MPLSによる
ブロードバンドアグリゲーション
ネットワークの構築

矢頭 俊英

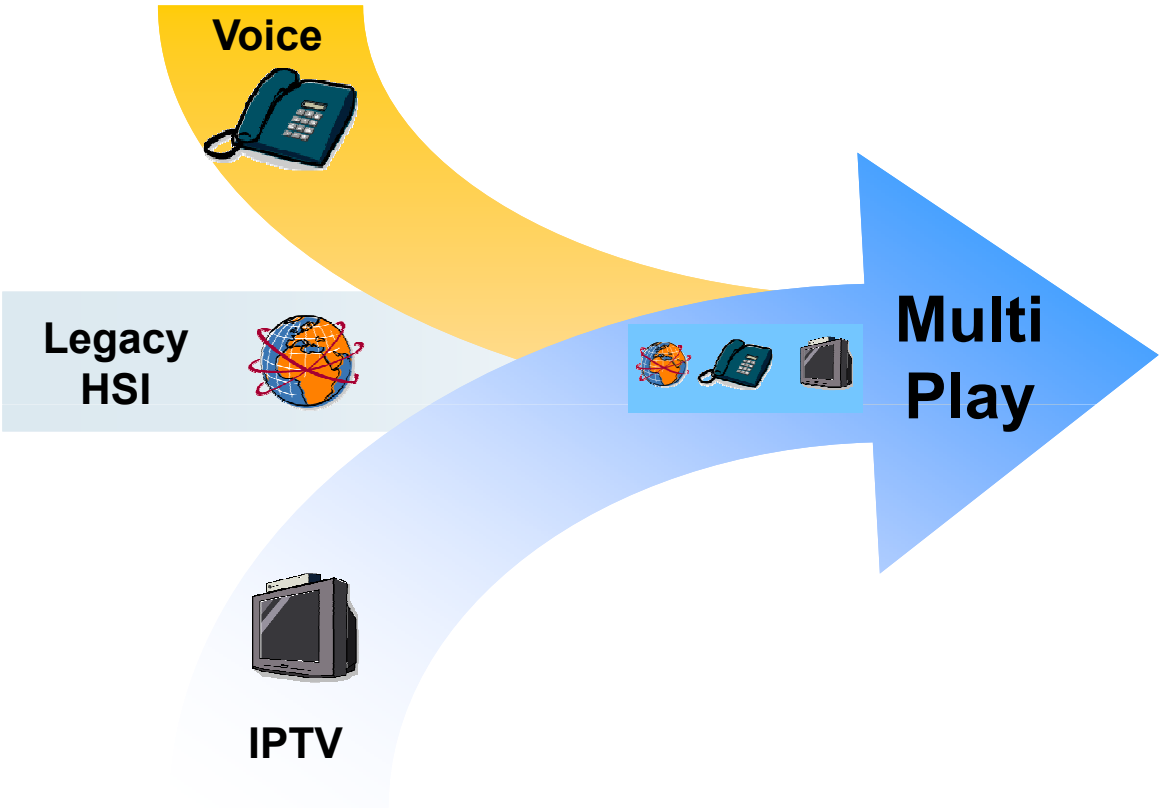
日本アルカテル・ルーセント

Agenda

1. 概要
2. 加入者管理
3. Multicast
4. QoS/CAC
5. 接続先指定接続・ホールセール

1 概要

今更ながら･･･Multi Play



1 ATMからEthernetへの
マイグレーション

コストと帯域の最適化

2 Fiberアクセス回線
(VDSL2, PON)

加入者アクセスの広帯域化

3 加入者アクセスの
コネクションレス化

プラグ&プレイ

4 BEインターネット接続から
常時接続のマルチサービスに

ユーザエクスペリエンスの
品質向上･多様化

MPLSによるブロードバンドアグリゲーション – 他国のケース

DSLAMのEtherアップリンク化・FTTH導入による広帯域化とサービスのmulti play化が同時

- 欧州では2006年のワールドカップへ向けての導入が多かった

サービス網統合

- モバイルバックホール
- 企業向け広域Etherサービス

脱・PPP

- 接続先指定接続以外では使い続ける価値無し?

純L2ベース、L3ベースのアグリゲーションと比較して・・・

- 切替えが高速 (FRR)
- 他のサービスとインフラ共有(仮想L2/L3インスタンス)
- 物理トポロジに関係無くL2/L3インスタンスが繋げられ、設計の柔軟度、スケーラビリティが高い(MS-PW、H-VPLS、PW termination on L3VPN…)

構成要素

加入者管理

ブリッジング(VPLS)インスタンス

- 加入者 or サービス毎のブロードキャストドメイン作成
  (但し、同一VPLS内でもL2 reachablity的に分離する事は可能)
- MAC/multicast snoopingテーブル分け
- PseudowireのL2集約

