DIF réseau de fournisseurs de services

9.4 La séparation du mécanisme de la politique

En RINA le principe du mécanisme de séparation de la politique [I.7] est utilisé pour séparer les parties fixes d'une fonction de processus IPC - qui sont les mêmes à travers DIF - à partir des parties variables. Par exemple, un accusé de réception est un mécanisme, quand reconnaître est la politique. Ce principe permet aux mêmes mécanismes pour être réutilisés dans DIF, ce qui réduit le nombre de différents mécanismes présents dans le réseau[I.34] tout en permettant la personnalisation des politiques de sécurité DIF. Les politiques écrites pour un peuvent être réutilisés DIF-utilisés dans d'autres DIF, ce qui maximise l'efficacité des spécifications et mises en œuvre.

Mécanisme de séparation de politique permet à chaque DIF d'adapter à différents environnements de fonctionnement tout en conservant une limite supérieure à la complexité de l'architecture, qui est l'un des paramètres essentiels lors de la fixation d'un système distribué [I.38]. Les architectes réseau ne ont pas besoin de concevoir des protocoles plus, juste des politiques adaptées aux besoins des différents DIF. Par exemple, la figure 28 IPCP B dans le bleu utiliser une DIF forme d'authentification cryptographique et le chiffrement lors de l'échange d'informations avec IPCP A sur le rouge DIF, puisque le rouge est partagé DIF entre le fournisseur et différents clients. Cependant, IPCP B peut utiliser sans authentification ni cryptage lors de l'échange d'informations avec IPCP C sur le vert DIF, car dans ce cas tous les systèmes sont sous le contrôle du fournisseur.

9.5 Le découplage de l'allocation orifice de synchronisation

Dans le TCP / TCP suite protocole IP surchargeant le port-id être à la fois une poignée locale (prise) et l'ID de connexion point final (CEPID). En outre, l'absence de noms d'applications surchargent port-ids avec la sémantique de l'application: paramètres d'application sont identifiés par une combinaison d'adresse IP et un port-id bien connu qui est attribué lorsque l'application se lie à une couche IP. les valeurs de port de destination identifiant statique doivent être connues par l'application source lors de la demande d'une connexion de transport. Par conséquent, un attaquant voulant intercepter une connexion TCP particulière n'a besoin que de deviner / spoof la source port-id.

Dans RINA port-allocation et de synchronisation sont des fonctions distinctes, en appliquant les résultats obtenus par Watson avec la conception du protocole delta-t[I.9]. La procédure port-allocation est déclenchée de façon explicite par une requête demandant un flux vers une application de destination. La source IPCP attribue dynamiquement local port-id de l'écoulement et crée une instance de protocole de EFCP qui prend en charge des aspects de synchronisation de rétroaction (débit et de contrôle de retransmission). L'instance de EFCP est identifié par un CEPID source généré dynamiquement qui est mappé sur le port-id via une liaison locale comme le montre laFigure 29. La destination IPCP fait les étapes équivalentes, ce qui entraîne dans un port local-id et une destination CEPID. La source et la destination sont CEPID les valeurs observées sur les PDU dans le fil; port-ids ne sont que d'une importance locale et utilisées par les applications pour lire / écrire des données de flux.

L'état des ports et des connexions est gérée avec des approches différentes: l'état du port est explicitement créé et supprimé par les applications (disque étatiques) alors que l'état de connexion est créé et supprimé suite à une approche par minuterie (soft-state): après de longues périodes sans trafic l'état de connexion est supprimé et créé à nouveau lorsque le nouveau trafic est envoyé / reçu sur la connexion. Bodappati et al. a montré dans[I.11] comment RINA met à profit cette conception pour obtenir une plus grande aux attaques de niveau de transport tan résilience TCP / IP telles que la numérisation du port, l'ouverture de la connexion ou le transfert de données.

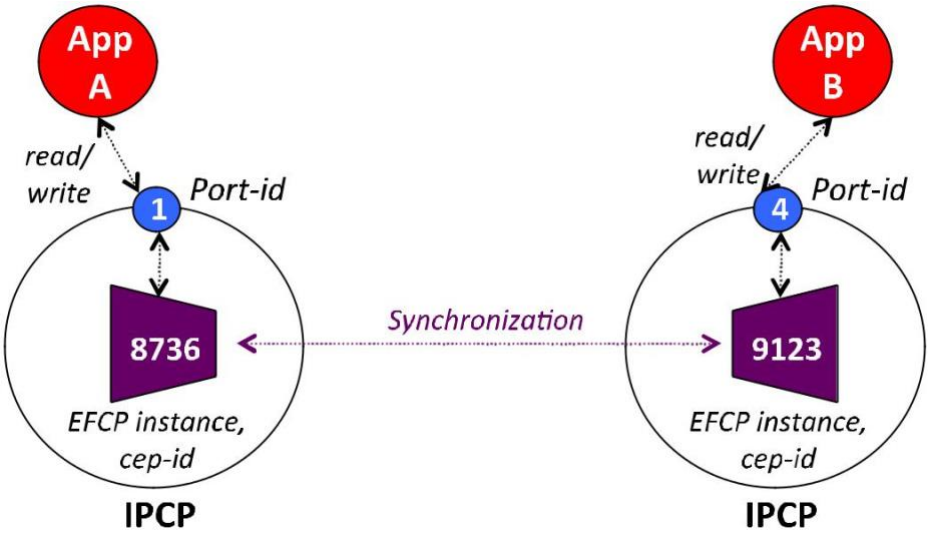


Figure 29: Le découplage de l'allocation de port et de synchronisation en RINA

9.6 L'utilisation d'une dénomination complète et architecture d'adressage

Nommage et d'adressage des considérations de conception ont également un impact profond sur la sécurité des architectures de réseau. Depuis la suite de protocoles TCP / IP ne pas les noms d'applications (DNS est un annuaire externe), les couches IP exposer les adresses aux applications. La divulgation de l'information facilite l'usurpation d'identité des adresses IP, et en combinaison avec l'utilisation d'outils de contrôle communs tels que traceroute ou ping permet aux pirates sur les hôtes finaux pour se renseigner sur les adresses des cibles potentielles dans une couche - routeurs ou d'autres hôtes - ainsi que le graphique de la connectivité réseau. Les pirates peuvent utiliser ces informations pour DDoS attaques de configuration en automatisant la découverte et l'infection des machines vulnérables[I.39], ou d'attaquer l'infrastructure réseau en prenant le contrôle sur les routeurs.

RINA dispose d'un réseau complet et architecture d'adressage, avec des noms d'application et des répertoires par-qui effectuent l'application DIF à la résolution d'adresse du processus IPC. Lorsqu'une application demande un d'allouer un DIF flux à une application de destination, il fournit la source et les noms de processus d'application de destination. Le résout en interne le DIF nom de l'application de destination à l'adresse du processus CIB où l'application de destination est enregistrée.

En raison de l'existence de noms d'application des informations d'adressage d'un DIF (format d'adresse, les adresses valides / actifs) ne soient pas divulguées en dehors du champ d'application du DIF. Un attaquant dans un hôte ne peut pas répondre aux processus IPC d'un à moins qu'elle rejoint DIF le SNDIF il veut attaquer, ce qui nécessite une authentification.

9.7 Résumé des principes de conception RINA relatifs à la sécurité

Cette clause résume la façon dont RINA aborde les problèmes identifiés à l'article 4.3.6:

- **Au lieu de sécurité DIF protocoles individuels.** RINA fournit un modèle de sécurité cohérente à travers les couches. Sont des conteneurs sécurisable DIF, ils peuvent ne pas être soumises à une menace fournissant l'authentification appropriée, contrôle d'accès et de protection des SDU politiques sont mises en place. En RINA, l'unité de protection est le DIF et non ses protocoles individuels. La décomposition fonctionnelle d'un définit naturellement le DIF placement des fonctions de sécurité et place les limites de confiance entre et au sein de DIF. L'authentification, le contrôle d'accès et de protection SDU sont des politiques qui peuvent être branchées dans une diffé - quel que soit son classement et exigences - réduisant ainsi le coût de la spécification et la mise en œuvre des politiques de sécurité « par rapport au modèle de sécurité par protocole de l'Internet actuel ».

