Virtual MAN: A VLAN Management System for Enterprise Networks

Sunil Dath Krothapalli, Suan Aik Yeo, Yu-Wei Eric Sung, Sanjay G. Rao
Dept. of ECE, Purdue University
West Lafayette, IN, USA
{*skrothap, yeo, sungy, sanjay*}*@purdue.edu*

ABSTRACT

In this demonstration, we present Virtual MAN, a system which addresses plethora of unique challenges network operators face in managing Virtual Local Area Networks (VLANs) in enterprise networks. Despite their wide prevalence in enterprise networks, the management process of VLANs is ad-hoc, error-prone, and has received little systematic treatment in the research community. We have identified the most commonly performed tasks by the network operators when managing VLANs and developed a system to automate these tasks. From an operator standpoint, the system not only provides a network wide view of how VLANs are organized in an enterprise network but also assists them in performing actions like extending current VLANs and configuring new VLANs. Network managers can also use this toolkit to detect and diagnose suboptimal root bridge placements and misconfigurations such as missing and redundant links. The system also provides an interactive graphical interface for visualizing the effect and impact of various VLAN design changes. The system already saw the first deployment of its beta version on Purdue University campus network and is effective in understanding VLANs design and in identifying VLANs with misconfigurations or suboptimal designs.

1. INTRODUCTION

Recent empirical studies have shown most enterprise networks surpass carrier networks in size and design complexity [5, 6]. While the existing research highly focuses on designing abstractions and tools for carrier networks, *e.g.* BGP [7, 4], very little attention has been paid on developing systems for managing enterprise networks. In spite of their prevalence, complexity and striking differences compared to carrier networks, the design and management of enterprise networks is ad-hoc, error prone and has received little systematic treatment in the research community [3].

Virtual Local Area Networks (VLANs) are extensively used in enterprise networks and are often used to ease management of hosts spread over physically disparate locations [3]. Managing VLANs is one of the unique challenges facing network operators of today's enterprise networks. There exists industry standards like Cisco's VLAN Trunking Protocol [1] to better manage VLANs, but are very limited in functionality. To the best of our knowledge there are no real world deployments of any such system or a comprehensive toolkit to manage VLANs in enterprise networks.

In this demonstration, we present the design of Virtual MAN, a VLAN visualization and management system for enterprise networks that can assist network operators in managing VLANs and in identifying misconfigurations. The system provides an interactive and flexible user interface to the network managers to specify top level actions they wish to perform. The graphical interface turns out to be the standout feature for its ability to visualize any enterprise VLAN's topological spread distinctly and clearly, while showing the impact of performing various VLAN design changes.

2. DESIGN GOALS OF VIRTUAL MAN

Virtual MAN has been designed with the following goals in mind: (i) support the most frequent tasks performed by a network manager; (ii) independence from network structure and semantics; (iii) scalability; and (iv) interactivity and flexibility of usage.

Based on our discussions with operators, we have identified visualizing a VLAN's spread, extending a VLAN, configuring a new VLAN, detecting suboptimal root bridge placements and identifying misconfigurations to constitute the most frequently performed VLAN management tasks. The primary goal while building such a system involves designing reliable algorithms that can work with any enterprise network configuration without assuming any network structure and semantics. Moreover, the system should be scalable enough to handle large enterprise networks and produce output in real time. We have invented unique, efficient algorithms and incorporated them in the system to perform the afore mentioned tasks.

Another primary objective is to design a system that is interactive and offers flexibility of usage to the network managers. We achieve this vision through the use of distinct graphical legends and notations to represent normal nodes, nodes that need reconfiguration and links that are misconfigured *e.g. redundant and missing links*. All the above goals contributed to the development of a system that presents a comprehensive view of a VLAN's topological spread to the network operator, while showing the effect and impact of performing various VLAN design changes.

3. INTERFACE OF VIRTUAL MAN

The entire application has been developed using the Java 2 Enterprise Edition framework. The inputs to the system are, (i) a bulk network configuration file, which has the running configurations of all the switches and routers in the network appended together, (ii) a network links file which has layer 2 topological connectivity information. While the configuration files are readily available on routers and switches, it is not a trivial task to obtain the network links file. In a network comprised of Cisco devices, one approach to generate the links information is through the use of Cisco Discovery Protocol.

3.1 Configuration Interface

The configuration interface presents a web interface to the network operator to configure and choose a set of actions he wishes to perform on a VLAN. A network manager can perform variety of actions from viewing a VLAN's spread to finding suboptimal root bridge placements to detecting misconfigurations. It also provides options to customize and anonymize the output views.

3.2 Visualization Interface

The visualization interface of the system is powered by the ZGR Viewer, which is based upon the Zoomable Visual Transformation Machine [2], to generate high quality network graphs. The system primarily supports two output views, (i) a *default view*, which shows the full topological spread of a VLAN, and (ii) a *core view*, which only shows the set of nodes and links attached to the core of the network and is particularly helpful when viewing the spread of large VLANs. The rest of the section presents various actions that can be performed on VLANs using the toolkit.

Viewing a VLAN Spread: The VLAN Spread feature helps the network operator visualize how and where a VLAN is spread across multiple sites via core and access switches, routers in the network. Figure 1 shows the spread of an enterprise VLAN generated using the toolkit. The leaves in the VLAN spread tree are the access switches, which connect to the end hosts of the VLAN. The spread also depicts the configured root bridge and the designated router of the VLAN.

