NETWORK SWITCH SIMULATION MODEL

Zdeněk Kraus
Doctoral Degree Programme (1), FIT BUT
E-mail: xkraus00@stud.fit.vutbr.cz

Supervised by: Petr Hanáček
E-mail: hanacek@fit.vutbr.cz

Abstract: This article describes principles and technologies used in the simulation model of a network switch created in ANSA project. It also contains specification of model architecture. It explains vital functions and modules used by simulation and highlights extendability by other network simulation modules within the ANSA project. Finally it compares experiment result with behaviour of real devices and suggests future development of the model.

Keywords: network, simulation, switch, OMNeT++, MAC, STP, VLAN

1 INTRODUCTION

The simulation model of a network switch was created within the ANSA project that focuses on networks simulation and analysis. The model is capable of basic intelligent switching with Virtual LAN support and redundancy handling mechanism – Spanning Tree Protocol. The model is also very configurable and can be extended by other modules, like Router module to create multilayer switch with routing support. Article is separated into three main parts: Switching principles part formally specifies switching function regards of other network technologies like switching behaviour in network with Virtual Local Area Networks. Active topology enforcement part describes spanning tree protocol function and then highlights different enhancements in further protocol versions. Model part shows model architecture, compares experiment results and outlines extendability of the model with existing modules.

1.1 NETWORK SWITCH

Term Network switch has various (marketing) meanings spread among people. In the original media access control standard [3] device is referred as bridge regardless of enhanced functions and well known name switch. Based on [6] and mentioned standard we can summarize terminology as:

bridge – hub device promiscuously listens to every frame, then retransmit it to (all) other port(s) (separated LANs). It's basically acting as repeater for connected segments.

learning bridge – inteligent hub device forwarding frame only to segment where destination device is located. Location is learned by listening to communication. When location is unknown behaviour falls back to basic bridge.

complete bridge – switch device is able to handle redundant topology without communication loops by using mechanism such as STP.

2 SWITCHING PRINCIPLES

This part describes device function on learning bridge level, then with addition of VLAN support and finally changes towards complete bridge level. It's based on [6, 3, 4].

For further description let these symbols be defined as a – address, s – source address, d – destination address, p – port, v – VLAN identifier, p_s – receiving port, $m = (s, d, m^+)$ – message, where m^+ is a payload (upper layer packet), $m = (s, d, v, m^+)$ – VLAN tagged version of message, $\mathbf{P}$ – set of ports, $(a, p) \in \mathbf{MT}$ – MAC table, holds destination addresses location associated with port, thus location in the segment, $(p, v) \in \mathbf{VT}_p$ – 1:1 port to VLAN mapping, used for resolving untagged frames, it's a portvid-table part of VLAN table, $(v, \mathbf{P}) \in \mathbf{VT}_v$ – 1:N VLAN to port mapping, used for frame access control by restricted by VLAN setup.

2.1 Basic Switching

This mechanism of forwarding frames relies on knowledge of locations of destination nodes[1], that knowledge is represented by MAC Table **MT**. Source address from each forwarded frame is saved in **MT**. If the location of target is known $\exists(a_i, p_j) \in \mathbf{MT}$ then frame is forwarded to particular port p_j, otherwise to all ports except receiving port – same as basic bridge behaviour.

2.2 VLAN Switching

With VLANs the situation is slightly more complex. There is additional table that consist of two separated parts, PortVID-Table $\mathbf{VT}_p$ and VLAN table $\mathbf{VT}_v$. The situation is different as the frame may have VLAN tag or have not.

If frame has no VLAN tag, then its VLAN is determined by $\mathbf{VT}_p$. Then set of destination ports is determined by combination of $\mathbf{VT}_v$ mac **MT** Frame is forwarded to all selected ports and VLAN tag is set regards of tagging settings for particular VLAN on particular port.

Learning of destination addresses is made only if the frame was successfully forwarded to at least one port.

2.3 Switching with Active topology

Switching process is driven by port state that is managed by Active topology enforcement. Receiving and forwarding is operational only on ports that are in Forwarding state. Learning process is modified so it can pre-learn addresses in case the port is in Learning state. Enabling learning sooner is problematic with VLANs, because it cannot be determined if a frame will be successfully forwarded. This functionality is vendor specific.

3 ACTIVE TOPOLOGY ENFORCEMENT

Section is based on [3, 4, 1, 2]. In redundant topology there is more than one connection between some switches. These connections may be located in same segment, thus creating a loop, even with VLANs. Actually it is property that is very requested, because it brings increased reliability of any network (switched, routed, ...).