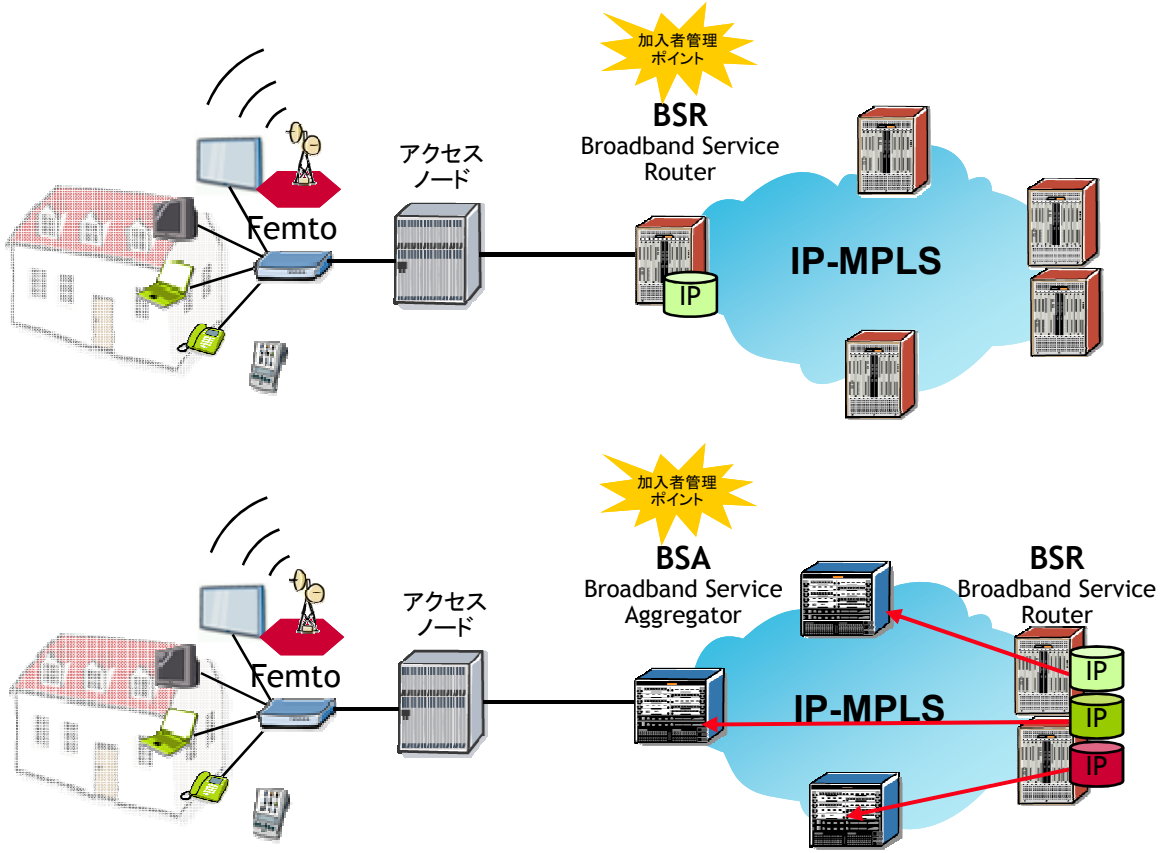
ルーティング(L3VPN)インスタンス

- 加入者のL3 first-hop
- ISP毎のVPN分け

Pseudowire

- 主にL2ベースでのトンネルとして使用
- L3VPN/VPLSの仮想インタフェースとして使用可能

2大導入モデル - Routed CO vs Bridged CO



Routed

- ルータによるアクセスノード収容
- PWによるEthernet以外のサービス(ATM、TDM等)収容や、CO折り返しが必要な場合に有効
- 全ての加入者トラフィックに対してサービス関連機能(DPI、SBC、NAT等)を提供すると高くつく

Bridged

- BSAによるアクセスノード収容
- BSA – BSRをpseudowire(H-VPLS spoke)で接続
- Routed COに比べ、加入者管理ポイントを変えずに低価格化が可能
- 高付加価値機能は集中配置

2 加入者管理

加入者管理の定義

アクセスプロトコルセッション(PPP/DHCP)情報に応じ加入者毎に下記のような機能を提供

- 加入者の単位
  - DHCP: DHCPクライアント (IP/MACアドレス、VLAN)
  - PPP: PPPoEクライアント(VLAN/MACアドレス、session ID)
- 加入者の識別、AAA、アドレス配布
- 加入者へのQoSポリシーの適用によるサービス・アプリケーション毎のSLA保証
  - 加入者間fairness
  - アプリケーションの差別化
- 認証・許可されていない加入者のアクセス制限
  - なり済まし防止
  - ACL
  - DDoS防御
- 加入者ステートの保持、サービスの継続性
- トラブルシューティング・OAM
- トラフィックの法的傍受

PPP vs DHCP

	PPP	DHCP
Authentication	LCP認証によるユーザ識別	Option 82によるユーザ識別
Authorization	RADIUSベースのauthorization	DHCPサーバ、RADIUS等によるauthorization
Accounting	BRAS/BSRによるRADIUS accounting	BRAS/BSRによるRADIUS accounting
加入者ステートの監視	PPP LCP keepalive	ARP keepalive
Multicast	Point-to-pointプロトコルのため、multicast replicationが非効率的	効率的なmulticast replication
クライアントへの要件	PPPoEサポートが必要	基本的にどのIPデバイスでもOK
対応クライアント	VoIP/STBデバイスではサポートされていない事も多い	ほぼ全てのデバイスでサポート
Femtoサポート	プロトコルオーバーヘッド増加、QoS差別化が難しい	オーバーヘッド無し、QoS差別化容易
加入者のサポート	プロトコルレイヤの多段化により切り分け難易度高、サードパーティ製クライアントソフトのサポート	L2/L3レベルの比較的容易なトラブルシューティング
冗長性	シャーシ内の冗長性の部分的なサポート(切替り中は新規呼受付付加、等)	シャーシ内、シャーシ間の冗長性サポート
ホールセール	L2TP・VR/VRF選択	DHCP+RADIUS、802.1x、web認証 with L3VPN/L2VPN

DHCPの特徴

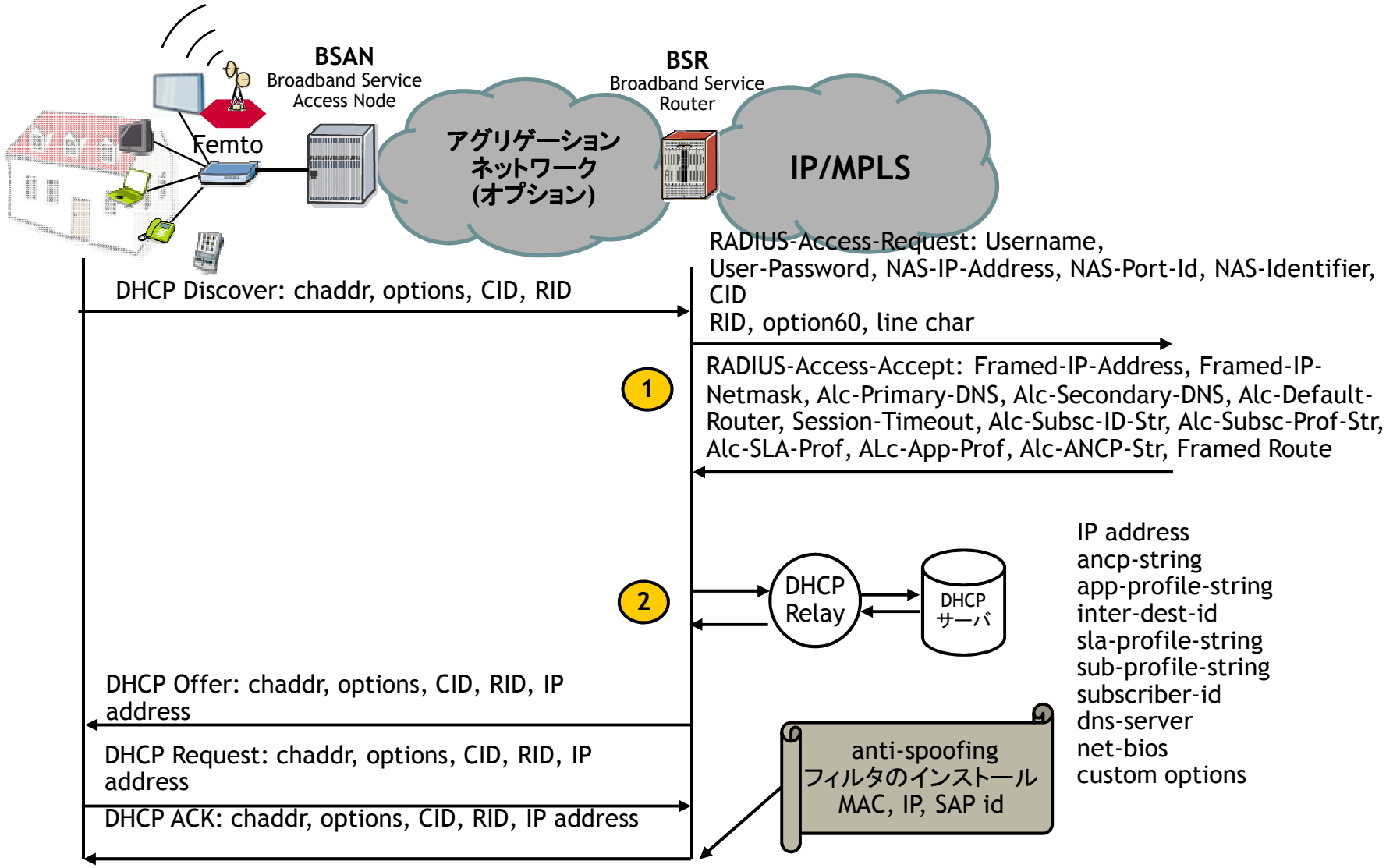
他の加入者アクセスプロトコル(PPP/L2TP、IPSec)と比較し、以下の点が相違