- **Découpler allocation de port de synchronisation de transfert de données - pas de « ports bien connus »**. Chaque DIF alloue des flux à base d'un nom de l'application de destination, qui est intérieurement résolu en une adresse du processus IPC. Lorsque le débit est alloué, l'application demandeuse obtient un (OS) identifiant local comme une poignée locale à l'écoulement: le port-id. Contrairement à l'Internet actuel, le port-ids sont générés dynamiquement et de signification locale «ainsi l'analyse des ports bien connu est pas une attaque efficace pour DIF ». En outre, l'état de transport associé à l'écoulement est dirigé par les instances du protocole EFCP, qui ont leurs propres identifiants distincts (IDS ou CEPIDs-noeud final connexion) mappés localement à port-ids. CEPIDs sont également générées dynamiquement au moment de l'allocation de débit.

- **Utilisation des noms d'application: les adresses sont internes à chaque DIF.**adresses de processus IPC sont internes à jamais divulgué DIF en dehors de celui-ci. Toutes une application utilisateur connaît un est son nom DIF et les classes de qualité de service qu'elle soutient. Par conséquent, une application à l'aide d'une adresse ne peut DIF tout membre du moins elle rejoint DIF le DIF. Si ce risque / menace existe, le concepteur aura configuré DIF le DIF utiliser le contrôle d'authentification et d'accès, donc un attaquant potentiel a besoin de contourner ces contrôles de sécurité avant de pouvoir communiquer à tout processus IPC dans ce DIF. RINA fournit un environnement plus contrôlé dans lequel le contrôle de l'association et le degré d'ouverture du réseau est une question de conception et non pas « ouvrir à tout le monde par défaut, mais ajouter l'infrastructure pour le fermer si la connectivité doit être limitée ».

dix La gestion du réseau

10.1 Les éléments communs d'un cadre de gestion

Une vue d'ensemble de haut niveau des éléments communs dans le cadre de la gestion du réseau est assurée par RINA Figure 30.Chaque système de traitement (boîtes rectangle) peut exécuter un ou plusieurs processus IPC, la mise en œuvre d'un ou plusieurs dans ce système DIF. Les processus IPC dans un système sont gérés par l'agent de gestion, qui a lire et écrire des autorisations à la base de données sur les ressources des processus IPC (RIB) s. Dans certaines configurations théoriques un ou plusieurs gestionnaires de communiquer avec les DIFF agents dans chaque système de son domaine de gestion pour fournir une configuration centralisée, faute, la sécurité et la gestion du rendement. Les agents de gestion et les gestionnaires DIFF forment ensemble une application distribuée qui gère les éléments d'un ou plusieurs DIF, et est appelé Network Management System - Facilité d'applications distribuées (ou NMS-DAF en bref).

Alors que les IPC-processus qui composent le échangent des informations DIF sur leur fonctionnement et les conditions qu'ils observent, il est généralement nécessaire d'avoir aussi une fenêtre extérieure dans le fonctionnement du réseau comprenant DIF. Alors que les membres peuvent atteindre une optimisation locale, il est souvent plus complexe à découvrir des optimisations globales sans perspective « extérieur ». Dans ces systèmes, le contrôle doit être automatique. Les événements se passent beaucoup trop vite et de l'État est en train de changer trop rapidement pour un système centralisé pour être efficace. En outre, la nature des systèmes distribués ouvre toujours la possibilité pour le partitionnement. Par conséquent, il devrait être possible pour les systèmes distribués en mode de sécurité sans contrôle central. Un NMS-DAF effectuera les fonctions traditionnelles de contrôle et de réparation, le déploiement de nouvelles configurations, le suivi des performances, etc.

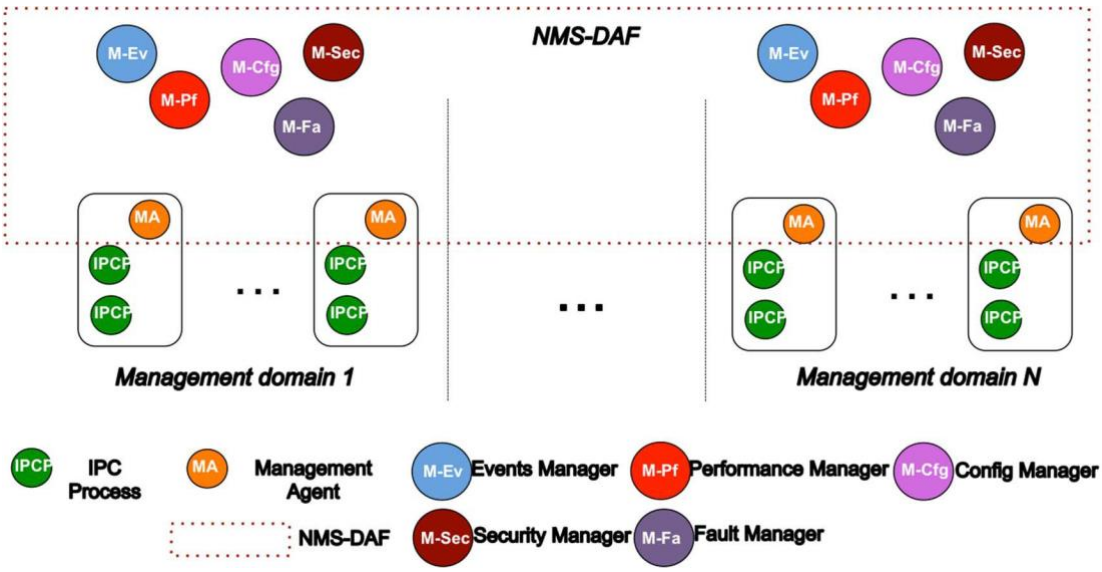


Figure 30: configuration typique d'un NMS-DAF centralisé avec plusieurs domaines de gestion

Dans l'architecture de gestion de réseau centralisé traditionnel, un NMS-DAF serait un DAF hétérogène constitué d'un ou plusieurs processus d'application assurant des fonctions de gestion, avec d'autres processus d'application fournissant télémétrie. Les points d'accès de gestion pourraient être les rôles ou les tâches de subdiviser au sein de la gestion du réseau ou de fournir la gestion des sous-domaines et de redondance pour l'autre. Un NMS-DAF aura typique des tâches habituelles de gestion des événements, gestion de configuration, gestion des pannes, la gestion des ressources, etc. Cela a aussi l'avantage de déplacer l'accent des boîtes à un modèle de système distribué.

