ISSN 2320 – 6675 EISSN 2320 – 6853

discovery Engineering

VLAN & Its Implementation over ATM by using IP: a communication

Komal Sharma☼, Meenu Yadav, Megha Pundir, Isha Malhotra, Jaskaran Singh

Dronacharya college of engineering, Gurgaon, Haryana-06

☼Correspondence: Dronacharya College of Engineering, Gurgaon, India

Publication History
Received: 17 September 2013
Accepted: 25 October 2013
Published: 1 November 2013

Citation
Komal Sharma, Meenu Yadav, Megha Pundir, Isha Malhotra, Jaskaran Singh. VLAN & Its Implementation over ATM by using IP: a communication. *Discovery Engineering*, 2013, 2(8), 105-109

1. INTRODUCTION

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN or VLAN. This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through *tagging*, so that a single interconnect (*trunk*) may be used to transport data for various VLANs. Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

1.1. VLAN

To understand VLANs, it is first necessary to have an understanding of LANs. A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Communications with devices on other LAN segments requires the use of a router.

Virtual LANs (VLANs) can be viewed as a group ofdevices on different physical LAN segments whichcan communicate with each other as if they were allon the same physical LAN segment. Switches using VLANs create the same division ofthe network into separate broadcast domains but donot have the latency problems of a router. Switches are also a more cost effective solution.

2. USES OF VLAN

Network architects set up VLANs to provide the segmentation services traditionally provided only by routers in LAN configurations. VLANs address issues such asscalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. By definition, switches may not bridge IP traffic between VLANs as doing so would violate the integrity of the VLAN broadcast domain. VLANs can also help create multiple layer 3 networks on the same layer 2 switch. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured to get its IP from a DHCP server. By using VLANs you can easily split the network up so some hosts won't use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server. Hosts may also use a DNS server if a DHCP server is not available. VLANs are layer 2 constructs, compared with IP subnets, which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent layer 2 and layer 3 constructs that map to one another and this correspondence is useful during the network design process. By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration. Partitioning a local network into several distinctive segments for e.g.

- production
- Voice over IP
- network management
- storage area network (SAN)
- guest network
- demilitarized zone (DMZ)

in a common infrastructure shared across VLAN trunks can provide a very high level of security with great flexibility to a comparatively low cost. Quality of Service schemes can optimize traffic on trunk links for realtime (VoIP) or low-latency requirements (SAN). VLANs could also be used in a school or work environment to provide easier access to local networks, to allow for easy administration, and to prevent disruption on the network.In cloud computing VLANs, IP addresses, and MAC addresses on them are resources which end users can manage. Placing cloud-based virtual machines on VLANs may be preferable to directly on the Internet to avoid security issues.

3. VLAN TYPES

There are 2 Types of VLAN

• Three basic VLAN memberships fordetermining and controlling how a packetentering a switch gets assigned to a VLAN.

• The network IP subnet address can be usedto classify VLAN membership

• IP addresses are used only as a mapping todetermine membership in VLAN's.

• In Layer 3 VLAN's; users can move theirworkstations without reconfiguring their network addresses. The only problem is thatit generally takes longer to forward packetsusing Layer 3 information than using MACaddresses.

4. IMPLEMENTATION

A basic switch not configured for VLANs has VLAN functionality disabled or permanently enabled with a *default VLAN* that contains all ports on the device as members. Every device connected to one of its ports can send packets to any of the others. Separating ports by VLAN groups separates their traffic very much like connecting the devices to another, distinct switch of their own. Configuration of the first *custom* VLAN port group usually involves removing ports from the default VLAN, such that the first custom group of VLAN ports is actually the second VLAN on the device, in addition to the default VLAN. The default VLAN typically has an ID of 1. If a VLAN port group were to exist only on one device, no ports that are members of the VLAN group need to be tagged. These ports would hence be considered "untagged". It is only when the VLAN port group is to extend to another device that tagging is used. Since communications between ports on two different switches travel via the uplink ports of each switch involved, every VLAN containing such ports must also contain the uplink port of each switch involved, and these ports must be tagged. This also applies to the default VLAN. Some switches either allow or require a name be created for the VLAN, but it is only the VLAN group number that is important from one switch to the next. Where a VLAN group is to simply

