

Overview of Routing between Virtual LANs

This chapter provides an overview of virtual LANs (VLANs). It describes the encapsulation protocols used for routing between VLANs and provides some basic information about designing VLANs.

What Is a Virtual LAN?

A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs. Several key issues need to be considered when designing and building switched LAN internetworks.

- LAN Segmentation
- Security
- Broadcast Control
- Performance
- Network Management
- Communication between VLANs

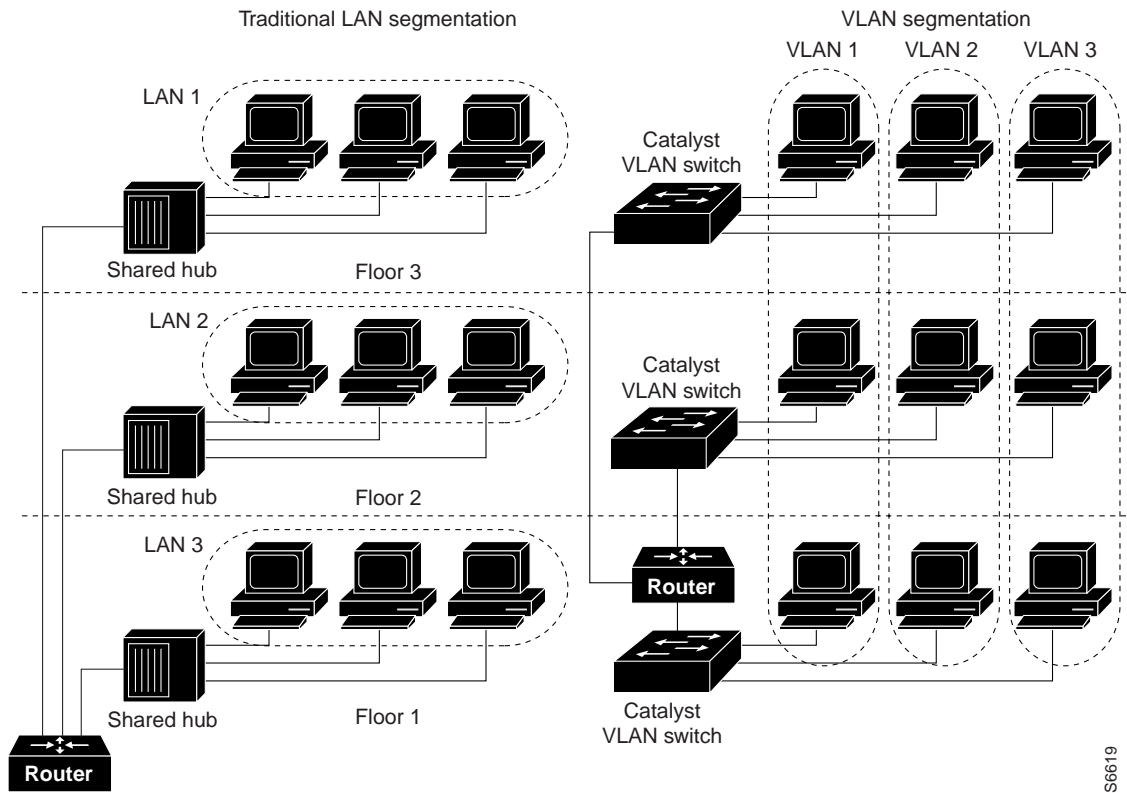
LAN Segmentation

VLANs allow logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains

whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.

Figure 8 illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation.

Figure 8 LAN Segmentation and VLAN Segmentation



Security

VLANs also improve security by isolating groups. High-security users can be grouped into a VLAN, possible on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Just as switches isolate collision domains for attached hosts and only forward appropriate traffic out a particular port, VLANs provide complete isolation between VLANs. A VLAN is a bridging domain and all broadcast and multicast traffic is contained within it.

Performance

The logical grouping of users allows an accounting group to make intensive use of a networked accounting system assigned to a VLAN that contains just that accounting group and its servers. That group's work will not affect other users. The VLAN configuration improves general network performance by not slowing down other users sharing the network.

Network Management

The logical grouping of users allows easier network management. It is not necessary to pull cables to move a user from one network to another. Adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.

Communication between VLANs

Communication between VLANs is accomplished through routing, and the traditional security and filtering functions of the router can be used. Cisco IOS software provides network services such as security filtering, quality of service (QoS), and accounting on a per VLAN basis. As switched networks evolve to distributed VLANs, Cisco IOS provides key inter-VLAN communications and allows the network to scale.

VLAN Colors

VLAN switching is accomplished through *frame tagging* where traffic originating and contained within a particular virtual topology carries a unique VLAN identifier (VLAN ID) as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions based on the embedded VLAN ID. Each VLAN is differentiated by a *color*, or VLAN identifier. The unique VLAN ID determines the *frame coloring* for the VLAN. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN (by the VLAN ID).

The VLAN ID allows VLAN switches and routers to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips header and forwards the frame to interfaces that match the VLAN color. If you are using a Cisco network management product such as VlanDirector, you can actually color code the VLANs and monitor VLAN graphically.

Why Implement VLANs?

Network managers can group logically networks that span all major topologies, including high-speed technologies such as, ATM, FDDI, and Fast Ethernet. By creating virtual LANs, system and network administrators can control traffic patterns and react quickly to relocations and keep up with constant changes in the network due to moving requirements and node relocation just by changing the VLAN member list in the router configuration. They can add, remove, or move devices or make other changes to network configuration using software to make the changes.

