

Virtual LANs and NetPilot

How to achieve cost effective and flexible LAN segmentation and security in a NetPilot Environment

With the NetPilot range of secure server appliances providing high performance and very secure transmission capabilities across Wide Area Networks (WANs) using Equinet's TurboVPN features, this paper discusses what can be easily achieved in providing comparable facilities across multiple Local Area Networks (LANs). In particular, this paper examines the benefits of Virtual LANs (VLANs), using NetPilot's ability to interact with IEEE 802.1q switches - for businesses and educational environments alike.

Put at its most simple, a single and comparatively cheap VLAN switch can provide a NetPilot with up to 24 LAN ports which can be independently isolated from each other or combined together to form flexible yet very secure virtual groupings of users and resources.

What is a VLAN ?

A Virtual LAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment – even though they may not be. For example, all the company's financial personnel may be in the same physical office, but their server is located in a server room elsewhere in the building. Ideally this server should be securely isolated from the rest of the organisation with access barred to anyone outside the finance department. In addition all the finance personnel need Internet access out through the corporate NetPilot, however, this facility must be shared by multiple other departments within the organisation. VLANs enable all these types of segmentation and security, extremely easily and cost effectively.

VLAN switches can also take segmentation down to the individual user. For example say all marketing personnel in a company may be spread throughout a building – with no two users physically on the same segment or in the same office. Yet if they are all

assigned to a single VLAN they can share resources and bandwidth as if they were connected to the same physical segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, at the IT manager's discretion. The same need for 'virtual teams' applies in the educational sector, where certain departments may require the same level of segmentation.

This logical grouping of network nodes helps free IT managers from the restrictions of their existing network design and cabling infrastructure. It offers a fundamental improvement in the ease with which LANs can be designed, administered and managed. And since VLANs are software-based, they allow the network structure to quickly and easily adapt to the addition, relocation or reorganization of nodes. No longer does each change necessitate plugging and unplugging patch panels.

Equally important, VLANs help performance needs by segmenting the network more effectively. Unlike standard switching, they restrict the dissemination of broadcast as well as node-to-node traffic, so the burden of extraneous traffic is reduced throughout the network. Security can also be improved for external access when the VLAN is connected to NetPilot - measures can be implemented to restrict access as needed on a per user or per group basis.

LAN evolution towards use of VLANs

Initially LAN routers were used to allow communication between network segments when necessary, while effectively segmenting traffic so that large shared networks were not swamped by excessive traffic. Unfortunately, traditional LAN to LAN routers were slow, complicated and expensive. As the need for faster networks emerged, a new solution was needed.

Switches were the next evolution of network structure. By segmenting the network and providing dedicated bandwidth where needed, they greatly increased performance while reducing cost and complexity. However, traditional switches segment only unicast – or node-to-node, traffic. Unlike routers, they do not limit broadcast traffic (packets that are addressed to all the nodes within a network) or multicast traffic

(packets that are distributed to a specific group of nodes). Crucially, non-VLAN switches offer almost as little security as a hub, whereby a connected user may successful access resources or eavesdrop on packet transmissions of others.

As networks have grown and traffic has increased, IT managers have been forced to segment their networks into more and more switched subnets to meet increasing performance demands. This plays well with VLAN switches, which may be used at the heart of the LAN. By limiting the distribution of broadcast, multicast and unicast traffic, VLANs offer an effective solution to free up not only bandwidth but implement affordable LAN based security.

VLANs coupled with Internet Access Controls in Education

Using the combination of VLAN switches with NetPilot can provide the ideal combination of secure and high performance LAN and WAN infrastructure.

In many schools there is the strong desire to segment the LAN network for security reasons. There is a need to segregate pupil access from teaching and administrative staff resources. Indeed there is a desire to segregate one class from another. However there is also the dilemma that some users, teachers or IT coordinators need the flexibility to get at a wide variety of - or indeed all available – network resources.

Coupled with these varying access requirements for differing LAN users – all users usually need Internet access – but this Internet access must be controlled depending on the category of user. Junior school pupils need differing access rights to senior pupils, as do Teachers, and potentially administrators and IT coordinators.

This segregation and access control can be achieved with a NetPilot coupled to a VLAN switch using IEEE 802.1q protocols. VLAN switches control which group or individuals may communication with LAN attached resources such as the NetPilot, it is NetPilot that then acts as the guardian - controlling content that is then viewed.

