

SPring-8の加速器制御系および利用実験系ネットワークの仮想化統合に向けた評価試験

EVALUATION OF SPRING-8 ACCELERATOR-CONTROL AND EXPERIMENTAL NETWORK VIRTUALIZATION

杉本崇^{*A)}、石井美保^{A)}、辻谷健一^{A)}、上田晃義^{A)}

Takashi Sugimoto^{*A)}, Miho Ishii^{A)}, Ken-ichi Tsujitani^{A)}, Teruyoshi Ueda^{A)}

^{A)}Japan Synchrotron Radiation Research Institute (JASRI/SPring-8)

Abstract

We report technical study of network virtualization at SPring-8. For the reason of both performance and security, the SPring-8 control system LAN is physically segregated from the SPring-8 user experimental LAN. Since the SPring-8 storage ring is circular shaped, physical location of two network systems are partially overlapped. Recent evolution of virtualization technologies enables us to integrate plural logical networks into one physical network system. To reduce instrumental cost, we started studying virtualization for SPring-8 control and experimental network.

1. 背景

SPring-8では運転開始当初よりネットワーク通信をベースとした制御システムを構築・運用している。現在デファクトスタンダードとなったTCP/IPを採用したことにより、高い拡張性を実現し、運用を継続している。SPring-8には制御系ネットワークだけでなく、オフィス系ネットワーク、利用実験系ネットワークが構築されている。蓄積リングの物理的形狀から、これら三種のネットワークの一部は地理的に重複して敷設されており、必要ネットワーク機器数・光ファイバ芯数の増大、すなわち、コスト増の原因となっている。

SPring-8では、VLAN^[1]およびレイヤ3ネットワークスイッチ(L3SW)の導入により^[2]、同系統ネットワークの重畳化とルーター等の機器数削減を進めてきた。しかしながら、信頼性、帯域、セキュリティ、運用スケジュールの違い、などの理由により、異種系統ネットワーク同士の重畳は行っていなかった。近年ネットワーク機器の性能が向上し、仮想化技術により要件の異なる複数系統のネットワークの重畳化が可能となりつつある。ネットワーク機器数削減を実現するため、我々は、制御系および実験計測系ネットワークの仮想化強盗に向けた評価試験を行った。

2. ネットワーク仮想化の評価・検証

ネットワーク仮想化による利点として、(1) 機器数減によるコスト削減、(2) 機器数減によるシステム全体としての平均故障間隔の向上、が期待される。特に(1)に関して、全体費用が現在以下であることは必須要件であり、仮想化対応のために高価な機器を購入することは選択肢の範囲外である。一方で懸念される点としては(i) 障害時の影響の全体への波及、(ii) 帯域・応答性などの通信性能の担保、(iii) 仮想化による機器設定の複雑化、などが挙げられる。特に(i)に関して、年間のべ10,000人以上が使用する利用実験ネットワークは小規模障害が比較的高頻度で発生している。ネットワークの仮想化統合を行った際に、利用実験系から制御系ネットワークへの障害の波及を防ぐ必要がある。(ii)に関して、低遅

延が要求される加速器制御系のために通信の優先制御、広帯域通信が要求される利用実験のため帯域制御を行う必要がある。(iii)に関して検討は必要であるが、設定の複雑さは機器メーカーに依存するため今回の評価検証の対象外とした。

2.1 レイヤ3ネットワークスイッチの仮想化

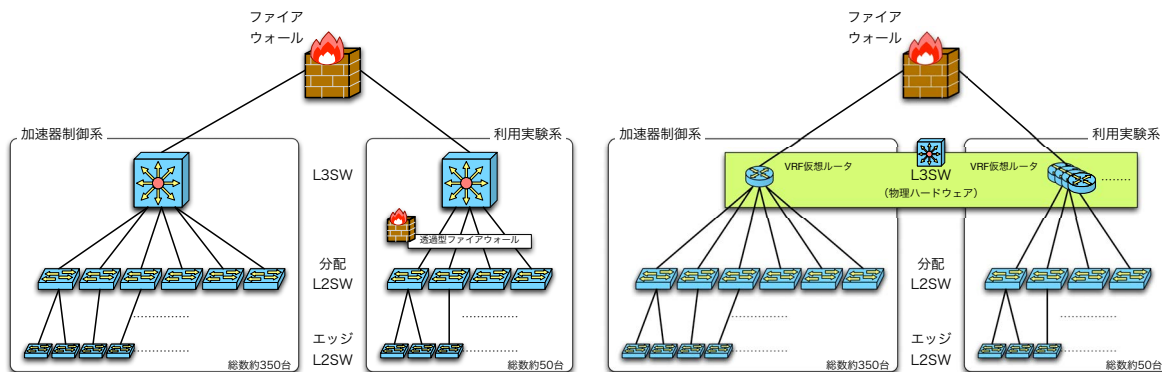
仮想化の第一フェーズとして、我々はルーティング機能を担うL3SWの仮想化を検討した。SPring-8加速器制御系および実験計測系ネットワークのうち最も高価な機器はL3SWであり、費用削減効果が大きいためである。本評価試験では、ルーティング機能の仮想化技術としてVirtual Routing and Forwarding(VRF)を採用した。VRFは標準化技術MPLS^[3]のサブセットであり、現在市販されているほぼ全てのL3SWで使用可能である。

