G-34

レイヤ 2 に対応したトラブルシューティング演習を可能とするネットワーク演習支援システムの実装

Implementation of Hands-on Network Exercise Support System enabling Troubleshooting Exercises for Layer 2

東雲 美幸† 吉原 和明‡§ 井口 信和‡§
Miyuki Shinonome Kazuaki Yoshihara Nobukazu Iguchi

1. 序論

我が国における IP トラフィック量は，新型コロナウイルス発生後に急激に増加し，2022 年は 2019 年に比べて 2 倍以上となった．このことからネットワークの需要が大幅に高まっていることがわかる[1]．それに対して，IT 技術者は不足しており 2030 年には最大 79 万人不足すると言われている[2]．総務省の通信利用動向調査報告書では，ICT 人材が足りていない企業においてどういった人材が不足しているかについて述べられており，全ての産業においてネットワーク技術者が最も不足しているという結果となった[3]．このことから，ネットワーク技術者の養成が急務となっている．

ネットワーク技術者には，ネットワークの設計・構築能力に加え，ネットワーク障害への対応能力の習得が求められる．令和 4 年度に報告された国内のネットワーク障害の報告件数は 7,500 件であり，ネットワーク障害が多発しているという現状がある[4]．ネットワーク障害が多発する原因の 1 つにヒューマンエラーがあり，ヒューマンエラーが原因で重大な事故に至るケースも少なくない[5]．このことから，ヒューマンエラーが原因のネットワーク障害が発生した場合に，素早く問題箇所を特定し対処する障害対応能力は，ネットワーク技術者にとってネットワークの可用性を高く保つために非常に重要となる．

障害に迅速に対応する能力を習得するには，ハンズオン形式のトラブルシューティング演習を反復実践することが重要となる．この時，同じ障害事例に対してより素早く正確に対応する演習だけでなく，様々な種類の障害事例に対応する演習を用いて訓練することが有効となる．

このようなハンズオン形式の演習の例として，本学では Cisco Networking Academy（以下，CNA）というネットワーク技術者の養成を目的としたプログラムが開講されている[6]．CNA では，ネットワークの構築や構築時のトラブルシューティングをハンズオン形式で実施することで実践的な学習を通して知識と理解の定着が期待できる．しかし，CNA におけるトラブルシューティング演習の実施にはいくつか課題がある．まず，トラブルシューティング演習を実施するには複数台の高価なネットワーク機器が必要となる点がある．次に，トラブルシューティングの演習準備として予め機器にネットワーク障害を含む設定を発行しておく必要があり，演習を開始するまでの作業に時間を要する点がある．

そこで我々は，ネットワーク障害をシステムが自動生成することでトラブルシューティング演習環境を即座に提供可能な仮想ネットワークを用いた演習支援システム（以下，既存システム）を開発してきた[7]．既存システムでは仮想化技術を用いることで，学習者はルータやスイッチなどの実機を用意することなく 1 台の PC のみでトラブルシューティング演習を実施できる．さらに，既存システムにはネットワーク障害を自動生成する機能（以下，障害自動生成機能）が実装されており，演習準備にかかる手間を軽減できる．障害自動生成機能は OSI 第 3 層（以下，レイヤ 3）の範囲のヒューマンエラーを原因とするネットワーク障害に対応しており，OSI 第 2 層（以下，レイヤ 2）の範囲のネットワーク障害には対応していなかった．しかし，レイヤ 2 の設定はレイヤ 3 と同様に，ネットワーク技術者が手作業で設定する．手作業でネットワーク機器の設定や変更を実施するとヒューマンエラーが起こることがあり，ヒューマンエラーによる障害の発生を完全に防ぐことは困難である．もしレイヤ 2 の設定ミスが起こると，ネットワークループの発生やデータ損失，セキュリティの問題が発生してしまう危険性がある．そのため，ネットワーク初学者はレイヤ 3 の障害に加え，レイヤ 2 の障害に対処するための障害対応能力を習得する必要がある．

そこで本稿では，学習者のネットワーク障害対応能力の習得の支援を目的とするレイヤ 2 に対応したトラブルシューティング演習支援システム（以下，本システム）の実装について述べる．本システムは，既存システムにレイヤ 2 に対応した障害自動生成機能を新たに実装した．また，学習者が演習中に仮想スイッチで使用できるコマンドを追加実装した．本システムにより，レイヤ 2，3 の両方のトラブルシューティング演習環境を時間や場所を選ばず即座に提供でき，学習者の障害対応能力の習得を支援可能となる．