Komal Sharma et al.
VLAN & Its Implementation over ATM by using IP: a communication,
Discovery Engineering, 2013, 2(8), 105-109,
www.discovery.org.in/de.htm

pass through an intermediate switch via two pass-through ports, only the two ports must be a member of the VLAN, and are tagged to pass both the required VLAN and the default VLAN on the intermediate switch. Management of the switch requires that the administrative functions be associated with one of the configured VLANs. If the default VLAN were deleted or renumbered without first moving the management connection to a different VLAN, it is possible for the technician to be locked out of the switch configuration, requiring a forced clearing of the device configuration (possibly to the factory default) to regain access. Switches typically have no built-in method to indicate VLAN port members to someone working in a wiring closet. It is necessary for a technician to either have administrative access to the device to view its configuration, or for VLAN port assignment charts or diagrams to be kept next to the switches in each wiring closet. These charts must be manually updated by the technical staff whenever port membership changes are made to the VLANs. Remote configuration of VLANs presents several opportunities for a technician to cut off communications accidentally and lose connectivity to the devices they are attempting to configure. Actions such as subdividing the default VLAN by splitting off the switch uplink ports into a separate new VLAN can suddenly terminate all remote connectivity, requiring the device to be physically accessed at the distant location to continue the configuration process. VLANs can logically group networks so that the network location of users is no longer so tightly coupled to their physical location.

4.1. Technologies able to implement VLANs are

- Asynchronous Transfer Mode (ATM)
- Fiber Distributed Data Interface (FDDI)
- Ethernet
- HiperSockets
- InfiniBand

5. WHY USE IP OVER ATM?

- Why IP?

IP is the dominant global data communicationsstandard.

- Why ATM?

ATM natively supports a specific Quality ofService. ATM is defined and available at higherspeeds than competing technologies. ATM is currently the enabling technology for the Internet.

• **IP over ATM** is an established and proven combination. The question is to find the best method of running IP over ATM. It is extremely common for Internet ServiceProviders (ISPs) to make use of an ATM core, tointerconnect a number of IP routers. Looking back tothe early 1990s, Internet Service Provider (ISP) networksconsisted of routers interconnected by leased lines. Examples of leased lines are E1 and E3in Europe, operating at 2 Mbit/s and 34 Mbit/s respectively, and TI and T3 in the USA, operating at 1.5 Mbit/s and 45 Mbit/s respectively. However, with the growth rate of the Internet ISP network operators were forced to migrate to higher-speed technologies by the mid-1990s. At that time, ATM was available at the higher speed of 155 Mbit/s, and soon after at 622 Mbit/s. High-capacity ATM switches were also significantly less expensive than high-capacity IP routers. Consequently, ATM became the backbone technology of choice for practically all of the world's large ISPs.

• IP over ATM enables the use of low cost equipment which provides very high speed forwarding

• Also traffic engineering very difficult to equally load the resources on a network can be done by assigning metrics to different links In practice this is quite rudimentary easier to perform traffic engineering by manually defining PVCs.

5.1. Running IP over ATM - the Issues

• IP is connectionless addressing
• IP routing ATM is connection orientated
• ATM addressing
• ATM routing
• ATM signalling

According to the points we have made so far, we can see that internetworking IP and ATM is not new, but is an established and proven combination. In fact, ATM is currently the enabling technology for the Internet.

5.2. Some significant problems faced in internetworking, IP and ATM

1. IP is a network layer protocol, that is, it can't berun 'on the wire'.
It has to be run 'over' something, in this case, ATM. In the LAN, IP is usually run over Ethernet.
2. IP is connectionless, ATM is connection orientated. Accordingly, ATM uses signaling protocols to set up connections. Being connectionless, IP has no need for signaling.

Komal Sharma et al.
VLAN & Its Implementation over ATM by using IP: a communication,
Discovery Engineering, 2013, 2(8), 105-109,
www.discovery.org.in/de.htm

3. Both IP and ATM have routing protocols, that is, protocols that update each node running them about the structure of the network. IP routing protocols, such as Open Shortest Path First (OSPF), the Routing Information Protocol (RIP), the Border Gateway Protocol (BGP), and ATM routing protocols such as Private Node-to-Node Interface (PNNI), are incompatible.

4. IP and ATM use different addressing schemes. IP Addresses and ATM Addresses

• ATM address 20 Bytes:

47.009181000000006170530118.00400BFF001

3.00 (Written in hexadecimal)

• IP Address 4 Bytes: 220.190.40.56 (Written in

dotted decimal notation)

IP addresses and ATM addresses are completely different. There is no correlation between them, that is, an ATM address does not contain an IP address. If you are given just an ATM address of a particular component, you cannot deduce that component's IP address directly from the ATM address. Recall that ATM addresses is 20-bytes long, consisting of a 13- byte prefix, a six byte end station identifier and a one-byte selector field. The prefix is assigned by an administrator, but the end station identifier portion is the MAC address of the ATM interface. Thus, ATM addresses are bound to specific interfaces. By contrast, an IP address is 4 bytes long and is assignedby an administrator. IP addresses only have a logicalbinding to interfaces.

