Using State Model Diagrams to Manage Secure Layer 2 Switches

S P Maj, D Veal

Edith Cowan University, Perth, Western Australia

Summary
A secure network is only as strong as its weakest link. It is recognized that the source of many security breaches are from users within an organization. User endpoints or hosts may be a variety of different devices such as laptops, IP phones and servers. All these user devices are connected via a switch fabric. This switch infrastructure must therefore be appropriately secured. There are standard techniques to provide protection against common attacks such as MAC spoofing, MAC table overflow etc. However, management of OSI layer 2 devices is typically text based using the Command Line Interface. The increasingly prevalent Security Device Manager graphical user interface can be used to configure and manage routers but, currently, cannot be used for securing switches. This paper presents details of using the State Model Diagram user interface for ensuring switches are securely configured.

Key words:
Network Security, State Model Diagrams, Layer 2 security.

1. Introduction

Security must be considered from a multi-dimensional perspective. Physical security is concerned with mechanisms for restricting access to network based devices. Typically a layered approach is employed i.e. restricted and controlled access to buildings, rooms and devices. Network devices must be logically secured by password protection for access via local console and remote Virtual Teletype (vty) connections. In addition to password protection both console and vty lines can be configured to timeout after a specified period of inactivity. Remote device access via the vty lines typically employs the Telnet protocol. Because of security concerns Secure Shell (SSH) is now the preferred option.

After being logically secured OSI layer 2 switch devices must be further configured to prevent security threats. Significantly layer 2 is often considered the weakest security link. OSI layer 2 threats include: MAC address spoofing, MAC address table overflow, STP manipulation, LAN storm attacks and VLAN hopping. Cisco, one of the world's largest suppliers of network equipment, recently released the graphical user interface tool Security Device Manager (SDM) to assist with secure device configuration and management [1]. However SDM currently cannot be used to configure switches. Consequently the standard text based Command Line Interface (CLI) is typically used. Whilst the CLI is a powerful tool it is not only difficult to use but also multiple CLI commands are needed to determine device status. Furthermore a switch fabric may consist of numbers switches which are likely to be distributed in different locations in different buildings.

This paper is an evaluation of State Model Diagrams (SDMs) and a graphical method for secure switch configuration and management.

2. Basic Switch Configuration

A switch fabric typically consists of multiple interconnected switches. The example employed in this paper will be three interconnected switches each with 24 ports. Note, sequential ports numbers are employed for trunking as an aid to clarity. Ports not used as interconnecting trunks are used for end user connections.

Redundant trunk connections between switches are needed to provide reliable communications and hence the Spanning Tree Protocol (STP) must be configured to prevent broadcast storms.

Virtual LAN (VLAN) protocols allow a switch to be segmented into separate VLAN broadcast domains. It is then possible to group hosts together based on a common set of functional requirements regardless of the physical location of the end users. VLANs are used to provide improved network management and security.

Proprietary protocols such as VLAN Trunking Protocol (VTP) are designed to assist network administration by the aggregation of switches into secure domains. The configuration of a new VLAN on one VTP switch server is then automatically distributed to all switches in that domain.

It is possible to aggregate multiple physical trunk connections into a single logical link. This type of link provides scalability and redundancy. Again various proprietary protocols are available such as Fast Etherchannel (FEC). Fast EtherChannel allows multiple physical Fast Ethernet links to combine into one logical channel. All four protocols (STP, VLAN, VTP and FEC) may be represented in a single State Model Diagram (SMD) (figure 1).

Manuscript received September 5, 2010
Manuscript revised September 20, 2010

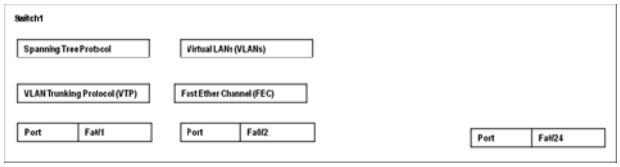

Figure 1. State Model Diagram (SMD)

The SMD method provides hierarchical decomposition and has been proven to be useful not only as a useful pedagogical tool but also a valuable network management tool [1], [2] [3-5], [6]. Hence it is possible to selectively obtain configuration and operational details of each protocol (figure 2).

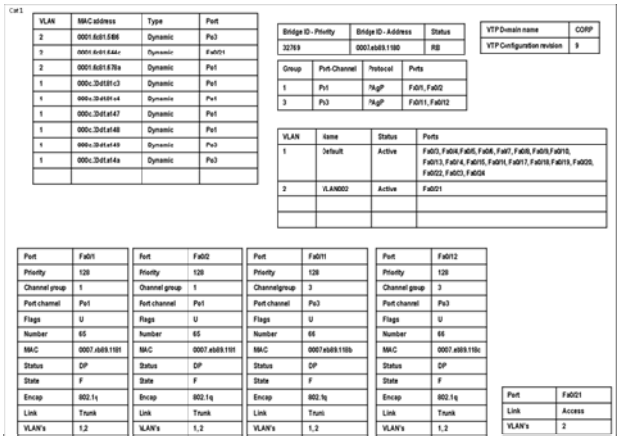

Figure 2. Level 2 SMD

This single diagram represents output obtained for ten different CLI outputs.