2. 関連研究

ネットワーク技術者の養成を目的とした学習環境の提供に関する研究として，文献[8]，[9]がある．

立岩らの研究では，UML を活用して仮想環境上に障害のあるネットワークをシミュレートする演習システムを開発している[8]．このシステムでは，学習者が演習したい障害の内容を自分で選択することでトラブルシューティング演習を実施できる．そのため，障害の原因を突き止めることなく演習が可能となる．これに対して本システムでは，Docker を活用しており，システムがランダムにネットワーク障害を自動生成することで障害のあるネットワークをエミュレートする．これによって学習者は障害の原因を自力で突き止め，ネットワーク全体を把握して障害に対応することが可能となる．

また，平畑らの研究では，擬似演習者ロボットとの協調演習を可能とするトラブルシューティング演習システムを開発している[9]．このシステムでは，協調演習者として動

† 近畿大学大学院総合理工学研究科，
Graduate School of Science and Engineering, Kindai University
‡ 近畿大学情報学部情報学科，
Faculty of Informatics Department of Informatics, Kindai University
§ 近畿大学情報学研究所，
Cyber Informatics Research Institute, Kindai University

作するコミュニケーションロボットと学習者が，実機を用いてネットワークのトラブルシューティングの協調演習が可能な環境を提供する．それに対して本システムでは，仮想環境上でトラブルシューティング演習を実施できる．そのため，1 台の標準的な仕様の PC を用意するだけで場所や費用を要さずトラブルシューティングの自己学習が可能となる．

さらに，オンライン上でネットワークのトラブルシューティング演習を実施できるシステムとして，Cisco Packet Tracer （以下，CPT）がある[10]． CPT は，ネットワーク機器をソフトウェア上で操作し，仮想ネットワーク環境を構築できるシミュレータである．CPT では予め用意されている演習ファイルを用いてトラブルシューティングを実施できるが，ファイル数が限られている．そのため，学習者が同じ範囲を反復演習する場合，障害の内容や発生箇所を覚えてしまう．それに対して本システムでは，システムが障害内容や障害箇所を演習ごとにランダムに指定して障害を生成する．そのため，学習者は同じ範囲の演習課題でも毎回違ったトラブルシューティング演習を実施可能となる．

3. 研究内容

3.1 システム概要

本システムは，仮想化技術を活用することで，Web ブラウザ上でネットワークのトラブルシューティング演習が実施可能な演習支援システムである．本システムの構成を図 1 に示す．本システムは管理サーバ，通信サーバ，及びクライアントで構成される．管理サーバはコンテナ技術の管理基盤である Docker を用いてコンテナを作成し，それを仮想ネットワーク機器（以下，仮想機器）として動作させることで仮想ネットワークを構築する．また，管理サーバは Java プログラムを用いて仮想ネットワークや演習情報などを管理する．通信サーバは管理サーバとクライアント間の通信を仲介する．クライアントには図 2 に示すような Web ベースの GUI が提供され，それを用いて仮想機器に対して設定が可能となる．

本システムの処理の流れを説明する．まず，クライアントの操作内容が通信サーバを介して管理サーバに送信される．次に，管理サーバはクライアントの操作内容を基に，仮想ネットワークに処理内容を発行する．最後に，仮想ネットワークに対する処理結果が，通信サーバを介してクライアントに送信される．以上の流れにより，クライアントである学習者は仮想ネットワークを用いて演習を実施することができる．

本システムでレイヤ 2 演習を可能とする仮想スイッチは Open vSwitch を用いて実現している[11]．Open vSwitch は，様々な Layer2 プロトコルをサポートするネットワークスイッチのソフトウェア実装である．仮想ブリッジを作成し，作成した仮想ブリッジに対して Layer2 プロトコルの設定を施すことで，仮想スイッチとしての動作を実現している．

3.2 障害自動生成機能

障害自動生成機能とは，正しく設定され正常に動作しているネットワークに対して，ランダムに機器を選択し，誤った設定を自動で上書きすることでネットワーク障害を生成する機能である．既存システムでは，前述したようにレイヤ 3 のネットワーク障害には対応していたがレイヤ 2 の

