

Using VLAN's for Security and Segmentation

Introduction

A Local Area Network (LAN) is a physical connection of wires used to connect host devices (PC's and Printers) on the same broadcast domain network so that they can communicate with one another [1]. Instead of using physical wires or routers, a Virtual LAN (VLAN) uses software running on a layer 3 switch to segregate devices into separate broadcast networks [2]. A VLAN is similar to a physical LAN in that it allows a group of host devices to be divided into distinct physical broadcast domains or cable segments and still let them communicate together securely as though they are on the same network. Most companies use a combination of LAN and VLAN technology for securing their network communications. This paper outlines the commercial applications of VLAN's for security and segmentation in a network and summarizes the current state-of-the-art usage.

Current Commercial Applications of VLANs

Most companies rely on VLAN's for their primary means of securing their internal network by separating devices into zones of trust or discrete broadcast domains [3]. Although physical separation of networks through the use of routers and switches is the best method of separating zones of trust, this is not always possible in modern complex networks [4]. One example of this is where many devices that are physically close to one another need to be on separate broadcast domains and the expense of separating the domains through routers and switches would be very costly. A VLAN deployed on a layer 3 switch is most commonly employed in networks where the additional expense of a router and multiple switches cannot be afforded or a reduction of hardware is desired.

Although there are many switch manufacturers, Cisco Systems is the industry leader in utilizing VLAN's by implementing VLAN technology in all of their Cisco Catalyst layer 3 series switches. A single Cisco switch running a VLAN can be used in place of two switches and a router, thus saving \$1,925 for the switch and \$1,586 for the router for a total of \$3,511 in savings [5].

Underlying Technology

Overview

A VLAN provides segmentation, network security and traffic flow control which has traditionally been provided by routers. IEEE's 802.1Q working group has developed a VLAN standard that allows users to work with different vendor switches [6]. Unlike bridging, where all traffic flows across the same IP subnet or broadcast domain, each VLAN has a unique IP subnet, thus segmenting traffic on one domain from traffic on another domain [7]. By utilizing different subnets, traffic flow is faster and safer because segmented domains only have to deal with traffic within its own subnet.

Detailed

Cisco has developed a proprietary Virtual Trunking Protocol (VTP) to administer the VLAN's on their switches. VTP shares VLAN information among each switch so that when a VLAN is configured on one switch, it is automatically distributed through all switches in the domain. When a Cisco layer 3 switch receives a data packet header, it compares the incoming domain name to its own and if the name is different, the switch simply ignores the packet [8]. This method provides for excellent network security against attacks such as Frame Tagging, Denial of Service, Flooding and Address Spoofing [3].

Implementation of a VLAN

Moving host devices from one domain to another can be done through VLAN software instead of having to physically move the device to another switch and network. Implementing a VLAN is simple and cheap if the network already contains a Cisco layer 3 switch. Multiple installation documents exist that outline in detail the procedures for setting up a VLAN on an existing switch. Since some Cisco 2900 series switches allow up to 64 VLAN's , then 64 separate broadcast domains can exist in a network on a single switch [9]. Thus, through the use of a single Cisco switch, most companies can provide proper segmentation, security and traffic flow.

- [1] IEEE Computer Society. IEEE Std 802.10, IEEE Standards for Local and Metropolitan Area Networks, 1998.
- [2] “*Virtual LAN*” [Online]. [Accessed: January 15th, 2009, Available: <http://en.wikipedia.org/wiki/VLAN>].
- [3] @stake. Secure use of VLANs: An @stake security assessment. Research report, @stake, August 2002.
- [4] H. F. Tipton and M. Krause, “An Examination of Firewall Architectures”, in *Information Security Management*, 5th Ed. New York: Auerback Publications, 2006, pp. 112-115.
- [5] “Shop CDW” [Online]. Available: <http://www.cdw.com/shop/search/results.aspx?key=cisco+router&searchscope=All&sr=1> [Accessed: January 15th, 2009].
- [6] IEEE Computer Society. IEEE 802.1: 802.1Q – Virtual LANs. Available: <http://www.ieee802.org/1/pages/802.1Q.html>, 2006.
- [7] D. Leifer. Visitor networks. *the Internet Protocol Journal*, 5th ed. pp.2–16, September 2002.
- [8] Cisco Systems, Understanding VLAN Trunk Protocol (VTP), Document ID: 10558, White paper, San Jose, CA, 2007.
- [9] Internetworking Technology Handbook, Cisco Systems, San Jose, CA. 2008.
- [10] R. Seifert. *The Switch Book: The Complete Guide to LAN Switching Technology*. John Wiley & Sons, June 2000, p. 23.