- 一般的なクライアント・サーバ実装においては認証方法が無い
  - 他の認証方法(EAP、web認証等)と組み合わせる必要がある
  - Option 90、PANA+option 136等あるが、まだ誰も使ってない風?
  - Option 60に無理矢理認証情報を埋められなくはないが・・・
- トンネリングプロトコルではない
  - 加入者・OLT – 加入者終端点(L3 first hop)間に他のプロトコルによるトンネルが必要(VLAN/pseudowire/VPLS/L3VPN等)
  - マルチキャストとの親和性が高い
- EAPや何らかのDHCP optionの埋め込みを必要としない限りはクライアント側の設定やソフトウェアのインストールは特に必要無し
  - Plug & playが実現可能
- PPPoE(oA/oE)からのmigrationが容易
  - RFC2684 bridged encap
- L2TP等のような呼制御的概念が無い
  - キャパ計画が困難だったが、multi play化に伴う常時接続化により手間が減ってきた

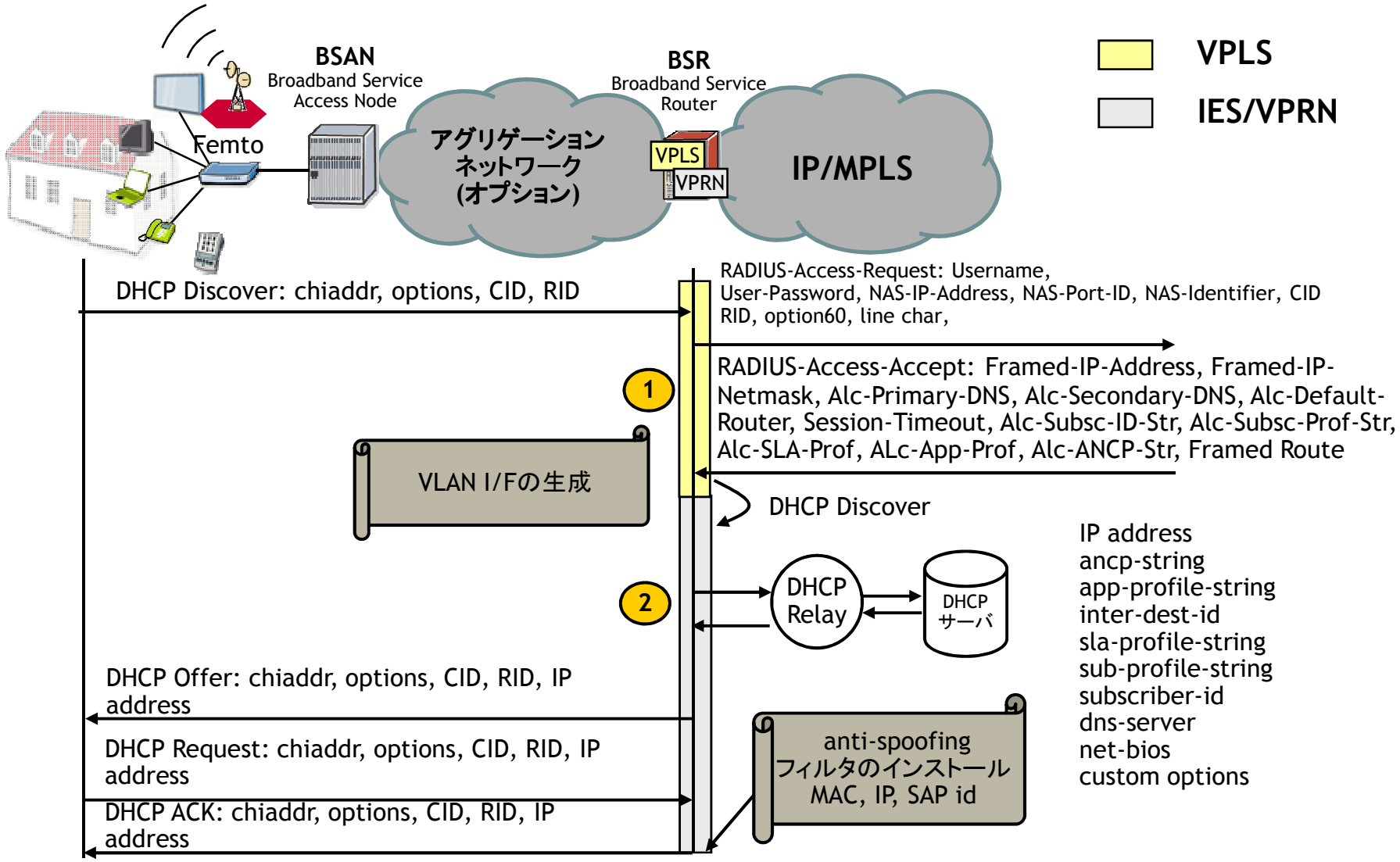
DHCP関連機能

- DHCP to RADIUS
  - DHCP discoverパケットの内容をRADIUS Access-Requestとして送信
  - RADIUSサーバからのAccess-Acceptに含まれるAVP(ポリシー等)をクライアントに適用
- VLAN auto-sense
  - DHCP/PPPパケットをトリガーに、VLAN単位の仮想I/Fを生成
  - VPLS or ルーティングインスタンスにマッピング

DHCP to RADIUS 接続シーケンス例



DHCP to RADIUS 接続シーケンス例 (with VLAN auto-sense)



EAP認証

L2スイッチや無線APの動的VLANアサイン機能による接続選択

- MACベース認証が必要
- VLANスケーラビリティに難

L2デバイスによる認証情報とBSA/BSRでのDHCP to RADIUS機能とのマッピング

- ALU 5750SSCによる実装例

  5750SSCにて、EAP認証時の情報をベースにDHCP用の加入者エントリを自動生成
  (デフォルトではEAP認証時のNAS-portをDHCP option 82に変換)