Issues regarding benefits of creating VLANs should have been addressed when you developed your network design. Issues to consider include

- Scalability
- Performance improvements

- Security
- Network additions, moves, and changes

Communicating between VLANs

Cisco IOS provides full-feature routing at Layer 3 and translation at Layer 2 between VLANs. There are three different protocols available for routing between VLANs:

- Inter-Switch Link (ISL)
- IEEE 802.10
- ATM LAN Emulation

All three of these technologies are based on OSI Layer 2 bridge multiplexing mechanisms.

Inter-Switch Link Protocol

Inter-Switch Link (ISL) protocol is used to inter-connect two VLAN-capable Fast Ethernet devices, such as the Catalyst 5000 or 3000 switches and Cisco 7500 routers. The ISL protocol is a packet-tagging protocol that contains a standard Ethernet frame and the VLAN information associated with that frame. The packets on the ISL link contain a standard Ethernet, FDDI, or token-ring frame and the VLAN information associated with that frame. ISL is currently supported only over Fast Ethernet links, but a single ISL link, or trunk, can carry different protocols from multiple VLANs.

IEEE 802.10 Protocol

The IEEE 802.10 protocol provides connectivity between VLANs. Originally developed to address the growing need for security within shared LAN/MAN environments, it incorporates authentication and encryption techniques to ensure data confidentiality and integrity throughout the network. Additionally, by functioning at Layer 2, it is well suited to high-throughput, low-latency switching environments. IEEE 802.10 protocol can run over any LAN or HDLC serial interface.

ATM LANE Protocol

The ATM LAN Emulation (LANE) protocol provides a way for legacy LAN users to take advantage of ATM benefits without requiring modifications to end-station hardware or software. LANE emulates a broadcast environment like IEEE 802.3 Ethernet on top of an ATM network that is a point-to-point environment.

LAN Emulation makes ATM function like a LAN. LAN Emulation allows standard LAN drivers like NDIS and ODI to be used. The virtual LAN is transparent to applications. Applications can use normal LAN functions without dealing with the underlying complexities of the ATM implementation. For example, a station can send broadcasts and multicasts, even though ATM is defined as a point-to-point technology and doesn't support any-to-any services.

To accomplish this, special low-level software is implemented on an ATM client workstation, called the LAN Emulation Client or LEC. The client software communicates with a central control point called a LAN Emulation Server, or LES. A Broadcast and Unknown Server (BUS) acts as a central point to distribute broadcasts and multicasts. The LAN Emulation Configuration Server (LECS) holds a database of LECs and the ELANs they belong to. The database is maintained by a network administrator.

These three protocols are described in detail in the *Cisco Internetworking Design Guide*.

VLAN Interoperability

Cisco IOS features bring added benefits to the VLAN technology. Enhancements to ISL, IEEE 802.10, and ATM LAN Emulation (LANE) implementations enable routing of all major protocols between VLANs. These enhancements allow users to create more robust networks incorporating VLAN configurations by providing communications capabilities between VLANs.

Inter-VLAN Communications

The Cisco IOS supports full routing of several protocols over ISL and ATM LANE virtual LANs. IP, Novell IPX, and AppleTalk routing are supported over IEEE 802.10 VLANs. Standard routing attributes, such as network advertisements, secondaries, and help addresses are applicable and VLAN routing is fast switched. Table 6 shows protocols supported for each VLAN encapsulation format and corresponding Cisco IOS releases.

Table 6 Inter-VLAN Routing Protocol Support

| Protocol | ISL | ATM LANE | IEEE 802.10 |
|---|--------------|-----------------|--------------------|
| IP | Release 11.1 | Release 10.3 | Release 11.1 |
| Novell IPX (default encapsulation) | Release 11.1 | Release 10.3 | Release 11.1 |
| Novell IPX (configurable encapsulation) | Release 11.3 | Release 10.3 | Release 11.3 |
| AppleTalk Phase II | Release 11.3 | Release 10.3 | |
| DECnet | Release 11.3 | Release 11.0 | |
| Banyan VINES | Release 11.3 | Release 11.2 | |
| XNS | Release 11.3 | Release 11.2 | |

VLAN Translation

VLAN translation refers to the ability of the Cisco IOS software to translate between different virtual LANs or between VLAN and non-VLAN encapsulating interfaces at Layer 2. Translation is typically used for selective inter-VLAN switching of non-routable protocols and to extend a single VLAN topology across hybrid switching environments. It is also possible to bridge VLANs on the main interface; the VLAN encapsulating header is preserved. Topology changes in one VLAN domain do not affect a different VLAN.

Designing Switched VLANs

By the time you are ready to configure routing between VLANs, you will have already defined them through the switches in your network. Issues related to network design and VLAN definition should be addressed during your network design. Refer to the *Cisco Internetworking Design Guide* and appropriate switch documentation for information on these topics:

- Sharing resources between VLANs
- Load Balancing
- Redundant Links
- Addressing
- Segmenting Networks with VLANs

Segmenting the network into broadcast groups improves network security. Use router access lists based on station addresses, application types, and protocol types.

- Routers and their Role in Switched Networks

In switched networks, routers perform broadcast management, route processing and distribution, and provide communications between VLANs. Routers provide VLAN access to shared resources and connect to other parts of the network that are either logically segmented with the more traditional subnet approach or require access to remote sites across wide-area links.