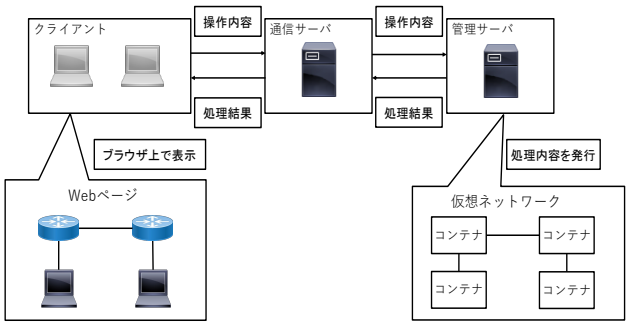

図 1：システム構成図

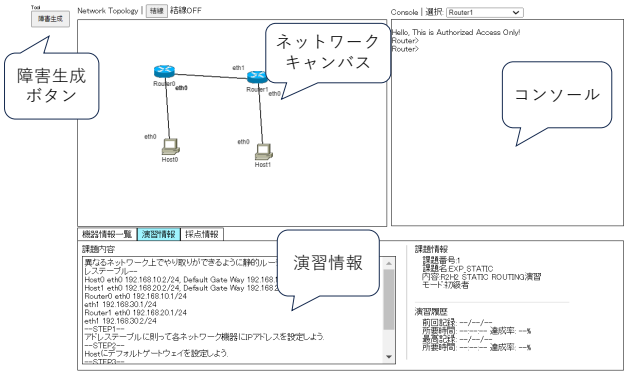

図 2：Web ページ上のシステム画面

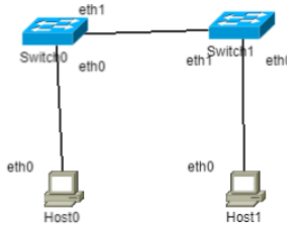

図 3：ネットワークトポロジ

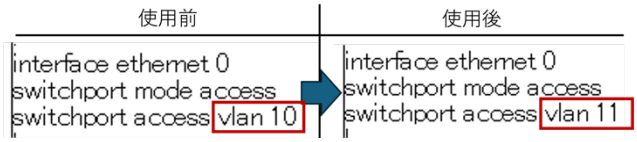

図 4：Switch0 のアクセスポートの設定の変化

ネットワーク障害には対応していなかった．そこで本機能では，レイヤ 2 に対応したトラブルシューティング演習環境を提供するため，既存システムで実装した障害自動生成機能に新たにレイヤ 2 のネットワーク障害の項目を実装した．本稿で実装したレイヤ 2 障害は，Virtual Local Area Network（以下，VLAN）と Link Aggregation Control Protocol（以下，LACP）の範囲を対象とした．VLAN は，ネットワークセグメントを分離し管理を簡便化するために，企業や教育機関のネットワークで広く利用されている．LACP は，帯域幅の増加や冗長性の向上のために，データセンターなどの大規模ネットワークで一般的に利用されている．これらの理由から，以上の 2 つの範囲の演習を対象とした．また，本稿ではネットワークトポロジとして，図 3 に示すようにスイッチ 2 台，ホスト 2 台の小規模なネットワークを使用する．向かって左側の仮想スイッチが Switch0，反対に右側の仮想スイッチが Switch1 とする．LACP 演習の場

合は，Switch 間のリンクが 2 本となる．以下に，本機能で実装した 3 つのネットワーク障害の項目を示す．

・VLAN ID の変更による障害
・allowed VLAN の変更による障害
・channel-group mode の変更による障害

3.2.1　VLAN ID の変更による障害の詳細

VLAN ID の障害の内容は，スイッチのアクセスポートに設定されている VLAN ID をシステムが変更するというものである．図 3 のトポロジの場合，スイッチからホストに接続されているポート（eth0）がアクセスポートで，スイッチ同士を接続するポート（eth1）がトランクポートである．本機能を使用すると，システムが Switch0 か Switch1 の中からアクセスポートを選択し，VLAN ID を変更する．

本機能の使用の前後に show running-config コマンドで Switch0 のアクセスポートの設定の変化を表示した様子を図 4 に示す．本機能使用前の Switch0 のアクセスポートの VLAN ID には 10 が設定されているが，本機能使用後の VLAN ID は 11 が設定されていることがわかる．アクセスポートに設定する VLAN ID が変わってしまうと，通信の失敗や意図しないアクセスが可能になるなどのネットワーク障害が発生する．