1. Show mac-address-table
2. Show spanning-tree
3. Show vlan
4. Show vtp
5. Show etherchannel summary
6. Show interface fa0/1
7. Show interface fa0/2
8. Show interface fa0/11
9. Show interface fa0/12
10. Show interface fa0/21

The advantage of the SMD is that it is possible to concurrently observe the operational status of the different protocols. For example it can be seen that ports fa0/1 and fa0/2 are aggregated into the Fastetherchannel Po1 (group 1) using the Port Aggregation Protocol (PAgP). Link aggregations are treated as single logical links by STP. This can be seen by examining the interface fa0/1 and fa0/2 – both of which now represent a single STP trunk connection. It can be clearly seen that each of these interfaces is now an STP Designated Port (DP) and in the Forwarding state (F) using the trunking encapsulation protocol 802.1q. As trunking interfaces fa0/1 and fa0/2 are no longer assigned to VLANs. It can be clearly seen that interface fa0/21 is in VLAN 2 and is an access port. This switch is an STP root bridge (RB). Furthermore this switch is in the VTP domain CORP and the configuration revision is number 9. Finally, the MAC address table shows the mapping between the learnt MAC addresses and the associated interfaces.

3. Secure Switch Configuration

The SMD method has been successful used to model complex security protocols such as IPSec [7] and dedicated devices such as PIX firewalls [1]. The SMD can also be used for secure switch configuration and management. Minimally the local console and remote vty lines must be secured with passwords and timeouts. However remote vty connectivity should be via the secure Secure Shell (SSH) protocol which has modifiable timeouts and retry attempts All these configuration can be represented using the SMD method (Figure 3).

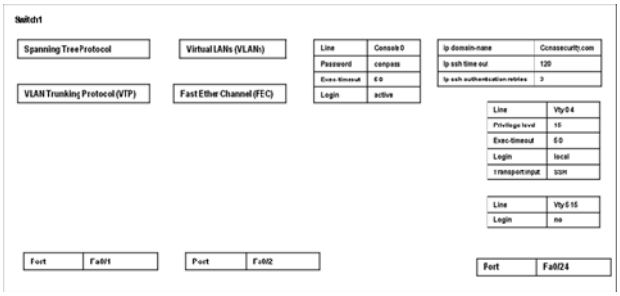

Figure 3. Secure switch console and vty lines

One switch security threat is VLAN hopping. This can be prevented by turning off the Dynamic Trunking Protocol (DTP) on each trunking interface. There are three different types of storm threats – unicast, broadcast and multicast. Each trunking interface can be configured to automatically either SNMP trap or shutdown when traffic levels exceed a predefined level (either %bandwidth or packets per second). To prevent a security breach by rogue switches or spoofing spanning-tree root guard should be enabled on all ports of a switch that are not root ports. All of these security features may be represented on a single SMD representation (figure 4).

None-trunk ports must be enabled as access ports. The portfast protocol allows workstations to become active more quickly without participating in the spanning-tree configuration protocol. Bridge Protocol Data Unit (BPDU) should be configured on each access port thereby preventing a security breach from a rogue switch or spoofing. Unused ports should be disabled.

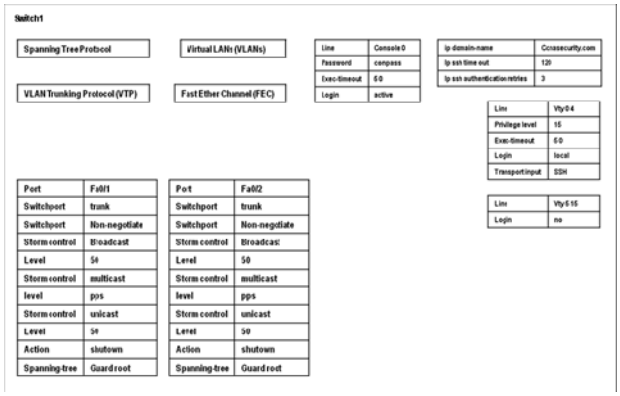

Figure 4. SMD of trunk security protocols

Again disabled and access port secure configurations can be displayed on a single SMD representation (Figure 5).