Solution for redundant topology Spanning Tree Protocol is specified by network standard IEEE 802.1d, protocol that was enhanced few times. As name implies, protocol function is to create a Spanning Tree on a network topology graph. By preventing some links, the protocol creates a loop free topology – Active topology.

When topology changes, the protocol appropriately updates active topology. The protocol needs a unique identifier to reliably resolve priority of particular devices and links. For that purpose, there is a compound identifier specified as (Bridge ID, Port ID, Link Cost), where Bridge ID represents (

[1] broadcast addresses are not subject to learning process, therefore they are not saved in MAC table. That means all broadcast traffic is forwarded to all ports, if other rules are met.

Bridge Priority, MAC Address), Port ID represents (Port Priority, Port Number) and Link Cost is based on link bandwidth. Lower value is better. Comparison of identifiers is made consecutively, that means the first lower value wins the comparison.

3.1 Spanning tree protocol

Original Spanning Tree Protocol is specified by IEEE 802.1d from year 1998 [NON-VIDI]. Protocol exchanges specific frames with priorities. Based on discovered priorities, the value of known best bridge (Root Bridge) is updated in such frames. Port that is connected to Root Bridge with best identifier is selected as Root Port and meant to be operational. Ports able to reach root bridge with worse identifier are selected as Alternate ports. And all other portd without path to Root are selected as Designated also meaning to be operational.

After roles has been selected and no changes occur for a period of time, port stated is set to forwarding for Root and Designated ports, and Blocking for Alternate. By setting all states as appropriate, network is converged. With original Spanning tree protocol, the convergence may take over 45 seconds, with default save values.

3.2 Rapid spanning tree protocol

Newer version od protocol is specified by current version of IEEE 802.1d. It's focused to minimize time of convergence. Basically it amends default values of times to shorten transition between port states.

Additional feature to minimize the time of convergence is Proposal/Agreement mechanism. It is initiated by root bridge and forwarded by consecutive bridges. When proposal arrives, the bridge change status of next ports to Blocking and agrees to the proposal. That means the bridge is synchronized, and originator is permitted to change synchronized ports to Forwarding. That is spread through whole topology until it's synchronized, thus converged. This is powerful mechanism that is able to speed up convergence. Unfortunately all devices have to cooperate, otherwise the convergence falls back to timers.

3.3 Per-VLAN spanning tree

This extension of Spanning tree was created by Cisco Systems, Inc.. Unlike previous versions of the protocol, PVST is able to operate with VLANs. The principle is to have one full instance of Spanning Tree Protocol for one particular VLAN.

That has one advantage. Administrator can specify different paths for particular VLANs, thus making a basic load balancing on network layer. Unfortunately, the solutions has a drawback. Device have to spend much more memory and execution time for managing many instances[2]. Additional modification by Cisco Systems, Inc. was made – RapidPVST+. That utilizes RSTP as instantiated protocol and speeds up convergence.

3.4 Multiple Spanning Tree

Last variant is specified by IEEE802.1q that is focused on active topology with VLAN support and minimizing resources. Function of this protocol is very complex, because it splits network topologies to Regions that share VLAN:Instance mapping and selects Active topology between the regions and additionally within particular regions. Regions behaves like single device from outside.

[2] there is solution to device resources consumption. MISTP – Multiple Instances Spanning Tree Protocol that consolidates more instances to one shared instance, and thus active topology. That is problematic with divergent spread of VLANs.

The unique identifier is extended by Priorities of Common Spanning tree and Instantiated Spanning Tree. When frame is forwarded within region, then uses the Regional Instance of spanning tree, otherwise it is forwarded to Regional root and then within Common spanning tree active topology.

4 MODEL

Section is based on [5], where you can find complete specification of simulation scenarios and model implementations. Simulation model is based on mechanism above. It is capable of VLAN based switching and has Per-VLAN spanning tree. It's highly configurable and has status output same as Cisco System, Inc. switches for better evaluation. Model is implemented in OMNeT++ simulator that utilizes C++ programming language with Tcl/Tk visualization. Development environment is based on Eclipse IDE.

4.1 ARCHITECTURE

Particular functions are managed by separate modules that are connected to Switching core. There is a MAC Table and VLAN Table for storing knowledge of topology. STP process manages port roles and states as appropriate, based on knowledge from VLAN table, and operates MAC tables as needed. Main part, the switching core, manages forwarding of frames based on port states from STP, MAC table and VLAN table. Modularity of the model provides extendability. It's possible to downgrade model to more basic devices such as non-STP bridge, i.e. Learning hub, by removing STP module.

