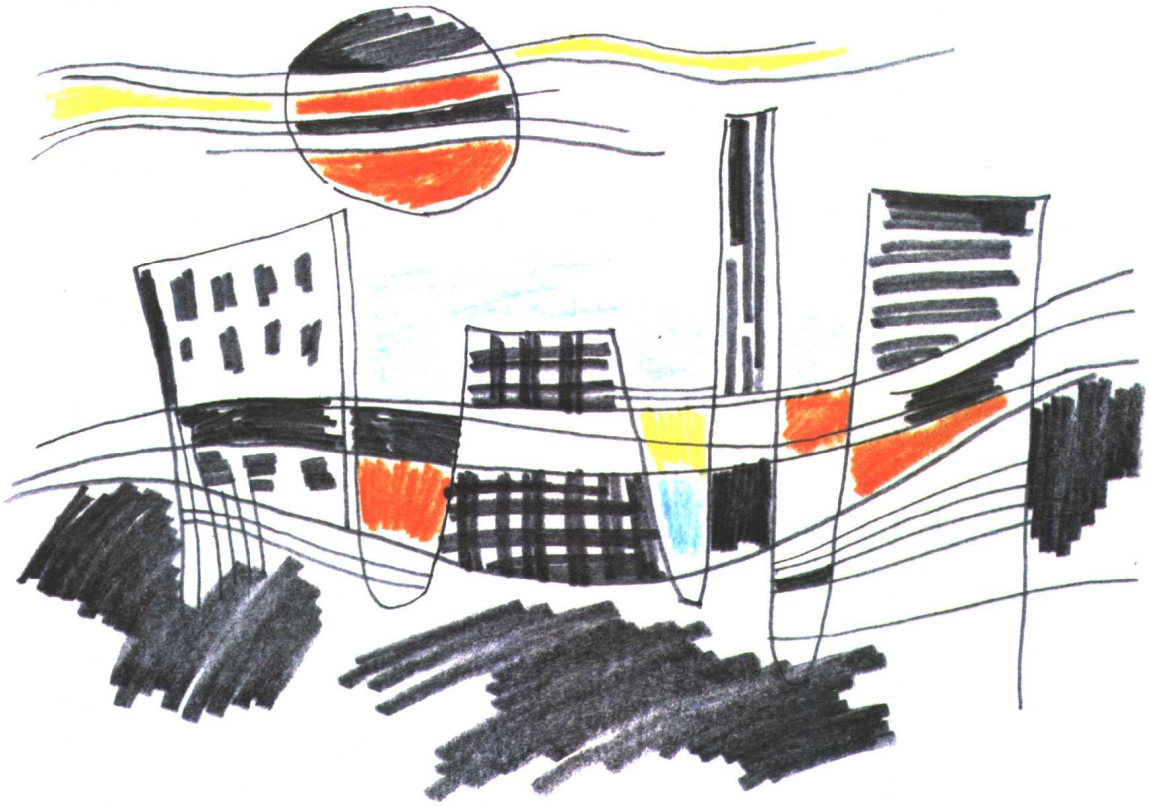
网络新技术系列丛书 影印版

Virtual LANs

虚拟局域网

Marina Smith



清华大学出版社
http://www.tup.tsinghua.edu.cn
McGraw-Hill

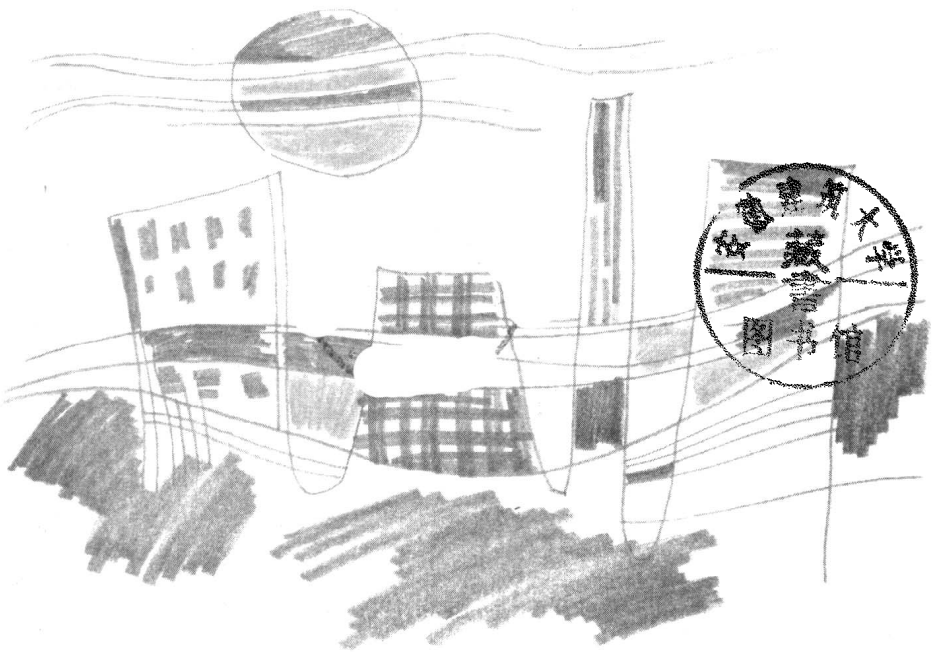
网络新技术系列丛书

影印版

Virtual LANs

虚拟局域网

Marina Smith



清华大学出版社
http://www.tup.tsinghua.edu.cn

McGraw-Hill

(京)新登字 158 号

Virtual LANs/ Marina Smith

北京市版权局著作权合同登记号:01-99-2517

书　名:虚拟局域网
作　者:Marina Smith
出版者:清华大学出版社(北京清华大学学研楼,邮编 100084)
　　http://www.tup.tsinghua.edu.cn
印刷者:清华大学印刷厂
发行者:新华书店总店北京发行所
开　本:787×960 1/16　印张:27
版　次:2000 年 1 月第 1 版　2000 年 1 月第 1 次印刷
书　号:ISBN 7-302-01081-1/TP·2207
印　数:0001～4000
定　价:40.00 元

出 版 前 言

21 世纪人类面对的将是一个网络化的新时代，网络化程度的高低将是衡量一个国家现代化水平和综合国力的重要标志。考虑到我国广大科技工作者面临着网络技术飞速发展的挑战，我们精选了一些反映网络技术最新发展的、且具有权威性的图书，组成“网络新技术系列丛书(影印版)”，奉献给广大读者。既表达对我国广大科技工作者的一种支持，也是我社为我国实施“科教兴国”的战略应尽的义务。

这套丛书包括：千兆以太网、移动 IP、虚拟局域网、交换式局域网、IP 组播技术、虚拟专用网、网络安全技术以及目录使能的网络等一系列先进技术。由于我们水平有限，希望各界专家和广大读者提出建议和要求，促使这套丛书出得更好。

清华大学出版社

1999.12

PREFACE

As companies worldwide change their information technology (IT) infrastructure to accommodate more flexible working practices, they are implementing new types of networking. The subject of one of these new ways, virtual local area networks (VLANs), is much bandied about at the moment. But what are they? How do they work? Do you need them in your networks? The topic is frequently discussed by marketeers, engineers, and network managers. Products are available (just about), although it is doubtful whether they work properly yet. The purpose of this book is to provide network managers and administrators and all readers who have an interest in the subject with general information as to the purpose and implementation of VLANs and detailed information on VLAN construction, operation, and utilization. It aids decision making by stating the case for and against VLANs as a whole, by discussing the different types available (or soon to become available), and by examining the problems that arise with them.

VLANs depends on switching, and a section on that subject will bring the reader up to speed on this latest networking technology. A backgrounder [including the OSI (Open Systems Interconnection) reference model], along with brief reminders as to the types of devices used in local area networks, will fill in any other gaps in the reader's knowledge. Then there is a detailed presentation of how VLANs are constructed and the types available. At present, given the proprietary nature of products now available, and the multiplicity of standards that have a bearing on VLANs, there is a summary of all the relevant standards.

A strong section on management of VLANs guides you through the pitfalls of implementation and is followed by an outline of the security implications of VLAN installation.

A useful feature of this work is the specific implementation notes given for all the major offerings in the field, together with a roundup of several others. The vendors are also briefly profiled.

MARINA SMITH

ACKNOWLEDGMENTS

I could not have done this book alone, even with the availability of information from the World Wide Web. Such information needs interpretation, and for that, and for a lot of help from friends, associates, and vendors, as well as from all the people who put information onto Web pages, I am truly grateful.