6. VLAN OPERATION

In order to facilitate routing between IP subnet VLAN, each switch needs to know the location of the router. Each switch must have at least one port that is on the forwarding path to the router. This can be achieved by having the router sending periodic multicast VLAN packet to all the switch ports that are in hybrid or trunk mode. Switch port that receives this packet must be member of all VLANs, otherwise the routing process will not work. Every second, the active router sends out a multicast VLAN packet to all the switches in the network. The packet consists of a multicast destination MAC address of 0100-0000-0001. Switch that receives this packet will forward it to all its neighboring switches immediately via all ports in hybrid or trunk mode. This packet is not forwarded to switch ports in access mode to ensure that end stations do not receive this packet. The switch will mark the port that receives this packet as a default VLAN port. Whenever, there is a broadcast, multicast, unknown unicast packet or packet destined to the router, the packet will be forwarded to this port. On the same point to point switch link, a default VLAN port can never be connected to another default VLAN port. Therefore default VLAN port may not receive all broadcast, multicast and unknown unicast traffic sent by its neighboring switch on the same link. The multicast VLAN packet sent by router contains needs very little information. The packet format is proprietary and 64 bytes in length. It consists of source MAC address, destination MAC address, length and a field indicating that it is a VLAN multicast packet. The number of packets need to be sent into the network to maintain this IP subnet VLAN are equal to the number of active spanning tree links in the network plus the link to the router.

7. PROS & CONS OF VLAN'S

7.1. Pros

1. Flexibility - at the allocation from nodes to network segments, independent from the physical location.
2. Easy Management - it is easy to configure large networks using VLAN technology even if the networks are spread across large geographic distances, an administrator is able to manage the entire global network from a single location where the main switching is done. Additionally it requires very little overhead if using a VLAN based on ports which reduces the managerial burden even more for some networks.
3. Physical Layer Independence - VLANs are independent on the physical topology and medium over which the network is connected. It is possible to use VLAN technology over a network consisting even of different physical mediums and on the user level this will be completely transparent. In addition the network can span across a large physical distance and even go through an ATM cloud while staying transparent to the users of the same VLAN which could be located across different countries around the globe.
4. Performance - For example a specific data traffic such VoIP in a VLAN and the transmission into this VLAN can be prioritizes. Frequently the reason is simply to reduce the broadcast domains so that broadcast don't spread on the entire network.
5. Security - VLANs provide inherent security to the network by delivering the frames only within the destined VLANs when sending broadcasts and to the specific recipient within the destined VLAN when a regular frame. This makes it much harder to sniff the traffic across the switch as it will require to both sniff the specific port and not just any port - which allows for extra security. Furthermore when dividing user by VLANs it is possible to make the division according to some security policy and offer sensitive data only to users on a given VLAN without exposing the

Komal Sharma et al.
VLAN & Its Implementation over ATM by using IP: a communication,
Discovery Engineering, 2013, 2(8), 105-109,
www.discovery.org.in/de.htm

information to the entire network. Switched network are watched as unsafe because there existsa lot of attack possibilities such as ARP-Spoofing. Routing, which is the only communication possibility between VLANs, is immune to such layer-2-attacks. Moreover routing offers the opportunity to use firewalls, whereby the security becomes increased.

6. Cost - Using a network switched with VLANs is cheaper than creating a routed network with expensive routers as routers cost a lot more then switches in general.

7.2. Cons

1. VLANs limit - it is possible to create only 4094 different VLANs for the same network, because of the 12 bit VID identifier. Each VLAN has its own unique ID between 0 and 4096, whereby 0 and 4096 are reserved, thus the switch knows where to route the frame. This should be more than enough for today, in most companies but could prove as a bottleneck in the future in the same manner IPV4 did.

Managerial Overhead - when using hard configured VLANs such as port based or MAC based it requires quite a lot of managerial work to manage the networks as they evolve and change with time (keeping track of port assignment or MAC assignment per VLANs is time consuming). On the other hand the usage of Subnet based VLANS requires stronger switches which cost more money, and also adds additional switching latency because it is required to decipher the layer 3 header partially.

RESOURCES

1. Chan WaiKok, M. Salim Beg Simple IP SubnetVLAN Implementation 1Faculty of InformationTechnology, 2 Faculty of EngineeringMultimedia University, CyberJaya, 63100,Malaysia, Ninth IEEE International Conferenceon Networks (ICON.01).
2. Sincoskie, WD (2002) "Broadband packet switching: a personal perspective." IEEE Commun 40: 54-66
3. VLAN IMPLEMENTATION USING IP OVER ATM by Pankaj D. Khambre, Amit Kumar and M.D. Gayakwad in IJES