

ポリシーベースのネットワーク管理における分散アーキテクチャの提案

3H-08

吉原 貴仁

堀内 浩規

小田 稔周

(株) KDD 研究所

1 はじめに

電子商取引や企業業務など、インターネットの商用化にともない、限られたネットワーク資源の有効利用が重要性を増し、ユーザやアプリケーション毎にカスタマイズした通信品質の確保が急務となっている。近年、このためのポリシーベース管理^[1]が注目され、ポリシーサーバ等のツールが入手可能である。

ポリシーベース管理では、ネットワークの利用状況に応じたポリシーのチューニングが必要である。しかしながら、従来のツールでは利用状況の監視結果からチューニングに重要な管理情報を運用者が別途収集する必要があり、利用状況に応じた実時間でのチューニングは困難であるという問題点がある。

本稿では上記問題点の解決の一環として、分散ネットワーク管理方式に基づき、ポリシーベース管理に必要な処理を記述した管理スクリプトを被管理装置に投入して実行させ、個々の被管理装置内でネットワークの利用状況に応じたポリシーのチューニングを実時間で行わせる、ポリシーベースのネットワーク管理における分散アーキテクチャを提案する。

2. 従来のポリシーベース管理とネットワークの利用状況に基づくポリシー決定の必要性

2.1 従来のポリシーベース管理

IETF(Internet Engineering Task Force)等によりアーキテクチャ(図1)をはじめとするポリシーベース管理の標準化が進められている。ポリシーは、以下のように、条件部と条件部を満足する場合に適用する動作部からなる。条件部には送受信 IP アドレス、ポート番号、および TOS(Type of Service) フィールド値などを指定する。動作部には、例えば、送信優先度の変更や輻輳時のパケット廃棄など、優先制御や帯域制御を指定する。

```
if (SrcIP == 192.1.0.0/24 &&  
    SrcPort == 80) /*条件部*/  
    queue_priority = 2; /*動作部*/
```

はじめに運用者はポリシーの決定(図1(1))を行う。決定したポリシーはLDAP(Lightweight Directory Access Protocol)等によりディレクトリサーバに蓄積し、再利用できる(図1(2))。ポリシーの配信のプロトコルにはCOPS(Common Open Policy Service)、SNMP(Simple Network Management Protocol)、およびCLI(Command Line Interface)等を用いて、ポリシーサーバからルータやスイッチ等の被管理装置に配信して(図1(3))実行する。また、ポリシーサーバ以外にも、ディレクトリサーバから配信したり(図1(4))、負荷分散や耐障害性のため、複数のポリシーサーバを配置し、ディレクトリサーバから(図1(5))slave ポリシーサーバを経由して被管理装置に配信して実行する(図1(6))。

被管理装置でのポリシー実行機構として Differentiated Service (Diffserv) (図2)^[2]がある。条件部に送受信 IP アドレスやポート番号など複数の値の組 (MF (Multi-Field) classifier) を指定し、ネットワークの入口の Edge インタフェースでパケットを分類して DSCP (Diffserv Code Point) を付与する。Diffserv ネットワーク内では、条件部に DSCP の値 (BA (Behavior Aggregate) classifier) を指定し、Core インタフェースでパケット