  7x50によるDHCP to RADIUS認証時にoption 82による加入者識別、サービス振分け

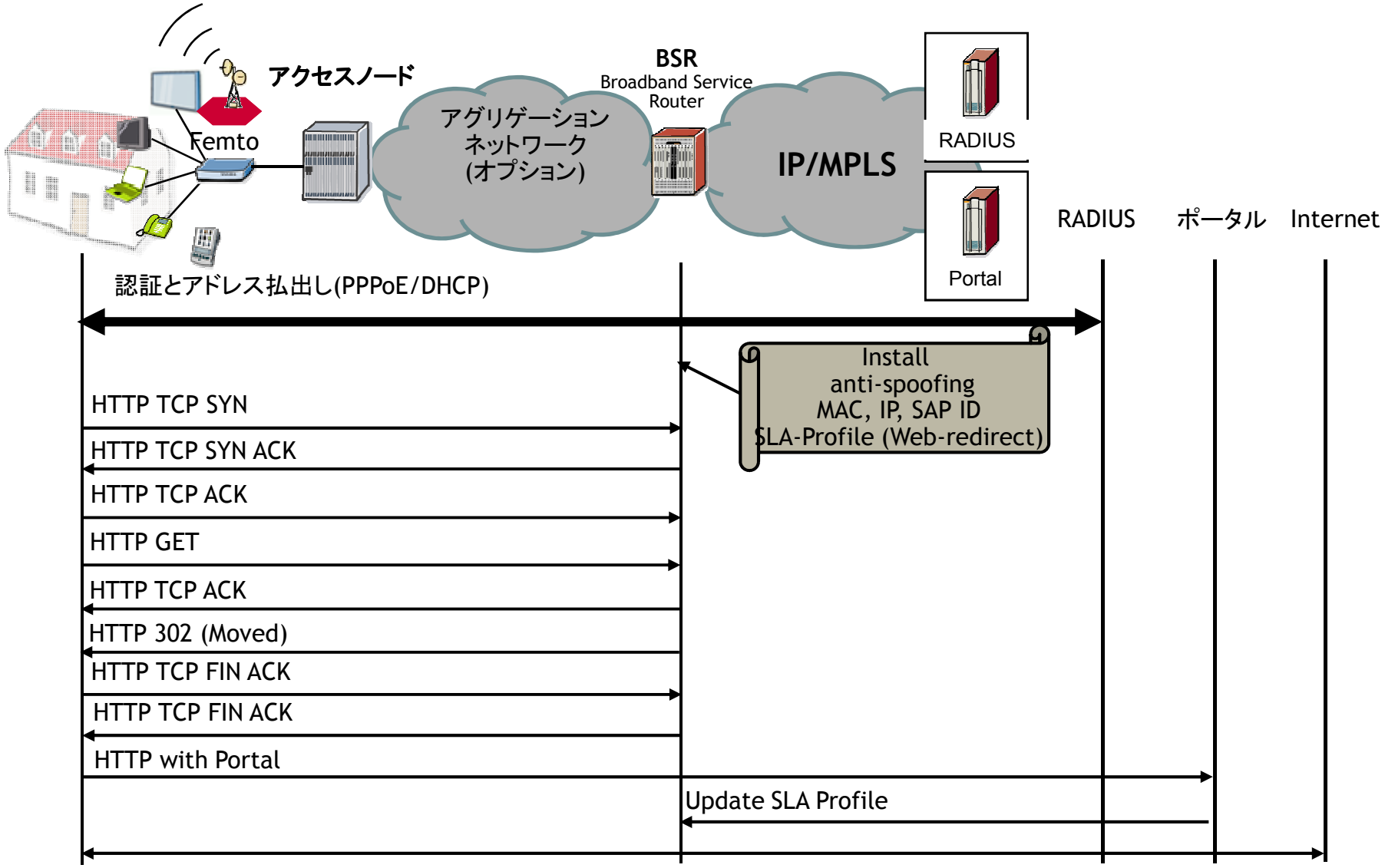
  上記認証情報マッピングはスクリプトにより行われており、スクリプトのカスタマイズによりその他の情報(MACアドレス)等をキーにしたマッピングも設定可能

Web認証

ポリシーサーバ、ポータルと組み合わせた使用例

1. 初期接続時、加入者にアドレス払出し(+ webポータルへのHTTP redirectionポリシー)
2. 加入者がwebブラウザを立ち上げるとポータルへリダイレクト
3. 認証・ISP選択用のwebページ表示、加入者は認証情報を入力
4. Webポータルよりポリシーサーバに加入者サービス情報を送信、ポリシーサーバが加入者情報をアップデート
5. DHCP leaseのlease expireもしくはFORCE-RENEWによりISP用プールアドレスの払出し
6. インターネット接続確立
7. 接続先変更時にはwebポータルに再アクセスし、認証情報を再入力