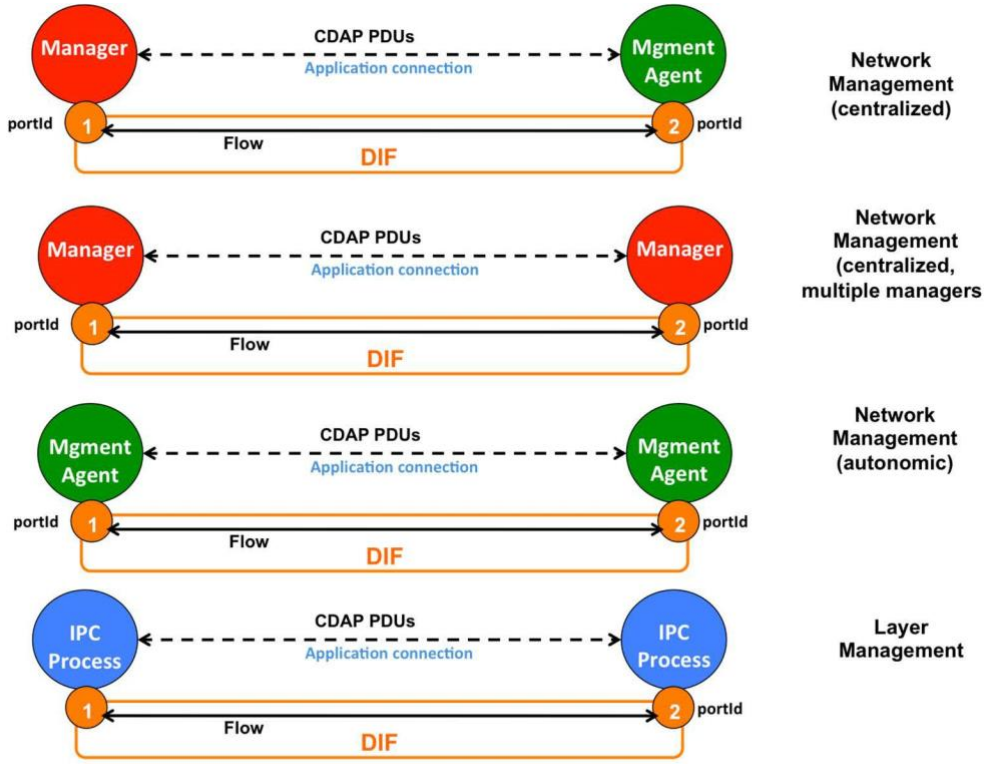


Figure 31: Différentes interactions entre les processus d'application NMS-DAF, et processus IPC pour la gestion de couche (down)

Le NMS-DAF est une application distribuée (un DAF), et exploite donc les éléments communs dans le cadre DAF. Pour interagir avec chaque système, les processus de gestion doivent avoir un en commun avec DIF elle. Il y a plusieurs façons d'y parvenir, allant d'utiliser un seul dédié à l'interconnexion DIF le gestionnaire à chaque agent de gestion, à l'utilisation de différents systèmes pour différents DIF. Une fois que le gestionnaire a alloué un flux à un agent de gestion, il établit une connexion d'application à via CACEP, qui comprend l'authentification facultative. Une fois la connexion d'application est en place, les gestionnaires et l'agent de gestion peut communiquer à distance en effectuant des opérations sur les semi-rigides des processus IPC via CDAP - le protocole d'application distribuée commun.

Figure 31 illustre les différentes interactions entre les points d'accès dans le NMS-DAF (à l'exception de la dernière, qui est une interaction de gestion de couche entre PCIP dans un DIF):

- **l'interaction de l'agent gestionnaire de gestion.** L'interaction la plus commune dans la configuration traditionnelle des systèmes de gestion de réseau, dans lequel un processus Manager utilise des agents dans chaque système informatique afin de surveiller les systèmes et mettre à jour sa configuration en cas de besoin.

- **interaction Manager-Manager.** Dans la plupart des cas, comme lorsqu'un DIF est détenue par plusieurs entités indépendantes ou pour diviser les fonctions de Manager dans des zones séparées (défaut, Configuration, événement, performance, etc.), il est nécessaire de partitionner la gestion d'un ou plusieurs DIF dans plusieurs domaines de gestion. Au moins un processus de gestionnaire est responsable de la gestion de l'un de ces domaines individuels. Par conséquent, les interactions Manager Manager sont également nécessaires.

- **Agent de gestion - interaction agent de gestion.** Dans cette configuration, les agents de gestion ont une plus grande autonomie pour prendre certaines décisions fondées sur les informations tirées des autres agents de gestion __gVirt_NP_NN_NNPS<__ voisins. Le degré d'autonomie peut varier en fonction de la configuration en cours d'utilisation: de l'utilisation des agents de gestion pour regrouper l'information de gestion dans les « sous-domaines » aux systèmes de gestion de réseau sans gestionnaires centraux à tous.

- **Procédé IPC - interactions de processus CIB.** Bien que ce type d'interaction ne tombe pas uniquement dans la catégorie « Gestion du réseau », les processus IPC dans un DIF utilisent les mêmes outils pour échanger des informations: CACEP pour l'établissement de connexion d'application et CDAP pour fonctionner sur les objets des voisins Processus IPC semi-rigides. Exemples d'utilisation de cette interaction sont l'inscription, le routage, l'allocation des flux ou l'allocation des ressources.

10.2 La gestion d'une structure de répétition

La structure commune de RINA peut être exploitée par la gestion du réseau dans un certain nombre de façons.

La simplification dans la gestion de plusieurs couches, mais avec la possibilité de configurer différentes politiques. Aujourd'hui, de plus en plus des couches exercent des fonctions qui ne sont pas à eux traditionnellement attribué (telles que le routage d'état de liaison dans la couche 2 des réseaux à courant continu[I.40] ou en couches mise en œuvre des soi-disant « réseaux virtuels »). Les couches sont en train de remplacer l'exécution d'une seule fonction pour devenir des unités d'allocation des ressources distribuées, ce modèle prédit RINA pleinement. Cependant, étant donné que les différentes couches traditionnelles ont évolué indépendamment des différents points de départ et ont été normalisés par différents comités, les mêmes fonctions (telles que le routage ou l'authentification) ont une sémantique très différentes.

En conséquence, la configuration, les performances ou la gestion des défauts devient complexe, étant donné que les nouveaux États membres doivent être au courant des détails de chaque technologie spécifique mis en œuvre dans les différentes couches. En revanche, les réseaux RINA fournissent la même structure; la configuration, par exemple un routage à état de liens dans le « DC-tissu DIF » ou dans chacun des différents « locataire » DIF avec exactement la même sémantique - les mêmes objets avec des valeurs différentes peut être utilisé partout[I.41].

Une gestion plus efficace des événements réseau complexe. Le point commun fourni l'architecture RINA permet la définition d'un modèle de performance qui est commune à toutes les couches, comme expliqué dans l'article 8. C'est un outil très puissant pour le système de gestion de réseau, depuis:

a) les nouveaux États membres seraient moins reçoivent les types d'événements, libérant de la traduction à un modèle de performance interne pour parvenir à une bonne compréhension de l'état général du réseau;

b) la corrélation des événements dans plusieurs couches deviendrait beaucoup plus simple, ce qui facilite l'identification des problèmes par les nouveaux États membres et permettant aux actions enroulables pour résoudre efficacement et de les atténuer.

Les mêmes arguments à la sécurité, peut-être même avec un impact plus large.

*Plus d'automatisation est possible: la gestion du réseau devrait être « surveiller et réparer » - pas « contrôle » [*I.42***]**. RINA la mise au point des nouveaux États membres peut passer de « protocoles » à « politiques », nécessitant une intervention moins humaine des opérateurs humains - et donc moins d'erreurs humaines. Étant donné que les protocoles deviendraient une marchandise - juste une partie de la commune, l'infrastructure de couche standard - la recherche et l'expérimentation pourraient se déplacer vers la compréhension du comportement des politiques ensembles différents dans des conditions différentes de fonctionnement. Cela permettrait aux administrateurs réseau de gérer le réseau de la manière suivante:

1) Au moment de la conception, de caractériser les différentes conditions que le réseau va expérimenter pendant son fonctionnement au jour le jour (par exemple en termes de charge offerts, l'échec des liens, des attaques de sécurité en cours identifiés, etc.).

2) A la conception, le groupe dans ces conditions bien définies « régions opérationnelles », et choisir politiques ensembles qui sont efficaces pour chacune des différentes régions.

3) Lors de l'exécution, que les nouveaux États membres surveillent le réseau, décider si les mesures appartiennent à l'une des régions opérationnelles « conçues ». Si la région opérationnelle n'a pas changé, continuer à surveiller. Si la région opérationnelle dans une autre transition « conçu » zone opérationnelle, appliquer automatiquement la politique liée ensemble. Si la région opérationnelle est inconnue - comme cela pourrait être le cas des catastrophes naturelles, attaques terroristes, etc. - informer l'opérateur humain.