4.2 SIMULATION

Experiments with simulation and real devices show that model successfully simulates real device with VLAN support and Per-VLAN spanning tree, e.g. Cisco Catalyst switches. I compared simulation and real devices behaviour on four specific scenarios. For all four scenarios, the convergence was performed in same manner and with very similar delay time. Simulation scenarios focus on these parts of the model: default behaviour of unconfigured device, restriction of communication within VLANs, convergence and reconfiguration of active topology, and STP functionality within VLANs. Last scenario is shown on Figure 1.

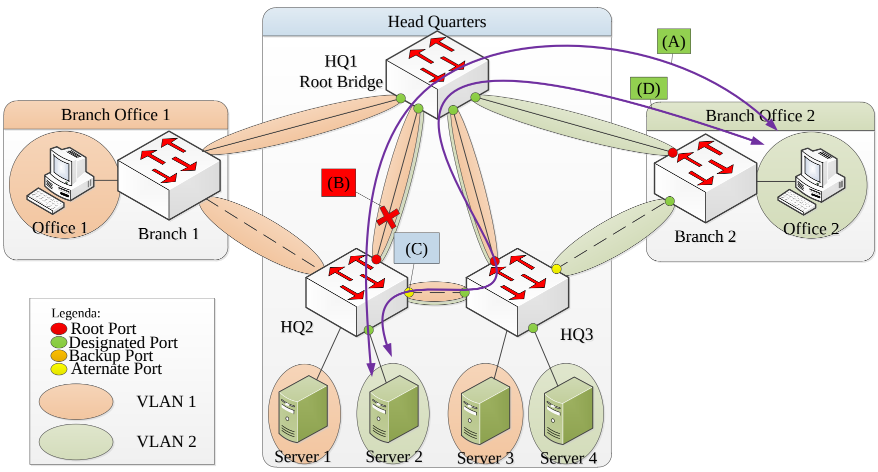

Figure 1: Simulation scenario of STP behaviour with differentiated VLAN topology

In the figure you can see:

A – previously functional path that was established on fully operational network

B – link is broken that causes reestablishment of active topology

C – new path established new root port for that VLAN is selected

D – connection restored on new path

4.3 EXTENDABILITY

The model is prepared to be extended by other modules. Router module could be connected to switching core. There are internal ports to upper layer prepared as well as internal context specifier. That enables Multilayer switching. There is also place to upgrade STP process to other version and replace existing module. Switching core relies only on port states transitions and forwards all STP traffic to STP module.

5 SUMMARY

The simulation model is part of ANSA project held on FIT BUT that focuses on Networks simulation and analysis. This model fills the gap in base network simulation models framework that lacks of proper network switch model. Only learning hub was contained.

The article describes principles of switched network devices and evaluates it's application on simulation model of such device. Evaluation is supported with series of experiments and compared to real device behaviour on particular scenarios.

ACKNOWLEDGEMENT

This article was created within the research plan of the Security-Oriented Research in Information (MSM0021630528). This work was supported by the TeamIT – Building Competitive Research Teams in IT (MŠMT CZ.1/07/2.3.00/09.0067), the Operational Programme Research and Development for Innovations under the IT4Innovations Centre of Excellence project (CZ.1.05/1.1.00/02.0070) and by the project Advanced Secured, Reliable and Adaptive IT (FIT-S-11-1).

REFERENCES

[1] Cisco Systems, I.: Multiple Instance STP (MISTP) / 802.1s: Introduction. [online], [vid. 2012-02-28].
URL http://www.cisco.com/en/US/tech/tk389/tk621/tk844/tsd_technology_support_sub-protocol_home.html

[2] Cisco Systems, I.: Per VLAN Spanning Tree (PVST). [online], [vid. 2012-02-28].
URL http://www.cisco.com/en/US/tech/tk389/tk621/tk846/tsd_technology_support_sub-protocol_home.html

[3] IEEE: *IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges*. IEEE, 2004.

[4] IEEE: *IEEE Standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks*. 2005.

[5] Kraus, Z.: *Modelování a analýza spolehlivosti počítačové sítě VUT*. FIT VUT v Brně, 2011.

[6] Perlman, R.: *Interconnections: Bridges, Routers, Switches and Internetworking Protocols*. Addison-Wesley, druhé vydání, 2001, ISBN 0-201-63448-1.