HTTP Redirectionによるユーザ認証



3 Multicast

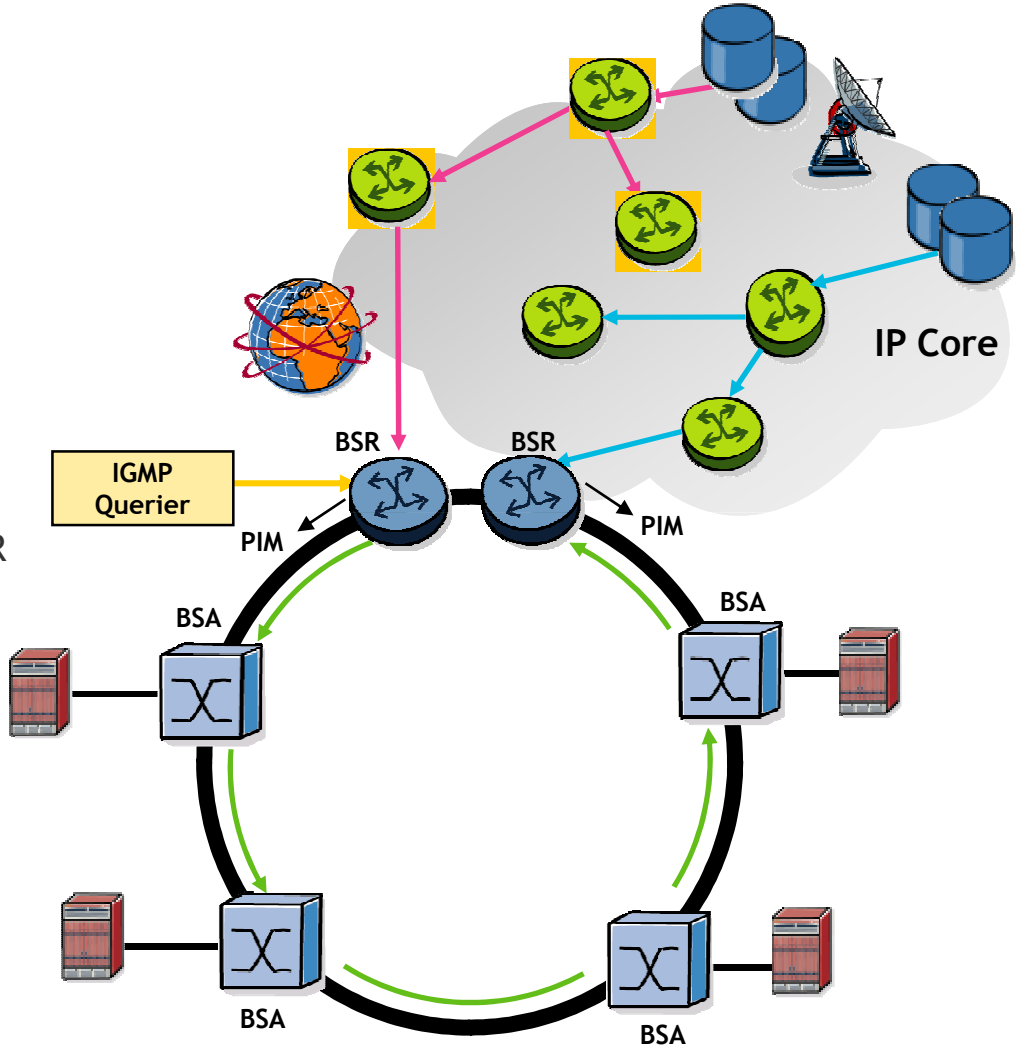
典型的なBridged COモデルにおけるMulticast転送構成例

基本ポリシー

- Core区間は2つのソースからのP2MP LSPによる”垂れ流し”
- メトロ・アグリゲーション区間はBSA間をH-VPLS spoke接続+path protection
- IGMP/MLD snoopingによりトラフィック量を抑制
- MVRにより最終replicationポイントを加入者の近くに持って行く

2台のBSRによるP2MP LSP終端、1台がPIM DRとして動作

- P2MP treeを2つ作る事により、ソースを冗長構成
- 通常時は1台のBSRがIGMP querierとして動作
- BSR障害はBFD for PIMにて検知



プライマリソース用P2MP LSPツリー

セカンダリソース用P2MP LSPツリー

BSR = Broadband Service Router

BSA = Broadband Service Aggregator

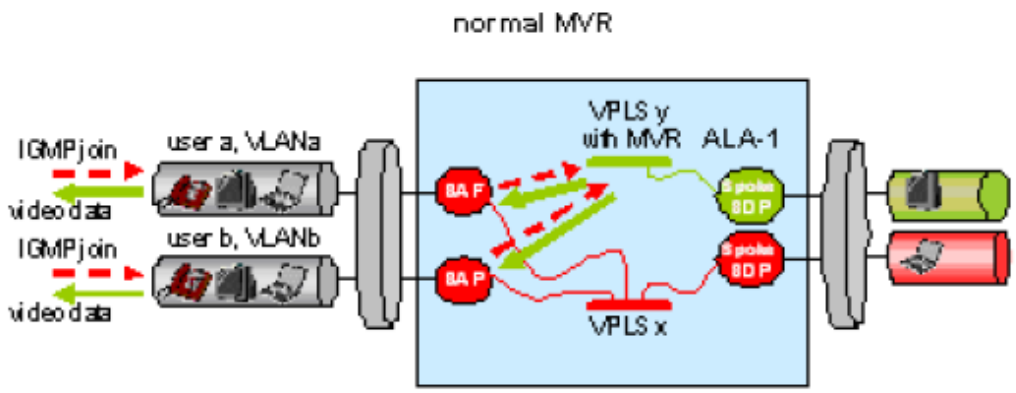
Multicast VLAN/VPLS Registration (MVR)

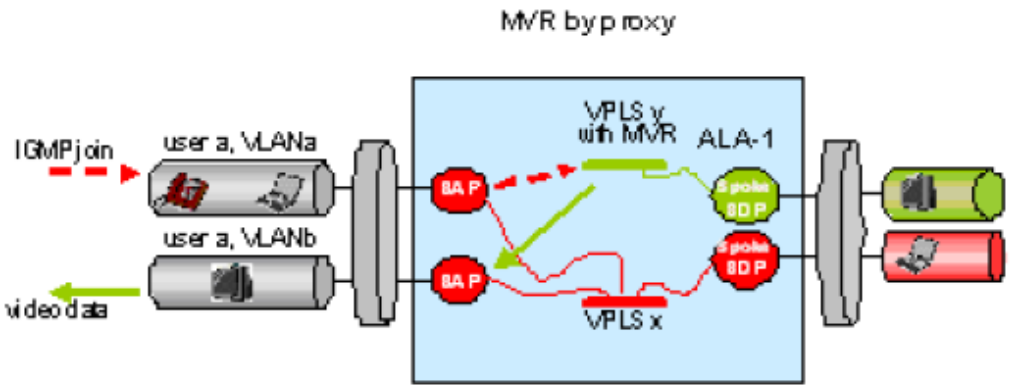
ネットワーク全体の”multicast VLAN/VPLS”上で転送されるストリームに加入者がjoin可能

- 加入者毎VLAN構成においてもCO局上でのreplication
- ルーティング・VPLSインスタンスに関わらずmulticastストリームを渡せる

MVR by Proxy

- MVR VPLS上のストリームをIGMP/MLDを受け取ったVLANとは違うVLANにコピー
- DSLAM/OLT上でのマルチキャスト配信効率化機能を使う場合にも有効