10.3 Résumé des principes de conception RINA liés à la gestion du réseau

Cette clause résume la façon dont RINA aborde les problèmes identifiés à l'article 4.3.7:

- **Deux cadres de protocole immuables et un ensemble bien défini des politiques.** Tout dans l'architecture RINA tente de maximiser les invariants et de réduire la variabilité des réseaux informatiques, ce qui réduit au sous-ensemble des fonctions essentielles qui doivent changer pour adapter à différentes applications et exigences de la couche physique. Le résultat immuable, structure commune avec un seul type de couche qui comporte deux cadres de protocole et un ensemble bien défini des politiques simplifie grandement la complexité du problème de la gestion du réseau. Cela est particulièrement vrai par rapport à la situation actuelle de protocoles redondants, indépendamment conçus à travers les couches et à l'intérieur des couches. Simplifier la structure du réseau non seulement réduit la complexité, mais permet également l'automatisation plus sophistiqués au sein du système de gestion.

- **API cohérente et fonctions à travers toutes les couches, la superposition stricte.** Les systèmes de gestion des réseaux RINA jamais besoin de se soucier des effets de la couche croisée, car la superposition stricte est appliquée par la conception. Les interactions entre les couches sont bien comprises et facile à modéliser en tant que couches de service IPC sur différents champs d'application et les gammes de QoS. Le système de gestion coordonne plusieurs couches, mais n'a pas besoin de les micro-gérer: puisque chaque couche est autonomique les NEM peuvent définir des stratégies de haut niveau que chaque couche exécutera via les fonctions de gestion de couche.

- **Protocole de gestion unique et le modèle d'objet couche commune.** Communité est la clé vers une gestion efficace du réseau. Les systèmes de gestion de réseaux RINA utilisent un protocole unique pour interagir avec les agents de gestion des systèmes à différents segments du réseau. Ce protocole de gestion, CDAP, est même pas spécifique à la gestion du réseau (il est également utilisé pour la gestion de la couche). CDAP est utilisé pour faire fonctionner sur les objets exposés par le RIB des agents de gestion à chaque système. Tous ont un modèle DIF RIB commun (voir[I.43] pour une spécification initiale), ce qui facilite encore la tâche de gérer DIF: la seule différence de la gestion d'un à l'autre DIF est dans les modèles d'objet de politiques individuelles.

- **Chaque couche a un ensemble borné et bien défini de points de programmabilité.** La séparation du mécanisme et de la politique (infrastructure immuable et mutable) définit l'ensemble des fonctions de réseau qui peuvent être programmées dans chaque couche, ainsi que le contrat abstrait de ces politiques doivent honorer (quels sont les paramètres d'entrée, ce qui est le comportement attendu, ce sont les paramètres de sortie le cas échéant). Ainsi, une couche est aussi flexible et programmable au besoin, mais pas plus: la programmabilité offerte par l'infrastructure commune rend les concepteurs de réseaux sûrs ne cassent pas les principes architecturaux RINA.

11 considérations relatives au déploiement

11.1 Principes généraux

11.1.1 applications de soutien

La grande majorité des applications distribuées utilisent aujourd'hui l'API Sockets pour demander des services de communication, que ce soit directement ou via un cadre logiciel de niveau supérieur qui utilise en interne Sockets. L'API Sockets ne pas abstraire le service de communication fourni par sa mise en œuvre très bien: les adresses réseau sont exposés et le développeur d'applications doit choisir explicitement le protocole de transport qui fournira le service de communication. Ce fait rend l'introduction de nouvelles technologies de transport très difficile, car il est transparent pour le développeur d'applications[I.6].

Par conséquent, un certain nombre de stratégies sont possibles pour permettre le support des applications héritées:

a) la modification du code d'application qui interagit avec le réseau afin qu'il parle à l'API du service IPC (ou même à une autre API de réseau qui est vraiment la technologie agnostique);

b) écrire un émulateur Sockets qui mappe les appels à l'API Sockets pour les appels à l'API du service IPC;

c) la modification de middleware d'applications / bibliothèques qui fonctionnent sur l'API Sockets fournissant une abstraction plus aux applications (ainsi plusieurs applications peuvent être pris en charge par simplement la modification d'une seule bibliothèque);

d) écrire un module RINA pour un service de transport (IETF TAPS) implémentation de l'API [I.6], puisque TAPS fournit une API qui vise à être protocole de transport agnostique.

D3.1 livrable de ARCFIRE [I.44] décrit une conception et la mise en œuvre d'une API de service IPC pour RINA qui est très proche de l'API de fichier défini dans la norme POSIX. Les flux sont modélisés comme des descripteurs de fichiers qui peuvent être attribués, lu, écrit et fermé par des applications. Le serveur et les flux de travail côté client sont très semblables à ceux de l'API prises (comme illustré parFigure 32, minimisant ainsi la courbe d'apprentissage pour les développeurs d'applications familières avec l'API Sockets. les chercheurs ont porté ARCFIRE deux applications de prises à ce POSIX comme API de service IPC: le serveur web Ngnix et le serveur SSH Dropbear[I.45]. Le portage de chaque application implique la réécriture d'environ 300 - 400 lignes de code, ce qui est un effort relativement faible.

Applications au portage API de service IPC a l'avantage que ces applications peuvent exploiter les fonctionnalités d'une architecture de réseau générique (IPC de nommage de l'application, l'indépendance de protocole, capacité de demander des options QoS pour le service de communication). Cependant, le coût de la modification d'une application à déployer sur un réseau RINA peut être trop élevé dans de nombreux cas. Un émulateur sockets est la meilleure option pour ces scénarios. Ce logiciel remplace les mises en œuvre des opérations de prises dans la bibliothèque standard C par des appels à une API de service IPC (comme l'API comme POSIX RINA). Une mise en œuvre initiale d'un émulateur Sockets a été lancé en[I.46]. Un problème général qu'un émulateur sockets doit résoudre est comment mapper les informations transmises à l'API Sockets à un nom d'application. Si l'application utilise des noms de domaine, il peut être directement mis en correspondance avec un nom d'application, mais les applications qui passent directement des adresses IP peut être plus problématique.