3.2.2　allowed VLAN の変更による障害

allowed VLAN の障害の内容は，スイッチのトランクポートに設定されている allowed VLAN のリスト内の VLAN ID をシステムが変更するというものである． 3.2.1 項と同様に，システムが Switch0 か Switch1 の中からトランクポートを選択し，allowed VLAN の一部を変更する．

本機能の使用の前後に show running-config コマンドで Switch0 のトランクポートの設定の変化を表示した様子を図 5 に示す．本機能使用前の Switch0 の allowed VLAN には 1, 10, 20 が設定されているが，本機能使用後には 1, 10, 30 が設定されていることがわかる．トランクポートを通過できる VLAN ID が変わってしまうと，通信障害やセキュリティの問題が発生する．

3.2.3　channel-group mode の変更による障害

channel-group mode の障害の内容は，LACP により形成した EtherChannel のモードを，2 つのスイッチの両方のインターフェースで active から passive にシステムが変更するというものである．図 3 の場合，スイッチ間のリンクが 2 本となり，eth1 と eth2 で EtherChannel を形成する．本機能を使用すると，システムが両方のスイッチの EtherChannel を形成しているポートの channel-group mode を passive に変更する．

本機能の使用の前後に show running-config コマンドで Switch0 の設定の変化を表示した様子を図 6 に示す．本機能使用前の Switch0 の両方のインターフェースで channel-group mode は active と設定されているが，本機能使用後には passive に設定されていることがわかる．これを Switch1 でも同様に実施する．channel-group mode が両側で passive になると，LACP パケットの送信が行われずにスイッチ間の EtherChannel の形成に失敗し，帯域幅の増加や冗長性などのリンクアグリゲーションの利点が得られない．

3.3　コマンドの実装

レイヤ 2 に対応したトラブルシューティング演習環境を提供するため，既存システムに実装されていた仮想スイッチで学習者が演習時に使用できるコマンドに新たに以下のコマンドを実装した．

・no switchport access vlan
・no switchport trunk allowed vlan
・no switchport trunk native vlan
・show running-config
・show vlan brief
・show etherchannel summary

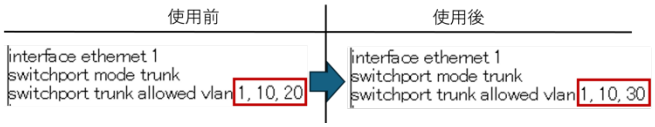

図 5：Switch0 のトランクポートの設定の変化

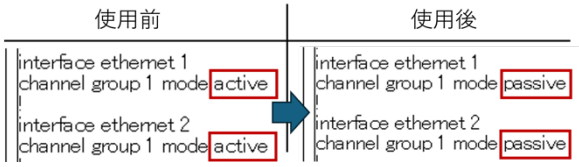

図 6：EatherChannel の設定の変化

図 7：show vlan brief コマンド実行の様子

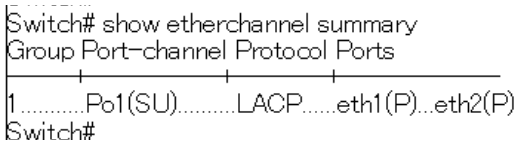

図 8：show etherchannel summary コマンド実行の様子

3.3.1　show vlan brief の詳細

本コマンドは，スイッチに設定されている VLAN ID やステータスなどの VLAN 情報を簡潔に表示するためのコマンドである．既存システムでは，VLAN の設定情報を確認するためのコマンドが実装されていなかった．しかし，VLAN 演習のトラブルシューティング時に学習者は機器にどういった VLAN の設定がされているかを確認しながら演習することが想定されるため，本コマンドを実装した．

本コマンド実行時の学習者のコンソール画面は図 7 のように表示される．表示内容は Cisco スイッチの show vlan brief コマンドの表示内容と同様に，VLAN ID，VLAN Name，Status，Ports を表示する．

3.3.2　show etherchannel summary の詳細

本コマンドは，スイッチに設定されている LACP で形成した EatherChannel のステータスなどの情報を簡潔に表示するためのコマンドである．既存システムでは，EtherChannel の設定情報を確認するためのコマンドが実装されていなかった．しかし，VLAN 演習のトラブルシューティング時に学習者は機器にどういった EtherChannel の設定がされているかを確認しながら演習することが想定されるため，本コマンドを実装した．