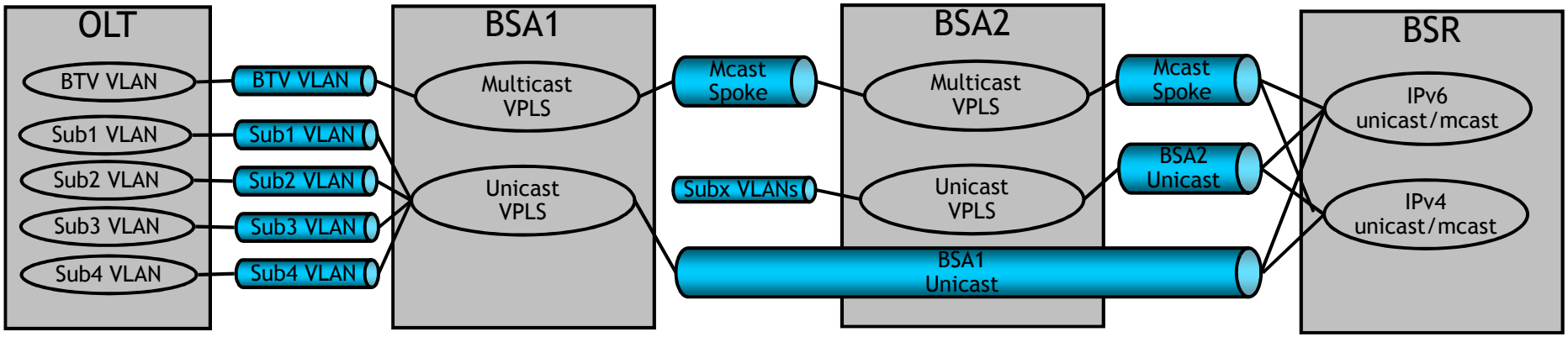


コネクションモデル – Unicast + Multicast

UnicastはBSR – 各BSA間でHub&Spoke

加入者間共有、サービス毎、もしくは加入者毎のVPLSインスタンス

- 接続先ISP毎にVPLSインスタンスを分けたい場合
- Unicast VPLS側にもmulticastを流したい場合



4 QoS/CAC

加入者QoS機能の変遷

初期の加入者管理:

- 加入者のAAAとインターネットアクセス帯域のfairness

第二世代の加入者管理:

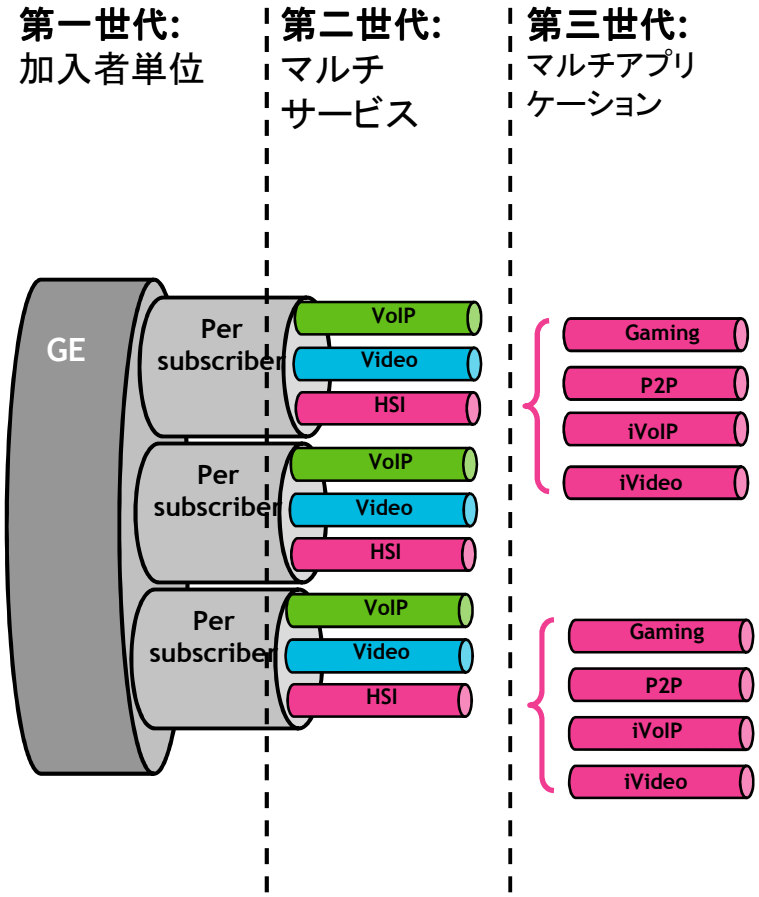
- 加入者間の帯域fairnessとサービス毎のキューイング

第三世代の加入者管理:

- DPIによるアプリケーション単位でのデータトラフィック識別

  P2P、OTTビデオトラフィック対策

  アプリケーションに特化した新サービスの可能性



2つの親スケジューラを持つキューイングモデル

- トラフィッククラス毎→加入者毎の階層化QoSモデル

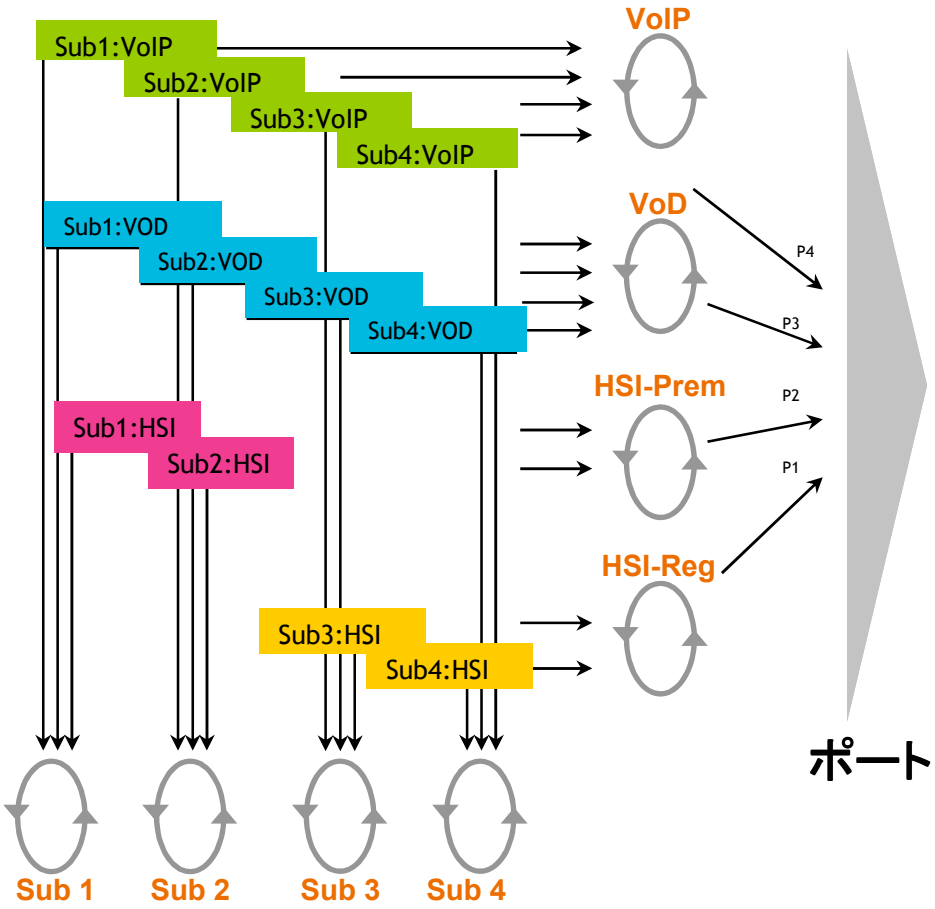
  加入者・位置に関わらずアプリケーションベースの優先度に基づいた第一階層のスケジューリング
  (加入者毎キューをベースにした階層化では高優先度キューの遅延が大きくなる)