Figure 1(a)に現在のネットワーク構成の概要を示す。L3SW、分配レイヤー2ネットワークスイッチ(L2SW)、エッジL2SWを含め、SPring-8加速器制御系と利用実験系はそれぞれ約350台、約50台のネットワークスイッチから構成される。現在のSPring-8加速器制御系L3SWおよび利用実験系L3SWはそれぞれCisco Systems社Catalyst 6504-E、同Catalyst 3750-Eである。利用実験系ネットワークではさらに透過型ファイアウォールを導入し、各ビームライン同士の通信を制限している。

Figure 1(b)に仮想化(第一フェーズ)後に想定しているネットワーク構成を示す。利用実験系L3SWをCatalyst 6504-E(あるいはその後継機)に統合し、VRFによる仮想ルーター構成を予定している。また、利用実験ネットワークにおいてはビームラインごとにVRFを定義する。VRFを用いてビームライン別にルーティングテーブルを分離することにより、利用実験系ネットワークに導入している透過型ファイアウォールも削減可能となる。

Figure 2に本評価試験における構成を示す。本評価試験ではL3SWの検証にCatalyst 3750-E(最大VRF数26)を使用した。分配およびエッジL2SWにはCatalyst 2960-X-24TS-L、HP社2530-24G、同5500-24G-EIを試験項目に応じて組み合わせて使用した。

* takashi.sugimoto@spring8.or.jp



(a) Current configuration of SPring-8 network system. The physical topology is well-known "three-layered" network. For the purpose of aggregating routers into one physical L3SW using VRF. By assigning VRF virtual access control at experimental network, we installed transparent fire-routers to each beamline, we will also remove transparent firewall wall between the core and distribution network switch.

Figure 1: Schematic view of SPring-8 accelerator and experimental network system.

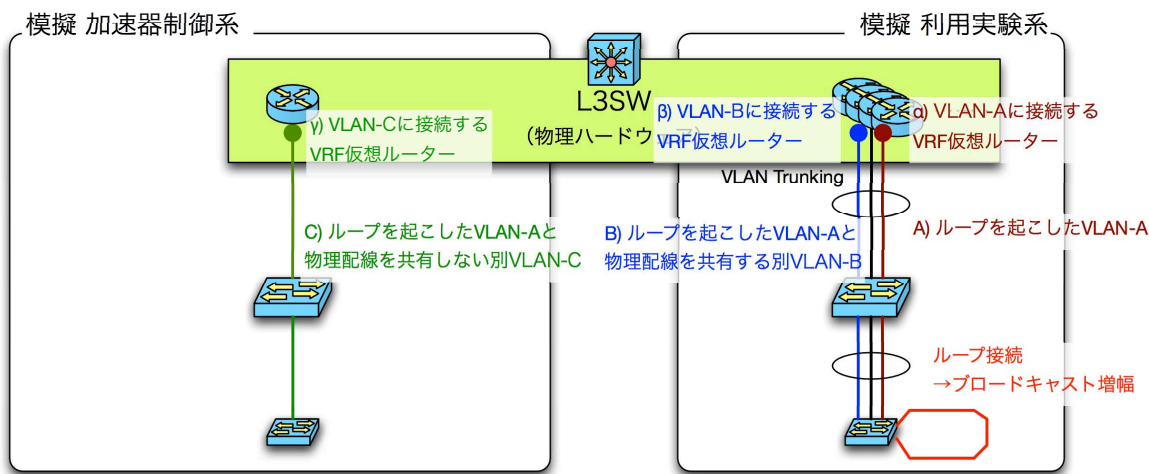


Figure 2: Test bench network for the evaluation.

2.2 想定される障害モードの検証

SPring-8 利用実験系ネットワークで発生する典型的なネットワーク障害の原因（機器故障以外）は、ネットワークループ、IP アドレス重複（ゲートウェイ上書き）である。VRF 仮想ルーター構成時これらの障害が発生した場合に、加速器制御系ネットワークに与える影響を検証した。

2.2.1 ネットワークループ障害

ネットワークループ障害とは、ブリッジネットワーク（同一 VLAN）においてループ状に接続することにより、ブロードキャスト増幅が引き起こされ帯域を占有する事象（ブロードキャストストーム）のことである。このようなネットワークループを防ぐ技術として、Spanning Tree Protocol (STP)^[4]、マルチキャストを用いたエッジポートループ検出機能等が一般的な L2SW に実装されている。評価試験では、ループ対策なし、STP、エッジポートループ検出、を適用した場合に、(A) ループを起こした VLAN-A、(B) ループを起こした VLAN-A と物理配線を共有する VLAN-B、(C) ループを起こした VLAN-A と物理配線を共有しない VLAN-C、および、