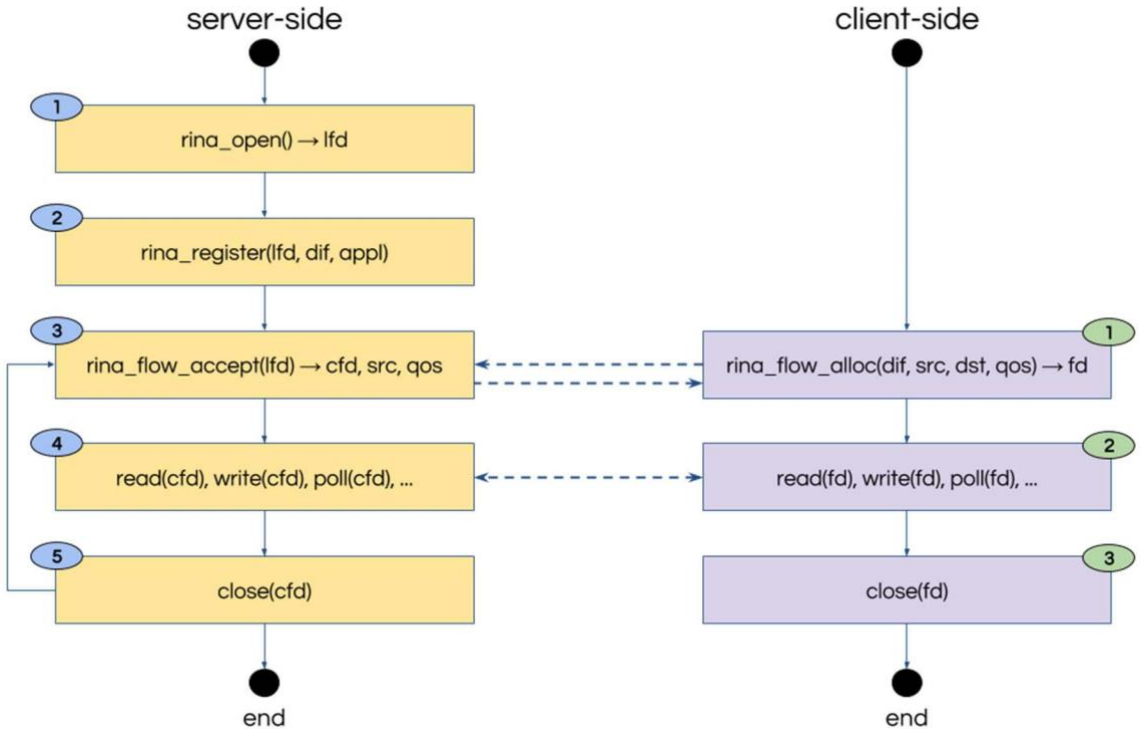


Figure 32: Posix comme API de service IPC conçu par le projet ARCFIRE

11.1.2 Superpositions: shim DIF

Peuvent être déployées DIF sur des couches existantes de protocoles comme une superposition. L'adaptation d'un protocole existant d'un DIF est effectuée par l'intermédiaire d'un DIF shim. La tâche d'un DIF cale est de mettre le plus petit possible un placage sur un protocole existant pour permettre un à l'utiliser DIF inchangé. En d'autres termes, cette cale permet de DIF au-dessus construit en utilisant DIF l'API du service IPC pour fonctionner sur Ethernet sans changement. Le DIF enveloppe la cale couche de protocole sous-jacent à l'interface de service IPC. L'objectif est de ne pas faire les protocoles existants fournissent un support complet pour le DIF et donc le DIF de cale devraient fournir plus de service ou de capacité que le protocole prévoit l'héritage.

Le projet IRATI défini Caler superposition DIF RINA sur le dessus de l'Ethernet (avec et sans VLANs) [I.47], TCP et UDP [I.48] et la mémoire partagée pour la communication VM-hypervisor [I.49]. ARCFIRE a également précisé et mis en œuvre un DIF de cale pour superposer RINA au-dessus du WiFi. L'abstraction shim a prouvé un DIF outil efficace pour superposer RINA sur des technologies de réseau existantes.

11.1.3 Comme le transport DIF multi-protocole (IP, Ethernet, etc.)

Peut également être DIF utilisé comme une technologie qui peut efficacement thibaude le transport IP, Ethernet ou des flux appartenant à d'autres protocoles avec le niveau de service adéquat. L'utilisation de ce DIF approche peut être utilisée comme une alternative ou un remplacement MPLS dans une variété de scénarios tels que les tissus de réseau de centre de données, le BGE sans backbones des fournisseurs de services, région métropolitaine de réseaux offrant des services Carrier Ethernet, etc. DIF peuvent fournir des services tels que le point flux -à point, réseaux privés virtuels IP, les instances Ethernet VPLS, etc.

11.1.4 passerelles de couche de transport

Les passerelles permettent l'interopérabilité des applications prises en charge par un réseau intégré au réseau générique d'architecture IPC et les applications en cours d'exécution dans les systèmes qui exécutent des protocoles de réseau traditionnels. De tels scénarios sont très probablement surtout dans les premiers jours de déploiement, où un certain nombre d'îles génériques d'architecture réseau IPC sera opérationnel entouré d'un océan de systèmes IP seulement. Par exemple, une architecture de réseau générique IPC centre de données a permis devra aider les clients qui peuvent soutenir tout IP, sans que les applications déployées au centre de données à être au courant des différences.

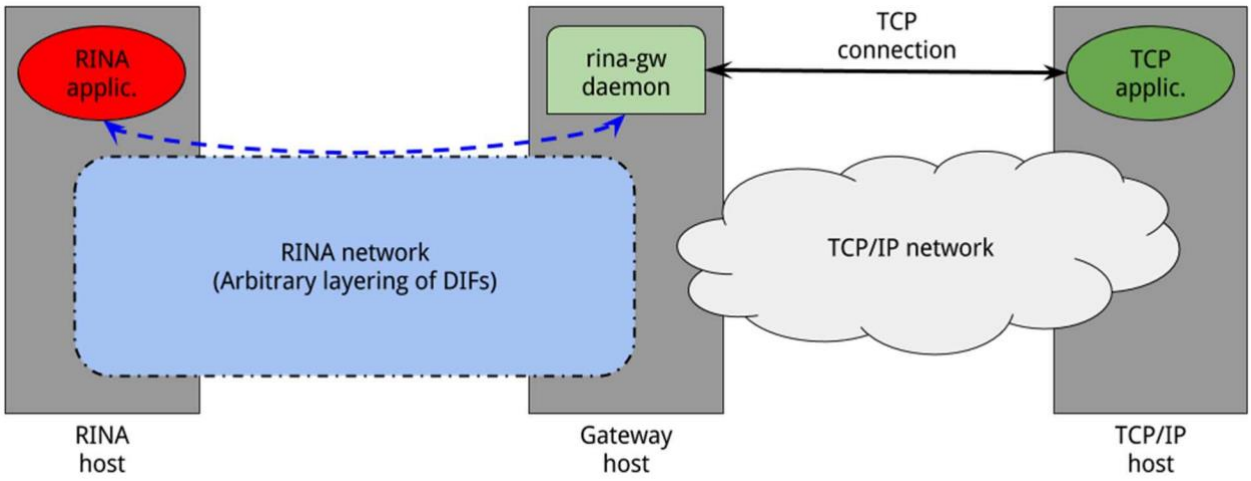


Figure 33: Exemple de configuration d'une passerelle TCP-RINA

Les projets immaculées et ARCFIRE ont travaillé dans la passerelle TCP-RINA, un démon qui agit comme un proxy / passerelle entre un réseau TCP / IP et un réseau RINA [I.50] comme le montre la figure 33. D'un côté, la passerelle accepte les connexions TCP provenant d'un réseau TCP / IP et les proxie en allouant des flux RINA vers les applications appropriées du serveur dans le réseau RINA. De l'autre côté, la passerelle accepte les demandes d'allocation de flux provenant du réseau RINA et les proxie vers un serveur TCP au moyen de nouvelles connexions TCP. La passerelle peut être facilement étendu pour supporter d'autres le relais des protocoles de transport tels que UDP.

passerelles de couche de transport viennent avec leurs propres inconvénients:

a) depuis la passerelle met fin à la connexion de transport et le flux RINA, la sémantique bout-en-bout de la connexion de transport et le flux RINA sont brisés;

b) les informations d'identification doivent être gérées correctement dans le cas où TLS (Transport Layer Security) est utilisé sur la connexion de transport.

Cependant, ces passerelles sont déployés aujourd'hui dans les réseaux de production pour d'autres raisons (augmenter le rendement ou proxies, par exemple PEPs), par conséquent, ils sont une solution viable pour soutenir l'interopérabilité dans les cas d'utilisation appropriés.

11.2 Exemples de scénarios d'interopérabilité

11.2.1 réseau datacentre

réseaux Datacentre sont organisés pour fournir un substrat de connectivité efficace aux applications en cours d'exécution dans un grand bassin de ressources informatiques (soit directement dans les machines physiques ou machines virtuelles). DC peut prendre en charge un seul type ou plusieurs applications, à partir d'un seul ou plusieurs utilisateurs. Certains pays en développement sont spécialisés pour fournir des services de cloud computing, l'attribution d'un sous-ensemble des ressources DC à une application ou un ensemble d'applications, qui sont isolées du reste du DC en termes de performance et de sécurité. Ce type de courant continu est dit support multi-location.