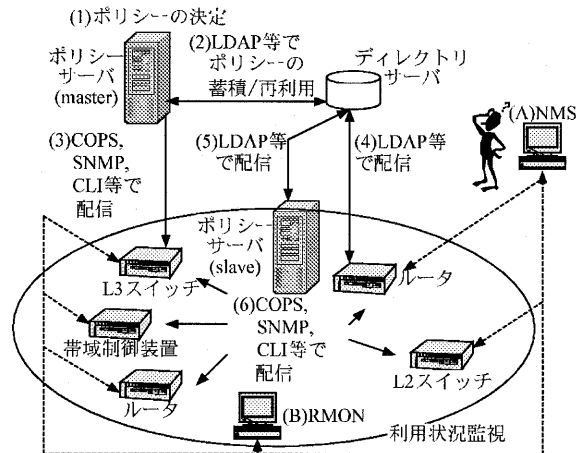


図1: 従来のポリシーベース管理アーキテクチャ。

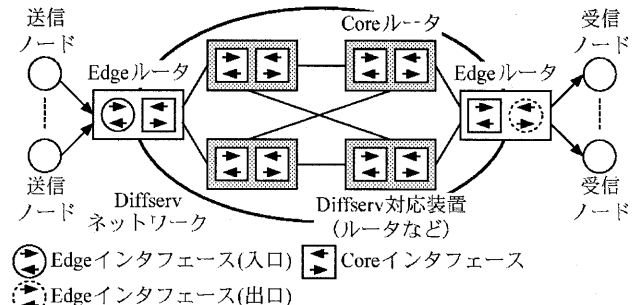


図2: Diffservの概略。

を分類して優先制御や帯域制御を行う。DSCPは出口のEdgeインタフェースで取り除く。

2.2 ネットワークの利用状況に応じた実時間でのポリシーのチューニングの必要性

ユーザ数やネットワークトラフィックの増大、および新規アプリケーション導入などにより、一般に、一度配信したポリシーがいつまでも有効に機能するとは限らず、決定したポリシーのチューニングが必要である。このためポリシーベース管理では、1) ポリシーの決定、2) 決定したポリシーの配信と実行、ならびに3) ポリシーの適用効果を評価するネットワークの利用状況監視からなる一連の繰り返しを実時間で行う必要がある。

従来、ポリシーサーバは決定したポリシーを配信するだけであり、監視結果からポリシーのチューニングに重要な管理情報を運用者がネットワーク管理システム(NMS)(図1(A))やRMON(Remote Monitoring)(図1(B))を使って別途収集、解析する必要があり、ネットワークの利用状況に応じた実時間でのポリシーのチューニングは困難である。

3. 分散ポリシーベース管理アーキテクチャの提案

提案する分散アーキテクチャを図3に示す。

3.1 前提

ポリシーの実行、適用効果の評価に必要な管理情報の監視、ならびにネットワークの利用状況に応じたポリシーのチューニングなど、ポリシーベース管理に必要な処理を記述した管理スクリプトを分散ポリシーベース管理システム(図3)から被管理装置に投入ならびに実行できる環境^[3,4]とする。また、被管理装置で実行できない場合には管理スクリプトの実行環境を提供す

Proposal of Distributed Policy-based Management Architecture

Kiyohito YOSHIHARA, Hiroki HORIUCHI,
and Toshikane ODA
KDD R&D Laboratories Inc.

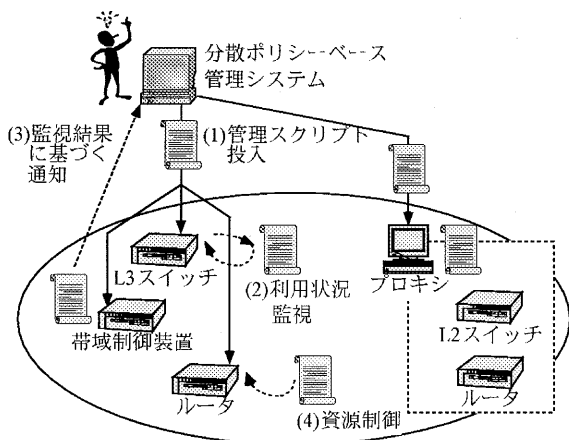


図 3: 提案する分散アーキテクチャ。

るプロキシ(図 3)で実行させる。

3.2 基本方針

(A) 物理インタフェース毎に管理スクリプトを投入

管理スクリプト提供の単位には、ポリシー単位や被管理システム単位などがある。ポリシー単位の場合、新たな管理スクリプト実行にともなう条件部の適用順序再構成の際に、実行中の管理スクリプトの順序変更が必要になるなど処理が複雑になる。一方、管理スクリプトを実行する被管理装置の負荷分散の観点から管理スクリプトの単位は細かいほど好ましく[5]、ポリシーの実行にともなう優先度制御や帯域制御は物理インタフェース毎に行われることから、被管理装置の物理インタフェース単位とする。

(B) すべての被管理装置に共通の管理スクリプトを投入
ポリシーベース管理では複数の被管理装置間で一貫したポリシーを実行させるため、単一の被管理装置の監視や制御を対象とする従来の分散ネットワーク管理とは異なり、共通の管理スクリプトをすべての被管理装置に投入(図 3(1))してポリシーを実行させる。

(C) 被管理装置内における利用状況監視とチューニングに重要な管理情報の提供

ポリシーを実行させた後、ネットワークの利用状況を監視(図 3(2))してポリシーの適用効果を評価する。例えば、帯域超過のために優先度を落とされる、または、廃棄されるパケット数があらかじめ指定される閾値を超えるなどの場合にのみ分散ポリシーベース管理システムに通知(図 3(3))し、ネットワークの利用状況に応じた実時間でポリシーのチューニングに重要な管理情報を運用者に提供する。