本コマンド実行時の学習者のコンソール画面は図 8 のように表示される．表示内容は Cisco スイッチの show etherchannel summary コマンドの表示内容と同様に，Channel Group，Port-channel，Protocol，Ports を表示する．

3.4 演習の流れ

本システムの演習の流れについて説明する．まず学習者が VLAN 演習か LACP 演習の中から演習したいものを選択する．演習課題が選択されると，図 2 で示したネットワークキャンバス上に学習者が選択したネットワークが構築される．次に，学習者は GUI 上にある障害自動生成ボタンを操作する．それによって，構築済みのネットワークに対して障害自動生成機能が動作し，選択された演習課題に合った障害をシステムが自動生成する．これにより，学習者はトラブルシューティング演習の実施が可能となる．

演習環境の用意が完了すると，学習者はまずネットワーク障害の発生箇所を特定するため，図 2 にある仮想機器のコンソール部分から仮想機器に対してコマンドを打ち込み，ネットワークの状態を収集し把握する作業を実施する．ネットワーク障害が発生している箇所を特定すると，次に，学習者はネットワークを復旧させるため，障害発生箇所の設定を課題の要件通りとなるように適切に更新する．最後に，本システムに実装されている，ネットワーク障害が復旧したかどうかを判定する機能を用いてトラブルシューティングが完了したかどうかを判定する．

以上の流れにより，本システムのトラブルシューティング演習が完了する．学習者は本システムを利用することで，ネットワーク全体の状態を把握して障害が発生している機器を正確に特定する訓練や，発生している障害に対して適切に対処する訓練が可能となる．この訓練を反復実践することで，ネットワーク障害に迅速に対応する能力の習得を支援可能となる．

4. 結論

本稿では，レイヤ 2 に対応したネットワーク障害の自動生成を可能とする演習システムについて述べた．本演習システムは，仮想ネットワーク技術を用いて実装している．本システムを用いることで，低コストで時間や場所を選ばずレイヤ 2，レイヤ 3 の両方の範囲におけるトラブルシューティング演習が即座に実施可能となる．本システムの利用によって，ネットワーク技術者に求められる障害対応能力の習得の支援が期待できる．

謝辞 本研究は JSPS 科研費 24K15238 の助成により実施しました．

参考文献

[1] 総務省：令和 5 年版情報通信白書，入手先<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n4200000.pdf>（参照 2024 年 07 月 25 日）．

[2] 経済産業省：- IT 人材需給に関する調査 - 調査報告書（p.20），入手先<https://www.meti.go.jp/policy/it_policy/jinzai/houkokusyo.pdf>（参照 2024 年 07 月 25 日）．

[3] 総務省：令和 3 年通信利用動向調査報告書（企業編）（p.35），入手先 <https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202100_002.pdf>（参照 2024 年 07 月 25 日）．

[4] 総務省：電気通信サービスの事故発生状況（令和 4 年度），入手先<https://www.soumu.go.jp/main_content/000897675.pdf>（参照 2024 年 07 月 25 日）．

[5] 総務省：令和 5 年 3 月 - 電気通信事故検証会議，入手先<https://www.soumu.go.jp/main_content/000878160.pdf>（参照 2024 年 07 月 25 日）．

[6] Cisco：シスコネットワーキングアカデミー，入手先<https://www.cisco.com/c/m/ja_jp/netacad.html>（参照 2024 年 07 月 25 日）．

[7] 東雲 美幸，吉原 和明，井口 信和：トラブルシューティング演習を可能とするネットワーク演習支援システムの開発，情報処理学会 第 86 回全国大会講演論文集，pp.963-964（2024）．

[8] 立岩 佑一郎，安田 孝美，横井 茂樹：仮想環境ソフトウェアに基づく Linux ネットワークトラブルシューティング実習環境提供システムの開発，情報処理学会研究報告コンピュータと教育（CE），pp.37-44（2007）．

[9] 平畑 聖也，井口信和：擬似演習者ロボットとの協調演習を可能とするネットワークトラブルシューティング演習システム，情報処理学会 第 82 回全国大会講演論文集，pp.725-726（2020）．

[10] Cisco Networking Academy：Cisco Packet Tracer，入手先 <https://www.netacad.com/courses/packet-tracer>（参照 2024 年 07 月 25 日）．

[11] Open vSwitch：Open vSwitch，入手先<https://www.openvswitch.org/>（参照 2024 年 07 月 25 日）．