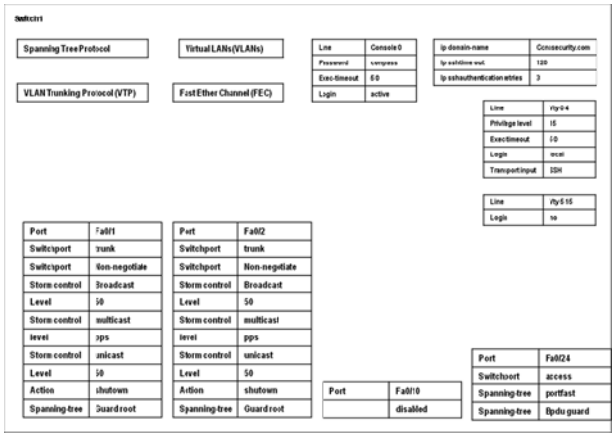

Figure 5. SMD secure access ports

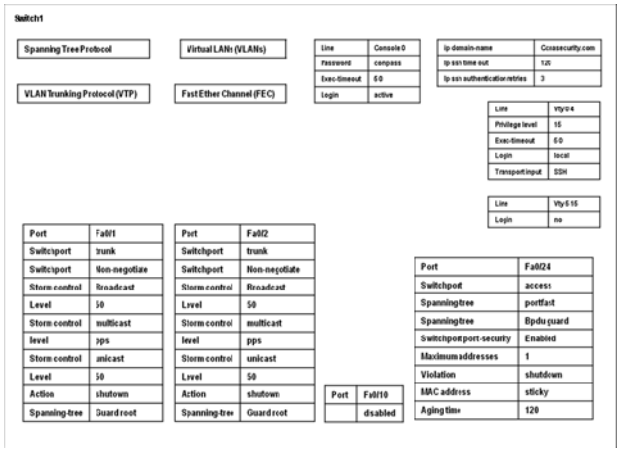

Figure 6. SMD access switchport security

It is recommended that access port security should also block a devices with a MAC address different from one specified for that port (figure 6). It is also possible to allow a range of up to 132 allowed MAC addresses. After MAC address allocation for the interface it is possible to specify the secure MAC address either manually or dynamically (i.e. sticky). Age time should also be configured. Security violation can be configured as either protect, restrict or shutdown. The shutdown mode is further configurable by specifying if the port will be permanently disabled or disabled for a specified time. The restrictive mode allows the port to remain enabled during the security violation and drop only frames from the insecure source.

It can be clearly seen from the above examples that switch configuration is relatively complex involving a number of different protocols such as VTP, STP, VLAN and Fastetherchannel. Configuring a secure switch requires a number of additional configurations. Failure to correctly configure any of the above security standards could result in a breach in security. Using the SMD it is possible to selectively interrogate these security configurations and hence quickly check the security status. The SMD software is currently only capable of managing level 3 devices but, based on these results it is recommended that the software be extended to include level 2 devices.

3. Conclusions

Switch security cannot be either configured or managed from the new Cisco Security Device (SDM) graphical user interface. The alternative CLI is useful but syntactically demanding. Furthermore using the CLI it is not possible to concurrently monitor device status in real-time. However all switch protocols, such as STP, VLAN, VTP and FEC can be configured using the State Model Diagram (SDM) method. This is useful because it is possible to concurrently display not only the active status of each protocol but also their interaction. For example FEC aggregation using Port Aggregation Protocol is employed by STP. The ability to concurrently observe this type of interaction is important not only during configuration and devices management but also during fault diagnosis. Furthermore using the SMD method it is also possible to display the status of security protocols and interfaces. This is important because failure to properly secure a switch can lead to a security breach. For example, using the SMD method it is simple to quickly ensure all ports not configured as either trunk or access are shutdown. The authors recommend the SMD method for secure switch configuration and management.

References

[1] Maj, S.P., Makasiranondh, W., Veal, D., An Evaluation of Firewall Configuration Methods. IJCSNS International Journal of Computer Science and Network Security, 2010. **10**(8): p. 1-7.

[2] Maj, S.P., Veal, D., An Evaluation of State Model Diagrams for Secure Network Configuration and Management. IJCSNS International Journal of Computer Science and Network Security, 2010. **10**(9).

[3] Maj, S.P., G. Kohli, and G. Murphy. State Models for Internetworking Technologies. in IEEE, Frontiers in Education, 34th Annual Conference. 2004. Savannah, Georgia, USA: IEEE.

[4] Maj, S.P., G. Kohli, and T. Fetherston. A Pedagogical Evaluation of New State Model Diagrams for Teaching Internetwork Technologies. in 28th Australasian Computer Science Conference (ACSC2005). 2005. Newcastle, Australia: Australian Computer Society and the ACM Digital Library.

[5] Maj, S.P. and B. Tran. State Model Diagrams - a Systems Tool for Teaching Network Technologies and Network Management. in International Joint Conferences on Computer, Information and Systems Sciences, and Engineering. 2006. University of Bridgeport: Springer.

[6] Maj, S.P. and D. Veal, State Model Diagrams as a Pedagogical Tool - An International Evaluation. IEEE Transactions on Education, 2007. **50**(3): p. 204-207.

[7] Nuangjamnong, C., Maj, S. P., Veal, D. Network Security Devices and Protocols Using State Model Diagrams. in 5th Australian Information Security Management 2007. Edith Cowan University, Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. In 2000 he was nominated ECU University Research Leader of the Year award He was awarded an ECU Vice-Chancellor's Excellence in Teaching Award in 2002, and again in 2009. He received a National Carrick Citation in 2006 for "*the development of world class curriculum and the design and implementation of associated world-class network teaching laboratories"*. He is the only Australian judge for the annual IEEE International Student Competition and was the first Australian reviewer for the American National Science Foundation (NSF) Courses, Curriculum and Laboratory Improvement (CCLI) program.

Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University and be a unit coordinator of all Cisco network technology units. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.