I have had a lot of help in the preparation of this book from consultants, vendors, Internet newsgroup correspondents, and friends. I want to thank them all, especially Ken Mann, independent consultant, for his help with the network management and security sections; John M. Wobus of Syracuse University for his DHCP (Dynamic Host Configuration Protocol) information; and James Eibisch for his help with the figures. I am also greatly indebted to Datapro Information Services for support during the preparation of this work and for permission to use parts of several reports within this book, especially to Rob McCombe.

I am also grateful to people at many of the vendors, especially Hamid Karimi (3 Com), Trevor Dearing (Bay Networks), Chris Gabriel (Cabletron), Bill Erdman (Cisco Systems), Ian Cowburn (Digital Equipment), Geoff Bennett (FORE Systems), and Michael Szabados and Mark Powell (Newbridge Networks when it was still UB Networks) for information about their companies' products and about standards and virtual LANs in general.

NOTE

I have been asked to remind all readers that information about the standards, particularly those from the IETF, is freely available on the Internet, as is much information about the vendors and their products.

CONTENTS

CHAPTER 1

Introduction

Before considering the whats and hows of virtual LANS, it is necessary to understand the changing nature of organizational structure and the ways we do business today. (This is explored in Chap. 2.) It is also vital to be fully versed in the structure of networks, especially switched networks. To make sure that we—that is, I as author and you as reader—are all working from the same perspective, an overview of networking is given in Chap. 3. From there we can move on to consider virtual LANs (from now on called VLANs): what they are, and how they work.

What is a virtual LAN? With the multitude of vendor-specific VLAN solutions and implementation strategies, defining precisely what VLANs are has become a contentious issue. VLANs can be seen as analogous to a group of end stations, perhaps on multiple physical LAN segments, that are not constrained by their physical location and can communicate as if they were on a common LAN. A VLAN is basically a limited broadcast domain, meaning that all members of a VLAN receive every broadcast packet sent by members of the same VLAN but not packets sent by members of a different VLAN. All the members of a VLAN are grouped logically into the same broadcast domain independent of their physical location. Adds, moves, and changes are achieved via software within a VLAN. No routing is required among members of a VLAN. The different types of VLANs possible (and there are several) and how they work are described in Chap. 4.

Standards

With so many different VLAN ideas and implementations around, it is essential that a standard be set up. The body that has taken on the task is the IEEE (Institute of Electrical and Electronics Engineers), holder of many of the LAN standards. However, being LAN-oriented, this ignores the work of the other standards bodies in the area, namely, the ATM Forum, the IETF [Internet Engineering Task Force; best known for IP (Internet Protocol) internetworking standards], and the NMForum, for network management—even though it could be argued that VLANs are a management matter. This has resulted in a proliferation of standards around the edges of the topic, which all bear on each other, and have far-reaching effects on the development of VLANs overall. So far, two VLAN standards have been proposed for use, one based on IEEE 802.10 and the other on IEEE 802.1Q. A standard is already set for Emulated LANs under ATM, by the ATM Forum. All the relevant standards are described individually and summarized in Chap. 5; meanwhile, the idea of standards in general is worth considering.

Before any standard for VLANs became moot, some vendors worked out their own VLANs—some purely proprietary, others based on an IEEE standard, but intended for another purpose: security tagging. ATM vendors ignored the issue because it was assumed that when LANE (LAN Emulation) came along, it would take care of it. The IETF had other things on its collective mind, such as inventing dynamic IP alloca-

tion. Unfortunately, it turned out that some VLAN memberships are based on IP addresses, and interoperation with the new and very useful IETF protocol would make the VLANs difficult and, in some cases, impossible, to operate in this way. These examples (and others could be cited, but the point is made) show that just saying "there is a standard for VLANs," which at the time of writing is expected to become possible by late 1997, is not the end of the problem. The next set of problems then appear:

- Migrating proprietary VLANs to the new standard
- Migrating security-tagged VLANs to the same standard as everybody else
- Adding to existing VLANs so that they can use sophisticated internetworking standards

In addition to all this, it is necessary that the vendors, their customers, and the standards bodies decide on what is actually (first) needed and (second) wanted out of the idea of virtual LANs—what are we all working toward. At present, some are simply additions to the network that make it work more efficiently, others are ambitious schemes that make all devices work seamlessly together, and still others are a reinvention of the business practices possible.