NetPilot provides the means to create access profiles for Groups or even individual users. Typically, Internet access rights are defined by membership of a school class or

whether the user is a teacher or IT administrator – perhaps 5 or six different Internet access profiles are established for simplicity - although there is no fixed limit on quantity. Each access profile would block or allow differing categories of content for the group. Obvious content categories to block in all access profiles would be ‘porn’ and similar common undesirables. However, other content containing subject matter like ‘school cheating’ information would be blocked to all pupils – but perhaps not to teachers; and categories like ‘weapons’, or ‘sex’, may need to be legitimately view by older pupils, but not their younger counterparts.

Do we have to completely re-cable our Network to implement a VLAN ?

No ! Some re-arrangement will be necessary at your wiring cabinet / patch panel. If your network comprises purely Ethernet hubs, or even includes simple non-VLAN switches, then these can all be patched through to the new VLAN switch acting as the head-end of your new network.

Perhaps you already have a hub in each class room or on each floor of your office complex. These would be fed through to their own port on the VLAN switch. Similarly NetPilot and other resources such as servers, to be accessed by all or selected users/groups would be given their own VLAN port. The IT manager then has two configuration choices configuring for :

a) Port-Based VLAN

This is the simplest implementation to manage. Each incoming port devoted to user (group) connectivity – be it pupils or workers – is given distinct access rights to central resources. For example Teachers and Administrators have access to central servers and the NetPilot. Pupils have no access to the Teachers resources or servers, no access to other classrooms and only the Internet access defined by the NetPilot.

b) MAC address based VLAN

The VLAN membership is defined by the user’s PC MAC address. This provides both the organisation and the individual with an extremely flexible method of providing security. For example a worker could be

asked to move offices, yet merely by plugging his PC at the new location the VLAN uses exactly the same access rights – regardless of the new physical location. Similarly if a teacher wishes to use a laptop computer linked to a classroom hub, he could have the same access rights as if he were sat in the staff room, while co-located pupil PCs still only have the limited rights associated with that device. The overhead with this mechanism is that the IT manager has to maintain a table of MAC addresses and their VLAN membership criteria.

Which VLAN products and at what price ?

There are a variety of manufactures with potentially suitable products including Netgear, 3Com, Cisco and D-Link. The bigger known names like Cisco and 3Com have both 12 and 24 port VLAN switch offerings, which have street prices of between £500 and £700 pounds. Netgear and D-Link both have 24 port offerings which can be purchased at under £400 – incredible value in our opinion for the technology provided.

Products that Equinet have tested to be compatible with NetPilot include the Netgear FSM726. This product has extremely easy to use interfaces – either via command line or graphical display. It's very good value at about £16 per port.

A list of some of the available VLAN products is given below.

123633 3C16981A-UK	SuperStack 3 3300 - Switch - 12 Port(s) - 10Base-T, 100Base-TX - 100 Mbps - EN, Fast EN
123639 3C16980A-UK	SuperStack 3 3300 - Switch - 24 Port(s) - 10Base-T, 100Base-TX - 100 Mbps - EN, Fast EN
134939 3C17203-UK	SuperStack 3 Switch 4400 - Switch - 24 Port(s) - 10Base-T, 100Base-TX - 100 Mbps - EN, Fast EN
171489 FSM726SUK	Netgear 24 port 10/100 Switch + 2 GENT slots Managed switch
149787 WS-C2950-12	Cisco Catalyst 2950-12 Switch with 12x10/100Base-T Ports and Cisco Cluster Management Suite Software
149786 WS-C2950-24	Cisco Catalyst 2950-24 Switch with 24x10/100Base-T Ports and Cisco Cluster Management Suite Software

Major Benefits of VLANs

- **Greatly enhance security with Virtual Segmentation**
- **Interoperability with VPNs and Internet Access Controls**
- **Better Performance**
- **Simple Management**

Summary

VLANs offer fundamental improvements to the LAN infrastructure, by providing flexible segmentation down to the user level, increasing overall performance and greatly enhancing security.

NetPilot's TurboVPN features designed for secure high performance connectivity between sites using WAN connectivity, can be cost effectively matched in the LAN environment by using VLAN technology provided by a number of compatible switch products.