  加入者毎にアプリケーションの帯域幅を指定

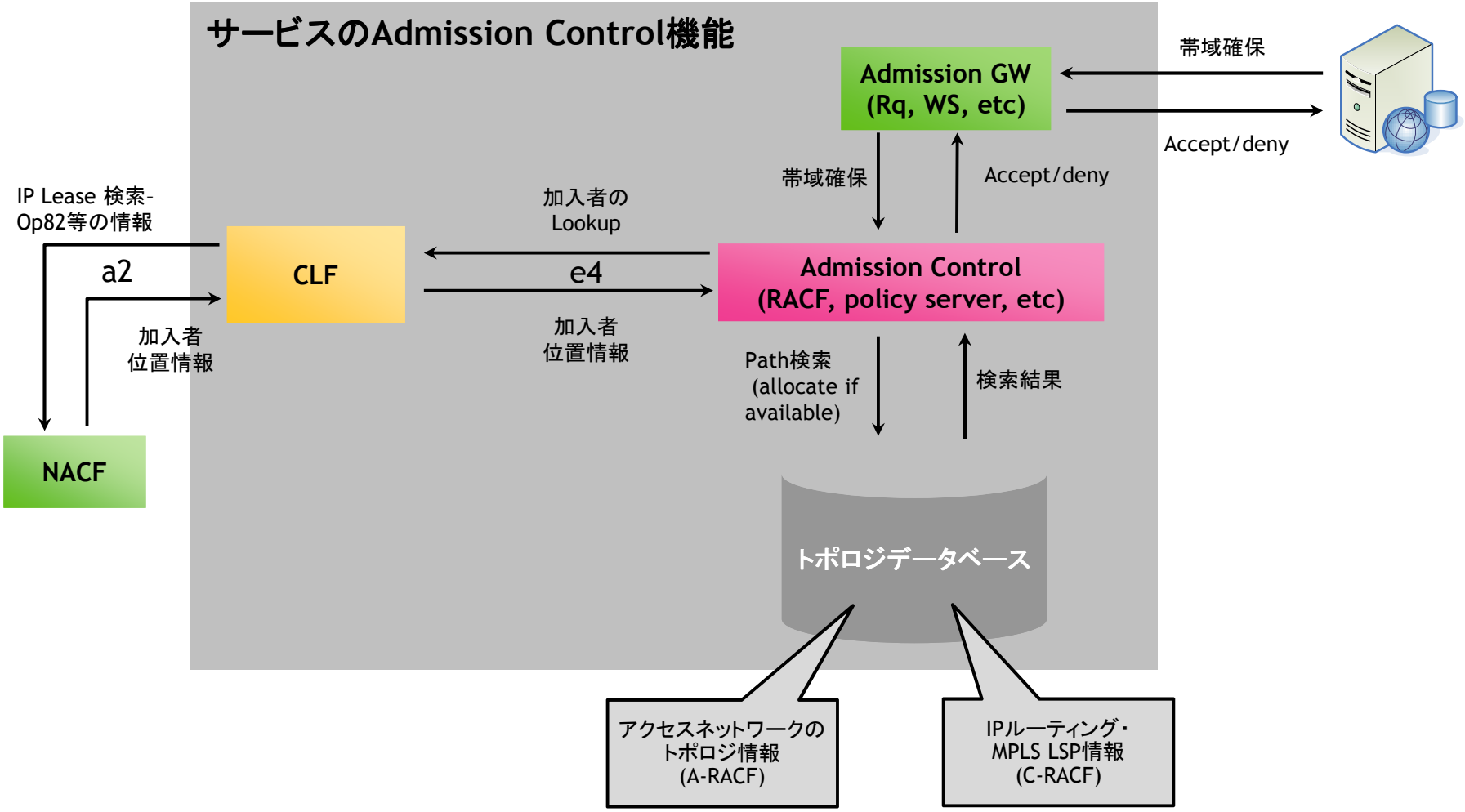
- 2つの親スケジューラを持つ加入者毎クラスキュー

  各キューはポート上のクラス毎キュー階層に所属→加入者間fairness

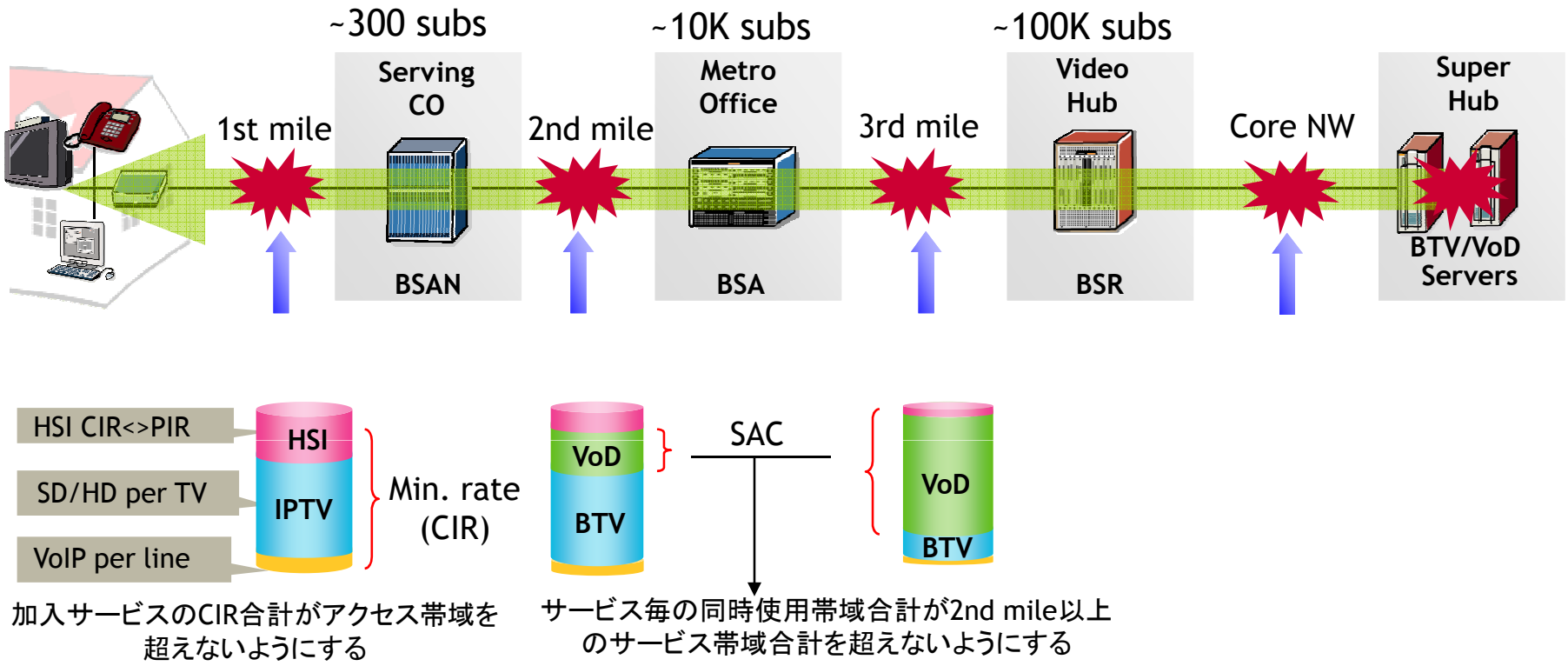
  加入者毎のスケジューラにも所属し、契約帯域に応じてshapingされる



Unicast CAC - ワークフロー



End-to-EndのCAC



ポリシーベースのCAC

- サービス種別、アプリケーションフロー単位の帯域計算
- 加入者毎の加入サービス判別 (HD, SD, etc)
- 高優先度チャンネル(緊急時放送、911呼等)の保護
- …