Network Management

Network management is discussed in Chap. 6 in terms of relevant SNMP (Simple Network Management Protocol) and RMON (Remote Network Monitoring) functionality and standards. After all, organizations which have installed high-speed and switched networks and advanced technologies, such as VLANs, do so in order to improve network performance. Two of the network manager's most popular management allies have been the protocol analyzer and the SNMP manager. The protocol analyzer allows the network manager to instantly go into a problem network and find and fix the problem which causes a failed or dysfunctional LAN. For many years, another popular tool used to "listen" for a properly functioning network has been the SNMP management station. (This "listening" function is explained in Chap. 3, section on carrier sense multiple access.) If the network is functioning properly, it is the SNMP management station's primary task to display and log

these network statistics in easy-to-interpret information management displays. RMON, for network monitoring, is a widely adopted industry standard for the retrieval of network statistics from remote devices. It comprises two elements: an agent and a client. The agent builds up information within 10 RMON groups. By combining RMON and network management tools with distributed data collection and analysis consoles, a detailed picture of traffic flow patterns, network utilization, and protocol turnaround times can be constructed.

Security

Networks are valuable, both as capital investments and as a critical part of the enterprise. Valuable assets need protection, and corporate managers must protect these assets. The security of the network infrastructure itself, then, is an issue. The management and self-management of the network must be protected, or the network can be deliberately or accidentally brought down. Unfortunately, VLANs do little to ease the security burden, but may actually add to it. Chapter 7 discusses the need for security, how to improve it, and how to ameliorate deficiencies in current VLAN structure. For example, if security is paramount, then the cruder, simpler, types of VLAN are better, although they increase the network manager's burden. Policy-based VLANs, although they sound as if they could implement security policies already in place, are among the least secure. With remote access to a LAN where a VLAN is in place, security is obviously of concern. Chapter 7 also goes into the mechanisms of implementing security policies within VLANs and ELANs (Emulated LANs), the standards, devices, and protocols that protect our networks.

VLANs—Benefits and Problems

There are good reasons why so much attention is being paid to VLANs right now; with large networks being converted to a switched structure, it makes sense to implement VLANs—making the network more efficient and obviating the problems that can come from having a fully switched network, given that switches are, in essence, simply multiport bridges. Costs can also be reduced. Traffic between VLANs is firewalled.

This limits the propagation of multicast and broadcast traffic between VLANs. There is a consistent representation of a VLAN across a VLAN fabric (including one across ATM), so that the shared VLAN knowledge of a particular packet remains the same as the packet travels from one point to another in the VLAN fabric. Chapter 8 looks into these benefits as well as problems not only with implementing VLANs but also the difficulties they can themselves cause. For example, there can be interoperability problems and increased management complexity. It is possible for a VLAN to degrade, rather than enhance, performance. It can also be costly to install and can cause premature discarding of otherwise good equipment. Costs are not only capital—they can also be a matter of time, and some VLANs can be costly in terms of a network manager's time. Others instead can be inflexible from being too automated.

The Vendors

Given the diversity of possible VLAN installations at present, it is wise to consider the major offerings, each on their own merits. In Chap. 9, therefore, the vendor scene is described. There are five large companies in networking: 3Com, Cisco, Bay Networks, Cabletron, and Newbridge Networks. There are lesser vendors which also cannot be ignored, often because of their size in a different market, or because of their large installed base. These vendors have often arisen from a base of competence in one area only to, nowadays, encompass all or most networking technologies. There are other companies which specialize in switching products, and which have made a name for themselves in that niche. Their products are examined with particular relevance to VLANs, and the major offerings are examined in detail together with a few hints on purchasing strategy.

CHAPTER 2

Virtual Organizations*

Businesses, along with the rest of society, are rapidly changing. Many people have told us that society is changing both its private and public faces. Who can deny it when we can see families around us breaking, remarking, and blending, or when we see millions of unemployed people (and usually not from choice) while most of us enjoy longer breaks from, and shorter days at, work?

*This is not an academic text, and I do not want to irritate the reader with constant footnotes and references. For more details on the subject matter of this chapter, the reader can refer to the publications listed in the Bibliography at the end of this book.