L-008

キャンパスネットワーク運用自動化に向けた設定反映の差異の吸収に関する一検討

A Discussion on Absorption of Differences in Configuration Deployment Toward Campus Network Operation Automation

大森 幹之[1)]
Motoyuki Ohmori

1 はじめに

キャンパスネットワークの運用自動化のためには，ネットワーク機器への設定反映の自動化が必要である．そして，キャンパスネットワークでは，更新時期により異なるメーカの機器を導入することがある．この場合，メーカによって設定反映方式に以下の差異が存在することがある．

1. コミット型: 全設定を投入後，最後に一度に反映
2. 即時反映型: 1 つの設定を投入直後，逐次的に即座に反映

設定の冪等性を保つためには，この差異の吸収が必要である．そこで，本研究では，キャンパスネットワークの運用自動化に向け，コミット型と即時反映型の設定反映方式の差異の吸収について議論する．

2 ネットワーク設定の冪等性とその必要性

本節では，コミット型と即時反映型で同一の設定を担保することを目的に掲げるため，キャンパスネットワークにおける設定の冪等性とその必要性について述べる．

2.1 冪等性

一般に，冪等性とは，数学で提唱され始めた概念で，同じ演算を複数回繰り返しても結果が変わらない性質を意味する．計算機科学においては，一連の処理を何度繰り返したとしても，結果が変わらない性質を意味する．この性質を担保することで，障害などによって処理が中断することがあり得る環境であっても，処理を再試行することによって，最終的に同一の結果が得られる．ネットワーク設定においても，インターネットでもパケット損失は完全には防げない．そのため，処理に関して冪等性は重要な意味を持つ．

2.2 ネットワーク設定における冪等性の必要性

キャンパスネットワークの設定における冪等性の担保は重要である．設定を投入する対象であるスイッチへの接続が設定中に途切れることは発生し，意図した設定が反映されていないことがあり得るからである．また，スイッチによっては，他の処理を実行中には設定を投入できないものもある．この様なスイッチでは，設定の投入に失敗することもあり得る．設定に失敗した場合，設定投入の再試行が必要だが，再試行によって結果が変わると通信障害を招きかねない．例えば，ファイアウォールのセキュリティポリシの設定であれば意図せぬパケット破棄が発生する可能性がある．また，VLAN (Virtual Local Area Network) [1] の設定であればループを招く可能性がある．スイッチによっては，不要な VLAN の設定が残っていると，収容できる VLAN 数を超え，ハードウェア転送できず通信障害が発生する可能性もある．このような通信障害を防ぐため，キャンパスネットワークの設定においては冪等性が必要であり，その担保も重要である．

2.3 ネットワーク設定の冪等性

本稿では，キャンパスネットワークにおける設定の冪等性を以下で定義する．

1. 再試行しても同じ設定が得られる．
2. 全ての設定を削除してから，新しい設定を投入しても，同じ設定が得られる (不要な設定が残らない).

1 は計算機科学における一般的な冪等性と同一である．一方，2 は不要な設定を排除し通信障害を防止するために，本稿で独自に定義するものである．

3 コミット型と即時反映型

3.1 コミット型

全ての設定を投入後に，コミットによって設定を一度に反映させるのがコミット型である．コミット型のスイッチでの冪等性の担保は比較的容易である．以下の手順で設定を投入することにより，当該機器上での 2.3 節で定義した 2 つの条件を満たせる．

1. 全ての設定を削除する．
2. 必要な設定を投入し直す．

特に，設定の投入により不要となる設定の削除に留意する必要がない．

その一方で，設定に必要な要素を別途記憶し，最終的な設定を生成する必要がある．

3.2 即時型

設定のためにコマンドを投入する度に，そのコマンドが即座に反映されるのが即時型である．コミット型とは異なり，不要な設定が残る余地がある．そのため，1 つのコマンド毎に以下を繰り返す必要がある．

1. コマンドを投入する．
2. 不要となった設定 (セキュリティポリシや VLAN の定義など) の有無を確認し，有れば削除する．

不要となる設定を検知するために，各設定との依存関係を検査する仕組みが必要となる．

もう 1 つの手法として，コミット型と類似した以下も考えられる．

1. 別途設定確認用の同型機を用意する．
2. 最終的な設定を設定確認用機器に全て投入し，設定を生成する．
3. 生成された設定と現在の設定との差分を取り，不要となった設定を検出・削除する．
4. 生成された設定を全て投入する．

この手法の場合，設定の依存関係を事前に把握する必要がなくなる．そのため，実現可能性が向上することが期待できる．その一方で，同型機を別途用意する必要が

1) 鳥取大学 情報戦略機構 Organization for Information Strategy and Management, Tottori University.