Multicast CAC

既存のIGMP/MLD CAC

- Joinしている(S,G)数のみをカウント
- チャンネル毎の帯域、優先度等の差別化は不可能

拡張Multicast CAC

- CACポリシーにより、チャンネル毎の帯域・優先度情報を保持
- ポート毎、加入者毎、チャンネル種別(HD、SD, etc)毎の帯域チェック

CACを行うデバイスが最終replication pointでなければならない

- 下流にsnooping/replicationを行う機器がいると、意味無し

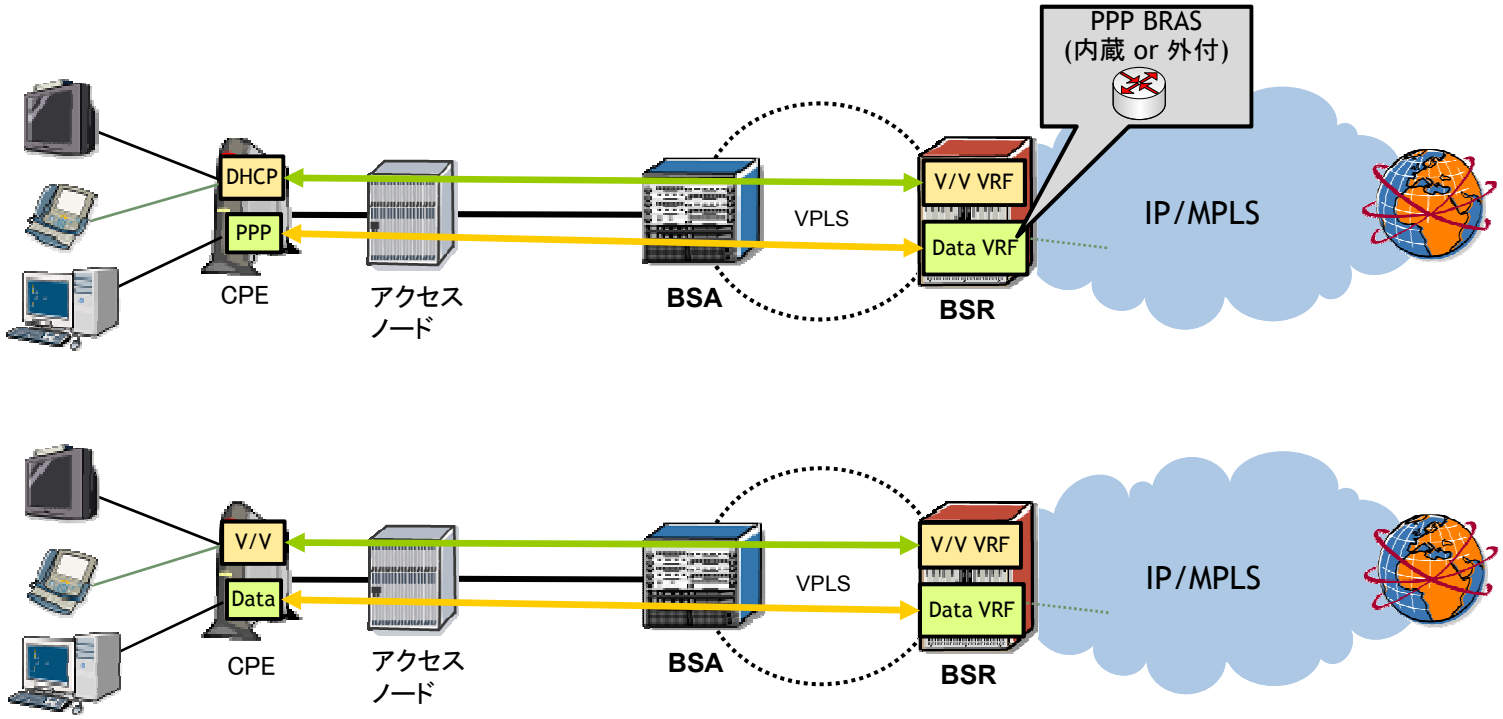
5 接続先指定接続・ホールセール

DHCPアクセスモデルにおける複数接続先サポート

ISP・企業アクセス等毎に別のルーティングインスタンスに収容

従来使われてきたモデル

- インターネットアクセスはPPP、それ以外はDHCP
- STB、ルータ等機能ブロック毎に別々のDHCPクライアント



ISP選択 or ホールセール?

手動での接続先ネットワーク選択

- 802.1x EAP認証もしくはWeb認証

接続先ISP固定のホールセール

- 前項のような加入者管理機能を使用し、加入者毎に接続先を決め打ち
  - NAS-Port、DHCP option 82、MACアドレス等により加入者識別
  - Web認証による半固定
- DHCPのplug & play的特長を活用
- ISPによるユーザ識別やaccountingが困難
  - Web認証であればISP RADIUSに飛ばせる
  - MACアドレスやcircuit ID等をキーにする?

今後の課題 - 加入者端末のSoC化

CPE設計の効率化の結果、単一DHCPクライアント・単一TCP/IPスタック化

ホールセール的サービスとmultiplayの同居が困難に

如何にサービス毎に振り分けるか?

- ポリシールーティング?
- DPI?
- Softwire or PPP?

　手軽なIPv6対応には使えるが、IPv4では同一IPスタックに乗るため意味無し

とりあえずルーティングベースで考えてみるが・・・

- ISP毎にルーティングインスタンスを分け、その他のサービスにNAT接続
- 全ISPで同一のアドレス空間を使用し、ISPに渡すところでNAT

6 まとめ

まとめ

日本では今から新規網を作る事はあまり無いかもしれないが、ポイントソリューションとしての適用可能性はあるのでは?

- L2アグリゲーション網を作る時
- 新規にアンバンドルサービスメニューを追加
- PPP→DHCPのマイグレーション時のソリューションとして
- ATM→Etherのマイグレーション時のソリューションとして

  過渡期のPPPoAはどうする?

www.alcatel-lucent.com