それらの VLAN が接続する VRF 仮想ルーター α, β, γ における影響を検証した。

Table 1 に、VLAN-A でネットワークループが発生している条件下における、L2 幹線区間の通信影響の検証結果を示す。STP は VLAN ごとにループ検出を適用できる RPVST+モードを使用した。STP を有効にした場合、エッジポートにおけるループ遮断が期待されたが、試験ネットワーク環境ではループが発生しているポートを遮断できず (A),(B) 区間がブロードキャストで占有された。一方、エッジループ検出を適用した場合、ループに該当するポート以外は通信を継続できた。

Table 2 に、ネットワークループが発生している条件下における VRF 仮想ルーターの通信可否の検証結果を示す。STP 有効の場合、ブロードキャストストームが達している仮想ルーター α だけでなく、物理配線を共有する仮想ルーター β 、共有しない仮想ルーター γ も通信不可であった。すなわち、VLAN-A で発生したブロードキャストストームの処理に L3SW の CPU 資源が占有され、全ての VRF のルーティング処理に影響を与えた。一方、エッジループ検出有効の場合、エッジポートにおいてループ遮断したため VRF 仮想ルーターの処理に影

Table 1: Result of layer-2 (bridge) communication test under the network loop condition. A, B, and C represent layer 2 network section in the Fig. 2.

	(A)	(B)	(C)
ループ対策無し	通信不可	通信不可	影響なし
STP (RPVST+) 有効	通信不可	通信不可	影響なし
エッジループ検出有効	影響なし*	影響なし	影響なし

*エッジ L2SW のポートより下流が遮断されるため、下流でループを形成していない別のポートから上流は通信可。

Table 2: Result of layer-3 (routing) communication test under the network loop condition. α , β , and γ represent VRF virtual router corresponding to VLAN-A, -B, and -C in the Fig. 2 respectively.

	(α)	(β)	(γ)
ループ対策無し	通信不可	通信不可	通信不可
STP (RPVST+) 有効	通信不可	通信不可	通信不可
エッジループ検出有効	影響なし	影響なし	影響なし

響を与えなかった。

以上の評価試験より、VRF 仮想ネットワーク環境におけるネットワークループ障害に対する防御策として、以下の二点が重要であることを確認した。

- エッジポートでネットワークループを遮断すること (ただし、STP は期待した動作が確認できなかった)
- VRF 仮想ルーターにブロードキャストストームを到達させない

2.2.2 ゲートウェイ IP アドレス重複障害

SPring-8 利用実験系ネットワークでは、PC 等の端末のインターフェースに誤ってデフォルトゲートウェイ (ルーター) の IP アドレスを設定するミスがしばしば発生している。現在のネットワーク構成 (Fig. 1(a)) では該当するセグメントからルーターを越える通信ができなくなるだけであり、障害はビームラインごとの VLAN 単位で閉じられる。VRF により単一のハードウェア上に仮想ルーターがまとめられた構成におけるゲートウェイ IP アドレス重複障害について、ネットワークシステム全体への影響を検証した。

VLAN-A に接続した端末に仮想ルーター α の IP アドレスを割り当てた。このとき仮想ルーター β および γ を経由する通信に影響は確認できなかった。以上の評価試験より、VRF による仮想化を行った場合においても、現在のネットワーク構成と同様に VLAN-A 内で障害が閉じられていることを確認した。

3. まとめ

SPring-8 加速器制御系および利用実験系ネットワークの仮想化統合を検討している。第一フェーズとして、最も高価な機器である L3SW を VRF を用いて統合する。想定される障害モードについて評価試験を行い、特にネットワークループ障害に対してはエッジループ検出と遮断が重要であることを確認した。今後、外部ファイアウォールおよび透過型ファイアウォールとの取り合いを

検証した上で、平成 28 年度のネットワークシステム更改で仮想化統合を導入する予定である。

さらに第二フェーズの計画として、分配 L2SW の仮想化統合を検討する。加速器制御系と利用実験系の物理配線を共有した場合、それぞれが要求する帯域・応答性を担保する必要がある。通信の優先制御・帯域制御についても今後検討・検証を進めていく。

参考文献

- [1] "Virtual Bridged Local Area Networks", IEEE Std. 802.1Q.
- [2] M. Ishii, et al., "Upgrade of SPring-8 Beamline Network with VLAN Technology over Gigabit Ethernet", Proceedings of ICALEPCS2001, TUAP056, San Jose, California, U.S., Nov. 27-30, 2001.
- [3] "Multiprotocol Label Switching Architecture", RFC 3031, IETF Standards Track, 2001.
- [4] "MAC bridges", IEEE Std. 802.1D (incorporated into IEEE Std. 802.1Q-2014).