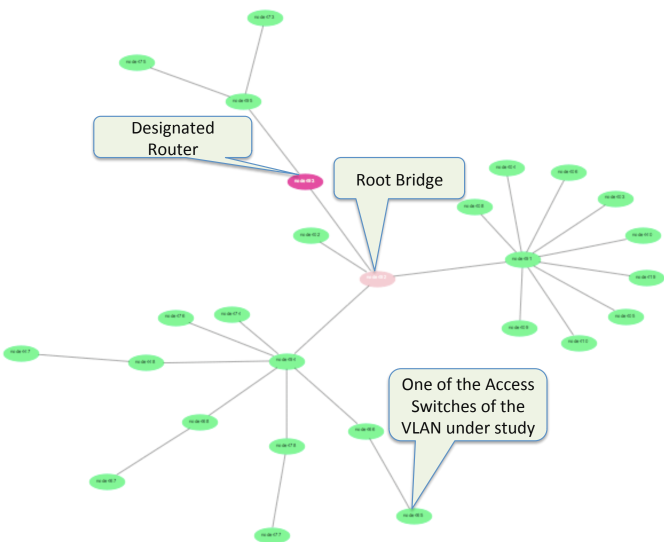

Figure 1: A snapshot of the VLAN Spread

Extending an existing VLAN: More often than not, network operators extend existing VLANs into new areas of an enterprise network as network dynamics change by adding hosts to the access switches. Extending VLANs manually into new locations may lead to redundant or missing links because of manual misconfigurations and automating the process eliminates the possibility of any such potential errors. This particular feature identifies only the links that need new configuration changes in order to permit the input VLAN's traffic after performing an extension.

Detecting misconfigurations: Manual configuration and management of large networks is always error prone and leads to misconfigurations. Very often, we see VLANs being unnecessarily specified on trunk links, which we term as *redundant links*. The other scenario is where a VLAN that should be permitted on a trunk link is not. We call it a *missing link*. These configuration errors lead to superfluous broadcast traffic in the network, unavailability of critical services etc. An interesting point to note here is that Cisco's VTP [1] has the ability to identify redundant links in a VTP domain. But there does not exist any industry standards to detect redundant links across VTP domains or identify missing links. Figure 2 presents one such case *(identifying missing links in a VLAN)* of how to use the system to detect and diagnose misconfigurations.

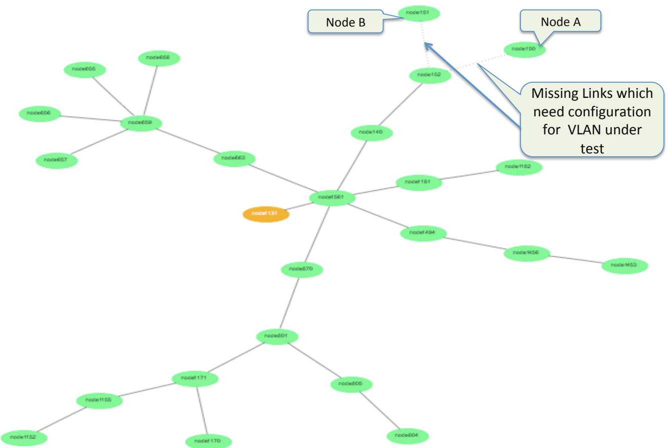

Figure 2: Detecting misconfigurations using Virtual MAN

Apart from the above, Virtual MAN can also be used to identify suboptimal root bridge placements, configure a new VLAN and detect network wide misconfigurations.

4. EVALUATION ON PURDUE UNIVERSITY NETWORK

We conducted a detailed analysis and evaluation of the system using the Purdue University network, which is comprised of a few hundred VLANs and thousands of switches and routers. We compare the results of the toolkit to what is configured manually in real network today. Our results indicate that (i) more than 70% of the VLANs in the network under study have redundant links. In particular, almost 14% of the VLANs have atleast 50 redundant links which highlights the fact that there is a lot of unnecessary traffic in the network outside a VLAN, (ii) around 32% of the VLANs have missing links, which could result in a group of hosts getting disconnected from the rest of the VLAN resulting in unavailability issues. While some of these missing links are a result of real misconfigurations, a significant fraction are a result of configurations that have not been removed even after the end hosts are removed or moved to new VLAN, (iii) despite the significant misconfigurations present in the network, our system showed that 68% of the VLANs have optimal root bridge placements and only 0.7% of the VLANs have 3 more links in their spanning trees than their corresponding minimal spanning trees, which highlights the fact that most of the current root bridge placements are already optimal. The ability to handle most of the VLAN management tasks added with network independence form the distinguishing features of this work.

5. REFERENCES

[1] Understanding vlan trunk protocol. http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml.
[2] Zvtm. http://zvtm.sourceforge.net/.
[3] P. Garimella, Y.-W. E. Sung, N. Zhang, and S. Rao. Characterizing vlan usage in an operational network. In *ACM SIGCOMM workshop on Internet Network Management (INM'07), Kyoto, Japan*, August 2007.
[4] J. Gottlieb, A. Greenberg, J. Rexford, and J. Wang. Automated provisioning of bgp customers. In *IEEE Network Magazine*, Dec. 2003.
[5] F. Le, G. G. Xie, D. Pei, J. Wang, and H. Zhang. Shedding light on the glue logic of the internet routing architecture. In *In Proceedings of ACM SIGCOMM*, 2008.
[6] D. Maltz, G. Xie, J. Zhan, H. Zhang, G. Hjalmtysson, and A. Greenberg. Routing design in operational networks: A look from the inside. In *In Proceedings of ACM SIGCOMM*, 2004.
[7] L. Z. Ying-Ju Chi, Ricardo Oliveira. Cyclops: The as-level connectivity observatory. In *ACM Computer Communication Review*, October 2008.