Réseaux de contrôleurs de domaine multi-locataires suivent généralement 3 ou 5 étape topologie Clos, avec TdR (Haut de rack) commutateurs / routeurs agrégeant le trafic des serveurs dans un seul rack, commutateurs Fabric / routeurs mettant en oeuvre une couche intermédiaire d'agrégation et de commutateurs Spine / routeurs mettant en oeuvre la partie de colonne vertébrale de l'interconnexion.Figure 34 montre une configuration typique des couches de protocole impliquées dans une telle configuration. Habituellement, il y a une couche de tissu qui fournit la connectivité IP entre tous les TDR au DC (en fonction de la taille et aux caractéristiques de la DC, DC tel tissu peut être couche 2 sur la base). Le tissu DC prend en charge plusieurs superpositions de réseau virtuel qui fournissent une connectivité IP privée entre les ressources (machines virtuelles ou des conteneurs) d'un locataire spécifique. superpositions de réseau virtuel sont généralement mis en œuvre par une couche 2 ou 3 solution de réseau virtuel tel que VXLAN ou NVGRE.

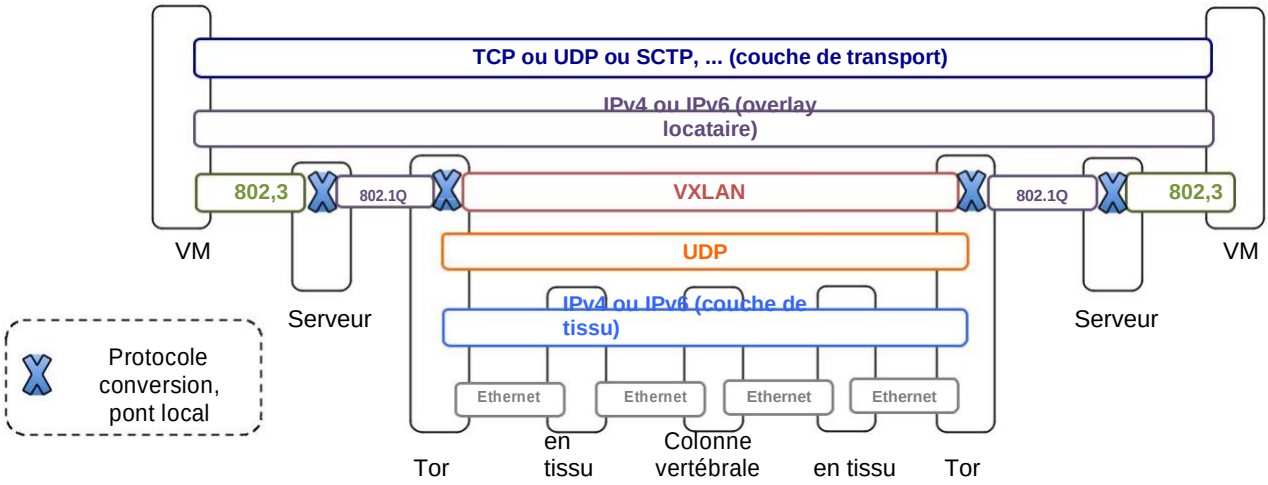


Figure 34: les couches de protocole dans un réseau de centre de données à locataires multiples typique

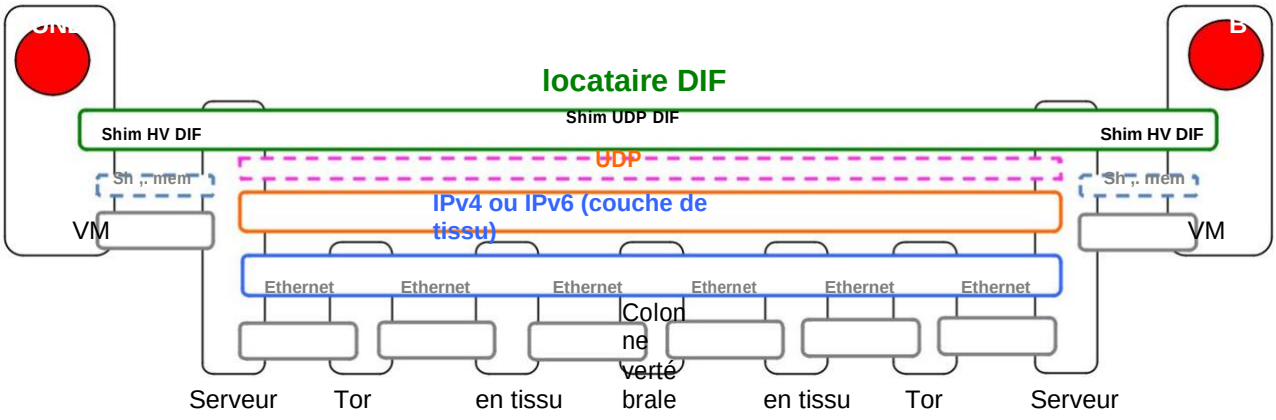


Figure 35: RINA basée sur la configuration de superposition de réseau virtuel

RINA peut prendre en charge les besoins en réseau de contrôleurs de domaine à locataires multiples dans un certain nombre de façons. Une solution logicielle (qui pourrait être basé sur une version optimisée des prototypes de RINA actuels) pourrait mener à bien le travail des superpositions de réseau virtuel, comme illustrerFigure 35. La connectivité entre les machines virtuelles de la même locataire est fourni par un DIF dédié qui se trouve au sommet de la mémoire partagée (par VM de communication hyperviseur hôte) [I.51] ou UDP (pour l'hôte hyperviseur de communication hyperviseur hôte). Dans ce scénario RINA n'est déployé sur les systèmes d'exploitation Hypervisor et VM. Les applications héritées sont prises en charge par l'émulateur sockets, alors que les applications natives RINA peuvent tirer parti de l'API RINA. Une passerelle RINA TCP / UDP peut permettre aux clients sur Internet (ou d'autres réseaux) pour se connecter aux applications prises en charge par le locataire DIF. Le Allocataire permettrait DIF aux clients des appareils compatibles RINA de se connecter au locataire approprié DIF.

En supposant que la disponibilité des mises en œuvre de RINA hautes performances pour les plateformes de routeur (basé sur FPGA, ASICs ou similaire), RINA peut également remplacer le tissu des centres de données IP avec un autre DIF. Un tissu de centre de données à base RINA faciliterait un meilleur contrôle de la congestion à travers le DC[I.52]réduire la taille de la table d'acheminement des routeurs de tissu [I.53] et de simplifier la gestion du réseau des centres de données [I.41].

11.2.2 Communication / Fournisseur de services Internet

noyaux de fournisseurs de services sont sans BGP un modèle de conception suivi par certains fournisseurs de services Internet pour cacher leur routeur principal du reste de l'Internet. routeurs de base prennent en charge le multiplexage et le transport des services VPN IP multiples (ou même Ethernet) entre les routeurs frontières, ainsi que les flux qui prennent en charge le service Internet. Cette conception est décrite dans la figure 36 et généralement mis en œuvre grâce à la technologie MPLS.

routeurs Provider Edge (PE) mettre en œuvre logiques, des cas isolés de moteurs de routage et le routage IP par VPN, appelé VRF (routage et expédition virtuel). Chaque VRF échange avec d'autres routes VRF appartenant au même réseau privé virtuel, le remplissage de la table de routage IP VPN local associé à la VRF. VRFs encapsulent le trafic allant vers le noyau de routeurs (P) avec deux étiquettes MPLS: une représentant le VPN (intérieur) et une autre (externe) pour le fil de pseudo au routeur saut suivant P. routeurs P transmettent le trafic basé sur l'étiquette MPLS externe jusqu'à ce qu'il atteigne le PE de destination, qui traite l'étiquette intérieure pour fournir le trafic à l'instance VRF droit.