(D) 管理スクリプトによるネットワーク資源の制御

上記(C)の通知や、例えば、1週間や1ヶ月に及ぶ利用状況の傾向から、必要以上に広い帯域を確保するポリシーから帯域不足が頻発するポリシーへ帯域を割譲させるなど、管理スクリプトによるネットワーク資源の制御(図 3(4))を行わせ、ポリシーのチューニングを行う。管理スクリプトは利用状況の傾向から変更前後の値を含めて通知し、運用者からの指示にしたがって実際にチューニングを行う。複数の被管理装置間で一貫したポリシーを実行させるため、チューニングするポリシーと他被管理装置における同一ポリシーとの同期が必要であり、分散ポリシーベース管理システムから集中して同期させる、またはチューニングするポリシーから各被管理装置に分散する管理スクリプト間で同期させる。

3.3 Diffserv への適用

図 4 の Diffserv におけるポリシーを例に提案アーキテクチャの適用例を示す。

(1) ポリシーの投入

Diffserv では DSCP の値を使い複数のフローを集約し

(a)MF classifier を持つポリシー

ポリシー	MF classifier	プロファイル		付与する DSCP	
		帯域	バーストサイズ	適合	不適合
A	SrcIP==10.0.0.0/24	2Mbps	2Kbyte	101110	001010
B	SrcIP==10.1.0.0/16 && DstIP==192.1.0.0/16 && SrcPort==80	1Mbps	1Kbyte	001100*1	001110*2
C	上記以外	なし	なし	000000	000000

(b)BA classifier を持つポリシー

ポリシー	BA classifier	プロファイル		置換する DSCP	
		帯域	バーストサイズ	適合	不適合
D	101110	5Mbps	20Kbyte	101110	廃棄
E	001010	2Mbps	100Kbyte	001010	001100
F	上記以外	なし	なし	000000	000000

図 4: Diffserv におけるポリシーの例。

て優先制御や帯域制御を行うため、3.2 節 (B) を若干変更してポリシーを投入する必要がある。1) Core ルータの Core インタフェースの場合、BA classifier でパケットを分類するため、BA classifier (図 4(b)) を持つポリシーを実行させる管理スクリプトを投入する。2) Edge ルータの Core インタフェースの場合、BA classifier または MF classifier を使ってパケットを分類する場合があるため、すべてのポリシーを実行させる管理スクリプトを投入する。3) Edge ルータの Edge インタフェースの場合、上記 2) に準じるが、分類したパケットは Diffserv ネットワークから出て行くため、MF classifier を持つポリシーの実行では DSCP を付与しない処理を、また、BA classifier を持つポリシーの実行では DSCP を取り除く処理を管理スクリプトに行わせる。

(2) ポリシーのチューニングに重要な管理情報の提供

図 4 のポリシーを被管理装置に実行させた後、管理スクリプトは、各ポリシーで許容される帯域やバーストサイズを指定したプロファイルに適合および不適合するパケット数やバイト数の監視を行う。図 4 のポリシー D や E のように、不適合により廃棄または優先度を落とされるパケット数やバイト数が単位時間内にあらかじめ指定される閾値を超えるなどの場合には分散ポリシーベース管理システムに通知する。

(3) 管理スクリプトによるネットワーク資源の制御

上記(2)での通知や、例えば、1週間や1ヶ月に及ぶ利用状況の傾向から、プロファイルの帯域、バーストサイズ、および付与、置換する DSCP の値を変更してチューニングを行う。また、3.2 節 (D) でのポリシーの同期を行う。

4. おわりに

本稿ではネットワークの利用状況に応じた実時間でポリシーのチューニングを可能とする分散アーキテクチャを提案し、IETF が標準化を進める Differentiated Service への適用を検討した。提案アーキテクチャに基づく実装を通じた実環境評価が今後の課題である。最後に日頃御指導頂く(株)KDD 研究所秋葉所長、浅見副所長、ならびに松島副所長に感謝する。

参考文献

- [1] M. Stevens et al. *Policy Framework*. IETF, INTERNET-DRAFT draft-ietf-policy-framework-00 edition, Sep. 1999.
- [2] S. Blake et al. *An Architecture for Differentiated Services*. IETF RFC2475, December 1998.
- [3] G. Goldszmidt and Y. Yemini. *Delegated Agents for Network Management*. *IEEE Comm. Mag.*, Vol.36, No.3, 1998.
- [4] K. Psounis. *Active Networks: Applications, Security, Safety, and Architectures*. *IEEE Comm. Surveys*, 1999.
- [5] K. Yoshihara et al. *Dynamic Load-balancing for Distributed Management in Active Networks*. In *Proc. of IWAN 2000*, 2000. To appear.