生じる．これは，機器の仮想マシンを用意することで，対応できる可能性がある．また，この手法では，不要となった設定を削除した時点で通信障害が発生する可能性がある．そのため，設定の削除には通信障害を生じないか検証する必要性が生じる．これは，他方の方式での各設定の依存関係の検査と類似している．このことから，本手法が優位であるとはいえない．

4 ネットワーク設定

本節では，キャンパスネットワークにおける設定として，VLAN の設定について考える．VLAN 設定では以下が与えられるものとする．

1. 始点となるスイッチとポート，動作モード
2. 終点となるスイッチとポート，動作モード

そして，スイッチ上の VLAN の設定には，大きく分けて以下があるものとする．

1. VLAN の定義
2. ポートの動作モードの指定
3. ポートへの VLAN の追加
4. ポートからの VLAN の削除

1 は，VLAN 上のパケットを転送するために必要な定義である．2 は，スイッチ上の特定ポートで VLAN をタグ有りもしくは無しで送信または受信するかを指定するものである．本設定を変更することにより，VLAN の追加・削除に必要なコマンドも変化することに注意されたい．3 は，VLAN 上のパケットを送受信するポートを追加するための設定である．本設定により，以前設定されていた別の VLAN の定義が不要になり，削除が必要な場合があり得ることに注意されたい．

5 機器単体での設定反映方式の差異の吸収

本節では，VLAN を設定する 1 つの機器，すなわち，1 つのスイッチ内での設定反映方式の差異の吸収について考える．差異を吸収するにあたり，以下を満たすことを目指す．

1. 設定変更に伴うループを発生させない
2. VLAN の上限を超えない

上記を鑑みると，以下の設定手順が考えられる．

1. VLAN のポートへの設定を削除
2. 不要な VLAN の定義を削除
3. VLAN に付随する不要な設定の削除と削除
4. VLAN の設定追加

ここで, VLAN に付随する設定としては, STP (Spanning Tree Protocol) や VLAN タグ変換などがある．例えば，STP を VLAN 毎に動作させている場合に，ルートとなるスイッチを固定するために，優先度を設定したいことがある．また，VLAN タグ変換とは，ある VLAN を他の ID を持つ VLAN として変換する VLAN に関連する機能である．以上のように，VLAN に付随した設定は，VLAN の定義が追加・削除される際に同時に追加・削除される必要がある．このことから，VLAN に付随する設定を関連付ける必要があると考えられる．

6 ネットワーク全体での差異の吸収

前節で 1 つの機器内での設定反映方法の差異の吸収について論じた．しかし，1 つのスイッチ内だけでなく，キャンパスネットワーク全体として，考える必要がある．これは，不要な VLAN な設定が残存していると，ループといった障害を招くからである．

そのため，キャンパスネットワーク全体としての VLAN 設定を保持しておき，全てのスイッチに設定を反映できるまで繰り返すことが必要になる．これには，NetBox [1)] によりスイッチの機種に依らない形で VLAN を設定するポートを記憶することで実現可能である．また，途中で設定が失敗した場合，全ての設定が完了するまで再試行が必要である．また，異なるスイッチに対応するための一手法としては，NetBox 上で保持している VLAN の情報を元に，Batfinsh [5, 6] を用いて，当該スイッチ用の設定を生成することが考えられる．

7 関連研究

手動での VLAN 設定では，遅延や誤り，不要な設定の残存などが発生し得るため，VLAN 設定の自動化も提案されている [2, 3, 4]．しかし，これらの提案では，それぞれの環境毎の独自方式に留まっており，統一的な手法ではない．

また，異なる大学のキャンパスネットワークでは，VLAN 設定の方針やネットワーク構成が異なることがある [7]．そのため，統合的な手法を検討する必要がある．

8 おわりに

本稿では，キャンパスネットワーク運用自動化に向け，コミット型と即時反映型の設定反映の差異を吸収する手法について論じた．実装と評価は今後の課題である．

謝辞

この研究は 2025 年度国立情報学研究所公募型共同研究（251S1-22744）の助成を受けている．

参考文献

[1] IEEE Std. 802.1Q-1998: *Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*, The IEEE Standards Association (1998).

[2] 近堂徹，田島浩一，岸場清悟，岩田則和，相原玲二：自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価，情報処理学会論文誌，Vol. 57, No. 3, pp. 998–1007 (2016).

[3] 北口善明，　金勇，友石正彦：OSS を活用したキャンパスネットワークの構成管理システム (2022).

[4] 北口善明，　金勇，友石正彦：キャンパスネットワーク運用自動化に向けた構成管理システムの実装と評価 (2023).

[5] Fogel, A., Fung, S., Pedrosa, L., Walraed-Sullivan, M., Govindan, R., Mahajan, R. and Millstein, T.: A General Approach to Network Configuration Analysis, *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*, Oakland, CA, USENIX Association, pp. 469–483 (online), https://www.usenix.org/conference/nsdi15/technical-sessions/presentation/fogel (2015).

[6] Brown, M., Fogel, A., Halperin, D., Heorhiadi, V., Mahajan, R. and Millstein, T.: Lessons from the evolution of the Batfish configuration analysis tool, *Proceedings of the ACM SIGCOMM 2023 Conference*, ACM SIGCOMM '23, New York, NY, USA, Association for Computing Machinery, pp. 122–135 (online), DOI: 10.1145/3603269.3604866 (2023).

[7] 大森幹之，北口善明：異なるキャンパスネットワークにおける VLAN 設定手順の共通要素の抽出と自動化の一検討 (2024).

1) https://github.com/netbox-community/netbox