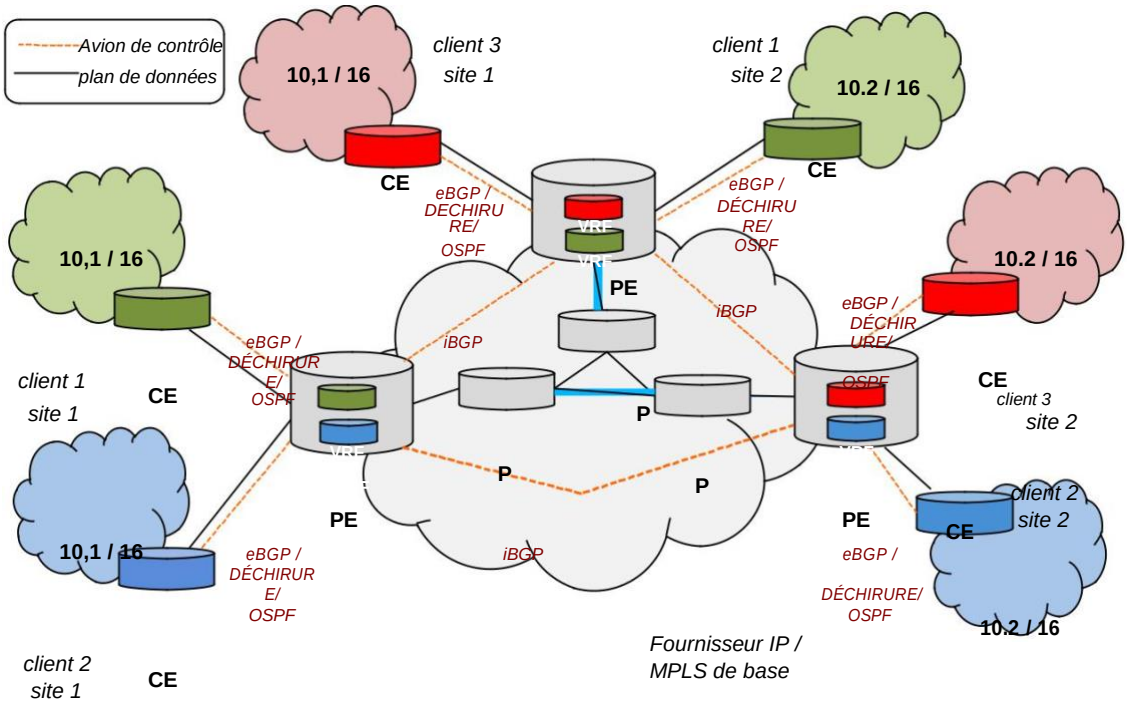


Figure 36: réseaux privés virtuels IP sur un noyau de fournisseur de services BGE sans

RINA peut être déployée dans ce cas d'utilisation comme une alternative à la technologie MPLS, en remplaçant les routeurs MPLS par les routeurs RINA au réseau de noyau comme on le voit Figure 36. instances VRF sont des instances de processus d'application qui enregistrent au DIF orange. Le nom de l'application des instances VRF devrait faciliter la découverte de tous les autres VRF qui font partie du même VPN. Par exemple, la figure utilise une convention de nommage de id VPN comme le nom du processus, identifiant du routeur comme l'instance de processus et une étiquette pour indiquer la nature du VPN (par exemple RINAIP) comme le nom de l'entité (parce que le même DIF peut transporter réseaux privés virtuels de d'autres protocoles). Une fois que les instances VRF sont créés, le système de gestion de réseau demande la création de point à point flux entre les instances VRF appartenant au même VPN. Certains de ces flux peut être dédié à communiquer des informations de commande (par exemple d'échange d'itinéraires via iBGP ou d'autres moyens), tandis que d'autres flux porteront le trafic de données VPN. Par exemple, toutes les instances VRF peuvent affecter un flux de contrôle pour une application agissant en tant que réflecteur de route BGP, puis répartir les flux de données à toutes les autres instances VRF dans le VPN. Ces flux apparaîtraient comme des interfaces de sortie pour le VRF, être en mesure de transférer le trafic IP à travers eux. ARCFIRE a réalisé une mise en œuvre du prototype de l'application VRF activé RINA, appelé le démon iporina[I.54]. Le démon se comporte comme expliqué dans le présent paragraphe, à l'exception qu'il n'utilise BGP pour annoncer les routes (il utilise un mécanisme plus simple à des fins de démonstration).

Très grands réseaux de fournisseurs de services de base bénéficieront de partitionner l'épine dorsale en plusieurs couches pour faciliter mise à l'échelle, qui peut être facilement fait en ajoutant une autre DIF en dessous du DIF orange dans la figure 37. Ce scénario est actuellement à l'étude dans le cadre de l « expérience ARCFIRE 3[I.55].

Le fournisseur de services de communication peut peer avec d'autres fournisseurs de services Internet / CSPs au niveau IP pour échanger des routes Internet ou VPN routes inter-domaines. Cependant, il est également possible d'opérer avec d'autres communes DIF fournisseurs de services qui mettent en œuvre RINA. Ces peuvent également être DIF pris en charge par l'épine dorsale du fournisseur de services activé RINA, en parallèle aux réseaux privés virtuels IP et d'autres services. De cette façon, un CSP compatible RINA peut garder RINA complètement caché dans son cœur de réseau quand il scrute avec les FAI IP, mais il peut aussi exposer à d'autres capacités RINA RINA capables CSPs. La même chose peut être fait pour les clients: ceux qui soutiennent que IP se connectera aux routeurs PE via IP; mais les clients qui sont RINA activés peuvent se voir offrir un VPN RINA au lieu d'un VPN IP.

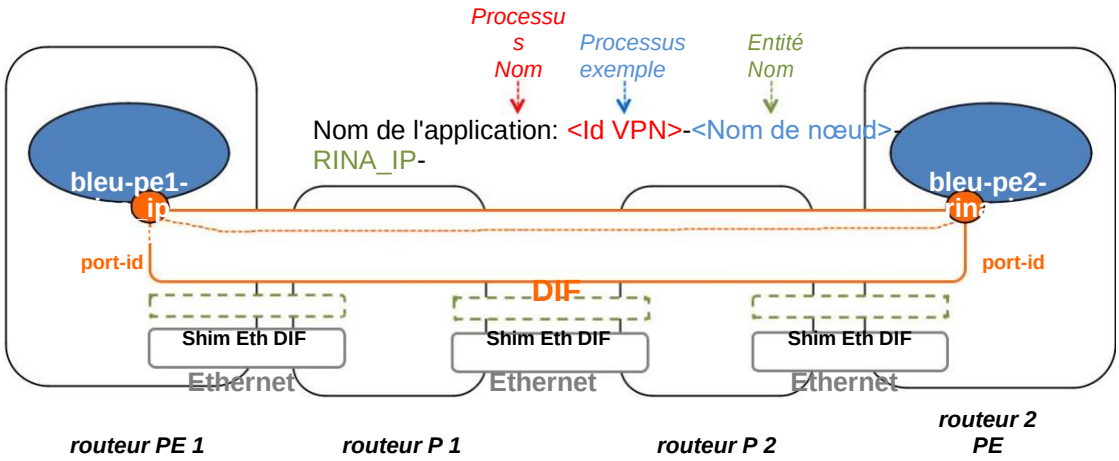


Figure 37: Backbone DIF fournir un écoulement entre deux instances VRF

11.2.3 WAN Software-Defined (SD-WAN)

Wide Area Networks Software Defined (SD-WAN) s apparaissent comme une solution alternative meilleur marché aux circuits dédiés dans le segment de la connectivité WAN. Utiliser des cas tels que la connectivité des succursales aux bureaux ou à un accès sécurisé nuage ont été la cible initiale de cette technologie. solutions SD-WAN sont généralement déployés entre les bords des clients et des fournisseurs (pour le client en nuage) ou entre la branche et les bords du bureau central. SD-WAN sont en mesure d'exploiter et d'optimiser des services multiples de connectivité sous-jacents disponibles sur les bords des clients (Internet, un circuit dédié, l'accès sans fil), le routage des flux généralement appartenant à une variété d'applications par le biais de différents supports en fonction des politiques définies par le client. Gestion des routeurs de périphérie SD-WAN est généralement effectuée à partir d'un emplacement centralisé, qui peut être un centre de données privé qui appartient au propriétaire SD-WAN ou un nuage public en cas d'une solution hébergée. Ce scénario est présenté dansFigure 38.

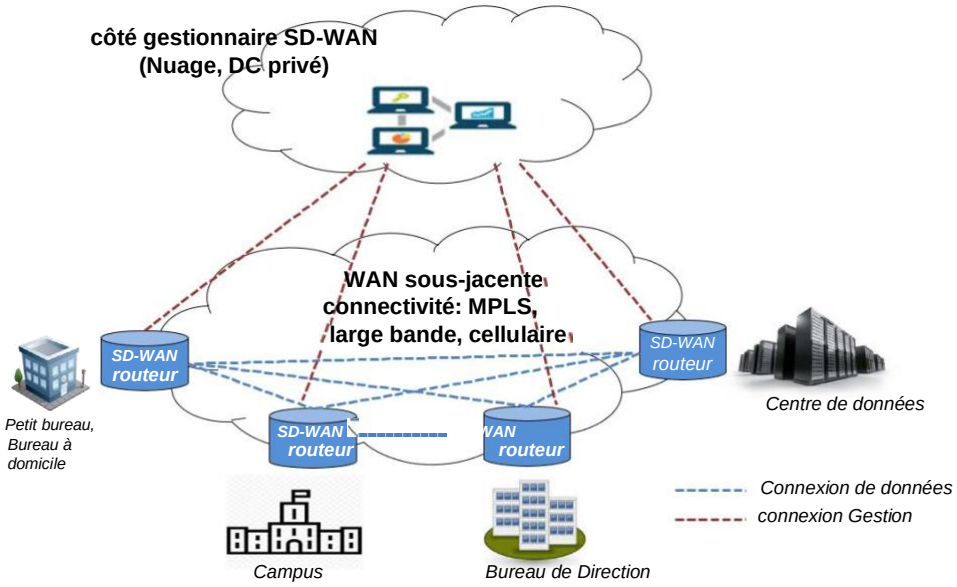


Figure 38: typique scénario SD-WAN

Le routeur logiciel SD-WAN est généralement configuré pour identifier différents flux IP (basé sur le 5-tuple), les classer dans des classes différentes, appliquer en option une sorte de mécanisme de sécurité, puis de les transmettre par l'une des interfaces sous-jacentes (par exemple à large bande ou circuit MPLS). Le fonctionnement du routeur SD-WAN peut impliquer effectuer la traduction d'adresses réseau (NAT), la réécriture l'en-tête IP pour ajouter des informations supplémentaires ou chiffrer des champs, etc. RINA peut fournir une solution propre au problème SD-WAN en tirant parti de DIF et leur Propriétés.Figure 39 montre un scénario simple, dans lequel on utilise un seul pour offrir un DIF de service SD-WAN sur plusieurs sites.

Figure 39 montre un exemple d'un routeur SD-WAN basé RINA. Un DIF SD-WAN se trouve au sommet des différentes technologies qui fournissent une connectivité WAN vers le côté client: dans cet exemple, une connexion à large bande xDSL et un circuit MPLS. Le flux vers alloue DIF la N-1 sur chacun DIF des technologies à tous les autres routeurs SD-WAN qui sont les plus proches voisins (la procédure de découverte peut être autonome ou orchestrée par le système de gestion). Ensuite, le système de gestion de réseau créé différents flux entre les machines de protocole IP de couches IP costumier (en rouge) à chaque routeur SD-WAN. Ces flux multiples offrent différentes options de QoS aux flux IP. Les machines de protocole IP classifient les paquets IP en fonction des flux auxquels ils appartiennent (spécifié via le Network Management System), et ensuite les transmettre à travers un des flux fournis par le DIF SD-WAN. Le DIF transmettra les paquets au saut suivant selon la qualité de service annoncés par le flux, donc des flux IP sera transmis, si le circuit MPLS et d'autres via le lien à large bande. Le DIF peut également définir des stratégies de protection en fonction des caractéristiques de l'écoulement N-1, et peut donc chiffrer les données qui sont transmis par la liaison à large bande.

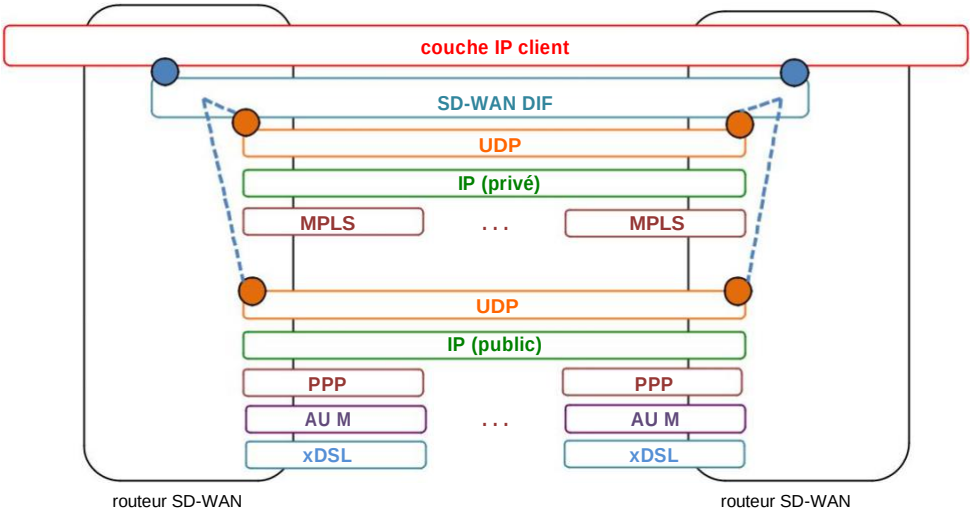


Figure 39: RINA à base de routeur SD-WAN

Annexe A:
Auteurs et contributeurs

Les personnes suivantes ont contribué au présent document:

Rapporteur:

Dr. Eduard Grasa, Fundació i2CAT, eduard.grasa@i2cat.net

Autres contributeurs:

Dr John Day, l'Université de Boston, jeanjour@comcast.net

Miquel Tarzan, Fundació i2CAT, miquel.tarzan@i2cat.net

Dr Diego López, Telefónica, diego.r.lopez@telefonica.com

Kevin Smith, Vodafone, kevin.smith@vodafone.com

Annexe B:
Historique des modifications

Date	Version	Informations sur les changements
mai 2017	0.0.1	Table des matières
novembre 2017	0.0.1	projet de début, contenu ajouté aux clauses 5.3, 7 et 10
août 2018	0.0.2	Complète projet de clauses 4 et 5, les fautes de frappe fixes et quelques chiffres dans d'autres clauses
septembre 2018	0.0.3	Changement de GS à GR, adapté titre et la portée
septembre 2018	0.0.4	l'article 6 Ajout projet
septembre 2018	0.0.5	clause ajoutée 8 et 9 projet
septembre 2018	0.0.6	projet stable
novembre 2018	0.0.7	projet stable, après le nettoyage Edithelp
novembre 2018	0.0.8	Les contributions de Vodafone intégrée
décembre 2018	1.0	rétroaction intégrée de # NGP13 réunion

Histoire

Historique du document		
V1.1.1	février 2019	Publication